

## 新温泉町情報セキュリティ対策指針

新温泉町情報セキュリティ対策指針（令和4年3月28日訓令第1号）の全部を改正する。

### 目次

- 第1章 情報セキュリティ基本方針（第1条—第9条）
- 第2章 情報セキュリティ対策組織等
  - 第1節 組織と責務（第10条—第14条）
  - 第2節 情報セキュリティ対策委員会（第15条—第22条）
- 第3章 情報セキュリティ対策基準
  - 第1節 情報資産の分類と管理（第23条—第25条）
  - 第2節 物理的セキュリティ対策（第26条—第29条）
  - 第3節 人的セキュリティ対策（第30条—第33条）
  - 第4節 技術的セキュリティ対策（第34条—第39条）
  - 第5節 運用面の対策（第40条—第56条）

### 附則

#### 第1章 情報セキュリティ基本方針

##### （目的）

第1条 この指針は、新温泉町（以下「町」という。）の情報資産を適正に保持するために必要な情報セキュリティ対策の基本方針及び具体的な対策を講ずるに当たっての基準を定めるものとする。

##### （定義）

第2条 この指針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- （1） 情報資産 情報システムの開発、運用、利用等に係る全ての電磁的に記録されたデータ、機器、文書等をいう。
- （2） 情報セキュリティ対策 情報資産の機密性（権限のない者への情報資産の提供を防止することをいう。）、完全性（情報資産の改ざん、破壊等による被害を防止することをいう。）及び可用性（権限のある者にいつでも情報資産の利用を可能にすることをいう。）を維持することをいう。
- （3） 情報システム コンピュータ、通信機器、通信回線及び記録媒体で構成され、業務に関する情報処理を行う仕組みをいう。
- （4） 不正アクセス 情報システムを利用する権限のない者が不正な手段でこれを利用することをいう。
- （5） コンピュータウイルス 情報システムの正常な動作を意図的に妨げるプログラムをいう。
- （6） バックアップ データの滅失及び毀損に備えた複製をいう。
- （7） ID 情報システムの利用者を識別するための記号をいう。

- (8) パスワード 情報システムの利用者であることを確認するために使用される記号をいう。
- (9) IDカード システム室の利用者を識別するための磁気カード又は新温泉町役場入退館用ICカード等をいう。
- (10) 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。
- (11) サーバ 情報システムを構成する機器のうち、特定のサービスを提供するコンピュータをいう。
- (12) ファイアウォール 組織内の情報通信機器及び端末に外部からの侵入を防ぐ目的で設置してあるセキュリティシステムをいう。
- (13) 基幹系 個人番号利用事務（社会保障、地方税又は防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。
- (14) 情報系 人事給与、財務会計及び文書管理等総合行政ネットワーク（以下「L-GWAN」という。）に接続された情報システム及びその情報システムで取り扱うデータをいう。
- (15) インターネット系 インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。
- (16) 通信経路の分割 情報系とインターネット系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。
- (17) 無害化通信 インターネットメール本文のテキスト化及び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ない等、安全が確保された通信をいう。

（情報資産への脅威）

第3条 情報セキュリティ対策は、町が保有する情報資産を次に掲げる脅威からの確かつ効率的に保護することを目的とする。

- (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又は部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的的要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害並びに事故、故障等による情報システムの損傷、中断及び停止
- (4) 大規模又は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

(対象範囲)

第4条 この指針は、町の各機関が構築し、及び運用する全ての情報資産と情報システムを対象とする。

2 前項の機関の範囲は、町長、教育委員会、議会、選挙管理委員会、監査委員、農業委員会及び固定資産評価審査委員会とする。

3 この指針は、前項の機関の全ての職員、非常勤職員、及び会計年度任用職員等（以下「職員等」という。）に適用する。

4 この基本方針が対象とする情報資産は、次のとおりとする。

(1) ネットワーク、情報システム並びにこれらに関する設備及び電磁的記録媒体

(2) ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

(3) 情報システムの仕様書、ネットワーク図等のシステム関連文書  
(職員等の遵守義務)

第5条 職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たってこの指針及び第9条の新温泉町情報セキュリティ実施手順を遵守しなければならない。

(情報セキュリティ対策)

第6条 第3条に規定する脅威から情報資産を保護するために、次に掲げる対策を講ずるものとする。

(1) 組織体制として、町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として、町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靱性の向上として、情報システム全体に対し、次の3段階の対策を講じる。

ア 基幹系においては、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及び端末の多要素認証の導入等により、住民情報の流出を防ぐ。

イ 情報系においては、LGWANと接続する業務用システムと、インターネット系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。

ウ インターネット系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ対策として、情報システムを構成する機器並びにこれらの附属機器及び設備を設置する施設の入退室管理等情報システムの設置に伴う

安全性を確保するために必要な対策を講ずる。

- (5) 人的セキュリティ対策として、職員等が遵守すべき事項を定めるとともに、情報セキュリティ対策に関する研修、啓発等の必要な対策を講ずる。
- (6) 技術的セキュリティ対策として、情報システムへの不正アクセスの防止、コンピュータウイルス対策、情報システムにおけるアクセス制御等の情報システムの開発及び運用における技術的信頼性を確保するために必要な対策を講ずる。
- (7) 運用面の対策として、情報システムの監視、この指針の遵守状況の確認、緊急事態に対応した危機管理、業務委託を行う際のセキュリティ確保等により情報システムの運用面における信頼性を確保し、この指針を効果的に運用するために必要な対策を講ずる。
- (8) 業務委託と外部サービス（クラウドサービス）の利用として、次の安全対策を講じる。
  - ア 業務委託する場合には、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書を締結し、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。
  - イ 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。
  - ウ 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を定める。
- (9) 評価及び見直しとして、この指針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主点検を実施し、運用改善を行い情報セキュリティの向上を図るとともに、この指針の見直しが必要な場合は、見直しを行う。

(情報セキュリティ監査及び自己点検の実施)

第7条 この指針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。

(情報セキュリティ対策指針の見直し)

第8条 情報セキュリティ監査及び自己点検の結果、この指針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、リスクを検討した上で、この指針を見直す。

(情報セキュリティ実施手順の策定)

第9条 第3章に規定する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新温泉町情報セキュリティ実施手順を策定するものとする。

2 前項の新温泉町情報セキュリティ実施手順は、公にすることにより町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 情報セキュリティ対策組織等

### 第1節 組織と責務

(最高情報セキュリティ責任者)

第10条 この指針に基づき、全庁的な情報セキュリティ対策を統括する責任者として、最高情報セキュリティ責任者（Chief Information Security Officer。以下「CISO」という。）を置く。

2 CISOには、副町長をもって充てる。

3 CISOは、町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。

4 CISOは、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

5 CISOは、情報セキュリティインシデント（以下「事故等」という。）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。

(統括情報セキュリティ責任者)

第11条 この指針に基づき、CISOを補佐するためCISO直属の統括情報セキュリティ責任者を置く。

2 統括情報セキュリティ責任者には、企画課長をもって充てる。

3 統括情報セキュリティ責任者は、町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。

4 統括情報セキュリティ責任者は、町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。

5 統括情報セキュリティ責任者は、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

6 統括情報セキュリティ責任者は、町の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

7 統括情報セキュリティ責任者は、町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新温泉町情報セキュリティ実施手順の維持及び管理を行う権限及び責任を有する。

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、統括情報セキュリティ責任者、次条第1項に規定する情報セキュリティ管理者、第13条第1項に規定する情報システム管理者及び第14条第1項に規定する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C I S O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。

(情報セキュリティ管理者)

第12条 この指針に基づき、各課室等の情報セキュリティ対策を統括する管理者として、情報セキュリティ管理者を置く。

- 2 情報セキュリティ管理者には、各課室等の長をもって充てる。
- 3 情報セキュリティ管理者は、当該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。
- 4 情報セキュリティ管理者は、この指針及び新温泉町情報セキュリティ実施手順の遵守状況を適宜点検し、これらの実効性が保たれるよう必要な措置を講ずるものとする。
- 5 情報セキュリティ管理者は、その所掌する課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、統括情報セキュリティ責任者及びC I S O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13条 この指針に基づき、情報システムの適正な運用を図るために、各情報システムの運用管理者として、情報システム管理者を置く。

- 2 情報システム管理者には、その所管する業務等において所有している情報システムの業務主管課長をもって充てる。ただし、当該情報システムにおいて他の業務管理者が定められている場合はこの限りでない。
- 3 情報システム管理者は、その所管する業務等において所有している情報システム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。
- 4 情報システム管理者は、その所管する業務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、見直し等を行う権限及び責任を有する。
- 5 情報システム管理者は、その所管する業務等において所有している情報システムに係る実施手順の維持・管理を行う。
- 6 情報システム管理者は、この指針及び新温泉町情報セキュリティ実施手順が遵守されるよう必要な措置を講じなければならない。

(情報システム担当者)

第14条 この指針に基づき、各情報システムの適正な利用を確保するため、情報システム担当者を置く。

- 2 情報システム担当者には、各業務の担当係長をもって充てる。
- 3 情報システム担当者は、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。

## 第2節 情報セキュリティ対策委員会

(情報セキュリティ対策委員会)

第15条 情報セキュリティ対策を円滑に推進するため、新温泉町情報セキュリティ対策委員会（以下「委員会」という。）を置く。

2 委員会の委員は、C I S O、統括情報セキュリティ責任者、温泉総合支所長、総務課長、税務課長、町民安全課長、健康課長、福祉課長及びこども教育課長をもって充てる。

(所掌事務)

第16条 委員会は、次に掲げる事項について審議する。

- (1) 対策指針の運用に関する事項
- (2) 対策指針の評価及び見直しに関する事項
- (3) 情報セキュリティ対策の確保及び普及啓発に関する事項
- (4) 情報セキュリティ対策の改善計画の策定及び実施状況の確認
- (5) その他情報セキュリティ対策に関する事項

(委員長及び副委員長)

第17条 委員会に委員長及び副委員長を置く。

- 2 委員長には、C I S Oをもって充てる。
- 3 委員長は、会務を総括し、委員会を代表する。
- 4 副委員長には、統括情報セキュリティ責任者をもって充てる。
- 5 副委員長は、委員長を補佐し、委員長に事故あるとき、又は委員長が欠けたときは、その職務を代理する。

(会議)

第18条 委員会の会議は、委員長が必要に応じて招集し、委員長が議長となる。

- 2 委員会の会議は、構成員の半数以上の出席で成立する。
- 3 委員会は、必要と認めるときは委員以外の者を委員会に出席させ、事案について意見又は説明を聴くことができる。
- 4 委員会の議事は出席委員の過半数で決し、可否同数のときは、委員長の決するところによる。

(庶務)

第19条 委員会の庶務は、企画課において行う。

(兼務の禁止)

第20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その承認者又は許可者は、同じ者が兼務してはならない。

- 2 監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

(C S I R Tの設置及び役割)

第21条 C I S Oは、事故等に対応するためにC S I R Tを設置する。

- 2 C I S Oは、C S I R Tに所属する職員を選任し、その中からC S I R T責任者

を置き、CSIRT内の業務統括及び外部との連携を行う職員を定める。

- 3 CSIRT責任者には企画課長をもって充てる。
- 4 CISOは、情報セキュリティの統一的な窓口を整備し、事故等について担当課等から報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。
- 5 統一的な窓口は、企画課をもって充てる。
- 6 CSIRT責任者は、CISOによる情報セキュリティ対策の意思決定が行われた際には、その内容を関係課等に提供する。
- 7 CSIRT責任者は、事故等を認知した場合には、CISO、総務省、兵庫県等へ報告する。
- 8 CSIRT責任者は、事故等を認知した場合には、その重要度及び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。
- 9 CSIRT責任者は、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

(クラウドサービス利用における組織体制)

第22条 統括情報セキュリティ責任者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

### 第3章 情報セキュリティ対策基準

#### 第1節 情報資産の分類と管理

(情報資産の分類)

第23条 町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。

(1) 機密性による情報資産は、次の表のとおり分類する。

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	ア 支給以外の端末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。) イ 必要以上の複製及び配付禁止
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及び性質上、取扱いに非常に留意すべき情報資産	ウ 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込禁止 エ 情報の送信並びに情報資産の運搬及び提供時における暗

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、業務の規模及び性質上、取扱いに留意すべき情報資産	号化・パスワード設定又は鍵付きケースへの格納 オ 復元不可能な処理を施しての廃棄 カ 信頼のできるネットワーク回線の選択
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、業務の規模及び性質上、取扱いに留意すべき情報資産	キ 外部で情報処理を行う際の安全管理措置の規定 ク 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	—

(2) 完全性による情報資産は、次の表のとおり分類する。

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、誤り又は破損により、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	ア バックアップ、電子署名付与 イ 外部で情報処理を行う際の安全管理措置の規定 ウ 電磁的記録媒体の施錠可能な場所への保管
自治体 完全性1	自治体完全性2の情報資産以外の情報資産	—

(3) 可用性による情報資産は、次の表のとおり分類する。

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	ア バックアップ、指定する時間以内の復旧 イ 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	—

(情報資産の管理)

第24条 情報資産の管理は、次の各号に掲げる事項を遵守しなければならない。

(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前条の分類に基づき管理しなければならない。

ウ 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。

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

#### (2) 情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル及び文書の隅等に、必要に応じて情報資産の分類を表示し、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、情報の作成時に前条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ 情報を作成する者は、作成途上の情報についても、紛失、流出等を防止しなければならない。

エ 情報を作成する者は、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、前条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

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には、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、前条の分類に基づき、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には、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又は情報システム管理者は、前条の分類に基づき、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又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

ウ 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。

エ 情報セキュリティ管理者又は情報システム管理者は、自治体機密性2以上、自治体完全性2又は自治体可用性2の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施設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) 情報資産の提供及び公表

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、必要に応じ暗号化又はパスワードの設定を行わなければならない。

イ 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) 情報資産の廃棄等

ア 情報資産を廃棄又はリース返却等する者は、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た上で廃棄しなければならない。

イ 情報資産の廃棄又は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 情報資産の廃棄又は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。

エ クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

(情報システム全体の強靱性の向上)

第25条 情報システムの強靱化を向上させるため、システムの構成とセキュリティ対策を講じなければならない。

(1) 基幹系

ア 基幹系と他の領域との分離

基幹系と他の領域を通信できないようにしなければならない。ただし、基幹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アドレス及び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）のレベルで限定を行わなければならない。また、外部接続先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、L2/L3を経由して、インターネット等と基幹系との双方向通信でのデータの移送を可能とする。

イ 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として、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、2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、業務ごとに専用端末を置くことが望ましい。

(イ) 情報の持ち出し対策として、原則として、USBメモリー等の電磁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。

ウ 基幹系と接続されるクラウドサービス上での情報システムの扱い

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

エ 基幹系と接続されるクラウドサービス上での情報資産の取扱い

基幹系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度5を持たなければならない。

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

(2) 情報系

ア 情報系とインターネット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、メール又はデータを情報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情報系に転送するメールテキスト化方式

(イ) インターネット系端末から情報系の端末へ画面転送する方式

(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、インターネット系から取り込む方式

イ LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

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

(3) インターネット系

ア インターネット系においては、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、事故等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。

イ 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、関係省庁及び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。

## 第2節 物理的セキュリティ対策

(サーバ等の管理)

第26条 情報システム管理者は、情報システムの機器の設置について、次に掲げる措置を講じなければならない。

(1) 機器の取付け

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、ほこり、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

ア 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必要に応じて冗長化し、同一データを保持しなければならない。

イ 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、必要に応じて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

ア 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。

イ 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

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

イ 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、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。

ウ 統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

エ 統括情報セキュリティ責任者及び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又は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

ア 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。

イ 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外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、事業者に故障を修理させるに当たり、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などを行わなければならない。

#### (6) 庁外への機器の設置

ア 統括情報セキュリティ責任者及び情報システム管理者は、庁外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。

イ 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、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

ア 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。

イ クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。なお、当該確認に当たっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書又は

認証等を取得している場合には、その監査報告書又は認証等を利用できる。

(管理区域 (情報システム室等) の管理)

第27条 統括情報セキュリティ責任者は、重要な情報システムの設置、運用及び管理を行うための施設を設置する場合は、次に掲げる対策を講じなければならない。

(1) 管理区域の構造等

ア 統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域 (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「電算機室」という。) 並びに電磁的記録媒体の保管庫をいう。以下同じ。) から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

イ 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、電算機室内の機器等に、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。

ウ 統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消火薬剤又は消防用設備等が、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。

エ 統括情報セキュリティ責任者及び情報システム管理者は、管理区域を地階又は1階に設けてはならない。

オ 統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。

(2) 管理区域の入退室管理等

ア 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、IDカードによる入退室管理を行わなければならない。

イ 職員等及び委託事業者は、管理区域に入室する場合には、身分証明書等を携帯し、求めにより提示しなければならない。

ウ 情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立入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。

エ 情報システム管理者は、自治体機密性2以上の情報資産を扱う情報システムを設置している管理区域について、当該情報システムに関連しない、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。

(3) 機器等の搬入出

ア 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、あらかじめ職員等又は委託した業者に確認を行わせなければならない。

イ 情報システム管理者は、電算機室の機器等の搬入出について、職員等を立ち

会わせなければならない。

(通信回線及び通信回線装置の管理)

第28条 統括情報セキュリティ責任者は、通信回線及び通信回線装置の管理を行うために、次に掲げる対策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て、適正に管理し、並びに通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。
- (2) 統括情報セキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。
- (3) 統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。
- (4) 統括情報セキュリティ責任者は、行政事務に使用するネットワークをL GW A Nに集約するように努めなければならない。
- (5) 統括情報セキュリティ責任者は、自治体機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択するとともに、必要に応じ、送受信される情報の暗号化を行わなければならない。
- (6) 統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。
- (7) 統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。
- (8) 統括情報セキュリティ責任者は、自治体可用性2の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択するとともに、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。

(職員等の利用する端末又は電磁的記録媒体等の管理)

第29条 統括情報セキュリティ責任者は、職員等のパソコン等の管理を行うために、次に掲げる対策を講じなければならない。

- (1) 情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワ イ ヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じるとともに、電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
- (2) 情報システム管理者は、情報システムへのログインに際し、パスワード、スマートカード、生体認証等の複数の認証情報入力を必要とするように設定しなければならない。

- (3) 情報システム管理者は、原則として、端末の電源起動時のパスワード（BIOSパスワード、ハードディスクパスワード等）を併用しなければならない。
- (4) 情報システム管理者は、基幹系では「知識」、「所持」及び「存在」を利用する認証手段のうち2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) 情報システム管理者は、原則として、パソコン及びモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。
- (6) 情報システム管理者は、モバイル端末の庁外での業務利用の際は、前2号の対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

### 第3節 人的セキュリティ対策

#### (職員等の遵守事項)

第30条 職員等は、次の各号に掲げる事項を遵守しなければならない。

#### (1) 職員等の遵守事項

##### ア この指針等の遵守

(ア) 職員等は、この指針及び新温泉町情報セキュリティ実施手順を遵守しなければならない。

(イ) 職員等は、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。

##### イ 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。

##### ウ モバイル端末、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及び自治体完全性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、町のモバイル端末、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。

(エ) 職員等は、外部で情報処理作業を行う際、情報セキュリティ管理者の許可を得た上で、安全管理措置に関する規定を遵守しなければならない。

エ 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ア) 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断を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、情報セキュリティ管理者の許可を得て利用することができる。

(イ) 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

オ 持ち出し及び持込みの記録

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

カ パソコン及び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、パソコン及びモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

キ 机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン及びモバイル端末のロック、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。

ク 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、その後も業務上知り得た情報を漏らしてはならない。

ケ クラウドサービス利用時等の遵守事項

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

(2) 非常勤及び会計年度任用職員への対応

ア この指針等の遵守

情報セキュリティ管理者は、非常勤及び会計年度任用職員に対し、採用時にこの指針等のうち、非常勤及び会計年度任用職員が守るべき内容を理解させ、並びに実施及び遵守させなければならない。

イ この指針等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び会計年度任用職員の採用の際、必要に応じ、この指針等を遵守する旨の同意書への署名を求めるものとする。

ウ インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び会計年度任用職員にパソコン及びモバ

イル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(3) この指針等の掲示

情報セキュリティ管理者は、職員等が常にこの指針及び新温泉町情報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。

(4) 外部委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発並びに保守等を事業者が発注する場合、再委託事業者も含めて、この指針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。

(研修及び訓練)

第31条 C I S Oは、次の各号に掲げる事項を実施しなければならない。

(1) 情報セキュリティに関する研修及び訓練

ア C I S Oは、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。

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

(2) 研修計画の策定及び実施

ア 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及びその実施体制の構築を定期的に行い、委員会の承認を得なければならない。

イ C I S Oは、研修計画において、職員等が毎年度最低1回は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。

ウ C I S Oは、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。

エ 研修は、統括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。

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

カ 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。

キ C I S Oは、毎年度1回、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

- ア C I S Oは、緊急時対応を想定した訓練を定期的実施しなければならない。
- イ 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。

(4) 研修及び訓練への参加

幹部を含めた全ての職員等は、定められた研修及び訓練に参加しなければならない。

(事故等の報告)

第32条 事故等の対応について、次の各号に掲げる事項を遵守しなければならない。

(1) 庁内での事故等の報告

- ア 職員等は、事故等を認知した場合には、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へ報告しなければならない。
- イ 報告を受けた情報セキュリティ管理者は、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報告しなければならない。
- ウ 情報セキュリティ管理者は、報告のあった事故等について、C I S Oに報告しなければならない。
- エ 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。
- オ 情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

(2) 住民等外部からの事故等の報告

- ア 職員等は、町が管理するネットワーク、情報システム等の情報資産に関する事故等について、住民等外部から報告を受けた場合には、情報セキュリティ管理者に報告しなければならない。
- イ 報告を受けた情報セキュリティ管理者は、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報告しなければならない。
- ウ 情報セキュリティ管理者は、当該事故等について、必要に応じてC I S O及び統括情報セキュリティ責任者に報告しなければならない。
- エ C I S Oは、情報システム等の情報資産に関する事故等について、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。
- オ 報告を受けるための窓口は、企画課をもって充てる。
- カ 統括情報セキュリティ責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告及び情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

(3) 事故等の原因の究明・記録、再発防止等

- ア C S I R Tは、報告された事故等の可能性について状況を確認し、事故等であるかの評価を行わなければならない。
- イ C S I R Tは、事故等であると評価した場合、C I S Oに速やかに報告しな

なければならない。

ウ CSIRTは、事故等に関係する情報セキュリティ管理者及び情報システム管理者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。また、CSIRTは、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。

エ CSIRTは、これらの事故等の原因を究明し、記録を保存しなければならない。

オ CSIRTは、事故等の原因究明結果から、再発防止策を検討し、CISOに報告しなければならない。

カ CISOは、CSIRTから、事故等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。

(ID及びパスワード等の管理)

第33条 職員等は、次の各号に掲げる事項を遵守しなければならない。

(1) ICカード等の取扱い

ア 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ー、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。

(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。

イ 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。

ウ 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。

ア 自己が利用しているIDは、他者に利用させてはならない。

イ 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。

ア 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。

イ 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。

ウ パスワードは、十分な長さとし、文字列は想像しにくいものにしなければならない。

エ 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。

オ 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。

カ 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。

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

ク 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。

#### 第4節 技術的セキュリティ対策

（コンピュータ及びネットワークの管理）

第34条 情報システム管理者は、次に掲げる対策を講じなければならない。

##### （1）文書サーバの設定等

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

イ 情報システム管理者は、文書サーバを課室等の単位で構成し、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

ウ 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、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

##### （2）バックアップの実施

ア 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、業務システムのデータベース及び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。

イ 統括情報セキュリティ責任者及び情報システム管理者は、重要な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。

ウ 統括情報セキュリティ責任者及び情報システム管理者は、重要な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。

エ 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、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバック

アップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が本町の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合又はバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

(3) 他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者及び情報セキュリティ管理者の許可を得なければならない。

(4) システム管理記録及び作業の確認

ア 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。

イ 統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、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又は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。

ウ 統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、2名以上で作業し、互いにその作業を確認しなければならない。

(5) 情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者による閲覧、紛失等がないよう、適正に管理しなければならない。

(6) ログの取得等

ア 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、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。

イ 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、ログとしての取得項目、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。

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

なければならない。

エ 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、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

#### (7) 障害記録

統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

#### (8) ネットワークの接続制御、経路制御等

ア 統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

イ 統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

ウ 統括情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により見直さなければならない。

#### (9) 外部の者が利用できるシステムの分離等

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

#### (10) 外部ネットワークとの接続制限等

ア 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、C I S O及び統括情報セキュリティ責任者の許可を得なければならない。

イ 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。

ウ 情報システム管理者は、接続した外部ネットワーク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。

エ 統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。

ない。

(ア) 庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

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

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

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

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

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

#### (11) 複合機のセキュリティ管理

ア 統括情報セキュリティ責任者は、複合機を調達する場合には、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。

イ 統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する事故等への対策を講じなければならない。

ウ 統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

#### (12) I o T機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

#### (13) 無線LAN及びネットワークの盗聴対策

ア 統括情報セキュリティ責任者は、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。

イ 統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

#### (14) 電子メールのセキュリティ管理

ア 統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよ

う、電子メールサーバの設定を行わなければならない。

イ 統括情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

ウ 統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

エ 統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

オ 統括情報セキュリティ責任者は、システムの開発、運用、保守等のため、外部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。

カ 統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上の措置を講じなければならない。

#### (15) 電子メールの利用制限

ア 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。

イ 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。

ウ 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。

エ 職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

#### (16) 電子署名及び暗号化

ア 職員等は、第23条の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、暗号化、パスワード設定等のセキュリティを考慮して、送信しなければならない。

イ 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。

ウ 職員等は、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。

エ 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。

#### (17) 無許可ソフトウェアの導入等の禁止

ア 職員等は、パソコン及び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。

イ 職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。この場合において、情報セキュリティ管理者又は情報システム管理者は、当該ソフ

トウェアのライセンスを管理しなければならない。

ウ 職員等は、不正にコピーしたソフトウェアを利用してはならない。

(18) 機器構成の変更の制限

ア 職員等は、パソコン及びモバイル端末に対し機器の改造並びに増設及び交換を行ってはならない。

イ 職員等は、業務上、パソコン及びモバイル端末に対し機器の改造並びに増設及び交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

(19) 業務外ネットワーク接続の禁止

ア 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。

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

(20) 業務以外の目的でのウェブ閲覧の禁止

ア 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。

イ 統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

(21) Web 会議サービスの利用時の対策

ア 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。

イ 職員等は、本町の定める利用手順に従い、Web 会議の参加者及び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。

ウ 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。

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

(アクセス制御)

第35条 統括情報セキュリティ責任者又は情報システム管理者は、次に掲げる対策を講じなければならない。

(1) アクセス制御等

ア アクセス制御

統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上の制限をしなければならない。

## イ 利用者 I D の取扱い

- (ア) 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、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向又は退職に伴う利用者 I D の取扱い等の方法を定めなければならない。
- (イ) 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。
- (ウ) 統括情報セキュリティ責任者及び情報システム管理者は、利用されていない I D が放置されないよう、人事管理部門と連携し、点検しなければならない。
- (エ) 統括情報セキュリティ責任者及び情報システム管理者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

## ウ 特権を付与された I D の管理等

- (ア) 統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与された I D を利用する者を必要最小限にし、当該 I D のパスワードの漏えい等が発生しないよう、当該 I D 及びパスワードを厳重に管理しなければならない。
  - (イ) 統括情報セキュリティ責任者及び情報システム管理者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作及び誤操作を防止するための措置を講じなければならない。
  - (ウ) 統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、C I S O が認めた者でなければならない。
  - (エ) C I S O は、(ウ) に規定する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、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。
  - (オ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された I D 及びパスワードの変更について、委託事業者に行わせてはならない。
  - (カ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された I D 及びパスワードについて、人事異動の際のパスワードの変更、入力回数制限等のセキュリティ機能を強化しなければならない。
  - (キ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された I D 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
- ア 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報シス

テム管理者の許可を得なければならない。

イ 統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

ウ 統括情報セキュリティ責任者は、外部からのアクセスを認める場合には、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。

エ 統括情報セキュリティ責任者は、外部からのアクセスを認める場合には、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。

オ 統括情報セキュリティ責任者及び情報システム管理者は、外部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には、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。

カ 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等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。

キ 統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、や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、通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

### (3) 自動識別の設定

統括情報セキュリティ責任者及び情報システム管理者は、ネットワークで 사용되는機器について、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。

### (4) 認証情報の管理

ア 統括情報セキュリティ責任者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。

イ 統括情報セキュリティ責任者又は情報システム管理者は、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。

ウ 統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

エ 統括情報セキュリティ責任者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

### (5) 特権による接続時間の制限

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。

(システム開発、導入、保守等)

第36条 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、次に掲げる対策を講じなければならない。

(1) 機器等及び情報システムの調達

ア 統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、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。

イ 統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

(2) 情報システムの開発

ア システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定し、並びにシステム開発のための規則を確立しなければならない。

イ システム開発における責任者及び作業者のIDの管理

(ア) 情報システム管理者は、システム開発の責任者及び作業者が使用するID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。

ウ システム開発に用いるハードウェア及びソフトウェアの管理

(ア) 情報システム管理者は、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。

(イ) 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には、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。

(3) 情報システムの導入

ア 開発環境と運用環境の分離及び移行手順の明確化

(ア) 情報システム管理者は、システム開発、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は、システム開発及び保守並びにテスト環境からシステム運用環境への移行について、システム開発及び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いき、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は、導入するシステム又は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。

#### イ テスト

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

(イ) 情報システム管理者は、運用テストを行う場合には、あらかじめ擬似環境による操作確認を行わなければならない。

(ウ) 情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

(エ) 情報システム管理者は、開発したシステムについて受入れテストを行う場合には、開発した組織及び導入する組織が、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。

#### ウ 機器等の納入時又は情報システムの受入れ時

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

(イ) 情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引き継がれる項目に、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

ア 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。

イ 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。

ウ 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

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

#### (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

ア 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。

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のセキュリティを維持するための対策

ウ 脅威又は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

エ 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) システム開発及び保守に関連する資料等の整備及び保管

ア 情報システム管理者は、システム開発及び保守に関連する資料並びにシステム関連文書を適正に整備及び保管しなければならない。

(ア) 情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告しなければならない。

(イ) 情報システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む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

イ 情報システム管理者は、テスト結果を一定期間保管しなければならない。

ウ 情報システム管理者は、情報システムに係るソースコードを適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

ア 情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

イ 情報システム管理者は、ウェブアプリケーション及び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及び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。

ウ 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は、情報システムを変更した場合には、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) 開発及び保守用のソフトウェアの更新等

情報システム管理者は、開発及び保守用のソフトウェア等を更新し、又はパッチの適用をする場合には、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は、システム更新又は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又は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、本町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。

(不正プログラム対策)

第37条 不正プログラム対策として、次に掲げる対策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。

ア 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。

イ 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。

ウ 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。

エ 所掌するサーバ、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。

オ 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。

カ 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。

キ 業務で利用するソフトウェアは、パッチ又はバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチ又は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。

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

## (2) 情報システム管理者の措置事項

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

ア 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。

イ 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。

ウ 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。

エ 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には、コンピュータウイルス等の感染を防止するために、町が管理している媒体以外を職員等に利用させないようにするとともに、不正プログラムの感染又は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て、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。

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

## (3) 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

ア パソコン又は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。
- イ 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。
  - ウ 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。
  - エ 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。
  - オ 添付ファイルがある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。
  - カ インターネット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情報系に取り込む場合は無害化しなければならない。
  - キ 統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。
  - ク 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及び、通信を行わない設定への変更などを実施しなければならない。

#### (4) 専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

(不正アクセス対策)

第38条 不正アクセス対策として、次に掲げる対策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、次の事項を措置しなければならない。

- ア 使用されていないポートを閉鎖しなければならない。
- イ 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。
- ウ 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者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。
- エ 重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。
- オ 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。

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

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

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

## （２） 攻撃への対処

C I S O及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じるとともに、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

C I S O及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス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。

## （４） 内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、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及び外部のサイトに対する攻撃を監視しなければならない。

## （５） 職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合には、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。

## （６） サービス不能攻撃

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

## （７） 標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）及び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。  
（セキュリティ情報の収集）

第39条 統括情報セキュリティ責任者は、次に掲げる対策を講じなければならない。

（1） セキュリティホールに関する情報の収集及び共有、ソフトウェアの更新等  
ア 統括情報セキュリティ責任者及び情報システム管理者は、サーバ装置、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、関係者間で共有するとともに、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。

イ 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、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本町の業務に対する影響及び保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者を確認しなければならない。

（2） 不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（3） 情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者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、関係者間で共有するとともに、情報セキュリティに関する社会環境及び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5節 運用面の対策

（情報システムの運用・保守時の対策）

第40条 統括情報セキュリティ責任者及び情報システム管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

2 統括情報セキュリティ責任者及び情報システム管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

3 統括情報セキュリティ責任者及び情報システム管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

（情報システムの監視機能）

第41条 統括情報セキュリティ責任者及び情報システム管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

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

3 統括情報セキュリティ責任者及び情報システム管理者は、新たな脅威の出現、運

用の状況等を踏まえ、情報システムにおける監視の対象及び手法を定期的に見直さなければならない。

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

(情報システムの監視)

第42条 統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

- 2 統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し、常時監視を行わなければならない。

- 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、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

- 4 統括情報セキュリティ責任者及びセキュリティ担当者は、監視した結果を正確に記録するとともに、消去又は改ざんをされないよう必要な措置を施し、安全な場所に保管しなければならない。

- 5 暗号化された通信データを監視のために復号することの可否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

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

- 7 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、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

- 8 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、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

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

(2) クラウドサービス利用の終了手順

(3) バックアップ及び復旧

(遵守状況の確認及び対処)

第43条 情報セキュリティ責任者及び情報セキュリティ管理者は、この指針等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C I S O及び統括情報セキュリティ責任者に報告しなければならない。

2 C I S O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この指針等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44条 C I S O及びC I S O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45条 職員等は、次の場合直ちに報告しなければならない。

(1) 職員等は、この指針に対する違反行為を発見した場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

(2) 当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者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。

(緊急時の対応等)

第46条 C I S O又は委員会は、次に掲げる対策を講じなければならない。

(1) 緊急時対応計画の策定

ア C I S O又は委員会は、事故等又はこの指針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。

イ C I S O 又は情報セキュリティ委員会は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、次の内容を定めなければならない。

ア 関係者の連絡先

イ 発生した事案に係る報告すべき事項

ウ 発生した事案への対応措置

エ 再発防止措置の策定

(3) 業務継続計画との整合性確保

自然災害、大規模又は広範囲にわたる疾病等に備えるとともに、別途業務継続計画を策定し、委員会は当該計画とこの指針との整合性を確保しなければならない。

(4) 緊急時対応計画の見直し

C I S O又は委員会は、情報セキュリティを取り巻く状況の変化及び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。

(例外措置)

第47条 情報セキュリティ管理者及び情報システム管理者は、次に掲げる対策を講じなければならない。

(1) 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、C I S O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つて、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C I S Oに報告しなければならない。

(3) 例外措置の申請書の管理

C I S O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。

(法令遵守)

第48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に、次の法令のほか関係法令を遵守し、これに従わなければならない。

(1) 地方公務員法（昭和25年法律第261号）

(2) 著作権法（昭和45年法律第48号）

(3) 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）

(4) 個人情報の保護に関する法律（平成15年法律第57号）

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

(6) サイバーセキュリティ基本法（平成26年法律第104号）

(7) 新温泉町個人情報の保護に関する法律施行条例（令和5年新温泉町条例第5号）

(8) その他情報セキュリティ対策に関する法令

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、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

(業務委託)

第49条 契約書が締結できる場合の業務委託の利用は、次に掲げる対策を講じなければならない。

(1) 業務委託に係る運用規程の整備

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

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

イ 委託事業者の選定基準

(ア) 情報セキュリティ管理者は、委託事業者の選定に当たり、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。

(イ) 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。

(2) 業務委託実施前の対策

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

(ア) 委託する業務内容の特定

(イ) 委託事業者の選定条件を含む仕様の策定

(ウ) 仕様に基づく委託事業者の選定

(エ) 情報セキュリティ要件を明記した契約の締結 (契約項目)

重要な情報資産を取り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。

a この指針及び新温泉町情報セキュリティ実施手順の遵守

b 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決め

c 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

d 提供されるサービスレベルの保証

e 委託事業者にアクセスを許可する情報の種類、範囲及び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

f 委託事業者の従業員に対する教育の実施

g 提供された情報の目的外利用及び受託者以外の者への提供の禁止

h 業務上知り得た情報の守秘義務

i 再委託に関する制限事項の遵守

j 委託業務終了時の情報資産の返還、廃棄等

k 委託業務の定期報告及び緊急時報告義務

l 町による監査及び検査

m 町による事故等発生時の公表

- n この指針が遵守されなかった場合の規定（損害賠償等）
- (オ) 委託事業者に重要情報を提供する場合は、秘密保持契約(NDA)の締結
- イ 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。
  - (ア) 仕様に準拠した提案
  - (イ) 契約の締結
  - (ウ) 委託事業者において重要情報を取り扱う場合は、秘密保持契約(NDA)の締結
- (3) 業務委託実施期間中の対策
  - ア 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。
    - (ア) 委託判断基準に従った重要情報の提供
    - (イ) 契約に基づき委託事業者を実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施
    - (ウ) 統括情報セキュリティ責任者へ措置内容の報告（重要度に応じてC I S O に報告）
    - (エ) 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求
  - イ 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。
    - (ア) 情報の適正な取扱いのための情報セキュリティ対策
    - (イ) 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告
    - (ウ) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処
- (4) 業務委託終了時の対策
  - ア 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
  - イ 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

(情報システムに関する業務委託)

第50条 情報システム又はアプリケーションプログラムの開発・運用・保守等の情報  
システムに関する業務を委託する場合は、次に掲げる対策を講じなければならない。

(1) 情報システムに関する業務委託における共通的対策

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

(2) 情報システムの構築を業務委託する場合の対策

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

ア 情報システムのセキュリティ要件の適切な実装

イ 情報セキュリティの観点に基づく試験の実施

ウ 情報システムの開発環境及び開発工程における情報セキュリティ対策

(3) 情報システムの運用・保守を業務委託する場合の対策

ア 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、委託事業者の実施を求めなければならない。

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

(4) 本町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

ア 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町  
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。

イ 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。

ウ 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。

エ 情報システム管理者又は情報セキュリティ管理者は業務委託サービスを利用  
する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ

当該サービスの利用申請を行わなければならない。

オ 統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

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

(ソーシャルメディアサービスの利用)

第51条 ソーシャルメディアサービスの利用は、次に掲げる対策を講じなければならない。

(1) 情報セキュリティ管理者は、町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 町のアカウントによる情報発信が、実際の町のものであることを明らかにするために、町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。

イ パスワード又は認証のためのコード等の認証情報及びこれを記録した媒体(ハードディスク、USBメモリ、紙等)等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

(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、本町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こと。

(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))

第52条 クラウドサービスを利用して自治体機密性2以上の情報を取り扱う場合は、次に掲げる対策を講じなければならない。

(1) クラウドサービスの選定に係る運用規程の整備

統括情報セキュリティ責任者は、自治体機密性2以上の情報を取り扱う場合、以下を含む外部サービス(クラウドサービス、以下「クラウドサービス」という。)の選定に関する規定を整備しなくてはならない。

ア クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準(本条において「クラウドサービス利用

判断基準」という。)

イ クラウドサービス提供者の選定基準

ウ クラウドサービスの利用申請の許可権限者と利用手続

エ クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

## (2) クラウドサービスの利用に係る運用規程の整備

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

ア 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及び責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

イ 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及び責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

ウ 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及び責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

(ア) クラウドサービスの利用終了時における対策

(イ) クラウドサービスで取り扱った情報の廃棄

(ウ) クラウドサービスの利用のために作成したアカウントの廃棄

## (3) クラウドサービスの選定

ア 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。

イ 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。

ウ 情報セキュリティ責任者は、以下の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用するクラウドサービスが、本町が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価しなければならない。

(ア) クラウドサービスの利用を通じて本町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、本町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又はリージョンの指定
  - (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
- エ 情報セキュリティ責任者は、クラウドサービスの中断又は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。
- オ 情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認しなければならない。
- カ 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町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ること。
- (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
- キ 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町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、必要に応じて本町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。
- ク 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町に提供し、本町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。
- ケ 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すること。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。
- コ 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、以下を全て含むセキュリティ要件を定めなければならない。

(ア) クラウドサービスに求める情報セキュリティ対策

(イ) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(ウ) クラウドサービスに求めるサービスレベル

サ 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

ア 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。

イ 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

ア 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らない。

イ 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。

ウ 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

ア 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及び責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

(ア) 不正なアクセスを防止するためのアクセス制御

(イ) 取り扱う情報の機密性保護のための暗号化

(ウ) 開発時におけるセキュリティ対策

(エ) 設計・設定時の誤りの防止

(オ) クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

イ 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。

ウ 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

エ 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。

オ 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、情報セキュリティに配慮した構築の手順及び実践がされているか、クラウドサービス事業者から情報を求め、実施状況を確認及び記録すること。

(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

ア 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及び責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

(ア) クラウドサービス利用方針の規定

(イ) クラウドサービス利用に必要な教育

(ウ) 取り扱う資産の管理

(エ) 不正アクセスを防止するためのアクセス制御

(オ) 取り扱う情報の機密性保護のための暗号化

(カ) クラウドサービス内の通信の制御

(キ) 設計・設定時の誤りの防止

(ク) クラウドサービスを利用した情報システムの事業継続

(ケ) 設計・設定変更時の情報及び変更履歴の管理

イ 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。

ウ 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。

エ 情報セキュリティ責任者は、クラウドサービスの特性及び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。

オ 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。

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

(8) クラウドサービスを利用した情報システムの更改・廃棄時の対策

ア 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及び責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。

(ア) クラウドサービスの利用終了時における対策

(イ) クラウドサービスで取り扱った情報の廃棄

(ウ) クラウドサービスの利用のために作成したアカウントの廃棄

イ 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。

ウ クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の1つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

(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わない場合）)

第53条 自治体機密性2以上の情報を取り扱わない前提でクラウドサービスを利用する場合は、次に掲げる対策を講じなければならない。

(1) クラウドサービスの利用に係る規定の整備

統括情報セキュリティ責任者は、自治体機密性2以上の情報を取り扱わない場合、以下を含むクラウド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。

ア クラウドサービスを利用可能な業務の範囲

イ クラウドサービスの利用申請の許可権限者と利用手続

ウ クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

エ クラウドサービスの利用の運用手順

(2) クラウドサービスの利用における対策の実施

ア 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。

イ 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。

(監査)

第54条 C I S Oは、情報セキュリティ監査統括責任者（以下「監査統括責任者」という。）を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

(1) 監査を行う者の要件

ア 監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

イ 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。

(2) 監査実施計画の立案及び実施への協力

ア 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、委員会の承認を得なければならない。

イ 被監査部門は、監査の実施に協力しなければならない。

(3) 委託事業者に対する監査

ア 事業者が業務委託を行っている場合、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、この指針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。

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

(4) 報告

監査統括責任者は、監査結果を取りまとめ、委員会に報告しなければならない。

(5) 保管

監査統括責任者は、監査の実施を通して収集した監査証拠及び監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

(6) 監査結果への対応

ア C I S O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。

イ C I S O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。

(7) この指針及び関係規程等の見直し等への活用

委員会は、監査結果をこの指針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。

(自己点検)

第55条 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、次に掲げる対策を講じなければならない。

(1) 実施方法

ア 統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、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。

イ 情報セキュリティ管理者は、情報システム管理者と連携して、所管する課室等におけるこの指針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、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

ア 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。

イ 委員会は、この点検結果をこの指針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。

(この指針、関係規程等の見直し)

第56条 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、この指針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。なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示し、措置の結果についてC I S Oに報告しなければならない。

附 則

この訓令は、令和7年8月1日から施行する。

提案理由