立山町情報セキュリティポリシー

平成 30 年 4 月 1 日

目次

はじめに　情報セキュリティポリシーの構成

情報セキュリティポリシーは、立山町が所掌する情報資産に関する業務に携わる全ての職員（他の団体からの出向職員、非常勤、臨時職員等を含む。以下同じ。）及び外部委託事業者に浸透、普及、定着させるものであり、普遍的な規範であることが要請される。一方で、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを、一定の普遍性を備えた部分（情報セキュリティ基本方針）と情報資産を取り巻く状況の変化に適切に対応する部分（情報セキュリティ対策基準）に分けて策定する

また、情報セキュリティポリシーに基づき、ネットワーク及び情報システムの情報セキュリティ対策の手順である実施手順を策定する。

情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、立山町が所掌する情報資産に関する情報セキュリティ対策について、総合的かつ体系的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

文　書　名		内　　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		情報セキュリティ対策基準に基づき、ネットワーク及び情報システムの情報セキュリティ対策を実施するための具体的な手順。

第１章　情報セキュリティ基本方針

１　目的

立山町の各情報システムが取り扱う情報には、町民の個人情報のみならず行政運営上の重要な情報など、漏洩や改ざん等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産、情報資産を取り扱うネットワーク及び情報システムを漏洩や改ざん等の様々な脅威から防御することは、町民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠であり、立山町に対する町民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるIT革命の進展により、電子申請の開始など電子自治体の構築が現実のものとなっている。立山町が電子自治体を構築するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

このため、立山町の情報セキュリティ対策を整備した、情報セキュリティポリシーを定める。

２　定義

（1）ネットワーク

コンピュータを相互に接続するための通信網、通信機器及び記録媒体で構成された、情報伝達を行う仕組みをいう。

（2）情報システム

コンピュータ及び記録媒体で構成された、業務処理を行う仕組みをいう。

（3）情報資産

ネットワーク及び情報システム上で管理される電磁的に記録された情報をいう。

（4）情報セキュリティ

情報資産の機密性、完全性、可用性を維持することをいう。

（5）情報セキュリティ対策

情報セキュリティの阻害要因から情報資産を守るための手段をいう。

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利用等の規定違反、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、水害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、通信、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）行政組織の範囲

立山町課設置条例（平成 16 年立山町条例第 26 号）第 1 条に掲げる課（出先機関を含む。）、会計課、教育委員会、消防本部及び消防署、議会事務局、監査委員事務局、農業委員会事務局、選挙管理委員会事務局、固定資産評価審査委員会及び専用回線で接続するその他の施設とする。とする。ただし、各教育機関（事務室及び職員室を除く。）は対象外とする。

（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。

ア 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

イ 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。）

ウ 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　職員及び外部委託事業者の義務

立山町が所掌する情報資産に関する業務に携わる職員及び外部委託事業者

は、情報セキュリティの重要性について共通の認識を持つとともに情報セキュリティポリシーを遵守する義務を負う。

6　情報セキュリティ対策

上記３で示した脅威から情報資産を保護するために、物理的、人的、技術的及び運用の観点からセキュリティ対策を講じる。

（１）組織体制

町の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２）情報資産の分類と管理

町の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（３）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。

（４）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。

（５）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。

（６）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、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

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が遵守されていることを検証するため、定期的または必要に応じて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となった場合には、情報セキュリティポリシーの見直しを行う。

９　情報セキュリティ対策基準の策定

上記６、７及び８の情報セキュリティ対策を実施するために、遵守すべき行為及び判断等の基準を具体的に定める情報セキュリティ対策基準を策定する。

10　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を遵守して情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本町の行政運営に重大な支障を及ぼす恐れがあることから非公開とする。

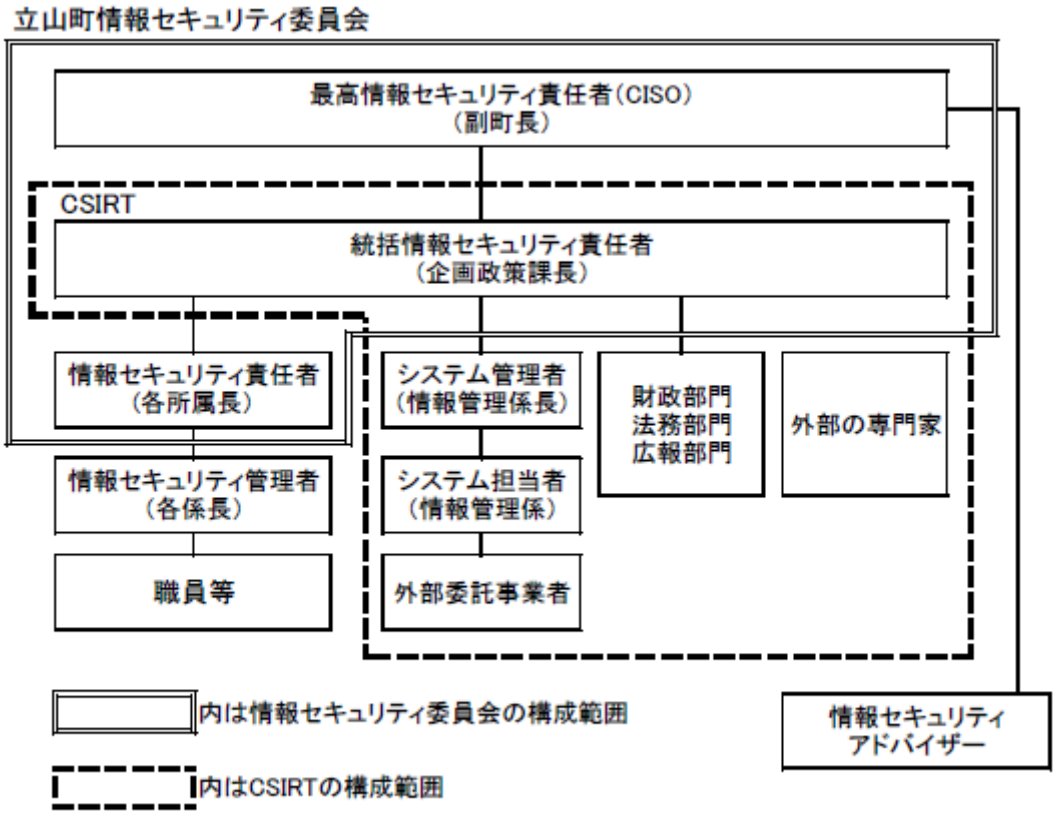
第２章　情報セキュリティ対策基準

１　目的

本対策基準は、情報セキュリティ基本方針（以下「基本方針」という。）に基づく情報セキュリティ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たものである。

２　情報セキュリティ管理体制

情報セキュリティの管理は、以下の組織体制で行う。



（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。）

①副町長を、CISO とする。CISO は、立山町における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最

終決定権限及び責任を有する。CISO は最高情報統括責任者を兼務する。

②CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置くことができる。

（2） 統括情報セキュリティ責任者

①企画政策課長を、CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は CISO を補佐する。

②統括情報セキュリティ責任者は、立山町の全てのネットワーク及び情報システムの開発、設定変更、運用、見直し等を行う統括的な権限及び責任を有する。

③統括情報セキュリティ責任者は、立山町の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統括的な権限及び責任を有する。

④統括情報セキュリティ責任者は、情報セキュリティ責任者、システム管理者及びシステム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤統括情報セキュリティ責任者は、立山町の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

⑥統括情報セキュリティ責任者は、立山町の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ共通実施手順の維持・管理を行う権限及び責任を有する。

⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を行うため、CISO、情報セキュリティ責任者、システム管理者、システム担当者を網羅する緊急連絡網を整備しなければならない。

⑧統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、復旧のための対策を講じなければならない。

（3） 情報セキュリティ責任者

①各部署の所属長を、情報セキュリティ責任者とする。

②情報セキュリティ責任者は、所管部署の情報資産の管理及び情報セキュリティ対策に関する統括的な権限及び責任を有する。

③情報セキュリティ責任者は、その所管部署において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④情報セキュリティ責任者は、所管部署において、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、それらに対応するとともに、必要に応じて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。

⑤情報セキュリティ責任者は、所管する情報システムの開発、設定変更、運用、見直し等を行う権限及び責任を有する。

⑥情報セキュリティ責任者は、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。

（4） 情報セキュリティ管理者

①各係の係長を、情報セキュリティ管理者とする。

②情報セキュリティ管理者は、所管する係の情報セキュリティ対策に関する権限及び責任を有する。

③情報セキュリティ管理者は、所管する係の職員等及び外部委託事業者に当町情報セキュリティポリシーを理解させ、遵守状況を管理する。

④情報セキュリティ管理者は、情報セキュリティ責任者の指示に従い、所管する係における情報資産の保護・管理を行う。

⑤情報セキュリティ管理者は、所管する係において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

（5） システム管理者

①情報管理係長をシステム管理者とする

②システム管理者は統括情報セキュリティ責任者の指示に従い情報システムにおける開発、設定の変更、運用、見直し等を実施する。

③システム管理者は、統括情報セキュリティ責任者の指示に従い、情報システムにおける情報セキュリティ対策を実施する。

④システム管理者は、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システム管理者は、情報システムを起因とする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、必要に応じて統括情報セキュリティ責任者へ報告を行い、指示を仰がなければならない。

（6） システム担当者

①情報管理係職員をシステム担当者とする

②システム担当者は、システム管理者の指示に従い、情報システムかかる作業を行う

③システム担当者は、情報セキュリティポリシーを管理・運用していくために必要な技術的な支援を行う。

（7）立山町情報セキュリティ委員会

①本町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、立山町情報セキュリティ委員会（以下「情報セキュリティ委員会」という。）において、情報システムの運営及び情報セキュリティに関する重要な事項を審議する。

②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ならびに情報セキュリティ責任者で構成する。

③情報セキュリティ委員会は、情報セキュリティに対する意識を醸成し保つために、全ての職員が情報セキュリティの重要性を認識し、対策規則を理解し、実践するために必要な教育・訓練等を計画的に実施するものとする。

（8）CSIRT（Computer Security Incident Response Team）

①CISO は、情報システム及び情報資産に関する事件及び事故に適切かつ迅

速に対応するため必要に応じ、CSIRT（情報セキュリティインシデントへ統一的に対応する窓口の機能を有する組織）を設置するものとする。

②CSIRT の体制については、別に定める。

3　情報資産の分類と管理

（1）情報資産の分類及び取扱制限

対象となる情報資産は、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。

機密性による情報の分類と取扱制限

分類	分類基準	取扱制限
機密性３	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報	・参照者の制限（機密性３は必須） ・電子データをサーバ内に保存する場合のアクセス制御（機密性３は必須） ・私物パソコンでの作業禁止（機密性３は必須） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の記録媒体等の持ち込み禁止 ・情報の送信、情報の運搬・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 ・送信に利用するネットワーク回線の制限 ・外部で情報処理を行う際の安全管理措置 ・記録媒体の施錠可能な場所への保
機密性２	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより住民の権利が侵害される、又は行政事務の遂行に支障を及ぼすおそれがある情報。	

		管 ・復元不可能な処理を施しての廃棄（必須）
機密性１	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又は機密性３の情報以外の情報	

完全性による情報の分類と取扱制限

分類	分類基準	取扱制限
完全性２	行政事務で取り扱う情報のうち、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	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・記録媒体の施錠可能な場所への保管
完全性１	完全性２の情報以外の情報	

可用性による情報の分類と取扱制限

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報のうち、滅失、紛失又は当該情報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	・バックアップ、指定する時間以内の復旧 ・記録媒体の施錠可能な場所への保管

	（軽微なものを除く。）を及ぼすおそれがある情報	
可用性１	可用性２の情報以外の情報	

（２）情報資産の管理方法

①管理責任

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

（イ）情報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）職員等は、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）職員等は、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、当該情報を廃棄しなければならない。

③情報資産の利用

（ア）職員等は、業務以外の目的に情報を利用してはならない。

（イ）職員等は、情報を利用する場合、情報の分類及び取扱制限に応じ、適切な取り扱いをしなければならない。

（ウ）職員等は、情報を利用する際、記録媒体に情報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情報資産の保管

（ア）職員等は、情報の分類及び取扱制限に従って、情報を適切に保管し

なければならない。

（イ）職員等は、情報を記録した記録媒体を長期保管する場合、書込禁止の措置を講じなければならない。

（ウ）職員等は、情報を利用する際、記録媒体に情報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。

（エ）職員等は、機密性２以上、完全性２又は可用性２の情報を記録した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。

⑤情報の送信

職員等は、電子メール等により機密性２以上の電子データを送信する場合、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。

⑥情報の運搬

（ア）車両等により機密性２以上の情報資産を運搬するものは、原則、鍵つ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）機密性２以上の情報資産を運搬するものは情報セキュリティ責任者に許可を得なければならない。

⑦ 情報の提供・公表

（ア）職員等は、機密性２以上の情報を外部に提供する場合、情報セキュリティ管理者に許可を得なければならない。

（イ）職員等は、機密性２以上の情報を外部に提供する場合、暗号化又はパスワードの設定を行わなければならない。

（ウ）職員等は、外部に情報を公表する場合、機密性１であることを確認のうえ、情報セキュリティ管理者に許可を得なければならない。

（エ）職員等は、住民に公表する情報について、完全性を確保しなければならない。

（オ）職員等は、電子データを提供又は公表する場合、プロパティ等に作成者名等が含まれていないことを確認しなければならない。

⑧ 情報の廃棄

（ア）職員等は、機密性２以上の情報の廃棄を行う場合、情報セキュリティ管理者の許可を得なければならない。

（イ）職員等は、不要となった機密性２以上の情報を廃棄する場合、記録媒体の初期化や文書の裁断等、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。

（ウ）職員等は、機密性３の情報の廃棄のために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。

４　物理的セキュリティ

（１）ネットワーク及び情報システム機器等

①機器の取付け

統括情報セキュリティ責任者及びシステム管理者は、サーバ等の機器を取付ける場合は、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、適切な固定器具を使用する等、必要な措置を講じなければならない。

②システムの冗長化

統括情報セキュリティ責任者及びシステム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、障害発生時のシステムの運用停止時間を最小減にしなければならない。

③機器の電源

統括情報セキュリティ責任者及びシステム管理者は、施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

④通信ケーブル等の配線

（ア）システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を利用する等必要な措置を講じなければならない。

（イ）システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルにつ

いて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

（ウ）システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

（エ）システム管理者は、システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

⑤機器の定期保守及び修理

（ア）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）システム管理者は、記録媒体を内蔵する機器を外部委託事業者に修理させる場合、守秘義務契約を締結する他、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

システム管理者は、庁外にサーバ等の機器及びその他の情報資産を設置する場合、システム所管部署の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の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

⑦機器の廃棄等

システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じねばならない。

（２）管理区域（電算室等）の管理

①管理区域の構造等

（ア）管理区域とは、電算室や記録媒体の保管庫をいう。

（イ）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、許可されていない立入りを防止しなければならない。

②管理区域の入退室管理等

（ア）システム管理者は、管理区域への入退室を許可された者のみに制限し、指紋認証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）職員及び外部委託事業者が管理区域に入る場合、身分証明書等を提示しなければならない。

（ウ）システム管理者は、管理区域について、システムに関連しないコンピュータ、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）システム管理者は、搬入する機器等が既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

（イ）システム管理者は電算室の機器等の搬入出について、職員を立ち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

①通信回線及び通信回線装置

システム管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

②ネットワーク

（ア）統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

（イ）統括情報セキュリティ責任者は、行政系のネットワークを集約するように努めなければならない。

（ウ）統括情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

（エ）統括情報セキュリティ責任者は、ネットワークに使用する回線につい

て、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

（オ）統括情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

5　人的セキュリティ

（1）職員等の遵守事項

①情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順に定められている事項を遵守しなければならない。また情報セキュリティ対策について、不明な点、遵守することが困難な点等については、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの利用及びインターネットへのアクセスを行ってはならない。

③パソコン等の持ち出し及び外部における情報処理の制限

（ア）CISO は情報資産を外部で処理する場合における措置等の必要な事項を定めなければならない。

（イ）職員等は、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、統括情報セキュリティ責任者の許可を得なければならない。

（ウ）職員等は、外部で情報処理業務を行う場合には、統括情報セキュリティ責任者の許可を得なければならない。

④私物パソコン等の持ち込み

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、統括情報セキュリティ責任者の許可を得て利用することができる。なお、機密性３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。

⑤パソコン等におけるセキュリティ設定変更の禁止

職員等は、パソコン等におけるソフトウェアに関するセキュリティ機能の設定を変更してはならない。ただし、業務上必要な場合は、電算システム管理者の許可を得なければならない。

⑥机上の端末等の管理

職員等は、パソコン等の端末や記録媒体、情報が印刷された文書等について、第三者に利用されること、及び情報を閲覧されることがないよう、離席時の端末のロックや記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

⑦退職時等の遵守事項

職員等及び外部委託事業者は、異動、退職又は契約終了等により業務を離れる場合、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

⑧非常勤及び臨時職員への対応

（ア）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への署名を求めるものとする。

（ウ）非常勤及び臨時職員は原則としてインターネットへの接続および電子メールの使用は行わせない。ただし、業務上必要な場合は統括情報セキュリティ責任者の許可を得てインターネットの接続及び電子メールの使用を行うことができるものとする。

⑨情報セキュリティポリシー及び実施手順の閲覧

統括情報セキュリティ責任者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるようにしなければならない。

（２） 外部委託に際しての管理

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

（３） 研修・訓練

①情報セキュリティに関する研修・訓練

統括情報セキュリティ責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

②研修計画の策定及び実施

（ア）統括情報セキュリティ責任者は、全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。

（イ）研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、システム管理者、システム担当者、新規採用職員、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を実施しなければならない。

③緊急時対応訓練

統括情報セキュリティ責任者は、緊急時対応を想定した訓練を適時実施しなければならない。訓練の計画に当たっては、各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適宜定めることとする。

④研修・訓練への参加

職員等は、定められた研修・訓練に参加しなければならない。

（４）情報セキュリティインシデントへの対応

①事故等の報告

（ア）職員等は、情報セキュリティに関する事故等を発見した場合、もしく

は住民等外部から報告を受けた場合、速やかに情報セキュリティ責任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責任者は、速やかに庁内 CSIRT に報告しなければならない。

（ウ）情報セキュリティ責任者は、情報セキュリティ事故等の報告を受けた場合、必要に応じて速やかに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及びシステム管理者に報告しなければならない。

②事故等への対応

情報セキュリティ事故等を引き起こした部署の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、必要に応じてシステム管理者及と連携し、これらの事故等に対応しなければならない。また、統括情報セキュリティ責任者より指示があった場合は、それに従う。

③情報セキュリティ事故の原因究明・記録、再発防止等

（ア）統括情報セキュリティ責任者は、情報セキュリティに関する事故を引き起こした部署の情報セキュリティ責任者、情報セキュリティ管理者、また必要に応じてシステム管理者と連携し、これらの事故等の原因を究明し、記録を保存しなければならない。また、事故原因の究明結果から、再発防止策を検討し、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。

（イ）最高情報セキュリティ責任者は、統括情報セキュリティ責任者から、再発防止策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。

（５） パスワード等の管理

① 端末ログイン用 IC カードの取扱い

（ア）職員等は、自己の管理する端末ログイン用 IC カード（以下「IC カード」という。）を、職員等間で共有してはならない。

（イ）職員等は、業務上必要のないときは、IC カード等をカードリーダから抜いておかなければならない。

（ウ）職員等は、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管理者及びシステム管理者に報告し、指示に従わなければならない。

（エ）システム管理者は、IC カードの紛失等の連絡が在り次第、当該 IC カードを利用したアクセス等を速やかに停止しなければならない。

（オ）システム管理者は、IC カードを廃棄する場合、粉砕するなど復元不可能な処理を行わなければならない。

②ID 及びパスワードの取り扱い

（ア）職員等は、自己が使用している ID 及びパスワードを、他者に使用させてはならない。

（イ）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。

（ウ）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。

（エ）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。

（オ）パスワードが流出した恐れがある場合、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。

（カ）パスワードは定期的に変更しなければならない。

（キ）職員間でパスワードを共有してはならない。

6　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

システム管理者は、町民の個人情報、人事記録等、特定の職員等しか取扱えないデータについて、当該職員以外の職員等が閲覧及び使用できないようにしなければならない。

②バックアップの実施

システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

③システム管理記録及び作業の確認

（ア）システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

（イ）統括情報セキュリティ責任者及び情報セキュリティ責任者は、所管するシステムにおいて、システム改修、変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

④情報システム仕様書等の管理

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等について、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、紛失したりすること等がないよう、適切に管理しなければならない。

⑤ログの取得等

（ア）統括情報セキュリティ責任者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

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

（ウ）統括情報セキュリティ責任者は、取得したログを定期的に点検し、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分析を実施しなければならない。

（エ）統括情報セキュリティ責任者は、重要なログ等を取得するサーバ及びネットワーク機器等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。

⑥障害記録

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、適切に保存しなければならない。

⑦ネットワークの接続制御、経路制御等

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

（イ）システム管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

⑧外部の者が利用できるシステムの分離等

統括情報セキュリティ責任者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと分離する等の措置を講じなければならない。

⑨外部ネットワークとの接続制限等

（ア）情報セキュリティ責任者は、所管するネットワークを外部ネットワークと接続しようとする場合には、統括情報セキュリティ責任者の許可を得なければならない。

（イ）システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、関連する全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

（ウ）情報セキュリティ責任者は、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）統括情報セキュリティ責任者は、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に、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

（オ）情報セキュリティ責任者は、所管するネットワークを外部ネットワークと接続した場合に、必要に応じて、当該外部ネットワークの管理責任者から、通信に係るログを提供させなければならない。

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

⑩複合機のセキュリティ管理

（ア）統括情報セキュリティ責任者は、複合機を調達する場合、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。

（イ）統括情報セキュリティ責任者は、複合機が備える機能について適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。

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

⑪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。

⑫無線 LAN 及びネットワークの盗聴対策

（ア）統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

（イ）統括情報セキュリティ責任者及び情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークを通信回線と接続する場合は、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。

⑬電子メールのセキュリティ管理

（ア）システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

（イ）システム管理者は、大量のスパムメール等の受信又は送信を検知した場合は、必要に応じてメールサーバの運用を停止しなければならない。

（ウ）統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

⑭電子メール等の利用制限

（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、情報セキュリティ責任者に報告しなければならない。

⑮電子署名・暗号化

職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、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。

⑯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、統括情報セキュリティ責任者及び情報セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する場合は、統括情報セキュリティ責任者は、ソフトウェアの追加導入記録簿を作成し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。

（エ）ソフトウェアの利用及び管理方法等に係る規定については、別に定める。

⑰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、統括情報セキュリティ責任者の許

可を得なければならない。

⑱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。

⑲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、統括情報セキュリティ責任者に通知し適切な措置を求めなければならない。

（２）ネットワーク及び情報システムを使用する際の制限等

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、必要なネットワーク及び情報システムのソフトウェアにパッチを当てる等、セキュリティ対策上必要な措置を講じなければならない。

システム管理者は、これらの情報を定期的に取りまとめ、関係課等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、情報セキュリティ委員会に報告しなければならない。

①ネットワーク

外部へのネットワーク接続は業務上必要な場合のみ行うものとし、できる限り接続ポイントを減らさなければならない。

ネットワークに使用する回線は、伝送途上において破壊、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が実施されたものでなければならない。

②情報システム

情報システムは、システム管理者から操作を認められた者以外の者が操作できないように、利用者 ID、パスワードの設定等の措置を講じなければならない。

主に外部の者が利用する情報システムにおいては、情報セキュリティ対策について特に暗号化送受信方式等による強固に対策をとらなければならない。

Web サイトにより情報を公開・提供する場合には、当該サイトに係るシステムについて、盗難、改ざん、踏み台、DoS 等に対する十分な防御措置を講じなければならない。

メールサーバにおいては、他のシステムに対する攻撃の踏み台とならないように適切な管理を実施しなければならない。

③ネットワーク及び情報システムの情報資産

アクセス記録等、ネットワーク及び情報システムの情報セキュリティの確保に必要な記録は、一定期間保存しなければならない。

ネットワーク構成図等、ネットワーク及び情報システムの仕組みを表す記録は、その仕組みが廃止されるまで適切に保管しなければならない。

④アクセス制御

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利用や他のネットワークとの接続などにあたって、アクセス制御を加えることができる。

⑤コンピュータウイルス対策

統括情報セキュリティ責任者は、コンピュータウイルスの脅威に対し十分な対策を講じなければならない。職員は、コンピュータウイルスの感染に対し、十分な注意を払わなければならない。

⑥不正アクセス対策

統括情報セキュリティ責任者は､不正アクセスの脅威に対し十分な対策を講じなければならない。

⑦セキュリティ情報の収集

統括情報セキュリティ責任者は､情報セキュリティに関する情報を収集し、必要なネットワーク及び情報システムのソフトウェアにパッチを当てる等、セキュリティ対策上必要な措置を講じなければならない。

統括情報セキュリティ責任者は、これらの情報を定期的に取りまとめ、関係課等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、情報セキュリティ委員会に報告しなければならない。

統括情報セキュリティ責任者は、緊急時対応計画に定める緊急に連絡す

べき情報を入手した場合は当該計画に定める情報連絡先に連絡しなければならない。

⑧情報システム開発、導入、保守等

情報管理者は、情報システムの開発、導入、保守等に当たって、対応の基準を明確にしなければならない。

7　運用

（1）ネットワーク及び情報システムの監視

統括情報セキュリティ責任者は、セキュリティに関する事案を検知するため、常にネットワーク及び情報システムの監視を行わなければならない。

統括情報セキュリティ責任者は、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必要に応じて分析、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

情報セキュリティ責任者は、所管する課等で情報セキュリティポリシーが遵守されているかどうかについて、また、問題が発生していないかについて常に確認を行い、問題が発生していた場合には速やかに最高情報統括責任者及び統括情報セキュリティ責任者に報告しなければならない。

職員は、情報セキュリティポリシーの違反が発生した場合には、直ちに情報管理者に報告を行わなければならない。情報管理者は、違反が発生し、それが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考えられる場合は、情報セキュリティ責任者、統括情報セキュリティ責任者及び最高情報統括責任者に報告しなければならない。

情報セキュリティ責任者は、所管する課等でサーバ等のシステム設定が情報セキュリティポリシーを遵守しているかどうかについて、また問題が発生していないか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速やかに適切に対応しなければならない。

（3）運用管理における留意点

統括情報セキュリティ責任者は、アクセス記録、メール受発信記録の情報

を閲覧できる権限を有する職員を定めなければならない。

システム管理者は、職員が常に情報セキュリティポリシー及び実施手順を参照できるよう配慮しなければならない。

（４）事故、欠陥に対する報告

職員は以下の場合、その状況を速やかに情報管理者に報告し、その指示に従い必要な措置を講じなければならない。

①情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合

②ネットワーク及び情報システムに関する事故、欠陥について住民から報告･連絡を受けた場合

③事故の内容は、システム管理者及び、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に報告しなければならない。なお、重大な事故の場合は、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。

④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は、これらの事故等を分析し、再発防止のための記録を保存しなければならない。

（５）侵害時の対応

情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じる緊急時対応計画については、立山町情報セキュリティ共通実施手順に定める。

（６）法令遵守

職員は、職務の遂行において使用する情報資産について、次の法令等を遵守しこれに従わなければならない。

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）

（７）違反時の対応

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

情報管理者が、職員による情報セキュリティポリシー違反を確認した場合、当該職員に対し、違反行為を是正するよう指導しなければならない。

情報管理者の指導によっても改善されない場合、情報管理者は、情報セキュリティ責任者又は統括情報セキュリティ責任者の同意を得て、当該職員のネットワーク又は情報システムの使用を停止することができる。

当該職員のネットワーク又は情報システムの使用を停止した場合、情報セキュリティ責任者又は統括情報セキュリティ責任者は、その旨を最高情報統括責任者に報告しなければならない。

（８）懲戒処分

情報セキュリティポリシーに違反した職員等及びその監査責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法に基づく懲戒処分の対象とする。

８　外部委託等

（１）外部委託先の選定基準

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

また、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

情報セキュリティ責任者は、所管する業務を外部委託する場合、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。

ア　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

イ　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

ウ　提供されるサービスレベルの保証

エ　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

オ　外部委託事業者の従業員に対する教育の実施

カ　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

キ　業務上知り得た情報の守秘義務

ク　再委託に関する制限事項の遵守

ケ　委託業務終了時の情報資産の返還、廃棄等

コ　委託業務の定期報告及び緊急時報告義務

サ　町による監査、検査

シ　町による事故時等の公表

ス　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

情報セキュリティ責任者は、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しなければならない。

（4）外部委託事業者への説明

情報セキュリティ管理者は、所管する業務を外部委託する場合、情報セキュリティポリシー等のうち外部委託事業者が遵守すべき内容及び機密事項等を説明しなければならない。

9　評価・見直し

(1) 監査

最高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情報セキュリティについて定期的に監査を行わなければならない。

ネットワーク及び情報システムの開発及び保守を外部委託事業者に委託している場合、情報セキュリティポリシーの遵守について監査しなければならない。

（2）点検

情報セキュリティ責任者は、職員へのアンケート等によって、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が実施されているかどうかについて、定期的に点検し、その結果を取りまとめ、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。

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について、定期的に点検を実施し、その結果について、情報セキュリティ責任者からの結果報告と合わせ、情報セキュリティ委員会に報告しなければならない。

（3）情報セキュリティポリシーの更新

情報セキュリティ委員会は、監査及び点検の結果を踏まえ、定期的に情報セキュリティポリシーの実効性を評価し、必要な部分の見直しを行わなければならない。

情報セキュリティポリシーの更新内容、時期については、情報セキュリティ委員会が決定する。