上毛町
情報セキュリティポリシー

平成１７年１０月１１日　策　　定

平成２７年１１月２４日　全部改定

令和　４年　４月　１日　一部改定

令和　８年　３月３１日　一部改訂

－目　　次－

第１章　上毛町情報セキュリティ基本方針

第２章　上毛町情報セキュリティ対策基準

情報セキュリティ緊急時対応計画

序　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、上毛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、上毛町が所掌する情報資産に関する業務に携わる全職員、会計年度任用職員（以下、「職員等」という。）及び外部委託事業者に浸透、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、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（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（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

①情報セキュリティ基本方針
②情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする。（下表参照）。

情報セキュリティポリシーの構成

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		ネットワーク及び情報システム毎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　上毛町情報セキュリティ基本方針

１　目的

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

本町は、町民の個人情報や行政運営上重要な情報などの重要な情報を多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、町民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。また、本町には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。

そのため、本基本方針は、本町が保有する情報資産の機密性、完全性及び可用性を維持するため、本町が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

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、ネットワーク及び電磁的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。

(4)　情報セキュリティポリシー

本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であり、情報セキュリティ対策の頂点に位置するものとする。

(5)　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。

(6)　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。

(7)　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。

(8)　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。

(9)　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。）。

(10)　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。

(11)　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。

(12)　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

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

(1)　不正アクセス、ウィルス攻撃、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

本基本方針が適用される行政機関は、町長部局、議会事務局、各行政委員会及び議会とする。

(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。

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

職員等は、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の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じる。

(1)　組織体制

本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

本町の保有する情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行う。

(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、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した上で、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

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。

(5)　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。

(6)　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。

(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じるものとする。また、情報資産に対するセキュリティ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。

(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、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を見直す。

9　情報セキュリティ対策基準の策定

上記６、７及び８に規定する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る情報セキュリティ対策基準を策定する。

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に基づき、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おそれがあることから非公開とする。

第２章　上毛町情報セキュリティ対策基準

１　対象範囲

(1)　行政機関の範囲

本対策基準が適用される行政機関は、町長部局、議会事務局及び各行政委員会（以下「町長部局等」という。）とする。

(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、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

２　組織体制

(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　町長部局等における全てのネットワーク（上毛町住民基本台帳ネットワークシステムを除く。以下同じ。）、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者として、CISO を置く。

②　CISO 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。

③　CISO は、副町長をもって充てる。

(2)　統括情報セキュリティ責任者

①　CISO を補佐する者として、統括情報セキュリティ責任者を置く。

②　統括情報セキュリティ責任者は、ネットワーク管理者、情報セキュリティ管理者及び情報システム管理者に対して、情報セキュリティに関する指導、監督及び助言を行う。

③　統括情報セキュリティ責任者は、本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。

④　統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、ネットワーク管理者、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を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑤　統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、

回復のための対策を講じなければならない。

⑥　統括情報セキュリティ責任者は企画開発課長をもって充てる。

(3)　ネットワーク管理者

①　町長部局等における全てのネットワークを管理する責任者として、ネットワーク管理者を置く。

②　ネットワーク管理者は、町長部局等における全てのネットワークの開発、設定の変更、運用、更新等を行う権限及び責任を有する。

③　ネットワーク管理者は、町長部局等における全てのネットワークに関する情報セキュリティ実施手順の策定、変更を行う。

④　ネットワーク管理者は、情報システムの追加、変更の承認を行う。

⑤　ネットワーク管理者は、企画開発課企画情報係長をもって充てる。

(4)　情報セキュリティ管理者

①　町長部局等における全てのネットワークに関する情報セキュリティ、情報システム及び情報資産に関する情報セキュリティを管理する責任者として、情報セキュリティ管理者を置く。

②　情報セキュリティ管理者は、町長部局等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。

③　 情報セキュリティ管理者は、情報システムの連絡体制の構築並びに本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、訓練、助言及び指示を行う。

④　情報セキュリティ管理者は、町長部局等における全てのネットワークに関する情報セキュリティ実施手順、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、管理を行い、緊急時対応計画の策定、変更を行う。

⑤　情報セキュリティ管理者は、企画開発課長をもって充てる。

(5)　情報システム管理者

①　各情報システムを管理する責任者として、情報システム管理者を置く。

②　情報システム管理者は、所管する情報システムにおける開発、運用、更新等を行う権限及び責任を有する。

③　情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

④　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の策定、変更を行う。

⑤　情報システム管理者は、情報資産を利用する職員等を指導、監督する。

⑥　情報システム管理者は、所管する情報資産に対するセキュリティ侵害が発生した場合またはセキュリティ侵害のおそれがある場合には、情報セキュリティ管理者、ネットワーク管理者、統括情報セキュリティ責任者、CISO へ速やかに報告を行い、 指示

を仰がなければならない。

⑦　情報システム管理者は、業務を所管する課長もしくは同等程度の職責を負う職員等（以下、「課長等」という。）をもって充てる。

(6)　情報システム担当者

①　情報システム担当者は、担当する情報システムに関して、情報システム管理者の指示に従い、開発、設定の変更、運用、更新等の作業を行う。

②　情報システム担当者は、各課に１名以上置くこととする。

(7)　上毛町情報化推進委員会

上毛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、情報化推進委員会において、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作成など、情報セキュリティに関する重要な事項を審議する。

また、上毛町情報化推進委員会は、情報セキュリティに対する意識を醸成し保つために、幹部をはじめとした全ての職員等が情報セキュリティの重要性を認識し、ポリシー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。

特に、緊急時対応計画の策定及び見直しを行い、ネットワーク管理者に緊急時対応計画に基づく訓練を実施させ、実際に情報資産の漏洩等の事故が発生した場合に即応できるように体制を整えなければならない。

(8)　情報セキュリティに関する統一的な窓口の設置

①　CISO は、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

②　CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

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

④　情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

3　情報資産の分類と管理方法

(1)　情報資産の分類

本町における情報資産は、次のとおり分類し必要に応じ取扱制限を行うものとする。

重要性分類		取扱制限
Ⅰ	個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報	・重要性分類Ⅰの情報資産については、私物端末での作業禁止 ・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
Ⅱ	公開することを予定していない情報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情報	
Ⅲ	外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に微妙な影響を及ぼす情報	
Ⅳ	上記以外の情報	

(2)　情報資産の管理

①　管理責任

ア　情報システム管理者は、その所管する情報資産について管理責任を有する。

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)、ヘッダー・フッター等)、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、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。

③　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　情報を作成する者は、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　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

ア　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。

イ　庁外の者が作成した情報資産を入手した者は、（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　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、情報システム管理者に判断を仰がなければならない。

⑤　情報資産の利用

ア　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。

イ　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。

ウ　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、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

ア　情報資産の分類に従って、情報資産を適切に保管しなければならない。

イ　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なければならない。

ウ　重要性分類Ⅱ以上の情報を記録した電磁的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。

⑦　情報の送信

ア　電子メール等により重要性分類Ⅱ以上の情報を送信する者は、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　電子メール等により重要性分類Ⅱ以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行うなど、情報資産の不正利用を防止するための措置を行わなければならない。

⑧　情報資産の運搬

ア　重要性分類Ⅱ以上の情報資産を運搬する者は、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　重要性分類Ⅱ以上の情報資産を運搬する者は、必要に応じ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

ア　重要性分類Ⅱ以上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に許可を得なければならない。

イ　重要性分類Ⅱ以上の情報資産を外部に提供する者は、必要に応じ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　住民に公開する情報資産については、完全性を確保しなければならない。

⑩　情報資産の廃棄

ア　重要性分類Ⅱ以上の情報資産を廃棄する者は、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。

ウ　情報資産の廃棄を行う者は、情報システム管理者の許可を得なければならない。

4　物理的セキュリティ

(1)　サーバ等の管理

①　サーバ等機器の取付け

ネットワーク管理者は、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　サーバの冗長化

ネットワーク管理者は、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、同一データを保持しなければならない。

③　機器の電源

ネットワーク管理者は、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。また、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。

④　通信ケーブル等の配線

ア　ネットワーク管理者は、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受けることがないように可能な限り必要な措置を講じなければならない。

イ　ネットワーク管理者は、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　ネットワーク管理者及び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　ネットワーク管理者及び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。

⑤　機器の定期保守及び修理

ア　ネットワーク管理者及び情報システム管理者は、所管する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　ネットワーク管理者及び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、ネットワーク管理者及び情報システム管理者は、外部の事業者に故障を修理させるにあたり、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などして、秘密保持体制の確認等を行わなければならない。

⑥　庁外への機器の設置

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。

⑦　機器の廃棄等

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)　管理区域の管理

①　管理区域の構造等

ア　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「電算室」という。）や電磁的記録媒体の保管庫をいう。

イ　ネットワーク管理者は、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、施錠等によって許可されていない立入りを防止しなければならない。

ウ　ネットワーク管理者は、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、防水措置等を講じなければならない。

②　管理区域の入退室管理等

ア　ネットワーク管理者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等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　職員等及び外部委託事業者は、管理区域に入室する場合、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　ネットワーク管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域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。

エ　ネットワーク管理者は、重要性分類Ⅱ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　ネットワーク管理者は、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　ネットワーク管理者は、電算室の機器等の搬入出について、職員を立ち会わせるものとする。

(3)　通信回線及び通信回線装置の管理

①　ネットワーク管理者は、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　ネットワーク管理者は、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。

④　ネットワーク管理者は、重要性分類Ⅱ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。

⑤　ネットワーク管理者は、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に十分なセキュリティ対策を実施しなければならない。

⑥　ネットワーク管理者は、重要性分類Ⅱ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)　職員等のパソコン等の管理

①　情報セキュリティ管理者は、情報システム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。

②　情報セキュリティ管理者は、取り扱う情報の重要度に応じてパスワード以外に指紋認証等の二要素認証を併用しなければならない。

5　人的セキュリティ

(1)　職員等の遵守事項

①　職員等の遵守事項

ア　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。

イ　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。

ウ　パソコン等の端末の持ち出し及び外部における情報処理作業の制限

（ア）　CISO は、重要性分類Ⅱ以上の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ）　職員等は、本町のパソコン等の端末、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、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）　職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

（エ）　職員等は、外部で情報処理作業を行う際、私物のパソコンを用いる場合には情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。また、重要性分類Ⅰ以上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。

エ　支給以外のパソコン等の端末及び電磁的記録媒体等の業務利用

（ア）　職員等は、支給以外のパソコン等の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、情報セキュリティ管理者の許可を得て利用することができる。

（イ）　職員等は、外部で情報処理作業を行う際、支給以外のパソコン等の端末及び電磁的記録媒体を用いる場合には、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。

オ　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、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

カ　パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、パソコン等の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。

キ　机上の端末等の管理

職員等は、パソコン等の端末、電磁的記録媒体及び情報が印刷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を閲覧されることがないように、離席時のパソコン等の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。

ク　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。

② 非常勤及び臨時職員への対応

ア　情報セキュリティポリシー等の遵守

情報システム管理者は、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　情報セキュリティポリシー等の遵守に対する同意

情報システム管理者は、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　インターネット接続及び電子メール使用等の制限

ネットワーク管理者は、非常勤及び臨時職員にパソコン等の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場合、これを利用できないようにしなければならない。

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掲示しなければならない。

④ 外部委託事業者に対する説明

ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、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。

(2) 研修・訓練

① 情報セキュリティに関する研修・訓練

上毛町情報化推進委員会は、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　上毛町情報化推進委員会は、幹部を含め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を構築しなければならない。

イ　情報セキュリティ管理者は、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。

③ 緊急時対応訓練

ネットワーク管理者は、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、また、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

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

(3)　情報セキュリティインシデントの報告

①　庁内からの情報セキュリティインシデントの報告

ア　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、速やかにネットワーク管理者及び情報システム管理者に報告しなければならない。

イ　報告を受けたネットワーク管理者は、速やかに統括情報セキュリティ責任者、情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

ウ　統括情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、必要に応じて CISO に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

ア　職員等は、本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、ネットワーク管理者及び情報システム管理者に報告しなければならない。

イ　報告を受けたネットワーク管理者は、速やか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しなければならない。

ウ　統括情報セキュリティ責任者は、当該情報セキュリティインシデントについて、必要に応じて CISO に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

ア　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、ネットワーク管理者、情報セキュリティインシデントを引き起こした部門の情報システム管理者及び情報セキュリティに関する統一的な窓口と連携し、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結果から、再発防止策を検討し、CISO に報告しなければならない。

イ　CISO は、統括情報セキュリティ責任者から、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。

(4)　ID 及びパスワード等の管理

①　IC カード等の取扱い

ア　職員等は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。

（ア）　認証に用いる IC カード等を、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、IC カード等をカードリーダ若しくはパソコン等の端末のスロット等から抜いておかなければならない。

（ウ）　IC カード等を紛失した場合には、速やかにネットワーク管理者及び情報システム管理者に通報し、指示に従わなければならない。

イ　ネットワーク管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

ウ　ネットワーク管理者は、IC 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。

② ID の取扱い

職員等は、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 は、他人に利用させてはならない。

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

③ 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。

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。

エ　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、パスワードを速やかに変更しなければならない。

オ　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、古いパスワードを再利用してはならない。

カ　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

キ　仮のパスワードは、最初のログイン時点で変更しなければならない。

ク　パソコン等の端末にパスワードを記憶させてはならない。

ケ　職員等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

ア　ネットワーク管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。

イ　ネットワーク管理者は、ファイルサーバを課室等の単位で構成し、職員等が他課室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。

ウ　ネットワーク管理者は、住民の個人情報、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、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、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、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、その重要度に応じて期間を定め、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。

③ 組織間との情報システムに関する情報等の交換

組織間において、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、ネットワーク管理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

ア ネットワーク管理者及び情報システム管理者は、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 ネットワーク管理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。

ウ ネットワーク管理者、情報システム管理者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がシステム変更等の作業を行う場合は、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

ネットワーク管理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、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

ア ネットワーク管理者及び情報システム管理者は、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。

イ ネットワーク管理者及び情報システム管理者は、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 ネットワーク管理者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、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点検又は分析を実施しなければならない。

⑦ 障害記録

ネットワーク管理者及び情報システム管理者は、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。

⑧ ネットワークの接続制御、経路制御等

ア ネットワーク管理者は、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　ネットワーク管理者は、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

ネットワーク管理者及び情報システム管理者は、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、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た上で、CISO、統括情報セキュリティ責任者及びネットワーク管理者の許可を得なければならない。

イ　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。

ウ　ネットワーク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。

エ　ネットワーク管理者及び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、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。

⑪　複合機のセキュリティ管理

ア　ネットワーク管理者及び情報システム管理者は、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　ネットワーク管理者及び情報システム管理者は、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　ネットワーク管理者及び情報システム管理者は、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

ネットワーク管理者及び情報システム管理者は、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。

⑬　無線 LAN 及びネットワークの盗聴対策

ネットワーク管理者は、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。

⑭　電子メールのセキュリティ管理

ア　ネットワーク管理者は、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　ネットワーク管理者は、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しなければならない。

ウ　ネットワーク管理者は、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。

エ　ネットワーク管理者は、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。

⑮　電子メールの利用制限

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、情報システム管理者に報告しなければならない。

オ　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　電子署名・暗号化

ア　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、定められた電子署名、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。

イ　職員等は、暗号化を行う場合に、定められた以外の方法を用いてはならない。また、定められた方法で暗号のための鍵を管理しなければならない。

⑰　無許可ソフトウェアの導入等の禁止

ア　職員等は、パソコン等の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、ネットワーク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。

ウ　職員等は、導入したソフトウェアのライセンスを管理しなければならない。

エ　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。

⑱　機器構成の変更の制限

職員等は、パソコン等の端末に対し機器の改造、増設及び交換を行ってはならない。ただし、業務上、必要がある場合には、ネットワーク管理者の許可を得て、パソコン等の端末に対し機器の改造、増設及び交換を行うことができる。

⑲　無許可でのネットワーク接続の禁止

職員等は、ネットワーク管理者の許可なくパソコン等の端末を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

ア　職員等は、本町の情報システムにおいて、業務以外の目的でウェブを閲覧してはならない。

イ　情報システム管理者は、本町の情報システムにおいて、職員等のウェブ利用する場合に、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、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)　アクセス制御

①　アクセス制御

ア　アクセス制御等

ネットワーク管理者又は情報システム管理者は、所管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等がアクセスできないように、システム上制限しなければならない。

イ　利用者 ID の取扱い

（ア）　ネットワーク管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 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、ネットワーク管理者又は情報システム管理者に通知しなければならない。

（ウ）　ネットワーク管理者は、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

（ア）　ネットワーク管理者は、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）　ネットワーク管理者の特権を代行する者は、ネットワーク管理者が指名した者でなければならない。

（ウ）　ネットワーク管理者は、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。

（エ）　ネットワーク管理者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（オ）　ネットワーク管理者は、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

ア 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にアクセスする場合は、ネットワーク管理者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

イ ネットワーク管理者は、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者に限定しなければならない。

ウ ネットワーク管理者は、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。

エ ネットワーク管理者は、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。

オ ネットワーク管理者は、外部からのアクセスに利用するパソコン等の端末等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。

カ 職員等は、外部から持ち込み、又は持ち帰ったパソコン等の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。

③ パスワードに関する情報の管理

ア ネットワーク管理者は、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。

イ ネットワーク管理者は、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) システム開発、導入、保守等

① 情報システムの調達

ア ネットワーク管理者及び情報システム管理者は、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 ネットワーク管理者及び情報システム管理者は、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） ネットワーク管理者及び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。

（イ）　ネットワーク管理者及び情報システム管理者は、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。

（ウ）　ネットワーク管理者及び情報システム管理者は、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）　ネットワーク管理者及び情報システム管理者は、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）　ネットワーク管理者及び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）　ネットワーク管理者及び情報システム管理者は、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）　開発したシステムについて受け入れテストを行う場合、ネットワーク管理者及び情報システム管理者は、それぞれ独立したテストを行わなければならない。

③　システム開発・保守に関連する資料等の整備・保管

ア　ネットワーク管理者及び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　ネットワーク管理者及び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。

ウ　ネットワーク管理者及び情報システム管理者は、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。

④　情報システムにおける入出力データの正確性の確保

ア　ネットワーク管理者及び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に情報システムを設計しなければならない。

イ　ネットワーク管理者及び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に情報システムを設計しなければならない。

ウ　ネットワーク管理者及び情報システム管理者は、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。

⑤　情報システムの変更管理

ネットワーク管理者及び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。

⑥　開発・保守用のソフトウェアの更新等

ネットワーク管理者及び情報システム管理者は、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。

⑦　システム更新又は統合時の検証等

ネットワーク管理者及び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。

(4)　不正プログラム対策

①　ネットワーク管理者の措置事項

ネットワーク管理者は、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。

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。

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。

ウ　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。

エ　所掌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ェアを常駐させなければならない。

オ　不正プログラム対策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。

カ　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。

キ　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。

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。

ア　情報システム管理者は、その所掌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ェアをシステムに常駐させなければならない。

イ　不正プログラム対策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。

ウ　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。

エ　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、本町が管理している媒体以外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。

③　職員等の遵守事項

職員等は、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。

ア　パソコン等の端末において、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、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。

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、速やかに削除しなければならない。

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　ネットワーク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。

キ　コンピュータウイ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。

(5)　不正アクセス対策

①　措置事項

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。

ア　ネットワーク管理者は、使用されていないポートを閉鎖しなければならない。

イ　ネットワーク管理者は、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　ネットワーク管理者は、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、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定しなければならない。

エ　情報セキュリティ管理者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切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

CISO 及び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。また、関係機関と連絡を密にして情報の収集に努めなければならない。

③　記録の保存

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が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）に違反等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

ネットワーク管理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

ネットワーク管理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、適切な処置を求めなければならない。

⑥　サービス不能攻撃

ネットワーク管理者は、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

ネットワーク管理者及び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、教育や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

ネットワーク管理者及び情報セキュリティ管理者は、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、ソフトウェア更新等の対策を実施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

ネットワーク管理者及び情報セキュリティ管理者は、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

ネットワーク管理者及び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、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

(1)　情報システムの監視

①　ネットワーク管理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検知するため、情報システムを常時監視するよう努めなければならない。

②　ネットワーク管理者及び情報システム管理者は、重要なログ等を取得する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　ネットワーク管理者及び情報システム管理者は、外部と常時接続するシステムを常時監視するよう努めなければならない。

(2)　情報セキュリティポリシーの遵守状況の確認

①　遵守状況の確認及び対処

ア　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 CISO 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。

イ　CISO 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。

ウ　ネットワーク管理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　パソコン等の端末及び電磁的記録媒体等の利用状況調査

CISO 及び CISO 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等の端末及び電磁的記録媒体等のログ、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

ア　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報システム管理者に報告を行わなければならない。

イ　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判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

(3)　侵害時の対応等

①　緊急時対応計画の策定

CISO は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により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、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

②　緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

ア　関係者の連絡先
イ　発生した事案に係る報告すべき事項
ウ　発生した事案への対応措置
エ　再発防止措置の策定

③　緊急時対応計画の見直し

CISO 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。

(4)　例外措置

①　例外措置の許可

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、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

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可避のときは、事後速やかに CISO に報告しなければならない。

(5)　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 12 月 13 日法律第 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 5 月 30 日法律第 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　上毛町個人情報保護条例（平成 17 年 10 月 11 日条例第 14 号）
⑦　上毛町特定個人情報保護条例（平成 27 年 10 月 1 日条例第 16 号）

(6)　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。

① 情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかにネットワーク管理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システムを使用する権利を停止

あるいは剥奪することができる。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剥奪した旨を CISO、ネットワーク管理者及び当該職員等が所属する課室等の情報システム管理者に通知しなければならない。

8　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、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要件を明記した契約を締結しなければならない。

・情報セキュリティポリシーの遵守
・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
・提供されるサービスレベルの保証
・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
・外部委託事業者の従業員に対する教育の実施
・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
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・町による監査、検査
・町による情報セキュリティインシデント発生時の公表
・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、必要に応じ、②の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて CISO に報告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　約款による外部サービスの利用に係る規定の整備

ア　情報セキュリティ管理者は、以下を含む約款による外部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。また、当該サービスの利用において、重要性分類

Ⅱ以上の情報が取扱われないように規定しなければならない。

（ア）　約款によるサービスを利用してよい範囲

（イ）　業務により利用する約款による外部サービス

（ウ）　利用手続及び運用手順

② 約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、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約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

(3) ソーシャルメディアサービスの利用

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。

① 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行うこと。

② 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（IC カード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

③ 重要性分類Ⅱ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。

④ 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。

9 評価・見直し

(1) 監査

① 実施方法

情報セキュリティ監査統括責任者は上毛町長をもって充て、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、必要に応じて監査を行わせることができるものとする。

② 監査を行う者の要件

ア　上毛町情報化推進委員会は、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、監査の実施を依頼するものとする。

イ　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とする。

③ 監査実施計画の立案及び実施への協力

ア　上毛町情報化推進委員会は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ監査統括責任者の承認を得なければならない。

イ　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

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託

事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を必要に応じて行わせることができるものとする。

⑤　報告

上毛町情報化推進委員会は、監査結果を取りまとめ、情報セキュリティ監査統括責任者に報告する。

⑥　保管

上毛町情報化推進委員会は、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。

⑦　監査結果への対応

情報セキュリティ監査統括責任者は、監査結果を踏まえ、指摘事項を所管する情報システム管理者に対し、当該事項への改善計画作成の指示をしなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

⑧　情報セキュリティポリシー及び関係規程等の見直し等への活用

上毛町情報化推進委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、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。

(2)　自己点検

①　実施方法

ア　ネットワーク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について、必要に応じて自己点検を実施するものとする。

イ　情報システム管理者は、所管する部局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、必要に応じて自己点検を実施するものとする。

②　報告

ネットワーク管理者及び情報システム管理者は、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、上毛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

ア　職員等は、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。

イ　上毛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及び関係規程等の見直し、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。

(3)　情報セキュリティポリシー及び関係規程等の見直し

上毛町情報化推進委員会は、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ふまえ、情報セキュリティポリシー及び関係規程等

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、改善を行うものとする。

情報セキュリティ緊急時対応計画

1　目的

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、情報セキュリティポリシーの違反等により情報資産に対する重大な侵害事案が発生した場合に、迅速かつ適切に被害の拡大防止、迅速な復旧等を図るため、必要な対応について定めることを目的とする。

2　連絡先

情報セキュリティに関する侵害事案が発生した場合の主な連絡先は次に掲げるとおりとする。

① 上毛町長
② 最高情報セキュリティ責任者（以下「CISO」という。）
③ 統括情報セキュリティ責任者
④ ネットワーク管理者
⑤ 情報セキュリティ管理者
⑥ 情報システム管理者
⑦ 情報セキュリティに関する統一的な窓口
⑧ ネットワーク及び情報システムに係る外部委託事業者
⑨ 福岡県の関係部局
⑩ 警察及び関係機関
⑪ 被害を受けるおそれのある個人及び法人

3　発生した事案に係る報告すべき事項

(1) 情報セキュリティに関する事案を発見した者は、次に掲げる項目について速やかにネットワーク管理者及び情報システム管理者に報告しなければならない。

① 事案の状況
② 事案が発生した原因として、想定される行為
③ 確認した被害及び影響範囲（事案の種類、損害規模、復旧に要する額等）
④ 記録

(2) 報告を受けたネットワーク管理者は、当該事案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判断した場合は、速やかに統括情報セキュリティ責任者、情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。また、事案の詳細な調査を行うとともに、CISO に報告しなければならない。

4　発生した事案への対応措置

(1)　ネットワーク管理者は、次に掲げる事案の区分に応じ、当該各事案に定められた連絡先へ連絡しなければならない。

①　サイバーテロその他情報資産及び住民に重大な被害が生じるおそれのあるとき。

・上毛町長、CISO、福岡県の関係部局、警察及び影響が考えられる個人及び法人

②　不正アクセスその他犯罪と思慮されるとき及び犯罪利用の中継地点に利用され、他者に被害を与えるおそれがあるとき。

・上毛町長、CISO、福岡県の関係部局及び警察

③　情報システムに関する被害が発生したとき。

・当該情報システムを所管する情報システム管理者及び必要と認められる事業者

④　上記に掲げるもののほか情報資産に係る被害が発生したとき。

・関係部局等

(2)　ネットワーク管理者は、次の事案が発生し、情報資産を保護するためにネットワークを切断することがやむを得ない場合は、ネットワークを切断する。

①　異常なアクセスが継続しているとき又は不正アクセスが判明したとき。

②　システムの運用に著しい支障をきたす攻撃が継続しているとき。

③　コンピュータウィルス等の不正プログラムがネットワーク経由で拡がっているとき。

④　情報資産に係る重大な被害が想定されるとき。

(3)　ネットワーク管理者及び情報システムを所管する情報システム管理者は、次に掲げる事案が発生し、情報資産の防護のために情報システムを停止することがやむを得ない場合は、情報システムを停止する。

①　コンピュータウィルス等の不正プログラムが情報資産に深刻な被害を及ぼしているとき

②　災害等により電源を供給することが危険又は困難なとき。

③　上記に掲げるもののほか情報資産に係る重大な被害が想定されるとき。

(4)　個々のパソコン等の端末のネットワークからの切断については、セキュリティポリシーにおいて特段の定めがあるものを除き、ネットワーク管理者の許可が必要である。ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合は、事後報告とすることができる。

(5)　ネットワーク管理責任者及び情報システムを所管する情報システム管理者は、事案に係るシステムの各種ログ及び現状を保存する。

(6)　ネットワーク管理者及び情報システムを所管する情報システム管理者は、事案に対処した経過を記録する。

(7)　ネットワーク管理者及び情報システムを所管する情報システム管理者は、事案に係る証拠保全の措置を講じるとともに、再発防止のための暫定措置を検討及び実施した後、情報システムを復旧する。

(8)　ネットワーク管理者及び情報システムを所管する情報システム管理者は、復旧後、必要と認められる期間、再発の監視を行う。

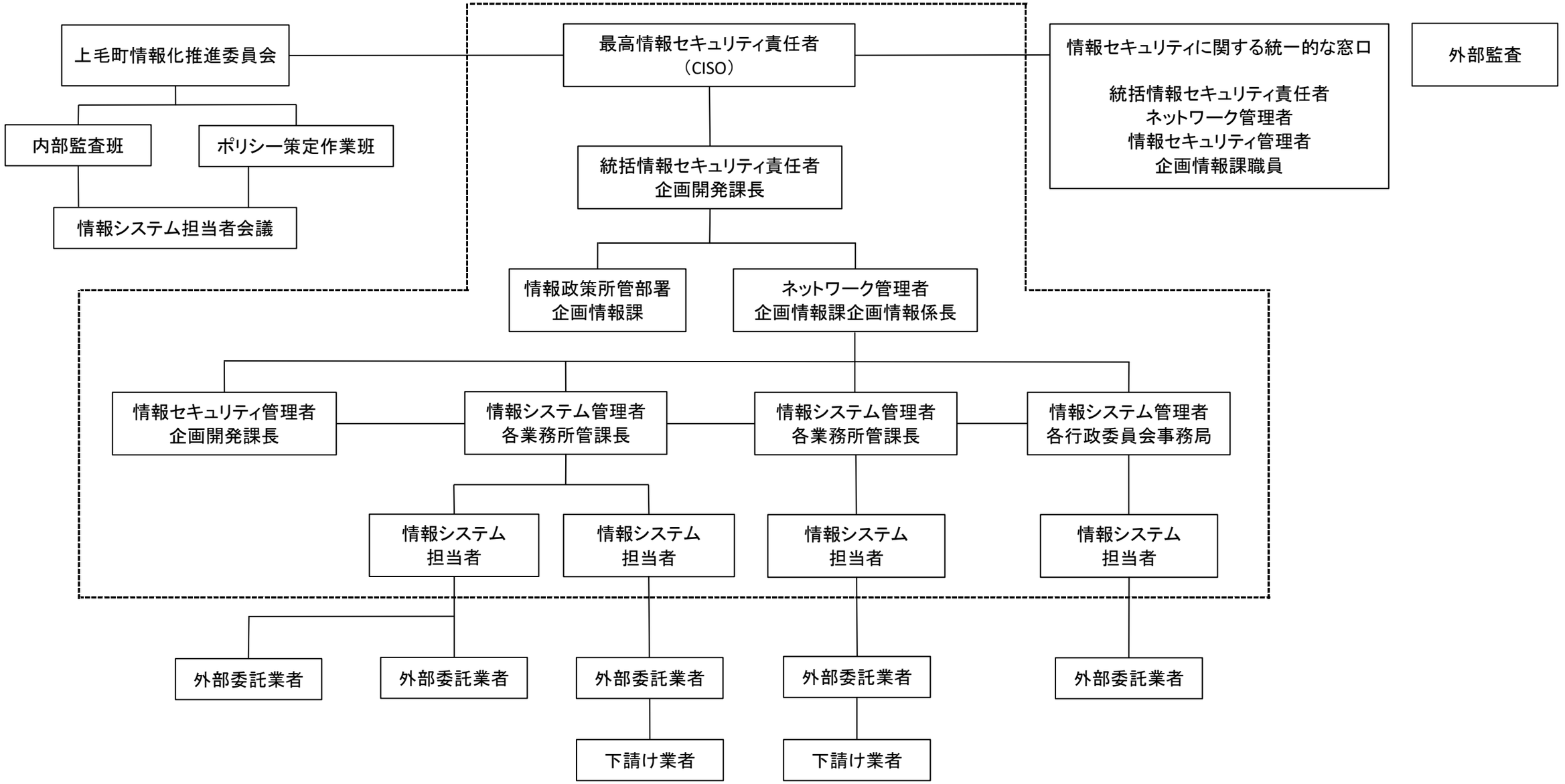
5　再発防止措置の策定

(1)　統括情報セキュリティ責任者は、当該事案に係る調査を実施し、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改善を含め、再発防止計画を策定し、CISO に報告するものとする。

(2)　CISO は、再発防止計画が有効であると認めた場合は、これを承認し、事案の概要と併せて職員等に周知するものとする。

別紙　上毛町情報セキュリティ管理体制（組織）図

最高情報セキュリティ責任者（CISO）	副町長
統括情報セキュリティ責任者	企画開発課長
ネットワーク管理者	企画情報係長
情報セキュリティ管理者	企画情報課長
情報システム管理者	各業務所管課長（同等程度の職責を負う職員）
情報システム担当者	各課職員１名以上
上毛町情報化推進委員会	



上毛町情報セキュリティポリシー　用語集

	用語	解説
あ	アクセス	コンピュータの資源やサービスを利用するために接続すること。端末等から直接アクセスする他に、ネットワーク越しに他のコンピュータと接続する場合もある。
	アクセス権限	コンピュータの利用者に与えられた、ハードディスクなどに保存されたファイルやフォルダ、あるいは接続された周辺機器等を利用する権限のこと。
	アクセス制御	ハードディスクなどに保存されたファイルやフォルダ、あるいは接続された周辺機器等に対し、許可された者以外の利用や、許可された方式以外での利用を防止すること。
	暗号化	インターネット等のネットワークを通じて文書や画像等のデジタルデータをやり取りする際に、通信途中で第三者に盗み見られたり、改ざんされたりされないよう、決まった規則に従ってデータを変換すること。なお、暗号化されたデータを元の状態に戻すことを復号という。
	インターネット	個人や企業、大学、行政機関等全世界のネットワークを電話回線や専用線で相互接続したコンピュータ・ネットワークのこと。平成 6 年に www が登場して以降、企業や家庭での利用が急増し、世界規模の情報通信基盤として発展を続けている。
	ウェブ	インターネット上で標準的に用いられる、文書の公開・閲覧システムのこと。
	ウェブページの改ざん	行政、企業などが運営する正規ウェブサイト内のコンテンツやシステムが、攻撃者によって意図しない状態に変更されてしまう攻撃のこと。
	オペレーティングシステム	キーボード入力や画面出力といった入出力機能やディスクやメモリの管理等、多くのアプリケーションソフトから共通して利用される基本的な機能を提供し、コンピュータシステム全体を管理するソフトウェアで、略して OS と呼ばれている。
か	カードリーダ	パソコンなどに接続してメモリカードや IC カードの読み書きを行う機器のこと。

	（情報システムの）外部委託	情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を外部の者に請け負わせること。
	外部からのアクセス	インターネット等を通じて庁外のネットワークから庁内のネットワークに接続すること。
	外部ネットワーク	インターネット等の庁外のネットワークのこと。
	可用性	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。情報システムに対する障害やセキュリティ侵犯があっても業務の継続性を確保すること。
	（情報システムの）監視	情報システムへの攻撃等を防ぐため、情報システムの稼働状況を監視すること。
	完全性	情報及び処理方法の正確さ及び完全である状態を安全防護すること。言い換えるならば、ハード、ソフト、データ等の正当性、正確性、整合性を脅かす脆弱性を制御して完全であることを確保すること。
	機密性	情報にアクセスを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。言い換えるならば、情報資産ごと適切なアクセス制御を行い、盗聴や不正アクセスによって情報が漏えいしないよう制御すること。
	緊急時対応訓練	実際に情報の漏えい等の情報セキュリティインシデントが発生した場合に即応できる態勢を構築しておくための緊急時を想定した訓練のこと。
	緊急時対応計画	情報セキュリティが侵害された場合又は侵害されるおそれがある場合等に備えて、あらかじめ実施すべき具体的な措置を定めた計画のこと。
	クラウドサービス	従来は利用者が手元のコンピュータで利用していたデータやソフトウェアを、ネットワーク経由で、サービスとして利用者に提供すること。
	ゲートウェイ	通信手段（プロトコル）が異なる二者間やネットワーク間の通信を中継する機器やソフトウェア、システムの一種で、最上位層のプロトコルの違いに対応できるものをいう。
	経路制御	複数のネットワークに接続しているホストコンピュータが受け取ったデータをどのネットワークを使って送るか決めること。ルーティングとも呼ばれている。

	個人情報	一般に、その情報によって、または他の情報と組み合わせることによって、個人を識別できる情報をいう。住所、氏名、電話番号、カード番号などが代表的である。個人情報が不用意に漏えいすると、予想もしない使われ方をされる危険があるため、個人情報の取り扱いには十分な注意を要する。
	コンピュータ	与えられた手順に従って複雑な計算を自動的に行う機械。特に、電子回路などを用いてデジタルデータの入出力、演算、変換などを連続的に行うことができ、詳細な処理手順を記述して与えることで、様々な用途に用いることができる電気機械のこと。
	コンピュータウィルス	不特定多数のコンピュータに、何らかの被害を与えることを目的に作成された不正プログラムのこと。ウィルスはインターネットから取得したファイル、他人から借りたUSBメモリ、電子メールを介して感染する。
さ	サーバ	コンピュータネットワークにおいて、他のコンピュータに対し、自身の持っている機能やサービス、データなどを提供するコンピュータのこと。
	サービス不能攻撃	DoS（Denial of Services attack）攻撃と呼ばれ、ウェブサーバやメールサーバなど、主にインターネット上のコンピュータ等に対して大量のデータや不正なデータを送りつけ、サーバの負荷を高めることによって処理を停止させたり、他の正当な利用者へのサービスを妨げたりすること。
	サイバー攻撃	コンピュータシステムやインターネット等を利用して、標的のコンピュータやネットワークに不正に侵入してデータの詐取、破壊、改ざん等を行い、標的のシステムを機能不全に陥らせること。
	時刻同期	サーバ間で時刻設定を自動的に合わせること。
	システムダウン	コンピュータシステムが予期せず動作停止状態になること。狭義には、アプリケーションソフトやOSが異常終了すること。システムダウンは、ハードウェアの損傷やソフトウェアの不具合、予想を超えた過大な処理要求、利用者の誤操作等の原因で発生する。
	自動再生無効化	CD-ROM、DVD、USBメモリ、外付けハードディスク、あるいはネットワークドライブなどをパソコン等の端末に挿入または接続したり、そのアイコンをダブルクリックし

		た際に、その中に格納されているソフトウェアや動画などを自動的に実行または再生する機能を無効にすること。
	自動転送機能	送られてきたメールを、設定した別のメールアドレスにそのまま転送する機能のこと。
	冗長化	最低限必要な量より多めに設備を用意しておき、一部の設備が故障してもサービスを継続して提供できるようにしておくこと。
	情報資産	ネットワーク、情報システム、これらに関する施設・設備、電磁的記録媒体、ネットワーク等で取り扱う情報及びシステム関連文書等のこと。
	情報システム	コンピュータ（ハードウェア、ソフトウェア及び電磁的記録媒体）やネットワークで構成され、特定の業務を処理するための仕組みをいう。
	情報セキュリティ	情報資産の機密性の保持及び正確性、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で、事故や人為的な不正行為等から情報資産の安全性や信頼性を確保すること。
	情報セキュリティインシデント	望まない単独もしくは一連の情報セキュリティ事象、又は予期しない単独もしくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確立及び情報セキュリティを脅かす確率が高いものをいう。
	スロット（IC カードスロット）	IC カード読み書きのためのカードの差込口のこと。
	スパムメール	受信者の都合を無視し、無差別に大量配信される迷惑メールのこと。
	生体認証	人の指紋や静脈等、個人の身体的特徴を用いて正当な利用者であることを認識することを生体認証という。認証に使用する身体的特徴は、指紋、静脈、手形、虹彩、声紋、顔、筆跡等があり、時間の経過によってあまり変化しないものが使われる。
	セキュリティホール	ソフトウェアの設計ミスや通信用機器及びコンピュータの設定ミス等によって生じた、システムのセキュリティ上の弱点のこと。
	ソーシャルメディアサービス	インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通等といった社会的な

		要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったウェブサイトやネットサービスなどを総称する用語で、電子掲示板やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄等を含む。
	ソースコード	プログラミング言語で記述されたテキストのこと。
	総合行政ネットワーク（LGWAN）	地方公共団体を相互に接続した行政専用のネットワークのことで、LGWAN(Local Government Wide Area Network)と呼ばれている。 LGWAN は、高度情報流通を可能とする通信ネットワークとして整備し、地方公共団体相互のコミュニケーションの円滑化、情報の共有による情報の高度利用を図ることを目的としており、行政事務の効率化や迅速化、重複投資の抑制、住民サービスの向上等を目指し、2001 年に創設されている。
	ソフトウェア	コンピュータを動作させる一連の手順・命令をコンピュータが理解できる形式で記述したもの。コンピュータを構成する電子回路や周辺機器などの物理的実態をハードウェアと呼ぶのに対して、形を持たない手順や命令等をソフトウェアと呼ぶ。
た	端末	情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいう。
	通信回線	情報を伝送する回線・ネットワークのこと。
	通信回線装置	通信回線に接続して、通信を行うための装置（ルータ等）のこと。
	電子署名	情報の正当性を保証するための電子的な署名情報をいう。
	特権を付与された ID	サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常の ID よりもシステムに対するより高いレベルでの操作が可能な ID をいう。
	特定用途機器	IP 電話システム、ネットワークカメラシステム、テレビ会議システム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているものをいう。

	ドメイン名	国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。
	二要素認証	二つの認証方式を組み合わせて認証する方式をいう。認証方式は大きく分けて、ID/パスワード等対象者の知識を利用したもの、USB トークンや IC カード等対象者の持ち物を利用したもの、生体認証等対象者の身体の特徴を利用したものの三つに分かれる。通常はこのうちどれか一つを利用して認証を行うが、それぞれ一長一短があり、単一の方法で精度を高めるには限界があるため、このうち二つの認証方式を組み合わせてセキュリティを高める方式である。
	ネットワーク	複数のコンピュータや周辺機器を通信媒体で結び、データの転送を行えるようにした通信網及びその構成機器のことをいう。
	ネットワークストレージサービス	インターネット上でデータやファイルを格納するディスクスペースを提供するサービスのことをいう。
	ハードウェア	コンピュータを構成している電子回路や周辺機器等の物理的実体のことをいう。
	パソコン	端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。
	パターンファイル	ウィルス対策ソフトがウィルスを発見するための参考とするファイルのことをいい、コンピュータウィルスに感染したファイルやネットワーク上で自己複製を繰り返すワームプログラムの特徴を収録している。
	バックアップ	コンピュータ等に記録されたデータファイルやシステムファイルを破損やウィルス感染等の事態に備え、別の電磁的記録媒体等に保存すること。
	パッチ	ソフトウェアのセキュリティ上の脆弱性を除去するプログラムのことをいう。
	ハブのポート	ネットワークで使われる集線装置をハブといい、コンピュータ機器に接続されたケーブルはハブに接続され、ハブを介して相互に通信する。ポートとはそのハブに用意された接続口を指す。

	標的型攻撃	明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。
	ファイアウォール	コンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システム等のことをいう。
	フィルタリング	一定の条件に基づいてデータ等を選別・排除する仕組みのことをいう。
	複合機	プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。複合機は、庁内ネットワークや公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。
	不正アクセス	情報や情報システムを利用する権限を持たない者がソフトウェアのセキュリティ上の弱点を悪用してアクセス権を取得し、地方公共団体等の内部のネットワーク外部から不正に侵入する行為をいう。
	不正プログラム	一般的には、コンピュータに害悪を及ぼすプログラムの総称のことで、マルウェアと同義である。
	フリーメール	インターネットを通じて無料で提供される電子メールサービスのこと。申し込めば無料で自分のメールアドレスを開設し、電子メールの送受信が行えるようになる。
ま	無線 LAN	無線を使って構築される LAN のことをいう。
	モバイル端末	端末のうち、業務上の必要に応じて移動させて使用する目的としたものをいい、端末の形態は問わない。
や	約款による外部サービス	有料、無料に関わらず、約款への同意及び簡易なアカウントの登録により利用可能なサービスをいい、代表例としては、電子メール、ファイルストレージ、グループウェア等のクラウドサービス等である。なお、電気通信サービスや郵便、運送サービス等は約款による外部サービス適用外となる。
ら	ログ	機器やソフトウェア、システムについて、その起動や停止、エラーや障害の発生、利用者による操作や設定の変更、外

		部との通信等、稼働中に起こった出来事の内容を日時等とともに時系列に記録したものをいう。
英	IC カード	薄い半導体集積回路（IC チップ）を埋め込み、情報を記録できるようにしたカードをいい、主に情報システムを利用する際の認証に用いられている。
	ID	ネットワークやコンピュータの利用者を識別するための記号（番号）をいう。
	LAN	ローカル・エリア・ネットワークの略で、同一建物内等限られた場所で複数のコンピュータを高速なデータ転送能力により相互接続したネットワークをいう。