

# 小川村情報セキュリティポリシー

## 対策基準

【令和8年 3月改訂】

## 目次

1 情報セキュリティ対策基準の位置付	4
2 情報セキュリティ対策基準の対象範囲	4
3 情報セキュリティの管理体制	4
(1) 最高情報セキュリティ責任者(CISO:Chief Information Security Officer)	4
(2) 統括情報セキュリティ管理者	4
(3) ネットワーク管理責任者	4
(4) 情報セキュリティ管理者	5
(5) 小川村セキュリティ委員会	5
(6) 兼務の禁止	6
(7) CSIRTの設置	6
4 情報資産の管理	7
(1) 情報の分類	7
(2) 情報の管理方法	7
5 情報システム全体の強靱性の向上	10
(1) 個人番号利用事務系	10
(2) LGWAN接続系	10
(3) インターネット接続系	11
6 物理的セキュリティ	11
(1) サーバ等	11
(2) 管理区域	12
(3) ネットワーク	12
(4) 端末等	13
7 人的セキュリティ	13
(1) 職員等	13
(2) 非常勤及び会計年度職員(臨時職員)	14
(3) 情報セキュリティポリシー等の掲示	14
(4) 委託事業者に対する説明	14
(5) 教育・訓練	14
(6) 事故、欠陥に対する報告及びCSIRT	15
(7) パスワードの管理	15
(8) ICカード等の管理	16
8 技術的セキュリティ	16
(1) コンピュータ、ネットワーク及び情報システムの管理	16

(2) ネットワーク及び情報システムを使用する際の規程	21
(3) アクセス制御	23
(4) 職員等による外部からのアクセス等の制限	24
(5) コンピュータ、情報システムの開発・導入・保守等	25
(6) コンピュータウイルス及びその他の悪意を持ったソフトウェアへの対策	26
(7) 不正アクセス対策	27
(8) セキュリティ情報の収集	28
9 運用	28
(1) 情報セキュリティポリシーの遵守状況の確認	28
(2) 緊急時対応計画	29
(3) セキュリティ障害時の対応	29
(4) 逸脱管理	31
(5) 法令等の遵守	31
(6) 情報セキュリティポリシーに関する違反に対する対応	32
10 外部サービス(クラウドサービス)の利用	32
(1) 業務委託先の選定基準	32
(2) 業務委託における管理事項	32
(3) 外部組織の情報システム等の利用における管理事項	33
(4) 外部サービス(クラウドサービス)の利用における管理事項(気密性2以上の情報を 取扱う場合)	33
(5) 外部サービス(クラウドサービス)の利用における管理事項(気密性2以上の情報を 取り扱わない場合)	38
(6) ソーシャルメディアサービスの利用	38
(7) Web会議サービスの利用時の対策	39
11 評価、見直し等	39
(1) 監査	39
(2) 自己点検	40
(3) 見直し	40

## 1 情報セキュリティ対策基準の位置付け

小川村の情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための小川村行政全般の情報資産に関する情報セキュリティ対策の基準である。

## 2 情報セキュリティ対策基準の対象範囲

情報セキュリティ対策基準の対象範囲は、情報セキュリティ基本方針第4条に定められた範囲とする。

## 3 情報セキュリティの管理体制

情報セキュリティの管理体制は以下の通りとする。

### (1) 最高情報セキュリティ責任者（CISO:Chief Information Security Officer）

(ア)最高情報セキュリティ責任者は、小川村におけるすべての情報資産の情報セキュリティを統括する最高責任者とし、副村長をもってこれに充てる。

(イ)最高情報セキュリティ責任者は、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によるアドバイザーを設置することができる。

### (2) 統括情報セキュリティ管理者

(ア)最高情報統括責任者を補佐し、小川村の情報セキュリティに対する統括的な権限及び責任を有する管理者とし、総務課長をもってこれに充てる。

(イ)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。

(ウ)統括情報セキュリティ管理者は、小川村の情報資産に対する侵害又は侵害の恐れがある場合には、最高情報統括責任者の指示に従い、最高情報統括責任者が不在の場合には自らの判断に基づき、必要かつ十分な全ての措置を行う権限及び責任を有する。

(エ)統括情報セキュリティ管理者は、小川村の全てのネットワーク、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、管理を行い、緊急時対応計画の策定及び見直しを行う。

(オ)統括情報セキュリティ管理者は、情報セキュリティに関する適切な管理及び運用を補佐する者を指名することができる。

### (3) ネットワーク管理責任者

村が管理するネットワーク、情報システムに対する統括的な権限及び責任を有する管理者とし、総務課長をもってこれに充てる。ネットワーク管理責任者の職務及び権限は、以下のとおりとする。

- (ア) 庁内ネットワーク、情報システムに関する情報セキュリティ実施手順の維持及び管理を行う。
- (イ) 情報セキュリティ管理者に対して、ネットワーク、情報システムに関する指導及び助言を行う権限を有する。
- (ウ) ネットワーク及び情報システムにおける適切な管理及び運用を補佐する者を指名することができる。

#### (4) 情報セキュリティ管理者

情報セキュリティの適切な管理及び運用を行うため、情報資産を取り扱う部署（課及びこれに準ずるものを含む）に、情報セキュリティに関する権限及び責任を有する情報セキュリティ管理者を置き、情報資産を取り扱う課等の長をもってこれに充てる。情報セキュリティ管理者の職務及び権限は、以下のとおりとする。

- (ア) 所掌する課等における情報資産及び部署ネットワークに対する侵害又は侵害の恐れのある場合には、最高情報セキュリティ責任者及び統括情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。
- (イ) 所掌する課等における情報セキュリティポリシーの遵守に関し、職員等に対し、教育・訓練・助言・指示を行わなければならない。
- (ウ) 所掌する課等が主管する情報システム、部署ネットワークにおける情報セキュリティに関しての権限及び責任を有し、適切な管理及び運用を行わなければならない。
- (エ) 使用する情報システムの機器や記録媒体について、第三者に使用させること又は許可なく情報を閲覧させることがないように、適切な措置を施さなければならない。
- (オ) 非常勤職員及び会計年度職員（臨時職員）の雇用時に情報セキュリティポリシーのうち、職員等が遵守すべき内容を非常勤職員及び会計年度職員（臨時職員）に理解させ、また実施及び遵守させなければならない。
- (ア) 部署内の情報セキュリティに関する適切な管理及び運用を補佐する者を指名することができる。

#### (5) 小川村セキュリティ委員会

- (ア) 小川村の情報セキュリティの維持管理を統一的な視点で行うため、小川村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、情報セキュリティ実施手順等の策定及び見直し、教育・研修、情報セキュリティ監査など、情報セキュリティに関する重要な事項を審議する。
- (イ) 統括情報セキュリティ管理者は委員長としてセキュリティ委員会を招集するとともに、委員会の議長を務める。
- (ウ) セキュリティ委員会の委員は統括情報セキュリティ管理者又はその補佐者の他、情報セキュリティ管理者又はその補佐者、及び必要と認めた者をもって組織する。

(エ) 統括情報セキュリティ管理者は、情報セキュリティに関する重要な事項を実践するため、必要と認めた者を構成員として、セキュリティ委員会に下部組織を設置することができる。

(オ) セキュリティ委員会の庶務は総務課で行う。

(カ) 情報セキュリティ委員会は、毎年度、村における情報セキュリティ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。

#### (6) 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。

#### (7) CSIRTの設置

ア 最高情報セキュリティ責任者は、情報セキュリティインシデントに対応するための体制CSIRT (Computer Security Incident Response Team)を整備し、その役割を明確にしなければならない。

イ 最高情報セキュリティ責任者は、CSIRTに所属する職員を選任し、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を定めなければならない。

ウ 最高情報セキュリティ責任者は、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署等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

エ CSIRTは、最高情報セキュリティ責任者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、その内容を関係部署等に提供しなければならない。

オ CSIRTは、情報セキュリティインシデントを認知した場合には、最高情報セキュリティ責任者、総務省、都道府県等へ、必要に応じて報告をしなければならない。

カ CSIRT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。

キ CSIRTは、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を必要に応じて行わなければならない。

#### 4 情報資産の管理

##### (1) 情報の分類

村における情報資産は、機密性に基づき次のとおり分類し、必要に応じ取扱い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
機密性 2	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産及び秘密文書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	<ul style="list-style-type: none"><li>・私物パソコンでの作業禁止</li><li>・必要以上の複製及び配付の禁止</li><li>・保管場所の制限、保管場所への必要以上の外部記録媒体等の持ち込み禁止</li><li>・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</li><li>・復元不可能な処理を施しての廃棄</li><li>・信頼のできるネットワーク回線の選択</li><li>・外部で情報処理を行う際の安全管理措置の規定</li><li>・外部記録媒体の施錠可能な場所への保管</li></ul>
機密性 1	機密性 2 の情報資産以外の情報資産	

##### (2) 情報の管理方法

###### (ア) 管理責任

- ① 情報は当該情報を作成した部署が管理責任を有し、当該部署の情報セキュリティ管理者を情報管理責任者とする。
- ② 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。

###### (イ) 情報の作成

- ① 職員等は、業務上必要のない情報を作成してはならない。
- ② 情報を作成する者は、情報の作成時に (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。
- ③ 情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しな

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。

(ウ) 情報資産の入手

- ① 庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
- ② 庁外の者が作成した情報資産を入手した者は、(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。
- ③ 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

(エ) 情報資産の利用

- ① 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない
- ② 情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。
- ③ 情報資産を利用する者は、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。
- ④ 取り外し可能な記録媒体を再利用する際には、記録されていた情報が復元できないよう措置を実施した上で、利用しなければならない。

(オ) 情報資産の保管

- ① 情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。
- ② 情報セキュリティ管理者は、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。
- ③ 情報セキュリティ管理者は、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、自然災害を被る可能性が低い地域に保管するよう配慮しなければならない。
- ④ 情報セキュリティ管理者は、機密性2の情報を記録した外部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するよう配慮しなければならない。また、特に重要なものについては、別の記録媒体に複製を作成し、複製された当該媒体は、保管場所とは異なる場所に別途保管しなければならない。

(カ) 情報の送信

電子メール等により機密性2の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

(キ) 情報資産の運搬

- ① 車両等により機密性2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。
- ② 機密性2の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

(ク) 情報資産の提供・公表

- ① 情報を公表する際は、当該情報が機密性1の情報であることを確認しなければならない。
- ② 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。
- ③ 機密性2の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。
- ④ 情報セキュリティ管理者は、住民等に公開する情報資産について、完全性を確保するため、改ざん、消去等から保護するために必要な措置を取らなければならない。
- ⑤ 機密性2の情報資産を外部に提供する者は、法令等の定めによるもの以外については、事前に提供先との間で守秘義務等を記載した契約を交わす等の保護措置を実施しなければならない。

(ケ) 情報資産の廃棄

- ① 機密性2の情報資産を廃棄やリース返却等をする者は、情報を記録している記録媒体について、記録媒体の初期化、破壊等、情報を復元できないように処置しなければならない。
- ② 情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録する等、その重要度に応じた適切な対応をしなければならない。
- ③ 情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

(コ) 書類、入力原票、出力帳票等の管理

- ① 書類、入力原票、出力帳票等（以下「書類等」という。）は、記載された情報の分類により、適切に管理しなければならない。
- ② 保管する際には、第三者による閲覧、盗難、改ざん等から保護できる安全な場所で管理しなければならない。
- ③ 機密性2の情報が記録された書類等が不要となった場合は、焼却、裁断、溶解等により復元できないものとして廃棄しなければならない。また、廃棄処理を外部業者に委託する場合、信頼できる業者を選定し、守秘義務等を記載した契約を取り交わして、管理しなければならない。
- ④ 複写、印刷等の際、入出力された書類等を放置してはならない。
- ⑤ 機密性2の情報が記録された書類等を外部に送付する場合は、不要な情報が識別できないよう措置を実施しなければならない。また、職員等又は信頼できる外部業者を選定し、複製の禁止、書類の物理的な保護、盗難対策等の措置を講じなければならない。
- ⑥ 機密性2の情報が記録された書類等を再利用してはならない。
- ⑦ その他、上記に規定するもののほか、小川村文書取扱規程（平成14年規程第3号）に基づき、管理を行わなければならない。

## 5 情報システム全体の強靱性の向上

### (1) 個人番号利用事務系

ア 個人番号利用事務系と他の領域との間で通信が行えないよう分離しなければならない。ただし、個人番号利用事務系からL G W A N等を経由して外部との通信を行う必要がある場合、ファイアウォール等で送信元・送信先及びアプリケーションプロトコルを特定通信として限定しなければならない。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い。

イ 情報のアクセス及び持ち出しに対し、以下を実施しなければならない。

- ① 情報システムが正規の利用者を識別するための認証方式として、二つ以上の手段を併用した多要素認証を利用しなければならない。
- ② 原則として、U S Bメモリ等の持ち運び可能な記録媒体による端末からの情報持出しができないように設定しなければならない。

### (2) L G W A N接続系

ア L G W A N接続系とインターネット接続系は両環境の通信を分離した上で、必要な通信のみを特定通信として許可できるようにしなければならない。また、メールやデータをインターネット接続系からL G W A N接続系に取り込む場合には、無害

化を実施しなければならない。

### (3) インターネット接続系

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

イ 市区町村のインターネット接続口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、その運営主体、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。

## 6 物理的セキュリティ

### (1) サーバ等

サーバ等は、当該機器で稼働する情報システムを管理する情報セキュリティ管理者により、以下のように管理されなければならない。なお、複数の情報システムが稼働する等の場合、ネットワーク管理責任者が同様に管理を行わなければならない。

(ア)サーバ等及びネットワーク機器のうち特に重要なものを設置する場合、火災、水害、地震、埃、集荷物衝突等の影響を可能な限り排除した場所に設置し、温度、湿度を許容範囲に保ち、耐震処理を施した上で、容易に取り外せないよう適切な固定等の措置を施さなければならない。

(イ)サーバはその重要度に応じて、本体の二重化あるいは外部記憶を二重化する等により、システムの運用の停止やデータ等の消失に対処する措置を行わなければならない。また、正確かつ安定的な稼働のために、定期的に保守を実施し、その記録を保管しなければならない。

(ウ)停電及び電圧異常等によりデータ等が破壊され、業務運用に支障を来す恐れのあるサーバ等の電源は、通常運転に十分な条件で供給されなければならない。また、当該装置を適切に停止するまでの間に必要な電力を供給する容量を持つ予備電源を備える等の措置を施さなければならない。さらに、落雷等による過電流からサーバ等の機器を保護する措置を講じなければならない。

(エ)配線は、傍受又は損傷等を受けることのないよう可能な限り必要な措置を施し、主要な箇所については、定期的に損傷等に関する点検を行わなければならない。

(オ)外部に設置する装置は、最高情報セキュリティ責任者の承認を受けたものでなければならない。また、最高情報セキュリティ責任者は、定期的に当該装置の情報セキュリティの水準について確認しなければならない。

(カ)特に重要な情報資産を取り扱うサーバにおいては、時間外の不正な利用から保護するため、運転時間を定め、不要な時間帯には自動的に停止するようにしなければならない。

## (2) 管理区域

(ア)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、当該装置の管理、運用を行う部屋（以下サーバ室という）は、外部から容易に侵入ができない措置を施した部屋としなければならない。また、サーバ室から外部に通ずる扉は1ヶ所のみとし、施錠により許可されない立入りを防止する措置を取らなければならない。

(イ)サーバ室に設置が困難なサーバについては、施錠されたラック（サーバキャビネット）に収納する、あるいは人の出入りが少ない部屋に設置し職員等が不在になる際には施錠する等、外部からの脅威に対して保護する措置を施さなければならない。

(ウ)サーバ室の入退室は、許可された者のみとし、入退室管理簿の記載等を行わなければならない。また、サーバ室内での作業内容は事前にネットワーク管理責任者の承認を得たもののみとしなければならない。

(エ)サーバ室へ機器等を搬入する場合及び委託業者がサーバ室にて作業を行う場合は、作業者に身分証明書等の提示を求め確認し、できるだけ職員等が立ち会う等の措置を施さなければならない。

(オ)サーバ室においては、ネットワーク管理責任者の許可無く、写真、ビデオの撮影、録画等を禁止する。

(カ)サーバ室はその場所及び存在を明らかにする標識を建物の内外を問わず表示してはならない。

(キ)サーバ室には危険物、不要な機材等を持ち込んで서는ならない。

## (3) ネットワーク

(ア)外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続点を1ヶ所とし、必要な場合には容易に切り離せるものとしなければならない。

(イ)ネットワークの配線は、傍受又は損傷等を受けることのないよう可能な限り必要な措置を施し、主要な箇所については、定期的に損傷等に関する点検を行わなければならない。また、不正に接続できないようハブなどに可能な限り必要な措置を施さなければならない。

(ウ)主要な通信回線には、落雷等から接続された機器を保護する措置を講じなければならない。

#### (4) 端末等

- (ア)職員等は執務室に職員等が不在となる場合には、入り口に施錠するなど部外者の侵入を防止する措置や、軽量端末盗難防止の対策などを施さなければならない。
- (イ)第三者の立ち入りが可能な場所から視認できる端末等のディスプレイには、設置方法の改善、必要に応じて左右からの覗き込みを防止するフィルターを装備する等、情報漏洩対策に配慮しなければならない。

### 7 人的セキュリティ

#### (1) 職員等

- (ア)職員等は、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に定められている事項を理解し、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及び遵守することが困難な点がある場合は、速やかに情報セキュリティ管理者に相談し、指示等を仰がなければならない。
- (イ)職員等は使用する端末や記録媒体について、第三者に使用されること、また許可なく情報資産を閲覧されることがないように、適切な措置を施さなければならない。
- (ウ)職員等は情報セキュリティ管理者の許可を得ず、端末等を執務室外に持ち出してはならない。許可により、持ち出して作業を行う際には、情報資産の漏洩、紛失、盗難等に対して、適切な措置を施さなければならない。
- (エ)職員等は、取り外し可能な記録媒体等を外部に持ち出すことを原則として禁止する。ただし、職務上やむを得ない理由がある場合、情報セキュリティ管理者の許可を得て、持ち出すことができる。その際、情報資産の漏洩、紛失、盗難等に対して、適切な措置を施さなければならない。
- (オ)職員等は異動等により業務を離れる場合、及び退職する場合には、知り得た情報資産を他に漏らしてはならない。
- (カ)職員等は、庁舎の内外を問わず、電話等による通話又は会話等の際には、第三者による傍受等を考慮して、情報漏えい等の防止に配慮すること。また、ファクシミリ等による情報送信の際には、誤送信等の防止に配慮しなければならない。
- (キ)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。
- (ク)職員等は外部で情報処理作業を行う際、私物パソコンを用いる場合には、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。また、機密性2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。

(2) 非常勤及び会計年度職員（臨時職員）

- (ア) 非常勤職員及び会計年度職員（臨時職員）には、雇用及び契約時に必ず情報セキュリティポリシーのうち非常勤職員及び会計年度職員（臨時職員）が遵守すべき内容を理解させ、実施及び遵守させなければならない。
- (イ) 非常勤及び会計年度職員（臨時職員）には、雇用及び契約の際、必要な場合は情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。
- (ウ) 非常勤職員及び会計年度職員（臨時職員）に端末による作業を行わせる場合には、使用できる機能は必要最低限とし、不要な機能についてはこれを利用できないように設定しなければならない。

(3) 情報セキュリティポリシー等の掲示

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の周知徹底をはかるため、職員等に対して、情報セキュリティポリシー及びその説明資料を適切に公開しなければならない。また、情報セキュリティポリシーが改訂された際にも、同様に公開しなければならない。

(4) 委託事業者に対する説明

統括情報セキュリティ責任者は、ネットワーク及び情報システムの開発・保守等を委託事業者が発注する場合、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委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

(5) 教育・訓練

- (ア) 統括情報セキュリティ管理者は、職員等に対し情報セキュリティポリシーについて啓発に努めるとともに、職員等を対象とした情報セキュリティ及びサイバーセキュリティに関する研修を設けなければならない。また、不正アクセス、不正プログラム、標的型攻撃等の被害を受けた場合の対応について、定期的に確認または訓練等を実施するよう配慮しなければならない。
- (イ) 研修及び訓練は、各管理者、その他職員等の職務と役割、理解度等に応じたものとしなければならない。
- (ウ) 職員等は、毎年度最低1回は情報セキュリティ及びサイバーセキュリティに関する研修を受講し、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理解し、情報セキュリティ上の問題が生じないようにしなければならない。
- (エ) 情報システムの開発・保守・運用管理に携わる職員等は、担当者として必要

な技術力を習得及び維持するための研修を受けなければならない。

#### (6) 事故、欠陥に対する報告及びC S I R T

- (ア)職員等は、情報セキュリティに関する事故、情報システム上の欠陥及び誤動作等を発見した場合には、速やかに情報セキュリティ管理者に報告し、その指示に従って必要な措置を講じなければならない。また、住民等外部から、村が管理する情報資産に関連する事故及び欠陥について、報告を受けた場合も同様にしなければならない。
- (イ)情報セキュリティ管理者は、報告のあった事故等について、全て最高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C S I R Tに報告しなければならない。
- (ウ)C S I R Tは、関係する情報セキュリティ管理者に対して、被害の拡大防止等を図るための応急措置の実施及び復旧に関わる指示を行わなければならない。
- (エ)C S I R Tは、これらの事故等を分析し、再発防止のための情報として記録を保存しなければならない。欠陥、誤動作等に関しては、その情報システムの利用者に対して通知し、注意を喚起しなければならない。その他、必要に応じて、各責任者等に指示を行い、また、再発防止のため必要であるならば、セキュリティ委員会を招集し、対策等の協議を行わなければならない。

#### (7) パスワードの管理

職員等は、自己の保有するパスワードについて、次の事項を遵守しなければならない。

- (ア)パスワードを秘密にし、パスワードの照会は一切応じないこと。
- (イ)パスワードのメモを作らない、又は、メモを他の者の目に触れないよう適切に管理すること。
- (ウ)パスワードの長さは十分な長さとし、容易に推測されない文字列にすること。
- (エ)パスワードは、定期的に変更し、古いパスワードの再利用はしないこと。
- (オ)仮のパスワードは最初のログイン時点で変更すること。
- (カ)端末にパスワードを記憶させないこと。
- (キ)認可されたグループでの利用者識別以外のパスワードを職員等の間で共有しないこと。また、当該グループに対する利用者識別で使用するパスワードは、グループに属さない者に漏らさないこと。
- (ク)パスワードが流出した、あるいはその恐れがある場合には、当該パスワードにかかわる管理者に報告の上、速やかにパスワードの変更を行うこと。

## (8) ICカード等の管理

職員等は、自己の管理するICカード等について、次の事項を遵守しなければならない。

- (ア) 認証に用いるICカード等は、複数の職員等の中で共有しないこと。
- (イ) ICカード等は安全に管理し、盗難、紛失、他者による利用等がないようにすること。
- (ウ) ICカード等は、カードリーダ等に常時挿入したままにしないこと。
- (エ) ICカード等を紛失した場合、直ちに情報セキュリティ管理者及び統括情報セキュリティ管理者に報告し、その指示を仰ぐこと。

## 8 技術的セキュリティ

### (1) コンピュータ、ネットワーク及び情報システムの管理

#### (ア) 情報システム及び情報資産の管理責任

情報セキュリティ管理者は、所掌する情報システム及び部署ネットワークを管理する責任を有する情報システム管理者とする。ただし、全体的に利用する情報システム又は部署ネットワーク以外のネットワークに関しては、ネットワーク管理責任者を情報システム管理者とする。

#### (イ) ファイル共有等

サーバに文書等の情報を保存する場合は、そのデータの閲覧及び使用は権限のある者のみが行えるように設定しなければならない。

#### (ウ) バックアップの取得

① 情報システム管理者は、サーバ等に格納された情報については、二重化措置等にかかわらず、必要に応じて、定期的に取り外し可能な記録媒体へのバックアップを取り、施錠等のできる安全な場所へ保管し、記録内容の劣化及び破損を防止できるようにしなければならない。バックアップに使用する記録媒体については、定期的に新品に交換すると共に、品質の劣化が予想される場合や劣化が原因と想定される障害が発生した場合は直ちに新品の媒体に交換を行わなければならない。そのため、バックアップの実行記録等から、記録媒体の劣化や機器の障害を確認しなければならない。

#### (エ) システム管理記録及び作業の確認

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。

#### (オ) 仕様書等の管理

① 情報システム管理者は、情報システムの開発及び導入を行う場合は、ソフトウェアの仕様書、ネットワーク構成図等を整備しなければならない。また、変更作業を実施した際には、その作業を記録し、適切に管理しなければならない。

ない。

- ② 情報システム管理者は、情報システムの仕様書、ネットワーク構成図等を業務上必要とする者のみが閲覧できる場所に保管しなければならない。
- ③ 情報セキュリティ管理者は、最新の部署ネットワークの構成図等を、ネットワーク管理責任者に提出しなければならない。

(カ) アクセス記録の取得

- ① 情報システム管理者は、アクセス記録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。また、必要に応じて、取り外し可能な記録媒体にバックアップしなければならない。
- ② 情報システム管理者は、アクセス記録及び情報セキュリティの確保に必要な記録が、窃取、改ざん又は消去されないように必要な措置を施さなければならない。
- ③ 情報システム管理者は、正確な記録の保持のため、コンピュータ及びネットワーク機器等の時刻を正確に保たなければならない。

(キ) 障害記録の作成

- ① 情報システム管理者は、職員等から報告のあった障害等の記録を作成し、一定の期間保存しなければならない。

(ク) 公共端末

- ① 情報システム管理者は、職員等以外の者が利用できる情報システムについては、情報セキュリティ対策について特に強固な対策を取らなければならない。
- ② 情報システム管理者は、公共端末の利用状況を確認し、設定変更の実施や無許可のソフトウェアの導入などが行われていないか等を、定期的に確認しなければならない。
- ③ 情報システム管理者は、公共端末については、必要最小限の機能のみとし、故意あるいはミスによる誤操作等が起こらないよう配慮しなければならない。

(ケ) 情報機器、サービス等のパスワード等の管理

- ① 情報システム管理者は、情報機器の ID、パスワードを厳重に管理しなければならない。
- ② 情報システム管理者は、ネットワーク並びにネットワーク上で利用する各種サービスの ID、パスワードを適切に管理しなければならない。

(コ) 庁内ネットワークの管理等

- ① ネットワーク管理責任者は、そのネットワークで利用される情報資産の重要性、利用権限等を考慮して、不正アクセスの防止等のため、不必要なネットワークサービスにアクセスできないよう、必要に応じてネットワークの分割を行い、ネットワーク内や複数のネットワーク相互間に接続制御や経路制御を実施しなければならない。

- ② ネットワーク管理責任者は、ネットワークの接続制御や経路制御に使用される機器やソフトウェアの設定に際しては、不整合の発生を抑えるよう設定を行うとともに、それらの機器やソフトウェアの管理情報、設定情報等は、安全に管理しなければならない。
- ③ 庁内ネットワークは、外部組織との接続箇所を除き、部外者が利用するネットワークと共用してはならない。やむを得ない理由により、ネットワークを共用する場合は、部外者が庁内ネットワークにアクセスできないよう経路制御等の必要な措置を講じなければならない。
- ④ 庁内ネットワークへの外部からのアクセスの許可は、必要最低限とし、必要な時のみ接続可能とする等の配慮を行わなければならない。
- ⑤ 外部との接続に際して公衆網を利用する場合には、着信の禁止、発信者番号による管理、コールバック、認証等により、不正な接続を防止する措置を施さなければならない。

(サ) 外部ネットワークとの接続

- ① ネットワーク管理責任者は、外部ネットワークとの接続に際しては、当該外部ネットワークのネットワーク構成、機器構成、情報セキュリティレベル等を詳細に検討し、村の情報資産に影響が生じないことを明確に確認したうえで、統括情報セキュリティ管理者の許可に基づき接続しなければならない。また、その際は責任の分界点を明確にしなければならない。
- ② ネットワーク管理責任者は、外部ネットワークとの接続を行うことで内部ネットワークの安全性が脅かされることの無いようにセキュリティ対策に努めなければならない。
- ③ 接続した外部ネットワークの情報セキュリティに問題が認められた場合には、ネットワーク管理責任者は、速やかに当該外部ネットワークとの接続を切断する等の手段により物理的に遮断しなければならない。
- ④ 内部ネットワークの情報セキュリティに問題が認められた場合には、ネットワーク管理責任者は速やかに当該内部ネットワークを、外部ネットワークから遮断しなければならない。
- ⑤ 外部ネットワークの接続に際し、その接続条件等が定められている場合には、当該条件等に従わなければならない。

(シ) インターネットとの接続

- ① ネットワーク管理責任者は、インターネットとの接続の際は、ファイアウォール等による不正アクセスを防止など情報セキュリティに留意した措置を取らなければならない。

- ② 機密性2に該当する情報を格納したサーバ等からのインターネットへのアクセスは禁止する。ただし、インターネットを利用した情報システムのうち住民等の利用に供するもの及び業務上やむを得ない理由のあるもので情報の保護に必要な措置を実施しているものについては、統括情報セキュリティ管理者及びネットワーク管理責任者の承認の上で利用を認める。
- ③ ネットワーク管理責任者は、インターネットからのアクセス可能な範囲は、公開用のサーバ類にのみ限定し、それ以外の機器、ネットワークへのアクセスができないような措置を取らなければならない。
- ④ ネットワーク管理責任者は、インターネットとの接続について、アクセス記録や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。
- ⑤ インターネットからのセキュリティ侵害の恐れがある場合、ネットワーク管理責任者は、直ちにインターネットとの接続を切断しなければならない。

(ス) インターネット等を利用した情報システム

インターネットを利用して、情報公開、申請、入札、施設予約等を住民等の利用に供する情報システム及び音声、ファクシミリ等を利用して情報公開等を行う情報システムを運用する場合は、以下の措置を取らなければならない。

- ① 情報の漏洩、改ざん等から保護する措置を行うこと。
- ② 公開する情報に対しては、情報セキュリティ管理者による承認を必要とし、完全性の確保に留意して行うこと。
- ③ 個人を識別する必要がある情報システムについては、公的個人認証あるいは事前の利用申請等を利用した本人確認の機能を備えなければならない。その際、通信内容は暗号化を行い、盗聴、漏洩、改ざん等から保護しなければならない。また、なりすまし、否認等を防止する機能を備えなければならない。
- ④ 利用者の識別に基づきアクセス範囲及び権限設定を厳格に行わなければならない。
- ⑤ 不要な機能を稼働させないようにしなければならない。
- ⑥ 電子的な文書を使用する際には、必要に応じて電子署名の付与等を行い、その真正性及び完全性を保護しなければならない。
- ⑦ オペレーションシステム、情報システム等におけるセキュリティ上の問題点は速やかに対策を行わなければならない。
- ⑧ コンピュータウイルスあるいは悪意を持ったプログラム等の侵入を防止する措置を取らなければならない。
- ⑨ 利用記録、アクセス記録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。その際、正確な情報が記録されるよう機器等の時刻同期を行い、また、記録等は改ざん、消去等から保護する措置

を施さなければならない。

- ⑩ インターネットからのセキュリティ侵害の恐れがある場合、ネットワーク管理責任者は、直ちに当該システムの利用を停止し、インターネットとの接続を切断しなければならない。
- ⑪ ネットワーク管理責任者は、当該システムの安全性について、定期的に確認しなければならない。

#### (セ) 電子メールのセキュリティ管理

- ① ネットワーク管理責任者は、権限のない利用者により外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。
- ② ネットワーク管理責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。
- ③ ネットワーク管理責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。
- ④ ネットワーク管理責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。
- ⑤ ネットワーク管理責任者は、システム開発や運用等のため事務所に常駐している委託事業者の作業員による電子メールアドレス利用について、委託先との間で利用方法を取り決めなければならない。
- ⑥ ネットワーク管理責任者は、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を防止するために、電子メールの利用記録あるいは電子メールそのものの保管、添付ファイルの監視等によりシステム上措置するよう配慮しなければならない。

#### (ソ) 複合機のセキュリティ管理

- ① ネットワーク管理責任者は、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、適切なセキュリティ要件を策定しなければならない。
- ② ネットワーク管理責任者は、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 ネットワーク管理責任者は、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。

(タ) 特定用途機器のセキュリティ管理

- ① ネットワーク管理責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(チ) 無線LANのセキュリティ管理

- ① ネットワーク管理責任者は、無線LANの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付ける等の盗聴及び不正接続に対する措置を講じなければならない。

(2) ネットワーク及び情報システムを使用する際の規程

(ア) 業務目的以外の使用の禁止

- ① 職員等は、業務目的以外での情報システムへのアクセス、ウェブの閲覧及びメールの使用等を行ってはならない。
- ② 職員等が、業務目的外の使用を行っていることを発見した場合には、当該職員等の所属部署における情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

(イ) ソフトウェアの導入に関する注意

- ① 職員等は、新たにソフトウェアを導入する場合は、ネットワーク管理責任者の許可を得なければならない。
- ② 職員等は、正規のライセンスのないソフトウェアを導入してはならない。
- ③ 職員等は、業務上不必要なソフトウェア及び出所不明なソフトウェア等安全性が確認されないソフトウェアをインストールしてはならない。
- ④ 職員等は、導入されているソフトウェアを適切に運用管理しなければならない。

(ウ) ファイル共有等

- ① サーバに文書等の情報を保存する場合、そのデータの閲覧及び使用は権限のある者のみが行えるように設定しなければならない。

(エ) 電子メールの送受信等

- ① 職員等は、メールの自動転送機能を用いて、業務上不必要な者へ職場のメールを転送してはならない。
- ② 職員等は、チェーンメールや不審なメールを他者に転送してはならない。
- ③ 職員等は、機密性2の行政情報に該当する情報をインターネットを利用したメールに添付して送信してはならない。

- ④ 職員等は、機密性2の行政情報に該当する添付ファイルのあるメールを送信する必要がある場合には、事前に情報セキュリティ管理者の承認を受けなければならない。
- ⑤ 職員等は、差出人が不明な、又は不自然なファイルが添付されたメールを受信した場合は、直ちに廃棄しなければならない。また、開封した電子メールに不審な点がある場合、直ちに情報セキュリティ管理者に報告しなければならない。
- ⑥ 電子メールを送信する場合は、送信先のメールアドレス入力が間違いないか確認をしなければならない。また、重要なメールを誤送信した際には、直ちに情報セキュリティ管理者に報告しなければならない。
- ⑦ 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。

#### (オ) 職員等が個人で所有する機器の設置

- ① 職員等は、統括情報セキュリティ責任者の許可なく、個人で所有する機器を設置、又は、小川村のネットワークに接続してはならない。ただし、職務上やむを得ない場合、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。
- ② 職員等は、外部から取り外し可能な記録媒体を持ち込んで、小川村に設置された機器で、利用してはならない。ただし、職務上やむを得ない場合、情報セキュリティ管理者の許可を得て、コンピュータウイルス等に感染していないことを確認の上、利用することができる。

#### (カ) 機器構成の変更

- ① 職員等は、情報システムの機器について業務を遂行するため機器の増設・交換を行う必要がある場合には、ネットワーク管理責任者の許可を得なければならない。
- ② 職員等は、モデム等の機器を増設して、他のネットワークへ接続を行う場合及び他のネットワークからアクセスを可能とする仕組みを構築する場合には、ネットワーク管理責任者の許可を得なければならない。ネットワーク管理責任者は、許可に当たって情報システム及び他の情報システムにセキュリティ上の問題を生じさせてはならない。

#### (キ) 情報システムの入出力データ

- ① 職員等は、情報システムに入力されるデータの適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

- ② 職員等は、情報システムから出力されるデータの処理が正しく行われていることを確認しなければならない。

(ク) 離席時等の対応

- ① 職員等は、離席時等には、端末をロックするか、端末の電源を切断するか、又は、パスワードで保護されたスクリーンセイバーが稼働するよう設定を行わなければならない。
- ② 職員等は、離席時には机上の記録媒体、書類等を放置せず、情報漏えい及び盗難等から保護するよう配慮しなければならない。

(3) アクセス制御

(ア) 利用者登録

- ① 情報セキュリティ管理者は、複数の利用者が使用する情報システムにおいて、正規の利用者を識別するために個人毎に利用者情報の登録、管理を行わなければならない。また、当該情報システムにおいては、利用者を識別するための機能を備えなければならない。
- ② 情報セキュリティ管理者は、情報システムの利用者の登録、変更、抹消等については、情報システム毎に定められた方法に従って行わなければならない。
- ③ 利用者登録、変更等は、当該情報システムを管理する情報セキュリティ管理者に対する申請により行わなければならない。その際、情報セキュリティ管理者は、申請者が間違いなく本人であることを確認しなければならない。さらに、情報セキュリティ管理者は、申請者が使用する利用者識別、パスワード等を、安全な方法で本人に通知しなければならない。また、ＩＣカード等を使用する場合は、安全な方法で本人に渡さなければならない。
- ④ 情報セキュリティ管理者は、利用者の登録等に際して、各利用者が利用できる機能は必要最低限のものとし、不要な機能の利用は行えないよう設定しなければならない。
- ⑤ 情報セキュリティ管理者は、管理する情報システムに対する各利用者のアクセス権限を、定期的に確認しなければならない。
- ⑥ 職員等が使用するＩＣカード等の紛失連絡を受けた場合、情報セキュリティ管理者は、直ちに当該ＩＣカード等を利用したアクセスを停止しなければならない。
- ⑦ 情報セキュリティ管理者は、情報システムの管理等に使用する特権を持った利用者は、必要最低限とし、厳格な管理を行わなければならない。
- ⑧ 情報セキュリティ管理者は、管理する情報システムに対する各利用者のアクセス権限を、定期的に確認しなければならない。

- ⑨ 職員等はパスワードを忘れてしまった場合、当該情報システムを管理する管理者に対し、新規パスワード発行の申請を行わなければならない。
- ⑩ 退職、異動等により利用権限等に変更が必要な場合には、適切な時期に利用者の抹消、利用権限の変更等を行わなければならない。
- ⑪ 複数の利用者からなるグループに対しての利用者識別の使用は、業務上必要であり、当該情報システム等を管理する管理者が認可した場合にのみ使用を認める。その際、グループから利用者が離脱した際には、パスワードの変更を行わなければならない。
- ⑫ 情報システムが使用する利用者情報、パスワード等は安全に管理し、消去、改ざん、漏えい等から保護し、破損等の際に迅速に復旧できるよう必要な措置を施さなければならない。
- ⑬ ネットワーク管理責任者及び情報システムの管理者は、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。

#### (4) 職員等による外部からのアクセス等の制限

- ア 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。
- イ 統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定し、アクセス可能な範囲も必要最低限に制限しなければならない。
- ウ 統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。
- エ 統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。
- オ 統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、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、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。
- キ 統括情報セキュリティ責任者は、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、ファイアウォールを経由した上で、多要素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。

ク 職員等が個人で所有する機器を用いて、外部からのアクセス及び村が利用する外部サービスへアクセスを行う場合、統括情報セキュリティ責任者及び情報システム管理者は、セキュリティ確保のために必要な措置を定めなければならない。

職員等は、外部からのアクセスを行う場合には、統括情報セキュリティ責任者の許可を得たうえで定められた措置を実施しなければならない。

#### (5) コンピュータ、情報システムの開発・導入・保守等

##### (ア) コンピュータ、情報システム等の調達

- ① 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。
- ② 情報システム管理者は、機器、ソフトウェアの調達、開発及び導入に当たっては、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 情報システム管理者は、開発若しくは変更したソフトウェアを情報システムに取り入れる場合、又は新たな設備を導入する場合は、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。
- ④ 情報システム管理者は、上記の開発及び試験については、実際に運用されている環境以外で行わなければならない。

##### (イ) ソフトウェアの保守及び更新

- ① 情報セキュリティ管理者は、情報セキュリティに重大な影響を及ぼすソフトウェアについては、適切な保守が行われるようにし、その不具合については、速やかに修正等の対応を行わなければならない。なお、修正等を実施するソフトウェアについては、ベンダーからの保証があるものなどの信頼できるものに限定しなければならない。
- ② 情報セキュリティ管理者は、情報システムのソフトウェアの更新等については、計画的に実施しなければならない。
- ③ 情報セキュリティ管理者は、使用するオペレーティングシステムの更新に際し、既に稼働している情報システムに問題が発生しないか、十分に検証を行わなければならない。

##### (ウ) 機器の修理及び廃棄

- ① 記録媒体の含まれる機器を、業者に修理させる場合又は貸借期限終了等により廃棄する場合は、可能な範囲でバックアップを取り、記録媒体内のすべての行政情報を消去しなければならない。

- ② 故障機器を業者に修理させる際、行政情報を消去することが難しい場合は、修理を委託する業者と守秘義務を明記した契約を締結しなければならない。

(6) コンピュータウイルス及びその他の悪意を持ったソフトウェアへの対策

(ア) ネットワーク管理責任者は、コンピュータウイルス及びその他の悪意を持ったソフトウェア（以下、「不正プログラム」という。）への対策として次の事項を実施しなければならない。

- ① 情報システムのサーバ及び必要な機器に不正プログラム対策ソフトを導入すること。
- ② 不正プログラムチェック用のパターンファイルは常に最新のものに保つこと。
- ③ 定期的に新種の不正プログラムに関する情報収集や情報システム内部の感染状況等について情報収集をすること。
- ④ 不正プログラム情報について、職員等に対する注意喚起を行うこと。
- ⑤ 不正プログラムについて、職員等に対して必要な啓発活動を行うこと。
- ⑥ 職員等より、不正プログラム発見の報告を受けた際には、直ちに当該機器のネットワークとの接続を遮断させ、不正プログラムの駆除が終了するまで、再接続を行わせないこと。
- ⑦ インターネットに接続していないシステムにおいて、記録媒体を使う場合、不正プログラム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の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。
- ⑧ 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。
- ⑨ 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。

(イ) 職員等は、次の事項を遵守しなければならない。

- ① 不正プログラム対策ソフトの常駐を解除しないこと。
- ② 外部からデータ又はソフトウェアを取り入れる場合、及び外部に持ち出す場合には、必ず不正プログラムチェックを行うこと。
- ③ 不正プログラムチェック（スキャン）の実行を途中で止めないこと。
- ④ 添付ファイルのあるメールを送受信する場合は、不正プログラムチェックを

行うこと。

- ⑤ ネットワーク管理責任者が提供する不正プログラム情報を常に確認すること。
- ⑥ 不正プログラムを発見した際には、ネットワークを直ちに切断し、それ以外はそのままの状態、直ちにネットワーク管理責任者に報告し、その指示に従うこと。
- ⑦ 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は無害化しなければならない。

#### (7) 不正アクセス対策

(ア) ネットワーク管理責任者は、次の事項を実施しなければならない。

- ① セキュリティホール等の情報収集に努め、メーカー等から修正プログラムの提供があり次第、速やかに対応するとともに、その修正履歴を記録・保存しなければならない。
- ② 情報システムに不正な侵入や利用があった場合に探知等できるよう、適切な対策に努めなければならない。
- ③ 情報システムに攻撃を受けていることが明らかな場合には、侵入経路の切断、システムの停止を含め必要な措置を施さなければならない。
- ④ 職員等により小川村のネットワーク及び外部ネットワークに対して不正なアクセスがあった場合は、情報セキュリティ管理者に通知し、適切な処置を求めなければならない。
- ⑤ 不正アクセス及びその未遂が発生した場合、当該不正アクセスが不正アクセス禁止法違反等犯罪の可能性がある場合、警察署に届出を行わなければならない。

(イ) 職員等は、次の事項を実施しなければならない。

- ① 外部ネットワークより不正アクセスがあった場合は、情報セキュリティ管理者に報告し、適切な措置を施さなければならない。

#### (8) セキュリティ情報の収集

(ア) ネットワーク管理責任者は、次の事項を実施しなければならない。

- ① セキュリティに関する情報について、国及び関係団体、民間事業者等から適宜情報を収集しなければならない。
- ② 専門家による助言を内部及び外部から求め、情報セキュリティの維持・管理に必要となる情報の収集を行わなければならない。
- ③ これらの情報を取りまとめ、情報セキュリティ管理者に通知するとともに、

情報セキュリティポリシーの改定につながる情報については統括情報セキュリティ管理者と小川村セキュリティ委員会に報告しなければならない。

## 9 運用

### (1) 情報セキュリティポリシーの遵守状況の確認

#### (ア) 遵守状況の確認及び対処

- ① 情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について、また、運用上支障が生じていないかについて確認を行わなければならない。問題を認めた場合には、速やかに最高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。
- ② 最高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、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管理者及び情報セキュリティ管理者は、ネットワーク、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。

#### (イ) 端末、記録媒体等の利用状況調査

- ① 最高情報セキュリティ責任者及び最高情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員が使用しているパソコン等の端末、記録媒体のアクセス記録、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。

#### (ウ) 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管理者及び情報セキュリティ管理者に報告を行わなければならない。
- ② 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管理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。

### (2) 緊急時対応計画

#### (ア) 緊急時対応計画の策定

セキュリティ委員会は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への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、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。

(イ) 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

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

(ウ) 緊急時対応計画の見直し

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、組織体制の変動等に対応し、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。

(3) セキュリティ障害時の対応

セキュリティ障害が発生した場合には、緊急時対応計画に従い、CSIRTは速やかに対応するとともに、再発防止の措置を講じなければならない。

(ア) 障害拡大の防止措置

- ① CSIRTは、故意の不正アクセス又は不正操作により情報システムに障害を及ぼすことが明らかな場合には、情報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。
- ② CSIRTはセキュリティ障害が発生した場合、障害の発生を速やかに統括情報セキュリティ管理者及びネットワーク管理責任者へ報告するとともに、その指示に従って、障害範囲及び被害等の拡大を防止するため、端末等の隔離、ネットワークの切断、情報システムの停止等、必要な措置を施さなければならない。
- ③ CSIRTは、情報システムに障害を受け、その障害の原因となる行為が不正アクセス禁止法違反等の可能性がある場合には、行為の記録の保存に努めなければならない。また、犯罪の可能性が無い場合においても、原因の追及等に活用できる記録を保存するよう努めなければならない。

(イ) 障害の調査

- ① 情報セキュリティ管理者は、セキュリティ障害が発生した場合、障害の発生を速やかに統括情報セキュリティ管理者へ報告するとともに、次の項目について調査をしなければならない。

1) 障害の内容

- 2) 障害が発生した原因
- 3) 確認した被害、影響範囲

調査した内容は速やかにCSIRT及び統括情報セキュリティ管理者へ報告しなければならない。CSIRTは報告された調査内容に基づき、障害への対応の要否を評価し、その結果を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。

②

#### (ウ) 障害への対応

- ① CSIRTは、統括情報セキュリティ管理者の指示の下に速やかにセキュリティ障害を復旧し、その措置について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。また、障害への対応は情報システムの重要度、障害の程度等により、迅速な復旧又は維持に必要な最低限の作業、完全な復旧作業に分割して行わなければならない。
- ② CSIRTは、当該情報システムの利用者等、影響を及ぼす恐れのある職員等に、障害の発生及びその影響度、想定されるサービスの停止期間等を通知しなければならない。
- ③ 障害が外部に重大な影響を及ぼすおそれがある場合には、CSIRTは速やかに統括情報セキュリティ責任者及び最高情報統括責任者に報告し、その指示を仰ぎ、必要とされる外部機関等へ連絡を行い、適切な対応、あるいは助言等を求めなければならない。

#### (エ) 再発防止の措置

- ① 情報セキュリティ管理者及びCSIRTは、必要な再発防止の措置を講じるとともに、その結果を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。
- ② 統括情報セキュリティ管理者は、報告を受けた内容が情報セキュリティポリシーの改定につながる場合については、小川村セキュリティ委員会に報告しなければならない。

#### (4) 逸脱管理

情報セキュリティポリシーの規定から逸脱する場合、その部分がセキュリティ上の脆弱性となるため、逸脱の管理について次のとおり実施する。

統括情報セキュリティ管理者は、セキュリティ上のリスクを的確に管理するため、情報セキュリティポリシーから逸脱する事項を把握しなければならない。

- (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が困難な事態が発生した場合、逸脱する事項について、期間、理由、代替手段等を統括情報セキ

セキュリティ管理者に報告しなければならない。

- (イ) 統括情報セキュリティ管理者は、報告された逸脱事項を調査、分析し、例外として許諾可能かを審査の上、セキュリティ委員会に諮らなければならない。
- (ウ) セキュリティ委員会は、逸脱事項について協議し、承認又は否認を行う。
- (エ) 統括情報セキュリティ管理者は、承認された逸脱事項を管理しなければならない。

#### (5) 法令等の遵守

職員等は、使用する情報資産について、次の法令等とその他不法行為を禁止する法令を遵守しなければならない。

- (ア) 地方公務員法（昭和 25 年法律第 261 号）
- (イ) 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）
- (ウ) 著作権法（昭和 45 年法律第 48 号）
- (エ) 個人情報の保護に関する法律（平成 15 年法律第 57 号）
- (オ) 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）
- (カ) サイバーセキュリティ基本法（平成 26 年法律第 104 号）
- (キ) 小川村個人情報の保護に関する法律施行条例（令和 5 年条例第 3 号）

#### (6) 情報セキュリティポリシーに関する違反に対する対応

職員等に情報セキュリティポリシーに違反する行動がみられた場合、速やかに次の措置を講じなければならない。

- (1) 違反行為を発見した場合、当該職員等が所属する部署の情報セキュリティ管理者に通知し、適切な対応を求める。
- (2) 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、ネットワーク管理責任者は、当該職員等のネットワーク又は情報システムの使用に関する権限の停止・剥奪等を実施し、その旨を最高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及び当該職員等が所属する部署の情報セキュリティ管理者に通知しなければならない。

### 10 外部サービス（クラウドサービス）の利用

#### (1) 業務委託先の選定基準

業務委託先の選定に当たっては、以下の点を考慮しなければならない。

- ① 統括情報セキュリティ責任者及び情報セキュリティ管理者は、業務委託先の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

- ② 統括情報セキュリティ責任者及び情報セキュリティ管理者は、業務委託先の選定に当たり、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等を参考にしなければならない。

## (2) 業務委託における管理事項

業務委託に際しては、以下の管理を実施しなければならない。

- ① 情報システムの開発、保守、運用管理、施設管理等を委託事業者に委託する場合は、以下に示すような、情報セキュリティポリシーのうち委託事業者が守るべき内容の遵守及びその守秘義務を明記した契約を締結し、その遵守を管理しなければならない。
  - 1) 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
  - 2) 委託先の責任者、委託内容、作業員及び作業場所の特定
  - 3) 提供されるサービスレベルの保証
  - 4) 従業員に対する教育の実施
  - 5) 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
  - 6) 業務上知り得た情報の守秘義務
  - 7) 再委託に関する制限事項の遵守
  - 8) 委託業務終了時の情報資産の返還、廃棄等
  - 9) 委託業務の定期報告及び緊急時報告義務
  - 10) 村による監査及び検査の権利
  - 11) 村による事故時等の公表
  - 12) 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)
- ② 業務委託する場合は、再委託は特別な事情があると認められた場合を除き禁止しなければならない。また、再委託先についても、守秘義務を明記した委託業者と再委託業者の間で取り交わされた契約書の写しの提示を求める等を実施し、それを遂行させなければならない。
- ③ 委託事業者より、情報資産に対する遠隔からの保守を行う際には、事前に最高情報セキュリティ責任者による承認を必要とする。また、個別の作業時においては、作業開始前に作業内容等について該当業務を主管する部署の情報システム管理者及びネットワーク管理責任者に報告し、作業完了時にも同様の報告義務を課するものとする。
- ④ 委託事業者の社員等が、村の施設において作業する場合は、身分を証明する証票等の提示を求めなければならない。また、統括情報セキュリティ責任者及び情報セキュリティ管理者は、その作業内容について認められた範囲内で実施していることを確認しなければならない。

### (3) 外部組織の情報システム等の利用における管理事項

外部組織の情報システム等を利用する際には、以下の管理を実施しなければならない。

- ① 情報セキュリティ管理者は、外部組織が提供する機器、情報システムの開発、保守、運用管理、施設管理等のサービス（以下「アウトソーシング」という。）を利用する場合は、提供されるサービスの水準及び必要なセキュリティ要件等を明記した契約を交わし、それを遂行させなければならない。また、必要ならば、監査を実施する権利等も明記した契約を交わさなければならない。
- ② 情報セキュリティ管理者は、機密性 2 に該当する情報をアウトソーシングで利用する際には、統括情報セキュリティ責任者及びネットワーク管理責任者に、提供されるサービスの水準及びセキュリティ要件の確認と承認を得なければならない。
- ③ 情報セキュリティ管理者は、定期的にセキュリティ対策が確保されていることを確認し、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) 外部サービス（クラウドサービス）の利用における管理事項（気密性 2 以上の情報を取扱う場合）

#### (ア) クラウドサービスの選定に係る運用規程の整備

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

- 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「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

#### (イ) 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管理者は、機密性 2 以上の情報を取り扱う場合、以下を含むクラウドサービス（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、クラウドサービスを利用して情報システムを運用・保守する際のセ

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、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。

- ・クラウドサービスの利用終了時における対策
- ・クラウドサービスで取り扱った情報の廃棄
- ・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

#### (ウ) クラウドサービスの選定

①情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。

②情報セキュリティ管理者は、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、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。

- i クラウドサービスの利用を通じて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の禁止
- ii 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
- iii 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、村の意図しない変更が加えられないための管理体制
- iv クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定
- v 情報セキュリティインシデントへの対処方法
- vi 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
- vii 情報セキュリティ対策の履行が不十分な場合の対処方法

③情報セキュリティ管理者は、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情報セキュリティ管理者は、クラウドサービスの利用を通じて村が取り扱う情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めなければならない。

i 情報セキュリティ監査の受入れ

ii サービスレベルの保証

⑤情報セキュリティ管理者は、クラウドサービスの利用を通じて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。

⑥情報セキュリティ管理者は、クラウドサービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本村に提供し、村の承認を受けるよう、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

⑦情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、クラウドサービスを選定しなくてはならない。また、クラウドサービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。

⑧情報セキュリティ管理者は、クラウドサービスの特性を考慮した上で、クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めなければならない。

i クラウドサービスに求める情報セキュリティ対策

ii 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

iii クラウドサービスに求めるサービスレベル

⑨統括情報セキュリティ管理者は、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。

#### (エ) クラウドサービスの利用に係る調達・契約

①情報セキュリティ管理者は、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を調達仕様に含めなければならない。

②情報セキュリティ管理者は、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。

(オ) クラウドサービスの利用承認

①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には、利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。

②利用申請の許可権限者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。

③利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名しなければならない。

(カ) 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等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

i 不正なアクセスを防止するためのアクセス制御

ii 取り扱う情報の機密性保護のための暗号化

iii 開発時におけるセキュリティ対策

iv 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を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

i クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

ii クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

iii 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

④クラウドサービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。

(キ) 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、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。

- i クラウドサービス利用方針の規定
- ii クラウドサービス利用に必要な教育
- iii 取り扱う資産の管理
- iv 不正アクセスを防止するためのアクセス制御
- v 取り扱う情報の機密性保護のための暗号化
- vi クラウドサービス内の通信の制御
- vii 設計・設定時の誤りの防止
- viii クラウドサービスを利用した情報システムの事業継続

②クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ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情報セキュリティ管理者は、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。

(ク) 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、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。

- i クラウドサービスの利用終了時における対策
- ii クラウドサービスで取り扱った情報の廃棄
- iii 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。

(5) 外部サービス（クラウドサービス）の利用における管理事項（気密性2以上の情報を取扱わない場合）

外部組織の情報システム等を利用する際には、以下の管理を実施しなければならない。

- ① 情報セキュリティ管理者は、以下を含む外部サービスの利用に関する規定を整備しなければならない。
  - ・ サービスを利用してよい範囲
  - ・ 業務により利用する外部サービス
  - ・ 利用手続及び運用手順
- ② 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外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

(6) ソーシャルメディアサービスの利用

- ① ネットワーク管理責任者は、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、以下を含む情報セキュリティ対策に関する運用手順等を定め、遵守させなければならない。
  - ・ 村のアカウントによる情報発信が実際の村のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。
  - ・ パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。
- ② ネットワーク管理責任者は、村において情報発信のためにソーシャルメディアサービスを利用する場合は、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。
- ③ 職員等は、住民への提供にソーシャルメディアサービスを用いる場合は、提供情報の重要度に応じて、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などの措置をとらなければならない。また、機密性2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。

(7) Web会議サービスの利用時の対策

- ① 統括情報セキュリティ責任者は、Web会議を適切に利用するための利用手順を定めなければならない。
- ② 職員等は、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、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。

## 1 1 評価、見直し等

### (1) 監査

- (ア) 統括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情報セキュリティについて、監査を定期的に又は必要に応じて行わなければならない。
- (イ) 監査を行う者は、被監査部門から独立した者で、客観的な判断が可能で、十分な専門知識を有する者でなければならない。
- (ウ) 監査の実施にあたっては、業務の中断等を最小限に抑えるよう計画を立案の上、実施しなければならない。
- (エ) 監査を外部委託する場合には、信頼できる事業者へ委託し、当該事業者へ守秘義務を課さなければならない。
- (オ) 監査結果については、外部委託された事業者は最高情報セキュリティ責任者に報告しなければならない。また、セキュリティ委員会は、監査結果を情報セキュリティ対策の見直しの際に参照する情報資産として活用するものとする。

### (2) 自己点検

- (ア) 情報セキュリティ管理者は、当該部署の情報セキュリティが確保されていることを確認するため、職員等にアンケート調査を行い、又は自己点検を行い、必要に応じ改善措置を施さなければならない。
- (イ) 点検結果は、統括情報セキュリティ管理者及びセキュリティ委員会に報告されなければならない。

### (3) 見直し

- (ア) 統括情報セキュリティ管理者は、評価及び見直しが必要となる事象が発生した場合には、小川村セキュリティ委員会に諮り必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。

附則 令和8年3月31日改訂