

北塩原村情報セキュリティポリシー

令和 8 年 3 月

北塩原村情報セキュリティ委員会

目次

序 情報セキュリティポリシーの構成	1
第1章 情報セキュリティ基本方針	2
1 目的	2
2 定義	2
3 対象とする脅威	3
4 職員等の遵守義務	3
5 情報セキュリティ対策	3
6 情報セキュリティ監査及び自己点検の実施	4
7 情報セキュリティポリシーの見直し	4
8 情報セキュリティ対策基準の策定	4
9 情報セキュリティ実施手順の策定	4
第2章 情報セキュリティ対策基準	6
1 対象範囲	6
2 組織体制	6
3 情報資産の分類と管理方法	9
4 情報システム全体の強靱性の向上	12
5 物理的セキュリティ	14
5.1 サーバ等の管理	14
5.2 管理区域(電算室等)の管理	15
5.3 通信回線及び通信回線装置の管理	16
5.4 職員等のパソコン等の管理	16
5.5 職場環境(執務室)の管理	17
6 人的セキュリティ	17
6.1 職員等の遵守事項	17
6.2 研修・訓練	20
6.3 情報セキュリティインシデントの報告	20
6.4 ID及びパスワード等の管理	22
7 技術的セキュリティ	22
7.1 コンピュータ及びネットワークの管理	22
7.2 アクセス制御	27
7.3 システム開発、導入、保守等	29
7.4 不正プログラム対策	32
7.5 不正アクセス対策	33
7.6 セキュリティ情報の収集	34
8 運用	35
8.1 情報システムの監視	35
8.2 情報セキュリティポリシーの遵守状況の確認	36
8.3 侵害時の対応等	36
8.4 例外措置	37
8.5 法令遵守	37
8.6 懲戒処分等	37
9 業務委託とクラウドサービスの利用	38

9. 1. 業務委託	38
9. 2. 情報システムに関する業務委託	40
9. 3. 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）	41
9. 4. 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）	45
10 評価・見直し	45
10. 1. 監査	45
10. 2. 自己点検	46
10. 3. 情報セキュリティポリシー等の見直し	47

序 情報セキュリティポリシーの構成

情報セキュリティポリシーとは、北塩原村（以下「村」という。）が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、村が所掌する情報資産に関する業務に携わる全職員、非常勤、会計年度任用職員、及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と情報資産を取り巻く状況の変化に依存する部分(対策基準)に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

- ① 情報セキュリティ基本方針
- ② 情報セキュリティ対策基準

の2階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする(下表参照)。

情報セキュリティポリシーの構成

文 書 名		内 容
情報セキュリティ ポ リ シ ー	情報セキュリティ 基 本 方 針	情報セキュリティ対策に関する統一かつ基本的な方針。
	情報セキュリティ 対 策 基 準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

第1章 情報セキュリティ基本方針

1 目的

本基本方針は、本村が保有する情報資産の機密性、完全性及び可用性を維持するため、本村が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2 定義

(1) ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器(ハードウェア及びソフトウェア)をいう。

(2) 情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

(5) 機密性

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

(6) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7) 可用性

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

(8) マイナンバー利用事務系(個人番号利用事務系)

個人番号利用事務(社会保障、地方税若しくは防災に関する事務)又は戸籍事務等に関わる情報システム及びデータをいう。

(9) LGWAN 接続系

LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう(マイナンバー利用事務系を除く。)

(10) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(11) 通信経路の分割

LGWAN接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(12) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

- ①不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の窃取、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 職員等の遵守義務

職員、非常勤職員、会計年度任用職員及び業務受託業者の職員(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。

5 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
本村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
本村の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。
- (3) 情報システム全体の強靱性の向上
情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。
 - ①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。
 - 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
サーバ等、電算室等、通信回線等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、システム開発等の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切に対応するため、緊急時対応計画を策定する。

(8) 業務委託とクラウドサービスの利用

業務委託を行う場合には、外部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。

クラウドサービスを利用する場合には、利用に係る規程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。

6 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。

7 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

8 情報セキュリティ対策基準の策定

上記5、6及び7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。当該基準は、情報セキュリティ対策を行う上での基本的な要件を明記するものである。

9 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村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基準

1 対象範囲

(1) 行政機関の範囲

本対策基準が適用される行政機関は、内部部局、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、公営企業及び議会とし各教育機関(学校等)は対象外とする。

なお、住民基本台帳ネットワークシステム及び喜多方地方広域市町村圏組合広域的地域情報通信ネットワークの情報システム等については、別に定めたセキュリティ対策に基づき運用するものとする。

(2) 情報資産の範囲

本対策基準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、情報システム及びこれらに関する設備、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

2 組織体制

(1) 最高情報統括責任者・最高情報セキュリティ責任者(CISO: Chief Information Security Officer、以下「CISO」という。)

- ①副村長を、CISOとする。CISOは、本村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。
- ③CISOは、情報セキュリティインシデントに対処するための体制(CSIRT: Computer Security Incident Response Team、以下「CSIRT」という。)を整備し、役割を明確化する。
- ④CISOは、CISOを助けて本村における情報セキュリティに関する事務を整理し、CISOの命を受けて本村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。
- 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。

(2) 統括情報セキュリティ責任者

- ①総務企画課長を、CISO直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者はCISOを補佐しなければならない。
- ②統括情報セキュリティ責任者は、本村の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
- ③統括情報セキュリティ責任者は、本村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統括的な権限及び責任を有する。
- ④統括情報セキュリティ責任者は、情報セキュリティ責任者、統括情報セキュリティ管理者、情報セキュリティ管理者、情報セキュリティ担当者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

- ⑤統括情報セキュリティ責任者は、本村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行う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、本村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・管理を行う統括的な権限及び責任を有する。
- ⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、統括情報セキュリティ管理者、情報セキュリティ管理者、情報セキュリティ担当者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。
- ⑧統括情報セキュリティ責任者は、緊急時にはCISOに早急に報告を行うとともに、回復のための対策を講じなければならない。
- ⑨統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じてCISOにその内容を報告しなければならない。

(3) 情報セキュリティ責任者

- ①各課等の長を、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、当該課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、その所管する課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、その所管する課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及び職員等に対する教育、訓練、助言及び指示を行う。

(4) 統括情報セキュリティ管理者

- ①電算業務担当班長を、統括情報セキュリティ管理者とする。統括情報セキュリティ管理者は統括情報セキュリティ責任者を補佐しなければならない。
- ②統括情報セキュリティ管理者は、本村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管理者は、本村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管理者は、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。
- ⑤統括情報セキュリティ管理者は、本村の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、CISO及び統括情報セキュリティ責任者の指示に従い、CISO及び統括情報セキュリティ責任者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行う権限及び責任を有する。
- ⑥統括情報セキュリティ管理者は、本村の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。
- ⑦統括情報セキュリティ管理者は、緊急時にはCISO及び統括情報セキュリティ責任者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。

(5) 情報セキュリティ管理者

- ①各課等の班長を、情報セキュリティ管理者とする。情報セキュリティ管理者は直属の情報セキュリティ責任者を補佐しなければならない。
- ②情報セキュリティ管理者は、その所管する課等の情報セキュリティ対策に関する権限及び責任を有する。

- ③情報セキュリティ管理者は、その所掌する課等において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及び最高情報統括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。
- (6) 情報セキュリティ担当者
情報セキュリティ管理者の指示等に従い、情報セキュリティ対策に関する作業を行う者を、情報セキュリティ担当者とする。
- (7) 情報システム管理者
①各情報システムの担当課等の長を、当該情報システムに関する情報システム管理者とする。
②情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
③情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。
④情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。
- (8) 情報システム担当者
情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を、情報システム担当者とする。
- (9) 情報セキュリティ委員会
①本村の情報セキュリティ対策を統一的行うため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。
②情報セキュリティ委員会は、必要に応じて、本村における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。
③情報セキュリティ委員会は、CISOによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。
④情報セキュリティ委員会は、情報セキュリティポリシー対策基準並びに情報セキュリティ実施手順の見直しの必要性を検討しなければならない。
- (10) 兼務の禁止
①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。
- (11) 情報セキュリティに関する統一的な窓口(「CSIRT(Computer Security Incident Response Team)」以下、「CSIRT」という。)の設置
①CISOは、CSIRTを整備し、情報セキュリティインシデントについて課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する。
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。
③CSIRTは、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。
④CSIRT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CSIRT、外部の事業者等との情報共有を行う。
- (12) クラウドサービス利用における組織体制
①統括情報セキュリティ責任者は、クラウドサービスを利用する場合には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなけれ

ばならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

3 情報資産の分類と管理方法

(1) 情報資産の分類

本村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 ・極秘文書：秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書（国防関連） ・秘文書：極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書（公益通報等）	<ul style="list-style-type: none"> ・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及び情報セキュリティ責任者等の許可（自治体機密性3以上） ・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（以降、村の外部施設は除く）で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体 機密性 3B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産 （住民記録システム、税務システム、国民健康保険システム、生活保護システム、農業委員会台帳システム、貸付金償還システム等に保存される住民の個人情報）	
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 ・職員としての属性に基づく個人情報 ・オンライン申請の処理等により、システム処理上一時的にインターネット上に保管されるデータ ・文書管理システムの決裁文書として保存されている個人情報 ・施設設計情報や入札予定価格など非公開情報	
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1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 ・政策検討に関する情報	
自治体 機密性	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	—

1	<ul style="list-style-type: none"> ・将来公表する予定の文書（白書の案等） ・公表された情報 	
---	---	--

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。）を及ぼす恐れがある情報資産	<ul style="list-style-type: none"> ・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体 完全性 1	自治体完全性2の情報資産以外の情報資産（改ざん、誤びゅう又は破壊されても復元が可能な情報）	—

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。）を及ぼす恐れがある情報資産	<ul style="list-style-type: none"> ・バックアップを行い、指定する時間内の復旧 ・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（一般的に利用不可能でも重大な支障を及ぼさない情報）	—

(2) 情報資産の管理

①管理責任

- (ア) 情報セキュリティ責任者は、その所管する情報資産について管理責任を有する。
- (イ) 情報システム管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。
- (ウ) 情報セキュリティ責任者は、情報資産が複製又は伝送された場合には、複製等された情報資産も(1)の分類に基づき管理しなければならない。
- (エ) 情報セキュリティ責任者は、クラウドサービスの環境に保存される情報資産についても(1)の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定める。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・フッター等)、格納する記録媒体(CD-R のラベル等)、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切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、情報セキュリティ責任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、適切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、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) 情報セキュリティ責任者又は情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。
- (イ) 情報セキュリティ責任者又は情報システム管理者は、情報資産を記録した外部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) 情報セキュリティ責任者又は情報システム管理者は、利用頻度が低い外部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外部記録媒体を長期保管する場合は、自然災害等により損害を受ける可能性が低い施設に保管しなければならない。
- (エ) 情報セキュリティ責任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

- (ア) 自治体機密性3C以上の情報を電子メール等で送信してはならない。ただし、業務上必要な場合は、情報セキュリティ責任者の許可を得て、これを送信することができる。
- (イ) 電子メール等により自治体機密性2又は自治体完全性2以上の情報を送信する者は、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。

⑧台帳による管理

情報セキュリティ責任者は、情報資産の重要性分類、利用目的、管理責任者、取扱者、保管場所、保存期間、収集方法、廃棄(削除)方法等を記録した台帳による情報資産の管理に努めなければならない。

⑨情報資産の運搬

(ア) 車両等により自治体機密性 3C 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 3C 以上の情報資産を運搬する者は、情報セキュリティ責任者に許可を得なければならない。

⑩情報資産の提供・公表

(ア) 自治体機密性 2 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 3C 以上の情報資産を外部に提供する者は、情報セキュリティ責任者に許可を得なければならない。

(ウ) 情報セキュリティ責任者は、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。

⑪情報資産の廃棄

(ア) 自治体機密性 2 以上の情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合、記録媒体の初期化等、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) 自治体機密性 2 以上の情報が記載された紙媒体は、シュレッダー又は焼却により処理することとし、裏面再利用をしてはならない。

(ウ) 情報資産の廃棄を庁舎外で行う場合は、行った処理について、日時、場所、処理者及び処理資産等を記録しなければならない。

(エ) 情報資産の廃棄を外部委託する場合は、依頼日時、担当職員及び廃棄方法を記録し、委託事業者が確実に廃棄した証拠を取得及び保管しなければならない。

(オ) 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、その自治体機密性 2 以上の場合は、情報を復元できないように処置しなければならない。

(カ) 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。

(キ) 情報資産の廃棄を庁舎外で行う場合、又は外部委託する場合、リース返却等を行う場合は、情報セキュリティ責任者の許可を得なければならない。

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

4 情報システム全体の強靱性の向上

(1) マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、インターネット等から LGWAN-ASP を経由してマイナンバー利用事務系にデー

タの取り込みを可能とする。

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、特定個人情報については 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を行ってはならない。

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

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

④マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

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

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

(2) LGWAN 接続系

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

②LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

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

(3) インターネット接続系

①インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

②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。

③業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情

報や職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

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

5 物理的セキュリティ

5. 1. サーバ等の管理

(1) 機器の取付け

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切に固定する等、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なければならない。
- ②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は、統括情報セキュリティ管理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、当該機器が適切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は、統括情報セキュリティ管理者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

(4) 通信ケーブル等の配線

- ①統括情報セキュリティ管理者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。
- ②統括情報セキュリティ管理者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。
- ③統括情報セキュリティ管理者及び情報システム管理者は、ネットワーク接続口(ハブのポート等)を他者が容易に接続できない場所に設置する等適切に管理しなければならない。
- ④統括情報セキュリティ管理者、情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

(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は、電磁的記録媒体を内蔵する機器を外部の事業者修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管

理者は、外部の事業者が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などを行わなければならない。

(6) 管理区域外への機器の設置

①統括情報セキュリティ管理者及び情報システム管理者は、管理区域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、定期的に又は必要に応じて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。

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、データセンターを利用する場合は、必要により外部委託事業者から「データセンターの安全・信頼性に係る情報開示指針（第3版）」の情報開示項目による情報提供を受けなければならない。

(7) 機器の廃棄等

①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、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

②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、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

5. 2. 管理区域(電算室等)の管理

(1) 管理区域の構造等

①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋(以下「電算室」いう。)や電磁的記録媒体の保管庫をいう。

②統括情報セキュリティ管理者及び情報システム管理者は、外部からの侵入が容易にできないように対策を講じなければならない。

③統括情報セキュリティ管理者及び情報システム管理者は、施設管理部門と連携して、管理区域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ち入りを防止しなければならない。

④統括情報セキュリティ管理者及び情報システム管理者は、電算室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤統括情報セキュリティ管理者及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部をすべて塞がなければならない。

⑥統括情報セキュリティ管理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や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

(2) 管理区域の入退室管理等

①情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。

②職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

③情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

④情報システム管理者は、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ないようにしなければならない。

(3) 機器等の搬入出

- ①情報システム管理者は、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した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は、電算室の機器等の搬入出について、職員を立ち合わせなければならない。

5. 3. 通信回線及び通信回線装置の管理

- (1) 統括情報セキュリティ管理者は、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、適切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切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) 統括情報セキュリティ管理者は、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) 統括情報セキュリティ管理者は、自治体機密性 2 以上の情報資産を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、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。
- (6) 統括情報セキュリティ管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。
- (7) 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。

5. 4. 職員等のパソコン等の管理

- (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、モバイル端末の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
- (2) 情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。
- (3) 情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証等の二要素認証を併用しなければならない。
- (4) 職員等が執務で利用するノートパソコンは原則、外部施設を除く庁舎外へ持ち出してはならない。在宅勤務以外でモバイル端末を庁外で業務利用する際は、専用機を利用することとする。
- (5) 情報システム管理者は、庁外へ持ち出すパソコンやモバイル端末等に自治体機密性 2 以上の情報を保存している場合は、情報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、自治体機密性 2 以上の情報を扱うモバイル端末を業務利用する際は、上記対策に加え、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。

5. 5. 職場環境（執務室）の管理

- (1) 情報セキュリティ責任者は、執務室を次に掲げる区域に分類し、職員等に周知するとともに、職員等以外にも認識できるように努めなければならない。
- ①特定の職員のみ立ち入りできる区域（CS 端末及び中間サーバ接続端末の設置場所等）
 - ②職員のみ立ち入りできる区域
 - ③職員の立会いにより職員以外も立ち入りできる区域
 - ④その他の区域
- (2) 情報セキュリティ責任者は、外部からの訪問者に対し、必要に応じて、次の事項を確認しなければならない。
- ①訪問先に関すること。
 - ②訪問理由に関すること。
 - ③身元に関すること。
 - ④その他
- (3) 情報セキュリティ責任者は、執務室内における搬入物及び搬出物の受渡区域を事前に指定しなければならない。
- (4) 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、執務室内に、FAX、コピー機、プリンター等の機器を設置する場合は、執務室の入り口から離れた場所又はそれに準ずる場所へ配置するよう努めなければならない。やむを得ず入り口付近に設置する場合は、パーテーション等により来訪者から容易に見えないようにしたり、職員から常に目が届くような配置にしたりするなどの措置を講じなければならない。

6 人的セキュリティ

6. 1. 職員等の遵守事項

- (1) 職員等の遵守事項

①情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ責任者に相談し、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、自治体可用性、自治体完全性のいずれかが 2 以上に該当する情報資産を外部で処理する場合は、必要に応じて、次のような安全管理措置を定めなければならない。

- a) 移動時における紛失、盗難等の防止措置
- b) 私物パソコンの利用制限

- c) ウイルス感染防止措置
- d) その他情報漏えい防止措置

(イ) 職員等は、本村のモバイル端末、電磁的記録媒体、ソフトウェア及び自治体機密性3以上の情報資産を外部に持ち出す場合には、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。

(ウ) 職員等は、外部で自治体機密性3以上の情報処理業務を行う場合には、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。

(エ) 職員等は、外部で情報処理作業を行う際、私物パソコン等の端末及び電磁的記録媒体等のハードウェアを用いて情報処理を行ってはならない。ただし、業務上必要な場合でこれらを使用する以外に方法がない場合に限り、情報セキュリティ責任者の許可を得た上で、これらを使用することができる。ただしこの場合においても、自治体機密性3以上の情報資産については、私物パソコンによる情報処理を行ってはならない。

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ア) 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を業務に利用してはならない。ただし、業務上必要な場合でこれらを使用する以外に方法がない場合に限り、情報セキュリティ責任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、情報セキュリティ責任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程を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

情報セキュリティ責任者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。また、その内容を定期的に又は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。

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

(ア) 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する場合は、情報システム管理者及び情報セキュリティ責任者の許可を得なければならない。

(イ) 職員等は、パソコン等の端末のメモリ、CPU、ハードディスク、電磁的記録媒体装置等の追加、交換その他の改造を行う場合は、情報システム管理者の許可を得なければならない。

(ウ) 職員等は、パソコンやモバイル端末にソフトウェアの追加又は設定の変更をする場合は、情報システム管理者の許可を得なければならない。この場合、ネットワークに対する影響が生じる恐れがあるときは、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と協議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責任者は、導入したソフトウェアのライセンスを適正に管理しなければならない。

⑦無許可ソフトウェアの導入等の禁止

(ア) 職員等は、パソコン等の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、不正にコピーしたソフトウェアを利用してはならない。

⑧無許可でのネットワーク接続の禁止

(ア) 職員等は、情報システム管理者の許可なく、パソコンやモバイル端末をネットワークに接続してはならない。

(イ) 職員等は、情報システム管理者の許可なく、WiFi ルータ等のネットワーク機器を持ち込み、パソコン等の端末を当該機器へ接続してはならない。私物のスマートフォンとの接続

も同様である。

⑨業務以外の目的でのウェブ閲覧の禁止

- (ア) 職員等は、業務以外の目的で村所有のパソコンやモバイル端末によるウェブ閲覧をしてはならない。
- (イ) 情報セキュリティ責任者は、職員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、速やかに注意して閲覧を中止させるなど、適切に措置しなければならない。

⑩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責任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、適切な措置を講じなければならない。

⑪不正プログラム対策

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。
- (イ) 外部からデータ又はソフトウェアを取り入れる場合は、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実施しなければならない。
- (オ) 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。
- (カ) コンピュータウイルス等の不正プログラムに感染したと思われる場合は、直ちにネットワークから分離し、その状態で情報セキュリティ責任者及びCSIRTに報告しなければならない。

⑫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。

⑬クラウドサービス利用時等の順守事項

職員等は、クラウドサービスの利用にあたっては情報セキュリティポリシーを順守し、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

①情報セキュリティポリシー等の遵守

情報セキュリティ責任者は、非常勤及び会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、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、また実施及び遵守させなければならない。

②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ責任者は、非常勤及び会計年度任用職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③インターネット接続及び電子メール使用等の制限

情報セキュリティ責任者は、非常勤及び会計年度任用職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(3) 情報セキュリティポリシー等の掲示

情報セキュリティ責任者は、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) 外部委託事業者に対する説明

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の開発・保守等を外部委託業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

6. 2. 研修・訓練

(1) 情報セキュリティに関する研修・訓練

①CISO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。

②CISO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、外部委託先を含む関係者については、外部委託先等で教育、訓練が行われていることを確認しなければならない。

③情報セキュリティ責任者は、職員等がCISOの実施する情報セキュリティ及び特定個人情報等の適正な取扱いに関する研修に参加できるよう配慮しなければならない。

④職員等は、情報セキュリティ及び特定個人情報の適切な取扱いに関する研修等を受講するよう努めなければならない。

(2) 研修計画の立案及び実施

①CISOは、課長等を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。

②研修は、職員等の役割、情報セキュリティ及び特定個人情報の適切な取扱いに関する理解度等に応じたものに行なければならない。また、新規採用の職員等を対象とする研修を実施しなければならない。

③情報セキュリティ責任者は、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。

④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。

⑤所管する課室等内に未受講者がいる場合、情報セキュリティ責任者は、未受講者へ研修教材等を元に研修内容を教示し、その履歴を記録する。

(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行う必要がある。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

課長等を含めたすべての職員等は、定められた研修・訓練に参加しなければならない。

6. 3. 情報セキュリティインシデントの報告

(1) 対象とする情報セキュリティに関する事故等

情報セキュリティ委員会への報告対象とする情報セキュリティに関する事故等は、次のとおりとする。

- ①個人情報等の機密情報が記録されているパソコン等の端末及び電磁的記録媒体等の情報資産の紛失及び盗難等（それらを印刷したものを含む）。
 - ②情報資産に対する部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因によるサービス及び業務の停止、情報漏えい、破壊、改ざん、消去等。
 - ③情報システムに関するプログラム上の欠陥又は操作ミス、故障等の非意図的な要因によるサービス及び業務の停止、情報漏えい、破壊、改ざん、消去等のうち、重大な支障が生じたもの。
 - ④地震、落雷、火災等の災害による情報システムに関するサービス及び業務の停止、情報資産の破壊、消失等のうち、重大な支障が生じたもの。
 - ⑤その他、前各号に準ずる情報資産に脅威を及ぼす事象の発生。
- (2) 庁内からの情報セキュリティインシデントの報告
- ①職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合、速やかに情報セキュリティ責任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。
 - ②報告を受けた情報セキュリティ責任者は、速やかに CSIRT 及び情報システム責任者に報告しなければならない。
 - ③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について、必要に応じて CISO、統括情報セキュリティ責任者に報告しなければならない。
 - ④情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。
 - ⑤情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。
- (3) 住民等外部からの情報セキュリティインシデントの報告
- ①職員等は、本村が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ責任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責任者は、速やかに CSIRT 及び情報システム責任者に報告しなければならない。
 - ③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について、必要に応じて CISO、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報告しなければならない。
 - ④CISO は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。
 - ⑤統括情報セキュリティ責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。
- (4) 情報セキュリティインシデント原因の究明・記録、再発防止等
- ①CSIRT は、情報セキュリティインシデントを引き起こした部門の情報セキュリティ責任者及び情報システム管理者と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、CISO に報告しなければならない。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。

- ②CISOは、CSIRTから、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

6. 4. ID及びパスワード等の管理

(1) ICカード等の取扱い

- ①職員等は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。
- (ア) 認証に用いるICカード等を、職員等間で共有してはならない。
 - (イ) 業務上必要のないときは、ICカード等をカードリーダー若しく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責任者に通報し、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責任者は、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責任者は、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パスワードは秘密にし、パスワードの照会等には一切応じてはならない。
- ③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。なお、詳細なパスワード要件は、統括情報セキュリティ責任者が定めることとする。
- ④パスワードが流出したおそれがある場合には、情報セキュリティ責任者に速やかに報告し、パスワードを速やかに変更しなければならない。
- ⑤パスワードは定期的に又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。
- ⑥複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
- ⑦仮のパスワードは、最初のログイン時点で変更しなければならない。
- ⑧パソコン等の端末にパスワードを記憶させてはならない。
- ⑨職員等間でパスワードを共有してはならない（ただし、共有IDに対するパスワードは除く）。
- ⑩パスワードを書いたメモは、他職員等に知られることがないよう、厳重に管理しなければならない。

7 技術的セキュリティ

7. 1. コンピュータ及びネットワークの管理

(1) 文書サーバの設定等

- ①情報システム責任者は、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。

- ②情報システム責任者は、文書サーバを課室等の単位で構成し、職員等が他課等のフォルダ及びファイルを開覧及び使用できないように、設定しなければならない。
- ③情報システム責任者は、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開覧及び使用できないようにしなければならない。
- ④同一の利用者 ID の複数職員での利用は、必要最小限とすること。

(2) バックアップの実施

- ①統括情報セキュリティ管理者及び情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。
- ②統括情報セキュリティ管理者及び情報システム管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。
- ③統括情報セキュリティ管理者及び情報システム管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。
- ④統括情報セキュリティ管理者及び情報システム管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の使用を要求し、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村の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

(3) 他団体との情報システムに関する情報等の交換

- ①情報システム責任者は、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の許可を得なければならない。
- ②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は、相手方の団体との間で、その取扱いに関する合意文書等を取り交わすなどの対策をとるよう努めなければならない。

(4) システム管理記録及び作業の確認

- ①情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。
- ②統括情報セキュリティ管理者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、窃取、改ざん等をされないように適切に管理しなければならない。
- ③統括情報セキュリティ管理者、情報システム管理者、情報セキュリティ担当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外部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管理者及び情報システム責任者は、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、自治体機密性 2・自治体完全性 2・自治体可用性 2 相当の情報資産として取扱い、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、適切に管理しなければならない。

(6) ログの取得等

- ①統括情報セキュリティ管理者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。
- ②統括情報セキュリティ管理者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。
- ③統括情報セキュリティ管理者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。
- ④統括情報セキュリティ管理者及び情報システム管理者は、監査及びデジタルフォレンジックに必要な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ない場合は、クラウドサービス事業者に提出を要求するための手続きを明確にしなければならない。
- ⑤統括情報セキュリティ管理者及び情報システム責任者は、必要に応じて、取得した記録及びログを電磁的記録媒体にバックアップしなければならない。

(7) 障害記録

統括情報セキュリティ管理者及び情報システム責任者は、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、適切に保存しなければならない。

(8) ネットワークの接続制御、経路制御等

- ①統括情報セキュリティ管理者は、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統括情報セキュリティ管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。
- ③統括情報セキュリティ管理者は、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。

(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

- ①情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO、統括情報セキュリティ責任者の許可を得なければならない。
- ②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、庁内のすべてのネットワーク、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は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。
 - ④統括情報セキュリティ管理者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。
 - (ア) 庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。
 - (イ) 脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。
 - (ウ) ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。
 - ⑤情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。
- (11) 複合機のセキュリティ管理
- ①統括情報セキュリティ管理者は、複合機を調達する場合、当該複合機が備える機能、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、適切なセキュリティ要件を策定しなければならない。
 - ②情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。
 - ③情報セキュリティ責任者は、複合機の運用を終了する場合、複合機を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) 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実施しなければならない。
- (13) 無線 LAN 及びネットワークの盗聴対策
- ①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しアクセスポイントへの不正な接続を防御しなければならない。また、必要に応じて、不正利用調査を行うよう努めなければならない。
 - ②統括情報セキュリティ責任者は、機密性の高い情報を扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。
- (14) 電子メールのセキュリティ管理
- ①統括情報セキュリティ管理者は、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統括情報セキュリティ管理者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。
 - ③統括情報セキュリティ管理者は、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統括情報セキュリティ管理者は、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統括情報セキュリティ管理者は、システム開発や運用、保守等のため庁舎内に常駐している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、外部委託事業者との間で利用方法を取り決めなければならない。

(15) 電子メールの利用制限

- ①職員等は、自動転送機能を用いて、外部の者に電子メールを転送してはならない。
- ②職員等は、業務上必要のない送信先に電子メールを送信してはならない。
- ③職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
- ④職員等は、自治体機密性 2 以上の重要な電子メールを誤送信した場合、CSIRT 及び情報セキュリティ責任者に報告しなければならない。
- ⑤職員等は、自治体機密性 2 以上、自治体完全性 2 の情報資産の送信に、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。ただし、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得るとともに、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た上で、使用することができる。

(16) 電子署名・暗号化

- ①職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。
- ②職員等は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また、CISO 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。
- ③CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(17) 無許可ソフトウェアの導入等の禁止

- ①職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
- ②職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ責任者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。
- ③職員等は、不正にコピーしたソフトウェアを利用してはならない。

(18) 機器構成の変更の制限

- ①職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。
- ②職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。ただし、情報資産を保管する機能のないキーボード、マウス及びディスプレイについては、統括情報セキュリティ責任者の許可を省略することができる。

(19) 無許可でのネットワーク接続の禁止

- 職員等は、統括情報セキュリティ責任者の許可なくパソコン等の端末をネットワークに接続してはならない。

(20) 業務外ネットワークへの接続の禁止

- ①職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。
- ②情報セキュリティ責任者は、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。

(21) Web 会議サービス利用時の対策

- ①情報システム管理者は、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、本村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

セキュリティ対策を実施すること。

③職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

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

(22) 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管理者は、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、情報セキュリティ責任者に通知し適切な措置を求めなければならない。

(23) ソーシャルメディアサービスの利用

①情報セキュリティ責任者は、本村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) 本村のアカウントによる情報発信が、実際の本村のものであることを明らかにするために、本村の自己管理 Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

(イ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（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、本村の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

7. 2. アクセス制御

(1) アクセス制御

①アクセス制御

統括情報セキュリティ管理者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

②利用者 ID の取扱い

(ア) 統括情報セキュリティ責任者及び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) 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管理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管理者及び情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

(エ) 職員等へ情報システムに対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

③特権を付与された ID の管理等

- (ア) 統括情報セキュリティ管理者及び情報システム管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。
- (イ) 管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。
- (ウ) 統括情報セキュリティ責任者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、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、統括情報セキュリティ管理者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。
- (オ) 統括情報セキュリティ管理者及び情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部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管理者及び情報システム管理者は、特権を付与された ID 及びパスワードについて、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) 統括情報セキュリティ管理者及び情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。
- (ク) 外部委託事業者へ特権（フルアクセス可能な）ID を付与する場合は、原則、当該事業者の担当者ごと個別にアカウントを作成し付与する。但し、必要最小限に限定された当該事業者の担当者が特権 ID を利用する場合は、アカウント利用者を把握することで共有することができる。

(2) 職員等による外部からのアクセス等の制限

- ①職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。
- ②統括情報セキュリティ管理者は、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統括情報セキュリティ管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。
- ④統括情報セキュリティ管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。
- ⑤統括情報セキュリティ管理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、セキュリティ確保のために必要な措置を講じなければならない。
- ⑥職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ責任者の許可を得るか、もしくは情報セキュリティ責任者によって事前に定義されたポリシーに従って接続しなければならない。
- ⑦統括情報セキュリティ責任者は、公衆通信回線（公衆無線 LAN 等）の庁外通信回線を庁内ネットワークに接続することは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 及びパスワード、生体認証に係る情報等の認証情報及びこれを

記録した媒体(ICカード等)による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

(3) 認証情報の管理

- ①情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワード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パスワード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、本人がログイン後直ちに仮のパスワードを変更しなければならないようにするなど、なりすまし防止対策を施さなければならない。
- ③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。

7. 3. システム開発、導入、保守等

(1) 機器等の調達に係る運用規程の整備

- ①統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられるリスクに係る懸念が払拭できない企業の機器等を調達してはならない。
- ②情報システム管理者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。

(2) 機器等及び情報システムの調達

- ①統括情報セキュリティ管理者及び情報システム管理者は、情報システム開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。
- ②統括情報セキュリティ管理者及び情報システム管理者は、機器及びソフトウェアの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

(3) 情報システムの開発

情報システムの開発においては、次の事項を遵守しなければならない。なお、②及び③は、本村が所管するサーバ又はパソコン等の端末を利用して情報システムを開発する場合の遵守事項となる。

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は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者、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。

③システム開発に用いるハードウェア及びソフトウェアの管理

- (ア) 情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(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、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。

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、既知の種類ウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

(4) 情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

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

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

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

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

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

③機器等の納入時又は情報システムの受入れ時

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

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

(5) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

利用するソフトウェアの特性を踏まえ、以下のセキュリティ対策が全て実施されていることを確認しなければならない。

①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を維持する手順の整備

②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の整備

(6) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

情報システムの開発においては、次の事項を遵守しなければならない。なお、②は、本村が所管するサーバ又はパソコン等の端末を利用して情報システムを開発する場合の遵守事項となる。

①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、以下のセキュリティ対策が全て実施されていることを確認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は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

(7) システム開発・保守に関連する資料等の保管

①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切に整備・保管しなければならない。また、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水準を維持する手順及び情報セキュリティインシデント発生時の対処手順を整備しなければならない。

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

(8) 情報システムにおける入出力データの正確性の確保

①情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力除去する機能を組み込むように情報システムを設計しなければならない。

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

(ア) 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの構築方法等を見直さなければならない。

(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) 情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいする恐れがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(9) 情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

(10) 開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を更新、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。

(11) 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・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に関する次の事項のほか、必要な検証を行うよう努めなければならない。

①システム更新又は統合作業時に遭遇する想定外の事象に対応する体制

②システム及びデータ移行手続が失敗した場合や移行直後に障害等が生じた場合における旧シ

システムへ戻す計画とその手順

③更新又は統合によって影響される業務運営体制

④システム及びデータ移行手続における検証チェックポイントや移行の妥当性基準の明確化

(12) リモートメンテナンス

保守委託によるリモートメンテナンスを行うにあたって、委託事業者は、定期メンテナンスについては計画書の提出、不定期メンテナンスについては事前承認の取得を行った上で実施しなければならない。また、リモートメンテナンス実施後は、報告書を提出しなければならない。

(13) 情報システムについての対策の見直し

情報システム責任者は、新たな脅威や脆弱性に対応すべく、庁内における横断的な改善も考慮し、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。

7. 4. 不正プログラム対策

(1) 統括情報セキュリティ管理者の措置事項

統括情報セキュリティ管理者は、不正プログラム対策として、次の事項を措置しなければならない。

①外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

②外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

④所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

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

情報システム責任者は、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情報システム責任者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。

②不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

- ③不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
- ④インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、村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、情報システム責任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、添付ファイルの開封やメール本文に記載された URL にアクセスしてはならない。
- ④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的実施しなければならない。
- ⑤添付ファイルが付いた電子メールを受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は無害化しなければならない。
- ⑥統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。
- ⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行い、直ちに CSIRT に報告しなければならない。
 - (ア) パソコン等の端末の場合
 - LAN ケーブルの即時取り外しを行わなければならない。
 - (イ) モバイル端末の場合
 - 直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

(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なければならない。

7. 5. 不正アクセス対策

(1) 統括情報セキュリティ管理者の措置事項

統括情報セキュリティ管理者は、不正アクセス対策として、以下の事項を措置しなければならない。

- ①使用されていないポートを閉鎖しなければならない。
- ②不要なサービスについて、機能を削除又は停止しなければならない。
- ③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ管理者及び情報システム管理者へ通報するよう、設定しなければならない。
- ④CSIRT は、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

- ⑤本村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。
- ⑥クラウドサービスを利用する際に、外部委託業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。
- ⑦パスワード等の認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本村の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

CSIRT 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、関係機関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

最高情報統括責任者、統括情報セキュリティ責任者及び統括情報セキュリティ管理者は、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

統括情報セキュリティ管理者及び情報システム責任者は、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

統括情報セキュリティ管理者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ責任者に通知し、適切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、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育、自動再生無効化等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

7. 6. セキュリティ情報の収集

(1) セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

- ①統括情報セキュリティ管理者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。
- ②統括情報セキュリティ管理者及び情報システム管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本村の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱

性に対する脆弱性管理の手順について、クラウドサービス事業者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、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然に防止するための対策を速やかに講じなければならない。

8 運用

8. 1. 情報システムの監視

(1) 情報システムの運用・保守時の対策

- ①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は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。
- ③情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。
- ④情報システム管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

- ⑤情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。
- ⑥情報システム管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。
 - (ア) サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除
 - (イ) クラウドサービス利用の終了手順
 - (ウ) バックアップ及び復旧

8. 2. 情報セキュリティポリシーの遵守状況の確認

(1) 遵守状況の確認及び対処

- ①情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CIS0、統括情報セキュリティ責任者及び統括情報セキュリティ管理者に報告しなければならない。
- ②CIS0 は、発生した問題について、適切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切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

CIS0、統括情報セキュリティ責任者、統括情報セキュリティ管理者及び CIS0 が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

(3) 職員等の報告義務

- ①職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに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報告を行わなければならない。
- ②違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性がある場合と統括情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

8. 3. 侵害時の対応等

(1) 緊急時対応計画の策定

- ①CIS0 又は情報セキュリティ委員会は、情報セキュリティインシデント、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切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。
- ②CIS0 又は情報セキュリティ委員会は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

(2) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

- ①関係者の連絡先

- ②発生した事案に係る報告すべき事項（事実関係）
- ③発生した事案への対応措置
- ④再発防止措置の策定
- (3) 事業継続計画との整合性確保
本村が自然災害、大規模・広範囲にわたる疾病等に備えて業務継続計画を策定する場合、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。
- (4) 緊急時対応計画の見直し
CISO 又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

8. 4. 例外措置

- (1) 例外措置の許可
情報セキュリティ責任者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、かつ、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、CISO の許可を得て、例外措置を取ることができる。
- (2) 緊急時の例外措置
情報セキュリティ責任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切に保管し、定期的に申請状況を確認しなければならない。

8. 5. 法令遵守

- (1) 職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。
 - ①地方公務員法(昭和 25 年法律第 261 号)
 - ②著作権法(昭和 45 年法律第 48 号)
 - ③不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)
 - ④個人情報の保護に関する法律(平成 15 年法律第 57 号)
 - ⑤行政手続における特定の個人を識別するための番号の利用等に関する法律(平成 25 年法律第 27 号)
 - ⑥サイバーセキュリティ基本法(平成 26 年法律第 104 号)
 - ⑦北塩原村個人情報保護法施行条例(令和 5 年北塩原村条例第 1 号)
- (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。

8. 6. 懲戒処分等

- (1) 懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、以下の法令又は条例等に基づいて懲戒処分も含めて罰則が科せられる場合がある。

- ①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
- ②住民基本台帳法
- ③地方公務員法
- ④北塩原村例規集 第4類 人事 第3章 分限・懲戒職員の懲戒の手續及び効果に関する条例

(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職員等が違反を確認した場合は、速やかに CIS0、統括情報セキュリティ責任者又は統括情報セキュリティ管理者に報告し、適切な措置を求めなければならない。
- ②CIS0、統括情報セキュリティ責任者又は統括情報セキュリティ管理者が違反を確認した場合は、当該職員等及びその監督責任者に通知し、違反の事実関係について報告を求めるとともに、当該職員等への指導など必要かつ適切な措置を講じなければならない。
- ③事実関係の報告及び事情聴取等により、当該職員等の故意又は重大な過失による違反であることを確認した場合又は監督責任者等の指導によっても改善されないと判断できる場合は、CIS0、統括情報セキュリティ責任者又は統括情報セキュリティ管理者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、当該職員等の権利を停止あるいは剥奪した者は、職員等の権利を停止あるいは剥奪した旨を CIS0、統括情報セキュリティ責任者、統括情報セキュリティ管理者及び当該職員等の監督責任者に通知しなければならない。

9 業務委託とクラウドサービスの利用

9. 1. 業務委託

(1) 業務委託判断基準の明確化

委託事業者に許可されていない情報の提供が行われないように、委託事業者に提供する情報に関する以下の事項を明確にしなければならない。

- ①業務委託を許可（又は禁止）する業務の範囲（委託事業者が開示できない情報を取り扱う業務は業務委託不可等）
- ②業務委託への提供を許可（又は禁止）する情報の範囲（委託業務に関係しない情報は提供不可等）
- ③情報資産の分類及び取扱制限その他提供する情報の特性に応じた情報の取扱いを許可（又は禁止）する場所（自治体機密性 3 情報は要管理対策区域外での取扱いを禁止するなど）

(2) 外部委託先の選定基準

- ①委託事業者の選定にあたっては、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、また、本村が果たすべき安全管理措置と同等の措置を講じることが可能なことを確認しなければならない。
- ②委託事業者の選定にあたっては、自治体機密性 3B 又は自治体機密性 3C の情報資産を取り扱う場合は、情報セキュリティマネジメントシステムの国際規格やプライバシーマークの取得状況、情報セキュリティ監査の実施状況等を参考にしなければならない。

③委託事業者の選定方法については、本対策基準に定めるもののほか、「公共 IT におけるアウトソーシングに関するガイドライン」（総務省平成 15 年 3 月）に準拠するよう努めなければならない。

(3) 契約項目

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

①情報セキュリティに関する規程、又はルールの策定とその遵守

②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

過去発生した重大トラブルが発生しないかを点検すると共に、異常を検出する機能を開発し、実装すること。

③個人情報の複製等の制限に関する取り決め

④委託事業者の責任者、委託内容、作業員、作業場所の特定

委託事業者の責任者や作業員を明確にするとともに、これらの者を変更する場合の手続を定めておき、担当者の変更を常に把握できるようにすること。また、情報資産の紛失等を防止するため、作業場所を特定し、特定個人情報については外部への持ち出しを禁止すること。

⑤提供されるサービスレベルの保証

通信の速度及び安定性、システムの信頼性の確保等の品質を維持するため、必要に応じて、サービスレベルを保証させること。

⑥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の実施

委託に関わる情報の種類を定義し、種類ごとのアクセス許可、アクセス時の情報セキュリティ要求事項並びにアクセス方法の監視及び管理を情報のライフサイクル全般で行う。

⑦委託事業者の従業員に対する教育の実施

委託事業者において、情報セキュリティに対する意識の向上を図るため、従業員に対し、教育を行うこと。

⑧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

委託事業者に提供した情報について、不正利用を防止させるため、業務以外での利用を禁止すること。

⑨業務上知り得た情報の守秘義務

業務中及び業務を終了した後も、業務上知り得た情報を漏らしてはならないこと。なお、委託事業者の事業主の誓約書を提出させること。

⑩再委託に関する制限事項の遵守

再委託を認める場合は、委託事業者から次の事項を記載した書面の提出を受け、再委託先事業者における情報セキュリティ対策が委託事業者と同等の水準であることを確認した上で、認めること。

(ア) 再委託の範囲

(イ) 作業手順

(ウ) 再委託先事業者の原因により生じた責任の所在

(エ) 再委託先事業者の事業主の誓約書

(オ) その他、情報セキュリティ責任者又は情報システム管理者が必要と認めた事項

⑪委託業務終了時の情報資産の返還、廃棄等

委託業務終了時に、不要になった情報資産を返却させるか廃棄させるかなど、その取扱いに

ついて明確に規定すること。

⑫委託業務の定期報告及び緊急時報告義務

定期報告及び緊急時報告の手順を定め、委託業務の状況を適切かつ速やかに確認できるようにすること。

⑬本村による監査、検査

委託事業者が実施する情報システムの運用、保守、サービス提供（クラウドサービス含む）等の状況を確認するため、当該委託事業者に対して、必要に応じて、監査及び検査を行うことを明確にすること。なお、再委託を行った場合は、当該委託事業者が再委託先に対して必要かつ適切な監督を行っているかどうかの監査も含まれる。

⑭本村による情報セキュリティインシデントの公表

委託業務に関し、情報セキュリティに関する情報セキュリティインシデントが発生した場合は、住民等に対し適切な説明責任を果たすため、当該情報セキュリティインシデントの公表を必要に応じて行うことについて、委託事業者と確認しておくこと。

⑮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）

委託事業者において、明記した情報セキュリティ要件が遵守されなかったため、被害を受けた場合は、当該委託事業者が損害賠償を行うことを契約上明記しておくこと。

(4) 業務委託実施期間中の対策

情報セキュリティ責任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。

①委託判断基準に従った重要情報の提供

②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（委託事業者の定期的な報告による確認を含む）及び措置の実施

③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 CIS0 に報告）

④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(3)の契約に基づく対処の要求

(5) 業務委託終了時の対策

情報セキュリティ責任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。

①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（委託事業者の報告による確認を含む）を含む検収

②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

9. 2. 情報システムに関する業務委託

(1) 情報システムに関する業務委託

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、情報システムに本村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。

- ①情報システムのセキュリティ要件の適切な実装
- ②情報セキュリティの観点に基づく試験の実施
- ③情報システムの開発環境及び開発工程における情報セキュリティ対策

(3) 情報システムの運用・保守を業務委託する場合の対策

- ①情報システム管理者は、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は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求めなければならない。

(4) 本村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責任者は、外部の一般の者が本村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責任者は、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責任者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。
- ④情報システム管理者は業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行わなければならない。
- ⑤統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。
- ⑥統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

9. 3. 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規程の整備

事業者等が不特定多数の利用者に対して提供する画一的な約款又は規約等への同意のみで利用可能となるクラウドサービスで自治体機密性2以上の情報は原則、インターネット環境で取り扱ってはならない。但し、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、当節「(3)クラウドサービスの選定」に示す情報セキュリティ対策が当該約款又は規約等で施されていることが定められ、政府情報システムのためのセキュリティ評価制度(ISMAP)に基づくクラウドサービスリストに登録されているクラウドサービスについては、統括情報セキュリティ責任者の承認を得ることで利用が可能である。

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

- ①クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準(以下9.3節において「クラウドサービス利用判断基準」という。)
- ②クラウドサービス提供者の選定基準

③クラウドサービスの利用申請の許可権限者と利用手続

④クラウドサービス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、以下を含むクラウドサービス（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。

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導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

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

③統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

(ア) クラウドサービスの利用終了時における対策

(イ) クラウドサービスで取り扱った情報の廃棄

(ウ) クラウドサービスの利用のために作成したアカウントの廃棄

(3) クラウドサービスの選定

①情報システム管理者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービスの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情報システム管理者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、以下のクラウドサービス提供者の選定基準に係る情報セキュリティ対策の実施情報を確認した上で、これらの基準に従ってクラウドサービス提供者を選定しなければならない。

(ア) サービス提供実績及び経営基盤等から信頼できる事業者が運用している。

(イ) サポート体制及び方法が明確である。

(ウ) クラウドサービスの利用を通じて本村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が禁止されている。

(エ) 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が明確である。

(オ) 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、本村の意図しない変更が加えられないための管理体制が構築されている。

(カ) 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が提供されている。

(キ) 情報セキュリティインシデントへの対処方法が定められている。

(ク) 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が定められている。

(ケ) 以下のセキュリティ要件を実装している、もしくは確認することができる。

- SSL サーバ証明書やSSHにより、通信データを暗号化している。

- ワンタイムパスワードや多要素（二段階）認証等の強固なユーザ認証により、厳格なアクセス制御を実施している。

- 脆弱性診断等によりセキュアなアプリケーション・OSを構築している。

- データの保管場所を明確にし、暗号化やバックアップの対策を行っている。

- ③情報システム管理者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、クラウドサービス提供者の選定条件に含めなければならない。
- ④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する。
- ⑤情報システム管理者は、クラウドサービスの利用を通じて本村が取り扱う情報の格付等を勘案し、必要に応じてクラウドサービス提供者のサービス利用規約等から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
 - (ウ) 情報資産に対する安全管理対策の十分性（受容可能性）
- ⑥情報システム管理者は、クラウドサービスの利用を通じて本村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、必要に応じて本村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。
- ⑦情報システム管理者は、クラウドサービスの特性、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 ※1
 - (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
- ⑧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情報システム管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件、また、施設の場所やリージョンの指定を調達仕様に含めなければならない。また、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、選定条件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手順が定められていることも調達仕様を含めなければならない。
- ②情報システム管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。

(5) クラウドサービスの利用承認

- ①情報セキュリティ責任者は、クラウドサービスを利用する場合には、情報システム管理者へクラウドサービスの利用申請を行わなければならない。
- ②情報システム管理者及び統括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。
- ③情報システム管理者は、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、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導入・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

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、前項において定める規程に対し、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、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
- (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) 設計・設定時の誤りの防止
- (キ) クラウドサービスを利用した情報システムの事業継続
- (ク) 仕様・設計・設定変更時の情報や変更履歴の管理

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、情報システム管理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、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又は保管
- (ウ) クラウドサービスの利用のために作成したアカウントの廃棄

②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。

※1：クラウドサービスを利用するにあたり、次の事項、及び(3)②(ケ)のセキュリティ要件を含めること。

- 目的外利用の禁止
- 本村の意図しない変更が加えられないための管理体制
- 情報セキュリティインシデントによる被害を最小限に食い止めるための対処方法(対処手順、責任分界、対処体制等)
- 格付及び取扱制限の明示、運搬又は送信、消去等の情報の取扱手順
- クラウドサービスに係るアクセスログ等の証跡の保存期間

9. 4. 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)

(1) クラウドサービスの利用に係る規程の整備

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

- ①クラウドサービスを利用可能な業務の範囲
- ②クラウドサービスの利用申請の許可権限者と利用手続
- ③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
- ④クラウドサービスの利用の運用手順

(2) クラウドサービスの利用における対策の実施

- ①職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で自治体機密性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情報システム管理者は、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. 5. ソーシャルメディアサービスの利用

①情報セキュリティ責任者は、本村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) 本村のアカウントによる情報発信が、実際の本村のものであることを明らかにするために、本村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行うこと。

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

- 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。

10 評価・見直し

10. 1. 監査

(1) 実施方法

CISO は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的に又は必要に応じて監査を行わせなければならない。

(2) 監査を行う者の要件

①情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

②監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

(3) 監査実施計画の立案及び実施への協力

①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

(4) 外部委託事業者に対する監査

①外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

②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はその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

(5) 報告

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

(6) 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

(7) 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。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責任者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

(8) 情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

10. 2. 自己点検

(1) 実施方法

①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、定期的に又は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、毎年度又は必要に応じ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。

10. 3. 情報セキュリティポリシー等の見直し

(1) 情報セキュリティ委員会は、情報セキュリティポリシーについて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ふまえ、毎年度評価を行い、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 CISO に報告しなければならない。

(2) 統括情報セキュリティ責任者は、情報セキュリティポリシーを見直した際には、その内容を職員等に周知しなければならない。

附則

このセキュリティポリシーは、令和8年3月16日から施行する。

改定履歴

施行日	区分	主な改定内容
平成17年10月28日	策定	北塩原村情報セキュリティポリシー策定
平成20年4月1日	改定	一部改定
平成23年6月1日	改定	一部改定
平成27年10月1日	改定	マイナンバー対応等、全面改定
令和3年10月1日	改正	組織体制・クラウドサービス対応等を追加し全面改正
令和5年11月1日	改正	情報システム全体の強靱性向上・業務委託規定等を追加し改正
令和8年3月16日	改正	地方自治法改正を踏まえた位置付けの整理、業務委託・クラウドサービス利用規定の整備、誤記等の修正