川俣町情報セキュリティポリシー

初　版

平成１６年3月２４日

川俣町電子社会推進本部決定

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とは、川俣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、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、川俣町が所掌する情報資産に関する業務に携わる全職員、非常勤及び臨時職員（以下、「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、川俣町情報セキュリティポリシーは、一定の普遍性を備えた部分としての「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依存する部分としての「情報セキュリティ対策基準」の２階層に分けて策定する。

また、情報セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定する。

川俣町情報セキュリティポリシー

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		情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

第１章　情報セキュリティ基本方針

１．目的

本町が取り扱う情報資産には、町民の個人情報をはじめとして、行政運営上重要な情報など、部外に漏洩等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おり、これらの情報資産を人的脅威や災害、事故等の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、安定的な行政サービス運営のためにも必要不可欠である。

また、近年のいわゆるＩＴ革命の進展により、電子政府や電子自治体の実現が期待されているところであり、本町がこれらに積極的に対応するためには、本町が管理する全ての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となる。

そのため、本町の情報資産の機密性、完全性及び可用性（注）を維持するための対策を整備するため、川俣町情報セキュリティポリシーを定めることとし、情報セキュリティの確保の取り組むこととする。

このうち、情報セキュリティ基本方針については本町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

(注):国際標準化機構（IS0）が定めるもの（IS07498-2:1989）

機密性（confidentiality）	：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
完全性（integrity）	：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
可用性（availability）	：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２．定義

(1)ネットワーク

本町における内部部局、各行政委員会、地方公営企業及び各教育機関（事務室及び職員室のみ）を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

(2)情報システム

電子計算機（業務系におけるネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、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の開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータをいう。

(4)情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

３．情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、本町の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

したがって、町長をはじめとして本町の情報資産に関する業務に携わる全ての職員等及び部外委託者は、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、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

４．情報セキュリティ管理体制

本町の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

５．情報資産の分類

情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行うものとする。

６．情報資産への脅威

セキュリティ対策を行ううえで、情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

(1)権限の無い者による故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難等

(2)職員等及び部外委託者による意図しない操作、故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び記録媒体の盗難及び規定外の情報システム端末操作によるデータ漏洩等

(3)地震、落雷、火災等の災害並びに事故、故障等による業務の停止

７．情報セキュリティ対策

上記６で示した脅威から本町の情報資産を保護するため、以下の情報セキュリティ対策を行うものとする。

(1)物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を行う。

(2)人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育、啓発及び訓練を行う。

(3)技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等、技術面の対策を行う。また、システム

開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等、運用面の対策を行う。

また、障害が発生した際に迅速な対応を可能とするための障害時対策を行う。

８．情報セキュリティ対策基準の策定

本町の情報資産について、上記７の情報セキュリティ対策を行うに当たっては、職員等が遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。

そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

９．情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産に関する手順を具体的に定めておく必要があるため、情報セキュリティ対策基準の基本的な要件に基づき、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、公開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のある情報であることから非公開とする。

10. 情報セキュリティ監査の実施

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、定期的に監査を実施する。

11. 評価及び見直しの実施

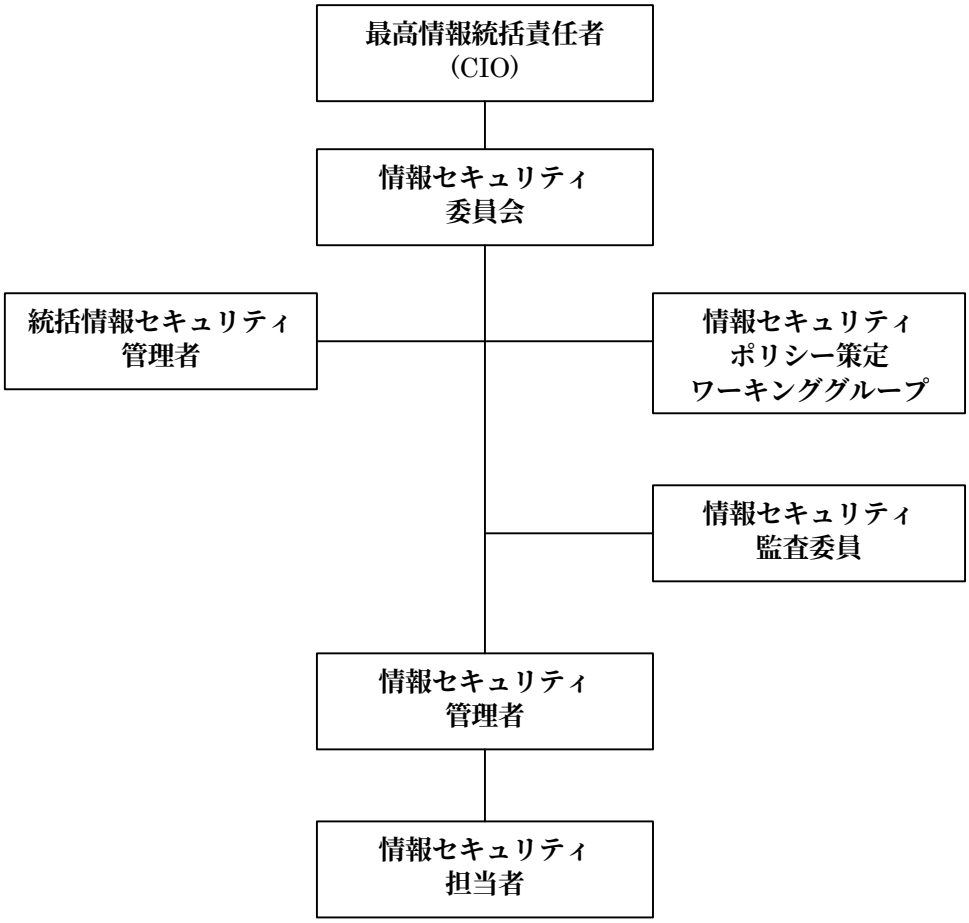
情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、適宜、情報セキュリティポリシーの見直しを実施する。

第２章　　情報セキュリティ対策基準

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本町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。

１．組織体制

情報セキュリティ対策の円滑な実施のため、次の組織体制及び役割とする。



名　　称	担当する組織 または役職	主　な　役　割
最高情報統括責任者 (Chief-Information-Officer)	助役	○情報セキュリティに関する全ての責任及び権限を有する ○情報セキュリティ会議を開催し、その委員長を務める
情報セキュリティ委員会	電子社会推進本部	○情報セキュリティに関する重要事項について協議及び承認する ○セキュリティ侵害、監査結果に対する改善策を協議する ○ポリシーの内容を審議し、必要に応じ情報セキュリティポリシー策定ワーキンググループに改訂を指示する

統括情報セキュリティ管理者	情報管理課長	○ポリシーの運営、普及、研修を行う ○情報セキュリティ委員会の決定事項を実施する ○情報セキュリティに係るヘルプデスク機能を担う ○庁内ネットワークの導入、保守を管理する ○各情報システムの適切な運用状況を管理する ○コンピューターウィルス対策の実施と徹底、セキュリティ侵害等の監視をする ○セキュリティ情報を収集し、必要に応じて各課への周知をする
情報セキュリティポリシー策定ワーキンググループ	情報化テクニカルリーダー	○情報セキュリティ委員会の指示によりポリシーの策定及び改訂を行う
情報セキュリティ監査委員	情報化テクニカルリーダー	○庁内におけるポリシーの遵守状況を監査する ○各情報システムのセキュリティレベルを監査する ○監査結果を情報セキュリティ委員会に報告する
情報セキュリティ管理者	各課（室）等の長	○所属内の情報セキュリティに関する責任及び権限を有する ○所属内で運用している情報システムの管理に関する責任及び権限を有する ○所属内において、ポリシーの普及及び指導を行い、遵守の徹底を図る ○セキュリティ侵害について、所属内に対処を指示し、統括情報セキュリティ管理者へ侵害内容、状況等を報告する
情報セキュリティ担当者	各課（室）等の長から指名された者	○情報セキュリティ管理者の指示により、所属内の情報セキュリティ対策を実施する ○セキュリティ侵害時には、情報セキュリティ管理者の指示により速やかに対処する

2．情報の分類と管理

(1)情報管理者の役割

情報の管理責任を明確にするため、情報管理者の役割は次のようにする。

名　称	対　象　者	該　当　者	主　な　役　割
情報所有者	情報の内容に関して責任を有する者	町長 または 各課（室）等の長	○情報に対して情報分類、開示範囲を指定する ○情報の開示範囲外への漏洩、改ざん、破壊が無いように適正に管理する ○情報の重要度の推移に応じて、適宜、情報分類、開示範囲を変更する
情報管理者	情報管理業務を実施する者	各課（室）等の長	○情報所有者が付与した情報分類、開示範囲に基づいて、情報の漏洩、改ざん、破壊等が生じないように管理し、利用状況についても把握する

情報利用者	情報を利用して業務を遂行する者	職員等	○情報所有者が付与した情報分類に基づき、情報を適切に扱い開示範囲外への開示を行わない ○情報所有者、情報分類、開示範囲の変更や内容の改ざんを行わない

(2)情報の分類

情報管理者及び利用者が適正な取り扱いを行えるようにするため、重要性に応じて次のとおり分類する。

情報分類	情　報　の　重　要　性
極秘	業務上の必要性に基づいて、庁内の特定の人物のみ開示される情報の分類である 情報所有者から開示を許可された者は、一切他の者に開示してはならない
部外秘	業務上の必要性に基づいて、庁内の特定の人物または特定の部署にのみ開示される情報の分類である 情報所有者から開示を許可された者は、付与された開示範囲外への開示をしてはならない
庁外秘	庁内において、業務に携わる職員等以外には開示されてはならない情報の分類である 情報所有者から開示を許可された者は、庁外への開示をしてはならない
公開	「極秘」、「部外秘」、「庁外秘」以外の情報である この情報については特別の分類表示は必要としない

(3)情報の管理及び取り扱い

情報の取得・作成、保管、利用、廃棄といった各場面において、情報を取り扱う者に判断基準を与えるため、情報分類ごとの取り扱い基準は次のとおりとする。

分類／場面	極　　秘	部　外　秘	庁　外　秘
取得・作成	○指定可能な開示範囲は特定の個人とする	○指定可能な開示範囲は特定の個人または組織とする	○指定可能な開示範囲は職員等とする
保　　管	○媒体は保管庫にて常時施錠管理する ○システム内の情報は暗号化またはパスワード保護及びアクセス権限の設定を実施する	○媒体は保管庫にて施錠管理する ○システム内の情報は、アクセス権限の設定を実施する	○媒体は保管庫にて施錠管理する ○システム内の情報は、アクセス権限の設定を実施する
利　　用	○情報所有者の許可のある場合に限り複製を可とする ○ネットワークでの流通に関しては、暗号化またはパスワード保護等の措置をとる	○開示範囲への配布目的に限り複製を可とする ○ネットワークでの流通に関しては、庁外への送信に限り暗号化、パスワード保護、または専用回線の利用等の保護措置をとる	○職員への配布目的に限り複製を可とする

廃　　棄	○媒体の場合は、裁断等により破壊する ○磁気媒体の場合は、統括情報セキュリティ管理者に依頼して廃棄する ○システム内の電子情報の場合は、復旧ツール等で復元できないよう完全に消去する	○媒体の場合は、裁断等により破壊する ○磁気媒体の場合は、統括情報セキュリティ管理者に依頼して廃棄する ○システム内の電子情報の場合は、復旧ツール等で復元できないよう完全に消去する	○媒体の場合は、裁断等により破壊する ○磁気媒体の場合は、統括情報セキュリティ管理者に依頼して廃棄する ○システム内の電子情報の場合は、復旧ツール等で復元できないよう完全に消去する

3．物理的セキュリティ

(1)入退室の管理

・　行政情報の記録されている媒体保管場所及びそれを取り扱う情報機器の設置場所（以下「情報システム室」という。）への入退室は許可された者のみとし、入退室管理簿の記載を行い、職員等及び外部委託事業者は身分証明書等を携帯し、求めにより提示しなければならない。

(2)職員の情報システムの機器管理

・　職員は執務室に職員が不在となる場合には、施錠するなど部外者の侵入を防ぐ措置を行わなければならない。

(3)機器等の搬入・搬出

・　情報システム室へ機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について、職員による確認を行わなければならない。

・　機器等の搬入・搬出には、職員が立ち会う等の必要な措置を施さなければならない。

(4)電源

・　停電及び電圧異常等によりデータ等が破壊され、業務処理に支障を来たす恐れのある情報システム等の機器は、当該機器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の予備電源を備え付ける等の措置を行わなければならない。

(5)配線

・　配線は、傍受または損傷等を受けることがないように可能な限り必要な措置を施さなければならない。

・　主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。

・　ネットワーク接続口（ハブ等）は、机上等への設置を避け、他の者が容易に発見できない場所に設置しなければならない。

(6)ネットワーク

・　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、できる限り接続ポイントを減らさなければならない。

４．人的セキュリティ

(1)職員

- 職員は、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。
- 職員は、情報セキュリティポリシー及び実施手順について不明な点、遵守することが困難な点等については、速やかに情報セキュリティ管理者に相談し、指示等を仰がなければならない。
- 職員は、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、または許可なく情報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。
- 情報セキュリティ担当者の許可を得ず、端末等を執務室外に持ち出してはならない。
- 職員は、異動、退職等により業務を離れる場合には、知り得た情報を秘匿しなければならない。

(2)非常勤及び臨時職員

- 非常勤及び臨時職員は、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。
- 非常勤及び臨時職員は、情報セキュリティポリシー及び実施手順について不明な点、遵守することが困難な点等については、速やかに情報セキュリティ管理者に相談し、指示等を仰がなければならない。
- 非常勤及び臨時職員には、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
- 非常勤及び臨時職員には、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
- 非常勤及び臨時職員は、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、または許可なく情報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。
- 非常勤及び臨時職員は、情報セキュリティ担当者の許可を得ず、端末等を執務室外に持ち出してはならない。
- 非常勤及び臨時職員は、異動、退職等により業務を離れる場合には、知り得た情報を秘匿しなければならない。

(3)外部委託に関する管理

- 情報システムの開発･保守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下請けとして受託する業者も含めて、情報セキュリティポリシーのうち外部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行わなければならない。

(4)教育・研修・訓練

- 最高情報統括責任者は、全ての職員及び関係する者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、職員を対象とした情報セキュリティポリシーに関する研修を設けなければならない。

・　情報セキュリティ管理者は、情報セキュリティ管理者として必要な知識を取得、維持するため、情報セキュリティに関する研修を受けなければならない。

・　職員は、情報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。

(5)パスワードの管理

・　職員は、自己の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いけない。

・　職員は、パスワードのメモを作らないこと。

・　職員は、パスワードを決めるとき、パスワードの長さは十分な長さとし、文字列は想像しにくいものとすること。

・　職員は、情報システムまたはパスワードに対する危険の恐れがある場合には、パスワードを速やかに変更すること。

・　複数の情報システムを扱う職員は、パスワードをシステム間で共有しないこと。

・　職員は、端末にパスワードを記憶させないこと。

・　職員は、職員間でパスワードを共有しないこと。

(6)ＩＣカード等の管理

・　職員は、ＩＣカード等の認証に用いるカード類を、職員等間で共有してはならない。

・　職員は、ＩＣカード等を、カードリーダ著しくは端末のスロット等に常時挿入したままにしてはならない。

・　職員は、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統括情報セキュリティ管理者に通報し、指示を仰がなければならない。

５．技術的セキュリティ

(1)情報システムの管理

①アクセス記録の取得

・　統括情報セキュリティ管理者は、各種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。

・　統括情報セキュリティ管理者は、アクセス記録等が窃取、改ざん、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。

・　統括情報セキュリティ管理者は、可能な範囲でアクセス記録等を分析しなければならない。

②情報システム管理記録の作成と確認

・　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、担当するシステムに対して行ったシステム変更等の処理について記録を作成し、適切に管理しなければならない。

③障害記録の作成

・　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、可能な範囲で障害記録作成し、一定の期間保存しなければならない。

④情報システム仕様書の管理

・　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、担当する情報システムの仕様書を最新の状態にしなければならない。また、システムの仕様変更の処理を行った場合は、その記録を作成し保存しなければならない。

・　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、情報システム仕様書については、記録媒体に関わらず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。また、構築に際して事業者に外部委託した場合、当該事業者に守秘義務を課さなければならない。

⑤バックアップの取得

・　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、ファイルサーバ等に記録された情報について、二重化措置に関わらずその重要度に応じて期間を設定し、定期的にバックアップ用の複製をとらなければならない。

⑥電子メールの送受信

・　統括情報セキュリティ管理者は、外部から外部へのメール転送(メールの中継処理)を不可能とする等、情報システム全般に悪影響を与えないような設定を施さなければならない。

・　職員は、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。

・　職員は、差出人が不明な、また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、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。

・　職員は、メールで重要な情報（情報分類における庁外秘以上）を送ってはならない。

⑦文書保存サーバー

・　統括情報セキュリティ管理者は、文書保存サーバーを設置する場合、課室等のフォルダ及びファイルを課室等単位で構成し、当該課室等に所属する職員以外の者が閲覧及び使用できないような設定を行わなければならない。

⑧職員以外の者が利用できる情報システム

・　統括情報セキュリティ管理者は、職員以外の者が利用できるシステムについては、必要に応じ他の情報システムと物理的に分ける等、情報セ

キュリティ対策について特に強固な対策をとらなければならない。

⑨情報システムの入出力データ

・　統括情報セキュリティ管理者は、情報システムに入力されるデータについて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。

・　情報セキュリティ管理者は、情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されていることを確認しなければならない。

⑩業務目的以外の使用の禁止

・　職員は、業務目的以外での情報システムへのアクセス及び電子メールの送受信を行ってはならない。

・　職員は、業務目的以外での情報システムへのアクセス、ウェブページの閲覧及び電子メールの送受信を行ってはならない。

⑪ソフトウェアの導入に関する注意

・　職員は、統括情報セキュリティ管理者に無断で、標準実装以外のアプリケーションソフトを端末にインストールしてはならない。

・　職員は、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。

⑫暗号化

・　暗号化については、統括情報セキュリティ管理者が定める方法を用いなければならない。

・　暗号のための鍵情報は、部外秘の行政情報として厳重に管理しなければならない。

⑬機器構成の変更

・　職員は、情報システムで使用する端末に対し、改造、機器の増設及び交換等を行ってはならない。

・　職員は、モデム等の機器を増設して他の環境へのネットワーク接続を行うことや、外部からのアクセスを可能とする仕組みを構築する場合は、統括情報セキュリティ管理者の許可及び指示に従わなければならない。

⑭利用プロトコル

・　統括情報セキュリティ管理者は、職員が利用できるプロトコルは、業務上必要最低限のものとしなければならない。

(2)情報システムのアクセス制御

①利用者登録

・　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、担当する情報システムの利用者の登録、変更、抹消等については、当該情報システムごとに定められた方法に従って行わなければならない。

・　利用者の登録、変更等は、統括情報セキュリティ管理者及び情報セキ

ュリティ管理者に対する申請により行わなければならない。

②インターネット以外のネットワークにおけるアクセス制御

・　統括情報セキュリティ管理者は、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な措置を行わなければならない。

③外部からのアクセス

・　統括情報セキュリティ管理者は、外部からのアクセスの許可について、必要最低限にしなければならない。

・　外部から本町の全てのネットワーク及び情報システムにアクセスする場合、外部アクセスサーバに対してのみ接続を許可することとし、直接内部のネットワークに接続してはならない。

・　外部から本町の全てのネットワーク及び情報システムにアクセスする場合、外部アクセスサーバに対してのみ接続を許可することとし、直接内部のネットワークに接続してはならない。また、この場合は、アクセス方法及び使用方法等は、利用者の真正性の確保が確定できるものでなければならない。

④外部ネットワークとの接続

・　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、セキュリティレベル等を詳細に検討し、本町の情報資産に影響が生じないと明確に確認したうえで、最高情報統括責任者の許可に基づき接続しなければならない。

・　統括情報セキュリティ管理者は、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。

・　統括情報セキュリティ管理者は、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、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。

・　統括情報セキュリティ管理者は、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、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物理的に遮断しなければならない。

⑤パスワードの管理方法

・　情報セキュリティ管理者は、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。

・　統括情報セキュリティ管理者は、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。

(3)情報システムの開発・導入・保守

①情報システムの開発・導入

・　統括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及び機

器を開発・導入する場合、情報セキュリティ上問題にならないかどうか、確認しなければならない。

・　統括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及び機器を開発・導入する場合、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。

・　統括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及び機器を開発・導入する場合、既に稼動している情報システムに接続する前に、十分な試験を行い、問題が無いことを確認しなければならない。

②情報システムの変更管理

・　統括情報セキュリティ管理者は、情報システムを追加、変更、廃棄等した場合、その際の設定・構成等の履歴を記録・保存し、必要な場合は復旧できるようにしなければならない。

③ソフトウェアの保守及び更新

・　統括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、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。

④機器の修理及び廃棄

・　記憶媒体の含まれる機器について、外部の業者に修理させまたは廃棄する場合は、その内容が消去された状態で行わなければならない。

・　故障を外部の業者に修理させる際、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に対し秘密を守ることを契約に定めなければならない。

(4)コンピューターウィルス対策

①統括情報セキュリティ管理者が行うもの

・　情報システムのサーバー及び必要な機器にウィルス対策ソフトを導入すること。

・　ウィルス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。

・　定期的に新種のウィルス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すること。

・　コンピューターウィルス情報について、職員に対する注意喚起を行うこと。

・　コンピューターウィルスについて、職員に対し必要な啓発活動を行うこと。

②職員が行うもの

・　外部からデータまた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、必ずウィルスチェックを行うこと。

・　ウィルスチェックの実行を途中で止めないこと。

・　添付ファイルのあるメールを送受信する場合は、ウィルスチェックを

行うこと。

・　統括情報セキュリティ管理者が提供するウィルス情報を常に確認すること。

(5)不正アクセス対策

・　統括情報セキュリティ管理者は、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等の提供があり次第、速やかに対応しなければならない。

・　情報セキュリティ管理者は、担当する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。

・　職員による不正アクセスがあった場合、統括情報セキュリティ管理者または情報セキュリティ管理者は、当該職員に対し、適切な処置をしなければならない。

・　職員による不正アクセスの結果、データの漏洩、破壊、改ざんまたはシステムダウン等により行政業務に深刻な影響をもたらした場合、当該職員を懲戒の対象とし、悪質な場合には刑事告発の対象とする。

(6)セキュリティ情報の収集

・　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情報を収集し、本町の全てのネットワーク及び情報システムについてセキュリティ対策上必要な措置を行わなければならない。

・　最高情報統括責任者は、セキュリティに関する情報を定期的に取りまとめ、関係部局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。

６．運用

(1)情報システムの監視

・　情報セキュリティ管理者は、担当する情報システムの運用にあたっては、常に情報システムを監視するとともに情報セキュリティ障害に対して注意を払わなければならない。

(2)情報セキュリティポリシーの遵守状況の確認

・　情報セキュリティ管理者は、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管理者に報告しなければならない。

(3)運用管理

・　統括情報セキュリティ管理者は、職員が常に情報セキュリティポリシーを参照できるようにしなければならない。

(4)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、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速やかに対応するとともに、再発防止の措置を行わなければならない。

①障害拡大の防止措置

・　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、故意の不正アクセスまたは不正操作により担当する情報システムに障害を及ぼすことが明らかな場合には、当該情報システムの停止を含む必要な措置を行わなければならない。

・　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、情報システムに障害を受け、その原因となる行為が不正アクセス禁止違反等の可能性がある場合には、行為の記録保存に努めなければならない。

②障害の調査

・　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、次の項目について調査をし、速やかに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。

(ｱ)障害の内容

(ｲ)障害が発生した原因

(ｳ)確認した被害、影響範囲

・　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から障害報告があった場合、その状況を確認した上で、最高情報統括責任者及び情報セキュリティ委員会へ報告しなければならない。

③障害への対応

・　情報セキュリティ管理者は、統括情報セキュリティ管理者の指示に基づき速やかにセキュリティ障害を復旧しなければならない。

・　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、統括情報セキュリティ管理者は、最高情報統括責任者に報告のうえ必要な指示を仰がなければならない。

④再発防止の措置

・　統括情報セキュリティ管理者は、当該障害を分析し、情報セキュリティポリシー及び実施手順の改善に係る再発防止計画を策定し、情報セキュリティ委員会へ報告しなければならない。

・　情報セキュリティ委員会は、情報セキュリティポリシー及び実施手順の改善に係る再発防止計画が有効であると認められる場合はこれを承認し、ポリシー策定ワーキンググループにポリシー改訂(案)の作成を指示する。

７．法令等遵守

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なければならない。

(1)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）

(2)著作権法（昭和４５年法律第４８号）
(3)行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（昭和６３年法律第９５号）
(4)川俣町個人情報保護条例（平成１１年条例第１号）

８．評価･見直し

(1)監査

・　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の監査を、情報セキュリティ監査委員に定期的に行わせなければならない。
・　情報セキュリティ監査委員は、所属の職員に対し監査を実施し、ポリシー及びこれに関連する規程等の遵守状況を把握・評価し、その結果を統括情報セキュリティ管理者に報告する。
・　統括情報セキュリティ管理者は、情報セキュリティ監査委員からの報告を取りまとめ、情報セキュリティ委員会に報告する。

(2)情報セキュリティポリシーの更新

・　新たに必要な対策が発生した場合または監査の結果を踏まえ、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実効性を評価･見直しを行い、新しい情報セキュリティポリシーを決定する。
・　最高情報統括責任者は、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。