青森市情報セキュリティポリシー

令和 7 年 4 月 1 日策定

令和 8 年 3 月 24 日改定

青森市

目次

第1章　青森市情報セキュリティ基本方針 1

1.目的 1

2.定義 1

3.対象とする脅威 2

4.適用範囲 2

5.職員等の遵守義務 3

6.情報セキュリティ対策 3

7.情報セキュリティ監査及び自己点検の実施 4

8.情報セキュリティポリシーの見直し 4

9.情報セキュリティ対策基準の策定 4

10.情報セキュリティ実施手順の策定 4

第2章　青森市情報セキュリティ対策基準 5

1.組織体制 5

2.情報資産の分類と管理 8

3.情報システム全体の強靭性の向上 11

4.物理的セキュリティ 12

5.人的セキュリティ 16

6.技術的セキュリティ 21

7.運用 33

8.業務委託と外部サービス（クラウドサービス）の利用 37

9.評価・見直し 42

【資料】権限・責任等一覧表 44

第１章　青森市情報セキュリティ基本方針

1.　目的

青森市情報セキュリティ基本方針（以下「基本方針」という。）は、本市が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産について、本市が実施する情報セキュリティに関する基本的な事項を定めることにより、行政の適正かつ円滑な運営を図り、もって市政に対する市民の信頼を確保す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

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

（６）完全性

情報資産が破壊、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

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

（８）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

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（個人番号利用事務系を除く。）。

（１０）インターネット接続系

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、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）地震、落雷、火災等の災害によるサービス及び業務の停止等

（４）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4. 適用範囲

（１）組織の範囲

本基本方針が適用される組織は、市長、行政委員会、議会事務局及び次に掲げる組織とする。

①青森市公営企業の設置等に関する条例（平成 17 年青森市条例第 219 号）第 2 条、第 5 条、第 8 条及び第 10 条の 2 に掲げる組織

②青森市行政組織規則（平成 17 年青森市規則第 10 号）第 3 条に掲げる組織

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク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

5. 職員等の遵守義務

職員及び会計年度任用職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

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個人番号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。

②LGWAN 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、情報システム室、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、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、

情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、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。

なお、情報セキュリティ対策基準は、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具体的事項については非公開とする。

10. 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

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。

第２章　青森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.　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。）

①CISO は、青森市長の職務を代理する副市長の順序を定める規則（令和５年青森市規則第４２号）（以下「副市長規則」という。）第一号に掲げる副市長をもって充て、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。

②CISO 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くことができ、その業務内容を定めることができる。

③CISO は、情報システムに対するサイバー攻撃等の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。

④CISO 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。副 CISO は副市長規則第二号に掲げる副市長をもって充てる。

⑤CISO は、本ガイドライン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。CISO に事故があるとき、又は CISO が欠けたときは、副 CISO がその職務を代理する。

（２）統括情報セキュリティ責任者

①総務部長を CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISO 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、情報セキュリティ管理者、情報システム管理者、個別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、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。

⑦CISO 及び副 CISO にともに事故があるとき、又は CISO 及び副 CISO がともに欠けたときは、統括情報セキュリティ責任者が CISO の職務を代理する。

⑧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、副 CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、個別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。

⑨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。

⑩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基本方針の適用範囲の各部局等の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及び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）情報セキュリティ管理者

①情報システムを使用する課等の長を情報セキュリティ管理者とする。

②情報セキュリティ管理者は、その所管する課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、その所管する課等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。また、情報システム管理者へ報告しなければならない。

（５）情報システム管理者

①総務部情報管理課長を情報システム管理者とする。

②情報システム管理者は、情報管理課が導入した情報システムに関する権限及び責任を有する。ただし、情報システムに関する権限及び責任について、別に定めがある場合はこの限りではない。

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。

④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。

⑤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。

（６）個別情報システム管理者

①課等において、個別に情報システムを導入している課等の長を個別情報システム管理者とする。

②個別情報システム管理者は、課等が個別に導入した情報システムに関する権限及び責任を有する。

③個別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。

④個別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。

⑤個別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又は個別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本市における情報セキュリティ対策を統一的に行うため、情報セキュリティポリシー等、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委員会を設置する。

②審議事項

情報セキュリティ委員会は、以下に掲げる事項を審議する。

（ア）情報セキュリティ対策の決定及び見直しに関する事項

（イ）情報セキュリティ対策の遵守状況の確認に関する事項

（ウ）情報セキュリティ対策の有効性の検証の実施に関する事項

（エ）研修及び訓練の実施に関する事項

（オ）その他情報セキュリティ対策実施に必要な事項

③構成員

情報セキュリティ委員会は、以下に掲げる者をもって組織する。

（ア）CISO

（イ）副 CISO

（ウ）統括情報セキュリティ責任者

（エ）情報セキュリティ責任者

④庶務

情報セキュリティ委員会の庶務は、総務部情報管理課において行う。

（９）兼務の禁止

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。

（１０）CSIRT の設置・役割

①CISO は、CSIRT を整備し、その役割を明確化しなければならない。
②CISO 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。
③CISO は、情報セキュリティの統一的な窓口を整備し、情報システムに対するサイバー攻撃等の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。
④CISO 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情報システムに対するサイバー攻撃等の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 CISO、総務省、都道府県等へ報告しなければならない。
⑥情報システムに対するサイバー攻撃等の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。

2. 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、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。

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
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	・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	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	－

（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及び個別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。

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）、へ

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

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

④情報資産の入手

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

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

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

⑤情報資産の利用

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

（イ）情報資産を利用する者は、情報資産の分類に応じ、適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、情報システム管理者及び個別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）情報セキュリティ管理者、情報システム管理者及び個別情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ）情報セキュリティ管理者、情報システム管理者及び個別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。

（エ）情報セキュリティ管理者、情報システム管理者及び個別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者は、必要に応じ、暗号化又は

パスワード設定を行わなければならない。

⑧情報資産の運搬

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

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

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

⑩情報資産の廃棄

（ア）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。

（イ）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。

（ウ）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。

3. 情報システム全体の強靭性の向上

（１）個人番号利用事務系

①個人番号利用事務系と他の領域との分離

個人番号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。個人番号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、インターネット等から LGWAN を経由して、インターネット等と個人番号利用事務系との双方向通信でのデータ移送を可能とする。

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。

（２）LGWAN 接続系

①LGWAN 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

（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する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

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

情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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。

（３）機器の電源

①情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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及び個別情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認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、情報システム管理者及び個別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

情報システム管理者及び個別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。

4.2. 入退室等管理

（１）入退室等管理区域

以下の表の左欄に掲げる室又は場所（以下「入退室等管理区域」という。）の区分に応じ、それぞれ右欄に掲げるセキュリティ区分を設定する。

（非公表）

上記に定めるセキュリティ区分に応じた入退室等管理の方法は、下表のとおりとする。

セキュリティ区分	入退室等管理の方法
レベル 3	入退室を行う場合には、情報セキュリティ管理者から事前に許可を得ている者のみが入退室を行い、その都度、入退室管理カードを用いて入退室を行う。 識別を行うために、入退室者には名札の着用を義務付ける。また、入退室に関する記録を行う。
レベル 2	入退室を行う場合には、情報セキュリティ管理者から事前に許可を得ている者のみが鍵又は入退室管理カードを用いて入退室を行う。 識別を行うために、入退室者には名札の着用を義務付ける。また、当該場所に勤務する者以外の入退室に関する記録を行う。
レベル 1	情報セキュリティ管理者から事前に許可を得ている者のみが端末操作に従事する。 識別を行うために、入退室者には名札等の着用を義務付ける。また、当該場所に勤務する者以外の入退室に関する記録を行う。

入退室等管理区域に該当する具体的な室及び場所は、次のとおりである。

（非公表）

（２）入退室等管理の実施

入退室等管理区域を所管する情報セキュリティ管理者は、入退室等の管理の実施及び入退室等の管理に関し必要な措置をとらなければならない。

（３）鍵及び入退室管理カードの管理

鍵及び入退室管理カードの管理は、入退室等管理区域を所管する情報セキュリティ管理者が行う。

鍵及び入退室管理カードの貸与については、上記情報セキュリティ管理者から許可を得ている者に対する場合に限るものとする。

（４）管理簿の作成

①入退室等管理簿の作成

入退室等管理区域を所管する情報セキュリティ管理者は、入退室等管理簿を作成し、10 年間保管しなければならない。

②鍵及び入退室管理カード管理簿の作成

入退室等管理区域を所管する情報セキュリティ管理者は、入退室等管理区域に係る鍵及び

入退室管理カードの管理簿を作成し、10 年間保管しなければならない。

③管理簿への記載事項

鍵及び入退室管理カードの管理簿には以下に掲げる事項を記載する。

（ア）貸与年月日

（イ）入退室被許可者の所属、職及び氏名

（ウ）入退室被許可者の職員コード

（エ）入退室被許可者の業務内容

（オ）入退室被許可者カード番号

（カ）返却年月日

（５）入退室等管理に関する指示について

CISO は、適切な入退室等管理の確保のため、入退室等管理区域を所管する情報セキュリティ管理者等から報告を聴取し、調査を行い、又は必要な指示を行うものとする。

（６）機器等の搬入出

①情報システム管理者及び個別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に確認を行わせなければならない。

②情報システム管理者及び個別情報システム管理者は、入退室等管理区域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。

4.3. 通信回線及び通信回線装置の管理

①情報システム管理者及び個別情報システム管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適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情報システム管理者及び個別情報システム管理者は、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情報システム管理者及び個別情報システム管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

④情報システム管理者及び個別情報システム管理者は、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情報システム管理者及び個別情報システム管理者は、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情報システム管理者及び個別情報システム管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、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情報システム管理者及び個別情報システム管理者は、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情報システム管理者及び個別情報システム管理者は、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。

4.4. 職員等が利用する端末機器等の管理

①統括情報セキュリティ責任者は、職員等が利用する端末機器等の運用管理について必要な事項を定めなければならない。

②情報セキュリティ管理者は、所管する課等に設置された端末機器等について、盗難防止のための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。

③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、利用者の認証を行い、不正利用防止のための措置を講じなければならない。

④情報システム管理者は、個人番号利用事務系では「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。

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、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

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。

⑤持ち出しの記録

情報セキュリティ管理者は、端末等の持ち出しについて、記録を作成し、保管しなければならない。

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システム管理者又は個別情報システム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返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（２）会計年度任用職員等への対応

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。

（３）情報セキュリティポリシー等の掲示

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

（４）委託事業者に対する説明

情報システム管理者及び個別情報システム管理者は、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や、事業者に情報システムを使用させる場合、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。

（５）指定管理者に対する説明

情報セキュリティ管理者は、指定管理者に情報システムを使用させる場合、指定管理者から再委託をう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指定管理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

CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（２）研修計画の策定及び実施

①CISO は、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研修計画において、職員等は計画的に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、職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤情報セキュリティ管理者は、所管する課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。

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、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。

⑦CISO 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

全ての職員等は、定められた研修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）庁内での情報セキュリティインシデント（サイバー攻撃以外）の報告

①職員等は、情報セキュリティインシデント（サイバー攻撃以外）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情報システム管理者に報告しなければならない。

③情報システム管理者は、報告のあった情報セキュリティインシデント（サイバー攻撃以外）について、必要に応じ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。

④情報セキュリティ責任者は、報告のあった情報セキュリティインシデント（サイバー攻撃以外）について、必要に応じて CISO に報告しなければならない。

⑤情報セキュリティインシデント（サイバー攻撃以外）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。

⑥情報セキュリティ管理者は、これらの情報セキュリティインシデント原因を究明し、被害の拡大防止等を図るための応急措置や復旧措置を実施し、記録を保存しなければならない。また、情報セキュリティ責任者は、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。

⑦CISO は、情報セキュリティ責任者から、情報セキュリティインシデント（サイバー攻撃以外）について報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

（２）住民等外部からの情報セキュリティインシデント（サイバー攻撃以外）の報告

①職員等は、本市が管理する情報システムや情報資産に関する情報セキュリティインシデント（サイバー攻撃以外）について、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③情報システム管理者は、報告のあった情報セキュリティインシデント（サイバー攻撃以外）について、必要に応じ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。

④情報セキュリティ責任者は、当該情報セキュリティインシデント（サイバー攻撃以外）について、必要に応じてCISOに報告しなければならない。

⑤情報セキュリティインシデント（サイバー攻撃以外）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。

⑥情報セキュリティ管理者は、これらの情報セキュリティインシデント原因を究明し、被害の拡大防止等を図るための応急措置や復旧措置を実施し、記録を保存しなければならない。また、情報セキュリティ責任者は、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。

⑦CISOは、情報セキュリティ責任者から、情報セキュリティインシデント（サイバー攻撃以外）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。

（３）情報システムに対するサイバー攻撃等の情報セキュリティインシデントの報告

①CSIRT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、情報システムに対するサイバー攻撃等の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。

②CSIRTは、情報システムに対するサイバー攻撃等の情報セキュリティインシデントであると評価した場合、必要に応じてCISOに速やかに報告しなければならない。

③情報システムに対するサイバー攻撃等の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。

④CSIRTは、情報システムに対するサイバー攻撃等の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、必要に応じて情報システム管理者及び個別情報システム管理者へ確認を指示しなければならない。

⑤CSIRTは、これらの情報システムに対するサイバー攻撃等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、情報システムに対するサイバー攻撃等の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。

⑥CISOは、CSIRTから、情報システムに対するサイバー攻撃等の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。

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、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、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統括情報セキュリティ責任者及び情報システム管理者は、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 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）共有ファイルサーバの設定等

①情報システム管理者及び個別情報システム管理者は、所管する共有ファイルサーバーにつ

いて、職員等が使用できる容量を設定し、職員等に周知しなければならない。

②情報システム管理者及び個別情報システム管理者は、所管する共有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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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。

（３）システム管理記録及び作業の確認

①情報システム管理者及び個別情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②情報システム管理者及び個別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、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。

（４）情報システム仕様書等の管理

情報システム管理者及び個別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。

（５）ログの取得等

①情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②情報システム管理者は、ログ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。

（６）障害記録

情報システム管理者及び個別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。

（７）ネットワークの接続制御、経路制御等

①情報システム管理者及び個別情報システム管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②情報システム管理者及び個別情報システム管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

③情報システム管理者及び個別情報システム管理者は、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

情報システム管理者及び個別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。

（９）外部ネットワークとの接続制限等

①情報システム管理者及び個別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、統括情報セキュリティ責任者の許可を得なければならない。

②情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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。

⑤情報システム管理者及び個別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。

（１０）複合機のセキュリティ管理

①情報システム管理者及び個別情報システム管理者は、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情報システム管理者及び個別情報システム管理者は、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情報システム管理者及び個別情報システム管理者は、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 及びネットワークの盗聴対策

①情報システム管理者及び個別情報システム管理者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

②情報システム管理者及び個別情報システム管理者は、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。

（１３）電子メールのセキュリティ管理

①情報システム管理者及び個別情報システム管理者は、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情報システム管理者及び個別情報システム管理者は、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情報システム管理者及び個別情報システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④情報システム管理者及び個別情報システム管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤情報システム管理者及び個別情報システム管理者は、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。

（１５）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、必要に応じて電子署名、パスワード等による暗号化等、セキュリティを考慮して、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情報システム管理者が定める以外の方法を用いてはならない。また、情報システム管理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情報システム管理者は、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。

（１６）無許可ソフトウェアの導入等の禁止
①職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
②職員等は、業務上の必要がある場合は、情報システム管理者又は個別情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者、情報システム管理者及び個別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。

（１７）機器構成の変更の制限
①職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。
②職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報システム管理者及び個別情報システム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、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及び個別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情報システム管理者及び個別情報システム管理者は、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。

（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。

（２１）ソーシャルメディアサービスの利用

①ソーシャルメディアサービスを所管する課の長は、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、本市の自己管理ウェブサイトに当該情報掲載し参照可能等するとともに、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（ハードディスク、USB メモリ、紙等）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）アクセス制御等

①アクセス制御

情報システム管理者及び個別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権限を付与する等、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）情報システム管理者及び個別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、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）情報システム管理者及び個別情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

（ウ）情報システム管理者及び個別情報システム管理者は、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）情報システム管理者及び個別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）情報システム管理者及び個別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）情報システム管理者及び個別情報システム管理者の特権を代行する者は、情報システム管理者及び個別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、情報セキュリティ管理者、情報システム管理者及び個別情報システム管理者に通知しなければならない。

（オ）情報システム管理者及び個別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）情報システム管理者及び個別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を強化しなければならない。

（キ）情報システム管理者及び個別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、情報セキュリティ管理者の許可を得なければならない。

②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情報システム管理者は、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情報システム管理者は、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。

（３）認証情報の管理

①情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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。

（４）特権による接続時間の制限

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。

6.3. システム開発、導入、保守等

（１）機器等及び情報システムの調達

①情報システム管理者及び個別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情報システム管理者及び個別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情報セキュリティ管理者は、情報システム及びそれに係る端末機器等を個別に調達する際は、事前に情報システム管理者と協議を行わなければならない。

（２）情報システムの開発

①システム開発における責任者及び作業者の特定

情報システム管理者及び個別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方針や手順等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、作業者の ID の管理

（ア）情報システム管理者及び個別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。

（イ）情報システム管理者及び個別情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③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

情報システム管理者及び個別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、それ以外のものを利用させてはならない。

④アプリケーション・コンテンツの開発時の対策

情報システム管理者及び個別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。

（３）情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

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

（イ）情報システム管理者及び個別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。

（ウ）情報システム管理者及び個別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。

（エ）情報システム管理者及び個別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

（ア）情報システム管理者及び個別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及び個別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及び個別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及び個別情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（オ）情報システム管理者及び個別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及び個別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及び個別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。

（４）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及び個別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応手順

（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運用時の対策

①情報システム管理者及び個別情報システム管理者は、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運用・保守する場合は、以下の全てのセキュリティ対策を実施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セキュリティを維持するための対策

（イ）脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

②情報システム管理者及び個別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。

（６）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及び個別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。

（ア）情報システム管理者及び個別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及び個別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、以下を全て含む情報システム関連文書を整備しなければならない。

・情報システムを構成するサーバ装置及び端末関連情報

・情報システムを構成する通信回線及び通信回線装置関連情報

（ウ）情報システム管理者及び個別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及び個別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及び個別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。

（７）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及び個別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及び個別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及び個別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。

（８）情報システムの変更管理

情報システム管理者及び個別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。

（９）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及び個別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。

（１０）システム更新又は統合時の検証等

情報システム管理者及び個別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。

（１１）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。

6.4. 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所管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。

（２）情報システム管理者及び個別情報システム管理者の措置事項

情報システム管理者及び個別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及び個別情報システム管理者は、その所管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及び個別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。

6.5. 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、情報システム管理者及び個別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。

（２）攻撃への対処

情報システム管理者及び個別情報システム管理者は、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、都道府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

情報システム管理者及び個別情報システム管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス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

情報システム管理者及び個別情報システム管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（５）職員等による不正アクセス

情報システム管理者及び個別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

情報システム管理者及び個別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

情報システム管理者及び個別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）や内部に侵入した攻撃を早期検知して対処する、侵入は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

情報システム管理者及び個別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）不正プログラム等のセキュリティ情報の収集・周知

情報システム管理者及び個別情報システム管理者は、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

情報システム管理者及び個別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。

7. 運用

7.1. 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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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情報システム管理者及び個別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。

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、統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
②CISO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
統括情報セキュリティ責任者は、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、速やかに情報セキュリティ管理者に報告しなければならない。
②報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
③情報システム管理者は、報告のあった情報セキュリティポリシーに対する違反行為について、必要に応じ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。
④情報セキュリティ責任者は、報告のあった情報セキュリティポリシーに対する違反行為について、必要に応じてCISOに報告しなければならない。
⑤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

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）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

①関係者の連絡先
②発生した事案に係る報告すべき事項
③発生した事案への対応措置
④再発防止措置の策定

（３）緊急時対応計画の見直し

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

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに CISO に報告しなければならない。

（３）例外措置の申請書の管理

CISOは、例外措置の申請書及び審査結果を適正に保管し、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

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令

を遵守し、これに従わなければならない。

①地方公務員法（昭和 25 年法律第 261 号）

②著作権法（昭和 45 年法律第 48 号）

③不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

④個人情報の保護に関する法律（平成 15 年法律第 57 号）

⑤行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）

⑥サイバーセキュリティ基本法（平成 28 年法律第 31 号）

⑦青森市個人情報の保護に関する法律施行条例（令和 5 年条例第 1 号）

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が違反を確認した場合は、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情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止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課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）業務委託実施前の対策

①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)
・委託事業者に重要情報を提供する場合は、秘密保持の規定

（２）業務委託実施期間中の対策

①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、以下を含む対策を実施しなければならない。

（ア）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

（イ）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）

（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

（３）業務委託終了時の対策

①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

8.2. 情報システムに関する業務委託

（１）情報システムの構築を業務委託する場合の対策

情報システム管理者及び個別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

（２）情報システムの運用・保守を業務委託する場合の対策

①情報システム管理者及び個別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情報システム管理者及び個別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。

（３）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。

8.3. 外部サービス（クラウドサービス）の利用（自治体機密性 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実施手順の整備

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、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。）の選定に関する実施手順を整備しなくてはならない。

（２）クラウドサービスの利用に係る実施手順の整備

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、クラウドサービス（自治体機密性２以上の情報を取り扱う場合）の利用に関する実施手順を整備しなければならない。

（３）クラウドサービスの選定

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、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情報セキュリティ責任者は、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情報セキュリティ責任者は、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。

④情報セキュリティ責任者は、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

⑤情報セキュリティ責任者は、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。

⑥情報セキュリティ責任者は、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。

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、クラウドサービスを選定しなくてはならない。また、クラウド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、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、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、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情報セキュリティ責任者は、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情報セキュリティ責任者は、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情報セキュリティ責任者は、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し、クラウドサービス管理者を指名しなければならない。

（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、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。

②クラウドサービス管理者は、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。

③クラウドサービス管理者は、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

④クラウドサービス管理者は、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。

（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、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。

②クラウドサービス管理者は、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クラウドサービス管理者は、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情報システム管理者及び個別情報システム管理者は、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クラウドサービス管理者は、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。

（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、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。

②クラウドサービス管理者は、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。

8.4. 外部サービスの利用（自治体機密性２以上の情報を取り扱わない場合）

（１）クラウドサービスの利用に係る実施手順の整備

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、クラウドサービスの利用に関する実施手順を整備しなければならない。

（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自治体機密性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、承認時に指名されたクラウドサー

ビス管理者は、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情報セキュリティ責任者は、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

統括情報セキュリティ責任者は、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なければならない。

（2）委託事業者に対する監査

事業者に業務委託を行っている場合、統括情報セキュリティ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。

（3）報告

統括情報セキュリティ責任者は、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。

（4）保管

統括情報セキュリティ責任者は、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。

（5）監査結果への対応

①CISO 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。

②CISO 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。

（6）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。

9.2. 自己点検

（1）実施方法

①情報システム管理者及び個別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、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）報告

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

（３）自己点検結果の活用

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

②情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー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。

9.3. 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、改善を行うものとする。

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）			項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	職員等の義務	CSIRT（統一的窓口）
1 組織体制	(1)	①	最高情報セキュリティ責任者の設置		△										
		②	最高情報セキュリティアドバイザーの設置		○										
		③	CSIRTの整備		○										
		④	最高情報セキュリティ副責任者の設置		○	△									
		⑤	ガイドラインに定められた担務の委譲		○	△	△	△	△	△	△		△		
	(2)	①	統括情報セキュリティ責任者の設置		△	△	△								
		②	ネットワークにおける開発等の権限及び責任				○								
		③	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				○								
		④	情報セキュリティ責任者等に対する指導及び助言				○	△	△	△	△	△			
		⑤	情報資産に対するセキュリティ侵害が発生した場合等の権限及び責任		△		○								
		⑥	情報セキュリティ実施手順の維持・管理の権限及び責任				○								
		⑦	CISO及び副CISOにともに事故があるときの職務の代理		△	△	○								
		⑧	最高情報セキュリティ責任者等との連絡体制の整備		△	△	○	△	△	△	△	△			
		⑨	緊急時の報告と回復のための対策		△		○								
		⑩	情報セキュリティ関係規程に係る課題及び問題点の報告		△		○								
	(3)	①	情報セキュリティ責任者の設置					△							
		②	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					○							
		③	部局等の情報システムの開発等の統括的な権限及び責任					○							
		④	部局等の情報システムにおける連絡体制の整備等					○							
	(4)	①	情報セキュリティ管理者の設置						△						
		②	課室等の情報セキュリティ対策に関する権限及び責任						○						
		③	情報資産に対するセキュリティ侵害が発生した場合等の報告等					△	○	△					
	(5)	①	情報システム管理者の設置							△					
		②	情報システム管理者の権限及び責任							○					
		③	情報システム管理者の情報システムにおける開発等の権限及び責任							○					
		④	情報システム管理者の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							○					
		⑤	情報システム管理者の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							○					
	(6)	①	個別情報システム管理者の設置								△				
		②	個別情報システム管理者の権限及び責任								○				
		③	個別情報システム管理者の情報システムにおける開発等の権限及び責任								○				
		④	個別情報システム管理者の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								○				
		⑤	個別情報システム管理者の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								○				
	(7)		情報システム担当者の設置							△	△	△			
	(8)	①	情報セキュリティ委員会の設置	△											
		②	情報セキュリティ委員会の審議事項	○											
		③	情報セキュリティ委員会の構成員		△	△	△	△							
		④	情報セキュリティ委員会の庶務												
	(9)		情報セキュリティ対策の実施における承認等の申請者とその承認者等の兼務の禁止												
	(10)	①	CSIRTの整備		○										
		②	CSIRTに属する職員等の選任		○										
		③	情報セキュリティに関する統一的な窓口の設置		○										△
		④	セキュリティ戦略の意思決定が行われた際に、内容を関係部局等に提供												○
		⑤	情報システムに対するサイバー攻撃等の情報セキュリティインシデントの関係機関への報告		△										○
		⑥	情報システムに対するサイバー攻撃等の情報セキュリティインシデントの報道機関への通知・公表等												○
		⑦	情報セキュリティに関する他の関係機関や窓口等との情報共有												○

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）					項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	職員等の義務	CSIRT（統一的窓口）
2 情報資産の分類と管理		(1)			情報資産の分類												
		(2)	①	(ア)	情報資産の管理責任						○						
				(イ)	情報システム台帳の整備							○	○				
				(ウ)	複製等された情報資産の管理責任						○						
			②		情報資産の分類の表示											○	
			③	(ア)	業務上必要のない情報の作成の禁止											○	
				(イ)	情報作成時の情報の分類と取扱制限の設定											○	
				(ウ)	作成途上の情報の取扱い											○	
			④	(ア)	庁内の者が作成した情報資産の取扱い											○	
				(イ)	庁外の者が作成した情報資産の分類と取扱い											○	
				(ウ)	分類が不明な情報資産を入手した際の対応						△					○	
			⑤	(ア)	情報資産の業務外目的の利用の禁止											○	
				(イ)	情報資産の分類に応じた適正な取扱い											○	
				(ウ)	情報資産の分類が異なる電磁的記録媒体の取扱い											○	
			⑥	(ア)	情報資産の分類に応じた適正な保管						○	○	○				
				(イ)	長期保管する情報資産を記録した電磁的記録媒体の保管						○	○	○				
				(ウ)	利用頻度の低い電磁的記録媒体等の保管						○	○	○				
				(エ)	電磁的記録媒体の施錠可能な場所への保管						○	○	○				
			⑦		電子メール等での送信時の対策											○	
			⑧	(ア)	車両等での情報資産運搬時の対策											○	
				(イ)	情報資産運搬の許可						許					○	
			⑨	(ア)	情報資産の外部への提供時の対策											○	
				(イ)	情報資産の外部への提供の許可						許					○	
				(ウ)	住民に公開する情報資産の取扱い						○						
			⑩	(ア)	情報資産廃棄時やリース返却時等の対策											○	
				(イ)	情報資産廃棄時やリース返却時等の処理の記録											○	
				(ウ)	情報資産廃棄時やリース返却時等の許可						許					○	
3 情報システム全体の強靭性の向上		(1)	①		個人番号利用事務系と他の領域との分離												
			②	(ア)	情報のアクセス対策											○	
				(イ)	情報の持ち出し不可設定											○	
		(2)	①		LGWAN接続系とインターネット接続系の分割												
		(3)	①		高度な情報セキュリティ対策												
			②		自治体情報セキュリティクラウドの導入												
4 物理的セキュリティ	4.1 サーバ等の管理	(1)			サーバ等取付け時の必要な措置							○	○				
		(2)	①		サーバの冗長化							○	○				
			②		システム運用停止時間の最小化							○	○				
		(3)	①		予備電源の設置				△			○	○				
			②		過電流に対する機器の保護措置				△			○	○				
		(4)	①		通信ケーブル等の損傷防止措置							○	○				
			②		通信ケーブル等の損傷等時の対応							○	○				
			③		ネットワーク接続口の管理							○	○				
			④		配線の変更・追加の防止措置							○	○	△			
		(5)	①		機器の定期保守の実施							○	○				
			②		修理時における事業者からの情報漏えい防止措置							○	○				
		(6)			庁外への機器の設置		承		○			○	○				
		(7)			機器の廃棄等の措置							○	○				

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）				項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	職員等の義務	CSIRT（統一的窓口）
	4.2 入退室等管理	(1)		入退室等管理区域												
		(2)		入退室等管理の実施						○						
		(3)		鍵及び入退室管理カードの管理						○						
		(4)	①	入退室等管理簿の作成						○						
			②	鍵及び入退室管理カード管理簿の作成						○						
			③	管理簿への記載事項												
		(5)		入退室等管理に関する指示について		○				△						
		(6)	①	搬入する機器の既存情報システムへの影響確認							○	○			△	
			②	機器等の搬入時の職員の立ち会い							○	○			△	
	4.3 通信回線及び通信回線装置の管理		①	庁内の通信回線等の適正な管理等							○	○				
			②	装置に対しての適切なセキュリティ対策の実施							○	○				
			③	外部へのネットワーク接続の限定措置							○	○				
			④	行政系ネットワークのLGWANへの集約							○	○				
			⑤	通信回線に利用する回線の選択等							○	○				
			⑥	回線の十分なセキュリティ対策の実施							○	○				
			⑦	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の策定							○	○				
			⑧	可用性の高い情報を扱う通信回線の可用性の確保							○	○				
	4.4 職員等が利用する端末機器等の管理		①	職員等が利用する端末機器等の運用管理				○								
			②	端末機器等の盗難防止措置						○						
			③	不正利用防止措置							○					
			④	多要素認証の設定							○					
5 人的セキュリティ	5.1 職員等の遵守事項	(1)	①	情報セキュリティポリシー等の遵守						△					○	
			②	情報資産の業務目的以外での使用の禁止											○	
			③	（ア）情報資産の外部での処理時の安全管理措置		○										
				（イ）モバイル端末や電磁的記録媒体等の持ち出しの許可						許					○	
				（ウ）外部での情報処理業務の許可						許					○	
			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禁止											○	
			⑤	端末等の持出の記録等						○						
			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							許	許			○	
			⑦	机上の端末等の管理						許					○	
			⑧	退職時等の遵守事項											○	
		(2)		会計年度任用職員等の採用時の対応						○					△	
		(3)		情報セキュリティポリシー等の掲示						○					△	
		(4)		委託事業者に対する説明							○	○				
		(5)		指定管理者に対する説明						○						
	5.2 研修・訓練	(1)		情報セキュリティに関する研修・訓練の実施		○										
		(2)	①	研修計画の策定等	承	○										
			②	情報セキュリティ研修の受講											○	
			③	新規採用の職員等に対する研修の実施											○	
			④	理解度等に応じた研修の実施											○	
			⑤	所管する課室等の研修実施状況の記録及び報告				△	△	○						
			⑥	研修実施状況の分析、評価及び報告		△		○								
			⑦	研修の受講状況の報告	△	○										
		(3)		緊急時対応訓練の実施		○										
		(4)		研修・訓練の参加義務											○	

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）					項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	職員等の義務	CSIRT（統一的窓口）
	5.3 情報セキュリティインシデントの報告	(1)	①		情報セキュリティインシデント（サイバー攻撃以外）の報告						△					○	△
			②		報告を受けた情報セキュリティ管理者の報告					△	○	△					
			③		報告を受けた情報システム管理者の報告				△			○					
			④		報告を受けた情報セキュリティ責任者の報告		△			○							
			⑤		個人情報保護委員会への報告												
			⑥		情報セキュリティインシデントの原因の究明、記録の保存、再発防止策の報告		△			○	○						
			⑦		再発防止策の実施に必要な措置の指示		○			△							
		(2)	①		住民等外部からの報告時の対応						△					○	
			②		報告を受けた情報セキュリティ管理者の報告					△	○	△					
			③		報告を受けた情報システム管理者の報告				△			○					
			④		報告を受けた情報セキュリティ責任者の報告		△			○							
			⑤		個人情報保護委員会への報告												
			⑥		情報セキュリティインシデントの原因の究明、記録の保存、再発防止策の報告		△			○	○						
			⑦		再発防止策の実施に必要な措置の指示		○			△							
		(3)	①		情報システムに対するサイバー攻撃等の情報セキュリティインシデントの可能性に対する評価												○
			②		情報システムに対するサイバー攻撃等の情報セキュリティインシデントの報告		△										○
			③		個人情報保護委員会への報告												
			④		応急措置の実施及び復旧に係る指示					△		△	△				○
			⑤		情報システムに対するサイバー攻撃等の情報セキュリティインシデントの原因の究明、記録の保存、再発防止策の報告		△										○
			⑥		再発防止策の実施に必要な措置の指示		○										△
	5.4 ID及びパスワード等の管理	(1)	①	(ア)	認証に用いるICカード等の職員等間共有の禁止											○	
				(イ)	ICカード等のカードリーダ等への常時挿入禁止											○	
				(ウ)	ICカード等紛失時の通報				△			△				○	
			②		ICカード紛失時のアクセス停止措置				○			○					
			③		ICカード切り替え時の旧カードの廃棄方法				○			○					
		(2)	①		自己のIDの他人による利用の禁止											○	
			②		共用ID利用者以外による共用ID利用禁止											○	
		(3)	①		パスワードの管理											○	
			②		パスワードの秘密保持											○	
			③		パスワードの文字及び文字数の選択											○	
			④		パスワードが流出したおそれのある時の措置						△					○	
			⑤		パスワードのシステム間の共有禁止											○	
			⑥		仮パスワードの変更											○	
			⑦		パスワードの記憶機能の利用禁止											○	
			⑧		職員等間でのパスワード共有禁止											○	
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)	①		共有ファイルサーバの容量の設定等							○	○				
			②		共有ファイルサーバの課室等単位での構成							○	○				
			③		特定の情報のためのディレクトリ設定							○	○				
		(2)	①		定期的なバックアップの実施							○	○				
			②		サーバ装置のバックアップ取得							○	○				
			③		装置の設定情報等バックアップ取得及び保管							○	○				
		(3)	①		情報システムの運用に係る作業記録の作成							○	○				
			②		システム変更等時の作業内容の記録作成等							○	○				
			③		システム変更の作業方法									○			
		(4)			情報システム仕様書等の管理							○	○				

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）				項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	職員等の義務	CSIRT（統一的窓口）
		(5)	①	ログの取得等							○					
			②	ログの管理							○					
			③	ログの点検・分析							○					
		(6)		システム障害等の記録、保存							○	○				
		(7)	①	通信ソフトウェア等の設定情報の管理							○	○				
			②	ネットワークのアクセス制御							○	○				
			③	リモートメンテナンスに係る情報セキュリティの確保							○	○				
		(8)		外部の者が利用できるシステムの分離等							○	○				
		(9)	①	ネットワークを外部接続する際の許可				許			○	○				
			②	外部ネットワークの接続による影響の確認							○	○				
			③	外部ネットワーク管理責任者による損害賠償責任の契約上の担保							○	○				
			④	(ア) ファイアウォール等の設置							○	○				
				(イ) ウェブサーバーが備える機能の利用							○	○				
				(ウ) ウェブサーバーからの不用意な情報漏えいを防止するための装置							○	○				
			⑤	問題発生時の物理的な遮断				△			○	○				
		(10)	①	複合機を調達する場合のセキュリティ要件の策定							○	○				
			②	複合機に対するセキュリティ設定と情報セキュリティインシデント対策の実施							○	○				
			③	複合機の運用終了時の対策							○	○				
		(11)	①	IoT機器を含む特定用途機器に対する対策の実施						○						
		(12)	①	無線LAN利用時の暗号化等の使用義務設定							○	○				
			②	機密性の高いネットワークへの暗号化等の措置							○	○				
		(13)	①	電子メールサーバへの中継処理禁止の設定							○	○				
			②	内部からのスパムメール等の送信を検知した際のメールサーバの運用停止							○	○				
			③	電子メールの送受信容量の上限設定等							○	○				
			④	電子メールボックスの容量の上限設定等							○	○				
			⑤	委託事業者の電子メールアドレス利用取り決め							○	○				
		(14)	①	電子メールの自動転送機能の禁止											○	
			②	業務上必要のない送信先への送信禁止											○	
			③	複数人に電子メールを送信する際の方法											○	
			④	重要メールの誤送信時の報告						△					○	
		(15)	①	電子署名、暗号化等による送信											○	
			②	暗号化の方法及び鍵の管理							△				○	
			③	電子署名の正当性を確認する手段の提供							○					
		(16)	①	ソフトウェアの無断導入の禁止											○	
			②	ソフトウェアの導入の許可の取得及びライセンスの管理						○	許	許			○	
			③	不正コピーしたソフトウェアの利用禁止											○	
		(17)	①	機器の改造及び増設・交換の禁止											○	
			②	機器の改造及び増設・交換の許可							許	許			○	
		(18)	①	支給端末の許可されたネットワーク以外への接続禁止							△	△			○	
			②	支給端末への技術的な制限の実施							○	○				
		(19)	①	業務目的以外でのウェブ閲覧の禁止											○	
			②	業務目的以外でのウェブ閲覧発見時の対応				○		△						
		(20)	①	Web会議サービスの利用手順の策定				○								
			②	Web会議サービス利用時の情報セキュリティ対策											○	
			③	Web会議主催時の対策											○	

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）					項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	職員等の義務	CSIRT（統一的窓口）
		(21)	①	（ア）	情報発信におけるなりすまし対策の実施												
				（イ）	認証情報及びこれを記録した媒体の適切な管理												
			②		自治体機密性２以上の情報のソーシャルメディアサービスでの発信禁止												
			③		利用するソーシャルメディアサービスごとの責任者の決定												
			④		アカウント乗っ取り確認時の措置												
			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の措置												
	6.2 アクセス制御	(1)	①		アクセス制御							○	○			△	
			②	（ア）	利用者の情報管理や利用者IDの取扱い等の設定							○	○				
				（イ）	利用されていないIDの点検							○	○				
				（ウ）	不要なアクセス権限付与の確認							○	○				
			③	（ア）	ID及びパスワードの管理							○	○				
				（イ）	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							○	○				
				（ウ）	統括情報セキュリティ責任者等の特権を代行する者の要件		承					○	○				
				（エ）	特権代行者の通知		○		△	△	△	△	△				
				（オ）	特権付与されたID等の変更の委託事業者への委託禁止							○	○				
				（カ）	特権付与されたID等のセキュリティ機能強化							○	○				
				（キ）	特権付与されたIDの初期設定以外のものへの変更							○	○				
		(2)	①		外部から内部ネットワーク等へのアクセスの許可						許					○	
			②		外部からのアクセス可能人数の制限						○						
			③		外部からのアクセス時の本人確認の機能の確保							○					
			④		外部からのアクセス時の通信の暗号化等の措置							○					
			⑤		外部アクセス用端末等付与時のセキュリティの確保						○					△	
			⑥		インターネットを介した庁内ネットワークへの接続禁止				○								
		(3)	①		職員等の認証情報の管理等							○	○				
			②		パスワード発行等							○	○			△	
			③		認証情報の不正利用防止							○	○				
		(4)			特権によるネットワーク等への接続時間の制限							○					
	6.3 システム開発、導入、保守等	(1)	①		調達仕様書への技術的なセキュリティ機能の明記							○	○				
			②		調達時のセキュリティ機能の調査等							○	○				
			③		個別調達の事前協議						○	△					
		(2)	①		システム開発の責任者及び作業者の特定と方針や手順等の確立							○	○				
			②	（ア）	システム開発の責任者等のIDの管理等							○	○				
				（イ）	システム開発の責任者等のアクセス権限の設定							○	○				
			③		システム開発におけるソフトウェア等の特定							○	○				
			④		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							○	○				
		(3)	①	（ア）	システム開発等環境とシステム運用環境の分離							○	○				
				（イ）	システム開発環境からシステム運用環境への移行の手順の明確化							○	○				
				（ウ）	移行に伴うシステム停止等の影響の最小化							○	○				
				（エ）	導入されるシステムやサービスの可用性の確保確認							○	○				
			②	（ア）	新たなシステム導入前の十分な試験の実施							○	○				
				（イ）	運用テスト時の擬似環境による操作確認の実施							○	○				
				（ウ）	テストデータとして個人情報等の使用禁止							○	○				
				（エ）	受け入れ時のテストの実施							○	○				
				（オ）	不具合を考慮したテスト計画の策定							○	○				
			③	（ア）	機器等の搬入時又は情報システムの受入れ時における情報セキュリティ対策に係る要件の確認							○	○				
				（イ）	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おける開発事業者から運用保守事業者へ引継がれる項目							○	○				

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）					項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	職員等の義務	CSIRT（統一的窓口）
		(4)	①		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							○	○				
			②	(ア)	情報セキュリティ水準の維持に関する手順の整備												
				(イ)	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の整備												
		(5)	①	(ア)	ソフトウェアのセキュリティを維持するための対策							○	○				
				(イ)	情報セキュリティインシデントを迅速に検知し対応するための対策							○	○				
			②		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の整備							○	○				
		(6)	①	(ア)	情報システム台帳のセキュリティ要件に係る内容の記録又は記載				△			○	○				
				(イ)	情報システム関連文書の整備							○	○				
				(ウ)	情報セキュリティ対策を実施するために必要となる実施手順の整備							○	○				
			②		テスト結果の保管							○	○				
			③		情報システムに係るソースコードの保管							○	○				
		(7)	①		入力データの正確性を確保できる情報システム設計							○	○				
			②	(ア)	アプリケーション及びウェブコンテンツの提供方式等の見直し							○	○				
				(イ)	定期的な脆弱性対策状況の確認							○	○				
				(ウ)	情報の改ざん等を検出する情報システム設計							○	○				
			③		出力データの正確性を確保できる情報システム設計							○	○				
		(8)			プログラム仕様書等の変更履歴の作成							○	○				
		(9)			ソフトウェア更新等時の他の情報システムとの整合性確認							○	○				
		(10)			システム更新又は統合時の検証等の実施							○	○				
		(11)			推進計画等に基づいた情報システムの情報セキュリティ対策見直し				△			○					
	6.4 不正プログラム対策	(1)	①		不正プログラムのシステムへの侵入防止措置				○								
			②		不正プログラムの外部への拡散防止措置				○								
			③		不正プログラム情報の収集、職員等への注意喚起				○								
			④		不正プログラム対策ソフトウェアの常駐				○								
			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の更新				○								
			⑥		不正プログラム対策ソフトウェアの更新				○								
		(2)	①		不正プログラム対策ソフトウェアの常駐							○	○				
			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の更新							○	○				
			③		不正プログラム対策ソフトウェアの更新							○	○				
			④		インターネットに接続していないシステムにおける電磁的記録媒体の制限及び不正プログラム対策ソフトウェアの導入等							○	○				
			⑤		不正プログラム対策ソフトウェア等の設定変更権限の一括管理							○	○			△	
		(3)	①		不正プログラム対策ソフトウェアの設定変更の禁止											○	
			②		外部からのデータ又はソフトウェア取込時のウイルスチェックの実施											○	
			③		差出人が不明等の添付ファイルの削除											○	
			④		不正プログラム対策ソフトウェアによる定期的なフルチェックの実施											○	
			⑤		添付ファイル送受信時のウイルスチェック、無害化処理の実施											○	
			⑥		パソコン等の端末のウイルス感染時の対処方法											○	

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）				項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	職員等の義務	CSIRT（統一的窓口）
	6.5 不正アクセス対策	(1)	①	使用されていないポートの閉鎖				○								
			②	不要なサービス機能の削除、停止				○								
			③	ウェブページの改ざんを防止するための設定				○			△	△				
			④	監視、通知、外部連絡窓口などの体制及び連絡窓口の構築				○								○
		(2)		攻撃を受けた場合、または受けるリスクがある場合への対応							○	○				
		(3)		攻撃を受けた記録の保存							○	○				
		(4)		内部からの攻撃等の監視							○	○				
		(5)		職員等による不正アクセス発見時の対応						△	○	○				
		(6)		サービス不能攻撃対策の実施							○	○				
		(7)		標的型攻撃対策の実施							○	○				
	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							○	○				
		(2)		不正プログラム等のセキュリティ情報の収集・周知							○	○				
		(3)		情報セキュリティに関する技術情報の収集及び共有							○	○				
7 運用	7.1 情報システムの監視	(1)	①	セキュリティ機能の適切な運用							○	○				
			②	情報システムの情報セキュリティ対策における新たな脅威の出現、運用、監視等の状況による見直し							○	○				
			③	危機的事象発生時の適切な対処							○	○				
		(2)	①	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、監視機能の実装							○	○				
			②	情報システムに実装された監視機能の適切な運用							○	○				
			③	情報システムにおける監視の対象や手法の定期的な見直し							○	○				
			④	サーバ装置を監視するための措置							○	○				
		(3)	①	情報システムの監視							○	○				
			②	サーバの正確な時刻設定等の措置およびクラウドサービスの時刻同期の確認							○	○				
			③	外部と常時接続するシステムの監視							○	○				
	7.2 情報セキュリティポリシーの遵守状況の確認	(1)	①	情報セキュリティポリシーの遵守状況の確認等		△		△	△	○	△					
			②	問題発生時の対処		○										
			③	システム設定等における情報セキュリティポリシー遵守状況の定期的な確認等				○								
		(2)		モバイル端末及び電磁的記録媒体等の利用状況調査				○								
		(3)	①	違反行為の発見時の報告						△					○	
			②	報告を受けた情報セキュリティ管理者の報告					△	○	△					
			③	報告を受けた情報システム管理者の報告				△			○					
			④	報告を受けた情報セキュリティ責任者の報告		△			○							
			⑤	緊急時対応計画に従った対応				○							○	
	7.3 侵害時の対応等	(1)		緊急時対応計画の策定		○										
		(2)		緊急時対応計画に盛り込むべき内容												
		(3)		緊急時対応計画の見直し		○										
	7.4 例外措置	(1)		例外措置の許可		許				○	○					
		(2)		緊急時の例外措置		△				○	○					
		(3)		例外措置の申請書の管理		○										
	7.5 法令遵守			主要な法令遵守											○	
	7.6 懲戒処分等	(1)		懲戒処分				○	○	○	○	○	○	○	○	
		(2)	①	違反時の対応(統括情報セキュリティ責任者確認時)				○		△						
			②	違反時の対応(情報システム管理者確認時)				△		△	○					
			③	違反を改善しない職員等のシステム使用の権利の停止等		△		○		△					△	

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）					項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ監査統括責任者	職員等の義務	CSIRT（統一的窓口）
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)	①	（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）						○	○					
		(2)	①	（ア）	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						○	○					
				（イ）	統括情報セキュリティ責任者へ措置内容の報告		△		△		○	○					
				（ウ）	契約に基づく対処の要求						○	○				△	
			②	（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）	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						○	○					
				（ウ）	委託事業の一時中断などの必要な措置を含む対処						○	○					
		(3)	①	（ア）	セキュリティ対策が適切に実施されたことの確認						○	○					
				（イ）	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	（ア）	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）	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)	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							○	○				
		(2)	①		契約に基づいた委託事業者への実施要求							○	○				
			②		情報システムの変更内容における速やかな報告の要求							○	○				
		(3)	①		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の追加						○	○					
			②		業務委託サービスの選定						○	○					
			③		委託事業者の信頼性が十分であることを総合的・客観的に評価した判断						○	○					
	8.3 外部サービス（クラウドサービス）の利用（自治体機密性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実施手順の整備				○								
		(2)			クラウドサービスの利用に係る実施手順の整備				○								
		(3)	①		クラウドサービスの利用の検討					○							
			②	（ア）	クラウドサービスで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る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に関する情報提供及び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		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					○							
			④	（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					○							
			⑤		クラウドサービスの利用を通じて取り扱う情報に対する国内法以外の法令及び規制が適用されるリスクの評価					○							
			⑥		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の対策					○							
			⑦		取り扱う情報の格付及び取扱制限に応じたセキュリティ要件とクラウドサービスの選定					○							
			⑧		クラウドサービスの特性を考慮したセキュリティ要件					○							
			⑨		情報セキュリティ監査報告書によるクラウドサービス提供者の評価				○								
		(4)	①		クラウドサービスの調達時の調達仕様に含める事項					○							
			②		クラウドサービスを調達する場合の契約までの確認事項と契約内容					○							
		(5)	①		クラウドサービスを利用する場合の利用申請					○							
			②		職員等によるクラウドサービスの利用申請の審査											△	
			③		クラウドサービスの利用承認時の記録とクラウドサービス管理者の指名												

【資料】権限・責任等一覧表

※記号：「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区　分（対策基準の規定箇所）					項　目	情報セキュリティ委員会	最高情報セキュリティ責任者（CISO）	最高情報セキュリティ副責任者（副CISO）	統括情報セキュリティ責任者	情報セキュリティ責任者	情報セキュリティ管理者	情報システム管理者	個別情報システム管理者	情報システム担当者	情報セキュリティ統括責任者　監査	職員等の義務	CSIRT（統一的窓口）
		(6)	①		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				○							
			②		情報システム台帳及び関連文書への記録											
			③	(ア)	情報セキュリティ水準の維持に関する手順											
				(イ)	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											
			④		規程内容の確認・記録											
		(7)	①		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				○							
			②		情報システム台帳及び関連文書の更新又は修正				△							
			③		新たな脅威の出現、運用、監視等の状況による見直し											
			④		クラウドサービスで発生したインシデントの対処手順の整備							○	○			
			⑤		クラウドサービス運用・保守時の確認・記録											
		(8)	①		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				○							
			②		クラウドサービス利用終了時の確認・記録											
	8.4 外部サービスの利用（自治体機密性２以上の情報を取り扱わない場合）	(1)			クラウドサービスの利用に係る実施手順の整備				○							
		(2)	①		自治体機密性２以上の情報を取り扱わない場合の利用申請と措置											○	
			②		クラウドサービスの利用申請審査とその記録					○						△	
9 評価・見直し	9.1 監査	(1)			情報セキュリティ対策状況について監査の実施				○								
		(2)			委託事業者に対する監査				○								
		(3)			監査結果の報告	△			○								
		(4)			監査証拠等の保管				○								
		(5)	①		監査結果への対処（改善計画の策定等）の指示		○				△						
			②		庁内で横断的に改善が必要な事項の指示		○		△		△						
		(6)			監査結果の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	○											
	9.2 自己点検	(1)	①		ネットワーク等の自己点検の実施							○	○				
			②		情報セキュリティ対策状況の自己点検					○	○						
		(2)			点検結果と改善策の報告	△			○	○		○					
		(3)	①		自己の権限の範囲内での改善											○	
			②		点検結果の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	○											
	9.3　情報セキュリティポリシー及び関係規程等の見直し				情報セキュリティポリシー及び関係規程等の見直しに関する規定	○											