北杜市情報セキュリティポリシー文書

第 5.0 版

基本方針・対策基準

令和 7 年 11 月

北杜市

改訂履歴

版	日付	区分	理由及び内容
第 1.0 版	平成 17 年 3 月	新規制定	
第 2.0 版	平成 28 年 8 月 1 日	一部改訂	総務省情報セキュリティガイドライン（平成 27 年 3 月版）に合わせて一部改訂
第 3.0 版	令和元年 11 月 6 日	一部改訂	総務省情報セキュリティガイドライン（平成 30 年 9 月版）に合わせて一部改訂
第 4.0 版	令和 5 年 3 月 14 日	一部改訂	総務省情報セキュリティガイドライン（令和 4 年 3 月版）に合わせて一部改訂
第 5.0 版	令和 7 年 11 月 25 日	一部改訂	総務省情報セキュリティガイドライン（令和 7 年 3 月版）に合わせて一部改訂

目次

北杜市情報セキュリティ基本方針

1 目的.....5
2 定義.....5
3 対象とする脅威.....6
4 適用範囲.....6
5 職員等の遵守義務.....7
6 情報セキュリティ対策.....7
7 情報セキュリティ監査及び自己点検の実施.....8
8 情報セキュリティポリシーの見直し.....8
9 情報セキュリティ対策基準の策定.....9
10 情報セキュリティ実施手順の策定.....9

北杜市情報セキュリティ対策基準

1 目的.....10
2 組織体制.....10
3 情報資産の分類と管理.....13
4 情報システム全体の強靭性の向上.....16
5 物理的セキュリティ.....17
5.1 サーバ等の管理.....17
5.2 管理区域（サーバ室等）の管理.....19
5.3 通信回線及び通信回線装置の管理.....20
5.4 職員等の利用する端末や電磁的記録媒体等の管理.....21
6 人的セキュリティ.....21
6.1 職員等の遵守事項.....21
6.2 研修・訓練.....23
6.3 情報セキュリティインシデントの報告.....24
6.4 ID 及びパスワード等の管理.....25
7 技術的セキュリティ.....26
7.1 コンピュータ及びネットワークの管理.....27
7.2 アクセス制御.....33
7.3 システム開発、導入、保守等.....35
7.4 不正プログラム対策.....39
7.5 不正アクセス対策.....41
7.6 セキュリティ情報の収集.....42
8 運用.....43

8.1 情報システムの監視.....43
8.2 情報セキュリティポリシーの遵守状況の確認.....45
8.3 侵害時の対応等.....45
8.4 例外措置.....46
8.5 法令遵守.....46
8.6 懲戒処分等.....47
9 業務委託と外部サービス（クラウドサービス、以下「外部サービス等」という。）の利用.....47
9.1 業務委託.....48
9.2 情報システムに関する業務委託.....50
9.3 外部サービス等の利用（自治体機密性２以上の情報を取り扱う場合）.....51
9.4 外部サービス等の利用（自治体機密性２以上の情報を取り扱わない場合）.....56
10 評価・見直し.....56
10.1 監査.....56
10.2 自己点検.....58
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.....58

北杜市情報セキュリティ基本方針

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。

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) 情報セキュリティ
情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 情報セキュリティポリシー
本基本方針及び情報セキュリティ対策基準をいう。

(5) 機密性
情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(6) 完全性
情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7) 可用性
情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(8) 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。

(9) 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（マイナンバー利用事務系を除く。）。

(10) 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。

(11) 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。

(12) 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。

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、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、風水害、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

4 適用範囲

(1) 適用範囲

情報セキュリティポリシーの適用範囲は、市全て（学校及び病院を除く。）の情報資産並びに情報資産を活用するための設備、さらに、これら情報資産に接する全ての職員（会計年度任用職員等、雇用形態によらず市の情報資産に接するすべての者（以下「職員等」という。））及び情報資産の取扱を委託された者（以下「委託事業者」という。）とする。

(2) 情報資産の範囲

情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。

① ネットワーク及び情報システム並びにこれらに関する設備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並びに行政情報（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

5 職員等の遵守義務

職員等は、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。

6 情報セキュリティ対策

上記 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な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実施する。

(3) 情報システム全体の強靭性の向上
情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、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、山梨県及び市町村のインターネットとの通信を集約した上で、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、サーバ室、通信回線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、業務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正に対応するため、緊急時対応計画を策定する。

(8) 業務委託と外部サービス（クラウドサービス）の利用
業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。
外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。
ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

(9) 評価・見直し
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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能

性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9 情報セキュリティ対策基準の策定

上記６、７及び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。

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。

北杜市情報セキュリティ対策基準

本対策基準は、情報セキュリティ基本方針を実行に移すための、本市における情報資産に関する情報セキュリティ対策の基準を定めたものである。

1 目的

本対策基準は、情報セキュリティ要求水準を実現するための遵守事項や判断基準等を定めることを目的とする。

2 組織体制

(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 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最高情報セキュリティアドバイザーとして置き、その業務内容を定めることができる。

③ CISO は、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

④ CISO は、CISO を助けて本市における情報セキュリティに関する事務を整理し、CISO の命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副 CISO」という。）１人を必要に応じて置くことができる。

⑤ CISO は、本対策基準に定められた自らの担務を、副 CISO その他の本対策基準に定める責任者に担わせることができる。

(2) 統括情報セキュリティ責任者

① 企画部長を 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 及び副 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 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責任者は、情報セキュリティ責任者、情報システム・情報セキュリティ総合管理者、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。

⑤ 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実施する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、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。

⑦ 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、情報システム・情報セキュリティ総合管理者、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含めた緊急連絡網を整備しなければならない。

⑧ 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。

⑨ 統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

(3) 情報セキュリティ責任者

① 部局の長、行政委員会事務局の長及び地方公営企業の局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並びに職員、会計年度任用職員等（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

(4) 情報システム・情報セキュリティ総合管理者(以下、総合管理者という。)

① 管財課長を総合管理者とする。

② 総合管理者は、全庁で共通的に利用される情報システム基盤、情報資産及び情報セキュリティ対策の運用管理について、権限及び責任を有する。

③ 総合管理者は、全庁的な情報資産の脆弱性情報を収集・分析し、その対応を統

括するとともに、情報システムのアクセスログ等を一元的に監視し、不正な利用の検知に努めなければならない。

④ 総合管理者は、各情報システム管理者及び情報セキュリティ管理者と緊密に連携し、共通基盤の利用に関する技術的な支援や、セキュリティ対策の導入支援を行う。

⑤ 総合管理者は、セキュリティ侵害が発生した場合、統括情報セキュリティ責任者の指示のもと、原因究明に必要なログ等の情報を提供し、共通基盤における被害拡大防止措置を実施しなければならない。

(5) 情報セキュリティ管理者

① 部局の課長、出先機関の長、行政委員会事務局の課長及び地方公営企業の課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、総合管理者、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 各情報システムの担当課長等を当該情報システム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等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

(8) 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実施するため、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。

(9) 専門部会

専門部会は、セキュリティ委員会の求めに応じ、本市の情報セキュリティポリシーに関する事項の分析、情報セキュリティに関連する課題の調査、研究等を

行う。

(10) 兼務の禁止

① 情報セキュリティ対策の実施において、止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 情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、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、その役割を明確化しなければならない。

② CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

③ CISO は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

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しなければならない。

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、山梨県へ報告しなければならない。

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、委託事業者等との情報共有を行わなければならない。

(12) クラウドサービス利用における組織体制

① 統括情報セキュリティ責任者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

3 情報資産の分類と管理

(1) 情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、別表 1 のとおり分類し、必要に応じ取扱制限を行うものとする。

(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） 情報システム管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

（ウ） 情報セキュリティ管理者は、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。

（エ） 総合管理者及び情報セキュリティ管理者は、クラウドサービスの環境に保存される情報資産についても（１）の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定めなければならない。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

② 情報資産の分類の表示

職員等は、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、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正な管理を行わなければならない。

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） 情報を作成する職員等は、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） 情報を作成する職員等は、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） 職員等が作成した情報資産を入手した他の職員等は、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職員等は、(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職員等は、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職員等は、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職員等は、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ） 情報資産を利用する職員等は、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） 総合管理者、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、情報資産を適正に保管しなければならない。

（イ） 総合管理者、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） 総合管理者、情報セキュリティ管理者又は情報システム管理者は、自治体機密性２以上、自治体完全性２又は自治体可用性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

電子メール等により自治体機密性２以上の情報を送信する職員等は、必要に応じ、パスワード等による暗号化を行わなければならない。

⑧ 情報資産の運搬

（ア） 車両等により自治体機密性２以上の情報資産を運搬する職員等は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用や流出・盗難を防止するための措置を講じなければならない。

（イ） 自治体機密性２以上の情報資産を運搬する職員等は、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） 自治体機密性２以上の情報資産を外部に提供する職員等は、必要に応じパスワード等による暗号化を行わなければならない。

（イ） 自治体機密性２以上の情報資産を外部に提供する職員等は、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 情報資産の廃棄等

（ア） 情報資産の廃棄やリース返却等を行う職員等は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

（イ） 情報資産の廃棄やリース返却等を行う職員等は、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） 情報資産の廃棄やリース返却等を行う職員等は、情報セキュリティ管理者の許可を得なければならない。

（エ） 情報資産の廃棄やリース返却等を行う職員等は、クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

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。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。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

② 情報のアクセス及び持ち出しにおける対策

（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。また、業務毎に専用端末を設置することが望ましい。

（イ） 情報の持ち出し不可設定

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。

③ マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離しなければならない。

④ マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用す

る場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

(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 接続系に転送するメールテキスト化方式

（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

（ウ） 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

② LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

(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 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 山梨県及び市町村のインターネットとの通信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、関係省庁や山梨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。

5 物理的セキュリティ

5.1 サーバ等の管理

(1) 機器の取付け

総合管理者及び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正に固定する等、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 総合管理者及び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冗長化し、同一データを保持するよう努めなければならない。

② 総合管理者及び情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にするよう努めなければならない。

(3) 機器の電源

① 総合管理者及び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、当該機器が適正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 総合管理者及び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。

(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、総合管理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、総合管理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。

③ 統括情報セキュリティ責任者、総合管理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正に管理しなければならない。

④ 統括情報セキュリティ責任者、総合委管理者及び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。

(5) 機器の定期保守及び修理

① 総合管理者及び情報システム管理者は、自治体可用性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。

② 総合管理者及び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、情報システム管理者は、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等を行わなければならない。

(6) 庁外への機器の設置

統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、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

① 総合管理者及び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 総合管理者及び情報システム管理者は、クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）を行う場合、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。

なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

5.2 管理区域（サーバ室等）の管理

(1) サーバ室の構造等

① サーバ室とは、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、当該機器等の管理及び運用を行うための部屋をいう。

② 総合管理者は、サーバ室における自然災害による被害を軽減する措置を講じなければならない。また、外部からの侵入が容易にできないよう措置を講じなければならない。

③ 総合管理者は、施設管理部門と連携して、サーバ室から外部に通ずる出入口は必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④ 総合管理者は、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤ 総合管理者は、サーバ室に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

(2) サーバ室の入退室管理等

① 総合管理者は、サーバ室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 職員等及び委託事業者は、サーバ室に入室する場合、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 総合管理者又はサーバ室を所管する情報セキュリティ管理者は、外部からの訪問者がサーバ室に入る場合には、立ち入り区域を制限した上で、必要に応じてサーバ室への入退室を許可された職員等が付き添うものとし、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 総合管理者又はサーバ室を所管する情報セキュリティ管理者は、自治体機密性２以上の情報資産を扱うシステムを設置しているサーバ室について、当該情報システムに関連しない、または個人所有であるコンピュータ、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 総合管理者は、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、あらかじめ情報システム担当者又は委託事業者に確認を行わせなければならない。

② 総合管理者は、サーバ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。

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、適正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正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、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

③ 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。

④ 統括情報セキュリティ責任者は、行政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。

⑤ 統括情報セキュリティ責任者は、自治体機密性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、適正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。

⑥ 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、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

⑦ 統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

⑧ 統括情報セキュリティ責任者は、自治体可用性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。

5.4 職員等の利用する端末や電磁的記録媒体等の管理

① 総合管理者及び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、モバイル端末及び電磁的記録媒体の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。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、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

③ 総合管理者及び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）を行うよう設定しなければならない。

6 人的セキュリティ

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 モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

（ア） CISO は、自治体機密性２以上、自治体可用性２、自治体完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ） 職員等は、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外部に持ち出す場合には、総合管理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。

（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 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア） 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断を統括情報セキュリティ責任者が行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、総合管理者の許可を得て利用することができる。

（イ） 職員等は、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た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑤ 持ち出し及び持ち込みの記録

情報セキュリティ管理者は、ノート型パソコン等の移動型ハードウェア及び USB メモリ等の電磁的記録媒体等の持ち出し及び持ち込みについて、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

職員等は、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、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、適正な措置を講じなければならない。

⑧ 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、当該情報資産の管理者へ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。

⑨ クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

(2) 会計年度任用職員等への対応

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、会計年度任用職員等に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員等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 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、会計年度任用職員等の採用の際、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。

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、会計年度任用職員等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

総合管理者は、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) 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・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち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。

6.2 研修・訓練

(1) 情報セキュリティに関する研修・訓練

① 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 CISO は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

(2) 研修計画の策定及び実施

① CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計

画の策定とその実施体制の構築を定期的に行い、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 新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

③ 研修は、情報セキュリティポリシーで定められた組織体制におけるそれぞれの役割や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。

④ 情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、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に対して、報告しなければならない。

⑤ 統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、CISO に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

⑥ CISO は、毎年度 1 回、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

(3) 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・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

6.3 情報セキュリティインシデントの報告

(1) 庁内で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及び総合管理者に報告しなければならない。

③ 総合管理者は、報告のあった情報セキュリティインシデントについて、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。

④ 情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報の取り扱い状況について監査及び監督を行う情報セキュリティ管理者が個人情報保護委員会へ報告しなければならない。

⑤ 情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象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。

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総合管理者に報告しなければならない。

③ 総合管理者は、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。

④ 統括情報セキュリティ責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

(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。また、CSIRT は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。

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。

6.4 ID 及びパスワード等の管理

(1) IC カード等の取扱い

① 職員等は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。

（ア） 認証に用いるICカード等を、職員等間で共有してはならない。
（イ） 業務上必要のないときは、ICカード等をカードリーダ又はパソコン等の端末のスロット等から抜いておかなければならない。
（ウ） ICカード等を紛失した場合には、速やかに情報セキュリティ責任者及び総合管理者に通報し、指示に従わなければならない。

② 情報セキュリティ責任者及び総合管理者は、ICカード等の紛失等の通報があり次第、当該ICカード等を使用したアクセス等を速やかに停止しなければならない。

③ 情報セキュリティ責任者及び総合管理者は、ICカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

(2) 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。

(3) 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、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（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）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 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

⑥ 仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

⑦ サーバ、ネットワーク機器及びパソコン等の端末に、パスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。

⑧ 職員等間でパスワードを共有してはならない（ただし、共用IDに対するパスワードは除く）。

7 技術的セキュリティ

7.1 コンピュータ及びネットワークの管理

(1) ファイルサーバの設定等

① 総合管理者及び情報システム管理者は、職員等が使用できるファイル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 総合管理者及び情報システム管理者は、ファイルサーバを課等の単位で構成し、職員等が他課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 総合管理者及び情報システム管理者は、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、別途ディレクトリを作成する等の措置を講じ、同一課等であっても、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

① 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、業務システムのデータベースや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かかわらず、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。

② 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。

③ 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

④ 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が本市の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

(3) 他団体との情報システムに関する情報等の交換

総合管理者及び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

① 総合管理者及び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 統括情報セキュリティ責任者、総合管理者及び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、詐取、改ざん等をされないように適正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

③ 統括情報セキュリティ責任者、総合管理者、情報システム管理者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委託事業者がシステム変更等の作業を行う場合は、原則 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。

(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、総合管理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、記録媒体にかかわらず、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、適正に管理しなければならない。

(6) ログの取得等

① 統括情報セキュリティ責任者、総合管理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。

② 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③ 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

④ 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合

は、クラウドサービス事業者に提出を要求するための手続を明確に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、総合管理者及び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又は問題等を、障害記録として記録し、適正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

① 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、ルータ等の通信制御情報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は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

③ 統括情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保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、定期的な確認により見直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

総合管理者及び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

① 総合管理者及び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、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 総合管理者及び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。

③ 総合管理者及び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、総合管理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、次のセキュリティ対策を実施しなければならない。

（ア） 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。

（イ） 脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。

（ウ） ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。

（エ） 情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定しなければならない。

（オ） インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じなければならない。

⑤ 総合管理者及び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

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及び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、適正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正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する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) IoT 機器を含む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講じなければならない。

(13) 無線 LAN のセキュリティ対策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、庁内ネットワークにおいて無線 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、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

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よう、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、スパムメール等が内部から送信されていることを検知した場合は、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。

⑤ 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、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。

(15) 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。

(16) 電子署名・暗号化

① 職員等は、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、統括情報セキュリティ責任者が定めた電子署名、パスワード等による暗号化等のセキュリティを考慮した方法で送信しなければならない。

② 職員等は、暗号化を行う場合に統括情報セキュリティ責任者が定める以外の方法を用いてはならない。また、統括情報セキュリティ責任者が定めた方法で暗号のための鍵を管理しなければならない。

③ 統括情報セキュリティ責任者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供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

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、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、総合管理者又は情報システム管理者が、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。

(18) 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、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) 業務外ネットワークへの接続の禁止

① 職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

② 情報セキュリティ管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

(20) 業務以外の目的でのウェブ閲覧の禁止

① 職員等は、業務以外の目的でウェブを閲覧してはならない。

② 統括情報セキュリティ責任者は、職員等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正な措置を求めなければならない。

(21) Web 会議サービスの利用時の対策

① 統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。

② 職員等は、本市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。

③ 職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講じなければならない。

④ 職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

(22) 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、本市ホームページに当該情報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実施すしなければならない。

（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（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施しなければならない。

② 自治体機密性 2 以上の情報は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。

④ アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

⑤ 自治体可用性 2 の情報の提供にソーシャルメディアサービスを用いる場合は、本市ホームページに当該情報を掲載して参照可能としなければならない。

(23) クラウドサービスの利用制限

職員等は、私的に契約したクラウドサービス（ウェブメール、オンラインストレージ等）を業務目的で使用してはならない。

7.2 アクセス制御

(1) アクセス制御等

① アクセス制御

統括情報セキュリティ責任者、総合管理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等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

② 利用者 ID の取扱い

（ア） 統括情報セキュリティ責任者及び総合管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、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。

（イ） 職員等は、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総合管理者に通知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総合管理者は、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。

（エ） 統括情報セキュリティ責任者及び総合管理者は、職員等に不要なアクセス権限が付与されていないか定期的に確認しなければならない。

③ 特権を付与された ID の管理等

（ア） 統括情報セキュリティ責任者、総合管理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。

（イ） 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための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、総合管理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、総合管理者及び情報システム管理者が指名し、CISO が認めた者でなければならない。

（エ） 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、総合管理者、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。

（オ） 統括情報セキュリティ責任者、総合管理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、委託事業者に行わせてはならない。

（カ） 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、特権を付与された ID 及びパスワードについて、定期的なパスワードの変更、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。

（キ） 統括情報セキュリティ責任者、総合管理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) 職員等による外部からのアクセス等の制限

① 職員等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。

② 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。

③ 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。

④ 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。

⑤ 統括情報セキュリティ責任者及び総合管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、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 職員等は、持ち込んだ又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、統括情報セキュリティ責任者の許可を得た上で接続しなければならない。

⑦ 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インターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、止むを得ず接続を許可する場合は、利用者の ID、パスワード及び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。

(3) ログイン時の表示等

総合管理者又は情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

(4) 認証情報の管理

① 統括情報セキュリティ責任者又は総合管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報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認証情報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。

② 総合管理者又は情報システム管理者は、職員等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、初回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。

③ 総合管理者又は情報システム管理者は、認証情報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。

(5) 特権による接続時間の制限

総合管理者又は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。

7.3 システム開発、導入、保守等

(1) 機器等の調達に係る運用規程の整備

① 統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような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、総合管理者及び情報システム管理者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。

(2) 機器等及び情報システムの調達

① 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、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。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

② 統括情報セキュリティ責任者、総合管理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。

(3) 情報システムの開発

① 情報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、情報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。また、情報システム開発のための規則を確立しなければならない。

② 情報システム開発における責任者、作業者の ID の管理

（ア） 総合管理者及び情報システム管理者は、情報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） 総合管理者及び情報システム管理者は、情報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 情報システム開発に用いるハードウェア及びソフトウェアの管理

（ア） 総合管理者及び情報システム管理者は、情報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、それ以外のものを利用させてはならない。

（イ） 総合管理者及び情報システム管理者は、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させなければならない。

④ アプリケーション・コンテンツの開発時の対策

総合管理者及び情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

(4) 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、情報システム開発・保守及びテスト環境から情報システム運用環境への移行について、情報システム開発・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。

（ウ） 情報システム管理者は、導入する情報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、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。

（エ） 情報システム管理者は、委託事業者と導入部署が、それぞれ独立して受け入れテストを実施するよう適切に管理し調整しなければならない。

（オ） 情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

③ 機器等の納入時又は情報システムの受入れ時

（ア） 情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

（イ） 情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

(5) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

① 情報システム管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じなければならない。

② 利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。

（ア） 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

（イ） 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

(6) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

① 情報システム管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

(7) 情報システム開発・保守に関連する資料等の整備・保管

① 情報システム管理者は、情報システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

（ア） 情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について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） 情報システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備しなければならない。

・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順
・情報セキュリティインシデントを認知した際の対処手順
・情報システムが停止した際の復旧手順

② 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。

③ 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正な方法で保管しなければならない。

(8) 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。

② 情報システム管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

（ア） 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直ししなければならない。

（イ） 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

（ウ） ウェブアプリケーションやウェブコンテンツにおいて、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、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。

(9) 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。

(10) 開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等に対し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。

(11) 情報システム更新又は統合時の検証等

情報システム管理者は、情報システム更新・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。

(12) 情報システムについての対策の見直し

情報システム管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本市内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、統括情報セキュリティ責任者へ報告しなければならない。

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 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。

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。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが

終了する予定がないことを確認しなければならない。

⑧ 仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

(2) 総合管理者及び情報システム管理者の措置事項

総合管理者及び情報システム管理者は、所管する情報システムに係る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 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等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。

⑤ 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

(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な添付ファイルを受信した場合は、速やかに当該ファイルを削除しなければならない。

④ 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。

⑤ 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。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをLGWAN 接続系に取り込む場合は無害化しなければならない。

⑥ 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。

⑦ 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、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてLAN ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

(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。

7.5 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

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 使用されていないポートを閉鎖しなければならない。

② 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。

③ 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者、総合管理者及び情報システム管理者へ通報するよう、設定しなければならない。

④ 統括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と連携し、監視、通知、外部連絡窓口及び適正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。

⑤ 本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

⑥ クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

⑦ パスワード等の認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認しなければならない。

(2) 攻撃への対処

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た場合又は攻撃を受けるリスクがある場合は、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、総務省、山梨県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

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、総合管理者及び情報システム管理者は、職員等及び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) 職員等による不正アクセス

統括情報セキュリティ責任者、総合管理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等の情報セキュリティ管理者に通知し、適正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、総合管理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、総合管理者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策)、内部に侵入した攻撃を早期検知して対処し、侵入範囲の拡大を防止する対策（内部対策)、外部との不正通信を検知して対処する対策（出口対策）を講じなければならない。

7.6 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

① 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、サーバ

装置、端末及び通信回線装置等における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 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有するデータへの影響について特定しなければならない。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認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、職員等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、総合管理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、セキュリティ侵害等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。

8 運用

8.1 情報システムの監視

(1) 情報システムの運用・保守時の対策

① 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

② 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な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、総合管理者及び情報システム管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

(2) 情報システムの監視機能

① 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなけ

ればならない。

② 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

③ 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

④ 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

(3) 情報システムの監視

① 統括情報セキュリティ責任者、総合管理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。

② 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、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。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

③ 統括情報セキュリティ責任者、総合管理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。

④ 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

⑤ 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

⑥ 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

（ア） サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（イ） クラウドサービス利用の終了手順

（ウ） バックアップ及び復旧

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、総合管理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 及び統括情報セキュリティ責任者は、発生した問題について、適正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、総合管理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正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

CISO 又は統括情報セキュリティ責任者が指名した者は、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磁的記録媒体等のログ、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。

(3) 職員等の報告義務

① 職員等は、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、直ちに情報セキュリティ責任者、総合管理者、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。

② 当該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情報セキュリティ責任者、総合管理者、及び情報セキュリティ管理者が判断した場合において、職員等は、統括情報セキュリティ責任者に報告し、緊急時対応計画に従って適正に対処しなければならない。

8.3 侵害時の対応等

(1) 緊急時対応計画の策定

① CISO 又は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及び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正に実施するために、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正に対処しなければならない。

② CISO 又は情報セキュリティ委員会は、クラウドサービス事業者と情報セキュ

リティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した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正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) 業務継続計画との整合性確保

市は自然災害、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、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。

(4) 緊急時対応計画の見直し

CISO 又は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。

8.4 例外措置

(1) 例外措置の許可

総合管理者、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する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、例外措置を講じることができる。

(2) 緊急時の例外措置

総合管理者、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) 例外措置の管理

CISO は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

8.5 法令遵守

(1) 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 26 年法律第 104 号）
⑦ 北杜市個人情報の保護に関する法律施行条例（令和 4 年北杜市条例第 24 号）
⑧ 北杜市文書管理規定（平成 22 年北杜市訓令第 13 号）

(2) 統括情報セキュリティ責任者、総合管理者及び情報システム管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

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、地方公務員法等による懲戒処分の対象とする。

(2) 違反時の対応
職員等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。

① 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等が所属する部局等の情報セキュリティ責任者に通知し、適正な措置を求めなければならない。
② 総合管理者又は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等が所属する課等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
③ 情報セキュリティ責任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、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する部局等の情報セキュリティ責任者に通知しなければならない。

9 業務委託と外部サービス（クラウドサービス、以下「外部サービ

ス等」という。）の利用

9.1 業務委託

(1) 業務委託に係る運用規程の整備

統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備しなければならない。

① 委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

② 委託事業者の選定基準

(2) 業務委託実施前の対策

① 総合管理者、情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

（ア） 委託する業務内容の特定

（イ） 委託事業者の選定条件を含む仕様の策定

（ウ） 仕様に基づく委託事業者の選定

（エ） 情報セキュリティ要件を明記した契約の締結（契約項目）

重要な情報資産を取扱う業務を委託する場合には、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等に係る要件を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

・個人情報漏えい防止のための技術的安全管理措置に関する取り決め

・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定

・提供されるサービスレベルの保証

・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法

・委託事業者の従業員に対する教育の実施

・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止

・業務上知り得た情報の守秘義務

・再委託に関する制限事項の遵守

・委託業務終了時の情報資産の返還、廃棄等

・委託業務の定期報告及び緊急時報告義務

・市による監査、検査

・市による情報セキュリティインシデント発生時の公表

・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（オ） 委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

② 総合管理者、情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

（ア） 仕様に準拠した提案

（イ） 契約の締結

（ウ） 委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結

(3) 業務委託実施期間中の対策

① 総合管理者、情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。

（ア） 委託判断基準に従った重要情報の提供

（イ） 契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

（ウ） 統括情報セキュリティ責任者へ措置内容の報告（重要度に応じて CISO に報告）

（エ） 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

② 総合管理者、情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア） 情報の適正な取扱いのための情報セキュリティ対策

（イ） 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

（ウ） 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

(4) 業務委託終了時の対策

① 総合管理者、情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

（ア） 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

（イ） 委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

② 総合管理者、情報セキュリティ管理者又は情報システム管理者は、業務委託の

終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア） 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

（イ） 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

9.2 情報システムに関する業務委託

(1) 情報システムに関する業務委託における共通的対策

総合管理者又は情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

(2) 情報システムの構築を業務委託する場合の対策

総合管理者又は情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

① 情報システムのセキュリティ要件の適切な実装

② 情報セキュリティの観点に基づく試験の実施

③ 情報システムの開発環境及び開発工程における情報セキュリティ対策

(3) 情報システムの運用・保守を業務委託する場合の対策

① 総合管理者又は情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

② 総合管理者又は情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

(4) 本市向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

① 総合管理者、情報システム管理者又は情報セキュリティ管理者は、外部の一般の者が本市向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

② 総合管理者、情報システム管理者又は情報セキュリティ管理者は、業務委託サ

ービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

③ 総合管理者、情報システム管理者又は情報セキュリティ管理者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

④ 総合管理者、情報システム管理者又は情報セキュリティ管理者は業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請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又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

⑥ 統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

9.3 外部サービス等の利用（自治体機密性２以上の情報を取り扱う場合）

(1) 外部サービス等の選定に係る運用規程の整備

統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、以下を含む外部サービス等の選定に関する規定を整備しなければならない。

① 外部サービス等を利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下 9.3 節において「外部サービス等利用判断基準」という。）

② 外部サービス等提供者の選定基準

③ 外部サービス等の利用申請の許可権限者と利用手続

④ 外部サービス等管理者の指名と外部サービス等の利用状況の管理

(2) 外部サービス等の利用に係る運用規程の整備

統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、以下を含む外部サービス等の利用に関する規定を整備しなければならない。

① 統括情報セキュリティ責任者は、外部サービス等の特性や責任分界点に係る考え方等を踏まえ、外部サービス等を利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

② 統括情報セキュリティ責任者は、外部サービス等の特性や責任分界点に係る考え方を踏まえ、外部サービス等を利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

③ 統括情報セキュリティ責任者は、外部サービス等の特性や責任分界点に係る考え方を踏まえ、以下を全て含む外部サービス等の利用を終了する際のセキュリ

ティ対策の基本方針を運用規程として整備しなければならない。

（ア） 外部サービス等の利用終了時における対策

（イ） 外部サービス等で取り扱った情報の廃棄

（ウ） 外部サービス等の利用のために作成したアカウントの廃棄

(3) 外部サービス等の選定

① 情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス等利用判断基準に従って、業務に係る影響度等を検討した上で外部サービス等の利用を検討しなければならない。

② 情報セキュリティ責任者は、外部サービス等で取り扱う情報の格付及び取扱制限を踏まえ、外部サービス等提供者の選定基準に従って外部サービス等提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス等提供者の選定条件に含めなければならない。

（ア） 外部サービス等の利用を通じて本市が取り扱う情報の外部サービス等提供者における目的外利用の禁止

（イ） 外部サービス等提供者における情報セキュリティ対策の実施内容及び管理体制

（ウ） 外部サービス等の提供に当たり、外部サービス等提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

（エ） 外部サービス等提供者の資本関係・役員等の情報、外部サービス等提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

（オ） 情報セキュリティインシデントへの対処方法

（カ） 情報セキュリティ対策その他の契約の履行状況の確認方法

（キ） 情報セキュリティ対策の履行が不十分な場合の対処方法

③ 情報セキュリティ責任者は、②（ア）～（キ）の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービス等が、本市が定めた外部サービス等の利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価しなければならない。

④ 情報セキュリティ責任者は、外部サービス等の中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス等提供者の選定条件に含めなければならない。

⑤ 情報セキュリティ責任者は、外部サービス等事業者と情報セキュリティに関する役割及び責任の分担について確認しなければならない。

⑥ 情報セキュリティ責任者は、外部サービス等の利用を通じて本市が取り扱う情

報の格付等を勘案し、必要に応じて以下の内容を外部サービス等提供者の選定条件に含めなければならない。

（注）外部サービス等の利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定めなければならない。外部サービス等事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関する外部サービス等事業者の定める条件を鑑み、その規約内容が本市によって受容可能か判断しなければならない。

（ア） 情報セキュリティ監査の受入れ

（イ） サービスレベルの保証

⑦ 情報セキュリティ責任者は、外部サービス等の利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス等提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

⑧ 情報セキュリティ責任者は、外部サービス等提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス等提供者の選定条件で求める内容を外部サービス等提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス等提供者の選定条件に含めなければならない。また、外部サービス等利用判断基準及び外部サービス等提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

⑨ 情報セキュリティ責任者は、外部サービス等の特性を考慮した上で、外部サービス等が提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めなければならない。

（ア） 外部サービス等に求める情報セキュリティ対策

（イ） 外部サービス等で取り扱う情報が保存される国・地域及び廃棄の方法

（ウ） 外部サービス等に求めるサービスレベル

⑩ 統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス等提供者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

(4) 外部サービス等の利用に係る調達・契約

① 情報セキュリティ責任者は、外部サービス等を調達する場合は、外部サービス等提供者の選定基準及び選定条件並びに外部サービス等の選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

② 情報セキュリティ責任者は、外部サービス等を調達する場合は、外部サービス等提供者及び外部サービス等が調達仕様を満たすことを契約までに確認し、統括情報セキュリティ責任者の利用承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。

(5) 外部サービス等の利用承認

① 情報セキュリティ責任者は、外部サービス等を利用する場合には、利用申請の許可権限者へ外部サービス等の利用申請を行わなければならない。

② 利用申請の許可権限者は、職員等による外部サービス等の利用申請を審査し、利用の可否を決定しなければならない。

③ 利用申請の許可権限者は、外部サービス等の利用申請を承認した場合は、承認済み外部サービス等として記録し、外部サービス等管理者を指名しなければならない。

(6) 外部サービス等を利用した情報システムの導入・構築時の対策

① 統括情報セキュリティ責任者は、外部サービス等の特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービス等を利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

（ア） 不正なアクセスを防止するためのアクセス制御

（イ） 取り扱う情報の機密性保護のための暗号化

（ウ） 開発時におけるセキュリティ対策

（エ） 設計・設定時の誤りの防止

（オ） 外部サービス等におけるユーティリティプログラムに対するセキュリティ対策

② 外部サービス等管理者は、情報システムにおいて外部サービス等を利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告しなければならない。

③ 外部サービス等管理者は、外部サービス等の情報セキュリティ対策を実施するために必要となる文書として、外部サービス等の運用開始前までに以下の全ての実施手順を整備しなければならない。

（ア） 外部サービス等で利用するサービスごとの情報セキュリティ水準の維持に関する手順

（イ） 外部サービス等を利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

（ウ） 利用する外部サービス等が停止又は利用できなくなった際の復旧手順

④ 外部サービス等管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。

⑤ 外部サービス等管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、外部サービス等事業者に情報を求め、実施状況を確認及び記録しなければならない。

(7) 外部サービス等を利用した情報システムの運用・保守時の対策

① 統括情報セキュリティ責任者は、外部サービス等の特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービス等を利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

（ア） 外部サービス等利用方針の規定

（イ） 外部サービス等利用に必要な教育

（ウ） 取り扱う資産の管理

（エ） 不正アクセスを防止するためのアクセス制御

（オ） 取り扱う情報の機密性保護のための暗号化

（カ） 外部サービス等内の通信の制御

（キ） 設計・設定時の誤りの防止

（ク） 外部サービス等を利用した情報システムの事業継続

（ケ） 設計・設定変更時の情報や変更履歴の管理

② 外部サービス等管理者は、外部サービス等の運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告しなければならない。

③ 外部サービス等管理者は、外部サービス等の情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

④ 情報セキュリティ責任者は、外部サービス等の特性や責任分界点に係る考え方を踏まえ、外部サービス等で発生したインシデントを認知した際の対処手順を整備しなければならない。

⑤ 外部サービス等管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

⑥ 外部サービス等管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、外部サービス等事業者に情報を求め、実施状況を定期的に確認及び記録しなければならない。

(8) 外部サービス等を利用した情報システムの更改・廃棄時の対策

① 統括情報セキュリティ責任者は、外部サービス等の特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービス等の利用を終了する際のセキュリティ対策を規定しなければならない。

（ア） 外部サービス等の利用終了時における対策
（イ） 外部サービス等で取り扱った情報の廃棄
（ウ） 外部サービス等の利用のために作成したアカウントの廃棄

② 外部サービス等管理者は、前項において定める規定に対し、外部サービス等の利用終了時に実施状況を確認・記録しなければならない。

③ 外部サービス等管理者は、外部サービス等上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除する等により、その情報資産を復元困難な状態としなければならない。

9.4 外部サービス等の利用（自治体機密性２以上の情報を取り扱わない場合）

(1) 外部サービス等の利用に係る規定の整備

統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱わない場合、以下を含む外部サービス等の利用に関する規定を整備しなければならない。

（ア） 外部サービス等を利用可能な業務の範囲
（イ） 外部サービス等の利用申請の許可権限者と利用手続
（ウ） 外部サービス等管理者の指名と外部サービス等の利用状況の管理
（エ） 外部サービス等の利用の運用手順

(2) 外部サービス等の利用における対策の実施

① 職員等は、利用するサービスの約款、その他の提供条件等から、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自治体機密性２以上の情報を取り扱わない場合の外部サービス等の利用を申請しなければならない。また、承認時に指名された外部サービス等管理者は、当該外部サービス等の利用において適切な措置を講じなければならない。

② 情報セキュリティ責任者は、職員等による外部サービス等の利用申請を審査し、利用の可否を決定しなければならない。また、承認した外部サービス等を記録しなければならない。

10 評価・見直し

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、毎年度及び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) 委託事業者に対する監査

① 事業者に業務委託を行っている場合、情報セキュリティ監査責任者は委託事業者（再委託事業者を含む。）に対して、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。

② 外部サービス等を利用している場合は、外部サービス等事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。外部サービス等事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

(5) 報告

情報セキュリティ監査責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告しなければならない。

(6) 保管

情報セキュリティ監査責任者は、監査の実施を通して収集した監査証拠、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正に保管しなければならない。

(7) 監査結果への対応

① 情報セキュリティ委員会は、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（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

② 情報セキュリティ委員会は、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。また、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対

処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

(8) 情報セキュリティポリシー及び関係規程等の見直し等への活用

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定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

10.2 自己点検

(1) 実施方法

① 情報セキュリティ管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

② 情報セキュリティ管理者は、情報セキュリティ責任者と連携して、所管する課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、毎年度及び必要に応じて自己点検を行わなければならない。

(2) 報告

情報セキュリティ管理者は、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、総合管理者に報告しなければならない。また、特に重要な事項は情報セキュリティ委員会へ報告しなければならない。

(3) 自己点検結果の活用

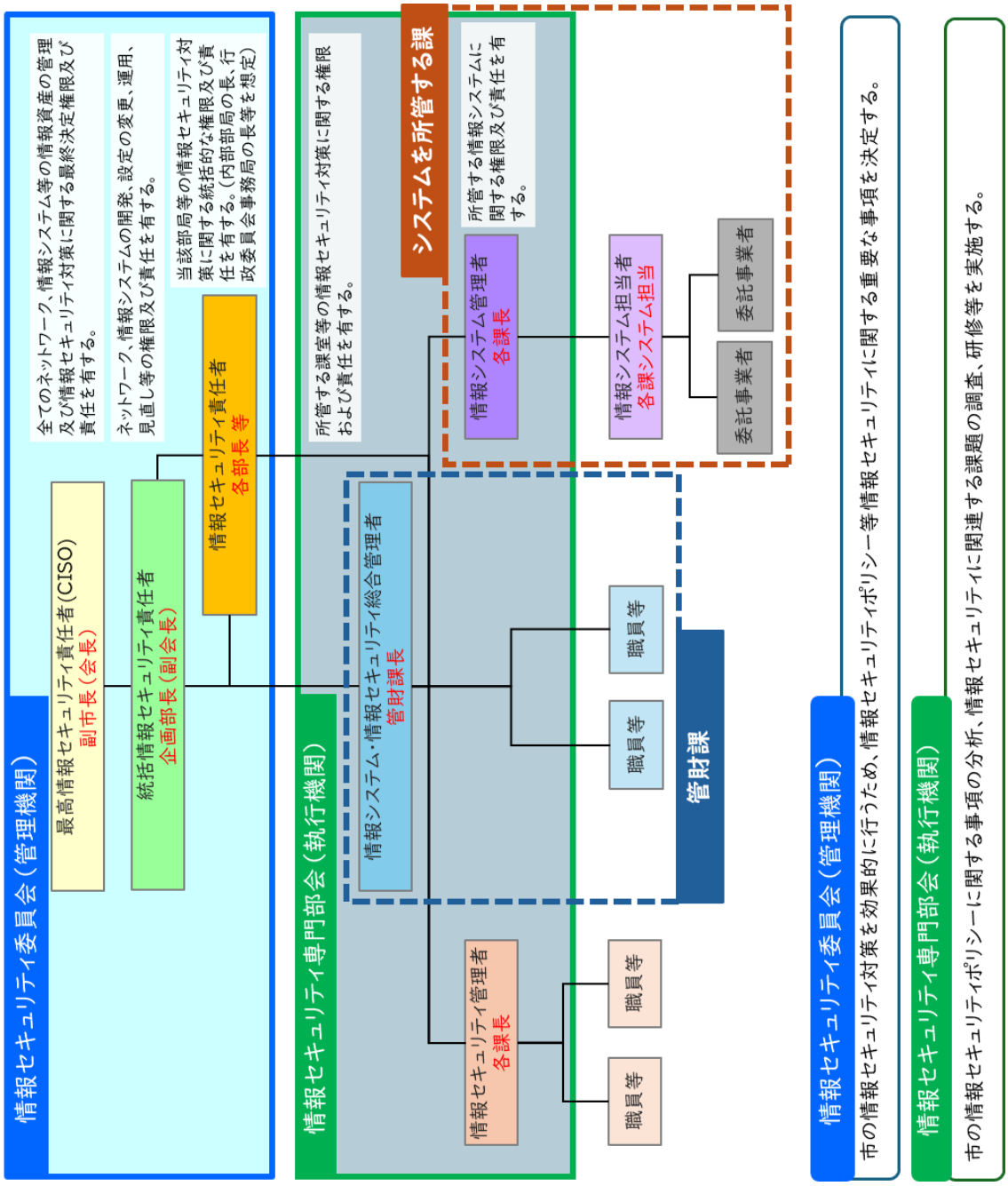
① 職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

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。

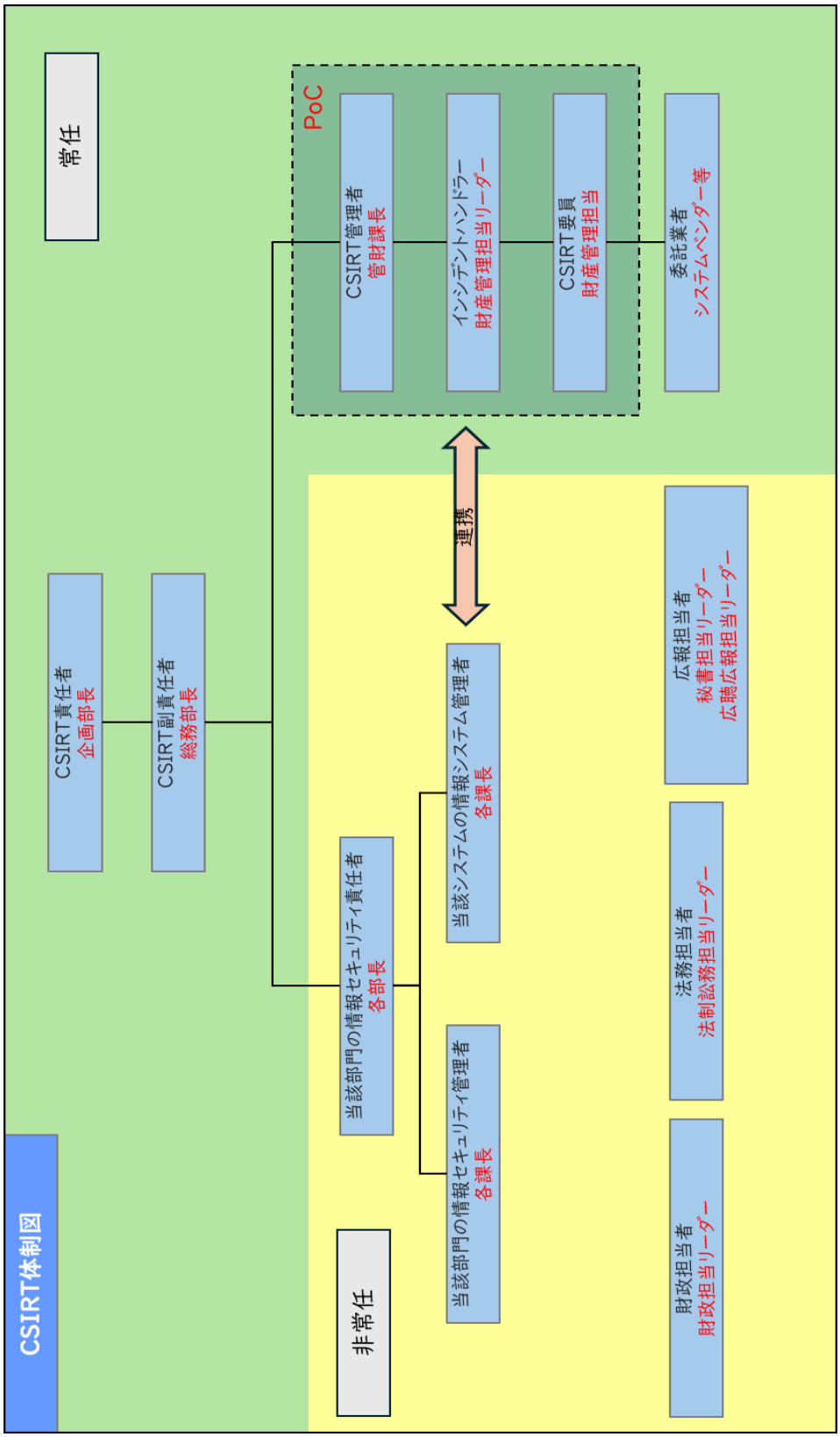
10.3 情報セキュリティポリシー及び関係規程等の見直し

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踏まえ、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リスク評価を行い、必要があると認めた場合、改善を行わなければならない。なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置を実施又は指示し、措置の結果について CISO に報告しなければならない。

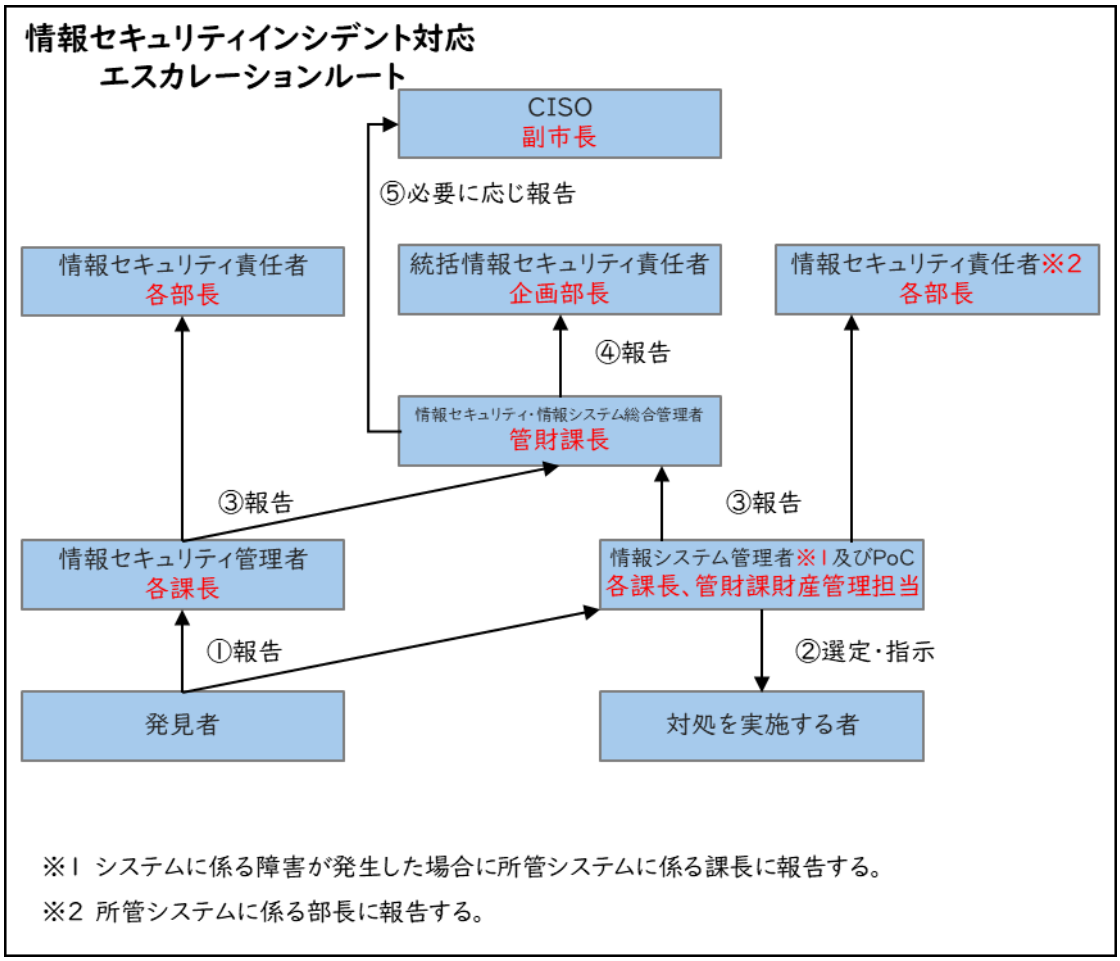
組織体制


情報セキュリティ委員会（管理機関）
最高情報セキュリティ責任者(CISO)
副市長（会長）
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。
統括情報セキュリティ責任者
企画部長（副会長）
ネットワーク、情報システムの開発、設定の変更、運用、見直し等の権限及び責任を有する。
情報セキュリティ責任者
各部長等
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。（内部部局の長、行政委員会事務局の長等を想定）
情報セキュリティ専門部会（執行機関）
所管する課室等の情報セキュリティ対策に関する権限および責任を有する。
情報システム・情報セキュリティ総合管理者
管財課長
管財課
職員等
職員等
情報セキュリティ管理者
各課長
職員等
職員等
システムを所管する課
所管する情報システムに関する権限及び責任を有する。
情報システム管理者
各課長
情報システム担当者
各課システム担当
委託事業者
委託事業者
情報セキュリティ委員会（管理機関）
市の情報セキュリティ対策を効果的に行うため、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。
情報セキュリティ専門部会（執行機関）
市の情報セキュリティポリシーに関する事項の分析、情報セキュリティに関連する課題の調査、研修等を実施する。

CSIRT 体制


CSIRT体制図
常任
非常任
CSIRT責任者
企画部長
CSIRT副責任者
総務部長
PoC
CSIRT管理者
管財課長
インシデントハンドラー
財産管理担当リーダー
CSIRT要員
財産管理担当
委託業者
システムベンダー等
連携
当該部門の情報セキュリティ責任者
各部長
当該部門の情報セキュリティ管理者
各課長
当該システムの情報システム管理者
各課長
広報担当者
秘書担当リーダー
広聴広報担当リーダー
法務担当者
法制訟務担当リーダー
財政担当者
財政担当リーダー

情報セキュリティインシデント対応の処理フロー



（別表 1）

機密性による情報資産の分類

分類	分類基準	取扱制限
自治体機密性３A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	・支給された端末以外での作業の原則禁止（自治体機密性３の情報資産に対して） ・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電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・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 ・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
自治体機密性３B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体機密性３C	行政事務で取り扱う情報資産のうち、自治体機密性３B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３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	
自治体機密性１	自治体機密性２又は自治体機密性３の情報資産以外の情報資産	―

完全性による情報資産の分類

分類	分類基準	取扱制限
自治体完全性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	・バックアップ、電子署名付与 ・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
自治体完全性１	自治体完全性２の情報資産以外の情報資産	―

可用性による情報資産の分類

分類	分類基準	取扱制限
自治体可用性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	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
自治体可用性１	自治体可用性２の情報資産以外の情報資産	―

（別表 2）

認証手段には「知識」「所持」「存在」の種類が存在する。認証の種類と手段及び情報システムが正規の利用者かどうかを判断する手段を以下に示す。

認証の種類と手段

種類	認証の手段
知識	正規の利用者“だけが知っている情報（知識）”をその人が知っているか否かで判断する
所持	正規の利用者“だけが持っているモノ（所持品）”をその人が持っているか否かで判断する
存在	正規の利用者の“身に備わっている特徴（利用者自身の存在）”でその人か否かを判断する

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

認証手段の概要と具体例		利点	欠点
「知識」を利用する手段	・パスワード ・パスフレーズ ・暗証番号 ・ピクチャーパスワード	・運用コストが安い ・特別な装置が不要で、非常に簡便	・複雑すぎる「知識」は記憶できない ・簡単な「知識」さえあれば、正規の利用者でなくても、「知識」を推定して正規の利用者になりすますことができる ・「知識」忘失のおそれがある
「知識」と「所持」を併用	・IC カードと暗証番号の併用 ・ワンタイムパスワードトークンとパスワード（暗証番号）の併用 ・SIM カード（携帯電話／スマートフォンの固有番号）と	・知識」と「所持」を併用することで、「知識」だけ、あるいは「所持」だけに頼るよりも安全性が高い	・カードやトークン等が必要で運用コストが高い ・カードやトークン等の盗難・紛失のおそれがある ・「知識」忘失のおそれがある

認証手段の概要と具体例		利点	欠点
	パスワードの併用		
「所持」を利用する手段	・IC カード ・USB トークン ・SIM カード（携帯電話／スマートフォンの固有番号）	・「知識」に頼らず、安全性を向上できる	・カードやトークン等が必要で運用コストが高い ・カードやトークン等の盗難・紛失のおそれがある ・正規の利用者でなくても、何らかの手段（例えば盗難や偽造）でカードやトークン等を「所持」することができれば、情報システムは正規の利用者と誤認する
「存在」を利用する手段	・バイオメトリックス認証（指紋、声紋、静脈等）	・「知識」や「所持」に頼らず、安全性を向上できる ・偽造がかなり困難 ・盗難・紛失のおそれがない	・特別な装置が必要で、運用コストが高い ・システム・装置によって認証精度に大きなばらつきがある ・認証データは本人固有の生体情報を基にして作られるため、万が一、認証データの漏えいや偽造が発生しても、認証データ自体を変えることができない
	・リスクベース認証（行動パターン、キーボードを使う時の癖など）	・行動パターンや癖などをまねるのは難しい ・完全に一致する行動パターンや癖が現れるのもかえって不自然と判断可能 ・盗難・紛失のおそれがない	・完全な利用者認証にはならない。“リスクベース”とは、行動パターンやキーボードを使う時の癖がいつもと違うことを検出した時に、“他人が利用しているかもしれない＝リスクの検知”と判断して、別の利用者認証を要求する、という意味 ・状態監視が常時必要なので、運用コストが比較的高い

用語集（出典：IT 用語辞典 e-Words）

インシデント	情報管理やシステム運用に関して保安上の脅威となる人為的な事象を「セキュリティインシデント」(security incident) と呼び、これを略して単にインシデントと呼ぶことが多い。 組織が運用するコンピュータシステムや管理下にある情報の機密性、完全性、可用性を脅かす（危険性のある）何らかの人為的な事象を指し、マルウェア感染や不正アクセス、パスワード漏洩、Web サイト改竄、機密情報流出、フィッシング、サービス拒否攻撃（DoS 攻撃）などが含まれる。
不正プログラム	コンピュータの正常な動作を妨げたり、利用者やコンピュータに害を成す不正な動作を行うソフトウェアの総称。
コンピュータウイルス	コンピュータの正常な利用を妨げる有害なコンピュータプログラムの一種で、他のプログラムの一部として自らを複製し、そのプログラムが起動されると便乗して悪質な処理を実行に移すもの。
ゲートウェイ	ネットワーク機器の一種で、伝送方式やプロトコル(通信規約)などが異なるネットワーク間の中継を行うもの。特に、最上位層のプロトコルやデータ形式の違いに対応できるものを指すことが多い。
パターンファイル	既知のコンピュータウイルスに特有・固有のデータ断片を登録したデータファイル。アンチウイルスソフト(ウイルス対策ソフト)がコンピュータに保存されたファイルなどからウイルスを検出するのに使用する。
パッチ	導入済みのプログラムやデータを最新版に改めるために開発元から提供される、旧版との差分データを指す。ファイルの形にまとめたものは「パッチファイル」という。
バージョンアップ	ソフトウェアが機能を向上したり不具合を修正したりして、新しい版となって再発売・再公開されること。また、利用者が手元のソフトウェアを新しい版に入れ替えて更新すること。 和製英語であり、英語では“update”（アップデート）あるいは“upgrade”（アップグレード）という。
不正アクセス	情報システムやデータへのアクセス権限を持たない者が、コンピュータを操作して本来認められていない活動を行うこと。重要な情報の窃取、公開情報の改竄や消去、不正な遠隔操作、外部システムへの攻撃(踏み台利用)などが含まれる。

サービス不能攻撃	通信ネットワークを通じてコンピュータや通信機器などに行われる攻撃手法の一つで、大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込むこと。
標的型攻撃	特定の個人や組織、情報を狙ったサイバー攻撃のこと。企業や国家の機密情報を盗み取る目的で行われることが多い。
セキュリティホール	コンピュータシステムに生じた保安上の弱点や欠陥。悪意ある人物やプログラムがシステムを不正に操作したり、データを不正に取得・変更することができるようになってしまう不具合のこと。
クラウドサービス	従来は手元のコンピュータに導入して利用していたようなソフトウェアやデータ、あるいはそれらを提供するための技術基盤(サーバなど)を、インターネットなどのネットワークを通じて必要に応じて利用者に提供するサービス。 機材やソフトウェア、処理性能、記憶領域、ファイル、データなど何らかの計算資源をインターネットなどの通信ネットワークを通じて提供し、利用者がいつでもどこからでも必要なときに必要なだけ資源にアクセスできるようなサービスの総称として用いられる。
約款	約款（やっかん）とは、たくさんの取引を画一的に処理するために、あらかじめ定型化された契約条項のこと。インターネットを利用したサービスを利用する際に、細かな契約内容が表示されて「同意する」にチェックを入れるようになっていることがあるが、そのようなものも約款になりえる。
ソーシャルメディア（SNS）	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、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。狭義にはいわゆる「SNS」(ソーシャルネットワーキングサービス)を指す。
アカウント	コンピュータやネットワークなどの利用者ごとに発行される利用権や属性値の集合などのことを指す。
CSIRT（シーサート）	CSIRT（Computer Security Incident Response Team）とは、企業や行政機関などに設置される組織の一種で、コンピュータシステムやネットワークに保安上の問題に繋がる事象が発生した際に対応する組織。

PoC（ポック） （Point of Contact）	情報セキュリティインシデントについて庁内外の者から連絡受付の役割を担う情報セキュリティに関する統一的な窓口のこと。