

深川市情報セキュリティ対策基準

第1章 総則

(目的)

第1条 本対策基準（以下「対策基準」という。）は、深川市情報セキュリティ基本方針（令和6年深川市訓令第37号。以下「基本方針」という。）に基づき、本市の情報資産のセキュリティ管理に必要な事項を定めることを目的とする。

(定義及び適用範囲)

第2条 対策基準における用語の意義は、次項及び第3項に定めるもののほか、基本方針の例による。

- 2 対策基準において、「学校ネットワーク」とは、学校教職員が校務で使用するネットワーク並びに児童及び生徒が授業等で使用する学習系情報ネットワークをいう。
- 3 対策基準において、「病院ネットワーク」とは、病院職員等が医療及び医療事務で使用するネットワークをいう。
- 4 対策基準の適用範囲は、基本方針の例による。ただし、第2項に規定する学校ネットワーク及び前項に既定する病院ネットワークに係る部分を除く。

第2章 組織体制

(最高情報セキュリティ責任者)

第3条 副市長を最高情報セキュリティ責任者（以下「C I S O」という。）とする。

- 2 C I S O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。
- 3 C I S O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。
- 4 C I S O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（以下「C S I R T」という。）を整備し、役割を明確化する。
- 5 C I S Oは、C I S O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C I S O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C I S O」という。）を必要に応じて置く。
- 6 C I S Oは、本対策基準に定められた自らの担務を、副C I S O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。

(統括情報セキュリティ責任者)

第4条 企画総務部長（情報セキュリティを担当する相当職があるときはその者）をC I S O直属の統括情報セキュリティ責任者とする。

- 2 統括情報セキュリティ責任者はC I S O及び副C I S Oを補佐しなければならない。
- 3 統括情報セキュリティ責任者は、情報セキュリティマネージャーに対して、情報セキュリティに関する指導及び助言を行う権限を有する。
- 4 統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、C I S Oの指示に従い、C I S O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。

(情報セキュリティマネージャー)

第5条 総務課長（情報セキュリティを担当する相当職があるときはその者）を情報セキュリティマネージャーとする。

- 2 情報セキュリティマネージャーは、統括情報セキュリティ責任者を補佐しなければならない。
- 3 情報セキュリティマネージャーは、統括情報セキュリティ責任者の指示に従い、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、見直し等の実施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。
- 4 情報セキュリティマネージャーは、統括情報セキュリティ責任者の指示に従い、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対し、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 情報セキュリティマネージャーは、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、統括情報セキュリティ責任者の指示に従い、被害の拡大防止、事態の回復のための対策実施、再発防止策の検討を行うものとする。
- 6 情報セキュリティマネージャーは、統括情報セキュリティ責任者の指示に従い、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「深川市情報セキュリティ実施手順」（以下「市セキュリティ実施手順」という。）の維持・管理を行う権限及び責任を有する。
- 7 情報セキュリティマネージャーは、緊急時等の円滑な情報共有を図るため、C I S O、統括情報セキュリティ責任者、情報セキュリティマネージャー、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者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 情報セキュリティマネージャーは、緊急時には統括情報セキュリティ責任者を通じてC I S Oに早急に報告を行うとともに、統括情報セキュリティ責任者の指示に従い、回復のための対策を講じなければならない。
- 9 情報セキュリティマネージャーは、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、必要に応じて統括情報セキュリティ責任者を通してC I S Oにその内容を報告しなければならない。

（情報セキュリティ責任者）

第6条 市長部局、行政委員会、議会事務局及び地方公営企業（以下「部局等」という。）の部長職を当該部局等の情報セキュリティ責任者とし、部長職が配置されていない部局等の情報セキュリティ責任者は企画総務部長とする。

- 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、深川市情報セキュリティポリシー（以下「セキュリティポリシー」という。）の遵守に関する意見の集約並びに職員及び会計年度任用職員（以下「職員等」という。）に対する指揮監督を行う。

（情報セキュリティ管理者）

第7条 各部局等の課室局所（以下「課室等」という。）の課長職を情報セキュリティ管理者とする。

- 2 情報セキュリティ管理者は、その所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。

- 3 情報セキュリティ管理者は、その所管する課室等において、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、CSIRT及び情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。
(情報システム管理者)

第8条 各情報システムの担当課室等の課長職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市セキュリティ実施手順の維持・管理を行う。
(情報システム担当者)

第9条 各情報システムの担当課長補佐、係長等を当該情報システムに関する情報システム担当者とする。

- 2 情報システム担当者は、情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う。
(情報セキュリティ委員会)

第10条 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（以下「委員会」という。）を設置する。

- 2 委員会は、次の内容について審議を行い、必要に応じてその結果を深川市庁議等規程（平成5年深川市訓令第25号）第2条に規定する深川市庁議に報告するものとする。
 - (1) 基本方針、対策基準及び市セキュリティ実施手順の策定、運用及び見直しに関すること。
 - (2) 情報セキュリティに関する事案の調査に関すること。
 - (3) 情報セキュリティ監査等の実施手順等に関すること。
 - (4) その他情報セキュリティに係る重要事項に関すること。
- 3 委員会は、CISO、統括情報セキュリティ責任者、情報セキュリティマネージャー及び情報セキュリティ管理者のうち深川市庁議等規程第11条第1号に掲げる職にある者（深川地区消防組合消防本部総務課長を除く。）をもって構成する。
- 4 CISOは、必要があると認めるときは、審議事項の所管課長の出席を求めることができる。
- 5 委員会の長は、CISOとする。
- 6 委員会の事務は、情報システムを管理する係が行う。
(兼務の禁止)

第11条 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者と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、や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。
(CSIRTの設置・役割)

第12条 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、深川市CSIRT設置要綱（平成29年深川市訓令第29号）第6条の規定に基づき、CSIRTに所属する職員を選任する。

- 3 C I S O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 C I S O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、必要に応じて、C I S O、総務省、北海道等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、外部の事業者等との情報共有を行わなければならない。

第3章 情報資産の分類と管理

(情報資産の分類)

第13条 本市における情報資産は、機密性、完全性、可用性等の観点により、重要度の高いものから重要性分類Ⅰ、Ⅱ、Ⅲ及びⅣとし、次の要件に従って分類する。

(1) 重要性分類Ⅰ

- ア 深川市情報公開条例（平成9年深川市条例第37号。以下「情報公開条例」という。）第5条第1項第1号、第2号、第5号、第6号及び第7号に規定されている情報を含むもの
- イ 個人情報保護に関する法律（平成15年法律第57号）第2条第1項及び第3項に規定されている情報を含むもの
- ウ 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）第2条第8項に定義されている情報を含むもの
- エ 情報システム運用管理に関する情報で、情報セキュリティを維持するため、機密の取扱いを要する情報を含むもの
- オ セキュリティ侵害が深川市の住民の生命、財産等へ重大な影響を及ぼす情報を含むもの
- カ アからオまでに掲げる場合のほか、情報セキュリティ管理者が情報の機密性、完全性、可用性その他の事情を考慮し、重要性分類Ⅰとして管理することが適当と認める情報を含むもの

(2) 重要性分類Ⅱ

- ア 情報公開条例第5条第1項第3号及び第4号に定義されている情報を含むもの
- イ 公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報を含むもの
- ウ ア及びイに掲げる場合のほか、情報セキュリティ管理者が情報の機密性、完全性、可用性、その他の事情を考慮し、重要性分類Ⅱとして管理することが適当と認める情報を含むもの

(3) 重要性分類Ⅲ

- ア 外部に公開される情報のうち、セキュリティ侵害が行政事務の執行等に軽微な影響を及ぼす情報を含むもの

イ アに掲げる場合のほか、情報セキュリティ管理者が情報の機密性、完全性、可用性、その他の事情を考慮し、重要性分類Ⅲとして管理することが適当と認める情報を含むもの

(4) 重要性分類Ⅳ

重要性分類Ⅰ、Ⅱ及びⅢ以外の情報を含むもの

(情報資産の管理)

第14条 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。また、庁内イントラネット等の組織が管理する情報資産については、情報セキュリティマネージャーが管理責任を有する。

2 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、複製等された情報資産も前条の分類に基づき管理しなければならない。

(情報資産の分類の表示)

第15条 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。

(情報の作成)

第16条 職員等は、業務上必要のない情報を作成してはならない。

2 情報を作成する者は、情報の作成時に第13条の分類に基づき、当該情報資産の分類と取扱制限を定めなければならない。

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

(情報資産の入手)

第17条 庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

2 庁外の者が作成した情報資産を入手した者は、第13条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

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

(情報資産の利用)

第18条 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。

2 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。

3 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。

(情報資産の保管)

第19条 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。

2 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。

3 情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

4 情報セキュリティ管理者又は情報システム管理者は、重要性分類Ⅱ以上の情報資産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設可能な場所に保管しなければならない。

(情報の送信)

第20条 電子メール等により重要性分類Ⅱ以上の情報資産を送信する者は、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。

(情報資産の運搬)

第21条 車両等により重要性分類Ⅱ以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、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を防止するための措置を講じなければならない。

2 重要性分類Ⅱ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。

(情報資産の提供・公表)

第22条 重要性分類Ⅱ以上の情報資産を外部に提供する者は、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。

2 重要性分類Ⅱ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。

3 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。

(情報資産の廃棄等)

第23条 情報資産の廃棄やリース返却等を行う者は、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。

2 情報資産の廃棄やリース返却等を行う者は、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。

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

第4章 情報システム全体の強靱性の向上

(マイナンバー利用事務系と他の領域との分離)

第24条 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。

2 前項の規定にかかわらず、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。

3 前項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、この限りでなく、L GWAN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。

(情報のアクセス及び持ち出しにおける対策)

第25条 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。

2 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。

（L GWAN接続系とインターネット接続系の分割）

第26条 L GWAN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L GWAN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。

（1） 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L GWAN接続系に転送するメールテキスト化方式

（2） インターネット接続系の端末から、L GWAN接続系の端末へ画面を転送等する方式

（3） 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

（インターネット接続系における情報セキュリティ対策）

第27条 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L GWAN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 北海道及び北海道内市町村等のインターネットとの通信を集約する北海道自治体情報セキュリティクラウドに参加するとともに、関係省庁や北海道等と連携しながら、情報セキュリティ対策を推進しなければならない。

3 業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産をL GWAN接続系に配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

4 業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

第5章 物理的セキュリティ

第1節 サーバ等の管理

（機器の取付け）

第28条 情報セキュリティマネージャー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。

（サーバの冗長化）

第29条 情報セキュリティマネージャー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、同一データを保持しなければならない。

2 情報セキュリティマネージャー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しなければならない。

(機器の電源)

第30条 情報セキュリティマネージャー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 情報セキュリティマネージャー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。

(通信ケーブル等の配線)

第31条 統括情報セキュリティ責任者、情報セキュリティマネージャー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、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、情報セキュリティマネージャー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、情報セキュリティマネージャー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、情報セキュリティマネージャー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外部委託事業者以外の者が配線を変更、追加できないよう必要な措置を講じなければならない。

(機器の定期保守及び修理)

第32条 情報セキュリティマネージャー及び情報システム管理者は、サーバ等の機器の定期保守を実施しなければならない。

2 情報セキュリティマネージャー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修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報セキュリティマネージャー及び情報システム管理者は、事業者修理にあたり、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。

(庁外への機器の設置)

第33条 情報セキュリティマネージャー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及び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、情報セキュリティマネージャー及び情報システム管理者は、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。

(機器の廃棄等)

第34条 情報セキュリティマネージャー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。

第2節 管理区域の管理

(管理区域の構造等)

第35条 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（以下「サーバ室」という。）や電磁的記録媒体の保管庫をいう。

- 2 情報セキュリティマネージャー及び情報システム管理者は、管理区域を地階又は1階に設けてはならない。
- 3 情報セキュリティマネージャー及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、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 情報セキュリティマネージャー及び情報システム管理者は、必要に応じ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 情報セキュリティマネージャー及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を塞がなければならない。
- 6 情報セキュリティマネージャー及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器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。

（管理区域の入退室管理等）

第36条 情報セキュリティマネージャー及び情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、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、情報セキュリティマネージャー又は情報システム管理者の求めにより提示しなければならない。
- 3 情報セキュリティマネージャー及び情報システム管理者は、外部からの訪問者が管理区域に入る場合、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員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 情報セキュリティマネージャー及び情報システム管理者は、重要性分類Ⅱ以上の情報資産を扱う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、又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。

（機器等の搬出入）

第37条 情報セキュリティマネージャー及び情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託事業者を確認を行わせなければならない。

- 2 情報セキュリティマネージャー及び情報システム管理者は、サーバ室の機器等の搬出入について、職員を立ち合わせなければならない。

第3節 通信回線及び通信回線装置の管理

（通信回線及び通信回線装置の管理）

第38条 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

- 3 情報セキュリティマネージャーは、本市が扱うネットワークを総合行政ネットワーク（L GWAN）に集約するように努めなければならない。
- 4 情報セキュリティマネージャーは、重要性分類Ⅱ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。
- 5 情報セキュリティマネージャーは、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分な情報セキュリティ対策を実施しなければならない。
- 6 情報セキュリティマネージャーは、重要性分類Ⅱ以上の情報資産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。

第4節 職員等の利用する端末や電磁的記録媒体等の管理

（職員等の利用する端末や電磁的記録媒体等の管理）

- 第39条 情報セキュリティマネージャー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保管等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
- 2 情報セキュリティマネージャー及び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、或いは必要に応じて生体認証等複数の認証情報の入力が必要とするように設定しなければならない。
 - 3 情報セキュリティマネージャー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。

第6章 人的セキュリティ

第1節 職員等の遵守事項

（職員等の遵守事項）

第40条 職員等の遵守事項については、次のとおりとする。

- （1）セキュリティポリシー等の遵守 職員等は、セキュリティポリシー及び市セキュリティ実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合、速やかに情報セキュリティ管理者又はC S I R Tへ相談し、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 C I S Oは、重要性分類Ⅱ以上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、情報セキュリティマネージャー又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) 支給以外のパソコン、モバイル端末、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、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CISO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、情報セキュリティマネージャー及び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。

イ 職員等は、支給以外のパソコン、モバイル端末、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 情報セキュリティマネージャーは、端末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マネージャー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マネージャー及び情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン及びモバイル端末の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返却しなければならない。また、その後も職務上知り得た情報を漏らしてはならない。

(会計年度任用職員への対応)

第41条 会計年度任用職員への対応については、次のとおりとする。

(1) セキュリティポリシー等の遵守 情報セキュリティマネージャーは、会計年度任用職員に対し、採用時（継続採用時を除く。）に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) インターネット接続及び電子メール使用等の制限 情報セキュリティマネージャーは、会計年度任用職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(セキュリティポリシー等の掲示)

第42条 情報セキュリティマネージャー及び情報セキュリティ管理者は、職員等が常にセキュリティポリシー及び市セキュリティ実施手順を閲覧できるように掲示しなければならない。

(委託事業者に対する説明)

第43条 情報セキュリティマネージャー及び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・保守等を事業者が発注する場合、再委託事業者も含めて、セ

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機密事項を説明しなければならない。

第2節 研修・訓練

(情報セキュリティに関する研修・訓練)

第44条 C I S O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。

(研修計画の策定及び実施)

第45条 研修計画の策定及び実施については、次のとおりとする。

- (1) C I S O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) 研修計画において、職員等が毎年度1回以上情報セキュリティ研修を受講できるようにしなければならない
- (3) 新規採用の職員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。
- (4) 研修は、統括情報セキュリティ責任者、情報セキュリティマネージャー、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対し、それぞれの役割、情報セキュリティに関する理解度等に応じたものに行なければならない。
- (5) 情報セキュリティマネージャーは、研修の実施状況を記録し、統括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。
- (6) 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、C I S O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。
- (7) C I S O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。

(緊急時対応訓練)

第46条 C I S Oは、緊急時対応を想定した訓練を定期的に行なければならない。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、効果的に実施できるようにしなければならない。

(研修・訓練への参加)

第47条 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。

第3節 情報セキュリティインシデントの報告

(庁内でのセキュリティインシデントの報告)

第48条 職員等は、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C S I R T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 C S I R T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C I S Oに報告しなければならない。

(住民等外部からのセキュリティインシデントの通報)

第49条 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セキュリティインシデントについて、住民等外部から通報を受けた場合、速やかに情報セキュリティ管理者及びCSIRT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、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。

(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)

第50条 CSIRTは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

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

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

4 CSIRTは、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISOに報告しなければならない。

5 CISOは、CSIRTから、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

第4節 ID及びパスワード等の管理

(ICカード等の取扱い)

第51条 職員等は、自己の管理するICカード及びUSBトークン等の媒体（以下「ICカード等」という。）に関し、次の事項を遵守しなければならない。

(1) 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。共用で利用する場合においては、利用簿等で管理し、共用の利用者以外に利用させてはならない。

(2) 業務上必要のないときは、ICカード等をカードリーダー又はパソコン等の端末のスロット等から抜いておかななければならない。

(3) 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マネージャー及び情報システム管理者に通報し、指示に従わなければならない。

2 情報セキュリティマネージャー及び情報システム管理者は、ICカード等の紛失等の報告があった場合、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 情報セキュリティマネージャー及び情報システム管理者は、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、破砕する等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。

(IDの取扱い)

第52条 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 I D は、他人に利用させてはならない。
- (2) 共用 I D を利用する場合、共用 I D の利用者以外に利用させてはならない。
(パスワードの取扱い)

第 5 3 条 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、情報セキュリティマネージャーに報告するとともに、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（初期パスワードを含む。）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、共有 I D に対するパスワードは除く。

第 7 章 技術的セキュリティ

第 1 節 コンピュータ及びネットワークの管理

(ファイルサーバの設定等)

第 5 4 条 情報セキュリティマネージャーは、職員等が利用できるファイルサーバを適切に管理しなければならない。

2 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、住民の個人情報、人事記録等、特定の職員等しか取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。

(バックアップの実施)

第 5 5 条 情報セキュリティマネージャー及び情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

(他団体との情報システムに関する情報等の交換)

第 5 6 条 情報セキュリティマネージャー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、情報セキュリティマネージャー（自らが実施する場合を除く。）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。

(システム管理記録及び作業の確認)

第 5 7 条 情報セキュリティマネージャー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 情報セキュリティマネージャー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なければならない。

3 情報セキュリティマネージャー、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、必要に応じ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。

(情報システム仕様書等の管理)

第58条 情報セキュリティマネージャー及び情報システム管理者は、ネットワーク構成図及び情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

(ログの取得等)

第59条 情報セキュリティマネージャー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 情報セキュリティマネージャー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 情報セキュリティマネージャー及び情報システム管理者は、必要に応じて取得したログを定期的に点検又は分析する機能を設け、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。

(障害記録)

第60条 情報セキュリティマネージャー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。

(ネットワークの接続制御、経路制御等)

第61条 情報セキュリティマネージャーは、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

2 情報セキュリティマネージャーは、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。

(外部の者が利用できるシステムの分離等)

第62条 情報セキュリティマネージャー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、物理的又は論理的に分離する等の措置を講じなければならない。

(外部ネットワークとの接続制限等)

第63条 情報セキュリティマネージャー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、統括情報セキュリティ責任者及び情報セキュリティマネージャー（自らが実施しようとする場合を除く。）の許可を得なければならない。

2 情報セキュリティマネージャー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 情報セキュリティマネージャー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、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 情報セキュリティマネージャー及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するため、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。
- 5 情報セキュリティマネージャー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及び情報セキュリティマネージャー（自らが実施する場合を除く。）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。

（複合機のセキュリティ管理）

第64条 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、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。

（I o T機器を含む特定用途機器のセキュリティ管理）

第65条 情報セキュリティマネージャーは、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。

（無線LAN及びネットワークの盗聴対策）

第66条 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、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。

（電子メールのセキュリティ管理）

第67条 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、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。

(電子メールの利用制限)

第68条 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及びC S I R Tに報告しなければならない。

5 職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等を使用してはならない。

(電子署名・暗号化)

第69条 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、C I S Oが定めた電子署名、パスワード等による暗号化等、セキュリティを考慮し、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C I S Oが定める以外の方法を用いてはならない。また、C I S O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 C I S O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。

(無許可ソフトウェアの導入等の禁止)

第70条 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、情報セキュリティマネージャー及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティマネージャー又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

3 職員等は、不正にコピーしたソフトウェアを利用してはならない。

(機器構成の変更の制限)

第71条 職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

2 職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報セキュリティマネージャー及び情報システム管理者の許可を得なければならない。

(業務外ネットワークへの接続の禁止)

第72条 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 情報セキュリティマネージャーは、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。

(業務以外の目的でのウェブ閲覧の禁止)

第73条 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 情報セキュリティマネージャーは、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、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。

(ウェブ会議サービスの利用時の対策)

第74条 情報セキュリティマネージャーは、ウェブ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、ウェブ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、ウェブ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、外部からウェブ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。

(ソーシャルメディアサービスの利用)

第75条 情報セキュリティマネージャー及び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。

(1) 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、本市の自己管理ウェブサイト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。

(2) 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等の方法で、不正アクセス対策を実施すること。

2 重要性分類Ⅱ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 重要性分類Ⅱ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。

第2節 アクセス制御

(アクセス制御等)

第76条 アクセス制御等については、次のとおりとする。

(1) アクセス制御 情報セキュリティマネージャー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、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 情報セキュリティマネージャー及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向及び退職に伴う利用者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、情報セキュリティマネージャー又は情報システム管理者に通知しなければならない。

ウ 情報セキュリティマネージャー及び情報システム管理者は、利用されていないIDが放置されないよう、人事管理部門と連携し、点検しなければならない。

(3) 特権を付与されたIDの管理等

- ア 情報セキュリティマネージャー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 情報セキュリティマネージャー及び情報システム管理者の特権を代行する者は、情報セキュリティマネージャー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。
- ウ 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、情報セキュリティマネージャー、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。
- エ 情報セキュリティマネージャー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、制約なしに委託事業者に行わせてはならない。
- オ 情報セキュリティマネージャー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、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能の強化に努めなければならない。
- カ 情報セキュリティマネージャー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。
(職員等による外部からのアクセス等の制限)

第77条 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、情報セキュリティマネージャー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 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、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 情報セキュリティマネージャーは、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 情報セキュリティマネージャー及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のため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、情報セキュリティ管理者の許可を得るか、若しくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。
- 7 情報セキュリティマネージャーは、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、セキュリティ確保のため必要な措置を講じなければならない。

(自動識別の設定)

第78条 情報セキュリティマネージャー及び情報システム管理者は、ネットワークで使用される機器について、特に機密性の高いネットワークにおいて、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

(ログイン時の表示等)

第79条 情報セキュリティマネージャー及び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。

(認証情報の管理)

第80条 情報セキュリティマネージャー又は情報システム管理者は、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 情報セキュリティマネージャー又は情報システム管理者は、職員等に対し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 情報セキュリティマネージャー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。

(特権による接続時間の制限)

第81条 情報セキュリティマネージャー及び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。

第3節 システム開発、導入、保守等

(情報システムの調達)

第82条 情報セキュリティマネージャー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。

2 情報セキュリティマネージャー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。

(情報システムの開発)

第83条 情報セキュリティマネージャー及び情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、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 システム開発における責任者及び作業者のIDの管理は次のとおりとする。

(1) 情報セキュリティマネージャー及び情報システム管理者は、システム開発の責任者及び作業者が使用するID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。

(2) 情報セキュリティマネージャー及び情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

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は次のとおりとする。

- (1) 情報セキュリティマネージャー及び情報システム管理者は、システム開発の責任者及び作業者が使用する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。
- (2) 情報セキュリティマネージャー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しなければならない。

(情報システムの導入)

第84条 開発環境と運用環境の分離及び移行手順の明確化については、次のとおりとする。

- (1) 情報セキュリティマネージャー及び情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を必要に応じて分離しなければならない。
- (2) 情報セキュリティマネージャー及び情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。
- (3) 情報セキュリティマネージャー及び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し、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。
- (4) 情報セキュリティマネージャー及び情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

2 テストについては、次のとおりとする。

- (1) 情報セキュリティマネージャー及び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。
- (2) 情報セキュリティマネージャー及び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。
- (3) 情報セキュリティマネージャー及び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。
- (4) 情報セキュリティマネージャー及び情報システム管理者は、開発したシステムについて受入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

(システム開発・保守に関連する資料等の整備・保管)

第85条 情報セキュリティマネージャー及び情報システム管理者は、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 情報セキュリティマネージャー及び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 情報セキュリティマネージャー及び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。

(情報システムにおける入出力データの正確性の確保)

第86条 情報セキュリティマネージャー及び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 情報セキュリティマネージャー及び情報システム管理者は、故意又は過失により情報が改ざんされる、又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

3 情報セキュリティマネージャー及び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。

(情報システムの変更管理)

第87条 情報セキュリティマネージャー及び情報システム管理者は、情報システムを変更した場合、実用に応じて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。

(開発・保守用のソフトウェアの更新等)

第88条 情報セキュリティマネージャー及び情報システム管理者は、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。

(システム更新又は統合時の検証等)

第89条 情報セキュリティマネージャー及び情報システム管理者は、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。

第4節 不正プログラム対策

(情報セキュリティマネージャーの措置事項)

第90条 情報セキュリティマネージャーは、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等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。

(情報システム管理者の措置事項)

第91条 情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

- (1) 情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。
- (2) 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
- (3) 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
- (4) インターネットに接続していないシステムにおいて、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、本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、職員等に当該権限を付与してはならない。

(職員等の遵守事項)

第92条 職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

- (1) パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
- (2) 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
- (3) 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに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 LAN 接続系に取り込む場合は無害化しなければならない。
- (6) 情報セキュリティマネージャー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。

(専門家の支援体制)

第93条 情報セキュリティマネージャーは、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。

第5節 不正アクセス対策

(情報セキュリティマネージャーの措置事項)

第94条 情報セキュリティマネージャーは、不正アクセス対策として、次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、情報セキュリティマネージャー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) CISOは、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。

(攻撃への対処)

第95条 CISO、統括情報セキュリティ責任者及び情報セキュリティマネージャーは、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、北海道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。

(記録の保存)

第96条 CISO、統括情報セキュリティ責任者及び情報セキュリティマネージャーは、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成11年法律第128号）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。

(内部からの攻撃)

第97条 情報セキュリティマネージャー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。

(職員等による不正アクセス)

第98条 情報セキュリティマネージャー及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

(サービス不能攻撃)

第99条 情報セキュリティマネージャー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、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。

(標的型攻撃)

第100条 情報セキュリティマネージャー及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するため、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。

第6節 セキュリティ情報の収集

(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)

第101条 情報セキュリティマネージャー及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、

当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

(不正プログラム等のセキュリティ情報の収集・周知)

第102条 情報セキュリティマネージャーは、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。

(情報セキュリティに関する情報の収集及び共有)

第103条 情報セキュリティマネージャー及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第8章 運用

第1節 情報システムの監視

(情報システムの監視)

第104条 情報セキュリティマネージャー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 情報セキュリティマネージャー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。
- 3 情報セキュリティマネージャー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。

第2節 セキュリティポリシーの遵守状況の確認

(遵守状況の確認及び対処)

第105条 情報セキュリティ管理者は、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、統括情報セキュリティ責任者及び情報セキュリティマネージャーに報告しなければならない。

- 2 CISOは、発生した問題について、適正かつ速やかに対処しなければならない。
- 3 情報セキュリティマネージャー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。

(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)

第106条 CISO及びCISOが指名した者は、不正アクセス、不正プログラム等の調査のために職員等が使用しているパソコン、モバイル端末及び電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。

(職員等の報告義務)

第107条 職員等は、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CSIRT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場合又はCSIRT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。

第3節 侵害時の対応等

(緊急時対応計画の策定)

第108条 CISOは、情報セキュリティインシデント、セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適

切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

(緊急時対応計画に盛り込むべき内容)

第109条 緊急時対応計画には、次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

(業務継続計画との整合性確保)

第110条 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。

(緊急時対応計画の見直し)

第111条 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。

第4節 例外措置

(例外措置の許可)

第112条 情報セキュリティマネージャー、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。

(緊急時の例外措置)

第113条 情報セキュリティマネージャー、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。

(例外措置の申請書の管理)

第114条 CISOは、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

第5節 法令遵守

(法令遵守)

第115条 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、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
- (4) 個人情報の保護に関する法律
- (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
- (6) サイバーセキュリティ基本法（平成28年法律第31号）
- (7) 深川市個人情報保護法施行条例（令和5年深川市条例第2号）

第6節 懲戒処分等

(懲戒処分)

第116条 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。

(違反時の対応)

第117条 職員等の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又は情報セキュリティマネージャーが違反を確認した場合は、統括情報セキュリティ責任者又は情報セキュリティマネージャー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情報セキュリティマネージャー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、情報セキュリティマネージャーは、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又は剥奪することができる。その後速やかに、情報セキュリティマネージャーは、職員等の権利を停止又は剥奪した旨をCISO、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なければならない。

第9章 業務委託と外部サービスの利用

第1節 業務委託

(委託事業者の選定基準)

第118条 情報セキュリティマネージャー及び情報セキュリティ管理者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

2 情報セキュリティマネージャー及び情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

(契約項目)

第119条 重要な情報資産を取扱う業務を委託する場合には、委託事業者との間に必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

- (1) セキュリティポリシー及び市セキュリティ実施手順の遵守
- (2) 委託事業者の責任者、委託内容、作業者の所属及び作業場所の特定
- (3) 提供されるサービスレベルの保証
- (4) 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
- (5) 委託事業者の従業員に対する教育の実施
- (6) 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
- (7) 業務上知り得た情報の守秘義務
- (8) 再委託に関する制限事項の遵守
- (9) 委託業務終了時の情報資産の返還、廃棄等
- (10) 委託業務の定期報告及び緊急時報告義務
- (11) 市による監査及び検査
- (12) 市による情報セキュリティインシデント発生時の公表

(13) 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）
（確認・措置等）

第120条 情報セキュリティマネージャー及び情報セキュリティ管理者は、委託事業者において必要な情報セキュリティ対策が確保されていることを定期的に確認し、必要に応じ前条の契約に基づき措置を実施しなければならない。また、内容を情報セキュリティマネージャー（情報セキュリティマネージャーが確認した場合は統括情報セキュリティ責任者）に報告するとともに、その重要度に応じてCISOに報告しなければならない。

第2節 外部サービスの利用（重要性分類Ⅱ以上の情報を取り扱う場合）
（外部サービスの利用に係る規定の整備）

第121条 情報セキュリティマネージャー及び情報セキュリティ管理者は、次の内容を含む外部サービスの利用に関する規定を整備しなければならない。

- (1) 外部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「外部サービス利用判断基準」という。）
- (2) 外部サービス提供者の選定基準
- (3) 外部サービスの利用申請の許可権限者と利用手続
- (4) 外部サービス管理者の指名と外部サービスの利用状況の管理
（外部サービスの選定）

第122条 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、外部サービス利用判断基準に従って外部サービスの利用を検討しなければならない。

2 情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定しなければならない。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提供者の選定条件に含めなければならない。

- (1) 外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止
- (2) 外部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
- (3) 外部サービスの提供に当たり、外部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
- (4) 外部サービス提供者の資本関係・役員等の情報、外部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
- (5) 情報セキュリティインシデントへの対処方法
- (6) 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
- (7) 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、外部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、外部サービス提供者の選定条件に含めなければならない。

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提供者の選定条件に含めなければならない。

- (1) 情報セキュリティ監査の受入れ
- (2) サービスレベルの保証

- 5 情報セキュリティ責任者は、外部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外部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。
- 6 情報セキュリティ責任者は、外部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、外部サービス提供者の選定条件で求める内容を外部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、外部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、外部サービス利用判断基準及び外部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。
- 7 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に応じてセキュリティ要件を定め、外部サービスを選定しなければならない。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。
- 8 情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部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、セキュリティ要件を定めなければならない。
- 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。

(外部サービスの利用に係る調達・契約)

第123条 情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部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 情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めなければならない。

(外部サービスの利用承認)

第124条 情報セキュリティ責任者は、外部サービス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、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名しなければならない。

(外部サービスを利用した情報システムの導入・構築時の対策)

第125条 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、次の内容を含む外部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。

- (1) 不正なアクセスを防止するためのアクセス制御
- (2) 取り扱う情報の機密性保護のための暗号化
- (3) 開発時におけるセキュリティ対策

(4) 設計・設定時の誤りの防止

2 外部サービス管理者は、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。

(外部サービスを利用した情報システムの運用・保守時の対策)

第126条 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次の内容を含む外部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。

- (1) 外部サービス利用方針の規定
- (2) 外部サービス利用に必要な教育
- (3) 取り扱う資産の管理
- (4) 不正アクセスを防止するためのアクセス制御
- (5) 取り扱う情報の機密性保護のための暗号化
- (6) 外部サービス内の通信の制御
- (7) 設計・設定時の誤りの防止
- (8) 外部サービスを利用した情報システムの事業継続

2 情報セキュリティ責任者は、外部サービス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。

3 外部サービス管理者は、前2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。

(外部サービスを利用した情報システムの更改・廃棄時の対策)

第127条 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次の内容を含む外部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。

- (1) 外部サービスの利用終了時における対策
- (2) 外部サービスで取り扱った情報の廃棄
- (3) 外部サービスの利用のために作成したアカウントの廃棄

2 外部サービス管理者は、前項において定める規定に対し、外部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。

第3節 外部サービスの利用（重要性分類Ⅱ以上の情報を取り扱わない場合）

(外部サービスの利用に係る規定の整備)

第128条 統括情報セキュリティ責任者は、次の内容を含む外部サービス（重要性分類Ⅱ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。

- (1) 外部サービスを利用可能な業務の範囲
- (2) 外部サービスの利用申請の許可権限者と利用手続
- (3) 外部サービス管理者の指名と外部サービスの利用状況の管理
- (4) 外部サービスの利用の運用手続

(外部サービスの利用における対策の実施)

第129条 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重要性分類Ⅱ以上の情報を取り扱わない場合の外部サービス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管理者は、当該外部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 情報セキュリティ責任者は、職員等による外部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、承認した外部サービスを記録しなければならない。

第10章 評価・見直し

第1節 監査

(実施方法)

第130条 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、適宜、必要に応じて監査を行わせなければならない。

(監査を行う者の要件)

第131条 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、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。

(監査実施計画の立案及び実施への協力)

第132条 情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

2 被監査部門は、監査の実施に協力しなければならない。

(委託事業者に対する監査)

第133条 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統括責任者は委託事業者（再委託事業者を含む。）に対して、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。

(報告)

第134条 情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告するものとする。

(保管)

第135条 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。

(監査結果への対応)

第136条 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。

(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)

第137条 情報セキュリティ委員会は、監査結果を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。

第2節 自己点検

(実施方法)

第138条 情報セキュリティマネージャー及び情報システム管理者は、所管するネットワーク及び情報システムについて、定期的に、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 情報セキュリティ責任者は、情報セキュリティ管理者と連携し、所管する部局における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、定期的に、及び必要に応じて自己点検を行わなければならない。

(報告)

第139条 情報セキュリティマネージャー、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

(自己点検結果の活用)

第140条 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。

第3節 セキュリティポリシー及び関係規程等の見直し

(セキュリティポリシー及び関係規程等の見直し)

第141条 情報セキュリティ委員会は、情報セキュリティ監査、自己点検の結果、情報セキュリティに関する状況の変化等を踏まえ、セキュリティポリシー、関係規程等について定期的及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

附 則

この訓令は、令和6年4月1日から施行する。