取扱注意

幸田町情報セキュリティポリシー

令和６年５月１日　５．０版

愛知県幸田町

改版履歴

版　数	作成日
初　版	平成１５年　７月１７日
第２版	平成１９年　４月　１日
第３版	平成２７年１２月　１日
第４版	令和　４年　４月　１日
第５版	令和　６年　５月　１日

《目　　次》

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、幸田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、幸田町が所掌する情報資産に関する業務に携わる職員（町のすべての職員をいう。以下同じ。）及び外部委託事業者に浸透、普及及び定着をさせるものであり、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ものとする。

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をいう。
	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をいう。
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をいう。

第１章　情報セキュリティ基本方針

１　目的

情報セキュリティ基本方針（以下「基本方針」という。）は、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、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

次の各号に掲げる用語の意義は、それぞれ当該各号に定めるとおりとする。

⑴　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及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑵　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及び情報処理を行う仕組みをいう。

⑶　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。

⑷　情報セキュリティポリシー　基本方針及び情報セキュリティ対策基準をいう。

⑸　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。

⑹　完全性　情報が破壊し、改ざんし、又は消去されていない状態を確保することをいう。

⑺　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。

⑻　マイナンバー利用事務系（いわゆる「個人番号利用事務系」をいう。）　個人番号利用事務（社会保障、地方税又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。

⑼　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。）。

⑽　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。

⑾　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。

⑿　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、次の脅威を想定し、情報セキュリティ対策を実施する。

⑴　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい、破壊、改ざん又は消去、重要情報の詐取、内部不正等

⑵　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、設計又は開発の不備、プログラム上の欠陥、操作又は設定ミス、メンテナンス不備、内部又は外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい、破壊又は消去等

⑶　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

⑷　大規模又は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

⑸　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

⑴　行政機関の範囲　基本方針が適用される行政機関は、町長部局、各行政委員会、消防本部及び地方公営企業とし、各教育機関（事務室及び職員室を除く。）は対象外とする。この場合において、各教育機関における教育のために用いるネットワーク、システム等は、この情報セキュリティポリシーの対象となるネットワーク及び情報システムと物理的に分けなければならない。

⑵　情報資産の範囲　基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

5　職員の遵守義務

職員は、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

３の各号に掲げる脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

⑴　組織体制　町の情報資産について情報セキュリティ対策を推進する全庁的な組織体制を確立する。

⑵　情報資産の分類と管理　町の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

⑶　情報システム全体の強靭性の向上　情報システム全体に対し、次の３段階の対策を講じる。

ア　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。

イ　ＬＧＷＡＮ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。この場合において、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。

ウ　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。この場合において、高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

⑷　物理的セキュリティ　サーバ、情報システム室、通信回線及び職員のパソコン等の管理について物理的な対策を講じる。

⑸　人的セキュリティ　情報セキュリティに関し、職員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。

⑹　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。

⑺　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。この場合において、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、必要に応じ、インシデント対応フローの見直しを行う。

⑻　外部サービスの利用　外部委託をする場合には、外部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、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。

⑼　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、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、新たに対策が必要になった場合には、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

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。この場合において、情報セキュリティ実施手順は、公にすることにより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　情報セキュリティ対策基準

１　対象範囲

⑴　行政機関の範囲　情報セキュリティ対策基準（以下「対策基準」という。）が適用される行政機関は、町長部局、各行政委員会、消防本部及び地方公営企業とし、各教育機関（事務室及び職員室を除く。）は対象外とする。この場合において、各教育機関における教育のために用いるネットワーク及びシステム等は、この情報セキュリティポリシーの対象となるネットワーク及び情報システムと物理的に分けなければならない。

⑵　情報資産の範囲　対策基準が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

２　組織・体制

⑴　最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）　副町長をCISOとし、CISOは町における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

⑵　統括情報セキュリティ責任者

ア　企画部長を、CISO直属の統括情報セキュリティ責任者とし、統括情報セキュリティ責任者はCISOを補佐しなければならない。

イ　統括情報セキュリティ責任者は、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。

ウ　統括情報セキュリティ責任者は、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。

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

オ　統括情報セキュリティ責任者は、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。

カ　統括情報セキュリティ責任者は、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及び管理を行う権限及び責任を有する。

キ　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、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及び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。

ク　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。

ケ　統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

⑶　情報セキュリティ責任者

ア　町長部局の長、各行政委員会事務局の長、消防長及び地方公営企業の部局等の長を情報セキュリティ責任者とする。

イ　情報セキュリティ責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

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

エ　情報セキュリティ責任者は、その所管する部局等において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、情報セキュリティポリシーの遵守に関する意見の集約並びに職員に対する教育、訓練、助言及び指示を行う。

⑷　情報セキュリティ管理者

ア　町長部局の課室長、町長部局の出先機関の長、各行政委員会事務局の課室長、消防本部の課室長及び地方公営企業の課室長を情報セキュリティ管理者とする。

イ　情報セキュリティ管理者はその所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。

ウ　情報セキュリティ管理者は、その所掌する課室等において、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は、情報セキュリティ責任者、統括情報セキュリティ責任者及び CISO へ速やかに報告を行い、指示を仰がなければならない。

⑸　情報システム管理者

ア　各情報システムの担当課室長等を、当該情報システムに関する情報システム管理

者とする。

イ　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、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ　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。

エ　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維持及び管理を行う。

⑹　情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、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。

⑺　ＤＸ推進委員会

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、ＤＸ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策定等、情報セキュリティに関する重要な事項を審議する。この場合において、ＤＸ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、管理職をはじめとした全ての職員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、インシデント対応フローの見直しを行い、統括情報セキュリティ責任者にインシデント対応フロー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。

⑻　兼務の禁止

ア　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。

イ　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。

⑼　情報セキュリティに関する統一的な窓口の設置

ア　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から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。

イ　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。

ウ　CISO は、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、報道機関への通知又は公表の対応を行わなければならない。

エ　CISO は、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の方法

⑴　情報資産の分類

町における情報資産は、次に掲げる重要性分類に従って主管する情報資産を分類し、必要に応じ取扱制限を行うものとする。

重 要 性 分 類
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
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 ⅠからⅢまで以外の情報

重要性分類は、重要度の厳格度の高い順に**Ⅰ、Ⅱ、Ⅲ、Ⅳと表記する。本文書中で、重要性分類Ⅱ以上と表記する場合は**厳格順の高さを意味し重要性分類**ⅠⅡが該当する。**

⑵　情報資産の管理

ア　管理責任

（ア）　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。

（イ）　情報資産が複製し、又は伝送された場合には、当該複製し、又は伝送された情報資産も 第１号 の分類に基づき管理しなければならない。

イ　情報資産の分類の表示

職員は、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、必要に応じて情報資産の分類の表示及び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。

ウ　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）　情報を作成する者は、情報の作成時に 第１号の分類に基づき、当該情報の分類と取扱制限を必要に応じて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。この場合において、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。

エ　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、第1号の分類に基づき、当該情報の分類と取扱制限を必要に応じて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、必要に応じて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。

オ 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。

カ 情報資産の保管

（ア） 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） 情報セキュリティ管理者又は情報システム管理者は、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なければならない。

（ウ） 情報セキュリティ管理者又は情報システム管理者は、重要性分類Ⅱ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。

キ 情報の送信

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わなければならない。

ク 情報資産の運搬

（ア） 車両等により重要性分類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、容易に個人を特定できない措置を行う、追跡可能な移送手段を利用する等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ） 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。

ケ 情報資産の提供及び公表

（ア） 重要性分類Ⅱ以上の情報資産を外部に提供する者は、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。

（イ） 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。

（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。

コ　情報資産の廃棄

（ア）　情報資産の廃棄を行う者は、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、記録されている情報の機密性に応じ、電磁的記録媒体の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、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　情報システム全体の強靭性の向上

⑴　マイナンバー利用事務系

ア　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 アドレス等)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。この場合において、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、インターネット等から LGWAN-ASP を経由してマイナンバー利用事務系にデータの取り込みを可能とする。

イ　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、２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。この場合において、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。

ウ　マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本町の他の領域とはネットワークを分離しなければならない。

エ　マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度 5 を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービ

ス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

⑵ LGWAN 接続系

ア 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。この場合において、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

イ LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

⑶ インターネット接続系

ア 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。

イ 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。

5 物理的セキュリティ

⑴ サーバ等の管理

ア 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、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。

イ サーバの冗長化

（ア） 情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ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。

（イ） 情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

ウ　機器の電源

（ア） 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ための措置を講じなければならない。

エ　通信ケーブル等の配線

（ア） 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、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講じなければならない。

（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、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） 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） 統括情報セキュリティ責任者、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し、又は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。

オ　機器の定期保守及び修理

（ア） 情報システム管理者は、重要性分類Ⅱ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、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ほか、秘密保持体制の確認等を行わなければならない。

カ　庁外への機器の設置

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、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。この場合において、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。

キ　機器の廃棄等

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。個人番号若しくは特定個人情報ファイルを削除した場合又は電子媒体等を廃棄した場合には、削除し、又は廃棄した記録を保存する。この場合において、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認する。

⑵　管理区域（情報システム室等）の管理

ア　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、当該機器等の管理及び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。

（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、管理区域を地階又は１階に設けてはならない。

（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、鍵、監視機能、警報装置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。

（エ）　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。

（オ）　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、管理区域に配置する消火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。

イ　管理区域の入退室管理等

（ア）　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、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）　情報システム管理者は、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が付き添うものとし、外見上職員と区別できる措置を講じなければならない。

（エ）　情報システム管理者は、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、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。

ウ　機器等の搬入出

（ア）　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響についてあらかじめ職員又は委託した業者に確認を行わせなければならない。

（イ）　情報システム管理者は、情報システム室の機器等の搬入出について職員を立ち会わせなければならない。

⑶　通信回線及び通信回線装置の管理

ア　統括情報セキュリティ責任者は、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。この場合において、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。

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

ウ　統括情報セキュリティ責任者は、行政系のネットワークを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。

エ　統括情報セキュリティ責任者は、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。この場合において、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。

オ　統括情報セキュリティ責任者は、ネットワークに使用する回線について伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

カ　統括情報セキュリティ責任者は、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。この場合において、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。

⑷　職員の利用する端末や電磁的記録媒体等の管理

ア　情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末の使用時以外の施錠管理等の物理的措置を講じなければならない。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。

イ　情報システム管理者は、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。

ウ　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」又は「存在」を利用する認証手段のうち２つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。

6　人的セキュリティ

⑴　職員の遵守事項

ア　職員（会計年度任用職員以外の職員）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。この場合において、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）　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

a　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。

b　職員は、町のモバイル端末、電磁的記録媒体、情報資産又は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。

c　職員は、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）　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

職員は、支給以外のパソコン、モバイル端末、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、支給以外の端末の業務利用の可否判断を CISO が行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、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。

（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

職員は、パソコン、モバイル端末、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。

（ク） 退職時等の遵守事項

職員は、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。この場合において、その後も業務上知り得た情報を漏らしてはならない。

イ 職員のうち会計年度任用職員への対応

（ア） 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員が守るべき内容を理解し、実施し、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

情報セキュリティ管理者は、会計年度任用職員の採用の際、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

情報セキュリティ管理者は、会計年度任用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場合、これを利用できないようにしなければならない。

ウ 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。

エ 外部委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発、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。

⑵ 研修及び訓練

ア 情報セキュリティに関する研修及び訓練

CISO は、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。

イ 研修計画の策定及び実施

（ア） CISO は、幹部を含め全ての職員に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、ＤＸ推進委員会の承認を得なければならない。

（イ） 研修計画において、職員は必要に応じて情報セキュリティ研修を受講できるようにしなければならない。

（ウ） 新規採用の職員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。

（エ） 研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、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その他職員に対して、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。

（オ） 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。

（カ） 統括情報セキュリティ責任者は、研修の実施状況を分析及び評価をし、CISO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。

（キ） CISO は、毎年度１回、ＤＸ推進委員会に対して、職員の情報セキュリティ研修の実施状況について報告しなければならない。

ウ 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。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、効果的に実施できるようにしなければならない。

エ 研修及び訓練への参加

幹部を含めた全ての職員は、定められた研修及び訓練に参加しなければならない。

⑶ 情報セキュリティインシデントの報告

ア 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。

（イ） 報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者並びに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） 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てCISO及び情報セキュリティ責任者に報告しなければならない。

イ 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） 職員は、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。

（イ） 報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責

任者及び情報システム管理者に報告しなければならない。

（ウ）　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必要に応じてCISO及び情報セキュリティ責任者に報告しなければならない。

（エ）　CISOは、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るための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

ウ　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、情報セキュリティインシデントを引き起こした部門の情報セキュリティ管理者、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。この場合において、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、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。

⑷　ID及びパスワード等の管理

ア　ICカード等の取扱い

（ア）　職員は、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。

a　認証に用いるICカード等を職員間で共有してはならない。

b　業務上必要のないときは、ICカード等をカードリーダ又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。

c　ICカード等を紛失した場合には、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通報し、指示に従わなければならない。

（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、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）　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、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。

イ　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。

ウ　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） 複数の情報システムを扱う職員は、同一のパスワードをシステム間で用いてはならない。ただし、システム連携等している場合を除く。

（カ） 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。

（キ） サーバ、ネットワーク機器及び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。

（ク） 職員間でパスワードを共有してはならない。ただし、共有 ID に対するパスワードは除く。

7 技術的セキュリティ

⑴ コンピュータ及びネットワークの管理

ア 文書サーバの設定等

（ア） 情報システム管理者は、職員が使用できる文書サーバの容量を設定し、職員に周知しなければならない。

（イ） 情報システム管理者は、文書サーバを課室等の単位で構成し、職員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） 情報システム管理者は、住民の個人情報、人事記録等、特定の職員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が閲覧及び使用できないようにしなければならない。

イ バックアップの実施

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

ウ 他団体との情報システム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、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。

エ　システム管理記録及び作業の確認

（ア）　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）　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は、その作業の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）　統括情報セキュリティ責任者、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。

オ　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。

カ　ログの取得等

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

（イ）　統括情報セキュリティ責任者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）　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、取得したログを定期的に又は随時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。

キ　障害記録

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、職員からのシステム障害の報告、システム障害に対する処理の結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

ク　ネットワークの接続制御、経路制御等

（ア）　統括情報セキュリティ責任者は、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）　統括情報セキュリティ責任者は、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。

ケ　外部の者が利用できるシステムの分離等

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。

コ　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、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

（イ）　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、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。

（エ）　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、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

（オ）　情報システム管理者は、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。

サ　複合機のセキュリティ管理

（ア）　統括情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境及び取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

（イ）　統括情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

（ウ）　統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消し、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。

シ　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、利用の方法、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。

ス　無線 LAN 及びネットワークの盗聴対策

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

（イ） 統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

セ　電子メールのセキュリティ管理

（ア） 統括情報セキュリティ責任者は、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） 統括情報セキュリティ責任者は、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） 統括情報セキュリティ責任者は、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） 統括情報セキュリティ責任者は、職員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に周知しなければならない。

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

（カ） 統括情報セキュリティ責任者は、職員が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置しなければならない。

ソ　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、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。

（オ） 職員は、ウェブで利用できるフリーメール及び情報システム管理者が許可した、町指定以外の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。

タ　電子署名及び暗号化

（ア） 職員は、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、CISO が定めた電子署名、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） 職員は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。この場合において、CISO が定めた方法で暗号のための鍵を管理しなければならない。

（ウ） CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

チ　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、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。この場合において、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。

（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。

ツ　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、増設及び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、増設及び交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

テ　無許可でのネットワーク接続の禁止

職員は、統括情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

ト　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） 統括情報セキュリティ責任者は、職員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、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。

ナ　Web 会議サービスの利用時の対策

（ア） 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の手順を定めなければならない。

（イ） 職員は、町の定める利用の手順に従い、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。

（ウ） 職員は、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。

（エ） 職員は、外部から Web 会議に招待される場合は、町の定める利用の手順に従い、必要に応じて利用の申請を行い、承認を得なければならない。

ニ　ソーシャルメディアサービスの利用

（ア） 情報セキュリティ管理者は、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の手順を定めなければならない。

a 町のアカウントによる情報発信が、実際の町のものであることを明らかにするために、町の自己管理 Web 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。

b 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。

（イ） 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。

（ウ） 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。

（エ） 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。

（オ） 重要性分類Ⅱ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、町の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

（カ） ソーシャルメディアサービスの提供事業者が、「認証アカウント（公式アカウント）」の発行を行っている場合は、これを取得すること。

⑵ アクセス制御

ア アクセス制御

（ア） アクセス制御等

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、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

a 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、利用者の登録、変更、抹消等の情報管理、職員の異動及び出向、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。

b 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、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

c 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、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

a 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。

b 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、

統括情報セキュリティ責任者及び情報システム管理者が指名し、CISO が認めた者でなければならない。

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

d　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 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。

e　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 及びパスワードについて職員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。

f　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。

イ　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、統括情報セキュリティ責任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）　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）　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。

（エ）　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、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）　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。

（カ）　職員は、持ち込んだ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、コンピュータウイ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、情報セキュリティ管理者の許可を得てから接続しなければならない。

（キ）　統括情報セキュリティ責任者は、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、パスワード及び生体認証に係る情報等の認証情報並びにこれらを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、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。

ウ　自動識別の設定

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。

エ　ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定並びにログイン及びログアウト時刻の表示等により、正当なアクセス権を持つ職員がログインしたことを確認することができるようシステムを設定しなければならない。

オ　認証情報に関する情報の管理

（ア）　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、職員の認証情報に関する情報を厳重に管理しなければならない。認証情報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）　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。

（ウ）　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。

カ　特権による接続時間の制限

情報システム管理者は、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。

⑶　システム開発、導入、保守等

ア　情報システムの調達

（ア）　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）　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。

イ　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

情報システム管理者は、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。この場合において、システム開発のための規則を確立しなければならない。

（イ）　システム開発における責任者及び作業者の ID の管理

a　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。

b　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

a　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ェア及びソフトウェアを特定しなければならない。

b　情報システム管理者は、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。

ウ　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

a　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。

b　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及び保守計画の策定時に手順を明確にしなければならない。

c　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。

d　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

a　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。

b　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。

c　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。

d　情報システム管理者は、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。

エ　システム開発及び保守に関連する資料等の整備・保管

（ア）　情報システム管理者は、システム開発及び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及び保管をしなければならない。

（イ）　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）　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。

オ　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）　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）　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。

カ　情報システムの変更管理

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。

キ　開発・保守用のソフトウェアの更新等

情報システム管理者は、開発及び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。

ク　システムの更新又は統合時の検証等

情報システム管理者は、システムの更新又は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又は統合後の業務運営体制の検証を行わなければならない。

⑷　不正プログラム対策

ア　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。

（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。

イ 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、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。この場合において、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。

（オ） 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に当該権限を付与してはならない。

ウ 職員の遵守事項

職員は、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、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。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。

(カ) 統括情報セキュリティ責任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、次の対応を行わなければならない。

a 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。

b 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。

エ 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、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。

⑸ 不正アクセス対策

ア 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、不正アクセス対策として、次の事項を措置しなければならない。

(ア) 使用され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し、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) 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、監視、通知、外部連絡窓口その他適切な対応等を実施できる体制及び連絡網を構築しなければならない。

イ 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。この場合において、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。

ウ 攻撃への対処

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た場合又は攻撃を受けるリスクがある場合は、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。この場合において、総務省、都道府県等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。

エ 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。

オ　内部からの攻撃

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、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。

カ　職員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、職員による不正アクセスを発見した場合は、当該職員が所属する課室等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

キ　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。

ク　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。この場合において、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対策、侵入範囲の拡大の困難度を上げる対策及び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。

ケ　情報提供ネットワークシステム接続規程の遵守

個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守しなければならない。

⑹　セキュリティ情報の収集

ア　セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等

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。この場合において、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。

イ　不正プログラム等のセキュリティ情報の収集及び周知

統括情報セキュリティ責任者は、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に周知しなければならない。

ウ　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。この場合において、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。

8　運用

⑴　情報システムの監視

ア　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検知するため、情報システムを常時監視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、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。

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は、外部と常時接続するシステムを常時監視しなければならない。

エ　暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

⑵　情報セキュリティポリシーの遵守状況の確認

ア　情報セキュリティポリシー遵守状況の確認及び対処

（ア）　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 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）　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。

イ　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

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。

ウ　職員の報告義務

（ア）　職員は、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。

（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統括情報セキュリティ責任者が判断した場合は、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。

⑶ 侵害時の対応等

ア インシデント対応フロー

CISO又はＤＸ推進委員会は、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、証拠の保全、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、インシデント対応フローを定めておき、セキュリティ侵害時には当該フローに従って適切に対処しなければならない。

イ インシデント対応フローの見直し

CISO 又はＤＸ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、必要に応じてインシデント対応フローを見直さなければならない。

⑷ 例外措置

ア 例外措置の許可

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。

イ 緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、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。

ウ 例外措置の申請書の管理

CISO は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請の状況を確認しなければならない。

⑸ 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、次に掲げる法令等の規定のほか、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）

カ　サイバーセキュリティ基本法（平成 26 年法律第 104 号）

キ　幸田町個人情報保護条例（平成 17 年幸田町条例第３号）

⑹　懲戒処分等

ア　懲戒処分

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

イ　違反時の対応

職員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）　統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員が所属する課室等の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。

（イ）　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統括情報セキュリティ責任者及び当該職員が所属する課室等の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。

（ウ）　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し、又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、職員の権利を停止あるいは剥奪した旨を CISO 及び当該職員が所属する課室等の情報セキュリティ管理者に通知しなければならない。

9　外部委託

⑴　業務委託

ア　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、委託の内容に応じた情報セキュリティ対策（特定個人情報の取扱いがある場合の安全管理措置を含む）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等を参考にして、事業者を選定しなければならない。

イ　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。

（ア）　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

（イ） 外部委託事業者の責任者、委託内容、作業者及び作業場所の特定
（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及びアクセス方法
（オ） 外部委託事業者の従業員に対する監督及び教育の実施
（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） 提供された個人情報（特定個人情報を含む。）を取り扱う従業者の明確化
（ク） 業務上知り得た情報の守秘義務
（ケ） 再委託に関する制限事項の遵守
（コ） 委託業務終了時の情報資産の返還、廃棄等
（サ） 委託業務の定期報告及び緊急時報告義務
（シ） 町による監査又は検査（実地の監査又は検査を含む。）
（ス） 町による情報セキュリティインシデント発生時の公表
（セ） 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)

ウ 監督

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（特定個人情報の取扱いがある場合の安全管理措置を含む。）が確保されていることを定期的に確認し、必要に応じ、イの契約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。

エ 再委託

外部委託事業者は、町の許諾を得た場合に限り、再委託をすることができる。町は、再委託先において必要なセキュリティ対策（特定個人情報の取扱いがある場合の安全管理措置を含む。）が確保されていることを確認した上で再委託の諾否を判断しなければならない。この場合において、町は外部委託事業者に対する監督義務だけではなく、再委託先に対しても間接的に監督義務を負うこととなる。

⑵ 外部サービスの利用（重要性分類Ⅱ以上の情報を取り扱う場合）

ア 外部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、次に掲げる要件を含む外部サービス（重要性分類Ⅱ以上の情報を取り扱う場合）の利用に関する規定を必要に応じ整備すること。

（ア） 外部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「外部サービス利用判断基準」という。）
（イ） 外部サービス提供者の選定基準
（ウ） 外部サービスの利用の申請の許可権限者と利用の手続
（エ） 外部サービス管理者の指名と外部サービスの利用の状況の管理

イ 外部サービスの選定

（ア） 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、外部

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外部サービスの利用を検討すること。

（イ） 情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。この場合において、次に掲げる内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

a 外部サービスの利用を通じて町が取り扱う情報の外部サービス提供者における目的外利用の禁止

b 外部サービス提供者における情報セキュリティ対策の実施の内容及び管理体制

c 外部サービスの提供に当たり外部サービス提供者若しくはその従業員又は再委託先その他の者によって、町の意図しない変更が加えられないための管理体制

d 外部サービス提供者の資本関係、役員等の情報、外部サービスの提供が行われる施設等の場所並びに外部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

e 情報セキュリティインシデントへの対処方法

f 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

g 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

（ウ） 情報セキュリティ責任者は、外部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、外部サービス提供者の選定条件に含めること。

（エ） 情報セキュリティ責任者は、外部サービスの利用を通じて町が取り扱う情報の格付等を勘案し、必要に応じて次に掲げる内容を外部サービス提供者の選定条件に含めること。

a 情報セキュリティ監査の受入れ

b サービスレベルの保証

（オ） 情報セキュリティ責任者は、外部サービスの利用を通じて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外部サービス提供者を選定し、必要に応じて町の情報が取り扱われる場所及び契約に定める準拠法及び裁判管轄を選定条件に含めること。

（カ） 情報セキュリティ責任者は、外部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、外部サービス提供者の選定条件で求める内容を外部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町に提供し、町の承認を受けるよう、外部サービス提供者の選定条件に含めること。この場合において、外部サービス利用判断基準及

び外部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すること。

（キ） 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に応じてセキュリティ要件を定め、外部サービスを選定すること。この場合において、外部サービスのセキュリティ要件としてセキュリティに係る国際規格（ISO/IEC27001）等と同等以上の水準を求めること。

（ク） 情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部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ること。

a 外部**サービスに求める情報セキュリティ対策**

b 外部**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**

c 外部**サービスに求めるサービスレベル**

（ケ） 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、各種の認定又は認証制度（ISO/IEC27017 によるクラウドサービス分野における ISMS 認証の国際規格。ISMAP 又は ISMAP-LIU の管理基準を満たすことの確認や ISMAP 又は ISMAP-LIU クラウドサービスリスト等、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービスクラウドサービス提供者等のセキュリティに係る内部統制の保証報告書である SOC 報告書)等の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的かつ客観的に評価し、判断すること。

ウ 外部サービスの利用に係る調達及び契約

（ア） 情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定の基準及び条件並びに外部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ること。

（イ） 情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部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ること。

エ 外部サービスの利用承認

（ア） 情報セキュリティ責任者は、外部サービスを利用する場合には、利用の申請の許可権限者へ外部サービスの利用の申請を行うこと。

（イ） 利用の申請の許可権限者は、職員による外部サービスの利用の申請を審査し、利用の可否を決定すること。

（ウ） 利用の申請の許可権限者は、外部サービスの利用の申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

オ 外部サービスを利用した情報システムの導入、構築時の対策

（ア） 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、次を含む外部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必要に応じ規定すること。

a 不正なアクセスを防止するためのアクセス制御

b 取り扱う情報の機密性保護のための暗号化

c 開発時におけるセキュリティ対策

d 設計及び設定時の誤りの防止

（イ） 外部サービス管理者は、オ（ア）において定める規定に対し、構築時に実施状況を確認し、及び記録すること。

カ 外部サービスを利用した情報システムの運用及び保守時の対策

（ア） 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次に掲げる要件を含む外部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必要に応じ規定すること。

a 外部サービス利用方針の規定

b 外部サービス利用に必要な教育

c 取り扱う資産の管理

d 不正アクセスを防止するためのアクセス制御

e 取り扱う情報の機密性保護のための暗号化

f 外部サービス内の通信の制御

g 設計又は設定時の誤りの防止

h 外部サービスを利用した情報システムの事業継続

（イ） 情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部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すること。

（ウ） 外部サービス管理者は、（ア）及び（イ）において定める規定に対し、運用及び保守時に実施状況を定期的に確認し、及び記録すること。

キ 外部サービスを利用した情報システムの更改・廃棄時の対策

（ア） 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次に掲げる要件を含む外部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すること。

a 外部サービスの利用終了時における対策

b 外部サービスで取り扱った情報の廃棄

c 外部サービスの利用のために作成したアカウントの廃棄

（イ） 外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認し、及び記録すること。

⑶　外部サービスの利用（重要性分類Ⅱ以上の情報を取り扱わない場合）

ア　外部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、次に掲げる要件を含む外部サービス（重要性分類Ⅱ以上の情報を取り扱わない場合）の利用に関する規定を必要に応じ整備すること。

（ア）　外部サービスを利用可能な業務の範囲

（イ）　外部サービスの利用の申請の許可権限者と利用の手続

（ウ）　外部サービス管理者の指名と外部サービスの利用の状況の管理

（エ）　外部サービスの利用の運用手順

イ　外部サービスの利用における対策の実施

（ア）　職員は、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重要性分類Ⅱ以上の情報を取り扱わない場合の外部サービスの利用を申請すること。この場合において、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

（イ）　情報セキュリティ責任者は、職員による外部サービスの利用の申請を審査し、利用の可否を決定すること。この場合において、承認した外部サービスを記録すること。

１０　評価・見直し

⑴　監査

ア　実施方法

CISO は、情報セキュリティ監査統括責任者を指名し、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毎年度及び必要に応じて監査を行わせなければならない。

イ　監査を行う者の要件

（ア）　情報セキュリティ監査統括責任者は、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。

（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でなければならない。

ウ　監査実施計画の立案及び実施への協力

（ア）　情報セキュリティ監査統括責任者は、監査を行うに当たって監査実施計画を立案し、ＤＸ推進委員会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。

エ　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定期的に又は必要に応じて行わなければならない。

オ　報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、ＤＸ推進委員会に報告する。

カ　保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査の証拠及び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。

キ　監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。この場合において、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。この場合において、庁内で横断的に改善が必要な事項については、統括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。

ク　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

ＤＸ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。

⑵　自己点検

ア　実施方法

（ア）　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及び情報システムについて毎年度及び必要に応じて自己点検を実施しなければならない。

（イ）　情報セキュリティ責任者は、情報セキュリティ管理者と連携して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毎年度及び必要に応じて自己点検を行わなければならない。

イ　報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、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ＤＸ推進委員会に報告しなければならない。

ウ　自己点検結果の活用

（ア）　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。

（イ）　ＤＸ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。

⑶　情報セキュリティポリシー及び関係規程等の見直し

ＤＸ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踏まえ、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。