高崎市情報セキュリティポリシー

改正：平成３１年４月１日

（第六版）

高　崎　市

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、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。

1.2. 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）高崎市情報ネットワーク

行政上必要な情報を送受信する目的で、高崎市の組織・施設間を接続したＬＡＮ及びＷＡＮをいう。

（4）情報資産

業務を実施するのに必要な情報及びそれを扱う情報システムをいう。

（5）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。

（6）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。

（7）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。

（8）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。

（9）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無く、情報にアクセスできる状態を確保することをいう。

（１０）個人情報

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるものをいう。

（１１）個人番号

住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

（１２）特定個人情報

個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報をいう。

（１３）マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（１４）ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等ＬＧＷＡＮに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１５）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１６）通信経路の分割

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、安全が確保された通信だけを許可できるようにすることをいう。

（１７）無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

1.3. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（1）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、重要情報の詐取、内部不正等

（2）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）地震、落雷、火災等の災害によるサービス及び業務の停止等

（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. 適用範囲

（1）情報セキュリティポリシーの適用範囲

本基本方針及び情報セキュリティ対策基準が適用される範囲は、次のとおりとする。

① 高崎市情報ネットワークに接続された市長部局、委員会、市議会事務局、消防局及び地方公営企業の組織及び施設

② 上記以外で、高崎市情報ネットワークにより接続された組織及び施設

（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、情報システム並びにこれらに関する設備及び電磁的記録媒体

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、ネットワーク図等のシステム関連文書

1.5. 職員等の遵守義務

職員及び再任用職員、嘱託職員、臨時職員、派遣社員（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。

1.6. 情報セキュリティ対策

上記１．３の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じる。

（１）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全庁的組織体制を確立する。

（２）情報資産の分類と管理

本市の保有する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講じる。

（３）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。

（４）物理的セキュリティ

サーバ等、情報システム機械室等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

（５）人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（６）技術的セキュリティ

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。

（７）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。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、緊急時対応計画を策定する。

1.7. 情報セキュリティ監査及び自己点検の実施

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監査及び自己点検を実施する。

1.8. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、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。

1.9. 情報セキュリティ対策基準の策定

上記１．６、１．７及び１．８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

1.10. 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。

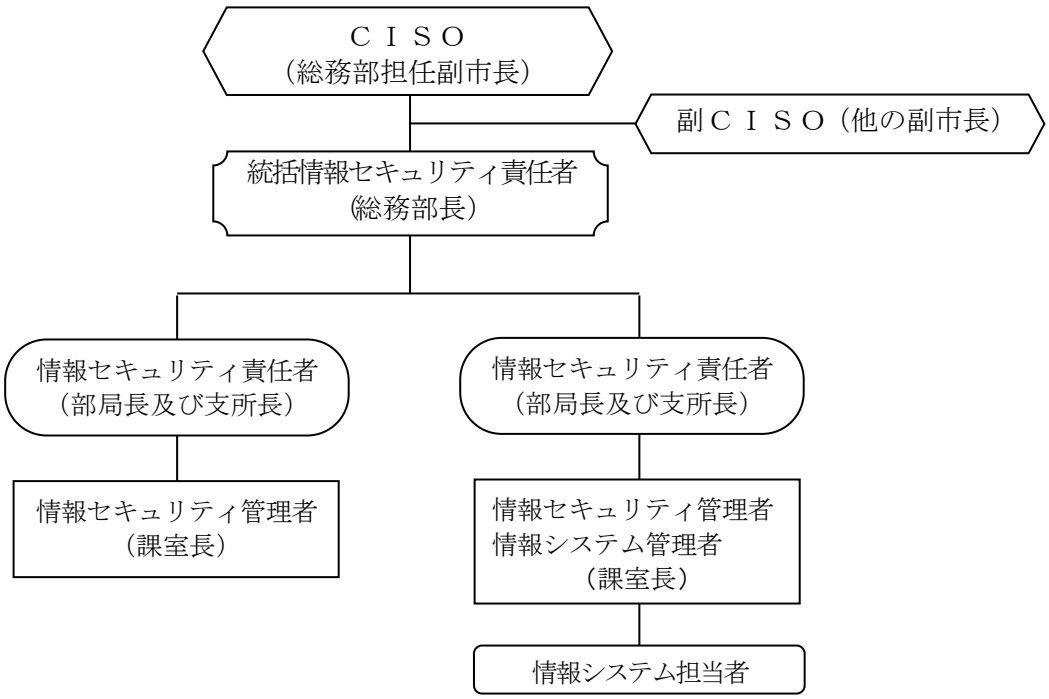
なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

情報セキュリティ対策基準

2.1. 対象範囲

対象となる行政機関の範囲及び情報資産の範囲は、情報セキュリティ基本方針の規定による。

2.2. 組織体制



高崎市情報セキュリティ運用組織体制図

（1）最高情報セキュリティ責任者（ＣＩＳＯ：Chief Information Security Officer、以下「ＣＩＳＯ」という。）

① 総務部を担任する副市長をＣＩＳＯとする。ＣＩＳＯは、本市における全てのネットワーク、情報システム等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 ＣＩＳＯは、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ことができる。

（2）最高情報セキュリティ副責任者（以下「副ＣＩＳＯ」という。）

他の副市長を副ＣＩＳＯとする。副ＣＩＳＯは、ＣＩＳＯを補佐し、ＣＩＳＯに事故があるときはその職務を代行する。

（3）統括情報セキュリティ責任者

① 総務部長を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、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、本市の全てのネットワーク、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。

③ 統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、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。

④ 統括情報セキュリティ責任者は、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、ＣＩＳＯの指示に従い、ＣＩＳＯ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。

⑤ 統括情報セキュリティ責任者は、本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑥ 統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、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、情報システム管理者、情報システム担当者を網羅する連絡体制を整備しなければならない。

⑦ 統括情報セキュリティ責任者は、緊急時には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。

（４）情報セキュリティ責任者

① 各部局長及び支所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及びネットワークにおける開発、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。

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所有している情報システム及びネットワークについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

（５）情報セキュリティ管理者

① 各課室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、その所掌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、統括情報セキュリティ責任者及びＣＩＳＯへ速やかに報告を行い、指示を仰がなければならない。

（６）情報システム管理者

① 各情報システム及びネットワークの担当課室長を、当該情報システム等に関する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等における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 情報システム管理者は、所管する情報システム等における情報セキュリティに関する権限及び責任を有する。

④ 情報システム管理者は、所管する情報システム等に係る情報セキュリティ実施手順の維持・管理を行う。

（7）情報システム担当者

情報システム管理者の指示に従い、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。

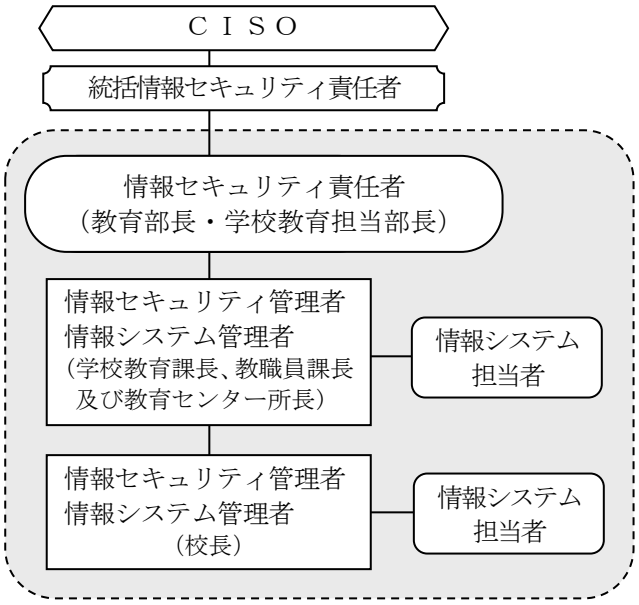
（8）学校における情報セキュリティ運用組織体制

① 校長を情報セキュリティ管理者とする。

② 校長は、その所管する学校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 校長を、その学校が所管する情報システム等に関する情報システム管理者とする。

④ 校長は、情報システム等の設定変更、運用、見直し等に関して、学校教育課長、教職員課長又は教育センター所長への申請、報告、連絡の義務を負うものとする。



学校における情報セキュリティ運用組織体制図

（9）情報セキュリティ委員会

① 本市の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、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。

② 情報セキュリティ委員会の組織、事務等については、情報セキュリティ委員会に関する要綱において定める。

③ 情報セキュリティ委員会は、毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

（１０）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。

（１１）ＣＳＩＲＴの設置・役割

① ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化すること。

② ＣＩＳＯは、ＣＳＩＲＴに所属する職員を選任し、その中からＣＳＩＲＴ責任者を置くこと。

また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員を定めること。

③ ＣＩＳＯは、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し、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。

④ 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こと。

⑤ 情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、総務省、都道府県等へ報告すること。

⑥ 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。

⑦ 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う。

2.3. 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、重要性に応じて次のとおり分類を行うものとする。

重　要　性　分　類
Ａ　個人情報（特定個人情報を含む）及び取扱いを必要最小限の者に限定する必要がある情報資産（非公開情報）
Ｂ　上記以外の情報資産

（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、管理台帳を作成のうえ管理する責任を有する。

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 識別番号の表記

情報セキュリティ管理者は、情報資産を格納する電磁的記録媒体について、固有の識別番号を表記した上で適切な管理を行わなくてはならない。

③ 情報の作成

ア 職員等は、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、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、Ａ分類の情報を記録した外部電磁的記録媒体を保管する場合、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

ア 職員等は、Ａ分類の情報資産について、ファックスで外部に送信してはならない。

イ 職員等は、Ａ分類の情報資産のうち、個人情報については電子メールで外部に送信してはならない。

ウ 職員等は、Ａ分類の情報資産のうち、個人情報以外の情報を電子メールで外部に送信する場合、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Ａ分類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 Ａ分類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 Ａ分類の情報資産を外部に提供する者は、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 Ａ分類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。ただし、当該情報資産が個人情報の場合は、高崎市個人情報保護条例（平成３年高崎市条例第６号）の規定に従うものとする。

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 Ａ分類の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、物理的に破壊する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。

2.4. 情報システム全体の強靭性の向上

（１）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

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・持ち込みにおける対策

（ア）情報のアクセス対策

情報システムが正規の利用者かどうかを判断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）を利用しなければならない。

（イ）情報の持ち出し及び持ち込み不可設定

原則として、ＵＳＢメモリ等の電磁的記録媒体による端末への情報持ち出し及び端末への情報持ち込みができないように設定しなければならない。

（２）ＬＧＷＡＮ接続系

① ＬＧＷＡＮ接続系とインターネット接続系の分割

ＬＧＷＡＮ接続系とインターネット接続系は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、メールやデータを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インターネットメールの本文のみをＬＧＷＡＮ接続系に転送する方式

（イ）インターネット接続系の端末から、ＬＧＷＡＮ接続系の端末へ画面を転送する方式

（３）インターネット接続系

① インターネット接続系においては、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 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。

2.5. 物理的セキュリティ

2.5.1. サーバ等の管理

（１）機器の取付け

情報システム管理者は、サーバ及びその付帯機器（以下「サーバ等」という。）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。

（２）サーバの冗長化

① 情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを二重化等により冗長化しなければならない。

② 情報システム管理者は、サーバに障害が発生した場合のシステム運用停止時間は最小限にしなければならない。

（３）機器の電源

① 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。

② 情報システム管理者は、重要なサーバについて 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。

（４）通信ケーブル等の配線

① 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。

② 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。

（５）機器の定期保守及び修理

① 情報システム管理者は、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 情報システム管理者は、A分類の情報を記録した機器を外部の事業者に修理させる場合、情報を消去した状態で行わせなければならない。情報を消去できない場合、情報システム管理者は、修理を委託する事業者との間で、守秘義務契約等を締結するほか、秘密保持体制の確認等を行わなければならない。

（６）外部への機器の設置

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、ハウジング等によりサーバ等の機器を外部設置する場合、ＣＩＳＯの承認を得なければならない。また、定期的に当該機器へ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。

（７）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すべ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。

2.5.2. 管理区域（情報システム機械室等）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「情報システム機械室」という。)又は電磁的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システム管理者は、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管理区域を設置しなければならない。また、外部からの侵入が容易にできないよう配慮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じるドアは必要最小限とし、鍵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 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、情報システム機械室内の機器等に、転倒及び落下防止、耐震対策等の防災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、可能な限り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

① 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、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を行わなければならない。

② 職員等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 情報システム管理者は、外部からの訪問者が管理区域に入る場合には、管理区域への入退室を許可された職員等に必要に応じて付き添わせ、外見上職員等と区別できる措置を講じなければならない。

④ 情報システム管理者は、A分類の情報資産を扱うシステム及びネットワークを設置している管理区域について、当該情報システム及びネットワーク上で必要としない、私物を含むコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（3）機器等の搬入出

① 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。

② 情報システム管理者は、情報システム機械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。

2.5.3. 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システム管理者は、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システム管理者は、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システム管理者は、A分類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及び情報システム管理者は、ネットワークに使用する回線について、伝送途上に情報の破壊、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。

2.5.4. 職員等のパソコン等の管理

① 情報システム管理者は、情報システムのログイン時にログインパスワードの入力、ＩＣカードまたは生態認証を必要とするように設定しなければならない。

② 情報システム管理者は、ＯＳのログイン時にログインパスワードの入力、ＩＣカードまたは生態認証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、必要に応じ、パソコンやモバイル端末におけるデータを暗号化できるようにしなければならない。

④ 情報システム管理者は、マイナンバー利用事務系では「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（多要素認証等）を行うよう設定しなけ

ればならない。

2.6. 人的セキュリティ

2.6.1. 職員等の遵守事項

（1）職員等の遵守事項

① 情報セキュリティポリシー等の遵守

職員等は、情報セキュリティ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

職員等は、業務以外の目的で情報資産の外部への持出し、情報システムへのアクセス、電子メール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 パソコン、モバイル端末及び電磁的記録媒体等の持出し及び外部における情報処理作業の制限

ア 統括情報セキュリティ責任者は、A分類の情報資産を外部で処理する場合における実施手順を定めなければならない。

イ 職員等は、A分類の情報資産、パソコン、モバイル端末及び電磁的記録媒体を外部に持ち出す場合には、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 職員等は、外部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。

④ 私物のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

職員等は、私物のパソコン、モバイル端末及び電磁的記録媒体等を業務に利用してはならない。ただし、私物のパソコン、モバイル端末については、業務上必要な場合、情報資産の処理に使用しないことを条件に、情報セキュリティ管理者の許可を得て利用することができる。

⑤ 持出しの記録

情報セキュリティ管理者は、A分類の情報資産を記録したパソコン、モバイル端末及び電磁的記録媒体の持出しについて、記録を作成し、保管しなければならない。

⑥ ＵＳＢメモリ等の電磁的記録媒体等の利用の制限

職員等は、同一のＵＳＢメモリ等の電磁的記録媒体をマイナンバー利用事務系、ＬＧＷＡＮ接続系及びインターネット接続系等の複数の端末で利用してはならない。

⑦ インターネット接続系端末の情報資産保存の制限

職員等はインターネット系端末にA分類の情報資産を保存してはならない。

⑧ 机上の端末等の管理

職員等は、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を閲覧されることがないように、離席時のパソコン及びモバイル端末のシャットダウン又はロックや電磁的記録媒体及び文書等を容易に閲覧されない場所へ保管するなど、適切な措置を講じなければならない。

⑨ 退職時等の遵守事項

職員等は異動、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）嘱託及び臨時職員への対応

① 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、嘱託及び臨時職員に対し、採用時に情報セキュリティポリシー等のうち、嘱託及び臨時職員が守るべき内容を理解させ、遵守させなければならない。

② 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、嘱託及び臨時職員の採用の際、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。

③ マイナンバー利用事務系、ＬＧＷＡＮ接続系及びインターネット接続系への接続制限

情報セキュリティ管理者は、嘱託及び臨時職員にパソコン等の端末による作業を行わせる場合において、マイナンバー利用事務系、ＬＧＷＡＮ接続系及びインターネット接続系への接続が不要のときは、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、職員等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

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を理解させなければならない。

2.6.2. 研修・訓練

（１）情報セキュリティに関する研修

ＣＩＳＯは、定期的に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）研修計画の立案及び実施

① 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計画を定期的に立案し、情報セキュリティ委員会の承認を得なければならない。

② 研修計画において、職員が毎年度最低１回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。

③ 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。

④ 研修は、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しなければならない。

⑤ ＣＩＳＯは、毎年度１回、情報セキュリティ委員会に対して、職員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）緊急時対応訓練

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。訓練計画は、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。

（4）研修への参加

幹部を含めたすべての職員は、定められた研修に参加しなければならない。

2.6.3. 情報セキュリティインシデントの報告

（1）庁内からの情報セキュリティインシデントの報告

① 職員等は、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。

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、情報システム管理者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。

（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

① 職員等は、本市が管理するネットワーク、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。

③ 情報セキュリティ管理者は、当該事故等について、必要に応じて統括情報セキュリティ責任者及びＣＩＳＯ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

① ＣＳＩＲＴは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

② ＣＳＩＲＴは、情報セキュリティインシデントであると評価した場合、ＣＩＳＯに速やかに報告しなければならない。

③ ＣＳＩＲＴは、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

④ ＣＳＩＲＴは、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、ＣＩＳＯに報告しなければならない。

⑤ ＣＩＳＯは、ＣＳＩＲＴ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。

2.6.4. ＩＤ及びパスワード等の管理

（１）ＩＤの取扱い

職員等は、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。

（２）パスワードの取扱い

職員等は、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。

② パスワードを他人の目に付く状態（ディスプレイへの貼付など）で放置してはならない。

③ パスワードは十分な長さとし、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変更し、古いパスワードを再利用してはならない。

⑥ 仮のパスワードは、速やかに変更しなければならない。

⑦ パソコン等の端末のパスワードの記憶機能を利用してはならない。

2.7. 技術的セキュリティ

2.7.1. コンピュータ及びネットワークの管理

（１）文書サーバ（共有フォルダ）の設定等

① 情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

② 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、職員等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、特定の職員等しか取り扱えないデータについて、当該ファイルにパスワードを設定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等が閲覧及び使用できないようにしなければならない。

（２）バックアップの実施

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、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）システム管理記録及び作業の確認

① 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。

② 情報システム管理者は、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、窃取、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。

（４）情報システム仕様書等の管理

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、記録する媒体にかかわらず、業務上必要とする者以外の者が閲覧できないよう、又は紛失等がないよう、適切に管理しなければならない。

（５）ログの取得等

① 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。

② 情報システム管理者は、ログが窃取、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。

③ 情報システム管理者は、システムから出力したログについて、必要に応じ、外部電磁的記録媒体にバックアップしなければならない。

（６）障害記録

情報システム管理者は、職員等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、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。

（７）ネットワークの接続制御、経路制御等

① 情報システム管理者は、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 情報システム管理者は、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。

（８）外部ネットワークとの接続制限等

① 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、必要に応じて高崎市個人情報保護審議会の意見を聴いた上で、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。

② 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、庁内のすべてのネットワーク、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。

③ 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。

④ 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。

⑤ 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。

（9）複合機のセキュリティ管理

① 統括情報セキュリティ責任者は、複合機を調達する場合、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。

② 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。

③ 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。

（１０）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。

（１１）無線LAN及びネットワークの盗聴対策

① 情報システム管理者は、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 情報システム管理者は、機密性の高い情報を扱うネットワークについて、情報の盗聴等を防ぐため、必要に応じ暗号化等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及び情報システム管理者は、大量のスパムメール等を受信しないための対策を講じなければならない。

② 情報システム管理者は、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。

③ 情報システム管理者は、職員等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等に周知しなければならない。

（１３）電子メールの利用制限

① 職員等は、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。

② 職員等は、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。

③ 職員等は、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。

④ 職員等は、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。

⑤ 職員等は、インターネット上で利用できるフリーメール、ストレージサービス等を統括情報セキュリティ責任者の許可なく使用してはならない。

（１４）無許可ソフトウェアの導入等の禁止

① 職員等は、パソコン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。

② 職員等は、業務上の必要がある場合は、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。

③ 職員等は、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 職員等は、パソコン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。

② 職員等は、業務上、パソコン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、情報システム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

職員等は、情報システム管理者の許可なくパソコンやモバイル端末等をネットワークに接続してはならない。

（１７）インターネットアクセスに関する措置

① 職員等は、業務以外の目的でインターネットを閲覧してはならない。

② 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、職員等のインターネット利用について、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。

③ 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、職員等及び市民が、本市のネットワーク経由でインターネットにアクセスする際、不適切なサイトへアクセスできないよう制限しなければならない。

2.7.2. アクセス制御

（１）アクセス制御

① アクセス制御

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等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・パスワードの取扱い

ア 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、職員等の異動、出向又は退職に伴う利用者ＩＤ・パスワードの取扱い等の方法を定めなければならない。

イ 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。

③ 特権を付与されたパスワードの管理等

ア 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パスワードを利用する者を必要最小限にし、当該パスワードの漏えい等が発生しないよう、当該パスワードを厳重に管理しなければならない。

イ 情報システム管理者は、特権を付与されたパスワードの変更について、許可なく外部委託事業者に行わせてはならない。

2.7.3. システム開発、導入、改修等

（1）情報システムの調達

① 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。

② 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、情報システム開発、導入、改修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

情報システム管理者は、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・パスワードの管理

ア 情報システム管理者は、システム開発の責任者及び作業者が使用するＩＤ・パスワードを管理し、開発完了後、開発用ＩＤ・パスワードを削除しなければならない。

イ 情報システム管理者は、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）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 情報システム管理者は、システム開発・改修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。

イ 情報システム管理者は、システム開発・改修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・改修計画の策定時に手順を明確にしなければならない。

ウ 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わなければならない。また、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。

② テスト

ア 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。

イ 情報システム管理者は、本番運用を行う前に、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。

③ システム開発・改修に関連する資料等の保管

ア 情報システム管理者は、システム開発・改修に関連する資料及び文書を適切な方法で保管しなければならない。

イ 情報システム管理者は、テスト結果を一定期間保管しなければならない。

ウ 情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

④ 情報システムにおける入出力データの正確性の確保

ア 情報システム管理者は、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

チェック機能及び不正な文字列等の入力を除去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。

イ 情報システム管理者は、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。

⑤ 情報システムの変更管理

情報システム管理者は、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。

⑥ 開発・改修用のソフトウェアの更新等

情報システム管理者は、開発・改修用の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。

2.7.4. 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。

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、必要に応じ職員等に対して注意喚起しなければならない。

④ 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。

⑤ 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。

（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。

① 情報システム管理者は、その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 コンピュータウイルス等の感染を防止するために、市が管理している電磁的記録媒体以外を職員等に利用させてはならない。

⑤ 侵入した不正プログラムを発見・駆除するため、必要なパソコンに対し、定期的に不正プログラムの検索（スキャン）を行わなければならない。

（３）職員等の遵守事項

職員等は、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。

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、添付ファイルを開かずに削除しなければならない。ただし、明らかに本市単独を攻撃の対象としている（標的型、やり取り型）と判断できた場合は、速やかに情報セキュリティ管理者、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。

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 情報システム管理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）パソコン等の端末の場合

LAN ケーブルの即時取り外し又は無線機能の無効化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。

（４）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。

2.7.5. 不正アクセス対策

（１）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。

② 使用されていないサーバのポートを閉鎖しなければならない。

② メーカー等からパッチの提供があり次第、必要に応じ、サーバ及びクライアントにパッチをあてなければならない。

③ ＩＰアドレスの自動取得用サーバを使用する場合には、認証等の不正アクセス対策を行わなければならない。

④ 公開を目的としたサーバは、内部ネットワークと異なるネットワーク上に設置しなければならない。

（２）攻撃の予告

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、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

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、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律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）職員等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、職員等による不正アクセスを発見した場合は、当該職員等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。

（5）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、庁外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。

（6）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、標的型攻撃による庁内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、庁内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。

2.7.6. セキュリティ情報の収集

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等のセキュリティ情報を収集し、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等の緊急度に応じて、職員等に周知し、ソフトウェア更新等の対策を実施しなければならない。

2.8. 運 用

2.8.1. 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、重要な情報システムについては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。

2.8.2. 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

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、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。

② 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。

③ 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）端末等の利用状況調査

ＣＩＳＯ及びＣＩＳＯ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、職員等が使用しているパソコン、モバイル端末及び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。

2.8.3 侵害時の対応

（1）緊急時対応計画の策定

情報セキュリティ委員会は、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、緊急時対応計画を定めておき、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。

（2）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 再発防止措置の策定

（3）緊急時対応計画の見直し

情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化又は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。

（4）業務継続計画との整合性確保

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た場合、情報セキュリティ委員会は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。

2.8.4. 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、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

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。

2.8.5. 法令遵守

職員等は、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サイバーセキュリティ基本法（平成２８ 年法律第３１ 号）
⑦ 高崎市個人情報保護条例（平成３年高崎市条例第６号）
⑧ 高崎市文書取扱規定（平成４年高崎市訓令第３号）

2.8.6. 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等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、地方公務員法及び高崎市職員の懲戒処分の基準に関する要綱（平成１７年高崎市訓令第９号）による懲戒処分の対象とする。

（２）違反時の対応

職員等が情報セキュリティポリシーに違反し、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、当該職員等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、職員等の権利を停止し、又は剥奪した旨をＣＩＳＯ及び当該職員等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。

2.9. 外部サービスの利用

2.9.1. 外部委託

（１）外部委託先の選定基準

① 情報セキュリティ管理者は、外部委託先の選定にあたり、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、情報の機密性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

情報システムの開発・運用等を外部委託する場合には、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。

① 情報セキュリティポリシーの遵守
② 委託内容及び作業場所の特定
③ 提供された情報の目的外利用の禁止及び業務上知り得た情報の守秘義務
④ 再委託に関する制限事項の遵守
⑤ 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・市による調査権
⑥ 市による情報セキュリティインシデント発生時の公表
⑦ 情報漏洩等により、市に損害が発生した場合の規定(損害賠償等)

（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、（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するとともに、その重要度に応じてＣＩＳＯに報告しなければならない。

（４）委託事業者の遵守義務

委託事業者は、高崎市長から開示された重要性分類Ａの情報資産を扱う場合、次の事項を遵守しなければならない。

① 委託事業者は、その中から、開示された情報資産の取扱いに関し、すべての責任と権限を有する情報取扱責任者を任命しなければならない。
② 委託事業者は、情報取扱責任者をはじめ、情報資産を取扱うすべての従事者の氏名を高崎市長に報告しなければならない。
③ 情報取扱責任者は、情報資産の機密を保持するため、情報資産を取扱うすべての従事者に対し、遵守すべき事項を研修等により理解させなければならない。
④ 委託事業者は、情報資産への不当なアクセス又は情報資産の漏洩、紛失、破壊、盗難、改ざん等（以下「漏洩等」という。）を防止するための方策を、高崎市長に報告しなければならない。
⑤ 委託事業者は、漏洩等のリスクを考慮し、最大限の注意をもって情報資産を管理しなければならない。

2.9.2. 約款による外部サービスの利用

（１）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、Ａ分類の情報が取扱われないように規定しなければならない。

（ア）約款によるサービスを利用してよい範囲

（イ）業務により利用する約款による外部サービス
（ウ）利用手続及び運用手順

（2）約款による外部サービスの利用における対策の実施
職員等は、利用するサービスの約款、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約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

2.9.3. ＳＭＳ（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ＳＭＳ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ＳＭＳ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、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）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 A分類の情報をＳＭＳで発信してはならない。
③ 利用するＳＭＳごとの責任者を定めなければならない。

2.10. 評価・見直し

2.10.1. 監 査

（1）実施方法
情報セキュリティ委員会は、情報セキュリティ監査統括責任者を指名し、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、定期的に又は必要に応じて監査を行わせなければならない。

（2）監査を行う者の要件
① 情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。
② 監査を行う者は、監査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）監査実施計画の立案及び実施への協力
① 情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。
② 被監査部門は、監査の実施に協力しなければならない。

（4）外部委託事業者に対する監査
外部委託事業者に委託している場合、情報セキュリティ監査統括責任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監査

を定期的に又は必要に応じて行わなければならない。

（5）報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

（6）保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠及び監査報告書の作成のための監査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）監査結果への対応

ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、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セキュリティ管理者に対しても、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の見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、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。

2.10.2. 自己点検

（1）実施方法

① 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、所管するネットワーク及び情報システムについて、定期的に又は必要に応じ自己点検を実施しなければならない。

② 情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度又は必要に応じ自己点検を行わなければならない。

（2）報告

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責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

（3）自己点検結果の活用

① 職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

② 情報セキュリティ委員会は、この点検結果を情報セキュリティポリシーの見直し、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。

2.10.3. 情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティ監査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毎年度及び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。

改正履歴

版	改正年月日	改正内容
第一版	平成１４年　８月　１日	制定
第二版	平成１７年１１月　１日	改正
第二版	平成１８年　１月２３日	支所及び支所長設置に伴う改正
第二版	平成１９年　４月　１日	地方自治法改正に伴う改正
第三版	平成２０年１１月　１日	改正
第三版	平成２１年　４月　１日	・副市長２人制に伴う改正 ・学校の情報セキュリティ運用組織体制に関する規定を追加
第三版	平成２２年１１月　１日	委託事業者の遵守義務を追加
第三版	平成２３年　４月　１日	機構改革に伴う改正他
第三版	平成２５年　４月　１日	機構改革に伴う改正
第四版	平成２７年　４月　１日	改正
第五版	平成２８年　４月　１日	改正
第五版	平成２９年　４月　１日	ネットワーク強靭化等に伴う改正
第六版	平成３１年　４月　１日	改正

用　語　解　説

索引	用　語	解　　説
あ	ＩＣカード	半導体集積回路（ＩＣチップ）を埋め込み、情報を記録できるようにしたカード。
	ＩＤ	集団の中で個人を識別するための符号。
	ＩＰアドレス	ネットワークに接続された機器を識別するための符号
	アクセス権限	コンピュータの利用者に与えられた、システムやファイル、フォルダ、周辺機器などを利用する権限。
	アクセス制御	システムやファイル、フォルダ、周辺機器などに対し、許可された者以外の利用や、許可された方式以外での利用を制限すること。
	暗号化	ネットワークを通じてデータをやり取りする際に、通信途中で第三者に盗み見られたり改ざんされたりしないよう、決まった規則に従ってデータを変換すること。
	イントラネット	インターネットと同じ技術で構築された組織内のネットワーク。
	ウェブサーバ	ホームページなどをインターネット上に公開するためのサーバ。
	ＳＭＳ（Ｓｏｃｉａｌ Ｍｅｄｉａ Ｓｅｒｖｉｃｅ）	インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったＷｅｂ サイトやネットサービスなどを総称する用語で、電子掲示板（ＢＢＳ）やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。
	ＯＳのパスワード	パソコンを起動する際に入力するパスワード
か	外部ネットワーク	インターネット等の庁外のネットワーク。
	仮のパスワード	システム等へ最初にログインするためのパスワード。ログイン後、正パスワードに変更する。
	クライアント	サーバが提供するサービスを利用するためのコンピュータ。主にパソコンのことを指す。
	経路制御	複数のネットワークに接続している通信回線装置が受け取ったデータを、どのネットワークを使って送るかを決めること。
	ゲートウェイ	組織内ネットワークと外部ネットワークの接続点（出入口）にある装置。データの中継を行う。
	コンピュータウイルス	インターネット等を介してコンピュータに入り込み、意図的に悪影響を及ぼすように作られたプログラム。悪質なものは、プログラム、データ等の破壊や情報漏えいなどを引き起こす。
さ	サイト	ウェブページ群が置かれているインターネット上の場所。ホームページと同義。
	サーバの冗長化	サーバが緊急停止した場合でも業務を継続できるようにすること。
	サーバの二重化	サーバのバックアップシステムを設置すること。
	サーバのポート	ソフトウェア又はハードウェアが外部とデータをやり取りするための出入口。
	サービス不能攻撃	ネットワークを経由した攻撃のひとつであり、相手のコンピュータやルータ

		などに不正なデータを送信して使用不能に陥らせたり、アクセス量を増大させて相手のネットワークやサーバを麻痺させる攻撃。
	時刻同期	サーバ間で時刻設定を自動的に合わせること。
	ＣＳＩＲＴ（Computer Security Incident Response Team）	（シーサート）情報セキュリティインシデントに対応する緊急時の庁内即応組織。
	システム関連文書	システム設計書やプログラム仕様書等、保有する情報システムに関わる文書。
	障害記録	システム障害の内容や発生日等を記録したもの。システム障害への対応時に過去に起きた類似障害を参考とするため、適切に保存する。
	情報システム仕様書	情報システムの仕様（スペック）を記載した文書。
	情報システムの監視	情報システムへの 攻撃等を防ぐため、情報システムの稼動状況を常に監視すること。
	情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いもの。
	スパムメール	受信者の意向とは関係なく、無差別に大量配信される迷惑メール。
	生体認証	指紋や静脈、眼球の虹彩などの身体的特徴によって本人確認を行う認証方式。
	セキュリティホール	ソフトウェアの設計ミスなどによって生じたセキュリティ上の弱点。
	ソースコード	プログラミング言語を用いて記述したプログラム。
た	多要素認証	システムが正規の利用者かどうかを判断する際の信頼性を高めるために、複数の認証手段を組み合わせて認証する方式をいう。
	端末	情報システムの構成要素である機器のうち、職員が情報処理を行うために直接操作するもの。（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）クライアント。
	通信回線	情報を伝送する回線・ネットワーク。
	通信回線装置	通信回線に接続して、通信を行うための装置。スイッチ、ルータ等。
	ディスプレイ	パソコン等で画面を表示するための装置。
	電子メールボックス	受信した電子メールを保存しておくサーバ内の領域（郵便箱）。
	電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、ＵＳＢ メモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ、磁気テープ等の外部電磁的記録媒体。
	特定用途機器	テレビ会議システム、ＩＰ電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているもの。
な	ネットワークストレージサービス	インターネット上で、ファイル保管用サーバを利用させるサービス。
は	ハウジング	サーバ等を委託業者の施設内に預けて運用するサービス。
	パソコン	端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。
	パターンファイル	ウイルス対策ソフトがウイルスを発見するために照合するファイル。個々のウイルスの特徴を収録している。
	バックアップ	コンピュータに保存されたデータやプログラムを、破損や消失、コンピュー

		タウイルス感染などに備え、別の電磁的記録媒体に保存すること。
	パッチ	一旦完成したプログラムの一部を修正すること。また、修正を行うための変更点のみを抜き出したファイル。
	ハブ	ＬＡＮで使われる集線装置。スイッチとも呼ぶ。
	標的型攻撃	明確な意思と目的を持った人間が、特定のターゲットや情報に対して、特定の目的のために行うサイバー攻撃の一種をいう。
	ファイアウォール	組織内のネットワークへ外部から侵入されるのを防ぐシステム。
	フィルタリング	許可された通信以外を制限すること。
	不正アクセス	組織内のネットワークに外部から不正に侵入する行為。
	不正プログラム	コンピュータを利用する者が意図しない結果を、コンピュータにもたらすソフトウェアの総称。コンピュータウイルス、スパイウェアなど。
	フリーメール	インターネット上で無料で提供される電子メールサービス。申請し自分のメールアドレスを開設できる。例：Ｙａｈｏｏメール、Ｇメールなど
ま	無線ＬＡＮ	無線を使って構築したＬＡＮ。
	モバイル端末	情報処理端末のうち、業務上の必要に応じて、移動させて使用することを目的としたものをいい、端末の形態は問わない。
や	約款による外部サービス	民間事業者等の庁外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。
	予備電源	何らかの要因で電力供給が途絶した場合に、機器が適正に停止するまでの間、電力を供給するために設けた予備の電源。
ら	ＬＡＮ	ローカルエリアネットワークの略。同一敷地内など限定地域内のネットワーク。
	ルータ	ネットワーク上を流れるデータを他のネットワークに中継する装置。
	ログ	サーバ等の利用状況を記録すること。利用者のＩＰアドレスや利用された日付、時刻、利用されたファイル名などを記録する。
	ログインパスワード	情報システムやネットワークへ接続（ログイン）するために入力する数字や文字列による符号。
わ	ＷＡＮ	ワイドエリアネットワークの略。ＬＡＮ同士を接続した広域のネットワーク。