

## 業務説明資料

本説明書に記載した内容には、現在検討中のものも含まれるため、本プロポーザルのみの設定条件とし、将来の業務（設計）実施の条件となるものではありません。

### 1 件名

放課後キッズクラブ等入退室管理・入所申込システム開発業務委託

### 2 総則

横浜市（以下「本市」という。）が「放課後キッズクラブ等入退室管理・入所申込システム開発業務」（以下「本業務」という。）を発注するにあたり、本業務の受託者は「委託契約約款」（別紙1）、「電子計算機処理等の契約に関する情報取扱特記事項」（別紙2）、「個人情報取扱特記事項」（別紙3）及び本業務説明資料、並びに本件調達における受託者の提案資料において提示した内容に基づき、業務を行うこと。定めのない事項については、必要に応じて受託者と本市との間で協議の上、定めるものとする。

### 3 用語の定義

	用語	意味
1	放課後児童健全育成事業	児童福祉法第6条の3第2項の規定に基づき、保護者が労働等により昼間家庭にいない小学校に就学している児童に対し、授業の終了後や長期休業日に小学校の余裕教室等を利用して、適切な遊び及び生活の場を与えて、その健全な育成を図る事業
2	放課後キッズクラブ	小学校施設を活用し、「遊びの場」と「生活の場」を兼ね備えた安全で快適な放課後の居場所
3	放課後児童クラブ（学童）	小学校外の施設を活用し、地域の理解と協力のもとに、対象となる児童に適切な遊び及び生活の場を与え、その健全な育成を図る事業
4	子育て応援サイト・アプリ	令和6年度から運用を開始する子育て等に関する情報提供・申請手続・サービスを受けることができるサイト・アプリ。令和7年度に連携を予定している
5	支援の単位	クラブにおける育成支援であって、クラブを利用する児童に対して一体的に行われる集団の規模を言う
6	対象児童数	クラブを毎日利用する児童の人数に一時的に利用する児童の平均利用人数を加えた数
7	利用区分	放課後キッズクラブの利用にあたり、利用目的別に区分を分けたもの わくわく【区分1】：遊びの場の利用で、16時までの利用 すくすく（ゆうやけ）【区分2A】：遊びの場＋生活の場の利用で、17時までの利用 すくすく（ほしぞら）【区分2B】：遊びの場＋生活の場の利用で、19時までの利用
8	スポット利用	わくわく【区分1】の児童で保護者の一時的な用事により、19時まで受け入れる制度。スポット利用料がかかる
9	延長利用	すくすく（ゆうやけ）【区分2A】の児童で一時的に、19時まで受け入れる制度。延長料がかかる。

10	おやつ	児童の生活リズムを整えるため、昼食と夕食の間の補食
11	運営主体	放課後キッズクラブや放課後児童クラブを運営する団体。株式会社やNPO法人、運営委員会などがある。
12	kintone	令和5年度より運用を開始しているクラブと区局を結ぶツール。各種連絡や補助金算定を行うことができる。
13	昼食提供システム	長期休業期間における昼食提供を保護者が発注するシステム（開発予定）
14	事故報告書	活動中に発生した事故に対して、区役所に提出する報告書
15	最低配置基準	クラブの開所時間を通じて放課後児童支援員を支援の単位ごとに2人以上配置しなければならないという配置基準。ただし、放課後児童支援員の内1人を除き、補助員でも可とする。
16	開所時間	運営規程で定められたクラブで児童を受け入れることができる時間。放課後キッズクラブは一律の時間だが、放課後児童クラブはクラブにより開所時間が異なる。
17	開所日	日曜日、祝日、12/31～1/2の年末年始を除くクラブを開所する日のうち、実施要綱に定められた開所時間と最低配置基準を満たし、実施要綱に定められた開所時間を満たした日を開所日として扱う。
18	月別状況報告書	クラブの運営日誌の内容を月ごとに集計した記録。児童数や開所日判定などが掲載されている
19	実施分類	開所判定に用いる分類。クラブが実際開所しているか、閉所しているかの状態を示すとともに、開所条件を満たしているか、閉所した理由等の条件により、補助金算定の一つの要素となる。
19	障害児受入推進、障害児受入強化推進の加配	障害児の利用登録がある場合、最低配置基準に加えて追加で職員を配置すること。（加配の状況に応じて補助金が加算される。）
20	長時間開所加算補助	実施要綱に定められている開所時間を超えて開所しているクラブに加算される補助
21	保護者負担減免	非課税世帯や生活保護世帯など条件に合致した世帯に利用料の一部減免を認める制度

#### 4 業務の課題・目的

放課後児童健全育成事業である放課後キッズクラブや放課後児童クラブ（以下「クラブ」という。）では、小学校に就学している児童の保護者が、労働等により昼間家庭にいないものにつき、家庭、地域等との連携の下、発達段階に応じた主体的な遊び及び生活が可能となるよう、当該児童の自主性、社会性及び創造性の向上、基本的な生活習慣の確立等を図り、児童の健全な育成を図ることを目的として実施されている事業である。運営は運営主体が条例及び事業実施要綱に定める事項を備えた良好な育成環境及び安全性を備えた、事業のための施設等において、専任の職員により事業が行われている。また、事業実施に伴い、クラブは、利用料等と本市から運営経費に対し補助金交付を受け、運営主体が運営を行っている。

現在、保護者がクラブに利用を申込みするためには、保護者がクラブの開所時間に直接申込書を提出する必要がある、欠席連絡なども電話で連絡する必要があるなど、就労している保護者にとっては、場所や時間に制約があり、負担となっている。また、補助金制度も年々複雑になり、地域住民や保護者が参画する運営委員会形式の放課後児童クラブなどは保護者が会計業務を担っているなど、その補助金申請業務も大きな負担となっている。

本市では、「デジタルの恩恵をすべての市民、地域にいきわたらせ、魅力ある都市をつくる」ことを基本目的

として、「デジタル×デザイン」をキーワードに、令和4年9月に「横浜DX戦略」を策定した。その中で、「子育て」DXを重点テーマの一つに位置付けており、子育て世代から選ばれる都市となるため、アプリ等を活用した子育て支援サービスを利用しやすい環境の充実や、各種手続きのオンライン化による利便性向上など、リーディングプロジェクトとして展開している。

また、横浜市中期計画においても、基本戦略として、「子育てしたいまち 次世代を共に育むまち ヨコハマ」をかかげ、子育て世帯に向けた支援を基本戦略に位置付けている。

そこで、クラブを利用する保護者に、利用申込みやクラブへの欠席連絡等の手続きの負担を軽減するとともに、児童の安全・保護者の安心感につながる入退室の情報などを提供するサービスを提供すること、またクラブが日々の活動状況をデジタル管理可能な環境を提供し、運営事務の負担軽減を図ることを目的に「放課後キッズクラブ等入退室管理・入所申込システム開発業務」を行うものである。

## 5 履行期間

契約の日から令和7年3月31日まで

## 6 履行場所

- ・受託者が用意する作業場所

(本業務における設計・構築・テスト業務について、委託者は受託者が常駐可能な開発室等の準備をしないため、作業場所等は受託者で準備すること。)

- ・その他本市が認めた場所

## 7 本業務の概要

### 7.1 プロジェクト管理

契約締結後、必要なスキル及び経験を有するメンバーを配したプロジェクト体制を整え、概ね2週間以内にスケジュールを作成し、本市担当者に事前承認を得た上でプロジェクトを実施すること。

なお、プロジェクトの管理状況については、本市が主催をする定例会等においてプロジェクト管理報告書を定期的に提出して報告するものとする。定例会は週1～2回程度の定期開催とし、必要に応じて定例会の実施回数を増やすものとする。報告頻度及び報告書の内容・形式については、契約締結後、受託者が提案し、本市担当者の承認を得るものとする。

本業務の遂行に当たり、本市が意図しない仕様の変更や個人情報の紛失・漏洩などが発生しないよう、受託者において一貫した推進体制を整備すること。また、本市、および必要に応じて他のシステム関連業者（既存の入退室管理システム業者、kintoneにおける補助金事務システム開発業者）とも緊密に連携して業務を遂行すること。

### 7.2 プロジェクトの概要

#### 7.2.1 対象とする利用者・利用人数

開発するシステムの利用者や利用人数は下記の通りである

	クラブ数	児童数	職員数
放課後キッズクラブ	338 クラブ	7～8 万人	1 万人
放課後児童クラブ	219 クラブ		
横浜市区局職員	-	-	100 人

## 7.2.2 使用する端末

- ・保護者：スマートフォンやパソコン、タブレットなど
- ・クラブ：クラブ所有のパソコン、タブレットなど
- ・市役所、区役所：市所有のパソコンなど

上記使用端末を想定し、使いやすいシステムを構築すること

## 7.2.3 システム開発方式

本プロジェクトにおいては、令和6年度中の短期に開発・稼働ができるシステムとする。また、利用児童が増加しても安定稼働し、多様なメニューや機能が容易かつ安価かつ早期に開発実装でき、補助金制度等の変更にも柔軟に改修できる構成と仕組みが必要である。

また、令和7年度以降も、利用者の増加と機能の拡張を予定しており、利用者の拡大や改修や機能拡張が容易にできる構成と仕組みが必要である。

上記のことから、本システムは、クラウドサービスに構築する。

### 7.2.3.1 クラウドサービスによるスケールアウト

サーバー環境、ネットワーク環境、セキュリティ環境などがデータセンターからサービスとして提供され、機器の整備や保守作業を必要としないこと。また、機器の増設やソフトウェア等の改変を伴わず、利用者数に応じた処理能力およびデータ保持能力が拡張（スケールアウト）できること。

### 7.2.3.2 児童の登録状況に合わせてメニュー表示

児童の登録区分、クラブ独自のイベントなど状況に合わせたサービスメニューを動的に生成して提示、申請できること。

### 7.2.3.3 利用者認証機能

多様な利用者の認証機能が基本的に備わっていること。

### 7.2.3.4 API 連携

API 機能が備わっており、他システムとの連携が容易であること。

#### 7.2.4 対象とする業務

今回システム化を行う業務は下記に示す No. 1～No. 26 の業務とする。

##### 対象業務一覧

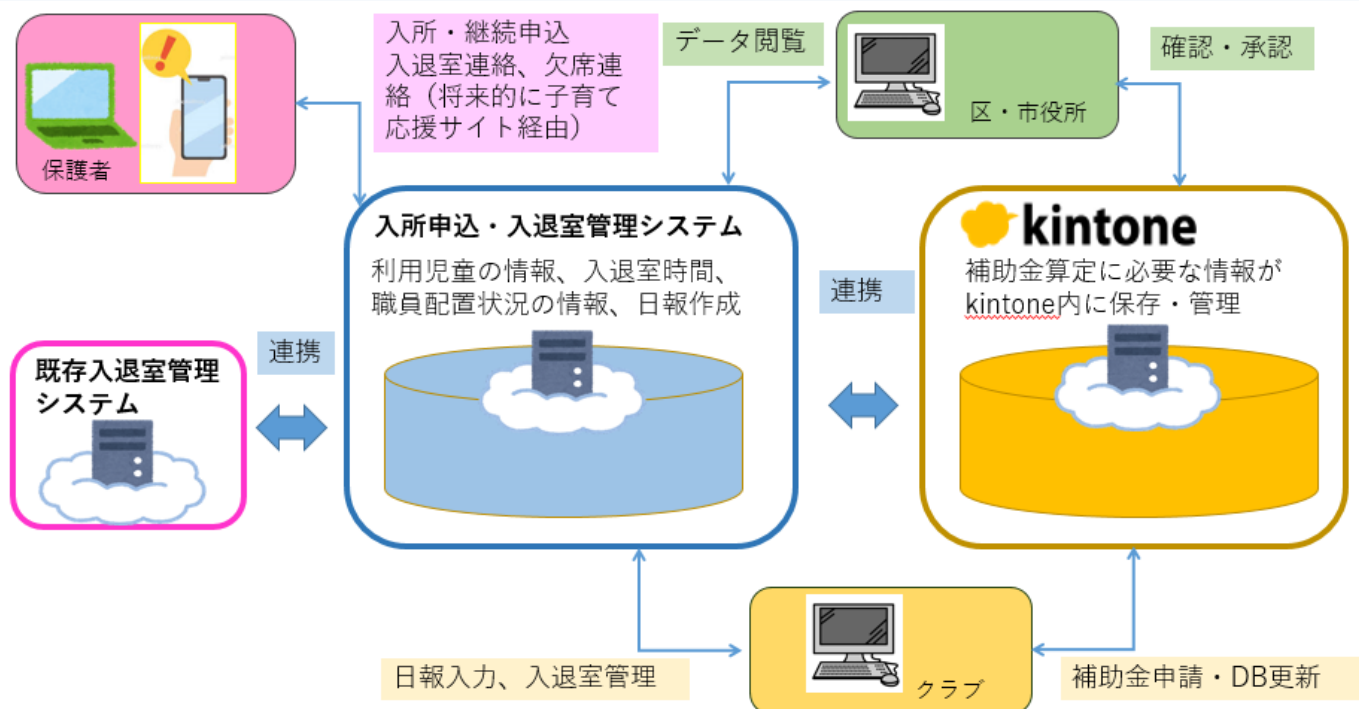
No	業務内容	頻度・時期
1	入所申込、継続利用申込受付	前年度1月ごろ～3月31日
2	就労証明書提出受付	前年度1月ごろ～3月31日
3	各種要件の挙証資料提出受付	前年度1月ごろ～3月31日
4	児童の傷害保険加入確認	前年度1月ごろ～3月31日
5	各種資料の提出受付	前年度1月ごろ～3月31日
6	区分利用変更申込受付	随時（5月以降）
7	退所届提出受付	随時（5月以降）
8	入所申込受付	随時（5月以降）
9	保護者就労証明書提出受付	随時（5月以降）
10	各種要件の挙証資料提出受付	随時（5月以降）
11	児童の傷害保険加入確認	随時（5月以降）
12	保護者への個別、一斉連絡	随時
13	利用予定表の変更受付	随時
14	児童の欠席連絡受付	随時
15	利用予定と異なる児童についての保護者への確認	随時
16	児童の入退室管理（保護者への連絡含む）	日次
17	児童の退室誘導	日次
18	職員の勤怠管理（出退勤時間の記録）	日次
19	クラブ日誌の作成	日次
20	職員の配置状況確認、開所判定	日次
21	利用予定表の受付	月次
22	クラブ日誌を取りまとめた月別状況報告書の作成	月次
23	区分変更や対象児童数の変更管理（児童データベースの更新）	月次
24	月次の利用料やおやつ代の算出	月次
25	利用料等保護者負担金の徴収	月次
26	非常勤職員の勤務時間集計（集計期間を変更可能）	月次
27	職員のシフト表作成（令和6年度開発対象外）	月次
28	子育て応援サイトとの連携（今年度開発対象外だが、要提案）	-

## 7.2.5 システム全体の概要図

システム全体の概要図を下記に示す。

システム全体の概要

# システム全体の概要



## 7.2.6 システム全体の求める機能

### 7.2.6.1 セキュリティ

受託者は、横浜市情報セキュリティ管理規程（別紙4）以下の規程等を遵守し、情報セキュリティ対策を講じること。また、本市から監査等の要請があった場合には速やかに応じること。（この他に遵守すべき資料があれば、契約締結後に別途提示する。）本市の情報セキュリティポリシーに定めのない項目であっても、総務省の公表する「地方公共団体における情報セキュリティポリシーに関するガイドライン（システム稼働時点）」（別紙5）に準じた対応を求めることとし、特にクラウドサービスの提供にあたっては、本市を所管する合意管轄裁判所を契約上規定することとする。また、データ（バックアップデータ含む）の保管場所も日本国内とすること。

そのほか求める情報セキュリティ要件は以下のとおりである。

- ・利用者、管理者別にアクセス権限を設定できること。
- ・所属組織、職務分掌の単位で権限グループを設定できること。
- ・ユーザー単位での権限設定ができること
- ・システムログ及びアプリケーションログ（ユーザーID、操作日時、対象データ、操作内容、IPアドレスなど）を取得できること。
- ・取得したログについては、権限のない者が変更できないようにするなど、適切に管理、保管すること。
- ・本システムを構築するプラットフォームは政府情報システムのためのセキュリティ評価

制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））の要件を満たし、その評価を受けて登録されているものが望ましい。

- ・通信経路の暗号化、通信回線の監視、ファイアウォールやウイルス対策ソフトの導入など、安全な管理のために必要な対策を行うこと。
- ・情報システムの開発、管理、運用を行う者には、個人ごとに ID を発行し、それぞれに推測困難なパスワードを設定させること。
- ・アクセス元 IP アドレスによるアクセス制限や多要素認証など、ID、パスワードが漏えいしたとしても、インターネットを経由した不特定多数からの不正アクセスが生じえない対策を講じること。
- ・常に脆弱性を利用したサイバー攻撃の情報を入手し、リスクの大きさに応じて適切に対応すること。
- ・WAF（Web Application Firewall）や仮想パッチ等、脆弱性を利用した攻撃を防ぐ仕組みを導入すること。
- ・データのバックアップ体制や緊急連絡先、復旧までの時間について、確認できていること。
- ・データを保存するサーバーは国内にあること。
- ・保護者のセキュリティは利便性を考慮した内容とすること。

#### 7.2.6.2 他システムとの連携

本市や各クラブが利用している既存のシステムとの連携について、関連情報の更新が煩雑とならないよう、また利用者の入力負荷が軽減できるように留意し、連携方法について具体的な提案をすること。

図表 連携を想定しているシステム

No	連携システム	想定する連携方式	備考（システム概要や連携内容など）
1	横浜市補助金事務システム（kintone）	API 連携	本市が開発しているクラブの補助金算定システム。児童情報や入退室、出退勤時刻などの補助金算定に必要なデータを連携する。
2	既存入退室管理システム	API 連携	一部クラブが使用している既存入退室管理システム。具体的な連携項目や方法は受託者と既存入退室管理システム業者と調整の上、決定する。
3	決済（集金）代行業者システム	CSV、API 連携	一部クラブが使用している決済代行業者との請求データの提供。具体的な連携先や方法については、受託者と調整の上、決定する。
4	横浜市子育て応援サイト・アプリ	API 連携	子育てに関する様々な手続きがオンラインで行え、様々な情報を入手できるサイト・アプリ。現在開発中、令和6年度公開予定。本システムとは令和7年度に連携を予定。利用者が本システム上で行う申込・連絡等は、当該サイト・アプリを介して行えるようにす

			る。また、本システムから発信する各種情報は、利用者が当該サイト・アプリから受け取れるようにする。具体的な連携方法は、受託者と調整の上、決定する。
5	昼食提供システム（仮称）	API	令和7年度連携予定
6	各社会計ソフト	別途協議	令和7年度以降連携検討
7	各社勤怠管理ソフト	別途協議	令和7年度以降連携検討

#### 7.2.6.3 その他機能

No	項目	説明ならびに必要とする機能
1	デザイン	小学生の保護者が親しみやすい、わかりやすいページデザイン（UI/UXの高いデザイン）
2	実装する各種機能の利用選択性	実装した機能や利用期間をクラブが柔軟に選択、設定できる機能
3	2事業（放課後キッズクラブ、放課後児童クラブ）の両事業への対応	事業内容や制度が異なる両事業に対応できるようなシステムやそれぞれの事業ごとにシステムを構築する。また、1人の児童がキッズクラブ、児童クラブ両施設の利用（重複利用）を前提にシステム構築する
4	エラーチェック機能	各種申請や保存時にエラーチェックを行う機能
5	任意の状態での保存機能	入力途中に任意の状態を入力内容を保存できる機能
6	バックアップ機能	定期的にバックアップを自動に行う機能。 クラブ側でも任意でバックアップを取る機能
7	本市からの児童の必要項目の閲覧機能	市職員、区職員が本システム内の各クラブの挙証資料を閲覧できるような権限を付与もしくは、クラブ側からの提出機能を付与
8	子育て応援アプリとの連携（令和7年度連携予定だが、要提案）	通知発信などリアルタイムでのアプリとの連携方法。企画調整に確認。

#### 7.2.6.4 サービスレベル

「別紙6\_SLA要件一覧」に定めたサービスレベルを目標とするが、詳細については、受託者との合意により定める。

クラウドサービスで、SLAがサービスで予め決定されている場合は、当該システムのSLAを本市に提示すること。

### 8 各機能の求める機能要件

#### 8.1 入所申込機能

##### 8.1.1 開発の目的

放課後児童健全育成事業所を利用する際、保護者は事前に利用申込書や入会申込書に必要事項を記入し、就労証明書などの挙証資料と一緒にクラブへ直接提出する必要がある。クラブも利用申込書等の情報をエクセル等に転記する必要があり、保護者、クラブともに手間がかかっている。

保護者の利便性を高め、クラブの業務効率化を進めることを目的とし、入所申込機能を開発する。



### 8.1.2 入所申込機能概要

保護者のスマートフォンや自宅のパソコンからシステムにアクセスし、利用申込ができることにより時間場所を問わず手続きを行うことを可能にし、保護者の利便性を高める。また、利用申込だけでなく、継続利用、退会、休会、区分変更申込等も対応できるようにするとともに、就労証明書等の挙証資料も添付できるようにする。ただし、入所前にクラブとの面談が必要な児童などいることから、クラブの状況に応じて、オンラインでの入所申込の条件付けできることが望ましい。

### 8.1.3 入所申込機能の求める要件

#### 8.1.3.1 キッズクラブ向け利用申込書（参考様式 1-1）

No	項目	機能の具体例
1	通所クラブへオンラインでの入所申込できるまでの条件設定	専用 QR コードの読み込みなどによる入所機能の表示など
2	別紙参考様式の項目を入力する申請ページの作成	参考様式 1-1 参照
3	保護者の入力項目を必要最低限にすること	前年度登録内容やきょうだい児登録内容の参照、きょうだい児の紐づけ機能など
4	就労証明書や療育手帳（写し）など挙証資料の確認機能	児童情報への挙証資料（参考様式 1-3～1-7 等）アップロード機能
5	保護者の入力情報（個人情報）が本市へ提供される事について同意確認機能をつけること	同意画面の方法や手順
6	参考様式 1-1 に記載されている項目に加え、記載項目を追加できること	
7	利用申込に対しての結果通知機能	申込の受理など保護者が申込内容を確認できる機能
8	転校などにより、退所手続きができるページの作成。ただし、容易に退所できないような機能を実装する	専用 QR コードの読み込みなどによる退所機能の表示など 参考様式なし
9	児童データベースの作成	児童の個別のページ作成や、条件に合致した児童の抽出など

#### 8.1.3.2 キッズクラブ向け利用区分変更申込書

No	項目	機能の具体例
1	別紙参考様式の項目を入力する申請ページの作成	参考様式 1-2 参照
2	保護者の入力項目を必要最低限にすること	利用申込書の参照やきょうだい児同時申請機能など
3	就労証明書や療育手帳（写し）など挙証資料の確認機能	児童情報への挙証資料（参考様式 1-3～1-7 等）アップロード機能
4	参考様式 1-2 に記載されている項目に加え、記載項目を追加できること	
5	変更申込に対しての結果通知機能	申込の受理など保護者が申込内容を確認できる機能

### 8.1.3.3 児童クラブ向け入会申込書

No	項目	機能の具体例
1	通所クラブへオンラインでの入所申込できるまでの条件設定	専用 QR コードの読み込みなどによる入所機能の表示など
2	別紙参考様式の項目を入力する申請ページの作成	参考様式 2-1 参照
3	保護者の入力項目を必要最低限にすること	前年度登録内容やきょうだい児登録内容の参照、きょうだい児の紐づけ機能など
4	療育手帳（写し）など挙証資料の確認機能	児童情報への挙証資料のアップロード機能
5	変更申込書の機能（ページの作成）	利用日数の変更申請等 参考様式なし
6	保護者の入力情報（個人情報）が本市へ提供される事について同意確認機能をつけること	同意画面の方法や手順
7	様式に記載されている項目に加え、記載項目を追加できること	
8	児童データベースの作成	児童の個別のページ作成や、条件に合致した児童の抽出など

### 8.1.3.4 児童クラブ向け継続利用申込書

No	項目	機能の具体例
1	別紙参考様式の項目を入力する申請ページの作成	参考様式 2-2 参照
2	保護者の入力項目を必要最低限にすること	昨年の入所申込書の参照やきょうだい児同時申請機能など
3	療育手帳（写し）など挙証資料の確認機能	児童情報に挙証資料のアップロード機能
4	保護者の入力情報（個人情報）が本市へ提供される事について同意確認機能をつけること	同意画面の方法や手順
5	様式に記載されている項目に加え、記載項目を追加できること	

### 8.1.3.5 児童クラブ向け退会届出書、休会申出書

No	項目	機能の具体例
1	別紙参考様式の項目を入力する申請ページの作成	参考様式 2-3、2-4 参照
2	保護者の入力項目を必要最低限にすること	入所（継続）申込書の参照やきょうだい児同時申請機能など
3	様式に記載されている項目に加え、記載項目を追加できること	
4	容易に退会・休会できないような機能を実装すること	専用 QR コードの読み込みなどによる退所機能の表示など

### 8.1.3.6 児童クラブ向け入会（継続利用）決定通知書

No	項目	機能の具体例
1	保護者が入力した情報をもとに決定通知書を作成する機能	参考様式 2-5 参照
2	クラブの入力項目を必要最低限にすること	入所（継続）申込書の参照やきょうだい児同時発行機能など
3	利用申込に対しての結果通知機能（決定通知書）の配信）	決定通知書（参考様式 2-5）の配信など保護者が申込内容・結果を確認できる機能

### 8.1.3.7 児童データベースの作成

No	項目	機能の具体例
1	児童の個別ページの作成	参考様式 1、2 に加え、クラブ独自項目の設定
2	個別ページの変更時のアラートと変更履歴の記録	変更申請の確認方法（アラートなど） 変更項目の把握機能と変更前後の履歴確認機能の実装
3	保護者ページの表示とクラブ管理ページの切り替え	保護者画面とクラブ側画面との表示切替等（表示、非表示項目の選択）
4	クラブが受理した挙証資料の添付	クラブが原本を受領した際の添付機能
5	児童番号の自動採番機能	J+〇〇〇〇〇〇（6桁数字）で自動採番
6	児童データからの抽出	条件に合致した児童の抽出など
7	（令和7年度実施予定） 事故の履歴と日誌、事故報告書との連携	（令和7年度実施予定） 事故や保育中の気になった点の記録の蓄積とデジタル日誌や事故報告書とリンク機能

## 8.2 利用予定並びに入退室管理機能

### 8.2.1 開発の目的

放課後キッズクラブ、放課後児童クラブの補助金算定は、クラブ職員の出退勤時間及び児童の入退室時間など日々の活動状況に影響される。時間帯ごとの児童の利用人数も確認する必要があり、人数の多いクラブでは職員の負担が大きい。また、欠席連絡の電話対応などでも時間がとられ、育成支援に集中しづらい環境である。システム導入により、児童の出欠状況を簡単に把握することにより、職員の負担を軽減する。

### 8.2.2 利用予定並びに入退室管理システムの開発の概要

児童ごとに QR コードや IC カードを割り振り、読み取り機で読み取ることにより、入室、退室時間が自動的に記録、並びに保護者に通知する機能を実装する。記録から、利用予定と実際の利用に差異がある児童の保護者に対して、容易に保護者に連絡する機能や欠席などを個別に連絡する機能などを実装し、保護者、クラブ両者の利便性を上げる。

### 8.2.3 利用予定並びに入退室管理機能の求める要件

#### 8.2.3.1 利用予定管理機能

No	項目	機能の具体例
1	保護者の利便性を重視した前月や当月の利用予定（利用有無、入退室時間、習い事等による中抜け、おやつの有無等）の申込・連絡	スマートフォンや自宅パソコンからの登録
2	保護者の入力項目を必要最低限にすること	申込内容の引用、参照やきょうだい児同時申請機能、コピー機能など短時間で登録できる機能
3	項目のクラブ設定	クラブの実情に合わせた項目の追加、削除ができる機能
4	スポット利用、延長利用、イベントの申込・連絡機能	保護者が内容や料金など間違ふことなく、容易に申込や申込内容が確認できる機能
5	保護者入力項目のクラブ設定	クラブが必要に応じて入力項目の増減ができる機能
6	申込した内容の変更機能	変更期限の設定などクラブの実情に合わせた設定ができる機能
7	登録された利用予定の集計	児童別や月別等様々な集計機能

#### 8.2.3.2 入室時間、退室時間記録と連絡機能

No	項目	機能の具体例
1	児童の入室、退室時間（習い事等による中抜け）の記録	ICカードやQRコードなどを利用した児童が容易に使用できる記録方法
2	児童の入室、退室時間（習い事等による中抜け）の保護者連絡（複数の連絡先）	クラブの負担をかけないような連絡方法
3	予定と異なる入室や欠席児童への保護者連絡（複数の連絡先）	利用予定と異なる出欠席状況の児童の迅速な把握とクラブの負担をかけない保護者への連絡方法
4	急な欠席や児童のケガ等クラブと保護者間の双方向の個別連絡機能（複数の連絡先）	時間、場所を問わず連絡ができるような連絡方法。写真等も送付を想定。
5	個別連絡機能の既読確認機能	保護者、クラブの既読確認機能などの実装
6	クラブから保護者への一斉連絡機能	イベントなどの案内やクラブ通信（クラブからの連絡）の一斉配信。
7	区役所、こども青少年局から保護者への一斉連絡機能	アンケートや通知文の一斉配信
8	入退室状況の表示機能	リアルタイムでの入室児童数や退室（中抜けを含む）した児童数などの現在の状況把握できるような機能
9	利用予定や利用履歴の等の一覧抽出	出欠簿を作成、閲覧できる機能（児童別、日別）

10	おやつ喫食実績の記録	おやつ喫食の記録機能（デジタル日誌での対応も可）
11	帰宅時間アラート機能	帰宅やお迎え予定の児童を、時間に応じて表示する機能。
12	延長利用の自動判定	各クラブで延長となる条件等の設定ができるような機能

### 8.3 職員勤怠管理機能

#### 8.3.1 開発の目的

放課後キッズクラブ、放課後児童クラブの補助金算定は、クラブ職員の入退室時間及び児童の入退室時間で決定される。また、職員の勤怠管理は専用のシステムやタイムカード等で管理しているクラブが多くあり、勤務時間を日誌に転記している。その際、誤って転記するクラブもあり、補助金返還等つながる場合もある。本システムにより職員の出退勤時間を記録し、後述のデジタル日誌機能に出退勤時間を取り込むことで、転記等によるミスを軽減する。

#### 8.3.2 職員勤怠管理機能の開発概要

職員ごとにQRコードやICカードを割り振り、読み取り機で読み取ることにより、出勤、退勤時間を自動的に記録する機能を実装する。また、職員の予定された勤務時間を入力することで、配置状況が確認でき、クラブは事前に最低配置基準を満たす配置かを確認できるようにする。

#### 8.3.3 職員勤怠管理機能の求める要件

No	項目	機能の具体例
1	職員の出勤、退勤、休憩時間の記録	ICカードやQRコードなどを利用した職員が容易に使用できる記録方法
2	デジタル日誌との連携	記録した出退勤時間クラブの職員配置欄への転記
3	職員配置状況の可視化	職員の勤務予定時間を入力することで、各時間帯の配置状況と最低配置基準との差異を視覚的に確認できるような機能の実装 (デジタル日誌の機能でも可)
4	勤務時間の集計	月ごとの勤務時間の集計機能の実装

### 8.4 デジタル日誌機能

#### 8.4.1 開発の目的

現在、開所時間や職員体制等の補助金算定に必要な情報は業務日誌に記録されているが、多くのクラブは手書きで作成しているため、時間を要し、記入漏れや転記ミス等も多く発生している。また、クラブの開所日判定なども、開所日となる条件が複雑であり、クラブも開所・閉所の判断を誤ることが多く、補助金の戻入なども発生している。

業務日誌のデジタル化により、上記のような児童の入退室の記録や職員の出退勤時間を日誌に取り込み、開所条件を満たしているかを自動判定する機能を実装することにより、補助金申請等の事務作業の効率化を行う。

#### 8.4.2 デジタル日誌開発の概要

児童の入退室管理システムや職員勤怠管理システムより児童の入退室時間や職員の出退勤時間を取込み、設定された開所条件と比較して単位ごとの開所・閉所を判定する機能を実装する。また、児童データベースやkintoneにある事故報告書と連携し、保育中に発生した事故やトラブルなどに対して各アプリにて適切に記録、申請が行える機能を実装する。

#### 8.4.3 デジタル日誌機能に求める要件

##### 8.4.3.1 活動記録の記載

No	項目	機能の具体例
1	デジタル日誌ページの作成	参考様式3、参考様式4に加えて、クラブ独自項目の追加設定機能、実施分類の入力欄
2	日誌の出力機能	必要に応じて日誌のPDF またエクセル様式等で出力できるような機能を実装
3	児童入退室管理機能との連携	時間ごとの利用児童数集計記録や障害児の利用記録との連携、集計記録
4	職員出退勤管理機能との連携	出勤職員の勤務時間記録との連携ならびに、時間ごとの配置人数の表示 (支援員資格有無含む) 打刻時間とシフト時間の差異発生時の処理方法をクラブによって設定できる機能
5	月別状況報告書の作成	横浜市放課後児童クラブ事業費補助金交付要綱第8号様式 横浜市放課後キッズクラブ事業実施要綱第2号様式日誌の情報を元に月別状況報告書の作成・区への提出機能
6	日誌作成終了後の修正箇所と修正履歴	
7	日誌未作成時のアラート機能	クラブ画面でのアラート表示
8	(令和7年度実施予定) 事故、トラブル等の記録と児童データベース、事故報告書との連携	(令和7年度実施予定) 事故や保育中の気になった点の記録の蓄積と児童データベースや事故報告書とのリンク機能

##### 8.4.3.2 配置確認及び開所判定機能

No	項目	機能の具体例
1	単位ごとの開所時間の判定	運営規程の開所時間と時間ごとの利用児童数から開所した単位の開所時間判定
2	単位ごとの職員配置確認	時間ごとの職員配置を確認し、その時間帯に開所している単位数に応じた放課後キッズクラブ及び放課後児童クラブそれぞれの最低配置基準をみたしているかの確認
3	「実施分類」「単位ごとの開所時間の判定」「単位ごとの職員配置確認」の情報からの単位ごとの開所判定実施	利用児童数、職員配置人数、最低配置基準の比較をクラブが目視で確認しやすい表示方法の提案ならび判定結果を認識しやすいような表示方法の提案

4	障害児受入推進、障害児受入強化推進の加配状況の判定	開所判定情報をもとに最低配置基準からの増員人数を表示し、加配で配置する単位や人数などをクラブで設定できる機能
5	長時間開所加算の加算対象時間数の算出	開所判定結果から、長時間開所加算対象時間数算出機能
6	職員配置状況表の作成	参考様式 5、参考様式 6 参照 日誌の情報を元に職員配置状況表の作成・区への提出機能

## 8.5 保護者負担金（利用料）計算・徴収補助機能の要件

### 8.5.1 開発の目的

現在、多くのクラブではおやつ代が都度払いであるため、おやつ喫食の実績や、複雑な減免制度などにより、保護者負担金（利用料）を個別計算する必要がある。保育料や延長料金、スポット料金なども含め、月ごとの利用料金を容易に算出できる機能や算出した金額の口座振替データの作成機能を実装し、クラブの請求・回収事務の削減を行う。

### 8.5.2 保護者負担金（利用料）計算・徴収補助機能の概要

児童の入退室時刻や利用区分、おやつの喫食実績等から、計算をおこない、請求書の作成、送付機能も実装する。また、決済代行業者を用いるクラブについては、指定の csv データを出力する機能もあわせて実装する。

### 8.5.3 保護者負担金（利用料）計算・徴収補助機能の機能

No	項目	機能の具体例ならびに提案を希望する事項
1	保育料の計算	利用区分や運営規程で定められた料金表から計算を行う
2	減免額の計算	運営規程で定められた料金表から計算を行う
3	おやつ代の計算	喫食状況から算出する。 請求方法は、前払いまたは後払いをクラブの状況の応じて選択できる
4	その他利用料の計算	スポット利用や材料費やイベント費用の計算を行う
5	各種料金の計算	各料金におけるクラブで設定した締日等を考慮した利用料の合計の算出方法
6	各種料金の請求書発行	算出金額の保護者へ通知方法
7	利用料金徴収機能（決済代行業者との連携）	代行業者に応じた請求データの作成

## 9 品質試験（テスト）

### 9.1 テスト計画

各種テスト（単体テスト、結合テスト、総合テスト等）について、目的・環境・手法・品質評価基準等を明記したテスト計画書を事前に作成し、承認を得ること。

### 9.2 テスト実施

- ・各テスト計画書等に基づいて、システムの品質試験（テスト）、結果分析及びその対策を実施すること。テストにおいて、エラー及び障害発生を確認した場合は、本市へ報告の上、その原因や影響をすみやかに特定し、設計変更・改修等しかるべき対応を実施すること。
- ・性能面での問題が発生した場合も同様に、原因を特定の上、適宜性能向上対策を実施すること。テストにあたっては、網羅的な検証が可能なテストデータを受託者自身で用意すること。
- ・他既存入退室管理システムとの連携テストについては、受託者が主体的にテスト基本計画書策定の段階から参画し、当該システムの本市担当課及び現行システム事業者と協議・調整の上、進めること。
- ・本市が構築中の補助金算定システム kintone との連携テストについては、テスト基本計画書策定の段階から受託者、kintone 開発受託者及び当該システムの本市担当者が協議・調整をし進めること。

### 9.3 テストの報告

テストの結果は、本市がテスト結果を定量的に判断可能な形式（評価項目、評価基準等）で報告すること。

### 9.4 テストデータの取り扱い

個人情報等を含むデータをテストで使用する場合は、セキュリティに十分に配慮した上で、本市と協議の上取り扱いを決定すること。

### 9.5 単体テスト

機能ごとに単体テストを行い正常に稼動することを担保すること。

### 9.6 結合テスト

#### 9.6.1 機能の網羅性に配慮し、以下の観点にて各機能が連携しての稼動品質を担保すること。

- ・本サイト・システム内の各機能連携テスト
- ・kintone との情報連携テスト
- ・他既存入退室管理システムとの情報連携テスト
- ・保護者端末（スマートフォン・タブレット・PC 等）との機能連携テスト
- ・市役所、区役所端末との機能連携テスト
- ・バックアップ、リストア等の保守運用テスト

#### 9.6.2 結合テストの環境

テストの実施にあたっては、システム構成（概観）、ソフトウェアのバージョン、権限等を本番環境と合わせること。

### 9.7 総合テスト

サービスリリース時と同等の環境で、システムが正しく稼動することを担保すること。以下の観点にてシステムの稼動品質を担保すること。

- ・利用者視点でのシナリオテスト
- ・情報連携テスト
- ・管理者・kintone 利用者・既存入退室管理システム管理者視点でのシステム運用テスト
- ・セキュリティテスト・ペネトレーションテスト
- ・性能評価（性能テスト、負荷テスト）
- ・リストアテスト



- ・その他必要なテスト

## 10 導入支援

### 10.1 導入支援の目的

入退所の申込や日誌のデジタル化の取組など多くのクラブでは、初めての取組であるため、支援を必要としている。また、放課後児童クラブは入退室管理システムの導入率も低く、入退室管理システムなども初めてであり、一気にデジタル化が進むため、支援を行う必要がある。

また、既に市中等の入退室管理システムを導入してクラブに対しても、本市は今回開発するシステムへの利用移行を勧奨するため、移行する場合の支援も必要である。

### 10.2 クラブへの導入支援の概要

導入するクラブの状況に応じて、システム導入時に適切な導入支援(マニュアル作成、研修、動画配信、訪問等)を行う。クラブによって支援の方法を変えることを妨げないが、クラブの理解に応じて、都度支援を行うようにし、導入後の問い合わせ対応なども行う。全クラブが契約中に何らかの導入支援を受けることができる環境を整える。また、クラブ向け、委託者向けマニュアル、保護者を作成すること。

### 10.3 保護者への導入支援の概要

クラブへの入所申込、継続利用申込は保護者が本システムを用いて申し込みを行うこととなる。保護者が入所申込などの手続きを自宅などから対応できるように各種手続きにおいて簡易なマニュアルに整備すること。

また、システムの保護者画面トップページからマニュアルが閲覧できるように、各種手続きの操作説明資料を準備すること。

## 11 利用規約（約款）作成支援

本システムをクラブが利用するあたり、本市から利用規約（約款）等を提示し、同意・利用申込等を受けたいうえで、利用に供する予定である。当該利用規約（約款）等の作成にあたり、支援を行うこと。また必要に応じ専門家の支援を受けられるようすること。

## 12 想定スケジュール

項目	開始	終了
各機能の開発	契約日	令和6年9月30日
各機能の動作試験	令和6年10月1日	令和6年10月31日
最終試験	令和6年11月1日	令和6年11月30日
各クラブへの導入支援	令和6年12月1日	令和7年1月31日
各機能の改良	令和6年12月1日	令和7年1月31日
kintone との連携	令和7年2月1日	令和7年3月31日
既存入退室管理システムとの連携	令和7年2月1日	令和7年3月31日

## 13 成果物一覧

想定される成果物として、別紙7 成果物一覧を参照のこと

- (1) 成果物の詳細については、受託者の提案事項を踏まえ、本市の協議の上決定し、プロジェクト計画書でさだめる
- (2) 成果物は原則として、Microsoft Word、Microsoft PowerPoint、Microsoft Excel 又は PDF 形式を用いて作成すること

## 14 留意事項

14.1 本業務の再委託受託者は、受託者以外の者に作業を実施させる必要があると判断した場合、クラウドサービスなど第三者のサービスを利用する場合、提案書にその旨および内容を提案書に記載すること。

受託者は、受託者以外の者に作業を実施させる場合、予め再委託申請書、再委託先の要員を記載した作業要員一覧、再委託先が押印した秘密保持誓約書を本市へ提出し、承諾を受けること。

なお、本市の承諾を受けるまでは、再委託先が関与する一切の作業を認めない。また、本業務のプロジェクト責任者や本市との直接の窓口になる担当者が、受託者ではなく再委託先になることを認めない。

### 14.2 法令等の遵守

受託者は、本業務の履行にあたり、プロジェクト責任者の責任において、再委託先を含む受託者配下の作業従事者に対し、本書及び契約書で定める事項、関係法令、本市の条例・規則・要綱等を十分に遵守・理解するよう徹底させること。

### 14.3 機密性の厳守

受託者は、本市の重要情報を取り扱う責任を自覚し、情報セキュリティの三原則（機密性・完全性・可用性）を十分に理解しなければならない。特に、成果物の作成や本市の情報資産を扱う作業、本市庁舎内で作業を行う際は、本市情報セキュリティポリシーと同水準以上で作業を行うこと。

また、受託者は、本市個人情報保護条例及び本市情報セキュリティポリシーを遵守するとともに、個人の権利及び利益を侵害してはならず、本件業務の履行により知り得た本業務及び関連する業務の内容を、グループ会社を含め一切第三者に漏らしてはならない。

### 14.4 著作権の取扱い

システムに格納されるデータや業務を行うなかで生成されたデータはすべて本市が所有権を有するものとする。また、将来、今回構築したシステムを別の新たなシステムに更改する際には、更改に必要なデータの移行を円滑に行えるよう協力すること。なお、知的財産権は、本市との契約事項に基づき運用するものとするが、以下の記載を遵守すること。

#### 14.4.1 著作権

本業務における成果物のうち、納品された各ドキュメントにおける一切の知的所有権に関して、著作権法（昭和45年法律第48号）第21条から第28条までに定める権利を含むすべての著作権は、本市に帰属する。成果物は、引渡し時を持って著作権を本市に譲渡する。

また、著作者人格権は、本市及び本市が指定する者に対して一切行使することができない。ただし、製品に附属されるマニュアルなどの原本そのものの著作権は、受託者に留保する。

なお、成果物にこの契約の前から受託者または第三者が著作権を有する著作物が含まれる場合の当該著作物、並びに成果物が受託者または第三者が権利を有するパッケージプログラム（無償提供のもの、いわゆるフリーソフトを含む。）である場合、これらの著作物は受託者または当該第三者に留保されるものとする。

#### 14.4.2 プログラム構成部品等の権利

本業務で採用された製品・サービスにおける一切の知的所有権に関して、著作権法第21条から第

28 条に定める権利を含むすべての著作権は、受託者（もしくは製品開発事業者またはサービス提供者）に留保する。

ただし、本業務で開発を行ったカスタマイズプログラム・部品及び新規作成プログラム・部品（汎用性のあるルーチン、モジュール、関数、テンプレート等含む。）における一切の知的所有権に関して、著作権法第 21 条から第 28 条に定める権利を含むすべての著作権は、本市に帰属する。

なお、受託者は、本市に帰属するプログラム・部品を営利目的にて他所で使用する場合、事前に本市の許諾を得なければ使用できないものとし、本市は将来に渡って本市に不利益が生じないこと及び日本全国公共の利益に供する理由が認められた場合にこれを許諾する。

#### 14.4.3 コンテンツ等の権利

本サイトの運営において、利用者への情報提供のために作成したコンテンツ（コンテキスト、映像、動画を含む）における一切の知的所有権に関して、著作権法（昭和 45 年法律第 48 号）第 21 条から第 28 条までに定める権利を含むすべての著作権は、本市に帰属する。成果物は、作成・掲載時を持って著作権を本市に譲渡する。

また、著作者人格権は、本市及び本市が指定する者に対して一切行使することができない。

なお、コンテンツにこの契約の前から受託者または第三者が著作権を有する著作物が含まれる場合の当該著作物、並びに成果物が受託者または第三者が権利を有する著作物（無償提供のもの、いわゆるフリーソフトを含む。）である場合、これらの著作物は受託者または当該第三者に留保されるものとする。

### 14.5 検査

#### 14.5.1 検査監督権

受託者は、本市から受けた、作業現場の現地調査を含めた受託者の作業に対する検査監督及び作業の実施に係る指示に従うこと。詳細は、本業務の契約書で定める。

#### 14.5.2 成果検査

本市は、履行届を受理した日から 10 日以内に、本業務の成果について検査を実施し、受託者に検査結果を通知する。受託者は、本業務の成果が検査に合格しなかった場合、本市が指定する期間内に、本市の指示に従って補正し、あらためて履行届を提出すること。

なお、検査合格通知後であっても、本書と成果との間に著しい乖離や不一致が見られた場合は、本市と協議の上、受託者は無償で是正措置を実施すること。詳細は、本業務の契約書で定める。

### 14.6 適用文書

#### 14.6.1 「委託契約約款」

受託者は、本業務を遂行するにあたり、別紙 1 「委託契約約款」を遵守しなければならない。

#### 14.6.2 「電子計算機処理等の契約に関する情報取扱特記事項」

受託者は、本業務を遂行するにあたり、別紙 2 「電子計算機処理等の契約に関する情報取扱特記事項」を遵守しなければならない。

#### 14.6.3 「個人情報取扱特記事項」

受託者は、本業務を遂行するにあたり、別紙 3 「個人情報取扱特記事項」を遵守しなければならない。

### 14.7 その他留意事項

14.7.1 業務内容に疑義が生じた場合や不明な点がある場合には、本市委託担当者と調整し、業務内容を明確にすること。

14.7.2 本市関係部署及び個別サービス提供者・個別サービスシステム管理者と調整する必要がある場合は、委託者担当者と調整すること。

14.7.3 業務上知り得た情報が第三者に漏洩することがないように情報を管理すること。本市および個別

サービス提供者から提供した資料等は、委託期間満了日までに提供元に返却すること。また、コピーした紙資料及び電子データがあれば、委託期間満了日までに確実に廃棄・削除すること。

年 月 日

〇〇年度 〇〇小学校 放課後キッズクラブ利用申込書

運営法人 宛 次のとおり〇〇小学校放課後キッズクラブの利用を申し込みます。

I 利用児童

ふりがな		学校名	市立・国立・私立・その他（1つを○囲み）
氏名		学年・組	年 組
生年月日	年 月 日（才）		
利用区分 (1つを○囲み)	1 わくわく【区分1】	利用料：無料 利用時間：～16時	※わくわく【区分1】は、スポット利用（800円/回）を除き、16時で一斉下校となります。また、警報発表時や猛暑時等は利用できない場合があります。
	2 すくすく（ゆうやけ）【区分2A】	利用料：2,000円/月 利用時間：～17時	【留守家庭児童等のみ選択可】 ※すくすく【区分2A・B】に登録する場合は、 <b>保護者の方の就労証明書等の提出</b> が必要です。 ※すくすく【区分2A・B】の7・8月の利用料は通常の利用料に加え、 <u>±500円</u> がかかります。
	3 すくすく（ほしぞら）【区分2B】	利用料：5,000円/月 利用時間：～19時	
利用開始希望日			

II 利用頻度 ※すくすく【区分2A・B】への申込みの場合のみ記入

おおむねの利用頻度を記入してください。（利用できる日数が以下の利用日数に限定されるわけではありません。）

平日（月～金） (1つを○囲み)	週 1・2・3・4・5 日程度	土曜日の利用 (どちらかを○囲み)	あり・なし
---------------------	-----------------	----------------------	-------

III 食物アレルギーについて

食物アレルギーの有無※ (どちらかを○囲み)	あり・なし	アレルギーのある食べ物 (「あり」の場合に記載)	
---------------------------	-------	-----------------------------	--

※ 食物アレルギーが「あり」の場合は、利用区分に関わらず学校に提出する「学校生活管理指導表」（写）を提出してください。  
 ※ 学校生活では提供されない食物（そば、くるみ等）に対するアレルギー疾患を持つ児童等、学校生活管理指導表を学校に提出していない場合でも、医師の診断に基づく「学校生活管理指導表」（写）をキッズクラブへ提出ください。

IV その他健康状態等の配慮すべき事項について

その他健康状態等の 配慮すべき事項	
児童の健康状態等の配慮する事項について、職員との面談を <u>希望する</u> ・ <u>希望しない</u> （どちらかを○囲み）	

V 減免利用について ※すくすく【区分2A・B】利用料減免を希望する場合（予定含む）のみ記入

「就学援助を受けている」「市民税非課税世帯である」「生活保護世帯である」のいずれかの場合のみ減免を受けることができます。

減免の適用 (希望する場合のみ○囲み)	希望する	昨年度の減免の適用 (どちらかを○囲み)	あり・なし
------------------------	------	-------------------------	-------

VI 確認事項

<ul style="list-style-type: none"> <li>〇〇年度〇〇小学校放課後キッズクラブの「入会のしおり」について確認しました。</li> <li>当該利用申込書の記載内容及び提出書類に虚偽はありません。</li> <li>放課後キッズクラブの運営にあたり、当該利用申込書の内容や提出書類の情報について、必要に応じて、区子ども家庭支援課や利用児童が通う〇〇小学校に対して提供することを認めます。</li> <li>児童育成の観点から、必要に応じて、〇〇小学校又は放課後キッズクラブでの利用児童の活動の様子を、〇〇小学校と放課後キッズクラブとで情報共有することに差支えはありません。</li> <li>（減免を受けたい場合のみ）虚偽又は不正な申請等により、減免を受けたい場合には、連年の利用料を遡つて又払いします。また、減免の対象でなくなった場合は、「放課後キッズクラブ利用料減免適用外申出書」を速やかに提出します。</li> </ul> <p style="text-align: right;">年 月 日 保護者氏名 (自署)</p>
--

【申込みのために記入された個人情報は、放課後キッズクラブの運営以外の目的には使用しません。】

(裏面あり)

## VII 保護者等連絡先

以下の連絡先は、児童の出欠席確認や急病時等に利用します。必ずつながる連絡先の記入をお願いします。

保護者代表 <small>(日常の連絡相手方)</small>	氏名	【続柄】	同じ学校に在籍している兄弟姉妹 (いる場合に記入)		
	住所	〒	—	年 組 (名)	
	電話 (携帯)	(自宅)		年 組 (名)	
	メールアドレス				
	勤務先	(電話)		キッズ(学校) から自宅までの略図	
連絡先①	氏名	【続柄】			
	住所	〒			—
	電話 (携帯)	(自宅)			
	メールアドレス				
	勤務先	(電話)			
連絡先②	氏名	【続柄】			
	住所	〒			—
	電話 (携帯)	(自宅)			
	メールアドレス				
	勤務先	(電話)			
連絡先③	氏名	【続柄】			
	住所	〒			—
	電話 (携帯)	(自宅)			
	メールアドレス				
	勤務先	(電話)			

\*枠内に収まらない場合は、別紙で提出してください。

## VIII 児童代理引取人届出

- ・代理引取人は「VII 保護者等連絡先」欄に記入した以外の方で、当該児童の引取人となる方をご記入ください。
- ・当該代理引取人がお迎えに来られた際には、本人確認を行いますので、**免許証等、身分を証明できるものをご持参ください。**
- ・当該項目が空欄の場合、引取人は、「VII 保護者等連絡先」欄に記入した方のみとさせていただきます。

代理引取人名	続柄	住所	電話番号

## 放課後キッズクラブ事務処理欄 ※保護者の方は当該欄に記入しないでください。

受付日	すくすく【区分2A・B】登録証明書類	利用料減免			保険加入確認
		適用	対象事由	書類受理日	
	就労(予定)証明書・自営業従事者等申告書 病気・障害等申告書、診断書(写)、身体障害手帳(写) 求職活動申告書・学生証(写)・在学証明書・罹災証明書 その他( )	あり ・ なし	・就学援助を受けている ・生活保護世帯 ・市民税所得割非課税世帯		
備考					

〇〇年度 〇〇小学校 放課後キッズクラブ利用区分変更申込書

運営法人 宛 次のとおり〇〇小学校放課後キッズクラブの利用区分の変更を申し込みます。

I 利用児童

ふりがな		学校名	市立・国立・私立・その他 (1つを○囲み)
氏名		学年・組	年 組
利用区分 変更 (該当するものを○囲み)	<現在の区分>	⇒	<変更後の区分>
	1 わくわく【区分1】	⇒	すくすく(ゆうやけ)【区分2A】
	2 わくわく【区分1】	⇒	すくすく(ほしぞら)【区分2B】
	3 すくすく(ゆうやけ)【区分2A】	⇒	わくわく【区分1】
	4 すくすく(ゆうやけ)【区分2A】	⇒	すくすく(ほしぞら)【区分2B】
	5 すくすく(ほしぞら)【区分2B】	⇒	わくわく【区分1】
6 すくすく(ほしぞら)【区分2B】	⇒	すくすく(ゆうやけ)【区分2A】	
区分変更の理由 (記入必須)		利用開始希望月	

※わくわく【区分1】は、スポット利用(800円/円)を除き、16時で一斉下校となります。  
 また、わくわく【区分1】は、警報発表時や猛暑時等において、利用できない場合があります。  
 ※すくすく【区分2A・B】に登録する場合は、保護者の方の就労証明書等の提出が必要です。  
 また、月額利用料として、すくすく(ゆうやけ)【区分2A】は2,000円(～17時まで)、すくすく(ほしぞら)【区分2B】は5,000円(～19時まで)がかかります(おやつ代除く)。

II 利用頻度 ※すくすく【区分2A・B】への変更の場合のみ記入

おおむねの利用頻度を記入してください。(利用できる日数が以下の利用日数に限定されるわけではありません。)

平日(月～金) (1つを○囲み)	週 1 ・ 2 ・ 3 ・ 4 ・ 5 日程度	土曜日の利用 (どちらかを○囲み)	あり ・ なし
---------------------	-------------------------	----------------------	---------

III 減免利用 ※すくすく【区分2A・B】利用料減免を希望する場合(予定含む)のみ記入

「就学援助を受けている」「市民税非課税世帯である」「生活保護世帯である」のいずれかの場合のみ減免を受けることができます。

減免の適用 (希望する場合のみ○囲み)	希望する	昨年度の減免の適用 (どちらかを○囲み)	あり ・ なし
------------------------	------	-------------------------	---------

IV 確認事項

当該変更届及び提出書類に虚偽はありません。

年 月 日 保護者氏名 (自署)

放課後キッズクラブ事務処理欄 ※保護者の方は当該欄に記載しないでください。

受付日	すくすく【区分2A・B】登録証明書類	利用料減免		
		適用	対象事由	書類受理日
	就労(予定)証明書・自営業従事者等申告書・病気・障害等申告書・診断書(写)・身体障害手帳(写)・求職活動申告書・学生証(写)・在学証明書・罹災証明書・その他( )	あり なし	・就学援助を受けている ・生活保護世帯 ・市民税所得割非課税世帯	
備考				

就労（予定）証明書

小学校放課後キッズクラブ運営法人代表者 様

【就労者記入欄】

就労者住所	
就労者氏名	児童から見た続柄：
放課後キッズクラブ名	小学校放課後キッズクラブ
申込児童氏名・学年 ※2人以上の申込みを行う場合は、全ての児童の氏名を記載	第 学年
	第 学年
	第 学年

【事業所記入欄】

採用（内定）年月日	年 月 日 から	
現在の雇用状況	<input type="checkbox"/> 就労中 <input type="checkbox"/> 産前産後・育児休業中（ 年 月 日～ 年 月 日） <input type="checkbox"/> 採用内定もしくは放課後キッズクラブ利用開始次第就労開始	
雇用の形態	<input type="checkbox"/> 正社員 <input type="checkbox"/> 契約社員 <input type="checkbox"/> 派遣社員 <input type="checkbox"/> アルバイト・パート <input type="checkbox"/> その他（ ） ◆雇用契約期間が決まっている場合 → 年 月 日 契約終了 ◆契約更新予定 → <input type="checkbox"/> 有 <input type="checkbox"/> 無 <input type="checkbox"/> 未定	
勤務先（派遣先）の名称	※【証明欄】と同じ場合は記入不要	
勤務先（派遣先）の所在地	※【証明欄】と同じ場合は記入不要 勤務（派遣）先の電話番号	
就労状況	定例勤務時間の方	シフト勤務の方
	◆勤務時間 時 分 ～ 時 分	◆シフトと月の勤務回数を記入 ① 時 分 ～ 時 分（月 回）
	◆育児短時間勤務の場合の勤務時間 時 分 ～ 時 分	② 時 分 ～ 時 分（月 回）
		③ 時 分 ～ 時 分（月 回）
	◆勤務日数 平均 日/週	
備考		
【証明欄】 上記のとおり相違ないことを証明します。 年 月 日 （事業所所在地） （事業所名） （電話番号） （代表者職氏名）		



## 自営業従事者等申告書

放課後キッズクラブ名 ( )  
 申込児童氏名・学年 ( )

小学校放課後キッズクラブ)  
 ・ 第 ( ) 学年)

※自営業

事業所名		電話 ( ) -	
代表者名		業種	
事業所所在地 (勤務場所)			
住居との関係	同一 ・ 同一敷地内別棟 ・ 居住外 ・ その他 ( )		
事業開始年月日	年 月 日	営業時間	: ~ :
事業に従事 しない曜日	日・月・火・水・木・金・土	家人以外の 従業員	無・有 ( 人)

※就労時間

利用児童との続柄	就労時間	就労日数 (週平均)
	: ~ :	週 日
	: ~ :	週 日
	: ~ :	週 日
	: ~ :	週 日
	: ~ :	週 日
	: ~ :	週 日

※備 考

(宛先) ○○小学校放課後キッズクラブ運営法人代表者  
 上記のとおり相違ないことを申告します。

年 月 日

保護者氏名  
 (申告者)

病気・障害等申告書

放課後キッズクラブ名 ( )  
 申込児童氏名・学年 ( )

小学校放課後キッズクラブ  
 ・ 第 第 学年)

※該当する方全員

該当する項目に記入してください。	利用児童との続柄			
	病 気	病名		
		状況	・入院 ・寝たり起きたり ・通院 ・寝たきり	・入院 ・寝たり起きたり ・通院 ・寝たきり
		病院名		
		期間	年 月 日～ 年 月 日	年 月 日～ 年 月 日
		通院・往診状況	(通院) 月・週 回 (往診) 月・週 回	(通院) 月・週 回 (往診) 月・週 回
	看護 ・ 介護	病人・障害者氏名 (続柄)		
		病名・障害名		
		状況 (入院・通院等)		
		病院・施設名		
		付き添い期間	月・週 日 時 分～ 時 分	月・週 日 時 分～ 時 分
	障害者	手帳名		
		障害名		
出産	出産 (予定) 日	年 月 日	年 月 日	
備考				
(宛先) ○○小学校放課後キッズクラブ運営法人代表者 上記のとおり相違ないことを申告します。  年 月 日 保護者氏名 (申告者)				

※「出産」については、原則として、出産 (予定) 日から起算して8週間前の日の属する月の1日から、出産日から起算して8週間後の日の翌日の属する月の末日までです。(多胎妊娠の場合は、出産 (予定日) の前14週間、後8週間となります。)

(横浜市・放課後キッズクラブ利用申込書用)

## 求職活動申告書

年 月 日

〇〇小学校放課後キッズクラブ運営法人代表者

私は求職活動を行い、就労する予定であることから、〇〇小学校放課後キッズクラブのすくすく【区分2A・B】への登録を希望します。すくすく【区分2A・B】に登録後、就労した際には、速やかに就労（予定）証明書を提出します。

なお、放課後キッズクラブ利用登録日から3か月以内に就労を開始できない場合は、すくすく【区分2A・B】からわくわく【区分1】へ変更することに同意します。

【求職活動者】 住所 \_\_\_\_\_  
 氏名 \_\_\_\_\_  
 児童名 \_\_\_\_\_  
 児童との続柄 \_\_\_\_\_

求職活動の状況については次のとおりです。（□欄をチェックして必要事項を記入してください）

現在の活動状況	<input type="checkbox"/> 求職活動中 ・ 求職活動の開始時期 年 月 ・ 活動の内容 <input type="checkbox"/> 週 ・ <input type="checkbox"/> 月 日程度 <input type="checkbox"/> ハローワークへ <input type="checkbox"/> 自分で 【現在 社申請】 <input type="checkbox"/> 児童が放課後キッズクラブ利用登録後、求職活動開始予定
希望職種	
希望勤務形態	<input type="checkbox"/> 常勤 <input type="checkbox"/> パート <input type="checkbox"/> その他（ ）
希望勤務時間	平日：午前・後 時 分～午前・後 時 分（実働 時間） 土曜：午前・後 時 分～午前・後 時 分（実働 時間）
希望勤務日数	<input type="checkbox"/> 週 日（ <input type="checkbox"/> 月 <input type="checkbox"/> 火 <input type="checkbox"/> 水 <input type="checkbox"/> 木 <input type="checkbox"/> 金 <input type="checkbox"/> 土 <input type="checkbox"/> 日） <input type="checkbox"/> 1か月の勤務日数 日

※就労後、すみやかに〇〇小学校放課後キッズクラブへ就労（予定）証明書を提出してください。

※求職活動を理由にすくすく【区分2A・B】に登録できるのは、登録日から3か月です。

※本申告書を連続して提出することや期間を延長することはできません。

（横浜市・放課後キッズクラブ利用申込書用）

## 放課後キッズクラブ利用料減免適用外申出書

年 月 日

〇〇小学校放課後キッズクラブ運営法人代表者

住 所 \_\_\_\_\_

保護者氏名  
(自署) \_\_\_\_\_

利用料減免の適用対象から外れたため、下記のとおり申告します。

## 記

(ふりがな) 児童氏名		学年	年生
利用料減免の 適用外の理由	1 就学援助を受給しなくなったため 2 生活保護世帯ではなくなったため 3 市民税所得割非課税世帯ではなくなったため 4 その他 ( )		
事由発生月	令和 年 月		

※事由発生月の翌月から減免が適用されなくなります。

## 放課後児童クラブ入会申込書

年 月 日

(クラブ名)

様

(保護者)

住 所 \_\_\_\_\_

署 名 \_\_\_\_\_

電 話 ( ) \_\_\_\_\_

次のとおり放課後児童クラブへの入会を申し込みます。

なお、利用にあたっては、運営者の関係事項を守り、指示に従います。

利用 する 児童	ふりがな		生年 月日	年 月 日
	氏 名			
	学 校 名			第 学 年

利 用 予 定 日 数	平日週 日 (月・火・水・木・金) ・ 土曜日 ・ その他 ( )
退 所 予 定 時 間	18:00 ・ 18:30 ・ 19:00～
入 会 申 込 の 理 由	
入 会 (予 定) 日	年 月 日

利用 する 児童 の 世 帯 状 況	氏 名	対象児童 との続柄	勤務先等の名称・所属・所在地・電話 番号等	労働等により昼間不在等 となる曜日、週日数
			( )	月・火・水・木・金・土 不定期( 日)
			( )	月・火・水・木・金・土 不定期( 日)
			( )	月・火・水・木・金・土 不定期( 日)
			( )	月・火・水・木・金・土 不定期( 日)

(備考) ・ 記名、押印で、署名に替えることができます。  
 ・ 年度途中に変更があった場合はすみやかに申出ること。  
 ・ ご記入いただいた個人情報、当クラブにて厳重に管理し、放課後児童ク  
 ラブの運営以外の目的では使用いたしません。

(裏面あり)

児 童 カ ー ド							
氏 名				生年月日	年 月 日		
住 所				電話番号	( )		
学 校 名				年度	年	組	担任名
				年度	年	組	担任名
				年度	年	組	担任名
				年度	年	組	担任名
				年度	年	組	担任名
				年度	年	組	担任名
健 康 状 況	(現在かかっている病気や日常飲んでいる薬や、健康上留意しなければならないことがあれば具体的に記載してください。)						
アレルギ-の有無	有 ・ 無						
アレルギ-の原因	食物【 】						
	食物以外【 】						
→アレルギーがある場合は、学校に提出する「 <u>学校生活指導管理表</u> 」(写)をあわせて提出してください。							
特 記 事 項							
ク ラ ブ 退 所 予 定 時 間	時 分						
自 宅 か ら ク ラ ブ ま だ の 略 図							
緊 急 連 絡 先 (氏名・電話番号)	1.			2.			

放課後児童クラブ継続利用申込書

年 月 日

(クラブ名)

様

(保護者)

住 所

署 名

電 話 ( )

次のとおり放課後児童クラブへの令和 年度の利用を申し込みます。

なお、利用にあたっては、運営者の関係事項を守り、指示に従います。

利用する児童	ふりがな		生年月日	年	月	日
	氏 名					
	学 校 名			第	学 年	

利用予定日数	平日週 日 (月・火・水・木・金) ・ 土曜日 ・ その他 ( )
退所予定時間	18:00 ・ 18:30 ・ 19:00～
継続利用の理由	

利用する児童の世帯状況	氏 名	対象児童との続柄	勤務先等の名称・所属・所在地・電話番号等	労働等により昼間不在等となる曜日、週日数
			( )	月・火・水・木・金・土 不定期( 日)
			( )	月・火・水・木・金・土 不定期( 日)
			( )	月・火・水・木・金・土 不定期( 日)
			( )	月・火・水・木・金・土 不定期( 日)

(備考) ・記名、押印で、署名に替えることができます。  
 ・年度途中に変更があった場合はすみやかに申出ること。  
 ・ご記入いただいた個人情報は、当クラブにて厳重に管理し、放課後児童クラブの運営以外の目的では使用いたしません。

(裏面あり)

# 児童カード

氏名			生年月日	年 月 日	
住所			電話番号	( )	
学校名		年度	年	組	担任名
		年度	年	組	担任名
		年度	年	組	担任名
		年度	年	組	担任名
		年度	年	組	担任名
		年度	年	組	担任名
健康状況	(現在かかっている病気や日常飲んでいる薬や、健康上留意しなければならないことがあれば具体的に記載してください。)				
アレルギーの有無	有 ・ 無				
アレルギーの原因	食物【 】				
	食物以外【 】				
→アレルギーがある場合は、学校に提出する「 <u>学校生活指導管理表</u> 」(写)をあわせて提出してください。					
特記事項					
クラブ退所予定時間	時 分				
自宅からクラブまでの略図					
緊急連絡先 (氏名・電話番号)	1.		2.		



## 放課後児童クラブ退会届出書

年 月 日

(クラブ名)

様

(保護者)

住 所

署 名

電 話 ( )

放課後児童クラブを退会したいので、次のとおり届け出ます。

退会児童	ふりがな		生年月日	年 月 日
	氏 名			
	学 校 名		学年	第 学年
退 会 日	年 月 日			
退 会 の 理 由				

(備考) 記名・押印で署名に替えることができる。

## 放課後児童クラブ休会申出書

年 月 日

(クラブ名)

様

(保護者)

住 所

署 名

電 話 ( )

放課後児童クラブを休会したいので、次のとおり届け出ます。

休会児童	ふりがな		生年月日	年 月 日
	氏 名			
	学 校 名		学年	第 学年
休会期間	年 月 日 ~ 年 月 日 (予定)			
休 会 の 理 由				

(備考) 記名・押印で署名に替えることができる。

## 放課後児童クラブ入会（継続利用）決定通知書

年 月 日

様  
\_\_\_\_\_名称  
〔法人はクラブ名も  
記入すること〕  
\_\_\_\_\_代表者職氏名  
\_\_\_\_\_

放課後児童クラブへの入会について、次のとおり決定します。

入 会 児 童	氏 名		生 年 月 日	年 月 日
	学 校 名		学 年	第 学年
保 護 者	氏 名			
	住 所			



放課後児童クラブ日誌

日時		天候		記録者	
開所時間					

【単位 1】

児童参加時間		開所時間				
参加児童	出席 (人)		欠席 (人)		障害児	
	障害児 (人)		障害児 (人)		氏名	参加時間
1年生						
2年生						
3年生						
4年生						
5年生						
6年生						
合計						

【単位 2】

児童参加時間		開所時間				
参加児童	出席 (人)		欠席 (人)		障害児	
	障害児 (人)		障害児 (人)		氏名	参加時間
1年生						
2年生						
3年生						
4年生						
5年生						
6年生						
合計						

【単位 3】

児童参加時間		開所時間				
参加児童	出席 (人)		欠席 (人)		障害児	
	障害児 (人)		障害児 (人)		氏名	参加時間
1年生						
2年生						
3年生						
4年生						
5年生						
6年生						
合計						



◆障害児の登録児童数

支援の単位	単位1	単位2	単位3	単位4	単位5	単位6	合計
わくわく【区分1】							
すくすく【区分2】							0人

◆職員追加配置の有無

以下の項目について、支援の単位ごとに、配置ができていた場合は「○」できていない場合には「×」を入力してください。

**推 進**：実施要綱第8条第1項で定める職員最低配置基準に加えて1名以上職員を追加配置できていた場合（障害児受入推進加算補助による追加配置）

**強化①**：障害児受入推進加算補助による追加配置に加えて1名以上職員を追加配置できていた場合

**強化②**：強化①による追加配置に加えて1名以上職員を追加配置できていた場合

**強化③**：強化②による追加配置に加えて1名以上職員を追加配置できていた場合

日	曜日	単位1			単位2			単位3			単位4			単位5			単位6				
		実施分類	推進	強化①	強化②	強化③	実施分類	推進	強化①	強化②	強化③	実施分類	推進	強化①	強化②	強化③	実施分類	推進	強化①	強化②	強化③
1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
18	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
19	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
21	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
22	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
23	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
24	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
26	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
27	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
28	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

◆障害児受入推進加算補助・障害児受入強化推進加算補助の算定対象となる日数

1 障害児受入推進加算補助

項目	単位1	単位2	単位3	単位4	単位5	単位6
配置人数を満たしている日数	0	0	0	0	0	0

2 障害児受入強化推進加算補助

項目	単位1	単位2	単位3	単位4	単位5	単位6
配置人数を満たしている日数	強化①	0	0	0	0	0
	強化②	0	0	0	0	0
	強化③	0	0	0	0	0

放課後児童クラブ 月別開所状況及び職員配置状況表 ( 0 月分)

クラブ名: \_\_\_\_\_ 0

◆職員追加配置の有無

以下の項目について、支援の単位ごとに、職員の追加配置ができていた場合は「○」、できていない場合には「×」を入力してください。  
 推 進：条例第10条第2項で定める職員の最低配置基準に加えて、1名以上職員を追加配置した場合。(=障害児受入推進加算補助による追加配置)  
 強化①：障害児受入推進加算補助による追加配置に加えて、1名以上職員を追加配置した場合。  
 強化②：強化①による追加配置に加えて、1名以上職員を追加配置した場合。  
 強化③：強化②による追加配置に加えて、1名以上職員を追加配置した場合。

日	曜日	開所日等の区分	単位1				単位2				単位3				単位4				単位5								
			開所日の算定	推進	強化①	強化②	強化③	開所日の算定	推進	強化①	強化②	強化③	開所日の算定	推進	強化①	強化②	強化③	開所日の算定	推進	強化①	強化②	強化③	開所日の算定	推進	強化①	強化②	強化③
1																											
2																											
3																											
4																											
5																											
6																											
7																											
8																											
9																											
10																											
11																											
12																											
13																											
14																											
15																											
16																											
17																											
18																											
19																											
20																											
21																											
22																											
23																											
24																											
25																											
26																											
27																											
28																											
29																											
30																											
31																											

◆障害児受入推進加算補助・障害児受入強化推進加算補助の算定対象となる日数

		単位1	単位2	単位3	単位4	単位5
障害児受入推進加算補助		0日	0日	0日	0日	0日
障害児受入強化推進加算補助	強化①	0日	0日	0日	0日	0日
	強化②	0日	0日	0日	0日	0日
	強化③	0日	0日	0日	0日	0日



## 委託契約約款

(総則)

第1条 委託者及び受託者は、この約款（契約書を含む。以下同じ。）に基づき、設計図書（別添の設計書、仕様書、図面、現場説明書及びこれらの図書に対する質問回答書をいう。以下同じ。）に従い、日本国の法令を遵守し、この契約（この約款及び設計図書を内容とする業務の委託契約をいう。以下同じ。）を履行しなければならない。

2 受託者は、契約書記載の契約の履行を履行期間内に全部完了（設計図書に定めがある場合は、契約の履行の目的物の引渡しを含む。以下同じ。）し、委託者は、その契約代金を支払うものとする。

3 履行方法その他契約を履行するために必要な一切の手段については、この約款及び設計図書に特別の定めがある場合を除き、受託者がその責任において定める。

4 受託者は、この契約の履行に関して知り得た秘密を漏らしてはならない。この契約が終了した後も同様とする。

5 この約款に定める請求、通知、報告、申出、承諾及び解除は、書面により行わなければならない。

6 この契約の履行に関して委託者と受託者との間で用いる言語は、日本語とする。

7 この約款に定める金銭の支払に用いる通貨は、日本円とする。

8 この契約の履行に関して委託者と受託者との間で用いる計量単位は、設計図書に特別の定めがある場合を除き、計量法（平成4年法律第51号）に定めるものとする。

9 この約款及び設計図書における期間の定めについては民法（明治29年法律第89号）及び商法（明治32年法律第48号）の定めるところによるものとする。

10 この契約は、日本国の法令に準拠するものとする。

11 この契約に係る訴訟については、専属管轄を除くほか、委託者の所在地を管轄する裁判所に行うものとする。

12 受託者が共同企業体を結成している場合においては、委託者は、この契約に基づくすべての行為を共同企業体の代表者に対して行うものとし、委託者が当該代表者に対して行ったこの契約に基づくすべての行為は、当該共同企業体のすべての構成員に対して行ったものとみなし、また、受託者は、委託者に対して行うこの契約に基づくすべての行為について当該代表者を通じて行わなければならない。

(内訳書及び工程表)

第2条 受託者は、この契約書を提出する際に設計図書に基づいて、内訳書を作成し、委託者に提出しなければならない。ただし、別添の設計書に内訳を記載することによりこれに代えることができる。

2 受託者は、この契約締結後5日（横浜市の休日を定める条例（平成3年12月横浜市条例第54号）第1条第1項に規定する本市の休日を除く。）以内に、設計図書に基づいて、工程表を作成し、委託者に提出しなければならない。ただし、

委託者が必要がないと認めるときは、省略することができる。

3 内訳書及び工程表は、委託者及び受託者を拘束するものではない。

(着手届出)

第3条 受託者は、この契約締結後5日（横浜市の休日を定める条例（平成3年12月横浜市条例第54号）第1条第1項に規定する本市の休日を除く。）以内に、契約履行着手届出書を、委託者に提出しなければならない。ただし、委託者が必要がないと認めるときは、省略することができる。

(権利義務の譲渡等の制限)

第4条 受託者は、この契約により生ずる権利又は義務を第三者に譲渡し、若しくは継承させ、又はその権利を担保に供してはならない。ただし、あらかじめ、委託者の承諾を得た場合は、この限りでない。

2 受託者は、契約の履行の目的物並びに材料のうち第11条第2項の規定による検査に合格したものと及び第32条第4項の規定による部分払のための確認を受けたものを第三者に譲渡し、貸与し、又は抵当権その他の担保の目的に供してはならない。ただし、あらかじめ、委託者の承諾を得た場合は、この限りでない。

(著作権の譲渡等)

第5条 受託者は、契約の履行の目的物が著作権法（昭和45年法律第48号）第2条第1項第1号に規定する著作物（以下この条において「著作物」という。）に該当する場合には、当該著作物に係る受託者の著作権（著作権法第21条から第28条までに規定する権利をいう。）を当該著作物の引渡時に委託者に無償で譲渡するものとする。ただし、受託者がこの契約の締結前から権利を有している著作物の著作権は、受託者に留保するものとし、この著作物を改変、翻案又は翻訳することにより作成された著作物の著作権は、当該著作権の引渡時に受託者が当該権利の一部を委託者に無償で譲渡することにより、委託者と受託者の共有とするものとする。

2 委託者は、契約の履行の目的物が著作物に該当するとしなにかかわらず、当該契約の履行の目的物の内容を受託者の承諾なく自由に公表することができ、また、当該契約の履行の目的物が著作物に該当する場合には、受託者が承諾したときに限り、既に受託者が当該著作物に表示した氏名を変更することができる。

3 受託者は、契約の履行の目的物が著作物に該当する場合において、委託者が当該著作物の利用目的の実現のためにその内容を改変しようとするときは、その改変に同意するものとする。また、委託者は、契約の履行の目的物が著作物に該当しない場合には、当該契約の履行の目的物の内容を受託者の承諾なく自由に改変することができる。

4 受託者は、契約の履行の目的物（契約を履行する上で得られた記録等を含む。）が著作物に該当するとしなにかかわらず、委託者が承諾した場合には、当該契約の履行

の目的物を使用又は複製し、また、第1条第4項の規定にかかわらず当該契約の履行の目的物の内容を公表することができる。

5 受託者は、第1項ただし書の規定により共有となった著作物を第三者に提供する場合においては、あらかじめ、委託者の承諾を得なければならない。この場合において、承諾の内容は、委託者と受託者とが協議して定める。

6 委託者は、受託者が契約の履行の目的物の作成に当たって開発したプログラム（著作権法第10条第1項第9号に規定するプログラムの著作物をいう。）及びデータベース（著作権法第12条の2に規定するデータベースの著作物をいう。）について、受託者が承諾した場合には、別に定めるところにより、当該プログラム及びデータベースを利用することができる。

7 受託者は、次条第1項ただし書の規定により第三者に委任し、又は請け負わせる場合には、前各号に定める規定を当該第三者が遵守するように必要な措置を講じなければならない。

（一括委任又は一括下請負の禁止）

第6条 受託者は、契約の履行の全部又は主たる部分を一括して第三者に委任し、又は請け負わせてはならない。ただし、あらかじめ、委託者の承諾を得た場合は、この限りでない。

2 受託者は、契約の履行において下請負契約を締結した場合は、下請負人の商号又は名称その他委託者の定める事項を、すみやかに委託者に通知しなければならない。

（特許権等の使用）

第7条 受託者は、特許権、実用新案権、意匠権、商標権その他日本国の法令に基づき保護される第三者の権利（以下「特許権等」という。）の対象となっている材料、履行方法等を使用するときは、その使用に関する一切の責任を負わなければならない。ただし、委託者がその材料、履行方法等を指定した場合において、設計図書に特許権等の対象である旨の明示がなく、かつ、受託者がその存在を知らなかったときは、委託者は、受託者がその使用に関して要した費用を負担しなければならない。

（特許権等の発明等）

第8条 受託者は、契約の履行に当たり、特許権等の対象となるべき発明又は考案をした場合には、委託者に通知しなければならない。

2 前項の場合において、当該特許権等の取得のための手続及び権利の帰属等に関する詳細については、委託者と受託者とが協議して定めるものとする。

（現場責任者等）

第9条 受託者は、この契約の履行に当たり、現場責任者を定め、契約締結後5日（横浜市の休日を含める（平成30年12月横浜市条例第54号）第1条第1項に規定する本市の休日を除く。）以内に、その氏名その他必要な事項を委託者に通知しなければならない。現場責任者を変更した場合も

同様とする。

2 現場責任者は、この契約の履行に関して従事者を指揮監督するものとする。

3 受託者は、この契約の履行の着手前に、契約の履行に従事する者の氏名その他必要な事項を委託者に通知しなければならない。

（監督員）

第9条の2 委託者は、監督員を置いたときは、その氏名を受託者に通知しなければならない。監督員を変更したときも、同様とする。ただし、市長、水道事業管理者又は交通事業管理者が、それぞれの権限（他の者に委任している場合は、当該受任者の権限を含むものとする。）に属する契約について特に定めた場合には、その氏名を受託者に通知しなくてよいものとする。

2 監督員は、この約款の他の条項に定めるもの及びこの約款に基づく委託者の権限とされる事項のうち委託者が必要と認めて監督員に委任したもののほか、設計図書に定めるところにより、次に掲げる権限を有する。

(1) この契約の履行についての受託者又は受託者の現場責任者に対する指示、承諾又は協議

(2) この契約の履行の進捗の確認、設計図書の記載内容と履行内容との照合その他契約の履行状況の調査

3 委託者は、2人以上の監督員を置き、前項の権限を分担させたときにあってはそれぞれの監督員の有する権限の内容を、監督員にこの約款に基づく委託者の権限の一部を委任したときにあっては当該委任した権限の内容を、受託者に通知しなければならない。

4 委託者が監督員を置いたときは、受託者は、この約款に定める請求、通知、報告、申出、承諾及び解除については、設計図書に定めるものを除き、監督員を経由して行うものとする。この場合においては、監督員に到達した日をもって委託者に到達したものとみなす。

5 委託者が監督員を置かないときは、この約款に定める監督員の権限は、委託者に帰属する。

（履行の報告）

第10条 受託者は、設計図書に定めるところにより、この契約の履行について、委託者に報告しなければならない。

（材料の品質、検査等）

第11条 受託者は、設計図書に品質が明示されていない材料については、中等の品質を有するものを使用しなければならない。

2 受託者は、設計図書において委託者の検査（確認を含む。以下この条において同じ。）を受けて使用すべきものと指定された材料については、当該検査に合格したものを使用しなければならない。この場合において、検査に直接必要な費用は、受託者の負担とする。

3 委託者は、受託者から前項の検査を求められたときは、当該請求を受けた日から7日以内に、これに応じなければならない。

(支給材料及び貸与品)

第12条 委託者から受託者に支給する材料（以下「支給材料」という。）及び貸与する機械器具（以下「貸与品」という。）の品名、数量、品質、規格又は性能、引渡場所及び引渡時期は、設計図書に定めるところによる。

2 委託者は、支給材料又は貸与品を受託者の立会いの上、委託者の負担において、検査して引き渡さなければならない。この場合において、当該検査の結果、その品名、数量、品質、規格又は性能が設計書の定めと異なり、又は使用に適当でないことを認めるときは、受託者は、遅滞なく、その旨を委託者に通知しなければならない。

3 受託者は、材料又は貸与品の引渡しを受けたときは、当該引渡しを受けた日から7日以内に、委託者に受領書又は借用書を提出しなければならない。

4 委託者は、受託者から第2項後段の規定による通知を受けた場合において、必要があると認められるときは、当該支給材料若しくは貸与品に代えて他の支給材料若しくは貸与品を引き渡し、又は支給材料若しくは貸与品の品名、数量、品質、規格若しくは性能を変更しなければならない。

5 委託者は、前項の規定にかかわらず、受託者に対して、その理由を明示して、当該支給材料又は貸与品の使用を求めることができる。

6 委託者は、必要があると認めるときは、支給材料又は貸与品の品名、数量、品質、規格若しくは性能、引渡場所又は引渡時期を変更することができる。

7 委託者は、前3項の場合において、必要があると認められるときは履行期間又は契約代金額を変更し、受託者に損害を及ぼしたときは、必要な費用を負担しなければならない。

8 受託者は、支給材料及び貸与品を善良な管理者の注意をもって保管しなければならない。

9 受託者は、支給材料又は貸与品の引渡しを受けた後、当該支給材料又は貸与品に種類、品質又は数量に関して契約の内容に適合しないもの（第2項の検査により発見することが困難であったものに限る。）があり、使用に適当でないことを認めるときは、直ちに、その旨を委託者に通知しなければならない。この場合においては、第4項、第5項及び第7項の規定を準用する。

10 受託者は、契約の履行の全部の完了、設計図書の変更等によって不用となった支給材料又は貸与品を、設計図書に定めるところにより、委託者に返還しなければならない。

11 受託者は、故意又は過失により支給材料又は貸与品が滅失し、若しくはき損し、又はその返還が不可能となったときは、委託者の指定した期間内に代品を納め、若しくは原状に復し、又は損害を賠償しなければならない。

12 受託者は、支給材料又は貸与品の使用方法が設計図書に明示されていないときは、委託者の指示に従わなければならない。

(設計図書に不適合な場合の措置等)

第13条 受託者は、契約の履行が設計図書に適合しない場合において、委託者が、再履行その他の措置を請求したときは、これに従わなければならない。

2 委託者は、前項の不適合が委託者の指示による等委託者の責めに帰すべき理由による場合であって、必要があると認められるときは履行期間又は契約代金額を変更し、受託者に損害を及ぼしたときは必要な費用を負担しなければならない。

(条件変更等)

第14条 受託者は、契約の履行に当たり、次の各号のいずれかに該当する事実を発見したときは、直ちに、その旨を委託者に通知し、その確認を求めなければならない。

(1) 設計図書の表示が明確でないこと（設計書、図面、仕様書、現場説明書及びこれらの図書に対する質問回答書が交互符合しないこと、並びに設計図書に誤り又は漏れがあることを含む。）。

(2) 履行場所の形状、地質、湧水等の状態、履行上の制約等設計図書に示された自然的又は人為的な履行条件と実際の履行場所の状態が一致しないこと。

(3) 設計図書で明示されていない履行条件について、予期することのできない特別の状態が生じたこと。

2 委託者は、前項の確認を求められたとき、又は自ら同項各号に掲げる事実を発見したときは、受託者の立会いの上、直ちに、調査を行わなければならない。ただし、受託者が立会いに応じない場合には、受託者の立会いを得ずに調査を行うことができる。

3 委託者は、前項の規定による調査について、受託者の意見を聴いた上、当該調査の結果（これに対して執るべき措置を指示する必要があるときは、当該指示を含む。）をとりまとめ、当該調査の終了後14日以内に、受託者に通知しなければならない。ただし、委託者は、当該期間内に受託者に通知することができないやむを得ない理由があるときは、あらかじめ、受託者の意見を聴いた上、当該期間を延長することができる。

4 前項の調査の結果、第1項各号に掲げる事実が委託者及び受託者によって確認された場合において、必要があると認められるときは、次に掲げるところにより、設計図書を訂正し、又は変更しなければならない。

(1) 第1項第1号に該当し 委託者が行う。  
、設計図書を訂正する場合

(2) 第1項第2号又は第3号に該当し、設計図書を変更する場合で、契約の履行の内容の変更を伴うもの

(3) 第1項第2号又は第3号に該当し、設計図書を変更する場合で、契約の

履行の内容の変更を伴わないもの

5 前項の規定により設計図書の訂正又は変更を行った場合において、委託者は、必要があると認められるときは履行期間又は契約代金額を変更し、受託者に損害を及ぼしたときは必要な費用を負担しなければならない。

(設計図書の変更)

第15条 委託者は、前条第4項に定めるものを除くほか、必要があると認めるときは、設計図書の変更の内容を受託者に通知して、設計図書を変更することができる。この場合において、委託者は、必要があると認められるときは履行期間又は契約代金額を変更し、受託者に損害を及ぼしたときは必要な費用を負担しなければならない。

(代替方法等の提案)

第16条 受託者は、設計図書等について、技術的又は経済的に優れた代替方法その他改良事項を発見し、又は発案したときは、委託者に対して、当該発見又は発案に基づき設計図書等の変更を提案することができる。

2 委託者は、前項に規定する受託者の提案を受けた場合において、必要があると認めるときは、設計図書等の変更を受託者に通知しなければならない。

3 委託者は、前項の規定により設計図書等が変更された場合において、必要があると認められるときは、履行期間又は契約代金額を変更しなければならない。

(契約の履行の一時中止)

第17条 履行場所等の確保ができない等のため又は暴風、豪雨、洪水、高潮、地震、地滑り、落盤、火災その他の自然的若しくは人為的な事象（以下「天災等」という。）であって受託者の責めに帰すことができないものにより、契約の履行の目的物等に損害を生じ、若しくは履行場所の状態が変動したため、受託者が契約を履行できないと認められるときは、委託者は、契約の履行の一時中止の内容を直ちに受託者に通知して、契約の履行の全部又は一部を一時中止させなければならない。

2 委託者は、前項に定めるものを除くほか、必要があると認めるときは、契約の履行の全部又は一部を一時中止させることができる。

3 委託者は、前2項の規定により契約の履行を一時中止させた場合において、必要があると認められるときは履行期間又は契約代金額を変更し、受託者が契約の履行の続行に備え履行場所を維持し、又は従事者、機械器具等を保持するための費用等の契約の履行の一時中止に伴う増加費用を必要としたときその他受託者に損害を及ぼしたときは必要な費用を負担しなければならない。

(履行期間の延長)

第18条 受託者は、その責めに帰すことができない理由により履行期間内に業務を完了することができないときは、その理由を明示した書面により、委託者に履行期間の延長を請求することができる。

2 委託者は、前項の規定による請求があった場合において、必要があると認められるときは、履行期間を延長しなければならない。委託者は、その履行期間の延長が委託者の責めに帰すべき理由による場合においては、契約代金額について必要と認められる変更を行い、又は受託者に損害を及ぼしたときは必要な費用を負担しなければならない。

(履行期間の短縮等)

第19条 委託者は、特別の理由により履行期間を短縮する必要があるときは、受託者に対して、履行期間の短縮を求めることができる。

2 委託者は、この約款の他の条項の規定により履行期間を延長すべき場合において、特別の理由があるときは、延長する履行期間について、受託者に通常必要とされる履行期間に満たない履行期間への変更を請求することができる。

3 前2項の場合において、委託者は、必要があると認められるときは契約代金額を変更し、受託者に損害を及ぼしたときは、必要な費用を負担しなければならない。

(履行期間の変更の方法)

第20条 第12条第7項（同条第9項後段において準用する場合を含む。）、第13条第2項、第14条第5項、第15条、第16条第3項、第17条第3項、第18条第2項又は前条第1項若しくは第2項の規定による履行期間の変更については、委託者と受託者とが協議して定める。ただし、当該協議の開始の日から14日以内に当該協議が成立しない場合には、委託者は、履行期間を変更し、受託者に通知するものとする。

2 前項の協議の開始の日については、委託者が受託者の意見を聴いて定め、受託者に通知する。

(契約代金額等の変更の方法)

第21条 第12条第7項（同条第9項後段において準用する場合を含む。）、第13条第2項、第14条第5項、第15条、第16条第3項、第17条第3項、第18条第2項又は第19条第3項の規定による契約代金額の変更については、契約締結時の価格を基礎として、委託者と受託者とが協議して定める。ただし、協議開始の日から21日以内に当該協議が成立しない場合には、委託者は、契約代金額を変更し、受託者に通知するものとする。

2 前項の協議の開始の日については、委託者が受託者の意見を聴いて定め、受託者に通知するものとする。

3 第12条第7項（同条第9項後段において準用する場合を含む。）、第13条第2項、第14条第5項、第15条、第17条第3項、第18条第2項、第19条第3項、第23条第4項、第24条ただし書又は第30条第3項の規定により委託者が負担する費用の額については、委託者と受託者とが協議して定める。

(賃金又は物価の変動に基づく契約代金額の変更)

第22条 委託者又は受託者は、契約期間内で委託契約締結の日から12月を経過した後に、日本国内における賃金水準又は物価水準の変動により契約代金額が不適当となったと認めるときは、相手方に対して契約代金額の変更を請求する

ことができる。

- 2 委託者又は受託者は、前項の規定による請求があったときは、変動前委託代金額（契約代金額から当該請求時の履行済部分に相応する委託代金額を控除した額をいう。以下この条において同じ。）と変動後委託代金額（変動後の賃金又は物価を基礎として算出した変動前委託代金額に相応する額をいう。以下この条において同じ。）との差額のうち、変動前委託代金額の1,000分の15を超える額につき、契約代金額の変更に応じなければならない。
- 3 変動前委託代金額及び変動後委託代金額は、請求のあった日を基準とし、物価指数等に基づき委託者と受託者が協議して定める。ただし、当該協議の開始の日から21日以内に当該協議が成立しない場合には、委託者は、変動前委託代金額及び変動後委託代金額を定め、受託者に通知する。
- 4 第1項の規定による請求は、この条の規定により契約代金額の変更を行った後、再度行うことができる。この場合においては、同項中「委託契約締結の日」とあるのは、「直前のこの条に基づく契約代金額変更の基準とした日」と読み替えるものとする
- 5 特別な要因により履行期間内に主要な材料の日本国内における価格に著しい変動を生じ、契約代金額が不適当となったときは、委託者又は受託者は、契約代金額の変更を求めることができる。
- 6 予期することのできない特別な事情により、履行期間内に日本国内において急激なインフレーション又はデフレーションを生じ、契約代金額が著しく不適当となったときは、委託者又は受託者は、前項の規定にかかわらず、契約代金額の変更を求めることができる。
- 7 前2項の規定による請求があった場合において、当該契約代金額の変更については、委託者と受託者とが協議して定める。ただし、当該協議の開始の日から21日以内に当該協議が成立しない場合には、委託者は、契約代金額を変更し、受託者に通知するものとする。
- 8 前項の協議の開始の日については、委託者が受託者の意見を聴いて定め、受託者に通知する。

#### （臨機の措置）

- 第23条 受託者は、災害防止等のため必要があると認めるときは、臨機の措置を執らなければならない。この場合において、必要があると認めるときは、受託者は、あらかじめ、委託者の意見を聴かなければならない。ただし、緊急やむを得ない事情があるときは、この限りでない。
- 2 受託者は、前項の場合においては、その執った措置の内容について委託者に直ちに通知しなければならない。
  - 3 委託者は、災害の防止その他契約の履行上特に必要があると認めるときは、受託者に対して臨機の措置を執ることを請求することができる。
  - 4 受託者が第1項又は前項の規定により臨機の措置を執った場合は、当該措置に要した費用のうち、受託者が契約代金額の範囲内において負担することが適当でないことと認めら

れる部分については、委託者がこれを負担する。

#### （一般的損害）

第24条 契約の履行について生じた損害（次条第1項又は第2項に規定する損害を除く。）は、受託者の負担とする。ただし、当該損害のうち委託者の責めに帰すべき理由により生じたもの（設計図書に定めるところにより付された保険によりてん補された部分を除く。）については、委託者がこれを負担しなければならない。

#### （第三者に及ぼした損害）

第25条 契約の履行について第三者に損害を及ぼしたときは、次項に定める場合を除き、受託者がその損害を賠償しなければならない。ただし、その損害のうち委託者の責めに帰すべき理由により生じたもの（設計図書に定めるところにより付された保険によりてん補された部分を除く。）については、委託者がこれを負担しなければならない。ただし、受託者がその材料又は指示が不適当であることを知りながらこれを通知しなかったときは、この限りでない。

- 2 契約の履行に伴い通常避けることができない騒音、振動、地盤沈下、地下水の断絶等の理由により第三者に損害（設計図書に定めるところにより付された保険によりてん補された部分を除く。）を及ぼしたときは、委託者がその損害を負担しなければならない。ただし、その損害のうち契約の履行につき受託者が善良な管理者の注意義務を怠ったことにより生じたものについては、受託者がこれを負担しなければならない。
- 3 前2項の場合その他契約の履行について第三者との間に紛争を生じた場合においては、委託者と受託者とが協議してその処理解決にあたるものとする。

#### （契約代金額の変更に代える設計図書の変更）

第26条 委託者は、第12条第7項（同条第9項後段において準用する場合を含む。）、第13条第2項、第14条第5項、第15条、第16条第3項、第17条第3項、第18条第2項、第19条第3項、第22条第1項、第5項若しくは第6項、第23条第4項、第24条又は第30条第3項の規定により契約代金額を変更すべき場合又は費用を負担すべき場合において、特別の理由があるときは、変更すべき契約代金額又は負担すべき費用の全部又は一部に代えて設計図書を変更することができる。この場合において、設計図書の変更の内容は、委託者と受託者とが協議して定める。ただし、協議開始の日から21日以内に当該協議が成立しない場合には、委託者は、設計図書の変更の内容を定め、受託者に通知するものとする。

- 2 前項の協議の開始の日については、委託者が受託者の意見を聴いて定め、受託者に通知する。

#### （中間検査）

第27条 受託者は、契約の履行に関し、委託者が必要と認めるときは、契約の履行の完了前に、受託者の立会いの上、委託者の検査を受けなければならない。この場合において、検査に直接必要な費用は、受託者の負担とする。ただし、

委託者の故意又は過失により、過分の費用を要した分については、委託者がこれを負担しなければならない。

2 中間検査の実施の期日及び場所は、委託者と受託者とが協議して定める。

3 受託者は、中間検査の期日までに、当該検査に係る準備を完了しなければならない。

4 受託者は、正当な理由なく中間検査に立ち会わなかったときは、中間検査の結果について異議を申し出ることができない。

(完了検査)

第28条 受託者は、契約の履行の全部が完了したときは、遅滞なく、その旨を委託者に通知しなければならない。

2 委託者は、前項の規定による通知を受けたときは、その日から起算して10日以内に、受託者の立会いの上、契約の履行の全部の完了を確認するための検査を完了しなければならない。この場合において、検査に直接必要な費用は、受託者の負担とする。ただし、委託者の故意又は過失により、過分の費用を要した分については、委託者がこれを負担しなければならない。

3 受託者は、契約の履行の内容が前項の規定による検査に合格しないときは、直ちに、必要な措置を執った上、委託者の検査を受けなければならない。この場合においては、必要な措置の完了を契約の履行の全部の完了とみなして前2項の規定を適用する。

(契約代金の支払)

第29条 受託者は、前条第2項(同条第3項後段の規定により適用される場合を含む。第3項において同じ。)の規定による検査に合格したときは、委託者に契約代金の支払を請求することができる。

2 委託者は、前項の規定による請求を受けたときは、その日から起算して30日以内に契約代金を支払わなければならない。

3 委託者がその責めに帰すべき理由により前条第2項に規定する期間内に検査をしないときは、その期限を超過した日から検査をした日までの日数は、前項の期間(以下この項において「約定期間」という。)の日数から差し引くものとする。この場合において、その遅延日数が約定期間の日数を超えるときは、約定期間は、遅延日数が約定期間の日数を超えた日において満了したものとみなす。

(消費税等率変動に伴う契約代金額の変更)

第29条の2 消費税法(昭63年法律第108号)等の改正等によって消費税等率に変動が生じた場合は、特段の変更手続を行うことなく、相当額を加減したものを契約代金額とする。ただし、国が定める経過措置等が適用され、消費税等額に変動が生じない場合には、当該経過措置等の取扱いに従うものとする。

(完了検査前の使用)

第30条 委託者は、第28条第2項の規定による検査前においても、契約の履行の目的物の全部又は一部を受託者の承諾

を得て使用することができる。

2 前項の場合においては、委託者は、その使用部分を善良な管理者の注意をもって使用しなければならない。

3 委託者は、第1項の規定による使用により受託者に損害を及ぼしたときは、必要な費用を負担しなければならない。(前金払)

第31条 受託者は、別に定めるところにより、前払金の支払を委託者に請求することができる。

(部分払及び部分検査)

第32条 受託者は、契約の履行の全部の完了前に、履行済部分に相応する契約代金額について、次項以下に定めるところにより、委託者に対して、部分払を請求することができる。

2 部分払の回数及び時期は、あらかじめ委託者の指定するところによる。

3 受託者は、部分払を請求しようとするときは、あらかじめ、当該請求に係る契約の履行の完了部分の確認を委託者に請求しなければならない。

4 委託者は、前項の規定による確認の請求があったときは、当該請求を受けた日から起算して10日以内に、受託者の立会いの上、設計図書に定めるところにより、当該確認をするための検査を行わなければならない。この場合において、検査に直接必要な費用は、受託者の負担とする。ただし、委託者の故意又は過失により、過分の費用を要した分については、委託者が負担しなければならない。

5 受託者は、契約の履行の内容が前項の規定による検査に合格しないときは、直ちに、必要な措置を執った上、委託者の検査を受けなければならない。この場合においては、必要な措置の完了を契約の履行の全部の完了とみなして前2項の規定を適用する。

6 受託者は、第4項の規定による検査に合格したときは、委託者に部分払を請求することができる。この場合において、委託者は、当該請求があった日から起算して30日以内に部分払金を支払わなければならない。

(部分払金の不払に対する契約の履行の中止)

第33条 受託者は、委託者が前条の規定に基づく支払を遅延し、相当の期間を定めてその支払を請求したにもかかわらず支払をしないときは、契約の履行の全部又は一部の履行を一時中止することができる。この場合においては、受託者は、直ちにその旨を委託者に通知しなければならない。

2 委託者は、前項の規定により受託者が契約の履行を中止した場合において、必要があると認められるときは履行期間若しくは契約代金額を変更し、又は受託者が契約の履行の続行に備え履行場所を維持し若しくは従事者、機械器具等を保持するための費用その他の契約の履行の一時中止に伴う増加費用を必要とし若しくは受託者に損害を及ぼしたときは必要な費用を負担しなければならない。

(契約不適合責任)

第34条 委託者は、契約の履行の目的物が種類、品質又は数

量に関して契約の内容に適合しないもの（以下、「契約不適合」という。）であるときは、受託者に対して当該契約不適合の修補又は代替物の引渡しによる履行の追完を求めることができる。ただし、その履行の追完に過分の費用を要するときは、委託者は、当該履行の追完を求めることができない。

2 前項の場合において、受託者は、委託者に不相当な負担を課するものでないときは、委託者が請求した方法と異なる方法による履行の追完をすることができる。

3 第1項の場合において、委託者が相当の期間を定めて履行の追完の催告をし、その期間内に履行の追完がないときは、委託者は、その不適合の程度に応じて代金の減額を請求することができる。ただし、次の各号のいずれかに該当する場合は、催告をすることなく、直ちに代金の減額を請求することができる。

- (1) 履行の追完が不能であるとき。
- (2) 受託者が履行の追完を拒絶する意思を明確に表示したとき。
- (3) 契約の履行の目的物の性質又は当事者の意思表示により、特定の日時又は一定の期間内に履行しなければ契約をした目的を達することができない場合において、受託者が履行の追完をしないでその時期を経過したとき。
- (4) 前3号に掲げる場合のほか、委託者がこの項の規定による催告をしても履行の追完を受ける見込みがないことが明らかであるとき。

(委託者の催告による解除権)

第35条 委託者は、受託者が次の各号のいずれかに該当するときは、相当の期間を定めてその履行の催告をし、その期間内に履行がないときは、この契約を解除することができる。ただし、その期間を経過したときにおける債務の不履行がこの契約及び取引上の社会通念に照らして軽微であるときは、この限りではない。

- (1) 正当な理由なく、契約の履行に着手すべき期日を過ぎても着手しないとき。
- (2) 履行期間内に契約の履行の全部を完了しないとき又は履行期間経過後相当の期間内に契約の履行の全部を完了する見込みが明らかでないとき認められるとき。
- (3) 第9条に規定する現場責任者を設置しなかったとき。
- (4) 正当な理由なく、第34条第1項の履行の追完がなされないとき又は同条第3項に規定する代金の減額がなされないとき。
- (5) 前各号に掲げる場合のほか、この契約に違反したとき。

(委託者の催告によらない解除権)

第36条 委託者は、受託者が次の各号のいずれかに該当するときは、直ちにこの契約の解除をすることができる。

- (1) 第4条の規定に違反し、この契約により生ずる権利又は義務を第三者に譲渡し、若しくは継承させ、又はその権利を担保に供したとき。
- (2) この契約の履行の全部を完了させることができないこと

が明らかであるとき。

- (3) 受託者がこの契約の履行の全部の完了を拒絶する意思を明確に表示したとき。
- (4) 受託者の債務の一部の履行が不能である場合又は受託者がその債務の一部の履行を拒絶する意思を明確に表示した場合において、残存する部分のみでは契約をした目的を達することができないとき。
- (5) 契約の目的物の性質や当事者の意思表示により、特定の日時又は一定の期間内に履行しなければ契約をした目的を達することができない場合において、受託者が履行をしないでその時期を経過したとき。
- (6) 前各号に掲げる場合のほか、受託者がその債務の履行をせず、委託者が前条の催告をしても契約をした目的を達するのに足りる履行がされる見込みがないことが明らかであるとき。
- (7) 契約の履行に当たって法令の規定により必要な許可又は認可等を失ったとき。
- (8) 経営状態が悪化し、又はそのおそれがあると認められる相当の理由があるとき。
- (9) 第39条又は第40条の規定によらないで契約の解除を申し出たとき。
- (10) 受託者が第44条の2第1項各号のいずれかに該当したとき。

第36条の2 委託者は、神奈川県警察本部長からの通知又は回答により、受託者が次の各号のいずれかに該当するときは、この契約を解除することができる。

- (1) 横浜市暴力団排除条例（平成23年12月横浜市条例第51号。以下、本条において、「条例」という。）第2条第2号に規定する暴力団（以下、「暴力団」という。）、条例第2条第4号に規定する暴力団員等（以下、「暴力団員等」という。）、条例第2条第5号に規定する暴力団経営支配法人等又は条例第7条に規定する暴力団員等と密接な関係を有すると認められる者であるとき。
  - (2) 神奈川県暴力団排除条例（平成22年神奈川県条例第75号）第23条第1項又は第2項に違反している事実があるとき。
  - (3) 受託者が、この契約に関して、下請負契約又は資材、原材料の購入契約その他の契約にあたり、その相手方が第1号又は第2号のいずれかに該当することを知りながら、当該者と契約を締結したと認められるとき。
  - (4) 受託者が、この契約に関して、第1号又は第2号のいずれかに該当する者を下請負契約又は資材、原材料の購入契約その他の契約の相手方としていた場合（第3号に該当する場合を除く。）に、委託者が受託者に対して当該契約の解除を求め、受託者がこれに従わなかったとき。
  - (5) 受託者が、この契約に関して、第1号又は第2号のいずれかに該当する者に契約代金債権を譲渡したとき。
- 2 受託者が共同企業体の場合にあつては、前項の規定は

その構成員が同項各号のいずれかに該当した場合に適用する。

3 第1項の規定により、委託者が契約を解除した場合においては、受託者は、契約代金額の10分の1に相当する額を違約金として委託者の指定する期間内に支払わなければならない。ただし、地方自治法第234条の3に基づく長期継続契約においては、この条における契約代金額を、契約代金の総額と読み替える。

4 前項の場合において、受託者が共同企業体であるときは、構成員は、連帯して委託者に支払わなければならない。

(委託者の責めに帰すべき事由による場合の解除の制限)

第37条 第35条又は第36条各号に定める場合が委託者の責めに帰すべき事由によるものであるときは、委託者は、前2条の規定による解除をすることができない。

(委託者の任意解除権)

第38条 委託者は、契約の履行が完了しない間は、第35条、第36条及び第36条の2に規定する場合のほか、必要があるときは、この契約を解除することができる。

(受託者の催告による解除権)

第39条 受託者は、委託者がこの契約に違反したときは、相当の期間を定めてその履行の催告をし、その期間内に履行がないときは、この契約を解除することができる。ただし、その期間を経過したときにおける債務の不履行がこの契約及び取引上の社会通念に照らして軽微であるときは、この限りではない。

(受託者の催告によらない解除権)

第40条 受託者は、次の各号のいずれかに該当するときは、直ちにこの契約を解除することができる。

(1) 第15条の規定により設計図書を変更したため契約代金額が3分の2以上増減(消費税等率の変動に伴う金額の増減は含まない。)したとき。

(2) 第17条の規定によるこの契約の履行の中止が履行期間の10分の5(履行期間の10分の5が6月を超えるときは、6月)を超えたとき。ただし、中止が契約の履行の一部のみの場合は、その一部を除いた他の部分の契約の履行が完了した後3月を経過しても、なおその中止が解除されないとき。

(3) 委託者がこの契約に違反し、その違反によってこの契約の履行が不可能となったとき。

2 受託者は、前項の規定によりこの契約を解除した場合において、損害があるときは、その損害の賠償を委託者に請求することができる。

(受託者の責めに帰すべき事由による場合の解除の制限)

第41条 第39条又は第40条各号に定める場合が受託者の責めに帰すべき事由によるものであるときは、受託者は、前2条の規定による解除をすることができない。

(合意解除)

第42条 委託者は、必要があると認めるときは、第35条から

前条までの規定にかかわらず、契約の相手方と協議して、契約の全部又は一部を解除することができる。

(解除に伴う措置)

第43条 委託者は、第35条、第36条、第36条の2、第39条、第40条又は第42条の規定によりこの契約が解除された場合においては、契約の履行の完了部分を検査の上、当該検査に合格した部分に相応する契約代金を受託者に支払わなければならない。この場合において、検査に直接要する費用は、受託者の負担とする。

2 前項の場合において、第31条の規定による前金払があったときは、当該前払金の額(第32条の規定による部分払をしているときは、その部分払において償却した前払金の額を控除した額)を前項の契約の履行の完了部分に相応する契約代金額から控除する。この場合において、受託者は、支払済みの前払金になお余剰があるときは、次の各号に定めるところにより、その余剰金を委託者に返還しなければならない。

(1) 解除が第35条、第36条又は第36条の2の規定に基づくとき。

当該余剰金に、前払金の支払の日から返還の日までの日数に応じ、契約日における、政府契約の支払遅延防止等に関する法律(昭和24年法律第256号)第8条第1項の規定に基づき財務大臣が決定する率を乗じて計算した額(計算して求めた額の全額が100円未満であるときは全額を、100円未満の端数があるときはその端数を切り捨てるものとする。)の利息を付した額

(2) 解除が第38条、第39条、第40条又は第42条の規定に基づくとき。

3 受託者は、この契約が解除になった場合において、支給材料があるときは、第1項の契約の履行の完了部分の検査に合格した部分に使用されているものを除き、委託者に返還しなければならない。この場合において、当該支給材料が受託者の故意又は過失により滅失し、若しくははき損したとき、その返還が不可能となったとき、又は契約の履行の完了部分の検査に合格しなかった部分に使用されているときは、代品を納め、若しくは原状に復して返還し、又は返還に代えてその損害を賠償しなければならない。

4 受託者は、この契約が解除になった場合において、貸与品があるときは、当該貸与品を委託者に返還しなければならない。この場合において、当該貸与品が受託者の故意又は過失により滅失し、若しくははき損したとき、又はその返還が不可能となったときは、代品を納め、若しくは原状に復して返還し、又は返還に代えてその損害を賠償しなければ



ばならない。

5 受託者は、この契約が解除になった場合において、履行場所に受託者が所有し、又は管理する材料、機械器具その他の物件（下請負人が所有し、又は管理するこれらの物件及び前2項の材料又は貸与品のうち委託者に返還しないものを含む。）があるときは、受託者は、当該物件を撤去するとともに、当該履行場所を修復し、取り片付けて、委託者に明け渡さなければならない。

6 前項の場合において、受託者が正当な理由なく、相当の期間内に当該物件を撤去せず、又は履行場所等の修復若しくは取片付けを行わないときは、委託者は、受託者に代わって当該物件を処分し、履行場所等の修復若しくは取片付けを行うことができる。この場合においては、受託者は、委託者の処分又は修復若しくは取片付けについて異議を申し出ることができず、また、委託者の処分又は修復若しくは取片付けに要した費用を負担しなければならない。

7 第3項前段又は第4項前段の規定により受託者が支給材料又は貸与品を返還する場合の期限、方法等については、次の各号に定めるところによる。

(1) 解除が第35条、第36条又は第36条の2の規定に基づくとき。

(2) 解除が第38条、第39条、第40条又は第42条の規定に基づくとき。

8 第3項後段、第4項後段及び第5項の規定により受託者が執るべき措置の期限、方法等については、委託者が受託者の意見を聴いて定めるものとする。

(委託者の損害賠償請求等)

第44条 委託者は、受託者が次の各号のいずれかに該当する場合は、これによって生じた損害の賠償を請求することができる。

(1) 受託者の責めに帰すべき理由により履行期間内に契約の履行の全部を完了することができないとき

(2) この契約の履行の目的物に契約不適合があるとき

(3) 第35条又は第36条の規定により、この契約が解除されたとき。

(4) 前各号に掲げる場合のほか、債務の本旨に従った履行をしないとき又は債務の履行が不能であるとき。

2 前項第1号の損害金の額は、契約代金額に、遅延日数に応じ、この契約の締結時における国の債権の管理等に關する法律施行令（昭和31年政令第337号）第29条第1項に規定する財務大臣が定める率（年当たりの割合は、間（じゅん）年の日を含む期間についても、365日の割合とする。）で計算した額を乗じて計算した額（計算して求めた額の全額が100円未満であるときは全額を、100円未満の端数があるときはその端数を切り捨てるものとする。）とする。こ

の場合において、委託者が認めた履行済部分に相応する契約代金額は控除するものとする。ただし、全部の履行がなされなければ契約の目的が達せられないときは、この限りでない。なお、遅延日数は、委託者の責めに帰すべき理由による日数を控除したものとする。また、地方自治法（昭和22年法律第67号）第234条の3に基づく長期継続契約においては、この条における契約代金額を、履行期間の始期から履行期間の満了までの契約代金の総額（以下「契約代金の総額」という。）と読み替える。

3 次の各号のいずれかに該当する場合においては、受託者は、第1項の損害賠償に代えて、契約代金額の10分の1に相当する額を違約金として委託者の指定する期間内に支払わなければならない。ただし、地方自治法第234条の3に基づく長期継続契約においては、この条における契約代金額を、契約代金の総額と読み替える。

(1) 第35条又は第36条の規定により契約の履行の全部の完了前に契約が解除された場合

(2) 契約の履行の全部の完了前に、受託者がその債務の履行を拒否し、又は、受託者の責めに帰すべき事由によって受託者の債務について履行不能となった場合

4 次の各号に掲げる者がこの契約を解除した場合は、前項第2号に該当する場合とみなす。

(1) 受託者について破産法（平成16年法律第75号）の規定による破産手続開始の決定があった場合において、同法の規定により選任された破産管財人

(2) 受託者について会社更生法（平成14年法律第154号）の規定による更生手続開始の決定があった場合において、同法の規定により選任された管財人

(3) 受託者について民事再生法（平成11年法律第225号）の規定による再生手続開始の決定があった場合において、同法の規定により選任された再生債務者等

5 第1項及び第3項各号に定める場合（第4項の規定により同項各号が第3項第2号に該当する場合とみなされる場合を除く。）がこの契約及び取引上の社会通念に照らして受託者の責めに帰することができない事由によるものであるときは、第1項及び第3項各号の規定は適用しない。

(談合等不正行為に対する措置)

第44条の2 受託者は、この契約に関して、次の各号のいずれかに該当するときは、該当した時点における契約代金額の10分の2に相当する額を損害賠償金として委託者の指定する期間内に支払わなければならない。ただし、地方自治法第234条の3に基づく長期継続契約においては、この条における契約代金額を、契約代金の総額と読み替える。

(1) 受託者又は受託者を構成事業者とする私的独占の禁止及び公正取引の確保に関する法律（昭和22年法律第54号。以下「独占禁止法」という。）第2条第2項の事業者団体（以下「受託者等」という。）が、この契約について独占禁止法第3条又は第8条第1号の規定に違反したとして、受託者等に対する独占禁止法第7条若しくは第8条の2の規

定に基づく排除措置命令（以下「排除措置命令」という。）又は独占禁止法第7条の2第1項（独占禁止法第8条の3において準用する場合を含む。）の規定に基づく課徴金の納付命令（以下「納付命令」という。）が確定したとき（確定した納付命令が独占禁止法第63条第2項の規定により取り消されたときを含む。）。

- (2) 前号に掲げるもののほか、確定した排除措置命令又は納付命令（独占禁止法第63条第2項の規定により取り消されたものを含む。次号において同じ。）により、受託者等が、この契約について独占禁止法第3条又は第8条第1号の規定に違反する行為があったとされたとき。
- (3) 確定した排除措置命令又は納付命令により、受託者等に独占禁止法第3条又は第8条第1号の規定に違反する行為があったとされた期間及び当該行為の対象となった取引分野が示された場合（この契約が示された場合を除く。）において、当該期間にこの契約の入札（見積書の提出を含む。）が行われたものであり、かつ、この契約が当該取引分野に該当するものであるとき。
- (4) 受託者（法人にあっては、その役員又は使用人を含む。）の刑法（明治40年法律第45号）第96条の6又は独占禁止法第89条第1項若しくは第95条第1項第1号に規定する刑が確定したとき。

2 前項の規定は、この契約による業務が完了した後においても同様とする。

3 第1項に規定する場合において、受託者が共同企業体であり、既に解散しているときは、委託者は、受託者の代表者であった者又は構成員であった者に賠償金を請求することができる。この場合において、受託者の代表者であった者及び構成員であった者は、連帯して当該賠償金を支払わなければならない。

（受託者の損害賠償請求等）

第45条 受託者は、委託者が次の各号のいずれかに該当する場合は、これによって生じた損害の賠償を請求することができる。ただし、当該各号に定める場合がこの契約及び取引上の社会通念に照らして委託者の責めに帰することができない事由によるものであるときは、この限りでない。

(1) 第38条、第39条又は第40条の規定によりこの契約が解除されたとき。

(2) 前号に掲げる場合のほか、債務の本旨に従った履行をしないとき又は債務の履行が不能であるとき。

2 委託者の責めに帰すべき理由により、第29条又は第32条の規定による契約代金の支払が遅れた場合においては、受託者は、未受領金額につき、遅延日数に応じ、契約日における、政府契約の支払遅延防止等に関する法律（昭和24年法律第256号）第8条第1項の規定に基づき財務大臣が決定する率を乗じて計算した額（計算して求めた額の全額が100円未満であるときは全額を、100円未満の端数があるときはその端数を切り捨てるものとする。）の遅延利息の支払を委託者に請求することができる。

（契約不適合責任期間）

第46条 受託者が契約の履行の目的物に関して契約の内容に適合しない目的物を委託者に引き渡した場合において、委託者がその不適合を知った時から1年以内にその旨を受託者に通知しないときは、委託者は、その不適合を理由として、履行の追完の請求、代金の減額の請求、損害賠償の請求又は契約の解除をすることができない。ただし、受託者が引渡しの際にその不適合を知り、又は重大な過失によって知らなかったときは、この限りでない。

2 前項の規定にかかわらず、委託者の権利の行使ができる期間について仕様書等で別段の定めをした場合は、その仕様書等の定めるところによる。

3 前2項の請求等は、具体的な契約不適合の内容、請求する損害額の算定の根拠等、当該請求等の根拠を示して、委託者の契約不適合責任を問う意思を明確に告げることで行う。

4 委託者が第1項又は第2項に規定する契約不適合に係る請求等が可能期間（以下、この項「契約不適合期間」という。）の内に契約不適合を知り、その旨を受託者に通知した場合において、委託者が通知から1年が経過する日までに前項に規定する請求等をしたときは、契約不適合期間の内に請求等をしたものとみなす。

5 委託者は、第1項又は第2項の請求等を行ったときは、当該請求等の根拠となる契約不適合に関し、民法の消滅時効の範囲で、当該請求等以外に必要と認められる請求等を行うことができる。

6 前各項の規定は、契約不適合が受託者の故意又は重過失により生じたものであるときには適用せず、契約不適合に関する受託者の責任については、民法の定めるところによる。

7 第1項の規定は、契約の履行の目的物の契約不適合が支給材料の性質又は委託者の指示により生じたものであるときは、委託者は契約不適合を理由として、請求等を行うことができない。ただし、受託者がその材料又は指示が不相当であることを知りながらこれを通知しなかったときは、この限りでない。

（暴力団等からの不当介入の排除）

第47条 受託者は、契約の履行に当たって、暴力団又は暴力団員等からの不当介入を受けた場合は、遅滞なく委託者に報告するとともに所轄の警察署に通報し、捜査上の必要な協力をしなければならない。

2 受託者は、前項の不当介入を受けたことにより、履行期間に遅れが生じるおそれがある場合は、委託者と履行期間に関する協議を行わなければならない。その結果、履行期間に遅れが生じると認められたときは、第18条の規定により、委託者に履行期間延長の請求を行うものとする。

3 受託者は、契約の履行に当たって、暴力団又は暴力団員等からの不当介入による被害を受けた場合には、その旨を直ちに委託者に報告するとともに、被害届を速やかに所轄

の警察署に提出しなければならない。

- 4 受託者は、前項の被害により履行期間に遅れが生じるおそれがある場合は、委託者と履行期間に関する協議を行わなければならない。その結果、履行期間に遅れが生じると認められたときは、第18条の規定により、委託者に履行期間延長の請求を行うものとする。

(相殺)

第48条 委託者は、この契約に基づいて委託者が負う債務をこの契約又は他の契約に基づいて受託者が負う債務と相殺することができる。

(概算契約)

第49条 この契約書に概算契約である旨の記載がある契約（以下この条において「概算契約」という。）にあつては、設計図書記載の数量及び契約書記載の契約代金額は概算であり、増減することがある。この場合にあつては、本市が支払う金額は、履行期間内の実際の履行数量に契約書又は内訳書に記載した単価を乗じた金額に消費税及び地方消費税相当額を加算した額とする。

- 2 概算契約においては、第44条中「契約代金額」は「履行期間内の実際の履行数量に契約書又は内訳書に記載した単価を乗じた金額に消費税及び地方消費税相当額を加算した額」と読み替える。

(補則)

第50条 この約款に定めのない事項については、横浜市契約規則（昭和39年3月横浜市規則第59号）（水道事業管理者の権限に属する契約にあつては「横浜市水道局契約規程（平成20年3月水道局規程第7号）第2条の規定により読み替えて準用する横浜市契約規則」と、交通事業管理者の権限に属する契約にあつては「横浜市交通局契約規程（平成20年3月交通局規程第11号）第2条の規定により読み替えて準用する横浜市契約規則」と読み替えるものとする。）の定めるところによるほか、必要に応じて、委託者と受託者とが協議して定める。

(情報を取り扱う際の基本的事項)

第1条 この特記事項(以下「特記事項」という。)は、委託契約約款(以下「約款」という。)の特記条項として、電子計算機処理等の委託契約に関する横浜市(以下「委託者」という。)が保有する情報の取扱いについて、必要な事項を定めるものである。

2 情報を電子計算機処理等により取り扱う者(以下「受託者」という。)は、情報の保護の重要性を認識し、この契約による業務(以下「本件業務」という。)を遂行するための情報の取扱いに当たっては、委託者の業務に支障が生じることのないよう、適正に取り扱わなければならない。

(定義)

第2条 特記事項において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 電子計算機処理等 電子計算機を使用して行われる情報の入力、蓄積、編集、加工、修正、更新、検索、消去、出力又はこれらに類する処理をいう。ただし、専ら文章を作成するための処理、専ら文書図画の内容を記録するための処理、製販その他の専ら印刷物を制作するための処理及び専ら文書図画の内容の伝達を電気通信の方法により行うための処理を除く。

(2) 不開示情報 横浜市の保有する情報の公開に関する条例(平成12年条例第1号)第7条第2項に規定する不開示情報をいう。

(3) 不開示資料等 不開示情報が記録された、文書、図画、写真、フィルム及び電磁的記録をいう。

(適正な管理)

第3条 受託者は、本件業務に係る情報の漏えい、滅失、毀損及び改ざん等(以下「漏えい等」という。)の防止その他の情報の適正な管理のために必要な措置を講じなければならない。

2 受託者は、情報の取扱いに関する規程類を整備するとともに、情報の適正な管理を実施する者として本件業務に係る情報の管理責任者を選任しなければならない。

3 受託者は、電子計算機を設置する場所、情報を保管する場所その他の情報を取り扱う場所(以下「作業場所」という。)を定めるとともに、作業場所に係る入退室の規制、防災・防犯対策その他の安全対策を講じなければならない。

4 受託者は、本件業務に着手する前に前3項に定める管理責任体制及び安全対策その他の安全管理措置について、委託者に報告しなければならない。

5 受託者は、前項の規定により報告した事項に関し、委託者が理由を示して異議を申し出た場合には、当該異議に関する事項を変更しなければならない。この場合において、当該変更を経費を要するときは、その費用負担は委託者と受託者とが協議して決定する。

(従事者の監督)

第4条 受託者は、本件業務に従事している者が、本件業務に関して知り得た不開示情報をみだりに他人に知らせ、又は不当な目的に使用しないよう、必要かつ適切な監督を行わなければならない。この契約が終了し、又は解除された後においても同様とする。

(収集の制限)

第5条 受託者は、本件業務を遂行するために必要な範囲内で、適正かつ公正な手段により情報を収集しなければならない。

(禁止事項)

第6条 受託者は、あらかじめ委託者の指示又は承諾があった場合を除き、本件業務に係る情報に関し、次に掲げる行為をしてはならない。

(1) 本件業務を処理する目的以外での利用

(2) 複写又は複製(作業場所内において効率的に作業を進めるためにやむを得ないものを除く)

(3) 作業場所の外への持ち出し

(再委託の禁止等)

第7条 受託者は、本件業務を遂行するための不開示情報を自ら取り扱うものとし、第三者に取り扱わせてはならない。ただし、あらかじめ、委託者の書面による承諾を得た場合は、この限りでない。

2 受託者は、前項ただし書の承諾を得て、本件業務に係る情報を第三者に取り扱わせる場合には、情報の保護に関し、特記事項と同等の内容及び委託者が指示する事項について、当該第三者(会社法(平成17年法律第86号)第2条第1項第3号の子会社を含む。以下「再受託者」という。)との間で約定しなければならない。2以上の段階にわたる委託(以下「再々委託等」という。)を行う場合も、この例によるべきことを再受託者又はこれに類する者に求めなければならない。

3 再受託者が本件業務に係る情報を第三者に取り扱わせる場合にあっては、受託者は、当該第三者(会社法第2条第1項第3号の子会社を含む。)における情報の取扱いに係る管理体制をあらかじめ確認し、当該確認内容を委託者に報告し、委託者の書面による承諾を受けた上でなければ、第1項ただし書の承諾に相当する承諾をしてはならない。再々委託等を行う場合も、同様とする。

4 業務内容が定型的であり、かつ、情報の漏えい等の危険性が低いものとして委託者が別に定める業務の委託(再委託及び再々委託等(以下「再委託等」と総称する。))を含む。)については、委託者が別に定める事項をあらかじめ

め委託者に報告した場合には、第1項ただし書の承諾及び前項に規定する受託者による承諾を要しない。

5 第3条第5項の規定は、前項に規定する報告について準用する。

(不開示資料等の返還等)

第8条 受託者は、本件業務を遂行するために委託者から貸与され、又は受託者が収集し、複製し、若しくは作成した不開示資料等を、業務の遂行上使用しないこととなったとき又はこの契約が終了したとき若しくは解除されたときは、委託者の指示に従い、直ちに委託者に返還し、若しくは引き渡し、若しくは消去し、又はその他の方法により処理(以下「返還等」という。)するものとする。

2 前項の場合において、委託者が当該不開示資料等の消去又はその他の方法による処理を指示した場合は、復元困難な消去、焼却、シュレッダー等による裁断等当該情報が第三者の利用に供されることのない方法によらなければならない。

3 第1項の場合において、受託者が正当な理由なく指定された期限内に不開示資料等の返還等をしないときは、委託者は、受託者に代わって当該不開示資料等を回収し、又は廃棄することができる。この場合において、受託者は、委託者の回収又は廃棄について異議を申し出ることができず、委託者の回収又は廃棄に要した費用を負担しなければならない。

(報告及び検査)

第9条 委託者は、情報を保護するために必要な限度において、委託契約期間中、受託者に対して、情報の管理の状況及び委託業務の履行状況について、報告を求めることができる。

2 委託者は、委託契約期間中必要と認めた場合は、情報の管理の状況及び委託業務の履行状況について、作業場所において検査することができる。

3 前2項の場合において、報告又は検査に直接必要な費用は、受託者の負担とする。ただし、委託者の事情により、過分の費用を要した分については、委託者が負担する。

(事故発生時等における報告)

第10条 受託者は、委託者の提供した情報並びに受託者及び再受託者が本件業務のために収集した情報について、火災その他の災害、盗難、漏えい、改ざん、破壊、コンピュータウイルスによる被害、不正な利用、不正アクセス等の事故が生じたとき、又は生ずるおそれがあることを知ったときは、速やかに委託者に報告し、委託者の指示に従うものとする。この契約が終了し、又は解除された後においても同様とする。

(引渡し)

第11条 受託者は、約款第28条第2項の規定による検査(以下「検査」という。)に合格したときは、直ちに、契約の履行の目的物を納品書を添えて委託者の指定する場所に納入するものとし、納入が完了した時をもって契約の履行の目的物の引渡しを完了したものとする。

(契約の解除及び損害の賠償)

第12条 委託者は、次のいずれかに該当するときは、この契約を解除し、又は受託者に対して損害賠償を請求することができる。

(1) 本件業務を遂行するために受託者が取り扱う不開示情報について、受託者の責に帰すべき理由による漏えい等があったとき。

(2) 前号に掲げる場合のほか、特記事項に違反し、本件業務の目的を達成することができないと認められるとき。

2 前項第1号の不開示情報の漏えい等に伴う損害賠償その他の一切の責任は、不開示情報の漏えい等が、受託者が再委託等をし、当該再委託等先において発生した場合であっても、当該受託者が負うものとする。

3 委託者は、受託者が検査に不合格となったときは、この契約を解除することができる。

(著作権等の取扱い)

第13条 この契約により作成される成果物の著作権等の取扱いについては、約款第5条の規定にかかわらず、次の各号に定めるところによる。

(1) 受託者は、著作権法(昭和45年法律第48号)第21条(複製権)、第26条の3(貸与権)、第27条(翻訳権、翻案権等)及び第28条(二次的著作物の利用に関する原著者の権利)に規定する権利を、目的物の引渡し時に委託者に無償で譲渡するものとする。

(2) 委託者は、著作権法第20条(同一性保持権)第2項第3号又は第4号に該当しない場合においても、その使用のために、この契約により作成される目的物を改変し、任意の著作者名で任意に公表できるものとする。

(3) 受託者は、委託者の書面による事前の同意を得なければ、著作権法第18条(公表権)及び第19条(氏名表示権)を行使することができないものとする。

(4) 受託者がこの契約の締結前から権利を有している著作物の著作権は、受託者に留保されるものとする。この場合において、受託者は、委託者に対し、当該著作物について、委託者が契約の履行の目的物を使用するために必要な範囲で、著作権法に基づく利用を無償で許諾するものとする。

2 前項の規定にかかわらず、著作物の利用について設計図書で別段の定めをした場合には、その図書の定めに従うものとする。

3 受託者は、この契約によるすべての成果物が、第三者の著作権、特許権その他の権利を侵害していないことを保証するものとする。ただし、委託者の責に帰すべき事由に起因する権利侵害となる場合は、この限りではない。

(最近改正：令和5年4月1日)

## 個人情報取扱特記事項

(令和5年4月)

(個人情報を取り扱う際の基本的事項)

第1条 横浜市（以下「委託者」という。）がこの特記事項が付帯する契約（以下「この契約」という。）において個人情報を取り扱わせる者（以下「受託者」という。）は、個人情報の重要性を認識し、この契約による事務（以下「本件事務」という。）を処理するに当たっては、個人情報の保護に関する法律、横浜市個人情報の保護に関する条例その他の関係法令等を遵守し、個人の権利利益を侵害することのないよう、個人情報を適正に取り扱わなければならない。

(適正な管理)

第2条 受託者は、本件事務に係る個人情報の漏えい、滅失、毀損及び改ざん等（以下「漏えい等」という。）の防止その他の個人情報の適正な管理のために必要な措置を講じなければならない。

- 2 受託者は、個人情報の取扱いに関する規程類を整備するとともに、本件事務に係る個人情報の管理責任者を選任しなければならない。
- 3 受託者は、個人情報を取り扱う場所及び保管する場所（以下「作業場所」という。）を定めるとともに、作業場所に係る入退室の規制、防災・防犯対策その他の安全対策を講じなければならない。
- 4 受託者は、本件事務に係る個人情報の取扱いに着手する前に前3項に定める管理責任体制、安全対策その他の安全管理措置について、安全管理措置報告書（第1号様式）により委託者に報告しなければならない。
- 5 受託者は、前項の規定により報告した事項に関し、委託者が理由を示して異議を申し出た場合には、当該異議に関する事項を変更しなければならない。この場合において、当該変更を経費を要するときは、その費用負担は委託者と受託者とが協議して決定する。

(従事者の監督)

第3条 受託者は、本件事務の処理に従事している者が本件事務に関して知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用しないよう必要かつ適切な監督を行わなければならない。この契約が終了し、又は解除された後においても同様とする。

(収集の制限)

第4条 受託者は、本件事務を処理するために必要な範囲内で、適正かつ公正な手段により個人情報を収集しなければならない。

(禁止事項)

第5条 受託者は、あらかじめ委託者の指示又は承諾があった場合を除き、本件事務に係る個人情報に関し、次に掲げる行為をしてはならない。

- (1) 本件事務を処理する目的以外での利用
- (2) 複写又は複製（作業場所内において効率的に作業を進めるためにやむを得ないものを

除く。)

(3) 作業場所の外への持ち出し

(再委託の禁止等)

第6条 受託者は、本件事務を処理するための個人情報を自ら取り扱うものとし、第三者に取り扱わせてはならない。ただし、あらかじめ、委託者の書面による承諾を得た場合はこの限りでない。

2 受託者は、前項ただし書の承諾を得て、本件事務に係る個人情報を第三者に取り扱わせる場合には、個人情報の保護に関し、本特記事項と同等の内容及び委託者が指示する事項について、当該第三者（会社法（平成17年法律第86号）第2条第1項第3号の子会社を含む。以下「再受託者」という。）との間で約定しなければならない。2以上の段階にわたる委託（以下「再々委託等」という。）を行う場合も、この例によるべきことを再受託者又はこれに類する者に求めなければならない。

3 再受託者が本件事務に係る個人情報を第三者に取り扱わせる場合にあっては、受託者は、当該第三者（会社法第2条第1項第3号の子会社を含む。以下「再々受託者」という。）における個人情報の取扱いに係る管理体制をあらかじめ確認し、当該確認内容を委託者に報告し、委託者の書面による承諾を受けた上でなければ、第1項ただし書の承諾に相当する承諾をしてはならない。再々委託等を行う場合も、同様とする。

4 業務内容が定型的であり、かつ、個人情報の漏えい等の危険性が低いものとして委託者が別に定める業務の委託（再委託及び再々委託等（以下「再委託等」と総称する。）を含む。）については、委託者が別に定める事項をあらかじめ委託者に報告した場合には、第1項ただし書の承諾及び前項に規定する受託者による承諾を要しない。

5 第2条第5項の規定は、前項に規定する報告について準用する。

(個人情報記録された資料等の返還等)

第7条 受託者は、本件事務を処理するために委託者から貸与され、又は受託者が収集し、複製し、若しくは作成した個人情報が記録された資料等を、業務の遂行上使用しないこととなったとき又はこの契約が終了したとき若しくは解除されたときは、委託者の指示に従い、直ちに委託者に返還し、若しくは引き渡し、若しくは消去し、又はその他の方法により処理するものとする。

(報告及び検査)

第8条 委託者は、個人情報を保護するために必要な限度において、委託契約期間中、受託者に対し、個人情報の管理状況及び委託業務の履行状況について報告を求めることができる。

2 委託者は、個人情報を保護するために必要な限度において、委託契約期間中少なくとも1年に一度、情報の管理の状況及び委託業務の履行状況について、原則として作業場所において検査するものとする。

3 前2項の場合において、報告、資料の提出又は検査に直接必要な費用は、受託者の負担とする。ただし、委託者の事情により過分の費用を要した分については、委託者が負担する。

(事故発生時等における報告)

第9条 受託者は、個人情報の漏えい等の事故が生じ、又は生ずるおそれがあることを知ったときは、速やかに委託者に報告し、委託者の指示に従うものとする。この契約が終了し、又は解除された後においても同様とする。

(研修実施報告書の提出)

第10条 受託者は、従事者に対し、個人情報を取り扱う場合に従事者が遵守すべき事項、個人情報の保護に関する法令等に基づく罰則の内容及び個人情報の漏えい等が生じた際に負う民事上の責任についての研修を実施し、研修実施報告書(第2号様式)を委託者に提出しなければならない。

2 受託者は、個人情報を取り扱う事務を再受託者に委託する場合には、再受託者に対し、前項の研修を実施させ、同項の研修実施報告書を受託者に提出させなければならない。

3 前項の場合において、受託者は、再受託者から提出された研修実施報告書を委託者に提出しなければならない。

(契約の解除及び損害の賠償)

第11条 委託者は、次のいずれかに該当するときは、この契約を解除し、又は受託者に対して損害賠償の請求をすることができる。

(1) 本件事務を処理するために受託者が取り扱う個人情報について、受託者の責に帰すべき理由による個人情報の漏えい等があったとき。

(2) 前号に掲げる場合のほか、この特記事項に違反し、本件事務の目的を達成することができないと認められるとき。

2 前項第1号の個人情報の漏えい等に伴う損害賠償その他の一切の責任は、個人情報の漏えい等が、受託者が再委託等をし当該再委託等先において発生した場合であっても、当該受託者が負うものとする。

(第1号様式)

### 安全管理措置報告書

調査項目	内容
1 業者名	<input type="checkbox"/> 横浜市競争入札有資格者 <input type="checkbox"/> その他( ) <input type="checkbox"/> 横浜市出資法人(条例第 条)
2 業務の作業担当部署名	
3 業務の現場責任者役職名	
4 業務の個人情報取扱者の人数	
5 個人情報保護関連資格等	<input type="checkbox"/> Pマーク <input type="checkbox"/> ISMS <input type="checkbox"/> その他の資格( ) <input type="checkbox"/> 個人情報関係の損害保険に加入
6 個人情報保護に関する社内規程等	<input type="checkbox"/> 個人情報の使用、保存、廃棄等に関する管理規程 <input type="checkbox"/> 個人情報漏えい・紛失・滅失・盗難等事故時の対応規程・マニュアル等 <input type="checkbox"/> 個人情報保護について従業員との雇用契約や誓約書等に明記 <input type="checkbox"/> その他の規程( ) <input type="checkbox"/> 規程なし
7 個人情報保護に関する研修・教育	<input type="checkbox"/> 個人情報保護に関する研修・教育を実施(年_回/従業員1人につき) <input type="checkbox"/> その他( )
8 個人情報保護に関する点検・検査・監査の方法等	
9 漏えい等の事案の対応規程・マニュアル等の内容	
(1) 対応規程・マニュアル等がある場合	名 称
	内 容
(2) 対応規程・マニュアル等がない場合	(漏えい等の事案が発生した場合にどのような対応を取るのかについて、なるべく具体的に記載してください。)



10 個人情報を取り扱う作業場所の管理体制

※ 作業を実施機関の施設内部のみで行い、かつ、受託者が、実施機関所有のPC、タブレット等の電子計算機のみを使用する場合には記入不要です。作業を実施機関の施設内部のみで行い、かつ、受託者所有の電子計算機を使用する場合には、(2)電磁媒体の項目、(4)及び(5)を記入してください。

<p>(1) 作業施設の入退室管理</p>	<p>作業期間中の入室可能人数  <input type="checkbox"/>上記4の作業者のみ  <input type="checkbox"/>作業員以外への入室可 ( <input type="checkbox"/>上記外___名 <input type="checkbox"/>その他 )</p> <p>入退室者名及び時刻の記録  <input type="checkbox"/>なし (施設のみ、身分証提示のみ等)  <input type="checkbox"/>あり <input type="checkbox"/>用紙記入  <input type="checkbox"/>ICカード等によりID等をシステムに記録  <input type="checkbox"/>カメラや生体認証等により特定個人の入退室時刻を記録  <input type="checkbox"/>その他 ( )  <input type="checkbox"/>その他 ( )</p>				
<p>(2) 個人情報の保管場所</p>	<table border="1"> <tr> <td data-bbox="544 728 683 824"> <p>紙媒体</p> </td> <td data-bbox="683 728 1444 824"> <p><input type="checkbox"/>鍵付き書庫 <input type="checkbox"/>耐火金庫 <input type="checkbox"/>専用の保管室  <input type="checkbox"/>その他 ( )</p> </td> </tr> <tr> <td data-bbox="544 824 683 920"> <p>電磁媒体</p> </td> <td data-bbox="683 824 1444 920"> <p><input type="checkbox"/>鍵付き書庫 <input type="checkbox"/>耐火金庫 <input type="checkbox"/>専用の保管室  <input type="checkbox"/>その他 ( )</p> </td> </tr> </table>	<p>紙媒体</p>	<p><input type="checkbox"/>鍵付き書庫 <input type="checkbox"/>耐火金庫 <input type="checkbox"/>専用の保管室  <input type="checkbox"/>その他 ( )</p>	<p>電磁媒体</p>	<p><input type="checkbox"/>鍵付き書庫 <input type="checkbox"/>耐火金庫 <input type="checkbox"/>専用の保管室  <input type="checkbox"/>その他 ( )</p>
<p>紙媒体</p>	<p><input type="checkbox"/>鍵付き書庫 <input type="checkbox"/>耐火金庫 <input type="checkbox"/>専用の保管室  <input type="checkbox"/>その他 ( )</p>				
<p>電磁媒体</p>	<p><input type="checkbox"/>鍵付き書庫 <input type="checkbox"/>耐火金庫 <input type="checkbox"/>専用の保管室  <input type="checkbox"/>その他 ( )</p>				
<p>(3) 作業施設の防災体制</p>	<p><input type="checkbox"/>常時監視 <input type="checkbox"/>巡回監視 <input type="checkbox"/>耐火構造 <input type="checkbox"/>免震・制震構造  <input type="checkbox"/>その他 ( )</p>				
<p>(4) 個人情報の運搬方法</p>	<table border="1"> <tr> <td data-bbox="544 1016 683 1220"> <p>紙媒体</p> </td> <td data-bbox="683 1016 1444 1220"> </td> </tr> <tr> <td data-bbox="544 1220 683 1429"> <p>電磁媒体</p> </td> <td data-bbox="683 1220 1444 1429"> </td> </tr> </table>	<p>紙媒体</p>		<p>電磁媒体</p>	
<p>紙媒体</p>					
<p>電磁媒体</p>					
<p>(5) 個人情報の廃棄方法</p>	<table border="1"> <tr> <td data-bbox="544 1429 683 1632"> <p>紙媒体</p> </td> <td data-bbox="683 1429 1444 1632"> </td> </tr> <tr> <td data-bbox="544 1632 683 1841"> <p>電磁媒体</p> </td> <td data-bbox="683 1632 1444 1841"> </td> </tr> </table>	<p>紙媒体</p>		<p>電磁媒体</p>	
<p>紙媒体</p>					
<p>電磁媒体</p>					
<p>(6) 施設外で作業を行う場合の個人情報保護対策 (行う場合のみ記入)</p>					

11 電算処理における個人情報保護対策 ※紙媒体しか取り扱わない業務を行う場合は記入不要です。 ※実施機関所有のPC、タブレット等の電子計算機のみを使用する場合には記入不要です。	
(1) 作業を行う機器	<input type="checkbox"/> 限定している（ノート型__台、デスクトップ型__台） <input type="checkbox"/> 限定していない
(2) 外部との接続	<input type="checkbox"/> 作業機器は外部との接続をしていない <input type="checkbox"/> 作業機器は外部と接続している 接続方法： <input type="checkbox"/> インターネット <input type="checkbox"/> 専用回線 <input type="checkbox"/> その他（ ） 通信の暗号化： <input type="checkbox"/> している <input type="checkbox"/> していない
(3) アクセス制限	<input type="checkbox"/> ID・パスワード付与によりアクセス制限をしている IDの設定方法（ ） パスワードの付け方（ ） <input type="checkbox"/> ID・パスワード付与によりアクセス制限をしていない
(4) 不正アクセスを検知するシステムの有無	<input type="checkbox"/> あり（検知システムの概要： ） <input type="checkbox"/> なし
(5) マルウェアを検知するシステムの有無	<input type="checkbox"/> あり（検知システムの概要： ） <input type="checkbox"/> なし
(6) ソフトウェアの更新	<input type="checkbox"/> 常に最新のものに自動アップデートするものとなっている <input type="checkbox"/> 上記以外（ ）
(7) アクセスログ	<input type="checkbox"/> アクセスログをとっている（ 年保存） <input type="checkbox"/> アクセスログをとっていない
(8) 停電時のデータ消去防止対策	<input type="checkbox"/> 無停電電源装置 <input type="checkbox"/> 電源の二重化 <input type="checkbox"/> その他（ ） <input type="checkbox"/> なし
(9) その他の対策	
12 外国における個人情報の取扱いの有無  ※ 実施機関所有のPC、タブレット等の電子計算機のみを使用する場合には記入不要です。	<input type="checkbox"/> あり <input type="checkbox"/> 外国のサーバ上に個人情報が保存されているが、外国のサーバ上での個人情報の取扱いはない <input type="checkbox"/> 外国のサーバ上に個人情報が保存されており、外国のサーバ上で個人情報を取り扱っている <input type="checkbox"/> なし ※「あり」の場合は、以下も記入してください。
(1) 個人情報の取扱いがある外国の名称	
(2) 当該外国における個人情報の制度・保護措置等	

年 月 日

(提出先)

---

(提出者)

団体名

責任者職氏名

## 研修実施報告書・誓約書

個人情報保護に関する法律第66条第2項の規定により準用される同条第1項に定める措置の一環として、横浜市の個人情報を取り扱う事務に従事する者に対し、個人情報を取り扱う場合に遵守すべき事項並びに個人情報保護に関する法令等に基づく罰則の内容及び漏えい等の事故が発生した場合の民事上の責任についての研修を実施しましたので、別紙(全枚)のとおり報告いたします。

個人情報保護に関する法令等及び個人情報取扱特記事項を遵守し、並びに従事者にも遵守させ、個人情報を適切に取り扱うことを誓約いたします。



## ●横浜市情報セキュリティ管理規程

令和5年3月24日  
達第1号  
庁中一般

横浜市情報セキュリティ管理規程を次のように定める。

横浜市情報セキュリティ管理規程

横浜市情報セキュリティ管理規程（平成17年3月達第2号）の全部を改正する。

### （目的）

第1条 この規程は、横浜市の保有する情報資産の取扱いに関し措置すべき事項を定めることにより、当該情報資産に対して機密性、完全性及び可用性の維持を図ること並びに当該情報資産の適正な運用による行政の信頼性の確保を図ることを目的とする。

### （基本理念）

第2条 本市は、保有する情報資産が、市民の安全と福祉の向上に資することを目的として市民から管理を負託されたものであることを基本認識とし、この市民の信頼に応えられるよう全力を挙げて適正に保護及び管理することを基本理念とする。

### （定義）

第3条 この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- (1) 区局 横浜市事務分掌条例（昭和26年10月横浜市条例第44号）第1条に掲げる統括本部及び局並びに横浜市消防本部及び消防署の設置等に関する条例（昭和38年10月横浜市条例第34号）第2条第2項に規定する消防局、横浜市会計室規則（平成19年3月横浜市規則第36号）第1条に規定する会計室、横浜市区役所事務分掌条例（平成28年2月横浜市条例第2号）第1条に規定する区役所をいう。
- (2) 情報システム ある目的を達成するためのハードウェア、ソフトウェア、ネットワーク等により構築する電子計算機処理の環境をいう。
- (3) 行政文書 横浜市行政文書管理規則（平成12年3月横浜市規則第25号）第2条第1項に規定する行政文書をいう。
- (4) システム関連文書 情報システムの開発及び運用に用いる行政文書をいう。
- (5) データ 情報システムで扱う電磁的記録（電子的方式、磁気的方式その他の他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）をいう。
- (6) 記録媒体 データを記録した磁気ディスク、磁気テープその他の媒体をいう。
- (7) 個人情報 個人情報の保護に関する法律（平成15年法律第57号）第2条第1項に規定する個人情報をいう。
- (8) 特定個人情報 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第2条第8項に規定する特定個人情報をいう。
- (9) 情報資産 区局が保有し、又は外部委託する情報システム、システム関連文書、情報システム利用時の認証に関する情報、データ及び記録媒体並びに個人情報及び特定個人情報を含む行政文書を

いう。

- (10) 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。
- (11) 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。
- (12) 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。
- (13) 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。
- (14) 情報セキュリティ対策 情報セキュリティの実現を目的として実施する対策をいう。
- (15) 職員 地方公務員法（昭和 25 年法律第 261 号）第 3 条に規定する一般職及び特別職の職員のうち、情報資産を使用する職員をいう。
- (16) 課等 横浜市事務分掌条例第 2 条の規定により設置された部、室、課及び係をいう。
- (17) 横浜市情報セキュリティポリシー 横浜市情報セキュリティ強化方針、横浜市サイバーセキュリティ強化方針、横浜市情報セキュリティ管理規程、横浜市情報セキュリティ管理要綱及び横浜市情報セキュリティ対策共通実施手順からなる、情報セキュリティに関する規程類の総称をいう。
- (18) 情報セキュリティ事故 情報資産の盗難、漏えい、改ざん、破壊等の機密性、完全性及び可用性が脅かされる事象をいう。

（対象とする脅威）

第 4 条 情報資産に対する脅威として、次に掲げる脅威を想定した、情報セキュリティ対策を実施する。

- (1) 不正アクセス、ウイルス攻撃及びサービス不能攻撃等のサイバー攻撃並びに部外者の侵入、内部不正等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的的要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害による情報資産の損壊・滅失並びにサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等、インフラの障害からの波及等

（職員の責務）

第 5 条 職員は、第 2 条に定める基本理念及び情報セキュリティの重要性について認識し、情報資産を適切に取り扱わなければならない。

2 職員は、情報資産の取扱いに当たっては、次に掲げる法令等を遵守しなければならない。

- (1) 著作権法（昭和 45 年法律第 48 号）
- (2) 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
- (3) 個人情報の保護に関する法律
- (4) 行政手続における特定の個人を識別するための番号の利用等に関する法律
- (5) サイバーセキュリティ基本法（平成 26 年法律第 104 号）
- (6) 横浜市個人情報の保護に関する条例（令和 4 年 12 月横浜市条例第 38 号）

- (7) 横浜市行政手続における特定の個人を識別するための番号の利用等に関する法律の施行に関する条例（平成 27 年 9 月横浜市条例第 52 号）

（組織体制）

- 第 6 条 第 4 条の脅威から情報資産を保護するため、次のとおり情報セキュリティ総括管理者、情報セキュリティ運用管理者、区局情報セキュリティ総括責任者、区局情報セキュリティ運用責任者、情報セキュリティ担当者及び情報資産管理者を置き、情報セキュリティ対策を推進する全庁的な組織体制を確立する。
- 2 情報セキュリティ総括管理者は、横浜市最高情報統括責任者等設置規則（平成 27 年 3 月横浜市規則第 36 号）第 5 条に規定する最高情報セキュリティ責任者（以下「CISO」という。）をもって充て、情報セキュリティ運用管理者及び区局情報セキュリティ総括責任者を総括し、これらの者に対し情報セキュリティに関する事項について指示及び指導を行い、CISO が設置する横浜市情報セキュリティ委員会において決定した事項について、区局の情報セキュリティ対策を決定する。
  - 3 情報セキュリティ運用管理者は、デジタル統括本部長をもって充て、情報セキュリティ総括管理者を補佐するとともに、職員への情報セキュリティ対策実施の徹底を図るため、区局情報セキュリティ総括責任者に対し情報セキュリティ対策に係る指示及び指導を行う。
  - 4 区局情報セキュリティ総括責任者は、当該区局の長をもって充て、区局情報セキュリティ運用責任者及び情報セキュリティ担当者を総括し、これらの者に対し情報セキュリティに関する事項について指示及び指導を行う。
  - 5 区局情報セキュリティ運用責任者は、当該区局の総務担当課長をもって充て、区局情報セキュリティ総括責任者を補佐するとともに、当該区局の職員への情報セキュリティ対策の実施の徹底を図るため、情報セキュリティ担当者に対し情報セキュリティ対策に係る指示及び指導を行う。
  - 6 情報セキュリティ担当者は、当該区局の課等の長をもって充て、取り扱う情報資産の情報資産管理者と密に連携して、課等内の情報セキュリティ対策を実施するとともに、情報資産を利用する課等の職員に対して指導及び監督を行う。
  - 7 情報資産管理者は、別に定める情報資産の分類に応じた情報資産を主管する課等の長又は担当課長をもって充て、当該情報資産を利用する職員が所属する課等の情報セキュリティ担当者と密に連携して、当該情報資産の適正な維持管理を実施するとともに、当該情報資産を利用する職員に対して指導及び監督を行う。

（情報セキュリティ対策）

第 7 条 情報セキュリティ運用管理者は、以下の各号に掲げる情報セキュリティ対策を実施する。

- (1) 情報資産の機密性、完全性及び可用性に応じた分類並びに当該分類に基づく管理
- (2) 情報システム全体の強靱性向上
- (3) 物理的・人的・技術的における情報セキュリティ対策
- (4) 横浜市情報セキュリティポリシーの運用
- (5) 情報セキュリティ事故発生時の対応
- (6) 業務委託及び外部サービス利用時における情報セキュリティの確保

(情報セキュリティ監査及び自己点検の実施)

第8条 情報セキュリティ総括管理者は、前条の情報セキュリティ対策の実施状況を年1回及び必要に応じ監査及び自己点検し、問題がある場合には、速やかに是正しなければならない。

2 情報セキュリティ運用管理者は、区局の情報セキュリティ対策の実施状況を必要に応じ監査及び自己点検し、問題がある場合には、是正を命じることができる。

3 前2項に規定する監査は、客観性を確保するために、外部の専門的知識・見識を有する者の協力を得て実施することができる。

(横浜市情報セキュリティポリシーの見直し)

第9条 情報セキュリティ総括管理者は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、横浜市情報セキュリティポリシーを年1回及び必要に応じ見直ししなければならない。

(例外措置)

第10条 情報セキュリティ担当者は、この規程を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、情報セキュリティ総括管理者と協議の上、例外措置をとることができる。

2 情報セキュリティ担当者は、行政事務の遂行に緊急を要する等の場合であって、前項に定める例外措置をとることが不可避の時は、事後速やかに情報セキュリティ総括管理者に報告しなければならない。

(施行細則)

第11条 この規程に定めるもののほか、この規程の施行に関し必要な事項は、情報セキュリティ運用管理者が定める。

附 則

この達は、令和5年4月1日から施行する。



地方公共団体における  
情報セキュリティポリシーに関する  
ガイドライン(令和4年3月版)

平成13年 3月30日 策定  
令和4年 3月25日 改定

総務省

(目次)

第1編 総則.....	i - 5
第1章 本ガイドラインの目的等.....	i - 9
1. 本ガイドラインの目的.....	i - 9
2. 本ガイドラインの経緯.....	i - 10
第2章 地方公共団体における情報セキュリティとその対策.....	i - 15
1. 地方公共団体における情報セキュリティの考え方.....	i - 15
2. 情報セキュリティポリシーの必要性と構成.....	i - 15
3. 情報セキュリティ対策の実施サイクル.....	i - 17
第3章 情報セキュリティの管理プロセス.....	i - 20
1. 策定及び導入.....	i - 20
2. 運用.....	i - 23
3. 評価・見直し.....	i - 23
第4章 本ガイドラインの構成と対策レベルの設定.....	i - 27
1. 本ガイドラインの構成.....	i - 27
2. 本ガイドラインにおける対策レベルの設定.....	i - 27
第2編 地方公共団体における情報セキュリティポリシー（例文）	ii - 1
第1章 情報セキュリティ基本方針（例文）.....	ii - 5
1. 目的.....	ii - 5
2. 定義.....	ii - 5
3. 対象とする脅威.....	ii - 6
4. 適用範囲.....	ii - 6
5. 職員等の遵守義務.....	ii - 6
6. 情報セキュリティ対策.....	ii - 6
7. 情報セキュリティ監査及び自己点検の実施.....	ii - 8
8. 情報セキュリティポリシーの見直し.....	ii - 8
9. 情報セキュリティ対策基準の策定.....	ii - 8
10. 情報セキュリティ実施手順の策定.....	ii - 8
第2章 情報セキュリティ対策基準（例文）.....	ii - 12
1. 組織体制.....	ii - 12
2. 情報資産の分類と管理.....	ii - 16
3. 情報システム全体の強靱性の向上.....	ii - 19
4. 物理的セキュリティ.....	ii - 21
5. 人的セキュリティ.....	ii - 25
6. 技術的セキュリティ.....	ii - 29
7. 運用.....	ii - 43

8. 業務委託と外部サービスの利用.....	ii - 46
9. 評価・見直し.....	ii - 50
<b>第3編 地方公共団体における情報セキュリティポリシー（解説）</b>	<b>iii - 1</b>
<b>第1章 情報セキュリティ基本方針（解説）</b>	<b>iii - 5</b>
1. 目的.....	iii - 5
2. 定義.....	iii - 5
3. 対象とする脅威.....	iii - 6
4. 適用範囲.....	iii - 7
5. 職員等の遵守義務.....	iii - 10
6. 情報セキュリティ対策.....	iii - 10
7. 情報セキュリティ監査及び自己点検の実施.....	iii - 12
8. 情報セキュリティポリシーの見直し.....	iii - 12
9. 情報セキュリティ対策基準の策定.....	iii - 12
10. 情報セキュリティ実施手順の策定.....	iii - 13
11. 宣言書の形式.....	iii - 13
<b>第2章 情報セキュリティ対策基準（解説）</b>	<b>iii - 18</b>
1. 組織体制.....	iii - 18
2. 情報資産の分類と管理.....	iii - 28
3. 情報システム全体の強靱性の向上.....	iii - 33
4. 物理的セキュリティ.....	iii - 49
5. 人的セキュリティ.....	iii - 52
6. 技術的セキュリティ.....	iii - 76
7. 運用.....	iii - 120
8. 業務委託と外部サービスの利用.....	iii - 132
9. 評価・見直し.....	iii - 155
10. 用語の定義.....	iii - 163
<b>第4編 付録</b> .....	<b>iv - 1</b>
付録1 権限・責任等一覧表.....	iv - 5

はじめに

「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下「本ガイドライン」という。）では、以下の構成としている。

第1編は、総則として、本ガイドラインの目的や構成について、第2編で、情報セキュリティポリシーの例文を示している。そして、第3編で、情報セキュリティポリシーの考え方及び内容について、第2編の例文と対応する形で解説する形式としている。また、関連する参考資料を第4編として付けている。

「情報セキュリティポリシー」は、「情報セキュリティ基本方針」と「情報セキュリティ対策基準」から構成されており、「情報セキュリティ基本方針」は情報セキュリティ対策における基本的な考え方を定めており、「情報セキュリティ対策基準」は、「情報セキュリティ基本方針」に基づき、情報システムに必要となる情報セキュリティ対策の基準を定めている。

本ガイドラインを参考として、各地方公共団体においては、必要に応じて内容を取込み、情報セキュリティ強化により一層ご尽力いただくことを願うものである。

# 第1編

## 総則

(目次)

第1編 総則.....	i -5
第1章 本ガイドラインの目的等.....	i -9
1. 本ガイドラインの目的.....	i -9
2. 本ガイドラインの経緯.....	i -10
第2章 地方公共団体における情報セキュリティとその対策.....	i -15
1. 地方公共団体における情報セキュリティの考え方.....	i -15
2. 情報セキュリティポリシーの必要性和構成.....	i -15
3. 情報セキュリティ対策の実施サイクル.....	i -17
第3章 情報セキュリティの管理プロセス.....	i -20
1. 策定及び導入.....	i -20
2. 運用.....	i -23
3. 評価・見直し.....	i -23
第4章 本ガイドラインの構成と対策レベルの設定.....	i -27
1. 本ガイドラインの構成.....	i -27
2. 本ガイドラインにおける対策レベルの設定.....	i -27

## 第1章

### 本ガイドラインの目的等

---

(目次)

第1章 本ガイドラインの目的等 .....	i -9
1. 本ガイドラインの目的 .....	i -9
2. 本ガイドラインの経緯 .....	i -10



## 第1章 本ガイドラインの目的等

### 1. 本ガイドラインの目的

情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。

地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産を守るにあたって自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。

本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したものである。したがって、本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げるものではない。

既に、多くの地方公共団体において、情報セキュリティポリシーが策定されているが、今後は情報セキュリティポリシーの定期的な評価・見直しを行い、情報セキュリティ対策の実効性を確保するとともに、対策レベルを高めていくことが重要である。本ガイドラインは、七次の改定を通じて、新たな情報機器、サービス及び脅威等に対応した情報セキュリティ対策を追加しているので、情報セキュリティポリシーの評価・見直しを行う際にも、本ガイドラインが活用されることが期待される。

本ガイドライン内で記載している例文は、参考としやすくするため基礎的な地方公共団体の中でも最も数の多い市制施行されている地方公共団体を想定して記述している。

なお、本ガイドラインは、読者として情報セキュリティポリシーの策定を行う者、セキュリティ上の職責を担う者などを想定して記述している。

## 2. 本ガイドラインの経緯

総務省では、地方公共団体における情報セキュリティポリシーの策定を推進するため、平成13年3月30日に「地方公共団体における情報セキュリティポリシーに関するガイドライン」を策定した。その後、平成15年3月18日に同ガイドラインを一部改定し、①外部委託に関する管理、②情報セキュリティ監査、③無線LAN等の新たな技術動向等を踏まえた記述等の追加を行った。さらに、平成18年9月29日に全部改定し、①地方公共団体のセキュリティ水準の強化、②「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」（以下「重要インフラ指針」という。）への対応、③分かりやすい表現への変更等を行った。

一方、平成18年2月2日、政府の情報セキュリティ政策会議は、「第1次情報セキュリティ基本計画」を決定し、この中で、地方公共団体に関して、政府は平成18年9月を目処に「地方公共団体における情報セキュリティポリシーに関するガイドライン」の見直しを行うこととされ、見直しに当たっては、重要インフラ指針を踏まえることとされた。

また、平成21年2月3日、政府の情報セキュリティ政策会議は、「第1次情報セキュリティ基本計画」に基づく各種の取組の進展や社会環境の変化などを踏まえ、引き続き我が国全体として情報セキュリティ問題への取組を力強く推進するために、平成21年度以降を念頭に置いた「第2次情報セキュリティ基本計画」を決定し、この中で、地方公共団体に関して、小規模な地方公共団体も含め、全ての地方公共団体において、望ましい情報セキュリティ対策が実施されることを目指し、対策の促進を行うこととされた。

さらに、平成22年5月11日、政府の情報セキュリティ政策会議は、「第2次情報セキュリティ基本計画」に基づく官民の各主体による取組を継続しつつ、新たな環境変化に対応した政府の取組を進めるために、「第2次情報セキュリティ基本計画」を含有する「国民を守る情報セキュリティ戦略」を決定し、平成32年までに、インターネットや情報システム等の情報通信技術を利用者が活用するに当たっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境（高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」を実現することを目標としている。

なお、重要インフラ指針については、平成18年2月2日に政府の情報セキュリティ政策会議によって決定以降、平成19年6月14日、平成22年5月11日及び平成25年2月22日に改定され、「対策編」が平成22年7月30日に策定、平成25年3月30日に改定され、平成27年5月25日に指針本編と「対策編」が改定された。さらに、平成30年4月4日に指針本編の改定と、新たに「手引書」が策定され、令和元年5月23日に指針本編と「手引書」が改定されている。

その他、地方公共団体に関連する法令として、平成25年5月24日に成立し、平成25年5月31日に公布された社会保障・税の分野における給付と負担の公平化や各種

行政事務の効率化のための「行政手続における特定の個人を識別するための番号の利用等に関する法律」や平成 26 年 11 月 6 日に成立し、平成 26 年 11 月 12 日に公布された、サイバーセキュリティに関する施策を総合的かつ効果的に推進することを目的とした「サイバーセキュリティ基本法」がある。

総務省では、これらの新たな対策技術の動向、政府の情報セキュリティ政策の改定及び新たに成立した法令等を踏まえ、平成 27 年 3 月 27 日に一部改定を行った。

平成 27 年度には、自治体情報セキュリティ対策検討チームを構成し、地方公共団体の情報セキュリティに関わる抜本的な対策の検討が実施され、「新たな自治体情報セキュリティ対策の抜本的強化について」（平成 27 年 12 月 25 日総行第 77 号総務大臣通知）にて、地方公共団体におけるセキュリティ対策の抜本的強化への取組が示された。自治体情報セキュリティ対策検討チームの報告、政府機関の情報セキュリティ対策のための統一基準の改定等を踏まえて、平成 30 年 9 月 25 日に一部改定を行った。

令和 2 年 5 月 22 日には、「クラウド・バイ・デフォルト原則」、行政手続のオンライン化、働き方改革、サイバー攻撃の増加といった新たな時代の要請や「三層の対策」の課題を踏まえた「自治体情報セキュリティ対策の見直しについて」がとりまとめられた。同とりまとめ及び平成 30 年 7 月の政府機関の情報セキュリティ対策のための統一基準の改定等を踏まえて、令和 2 年 12 月 28 日に一部改定を行った。

令和 3 年度には、「デジタル庁設置法」、「デジタル社会形成基本法」、「地方公共団体情報システムの標準化に関する法律」等のデジタル改革関連法が成立・施行され、国及び地方のデジタル・トランスフォーメーション（DX）が推し進められることとなった。総務省では、これらの地方公共団体におけるデジタル化の動向や令和 3 年 7 月の政府機関のサイバーセキュリティ対策のための統一基準の改定を踏まえて、今般ガイドラインを改定したものである。

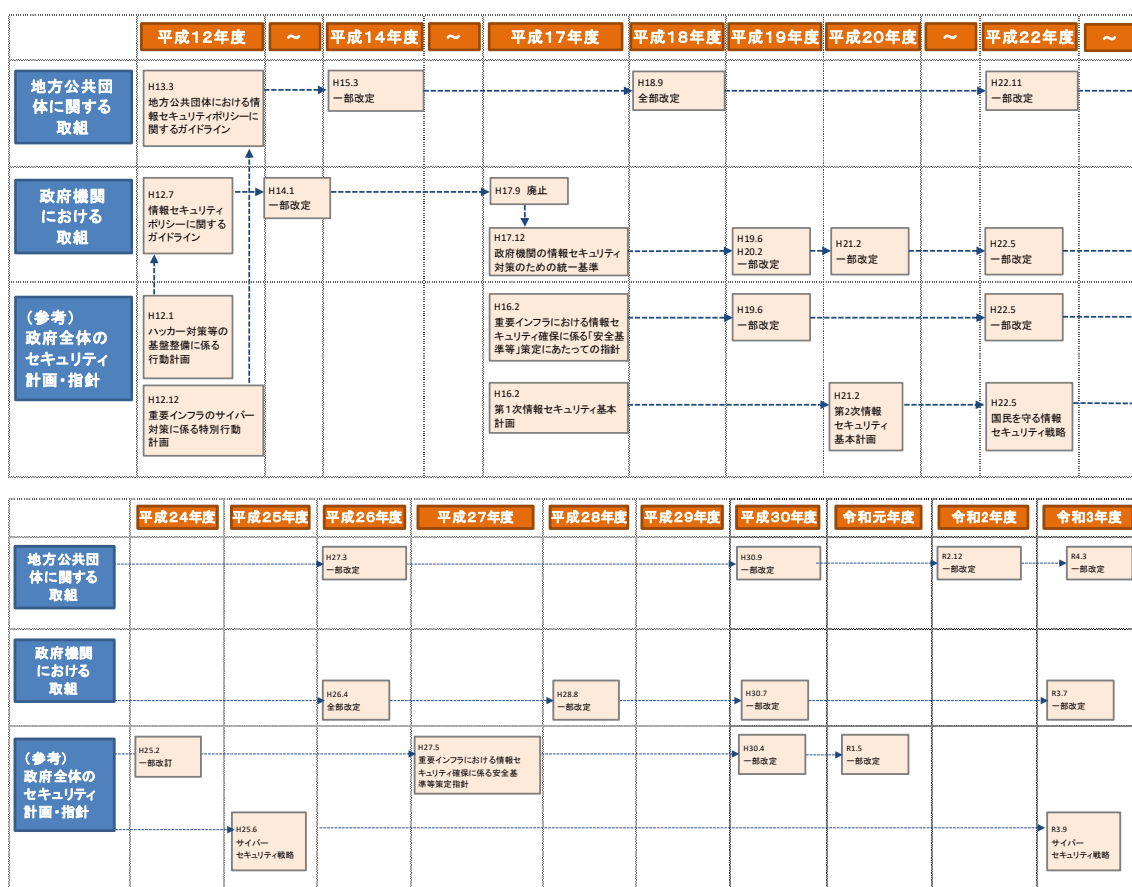
#### 【参考】政府機関の情報セキュリティ対策

政府機関については、平成 12 年 7 月 18 日に情報セキュリティ対策推進会議が「情報セキュリティポリシーに関するガイドライン」を決定し、このガイドラインに基づき、各府省庁が情報セキュリティポリシーを策定することにより、情報セキュリティ対策を実施してきた。

しかし、各府省庁の情報セキュリティ対策の整合化・共通化を促進し、政府機関全体としての情報セキュリティ水準の向上を図るため、平成 17 年 12 月 13 日に情報セキュリティ政策会議が、新たに「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版）」を策定し、各府省は統一基準を踏まえ、情報セキュリティポリシー等の見直しを行い、対策を実施している。

なお、「政府機関の情報セキュリティ対策のための統一基準」は、技術や環境の変化を踏まえ見直しを行うこととされており、平成 19 年 6 月 14 日、情報セキュ

リティ政策会議第 12 回会合、平成 20 年 2 月 4 日、情報セキュリティ政策会議第 16 回会合、平成 21 年 2 月 3 日、情報セキュリティ政策会議第 20 回会合、平成 22 年 5 月 11 日、情報セキュリティ政策会議第 23 回会合及び平成 26 年 5 月 19 日、情報セキュリティ政策会議第 39 回会合、平成 28 年 8 月 31 日、サイバーセキュリティ戦略本部第 9 回会合、平成 30 年 7 月 25 日、サイバーセキュリティ戦略本部第 19 回会合、令和 3 年 7 月 7 日、サイバーセキュリティ戦略本部第 30 回会合において改定版が決定されている。



図表 1 情報セキュリティポリシー等に関する取り組みの推移

## 第2章

# 地方公共団体における情報セキュリティとその対策

(目次)

第2章 地方公共団体における情報セキュリティとその対策 .....	i - 15
1. 地方公共団体における情報セキュリティの考え方 .....	i - 15
2. 情報セキュリティポリシーの必要性和構成 .....	i - 15
3. 情報セキュリティ対策の実施サイクル .....	i - 17

## 第2章 地方公共団体における情報セキュリティとその対策

### 1. 地方公共団体における情報セキュリティの考え方

地方公共団体は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、ほかに代替することができない行政サービスを提供している。また、地方公共団体の業務の多くが情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、地方公共団体は、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。

今後、各種手続のオンライン利用の本格化や情報システムの高度化等、電子自治体が進展することにより、情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。また、地方公共団体は LGWAN 等のネットワークにより相互に接続しており、一部の団体で発生した IT 障害がネットワークを介して他の団体に連鎖的に拡大する可能性は否定できない。

これらの事情から、全ての地方公共団体において、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっている。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下「情報セキュリティインシデント」という。）の未然防止のみならず、情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

なお、情報セキュリティ対策は、個人情報保護対策と内容的に重なる部分も多い。また、自然災害時や大規模・広範囲にわたる疾病における対応という意味では防災対策とも重なる。情報セキュリティを対策する部署とこれらを担当する部署は、相互に連携をとって、それぞれの対策に取り組むことが求められる。

また、地方公共団体は、自らの情報セキュリティを確保するとともに、地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献することが望まれる。例えば、住民等への広報による啓発、IT 講習等による住民等への情報セキュリティに関する研修の実施、業務面で関係する団体に対する情報セキュリティポリシーの策定の働きかけなどの取組を行うことが考えられる。

### 2. 情報セキュリティポリシーの必要性と構成

地方公共団体においては、情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、そのためには組織として意思統一し、明文化された文書として、情報セキュリティポリシーを定めなければならない。

なお、「サイバーセキュリティ基本法」第 5 条では、地方公共団体においてサイバーセキュリティに関する自主的な施策の策定と実施が責務規定として法定化され

た。これにより、情報セキュリティポリシーの未策定団体においては策定が必須となり、策定済み団体においても、適時適正な見直しとそれを遵守することが重要となっている。

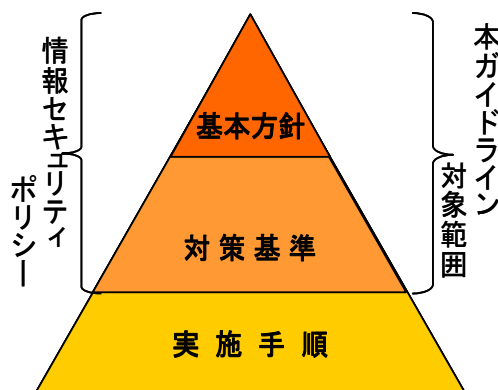
また、番号制度等の最新の制度に係るセキュリティ対策、例えば、情報提供ネットワークシステム等の技術的基準、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」（令和3年8月改正 個人情報保護委員会）が示す安全管理措置等についても遵守しなければならない。

情報セキュリティポリシーの体系は、図表2に示す階層構造となっている。

各地方公共団体の情報セキュリティ対策における基本的な考え方を定めるものが、「基本方針」である。この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。この「対策基準」を、具体的なシステムや手順、手続に展開して個別の実施事項を定めるものが「実施手順」である。

このように、情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、地方公共団体の長をはじめ、全ての職員等及び委託事業者は、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負う。

なお、本ガイドラインの対象とする範囲は「情報セキュリティポリシー」を構成する「基本方針」及び「対策基準」であり、「実施手順」は含まれない。

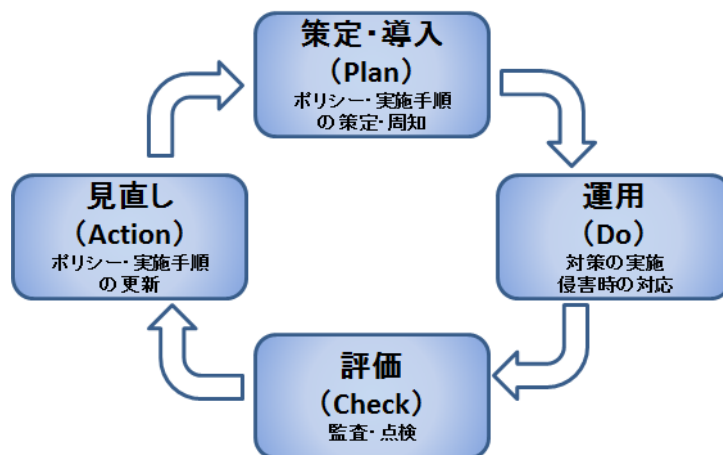


図表2 情報セキュリティポリシーに関する体系図



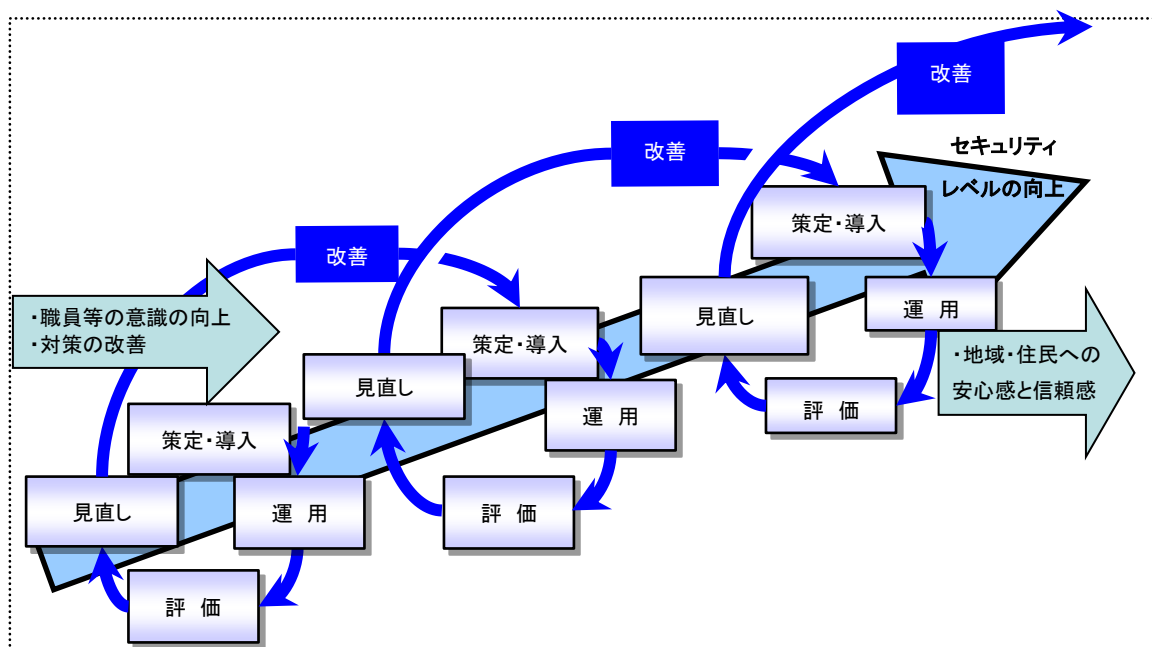
### 3. 情報セキュリティ対策の実施サイクル

情報セキュリティ対策の実施プロセスは、図表3のとおり、策定・導入（Plan）、運用（Do）、評価（Check）、見直し（Action）の4段階に分けることができ、この実施サイクルを繰り返すことによって情報セキュリティは確保される。この実施サイクルは、それぞれの項目の頭文字をとって、PDCA サイクルとも呼ばれる。



図表3 情報セキュリティ対策のPDCA サイクル

情報セキュリティを取り巻く脅威や対策は常に変化しており、以上のPDCA サイクルは、一度限りではなく、図表4のとおり、これを定期的に繰り返すことで、環境の変化に対応しつつ、情報セキュリティ対策の水準の向上を図らなければならない。



図表4 PDCA サイクルの繰り返しによる情報セキュリティ対策の水準の向上

## 第3章

# 情報セキュリティの 管理プロセス

(目次)

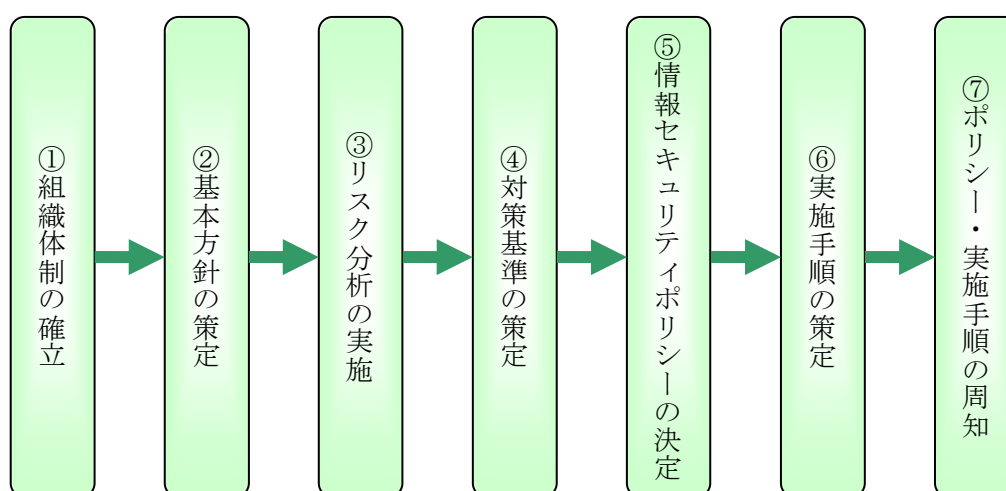
第3章 情報セキュリティの管理プロセス.....	i - 20
1. 策定及び導入.....	i - 20
2. 運用.....	i - 23
3. 評価・見直し.....	i - 23

### 第3章 情報セキュリティの管理プロセス

#### 1. 策定及び導入

##### (1) 策定及び導入の概要

情報セキュリティポリシーの策定及び導入は、図表5のとおり、まず、①策定のための組織体制を確立し、その組織体制の下で、②地方公共団体の基本方針を策定する。次に、③リスク分析を実施し、その結果に基づき、④対策基準の策定を行い、⑤情報セキュリティポリシーを正式に決定する。この後、情報セキュリティポリシーに基づき、⑥実施手順を策定し、⑦ポリシー・実施手順の周知を行うというプロセスになる。



図表5 情報セキュリティポリシーの策定・導入のプロセス

##### (2) 組織体制の確立

###### ① 組織体制の確立

情報セキュリティポリシーの策定には、幹部職員の関与が不可欠である。また、情報セキュリティポリシーは、組織内の様々な部局の情報資産に係る問題を取り扱うことから、責任の所在を明確にするため、全ての部局の長、情報システムを所管する課室長及び情報セキュリティに関する専門的知識を有する者などで構成する組織又はこれに代わる組織（以下、本章において、「情報セキュリティ委員会等」という。）が行う。

（注1）小規模の団体の場合には、新たに組織を立ち上げるのではなく、「情報化推進委員会」等の既存の類似する組織が行う場合もあり得る。

（注2）組織が有機的に機能するために全組織横断的な指示、連絡可能な役割及び権限を明確にすることが望ましい。

###### ② 情報セキュリティポリシー策定チームの編成

情報セキュリティ委員会等は、情報セキュリティポリシーの策定作業の一部を下部の組織（情報セキュリティポリシー策定チーム等）に行わせることができる。

策定チームには、全ての部、課等の関係者が関与することが望ましいが、主たる関係部署に絞って構成する場合もある。（注：情報セキュリティポリシー監査の見直し等については、本ガイドライン「第1編 第3章 3. 評価・見直し」を参照されたい。）

部署	選定の理由
情報政策担当課	庁内業務の情報政策の主管
情報システム担当課	庁内の情報システムの主管
総務担当課	個人情報保護条例の主管
文書担当課	文書管理規程、文書管理システムの主管
防災担当課	災害等の危機管理の主管
施設管理担当課	庁内の施設管理の主管
広報担当課	報道機関への対応の主管

図表6 情報セキュリティポリシー策定チームの編成例

### (3) 情報セキュリティ基本方針の策定

情報セキュリティ基本方針においては、情報セキュリティ対策の目的、体系等、各地方公共団体の情報セキュリティに対する基本的な考え方を示す。

### (4) リスク分析の実施

リスク分析とは、各地方公共団体が保有する情報資産を明らかにし、それらに対するリスクを評価することである。具体的なリスク分析・評価方法については「地方公共団体における情報資産のリスク分析・評価に関する手引き」（平成21年3月総務省）、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（平成28年10月7日 サイバーセキュリティ対策推進会議）及び「高度サイバー攻撃対処のためのリスク評価等のガイドライン 付属書」（平成28年10月7日 内閣官房内閣サイバーセキュリティセンター）を参照されたい。

進め方として、まずは、利用している情報資産に関わらない組織全体としての情報セキュリティ対策の現状に対するリスク分析・評価を行い、次のステップとして図表7にあるような、情報資産に関わる情報セキュリティ対策の現状に対するリスク分析・評価を行う方法もある。

#### 第1ステップ

庁内の情報セキュリティ規程・規則等の策定状況、組織体制の確立状況について、マネジメント体制の観点（組織的対策、人的対策）からリスク分析・評価を行う。

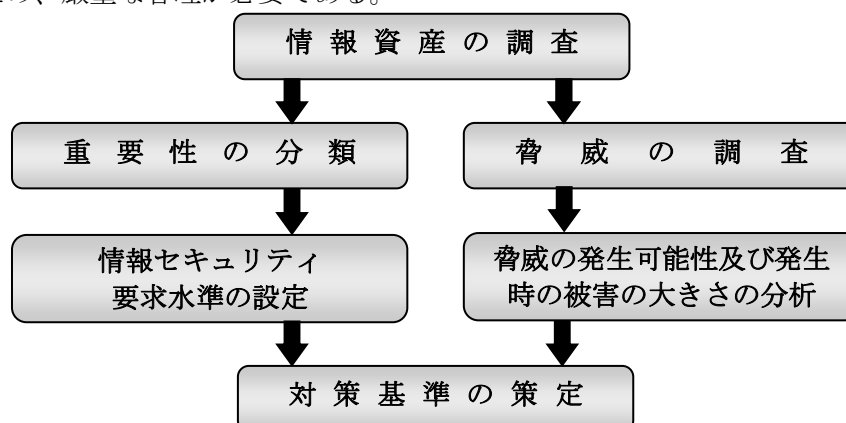
#### 第2ステップ

保有する情報資産における情報セキュリティリスクを分析・評価する。具体的には以下の作業を行う。

- ① 各地方公共団体の保有する情報資産を調査の上、重要性の分類を行い、この結果に基づき、要求されるセキュリティの水準を定める。
- ② 各地方公共団体の情報資産を取り巻く脅威及び脆弱性を調査し、リスクを特定する。リスクの発生可能性及び発生した際の被害の大きさからリスクの大きさを求める。なお、一般的に両者の積をリスクの大きさとしている。
- ③ リスクの大きさがセキュリティ要求水準を下回るよう対策基準を策定し、適正なリスク管理を行う。

なお、スマートデバイス等の新しいモバイル端末、クラウドサービス等の新しい技術の導入や新たな脅威の発生等の情報セキュリティに関する環境変化により、情報資産や情報資産に対するリスクに大きな変化が生じたときには、関係する情報資産についてリスク分析を再度行い、その結果、情報セキュリティポリシーの見直しが必要と判断される場合にはその見直しを行う。また、定期的な情報セキュリティポリシーの評価・見直しの際にもリスク分析から再検討することが必要である。

リスク分析に関する資料は、情報セキュリティポリシー策定の基礎資料として保管する必要があるが、当該資料には情報資産の脆弱性に関する事項が記載されているため、厳重な管理が必要である。



図表7 リスク分析の事例

(5) 情報セキュリティ対策基準の策定

リスク分析の結果得られる情報セキュリティ要求水準に対して、それを実現するための遵守事項や判断基準等を定める情報セキュリティ対策基準を策定する。情報セキュリティ対策基準は、想定される情報リスクに十分に対処し、情報セキュリティ要求水準を満たすものでなければならない。

(6) 情報セキュリティポリシーの決定

情報セキュリティ委員会等が策定した情報セキュリティ基本方針及び情報セキュリティ対策基準について、地方公共団体の長又はこれに準じる者の決裁により、当該地方公共団体における情報セキュリティポリシーとして正式に決定する。

(7) 実施手順の策定

実施手順は、職員等関係者が、各々の扱うネットワーク及び情報システムや携わ

る業務において、どのような手順で情報セキュリティポリシーに記述された内容を実行していくかを定めるマニュアルに該当する。このマニュアルには、主要な情報資産に対するセキュリティ対策実施手順も含まれる。

実施手順は、個別の目的のために作成し、見直し等を柔軟に行っていくため、業務担当課において情報システムや情報資産を管理する者等が策定することが適当である。

#### (8) 情報セキュリティポリシー及び実施手順の周知

情報セキュリティ対策を最終的に実施するのは職員等であるため、実効性を確保するため情報セキュリティポリシーの配布や説明会などにより、情報セキュリティポリシーを職員等に十分に周知する。また、実施手順については、各課部局の責任者が当該手順を実行する者に周知する。

### 2. 運用

情報セキュリティポリシーを確実に運用していくため、情報システムの監視や情報セキュリティポリシーに従って対策が適正に遵守されているか否かを確認し、情報資産に対するセキュリティ侵害や情報セキュリティポリシー違反に対し、適正に対応しなければならない。このため、緊急時対応計画の策定、同計画に基づく訓練、同計画の評価・見直し等を実施する。

### 3. 評価・見直し

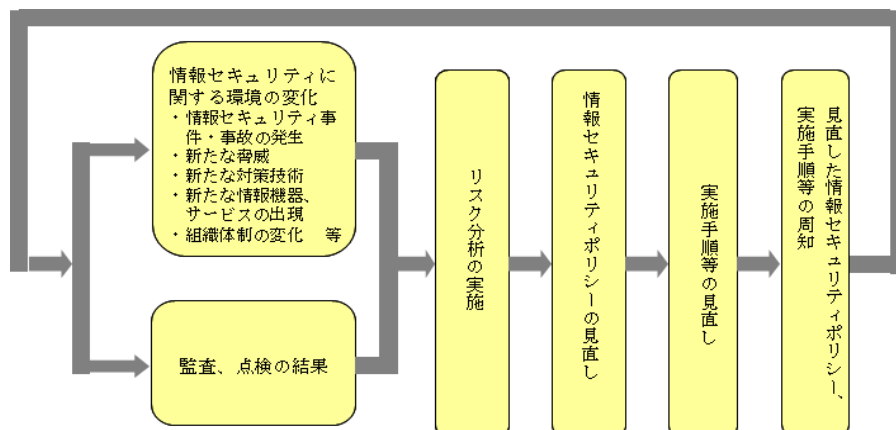
情報セキュリティポリシーの実効性を確保するとともに、情報資産や情報システム等の変化、情報セキュリティに関する脅威や対策等の変化に対応していくためには、情報セキュリティポリシーの評価・見直しを行い、前述の PDCA サイクル（第1編 第2章 3. 情報セキュリティ対策の実施サイクル 図表3 参照）を繰り返すとともに、PDCA サイクルの有効性の確認のために監査・自己点検を活用し、情報セキュリティ対策を不断に強化し続けることが不可欠である。

#### (1) 監査・自己点検

地方公共団体において情報セキュリティ対策の実効性を確保するには、情報セキュリティ対策の実施状況を検証し、情報セキュリティポリシーの見直しに反映させることが必要である。このため、独立かつ専門的知識を有する専門家（部内者であっても監査対象から独立した監査担当者等が行う場合を含む。）による検証である情報セキュリティ監査や情報システム等を運用する者自らによる検証である自己点検を行う。なお、総務省では、本ガイドラインで記述されている内容を踏まえ、監査・点検の手順や監査テーマに応じた監査項目の選定のための「地方公共団体における情報セキュリティ監査に関するガイドライン」（令和4年3月 総務省）を策定しており、同ガイドラインの「第2章 情報セキュリティ監査手順」を参照されたい。

(2) 情報セキュリティポリシーの見直し

情報セキュリティポリシーの見直し作業は、情報セキュリティ委員会等の下で、情報セキュリティポリシーの策定手順（第1編 第3章 1. 策定及び導入 参照）に準じて、図表8のとおり実施する。



図表8 情報セキュリティポリシーの見直しのプロセス



## 第4章

### 本ガイドラインの構成と 対策レベルの設定

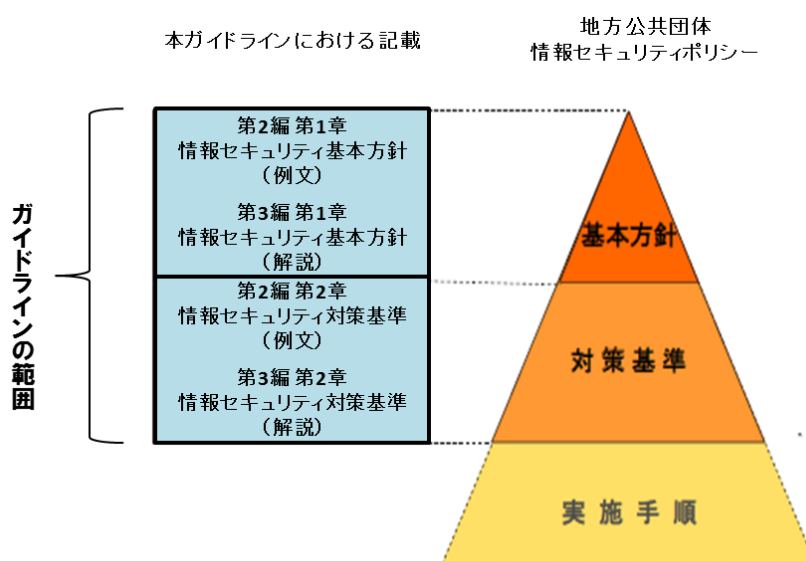
(目次)

第4章 本ガイドラインの構成と対策レベルの設定 .....	i - 27
1. 本ガイドラインの構成 .....	i - 27
2. 本ガイドラインにおける対策レベルの設定.....	i - 27

## 第4章 本ガイドラインの構成と対策レベルの設定

### 1. 本ガイドラインの構成

本ガイドラインの構成は図表 9 のとおり、第 2 編 第 1 章が「情報セキュリティ基本方針」の例文、第 3 編 第 1 章が「情報セキュリティ基本方針」に関する解説、第 2 編 第 2 章が「情報セキュリティ対策基準」の例文、第 3 編 第 2 章が「情報セキュリティ対策基準」に関する解説となっている。



図表 9 本ガイドラインの構成と地方公共団体情報セキュリティポリシーの対応関係

### 2. 本ガイドラインにおける対策レベルの設定

地方公共団体において扱う情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一律でないことから、本ガイドラインでは、特段の理由がない限り対策を講じることが望まれる事項に加え、各地方公共団体において、その事項の必要性の有無を検討し、必要と認められる時に選択して実施することが望ましいと考えられる対策事項については、推奨事項として示している。推奨事項の項目を情報セキュリティポリシーに記載するか否かの判断は地方公共団体の裁量に委ねるが、記載した場合は遵守する必要があることに留意されたい。

各地方公共団体においては、組織の実態に合わせ、必要に応じて推奨事項も含めて、情報セキュリティポリシーを策定することが期待される。

## 第2編

# 地方公共団体における 情報セキュリティポリシー (例文)

第2編 地方公共団体における情報セキュリティポリシー (例文)

(目次)

第2編	地方公共団体における情報セキュリティポリシー（例文）	ii - 1
第1章	情報セキュリティ基本方針（例文）	ii - 5
1.	目的	ii - 5
2.	定義	ii - 5
3.	対象とする脅威	ii - 6
4.	適用範囲	ii - 6
5.	職員等の遵守義務	ii - 6
6.	情報セキュリティ対策	ii - 6
7.	情報セキュリティ監査及び自己点検の実施	ii - 8
8.	情報セキュリティポリシーの見直し	ii - 8
9.	情報セキュリティ対策基準の策定	ii - 8
10.	情報セキュリティ実施手順の策定	ii - 8
第2章	情報セキュリティ対策基準（例文）	ii - 12
1.	組織体制	ii - 12
2.	情報資産の分類と管理	ii - 16
3.	情報システム全体の強靱性の向上	ii - 19
4.	物理的セキュリティ	ii - 21
5.	人的セキュリティ	ii - 25
6.	技術的セキュリティ	ii - 29
7.	運用	ii - 43
8.	業務委託と外部サービスの利用	ii - 46
9.	評価・見直し	ii - 50

## 第1章

# 情報セキュリティ基本方針 (例文)

(目次)

第1章 情報セキュリティ基本方針（例文） .....	ii - 5
1. 目的.....	ii - 5
2. 定義.....	ii - 5
3. 対象とする脅威.....	ii - 6
4. 適用範囲.....	ii - 6
5. 職員等の遵守義務.....	ii - 6
6. 情報セキュリティ対策.....	ii - 6
7. 情報セキュリティ監査及び自己点検の実施.....	ii - 8
8. 情報セキュリティポリシーの見直し.....	ii - 8
9. 情報セキュリティ対策基準の策定.....	ii - 8
10. 情報セキュリティ実施手順の策定.....	ii - 8

## 第1章 情報セキュリティ基本方針（例文）

### 1. 目的

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

### 2. 定義

#### (1) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

#### (2) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

#### (3) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

#### (4) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

#### (5) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

#### (6) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

#### (7) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

#### (8) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

#### (9) LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

#### (10) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

#### (11) 通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安



全が確保された通信だけを許可できるようにすることをいう。

#### (1 2) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

### 3. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

- (1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

### 4. 適用範囲

#### (1) 行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

#### (2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
- ②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- ③情報システムの仕様書及びネットワーク図等のシステム関連文書

### 5. 職員等の遵守義務

職員、非常勤職員及び臨時職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

### 6. 情報セキュリティ対策

上記3の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

#### (1) 組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2) 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3) 情報システム全体の強靱性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(8) 業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

#### (9) 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

### 7. 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

### 8. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

### 9. 情報セキュリティ対策基準の策定

上記6、7及び8に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

### 10. 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

## 第2章

# 情報セキュリティ対策基準 (例文)

## (目次)

第2章 情報セキュリティ対策基準 (例文)	ii - 12
1. 組織体制	ii - 12
2. 情報資産の分類と管理	ii - 16
3. 情報システム全体の強靱性の向上	ii - 19
4. 物理的セキュリティ	ii - 21
4.1. サーバ等の管理	ii - 21
4.2. 管理区域 (情報システム室等) の管理	ii - 22
4.3. 通信回線及び通信回線装置の管理	ii - 23
4.4. 職員等の利用する端末や電磁的記録媒体等の管理	ii - 24
5. 人的セキュリティ	ii - 25
5.1. 職員等の遵守事項	ii - 25
5.2. 研修・訓練	ii - 26
5.3. 情報セキュリティインシデントの報告	ii - 27
5.4. ID 及びパスワード等の管理	ii - 28
6. 技術的セキュリティ	ii - 29
6.1. コンピュータ及びネットワークの管理	ii - 29
6.2. アクセス制御	ii - 35
6.3. システム開発、導入、保守等	ii - 37
6.4. 不正プログラム対策	ii - 39
6.5. 不正アクセス対策	ii - 41
6.6. セキュリティ情報の収集	ii - 42
7. 運用	ii - 43
7.1. 情報システムの監視	ii - 43
7.2. 情報セキュリティポリシーの遵守状況の確認	ii - 43
7.3. 侵害時の対応等	ii - 44
7.4. 例外措置	ii - 44
7.5. 法令遵守	ii - 45
7.6. 懲戒処分等	ii - 45
8. 業務委託と外部サービスの利用	ii - 46
8.1. 外部委託	ii - 46
8.2. 外部サービスの利用 (機密性2以上の情報を取り扱う場合)	ii - 47
8.3. 外部サービスの利用 (機密性2以上の情報を取り扱わない場合)	ii - 50
9. 評価・見直し	ii - 50
9.1. 監査	ii - 50
9.2. 自己点検	ii - 51

9.3. 情報セキュリティポリシー及び関係規程等の見直し . . . . . ii - 52

## 第2章 情報セキュリティ対策基準（例文）

本対策基準は、情報セキュリティ基本方針を実行に移すための、本市における情報資産に関する情報セキュリティ対策の基準を定めたものである。

### 1. 組織体制

(1) 最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

- ①副市長を CISO とする。CISO は、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。
- ②CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。【推奨事項】
- ③CISO は、情報セキュリティインシデントに対処するための体制（CSIRT: Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。
- ④CISO は、CISO を助けて本市における情報セキュリティに関する事務を整理し、CISO の命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副 CISO」という。） 1 人を必要に応じて置く。
- ⑤CISO は、本対策基準に定められた自らの担務を、副 CISO その他の本対策基準に定める責任者に担わせることができる。

(2) 統括情報セキュリティ責任者

- ①情報政策担当部長を CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISO 及び副 CISO を補佐しなければならない。
- ②統括情報セキュリティ責任者は、本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
- ③統括情報セキュリティ責任者は、本市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。
- ④統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。
- ⑤統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO

が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

- ⑥統括情報セキュリティ責任者は、本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。
- ⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。
- ⑧統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。
- ⑨統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

### (3) 情報セキュリティ責任者

- ①内部部局の長、行政委員会事務局の長、消防長及び地方公営企業の局長を情報セキュリティ責任者とする。
- ②情報セキュリティ責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。
- ③情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
- ④情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員、非常勤職員及び臨時職員等（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

### (4) 情報セキュリティ管理者

- ①内部部局の課室長、内部部局の出張所等出先機関の長、行政委員会事務局の課室長、消防本部の課室長及び地方公営企業の課室長を情報セキュリティ管理者とする。
- ②情報セキュリティ管理者は、その所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。
- ③情報セキュリティ管理者は、その所掌する課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及び CISO へ速やかに報告を行い、指示を仰がなければならない。



(5) 情報システム管理者

- ①各情報システムの担当課室長等を当該情報システムに関する情報システム管理者とする。
- ②情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
- ③情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。
- ④情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

(6) 情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

(7) 情報セキュリティ委員会

- ①本市の情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。
- ②情報セキュリティ委員会は、毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。【推奨事項】

(8) 兼務の禁止

- ①情報セキュリティ対策の実施において、止むを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。
- ②情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

(9) CSIRT の設置・役割

- ①CISO は、CSIRT を整備し、その役割を明確化しなければならない。
- ②CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。
- ③CISO は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

- ④CISOによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。
- ⑤情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告しなければならない。
- ⑥情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。
- ⑦情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

## 2. 情報資産の分類と管理

### (1) 情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

#### 機密性による情報資産の分類

分類	分類基準	取扱制限
機密性3	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	<ul style="list-style-type: none"><li>・支給以外の端末での作業の原則禁止（機密性3の情報資産に対して）</li><li>・必要以上の複製及び配付禁止</li></ul>
機密性2	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	<ul style="list-style-type: none"><li>・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止</li><li>・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納</li><li>・復元不可能な処理を施しての廃棄</li><li>・信頼のできるネットワーク回線の選択</li><li>・外部で情報処理を行う際の安全管理措置の規定</li><li>・電磁的記録媒体の施錠可能な場所への保管</li></ul>
機密性1	機密性2又は機密性3の情報資産以外の情報資産	—

### 完全性による情報資産の分類

分類	分類基準	取扱制限
完全性 2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> <li>・バックアップ、電子署名付与</li> <li>・外部で情報処理を行う際の安全管理措置の規定</li> <li>・電磁的記録媒体の施錠可能な場所への保管</li> </ul>
完全性 1	完全性 2 の情報資産以外の情報資産	—

### 可用性による情報資産の分類

分類	分類基準	取扱制限
可用性 2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> <li>・バックアップ、指定する時間以内の復旧</li> <li>・電磁的記録媒体の施錠可能な場所への保管</li> </ul>
可用性 1	可用性 2 の情報資産以外の情報資産	—

## (2) 情報資産の管理

### ①管理責任

- (ア) 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。
- (イ) 情報資産が複製又は伝送された場合には、複製等された情報資産も(1)の分類に基づき管理しなければならない。

### ②情報資産の分類の表示

職員等は、情報資産について、ファイル(ファイル名、ファイルの属性(プロパティ)、ヘッダー・フッター等)、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

### ③情報の作成

- (ア) 職員等は、業務上必要のない情報を作成してはならない。
- (イ) 情報を作成する者は、情報の作成時に(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
- (ウ) 情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

### ④情報資産の入手

- (ア) 庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
- (イ) 庁外の者が作成した情報資産を入手した者は、(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
- (ウ) 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

### ⑤情報資産の利用

- (ア) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
- (イ) 情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。
- (ウ) 情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

### ⑥情報資産の保管

- (ア) 情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。
- (イ) 情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。
- (ウ) 情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。【推奨事項】
- (エ) 情報セキュリティ管理者又は情報システム管理者は、機密性2以上、完全性2又は可用性2の情報を記録した電磁的記録媒体を保管する場合は、耐火、耐熱、耐水及

び耐湿を講じた施設可能な場所に保管しなければならない。

#### ⑦情報の送信

電子メール等により機密性 2 以上の情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

#### ⑧情報資産の運搬

(ア) 車両等により機密性 2 以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

(イ) 機密性 2 以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

#### ⑨情報資産の提供・公表

(ア) 機密性 2 以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

(イ) 機密性 2 以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

(ウ) 情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

#### ⑩情報資産の廃棄等

(ア) 情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

(イ) 情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(ウ) 情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

### 3. 情報システム全体の強靱性の向上

#### (1) マイナンバー利用事務系

##### ①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定 (MAC アドレス、IP アドレス) 及びアプリケーションプロトコル (ポート番号) のレ

ベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

## ②情報のアクセス及び持ち出しにおける対策

### (ア) 情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

### (イ) 情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

## (2) LGWAN 接続系

### ①LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

(ア) インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

(イ) インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

(ウ) 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

## (3) インターネット接続系

①インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

②都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

③(B モデルを採用する場合) 業務の効率性・利便性の向上を目的として、インターネッ

ト接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産を LGWAN 接続系に配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

(B'モデルを採用する場合) 業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

#### 4. 物理的セキュリティ

##### 4.1. サーバ等の管理

###### (1) 機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

###### (2) サーバの冗長化

①情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。【推奨事項】

②情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。【推奨事項】

###### (3) 機器の電源

①情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

###### (4) 通信ケーブル等の配線

①統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等



必要な措置を講じなければならない。

- ②統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。
- ③統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。
- ④統括情報セキュリティ責任者及び情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

#### （5） 機器の定期保守及び修理

- ①情報システム管理者は、可用性 2 のサーバ等の機器の定期保守を実施しなければならない。
- ②情報システム管理者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

#### （6） 庁外への機器の設置

統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

#### （7） 機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

### 4.2. 管理区域（情報システム室等）の管理

#### （1） 管理区域の構造等

- ①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。
- ②統括情報セキュリティ責任者及び情報システム管理者は、管理区域を地階又は 1 階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。【推奨事項】

- ③統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。
- ④統括情報セキュリティ責任者及び情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。
- ⑤統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。【推奨事項】
- ⑥統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

## (2) 管理区域の入退室管理等

- ①情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。
- ②職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。
- ③情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。
- ④情報システム管理者は、機密性2以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

## (3) 機器等の搬入出

- ①情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託事業者を確認を行わせなければならない。
- ②情報システム管理者は、情報システム室の機器等の搬入出について、職員を立ち合わせなければならない。

### 4.3. 通信回線及び通信回線装置の管理

- ①統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

- ②統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。
- ③統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。
- ④統括情報セキュリティ責任者は、機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。
- ⑤統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。
- ⑥統括情報セキュリティ責任者は、可用性2の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

#### 4.4. 職員等の利用する端末や電磁的記録媒体等の管理

- ①情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
- ②情報システム管理者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力が必要とするように設定しなければならない。
- ③情報システム管理者は、端末の電源起動時のパスワード（BIOSパスワード、ハードディスクパスワード等）を併用しなければならない。【推奨事項】
- ④情報システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。
- ⑤情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。【推奨事項】
- ⑥情報システム管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。【推奨事項】

## 5. 人的セキュリティ

### 5.1. 職員等の遵守事項

#### (1) 職員等の遵守事項

##### ①情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

##### ②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

##### ③モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限 (ア) CISO は、機密性 2 以上、可用性 2、完全性 2 の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

(イ) 職員等は、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

(ウ) 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

##### ④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ア) 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断を CISO が行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得て利用することができる。

(イ) 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

##### ⑤持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

##### ⑥パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

##### ⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記

録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

#### ⑧退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

### (2) 非常勤及び臨時職員等への対応

#### ①情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び臨時職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

#### ②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び臨時職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

#### ③インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び臨時職員等にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

### (3) 情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

### (4) 委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

## 5.2. 研修・訓練

### (1) 情報セキュリティに関する研修・訓練

CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

### (2) 研修計画の策定及び実施

①CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。

- ②研修計画において、職員等は毎年度最低1回は情報セキュリティ研修を受講できるようにしなければならない。【推奨事項】
- ③新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。
- ④研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものに行なければならない。
- ⑤情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、統括情報セキュリティ責任者及び情報セキュリティ責任者に対して、報告しなければならない。
- ⑥統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、CISOに情報セキュリティ対策に関する研修の実施状況について報告しなければならない。
- ⑦CISOは、毎年度1回、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

(3) 緊急時対応訓練

CISOは、緊急時対応を想定した訓練を定期的に行う必要がある。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

(4) 研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

### 5.3. 情報セキュリティインシデントの報告

(1) 庁内での情報セキュリティインシデントの報告

- ①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口へ報告しなければならない。
- ②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
- ③情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、CISO及び情報セキュリティ責任者に報告しなければならない。

(2) 住民等外部からの情報セキュリティインシデントの報告

- ①職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

- ②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
- ③情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じて CISO 及び情報セキュリティ責任者に報告しなければならない。
- ④CISO は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。【推奨事項】

(3) 情報セキュリティインシデント原因の究明・記録、再発防止等

- ①CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。
- ②CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速やかに報告しなければならない。
- ③CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。
- ④CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。
- ⑤CISO は、CSIRT から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

#### 5.4. ID 及びパスワード等の管理

(1) IC カード等の取扱い

- ①職員等は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。
  - (ア) 認証に用いる IC カード等を、職員等間で共有してはならない。
  - (イ) 業務上必要のないときは、IC カード等をカードリーダー又はパソコン等の端末のスロット等から抜いておかななければならない。
  - (ウ) IC カード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。
- ②統括情報セキュリティ責任者及び情報システム管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。
- ③統括情報セキュリティ責任者及び情報システム管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄

しなければならない。

(2) IDの取扱い

職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

- ①自己が利用しているIDは、他人に利用させてはならない。
- ②共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

(3) パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

- ①パスワードは、他者に知られないように管理しなければならない。
- ②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
- ③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
- ④パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
- ⑤複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
- ⑥仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
- ⑦サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。
- ⑧職員等間でパスワードを共有してはならない（ただし、共用IDに対するパスワードは除く）。

## 6. 技術的セキュリティ

### 6.1. コンピュータ及びネットワークの管理

(1) 文書サーバの設定等

- ①情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。
- ②情報システム管理者は、文書サーバを課室等の単位で構成し、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。
- ③情報システム管理者は、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

(2) バックアップの実施

統括情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ等に記録



された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

(3) 他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

(4) システム管理記録及び作業の確認

①情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

③統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、2名以上で作業し、互いにその作業を確認しなければならない。

(5) 情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

(6) ログの取得等

①統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(7) 障害記録

統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正

に保存しなければならない。

(8) ネットワークの接続制御、経路制御等

- ①統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。
- ②統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

(9) 外部の者が利用できるシステムの分離等

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

(10) 外部ネットワークとの接続制限等

- ①情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。
- ②情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。
- ③情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。
- ④統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。
- ⑤情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(11) 複合機のセキュリティ管理

- ①統括情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

- ②統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。
- ③統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講じなければならない。

(1 2) IoT 機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(1 3) 無線 LAN 及びネットワークの盗聴対策

- ①統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。
- ②統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(1 4) 電子メールのセキュリティ管理

- ①統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。
- ②統括情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。
- ③統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。
- ④統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。
- ⑤統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めなければならない。
- ⑥統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置を講じなければならない。【推奨事項】

(15) 電子メールの利用制限

- ①職員等は、自動転送機能を用いて、電子メールを転送してはならない。
- ②職員等は、業務上必要のない送信先に電子メールを送信してはならない。
- ③職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
- ④職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

(16) 電子署名・暗号化

- ①職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISOが定めた電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。
- ②職員等は、暗号化を行う場合にCISOが定める以外の方法を用いてはならない。また、CISOが定めた方法で暗号のための鍵を管理しなければならない。
- ③CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(17) 無許可ソフトウェアの導入等の禁止

- ①職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
- ②職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。
- ③職員等は、不正にコピーしたソフトウェアを利用してはならない。

(18) 機器構成の変更の制限

- ①職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。
- ②職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

(19) 業務外ネットワークへの接続の禁止

- ①職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

②情報セキュリティ管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

(20) 業務以外の目的でのウェブ閲覧の禁止

- ①職員等は、業務以外の目的でウェブを閲覧してはならない。
- ②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

(21) Web 会議サービスの利用時の対策

- ①統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。
- ②職員等は、本市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。
- ③職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。
- ④職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

(22) ソーシャルメディアサービスの利用

- ①情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。
  - (ア) 本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理 Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。
  - (イ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。
- ②機密性 2 以上の情報はソーシャルメディアサービスで発信してはならない。
- ③利用するソーシャルメディアサービスごとの責任者を定めなければならない。
- ④アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。
- ⑤可用性 2 の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己

管理 Web サイトに当該情報を掲載して参照可能とすること。

## 6.2. アクセス制御

### (1) アクセス制御等

#### ①アクセス制御

統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

#### ②利用者 ID の取扱い

(ア) 統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

(イ) 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

(ウ) 統括情報セキュリティ責任者及び情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

#### ③特権を付与された ID の管理等

(ア) 統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

(イ) 統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、CISO が認めた者でなければならない。

(ウ) CISO は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

(エ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。

(オ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

(カ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

### (2) 職員等による外部からのアクセス等の制限

①職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統

括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

- ②統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。
- ③統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。
- ④統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。
- ⑤統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。
- ⑥職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。
- ⑦統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、止むを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

### (3) 自動識別の設定

統括情報セキュリティ責任者及び情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。【推奨事項】

### (4) ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

### (5) 認証情報の管理

- ①統括情報セキュリティ責任者又は情報システム管理者は、職員等の認証情報を厳重

に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

②統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

③統括情報セキュリティ責任者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

#### (6) 特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

### 6.3. システム開発、導入、保守等

#### (1) 情報システムの調達

①統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

#### (2) 情報システムの開発

##### ①システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

##### ②システム開発における責任者、作業者の ID の管理

(ア) 情報システム管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

(イ) 情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

##### ③システム開発に用いるハードウェア及びソフトウェアの管理

(ア) 情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(イ) 情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。



### (3) 情報システムの導入

#### ①開発環境と運用環境の分離及び移行手順の明確化

- (ア) 情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。【推奨事項】
- (イ) 情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。
- (ウ) 情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実にし、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。
- (エ) 情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

#### ②テスト

- (ア) 情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。
- (イ) 情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。
- (ウ) 情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。
- (エ) 情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

### (4) システム開発・保守に関連する資料等の整備・保管

- ①情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。
- ②情報システム管理者は、テスト結果を一定期間保管しなければならない。
- ③情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

### (5) 情報システムにおける入出力データの正確性の確保

- ①情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力除去する機能を組み込むように情報システムを設計しなければならない。
- ②情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを

設計しなければならない。

③情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(6) 情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

(7) 開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(8) システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

#### 6.4. 不正プログラム対策

(1) 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

①外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

②外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

④所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定が

ないことを確認しなければならない。

## (2) 情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

- ①情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。
- ②不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
- ③不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
- ④インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。
- ⑤不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

## (3) 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

- ①パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
- ②外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
- ③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
- ④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的実施しなければならない。
- ⑤添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は無害化しなければならない。
- ⑥統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。
- ⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合

は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

#### (4) 専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

### 6.5. 不正アクセス対策

#### (1) 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

- ①使用されていないポートを閉鎖しなければならない。
- ②不要なサービスについて、機能を削除又は停止しなければならない。
- ③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定しなければならない。
- ④重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。【推奨事項】
- ⑤統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

#### (2) 攻撃への対処

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、都道府県等と連絡を密にして情報の収集に努めなければならない。

#### (3) 記録の保存

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

(4) 内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) 職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

(6) サービス不能攻撃

統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(7) 標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

## 6.6. セキュリティ情報の収集

(1) セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

(2) 不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

(3) 情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュ

リティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

## 7. 運用

### 7.1. 情報システムの監視

- ①統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。
- ②統括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。
- ③統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。
- ④暗号化された通信データを監視のために復号することの可否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。【推奨事項】

### 7.2. 情報セキュリティポリシーの遵守状況の確認

#### (1) 遵守状況の確認及び対処

- ①情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及び統括情報セキュリティ責任者に報告しなければならない。
- ②CISO は、発生した問題について、適正かつ速やかに対処しなければならない。
- ③統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

#### (2) パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

CISO 及び CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

#### (3) 職員等の報告義務

- ①職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

- ②当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

### 7.3. 侵害時の対応等

#### (1) 緊急時対応計画の策定

CISO 又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

#### (2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

- ①関係者の連絡先
- ②発生した事案に係る報告すべき事項
- ③発生した事案への対応措置
- ④再発防止措置の策定

#### (3) 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

#### (4) 緊急時対応計画の見直し

CISO 又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

### 7.4. 例外措置

#### (1) 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、CISO の許可を得て、例外措置を講じることができる。

(2) 緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに CISO に報告しなければならない。

(3) 例外措置の申請書の管理

CISO は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

### 7.5. 法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

- ① 地方公務員法(昭和 25 年法律第 261 号)
- ② 著作権法(昭和 45 年法律第 48 号)
- ③ 不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)
- ④ 個人情報の保護に関する法律(平成 15 年法律第 57 号)
- ⑤ 行政手続における特定の個人を識別するための番号の利用等に関する法律(平成 25 年法律第 27 号)
- ⑥ サイバーセキュリティ基本法(平成 26 年法律第 104 号)
- ⑦ ○○市個人情報保護条例(平成○○年条例第○○号)

### 7.6. 懲戒処分等

(1) 懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

(2) 違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

- ①統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
- ②情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
- ③情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリ



ティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

## 8. 業務委託と外部サービスの利用

### 8.1. 業務委託

#### (1) 委託事業者の選定基準

- ①情報セキュリティ管理者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。
- ②情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。【推奨事項】

#### (2) 契約項目

情報システムの運用、保守等を業務委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

- ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
- ・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
- ・提供されるサービスレベルの保証
- ・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
- ・委託事業者の従業員に対する教育の実施
- ・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
- ・業務上知り得た情報の守秘義務
- ・再委託に関する制限事項の遵守
- ・委託業務終了時の情報資産の返還、廃棄等
- ・委託業務の定期報告及び緊急時報告義務
- ・市による監査、検査
- ・市による情報セキュリティインシデント発生時の公表
- ・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

#### (3) 確認・措置等

情報セキュリティ管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、(2)の契約に基づき措置を実施しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

## 8.2. 外部サービスの利用（機密性2以上の情報を取り扱う場合）

### (1) 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性2以上の情報を取り扱う場合）の利用に関する規定を整備すること。

- ①外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下8.2節において「外部サービス利用判断基準」という。）
- ②外部サービス提供者の選定基準
- ③外部サービスの利用申請の許可権限者と利用手続
- ④外部サービス管理者の指名と外部サービスの利用状況の管理

### (2) 外部サービスの選定

①情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

②情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

(ア) 外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止

(イ) 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

(ウ) 外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

(エ) 外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

(オ) 情報セキュリティインシデントへの対処方法

(カ) 情報セキュリティ対策その他の契約の履行状況の確認方法

(キ) 情報セキュリティ対策の履行が不十分な場合の対処方法

③情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。

④情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

- ⑤情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。
- ⑥情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。
- ⑦情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。【推奨事項】
- ⑧情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。
- ⑨ 統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

### (3) 外部サービスの利用に係る調達・契約

- ①情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。
- ②情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

### (4) 外部サービスの利用承認

- ①情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。
- ②利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

③利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

(5) 外部サービスを利用した情報システムの導入・構築時の対策

①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。

(ア) 不正なアクセスを防止するためのアクセス制御

(イ) 取り扱う情報の機密性保護のための暗号化

(ウ) 開発時におけるセキュリティ対策

(エ) 設計・設定時の誤りの防止

②外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

(6) 外部サービスを利用した情報システムの運用・保守時の対策

①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。

(ア) 外部サービス利用方針の規定

(イ) 外部サービス利用に必要な教育

(ウ) 取り扱う資産の管理

(エ) 不正アクセスを防止するためのアクセス制御

(オ) 取り扱う情報の機密性保護のための暗号化

(カ) 外部サービス内の通信の制御

(キ) 設計・設定時の誤りの防止

(ク) 外部サービスを利用した情報システムの事業継続

②情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

③外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。

(7) 外部サービスを利用した情報システムの更改・廃棄時の対策

①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。

(ア) 外部サービスの利用終了時における対策

(イ) 外部サービスで取り扱った情報の廃棄

(ウ) 外部サービスの利用のために作成したアカウントの廃棄

②外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。

### 8.3. 外部サービスの利用（機密性2以上の情報を取り扱わない場合）

#### (1) 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性2以上の情報を取り扱わない場合）の利用に関する規定を整備すること。

(ア) 外部サービスを利用可能な業務の範囲

(イ) 外部サービスの利用申請の許可権限者と利用手続

(ウ) 外部サービス管理者の指名と外部サービスの利用状況の管理

(エ) 外部サービスの利用の運用手順

#### (2) 外部サービスの利用における対策の実施

①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性2以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

②情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

## 9. 評価・見直し

### 9.1. 監査

#### (1) 実施方法

CISOは、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

#### (2) 監査を行う者の要件

①情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

②監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

- (3) 監査実施計画の立案及び実施への協力
- ①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。
  - ②被監査部門は、監査の実施に協力しなければならない。
- (4) 委託事業者に対する監査
- 事業者が業務委託を行っている場合、情報セキュリティ監査統括責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。
- (5) 報告
- 情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。
- (6) 保管
- 情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。
- (7) 監査結果への対応
- CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。
- (8) 情報セキュリティポリシー及び関係規程等の見直し等への活用
- 情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

## 9.2. 自己点検

- (1) 実施方法
- ①統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

②情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

(2) 報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

(3) 自己点検結果の活用

①職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

### 9.3. 情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認められた場合、改善を行うものとする。

## 第3編

# 地方公共団体における 情報セキュリティポリシー (解説)

第3編 地方公共団体における情報セキュリティポリシー (解説)



(目次)

第3編 地方公共団体における情報セキュリティポリシー (解説)	iii-1
第1章 情報セキュリティ基本方針 (解説)	iii-5
1. 目的	iii-5
2. 定義	iii-5
3. 対象とする脅威	iii-6
4. 適用範囲	iii-7
5. 職員等の遵守義務	iii-10
6. 情報セキュリティ対策	iii-10
7. 情報セキュリティ監査及び自己点検の実施	iii-12
8. 情報セキュリティポリシーの見直し	iii-12
9. 情報セキュリティ対策基準の策定	iii-12
10. 情報セキュリティ実施手順の策定	iii-13
11. 宣言書の形式	iii-13
第2章 情報セキュリティ対策基準 (解説)	iii-18
1. 組織体制	iii-18
2. 情報資産の分類と管理	iii-28
3. 情報システム全体の強靱性の向上	iii-33
4. 物理的セキュリティ	iii-49
5. 人的セキュリティ	iii-62
6. 技術的セキュリティ	iii-76
7. 運用	iii-120
8. 業務委託と外部サービスの利用	iii-132
9. 評価・見直し	iii-155
10. 用語の定義	iii-163

# 第1章

## 情報セキュリティ基本方針 (解説)

## (目次)

第1章 情報セキュリティ基本方針（解説）	iii-5
1. 目的	iii-5
2. 定義	iii-5
3. 対象とする脅威	iii-6
4. 適用範囲	iii-7
5. 職員等の遵守義務	iii-10
6. 情報セキュリティ対策	iii-10
7. 情報セキュリティ監査及び自己点検の実施	iii-12
8. 情報セキュリティポリシーの見直し	iii-12
9. 情報セキュリティ対策基準の策定	iii-12
10. 情報セキュリティ実施手順の策定	iii-13
11. 宣言書の形式	iii-13

## 第1章 情報セキュリティ基本方針（解説）

地方公共団体における情報セキュリティ対策の基本的な考え方を示すものが情報セキュリティ基本方針である。地方公共団体としての基本的な取組事項として、セキュリティ対策を実施する目的、対象とする脅威、情報セキュリティポリシーが適用される行政機関や情報資産の範囲、職員等の義務、必要な情報セキュリティ対策の実施、情報セキュリティ対策基準の策定及び情報セキュリティ実施手順の策定等について、情報セキュリティ基本方針に示すものである。必要に応じて住民や外部機関に対して公開することが望ましい。

### 1. 目的

#### 【例文】

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

（解説）

ここでは、なぜ、情報セキュリティが必要なのか、情報セキュリティ対策に取り組む必要性について定めている。情報セキュリティとは、地方公共団体の情報資産を「機密性」、「完全性」、「可用性」に関わる脅威から保護することであり、これを目的としている。「機密性」、「完全性」、「可用性」については、情報セキュリティ基本方針の例文「2. 定義」に定義している。

### 2. 定義

#### 【例文】

(1) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

(2) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

- (5) 機密性  
情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。
- (6) 完全性  
情報が破壊、改ざん又は消去されていない状態を確保することをいう。
- (7) 可用性  
情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。
- (8) マイナンバー利用事務系（個人番号利用事務系）  
個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。
- (9) LGWAN 接続系  
LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。
- (10) インターネット接続系  
インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。
- (11) 通信経路の分割  
LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。
- (12) 無害化通信  
インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

(解説)

情報セキュリティ基本方針及び情報セキュリティ対策基準で使用する情報セキュリティに関わる用語について、定義している。

### 3. 対象とする脅威

【例文】

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

- (1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵

入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

(解説)

情報資産の「機密性」、「完全性」、「可用性」を脅かす脅威を明確にしている。

例文には、昨今、想定される脅威の例を挙げている。

#### 4. 適用範囲

##### 【例文】

##### (1) 行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

##### (2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ① ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
- ② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- ③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

(解説)

情報セキュリティ対策について限られたリソースで最大限の効果が発揮できる様に、情報セキュリティポリシーを適用する行政機関及び情報資産の範囲を明確にして、対策の範囲を決める必要がある。

なお、教育委員会や市立病院等においては、「行政系ネットワーク」（マイナンバー利用事務系及び LGWAN 接続系）とは別に、「教育学習に利用するネットワーク」（校務系、学習系、校務外部接続系等）や「医療情報系ネットワーク」がある。これらのネットワークについては、セキュリティポリシーに関する対策基準のガイドラインが監督官庁において策定されている場合があり、その場合は本ガイドラインの対象外とするが、これらのネットワークが「行政系ネットワーク」と分割されていない場合は、本ガイドラインが適

用されるので注意が必要である。

実際には、各団体の実情に応じて適用させる行政機関を決定することになるが、それぞれの行政機関によって情報セキュリティ対策を進める必要があることに変わりはない。そのため、基本的に全ての行政を司る執行機関を対象とすることが望ましい。

情報セキュリティポリシーの対象とする情報資産の範囲と情報資産の例は下表に示す通りであるが、文書で対象としているのは、ネットワーク、情報システムで取り扱うデータを印刷した文書及びシステム関連文書である。これら以外の文書は、情報資産に含めていないが、文書管理規程等により適正に管理しなければならない。

文書一般を情報資産に含めなかったのは、従来電子データ等の管理と文書の管理が、一般に異なる部署、制度によって行われてきた経緯、実態を踏まえたものである。しかしながら、情報資産の重要性自体は、電子データ等と文書の場合で異なるものでないことから、情報セキュリティ対策が進んだ段階では、全ての文書を情報セキュリティポリシーの対象範囲に含めることが望ましい。

情報資産の種類	情報資産の例
①ネットワーク	通信回線、ルータ等の通信機器等
②情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等
③①・②に関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
④電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体等
⑤ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ等（これらを印刷した文書を含む。）
⑥システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

図表 10 情報資産の種類と例



## 5. 職員等の遵守義務

### 【例文】

職員、非常勤職員及び臨時職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

（解説）

情報セキュリティポリシー及び情報セキュリティ実施手順に対する誤った認識や、遵守しなかったことで情報セキュリティインシデントが発生し、情報システム停止や情報漏えいといった重大事故につながる可能性があるため、職員等は情報セキュリティ対策を実施するにあたり、内容を十分理解し、それらを遵守する必要がある。

また、情報セキュリティポリシーの策定を行う者や、セキュリティ上の職責を担う者は、情報セキュリティポリシーを定めるだけでなく、職員等に対して十分に教育や啓発を行うことが望ましい。

なお、「職員等」とは、例示された者を含む全ての職員が該当するものである。

## 6. 情報セキュリティ対策

### 【例文】

上記3の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

#### (1) 組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

#### (2) 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

#### (3) 情報システム全体の強靱性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

- ③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。
- (4) 物理的セキュリティ  
サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。
- (5) 人的セキュリティ  
情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。
- (6) 技術的セキュリティ  
コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。
- (7) 運用  
情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。
- (8) 業務委託と外部サービスの利用  
業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。  
外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。  
ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。
- (9) 評価・見直し  
情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

(解説)

情報セキュリティ対策の基本方針について記載する。例文では、組織体制、情報資産の分類と管理、情報システム全体の強靱性の向上、物理的セキュリティ、人的セキュリティ、技術的セキュリティ、運用、業務委託と外部サービスの利用及び評価・見直しにおける情

報セキュリティ基本方針を記載している。

## 7. 情報セキュリティ監査及び自己点検の実施

### 【例文】

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

### (解説)

情報セキュリティ上のリスクは、常に変化している。地方公共団体における情報セキュリティ対策もその変化に対応する必要がある。そのため、常に最新の情報セキュリティ関連の情報を収集する体制が必要であり、収集した情報を参考にして、現在の情報セキュリティポリシーの内容に不足している項目がないかどうかを評価しなければならない。

評価のためには、日常的に職員等へのモニタリングを行い、地方公共団体の情報セキュリティポリシー及び情報セキュリティ実施手順が運用の中で遵守されているかについて、職員等や外部の組織によって定期的又は必要に応じて確認しなければならないことを明確にしている。この際に、情報セキュリティポリシーが現場の状況に適合しているか、最新の法令や組織の現状を踏まえ、情報セキュリティポリシーに不備や不足はないか、なども考慮する必要がある。

## 8. 情報セキュリティポリシーの見直し

### 【例文】

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

### (解説)

情報セキュリティの監査及び自己点検の結果並びに内部及び外部の環境の変化から、定期的又は必要に応じて情報セキュリティポリシーを見直さなければならないことを明確にしている。情報セキュリティは、マネジメントの実施サイクル(PDCA サイクル)によって、実態に沿った内容になっているかを常にチェックし、絶えず見直し、改善を図る必要がある。

## 9. 情報セキュリティ対策基準の策定

### 【例文】

上記6、7及び8に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

(解説)

情報セキュリティ基本方針「6. 情報セキュリティ対策」、「7. 情報セキュリティ監査及び自己点検の実施」及び「8. 情報セキュリティポリシーの見直し」で示した情報セキュリティ対策について、遵守事項及び判断基準を定める必要がある。遵守事項及び判断基準は本ガイドラインの情報セキュリティ対策基準に記載している。情報セキュリティ対策基準は、公にすると、サイバー攻撃を受けるリスクがあるため、必要に応じて非公開にすることも考えられる。

#### 10. 情報セキュリティ実施手順の策定

【例文】

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

(解説)

情報セキュリティ対策基準を策定するとともに、その対策基準に対して具体的な手順を定めた情報セキュリティ実施手順を策定する必要がある。情報セキュリティ実施手順は、公にすると、サイバー攻撃を受けるリスクが高くなってしまうため、非公開にする必要がある。

#### 11. 宣言書の形式

(解説)

情報セキュリティ基本方針の記載形式には、地方公共団体が実施する情報セキュリティ対策の基本的事項を規定し、宣言書形式にしても良い。

冒頭で情報セキュリティ対策に取り組む必要性や理念を記載し、全庁的な推進体制、情報セキュリティ対策基準及び情報セキュリティ実施手順の策定、主要な情報セキュリティ対策の実施、職員等の情報セキュリティポリシー遵守義務等を規定している。

地方公共団体の長又は最高情報セキュリティ責任者が、情報セキュリティ対策に積極的に取り組むことを対外的に宣言することができる。

【宣言書の形式例】

## 情報セキュリティ基本方針（宣言書）

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報への漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

本市は、市民の個人情報や行政運営上重要な情報などを多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。また、本市には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。

これらの状況を鑑み、本市における情報資産に対する安全対策を推進し、市民からの信頼を確保し、さらに地域に貢献するため、以下に積極的に取り組むことを宣言する。

- (1) 情報セキュリティ対策に取り組むための全庁的な体制を確立する。
- (2) 情報セキュリティ対策の基準として情報セキュリティ対策基準を策定し、その実行のための手順等を盛り込んだ実施手順を策定する。
- (3) 本市の保有する情報資産を適正に管理する。
- (4) 情報セキュリティ対策の重要性を認識させ、当該対策を適正に実施するために、職員等に対して必要な教育を実施する。
- (5) 情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定める。
- (6) 情報セキュリティ対策の実施状況の監査及び自己点検等を通して、定期的に対策の見直しを実施する。
- (7) 全ての職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守する。
- (8) 地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献する。

令和〇〇年〇〇月〇〇日

〇〇市長（又は、最高情報セキュリティ責任者）

## 第2章

# 情報セキュリティ対策基準 (解説)

## (目次)

第2章 情報セキュリティ対策基準（解説）	iii-18
1. 組織体制	iii-18
2. 情報資産の分類と管理	iii-28
3. 情報システム全体の強靱性の向上	iii-33
4. 物理的セキュリティ	iii-49
4.1. サーバ等の管理	iii-49
4.2. 管理区域(情報システム室等)の管理	iii-54
4.3. 通信回線及び通信回線装置の管理	iii-57
4.4. 職員等の利用する端末や電磁的記録媒体等の管理	iii-59
5. 人的セキュリティ	iii-62
5.1. 職員等の遵守事項	iii-62
5.2. 研修・訓練	iii-68
5.3. 情報セキュリティインシデントの報告	iii-71
5.4. ID及びパスワード等の管理	iii-74
6. 技術的セキュリティ	iii-76
6.1. コンピュータ及びネットワークの管理	iii-76
6.2. アクセス制御	iii-91
6.3. システム開発、導入、保守等	iii-99
6.4. 不正プログラム対策	iii-107
6.5. 不正アクセス対策	iii-111
6.6. セキュリティ情報の収集	iii-116
7. 運用	iii-120
7.1. 情報システムの監視	iii-120
7.2. 情報セキュリティポリシーの遵守状況の確認	iii-122
7.3. 侵害時の対応等	iii-124
7.4. 例外措置	iii-129
7.5. 法令遵守	iii-130
7.6. 懲戒処分等	iii-131
8. 業務委託と外部サービスの利用	iii-132
8.1. 業務委託	iii-132
8.2. 外部サービスの利用（機密性2以上の情報を取り扱う場合）	iii-138
8.3. 外部サービスの利用（機密性2以上の情報を取り扱わない場合）	iii-152
9. 評価・見直し	iii-155
9.1. 監査	iii-155
9.2. 自己点検	iii-159

9.3. 情報セキュリティポリシー及び関係規程等の見直し .....	iii-161
10. 用語の定義.....	iii-163



## 第2章 情報セキュリティ対策基準（解説）

### 1. 組織体制

#### 【趣旨】

組織として、情報セキュリティ対策を確実に実施するには、情報セキュリティ対策に取り組む十分な組織体制を整備し、一元的に情報セキュリティ対策を実施する必要がある。このことから、情報セキュリティ対策のための組織体制、権限及び責任を規定する。

#### 【例文】

(1) 最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

- ①副市長を CISO とする。CISO は、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。
- ②CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。【推奨事項】
- ③CISO は、情報セキュリティインシデントに対処するための体制（CSIRT : Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。
- ④CISO は、CISO を助けて本市における情報セキュリティに関する事務を整理し、CISO の命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副 CISO」という。） 1 人を必要に応じて置く。
- ⑤CISO は、本対策基準に定められた自らの担務を、副 CISO その他の本対策基準に定める責任者に担わせることができる。

(2) 統括情報セキュリティ責任者

- ①情報政策担当部長を CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISO 及び副 CISO を補佐しなければならない。
- ②統括情報セキュリティ責任者は、本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
- ③統括情報セキュリティ責任者は、本市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。
- ④統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関

- する指導及び助言を行う権限を有する。
- ⑤統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。
  - ⑥統括情報セキュリティ責任者は、本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。
  - ⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。
  - ⑧統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。
  - ⑨統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

(3) 情報セキュリティ責任者

- ①内部部局の長、行政委員会事務局の長、消防長及び地方公営企業の局長を情報セキュリティ責任者とする。
- ②情報セキュリティ責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。
- ③情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
- ④情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員、非常勤職員及び臨時職員等（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

(4) 情報セキュリティ管理者

- ①内部部局の課室長、内部部局の出張所等出先機関の長、行政委員会事務局の課室長、消防本部の課室長及び地方公営企業の課室長を情報セキュリティ管理者とする。
- ②情報セキュリティ管理者は、その所管する課室等の情報セキュリティ対策に関す

る権限及び責任を有する。

- ③情報セキュリティ管理者は、その所掌する課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及び CISO へ速やかに報告を行い、指示を仰がなければならない。

(5) 情報システム管理者

- ①各情報システムの担当課室長等を当該情報システムに関する情報システム管理者とする。
- ②情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
- ③情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。
- ④情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

(6) 情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

(7) 情報セキュリティ委員会

- ①本市の情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。
- ②情報セキュリティ委員会は、毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。【推奨事項】

(8) 兼務の禁止

- ①情報セキュリティ対策の実施において、止むを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。
- ②情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

(9) CSIRT の設置・役割

- ①CISO は、CSIRT を整備し、その役割を明確化しなければならない。
- ②CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かな

なければならない。また、CSIRT内の業務統括及び外部との連携等を行う職員等を定めなければならない。

- ③CISOは、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。
- ④CISOによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。
- ⑤情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告しなければならない。
- ⑥情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。
- ⑦情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

(解説)

各地方公共団体においては、図表11のような組織体制を構築して、以下のような情報セキュリティ対策に取り組むことを想定している。

- ・CISO・CSIRTの設置
- ・インシデント連絡ルートの多重化
- ・緊急時対応計画の見直し、緊急時対応訓練の実施及び要員へ適切な教育の実施
- ・標的型攻撃への対策

(注1) 情報セキュリティ対策を確実に実施するには、組織体制を整備するとともに、必要な予算、人員などの資源を確保することが重要である。

(注2) 情報セキュリティポリシーにおいて、誰がどのような権限及び責任を持っているのかを容易に把握できるように一覧表で整理しておくことが望ましい。

(注3) 情報セキュリティインシデントの発生時の連絡ルートは多重化することが望ましい。

(1) 最高情報セキュリティ責任者 (CISO: Chief Information Security Officer、以下「CISO」という。)

CISOは、地方公共団体における全てのネットワーク、情報システム等の情報資産の管理や情報セキュリティに関する権限及び責任を有する。

例文では、CISOが、情報資産の管理や情報セキュリティ対策に関する最終決定権限及び責任を有することとしているが、小規模の地方公共団体などにおいては、情報通信技術の活用による住民の利便性の向上及び行政運営改善等に関するものを統括する最高情報統括責任者 (CIO: Chief Information Officer、以下「CIO」という。)



わって行使できるよう、権限の委譲についても規定しておく。また、情報セキュリティインシデント発生時等の緊急時には、統括情報セキュリティ責任者が中心となり、被害の拡大防止、事態の回復のための対策実施、再発防止策の検討を行う必要がある。

(注5) 統括情報セキュリティ責任者には、具体的には情報政策担当部長、CIO 補佐官等が考えられる。

(3) 情報セキュリティ責任者

情報セキュリティ責任者は、各部局等の情報セキュリティ対策に関する権限及び責任を有する。

(注6) 情報セキュリティ責任者には、内部部局の長、各行政委員会事務局の長、消防長及び各地方公営企業の管理者をあてることが想定される。

(4) 情報セキュリティ管理者

情報セキュリティ管理者は、所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。

情報セキュリティ管理者は、システムの利用現場の担当者であり、所管する課室等において、情報資産に対するセキュリティ侵害又はセキュリティ侵害のおそれがある状況に直面する可能性が高い。そのため、このような場合を想定し、情報セキュリティ責任者、統括情報セキュリティ責任者及び CISO に対する報告義務を定める。

(注7) 情報セキュリティ管理者には、内部部局の課室長、内部部局の出張所等出先機関の長、各行政委員会事務局の課室長、消防本部の課室長及び各地方公営企業の課室長をあてることが想定される。

(5) 情報システム管理者

情報システム管理者は、個々の情報システムの開発、設定の変更、運用、見直し等の権限及び責任を有するほか、所管する情報システムに対する情報セキュリティ対策に関する権限及び責任を負う。

個々の情報システムに関する情報セキュリティ実施手順の維持・管理は、情報システム管理者が行う。

(注8) 情報システム管理者には、各情報システムの担当課室長等をあてることが想定される。

(6) 情報システム担当者

情報システム担当者とは、情報システム管理者の指示等に従う職員で、開発、設定の変更、運用、更新等の作業を行う。

(7) 情報セキュリティ委員会

情報セキュリティに関する重要事項を決定する機関として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は、リスク情報の共有、情報セキュリティポリシーの決定等、情報セキュリティに関する重要な事項を決定する。

(注9) 情報セキュリティ委員会の構成員は、CISO、CIO、統括情報セキュリティ

責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者等が想定され、定期的及び必要に応じて CISO が構成員を招集し、開催する。

(注 1 0) 小規模の地方公共団体等においては、情報化推進委員会が情報セキュリティ委員会を兼ねるなど、地方公共団体の実情に応じた柔軟な運営が必要である。

(注 1 1) 情報セキュリティに関する意思決定機関として情報セキュリティ委員会以外に庁議や幹部会議等を位置付けることも可能である。

#### (8) 兼務の禁止

情報セキュリティ対策に係る組織において、申請者と承認者が同一であることや監査人と被監査部門の者が同一である場合は、承認や監査の客観性が担保されないため、兼務の禁止を定める。

「止むを得ない場合」とは、例えば、統括情報セキュリティ責任者のみに認められた承認について、統括情報セキュリティ責任者が申請する場合や小規模団体に代替する者がいない場合などをいう。

#### (9) CSIRT の設置・役割

情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生状況のとりまとめ、CISO・CIO への報告、報道機関等への通知・公表、関係機関との情報共有など、情報セキュリティインシデントに関するコミュニケーションの核となる体制を、危機管理等の既存の枠組み等を活用するなどして構築する必要がある。CISO は、コミュニケーションの核となる体制として CSIRT を整備し、その役割を明確化する必要がある。

CSIRT は、報告された事案について、その状況を確認し、情報セキュリティインシデントであるかの評価を行う。その結果、情報セキュリティインシデントであると評価した場合、統括情報セキュリティ責任者は、CISO に速やかに報告する。CSIRT は、被害の拡大防止等を図るため、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、応急措置の実施及び復旧に係る指示、勧告及び助言を行う。CSIRT は、CISO、総務省、都道府県等に報告し、情報システムの停止を含む必要な措置を講じる。CSIRT は、情報セキュリティインシデントに関する対処の内容を記録する必要がある。

また、CSIRT は、職員等に対して情報セキュリティインシデントの予防や啓発のための活動等を行うことが望ましい。

(注 1 2) CSIRT の設置においては、役割を明確にする必要があるため、以下を参考に構築や役割の明確化を実施することが望ましい。

- ・「情報セキュリティインシデント対応ハンドブック（令和 2 年 3 月版）」（地方公共団体情報システム機構）
- ・「小規模自治体のための CSIRT 構築の手引き」（地方公共団体情報システム

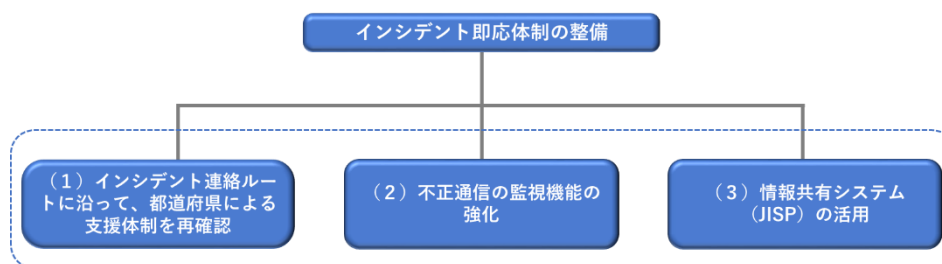
機構)

また、地方公共団体情報システム機構（自治体 CEPTOAR 事務局）等の関係機関や他の地方公共団体における同様の窓口機能、委託事業者、有識者及び専門家等と連携して体制を強化するとともに、有事の際においても専門家との連携ができるようにしておくことが望ましい。

（注1 3）一般的に情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を CSIRT と呼ぶ。CSIRT の持つ機能や在り方は組織によって様々であるが、まずは、地方公共団体においては情報セキュリティに関する統一的な窓口の機能を有する体制を整えることが重要である。

（注1 4）情報セキュリティインシデントに関しては、単独で対応することが困難なケースもあること、また同様の被害拡大防止、発生の予防が重要であることから、インシデント即応体制は図表 12 の3つの視点から整備することが必要である。都道府県は、各都道府県内の市区町村における情報セキュリティインシデント発生時において、国への連絡を行うとともに、当該市区町村の情報セキュリティインシデント対応の支援を実施することが期待される。平常時から、都道府県と管内市区町村との間の連絡を密にして、各都道府県において、都道府県 CSIRT と市区町村 CSIRT の連携体制を構築しておくことが望ましい。

都道府県においては、自らの対策の充実とともに、市区町村に対する初動対応の支援体制の強化及び自治体情報セキュリティクラウドの構築等により、各市区町村における必要な情報セキュリティ水準の確保に努めることが望ましい。



図表 12 インシデント即応体制の整備例

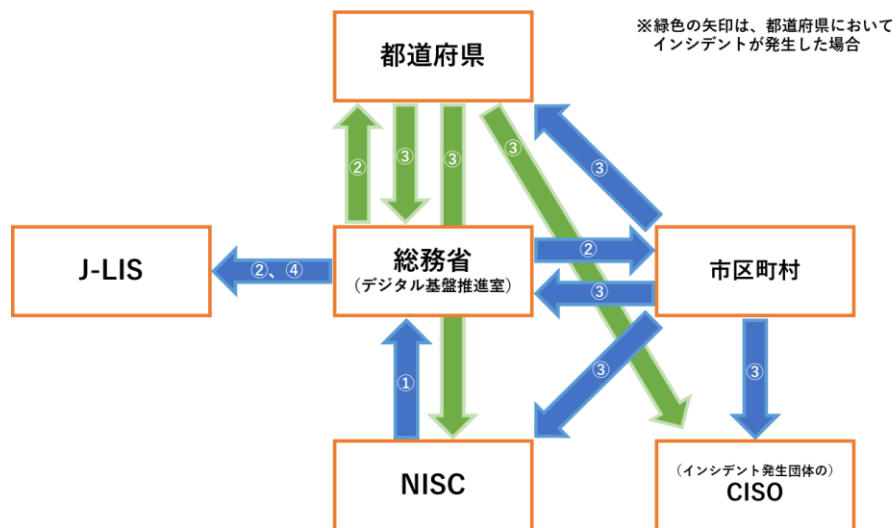
（注1 5）情報セキュリティインシデント発生時の連絡ルートは、インシデントの検知元により連絡ルートが異なるため注意すること。報告の際は、原則 LGWAN を利用すること。

(a) 内閣官房内閣サイバーセキュリティセンター (NISC) が検知したイン



シデントの連絡ルート

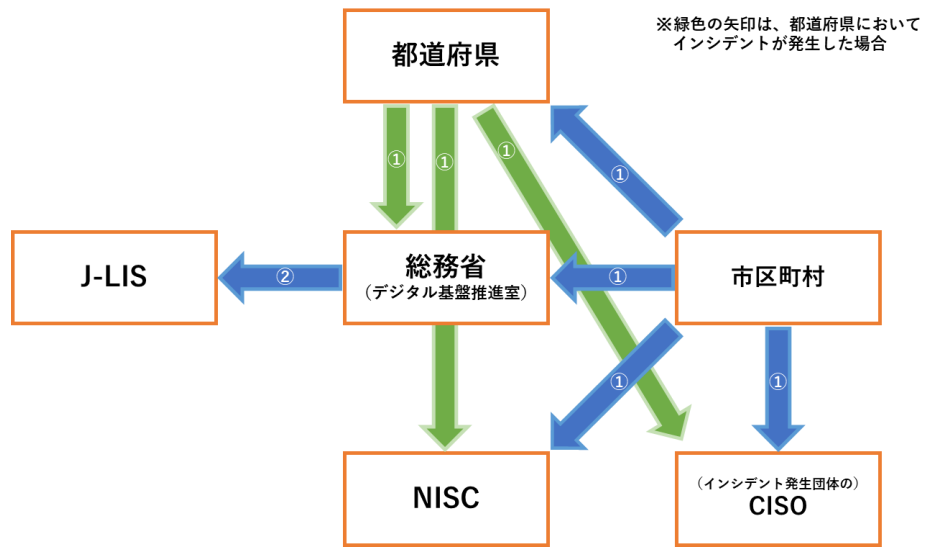
- ①NISC は、総務省に情報提供を行う。
- ②総務省は、インシデントが発生した自治体及び当該団体が所在する都道府県に情報提供を行う。また、必要に応じて J-LIS に情報提供する。  
 ※サイバー攻撃（と考えられる事案を含む）に係るものについては全て情報提供を行う。
- ③インシデントが発生した市区町村（指定都市を含む）は、対応状況について速やかに都道府県、総務省、NISC 及び市区町村内 CISO に報告する。（都道府県においてインシデントが発生した場合も同様）
- ④総務省は、③の内容を必要に応じて J-LIS に情報提供する。



図表 13 NISC が検知したインシデントの連絡フロー

(b) 各地方公共団体が検知したインシデントの連絡ルート

- ①インシデントが発生した市区町村（指定都市を含む）は、対応状況について速やかに都道府県、総務省、NISC 及び市区町村内 CISO に報告する。（都道府県においてインシデントが発生した場合も同様）
- ②総務省は、必要に応じて J-LIS に情報提供する。



図表 14 各地方公共団体が検知したインシデントの連絡フロー

## 2. 情報資産の分類と管理

### 【趣旨】

情報資産を保護するには、まず情報資産を分類し、分類に応じた管理体制を定める必要がある。情報資産の管理体制が不十分な場合、情報の漏えい、紛失等の被害が生じるおそれがある。そこで、機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じて取るべき管理方法を規定する。

### 【例文】

#### (1) 情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

#### 機密性による情報資産の分類

分類	分類基準	取扱制限
機密性 3	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	<ul style="list-style-type: none"> <li>・支給以外の端末での作業の原則禁止（機密性 3 の情報資産に対して）</li> </ul>
機密性 2	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	<ul style="list-style-type: none"> <li>・必要以上の複製及び配付禁止</li> <li>・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止</li> <li>・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納</li> <li>・復元不可能な処理を施しての廃棄</li> <li>・信頼のできるネットワーク回線の選択</li> <li>・外部で情報処理を行う際の安全管理措置の規定</li> <li>・電磁的記録媒体の施錠可能な場所への保管</li> </ul>
機密性 1	機密性 2 又は機密性 3 の情報資産以外の情報資産	—

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性 2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> <li>・バックアップ、電子署名付与</li> <li>・外部で情報処理を行う際の安全管理措置の規定</li> <li>・電磁的記録媒体の施錠可能な場所への保管</li> </ul>
完全性 1	完全性 2 の情報資産以外の情報資産	—

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性 2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> <li>・バックアップ、指定する時間以内の復旧</li> <li>・電磁的記録媒体の施錠可能な場所への保管</li> </ul>
可用性 1	可用性 2 の情報資産以外の情報資産	—

(2) 情報資産の管理

①管理責任

(ア) 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

(イ) 情報資産が複製又は伝送された場合には、複製等された情報資産も(1)の分類に基づき管理しなければならない。

②情報資産の分類の表示

職員等は、情報資産について、ファイル(ファイル名、ファイルの属性(プロパティ)、ヘッダー・フッター等)、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

③情報の作成

(ア) 職員等は、業務上必要のない情報を作成してはならない。

(イ) 情報を作成する者は、情報の作成時に(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ウ) 情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しな

なければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④情報資産の入手

(ア) 庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

(イ) 庁外の者が作成した情報資産を入手した者は、(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ウ) 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

⑤情報資産の利用

(ア) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

(イ) 情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

(ウ) 情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥情報資産の保管

(ア) 情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

(イ) 情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

(ウ) 情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。【推奨事項】

(エ) 情報セキュリティ管理者又は情報システム管理者は、機密性2以上、完全性2又は可用性2の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施設可能な場所に保管しなければならない。

⑦情報の送信

電子メール等により機密性2以上の情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

⑧情報資産の運搬

(ア) 車両等により機密性2以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

(イ) 機密性 2 以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑨情報資産の提供・公表

(ア) 機密性 2 以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

(イ) 機密性 2 以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

(ウ) 情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑩情報資産の廃棄等

(ア) 情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

(イ) 情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(ウ) 情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

(解説)

(1) 情報資産の分類

情報資産について、機密性、完全性及び可用性を踏まえ、被害を受けた場合に想定される影響の大きさをもとに分類を行い、必要に応じ取扱制限を定める必要がある。

(注 1) 情報資産の分類は、機密性、完全性及び可用性に基づき、分類することが望ましいが、職員の理解度等に応じ、以下のような重要性に基づき分類することもあり得る。

重 要 性 分 類	
I	個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報。
II	公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。
III	外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に微妙な影響を及ぼす情報。
IV	上記以外の情報。

## (2) 情報資産の管理

### ①管理責任

情報資産の管理は、その情報資産に係る実務に精通している者が行う必要があり、本ガイドラインでは、情報資産の管理責任者を情報セキュリティ管理者（課室長等）と想定している。

（注2）管理に当たっては、重要な情報資産について台帳を作成することが望ましい。これにより、情報資産の所在、分類、管理責任が明確になる。また、情報資産の管理について、管理者不在の状態や二重管理にならないように留意することが重要である。

### ②情報資産の分類の表示

（注3）情報システムについて、当該情報システムに記録される情報の分類を規定等により明記し、当該情報システムを利用する全ての者に周知する方法もある。

（注4）機密性2以上、完全性2、可用性2の情報資産についてのみ表示を行い、表示のない情報資産は、機密性1、完全性1、可用性1とする運用もある。

### ③情報の作成～⑩情報資産の廃棄

情報資産の取扱いについて遵守すべき事項は、情報のライフサイクルに着目し定める。情報のライフサイクルには、作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等の局面がある。これらの局面ごとに、情報資産の分類に応じ取扱制限を定める。また、情報のライフサイクルの局面、情報資産の分類及び分類に応じた取扱制限については、定期的又は必要に応じて見直すことが重要である。なお、庁外の者が提供するアプリケーション・コンテンツに関する情報を告知する場合は、アプリケーション・コンテンツのリンク先のURLやドメイン名の有効性や管理する組織名等の必要情報を明記するなどの対策を講じる必要がある。

（注5）情報の提供、行政手続、意見募集等の行政サービスのためにアプリケーション・コンテンツを提供する場合は、利用者端末の情報セキュリティ水準の低下を招いてしまうことを避けるため、アプリケーション・コンテンツの作成に係る規定の整備やセキュリティ要件の策定等の情報セキュリティ対策を講じておく必要がある。

（注6）電子メール等により情報を送信する場合の暗号化に用いるパスワードについては、あらかじめ受信者と合意した文字列を用いるか、あるいは、電子メールで送信せずに電話などの別手段を用いて伝達することが望ましい。

### 3. 情報システム全体の強靱性の向上

#### 【趣旨】

複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、各地方公共団体においては、機密性はもとより、可用性や完全性の確保にも十分配慮された攻撃に強い情報システムが望まれる。

#### 【例文】

##### (1) マイナンバー利用事務系

###### ①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル(ポート番号)のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

###### ②情報のアクセス及び持ち出しにおける対策

###### (ア) 情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証(多要素認証)を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

###### (イ) 情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

##### (2) LGWAN 接続系

###### ①LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

(ア) インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

(イ) インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式



(ウ) 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(3) インターネット接続系

①インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

②都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

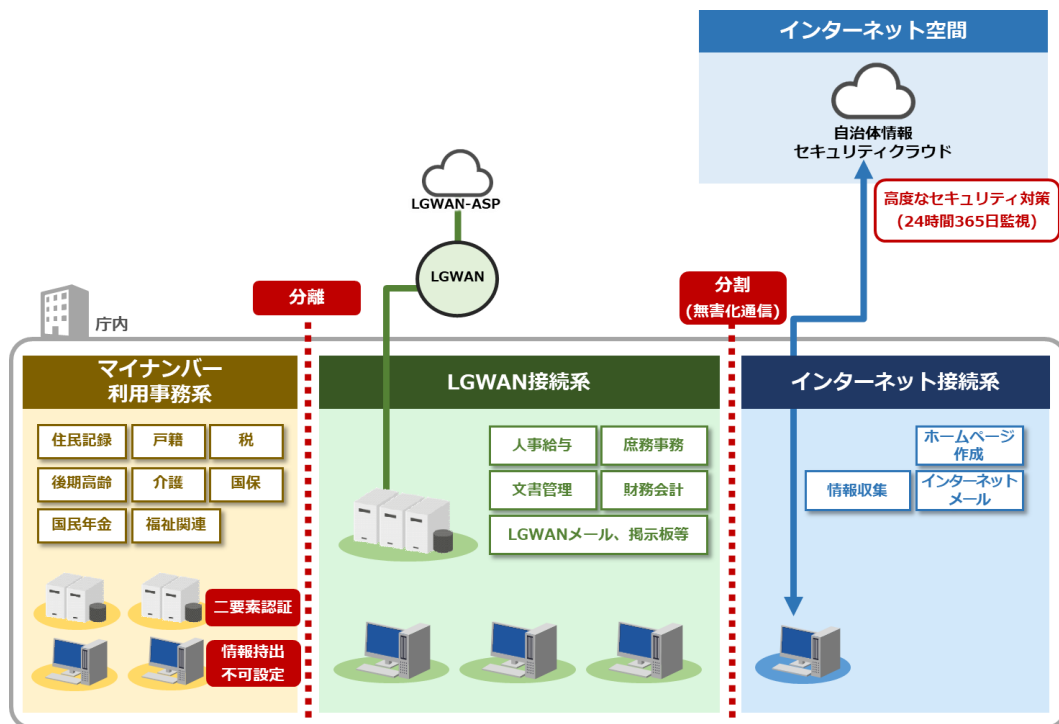
③ (B モデルを採用する場合) 業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産を LGWAN 接続系に配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

(B'モデルを採用する場合) 業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

(解説)

情報システム全体の強靱性の向上を図るため、情報セキュリティ対策の抜本的強化が必要であり、これを実現させる手法を「三層の構え」という。

三層の構えによる情報セキュリティ対策の詳細については、「新たな自治体情報セキュリティ対策の抜本的強化に向けて」(平成 27 年 11 月 24 日自治体情報セキュリティ対策検討チーム報告)及び「新たな自治体情報セキュリティ対策の抜本的強化について」(平成 27 年 12 月 25 日総行情第 77 号 総務大臣通知)等を参照されたい。



図表 15 三層の構えによる自治体情報システム例

(1) マイナンバー利用事務系

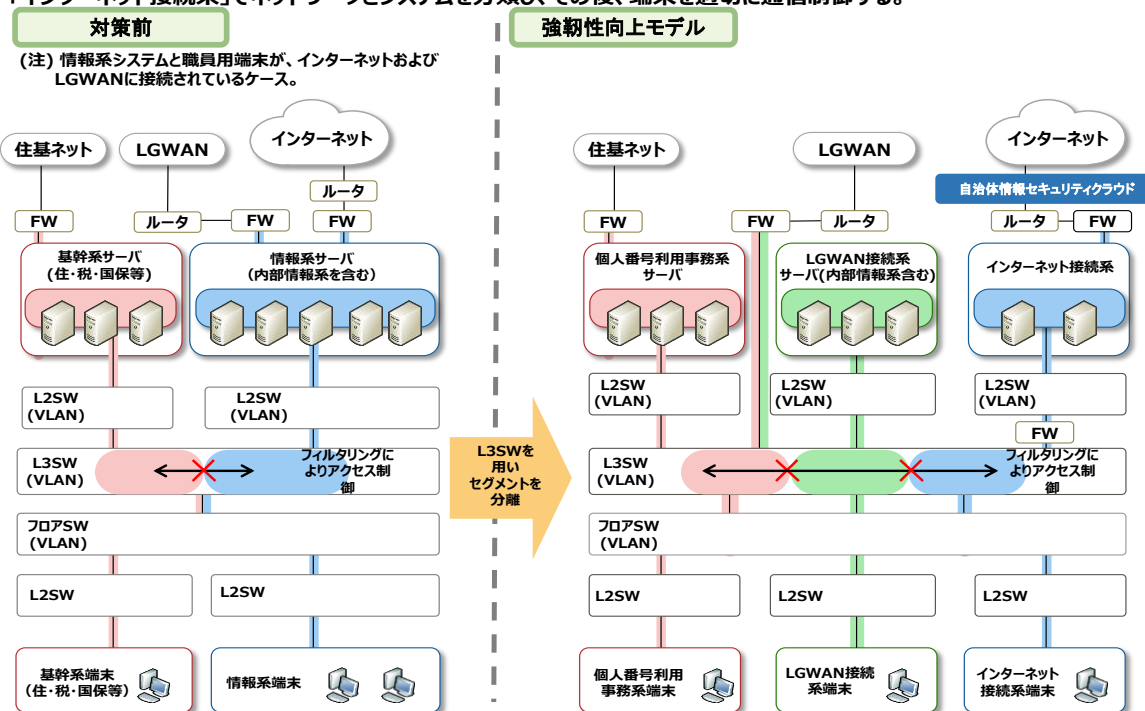
① マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系においては、住民情報の流失を防ぐ必要があることから、他の領域（LGWAN 接続系及びインターネット接続系）との通信をできないようにしなければならない。統合パッケージシステムを利用している場合であっても、マイナンバー利用事務系と LGWAN 接続系との端末は分けなければならない。総合窓口を実施している場合等、業務毎に専用端末を設置することが難しい場合には、端末からの情報持ち出し不可設定や端末への多要素認証の導入を図り、利用状況をチェックする運用体制などを整備した上で実施することが望ましい。

マイナンバー利用事務系と LGWAN 接続系のサーバが仮想化基盤上にあり、物理的なサーバに共存している場合は、各システムの通信について、分離を徹底することが重要であることから、通信が分離されていることの確認を行わなければならない。

なお、地方公共団体が共同で利用するデータセンターに構築しているネットワークについても、庁内ネットワークとして同様の措置を行わなければならない。

LGWAN環境とインターネット環境を分割し、「個人番号利用事務系」、「LGWAN接続系」、「インターネット接続系」でネットワークとシステムを分類し、その後、端末を適切に通信制御する。



図表 16 強靱性向上モデルにおけるネットワーク再構成の一つのイメージ

マイナンバー利用事務系と外部との通信の必要がある場合は、通信経路の限定 (MAC アドレス、IP アドレス) に加えて、アプリケーションプロトコル (ポート番号) のレベルでの限定を行わなければならない。これらの限定を行った通信を特定通信という。

特定通信を行う際は、以下の点に留意しなければならない。

- (ア) L2SW/L3SW による通信経路限定、ファイアウォールによる通信プロトコル限定等を行うことで通信を制限すること。
- (イ) その他外部ネットワークとの通信が発生する場合は専用回線サービス (IP-VPN や SSL-VPN など仮想技術を利用した通信を含む) を検討すること。
- (ウ) 特定通信は、マイナンバー利用事務系が、住民基本台帳ネットワーク、中間サーバ連携、コンビニ交付や LGWAN-ASP サービスなど接続先が信頼される特定先との通信のことであり、マイナンバー利用事務系は、LGWAN 接続系やインターネット接続系と特定通信として接続してはならない。

特定通信となる外部接続の例として、住民基本台帳ネットワークシステム、マイナンバー制度における中間サーバ連携や住民票の写し等のコンビニ交付用の LGWAN 接続、データバックアップセンターや共同利用/クラウドセンター等、十分に情報セキュリティが確保された通信先との限定的な接続がある。また、特定通信を行う外部接続先についても、インターネット等と接続されてはならない。

い。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、LGWAN を経由してマイナンバー利用事務系にデータの移送を可能とする。

(注1) 現在、国等の公的機関が構築したインターネットに接続されたシステム等で十分に安全性が確保された外部接続先との通信として eLTAX、マイナポータル、自治体情報セキュリティ向上プラットフォームが考えられる。これらの外部接続先と LGWAN を経由してマイナンバー利用事務系が双方向でデータを移送する場合、特定通信を行う際の留意点に加え、以下の対策が必要である。

- ・外部接続先とは、連携サーバを設置して通信を行うこととする。外部接続先からのデータやファイルは、連携サーバを介してマイナンバー利用事務系と通信する。また、ファイアウォールやプロキシサーバ等でマイナンバー利用事務系から外部接続先に直接通信する経路が許可されないよう設定する。
- ・ファイアウォールや連携サーバで外部接続先との通信を制限 (FQDN 指定) することで通信先を限定する。
- ・許可されていないマイナンバー利用事務系の端末から外部接続先へ接続することがないように、ファイアウォールや連携サーバで通信を制限する。
- ・マイナンバー利用事務系のサーバ、端末については、ウイルス対策ソフトを導入し、最新の定義ファイルを常時更新する。また、OS の修正プログラムについても最新の修正プログラムを常時更新する運用や対策を行わなければならない。
- ・住民の情報を扱う場合は、外部接続先とは TLS プロトコルを利用し、認証、暗号化、改ざんの検知等の対策を実施する。これらの対策に加え、ファイアウォール及び連携サーバの通信の履歴等を取得することが望ましい。
- ・USB メモリ等の電磁的記録媒体により不正プログラムに感染する可能性があるため、マイナンバー利用事務系の端末及び外部接続先との接続に利用する端末について、電磁的記録媒体の利用制御を実施しなければならない。なお、電磁的記録媒体の利用制御については、本解説の「(1) ② (イ) 情報の持ち出し不可設定」を参照されたい。
- ・ウェブアプリケーションを利用しているシステムの場合は、ウェブアプリケーションの実装面として脆弱性を作り込まない対策、定期的な診断などを行って脆弱性を検出・対処する対策が必要となる。脆弱性を作り込まない対策としては「6.3. システム開発、導入、保守等 (解説) (5) (注11)」を、脆弱性の検出・対処の対策としては「6.6. セキュリティ情報の収集 (解説) (1) (注4)」を参照されたい。

(注2) (注1) の接続先以外の外部接続先については、止むを得ずインターネット

トとデータをやり取りする場合は、専用回線を新たに設置し、必要最小限の通信とし、外部のネットワークと通信する専用の端末を管理区域内に設置した上で、電磁的記録媒体を経由したデータのやり取りを行わなければならない。その際には情報システム管理者の許可を受けた上で、電磁的記録媒体の接続禁止設定を一時的に解除し、他の職員の立ち合い又は監視カメラで撮影された状態で、管理区域内において作業を行うなどの取扱いを行わなければならない。また、保守用の外部接続先がある場合は、保守の委託先の情報セキュリティ対策が確実に実施されるよう職員等が当該委託先の情報セキュリティ対策を直接管理したり、委託先への要求事項を調達仕様書等に定め、契約条件とするなどの対策が必要である。その他、運用面として保守用の外部接続先との通信は保守の時のみに限定するなどの対策も考えられる。なお、外部接続先との通信については、本解説の「(4) ⑤VPN 接続による外部との通信」も参照されたい。

(注3) 指定金融機関から税などの口座引落済みデータ（消し込みデータ）等の外部データを受信し、マイナンバー利用事務系へ取り込みを行う場合は、LGWAN-ASP 等を利用して受信しなければならない。マルウェア感染しているファイルをマイナンバー利用事務系に取り込んでしまうことを防止するため、以下の手順で取り込むことが考えられる。

- ・ 予め指定された職員等が、他の職員等の立ち合い又は操作が監視カメラで記録される管理区画等において、LGWAN 接続系端末でウイルスチェックを実施
- ・ 他の用途で使用されることのない専用の電磁的記録媒体に保存
- ・ システム管理責任者による電磁的記録媒体接続禁止の一時的解除
- ・ マイナンバー利用事務系端末でウイルスチェックを実施後に取り込む

## ②情報のアクセス及び持ち出しにおける対策

### (ア) 情報のアクセス対策

認証手段には「知識」「所持」「存在」の種類が存在する。認証の種類と手段及び情報システムが正規の利用者かどうかを判断する手段を以下に示す。

種類	認証の手段
知識	正規の利用者“だけが知っている情報（知識）”をその人が知っているか否かで判断する
所持	正規の利用者“だけが持っているモノ（所持品）”をその人が持っているか否かで判断する
存在	正規の利用者の“身に備わっている特徴（利用者自身の存在）”でその人か否かを判断する

図表 17 認証の種類と手段

認証手段の概要と具体例	利点	欠点	
「知識」を利用する手段	<ul style="list-style-type: none"> <li>● パスワード</li> <li>● パスフレーズ</li> <li>● 暗証番号</li> <li>● ピクチャーパスワード</li> </ul>	<ul style="list-style-type: none"> <li>● 運用コストが安い</li> <li>● 特別な装置が不要で、非常に簡便</li> </ul>	<ul style="list-style-type: none"> <li>● 複雑すぎる「知識」は記憶できない</li> <li>● 簡単な「知識」さえあれば、正規の利用者でなくても、「知識」を推定して正規の利用者になりすますことができる</li> <li>● 「知識」忘失の恐れがある</li> </ul>
「知識」と「所持」を併用	<ul style="list-style-type: none"> <li>● IC カードと暗証番号の併用</li> <li>● ワンタイムパスワードとトークンとパスワード(暗証番号)の併用</li> <li>● SIM カード(携帯電話/スマートフォンの固有番号)とパスワードの併用</li> </ul>	<ul style="list-style-type: none"> <li>● 「知識」と「所持」を併用することで、「知識」だけ、あるいは「所持」だけに頼るよりも安全性が高い</li> </ul>	<ul style="list-style-type: none"> <li>● カードやトークン等が必要で運用コストが高い</li> <li>● カードやトークン等の盗難・紛失の恐れがある</li> <li>● 「知識」忘失の恐れがある</li> </ul>
「所持」を利用する手段	<ul style="list-style-type: none"> <li>● IC カード</li> <li>● USB トークン</li> <li>● SIM カード(携帯電話/スマートフォンの固有番号)</li> </ul>	<ul style="list-style-type: none"> <li>● 「知識」に頼らず、安全性を向上できる</li> </ul>	<ul style="list-style-type: none"> <li>● カードやトークン等が必要で運用コストが高い</li> <li>● カードやトークン等の盗難・紛失の恐れがある</li> <li>● 正規の利用者でなくても、何らかの手段(例えば盗難や偽造)でカードやトークン等を「所持」することができれば、情報システムは正規の利用者と誤認する</li> </ul>

認証手段の概要と具体例		利点	欠点
「存在」を利用する手段	● バイオメトリックス認証 (指紋、声紋、静脈等)	<ul style="list-style-type: none"> <li>● 「知識」や「所持」に頼らず、安全性を向上できる</li> <li>● 偽造がかなり困難</li> <li>● 盗難・紛失の恐れがない</li> </ul>	<ul style="list-style-type: none"> <li>● 特別な装置が必要で、運用コストが高い</li> <li>● システム・装置によって認証精度に大きなばらつきがある</li> <li>● 認証データは本人固有の生体情報を基にして作られるため、万が一、認証データの漏えいや偽造が発生しても、認証データ自体を変えることができない</li> </ul>
	● リスクベース認証 (行動パターン、キーボードを使う時の癖など)	<ul style="list-style-type: none"> <li>● 行動パターンや癖などをまねるのは難しい</li> <li>● 完全に一致する行動パターンや癖が現れるのもかえって不自然と判断可能</li> <li>● 盗難・紛失の恐れがない</li> </ul>	<ul style="list-style-type: none"> <li>● 完全な利用者認証にはならない。“リスクベース”とは、行動パターンやキーボードを使う時の癖がいつもと違うことを検出した時に、“他人が利用しているかもしれない＝リスクの検知”と判断して、別の利用者認証を要求する、という意味</li> <li>● 状態監視が常時必要なので、運用コストが比較的高い</li> </ul>

図表 18 情報システムが正規の利用者かどうかを判断する認証手段

(注 4) 接続する端末を特定するために MAC アドレスの管理を行うことが望ましい。

#### (イ) 情報の持ち出し不可設定

納付書など大量帳票のアウトソーシングや指定金融機関に対する口座振替情報の提供等の電磁的記録媒体の利用が止むを得ない場合においては、管理者権限を持つ職員によってその都度限定を解除する又は管理者権限を持つ職員のみ許可する設定とすることを例外として取り扱わなければならない。

USB メモリ等の電磁的記録媒体による端末からの情報持ち出しを行う場合は、次の手段により実施しなければならない。

- ・ 端末には利用許可された媒体のみ接続可能とすること。
- ・ データは暗号化しパスワードを設定すること。
- ・ 利用媒体は、全て管理し利用履歴を残せること。
- ・ データの受け渡しには、必ず情報セキュリティ管理者の承認と承認記録を残せること。

## (2) LGWAN 接続系

### ①LGWAN 接続系とインターネット接続系の分割

分割とは、一旦両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにすることをいう。

(ア) インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

LGWAN 接続系へインターネットメールを転送する際には、インターネットメールの転送に必要な特定サーバ間以外の通信を遮断するとともに、LGWAN 環境とインターネット環境は SMTP 以外の Web 通信を始めとするプロトコルを遮断し、インターネットメールの添付ファイルの削除及び HTML メールテキスト化を行う。

(イ) インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

インターネット接続系の端末を仮想デスクトップ化し、LGWAN 接続系の端末から添付ファイルも含むメールの閲覧を可能とする。

(ウ) 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

危険因子が埋め込まれたファイルを LGWAN 接続系に取り込んだ場合、脆弱性を突いた悪意あるコード等が実行される恐れがある。インターネット接続系から LGWAN 接続系にファイルを取り込む際は、以下のような手法により、危険因子をファイルから除去又は危険因子がファイルに含まれていないことの確認を行った上で、取り込まなければならない。(いずれかの手法のみ又は複数の手法を組み合わせることで採用することが考えられる。)

- ・ファイルからテキストのみを抽出
- ・ファイルを画像 PDF に変換
- ・サービス等を活用してサニタイズ処理(ファイルを一旦分解した上で危険因子を除去した後、ファイルを再構築し、分解前と同様なファイル形式に復元する)
- ・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等で危険因子が含まれていないことを確認

なお、上記のいずれか又は複数の手法による対策を実施した場合であっても、マルウェア等の除去が完全に保証されるものではないため、LGWAN 接続系において以下のようなセキュリティ対策を実施しなければならない。

- ・OS 等の修正プログラムの適時適用(自治体情報セキュリティ向上プ



ラットフォームの利用等)

- ・アンチウイルスソフトウェアの最新化(定義ファイルのアップデート等)
- ・業務に必要なファイルやメール等の定期的なバックアップの実施

また、上記の LGWAN 接続系における対策に加え、業務システムの停止を狙ったマルウェアの感染を防ぐ対策として、LGWAN 接続系端末にアプリケーションホホワイトリストを設定し、実行できるアプリケーションの制限等を行うことを強く推奨する。

(注5)「目視で確認」とは、ファイルが添付されたメールを開く際に、送信元は適切か(見覚えのないアドレス、フリーアドレス又は正規の組織名若しくはドメインに似せたアドレスではないか)、メールの件名や内容が適切か(見慣れない日本語やフォントが使用されていないか)などを確認することである。未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等の製品の導入に加え、人的対策として「目視で確認」を求めるものである。

(注6) サニタイズ処理等を実現する手法は多岐にわたるため、適正な製品を選定し導入することが望ましい。

(注7) 仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系から LGWAN 接続系へマルウェア感染を防ぐ必要がある。

### (3) インターネット接続系

① インターネット接続系で実施する情報セキュリティ対策の内容は具体的には以下のものがある。

#### (ア) サーバ等の監視

Web サーバ、メールリレーサーバ、プロキシサーバ、外部 DNS サーバのログの監視を行う。

#### (イ) 情報セキュリティ機器の導入

通信パケットの監視及び破棄、通信ポートの制御、不正なプログラムの検知、不審なメールの検知及び遮断、不審な URL へのアクセス遮断、ログ監視、コンテンツの改ざん検知等の機能を持った高度な情報セキュリティ機器を導入する。

#### (ウ) 情報セキュリティ運用監視

情報セキュリティ専門人材による高水準なセキュリティ運用監視を行う。

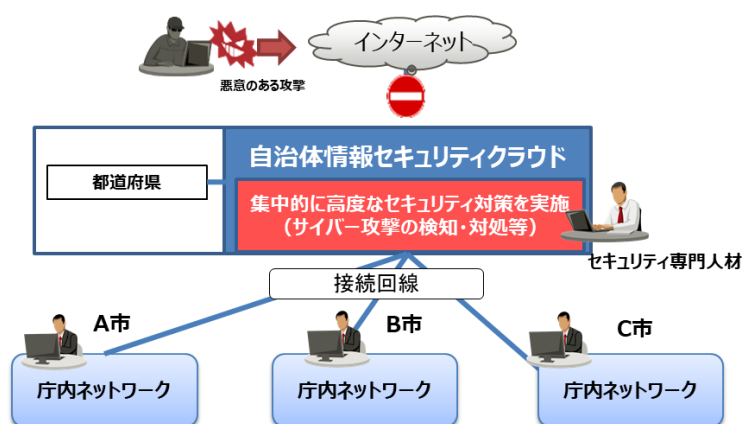
② 自治体情報セキュリティクラウドの導入等による情報セキュリティ対策では、以下のような情報セキュリティレベルの向上とコスト削減が期待される。

- ・各市区町村において必要な情報セキュリティレベルの確保・向上
- ・情報セキュリティ専門人材によるインシデントの早期発見と対処

- ・ 機器・運用の共同利用によるコスト削減

(注8) 都道府県及び市区町村のインターネットとの通信を監視するため、業務に支障のない稼働が望まれる。情報セキュリティインシデントに対し迅速かつ適正に対応するために、セキュリティの専門人材が24時間365日有人で集中監視と分析を行う監視機能を持つSOC(Security Operation Center)を設置し、インシデントの予兆を含め早期検知を図らなければならない。

(注9) 「次期自治体情報セキュリティクラウドの標準要件について」(令和2年8月18日総行情109号 総務省自治行政局地域情報政策室長通知)における標準要件等に基づき自治体情報セキュリティクラウドを導入しなければならない。なお、都道府県とは別に、市区町村において独自に自治体情報セキュリティクラウドの調達を行った場合は、市区町村の調達した自治体情報セキュリティクラウドが標準要件に基づいた機能を有すること及び運用がなされていることについて、定期的に外部監査を受けなければならない。



図表 19 自治体情報セキュリティクラウド

③業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末・システムを配置する場合、以下のモデルが考えられる。

- ・ Bモデル：インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産は LGWAN 接続系に配置する方式・・・(ア)
- ・ B'モデル：インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する方式・・・(イ)

(注10) B'モデルで取り扱う重要な情報資産とは、機密性3に該当する秘密情報に相当する機密性を要する情報資産を想定する。なお、インターネット接続系に職員のマインumber情報を配置する場合には、情報の取扱いに十分留意し、アクセス制御等のセキュリティ対策を適正に実施する必要がある。

これらのモデルは、クラウドサービスの活用、テレワーク、事業者とのやり取り等でメリットがある一方、インターネットからのリスクも増加することとなる。また、サイバー攻撃の高度化・複雑化により、自治体情報セキュリティクラウド側でのファイアウォールや IPS/IDS 等の防御による対策だけでは、マルウェアの侵入等を防ぐことが困難となっている。

このため、特に、これらのモデルを採用する自治体においては、インターネット接続系に配置する情報の重要性を踏まえ、各端末（エンドポイント）でのセキュリティ対策や不正な挙動等を検知し、早期対処する仕組みを構築する必要がある。早期検知のための仕組みの構築には未知の不正プログラム対策（エンドポイント対策）の導入が有効である。エンドポイント対策は、従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらに、インシデント発生要因の詳細な調査を実施することで、検知、復旧等の早期対処を可能とする。

加えて、情報資産単位でのアクセス制御、監視体制や CSIRT など緊急時即応体制の整備、個々の職員のリテラシー向上など人的セキュリティ対策が必須となる。

また、 $\beta$ モデル又は $\beta'$ モデルを採用する場合は、従来モデル（ $\alpha$ モデル）と比較してインターネットからのリスクが増加し、より高度なセキュリティ対策の確実な実施が必要になることから、インターネット接続系と LGWAN 接続系を完全に分離する場合を除き、その実施について事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出することとする。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出することとする。なお、外部による事前確認や外部監査を行う者については、監査の対象となる情報資産に直接関与しない者であることが望ましい。

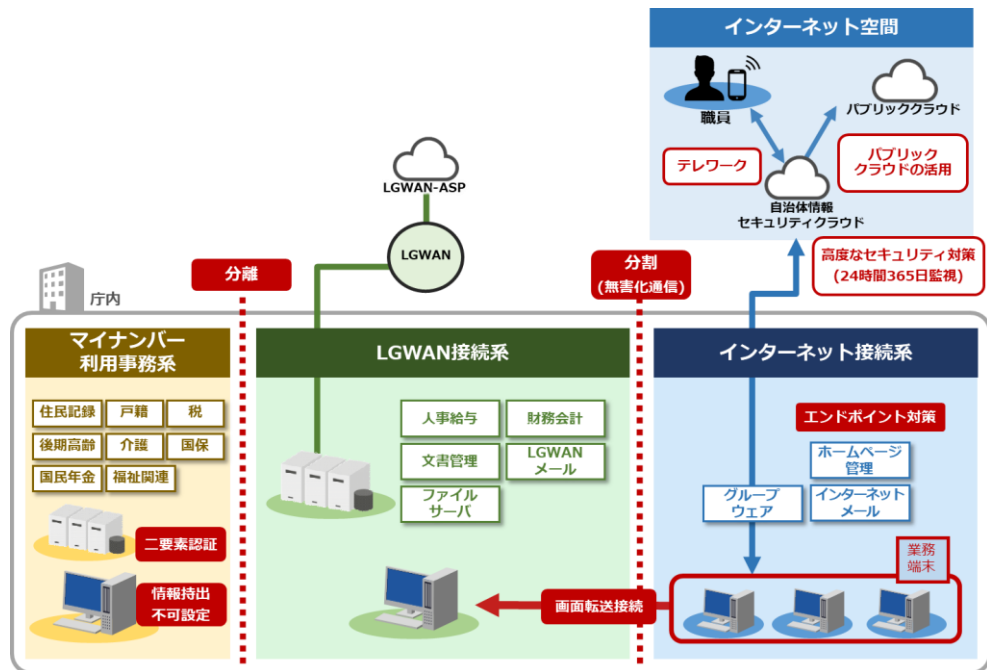
具体的には、以下の（ア）、（イ）のとおり、対策を実施しなければならない。

（ア） $\beta$ モデル：インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産は LGWAN 接続系に配置する方式

本モデルは、業務システムを LGWAN 接続系に残しつつ、業務端末及びグループウェア等をインターネット接続系に配置し、画面転送により LGWAN 接続系業務システムを利用できるようにしたモデルである。本モデルにおいては、以下の図表に記載された対策を講じなければならない。

対策区分	セキュリティ対策	概要
技術的対策	無害化処理	・ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認する方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。
	LGWAN接続系の画面転送	・インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 ・LGWAN接続系からインターネット接続系へのデータ転送(クリップボードのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。
	未知の不正プログラム対策(エンドポイント対策)	・従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。
	業務システムログ管理	・インシデントの兆候検知や、インシデント発生後の調査に使用するため、LGWAN接続系の業務システムのログの収集、分析、保管を実施する。
	脆弱性管理	・OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応する。
組織的・人的対策	組織的なセキュリティ対策基準の遵守	・インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。
	住民に関する情報をインターネット接続系に保存させない規定の整備	・住民の名簿など、住民の個人情報をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。
<p>本ガイドライン対策基準(例文)「1. 組織体制 (9) CSIRTの設置・役割」「5. 人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。</p> <ul style="list-style-type: none"> <li>・職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定</li> <li>・職員等の実践的サイバー防御演習(CYDER)の受講</li> <li>・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有</li> <li>・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し</li> </ul>		

図表 20 Bモデルにおける必須のセキュリティ対策について



図表 21 Bモデルイメージ図

(イ) B'モデル：インターネット接続系に主たる業務端末と重要な情報資産を配置する方式

本モデルは、Bモデルと同様に業務端末及びグループウェア等をインターネット接続系に配置し、さらに入札情報や職員の情報等重要な情報資産をインターネット接続系に配置するモデルである。本モデルにおいては、以下の図表に記載された対策を講じなければならない。

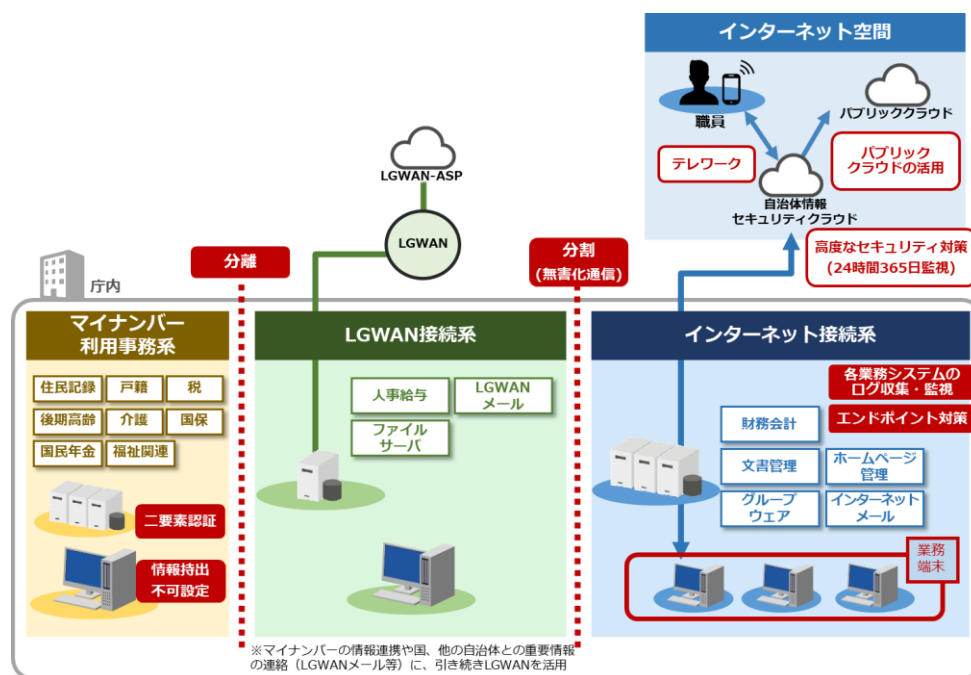
対策区分	セキュリティ対策	概要
技術的対策	無害化処理	・ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。
	LGWAN接続系の画面転送	・インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 ・LGWAN接続系からインターネット接続系へのデータ転送(クリップボードのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。
	未知の不正プログラム対策(エンドポイント対策)	・従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。
	業務システムログ管理	・インシデントの兆候検知や、インシデント発生後の調査に使用するため、業務システムのログの収集、分析、保管を実施する。
	情報資産単位でのアクセス制御	・情報資産の機密性レベルに応じて業務システム単位でのアクセス制御を行う。文書を管理するサーバ等は課室単位でのアクセス制御を必須とし、係単位でのアクセス制御は推奨とする。
	脆弱性管理	・OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応する。
組織的・人的対策	セキュリティの継続的な検知・モニタリング体制の整備	・標的型攻撃訓練や研修等の職員等の受講状況や結果を確認し、セキュリティ対策の浸透状況や効果を測定する。測定した結果をもとに改善につなげていく。
	組織的なセキュリティ対策基準の遵守	・インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。
	住民に関する情報をインターネット接続系に保存させない規定の整備	・住民の名簿など、住民の個人情報をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。
	情報セキュリティ研修、標的型攻撃訓練、セキュリティインシデント訓練の受講	・職員等は情報セキュリティ研修、標的型攻撃訓練を年1回以上受講する。また、情報システム管理者、情報システム担当者はセキュリティインシデントが発生した場合の訓練を年1回以上受講する。
	本ガイドライン対策基準(例文)「1. 組織体制 (9) CSIRTの設置・役割」「5. 人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 ・職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 ・職員等の実践的サイバー防衛演習(CYDER)の受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有 ・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し	

図表 22 B'モデルにおける必須のセキュリティ対策について

また、B'モデルについては、定期的な脆弱性診断、プラットフォーム診断等の実施が有効である。加えて、情報漏えいに対する対策として、以下の対策も有効である。

- ・万が一ファイルが外部に漏れいしても解読できないよう、データベースやファイルの暗号化

- ・組織が定義したポリシーに従ってデータへの操作を監視・制限し情報の流出を防止（Data Loss Prevention）
- ・組織が許可していない外部接続先のサービスへのアクセスを監視、遮断



図表 23 B'モデルイメージ図

（注 1 1）未知の不正プログラムへの対策（エンドポイント対策）

未知の不正プログラム対策として、OS のプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、その実行ファイル又は端末を隔離する方式があり、不審な挙動を示す端末のホスト名や IP アドレスなどの情報をログとして取得し、管理者へ通知する必要がある。なお、製品の導入だけでは未知の不正プログラムへの対策とはならない。監視体制や CSIRT との連携等、組織的な対策と合わせて検討が必要となることに留意する必要がある。

（4）その他のセキュリティ対策

①プリンタ・複合機の情報セキュリティ対策

プリンタ・複合機は、必要に応じてマイナンバー利用事務系、LGWAN 接続系、インターネット接続系のネットワーク毎に設置されることが望ましい。共有する場合においてもマイナンバー利用事務系又は LGWAN 接続系について、インターネット接続系と共有することは認められない。共有する場合には、1 台のプリンタ・複合機にネットワーク毎に専用の LAN ポートを設け、他の領域と分離された

通信を保証することが望ましい。それが困難である場合には、ネットワークの一方を LAN ポートに、もう一方は USB ポートにプリンタサーバを繋ぐなどの方法を検討する必要がある。

#### ②本庁・支所・出先機関間でのネットワーク通信

本庁、支所、出先機関でマイナンバー利用事務系と LGWAN 接続系を構築するネットワークは、原則としてインターネット回線ではなく閉域網を利用すること。インターネット回線を利用する場合、VPN 通信等を用いて、通信元と通信先が特定されており、通信経路が限定されるようにすること。

#### ③修正プログラム及びパターンファイルの更新

マイナンバー利用事務系及び LGWAN 接続系では、OS・アプリケーションの修正プログラム及びウイルス対策ソフトのパターンファイルの更新等においても、インターネットに接続して利用してはならない。LGWAN-ASP 等を利用して修正プログラム等を取得し適用することが望ましい。WSUS のファイル更新サーバ及びウイルス対策ソフトのパターンファイル更新サーバ等についても、マイナンバー利用事務系及び LGWAN 接続系からのインターネット接続は認められない。

#### ④自動交付機による証明交付

自動交付機による証明交付をしている場合、個人番号利用事務の範囲に限定しているのであれば自動交付機をマイナンバー利用事務系と分離する必要はない。

#### ⑤VPN 接続による外部との通信

遠隔での情報システム保守により、マイナンバー利用事務系及び LGWAN 接続系について VPN 接続による通信を許可する場合は、特定通信としての設定がされており、かつ IP-VPN 等の閉域網又は LGWAN で接続されなければならない。

#### ⑥J-ALERT 等の LGWAN 接続系とインターネット接続系の双方への接続が必要な情報システムへの対応

J-ALERT 等の LGWAN 接続系とインターネット接続系の双方への接続が必要な情報システムがある場合は、ファイアウォールを設置し、さらに特定通信としなければならない。あるいはデータベースのみを共用し、情報システムは LGWAN 接続系とインターネット接続系の各システムで別に設置する方法で実現してもよい。

#### ⑦インターネットメールによる障害通報

インターネット接続系についてはインターネットメールを利用してシステム障害通報を行ってもよい。マイナンバー利用事務系及び LGWAN 接続系については、特定サーバ間通信に限定した上で、LGWAN-ASP を活用することが望ましい。

#### ⑧アクセス記録を外部に提供する又は他団体からアクセス記録を受領する際、アクセス記録に個人情報が含まれる場合は、個人情報保護条例及び情報セキュリティ管理関係の規程に従わなければならない。

## 4. 物理的セキュリティ

### 4.1. サーバ等の管理

#### 【趣旨】

サーバ等のハードウェアは、情報システムの安定的な運用のために適正に管理する必要があり、管理が不十分な場合、情報システム全体に悪影響が及んだり、業務の継続性に支障が生じるおそれがある。このことから、サーバ等の設置や保守・管理、配線や電源等の物理的セキュリティ対策を規定する。

#### 【例文】

##### (1) 機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

##### (2) サーバの冗長化

①情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。【推奨事項】

②情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。【推奨事項】

##### (3) 機器の電源

①情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

##### (4) 通信ケーブル等の配線

①統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケー



ブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

④統括情報セキュリティ責任者及び情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

#### （５） 機器の定期保守及び修理

①情報システム管理者は、可用性 2 のサーバ等の機器の定期保守を実施しなければならない。

②情報システム管理者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、事業者へ故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

#### （６） 庁外への機器の設置

統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

#### （７） 機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

### （解説）

#### （１） 機器の取付け

情報システムで利用する機器は、温度、湿度等に敏感であることから、室内環境を整えることが必要である。

（注 1）機器の排気熱が、特定の場所に滞留しないよう室内の空気を循環させることにも注意する必要がある。熱が機器周辺に滞留すると機器内部が高温になり、緊急停止する場合がある。

#### （２） サーバの冗長化

サーバ等の機器が緊急停止した場合にも、業務を継続できるようにするために、

バックアップシステムを設置することが有効である。

(注2) ハードウェアやソフトウェアが二重に必要となるほか、運用面でデータの同期化等が必要となり、多額の費用を要するので、これらの費用とサーバ等の緊急停止による損失の可能性を検討した上で、冗長化を行うか否かを判断する必要がある。

### (3) 機器の電源

何らかの要因で電力供給が途絶し、機器が緊急停止した場合には、情報システムの機能が損なわれるおそれがある。これを避けるために、機器が適正に停止するまでの間電力を供給する予備電源を設ける必要がある。

(注3) 予備電源は、パソコン等に接続する小型のUPS（無停電電源装置）、蓄電池設備による給電を行うものや、自家発電機等様々な種類がある。また、これらの予備電源が緊急時に機能した場合に、現状どのくらい給電が行えるかを把握しておくべきである。例えば、1年前には、蓄電池設備により30分程度の電源供給ができていたものが、サーバの増設等により15分程度しか供給できなくなっている場合もある。このために、施設管理部門から予備電源が給電可能な時間等について定期的に確認しておくことが必要である。

### (4) 通信ケーブル等の配線

執務室に通信ケーブル等を配線する場合に、ケーブルを剥き出しにしたままにしておくと、踏まれるなどして損傷する可能性が高くなる。配線収納管等を利用し、通信ケーブル等の損傷を防ぐ必要がある。

### (5) 機器の定期保守及び修理

情報システムの安定的な運営のためには、定期的に保守を行うことが不可欠である。また、機器を修理に出す場合には、できる限り故障した部品を特定し、情報を消去できる場合は消去を行った上で引き渡すことにより、修理を委託する業者から情報が漏えいする可能性を低くしなければならない。内容を消去できないときは、守秘義務契約を締結するほか、秘密保持に関する体制や運用などが適正であることを確認しなければならない。

### (6) 庁外への機器の設置

庁外にサーバ等の機器を設置する場合には、十分なセキュリティ対策が実施されているか、定期的に確認する必要がある。

(注4) 委託事業者のデータセンターに、システム機器等を設置している場合は、定期的に物理的なセキュリティ状況を確認する必要がある。委託事業者を定期的に訪問し、定期報告では把握しきれない設置室内の状況の変化、当該委託事業者の要員の変化等を把握する。地方公共団体職員によるデータセンター内部への立入りがデータセンターのセキュリティポリシーに違反する等、委託事業者を訪問できない場合は、訪問調査に代えて第三者による情報セキュリティ監査報告書、委託事業者の内部監査部門による情報セキュリティ監査

報告書等によって確認する。

(7) 機器の廃棄等

情報システム機器が不要になった場合やリース返却等を行う場合には、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS 及び記憶装置の初期化（フォーマット等）による方法は、ハードディスク等の記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。また、原則として、以下の表に記載されている方法により、記録されている情報の機密性に応じて、情報システム機器の廃棄等を行わなければならない。なお、運用にあたっては、「情報システム機器の廃棄等時におけるセキュリティの確保について」（令和 2 年 5 月 22 日総行情第 77 号 総務省自治行政局地域情報政策室長通知）を参照されたい。

分類	機器の廃棄等の方法	確実な履行を担保する方法
<p>(1) マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ</p>	<p>当該媒体を分解・粉碎・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。</p> <p>なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。</p>	<p>職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等へ引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。</p>
<p>(2) 機密性2以上に該当する情報を保存する記憶媒体(上記(1)に該当するものを除く。)</p>	<p>一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。</p> <p>具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。</p>	<p>庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等へ引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。</p>
<p>(3) 機密性1に該当する情報を保存する記憶媒体</p>	<p>一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。</p> <p>具体的には、(2)に記述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。</p> <p>OS及び記憶装置の初期化(フォーマット等)による方法は、HDDの記憶演算子にはデータの記憶が残った状態となるため、適当ではない</p>	<p>庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。</p>
<p>※上記(1)は、オンプレミスの場合を想定したもの(ハウジングやプライベートクラウドを含む)</p>		

図表 24 情報の機密性に応じた機器の廃棄等の方法

## 4.2. 管理区域(情報システム室等)の管理

### 【趣旨】

情報システム室等は、重要な情報資産が大量に保管又は設置されており、特に厳格に管理する必要がある。情報システム室等が適正に管理されていない場合には、盗難、損傷等により重大な被害が発生するおそれがあり、このことから、情報システム室等の備えるべき要件や入退室管理、機器等の搬入出に関する対策を規定する。

ただし、対策によっては建物の改修を必要とするなど多額の費用を要するものもある。対策の実施に当たっては、費用対効果を考慮して行う必要がある。

### 【例文】

#### (1) 管理区域の構造等

- ①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。
- ②統括情報セキュリティ責任者及び情報システム管理者は、管理区域を地階又は1階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。【推奨事項】
- ③統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立ち入りを防止しなければならない。
- ④統括情報セキュリティ責任者及び情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。
- ⑤統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。【推奨事項】
- ⑥統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

#### (2) 管理区域の入退室管理等

- ①情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。
- ②職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。
- ③情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じ

て立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

- ④情報システム管理者は、機密性2以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

### (3) 機器等の搬入出

- ①情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託事業者を確認を行わせなければならない。
- ②情報システム管理者は、情報システム室の機器等の搬入出について、職員を立ち会わせなければならない。

## (解説)

### (1) 管理区域の構造等

情報システムの安定的な運営等のために、情報システム室や保管庫(磁気テープ等の保管庫)である管理区域の管理方法について定める。管理区域内には精密機器が多いことから、火災、水害、埃、振動、温度、湿度等への対策を講じる必要がある。

また、地方公共団体においては、多くの住民等の出入りがあることから、管理区域には施錠等を施し、監視カメラや認証機能等を活用して不正な者の入室を防止することが重要である。

(注1) ICカード等で扉を自動開閉制御している場合、サーバ室内で発生した火災等により、自動制御の扉が故障し開閉ができず、室内にいる要員が閉じ込められてしまう危険性がある。このような事態を回避するため、手動で扉を開閉できるように、平時から管理区域を管理している情報システム管理者が、自動扉開閉制御を解除するスイッチの場所を入室権限のある職員等に周知しておく必要がある。鍵等による立ち入り防止措置についても、同様である。

(注2) 管理区域に配置する消火薬剤は、発泡性のものを避けるべきである。また、情報システム機器等に水がかかる位置にスプリンクラーを設置してはならない。

(注3) 情報システム室内では機器等をサーバラックに固定した上で、管理権限の異なる複数のシステムが同一の室内に設置されている場合は、他システムの管理者による不正操作を回避するため、サーバラックの施錠管理を行うことが必要である。

### (2) 管理区域の入退室管理等

管理区域は情報資産の分類に応じて厳格な管理が行われなければならない。リスク評価を行って許可する範囲を検討し、入室できる者は許可された者のみに制限す

る。また、外部からの訪問者が管理区域に入室する場合、職員が付き添うとともに、訪問者であることを明示したネームプレートを着用させるなど外見上訪問者であることが分かるようにしておくべきである。また、情報漏えい等を回避するため、不要な電子計算機、モバイル端末、電磁的記録媒体等を管理区域に持ち込ませないことが重要である。

(注4) 入退室の記録簿は、事業者名、訪問者名等を記録する場合が多い。これらの記録簿に個人情報等を記述している場合は、紛失等が生じないように保管することが必要である。

### (3) 機器等の搬入出

搬入出に伴い外部の者が管理区域に立入る場合は、同行、立会いを行い、相手の行動を監視する必要がある。

(注5) 同行、立会いについては、原則として非常勤職員や臨時職員等ではなく、職員が行う必要がある。

### 4.3. 通信回線及び通信回線装置の管理

#### 【趣旨】

ネットワーク利用における通信回線及び通信回線装置が適正に管理されていない場合は、ネットワークそれ自体のみならず、ネットワークに接続している情報システム等に対しても損傷や不正アクセス等が及ぶおそれがある。このことから、外部ネットワーク接続等の通信回線及び通信回線装置の管理にセキュリティ対策を規定する。

#### 【例文】

- ①統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。
- ②統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。
- ③統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。
- ④統括情報セキュリティ責任者は、機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。
- ⑤統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。
- ⑥統括情報セキュリティ責任者は、可用性2の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

#### （解説）

庁内の通信回線は、施設管理部門が敷設・管理を行っていることが多く、統括情報セキュリティ責任者及び情報システム管理者は、ネットワークに関する工事を行う場合、施設管理部門と連携して実施する必要がある。庁舎内の通信回線敷設図、結線図等は、外部への漏えい等がないよう、厳重に管理しなければならない。

また、外部のネットワークへの不必要な接続は情報セキュリティ上の危険性が高まることから、接続は必要最低限のものに限定し、特に行政系のネットワークは、安全性の高い総合行政ネットワークに集約するように努めることが必要である。

通信回線として利用する回線は、当該システムで取り扱う情報資産の重要性に応じて、適正なセキュリティ機能を備えたものを選択することが必要であり、通信回線の性能低下や異常によるサービス停止を防ぐために、通信回線や通信回線装置を冗長構成にした



り、回線の種類を変えて複数の回線を構築しておくことが望ましい。また、庁内から外部に敷設する通信回線の管路についても、例えば異なる通信事業者による複数の経路で構築しておくこと、災害発生時の復旧にかかる時間が短縮されるなどの効果が期待される。

(注1) 図面管理を委託事業者に依頼する場合でも、当該委託事業者が紛失する場合に備えて、各地方公共団体で控えを保管しておくことが必要である。

#### 4.4. 職員等の利用する端末や電磁的記録媒体等の管理

##### 【趣旨】

職員等が利用するパソコン、モバイル端末及び電磁的記録媒体等が適正に管理されていない場合は、不正利用、紛失、盗難、情報漏えい等の被害を及ぼすおそれがある。このことから、これらの被害を防止するために、職員等の利用するパソコン、モバイル端末及び電磁的記録媒体等の盗難及び情報漏えい防止策、持ち出し・持ち込み等に関する対策を規定する。

##### 【例文】

- ①情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
- ②情報システム管理者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力が必要とするように設定しなければならない。
- ③情報システム管理者は、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用しなければならない。【推奨事項】
- ④情報システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。
- ⑤情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。【推奨事項】
- ⑥情報システム管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。【推奨事項】

##### (解説)

執務室等からパソコン、モバイル端末及び電磁的記録媒体等が盗難され、情報が漏えいする事例は多く、盗難を防止するための物理的措置が必要である。

また、各団体が保有しているパソコン、モバイル端末及び電磁的記録媒体等が盗難等に遭った場合でも、指紋又は顔等を用いた生体認証、パスワード等の設定、暗号化により使用できないようにしておくことで、情報が不正使用等される可能性を減らすことができる。特に、パソコン起動時のパスワード機能の利用と、電磁的記録媒体の暗号化の併用が情報の漏えいに対する有効な防止対策になる。また、次のパソコンの不正利用を防止するためのパスワード機能及び暗号化機能を活用することが必要である。

①ログインパスワード

OS やソフトウェアにログインする際に使用するパスワードであり、ログインパスワードによって、パソコンの多くの機能の不正利用を防御できる。

②多要素認証の利用

取り扱う情報の重要度等に応じて「知識」「所持」「存在」を利用する認証の手段のうち、二つ以上を併用する多要素認証を行うことによりセキュリティ機能が強化されることになる。多要素認証の詳細は、「3. 情報システム全体の強靱性の向上」を参照されたい。

③電源起動時のパスワード (BIOS パスワード)

パソコンを起動したときに、OS が起動する前に入力するパスワードであり、この BIOS パスワードの設定をしておくことで、オペレーティングシステムが自動起動しない。

④電源起動時のパスワード (ハードディスクパスワード)

ハードディスクパスワードを設定しておけば、不正利用を防御できる。ただし、ハードディスクパスワードについては、失念すると解除が不可能になる場合があるために留意する必要がある。

⑤セキュリティチップの暗号化機能

セキュリティチップを搭載したパソコン、モバイル端末及び電磁的記録媒体の場合は、暗号鍵が当該チップに記録されているために、ハードディスクの暗号化機能を利用することによって、ハードディスク装置を抜き取られても不正利用を防御できる。

⑥モバイル端末のセキュリティ

モバイル端末を庁外で業務利用する場合は、端末の紛失・盗難対策として、前述のように普段からパスワードによる端末ロックを設定しておくことが必要である。また、紛失・盗難に遭った際は、遠隔消去 (リモートワイプ) や自己消去機能により、モバイル端末内のデータを消去する対策も有効である。

なお、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めなければならない。

(注1) USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順には、以下の事項を含めることが望ましい。

- ・職員等は支給された外部電磁的記録媒体、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により外部の組織との間で取り決めた外部の組織から受け取った外部電磁的記録媒体を使用すること。
- ・外部の組織から受け取った外部電磁的記録媒体は、情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこ

れに情報を書き出す場合の安全確保のために必要な措置を講ずること。

(注2) 特にセキュリティ機能を強化する必要がある場合には、パスワードの流用等による悪用を防止するため、認証のために一度しか使えないワンタイムパスワードを使用することも考えられる。

(注3) ディスク装置を持たない形態のシンクライアント端末は、端末から情報が漏えいする可能性が非常に低くなることから、情報漏えい防止にも有効であり、導入する地方公共団体も出ている。ただし、シンクライアント端末の場合、サーバ、ネットワークに障害が生じると、業務ができなくなる可能性があることから、その場合の対応、特に災害時等の対応も考慮した上で導入を行う必要がある。

(注4) パソコン、モバイル端末、通信機器、ケーブル等からは、微弱電磁波が流れている。これらから流れる電磁波から、指向性の高いアンテナを利用して、情報を盗聴することが技術的には可能である。このため、機密性の非常に高い情報を取り扱う企業等では、電磁波により重要情報が外部に漏えいすることを防止する対策を実施することがある。この電磁波盗聴対策は、シールドルーム工事等、多額の費用を要するため、盗聴された場合のリスクを考慮した上で、実施の可否を判断する必要がある。

(注5) モバイル端末の遠隔消去（リモートワイプ）機能は、モバイル端末に電源が入っており、かつ通信状態が良好な場合にしか効果が期待できない点に留意する必要がある。このことから、本機能とあわせて、データを暗号化する等、漏えいしても内容が知られることのない仕組みを合わせて導入することが有効である。

## 5. 人的セキュリティ

### 5.1. 職員等の遵守事項

#### 【趣旨】

職員等が情報資産を不正に利用したり、適正な取扱いを怠った場合、コンピュータウイルス等の感染、情報漏えい等の被害が発生し得る。このことから、情報セキュリティポリシーの遵守や情報資産の業務以外の目的での使用の禁止等、職員等が情報資産を取り扱う際に遵守すべき事項を明確に規定する。職員だけでなく、非常勤職員、臨時職員及び委託事業者等についても、遵守事項を定めなければならない。

情報漏えい事案の多くが、職員等の過失又は故意による規定違反から生じており、職場の実態等を踏まえつつ、職員等の遵守事項を適正に定めるとともに、規程の実効性を高める環境を整備することが重要である。

#### 【例文】

##### (1) 職員等の遵守事項

###### ①情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

###### ②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

###### ③モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

(ア) CISO は、機密性 2 以上、可用性 2、完全性 2 の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

(イ) 職員等は、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

(ウ) 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

###### ④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ア) 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断を CISO が行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定め

る実施手順に従い、情報セキュリティ管理者の許可を得て利用することができる。

(イ) 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑧退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

(2) 非常勤及び臨時職員等への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び臨時職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び臨時職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び臨時職員等にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(3) 情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手

順を閲覧できるように掲示しなければならない。

(4) 委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を事業者が発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

(解説)

(1) 職員等の遵守事項

情報セキュリティを確保するために、情報セキュリティポリシー及び実施手順に定められている事項等、全ての職員が遵守すべき事項について定めたものである。

情報セキュリティ管理者は、異動、退職等により業務を離れる場合、職員等が利用している情報資産を返却させる。また ID についても、速やかに利用停止等の措置を講じる必要がある。

① モバイル端末の持ち出し及び外部における情報処理作業

情報の漏えいは、不正なモバイル端末の持ち出しや移動中にモバイル端末が盗難に遭うなどしたことが原因で発生するケースが多い。重要な情報資産を使って外部で作業する場合には、庁内の安全対策に加え、安全管理に関して追加的な措置を定めた上で、モバイル端末の持ち出しや外部での作業の実施については許可制とするのが適正である。

(注1) モバイル端末の持ち出しを許可した場合にも、モバイル端末は常に携帯することを職員等に周知する必要がある。特に交通機関（電車、バス、自家用車等）による移動時の携帯に際しては、紛失、盗難等に留意する必要がある。

(注2) 共用しているモバイル端末の持ち出しでは、管理者が不明確になりやすく、その結果として所在不明になりやすいので特に注意する必要がある。

(注3) 持ち出し専用パソコンによる情報の持ち出しにおいては、万一当該パソコンを紛失した場合に、記録されている情報を容易に特定するため、日常においては当該パソコンに情報を記録しないようにし、持ち出し時においては持ち出し情報が必要最小限であるかどうか確認を行った上で情報を記録し、返却時においては情報の完全削除をするといった運用を行う必要がある。

(注4) テレワーク等におけるセキュリティ対策については、「6.2. アクセス制御」を併せて参照されたい。

② 支給以外のパソコンやモバイル端末等の業務利用

自宅や庁外等での情報処理作業においては支給された端末を使用することとし、支給以外の端末の使用は原則禁止とする。

止むを得ず支給以外の端末を使用する場合は、以下のような対策を実施するこ

とが必要である。

- ・統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得る
- ・支給以外の端末のコンピュータウイルスチェックが実施されていることやファイル共有ソフトウェアの導入がされていないことを情報セキュリティ管理者が確認する
- ・パスワードによる端末ロック機能や遠隔消去機能などの要件を満たしていることを情報セキュリティ管理者が確認する
- ・機密性3の情報資産については支給以外の端末での作業を禁止とする
- ・支給以外の端末のセキュリティに関する教育を受けた者のみ使用を許可する
- ・無許可で行政情報等を記録、持ち出す行為を禁止する
- ・業務利用する必要がなくなった場合は、支給以外のパソコンやモバイル端末等から業務に関係する情報を削除する

(注5) 支給以外の端末の利用申請内容については、以下を含めること。

- ・申請者の氏名、所属、連絡先
- ・利用する端末の契約者の名義(スマートフォン等の通信事業者と契約を行う端末の場合)
- ・利用する端末の製造企業名、機種名、OSの種類及びバージョン
- ・利用目的、取り扱う情報の概要、機密性2以上の情報の利用の有無等
- ・主要な利用場所
- ・利用する主要な通信回線サービス
- ・利用する期間

(注6) 支給以外の端末から庁内ネットワークに接続を行う可能性がある場合は、利用者の機密情報の持出しを防ぐこと以外にも支給以外の端末のOS改造による脆弱性や不正なアプリケーションの利用による支給以外の端末の不正プログラム感染による情報漏えい等に留意する必要がある。また、支給以外の端末の盗難・紛失等による情報漏えいや不正アクセスのリスクにも注意が必要である。そのため、以下のような対策を講じ、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能の導入及び許可された端末や利用者であることを確認する仕組みの導入を行う必要がある。

- ・シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。
- ・ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。
- ・端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能



を設ける。

- ・上記のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける。
- ・ハードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設ける。
- ・端末の OS 改造の検知、私有領域へのデータのコピーの制御やアクセスログ取得等の機能を持つ MDM (Mobile Device Management)、MAM (Mobile Application Management) 等のソフトウェアを利用して支給以外の端末を管理する。
- ・電子証明書による端末認証や、接続する機器の IP アドレス、MAC アドレス等の認証情報を利用し端末を制限する機能及び多要素認証による利用者を識別・認証する機能を設ける。

また、支給以外のパソコン、モバイル端末及び電磁的記録媒体を情報システム室に持ち込むことは禁止する。

その他、職員等が講じるべき以下の事項を含む利用時の実施手順に係る安全管理措置をあらかじめ定め、情報セキュリティ管理者は職員に安全管理措置を講じさせなければならない。

- ・パスワード等による端末ロックの常時設定
- ・OS やアプリケーションの最新化
- ・不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）
- ・端末内の機密性 2 以上の情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある）
- ・市等提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）

また、以下を例とする禁止事項を遵守させなければならない。

- ・端末、OS、アプリケーション等の改造行為
- ・安全性が確認できないアプリケーションのインストール及び利用
- ・利用が禁止されているソフトウェアのインストール及び利用
- ・許可されない通信回線サービスの利用（利用する回線を限定する場合）
- ・第三者への端末の貸与

### ③持ち出し及び持ち込みの記録

庁内のパソコン、モバイル端末及び電磁的記録媒体の持ち出しや業務利用を許可された支給以外のパソコン、モバイル端末及び電磁的記録媒体の持ち込みについては現状把握や資産管理のためこれを記録する必要がある。

（注 7）記録簿に記録を作成する場合は、持ち出しの項目として、所属課室名、

名前、日時、持出物、個数、用途、持出の場所、返却日、管理者の確認等を設ける。

(注8) 持ち込みの項目としては、所属課室名、名前、日時、持込物、個数、用途、持込の場所、持ち帰り日、管理者の確認等を設ける。

(2) 非常勤及び臨時職員等への対応

情報セキュリティ管理者は、非常勤職員等の採用時に情報セキュリティポリシー等のうち守るべき内容を理解させ、必要に応じて情報セキュリティポリシーの遵守の同意書への署名を求める。また、パソコンやモバイル端末の機能は、非常勤職員等の業務内容に応じて、不必要な機能については制限することが適正である。

(3) 情報セキュリティポリシー等の掲示

職員等が情報セキュリティポリシーを遵守する前提として、イントラネット等に掲示する方法により、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるようにしなければならない。

(4) 委託事業者に対する説明

委託事業者の内部管理が不十分であることから、情報の漏えい等が発生する事例は多い。したがって、各地方公共団体が委託事業者（再委託事業者を含む。）等に情報システムの開発及び運用管理を委託する場合、情報セキュリティ管理者は、契約の遵守を求め、委託の業務範囲に従って、情報セキュリティポリシー及び実施手順に関する事項を説明する必要がある。

なお、業務委託については、「8. 業務委託と外部サービスの利用」を参照のこと。

## 5.2. 研修・訓練

### 【趣旨】

情報セキュリティを適正に確保するためには、情報セキュリティ対策の必要性と内容を幹部を含め全ての職員等が十分に理解していることが必要不可欠である。情報セキュリティに関する情報セキュリティインシデントの多くが、職員等の規定違反に起因している。情報セキュリティの向上は、利便性の向上とは、必ずしも相容れない場合があり、職員等の意識として業務優先で情報セキュリティ対策の軽視につながることもある。また、情報セキュリティに関する脅威や技術の変化は早く、職員等には常に最新の状況を理解させることが必要である。

また、実際に情報セキュリティインシデントが発生した場合に的確に対応できるようにするため、緊急時に対応した訓練を実施しておくことが必要である。

これらのことから、職員等に情報セキュリティに関する研修・訓練を行うことを規定する。

### 【例文】

#### (1) 情報セキュリティに関する研修・訓練

CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

#### (2) 研修計画の策定及び実施

①CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。

②研修計画において、職員等は毎年度最低1回は情報セキュリティ研修を受講できるようにしなければならない。【推奨事項】

③新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

④研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものに行なければならない。

⑤情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、統括情報セキュリティ責任者及び情報セキュリティ責任者に対して、報告しなければならない。

⑥統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、CISO に情報セ

セキュリティ対策に関する研修の実施状況について報告しなければならない。

⑦CISOは、毎年度1回、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

(3) 緊急時対応訓練

CISOは、緊急時対応を想定した訓練を定期的実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

(4) 研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

(解説)

(1) 情報セキュリティに関する研修・訓練

情報セキュリティに関する研修・訓練を実施する責任はCISOにあり、研修・訓練を定期的に行わなければならない。

(2) 研修計画の立案及び実施

CISOは、幹部を含めた全ての職員等が、情報セキュリティの重要性を認識し、情報セキュリティポリシーを理解し、実践するために、研修及び訓練を定期的かつ計画的に実施する必要がある。

(注1) 研修計画には、研修内容や受講対象者のほか、e-ラーニング、集合研修、説明会等の実施方法、時期、日程、講師等を盛り込む。

(注2) 部外の研修等に、職員等を参加させることも有益である。

情報セキュリティポリシーを運用する際、多くの部分は組織の責任者及び利用者の判断や行動に依存している。したがって、全ての職員等を対象に研修を行う必要がある。情報セキュリティに関する環境変化は早いことから、毎年度最低1回は研修を受講するようにすることが望ましい。

研修内容は、毎回同じ内容ではなく、情報セキュリティ監査の結果や庁内外での情報セキュリティインシデントの発生状況等を踏まえ、継続的に更新することや職員等が具体的に行動すべき事項を考慮することが望ましい。

新規採用の職員等に対しては、採用時に情報セキュリティ研修を行うことによって、情報セキュリティの大切さを深く認識させることができる。

また、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及び職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じた研修を実施することが必要である。これは不正アクセスから情報資産を防御することはもとより、不正プログラムの

感染、侵入、内部者による情報の漏えい、外部への攻撃等を防ぐ観点からも重要である。

研修受講を確実にするため、CISO に、毎年度 1 回、情報セキュリティ委員会に対して職員等の研修の実施状況を報告させなければならない。

また、CISO は、研修計画を通じて将来の情報セキュリティを担う人材の育成や要員の管理を行うとともに、地方公共団体の長によるメールでの周知等、研修効果を向上させる施策を講じることが望ましい。

なお、外部の専門家や内部の職員を最高情報セキュリティアドバイザー等として登用している場合は、それらの専門家等を内部教育に有効活用することも考えられる。

### (3) 緊急時対応訓練

実際に情報の漏えい等の情報セキュリティインシデントが発生した場合に、即応できる態勢を構築しておくため、緊急時を想定した訓練を定期的実施しなければならない。

(注3) 参考として受講が望まれる訓練等を以下に示すので、計画的な受講を推進されたい。

- ・実践的サイバー防御演習 (CYDER) : NICT ナショナルサイバートレーニングセンター主催
- ・インシデント対応訓練 (基礎/高度) : 地方公共団体情報システム機構主催
- ・分野横断的演習 : NISC 主催 (地方公共団体情報システム機構同時開催)

### (4) 研修・訓練への参加

幹部を含めた全ての職員に対し、研修・訓練に参加させることが情報セキュリティ確保にとって必要であることから、義務規定を設ける。

(注4) 教育・訓練の実施後、理解度試験等を行い、その有効性を評価し、次回の研修・訓練の改善に活用すれば、より効果を上げることができる。

(注5) 啓発や訓練を通じた各自治体の職員等のセキュリティ・リテラシーの向上として、地方公共団体情報システム機構主催の以下の研修等があるので、積極的に活用いただき、受講を推進されたい。また、自治体情報セキュリティクラウドに関して、都道府県が主催する演習・研修がある場合は、それらも積極的に受講する必要がある。

- ・リモートラーニングによるデジタル人材育成のための基礎研修 (e ラーニング)
- ・情報セキュリティ対策セミナー/情報セキュリティマネジメントセミナー (オンライン研修)
- ・専門 e ラーニング (専門・ICT 基礎/専門・ICT 中級)

### 5.3. 情報セキュリティインシデントの報告

#### 【趣旨】

情報セキュリティインシデントやその発生の予防が重要なことは言うまでもないが、完全な予防は事実上困難であることから、実際に情報セキュリティインシデントを認知した場合に、責任者に報告を速やかに行うことにより、被害の拡大を防ぎ、早期に回復を図れるようにしておく必要がある。このことから、情報セキュリティインシデントを認知した場合の報告義務について規定する。

なお、報告に対する対応については、「7.3. 侵害時の対応等」による。

#### 【例文】

##### (1) 庁内での情報セキュリティインシデントの報告

- ①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口へ報告しなければならない。
- ②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
- ③情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、CISO 及び情報セキュリティ責任者に報告しなければならない。

##### (2) 住民等外部からの情報セキュリティインシデントの報告

- ①職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。
- ②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
- ③情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じて CISO 及び情報セキュリティ責任者に報告しなければならない。
- ④CISO は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。【推奨事項】

##### (3) 情報セキュリティインシデント原因の究明・記録、再発防止等

- ①CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。
- ②CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速や

かに報告しなければならない。

- ③CSIRT は、情報セキュリティインシデントに関する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。
- ④CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。
- ⑤CISO は、CSIRT から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

(解説)

(1) 庁内からの情報セキュリティインシデントの報告

職員等は、情報セキュリティインシデントを認知した場合に、自らの判断でその情報セキュリティインシデントの解決を図らずに速やかに管理者に報告し、その指示を仰ぐことが必要である。その情報セキュリティインシデントによる被害を拡大しないためにも、報告ルート及びその方法を事前に定めておく必要がある。

(注1) CSIRT は、情報セキュリティインシデント発生時の対処手順のうち、意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等をあらかじめ定めておく必要がある。

(注2) CSIRT は、自組織において発生した情報セキュリティインシデントについて、報告・連絡を受ける情報セキュリティに関する統一的な窓口を設置し、情報セキュリティインシデント発生が報告された際に、CISO、総務省、都道府県等への報告手順を定めておく必要がある。

(注3) 情報セキュリティインシデント発生時の報告ルートは、団体の意思決定ルートと整合性を図ることが重要である。

(2) 住民等外部からの情報セキュリティインシデントの報告

住民からの報告が契機となって、重大な情報セキュリティインシデントの発見につながる場合等も想定されることから、当該報告、連絡を受ける窓口を設置する。

(注4) 住民からの報告に対しては、適正に処理し、必要に応じ対応した結果について、報告を行った住民等に通知する必要がある。

(3) 情報セキュリティインシデント原因の究明・記録、再発防止等

CSIRT は、報告された情報セキュリティインシデントについて評価を行い、情報セキュリティインシデントであると評価した場合は、CISO に速やかに報告することが必要である。さらに、被害の拡大防止等を図るための応急措置の実施及び復旧に係

る指示又は勧告を行う必要がある。

CSIRT は、情報セキュリティインシデントの原因を究明し、効果的な再発防止策を検討するために、情報セキュリティインシデントを引き起こした部門の情報セキュリティ管理者は、情報セキュリティインシデントの発生から対応までの記録を作成し、保存しておく必要がある。

(注5) 他部門も含めて同様の情報セキュリティインシデントの再発を防止するために全庁横断的に再発防止策を検討する必要がある。再発防止処置の策定については、「7.3. 侵害時の対応 (2) ④再発防止措置の策定」を参照されたい。



#### 5.4. ID 及びパスワード等の管理

##### 【趣旨】

情報システムを利用する際の ID 及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（IC カード等）の管理が適正に行われなかった場合は、情報システム等を不正に利用されるおそれがある。このことから、ID 及びパスワード等の管理に関する遵守事項を規定する。

認証情報等は、人的な原因により漏えいしやすい情報である。情報システム管理者からの認証情報等の発行から職員等での管理に至るまで、人的な原因で情報が漏えいするリスクを最小限にとどめる必要がある。

##### 【例文】

###### (1) IC カード等の取扱い

- ①職員等は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。
  - (ア) 認証に用いる IC カード等を、職員等間で共有してはならない。
  - (イ) 業務上必要のないときは、IC カード等をカードリーダー又はパソコン等の端末のスロット等から抜いておかななければならない。
  - (ウ) IC カード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。
- ②統括情報セキュリティ責任者及び情報システム管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。
- ③統括情報セキュリティ責任者及び情報システム管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

###### (2) ID の取扱い

- 職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。
- ①自己が利用している ID は、他人に利用させてはならない。
  - ②共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

###### (3) パスワードの取扱い

- 職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。
- ①パスワードは、他者に知られないように管理しなければならない。

- ②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
- ③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
- ④パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
- ⑤複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
- ⑥仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
- ⑦サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。
- ⑧職員等間でパスワードを共有してはならない（ただし、共用 ID に対するパスワードは除く）。

（解説）

（1） IC カード等の取扱い

認証のため、IC カードや USB トークン等の媒体を利用する場合は、情報のライフサイクルに着目し、利用、保管、返却、廃棄等の各段階における取扱い方法を定めておくことが必要である。

（2） ID の取扱い

ID の利用は本人に限定することを規定する。

また、共用 ID の利用は、業務上止むを得ない場合に限定する必要がある。その上で、止むを得ず共用 ID を利用する場合には、過去に遡って共用 ID の利用者を特定できるように記録・管理することが望ましい。

（3） パスワードの取扱い

パスワードの秘密を担保するため、想像しにくいパスワード設定（例えば、大文字及び小文字を組み合わせる、数字、アルファベット及び記号を組み合わせる等）、パスワードの共有禁止などを定める。

（注1）複数のシステムを取り扱う等により、複数の異なるパスワードが必要となる場合があるが、全てを覚えることの困難性から、安易なパスワードを数個使い回すといった運用が起こる可能性がある。

パスワードのメモを作成し、机上、キーボード、ディスプレイ周辺等にメモを置くことは禁止する必要があるが、特定の場所に施錠して保存する等により他人が容易に見ることができないような措置を講じていれば、メモの存在がパスワードの効果を削ぐものではないため、メモの作成を禁止するものではない。

## 6. 技術的セキュリティ

### 6.1. コンピュータ及びネットワークの管理

#### 【趣旨】

ネットワークや情報システム等の管理が不十分な場合、不正利用による情報システム等へのサイバー攻撃、情報漏えい、損傷、改ざん、重要情報の詐取、内部不正等の被害が生じるおそれがある。このことから、情報システム等の不正利用を防止し、また不正利用に対する証拠の保全をするために、ログの管理やシステム管理記録の作成、バックアップ、無許可ソフトウェアの導入禁止、機器構成の変更禁止等の技術的なセキュリティ対策を規定する。

#### 【例文】

##### (1) 文書サーバの設定等

- ①情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。
- ②情報システム管理者は、文書サーバを課室等の単位で構成し、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。
- ③情報システム管理者は、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

##### (2) バックアップの実施

統括情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

##### (3) 他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

##### (4) システム管理記録及び作業の確認

- ①情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

③統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、2名以上で作業し、互いにその作業を確認しなければならない。

(5) 情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

(6) ログの取得等

①統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(7) 障害記録

統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

(8) ネットワークの接続制御、経路制御等

①統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

(9) 外部の者が利用できるシステムの分離等

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

(10) 外部ネットワークとの接続制限等

- ①情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。
- ②情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。
- ③情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。
- ④統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。
- ⑤情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(11) 複合機のセキュリティ管理

- ①統括情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。
- ②統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。
- ③統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講じなければならない。

(1 2) IoT 機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(1 3) 無線 LAN 及びネットワークの盗聴対策

- ①統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。
- ②統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(1 4) 電子メールのセキュリティ管理

- ①統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。
- ②統括情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。
- ③統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。
- ④統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。
- ⑤統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めなければならない。
- ⑥統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置を講じなければならない。【推奨事項】

(1 5) 電子メールの利用制限

- ①職員等は、自動転送機能を用いて、電子メールを転送してはならない。
- ②職員等は、業務上必要のない送信先に電子メールを送信してはならない。
- ③職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
- ④職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

(16) 電子署名・暗号化

- ①職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。
- ②職員等は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また、CISO が定めた方法で暗号のための鍵を管理しなければならない。
- ③CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(17) 無許可ソフトウェアの導入等の禁止

- ①職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
- ②職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。
- ③職員等は、不正にコピーしたソフトウェアを利用してはならない。

(18) 機器構成の変更の制限

- ①職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。
- ②職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

(19) 業務外ネットワークへの接続の禁止

- ①職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。
- ②情報セキュリティ管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

(20) 業務以外の目的でのウェブ閲覧の禁止

- ①職員等は、業務以外の目的でウェブを閲覧してはならない。

②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

(2 1) Web 会議サービスの利用時の対策

①統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。

②職員等は、本市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

③職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

④職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

(2 2) ソーシャルメディアサービスの利用

①情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(ア)本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理 Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

(イ)パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

②機密性 2 以上の情報はソーシャルメディアサービスで発信してはならない。

③利用するソーシャルメディアサービスごとの責任者を定めなければならない。

④アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

⑤可用性 2 の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

(解説)

(1) 文書サーバの設定等

文書サーバは、複数の課室等で共用している場合が多いため、職員等が利用可能な容量を取り決める必要がある。また、複数の課室等で利用している場合には、アクセ



ス制御を行う必要がある。

(注1) 土木部門等では、静止画像を業務で利用するために大容量の蓄積容量を使用し、共用の文書サーバでは容量不足が生じ、専用のディスク装置を執務室等に設置している場合がある。このような場合には、専用のディスク装置に備わったセキュリティ機能を有効に活用するほか、物理的セキュリティ対策を実施する必要がある。

#### (2) バックアップの実施

緊急時に備え、ファイルサーバ等に記録される情報について、バックアップを取ることが必要である。

(注2) バックアップを行う場合には、データの保全を確保するため、バックアップ処理の成否の確認、災害等による同時被災を回避するためバックアップデータの別施設等への保管、システムを正常に再開するためのリストア手順の策定及びリストアテストによる検証が必要である。

(注3) バックアップはシステムの重要度に応じて、バックアップの取得間隔や遠隔地へのバックアップ保管の有無を決定しなければならない。

#### (3) 他団体との情報システムに関する情報等の交換

他団体との間で情報システムに関する情報及びソフトウェアを交換する場合は、その用途等を明確にして目的外利用や紛失、改ざん等が起こらないようにしなければならず、相手方の団体との間で当該内容を明記した合意文書を取り交わす等の対策を実施することが望ましい。

#### (4) システム管理記録及び作業の確認

情報システムに対して行った日常の運用作業については、記録を残しておくことが必要である。特に、システム変更等の作業を行った場合は、情報システムの現状を正確に把握するため、当該作業内容を記録し、詐取、改ざん等のないよう適正に管理しておくことが必要である。

また、システム変更等の作業を行う場合は、2人以上で確認を行い、設定ミス、プログラムバグ等によるシステム障害のリスクを減らさなければならない。

#### (5) 情報システム仕様書等の管理

情報システム及びネットワークに関する文書は、悪意を持つ者に攻撃材料として使われるおそれがあることから、機密性3相当の文書として扱い、業務上必要のある者以外が閲覧したり、紛失等が生じないように管理する必要がある。

#### (6) ログの取得等

ログ（アクセスログ、システム稼動ログ、障害時のシステム出力ログ）及び障害対応記録は、第三者等による不正侵入や不正操作等の情報セキュリティインシデントを検知するための重要な材料となる。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログ等は、事後の調査の過程で、問題を解明するた

めの重要な材料となる。したがって、情報システムにおいては、仕様どおりにログ等が取得され、また、改ざんや消失等が起こらないよう、ログ等が適正に保存されなければならない。目的や取得する機器の明確化のほか、取得後において定期的又は必要に応じて確認をしなければならない。また、ログは1年以上保管することが望ましい。なお、ログの保管期間については、システムが遵守すべき法令等によって定められている場合があるため、関係法令等を確認の上、決定する必要がある。

(注4) 保管期限を設定し、期限が切れた場合は、これらの記録を確実に消去する必要がある。

#### (7) 障害記録

システム障害への対応を決める際、過去に起きた類似障害が参考になるので、障害記録を適正に保存しておく必要がある。

(注5) 障害記録のデータベース化を図るなど、障害対応を決める場合に活用できるように保管しておくことが重要である。

#### (8) ネットワークの接続制御、経路制御等

ネットワーク上では、フィルタリング、ルーティング、侵入検知システム等が機能しているが、これらの機能を十分活用するため、ハードウェア及びソフトウェアの設定を適正に行うよう注意する必要がある。また、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

なお、クラウドサービスを利用し、住民情報等の重要な情報を外部のデータセンターとやり取りする場合は、VPN 接続による通信経路の暗号化や本人認証等の高度なセキュリティ対策を実施する必要がある。さらに、仮想ネットワークを構築する場合には、仮想ネットワークと物理ネットワークとの対応関係、仮想ネットワークの運用設定方針及び設定承認方針並びに庁内設備をクラウドサービスに移行する場合の注意事項等について確認し、適正な対策を講じる必要がある。

#### (9) 外部の者が利用できるシステムの分離等

電子申請受付システム、庁舎を訪問した住民等に対する庁舎案内システムなど、外部の者が利用できるシステムは、不正アクセス等を防御するため、必要に応じ、他のシステムのネットワークと切り離すなどの措置が必要である。

#### (10) 外部ネットワークとの接続制限等

インターネットに接続し、公開しているウェブサーバ等が、外部から攻撃を受けた場合に、庁内ネットワークへの侵入を可能な限り阻止するために、庁内と外部ネットワークの境界にファイアウォールを設置する必要がある。

(注6) このほか、非武装セグメントを設け公開サーバを接続すると有効である。

また、非武装セグメントに接続している公開サーバについて、不要なポートの閉鎖、不要なサービスの無効化、エラーメッセージの簡略化(攻撃者に対して、システムの技術情報を過度に表示し、与えない対策)を実施することによって、

防御能力を高めることができる。

(1 1) 複合機のセキュリティ管理

(注7) プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器を「複合機」という。複合機は、庁内ネットワークや公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定されることに注意が必要である。

(1 2) IoT 機器を含む特定用途機器のセキュリティ管理

テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているものを「特定用途機器」という。これらの機器についても当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により想定される脅威に注意が必要である。例えば、テレビ会議システム、IP 電話システム等は組織等 LAN を経由してインターネットに接続されて利用されることが想定され、その場合外部からの攻撃対象となり得る。これらの IoT 機器等の脆弱性がサイバー攻撃の標的となることが懸念される。また、内蔵電磁的記録媒体を備える場合は、運用終了時に内蔵電磁的記録媒体に残された情報が漏えいするおそれがある。そのため、特定用途機器の特性に応じて、以下の対策を講じる必要がある。

- ・特定用途機器について、認証情報を初期設定から変更した上で、適切に管理する。
- ・特定用途機器にアクセスする主体に応じて必要な権限を割り当て、管理する。
- ・特定用途機器が備える機能のうち利用しない機能を停止する。
- ・インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットやインターネットに接点を有する情報システムに接続しない。
- ・特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。
- ・特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。
- ・特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。
- ・特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消する。

(注8) IoT 機器に関するセキュリティ対策については、「IoT セキュリティガイ

ドライン ver 1.0」(平成 28 年 7 月 IoT 推進コンソーシアム 総務省 経済産業省)を参照されたい。

#### (1 3) 無線 LAN 及びネットワークの盗聴対策

無線 LAN を利用する場合は、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防御する必要がある。特に、LGWAN 接続系で無線 LAN を利用する場合は、盗聴及びなりすましアクセスポイント (AP) などによる情報漏えいや不正アクセスに対して、認証サーバを利用した WPA2/WPA3 エンタープライズによる認証 (IEEE802.1X 認証) を採用する等、セキュリティ対策を実施しなければならない。遵守すべきセキュリティ要件は、「庁内無線 LAN のセキュリティ要件について」を参照されたい。なお、マイナンバー利用事務系においては、無線 LAN は利用しないこととしなければならない。

(注 9) 暗号化方式の 1 つである WEP (Wired Equivalent Privacy) /WPA (Wi-Fi Protected Access) については、既に脆弱性が公知となっているため、暗号強度が確認されている暗号方式 (WPA2/WPA3) を採用しなければならない。

(注 1 0) アクセスポイントの管理者パスワードを適切に設定 (強固な ID・パスワードの設定、アクセスポイント単位での管理など) を行うとともに、無線端末間の通信が行われないよう適切な設定を行わなければならない。また、無線 LAN の不正利用調査を行い、探査ツール等を用い、無許可のアクセスポイントや使用されていないアクセスポイントが設置されていないことを点検することも有益である。

#### (1 4) 電子メールのセキュリティ管理

メールサーバに対するセキュリティ対策等、電子メールのセキュリティ管理について定める。外部からの電子メール受信及び外部への電子メール送信においてなりすましを防ぐため、メールサーバのセキュリティ対策として電子署名を用いた DKIM (DomainKeys Identified Mail) や SPF (Sender Policy Framework) 等の対策を実施するとともに、DMARC (Domain-based Message Authentication, Reporting & Conformance) も実施しなければならない。また、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、SMTP によるサーバ間通信を TLS による保護や、S/MIME 等の電子メールにおける暗号化及び電子署名の技術の利用等、電子メールのサーバ間通信の暗号化の対策を講ずることも考えられる。

加えて、電子メールの不正な中継を行わないようにメールサーバを設定しなければならない。外部へ情報を持ち出すために電子メールが用いられることを考慮し、フィルタリングソフトウェア等による監視を実施することが望ましい。

中継処理の禁止は、メールサーバが踏み台となり他のサーバに攻撃を行うことを防止するために必要がある。

職員等が電子メールの送信等により情報の外部への不正な持ち出しをしていないか監視するためには、フィルタリングソフトウェア等を利用する。

(注1 1) 上司など指定した職員に同報しなければ、送信できないように設定し、外部への持ち出しを牽制する方法もある。

(注1 2) 電子メールの送信に使われる通信方式の1つである SMTP (Simple Mail Transfer Protocol) では、差出人のメールアドレスを誰でも自由に名乗ることができるため、送信者のアドレス詐称(なりすまし)が容易にできる問題がある。このため、電子メールのなりすまし対策として、「送信ドメイン認証技術」を採用しなければならない。なお、送信ドメイン認証技術については、「送信ドメイン認証技術導入マニュアル」(迷惑メール対策推進協議会)を参照されたい。

(注1 3) 職員等は、庁外に電子メールにより情報を送信する場合は、当該電子メールのドメイン名にあらかじめ指定された「lg.jp」ドメイン名を使用することが望ましい。ただし、当該庁外の者にとって、当該職員等が既知の者である場合は除く。

(注1 4) 受信した電子メールをテキスト形式で表示するメールソフトの機能を有効化することによって、マルウェア感染の可能性の低減を図ることができる。

#### (1 5) 電子メールの利用制限

職員等が電子メールを利用する際の取扱いについて規定したものである。不正な情報の持ち出しを防止する観点から、電子メールの自動転送を禁止する。

プロバイダーが提供するサービスである、電子メールやオンラインストレージサービスに対しては、外部への不正な情報の持ち出し等に利用される場合があることから、適正なセキュリティ対策を講じる必要がある。

複数の送信先に電子メールを送る場合、他の送信先の電子メールアドレスが分からないようにするには、宛先や CC ではなく、BCC に送信先を入力する方法がある。

#### (1 6) 電子署名・暗号化

職員等が自由に暗号方法を利用すると、暗号鍵を紛失した場合に、復号が困難になり、データ自体が完全に破壊されたのと同じ状態になってしまうため、暗号方法は組織として特定の方法を定める必要がある。

その方法について情報システム管理者は、暗号技術検討会及び関連委員会(CRYPTREC)により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システム及び電子署名のアルゴリズム並びにそれを使用した安全なプロトコル及びその運用方法について、定めなければならない。

また、署名検証者が電子署名を検証するための電子証明書を信頼できる機関からダウンロードできる環境を整備したり、電子署名の付与を行う情報システム管理者

から電磁的記録媒体等で入手できる体制を整備する必要がある。暗号化された情報の復号又は電子署名の付与に用いる鍵の管理手順として、鍵のライフサイクルを考慮した管理手順を策定することが望ましい。

なお、電子署名を行うに当たっては、地方公共団体組織認証基盤(LGPKI : Local Government Public Key Infrastructure) の利用など、目的に応じた適切な公開鍵基盤を使用するように定めること。

#### (17) 無許可ソフトウェアの導入等の禁止

インターネットからソフトウェアをダウンロードし、パソコンやモバイル端末に導入すると、不正プログラムの感染、侵入の可能性が高まることや、導入済みのソフトウェアに不具合が発生する場合もあり、許可を得ない導入は禁止する必要がある。また、不正にコピーしたソフトウェアは、ライセンス違反や著作権法違反となることから、明確に禁止しなければならない。なお、許可を得てインターネットからソフトウェアをダウンロードする場合においても、提供元のサイト等の信頼性が確保できることを確認した上で入手する必要がある。

(注15) あらかじめ、一定のソフトウェアを指定して、その範囲では個別の許可を不要とする運用もあり得る。

#### (18) 機器構成の変更の制限

職員等が、メモリ増設等の際に静電気を発生させるなど、パソコンを故障させたり、ネットワーク全体にも悪影響を及ぼす可能性があり、許可を得ない構成変更は禁止する必要がある。

#### (19) 業務外ネットワークへの接続の禁止

セキュリティ上、ネットワークとの接続には適正な管理が必要であることから、無許可での接続を禁止する。あわせて、接続が許可されたものであることを確認するための措置を講じるとともに、許可手続を定める必要がある。(支給以外の端末を接続する場合も同様とする。)

(注16) 庁外の通信回線に接続した支給以外の端末を庁内の通信回線に接続することの許可手続として、以下を含む手続を規定し、職員等に遵守させること。

- ・利用時の許可申請手続
- ・手続内容(利用者、目的、利用する情報、端末等)
- ・利用期間満了時の手続
- ・庁内通信回線への接続時の手続(端末の事前検疫等)
- ・許可権限者(情報セキュリティ管理者)による手続内容の記録

(注17) 特に、庁内で無線LANを使用している場合に、職員等や委託事業者がパソコンやモバイル端末等を持ち込み、無許可でアクセスポイントへ接続する行為を禁止する必要がある。

#### (20) 業務以外の目的でのウェブ閲覧の禁止

業務外の外部サイトを閲覧している場合、不正プログラムの感染、侵入の可能性が高まるため、業務以外の目的でのウェブ閲覧は禁止しなければならない。また、閲覧先サイトのサーバにドメイン名等の組織を特定できる情報がログとして残ることにより、外部から指摘を受けるようなことがあってはならない。統括情報セキュリティ責任者は、業務外での閲覧を発見した場合は、情報セキュリティ管理者に通知し、対応を求めなければならない。

## (2 1) Web 会議サービスの利用時の対策

職員等は、Web 会議サービスの利用に当たり、以下の情報セキュリティ対策を実施する必要がある。

- ・原則として、自組織から支給された端末を利用すること。
- ・原則として、自組織で許可された Web 会議サービスを利用すること。
- ・利用する Web 会議サービスのソフトウェアが、最新の状態であることを確認すること。
- ・機密性 2 以上の情報を取り扱う場合は、可能な限りエンドツーエンド (E2E) の暗号化を行うこと。
- ・機密性 2 以上の情報を取り扱う場合は、Web 会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、E2E の暗号化を利用できなくなる機能を可能な限り使用しないこと。
- ・音声を扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意すること。

また、職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう以下の情報セキュリティ対策を講ずる必要がある。

- ・会議室にアクセスするためのパスワード等をかける。
- ・会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知する。
- ・待機室を設けて参加者と確認できた者だけを会議室に入室させる。
- ・なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させる。

(注 1 8) Web 会議サービスを利用する場合、Web 会議サービスのソフトウェアで録画等を防止する設定を行っていても、ビデオカメラで撮影されれば会議内容は保存されるため、会議内容は会議の参加者に保存されることを前提として、会議で取り扱う情報を確認する必要がある。

(注 1 9) Web 会議サービスでは音声・映像、参加者のメールアドレス等の属性等様々な個人情報を取り扱うことが考えられるため、Web 会議に招待される場合は、原則として、許可された Web 会議サービスを利用する。止むを得ず自組織で許可されていない Web 会議サービスに招待される場合は、サービスの利用は

あくまでも限定的な利用とする。具体的には、機密性 2 以上の情報を含んだチャットへの書き込みや資料共有を行わないなど、情報を保存させないように利用手順を定める必要がある。

(注 2 0) Web 会議サービスのセキュリティ対策については、「Web 会議サービスを使用する際のセキュリティ上の注意事項」(2020 年 7 月 14 日 IPA (独立行政法人 情報処理推進機構)) を併せて参照されたい。

## (2 2) ソーシャルメディアサービスによる情報発信

①情報セキュリティ管理者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定めること。

(ア) アカウント運用ポリシー (ソーシャルメディアポリシー) を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている自組織の Web サイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。

(イ) URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。

②情報セキュリティ管理者は、自組織のアカウントによる情報発信が実際のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定めること。

(ア) 自組織からの情報発信であることを明らかにするために、自組織のドメイン名を用いて管理している Web サイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

(イ) 自組織からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、自組織が運用していることを利用者に明示すること。

(ウ) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている自組織の Web サイト上のページの URL を記載すること。

(エ) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント (公式アカウント)」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

③情報セキュリティ管理者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止す



るために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定めること。

- (ア) パスワードを適切に管理すること。具体的には、ログインパスワードには十分な長さとし、複雑さを持たせた容易に推測されないものを設定するとともに、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。
  - (イ) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。
  - (ウ) ソーシャルメディアへのログインに利用する端末を紛失した又は当該端末が盗難に遭った場合は、当該端末を悪用され、アカウント乗っ取りの可能性があるため、当該端末の管理を厳重に行うこと。
  - (エ) ソーシャルメディアへのログインに利用する端末が不正アクセスされた場合、当該端末が不正に遠隔操作される又は、当該端末に保存されたパスワードが窃取される可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。
- ④情報セキュリティ管理者は、なりすましや不正アクセスを確認した場合の対処として、以下を含む対処手順を定めること。
- (ア) 自己管理 Web サイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行うとともに、信用できる機関やメディアを通じて注意喚起を行うこと。
  - (イ) アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理 Web サイト等で周知を行うとともに、自組織のエスカレーションルールに従い報告すること。

## 6.2. アクセス制御

### 【趣旨】

情報システム等がアクセス権限のない者に利用できる状態にしておくと、情報漏えいや情報資産の不正利用等の被害が発生し得る。そこで、アクセス制御を業務内容、権限ごとに明確に規定しておく必要がある。また、不用意なアクセス権限付与による不正アクセスを防ぐために、アクセス権限の管理は統括情報セキュリティ責任者及び情報システム管理者に集約することが重要である。

このことから、利用者登録や特権管理等を用いた情報システムへのアクセス制御、ログイン手順、接続時間の制限等不正なアクセスを防止する手段について規定する。

また、働き方改革実行計画（平成 29 年 3 月 28 日 働き方改革実現会議決定）により、柔軟な働き方に対応しやすい環境整備が求められているところ、職員等が業務を遂行する上で、必ずしも勤務庁舎に出勤する必要はなく、自宅やサテライトオフィス等から遠隔で業務を遂行する形態への対応が求められることとなった。また、大規模感染症の感染予防対策として、勤務庁舎への出勤が抑制されるような状況下では、大半の職員等が勤務庁舎以外から業務を遂行できるようにテレワーク環境の整備が必要となり、その実施に必要な対策についても解説する。

### 【例文】

#### (1) アクセス制御等

##### ①アクセス制御

統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

##### ②利用者 ID の取扱い

(ア) 統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

(イ) 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

(ウ) 統括情報セキュリティ責任者及び情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

##### ③特権を付与された ID の管理等

(ア) 統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特

権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

(イ) 統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、CISO が認めた者でなければならない。

(ウ) CISO は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

(エ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。

(オ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

(カ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

## (2) 職員等による外部からのアクセス等の制限

①職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

②統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。

い。

⑦統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、止むを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

(3) 自動識別の設定

統括情報セキュリティ責任者及び情報システム管理者は、ネットワークで 사용되는機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。【推奨事項】

(4) ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

(5) 認証情報の管理

①統括情報セキュリティ責任者又は情報システム管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

②統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

③統括情報セキュリティ責任者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

(6) 特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

(解説)

(1) アクセス制御

管理者権限（サーバ等の全ての機能を利用できる権限）等の特権は、全ての機能を利用可能にするので、利用者登録を厳格に行うとともに、特権で利用する ID 及びパスワードを厳重に管理する必要がある。

情報システムの管理者とデータベースの管理者を別にすることが望ましい。データベースに対するアクセス管理、データの暗号化、脆弱性対策の実施と、管理権限の不適切な付与の検知について措置を講じることが望ましい。

アクセス制御の要件を定めるにあたっては、必要に応じて、以下を例とするアクセス制御機能の要件を定めることが望ましい。

- a) 利用時間や利用時間帯によるアクセス制御
- b) 同一主体による複数アクセスの制限
- c) IP アドレスによる端末の制限
- d) ネットワークセグメントの分割によるアクセス制御

(注1) 委託事業者が利用する場合にも、ID 及びパスワードの利用については、全て統括情報セキュリティ責任者及び情報システム管理者が管理しなければならない。

(注2) 管理者権限等の特権の悪用を防ぐために、「セキュア OS」(これまでの OS では対応できなかったアクセス制御を実施し、セキュリティ強化を図る機能)を利用することが考えられる。セキュア OS は、「強制アクセス制御」及び「最小特権」の機能に特徴がある。

強制アクセス制御	特権の操作に対しても、情報へのアクセス制御を実施させる機能
最小特権	特権の ID を利用できる者でも、強制アクセス制御機能で必要最小限のアクセスしか認めない機能

(注3) ファイルベースでのアクセス制御を行うことも考えられる。その場合には、ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能とすることをアクセス制御機能の要件とすることが望ましい。

(2) 職員等による外部からのアクセス等の制限

外部から社内ネットワークや情報システムに接続を認める場合は、外部から攻撃を受けるリスクが高くなることから、本人確認手段の確保、通信途上の盗聴を防御するために、原則、安全な通信回線サービスを利用しなければならない。その際、通信する情報の機密性に応じて、ファイル暗号化、通信経路の暗号化、専用回線の利用等の必要な措置を実施することが求められる。また、接続に当たっては許可制とし、許

可は必要最小限の者に限定しなければならない。

職員等がテレワークにより庁内ネットワークや情報システムに接続を認める場合、情報資産の重要性を踏まえて対象となる資産を明確化し、テレワーク等で扱うことができる情報資産やテレワーク実施時の情報セキュリティ対策について規則を整備するとともに、外部からの不正な通信、マルウェアによる情報漏えいを防ぐためにアクセス制御等の技術的対策を行うことが求められる。また、なりすまし、情報漏えい及び盗難・紛失といったリスク等を踏まえ、取り扱う情報の重要度を勘案しつつ、適切なセキュリティ対策を講じる必要がある。なお、マイナンバー利用事務系は、住民情報等の特に重要な情報資産が大量に配置されており、情報漏えいリスクが高いこと等を踏まえ、テレワークの対象外としなければならない。

(LGWAN 接続系のテレワークを認める場合のセキュリティ対策について)

LGWAN 接続系の情報資産には、職員の個人情報等重要な情報資産が配置されている。テレワークにおいては、情報資産の重要性を踏まえ、取り扱う情報資産を明確にする必要がある。また、取り扱う情報の重要性に応じて、テレワークの実施可否の規則を整備するとともに、アクセス制御等の技術的対策を行わなければならない。なお、大量又は機微な住民情報を扱う業務がある場合、庁舎と同等の物理的な対策がなされたサテライトオフィスでの場合を除き、テレワークの対象外とすることが適当である。

また、以下のリスクとセキュリティ対策の方向性のとおり、適切なセキュリティ対策を行わなければならない。

リスク		概要	対策の方向性
①なりすまし		悪意のある第三者の ID・パスワードの窃取等により、庁内システムが不正アクセスされるリスク	許可された端末・職員のみ可能となるよう認証の仕組みの整備
②漏えい (盗聴・改ざん等)	通信	インターネット上で、悪意のある第三者に通信内容を傍受されるリスク	通信回線は、閉域網を使用する等、安全な接続方式を採用
	データ	不正アクセスにより、データを窃取／改ざんされるリスク	端末内での業務データ非保持(端末仮想化等)、端末データの暗号化等、第三者による端末の操作・データ窃取の防止や被害拡大を防ぐ仕組みの整備
③盗難/紛失		端末の盗難・紛失により、情報漏洩するリスク	盗難／紛失時に端末内の情報をリモートで管理できる仕組みの整備

リスク	概要	対策の方向性
④不正利用	利用者が故意又は過失により、システムを不正に利用することに起因するリスク 例) 権限を持たない第三者による不正なアクセスフリーソフト等許可されていないアプリケーションに起因したウイルス感染	権限に応じた情報へのアクセス制限、ポリシーの一元管理 業務に不要なアプリケーション導入の制限 操作ログの収集・管理
⑤不正持ち出し	利用者が故意又は過失により、不正なデータ持ち出しを行うリスク 例) 外部記録媒体などを用いたデータ不正持ち出し	端末に対する記録媒体の接続制限
⑥脆弱性・マルウェア	OS やソフトウェアの脆弱性を利用した攻撃により、端末がウイルスに感染するリスク 感染端末がセキュリティホールとなり、庁内のサーバや端末等に不正アクセスやウイルス感染を引き起こすリスク	端末の OS/ソフトウェアの適切なプログラム更新、パターンファイルの最新化 ネットワークのセキュリティ対策の実施
※上記リスクのうち①～③がリモートアクセス特有のリスク		

図表 25 テレワークにおけるリスクと対策の方向性

具体的には、以下のモデルを採用し、各モデルを導入する際は、「新型コロナウイルスへの対応等を踏まえた LGWAN 接続系のテレワークセキュリティ要件について」（令和 2 年 8 月 18 日総行情第 111 号 総務省自治行政局地域情報政策室長通知）にある技術要件を遵守しなければならない。

インターネット回線を使用しないモデル：

- ・閉域 SIM による接続サービスを利用するモデル

インターネット回線を使用するモデル：

- ・LGWAN-ASP サービスを利用して庁内にある LGWAN 接続系の端末に接続するモデル

- ・インターネット接続系を経由して LGWAN 接続系の端末に接続するモデル

（注 4）テレワークのセキュリティ対策については、「テレワークセキュリティガイドライン（第 5 版）」（令和 3 年 5 月 総務省）を併せて参照されたい。

（注 5）持ち込んだモバイル端末を確認するシステムとして、検疫システムがある。

検疫システムとは、OS のパッチやコンピュータウイルス対策ソフトウェアのパターンファイルが最新でない、不正プログラムが侵入しているなど、十分なセキュリティ対策が実施されていないモバイル端末を庁内ネットワークに接続させないシステムである。モバイル端末を庁内に持ち帰った場合等に、検疫システムによる確認を義務付けることにより、様々な脅威の発生を防止する。

(注6) 庁外から庁内のネットワークや情報システムにアクセスする際に公衆無線 LAN 等の庁外通信回線を利用することは原則禁止であるが、止むを得ず利用する場合は、統括情報セキュリティ責任者の許可を得た上で、必要最小限の範囲のみのアクセスとする。さらに、ログを取得し、不正なアクセスがないかを定期的に確認することが求められる。

(注7) 画面ののぞき見や盗聴を防止できるような環境を選定することで情報の漏えい対策につながる。また、テレワーク実施時の離席時の端末等の盗難に注意する。

(注8) 統括情報セキュリティ責任者及び情報システム管理者は、テレワーク実施時の情報セキュリティ対策を確実に実施させるため、端末に情報を保存させない等のチェックすべき項目を定め、テレワーク実施前及び実施後に、職員等に当該チェックを実施させること。

### (3) 自動識別の設定

ネットワークに不正な機器の接続を防止するために、電子証明書による端末認証や、接続する機器の IP アドレス、MAC アドレス等の認証情報を利用し制限する必要がある。

### (4) ログイン時の表示等

ソフトウェアに、ログイン試行回数の制限や、直近に使用された日時が表示される機能等がある場合は、それらを有効に活用し、不正にパソコン等の端末が利用されないようにする必要がある。

### (5) 認証情報の管理

認証機能として、指紋又は顔等を利用した生体認証、スマートカードを利用した認証及びパスワード認証等が存在する。認証の機能は、ソフトウェアにより様々な認証機能があるために、これらの機能を有効に利用することが求められる。認証機能を利用するにあたり、認証情報を不正利用から保護する必要があり、オペレーティングシステム等で認証に関する設定のセキュリティ強化を行わなければならない。認証情報の管理について、以下の点に注意する必要がある。

- ①パスワード認証を利用する際は情報システム間で同一パスワードの使い回しを行ってはならない。
- ②スマートカードを利用する際は紛失時に直ちにそのカードを無効化する等の処置を講じなければならない。
- ③利用者が認証情報を変更する際に、以前に設定した認証情報の再設定を防止する機能を実装することが望ましい。
- ④利用者が情報システムを利用する必要がなくなった場合は、ID の無効化や認証情報の廃棄等、当該利用者の ID や認証情報の不正な利用を防止するための措置を講じなければならない。



利用するパスワードの機能は、「5.4. ID 及びパスワード等の管理」に記載されているパスワードの取扱いに従い、パスワードを設定する必要がある。

(6) 特権による接続時間の制限

管理者権限等の特権を利用している際に、システムにログインしたままで端末を放置しておく、他者に不正利用されるおそれがあることから、システムの未使用時には自動的にネットワーク接続を終了するなどの措置を講じる必要がある。

### 6.3. システム開発、導入、保守等

#### 【趣旨】

システム開発、導入、保守等において、技術的なセキュリティ対策が十分に実施されていない場合は、プログラム上の欠陥（バグ）によるシステム障害等により業務に重大な支障が生じるおそれがある。このことから、システム開発、導入、保守のそれぞれの段階における対策を規定する。なお、本規定にはシステムの更新又は統合時の十分な検証等も含まれる。

#### 【例文】

##### (1) 情報システムの調達

- ①統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。
- ②統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

##### (2) 情報システムの開発

- ①システム開発における責任者及び作業者の特定  
情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。
- ②システム開発における責任者、作業者の ID の管理
  - (ア) 情報システム管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。
  - (イ) 情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。
- ③システム開発に用いるハードウェア及びソフトウェアの管理
  - (ア) 情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。
  - (イ) 情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

##### (3) 情報システムの導入

- ①開発環境と運用環境の分離及び移行手順の明確化

(ア) 情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。【推奨事項】

(イ) 情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

(ウ) 情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実にいき、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(エ) 情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

## ②テスト

(ア) 情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

(イ) 情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(ウ) 情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

(エ) 情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

## (4) システム開発・保守に関連する資料等の整備・保管

①情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

## (5) 情報システムにおける入出力データの正確性の確保

①情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力除去する機能を組み込むように情報システムを設計しなければならない。

②情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(6) 情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

(7) 開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(8) システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

(解説)

(1) 情報システムの調達

情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、情報システムのライフサイクルで必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。例えば、アクセス制御の機能、パスワード設定機能、ログ取得機能、データの暗号化等である。

(注1) 情報機器及びソフトウェア等の情報セキュリティ機能の評価に当たっては、第三者機関による客観的な評価である、ISO/IEC15408に基づくITセキュリティ評価及び認証制度による認証の取得の有無を評価項目として活用することも考えられる。また、構築する情報システムに重要な情報セキュリティ要件があると認められた場合には、第三者機関による当該情報システムのセキュリティ設計仕様書(ST: Security Target)のST評価・ST確認を活用することも考えられる。「ITセキュリティ評価及び認証制度(JISEC)」については、独立行政法人情報処理推進機構のサイトを参照のこと。

(注2) 情報システム管理者は、システム調達、開発、導入を行うに当たっては、CISOの許可を得て実施することが望ましい。また、情報システム管理者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、CISOに求めることが望ましい。

CISOは体制の確保に際し、CIOの協力を得ることが必要な場合は、CIOに当該体制の全部又は一部の整備を求めることが望ましい。

(注3) 情報システムの利用を満足できるものにするためには、情報システムが当

該利用に足りる十分な処理能力と記憶容量を持つことが必要である。また、処理能力と記憶容量の使用状況を監視し、将来的に必要とされる能力・容量を予測して、ハードディスクの増強等適正な措置を講じることが望まれる。

(注4) 情報システムは可用性の観点から、冗長性を組み入れることを考慮することが望ましい。ただし、冗長性を組み入れることにより、情報システムの完全性、機密性に対するリスクが生じる可能性があるため、この点についても考慮すること。

・機密性を高める対策例

サーバを二重化することにより場合によっては機密性の高い情報が二カ所に保存されることになるため、修正プログラムの適用やソフトウェアの最新化、不要なサービスの停止といったセキュリティの確保を二重化した双方のサーバに同時・同等に実施する。

・完全性を高める対策例

二重化したサーバ内の情報の整合性を確保するために、双方のサーバ内のデータの突合確認や誤り訂正機能の実装などの対策を実施する。

(注5) IT 製品の調達において、その製品に他の供給者から供給される構成部品やソフトウェアが含まれる場合には、そのサプライチェーン全体に適正なセキュリティ慣行を伝達し、サプライチェーンの過程において意図せざる変更が加えられないよう、直接の供給者に要求することが必要である。また、提供された IT 製品が機能要件として取り決められたとおりに機能すること、構成部品やソフトウェアについてはその供給元が追跡可能であることを保証させることが望ましい。

(注6) 調達する情報システムに応じた要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月 地方自治情報センター）「IT 製品の調達におけるセキュリティ要件リスト」（平成30年2月28日 経済産業省）を参照されたい。

(注7) オンラインでの申請及び届出等の手続を提供するシステムについては、住民が情報システムのアクセス主体になることにも留意し、オンライン手続におけるリスクを評価した上で、認証に係る要件を策定する必要がある。

なお、オンライン手続におけるリスク評価等に関しては、「政府機関等の対策基準策定のためのガイドライン」（令和3年7月7日 内閣官房内閣サイバーセキュリティセンター）を参照されたい。

## (2) 情報システムの開発

### ① システム開発における責任者及び作業者の特定

システム開発においては、その責任の所在や実施体制を把握する観点から、責任者と作業者を特定する必要がある。また、システム開発の方針、手順等の規則を決

定し、開発に適用する必要がある。

(注8) システム開発において、作業進捗が悪い場合等に、要員の投入が逐次行われるケースがあるが、これらのことが、要員の調整等に不備が生じるケースがある。特に、業務委託でシステム開発を行う場合等は、その理由を明確にして、要員の変更や増減の許可をする必要がある。

② システム開発における管理者及び作業者の ID の管理

システム開発において、開発用の ID は、管理がずさんになりやすい傾向があることから、適正な管理が必要である。

③ システム開発に用いるハードウェア及びソフトウェアの管理

委託事業者が選定した開発用ソフトウェアについて、一般的に利用が知られていないソフトウェアは、その理由を確認する必要がある。また、利用することとしたソフトウェア以外のソフトウェアは削除することとする。

(3) 情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

システム開発において、開発環境と運用環境が同一であると、運用環境で使用しているプログラムやファイルを誤って書き換えてしまうことが発生しやすくなるので、システムの開発環境と運用環境は、できる限り分離し、セキュリティに配慮した設計にすることが必要である。また、情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

(注9) 情報システムの導入に当たっては、利用する業務の内容や取り扱う情報の重要度に応じて、万一の障害に備えた冗長性や可用性が必要となる場合がある。事前に確認しておく事項としては、例えば次のものがある。

- ・その箇所が働かないとシステム全体が停止してしまう箇所の有無とその対策内容（冗長化・障害時の円滑な切り替えなど）
- ・広域災害対策の有無（バックアップ設備を遠隔地に配置しているなど）や対応方針（サービス継続を優先するかセキュリティ対策の確保を優先するかなど）

② テスト

運用環境への移行は、業務に精通している利用部門の協力を得て、擬似環境における操作についてテストを行い、その結果を確認した後に行う必要がある。

(4) システム開発・保守に関連する資料等の整備・保管

① システム開発や機器等の導入において、開発や機器等の導入に関する資料やシステム関連文書等は、保守や機器更新の際に必要なことから、適正に整備し保管することが必要である。

② 情報システム管理者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備することが望ましい。

a) サーバ装置及び端末を管理する職員等及び利用者を特定する情報

b) サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン

c) サーバ装置及び端末で利用するソフトウェアを動作させるために用いられる他のソフトウェアであって、以下を含むものの種類及びバージョン

- ・動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの
- ・フレームワーク等、ソフトウェアを実行するための実行環境となるもの
- ・プラグイン等、ソフトウェアの機能を拡張するもの
- ・静的リンクライブラリ等、ソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの
- ・インストーラー作成ソフトウェア等、ソフトウェアを開発する際に開発を支援するために使用するもの

d) サーバ装置及び端末の仕様書又は設計書

③ 情報システム管理者は、前項 b) 及び c) の情報を収集するため、自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェアを導入するなどにより、これら情報を効率的に収集する手法を決定することが望ましい。

#### (5) 情報システムにおける入出力データの正確性の確保

情報システムの処理は、入力処理、内部処理、出力処理で構成されている。これらの処理を行うプログラムの設計が正確に行われないと、データが不正確なものになるおそれがある。

入力処理の際は、不正確なデータの取り込みが行われないう、入力データの範囲チェックや不正な文字列等の入力を除去する機能を組み込むことが必要になる。

内部処理においても、データの抽出条件の誤りやデータベースの更新処理での計算式ミス等で、データ内容を誤った結果に書き換えてしまうことのないよう、これらを検出するチェック機能を持たせる必要がある。さらには、内部処理が正確に行われていた場合であっても、出力処理で誤った処理がされると、端末画面の表示や印刷物を利用する者に対して、誤ったデータ内容を認識させてしまうおそれがある。このことから、情報システムの処理した結果の正確性が確保されるよう、システム及びプログラムの設計を行う必要がある。

(注 10) ウェブシステムの設計においては、ソースコードの記述内容にセキュリティ機能の必要性を調査せずに設計が行われるとセキュリティホールを残してしまうことがある。そこで、セキュリティ上の機能要件を洗い出し、システム開発の計画時に盛り込む必要があるほか、現在、運用しているウェブシステムについても、これらのソースコードの記述内容にセキュリティホールが潜

んでいる場合があるため、ソースコードを確認する必要がある。

(注1 1) ウェブアプリケーションの開発においては、セキュリティを考慮した実装を行わなければ脆弱性を作り込んでしまうおそれがある。適正なセキュリティを考慮したウェブサイト等を構築するための注意点や脆弱性の有無の判定基準については、「安全なウェブサイトの作り方 改訂第7版」及びその別冊資料（平成28年1月27日 情報処理推進機構）を参照されたい。

また、ウェブサイトを構築する場合は、「lg.jp」を含むドメイン名の使用を調達仕様書に含めることが必要である。「lg.jp」ドメインの適用が困難なサービスを利用する場合は、そのドメインが団体のものとは異なることとその理由を団体のウェブサイトに掲示する等により、ドメインは異なるが確かにその団体が提供するサービスであることを住民が確認できる状態とすることが望ましい。インターネットに公開するウェブサイトにおいては、転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策（常時 TLS 化）を講じることが望ましい。

(注1 2) 庁外の者が地方公共団体の名前をタイトルに掲げるなどし、地方公共団体のウェブサイトと誤解されかねないウェブサイトを構築することがあり、これを完全に防ぐことは困難である。このため、以下を例とする対策を実施する必要がある。

- ・ 正規のウェブサイトが検索サイトで上位に表示されるよう検索エンジン最適化の措置を実施する
- ・ 情報システム管理者は、庁外に提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、不審なサイトが検索結果に表示された場合は、検索サイト事業者に報告するなどの対策を実施する
- ・ 以前利用していたドメイン（旧ドメイン）を運用停止する場合は、第三者に不正に取得されないようドメインを一定期間保持する。また、旧ドメインへのアクセスがあった際に後継となるサイト（後継サイトがない場合は終了を告知したページや団体トップページ等）へ HTTP 応答コード 301 を用いた転送を行うことで、旧ドメインが検索サイトの上位に表示される機会をできるだけなくすことが望ましい。詳細は「ドメイン管理ガイド(2.0 版)」（平成28年12月1日 内閣官房情報通信技術（IT）総合戦略室）を参照されたい。

(注1 3) ウェブサイトや電子メール等を利用し、庁外の者が提供するウェブアプリケーション・コンテンツを告知する場合は、以下の対策を講じること。

- ・ 告知するアプリケーション・コンテンツを管理する組織名を明記する
- ・ 告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する機



関について明記する

- ・電子メールにて告知する場合は、告知内容についての問合せ先を明記する

(6) 情報システムの変更管理

情報システムのプログラムを保守した場合は、必ず変更履歴を作成しておくことが必要になる。変更履歴がないと、プログラム仕様書と実際のソースコードに不整合が生じ、変更時の見落としからシステム障害を招く可能性が高まる。

(7) 開発・保守用のソフトウェアの更新等

数年間のシステム開発等、長期の開発期間を要する場合には、運用環境のシステム保守状況を踏まえて、移行時にシステム障害が生じないように、開発環境のソフトウェアの更新を行っておく必要がある。ソフトウェアのバージョンが違っていたために、運用環境でシステムが緊急停止をすることや、他のシステムに影響を与えることがあり、これを未然に防止することが重要である。

(8) システム更新又は統合時の検証等

システムを更新又は統合する場合は、システムの長時間の停止や誤動作等による業務への影響が生じないように、事前に慎重な検証等を行っておく必要がある。

(注14) 検証等を行う事項としては、例えば次のものがある。

- ・システム更新又は統合作業時に遭遇する想定外の事象に対応する体制
- ・システム及びデータ移行手続が失敗した場合や移行直後に障害等が生じた場合における、旧システムへ戻す計画とその手順
- ・更新又は統合によって影響される業務運営体制
- ・システム及びデータ移行手続における検証チェックポイントや移行の妥当性基準の明確化

#### 6.4. 不正プログラム対策

##### 【趣旨】

情報システムにコンピュータウイルス等の不正プログラム対策が十分に実施されていない場合は、システムの損傷、情報漏えい等の情報セキュリティインシデントが発生するおそれがある。不正プログラム対策としては、不正プログラム対策ソフトウェアを導入するとともに、パターンファイルの更新、ソフトウェアのパッチの適用等を確実に実施することが基本であり、被害の拡大を防止することになる。

これらを踏まえ、不正プログラムの感染、侵入を予防し、さらには感染時の対応として取るべき手段を規定する。

##### 【例文】

###### (1) 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

- ①外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。
- ②外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。
- ③コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。
- ④所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
- ⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
- ⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
- ⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

###### (2) 情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

- ①情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。
- ②不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
- ③不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
- ④インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。
- ⑤不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

### (3) 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

- ①パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
- ②外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
- ③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
- ④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的実施しなければならない。
- ⑤添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は無害化しなければならない。
- ⑥統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。
- ⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

#### (4) 専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

#### (解説)

##### (1) 統括情報セキュリティ責任者の措置事項

インターネットからの不正プログラム感染、侵入を防御するためには、庁内ネットワークとインターネットの境界で不正プログラム対策ソフトウェアを導入する必要がある。

(注1) 不正プログラムには、コンピュータシステムの破壊、無差別の電子メールの送信による感染の拡散を行うコンピュータウイルスのほか、暗証番号やパスワード等を盗むことを目的にしているスパイウェアなど、多くの種類が存在している。また、ウィニー等のファイル共有ソフトウェアがコンピュータウイルスに感染したことによる情報漏えい事案が数多く発生している。

(注2) ソフトウェアの更新は、開発元等から提供されるセキュリティホールのパッチ適用やバージョンアップ等で行うが、これらは開発元がサポートしている期間内でのみ行うことができるため、適宜サポートが終了していないソフトウェアへ切り替え等を行う必要がある。なお、ソフトウェアの更新についてはパソコン等の端末だけでなくサーバやモバイル端末についても同様にOSの更新や修正プログラムを適用する必要がある。

(注3) インターネットからの不正プログラム感染、侵入を防御するための方式として、パターンファイルでは未知の不正プログラムの検知が難しいことから、不正プログラムの挙動を検知する方式等によって既知及び未知の不正プログラムの検知並びにその実行を防止する機能を有するソフトウェアを導入することも有益である。

##### (2) 情報システム管理者の措置事項

ウイルスチェック等のパターンファイルや不正プログラム対策ソフトウェアは常に最新の状態に保って利用することが不可欠である。

なお、インターネットに接続していないシステムは、不正プログラムの感染、侵入の可能性は低いですが、原則として職員等が持ち込んだ電磁的記録媒体や古くから保管していた電磁的記録媒体から感染することもあり得るので、電磁的記録媒体の使用は組織内で管理しているものに限るとともに、不正プログラム対策ソフトウェアを開発元等から定期的に取り寄せ、パターンファイルの更新やパッチの適用を確実に

実施することが必要である。

(3) 職員等の遵守事項

職員等には、不正プログラムに関する情報及び対策を周知して対策を徹底することが必要であり、特に、不審なメールやファイルの削除、不正プログラム対策ソフトウェアを常に最新の状態に保たせることが重要である。コンピュータウイルスに感染した兆候がある場合には、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてLANケーブルの取り外し（パソコン等の端末の場合）や、通信を行わない設定への変更（モバイル端末の場合）などを実施しなければならない。

(4) 専門家の支援体制

不正プログラム対策ソフトウェアの開発元等の専門家と連絡を密にし、不正プログラム感染時等に、支援を受けられるようにしておく必要がある。

## 6.5. 不正アクセス対策

### 【趣旨】

情報システムに不正アクセス対策が十分に実施されていない場合は、システムへの攻撃、情報漏えい、損傷、改ざん等の被害を及ぼすおそれがある。このことから、不正アクセスの防止又は被害を最小限にするため、不正アクセス対策として取るべき措置、攻撃を受けた際の対処及び関係機関との連携等について規定する。

### 【例文】

#### (1) 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

- ①使用されていないポートを閉鎖しなければならない。
- ②不要なサービスについて、機能を削除又は停止しなければならない。
- ③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定しなければならない。
- ④重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。【推奨事項】
- ⑤統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

#### (2) 攻撃への対処

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、都道府県等と連絡を密にして情報の収集に努めなければならない。

#### (3) 記録の保存

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

#### (4) 内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員等及び委託事業者

が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) 職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

(6) サービス不能攻撃

統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(7) 標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

(解説)

(1) 統括情報セキュリティ責任者の措置事項

使用されていない TCP/UDP ポートや不要なサービスは、不正アクセスによる侵入や悪用に利用される可能性が高いため、ポート閉鎖やサービス停止処理を行う。

(注1) 重要なファイルの改ざんについては、改ざん検知ソフトウェアの利用によって、不正アクセス、不正プログラムの侵入を検知することが可能である。

(注2) DNS の導入時には以下の対策を講じなければならない。

- ・庁外からの名前解決の要求に応じる必要があるかについて検討し、必要性がないと判断される場合は庁内からの名前解決の要求のみに応答をするよう措置を講じる。
- ・DNS キャッシュポイズニング攻撃から保護するための措置を講じる。
- ・キャッシュサーバにおいて、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（3か月に一度程度）に確認し、最新の DNS ルートサーバの情報を維持する。

(注3) 庁内の CSIRT を活用して CISO への報告、各部部局への指示、ベンダと

の情報共有及び報道機関への通知・公表などの対応を行うとともに、地方公共団体情報システム機構（自治体 CEPTOAR）等の関係機関や他の地方公共団体の同様の窓口機能、委託事業者等と連携して情報共有を行うことが望ましい。

## （２） 攻撃への対処

情報システムに対する攻撃予告があり、攻撃を受けることが確実な場合には、システム停止等の措置を講じなければならない。また、総務省、都道府県等との連絡を密にし、情報収集に努めなければならない。

（注４） 攻撃を受けた際の対応として、「緊急時対応計画」に基づき、ログの確保、被害を受けた場合の復旧手順の策定、庁内関係者の役割等を再確認しておく必要がある。

## （３） 記録の保存

外部から不正アクセスを受けた場合に、その記録としてログ、対応した記録等を保存しておくことは、事実確認、原因追及及び対策検討のため、必要であり、記録の保存について定めておく必要がある。

（注５） 不正アクセスについてログ解析を行う場合は、証拠保全用と解析用と分けて保管する必要がある。

## （４） 内部からの攻撃

庁内ネットワークに接続したパソコン、モバイル端末及び不正プログラムに感染した庁内サーバを使って、庁内のサーバや外部のサーバ等に攻撃を仕掛けられる場合があり、これらを監視しなければならない。

（注６） 庁舎内で住民、観光客に公衆通信回線を提供する場合は、内部の情報システムとネットワークを切り分け、不正アクセスを防止する対策を講じなければならない。

## （５） 職員等による不正アクセス

職員等が庁内にあるパソコンやモバイル端末を利用し、不正アクセスを発見した場合には、情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

## （６） サービス不能攻撃

サービス不能攻撃は DoS (Denial of Service) 攻撃や DDoS (Distributed Denial of Service) 攻撃とも呼ばれている。第三者からサービス不能攻撃を受けた場合でも、情報システムの可用性を維持するために次の例のような対策を実施する必要がある。また、これらの対策が適正に実施されているかをモニタリングし、確かめる必要がある。

### ① 情報システムを構成する機器の装備している機能による対策の実施

- ・ サーバ装置、端末及び通信回線装置について、サービス不能攻撃に対抗するための機能が実装されている場合は、これらを有効にする。



- ・通信事業者と協議し、サービス不能攻撃が発生時の対処手順や連絡体制を整備する。

#### ② サービス不能攻撃を想定した情報システムの構築

- ・サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断したり、通信回線の通信量を制限したりするなどの手段を有する情報システムを構築する。
- ・サービスを提供する情報システムを構築するサーバ装置、端末、通信回線装置及び通信回線を冗長化し、許容される時間内に切り替えられるようにする。
- ・サービス不能攻撃の影響を排除又は低減するための専用の対策装置を導入する。

#### ③ 通信事業者の提供するサービスの利用

- ・通信事業者が別途提供する、サービス不能攻撃に係る通信の遮断等のサービスがある場合は、これを利用する。

#### ④ 情報システムの監視及び監視記録の保存

- ・庁外からアクセスされるサーバ装置や、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるものを優先的に監視する。
- ・監視の記録については、監視対象の状態の変動を考慮した上で記録を一定期間保管する。

### (7) 標的型攻撃

標的型攻撃による外部から庁内への侵入を防ぐため、標的型攻撃メール受信時の人的対策のほか、電磁的記録媒体やネットワークに対する技術的対策についても次の例のような対策を実施する必要がある。また、これらの対策が適正に実施されているかをモニタリングし、確かめる必要がある。なお、対策の検討にあたっては、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」(平成 28 年 10 月 7 日 サイバーセキュリティ対策推進会議) 及び「高度サイバー攻撃対処のためのリスク評価等のガイドライン 付属書」(平成 28 年 10 月 7 日 内閣官房内閣サイバーセキュリティセンター) も参照されたい。

#### ① 人的対策例 (標的型攻撃メール対策)

- ・差出人に心当たりがないメールは、たとえ興味のある件名でも開封しない。
- ・不自然なメールが着信した際は、ウェブ等の当該メール以外の情報源から当該組織の電話番号や問合せメールアドレスを調べ、この差出人が実在するか、このメールを送信したかなどを確認する。
- ・メールを開いた後で標的型攻撃と気付いた場合、添付ファイルは絶対に開かず、メールの本文に書かれた URL もクリックしない。
- ・標的型攻撃と気付いた場合、システム管理者に対して着信の事実を通知し、組

織内への注意喚起を依頼した後に、メールを速やかに削除する。

- ・システム管理者は、メールやログを確認し、不正なメールがなかったかチェックする。(事後対策)

#### ②電磁的記録媒体に対する対策例

- ・出所不明の電磁的記録媒体を内部ネットワーク上の端末に接続させない。
- ・電磁的記録媒体をパソコン等の端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。
- ・パソコン等の端末について、自動再生（オートラン）機能を無効化する。
- ・パソコン等の端末について、電磁的記録媒体内にあるプログラムを媒体内から直接実行することを拒否する。

#### ③ネットワークに対する対策例

- ・ネットワーク機器のログ監視を強化することにより、情報を外部に持ち出そうとするなどの正常ではない振る舞いや外部との不正な通信を確認し、アラートを発したりその通信を遮断する。
- ・不正な通信がないか、ログをチェックする。(事後対策)

## 6.6. セキュリティ情報の収集

### 【趣旨】

ソフトウェアにセキュリティホールが存在する場合、システムへの侵入、改ざん、損傷、漏えい等の被害を及ぼすおそれがある。また、情報セキュリティを取り巻く社会環境や技術環境等は刻々と変化しており、新たな脅威により情報セキュリティインシデントを引き起こすおそれがある。これらのことから、セキュリティホールをはじめとするセキュリティ情報の収集、共有及び対策を講じることについて規定する。

### 【例文】

- (1) セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等  
統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。
- (2) 不正プログラム等のセキュリティ情報の収集・周知  
統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。
- (3) 情報セキュリティに関する情報の収集及び共有  
統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

### (解説)

- (1) セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等  
セキュリティホールは日々発見される性質のものであることから、積極的に情報収集及び対応の検討を行う必要がある。セキュリティホールの対策状況の定期的な確認により、セキュリティホールへの対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連するセキュリティホールの情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関するセキュリティホールへの対策計画を策定し、措置を講ずることが必要である。

(注1) セキュリティホールの情報収集に関しては、情報収集の体制、分析の手順、情報収集先、情報共有先等を決めておくことが望まれる。

(注2) セキュリティホールの緊急度のレベルに応じて、更新の実施の有無を検討する。深刻なセキュリティホールが発見された場合は、直ちに対応しなければならないが公開された脆弱性の情報がない段階においては、サーバ、端末及び通信回線上で取り得る対策を検討する。また、更新計画を定め、他のシステムへの影響、テスト方法、バックアップの実施、パッチの適用後のシステム障害が生じた場合の復旧手順等を盛り込むことが望ましい。

なお、近年のITの利活用拡大により、システムで使用しているソフトウェア等の種類も増加していることから、IT資産を手作業で漏れなく正確に把握するには多大な労力が必要となる。そのため、自動でソフトウェアの種類及びバージョンを管理する機能を有するIT資産管理ソフトウェアを導入することが考えられる。また、脆弱性対策が計画通りに実施されないことは、システムの損傷、情報漏えい等の情報セキュリティインシデントが発生する原因にもなるため、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認することが望ましい。

(注3) 不正プログラム、セキュリティホールのパッチの適用情報については、必要に応じ、イントラネットを利用して閲覧できるようにし、職員等に対して速やかに周知することが望ましい。

(注4) OSや各種サーバ、ファイアウォール等の通信回線装置等におけるセキュリティホールの対策状況を効率的に確認する方法として、専用ツールを用いて自らが脆弱性診断を行ったり、事業者が提供するサービス等を利用して脆弱性診断を行うことが挙げられる。脆弱性診断には、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、ソフトウェアの種類によって利用する脆弱性診断を使い分ける必要がある。

ソースコード診断では、独自に開発したソフトウェアのソースコードを対象に、静的解析ツール等を用いて脆弱性の有無を検証する。したがって、運用開始までにソースコード診断を実施し、運用開始後にソースコードへ修正を加えた場合は、再度診断を実施することが望ましい。

プラットフォーム診断では、OSや各種サーバ、ファイアウォール等を対象に、テスト用の通信パケットを送信するなどの方法によって、最新のセキュリティパッチが適用されているか、設定が適切に行われているか、不要な通信ポートが開いていないかなどを検証する。したがって、運用開始までにプラットフォーム診断を実施し、その後も例えば年に1回診断を実施するなど、定期的に実施することが望ましい。

ウェブアプリケーション診断では、独自に開発したウェブアプリケーションを対象に、実際に不正なデータをウェブアプリケーションに送信する方法によって、SQLインジェクションやクロスサイトスクリプティング等の脆弱性が存在しないかを検証する。したがって、運用開始までにウェブアプリケーション診断を実施し、運用開始後においても、ウェブアプリケーション

へ修正を加えた場合や新たな脅威が確認された場合は、再度診断を実施することが望ましい。なお、事業者が提供するサービス等を利用して脆弱性診断を行う場合には、事業者における一定の技術要件及び品質管理要件を確保する観点から、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を掲載した「情報セキュリティサービス基準適合サービスリスト」（うち脆弱性診断サービスに係る部分）を活用することが考えられる。

(2) 不正プログラム等のセキュリティ情報の収集・周知

(注5) セキュリティ情報の入手先としては、情報システムの納入業者のほかに、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）、IPA（独立行政法人 情報処理推進機構）等がある。

(3) 情報セキュリティに関する情報の収集及び周知

情報セキュリティに関する技術は、新たな技術の開発や普及状況の変化により、期待した情報セキュリティの有効性が失われることや新技術への移行によって既存技術を利用したサービスを受けることができなくなる等、新たなリスクを発生する可能性もあり、情報システム等の情報セキュリティインシデントやセキュリティ侵害の未然の防止のために情報セキュリティに関する技術の動向や技術環境等の変化に関する情報収集と対策を講じる必要がある。

(注6) 情報セキュリティに関する技術の変化による新たな脅威として、「重要インフラにおける情報セキュリティ確保に係る「安全対策基準等」策定に当たっての指針（第3版）対策編」（平成22年7月30日（平成26年3月26日改定）重要インフラ専門委員会）では、下記の事項が挙げられている。

- ・電子計算機の性能向上等により暗号の安全性が低下する「暗号の危殆化」
  - ・インターネットの普及による IPv4 アドレス枯渇化に伴う「IPv6 移行」
- また、情報収集と対策の検討に当たっては、必要に応じて、外部専門家等の活用も検討する必要がある。

(注7) 暗号の危殆化については、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（平成25年3月1日（令和3年4月1日最終更新）総務省・経済産業省）及び同リストを策定した CRYPTREC の今後の報告を参考とすることができる。

(注8) TLS 暗号設定については、「TLS 暗号設定ガイドライン Ver3.0.1」（CRYPTREC 令和2年7月）を参照されたい。

(注9) IPv6 への移行については、IPv6 通信を導入する場合における他の情報システムへの影響や、IPv6 通信を想定していないネットワークに接続される全ての情報システム及びネットワークに対する IPv6 通信を抑止するための措置、IPv6 通信を想定していないネットワークを監視し、IPv6 通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を講じる必要がある。

(注10) 導入しているソフトウェア (OS を含む。) のサポートが終了した場合、新たな脆弱性が発見されたとしても修正プログラムが製造元から提供されず、情報の流出や第三者を攻撃するための踏み台として利用される等の可能性が高まるため、サポート期間の情報を収集し、適正な対策を講じる必要がある。

## 7. 運用

### 7.1. 情報システムの監視

#### 【趣旨】

情報システムにおいて、不正プログラム、不正アクセス等による情報システムへの攻撃・侵入、社内職員の不正な利用、自らのシステムが他の情報システムに対する攻撃に悪用されることを防ぐためには、ネットワーク監視等により情報システムの稼働状況について常時監視を行うことが必要である。したがって、情報システムの監視に係る対策について規定する。

#### 【例文】

- ①統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。
- ②統括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。
- ③統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。
- ④暗号化された通信データを監視のために復号することの可否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。【推奨事項】

#### (解説)

監視に必要な要素は、不正アクセスや不正利用の検知と記録（ログ等）である。情報システムの稼働状況について、インターネットからの不正アクセスの状況や社内職員の利用状況も含め、ネットワーク監視等により常時確認を行うことが必要である。また、記録については、証拠としての正確性を確保するために、サーバの時刻設定を正確に行う必要がある。サーバ間で時刻記録に矛盾が生じると、ログ解析等追跡が困難になるとともに、証拠としての正確性が担保できないことになる。

ウェブの常時暗号化（TLS化）や電子メールサーバ間通信の暗号化（TLS化）等といった通信の暗号化が社会的に進められ、その利用割合が上昇する中で、不正なプログラム等の脅威が暗号化された通信の中に含まれていると、当該通信の監視による脅威の検知が困難になる。このため、監視に際しては、監視対象のデータが暗号されているかどうかを把握し、対象とする脅威の監視可否に与える影響を考慮した上で復号の可否を判断し、必要と判断した場合にはその対策を講じなければならない。なお、自治体情報セキュリティクラウド側の機能とした上で、活用することも可能である。

（注1） ネットワーク及び情報システムの稼働中は常時監視し、障害が起きた際にも速やかに対応できる体制である必要がある。このため、リスクに応じて侵入検知シ

システム（IDS: Intrusion Detection System）等の利用、監視体制の整備等の措置を講じる必要がある。ネットワーク監視で侵入検知に利用する、IDSは、不正プログラム対策ソフトウェアのパターンファイルと同様に、不正アクセスのパターンを検知するためのファイルの更新を行い、検知能力を維持する必要がある。また、侵入検知だけではなく、侵入を防御する、侵入防御システム（IPS: Intrusion Prevention System）も存在する。

(注2) システム管理者などの特別な権限を持つIDの利用者の記録の確認については、本人以外のシステム管理者又はシステム管理者以外の者が確認するようにし、客観的に確認できる仕組みを構築する必要がある。

(注3) 監視を実施するに当たり、監視業務を事業者に請け負わせることも考えられる。このとき、当該業務を事業者に請け負わせることは、業務委託に該当することから、関連する規定にも留意する必要がある。また、事業者の選定に際しては、事業者における一定の技術要件及び品質管理要件を確保する観点から、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を掲載した「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監視・運用サービスに係る部分）を活用することが考えられる。



## 7.2. 情報セキュリティポリシーの遵守状況の確認

### 【趣旨】

情報セキュリティポリシーの遵守を確保するため、情報セキュリティポリシーの遵守状況等を確認する体制を整備するとともに、問題があった場合の対応について規定する。

### 【例文】

#### (1) 遵守状況の確認及び対処

- ①情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及び統括情報セキュリティ責任者に報告しなければならない。
- ②CISO は、発生した問題について、適正かつ速やかに対処しなければならない。
- ③統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

#### (2) パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

CISO 及び CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

#### (3) 職員等の報告義務

- ①職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。
- ②当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

### (解説)

#### (1) 遵守状況の確認及び対処

情報セキュリティポリシーを運用する過程において、遵守状況を確認し、違反の有無、情報セキュリティポリシーの問題点などを明らかにすることが求められる。確認の結果、問題があった場合には、CISO は速やかに対処する必要がある。

(注1) 遵守状況の確認方法としては、自己点検等の実施、情報セキュリティインシデントの報告、日常の業務からの情報セキュリティ対策の問題事項の報告、ログ等からの異常時の発見などがある。

#### (2) パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

職員等はパソコン、モバイル端末及び電磁的記録媒体等を業務のため使用しているのであって、私的な使用はあってはならない。職員等の業務以外の目的での利用を抑止するため、電子メールの送受信記録等を調査できる権限を CISO 及びその指名した者に付与する。

(注2) 職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等や電子メールの送受信記録等の情報を調査することをあらかじめ周知しておくことも重要である。調査が行われるかもしれないということが、不正行為に対する抑止力として効果がある。

(注3) 職員等が利用しているパソコン、モバイル端末及び電磁的記録媒体等の状況を調査することは、職員等のプライバシーとの関係が問題になるが、基本的には業務利用のパソコン、モバイル端末及び電磁的記録媒体等には、個人のプライバシー侵害になる記録は存在しないと考えられる。したがって、インターネット閲覧記録、電子メールの送受信記録等の調査権を確保しておくことは重要なことになる。ただし、調査は、CISO 又は CISO が指名した者が行う必要がある。

### (3) 職員等の報告義務

職員等は、日々の業務で、情報セキュリティポリシーに違反した行為を発見した場合、その報告が求められる。統括情報セキュリティ責任者は、その報告を受け、情報セキュリティ上重大な影響があると判断した場合に、緊急時対応計画に沿って適正に対処する。

### 7.3. 侵害時の対応等

#### 【趣旨】

情報セキュリティインシデント、システム上の欠陥及び誤動作並びに情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害事案が発生した場合に、迅速かつ適正に被害の拡大防止、迅速な復旧等の対応を行うため、緊急時対応計画の策定について規定する。

#### 【例文】

##### (1) 緊急時対応計画の策定

CISO 又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

##### (2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

- ①関係者の連絡先
- ②発生した事案に係る報告すべき事項
- ③発生した事案への対応措置
- ④再発防止措置の策定

##### (3) 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

##### (4) 緊急時対応計画の見直し

CISO 又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

#### (解説)

##### (1) 緊急時対応計画の策定

情報セキュリティが侵害された場合又は侵害されるおそれがある場合等における具体的な措置について、緊急時対応計画として定める。

緊急時対応計画には、情報資産に対するセキュリティ侵害が発生した場合等における連絡、証拠保全、被害拡大の防止、復旧等の迅速かつ円滑な実施と、再発防止策

の措置を講じるために必要な事項を定める必要がある。

また、自らが所有する情報資産における被害拡大防止のほか、外部への被害拡大のおそれがある場合には、その防止に努めることを定める必要がある。情報が漏えいすることなどにより被害を受けるおそれのある関係者に対し早急に連絡することが重要である。

当該事案が不正アクセス禁止法違反等の犯罪の可能性がある場合には、警察・関係機関と緊密な連携に努めることも重要である。

(注1) 緊急時対応計画を策定する場合は、他の危機管理に関する規程等と整合性を確保し策定する必要がある。また、他の危機管理に関する規程の改定と情報セキュリティポリシーの見直しの時期が異なることにより一時的に不整合が生じないように、配慮する必要がある。

(注2) 庁内の CSIRT が担う役割についても緊急時対応計画を策定する場合に考慮することが望ましい。また、インシデントレスポンスにおいては、一部業務を事業者に請け負わせることも考えられる。このとき、当該業務を事業者に請け負わせることは、業務委託に該当することから、関連する規定にも留意する必要がある。また、事業者の選定に際しては、事業者における一定の技術要件及び品質管理要件を確保する観点から、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を掲載した「情報セキュリティサービス基準適合サービスリスト」（うちデジタルフォレンジックサービスに係る部分）を活用することが考えられる。

## (2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画に定める事項としては、例えば次のものがある。

### ①関係者の連絡先

- ・ 地方公共団体の長
- ・ CISO
- ・ 統括情報セキュリティ責任者
- ・ 情報システム管理者
- ・ 情報セキュリティに関する統一的な窓口（庁内の CSIRT）
- ・ ネットワーク及び情報システムに係る委託事業者
- ・ 広報担当課
- ・ 都道府県の関係部局
- ・ 警察
- ・ 関係機関
- ・ 被害を受けるおそれのある個人及び法人

### ②発生した事案に係る報告すべき事項

セキュリティに関する事案を発見した者は、次の項目について速やかに統括情報セキュリティ責任者に報告しなければならない。

- ・ 事案の状況

- ・事案が発生した原因として、想定される行為
- ・確認した被害・影響範囲（事案の種類、損害規模、復旧に要する額等）
- ・事案が情報セキュリティインシデントに該当するか否かの判断結果
- ・記録

また、統括情報セキュリティ責任者は、事案の詳細な調査を行うとともに、CISO及び情報セキュリティ委員会へ報告しなければならない。

（注3）統括情報セキュリティ責任者が事案の詳細な調査を行うに当たっては、必要に応じて外部専門家のアドバイスを受ける、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）及び地方公共団体情報システム機構（自治体 CEPTOAR）等の関係機関に相談する等、事実確認を見誤らないように努める必要がある。

（注4）庁内の CSIRT に報告を集約し、窓口経由で外部への問合せや相談を行うことが考えられる。

（注5）情報共有や相談については、「地方公共団体における情報セキュリティ対策及び政府の一層の充実・強化について（依頼）」（平成23年10月11日総務省 事務連絡）を参照されたい。

### ③発生した事案への対応措置

（ア）統括情報セキュリティ責任者は、次の事案が発生した場合、定められた連絡先へ連絡しなければならない。

- ・サイバーテロのほか市民に重大な被害が生じるおそれのあるとき
  - 地方公共団体の長、CISO、都道府県の関係部局、警察、影響が考えられる個人及び法人に連絡
- ・不正アクセスのほか犯罪と思慮されるとき
  - 地方公共団体の長、CISO、都道府県の関係部局、警察に連絡
- ・踏み台となって他者に被害を与えるおそれがあるとき
  - 地方公共団体の長、CISO、都道府県の関係部局、警察に連絡
- ・情報システムに関する被害
  - 情報システム管理者、必要と認められる委託事業者に連絡
- ・その他情報資産に係る被害
  - 関係部局等に連絡

（イ）統括情報セキュリティ責任者は、次の事案が発生し、情報資産を保護するためにネットワークを切断することが止むを得ない場合、ネットワークを切断する。

- ・異常なアクセスが継続しているとき又は不正アクセスが判明したとき
- ・システムの運用に著しい支障をきたす攻撃が継続しているとき
- ・コンピュータウイルス等、不正プログラムがネットワーク経由で拡がっているとき
- ・情報資産に係る重大な被害が想定されるとき

(ウ) 情報システム管理者は、次の事案が発生し、情報資産の防護のために情報システムを停止することが止むを得ない場合、情報システムを停止する。

- ・コンピュータウイルス等、不正プログラムが情報資産に深刻な被害を及ぼしているとき
- ・災害等により電源を供給することが危険又は困難なとき
- ・そのほかの情報資産に係る重大な被害が想定されるとき

(エ) 個々のパソコン等の端末のネットワークからの切断については、セキュリティポリシーにおいて特段の定めがあるものを除き、統括情報セキュリティ責任者の許可が必要である。

ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合は、事後報告とすることができる。

(オ) 事案に係るシステムのログ及び現状を保存する。

(カ) 事案に対処した経過を記録する。

(キ) 事案に係る証拠保全の実施を完了するとともに、応急措置を講じる。

(ク) 応急措置を講じた後、復旧する。

(ケ) 復旧後、必要と認められる期間、再発の監視を行う。

#### ④再発防止措置の策定

(ア) 統括情報セキュリティ責任者は、当該事案に係る調査を実施し、情報セキュリティポリシー及び実施手順の改善を含め、再発防止計画を策定し、情報セキュリティ委員会へ報告する。

(イ) 情報セキュリティ委員会は、再発防止計画が有効であると認められた場合はこれを承認し、事案の概要とあわせ職員等に周知する。

#### (3) 業務継続計画との整合性確保

地震及び風水害等の自然災害等や大規模・広範囲にわたる疾病等の事態に備えて、情報セキュリティにとどまらない危機管理規定として業務継続計画（あるいは、ICT部門における業務継続計画）を策定することが重要である。ただし、業務継続計画と情報セキュリティポリシーの間に矛盾があると、職員等は混乱し、適正な対応をとることができなくなるおそれがあるため、各地方公共団体において業務継続計画を策定する際には、情報セキュリティポリシーとの整合性をあらかじめ検討し、必要があれば、情報セキュリティポリシーを改定しなければならない。

(注6) 整合性を検討すべき事項は、例えば、施設の耐災害性対策、施設・情報システムの地理的分散、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用、事態発生時の対応体制及び要員計画などがある。

(注7) 危機管理には、大規模・広範囲にわたる疾病等によるコンピュータ施設の運用にかかる機能不全等への考慮も望まれる。

(注8) 大地震を対象事態とした ICT 部門における業務継続計画の策定については、「地方公共団体における ICT 部門の業務継続計画 (BCP) 策定に関するガ

イドライン」(平成 20 年 8 月 総務省)及び「地方公共団体における ICT 部門の業務継続計画 (ICT-BCP) 初動版サンプル」(平成 25 年 5 月 8 日 総務省)を参照されたい。

(4) 緊急時対応計画の見直し

緊急時対応計画の実効性を確保するため、新たな脅威の出現等の情報セキュリティに関する環境の変化や組織体制の変化等を盛り込んだ最新の内容となるよう、定期的に見直すことが必要である。また、緊急時対応計画の発動した場合を仮定した訓練や机上試験を定期的実施しておくことも、緊急時対応計画の実効性を確保する観点から重要である。

#### 7.4. 例外措置

##### 【趣旨】

情報セキュリティポリシーの規定をそのまま適用した場合に、行政事務の適正な遂行を著しく妨げるなどの理由により、これに代わる方法によることやポリシーに定められた事項を実施しないことを認めざるを得ない場合がある。このことから、あらかじめ例外措置について規定する。

##### 【例文】

###### (1) 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、CISOの許可を得て、例外措置を講じることができる。

###### (2) 緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにCISOに報告しなければならない。

###### (3) 例外措置の申請書の管理

CISOは、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

##### (解説)

例外措置は、情報セキュリティポリシーの適用を例外的に排除するものであることから、その承認は、ポリシーの適用が著しく行政事務の遂行を妨げる、緊急を要し通常の手続を取る時間的な猶予がない、技術的に困難であるなどの合理的な理由が必要である。なお、その場合でも、例外措置は単に適用を排除するだけでなく、リスクに応じて代替措置を定めること及び期限を設けて認めることが望ましい。

CISOは、例外措置についての手続を定め、明示することによって、ローカルルールの氾濫や、対策の未実施を防止することができる。

(注1) 例外措置の内容から判断し、情報セキュリティポリシーの遵守自体に無理があると判断される場合には、当該ポリシーの見直しについて検討する必要がある。



## 7.5. 法令遵守

### 【趣旨】

職員等は、全ての法令を遵守することは当然であるが、職員等が業務を行う際の参考として、情報セキュリティに関する主要な法令を明示し、法令の遵守を確実にする。

### 【例文】

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

- ①地方公務員法（昭和 25 年法律第 261 号）
- ②著作権法（昭和 45 年法律第 48 号）
- ③不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
- ④個人情報の保護に関する法律（平成 15 年法律第 57 号）
- ⑤行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）
- ⑥サイバーセキュリティ基本法（平成 26 年法律第 104 号）
- ⑦〇〇市個人情報保護条例（平成〇〇年条例第〇〇号）

### （解説）

情報セキュリティ対策において関連のある主要な法令について明示し、法令遵守を確実にする。また、法令への適合を確実なものにするためには、必要に応じて有識者による法的な助言を受けることが望ましい。

また、関連する最新の法令に基づき定期的に情報セキュリティポリシーの見直しを行い、最新に保つことが望ましい。

## 7.6. 懲戒処分等

### 【趣旨】

情報セキュリティポリシーの遵守事項に対して、職員等が違反した場合の事項を定めておくことは、情報セキュリティポリシー違反の未然防止に一定の効果が期待される。このことから、情報セキュリティポリシー違反に対する懲戒処分の規定及び懲戒に係る手続について規定する。

### 【例文】

#### (1) 懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

#### (2) 違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

- ①統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
- ②情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
- ③情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

## 8. 業務委託と外部サービスの利用

### 8.1. 業務委託

#### 【趣旨】

外部の者に、情報システムやアプリケーションプログラムの開発・運用・保守等を委託する際に、職員等が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において対策基準に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

業務委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任、約款への同意等様々であるが、いずれの場合においても、前述のように委託先において対策基準に適合した情報セキュリティ対策が確実に実施される必要のある業務委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

なお、委託先で外部サービスを利用する場合は、委託先においても外部サービス特有のリスクがあることから、「8.2. 外部サービスの利用（機密性2以上の情報を取り扱う場合）」で規定する内容についても委託先への要求事項に含める必要がある。

#### <業務委託の例>

- ・ 情報システムの開発及び構築業務
- ・ アプリケーション・コンテンツの開発業務
- ・ 情報システムの運用業務
- ・ 業務運用支援業務（統計、集計、データ入力、媒体変換等）
- ・ プロジェクト管理支援業務
- ・ 調査・研究業務（調査、研究、検査等）

#### 【例文】

##### (1) 委託事業者の選定基準

- ①情報セキュリティ管理者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。
- ②情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。【推奨事項】

##### (2) 契約項目

情報システムの運用、保守等を業務委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

- ・ 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

- ・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
- ・提供されるサービスレベルの保証
- ・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
- ・委託事業者の従業員に対する教育の実施
- ・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
- ・業務上知り得た情報の守秘義務
- ・再委託に関する制限事項の遵守
- ・委託業務終了時の情報資産の返還、廃棄等
- ・委託業務の定期報告及び緊急時報告義務
- ・市による監査、検査
- ・市による情報セキュリティインシデント発生時の公表
- ・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

### （３） 確認・措置等

情報セキュリティ管理者は、委託事業者において十分なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（２）の契約に基づき措置を実施しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

## （解説）

### （１） 委託事業者の選定基準

委託事業者を選定するに当たっては、情報セキュリティ上、重要な情報資産を取り扱う可能性があることから、技術的能力、信頼性等について考慮して、情報セキュリティ対策が確保されることを確認する必要がある。

また、委託事業者の選定にあたり、事業者の情報セキュリティ水準を評価する際には、国際規格の認証取得状況等を参考にして決定することが望ましい。

なお、委託事業者の選定条件として仕様等に盛り込む内容としては、例えば次のものがある。

- ・委託事業者に提供する情報の委託事業者における目的外使用の禁止
- ・委託事業者における情報セキュリティ対策の実施内容及び管理体制
- ・業務委託事業の実施にあたり、委託事業者の組織若しくはその従業員、再委託事業者、又はその他の者による意図せざる変更が加えられないための管理体制
- ・委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供
- ・情報セキュリティ要件の適正な実装
- ・情報セキュリティの観点に基づく試験の実施
- ・情報セキュリティインシデントへの対処方法

- ・情報セキュリティ対策その他の契約の履行状況の確認方法
- ・情報セキュリティ対策の実施が不十分な場合の対処方法

(注1) これらの選定方法については、「公共 IT におけるアウトソーシングに関するガイドライン」(平成 15 年 3 月 総務省)を参照されたい。

(注2) 現在の最新の規格である ISO/IEC27001 については、一般財団法人日本情報経済社会推進協会のホームページ (ISMS 適合性評価制度) 又は一般財団法人日本規格協会のホームページを参照されたい。

(注3) ホスティングサービスの利用等においては、サービス提供者側のミスや機器の故障などの不測の事態によりデータの消失などの事態が発生するおそれがあるため、情報システムや取り扱う情報の重要度に応じたバックアップなどの必要な対策を講じておく必要がある。なお、ホスティング時のデータ消失に関する対策については、「ホスティングサービス等利用時におけるデータ消失事象への対策実施及び契約内容の再確認等について (注意喚起)」(平成 24 年 7 月 6 日 総務省 事務連絡)を参照されたい。

(注4) 委託事業者の委託判断基準

業務委託にあたっては、委託事業者の委託判断基準を作成しておくことが望ましい。規定すべき内容としては、例えば次のものがある。

- ・業務委託を許可 (又は禁止) する業務又は情報システムの範囲
- ・業務委託を許可 (又は禁止) する業務又は情報システムの具体的例示 (公開ウェブサーバは業務委託可等)
- ・格付及び取扱制限その他取り扱う情報の特性に応じた、情報の取扱いを許可 (又は禁止) する場所

特に、委託業務において取り扱われる情報が海外のデータセンターに存在する場合等においては、保存している情報に対して現地の法令等が適用されるため、国内であれば不適切と判断されるアクセスが行われる可能性があることに注意が必要である。

## (2) 契約項目

委託事業者に起因する情報漏えい等の事案を防ぐため、各団体で実施する場合と同様の対策を当該委託事業者に実施させるよう必要な要件を契約等に定める必要がある。以下に示す項目について、委託する業務の内容に応じて明確に要件を規定することが必要である。

### ①情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

委託事業者の要員に対して、情報セキュリティポリシー及び情報セキュリティ実施手順について、委託業務に係る事項を遵守することを定める。委託事業者において情報セキュリティインシデントが発生した場合に備えて、対処方法 (対処手順、責任分界、対処体制等) について契約前に合意しておかなければならない。

### ②委託事業者の責任者、委託内容、作業者、作業場所の特定

委託事業者の責任者や作業者を明確にするとともに、これらの者が変更する場

合の手続を定めておき、担当者の変更を常に把握できるようにする。また、作業場所を特定することにより、情報資産の紛失等を防止する。

③提供されるサービスレベルの保証

通信の速度及び安定性、システムの信頼性の確保等の品質を維持するために、必要に応じて、サービスレベルを保証させる。

④委託事業者に許可する情報の種類とアクセス範囲、アクセス方法

委託に関わる情報の種類を定義し、種類ごとのアクセス許可、アクセス時の情報セキュリティ要求事項並びにアクセス方法の監視及び管理を行う。

⑤従業員に対する教育の実施

委託事業者において、情報セキュリティに対する意識の向上を図るために、従業員に対し教育を行うように規定しておく。

⑥提供された情報の目的外利用及び委託事業者以外の者への提供の禁止

委託事業者に提供した情報について、不正な利用を防止させるために、業務以外での利用を禁止する。

⑦業務上知り得た情報の守秘義務

業務中及び業務を終了した後も、情報の漏えいを防止するために、業務上知り得た秘密を漏らしてはならない旨を規定する。

⑧再委託に関する制限事項の遵守

一般的に、再委託した場合、再委託事業者のセキュリティレベルは下がることが懸念されるために、再委託は原則禁止する。例外的に再委託を認める場合には、再委託事業者における情報セキュリティ対策が、他の委託事業者と同等の水準であることを確認し、委託事業者に担保させた上で許可しなければならない。

⑨委託業務終了時の情報資産の返還、廃棄等

委託業務終了時に、不要になった情報資産を返還させるか廃棄させるか等その取扱いについて明確に規定する必要がある。委託終了後の取扱いを明確にすることにより、不要になった情報資産から情報が漏えいする可能性を減らす。なお、マイナンバー利用事務系の領域において取り扱われる機器をリースにより調達しようとする場合には、当該機器についてリース契約終了後、物理的破壊を行う旨、入札における仕様に明記するとともに、契約に位置づけることが望ましい。

⑩委託業務の定期報告及び緊急時報告義務

定期報告及び緊急時報告の手順を定め、委託業務の状況を適正かつ速やかに確認できるようにすることが必要である。緊急時の職員への連絡先は、委託業者に通知しておく必要がある。連絡網には、職員の個人情報が記載される場合もあるため、取扱いに注意する。

⑪地方公共団体による監査、検査

委託事業者が実施する情報システムの運用、保守、サービス提供（クラウドサービス含む）等の状況を確認するため、当該委託事業者に監査、検査を行うことを明確に規定しておくことが必要である。

なお、地方公共団体において、当該委託事業者に監査、検査を行うことが困難な場合は、地方公共団体による監査、検査に代えて、第三者や第三者監査に類似する客観性が認められる委託事業者の内部監査部門による監査、検査又は国際的なセキュリティの第三者認証(ISO/IEC27001 等)の取得等によって確認する。

⑫地方公共団体による情報セキュリティインシデントの公表

委託業務に関し、情報セキュリティインシデントが発生した場合、住民に対し適正な説明責任を果たすため、当該情報セキュリティインシデントの公表を必要に応じ行うことについて、委託事業者と確認しておく。

⑬情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

委託事業者においての情報セキュリティポリシーが遵守されなかったため、被害を受けた場合には、当該委託事業者が損害賠償を行うことを契約書上明記しておく。

(注5) これらの契約項目については、「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」報告書(平成21年3月 総務省)を参照し、「個人情報の取扱いに関する特記仕様書(雛型)」を活用されたい。

(注6) 委託事業者に対して、情報セキュリティポリシーの該当部分について、十分に説明しておくことが必要である。

(注7) 指定管理者制度に関する考慮事項

指定管理者制度においては、条例により、地方公共団体と指定管理者との間で協定を締結することになるが、その協定において、委託内容に応じた情報セキュリティ対策が確保されるよう必要な事項を定める必要がある。

(注8) IT サプライチェーンを構成して提供されるサービスを利用する場合は、委託事業者との関係におけるリスク(サービスの供給の停止、故意又は過失による不正アクセス、委託事業者のセキュリティ管理レベルの低下など)を考慮しそのリスクを防止するための事項について委託事業者と合意し、その内容を文書化しておくことが望ましい。

(注9) 委託事業者に適用される法令としては、法律のほか、各地方公共団体の制定する個人情報保護条例も適用されることを明記しておく必要がある。

(注10) 業務の内容に応じて規定する要件の詳細については、「非機能要求グレード(地方公共団体版)利用ガイド」(平成26年3月 地方自治情報センター)を参照されたい。

(3) 確認・措置等

情報セキュリティ管理者は、委託事業者において十分なセキュリティ対策が実施されているか、定期的に確認し、必要に応じ、改善要求等の措置を講じる必要がある。確認した内容は定期的に統括情報セキュリティ責任者に報告する。個人情報の漏えい等の重大なセキュリティ侵害行為が発見された場合には、速やかに CISO に報告を行う。また、情報セキュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に

把握するため、当該対策による情報システムの変更内容について、速やかに報告させる必要がある。

なお、委託事業者に対する監査については、本ガイドラインの「9.1 監査（4）委託事業者に対する監査」を参照されたい。



## 8.2. 外部サービスの利用（機密性2以上の情報を取り扱う場合）

### 【趣旨】

今後クラウドサービスなどの外部サービスの利用の拡大が見込まれているところ、外部サービスの利用に当たっては、外部サービス基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計した上で、セキュリティを確保する必要がある。

外部サービス提供者に取扱いを委ねる情報は、当該提供者によって適正に取り扱われなければならないが、外部サービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用する可能性があり、自身を含む他の利用者にも関係する情報の開示を受けることが困難になる場合もある。外部サービスを利用して機密性2以上の情報を取り扱う場合は、外部サービス提供者を適正に選択するために、このような外部サービスの特性を理解し、自組織による外部サービス提供者へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分に考慮し、自組織と外部サービス提供者の役割や責任分担を明確にした上で、外部サービスが選定基準及びセキュリティ要件を満たすことを確実にすることが求められる。

さらに、外部サービスを利用する際のセキュリティ対策は、選定や契約時における対策だけでなく、契約後の情報システムの導入・構築、その後の運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要がある。特に外部サービスのサービス内容は非常に速いサイクルで変化しており、利用開始時に行ったセキュリティ対策が途中で無効になることも考えられるため、運用・保守のフェーズにおける対策は定期的に漏れなく実施することが求められる。

<外部サービスの例>

- ・ クラウドサービス
- ・ Web 会議サービス
- ・ SNS（ソーシャルネットワーキングサービス）
- ・ 検索サービス、翻訳サービス、地図サービス
- ・ ホスティングサービス

なお、事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービス（ただし、電気通信サービスや郵便、運送サービス等は除く）では、セキュリティ対策やデータの取扱いなどについて自組織への特別な扱いを求めることができない場合が多く、機密性2以上の情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として機密性2以上の情報を取り扱うことはできない。

### 【例文】

#### (1) 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性2以上の情報を

取り扱う場合)の利用に関する規定を整備すること。

- ①外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準(以下8.2節において「外部サービス利用判断基準」という。)
- ②外部サービス提供者の選定基準
- ③外部サービスの利用申請の許可権限者と利用手続
- ④外部サービス管理者の指名と外部サービスの利用状況の管理

## (2) 外部サービスの選定

- ①情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。
- ②情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。
  - (ア) 外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止
  - (イ) 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制
  - (ウ) 外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制
  - (エ) 外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定
  - (オ) 情報セキュリティインシデントへの対処方法
  - (カ) 情報セキュリティ対策その他の契約の履行状況の確認方法
  - (キ) 情報セキュリティ対策の履行が不十分な場合の対処方法
- ③情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。
- ④情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。
  - (ア) 情報セキュリティ監査の受入れ
  - (イ) サービスレベルの保証
- ⑤情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠

法・裁判管轄を選定条件に含めること。

⑥情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

⑦情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。【推奨事項】

⑧情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

⑨統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

### (3) 外部サービスの利用に係る調達・契約

①情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

②情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

### (4) 外部サービスの利用承認

①情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

②利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

③利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

- (5) 外部サービスを利用した情報システムの導入・構築時の対策
- ①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。
    - (ア) 不正なアクセスを防止するためのアクセス制御
    - (イ) 取り扱う情報の機密性保護のための暗号化
    - (ウ) 開発時におけるセキュリティ対策
    - (エ) 設計・設定時の誤りの防止
  - ②外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。
- (6) 外部サービスを利用した情報システムの運用・保守時の対策
- ①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。
    - (ア) 外部サービス利用方針の規定
    - (イ) 外部サービス利用に必要な教育
    - (ウ) 取り扱う資産の管理
    - (エ) 不正アクセスを防止するためのアクセス制御
    - (オ) 取り扱う情報の機密性保護のための暗号化
    - (カ) 外部サービス内の通信の制御
    - (キ) 設計・設定時の誤りの防止
    - (ク) 外部サービスを利用した情報システムの事業継続
  - ②情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。
  - ③外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。
- (7) 外部サービスを利用した情報システムの更改・廃棄時の対策
- ①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。
    - (ア) 外部サービスの利用終了時における対策
    - (イ) 外部サービスで取り扱った情報の廃棄
    - (ウ) 外部サービスの利用のために作成したアカウントの廃棄
  - ②外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了

時に実施状況を確認・記録すること。

(解説)

(1) 外部サービスに係る規定（外部サービス利用判断基準）の整備

①外部サービスの利用においても、「8.1.業務委託（1）委託事業者の選定基準」で整備を求めている「委託事業者の選定基準」と同等の規定が求められる。また、外部サービス利用者が外部サービスを利用する際の接続方法等（テレワーク等により、外部の通信回線から直接外部サービスにアクセスすることの可否等）についても規定することが必要である。

外部サービスの利用に当たっては、情報の管理や処理を外部サービス提供者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなる。そこで、適切な外部サービス提供者を選定することにより以下のようなリスクを低減することが考えられる。

- ・外部サービスは、そのサービス提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる半面、外部サービス提供者の運用詳細は公開されないために外部サービス利用者にブラックボックスとなっている部分があり、外部サービス利用者の情報セキュリティ対策の運用において必要な情報の入手が困難である。
- ・オンプレミスと外部サービスの併用や外部サービスと他の外部サービスの併用等、多様な利用形態があるため、利用者と外部サービス提供者との間の責任分界点やサービスレベルの合意が容易ではない。
- ・外部サービス提供者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムを一つの外部サービス基盤で共用することとなるため、情報が漏えいするリスクが存在する。
- ・外部サービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスクが存在する。
- ・サーバ装置等機器の整備環境が外部サービス提供者の都合で急変する場合、サプライチェーン・リスクへの対策の確認が容易ではない。

なお、情報セキュリティ確保のために外部サービス利用者自らが行うべきことと、外部サービス提供者に対して求めるべきこと等をまとめたガイドラインについては、以下の取組を参考にするとよい。

参考：内閣官房内閣サイバーセキュリティセンター「クラウドを利用したシステム運用に関するガイダンス」（令和3年11月30日）

([https://www.nisc.go.jp/active/infra/pdf/cloud\\_guidance.pdf](https://www.nisc.go.jp/active/infra/pdf/cloud_guidance.pdf))

参考：総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（2021年9月）

（[https://www.soumu.go.jp/main\\_content/000771515.pdf](https://www.soumu.go.jp/main_content/000771515.pdf)）

参考：経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（2013年度版）

（<https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf>）

参考：経済産業省「クラウドセキュリティガイドライン活用ガイドブック」（2013年度版）

（<https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf>）

参考：公益財団法人 金融情報システムセンター「金融機関におけるクラウド利用に関する有識者検討会報告書」（平成26年11月）

（<https://www.fisc.or.jp/document/fintech/file/1900.pdf>）

#### ②利用申請の許可権限者と外部サービス管理者

例文では、「利用申請の許可権限者」と「外部サービス管理者」を設けることとしているが、小規模の地方公共団体などにおいては、統括情報セキュリティ責任者と利用申請の許可権限者の兼務や情報セキュリティ責任者と外部サービス管理者の兼務など、柔軟に対応することが必要となる。ただし、利用申請を行う職員等が利用申請の許可権限者や外部サービス管理者を兼務することは職務の分離の観点から禁止とする。

#### ③外部サービスの名称

外部サービスの中には複数のサービス（機能）を含んだものが存在する。含まれる個々のサービス（機能）において情報セキュリティの対策が異なる場合は、個々のサービスに分割して申請が必要である。

#### ④外部サービスの利用状況

外部サービスの中には職員等が直接登録し利用可能なものがあり、その利用状況を自組織として一元的に把握するのが困難であることが多い。所属する組織の承認を得ずに職員等が外部サービスを利用することは“シャドーIT”と呼ばれるが、シャドーITは監視が不十分になりやすく、セキュリティリスクが高まる等の問題がある。そのため、シャドーITの対策としては、職員等が外部サービスを利用する場合に必ず申請を行い自組織が承認を行う運用が考えられる。

### (2) 外部サービスの選定

①外部サービスの利用に当たっては、情報の管理や処理を外部サービス提供者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなることを踏まえ、適切な外部サービス提供者を選定することによりリスクを低減することが考えられる。

（注1）外部サービスの利用に当たっては、「地方公共団体におけるASP・SaaS導入活用ガイドライン」（平成22年4月 総務省）を参照されたい。

②インターネットを介して提供される外部サービスの利用に当たっては、外部サービス提供者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、外部サービス提供者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

管轄裁判所に関しては、国外の裁判所で裁判を行うこととならないよう、契約において日本国内の裁判所（必要に応じて地方公共団体の所在地を管轄する裁判所）を合意管轄裁判所として規定する必要がある。また、外国に本社を置く企業が提供するサービスを地方公共団体が利用する場合の紛争を当該企業の本社の所在地を管轄する裁判所が管轄することも考えられる一方、その場合は日本の国内法と同等の個人情報の保護などが確立されないおそれがあることについては利用者である地方公共団体において契約締結の際に十分な留意が必要となる。

(注2) 情報セキュリティ対策その他の契約の履行状況の具体的な確認方法に関しては、「政府機関等の対策基準策定のためのガイドライン」(令和3年7月7日 内閣官房内閣サイバーセキュリティセンター)を参照されたい。

③外部サービスを利用するに当たり、サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することを外部サービスの選定条件とし、仕様内容にも含める必要がある。

- ・取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件
- ・取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

④情報セキュリティ管理者は、外部サービス部分を含む情報の流通経路全般にわたるセキュリティ対策を実施する必要がある。システムの重要度に応じて求められる可用性のレベル等(稼働率、目標復旧時間、バックアップの保管方法など)を十分に検討し、調達の際に、検討した結果を調達仕様書に具体的に盛り込まなければならない。また、必要となる条項(インシデントの報告義務、損害賠償等)を盛り込んだ契約及びサービスレベルを保証させるためのSLAを締結する必要がある。特に、バックアップについては、契約において、各業務システムの重要度を勘案した適切なバックアップレベルを設定し、別途のバックアップの取得など、レベルに応じた適切な対策を実施することが重要である。

(注2) 外部サービスの大規模障害により、自治体の業務に長時間支障が発生した事案を踏まえたセキュリティ対策については、「「Jip-Base」事案を踏まえたクラウドサービスの利用に係る注意喚起」(令和2年5月22日 総行情第76号 総務省自治行政局地域情報政策室長通知)を参照されたい。

(注3) 契約に必要なとなる条項については「8.1. 業務委託(3) 契約項目」及び「地

方公共団体における ASP・SaaS 導入活用ガイドライン」(平成 22 年 4 月 総務省)を参照されたい。また、セキュリティ要件の検討を行う際は、「非機能要求グレード(地方公共団体版)利用ガイド」(平成 26 年 3 月 地方自治情報センター)も併せて参照されたい。

- ⑤情報セキュリティ管理者は、外部サービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

外部サービス提供者及び当該サービスの信頼性が十分であることを総合的に判断するためには、外部サービスで取り扱う情報の機密性・完全性・可用性が確保されるように、外部サービス提供者のセキュリティ対策を含めた経営が安定していること、サービスを提供する基盤環境やアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

このような評価に当たって、外部サービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する必要がある。

なお、選定条件となる認証には、ISO/IEC 27017 によるクラウドサービス分野における ISMS 認証の国際規格がある。また、ISMAP の管理基準を満たすことの確認や ISMAP クラウドサービスリスト等のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービス提供者等のセキュリティに係る内部統制の保証報告書である SOC 報告書(Service Organization Control Report)を活用することを推奨する。外部サービス利用時のセキュリティ対策や内部統制に関する報告書等については、以下を参照されたい。

参考：国際規格

「ISO/IEC 27017 (安全なクラウドサービス利用のための分野別 ISMS 規格)」

参考：日本セキュリティ監査協会

「クラウド情報セキュリティ管理基準」

(<https://jcispa.jasa.jp/documents/>)

「クラウド情報セキュリティ監査制度規程」

([https://jcispa.jasa.jp/cloud\\_security/jcispa\\_regulation/](https://jcispa.jasa.jp/cloud_security/jcispa_regulation/))

参考：日本公認会計士協会「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書(日本公認会計士協会 IT 委員会実務指針第 7 号)」

([https://jicpa.or.jp/specialized\\_field/45\\_8.html](https://jicpa.or.jp/specialized_field/45_8.html))

参考：米国公認会計士協会「Service Organization Control (SOC) Reports」

(<https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html>)

- ⑥目的外利用の禁止



自組織が取り扱う情報は、外部サービス提供者において外部サービスの提供に必要な範囲で利用を認めるものであって、それ以外の目的で利用をさせてはならない。

目的外利用に当たる場合としては、例えば、外部サービス提供者が自組織の利用する外部サービスの契約情報等を保有し、今後の営業活動で利用するなどが考えられる。

#### ⑦本市の意図しない変更が加えられないための管理体制

外部サービス提供者が行う外部サービスの開発及び運用において、「本市の意図しない変更が加えられないための管理体制」が確保されることを求めている。

具体的に外部サービス提供者の選定条件に含める内容としては、例えば以下が考えられる。

- ・外部サービスの開発及び運用において、自組織の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。
- ・外部サービスに自組織の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、自組織と外部サービス提供者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

#### ⑧情報セキュリティインシデントへの対処方法

外部サービス提供者において発生した情報セキュリティインシデントによる被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について、外部サービス提供者の選定条件に含めておくことよい。対処方法についての合意がないと、インシデントが発生しているにもかかわらず外部サービス提供者と連絡がつかない、営業時間外の対応を断られるなどのトラブルになるおそれがあるため、可能な範囲で事前に具体化することが重要である。対処方法には、例えば、復旧を優先する場合は外部サービスの利用を一時的に停止するための手順を規定し、業務継続を優先する場合は、外部サービスの利用を継続した上で情報セキュリティインシデントに対処する手順について、対処の主体とともに規定することが考えられる。また、情報セキュリティインシデントに係る外部サービス提供者と自組織間の情報エスカレーション方法やそのタイミングについて規定することも考えられる。

#### ⑨情報の取扱手順

格付及び取扱制限の明示等、運搬又は送信、消去等の情報の取扱いに関して、外部サービス提供者においても自組織の対策基準に定める内容と同等の取扱いが行われるよう、あらかじめ外部サービス提供者と合意しておくことが重要である。また、外部サービス提供者に提供する情報は必要最小限にとどめる必要があるが、情報システムの利用等において目的外の不必要なアクセスが行われる可能性も考慮し、外部サービス提供者における情報の取扱状況を適宜把握することも重要であ

る。

なお、外部サービス提供者において、業務委託、他の外部サービス等を用いて外部サービスを提供することが考えられる場合は、「8.1. 業務委託」、「8.2. 外部サービスの利用（機密性2以上の情報を取り扱う場合）」の規定を外部サービス提供者においても遵守させるよう仕様書等に規定し、外部サービス提供者とあらかじめ合意しておくことが望ましい。

(注4) 外部サービスには様々なサービスがあり、利用においては以下のような点に留意する必要がある。

- ・ SNS サービスの利用においては、公式アカウントを利用した相談業務等を行う際に、SNS サービス提供事業者とは別の委託先に適切にセキュリティが確保されたシステムを構築させ、相談内容や住民の個人情報が SNS サービス提供事業者側に残らず、委託先等のデータベース等に直接格納・保管されるシステム構成とする必要がある。ただし、機密性2以上の情報を取り扱わない場合は、約款や規約等への同意のみで利用可能となる外部サービスの利用が許容される。
- ・ オンライン申請サービスの利用においては、住民側のスマートフォンアプリ上の QR コードを後日窓口でかざし申請手続を行うようなサービスの場合、住民等の個人情報が外部サービス提供事業者側に残らないシステム構成とする必要がある。
- ・ 検索サービス、翻訳サービス及び地図サービスの利用においては、検索の文言、写真、動画、翻訳の内容及び履歴などがマーケティングや情報収集のために蓄積される場合がある。
- ・ 自組織が直接契約する収納代行業者が SNS サービスを介してキャッシュレスサービスを利用する場合は、自組織が保有する住民等の個人情報をキャッシュレスサービス事業者に提供する仕組みとならない構成とする必要がある。

#### ⑩外部サービスに係るアクセスログ等の証跡の保存

外部サービス上におけるアクセスログ等の証跡に係る保存期間については、情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは1年間以上保存することが望ましい。

なお、記憶媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する（「6.1. コンピュータ及びネットワークの管理 (6)ログの取得等」を参照のこと。）。

#### ⑪外部サービス提供者による情報の管理・保管

情報管理上の問題として、仮に情報が外部サービス上にあつたとしても、当該情報の責任は利用者である情報オーナーが負うことになるため、利用者は外部サービス提供者による情報の管理・保管方法について事前に把握する必要がある。

また、外部サービス提供者が情報の管理・保管を他の事業者へ委託する場合、当該情報が外部サービス利用者の意図しない場面で二次利用されることも懸念され

るため、当該事業者における情報セキュリティ水準や情報の取扱方法に関して外部サービス提供者に確認の上、合意しておく必要がある。

⑫情報開示請求に対する開示項目や範囲

外部サービスに関し、外部サービス提供者が一般に公開している内容以上の情報提供について、情報セキュリティ対策や監査の観点から、事前に自組織と外部サービス提供者が協議の上、外部サービス提供者が提供する内容の項目や範囲を契約において明記することが必要である。また、対象情報の機密性が高い場合、両者間で秘密保持契約（NDA：Non-Disclosure Agreement）を締結するなど必要な措置を講じた上で取得することが求められる。

(3) 外部サービスの利用に係る調達・契約

①調達仕様の内容を契約に含める際、外部サービス提供者との情報セキュリティに関する役割及び責任の範囲が明確になっていることを確認すること。

(4) 外部サービスを利用した情報システムの導入・構築時の対策

①構築時におけるアクセス制御に係る規定を策定する場合、以下を含む内容を規定すること。

(ア) 外部サービスを利用する際に外部サービス提供者が付与又は外部サービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

(イ) 外部サービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御

(ウ) 外部サービスを利用する情報システムの管理者特権を保有する外部サービス利用者に対する強固な認証技術の利用

(エ) 外部サービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことの確認

(オ) 外部サービス上に保存する情報や外部サービスの機能に対してアクセス制御できることの確認

(カ) 外部サービス利用者による外部サービスに多大な影響を与える操作の特定と誤操作の抑制

(キ) 外部サービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施

(ク) インターネット等の外部の通信回線から庁内通信回線を経由せずに外部サービス上に構築した情報システムにログインすることの可否の判断と認める場合の適切なセキュリティ対策の実施

②構築時における暗号化に係る規定を策定する場合、以下を含む内容を規定すること。

(ア) 外部サービス内及び通信経路全般における暗号化の確認

(イ) 利用する情報システムに係る法令や規則に対する暗号化方式の遵守度合い

③構築時における開発に係る規定を策定する場合、以下を含む内容を規定すること。

- (ア) 情報システムの構築において外部サービスを利用する場合の外部サービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用
  - (イ) 情報システムの構築において、外部サービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアの外部サービス上におけるライセンス規定
- ④構築時における設計・設定に係る規定を策定する場合、以下を含む内容を規定すること。
- (ア) 外部サービス上に情報システムを構築する際の外部サービス提供者への設計、構築における知見等の情報の要求とその活用
  - (イ) 外部サービス上に情報システムを構築する際の設定の誤りを見いだすための対策
  - (ウ) 外部サービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視
  - (エ) 利用する外部サービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測
  - (オ) 利用する外部サービス上で可用性 2 の情報を取り扱う場合の可用性を考慮した設計
  - (カ) 外部サービス内における時刻同期の方法の確認
- (5) 外部サービスを利用した情報システムの運用・保守時の対策
- ①統括情報セキュリティ責任者は、運用・保守時における利用方針に係る規定を策定する場合、以下を含む内容を規定すること。
- (ア) 責任分界点を意識した外部サービスの利用
  - (イ) 利用承認を受けていない外部サービスの利用禁止
  - (ウ) 外部サービス提供者に対する定期的なサービスの提供状態の確認
  - (エ) 利用する外部サービスに係る情報セキュリティインシデント発生時の連絡体制
- ②統括情報セキュリティ責任者は、運用・保守時における教育に係る規定を策定する場合、以下を含む内容を規定すること。
- (ア) 外部サービス利用のための規定及び手順について
  - (イ) 外部サービス利用に係る情報セキュリティリスクとリスク対応について
  - (ウ) 外部サービス利用に関する適用法令や関連する規制等について
- ③統括情報セキュリティ責任者は、運用・保守時における資産管理に係る規定を策定する場合、以下を含む内容を規定すること。
- (ア) 外部サービス上で利用する IT 資産の適切な管理
  - (イ) 外部サービス上に保存する情報に対する適切な格付・取扱制限の明示
  - (ウ) 外部サービスの機能に対する脆弱性対策について、外部サービス利用者の責任範囲の明確化と対策の実施
- ④統括情報セキュリティ責任者は、運用・保守時におけるアクセス制御に係る規定を

策定する場合、以下を含む内容を規定すること。

(ア) 管理者権限を外部サービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

(イ) 外部サービス利用者へ割り当てたアクセス権限に対する定期的な見直し

(ウ) 外部サービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限

(エ) 利用する外部サービスの不正利用の監視

⑤統括情報セキュリティ責任者は、運用・保守時における暗号化に係る規定を策定する場合、以下を含む内容を規定すること。

(ア) 暗号化に用いる鍵の管理者と鍵の保管場所

(イ) 鍵管理機能を外部サービス提供者が提供する場合の鍵管理手順と鍵の種類情報の要求とリスク評価

(ウ) 鍵管理機能を外部サービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

⑥統括情報セキュリティ責任者は、運用・保守時における通信に係る規定を策定する場合、以下を含む内容を規定すること。

(ア) 利用する外部サービスのネットワーク基盤が他のネットワークと分離されていることの確認

⑦統括情報セキュリティ責任者は、運用・保守時における設計・設定に係る規定を策定する場合、以下を含む内容を規定すること。

(ア) 外部サービスの設定を変更する場合の設定の誤りを防止するための対策

(イ) 外部サービス利用者が行う可能性のある重要操作の手順書の作成と監督者の指導の下での実施

⑧統括情報セキュリティ責任者は、運用・保守時における事業継続に係る規定を策定する場合、以下を含む内容を規定すること。

(ア) 不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施（外部サービス提供者が提供する機能を利用する場合は、その実施の確認）

(イ) 可用性2の情報を外部サービスで取り扱う場合の十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施

(ウ) 外部サービス提供者からの変更通知の内容確認と復旧手順の確認

(エ) 外部サービスで利用しているデータ容量、性能等の監視

⑨情報セキュリティ責任者は、運用・保守時におけるインシデント対応に係る規定を策定する場合、以下を含む内容を規定すること。

(ア) 外部サービス上での情報セキュリティインシデント、情報の目的外利用等を認知した場合の外部サービス管理者への報告

(イ) 外部サービス管理者がインシデント報告を受けた場合の対応

(6) 外部サービスを利用した情報システムの更改・廃棄時の対策

- ①統括情報セキュリティ責任者は、更改・廃棄時における利用終了手順に係る規定を策定する場合、以下を含む内容を規定すること。
  - (ア) 外部サービスの利用を終了する場合の移行計画書又は終了計画書の作成
  - (イ) 移行計画書又は終了計画書の外部サービス利用者への事前通知
- ②統括情報セキュリティ責任者は、更改・廃棄時における情報の廃棄に係る規定を策定する場合、以下を含む内容を規定すること。なお、情報資産の廃棄は「2. 情報資産の分類と管理 (2) 情報資産の管理 ⑩情報資産の廃棄」、「4. 1. サーバ等の管理 (7) 機器等の廃棄」を参照すること。
  - (ア) 情報の廃棄方法
    - (イ) 基盤となる物理機器の廃棄
- ③統括情報セキュリティ責任者は、更改・廃棄時におけるアカウントの廃棄に係る規定を策定する場合、以下を含む内容を規定すること。
  - (ア) 作成された外部サービス利用者アカウントの削除
  - (イ) 利用した外部サービス管理者アカウントの削除・返却と再利用の確認
  - (ウ) 外部サービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

### 8.3. 外部サービスの利用（機密性2以上の情報を取り扱わない場合）

#### 【趣旨】

機密性2以上の情報を取り扱わない場合であって、外部サービス提供先における高いレベルの情報管理を要求する必要がない場合においても、種々の情報を送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断して利用することが求められる。一方、機密性2以上の情報を取り扱う場合と同等のセキュリティ対策を求めることは外部サービスの利用推進を妨げるものであるため、機密性2以上の情報を取り扱わない前提で外部サービスを利用する場合は、「8.3. 外部サービスの利用（機密性2以上の情報を取り扱わない場合）」で定めた遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

#### 【例文】

##### (1) 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性2以上の情報を取り扱わない場合）の利用に関する規定を整備すること。

- (ア) 外部サービスを利用可能な業務の範囲
- (イ) 外部サービスの利用申請の許可権限者と利用手続
- (ウ) 外部サービス管理者の指名と外部サービスの利用状況の管理
- (エ) 外部サービスの利用の運用手順

##### (2) 外部サービスの利用における対策の実施

- ①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性2以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。
- ②情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

#### (解説)

##### (1) 外部サービスの利用に係る規定の整備

①統括情報セキュリティ責任者は、以下のようなリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、許可する業務の範囲を決定する必要がある。

##### (ア) 検討すべきリスクの例

- ・外部サービス提供者は、保存された情報を自由に利用することが可能である。また、約款、利用規約等でその旨を条件として明示していない場合がある。加えて、外部サービス提供者は、利用者から収集した種々の情報を分析し、利用者の関心

事項を把握し得る立場にある。

- ・情報が改ざんされた場合でも、利用形態によっては外部サービス提供者が一切の責任を負わない場合がある。
- ・外部サービス提供者が海外のデータセンター等にサーバ装置を設置してサービスを提供している場合は、当該サーバ装置に保存されている情報に対し、現地の法令等が適用され、現地の政府等による検閲や接收を受ける可能性がある。
- ・突然サービス停止に陥ることがある。また、その際に預けた情報の取扱いは保証されず、損害賠償も行われなない場合がある。約款の条項は一般的にサービス提供者に不利益が生じないようにしており、このような利用条件に合意せざるを得ない。また、サービスの復旧についても保証されない場合が多い。
- ・保存された情報が誤って消去又は破壊されてしまった場合に、サービス提供者が情報の復元に応じない可能性がある。また、復元に応じる場合でも復旧に時間がかかることがある。
- ・約款及び利用規約の内容が、外部サービス提供者側の都合で利用開始後事前通知等無しで一方的に変更されることがある。
- ・情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。
- ・利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、万が一対応を承諾された場合でも、その対応には時間を要することが多い。

②統括情報セキュリティ責任者は、自組織において機密性2以上の情報を取り扱わない前提で外部サービスを業務に利用する場合は、以下を例に利用手続を定めること。

(ア) 利用申請の許可権限者

(イ) 利用申請時の申請内容

- ・外部サービスの名称（必要に応じて機能名までを含む）
- ・外部サービス提供者の名称
- ・利用目的（業務内容）
- ・取り扱う情報の格付
- ・利用期間
- ・利用申請者（所属・氏名）
- ・利用者の範囲（自組織の関係者内に限る、部局内に限る など）
- ・選定時の確認結果

③情報セキュリティ責任者は、機密性2以上の情報を取り扱わない場合の外部サービスの利用状況を、以下を例に管理すること。

(ア) 利用申請の許可権限者は、申請ごとに外部サービス管理者を指名すること。

(イ) 利用承認した外部サービスは、その内容を遅滞なく記録するよう運用ルールを定め、常に最新の外部サービスの利用状況を把握できるようにする。記録する際は、以下を例とする項目を記録し自組織内で共有すること。



- ・外部サービスの名称（必要に応じて機能名までを含む）
  - ・外部サービス提供者の名称
  - ・利用目的（業務内容）
  - ・取り扱う情報の格付
  - ・利用期間
  - ・利用申請者（所属・氏名）
  - ・利用者の範囲（自組織の関係者内に限る、部局内に限る など）。
  - ・外部サービス管理者（所属・氏名）
- ④情報セキュリティ責任者は、機密性 2 以上の情報を取り扱わない前提で外部サービスを業務に利用する場合は、以下を例に運用手順定めること。
- (ア) サービス利用中の安全管理に係る運用手順
- ・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
  - ・情報の滅失、破壊等に備えたバックアップの取得
  - ・利用者への定期的な注意喚起（禁止されている機密性 2 以上の情報の取扱いの有無の確認等）
- (イ) 情報セキュリティインシデント発生時の連絡体制

## 9. 評価・見直し

### 9.1. 監査

#### 【趣旨】

情報セキュリティポリシーの実施状況について、客観的に専門的見地から評価を行う監査が実施されない場合は、情報セキュリティ対策が徹底されない状態や情報セキュリティポリシーが業務に沿わない状態が続くおそれがある。このことから、監査の実施及びその方法について規定する。

監査を行う者は、十分な専門的知識を有するものでなければならない。また、適正な監査の実施の観点から、監査の対象となる情報資産に直接関係しない者であることが望ましい。また、地方公共団体内の情報セキュリティ対策の監査・報告について中立性を保証され、監査に必要な情報へのアクセス等の権限が明確に与えられる必要がある。監査作業に伴う情報の漏えいのリスクを最小限とするため、監査人等が取り扱う監査に係る情報について、漏えい、紛失等が発生しないように保管する必要がある。

#### 【例文】

##### (1) 実施方法

CISOは、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

##### (2) 監査を行う者の要件

- ①情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。
- ②監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

##### (3) 監査実施計画の立案及び実施への協力

- ①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。
- ②被監査部門は、監査の実施に協力しなければならない。

##### (4) 委託事業者に対する監査

事業者が業務委託を行っている場合、情報セキュリティ監査統括責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

(5) 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

(6) 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

(7) 監査結果への対応

CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

(8) 情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

(解説)

(1) 実施方法

情報セキュリティ対策状況に対して、定期的な監査だけでなく、様々な状況に対応して監査が行えることを定めておく必要がある。随時監査を行うことを明確にすることにより、情報セキュリティポリシーの違反行為に対する抑止効果も期待できる。

(2) 監査を行う者の要件

内部監査、外部監査、いずれの場合も、監査人は、監査対象範囲から独立性を有し、公平な立場で客観的に評価を行うことが求められる。監査人は、監査及び情報セキュリティについて、十分な専門的知識を有する者でなければならない。

(注1) 一部又は全部の監査対象範囲に対して、小規模な組織等の理由によって、独立性を維持することができない場合又は組織内に十分な専門的知識を有する者が確保できない場合は、必要な範囲に対して外部の監査人を利用することを検討することが必要である。また、職員等が自らが所属しないその他の部門に対して監査をする相互監査や近隣の地方公共団体との相互監査も有効である。

(注2) 監査業務を事業者に請け負わせる場合には、経済産業省が定める「情報セ

セキュリティサービス基準」及び当該基準を満たすと認められた企業を記載した「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監査サービスに係る部分）を活用することも考えられる。

（注3）監査人は、監査項目が実施できているか否かだけでなく適正な記録が取得されているかについても確認する必要がある。また、監査項目が実施できていない又は適正な記録が取得されていない場合は、なぜできていないのかその原因にまで踏み込んで分析・報告できることが望ましい。

### （3） 監査実施計画の立案及び実施への協力

情報セキュリティ監査統括責任者は、情報セキュリティ監査を行うに当たって、監査人の権限、監査実施に関する項目及び内容を定め、これに基づいて監査実施計画を立案する。監査人は、この計画に基づき監査を実施する。なお、システムに対する監査の実施によって業務が中断される可能性があるため、計画の立案に当たっては中断のリスクを最小限に抑えるよう配慮することが必要である。また、システム監査を行うツールにより、監査人は特権的にデータ等へアクセスし得ることから、誤用・悪用を防止するための適正な管理が求められる。

（注4）情報セキュリティ監査統括責任者は、監査計画及びそれに付随するリスクを効果的かつ効率的に管理するのに必要な資質、並びに次の領域における知識及び技能を有することが望ましい。ただし、必要な資質、並びに知識及び技能を有することが困難な場合は、外部の専門家をあてて能力を補完することも考えられる。

- ・ 監査の原則、手順及び方法に関する知識
- ・ マネジメントシステム規格及び基準文書に関する知識
- ・ 被監査部門の業務、製品及びプロセスに関する知識
- ・ 被監査部門の業務及び製品に関し、適用される法的及びその他の要求事項に関する知識
- ・ 該当する場合には、被監査部門の利害関係者に関する知識

また、情報セキュリティ監査統括責任者は、監査計画を管理するのに必要な知識及び技能を維持するために適正な専門能力の継続的開発・維持活動に積極的にかかわることが望ましい。

（注5）監査項目には、庁内外において発生した情報セキュリティインシデントから学んだ対策等の遵守状況の確認や、電磁的記録媒体の管理、情報の持ち出し管理、ソフトウェアライセンス管理、FAX 誤送信防止策等の具体的な情報セキュリティ対策の運用状況の確認も含まれることが望ましい。

### （4） 委託事業者に対する監査

情報システムの運用、保守等を業務委託している場合は、情報資産の管理が契約に従い適正に実施されているかを点検、評価する必要がある。また、これによって、セキュリティ侵害行為に対する抑止効果も期待できる。

### （5） 報告

情報セキュリティ監査統括責任者は、監査調書をもとに、被監査部門に対する監査人の指摘事項の正確性や指摘に対する改善提案の実現性を確認し監査報告書を作成し、監査報告書を情報セキュリティ委員会に報告する。

CISO は、監査報告を受けて、被監査部門に改善を指示する。被監査部門は、改善計画を立案し実施する。最後に監査人は、フォローアップ監査により、改善状況や改善計画の完了について確認を行う必要がある。

(6) 保管

監査により作成した監査調書には、脆弱性の情報等機微な情報が含まれていることが多いことから、情報セキュリティ監査統括責任者は、紛失等が生じないように保管する必要がある。

(7) 監査結果への対応

監査結果を適正にセキュリティ改善に結び付けるため、CISO に関係部局への指示を義務付けた規定である。また、監査の指摘事項と同種の課題が他の部署にも存在する可能性があることから、当該可能性の高い部署に対しては、課題や問題点の有無を確認させる必要がある。

(8) 情報セキュリティポリシー及び関係規程の見直し等への活用

監査結果は、情報セキュリティポリシー及び関係規程の見直し等の基礎資料として活用しなければならない。

(注6) 情報セキュリティ監査の実施方法等については、「地方公共団体における情報セキュリティ監査に関するガイドライン」(令和4年3月 総務省)及び「地方公共団体情報セキュリティ管理基準解説書」(平成17年2月 総務省)を参考にされたい。

## 9.2. 自己点検

### 【趣旨】

情報セキュリティポリシーの履行状況等を自ら点検、評価することは、情報セキュリティポリシーの遵守事項を改めて認識できる有効な手段である。自己点検は、情報システム等を運用する者又は利用する者自らが実施するので、監査のような客観性は担保されないが、監査と同様に、点検結果を踏まえ各部門で改善を図ったり、組織全体のセキュリティ対策の改善を図る上での重要な情報になる情報セキュリティ対策の評価を行い、対策の見直しに資するものである。また、職員等の情報セキュリティに関する意識の向上や知識の習得にも有効である。

このことから、自己点検を定期的実施する規定を設け、その活用方法とあわせて規定する。

### 【例文】

#### (1) 実施方法

- ①統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。
- ②情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

#### (2) 報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

#### (3) 自己点検結果の活用

- ①職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。
- ②情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

(解説)

(1) 実施方法

情報セキュリティ対策の実施状況について、定期的な自己点検だけでなく、様々な状況に対応して自己点検を実施する。

(注1) 自己点検は自己点検票を用いた、アンケート方式で行う場合が多い。

アンケートを行う場合に留意すべき点は、そのセキュリティ対策上担う役割に応じたアンケート項目とすることである。アンケートは、回答者による再認識や新たな発見にもつながり得る。アンケート項目によって、自部門の対策で、何が欠落しているのか鮮明にすることが可能になるために、改善の必要性の認識をさせられる効果もある。

(注2) 保有する個人情報の人的な要因による漏えいを踏まえた点検については、「地方公共団体の保有する情報資産の管理状況等の再点検について(周知)」(平成24年10月29日 総行情第71号 総務省自治行政局地域情報政策室長通知)及び「地方公共団体における個人情報の漏洩防止対策について(注意喚起)」(平成25年8月5日 総務省 事務連絡)を参照されたい。

(注3) 技術的な脆弱性の悪用に対する点検については、「地方公共団体等が管理するウェブサイトに係る脆弱性の確認及び対策の点検・実施等について(依頼)」(平成24年9月26日 総行情第66号 総務省自治行政局地域情報政策室長通知)を参照されたい。

(2) 報告

情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価することが望ましい。また、統括情報セキュリティ責任者は、共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価することが望ましい。

(3) 自己点検結果の活用

自己点検結果は、職員等が自らの業務の見直しに活用するとともに、監査結果と同様に、情報セキュリティポリシーの見直し等の情報として活用することができる。

(注4) 総務省が平成18年3月に公表した「地方公共団体の情報セキュリティレベルの評価に係る制度の在り方に関する調査研究報告書」の参考資料である「情報セキュリティレベル評価ツール」を自己点検に用いることも可能である。

### 9.3. 情報セキュリティポリシー及び関係規程等の見直し

#### 【趣旨】

情報セキュリティ対策は、情報セキュリティに関する脅威や技術等の変化に応じて、必要な対策が変化するものであり、情報セキュリティポリシー及び関係規程等は、定期的に見直すことが求められる。また監査や自己点検の結果等から、同ポリシー及び関係規程等の見直しの必要性が確認される場合もある。

このことから、情報セキュリティポリシー及び関係規程等の見直しについて規定する。

#### 【例文】

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認められた場合、改善を行うものとする。

#### (解説)

情報セキュリティ委員会は、情報セキュリティインシデント、監査や自己点検の結果を受けて、情報セキュリティ分野の専門家による評価や保有する情報システムに関するリスク評価の結果等を活用しつつ、情報セキュリティポリシー及び関係規程等の見直しを行う。

また、情報セキュリティポリシー及び関係規程等は、組織にとっての脅威の変化や組織体制の変更、新たな対策技術の提供等によっても見直すべきものであり、あらかじめ定めた間隔及び重大な変化が発生した場合等、状況に応じて柔軟に運用していくことが必要である。

(注1) 見直しに当たっては、情報セキュリティポリシー及び関係規程等と実態との相違を十分考慮することが重要であり、関係部局から意見聴取等を行い、実態把握を行うことが望ましい。また、情報セキュリティポリシー及び関係規程等を見直す際には、必要に応じてリスク分析の見直しを行うことが重要である。日頃から新たな攻撃方法や対策技術の情報収集に努め、情報セキュリティポリシー及び関係規程等の見直しに活用することも必要である。

(注2) 情報セキュリティポリシー及び関係規程等の見直しは、地方公共団体の長及びこれに準じる者の決裁により正式に決定される。

(注3) 情報セキュリティポリシー及び関係規程等を見直した際には、その内容を職員等や委託事業者十分に周知する必要がある。

(注4) 見直しの際は、情報セキュリティポリシー及び関係規程等に次の事項によって生じる要求事項が含まれているか確認すること。

- ・事業計画



- ・規制、法令及び契約
- ・現在及び将来予想される情報セキュリティの脅威環境

## 10. 用語の定義

本ガイドラインにおいて次の各号に掲げる用語の定義は、当該各号に定めるところによる。

### 【あ】

- 「遠隔消去機能」

「遠隔消去機能」→「リモートワイプ機能」を参照。

- 「暗号化消去」

「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。

- 「Web（ウェブ）会議サービス」

「Web（ウェブ）会議サービス」とは、専用のアプリケーションや Web ブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。

### 【か】

- 「外部サービス」

「外部サービス」とは、事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。

- 「外部サービス管理者」

「外部サービス管理者」とは、外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。

- 「外部サービス提供者」

「外部サービス提供者」とは、外部サービスを提供する事業者をいう。外部サービスを

利用して自組織に向けて独自のサービスを提供する事業者は含まれない。

● 「外部サービス利用者」

「外部サービス利用者」とは、外部サービスを利用する自組織の職員等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう

● 「供給者」

「供給者」とは、サプライチェーンの一部を構成し、データの処理やサービス等で連携する組織をいう。

● 「クラウドサービス」

「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。この構成要素として、SaaS (Software as a Service)、PaaS (Platform as a Service)、IaaS (Infrastructure as a Service) が存在する。

【さ】

● 「サプライチェーン」

「サプライチェーン」とは、部品やサービス等の供給に多種多様な主体が係わった取引の連鎖をいう。

● 「シンクライアント」

「シンクライアント」とは、サーバ側に仮想的なクライアント環境を設けた上で、当該クライアント環境にパソコンやモバイル端末が専用のアプリケーションを使用してアクセスし、パソコンやモバイル端末にデータを保存せずに、データの閲覧や編集を行うことを可能とする機能をいう。

● 「事業継続計画」

「事業継続計画」 → 「BCP」を参照。

● 「情報セキュリティインシデント」

「情報セキュリティインシデント」とは、望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の

遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

● 「情報セキュリティ事象」

情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象

● 「送信ドメイン認証技術」

「送信ドメイン認証技術」とは、メール送信者情報のドメインが正しいものかどうかを検証することができる仕組みをいう。現在のメール送信においては、送信者情報を詐称することが可能で、実際、多くの迷惑メールは他のアドレスになりすまして送られているため、成りすまし対策として用いられる。

● 「ソーシャルメディアサービス」

「ソーシャルメディアサービス」とは、インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持った Web サイトやネットサービスなどを総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。

【た】

● 「多要素認証」

「多要素認証」とは、システムが正規の利用者かどうかを判断する際の信頼性を高めるために、複数の認証手段を組み合わせる方式をいう。認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。それぞれの認証手段には各々異なった利点と欠点があり、複数の認証方式を組み合わせることが利用者認証の信頼性を高める意味でも有効である。

● 「端末」

「端末」とは、情報システムの構成要素である機器のうち、職員が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りが無い限り、地方公共団体が調達又は開発するものをいう。

● 庁内ネットワーク

「庁内ネットワーク」とは、地方公共団体の庁舎・出先機関を含めた団体が管理主体となるネットワーク及び同ネットワークを委託しているデータセンターに設置している情報システムをいう。

● 「電子署名」

「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。

● 「特権 ID」

「特権 ID」とは、サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常の ID よりもシステムに対するより高いレベルでの操作が可能な ID をいう。

● 「ドメイン名」

「ドメイン名」とは、国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。

【は】

● 「パソコン」

「パソコン」とは、端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

● 「標的型攻撃」

「標的型攻撃」とは、明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

【ま】

● 「モバイル端末」

「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【ら】

● 「リスク分析」

「リスク分析」とは、リスク特定、リスク分析、リスク評価を網羅するプロセス全体を指す。リスク分析を行った後、リスク対応を行う。リスク対応の手段には、リスク源の除去、起こりやすさの変更、結果の変更、他者とのリスクの共有、リスクの保有などがある。

● 「リモートワイプ機能」

「リモートワイプ機能」とは、携帯電話などに記録してあるデータを、当該端末から操作するのではなく離れた場所から、遠隔操作（リモート）で、消去、無効化する機能をいう。携帯電話を紛失したり盗難にあった場合の、情報漏えいを防ぐ目的で利用される。

## 【A～Z】

### ● 「BCP (Business Continuity Plan : 事業継続計画)」

「BCP」とは、組織において特定する事業の継続に支障をきたすと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適正に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。

### ● 「CRYPTREC (Cryptography Research and Evaluation Committiees)」

「CRYPTREC」とは、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。

### ● 「CSIRT (Computer Security Incident Response Team)」

「CSIRT」とは、コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う組織の総称。

### ● 「SLA (Service Level Agreement)」

「SLA」とは、サービス提供者と利用者との間でサービス内容に関し明示的になされた合意であり、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を決定し、サービス提供者に保証させることをいう。

### ● 「URL (Uniform Resource Locator)」

「URL」とは、インターネット上の情報資源の場所とその属性を指定する記述方式。情報資源の種類やアクセス方法、情報を提供するウェブサーバの識別名、ファイルの所在を指定するパス名などで構成される。

### ● 「VPN (Virtual Private Network)」

「VPN」とは、暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術である。

# 第4編

## 付録



(目次)

第4編 付録 .....	iv-1
付録1 権限・責任等一覧表 .....	iv-5

# 権限・責任等一覧表

付録1 権限・責任等一覧表

(目次)

付録 1 権限・責任等一覧表 ..... iv-5

# 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ委員会	情報セキュリティ責任者	最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報セキュリティ管理者	情報セキュリティ担当者	情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	情報セキュリティ許可権限者	利用申請の管理者	外部サービスの職員の義務	CSIRT(統一的窓口)	外部委託関係規定		
1 組織体制	(1)	① 最高情報セキュリティ責任者の設置		○															
		② 最高情報セキュリティアドバイザーの設置		○															
		③ CSIRTの整備		○															
		④ 最高情報セキュリティ副責任者の設置		○															
		⑤ 対策基準に定められた担務の委譲		○	△	△	△	△					△						
	(2)	① 統括情報セキュリティ責任者の設置		△	○														
		② ネットワークにおける開発等の権限及び責任			○														
		③ ネットワークにおける情報セキュリティ対策に関する権限及び責任			○														
		④ 情報セキュリティ責任者等に対する指導及び助言			○	△	△	△	△										
		⑤ 情報資産に対するセキュリティ侵害が発生した場合等の権限及び責任		△	○														
		⑥ 情報セキュリティ実施手順の維持・管理の権限及び責任			○														
		⑦ 最高情報セキュリティ責任者等との連絡体制の整備		△	○	△	△	△	△										
		⑧ 緊急時の報告と回復のための対策		△	○														
		⑨ 情報セキュリティ関係規程に係る課題及び問題点の報告		△	○														
	(3)	① 情報セキュリティ責任者の設置					○												
		② 部局等の情報セキュリティ対策に関する統括的な権限及び責任					○												
		③ 部局等の情報システムの開発等の統括的な権限及び責任					○												
		④ 部局等の情報システムにおける連絡体制の整備等					○												
	(4)	① 情報セキュリティ管理者の設置						○											
		② 課室等の情報セキュリティ対策に関する権限及び責任						○											
		③ 情報資産に対するセキュリティ侵害が発生した場合等の報告等		△	△	△	○												
	(5)	① 情報システム管理者の設置							○										
		② 情報システムにおける開発等の権限及び責任							○										
		③ 情報システムにおける情報セキュリティに関する権限及び責任							○										
		④ 情報システムに係る情報セキュリティ実施手順の維持・管理							○										
	(6)	情報システム担当者の設置							△	○									
	(7)	① 情報セキュリティ委員会の設置	○																
		② 情報セキュリティ対策の改善計画の策定、実施状況の確認	○																
	(8)	① 情報セキュリティ対策の実施における承認等の申請者とその承認者等の兼務の禁止																	
		② 監査を受ける者と監査を実施する者の兼務の禁止																	
	(9)	① CSIRTの整備		○															
		② CSIRTに属する職員等の選任		○	△	△	△	△											
		③ 情報セキュリティに関する統一的な窓口の設置		○															
		④ セキュリティ戦略の意思決定が行われた際に、内容を関係部局等に提供		△	△	△	△	△										○	
		⑤ 情報セキュリティインシデントの関係機関への報告																	○
		⑥ 情報セキュリティインシデントの報道機関への通知・公表等																	○
		⑦ 情報セキュリティに関する他の関係機関や窓口等との情報共有																	○

## 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ委員会	情報セキュリティ責任者	最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報セキュリティ担当者	情報システム担当者	監査統括責任者	情報セキュリティ許可権限者	利用申請の管理者	外部サービスの管理者	職員等の義務(統一的窓口)	CSIRT	外部委託関係規定					
2 情報資産の分類と管理	(1)	情報資産の分類																			
	(2)	①	(ア)	情報資産の管理責任													○				
			(イ)	複製等された情報資産の管理責任													○				
		②	情報資産の分類の表示																		
		③	(ア)	業務上必要のない情報の作成の禁止															○		
			(イ)	情報作成時の情報の分類と取扱制限の設定													○				
			(ウ)	作成途上の情報の取扱い													○				
		④	(ア)	庁内の者が作成した情報資産の取扱い													○				
			(イ)	庁外の者が作成した情報資産の分類と取扱い													○				
			(ウ)	分類が不明な情報資産を入手した際の対応													△				
		⑤	(ア)	情報資産の業務外目的の利用の禁止															○		
			(イ)	情報資産の分類に応じた適正な取扱い													○				
			(ウ)	情報資産の分類が異なる電磁的記録媒体の取扱い													○				
		⑥	(ア)	情報資産の分類に応じた適正な保管															○	○	
			(イ)	長期保管する情報資産を記録した電磁的記録媒体の保管													○	○			
			(ウ)	利用頻度の低い電磁的記録媒体等の保管													○	○			
			(エ)	電磁的記録媒体の施設可能な場所への保管													○	○			
		⑦	電子メール等での送信時の対策																	○	
		⑧	(ア)	車両等での情報資産運搬時の対策																	○
			(イ)	情報資産運搬の許可													許		○		
		⑨	(ア)	情報資産の外部への提供時の対策																	○
			(イ)	情報資産の外部への提供の許可													許		○		
			(ウ)	住民に公開する情報資産の取扱い													○				
		⑩	(ア)	情報資産廃棄時やリース返却時等の対策																	○
			(イ)	情報資産廃棄時やリース返却時等の処理の記録															○		
			(ウ)	情報資産廃棄時やリース返却時等の許可													許		○		
	3 情報システム全体の強靱性の向上	(1)	①	マイナンバー利用事務系と他の領域との分離															○	○	
		②	(ア)	情報のアクセス対策																	○
			(イ)	情報の持ち出し不可設定																	○
		(2)	①	LGWAN接続系とインターネット接続系の分割															○	○	
		(3)	①	高度な情報セキュリティ対策															○	○	
			②	自治体情報セキュリティクラウドの導入															○	○	
			③	βモデルやβ'モデルを採用する場合の外部確認と外部監査															○	○	



## 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ委員会	最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報セキュリティ担当者	情報システム管理者	情報システム担当者	監査統括責任者	情報セキュリティ許可権限者	利用申請の管理者	外部サービスの管理者	職員等の義務(統一的窓口)	CSIRT	外部委託関係規定		
5 人的セキュリティ	5.1 職員等の遵守事項	(1) ①	情報セキュリティポリシー等の遵守				△							○				
		②	情報資産の業務目的以外での使用の禁止												○			
		③	(ア)	情報資産の外部での処理時の安全管理措置		○												
			(イ)	モバイル端末や電磁的記録媒体等の持ち出しの許可				許								○		
			(ウ)	外部での情報処理業務の許可				許								○		
		④	(ア)	支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用禁止												○		
				支給以外の端末の業務利用可否判断		○												
				支給以外の端末の業務利用に係る実施手順			○	許										
			(イ)	支給以外のパソコン、モバイル端末及び電磁的記録媒体等の安全管理措置				許								○		
		⑤	端末等の持出及び持込の記録等				○											
	⑥	パソコンやモバイル端末におけるセキュリティ設定変更の禁止				許									○			
	⑦	机上の端末等の管理				許									○			
	⑧	退職時等の遵守事項													○			
	(2)	①	非常勤職員等の採用時の対応				○									△		
		②	非常勤職員等の採用時の同意書への署名				○									△		
		③	インターネット接続等の利用の制限				○									△		
	(3)	情報セキュリティポリシー等の掲示				○									△			
	(4)	委託事業者に対する説明				○											△	
	5.2 研修・訓練	(1)	情報セキュリティに関する研修・訓練の実施		○													
		(2)	①	研修計画の策定等	承	○												
②			情報セキュリティ研修の受講												○			
③			新規採用の職員等に対する研修の実施		○											△		
④			理解度等に応じた研修の実施		○	△	△	△	△	△						△		
⑤			所管する課室等の研修実施状況の記録及び報告			△	△	○										
⑥			研修実施状況の分析、評価及び報告		△	○												
⑦			研修の受講状況の報告	△	○													
(3)		緊急時対応訓練の実施		○														
(4)		研修・訓練の参加義務													○			
5.3 情報セキュリティインシデントの報告	(1)	①	情報セキュリティインシデントの報告				△							○	△			
		②	情報システムに関連する報告			△	○	△								△		
		③	情報セキュリティインシデントの必要に応じた報告		△		△	○										
	(2)	①	住民等外部からの報告時の対応				△								○			
		②	情報システム又はネットワークに関連する情報セキュリティインシデントの報告			△	○	△										
		③	情報セキュリティインシデントに関する報告		△		△	○										
		④	住民等外部に対する窓口の設置等		○													
	(3)	①	情報セキュリティインシデントの可能性に対する評価													○		
		②	情報セキュリティインシデントの報告		△											○		
		③	応急措置の実施及び復旧に係る指示			△	△	△	△	△					△	○		
		④	情報セキュリティインシデントの原因の究明、記録の保存、再発防止策の報告		△											○		
		⑤	再発防止策の実施に必要な措置の指示		○												△	

## 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)		項目		情報セキュリティ委員会	情報セキュリティ責任者	最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報セキュリティ担当者	情報セキュリティ監査統括責任者	情報セキュリティ許可権限者	利用申請の管理者	外部サービスの管理者	職員等の義務(統一的窓口)	CSIRT	外部委託関係規定	
5.4 ID及びパスワード等の管理	(1)	①	(ア) 認証に用いるICカード等の職員等間共有の禁止												○			
			(イ) ICカード等のカードリーダー等への常時挿入禁止													○		
			(ウ) ICカード等紛失時の通報			△				△						○		
		②	ICカード紛失時のアクセス停止措置			○			○									
		③	ICカード切り替え時の旧カードの廃棄方法			○			○									
	(2)	①	自己のIDの他人による利用の禁止													○		
		②	共用ID利用者以外による共用ID利用禁止													○		
	(3)	①	パスワードの管理													○		
			パスワードの秘密保持													○		
		②	パスワードの文字及び文字数の選択													○		
			パスワードが流出したおそれのある時の措置							△						○		
		③	パスワードのシステム間の共有禁止													○		
			仮パスワードの変更													○		
			パスワードの記憶機能の利用禁止													○		
			職員等間でのパスワード共有禁止													○		
	6 技術的セキュリティ	(1)	①	文書サーバの容量の設定等							○							
②			文書サーバの課室等单位での構成							○								
③			特定の情報のためのディレクトリ設定							○								
(2)		定期的なバックアップの実施			○				○									
(3)		他団体との情報システムに関する情報等の交換する場合の許可等			許	許			○									
(4)		①	情報システムの運用に係る作業記録の作成							○								
		②	システム変更等時の作業内容の記録作成等			○				○								
		③	システム変更の作業方法			○				○	○							○
(5)		情報システム仕様書等の管理			○				○									
(6)		①	ログの取得等			○				○								
		②	ログの管理			○				○								
		③	ログの点検・分析			○				○								
(7)		システム障害等の記録、保存			○				○									
(8)		①	通信ソフトウェア等の設定情報の管理			○												
		②	ネットワークのアクセス制御			○												
(9)		外部の者が利用できるシステムの分離等								○								
(10)		①	ネットワークを外部接続する際の許可			許	許			○								
		②	外部ネットワークの接続による影響の確認							○								
		③	外部ネットワーク管理責任者による損害賠償責任の契約上の担保							○								
		④	ファイアウォール等の設置			○				○								
		⑤	問題発生時の物理的な遮断			△				○								
(11)		①	複合機を調達する場合のセキュリティ要件の策定			○												
		②	複合機に対するセキュリティ設定と情報セキュリティインシデント対策の実施			○												
		③	複合機の運用終了時の対策			○												
(12)		①	IoT機器を含む特定用途機器に対する対策の実施			○												
(13)		①	無線LAN利用時の暗号化等の使用義務設定			○												
	②	機密性の高いネットワークへの暗号化等の措置			○													



# 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ委員会	情報セキュリティ責任者	最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報セキュリティ担当者	情報システム管理者	情報システム担当者	監査統括責任者	情報セキュリティ許可権限者	利用申請の管理者	外部サービスの管理者	職員等の義務(統一的窓口)	C S I R T	外部委託関係規定		
	(14)	① 電子メールサーバの中継処理禁止の設定				○													
		② 内部からのスパムメール等の送信を検知した際のメールサーバの運用停止				○													
		③ 電子メールの送受信容量の上限設定等				○													
		④ 電子メールボックスの容量の上限設定等				○													
		⑤ 委託事業者の電子メールアドレス利用取り決め				○													○
		⑥ 電子メールの添付ファイルの監視等				○													
	(15)	① 電子メールの自動転送機能の禁止																○	
		② 業務上必要のない送信先への送信禁止																○	
		③ 複数人に電子メールを送信する際の方法																○	
		④ 重要メールの誤送信時の報告							△									○	
	(16)	① 電子署名、暗号化等による送信		○														○	
		② 暗号化の方法及び鍵の管理		○														○	
		③ 電子署名の正当性を確認する手段の提供		○														○	
	(17)	① ソフトウェアの無断導入の禁止																○	
		② ソフトウェアの導入の許可の取得及びライセンスの管理					許			許								○	
		③ 不正コピーしたソフトウェアの利用禁止																○	
	(18)	① 機器の改造及び増設・交換の禁止																○	
		② 機器の改造及び増設・交換の許可					許			許								○	
	(19)	① 支給端末の許可されたネットワーク以外への接続禁止								許								○	
		② 支給端末への技術的な制限の実施							○										
	(20)	① 業務目的以外でのウェブ閲覧の禁止																○	
		② 業務目的以外でのウェブ閲覧発見時の対応					○		△										
	(21)	① Web会議サービスの利用手順の策定					○												
		② Web会議サービス利用時の情報セキュリティ対策																○	
		③ Web会議主催時の対策																○	
		④ 外部からWeb会議に招待される場合の必要に応じた利用申請																○	
(22)	① (ア) 情報発信におけるなりすまし対策の実施								○										
		(イ) 認証情報及びこれを記録した媒体の適切な管理							○										
	② 機密性2以上の情報のソーシャルメディアサービスでの発信禁止								○										
	③ 利用するソーシャルメディアサービスごとの責任者の決定								○										
	④ アカウント乗っ取り確認時の措置								○										
⑤ 可用性2の情報の提供にソーシャルメディアサービスを用いる場合の措置								○											

## 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ 委員会	情報セキュリティ 責任者	最高情報セキュリティ 責任者	統括情報セキュリティ 責任者	情報セキュリティ 責任者	情報セキュリティ 管理者	情報セキュリティ 管理者	情報システム 担当者	情報システム 担当者	情報セキュリティ 監査統括責任者	情報セキュリティ 許可権限者	利用申請の 管理者	外部サービス 管理者	職員等の義務 (統一的窓口)	CSIRT	外部委託 関係規定			
6.2 アクセス 制御	(1)	①	アクセス制御			○			○											
		②	(ア)	利用者の情報管理や利用者IDの取扱い等の設定			○			○										
			(イ)	利用者登録抹消の申請			△			△							○			
			(ウ)	利用されていないIDの点検			○			○										
		③	(ア)	ID及びパスワードの管理			○			○										
			(イ)	統括情報セキュリティ責任者等の特権を代行する者の要件		○	○			○										
			(ウ)	特権代行者の通知		○	△	△	△	△										
			(エ)	特権付与されたID等の変更の委託事業者への委託禁止			○			○										○
			(オ)	特権付与されたID等のセキュリティ機能強化			○			○										
			(カ)	特権付与されたIDの初期設定以外のものへの変更			○			○										
	(2)	①	外部から内部ネットワーク等へのアクセスの許可				許			許						○				
		②	外部からのアクセス可能人数の制限			○														
		③	外部からのアクセス時の本人確認の機能の確保			○														
		④	外部からのアクセス時の通信の暗号化等の措置			○														
		⑤	外部アクセス用端末等付与時のセキュリティの確保			○			○											
		⑥	外部から持ち込んだ端末等のウィルスの確認等						許							○				
		⑦	インターネットを介した庁内ネットワークへの接続禁止			○														
	(3)	自動識別の設定			○				○											
	(4)	ログイン時のシステム設定							○											
	(5)	①	職員等の認証情報の管理等			○			○											
		②	パスワード発行等			○			○											
		③	認証情報の不正利用防止			○			○											
	(6)	特権によるネットワーク等への接続時間の制限							○											

# 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ委員会	情報セキュリティ責任者	最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報セキュリティ担当者	情報セキュリティ監査統括責任者	情報セキュリティ許可権限者	利用申請の管理者	外部サービスの管理者	職員等の義務(統一的窓口)	CSIRT	関係規定	外部委託			
6.3 システム開発、導入、保守等	(1)	① 調達仕様書への技術的なセキュリティ機能の明記			○														
		② 調達時のセキュリティ機能の調査等			○														
	(2)	① システム開発の責任者及び作業者の特定と規則の確立																	
		② (ア) システム開発の責任者等のIDの管理等 (イ) システム開発の責任者等のアクセス権限の設定																	
	(3)	③ (ア) システム開発におけるソフトウェア等の特定 (イ) 認定外のソフトウェアの削除																	
		④ (ア) システム開発等環境とシステム運用環境の分離 (イ) システム開発環境からシステム運用環境への移行の手順の明確化 (ウ) 移行に伴うシステム停止等の影響の最小化 (エ) 導入されるシステムやサービスの可用性の確保確認																	
	(4)	① システム開発等の資料等の整備・保管																	
		② テスト結果の保管																	
	(5)	③ 情報システムに係るソースコードの保管																	
		① 入力データの正確性を確保できる情報システム設計 ② 情報の改ざん等を検出する情報システム設計 ③ 出力データの正確性を確保できる情報システム設計																	
	(6)	プログラム仕様書等の変更履歴の作成																	
	(7)	ソフトウェア更新等時の他の情報システムとの整合性確認																	
	(8)	システム更新又は統合時の検証等の実施																	
	6.4 不正プログラム対策	(1)	① 不正プログラムのシステムへの侵入防止措置			○													
			② 不正プログラムの外部への拡散防止措置			○													
			③ 不正プログラム情報の収集、職員等への注意喚起			○													
			④ 不正プログラム対策ソフトウェアの常駐			○													
			⑤ 不正プログラム対策ソフトウェアのパターンファイルの更新			○													
			⑥ 不正プログラム対策ソフトウェアの更新			○													
			⑦ サポート終了ソフトウェアの使用禁止			○													
		(2)	① 不正プログラム対策ソフトウェアの常駐																
			② 不正プログラム対策ソフトウェアのパターンファイルの更新																
			③ 不正プログラム対策ソフトウェアの更新																
			④ インターネットに接続していないシステムにおける電磁的記録媒体の制限及び不正プログラム対策ソフトウェアの導入等																
			⑤ 不正プログラム対策ソフトウェア等の設定変更権限の一括管理																
		(3)	① 不正プログラム対策ソフトウェアの設定変更の禁止																○
			② 外部からのデータ又はソフトウェア取込時のウイルスチェックの実施																○
			③ 差出人が不明等の添付ファイルの削除																○
④ 不正プログラム対策ソフトウェアによる定期的なフルチェックの実施																		○	
⑤ 添付ファイル送受信時のウイルスチェック、無害化処理の実施																		○	
⑥ ウイルス情報の確認																		△	
⑦ パソコン等の端末のウイルス感染時の対処方法																		○	
(4)		外部の専門家の支援体制の整備																○	

## 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ委員会	情報セキュリティ責任者	最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報セキュリティ担当者	情報システム監査統括責任者	情報セキュリティ利用申請の許可権限者	外部サービスの管理者	職員等の義務(統一的窓口)	外部委託関係規定	
6.5 不正アクセス対策	(1)	① 使用されていないポートの閉鎖				○								
		② 不要なサービス機能の削除、停止				○								
		③ ウェブページの改ざんを防止するための設定				○		△						
		④ 定期的なファイルの改ざんの有無の検査				○								
		⑤ 監視、通知、外部連絡窓口などの体制及び連絡窓口の構築				○							○	
	(2)	① 攻撃を受けた場合、または受けるリスクがある場合への対応		○	○									
		② 攻撃を受けた記録の保存		○	○									
		③ 内部からの攻撃等の監視		○	○			○						
		④ 職員等による不正アクセス発見時の対応		○	○		△	○						
		⑤ サービス不能攻撃対策の実施		○	○			○						
6.6 セキュリティ情報の収集	(3)	① セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等		○			○							
		② 不正プログラム等のセキュリティ情報の収集・周知		○										
		③ 情報セキュリティに関する技術情報の収集及び共有		○				○						
7 運用	7.1 情報システムの監視	① 情報システムの監視				○		○						
		② サーバの正確な時刻設定等の措置				○		○						
		③ 外部と常時接続するシステムの監視				○		○						
		④ 通信データの監視のための復号				○		○						
	7.2 情報セキュリティポリシーの遵守状況の確認	(1)	① 情報セキュリティポリシーの遵守状況の確認等		△	△	○	○						
			② 問題発生時の対処		○									
			③ システム設定等における情報セキュリティポリシー遵守状況の定期的な確認等			○			○					
		(2)	① モバイル端末及び電磁的記録媒体等の利用状況調査		○									
			② 違反行為の発見時の報告			△		△					○	
	7.3 侵害時の対応等	(3)	① 緊急時対応計画の策定	○	○									
			② 緊急時対応計画に盛り込むべき内容	○	○									
			③ 業務継続計画と情報セキュリティポリシーの整合性の確保	○										
			④ 緊急時対応計画の見直し	○	○									
	7.4 例外措置	(1)	① 例外措置の許可		許			○						
			② 緊急時の例外措置		△			○						
③ 例外措置の申請書の管理				○										
7.5 法令遵守											○			
7.6 懲戒処分等	(1)	① 懲戒処分				○	○	○	○	○		○		
		② 違反時の対応(統括情報セキュリティ責任者確認時)			○		△							
		③ 違反時の対応(情報システム管理者確認時)			△		△	○						
		④ 違反を改善しない職員等のシステム使用の権利の停止等		△	○		△							
8 業務委託と外部サービスの利用	8.1 業務委託	(1)	① 委託事業者の選定時の確認事項					○					○	
			② 国際規格の認証取得状況等を参考にした事業者の選定					○					○	
		(2)	契約項目										○	
	(3)	委託事業者のセキュリティ確保の確認・措置等		△	△		○					○		

# 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。  
 ※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ委員会	情報セキュリティ責任者	最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報セキュリティ担当者	情報セキュリティ監査統括責任者	情報セキュリティ許可権限者	外部サービス利用者	外部サービス管理者	職員等の義務	CSIRT (統一的窓口)	外部委託 関係規定		
8.2 外部サービスの利用 (機密性2以上の情報を取り扱う場合)	① 外部サービスを利用可能な範囲の規定				○												
		② 外部サービス提供者の選定基準			○												
			③ 外部サービスの利用申請の許可権限者と利用手続			○											
				④ 外部サービス管理者の指名と外部サービスの利用状況の管理			○										
	② 外部サービスの利用の検討		① 外部サービスで取り扱う情報の外部サービス提供者における目的外利用の禁止				○										
		② 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制	(イ) 外部サービス提供者若しくはその従業員、再委託先又はその他の者による本市の意図しない変更が加えられないための管理体制				○										
			(ウ) 外部サービス提供者に関する情報提供及び調達仕様書による施設の場所やリージョンの指定				○										
		(エ) 情報セキュリティインシデントへの対処方法				○											
		(オ) 情報セキュリティ対策その他の契約の履行状況の確認方法				○											
		(カ) 情報セキュリティ対策の履行が不十分な場合の対処方法				○											
		③ 外部サービスの中断や終了時に円滑に業務を移行するための対策				○											
		④ 情報セキュリティ監査の受入れ	(ア) 情報セキュリティ監査の受入れ				○										
			(イ) サービスレベルの保証				○										
		⑤ 外部サービスの利用を通じて取り扱う情報に対する国内法以外の法令及び規制が適用されるリスクの評価					○										
		⑥ 外部サービス提供者がその役務内容を一部再委託する場合の対策					○										
		⑦ 取り扱う情報の格付及び取扱制限に応じたセキュリティ要件と外部サービスの選定					○										
		⑧ 外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティ要件					○										
		⑨ 情報セキュリティ監査報告書による外部サービス提供者の評価					○										
	③ 外部サービスの調達時の調達仕様書に含める事項	① 外部サービスを調達する場合の契約までの確認事項と契約内容				○											
		② 外部サービスを利用する場合の利用申請				○											
	④ 職員等による外部サービスの利用申請の審査	① 外部サービスの利用承認時の記録と外部サービス管理者の指名									○						
		② 不正なアクセスを防止するためのアクセス制御				○											
		(イ) 取り扱う情報の機密性保護のための暗号化				○											
	⑤ 開発時におけるセキュリティ対策	(ウ) 設計・設定時の誤りの防止				○											
		② 前項において定める規定内容の確認・記録				○						○					
	⑥ 外部サービス利用方針の規定	① 外部サービス利用に必要な教育	(ア) 外部サービス利用に必要な教育			○											
			(イ) 取り扱う資産の管理			○											
			(ウ) 不正アクセスを防止するためのアクセス制御			○											
			(エ) 取り扱う情報の機密性保護のための暗号化			○											
			(オ) 外部サービス内の通信の制御			○											
			(カ) 設計・設定時の誤りの防止			○											
			(キ) 外部サービスを利用した情報システムの事業継続			○											
			(ク) 外部サービスで発生したインシデントの対処手順の整備				○										
		② 外部サービス運用・保守時の確認・記録										○					
		⑦ 外部サービス利用終了時の確認・記録	① 外部サービス利用終了時における対策	(ア) 外部サービスで取り扱った情報の廃棄			○										
				(イ) 外部サービスの利用のために作成したアカウントの廃棄			○										
	(ウ) 外部サービス利用終了時の確認・記録						○						○				

## 権限・責任等一覧表

※本一覧表は「第2章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ委員会	情報セキュリティ責任者	最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報セキュリティ担当者	情報システム管理者	情報セキュリティ監査統括責任者	情報セキュリティ許可権限者	利用申請の管理者	外部サービスの職員等の義務	CSIRT (統一的窓口)	外部委託関係規定
8.3 外部サービスの利用 (機密性2以上の情報を取り扱わない場合)	(1)	(ア)			○										
		(イ)			○										
		(ウ)			○										
		(エ)			○										
	(2)	①											○	○	
		②						許						○	
9 評価・見直し	9.1 監査	(1)	○							△					
		(2)	①							○					
			②												
		(3)	①		承						○				
			②												
		(4)									○				○
		(5)		△							○				
		(6)									○				
	(7)			○	△		△								
	(8)		○												
9.2 自己点検	(1)	①				○			○						
		②					○	○							
	(2)		△			○	○		○						
	(3)	①											○		
②			○												
9.3 情報セキュリティポリシー及び関係規程等の見直し	情報セキュリティポリシー及び関係規程等の見直しに関する規定	○													

別紙6 SLA要求一覧

別紙6 SLA要件

・求めるサービスレベルは以下の通り

・詳細については受託者との合意によりSLAを結ぶものとする

要件分類	内容	サービスレベル評価項目	定義(測定式)	備考	SLA要求水準	目標制約	
サービス運用時							
可用性	重大障害発生件数	クラウドサービス上におけるシステム使用不能等の重大な障害発生状況を管理する。	重大障害発生件数(クラウドサービス)	・カテゴリ別の重大障害発生件数 ※重大障害の定義については本市と協議の上決定する。		0件/月	目標保証すること
	オンライン稼働率	サービス利用時間内(日常業務時間内)のシステム利用可能状況を管理する。	オンライン稼働率	・「サービス提供時間」÷「サービス利用時間」×100 (%)		99.99%	目標保証すること
	障害復旧時間	障害が発生してから復旧するまでの時間を管理する。	障害復旧時間	・復旧時間目標(RTO)の設定		4時間以内	努力目標
	障害回復予定時間の未遵守障害件数	予定通り、障害が回復したかを管理する。	障害回復予定時間の未遵守障害件数	・受託事業者が提示した障害回復予定時間を遵守できなかった障害件数		0件/月	努力目標
	リソース管理	バージョンアップ、カスタマイズ、障害対応等により、システムに適用したリソースのバージョンを適正に管理する。	リリースミス障害発生件数	・リリースミスによる障害発生件数		0件/月	努力目標
バージョン管理完備率			・「リソースのバージョン管理登録件数」÷「リリース対象のリソース数」×100 (%)		100%	努力目標	
性能	バッチ処理完了予定時間の未遵守件数	決められた時刻にバッチ処理が開始され、後続の処理に影響がない時間で終了することを確認する。他システムへのファイル・データ送信に関する処理においては適切な内容により送信先システムが受信した時点を終了とみなす。	バッチ処理完了予定時間の未遵守件数	・予め通知されたバッチ処理完了予定時間内にバッチ処理が完了した遵守率 「バッチ処理完了件数」÷「バッチ処理件数」×100 (%)	最大124万人の利用者情報を一括出力することを想定	99.5%以上/月	努力目標
	オンライン応答時間	ユーザーの業務オペレーションへの支障が出ることを防止するため、オンライン応答時間を監視する。	ユーザーの業務オペレーションへの影響を防止するため、オンライン応答時間を監視する。	・オンライン応答時間 ※データ更新、画面遷移、検索機能等本市と予め設定する処理について、オペレーションを開始できる状態になるまでの応答時間を分析	ネットワークに起因すると考えられる遅延については、これを除外する。オンライン測定対象画面を本市と協議のうえ、決定し、定期的に測定を行うこと。	3秒以内	目標保証すること
	リソース監視	システム安定稼働を確保するために、必要だと思われる項目を監視する。	ディスク使用率警告通知時間	・ディスク使用率の閾値越えを検知してから本市担当へ報告するまでの時間	閾値の瞬間的な超過は含まない。	30分以内	努力目標
CPU使用率警告通知時間			・CPU使用率の閾値越えを検知してから本市担当へ報告するまでの時間	30分以内		努力目標	
メモリ使用率警告通知時間			・メモリ使用率の閾値越えを検知してから本市担当へ報告するまでの時間	30分以内		努力目標	
機密性	システム利用実績管理	システムログイン/ログアウト情報のログ等、システム利用実績を定期的に収集し、不正等を監視する	・システムログイン/ログアウトに関するログ集計から報告までの時間	・ログを集計してから報告するまでの時間  ※月次での集計・報告を想定している。運用保守報告会での報告とする場合は、本市と協議の上、その開催日程に拠るものとする		30日以内	努力目標

別紙7 SLA要求一覧

要件分類	内容	サービスレベル評価項目	定義(測定式)	備考	SLA要求水準	目標制約	
セキュリティ	ウイルス検出通知時間	ウイルス検出通知時間	・ウイルス感染発見から、本市担当者へ報告するまでの時間		30分以内	努力目標	
	最新パターンファイル適用時間	最新のウイルスに対応したパターンファイルの適用状況を管理する。	最新パターンファイル適用時間	・最新パターンファイルの公開から適用までの時間	24時間以内	努力目標	
	最新セキュリティパッチの適用時間	適用する必要があるセキュリティパッチを確実に適用されたかを管理する。	最新セキュリティパッチの適用時間	・最新セキュリティパッチ公開から本市担当者へ通知するまでの時間と本市担当者へ通知後、パッチ適用可否を決定(分析)し、通知するまでの時間	セキュリティパッチの適用自体は本市担当者として協議のうえ決定する。	15日以内	努力目標
	サイバー攻撃への対応	DoS攻撃等のサービス妨害攻撃に対処する	サイバー攻撃による被害件数	・サイバー攻撃を受けたことによる障害件数		0件	目標保証すること
運用保守	ヘルプデスクの応答時間	サポート時間内の問い合わせに対して、遅延無く対応する。	一次回答時間	・問い合わせの連絡をヘルプデスクが受けてから、問い合わせ職員へ一次回答を行うまでの時間	時間外の問合せは、翌営業日の受付開始時間に受けたこととする。	24時間以内	努力目標
	SLAモニタリング結果の報告	SLAのモニタリング結果が報告されたかを管理する。	SLAのモニタリング結果の報告回数	・月次の報告回数 ※事前の日程調整により、N月度分がN+1月に報告された場合も、N月度分とみなす	合理的な理由がある場合は、事前に本市と協議の上、報告を見送ることは可とする。	1回/月	努力目標
	障害発生通知	障害を検知してから、本市監督職員へ報告するまでの時間を管理する。  ※休日及び夜間において影響が出ないと推測される場合に限っては事後報告を可とする	・障害発生通知時間	・障害を検知してから本市担当職員に報告するまでの時間  ※受託事業者の故意または過失により、障害検知が遅れた場合は、障害が発生したと想定される時間からの計測とする	必要に応じて、他事業者と連携し対応すること。	30分以内	努力目標
業務影響	作業品質	受託事業者の実施する作業に起因した、本市の業務品質に影響のある障害等事象を管理する。	業務遂行に関連して、受託事業者の作業に起因する以下の事象が発生していないこと。 ・重大かつ直接的に本市民に影響を与える事故事象(庁外)の発生(画面表示情報に誤りがある等) ・直接的に本市民に影響を与える事故事象(庁内)の発生(処理停滞などによる窓口業務の遅延) ・業務遂行上の事故事象の発生(一括処理や締め処理の遅延・再処理)	緊急事態報告、受託事業者の障害報告等から事故事象の発生回数をカウントする。	遅延や再処理について本市と事前に協議/合意された合理的な判断のもとに発生した業務影響については、これを除外する。	0件/月	努力目標



別紙7 本市が想定する成果物

	カテゴリ	納品物	提出時期
1	基本計画	プロジェクト計画書	契約締結から2週間以内
2	要件定義	要件定義書	基本設計着手前
3	設計（基本設計・詳細設計）	基本設計書	詳細設計着手前
		詳細設計書	プログラム開発前
		テスト計画書	単体・結合テスト実施前
4	プログラム開発	パラメータ設計書	単体・結合テスト実施前
		結合テスト計画書	単体・結合テスト実施前
		総合テスト計画書	総合テスト実施前
5	システム環境構築	構成管理台帳	環境構築実施前
		システム環境構築手順書・マニュアル	結合テスト実施前
6	単体・結合テスト	単体テスト実施結果報告書	結合テスト実施前
		結合テスト実施結果報告書	総合テスト実施前
7	総合テスト	運用管理マニュアル	総合テスト実施前
		総合テスト実施結果報告書	運用テスト実施前
8	セキュリティ診断	セキュリティ診断結果報告書 (7.2.6.1 セキュリティ対策への対応)	運用テスト実施前
9	研修	管理者向けシステム操作マニュアル	研修実施前
		個別サービス利用者向け操作マニュアル	研修実施前
		一般市民向け操作マニュアル	研修実施前
		研修計画書	研修実施前
		研修マニュアル	研修実施前
10	運用保守	運用・保守設計書	リリース前
		稼働報告書	稼働確認後1週間以内、全機能の稼働確認後1週間以内
11	運用保守(稼働後) ※設計のみ	定例運用報告書	毎月1回
		SLAモニタリング報告書	毎月1回
		SLA改善報告書	毎月1回(必要に応じて)
		災害対応(業務継続)手順	総合テスト実施前

## 横浜市放課後キッズクラブ事業実施要綱

制 定 平成 22 年 3 月 17 日 こ放第 879 号（市長決裁）  
最近改正 令和 5 年 4 月 1 日 こ放第 3222 号（局長決裁）

### （目 的）

第 1 条 この要綱は、放課後キッズクラブ事業（以下「キッズクラブ事業」という。）の実施について必要なことを定める。

2 キッズクラブ事業は、次の各号を目的とした事業を一体的に行うものとする。

(1) 児童が通い慣れている学校施設等を利用して、異年齢児間の遊びを通じた交流を促進し、児童の創造性、自主性、社会性などを養うこと

(2) 児童福祉法（昭和 22 年法律第 164 号。以下「法」という。）第 6 条の 3 第 2 項の放課後児童健全育成事業として、対象となる児童に適切な遊び及び生活の場を与え、その健全な育成を図ること

3 前項第 2 号の事業の実施及び運営にあたって必要な事項については、横浜市放課後児童健全育成事業の設備及び運営の基準に関する条例（平成 26 年 9 月横浜市条例第 49 号。以下「条例」という。）及び横浜市放課後児童健全育成事業の届出等に関する要綱（平成 27 年 2 月 26 日こ放第 930 号。以下「届出要綱」という。）のほか、この要綱の定めるところによる。

4 キッズクラブ事業の実施に伴う補助金の交付については、横浜市補助金等の交付に関する規則（平成 17 年 11 月横浜市規則第 139 号）及び横浜市放課後キッズクラブ事業費補助金交付要綱（平成 18 年 3 月 2 日福子放第 10304 号。以下「補助金交付要綱」という。）に定める。

### （用語の定義）

第 2 条 この要綱において「放課後キッズクラブ」とは、キッズクラブ事業の運営主体（以下「運営主体」という。）が、条例及びこの要綱に定める事項を備えた良好な衛生環境及び安全性を備えた、キッズクラブ事業のための専用施設（以下「専用ルーム」という。）等において、専任の職員によりキッズクラブ事業を行い、かつ、放課後キッズクラブが所在する区の区長（以下「区長」という。）が適当と認めたものをいう。

2 この要綱において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) わくわく【区分 1】 第 1 条第 2 項第 1 号を目的に放課後キッズクラブを利用する児童が登録する区分

(2) すくすく【区分 2】 第 1 条第 2 項第 1 号かつ第 2 号を目的に放課後キッズクラブを利用する児童が登録する区分。なお、すくすく【区分 2】は利用時間に応じて、すくすく（ゆうやけ）【区分 2A】とすくすく（ほしぞら）【区分 2B】の 2 つの区分に分かれる。

3 この要綱において「支援の単位」とは、クラブにおける育成支援であって、クラブを利用する児童に対して一体的に行われる集団の規模をいう。

4 この要綱において「対象児童数」とは、すくすく【区分 2】登録児童の利用希望日数から算出した人数を指す。「対象児童数」の算出は、放課後キッズクラブに利用の登録をし、かつ継続的に利用する者で、毎日利用する児童の人数に、一時的に利用する児童の平均利用人数を加えることで行う。

- 5 この要綱における用語の意義は、前4項に定めるもののほか、法、条例、補助金交付要綱、横浜市放課後キッズクラブ運営法人の選定に関する要綱（平成17年12月20日福子放第10167号。以下「選定要綱」という。）及び横浜市放課後キッズクラブ運営法人の再選定に関する要綱（平成23年7月1日こ放第206号。以下「再選定要綱」という。）の例による。

#### （運営主体）

第3条 キッズクラブ事業の運営主体は、選定要綱及び再選定要綱に基づき、区長により選定され、かつ法第34条の8第2項に規定される放課後児童健全育成事業の届出を行っている法人とする。

- 2 選定要綱及び再選定要綱に基づき区長が選定した法人は、選定期間中において、当該選定及び再選定により生ずる権利及び義務を第三者に譲渡し、継承させることができない。ただし、会社法に基づく合併、分割（当該キッズクラブ事業にかかる業務の全てを継承させるものに限る。）又はその他これらに類する行為により、当該キッズクラブ事業にかかる業務の全てを別の法人が行おうとする場合は、あらかじめ区長の承認を得て、これを継承することができる。

#### （対象児童）

第4条 キッズクラブ事業の対象児童は、当該小学校又は当該義務教育学校前期課程（以下「当該小学校等」という。）に通学している児童とする。

- 2 前項の規定にかかわらず、当該小学校区又は当該義務教育学校区に居住し、国立小学校、私立小学校、または特別支援学校等に通学する児童についても対象児童とする。
- 3 前2項の児童のうち、第1条第2項第2号の放課後児童健全育成事業の対象となる児童は、次の各号のいずれかに該当する児童とする。
- (1) その保護者が、労働等により、放課後に当該児童が帰宅する時間帯（土曜日及び学校休業日（日曜日を除く。）にあつては、当該時間帯に相当する時間帯）に、家庭にいないこと
  - (2) その保護者が、健康上の理由等により、昼間家庭にいても当該児童の健全育成ができる環境にない状態であること
- 4 放課後キッズクラブの利用にあたっては、第2条第2項に規定する利用区分により、保護者が事前に運営主体に利用の登録をするものとする。
- 5 第2条第2項に規定する利用区分は年度途中での変更ができるものとし、変更にあたっては保護者が事前に運営主体に利用区分変更の届出をするものとする。

#### （事業内容）

第5条 キッズクラブ事業の実施にあたっては、次に掲げる活動を行うものとする。

- (1) 児童の健康管理、安全確保、情緒の安定
- (2) 児童の活動への意欲と態度の形成
- (3) 遊びを通じた児童の自主性、社会性、創造性の向上
- (4) 児童の活動状況の把握と児童の家庭との日常的な連絡及び情報交換
- (5) 学校との迅速な情報交換と日常的な連携
- (6) 家庭や地域での遊びの環境づくりへの支援
- (7) 保護者との連携による親子参加活動
- (8) 地域の子育て支援に関する活動

(9) その他児童の健全育成に関して必要な活動

(開所日及び開所時間)

第6条 放課後キッズクラブは、次に掲げる日を除き、毎日開所しなければならない。

(1) 日曜日

(2) 国民の祝日に関する法律（昭和23年法律第178号）第3条に規定する休日

(3) 1月2日、1月3日及び12月29日から12月31日まで

2 放課後キッズクラブは、次に掲げる時間帯において開所しなければならない。

(1) 平日は、授業終了後から午後7時まで

(2) 土曜日は、午前8時30分から午後7時まで

(3) 学校休業日（土曜日を除く）は、午前8時から午後7時まで

3 運営主体は、前2項の規定に基づき、放課後キッズクラブを開所するとともに、別表1に定める利用区分ごとの利用時間を遵守しなければならない。

4 第1項及び第2項の規定にかかわらず、事前に児童の利用希望を確認し、利用希望の児童がいないことが確認できた場合は、利用者に周知したうえで、閉所することができる。

5 第1項及び第2項の規定にかかわらず、区長がやむを得ないと認める場合は、臨時に閉所することができる。

(実施場所)

第7条 キッズクラブ事業の実施場所は、当該小学校等の余裕教室の状況等を学校長と調整し、原則当該小学校内に設置する専用ルームその他学校施設とする。ただし、公園、市民利用施設等での実施は妨げない。

(職員の配置基準、雇用等)

第8条 運営主体は、1つの活動場所には必ず1名以上の職員を配置することとし、別表2に定める職員最低配置基準を遵守しなければならない。

2 運営主体は、第5条に規定する事業内容を円滑に実施し、利用児童の安全を確保するため、次の職員を雇用するものとする。

(1) 常勤職員（主任） 1名

(2) 常勤職員（副主任） 1名以上

(3) 非常勤職員 必要数

3 職員は、勤務時間内は専任とし、兼務しないものとする。

4 第2項における常勤職員は、原則として週30時間以上勤務となるよう努めなければならない。

(研 修)

第9条 運営主体は、職員の資質向上を図り、第5条に規定する事業内容を円滑かつ安全に実施するため、職員に対し、障害児の対応をはじめとする、活動に必要な知識・経験を養うための研修を実施しなければならない。

2 運営主体は、条例第8条に定める職員の知識及び技能の向上と資質向上を図るため、横浜市が実施する人材育成研修について、職員の参加の機会を提供しなければならない。

3 運営主体は、関係機関が実施する研修について、職員の参加の機会を提供するよう努めな

ればならない。

4 運営主体は、前3項を実現するために、研修計画を策定しなければならない。

(安全管理)

第10条 運営主体は、平常時から危機を想定してその予防に最善を尽くすこととし、事件、事故及び災害等（以下「事故等」という。）の危機管理について、本市の指示に基づき対応マニュアルを作成するとともに、事故等の発生時に迅速かつ確な緊急対策を実施できるよう、学校及び関係機関との連携に努めなければならない。

2 運営主体は、放課後キッズクラブにおいて事故等が発生した場合、届出要綱第7条第2項に規定する放課後児童健全育成事業事故報告書（第8号様式）により速やかに区長に報告しなければならない。

(評議会)

第11条 運営主体は、学校・地域と情報共有しながら相互に連携・協力を図るため、評議会を設置し、半期に1回以上評議会を開催しなければならない。

2 評議会は、次の事項を協議し、運営主体に意見具申するものとする。また、運営主体は評議会の意見を放課後キッズクラブの運営に反映するよう努めなければならない。

(1) 放課後キッズクラブの運営状況、予算、決算に関すること。

(2) 学校・地域との連携に関すること。

(3) 保護者からの意見、要望等の調整に関すること。

(4) その放課後キッズクラブの安全かつ円滑な運営に関すること。

3 評議会は、次の各号に規定する者から運営主体が選任した者（以下「評議会委員」という。）をもって組織するものとする。

(1) 学校長

(2) 保護者代表

(3) 地域代表

(4) その他運営主体が必要と認める者

4 評議会には会長、副会長を置く。会長は評議会を代表し、会務を掌理するものとし、副会長は会長を補佐し、会長が欠けたときはその職務を代理するものとする。ただし、運営主体の構成員等が評議会委員を兼ねることはできない。

5 新規に放課後キッズクラブを開設した場合及び評議会委員に変更がある場合は区長の定める期日までに「評議会委員名簿（第1号様式）」により区長に報告するものとする。

6 運営主体は、評議会開催後、評議会開催記録を作成し、内容を会長に確認したうえで評議会委員全員に共有を図るものとする。

(保護者会等)

第12条 運営主体は、保護者と協力して事業を実施するとともに、保護者の意見、要望等を踏まえた運営を行うため、半期に1回以上保護者会を開催しなければならない。

2 運営主体は、保護者会等の開催後、保護者会等開催記録を作成し、運営主体で保管するものとする。

(保護者負担金)

第13条 運営主体は、あらかじめ保護者の同意を得た上で、利用料、おやつ代及び特別な行事や教材に係る費用等について、別表3のとおり利用児童の保護者から徴収するものとする。

2 運営主体は、こども青少年局長が別に定める仕様を満たす保険に加入し、放課後キッズクラブの利用を希望する児童の保護者に対し、保険料を利用登録前までに負担させるものとする。

(事業の実施報告等)

第14条 運営主体は、毎月20日までに、「放課後キッズクラブ月別状況報告書(第2号様式)」により前月分のキッズクラブ事業の実施状況を区長に報告するものとする。

2 運営主体は、すくすく【区分2】の登録児童について名簿を作成し、管理することとする。

3 運営主体は、すくすく【区分2】の登録児童について、次に掲げる書類により、区長が定める期日までに区長に報告するものとする。

(1) すくすく【区分2】登録者名簿(第3号様式)

(2) すくすく【区分2】登録児童の利用申込書の写し

(備品管理等)

第15条 キッズクラブ事業の実施にあたり運営主体が補助金により取得した備品について、運営主体は善良な管理者の注意をもって取り扱うものとする。

2 横浜市が調達し貸与した施設や備品(はまっ子ふれあいスクールで使用していたものも含む)について、運営主体は善良な管理者の注意をもって取り扱うものとし、故意または重大な過失により滅失し、若しくはき損し、またはその返還が不可能となったときは、区長の指定した期間内に代品を納め、若しくは原状に復し、または損害を賠償しなければならない。また、運営主体の故意または過失によらない施設の修繕及び備品の修理等については、別途区長に協議するものとする。

(個人情報の保護)

第16条 運営主体は、キッズクラブ事業による事務を処理するための個人情報の取り扱いについては、別に定める「横浜市放課後児童健全育成事業個人情報取扱特記事項」(平成18年3月福子放第10304号)を遵守しなければならない。

(情報提供)

第17条 運営主体は、キッズクラブ事業の実施にあたって学校と調整し、毎年度、新入生の保護者向けに説明会や見学会を開催しなければならない。なお、新規に放課後キッズクラブを開設する場合については、学校と調整し、開設前に保護者説明会を開催しなければならない。

2 運営主体は、事業予定等を掲載した広報紙を毎月作成し、当該小学校等の保護者及び関係機関に配布するものとする。

(引継)

第18条 運営主体または常勤職員の変更が生じる場合は、運営に支障がないよう事前に必要な引継ぎを行うものとする。

(調査又は報告)

第 19 条 区長は、本要綱に基づく適正な事業実施を維持するため、運営主体に対して、関係書類を閲覧し、又は提出を求め、運営状況を調査し、又は報告を徴することができる。

(ウクライナからの避難民への支援)

第 20 条 第 13 条によらず、保護者等からの申告に基づき、ウクライナからの避難民であるところども青少年局長が認める者については、当面の間、保護者負担金を徴収しないことができるものとする。

(補 則)

第 21 条 この要綱に定めるもののほか、この要綱の実施に関して必要な事項については、別にところども青少年局長が定める。

附 則 (平成 22 年 3 月 17 日こ放第 879 号)

この要綱は、平成 22 年 3 月 17 日から施行し、平成 22 年度の予算に係る補助金等から適用する。

附 則 (平成 22 年 10 月 21 日こ放第 493 号)

この要綱は、平成 22 年 10 月 21 日から施行する。

附 則 (平成 23 年 3 月 11 日こ放第 899 号)

この要綱は、平成 23 年 4 月 1 日から施行する。

附 則 (平成 24 年 3 月 15 日こ放第 959 号)

この要綱は、平成 24 年 4 月 1 日から施行する。

附 則 (平成 24 年 8 月 7 日こ放第 390 号)

この要綱は、平成 24 年 8 月 7 日から施行する。

附 則 (平成 25 年 3 月 11 日こ放第 994 号)

この要綱は、平成 25 年 3 月 11 日から施行する。

附 則 (平成 27 年 3 月 10 日こ放第 975 号)

この要綱は、平成 27 年 3 月 10 日から施行する。

附 則 (平成 28 年 3 月 10 日こ放第 1157 号)

この要綱は、平成 28 年 3 月 10 日から施行する。

附 則 (平成 29 年 3 月 10 日こ放第 1117 号)

この要綱は、平成 29 年 3 月 10 日から施行する。

附 則 (平成 30 年 3 月 8 日こ放第 1047 号)

この要綱は、平成 30 年 3 月 8 日から施行し、平成 30 年度の予算に係る補助金から適用する。

附 則（平成 30 年 8 月 1 日こ放第 327 号）

この要綱は、平成 30 年 8 月 1 日から施行する。

附 則（平成 31 年 3 月 4 日こ放第 1137 号）

この要綱は、平成 31 年 3 月 4 日から施行し、平成 31 年度の予算に係る補助金から適用する。

附 則（令和元年 10 月 15 日こ放第 630 号）

この要綱は、令和元 年 10 月 15 日から施行する。

附 則（令和 2 年 3 月 1 日こ放第 1091 号）

この要綱は、令和 2 年 3 月 1 日から施行し、令和 2 年度の予算に係る補助金から適用する。

附 則（令和 3 年 3 月 1 日こ放第 2061 号）

この要綱は、令和 3 年 3 月 1 日から施行し、令和 3 年度の予算に係る補助金から適用する。

附 則（令和 4 年 2 月 25 日こ放第 2157 号）

（施行期日）

- 1 この要綱は、令和 4 年 2 月 25 日から施行し、令和 4 年度の予算に係る補助金から適用する。  
ただし、第 6 条第 2 項及び別表 1 に定める学校休業日（土曜日を除く）の開所時間等は令和 4 年夏季休業日から適用するものとし、それまでの間は「午前 8 時」とあるのは「午前 8 時 30 分」とする。

（経過措置）

- 2 施行日から当面の間、第 8 条第 4 項の規定の適用については、令和 4 年 3 月 31 日まで週 25 時間勤務をしていた副主任はこの限りではない。
- 3 施行日から令和 7 年 3 月 31 日までの間、第 9 条第 4 項の規定の適用については、同項中「しなければ」とあるのは、「となるよう努めなければ」とする。

附 則（令和 4 年 6 月 1 日こ放第 1012 号）

この要綱は、令和 4 年 6 月 1 日から施行する。

附 則（令和 5 年 4 月 1 日こ放第 3222 号）

この要綱は、令和 5 年 4 月 1 日から施行する。



別表1（第6条）

利用区分ごとの利用時間

	わくわく【区分1】 (注1)(注2)	すくすく(ゆうやけ) 【区分2A】	すくすく(ほしぞら) 【区分2B】
平日	授業終了後から 午後4時まで	授業終了後から 午後5時まで	授業終了後から 午後7時まで
土曜日	なし	午前8時30分から 午後5時まで	午前8時30分から 午後7時まで
学校休業日 (土曜日を除く)	1人あたり2時間程度 (注3)	午前8時から 午後5時まで	午前8時から 午後7時まで

注1 警報発表時等は、別に子ども青少年局長が定める基準に基づき、運営主体はわくわく【区分1】の利用制限を行うことができる。

注2 地域や保護者との交流を目的としたプログラムを実施する場合は、特例としてわくわく【区分1】の利用時間を超えてプログラムを実施することができる。(以下、「プログラムの特例」という。)なお、プログラムの特例を実施する場合の実施頻度や実施時間は下表のとおりとする。

	実施頻度	実施時間
平日	週1回程度	授業終了後から午後4時30分まで
土曜日	月1回程度	午前9時から午後4時30分までの間で、4時間程度
学校休業日 (土曜日を除く)	週1回程度	午前9時から午後4時30分までの間で、4時間程度

注3 学校休業日(土曜日を除く)のわくわく【区分1】の利用時間は、午前9時から午後4時までの間で、放課後キッズクラブごとに設定し、1人あたりの利用時間は2時間程度とする。

別表2（第8条）

職員最低配置基準

支援の単位数		1単位	2単位	3単位	4単位	5単位	6単位
平日	放課後～16時（注1）	4名	6名	8名	10名	12名	14名
土曜日	開所時間のうち、クラブが指定するわくわく【区分1】の利用時間（注1）						
学校休業日（土曜日を除く）							
上記以外の時間		2名	4名	6名	8名	10名	12名

注1 プログラムの特例を実施する場合は、その実施時間までとする。

注2 条例第10条に基づき、支援の単位数に応じて、放課後児童支援員を配置しなければならない。

注3 支援の単位数が7単位以降についても、支援の単位数ごとに2名以上配置するとともに、表中の（注1）の時間においてはこれに2名追加で配置しなければならない。

別表3（第13条）

保護者負担金

項目		わくわく 【区分1】	すくすく（ゆうやけ） 【区分2A】	すくすく（ほしぞら） 【区分2B】
月額 利用料	4～3月 （7～8月 を除く）	無料	月額2,000円 （保護者負担減免額相当補助の対象となる世帯（注2）は減免あり）	月額5,000円 （保護者負担減免額相当補助の対象となる世帯（注2）は減免あり）
	7～8月		月額2,500円 （保護者負担減免額相当補助の対象となる世帯（注2）は減免あり）	月額5,500円 （保護者負担減免額相当補助の対象となる世帯（注2）は減免あり）
一時利用料 （注1）		1回800円	1回400円	なし
おやつ代		なし （一時利用料を支払って 利用する場合は実費相当額）	実費相当額	
保険料		実費相当額		
特別な行事や 教材に係る費用		実費相当額		

注1 わくわく【区分1】及びすくすく（ゆうやけ）【区分2A】の児童は、一時利用料を支払うことで、当該日は午後7時まで利用することができる。なお、わくわく【区分1】の児童については、定員に空きがある場合に限り、一時利用の利用ができる。

注2 「保護者負担減免額相当補助の対象となる世帯」とは、横浜市の就学援助を受けている世帯、生活保護受給世帯及び市民税所得割非課税世帯を指す。

注3 保護者負担減免額相当補助の対象となる世帯の減免金額は下表のとおりとする。

項目		すくすく（ゆうやけ） 【区分2A】	すくすく（ほしぞら） 【区分2B】
減免額 （減免後の 月額利用料）	4～3月 （7～8月を除く）	月額2,000円（0円）	月額2,500円（0円）
	7～8月	月額2,500円（0円）	月額2,500円（月額3,000円）

## 評 議 会 委 員 名 簿

クラブ名：  放課後キッズクラブ

運営法人：

年 月 日現在

No.	役 職	氏 名	所 属	住 所	電 話 番 号	新 規 任 命 者
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

※委員に対して、氏名・所属・住所・電話番号の情報を区役所に提供すること、及び区役所から連絡がある場合があることを説明し、同意を得たうえで、名簿を作成してください。

※住所、電話番号は連絡が取れる連絡先を記入してください。

※新規に開設した放課後キッズクラブについては、委員全員分の住所、電話番号が必要です。

※委員に変更があった場合も委員全員分の記入が必要です。新たに委員に任命された方については、新規任命者の欄に「○」を記入します。

※区役所から委員の住所宛に文書を送付させていただくことがあります。また、この内容は、放課後キッズクラブ事業に関する事以外には使用しません。

放課後キッズクラブ月別状況報告書

年 月 日

クラブ名:

◆ 末日現在児童数・登録率

Table with columns for grade levels (1st to 6th), total counts, and enrollment rates for various club types (e.g., 在籍児童数, 登録児童数).

【実施分類】

Table defining implementation categories (1-4) based on criteria like staff ratios and support unit counts.

※「在籍児童数①」及び「登録児童数②」の欄については、当該校の通学児童のみを記入してください。(当該校以外の児童については、ここでは記入しません。)

◆ 児童利用状況及び開所状況

Main data table showing daily attendance and opening status for 6 support units across 27 days of the month.

※ 支援の単位ごとの実施分類日数

Summary table for implementation classification counts per support unit (1-6).

※ 支援の単位ごとの実施分類日数

Summary table for implementation classification counts per support unit (1-6).

◆ 当該校以外の登録児童数

	国立・私立小学校	特別支援学校
登録児童数	0人	0人
うち わくわく【区分1】		
うち すくすく (ゆうやけ)【区分2A】		
うち すくすく (ほしぞら)【区分2B】		

※当該校以外の登録児童数は、参考数値のため、  
末日現在登録児童数及び在籍児童数には含めません。

◆ 補助金交付要綱第8号様式 横浜市放課後キッズクラブ事業費補助金執行状況報告書 記入事項

※下表については、放課後キッズクラブ補助金交付要綱 第8号様式横浜市放課後キッズクラブ事業費補助金執行状況報告書に対応しています。

基本補助（基礎部分）

	単位1	単位2	単位3	単位4	単位5	単位6
対象児童数						
開所日数						

※開所日数は実施分類が①または③の日数の合計

長時間開所加算補助

	単位2	単位3	単位4	単位5	単位6
補助対象 平均時間数					

子ども教室加算補助

利用児童数	うちわくわく 【区分1】 利用児童数

障害児受入加算補助

利用児童数

◆ 4月から当該月までの累計収入額及び累計支出額 ※7月分以降の月別状況報告書から記入すること

【収入の部】

項目	累計収入額
横浜市補助金	
保護者負担金	
利用料	
保険料	
おやつ代	
材料費	
その他	
その他収入	
合計	

【支出の部】

項目	累計支出額
人件費	
常勤職員給与	
非常勤職員給与	
新型コロナウイルス感染拡大防止加算補助経費	
障害児受入推進加算補助経費	
障害児受入強化推進加算補助経費	
放課後児童支援員等キャリアアップ処遇改善費補助経費	
育成支援体制強化加算補助経費	
賃金改善加算補助	
その他	
事業費	
管理運営費	
児童処遇費	
保険料	
おやつ代	
材料費	
その他	
その他	
合計	

◆ 特記事項

(平均利用児童数と対象児童数の乖離理由・乖離の是正対応状況・その他運営に関わる特記事項 等)

◆ 保護者会等・評議会開催日

	1回目	2回目
保護者会等		
評議会		

※3月の月報にのみ保護者会等と評議会の開催日を記載してください。

※月別状況報告書は、翌月20日までに、  
区役所こども家庭支援課へ提出してください。

放課後キッズクラブ月別状況報告書

クラブ名: \_\_\_\_\_

年 \_\_\_\_\_ 月 \_\_\_\_\_ 日

(領出先) 領出日 \_\_\_\_\_ 区長 \_\_\_\_\_

◆ 本日現在児童・登録者

Table with columns for age groups (1-6 years) and total counts for various categories like enrollment, attendance, and withdrawal.

◆ 来日現在児童・登録者

Table with columns for age groups (1-6 years) and total counts for various categories like enrollment, attendance, and withdrawal.

【表紙分類】

Classification table with 4 rows and 3 columns: 期別 (Period), 児童の単位 (Child Unit), 児童の単位8 (Child Unit 8).

※ 「有期児童数①」及び「無期児童数②」の欄については、当該月の児童の人数を記入してください。( )

◆ 児童利用状況及び開所状況

Main data table with columns for dates (1-30), child units (1-8), and utilization status (開所/閉所/休所).

※ 支所の閉所日の基礎分類日数

Summary table for closure days, categorized by child unit (1-8) and total counts.

◆ 当該校以外の登録児童数

	国立・私立小学校	特別支援学校
登録児童数	0人	0人
うち わくわく【区分1】		
うち すくすく (ゆうやけ)【区分2A】		
うち すくすく (ほしぞら)【区分2B】		

※当該校以外の登録児童数は、参考数値のため、  
末日現在登録児童数及び在籍児童数には含めません。

◆ 補助金交付要綱第8号様式 横浜市放課後キッズクラブ事業費補助金執行状況報告書 記入事項

※下表については、放課後キッズクラブ補助金交付要綱 第8号様式横浜市放課後キッズクラブ事業費補助金執行状況報告書に対応しています。

基本補助（基礎部分）

	単位1	単位2	単位3	単位4	単位5	単位6	単位7	単位8
対象児童数								
開所日数								

※開所日数は実施分類が①または③の日数の合計

長時間開所加算補助

	単位2	単位3	単位4	単位5	単位6	単位7	単位8
補助対象 平均時間数							

子ども教室加算補助

利用児童数	うちわくわく 【区分1】 利用児童数

障害児受入加算補助

利用児童数

◆ 4月から当該月までの累計収入額及び累計支出額

※7月分以降の月別状況報告書から記入すること

【収入の部】

項目	累計収入額
横浜市補助金	
保護者負担金	
利用料	
保険料	
おやつ代	
材料費	
その他	
その他収入	
合計	

【支出の部】

項目	累計支出額
人件費	
常勤職員給与	
非常勤職員給与	
新型コロナウイルス感染拡大防止加算補助経費	
障害児受入推進加算補助経費	
障害児受入強化推進加算補助経費	
放課後児童支援員等キャリアアップ処遇改善費補助経費	
育成支援体制強化加算補助経費	
資金改善加算補助	
その他	
事業費	
管理運営費	
児童処遇費	
保険料	
おやつ代	
材料費	
その他	
その他	
合計	

◆ 特記事項

(平均利用児童数と対象児童数の乖離理由・乖離の是正対応状況・その他運営に関わる特記事項 等)

◆ 保護者会等・評議会開催日

	1回目	2回目
保護者会等		
評議会		

※3月の月報にのみ保護者会等と評議会の開催日を記載してください。

※月別状況報告書は、翌月20日までに、  
区役所こども家庭支援課へ提出してください。



## すくすく【区分2】登録者名簿

クラブ名：  放課後キッズクラブ

支援の単位数：  単位

支援の単位ごとの対象児童数（人）

単位	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
単位1												
単位2												
単位3												
単位4												
単位5												
単位6												
合計	-	-	-	-	-	-	-	-	-	-	-	-

別添名簿に記載する者は、横浜市放課後キッズクラブ事業実施要綱第4条第3項に規定する対象児童であることを証します。

運営主体名

代表者職氏名

## すくすく【区分2】登録者名簿

クラブ名： 放課後キッズクラブ

支援の単位数： 単位

支援の単位ごとの対象児童数（人）

単位	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
単位1												
単位2												
単位3												
単位4												
単位5												
単位6												
単位7												
単位8												
合計	-	-	-	-	-	-	-	-	-	-	-	-

別添名簿に記載する者は、横浜市放課後キッズクラブ事業実施要綱第4条第3項に規定する対象児童であることを証します。

運営主体名

代表者職氏名



## 横浜市放課後キッズクラブ事業費補助金交付要綱

制 定 平成18年3月2日 福子放第10304号（市長決裁）

最近改正 令和5年12月7日 こ放第1118号（局長決裁）

### （目的）

第1条 この要綱は、横浜市放課後児童健全育成事業の届出等に関する要綱（平成27年2月26日こ放第930号。以下「届出要綱」という。）に基づき届出を行った事業所で、横浜市放課後キッズクラブ事業実施要綱（平成22年3月17日こ放第879号。以下「実施要綱」という。）に定める放課後キッズクラブ事業（以下「キッズクラブ事業」という。）を実施する運営主体等に対して予算の範囲内で交付する放課後キッズクラブ事業費補助金（以下「補助金」という。）について、必要な事項を定める。

2 補助金の交付については、横浜市補助金等の交付に関する規則（平成17年11月横浜市規則第139号。以下「補助金規則」という。）に定めるもののほか、この要綱に定めるところによる。

### （用語の定義）

第2条 この要綱における用語の意義は、横浜市放課後児童健全育成事業の設備及び運営の基準に関する条例（平成26年9月横浜市条例第49号。以下「条例」という。）、補助金規則、届出要綱及び実施要綱の例による。

### （補助金の区分及び補助対象経費）

第3条 この要綱における補助金の区分は次の各号に掲げるとおりとする。

- (1) 運営費補助
- (2) 開設費補助
- (3) 準備費補助

2 前項に掲げる補助対象経費、補助基準額等は、別表1から別表11に定めるものとする。なお、運営費補助のうち、放課後児童支援員等キャリアアップ処遇改善費補助については本要綱に定めるほか「放課後児童支援員等キャリアアップ処遇改善費補助実施細目」（平成29年10月31日こ放第680号。以下「実施細目」という。）に必要な事項を定める。

3 第2項に基づき積算する補助金は、補助金の総額に百円未満の端数があるときは、その端数金額を切り捨てるものとする。

4 第2項の規定にかかわらず、放課後キッズクラブが所在する区の区長（以下「区長」という。）が特に必要と認める場合は、こども青少年局長と協議の上、別表1から別表11に定める補助金を変更することができる。

### （補助事業者）

第4条 この要綱における補助事業者は、次の各号に掲げる補助金の区分に応じ、当該各号に定める者とする。

- (1) 運営費補助 実施要綱第3条に規定する者

- (2) 開設費補助及び準備費補助 横浜市放課後キッズクラブ運営法人の選定に関する要綱（平成17年12月20日福子放第10167号）第3条第1項及び第2項に規定する放課後キッズクラブ運営法人の選定を、当該年度に受けた者

2 前項の規定にかかわらず、区長は、前条第1項第2号に係る経費に関して、特に必要と認められた者について、こども青少年局長と協議のうえ、補助事業者とすることができる。

（交付の申請）

第5条 運営費補助の交付を受けようとする補助事業者は、区長が定める期日までに横浜市放課後キッズクラブ事業費補助金交付申請書〔運営費補助〕（第2-1号様式）に次の各号に掲げる書類を添付し、区長に提出しなければならない。ただし、添付書類については、その内容を満たす補助事業者の資料をもって代えることができるものとする。

- (1) 運営概況（第3号様式）
- (2) 活動計画書（第4号様式）
- (3) 収支予算書（第5号様式）
- (4) 資金計画表（第6号様式）
- (5) その他区長が必要と認める書類

2 開設費補助の交付を受けようとする補助事業者は、区長が定める期日までに横浜市放課後キッズクラブ事業費補助金交付申請書〔開設費補助〕（第2-2号様式）に区長が必要と認める書類を添付し、区長に提出しなければならない。

3 準備費補助の交付を受けようとする補助事業者は、区長が定める期日までに横浜市放課後キッズクラブ事業費補助金交付申請書〔準備費補助〕（第2-3号様式）に区長が必要と認める書類を添付し、区長に提出しなければならない。

（交付の決定）

第6条 区長は、前条第1項の規定による申請を受理したときは、その内容を審査し、適正と認める場合は補助金の交付額を決定し、横浜市放課後キッズクラブ事業費補助金交付決定通知書〔運営費補助〕（第7-1号様式）により、補助事業者に通知するものとする。

2 区長は、前条第2項の規定による申請を受理したときは、その内容を審査し、適正と認める場合は補助金の交付額を決定し、横浜市放課後キッズクラブ事業費補助金交付決定通知書〔開設費補助〕（第7-2号様式）により、補助事業者に通知するものとする。

3 区長は、前条第3項の規定による申請を受理したときは、その内容を審査し、適正と認める場合は補助金の交付額を決定し、横浜市放課後キッズクラブ事業費補助金交付決定通知書〔準備費補助〕（第7-3号様式）により、補助事業者に通知するものとする。

（交付の時期等）

第7条 補助事業者の資金状況を勘案し、補助事業の完了前に補助金を交付しなければ、補助事業等を実施できない場合は、補助金規則第17条ただし書の規定により、補助事業の完了前に補助金の全部又は一部を交付することができる。

- 2 前項に定める補助金の交付は、補助事業者からの請求に基づいて交付するものとする。
- 3 補助金の交付の時期及び各期の交付額は、前条に規定する交付決定通知書において示すところによる。

(執行状況報告及び交付額の変更)

第8条 運営費補助の交付を受けた補助事業者は、当該年度の7月、1月及びその他区長が必要と認める月において、補助金の執行状況を区長が定める期日までに横浜市放課後キッズクラブ事業執行状況報告書(第8号様式)により報告しなければならない。ただし、当該年度の年度途中に開設する放課後キッズクラブについてはこの限りではない。

- 2 運営費補助のうち別表1の加算補助を受ける補助事業者は、前項の書類と合わせて別表12に定める書類を区長に提出しなければならない。ただし、届出要綱や実施要綱等に基づき、区長が補助事業者から既に報告を受けている書類について、区長はその書類の提出を省略させることができる。
- 3 前項に定めるほか、区長は必要に応じて補助金の執行状況に関する書類の提出を補助事業者を求めることができる。
- 4 第1項及び第2項に定める執行状況報告又はその他事情により、交付額の変更申請を行うときは、区長が定める期日までに横浜市放課後キッズクラブ事業費補助金変更交付申請書(第17号様式)に資金計画表(第6号様式)を添付し、区長に提出するものとする。
- 5 区長は、前項の規定による申請を受理したときは、その内容を審査し、適正と認める場合は補助金の交付額を決定し、横浜市放課後キッズクラブ事業費補助金変更交付決定通知書(第18号様式)により、補助事業者に通知するものとする。

(申請の取下げ)

第9条 補助金規則第9条第1項の規定により定める申請の取下げの期間は、補助事業者が第6条に規定する交付決定通知書又は前条第5項に規定する変更交付決定通知書の交付を受けた日の翌日から起算して10日以内の日とする。

(実績報告)

第10条 運営費補助の交付を受けた補助事業者は事業終了後、区長が定める期日までに横浜市放課後キッズクラブ事業実績報告書[運営費補助](第19-1号様式)及び基本事業費報告書(第20号様式)に区長が必要と認める書類を添付し、区長に提出しなければならない。また、第7条第1項の規定により補助事業の完了前に補助金の全部又は一部の交付を受けた場合は、補助金の精算を行わなければならない。

- 2 運営費補助のうち、障害児受入推進加算補助及び障害児受入強化推進加算補助の交付を受けた補助事業者は、前項に規定する実績報告時に、障害児受入に係る補助対象経費等報告書(第21号様式)とその他区長が必要と認める書類を提出しなければならない。
- 3 運営費補助のうち、医療的ケア児受入加算補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、医療的ケア児受入加算補助対象経費等報告書(第22号様式)とその他区長が必要と認める書類を提出しなければならない。

- 4 運営費補助のうち、育成支援体制強化加算補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、育成支援体制強化加算補助対象経費等報告書（第23号様式）とその他区長が必要と認める書類を提出しなければならない。
- 5 運営費補助のうち、放課後児童支援員等キャリアアップ処遇改善費補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、放課後児童支援員等キャリアアップ処遇改善費補助対象経費積算書（第24号様式）とその他区長が必要と認める書類を提出しなければならない。
- 6 運営費補助のうち、賃金改善加算補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、賃金改善加算補助実施報告書（第25号様式）及び賃金改善加算補助賃金改善額等内訳書（第26号様式）とその他区長が必要と認める書類を提出しなければならない。
- 7 運営費補助のうち、新型コロナウイルス感染拡大防止加算補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、新型コロナウイルス感染拡大防止加算補助対象経費等報告書（第27号様式）とその他区長が必要と認める書類を提出しなければならない。
- 8 開設費補助の交付を受けた補助事業者は事業終了後、区長が定める期日までに横浜市放課後キッズクラブ事業実績報告書[開設費補助]（第19-2号様式）に区長が必要と認める書類を添付し、区長に提出しなければならない。また、第7条第1項の規定により補助事業の完了前に補助金の全部又は一部の交付を受けた場合は、補助金の精算を行わなければならない。
- 9 準備費補助の交付を受けた補助事業者は事業終了後、区長が定める期日までに横浜市放課後キッズクラブ事業実績報告書[準備費補助]（第19-3号様式）に区長が必要と認める書類を添付し、区長に提出しなければならない。また、第7条第1項の規定により補助事業の完了前に補助金の全部又は一部の交付を受けた場合は、補助金の精算を行わなければならない。

#### （補助金額の確定）

- 第11条 運営費補助の交付を受けた補助事業者に対する補助金規則第15条の規定による補助金額の確定の通知は、横浜市放課後キッズクラブ事業費補助金交付額確定通知書 [運営費補助]（第28-1号様式）により通知するものとする。
- 2 開設費補助の交付を受けた補助事業者に対する補助金規則第15条の規定による補助金額の確定の通知は、横浜市放課後キッズクラブ事業費補助金交付額確定通知書 [開設費補助]（第28-2号様式）により通知するものとする。
  - 3 準備費補助の交付を受けた補助事業者に対する補助金規則第15条の規定による補助金額の確定の通知は、横浜市放課後キッズクラブ事業費補助金交付額確定通知書 [準備費補助]（第28-3号様式）により通知するものとする。

#### （決定の取消）

- 第12条 区長は、次のいずれかの事情が生じたときは、交付の決定の全部又は一部を取消することができる。
- (1) 実績報告書その他の書類を確認した結果、虚偽又は不正な手続によって補助金の交付を受けたものと認められるとき。
  - (2) この要綱及び実施要綱等に違反したとき。
  - (3) キッズクラブ事業実施方法が不相当であると区長が認めたとき。

- (4) 実施要綱に定める条件を欠くに至った場合、その他キッズクラブ事業を補助する必要がなくなると区長が認めたとき。
- 2 運営費補助の交付の決定の取消は、横浜市放課後キッズクラブ事業費補助金交付決定取消通知書[運営費補助]（第29-1号様式）により、補助事業者へ通知するものとする。
- 3 開設費補助の交付の決定の取消は、横浜市放課後キッズクラブ事業費補助金交付決定取消通知書[開設費補助]（第29-2号様式）により、補助事業者へ通知するものとする。
- 4 準備費補助の交付の決定の取消は、横浜市放課後キッズクラブ事業費補助金交付決定取消通知書[準備費補助]（第29-3号様式）により、補助事業者へ通知するものとする。

#### （補助金の返還）

第13条 区長は、補助金の交付の決定を取り消した場合において、事業の当該取消しに係る部分に関し、すでに補助金が交付されているときは、期限を定めて、その返還を命ずるものとする。

- 2 区長は、補助事業者へ交付すべき補助金の額を確定した場合において、既にその額を超える補助金が交付されているときは、期限を定めて、確定額を超える部分の補助金の返還を命ずるものとする。

#### （消費税及び地方消費税に係る仕入控除税額の確定に伴う補助金の返還）

第14条 補助事業者は、事業完了後に消費税及び地方消費税の申告によりこの補助金に係る消費税及び地方消費税に係る仕入控除税額が確定した場合は、速やかに、消費税及び地方消費税に係る仕入控除税額報告書（第30号様式）に必要な書類を添付し、区長へ報告しなければならない。

- 2 前項に定める報告について、補助事業者が全国的に事業を展開する組織の支部（又は支社、支所等）であって、自ら消費税及び地方消費税の申告を行わず、本部（又は本社、本所等）で消費税及び地方消費税の申告を行っている場合は、本部の課税売上割合等の申告に基づき報告を行うこと。
- 3 補助事業者は、第1項に規定する区長への報告を行った後、当該仕入控除税額分の補助金を市に返還しなければならない。

#### （財産の処分の制限）

第15条 補助金規則第25条の規定により財産の処分の制限がかからなくなるために必要な期間は、補助事業により取得し、又は効用の増加した不動産及びその従物並びに補助事業により取得し、又は効用の増加した価格が単価50万円以上の機械器具等については、「補助事業等により取得し、又は効用の増加した財産の処分制限期間」（令和5年こども家庭庁告示第9号）又は「補助事業等により取得し、又は効用の増加した財産の処分制限期間」（平成14年文部科学省告示第53号）に定めるとおりとする。

#### （暴力団排除に関する取扱い）

第16条 次の各号に該当する者は、この補助金の交付の対象としない。

- (1) 横浜市暴力団排除条例（平成23年12月横浜市条例第51号）第2条第2号の暴力団



- (2) 同条例同条第4号の暴力団員等
  - (3) 同条例同条第5号の暴力団経営支配法人等
  - (4) 同条例第7条の暴力団員等と密接な関係を有すると認められる者
- 2 区長は、必要に応じ申請者又は第6条の交付の決定を受けたものが、前項各号のいずれかに該当するか否かを神奈川県警察本部長に対して確認を行うことができる。
- 3 区長は、交付の決定を受けたものが、第1項各号のいずれかに該当するときは、交付決定の全部又は一部を取り消すことができる。

(書類の整備等)

第17条 補助事業者は、キッズクラブ事業の適正な管理を図るため、児童の利用状況、職員の出勤状況及びキッズクラブ事業に係る収入及び支出の状況を明らかにした帳簿等を備え保管するとともに、これらについての証拠書類を整理し、各年度のキッズクラブ事業終了後5年間保存しなければならない。

(調査又は報告)

第18条 区長は、補助金の適正な執行を確認するため等、必要があると認めるときは、補助事業者に対して、前条の書類を閲覧し、又は提出を求め、運営状況を調査し、又は報告を徴することができる。

(補則)

第19条 この要綱に定めるもののほか、この要綱の実施に関して必要な事項については、別に子ども青少年局長が定める。

附 則 (平成18年3月2日福子放第10304号)

(施行期日)

- 1 この要綱は、平成18年3月2日から施行し、平成18年度の予算に係る補助金等から適用する。  
(横浜市放課後キッズクラブ実施要綱の廃止)
- 2 横浜市放課後キッズクラブ事業実施要綱(平成16年7月1日)は、平成18年3月31日限り廃止する。

附 則 (平成18年6月12日こ放第210号)

この要綱は、平成18年6月12日から施行する。

附 則 (平成18年9月30日こ放第377号)

この要綱は、平成19年1月1日から施行する。

附 則 (平成19年3月12日こ放第841号)

この要綱は、平成19年3月12日から施行し、平成19年度の予算に係る補助金等から適用する。

附 則 (平成19年3月30日こ放第981号)

この要綱は、平成19年4月1日から施行する。

附 則（平成19年 5月31日こ放第142号）  
この要綱は、平成19年 7月 1日から施行する。

附 則（平成19年 9月 6日こ放第433号）  
この要綱は、平成19年11月 1日から施行する。

附 則（平成19年11月28日こ放第670号）  
この要綱は、平成20年 1月 4日から施行する。

附 則（平成20年 2月28日こ放第884号）  
この要綱は、平成20年 2月28日から施行し、平成20年度の予算に係る補助金等から適用する。

附 則（平成20年 8月27日こ放第353号）  
この要綱は、平成20年 9月 1日から施行する。

附 則（平成21年 3月19日こ放第839号）  
この要綱は、平成21年 4月 1日から施行し、平成21年度の予算に係る補助金等から適用する。

附 則（平成21年 8月27日こ放第458号）  
この要綱は、平成21年 9月 1日から施行する。

附 則（平成22年 3月17日こ放第880号）  
この要綱は、平成22年 4月 1日から施行し、平成22年度の予算に係る補助金等から適用する。

附 則（平成22年10月21日こ放第494号）  
この要綱は、平成22年10月21日から施行する。

附 則（平成23年 3月11日こ放第900号）  
この要綱は、平成23年 4月 1日から施行し、平成23年度の予算に係る補助金等から適用する。

附 則（平成23年 6月30日こ放第662号）  
この要綱は、平成23年 6月30日から施行し、平成23年度の予算に係る補助金から適用する。

附 則（平成24年 3月15日こ放第958号）  
この要綱は、平成24年 4月 1日から施行し、平成24年度の予算に係る補助金から適用する。

附 則（平成24年 6月29日こ放第281号）  
この要綱は、平成24年 6月29日から施行し、平成24年度の予算に係る補助金から適用する。

附 則（平成24年 8月 7日こ放第391号）  
この要綱は、平成24年 8月 7日から施行する。  
なお、税制改正前の扶養控除を適用した減免については、平成24年 6月 1日より施行する。

附 則（平成24年10月 1日こ放第720号）  
この要綱は、平成24年10月 1日から施行する。

附 則（平成25年 3月11日こ放第995号）  
この要綱は、平成25年 3月11日から施行し、平成25年度の予算に係る補助金から適用する。ただし、横浜市放課後キッズクラブ事業実績報告書（第15号様式）に係る改正規定は、平成24年度の予算に係る補助金から適用する。

附 則（平成25年10月18日こ放第 632 号）  
この要綱は、平成25年10月18日から施行し、平成25年度の予算に係る補助金から適用する。

附 則（平成26年 3 月10日こ放第948号）  
この要綱は、平成26年 3 月10日から施行し、平成26年度の予算に係る補助金から適用する。

附 則（平成26年10月 1 日こ放第623号）  
この要綱は、平成26年10月 1 日から施行し、平成26年度中に交付する補助金から適用する。

附 則（平成 27 年 3 月 10 日こ放第 971 号）  
この要綱は、平成27年 3 月10日から施行し、平成27年度の予算に係る補助金から適用する。

附 則（平成27年10月 1 日こ放第656号）  
この要綱は、平成 27 年 10 月 1 日から施行し、平成 27 年度中に交付する補助金から適用する。

附 則（平成 28 年 3 月 10 日こ放第 1158 号）  
この要綱は、平成28年 3 月10日から施行し、平成28年度の予算に係る補助金から適用する。

附 則（平成28年 7 月25日こ放第403号）  
この要綱は、平成28年 7 月25日から施行し、平成28年度中に交付する補助金から適用する。

附 則（平成 28 年 11 月 1 日こ放第 663 号）  
この要綱は、平成28年11月 1 日から施行し、平成28年度中に交付する補助金から適用する。

附 則（平成 29 年 3 月 10 日こ放第 1118 号）  
この要綱は、平成 29 年 3 月 10 日から施行し、平成 29 年度の予算に係る補助金から適用する。

附 則（平成 29 年 10 月 31 日こ放第 678 号）  
この要綱は、平成 29 年 11 月 1 日から施行し、平成 29 年度の予算に係る補助金から適用する。

附 則（平成 30 年 1 月 15 日こ放第 882 号）  
この要綱は、平成 30 年 1 月 15 日から施行し、平成 29 年度の予算に係る補助金から適用する。

附 則（平成 30 年 3 月 8 日こ放第 1068 号）  
この要綱は、平成 30 年 3 月 8 日から施行し、平成 30 年度の予算に係る補助金から適用する。

附 則（平成 30 年 10 月 1 日こ放第 623 号）  
この要綱は、平成 30 年 10 月 1 日から施行し、平成 30 年度の予算に係る補助金から適用する。

附 則（平成 31 年 3 月 1 日こ放第 1090 号）  
この要綱は、平成 31 年 3 月 1 日から施行し、平成 31 年度の予算に係る補助金から適用する。

附 則（令和 2 年 3 月 1 日こ放第 1098 号）

この要綱は、令和2年3月1日から施行し、令和2年度の予算に係る補助金から適用する。

附 則（令和2年9月10日こ放第977号）

この要綱は、令和2年9月10日から施行し、令和2年度中に交付する補助金から適用する。

附 則（令和3年3月1日こ放第2142号）

この要綱は、令和3年3月1日から施行し、令和3年度中に交付する補助金から適用する。

附 則（令和4年2月25日こ放第2225号）

この要綱は、令和4年2月25日から施行し、令和4年度中に交付する補助金から適用する。賃金改善加算補助については、令和3年度に当該事業所において運営費補助の交付を受けた事業者のみ補助対象期間を令和4年2月1日に遡及して適用する。

附 則（令和4年7月1日こ放第1641号）

この要綱は、令和4年7月1日から施行し、令和4年度中に交付する補助金から適用する。

附 則（令和5年2月27日こ放第2747号）

この要綱は、令和5年2月27日から施行し、令和5年度の予算に係る補助金から適用する。

附 則（令和5年6月20日こ放第479号）

この要綱は、令和5年6月20日から施行し、令和5年度中に交付する補助金から適用する。

附 則（令和5年8月23日こ放第728号）

この要綱は、令和5年8月23日から施行し、令和5年度中に交付する補助金から適用する。

附 則（令和5年12月7日こ放第1118号）

この要綱は、令和5年12月7日から施行し、令和5年度中に交付する補助金から適用する。

別表1 (第3条第2項)

## 【放課後キッズクラブ事業費補助金算定基準】

項目		金額		基準年月	算定基準	補助対象経費
基本補助	基礎部分 (支援の単位あたり)	別表2のとおり				
	子ども教室基礎部分 (1クラブあたり)					
	子ども教室規模調整部分 (1クラブあたり)					
	開所日数加算補助 (支援の単位あたり)	19,000円/日	当該年度の4月から3月までの実績	年間250日を超えて開所している日数	人件費・事業費・ 管理運営費等	
長時間開所加算補助 (支援の単位あたり)	30分あたり 92,000円/年	当該年度の4月から3月までの実績	支援の単位が2つ以上あるクラブについて、2単位目以降の支援の単位が土曜日及び学校休業日に8時間を超えて開所している年間平均時間数 ※年間平均時間数は、30分単位で算定するものとする。(30分未満の端数は切り捨て)			
夏季休業期間加算補助 (1クラブあたり)	19,000円/日	当該年度の4月から8月までの実績	7・8月の支援の単位数の平均(※)が、4～6月の支援の単位数の平均(※)と比較して増えているクラブについて、当該単位に必要な条例第10条第2項で定める職員最低配置基準を満たし、開所している日数 ※小数点以下切り上げ			
子ども教室加算補助 (1クラブあたり)	1,066,000円/年	当該年度の4月から6月までの実績	クラブ全体の平均利用児童数に対するわくわく【区分1】の平均利用児童数の各月の割合の平均が40%から50%を占める場合 ※小数点以下切り上げ			
	1,332,000円/年		クラブ全体の平均利用児童数に対するわくわく【区分1】の平均利用児童数の各月の割合の平均が51%以上を占める場合 ※小数点以下切り上げ			
運営費補助	障害児受入加算補助 (1人あたり)	別表3のとおり				
	障害児受入推進加算補助 (支援の単位あたり)	別表4のとおり				
	障害児受入強化推進加算補助 (支援の単位あたり)	別表5のとおり				
	医療的ケア児受入加算補助 (支援の単位あたり)	別表6のとおり				
	育成支援体制強化加算補助 (1クラブあたり)	別表7のとおり				
	放課後児童支援員等キャリアアップ処遇改善費補助 (支援の単位あたり)	上限 919,000円/年	当該年度の4月から3月までの実績 ※2、3月は1月の実績を適用するものとする	放課後児童支援員等の賃金改善に要した費用	賃金改善に要する経費	
	賃金改善加算補助 (常勤職員換算1.0人あたり)	別表8のとおり				
特別加算	保護者負担減免額相当補助 (1人あたり)	上限 2,500円/月	当該年度の4月から3月までの実績 ※1～3月は12月の実績を適用するものとする	実施要綱別表3に規定する保護者負担減免額相当補助の対象となる世帯の児童	減免対象児童の保護者負担金の減免に要する費用	
	人材育成加算補助 (1クラブあたり)	常勤職員1人あたり 4,000円 非常勤職員1人あたり 2,230円	当該年度の4月から12月までの実績	横浜市が指定する研修を受講した職員の人数 ※実施要綱第9条4項に基づく研修計画を策定し、運営法人が主催となる研修を1回以上実施することを要件とする。 ※同一人物が複数回研修を受講した場合でも人数は1人分とする。	研修受講に要する人件費・研修開催に要する経費等	
	常勤職員の産前・産後休暇に伴う代替職員配置経費補助 (1人あたり)	別表9のとおり				
	新型コロナウイルス感染拡大防止加算補助 (支援の単位あたり)	別表10のとおり				
活動場所加算補助 (1クラブあたり)	別表11のとおり					
その他	ウクライナ避難民支援加算補助 (1人あたり)	利用料 上限 5000円/月 (7、8月のみ 5500円/月)	当該年度の4月から3月までの実績 ※1～3月は12月の実績を適用するものとする	実施要綱第20条に規定されている児童	利用料相当額(利用実態がある場合に限る。一時利用料を含む。)	
		保険料 上限 800円/年			保険料相当額	
		おやつ代 実費相当額			実費相当額	
		その他保護者負担金 実費相当額			実費相当額 (特別な行事や教材にかかる費用等)	
開設費補助 (1か所あたり)	800,000円/年		新規に開設または運営法人が変更になる放課後キッズクラブの初度調弁費	初度調弁費		

準備費補助 (1か所あたり)	400,000円/年		新規に開設または運営法人が変更になる放課後キッズクラブの準備人件費	人件費等
-------------------	------------	--	-----------------------------------	------

注1 開所月数が12か月に満たない放課後キッズクラブについては、原則として開所月数に応じた補助金額とする（百円未満切捨て）。

注2 実績の小数点以下の端数は切り上げて計算するものとする。

注3 常勤職員については、運営主体は令和3年度の処遇を維持または向上するよう努めなければならない。非常勤職員は、神奈川県最低賃金を下回らないものとする。

注4 新たに設置する小学校（統合校及び分校を除く）に放課後キッズクラブを開設する場合には、開設費補助は1,600,000円/年とする。

注5 日枝小学校放課後キッズクラブについては、2,224,000円を基本補助額に加算するものとする。

注6 市場小学校放課後キッズクラブについては、7,610,000円を基本補助額に加算するものとする。

注7 勝田小学校放課後キッズクラブについては、1,271,000円を基本補助額に加算するものとする。

注8 上菅田笹の丘小学校放課後キッズクラブについては、869,000円を基本補助額に加算するものとする。

注9 補助対象経費には、当該放課後キッズクラブの実施に関わらない経費は含まない。

注10 当該年度の4月から3月までの年間開所日数が200日に満たない支援の単位については、基本補助（基礎部分）、障害児受入推進加算補助、障害児受入強化推進加算補助、医療的ケア児受入加算補助、放課後児童支援員等キャリアアップ処遇改善費補助及び新型コロナウイルス感染拡大防止加算補助の補助対象とならない。

注11 クラブが運営する全ての支援の単位の当該年度の4月から3月までの年間開所日数が200日に満たない場合は、基本補助（子ども教室基礎部分及び子ども教室規模調整部分）及び子ども教室加算補助を除き別表1に規定する全ての基本事業費及び特別加算について、補助対象とならない。

別表2（第3条第2項）

項目	基本補助																													
補助基準額	<p>基本補助は、次の（1）から（3）の合計額とする。</p> <p>（1）基礎部分            当該年度の4月から3月の各月1日時点における支援の単位ごとの対象児童数の平均及び当該年度の4月から3月までの支援の単位ごとの年間開所日数に応じて、支援の単位ごとに次のとおり補助上限額（年額）を決定する。</p> <table border="1" data-bbox="408 369 1358 533"> <thead> <tr> <th rowspan="2">対象児童数</th> <th colspan="2">年間開所日数</th> </tr> <tr> <th>200～249日</th> <th>250日以上</th> </tr> </thead> <tbody> <tr> <td>1～19人</td> <td>2,351,000円</td> <td>3,716,000円</td> </tr> <tr> <td>20～40人</td> <td>3,099,000円</td> <td>5,267,000円</td> </tr> </tbody> </table> <p>（2）子ども教室基礎部分            1クラブあたり 2,164,000円（年額）</p> <p>（3）子ども教室規模調整部分            当該年度の4月から6月の支援の単位数の平均及び対象児童数に応じて、次の通り補助額を決定する。なお、対象児童数の平均については、小数点以下を切り上げるものとする。</p> <table border="1" data-bbox="408 772 1358 1021"> <thead> <tr> <th>支援の単位数</th> <th>対象児童数</th> <th>補助額（年額）</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>19人以下</td> <td>2,131,000円</td> </tr> <tr> <td>1</td> <td>20人以上</td> <td>1,998,000円</td> </tr> <tr> <td>2</td> <td>-</td> <td>1,732,000円</td> </tr> <tr> <td>3</td> <td>-</td> <td>1,598,000円</td> </tr> <tr> <td>4以上</td> <td>-</td> <td>933,000円</td> </tr> </tbody> </table>	対象児童数	年間開所日数		200～249日	250日以上	1～19人	2,351,000円	3,716,000円	20～40人	3,099,000円	5,267,000円	支援の単位数	対象児童数	補助額（年額）	1	19人以下	2,131,000円	1	20人以上	1,998,000円	2	-	1,732,000円	3	-	1,598,000円	4以上	-	933,000円
対象児童数	年間開所日数																													
	200～249日	250日以上																												
1～19人	2,351,000円	3,716,000円																												
20～40人	3,099,000円	5,267,000円																												
支援の単位数	対象児童数	補助額（年額）																												
1	19人以下	2,131,000円																												
1	20人以上	1,998,000円																												
2	-	1,732,000円																												
3	-	1,598,000円																												
4以上	-	933,000円																												
補助対象経費	人件費・事業費・管理運営費等																													
特記事項	<ul style="list-style-type: none"> <li>・実施要綱第6条第2項に定める開所時間を通じて、条例第10条第2項に定める職員の最低配置基準を満たしていない日については、基礎部分の開所日数の算定に含めることができない。ただし、支援の単位が2つ以上あるクラブにおいて、2以降の支援単位が、条例第18条第1項第1号又は第2号に定める時間を通じて、条例第10条第2項に定める職員の最低配置基準を満たしている場合は、当該支援の単位について基礎部分の開所日数の算定に含めることができる。</li> <li>・当該年度の4月1日時点の支援単位ごとの対象児童数が40人以下であったが、当該年度の4月から3月までの対象児童数の平均が41人以上45人以下となった支援の単位については、基礎部分は「20～40人」の欄の補助額を適用するものとする。</li> </ul>																													

別表3（第3条第2項）

項目	障害児受入加算補助
補助対象児童	わくわく【区分1】登録かつ以下のいずれかの条件を満たす児童 (1) 特別支援学校又は個別支援学級に在籍している児童 (2) 一般学級に在籍している児童のうち、「身体障害者手帳」、「療育手帳（愛の手帳）」または「精神障害者保健福祉手帳」の写しが提出されている児童 (3) 就学している小学校等から児童の状況についての副申が記載された「支援や配慮を要する児童の申立書（第1号様式）」及び「児童状況書（第1の2号様式）」が提出されている児童
算定基準	当該年度の4月から3月までの補助対象児童の利用児童数 ※1～3月は12月の実績を適用するものとする。
補助額 （年額）	1人あたり 483,000円
補助対象経費	人件費・事業費・管理運営費等

別表4（第3条第2項）

項目	障害児受入推進加算補助														
補助対象児童	次のいずれかの条件を満たす児童 (1) 特別支援学校又は個別支援学級に在籍している児童 (2) 一般学級に在籍している児童のうち、「身体障害者手帳」、「療育手帳（愛の手帳）」または「精神障害者保健福祉手帳」の写しが提出されている児童 (3) 就学している小学校等から児童の状況についての副申が記載された「支援や配慮を要する児童の申立書（第1号様式）」及び「児童状況書（第1の2号様式）」が提出されている児童 (4) 別表6に定める医療的ケア児受入加算補助の補助対象児童														
補助上限額の算定期間	当該年度の4月から3月までのうち、すくすく【区分2】登録の補助対象児童の利用見込みがある月 ※1～3月は12月の実績を適用するものとする <b>【利用見込みがあるとする条件と補助対象期間】</b> 次のいずれかの条件に該当する場合、利用見込みがあるものとする。 条 件①：すくすく【区分2】登録の補助対象児童の利用登録があった場合 補助対象期間：すくすく【区分2】登録の補助対象児童の利用登録があった月から3月まで  条 件②：わくわく【区分1】登録の補助対象児童の利用登録があった場合 ※条件①に該当する支援の単位がない場合に限り、申請することができる。 補助対象期間：わくわく【区分1】登録の補助対象児童の利用登録があった月から3月まで														
補助上限額	当該年度の4月から3月において、実施要綱第6条第1項に定める開所日のうち、条例第10条第2項及び実施要綱第8条第1項で定める職員最低配置基準に加えて1人以上職員を追加配置した日数に応じて、次のとおり支援の単位ごとに各月の補助上限額を決定する。1月から3月の実績については12月の実績を適用する。なお、支援の単位ごとの年間の補助上限額は2,009,000円とする。 <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>職員を追加配置した日数（1か月あたり）</th> <th>補助上限額（月額）</th> </tr> </thead> <tbody> <tr> <td>18日以上</td> <td>168,000円</td> </tr> <tr> <td>13日以上17日以下</td> <td>151,000円</td> </tr> <tr> <td>9日以上12日以下</td> <td>118,000円</td> </tr> <tr> <td>5日以上8日以下</td> <td>84,000円</td> </tr> <tr> <td>3日以上4日以下</td> <td>50,000円</td> </tr> <tr> <td>2日以下</td> <td>0円</td> </tr> </tbody> </table>	職員を追加配置した日数（1か月あたり）	補助上限額（月額）	18日以上	168,000円	13日以上17日以下	151,000円	9日以上12日以下	118,000円	5日以上8日以下	84,000円	3日以上4日以下	50,000円	2日以下	0円
職員を追加配置した日数（1か月あたり）	補助上限額（月額）														
18日以上	168,000円														
13日以上17日以下	151,000円														
9日以上12日以下	118,000円														
5日以上8日以下	84,000円														
3日以上4日以下	50,000円														
2日以下	0円														
補助対象経費	年間を通じて障害児を受け入れるために配置した職員（「以下、障害児受入職員」という。）に要した人件費（ただし、異なる支援の単位で同一の職員を補助対象とすることはできない。） ※年間の補助上限額と補助対象経費を比較して、低い額で決定														
研修の受講	障害児受入推進加算補助の交付を受ける放課後キッズクラブは、交付を受ける年度において、児童の育成支援にあたる職員全員に横浜市が指定する研修を受講させなければならない。														



別表5（第3条第2項）

項目		障害児受入強化推進加算補助			
補助対象児童	次のいずれかの条件を満たす児童 (1) 特別支援学校又は個別支援学級に在籍している児童 (2) 一般学級に在籍している児童のうち、「身体障害者手帳」、「療育手帳（愛の手帳）」または「精神障害者保健福祉手帳」の写しが提出されている児童 (3) 就学している小学校等から児童の状況についての副申が記載された「支援や配慮を要する児童の申立書（第1号様式）」及び「児童状況書（第1の2号様式）」が提出されている児童				
区分	支援の単位ごとの補助対象児童の登録児童数に応じて、交付を受けることができる区分を支援の単位ごとに決定する。				
	区分	区分の説明	交付を受けるための要件	交付を受けることができる区分	
	強化①	障害児受入推進加算補助による追加配置に加え、更に1名職員を配置する	支援の単位ごとの補助対象児童の登録児童数が3人以上	強化①	
	強化②	強化①による追加配置に加え、更に1名職員を配置する	支援の単位ごとの補助対象児童の登録児童数が6人以上	強化①+強化②	
強化③	強化②による追加配置に加え、更に1名職員を配置する	支援の単位ごとの補助対象児童の登録児童数が9人以上	強化①+強化②+強化③		
補助上限額の算定期間	支援の単位ごとに、それぞれ下記の期間とする。なお、1～3月は12月の実績を適用するものとする。				
	区分	算定期間			
	強化①	支援の単位ごとの補助対象児童の登録児童数が3人以上である月数			
	強化②	支援の単位ごとの補助対象児童の登録児童数が6人以上である月数			
	強化③	支援の単位ごとの補助対象児童の登録児童数が9人以上である月数			
補助上限額	実施要綱第6条第1項に定める開所日のうち、障害児受入推進加算補助による追加配置に加え、更に職員を追加配置した日数に応じて、強化①、強化②、強化③でそれぞれ、次のとおり支援の単位ごとに各月の補助上限額を決定する。1月から3月については12月の実績を適用する。なお、支援の単位ごとの年間の補助上限額は強化①、強化②、強化③それぞれ2,000,000円とする。				
	職員を追加配置した日数（1か月あたり）	補助上限額（月額）			
	18日以上	167,000円			
	13日以上17日以下	150,000円			
	9日以上12日以下	117,000円			
	5日以上8日以下	84,000円			
	3日以上4日以下	50,000円			
	2日以下	0円			
補助対象経費	年間を通じて障害児受入職員の配置に要した人件費（ただし、異なる支援の単位で同一の職員を補助対象とすること及び障害児受入推進加算補助の補助対象となった職員を補助対象とすることはできない。） ※年間の補助上限額と補助対象経費を比較して、低い金額で決定				

別表6（第3条第2項）

項目	医療的ケア児受入加算補助									
補助対象児童	<p>次のすべての条件を満たす児童</p> <p>(1) 放課後キッズクラブのすくすく区分（区分2A・B）に在籍する児童で日常的に看護師等による医療的ケアを必要とする児童のうち、児童が通う学校において医療的ケアを受けている又は受ける予定である児童</p> <p>(2) 主治医からキッズクラブでの活動において医療的ケアが必要とされた児童</p> <p>(3) 保護者から医療的ケアの利用申し込みがあり、放課後キッズクラブでの医療的ケアの実施内容について保護者の同意が得られた児童</p> <p>(4) 上記(1)～(3)の条件を満たす児童の受入れについて、看護師等の配置が可能な見込みであると本市が確認していること。</p> <p>※ 医療的ケアとは次のいずれかに該当するものをいう。</p> <table border="1" data-bbox="386 483 1169 694"> <tr> <td>・ 口腔内の喀痰吸引（①口腔内、②鼻腔内、③気管カニューレ内部）</td> </tr> <tr> <td>・ 経管栄養（①胃ろう又は腸ろう、②経鼻）</td> </tr> <tr> <td>・ 導尿</td> </tr> <tr> <td>・ その他こども青少年局長が必要と定める医療的ケア</td> </tr> </table>	・ 口腔内の喀痰吸引（①口腔内、②鼻腔内、③気管カニューレ内部）	・ 経管栄養（①胃ろう又は腸ろう、②経鼻）	・ 導尿	・ その他こども青少年局長が必要と定める医療的ケア					
・ 口腔内の喀痰吸引（①口腔内、②鼻腔内、③気管カニューレ内部）										
・ 経管栄養（①胃ろう又は腸ろう、②経鼻）										
・ 導尿										
・ その他こども青少年局長が必要と定める医療的ケア										
補助上限額の算定期間	補助対象児童が放課後キッズクラブを利用し、看護師等を配置した月数									
補助上限額	<p>実施要綱第6条第1項に定める開所日のうち、看護師等を配置した期間に応じて、次のとおり支援の単位ごとに各月の補助額を決定する。1月から3月の実績については12月の実績を適用する。なお、支援の単位ごとの年間補助上限額は「配置」が4,061,000円、「送迎」が1,353,000円とする。</p> <table border="1" data-bbox="386 996 1257 1164"> <thead> <tr> <th>区分</th> <th>要件</th> <th>補助上限額（月額）</th> </tr> </thead> <tbody> <tr> <td>配置</td> <td>医療的ケアを実施する看護師等を配置した場合</td> <td>339,000円</td> </tr> <tr> <td>送迎</td> <td>送迎、付き添いに伴う看護師等を配置した場合</td> <td>113,000円</td> </tr> </tbody> </table>	区分	要件	補助上限額（月額）	配置	医療的ケアを実施する看護師等を配置した場合	339,000円	送迎	送迎、付き添いに伴う看護師等を配置した場合	113,000円
区分	要件	補助上限額（月額）								
配置	医療的ケアを実施する看護師等を配置した場合	339,000円								
送迎	送迎、付き添いに伴う看護師等を配置した場合	113,000円								
補助対象経費	<p>配置：医療的ケアを実施する看護師等の人件費・交通費</p> <p>送迎：補助対象児童の送迎付き添いに伴う看護師等の人件費・交通費</p> <p>※年間の補助上限額と補助対象経費を比較して、低い額で決定</p>									
特記事項	<ul style="list-style-type: none"> <li>・ 当面の間「看護師等」は「看護師」と読み替えるものとする。</li> <li>・ 補助対象経費に記載している看護師等の業務を外部委託等により実施し、クラブの運営主体が委託費等として支出する場合も、当該加算補助の対象とする。</li> <li>・ 補助金規則第24条ただし書きの規定により、補助事業者は、補助対象児童の受入れ支援にかかる補助金の補助事業に係る業務の委託等を行う場合、2人以上の市内事業者による入札又は見積書の徴収を省略することができる。</li> <li>・ 当該加算補助の補助対象となった看護師等は、条例第10条第2項及び実施要綱第8条第1項に定める職員の最低配置基準に含めることはできない。</li> <li>・ 当該加算補助の補助対象となった看護師等は、障害児受入推進加算補助及び障害児受入強化推進加算補助の補助対象とすることができない。</li> </ul>									

別表7（第3条第2項）

項目	育成支援体制強化加算補助
補助上限額 (年額)	1クラブあたり 1,451,000円
補助対象経費	<p>育成支援の周辺業務を行う職員（以下「運営事務等を行う職員」という。）の配置等に要する経費            なお、運営事務等を行う職員は次の業務を行うこととする。</p> <p>(1) 業務の実施状況に関する日誌（児童の出欠席、職員の服務に関する状況等）の作成            (2) おやつ発注、購入等            (3) 遊びの環境と施設の安全点検、衛生管理（清掃や消毒等）、整理整頓            (4) 会計事務等            (5) 児童の宿題等の学習活動が自主的に行える環境整備の補助            (6) その他、クラブの運営に関わる業務や育成支援の周辺業務</p>
特記事項	<ul style="list-style-type: none"> <li>・上記(1)～(6)に記載している運営事務等を行う職員の業務を外部委託等により実施し、クラブの運営主体が委託費等として支出する場合も、当該加算補助の対象とする。</li> <li>・放課後児童支援員等、児童の育成支援にあたる職員の人件費は、当該加算補助の対象とならない。ただし、育成支援にあたる常勤職員が事務処理等の事務を行うための超過勤務手当その他これに類する費用については、当該加算補助の対象とする。</li> <li>・当該加算補助の補助対象となった運営事務等を行う職員は、実施要綱第8条第1項に定める職員の最低配置基準に含めることはできない。</li> </ul>

別表8（第3条第2項）

項目	賃金改善加算補助
補助対象者	放課後児童支援員、補助員、事務職員等のクラブに勤務する職員（非常勤職員を含み、経営に携わる運営主体の役員である職員を除く）
補助対象経費	<p>(1) 職員の賃金改善に要する経費            (2) 当該賃金改善に伴い増加する法定福利費等の事業主負担分</p>
補助額	<p>補助額は、次の計算式により算出された金額とする。</p> <p><math>11,000円 \times 賃金改善対象者数 \times 事業実施月数</math></p> <p>※賃金改善対象者数とは、賃金改善を行う常勤職員数に、1か月あたりの勤務時間数を就業規則等で定めた常勤職員の1か月あたりの勤務時間数で除した非常勤職員数（常勤換算）を加えたものをいう。</p>
補助要件	<p>(1) 賃金改善加算補助実施計画書（第12号様式）を作成すること。また、計画の具体的な内容を職員に周知すること。</p> <p>(2) 賃金改善加算補助の補助額は、職員の賃金改善及び当該賃金改善に伴い増加する法定福利費等の事業主負担分に全額充てること。</p> <p>(3) 賃金改善加算補助の実施に伴う賃金改善が賃上げ効果の継続に資するよう、最低でも賃金改善の合計額の3分の2以上は、基本給又は決まって毎月支払われる手当の引上げにより改善を図ること。</p> <p>(4) 賃金改善加算補助の実施により改善を行う賃金項目以外の賃金項目（業績等に応じて変動するものを除く。）の水準を低下させていないこと。</p> <p>(5) 賃金改善加算補助の実施により講じた賃金改善の水準を維持すること。</p>

別表9（第3条第2項）

項目	常勤職員の産前・産後休暇に伴う代替職員配置経費補助						
補助額	<p>産前・産後休暇を取得する職員の職位に応じて、次のとおり補助上限額を決定する。ただし、下表の補助上限額の括弧内の金額については、当該職員が多胎妊娠の場合に適用する。</p> <table border="1"> <thead> <tr> <th>産前・産後休暇を取得する職員の職位</th> <th>補助上限額（年額）</th> </tr> </thead> <tbody> <tr> <td>主任</td> <td>498,000円（783,000円）</td> </tr> <tr> <td>副主任</td> <td>420,000円（660,000円）※</td> </tr> </tbody> </table> <p>※ただし、副主任の勤務時間数が週30時間以上の場合は、498,000円（783,000円）とする。</p>	産前・産後休暇を取得する職員の職位	補助上限額（年額）	主任	498,000円（783,000円）	副主任	420,000円（660,000円）※
産前・産後休暇を取得する職員の職位	補助上限額（年額）						
主任	498,000円（783,000円）						
副主任	420,000円（660,000円）※						
補助対象経費	<p>主任又は副主任が産前・産後休暇を取得する期間について、運営主体が当該職員に第3条第3項に定める職員給与最低基準以上の給与を支払う場合の当該期間（14週。ただし、多胎妊娠の場合は22週）の代替職員の配置にかかる人件費。 なお、当該職員の産前・産後休暇が当該年度だけでなく次年度に渡る場合は、日割りで加算額を積算する。</p>						

別表10（第3条第2項）

項目	新型コロナウイルス感染拡大防止加算補助						
補助上限額	<p>当該年度の4月から3月までの支援の単位ごとの対象児童数の平均に応じて、次のとおり支援の単位ごとに補助上限額を決定する。※1～3月は12月の実績を適用するものとする。</p> <table border="1"> <thead> <tr> <th>対象児童数</th> <th>補助上限額</th> </tr> </thead> <tbody> <tr> <td>1～19人</td> <td>300,000円</td> </tr> <tr> <td>20～40人</td> <td>400,000円</td> </tr> </tbody> </table>	対象児童数	補助上限額	1～19人	300,000円	20～40人	400,000円
対象児童数	補助上限額						
1～19人	300,000円						
20～40人	400,000円						
補助対象経費	<p>新型コロナウイルスの感染者や濃厚接触者が発生した場合に、職員が感染症対策の徹底を図りながら、事業を継続的に実施していくために必要な経費</p>						

別表11（第3条第2項）

項目	活動場所加算補助															
補助対象クラブ	<p>以下のいずれかの条件を満たすクラブ            (1) 活動場所(※)が3か所以上のクラブ            (2) 活動場所(※)が2か所であり、活動場所の所在する階または棟が異なるクラブ            ※当該加算補助における活動場所とは、届出要綱第3条第1項に定める放課後児童健全育成事業開始届または届出要綱第4条第1項に基づく放課後児童健全育成事業変更届（以下、「届出」という。）の「面積及び構造」に記載している専用ルームまたは兼用ルームを指す。ただし、区長が認める場合はこの限りではない。            なお、学校の校舎内に兼用ルームがある場合を除き、別棟のキッズクラブについては当該加算補助の対象外となる。</p>															
算定基準	<p>当該年度の6月、9月、12月の各月1日時点の届出に基づき決定する。</p>															
補助額	<p>補助額は四半期ごとに以下のとおりとする。</p> <table border="1"> <thead> <tr> <th>期間</th> <th>算定時点</th> <th>補助額</th> </tr> </thead> <tbody> <tr> <td>第1四半期</td> <td>6月1日時点</td> <td>228,000円</td> </tr> <tr> <td>第2四半期</td> <td>9月1日時点</td> <td>228,000円</td> </tr> <tr> <td>第3四半期</td> <td>12月1日時点</td> <td>238,000円</td> </tr> <tr> <td>第4四半期</td> <td>12月1日時点</td> <td>239,000円</td> </tr> </tbody> </table>	期間	算定時点	補助額	第1四半期	6月1日時点	228,000円	第2四半期	9月1日時点	228,000円	第3四半期	12月1日時点	238,000円	第4四半期	12月1日時点	239,000円
期間	算定時点	補助額														
第1四半期	6月1日時点	228,000円														
第2四半期	9月1日時点	228,000円														
第3四半期	12月1日時点	238,000円														
第4四半期	12月1日時点	239,000円														
補助対象経費	<p>人件費・事業費・管理運営費等</p>															

別表12（第8条第2項）

項目	提出書類
基本補助	
開所日数加算補助	<ul style="list-style-type: none"> <li>・すくすく【区分2】登録者名簿（実施要綱第3号様式）</li> <li>・すくすく【区分2】登録児童の利用申込書の写し</li> </ul>
夏季休業期間加算補助	
障害児受入加算補助	<ul style="list-style-type: none"> <li>・障害児等受入に係る加算補助対象児童名簿（第9号様式）</li> </ul>
障害児受入推進加算補助	<ul style="list-style-type: none"> <li>・補助対象児童であることがわかる書類（支援や配慮を要する児童の申立書（第1号様式）及び児童状況書（第1の2号様式）の写し、身体障害者手帳の写し 等）</li> </ul>
障害児受入強化推進加算補助	<ul style="list-style-type: none"> <li>・月別開所状況及び職員配置状況を証する書類</li> <li>・障害児の受入に係る研修の受講状況を証する書類</li> </ul>
医療的ケア児受入加算補助	<ul style="list-style-type: none"> <li>・障害児等受入に係る加算補助対象児童名簿（第9号様式）</li> <li>・医療的ケア児受入加算補助対象児童であることが分かる書類 ※次の(1)～(4)の書類全て <ul style="list-style-type: none"> <li>(1) 補助対象児童が通う学校の「医療的ケア実施可否結果通知書」の写し</li> <li>(2) 医療的ケアに関する主治医指示書の写し</li> <li>(3) 保護者からの医療的ケアに関する申込書兼同意書の写し</li> <li>(4) 医療的ケア児受入実施計画書</li> </ul> </li> </ul>
放課後児童支援員等キャリアアップ処遇改善費補助	<ul style="list-style-type: none"> <li>・放課後児童支援員等キャリアアップ処遇改善費補助 対象者一覧（第10号様式）</li> <li>・放課後児童支援員等キャリアアップ処遇改善費補助 要件確認表（第11号様式）</li> <li>・放課後児童支援員であることを証する書類（研修受講修了証等） ※申請初年度のみ</li> <li>・職歴を証する書類（勤務実績証明書等） ※過年度に同一の内容で提出している場合は省略可</li> <li>・本市が指定する研修を受講したことを証する書類</li> <li>・キャリアアップ体系を設けていることを証する書類（就業規則等）</li> <li>・賃金が改善されたことを証する書類（前年度の就業規則等）</li> </ul> <p>※過年度に提出している場合は省略可</p>
賃金改善加算補助	<ul style="list-style-type: none"> <li>・賃金改善加算補助実施計画書（第12号様式）</li> <li>・賃金改善加算補助賃金改善見込額等内訳書（第13号様式）</li> <li>・賃金が改善されたことを証する書類（前年度の就業規則等）</li> </ul> <p>※過年度に提出している場合は省略可</p>
保護者負担減免額相当補助	<ul style="list-style-type: none"> <li>・保護者負担減免額相当補助対象児童名簿（第14号様式）</li> <li>・実施要綱別表3に規定する保護者負担減免額相当補助の対象世帯であることがわかる書類（就学援助申請の審査結果及び支給についてのお知らせの写し、保護証明書の写し、市民税・県民税課税（非課税）証明書の写し 等）</li> </ul>
人材育成加算補助	<ul style="list-style-type: none"> <li>・実施要綱第9条第4項に基づく研修計画※7月の執行状況報告のみ</li> <li>・人材育成加算補助実施報告書（第15号様式）※1月の執行状況報告のみ</li> </ul>
常勤職員の産前・産後休暇に伴う代替職員配置経費補助	<ul style="list-style-type: none"> <li>・常勤職員の産前・産後休暇に伴う代替職員配置経費補助確認書（第16号様式）</li> <li>・常勤職員の出産予定日がわかる書類（母子健康手帳の写し、診断書の写し 等）</li> </ul>
ウクライナ避難民支援加算補助	<ul style="list-style-type: none"> <li>・ウクライナからの避難民への支援内容を証する書類</li> </ul>

## 支援や配慮を要する児童の申立書

年 月 日

横浜市 区長

所在地

法人名

代表者職氏名

(クラブ名)

放課後キッズクラブ

横浜市放課後キッズクラブ事業費補助金交付要綱別表1に基づき、支援や配慮を要する児童であることを申し立てます。

児童氏名	
学年	
利用区分 (該当するものを ○囲み)	<ul style="list-style-type: none"> <li>・わくわく【区分1】</li> <hr/> <li>・すくすく(ゆうやけ)【区分2A】</li> <hr/> <li>・すくすく(ほしぞら)【区分2B】</li> </ul>
登録年月日	

## 【保護者確認欄】

放課後キッズクラブから、次の①から③について説明を受け、了解しました。

- ①放課後キッズクラブの運営主体が、支援や配慮を要する児童の申立てを行うこと
- ②放課後キッズクラブにおける児童の状況及び児童への支援や配慮の内容
- ③必要に応じて、児童の状況及び児童への支援や配慮の内容について学校と情報を共有すること

年 月 日

保護者氏名(自署)

\_\_\_\_\_



(申請先)  
横浜市 区長

(申請者)  
所在地  
法人名  
代表者職氏名  
(クラブ名)

横浜市放課後キッズクラブ事業費補助金交付申請書〔運営費補助〕

年度横浜市放課後キッズクラブ事業費補助金〔運営費補助〕の交付を受けたいので、次のとおり申請します。  
なお、補助金の交付を受けるにあたっては、横浜市補助金等の交付に関する規則(平成17年11月30日横浜市規則第139号)及び横浜市放課後キッズクラブ事業費補助金交付要綱を遵守します。

1 補助対象期間 年 月 日 ~ 年 月 日

2 申請額 円

【回ごとの金額内訳】

第1回受領予定額	第2回受領予定額	第3回受領予定額	第4回受領予定額

3 算定根拠(要綱別表1~7)

(1) 基本補助

① 基礎部分

	単位1	単位2	単位3	単位4	単位5	単位6
対象児童数※1						
開所日数※2						
補助額						

※1 前年度の4~12月実績平均等により算出

※2 前年度の4~12月実績及び1~3月見込みの合計等により算出

② 子ども教室基礎部分(一律2,148,000円)

③ 子ども教室規模調整部分

支援の単位数	
対象児童数	
補助額	

※ 前年度の4~12月実績平均等により算出

基本補助合計 (①+②+③)

(2) 開所日数加算補助

	単位1	単位2	単位3	単位4	単位5	単位6
補助対象日数 (250日超過分)						
補助額						

※ 前年度の4~12月実績及び1~3月見込みの合計等により算出

開所日数加算補助 合計



(3) 長時間開所加算補助

	単位 2	単位 3	単位 4	単位 5	単位 6
補助対象時間数					
補助額					

長時間開所 加算補助 合計

※ 前年度の4～12月実績及び1～3月見込みの合計等により算出

(4) 子ども教室加算補助

クラブ全体の 平均利用児童数 (A)	
わくわく【区分1】の 平均利用児童数 (B)	
割合 (B/A)	
補助額	

子ども教室 加算補助

※ 前年度の4～6月実績により算出

(5) 障害児受入加算補助

障害児 利用児童数	
--------------	--

障害児受入 加算補助

※前年度の年間実績平均等により算出

(6) 障害児受入推進加算補助 ※利用見込みの該当事由を選択。(本要綱別表4の算定基準①～②)

	単位 1	単位 2	単位 3	単位 4	単位 5	単位 6
事由						
補助額						

障害児受入推進 加算補助 合計

※前年度の障害児の利用実績等に応じて算出

①：すくすく【区分2A・B】登録の補助対象児童の利用登録があった場合

②：条件①に該当しないが、わくわく【区分1】登録の補助対象児童の利用登録があった場合  
(※当該条件に該当し補助対象となる支援の単位数は各月において「1」を超えないものとする)

(7) 障害児受入強化推進加算補助

	単位 1	単位 2	単位 3	単位 4	単位 5	単位 6
補助対象 児童数						
補助額						

障害児受入強化推 進加算補助 合計

※前年度4月のすくすく【区分2A・B】の障害児の登録人数等に応じて算出

(8) 医療的ケア児受入加算補助

	単位 1	単位 2	単位 3	単位 4	単位 5	単位 6
配置						
送迎						
補助額						

医療的ケア児受入 加算補助 合計

※前年度12月の医療的ケア児に対する看護師等の配置の実績等により算出

(9) 育成支援体制強化加算補助 (一律1,444,000円)

育成支援体制強化 加算補助

(10) 放課後児童支援員等キャリアアップ処遇改善費補助

	単位1	単位2	単位3	単位4	単位5	単位6
支援員Ⅰ						
支援員Ⅱ						
支援員Ⅲ						
補助額						

キャリアアップ 加算補助 合計

※前年度のキャリアアップ処遇改善費補助の対象職員数において算出  
 ※支援の単位あたりの上限：919,000円

(11) 賃金改善加算補助

賃金改善 対象者数※	
---------------	--

賃金改善加算補助 合計

※前年度1月執行状況報告の賃金改善対象者数等により算出

(12) 保護者負担減免額相当補助

	補助対象児童数	補助額	
		4～6、9～3月	7～8月
すくすく(ゆうやけ) 【区分2A】			
すくすく(ほしぞら) 【区分2B】			

保護者負担減免 加算補助 合計

※前年度12月の保護者負担減免の対象児童数等に応じて算出

(13) 新型コロナウイルス感染拡大防止加算補助

	単位1	単位2	単位3	単位4	単位5	単位6
対象児童数 (再掲)						
補助額						

新型コロナウイルス 感染拡大防止 加算補助 合計

※前年度の4～12月実績平均等により算出

(14) 活動場所加算補助

活動場所数	
活動場所の状況(※)	

活動場所加算補助

※前年度3月1日時点により記載  
 ※活動場所数が「2」の場合のみ

(15) その他 (別表1注5～注8に該当する場合等)

その他 補助額

4 添付書類

- (1) 運営概況 (第3号様式)
- (2) 活動計画書 (第4号様式)
- (3) 収支予算書 (第5号様式)
- (4) 資金計画表 (第6号様式)
- (5) その他区長が必要と認める書類







# 活動計画書

クラブ名:   放課後キッズクラブ

月	実施内容(プログラム)
4	
5	
6	
7	
8	
9	
10	
11	
12	
1	
2	
3	
評議会開催予定月	開催予定月を記入 半期に1回以上開催してください。 ( <span style="background-color: #d9ead3; border: 1px solid black; padding: 2px 10px;"> </span> . <span style="background-color: #d9ead3; border: 1px solid black; padding: 2px 10px;"> </span> )
保護者会等開催予定月	開催予定月を記入 半期に1回以上開催してください。 ( <span style="background-color: #d9ead3; border: 1px solid black; padding: 2px 10px;"> </span> . <span style="background-color: #d9ead3; border: 1px solid black; padding: 2px 10px;"> </span> )

年度 収支予算書

クラブ名： 放課後キッズクラブ

(収入)

項目	金額(円)	説明
1. 横浜市補助金		
2. 保護者負担金 (1)+(2)+(3)+(4) +(5)		
(1) 利用料		
		わくわく【区分1】
		すくすく(ゆうやけ) 【区分2A】
		すくすく(ほしぞら) 【区分2B】
(2) 保険料		
(3) おやつ代		
(4) 材料費		
(5) その他		
3. その他収入		
総収入額 (1+2+3)		

（支出）

項目	金額（円）	説明
1. 人件費（(1) + (2) + (3) + (4) + (5) + (6) + (7) + (8) + (9) + (10)）		
(1) 主任基本給（賞与含む）		
(2) 副主任基本給（賞与含む）		
(3) 障害児受入推進加算補助経費		
(4) 障害児受入強化推進加算補助経費		
(5) 医療的ケア児受入加算補助経費		
(6) 育成支援体制強化加算補助経費		
(7) キャリアアップ処遇改善費補助経費		
(8) 賃金改善加算補助経費		
(9) 新型コロナウイルス感染症拡大防止加算補助経費		
(10) その他人件費		
2. 事業費（(1) + (2) + (3)）		
(1) 育成支援体制強化加算補助経費		
(2) 新型コロナウイルス感染症拡大防止加算補助経費		
(3) その他事業費		
3. 管理運営費（(1) + (2) + (3) + (4)）		
(1) 医療的ケア児受入加算補助経費		
(2) 育成支援体制強化加算補助経費		
(3) 新型コロナウイルス感染症拡大防止加算補助経費		
(4) その他管理運営費		
4. 児童処遇費（(1) + (2) + (3) + (4)）		
(1) 保険料		
(2) おやつ代		
(3) 材料費		
(4) その他		
5. その他		
総支出額（1 + 2 + 3 + 4 + 5）		





第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

## 横浜市放課後キッズクラブ事業費補助金交付決定通知書〔運営費補助〕

年 月 日付で申請のあった横浜市放課後キッズクラブ事業費補助金〔運営費補助〕を次のとおり交付します。

## 1 交付金額

- 円

※ 金額内訳及び  
交付時期

月（第1回支払額）	円
月（第2回支払額）	円
月（第3回支払額）	円
月（第4回支払額）	円

## 2 交付対象クラブ

## 3 補助対象期間

年 月 日 ～ 年 月 日

## 4 交付条件

- (1) 放課後キッズクラブ事業実施のために使用し、他の用途に流用しないこと。
- (2) 補助金支払いの請求にあたっては、本通知書の写しを添付すること。
- (3) 区長が定める期日までに、横浜市放課後キッズクラブ事業費補助金執行状況報告書（第8号様式）を提出すること。
- (4) 補助事業終了後、区長が定める期日までに、横浜市放課後キッズクラブ事業実績報告書〔運営費補助〕（第19-1号様式）を提出すること。

## 5 留意事項

- (1) 交付金額確定後、実績金額との差引を精算します。
- (2) 補助金事業に係る収支を明らかにした帳簿を備え、当該収支及び支出についての帳票類は事業年度終了後5か年保管してください。
- (3) 余剰金が生じたときは、速やかに返還してください。
- (4) 虚偽その他不正な手続きによって補助金の交付を受けたときは、補助金の全部又は一部の返還を求める場合があります。
- (5) 必要があると認めるときは、経理等の状況について調査をすることがあります。

## 6 備考

第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

横浜市放課後キッズクラブ事業費補助金交付決定通知書〔開設費補助〕

年 月 日付で申請のあった横浜市放課後キッズクラブ事業費補助金〔開設費補助〕を次のとおり交付します。

1 交付金額 \_\_\_\_\_ 円（交付時期： 月）

2 交付対象クラブ \_\_\_\_\_

3 補助対象期間 \_\_\_\_\_ 年 月 日 ～ \_\_\_\_\_ 年 月 日

4 交付条件

- (1) 新規に開設または運営法人が変更になる放課後キッズクラブの初度調弁のために使用し、他の用途に流用しないこと。
- (2) 補助金支払いの請求にあたっては、本通知書の写しを添付すること。
- (3) 補助事業終了後、区長が定める期日までに、横浜市放課後キッズクラブ事業実績報告書〔開設費補助〕（第19-2号様式）を提出すること。

5 留意事項

- (1) 交付金額確定後、実績金額との差引を精算します。
- (2) 補助金事業に係る収支を明らかにした帳簿を備え、当該収支及び支出についての帳票類は事業年度終了後5か年保管してください。
- (3) 余剰金が生じたときは、速やかに返還してください。
- (4) 虚偽その他不正な手続きによって補助金の交付を受けたときは、補助金の全部又は一部の返還を求める場合があります。
- (5) 必要があると認めるときは、経理等の状況について調査をすることがあります。

6 備考

第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

横浜市放課後キッズクラブ事業費補助金交付決定通知書[準備費補助]

年 月 日付で申請のあった横浜市放課後キッズクラブ事業費補助金〔準備費補助〕を次のとおり交付します。

1 交付金額 \_\_\_\_\_ 円 (交付時期: 月)

2 交付対象クラブ \_\_\_\_\_

3 補助対象期間 \_\_\_\_\_ 年 月 日 ~ \_\_\_\_\_ 年 月 日

4 交付条件

- (1) 放課後キッズクラブ事業実施にあたっての常勤職員の研修参加に要する人件費、開設準備に要する人件費に使用するものとし、他の用途に流用しないこと。
- (2) 補助金支払いの請求にあたっては、本通知書の写しを添付すること。
- (3) 補助事業終了後、区長が定める期日までに、横浜市放課後キッズクラブ事業実績報告書[準備費補助](第19-3号様式)を提出すること。

5 留意事項

- (1) 交付金額確定後、実績金額との差引を精算します。
- (2) 補助金事業に係る収支を明らかにした帳簿を備え、当該収支及び支出についての帳票類は事業年度終了後5か年保管してください。
- (3) 余剰金が生じたときは、速やかに返還してください。
- (4) 虚偽その他不正な手続きによって補助金の交付を受けたときは、補助金の全部又は一部の返還を求める場合があります。
- (5) 必要があると認めるときは、経理等の状況について調査をすることがあります。

6 備考

（報告先）  
横浜市 区長

（報告者）  
所在地  
法人名  
代表者職氏名  
（クラブ名） 放課後キッズクラブ

横浜市放課後キッズクラブ事業費補助金執行状況報告書（月提出分）

年度放課後キッズクラブ事業費補助金について、以下のとおり執行状況を報告します。

1 基本補助

(1) 基礎部分

・対象児童数（単位：人）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	平均
単位1													
単位2													
単位3													
単位4													
単位5													
単位6													

※1月から3月は12月実績

・開所日数（単位：日）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	合計	補助額
単位1														
単位2														
単位3														
単位4														
単位5														
単位6														

※1月から3月は実施要綱第6条第1項に基づく開所日全てを開所する日数

(2) 子ども教室基礎部分

補助額
-----

(3) 子ども教室規模調整部分

	4月	5月	6月
支援の単位数			
平均			

	4月	5月	6月
対象児童数(※)			
平均			

※1単位の場合のみ

補助額
-----

(1)～(3)補助額
------------

円

2 開所日数加算補助

・補助対象日数（250日超過分）

	日数	補助額
単位1		
単位2		
単位3		
単位4		
単位5		
単位6		

※1月から3月は実施要綱第6条第1項に基づく開所日全てを開所する日数

補助額
-----

円

3 長時間開所加算補助  
・補助対象時間数

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	平均	補助額
単位2														
単位3														
単位4														
単位5														
単位6														

※1月から3月は12月実績

補助額
円

4 夏季休業期間加算補助

					7月		8月
支援の単位数							
平均							
					増えた単位の 開所日数		
					合計		

※1月以降の執行状況報告時に算出

補助額
円

5 子ども教室加算補助

	4月	5月	6月
クラブ全体の 平均利用児童数 (A)			
わくわく【区分1】の 平均利用児童数 (B)			
割合 (B/A)			
平均			

補助額
円

6 障害児受入加算補助

(単位：人)

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	平均
利用児童数													

※1月から3月は12月実績

補助額
円

7 障害児受入推進加算補助

(単位：円)

支援の単位		追加配置できていた日数 (※)											補助額	
		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月		3月
1	対象月													
	日数													
2	対象月													
	日数													
3	対象月													
	日数													
4	対象月													
	日数													
5	対象月													
	日数													
6	対象月													
	日数													

※1月から3月は12月実績

補助額
円

8 障害児受入強化推進加算補助

(単位：円)

支援の単位		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	補助額	
1	障害児数														
	日数	強化①													
		強化②													
		強化③													
2	障害児数														
	日数	強化①													
		強化②													
		強化③													
3	障害児数														
	日数	強化①													
		強化②													
		強化③													
4	障害児数														
	日数	強化①													
		強化②													
		強化③													
5	障害児数														
	日数	強化①													
		強化②													
		強化③													
6	障害児数														
	日数	強化①													
		強化②													
		強化③													

※1月から3月は12月実績

補助額
円

9 医療的ケア児受入加算補助（単位：円）

支援の単位	医療的ケア児の利用実績（看護師等を配置していた月のみ○を選択）												補助額	
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月		
配置														
送迎														
配置														
送迎														
配置														
送迎														

補助額
円

10 育成支援体制強化加算補助（単位：円）

補助額
円

11 放課後児童支援員等キャリアアップ処遇改善費補助（単位：円）

	単位1	単位2	単位3	単位4	単位5	単位6
補助額						

補助額
円

12 賃金改善加算補助（単位：円）

補助額
円

13 保護者負担減免額相当補助

（単位：人）

利用区分	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	合計
すくすく （ゆうやけ） 【区分2A】													
すくすく （ほしぞら） 【区分2B】													

※1月から3月は12月実績

補助額
円

14 人材育成加算補助（単位：人）

	常勤職員	非常勤職員
対象職員数		

補助額
円

15 常勤職員の産前・産後休暇に伴う代替職員配置経費補助（単位：円）

補助額	
-----	--

補助額
円

16 新型コロナウイルス感染拡大防止加算補助（単位：人）

	対象児童数（再掲）
単位1	
単位2	
単位3	
単位4	
単位5	
単位6	

※1月から3月は12月実績

補助額
円

17 活動場所加算補助

	6月	9月	12月
活動場所数			
活動場所の状況（※）			

※活動場所数が「2」の場合のみ

算定基準
------

補助額
円

18 その他（別表1注5～注8に該当する場合等）

補助額
円

合計額（A）	円
交付決定済額（B）	円
差額（A - B）	円

19 添付書類（該当がある場合のみ）

- (1) すくすく【区分2】登録者名簿（実施要綱第3号様式）
- (2) すくすく【区分2】登録児童の利用申込書の写し
- (3) 障害児等受入に係る加算補助対象児童名簿（第9号様式）
- (4) 補助対象児童であることがわかる書類（支援や配慮を要する児童の申立書（第1号様式）及び児童状況書（第1の2号様式）の写し等）
- (5) 月別開所状況及び職員配置状況を証する書類
- (6) 障害児の受入に係る研修の受講状況を証する書類
- (7) 放課後児童支援員等キャリアアップ処遇改善費補助 対象者一覧（第10号様式）
- (8) 放課後児童支援員等キャリアアップ処遇改善費補助 要件確認表（第11号様式）
- (9) 放課後児童支援員であることを証する書類（研修受講修了証等）
- (10) 職歴を証する書類（勤務実績証明書等）
- (11) 本市が指定する研修を受講したことを証する書類
- (12) キャリアアップ体系を設けていることを証する書類（就業規則等）
- (13) 賃金が改善されたことを証する書類（前年度の就業規則等）
- (14) 賃金改善加算補助実施計画書（第12号様式）
- (15) 賃金改善加算補助改善額見込額等内訳書（第13号様式）
- (16) 賃金改善を行っていることを証する書類（改正前及び改正後の就業規則等）
- (17) 保護者負担減免額相当補助対象児童名簿（第14号様式）
- (18) 保護者負担減免額相当補助の対象世帯であることを証する書類（市民税・県民税課税（非課税）証明書の写し等）
- (19) 実施要綱第9条第4項に基づく研修計画
- (20) 人材育成加算補助実施報告書（第15号様式）
- (21) 常勤職員の産前・産後休暇に伴う代替職員配置経費補助確認書（第16号様式）
- (22) 常勤職員の出産予定日がわかる書類（母子健康手帳の写し、診断書の写し等）
- (23) その他（ ）

※行が足りない場合は適宜追加すること。

障害児等受入に係る加算補助対象児童名簿（ 月提出分）

クラブ名： \_\_\_\_\_

1. 補助対象児童利用登録状況

No.	学年	児童氏名	事由	利用登録状況（上段：利用区分、下段：支援の単位）														
				4月	5月	6月	7月	8月	9月	10月	11月	12月						
1																		
2																		
3																		
4																		
5																		
6																		
7																		
8																		
9																		
10																		

※「事由」欄は以下に基づいて記入すること。

- ① 個別支援学級または特別支援学校等在籍児童
- ② 身体障害者手帳、療育手帳（愛の手帳）または精神障害者手帳が提出されている児童
- ③ 支援や配慮を要する児童の申立書（第1号様式）及び児童状況書（第1の2号様式）が提出されている児童
- ④ 別表6に定める医療的ケア児受入加算補助の補助対象であって、看護師等の措置を受けている児童

2. 利用区分別利用登録状況

利用区分別利用登録状況	利用登録状況												
	4月	5月	6月	7月	8月	9月	10月	11月	12月				
わくわく【区分1】	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
すくすく【区分2】	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
支援の単位①	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
支援の単位②	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
支援の単位③	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
支援の単位④	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
支援の単位⑤	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )
支援の単位⑥	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )	( )

※ 上記利用区分別登録状況の ( ) 内の数字は医療的ケア児（事由④）の人数を含まない数字

3. 添付書類（当該年度に既に提出されている書類については区長の判断により添付を省略できることとする）

(1) 利用申込書

(2) 以下の書類（「1. 補助対象児童利用登録状況」の「事由」が①の場合を除き、各事由に応じて添付すること）

- 「身体障害者手帳、療育手帳（愛の手帳）または精神障害者手帳」の写し（事由②の場合）
- 「支援や配慮を要する児童の申立書」（第1号様式）及び「児童状況書」（第1の2号様式）（事由③の場合）
- 別表6に定める以下の書類すべて（事由④の場合）
  - 医療的ケア実施可否結果通知書の写し
  - 医療的ケアに関する主治医指示書の写し
  - 医療的ケアに関する申込書兼同意書の写し
  - 医療的ケア実施計画書

※ 行が足りない場合は適宜追加すること。



放課後児童支援員等キャリアアップ処遇改善費補助 対象者一覧（ 月提出分）

該当するものに○

新規 ・ 継続

クラブ名： \_\_\_\_\_

支援の単位： \_\_\_\_\_

（単位：円）

No.	職員名	事由（※）											上段：補助金算定基準額【A】 下段：補助対象経費上限額【B】			
		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月			
1																
2																
3																
4																
5																
6																
7																
8																
9																
10																
合計																

※行が足りない場合は適宜追加すること。

補助額（補助金算定基準額合計と補助上限額を比較して少ない方の額） \_\_\_\_\_ 円

※「事由」欄は以下に基づいて記入すること。

- ① 支援員Ⅰ 放課後児童支援員
- ② 支援員Ⅱ 経験年数が概ね5年以上の放課後児童支援員で、キャリアアップ研修を受講した者
- ③ 支援員Ⅲ 経験年数が概ね10年以上の放課後児童支援員で、キャリアアップ研修を受講した事業所長的立場にある者
- ④ 補助員Ⅰ 補助員
- ⑤ 補助員Ⅱ 経験年数が概ね5年以上の補助員で、キャリアアップ研修を受講した者

<添付資料>

要件に応じて次の書類を添付すること。

- 1 放課後児童支援員等キャリアアップ処遇改善費補助 要件確認表（第11号様式） ※必須
- 2 ①支援員Ⅰ、②支援員Ⅱ及び③支援員Ⅲ）放課後児童支援員であることを証する書類（研修受講修了証等）※当該職員が初めて補助対象となる場合のみ
- 3 ②支援員Ⅱ、③支援員Ⅲ及び⑤補助員Ⅱ）職歴を証する書類（勤務実績証明書等） ※当該職員が当該事由で初めて補助対象となる場合のみ
- 4 ②支援員Ⅱ、③支援員Ⅲ及び⑤補助員Ⅱ）本市が指定する研修を受講したことを証する書類 ※1月執行状況報告時に添付
- 5 キャリアアップ体系を設けていることを証する書類 ※必須
- 6 前年度の賃金を証する書類 ※事業所として、初めて放課後児童支援員等キャリアアップ処遇改善費補助を申請する場合のみ

放課後児童支援員等キャリアアップ処遇改善費補助 要件確認表

該当するものに○

新規 ・ 継続

クラブ名：

支援の単位：

申請日： 年 月 日

No.	職員名	該当要件	新規・変更 (※1)	キャリアアップ研修 要受講者	経験年月（ 年4月1日現在）						給与（※2）		賃金改善項目				
					現在の事業所		過去に勤務していた事業所		合計		前年度給与		今年度給与		基本給	手当	賞与
1					年	か月	年	か月	年	か月							
2					年	か月	年	か月	年	か月							
3					年	か月	年	か月	年	か月							
4					年	か月	年	か月	年	か月							
5					年	か月	年	か月	年	か月							
6					年	か月	年	か月	年	か月							
7					年	か月	年	か月	年	か月							
8					年	か月	年	か月	年	か月							
9					年	か月	年	か月	年	か月							
10					年	か月	年	か月	年	か月							

- ※1 新たに支援員Ⅱ、支援員Ⅲ、補助員Ⅱ（要件の変更を含む）になった職員は「○」を記入し、職歴を証する書類を添付すること
- ※2 給与欄は新たにキャリアアップ処遇改善費補助を申請するクラブのみ記入
- ※3 行が足りない場合は適宜追加すること。

## 賃金改善加算補助 実施計画書

クラブ名：

### 1. 補助額

① 事業実施期間	令和 <input style="background-color: #d9ead3;" type="text"/> 年 <input style="background-color: #d9ead3;" type="text"/> 月 ~ 令和 <input style="background-color: #d9ead3;" type="text"/> 年 <input style="background-color: #d9ead3;" type="text"/> 月
② 補助基準額	<input style="background-color: #d9ead3;" type="text"/> 円

### 2. 賃金改善見込額

③ 賃金改善見込額	<input style="background-color: #d9ead3;" type="text"/> 円
④ うち、基本給又は決まって毎月支払う手当による賃金改善見込額	<input style="background-color: #d9ead3;" type="text"/> 円
⑤ 賃金改善に伴い増加する法定福利費等の事業主負担分	<input style="background-color: #d9ead3;" type="text"/> 円
⑥ 賃金改善見込額合計(③+⑤)	<input style="background-color: #d9ead3;" type="text"/> 円

### 3. 要件の確認

※合致しない要件がある場合は、補助対象外です。

賃金改善額の2/3以上が基本給又は決まって毎月支払う手当によって改善されていること (③×2/3≦④)	<input style="background-color: #d9ead3;" type="text"/>
賃金改善額合計 (⑥) が補助基準額 (②) 以上となっていること	<input style="background-color: #d9ead3;" type="text"/>
本加算補助による賃金改善に係る計画の具体的内容を職員に周知していること	<input style="background-color: #d9ead3;" type="text"/>
本加算補助の実施により講じた賃金改善の水準を維持すること	<input style="background-color: #d9ead3;" type="text"/>

上記の内容について、全ての職員に対し周知をした上で、提出していることを証明いたします。

年  月  日

運営主体名：   
 代表者職氏名：

## 賃金改善加算補助 賃金改善見込額等内訳書

クラブ名：

就業規則等で定めた常勤職員の1か月あたりの勤務時間数	120.0 時間
----------------------------	----------

NO.	職員名	職種	常勤・非常勤の別	新規・変更 (※1)	補助単価 (月額)	常勤職員数	非常勤職員数(常勤換算)		賃金改善実施月数	補助基準額	令和 年 月～令和 年 月分			賃金改善に伴う法定福利費等の事業主負担分の増分	1か月あたりの平均賃金改善見込額	備考
							1か月あたりの勤務時間数	常勤換算値			賃金改善見込額					
											基本額又は決まって毎月支払う手当	その他				
1				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
2				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
3				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
4				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
5				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
6				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
7				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
8				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
9				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
10				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
11				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
12				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
13				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
14				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
15				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
16				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
17				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
18				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
19				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
20				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
21				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
22				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
23				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
24				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
25				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
26				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
27				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
28				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
29				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
30				<input type="checkbox"/>	11,000円			0.0人		0円			0円			
合計						0.0人		0.0人	0か月	0円	0円	0円	0円			

※1 新たに賃金改善を行う者（賃金改善額の変更を含む）は  または  を記入し、賃金改善を行っていることを証する書類を添付すること。  
 ※2 クラブで勤務する職員のうち、賃金改善を行う者（職種問わず、非常勤を含み、経営に携わる法人の役員を除く。）を記載すること。  
 ※3 行が足りない場合は適宜追加すること。

保護者負担減免額相当補助対象児童名簿（ 月提出分）

クラブ名：

1. 利用料減免状況

No.	学年	児童氏名	利用料減免状況（上段：利用区分、下段：事由※）									
			4月	5月	6月	7月	8月	9月	10月	11月	12月	
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
合計	すくすく（ゆうやけ）【区分2A】											
	すくすく（ほしぞら）【区分2B】											

※利用料減免状況の下段の欄は、以下の減免事由から選択し、記入すること。

- ① 「横浜市の就学援助を受けている世帯」に該当
- ② 「市民税所得割非課税世帯」に該当
- ③ 「生活保護世帯」に該当

※行が足りない場合は適宜追加すること。

2. 添付書類（当該年度に既に提出されている書類については区長の判断により添付を省略できることとする）

(1) 利用申込書

(2) 以下のいずれかの書類

- 「就学援助申請の審査結果及び支給についてのお知らせ、私立学校等就学奨励費の審査結果及び支給についてのお知らせ、私立学校等就学奨励費の認定審査結果のお知らせ、または就学援助認定通知」の写し（減免事由①の場合）
- 「市民税・県民税課税（非課税）証明書、給与所得等に係る市民税・県民税特別徴収税額通知書または市民税・県民税税額決定・納税通知書」の写し（減免事由②の場合） ※ 4～5月は前年度分、6～12月は当該年度分の証明書等を添付すること。
- 「保護証明書または生活保護費支給証」の写し（減免事由③の場合）

## 人材育成加算補助実施報告書

クラブ名：

1 運営主体主催の研修の実施日及び内容

	研修名	研修内容	研修時間	研修実施日
1				
2				
3				
4				
5				

2 人材育成加算補助の補助対象となる研修の受講者名簿

	氏名	常勤職員・非常勤職員の別
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		

	合計
常勤職員	0
非常勤職員	0

※行が足りない場合は適宜追加すること。

## 常勤職員の産前・産後休暇に伴う代替職員配置経費補助確認書

クラブ名： \_\_\_\_\_

### 1 産前・産後休暇取得職員

(1) 氏名	
(2) 職位	
(3) 出産予定日	年 月 日
(4) 休暇付与予定期間	年 月 日 ～ 年 月 日
(5) 多胎妊娠の有無 (多胎妊娠の場合は○を選択)	

### 2 補助額

\_\_\_\_\_ 円

### 3 添付書類

母子健康手帳の写し 又は 診断書の写し

### 4 留意事項

- (1) 主任又は副主任が産前・産後休暇を取得する期間について、運営主体が当該職員に第3条第3項に定める職員最低給与基準以上の給与を支払っていない場合は、当該補助金を取消し、返還を求めることがあります。
- (2) 産前・産後休暇が次年度に渡る場合は、日割りで補助額を積算します。

(申請先)

横浜市 区長

(申請者)

所在地

法人名

代表者職氏名

(クラブ名)

横浜市放課後キッズクラブ事業費補助金変更交付申請書

年 月 日に交付決定を受けた横浜市放課後キッズクラブ事業費補助金について、交付金額の変更を申請します。

1 補助対象期間 年 月 日 ~ 年 月 日

2 補助金変更交付申請額 円

(1) 交付決定済額 円

(2) 差引 (追加交付金額) 円

3 変更申請額内訳

項目	交付決定済額	変更交付申請額	差引 (追加交付金額)
基本事業費			
基本補助			
基礎部分			0円
子ども教室基礎部分			0円
子ども教室規模調整部分			0円
開所日数加算補助			0円
長時間開所加算補助			0円
夏季休業期間加算補助			0円
子ども教室加算補助			0円
特別加算			
障害児受入加算補助			0円
障害児受入推進加算補助			0円
障害児受入強化推進加算補助			0円
医療的ケア児受入加算補助			0円
育成支援体制強化加算補助			0円
放課後児童支援員等キャリアアップ処遇改善費補助			0円
賃金改善加算補助			0円
保護者負担減免額相当補助			0円
人材育成加算補助			0円
産前・産後休暇に伴う代替職員配置経費補助			0円
新型コロナウイルス感染拡大防止加算補助			0円
活動場所加算補助			0円
その他			0円
合 計			



第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

横浜市放課後キッズクラブ事業費補助金変更交付決定通知書

年度放課後キッズクラブ事業費補助金について、次のとおり変更して交付します。

1 変更交付決定額 \_\_\_\_\_ 円

(1) 交付決定済額 \_\_\_\_\_ 円

(2) 追加交付額 \_\_\_\_\_ - 円

※ 金額内訳及び  
交付時期 {

月 (第1回支払額)	_____ 円
月 (第2回支払額)	_____ 円
月 (第3回支払額)	_____ 円
月 (第4回支払額)	_____ 円
月 (その他)	_____ 円

2 交付対象クラブ \_\_\_\_\_

3 補助対象期間 \_\_\_\_\_ 年 月 日 ~ \_\_\_\_\_ 年 月 日

4 交付条件

- (1) 放課後キッズクラブ事業実施のために使用し、他の用途に流用しないこと。
- (2) 補助金支払いの請求にあたっては、本通知書の写しを添付すること。
- (3) 補助事業終了後、区長が定める期間までに横浜市放課後キッズクラブ事業実績報告書[運営費補助]（第19-1号様式）を提出すること。

5 留意事項

- (1) 交付金額確定後、実績金額との差引を精算します。
- (2) 補助金事業に係る収支を明らかにした帳簿を備え、当該収支及び支出についての帳票類は事業年度終了後5か年保管してください。
- (3) 余剰金が生じたときは、速やかに返還してください。
- (4) 虚偽その他不正な手続によって補助金の交付を受けたときは、補助金の全部又は一部を取り消し、返還を求める場合があります。
- (5) 必要があると認めるときは、経理等の状況について調査をすることがあります。

6 備考

(報告先)  
横浜市 区長

年 月 日

(報告者)  
所在地  
法人名  
代表者職氏名  
(クラブ名)

放課後キッズクラブ

年度 横浜市放課後キッズクラブ事業実績報告書[運営費補助]

年度横浜市放課後キッズクラブ事業[運営費補助]の実績について、次のとおり報告します。

1 収支報告

(うち補助金額)

- 1 総収入額 \_\_\_\_\_ 円 ( \_\_\_\_\_ ) 円
- 2 総支出額 \_\_\_\_\_ 円 ( \_\_\_\_\_ ) 円
- 3 差引残額 \_\_\_\_\_ 円 ( \_\_\_\_\_ ) 円

2 戻入額

項目	戻入額
収支報告の差引による戻入額(うち補助金)	
基本事業費の戻入額	
基本補助(基礎部分)	
開所日数加算補助	
長時間開所加算補助	
特別加算の戻入額	
障害児受入推進加算補助	
障害児受入強化推進加算補助	
医療的ケア児受入加算補助	
育成支援体制強化加算補助	
放課後児童支援員等 キャリアアップ処遇改善費補助	
賃金改善加算補助	
新型コロナウイルス感染拡大防止加算補助	
執行状況報告による戻入	
合計	

3 補助金確定額 \_\_\_\_\_ 円

4 添付書類(該当がある場合のみ)

- (1) 基本事業費報告書(第20号様式)
- (2) すくすく【区分2】登録者名簿(実施要綱第3号様式)
- (3) 職員別、補助項目別の当該年度の給与額が分かる書類
- (4) 領収書の写し(1件あたりの支払額が10万円以上の場合)
- (5) 見積書の写し(1件あたりの支払額が100万円以上と見込まれる場合に徴収した2社以上の見積書の写し)
- (6) 障害児受入に係る補助対象経費等報告書(第21号様式)
- (7) 医療的ケア児受入加算補助対象経費等報告書(第22号様式)
- (8) 育成支援体制強化加算補助対象経費等報告書(第23号様式)
- (9) 放課後児童支援員等キャリアアップ処遇改善費補助 対象経費積算書(第24号様式)
- (10) 賃金改善加算補助実施報告書(第25号様式)
- (11) 賃金改善加算補助賃金改善額内訳書(第26号様式)
- (12) 新型コロナウイルス感染拡大防止加算補助対象経費等報告書(第27号様式)
- (13) 積立金額が分かる通帳等の写し(積立金がある場合)
- (14) その他区長が必要と認める書類

【総収入額内訳】

項目	金額	説明
1. 横浜市補助金		第1回      年 月 日    ¥            - 第2回      年 月 日    ¥            - 第3回      年 月 日    ¥            - 第4回      年 月 日    ¥            - その他     年 月 日    ¥            - その他     年 月 日    ¥            -
2. 保護者負担金 ((1) + (2) + (3) + (4) + (5))		
(1) 利用料		
(2) 保険料		
(3) おやつ代		
(4) 材料費		
(5) その他		
3. その他収入		
総収入額 (1 + 2 + 3)		

【総支出額内訳】

項目	横浜市補助金		保護者負担金	その他収入	合計	説明
	補助金	戻入金				
1. 人件費（(1)+(2)+(3)+(4)+(5)+(6)+(7)+(8)+(9)+(10)）						
(1) 常勤職員						
(2) 非常勤職員						
(3) 障害児受入推進加算補助経費						
(4) 障害児受入強化推進加算補助経費						
(5) 医療的ケア児受入加算補助経費						
(6) 育成支援体制強化加算補助経費						
(7) キャリアアップ処遇改善費補助経費						
(8) 賃金改善加算補助経費						
(9) 新型コロナウイルス感染拡大防止加算補助経費						
(10) その他						
2. 事業費（(1)+(2)+(3)）						
(1) 育成支援体制強化加算補助経費						
(2) 新型コロナウイルス感染拡大防止加算補助経費						
(3) その他						
3. 管理運営費（(1)+(2)+(3)+(4)）						
(1) 医療的ケア児受入加算補助経費						
(2) 育成支援体制強化加算補助経費						
(3) 新型コロナウイルス感染拡大防止加算補助経費						
(4) その他						
4. 児童処遇費（(1)+(2)+(3)+(4)）						
(1) 保険料						
(2) おやつ代						
(3) 材料費						
(4) その他						
5. 執行状況報告による戻入						
6. その他						
総支出額（1+2+3+4+5+6）						

(報告先)

横浜市

区長

(報告者)

所在地

法人名

代表者職氏名

(クラブ名)

放課後キッズクラブ

年度 横浜市放課後キッズクラブ事業実績報告書[開設費補助]

年度横浜市放課後キッズクラブ事業〔開設費補助〕の実績について、次のとおり報告します。

1 収支報告

(うち補助金額)

- 1 総収入額 \_\_\_\_\_ 円 ( \_\_\_\_\_ ) 円
- 2 総支出額 \_\_\_\_\_ 円 ( \_\_\_\_\_ ) 円
- 3 差引残額 \_\_\_\_\_ 円 ( \_\_\_\_\_ ) 円

【総収入額内訳】

(単位：円)

項目	金額	説明
横浜市補助金		( 年 月 日 ) ¥
その他収入		
合計		

【総支出額内訳】

(単位：円)

項目	横浜市補助金	その他収入	合計	説明
支出額				

2 対象経費一覧

件名	金額	備考
合計		

(報告先)

横浜市

区長

(報告者)

所在地

法人名

代表者職氏名

(クラブ名)

放課後キッズクラブ

年度 横浜市放課後キッズクラブ事業実績報告書〔準備費補助〕

年度横浜市放課後キッズクラブ事業〔準備費補助〕の実績について、次のとおり報告します。

1 収支報告

(うち補助金額)

- 1 総収入額 \_\_\_\_\_ 円 ( \_\_\_\_\_ ) 円
- 2 総支出額 \_\_\_\_\_ 円 ( \_\_\_\_\_ ) 円
- 3 差引残額 \_\_\_\_\_ 円 ( \_\_\_\_\_ ) 円

【総収入額内訳】

(単位：円)

項目	金額	説明
横浜市補助金		( 年 月 日 ) ¥
その他収入		
合計		

【総支出額内訳】

(単位：円)

項目	横浜市補助金	その他収入	合計	説明
支出額				

2 対象経費一覧

件名	金額	備考
合計		

基本事業費報告書

クラブ名：

1 開所状況の報告

(1) 基本補助（基礎部分）

・対象児童数（単位：人）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	平均
単位1													
単位2													
単位3													
単位4													
単位5													
単位6													

・開所日数（単位：日）

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	合計	補助額
単位1														
単位2														
単位3														
単位4														
単位5														
単位6														

(2) 開所日数加算補助

・補助対象日数（250日超過分）

	日数	補助額
単位1		
単位2		
単位3		
単位4		
単位5		
単位6		

(3) 長時間加算補助対象時間数

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	平均	補助額
単位2														
単位3														
単位4														
単位5														
単位6														

2 補助額の算定

項目	執行状況報告（1月）によって算定された補助額	実績報告によって算定された補助額	戻入額
基本補助（基礎部分）			
開所日数加算補助			
長時間開所加算補助			

※行が足りない場合は、適宜追加すること。

## 障害児受入に係る補助対象経費等報告書

クラブ名：

### 1 障害児受入推進加算補助

#### (1) 補助対象者等

No.	氏名	属する 支援の単位	補助対象経費(円)
1			
2			
3			
4			
5			
6			
7			
8			

#### (2) 補助対象経費合計

(単位：円)

支援の単位	1	2	3	4	5	6	合計
対象経費							
補助上限額							
補助額※1							
戻入額※2							

※1 補助額は支援の単位ごとの対象経費と補助上限額を比較して低い金額

※2 対象経費が補助上限額を下回る場合、その差額

### 2 障害児受入強化推進加算補助

#### (1) 補助対象者等

No.	氏名	属する 支援の単位	補助対象経費(円)
1			
2			
3			
4			
5			
6			
7			
8			

#### (2) 補助対象経費合計

(単位：円)

支援の単位	1	2	3	4	5	6	合計
対象経費							
補助上限額							
強化①							
強化②							
強化③							
補助額※1							
戻入額※2							

※1 補助額は支援の単位ごとの対象経費と補助上限額を比較して低い金額

※2 対象経費が補助上限額を下回る場合、その差額

※行が足りない場合は適宜追加すること。



医療的ケア児受入加算補助対象経費等報告書

クラブ名：

1 対象経費一覧

	月	支出科目	摘要	補助対象経費(円)
配置	4			
	5			
	6			
	7			
	8			
	9			
	10			
	11			
	12			
	1			
	2			
	3			
合 計				0 円
送迎	4			
	5			
	6			
	7			
	8			
	9			
	10			
	11			
	12			
	1			
	2			
	3			
合 計				0 円

2 補助額

<u>配置</u>	(1) 補助対象経費	0 円
	うち、人件費	0 円
	うち、管理運営費	0 円
	(2) 補助上限額	0 円
	(3) 補助額（(1)と(2)を比較して低い額）	0 円
	(4) 戻入額（(1) < (2)の場合、その差額）	0 円
<u>送迎</u>	(1) 補助対象経費	0 円
	うち、人件費	0 円
	うち、管理運営費	0 円
	(2) 補助上限額	0 円
	(3) 補助額（(1)と(2)を比較して低い額）	0 円
	(4) 戻入額（(1) < (2)の場合、その差額）	0 円

## 育成支援体制強化加算補助対象経費等報告書

クラブ名：

本報告書に記載している対象経費には、他の助成を受けているものは含まれていません。

### 1 対象経費一覧

No.	支出科目	摘要	補助対象経費(円)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
合 計			

※行が足りない場合は適宜追加すること。

### 2 補助額

(1) 補助対象経費

うち、人件費

うち、事業費

うち、管理運営費

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

(2) 補助上限額

(3) 補助額（(1)と(2)を比較して低い額）

\_\_\_\_\_

(4) 戻入額（(1) < (2)の場合、その差額）

\_\_\_\_\_

放課後児童支援員等キャリアアップ処遇改善費補助 対象経費積算書

クラブ名:  支援の単位:

(単位:円)

No.	職員名	事由(※)												補助対象経費 上限額【A】	賃金改善額等 (実績)【B】	(内 訳)		補助対象経費(実績) 【C】 〔AとBを比較して 少ない方の額〕	
		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月			賃金改善額	その他 対象経費		
1																			
2																			
3																			
4																			
5																			
6																			
7																			
8																			
9																			
10																			
合計																			

※行が足りない場合は適宜追加すること。

- 1 執行状況報告(1月分)によって算定された補助額  円
- 2 補助対象経費(各職員の補助対象経費(実績)【C】の合計額) \_\_\_\_\_ 円
- 3 補助額(1、2を比較して低い額) \_\_\_\_\_ 円
- 4 戻入額(1>2の場合、その差額) \_\_\_\_\_ 円

※ 「事由」欄は以下に基づいて記入すること。

- ① 支援員Ⅰ 放課後児童支援員
- ② 支援員Ⅱ 経験年数が概ね5年以上の放課後児童支援員で、キャリアアップ研修を受講した者
- ③ 支援員Ⅲ 経験年数が概ね10年以上の放課後児童支援員で、キャリアアップ研修を受講した事業所長的立場にある者
- ④ 補助員Ⅰ 補助員
- ⑤ 補助員Ⅱ 経験年数が概ね5年以上の補助員で、キャリアアップ研修を受講した者

## 賃金改善加算補助 実施報告書

クラブ名： 

## 1. 補助額

① 事業実施期間	令和 <input type="text"/> 年 <input type="text"/> 月 ~ 令和 <input type="text"/> 年 <input type="text"/> 月
② 補助基準額	<input type="text"/> 円

## 2. 賃金改善額

③ 賃金改善額	<input type="text"/> 円
④ うち、基本給又は決まって毎月支払う手当による賃金改善額	<input type="text"/> 円
⑤ 賃金改善に伴い増加する法定福利費等の事業主負担分	<input type="text"/> 円
⑥ 賃金改善額合計(③+⑤)	<input type="text"/> 円

## 3. 要件の確認

※合致しない要件がある場合は、補助対象外です。

賃金改善額の2/3以上が基本給又は決まって毎月支払う手当によって改善されていること (③×2/3≤④)	<input type="text"/>
賃金改善額合計 (⑥) が補助基準額 (②) 以上となっていること	<input type="text"/>
本加算補助による賃金改善に係る計画の具体的内容を職員に周知していること	<input type="text"/>
本加算補助の実施により講じた賃金改善の水準を維持すること	<input type="text"/>

上記の内容について、全ての職員に対し周知をした上で、提出していることを証明いたします。

 年  月  日運営主体名：  
代表者職氏名：

## 賃金改善加算補助 賃金改善額内訳書

クラブ名：

NO.	職員名	常勤・ 非常勤の別	令和 年 月 ～ 令和 年 月分			
			賃金改善 実施月数	賃金改善額		
					基本給又は 決まって毎月 支払う手当	その他
1				円	円	円
2				円	円	円
3				円	円	円
4				円	円	円
5				円	円	円
6				円	円	円
7				円	円	円
8				円	円	円
9				円	円	円
10				円	円	円
11				円	円	円
12				円	円	円
13				円	円	円
14				円	円	円
15				円	円	円
16				円	円	円
17				円	円	円
18				円	円	円
19				円	円	円
20				円	円	円
21				円	円	円
22				円	円	円
23				円	円	円
24				円	円	円
25				円	円	円
26				円	円	円
27				円	円	円
28				円	円	円
29				円	円	円
30				円	円	円
計				円	円	円

※クラブで勤務する職員のうち、賃金改善を行う者（職種問わず、非常勤を含み、経営に携わる法人の役員を除く。）を記載すること。

※行が足りない場合は適宜追加すること。

## 新型コロナウイルス感染拡大防止加算補助対象経費等報告書

クラブ名：

本報告書に記載している対象経費には、他の助成を受けているものは含まれていません。

### 1 対象経費一覧

No.	支出科目	摘要	補助対象経費(円)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
合 計			

※行が足りない場合は適宜追加すること。

### 2 補助額

(1) 補助対象経費

うち、人件費

うち、事業費

うち、管理運営費

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

(2) 補助上限額

(3) 補助額（(1)と(2)を比較して低い額）

\_\_\_\_\_

(4) 戻入額（(1) < (2)の場合、その差額）

\_\_\_\_\_

第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

横浜市放課後キッズクラブ事業費補助金交付額確定通知書〔運営費補助〕

年 月 日付で交付決定した 年度横浜市放課後キッズクラブ事業  
費補助金〔運営費補助〕について、年 月 日付実績報告書等に基づき、次  
のとおり確定したので通知します。

1 対象クラブ

\_\_\_\_\_

2 確定額

円

\_\_\_\_\_

第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

横浜市放課後キッズクラブ事業費補助金交付額確定通知書〔開設費補助〕

年 月 日付で交付決定した 年度横浜市放課後キッズクラブ事業  
費補助金〔開設費補助〕について、年 月 日付実績報告書等に基づき、次  
のとおり確定したので通知します。

1 対象クラブ

\_\_\_\_\_

2 確定額

円

\_\_\_\_\_



第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

横浜市放課後キッズクラブ事業費補助金交付額確定通知書〔準備費補助〕

年 月 日付で交付決定した 年度横浜市放課後キッズクラブ事業  
費補助金〔準備費補助〕について、年 月 日付実績報告書等に基づき、次  
のとおり確定したので通知します。

1 対象クラブ

\_\_\_\_\_

2 確定額

円

\_\_\_\_\_

第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

横浜市放課後キッズクラブ事業費補助金交付決定取消通知書[運営費補助]

年 月 日付で交付決定した横浜市放課後キッズクラブ事業費補助金[運営費補助]について、次のとおり取消しましたので通知します。

1 交付対象クラブ

---

2 取消額

---

3 取消理由

---

第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

横浜市放課後キッズクラブ事業費補助金交付決定取消通知書〔開設費補助〕

年 月 日付で交付決定した横浜市放課後キッズクラブ事業費補助金〔開設費補助〕について、次のとおり取消しましたので通知します。

1 交付対象クラブ

---

2 取消額

---

3 取消理由

---

第 号  
年 月 日

(名称)

(代表者名)

様

横浜市 区長

横浜市放課後キッズクラブ事業費補助金交付決定取消通知書〔準備費補助〕

年 月 日付で交付決定した横浜市放課後キッズクラブ事業費補助金〔準備費補助〕について、次のとおり取消しましたので通知します。

1 交付対象クラブ

---

2 取消額

---

3 取消理由

---

年 月 日

横浜市  区長

(申請者)

所在地

法人名

代表者職氏名

(クラブ名)

放課後キッズクラブ

### 消費税及び地方消費税に係る仕入控除税額報告書

年度横浜市放課後キッズクラブ事業に関する補助金における消費税及び地方消費税に係る仕入控除税額について、次のとおり報告します。

1 消費税及び地方消費税に係る確定申告の有無（該当するものに○）

（ 有 ・ 無 ）

2 補助額及び消費税仕入控除税額（1で「有」とした場合のみ記載）

補助金名称	補助金交付額確定通知書		補助金の確定額（円）	消費税及び地方消費税の申告に係る仕入控除税額（円）
	日付	文書番号		

※該当がある場合のみ記載

※行が足りない場合は適宜追加すること。

3 添付書類（1で「無」と記入した場合は添付不要）

- (1) 仕入控除税額の積算の内訳を証する書類
- (2) 課税期間分の消費税及び地方消費税の確定申告書（写し）
- (3) 課税売上割合、控除対象仕入税額等の計算表（写し）
- (4) 特定収入割合の計算表（該当がある場合のみ）（写し）

## 横浜市放課後児童クラブ事業実施要綱

制 定 平成22年3月8日 こ放第 891 号（局長決裁）  
全部改正 令和4年2月25日 こ放第 2124 号（局長決裁）

横浜市放課後児童クラブ事業実施要綱を次のとおり定める。

横浜市放課後児童クラブ事業実施要綱

横浜市放課後児童クラブ事業実施要綱（平成22年3月8日制定）の全部を改正する。

### （目的）

- 第1条 この要綱は、地域の理解と協力のもとに実施する横浜市放課後児童クラブ事業（以下、「事業」という。）の実施について、必要な事項を定める。
- 2 この事業は、児童福祉法（昭和22年法律第164号。以下「法」という。）第6条の3第2項に規定される放課後児童健全育成事業（以下、「放課後児童健全育成事業」という。）として、児童に適切な遊び及び生活の場を与え、その健全な育成を図ることを目的とする。
- 3 事業の実施にあたっては、法、横浜市放課後児童健全育成事業の設備及び運営の基準に関する条例（平成26年9月横浜市条例第49号。以下「条例」という。）及び横浜市放課後児童健全育成事業の届出等に関する要綱（平成27年2月26日こ放第930号。以下「届出要綱」という。）のほか、この要綱の定めるところによる。
- 4 事業の実施に伴う補助金の交付については、横浜市補助金等の交付に関する規則（平成17年11月横浜市規則第139号）及び横浜市放課後児童クラブ事業費補助金交付要綱（平成18年3月2日福子放第10191号。以下「補助金交付要綱」という。）に定める。

### （用語の定義）

- 第2条 この要綱において「放課後児童クラブ（以下「クラブ」という。）」とは、事業の運営主体（以下「運営主体」という。）が条例及びこの要綱に定める事項を備えた良好な衛生環境及び安全性を備えた、事業のための施設等において、専任の職員により事業を行い、かつ、横浜市放課後児童クラブ事業の決定に関する要綱（令和4年2月25日こ放第2124号。以下「決定要綱」という。）に基づき、クラブが所在する区の区長（以下「区長」という。）が適当と認めたものをいう。
- 2 この要綱において「支援の単位」とは、クラブにおける育成支援であって、クラブを利用する児童に対して一体的に行われる集団の規模をいう。
- 3 この要綱において「対象児童数」とは、当該クラブを毎日利用する児童の人数に一時的に利用する児童の平均利用人数を加えた数をいう。
- 4 この要綱における用語の定義は、前項に定めるもののほか、法、条例、補助金交付要綱、決定要綱の例による。

### （運営主体）

第3条 運営委員会が運営主体となる場合は、クラブの運営にあたり次の各号を行うものとする。

（1）運営委員会には以下の役員を設置し、所管する業務を行うこと。

ア 委員長

イ 副委員長

- ウ 会計
- エ 会計監査
- オ その他必要な役員

- (2) 運営委員会の意思決定は総会を開催して行うこと。総会の開催等に必要な事項は、各運営委員会において定めること。
  - (3) 各年度2回以上総会を開催し、予算、決算及び運営に必要な事項について審議すること。
  - (4) 予算、決算については、原則として区長に提出する前に総会に付議すること。
  - (5) 総会を開催した場合は、議事録を作成し、希望する保護者等の縦覧に供すること。
  - (6) 運営状況について、保護者や学校等に積極的に情報提供を行うこと。
- 2 法人が運営主体となる場合は、前項第4号、第5号及び第6号に準じた内容を行うものとする。

#### (対象児童)

第4条 事業の対象児童は、横浜市内に在住し、かつ、小学校に就学している児童であって、次のいずれかに該当するものとする。

- (1) その保護者が、労働等により、放課後に当該児童が帰宅する時間帯（学校休業日（日曜日を除く。）にあつては、当該時間帯に相当する時間帯）に、家庭にいないこと。
- (2) その保護者が、健康上の理由等により、昼間家庭にいても当該児童の健全育成ができる環境にならない状態であること。

#### (事業内容)

第5条 事業の実施にあたっては、次に掲げる活動を行うものとする。

- (1) 児童の健康管理、安全確保、情緒の安定
- (2) 児童の活動への意欲と態度の形成
- (3) 遊びを通じた児童の自主性、社会性、創造性の向上
- (4) 児童の活動状況の把握と児童の家庭との日常的な連絡及び情報交換
- (5) 学校との迅速な情報交換と日常的な連携
- (6) 地域及び関係機関との連携
- (7) その他児童の健全育成に関して必要な活動

#### (開所日及び開所時間)

第6条 クラブは、次の各号に規定する日を除き毎日開所しなければならない。ただし、土曜日については開所しないことができるが、その場合でも原則として年間250日以上開所するよう努めなければならない。

- (1) 日曜日
- (2) 国民の祝日に関する法律（昭和23年法律第178号。）第3条に規定する休日
- (3) 1月2日、1月3日及び12月29日から12月31日まで

2 クラブは、次に掲げる時間帯において開所しなければならない。

- (1) 平日に開所する場合  
放課後から午後7時まで
- (2) 土曜日に開所する場合  
1日につき10時間以上かつ午後7時まで

### (3) 学校休業日に開所する場合

1 日につき 10 時間以上かつ午後 7 時まで

- 3 前項の規定にかかわらず、当該日における利用する児童がいないことが確認できた場合は、事前に利用者へ周知したうえで、閉所又は開所時間の変更を行うことができる。
- 4 第 1 項及び第 2 項の規定にかかわらず、区長がやむを得ないと認める場合は、臨時に閉所することができる。

### (実施場所の基準)

- 第 7 条 事業を行う実施場所（以下「実施場所」という）は、条例第 9 条に規定される設備の基準を満たさなければならない。
- 2 条例第 9 条に規定される専用区画の面積の算定にあたっては、物置、便所等利用児童が直接活動において使用しない部分を除くものとする。
  - 3 実施場所は、次のいずれかの要件を満たす建築物の中において確保しなければならない。
    - (1) 昭和 56 年 6 月 1 日以降に建築確認を得て着工され、検査済証を取得していること（検査済証と同等の建築関係法令適合状況を証明できる場合を含む）。
    - (2) 平成 18 年国土交通省告示第 184 号別添の規定に基づき建築物の耐震性を判定し（以下、「耐震診断」という。）、耐震性が確保されていると判定されていること。
    - (3) 耐震診断の結果、耐震性が確保されていないと判定された建築物に対し、判定した際に用いた診断法に基づき、耐震性が確保されていると判定されるよう改修計画を策定し、当該改修計画に基づき耐震改修工事を行い、耐震性を確保していること。
  - 4 実施場所の近隣には活動に利用できる公園・広場等があることが望ましい。また、実施場所の近隣や通学路には広い歩道やガードレールが設置されているなど、安全が確保できていることが望ましい。

### (支援の単位)

- 第 8 条 支援の単位は、対象児童数が概ね 40 人までとなるよう構成しなければならない。
- 2 対象児童数が 40 人を超える場合は、1 つの支援の単位の対象児童数が概ね 40 人までで構成できるよう、複数の支援の単位を構成しなければならない。この場合、それぞれの支援の単位ごとに属する児童を決めることとする。

### (職員)

- 第 9 条 条例第 10 条に定める職員は、勤務時間内は専任とし、兼務しないものとする。
- 2 運営主体は、第 5 条に規定する事業内容を円滑に実施し、利用児童の安全を確保するため、別表 1 に規定する常勤職員の人数を雇用するものとする。
  - 3 前項における常勤職員は、週 30 時間以上勤務しなければならない。

### (研修)

- 第 10 条 運営主体は、職員の資質向上を図り、第 5 条に規定する事業内容を円滑かつ安全に実施するため、職員に対し、障害児の対応をはじめとする、活動に必要な知識・経験を養うための研修を実施するよう努めなければならない。
- 2 運営主体は、条例第 8 条に定める職員の知識及び技能の向上と資質向上を図るため、横浜市が実施する人材育成研修について、職員の参加の機会を提供しなければならない。



- 3 運営主体は、関係機関が実施する研修について、職員の参加の機会を提供するよう努めなければならない。
- 4 運営主体は、職員が自発的、継続的に研修に参加できるよう、研修計画を策定しなければならない。

(安全管理)

第11条 運営主体は、平常時から危機を想定してその予防に最善を尽くすこととし、事件、事故及び災害等（以下「事故等」という。）の危機管理についての対応マニュアルを作成するとともに、事故等の発生時に迅速かつ確かな緊急対策を実施できるよう関係機関との連携に努めなければならない。

(保護者会の開催)

第12条 運営主体は、保護者と協力して事業を実施するとともに、保護者の意見、要望等を踏まえた運営を行うため、利用する児童の保護者をもって組織する保護者会を設置し、保護者会を各年度に2回以上開催し、運営状況等について開示しなければならない。

(個人情報の保護)

第13条 運営主体は、事業による事務を処理するための個人情報の取り扱いについて、別に定める「横浜市放課後児童健全育成事業個人情報取扱特記事項」（平成18年3月福子放第10304号）を遵守しなければならない。

(調査又は報告)

第14条 区長は、本要綱に基づく適正な事業実施を維持するため、運営主体に対して、関係書類を閲覧し、又は提出を求め、運営状況を調査し、又は報告を徴することができる。

(留意事項)

- 第15条 第1条第2項に基づき実施する放課後児童クラブ事業と目的を異にするスポーツクラブや塾等、その他公共性を欠くものは、本事業に該当しない。
- 2 利用者の募集に当たっては、事業の公共性に留意して行うこと。

(補則)

第16条 この要綱に定めるもののほか、この要綱の実施に関して必要な事項については、別に子ども青少年局長が定める。

附 則（令和4年2月25日こ放第2124号）

(施行期日)

- 1 この要綱は、令和4年2月25日から施行し、令和4年度の予算に係る補助金等から適用する。

(経過措置)

- 2 当面の間、平成27年3月31日以前から存するクラブに対する第7条第3項の規定の適用については、同項中「しなければならない」とあるのは、「するよう努めなければならない」とする。
- 3 施行日から令和7年3月31日までの間、第10条第4項中「策定しなければならない」とあるのは、「策定するよう努めなければならない」と読み替えて適用する。

別表1(第9条第2項)

常勤職員の最低雇用人数		
1つの支援の単位で運営しているクラブ		複数の支援の単位で運営しているクラブ
対象児童数 19人以下	対象児童数 20人以上	支援の単位ごとに最低1人
最低1人	最低2人	

## 横浜市放課後児童クラブ事業費補助金交付要綱

制 定 平成 18 年 3 月 2 日 福子放第 10191 号（市長決裁）  
全部改正 令和 4 年 2 月 25 日 こ放第 2212 号（局長決裁）  
最近改正 令和 5 年 12 月 8 日 こ放第 1129 号（局長決裁）

横浜市放課後児童クラブ事業費補助金交付要綱を次のとおり定める。

### 横浜市放課後児童クラブ事業費補助金交付要綱

横浜市放課後児童クラブ事業補助金交付要綱（平成 18 年 3 月 2 日制定）の全部を改正する。

#### （目的）

- 第 1 条 この要綱は、横浜市放課後児童クラブ事業実施要綱（平成 22 年 3 月 8 日こ放第 891 号。以下「実施要綱」という。）に定める放課後児童クラブ（以下「クラブ」という。）の運営主体に対して、年度ごとに横浜市の予算の範囲内で交付する放課後児童クラブ事業費補助金（以下「補助金」という。）について必要な事項を定める。
- 2 補助金の交付については、横浜市補助金等の交付に関する規則（平成 17 年 11 月 30 日横浜市規則第 139 号。以下「補助金規則」という。）に定めるもののほか、この要綱の定めるところによる。

#### （用語の定義）

- 第 2 条 この要綱における用語の定義は、児童福祉法（昭和 22 年法律第 164 号）、横浜市放課後児童健全育成事業の設備及び運営の基準に関する条例（平成 26 年 9 月横浜市条例第 49 号。以下「条例」という。）、補助金規則、横浜市放課後児童健全育成事業の届出等に関する要綱（平成 27 年 2 月 26 日こ放第 930 号。以下「届出要綱」という。）、横浜市放課後児童クラブ決定要綱（令和 4 年 2 月 25 日こ放第 2124 号。以下「決定要綱」という。）及び実施要綱の例による。

#### （補助事業者の要件）

- 第 3 条 この要綱における補助事業者は、決定要綱第 9 条第 1 項に規定する決定を受けたクラブの運営主体とする。
- 2 補助金の交付を受けるには、当該年度の 4 月 1 日において、クラブの対象児童数が 10 人以上となっていなければならない。
- 3 補助事業者は、当該年度の 4 月 1 日から 3 月 31 日までの 12 か月間、かつ 200 日以上クラブを開所しなければならない。ただし、クラブが所在する区の区長（以下「区長」という。）がやむを得ないと認める場合は、この限りではない。

#### （補助金の区分、補助対象経費及び補助金額の算定）

- 第 4 条 この要綱における補助金の区分は次の各号に掲げるとおりとする。

- (1) 基本事業費
- (2) 特別加算

- 2 前項に掲げる補助対象経費、補助金額等は、別表 1 から別表 9 に定めるものとする。なお、特別加算のうち、放課後児童支援員等キャリアアップ処遇改善費補助については本要綱に定めるほか、「放課後児童支援員等キャリアアップ処遇改善費補助実施細目」（平成 29 年 10 月 31 日こ放第 680 号。以下「キ

キャリアアップ実施細目」という。)に必要な事項を定める。

- 3 前項に基づき積算する補助金は、補助金の総額に百円未満の端数があるときは、その端数金額を切り捨てるものとする。
- 4 第2項に規定する補助対象経費には、本補助金とは別に国や地方公共団体等から助成等を受けた額は含まないものとする。
- 5 第2項の規定にかかわらず、区長が特に必要と認める場合は、こども青少年局長と協議の上、別表1から別表9に定める補助金を変更することができる。

(事業実施月数が12か月に満たない場合の補助金額の算定)

第5条 第3条第3項ただし書に該当する事業者は、前条第2項の規定にかかわらず、次の各号に規定する月数に応じて、別表10に定めるとおり補助金額を算定する。

- (1) 当該年度の中途において開所又は休止後の再開(以下「開所等」という。)をした場合  
開所等の日(以下「事業開始日」という。)から当該年度の3月31日まで
  - (2) 当該年度の中途において廃止又は休止(以下「廃止等」という。)をした場合  
当該年度の4月1日から廃止等の日(以下「事業廃止日」という。)まで
  - (3) 当該年度の中途において開所等をし、当該年度の中途において廃止等をした場合  
事業開始日から事業廃止日まで
  - (4) 前3号の当該年度における放課後児童クラブ事業を実施する月数(以下「事業実施月数」という。)は、暦に従って計算し、一月に満たない端数が生じたときは、これを切り捨てるものとする。
- 2 前項の規定にかかわらず、区長が特に必要と認める場合は、こども青少年局長と協議の上、別表10に定める補助金を変更することができる。

(交付の申請)

第6条 補助金の交付を受けようとする補助事業者は、区長が定める期日までに横浜市放課後児童クラブ事業費補助金交付申請書(第1号様式)に次の各号に掲げる書類を添付し、区長に提出しなければならない。

- (1) 運営概要書(第2号様式)
  - (2) 収支予算書(第3号様式)
  - (3) 資金計画表(第4号様式)
  - (4) その他区長が必要と認める書類
- 2 補助金規則第5条第3項の規定により、横浜市放課後児童クラブ事業費補助金交付申請書(第1号様式)への添付を省略させることができる書類は、補助事業者の資産及び負債に関する事項を記載した書類とする。

(交付の決定)

第7条 区長は、前条第1項に規定する申請を受理したときは、その内容を審査し、適正と認める場合は補助金の交付額を決定し、横浜市放課後児童クラブ事業費補助金交付決定通知書(第5号様式)により、補助事業者に通知するものとする。

- 2 区長は、前項に規定する交付決定通知書により通知する場合において、必要があるときは当該補助金の交付について条件を付すことができる。

(補助金の交付及び交付の時期)

第8条 補助事業者の資金状況を勘案し、補助事業の完了前に補助金を交付しなければ、補助事業等を実施できない場合は、補助金規則第17条ただし書の規定により、補助事業の完了前に補助金の全部又は一部を交付することができる。

- 2 前項に定める補助金の交付は、補助事業者からの請求に基づいて交付するものとする。
- 3 補助金の交付の時期及び各期の交付額は、前条第1項に規定する交付決定通知書又は第9条第5項に規定する変更交付決定通知書において示すところによる。

(執行状況報告及び交付額の変更)

第9条 補助事業者は、当該年度の7月、1月及びその他区長が必要と認める月において、補助金の執行状況を区長が定める期日までに、横浜市放課後児童クラブ事業費補助金執行状況報告書(第6号様式)により報告しなければならない。

- 2 補助事業者は、前項の書類と合わせて別表11に定める書類を区長に提出しなければならない。ただし、届出要綱や実施要綱等に基づき、区長が補助事業者から既に報告を受けている書類について、区長はその書類の提出を省略させることができる。
- 3 前項に定めるほか、区長は必要に応じて補助金の執行状況に関する書類の提出を補助事業者に求めることができる。
- 4 第1項に規定する執行状況報告又はその他の事情により、交付額の変更申請を行うときは、区長が定める期日までに横浜市放課後児童クラブ事業費補助金変更交付申請書(第18号様式)に資金計画表(第4号様式)を添付し、区長に提出するものとする。
- 5 区長は、前項の規定による申請を受理したときは、その内容を審査し、適正と認める場合は補助金の交付額の変更を決定し、横浜市放課後児童クラブ事業費補助金変更交付決定通知書(第19号様式)により、補助事業者へ通知するものとする。
- 6 区長は、前項に規定する変更交付決定を通知する場合において、必要があるときは当該補助金の交付について条件を付すことができる。

(申請の取下げ)

第10条 補助金規則第9条第1項の規定により定める申請の取下げの期間は、補助事業者が第7条第1項に規定する交付決定通知書又は前条第5項に規定する変更交付決定通知書の交付を受けた日の翌日から起算して10日以内の日とする。

(実績報告)

第11条 補助事業者は事業終了後、区長が定める期日までに横浜市放課後児童クラブ事業費補助金実績報告書(第20号様式)に基本事業費補助額算定書(第21号様式)及び区長が必要と認める書類を添付し、区長に提出しなければならない。また、第8条第1項の規定により補助事業の完了前に補助金の全部又は一部の交付を受けた場合は、補助金の精算を行わなければならない。

- 2 障害児受入推進加算補助及び障害児受入強化推進加算補助の交付を受けた補助事業者は、前項に規定する実績報告時に、障害児受入に係る補助対象経費等報告書(第22号様式)とその他区長が必要と認める書類を提出しなければならない。
- 3 医療的ケア児受入加算補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、医療的ケア児受入に係る補助対象経費等報告書(第23号様式)とその他区長が必要と認める書類を提出しなけ

ればならない。

- 4 育成支援体制強化加算補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、育成支援体制強化加算補助対象経費等報告書（第24号様式）とその他区長が必要と認める書類を提出しなければならない。
- 5 放課後児童支援員等キャリアアップ処遇改善費補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、放課後児童支援員等キャリアアップ処遇改善費補助対象経費積算書（第25号様式）とその他区長が必要と認める書類を提出しなければならない。
- 6 賃金改善加算補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、賃金改善加算補助実施報告書（第26号様式）、賃金改善加算補助賃金改善額内訳書（第27号様式）及びその他区長が必要と認める書類を提出しなければならない。
- 7 新型コロナウイルス感染拡大防止加算補助の交付を受けた補助事業者は、第1項に規定する実績報告時に、新型コロナウイルス感染拡大防止加算補助対象経費等報告書（第28号様式）とその他区長が必要と認める書類を提出しなければならない。

#### （補助金額の確定）

第12条 補助事業者に対する補助金規則第15条の規定による補助金額の確定の通知は、横浜市放課後児童クラブ事業費補助金交付額確定通知書（第29号様式）により行うものとする。

#### （補助金の請求）

第13条 補助金の交付請求は、請求書（第30号様式）により行わなければならない。

#### （決定の取消）

第14条 区長は、次のいずれかの事情が生じたときは、交付の決定の全部又は一部を取消することができる。

- (1) 補助金交付要件を満たさなくなったとき。
- (2) 第10条に規定する補助金申請の取下届が提出されたとき。
- (3) 偽りその他不正な手段により、補助金の交付を受けたとき。
- (4) 補助金を交付の目的以外に使用したとき。
- (5) 決定要綱、実施要綱及び本要綱の規定に違反したとき。
- (6) 第7条第1項又は第9条第5条に基づき交付決定した内容又はこれに付した条件に違反したとき。
- (7) その他区長が不相当と認める事情が生じたとき。

2 区長は、第1項の規定による補助金の交付決定を取り消した場合は、当該補助事業者に対し、横浜市放課後児童クラブ事業費補助金交付決定取消通知書（第31号様式）により、速やかに、その旨を通知するものとする。

#### （補助金の返還）

第15条 区長は、補助金の交付の決定を取り消した場合において、事業の当該取消しに係る部分に関し、既に補助金が交付されているときは、期限を定めて、その返還を命ずるものとする。

2 区長は、補助事業者に交付すべき補助金の額を確定した場合において、既にその額を超える補助金が交付されているときは、期限を定めて、確定額を超える部分の補助金の返還を命ずるものとする。

(消費税及び地方消費税に係る仕入控除税額の確定に伴う補助金の返還)

第 16 条 補助事業者は、事業完了後に消費税及び地方消費税の申告によりこの補助金に係る消費税及び地方消費税に係る仕入控除税額が確定した場合は、速やかに、消費税及び地方消費税に係る仕入控除税額報告書(第 32 号様式)に必要な書類を添付し、区長へ報告しなければならない。

2 前項に定める報告について、補助事業者が全国的に事業を展開する組織の支部(又は一支社、一支所等)であって、自ら消費税及び地方消費税の申告を行わず、本部(又は本社、本所等)で消費税及び地方消費税の申告を行っている場合は、本部の課税売上割合等の申告に基づき報告を行うこと。

3 補助事業者は、第 1 項に規定する区長への報告を行った後、当該仕入控除税額分の補助金を市に返還しなければならない。

(財産の処分の制限)

第 17 条 補助金規則第 25 条ただし書の規定により財産の処分の制限がかからなくなるために必要な期間は、補助事業により取得し、又は効用の増加した不動産及びその従物並びに補助事業により取得し、又は効用の増加した価格が単価 50 万円以上の機械器具等については、「補助事業等により取得し、又は効用の増加した財産の処分制限期間」(令和 5 年こども家庭庁告示第 9 号)に定めるとおりとする。

(暴力団排除に関する取扱い)

第 18 条 次の各号に該当する者は、この補助金の交付の対象としない。

- (1) 横浜市暴力団排除条例(平成 23 年 12 月横浜市条例第 51 号)第 2 条第 2 号の暴力団
- (2) 同条例同条第 4 号の暴力団員等
- (3) 同条例同条第 5 号の暴力団経営支配法人等
- (4) 同条例第 7 条の暴力団員等と密接な関係を有すると認められる者

2 区長は、必要に応じ申請者又は第 7 条の交付の決定を受けたものが、前項各号のいずれかに該当するか否かを神奈川県警察本部長に対して確認を行うことができる。

3 区長は、交付の決定を受けたものが、第 1 項各号のいずれかに該当するときは、交付決定の全部又は一部を取り消すことができる。

(書類の整備等)

第 19 条 補助事業者は、放課後児童クラブ事業の適正な管理を図るため、児童の利用状況、職員等の出勤状況及び放課後児童クラブ事業に係る収入及び支出の状況を明らかにした帳簿等を備え保管するとともに、これらについての証拠書類を整理し、各年度の事業終了後 5 年間保存しなければならない。ただし、補助事業により取得し、又は効用の増加した不動産及びその従物並びに補助事業により取得し、又は効用の増加した価格が単価 50 万円以上の機械器具等がある場合は、「補助事業等により取得し、又は効用の増加した財産の処分制限期間」(令和 5 年こども家庭庁告示第 9 号)を経過する日まで保存しなければならない。

(調査又は報告)

第 20 条 区長は、補助金の適正な執行を確認するため等、必要があると認めるときは、補助事業者に対して、前条の書類を閲覧し、又は提出を求め、運営状況を調査し、又は報告を徴することができる。

(補則)

第 21 条 補助事業者が第 14 条第 1 項の規定に該当し、かつ、著しい不正があったと区長が認める場合、翌年度以降、本補助金の対象としないことができる。

2 この要綱に定めるもののほか、この要綱の実施に関して必要な事項については、別に子ども青少年局長が定める。

附則（令和 4 年 2 月 25 日こ放第 2212 号）

（施行期日）

1 この要綱は、令和 4 年 2 月 25 日から施行し、令和 4 年度の予算に係る補助金から適用する。

（横浜市放課後児童クラブ事業補助金施設賃借料加算要綱の廃止）

2 横浜市放課後児童クラブ事業補助金施設賃借料加算要綱（令和 2 年 1 月 30 日こ放第 960 号）は、この要綱の施行をもって廃止する。なお、令和 3 年度までの予算に係る施設賃借料加算については、従前の例による。

（補助事業者の要件の特例）

3 第 3 条第 2 項の規定にかかわらず、当面の間、当該年度の 4 月 1 日時点のクラブの対象児童数が 10 人未満となった場合であっても、前年度の 4 月から 12 月の各月 1 日時点の対象児童数の平均が 10 人以上であったクラブは、補助金の交付を受けることができるものとする。

（賃金改善加算補助の補助対象期間）

4 別表 6 に規定する賃金改善加算補助の令和 4 年度の補助対象期間については、令和 3 年度の横浜市放課後児童クラブ事業費補助金の交付を受けたクラブの補助事業者に限り、補助対象期間を令和 4 年 2 月 1 日に遡及して適用する。

（移転支援加算の取扱い）

5 横浜市放課後児童クラブ移転事業実施要綱（平成 31 年 4 月 1 日こ放第 1211 号）により移転支援加算の交付を受けた補助事業者（当該補助事業者が決定要綱第 4 条第 2 項及び第 3 項に該当したことにより新たに決定要綱第 9 条第 1 項に規定する決定を受けた補助事業者を含む）は、第 4 条第 2 項の規定にかかわらず、当該移転支援加算の加算額に相当する額を 5 で除して得た額を別表 2 に規定する基本補助から調整し、移転を実施した日が属する年度の翌年度の 4 月 1 日から 60 か月間（補助金が交付されていない期間を除く）適用する。

なお、当該移転支援加算の加算額に相当する額の基本補助からの調整を適用する補助事業者、適用期間及びその他適用に係る事項については、別に子ども青少年局長が定める。

（利用者負担緩和補助の取扱い）

6 横浜市放課後児童クラブ利用者負担緩和補助実施要綱（令和元年 6 月 10 日こ放第 146 号）により利用者負担緩和補助の交付を受けた補助事業者について、当該利用者負担緩和補助は、当該要綱第 6 条第 2 項にて認定した補助基準額、補助対象児童及び補助対象期間を基に算定する。

附則（令和 4 年 11 月 1 日こ放第 1692 号）

（施行期日）

この要綱は、令和 4 年 11 月 1 日から施行し、令和 4 年度中に交付する補助金から適用する。

附則（令和 5 年 2 月 27 日こ放第 2735 号）

（施行期日）

この要綱は、令和 5 年 2 月 27 日から施行し、令和 5 年度の予算に係る補助金から適用する。



附則（令和5年6月20日こ放第436号）

（施行期日）

この要綱は、令和5年6月20日から施行し、令和5年度の予算に係る補助金から適用する。

附則（令和5年8月23日こ放第698号）

（施行期日）

この要綱は、令和5年8月23日から施行し、令和5年度の予算に係る補助金から適用する。

附則（令和5年11月13日こ放第993号）

（施行期日）

この要綱は、令和5年11月13日から施行し、令和5年度の予算に係る補助金から適用する。

附則（令和5年12月8日こ放第1129号）

（施行期日）

この要綱は、令和5年12月8日から施行し、令和5年度の予算に係る補助金から適用する。

別表1 (第4条第2項)  
【放課後児童クラブ事業費補助金算定基準】

項目		金額	基準年月	算定基準・説明等	補助対象経費	
基本 補助	基礎部分 (支援の単位あたり)	別表2のとおり				人件費・管理運営費・児童処遇費・施設利用料等
	規模調整部分 (1クラブあたり)					
	開所日数加算補助 (支援の単位あたり)	19,000円/日	当該年度の4月から3月までの実績	年間250日を超えて開所している日数		
	長時間開所加算補助 【平日分】 (1クラブあたり)	30分あたり 204,500円/年	当該年度の4月から3月までの実績	平日に6時間を超えて開所し、かつ、午後7時以降も開所している年間平均時間数 ※年間平均時間数は、30分単位で算定するものとする。(30分未満の端数は切り捨て)		
	長時間開所加算補助 【学校休業日等分】 (1クラブあたり)	30分あたり 92,000円/年	当該年度の4月から3月までの実績	土曜日及び学校休業日に、実施要綱第6条第2項に定める開所時間を満たした上で、10時間を超えて開所している年間平均時間数 ※年間平均時間数は、30分単位で算定するものとする。(30分未満の端数は切り捨て)		
小規模激変緩和加算補助 (1クラブあたり)	200～249日	198,000円/年	当該年度の4月から3月までの実績	前年度の4月から3月のクラブ全体の対象児童数の平均が20人以上であったが、当該年度の4月から3月のクラブ全体の対象児童数の平均が19人以下となったクラブ(年度途中で分割を行ったクラブは除く。) ※当該年度の4月から3月までの年間開所日数に応じて、それぞれ左記の補助額とする。		
	250日以上	1,001,000円/年				
障害児受入推進加算補助 (支援の単位あたり)		別表3のとおり				
障害児受入強化推進加算補助 (支援の単位あたり)		別表4のとおり				
医療的ケア児受入加算補助 (支援の単位あたり)		別表5のとおり				
育成支援体制強化加算補助 (1クラブあたり)		別表6のとおり				
放課後児童支援員等キャリアアップ処遇改善費補助 (支援の単位あたり)		上限 919,000円/年	当該年度の4月から3月までの実績 ※2、3月は1月の実績を適用するものとする	放課後児童支援員等の賃金改善に要した費用	賃金改善に要する経費	
賃金改善加算補助 (常勤換算1.0人あたり)		別表7のとおり				
保護者負担減額相当補助 (1人あたり)		2,500円/月	当該年度の4月から3月までの実績 ※1～3月は12月の実績を適用するものとする	横浜市の就学援助を受けている世帯、生活保護受給世帯及び市民税所得割非課税世帯の児童(以下「減免対象児童」という。)の人数 ※月の途中で新たに減免対象児童に該当した場合、当該月は補助対象とする。	減免対象児童の保護者負担金の減免に要する経費	
人材育成加算補助 (1クラブあたり)		常勤職員1人あたり 4,000円 非常勤職員1人あたり 2,230円	当該年度の4月から12月までの実績	横浜市が指定する研修を受講した職員の人数 ※実施要綱第10条4項に基づく研修計画の策定し、運営主体が主催となる研修を1回以上実施することを要件とする。 ※同一人物が複数回研修を受講した場合でも、人数は1人分とする。	研修受講に要する人件費・研修開催に要する経費等	
常勤職員の産前・産後休暇に伴う代替職員配置経費補助 (1人あたり)		656,600円/年  (※多胎妊娠の場合) 1,031,800円/年	出産予定日から起算して産前6週(多胎妊娠の場合は14週)及び産後8週	産前・産後休暇を取得する常勤職員数 ※産前・産後休暇が次年度に渡る場合は、日割りで補助額を算定する。 ※運営主体が常勤職員の産前・産後休暇期間の給与を支給しない場合は、補助対象外とする。	常勤職員が産前・産後休暇を取得する14週間分(多胎妊娠の場合は22週間分)の代替職員の配置にかかる人件費	
新型コロナウイルス感染拡大防止加算補助 (支援の単位あたり)		別表8のとおり				
施設賃借料加算Ⅱ (1クラブあたり)		別表9のとおり				
物価高騰対策加算 (支援の単位あたり)		22,500円	当該年度の4月から9月までの実績	当該年度の4月から9月までにクラブが運営している最大の支援の単位数	クラブの活動場所における施設の光熱費等	
		15,000円	当該年度の10月から3月までの実績	当該年度の10月から1月までにクラブが運営している最大の支援の単位数		

- ※1 基準年月については、別に規定している場合を除き、各月の実績は1日時点の実績を採用する。
- ※2 補助対象経費には、当該クラブの放課後児童クラブ事業の実施に関与しない経費は含まない。
- ※3 複数の補助項目で、同一の経費を重複して計上することはできない。
- ※4 当該年度の4月から3月までの年間開所日数が200日に満たない支援の単位については、基本補助のうちの基礎部分、障害児受入推進加算補助、障害児受入強化推進加算補助、医療的ケア児受入加算補助、放課後児童支援員等キャリアアップ処遇改善費補助、新型コロナウイルス感染拡大防止加算補助及び物価高騰対策加算の補助対象とはならない。なお、第3条第3項ただし書に該当するクラブについては、「当該年度の4月から3月までの年間開所日数が200日に満たない」とあるのは、「当該年度の事業実施月の開所日数の月平均が17日に満たない」と読み替えるものとする。
- ※5 当該クラブが運営する全ての支援の単位について、当該年度の4月から3月までの年間開所日数が200日に満たない場合は、別表1に規定する全ての基本事業費及び特別加算の交付を受けることができない。なお、第3条第3項ただし書に該当するクラブについては、「当該年度の4月から3月までの年間開所日数が200日に満たない」とあるのは、「当該年度の事業実施月の開所日数の月平均が17日に満たない」と読み替えるものとする。

別表2（第4条第2項）

項目	基本補助																										
補助上限額	<p>基本補助は、「基礎部分」と「規模調整部分」の合計額とし、「基礎部分」と「規模調整部分」はそれぞれ下記のとおり算定する。</p> <p>(1) 基礎部分（支援の単位あたり） 当該年度の4月から3月の支援の単位ごとの対象児童数の平均及び当該年度の4月から3月までの支援の単位ごとの年間開所日数に応じて、次のとおり支援の単位ごとに補助上限額を決定する。</p> <p style="text-align: center;"><b>【基礎部分の補助上限額（年額）】</b></p> <table border="1" data-bbox="408 356 914 510"> <thead> <tr> <th rowspan="2">対象児童数</th> <th colspan="2">年間開所日数</th> </tr> <tr> <th>200～249日</th> <th>250日以上</th> </tr> </thead> <tbody> <tr> <td>10～19人</td> <td>2,351,000円</td> <td>3,551,000円</td> </tr> <tr> <td>20～40人</td> <td>3,099,000円</td> <td>5,102,000円</td> </tr> </tbody> </table> <p>(2) 規模調整部分（1クラブあたり） 当該年度の4月から3月までにクラブが運営している最大の支援の単位数及び当該年度の4月から3月までの対象児童数の平均に応じて、次のとおり補助上限額を決定する。</p> <p style="text-align: center;"><b>【規模調整部分の補助上限額（年額）】</b></p> <table border="1" data-bbox="408 674 997 880"> <thead> <tr> <th>支援の単位数</th> <th>対象児童数</th> <th>補助上限額</th> </tr> </thead> <tbody> <tr> <td>1単位</td> <td>10～19人</td> <td>2,800,000円</td> </tr> <tr> <td>1単位</td> <td>20～40人</td> <td>2,250,000円</td> </tr> <tr> <td>2単位</td> <td>—</td> <td>1,200,000円</td> </tr> <tr> <td>3単位以上</td> <td>—</td> <td>150,000円</td> </tr> </tbody> </table>	対象児童数	年間開所日数		200～249日	250日以上	10～19人	2,351,000円	3,551,000円	20～40人	3,099,000円	5,102,000円	支援の単位数	対象児童数	補助上限額	1単位	10～19人	2,800,000円	1単位	20～40人	2,250,000円	2単位	—	1,200,000円	3単位以上	—	150,000円
対象児童数	年間開所日数																										
	200～249日	250日以上																									
10～19人	2,351,000円	3,551,000円																									
20～40人	3,099,000円	5,102,000円																									
支援の単位数	対象児童数	補助上限額																									
1単位	10～19人	2,800,000円																									
1単位	20～40人	2,250,000円																									
2単位	—	1,200,000円																									
3単位以上	—	150,000円																									
補助額の減算	<p>次の(1)から(3)により算定した額を、「基礎部分」と「規模調整部分」の合計額から減算する。</p> <p>(1) 施設賃借料に伴う減算 クラブの運営主体が、施設賃借料（施設管理に伴う負担金含む）として貸主に支払っている土地・建物の年額賃料が2,400,000円に満たない場合は、差額の2分の1の額を減算する。なお、一円未満の端数があるときは、その端数金額を切り捨てるものとする。</p> <p>※1 「施設管理に伴う負担金」とは、自治会館等を賃貸借契約によらず借用する場合の負担金とし、金額の正当性が確認できる書類を添付する。</p> <p>※2 「土地・建物の年額賃料」には、共益費、光熱水費、駐車場・倉庫の借上料は含まないものとする。</p> <p>※3 施設賃借料加算Ⅱの適用を受けているクラブについては、分室先の家賃、間代及び地代は「土地・建物の年額賃料」に含まないものとする。</p> <p>(2) 次年度繰越金の上限額超過に伴う減算 次年度繰越金が決算年度の運営経費（積立金を除く）の1割を超えた場合は、1割を超えた金額分を減算する。</p> <p>(3) 対象児童数が10人未満となったことに伴う減算 下記の①又は②に該当するクラブは、基礎部分及び規模調整部分は対象児童数が「10～19人」の欄の金額を適用するものとするが、基礎部分と規模調整部分の合計額より290,000円を減算する。</p> <p>①当該年度の4月1日時点でクラブ全体の対象児童数が10人以上であったが、4月から3月までのクラブ全体の対象児童数の平均が10人未満となったクラブ</p> <p>②附則（令和4年2月25日こ放第2212号）第3条の適用を受けており、当該年度の4月から3月までのクラブ全体の対象児童数の平均も10人未満となったクラブ</p>																										
補助対象経費	人件費・管理運営費・児童処遇費・施設利用料等																										
留意事項	<ul style="list-style-type: none"> <li>実施要綱第6条第2項に定める開所時間を通して、条例第10条第2項に定める職員の最低配置基準を満たしていない日については、基礎部分の開所日数の算定に含めることができない。ただし、次の(1)～(3)のいずれかに該当する場合は、基礎部分の開所日数の算定に含めることができる。</li> <li>(1)複数の支援の単位で運営しているクラブにおいて、条例第18条第1項第1号又は第2号に定める時間を通して、条例第10条第2項に定める職員の最低配置基準を満たしている場合は、1つの支援の単位を除く当該支援の単位。</li> <li>(2)土曜日及び実施要綱第6条第1項各号に定める日に、実施要綱第6条第3項に基づき閉所又は開所時間の変更を行うクラブにおいて、条例第18条第1項第1号に定める時間を通じて、条例第10条第2項に定める職員の最低配置基準を満たしている場合。</li> <li>(3)実施要綱第6条第4項に基づき、臨時に閉所した場合。</li> <li>当該年度の4月1日時点の対象児童数が40人以下であったが、4月から3月までの対象児童数の平均が41人以上45人以下となった支援の単位については、基礎部分は対象児童数が「20～40人」の欄の金額を適用するものとする。また、当該年度を通して1支援単位で運営しているクラブで、当該年度の4月1日時点の対象児童数が40人以下であったが、4月から3月までの対象児童数の平均が41人以上45人以下となった場合、規模調整部分は支援の単位数が「1単位」かつ対象児童数が「20～40人」の欄の金額を適用する。</li> <li>運営主体は、令和3年度の常勤職員の処遇を維持しなければならない。また、非常勤職員については、神奈川県最低賃金を下回ってはならない。なお、運営主体は、職員の処遇の向上に努めなければならない。</li> </ul>																										

別表3（第4条第2項）

項目	障害児受入推進加算補助														
補助対象児童	<p>次のいずれかの条件を満たす児童</p> <p>(1) 特別支援学校又は個別支援学級に在籍している児童</p> <p>(2) 一般学級に在籍している児童のうち、「身体障害者手帳」、「療育手帳（愛の手帳）」または「精神障害者保健福祉手帳」の写しが提出されている児童</p> <p>(3) 就学している小学校等から児童の状況についての副申が記載された「支援や配慮を要する児童の申立書」（第10号様式）及び「児童状況書」（第10の2号様式）が提出されている児童</p> <p>(4) 別表5に定める医療的ケア児受入加算補助の補助対象児童</p>														
補助上限額の算定期間	<p>支援の単位ごとに、補助対象児童の利用見込みがある月</p> <p>※1～3月は12月の実績を適用するものとする。</p> <p>【利用見込みがあるとする条件と補助対象期間】</p> <p>次のいずれかの条件に該当する場合、利用見込みがあるものとする。</p> <p>条 件①：補助対象児童の利用登録があった場合 補助対象期間：補助対象児童の利用登録があった月から3月まで</p> <p>条 件②：補助対象児童の利用登録はないが、前年度に補助対象児童の利用登録があった場合 補助対象期間：当該年度の4月から3月まで</p>														
補助上限額	<p>実施要綱第6条第1項に定める開所日のうち、条例第10条第2項に定める職員の最低配置基準に加えて、障害児受入対応のために1人以上職員を追加配置した日数に応じて、次のとおり支援の単位ごとに各月の補助上限額を決定する。1月から3月については12月の実績を適用する。なお、支援の単位ごとの年間の補助上限額は2,009,000円とする。</p> <table border="1" data-bbox="395 792 1007 1077"> <thead> <tr> <th data-bbox="395 792 746 853">職員を追加配置した日数 (1か月あたり)</th> <th data-bbox="746 792 1007 853">補助上限額（月額）</th> </tr> </thead> <tbody> <tr> <td data-bbox="395 853 746 891">18日以上</td> <td data-bbox="746 853 1007 891">168,000円</td> </tr> <tr> <td data-bbox="395 891 746 929">13日以上17日以下</td> <td data-bbox="746 891 1007 929">151,000円</td> </tr> <tr> <td data-bbox="395 929 746 967">9日以上12日以下</td> <td data-bbox="746 929 1007 967">118,000円</td> </tr> <tr> <td data-bbox="395 967 746 1005">5日以上8日以下</td> <td data-bbox="746 967 1007 1005">84,000円</td> </tr> <tr> <td data-bbox="395 1005 746 1043">3日以上4日以下</td> <td data-bbox="746 1005 1007 1043">50,000円</td> </tr> <tr> <td data-bbox="395 1043 746 1077">2日以下</td> <td data-bbox="746 1043 1007 1077">0円</td> </tr> </tbody> </table>	職員を追加配置した日数 (1か月あたり)	補助上限額（月額）	18日以上	168,000円	13日以上17日以下	151,000円	9日以上12日以下	118,000円	5日以上8日以下	84,000円	3日以上4日以下	50,000円	2日以下	0円
職員を追加配置した日数 (1か月あたり)	補助上限額（月額）														
18日以上	168,000円														
13日以上17日以下	151,000円														
9日以上12日以下	118,000円														
5日以上8日以下	84,000円														
3日以上4日以下	50,000円														
2日以下	0円														
補助対象経費	<p>年間を通じて障害児を受け入れるために配置した職員（以下「障害児受入職員」という。）に要した人件費（ただし、異なる支援の単位で同一の職員を補助対象とすることはできない。）</p> <p>※年間の補助上限額と補助対象経費を比較して、低い金額で決定</p>														
研修の受講	<p>障害児受入推進加算補助の交付を受けるクラブは、交付を受ける年度において、児童の育成支援にあたる職員全員に横浜市が指定する研修を受講させなければならない。</p>														

別表4（第4条第2項）

項目	障害児受入強化推進加算補助			
補助対象児童	<p>次のいずれかの条件を満たす児童</p> <p>(1) 特別支援学校又は個別支援学級に在籍している児童</p> <p>(2) 一般学級に在籍している児童のうち、「身体障害者手帳」、「療育手帳（愛の手帳）」または「精神障害者保健福祉手帳」の写しが提出されている児童</p> <p>(3) 就学している小学校等から児童の状況についての副申が記載された「支援や配慮を要する児童の申立書」（第10号様式）及び「児童状況書」（第10の2号様式）が提出されている児童</p>			
区分	支援の単位ごとの補助対象児童の登録児童数に応じて、交付を受けることができる区分を支援の単位ごとに決定する。			
	区分	区分の説明	交付を受けるための要件	交付を受けることができる区分
	強化①	障害児受入推進加算補助による追加配置に加え、更に1名職員を配置する	支援の単位ごとの補助対象児童の登録児童数が3人以上	強化①
	強化②	強化①による追加配置に加え、更に1名職員を配置する	支援の単位ごとの補助対象児童の登録児童数が6人以上	強化①+強化②
強化③	強化②による追加配置に加え、更に1名職員を配置する	支援の単位ごとの補助対象児童の登録児童数が9人以上	強化①+強化②+強化③	
補助上限額の算定期間	支援の単位ごとに、それぞれ下記の期間とする。なお、1～3月は12月の実績を適用するものとする。			
	区分	算定期間		
	強化①	支援の単位ごとの補助対象児童の登録児童数が3人以上である月数		
	強化②	支援の単位ごとの補助対象児童の登録児童数が6人以上である月数		
強化③	支援の単位ごとの補助対象児童の登録児童数が9人以上である月数			
補助上限額	<p>実施要綱第6条第1項に定める開所日のうち、障害児受入推進加算補助による追加配置に加え、更に職員を追加配置した日数に応じて、強化①、強化②、強化③でそれぞれ、次のとおり支援の単位ごとに各月の補助上限額を決定する。1月から3月については12月の実績を適用する。なお、支援の単位ごとの年間の補助上限額は強化①、強化②、強化③それぞれ2,000,000円とする。</p>			
	職員を追加配置した日数 (1か月あたり)	補助上限額 (月額)		
	18日以上	167,000円		
	13日以上17日以下	150,000円		
	9日以上12日以下	117,000円		
	5日以上8日以下	84,000円		
	3日以上4日以下	50,000円		
2日以下	0円			
補助対象経費	<p>年間を通じて障害児受入職員の配置に要した人件費（ただし、異なる支援の単位で同一の職員を補助対象とすること及び障害児受入推進加算補助の補助対象となった職員を補助対象とすることはできない。）</p> <p>※年間の補助上限額と補助対象経費を比較して、低い金額で決定</p>			

別表5（第4条第2項）

項目	医療的ケア児受入加算補助									
補助対象児童	<p>次のすべての条件を満たす児童</p> <p>(1) クラブに在籍する児童で日常的に看護師等による医療的ケアを必要とする児童のうち、児童が通う学校において医療的ケアを受けている又は受ける予定である児童</p> <p>(2) 主治医からクラブでの活動において医療的ケアが必要とされた児童</p> <p>(3) 保護者から医療的ケアの利用申し込みがあり、クラブでの医療的ケアの実施内容について保護者の同意が得られた児童</p> <p>(4) 上記(1)～(3)の条件を満たす児童の受入れについて、看護師等の配置が可能な見込みであると本市が確認していること。</p> <p>※ 医療的ケアとは次のいずれかに該当するものをいう。</p> <table border="1" data-bbox="395 497 1177 703"> <tr> <td data-bbox="395 497 1177 548">(1) 口腔内の喀痰吸引（①口腔内、②鼻腔内、③気管カニューレ内部）</td> </tr> <tr> <td data-bbox="395 548 1177 600">(2) 経管栄養（①胃ろう又は腸ろう、②経鼻）</td> </tr> <tr> <td data-bbox="395 600 1177 651">(3) 導尿</td> </tr> <tr> <td data-bbox="395 651 1177 703">(4) その他こども青少年局長が必要と定める医療的ケア</td> </tr> </table>	(1) 口腔内の喀痰吸引（①口腔内、②鼻腔内、③気管カニューレ内部）	(2) 経管栄養（①胃ろう又は腸ろう、②経鼻）	(3) 導尿	(4) その他こども青少年局長が必要と定める医療的ケア					
(1) 口腔内の喀痰吸引（①口腔内、②鼻腔内、③気管カニューレ内部）										
(2) 経管栄養（①胃ろう又は腸ろう、②経鼻）										
(3) 導尿										
(4) その他こども青少年局長が必要と定める医療的ケア										
補助上限額の算定期間	補助対象児童がクラブを利用し、看護師等を配置した月数									
補助上限額	<p>実施要綱第6条第1項に定める開所日のうち、看護師等を配置した期間に応じて、次のとおり支援の単位ごとに各月の補助額を決定する。1月から3月の実績については12月の実績を適用する。なお、支援の単位ごとの年間補助上限額は「配置」が4,061,000円、「送迎」が1,353,000円とする。</p> <table border="1" data-bbox="395 1010 1267 1173"> <thead> <tr> <th data-bbox="395 1010 480 1061">区分</th> <th data-bbox="480 1010 1007 1061">要件</th> <th data-bbox="1007 1010 1267 1061">補助上限額 (月額)</th> </tr> </thead> <tbody> <tr> <td data-bbox="395 1061 480 1113">配置</td> <td data-bbox="480 1061 1007 1113">医療的ケアを実施する看護師等を配置した場合</td> <td data-bbox="1007 1061 1267 1113">339,000円</td> </tr> <tr> <td data-bbox="395 1113 480 1173">送迎</td> <td data-bbox="480 1113 1007 1173">送迎、付き添いに伴う看護師等を配置した場合</td> <td data-bbox="1007 1113 1267 1173">113,000円</td> </tr> </tbody> </table>	区分	要件	補助上限額 (月額)	配置	医療的ケアを実施する看護師等を配置した場合	339,000円	送迎	送迎、付き添いに伴う看護師等を配置した場合	113,000円
区分	要件	補助上限額 (月額)								
配置	医療的ケアを実施する看護師等を配置した場合	339,000円								
送迎	送迎、付き添いに伴う看護師等を配置した場合	113,000円								
補助対象経費	<p>配置：医療的ケアを実施する看護師等の人件費・交通費</p> <p>送迎：補助対象児童の送迎付き添いに伴う看護師等の人件費・交通費</p> <p>※年間の補助上限額と補助対象経費を比較して、低い額で決定。</p>									
特記事項	<ul style="list-style-type: none"> <li>・当面の間「看護師等」は「看護師」と読み替えるものとする。</li> <li>・補助対象経費に記載している看護師等の業務を外部委託等により実施し、クラブの運営主体が委託費等として支出する場合も、当該加算補助の対象とする。</li> <li>・補助金規則第24条ただし書きの規定により、補助事業者は、補助対象児童の受入れ支援にかかる補助金の補助事業等に係る業務の委託等を行う場合、いかなる場合においても市内事業者による入札又は見積書の徴収を行う必要はない。</li> <li>・当該加算補助の補助対象となった看護師等は、条例第10条第2項に定める職員の最低配置基準に含めることはできない。</li> <li>・当該加算補助の補助対象となった看護師等は、障害児受入推進加算補助及び障害児受入強化推進加算補助の補助対象とすることができない。</li> </ul>									

別表6（第4条第2項）

項目	育成支援体制強化加算補助
補助上限額 (年額)	1クラブあたり 1,451,000円
補助対象経費	育成支援の周辺業務を行う職員（以下「運営事務等を行う職員」という。）の配置等に要する経費 なお、運営事務等を行う職員は次の業務を行うこととする。 (1) 業務の実施状況に関する日誌（児童の出欠席、職員の服務に関する状況等）の作成 (2) おやつ発注、購入等 (3) 遊びの環境と施設の安全点検、衛生管理（清掃や消毒等）、整理整頓 (4) 会計事務等 (5) 児童の宿題等の学習活動が自主的に行える環境整備の補助 (6) その他、クラブの運営に関わる業務や育成支援の周辺業務
留意事項	<ul style="list-style-type: none"> <li>上記(1)～(6)に記載している運営事務等を行う職員の業務を外部委託等により実施し、クラブの運営主体が委託費等として支出する場合も、当該加算補助の対象とする。</li> <li>放課後児童支援員等、児童の育成支援にあたる職員の人件費は、当該加算補助の対象とならない。ただし、育成支援にあたる常勤職員が事務処理等の事務を行うための超過勤務手当その他これに類する費用については、当該加算補助の対象とする。</li> <li>当該加算補助の補助対象となった運営事務等を行う職員は、条例第10条第2項に定める職員の最低配置基準に含めることはできない。</li> </ul>

別表7（第4条第2項）

項目	賃金改善加算補助
補助対象者	放課後児童支援員、補助員、事務職員等のクラブに勤務する職員（非常勤職員を含み、経営に携わる運営主体の役員である職員を除く）
補助対象経費	(1) 職員の賃金改善に要する経費 (2) 当該賃金改善に伴い増加する法定福利費等の事業主負担分
補助上限額	補助額は、次の計算式により算出された金額とする。 $11,000円 \times 賃金改善対象者数 \times 事業実施月数$ ※賃金改善対象者数とは、賃金改善を行う常勤職員数に、1か月あたりの勤務時間数を就業規則等で定めた常勤職員の1か月あたりの勤務時間数で除した非常勤職員数（常勤換算）を加えたものをいう。
補助要件	<ol style="list-style-type: none"> <li>賃金改善加算補助実施計画書（第13号様式）を作成すること。また、計画の具体的な内容を職員に周知すること。</li> <li>賃金改善加算補助の補助額は、職員の賃金改善及び当該賃金改善に伴い増加する法定福利費等の事業主負担分に全額充てること。</li> <li>賃金改善加算補助の実施に伴う賃金改善が賃上げ効果の継続に資するよう、最低でも賃金改善の合計額の3分の2以上は、基本給又は決まって毎月支払われる手当の引上げにより改善を図ること。</li> <li>賃金改善加算補助の実施により改善を行う賃金項目以外の賃金項目（業績等に応じて変動するものを除く。）の水準を低下させていないこと。</li> <li>賃金改善加算補助の実施により講じた賃金改善の水準を維持すること。</li> </ol>

別表8（第4条第2項）

項目	新型コロナウイルス感染拡大防止加算補助						
補助上限額	<p>当該年度の4月から3月までの支援の単位ごとの対象児童数の平均に応じて、次のとおり支援の単位ごとに補助上限額を決定する。            ※1～3月は12月の実績を適用するものとする。</p> <table border="1"> <thead> <tr> <th>対象児童数</th> <th>補助上限額</th> </tr> </thead> <tbody> <tr> <td>1～19人</td> <td>300,000円</td> </tr> <tr> <td>20～40人</td> <td>400,000円</td> </tr> </tbody> </table>	対象児童数	補助上限額	1～19人	300,000円	20～40人	400,000円
対象児童数	補助上限額						
1～19人	300,000円						
20～40人	400,000円						
補助対象経費	新型コロナウイルスの感染者や濃厚接触者が発生した場合に、職員が感染症対策の徹底を図りながら、事業を継続的に実施していくために必要な経費						

別表9（第4条第2項）

項目	施設賃借料加算Ⅱ
補助対象事業者	条例附則第2条に規定する経過措置が適用され、かつ、平成27年4月1日から令和2年3月31日までの間に分室を確保したことにより、実施要綱第7条に規定する基準を満たしているクラブの運営主体。なお、横浜市放課後児童クラブ事業補助金 施設賃借料加算要綱（令和2年1月30日こ放第960号制定、令和4年2月25日廃止）第5条第1項に基づき、区長が加算決定を行ったクラブの運営主体のみを対象とする。 ※分室とは、面積基準を満たし、かつ、従前の実施場所と同じ集合住宅内等で一体的に運営する目的で新たに確保した実施場所をいう。
補助上限額	月額150,000円を上限に、横浜市放課後児童クラブ事業補助金 施設賃借料加算要綱（令和2年1月30日こ放第960号制定、令和4年2月25日廃止）第5条第1項に基づき、区長が決定した加算額に当該年度の月数を乗じて算定する。
補助対象経費	当該分室先における実施場所を確保するための家賃、間代及び地代 ただし、共益費、光熱水費及び駐車場並びに倉庫等に要する費用は除く。
基準日	当該年度の4月1日 ※年度途中に変更が生じた場合は各月1日時点
留意事項	横浜市放課後児童クラブ事業補助金 施設賃借料加算要綱（令和2年1月30日こ放第960号制定、令和4年2月25日廃止）第5条第1項に基づき、区長が決定した加算の対象となる実施場所に変更が生じた場合は、変更が生じた月の翌月（ただし、変更が生じた日が1日の場合は当月）から当該加算の対象にならない。



別表10（第5条）

項目		事業実施月数が12か月に満たない場合の補助上限額の算定																	
基本 補助	基礎部分 (支援の単位あたり)	当該年度の事業実施月の支援の単位ごとの対象児童数の平均及び当該年度の事業実施月の支援の単位ごとの開所日数の月平均に応じて、下表の金額に「事業実施月数÷12」を乗じた額（一円未満切捨て）を補助上限額とする。																	
		<table border="1"> <thead> <tr> <th rowspan="2">対象児童数</th> <th colspan="2">開所日数（月平均）</th> </tr> <tr> <th>17日以上21日未満</th> <th>21日以上</th> </tr> </thead> <tbody> <tr> <td>10～19人</td> <td>2,351,000円</td> <td>3,551,000円</td> </tr> <tr> <td>20～40人</td> <td>3,099,000円</td> <td>5,102,000円</td> </tr> </tbody> </table>			対象児童数	開所日数（月平均）		17日以上21日未満	21日以上	10～19人	2,351,000円	3,551,000円	20～40人	3,099,000円	5,102,000円				
	対象児童数	開所日数（月平均）																	
17日以上21日未満		21日以上																	
10～19人	2,351,000円	3,551,000円																	
20～40人	3,099,000円	5,102,000円																	
規模調整部分 (1クラブあたり)	当該年度に事業実施月にクラブが運営している最大の支援の単位数及び当該年度の事業実施月の対象児童数の平均に応じて、下表の金額に「事業実施月数÷12」を乗じた額（一円未満切捨て）を補助上限額とする。																		
		<table border="1"> <thead> <tr> <th>支援の単位数</th> <th>対象児童数</th> <th>補助上限額（年額）</th> </tr> </thead> <tbody> <tr> <td>1単位</td> <td>10～19人</td> <td>2,800,000円</td> </tr> <tr> <td>1単位</td> <td>20～40人</td> <td>2,250,000円</td> </tr> <tr> <td>2単位</td> <td>—</td> <td>1,200,000円</td> </tr> <tr> <td>3単位以上</td> <td>—</td> <td>150,000円</td> </tr> </tbody> </table>			支援の単位数	対象児童数	補助上限額（年額）	1単位	10～19人	2,800,000円	1単位	20～40人	2,250,000円	2単位	—	1,200,000円	3単位以上	—	150,000円
支援の単位数	対象児童数	補助上限額（年額）																	
1単位	10～19人	2,800,000円																	
1単位	20～40人	2,250,000円																	
2単位	—	1,200,000円																	
3単位以上	—	150,000円																	
	基本補助の減算 (1クラブあたり)	<p>(1) 施設賃借料に伴う減算 クラブの運営主体が、施設賃借料（施設管理に伴う負担金含む）として貸主に支払っている土地・建物の月額賃料が200,000円に満たない場合は、差額の2分の1の額を事業実施月数分、減算する。なお、一円未満の端数があるときは、その端数金額を切り捨てるものと</p> <p>(2) 対象児童数が10人未満となったことに伴う減算 下記の①又は②に該当するクラブは、基礎部分及び規模調整部分はそれぞれ対象児童数が「10～19人」の欄の金額に「事業実施月数÷12」を乗じた額（一円未満切捨て）とするが、基礎部分と規模調整部分の合計額より290,000円に「事業実施月数÷12」を乗じた額（一円未満切捨て）を減算する。 ①当該年度の4月1日時点でクラブ全体の対象児童数が10人以上であったが、当該年度の事業実施月のクラブ全体の対象児童数の平均が10人未満となったクラブ ②附則（令和4年2月25日こ放第2212号）第3条の適用を受けており、当該年度の事業実施月のクラブ全体の対象児童数の平均も10人未満となったクラブ</p>																	
	開所日数加算補助 (支援の単位あたり)	別表1に基づき算定した補助額																	
	長時間開所加算補助【平日分】 (1クラブあたり)	別表1に基づき算定した補助額に「事業実施月数÷12」を乗じた額（一円未満切捨て） ※別表1で「年間平均時間数」とあるのは、「事業実施月における平均時間数」と読み替える。																	
	長時間開所加算補助【学校休業日等分】 (1クラブあたり)	別表1に基づき算定した補助額に「事業実施月数÷12」を乗じた額（一円未満切捨て） ※別表1で「年間平均時間数」とあるのは、「事業実施月における平均時間数」と読み替える。																	
	小規模激変緩和加算補助 (1クラブあたり)	<p>前年度の4月から3月のクラブ全体の対象児童数の平均が20人以上であったが、当該年度の事業実施月のクラブ全体の対象児童数の平均が19人以下となったクラブ（年度途中で分割を行ったクラブは除く。）について、当該年度の事業実施月の開所日数の月平均に応じて、それぞれ下表の金額に「事業実施月数÷12」を乗じた額（一円未満切捨て）を補助上限額とする。</p> <table border="1"> <thead> <tr> <th>開所日数（月平均）</th> <th>補助上限額（年額）</th> </tr> </thead> <tbody> <tr> <td>17日以上21日未満</td> <td>198,000円</td> </tr> <tr> <td>21日以上</td> <td>1,001,000円</td> </tr> </tbody> </table>			開所日数（月平均）	補助上限額（年額）	17日以上21日未満	198,000円	21日以上	1,001,000円									
開所日数（月平均）	補助上限額（年額）																		
17日以上21日未満	198,000円																		
21日以上	1,001,000円																		
特別 加算	障害児受入推進加算補助 (支援の単位あたり)	別表3に基づき、事業実施月における各月の補助上限額を算定し、その合計額 ※1月から3月について、事業実施月に含まれる場合は、12月実績を適用する。																	
	障害児受入強化推進加算補助 (支援の単位あたり)	別表4に基づき、事業実施月における各月の補助上限額を算定し、その合計額 ※1月から3月について、事業実施月に含まれる場合は、12月実績を適用する。																	
	医療的ケア児受入加算補助 (支援の単位あたり)	別表5に基づき、事業実施月における各月の補助上限額を算定し、その合計額 ※1月から3月について、事業実施月に含まれる場合は、12月実績を適用する。																	
	育成支援体制強化加算補助 (1クラブあたり)	別表6に規定している補助上限額に「事業実施月数÷12」を乗じた額（一円未満切捨て）																	
	放課後児童支援員等キャリアアップ処遇改善費補助 (支援の単位あたり)	キャリアアップ実施細目別表1に基づき算定した加算基準額とキャリアアップ実施細目別表2に基づき算定した補助対象経費を比較して低い額 ※2月から3月について、事業実施月に含まれる場合は、1月実績を適用する。																	
	賃金改善加算補助 (常勤換算1.0人あたり)	別表7に基づき算定した補助額																	
	保護者負担減額相当補助 (1人あたり)	別表1に基づき算定した補助額 ※1月から3月について、事業実施月に含まれる場合は、12月実績を適用する。																	
	人材育成加算補助 (1クラブあたり)	別表1に基づき算定した補助額																	
	常勤職員の産前・産後休暇に伴う代替職員配置経費補助 (1人あたり)	別表1に基づき算定した補助額 ※産前・産後休暇が事業実施月数の期間外に渡る場合は、日割りで補助額を算定する。																	
	新型コロナウイルス感染拡大防止加算補助 (支援の単位あたり)	別表8に基づき算定した補助額に「事業実施月数÷12」を乗じた額（一円未満切捨て） ※「当該年度の4月から3月までの支援の単位ごとの対象児童数の平均」とあるのは、「当該年度の事業実施月の支援の単位ごとの対象児童数の平均」と読み替える。																	
施設賃借料加算Ⅱ (1クラブあたり)	別表9に基づき算定した補助額																		
物価高騰対策加算 (支援の単位あたり)	22,500円に「当該年度の4月から9月までの事業実施月数÷6」を乗じた額及び15,000円に「当該年度の10月から3月までの事業実施月数÷6」を乗じた額（一円未満切捨て）																		

※補助対象経費等は、別表1から別表9に定めるとおりとする。

別表11（第9条第2項）

項目	提出書類
基本補助	
開所日数加算補助	<ul style="list-style-type: none"> <li>・利用児童名簿（第7号様式）</li> <li>・入会申込書及び継続利用申込書の写し</li> </ul>
長時間開所加算補助【平日分】	<ul style="list-style-type: none"> <li>・退会申出書及び休会申出書の写し</li> <li>・賃貸借契約書等の写し</li> </ul>
長時間開所加算補助【学校休業日等分】	<ul style="list-style-type: none"> <li>・放課後児童クラブ月別状況報告書（第8号様式）</li> </ul>
障害児受入推進加算補助	<ul style="list-style-type: none"> <li>・障害児等受入に係る加算補助対象児童名簿（第9号様式）</li> <li>・補助対象児童であることが分かる書類（支援や配慮を要する児童の申立書（第10号様式）及び児童状況書（第10の2号様式）の写し、身体障害者手帳の写し 等）</li> </ul>
障害児受入強化推進加算補助	<ul style="list-style-type: none"> <li>・月別開所状況及び職員配置状況を証する書類</li> <li>・障害児の受入に係る研修の受講状況を証する書類</li> </ul>
医療的ケア児受入加算補助	<ul style="list-style-type: none"> <li>・障害児等受入に係る加算補助対象児童名簿（第9号様式）</li> <li>・医療的ケア児受入加算補助対象児童であることが分かる書類</li> <li>※次の(1)～(4)の書類全て</li> <li>(1) 補助対象児童が通う学校の「医療的ケア実施可否結果通知書」の写し</li> <li>(2) 医療的ケアに関する主治医指示書の写し</li> <li>(3) 保護者からの医療的ケアに関する申込書兼同意書の写し</li> <li>(4) 医療的ケア児受入実施計画書</li> </ul>
放課後児童支援員等キャリアアップ処遇改善費補助	<ul style="list-style-type: none"> <li>・放課後児童支援員等キャリアアップ処遇改善費補助 対象者一覧（第11号様式）</li> <li>・放課後児童支援員等キャリアアップ処遇改善費補助 要件確認表（第12号様式）</li> <li>・放課後児童支援員であることを証する書類（研修受講修了証等） ※申請初年度のみ</li> <li>・職歴を証する書類（勤務実績証明書等）</li> <li>・本市が指定する研修を受講したことを証する書類</li> <li>・キャリアアップ体系を設けていることを証する書類（就業規則等）</li> <li>・賃金が改善されたことを証する書類（前年度の就業規則等）</li> <li>※過年度に提出している場合は省略可</li> </ul>
賃金改善加算補助	<ul style="list-style-type: none"> <li>・賃金改善加算補助実施計画書（第13号様式）※修正がない場合は省略可</li> <li>・賃金改善加算補助賃金改善見込額等内訳書（第14号様式）※修正がない場合は省略可</li> <li>・賃金改善を行っていることを証する書類（改正前及び改正後の給与規定等）</li> <li>※過年度に提出している場合は省略可</li> </ul>
保護者負担減免額相当補助	<ul style="list-style-type: none"> <li>・保護者負担減免額相当補助対象児童名簿（第15号様式）</li> <li>・保護者負担減免額相当補助の対象世帯であることが分かる書類（就学援助申請の審査結果及び支給についてのお知らせの写し、保護証明書の写し、市民税・県民税課税（非課税）証明書の写し 等）</li> </ul>
人材育成加算補助	<ul style="list-style-type: none"> <li>・実施要綱第10条第4項に定める研修計画※7月のみ</li> <li>・人材育成加算補助実施報告書（第16号様式）※1月のみ</li> </ul>
常勤職員の産前・産後休暇に伴う代替職員配置経費補助	<ul style="list-style-type: none"> <li>・常勤職員の産前・産後休暇に伴う代替職員配置経費補助確認書（第17号様式）</li> <li>・常勤職員の出産予定日が分かる書類（母子健康手帳の写し、診断書の写し 等）</li> </ul>
施設賃借料加算Ⅱ	<ul style="list-style-type: none"> <li>・賃貸借契約書等の写し</li> </ul>

年 月 日

(申請先)

横浜市 区長

(申請者)

所在地 :

運営主体名 :

代表者職氏名 :

クラブ名 :

## 横浜市放課後児童クラブ事業費補助金交付申請書

年度横浜市放課後児童クラブ事業費補助金の交付を受けたいので、次のとおり申請します。なお、補助金の交付を受けるにあたっては、横浜市補助金等の交付に関する規則（平成17年11月30日横浜市規則第139号）及び横浜市放課後児童クラブ事業費補助金交付要綱を遵守します。

1 補助対象期間 年 月 日 ~ 年 月 日

2 申請額 円

## 【回ごとの金額内訳】

第1回 受領予定額	第2回 受領予定額	第3回 受領予定額	第4回 受領予定額
円	円	円	円

## 3 算定根拠（要綱別表1～9）

(1) 基本補助

① 基礎部分

	単位1	単位2	単位3	単位4	単位5
対象児童数※1	人	人	人	人	人
開所日数※2	日	日	日	日	日
補助額	円	円	円	円	円

※1 前年度の4～12月実績平均等により算出

※2 前年度の4～12月実績と1～3月見込みの合計等により算出

② 規模調整部分

支援の単位数	単位
クラブ全体の 対象児童数	人
補助額	円

③ 施設賃借料に伴う減算

施設賃借料 (年額)	円
減算額	円

基本補助 合計  
(①+②-③)

円

(2) 開所日数加算補助

	単位1	単位2	単位3	単位4	単位5
開所日数 (250日超過分)	日	日	日	日	日
補助額	円	円	円	円	円

開所日数加算補助 合計	
	円

(3) 長時間開所加算補助【平日分】、長時間開所加算補助【学校休業日等分】

	平日分	学校休業日等分
補助対象時間数	時間	時間
補助額	円	円

長時間開所加算補助 合計	
	円

※前年度の4～12月実績と1～3月見込みの合計等により算出

(4) 障害児受入推進加算補助

	単位1	単位2	単位3	単位4	単位5
該当の有無※					
補助額	円	円	円	円	円

障害児受入推進 加算補助 合計	
	円

※前年度12月の障害児の利用登録実績等により算出

(5) 障害児受入強化推進加算補助

	単位1	単位2	単位3	単位4	単位5
補助対象 児童数※	人	人	人	人	人
補助額	円	円	円	円	円

障害児受入強化 推進加算補助 合計	
	円

※前年度12月の障害児の利用登録人数等により算出

(6) 医療的ケア児受入加算補助

	単位1	単位2	単位3	単位4	単位5
配置					
送迎					
補助額	円	円	円	円	円

医療的ケア児受入 加算補助 合計	
	円

※前年度12月の医療的ケア児に対する看護師等の配置の実績等により算出

(7) 育成支援体制強化加算補助（1クラブあたりの上限：1,444,000円）

育成支援体制強化 加算補助	
	円

(8) 放課後児童支援員等キャリアアップ処遇改善費補助

	単位1	単位2	単位3	単位4	単位5
支援員Ⅰ※	人	人	人	人	人
支援員Ⅱ※	人	人	人	人	人
支援員Ⅲ※	人	人	人	人	人
補助額	円	円	円	円	円

キャリアアップ処遇 改善費補助 合計	
	円

※前年度1月の放課後児童支援員等キャリアアップ処遇改善費補助の対象職員数等により算出

※支援の単位あたりの上限：919,000円



## 運営概要書

クラブ名：

### 1 開所時間

	通常の開所時間						希望者がいる場合の延長時間					
	開始			終了			開始			終了		
平日		時			時			時			時	
土曜日		時			時			時			時	
学校休業日		時			時			時			時	

### 2 年間開所日数（予定）

	単位1	単位2	単位3	単位4	単位5	
年間開所日数		日		日		日

### 3 職員数

	支援員	補助員	その他職員	合計		
常勤職員		人		人		人
非常勤職員		人		人		人

### 4 保護者負担金

児童1人あたり（小学1年生が週5日、午後7時まで利用する場合）の月額  
の保護者負担金を記載してください。

保育料	おやつ代	積立金	その他	合計
円	円	円	円	円

### 5 保護者負担金の減免

減免を実施している項目に☑又は■を記入し、減免額を記載してください。

項目	実施の有無	減免額	説明
生活保護受給世帯	<input type="checkbox"/>		円
市民税所得割非課税世帯	<input type="checkbox"/>		円
就学援助世帯	<input type="checkbox"/>		円
ひとり親世帯	<input type="checkbox"/>		円
兄弟姉妹利用世帯	<input type="checkbox"/>		円
			円
			円
その他	<input type="checkbox"/>		円

6 放課後児童健全育成事業に係る届出状況

専用区画面積	上限人数	定員					合計
		単位1	単位2	単位3	単位4	単位5	
㎡	人	人	人	人	人	人	人

7 年間の活動計画

プログラム・イベント等の活動計画（開催頻度、実施時期や実施内容）を記載してください。

【定期的実施するプログラム】

【季節のイベント、課外活動等】

8 運営者会議・保護者会等の開催予定

	実施回数		開催予定月
運営者会議	年	回	
保護者会等	年	回	

9 添付書類

保護者負担金の金額、開所時間が分かる書類（規定、保護者説明会資料、ちらし等）

## 収支予算書

クラブ名： \_\_\_\_\_

【収入】

(単位：円)

項目	金額	説明
1. 横浜市補助金		
2. 保護者負担金		
(1) 入会金		
(2) 保育料		
(3) おやつ代		
(4) 教材費		
(5) 積立金		
(6) その他（冷暖房費等）		
3. その他収入（寄付金等）		
総収入額		



## 【支出】

（単位：円）

項目	金額	説明
1. 人件費		
(1) 常勤職員給料（基本給・賞与）		
(2) 障害児受入推進加算補助経費		
(3) 障害児受入強化推進加算補助経費		
(4) 医療的ケア児受入加算補助経費		
(5) 育成支援体制強化加算補助経費		
(6) 放課後児童支援員等キャリアアップ処遇改善費補助経費		
(7) 賃金改善加算補助経費		
(8) 新型コロナウイルス感染拡大防止加算補助経費		
(9) その他人件費		
2. 管理運営費		
(1) 医療的ケア児受入加算補助経費		
(2) 育成支援体制強化加算補助経費		
(3) 新型コロナウイルス感染拡大防止加算補助経費		
(4) その他管理運営費		
①保険料		
②会議費		
③光熱水費・通信費		
④備品費・消耗品費		
⑤修繕費		
⑥行事費		
⑦研修費・出張旅費		
⑧防災用品費		
⑨外注費		
⑩その他		
3. 児童処遇費		
(1) おやつ代		
(2) 教材費		
(3) その他		
4. 施設利用料		
(1) 施設賃借料・負担金		
(2) 共益費・駐車場代等		
5. 積立金		
総支出額		

### 資金計画表

クラブ名：

(単位：円)

項目		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	年間計
支出	人件費													
	管理運営費													
	児童処遇費													
	施設利用料													
	積立金													
支出合計(ア)														
収入	横浜市補助金													
	保護者負担金													
	その他													
収入合計(イ)														
差引残高 (イ-ア+前月残高)														/

第 号  
年 月 日

(運営主体名)

(代表者職氏名)

様

横浜市

区長

## 横浜市放課後児童クラブ事業費補助金 交付決定通知書

年 月 日付で申請のあった横浜市放課後児童クラブ事業費補助金については、次のとおり交付することを決定したので、通知します。

1 交付金額 \_\_\_\_\_ 円

## 【交付時期及び交付額内訳】

	交付時期	交付金額
第1回	月	円
第2回	月	円
第3回	月	円
第4回	月	円

2 交付対象クラブ \_\_\_\_\_

3 補助対象期間 \_\_\_\_\_ 年 月 日 ~ \_\_\_\_\_ 年 月 日

## 4 交付条件

- 放課後児童クラブ事業の実施のために使用し、他の用途に流用しないこと。
- 区長が定める期日までに、横浜市放課後児童クラブ事業費補助金執行状況報告書（第6号様式）を提出すること。
- 事業終了後、区長が定める期日までに、横浜市放課後児童クラブ事業費補助金実績報告書（第20号様式）を提出すること。

## 5 留意事項

- 交付金額の確定後、交付済額と確定額の差額を精算します。
- 補助事業に係る収支を明らかにした帳簿を備え、当該収入及び支出についての帳票類は事業年度終了後5か年保管してください。
- 余剰金が生じたときは、速やかに返還してください。
- 虚偽その他不正な手続きによって補助金の交付を受けたときは、補助金の全部又は一部の返還を求める場合があります。
- 必要があると認めるときは、経理等の状況について調査をすることがあります。

## 6 備考

年 月 日

(報告先)  
横浜市 区長

(報告者)  
所在地 :  
運営主体名 :  
代表者職氏名 :  
クラブ名 :

横浜市放課後児童クラブ事業費補助金執行状況報告書 ( 月提出分)

年度放課後児童クラブ事業費補助金について、以下のとおり執行状況を報告します。

1 基本補助

(1) 基礎部分

①対象児童数

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	平均
単位1	人	人	人	人	人	人	人	人	人	人	人	人	人
単位2	人	人	人	人	人	人	人	人	人	人	人	人	人
単位3	人	人	人	人	人	人	人	人	人	人	人	人	人
単位4	人	人	人	人	人	人	人	人	人	人	人	人	人
単位5	人	人	人	人	人	人	人	人	人	人	人	人	人

※1月から3月は12月実績等を適用

②開所日数

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	合計	補助額
単位1	日	日	日	日	日	日	日	日	日	日	日	日	日	円
単位2	日	日	日	日	日	日	日	日	日	日	日	日	日	円
単位3	日	日	日	日	日	日	日	日	日	日	日	日	日	円
単位4	日	日	日	日	日	日	日	日	日	日	日	日	日	円
単位5	日	日	日	日	日	日	日	日	日	日	日	日	日	円

※1月から3月は、月の全日から実施要綱第6条第1項各号に規定する日を除いた日数等を適用

(2) 規模調整部分

支援の単位数	単位	補助額
クラブ全体の対象児童数	人	円

(3) 基本補助の減算

①施設賃借料に伴う減算

施設賃借料 (年額・予定)	円	減算額
		円

②クラブ全体の対象児童数が10人未満の場合の減算

クラブ全体の対象児童数(再掲)	人	減算額
		円

補助額 ((1)+(2)-(3))
円

2 開所日数加算補助

	単位1	単位2	単位3	単位4	単位5	補助額
開所日数 (250日超過分)	日	日	日	日	日	
補助額	円	円	円	円	円	円

※「1 基本補助」の「(1) 基礎部分」の「②開所日数」の「合計」欄の日数から250日を差し引いた日数

3 長時間開所加算補助【平日分】

(単位：時間)

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	平均
月平均時間数	h	h	h	h	h	h	h	h	h	h	h	h	h

※1月から3月は12月実績等を適用

補助額
円

4 長時間開所加算補助【学校休業日等分】

(単位：時間)

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	平均
月平均時間数	h	h	h	h	h	h	h	h	h	h	h	h	h

※1月から3月は12月実績等を適用

補助額
円

5 小規模激変加算補助

前年度のクラブ全体の対象児童数	人
クラブ全体の対象児童数(再掲)	人
クラブの開所日数	日

補助額
円

6 障害児受入推進加算補助

支援の単位	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	補助額
1	対象月												円
	日数	日	日	日	日	日	日	日	日	日	日	日	
2	対象月												円
	日数	日	日	日	日	日	日	日	日	日	日	日	
3	対象月												円
	日数	日	日	日	日	日	日	日	日	日	日	日	
4	対象月												円
	日数	日	日	日	日	日	日	日	日	日	日	日	
5	対象月												円
	日数	日	日	日	日	日	日	日	日	日	日	日	

※日数欄には、条例第10条第2項で定める「職員の最低配置基準」より1名以上職員を加配した日数を記載

※1月から3月は12月実績を適用

補助額
円

7 障害児受入強化推進加算補助

支援の単位	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	補助額
1	障害児数	人	人	人	人	人	人	人	人	人	人	人	円
	強化①	日	日	日	日	日	日	日	日	日	日	日	
	強化②	日	日	日	日	日	日	日	日	日	日	日	
	強化③	日	日	日	日	日	日	日	日	日	日	日	
2	障害児数	人	人	人	人	人	人	人	人	人	人	人	円
	強化①	日	日	日	日	日	日	日	日	日	日	日	
	強化②	日	日	日	日	日	日	日	日	日	日	日	
	強化③	日	日	日	日	日	日	日	日	日	日	日	
3	障害児数	人	人	人	人	人	人	人	人	人	人	人	円
	強化①	日	日	日	日	日	日	日	日	日	日	日	
	強化②	日	日	日	日	日	日	日	日	日	日	日	
	強化③	日	日	日	日	日	日	日	日	日	日	日	
4	障害児数	人	人	人	人	人	人	人	人	人	人	人	円
	強化①	日	日	日	日	日	日	日	日	日	日	日	
	強化②	日	日	日	日	日	日	日	日	日	日	日	
	強化③	日	日	日	日	日	日	日	日	日	日	日	
5	障害児数	人	人	人	人	人	人	人	人	人	人	人	円
	強化①	日	日	日	日	日	日	日	日	日	日	日	
	強化②	日	日	日	日	日	日	日	日	日	日	日	
	強化③	日	日	日	日	日	日	日	日	日	日	日	

※強化①、強化②、強化③の欄には、それぞれの区分ごとに職員を追加配置した日数を記載

※1月から3月は12月実績を適用

補助額
円

8 医療的ケア児受入加算補助

支援の単位	医療的ケア児の利用実績（看護師等を配置していた月のみ○を選択）												補助額	
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月		
1	配置													円
	送迎													
2	配置													円
	送迎													
3	配置													円
	送迎													
4	配置													円
	送迎													
5	配置													円
	送迎													

※1月から3月は12月実績を適用

補助額	円
-----	---

9 育成支援体制強化加算補助

補助額	円
-----	---

10 放課後児童支援員等キャリアアップ処遇改善費補助

	単位1	単位2	単位3	単位4	単位5
補助額	円	円	円	円	円

補助額	円
-----	---

11 賃金改善加算補助

補助額	円
-----	---

12 保護者負担減免額相当補助

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	合計
減免対象児童数	人	人	人	人	人	人	人	人	人	人	人	人	人

※1月から3月は12月実績を適用

補助額	円
-----	---

13 人材育成加算補助

	常勤職員	非常勤職員
対象職員数	人	人

補助額	円
-----	---

14 常勤職員の産前・産後休暇に伴う代替職員配置経費補助

補助額	円
-----	---

15 新型コロナウイルス感染拡大防止加算補助

	単位1	単位2	単位3	単位4	単位5
対象児童数（再掲）	人	人	人	人	人
補助額	円	円	円	円	円

補助額	円
-----	---

16 施設賃借料加算Ⅱ

加算決定額（月額）	円
-----------	---

補助額	円
-----	---

17 物価高騰対策加算

補助額	円
-----	---

18 その他（移転支援加算の適用を受けている場合等）

補助額	円
-----	---

合計額(A)	円
交付決定済額(B)	円
差額(A-B)	円

## 19 添付書類 該当する項目に☑又は■を記入してください。

- (1) 利用児童名簿（第7号様式）
- (2) 入会申込書及び継続利用申込書の写し
- (3) 退会申出書及び休会申出書の写し
- (4) 賃貸借契約書等の写し
- (5) 放課後児童クラブ月別状況報告書（第8号様式）
- (6) 障害児等受入に係る加算補助対象児童名簿（第9号様式）
- (7) 補助対象児童であることがわかる書類（支援や配慮を要する児童の申立書（第10号様式）及び児童状況書（第10の2号様式）の写し等）
- (8) 月別開所状況及び職員配置状況を証する書類
- (9) 補助対象児童が通う学校学校の「医療的ケア実施可否結果通知書」の写し
- (10) 医療的ケア実施に関する主治医指示書の写し
- (11) 保護者からの医療的ケアに関する申込書兼同意書の写し
- (12) 医療的ケア児受入実施計画書
- (13) 障害児の受入に係る研修の受講状況を証する書類
- (14) 放課後児童支援員等キャリアアップ処遇改善費補助 対象者一覧（第11号様式）
- (15) 放課後児童支援員等キャリアアップ処遇改善費補助 要件確認表（第12号様式）
- (16) 放課後児童支援員であることを証する書類（研修受講修了証等）
- (17) 職歴を証する書類（勤務実績証明書等）
- (18) 本市が指定する研修を受講したことを証する書類
- (19) キャリアアップ体系を設けていることを証する書類（就業規則等）
- (20) 賃金が改善されたことを証する書類（前年度の就業規則等）
- (21) 賃金改善加算補助実施計画書（第13号様式）
- (22) 賃金改善加算補助賃金改善見込額等内訳書（第14号様式）
- (23) 賃金改善を行っていることを証する書類（改正前及び改正後の給与規定等）
- (24) 保護者負担減免額相当補助対象児童名簿（第15号様式）
- (25) 保護者負担減免額相当補助の対象世帯であることがわかる書類（保護証明書、市民税・県民税課税（非課税）証明書の写し等）
- (26) 実施要綱第10条第4項に定める研修計画
- (27) 人材育成加算補助実施報告書（第16号様式）
- (28) 常勤職員の産前・産後休暇に伴う代替職員配置経費補助確認書（第17号様式）
- (29) 常勤職員の出産予定日がわかる書類（母子健康手帳の写し、診断書の写し等）
- (30) その他（ )

利用児童名簿（第 四半期分）

クラブ名：

支援の単位：

No.	小学校名	学年	児童氏名	利用日数	対象児童数		
					月	月	月
1				日/5日	人	人	人
2				日/5日	人	人	人
3				日/5日	人	人	人
4				日/5日	人	人	人
5				日/5日	人	人	人
6				日/5日	人	人	人
7				日/5日	人	人	人
8				日/5日	人	人	人
9				日/5日	人	人	人
10				日/5日	人	人	人
11				日/5日	人	人	人
12				日/5日	人	人	人
13				日/5日	人	人	人
14				日/5日	人	人	人
15				日/5日	人	人	人
16				日/5日	人	人	人
17				日/5日	人	人	人
18				日/5日	人	人	人
19				日/5日	人	人	人
20				日/5日	人	人	人
21				日/5日	人	人	人
22				日/5日	人	人	人
23				日/5日	人	人	人
24				日/5日	人	人	人
25				日/5日	人	人	人
26				日/5日	人	人	人
27				日/5日	人	人	人
28				日/5日	人	人	人
29				日/5日	人	人	人
30				日/5日	人	人	人



No.	小学校名	学年	児童氏名	利用日数	対象児童数		
					月	月	月
31				日/5日	人	人	人
32				日/5日	人	人	人
33				日/5日	人	人	人
34				日/5日	人	人	人
35				日/5日	人	人	人
36				日/5日	人	人	人
37				日/5日	人	人	人
38				日/5日	人	人	人
39				日/5日	人	人	人
40				日/5日	人	人	人
41				日/5日	人	人	人
42				日/5日	人	人	人
43				日/5日	人	人	人
44				日/5日	人	人	人
45				日/5日	人	人	人
46				日/5日	人	人	人
47				日/5日	人	人	人
48				日/5日	人	人	人
49				日/5日	人	人	人
50				日/5日	人	人	人
51				日/5日	人	人	人
52				日/5日	人	人	人
53				日/5日	人	人	人
54				日/5日	人	人	人
55				日/5日	人	人	人
56				日/5日	人	人	人
57				日/5日	人	人	人
58				日/5日	人	人	人
59				日/5日	人	人	人
60				日/5日	人	人	人
対象児童数 合計					人	人	人

放課後児童クラブ月別状況報告書（ 年 月分）

クラブ名：

日	曜日	開所日等の区分	クラブ全体					支援の単位1					支援の単位2					支援の単位3					支援の単位4					支援の単位5																		
			長時間開所加算対象			利用児童数	やむを得ない閉所	開所時間		確認欄 開所時間 職員配置	利用児童数	やむを得ない閉所	開所時間		確認欄 開所時間 職員配置	利用児童数	やむを得ない閉所	開所時間		確認欄 開所時間 職員配置	利用児童数	やむを得ない閉所	開所時間		確認欄 開所時間 職員配置	利用児童数	やむを得ない閉所	開所時間		確認欄 開所時間 職員配置	利用児童数	やむを得ない閉所														
			開始	終了	時間数			開始	終了				開始	終了				開始	終了				開始	終了				開始	終了				開始	終了	開始	終了	開始	終了	開始	終了	開始	終了	開始	終了	開始	終了
1						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
2						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
3						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
4						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
5						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
6						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
7						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
8						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
9						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
10						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
11						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
12						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
13						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
14						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
15						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
16						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
17						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
18						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
19						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
20						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
21						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
22						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
23						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
24						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
25						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
26						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
27						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
28						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
29						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
30						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
31						人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人	:	:			人					
			合計	人				合計	人				合計	人				合計	人				合計	人				合計	人				合計	人				合計	人							

【特記事項記入欄】

【集計欄】

◆区分ごとの日数

平日	日
土曜日	日
学校休業日	日
日曜日・祝日等	日
閉所日	日
合計	日

◆長時間開所加算月平均時間数

	平日分	学校休業日等分
対象時間数合計	時間	時間
日数	日	日
月平均時間数	時間	時間

◆延べ利用児童数

延べ利用児童数	人
---------	---

◆開所日数、閉所日数

	単位1	単位2	単位3	単位4	単位5
開所日数	日	日	日	日	日
閉所日数	日	日	日	日	日

◆土曜日等開所時間短縮平均時間数

対象時間数合計	時間
日数	日
月平均時間数	時間



支援や配慮を要する児童の申立書

年 月 日

(提出先)

横浜市

区長

(提出者)

所在地 :

運営主体名 :

代表者職氏名 :

クラブ名 :

横浜市放課後児童クラブ事業費補助金交付要綱第9条第2項に基づき、支援や配慮を要する児童であることを申し立てます。

児童氏名	
学校名	
学年	
入所年月日	

【保護者確認欄】

放課後児童クラブから、次の①と②について説明を受け、了解しました。

- ①放課後児童クラブの運営主体が、支援や配慮を要する児童の申立てを行うこと
- ②放課後児童クラブにおける児童の状況及び児童への支援や配慮の内容

年 月 日

保護者氏名（自署）

\_\_\_\_\_

## 児 童 状 況 書

児童氏名		クラブ名	
学校名		学年	

1 次の項目について、該当する番号に☑又は■を記入してください。

<input type="checkbox"/> 1 状況や場面に応じた行動ができない。 <input type="checkbox"/> 2 静かに遊んだり余暇活動を行ったりすることができない。 <input type="checkbox"/> 3 質問が終わる前に出し抜けに答えてしまう。 <input type="checkbox"/> 4 順番を待つことが出来ない。（一番になりたがる、非常に勝敗にこだわる） <input type="checkbox"/> 5 他人を妨害し、邪魔をする。（他人の会話やゲームなどに干渉する） <input type="checkbox"/> 6 特定のこと、ものなどに強度のこだわりを持つ。 <input type="checkbox"/> 7 突然興奮することがあり、乱暴な言葉遣いや振る舞いをする。 <input type="checkbox"/> 8 全体のルールを受け入れられず、友達との遊びに入れない。 <input type="checkbox"/> 9 その他（ ）
--

2 該当する項目について、どのような支援や配慮が必要か記載してください。

（具体的な状況、支援や配慮の内容を記載）

<具体的な状況の詳細>          <支援や配慮の内容>
---

3 保護者への説明状況

--

記入者	職名	氏名
-----	----	----

## 【学校等関係機関確認欄】

上記の記載内容について放課後児童クラブから説明を受け、当該児童が、放課後児童クラブを利用するにあたり、支援や配慮が必要であることを確認しました。		
年 月 日		
記入者	所属	職氏名

放課後児童支援員等キャリアアップ処遇改善費補助 対象者一覧（ 月提出分）

該当する方に☑又は■を記入

新規  継続

クラブ名： \_\_\_\_\_

支援の単位： \_\_\_\_\_

(単位：円)

No.	職員名	事由 (※)												上段：補助金算定基準額【A】 下段：補助対象経費上限額【B】	
		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月		
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
合計															

補助額（補助金算定基準額合計と補助上限額を比較して少ない方の額） \_\_\_\_\_ 円

- ※「事由」欄は以下に基づいて記入すること。
- ① 支援員Ⅰ 放課後児童支援員
  - ② 支援員Ⅱ 経年数が概ね5年以上の放課後児童支援員で、キャリアアップ研修を受講した者
  - ③ 支援員Ⅲ 経年数が概ね10年以上の放課後児童支援員で、キャリアアップ研修を受講した事業所長的立場にある者
  - ④ 補助員Ⅰ 補助員
  - ⑤ 補助員Ⅱ 経年数が概ね5年以上の補助員で、キャリアアップ研修を受講した者

放課後児童支援員等キャリアアップ処遇改善費補助 要件確認表

該当する方に☑又は■を記入

<input type="checkbox"/> 新規	<input type="checkbox"/> 継続
-----------------------------	-----------------------------

クラブ名：

支援の単位：

No.	職員名	該当要件	新規・変更 (※1)	キャリアアップ研修 要受講者 (※2)	経験年数（ 年4月1日現在）						給与（※3）				賃金改善項目		
					現在の事業所		過去に勤務していた事業所		合計		前年度給与		今年度給与		基本給	手当	賞与
1			<input type="checkbox"/>		年	か月	年	か月	年	か月							
2			<input type="checkbox"/>		年	か月	年	か月	年	か月							
3			<input type="checkbox"/>		年	か月	年	か月	年	か月							
4			<input type="checkbox"/>		年	か月	年	か月	年	か月							
5			<input type="checkbox"/>		年	か月	年	か月	年	か月							
6			<input type="checkbox"/>		年	か月	年	か月	年	か月							
7			<input type="checkbox"/>		年	か月	年	か月	年	か月							
8			<input type="checkbox"/>		年	か月	年	か月	年	か月							
9			<input type="checkbox"/>		年	か月	年	か月	年	か月							
10			<input type="checkbox"/>		年	か月	年	か月	年	か月							

※1 新たに支援員Ⅱ、支援員Ⅲ、補助員Ⅱ（要件の変更を含む）になった職員は☑又は■を記入し、職歴を証する書類を添付すること。

※2 支援員Ⅱ、支援員Ⅲ及び補助員Ⅱに該当する職員は、当該年度中に横浜市が指定する研修（キャリアアップ研修）を受講すること。

※3 給与欄は新たにキャリアアップ処遇改善費補助を申請するクラブのみ記入すること。

## 賃金改善加算補助 実施計画書

クラブ名：

## 1. 補助額

① 事業実施期間	令和 年 月 ~ 令和 年 月
② 補助基準額	円

## 2. 賃金改善見込額

③ 賃金改善見込額	円
④ うち、基本給又は決まって毎月支払う手当による賃金改善見込額	円
⑤ 賃金改善に伴い増加する法定福利費等の事業主負担分	円
⑥ 賃金改善見込額合計(③+⑤)	円

## 3. 要件の確認

※合致しない要件がある場合は、補助対象外です。

賃金改善額の2/3以上が基本給又は決まって毎月支払う手当によって改善されていること(③×2/3≤④)	
賃金改善額合計(⑥)が補助基準額(②)以上となっていること	
本加算補助による賃金改善に係る計画の具体的内容を職員に周知していること	
本加算補助の実施により講じた賃金改善の水準を維持すること	

上記の内容について、全ての職員に対し周知をした上で、提出していることを証明いたします。

年 月 日

運営主体名：

代表者職氏名：



## 賃金改善加算補助 賃金改善見込額等内訳書

クラブ名:

就業規則等で定めた常勤職員の1か月あたりの勤務時間数	
時間	

NO.	職員名	職種	常勤・非常勤の別	新規・変更 (※1)	補助単価 (月額)	常勤職員数	非常勤職員数(常勤換算)		令和 年 月～令和 年 月分					賃金改善に伴う法定福利費等の事業主負担分の増分	1か月あたりの平均賃金改善見込額	備考	
							1か月あたりの勤務時間数	常勤換算値	賃金改善実施月数	補助基準額	賃金改善見込額		基本給又は決まって毎月支払う手当				その他
											0円	0円					
1				<input type="checkbox"/>	11,000円												
2				<input type="checkbox"/>	11,000円												
3				<input type="checkbox"/>	11,000円												
4				<input type="checkbox"/>	11,000円												
5				<input type="checkbox"/>	11,000円												
6				<input type="checkbox"/>	11,000円												
7				<input type="checkbox"/>	11,000円												
8				<input type="checkbox"/>	11,000円												
9				<input type="checkbox"/>	11,000円												
10				<input type="checkbox"/>	11,000円												
11				<input type="checkbox"/>	11,000円												
12				<input type="checkbox"/>	11,000円												
13				<input type="checkbox"/>	11,000円												
14				<input type="checkbox"/>	11,000円												
15				<input type="checkbox"/>	11,000円												
16				<input type="checkbox"/>	11,000円												
17				<input type="checkbox"/>	11,000円												
18				<input type="checkbox"/>	11,000円												
19				<input type="checkbox"/>	11,000円												
20				<input type="checkbox"/>	11,000円												
21				<input type="checkbox"/>	11,000円												
22				<input type="checkbox"/>	11,000円												
23				<input type="checkbox"/>	11,000円												
24				<input type="checkbox"/>	11,000円												
25				<input type="checkbox"/>	11,000円												
26				<input type="checkbox"/>	11,000円												
27				<input type="checkbox"/>	11,000円												
28				<input type="checkbox"/>	11,000円												
29				<input type="checkbox"/>	11,000円												
30				<input type="checkbox"/>	11,000円												
合計						0.0人		0.0人	0か月	0円	0円	0円	0円				

※1 新たに賃金改善を行う者(賃金改善額の変更を含む)は☑又は■を記入し、賃金改善を行っていることを証する書類を添付すること。  
 ※2 クラブで勤務する職員のうち、賃金改善を行う者(職種問わず、非常勤を含み、経営に携わる法人の役員を除く。)を記載すること。  
 ※3 行が足りない場合は適宜追加すること。

保護者負担減免額相当補助対象児童名簿（ 月提出分）

クラブ名： 

1. 利用料減免状況

No.	児童氏名	減免事由※									
		4月	5月	6月	7月	8月	9月	10月	11月	12月	
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
減免対象児童数											

※減免事由の欄は、以下から選択し、記入すること。

- ① 「横浜市の就学援助を受けている世帯」に該当
- ② 「生活保護受給世帯」に該当
- ③ 「市民税所得割非課税世帯」に該当

2. 添付書類

- 「就学援助申請の審査結果及び支給についてのお知らせ」の写し、「私立学校等就学奨励費申請の審査結果及び支給についてのお知らせ」の写し又は「私立学校等就学奨励費の認定審査結果のお知らせ」の写し（減免事由①の場合）
- 「市民税・県民税課税（非課税）証明書」（写し）、「市民税・県民税税額決定・納税通知書」の写し又は「給与所得等に係る市民税・県民税特別徴収税額決定通知書」の写し（減免事由③の場合） ※4～5月は前年度分、6～12月は当該年度分の証明書等を添付すること。
- 「保護証明書」（写し）又は「生活保護費支給証」の写し（減免事由②の場合）

## 人材育成加算補助実施報告書

クラブ名： \_\_\_\_\_

1 運営主体主催の研修の実施日及び内容

	研修名	研修内容	研修時間	研修実施日
1				
2				
3				
4				
5				

2 人材育成加算補助の補助対象となる研修の受講者名簿

	氏名	常勤職員・非常勤職員の別
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		

	合計
常勤職員	0
非常勤職員	0

※行が足りない場合は適宜追加すること。

## 常勤職員の産前・産後休暇に伴う代替職員配置経費補助確認書

クラブ名： \_\_\_\_\_

### 1 産前・産後休暇取得職員

(1) 氏名	
(2) 出産予定日	年 月 日
(3) 休暇付与予定期間	年 月 日 ~ 年 月 日

### 2 補助額

\_\_\_\_\_ 円

### 3 添付書類

母子健康手帳の写し 又は 診断書の写し

### 4 留意事項

- (1) 運営主体が常勤職員の産前・産後休暇期間の給与を支給していない場合は、当該補助金を取消し、返還を求めることがあります。
- (2) 産前・産後休暇が次年度に渡る場合は、日割りで補助額を積算します。

年 月 日

(申請先)  
横浜市 区長

(申請者)  
所在地：  
運営主体名：  
代表者職氏名：  
クラブ名：

### 横浜市放課後児童クラブ事業費補助金変更交付申請書

年 月 日に交付決定を受けた横浜市放課後児童クラブ事業費補助金について、交付金額の変更を申請します。

1 補助対象期間 年 月 日 ~ 年 月 日

2 補助金変更交付申請額 円

(1) 交付決定済額 円

(2) 差引（追加交付金額） 円

3 変更交付申請額内訳

項目	交付決定済額【A】	変更交付申請額【B】	差引(【B】-【A】) (追加交付金額)
基本補助	円	円	円
開所日数加算補助	円	円	円
長時間開所加算補助【平日分】	円	円	円
長時間開所加算補助【学校休業日等分】	円	円	円
小規模激変緩和加算補助	円	円	円
障害児受入推進加算補助	円	円	円
障害児受入強化推進加算補助	円	円	円
医療的ケア児受入加算補助	円	円	円
育成支援体制強化加算補助	円	円	円
放課後児童支援員等キャリアアップ処遇改善費補助	円	円	円
賃金改善加算補助	円	円	円
保護者負担減免額相当補助	円	円	円
人材育成加算補助	円	円	円
常勤職員の産前・産後休暇に伴う代替職員配置経費補助	円	円	円
新型コロナウイルス感染拡大防止加算補助	円	円	円
施設賃借料加算Ⅱ	円	円	円
物価高騰対策加算	円	円	円
その他 ( )	円	円	円
合計	円	円	円

第 号  
年 月 日

(運営主体名)

(代表者職氏名) 様

横浜市 区長

## 横浜市放課後児童クラブ事業費補助金 変更交付決定通知書

年度横浜市放課後児童クラブ事業費補助金については、次のとおり変更して交付します。

1 変更交付決定額 \_\_\_\_\_ 円

(1) 交付決定済額 \_\_\_\_\_ 円

(2) 追加交付額 \_\_\_\_\_ 円

## 【交付時期及び交付額内訳】

	交付時期	交付金額
第 1 回	月	円
第 2 回	月	円
第 3 回	月	円
第 4 回	月	円
その他	月	円

2 交付対象クラブ \_\_\_\_\_

3 補助対象期間 \_\_\_\_\_ 年 月 日 ~ \_\_\_\_\_ 年 月 日

## 4 交付条件

- (1) 放課後児童クラブ事業の実施のために使用し、他の用途に流用しないこと。
- (2) 事業終了後、区長が定める期日までに、横浜市放課後児童クラブ事業費補助金実績報告書（第 20 号様式）を提出すること。

## 5 留意事項

- (1) 交付金額の確定後、交付済額と確定額の差額を精算します。
- (2) 補助事業に係る収支を明らかにした帳簿を備え、当該収入及び支出についての帳票類は事業年度終了後 5 年保管してください。
- (3) 余剰金が生じたときは、速やかに返還してください。
- (4) 虚偽その他不正な手続きによって補助金の交付を受けたときは、補助金の全部又は一部の返還を求められます。
- (5) 必要があると認めるときは、経理等の状況について調査をすることがあります。

## 6 備考

年 月 日

(報告先)  
横浜市 区長

(報告者)  
所在地：  
運営主体名：  
代表者職氏名：  
クラブ名：

## 年度 横浜市放課後児童クラブ事業費補助金実績報告書

横浜市放課後児童クラブ事業費補助金に関する実績について、次のとおり関係書類を添えて報告します。

## 1 収支報告

(1) 総収入額 円 (うち補助金交付額 (A) 円)  
(2) 総支出額 円 (うち戻入額 (B) 円)  
(3) 補助金確定額 (A - B) 円

## 2 会計監査

## 【会計監査記入欄】

会計監査を実施した結果、会計帳簿の記載は正確で、関係書類ならびに会計処理は、すべて適正であることを認めます。

年 月 日

会計監査 (自署)

(自署)

## 3 添付書類

該当する項目の確認欄に  又は  を記入してください。

	添付書類	確認欄
(1)	基本事業費補助額算定書 (第21号様式)	<input type="checkbox"/>
(2)	職員別、補助項目別の当該年度の給与額が分かる書類	<input type="checkbox"/>
(3)	領収書の写し (1件あたりの支払金額が10万円以上のもの)	<input type="checkbox"/>
(4)	見積書の写し (1件あたりの支払金額が100万円以上の場合に徴収した、2社以上の見積書の写し)	<input type="checkbox"/>
(5)	積立金がある場合は、金額の分かる通帳等の写し	<input type="checkbox"/>
(6)	障害児受入に係る補助対象経費等報告書 (第22号様式)	<input type="checkbox"/>
(7)	医療的ケア児受入加算補助対象経費等報告書 (第23号様式)	<input type="checkbox"/>
(8)	育成支援体制強化加算補助対象経費等報告書 (第24号様式)	<input type="checkbox"/>
(9)	放課後児童支援員等キャリアアップ処遇改善費補助対象経費積算書 (第25号様式)	<input type="checkbox"/>
(10)	賃金改善加算補助実施報告書 (第26号様式)	<input type="checkbox"/>
(11)	賃金改善加算補助賃金改善額等内訳書 (第27号様式)	<input type="checkbox"/>
(12)	新型コロナウイルス感染拡大防止加算補助対象経費等報告書 (第28号様式)	<input type="checkbox"/>
(13)	その他区長が必要と認める書類 ( )	<input type="checkbox"/>

作成担当者：

連絡先：

## 【戻入額内訳】

項目	戻入額
①基本事業費※	円
②次年度繰越額超過分	円
③障害児受入推進加算補助	円
④障害児受入強化推進加算補助	円
⑤医療的ケア児受入加算補助	円
⑥育成支援体制強化加算補助	円
⑦放課後児童支援員等キャリアアップ処遇改善費補助	円
⑧貸金改善加算補助	円
⑨新型コロナウイルス感染拡大防止加算	円
⑩施設賃借料加算Ⅱ	円
⑪執行状況報告（1月提出分）による戻入	円
⑫その他（ ）	円
戻入額合計	円

※「①基本事業費」の戻入額には、「②次年度繰越額超過分」の戻入額は含めないこと。

## 【総収入額内訳】

項目	金額	説明
1. 前年度繰越金	円	
2. 横浜市補助金	円	<b>【受領日及び金額】</b> 第1回（ 年 月 日）： 円 第2回（ 年 月 日）： 円 第3回（ 年 月 日）： 円 第4回（ 年 月 日）： 円 その他（ 年 月 日）： 円 その他（ 年 月 日）： 円
3. 保護者負担金	円	
(1) 入会金	円	
(2) 保育料	円	
(3) おやつ代	円	
(4) 教材費	円	
(5) 積立金	円	
(6) その他(冷暖房費等)	円	
4. その他収入 （寄付金・バザー収益等）	円	
総収入額（1 + 2 + 3 + 4）	円	



## 【総支出額内訳】

項目	金額	説明
1. 人件費	円	
(1) 常勤職員人件費	円	
(2) 障害児受入推進加算補助経費	円	
(3) 障害児受入強化推進加算補助経費	円	
(4) 医療的ケア児受入加算補助経費	円	
(5) 育成支援体制強化加算補助経費	円	
(6) 放課後児童支援員等キャリアアップ処遇改善費補助経費	円	
(7) 賃金改善加算補助経費	円	
(8) 新型コロナウイルス感染拡大防止加算補助経費	円	
(9) その他人件費	円	
2. 管理運営費	円	
(1) 医療的ケア児受入加算補助経費	円	
(2) 育成支援体制強化加算補助経費	円	
(3) 新型コロナウイルス感染拡大防止加算補助経費	円	
(4) その他管理運営費	円	
①保険料	円	
②会議費	円	
③光熱水費・通信費	円	
④備品費・消耗品費	円	
⑤修繕費	円	
⑥行事費	円	
⑦研修費・出張旅費	円	
⑧防災用品費	円	
⑨外注費	円	
⑩その他	円	
3. 児童処遇費	円	
(1) おやつ代	円	
(2) 教材費	円	
(3) その他	円	
4. 施設利用料	円	
(1) 施設賃借料・負担金	円	
(2) 共益費・駐車場代等	円	
5. その他	円	
6. 積立金	円	使用目的：
7. 次年度繰越金	円	上限金額((1 + 2 + 3 + 4 + 5) × 10%)：
8. 戻入額	円	
支出合計(1 + 2 + 3 + 4 + 5 + 6 + 7 + 8)	円	



5 小規模激変加算補助

前年度のクラブ 全体の対象児童数		人
クラブ全体の 対象児童数(再掲)		人
クラブの開所日数		日

補助額
円

6 基本事業費 補助額算定

	執行状況報告(1月)にて算定 された補助額	基本事業費補助額算定書にて 算定された補助額	戻入額
基本補助	円	円	円
開所日数加算補助	円	円	円
長時間開所加算補助【平日分】	円	円	円
長時間開所加算補助【学校休業日等 分】	円	円	円
小規模激変緩和加算補助	円	円	円
合 計	円	円	円

※基本補助の「繰越金の上限超過に伴う減算」の減算額については、横浜市放課後児童クラブ事業費補助金実績報告書（第20号様式）にて算定を行う。

※小規模激変緩和加算補助のみ、「基本事業費補助額算定書にて算定された補助額」が「執行状況報告(1月)にて算定された補助額」を上回った場合、「基本事業費補助額算定書にて算定された補助額」を適用するものとする。

7 添付書類 該当する項目の確認欄に  又は  を記入してください。

- (1) 利用児童名簿（第7号様式）
- (2) 入会申込書及び継続利用申込書の写し
- (3) 退会申出書及び休会申出書の写し
- (4) 賃貸借契約書等の写し
- (5) 放課後児童クラブ月別状況報告書（第8号様式）

## 障害児受入に係る補助対象経費等報告書

クラブ名： \_\_\_\_\_

## 1 障害児受入推進加算補助

## (1) 補助対象職員

No.	氏名	属する 支援の単位	非常勤職員である こと	研修受講済である こと	補助対象経費
1			<input type="checkbox"/>	<input type="checkbox"/>	円
2			<input type="checkbox"/>	<input type="checkbox"/>	円
3			<input type="checkbox"/>	<input type="checkbox"/>	円
4			<input type="checkbox"/>	<input type="checkbox"/>	円
5			<input type="checkbox"/>	<input type="checkbox"/>	円
6			<input type="checkbox"/>	<input type="checkbox"/>	円
7			<input type="checkbox"/>	<input type="checkbox"/>	円
8			<input type="checkbox"/>	<input type="checkbox"/>	円
9			<input type="checkbox"/>	<input type="checkbox"/>	円
10			<input type="checkbox"/>	<input type="checkbox"/>	円

## (2) 対象経費合計

	単位 1	単位 2	単位 3	単位 4	単位 5	合計
対象経費	円	円	円	円	円	
補助上限額※ 1	円	円	円	円	円	
補助額※ 2	円	円	円	円	円	円
戻入額※ 3	円	円	円	円	円	円

※ 1 執行状況報告書（1月提出分）から転記

※ 2 補助額は支援の単位ごとの対象経費と補助上限額を比較して低い金額

※ 3 対象経費が補助上限額を下回る場合、その差額

## 2 障害児受入強化推進加算

## (1) 補助対象職員

No.	氏名	属する 支援の単位	非常勤職員である こと	研修受講済である こと	補助対象経費
1			<input type="checkbox"/>	<input type="checkbox"/>	円
2			<input type="checkbox"/>	<input type="checkbox"/>	円
3			<input type="checkbox"/>	<input type="checkbox"/>	円
4			<input type="checkbox"/>	<input type="checkbox"/>	円
5			<input type="checkbox"/>	<input type="checkbox"/>	円
6			<input type="checkbox"/>	<input type="checkbox"/>	円
7			<input type="checkbox"/>	<input type="checkbox"/>	円
8			<input type="checkbox"/>	<input type="checkbox"/>	円
9			<input type="checkbox"/>	<input type="checkbox"/>	円
10			<input type="checkbox"/>	<input type="checkbox"/>	円

## (2) 対象経費合計

	単位 1	単位 2	単位 3	単位 4	単位 5	合計
対象経費	円	円	円	円	円	
補助上限額※ 1	円	円	円	円	円	
強化①	円	円	円	円	円	
強化②	円	円	円	円	円	
強化③	円	円	円	円	円	
補助額※ 2	円	円	円	円	円	円
戻入額※ 3	円	円	円	円	円	円

※ 1 執行状況報告書（1月提出分）から転記

※ 2 補助額は支援の単位ごとの対象経費と補助上限額を比較して低い金額

※ 3 対象経費が補助上限額を下回る場合、その差額

医療的ケア児受入加算補助対象経費等報告書

クラブ名 :

1 対象経費一覧

	月	支出科目	摘要	補助対象経費
配置	4			
	5			
	6			
	7			
	8			
	9			
	10			
	11			
	12			
	1			
	2			
	3			
		合 計		
送迎	4			
	5			
	6			
	7			
	8			
	9			
	10			
	11			
	12			
	1			
	2			
	3			
		合 計		

2 補助額

配置 (1) 補助対象経費

うち、人件費 \_\_\_\_\_

うち、管理運営費 \_\_\_\_\_

(2) 補助上限額

(3) 補助額（(1)と(2)を比較して低い額） \_\_\_\_\_

(4) 戻入額（(1) < (2)の場合、その差額） \_\_\_\_\_

送迎 (1) 補助対象経費

うち、人件費 \_\_\_\_\_

うち、管理運営費 \_\_\_\_\_

(2) 補助上限額

(3) 補助額（(1)と(2)を比較して低い額） \_\_\_\_\_

(4) 戻入額（(1) < (2)の場合、その差額） \_\_\_\_\_

育成支援体制強化加算補助対象経費等報告書

クラブ名： \_\_\_\_\_

1 対象経費一覧

No.	支出科目	内容	補助対象経費
1			円
2			円
3			円
4			円
5			円
6			円
7			円
8			円
9			円
10			円
11			円
12			円
13			円
14			円
15			円
16			円
17			円
18			円
19			円
20			円
21			円
22			円
23			円
24			円
25			円

2 加算額

- (1) 補助対象経費 \_\_\_\_\_ 円
  - (うち、人件費 \_\_\_\_\_ 円)
  - (うち、管理運営費 \_\_\_\_\_ 円)
- (2) 補助上限額 \_\_\_\_\_ 円 執行状況報告書(1月提出分)から転記
- (3) 補助額 \_\_\_\_\_ 円 ((1)と(2)を比較して低い額)
- (4) 戻入額 \_\_\_\_\_ 円 ((1)<(2)の場合、その差額)

放課後児童支援員等キャリアアップ処遇改善費補助対象経費積算書

クラブ名： \_\_\_\_\_

支援の単位： \_\_\_\_\_

No.	職員名	事由（※）											補助対象経費 上限額【A】	（内 訳）		賃金改善額等 （実績）【B】 <自動計算>	補助対象経費 （実績）【C】 〔AとBを比較して 少ない方の額〕		
		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月		3月	賃金改善額			その他 対象経費	
1															円	円	円	円	円
2															円	円	円	円	円
3															円	円	円	円	円
4															円	円	円	円	円
5															円	円	円	円	円
6															円	円	円	円	円
7															円	円	円	円	円
8															円	円	円	円	円
9															円	円	円	円	円
10															円	円	円	円	円
合計													円	円	円	円	円		

- 1 執行状況報告（1月）によって算定された補助基準額 \_\_\_\_\_ 円
- 2 補助対象経費（各職員の補助対象経費（実績）【C】の合計額） \_\_\_\_\_ 円
- 3 補助額（1、2を比較して低い額） \_\_\_\_\_ 円
- 4 戻入額（1 > 2の場合、その差額） \_\_\_\_\_ 円

※ 「事由」欄は以下に基づいて記入すること。

- ① 放課後児童支援員
- ② 経験年数が概ね5年以上の放課後児童支援員で、キャリアアップ研修を受講した者
- ③ 経験年数が概ね10年以上の放課後児童支援員で、キャリアアップ研修を受講した事業所長
- ④ 補助員
- ⑤ 経験年数が概ね5年以上の補助員で、キャリアアップ研修を受講した者



## 賃金改善加算補助 実施報告書

クラブ名：

## 1. 補助額

① 事業実施期間	令和 年 月 ~ 令和 年 月
② 補助基準額	円

## 2. 賃金改善額

③ 賃金改善額	円
④ うち、基本給又は決まって毎月支払う手当による賃金改善額	円
⑤ 賃金改善に伴い増加する法定福利費等の事業主負担分	円
⑥ 賃金改善額合計(③+⑤)	円

## 3. 要件の確認

※合致しない要件がある場合は、補助対象外です。

賃金改善額の2/3以上が基本給又は決まって毎月支払う手当によって改善されていること(③×2/3≤④)	
賃金改善額合計(⑥)が補助基準額(②)以上となっていること	
本加算補助による賃金改善に係る計画の具体的内容を職員に周知していること	
本加算補助の実施により講じた賃金改善の水準を維持すること	

上記の内容について、全ての職員に対し周知をした上で、提出していることを証明いたします。

年 月 日

運営主体名：

代表者職氏名：

## 賃金改善加算補助 賃金改善額内訳書

クラブ名：

NO.	職員名	常勤・非常勤の別	令和 年 月 ～ 令和 年 月分			
			賃金改善実施月数	賃金改善額		
					基本給又は 決まって毎月 支払う手当	その他
1				円	円	円
2				円	円	円
3				円	円	円
4				円	円	円
5				円	円	円
6				円	円	円
7				円	円	円
8				円	円	円
9				円	円	円
10				円	円	円
11				円	円	円
12				円	円	円
13				円	円	円
14				円	円	円
15				円	円	円
16				円	円	円
17				円	円	円
18				円	円	円
19				円	円	円
20				円	円	円
21				円	円	円
22				円	円	円
23				円	円	円
24				円	円	円
25				円	円	円
26				円	円	円
27				円	円	円
28				円	円	円
29				円	円	円
30				円	円	円
計				円	円	円

※クラブで勤務する職員のうち、賃金改善を行う者（職種問わず、非常勤を含み、経営に携わる法人の役員を除く。）を記載すること。

※行が足りない場合は適宜追加すること。

## 新型コロナウイルス感染拡大防止加算補助対象経費等報告書

クラブ名： \_\_\_\_\_

### 1 対象経費一覧

No.	支出科目	内容	補助対象経費
1			円
2			円
3			円
4			円
5			円
6			円
7			円
8			円
9			円
10			円
11			円
12			円
13			円
14			円
15			円
16			円
17			円
18			円
19			円
20			円
21			円
22			円
23			円
24			円
25			円

### 2 加算額

- (1) 補助対象経費 \_\_\_\_\_ 円
- (うち、人件費 \_\_\_\_\_ 円)
- (うち、管理運営費 \_\_\_\_\_ 円)
- (2) 補助上限額 \_\_\_\_\_ 円      執行状況報告書(1月提出分)から転記
- (3) 補助額 \_\_\_\_\_ 円      ((1)と(2)を比較して低い額)
- (4) 戻入額 \_\_\_\_\_ 円      ((1)<(2)の場合、その差額)

第 号  
年 月 日

(運営主体名)

(代表者職氏名)

様

横浜市

区長

横浜市放課後児童クラブ事業費補助金 交付額確定通知書

年 月 日付で交付決定した 年度横浜市放課後児童クラブ事業費補助金について、  
年 月 日付実績報告書等に基づき、次のとおり確定したので、通知します。

1 対象クラブ

\_\_\_\_\_

2 確定額

\_\_\_\_\_ 円

請求書番号	
業者コードー口座枝番	—

## 請 求 書

¥ \_\_\_\_\_

ただし、 \_\_\_\_\_ 年度横浜市放課後児童クラブ事業費補助金として、上記金額を請求します。

※該当する方に  又は  を記入してください。

[  4月受領分       その他( \_\_\_\_\_ 回目受領分) ]

\_\_\_\_\_ 年      月      日

(請求先)

横浜市                      区長

(請求者)

所在地 :

運営主体名 :

代表者職氏名 :

クラブ名 :

振込先	金融機関等の名称	銀行 信用金庫 農協	支店
	預金の種類	普通預金	当座預金
	口座番号		
	フリガナ		
	口座名義人		

※請求者（代表者氏名）と口座名義人が異なる場合は、下欄に記入・押印をお願いします。

上記振込先口座に補助金を振り込み下さい。

代表者職氏名 : \_\_\_\_\_ ⑩  
 口座名義人氏名 : \_\_\_\_\_ [クラブでの役割 : \_\_\_\_\_]  
 口座名義人住所 : \_\_\_\_\_

第 号  
年 月 日

(運営主体名)

(代表者職氏名)

様

横浜市

区長

横浜市放課後児童クラブ事業費補助金 交付決定取消通知書

年 月 日付で交付決定した 年度横浜市放課後児童クラブ事業費補助金について、次のとおり取消しましたので、通知します。

1 交付対象クラブ \_\_\_\_\_

2 取消額 \_\_\_\_\_ 円

3 取消理由 \_\_\_\_\_

年 月 日

(報告先)

横浜市 区長

(報告者)

所在地 :

運営主体名 :

代表者職氏名 :

クラブ名 :

## 消費税及び地方消費税に係る仕入控除税額報告書

年度横浜市放課後児童クラブ事業に関する補助金における消費税及び地方消費税に係る仕入控除税額について、次のとおり報告します。

### 1 消費税及び地方消費税に係る確定申告の有無

該当する項目に  又は  を記入してください。

有 ・  無

### 2 補助額及び消費税仕入控除税額（1で「有」とした場合のみ記載）

補助金名称	補助金交付額確定通知書		補助金の確定額	消費税及び地方消費税の申告に係る仕入控除税額
	日付	文書番号		
			円	円
			円	円
			円	円

### 3 添付書類（1で「無」の場合は添付不要）

- 仕入控除税額の積算の内訳を証する書類
- 課税期間分の消費税及び地方消費税の確定申告書（写し）
- 課税売上割合、控除対象仕入税額等の計算表（写し）
- 特定収入割合の計算表（該当がある場合のみ）（写し）