山江村
情報セキュリティポリシー

令和８年３月

目次

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、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（３）　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（４）　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（５）　機密性

情報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

人事給与、財務会計及び文書管理等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。

（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）　情報経路の分割

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

（１２）　無害化通信

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

３　対象とする脅威

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

（１）　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）　地震、落雷、火災等の災害によるサービス及び業務の停止等

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

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

４　適用範囲

（１）　行政機関の範囲

本基本方針が適用される行政機関は、山江村課設置条例で定める課等、山江村議会、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、会計室とする。

（２）　情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、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

５　職員等の遵守義務

職員、非常勤職員及び臨時職員（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。

6　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１）　組織体制

本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靭性の向上

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

サーバ等、情報システム室等、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、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速か

つ適正に対応するため、緊急時対応計画を策定する。

（８）　外部サービスの利用

外部委託する場合には、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、外部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。

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策をじる。

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、情報セキュリティポリシーの見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

８　情報セキュリティポリシーの見直し

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

９　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

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

なお、情報セキュリティポリシー（情報セキュリティ対策基準）及び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。

情報セキュリティ対策基準

1　対象範囲

本情報セキュリティ対策基準が適用される範囲は、次の通りとする。

（1） 行政機関の範囲

本対策基準が適用される行政機関は、山江村課設置条例で定める課等、山江村議会、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、会計室とし、各教育機関（事務室及び職員室は除く）は対象外とする。

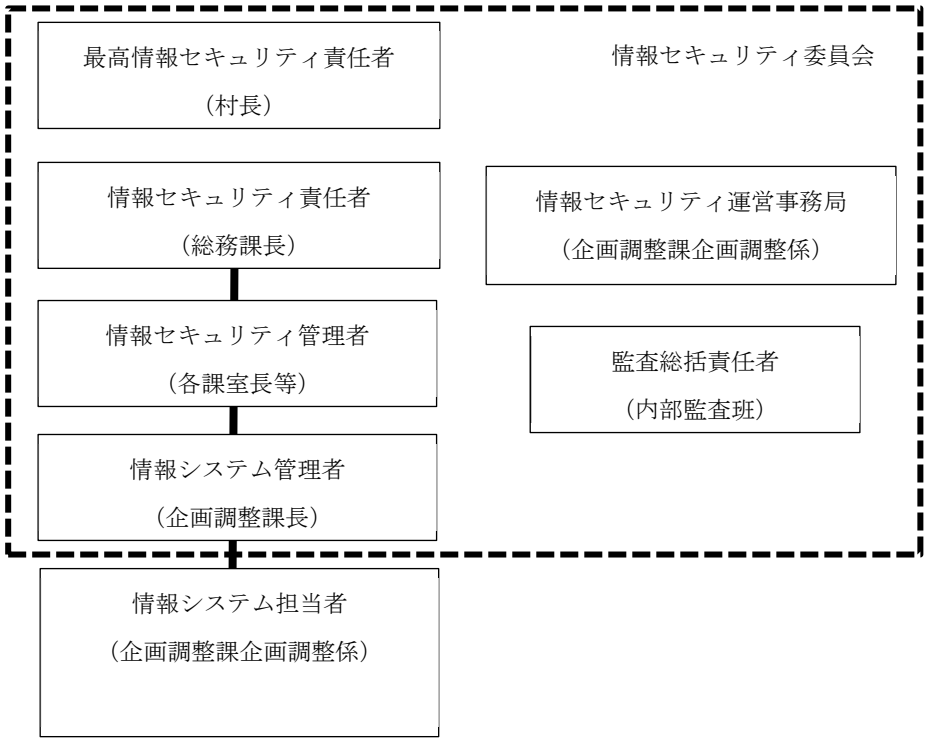
なお、各教育機関における教育のために用いるネットワーク及びシステム等は、この情報セキュリティポリシーの対象となるネットワーク及び情報システムと物理的に分けなければならない。

（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。

・ネットワーク、情報システム、これらに関する設備、電磁的記録媒体
・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。）
・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



体制内役職名	該当者
最高情報セキュリティ責任者（CISO: Chief Information Security Officer）	村長
情報セキュリティ責任者	総務課長
情報セキュリティ管理者	各課の長、**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及び議会**の課室長等
情報システム管理者	企画調整課長
情報システム担当者	企画調整課企画調整係
情報セキュリティ委員会	最高情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、CISO の指名する者
情報セキュリティ運営事務局	企画調整課企画調整係

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

ア　村長を CISO とする。CISO は、本村におけるすべてのネットワーク、情報システム等の情報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。

イ　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。

ウ　CISO 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　Resuponse Team、以下「CSIRT」という。）を整備し、役割を明確化する。

（2）情報セキュリティ責任者

ア　総務課長を、CISO 直属の情報セキュリティ責任者とする。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。

イ　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、見直し等を行う権限及び責任を有する。

ウ　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

ティ対策に関する権限及び責任を有する。

エ　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。

オ　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。

カ　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・管理を行う権限及び責任を有する。

キ　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、情報セキュリティ管理者及び情報システム管理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。

ク　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。

（3）情報セキュリティ管理者

ア　内部部局の各課室等の長、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及び議会の長を情報セキュリティ管理者とする。

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

ウ　情報セキュリティ管理者は、その所管する課室等において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。

エ　情報セキュリティ管理者は、その所管する課室等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員、非常勤職員及び臨時職員（以下、「職員等」という。）に対する教育、訓練、助言及び指示を行う。

ウ　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、情報セキュリティ責任者及び CISO へ速やかに報告を行い、指示を仰がなければならない。

（4）情報システム管理者

ア　企画調整課長を情報システム管理者とする。

イ　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。

ウ　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対策に関する権限及び責任を有する。

エ　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。

（5）情報システム担当者

ア　企画調整課企画調整係を情報システム担当者とする。

イ　情報システム担当者は、情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う。

（6）情報セキュリティ委員会

ア　情報セキュリティ委員会は、CISO を委員長に、情報セキュリティ責任者、情報セキュリティ管理者及び CISO が指名するメンバーで構成する。

イ　委員長は、委員会に関する一切の事務を統括し委員会を代表する。この場合において、委員会に事故がある時は総合政策課長がその職務を代理する。

ウ　委員会に内部監査班を設置し、CISO の指名する者を監査統括責任者とする。

エ　情報セキュリティ委員会は、本村の情報セキュリティ対策を統一的に行うため、情報セキュリティポリシーの運用、情報セキュリティ事故・事件への対応等、情報セキュリティに関する重要な事項を審議・決定する。

オ　情報セキュリティ委員会は、毎年度、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。

カ　委員会の庶務は、企画調整課企画調整係に設置された情報セキュリティ運営事務局において処理する。

（7）兼務の禁止

ア　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。

イ　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。

（8）CSIRT の設置・役割

ア　CISO は、CSIRT を整備し、その役割を明確化すること。

イ　CISO は、CSIRT に所属する職員を選任し、その中から CSIRT 責任者を置くこと。また、CSIRT 内の業務統括及び外部との連携等を行う職員を定めること。

ウ　CISO は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備すること。

エ　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こと。

オ　情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告すること。

カ　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。

キ　情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行なうこと。

3　情報資産の分類と管理方法

（1）情報資産の分類

対象となるネットワーク及び情報システムの情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

重要性分類
Ⅰ　個人情報及びセキュリティ侵害が本村の住民の生命、財産等へ重大な影響を及ぼす情報。
Ⅱ　公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。
Ⅲ　外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に軽微な影響を及ぼす情報。
Ⅳ　上記以外の情報。

（2）情報資産の管理

①管理責任

ア　情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

イ　情報資産が複製又は伝送された場合には、複製等された情報資産も（1）の分類に基づき管理しなければならない。

②情報資産の分類の表示

職員等は、情報資産について、格納する電磁的記録媒体のラベルに、情報資産

の重要性分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

③情報の作成

ア　職員等は、業務上必要のない情報を作成してはならない。

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

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

④情報資産の入手

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

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

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

⑤情報資産の利用

ア　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

イ　情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

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

⑥情報資産の保管

ア　情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

イ　情報セキュリティ管理者は、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は、重要な情報資産（重要性分類Ⅱ以上）を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦情報の送信

電子メール等により重要な情報資産（重要性分類Ⅱ以上）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　車両等により重要な情報資産（重要性分類Ⅱ以上）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　重要な情報資産（重要性分類Ⅱ以上）を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑨情報資産の提供・公表

ア　重要な情報資産（重要性分類Ⅱ以上）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　重要な情報資産（重要性分類Ⅱ以上）を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

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

⑩情報資産の廃棄

ア　重要な情報資産（重要性分類Ⅱ以上）を記録している電磁的記録媒体が不要になった場合には、電磁的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　重要な情報資産（重要性分類Ⅱ以上）を記載した文書を廃棄する場合には、情報が再読できないようにシュレッダー処分又は焼却処分等をしなければならない。

ウ　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

エ　情報資産の廃棄を行う者は、情報システム管理者の確認を得なければならない。

4　情報システム全体の強靭性の向上

（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。ただし、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。なお、外部接続先もインターネット等と接続してはならない。

②情報のアクセス及び持ち出しにおける対策

ア　情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また業務毎に専用端末を設置することが望ましい。

イ　情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

（2）LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分離

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

（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 への不適正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市区町村のインターネット接続口を集約する自治体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。

5　物理的セキュリティ

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

②サーバの冗長化

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、住民サービスに関するサーバ及びその他の基幹サーバについては、同一データを保持できるよう冗長化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、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、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は、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、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　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、配線収納管等を使用する等必要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には、関係部署が連携し速やかに対応しなければならない。

ウ　情報セキュリティ責任者は、ネットワーク接続口（ハブのポート等）は、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　情報セキュリティ責任者及び情報システム管理者は、自ら又は自らが認めた職員等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

ア　情報システム管理者は、サーバ等の機器の定期保守を実施しなければならない。

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、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

⑥庁外への機器の設置

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。また、必要に応じ当該機器への情報セキュリティ対策状況について確認しなければならない。

⑦機器の廃棄等

情報システム管理者は、機器の廃棄、リース返却等をする場合には、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）管理区域（サーバ室等）の管理

①管理区域の構造等

ア　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「サーバ室」という。）や電磁的記録媒体の保管庫をいう。

イ　情報セキュリティ責任者及び情報システム管理者は、管理区域を地下及び1階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。

ウ　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、管理区域から外部に通ずるドアは必要最小限とし、鍵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。

エ　情報セキュリティ責任者及び情報システム管理者は、サーバ室内の機器等には、転倒及び落下防止等の対策を講じなければならない。

オ　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。

カ　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

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ものに制限し、ICカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

イ　職員等及び外部委託事業者は、管理区域に入室する者は、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。

エ　情報システム管理者は、重要な情報資産（重要性分類Ⅱ以上）を扱うシステムを設置している管理区域には、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、機器等を搬入する場合には、既存の情報システムに与える影響について、あらかじめ確認しなければならない。

イ　情報システム管理者は、外部委託事業者がサーバ室の機器等の搬入出を行う場合には、職員等を立ち会わせなければならない。

（３）通信回線及び通信回線装置の管理

ア　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、適正に管理し、関連する文書を適正に保管しなければならない。

イ　情報セキュリティ責任者は、外部へのネットワーク接続は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。

ウ　情報セキュリティ責任者は、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。

エ　情報セキュリティ責任者は、重要な情報資産（重要性分類Ⅱ以上）を取扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

オ　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十分なセキュリティ対策を実施しなければならない。

カ　情報セキュリティ責任者は、重要な情報資産（重要性分類Ⅱ以上）を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

（4）職員等の利用する端末や電磁的記録媒体等の管理

ア　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。

イ　情報セキュリティ責任者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とする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、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。※推奨事項

エ　情報システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。

オ　情報システム管理者は、パソコンや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。※推奨事項

カ　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、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。

6　人的セキュリティ

（1）職員等の遵守事項

①職員等の遵守事項

ア　情報セキュリティポリシー等の遵守

全ての職員等は、情報セキュリティ管理者の指示に従い、情報セキュリティポリシーに定められている事項を遵守しなければならない。

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につい

ては、速やかに情報セキュリティ管理者に相談し、指示等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　モバイル端末や電磁的記録媒体等の端末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、重要な情報資産（重要性分類Ⅱ以上）を外部で処理する場合における安全管理措置を定めなければならない。

（イ）職員等は、本村のモバイル端末、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　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、業務上必要な場合は、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は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　持ち出し及び持ち込みの記録

情報セキュリティ管理者は、パソコン、モバイル端末及び電磁的記録媒体等の持ち出しについて、記録を作成し、保管しなければならない。

カ　パソコンやモバイル端末等におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末等のソフトウェアに関するセキュリティ機能の設定を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、離席時には、パソコン等の端末や電磁的記録媒体、情報が印刷された文書等が、第三者に使用又は許可なく閲覧されることがないように、パソコン、モバイル端末のロックや電磁的記録媒体、文書等が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

異動、退職等により職員等が業務を離れる場合には、利用していた情報を、

返却しなければならない。また、業務上知り得た情報はその後も漏らしてはならない。

②非常勤及び臨時職員への対応

ア　情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び臨時職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時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。

イ　情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び臨時職員の採用の際、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「情報セキュリティポリシー遵守同意書」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、非常勤及び臨時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

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

③ 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・保守等を外部委託事業者に発注する場合には、外部委託事業者から再委託を受ける事業者を含めて、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。

（2）研修・訓練

①情報セキュリティに関する研修

CISO は、毎年定期的に研修を実施しなければならない。

②研修計画の立案及び実施

ア　CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を行なわなければならない。

イ　研修計画において、職員等は適時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　新規採用の職員等に対しては、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、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　CISO は、毎年度 1 回、情報セキュリティ委員会に対して、職員等の情報セキュリティの実施状況について報告しなければならない。

③緊急時対応訓練

CISO は、必要に応じ緊急時対応を想定した訓練を実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を定め、効果的に実施できるようにしなければならない。

④研修・訓練への参加

情報セキュリティに関する研修・訓練には、すべての職員等が参加しなければならない。

（3）情報セキュリティインシデントの報告

①庁内での情報セキュリティインシデントの報告

ア　職員等は、情報セキュリティインシデントを認知した場合、「インシデント報告書（IT 障害)」により速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

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

ウ　情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、CISO 及び情報セキュリティ責任者に報告しなければならない。

②住民等外部からの情報セキュリティインシデントの報告

ア　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 CISO 及び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、報告のあった情報セキュリティインシデントについて、必要に応じて CISO 及び情報セキュリティ責任者に報告しなければならない。

エ　CISO は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

③情報セキュリティインシデントの原因究明・記録、再発防止等

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

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

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

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

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

（4）ID 及びパスワード等の管理

①IC 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　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　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。

②ID 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

ア　自己が利用している ID は､他人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（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。

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）。

7　技術的セキュリティ

（1）コンピュータ及びネットワークの管理

①ファイルサーバの設定等

ア　情報システム管理者は、職員等が使用できるファイル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、ファイル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、特定の者しか取り扱えないデータについては、別途ディレクトリを作成する等の措置を講じ、同一部署であっても、担当職員以外の者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

情報セキュリティ責任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は、サーバの冗長化対策にかかわらず、必要に応じてバックアップを実施しなければならない。

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には、その取扱に関する事項をあらかじめ、情報セキュリティ責任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は、作業記録を作成しなければならない。

イ　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、作業内容についての記録を作成し、詐取、改ざん等がないように適正に管理しなければならない。

ウ　情報セキュリティ責任者、情報システム管理者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

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が閲覧したり、紛失等がないよう、適正に管理しなければならない。

⑥ログの取得等

ア　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ために取得した記録は、詐取、改ざん、誤消去等されないよう適正に管理し、一定期間保存しなければならない。

イ　情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

ウ　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。

⑦障害記録

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　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は、設定の不整合が発生しないようファイアウォール、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　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。

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、電子申請の汎用受け付けシステム等、外部の者が利用できるシステムは、必要に応じ他のネットワーク及び情報システムと分離する等の措置を講じなければならない。

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、庁内の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 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　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ついては、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。

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

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、情報に脅威が生じることが想定される場合には、速やかに当該外部ネットワークとの接続を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　情報セキュリティ責任者は、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、適正なセキュリティ要件を策定しなければならない。

イ　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。

ウ　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

ア　情報セキュリティ責任者は、無線 LAN の利用を認める場合には、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　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は、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

⑭電子メールのセキュリティ管理

ア　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）が行われることがないよう、電子メールサーバの設定しなければならない。

イ　情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合には、メールサーバの運用を停止しなければならない。

ウ　情報セキュリティ責任者は、電子メールの送受信容量には上限を設定し、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　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には上限を設定し、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　情報セキュリティ責任者は、システム開発や運用等のため庁舎内に常駐す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は、委託先と

の間で利用方法を取りきめなければならない。

カ　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。

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

⑯電子署名・暗号化

ア　職員等は、情報資産の重要性分類に従い、その取扱いの際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。

イ　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。

ウ　CISO 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。

イ　職員等は、業務上の必要がある場合は、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、情報セキュリティ管理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。

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。

イ　職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報セキュリティ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無許可でのネットワーク接続の禁止

職員等は、情報セキュリティ責任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。

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　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。

（2）アクセス制御

①アクセス制御等

ア　アクセス制御

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、システム上制限しなければならない。

イ　利用者 ID の取扱い

（ア）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・抹消等の情報管理及び職員等の異動・出向・退職者に伴う利用者 ID の取扱等の方法を定めなければならない。

（イ）職員等は、業務上の必要がなくなった場合は、利用者登録を抹消するよう、情報セキュリティ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）情報セキュリティ責任者又は情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

ウ　特権を付与された ID の管理等

（ア）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 ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

（イ）情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、

情報セキュリティ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。

（ウ）CISO は、代行者を認めた場合、速やかに情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

（エ）情報セキュリティ責任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。

（オ）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 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。

（カ）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 ID を初期設定以外のものに変更しなければならない。

②職員等による外部からのアクセス等の制限

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、情報セキュリティ責任者及び当該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　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　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、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　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、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　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、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なければならない。

キ　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自動識別の設定

情報セキュリティ責任者及び情報システム管理者は、ネットワークで使用される機器について、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ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

⑤認証情報の管理

ア　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。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。

イ　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。

ウ　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。

⑥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。

（3）システム開発、導入、保守等

①情報システムの調達

ア　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。

イ　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が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　情報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。

イ　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。

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・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行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（エ）情報システム管理者は、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。

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、既に稼働している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。

④システム開発・保守に関連する資料等の整備・保管

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

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。

⑤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、故意また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。

⑥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。

⑦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。

⑧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の検証を行わなければならない。

（4）不正プログラム対策

①情報セキュリティ責任者の措置事項

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害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　所掌するサーバ及びパソコン等の端末には、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。

キ　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。

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の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、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。

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　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをLGWAN 接続系に取込む場合は無害化しなければならない。

カ　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。

キ　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、以下の対応を行わなければならない。

（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

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。

（５）不正アクセス対策

①情報セキュリティ責任者の措置事項

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

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、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　情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

②攻撃への対処

CISO 及び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なければならない。また、総務省、都道府県等と連絡を密にして情報の収集に努めなければならない。

③記録の保存

CISO 及び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禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

④内部からの攻撃

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

⑤職員等による不正アクセス

情報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

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

⑦標的型攻撃

情報セキュリティ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、標的型攻撃による庁内への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、庁内に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

（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収集・共有及びソフトウェアの更新等

情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

②不正プログラム等のセキュリティ情報の収集・周知

情報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

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

（1）情報システムの監視

①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。

③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を常時監視しなければならない。

（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

ア　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、問題が認められた場合には、速やかに CISO 及び情報セキュリティ責任者に報告しなければならない。

イ　CISO は、発生した問題について適正かつ速やかに対処しなければならない。

ウ　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は、定期的に確認を行い問題が発生していた場合には適正かつ速やかに対処しなければならない。

②パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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

④ 職員等の報告義務

ア　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報セキュリティ責任者及び情報セキュリティ管理者に報告しなければならない。

イ　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。

（３）侵害時の対応等

①緊急時対応計画の策定

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

②緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

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・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と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。

（4）例外措置

①例外措置の許可

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

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

③例外措置の申請書の管理

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

（5）法令遵守

職員等は、職務の遂行において使用する情報を保護するために、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(昭和二十五年十二月十三日法律第二百六十一号)
②　著作権法（昭和四十五年法律第四十八号）

③　不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）
④　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）
⑤　山江村個人情報保護条例（平成１７年３月２２日条例第２号）
⑥　山江村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に基づく個人番号の利用及び特定個人情報の提供に関する条例（平成２７年１２月１１日条例第２１号）
⑦　サイバーセキュリティ基本法（平成二十八年法律第三十一号）

（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監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

②違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

ア　情報セキュリティ責任者が違反を確認した場合は、情報セキュリティ責任者は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

イ　情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

ウ　情報セキュリティ管理者の指導によっても改善されない場合、情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

８　外部サービスの利用

（１）外部委託

①外部委託事業者の選定基準

ア　情報セキュリティ管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない

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、事業

者を選定しなければならない。

ウ　情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

②契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・外部委託事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・外部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
・外部委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・村による監査、検査
・村による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

③確認・措置等

情報セキュリティ管理者は、外部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定期的に確認し、必要に応じ、（２）の契約に基づき措置を実施しなければならない。また、その内容を情報セキュリティ責任者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

（２）約款による外部サービスの利用

①約款による外部サービスの利用に係る規定の整備

情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、重要性分類Ⅱ以上の情報が取扱われないように規定しなければならない。

ア　約款によるサービスを利用してよい範囲
イ　業務により利用する約款による外部サービス

ウ　利用手続及び運用手順

②約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、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約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

（3）ソーシャルメディアサービスの利用

①情報セキュリティ管理者は、本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）等を適正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重要性分類Ⅱ以上の情報はソーシャルメディアサービスで発信してはならない。

③利用するソーシャルメディアサービスごとの責任者を定めなければならない。

9　評価・見直し

（1）監査

①実施方法

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

②監査を行う者の要件

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。

③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、情報セ

キュリティ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。

④外部委託事業者に対する監査

外部委託事業者に委託している場合、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。

⑤報告

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

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

⑦監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

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。

（2）自己点検

①実施方法

ア　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、毎年及び必要に応じて自己点検を実施しなければならない。

②報告

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

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　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。

（3）情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。