富士川町情報セキュリティポリシー

平成２１年　３月　８日　　策定
平成２７年　４月　１日　全部改定
平成２８年　４月　１日　一部改定
平成３１年　４月　１日　一部改定
令和　８年　４月　１日　一部改定

目次

第１章　情報セキュリティ基本方針

１．目的

富士川町の各情報システムが取扱う情報には、町民の個人情報、行政運営上重要な情報など、外部への漏洩、消失、破壊、改竄、情報システムの停止等が発生した場合、極めて重大な結果を招くものが含まれている。これらの情報及び情報を取り扱うシステムを様々な脅威から防御することは、事務の安定的な運営を図り、町民の財産、プライバシー等を守るため不可欠である。また、情報技術の進歩にともない、より高度で広範囲な行政の情報化が進められている。富士川町がこれに対応していくためには、全ての情報システムの運用に対して十分な安全性を維持していくことが求められる。この要求に答えるため、富士川町職員等が情報資産を安全に取り扱うための規範である富士川町情報セキュリティポリシーを定める。富士川町情報セキュリティポリシーは、これを職員等に浸透、普及、定着を図ることにより、取り扱われる情報資産の安全性を高め、町民からの信頼の維持向上に寄与するためのものである。

２．定義

（１）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

（３）情報資産

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情報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

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（５）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（６）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（７）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（８）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（9）マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（１０）LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

（１１）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１２）通信経路の分割

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

（１３）無害化通信

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

３．対象とする脅威

情報資産への脅威は、情報を取り扱う環境に広く存在し、その形態も多様であるうえ、新たな種類の脅威が発生する場合もあるので、脅威の存在やその影響を常に監視するように努めるものとする。

本情報セキュリティポリシー策定時に特に考慮した、注意すべき脅威は以下のとおりである。

（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･盗聴･改ざん･消去、重要情報の搾取、内部不正等

（２） 情報資産の持出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、パスワードの不適切管理、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・盗聴・改ざん・消去等、搬送中の事故等による機器または情報資産の盗難等

（３） 地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止等

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

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

４．適用範囲

（１） 行政機関の範囲

本セキュリティポリシーが適用される行政機関は、内部の各所属、付属機関、教育委員会、議会事務局及び公営企業とする。

（２） 情報資産の範囲

本セキュリティポリシーが対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

5．職員等の遵守義務

職員、非常勤職員及び臨時職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6．情報セキュリティ対策

上記３で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

（１） 組織体制

富士川町の情報資産について、管理職が率先して情報管理対策を推進・管理するための全庁的な体制を確立するものとする。

（２） 情報資産の分類と管理

富士川町の情報資産を機密性、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ものとする。

（３） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、自治体情報セキュリティクラウドの導入等を実施する。

（４） 物理的セキュリティ対策

サーバ室、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講ずる。

（５） 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、全ての職員等及び外部委託事業者に情報セキュリティに関して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ずる。

（6） 技術的セキュリティ対策

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、コンピュータの管理、情報資産へのアクセス制御、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ずる。

（7） 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講ずる。また、情報資産へのセキュリティ侵害が発生した場合等に迅速かつ適切な対応を可能とするための緊急時対応体制を策定する。

（8） 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9） 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7．情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーが遵守されていることを検証するために、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8．情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果により、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を取り巻く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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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書の見直しを実施する。

９．情報セキュリティ対策基準の策定

富士川町の様々な情報資産について、上記６、７及び８の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為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。

１０．情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、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富士川町の行政運営に重大な支障を及ぼす恐れのある情報資産で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．対象範囲

1.1 行政機関の範囲

本対策基準が適用される行政機関は、富士川町の内部部局、出先機関、教育委員会、議会事務局、福祉・保健施設とする。

1.2 情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

（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

1.3 峡南広域行政組合情報センターとの連携

本対策基準の対象範囲に含まれる、峡南広域行政組合情報センターへの委託により運用される情報システム及びネットワーク、並びに峡南広域行政組合情報センターに保管される一部の情報資産については、富士川町と峡南広域行政組合情報センターとの緊密な連携により、管理方法及び運用方針の整合性を確認のうえ、以下に記載される基準が適用されるものとする。

1.4 住民基本台帳ネットワークシステムとの関係

この情報セキュリティポリシーの対象範囲に含まれる、住民基本台帳ネットワークシステムについては、住民基本台帳ネットワークシステムのセキュリティ規則に従い運用されるものとし、この情報セキュリティポリシーは、これを補完するものとする。

２．組織体制

富士川町の情報セキュリティ管理については、以下の組織・体制で運用するものとする。

2.1 統括情報セキュリティ責任者

政策秘書課長を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、次の事項を所掌する。

（１） 本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最終決定権限及び責任を有する。

（2） 副統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者等に対して、情報セキュリティに関する指導、助言、勧告、調査・報告依頼等を行う権限を有する。
（3） 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アドバイザーとして置くことができる。
（4） 本町の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
（5） 本町の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。
（6） 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必要かつ十分な措置を行う権限及び責任を有する。
（7） 本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実施手順の維持・管理を行う権限及び責任を有する。
（8） 緊急時等の円滑な情報共有を図るため、統括情報セキュリティ責任者、副統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及び関係者を網羅する連絡体制を整備する。
（9） 富士川町情報化推進委員会を設置し、主宰、統括する。

2.2 副統括情報セキュリティ責任者

財務課長を、副統括情報セキュリティ責任者とする。副統括情報セキュリティ責任者は、次の事項を所掌する。
（1） 統括情報セキュリティ責任者を補佐するものとする。
（2） 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おいて、統括情報セキュリティ責任者が不在その他緊急の場合には、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。

2.3 情報セキュリティ責任者

各所属の課長、出先施設の所長・局長・課長、議会事務局の局長、教育長を情報セキュリティ責任者とし、次の事項を所掌する。
（1） 情報セキュリティ対策に関する当該課等における統括的な権限及び責任を有する。
（2） 課内で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。
（3） 課内で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、富士川町情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、研修、訓練、助言及び指示を行う。
（4） 富士川町情報化推進委員会へ必要事項を報告する。

（5） 富士川町情報セキュリティポリシーに基づき、課内における情報システムの情報セキュリティ実施手順等を定めるとともに、情報セキュリティ対策の計画を定め、これを推進する。
（6） 課内で所有している情報システムについて、情報セキュリティ監査、自己点検を実施する。
（7） 情報資産の持ち出し等に関する安全管理措置を定め、職員等に周知する。
（8） 富士川町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遵守状況を把握、確認し、富士川町情報化推進委員会へ報告する。

2.4 情報セキュリティ管理者

各担当において、情報セキュリティ対策を実施するため、各リーダーを情報セキュリティ管理者とし、次の事項を所掌する。
（1） 富士川町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に基づき、必要な情報セキュリティ対策を実施する責任を有する。
（2） 情報セキュリティ対策の実施に際して、情報システム担当者を補助者とすることができる。
（3） 情報資産に対する侵害が発生した場合、又は侵害の恐れがある場合には、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、必要に応じて指示を仰がなければならない。

2.5 情報システム管理者

情報システム等の運用を担当するリーダー等を情報システム管理者とし、所管する情報システム等において次の事項を所掌する。
（1） 情報セキュリティ対策に関する権限及び責任を有する。
（2） 情報セキュリティ実施手順の作成及び維持・管理を行う。
（3） 情報セキュリティ対策について、所管するシステムの運用、利用における手順等を作成し、当該システムにかかる情報システム担当者、利用者及び委託会社等の関係者へ周知徹底する。
（4） 情報資産に対する侵害が発生した場合、又は侵害の恐れがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者へ速やかに報告を行い、必要に応じて指示を仰がなければならない。

2.6 情報システム担当者

情報システム管理者の指示に従い、情報システム等の開発、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する

2.7 富士川町情報化推進委員会

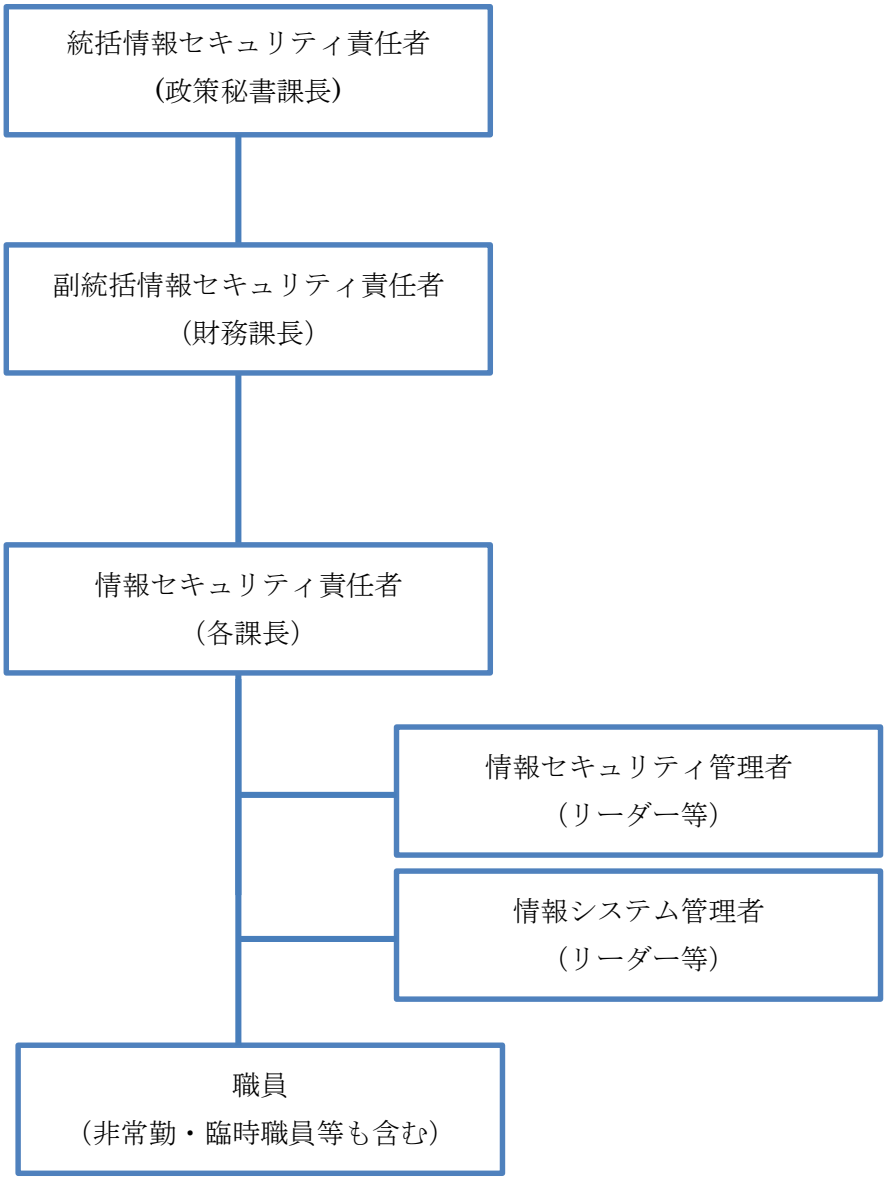
富士川町の情報セキュリティ対策を統一的に行うため、富士川町情報化推進委員会において、

情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。委員会に関する詳細事項については、統括情報セキュリティ責任者が別途定める。

2.8 兼務の禁止

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。また、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。

2.9 情報セキュリティ体制体系図



3．情報資産の分類と管理

3.1 情報資産の分類

（1） 情報資産の分類方法

対象となる情報システムの情報資産は、機密性、完全性及び可用性を踏まえ、次の通り分類する。分類に従い、必要に応じた管理基準、取扱い条件・制限等を設定し、適切に情報セキュリティ対策を実施するものとする。なお、分類については、情報システムの単位で重要度を設定できるものとする。

① 機密性による情報資産の分類

分類	分類基準	取扱制限
自治体機密性３A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	・ 支給された端末以外での作業の原則禁止（自治体機密性３の情報資産に対して） ・ 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電磁的記録媒体等の持ち込み禁止 ・ 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 ・ 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
自治体機密性３B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体機密性３C	行政事務で取り扱う情報資産のうち、自治体機密性３B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３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	
自治体機密性１	自治体機密性２ 又は自治体機密性３の情報資産以外の情報資産	・ 支給された端末以外での作業禁止

② 完全性による情報資産の分類

分類	分類基準	取扱制限
自治体 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、又は行政業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	・ 情報資産への不正なアクセスの遮断、また誤操作、機器障害等からの情報資産破損等の防御など、厳重な情報システム等の制御、監視等バックアップ、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 ・ 電磁的記録媒体の施錠可能な場所への保管
自治体 完全性１	自治体完全性２の情報資産以外の情報資産	

③ 可用性による情報資産の分類

分類	分類基準	取扱制限
自治体 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	・ 自然災害や停電等に際し、情報システム等が停止しても、一定時間内~~に~~の再稼動 ・ 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
自治体 可用性１	自治体可用性２の情報資産以外の情報資産	

④ 情報システム等の総合重要度による分類

上記を踏まえ、情報システム管理者は、所管する情報システム等において総合的に判断し、次のように総合重要度を設定する。

重要性分類	
Ⅰ	個人情報（富士川町個人情報保護条例及び同施行規則で規定するもの）及び富士川町の幹部及び業務上必要とする最小限の職員のみが扱う特に重要な情報。
Ⅱ	上記Ⅰ以外の非公開情報（富士川町情報公開条例により公開しないことができる情報等）及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす重要な情報。
Ⅲ	外部に公開する、または公開可能な情報のうち、セキュリティ侵害や情報の利用に関る障害が行政事務の執行等に影響を及ぼす情報。
Ⅳ	上記以外の情報。

3.2 情報資産の管理

（1） 管理責任

① 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

② 情報システム管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

③ 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”3.1 情報資産分類”に基づき管理しなければならない。

（2） 情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダ・フッター等)、格納する電磁的記録媒体(CD-R のラベル等)、文書の隅等に、情報資産の分類又は機密性が高い旨を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。また直ちに情報資産の分類等の表示が困難な場合は、情報セキュリティ管理者は情報システム等に記録される情報の分類を規程等により明記し、当該情報システムを利用する全ての者に周知させるものとする。

（3） 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、”3.1 情報資産分類“に基づき、当該情報の分類と取扱いの条件、制限等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ければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

（4） 情報資産の入手

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、”3.1 情報資産分類“に基づき、当該情報の分類と取扱いの条件、制限等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。

④ 特に重要な情報（重要性Ⅰ）及び重要な情報（重要性Ⅱ）を入手しようとする者は、情報資産の入手に際し、相手方に対して情報資産の暗号化又はパスワードの設定を要請しなければならない。

（5） 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、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、その中での最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

（6） 情報資産の保管

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存、保管しなければならない。特に重要な情報（重要性Ⅰ）については、盗難や情報漏えいの防止のため適切な物理的構造等となっている施錠できる保管庫等に保管すること。

② 情報セキュリティ管理者は、特に重要な情報（重要性Ⅰ）を保管している保管庫等については、鍵の管理について万全を期するとともに、保管状況等を定期的に点検しなければならない。

③ 情報セキュリティ管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じるとともに、定期的な確認、点検を行わなければならない。

④ 情報セキュリティ管理者は、特に重要な情報（重要性Ⅰ）を記録した電磁的記録媒体を保管する場合、極力、耐火、耐熱、耐水及び耐湿を講じた施錠可能な安全な場所に保管しなければならない。

（7） 情報資産の送信

自治体機密性３の情報は、電子メール等による送信を禁止する。ただし、業務遂行上他の手段により難い場合で、統括情報セキュリティ責任者の許可を得た場合は、この限りでない。なお許可を得て送信する場合であっても、自治体機密性３の情報を送信する者は、暗号化又はパスワード設定を行わなければならない。自治体機密性２の情報については、必要に応じ同様とする。

（8） 情報資産の運搬

① 特に重要な情報（重要性Ⅰ）又は、重要な情報（重要性Ⅱ）を運搬する者は、情報セキュリティ管理者の許可を得なければならない。なお、情報セキュリティ管理者は、必要に応じ適切な運搬方法についての指示を行うものとする。

② 車両等により特に重要な情報（重要性Ⅰ）又は、重要な情報（重要性Ⅱ）を運搬する者は、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。

（9） 情報資産の提供・公表

① 自治体機密性３以上の情報資産を、外部（当該情報資産を管理する所管以外の組織、個人）へ提供することを基本的に禁止する。但し、法令等により提供が認められており、かつ情報セキュリティ責任者の許可を得た場合は、この限りではない。

② 自治体機密性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の許可を得なければならない。

③ 自治体機密性２以上の情報資産を外部に提供する者は、暗号化又はパスワードの設定を行わなければならない。

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、完全性を確保しなければならない。

（１０） 情報資産の廃棄

① 情報資産の廃棄や返却等を行う者は、電磁的記録媒体内の情報について、その情報の機密性に応じ、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。

② 情報資産の廃棄や返却等を行う者は、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。

3.3 情報システム全体の強靭性の向上

(1)マイナンバー利用事務系

① マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。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、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

② 情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

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

（イ）情報の持ち出し不可設定

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

(2)LGWAN 接続系

① LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

（ア）インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

（イ）インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

（ウ）危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(3)インターネット接続系

① インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適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。

② 都道府県及び市区町村のインターネットとの通信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、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。

4．物理的セキュリティ

4.1 サーバ等の管理

（1） 機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合は、火災、水害、埃、振動、温度、湿度等の影響に対して、情報資産等の分類に基づく対策を施した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（2） 機器の電源

① 情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、 サーバ等の機器の電源については、停電等による電源供給の停止に備え、当該機器を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。

② 情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し 落雷等による過電流に対してサーバ等の機器を保護する措置を施さなければならない。

（3） 通信ケーブル等の配線

① 情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を施さなければならない。

② 情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

③ 情報システム管理者は、ネットワーク接続口（ハブのポート等）を管理者以外の者が容易に接続できないよう適切に管理しなければならない。

④ 情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者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。

（4） 機器の定期保守及び修理

① 情報システム管理者は、自治体可用性２以上のサーバ等の機器の定期保守を実施しなければならない。

② 情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を他の媒体にバックアップした上で、当該電磁的記録媒体内のデータを消去した状態で行わせなければならない。内容を消去できない場合は、点検･修理を委託する事業者との間で、守秘義務契約を締結する他、秘密保持体制の確認などを行わなければならない。

（5） 庁舎敷地外への機器の設置

情報システム管理者は、庁舎の敷地外にサーバ等の機器を設置する場合、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。また情報システム管理者は、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、立ち入り検査をするなどし、確認しなければならない。

（6） 機器等の廃棄

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

4.2 管理区域（情報システム室等）の管理

（1） 管理区域の構造等

① 管理区域とは、ネットワークの基幹機器や重要な情報システムに係る機器等を設置し、当該機器等の管理及びに運用を行うための部屋（以下「情報システム室」という。）や、電磁的記録媒体の保管庫をいう。

② 情報システム管理者は、管理区域を外壁等に囲まれた構造等により、外部からの進入が容易にできないようにしなければならない。

③ 情報システム管理者は、施設管理部門と連携して、管理区域から外部に通じるドアは、必要最小限とし、制御機能、鍵、警報装置等によって入退室管理を行い、許可されていない立入りを防止しなければならない。

④ 情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を施さなければならない。なお、情報システム室内の機器類の配置は、緊急時に職員等が円滑に避難できるように配慮しなければならない。

⑤ 情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部は全て塞ぐなど、容易に侵入できないようにしなければならない。

⑥ 情報システム管理者は、管理区域に配置する消化剤及び消防用設備等が、機器及び記録媒体に影響を与えないようにしなければならない。

（2） 情報システム室の入退室管理

① 情報システム管理者は、情報システム室の入退室は許可された者のみとし、IC カード入退室管理簿の記載等による入退室管理を行なわなければならない。

② 職員等及び外部委託事業者は、情報システム室に入室する場合、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。

③ 情報システム管理者は、外部からの訪問者が情報システム室に入室する場合には、必要に応じて立ち入り区域を制限した上で、情報システム室への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

④ 情報システム管理者は、自治体機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（3） 機器等の搬入出

① 情報システム管理者は、情報システム室へ搬入する機器が既存の情報システム等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。

② 情報システム管理者は、情報システム室への機器等の搬入出について、職員が同行する等の必要な措置を施さなければならない。

4.3 通信回線及び通信回線装置の管理

（1） 情報システム管理者は、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） 情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

（3） 情報システム管理者は、外部へのネットワーク接続は必要最小限のものに限定し、できる限り接続ポイントを減らさなければならない。

（4） 情報システム管理者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

（5） 情報システム管理者は、自治体機密性２以上の情報資産を取り扱う情報システム等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。

（6） 情報システム管理者は、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、不正な通信の有無を監視するセキュリティ対策を実施しなければならない。

（7） 情報システム管理者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

（8） 情報システム管理者は、自治体可用性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。

4.4 職員等のパソコン等の管理

（1） 情報システム管理者は、執務室等に職員等がいない場合は、執務室等の施鍵やワイヤーによる固定等による盗難防止のための物理的措置を施さなければならない。

（2） 電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

（3） 情報システム管理者は、情報システム等へのログインパスワードの入力を必要とするように設定しなければならない。

（4） 情報システム管理者は、極力、BIOS パスワード、ハードディスクパスワード等を併用しなければならない。

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

5．人的セキュリティ

5.1 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、その他情報セキュリティの確保に必要な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、指示を仰がなければならない。

（2） 業務以外の目的での使用等の禁止

職員等は、業務以外の目的で情報資産の使用、情報システム等へのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

（3） 情報資産の外部への持ち出し等の制限

① 統括情報セキュリティ責任者は、情報資産を外部へ移動又は持ち出しする場合等における安全管理措置を定めるとともに、職員に周知し遵守させなければならない。

② 重要性Ⅰの情報資産は、外部への移動又は持ち出しを禁止する。ただし、業務遂行上移動又は持ち出しが不可欠で、情報セキュリティ責任者の許可を得た場合はこの限りでない。

③ 職員等は、パソコン等の端末、記録媒体、情報資産及びソフトウエアを外部に移動又は持ち出す場合は、情報セキュリティ管理者の許可を得なければならない。

④ 職員等は、情報資産を外部に移動又は持ち出しする場合は、情報セキュリティ管理者の指示に従い、安全管理措置を遵守しなければならない。

（4） 支給以外のパソコン、モバイル端末及び電磁的記憶媒体等の持ち込み

職員等は、情報セキュリティ責任者に無断で支給以外のパソコン、モバイル端末及び電磁的記録媒体を庁舎内に持ち込み、作業を行ってはならない。また無断で支給以外のパソコン等の機器類をネットワークや情報システム等に接続してはならない。ただし、情報セキュリティ責任者が、業務上必要であると認める場合は、情報セキュリティ責任者の許可を得て、これらを持ち込んで作業することができる。この場合において、情報セキュリティ責任者は当該機器類について情報セキュリティに関して点検ができる。

（5） 持ち出し及び持ち込みの記録

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

（6） パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウエアに関するセキュリティ機能の設定を情

報セキュリティ責任者の許可なく変更してはならない。また、ソフトウエア等の更新について、情報システム管理者等の指示に従い、確実に実施しなければならない。

（7） 机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記憶媒体及び情報が印字された文書等について、第三者に使用されること、又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等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。

（8） 退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、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。

5.2 非常勤、臨時職員及び派遣職員への対応

（1） 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤職員､臨時職員及び派遣職員に対し、採用時又は派遣受入れ時に情報セキュリティポリシー等のうち、守るべき内容を説明し、実施及び遵守させなければならない。

（2） 情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤職員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を遵守する旨の同意書への署名を求めるものとする。

派遣職員は、業務以外の目的で情報資産の使用、情報システム等へのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

（3） インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤職員、臨時職員及び派遣職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要のときは、これを利用できないようにするなど、必要な制限を施さなければならない。

5.3 情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、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。

5.4 外部委託事業者等への対応

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等の開発・保守、運用等を外部委託事業者に行わせる場合は、外部委託事業者から再委託を受けている事業者も含めて、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について説明し、同意を求めなければならない。

5.5 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） 研修計画の立案及び実施

統括情報セキュリティ責任者は、情報セキュリティ研修について、基本的な方針を定めなければならない。

① 統括情報セキュリティ責任者は、幹部を含めすべ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を策定し、富士川町情報化推進委員会に報告しなければならない。

② 研修計画において、職員等が毎年度最低1回は情報セキュリティ研修等を受講できるようにしなければならない。

③ 新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

④ 研修は、情報セキュリティ責任者、情報システム管理者及びその他職員等に対して、それぞれの役割､情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤ 情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、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に対して、報告しなければならない。

⑥ 情報セキュリティ責任者は、研修の実施状況を分析、評価し、統括情報セキュリティ責任者に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

⑦ 統括情報セキュリティ責任者は、毎年度1回、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。

（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定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報処理システムの規模等を考慮し、訓練実施の体制、範囲等を定め、効果的に実施できるようにしなければならない。

（4） 研修・訓練への参加

すべての職員等は、定められた情報セキュリティ研修・緊急時対応訓練に参加しなければならない。

5.6 事故、欠陥に対する報告

（1） 庁内での情報セキュリティインシデントの報告

① 職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者に報告しなければならない。

② 報告を受けた情報セキュリティ管理者は、当該情報セキュリティインシデントに関連する場合、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③ 情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じ、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 情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。

（2） 住民等外部からの情報セキュリティインシデントの報告

① 職員等は、富士川町が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

② 報告を受けた情報セキュリティ管理者は、当該情報セキュリティインシデントに関連する場合、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③ 情報セキュリティ管理者は、当該情報セキュリティインシデントについて、適時、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追加報告しなければならない。

（3） 情報セキュリティインシデント原因の究明・記録、再発防止等

① 情報セキュリティ管理者及び情報システム管理者は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

② 情報セキュリティ管理者及び情報システム管理者は、情報セキュリティインシデントであると評価した場合、統括情報セキュリティ責任者に速やかに報告しなければならない。

③ 情報セキュリティ管理者及び情報システム管理者は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。また、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。

④ 情報セキュリティ管理者及び情報システム管理者は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、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。

⑤ 統括情報セキュリティ責任者は、情報セキュリティ管理者及び情報システム管理者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

5.7 ＩＤ及びパスワード等の管理

（1） ＩＤの取扱い

職員等は、自己の管理する又は共用のＩＤに関し、次の事項を遵守しなければならない。

① 自己が使用しているＩＤは、他人に使用させてはならない。

② 共用ＩＤを使用する場合は、共用ＩＤの使用者以外に使用させてはならない。

（2） パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

① 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ないこと。

② パスワードを記載したメモを容易に他人の目に触れるようにしてはならない。
③ 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。
④ パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを直ちに変更しなければならない。
⑤ パスワードは定期的に、又はアクセス回数に基づいて変更しなければならない。
⑥ 仮のパスワードは、最初のログイン時に変更しなければならない。
⑦ 端末にパスワードを記憶させないこと。
⑧ 職員等間でパスワードを共有しないこと。

（3） ＩＣカード等の管理

職員等が、ＩＣカード等の認証に用いるカードを利用してシステムを使用する場合は、次の事項を遵守すること。

① 職員等は、自己の管理するＩＤカード等に関し、次の事項を遵守しなければならない。
(ア) ＩＣカード等の認証に用いるカード類は、職員等間で共有してはならない。
(イ) 業務上必要のないときは、ＩＤカード等をカードリーダ若しくはパソコン等端末のスロット等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情報システム管理者に報告し、指示を仰がなければならない。
② 情報システム管理者は、ＩＣカード等の紛失等の通報があり次第、速やかに当該ＩＣカード等を使用したアクセス等を停止しなければならない。
③ 情報システム管理者は、ＩＤカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

6．技術的セキュリティ

6.1 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（文書サーバ）の設定等

① 情報システム管理者は、使用できるファイルサーバの容量を適切に設定しなければならない。
② 情報システム管理者は、ファイルサーバを組織等の適切な単位で構成し、職員等が他課等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。
③ 情報システム管理者は、個人情報、人事記録等、特定の職員等しか取扱いえないデータについて、別途保存場所（ディレクトリ）を作成する等の措置を講じ、同一組織であっても、担当職員以外の職員等が閲覧及び使用できないようにするなど、適切なアクセス権限を設定しなければならない。

（2） バックアップの実施

情報システム管理者は、情報処理システムやファイルサーバ等に記録された情報について、サーバの二重化対策に関わらず、情報資産の分類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） 他団体との情報システム等に関する情報等の交換

情報システム管理者は、他の団体と情報システム等に関する情報及びソフトウエアを交換する場合、その取扱いに関する事項をあらかじめ定め、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を得なければならない。

（4） システム管理記録及び作業の確認

① 情報システム管理者は、担当する情報システムにおいて行った作業記録を作成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システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合、作業内容について記録を作成し、窃取、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。

③ 統括情報セキュリティ責任者、情報システム管理者または情報システム担当者及び契約により操作を認められた外部委託事業者が、担当するシステムにおいてシステム変更等の作業を行う場合には、2名以上で作業し、互いにその作業を確認しなければならない。

（5） 情報システム仕様書等の管理

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、ネットワーク構成図、情報システム仕様書について、原則として秘密扱いとし、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

（6） アクセス記録の取得等

① 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、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システムの状態記録（ログ）を取得し、一定の期間保存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システム管理者は、アクセス記録等が、窃取、改ざん、誤消去等されないように必要な措置を施されなければならない。

③ 統括情報セキュリティ責任者又は情報システム管理者は、重要度Ⅰの情報システム等についてシステムから自動出力したアクセス記録等について、必要に応じ電磁的記録媒体にバックアップしなければならない。

（7） 障害記録

情報システム管理者は、職員等からのシステム等に関する不具合の情報、システム等に発生した障害報告、障害に対応した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。また、統括情報セキュリティ責任者から説明等の求めがあった場合、これに応じなければならない。

（8） ネットワークの接続制御、経路制御等

① 情報システム管理者は、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エア等を設定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。

③ 統括情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリ

ティを確保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、定期的な確認により見直さなければならない。

（9） 職員等以外の者が利用できる情報システム等の分離

情報システム管理者は、職員等以外の者が利用できるシステム等について、必要に応じ他のネットワーク及び情報システムと物理的に分離するなどの措置を講じなければならない。

（１０） 外部ネットワークとの接続制限

① 情報システム管理者は、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。

② 情報システム管理者は、接続しようとする外部ネットワークに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、所管するネットワーク、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。

③ 情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

④ 情報セキュリティ管理者及び情報システム管理者は、ウェブサーバ等をインターネットを介して公開する場合、所管する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設置したうえで接続しなければならない。

⑤ 情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められるなど、情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑥ 情報システム管理者は、外部との接続に際しての仕様、制限条件、及び障害発生時の連絡体制等、必要な事項を当該外部ネットワーク管理者との間で定めなければならない。

（１１） 複合機のセキュリティ管理

① 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及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

② 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正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③ 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する又は再利用できないようにする対策を講じなければならない。

（１２） IoT 機器を含む特定用途機器のセキュリティ管理

統括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講じなければならない。

（１３） 無線ＬＡＮの扱い及びネットワーク盗聴対策

① 職員等は、統括情報セキュリティ責任者及び情報システム管理者の承認のない無線ＬＡＮを使用してはならない。

② 統括情報セキュリティ責任者は、無線ＬＡＮの利用を例外的に認める場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

③ 統括情報セキュリティ責任者は、機密性の高い情報を扱うネットワークについて、情報の盗聴、不正アクセス等を防ぐため、暗号化等、必要な措置を講じなければならない。

（１４） 電子メールのセキュリティ管理

① 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、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 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、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、メールサーバの運用を停止するなど、必要な措置をとらなければならない。

③ 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、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 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、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 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、システム開発や運用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。

（１５） 電子メールの利用制限

① 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。

② 職員等は、業務上必要のない電子メールを送信してはならない。

③ 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。

④ 職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

⑤ 職員等は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。

（１６） 暗号化・電子署名

① 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、統括情報セキュリティ責任者が定めた電子署名、暗号化又はパスワード設定の方法を使用して、送信しなければならない。

② 職員等は、暗号化を行う場合に統括情報セキュリティ責任者が定める以外の方法を用いてはならない。また暗号のための鍵を適切に管理しなければならない。

（１７） 無許可ソフトウエアの導入等の禁止

① 職員等は、統括情報セキュリティ責任者の許可を得ずに、パソコン等の端末に許可を得ずにソフトウエアを導入してはならない。

② 職員等は、パソコン等の端末に不正にコピーした、又は出所の不明なソフトウエアを導入してはならない。

③ 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システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

（１８） 機器構成の変更の制限

① 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。

② 職員等は、業務上、パソコン等の端末に対し機器の分解、改造及び増設・交換を行う必要がある場合には、情報システム管理者の許可を得なければならない。

（１９） 業務外ネットワーク接続の禁止

職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

（２０） 業務以外の目的でのウェブ閲覧の禁止

① 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。

② 統括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、その程度や状況に応じ、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。

（２１） 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、本町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、本町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。

（２２） ソーシャルメディアサービスの利用

① 情報セキュリティ管理者は、本町が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない

(ア) 本町のアカウントによる情報発信が、実際の本町のものであることを明らかにするために、本町の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

(イ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（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すること。

② 自治体機密性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ならない。

③ 利用するソーシャルメディアサービスごとの責任者を定めなければならない。

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らない。

⑤ 自治体可用性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、本町の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

6.2 アクセス制御

（1） アクセス制御等

① アクセス制御

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、所管するネットワーク又は情報処理システムごとに、アクセスする権限のない職員等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上必要な措置をとらなければならない。

② 利用者ＩＤの取扱い

(ア) 情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

(イ) 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報システム管理者に通知しなければならない。

(ウ) 情報システム管理者は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、適切な時期及び頻度で点検しなければならない。

(エ) 情報システム管理者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

③ 特権を付与されたＩＤの管理等

(ア) 情報セキュリティ管理者及び情報システム管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

(イ) 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、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置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及び情報システム管理者の特権を代行する者は、情報システム管理者が指名し、統括情報セキュリティ責任者が認めた者でなければならない。

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

(オ) 情報セキュリティ管理者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードの変更について、外部委託事業者に行わせてはならない。

(カ) 情報セキュリティ管理者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードについて、変更頻度、入力回数制限等のセキュリティ機能について、職員等のそれよりも強化しなければならない。登録されているアクセス権限のレベルが、

業務の目的と合致し、情報資産の分類と利用の状態と整合しているかを定期的に確認しなければならない。

(キ) 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、特権を付与されたIDを初期設定以外のものに変更しなければならない。

（2） 職員等による外部からのアクセス等の制限

① 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等にアクセスしようとするときは、あらかじめ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。

② 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処理システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③ 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。

④ 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。

⑤ 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パソコン等の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。

（3） パスワード等に関する認証情報の管理

① 統括情報セキュリティ責任者又は情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

② 統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

③ 統括情報セキュリティ責任者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（4） 住民基本台帳ネットワークシステムとの接続

統括情報セキュリティ責任者及び住民基本台帳システムの情報システム管理者は、「富士川町住民基本台帳ネットワークシステムセキュリティ対策規則」に基づき適切なアクセス管理をしなければならない。

（5） 総合行政ネットワークとの接続

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、「総合行政ネットワーク接続仕様書」に基づき適切なアクセス管理をしなければならない。

6.3 システム開発、導入、保守等

（1） 情報システム及びソフトウエアの調達

① 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、情報システム及びソフトウエ

アの開発、導入及び保守等の調達については、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 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、機器及びソフトウエアの調達に当たっては、当該製品セキュリティ機能を調査し、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 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、機器及びソフトウエアの調達にあたっては、機器等におけるリース又は償却期間において、十分な最新パッチの提供等、セキュリティ対策の速やかな支援を得られるよう、契約書等に明記しなければならない。

（2） 情報システムの開発

① システム開発における責任者及び作業者の指定

情報システム管理者は、職員の中から、及び、委託する場合は委託事業者から、それぞれシステム開発の責任者及び作業者を指定しなければならない。

② システム開発における責任者、作業者のＩＤの管理

(ア) 情報システム管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

(イ) 情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③ システム開発に用いるハードウエア及びソフトウエアの管理

(ア) 情報システム管理者は、システム開発の責任者及び作業者が使用するハードウエア及びソフトウエアを特定しなければならない。

(イ) 情報システム管理者は、使用を認めたソフトウエア以外のソフトウエアが導入されている場合は、当該ソフトウエアをシステムから削除しなければならない。

④ アプリケーション・コンテンツの開発時の対策

情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

（3） 情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

(ア) 情報システム管理者は、システム開発・保守及びテスト環境とシステム運用環境を分離しなければならない。

(イ) 情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

(ウ) 情報システム管理者は、移行の際、情報システム等に記録されている情報資産の保存を確実に行い、移行に伴う情報システム等の停止等の影響が最小限になるよう配慮しなければならない。また、移行前に、導入されるソフトウエアに不正プログラム等の脅威がないことを確認しなければならない。

② テスト

(ア) 情報システム管理者は、新たに情報システム等を導入する場合、既に稼働している情報システム等に接続する前に十分な試験を行わなければならない。

(イ) 情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(ウ) 情報システム管理者は、個人情報及び機密性の高いデータを、テストデータに使用してはならない。

③ 機器等の納入時又は情報システムの受入れ時

(ア) 情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

(イ) 情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

(4) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。

(ア) 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

(イ) 情報システムの基盤を管理又は制御するソフトウェアで発生した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

(5) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

情報システム管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

(6) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

情報システム管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

(7) システム開発・保守に関連する資料等の整備・保管

① 情報システム管理者は、システム開発・保守に関連する資料及び文書を適切な方法で保管しなければならない。

(ア) 情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について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。

(イ) 情報システム管理者は、所管する情報システム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、以下を全て含む実施手順を整備しなければならない。

・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

・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

・情報システムが停止した際の復旧手順

② 情報システム管理者は、テスト結果を一定期間保管しなければならない。

③ 情報システム管理者は、情報処理システムに係るソースコードを適切な方法で保管しなければならない。

（8） 情報システムにおける入出力データの完全性、正確性の確保

① 情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むよう、設計しなければならない。

② 情報システム管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(ア) 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直ししなければならない。

(イ) 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

(ウ) ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

(エ) 情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むよう、設計しなければならない。

(オ) 情報システム管理者は、情報システム等から出力されるデータについて、情報の処理が正しく反映され、出力されるよう、設計しなければならない。

（9） 情報システム等の変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（１０） 開発・保守用のソフトウエアの更新等

情報システム管理者は、開発・保守用のソフトウエア等を更新、又はパッチの適用をする場合、他の情報システム等との整合性を確認しなければならない。

（１１） システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

（１２） 情報システムについての対策の見直し

情報システム管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本町内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、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。

6.4 不正プログラム対策

（1） 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

① 外部ネットワークから受信したファイルは、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。

② 外部ネットワークに送信するファイルは、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。

③ コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

④ 所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウエアを常駐させなければならない。なお、常駐により、本来目的とする機能が阻害される場合、又は常駐できない場合、これとは別に独立した不正プログラム検査用パソコン等を設け、これに代えることとする。この場合、前者パソコン等は外部ネットワークとの直接の接続をしてはならない。

⑤ 不正プログラム対策ソフトウエア及びパターンファイルは、常に最新の状態に保たなければならない。

⑥ 業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

（2） 情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

① 所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウエアをシステムに常駐させなければならない。

② 不正プログラム対策ソフトウエア及びパターンファイルは、常に最新の状態に保たなければならない。

③ インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、組織が管理している電磁的記録媒体以外の媒体を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウエアを導入し、定期的に当該ソフトウエ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。

④ 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

（1） 職員等の遵守事項

職員等は、コンピュータウィルス等の不正プログラム対策に関し、次の事項を遵守しなければならない。

① パソコン等の端末において、セキュリティ対策のための機能及びソフトウエアの設定を

変更してはならない。

② 外部からデータ又はソフトウエアを取り入れる場合には、必ず不正プログラム対策ソフトウエアによるチェックを行わなければならない。

③ 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④ 端末に対して、不正プログラム対策ソフトウエアによるすべての領域のチェックを定期的に実施しなければならない。

⑤ 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エアでチェックを行わなければならない。

⑥ 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 情報セキュリティ管理者又は情報システム管理者が提供するウイルス情報を、常に確認しなければならない。

⑧ コンピュータウイルス等の不正プログラムを検知又は感染が疑われる場合は、前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において直ちにＬＡＮケーブルの取り外しや、通信を行わない設定又は、機器の電源遮断を行わなければならない。

⑨ 情報セキュリティ管理者及び情報システム管理者の指示に従わなければならない。

（2） 専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、必要に応じて外部の専門家の支援を受けられるようにしておかなければならない。

6.5 不正アクセス対策

（1） 情報システム管理者の措置事項

情報システム管理者は、不正アクセス対策として、以下の事項を措置しなければならない。

① 使用されていないポートを閉鎖しなければならない。

② 不要なサービスについて、機能を削除又は停止しなければならない。

③ 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、情報システム管理者へ通報するよう、極力、設定しなければならない。

④ システムの重要な設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

⑤ 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統一的な窓口と連携し

⑥ 監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2） 攻撃の予告への対応

統括情報セキュリティ責任者は、サーバ等に攻撃を受けることが事前に明確になった場合あるいは可能性が高くなったと判断した場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関との連絡を密にして情報の収集に努めなければならない。

（3） アクセス記録の保存

統括情報セキュリティ責任者は、サーバ等が攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察・関係機関との緊密な連携に努めなくてはならない。

（4） 内部からの攻撃への対応

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、職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5） 職員等による不正アクセス

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、職員等による不正アクセスやその痕跡を発見した場合は、当該職員等が所属する課室等の情報セキュリティ責任者及び情報セキュリティ管理者に連絡し、適切な処置を求めなければならない。

（6） サービス不能攻撃

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、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（7） 標的型攻撃

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、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

6.6 セキュリティ情報の収集

（1） セキュリティホールに関する情報の収集・共有及びソフトウエアの更新等

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、セキュリティホールなど情報機器やソフトウエアの脆弱性に関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウエア更新等の対策を実施しなければならない。なお、この場合において、更新等の実施前に必要な試験、検査ができる。

（2） 不正プログラム等のセキュリティ情報の収集・周知

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、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない

（3） 情報セキュリティに関する情報の収集及び共有

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、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

7．運用

7.1 情報システムの監視

（1） 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責任者及び情報システム管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用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システム管理者は、情報システム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。

③ 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、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

（2） 情報システムの監視機能

① 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、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装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システム管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

③ 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、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

④ 統括情報セキュリティ責任者及び情報システム管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

（3） 情報システムの監視

① 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、セキュリティに関する事案を早期に検知するため、情報処理システムを運用時間中、常時監視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システム管理者は、重要なアクセスログ等を取得するとともに、サーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③ 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、外部と常時接続する情報システム等については、運用時間中、常時監視しなければならない。

7.2 情報セキュリティポリシーの遵守状況の確認

（1） 遵守状況の確認及び対処

① 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、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに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。

② 統括情報セキュリティ責任者は、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責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、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。

（2） パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

統括情報セキュリティ責任者又は、情報セキュリティ管理者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のアクセス記録、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。

（3） 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を発見した場合は、ただちに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に報告を行わなければならない。

② 当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると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が判断した場合は、緊急時対応体制に従って迅速な対処をしなければならない。

7.3 侵害時の対応

（1） 緊急時対応体制の整備

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や、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、緊急時対応体制を整備し、事故の発生時や情報資産への侵害発生時には当該体制に従って適切に対処しなければならない。

（2） 緊急時対応体制の内容

緊急時対応体制には、以下の内容を定めなければならない。

① 関係者の連絡先及び電子メールを含む連絡方法

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を指示する者

④ 事案の分析と再発防止措置の策定

⑤ 携帯電話等のロック等、盗難・紛失対策、及び、バックアップ等データ毀損対策、緊急時対応体制の見直し富士川町情報化推進委員会は、情報セキュリティを取り巻く状況の変化

や組織体制の変動等に応じ、必要に応じて緊急時対応体制を見直さなければならない。

（3） 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（4） 緊急時対応計画の見直し

統括情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

8. 業務委託と外部サービス（クラウドサービス）の利用

8.1 業務委託

（1） 業務委託に係る運用規程の整備

統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備しなければならない。

① 委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

② 委託事業者の選定基準

（2） 業務委託実施前の対策

① 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

(ア) 委託する業務内容の特定

(イ) 委託事業者の選定条件を含む仕様の策定

(ウ) 仕様に基づく委託事業者の選定

(エ) 情報セキュリティ要件を明記した契約の締結（契約項目）

情報システム等の運用等を外部委託する場合には、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に関する要件を明記した契約を締結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等の遵守
2. 委託先の責任者、委託内容、作業者、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. 発注者又は情報セキュリティ管理者による監査、点検、検査があり得ること、及び、その場合の協力義務

11. 事故発生時の報告及び対応義務
12. 遵守事項についての同意書等の提出
13. 情報セキュリティに関する要件が遵守されず、事故が発生した場合の規定（損害賠償等）
14. 情報セキュリティ事故発生時の事故内容、事業者名等の公表があり得ること
15. 個人情報漏えい防止のための技術的安全管理措置に関する取り決め
16. 委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法

（オ）委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

② 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

（ア） 仕様に準拠した提案

（イ） 契約の締結

（ウ） 委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結

（3） 業務委託実施期間中の対策

① 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。

（ア）委託判断基準に従った重要情報の提供

（イ）契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

（ウ）統括情報セキュリティ責任者へ措置内容の報告（重要度に応じて統括情報セキュリティ責任者に報告）

（エ）委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

② 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア）情報の適正な取扱いのための情報セキュリティ対策

（イ）契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

（ウ）委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

（4） 業務委託終了時の対策

① 情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

（イ）委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

② 情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。

(ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

(イ) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

（5） 確認・措置等

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、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、(2)の契約内容に基づき措置しなければならない。この場合において、その重要度に応じて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。

（6） 事故等発生時の事業者名の公表

統括情報セキュリティ責任者は、事業者の責任により、情報セキュリティ事故が発生した場合、町長と協議の上、内容や状況を考慮した上で、事業者名等の公表を行うことができる。

（5） その他の契約における扱い

職員等は、機器の賃借契約など、委託契約以外の契約について、情報セキュリティ確保の観点から必要と認められる場合は、必要に応じて対応するものとする。

8.2 情報システムに関する業務委託

（1） 情報システムに関する業務委託における共通的対策

情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本町の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

（2） 情報システムの構築を業務委託する場合の対策

情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

① 情報システムのセキュリティ要件の適切な実装

② 情報セキュリティの観点に基づく試験の実施

③ 情報システムの開発環境及び開発工程における情報セキュリティ対策

（3） 情報システムの運用・保守を業務委託する場合の対策

① 情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

② 情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

（4） 本町向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

① 情報システム管理者又は情報セキュリティ管理者は、外部の一般の者が本町向けに重

要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

② 情報システム管理者又は情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

③ 情報システム管理者又は情報セキュリティ管理者は、委託事業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。

④ 情報システム管理者又は情報セキュリティ管理者は業務委託サービスを利用する場合には、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へ当該サービスの利用申請を行わなければならない。

⑤ 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は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

⑥ 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は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

8.3 外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱う場合）

（１） 本町向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

統括情報セキュリティ責任者は、自治体機密性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 8.3 節において「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

（２） クラウドサービスの利用に係る運用規程の整備

① 統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、以下を含クラウドサービス（自治体機密性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。

② 統括情報セキュリティ責任者は、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、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。

③　統括情報セキュリティ責任者は、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。

④　統括情報セキュリティ責任者は、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。

(ア) クラウドサービスの利用終了時における対策

(イ) クラウドサービスで取り扱った情報の廃棄

(ウ) 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

（3） クラウドサービスの選定

①　情報セキュリティ責任者は、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　情報セキュリティ責任者は、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。

(ア) クラウドサービスの利用を通じて本町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

(イ) 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

(ウ) 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、本町の意図しない変更が加えられないための管理体制

(エ) 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

(オ) 情報セキュリティインシデントへの対処方法

(カ) 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

(キ) 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　情報セキュリティ責任者は、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　情報セキュリティ責任者は、クラウドサービスの利用を通じて本町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。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

⑤　情報セキュリティ責任者は、クラウドサービスの利用を通じて本町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、必要に応じて本町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 情報セキュリティ責任者は、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町に提供し、本町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 情報セキュリティ責任者は、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。

(ア) クラウドサービスに求める情報セキュリティ対策

(イ) 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

(ウ) クラウドサービスに求めるサービスレベル

⑧ 統括情報セキュリティ責任者は、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。

（4） クラウドサービスの利用に係る調達・契約

① 情報セキュリティ責任者は、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 情報セキュリティ責任者は、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。

（5） クラウドサービスの利用承認

① 情報セキュリティ責任者は、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。

（6） 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責任者は、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。

(ア) 不正なアクセスを防止するためのアクセス制御

(イ) 取り扱う情報の機密性保護のための暗号化

(ウ) 開発時におけるセキュリティ対策
(エ) 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責任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。

(ア) 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
(イ) 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
(ウ) 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。

(7) 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責任者は、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。

(ア) クラウドサービス利用方針の規定
(イ) クラウドサービス利用に必要な教育
(ウ) 取り扱う資産の管理
(エ) 不正アクセスを防止するためのアクセス制御
(オ) 取り扱う情報の機密性保護のための暗号化
(カ) クラウドサービス内の通信の制御
(キ) 設計・設定時の誤りの防止
(ク) 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責任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 情報セキュリティ責任者は、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。

（8） 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責任者は、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。

(ア) クラウドサービスの利用終了時における対策

(イ) クラウドサービスで取り扱った情報の廃棄

(ウ) 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。

8.4 外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱わない場合）

（1） クラウドサービスの利用に係る規定の整備

統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱わない場合、以下を含むクラウド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。

(ア) クラウドサービスを利用可能な業務の範囲

(イ) クラウドサービスの利用申請の許可権限者と利用手続

(ウ) 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

(エ) クラウドサービスの利用の運用手順

（2） クラウドサービスの利用における対策の実施

① 職員等は、利用するサービスの約款、その他の提供条件等から、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自治体機密性２以上の情報を取り扱わない場合のクラウドサービスの利用を申請しなければならない。また、承認時に指名されたクラウドサービス管理者は、当該クラウドサービスの利用において適切な措置を講じなければならない。

② 情報セキュリティ責任者は、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。また、承認したクラウドサービスを記録しなければならない。

９．例外処置

（1） 例外措置の許可

情報セキュリティ管理者又は情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、業務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、その期間を明示し、統括情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

（2） 緊急時の例外措置

情報セキュリティ管理者又は情報システム管理者は、業務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに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。

（3） 例外措置の申請書の管理

統括情報セキュリティ責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

１０．法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

① 地方公務員法(昭和 25 年法律第 261 号)
② 著作権法（昭和 45 年法律第 48 号）
③ 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）
④ 個人情報の保護に関する法律（平成 15 年法律第 57 号）
⑤ 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）
⑥ サイバーセキュリティ基本法（平成 26 年法律第 104 号）
⑦ 富士川町個人情報保護法施行条例（令和 4 年条例第 25 号）

１１．懲戒処分等

(1) 懲戒処分

情報セキュリティポリシーに違反し、重大な事故を発生させた職員等、あるいは重大な事故を発生させかねない状況に至らしめた職員等及びその管理監督者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象となる。

(2) 違反時の対応

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

① 統括情報セキュリティ責任者が違反を確認した場合、統括情報セキュリティ責任者は当該職員等が所属する課等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に通知し、適切な措置を求めなければならない。
② 情報システム管理者等が違反を確認した場合は、速やかに統括情報セキュリティ責任者及び当該職員等が所属する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。
③ 情報セキュリティ責任者又は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、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報処理システムを使用する権利を停止あるいは制限することができる。その後速やかに、統括情報セキ

ュリティ責任者は、職員等の権利を停止あるいは制限した旨を当該職員等が所属する課等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に通知しなければならない。

④ 違反及び対応のうち重大な事案については、情報セキュリティ管理者は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。

１２．評価・見直し

12.1 監査

（1） 実施方法

富士川町情報化推進委員会は、情報セキュリティ監査責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的及び必要に応じて情報セキュリティに関する監査を行わせなければならない。

（2） 監査を行う者の要件

① 情報セキュリティ監査責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

② 監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（3） 監査の実施計画の立案及び実施への協力

① 情報セキュリティ監査責任者は、監査等を行うに当たって、監査の実施計画を立案し、富士川町情報化推進委員会の承認を得なければならない。

② 被監査部門は、監査の実施に協力しなければならない。

（4） 外部委託事業者に対する監査

情報セキュリティ監査責任者は、情報システム等に係る業務の一部又は全部を外部委託事業者に委託している場合は、情報セキュリティ監査責任者は外部委託事業者から再委託を受けている事業者も含め、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（5） 報告

情報セキュリティ監査責任者は、監査の結果を取りまとめ、統括情報セキュリティ責任者及び富士川町情報化推進委員会に報告する。

（6） 保管

情報セキュリティ監査責任者は、監査の実施を通して収集した監査の証拠、報告書の作成のための調書を、紛失・毀損等が発生しないように適切に保管しなければならない。

（7） 監査等の結果への対応

統括情報セキュリティ責任者は、監査の結果を踏まえ、情報セキュリティ管理者及び指摘事項を所管する情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。また、当該所管部署以外の情報セキュリティ責任者に対しても、同種の課題及び問題点がある可能性がある場合には、当該課題及び問題点の有無を確認させ、必要に応じて対処を指示しなければならない。

（8） 情報セキュリティポリシーの見直し等への活用

富士川町情報化推進委員会は、監査結果を集約し、情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

12.2 自己点検

（1） 実施方法

① 情報セキュリティ管理者及び情報システム管理者は、所管するネットワーク及び情報システム等について、定期的及び必要に応じ自己点検を実施しなければならない。

② 情報セキュリティ管理者は、情報セキュリティ責任者と連携して、所管する組織における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じ自己点検を行わなければならない。

（2） 報告

情報セキュリティ管理者は、自己点検結果及び自己点検結果に基づく改善策を取りまとめ、富士川町情報化推進委員会に報告しなければならない。

（3） 自己点検結果の活用

① 情報セキュリティ管理者、情報システム管理者及び職員等は、自己点検の結果に基づき、改善を図らなければならない。

② 富士川町情報化推進委員会は、この点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

12.3 情報セキュリティポリシーの見直し

統括情報セキュリティ責任者及び富士川町情報化推進委員会は、情報セキュリティポリシーについて情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、必要に応じその見直しを行う。

附　則（平成２１年３月８日策定

１．富士川町情報セキュリティポリシーは、平成２２年３月８日から施行する。

２．このセキュリティポリシーの「情報資産の分類」に関する基準は、富士川町行政機関の職員による分類、整理がなされた情報資産から適用する。

附　則（平成２７年４月１日全部改定）

１．富士川町情報セキュリティポリシーは、平成２７年４月１日から施行する。

附　則（平成２８年４月１日一部改定）

１．富士川町情報セキュリティポリシーは、平成２８年４月１日から施行する。

附　則(平成 31 年４月１日一部改定)

１．富士川町情報セキュリティポリシーは、平成３１年４月１日から施行する。

附　則(令和８年４月１日一部改定)

１．富士川町情報セキュリティポリシーは、令和８年４月１日から施行する。