小谷村情報セキュリティ実施手順

令和４年 12 月改訂

総務課

目次

1　役割・責任体制

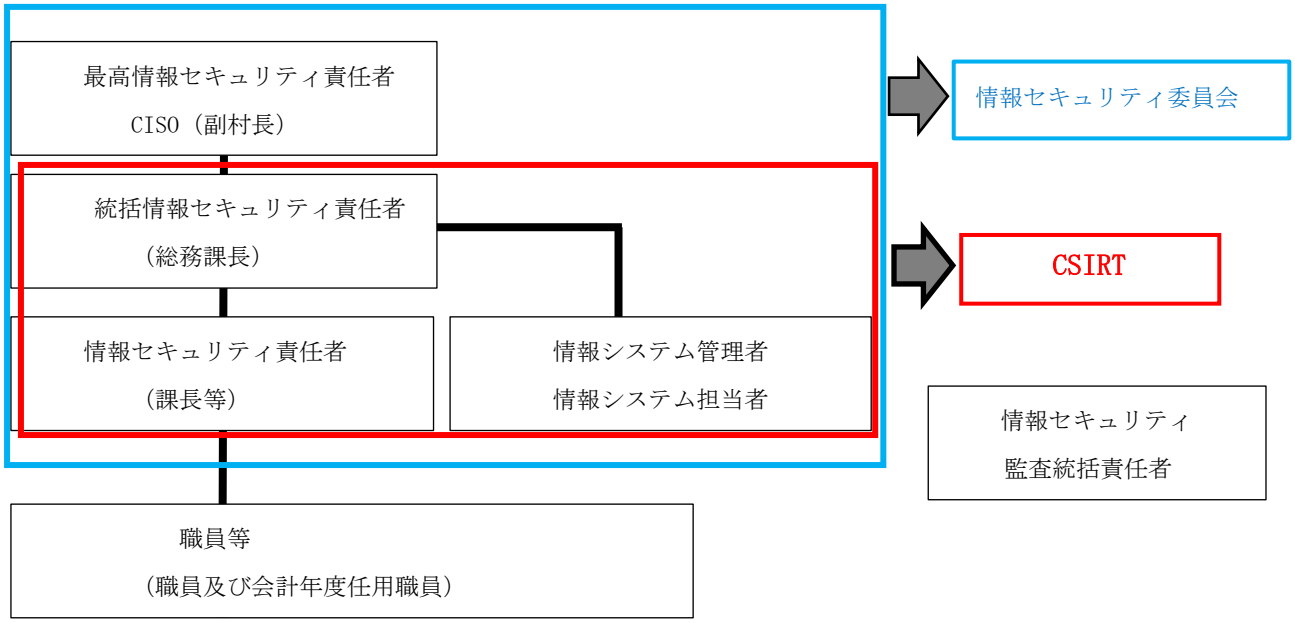
1　組織体制

（対象範囲）

本実施手順が適用される行政機関は、村長、教育委員会、その他の委員会、及び議会とします。

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）	副村長
統括情報セキュリティ責任者	総務課長
情報セキュリティ責任者	課長等
情報システム管理者	情報システムの担当課長等
情報システム担当者	情報システム管理者が指名する者
情報セキュリティ委員会	最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュリティ責任者、情報システム管理者他
CSIRT （Computer Security Incident Response Team）	統括情報セキュリティ責任者、情報セキュリティ責任者、情報システム管理者他

※　課長等は、各課の課長、議会事務局長、選挙管理委員長、監査委員の代表者、固定資産評価審査委員会の代表者及び教育委員会の次長をいいます。



（１）最高情報セキュリティ責任者

（CISO: Chief Information Security Officer、以下「CISO」といいます。）

① 副村長をCISOとします。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します。

（２）統括情報セキュリティ責任者

① 総務課長を、CISO 直属の統括情報セキュリティ責任者とします。統括情報セキュリティ責任者はCISOを補佐しなければなりません。

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、見直し等を行う権限及び責任を有します。

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権限及び責任を有します。

④ 統括情報セキュリティ責任者は、本村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します。

⑤ 統括情報セキュリティ責任者は、本村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、見直し等を行う総括的な権限及び責任を有します。

⑥ 統括情報セキュリティ責任者は、情報セキュリティ責任者、情報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します。

⑦ 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・管理を行う権限及び責任を有します。

⑧ 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実施する権限及び責任を有します。

⑨ 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、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りません。

⑩ 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りません。

⑪ 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りません。

（３）情報セキュリティ責任者

① 課長等を、情報セキュリティ責任者とします。

② 情報セキュリティ責任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統括的な権限及び責任を有します。

③ 情報セキュリティ責任者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有します。

④ 情報セキュリティ責任者は、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します。

⑤ 情報セキュリティ責任者は、所管する情報システムにおける情報セキュリティ実施手順の維持・管理を行います。

⑥ 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並びに職員、会計年度任用職員（以下「職員等」という。）に対する教育、訓練、助言及び指示を行います。

⑦ 情報セキュリティ責任者は、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、CSIRT 及び CISO へ速やかに報告を行い、指示を仰がなければなりません。

（４）情報システム管理者

① 情報システムの担当課長等を当該情報システムに関する情報システム管理者とします。

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します。

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します。

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・管理を行います。

（５）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します。

（６）情報セキュリティ委員会

情報セキュリティ委員会は、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報システム管理者他のメンバーで構成し、本村の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、情報セキュリティポリシーの運用、情報セキュリティインシデントの対応等、情報セキュリティに関する重要な事項を審議します。

（７）CSIRT の設置

① CISO は、情報セキュリティインシデントの統一的な窓口の機能を有する組織として CSIRT を設置し、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します。

② 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、その内容を関係課等に周知します。

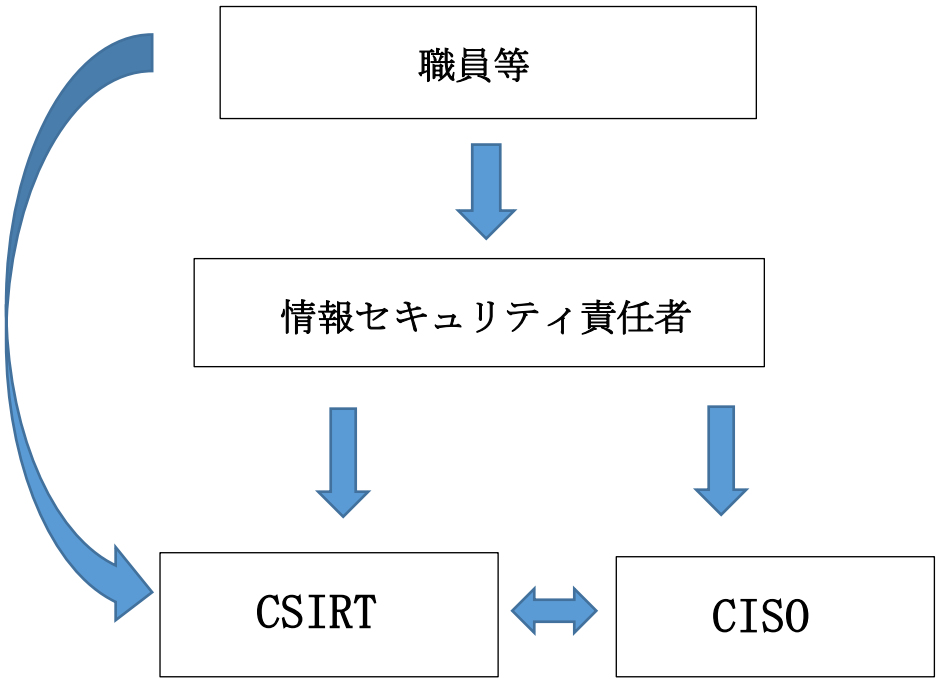
③ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければなりません。

④ 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 CSIRT、及び委託事業者等との情報共有を行います。

⑤ 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、県等へ報告しなければなりません。

⑥ 職員等は、インシデント発生若しくは、そのおそれがある場合は、所属の長である情報セキュリティ責任者及び CSIRT に沈滞なく報告をしなくてはなりません。

◇情報セキュリティインシデント報告フロー



◇所属内の管理体制

◇管理体制役割一覧

名称	主な役割等
	所属内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します。 ① 所属で所管する情報システムの管理に関する統括的な権限及び責任を有し、所管する情報セキュリティ実施手順の維持・管理を行います。
情報セキュリティ責任者 （各課等の長）	② 情報資産に対する侵害が発生又は侵害のおそれがある場合には、CSIRT 及び CISO に速やかに報告し、指示を仰がなければなりません。 ③ 所属内において、情報セキュリティポリシー及び実施手順の周知及び遵守の徹底を図ります。 ④ 職員等に対して、情報セキュリティ指導を行います。
職員等 （職員及び会計年度任用職員）	情報セキュリティ責任者の指示のもと、所属内の情報セキュリティ対策を実施します。 ① 情報資産に対する侵害が発生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及び CSIRT の指示のもと、速やかに対処します。

２　職員向け情報セキュリティ実施手順

１　情報資産の管理方法

情報資産は、その漏えいや紛失等を防ぐため、重要性に基づく分類を行い、分類に応じた適切な利用と安全管理を行わなければなりません。

◇　情報資産とは

(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

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルーター等の通信機器
情報システム	サーバ、パソコン、オペレーティングシステム、ソフトウェア、ネットワークシステム
上記に関する設備	サーバ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録媒体	CD－R、DVD－R、MO、USB メモリ
ネットワーク及び情報システムで取り扱う情報	ネットワーク及び情報システムで取り扱うデータ（これらを印刷した文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図

◇　管理方法等

(1) 管理責任

情報セキュリティ責任者は、所管する情報資産について管理責任を有します。

なお、情報資産を取り扱う、又は保管している事務室等が複数に分かれている場合は、必要に応じて、情報セキュリティ責任者の判断により、事務室等ごとに管理者を置くことができます。

(2) 台帳による管理

情報資産は、その重要性を分類し、保管場所、複製の履歴、暗号化の有無、保存期間等を記録した台帳を作成し、適切に管理するよう努めてください。

(3) 情報資産の取扱者の特定

①　機密性分類３、可用性分類２及び完全性分類２の情報資産については、取扱者を特定してください。

②　特定した取扱者の所属部署、役職名及び氏名等を台帳に記載し、取扱者以外の者が取り扱うことのないよう管理してください。

(4) 情報資産の保管

① 情報資産の分類に従って、情報資産を適切に保管・管理してください。

② 情報資産の各分類２以上の情報を記録した電磁的記録媒体を保管する場合は、耐火、耐熱、耐水、耐湿等を講じた施錠可能な場所に保管してください。

③ 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、無断で書き込みされないよう対策してください。

◇ 情報資産の分類

（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します。

◇機密性による情報資産の分類

分類	分類基準	分類基準の解釈	取扱制限
機密性３	行政事務で取り扱う情報資産のうち、秘密文書[注1]に相当する機密性を要する情報資産	・村が行う事務又は事業で取り扱う情報のうち、小谷村情報公開条例（平成 28 年条例第８号改正）（以下「情報公開条例」という。）第７条各号における不開示情報[注2]に該当すると判断される蓋然性の高い情報を含む情報	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・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 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持込禁止
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	・「機密性３の情報」以外の情報で、直ちに一般に公表することを前提としていない情報	・必要以上の複製及び配付禁止 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管

分類	分類基準	分類基準の解釈	取扱制限
機密性１	機密性２又は機密性３の情報資産以外の情報資産	・公表済みの情報、公表しても差し支えない情報等、機密性２の情報又は機密性３の情報以外の情報	

注１：秘密文書

行政事務で取り扱う情報のうち、「行政文書の管理に関するガイドライン」に定める秘密文書に相当する機密性を要する情報を含む情報です。

注２：機密性３に該当する情報公開条例第７条各号における不開示情報は以下の情報

(1) 法令若しくは条例（以下「法令等」といいます。）の定めるところにより、又は実施機関が法律上従う義務を有する各大臣その他国の機関の指示により、公にすることができないと認められる情報です。

(2) 個人に関する情報（事業を営む個人の当該事業に関する情報を除きます。）であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と照合することにより、特定の個人を識別することができることとなるものを含む。）、又は特定の個人を識別することはできないが、公にすることにより、なお個人の権利利益を害するおそれがあるものです。ただし、次に掲げる情報を除きます。

ア　法令等の規定により又は慣行として公にされ、又は公にすることが予定されている情報

イ　人の生命、健康、生活又は財産を保護するため、公にすることが必要であると認められる情報

ウ　当該個人が公務員（国家公務員法（昭和22年法律第120号）第２条第１項に規定する国家公務員及び地方公務員法（昭和25年法律第261号）第２条に規定する地方公務員をいう。）である場合において、当該情報がその職務の遂行に係る情報であるときは、当該情報のうち、当該公務員の職及び当該職務遂行の内容に係る部分

(3) 法人その他の団体（国及び地方公共団体を除きます。以下「法人等」といいます。）に関する情報又は事業を営む個人の当該事業に関する情報であって、次に掲げるものです。ただし、人の生命、健康、生活又は財産を保護するため、公にすることが必要であると認められる情報を除きます。

ア　公にすることにより、当該法人等又は当該個人の権利、競争上の地位その他正当な利益を害するおそれがあるもの

イ　実施機関の要請を受けて、公にしないとの条件で任意に提供されたものであ

って、法人等又は個人における通例として公にしないこととされているもの、その他の当該条件を付することが当該情報の性質、当時の状況等に照らして合理的であると認められるもの

(4) 公にすることにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがあると実施機関が認めることにつき相当の理由がある情報です。

(5) 村の機関並びに国の機関及び他の地方公共団体の内部又は相互間における審議、検討又は協議に関する情報であって、公にすることにより、率直な意見の交換若しくは意思決定の中立性が不当に損なわれるおそれ、不当に村民等の間に混乱を生じさせるおそれ又は特定の者に不当に利益を与え若しくは不利益を及ぼすおそれがあるものです。

(6) 村の機関又は国の機関若しくは他の地方公共団体が行う事務又は事業に関する情報であって、公にすることにより、次に掲げるおそれその他当該事務又は事業の性質上、当該事務又は事業の適正な遂行に支障を及ぼすおそれがあるものです。

ア　監査、検査、取締り又は試験に係る事務に関し、正確な事実の把握を困難にするおそれ又は違法若しくは不当な行為を容易にし、若しくはその意見を困難にするおそれ

イ　契約、交渉又は争訟に係る事務に関し、国又は地方公共団体の財産上の利益又は当事者としての地位を不当に害するおそれ

ウ　調査研究に係る事務に関し、その公正かつ能率的な遂行を不当に阻害するおそれ

エ　人事管理に係る事務に関し、公正かつ円滑な人事の確保に支障を及ぼすおそれ

オ　地方公共団体が経営する企業に係る事業に関し、その企業経営上の正当な利益を害するおそれ

◇完全性による情報資産の分類

分類	分類基準	分類例	取扱制限
完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・戸籍 ・住民基本台帳 ・障害者手帳 ・認定通知書 ・工事設計書 ・保守図面 ・地籍図 ・検査結果 ・公式 Web サイト公開情報 ・国県からの通達	・バックアップ、情報資産管理台帳、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
完全性１	完全性２の情報資産以外の情報資産	・公開を前提としない参考資料で、消失しても再作成又は再入手が容易であり、業務に支障のない情報	

◇可用性による情報資産の分類

分類	分類基準	分類例	取扱制限
可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・証明書発行のためのデータ ・防災関係文書 ・災害避難における障害者リスト ・上下水道配管図	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	・イベント開催記録 ・避難場所情報	

◇　管理方法等

１　機密性分類３の情報資産は、次の表に従って管理してください。

取扱い	管理方法
電子メール等での送信	・禁止
庁舎外への持ち出し	・禁止 ・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が必要 ・持ち出し時及び返却時の記録（「機密情報外部持ち出し申請書（様式２）」の整備） ・鍵付きケース等への格納、暗号化又はパスワード設定の対策が必要
廃棄・再利用	・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が必要 ・復元不可能な方法で廃棄又は消去等が必要 ・シュレッダー等による物理的破壊等の対策が必要 ・紙媒体の裏面再利用禁止 ・廃棄日、担当者、処理内容の記録（情報資産管理台帳）
保管	・施錠管理 ・電磁的記録媒体の長期保管の際は書込禁止措置

２　機密性分類２の情報資産は、次の表に従って管理してください。

取扱い	管理方法
電子メール等での送信	・原則禁止（LGWAN 回線又は専用回線での送信可） ・情報セキュリティ責任者の許可が必要 ・許可を得て送信の場合、暗号化又はパスワード設定等の対策が必要
庁舎外への持ち出し	・原則禁止 ・情報セキュリティ責任者の許可が必要 ・持ち出し時及び返却時の記録（「機密情報外部持ち出し申請書（様式２）」の整備） ・鍵付きケース等への格納、暗号化又はパスワード設定の対策か必要
廃棄・再利用	・情報セキュリティ責任者の許可が必要 ・復元不可能な方法で廃棄又は消去等が必要 ・シュレッダー等による物理的破壊等の対策が必要 ・紙媒体の裏面再利用禁止 ・廃棄日、担当者、処理内容の記録（情報資産管理台帳）
保管	・施錠管理 ・電磁的記録媒体の長期保管の際は書込禁止措置

(1) 情報資産は、業務目的の範囲内で利用してください。

(2) 盗難や盗み見による情報漏えいを防ぐため、机上には重要な情報を含んだ機器、紙資料、電子媒体等を放置しないようにしてください。

(3) 離籍時には、パソコンをコンピュータロック等パスワードの入力が必要な状態にしてください。

(4) 重要な情報を含んだ機器、紙資料、電子媒体等は、施錠管理できる場所に保管し、鍵は情報セキュリティ責任者が厳重に管理するようにしてください。

(5) 重要な情報を含んだ機器、紙資料、電子媒体等を廃棄する際は、廃棄するまで施錠管理された場所で保管し、裁断、溶解等により情報を復元できないように処理してください。

(6) コピー、FAX、プリンター使用時は、出力された資料や原稿の放置に気を付けてください。特に、重要資料のプリントアウトや、FAXで送信する場合は、速やかに出力確認や受領確認を行ってください。

(7) 重要な情報が記載されている用紙を裏面再利用しないでください。

(8) 職場の個人情報やID・パスワード等の重要な情報に関する会話は、周囲に漏れることのないよう十分配慮してください。

(9) 外での食事中や宴席等での重要な情報に関する会話は控えてください。組織外の第三者に盗み聞きされるおそれがあります。

(10) 業務を遂行するため、やむを得ず外部に重要な情報を含んだ機器、紙資料、電子媒体等を持ち出す場合は、「機密情報外部持ち出し申請書（様式２）」により情報セキュリティ責任者の許可を得るようにしてください。また、外出時の行動については「２　情報資産の持ち出し」に従って行動するようにしてください。

(11) 機密性分類３の情報をパソコン内のハードディスク等に保存しないでください。保存する場合は、情報セキュリティ責任者の許可を得るようにしてください。

(12) 機密性分類３、完全性分類２又は可用性分類２の情報資産については、破壊、改ざん、紛失等のリスクに備えて、定期的にバックアップを実施してください。

【補足事項】

・電話による重要な情報の取扱いはしないでください。
・エレベータ内は、組織外の来訪者が乗っている場合もあるため、重要な情報を含む会話は控えてください。
・会議で使用したホワイトボードの内容は、使用後には必ず消去してください。
・会議室で使用した資料は、放置しないよう気を付けてください。
・紙・電子媒体にかかわらず、機密性の高い重要情報は、所在や情報の正確性を定期的に確認するようにしてください。

２　情報資産の持ち出し

重要な情報（機密性分類３）を含んだ機器、電磁的記録媒体、紙資料等は、個人の判断で持ち出してはいけません。持ち出す場合は、事前に情報セキュリティ責任者の許可を得てください。

◇　管理方法等

(1) 機密性分類３の情報は、原則として庁舎外へ持ち出してはいけません。

(2) 外部に重要な情報資産を持ち出す場合は、必ず事前に情報セキュリティ責任者の許可を得るようにしてください。また、「機密情報外部持ち出し申請書（様式２）」に記録し、押印による許可を得るようにするとともに、返却時にも記録してください。

(3) 情報セキュリティ責任者は、持ち出す理由を確認し、他の方法等がないかどうかを十分に考慮した上で許可することとし、持ち出す情報資産は、必要最小限の範囲としてください。

(4) 持ち出した情報資産の利用方法について確認し、必要なセキュリティ対策が確保されているかどうかを検証してください。特に、不正プログラム対策のソフトウェアがインストールされてないパソコン等、情報漏えいの危険性の高いパソコンでの作業は行わないようにしてください。

(5) 外部に情報資産を持ち出す場合は、盗難・紛失等の情報漏えいのリスクを常に意識し、手元から離さないよう注意してください。

(6) 電磁的記録媒体内のデータについては、暗号化やパスワード設定等の対策を行ってください。

(7) 帰庁したら速やかに、持ち出した機器、電磁的記録媒体、紙資料等が全てそろっているか確認してください。不足があることが分かったときには、直ちに情報セキュリティ責任者に報告してください。

【補足事項】

・重要な情報資産を持ち出す場合は、事前に情報セキュリティ責任者の許可を得るとともに、持ち出す対象は必要最小限とし、適切なセキュリティ対策を確保してください。

・全ての情報資産は、職員個人の判断で持ち出すことはできません。また、機密性分類３の情報は、原則として庁舎外への持ち出しを禁止しています。

・持ち出す情報の利用場所、期間、移送方法等を確認し、適切な情報セキュリティ対策が確保されているかどうかを検証してください。特に、情報の漏えいは、移動中の紛失や盗難による場合が多いことから、紛失・盗難による情報漏えいのリスクを常に意識し、手元から離さないよう注意してください。

・情報の漏えいを防止するため、鍵付きケース等への収納や暗号化又はパスワード設定等の対策をとってください。

・機密情報外部持ち出し申請書（様式２）は、記入漏れ等をなくすとともに、適正に保管してください。

・総務課管理パソコンを庁舎外に持ち出す場合も、情報セキュリティポリシーに定める手続を行うとともに、情報セキュリティ責任者の指示に従った方法で利用してください。

・機密性分類２の情報を「電子メール等で送信する場合」、「外部に提供する場合」も同様の取扱いをしてください（LGWAN 回線又は専用回線での送付は除きます。）。

・機密性分類３の情報は電子メール等で送信することは禁止です。外部に提供することも禁止ですが、どうしても必要な場合は、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が必要となります。

3　スタンドアロンパソコン対策

スタンドアロンパソコン等についても、不正プログラム対策ソフトウェアのインストール等の基本的なセキュリティ対策を行ってください。

◇　管理方法等

(1)　不正プログラム対策ソフトウェアをインストールし、自動アップデートを施すなど常に最新の状態を保ってください。

(2) OSのアップデートも更新プログラムの提供の都度、行ってください。

(3) ファイル交換ソフト（Winny等）がインストールされていないか確認し、インストールされている場合は、アンインストールしてください。

4　情報システム機器の利用

ウイルス感染やシステム障害を防ぐため、ソフトウェアの導入や機器構成の変更等を無断で行ってはいけません。業務上必要な場合は、関係する情報セキュリティ責任者の許可を得てください。

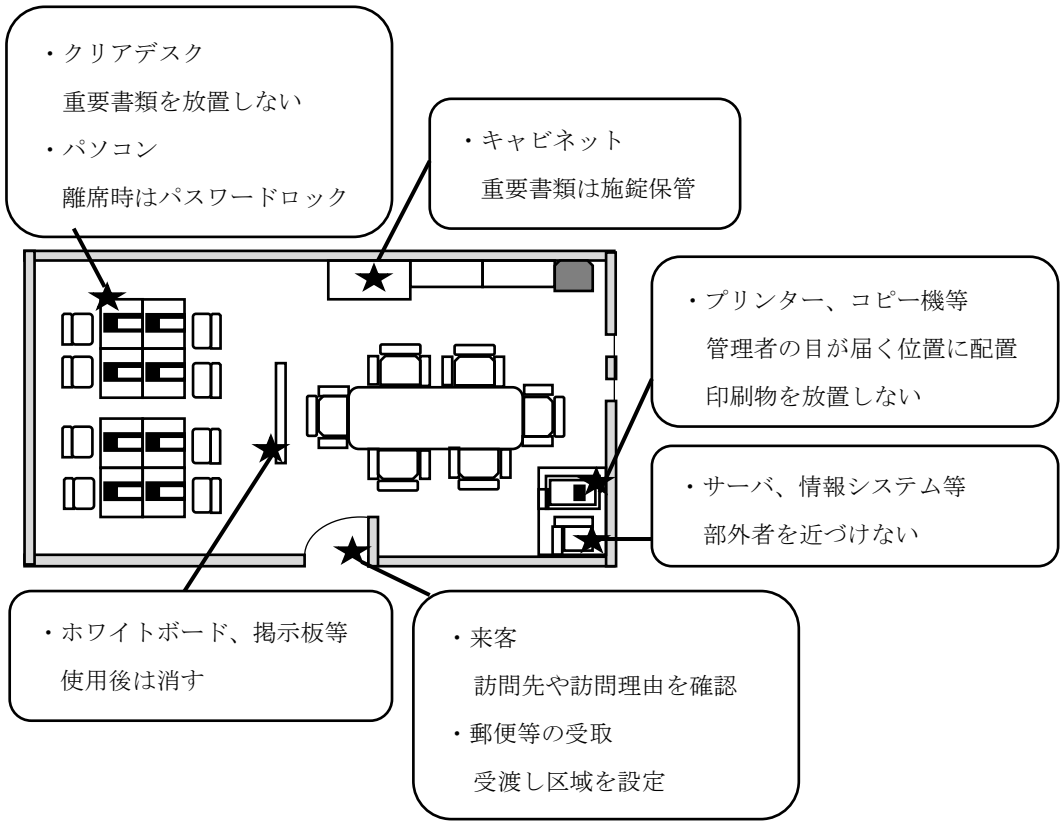
◇　管理方法等

(1)　パソコン等の情報システム機器の設定変更や改造、ソフトウェアのインストールを行う場合は、統括情報セキュリティ責任者及び当該パソコン等を所管する情報セキュリティ責任者の許可を得るようにしてください。

(2)　OSやソフトウェアにはセキュリティホールという情報セキュリティ上の欠陥が発見されることがあるため、迅速に最新バージョンへの更新やセキュリティパッチ（修正プログラム）を適用してください。

(3) USBメモリ等の電磁的記録媒体も、使用の都度、ウイルスチェックを行ってください。

5　事務室内の管理



(1) 書類・媒体等の取扱いと保管

① 直ちに使用しない書類や電磁的記録媒体は、机の引き出しやキャビネット等に収納し、机上等に放置しないようにしてください。

② 重要な情報が記録された書類や電磁的記録媒体は、施錠保管してください。

(2) パソコン画面に表示する情報の管理

他人による盗み見や不正操作等を防止するため、離席時にはパスワードロック等の保護機能を使用してください。

(3) 情報通信機器等の取扱い

① コピー機、FAX、プリンター等の機器は、管理者等の目が届く場所に設置してください。

② コピー機、FAX、プリンター等に印刷物や原稿等の書類を放置しないでください。特に重要な情報の場合は、印刷及び送受信の間、職員が立ち会うようにしてください。

③ FAX 送信時は、誤送信しないよう、必ずあて先を確認してください。複数のあて先に一斉送信する場合は、複数の職員による確認をしてください。

④ ホワイトボード等への書き込み内容を使用後に必ず消去し、放置しないでください。

(4) 搬入物等の受渡し

① 搬入物等の受渡しについては、受渡し区域を指定してください。

② 搬入物等の受入れの際には、危険物の持込みや情報漏えい等のリスクがないか点検してください。

③ 受渡し区域に搬入物等を放置しないでください。

(5) 部外者（第三者）に対する情報漏えいの防止

① 職員は、外部の者と区別がつくように、名札の着用や身分証を携帯し、職員であることが分かるようにしてください。

② 外部の者が多く出入りする場所には、個人情報等の重要資産を放置しないでください。

③ 職員の電話や立ち話、オープンな打合せスペースでの発言について、第三者による盗み聞きを防止するよう配慮してください。

④ 外部の者が入室しようとするときは、必ず理由や用件を尋ねるようにしてください。また、事務室内へ来訪者を案内する場合は、必ず付き添うようにしてください。

⑤ 施錠が必要な部屋では、職員が不在になる場合、たとえわずかな時間でも、必ず施錠するようにしてください。

6 離席時の対策

離席する場合は、盗み見等による情報漏えいを防ぐため、パソコンをパスワードロック等のパスワード入力が必要な状態にしてください。

◇ 管理方法等

(1) 離席する場合は、作業中のファイルや使用ソフト等を閉じるとともに、机の上に書類を置いたままにしないでください。

(2) 使用しているUSBメモリ等は取り外して、机の中にしまうなど、放置しないようにしてください（機密性分類３の情報資産は施錠管理）。

(3) パソコンは、電源を切るか、パスワードロック等を行い、他人に勝手に使用されないようにしてください。

(4) FAX、コピー機、プリンター等の機器から出力された書類を放置しないでください。

7　ソフトウェアの利用

ソフトウェアの違法コピーはしないでください。不正にコピーしたソフトウェアは、ライセンス違反や著作権法違反になります。

◇　管理方法等

(1)　パソコンにソフトウェアをインストールする場合は、統括情報セキュリティ責任者及び当該パソコンを所管する情報セキュリティ責任者の許可を得るようにしてください。また、導入したソフトウェアのライセンスを適正に管理してください。

(2)　ソフトウェアの違法コピーをしてはいけません。不正にコピーしたソフトウェアは、ライセンス違反や著作権法違反になります。

(3)　村がライセンスを所有するソフトウェアを私物のパソコンにインストールしないでください。

(4)　業務に使用しないソフトウェアや出所不明のソフトウェアは、インストールしないでください。インターネットからダウンロードしたソフトウェアそのものがスパイウェアである可能性もあります。

8　インターネットの利用

インターネット利用時は、業務に必要のない Web ページ、不審な Web ページにアクセスしないようにしてください。

◇　管理方法等

(1) インターネットの私的利用は、禁止されています。明らかに業務に関係のないWebページを閲覧している職員がいた場合は、注意しましょう。

(2)　インターネットでWebページを閲覧する場合は、信頼できるWebページ以外にはアクセスしないでください。

(3) Webページに掲載されたリンクをむやみに開かないでください。

(4) インターネット上（ホームページ）に情報を公開するときには、不開示情報が含まれていないことを確認してください。

(5) 業務と関係のないファイル等のダウンロードはしないでください。

(6)　不正プログラム対策ソフトウェアは常時起動させ、パターンファイル等の自動更新を設定するなど、常に最新の状態を保つようにしてください。

(7) ウイルス感染時に備えて、定期的にデータのバックアップを行ってください。

(8)　ウイルスに感染した場合又は感染の疑いがある場合は、直ちにネットワークから

切り離し、情報セキュリティ責任者へ報告してください。その際に使用していたUSBメモリ等の電磁的記録媒体も他で使用せずに隔離し、情報セキュリティ責任者の指示に従ってください。

9　電子メールの利用

重要な情報（機密性分類２）を電子メールで送信する場合は、事前に情報セキュリティ責任者の許可を得るとともに、暗号化やパスワード設定等の対策をとってください（LGWAN 回線又は専用回線での送付は除きます。）。機密性分類３の情報はインターネットメールで送信してはいけません。

不審なメールを受信した場合は、添付ファイルを開いたり、本文中に記載されたリンクを開いたりしないようにしてください。

◇　管理方法等

(1)　重要な情報をインターネットメールで送受信してはいけません。業務上やむを得ず送信する場合は、必ず事前に情報セキュリティ責任者の許可を得るとともに、暗号化やパスワード設定等の対策をとってください。

(2)　電子メールの私的利用は禁止されていますので、私物のパソコン等に電子メールメールを転送したりしないでください。

(3) 送信時には、送信先や内容、添付ファイルの確認を行ってください。特に、重要な電子メールの場合は、複数人でチェックするなど、慎重に行ってください。

(4)　重要な電子メールを誤送信した場合は、情報セキュリティ責任者に報告してください。

(5) 互いに面識のない複数の送信先へ電子メールを送信する場合は、BCC機能を使用し、メールアドレスが全員に開示されないようにしてください。

(6) 不審なインターネットメールを受信した場合は、添付ファイルや、本文中に記載されたリンクを開かないようにしてください。

(7) 標的型攻撃メール*など、「一見正しいメールに見えるが、普段メールのやりとりをしていない人から届き、なぜ自分あてに送られてきたか心当たりがない」ようなメールの添付ファイル、およびリンク（URL）は原則として開かないでください。

*標的型攻撃メール：特定の組織等が保有する機密情報等の窃取を目的に送信されたウイルスメール。実在の企業名や官公庁名を装い送信されるのが一般的であるため、標的型攻撃メールと気づかずに開封してしまうケースが多い。

10　コンピュータウイルス対策

ウイルスに感染した場合は、直ちに情報機器や電磁的記録媒体をネットワークから切り離し、感染の拡大を防いでください。

◇　管理方法等

(1) 総合行政ネットワーク（LGWAN）に接続しないパソコン（スタンドアロンで使用）についても、不正プログラム対策ソフトウェアをインストールしなければなりません。

(2) 不正プログラム対策ソフトウェアは常時起動させ、パターンファイル等の自動更新を設定するなど、常に最新の状態を保つようにしてください。

(3) ウイルス感染時に備えて、定期的にデータのバックアップを行ってください。

(4) ウイルスに感染した場合又は感染の疑いがある場合は、直ちに情報機器や電磁的記録媒体をネットワークから切り離し、情報セキュリティ責任者へ報告してください。その際に使用していた情報機器やUSBメモリ等の電磁的記録媒体は、他で使用せずに隔離し、情報セキュリティ責任者の指示に従ってください。

11　ID・パスワードの利用と設定

ID及びパスワードは、個人ごとに管理するようにし、貸し借り禁止等の注意事項を遵守しなければなりません（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が認めた共用ID等を利用する場合を除きます。）。

◇　管理方法等

(1) IDとパスワードは、個人ごとに管理するようにし、メモを作成したり、他人の目につくような場所に放置してはいけません。メモを作成した場合は、施錠保管するなど、厳重に管理してください。また、パスワードの照会には一切応じないでください。

(2) パスワードについて初期に設定されたものは速やかに変更してください。古いパスワードの再利用も原則として使用しないようにしてください。

(3) パスワードの設定については、情報セキュリティ対策基準に定められた要件を守り、十分な長さと文字列は本人の属性に関係ないものなど想像しにくいものにしてください。また、英字については、大文字・小文字を区別し、その両方を組み合わ

せることで安全性が高まります。

(4) ID・パスワードを共有したり、貸し借りしないでください。他人のIDやパスワードを使って情報システム等にログインしてはいけません。

【補足事項】

・システムに定められたパスワード設定基準を守ること
・単純な文字列や本人の属性等から他人に類推されやすい文字列等でないこと
・ID・パスワードは、個人ごとに管理すること
・パスワードの照会には一切応じないこと

12　電子データのファイル共有

電子データを利用するため、ネットワークを介したファイル共有を行う場合は、業務に必要のない者がファイル等の閲覧及び利用ができないよう設定してください。

◇　管理方法等

(1)　電子データをネットワーク上の共有されている領域に保存する場合は、共有領域又は個別ファイルについて、電子データの重要度に応じてアクセス可能なID、パスワード及びそれらへの読み出し・書き込み・実行等、適切なアクセス権を設定してください。

(2) 機密性分類３の電子データは、共有されている領域上に保存しないでください。また、同一所属内であっても、担当以外の職員が閲覧及び使用できないよう設定してください。

(3)　同一の利用者IDの複数職員での利用は、業務上必要な場合等の最小限にしてください。

(4)　ファイルサーバ等に記録された情報について、機器の障害等による電子データ消滅に備え、定期的なバックアップを実施し、必要に応じて、サーバ等の冗長化対策を実施してください。

13　各課等で管理責任のあるシステムのバックアップ

各課等で管理しているシステムに記録された情報は、冗長化対策の有無にかかわらず、必要に応じてバックアップを実施しなければなりません。

◇　管理方法等

(1)　重要なサーバについては、そのデータ及びログを定期的にバックアップしなければなりません。

(2) バックアップに使用する媒体は、鍵付きの保管場所に保存し、担当者が責任を持って管理しなければなりません。

(3) パッチの適用など、サーバのシステムに対して何らかの変更を行う場合、変更後の不具合が発生する可能性があります。そのため、サーバに対して変更を行う前にサーバのシステムバックアップを行わなければなりません。

14　情報資産の廃棄手順

パソコン等の情報資産を廃棄する場合は、情報セキュリティ責任者の許可を得るとともに、情報漏えいを防ぐため、記録された情報を復元できないように処置しなければなりません。

◇　管理方法等

(1) 情報セキュリティ責任者の許可

①　情報資産の廃棄を行う場合は、事前に情報セキュリティ責任者の許可を得てください。

②　情報セキュリティ責任者は、廃棄する情報資産の範囲、廃棄理由、処分方法等を確認してください。

(2) データのバックアップ

①　廃棄する情報資産に記録されている情報を確認してください。

②　重要な情報が保存されている場合は、バックアップをとり、適正に保管してください。

(3) データの消去

①　データ消去ソフト等を利用し、保存されている全データを消去してください。

②　機密性分類２以上の情報を記録している電磁的記録媒体を廃棄する場合は、裁断等の物理的な破壊等により、情報を復元できないようにしてください。

③　データが全く消去できない場合は、内蔵されているハードディスク等を取り外し、裁断等により、物理的に破壊してください。内蔵ハードディスク等を取り外すことができない場合は、パソコン等の情報資産自体を物理的に破壊してください。

④　機密性分類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、裏面再利用はしないでください。

(4) その他

① 廃棄に当たっては、適切に処理するとともに、廃棄処理日時、内容等を記録してください。

② 物品の廃棄について、上記手順のほか、別に定める手順がある場合は、それに従ってください。

③ パソコン等のリース物件を返却する場合は、保存している全データを消去してください。また、リース契約の内容や仕様を確認するとともに、当該リース業者に確認をとりながら処理してください。

15 情報セキュリティインシデント発生時の対応

日頃から、情報セキュリティインシデント発生時の対応手順を確認しておき、実際に事故が発生した場合には、対応手順に従い、迅速かつ適正に対応しなければなりません。

◇ 管理方法等

(1) 情報漏えい、紛失、盗難、ウイルス感染等の情報セキュリティインシデントが発生した場合は、速やかに情報セキュリティ責任者（不在時にはCSIRT）に報告し、指示を仰いでください。

(2) 具体的な対応手順については、別に定める「３ 情報セキュリティインシデント対応実施手順」により行ってください。

16　テレワークの情報セキュリティ留意点

日常業務を自宅など庁舎外で行う場合の留意点を確認し、外部からのサイバー攻撃や、人的ミスからのインシデントにつながらないよう十分注意を払ってください。

◇　管理方法等

(1) 個人使用パソコンの修正プログラム適用

村支給のパソコン使用が前提ですが、情報セキュリティ責任者の許可を得た個人利用パソコンは、最新のOSと不正プログラム対策ソフトウェア環境を必須とします。特に、不正プログラム対策ソフトウェアは、責任を持って最新のバージョンに更新してください。

(2) パスワードの適切な設定と管理

パスワードは可能な範囲で複雑な長い文字列を設定し、大小英字、数字及び記号を混在させてください。他のシステムやインターネットサービスで、同じパスワードを使い回さないでください。

(3) 不審なメールに注意

日々届くメールの中には、ウイルスを組み込んだファイルが添付されていたり、ウイルスを仕掛けたサイトやフィッシングサイトへ誘導するURLが記載されていたりという可能性があります。これらの添付ファイルを開く、あるいはURLをクリックする等により被害に遭う場合があります。少しでも不審を抱いたメールの添付ファイルやURLは不用意にクリックせずに、情報セキュリティ責任者に報告してください。なお、標的型攻撃メールのように、実在の組織や人物をかたったり、ごく自然な日本語表現で違和感がなかったりと、一見して不審を抱きにくい場合があります。受信したメールの正当性が判断できない場合は、情報セキュリティ責任者へ相談し、必要に応じてメールの送信者となっている組織への確認をしてください。

(4) USBメモリ等の取扱いの注意

ウイルス感染の可能性があるため、村支給以外のUSBメモリ等の電磁的記録媒体は、パソコンに接続しないでください。

(5) 庁内ネットワークへの機器接続ルールの遵守

LGWANへのアクセスは定められたアクセス制限の範囲で行ってください。

機密性２、可用性２、完全性２以上の情報にアクセスする際は、情報セキュリティ責任者の許可をとった上でアクセス権限を受けてください。

(6) 電子メールの注意点

長野県セキュリティクラウド経由のメール送受信のみを可能とします。フリーメール等は不可とします。個人使用のメールアドレスを誤って使用しないよう、注意してください。

(7) ソフトウェアをインストールする際の注意

ソフトウェア（フリーソフト等）をインターネットからダウンロードしたり、自身のパソコンにインストールしたりする場合は、情報セキュリティ責任者に事前に許可をとってください。

(8) パソコン等の画面ロック機能の設定

家族を含め、第三者に見られたり、操作されたりしないよう、パソコンには画面ロックを設定してください。

(9) 紙媒体（各資料等）の持ち出し

機密性２、可用性２、完全性２以上の情報を自宅などに持ち出す場合は、機密情報外部持ち出し申請書（様式２）に記入後、情報セキュリティ責任者の許可を得てください。基本的に、マイナンバー情報、個人情報は持ち出し不可とします。

(10) データ保存について

機密性２、可用性２、完全性２以上の情報をパソコン処理した場合は、処理後にデータを消去し、パソコンが盗難や故障などのトラブルに陥った場合でも、データの漏えいや破損にならぬよう運用してください。

17　Web 会議サービスの利用時の対策

原則として、村支給のパソコンを使用し、許可された最新バージョンの Web 会議サービスを使用する等、情報セキュリティ対策を講じての利用が必要です。

(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りません。

(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ュリティ対策を実施してください。

(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じてください。

(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りません。

18　ソーシャルメディアサービスの利用

ソーシャルメディアサービス運用手順にのっとり、他者の乗っ取りやなりすまし対策を講じることはもちろん、私的な活用は厳禁とします。

(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りません。

（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が必要です。

（イ）パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USBメモリ、紙等）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してください。

(2) 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いけません。

(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りません。

(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りません。

(5) 可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、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にしてください。

３　情報セキュリティインシデント対応実施手順

１　情報セキュリティインシデント対応の基本的な心構え

情報セキュリティインシデント発生後に行う対応の最大の目的は、「インシデントによる直接的・間接的被害を最小限に抑える」ことにあります。
CSIRT との共同体制で適切な対応を実施してください。

(1) 被害拡大防止・二次被害防止・再発防止

情報セキュリティインシデントが発生した場合に、最も大切なのは、事故による被害・影響を最小限にすることです。また、一度発生した事故は、二度と起こることのないよう再発防止にも努めなければなりません。

(2) 事実確認と情報の一元管理

情報セキュリティインシデントの対応に当たっては、正確な情報の把握に努めてください。臆測や類推による判断や不確かな情報による発言等は、事態の混乱を招くおそれがあります。また、所属内の情報を一元管理し、インシデントの調査内容の報告や外部に対する情報提供に関しても窓口をCSIRTに一本化してください。

(3) 透明性・情報開示

被害拡大防止や類似情報セキュリティインシデントの防止、説明責任の観点から必要と判断される場合は、組織の透明性を確保し、情報を開示する姿勢で臨むことが好ましく、村への信頼にもつながると考えられます。公表により、被害拡大が見込まれる特殊なケース以外は、情報セキュリティインシデントに関する情報を公開することを前提とした対応を心がけてください。

(4) 組織としての対応

情報セキュリティインシデント対応においては、様々な困難な判断を迅速に行わなければならず、精神的にも大きな負担がかかります。また、行政運営、広報、技術、法律等、様々な要素を考慮する必要があるため、組織で対応していくことが重要です。職員個人の判断で行動することのないよう注意してください。

(5) 事前対策の徹底

情報セキュリティインシデント発生時における体制や連絡要領等を事前に準備しておくと、いざというときに大変役立ちます。緊急時、夜間、休日の対応方針や手順を作成し、日頃から点検、訓練等をしておくように努めてください。

2　情報セキュリティインシデント対応の基本的な対応手順

対応の手順は、情報セキュリティインシデントの内容によって異なりますが、おおむね次の手順により対応してください。いくつかの手順を同時に進行しなければならない事態も考えられます。

		CSIRT への報告時期
発生Ⅰ		
（1） 発見・報告	情報セキュリティインシデントの予兆や具体的な事実を確認した場合は、情報セキュリティ責任者に報告し、速やかに事故対応のための体制をとります。不正アクセスや不正プログラム等の場合は、不用意な操作はせず、残された証拠を消さないようにしてください。また、外部からの通報の場合は、相手の連絡先等を必ず控えるようにしてください。	①　第一報（発生） CSIRT への報告、共同対応
（2） 初期対応	対応の体制を整え、当面の対応方針を決定してください。事情報セキュリティインシデントによる影響（被害）の拡大、二次被害の防止のために、情報の隔離、ネットワークの遮断、サービス停止等、必要な応急措置を行ってください。	
（3） 調査	適切な対応を行うために５Ｗ１Ｈ（いつ、どこで、誰が、何を、なぜ、どうしたのか）の観点で調査し、情報を整理してください。また、事実関係を裏付ける情報や証拠を確保してください。	②　中間報告（原因・対応状況）
（4） 通知・公表等	情報セキュリティインシデントの影響が及ぶ住民等への通知、警察等への届出、ホームページやマスコミ等による公表を検討してください。ただし、公表により被害拡大を招くおそれがある場合もあるので、公表の時期や対象等を十分考慮してください。	
（5） 抑制措置と復旧	情報セキュリティインシデントによる影響（被害）の拡大防止と復旧のための措置を行ってください。また、再発防止に向けた具体的な取組を行い、停止したサービス、アカウント等を復旧してください。	
（6） 事後対応	抜本的な再発防止策を検討し実施してください。また、情報セキュリティインシデントについて統括し、被害者への説明・謝罪・補償、関係職員の処分等、必要な措置を行ってください。	③　最終報告（原因・対応状況・再発防止策）

3　情報セキュリティインシデント報告におけるポイント

情報セキュリティインシデント対応においては、事実確認と情報の一元管理が重要です。情報セキュリティインシデントに関する正確な情報を整理し、情報セキュリティインシデント情報共有シート等により、まとめてください。

(1) 情報セキュリティインシデント情報の一元管理

情報セキュリティインシデントに関する正確な情報を把握し、「インシデント報告書（IT障害）（様式13）」にまとめて所属内及びCSIRTで情報を共有してください。

(2) CSIRTへの報告

① 第一報

情報セキュリティインシデントの予兆や具体的な事実を確認した場合は、「インシデント報告書（IT 障害）（様式 13)」により、速やかに CSIRT に報告してください。

CSIRT

――内線（総務課 企画財政係）120～123

e-mail　kikakuzaisei@vill.otari.nagano.jp 及び kikaku@vill.otari.nagano.jp

② 中間報告

情報セキュリティインシデント原因等の調査が進み、全容がおおむね把握できた場合は、「インシデント報告書（IT 障害）（様式 13)」により、CSIRT に中間報告をしてください。事故内容等により、CSIRT が、報告の時期や回数等を指示することがあります。

③ 最終報告

おおむね情報セキュリティインシデント対応が終了した場合は、「インシデント報告書（IT 障害）（様式 13)」により、CSIRT に最終報告をしてください。

【報告対象となる情報セキュリティインシデント等】

- 個人情報等の機密情報が記録されているパソコン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。）
- 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、改ざん、消去等
- 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
- 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、消去等のうち、重大な支障が生じたもの
- その他、上記に準ずる情報資産に脅威を及ぼす事象の発生

4　情報セキュリティインシデントのタイプによる対応ポイント

情報セキュリティインシデントには、その原因によりいくつかのタイプがあり、そのタイプや漏えいした情報の種類により、必要な対応が異なります。

(1) 紛失・盗難　　(2) 誤送信・Web での誤公開等
(3) 内部犯行　　(4) ファイル交換ソフトの利用
(5) 不正プログラム　　(6) 不正アクセス
(7) ブログ・掲示板等掲載

(1) 紛失・盗難

これは、パソコンやUSBメモリの入った鞄を電車内や店舗に忘れたり、事務室等に保管していたパソコンが盗難に遭い、情報の紛失、漏えいにつながるケースです。

① 発見及び報告

イ　職員の自己申告、警察や拾得者からの連絡により発覚します。

ロ　職員の自己申告の場合は、もう一度所持品等を確認し、紛失又は盗難に間違いない場合には、紛失場所と思われる施設等の窓口（鉄道会社担当窓口、店舗窓口等）に連絡してください。

ハ　「インシデント報告書（IT障害）（様式13）」により、速やかにCSIRTに報告してください。

② 初期対応

イ　何の情報がどの程度含まれていたのか、暗号化やアクセス制限による保護の有無を確認してください。

ロ　事実関係を５Ｗ１Ｈ（いつ、どこで、誰が、何を、なぜ、どうしたのか）で整理してください。

ハ　CSIRTと共同で警察に遺失届又は被害届を提出してください。

ニ　アカウント情報が含まれている場合は、パスワードの変更やアカウント停止等の措置をとってください。

③ 調査

イ　残っている記録等から紛失・盗難に遭った情報をなるべく正確に把握してください。

ロ　情報の内容、保護措置の有無等から、想定される二次被害を確認してください。

ハ　紛失物等がネットオークション等に出品されていないか、必要に応じて確認してください。

④ 通知・公表等

イ　「５　公表、警察への届出に当たっての考え方」を参照してください。

ロ　個人情報の漏えいのおそれがある場合は、本人への通知と謝罪を行うととも

に、二次被害に遭わないよう注意喚起してください。

⑤　抑制措置及び復旧

イ　二次被害防止策をとってください。例えば、情報に銀行口座番号が含まれていた場合は、口座の停止を促すなどが考えられます（他の情報セキュリティインシデントのタイプにおいても同様です。）。

ロ　必要に応じてバックアップやコピー等から修復可能な情報を復旧してください。

⑥　事後対応

イ　情報セキュリティインシデントの再発防止策を検討し、実施してください。例えば、庁舎への侵入防止、情報資産の保管・持ち出し管理等、物理面や運用面での問題点を総合的に勘案して実施します。

ロ　必要に応じて、情報漏えいによる被害の補償等救済処置を検討してください。

ハ　おおむね情報セキュリティインシデント対応が終了した場合は、「インシデント報告書（IT障害）（様式13）」により、CSIRTに最終報告をしてください。

(2) 誤送信・Webでの誤公開等

BCCで送信すべきところをToやCCで送信し、他人の電子メールアドレスが漏えいしたり、Webページの公開サーバの設定を誤り、個人情報が公開されてしまうなど、システム等の誤操作、誤設定等により情報が流出するケースです。

①　発見及び報告

イ　職員の自己申告や受信者等の第三者からの連絡により発覚します。外部から指摘された場合は、通報者の連絡先を確認してください。

ロ　「インシデント報告書（IT障害）（様式13）」により、速やかにCSIRTに報告してください。

②　初期対応

イ　何の情報がどの程度含まれていたのか、暗号化やアクセス制限による保護の有無を確認してください。

ロ　事実関係を５Ｗ１Ｈ（いつ、どこで、誰が、何を、なぜ、どうしたのか）で整理してください。

ハ　誤送信の場合は、受信者に対し誤送信について謝罪し、受信した情報を削除するよう依頼してください。

ニ　誤公開の場合は、直ちに当該情報を削除するかアクセス制限を施し、外部から閲覧できないようにしてください。

③　調査

イ　漏えいした情報の範囲、原因、被害の状況等について調査してください。

ロ　誤公開の場合は、どういった範囲で何人が閲覧したかアクセスログを使って調査してください。

ハ　情報の内容、保護措置の有無等から、想定される二次被害を確認してください。

④　通知・公表等

イ　「５　公表、警察への届出に当たっての考え方」を参照してください。

ロ　個人情報の漏えいのおそれがある場合は、本人への通知と謝罪を行うとともに、二次被害に遭わないよう注意喚起してください。

⑤　抑制措置及び復旧

二次被害防止策をとってください。例えば、情報システムの不具合が原因の場合は、システムの修正や使用の制限が考えられます。また、人的なミスの場合は、ミスを見逃さないようなチェック体制を検討したり、Web ページの設定を再確認し、必要な設定変更をすることが考えられます。

⑥　事後対応

イ　情報セキュリティポリシーの内容を確認するとともに、情報セキュリティインシデントの再発防止策を検討し、実施してください。例えば、多数の送信先に一斉送信する場合の手順について、ミスの原因とミスを見逃した原因の両面から検討し、新たな作業手順を策定したり、Webページの設定要領の見直し等があげられます。

ロ　必要に応じて、情報漏えいによる被害の補償等救済処置を検討してください。

ハ　おおむね情報セキュリティインシデント対応が終了した場合は、「インシデント報告書（IT障害）（様式13）」により、CSIRTに最終報告をしてください。

(3) 内部犯行（情報の持ち出し等）

これは、職員が不正に情報を持ち出し、外部の第三者に売ったり渡したりするケースです。CSIRTを中心に調査及び報告等を行います。

①　発見及び報告

イ　ダイレクトメールや架空請求、振り込め詐欺等、外部の第三者から自分の情報が不正に利用されているようだとの連絡により、発覚する傾向があります。外部から通報された場合は、通報者の連絡先を確認するとともに、どういった情報が不正利用されているのかを確認してください。

ロ　「インシデント報告書（IT障害）（様式13）」により、速やかにCSIRTに報告してください。

②　初期対応

イ　何の情報がどの程度含まれていたのか、暗号化やアクセス制限による保護の有無を確認してください。

ロ　事実関係を５Ｗ１Ｈ（いつ、どこで、誰が、何を、なぜ、どうしたのか）で整理してください。

ハ　内部犯行の場合は、漏えいの規模や範囲が大きくなる傾向があるため、慎重に対応してください。また、職員による犯行の可能性がある場合は、証拠を隠滅さ

れないよう注意する必要があります。

③　調査

イ　漏えいした情報の範囲、原因、被害の状況等について調査してください。

ロ　漏えい情報の範囲から、情報が持ち出された時期や当該情報にアクセスできた人物を絞り込んでください。

ハ　情報の内容、保護措置の有無等から、想定される二次被害を確認してください。

④　通知・公表等

イ　「５　公表、警察への届出に当たっての考え方」を参照してください。

ロ　犯罪に発展する可能性がある場合は、早めに警察に相談してください。

ハ　個人情報の漏えいのおそれがある場合は、本人への通知と謝罪を行うとともに、二次被害に遭わないよう注意喚起してください。

⑤　抑制措置及び復旧

イ　内部犯行当事者を特定し、二次被害防止策をとってください。例えば、漏えい情報の回収やID・パスワード、アクセス権限の見直し等の情報管理体制の強化が考えられます。

ロ　必要に応じて、アカウントの再発行や登録情報の変更等を行い、通常業務に復帰してください。

⑥　事後対応

イ　情報セキュリティポリシーの内容を確認するとともに、情報セキュリティインシデントの再発防止策を検討し、実施してください。例えば、重要情報の施錠管理の徹底や適正なアクセス権限の設定等があります。

ロ　必要に応じて、情報漏えいによる被害の補償等救済処置を検討してください。

ハ　おおむね情報セキュリティインシデント対応が終了した場合は、「インシデント報告書（IT障害）（様式13）」により、CSIRTに最終報告をしてください。

(4) ファイル交換ソフトの利用

これは、Winny、Shareに代表される匿名ファイル交換ソフトの利用者がウイルスに感染し、自宅に持ち帰った業務データや電子メールの内容等を流出させてしまうようなケースです。

①　発見及び報告

イ　外部の第三者からの通報により、発覚する傾向があります。外部から通報された場合は、通報者の連絡先を確認するとともに、どのような情報が漏えいしているのかなどを確認してください。

ロ　「インシデント報告書（IT障害）（様式13）」により、速やかにCSIRTに報告してください。

②　初期対応

イ　漏えいした情報の内容や範囲を確認してください。また、漏えい元を特定し、

関係する職員に調査の協力を依頼してください。

ロ　事実関係を５Ｗ１Ｈ（いつ、どこで、誰が、何を、なぜ、どうしたのか）で整理してください。

ハ　漏えい元となったパソコンをネットワークから分離するとともに、ファイル交換ソフトがまだインストールされている場合は、利用を停止させてください。また、漏えい情報の特定のためにも、漏えい元パソコンは可能な限り手を加えない状態で提出させてください。

③　調査

イ　CSIRTは漏えいした情報の内容、範囲等について調査してください。また、情報漏えいの原因や漏えいに至った経緯について、職員からの聞き取り等により調査してください。

ロ　情報の内容、保護措置の有無等から、想定される二次被害を確認してください。

④　通知・公表等

イ　「５　公表、警察への届出に当たっての考え方」を参照してください。

ロ　個人情報の漏えいのおそれがある場合は、本人への通知と謝罪を行うとともに、二次被害に遭わないよう注意喚起してください。

ハ　Winny等は要求の多いファイルをネットワーク上の多くのコンピュータに拡散させる仕組みを持っているため、漏えいがいつまでも続く可能性があります。事件の公表により、Winny等のダウンロードを誘発するおそれがある場合は、公表を控えるという考え方もありますが、被害拡大防止の観点から最善と思われる措置をとる必要があります。

⑤　抑制措置及び復旧

イ　二次被害防止策をとってください。例えば、ウイルスの駆除、職員の私物パソコンからの重要情報の削除、ファイル交換ソフトのアンインストール等が考えられます。

ロ　Winny等による情報漏えいの場合、ネットワーク上から情報を完全に削除することは不可能であることから、話題性を高めずにネットワーク上からファイルが自然消滅するのを待つのが得策と考えられています。

ハ　業務データを持ち出して自宅のパソコンに保存することにより漏えいすることが多いため、庁舎外への重要情報の持ち出し制限を再徹底してください。

二　職員に対し、ファイル交換ソフトの危険性を周知するとともに、必要に応じて、ファイル交換ソフトの利用状況調査等を行うことも考えられます。

⑥　事後対応

イ　情報セキュリティポリシーの内容を確認するとともに、情報セキュリティインシデントの再発防止策を検討し、実施してください。例えば、重要情報の持ち出し制限や私物パソコンの利用制限等を職員に周知し、徹底させることなどが

考えられます。

ロ　必要に応じて、情報漏えいによる被害の補償等救済処置を検討してください。

ハ　おおむね情報セキュリティインシデント対応が終了した場合は、「インシデント報告書（IT障害）（様式13）」により、CSIRTに最終報告をしてください。

(5) 不正プログラム（ウイルス、スパイウェア等）

これは、ウイルスに感染してデータ等が流出したり、スパイウェアによりパソコンで入力した内容が外部に送信されたりするケースです。

① 発見及び報告

イ　不正プログラム対策ソフトウェアによる検知、ネットワークの監視、メール等を受信した外部の第三者からの通報により発覚します。外部から通報された場合は、通報者の連絡先を確認してください。

ロ　「インシデント報告書（IT障害）（様式13）」により、速やかにCSIRTに報告してください。

② 初期対応

イ　何の情報がどの程度含まれていたのか、暗号化やアクセス制限による保護の有無を確認してください。

ロ　事実関係を５Ｗ１Ｈ（いつ、どこで、誰が、何を、なぜ、どうしたのか）で整理してください。

ハ　不正プログラムに感染した場合は、パソコン等の端末をネットワークから分離するとともに、情報システムの運用を停止し、不正プログラムの除去を行ってください。

二　不正プログラムの種類を特定できる場合は、独立行政法人情報処理推進機構（IPA）やウイルス対策ベンダー等が公開している情報に基づき対処してください。

③ 調査

イ　重要な情報を電磁的記録媒体にバックアップしてください。バックアップにも不正プログラムが混入している可能性があるので、注意してください。

ロ　パソコンに残されたデータやアクセス履歴等から漏えいした情報を特定してください。

ハ　情報の内容、保護措置の有無等から、想定される二次被害を確認してください。

④ 通知・公表等

イ　「５　公表、警察への届出に当たっての考え方」を参照してください。

ロ　個人情報の漏えいのおそれがある場合は、本人への通知と謝罪を行うとともに、二次被害に遭わないよう注意喚起してください。

⑤ 抑制措置及び復旧

イ　二次被害防止策をとってください。例えば、ウイルス名の特定と駆除、セキュ

リティホール等の脆弱性の除去等が考えられます。

ロ　感染したパソコンは、念のためOSからインストールし直すほか、ソフトウェア等もバックアップから戻さず、再インストールしてください。

ハ　バックアップしておいたデータをパソコンに復旧する場合は、アップデートを実施して最新の状態にした不正プログラム対策ソフトウェアでチェックを行い、安全を確認してから復旧してください。

⑥　事後対応

イ　情報セキュリティポリシーの内容を確認するとともに、情報セキュリティインシデントの再発防止策を検討し、実施してください。例えば、添付ファイルやリンクをむやみに開かない、使用しているアプリケーションに最新のセキュリティパッチを適用して脆弱性を除去するなど、電子メールやインターネット利用時の注意点を周知徹底させるなどが考えられます。

ロ　必要に応じて、情報漏えいによる被害の補償等救済処置を検討してください。

ハ　おおむね情報セキュリティインシデント対応が終了した場合は、「インシデント報告書（IT障害）（様式13）」により、CSIRTに最終報告をしてください。

(6) 不正アクセス

これは、アクセス制限を設けているコンピュータにネットワーク外部から不正に侵入されて情報を盗まれるようなケースです。

①　発見及び報告

イ　不正アクセスは、インターネットに接続しているサーバに対し行われることが多いことから、アクセスログの確認やセキュリティ対策機器の警報によって発覚する傾向があります。

ハ　不正アクセスが明らかな場合は、必要に応じて、警察に相談してください。

ロ　「インシデント報告書（IT障害）（様式13）」により、速やかにCSIRTに報告してください。

②　初期対応

イ　何の情報がどの程度含まれていたのか、暗号化やアクセス制限による保護の有無を確認してください。

ロ　事実関係を５Ｗ１Ｈ（いつ、どこで、誰が、何を、なぜ、どうしたのか）で整理してください。

ハ　不正アクセスにより、個人情報等の重要な情報が漏えいする危険が確認された場合は、直ちにネットワークから切り離し、システムの運用停止等の処置をとってください。

二　不正アクセスされた原因や経路を特定しないうちに、不正アクセスを受けたサイトの代替サイトを立ち上げる場合は、再び不正アクセスされる可能性があるため注意が必要です。

③　調査

イ　不正アクセスされた原因や経路のほか、何の情報にアクセスした形跡があるかなどを調査してください。

ロ　不正アクセスの場合、機器に残された記録が重要な証拠になるため、内容が変更されたりしないように証拠保全の措置をとってください。

ハ　情報の内容、保護措置の有無等から、想定される二次被害を確認してください。

④　通知・公表等

イ　「５　公表、警察への届出に当たっての考え方」を参照してください。

ロ　個人情報にアクセスされた可能性がある場合は、その範囲を特定した上で、本人への通知と謝罪を行うとともに、二次被害に遭わないよう注意喚起してください。

⑤　抑制措置及び復旧

イ　二次被害防止策をとってください。例えば、Webサーバの設定見直し、ID・パスワード、アクセス権限の見直し、Webアプリケーション等の脆弱性の除去等が考えられます。

ロ　不正アクセスを受けたサーバ等の内容をバックアップし、再発防止策をとった上で業務を復旧します。

ハ　アカウント情報が漏えいした場合には、アカウントの再発行やパスワードの変更等を行ってください。

⑥　事後対応

イ　情報セキュリティポリシーの内容を確認するとともに、情報セキュリティインシデントの再発防止策を検討し、実施してください。例えば、使用していないポートの閉鎖、Webページ改ざん検知ソフトの利用、不正アクセス監視の強化等が考えられます。

ロ　必要に応じて、情報漏えいによる被害の補償等救済措置を検討してください。

ハ　おおむね情報セキュリティインシデント対応が終了した場合は、「インシデント報告書（IT障害）（様式13）」により、CSIRTに最終報告をしてください。

(7) ブログ・掲示板等掲載

これは、職員がブログやホームページで本来非公開の情報を掲載してしまったり、特定の職員しか知らないはずの情報が掲示板に書き込まれたりするケースです。

①　発見及び報告

イ　職員による発見や第三者からの通報により発覚します。外部から通報された場合は、通報者の連絡先を確認してください。

ロ　「インシデント報告書（IT障害）（様式13）」により、速やかにCSIRTに報告してください。

② 初期対応

イ 何の情報がどの程度掲載されていたのかを確認してください。

ロ 事実関係を５Ｗ１Ｈ（いつ、どこで、誰が、何を、なぜ、どうしたのか）で整理してください。

ハ 職員個人のブログの場合は、当該職員に注意し、削除させてください。

ニ 掲示板への書き込みの場合は、掲示板の管理人に対し、削除を依頼してください。なお、管理人が削除に応じない場合は、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）（平成13年法律第137号）」に基づく法的手続も検討してください。

③ 調査

イ CSIRTは漏えいの経路等を職員からの聞き取り等により調査してください。

ロ 必要に応じて、同様の情報が他の掲示板等に掲載されていないか調査してください。

ハ 情報の内容等から、想定される二次被害を確認してください。

④ 通知・公表等

イ 「５ 公表、警察への届出に当たっての考え方」を参照してください。

ロ 個人情報が含まれている場合は、本人への通知と謝罪を行うとともに、二次被害に遭わないよう注意喚起してください。

⑤ 抑制措置及び復旧

イ 二次被害防止策をとってください。例えば、情報の重要性分類を実施することや当該分類に応じた管理方法を周知徹底するなどが考えられます。

ロ 情報漏えいに至った原因に対応した再発防止策を検討します。

⑥ 事後対応

イ 情報セキュリティインシデントの再発防止策を検討し、実施してください。例えば、重要性に基づく情報分類の確認、重要性分類に応じた情報の取扱制限の確認、これらの職員に対する研修等の実施等が考えられます。

ロ 必要に応じて、情報漏えいによる被害の補償等救済処置を検討してください。

ハ おおむね情報セキュリティインシデント対応が終了した場合は、「インシデント報告書（IT障害）（様式13）」により、CSIRTに最終報告をしてください。

５ 公表、警察への届出に当たっての考え方

情報の公開により被害の拡大が見込まれるようなケースを除き、情報を公開することを前提として対応することにより、組織の透明性確保や村への信頼につながります。

(1) 公表等の考え方

① 組織の透明性の確保や村への信頼の観点から、情報セキュリティインシデントに関する情報を公開することを前提とした対応を心がけてください。

② 個人情報が漏えいした場合は、本人にその事実を知らせ謝罪するとともに、詐欺や迷惑行為等の二次被害に遭わないよう注意喚起してください。

③ 公表は個人情報漏えいの被害者や関係者の意向を確認した上で、最終的に判断し、ホームページへの掲載、記者発表（プレスリリース）、記者会見等により公表します。

④ 公表に当たっては関係課等と調整を行ってください。

⑤ ホームページや記者発表資料に盛り込む内容は下記を参考にしてください。

タイトル（「○○の情報漏えいについて」等）

序文（情報セキュリティインシデント発生に対する謝罪、村としての姿勢等）

1 情報セキュリティインシデントの経緯（発生～発覚～現在）

2 調査方法及び状況

3 漏えいした情報の内容

4 情報セキュリティインシデントの被害状況（二次被害二次被害を含む）

5 情報セキュリティインシデントの原因

6 当面の対応策

7 再発防止策

8 問合せ窓口

⑥ マスコミとの対応に当たっては、窓口を一本化し、対外的な情報に不整合が生じないようにします。また、取材は電話ではなく、なるべく対面での対応とし、２～３件以上の取材申込みがきた場合は、記者会見の開催を検討します。

⑦ 取材や記者会見での対応においては、記者発表資料のほかに事実関係等を説明する手持ち資料を準備し、正確な情報が伝わるようにします。記者会見の場合は、仮想問答集を作成するなど対応の準備をしますが、回答できない質問があった場合は、その場で無理に対応しようとせず、確認の上、追って回答するようにします。

(2) 警察への届出

① 紛失の場合は、遺失届を提出してください。

② 盗難の場合は、被害届を提出してください。

③ 以下のような場合は、被害届を提出することを検討してください。

イ　職員の内部犯行により情報が漏えいした場合（収賄、「地方公務員法」違反等）
ロ　外部からの不正アクセス等によって情報が漏えいした場合（「不正アクセス行為の禁止等に関する法律」（不正アクセス禁止法）違反）
ハ　漏えい情報に関して不正な金銭等の要求を受けた場合（恐喝、脅迫、強要等）

様式13

最高情報セキュリティ責任者	統括情報セキュリティ責任者	情報セキュリティ責任者

最高情報セキュリティ責任者（副村長）　様

インシデント報告書（IT障害）

（第　　報）

情報連絡日時　　年　　月　　日　　時

情報連絡元	課室名		情報セキュリティ責任者（課室長名）	㊞
	報告者名	㊞		
	電話番号（内線）			
	電子メールアドレス		FAX番号	

①発生した事象の分類

事象の類型		事　象　の　例	チェック（1つのみ選択）
未発生の事象		予兆・ヒヤリハット	
発生した事象	機密性を脅かす事象	情報の漏えい（組織の機密情報等の流出など）	
	完全性を脅かす事象	情報の破壊（Webサイト等の改ざんや組織の機密情報等の破壊など）	
	可用性を脅かす事象	システム等の利用困難（制御システムの継続稼働が不能やWebサイトの閲覧が不可能など）	
	上記につながる事象	コンピュータウイルス等の感染（コンピュータウイルス等によるシステム等への感染）	
		不正プログラム等の実行（システムの脆弱性等をついた不正コード等の実行）	
		システム、サーバ等への侵入（外部からのサイバー攻撃等によるシステム等への侵入）	
		システムの動作不良（コンピュータウイルス等の感染、故障）	
		システム非稼働・非起動（電源供給なし・故障）	
		その他	

②上記事象における原因の分類

原因の類型	原　因	チェック（複数選択可）
意図的な原因	不審メール等の受信	
	ユーザID等の誤り（なりすまし等）	
	DoS攻撃等の大量アクセス	
	情報の不正取得	
	内部不正	
	適切なシステム運用等の未実施	
偶発的な原因	ユーザの操作ミス	
	ユーザの管理ミス	
	不審なファイルの実行	
	不審なサイトの閲覧	
	委託先の管理ミス	
	機器等の故障・電源供給なし	
	システムの脆弱性	
	他分野の障害からの波及	
環境的な原因	災害等	
その他の原因	その他 （　　）	
不　　明		

（報告）

担当職員（申請者）→ 情報セキュリティ責任者 → 統括情報セキュリティ責任者 → 最高情報セキュリティ責任者

◆情報連絡の内容(※1)　(別紙有無　□有　□無)

<table>
<tr><th>項　目</th><th colspan="2">情　報　の　内　容</th></tr>
<tr><td>③IT 障害の発生日時</td><td colspan="2">年　月　日　時　分</td></tr>
<tr><td rowspan="3">④概　要</td><td colspan="2">判明日時：　年　月　日　時　分
(発生日時：　年　月　日　時　分)</td></tr>
<tr><td colspan="2">事象が発生したシステム等　：</td></tr>
<tr><td colspan="2">発生事象の概要　：

システムの稼働状況　：□影響なし　□停止中　□一部稼働中　□復旧済</td></tr>
<tr><td>⑤重要インフラや
サービス等への影響</td><td colspan="2">重要インフラやサービスの維持レベル逸脱の有無　：　□有　□無
他の重要インフラ分野への波及の可能性　：　□有　□無</td></tr>
<tr><td rowspan="10">⑥当該事象に係る推移等</td><td>日　時</td><td>事象・対応状況等</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">(補足情報)</td></tr>
<tr><td colspan="2">対外的な対応状況
報道発表、報道等への掲載　：□済　□予定有　□予定無
連絡を行った先(CSIRT 等実施機関内)　：(　)
連絡を行った先(実施機関外)
□総務省　長野県　長野県警　個人情報保護委員会
□その他（　）</td></tr>
<tr><td>⑦今後の予定</td><td colspan="2">□事象継続中　(続報あり)
□事後調査実施中　(続報あり)
□今後の対応策を継続検討　(続報なし)
□総務省</td></tr>
<tr><td>⑧その他
・得られた教訓等</td><td colspan="2"></td></tr>
</table>

※1：情報連絡の迅速性を優先するため、必ずしも全ての項目を記載する必要はありません。

4　業務委託における情報セキュリティの遵守

以下については、情報システムの運用、保守等を事業者に業務委託する場合に、必要に応じて、受託者が遵守すべき情報セキュリティ要件を特記事項としてまとめるとともに、各規定の解説を記載したものです。

本実施手順に定められた全部又は一部を受託者に遵守させる必要がある場合は、下記の契約書記載例のように、契約書に受託者は本特記事項を遵守しなければならない旨を記載するものとします。

また、規定中、「甲」は発注者（村）を、「乙」は受託者（委託事業者）をいいます。

【契約書記載例】

（情報セキュリティの確保）
第〇条　乙は、本委託業務を履行する場合における情報セキュリティの確保については、別記「情報セキュリティ特記事項」を遵守しなければならない。

以下、特記事項を順に解説します。

1　委託先の責任者、作業者、作業場所の特定

(1) 責任体制の整備

第１　乙は、甲が引き渡す情報資産の安全管理について、内部における責任体制を構築し、その体制を維持しなければならない。

委託業者の管理体制や責任者を明確にすることで、委託先の従業員自身にとって、誰に指揮監督する責任があるのかが確認され、情報資産保護の実効性を確保します。

(2) 作業責任者等の届出

第２　乙は、情報資産の取扱いに係る作業責任者及び作業従事者を定め、書面により甲に報告しなければならない。
２　乙は、情報資産の取扱いに係る作業責任者及び作業従事者を変更する場合の手続を定めなければならない。
３　乙は、作業責任者又は作業従事者を変更する場合は、事前に書面により甲に報告しなければならない。
４　作業責任者は、本特記事項に定める事項を適切に実施するよう作業従事者を監督しなければならない。
５　作業従事者は、作業責任者の指示に従い、本特記事項に定める事項を遵守しなければならない。

①　作業責任者及び作業従事者を把握することで、委託事業者の従業員に対する抑制力が働きます。
②　作業責任者及び作業従事者が異動や退職等の理由で変更になった場合に、それまでの実施事項や遵守すべき事項等を適切に後任者へ伝達させたり、変更内容を報告させたりする手続を定めさせることにより、変更の事実を村が承知していなかったということがないようにします。
③　委託事業者側の都合で、責任者としての能力を有しない者が後任となることや、情報資産保護に必要な知識・責任感を有しない従事者が作業に就くことを防ぎ、情報資産保護の実効性を確保します。
④　作業責任者に対して、作業従事者の行動を監督する責務があることを明確にすることで、委託事業者内部の管理体制が弛緩しないようにします。
⑤　作業従事者が作業責任者の指揮に沿った行動をとらなければならないことを明確にし、委託事業者における情報資産保護に関する統一的な体制を確保します。

(3) 作業場所の特定

第３　乙は、情報資産を取り扱う場所（以下「作業場所」という。）を定め、業務の着手前に書面により甲に報告しなければならない。また、作業場所を変更する場合も同様とする。
２　乙は、甲の事務所内に作業場所を設置する場合は、作業責任者及び作業従事者に対して、所属名等が分かるように身分証明書等を常時携帯させなければならない。

① 作業場所の特定及び当該作業場所の把握により、委託業務の特性、情報資産の件数や内容に応じた作業環境上のリスクを村が認識します。また、作業環境上のリスクを認識することで、委託事業者がとるべき保護措置が明確になります。さらに、委託事業者の都合により、当初報告していた作業場所とは異なる作業環境において作業が行われることを防ぎ、実施する保護措置を有効に機能させます。

② 作業従事者が誰かを認識できるようにし、作業従事者が事務所内の届け出た場所以外で作業を行うことを抑制します。

(4) 派遣労働者等の利用時の措置

第４　乙は、本委託業務を派遣労働者、契約社員その他の正社員以外の労働者に行わせる場合は、正社員以外の労働者に本特記事項に基づく一切の義務を遵守させなければならない。

２　乙は、甲に対して、正社員以外の労働者の全ての行為及びその結果について責任を負うものとする。

① 委託事業者が、直接的な雇用関係にない派遣社員やアルバイト等を作業従事者とする場合に、それらの作業従事者に対しても本特記事項に基づく一切の義務を遵守させる責務があることを明確にすることで、委託事業者内部の管理体制を確立させます。

② 委託事業者が、派遣社員やアルバイト等を作業従事者とする場合、その管理責任は委託事業者にあることを明確にし、管理を徹底するよう委託事業者に動機付けをします。

２　従業員に対する教育の実施

第５　乙は、情報資産の保護、情報セキュリティに対する意識の向上、本特記事項における作業従事者が遵守すべき事項その他本委託業務の適切な履行に必要な教育及び研修を、作業従事者全員に対して実施しなければならない。

２　乙は、前項の教育及び研修を実施するに当たり、実施計画を策定し、実施体制を確立しなければならない。

① 実際の業務を実施するのは作業従事者であり、その意識が低いまま（例えば、情報資産保護よりも業務を優先するなど）では、情報資産の持ち出し等が起こり得るため、教育を実施し、情報セキュリティに対する意識の向上を図ります。

② 情報資産の保護に係る具体的な教育及び研修計画の策定を義務付けることにより、研修の確実な実施を担保します。

3 業務上知り得た情報の守秘義務

第６ 乙は、本委託業務の履行により直接又は間接に知り得た情報を第三者に漏らしてはならない。また、契約期間満了後又は契約解除後も同様とする。
２ 乙は、本委託業務に携わる作業責任者及び作業従事者に対して、秘密保持に関する誓約書を提出させなければならない。

① 委託事業者の機密保持責任・守秘義務を明確にするとともに、守秘義務の期間を契約期間以外にも及ぶことを明確に示すことで、守秘義務の期間を契約期間に限るものと解釈されないようにします。
② 作業従事者に誓約書を提出させることで、情報資産保護のための意識向上とけん制を行えるようにします。

4 再委託に関する制限事項の遵守

第７ 乙は、本委託業務を第三者へ委託（以下「再委託」という。）してはならない。ただし、本委託業務の一部をやむを得ず再委託する必要がある場合は、再委託先の名称、再委託する理由、再委託して処理する内容、再委託先において取り扱う情報、再委託先における安全性及び信頼性を確保する対策並びに再委託先に対する管理及び監督の方法を明確にした上で、業務の着手前に、書面により再委託する旨を甲に申請し、その承認を得なければならない。
２ 前項ただし書により、本委託業務の一部をやむを得ず再委託する必要がある場合、乙は、再委託先に本特記事項に基づく一切の義務を遵守させるとともに、甲に対して、再委託先の全ての行為及びその結果について責任を負うものとする。
３ 乙は、再委託先との契約において、再委託先に対する管理及び監督の手続及び方法について具体的に規定しなければならない。
４ 乙は、再委託先に対して本委託業務を委託した場合は、その履行状況を管理・監督するとともに、甲の求めに応じて、管理・監督の状況を甲に対して適宜報告しなければならない。

① いわゆる丸投げを禁止し、事業者としての責任ある対応を求めます。また、業務の一部をやむを得ず再委託する場合に、村が委託事業者の責任や再委託先の安全管理の状況等を必要に応じて確認できるようにします。
なお、再委託先より先の委託事業者に対しては、情報資産保護のためのコントロールを村が直接行うことが難しいため、基本的には再々委託を認めないことが望ましいです。

② 再委託に関する委託事業者の責任を明確にすることで、安易な再委託を抑制すること、再委託をする場合でも、再委託事業者の選定に関して適切な管理能力のある事業者とするよう方向付けます。

③ 特にIT関係の開発・運用等では再委託が一般的であり、委託先に対して明確に再委託先の管理責任があることと、具体的な管理・監督の方法等を規定させることで、再委託に関する情報資産保護の実効性の確保を図ります。

④ 再委託事業者の情報資産の取扱いを適正に行うことについて、委託事業者に管理・監督する義務があることを明確にし、発注者である村に報告をさせることで、その履行を確実にさせます。

5 情報資産の管理

(1) 情報資産の管理

第８ 乙は、本委託業務において利用する情報資産を保持している間は、次の各号の定めるところにより、情報資産の管理を行わなければならない。
２ 施錠が可能な保管庫又は施錠若しくは入退室管理の可能な保管室で厳重に情報資産を保管すること。
３ 甲が指定した場所へ持ち出す場合を除き、情報資産を定められた場所から持ち出さないこと。
４ 情報資産を電子データで持ち出す場合は、電子データの暗号化処理又はこれと同等以上の保護措置を施すこと。
５ 事前に甲の承認を受けて、業務を行う場所で、かつ業務に必要最小限の範囲で行う場合を除き、情報資産を複製又は複写しないこと。
６ 情報資産を移送する場合は、移送時の体制を明確にすること。
７ 情報資産を電子データで保管する場合は、当該データが記録された媒体及びそのバックアップの保管状況並びに記録されたデータの正確性について、定期的に点検すること。

8　情報資産を管理するための台帳を整備し、情報資産の利用者、保管場所その他の情報資産の取扱状況を当該台帳に記録すること。
9　情報資産の紛失、漏えい、改ざん、破損その他の事故（以下「情報資産の漏えい等の事故」という。）を防ぎ、機密性、完全性及び可用性の維持に責任を負うこと。
10　作業場所に、私物のパソコン及び電磁的記録媒体、その他の私物を持ち込んで、情報資産を取り扱う作業を行わせないこと。
11　情報資産を利用する作業を行うパソコンに、情報資産の漏えいにつながると考えられる業務に関係のないアプリケーションをインストールしないこと。

① 情報資産に対して実施する必要のある管理方策を明確にすることで、情報資産の漏えいリスクを低減させます。
なお、各号は情報の秘匿性等その内容に応じて、業務ごとに選択して利用します。
② 情報資産の保管について施錠管理を求めることで、不注意による紛失や不適切な持ち出しを防ぎます。
③ 情報資産の取扱場所や保管場所を定めた上で、村の許可なく定められた場所以外での情報資産の利用を防ぎます。
④ 情報資産が流出した場合でも、必要な保護措置を講じることで、第三者に読み取られないようにします。
⑤ 特に電子データの場合は、容易に複製等ができるため、厳格な取扱いを求めることを事前に伝えることで、安易な複製等を行わないようにさせます。
⑥ 情報資産の移送の途中は、必要な安全性が確保できないことが多いため、安全性の確保のための体制や確実な受渡し方法等を検討し、実施させます。
⑦ バックアップされたデータが不正に持ち出されたり、誤って廃棄・消去されないよう保管状況の定期的な確認を求めます。
⑧ 取り扱う情報資産等を台帳によって目視確認ができるようにすることで、他の発注者等の情報と明確に判別可能とし、情報の取り違い等の発生を防止します。
また、作業従事者が自ら記録することにより、情報資産の持ち出し等の抑制を図ります。
⑨ 取り扱う情報資産について、機密性、完全性、可用性を確保する義務があることを明確にし、必要な対策を講じるよう規定します。
⑩ 私物のパソコンや電磁的記録媒体の持込みを防止することで、取り扱う情報資産が外部に持ち出されるのを防ぎます。
⑪ 情報資産を利用するパソコンにWinny、Shareといった情報資産の漏えい等の事故を発生させやすい、業務上関係のないファイル交換ソフト（P2Pソフト）がインストールされることを防ぎます。

(2) 目的外利用及び第三者への提供の禁止

第９　乙は、本委託業務において利用する情報資産について、本委託業務以外の目的で利用してはならない。また、甲に無断で第三者へ提供してはならない。

委託事業者に目的外利用を禁止し、他業務への流用や第三者への提供を行えないようにすることで、村として業務を委託するという仕組みの信頼性を確保します。

(3) 情報資産の受渡し

第 10　乙は、甲乙間の情報資産の受渡しに関しては、甲が指定した手段、日時及び場所で行った上で、甲に情報資産の預かり証を提出しなければならない。

取り扱う情報資産の重要性や件数等に応じて、安全性が確保できる場所や方法で情報資産の受渡しを行うことにより、不注意による紛失や第三者による盗難といった危険を防止します。

(4) 情報資産の返却及び廃棄

第 11　乙は、本委託業務の終了時に、本委託業務において利用する情報資産について、甲の指定した方法により、返却又は廃棄を実施しなければならない。 ２　乙は、本委託業務において利用する情報資産を消去又は廃棄する場合は、事前に消去又は廃棄すべき情報資産の項目、媒体名、数量、消去又は廃棄の方法及び処理予定日を書面により甲に申請し、その承認を得なければならない。 ３　乙は、情報資産の消去又は廃棄に際し、甲から立会いを求められた場合は、これに応じなければならない。 ４　乙は、本委託業務において利用する情報資産を廃棄する場合は、当該情報が記録された電磁的記録媒体の物理的な破壊その他当該情報資産を判読不可能とするのに必要な措置を講じなければならない。 ５　乙は、情報資産の消去又は廃棄を行った後、消去又は廃棄を行った日時、担当者名及び消去又は廃棄の内容を記録し、書面により甲に報告しなければならない。

①　情報資産の返却又は廃棄に関する委託事業者の義務を明記することで、業務終了後の情報資産の不正な流用や放置といった事態が発生することを防止します。

②　委託事業者が情報資産を消去又は廃棄する場合に、村側にその承認を求める仕

組みを講じることにより、確実に消去等の処分がなされることを記録上担保します。

③　委託事業者が情報資産を消去又は廃棄するときに、村側の立会いを求めることで、確実に情報資産の消去又は廃棄がなされることを担保します。

④　情報資産を委託事業者が廃棄する場合は、物理的に再利用できないような措置を義務付けることで、第三者により閲覧、利用される危険を防止します。

⑤　情報資産を委託事業者が消去又は廃棄する場合は、消去又は廃棄した日時、その担当者及び処理内容を記録として残すことを明記することにより、正しく消去又は廃棄されていることを保証させます。

6　情報資産の取扱状況に関する定期報告及び緊急時報告義務

第 12　乙は、甲から、情報資産の取扱状況について報告を求められた場合は、直ちに報告しなければならない。

2　乙は、情報資産の取扱状況に関する定期報告及び緊急時報告の手順を定めなければならない。

①　委託事業者に情報資産の取扱いに関する状況報告を義務付けることで、委託業務において利用されている情報資産の管理状況を村が把握できるようにします。

②　委託事業者の村に対する報告手続を事前に定めることを義務付けることにより、迅速な報告の聴取や報告自体の手順の適正化を確保します。

7　監査及び検査

第 13　甲は、本委託業務に係る情報資産の取扱いについて、本特記事項の規定に基づき、必要な措置が講じられているかどうかを検証及び確認するため、乙及び再委託先に対して、監査及び検査を行うことができる。

2　甲は、前項の目的を達するため、乙に対して必要な情報を求め、又は本委託業務の処理に関して必要な指示をすることができる。

①　委託事業者の履行状況を発注者として監査及び検査することで、実際に本特記事項に記載された情報資産保護措置が実施されているかどうかを検証します。
また、監査及び検査の実施により、改善すべき事項を早期に発見・改善し、情報資産の漏えい等の事故へ発展することを防止します。

② 監査及び検査について委託事業者の協力義務を明確にし、必要な指示に従うよう明記することで、業務多忙を理由に監査や検査を遅延したり、必要な情報や協力が得られなくなることを防ぎます。

8 事故時の対応

第 14 乙は、本委託業務に関し、情報資産の漏えい等の事故が発生した場合は、その事故の発生に係る帰責の有無にかかわらず、直ちに甲に対して、当該事故に関する情報資産の内容、件数、事故の発生場所、発生状況を書面により報告し、甲の指示に従わなければならない。

2 乙は、情報資産の漏えい等の事故が発生した場合に備え、甲その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止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なければならない。

3 甲は、本委託業務に関し情報資産の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

① 事故を隠ぺいさせず、二次被害等が発生しないよう早期に対応できる体制を整備します。

② どれほど注意をしても事故が発生する確率をゼロにすることはできないことから、事故が起こった場合を想定し、事前に緊急時の対応計画を定め、発生する被害を最小限とする措置を講じます。

③ 事故の性質、その内容に応じて、二次被害の防止や住民等に対する説明責任を果たす意味から、事故に関する情報の公表について明記します。

9 特記事項が遵守されなかった場合

(1) 契約解除

第 15 甲は、乙が本特記事項に定める義務を履行しない場合は、本特記事項に関連する委託業務の全部又は一部を解除することができる。

2 乙は、前項の規定による契約の解除により損害を受けた場合においても、甲に対して、その損害の賠償を請求できないものとする。

① 特記事項の内容を遵守しない場合のペナルティを明記することで、情報資産保

護対策の実効性を確保します。

② 委託事業者側の事由による契約解除に起因する損害について、委託事業者からの賠償請求を防止することで、契約解除権行使の実効性を確保します。

(2) 損害賠償

> 第 16 乙の故意又は過失を問わず、乙が本特記事項の内容に違反し、又は怠ったことにより、甲に対する損害を発生させた場合は、乙は、甲に対して、その損害を賠償しなければならない。

賠償請求権を明記することにより、委託事業者に対する契約の内容の遵守を間接的に強制します。

なお、条文上は損害賠償の上限について明記していませんが、必要に応じて、損害賠償の予定額又は違約金の設定に関して明記することも考えられます。

別記

情報セキュリティ特記事項

（責任体制の整備）

第１　乙は、甲が引き渡す情報資産の安全管理について、内部における責任体制を構築し、その体制を維持しなければならない。

（作業責任者等の届出）

第２　乙は、情報資産の取扱いに係る作業責任者及び作業従事者を定め、書面により甲に報告しなければならない。

２　乙は、情報資産の取扱いに係る作業責任者及び作業従事者を変更する場合の手続を定めなければならない。

３　乙は、作業責任者又は作業従事者を変更する場合は、事前に書面により甲に報告しなければならない。

４　作業責任者は、本特記事項に定める事項を適切に実施するよう作業従事者を監督しなければならない。

５　作業従事者は、作業責任者の指示に従い、本特記事項に定める事項を遵守しなければならない。

（作業場所の特定）

第３　乙は、情報資産を取り扱う場所（以下「作業場所」という。）を定め、業務の着手前に書面により甲に報告しなければならない。また、作業場所を変更する場合も同様とする。

２　乙は、甲の事務所内に作業場所を設置する場合は、作業責任者及び作業従事者に対して、所属名等が分かるように身分証明書等を常時携帯させなければならない。

（派遣労働者等の利用時の措置）

第４　乙は、本委託業務を派遣労働者、契約社員その他の正社員以外の労働者に行わせる場合は、正社員以外の労働者に本特記事項に基づく一切の義務を遵守させなければならない。

２　乙は、甲に対して、正社員以外の労働者の全ての行為及びその結果について責任を負うものとする。

（教育の実施）

第５　乙は、情報資産の保護、情報セキュリティに対する意識の向上、本特記事項における作業従事者が遵守すべき事項その他本委託業務の適切な履行に必要な教育及び研修を、作業従事者全員に対して実施しなければならない。

２　乙は、前項の教育及び研修を実施するに当たり、実施計画を策定し、実施体制を確立しなければならない。

（守秘義務）

第６　乙は、本委託業務の履行により直接又は間接に知り得た情報を第三者に漏らしてはならない。また、契約期間満了後又は契約解除後も同様とする。

２　乙は、本委託業務に携わる作業責任者及び作業従事者に対して、秘密保持に関する誓約書を提出させなければならない。

（再委託）

第７　乙は、本委託業務を第三者へ委託（以下「再委託」という。）してはならない。ただし、本委託業務の一部をやむを得ず再委託する必要がある場合は、再委託先の名称、再委託する理由、再委託して処理する内容、再委託先において取り扱う情報、再委託先における安全性及び信頼性を確保する対策並びに再委託先に対する管理及び監督の方法を明確にした上で、業務の着手前に、書面により再委託する旨を甲に申請し、その承認を得なければならない。

２　前項ただし書により、本委託業務の一部をやむを得ず再委託する必要がある場合、乙は、再委託先に本特記事項に基づく一切の義務を遵守させるとともに、甲に対して、再委託先の全ての行為及びその結果について責任を負うものとする。

３　乙は、再委託先との契約において、再委託先に対する管理及び監督の手続及び方法について具体的に規定しなければならない。

４　乙は、再委託先に対して本委託業務を委託した場合は、その履行状況を管理・監督するとともに、甲の求めに応じて、管理・監督の状況を甲に対して適宜報告しなければならない。

（情報資産の管理）

第８　乙は、本委託業務において利用する情報資産を保持している間は、次の各号の定めるところにより、情報資産の管理を行わなければならない。

２　施錠が可能な保管庫又は施錠若しくは入退室管理の可能な保管室で厳重に情報資産を保管すること。

３　甲が指定した場所へ持ち出す場合を除き、情報資産を定められた場所から持ち出さないこと。

４　情報資産を電子データで持ち出す場合は、電子データの暗号化処理又はこれと同等以上の保護措置を施すこと。

５　事前に甲の承認を受けて、業務を行う場所で、かつ業務に必要最小限の範囲で行う場合を除き、情報資産を複製又は複写しないこと。

６　情報資産を移送する場合は、移送時の体制を明確にすること。

７　情報資産を電子データで保管する場合は、当該データが記録された媒体及びそのバックアップの保管状況並びに記録されたデータの正確性について、定期的に点検すること。

８　情報資産を管理するための台帳を整備し、情報資産の利用者、保管場所その他の情報資産の取扱状況を当該台帳に記録すること。

９　情報資産の紛失、漏えい、改ざん、破損その他の事故（以下「情報資産の漏えい等の事故」という。）を防ぎ、機密性、完全性及び可用性の維持に責任を負うこと。

10　作業場所に、私物のパソコン及び電磁的記録媒体、その他の私物を持ち込んで、情報資産を取り扱う作業を行わせないこと。

11　情報資産を利用する作業を行うパソコンに、情報資産の漏えいにつながると考えられる業務に関係のないアプリケーションをインストールしないこと。

（目的外利用及び第三者への提供の禁止）

第９　乙は、本委託業務において利用する情報資産について、本委託業務以外の目的で利用してはな

らない。また、甲に無断で第三者へ提供してはならない。

（情報資産の受渡し）

第 10　乙は、甲乙間の情報資産の受渡しに関しては、甲が指定した手段、日時及び場所で行った上で、甲に情報資産の預かり証を提出しなければならない。

（情報資産の返却及び廃棄）

第 11　乙は、本委託業務の終了時に、本委託業務において利用する情報資産について、甲の指定した方法により、返却又は廃棄を実施しなければならない。

2　乙は、本委託業務において利用する情報資産を消去又は廃棄する場合は、事前に消去又は廃棄すべき情報資産の項目、媒体名、数量、消去又は廃棄の方法及び処理予定日を書面により甲に申請し、その承認を得なければならない。

3　乙は、情報資産の消去又は廃棄に際し、甲から立会いを求められた場合は、これに応じなければならない。

4　乙は、本委託業務において利用する情報資産を廃棄する場合は、当該情報が記録された電磁的記録媒体の物理的な破壊その他当該情報資産を判読不可能とするのに必要な措置を講じなければならない。

5　乙は、情報資産の消去又は廃棄を行った後、消去又は廃棄を行った日時、担当者名及び消去又は廃棄の内容を記録し、書面により甲に報告しなければならない、

（定期報告及び緊急時報告）

第 12　乙は、甲から、情報資産の取扱状況について報告を求められた場合は、直ちに報告しなければならない。

2　乙は、情報資産の取扱状況に関する定期報告及び緊急時報告の手順を定めなければならない。

（監査及び検査）

第 13　甲は、本委託業務に係る情報資産の取扱いについて、本特記事項の規定に基づき、必要な措置が講じられているかどうかを検証及び確認するため、乙及び再委託先に対して、監査及び検査を行うことができる。

2　甲は、前項の目的を達するため、乙に対して必要な情報を求め、又は本委託業務の処理に関して必要な指示をすることができる。

（事故時の対応）

第 14　乙は、本委託業務に関し、情報資産の漏えい等の事故が発生した場合は、その事故の発生に係る帰責の有無にかかわらず、直ちに甲に対して、当該事故に関する情報資産の内容、件数、事故の発生場所、発生状況を書面により報告し、甲の指示に従わなければならない。

2　乙は、情報資産の漏えい等の事故が発生した場合に備え、甲その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止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なければならない。

3　甲は、本委託業務に関し情報資産の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

（契約解除）

第15　甲は、乙が本特記事項に定める義務を履行しない場合は、本特記事項に関連する委託業務の全部又は一部を解除することができる。

２　乙は、前項の規定による契約の解除により損害を受けた場合においても、甲に対して、その損害の賠償を請求できないものとする。

（損害賠償）

第16　乙の故意又は過失を問わず、乙が本特記事項の内容に違反し、又は怠ったことにより、甲に対する損害を発生させた場合は、乙は、甲に対して、その損害を賠償しなければならない。

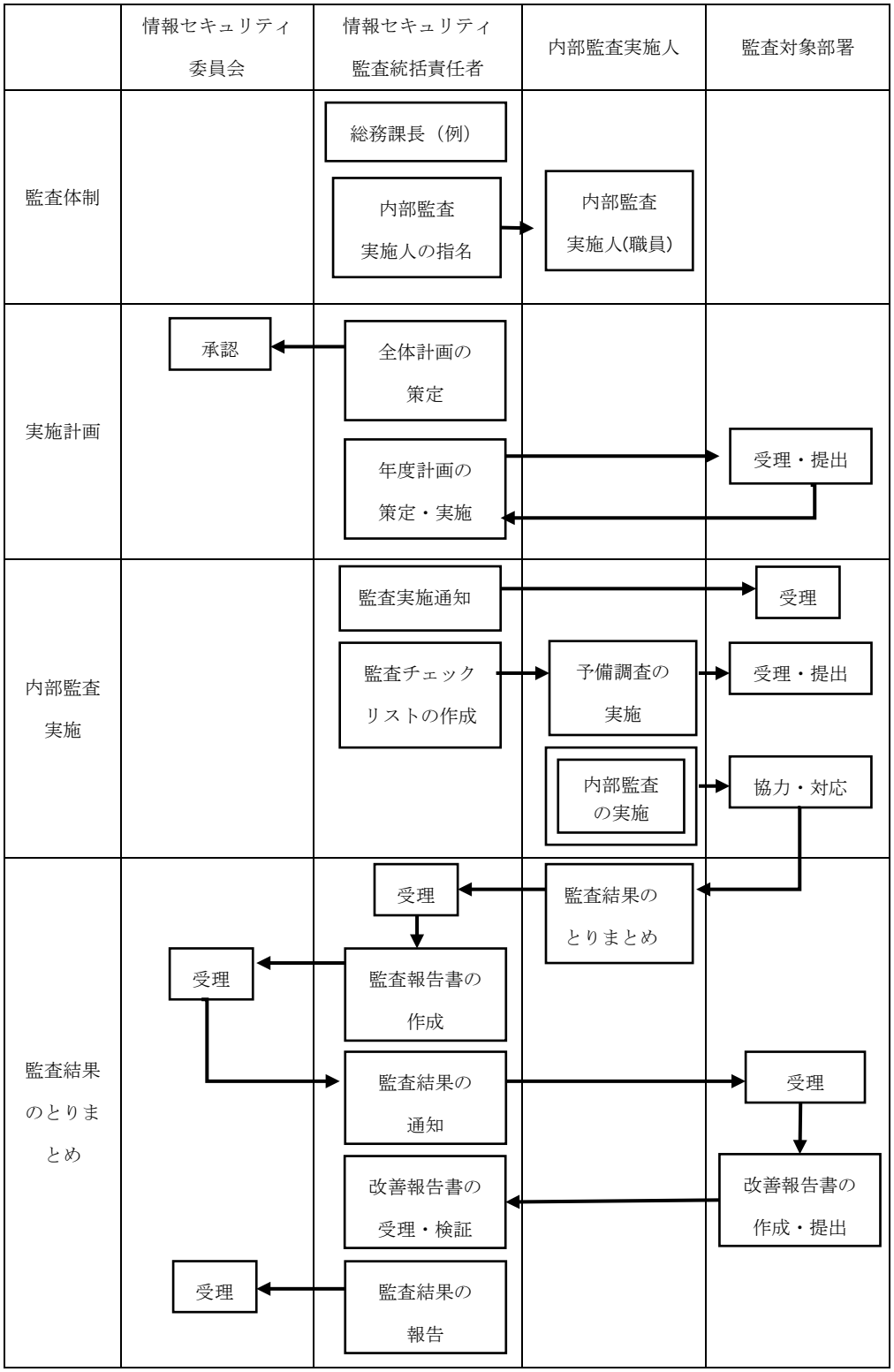
注１　委託業務の内容により、必要な事項を追加し、及び不要な事項を削除するものとする。

２　契約に違反した場合における契約解除、それに伴う損害賠償については、通常、本契約に盛り込まれるものであるため、本契約において契約事項として措置した場合には、本特記事項からは削除するものとする。

5　情報セキュリティ内部監査実施手順

1　情報セキュリティ内部監査の流れ

情報セキュリティ内部監査の全体の流れは、次のとおりです。



2　監査体制の整備

(1) 情報セキュリティ監査統括責任者の指名

CISOは情報セキュリティ内部監査を実施するに当たり、情報セキュリティ監査に関する責任と権限を有する情報セキュリティ監査統括責任者を指名します。

(2) 内部監査実施人の任命

情報セキュリティ監査統括責任者は、内部監査実施人（以下「監査人」といいます。）を任命し、監査体制を整備します。

(3) 実施体制

監査は、原則として監査人２人を１チームとして実施します。

3　実施計画の策定

(1) 全体計画の策定

情報セキュリティ監査統括責任者は、情報セキュリティ内部監査に関する中期的な基本方針として「全体計画」を策定しなければなりません。

(2) 年度計画の策定、通知

情報セキュリティ監査統括責任者は、全体計画に基づき、当該年度の監査目的、監査対象部署、監査日程等を定めた「年度計画」を策定し、情報セキュリティ委員会に諮り、承認を得た後、全部署の情報セキュリティ責任者へ周知します。

4　内部監査の実施

(1) 監査実施通知

情報セキュリティ監査統括責任者は、年度計画に基づき、当該年度の監査対象部署に対して、内部監査の実施を通知し、効率的に監査を実施するため、担当者の選出、監査資料の準備等の必要な協力を求めます。

(2) 監査チェックリストの作成

情報セキュリティ監査統括責任者は、内部監査の実施に当たり、監査を効率的かつ効果的に実施するため、確認すべき具体的な項目を事前に選定し、監査チェックリストを作成します。

(3) 予備調査の実施

監査人は、監査チェックリストを予備調査票とし、監査対象部署に対して監査実施前に送付し、事前に自己点検により確認してもらい、必要に応じて事前に提出を求めます。

(4) 内部監査の実施

内部監査は、次の流れで実施します。

①　オープニングミーティング

監査対象部署に対し、監査の目的や内容の確認、タイムスケジュール、評価方法等について説明します。

②　質問・閲覧・再実施

監査対象部署が予備調査アンケート等により実施した自己点検結果に基づき、質問、閲覧又は再実施を行い確認します。

確認は以下のように行います。

・対応策に対象とする情報資産、主体又は適用範囲などが明確に定義されているか
・対応策を実施するための手順が明確にルール化されているか
・対応策と手順が実装され運用されているか
・対応策の実施結果が記録され、完全性を確保して適正に保存されているか

③　現場観察

事務室やサーバ室等を確認します。

④　監査人ミーティング

監査結果について、監査人間で整理します。

⑤　クロージングミーティング

監査対象部署に対し、監査結果の確認、今後の予定等について説明します。

5　監査結果のとりまとめ

(1) 監査結果のとりまとめ

監査人は、内部監査の終了後、監査対象部署ごとに監査結果をとりまとめ、情報セキュリティ監査統括責任者に提出します。

(2) 監査結果報告書の作成

情報セキュリティ監査統括責任者は、監査人から提出された監査対象部署ごとの監査結果に基づき、監査結果報告書を作成します。

(3) 監査結果の通知

情報セキュリティ監査統括責任者は、監査対象部署の情報セキュリティ責任者に対し、監査結果を通知します。また、要改善事項がある場合は、期限を付して、これに対する改善処置を実施するよう通知するとともに、改善報告書の提出を求めます。

(4) 改善報告書の提出

監査対象部署の情報セキュリティ責任者は、監査結果の通知に要改善事項がある場合は、改善報告書を作成し、期限までに情報セキュリティ監査統括責任者へ提出します。

(5) 改善報告書の検証

情報セキュリティ監査統括責任者は、提出された改善報告書を検証し、不十分と認められるときは、監査対象部署の情報セキュリティ責任者に対し、改善報告書の修正・再提出を求めます。

(6) 監査結果の報告

情報セキュリティ監査統括責任者は、各情報セキュリティ責任者から提出された改善報告書をとりまとめ、是正状況を含めた最終結果を情報セキュリティ委員会へ報告するとともに、必要に応じて全情報セキュリティ責任者へ周知します。