阪南市情報セキュリティポリシー

平成１９年　４月 策定
平成２２年　４月 一部改定
平成３１年　３月 全部改定
令和　４年　７月 一部改定

令和4年7月

LOVE NATURE
HANNAN
阪南市

〈目　次〉

〈目　次〉

〈目　次〉

序章　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、阪南市が保有する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に定めるものである。

情報セキュリティポリシーは、情報資産に関する業務に携わる本市の職員（地方公務員法第３条に規定する地方公務員及び地方教育行政の組織及び運営に関する法律第４３条第１項の規定により本市教育委員会がその服務について監督権を有する者をいう。以下同じ。）及び外部委託事業者ならびに指定管理者に浸透、普及並びに定着させるものであり、安定的な規範であることが要請される。一方、情報技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

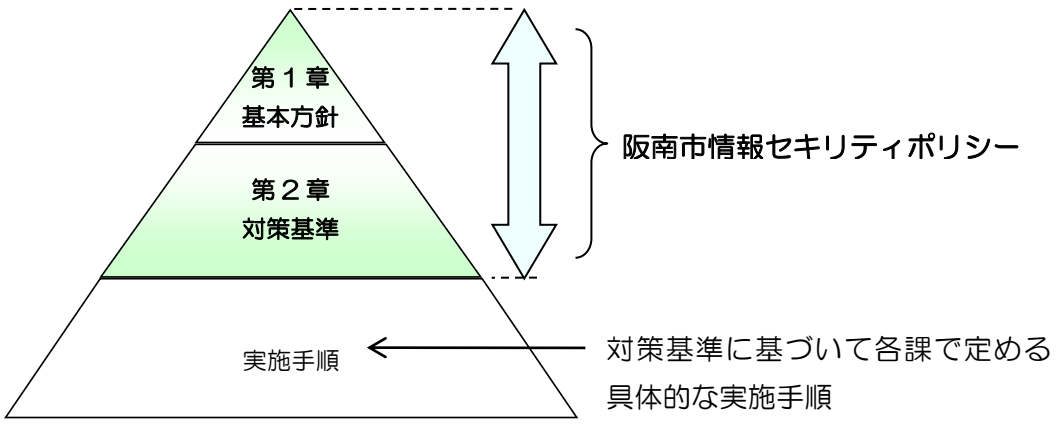
このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定するものとする。

具体的には、「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」の２階層に分け、それぞれを策定する。

また、情報システムごとの具体的な情報セキュリティ対策の運用マニュアルについては、本情報セキュリティポリシーに基づき、各課において「情報セキュリティ実施手順」として策定する。

情報セキュリティポリシーの構成

構　　成		内　　容
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に関する全庁的かつ統一的な基本方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すためのネットワーク及び情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順（運用マニュアル）		情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順



情報セキュリティ基本方針

第１章　情報セキュリティ基本方針

１　目的

阪南市情報セキュリティポリシー（以下「本ポリシー」という。）は、本市における情報セキュリティ対策の最上位に位置するものであり、本市が保有する情報資産に係る機密性（アクセスを許可されていない者には情報にアクセスさせないことを確実にすること。以下同じ。）、完全性（情報及び処理方法が、正確であること及び完全であることを保護すること。以下同じ。）及び可用性（許可された利用者に対して、要求があった場合に、情報及び関連する資産にアクセスできることを確実にすること。以下同じ。）を維持するための対策を総合的、体系的かつ具体的に定めることにより、市民の生命、財産、プライバシー等を保護すること及び安定的な行政事務の運営を図ることを目的とする。

２　定義

本ポリシーにおける用語の定義は、次のとおりとする。

⑴　職員

市長部局、教育委員会部局、選挙管理委員会事務局、公平委員会事務局、監査委員事務局、農業委員会事務局及び議会事務局の職員（臨時・非常勤職員及び任期付職員を含む。以下同じ。）並びに市立小中学校等の府費負担職員をいう。

⑵　ネットワーク

ハードウェアを相互に接続するための通信網をいう。

⑶　情報システム

ハードウェア、ソフトウェア及びネットワークにより業務処理を行う仕組みをいう。

⑷　記録媒体

電子的方式又は磁気的方式により、電子情報を記録・保存するための媒体をいう。

⑸　電子情報

情報システムで取り扱う全てのデータをいう。

⑹　情報資産

情報資産は、次のとおりとする。

①　情報システム

②　記録媒体及びパソコン等（パソコン及びモバイル端末等をいう。以下同じ。）

③　電子情報

④　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

⑺　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。

⑻　個人番号

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（以下「番号法」という。）第２条第５項に規定するものをいう。

⑼　特定個人情報

番号法第２条第８項に規定するものをいう。

⑽ 個人番号利用事務

番号法第２条第１０項に規定するものをいう。

⑾ マイナンバー利用事務系

個人番号利用事務又は戸籍事務等に関わる情報システム及び電子情報をいう。

⑿ LGWAN 接続系

人事給与、財務会計、文書管理等の LGWAN に接続された情報システム及び電子情報をいう。

⒀ インターネット接続系

インターネットメール等のインターネットに接続された情報システム及び電子情報をいう。

⒁ 無害化通信

コンピュータウイルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

３　適用範囲

⑴　本ポリシーは、本市における全ての情報資産及び全ての職員に適用する。

⑵　本市の情報資産に係る業務を外部に委託する場合又は指定管理者に実施させる場合は、当該業務の受託者又は指定管理者に対しても本ポリシーを遵守させるための措置を講ずるものとする。

４　職員の責務等

⑴　遵守義務

職員は、情報セキュリティの重要性を認識するとともに、業務の遂行に当たっては、本ポリシーを遵守する義務を負うものとする。

⑵　処分等

本ポリシーに違反した職員は、当該違反により生じた結果の重大性及び当該違反の態様の悪質性等の状況に応じて処分の対象となる。

５　情報セキュリティ対策基準の策定

情報セキュリティに関する対策を講ずるに当たり、基本的な情報セキュリティ対策基準を定めるものとする。

⑴　情報セキュリティ組織体制

本ポリシーで定める情報セキュリティを積極的に推進するための体制及び役割を定める。

⑵　情報資産の分類及び管理

情報資産をその重要度に応じて分類し、当該重要度に応じた管理方法を定める。

⑶　情報システム全体の強靭性の向上

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。
② LGWAN 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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

⑷ 物理的セキュリティ対策

ハードウェアを設置する場所の安全性の確保、当該場所への入退室の管理等の物理的な対策を定める。

⑸ 人的セキュリティ対策

情報セキュリティに関する職員の責務、職員に対する本ポリシーの啓発、情報資産に対する侵害が発生した場合の職員の報告義務等の人的な対策を定める。

⑹ 技術的セキュリティ対策

情報資産を不正なアクセスから適切に保護するためのネットワークの管理、アクセス制御等の技術的な対策を定める。

⑺ 運用面におけるセキュリティ対策

情報資産を適切に保護するための運用管理に関する対策を定める。

⑻ 外部委託等におけるセキュリティ対策

本ポリシーの適用範囲内で行う作業を外部に委託する場合等における、セキュリティに関する要求事項を明確にした契約を結ぶための必要な対策を定める。

⑼ 監査、評価及び改定

本ポリシーの実効性を検証するための監査及び点検に関する事項、本ポリシーの評価に関する事項並びに本ポリシーの改定に関する事項を定める。

⑽ その他

前各号に定めるもののほか、情報セキュリティ対策基準に関して必要な事項を定める。

6 情報セキュリティ実施手順の策定

情報セキュリティに関する対策の具体的な運用マニュアルとして、本ポリシーで定める情報セキュリティ対策基準に基づき、情報システムを利用する課において情報セキュリティ実施手順を定める。

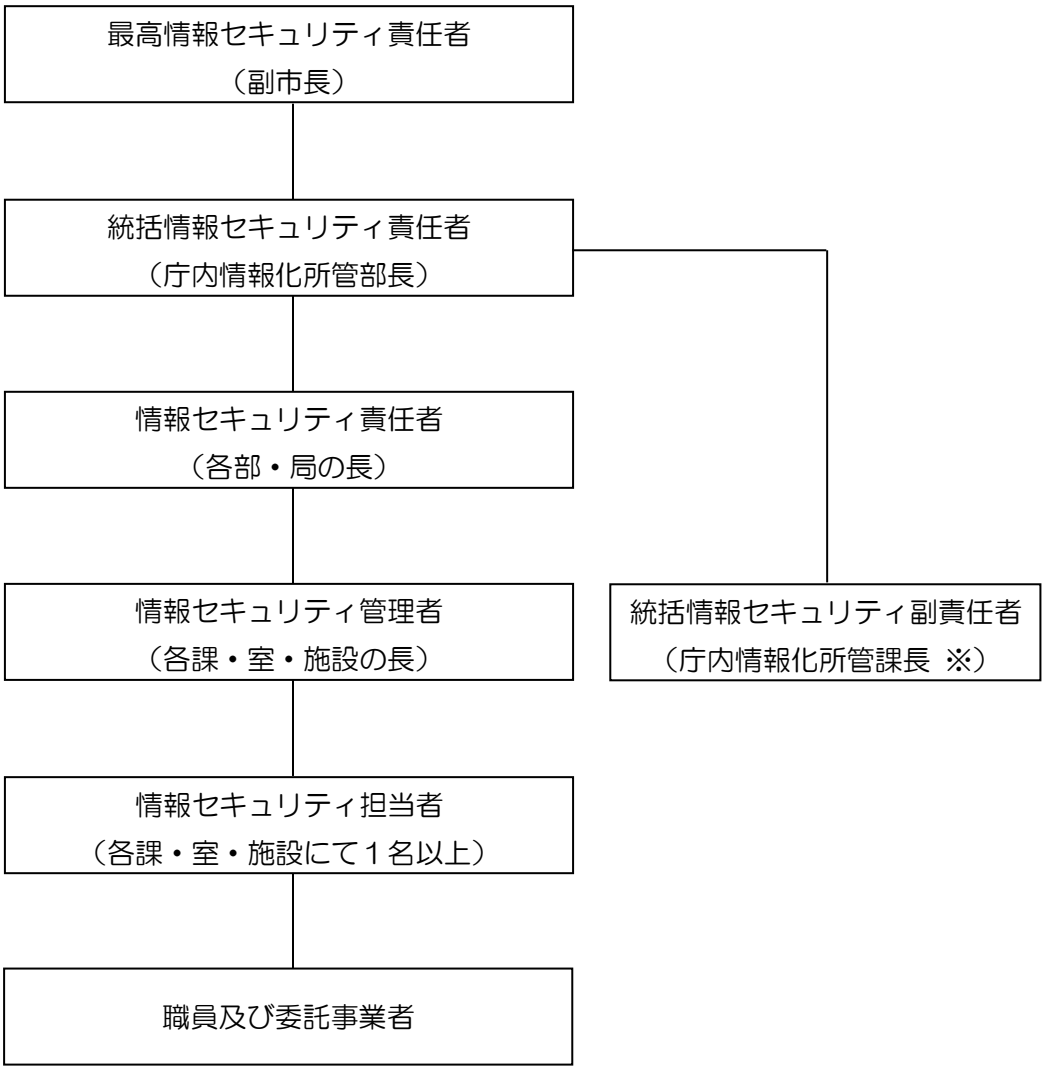
情報セキュリティ対策基準

第２章　情報セキュリティ対策基準

１　情報セキュリティ組織体制

（1）　情報セキュリティの組織体制

情報セキュリティ対策を実施するための組織体制は、以下のとおりとする。



※　統括情報セキュリティ責任者は、自身の権限に属する事務を統括情報セキュリティ副責任者に処理させることができる。

⑵　組織の構成員と役割

各組織の構成員及びその役割は以下のとおりとする。

組織・役職名	対象者・構成員	役割・権限等
最高情報セキュリティ責任者	副市長	本市における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。
統括情報セキュリティ責任者	庁内情報化所管部長	1　最高情報セキュリティ責任者を補佐する。 2　最高情報セキュリティ責任者に事故があるとき、又は最高情報セキュリティ責任者が欠けたときは、その職務を代理する。 3　情報システムを相互に接続するネットワーク等の情報システム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副責任者、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　本市の共通的な情報システムに関する情報セキュリティ実施手順の策定及び維持・管理を行う権限及び責任を有する。 6　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、最高情報セキュリティ責任者の指示に従い、最高情報セキュリティ責任者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行う権限及び責任を有する。 7　緊急時等の円滑な情報共有を図るため、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、統括情報セキュリティ副責任者、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セキュリティ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　緊急時には最高情報セキュリティ責任者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　自身の権限に属する事務を統括情報セキュリティ副責任者に処理させ

組織・役職名	対象者・構成員	役割・権限等
		ることができる。
統括情報セキュリティ副責任者	庁内情報化所管課長	統括情報セキュリティ責任者の委任により、統括情報セキュリティ責任者の権限に属する事務を処理するとともに、所管する課において所管する情報システムにおける情報セキュリティ管理者を兼ねる。
情報セキュリティ責任者	各部・局の長	1　所管する部局等及び情報システム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。 2　所管する部局等において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を策定する。なお、策定にあたっては、統括情報セキュリティ責任者に意見を求めなければならない。 3　所管する部局等において所管する情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
情報セキュリティ管理者	各課・室・施設の長	1　所管する課・室・施設（以下「課室等」という。）及び情報システム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。 2　情報セキュリティ責任者の指示に従い、所管する課室等において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策定及び更新を行う。 3　所管する課室等において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。 4　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及び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へ速やかに報告をしなければならない。また、必要に応じて最高情報セキュリティ責任者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。
情報セキュリティ担当者	各課・室・施設にて１名以上（阪南市 DX リーダ	情報セキュリティ管理者の指示等に従い、その所属する課室等の情報セキ

組織・役職名	対象者・構成員	役割・権限等
	ー設置要綱第３条第１項の規定に基づき任命された職員をもって充てる。）	ュリティに関する対策の向上を図る。
職員及び委託事業者	職員及び委託事業者	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本ポリシー及び情報セキュリティ実施手順を遵守する。

⑶　兼務の禁止

①　情報セキュリティ対策の実施において、や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　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

⑷　情報セキュリティに関する統一的な窓口の設置

①　最高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の機能を有する部署（以下「情報セキュリティに関する統一的な窓口」という。）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、自らへの報告及び関係機関との情報共有が行われる体制を整備する。

②　情報セキュリティに関する統一的な窓口は、最高情報セキュリティ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する。

③　情報セキュリティに関する統一的な窓口は、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・公表対応を行う。

２　情報資産の分類及び管理

２．１　情報資産の分類及び取扱制限

⑴　分類

本市における情報資産は、その機密性、完全性及び可用性により、次のとおり分類する。

①　重要度Ａ

阪南市個人情報保護条例（平成 12 年条例第 27 号）第２条第１項に規定する個人情報、特定個人情報及び同法第 23 条第 1 項及び第 2 項の規定により記録された特定個人情報である情報提供等記録等（以下「個人情報等」という。）や、高い機密性、完全性及び可用性を要し、漏えい、誤びゅう、損壊、滅失、紛失又は利用不可能等のセキュリティ侵害があった場合に市民の生命、財産又はプライバシーが侵害され、又は行政事務の遂行に著しい支障を及ぼすおそれがあり、取扱いを許可される職員の範囲が業務上最小限度であるべき情報資産。

② 重要度Ｂ

開示することを予定していない情報資産や、機密性、完全性及び可用性を要し、セキュリティ侵害があった場合に行政事務の遂行に支障を及ぼすおそれがあり、取扱いを許可される職員の範囲を制限するべき情報資産。

③ 重要度Ｃ

重要度Ａ及び重要度Ｂに該当しない情報資産。

⑵ 取扱制限

重要度Ａから重要度Ｃまでの情報資産について、必要に応じて次の取扱制限を行うものとする。

- 支給以外のパソコン等での作業の原則禁止
- 必要以上の複製及び配付禁止
- 保管場所の制限、保管場所への必要以上の記録媒体等の持込禁止
- 情報資産の送信、運搬及び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
- 復元不可能な処理を施しての廃棄
- 信頼のできるネットワーク回線の選択
- 電子情報のバックアップ
- 電子署名の付与
- 指定する時間以内の復旧
- 外部で情報処理を行う際の安全管理措置の規定
- 記録媒体の施錠可能な場所への保管

２．２ 情報資産の管理

⑴ 管理責任

① 情報セキュリティ管理者は、その所管する課室等において利用する情報資産及び複製され、又は伝送された情報資産について、重要度を分類し、その重要度に応じて適切に保護し、及び管理する責任を有する。ただし、１つの情報システムにおいて複数の電子情報が利用される場合で、当該複数の電子情報に係る重要度が多岐にわたる場合は、最高度の重要度に従って、当該情報システムの情報資産を取り扱わなければならない。

② 情報セキュリティ管理者は、重要度Ａ又は重要度Ｂに分類される情報資産を取り扱うことができる職員の範囲を定めなければならない。

③ 複数の情報システムで使用される電子情報を作成した課室等の情報セキュリティ管理者は、当該電子情報を適切に保護し、管理する責任を有する。

⑵ 情報資産の作成

① 職員は、業務上必要のない情報を作成してはならない。

② 情報資産を作成した者は、情報資産の分類に基づき、当該情報資産を分類し、必要に応じて取扱制限を定めなければならない。

③　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。

⑶　情報資産の入手

①　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。

②　庁外の者が作成した情報資産を入手した者は、情報資産の分類に基づき、当該情報資産を分類し、必要に応じて取扱制限を定めなければならない。

③　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。

⑷　情報資産の利用

①　情報資産を利用する者は、当該業務以外の目的に情報資産を利用してはならない。ただし、統括情報セキュリティ責任者又は当該情報資産を所管する情報セキュリティ管理者の許可を受けた場合は、この限りではない。

②　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

③　情報資産を利用する者は、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、当該記録媒体を取り扱わなければならない。

⑸　情報資産の保管

①　情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

②　情報セキュリティ管理者は、情報資産を記録した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。

③　情報セキュリティ管理者は、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記録媒体を長期保管する場合は、本市と同時に被災する可能性が低い地域に保管しなければならない。

④　情報セキュリティ管理者は、重要度Ａの情報を記録した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錠可能な場所に保管しなければならない。

⑤　職員は、情報資産を職場外に持ち出してはならない。ただし、当該情報資産を所管する情報セキュリティ管理者の許可を受けた場合は、この限りではない。

⑹　情報資産の送信

電子メール等により重要度Ａの情報資産を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑺　情報資産の運搬

①　車両等により重要度Ａの情報資産を運搬する者は、必要に応じ鍵付きの硬質ケース等に格納し、暗号化又はパスワードの設定を行う等、記録媒体を物理的に保護するための措置及び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。

② 重要度Ａの情報資産を運搬する者は、情報セキュリティ管理者の許可を得なければならない。

⑻ 情報資産の提供

① 重要度Ａの情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

② 重要度Ａ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の許可を得なければならない。

⑼ 情報資産の廃棄

① 情報資産を廃棄する者は、必要に応じて、記録媒体の初期化等の手法による情報を復元できない処理を施した上で廃棄しなければならない。

② 重要度Ａの情報資産を記録した記録媒体を廃棄する者は、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。

③ 重要度Ａの情報資産を記録した記録媒体を廃棄する者は、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靭性の向上

⑴ 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

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は、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。ただし、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。なお、外部接続先もインターネット等と接続してはならない。

② 情報のアクセス及び持ち出しにおける対策

ア 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）を行うように設定しなければならない。また、業務ごとに専用端末を設置することが望ましい。

イ 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は、原則として、USB メモリ等の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。

⑵ LGWAN 接続系

① LGWAN 接続系とインターネット接続系の分割

統括情報セキュリティ責任者は、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、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、メールやファイルをインターネット接続系から 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メールの本文をテキスト化した上で、本文の

みを転送する方式

イ　画面転送用のプロトコルにより、画面を転送する方式

ウ　無害化するサービス等を活用してファイルのサニタイズ処理（ファイルを一旦分解した上で、ウイルスが潜んでいる可能性のある部分について除去を行った後、ファイルを再構築し、分解前と同様のファイル形式に復元する方法のこと。）を行った上で、ファイルを転送する方式

⑶　インターネット接続系

①　統括情報セキュリティ責任者は、インターネット接続系において、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　統括情報セキュリティ責任者は、市区町村のインターネット接続口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。

4　物理的セキュリティ対策

4．1　サーバ等の管理

⑴　機器の取付け

情報セキュリティ管理者は、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切に固定する等、必要な措置を講じなければならない。

⑵　機器の電源

①　情報セキュリティ管理者は、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、当該機器が適切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　情報セキュリティ管理者は、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。

⑶　通信ケーブル等の配線

①　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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切に管理しなければならない。

③　情報セキュリティ管理者は、自ら又は情報セキュリティ担当者若しくは契約により操作を認められた外部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。

⑷　機器の定期保守及び修理

①　情報セキュリティ管理者は、重要度Ｂ以上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 情報セキュリティ管理者は、記録媒体を内蔵する機器を外部の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、情報セキュリティ管理者は、外部の事業者に故障を修理させるに当たり、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などを行わなければならない。

⑸ 庁外への機器の設置

情報セキュリティ管理者は、庁外にサーバ等の機器を設置する場合、最高情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器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。

⑹ 機器の廃棄等

情報セキュリティ管理者は、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、記録媒体の初期化等の手法による情報を復元できない処置を講じなければならない。

４．２ 管理区域の管理

⑴ 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、当該機器等の管理運用を行うための区域や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セキュリティ管理者は、施設管理部門と連携して、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。

③ 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は、管理区域内の機器等に、転倒及び落下の防止等の耐震対策、防火措置、防水措置等を講じなければならない。

④ 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、機器等及び記録媒体に影響を与えないようにしなければならない。

⑵ 管理区域の入退室管理等

① 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、パスワード認証又は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 職員及び外部委託事業者は、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 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が付き添うものとし、外見上職員と区別できる措置を講じなければならない。

⑶ 機器等の搬入出

① 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した事業者に確認を行わせなければならない。

② 統括情報セキュリティ責任者及び情報セキュリティ管理者は、管理区域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。

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及び情報セキュリティ管理者は、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、適切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切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及び情報セキュリティ管理者は、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及び情報セキュリティ管理者は、内部情報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及び情報セキュリティ管理者は、重要度Ｂ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、適切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等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及び情報セキュリティ管理者は、重要度Ｂ以上のデータ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 パソコン等の管理

① 情報セキュリティ管理者は、盗難防止のため、執務室等で利用するパソコン等について、ワイヤーによる固定、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。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 情報セキュリティ管理者は、情報システムへのログインに際し、パスワードの入力等を必要とするように設定しなければならない。

５ 人的セキュリティ対策

５．１ 職員の遵守事項

(1) 職員の遵守事項

① 本ポリシー等の遵守

職員は、本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

職員は、担当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 情報資産の持ち出し及び職場外における情報処理作業の制限

ア 職員は、情報資産を職場外に持ち出す場合には、当該情報資産を所管する情報セキュリティ管理者の許可を得なければならない。

イ 職員は、職場外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。

ウ 職員は、職場外で情報処理作業を行う際、支給以外のパソコン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なければならない。ただし、重要度Ａの情報資産については、支給以外のパソコン等による情報処理を行ってはならない。

④ 未許可又は不許可の記録媒体及び支給以外のパソコン等の業務利用の制限

ア 職員は、統括情報セキュリティ責任者があらかじめ使用を許可した記録媒体以外の記録媒体を業務に利用するパソコン等に接続し、及び業務に利用してはならない。

イ 職員は、支給以外のパソコン等を業務に利用するネットワークに接続し、及び業務に利用してはならない。ただし、業務上必要な場合は、統括情報セキュリティ責任者の許可を得て利用することができる。

⑤ 持ち出し及び持込みの記録

職員は、パソコン等の持ち出し及び持込みについて、記録を作成し、保管しなければならない。

⑥ パソコン等におけるセキュリティ設定変更の禁止

職員は、パソコン等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 机上のパソコン等の管理

職員は、記録媒体及びパソコン等について、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、記録媒体の容易に持ち出しをされない場所への保管や離席時のパソコン等のロック等、適切な措置を講じなければをならない。

⑧ 電子メールの利用制限

ア 職員は、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。

イ 職員は、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。

ウ 職員は、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。

エ 職員は、統括情報セキュリティ責任者が許可した場合を除き、ウェブで利用で

きるフリーメール、ネットワークストレージサービス等を使用してはならない。

⑨　退職時等の遵守事項

職員は、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。

⑵　臨時・非常勤職員及び任期付職員への対応

①　本ポリシー等の遵守

情報セキュリティ管理者は、臨時・非常勤職員及び任期付職員に対し、採用時に本ポリシー等のうち、臨時・非常勤職員及び任期付職員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　本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、臨時・非常勤職員及び任期付職員の採用の際、必要に応じ、本ポリシー等を遵守する旨の同意書への署名等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、臨時・非常勤職員及び任期付職員にパソコン等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。

⑶　外部委託事業者に対する説明

情報セキュリティ管理者は、情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、本ポリシー等のうち外部委託事業者が守るべき内容を説明し、その遵守を求めなければならない。

５．２　研修・訓練

⑴　情報セキュリティに関する研修・訓練

①　最高情報セキュリティ責任者は、定期的に職員に対する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　最高情報セキュリティ責任者は、新規採用の職員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、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及びその他職員に対して、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しなければならない。

⑵　緊急時対応訓練

最高情報セキュリティ責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練は、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。

⑶　研修・訓練への参加

全ての職員は、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

⑴　庁内からの報告

① 職員は、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、速やかに情報セキュリティ責任者及び情報セキュリティに関する統一的な窓口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、必要に応じて最高情報セキュリティ責任者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。

⑵ 住民等外部からの報告

① 職員は、本市が管理する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、速やかに情報セキュリティ責任者及び情報セキュリティに関する統一的な窓口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、必要に応じて最高情報セキュリティ責任者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。

⑶ 原因の究明・記録、再発防止等

① 統括情報セキュリティ責任者は、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及び情報セキュリティに関する統一的な窓口と連携し、これらの情報セキュリティインシデント原因を究明し、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結果から、再発防止策を検討し、最高情報セキュリティ責任者に報告しなければならない。

② 最高情報セキュリティ責任者は、統括情報セキュリティ責任者から、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 及びパスワードの取扱い

⑴ ID の取扱い

職員は、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。

⑵ パスワードの取扱い

職員は、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、統括情報セキュリティ責任者、情報セキュリティ管理者等の当該情報システムを管理する権限と責任を有する者の指示によるものを除き、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　パスワードは定期的に又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。

⑥　複数の情報システムを扱う職員は、同一のパスワードをシステム間で用いてはならない。

⑦　新規ユーザ登録等による仮のパスワードは、最初のログイン時点で変更しなければならない。

⑧　パソコン等にパスワードを記憶させてはならない。

⑨　職員間でパスワードを共有してはならない。

６　技術的セキュリティ対策

６．１　コンピュータ及びネットワークの管理

⑴　ファイルサーバの設定等

①　情報セキュリティ管理者は、職員が使用できる文書サーバの容量を設定し、職員に周知しなければならない。

②　情報セキュリティ管理者は、ファイルサーバを課室等の単位で構成し、職員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　情報セキュリティ管理者は、住民の個人情報、人事記録等、特定の職員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が閲覧及び使用できないようにしなければならない。

⑵　バックアップの実施

情報セキュリティ管理者は、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。

⑶　他団体との情報システムに関する情報等の交換

情報セキュリティ管理者は、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。

⑷　システム管理記録及び作業の確認

①　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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切に管理しなければならない。

③　情報セキュリティ管理者又は情報セキュリティ担当者及び契約により操作を認められた外部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。

⑸　情報システム仕様書等の管理

情報セキュリティ管理者は、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について、紛失又は業務上必要とする者以外の者の閲覧等がないよう、適切に管理しなければならない。

⑹　ログの取得等

①　情報セキュリティ管理者は、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　情報セキュリティ管理者は、悪意ある者による不正侵入、不正操作等の有無について、取得したログの点検又は分析を実施しなければならない。

⑺　障害記録

情報セキュリティ管理者は、職員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、適切に保存しなければならない。

⑻　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及び情報セキュリティ管理者は、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及び情報セキュリティ管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

⑼　外部の者が利用できるシステムの分離等

情報セキュリティ管理者は、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、必要に応じて他の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。

⑽　外部ネットワークとの接続制限等

①　情報セキュリティ管理者は、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、最高情報セキュリティ責任者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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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セキュリティ管理者は、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　情報セキュリティ管理者は、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) 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の措置を講じなければならない。

(12) 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など、不正操作等がなされないよう、情報セキュリティに係る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、大量のスパムメール等の受信又は送信を検知した場合は、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に周知しなければならない。

(13) 電子署名・暗号化

① 職員は、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、電子署名、暗号化又はパスワードを設定するなど、セキュリティを考慮して送信しなければならない。

② 職員は、暗号のための鍵を安全に管理しなければならない。

③ 職員は、電子署名等の正当性を検証するための情報又は手段を署名検証者等へ提供する場合は、安全な方法で提供しなければならない。

(14) 無許可ソフトウェアの導入等の禁止

① 職員は、パソコン等に無断でソフトウェアを導入してはならない。

② 職員は、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セキュリティ管理者の許可を得て、パソコン等に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。

(15) 機器構成の変更の制限

① 職員は、パソコン等に対し、機器の改造及び増設・交換を行ってはならない。

② 職員は、パソコン等に対し、業務上、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セキュリティ管理者の許可を得なければならない。

(16) 無許可でのネットワーク接続の禁止

職員は、統括情報セキュリティ責任者の許可なくパソコン等をネットワークに接続してはならない。

(17) ウェブ閲覧の制限

統括情報セキュリティ責任者は、職員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切な措置を求めなければならない。

6．2 アクセス制御

(1) アクセス制御

① アクセス制御等

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は、所管する情報システムごとに、アクセスする権限のない職員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 及びパスワードの管理

ア 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は、利用者の登録、変更及び抹消等並びに職員の異動、出向及び退職等に伴う利用者 ID 及びパスワードを適切に取り扱わなければならない。

イ 統括情報セキュリティ責任者又は情報セキュリティ管理者は、職員に対して ID 及びパスワードを発行する場合は、仮のパスワードを発行し、発行を受けた職員は、ログイン後直ちに仮のパスワードを変更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セキュリティ管理者は、職員の ID 及びパスワードに関する情報を厳重に管理しなければならない。また、パスワード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パスワード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。

エ 職員は、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セキュリティ管理者に届け出なければならない。

オ 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 及びパスワードの管理等

ア 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、統括情報セキュリティ責任者、情報セキュリティ管理者及び特権を付与された ID の発行を受けた者は、当該 ID 及びパスワードの漏えい等が発生しないよう、これら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セキュリティ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セキュリティ管理者が指名し、最高情報セキュリティ責任者が認めた者でなければならない。

ウ 最高情報セキュリティ責任者は、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及び情報セキュリティ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セキュリティ管理者は、業務上やむを得ない場合を除き、特権を付与された ID 及びパスワードの変更について、外部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セキュリティ管理者は、特権を付与された ID のパスワードについて、職員のパソコン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セキュリティ管理者は、特権を付与された ID のパスワードを初期設定以外のものに変更しなければならない。

⑵　職員による外部からのアクセス等の制限

①　職員が外部から内部の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所管する情報セキュリティ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及び情報セキュリティ管理者は、内部の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及び情報セキュリティ管理者は、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及び情報セキュリティ管理者は、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セキュリティ管理者は、外部からのアクセスに利用するパソコン等を職員に貸与する場合、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　職員は、外部から持ち込んだ、又は持ち帰ったパソコン等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、セキュリティパッチの適用状況等を確認しなければならない。

⑦　統括情報セキュリティ責任者は、公衆通信回線（公衆無線 LAN 等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID 及びパスワード、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。

⑶　特権による接続時間の制限

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は、特権による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

⑴　情報システムの調達

①　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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。

⑵　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

情報セキュリティ管理者は、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。

②　システム開発における責任者、作業者の ID の管理

ア　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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。

⑶　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　情報セキュリティ管理者は、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。

イ　情報セキュリティ管理者は、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行い、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。

ウ　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、開発したシステムについて受入テストを行う場

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。

⑷　システム開発・保守に関連する資料等の整備・保管

①　情報セキュリティ管理者は、システム開発・保守に関連する資料及びプログラムを適切に整備・保管しなければならない。

②　情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

⑸　情報システムにおける入出力データの正確性の確保

①　情報セキュリティ管理者は、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又は不正な文字列等の入力を除去する機能等の入出力データの正確性を確保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　情報セキュリティ管理者は、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、操作ログ等の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　情報セキュリティ管理者は、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。

⑹　情報システムの変更管理

情報セキュリティ管理者は、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。

⑺　開発・保守用のソフトウェアの更新等

情報セキュリティ管理者は、開発・保守用のソフトウェア等を更新し、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。

⑻　システム更新又は統合時の検証等

情報セキュリティ管理者は、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

⑴　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の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、必要に応じ職員に対して注意喚起しなければならない。

④　所管するサーバ及びパソコン等に、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。

⑵　情報セキュリティ管理者の措置事項

情報セキュリティ管理者は、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　所管するサーバ及びパソコン等に、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、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。

⑶　職員の遵守事項

職員は、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　パソコン等において、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　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。

⑤　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。

⑥　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、以下の対応を行わなければならない。

ア　パソコン端末の場合

LAN ケーブルの即時取外しを行わなければならない。

イ　モバイル端末の場合

直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

⑷　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

⑴　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　不要なサービスについて、機能を削除し、又は停止しなければならない。

②　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切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。

⑵　攻撃の予告

最高情報セキュリティ責任者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ることが明確になった場合、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、関係機関と連絡を密にして情報の収集に努めなければならない。

⑶　記録の保存

最高情報セキュリティ責任者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。

⑷　内部からの攻撃

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は、職員及び外部委託事業者が使用しているパソコン等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。

⑸　職員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セキュリティ管理者は、職員による不正アクセスを発見した場合は、当該職員が所属する課室等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

⑹　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セキュリティ管理者は、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。

⑺　標的型攻撃

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は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、職員への教育等の人的対策や内部に侵入した攻撃を早期検知して対処するための内部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セキュリティ管理者は、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・共有

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　運用管理

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セキュリティ管理者は、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セキュリティ管理者は、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セキュリティ管理者は、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。

７．２　本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、本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、速やかに最高情報セキュリティ責任者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。

②　最高情報セキュリティ責任者は、発生した問題について、適切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セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における本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切かつ速やかに対処しなければならない。

⑵　記録媒体及びパソコン等の利用状況調査

最高情報セキュリティ責任者及び最高情報セキュリティ責任者が指名した者は、不正プログラム、不正アクセス等の調査のために、職員が使用している記録媒体及びパソコン等のログ、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。

7．3　侵害時の対応等

⑴　緊急時対応計画の策定

最高情報セキュリティ責任者は、情報セキュリティインシデント、本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切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切に対処しなければならない。

⑵　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　再発防止の措置

⑶　業務継続計画との整合性確保

最高情報セキュリティ責任者は、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、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。

⑷　緊急時対応計画の見直し

最高情報セキュリティ責任者は、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

⑴　例外措置の許可

情報セキュリティ管理者は、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、最高情報セキュリティ責任者又は統括情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

⑵　緊急時の例外措置

情報セキュリティ管理者は、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、最高情報セキュリティ責任者及び統括情報セキュリティ責任者の許可を得ることなく、例外措置を取ることができる。ただし、事後速やかに最高情報セキュリティ責任者又は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。

⑶　例外措置の記録の管理

最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、例外措置の記録を適切に保管し、定期的に状況を確認しなければならない。

7．5　法令遵守

職員は、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 阪南市個人情報保護条例（平成 12 年条例第 27 号）

7．6　違反行為確認時の対応

職員の本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は、違反行為を確認した場合、当該職員が所属する課室等の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
② 情報セキュリティ管理者は、違反行為を確認した場合、速やかに当該職員が所属する課室等を所管する情報セキュリティ責任者及び情報セキュリティに関する統一的な窓口に報告し、適切な措置をとらなければならない。
③ 職員は、違反行為を確認した場合、以下の対応を行わなければならない。
ア　本ポリシーに対する違反行為を発見した場合、直ちに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。
イ　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は、統括情報セキュリティ責任者の指示に従って適切に対処しなければならない。
④ 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、当該職員の情報システムを使用する権利を停止し、又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、職員の権利を停止し、又は剥奪した旨を当該職員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　外部委託及び外部サービスの利用

8．1　外部委託

⑴　外部委託事業者の選定基準

① 情報セキュリティ管理者は、外部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、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。

⑵ 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。

- 本ポリシーの遵守
- 外部委託事業者の責任者、委託内容及び作業場所の特定
- 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
- 情報資産の複写及び複製の禁止
- 情報資産の厳重な保管及び搬送
- 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
- 本ポリシーが遵守されなかった場合の規定（損害賠償等）

⑶ 確認及び措置等

情報セキュリティ管理者は、外部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、⑵に基づき措置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最高情報セキュリティ責任者に報告しなければならない。

８．２ 約款による外部サービスの利用

⑴ 約款による外部サービスの利用に係る規定の整備

情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、重要度Ｂ以上の情報が取り扱われないようにしなければならない。

① 約款による外部サービスを利用してよい範囲

② 業務により利用する約款による外部サービス

③ 利用手続及び運用手順

⑵ 約款による外部サービスの利用における対策の実施

職員は、当該サービスの約款、その他提供条件から、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利用を申請し、適切な措置を講じた上で利用しなければならない。

８．３ 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、本市のウェブサイトに当該情報及び当該サービスへのリンク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行うこと。

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（ICカード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

② 重要度Ｂ以上の情報を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。

９ 監査及び評価等

⑴ 監査

① 情報セキュリティ管理者は、本ポリシーの実効性を検証するため、定期的に所管する情報システムの監査を実施しなければならない。

② 情報セキュリティ管理者は、監査を実施した後、速やかにその結果を評価し、その内容を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。

③ 最高情報セキュリティ責任者は、監査の結果、本ポリシーの見直しが必要と認められるときは、市長に本ポリシーの改定を勧告するものとする。

④ 統括情報セキュリティ責任者は、情報セキュリティ管理者に対し、所管する情報システムの監査を実施するよう勧告することができる。

⑵ リスク分析

情報セキュリティ管理者は、所管する課において利用する情報資産に対する脅威及び情報資産の脆弱性を識別し、情報セキュリティの観点から、どのようなリスクが発生する可能性があるかを評価するため、必要に応じてリスク分析を実施しなければならない。

⑶ 点検

① 情報セキュリティ管理者は、本ポリシーの適正な運用を確保するため、情報セキュリティに関する対策の実施状況を点検し、その結果を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。

② 統括情報セキュリティ責任者は、点検の結果を評価しなければならない。

⑷ 本ポリシーの改定

市長は、監査及び評価、情報セキュリティ管理者の点検の結果等を踏まえ、本ポリシーの改定が必要と認めるときは、最高情報セキュリティ責任者に本ポリシーの改定を指示することができる。