情報セキュリティ対策基準

第１　組織体制等

１　組織体制

構成		役割
最高情報セキュリティ責任者（CISO）	総務課長をもって充てる。	・本町の全ての情報資産の管理及び情報セキュリティ対策に関する方針を示す。 ・本町の全ての情報資産の管理及び情報セキュリティ対策のうち重要な事項についての決定を行う。
情報セキュリティ責任者	総務課企画推進係長をもって充てる。	・CISO を補佐する
情報セキュリティ管理者	各課等の長をもって充てる。	・各課等において所管する情報資産の管理及び情報セキュリティ対策を行う。
情報セキュリティ担当者	各課等において情報セキュリティ管理者が指名する者をもって充てる。	・情報セキュリティ管理者を補佐する。
最高情報セキュリティアドバイザー	CISO が、指名する者をもって充てる。	・CISO が定めた業務を行う。

２　情報セキュリティに関する意思決定

情報セキュリティに関する意思決定については、定例庁議の場において行うものとする。

３　情報セキュリティインシデントに関する統一的な窓口（CSIRT）の設置

(1)　CISO は、本町の情報資産に対する情報セキュリティインシデント（以下「インシデント」という。）が発生した場合又はインシデントのおそれがある場合に、速やかに自身への報告がなされるよう CSIRT を設置する。

(2)　CISO は、庁外の者からの問い合わせ先として、次の内容について周知及び公表する。

受付窓口	CSIRT（総務課企画推進係）
所在地	福島県石川郡古殿町大字松川字新桑原３１番地
連絡先	０２４７－５３－４６１１
対応時間	平日　８時３０分～１７時１５分

(3)　CSIRT の役割及び対応については、次のとおりとする。

役割	対応
インシデント発生時の対応	(1)　インシデントの発生に関する予兆等の検知及び発見並びに内部又は外部からのインシデントに関する連絡及び報告等の受付を行う。 (2)　事実関係を確認の上、インシデントが発生したかどうかを検査又は分析により判断し、被害状況や影響範囲等の事態全体像を把握した上で、インシデントの処理に優先順位を付ける。 (3)　初動対応（対応方針の検討、証拠の取得、保全、確保及び記録、インシデントの封じ込め及び根絶）の実施、復旧措置（暫定対策）の実施

	及び再発防止策（恒久対策）の検討を行う。 (4)　被害状況や影響範囲等に応じ、内外の関係者（総務省、福島県、内閣サーバセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity、以下「NISC」という。）警察機関等）への報告及び対外的な対応（報道発表及び関係住民への連絡）を行う。 (5)　インシデントの収束宣言を行い、報告書をまとめる。
平常時の事前準備及び予防対策等	(1)　インシデント発生時の対応に必要な事前準備及び予防対策を行う。 (2)　インシデント発生を想定した訓練及び演習の定期的な実施を行う。 (3)　インシデントの対応に関する手順等の定期的な評価及び見直しを行う。 (4)　その他 CSIRT 責任者が定める必要な事前準備及び予防対策を行う。

(4)　CSIRT の組織体制については、次のとおりとする。

構成		役割
CSIRT 責任者	CISO をもって充てる。	・インシデント対応の責任者。高い技能とインシデント対応経験を持ち、インシデント対応の作業を監督し、評価する責任を負う。また他の組織などとの調整役になり、危機を打開し、チームに必要な要員、リソース及び技能を確保する。その他インシデントハンドラーの作業を調整し、インシデントハンドラーからの情報を収集し、インシデントに関する最新情報を必要な関係者に提供する。
インシデントハンドラー	情報セキュリティ責任者をもって充てる。	・インシデント発生時のインシデント分析及び対処法の検討、関係部署との調整を行う等、インシデントに対応する CSIRT を実務的な観点から中核として支え、対応方針を検討し、インシデント発生時の対応全体（以下「インシデントハンドリング」という。）に係るプロジェクトマネジメント等を行う。
CSIRT 要員	インシデントの発生もととなる情報資産を管理する情報セキュリティ管理者及び情報セキュリティ担当者	・インシデントハンドラーを補助し、ともにインシデントハンドリングに当たる。
外部委託事業者	システムベンダー（開発事業者、運用・保守事業者等）、インターネットに接続するサービスを提供する事業者（ISP）、インターネッ	・検査又は分析、証拠の取得、保全、確保及び記録、インシデントの封じ込め及び根絶、復旧措置、再発防止策の検討等に係る一部の作業を行う。

	トなどを通じてソフトウェアを利用するサービスを提供する事業者（ASP)、クラウド事業者等のうち契約関係にある外部の事業者に対して、CSIRT 責任者が支援を依頼する者	
内部関係者	財政部門	・インシデントハンドリングにおける予算対応等行う。
	法務部門	・インシデントハンドリングにおける法的対応（契約を含む。）等を行う。
	広報部門	・インシデントハンドリングにおけるマスコミ対応等を行う。
外部の専門家	セキュリティ対策ソフトウェアや関連サービスを開発又は提供している事業者、NISC、情報処理推進機構（IPA)、JPCERT コーディネーション（JPCERT/CC)、警察等から CSIRT 責任者が支援を要請する者	・左記により要請等された作業を行う。

(5) CSIRT が扱うインシデントは、次のとおりとする。

インシデント	内容
情報システムの停止等	情報システム、ネットワーク、サーバ、端末等の利用に支障をきたす状態をいう。
外部からのサイバー攻撃	コンピュータウィルス、不正アクセス、Dos 攻撃、DDos 攻撃、標的型攻撃及びホームページ等の改ざんの発生又は発生が疑われる状態をいう。
盗難又は紛失	古殿町が管理する重要な情報（住民情報、企業情報、入札情報等）の盗難若しくは紛失又はこれらの可能性が疑われる状態（内部犯行に起因するものを含む。）をいう。

第２　情報資産の分類と管理方法

１　情報資産の分類

(1) 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。）による分類

分類	分類基準	取扱制限
機密性２	行政事務で取扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・支給されたパソコン、モバイル端末等以外での作業の禁止 ・必要以上の複製及び配布の禁止 ・原則施錠管理 ・情報の送信時におけるパスワード設定 ・情報資産の運搬時におけるパスワード設定等 ・情報資産の提供時におけるパスワード設定等 ・復元不可能な処理を施しての廃棄
機密性１	機密性２以外の情報資産	

(2) 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。）による分類

分類	分類基準	取扱制限
完全性２	行政事務で取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	・バックアップ ・原則施錠管理
完全性１	完全性２以外の情報資産	

(3)　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。）による分類

分類	分類基準	取扱制限
可用性２	行政事務で取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	・バックアップ ・復旧時間の指定 ・原則施錠管理
可用性１	可用性２以外の情報資産	

２　情報資産の管理

(1)　情報セキュリティ管理者は、所管する情報資産について管理責任を有し、当該情報資産に係る情報セキュリティ実施手順を整備するものとする。

(2)　情報資産が複製又は伝送された情報資産についても、複製等の元となった情報資産の分類に基づき管理しなければならない。

(3)　情報資産の分類表示

職員（非常勤職員及び臨時職員を含む。）は、機密性２、完全性２及び可用性２の情報資産については、電子データであればファイル名等での表示、機器等であればラベルシール等での表示をする等、当該情報資産の形態に合った形で分類表示を行わなければならない。

(4)　情報の作成

ア　職員は、業務上必要のない情報を作成してはならない。

イ　職員は、情報の作成時に当該情報資産の分類を定めなければならない。

ウ　職員は、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、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。

(5)　情報資産の入手

ア　職員が作成した情報資産を入手した職員は、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。

イ　職員以外の者が作成した情報資産を入手した者は、当該情報資産の分類を定めなければならない。

ウ　情報資産を入手した職員は、入手した情報資産の分類が不明な場合、当該情報資産を管理することとなる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。

(6)　情報資産の利用

ア　職員は、業務以外の目的に情報資産を利用してはならない。

イ　職員は、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。

ウ　職員は、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、最高度の分類に従って、当該電磁的記録媒体を取扱わなければならない。

(7)　情報資産の保管

情報セキュリティ管理者は、機密性２、完全性２及び可用性２の情報資産について施錠管理できるものについては、原則施錠管理しなければならない。

(8)　情報の送信

電子メール等により機密性２の情報を送信する職員は、パスワード設定を行わなければならない。

(9)　情報資産の運搬

ア　車両等により機密性２の情報資産を運搬する職員は、運搬する情報資産にパスワード設定を施さなければならない。ただし、パスワード設定を施すことができないものについては、２名体制で運搬する等して機密性を確保しなければならない。

イ　機密性２の情報資産を運搬する職員は、当該情報資産を管理する情報セキュリティ管理者の許可を得なければならない。

(10)　情報資産の提供・公表

ア　機密性２の情報資産を外部に提供する職員は、パスワード設定を行わなければならない。ただし、パスワード設定を施すことができないものについては、別な方法により機密性を確保しなければならない。

イ　機密性２の情報資産を外部に提供する職員は、当該情報資産を管理する情報セキュリティ管理者の許可を得なければならない。

ウ　情報セキュリティ管理者は、住民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。

(11)　情報資産の廃棄

ア　機密性２の情報資産を廃棄する職員は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、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。

イ　情報資産の廃棄を行う職員は、行った処理について、日時、担当者及び処理内容を当該情報資産を管理する情報セキュリティ管理者に報告しなければならない。

ウ　情報資産の廃棄を行う職員は、当該情報資産を管理する情報セキュリティ管理者の許可を得なければならない。

第３　物理的セキュリティ

１　サーバ等の管理

(1)　機器の取付け

情報セキュリティ管理者は、サーバ等の機器の取付けを行う場合、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、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

ア　情報セキュリティ管理者は、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。

イ　情報セキュリティ管理者は、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ための措置を講じなければならない。

(3)　通信ケーブル等の配線

ア　情報セキュリティ管理者は、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、主要な箇所について配線収納管を使用する等必要な措置を講じなければならない。

イ　情報セキュリティ管理者は、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な管理をしなければならない。

(4)　機器の定期保守及び修理

ア　情報セキュリティ管理者は、可用性２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。

イ　情報セキュリティ管理者は、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、情報セキュリティ管理者は、外部の事業者に故障を修理させるに当り、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ほか、秘密保持体制の確認などを行わせなければならない。

(5)　庁外への機器の設置

情報セキュリティ管理者は、庁外にサーバ等の機器を設置する場合、CISO 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。

(6)　機器の廃棄等

情報セキュリティ管理者は、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、全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。

2　サーバ室の管理

(1)　サーバ室の構造等

ア　CISO は、サーバ室を地階又は１階に設けてはならない。

イ　CISO は、サーバ室に通ずるドアを必要最小限とし、施錠管理によって許可されていない職員の立入りを防止しなければならない。

ウ　情報セキュリティ管理者は、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

エ　CISO は、サーバ室に配置する消化薬剤や消防用設備等が、機器等及び電磁的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)　サーバ室の入退室管理等

ア　CISO は、サーバ室への入退室を許可した者に制限し、入退室管理簿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は、サーバ室に入室する場合、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。

ウ　情報セキュリティ管理者は、許可されていない者をサーバ室に入室させたい場合は、CISO の許可を得なければならない。また、CISO が許可した場合、外見上職員等と区別できる措置を講じた上で、入室を許可されている職員を付き添わせなければならない

エ　サーバ室に入室する者は、パソコン、モバイル端末、通信回線装置、電磁的記録媒体等を必要以上に持ち込んではならない。

(3)　機器等の搬入出

ア　情報セキュリティ管理者は、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　情報セキュリティ管理者は、サーバ室への機器の搬入又はサーバ室からの機器の搬出について、サーバ室への入退室を許可された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)　情報セキュリティ管理者は、庁内の通信回線及び通信回線装置を、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)　情報セキュリティ管理者は、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。

(3)　情報セキュリティ管理者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するよう努めなければならない。

4　職員の利用する端末や電磁的記録媒体等の管理

(1)　情報セキュリティ管理者は、職員の利用する端末について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

(2)　情報セキュリティ管理者は、電磁的記録媒体の使用について記録を取らなければならない。記録する事項としては、使用・返却日時、担当者及び内容とする。

(3)　電磁的記録媒体を使用する職員は、当該電磁的記録媒体を管理する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)　電磁的記録媒体の使用を許可された職員は、使用目的を達成した場合、速やかに当該電磁的記録媒体を管理する情報セキュリティ管理者に返却しなければならない。また返却する場合において､保存する必要がない情報については返却前に消去しなければならない。

第４　人的セキュリティ

1　職員の遵守事項

(1)　職員の遵守事項

ア　情報セキュリティポリシー等の遵守

職員は、情報セキュリティポリシー及び実施手順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、速やかに当該情報資産を管理する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。

イ　業務以外の目的での使用の禁止

職員が業務以外の目的で、次に掲げる事項を行うことは禁止する。

(ｱ)　情報資産の外部への持ち出し

(ｲ)　情報システムへのアクセス

(ｳ)　電子メールアドレスの使用

(ｴ)　インターネットへのアクセス

ウ　モバイル端末や電磁的記録媒体の持ち出し及び外部における情報処理作業の制限

(ｱ)　情報セキュリティ管理者は、情報資産の外部への持ち出しについて記録をとならなければならない。記録する事項としては、持ち出し・返却日時、担当者及び目的とする。

(ｲ)　情報資産を外部に持ち出す職員は、当該情報資産を管理する情報セキュリティ管理者の許可を得なければならない。

エ　支給されたもの以外の情報資産の業務利用

(ｱ)　情報セキュリティ管理者は、支給されたもの以外の情報資産の業務利用について、原則禁止しなければならない。ただし、業務上の必要があると認めた場合は、使用を許可するものとする。

(ｲ)　支給されたもの以外の情報資産を使用する許可を得た職員は、当該情報資産について､業務上必要がなくなった場合は､速やかに許可した情報セキュリティ管理者に申し出て､使用を止めなければならない。また､当該情報資産の使用停止に伴い､記録されている情報についても､復元不可能な形で破棄しなければならない。

オ　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

職員は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を当該情報資産を管理する情報セキュリティ管理者の許可なく変更してはならない。

カ　机上の端末等の管理

職員は、離席時おけるパソコン、モバイル端末のロック並びに電磁的記録媒体等の施錠保管等をする等して第三者に使用されないよう必要な措置を講じなければならない。

2　研修・訓練

(1)　情報セキュリティに関する研修

CISO 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)　緊急時対応訓練

CISO 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。

(3)　研修・訓練への参加

職員は、定められた研修・訓練に参加しなければならない。

3　情報セキュリティインシデントの報告

(1)　庁内からのインシデントの報告

ア　職員は、インシデントを認知した場合、速やかに当該情報資産を管理する情報セキュリティ管理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管理者は、速やかに CSIRT に報告しなければならない。

(2)　庁外の者からのインシデントの報告

ア　職員は、本町が管理する情報資産に関するインシデントについて、庁外からの報告を受けた場合、当該情報資産を管理する情報セキュリティ管理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管理者は、速やかに CSIRT に報告しなければならない。

4　ID 及びパスワードの取扱い

(1)　ID の取扱い

職員は、自己の管理する ID に関し、次の事項を遵守しなければならない。

(ｱ)　自己が利用している ID を他人に利用させてはならない。

(ｲ)　共用 ID を利用する場合、共用 ID を利用者以外に利用させてはならない。

(2)　パスワードの取扱い

職員は、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。

(ｱ)　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。

(ｲ)　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。

(ｳ)　パスワードが流出したおそれがある場合には、当該情報資産を管理する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。

(ｴ)　職員間でパスワードを共有してはならない。

第5　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

ファイルサーバを管理する情報セキュリティ管理者は、ファイルサーバを課等の単位で構成し、職員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。

(2)　バックアップの実施

　ファイルサーバを管理する情報セキュリティ管理者は、ファイルサーバ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、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に関する情報等の交換

　情報セキュリティ管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、CISO 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

ア　情報セキュリティ管理者は、管理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　情報セキュリティ管理者は、管理する情報システムにおいて、システム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。

(5)　情報システム仕様書等の管理

　情報セキュリティ管理者は、ネットワーク構成図、情報システム仕様書について、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)　ログの取得等

　情報セキュリティ管理者は、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。

(7)　障害記録

　情報セキュリティ管理者は、職員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、一定期間保存しなければならない。

(8)　ネットワークの接続制御、経路制御等

ア　情報セキュリティ管理者は、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ェア等を設定しなければならない。

イ　情報セキュリティ管理者は、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。

(9)　外部の者が利用できるシステムの分離等

　情報セキュリティ管理者は、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物理的に分離する等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等

ア　情報セキュリティ管理者は、管理するネットワークを外部ネットワークに接続しようとする場合には、CISO の許可を得なければならない。

イ　情報セキュリティ管理者は、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、庁内の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。

エ　情報セキュリティ管理者は、ウェブサーバ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あると認められ、情報資産に脅威が生じることが想定される場合には、CISO 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。

(11)　複合機のセキュリティ管理

ア　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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インシデントへの対策を講じなければならない。

ウ　情報セキュリティ管理者は、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。

(12)　特定用途機器のセキュリティ管理

情報セキュリティ管理者は、特定用途機器について、取扱う情報、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。

(13)　無線 LAN 及びネットワークの盗聴対策

ア　情報セキュリティ管理者は、無線 LAN を使用する場合、解読が困難な暗号化された通信により使用できるものを選定しなければならない。

イ　情報セキュリティ管理者は、無線 LAN を使用する場合、CISO の許可を得なければならない。

ウ　情報セキュリティ管理者は、機密性の高い情報を取扱うネットワークについて、情報の盗聴を防ぐため、必要に応じて暗号化等の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

情報セキュリティ管理者は、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。

(15)　電子メールの利用制限

ア　職員は、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)　無許可ソフトウェアの導入等の禁止

ア　職員は、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　職員は、業務上の必要がある場合は、導入に係る情報資産を管理する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、導入する際は、当該情報セキュリティ管理者は、当該ソフトウェアのライセンスを管理しなければならない。

ウ　職員は、不正にコピーしたソフトウェアを利用してはならない。

(17)　機器構成の変更の制限

ア　職員は、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、当該変更に係る情報資産を管理する情報セキュリティ管理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

職員は、ネットワークにパソコンやモバイル端末を接続する場合、当該ネットワークを管理する情報セキュリティ管理者の許可を得なければならない。

(19)　業務以外の目的でのウェブ閲覧の禁止

ア　職員は、業務以外の目的でウェブを閲覧してはならない。

イ　職員は、業務以外の目的でウェブを閲覧している職員を見かけた場合、当該情報資産を管理する情報セキュリティ管理者に報告しなければならない。

ウ　報告を受けた情報セキュリティ管理者は、当該職員に対し適切な対応をしなければならない。

2　アクセス制御

(1)　アクセス制御等

ア　アクセス制御

情報セキュリティ管理者は、管理するネットワーク又は情報システムごとに、アクセスする権限のない職員がアクセスできないようにシステム上制限をしなければならない。

イ　利用者 ID の取扱い

(ｱ)　情報セキュリティ管理者は、アクセスを許可した者の利用者 ID を適切に管理しなければならない。

(ｲ)　職員は、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、当該情報資産を管理する情報セキュリティ管理者に申し出なければならない。

(ｳ)　情報セキュリティ管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

ウ　特権を付与された ID の管理等

情報セキュリティ管理者は、管理者権限等の特権を付与された ID を利用する職員を必要最小限にし、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。

(2)　職員による外部からのアクセス等の制限

ア　職員が外部から内部のネットワーク又は情報システムにアクセスする場合は、当該ネットワーク又は当該情報システムを管理する情報セキュリティ管理者の許可を得なければならない。

イ　情報セキュリティ管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の職員に限定しなければならない。

ウ　情報セキュリティ管理者は、外部からのアクセスに利用するモバイル端末を職員に貸与する場合、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。

エ　職員は、持ち込んだパソコン又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウィルスに感染していないこと、パッチの適用状況等を確認しなければならない。

オ　情報セキュリティ管理者は、公衆通信回線（公衆無線 LAN 等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID 及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（IC カード等）による認証に加えて通

信内容の暗号化、情報セキュリティ確保のために必要な措置を講じなければならない。

(3) 自動識別の設定

情報セキュリティ管理者は、管理する情報資産のうちネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

(4) パスワードに関する情報の管理

情報セキュリティ管理者は、職員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。

(5) 特権による接続時間の制限

情報セキュリティ管理者は、管理する情報資産への特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

3 システム開発、導入、保守等

(1) 情報システムの調達

ア 情報セキュリティ管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

イ 情報セキュリティ管理者は、機器及びソフトウェアの調達に当たっては、当該製品の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。

(2) 情報システムの開発

ア システム開発における責任者及び作業者の特定

情報セキュリティ管理者は、システム開発の責任者及び作業者を特定しなければならない。

イ システム開発における責任者、作業者の ID の管理

(ｱ) 情報セキュリティ管理者は、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) 情報セキュリティ管理者は、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い。

ウ システム開発に用いるハードウェア及びソフトウェアの管理

(ｱ) 情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(ｲ) 情報セキュリティ管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

(3) 情報システムの導入

ア 開発環境と運用環境の分離及び移行手順の明確化

(ｱ) 情報セキュリティ管理者は、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) 情報セキュリティ管理者は、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) 情報セキュリティ管理者は、移行の際、情報システム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。

(ｴ) 情報セキュリティ管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

イ テスト

(ｱ) 情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

(ｲ) 情報セキュリティ管理者は、運用テストを行う場合、あらかじめ疑似環境による操作確認を行わなければならない。

(ｳ) 情報セキュリティ管理者は、個人情報及び機密性の高い生データをテストデータに使用してはならない。

(ｴ) 情報セキュリティ管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

(4) システム開発・保守に関連する資料等の整備・保管

ア 情報セキュリティ管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

イ 情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

ウ 情報セキュリティ管理者は、情報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。

(5) 情報システムにおける入出力データの正確性の確保

ア 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、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に情報システムを設計しなければならない。

イ 情報セキュリティ管理者は、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に情報システムを設計しなければならない。

ウ 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について、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(6) 情報システムの変更管理

情報セキュリティ管理者は、情報システムを変更した場合、プログラム仕様書の変更履歴を作成しなければならない。

(7) 開発・保守用のソフトウェアの更新等

情報セキュリティ管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(8) システム更新又は統合時の検証等

情報セキュリティ管理者は、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。

4 不正プログラム対策

(1) 情報セキュリティ管理者の措置事項

ア 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウィ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。

イ 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウィ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。

ウ　管理するサーバ及びパソコン等の端末に、コンピュータウィルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
エ　不正プログラム対策のソフトウェアの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。
オ　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
カ　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。
キ　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、コンピュータウィルス等の感染を防止するために、町が管理している媒体以外を職員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ェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

(2)　職員の遵守事項

ア　パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
イ　外部からデータ又はソフトウェアを取り入れる場合には、不正プログラム対策ソフトウェアによるチェックを行わなければならない。
ウ　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、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
エ　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。
オ　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。
カ　CISO が提供するウィルス情報を、常に確認しなければならない。
キ　コンピュータウィルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。
(ｱ)　パソコン等の端末の場合　LAN ケーブルの即時取り外しを行わなければならない。
(ｲ)　モバイル端末の場合　直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

(3)　専門家の支援体制

CISO 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、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。

5　不正アクセス対策

(1)　情報セキュリティ管理者の措置事項

ア　使用していないポートを閉鎖しなければならない。
イ　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。
ウ　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の対策を講じなければならない。

(2)　攻撃の予告

CISO は、サーバ等に攻撃を受けることが明確になった場合、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。

(3)　記録の保存

CISO は、サーバ等に攻撃を受け、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、警察及び関係機関との緊密な連携に努めなければならない。

(4) 内部からの攻撃

情報セキュリティ管理者は、職員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) 職員及び外部委託事業者による不正アクセス

職員及び外部委託事業者による不正アクセスを発見した職員は、当該情報資産を管理する情報セキュリティ管理者に通知しなければならない。

(6) サービス不能攻撃

情報セキュリティ管理者は、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ための対策を講じなければならない。

(7) 標的型攻撃

情報セキュリティ管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

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・共有及びソフトウェアの更新等

CISO は、セキュリティホール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、情報セキュリティ管理者にソフトウェア更新等の対策をするよう指示しなければならない。

(2) 不正プログラム等のセキュリティ情報の収集・周知

CISO 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

CISO 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るよう情報セキュリティ管理者に指示しなければならない。

第6 運用

1 例外措置

(1) 例外措置の許可

情報セキュリティ管理者は、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守することが困難な状況で、行政事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、CISO 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は、行政事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回避のときは、事後速やかに CISO に報告しなければならない。

(3) 例外措置の記録の管理

CISO は、例外措置を許可したことについて記録をとらなければならない。記録する事項としては、日時、申請者名、内容及び理由とする。

2 法令遵守

職員は、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。

ア　地方公務員違法（昭和２５年法律第２６１号）

イ　著作権法（昭和４５年法律第４８号）

ウ　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）

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）

3　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た職員は、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する。

(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、速やかに次の措置を講じなければならない。

ア　違反を確認した職員は、当該違反に係る情報資産を管理する情報セキュリティ管理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管理者は、当該職員に対し、適正な取扱いをするよう指導しなければならない。

ウ　指導しても改善されない場合には、情報セキュリティ管理者は当該職員のネットワーク又は情報システムを使用する権利を停止或いは剥奪しなければならない。また、その内容について CISO に報告しなければならない。

第７　外部サービスの利用

1　外部委託

(1)　外部委託事業者の選定基準

ア　情報セキュリティ管理者は、外部委託事業者の選定にあたり、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。

イ　情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況を参考にして、事業者を選定しなければならない。

ウ　情報セキュリティ管理者は、クラウドサービスを利用する場合は、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するものとする。

(2)　契約項目

情報セキュリティ管理者は、情報システムの運用、保守等を外部委託する場合には、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ポリシー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、作業者、委託内容、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) 町によるインシデント発生時の公表
(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

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なければならない。

2 約款による外部サービスの利用

(1) 職員は、利用する外部サービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で、当該外部サービス利用しなければならない。

(2) 当該外部サービスを利用する職員は、その利用に係る情報資産を管理する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) 情報セキュリティ管理者は、許可した外部サービスについて記録をとらなければならない。記録する事項としては、サービス提供者、サービス名、利用目的、利用期間、利用する職員名とする。

3 ソーシャルメディアサービスの利用

(1) 職員は、本町のアカウントにより情報発信を行う場合、現に本町のものであることを明らかにするために、本町の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己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行わなければならない。

(2) 機密性２の情報は、ソーシャルメディアサービスで発信してはならない。

第８ 評価・見直し

1 監査

(1) 実施方法

CISO は、監査する者（以下「監査実施者」という。）を外部から選任し、本町の情報資産における情報セキュリティ対策の状況について、定期的に監査を行わせなければならない。

(2) 監査を行う者の要件

ア 被監査部門から独立した者であること。

イ 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あること。

(3) 監査の実施への協力

被監査部門は、監査の実施に協力しなければならない。

(4) 報告

監査実施者は、監査結果を取りまとめ、CISO に報告する。

(5) 保管

監査実施者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

(6) 監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を全ての情報セキュリティ管理者に周知するものとし、改善を要する取扱いをしている情報セキュリティ管理者には、その改善を指示するものとする。

2 自己点検

(1) 実施方法

情報セキュリティ管理者は、管理する情報資産における情報セキュリティ対策の状況について、定期的に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、自己点検結果と自己点検結果に基づく改善策を取り

まとめ、CISO に報告しなければならない。

(3)　自己点検結果の活用

職員は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

3　情報セキュリティポリシーの見直し

CISO は、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踏まえ、情報セキュリティポリシーについて毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合見直しを行うものとする。