

令和3年度一時預かり WEB 予約システムの導入及び運用保守業務委託
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、将来の業務実施の条件となるものではありません。

1 件名

令和3年度一時預かり WEB 予約システムの導入及び運用保守業務委託

2 履行期限

契約締結日から令和4年3月31日まで

(システムの試行運用は令和4年3月1日からを予定)

3 履行場所

こども青少年局保育・教育運営課他

4 業務目的

(1) 目的

本市の保育施設における一時預かり事業（乳幼児一時預かり事業、一時保育事業等）については、現在、利用者が各施設に空き状況を直接電話等で確認し、予約する方法が取られており、利便性に課題があります。このたび、現行の予約方法の効率化による市民サービスの向上、及び保育事業者の事務効率化を目的として、WEB 予約システムを調達します。また試行運用中のシステム改善及びメンテナンスのために、運用保守も委託します。

なお、令和3年度は乳幼児一時預かり事業 29 施設において試行運用を行い、システム改善を得て、次年度以降はさらに一時保育施設約 500 施設を対象とすることを見込んでいます。

(2) 一時預かり事業の概要

一時的に未就学児を預かることにより、保護者の子育てに伴う身体的・精神的負担の軽減を図ることを目的とした事業です。

ア 事業種別

事業種別は次の通り複数あります。

事業名	事業概要	施設数	利用件数 (延べ)	システム参 入 スケジュール
乳幼児一時預かり 事業	認可外保育施設等による一時預かりを専門に行う事業	29(R3年度) 32(R4年度予定)	85,000件 (R4年度予定)	R3年度中に 29施設 R4年4月から 32施設
一時保育事業	認可保育所等による一時預かり事業	約500施設 (R4年度予定)	130,000件 (R4年度予定)	R4年度10月 以降随時(R 4年度は100 施設見込み)
休日一時保育事業	認可保育所等による休日一時保育事業	8施設 (R4年度予定)	2,400件 (R4年度予定)	R4年度10月 以降随時(R 4年度は8 施設見込み)
その他の一時預かり	24時間緊急一時保育事業、地域子育て支援拠点における一時預かり事業等			未定

5 業務範囲

本委託業務では、一時預かり事業にかかる次の業務を実施します。

- (1) プロジェクト管理
- (2) 要件定義
- (3) 導入準備
- (4) データ移行支援
- (5) 機能開発
- (6) システムの検証及び改善
- (7) システム運用・保守
- (8) 操作マニュアルの作成
- (9) その他付随する作業

6 業務内容

(1) 令和3年度一時預かり WEB 予約システムの概要

一時預かり WEB 予約システムは、未就学児を保育施設に一時的に預けたい市民が、インターネットを利用してスマートフォンやパソコンを使って、利用予約等を行うことができるシステムです。市民がシステムを通じて、利用したい日時の各施設の空き情報を確認し、予約等を行

うための市民側利用者機能、日々の空き状況を管理し、予約受け等を行うための施設側利用者機能、施設から事業の実施状況等のデータを抽出できる本市職員側利用者機能等を備えます。

(2) システムの方針

- ア 一時預かりに関する空き状況の確認や利用予約を、スマートフォンやパソコンなど多くの市民が使用するインターネット端末で容易に行えること。
- イ 一時預かり事業実施施設が、日々の利用状況や利用者情報の管理を容易に行えること。また施設ごとに利用時間枠の設定方法などを変更でき、多様な現場に応じた活用ができること。
- ウ 利用者による施設の検索方法や入力項目の設計、施設側の利用状況や利用者情報の管理画面等の設計において、GUI による使いやすい設計画面とし、市民サービスの向上に資するとともに施設や本市職員の負担軽減を図ることができること。
- エ 将来的な参加施設数や予約想定量（約 530 施設、予約数延べ 200,000 件／年）以上を処理できる、または拡張可能なシステムであること。
- オ 利用者の手続きや入力項目を最小限にできる、入力内容のチェックが可能など、ユーザビリティに優れたものであること。
- カ 施設ごとの利用状況を日ごと、月ごとにデータで書き出せるなど、施設側職員及び本市職員の業務効率化に寄与するものであること。
- キ 高い可用性及び堅牢なセキュリティを確保したシステムであること。

(3) システム導入業務内容

- ア システムの開発
- イ システムの導入作業
- ウ 現行データ等からのデータ移行作業支援
- エ マニュアル整備（市民側利用者用、施設側利用者用、本市職員側利用者用）

(4) 運用保守業務内容

- ア 基本サービス提供
- イ システムの検証と改善
- ウ 本市職員支援
- エ マニュアルの更新

7 スケジュール等

(1) 現時点で想定している全体スケジュール

年度	月	内容
令和 3	10 月	契約締結
	11 月～2 月	開発
	2 月	試行運用に向けた準備 ・施設データ入力（乳幼児一時預かり事業 29 施設） 試行運用にむけた仮マニュアルの納品

	3月	試行運用 ・乳幼児一時預かり事業にて試行 運用保守 検証、システム改善 マニュアルの納品
令和4	通年	運用保守
	4月	3施設 増（乳幼児一時預かり事業 計 32 施設）
	4月～9月	検証、システム改善
	8月～9月	施設増に向けたデータ入力 ・施設データ入力（一時保育事業 100 施設見込、休日一時保育事業 8 施設見込み）
	10月	施設増（一時保育事業 100 施設見込、休日一時保育事業 8 施設見込み、合計約 140 施設）
	1月～3月	検証、システム改善
令和5 以降	通年	運用保守 随時、施設追加

(2) 参入施設の増加予定

令和4年度10月以降、参入施設が増加する予定のため、対象拡大に係る考え方についても提案の対象とします。

ア 一時保育事業、休日一時保育事業

施設情報の掲載は必須とする予定ですが、それ以外の機能（空き情報の公表、予約機能）への参入については、施設により異なります。また、各施設、空き情報の公表や予約機能への参入時期も施設により異なることが想定されます。

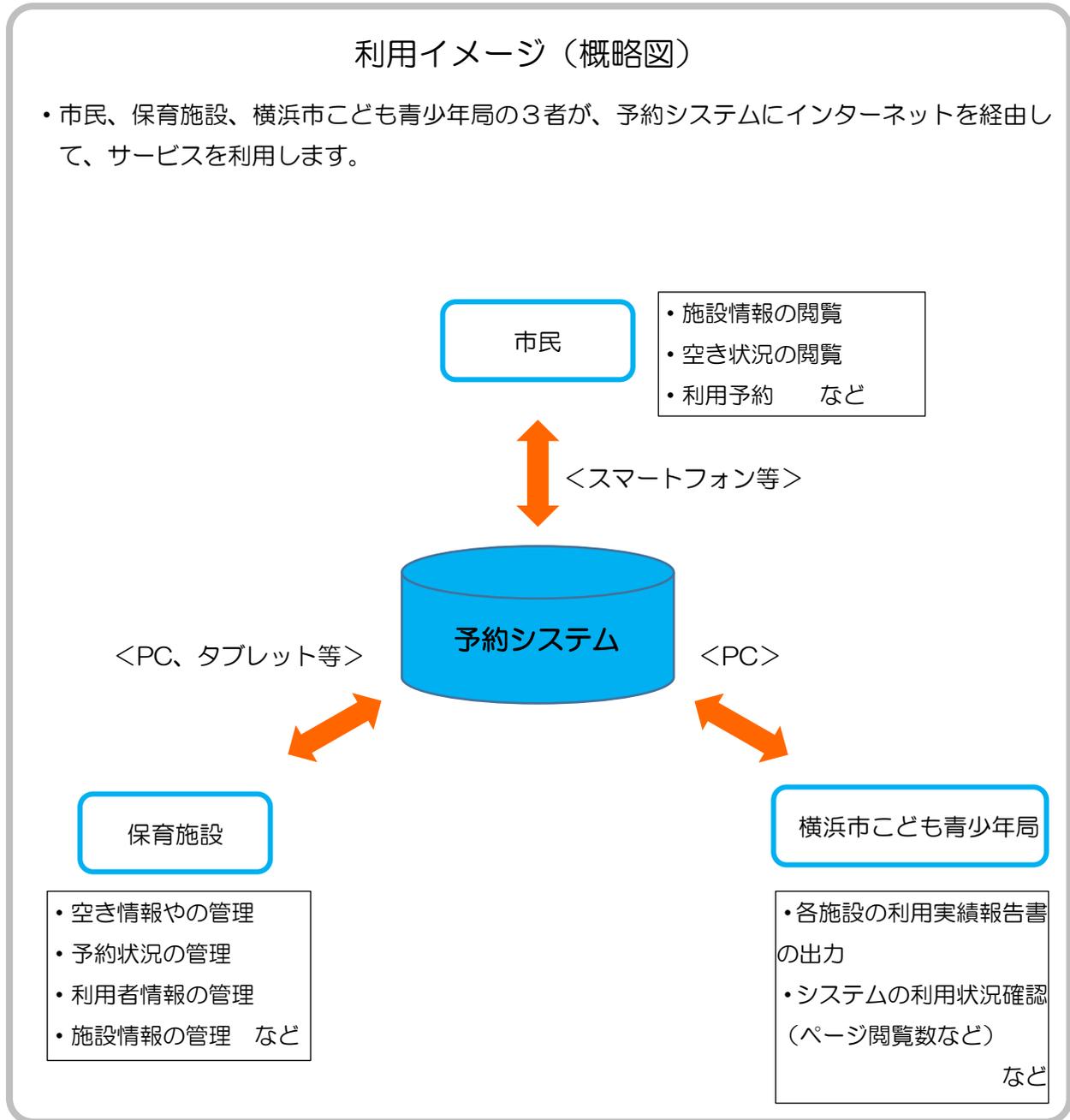
年度途中での事業開始、事業廃止があり、施設数に変動があります。

イ 24時間緊急一時保育事業及びその他の保育事業

現時点では本予約システムへの参入予定はありませんが、令和4年度以降、参入する可能性があります。

8 一時預かり予約システムの概要

(1) 利用イメージ



このほか、別紙＜システムのイメージ＞のとおり。

(2) 機能構成

ア 市民側利用者

おもな基本機能	おもなオプション機能
・施設情報の閲覧	・キャンセル待ち機能
・空き状況の閲覧	・位置情報を用いた施設検索など、利便性の高い機能の付加
・利用登録申請	
・利用予約	
・マイページ管理	
・利用登録情報の変更、削除	
・予約内容の変更、キャンセル	

※その他、別紙「機能要件一覧」のとおり

イ 施設側利用者

おもな基本機能	おもなオプション機能
・施設情報の管理	・利用（予約）状況一覧のデータ書き出し
・空き情報の管理	・利用者情報の管理
・予約状況の管理	・利用料の表示

※その他、別紙「機能要件一覧」のとおり

ウ 職員側利用者

おもな基本機能	おもなオプション機能
・施設情報の管理	・各施設の利用状況一覧の出力
	・システムの利用状況確認（ページ閲覧数など）

※その他、別紙「機能要件一覧」のとおり

(3) 業務フロー

別紙<業務フロー>のとおり。

(4) 機能要件

別紙<機能要件一覧>のとおり。

8 システムの仕様について

本委託業務において、システムが備えるべき仕様については、別紙<基本仕様書>を参照してください。

本業務委託において、別途本市の費用負担が必要な内容・項目がある場合はその内容・項目及び概算費用を提案書に記載してください。

9 成果品

本予約システム

市民側利用者用マニュアル

紙媒体 1 部、電子媒体 2 部

施設側利用者用マニュアル

紙媒体 1 部、電子媒体 2 部

職員側利用者用マニュアル

紙媒体 1 部、電子媒体 2 部

報告書

紙媒体 1 部、電子媒体 2 部

本業務委託により作成した資料

紙媒体 1 部、電子媒体 2 部

【別紙】 システムのイメージ

I 利用者用画面

利用者がスマホやPC等から利用する画面です。

主な仕様

- 施設の空き状況は誰でも閲覧できる。
- 利用予約は、利用登録後に発行されるIDとパスワードが必要。
- 利用登録（初回面談）の申請ができる。
- 乳幼児一時預かり、認可等の一時保育等を一緒に掲載

<①利用者画面トップページ>

横浜市一時預かり 予約サイト

空き状況を見る

→②-1へ

施設に利用登録を申請する
(面談あり)

→③-1へ

マイページ
(予約の確認・取消)

→④-1へ

施設一覧

→⑤-1へ

更新情報

[2021年〇月〇日 新型コロナウイルス対策について](#)

[2021年〇月〇日 年末年始の利用について](#)

ご利用に関する注意事項

[•ご利用当日の検温のお願い。](#)

[•〇〇〇〇](#)

<②-1 空き状況を見る>

確認したい期間を入力

月 日 から 月 日 まで

確認したい施設を選択

施設を選択 ▼

または区を選択

区を選択 ▼

例えば0歳児とその他の年齢とで、入りを分けることが施設ごとにできると望ましい。

施設検索方法は
今後業者と検討

この条件で空き状況を見る

→②-2へ

<②-2 空き状況 施設ごとのシート>

- … 予約可
- △ … 残りわずか。お問合せください
- × … 空きなし（予約不可）
- … 対象外

	A園			B園			C園			
	2021年6月									次の1週間
	14 (月)	15 (火)	16 (水)	17 (木)	18 (金)	19 (土)	20 (日)	21 (月)		
9:00	×	×	×	×	○	—	—	×	9:00	
10:00	×	○	○	×	×	—	—	×	10:00	
11:00	×	×	×	×	×	—	—	×	11:00	
12:00	○	×	×	×	×	—	—	×	12:00	
13:00	○	×	×	×	×	—	—	△	13:00	
14:00	○	○	△	○	○	—	—	△	14:00	
15:00	○	○	△	○	○	—	—	△	15:00	
16:00	×	○	△	○	○	—	—	○	16:00	
17:00	×	○	△	○	○	—	—	○	17:00	



<②-3 施設予約ログイン画面>

A園 6月18日の予約について

予約するには、施設から発行されたIDとパスワードを入力して、ログインしていただく必要があります。

ID

パスワード

ログイン

→②-4へ

IDとパスワードは、施設に利用登録（面談あり）を行うことにより、各施設から発行されます。利用登録はこちらからお願いします。

仮予約の上、施設に利用登録をする

→③-1へ

※利用登録と同時に、仮予約できると望ましい

<②-4 予約時間入力>

予約したい時間帯を入力してください。

A園

6月18日（金）

時 分 から 時 分

確認画面に進む

→②-4へ

<②-5 予約内容確認>

予約内容をご確認ください。

予約日時	2021年6月18日（金）15時00分～17時00分
利用児童氏名	横浜 太郎
利用施設名	A園

この内容で予約する

<※キャンセル待ちについて>

キャンセル待ち機能については、次の仕様を検討しています。

※オプション機能

- その枠にキャンセルが発生した場合、【キャンセル待ち】をした方全員にメール通知が自動的に届く。
「キャンセルが発生しました。予約しますか？」。
- メールが届いた方のうち、すぐに再度予約申請した人が、予約できる。
- この機能を利用するか、しないかは、各施設が選択できる。

<③-1 利用登録を申請する>

利用登録は、次のフォームを入力・送信の上、各施設と、児童を含めた3者で面談することで完了します。

保護者（申請者）について

氏名
続柄
住所
電話番号
メール

児童について

氏名
生年月日

登録希望施設

面談希望日

○月○日 AM・PM

入力項目は
今後調整

この内容で利用登録を申請する

→この後、施設からメール・電話等で
面談の日程調整

<④-1 マイページ>

登録情報

保護者氏名	横浜 太郎
住所	港北区〇〇 〇-〇
児童氏名	横浜 花子

登録情報を変更する

）

登録施設1	A園
登録施設2	B園
登録施設3	C園

現在の予約状況

予約日時	施設名
2021年6月17日（木） 10時00分～16時30分	A園
2021年6月18日（金） 15時00分～17時00分	A園
2021年7月2日（金） 15時00分～17時00分	B園

キャンセル

キャンセル

キャンセル

Ⅱ 保育施設用画面

保育施設がPC等から管理する画面です。

主な仕様

- 空き枠の表示方法を随時入力できる。
- 予約開始時期を設定できる。
- 予約できる時間の区切りを設定できる。
- 利用登録申請、面談申込を受けることができる
- 登録者情報を管理できる。

予約状況管理

- 現在の予約状況、キャンセル待ち状況を確認できる。
- 空き枠の表示方法を随時入力できる。
- WEB以外で受付けた予約を入力できる。

利用者情報管理

- 利用登録申請を受付け、面談の日程調整を行う（メールor電話）
- 面談後に利用者登録を行い、ID、パスワードを発行（すでに他施設で発行済の場合は、発行済IDに登録済み施設情報を付与）。
- 利用者情報を管理できる（利用者情報の追記など）。

設定

- 予約できる時間の区切り設定
- 定員、WEB管理枠、手動枠の設定
- 予約開始時期を設定

施設情報管理

- 施設情報の編集

報告書作成

- 実績報告書を作成できる機能を検討中

- 定員のうち、どれだけの枠をWEB予約システムに公表するかは、各施設が選択可能
- 緊急枠など、WEB予約システムで管理しない枠についても、この施設用画面から管理することで、実績報告書の作成が不要とできないか、検討中。

<⑦ 予約に関して各施設が設定できること①>

A園			
2021年 6月			
	14 (月)	15 (火)	16 (水)
9:00	×	×	×
10:00	×	○	○
11:00	×	×	×
12:00	○	×	×
13:00	○	×	×
14:00	○	△	△
15:00	○	△	△
16:00	×	○	△
17:00	×	○	△

時間の区切りを変更（30分単位や1時間単位など）

空き状況を変更できる

- … 予約可
- △ … 残りわずか。お問合せください
- × … 空きなし（予約不可）
- … 対象外

※直前の3日間は、○ではなく△と表示することも調整中

予約開始時期を設定できる（毎月1日に翌月分を受付開始 等）

WEB以外で受付けた予約を入力できる → 実績報告書の自動作成

<⑧ 予約に関して各施設が設定できること②>

定員 名WEB予約で管理する枠数 1日 名
※利用日の 日前からは問合せのみ。直接管理する枠数 1日 名

WEB予約開始タイミング

- 利用日の 日前の 時より予約受付
- 毎月1日から、翌月分（1か月分）の予約受付
- 毎月1日から予約受付（当月16～末日分）
毎月15日から予約受付（翌月1～15日分）

一人当たりの予約上限数

- 一カ月 日まで
- 一カ月 時間まで

など

機能要件一覧(必須及び任意項目)

項番	大項目	必須/任意	小項目(概要)
1	基本	必須	原則として24時間365日サービスが利用可能であること。
2	基本	必須	1時間に5,000件以上の申請等を受け付けられること。
3	基本	必須	職員側利用者の機能について、PC利用におけるウェブブラウザは少なくともChrome、Edgeを動作保証すること。
4	基本	必須	市民側利用者及び施設側利用者のウェブブラウザは少なくともChrome、Edge、Safari、Firefoxを動作保証すること。
5	基本	必須	市民側利用者がオンラインで各施設の空き確認、利用登録申請、予約等の手続を行うことができ、施設側利用者は空き状況の制御や利用登録申請の受付、利用者情報の管理等を行うことができるシステムを実現すること。
6	基本	必須	市民側利用者は、スマートフォン、パソコン等、多くの利用者が利用する端末を利用して、予約等の市民側利用者機能が利用できること。
7	基本	必須	施設側利用者は、パソコンやタブレット等を利用して、予約の管理や利用者管理等の施設側利用者機能が利用できること。
8	基本	必須	利用者の誤入力を防止するための対策を施すこと。(範囲内の日付や数字しか入力不可とする、郵便番号を入力したら住所が自動入力されるなど)
9	基本	必須	レスポンシブデザイン(端末情報を認識して最適化されたデザインを表示する)となっていること。
10	基本	必須	ポータル画面を備え、障害情報やお知らせの表示、利用者登録、空き情報の閲覧や施設予約などが行えること。
11	基本	必須	システム内から、市民側利用者および施設側利用者に対して、利用登録時や予約の受付、予約内容変更、キャンセル等の通知メールを送信できる機能があること。
12	基本	必須	市民側利用者の本人認証にIDパスワードによる認証が可能であること。
13	基本	必須	市民側利用者の登録・登録情報変更時に、登録メールアドレスへの発信通知ができること。
14	基本	任意	市民側利用者の登録・登録情報変更時の本人の携帯電話番号の確認に、SMSによる認証が実装可能であること。
15	基本	必須	市民側利用者の登録済(面談済)施設の情報は、同一のIDパスワードに関連づけること。
16	基本	必須	市民側利用者は、利用登録済(面談済)施設のみ、予約可能とすること。
17	基本	任意	市民側利用者は、利用登録の済んでいない施設でも、登録申請と共に仮予約ができること。また、その機能の利用については、施設ごとに選択できること。
18	基本	必須	施設の空き情報の閲覧は、全ての利用者が可能であること。
19	基本	必須	市民側利用者から利用登録申請のあった施設側利用者のみ、その市民側利用者の情報を閲覧できること。
20	基本	必須	市民側利用者がIDまたはパスワードを紛失した場合の再発行や確認の手続をわかりやすく示し、ユーザビリティを十分考慮すること。
21	基本	必須	施設側利用者の本人認証にIDパスワードの利用ができること。なお、施設側利用者のアカウントは1施設1アカウントとする。

22	基本	必須	施設ごとに、予約枠の時間単位を設定できること(30分単位、1時間単位、1日単位等)。
23	基本	必須	施設ごとに、予約受付期間開始時期(1か月前など)、受付期間終了日時(三日前まで等)を設定することにより、各施設が異なるタイミングで自動的に予約の受付を開始、終了できること。
24	基本	必須	空き情報は○(予約可)、△(お問合せ下さい(残り3枠))、×(予約不可)、-(対象外)、のように、空き枠数を明記しない表示形式とすること。
25	基本	任意	予約申請を受け付けた施設側利用者が、予約を確定する操作をすることで、予約が確定するフローを実現すること。また、施設ごとにその機能を使用するか否か選択できること。
26	基本	任意	年齢別に(1歳未満児、1歳以上児など)、空き枠の管理、予約受付ができること。
27	基本	任意	0歳児は2枠分、のように、年齢別に使用枠の重みづけを施設ごとに変更できること。
28	基本	任意	システムの利用状況が分かる統計資料(アクセス数、ページ閲覧数など)を出力できること。
29	基本	必須	児童の生年月日を登録し、システム及び施設側利用者が児童の年齢確認に使用できること。
30	基本	任意	市民側利用者情報の年度更新機能を実装し、毎年10月1日に6歳児以上の情報を自動削除できること(就学年齢に達した6カ月後)。
31	基本	任意	一回の利用ごとに、利用料を算出できること。
32	基本	任意	市民側利用者情報には減免(非課税世帯、生活保護世帯、ひとり親世帯、多胎児)の対象か否かを登録できること。
33	基本	任意	減免について、利用料算出に反映できること。
34	基本	任意	職員側利用者は、児童1人のひと月の利用時間・日数に上限を設けることができること(ひと月120時間または15日以内等)。また、市民側利用者が、その上限を超えて利用しようとしたときに、予約不可にできること。
35	基本	任意	職員側利用者は、事業種別(乳幼児一時預かり事業、一時保育事業等)ごとに、児童1人のひと月の予約時間・日数に上限を設けることができること(1人ひと月120時間以内等)。
36	基本	任意	施設側利用者は、児童1人のひと月の予約時間・日数に、施設ごとの上限を設けることができること(1人ひと月4日以内等)。※事業種別ごとの利用上限の範囲内に限る。
37	基本	任意	キャンセル待ち機能を有すること。
38	基本	任意	キャンセル待ちをしている日時に空きが生じた場合は、キャンセル待ちしている利用者全員に空きが生じた旨を通知するメールを自動送信する機能を有すること。
39	基本	任意	施設ごとに、受け入れ可能年齢を設定でき(A施設は1歳から5歳まで、B施設は生後6カ月から5歳まで等)、対象外の児童の予約は不可とすること。
40	基本	任意	利用日数日前(2日前を想定)以降の予約内容の変更、キャンセルは、WEB受付不可(電話のみ)とする設定が、施設ごとにできること。
41	市民側機能	必須	市民側利用者が、自らの登録情報(氏名、住所等)の他、登録済み施設、予約状況などを確認できる機能があること。
42	市民側機能	必須	市民側利用者が、自らの予約内容を変更、キャンセルできる機能があること。
43	市民側機能	任意	予約をする際に、園給食やおやつの利用の有無の選択や利用理由の選択の他、市民側利用者による自由記入欄があること。
44	市民側機能	任意	きょうだい児の場合は、複数名同時に予約申請ができること。
45	市民側機能	任意	市民側利用者には、複数の児童(きょうだい児)を登録情報として有することができること。また、児童単位で施設を予約できること。
46	職員側機能	任意	職員側利用者機能として、利用実績データの抽出機能(施設ごと、月ごとの利用実績データの抽出)を有すること。

47	職員側機能	任意	職員側利用者機能として、複数の施設情報を一括で入力できる機能を実現すること。(CSV形式ファイルのアップロードなど)
48	職員側機能	必須	システムを利用する職員側利用者のIDに対して、管理者としてのシステム利用の権限設定ができること。
49	施設側機能 職員側機能	任意	施設ごとの月ごとの利用実績データをCSV形式で出力できること。(出力データ項目は、児童氏名、利用日、利用時間、利用理由、減免の有無等であり、詳細は委託者と協議)
50	施設側機能	任意	施設ごとの予約可能人数は、日付と時間帯ごとに設定できること
51	施設側機能	任意	施設ごとの日ごとの利用予約及び実績データをCSV形式で出力できること。
52	施設側機能	任意	施設情報画面に、画像(施設写真など)を掲載できること。
53	施設側機能	任意	施設情報画面に、地図情報(リンクも可)を掲載できること。
54	施設側機能	必須	施設情報画面に、保育施設のWEBページへのリンクを掲載できること。
55	施設側機能	必須	施設側利用者が市民側利用者情報の登録・変更(氏名、住所等の入力)を本人に代わって入力を行えること。
56	施設側機能	必須	施設側利用者が市民側利用者から電話等で受付けた予約の入力、取下げ、訂正が行えること。
57	施設側機能	任意	施設側利用者が、施設に登録済の市民側利用者情報をCSV等で出力できること。
58	施設側機能	任意	施設側利用者が、日ごとの予約内容をCSV等で出力できる機能を有すること。
59	アクセスログ	必須	本人開示請求等に対応するため、職員側利用者が全利用者のアクセスログを取得し、必要に応じて開示ができること。
60	手続	必須	本予約サイトは横浜市ドメインとすること。 *city.yokohama.lg.jp(LGドメイン)。 これが不可能な場合、ネットワーク管理責任者と協議を行い、市のドメイン名又はそれらのサブドメイン名とは異なるドメイン名による情報受発信について許可を得ること。
61	手続	必須	サービス利用にあたって、少なくとも1回は利用規約に同意する又は同意したとするプロセスを通過するようにできること。
62	手続	任意	予約成立を市民側利用者へに通知するメールにおいて、施設ごとに異なる内容を通知できること。
63	手続	任意	予約情報を、利用日前日に市民側利用者へにリマインド通知する機能を有すること。
64	手続	任意	市民側利用者による同一施設への予約可能数に、施設ごとの上限を設定できる機能を有すること(A施設は1人3回まで予約可。B施設は1人15回まで予約可等)。
65	手続	必須	クラウドサービスのシステムは国内のデータセンターにあること。
66	手続	必須	災害等でデータセンターが使用できなくなる事態に備えたディザスタリカバリの体制が取られていること。
67	手続	任意	クラウドサービスのシステムは同一データセンター内で冗長化されており、片方のシステム停止時はもう一方のシステムからサービス提供されること。
68	手続	任意	クラウドサービスのシステムは異なる2か所以上の立地場所もしくは電源設備が異なるデータセンターで冗長化されており、片方のデータセンター停止時はもう一方のデータセンターからサービス提供されること。

対応欄については、以下の基準で記入してください。

○：稼働開始(令和4年3月1日)までに対応可能。

△：令和4年3月末日までには対応可能だが、稼働開始(令和4年3月1日)までには対応不可。

×：対応不可(必須項目の場合、対応不可が1項目でもあると不合格)

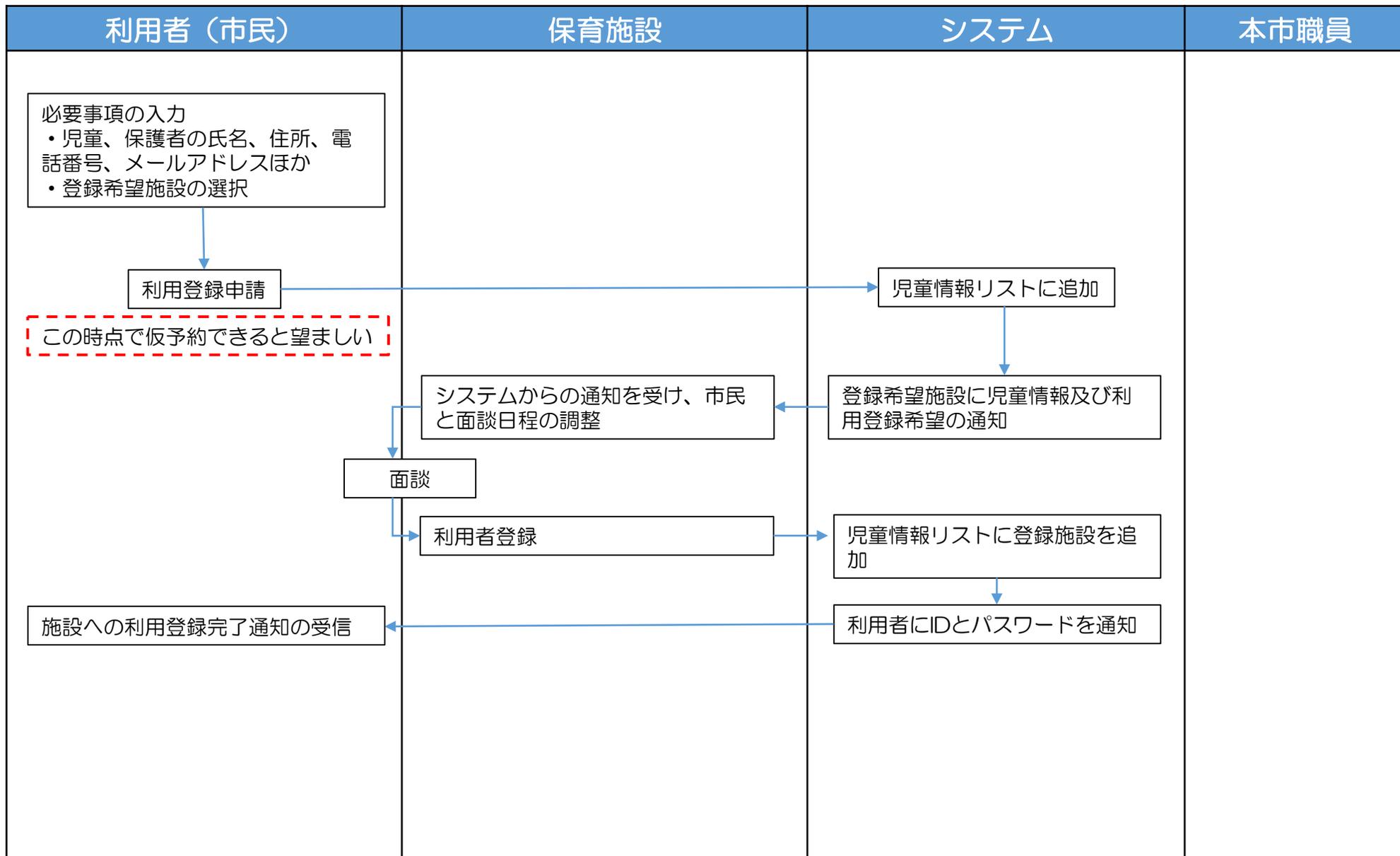
各項目について、次の通り扱うこととする。

必須項目：全項目において○または△の場合、要件を満たしていることとする。

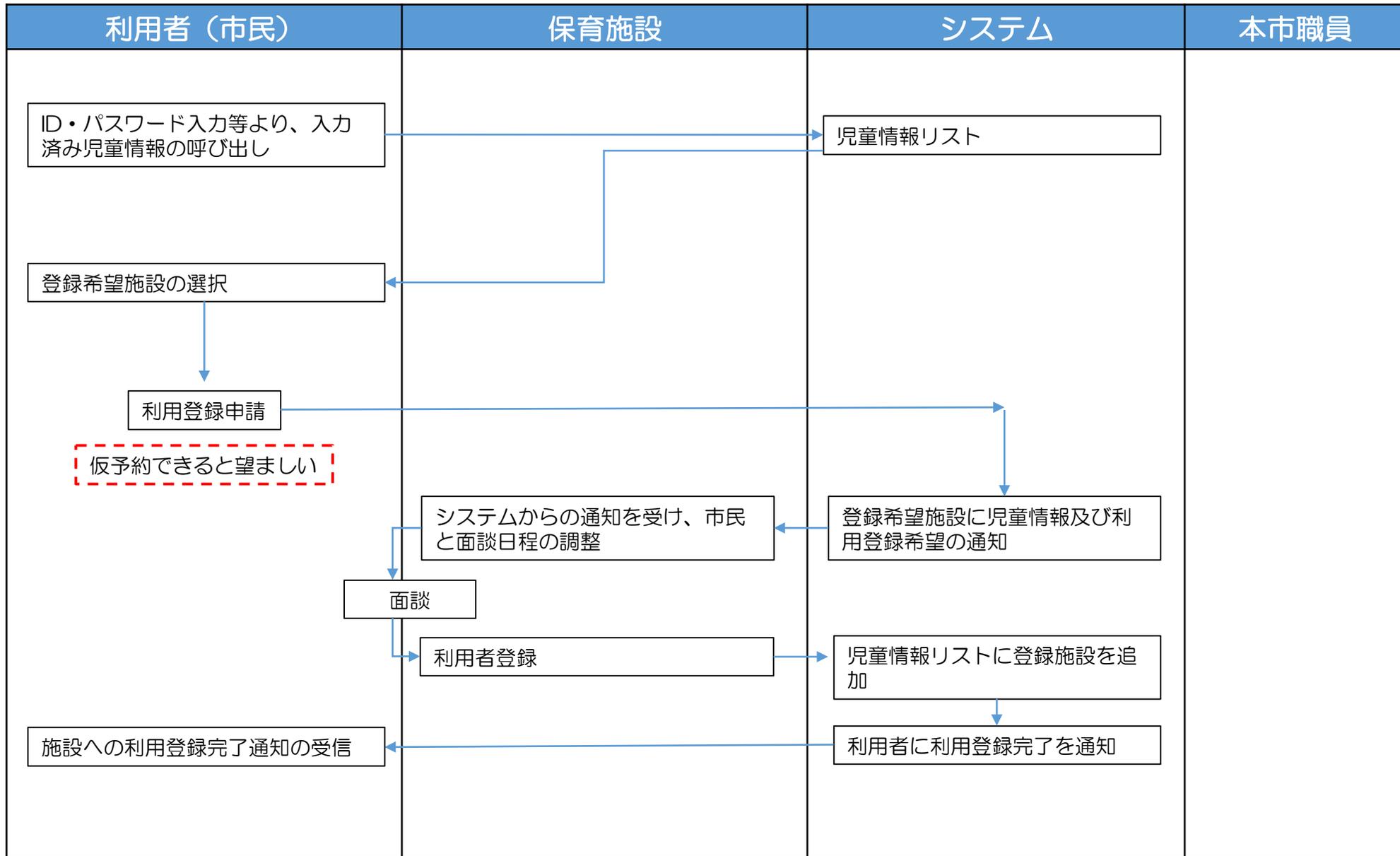
任意項目：○または△に応じて加点をし、評価対象とする。

業務フロー ※主な業務のフローを示します。設計の参考としてください。

① 施設への利用登録申請 (1施設目の登録)



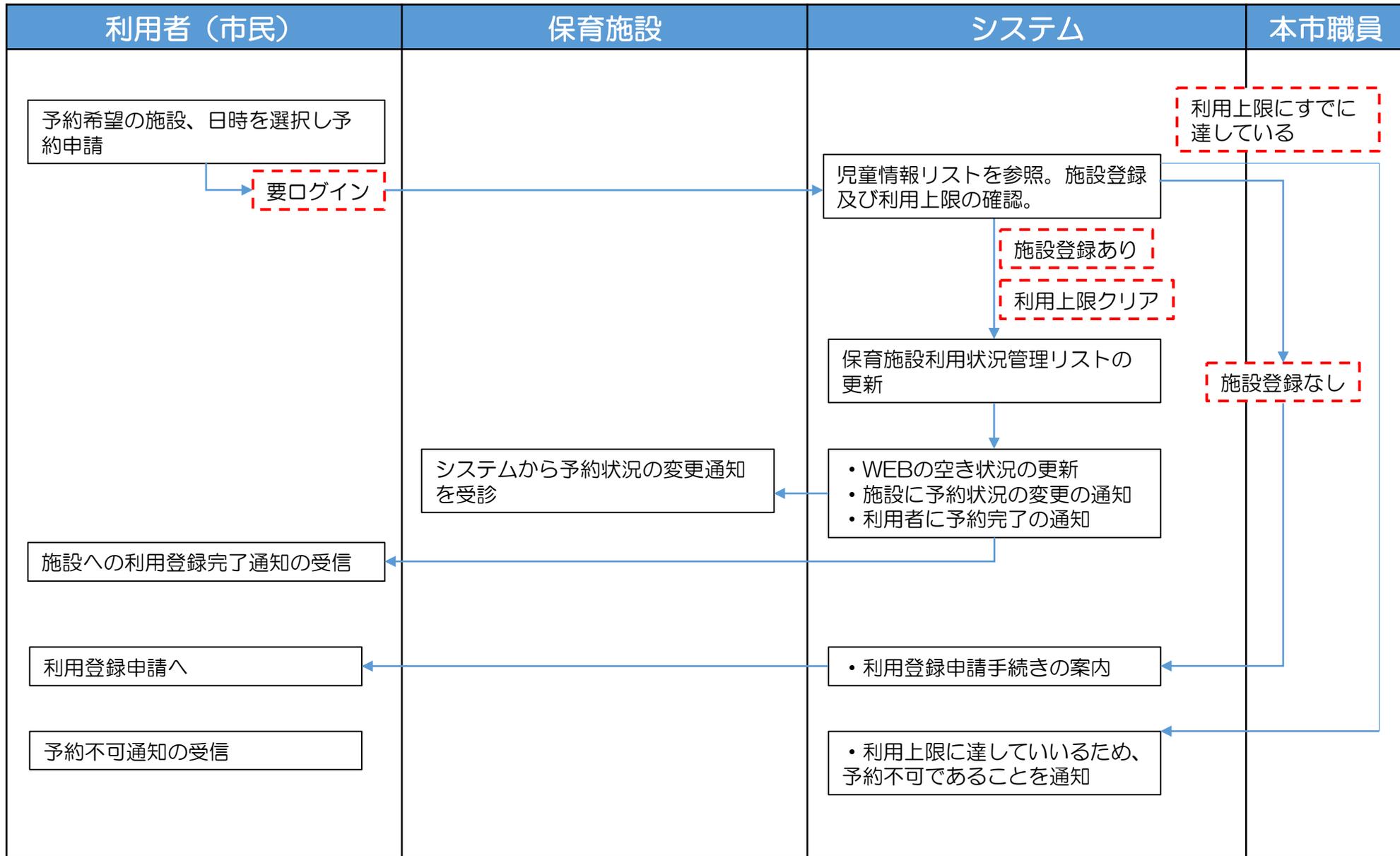
② 施設への利用登録申請 (2施設目以降の登録)



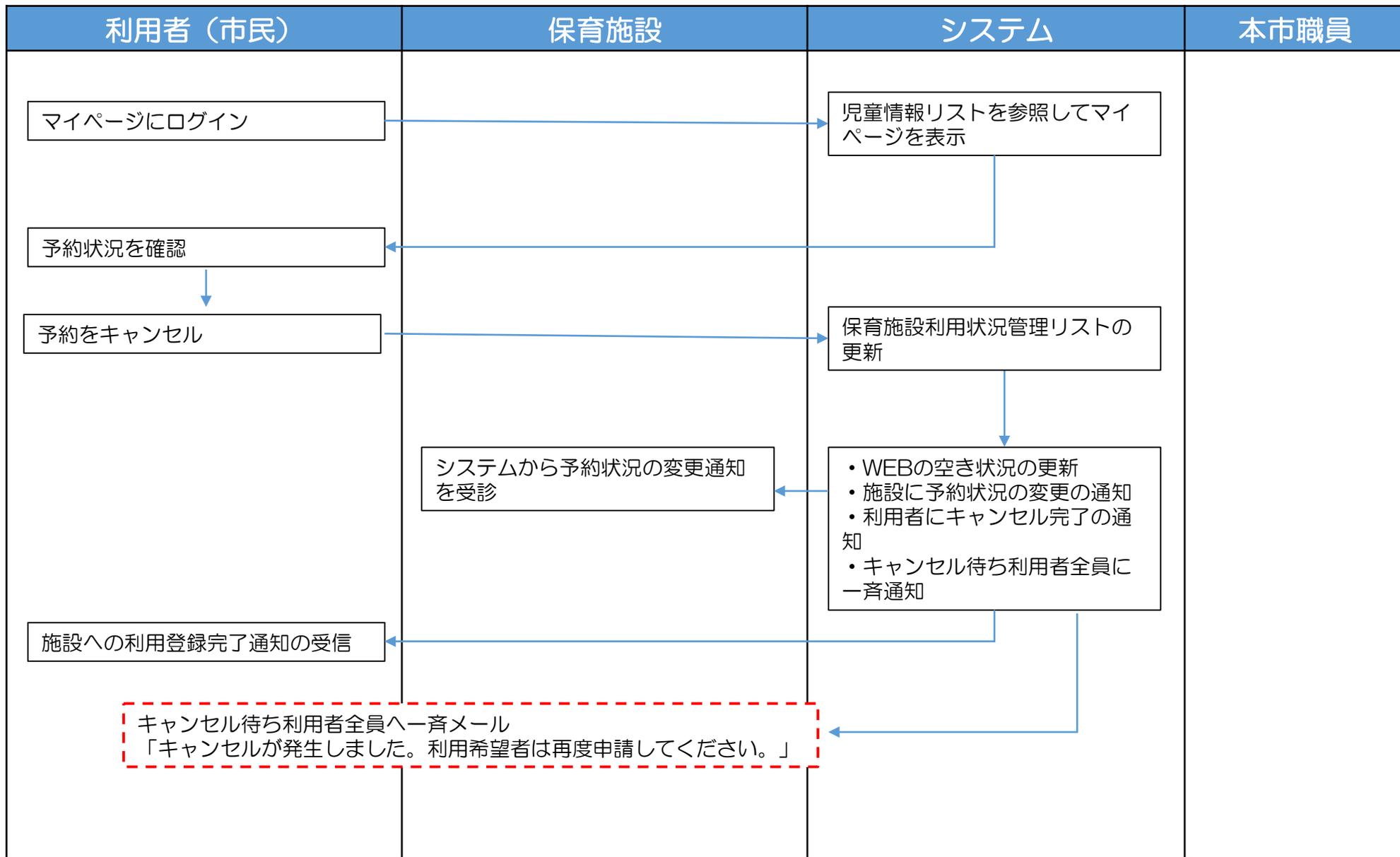
③ 空き状況の確認



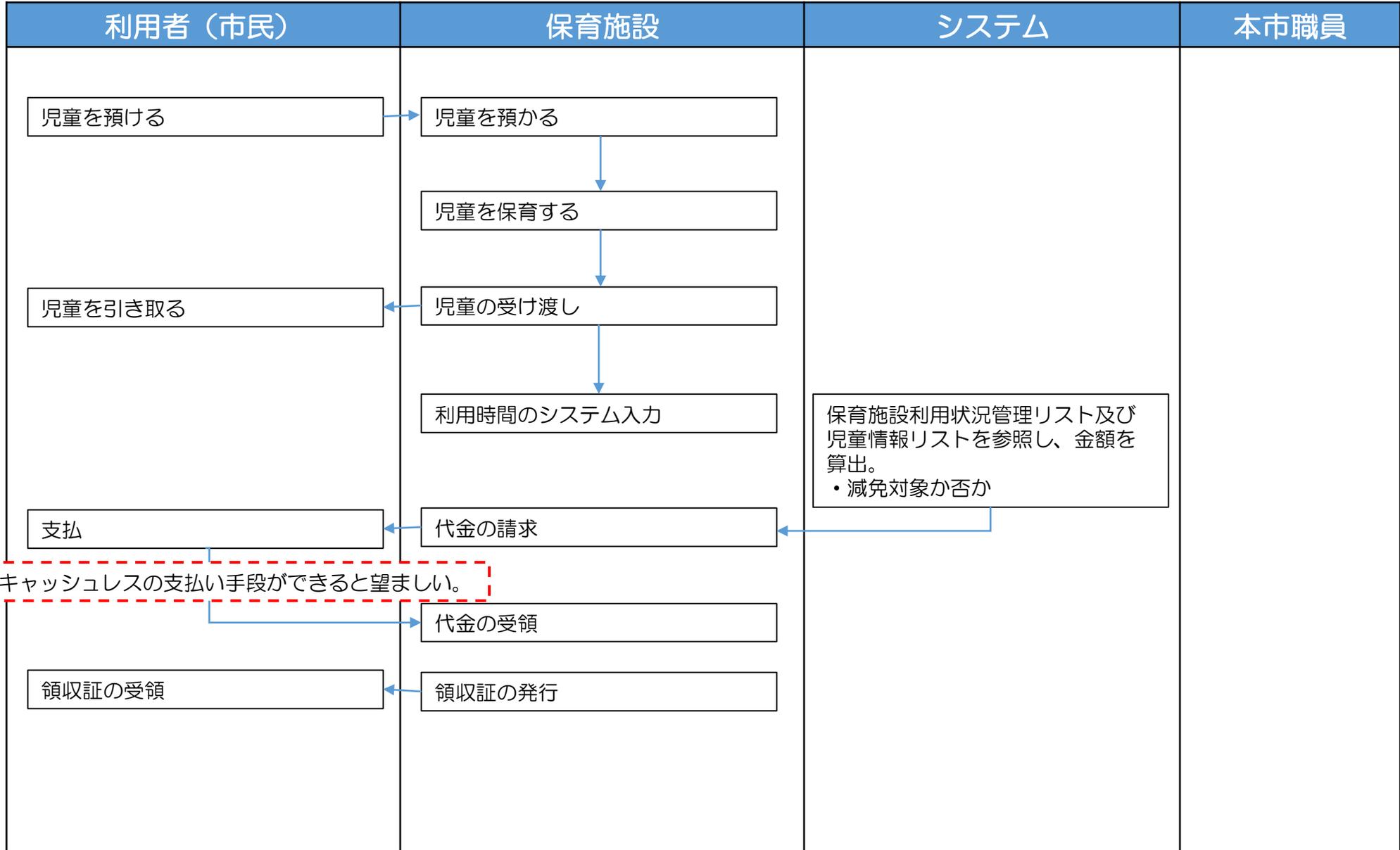
④ 予約



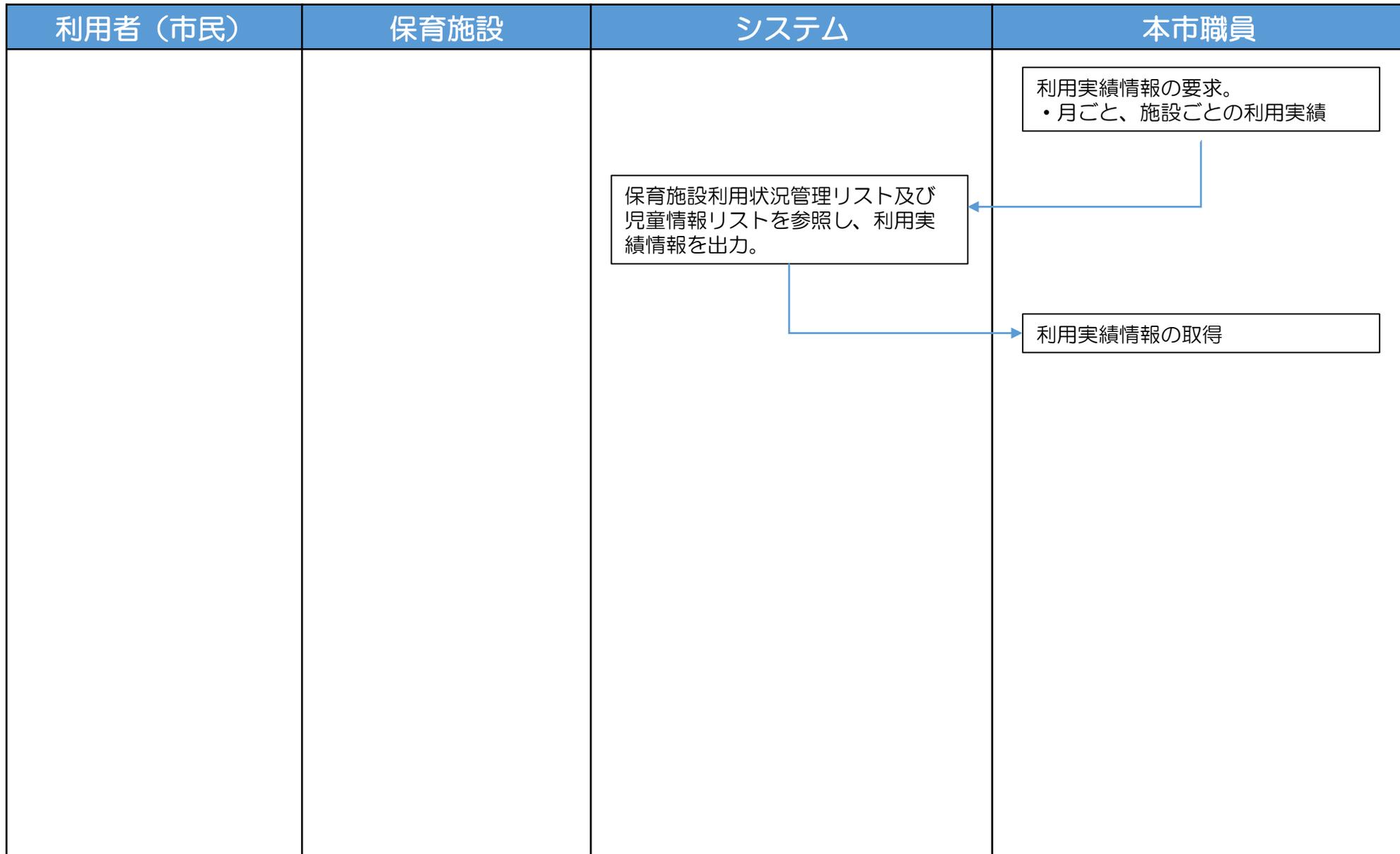
⑤ 予約のキャンセル



⑥ 児童を預ける～迎えに行く～代金の支払



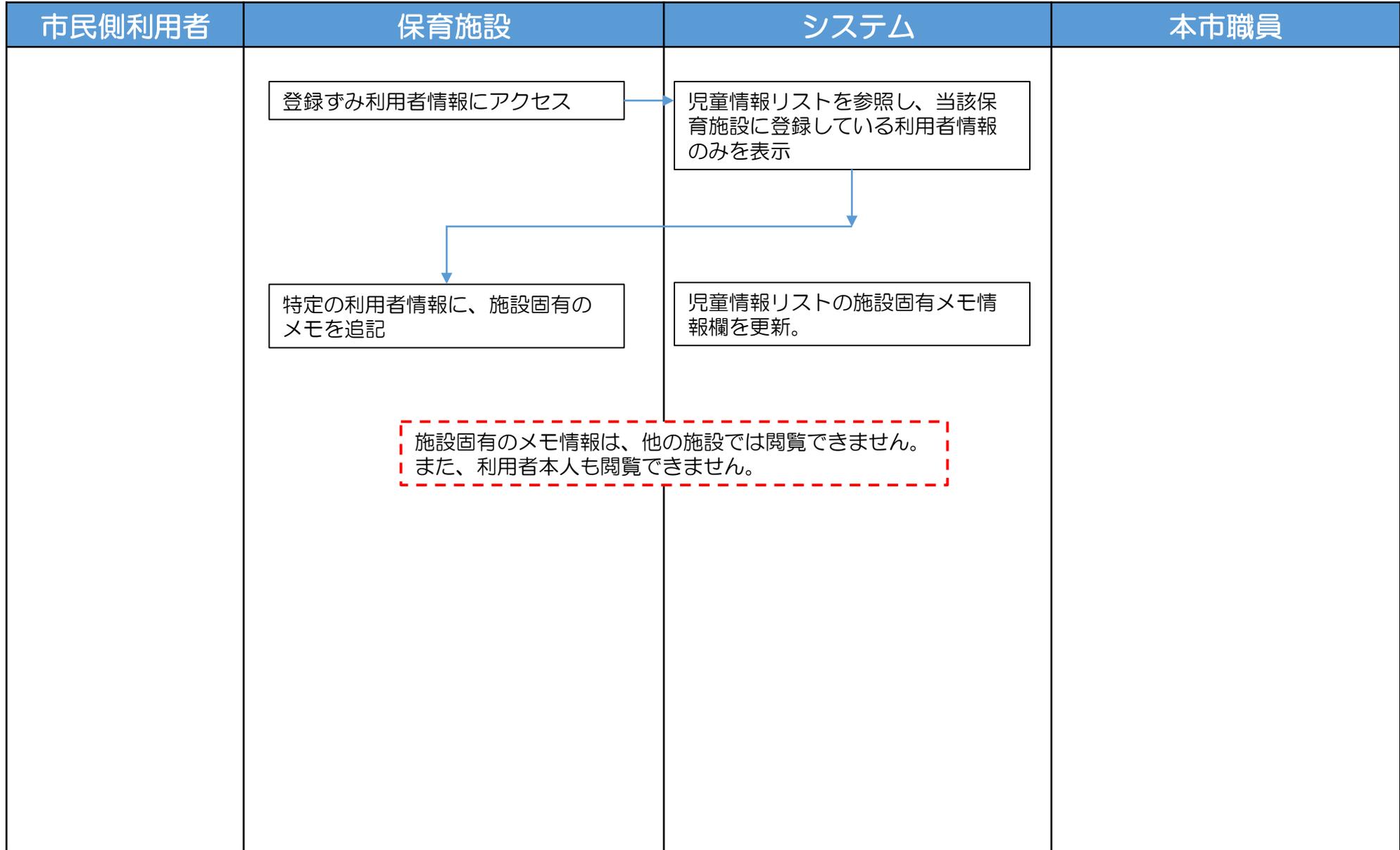
⑦ 利用実績情報の取得



⑧ 市民側利用者による利用者情報の変更（パスワード変更や、登録抹消を含む）



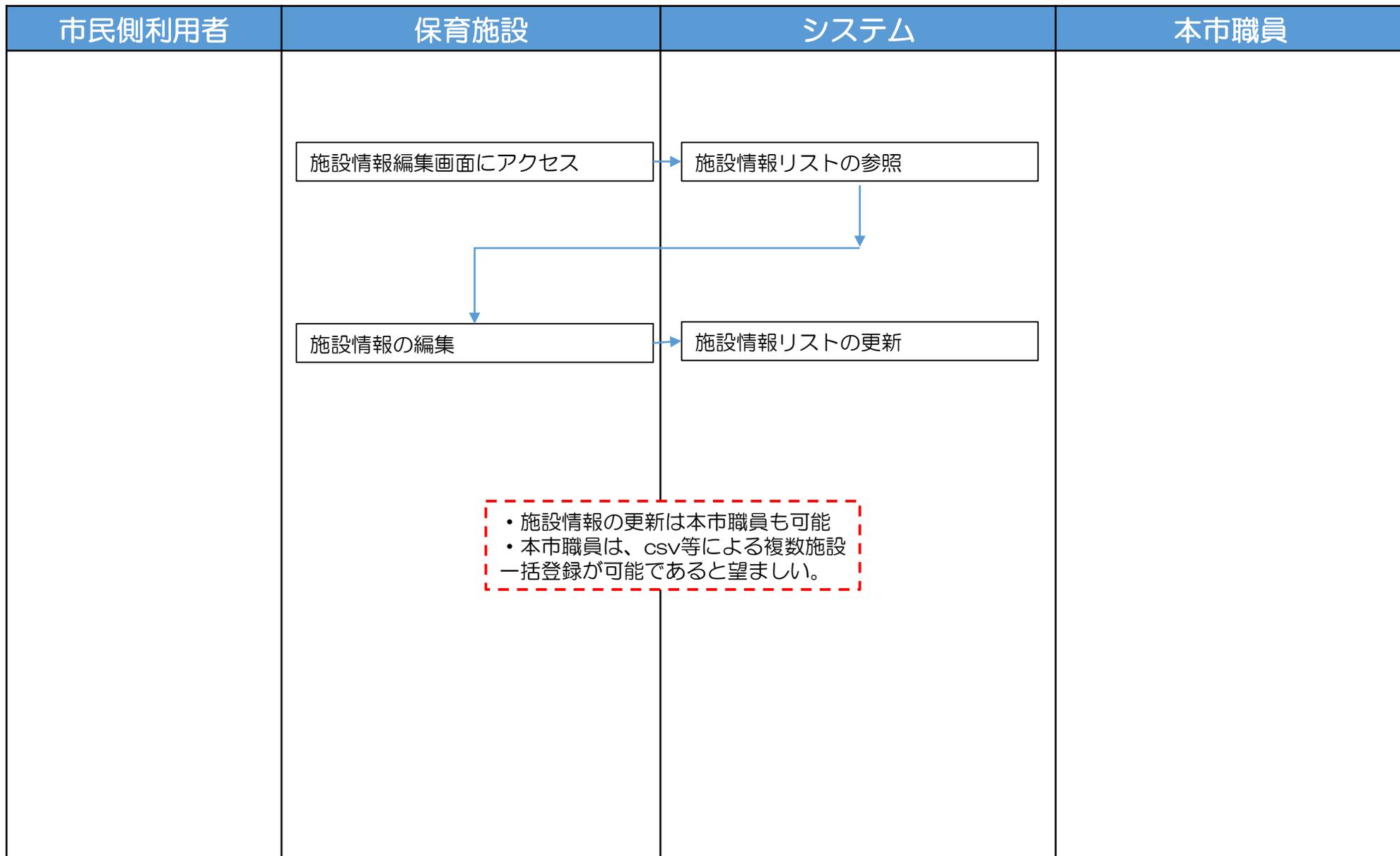
⑨ 施設側利用者による、利用者情報への追記（施設固有のメモ）



⑩ 利用者情報の自動更新

市民側利用者	保育施設	システム	本市職員
		<p>【年度更新】</p> <p>毎年4月1日に、児童情報リストを自動更新</p> <ul style="list-style-type: none"> ・6歳児の登録情報の削除 ・年齢区分の更新 (1歳児→2歳児) ・ 	
<p>減免の有効期間が間もなく切れる通知を受信</p>		<p>【定期更新（減免対象者の確認）】</p> <p>毎月1日に、児童情報リストの減免対象者情報を確認。</p> <ul style="list-style-type: none"> ・減免の有効期間が来月中に切れる利用者を抽出して、利用者へ通知 	

⑪ 施設情報の更新



令和3年度一時預かりWEB予約システムの
導入及び運用保守業務委託
基本仕様書

令和3年8月

横浜市

こども青少年局保育・教育運営課

用語の定義

本基本仕様書に記載する重要な用語を以下に示す。

本基本仕様書	「令和3年度一時預かり WEB 予約システムの導入及び運用保守業務委託基本仕様書」（本書）
一時預かり WEB 予約システム	本書で規定する WEB 予約システム（以下「本予約システム」という。）
一時預かり事業	本市の乳幼児一時預かり事業、一時保育事業、休日一時保育事業のほか、本市の地域子育て支援拠点等で実施される一時預かり事業を含む。対象事業は順次拡大する見込み。
市民側利用者	一時預かりを利用数ために、本予約システムを利用する個人の総称。
施設側利用者	本予約システムを利用する保育施設の総称。
職員側利用者	本予約システムを利用する本市職員の総称。
利用者	本予約システムを利用する市民側利用者、施設側利用者、職員側利用者を含む利用者全体の総称
管理者	手続管理やメンテナンス等、本予約システムを管理する本市職員
運用業務	令和4年3月からの本予約システム運用に係る業務

本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、将来の業務実施の条件となるものではありません。

1 目的

本市の保育施設における一時預かり事業（乳幼児一時預かり事業、一時保育事業等）については、現在、市民側利用者が各施設に空き状況を直接電話等で確認し、予約する方法が取られており、利便性に課題があります。このたび、現行の予約方法の効率化による市民サービスの向上、及び保育事業者の事務効率化を目的として、WEB 予約システムを調達します。また、今後の施設数増加への対応、施設側利用者や職員側利用者の業務効率化に資する機能の提供、運用保守も併せて実施します。

本業務委託は、現行手続から、より市民サービス向上及び業務効率化に寄与するとともに、適切なセキュリティ対策を講じた、安全性・信頼性・利便性・拡張性の高い、WEB 予約システムとすることを目的とします。

2 基本方針

- (1) 利用者はインターネットからシステムにアクセスする構成であること。
- (2) 市民側利用者が、スマートフォン、パソコンなど、多くの市民が使用するインターネット端末で一時預かりのWEB予約を行うことができること。
- (3) 将来的な利用想定量（200,000件／年の予約申請等）以上を処理できる、または拡張性を備えたシステムであること。
- (4) 利用者のUI（ユーザインターフェース）、UX（ユーザエクスペリエンス）に優れた使いやすいシステムであること。そのため、市民側利用者が探したい施設の情報を容易に見つけることが可能であること、初期登録申請の入力内容のチェックが可能であることなど、ユーザビリティに優れ、市民サービス向上に資するものであること。
さらに、市民側利用者が必要とする手続について、市民側利用者がわかりやすく簡便に検索・選択できる仕組みを備えていること。
- (5) 施設側利用者の業務効率化に寄与するシステムであること。このため、GUIによる使いやすい設計画面で予約管理や利用者管理ができる業務処理機能を有するシステムであること。
また、本市の一時預かり関連の補助金の関連様式（実績報告等）と連携機能を持つなど、施設側利用者、職員側利用者双方の業務効率化に寄与するものであること。
- (6) 既存のIaaS、PaaS、SaaS等のカスタマイズする部分については必要最低限の内容とし、不必要なカスタマイズは避けること。または、カスタマイズではなくIaaS、PaaS、SaaSの標準サービスとして反映し提供すること。
- (7) 適切なセキュリティ対策を講じた、安全性・信頼性・可用性の高いサービスが提供できるシステムとすること。
- (8) OSやブラウザなどの利用者環境が拡大された際に、システムへの対応は保守内で行えること。
- (9) 運用業務では、職員側利用者からの問合せ、障害報告の受付・対応等を行うこと。市民側利用者から受ける「よくある質問」を、職員側利用者がFAQに掲載できるなど、利用者支援の仕組みを備えていること。

3 運用形態

事業者が本予約システムの機能をネットワーク経由して提供するサービス（SaaS）またはIaaS、PaaS等のクラウドプラットフォームにて構築されたサービスを利用する。

4 全体スケジュール

令和3年度に、一部施設（乳幼児一時預かり事業29施設）における本予約システムの導入、試行、システム改善を行い、令和4年度中に対象施設を拡大（一時保育事業約500施設の一部、休日一時保育事業約8施設）した本格稼働を行うことを基本とする。

以下にスケジュール案を示すが、詳細な日程については受託者及び委託者との協議により決定する。

(1) システム開発作業

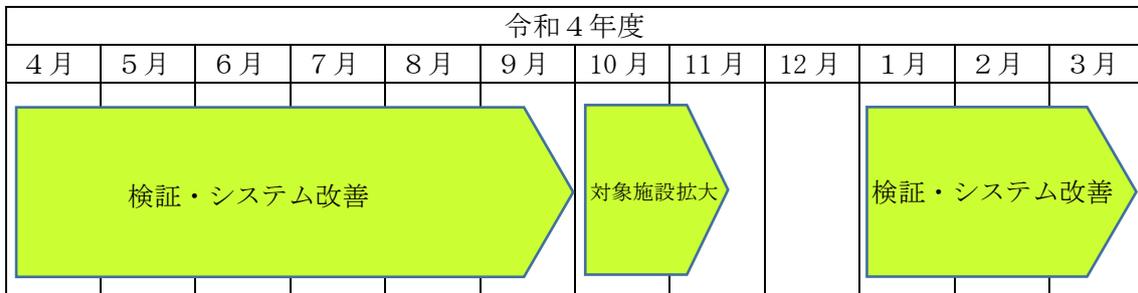
令和3年11月から令和4年2月まで

(2) 試行運用、システム改善期間（運用保守業務開始）

令和3年3月1日から

(4) 対象施設拡大、本格稼働、

令和4年10月から



5 サービス要件

(1) 機能

別紙「機能要件一覧」の必須項目の機能を実現できること。また、任意項目の機能についても可能な限り実現すること。

(2) アクセシビリティ

利用者のインターフェイスは、アクセシビリティに配慮して、利用しやすいものとする。

別紙「アクセシビリティ要件」の対応を行うこと。

(3) 保守性・将来性

ア OS、ブラウザのバージョンアップ（サービスパック等を含む）に迅速に対応すること。

イ システムのエンハンス（機能改善）を無償で行うこと。

ウ システム改修等を実施した場合は、随時、変更内容を反映した操作マニュアル及びサービス仕様書等の資料を提供すること。

エ システムデータ及び利用者情報のデータ、利用者のログインや予約に関するデータなど、システム再構築・再稼働に必要なデータのバックアップを行うこと。

オ カスタマイズ、追加機能等の開発においてはシステム固有の言語ではなく、Openな言語（JavaScriptなどの一般言語）が活用できる環境であること。

(4) セキュリティ

- ア 市民側利用者機能に認証機能を持ち、申請等の情報を送受信する際にはSSL等を利用し、通信経路の暗号化を行う。
- イ システムのセキュリティ対策及び障害対策のための情報提供及び修正モジュール等の適用を無償で行うこと。
- ウ システムには、十分な個人情報保護対策及び情報セキュリティ対策を行うこと。
- エ 市民側利用者の個人情報を蓄積するデータベース部分は、他の契約者と共有せず、論理的に独立性を保持すること。
- オ システムの運用状況を監視し、障害を迅速に発見して対策が取れること。
- カ ファイアウォール、ウィルス対策ソフト、ソフトウェア脆弱性対策等、外部からの攻撃に対するセキュリティ対策が施されていること。
- キ ネットワーク構成等の外部からの攻撃目標となり得る情報が漏れないよう対策を取ること。
- ク 本市の承認なしに、利用者情報のデータにアクセスしないこと。
- ケ 利用者（市民、施設及び職員）のアクセスログの開示ができること。

(5) ネットワーク

- 利用者はインターネット接続によりサービスを利用できること。

(6) プロジェクト運用

- ア 導入のスケジュール及び実施方法を明確にし、委託者に紙面または電子ファイルの形式で提出すること。
- イ マイルストーンごとに本市に対して報告を行うこと。
- ウ テスト環境で十分にテストを行った上で、本番環境への移行を行うこと。

(7) 運用支援

- 職員側利用所の運用支援を行うこと。

(8) 職員研修、マニュアルの整備

- ア 市民側利用者、施設側利用者、職員側利用者それぞれの操作に応じたマニュアルをデータで整備すること。
- イ 職員側利用者に対して、市民側利用者、施設側利用者部分を含む本予約システム全般の操作説明を実施すること。

(9) サービスレベル

- ア 本予約システムの運用については、受託者及び委託者が、SLA契約を締結し、それに従い実施すること。
- イ SLAの内容については、年度毎に評価を実施し、見直しを行うものとする。

(10) その他

- ア 最新の技術等を積極的に採用してサービス向上に努めること。
- イ 明記していない事項について疑義が生じた場合は、受託者及び委託者で協議して決定すること。
- ウ 別システムへ移行となった際には、必要とする資産（手続様式やデータベースなど）についての情報を無償で提供し、移行作業に協力すること。

6 参考データ

本市での一時預かりの利用状況の想定件数を以下に示します。サービス提供の内容は以下の直近の施設数や利用状況及び令和3年度以降の想定施設数や利用状況を考慮して提案してください。

(1) 施設数

事業名	R2年	R3年	R4年
乳幼児一時預かり事業	25	29	32
一時保育	500	500	500
休日一時保育	8	8	8

(2) 利用者数（延べ）

事業名	R1年	R3年	R4年
乳幼児一時預かり事業	85,000	110,000	125,000
一時保育	110,000	110,000	110,000
休日一時保育	1400	1500	1600

※R2年の利用者数は新型コロナウイルスの影響が大きいため参照せず。

(3) 職員側利用者数

こども青少年局 保育・教育運営課 3名
保育・教育給付課 3名

7 データ移行

(1) 対象データ

ア 利用者情報

各施設が保有する市民側利用者の情報

- ・項目は保護者名、児童名、住所等の個人情報。本予約システムの利用者情報の登録形式によります。
- ・想定件数：約20,000件
- ・データの入力は市民側利用者が直接入力することを原則とするが、施設側利用者が、CSV等による一括の入力を行うことも可能とすること。

イ 施設情報

各施設の基本情報

- ・項目は施設名、開所時間、URL、写真などの基本情報。本予約システムの利用者情報の登録形式によります。
- ・データの入力は施設側利用者が直接入力することを原則とするが、職員側利用者が、CSV等による一括の入力を行うことも可能とすること。

(2) 移行支援

施設側利用者や職員側利用者がデータ移行作業を行うにあたり、移行作業が円滑に行えるよう支援すること。（例：職員が移行作業を行う際のマニュアル作成や問合せ対

応を行うなど)

8 マニュアルの整備

市民側利用者、施設側利用者及び職員側利用者が、システムの機能を理解し、操作方法等を習得するため、各々の操作内容や業務内容に応じたマニュアルを整備すること。

9 利用者サポート

利用者からの問合せ、障害報告等は職員側利用者が受けます。職員側利用者からの対応相談、障害報告等を受け付ける体制を整備すること。

10 運用報告

運用業務では、毎月、前月分の運用実績概要を本市に報告すること。本報告については、報告資料は電子ファイルの形式で提出すること。

また、定期的に本市からの機能改善などの要望をくみ取る仕組みを設けること。

以下に報告内容の案を示すが、詳細な内容については受託者及び委託者との協議により決定する。

(1) 本予約システム利用件数

ア 閲覧件数（ページ別件数、総件数）

イ 利用件数（手続別件数、総件数）

(2) S L Aに関する報告

ア S L Aの達成状況

イ 障害報告

(3) システム運用報告

ア 計画停止

イ 機能改善・機能改修

ウ 保守作業等

11 その他

(1) 次に掲げる認定を受けていること。または、認定に相当する体制構築・運用を行い、可能な限り早期に認定を受けること。

ア プライバシーマークの付与認定を受けていること。なお、会社の一部門が認定を受けていれば良い。ただし、当該部門が本業務に適切に携わる体制を構築すること。

イ 情報セキュリティマネジメント（I SMS）の認証（J I S Q27001、I S O / I E C27001）の認証を受けていること。なお、会社の一部門が認定を受けていれば良い。ただし、当該部門が本業務に適切に携わる体制を構築すること。

(2) セキュリティは別添の「一時預かり WEB 予約システムのW e bアプリケーションセキュリティに係る特記仕様書」に準拠したものであること。

(3) 受託者は、別添の「委託契約約款」、「個人情報取扱特記事項」及び「電子計算機処理等の契約に関する情報取扱特記事項」に記載される事項を遵守すること。

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る。

(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

ア 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。

イ (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

ア 「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。

イ 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。

ウ 試験内容については、発注者に説明し、承認を得ること。

エ 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。なお、40 ページの中には次のページを含めること。

■ 試験を必ず実施するページ

- ・ トップページ
- ・ サブディレクトリ直下の代表ページ(sub-content/index.html 等)
- ・ アクセシビリティに関連するページ
- ・ 利用者から問い合わせを受けるウェブページ（存在する場合）

(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。

ア 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。

イ 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) ウェブアクセシビリティ方針及び試験結果のページの作成・公開について

ア ウェブアクセシビリティ方針及び試験結果のページの作成について

「(3)」で策定したウェブアクセシビリティ方針のページを作成すること。また、「(6) ア」で作成した達成基準チェックリストを基に、試験結果のページを作成すること。

イ ウェブアクセシビリティ方針及び試験結果のページの公開について

「(8) ア」で作成したページを公開すること。なお、ウェブアクセシビリティ方針のページは、当該サイトの全画面から 2 クリック以内にたどりつけるよう、フッター等にリンクを配置すること。

※ パッケージシステムの仕様等により各画面に任意のリンクを設置できない場合は、当該システムの利用方法等を示したページや利用者向けマニュアル等にリンクを配置すること。

2 参考ページ

(1) JIS 検索

本ウェブページで「JIS X 8341-3」を検索すると規格の閲覧ページに遷移できます。

<https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html>

(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

(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

一時預かりWEB予約システムの
Web アプリケーションセキュリティに係る
特記仕様書

横浜市こども青少年局子育て支援部
保育・教育運営課

1 基本事項

本特記仕様書（以下「本書」という。）は、本市が導入する一時預かりWEB予約システム（以下「本システム」という。）の基本仕様書に加え、本システムに追加で求めるセキュリティ要件、対応指針を記載するものである。受託者は本書に従わなくてはならない。

なお、本書に記載のないセキュリティ要求仕様に関しては基本仕様書による。

2 保守性・運用性要件

システムのプラットフォームソフトウェア（OS、ミドルウェア、ソフトウェア部品（ライブラリ等）を指す。）及びWebアプリケーションソフトウェア（パッケージWebアプリケーションを含み、以下「Webアプリケーション」という。）は次の要件を満たすこと。また、一部要件を満たせない場合の方法については要件の記述に従うこと。

(1) 情報資産（ソフトウェア、データ等）に対して、次に掲げる情報セキュリティ対策を実施しなければならない。

ア インターネットを経由したサイバー攻撃のリスクを放置してはならない。

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なければならない。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 特権のアクセス権を用いて利用する機能について、当該権限を有するID及びその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なければならない。

エ 脆弱性を利用したサイバー攻撃の情報を常に入手し、リスクの大きさに応じて緊急に対応できる体制をとらなければならない。

オ 運用期間において、毎年本市が実施するセキュリティ診断によって発見された脆弱性について対応すること。

(2) 契約終了時や記憶媒体の廃棄等を実施する場合、次に掲げる措置を実施しなければならない。

ア データの復元が困難な状態とした上で、データを確実に消去した証明を提出すること。

イ 証明と合わせて、作業日時、作業者及び確認者等、データ消去作業が確実に行われたことを担保する作業記録を提出すること。

3 Webアプリケーション脆弱性対応

本システムにおけるWebアプリケーションの脆弱性対応として、『別紙 ウェブアプリケーションのセキュリティ実装リスト』（以下「実装リスト」という）の脆弱性が本システムに混入しないように、少なくとも「対策の性質」欄が「根本的解決」となっている実施項目の対策を実施すること。

参考：IPA 安全なウェブサイトの作り方

<https://www.ipa.go.jp/security/vuln/websecurity.html>

4 検収

『別紙 ウェブアプリケーションのセキュリティ実装リスト』の記入提出及び当該脆弱性の対応がされていることについて、受託者の提出する検査報告書をもって検査する。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト (1/3)

No	脆弱性の種類	対策の性質	チェック	実施項目	解説
1	SQLインジェクション	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> SQL文の組み立ては全てプレースホルダで実装する。	1-(i)-a
				<input type="checkbox"/> SQL文の構成を文字列連結により行う場合は、アプリケーションの変数をSQL文のリテラルとして正しく構成する。	1-(i)-b
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	ウェブアプリケーションに渡されるパラメータにSQL文を直接指定しない。	1-(ii)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	エラーメッセージをそのままブラウザに表示しない。	1-(iii)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	データベースアカウントに適切な権限を与える。	1-(iv)
2	OSコマンド・インジェクション	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> シェルを起動できる言語機能の利用を避ける。	2-(i)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。	2-(ii)
3	パス名パラメータの未チェック/ ディレクトリ・トラバーサル	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> 外部からのパラメータでウェブサーバ内のファイル名を直接指定する実装を避ける。	3-(i)-a
				<input type="checkbox"/> ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする。	3-(i)-b
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	ウェブサーバ内のファイルへのアクセス権限の設定を正しく管理する。	3-(ii)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	ファイル名のチェックを行う。	3-(iii)
4	セッション管理の不備	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	セッションIDを推測が困難なものにする。	4-(i)
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	セッションIDをURLパラメータに格納しない。	4-(ii)
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	HTTPS通信で利用するCookieにはsecure属性を加える。	4-(iii)
		根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> ログイン成功後に、新しくセッションを開始する。	4-(iv)-a
				<input type="checkbox"/> ログイン成功後に、既存のセッションIDとは別に秘密情報を発行し、ページの遷移ごとにその値を確認する。	4-(iv)-b
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	セッションIDを固定値にしない。	4-(v)
保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	セッションIDをCookieにセットする場合、有効期限の設定に注意する。	4-(vi)		

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト (2/3)

No	脆弱性の種類	対策の性質	チェック	実施項目	解説	
5	クロスサイト・スクリプティング	HTMLテキストの入力を許可しない場合の対策	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	ウェブページに出力する全ての要素に対して、エスケープ処理を施す。	5-(i)
			根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	URLを出力するときは、「http://」や「https://」で始まるURLのみを許可する。	5-(ii)
			根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<script>...</script> 要素の内容を動的に生成しない。	5-(iii)
			根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	スタイルシートを任意のサイトから取り込めるようにしない。	5-(iv)
			保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	入力値の内容チェックを行う。	5-(v)
	HTMLテキストの入力を許可する場合の対策	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	入力されたHTMLテキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。	5-(vi)	
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	入力されたHTMLテキストから、スクリプトに該当する文字列を排除する。	5-(vii)	
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	HTTPレスポンスヘッダのContent-Typeフィールドに文字コード(charset)の指定を行う。	5-(viii)	
	全てのウェブアプリケーションに共通の対策	保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	Cookie情報の漏えい対策として、発行するCookieにHttpOnly属性を加え、TRACEメソッドを無効化する。	5-(ix)	
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	クロスサイト・スクリプティングの潜在的な脆弱性対策として有効なブラウザの機能を有効にするレスポンスヘッダを返す。	5-(x)	
6	CSRF (クロスサイト・リクエスト・フォージェリ)	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> 処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。	6-(i)-a	
				<input type="checkbox"/> 処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	6-(i)-b	
				<input type="checkbox"/> Refererが正しいリンク元かを確認し、正しい場合のみ処理を実行する。	6-(i)-c	
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	重要な操作を行った際に、その旨を登録済みのメールアドレスに自動送信する。	6-(ii)	
7	HTTPヘッダ・インジェクション	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用APIを使用する。	7-(i)-a	
				<input type="checkbox"/> 改行コードを適切に処理するヘッダ出力用APIを利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。	7-(i)-b	
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	外部からの入力の全てについて、改行コードを削除する。	7-(ii)	

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト (3/3)

No	脆弱性の種類	対策の性質	チェック	実施項目	解説
8	メールヘッダ・インジェクション	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> メールヘッダを固定値にして、外部からの入力はずべてメール本文に出力する。	8-(i)-a
				<input type="checkbox"/> ウェブアプリケーションの実行環境や言語に用意されているメール送信用APIを使用する(8-(i)を採用できない場合)。	8-(i)-b
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	HTMLで宛先を指定しない。	8-(ii)
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	外部からの入力の全てについて、改行コードを削除する。	8-(iii)
9	クリックジャッキング	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限する。	9-(i)-a
				<input type="checkbox"/> 処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	9-(i)-b
		保険的対策	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	重要な処理は、一連の操作をマウスのみで実行できないようにする。	9-(ii)
10	バッファオーバーフロー	根本的解決	※ <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input type="checkbox"/> 直接メモリにアクセスできない言語で記述する。	10-(i)-a
				<input type="checkbox"/> 直接メモリにアクセスできる言語で記述する部分を最小限にする。	10-(i)-b
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	脆弱性が修正されたバージョンのライブラリを使用する。	10-(ii)
11	アクセス制御や認可制御の欠落	根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	アクセス制御機能による防御措置が必要とされるウェブサイトには、パスワード等の秘密情報の入力を必要とする認証機能を設ける。	11-(i)
		根本的解決	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人になりすましてアクセスできないようにする。	11-(ii)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。