「大阪くらしの今昔館」市民ボランティア「町家衆」

参考資料e

大阪くらしの今昔館は、市民ボランティアによる自発的な活動によって、江戸時代の町並みに活気と賑わいを創り出し、生きた博物館活動をめざしている。ボランティアは自ら「町家衆」を名乗って様々なイベントを行い、町家衆と館が車の両輪となって多彩な催しを行い、今昔館の賑わいを創出している。

「町家衆」は、ミュージアムが主催する紙芝居の上演やもちつきなど、各種イベントの準備・運営、江戸時代の町家を案内する「町家ツアー」等を行っている。

ボランティアの養成、登録については、住むまちとしての大阪の歴史と魅力を学ぶ養成講座を毎年開催し、修了者のうち希望者をボランティアとして登録している。

(令和５年３月現在１７６名)

ボランティア養成講座

ボランティア研修

おじゃみ（お手玉）づくり

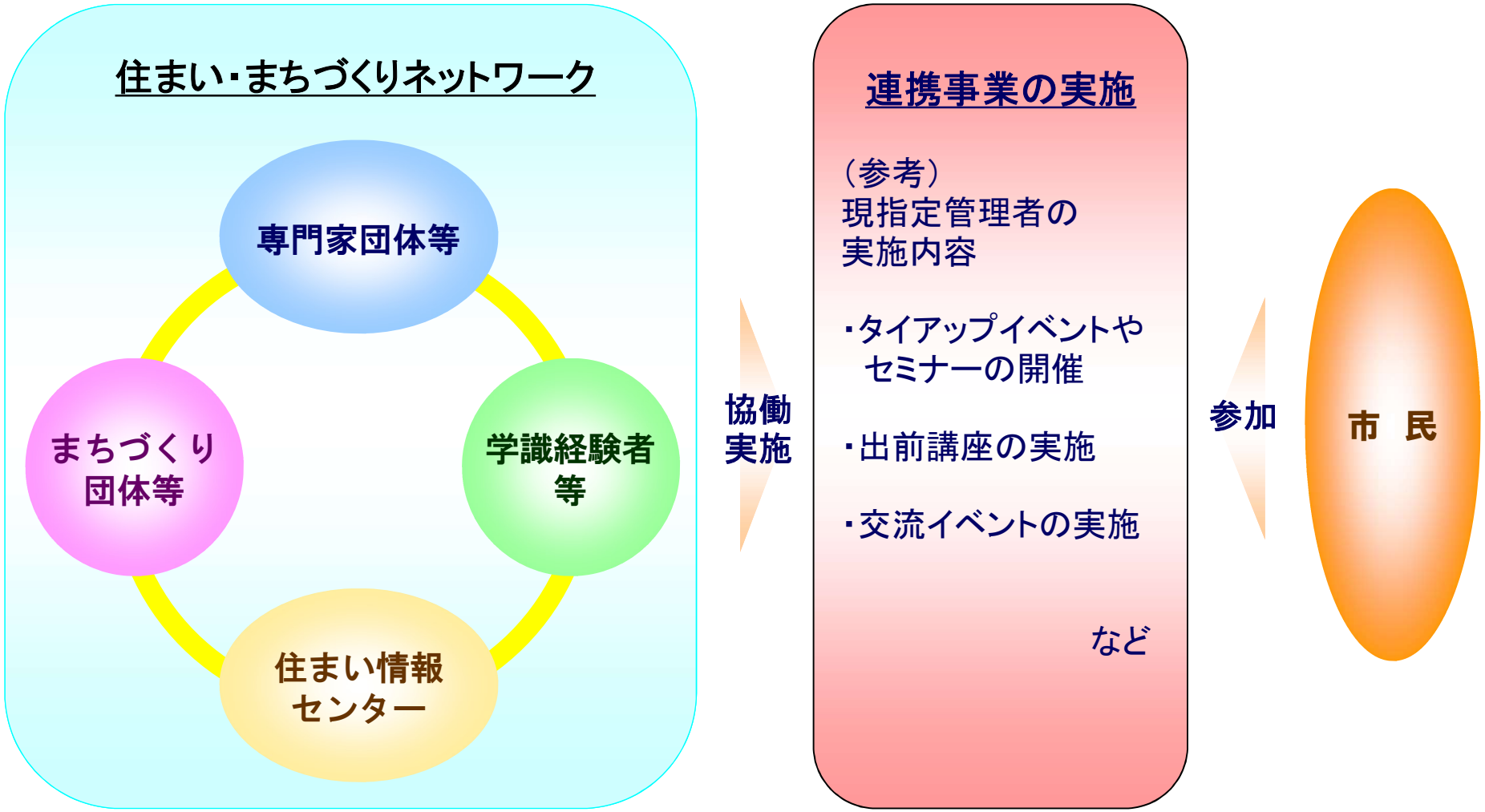
南京玉すだれ

町家ツアー

住まい・まちづくりネットワーク事業

参考資料f

住まい・まちづくりに取り組む専門家団体やNPO等と連携し、団体等の持つノウハウ等を活用することにより、相談・情報提供の充実や、居住地魅力の向上を図ることを目的とした事業



大阪市住まい情報センター管理運営システム　情報セキュリティ実施手順

都市整備局企画部住宅政策課（住宅政策グループ）

１．目的・対象範囲

（１）目的

この情報セキュリティ実施手順（以下「実施手順」という。）は、大阪市情報セキュリティ管理規程及び情報セキュリティ対策基準（以下「ポリシー」という。）に基づき、都市整備局企画部住宅政策課（住宅政策グループ）が所管する大阪市住まい情報センター管理運営システム（以下「システム」という。）における情報セキュリティを確保するために実施すべき具体的な対策をまとめたものであり、システムが保有する情報資産を保護することを目的とする。

（２）対象範囲

ア　情報資産

大阪市立住まい情報センター（以下「センター」という。）に設置するシステムに関係するハードウェア・ソフトウェア及びシステムで取り扱う全ての情報資産

イ　対象者

・システムを開発・管理する本市職員及びシステムを利用する外部委託事業者（センターの指定管理者）の職員（以下「職員」という。）

・システムを保守する外部委託事業者（保守業者）

２．管理・連絡体制

（１）管理体制

本システムにおける体制及び役割は次のとおりとする。(表１　管理体制一覧表参照)

ア　業務管理者（大阪市情報セキュリティ対策基準６（2）①）

(ｱ) 業務管理者は、住宅政策課長が担当し、システムの開発及び運用、保守の実施並びに管理を担う。

(ｲ) 副業務管理者は、住宅政策課長代理が担当し、業務管理者が不在かつ緊急の際には権限を代行する。

イ　サーバ等管理者（大阪市情報セキュリティ対策基準６（2）②）

(ｱ) サーバ等管理者は、住宅政策課長が担当し、システムが正常に稼働するよう、安全性に十分配慮し適切な稼働管理を担う。

(ｲ) 副サーバ等管理者は、住宅政策課長代理が担当し、サーバ等管理者が不在かつ緊急の際には権限を代行する。

ウ　端末機管理者　（大阪市情報セキュリティ対策基準６（2）③）

端末機管理者は、住宅政策課長が担当し、円滑に業務処理が実施されるようシステムの利用管理及び端末機等の運用管理を担う。

エ　システム運用管理責任者

システム運用管理責任者は、業務管理者（兼サーバ等管理者、端末機管理者）が指定管理者の統括責任者の中から任命し、サーバ等及び端末機の日常的な運用管理を代行する。

オ　局等情報通信ネットワーク管理責任者（大阪市情報セキュリティ対策基準６（3）②）

局等情報通信ネットワーク管理責任者は、住宅政策課長が担当し、局等情報通信ネットワークの整備及び運用管理を担う。

カ　情報セキュリティ責任者（大阪市情報セキュリティ対策基準６（1）⑤）

情報セキュリティ責任者は、住宅政策課長が担当し、住宅政策課（住宅政策グループ）及びセンターにおける情報資産の情報セキュリティに関する権限及び責任を有する。

（表１）　管理体制一覧表

管理体制	管理者役職	備考
業務管理者	住宅政策課長	副業務管理者は住宅政策課長代理
サーバ等管理者	住宅政策課長	副サーバ等管理者は住宅政策課長代理
端末機管理者	住宅政策課長	
システム運用管理責任者	運用管理代行の命を受けた 指定管理者の統括責任者	
局等情報通信ネットワーク 管理責任者	住宅政策課長	
情報セキュリティ責任者	住宅政策課長	

（２）連絡体制

本システムにおける、障害・侵害時の対応は次のとおりとする。（図１　連絡体制図参照）

ア　システムを利用する職員は、システムに関する障害（以下「障害」という。）及び不正行為等による情報の漏えい、滅失、改ざん等の侵害事案（以下「侵害」という。）を発見した場合、システム運用管理責任者に報告し、報告を受けたシステム運用管理責任者は端末機管理者（兼業務管理者）に報告する。

イ　障害や侵害を発見したシステムを管理する職員は、サーバ等管理者（兼業務管理者）に報告する。

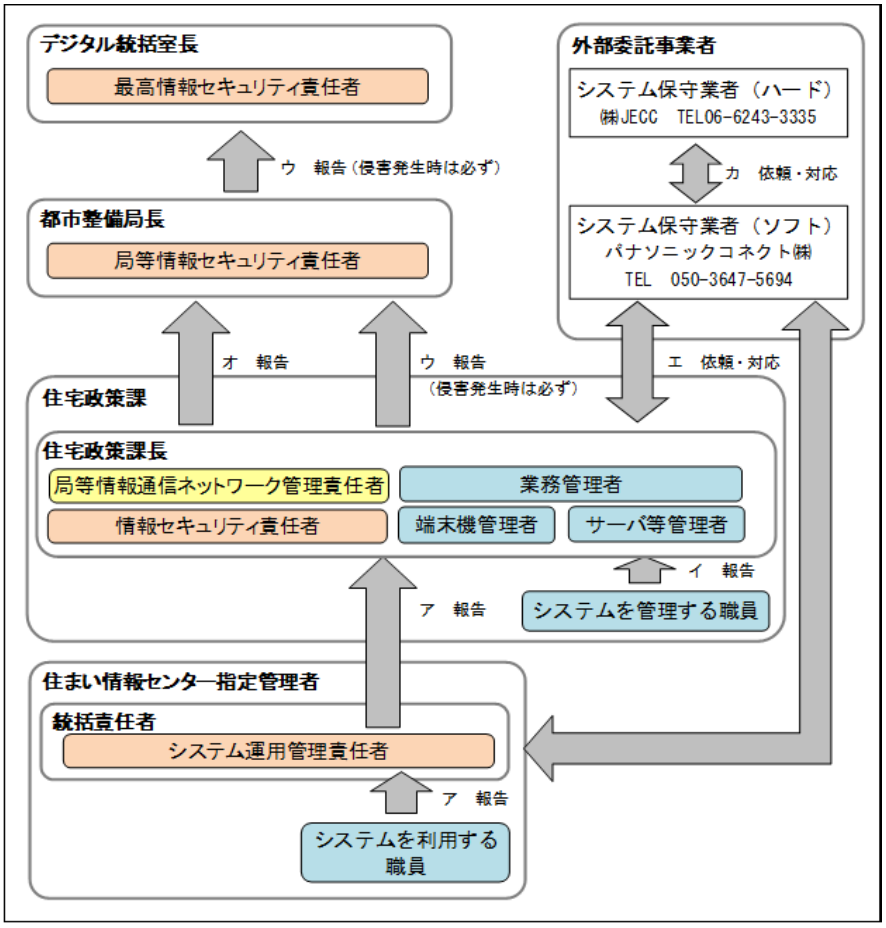
ウ　障害の報告を受けた業務管理者は、内容を把握するとともに、その対応策を検討し、

必要に応じてポリシーにおける上位の管理者に報告する。なお、重大障害時及び侵害発生時には、必ずポリシーにおける上位の管理者に報告する。

エ　業務管理者は、必要に応じて発生した問題に関して外部委託事業者（保守業者）に直接又はシステム運用管理責任者を通じて連絡を行い、対応を依頼する。

オ　局等情報通信ネットワークの障害・侵害を発見した場合、局等情報通信ネットワーク管理責任者を通じて局等情報セキュリティ責任者へ報告する。

（図１）連絡体制図



３．情報の管理方法

（１）データの管理

ア　システムが取り扱う情報のうち、表２「重要データ一覧表」に挙げる重要なデータ（以下「重要データ」という。）は、データを格納したサーバにアクセス権限を設定するなど適切に取り扱う。

イ　上記アのデータを基に作成された文書やデータに関しても、同様に取り扱う。

ウ　業務上必要のないデータを作成しない。

エ　作成途上のデータであっても、漏えい、き損、改ざん等を防止し、不要となった場合は、速やかにデータを削除する。

（表２）重要データ一覧表

重要性分類	データの重要度	データ名	ﾃﾞｰﾀ保護管理要綱※
I	個人情報及び業務上必要とする最小限の者のみが扱うデータ	ライブラリー利用者データ、相談記録	(1) (4)
Ⅳ	上記以外のデータ	書誌情報	

※　大阪市データ保護管理要綱第３条第２項の各号を指す。

（２）情報資産の管理

ア　業務以外の目的にシステム（端末機・サーバ・プリンタ等）の情報資産は利用しない。

イ　情報セキュリティ責任者は別途定める「記録媒体等取扱手順書」（以下「手順書」という。）　に基づき記録媒体等を適切に管理する。

ウ　記録媒体や端末機等の情報資産は定められた場所から持ち出さない。ただし、業務遂行上定められた場所以外への持ち出しが不可欠な場合は、手順書に基づき情報セキュリティ責任者又はシステム運用管理責任者の許可を得て持ち出す。また、持ち出しの際情報セキュリティ責任者又はシステム運用管理責任者は記録を作成する。

エ　重要データは、アクセス制御を設定しているサーバ上に保管する。同様の情報が格納された記録媒体は必要最小限とし、金庫に保管し適切に管理する。

オ　重要データをもとに作成された帳票等文書類は、金庫に保管し適切に管理する。

カ　情報セキュリティ責任者又はシステム運用管理責任者は、エ及びオの保管状況を２ヶ月に１回確認する。

（３）情報資産の廃棄

ア　重要なデータを含む端末機等機器や記録媒体等を廃棄又はリース返却等をする場合には、復元ができないように確実に破壊あるいはデータを消去する。なお、当該作業を外部委託事業者に委託する場合は、委託先事業者から処理の日時、責任者等、確実に処理されたことがわかる結果の報告を得る。

イ　重要データを記載した書類等を廃棄する場合は溶解により処理する。なお、当該作業を外部委託事業者に委託する場合は、委託先事業者に対して処理の日時、責任者等、処理結果の報告を得る。

４．機器の設置

（１）機器の設置場所

ア　サーバ等の主要な機器は、火気、水等の影響を受けない場所に設置し管理する。また機器の周辺では、喫煙、飲食を禁止し、ほこり等の影響が最小限となるよう清掃・整頓に努める。

イ　サーバ等の主要な機器は、サーバ室（情報システム室）へ設置し、サーバ等管理者又はシステム運用管理責任者が許可した場合のみ作業することができる。

ウ　サーバ等の主要な機器の取付けにあたっては、震災時の転倒を防止するため、ラックを床に固定する。

エ　職員不在時には、ノート型の端末機を設置する執務室を施錠する。

（２）電源管理

サーバには、無停電電源装置（UPS）を設置することにより、突発的な停電等に備え、サーバを適切に停止できるようにする。

（３）ケーブル類の措置

ケーブル類は、人為的な過失等による被害を防止するために、フロア下への配線を行う。

５．執務室等の運営

（１）執務室等の入退室管理

ア　システムを設置している執務室（以下「執務室」という。）には、執務時間内は必ず指定管理者職員が在席し、不在になる場合には、部屋を施錠する。執務室における施錠担当者は、最終退室者とする。

イ　指定管理者職員は、執務室に在席している間は、名札等を着用する。また、外部委託事業者の入退室にあたっては、管理記録簿により日時・氏名・作業内容等を把握するなど必要な措置を講じる。

（２）一般コーナーの分離

ア　執務室において市民等の第三者が出入りする部分は、一般コーナーとして職員が執務を行う部分とパーテーション等で明確に区別する。

イ　端末機やプリンタ、コピー機等は、画面や出力した帳票が一般コーナーから容易に見えない場所に設置する。

６．職員への研修・教育

（１）実施手順の周知等

情報セキュリティ責任者及びシステム運用管理責任者は、自所属の職員に対して実

施手順を理解させ、情報セキュリティ上の問題が生じないよう教育、指導を行う。

（２）システムに係る情報セキュリティの徹底

業務管理者及びシステム運用管理責任者は、システムの運用に関わる職員に対して実施手順ならびに実施に必要な知識及び技術等について教育、指導を行う。

（３）職員における情報管理

ア　職員は、貸与以外の端末機及び記録媒体（以下、「私物端末機等」という。）を持ち込まない。また、原則として、私物端末機等を業務に使用しない。

イ　職員は、情報セキュリティ責任者又はシステム運用管理責任者の許可なくして、端末機や記録媒体を持ち出さない。

ウ　システム運用管理責任者は、イの承認又はウの許可を行った場合は、情報セキュリティ責任者に報告する。

エ　職員は、自己の管理する ID について、次の事項に留意し管理する。

・端末機へのログイン及び相談サブシステムへのログインに利用するユーザ ID は個人 ID とし、他人には利用させない。

・図書サブシステムへのログインに利用するユーザ ID は共用 ID とし、共用 ID の利用者以外に利用させない。

オ　職員はパスワードの使用に際して、次の項目に留意し管理する。

・パスワードは他者に知られないように管理する。

・パスワードは秘密にし、他の人物からのパスワード照会等には一切応じない。

・パスワードは、十分な長さ（８文字以上とする。）とし、文字列は想像しにくいものから構成する。

・90 日に１回、パスワードを変更し、古いパスワードは再利用しない。

・初回ログイン時に配付された仮のパスワードは、最初のログイン時に変更する。

・パスワードは、氏名や生年月日、職員番号等の他の人物が類推しやすいものにしない。

・職員間でのパスワード共有は行わない。

・端末機にパスワードを記憶させない。

・パスワードが流出した可能性がある場合、速やかにシステム運用管理責任者に報告し、パスワードを変更する。

・パスワード流出の報告を受けたシステム運用管理責任者は、端末機管理者に報告する。

カ　職員は、端末機から離れる場合には必ずコンピューターロックやログオフ、電源を切るなど、不正な利用を防止する。

キ　職員は、許可なく新たなソフトウェアをサーバや端末機にインストールしない。業務上やむを得ず、新たなソフトウェアをインストールする必要がある場合には、業務管

理者の承認を得る。

ク　職員は著作権法等に違反するソフトウェアの使用や複製等を行わない。

ケ　職員は、異動や退職等によりシステムを利用しなくなる場合は、利用していた情報資産を返却する。また、その後も、知りえた情報を漏らさない。

７．外部委託における管理

（１）外部委託契約

業務管理者は、外部委託事業者と契約を交わす場合には、次の項目を契約書に明記する。

・ポリシー及び実施手順の遵守
・事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・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
・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受託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
・本市による監査、検査
・本市によるセキュリティインシデント発生時の公表
・ポリシーが遵守されなかった場合の規定(損害賠償等)

（２）外部委託事業者への管理、指導

ア　業務管理者は、外部委託事業者に対して、実施手順に準拠した情報管理体制、情報セキュリティ対策を講じるよう要求し、その運用状況について必要なセキュリティ対策が確保されているか年に１回確認、調査を行う。その際には、必要に応じて管理記録簿等の提示を求め、作業場所への立ち入り検査を行う。

イ　業務管理者は、外部委託事業者に対して、その管理下にある社員がポリシー及び実施手順を遵守するように必要な対策を講じることを要求する。

８．アクセス制御

（１）アクセス制御

ア　業務管理者は、システムへのアクセスが可能な利用者及びその利用範囲等アクセス権限を明確にし、システム運用管理責任者を通じてシステムへのアクセス権限を設

定する。

イ　システムへのアクセス権限は、ユーザ ID 及びパスワードにより管理を行う。

ウ　業務管理者は、管理者権限等の特権を付与された ID は初期設定以外のものに変更する。

エ　業務管理者は､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する。

オ　職員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､ログイン後直ちに仮のパスワードを変更させる。

カ　業務管理者は、システム運用管理責任者を通じてシステムへのアクセス権限の把握、管理を適切に行う。特に職員の異動や退職時にともない発生する不要なユーザ ID は速やかに消去又は権限の変更を行う。

キ　業務管理者は、利用されていない ID が放置されないよう、年に１回点検する。

ケ　システムのアクセス制御の設定は、表３のとおりとする。

（表３）　システムアクセス権限一覧

項番	権限名	説明	アクセス可能者
1	システム管理権限 （administrator）	システムのすべての機能を利用できる。	業務管理者 保守業者
2	ユーザ登録権限 （master）	管理対象データへのすべての機能が利用できる。	端末機管理者 システム運用管理責任者
3	編集権限 （user）	管理対象データへの登録､照会機能が利用できる。	システム利用担当者

９．不正アクセス対策

（１）ファイアウォールの設置等

外部ネットワークと接続される部分にあたっては、ファイアウォールを設置するとともに､不正アクセスから保護するため､本来の通信に不必要なポートはすべて閉鎖しなければならない。

（２）セキュリティホールへの対応

ア　システムで利用する OS やアプリケーション等は、パッチやバージョンアップなどの開発元のサポートが継続中であるものを利用する。

イ　業務管理者（兼サーバ等管理者）は､定期的に JPCERT や IPA セキュリティセンター、Microsoft 等の利用ソフトウェアベンダーの Web サイトからセキュリティに関する情報を定期的に収集し、最新の動向を把握する。

ウ　業務管理者（兼サーバ等管理者）は、収集したセキュリティ情報から判断し、OS やアプリケーション等のバージョンアップやプログラム修正の適用等の対応を適切に行う。

エ　OS やアプリケーション等のバージョンアップやプログラム修正等については、常に最新のものを適用する。

（３）各種ログ

ア　業務管理者は、システム運用管理責任者を通じて表４のとおりログを取得する。

イ　システム運用管理責任者は、アにおけるログを１年間保存する。

（表４）取得ログ一覧表

項番	機器と操作内容	ログ取得項目
1	端末機へのログイン	ログインしたユーザ ID
		ログイン日時
		ログインの成功／失敗
2	サーバ上の重要データへのアクセス（ローカルログイン／リモートログイン）	IP アドレス
		アクセス日時
		アクセスの成功／失敗

10. コンピュータウイルス対策

本システムにおける、ウイルス対策は次のとおりとする。(表５　コンピュータウイルス対策一覧表参照)

（１）ウイルス対策ソフト

ア　サーバ及びすべての端末機にウイルス対策ソフトを導入する。

イ　ウイルス対策ソフトは、常駐監視機能を設定する。

ウ　ウイルス対策ソフトのパターンファイルは、自動更新設定を行い、常に最新の状態に更新する。

（２）ウイルスチェック

ア　記録媒体等によりデータをやり取りする場合には、必ず事前にウイルスチェックを実施する。

イ　業務管理者はウイルス対策ソフトのスケジュール設定により、週１回 ハードディスクの全ファイルのウイルスチェックを実施する。スケジュールで設定した時間に起動していなかった端末機等は、次回使用時までに必ずウイルスチェックを実施する。

（３）ウイルスに関する報告・連絡

ア　ウイルスの侵入や感染及びその兆候を発見した職員は、端末機から LAN ケーブルを

抜き、「２．管理・連絡体制　(2)　連絡体制」に基づき速やかにシステム運用管理責任者へ報告する。

イ　アにて報告を受けたシステム運用管理責任者は、ウイルスチェックを行い、その結果、ウイルスの感染を発見したときは、影響範囲及び感染経路等を調査し、ウイルス駆除に必要な対策を速やかに講じる。また、システム等情報資産に影響が生じたときは、「２．管理・連絡体制　(2)　連絡体制」に定める侵害時の対応に基づいて必要な措置を講じる。

ウ　業務管理者（兼サーバ等管理者、局等情報通信ネットワーク管理責任者）は、定期的に JPCERT や IPA セキュリティセンター等の Web サイトからウイルスに関する情報を収集する。業務やシステム形態により特に注意が必要と判断するウイルスの情報については、その特徴等を職員に通知して当該ウイルスに対する注意喚起を行う。

（４）ウイルス対策等における職員の役割

職員はウイルスによるシステム等情報資産への影響を防ぐため、次の事項に留意する。

・情報セキュリティ責任者又はシステム運用管理責任者の許可を得て外部から持ち込んだ又は持ち帰った端末機等をシステムに接続するときは、ウイルスの感染有無及びセキュリティパッチ等の適用状況を確認し、問題のないことを確認する。
・情報セキュリティ責任者又はシステム運用管理責任者が許可した記録媒体を使用する。
・業務管理者が周知するウイルスに関する情報に留意し対応する。
・端末機に導入されているウイルス対策ソフトの設定を変更しない。

（表５）コンピュータウイルス対策一覧表

対象機器	ウイルス対策ソフト	ウイルスパターン更新サイクル	常駐監視	ウイルススキャン実施サイクル
業務用端末	導入	月～金曜日 10:00	実施	毎週月曜日 0:00 から
サーバ	導入	月～金曜日 10:00	実施	毎週日曜日 12:00 から

11. システムの保守

（１）システム保守時における留意事項

ア　業務管理者（兼サーバ等管理者）は、システム変更等の保守作業を行う場合は、不具合の確認を行い、既存システムの運用に影響がないようにする。

（２）機器保守時における留意事項

ア　機器の保守点検を実施した場合には、点検結果等の記録を備える。

イ　記録媒体（ハードディスク等）を含む機器の修理を外部委託事業者に委託する場合は、記録媒体の情報を消去し委託する。情報を消去できない場合は、修理を委託する外部委託事業者との契約において秘密保持に関する事項を定める。

（３）テストの実施

業務管理者は、システム変更等に際し、既存のシステムの運用に影響が生じないように留意してテストを行う。

（４）ドキュメント等の管理

業務管理者（兼サーバ等管理者）は、システムに変更が発生した場合は、管理の引継ぎや職員の利用時を考慮して、その履歴を記録するとともに関係するドキュメントに対して適宜変更を反映し、必要時に閲覧可能な環境を整える。

12. システムの運用

（１）運用管理、運用計画

ア　業務管理者は、サーバ等管理の手法及び体制等について、必要なマニュアル等を整理し、必要時に閲覧可能な環境を整える。

イ　システム運用責任者はサーバ等管理者（兼業務管理者）と協議して、システムの運用計画を策定し、年間、月間、週間等における運用スケジュール及びシステムの運用時間等、サーバ等に必要な事項を明確にする。システムの稼働時間については表６「システム稼働時間等一覧表」のとおり。

（表６）システム稼働時間等一覧表

稼働日	システム稼働時間	サービス可能時間（ユーザの利用時間）	延長・休日運用の可否
開館日（火曜日を除く平日、土曜日）	24 時間	24 時間	可
開館日（日祝日）	24 時間	24 時間	可
休館日（火曜日、祝日の翌日、年末年始）	24 時間	24 時間	可

（２）サーバ利用時の対策

ア　サーバは、サーバ等管理者の承認を得た職員または外部委託事業者のみが、許可された目的にのみ使用する。

イ　サーバを運用時間外に使用する場合には、事前にサーバ等管理者又はシステム運用管理責任者の承認を得る。

ウ　サーバは、必要な場合を除いてはログインしない。また作業終了時には必ずログオフする。

（3）端末機利用時の対策

ア　業務管理者は、端末操作マニュアル等を作成し、システムを利用する職員に周知する。

イ　執務室の最終退室者は、端末機の電源が切れていること等を確認する。

（4）バックアップの取得

ア　サーバ等管理者は、サーバに格納したデータやプログラムを定められた媒体にバックアップを取得する。バックアップの運用については表７「バックアップ運用一覧表」のとおりとする。

イ　バックアップ作業は、日々の業務終了後にフルバックアップを取得する。

（表７）バックアップ運用一覧表

サーバ名	取得内容	取得媒体	世代数	取得タイミング	取得レベル	遠隔地保管
外部図書サーバ	データベース	外部HDD	6	毎日	完全	なし
内部図書サーバ	データベース	外部HDD	6	毎日	完全	なし
相談サーバ	データベース	外部HDD	6	毎日	完全	なし

（5）障害・侵害発生時の対応

ア　職員はシステムに障害・侵害が発生した場合は、障害時対応マニュアルに基づき対応し、速やかにシステムを回復させる。

イ　システムに障害・侵害が発生し、利用できない場合には、職員は代替処理として手書き等により業務を継続する。また、システム復旧後は代替処理により行った手書き等処理分の入力処理等を行う。

ウ　システムの運用に著しい支障をきたしている場合や、侵害により情報資産にかかる重大な被害が想定される場合には、サーバ等管理者（兼業務管理者）はシステムを停止する。

エ　業務管理者（兼サーバ等管理者）は、障害・侵害の原因及び処理結果について記録し、再発防止に向け必要な改善措置を講じる。

13. 点検・評価及び見直し

（１）点検・評価

ア　情報セキュリティ責任者及びシステム運用管理責任者は、職員の行動を把握し、システムが実施手順どおりに運用されているかどうか確認する。

イ　情報セキュリティ責任者及びシステム運用管理責任者は、アにおいて実施手順が遵守されていない点が明らかになった場合には、職員に対して改善するように指導する。

（２）実施手順の見直し、変更

ア　業務管理者は、新たな脅威の発生やシステム変更等によりセキュリティ対策を追加する必要が生じた場合には、ポリシーに準じて実施手順を見直し、変更する。

イ　業務管理者は、アの変更に基づいて、必要に応じて業務マニュアル等の見直しを行なう。

ウ　業務管理者は、上記ア及びイに定められた実施手順や業務マニュアル等の変更を行った場合には、実施手順の対象者に変更内容の周知徹底を行う。

14. その他

実施手順に基づくシステムの利用にあたり、その他必要な事項については、業務管理者が定める。

附　則

この実施手順は平成 16 年３月 24 日より施行する。

附　則

この改正実施手順は平成 23 年８月 22 日より施行する。

附　則

この改正実施手順は平成 25 年８月 30 日より施行する。

附　則

この改正実施手順は令和５年１月 30 日より施行する。

津波災害等における緊急一時避難施設としての使用に関する協定書

大阪市北区役所（以下「甲」という。）と大阪市立住まい情報センター等建物管理組合（以下「乙」という。）とは、津波又は河川の氾濫（以下「津波災害等」という。）が発生、又は発生するおそれがあるときに、地域住民等の避難の円滑化を図るため、乙の所有する施設を緊急一時避難施設（以下「避難建物」という。）として使用することに関し、次のとおり協定を締結する。

（使用物件）

第１条　乙は、自己の所有する次に掲げる建物を、津波災害等が発生し又は発生するおそれのあるときに、避難建物として地域住民等に使用させるものとする。

（１）　住　所　大阪市北区天神橋６丁目４番20号
（２）　名　称　大阪市立住まい情報センター等建物
（３）　構造等　鉄骨鉄筋コンクリート造、一部鉄骨造
　　地下１階、地上10階、塔屋１階
（５）　建築年　平成11年10月
（６）　使用場所　３階ＥＶホール及び共用通路部分等　約393㎡〔別図のとおり〕
（７）　使用可能時間　24時間使用可能
（８）　収容人数　245名（※1.6㎡／人で算出）

（避難対象者）

第２条　避難建物の避難対象者は大阪市北区の住民を基本とするが、当該地域において就労中又は旅行中（通過中）の者も同様とする。（以下「地域住民等」という。）

（使用目的及び期間）

第３条　避難建物の使用目的及び期間は、地域住民等の避難施設として、津波災害等が発生し又は発生するおそれがあるときから、国、地方公共団体等、公の機関が安全を確認したときまでとする。使用後は災害救助法等に基づき甲において現状に復するよう努めるものとする。（但し、地震・津波災害等に起因する損害は除く。）

（目的外使用の禁止）

第４条　甲は、避難建物を前条に定める規定以外には使用しないものとする。

（使用料等）

第５条　避難建物の使用料は無料とする。

（使用者責任）

第６条　甲及び乙は、避難建物に地域住民等が避難した際に発生した事故等に対する責任を一切負わない。

（相互協力）

第７条　乙及び当該建物の管理受託者は、津波災害等による避難時に地域住民等と相互協力できるよう、日頃から地域住民等と交流及び情報交換を行うよう努める。また、津波災害等が発生した際には、当該地域に居住しない人々に対しても地域

住民と同様に扱い、一人でも多くの命を守ることができるよう努める。

(施設変更の情報提供)

第８条　乙は、避難建物が増改築により、使用場所や経路等が変更になった場合は甲に情報提供し、必要に応じて甲、乙が協議し、協定内容を変更する。

(施設の情報公開)

第９条　甲は、この協定の締結期間において、第１条で定める使用物件の所在地及び建物名又は事業所名等をホームページ等にて公開することができる。

(有効期限)

第 10 条　この協定の締結期間は、協定締結の日の属する年度の３月 31 日までとする。

２　前項の期間満了の日から１ヶ月前までに、甲、乙いずれかから申出がない場合は自動的に１年延長するものとし、その後も毎年この例による。

３　年度とは、毎年の４月１日から翌年３月 31 日までとする。

(協議事項)

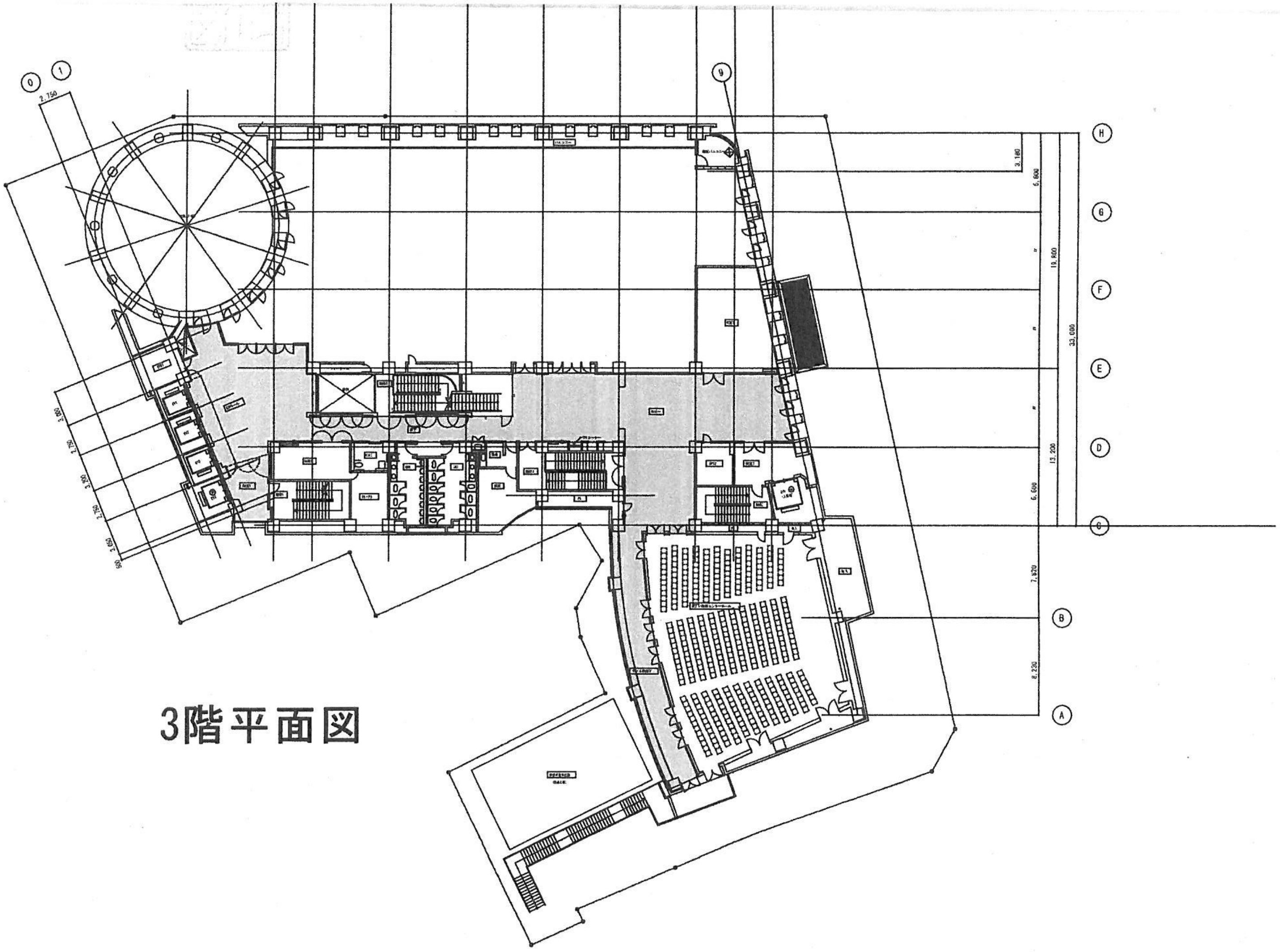
第 11 条　この協定に定めのない事項及びこの協定に関して疑義が生じた事項については、その都度、甲乙が協議して定めるものとする。

この協定の成立を証するため、この協定書を２通作成し、甲乙が記名押印のうえ、各自その１通を保有する。

平成 27 年 1 月 19 日

甲　大阪市北区扇町２丁目１番 27 号
大阪市北区長　古屋　和彦　印

乙　大阪市北区天神橋６丁目４番 20 号
大阪市立住まい情報センター等建物管理組合
代表者　大阪市長　橋下　徹　印


0
1
2,750
9
H
G
F
E
D
C
B
A
3,180
5,600
19,800
33,080
13,200
6,600
7,920
8,230
3,850
1,750
3,920
1,750
900
2,650

3階平面図