

## 業務説明資料

### 1 委託業務名

園選び支援A I チャットボット構築等業務委託

### 2 委託期間

契約締結日から令和7年3月末まで

### 3 業務目的

本市では、保育所等の利用を希望する保護者に対し、情報収集や園見学などを通じて希望施設の選択肢を広げていただくため、園選びサイト「えんさがしサポート★よこはま保育」（以下、「園選びサイト」という。）にて各園の基本情報や園内の写真等を掲載している。

この園選びサイトを利用する保護者の検索時間の短縮と利便性の向上を図るため、利用者との会話を通じて、利用者にあった保育所等をおすすめできるA I チャットボットを当該サイトに新たに搭載し、利用者の検索時間の短縮と利便性の向上を図ることを目的とする。

### 4 A I チャットボットの概要

園選びサイトを見た市民の自己解決を促す仕組みとして、人工知能（A I）により利用者の質問の意図を理解して適切な受け答えを行う自動会話プログラム（チャットボット）を導入する。

#### (1) チャットボット化する範囲

園選びサイトの掲載に用いている「施設情報データ」及び園選びにおける「よくある質問と回答のリスト」を対象とする。チャットボット化するにあたり、元データをできる限り変換せずに用いることができることが望ましく、その取り扱い易さを提案事項とする。

#### (2) チャットボットの回答の仕組み

施設情報データからおすすめ園を絞り込んで提案していく「シナリオ型」と、よくある質問のリストから適切に回答していく「一問一答型」を複合した形式を基本とする。なお、誤答の可能性があるため、言語予測モデル（いわゆる生成A I）等を用いたチャットボットは不可とする。

#### (3) チャットボットの運用方法

構築後もローコード又はノーコードで、市の職員によって応答率の向上を図ることが可能なものが望ましく、メンテナンスの行いやすさや、分析のしやすさを提案事項とする。また、運用サポートの範囲を提案事項とする。

#### (4) チャットボットの起動・表示イメージ

園選びサイトの隅に表示されるアイコンから起動することを予定している。起動後は、ウェブブラウザにおいては園選びサイト上にオーバーレイ表示され、スマートフォンの場合は全画面に表示されることを基本とする。

なお、横浜市では、あらゆる手続きがオンラインで行えて、様々な情報を入手できる、子育て世代を対象とした「子育て応援サイト・アプリ（仮称）」を開発している（Webアプリ、令和6年6月末リリース予定）。本サイト・アプリからチャットボットを起動・表示できる方法も提案事項とする。

## 5 業務概要

### (1) 業務の流れと業務範囲

本委託業務で実施する業務の主な流れと業務の最低限の範囲について以下に示す。具体的なスケジュール等については提案事項とする。

#### ア 詳細検討

本業務説明資料を参考に、システムの機能概要、基本構成をまとめ、本市こども青少年局の承認を得る。承認を得た内容をもとにさらに詳細に検討を深め、開発すべきシステムをまとめ承認を得る。本検討にあたっては、入念に打ち合わせを行うこと。

#### イ システムの開発

アで承認を得たシステムの構築を行う。開発作業に伴う環境の一切について、本市は提供を行わないので注意されたい。システム構築中に発生した調整点・問題点等は速やかに対応案を添えて本市に情報提供し指示を仰ぐこと。

#### ウ テストの実施及び導入サポート

仮のシステム稼働環境を構築し、システムが問題なく動作するかテストを行うこと。テスト状況は本市に一定期間公開し、本市からのフィードバックを踏まえて応答の精度が向上するようチューニングを行うこと。また、本市が本番環境において稼働を行う際には、これをサポートすること（後述7(6)参照）。

#### エ マニュアル整備及び運用研修

システム操作マニュアル及び管理者マニュアルを作成し、これを用いた利用者研修を実施すること。研修対象者は最低4名（こども青少年局保育対策課職員）とします。

### (2) 体制・納品等

ア 本委託業務に関する実施体制及び要員を十分に確保し、緊急時にも迅速に対応すること。

イ 本委託業務の完了時に成果物等一式を提出すること。成果物の種類、提出時期の具体的な期日は、発注者と協議の上、決定すること。

## 6 運用開始期日

令和6年9月

## 7 サービス要件

### (1) 想定する利用対象者

保育所等の利用を希望する本市の市民

### (2) 利用対象者数

令和5年4月入所新規申請者数 約17,000人

園選びサイトの表示回数 最大月約84,000件（令和5年10月）

### (3) 想定アクセス数

1か月あたりのアクセス数は以下の件数を想定

月平均500件程度とし8～10月の保育所等の利用申請に近い時期は月平均5,500件程度

### (4) 登録保育所等数

1,600件程度

(5) システム管理者

本市職員4名を想定

(6) 園選びサイトへの設置

ア 園選びサイト側の修正は業務に含まれませんが、受託後に園選びサイトの保守業務受託者と連携し、簡便な改修で、最大限の効果を目指すべく調整を図ること。

イ 園選びサイトへの設置にあたり、HTMLのソースサンプルを提示すること。

ウ ページ内検索が動作しなくなる等、園選びサイトに影響を与えること無く配置できること。また、チャットボット設置後、園選びサイトが動作しないときは、チャットボット側の関連ファイルを修正すること。

8 業務要件

チャットボットに関する業務要件を記載する。これらの要件（なお書きの部分を除く）をすべて満たすものとし、その他の事項を提案事項として提案を求めることとする。

(1) 基本仕様	
稼働時間	サービス提供時間は、原則、24時間、365日とする。システムメンテナンス等のため、あらかじめ定められた計画に沿い、稼働を停止することは例外とする。ただし、稼働停止に関しては必ず事前に委託者の承認を得ること。
応答時間	システム利用者が使用する機能については、原則、3秒以内のレスポンスを想定。
サーバー	クラウド型とオンプレミス型のどちらを選定するかは提案事項とする。オンプレミス型での構築を行う場合、本市関連部署との調整が必要となる。またクラウド型の場合、別添「サーバ等及び情報システム管理手順」を踏まえて構築されていることを要する。
利用環境	特定のウェブブラウザや機能に依存しないこととし、閲覧者の利用環境（利用端末、OS、ブラウザ、通信回線など）に関わらず、該当システムの利用ができること。
自然言語理解機能	自由記入欄を備え、キーワードの不一致や表記のゆれ、複数の意味を持つ単語等の入力があった場合においても、文脈や言葉の構成から意図を理解し、的確な応対や回答を導き出せること。
シナリオ型対話機能	あらかじめ設定した会話の流れに沿って、ユーザーから回答を引き出し、ユーザーの求める情報を提示していけること。具体的には、園選びサイトに掲載されている保育所等について、本機能から質問を投げかけ、ユーザーが回答することで、最適な保育園に導くことを想定している。シナリオは複数持つことができること。 なお、会話の冒頭だけでなく、自由記入欄の入力に基づく意図の理解を経て、特定のシナリオに進むことができればなおよい。
一問一答型対話機能	自由記入欄にユーザーが入力した文章等について、自然言語理解

	を踏まえ、あらかじめ設定した一問一答型の質問集の中から最もふさわしい回答を選び出し、回答を行えること。
データベースとの連動機能	シナリオ型対話機能が適宜、参照するデータベースの機能を備えること。データベースには保育所に関する各種情報を格納することを想定している。データベースは定期的に更新できる機能を備えていること。なお、高頻度で簡便に更新できるとより望ましい。
利用者のアクティビティ及び評価の収集機能	利用者の行動を適宜サーバーに記録するほか、回答が役に立ったかななどのダイアログを適宜表示することで利用者による評価を回収し、これを管理画面で閲覧できること。なお、評価結果等をもとに自動的に自然言語理解を担う機能が学習することで、回答精度が向上ができればなおよい。
(2) ユーザーインターフェース	
基本事項	直観的なユーザーインターフェースであり、操作性、わかりやすさに十分配慮したものであること。
表示位置	園選びサイトの隅に配置したアイコンから起動すること。アイコンは画面のスクロールに合わせて移動して表示できるようにすること。会話画面はウェブブラウザの場合、オーバーレイ表示とし、スマートフォンの場合は全画面表示とすることを基本とする。
表示オフ機能	ユーザーがアイコンを任意に消すことができる機能を（閉じるボタン等）を設けること。
アイコン	アイコンは本市が任意に設定したものであること。本市が変更を希望する場合、簡便に変更できることが望ましい。
(3) セキュリティ	
基本事項	管理画面へのログインについて、アカウント管理やアクセス制限が実施できる等、不正アクセスを防止するための対策を実施すること。
(4) 運用保守	
問合せ対応	本市からの求めに応じて、システム稼働状況等の問合せに対応すること。
障害管理	障害発生状況、障害対応等の履歴を管理する障害管理を行うこと。また、速やかに障害原因、影響範囲、対応方針、復旧見込みを委託者に報告すること。
変更管理	システムバージョン、パッチ情報等の変更管理を行うこと。
運用報告	定期メンテナンスを実施し、運用報告書を提出すること。

その他のアイデア（市民の利便性・満足度の向上、本市の業務効率化、費用低減につながるソリューション等）があれば積極的な提案を求める。ただし、有人対応による機能強化の提案は想定しておらず不可とする。

## 9 留意事項

(1) 機器類の準備

本システムの構築及び運用・保守に必要なサーバ機器・ソフトウェア等の機器類はすべて受託者において準備すること。

(2) 秘密保持・個人情報管理

受託者は、本業務終了後においても、本業務で知り得た個人・企業等の業務上の秘密を保持すること。個人情報については、本市個人情報保護条例等を遵守し、適正に管理すること。

(3) セキュリティ対策・ウェブアクセシビリティの確保

ア 高齢者等でも利用できるような十分なウェブアクセシビリティを確保すること。詳しくは、「(別紙①)ウェブアクセシビリティの確保について」を参照してください。

イ 原則、市のドメイン名である「city.yokohama.lg.jp」又はそのサブドメイン名を利用すること。また、外部サーバ機器等又は外部ドメイン名を利用する場合、事前にネットワーク管理責任者及び関連する業務所管課の長と必要な協議を行い、承認を得ること。

ウ インターネットで提供するサービスとして、「(別紙②)サーバ等及び情報システム管理手順」に則り、通常求められる水準以上のセキュリティ対策を実施し、不正アクセス等のサイバー攻撃防止対策を行うこと。

(4) スケーラビリティの確保

リリース後の本システムの運用において、シナリオや質問集の追加が見込まれることから、それらに対応できるスケーラビリティを確保すること。

(5) 業務の再委託

受託者は、デザイン、設計、データ移行、公開、保守など各工程を一括して受託者内で完結できること。基本的には第三者委託を禁止とする。ただし、作業工程の一部を委託する場合には、あらかじめ本市の同意を得るものとし、再委託先の行った作業の結果については、受託者が全責任を負うこと。

(6) 特記事項

ア 受託者は、受託業務の効率的実施と業務の公共性を十分に認識し、常に横浜市の業務を請け負っていることを念頭におき、市民の信頼を損なわないようにし、市民への奉仕を心がけること。

イ 受託者は、運営における業務上の課題、応対手順の整理及び業務の見直しの必要がある場合は、適宜会議の申し出を行い、委託者と協議の上、その解決に努めること。

ウ 受託者は、本業務における成果（受付状況などの統計情報）について、委託者がインターネットを含む対外的な発表を行うこと、複製、譲渡及び貸与することに関して、一切の異議を申し立てないこと。

エ 受託者は、この契約に基づく業務を遂行するため、委託者が提供した資料等を、委託者の許諾なくして複写、複製、譲渡及び貸与をしないこと。

オ 受託者は業務を行うにあたって、委託者の施策に協力すること。

カ 本説明資料に規定していない事項や、運営上、内容の変更等が必要となった場合は、委託者と協議の上、決定するものとする。

10 その他特記事項

本業務によって作成した資料については、本市の了解なく使用又は公表してはならない。

## (別紙①) ウェブアクセシビリティの確保について

### 1 適合レベル及び対応度

JIS X 8341-3:2016のレベルAAに準拠すること。

※本仕様書における「準拠」という表記は、情報通信アクセス協議会ウェブアクセシビリティ基盤委員会（以下、「WAIC」という。）の「ウェブコンテンツのJIS X 8341-3:2016 対応度表記ガイドライン 2016年3月版」で定められた表記によります。

### 2 対象範囲

本業務委託で作成する全てのウェブページ

### 3 アクセシビリティ方針の策定について

総務省の「みんなの公共サイト運用ガイドライン」、及びWAICの「ウェブアクセシビリティ方針策定ガイドライン」に基づき、発注者と協議の上、ウェブアクセシビリティ方針を策定すること。

### 4 試験前の事前確認について

- (1) HTML、CSSの雛形作成段階において、達成基準への対応状況を確認すること。テストツール(miChecker等)による判定が可能な検証項目については、ツールを使用し、対応状況を確認すること。その結果は発注者へ情報提供すること。
- (2) 1で定められた「適合レベル及び対応度」が、技術的に達成が困難である場合、代替案や例外事項の追加等を発注者へ提案し、発注者と協議の上、ウェブアクセシビリティ方針の変更を行うこと。

### 5 試験の実施について

- (1) 「みんなの公共サイト運用ガイドライン」及びWAICの「JIS X 8341-3:2016 試験実施ガイドライン」に基づき、試験を実施すること。
- (2) 試験の実施においては、テストツールによる判定だけでなく人間による判断も行うこと。
- (3) 試験内容については、発注者に説明し、承認を得ること。
- (4) 試験実施の範囲
  - ア 総ページ数が40ページ未満である場合  
試験を全ページで実施すること
  - イ 総ページ数が40ページ以上である場合  
当該システムからランダムに40ページ抽出し、試験を実施すること。

### 6 達成基準チェックリスト及びその検証方法を特定できる技術的根拠（実装チェックリスト）の作成について

「みんなの公共サイト運用ガイドライン」及びWAICの「JIS X 8341-3:2016 試験実施ガイドライン」に基づき、次のチェックリストを作成すること。

- (1) 達成基準チェックリストの作成について  
WAICの「達成基準チェックリストの例」を参考に、各項目の試験結果を記載した達成基準チェックリストを作成すること。
- (2) 実装チェックリスト(達成方法及びその検証方法を特定できる技術的根拠)の作成について  
WAICの「JIS X 8341-3:2016 試験実施ガイドライン」の「3.1 達成方法及びその検証方

法を特定できる技術的根拠を示す方法の例」を参考にして実装チェックリストを作成すること。

## 7 試験結果の説明及び不備の修正について

達成基準チェックリストの各項目の試験結果について発注者に説明し、試験結果の妥当性について承認を得ること。不備等が発覚した際には、速やかに該当箇所の修正、及び再度試験実施を行い、発注者の承認を得るまで対応すること。

## 8 参考ページ

(1) JIS規格詳細画面(JISX8341-3)

[http://www.jisc.go.jp/app/pager?RKKNP\\_vJISJISNO=X8341-3&%23jps.JPSH0090D:JPS00020:/JPS/JPS00090.jsp](http://www.jisc.go.jp/app/pager?RKKNP_vJISJISNO=X8341-3&%23jps.JPSH0090D:JPS00020:/JPS/JPS00090.jsp)

(2) みんなの公共サイト運用ガイドライン

[http://www.soumu.go.jp/main\\_content/000439213.pdf](http://www.soumu.go.jp/main_content/000439213.pdf)

(3) WAICの公開しているガイドライン一式

ア ウェブコンテンツの JIS X 8341-3:2016 対応度表記ガイドライン

<http://waic.jp/docs/jis2016/compliance-guidelines/201603/>

イ ウェブアクセシビリティ方針策定ガイドライン

<http://waic.jp/docs/jis2010/accessibility-plan-guidelines/201308/index.html>

ウ JIS X 8341-3:2016 試験実施ガイドライン

<http://waic.jp/docs/jis2016/test-guidelines/201604/>

エ 達成基準チェックリストの例

[http://waic.jp/docs/jis2016/test-guidelines/201604/gcl\\_example.html](http://waic.jp/docs/jis2016/test-guidelines/201604/gcl_example.html)

## (別紙②) サーバ等及び情報システム管理手順

### 1 サーバ等の設置場所

- (1) サーバ等は、第三者が自由に操作できないような場所に設置すること。
- (2) サーバ等は、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すること。
- (3) サーバ等は、容易に取り外せないよう適切に固定すること。
- (4) サーバ等に使用する物品や出力物の受け渡し場所は、原則として、サーバ等を設置した部屋とは別の場所にする。やむを得ず同一室内とする場合、受け渡しの際に入室権限がある者が立ち会うこと。ただし、同一室内であっても、サーバ等に物理的及びネットワーク的に接触できないよう保護措置が講じられている場合を除く。
- (5) サーバ等を設置した部屋には、そこがサーバ等の設置場所であるようなことを示す表示をしないこと。
- (6) サーバ等を設置した部屋は、施錠設備を有する必要最小限の出入口を備えた部屋とすること。
- (7) サーバ等を設置した部屋には、必要に応じて、防犯カメラ、侵入報知機等の防犯設備を設置すること。
- (8) サーバ等を設置した部屋には、必要に応じて、非常電話、非常ベル等の非常用連絡設備を設置すること。
- (9) サーバ等を設置した部屋にはコピー又は FAX 等、データの複写や送信のための設備を設置しないこと。ただし、同一室内であっても、部外者が利用できないよう保護措置が講じられている場合を除く。
- (10) サーバ等を設置した部屋には、必要十分な電源を確保すること。また、必要に応じて、無停電電源装置を用意すること。
- (11) サーバ等を設置した部屋には、必要に応じて空調設備を用意すること。
- (12) サーバ等を設置した部屋内の機器は、保守等を容易にするため合理的で適切な配置に努め、必要に応じて配置図を作成すること。

### 2 サーバ等の設置場所の運用

- (1) サーバ等を設置した部屋への入室権限のない者の入室及び作業実施については、事前に部屋の管理者の許可を得た上で、入室権限のある者が同伴すること。ただし、同一室内であっても、サーバ等に物理的及びネットワーク的に接触できないよう保護措置が講じられている場合を除く（以下(7)まで同じ）。
- (2) サーバ等を設置した部屋内に入室権限のある者が不在となる場合、入室権限の無い者を退室させた上で、施錠すること。
- (3) サーバ等を設置した部屋への入退室は、記録しておくこと。
- (4) サーバ等を設置した部屋への入室権限は、職員の異動や分担替えなどにあわせて速やかに見直すこと。
- (5) サーバ等を設置した部屋に入室不要となった者は速やかに登録を抹消し、入室のための

認証を無効にすること。

- (6) サーバ等を設置した部屋内では、部屋の管理者の許可なく撮影・模写・録音等を行わないこと。
- (7) サーバ等を設置した部屋には作業に必要なものを置かないこと。
- (8) サーバ等を設置した部屋内の環境（機器・設備の有無、配置、利用状況等）に問題がないことを定期的に点検すること。
- (9) サーバ等の安全な運用のため、必要に応じて停電や落雷、水害等への対策を行うこと。
- (10) サーバ等を設置した部屋への入室は、必要に応じてパスワード、IC カード、生体認証などによる認証がなければ入室できないよう制限すること。また、パスワードの定期的な変更や IC カードの管理など、運用に関する定めを整備し、遵守すること。

### 3 サーバ等の廃棄・返却・修理等

- (1) 非開示情報を格納しているサーバ等を廃棄する場合は、原則として、データ消去等を実施してから廃棄をすること。
- (2) リース契約等により借用していたサーバ等を返却する際、非開示情報を格納しているサーバ等については、原則として、データ消去等を実施してから返却すること。
- (3) 非開示情報を格納しているサーバ等を修理するために外部へ持ち出す場合は、事前に、データ消去等を実施すること。ただし、これが困難な場合には、信頼できる事業者を選定し、秘密保持及び、処分品の再利用の禁止を契約時に特約として含めた上で、外部に委託して修理を行うことができる。
- (4) 非開示情報を格納しているかどうか不明な場合には、非開示情報を格納しているものとして取り扱うこと。

### 4 通信機器等の管理

- (1) サーバ等のための通信機器等は、容易に第三者が触れられないように、かつ接触による断線や電源断などが起きないように敷設すること。
- (2) 無線による通信を行う場合、解読が困難な暗号化及び認証技術を使用する等の盗聴対策を講じること。
- (3) ファイアウォール、ルータ等の設定を行えるサーバ等のための通信機器等は、パスワードを設定するなどして、第三者が設定の変更等を行えないようにすること。
- (4) ファームウェアの更新や適切な設定を行うなど、不正な利用がされないようにすること。

### 5 情報システム開発時の規定

- (1) 情報システムを開発する際には、事前に区局情報セキュリティ総括責任者の承認を得ること。
- (2) 管理するデータについて、漏えい・改ざん・破壊といった問題が発生した場合の影響の評価などのリスク分析を実施すること。また、データの入力チェック、内部でのデータの処理プロセスの正当性評価、出力されるデータの妥当性評価などの、データの完全性に関する検査も併せて実施すること。
- (3) サーバ等には、情報システムの趣旨、用途に応じた必要最低限のソフトウェア以外のもの

のをインストールしないこと。

- (4) 管理者を含む開発用の利用者登録では、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。特に重要な権限を持つ利用者のパスワードは、漏れることのないよう厳重に管理すること。

## 6 情報システム導入時の規定

- (1) 情報システムの利用を開始する際には、事前に区局情報セキュリティ総括責任者の了承を得ること。
- (2) データ及び情報システムの安全かつ正常な運用を確実にするために、情報資産の一覧を作成し、各情報資産の情報資産管理者を明確にすること。
- (3) 安全かつ正常な運用のための手順書を作成すること。また、情報セキュリティ事故に備え、事故時のための手順書を作成すること。
- (4) 使用するソフトウェアについて、信頼性の高い安全なものを導入すること。
- (5) 基本ソフトウェアのアクセス制御、ファイルのアクセス制御、業務用のソフトウェアの実行権限の制御等に関して、厳密なアクセス権を設定すること。
- (6) 利用者に対して、必要最低限のアクセス権限のみ許可するようにすること。特に、特定個人情報ファイルへのアクセス権限は真に必要な場合に限り許可すること。
- (7) 情報資産に対して、権限のある者に認められた範囲でのみ利用させるようにするため、扱う情報資産の内容及び不正アクセスのリスクに応じて、利用者の認証、利用する端末機等の認証もしくは接続元による制限を実施すること。
- (8) サーバ等で利用するソフトウェアは、当該ソフトウェアのメーカー等による製品サポートが提供される状態で利用すること。また、利用期間中に製品サポートの提供が途切れることのないよう、計画的な更新を行うこと。
- (9) 情報セキュリティ担当者及び情報資産管理者は、業務で利用する専用のソフトウェア及びハードウェアが対応していない等、真にやむを得ない事由により一時的にサポート切れソフトウェアを利用する場合、共通実施手順第5条に定める措置を実施すること。

## 7 情報システム運用時の規定

- (1) 製造元が提供する修正プログラム等を導入するなど、使用するソフトウェアを常に安全で正しく機能する状態で使用するよう努めること。
- (2) 通信経路の暗号化、通信回線の監視、ファイヤ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。
- (3) インターネットを経由した不特定多数からのアクセスが可能な状態にある情報機器等は、Webアプリケーションファイヤウォール (WAF) や仮想パッチを導入するなど、サイバー攻撃のリスクに対して、適切なセキュリティ対策を行うこと。
- (4) 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。特に重要な権限を持つ利用者のパスワードは、漏れることのないよう厳重に管理すること。
- (5) 情報システムの保守の記録を残すこと。
- (6) 個人情報を扱う情報システムでは、個人情報を記録したシステムにおける端末機による

- データの更新、検索等の操作の記録に関する要綱に基づき、操作記録の採取を行うこと。  
それ以外の情報システムでは、必要に応じて、操作記録の採取を行うこと。
- (7) 業務用のデータは、その重要性に応じ、定期的にバックアップを取得し、安全に保管すること。また、必要に応じて、データ更新の詳細な記録を保管する等により、確実に復旧できる状態を維持すること。
- (8) 障害時の代替品を用意するなど、障害発生時の対策を用意すること。
- (9) 端末機等及び携帯端末について、新規利用者の登録・既存利用者の利用者コード又はパスワード変更・利用者の登録抹消の申請を受けた場合には、正当性を審査し、速やかに対応すること。
- (10) 必要に応じて、定期的に次のような検査を行うこと。
- ア 脆弱性検査ソフトによる最新の脆弱性情報を含む検査
  - イ 情報システムの仕様書と実際の利用機器との整合性
  - ウ 不要なアクセス権が存在しないこと
  - エ 不要なサービスの起動が存在しないこと
  - オ 不要なアカウントが存在しないこと
  - カ 推測されやすいパスワードが設定されていないこと
- (11) (10)の検査結果は、必ず記録し、原則5年間保管すること。
- (12) (10)の検査により不備が発見された場合には、速やかに是正すること。
- (13) 著作権を侵害することがないように、ソフトウェアのライセンス管理を適切に行うこと。
- (14) 特定個人情報を取り扱うシステムにおいては、情報システムの運用を行う者に対して、運用で利用する端末周辺へのカメラ付き携帯電話やスマートフォンの持ち込みを禁止する、必ず複数人で運用作業を実施するなど、その情報システムの運用状況において発生するリスクに応じた情報持ち出し防止策を講じること。
- (15) 情報システムの開発・管理・運用を外部委託事業者に行わせる場合、委託内容に応じた情報セキュリティ対策が確保されている事業者を選定すること。
- (16) クラウドサービスを利用する場合、取り扱う情報の重要性から確保すべき機密性、完全性及び可用性を検討し、それに応じたセキュリティレベルが確保されているサービスを選定すること。
- (17) インターネットを経由して、不特定多数から攻撃を意図した通信が届く環境にある場合、インターネットからサイバー攻撃のリスクに対応するため、最低限、次の対策を実施すること。また、その対策が実施可能な体制を整備・維持すること。
- ア 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。
  - イ 情報システム等に脆弱性があり、当該脆弱性を利用したサイバー攻撃が実際に行われていることが判明した場合、当該サイバー攻撃を防止する措置を直ちに講じること。なお、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による対策も可とする。
  - ウ 管理者が利用する機能は、管理者の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。

## 8 情報セキュリティ事故

- (1) 情報セキュリティ事故の発生に備え、情報セキュリティ事故対応手順に基づき事前の準備を行うこと。
- (2) 情報セキュリティ事故が発生した場合、情報セキュリティ事故対応手順に基づき、速やかに対処すること。