和泉市情報セキュリティポリシー

情報セキュリティ基本方針
情報セキュリティ対策基準

平成16年　2月　5日　適用開始
平成20年11月　1日　一部改正
平成22年　4月　1日　一部改正
平成27年　9月29日　全部改正
令和4年　3月22日　全部改正

目 次

1.情報セキュリティ基本方針
1.1.目的

1.2.用語の定義

1.3.情報資産への脅威

1.4.基本原則

1.5.適用範囲

1.6.職員等の遵守義務

1.7.情報セキュリティ対策

1.8.情報セキュリティ点検及び自己点検等の実施

1.9. 情報セキュリティポリシーの見直し

1.10.情報セキュリティ対策基準の策定

1.11.情報セキュリティ実施手順の策定

1.11.情報セキュリティ対策の経過措置について

2. 情報セキュリティ対策基準

2.1. 組織体制

2.1.1. 各担当者の責務

2.2. 大前提

2.2.1. 情報資産の分類と管理方法

2.2.2. ネットワーク構成

2.2.3. システム構成

2.3. 事業者関係

2.4. 在宅勤務

2.5. 管理区域（サーバ室等）の管理

2.6. 情報セキュリティインシデントの報告

2.7. 研修・訓練

2.8. 評価・見直し

2.8.1. 点検

2.8.2. 情報セキュリティポリシー及び関係規程等の見直し

和泉市情報セキュリティ基本方針

1.情報セキュリティ基本方針

1.1.目的

本基本方針は、本市が保有する情報資産の機密性等を維持するため、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。

1.2.用語の定義

（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）真正性

情報にアクセスする企業組織や個人あるいは媒体が「アクセス許可された者」であることを確実にすることをいう。

（9）信頼性

情報やシステムを利用した動作が、意図した通りの結果を出すことをいう。

（１０）責任追跡性

情報やシステムに対して、誰が何をしたのかを明確に追跡できることをいう。

（１１）否認防止

情報が後に否定されないように証明できることをいう。

（１２）情報セキュリティ７要素

機密性、完全性、可用性、真正性、信頼性、責任追跡性、否認防止をまとめて示す呼称

（１３）CSIRT

「Computer Security Incident Response Team」の頭文字を取った略語で、一般的にはコンピューターセキュリティに関する事故対応チームのことをいうが、ここでは情報システムに関係する事故

対応チームのことをいう。

（１４）情報セキュリティインシデント

外部、もしくは内部からの攻撃や不正な手口による被害、または地震や火事、雷などの天災による被害、そして故意や悪意はないが人為的な被害などによって以下の状況に陥った状況のことをいう。

・情報資産に対して何らかの悪意のある操作が行われてしまった場合。あるいはその危険性が迫っている場合
・行政サービスが一時的に停止、もしくは機能不全で正常な状態でなくなった場合

1.3. 情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（１）部外者による故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去・漏洩、機器及び媒体の盗難等
（２）職員及び外部委託者等による意図しない操作、操作ミス、あるいは故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去・漏洩、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等
（３）地震、落雷、火災等の災害並びに事故、故障によるサービス及び業務の停止
（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

1.4. 基本原則

情報セキュリティ対策の基本原則は以下のものとする。

・機密情報を第三者に漏洩しない
・対市民・事業者への行政サービスを滞らせない
・万が一被害が発生した場合に、速やかに全容把握できるようにする
・過剰なセキュリティ対策はせずに、利便性も考慮する
・長期的な視点をもって運用・構築していく
・人間は間違う、ということを考慮する
・法令順守

1.5. 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、市長、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、水道事業、公共下水道事業及び公共浄化槽事業の管理者の権限を行う市長、消防長並びに議会とする。

（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、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
④ 上記情報資産については、クラウドサービス等を利用している場合も含むこととする（市が保有する情報に限る）

1.6. 職員等の遵守義務

職員（再任用職員も含む。）、会計年度職員（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等を遵守しなければならない。

1.7. 情報セキュリティ対策

情報セキュリティの遵守にあたり、以下の対策を講じる。

（1）情報セキュリティ管理体制

本市の情報資産について、適切で統一的な情報セキュリティ対策を推進及び管理するため全庁的な体制を確立する。また、管理責任者を定め、義務と責任の所在の明確化を図る。

（2）情報資産の分類と管理

情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行うものとする。

（3）物理的セキュリティ

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講じる。

（4）人的セキュリティ

情報セキュリティに関する権限や責任を定め、全ての職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発を行う等の人的な対策を講じる。

（5）技術的セキュリティ対策

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。

（6）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、外部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、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講じる。

1.8. 情報セキュリティ点検及び自己点検等の実施

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点検及び自己点検を実施する。

1.9. 情報セキュリティポリシーの見直し

情報セキュリティ点検及び自己点検等の結果、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。

1.10. 情報セキュリティ対策基準の策定

情報セキュリティ対策を講ずるに当たっては、遵守すべき事項、判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

1.11. 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対策実施手順を必要に応じて策定するものとする。

なお、情報セキュリティ対策実施手順は、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。

1.11. 情報セキュリティ対策の経過措置について

情報セキュリティポリシー及び情報セキュリティ対策基準、情報セキュリティ対策実施手順に基づき、情報セキュリティ対策を実施しなければならない。しかし現行システムの構成上順守が難しい場合は、情報セキュリティ管理者の許可を得た上で、本ポリシー改訂後 2 年以内に対策を施さなければならない

和泉市情報セキュリティ対策基準

2.情報セキュリティ対策基準

2.1.組織体制

（1）最高情報総責任者

①情報政策担当部署を担任する副市長を最高情報総責任者とし、本市の全て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。

②本市の情報セキュリティ及び情報システムの運用方針に関する権限及び責任を有する。

②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アドバイザーとして置くものとする。

③情報政策担当部署を担任する部長を補佐とする

（2）情報セキュリティ管理者

①個人情報保護担当部署を担任する副市長を情報セキュリティ管理者とし、主に情報セキュリティ面での実務を担当することで、最高情報総責任者を補佐する。

②共通的な情報資産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。

④共通的な情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、最高情報総責任者へ速やかに報告を行い、指示を仰がなければならない。

⑤情報セキュリティ管理者が任名する者を補佐とする

（3）情報運用管理者

①情報政策担当部署を担任する部署の所属長を情報運用管理者とし、主に情報システムの運用面を担当することで、最高情報総責任者を補佐する。

②共通的な情報資産の構築・運用に関する権限及び責任を有する。

③共通的な情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、最高情報総責任者及び情報セキュリティ管理者へ速やかに報告を行い、指示を仰がなければならない。

④情報政策担当部署に所属する者を補佐とする

⑤必要に応じて情報運用管理者が任名する者も補佐とすることができる

（4）情報管理者

①各課（室）等の長を、情報管理者とする。

②所管課内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。

③必要に応じて、所管する情報資産に係る情報セキュリティ実施手順を策定し、その維持・管理を行う。

④所管するネットワーク及び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。

⑤所管する課（室）等において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ管理者及び情報運用管理者へ速やかに報告を行い、指示を仰がなければならない。

（5）情報システム担当者

情報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。

（6）ＩＴ推進本部

本市の情報セキュリティ対策を統一的に行うため、ＩＴ推進本部において、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。

（7）CSIRT

重大な案件に該当する情報セキュリティインシデントが発生した場合に、その対応を主担する。

2.1.1.各担当者の責務

●最高情報総責任者

・本市のセキュリティ対策や情報システム運用方針の大前提を考案・決定する
・情報漏洩等の事故が発生した場合、最終責任者として対外部・対内部への説明を行う

●情報セキュリティ管理者

・本市のセキュリティ対策や運用方針に基づき、セキュリティ対策方針を策定するものとする
・情報運用管理者及び情報管理者が適切に情報システムを運用する上で必要なセキュリティ対策・管理運用を実施しているかを点検し、指示・指導・助言を行うものとする。
・情報漏洩等の事故が発生した場合、速やかな全容把握ができるよう、適切に指揮・監督を行うものとする
・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、必要に応じて最高情報総責任者 にその内容を報告しなければならない。
・年に１度以上、外部の識者による点検を実施し、本市のセキュリティ対策や運用正しく実施されているか、情報セキュリティ管理者や情報運用管理者が正しく機能しているか、点検を受けなければならない

●情報運用管理者

・本市のセキュリティ対策や運用方針に基づき、本市の全体に関わるネットワーク構成、システム構成、運用方法等の構築・運用・管理・保守
・情報資産に脅威が及んでいないかの監視
・情報管理者が適切に業務を遂行しているのかの管理・指導
・情報漏洩等の事故が発生した場合、速やかな全容把握
・市職員に対する本市のセキュリティ対策や運用方針の研修・周知
・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、必要に応じて最高情報総責任者及び情報セキュリティ管理者にその内容を報告しなければならない。

●情報管理者

・本市のセキュリティ対策や運用方針に基づき、所管業務のネットワーク、システム等の構築・運用・管理・保守
・情報資産に脅威が及んでいないかの監視
・情報システム担当者及び市職員が適切に業務を遂行しているのかの管理・指導
・所管業務での情報漏洩等の事故が発生した場合、速やかな全容把握
・本市の共通的なネットワークを利用しない環境を構築する場合、本市のセキュリティ対策や運用方針に基づいた環境を構築しなければならない

●情報システム担当者

・本市のセキュリティ対策や運用方針に基づき、所管業務のネットワーク、システム等の構築・運用・管理・保守
・情報資産に脅威が及んでいないかの監視
・所管業務での情報漏洩等の事故が発生した場合、速やかな全容把握

●市職員

・本市のセキュリティ対策や運用方針の理解と順守
・業務に関係のない、あるいは業務上不必要な情報システム・情報資産の操作・提供等の禁止
・本市所管外情報システム等での、情報資産の操作等の禁止
・本市所管情報システムの業務上不必要な場所での利用
・情報資産の分類と適切な運用・管理
・本市のセキュリティ対策や運用方針の原則を理解し、記載のない事例に対しても原則に基づき対処すること

●CSIRT の設置・役割

・最高情報総責任者は、CSIRT を整備し、その役割を明確化しなければならない。
・最高情報総責任者は、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。なお、CSIRT 責任者を情報セキュリティ管理者が兼任し、CSIRT 所属職員を情報セキュリティ管理者の補佐職員が兼任することも可とする。
・情報セキュリティ管理者は、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することしなければならない。
・最高情報総責任者 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。
・情報セキュリティインシデントを認知した場合には、最高情報総責任者、総務省、大阪府等へ報告しなければならない。
・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。
・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、外部の事業者等との情報共有を行わなければならない

2.2.大前提

2.2.1.情報資産の分類と管理方法

（1）情報資産の分類

本市における情報資産は、その重要性に応じて、次のとおり分類し、必要に応じ取扱い制限を行うものとする。

重要度分類	情報の内容	具体例	取扱い制限（参考例）
Ⅲ	セキュリティ侵害が行政事務の執行等に重大な支障を及ぼさない情報	・HP に掲載している情報 ・庁内通知文	・必要に応じてバックアップの作成、保管 ・保管場所の制限、保管場所への必要以上の外部記録媒体等の持ち込みの禁止 ・外部記録媒体の施錠可能な場所への保管 ・関係者以外の目に留まる場所に保管しない ・不必要な公開をしない ・システム操作者を明確にする
Ⅱ	セキュリティ侵害が行政事務の執行や信頼等に重大な支障を及ぼす情報	・業務資料（入札仕様書等） ・オンライン申請にて収集された個人情報	・上記重要度分類Ⅲに掲げる対策の実施 ・許可された者以外による閲覧・編集の制限 ・不必要な複製及び配付の禁止 ・情報の送信、情報資産の運搬及び提供時における暗号化及びパスワード設定や鍵付きケースへの格納 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・復元不可能な処理を施しての廃棄 ・バックアップの作成、保管
Ⅰ	個人に関する情報であって、特定の個人を識別し得る情報	・基幹系システムで扱う個人情報	・上記重要度分類Ⅱに掲げる対策の実施 ・個人系ネットワークでの利用 ・原則外部への情報の提供の禁止

●重要度分類Ⅰ

個人に関する情報であって、特定の個人を識別し得る情報は重要度分類Ⅰとする。本情報資産は、可用性が損なわれると市民サービスに悪影響が出る、機密性が損なわれると行政への信頼が失墜するなど、本市業務の中で最も重要な情報であるため、情報セキュリティ７要素を完全に満たしている条件下で利用すること。

・機密性：外部への接続禁止（一部 LGWAN や住基ネットワーク等は申請に基づき許可）。
　　外部持ち出しの原則禁止と例外対応の際の複数人チェック。
　　廃棄の際は、物理破壊で復元不可能にしなければならない
　　情報資産を保有している機器は管理区域に保管
・完全性：変更履歴の保存
・可用性：情報資産および情報システムの冗長化

UPS 等による停電対策
・真正性：二要素認証
・信頼性：責任の所在が明確な設計・構築
・責任追跡性：操作履歴の保存
・否認防止：操作履歴の保存

●重要度分類Ⅱ

セキュリティ侵害が行政事務の執行や信頼等に重大な支障を及ぼす情報は重要度分類Ⅱとする。なお、個人に関する情報であるが、重要度分類Ⅰに当たる半ば強制的に保有している個人情報ではなく、電子申請時に同意の上で提供された個人情報等については重要度分類Ⅱに該当するものとする。本情報資産は、可用性が損なわれると行政サービスに悪影響が出る、機密性が損なわれると行政への信頼が失墜するなど、本市業務の中で重要な情報であるため、情報セキュリティ７要素を完全に満たしている条件下で利用すること。

・機密性：LGWAN のみに接続（一部インターネットサイトは申請に基づき許可)。
外部持ち出しの際の複数人チェック。
廃棄の際は、論理破壊以上で復元不可能にしなければならない
情報資産を保有している機器は管理区域に保管
・完全性：決裁等の重要情報については、変更履歴の保存
・可用性：情報資産および情報システムの冗長化
UPS 等による停電対策
セキュリティ対策プログラム等の随時更新
・真正性：一要素認証
・信頼性：責任の所在が明確な設計・構築
・責任追跡性：操作履歴の保存
・否認防止：操作履歴の保存

●重要度分類Ⅲ

セキュリティ侵害が行政事務の執行等に重大な支障を及ぼさない（市民や事業者の生命・財産に影響がない、行政サービスにおける公平性等が損なわれない、本市のセキュリティに影響がない等）情報は重要度分類Ⅲとする。

・機密性：インターネットに接続。ただし危険なサイト等へは接続不可
・完全性：HP 情報等市民サービスに関わる情報については、変更履歴の保存
・可用性：必要に応じて情報資産の冗長化
セキュリティ対策プログラム等の随時更新
・真正性：一要素認証
・信頼性：責任の所在が明確な設計・構築
・責任追跡性：操作履歴の保存
・否認防止：操作履歴の保存

2.2.2 ネットワーク構成

原則的に本市の業務を遂行する場合は、その利用する情報資産の重要度に応じて、以下のネットワークのいずれかに接続することとする。なお、やむを得ず以下のネットワーク以外でなければ稼働しないシステムを導入する場合は、情報セキュリティ７要素を満たした上で、運用管理を行わなければならない。

名称	取り扱う情報資産	概要
個人系ネットワーク	重要度分類Ⅰ	・外部（インターネット）と切断されている ・一部許可された LGWAN と接続している
LG 系ネットワーク	重要度分類Ⅱ	・一部許可された外部（インターネット）と接続している ・LGWAN と接続している
インターネット系ネットワーク	重要度分類Ⅲ	・外部（インターネット）と接続している ・LGWAN と切断している

●個人系ネットワーク

外部と直接接続されないように、FW 等によって隔離していなければならない。許可された LGWAN との接続（インターネット等から LGWAN-ASP を経由してマイナンバー利用事務系にデータの取り込み等も含む）についても、FW 等により必要最小限の機器、通信内容に留めるとともに、利用者・利用内容・利用時期を明確化できること（履歴保存は１年以上。市職員だけでなく、ウイルス等による情報流出等の履歴も取得すること）。

原則有線 LAN を利用し、廊下等事務室以外の場所で利用できない環境にしなければならない。

●LG 系ネットワーク

LGWAN と接続するにあたり、FW 等により必要最小限の機器、通信内容に留めるとともに、利用者・利用内容・利用時期を明確化できること（履歴保存は１年以上。市職員だけでなく、ウイルス等によるものも取得すること）

また許可されたインターネットとの接続についても FW 等により必要最小限の機器、通信内容に留めるとともに、何が、何時、何処から何処に、どのように送られたのかを明確化できること（履歴保存は１年以上。市職員だけでなく、ウイルス等によるものも取得すること）

情報資産を取り込む際は原則無害化処理を行い、安全なものでなければ本ネットワークに持ち込んではならない。

なお LG 系ネットワークに属する端末については、セキュリティ対策を十分考慮した上であれば無線 LAN での環境構築も可とする。

●インターネット系ネットワーク

インターネットと接続するにあたり、FW 等により必要最小限の機器、通信内容に留めるとともに、利用者・利用内容・利用時期を明確化できること（履歴保存は１年以上。市職員だけでなく、ウイルス等によるものも取得すること）。

原則としてインターネットに接続する出入口は大阪セキュリティクラウドを経由すること。

2.2.3. システム構成

システムを構築・運用するにあたっては、情報セキュリティ７要素を満たすものを構築すること。ただし取り扱う情報資産の重要度に応じて、各システムにおいて最低限の対策を施すこととする。

基準となる考え方

・情報セキュリティ７要素を満たすことを運用に任せず、システム構成上普段の運用の中で自動的に情報セキュリティ７要素を満たすことができる構成にすること
・利用者・利用内容・利用時期を明確化できること（履歴保存は１年以上）
・重要度分類Ⅱ以上の情報資産を持ち出す場合は、システム構成上複数人チェックが必須となる構成にすること
・情報資産の出入口（外部記録媒体への書き込み、メール、インターネットへの情報アップロード等）には、利用者・利用内容・利用時期を明確化できること（履歴保存は１年以上。市職員だけでなく、ウイルス等によるものも取得すること）
・業務上不必要な情報システムやソフトウェア等の導入をしてはならない
・市民の生命・財産・権利や、市業務の重要な決定に関する情報については、否認防止対策を施すこと
・情報漏洩や紛失、システム障害が発生する前提で、被害の全容把握、早期発見・対応、被害の最小限化、早期復旧を図る構成・運用にすること
・情報運用管理者の管理外の機器（いわゆるシャドウ IT）は撲滅すること。これが発生するということは、運用と市業務との間に乖離が生じているので、運用やシステム構成を見直すこと

2.3. 事業者関係

事業者に本市業務を委託する場合等は、本市セキュリティポリシーを順守させなければならず、また定期的にその確認を行わなければならない。やむを得ず、事業者の社内規定等により順守できない場合は、情報運用管理者に諮り、対策を講じること。

（１）外部事業者やサービスの選定基準

①情報運用管理者及び情報管理者は、外部委託事業者の選定にあたり、委託内容やサービス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情報運用管理者及び情報管理者は、事業者の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、事業者を選定するよう努めなければならない。

③情報運用管理者及び情報管理者は、クラウドサービスを利用する場合は、情報の重要度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利用しなければならない。

④情報運用管理者及び情報管理者は、ソーシャルメディアサービスを利用する場合は、その利用規約等を確認し、発信する情報の重要度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利用しなければならない。

（２）契約項目

情報システムの運用、保守等を外部委託する場合には、外部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等の遵守

・外部委託事業者の責任者、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
・外部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
・外部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
・市による監査、検査
・市による情報セキュリティ危機発生時の公表
・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

情報運用管理者及び情報管理者は、外部委託事業者が必要なセキュリティ対策を講じ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しなければならない。また、その内容を情報運用管理者に報告しなければならない。

（４）職員等の遵守事項

職員等は、外部委託事業者への情報の提供等において、以下の事項を遵守しなければならない。

①外部委託事業者に情報資産を提供する場合、提供する情報を必要最小限とし、安全な受渡し方法により提供すること。

②提供した情報資産が委託先において不要になった場合は、これを確実に返却又は抹消させること。

③外部委託事業者に情報資産を提供する場合、提供する情報に関する授受の記録の管理をすること。

④委託業務において、情報セキュリティ危機の発生又は情報の目的外利用等を認知した場合は、速やかに情報運用管理者に報告すること。

2.4.在宅勤務

●在宅勤務について

本項目では、特に在宅勤務で庁内ネットワーク・庁内システム等を利用する場合について記載する。

●在宅勤務で取り扱う情報資産

在宅勤務業務にて、取り扱うことが可能な情報資産は重要度分類Ⅱ及びⅢの情報に限る

●在宅勤務で利用するネットワーク

在宅勤務業務にて、利用できるネットワークは原則LGWAN系ネットワーク及びインターネット系ネットワークとし、重要度分類Ⅰの情報資産が保管されている個人系ネットワーク等は利用してはならない。

●在宅勤務を実施するための機器

在宅勤務を行うにあたって、原則として市役所所管の機器を利用しなければならない。ただし、在宅勤務者が自宅等で操作する機器に限り情報運用管理者及び情報管理者の許可の上で在宅勤務実施者所

有の機器を利用することを認める。自宅等に持ち帰る機器には情報資産が一切残らない仕組みを備えていなければならない。

●情報運用管理者の責務

・自宅等に持ち帰る機器には情報資産が一切残らない仕組みを構築しなければならない
・在宅勤務時に重要度分類Ⅰ及び個人系ネットワークが扱えない仕組みを構築しなければならない
・在宅勤務に利用する機器は全て市役所所管の機器にするよう努めなければならない
・前例にとらわれず、利便性やセキュリティ等を十分に兼ね備えた仕組みを構築しなければならない

2.5.管理区域（サーバ室等）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、当該機器等の管理並びに運用を行うための部屋（以下「サーバ室」いう。）をいう。

②情報運用管理者・情報管理者は、管理区域を新設する場合に、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しなければならない。

③情報運用管理者・情報管理者は、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情報運用管理者・情報管理者は、サーバ室内の機器等に、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情報運用管理者・情報管理者は、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。

⑥情報運用管理者・情報管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

⑦情報運用管理者・情報管理者は、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しなければならない。

（2）管理区域の入退室管理等

①情報運用管理者･情報管理者は､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、生体認証や入退室管理簿の記載による入退室管理の実施に努めなければならない。

②職員等及び外部の事業者は、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情報運用管理者・情報管理者は、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わなければならない。

④情報運用管理者･情報管理者は､当該情報システムに関連しないコンピュータ､モバイル端末、通信回線装置、電磁的記録媒体等を使用させないようにしなければならない。

（3）情報機器の搬入出

①情報運用管理者・情報管理者は、搬入する情報機器が、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した外部の事業者に確認を行わせなければならない。また、確

認結果を情報運用管理者に報告しなければならない。

②情報運用管理者・情報管理者は、サーバ室の情報機器の搬入出について、職員を立ち会わせなければならない。

2.6.情報セキュリティインシデントの報告

（1） 情報セキュリティインシデント発生時

情報セキュリティインシデントが発生した場合、以下の対応を実施しなければならない。

●報告

・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を認知した場合やその危険性が著しく高い場合、若しくは住民等外部から報告を受けた場合、速やかに情報管理者に報告しなければならない。

・報告を受けた情報管理者は、速やかに情報セキュリティ管理者及び情報運用管理者に報告しなければならない。

・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、市民や事業者の生命・財産・権利に悪影響を及ぼす可能性がある事案については速やかに、情報の精査前に最高情報総責任者に報告しなければならない。

●対応

情報管理者および情報運用管理者は、速やかに当該情報セキュリティインシデントの早期解消と全容把握をしなければならない。対応に当たっては被害の範囲や深刻度に応じて CSIRT を設置し、対応や公表を行うこととする。

対応方針としては情報セキュリティインシデントの早期解消を第一優先させ、被害の拡大を防がなければならない。同時に全容把握に努め、認知していない被害が他に起きていないかを早急に確認しなければならない。被害の拡大が止まったことを確認した後、早期に全容把握に努め、復旧の目処などについては希望的観測を交えずに把握に努める。

全容把握とは、最低限以下の項目を究明することを言う。

・発生日、判明日、情報セキュリティインシデントの内容、判明した経緯、原因、被害範囲、被害内容、対象者

●公表

原則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管理者は、以下の基準に従い、その事実を速やかに当該対象者に公表しなければならない。被害内容が重大な場合は、最高情報総責任者が公表しなければならない。

・発生日、判明日、情報セキュリティインシデントの内容、判明した経緯、原因、被害範囲、被害内容、対象者を公表すること

・「事実」と「予想」を明確に区別し、公表すること

・被害範囲が不明な場合は、最悪の場合を想定した内容を「予想」として公表すること

・公表に当たっては、個人情報や機密情報は伏せた情報で公表すること

・システム停止等で現に市民サービスに影響が出ている場合等は、情報の収集・精査に拘らずに早急な第一報を公表しなければならない
・解決に日数を要する場合は、適宜中間報告を公表しなければならない。

（2）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

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管理者は、情報セキュリティ管理者及び情報運用管理者と連携し、これらの情報セキュリティインシデント原因を究明し、対応策及び再発防止策を講じ、必要に応じて記録を保存しなければならない。また、被害状況や対策状況を、必要に応じて最高情報総責任者に報告しなければならない。

2.7.研修・訓練

（1）情報セキュリティに関する研修・訓練

情報運用管理者は、定期的又は必要に応じて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

①情報運用管理者は、職員等に対する情報セキュリティに関する研修計画を定期的に又は必要に応じて策定しなければならない。

②情報運用管理者は、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。

③研修は、情報セキュリティ管理者、情報運用管理者、情報管理者、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するよう努めなければならない。

④情報セキュリティ管理者は、定期的に又は必要に応じて、最高情報総責任者に対して、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）研修・訓練への参加

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。

2.8.評価・見直し

2.8.1. 点検

（1）実施方法

最高情報総責任者は、情報セキュリティ管理者に対して、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、定期的又は必要に応じて点検を行わせなければならない。

（2）点検を行う者の要件

①情報セキュリティ管理者又は情報運用管理者は、点検を実施する場合には、被点検部門の所属外の者に対して、点検の実施を依頼しなければならない。
②点検を行う者は、点検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外部の識者による点検を依頼する場合は、情報セキュリティとその運用の専門家に依頼しなければならない。

（3）点検実施計画の立案及び実施への協力
①情報セキュリティ管理者は、点検を行うに当たって、点検実施計画を立案し、最高情報総責任者の承認を得なければならない。
②被点検部門は、点検の実施に協力しなければならない。

（4）点検のレベルは以下のとおりとする

点検レベル	定期的（長期）な確認項目	定期的（短期）な確認項目
Ⅲ	・情報運用管理者への定期報告	・情報システムの正常性確認 ・不要なアカウント等の削除 ・外部記録媒体等の把握 ・情報資産の重要度分類に基づいた適切な運用の確認 ・市職員の情報セキュリティへの理解と順守の確認 等
Ⅱ	・情報セキュリティ管理者（情報運用管理者）による内部点検	・上記点検レベルⅢの順守 ・情報セキュリティ管理者（情報運用管理者）への定期報告
Ⅰ	・外部の識者による点検	・上記点検レベルⅡの順守 ・情報運用管理者による内部点検

点検レベルⅠ
重要度分類Ⅱに該当する情報資産や情報システムをインターネット系あるいは特例的なネットワークに設置し、運用する情報管理者は、点検レベルⅠを実施しなければならない。
数か月に一度、情報セキュリティ管理者による内部点検を受け、毎月情報セキュリティ管理者への定期報告をしなければならない。また年に1度以上、外部の識者による点検を受けなければならない。

点検レベルⅡ
重要度分類Ⅱに該当する情報資産を、LG系ネットワークからインターネット上に持ち出し、情報のやり取りを実施・運用する情報管理者および情報運用管理者は、点検レベルⅡを実施しなければならない。なお本市HPへの情報掲載は和泉市HP掲載時における和泉市HP所管課における掲載内容の確認が行われている場合は、これに該当しない。
情報管理者は、毎月情報システムのログ確認による不正アクセス等の確認を行い、数か月に一度、情報運用管理者への定期報告をしなければならない。また年に1度以上、情報運用管理者による点検を受

けなければならない。

情報運用管理者は、毎月情報システムのログ確認による不正アクセス等の確認を行い、数か月に一度、情報セキュリティ管理者への定期報告をしなければならない。また年に１度以上、情報セキュリティ管理者による点検を受けなければならない。

点検レベルⅢ

上記点検レベルⅠあるいはⅡに該当せず情報資産および情報システムを運用する情報管理者は、点検レベルⅢを実施しなければならない。

毎月情報システム及び情報資産が適切に運用されているか、外部記録媒体等の紛失が無いか、市職員の情報セキュリティへの理解と順守が適切になされているかの確認をしなければならない。また年に１度以上、情報運用管理者への定期報告をしなければならない。

なお、セキュリティ危機を招いてしまった情報管理者は、最高情報総責任者及び情報セキュリティ管理者の判断により、点検レベルを上げる場合がある。

（５）外部委託事業者に対する点検

外部委託事業者に委託している場合、情報セキュリティ管理者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について点検を定期的に又は必要に応じて行わなければならない。

（６）保管

情報セキュリティ管理者及び情報運用管理者は、点検の実施を通して収集した点検証拠、点検報告書の作成のための点検調書を、紛失等が発生しないように適切に保管しなければならない。

（７）点検結果への対応

情報セキュリティ管理者及び情報運用管理者は、点検結果を踏まえ、指摘事項を所管する情報管理者に対し、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。

（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

ＩＴ推進本部は、点検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）市のセキュリティ対策についての点検

情報セキュリティ管理者及び情報運用管理者は年に１度以上、外部の識者による点検を受けなければならない。点検の目的は、本市のセキュリティ対策や運用が正しく実施されているか、情報セキュリティ管理者や情報運用管理者が正しく機能しているか、本市のセキュリティ対策や運用が実社会に適合しているのかを評価することにある。情報セキュリティ管理者及び情報運用管理者は点検結果を真摯に受け止め、常に改善していかなければならない。

2.8.2. 情報セキュリティポリシー及び関係規程等の見直し

ＩＴ推進本部は、情報セキュリティ点検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ふまえ、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、必要があると認めた場合、改善を行うものとする。