富山市情報セキュリティポリシー

平成17年4月1日　制定

平成18年10月12日　改定
平成19年　6月15日　改定
平成27年　3月　3日　改定
平成27年10月　5日　改定
平成29年　4月　1日　改定
平成30年　9月　1日　改定
平成31年　4月　1日　改定
令和　2年　4月　1日　改定
令和　3年　4月　1日　改定
令和　4年　4月　1日　改定
令和　7年　4月　1日　改定
令和　7年　9月　1日　改定
令和　8年　4月　1日　改定

《目 次》

はじめに

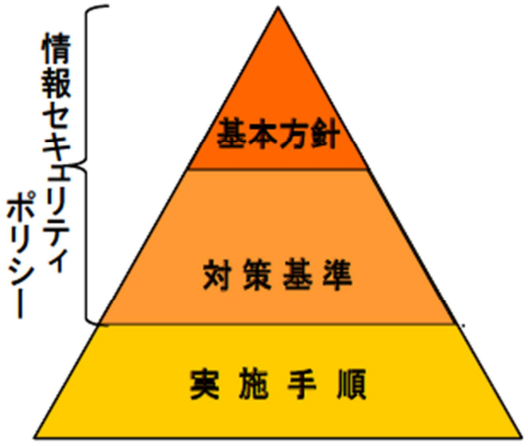
情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書であり、本市の情報セキュリティ対策の頂点に位置するものである。

市長以下、全ての職員等は、業務の遂行に当たって、本情報セキュリティポリシーを遵守する義務を負う。

情報セキュリティポリシーの体系は、以下の図表に示す階層構造となっている。

情報セキュリティ対策における基本的な考え方を定めたものが、「基本方針」であり、この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めたものが「対策基準」である。

この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」といい、「対策基準」を、具体的なシステムや手順、手続に展開して個別の実施事項を定めたものが「実施手順」である。



情報セキュリティポリシー体系図

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に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とともに、地方自治法（昭和22年法律第67号）第244条の6第1項に規定するサイバーセキュリティを確保するための方針として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

本基本方針及び各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）情報セキュリティインシデント

情報セキュリティに関する障害・事故及びシステム上の欠陥をいう。

（9）情報資産

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（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

（10）情報端末

情報にアクセスするためのパソコン、モバイル端末（タブレット、スマートフォン、ハンディ等）その他の機器及び機械をいう。

（11）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。

（12）LGWAN接続系

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。）。

（13）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。

（14）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。

（15）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. 適用範囲

情報セキュリティポリシーは、本市が保有する全ての情報資産及びこれらを利用する者に適用する。

4. 適用対象者の責務

職員等（会計年度任用職員及び派遣労働者を含む。）及び委託事業者（指定管理者を含む。）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。

5. 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・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、火災、水害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、通信の途絶等のインフラの障害からの波及等

6. 情報セキュリティ対策

上記に掲げた脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（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行う。

（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、都道府県及び市区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、管理区域、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、委託業務（指定管理を含む。）を行う際のセキュリティ確保等、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ポリシーを定め、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。

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、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。

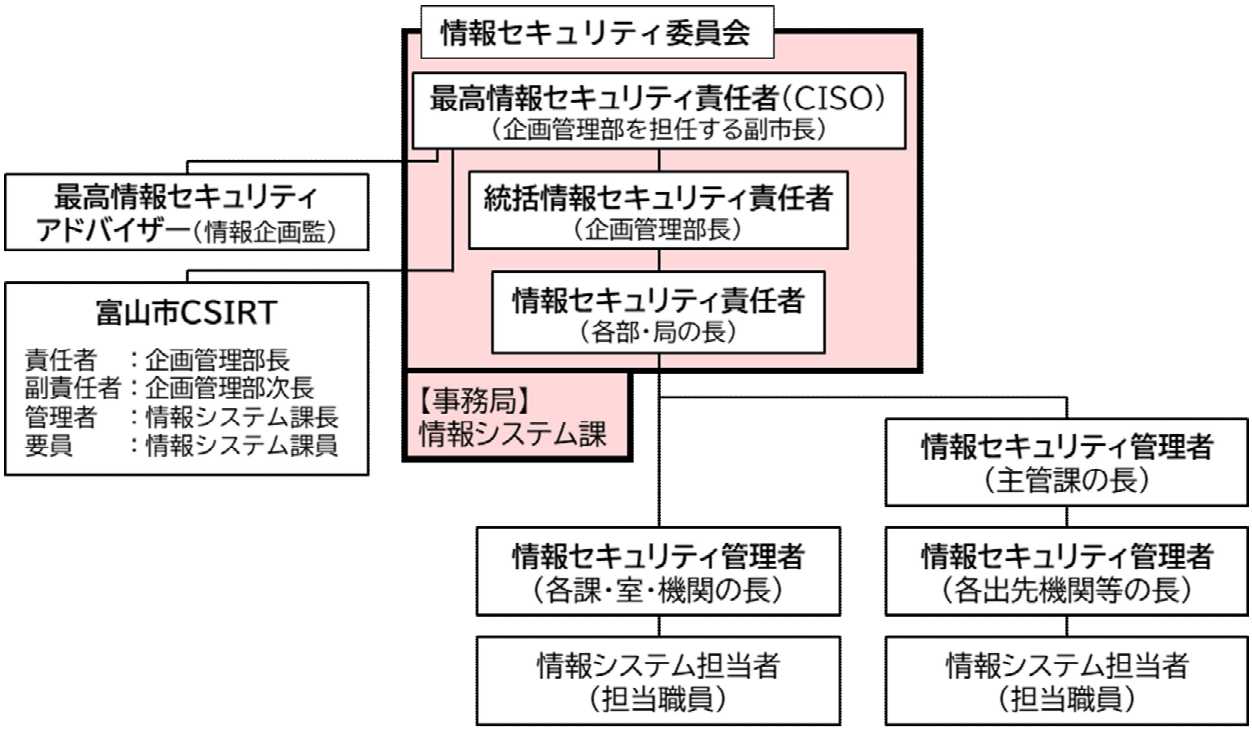
情報セキュリティ共通対策基準

1. 目的

本共通対策基準は、富山市情報セキュリティ基本方針に規定する対策等を実施するための、具体的な遵守事項及び判断基準等を定めたものである。

2. 情報セキュリティ管理体制

情報セキュリティ対策を実施するための管理体制は、以下のとおりとする。



（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 企画管理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ものとする。最高情報セキュリティアドバイザーは情報企画監をもって充てる。

（2）統括情報セキュリティ責任者

① 企画管理部長を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を補佐する。

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及び情報システムの開発、設定変更、運用、見直し等を行う統括的な権限及び責任を有する。

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、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統括的な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、情報セキュリティ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、情報セキュリティ管理者、情報システム担当者を網羅する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、復旧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、自身の権限に属する事務を情報システム課長に処理（専決を含む。）させることができる。

（3）情報セキュリティ責任者

① 各行政組織の部局等（以下「部局等」という。）の情報セキュリティ責任者は、次のとおりとする。

部局等	情報セキュリティ責任者
企画管理部 公平委員会	企画管理部長
財務部 固定資産評価審査委員会	財務部長
防災危機管理部	防災危機管理部長
福祉保健部	福祉保健部長
こども家庭部	こども家庭部長
市民生活部	市民生活部長
環境部	環境部長
商工労働部	商工労働部長
農林水産部	農林水産部長
活力都市創造部	活力都市創造部長
建設部	建設部長
出納局	会計管理者

部局等	情報セキュリティ責任者
上下水道局	上下水道局長
病院事業局	病院事業局管理部長
選挙管理委員会	選挙管理委員会事務局長
監査委員	監査委員事務局長
教育委員会	教育委員会事務局長
農業委員会	農業委員会事務局長
消防局	消防局長
議会事務局	議会事務局長

② 情報セキュリティ責任者は、当該部局等のネットワーク、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、当該部局等において所有しているネットワーク及び情報システムの開発、設定変更、運用、見直し等を行う権限及び責任を有する。

（4）情報セキュリティ管理者

① 各部局等の課室等の所属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ネットワーク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、富山市CSIRTへ速やかに報告を行い、指示を仰がなければならない。併せて情報セキュリティ責任者へ報告しなければならない。

④ 情報セキュリティ管理者は、所管する情報システムの開発、設定変更、運用、見直し等を行う権限及び責任を有する。

⑤ 情報セキュリティ管理者は、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。

⑥ 情報セキュリティ管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

⑦ 情報セキュリティ管理者は、ガバメントクラウド並びにガバメントクラウドと同等の情報セキュリティ対策が実施されているクラウドサービス（以下「ガバメントクラウド等」という。）上で標準準拠システム（標準化基準（地方公共団体情報システムの標準化に関する法律（令和3年法律第40号）第6条第1項及び第7条第1項に規定する標準化基準をいう。）に適合する基幹業務システムをいう。以下同じ。）・関連システム等の業務システム（以下「標準準拠システム等」という。）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。

（5）情報システム担当者

情報セキュリティ管理者の指示等に従い、情報システムの開発、設定変更、運用、更新等の作業を行う者を、情報システム担当者とする。

（6）富山市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、情報セキュリティポリシー等、情報セキュリティに関する重要な事項は、富山市情報セキュリティ委員会において、審議する。

② 富山市情報セキュリティ委員会はCISO、統括情報セキュリティ責任者並びに情報セキュリティ責任者で構成する。

③ 本基準に定めるもののほか、富山市情報セキュリティ委員会の設置、運営に関し必要な事項は、「富山市情報セキュリティ委員会運営要綱」において定める。

（7）富山市CSIRT

① CISOは、富山市CSIRT（情報セキュリティインシデントに対処するための体制。以下「CSIRT」という。）を整備し、情報セキュリティインシデントが発生した場合に、速やかにその状況を確認し、自らへの報告が行われる体制を整備する。

② CSIRTは、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。

③ 本基準に定めるもののほか、CSIRTの設置、運営に関し必要な事項は、「富山市CSIRT運営要綱」において定める。

3. 情報資産の分類と管理

（1）適用範囲

この共通対策基準を適用する情報資産の範囲は、小学校、中学校及び義務教育学校の教育に関するものを除いた、本市が保有する全ての情報資産とする。

（2）情報資産の分類

本共通対策基準が対象とする情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。また、機密性2以上、完全性2又は可用性2のいずれかに該当する情報資産を重要情報とする。

機密性による情報資産の分類

分類	分類基準	
機密性3	3A	情報資産のうち、秘密文書に相当する機密性を要する情報資産
	3B	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
	3C	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情報資産
機密性2	情報資産のうち、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	
機密性1	機密性2又は機密性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
完全性2	情報資産のうち、改ざん、誤謬又は破損により、市民の権利が侵害される又は業務の適確な遂行に支障（軽微なものを除く。）を及ぼす恐れがある情報資産
完全性1	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
可用性2	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、市民の権利が侵害される又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼす恐れがある情報資産
可用性1	可用性2の情報資産以外の情報資産

（3）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） 情報セキュリティ管理者は、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、情報システム台帳に記載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（2）の分類に基づき管理しなければならない。

（エ） 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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（2）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）の取扱いを定める。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クラウドサービスからの削除等のサービス終了に関する対応について、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、その分類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

情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④ 情報資産の入手

（ア） 庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ） 庁外の者が作成した情報資産を入手した者は、（2）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ） 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

⑤ 情報資産の利用

（ア） 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

（イ） 情報資産を利用する者は、情報資産の分類に応じ、適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者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥ 情報資産の保管

（ア） 情報セキュリティ管理者は、情報資産の分類に従って、情報資産を第三者が閲覧、持ち出しできないように保管する等、適正に保管しなければならない。

（イ） 情報セキュリティ管理者は、情報を記録した電磁的記録媒体を長期保管する場合は、書込禁止等の措置を講じなければならない。

（ウ） 情報セキュリティ管理者は、機密性2以上、完全性2又は可用性2の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦ 情報の送信

（ア） 電子メール等により機密性2以上の情報を送信する者は、原則、暗号化又はパスワード設定を行わなければならない。

（イ） 機密性2以上の情報を送信する者は、情報セキュリティ管理者に許可を得なければならない。

⑧ 情報資産の運搬

（ア） 車両等により機密性2以上の情報資産を運搬する者は、原則、鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

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

⑨ 情報資産の提供・公表

（ア） 機密性2以上の情報資産を外部に提供する者は、原則、暗号化又はパスワードの設定を行わなければならない。

（イ） 機密性2以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

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

⑩ 電磁的記録媒体の廃棄

（ア） 情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体が不要になった場合、記録されている情報の機密性に応じ、電磁的記録媒体の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） （ア）の電磁的記録媒体の廃棄を行う者は、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） （ア）の電磁的記録媒体の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

（エ） 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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. 物理的セキュリティ

4-1 サーバ等の管理

（1）機器の取付け

情報セキュリティ管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

（2）システムの冗長化

情報セキュリティ管理者は、重要情報を格納しているサーバ、セキュリティサーバ、市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、システムの運用

停止時間を最小限にしなければならない。

（3）機器の電源

① 情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適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 情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（4）通信ケーブル等の配線

① 情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

② 情報セキュリティ管理者は、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 情報セキュリティ管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

④ 情報セキュリティ管理者は、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 情報セキュリティ管理者は、可用性2のサーバ等機器については、定期保守を実施するなど可用性を維持するよう努めなければならない。

② 情報セキュリティ管理者は、情報端末及び電磁的記録媒体を外部の事業者に修理させる場合、守秘義務契約を締結する等、秘密保持の対策を講じなければならない。

（6）庁外への情報資産の設置

情報セキュリティ管理者は、庁外にサーバ等の情報資産を設置する場合、統括情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器の情報セキュリティ対策状況について確認しなければならない。

（7）機器の廃棄等

① 情報セキュリティ管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利

用する際には、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）について、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。当該確認に当たっては、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することができる。

4-2 管理区域の管理

（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、当該機器等の管理及び運用を行うための部屋をいう。

② 情報セキュリティ管理者は、施設管理者と連携して、管理区域外に通ずるドアは必要最小限とし、鍵、監視装置等によって、許可されていない者の立入りを防止しなければならない。

③ 情報セキュリティ管理者は、管理区域内の機器等に、転倒及び落下防止等の耐震・免震対策、防火措置、防水措置等を講じなければならない。

④ 情報セキュリティ管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器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）管理区域の入退室管理等

① 情報セキュリティ管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証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、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 情報セキュリティ管理者は、機密性2以上の情報を取り扱う情報システムを設置している管理区域について、当該情報システムに関連しない情報端末、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 情報セキュリティ管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託事業者に確認を行わせなければならない。

② 情報セキュリティ管理者は、管理区域への機器等の搬入出の際に、職員等を立ち会わせなければならない。

4-3 通信回線及び通信回線装置の管理

① 情報セキュリティ管理者は、所管する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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。
④ 情報セキュリティ管理者は、本市が管理するネットワークを集約するように努めなければならない。
⑤ 情報セキュリティ管理者は、機密性2以上の情報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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、可用性2の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

4-4 職員等のパソコン等の管理

① 情報セキュリティ管理者は、盗難防止のため、機密性2以上の情報が保存されたパソコンが設置された執務室等における職員等退出後の施錠管理、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 情報セキュリティ管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。
③ 情報セキュリティ管理者は、取り扱う情報が機密性3の場合、「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。

5. 人的セキュリティ

5-1 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 情報資産の持ち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、機密性2以上、可用性2、完全性2の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ） 職員等は、情報資産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 貸与以外の情報端末及び電磁的記録媒体等の業務利用

（ア） 職員等は、貸与以外の情報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、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、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。なお、機密性3の情報については、私物パソコン等による情報処理を行ってはならない。

（イ） 職員等は、貸与以外の情報端末及び電磁的記録媒体等を用いる場合には、外部で情報処理作業を行う際の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 情報端末におけるセキュリティ設定変更の禁止

職員等は、情報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。

⑥ 机上の端末等の管理

職員等は、情報端末、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、離席時の情報端末のロックや、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。

⑦ 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。

⑧ クラウドサービス利用時等の遵守事項

職員等は、ガバメントクラウド等上で標準準拠システム等を利用する際には、クラウドサービスの利用に当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誓約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、会計年度任用職員に情報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等

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・保守等を委託事業者に発注する場合、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。

5-2 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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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わなければならない。

② 研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム担当者、新規採用職員、その他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものを実施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。

5-3 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に報告しなければならない。

③ CSIRT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及び情報セキュリティ責任者に報告しなければならない。

④ CSIRTは、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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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CSIRTに報告しなければならない。

③ CSIRT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及び情報セキュリティ責任者に報告しなければならない。

④ CISOは、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るための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

⑤ 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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の原因究明・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について状況を確認し、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について、評価に基づきCISO、総務省、県等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管理者に対し、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、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セキュリティ管理者へ確認を求めなければならない。

④ CSIRTは、情報セキュリティインシデントを引き起こした部門の情報セキュリティ管理者と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、必要に応じて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。

（4）情報セキュリティインシデントの公表

情報セキュリティインシデントの公表については、別に定める。

5-4 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 情報セキュリティ管理者は、ICカード等の紛失等通報があり次第、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、必要に応じてデータの消去や破砕するなど適正に処理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 パスワードを変更する場合は、古いパスワードを再利用してはならない。

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

⑦ 仮のパスワードは、最初のログイン時点で変更しなければならない。

⑧ 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てはならない。

⑨ 職員等間でパスワードを共有してはならない（ただし、共有IDに対するパスワードは除く）。

6. 技術的セキュリティ

6-1 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

情報セキュリティ管理者は、市民の個人情報、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 情報セキュリティ管理者は、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関わらず、必要に応じて定期的にバックアップを実施しなければならない。

② 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利

用する際には、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）システム管理記録及び作業の確認

① 情報セキュリティ管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

② 情報セキュリティ管理者は、所管するシステムにおいて、システム改修、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。

（4）情報システム仕様書等の管理

情報セキュリティ管理者は、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすること等がないよう、適正に管理しなければならない。

（5）ログの取得等

① 統括情報セキュリティ責任者及び情報セキュリティ管理者は、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及び情報セキュリティ管理者は、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及び情報セキュリティ管理者は、取得したログを定期的に点検し、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分析を実施しなければならない。なお、ガバメントクラウド等上で標準準拠システム等を利用する際には、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及び情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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

するための手続を確認しなければならない。

（6）障害記録

情報セキュリティ管理者は、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。

（7）ネットワークの接続制御、経路制御等

① 情報セキュリティ管理者は、所管するネットワークの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 情報セキュリティ管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

③ 情報セキュリティ管理者は、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。

（8）外部の者が利用できるシステムの分離等

情報セキュリティ管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと分離する等の措置を講じなければならない。

（9）外部ネットワークとの接続制限等

① 情報セキュリティ管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、統括情報セキュリティ責任者の許可を得なければならない。

② 情報セキュリティ管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、関連する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 情報セキュリティ管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④ 情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。

（ア） 内部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） 情報セキュリティ管理者は、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。

⑤ 情報セキュリティ管理者は、所管するネットワークを外部ネットワークと接続した場合に、必要に応じて、当該外部ネットワークの管理責任者から、通信に係るログを提供させなければならない。

⑥ 情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（10）複合機のセキュリティ管理

① 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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。

（11）IoT機器を含む特定用途機器のセキュリティ管理

情報セキュリティ管理者は、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。

（12）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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、機密性の高い情報を取り扱うネットワークを通信回線と接続する場合は、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。

（13）電子メールのセキュリティ管理

① 情報セキュリティ管理者は、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 情報セキュリティ管理者は、大量のスパムメール等の受信又は送信を検知した場合は、必要に応じてメールサーバの運用を停止しなければならない。

③ 情報セキュリティ管理者は、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。

（14）電子メール等の利用制限

① 職員等は、自動転送機能を用いて、私物の情報端末及び外部に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、直ちに情報セキュリティ管理者に報告しなければならない。

（15）電子署名・暗号化

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、電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

（16）無許可ソフトウェアの導入等の禁止

① 職員等は、情報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セキュリティ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、導入する場合は、情報セキュリティ管理者は、ソフトウェアのライセンス台帳等を作成し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。

④ ソフトウェアの利用及び管理方法等に係る規定については、別に定める。

（17）機器構成の変更の制限

① 職員等は、情報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、情報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、情報セキュリティ管理者の許可を得なければならない。

（18）業務外ネットワークへの接続の禁止

① 職員等は、貸与された端末を、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セキュリティ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、貸与した端末について、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。

（19）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及び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。

（20）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すること。

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ずること。

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わなければならない。

（21）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、統括情報セキュリティ責任者の許可を得た上で、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ポリシーを定めなければならない。

（ア） 本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイト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ること。

（イ） パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ICカード等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること

② 情報セキュリティ管理者は、機密性2以上の情報をソーシャルメディアサービスで発信してはならない。

③ 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 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、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

6-2 アクセス制御

（1）アクセス制御

① アクセス制御等

情報セキュリティ管理者は、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） 情報セキュリティ管理者は、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、情報セキュリティ管理者に通知しなければならない。

（ウ） 情報セキュリティ管理者は、利用されていないIDが放置されないよう、点検しなければならない。

（エ） 情報セキュリティ管理者は、主体から対象に対する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） 情報セキュリティ管理者は、所管するネットワーク及びシステムについて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） 情報セキュリティ管理者は、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） 情報セキュリティ管理者は、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。

（エ） 情報セキュリティ管理者は、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の許可を得なければならない。

② 情報セキュリティ管理者は、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 情報セキュリティ管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④ 情報セキュリティ管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。
⑤ 情報セキュリティ管理者は、外部からのアクセスに利用する情報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本市が管理するネットワークに接続する際に、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、情報セキュリティ管理者の許可を得なければならない。

（3）認証情報の管理

① 情報セキュリティ管理者は、職員等の認証情報を厳重に管理しなければならない。
② 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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。

（4）特権ユーザIDによる接続時間の制限

情報セキュリティ管理者は、特権ユーザID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するよう努めなければならない。

6-3 システム開発、導入、保守等

（1）情報システムの調達

① 情報セキュリティ管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。
② 情報セキュリティ管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（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

情報セキュリティ管理者は、システム開発の責任者及び作業者を特定しなければならない。

② システム開発における責任者、作業者のIDの管理

（ア） 情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発用IDを削除しなければならない。

（イ） 情報セキュリティ管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

③ システム開発に用いるハードウェア及びソフトウェアの管理

（ア） 情報セキュリティ管理者は、システム開発の責任者及び作業者が使用する

ハードウェア及びソフトウェアを特定しなければならない。

（イ） 情報セキュリティ管理者は、利用を認めたソフトウェア以外のソフトウェアを使用させてはならない。

（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） 情報セキュリティ管理者は、原則、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

（イ） 情報セキュリティ管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（ウ） 情報セキュリティ管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（エ） 情報セキュリティ管理者は、導入するシステムやサービスの機密性、完全性並びに可用性が確保されていることを確認した上で導入しなければならない。

② テスト

（ア） 情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（イ） 情報セキュリティ管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

（ウ） 情報セキュリティ管理者は、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。

（4）システム開発・保守に関連する資料等の整備・保管

① 情報セキュリティ管理者は、システム開発・保守に関連する資料及び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。

② 情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

（5）情報システムにおける入出力データの正確性の確保

① 情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能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 情報セキュリティ管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（6）情報システムの変更・改修管理

情報セキュリティ管理者は、情報システムを変更又は改修した場合、仕様書等の変更・改修履歴を作成しなければならない。

（7）開発・保守用のソフトウェアの更新等

情報セキュリティ管理者は、開発・保守用のソフトウェア等を更新、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。

（8）システム更新又は統合時の検証等

情報セキュリティ管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

6-4 不正プログラム対策

（1）情報セキュリティ管理者の措置事項

情報セキュリティ管理者は、不正プログラム対策として、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（OSを含む。）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 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、本市が管理している媒体以外を職員等に原則、利用させてはならない。

⑨ ガバメントクラウド等上で標準準拠システム等を利用する際には、仮想マシンを設定する際に不正プログラムへの対策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。

⑩ インターネットに接続していないシステム及び端末において、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。

（2）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 情報端末において、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、速やかに削除しなければならない。なお、職員等で判断がつかない場合は情報セキュリティ管理者へ連絡し、指示に従うこと。

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。

⑥ 統括情報セキュリティ責任者及び情報セキュリティ管理者が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、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等を実施した後、直ちに情報セキュリティ管理者並びにCSIRTに報告するとともに、CSIRTの指示に従わなければならない。

（3）専門家の支援体制

統括情報セキュリティ責任者及び情報セキュリティ管理者は、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、専門家の支援を受けられるようにしておかなければならない。

6-5 不正アクセス対策

（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の措置事項

情報セキュリティ責任者及び情報セキュリティ管理者は、不正アクセス対策として、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は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の対策を講じなければならない。

④ CSIRT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 ガバメントクラウド等上で標準準拠システム等を利用する際には、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 ガバメントクラウド等上で標準準拠システム等を利用する際には、委託事業者等に管理権限を与える場合、多要素認証等の確実な認証方式を用いて認証させ、クラウドサービスにアクセスさせなければならない。

⑦ ガバメントクラウド等上で標準準拠システム等を利用する際には、パスワードなど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、本市の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、CSIRTと連携し、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、県等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、CSIRTと連携し、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（4）内部からの攻撃

統括情報セキュリティ責任者及び情報セキュリティ管理者は、CSIRTと連携し、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及び情報セキュリティ責任者は、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所属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

情報セキュリティ管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（7）標的型攻撃

情報セキュリティ管理者は、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）や、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

6-6 セキュリティ情報の収集

（1）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

① 統括情報セキュリティ責任者及び情報セキュリティ管理者は、セキュリティ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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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する。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及び情報セキュリティ管理者は、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及び情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

7. 運用

7-1 ネットワーク及び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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、情報システム運用時の情報資産の分類や取扱制限等を考慮し、必要な監視機能を実装しなければならない。

② 情報セキュリティ管理者は、情報システムの運用において、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 情報セキュリティ管理者は、情報システムに実装した監視機能について、新たな脅威の出現、運用の状況等を踏まえ、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、セキュリティに関する事案を検知するため、ネットワーク及び情報システムを常時監視しなければならない。

② 統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要なログ等を取得するサーバ等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、ガバメントクラウド等上で標準準拠システム等を利用する際には、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 情報セキュリティ管理者は、外部と常時接続するシステムを常時監視しなければならない。

④ 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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

7-2 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、重要度に応じて、速やかにCISO若しくは統括情報セキュリティ責任者に報告しなければならない。

② CISO若しくは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 情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における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）情報端末及び電磁的記録媒体等の利用状況調査

CISO及び統括情報セキュリティ責任者は、業務上必要な場合、職員等が使用している情報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統括情報セキュリティ責任者及び情報セキュリティ管理者が判断した場合において、職員等は、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。

7-3 侵害時の対応等

（1）緊急時対応計画の策定

① CISOは、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適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は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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

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（ICT-BCP: Information and Communication Technology - Business Continuity Plan）を策定し、当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（4）緊急時対応計画の見直し

CISOは、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

7-4 例外措置

（1）例外措置の許可

情報セキュリティ管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用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

情報セキュリティ管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、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。

7-5 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12月13日法律第261号）

② 教育公務員特例法（昭和24年1月12日法律第1号）
③ 著作権法（昭和45年法律第48号）
④ 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）
⑤ 個人情報の保護に関する法律（平成15年5月30日法律第57号）
⑥ 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）
⑦ サイバーセキュリティ基本法（平成26年法律第104号）

（2）情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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。

7-6 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課室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。
② 情報セキュリティ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室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及び情報セキュリティ管理者は、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、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課室等の情報セキュリティ管理者に通知しなければならない。

8. 業務委託と外部サービス（クラウドサービス）の利用

8-1 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ルールを定めなければならない。

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 情報セキュリティ管理者は、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受託者以外の者への提供の禁止
- 業務上知り得た情報の守秘義務
- 再委託に関する制限事項の遵守
- 委託業務終了時の情報資産の返還、廃棄等
- 委託業務の定期報告及び緊急時報告義務
- 市による監査、検査
- 市による情報セキュリティ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ことにより市に損害が生じた場合の規定（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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、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

8-2 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

情報セキュリティ管理者は、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

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

8-3 外部サービス（クラウドサービス）の利用（機密性2以上の情報を取り扱う場合）

（1）クラウドサービス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、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）（機密性2以上の情報を取り扱う場合）の選定に関する規定を整備しなければならない。

① クラウドサービス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8-3節において「クラウドサービス利用判断基準」という。）
② クラウドサービス提供者の選定基準
③ クラウドサービスの利用申請の許可権限者と利用手続
④ クラウドサービスの利用状況の管理

（2）クラウドサービス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、以下を含むクラウドサービス（機密性2以上の情報を取り扱う場合）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、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービス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、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービス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、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービス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） クラウドサービスの利用終了時における対策
（イ） クラウドサービスで取り扱った情報の廃棄
（ウ） クラウドサービスの利用のために作成したアカウントの廃棄

（3）クラウドサービスの選定

① 情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス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クラウドサービスの利用を検討しなければならない。
② 情報セキュリティ管理者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者

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クラウドサービス提供者の選定条件に含めなければならない。

（ア） クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止

（イ） クラウドサービス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） クラウドサービスの提供に当たり、クラウドサービス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） クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、前項（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、利用するクラウドサービスが、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 情報セキュリティ管理者は、クラウドサービス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、クラウドサービス提供者の選定条件に含めなければならない。

⑤ 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、クラウドサービス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する。

⑥ 情報セキュリティ管理者は、クラウドサービス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クラウドサービス提供者の選定条件に含めなければならない。

（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 情報セキュリティ管理者は、クラウドサービス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クラウドサービス提供者を選定し、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 情報セキュリティ管理者は、クラウドサービス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、クラウドサービス提供者の選定条件で求める内容をクラウドサービス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、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス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 情報セキュリティ管理者は、クラウドサービスの特性を考慮した上で、クラウドサービス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） クラウドサービスに求める情報セキュリティ対策

（イ） クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

（ウ） クラウドサービスに求めるサービスレベル

⑩ 情報セキュリティ管理者は、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、クラウドサービス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）クラウドサービスの利用に係る調達・契約

① 情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービス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 情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、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）クラウドサービスの利用承認

① 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には、利用申請の許可権限者へクラウドサービス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、職員等によるクラウドサービス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、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録する。

（6）クラウドサービス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、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービス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）クラウドサービス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
（ガバメントクラウド等上で標準準拠システム等を利用する場合のみ）

② 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、前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、クラウドサービス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。

③ 情報セキュリティ管理者は、情報システムにおいてクラウドサービスを利用する際には、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。

④ 情報セキュリティ管理者は、クラウドサービス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、クラウドサービス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） クラウドサービス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） クラウドサービス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） 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

（7）クラウドサービス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、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービス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） クラウドサービス利用方針の規定
（イ） クラウドサービス利用に必要な教育
（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） クラウドサービス内の通信の制御
（キ） 設計・設定時の誤りの防止
（ク） クラウドサービス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（ガバメントクラウド等上で標準準拠システム等を利用する場合のみ）

② 情報セキュリティ管理者は、クラウドサービスの運用・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 情報セキュリティ管理者は、クラウドサービス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 情報セキュリティ管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービス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 情報セキュリティ管理者は、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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、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、クラウドサービス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）クラウドサービス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、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービス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） クラウドサービスの利用終了時における対策

（イ） クラウドサービスで取り扱った情報の廃棄

（ウ） クラウドサービスの利用のために作成したアカウントの廃棄

② 情報セキュリティ管理者は、前項において定める規定に対し、クラウドサービス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 情報セキュリティ管理者は、ガバメントクラウド等上で標準準拠システム等を利用する際には、クラウドサービス上で機密性の高い情報を保存する場合は、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）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

8-4 外部サービス（クラウドサービス）の利用（機密性2以上の情報を取り扱わない場合）

（1）クラウドサービス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、以下を含むクラウドサービス（機密性2以上の情報を取り扱わない場合）の利用に関する規定を整備しなければならない。

（ア） クラウドサービスを利用可能な業務の範囲

（イ） クラウドサービスの利用申請の許可権限者と利用手続

（ウ） クラウドサービスの利用状況の管理

（エ） クラウドサービスの利用の運用手順

（2）クラウドサービス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機密性2以上の情報を取り扱わない場合のクラウドサービスの利用を申請しなければならない。また、情報セキュリティ管理者は、当該クラウドサービスの利用において適切な措置を講じなければならない。

② 利用申請の許可権限者は、職員等によるクラウドサービス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、承認したクラウドサービスを記録しなければならない。

9. 評価・見直し

9-1 監査

（1）実施方法

CISO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、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、CISO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）委託事業者等に対する監査

① 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。

② ガバメントクラウド等上で標準準拠システム等を利用する際には、クラウドサービス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。クラウドサービス事業者にその証拠（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統括責任者は、監査結果を取りまとめ、CISO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、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

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。なお、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定等の見直し等への活用

CISO又は富山市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。

9-2 自己点検

（1）実施方法

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、毎年度及び必要に応じて自己点検を行わなければならない。

（2）自己点検結果の活用

① 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は、自己点検結果と自己点検結果に基づく改善策を策定し、実施しなければならない。

② 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。

9-3 情報セキュリティポリシー及び関係規定等の見直し

CISO又は、富山市情報セキュリティ委員会は、情報セキュリティ監査及び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定等について毎年度又は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。