成田市情報セキュリティポリシー

平成２８年１月

成　田　市

＜目　　次＞

序　成田市情報セキュリティポリシーの構成・・・・・・・・・・・・・・・・・・・・　1
第１章　情報セキュリティ基本方針・・・・・・・・・・・・・・・・・・・・・・・・　2
１　目的・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
２　定義・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
（１）　ネットワーク・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
（２）　情報システム・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
（３）　情報資産・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
（４）　情報セキュリティ・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
（５）　職員・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
（６）　外部委託事業者・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
（７）　機密性・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
（８）　完全性・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　3
（９）　可用性・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　3
３　情報セキュリティポリシーの対象範囲・・・・・・・・・・・・・・・・・・・・・　3
４　職員及び外部委託事業者の義務・・・・・・・・・・・・・・・・・・・・・・・・　3
５　情報セキュリティ組織体制・・・・・・・・・・・・・・・・・・・・・・・・・・　3
６　情報資産の分類と管理・・・・・・・・・・・・・・・・・・・・・・・・・・・・　3
７　対象とする脅威・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　3
（１）　物理的脅威・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　3
（２）　人的脅威・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　3
（３）　技術的脅威・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　4
８　情報セキュリティ対策・・・・・・・・・・・・・・・・・・・・・・・・・・・・　4
（１）　物理的セキュリティ対策・・・・・・・・・・・・・・・・・・・・・・・・　4
（２）　人的セキュリティ対策・・・・・・・・・・・・・・・・・・・・・・・・・　4
（３）　技術的セキュリティ対策・・・・・・・・・・・・・・・・・・・・・・・・　4
（４）　運用・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　4
９　情報セキュリティ対策基準の策定・・・・・・・・・・・・・・・・・・・・・・・　4
10　情報セキュリティ実施手順の策定・・・・・・・・・・・・・・・・・・・・・・・　4
11　情報セキュリティポリシーの公開・・・・・・・・・・・・・・・・・・・・・・・　5
12　見直しの実施・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　5

第２章　情報セキュリティ対策基準・・・・・・・・・・・・・・・・・・・・・・・・　6
１　組織体制・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　6
（１）　最高情報セキュリティ責任者(ＣＩＳＯ)・・・・・・・・・・・・・・・・　6
（２）　統括情報セキュリティ責任者・・・・・・・・・・・・・・・・・・・・・・　6
（３）　情報セキュリティ責任者・・・・・・・・・・・・・・・・・・・・・・・・　6
（４）　情報セキュリティ管理者・・・・・・・・・・・・・・・・・・・・・・・・　6

（５） 情報システム管理者・・・・・・・・・・・・・・・・・・・・・・・・ ７
（６） 情報システム担当者・・・・・・・・・・・・・・・・・・・・・・・ ７
（７） 情報化推進リーダー（ＩＣＴ推進リーダー）・・・・・・・・・・・・・ ７
（８） 情報セキュリティに関する統一的な窓口・・・・・・・・・・・・・・ ７
２ 情報資産の分類と管理・・・・・・・・・・・・・・・・・・・・・・・・ ８
（１） 情報資産の分類・・・・・・・・・・・・・・・・・・・・・・・・・ ８
（２） 情報資産の管理・・・・・・・・・・・・・・・・・・・・・・・・・ ９
３ 物理的セキュリティ・・・・・・・・・・・・・・・・・・・・・・・・・１１
（１） サーバ等の管理・・・・・・・・・・・・・・・・・・・・・・・・・１１
（２） 管理区域・・・・・・・・・・・・・・・・・・・・・・・・・・・・１２
（３） 通信回線及び通信回線装置の管理・・・・・・・・・・・・・・・・・１３
（４） 職員の利用する端末や電磁的記録媒体等の管理・・・・・・・・・・・１３
４ 人的セキュリティ・・・・・・・・・・・・・・・・・・・・・・・・・・１４
（１） 職員の遵守事項・・・・・・・・・・・・・・・・・・・・・・・・・１４
（２） 研修・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・１６
（３） 情報セキュリティインシデント等の報告・・・・・・・・・・・・・・１６
（４） ＩＤ及びパスワード等の管理・・・・・・・・・・・・・・・・・・・１７
５ 技術的セキュリティ・・・・・・・・・・・・・・・・・・・・・・・・・１７
（１） 情報システムの管理・・・・・・・・・・・・・・・・・・・・・・・１７
（２） アクセス制御・・・・・・・・・・・・・・・・・・・・・・・・・・２１
（３） システム調達、導入、保守等・・・・・・・・・・・・・・・・・・・２２
（４） 不正プログラム対策・・・・・・・・・・・・・・・・・・・・・・・２３
（５） 不正アクセス対策・・・・・・・・・・・・・・・・・・・・・・・・２５
（６） セキュリティ情報の収集・・・・・・・・・・・・・・・・・・・・・２５
６ 運用・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・２６
（１） 情報システムの監視・・・・・・・・・・・・・・・・・・・・・・・２６
（２） 情報セキュリティポリシーの遵守状況の確認・・・・・・・・・・・・２６
（３） 侵害時の対応等・・・・・・・・・・・・・・・・・・・・・・・・・２７
（４） 外部委託・・・・・・・・・・・・・・・・・・・・・・・・・・・・２７
（５） 例外措置・・・・・・・・・・・・・・・・・・・・・・・・・・・・２８
（６） 法令遵守・・・・・・・・・・・・・・・・・・・・・・・・・・・・２８
（７） 懲戒処分等・・・・・・・・・・・・・・・・・・・・・・・・・・・２８
７ 評価・見直し・・・・・・・・・・・・・・・・・・・・・・・・・・・・２９

序　成田市情報セキュリティポリシーの構成

「成田市情報セキュリティポリシー」（以下「情報セキュリティポリシー」という。）は、成田市が所掌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取りまとめたものである。

情報セキュリティポリシーは、情報資産を取り扱う全ての職員及び外部委託事業者に浸透、普及、定着させる必要があることから安定的な規範であることが要求される。

また一方では、情報処理技術や情報通信技術の進展に伴い、情報セキュリティに対する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は、情報セキュリティ対策における基本的な方針を「情報セキュリティ基本方針」として、また、この基本方針に基づき、全ての情報システム、情報ネットワークに共通する情報セキュリティ対策の基準として「情報セキュリティ対策基準」の２階層に分けて策定することとする。

また、「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「情報セキュリティ実施手順」を策定することとする（下表参照）。

情報セキュリティポリシーの構成

文　書　名		内　容
成田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に関する統一的かつ基本的な方針。
	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全て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。
成田市情報セキュリティ実施手順		ネットワーク及び情報システム毎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。

第１章　情報セキュリティ基本方針

１　目的

成田市は、市民サービスの向上を実現するため、情報システムやネットワークを使用して行政運営に関る住民情報等、重要な情報資産を取り扱っている。

万が一、これらの情報が外部へ漏えいした場合は、極めて重大な結果を招くことが予想される。

従って、市民の財産及びプライバシー等への被害を発生させないために、情報資産や情報システム及びネットワークに対する不正アクセス、情報資産の漏えい等の脅威から保護することが必要となっている。

このようなことから、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、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。

２　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(ハードウエア及びソフトウエア)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）　情報資産

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、情報システム及び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）　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。

（５）　職員

情報資産を取り扱う全ての職員（非常勤職員を含む）。

（６）　外部委託事業者

情報システムの開発、更新、運用等を委託した事業者をいう。

（７）　機密性(confidentiality)

情報資産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。

（8） 完全性(integrity)

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。

（9） 可用性(availability)

情報資産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。

3 情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの対象範囲は、成田市役所各部課等、各支所、各行政委員会等の事務局及び各課等、消防本部及び消防署の各課等、関連各施設等のネットワーク接続機関とする。

4 職員及び外部委託事業者の義務

職員及び外部委託事業者は、情報セキュリティの重要性について統一された認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を尊守するものとする。

5 情報セキュリティ組織体制

本市の情報資産について、情報セキュリティ対策を推進するための組織体制を確立する。

6 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

7 対象とする脅威

情報セキュリティポリシーを策定するうえで、情報資産への脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべきものは次のとおりである。

（1） 物理的脅威

地震、落雷、火災等の災害によるサービス及び業務の停止、大規模・広範囲にわたる疫病による要員不足に伴うシステム運用の機能不全、電力供給の途絶、通信の途絶等のインフラの障害からの波及等

（2） 人的脅威

情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的

要因による情報資産の漏えい・破壊・消去等

（3） 技術的脅威

不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい、破壊、改ざん、消去、重要情報の搾取、内部不正等

8 情報セキュリティ対策

上記7で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

（1） 物理的セキュリティ対策

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ずる。

（2） 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員及び外部委託事業者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が講じられるように必要な対策を講ずる。

（3） 技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

（4） 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、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応マニュアルを策定する。

9 情報セキュリティ対策基準の策定

前項の情報セキュリティ対策を講ずるに当たっては、遵守すべき項目や判断基準を統一する必要がある。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」を定めるものとする。

10 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「情報セキュリティ実施手順」を策定するものとする。

11　情報セキュリティポリシーの公開

情報セキュリティポリシーは，本市の情報セキュリティ対策の指針であることから、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は公開とする。ただし、情報セキュリティ実施手順は、詳細なセキュリティ対策を示したもので、公にすることにより行政運営に重大な影響を及ぼす恐れがあるため、外部への公開は行わないものとする。

12　見直しの実施

ネットワークや情報システムの変更、新たな情報資産への脅威等、情報セキュリティを取り巻く状況の変化に対応するため、必要に応じて情報セキュリティポリシーの見直しを実施する。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための本市の情報資産に関する情報セキュリティ対策の基準である。

１　組織体制

（１）　最高情報セキュリティ責任者[ＣＩＳＯ](Chief Information Security Officer)

①　副市長を、最高情報セキュリティ責任者[ＣＩＳＯ]とする。最高情報セキュリティ責任者[ＣＩＳＯ]は、情報資産の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）　統括情報セキュリティ責任者

①　総務部長を、最高情報セキュリティ責任者[ＣＩＳＯ]直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は最高情報セキュリティ責任者[ＣＩＳＯ]を補佐しなければならない。

②　統括情報セキュリティ責任者は、本市の全て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。

③　統括情報セキュリティ責任者は、情報システムの追加、変更等を行う権限及び責任を有する。

④　統括情報セキュリティ責任者は、情報資産に関する情報セキュリティ実施手順の維持・管理等を行う権限及び責任を有する。

⑤　統括情報セキュリティ責任者は、緊急時には最高情報セキュリティ責任者[ＣＩＳＯ]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。

（３）　情報セキュリティ責任者

①　各部の長、行政委員会等の事務局の長、消防長を情報セキュリティ責任者とする。

②　情報セキュリティ責任者は、当該部局等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。

③　情報セキュリティ責任者は、その所管する部局等において所有している情報システムの追加、変更等を行う権限及び責任を有する。

④　情報セキュリティ責任者は、その所管する部局等において情報セキュリティポリシーの遵守に関し、職員に対する教育、訓練、助言及び指示を行う。

（４）　情報セキュリティ管理者

①　各課等の長、各支所長、行政委員会等の事務局の長及び各課等の長、消防本部及び消防署の各課等の長を情報セキュリティ管理者とする。

②　情報セキュリティ管理者は、その所管する課室等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。

③　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所有している情報システムの追加、変更等を行う権限及び責任を有する。

④　情報セキュリティ管理者は、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・維持・管理を行う。

（５） 情報システム管理者

① 行政管理課長を情報システム管理者とする。

② 情報システム管理者は、所管する情報システムの追加、変更等を行う権限及び責任を有する。

③ 情報システム管理者は、所管する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。

（６） 情報システム担当者

① 行政管理課情報推進係の職員を情報システム担当者とする。

② 情報システム担当者は、情報システム管理者の指示等に従い、情報システムの追加、変更等の作業を行う。

（７） 情報化推進リーダー（以下「ＩＣＴ推進リーダーという。」）

① 情報セキュリティ管理者は、所属の職員からＩＣＴ推進リーダーの職務を適切に果たせると認める職員を指名する。

② ＩＣＴ推進リーダーは、情報セキュリティ管理者をサポートし、職場における情報セキュリティ対策を推進する。

（８） 情報セキュリティに関する統一的な窓口[ＣＳＩＲＴ]（Computer Security Incident Response Teamをいう。以下、「セキュリティ対策チーム」という。）

① 統括情報セキュリティ責任者、情報システム管理者及び情報システム担当者をセキュリティ対策チームの構成員とする。

② 統括情報セキュリティ責任者をセキュリティ対策チーム責任者とする。

③ セキュリティ対策チームは、情報セキュリティインシデントについて部局等により報告を受けた場合には、その状況を確認し、最高情報セキュリティ責任者[ＣＩＳＯ]へ報告する。

④ セキュリティ対策チームは、最高情報セキュリティ責任者[ＣＩＳＯ]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。

⑤ セキュリティ対策チームは､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・公表対応を行わなければならない。

⑥ セキュリティ対策チームは、情報セキュリティに関して、関係機関やほか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う。

２　情報資産の分類と管理

（１）　情報資産の分類

情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱/制限を行うものとする。

①　機密性による情報資産の分類

分類	分類基準	情報資産の例	取扱/制限事項
３	成田市情報公開条例第７条に規定する不開示情報のうち、特定の職員等または組織など、業務上必要とする最小限の者のみが扱う情報	・特定個人情報ファイル ・基幹系ネットワークで取り扱う情報資産 ・その他、行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	分類２に掲げる対策の他、以下に掲げる事項 ・暗号化やパスワード設定し、保管すること ・インターネットに接続したパソコンへの作成・保管・複製の禁止 なお、特定個人情報については、上記に掲げる対策他、法令に定める以外の事務での取扱いを禁止する。
２	成田市情報公開条例第７条に規定する不開示情報のうち、分類３に該当する情報以外の情報資産	・行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産 ・情報系ネットワークで取り扱う情報資産	・ウイルス対策を徹底すること ・必要以上の複製及び配付の禁止 ・情報の送信、情報資産の運搬・提供時においては暗号化・パスワード設定や鍵付きケースへ格納すること ・復元不可能な処理を施して廃棄すること ・信頼のできるネットワーク回線を選択すること ・外部で情報処理を行う際は、あらかじめ安全管理措置を規定すること ・電磁的記録媒体は施錠可能な場所へ保管すること ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・許可された者以外の閲覧を制限すること
１	分類２又は分類３の情報資産以外の情報資産	・ホームページ掲載情報等	

② 完全性による情報資産の分類

分類	分類基準	情報資産の例	取扱/制限事項
2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は行政事務の適確な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	・基幹系ネットワークで取り扱う情報資産 ・契約書 ・会計情報 ・公文書等	・バックアップの作成、保管 ・権限を与えられた者だけが、アクセスできるようなシステム構築 ・ウイルス対策の徹底 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
1	分類２の情報資産以外の情報資産	・業務マニュアル等	

③ 可用性による情報資産の分類

分類	分類基準	情報資産の例	取扱/制限事項
2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は行政事務の安定的な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	・基幹系ネットワークで取り扱う情報資産	・バックアップの作成、保管及び相当時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管 ・無停電電源装置等の設置 ・サーバやネットワーク等の冗長化
1	分類２の情報資産以外の情報資産	・業務マニュアル等	

（２） 情報資産の管理

① 管理責任

ア 情報セキュリティ管理者は､その所管する情報資産について管理責任を有する。

イ 情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

② 情報資産の分類の表示

職員は、機密性２以上、完全性２、可用性２の情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル等、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

③　情報の作成

ア　職員は、業務上必要のない情報を作成してはならない。

イ　情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ　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。

④　情報資産の入手

ア　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。

イ　庁外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ　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。

⑤　情報資産の利用

ア　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

イ　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。

ウ　情報資産を利用する者は、電磁的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、当該電磁的記録媒体を取り扱わなければならない。

⑥　情報資産の保管

ア　情報セキュリティ管理者又は情報システム管理者は､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。

イ　情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的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。

ウ　情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や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電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い場所に保管しなければならない。

エ　情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的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。

⑦　情報の送信

機密性３の情報は、電子メール等により情報を送信してはならない。また、電子メール等により機密性２の情報を送信する者は、暗号化又はパスワード設定を行わなければならない。

⑧　情報資産の運搬

ア　車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、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。

イ　機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑨　情報資産の提供・公表

ア　機密性２以上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。

イ　機密性２以上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に許可を得なければならない。

ウ　情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑩　情報資産の廃棄

ア　機密性２以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

イ　情報資産の廃棄を行う者は、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。

ウ　情報資産の廃棄を行う者は、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　物理的セキュリティ

（１）　サーバ等の管理

①　機器の取付け

ア　情報システム管理者は、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。

イ　重要な情報資産を格納しているサーバは、ミラーリング等によるデータの二重化を図るなど、障害発生時に対応できるよう措置を講じなければならない。

ウ　ネットワーク管理者、情報システム管理者及び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容易に操作できないように、利用者のID、パスワードの設定等の措置を施さなければならない。

エ　無線LANの導入に当たっては、機密性２以上、完全性２、可用性２の情報資産を送信する際には経路を暗号化する等、十分な漏洩防止策を実施しなければならない。

②　機器の電源

ア　情報システム管理者は、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。

イ　情報システム管理者は、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。

③　通信ケーブル等の配線

ア　統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、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。

イ　統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて､施設管理部門から損傷等の報告があった場合、連携して対応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システム管理者は、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。

エ　統括情報セキュリティ責任者、情報システム管理者は、自ら又は情報システム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施さなければならない。

④　機器の定期保守及び修理

ア　情報システム管理者は、可用性２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。

イ　情報システム管理者は、電磁的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、庁舎内など指定した場所で修理を行わせることとする。

　又、外部に持ち出して修理をしなければならない場合は、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、情報システム管理者は、外部の事業者に故障を修理させるにあたり、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。

⑤　機器の廃棄等

情報システム管理者は、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、復元不可能な状態にする措置を講じなければならない。

（２）　管理区域

①　管理区域の構造等

ア　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や電磁的記録媒体の保管庫をいう。

イ　統括情報セキュリティ責任者及び情報システム管理者は、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な管理区域と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システム管理者は、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。

エ　統括情報セキュリティ責任者及び情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置等を講じなければならない。

オ　統括情報セキュリティ責任者及び情報システム管理者は、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。

カ　統括情報セキュリティ責任者及び情報システム管理者は、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。

②　管理区域の入退室管理等

ア　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、静脈認証等の生体認証及びパスワードによる入退室管理及び入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。

イ　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。

ウ　外部からの訪問者が管理区域に入る場合には、情報システム担当者の承認を得なければならない。

③　機器等の搬入出

ア　情報システム管理者は、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業者に確認を行わせなければならない。

イ　情報システム管理者は、情報システム室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。

（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は、機密性２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を行わなければならない。

④　統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑤　統括情報セキュリティ責任者は、可用性２の情報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に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）　職員の利用する端末や電磁的記録媒体等の管理

①　情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末の使用時以外の施錠保管等の物理的措置を講じなければならない。電磁的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 情報システム管理者は、職員が機密性２以上の情報資産を使用する場合、ログインパスワードの入力を必要とするように設定しなければならない。

③ 情報システム管理者は、端末の電源起動時のパスワード（BIOSパスワード、ハードディスクパスワード等）を併用しなければならない。

④ 情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に指紋認証等の二要素認証を併用しなければならない。

④ 情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効にしなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

⑤ 情報システム管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

⑥ 情報システム管理者は、スマートフォン、電磁的記録媒体等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講じなければならない。

４　人的セキュリティ

（１） 職員の遵守事項

① 職員の遵守事項

ア 情報セキュリティポリシー等の遵守

職員は、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。

イ 業務以外の目的での使用の禁止

職員は、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。

ウ 外部における情報処理作業の制限

最高情報セキュリティ責任者[ＣＩＳＯ]は、重要な情報資産（機密性２以上、可用性２、完全性２）の情報資産を外部で処理する場合における安全措置を定めなければならない。

エ パソコン等の持ち出し制限

職員は、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを執務室外に持ち出してはならない。但し、業務上必要な場合で、情報システム管理者の許可を受けたときは、この限りでない。

オ 持ち出しの記録

情報システム管理者は、モバイル端末、電磁的記録媒体等の持ち出しについて、記録を作成し、保管しなければならない。

カ　パソコン等の端末の持込み制限

職員は、支給以外のパソコン、モバイル端末及び電磁的記録媒体を執務室内に持ち込んではならない。

キ　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員は、パソコンやモバイル端末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システム管理者の許可なく変更してはならない。

ク　机上の端末等の管理

職員は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、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資産を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

ケ　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。

②　職員のうち非常勤職員への対応

ア　情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、職員のうち非常勤職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤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。

イ　情報セキュリティ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、職員のうち非常勤職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

ウ　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、職員のうち非常勤職員にパソコンやモバイル端末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。

③　情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

④　外部委託事業者に対する説明

ア　情報セキュリティ管理者は、ネットワーク及び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、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

イ　重要な情報資産（機密性２以上、可用性２、完全性２）に関しては、情報システムにおける取り扱いのみでなく、外部施設との搬入出時においても情報資産を暗号化、又は認証等アクセス制限を施すなど社会通念上安全が確保された措置を

講じる旨を契約書に明記しなければならない。

（２） 研修

① 情報セキュリティに関する研修の実施

最高情報セキュリティ責任者[ＣＩＳＯ]は、幹部を含めすべての職員に対する情報セキュリティに関する研修を定期的に実施しなければならない。

ア 研修は、職員に対し、毎年度１回は情報セキュリティ研修を受講できるようにしなければならない。

イ 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。

② 研修への参加

幹部を含めたすべての職員は、積極的に研修に参加しなければならない。

③ 緊急時対応訓練

最高情報セキュリティ責任者[ＣＩＳＯ]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。

（３） 情報セキュリティインシデントの報告

① 庁内からの事故等の報告

ア 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。

イ 報告を受けた情報セキュリティ管理者は、当該事故等が情報システムに関連する場合、速やかに統括情報セキュリティ責任者、情報システム管理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。

ウ 情報セキュリティ管理者は、報告のあった事故等について、必要に応じて最高情報セキュリティ責任者[ＣＩＳＯ]及び情報セキュリティ責任者に報告しなければならない。

エ ＩＣＴ推進リーダーは、所属する課等において、情報セキュリティインシデントが発生した場合、情報セキュリティ管理者をサポートし、当該セキュリティインシデントに対する初動対応を行わなければならない。

② 住民等外部からの情報セキュリティインシデントの報告

ア 職員は、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。

イ 報告を受けた情報セキュリティ管理者は、当該事故等が情報システムに関連する場合、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

ウ 情報セキュリティ管理者は、当該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[ＣＩＳＯ]及び情報セキュリティ責任者に報告しなければならない。

③ 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

ア　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システム管理者と連携し、これらの情報セキュリティインシデント原因を究明し、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の結果から、再発防止策を検討し、最高情報セキュリティ責任者[ＣＩＳＯ]に報告しなければならない。

イ　最高情報セキュリティ責任者[ＣＩＳＯ]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、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。

（4）　ＩＤ及びパスワード等の管理

①　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。

ア　自己が利用しているＩＤは、他人に利用させてはならない。

イ　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。

②　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。

ア　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

イ　パスワードは基本的に十分な長さとし、文字列は想像しにくいものにしなければならない。

ウ　パスワードが流出した恐れがある場合には、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。

エ　パスワードは定期的に変更しなければならない。

オ　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。

カ　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。

キ　パソコン等の端末にパスワードを記憶させてはならない。

ク　職員間でパスワードを共有してはならない。

５　技術的セキュリティ

（1）　情報システムの管理

①　文書ファイルサーバ等の設定等

ア　情報システム管理者は、職員が使用できる文書ファイルサーバ及び画像ファイルサーバの容量を設定し、職員に周知しなければならない。

イ　情報システム管理者は、文書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。

ウ　職員は，情報保護のため重要な情報を文書ファイルサーバ及び画像ファイルサーバに保存しなければならない。また，重要な情報をパソコン等の端末に保存してはならない。

②　バックアップの実施

統括情報セキュリティ責任者及び情報システム管理者は、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。

③　他団体との情報システムに関する情報等の交換

情報システム管理者は、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。

④　システム管理記録及び作業の確認

情報システム管理者は、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。

⑤　情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

⑥　ログの取得等

ア　統括情報セキュリティ責任者及び情報システム管理者は、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。

イ　統括情報セキュリティ責任者及び情報システム管理者は、アクセス記録等が詐取、改ざん、誤消去等されないように必要な措置を講じなければならない。

ウ　統括情報セキュリティ責任者及び情報システム管理者は、システムから自動出力したアクセス記録等について、必要に応じ、外部記録媒体にバックアップ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システム管理者は、必要に応じ、悪意ある第三者からの攻撃等の有無について、点検等を実施しなければならない。

⑦　障害記録

統括情報セキュリティ責任者及び情報システム管理者は、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。

⑧　ネットワークの接続制御、経路制御等

ア　統括情報セキュリティ責任者は、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。

イ　統括情報セキュリティ責任者は、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。

⑨　外部の者が利用できるシステムの分離等

情報システム管理者は、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、必要に応じ他のネットワーク及び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。

⑩　外部ネットワークとの接続制限等

ア　情報システム管理者は、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[ＣＩＳＯ]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。

イ　情報システム管理者は、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、庁内の全てのネットワーク、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。

ウ　情報システム管理者は、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。

エ　統括情報セキュリティ責任者及び情報システム管理者は、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。

オ　情報システム管理者は、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　複合機のセキュリティ管理

ア　統括情報セキュリティ責任者は、複合機を調達する場合は、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

イ　統括情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ　統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

⑫　特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

⑬　無線LAN 及びネットワークの盗聴対策

ア　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。

イ　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、暗号化等の措置を講じなければならない。

⑭　電子メールのセキュリティ管理

ア　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よう、

電子メールサーバの設定を行わなければならない。

イ　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。

ウ　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。

エ　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。

オ　統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

カ　統括情報セキュリティ責任者は、職員が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置しなければならない。

⑮　電子メールの利用制限

ア　職員は、自動転送機能を用いて、電子メールを転送してはならない。

イ　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。

ウ　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。

エ　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。

オ　職員は、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。

⑯　暗号化

職員は、情報資産の分類により定めた取扱制限に従い、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、最高情報セキュリティ責任者[ＣＩＳＯ]が定めた暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

⑰　無許可ソフトウェアの導入等の禁止

ア　職員は、パソコン等やモバイル端末に無断でソフトウェアを導入してはならない。

イ　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システム管理者の許可を得て、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又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

ウ　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。

⑱　機器構成の変更の制限

ア　職員は、パソコン等やモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

イ　職員は、業務上、パソコン等やモバイル端末に対し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システム管理

者の許可を得なければならない。

⑲　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やモバイル端末をネットワークに接続してはならない。

⑳　業務以外の目的でのウェブ閲覧の禁止

ア　職員は、業務以外の目的でウェブを閲覧してはならない。

イ　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。

（２）　アクセス制御

①　アクセス制御等

ア　アクセス制御

ⅰ　統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は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。

ⅱ　情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に指紋認証等の二要素認証を併用しなければならない。

イ　利用者ＩＤの取扱い

ⅰ　統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

ⅱ　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システム管理者に通知しなければならない。

ⅲ　統括情報セキュリティ責任者及び情報システム管理者は、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。

ウ　特権を付与されたＩＤの管理等

ⅰ　統括情報セキュリティ責任者及び情報システム管理者は、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しなければならない。

ⅱ　統括情報セキュリティ責任者及び情報システム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システム管理者が指名し、最高情報セキュリティ責任者[ＣＩＳＯ]が認めた者でなければならない。

ⅲ　最高情報セキュリティ責任者[ＣＩＳＯ]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、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

ⅳ　統括情報セキュリティ責任者及び情報システム管理者は、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。

ⅴ　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された

ＩＤを初期設定以外のものに変更しなければならない。

② 職員による外部からのアクセス等の制限

ア 職員が外部から内部のネットワーク又は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管理する情報システム管理者の許可を得なければならない。

イ 統括情報セキュリティ責任者は、内部のネットワーク又は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。

ウ 統括情報セキュリティ責任者は、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。

エ 統括情報セキュリティ責任者は、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。

オ 統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末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。

カ 職員は、外部から持ち帰ったモバイル端末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、パッチの適用状況等を確認しなければならない。

キ 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ＩＤ及びパスワード、生体認証に係る情報等の認証情報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。

ク 統括情報セキュリティ責任者又は情報システム管理者は、職員の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。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。

ケ 統括情報セキュリティ責任者又は情報システム管理者は、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なければならない。

コ 情報システム管理者は、特権によるネットワーク及び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。

（３） システム調達、導入、保守等

① 情報システムの調達

ア 統括情報セキュリティ責任者及び情報システム管理者は、情報システムの開発、導入、保守等の調達にあたっては、情報セキュリティ上問題にならないかどうか、確認しなければならない。

イ 情報セキュリティ管理者は、その所管する課室等が独自に情報システムの開発、導入、保守等の調達を行ときは、統括情報セキュリティ責任者及び情報システム

管理者に報告し、情報セキュリティ上問題にならないか、確認を求めなければならない。

ウ　統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達にあたっては、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。

エ　情報セキュリティ管理者は、その所管する課室等が独自に機器及びソフトウェアの調達を行うときは、統括情報セキュリティ責任者及び情報システム管理者に報告し、当該製品のセキュリティ機能が情報セキュリティ上問題にならないか、確認を求めなければならない。

② 情報システムの導入

ア　開発環境と運用環境の分離及び移行手順の明確化

ⅰ　情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

ⅱ　情報システム管理者は、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。

ⅲ　情報システム管理者は、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。

ⅳ　情報システム管理者は、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。

イ　テスト

ⅰ　情報システム管理者は、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。

ⅱ　情報システム管理者は、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。

ⅲ　情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

ⅳ　情報システム管理者は、開発したシステムについて受け入れテストを行う場合、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。

③ ソフトウェアの保守及び更新

情報システム管理者は、ソフトウェア等を更新、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。

（4） 不正プログラム対策

① 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。

ア　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。

イ　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。

② 情報システム管理者の措置事項

情報システム管理者は、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。

ア　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、必要に応じ職員等に対して注意喚起しなければならない。

イ　所掌するサーバ及びパソコン等の端末に、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。

ウ　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。

エ　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。

オ　インターネットに接続していないシステムにおいて、電磁的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。

③ 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。

ア　パソコン等やモバイル端末において、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。

イ　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。

ウ　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。なお、標的型攻撃と疑われる不審なメールについては削除する前に、情報システム管理者に報告し、指示に従わなければならない。

エ　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

オ　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。

カ　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。

キ　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、以下の対応を行った後、情報システム管理者に報告しなければならない。また、ＩＣＴ推進リーダーは、その対応のサポートを行わなければならない。

ｉ　パソコン等の端末の場合

ＬＡＮケーブルの即時取り外しを行わなければならない。

ⅱ　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。

（５）　不正アクセス対策

①　統括情報セキュリティ責任者の措置事項

ア　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、使用されていないポートを閉鎖しなければならない。

イ　不要なサービスについて、機能を削除又は停止しなければならない。

ウ　統括情報セキュリティ責任者は、セキュリティ対策チームと連携し、監視、通知、外部連絡窓口およ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。

②　攻撃の予告

最高情報セキュリティ責任者[ＣＩＳＯ]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。

③　記録の保存

最高情報セキュリティ責任者[ＣＩＳＯ]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。

④　内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員及び外部委託事業者が使用しているパソコン等の端末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。

⑤　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システム管理者は、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。

⑥　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システム管理者は、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。

⑦　標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、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、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

（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システム管理者は、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及び共有

統括情報セキュリティ責任者及び情報システム管理者は、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。

６　運用

（1） 情報システムの監視

ア　統括情報セキュリティ責任者及び情報システム管理者は、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。

イ　統括情報セキュリティ責任者及び情報システム管理者は、重要なアクセス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。

ウ　統括情報セキュリティ責任者及び情報システム管理者は、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。

（2） 情報セキュリティポリシーの遵守状況の確認

① 遵守状況の確認及び対処

ア　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[ＣＩＳＯ]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。

イ　最高情報セキュリティ責任者[ＣＩＳＯ]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。

ウ　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティ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。

② パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

最高情報セキュリティ責任者[ＣＩＳＯ]及び最高情報セキュリティ責任者[ＣＩ

ＳＯ]が指名した者は、不正アクセス、不正プログラム等の調査のために、職員が使用しているパソコン、モバイル端末及び電磁的記録媒体のログ、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。

③　職員の報告義務

ア　職員は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに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、情報セキュリティ実施手順及び緊急時対応マニュアルに従って適切に対処しなければならない。

（３）　侵害時の対応等

①　緊急時対応マニュアルの策定

最高情報セキュリティ責任者[ＣＩＳＯ]は、情報セキュリティインシデント、情報セキュリティ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、緊急時対応マニュアルを定めておき、セキュリティ侵害時には当該マニュアルに従って適切に対処しなければならない。

②　緊急時対応マニュアルに盛り込むべき内容

緊急時対応マニュアルには、以下の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

③　緊急時対応マニュアルの見直し

最高情報セキュリティ責任者[ＣＩＳＯ]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マニュアルの規定を見直さなければならない。

（４）　外部委託

①　外部委託事業者の選定基準

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　覚書等

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情報セキュリティ実施手順に定める要件について、覚書を交わす等注意しなければならない。

③　確認・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、前項の覚書等に基づき措置しなければならない。

（５） 例外措置

① 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、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[ＣＩＳＯ]の許可を得て、例外措置を取ることができる。

② 緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、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、事後速やかに最高情報セキュリティ責任者[ＣＩＳＯ]に報告しなければならない。

③ 例外措置の申請書の管理

最高情報セキュリティ責任者[ＣＩＳＯ]は、例外措置の申請書及び審査結果を適切に保管しなければならない。

（６） 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12月13日法律第261号)
② 著作権法(昭和45年5月6日法律第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8月13日法律第128号)
④ 個人情報の保護に関する法律(平成15年5月30日法律第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5月31日法律第27号)
⑥ 成田市個人情報保護条例(平成17年12月28日条例第53号)

（７） 懲戒処分等

① 懲戒処分

情報セキュリティポリシーに違反した職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

② 違反時の対応

職員の情報セキュリティ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。

ア 統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者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、適切な措置を求めなければならない。

イ 情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに

統括情報セキュリティ責任者及び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。

ウ　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、当該職員のネットワーク又は情報システムを使用する権利を停止あるい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､職員の権利を停止あるいは剥奪した旨を最高情報セキュリティ責任者[ＣＩＳＯ]及び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。

7　評価・見直し

（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、当該部課の情報セキュリティが確保されていることを確認するため、自主点検を行い、必要に応じ改善措置を講じなければならない。

（2）　最高情報セキュリティ責任者[ＣＩＳＯ]は、評価及び見直しが必要となる事象が発生した場合には、必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。

（3）　最高情報セキュリティ責任者[ＣＩＳＯ]は、自主点検の結果及び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毎年度および重大な変化が発生した場合に、必要があると認めた場合、改善を行うものとする。