砥部町情報セキュリティポリシー

令和８年３月 31 日
訓令第３号
議会訓令第１号
教育委員会訓令第２号
選挙管理委員会訓令第１号
監査委員訓令第１号
農業委員会訓令第１号
固定資産評価審査委員会訓令第１号
企業管理規程第２号

砥部町情報セキュリティポリシーを次のように定める。

目次

第１章　総則

(趣旨)

第１条　この訓令は、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を定めるものとする。

２　第２章は、第１項の情報セキュリティ対策について、基本的な事項を定めるものとする。

３　第３章は、第２章に基づき、具体的な遵守事項、判断基準その他の事項を定めるものとする。

(定義)

第２条　この訓令において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　ネットワーク　コンピュータその他の機器を相互に接続するための通信網及びその構成機器(ソフトウエアを含む。)をいう。

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

(3)　サーバ　ネットワークで提供するコンピュータ処理を行い、ネットワークの中心となるコンピュータをいう。

(4)　ソフトウエア　コンピュータで動作するプログラム全般(周辺機器のためのドライバ類を含む。)をいう。

(5)　情報セキュリティ対策　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。

(6)　ポリシー　この訓令をいう。

(7)　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することができる状態をいう。
(8)　完全性　情報が破壊され、改ざんされ、又は消去されていない状態をいう。
(9)　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、情報にアクセスすることができる状態をいう。
(10)　職員等　本町が所掌する情報資産に関する業務に携わる正規職員及び会計年度任用職員をいう。
(11)　業務系　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をいう。)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。
(12)　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(業務系を除く。)。
(13)　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。
(14)　通信経路の分断　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することができるようにすることをいう。
(15)　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。
(16)　LAN　本庁及び出先機関のコンピュータ、プリンタその他の機器を接続し、通信回線を介して本庁電算機械室のサーバを利用するコンピュータネットワークをいう。
(17)　端末　職員等が使用するLANに接続されたパソコン及びモバイル端末をいう。
(18)　ID　LANを利用するために登録された利用者の符号をいう。
(19)　パスワード　機密保護のため、正式に登録された利用者であることを確認するための符号をいう。

(対象とする脅威)

第３条　情報資産に対する脅威として、次に掲げる事項を想定し、情報セキュリティ対策を実施するものとする。
(1)　部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃その他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、内部不正その他の事項
(2)　情報資産の無断持ち出し、無許可ソフトウエアの使用その他の規程違反並びにプログラム上の欠陥、操作及び設定ミス、メンテナンス不備、外部委託管理の不備、監査機能の不備、機器故障その他の非意図的要因による情報資産の漏えい、破壊、消去その他の事項
(3)　地震、落雷、火災その他の災害によるサービス、業務の停止その他の事項
(4)　大規模及び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、通信又は水道供給の途絶等のインフラの障害からの波及等

(適用範囲)

第４条　この訓令が適用される行政機関は、町長部局、議会、行政委員会(学校を除く。)及び地方公営企業とする。

２　この訓令が対象とする情報資産は、次に掲げるものとする。

(1)　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

(2)　ネットワーク及び情報システムで取り扱う情報並びにこれらを印刷した文書

(3)　情報システムの仕様書、ネットワーク図その他のシステム関連文書

第２章　情報セキュリティ基本方針

(職員等の遵守義務)

第５条　職員等は、情報セキュリティ対策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は、ポリシー及び第10条に規定する実施要領を遵守しなければならない。

(情報セキュリティ対策)

第６条　第３条に規定する脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講ずるものとする。

(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機密性、完全性及び可用性を踏まえた重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

(3)　情報セキュリティ対策の強化を目的とし、業務の効率性及び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ずる。

ア　業務系においては、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の分断を実施する。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。

ウ　インターネット接続系においては、高度な情報セキュリティ対策として、不正通信の監視機能の強化等並びに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、電算機械室、通信回線、職員等のパソコンその他の情報資産の管理について、物理的な対策を講ずる。

(5)　人的セキュリティ　情報セキュリティ対策に関し、職員等が遵守すべき事項を定めるとともに、十分な教育、啓発その他の人的な対策を講ずる。

(6)　技術的セキュリティ　コンピュータの管理、アクセス制御、不正プログラム対策、不正アクセス対策その他の技術的対策を講ずる。

(7)　運用　情報システムの監視、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その他の運用面の対策を講ずるとともに、情報資産への侵害その他の事

案が発生した場合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)　外部サービスの利用　外部サービスを利用する場合には、利用形態に応じて次の対策を講ずる。

ア　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ずる。

イ　約款による外部サービスを利用する場合には、利用に係る規程を整備し対策を講ずる。

ウ　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することが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。

(情報セキュリティ監査及び自己点検の実施)

第７条　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ものとする。

(ポリシーの見直し)

第８条　情報セキュリティ監査及び自己点検の結果、ポリシーの見直しが必要となった場合又は情報セキュリティ対策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、ポリシーを見直すものとする。

(対策基準の策定)

第９条　前３条に規定する対策その他の事項を実施するために、具体的な遵守事項、判断基準その他の事項を定める対策基準を策定するものとする。

(実施要領の策定)

第10条　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要領を定めた実施要領を策定するものとする。

(非公開)

第11条　前条に規定する実施要領は、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３章　情報セキュリティ対策基準

第１章　組織体制

(最高情報セキュリティ責任者)

第12条　副町長を、最高情報セキュリティ責任者(以下「最高責任者」という。)とする。

２　最高責任者は、本町における全てのネットワーク、情報システムその他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ものとする。

(統括情報セキュリティ責任者)

第13条　企画財政課長を、最高責任者直属の統括情報セキュリティ責任者(以下「統括責任者」という。)とする。

２　統括責任者は、最高責任者を補佐しなければならない。

３　統括責任者は、本町の全てのネットワーク及び情報システムにおける開発、設定の変

更、運用、見直しその他の行為の権限及び責任を有するものとする。

4　統括責任者は、本町の全てのネットワーク及び情報システム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ものとする。

5　統括責任者は、情報セキュリティ管理者及び情報システム担当者に対して、情報セキュリティ対策に関する指導及び助言を行う権限を有するものとする。

6　統括責任者は、本町の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、最高責任者の指示に従い、最高責任者が不在の場合には、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ものとする。

7　統括責任者は、本町の共通的なネットワーク、情報システム及び情報資産に関する砥部町情報セキュリティ実施要領(以下、「実施要領」という。)の維持及び管理を行う権限及び責任を有するものとする。

8　統括責任者は、緊急時の円滑な情報共有を図るため、最高責任者、統括責任者、情報セキュリティ管理者及び情報システム担当者を網羅する連絡体制を整備しなければならない。

9　統括責任者は、緊急時には最高責任者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。

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

(情報セキュリティ管理者)

第14条　町長部局の課長、町長部局の出先機関の長、議会事務局の局長、行政委員会事務局の課長、行政委員会の出先機関の長及び地方公営企業の課長を、情報セキュリティ管理者(以下「管理者」という。)とする。

2　管理者は、その所管する部署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ものとする。

3　管理者は、その所管する部署において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、統括責任者及び最高責任者へ速やかに報告を行い、指示を仰がなければならない。

(情報システム担当者)

第15条　統括責任者の指示に従い、情報システムの開発、設定の変更、運用、更新その他の作業を行う者を、情報システム担当者(以下「担当者」という。)とする。

(情報化推進委員会)

第16条　本町の情報セキュリティ対策を統一的に行うため、砥部町情報化推進委員会設置規程(平成17年砥部町訓令第35号)に規定する砥部町情報化推進委員会(以下「委員会」という。)において、ポリシーその他の情報セキュリティに関する重要な事項を決定するものとする。

(兼務の禁止)

第17条　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。

２　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。

第２節　情報資産の分類及び管理方法

(情報資産の分類)

第18条　本町における情報資産は、機密性、完全性及び可用性を踏まえ、次のとおり分類し、必要に応じて取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性3	行政事務で取り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	・支給以外の端末での作業の原則禁止(機密性3の情報資産に限る。) ・必要以上の複製及び配付の禁止 ・保管場所の制限及び保管場所への必要以上の電磁的記録媒体等の持込禁止 ・情報の送信時並びに情報資産の運搬時及び提供時における暗号化、パスワード設定及び鍵付きのケースへの格納 ・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
機密性2	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性1	機密性2又は機密性3の情報資産以外の情報資産	

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は行政事務の的確な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	・バックアップ及び電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁記録媒体の施錠可能な場所への保管
完全性1	完全性2の情報資産以外の情報資産	

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は行政事務の安定的な遂行に支障(軽微なものを除く。)を及ぼすおそれがある情報資産	・バックアップ及び電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁記録媒体の施錠可能な場所への保管
可用性1	可用性2の情報資産以外の情報資産	

(情報資産の管理責任)

第19条　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ものとする。

2　情報資産が複製され、又は伝送された場合には、当該情報資産も前条に規定する分類に基づき管理しなければならない。

(情報資産の分類の表示)

第20条　職員等は、情報資産について、必要に応じてフォルダ、ファイル、格納する記録媒体又は文書の隅に情報資産の分類を表示するとともに、必要に応じて取扱制限についても明示しなければならない。

(情報の作成)

第21条　職員等は、業務上必要のない情報を作成してはならない。

2　情報を作成する者は、情報の作成時に第18条に規定する分類に基づき、当該情報の分類及び取扱制限を定めなければならない。

3　情報を作成する者は、作成途上の情報について、紛失、流出その他の事故を防止しなければならない。

4　情報を作成する者は、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。

(情報資産の入手)

第22条　職員等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応じた取扱いをしなければならない。

2　職員等以外の者が作成した情報資産を入手した者は、第18条に規定する分類に基づき、当該情報の分類及び取扱制限を定めなければならない。

3　情報資産を入手した者は、入手した情報資産の分類が不明な場合、管理者に判断を仰がなければならない。

(情報資産の利用)

第23条　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

2　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

3　情報資産を利用する者は、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

いる場合は、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

(情報資産の保管)

第24条　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。

２　管理者又は統括責任者は、情報資産を記録した外部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。

３　管理者又は統括責任者は、機密性２以上、完全性２又は可用性２の情報を記録した外部記録媒体を保管する場合は、耐火及び耐熱を講じた施錠可能な場所に保管しなければならない。

(情報の送信)

第25条　電子メールにより機密性２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。

(情報資産の運搬)

第26条　機密性２以上の情報資産を外部へ運搬する者は、必要に応じて、鍵付きのケースへの格納、暗号化又はパスワードの設定その他の方法により、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。

２　機密性２以上の情報資産を外部へ運搬する者は、管理者に許可を得なければならない。

(情報資産の提供及び公開)

第27条　機密性２以上の情報資産を外部に提供する者は、必要に応じて暗号化又はパスワードの設定を行わなければならない。

２　機密性２以上の情報資産を外部に提供する者は、管理者に許可を得なければならない。

３　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。

(情報資産の廃棄等)

第28条　情報資産の廃棄、リース返却等を行う者は、情報を記録している記録媒体が不要になった場合は、記録されている情報の機密性に応じ、記録媒体の情報を復元できないように処置しなければならない。

２　情報資産の廃棄、リース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

３　情報資産の廃棄、リース返却等を行う者は、管理者の許可を得なければならない。

第３節　情報システム全体の強靭性の向上

(業務系の対策)

第29条　業務系と外部を通信できないようにしなければならない。

２　前項の規定について、業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アドレス及びIPアドレス)及びアプリケーションプロトコル(ポート番号)のレベルでの限定を行わなければならない。

３　業務系と外部との接続先について、インターネット等と接続してはならない。

４　前項の規定にかかわらず、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、LGWANを経由して、インターネット等と業務系との双方向通信でのデータの移送を可能とする。

５　業務系の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について、「知識」、「所持」及び「存在」を利用する認証手段のうち二つ以上を併用する認証(以下「多要素認証」という。)を利用しなければならない。

６　業務ごとに専用端末を設置するよう努めるものとする。

７　業務系端末においては、原則として、USBメモリ等の電磁的記録媒体による情報の持ち出しができないように設定しなければならない。

(LGWAN接続系とインターネット接続系の分離)

第30条　LGWAN接続系及びインターネット接続系は、両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メール及びデータを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。

(1)　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

(2)　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

(3)　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

(インターネット接続系の対策)

第31条　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及び対処並びにLGWANへの不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

２　都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁、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。

第４節　物理的セキュリティ

第１款　サーバ等の管理

(機器の取付け)

第32条　統括責任者は、サーバその他の機器の取付けを行う場合は、火災、水害、埃、振動、温度及び湿度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。

(機器の電源)

第33条　統括責任者は、施設管理部門と連携し、サーバその他の機器の電源について、停電その他の事故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。

２　統括責任者は、施設管理部門と連携し、落雷その他の災害又は事故による過電流に対して、サーバその他の機器を保護するための措置を講じなければならない。

(通信ケーブル等の配線)

第34条　統括責任者は、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。
2　統括責任者は、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その他の障害の報告があった場合は、連携して対応しなければならない。
3　統括責任者及び管理者は、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正に管理しなければならない。
4　統括責任者は、自ら又は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又は追加をすることができないように必要な措置を施さなければならない。

(機器の保守及び修理)

第35条　統括責任者は、可用性２のサーバその他の機器の保守を実施しなければならない。
2　統括責任者は、記憶媒体を内蔵する機器を外部の事業者に修理させる場合は、内容を消去した状態で行わせなければならない。ただし、内容を消去できない場合は、修理を委託する事業者の秘密保持体制の確認等を行うことにより、当該機器の修理を行わせることができる。

(敷地外への機器の設置)

第36条　統括責任者は、町の施設の敷地外にサーバその他の機器を設置する場合は、最高責任者の承認を得なければならない。
2　統括責任者は、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

(機器の廃棄等)

第37条　統括責任者は、機器を廃棄又はリース返却を行う場合は、専用のソフトウエアによる消去又は記憶媒体の物理的破壊により、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。

第２款　管理区域の管理

(管理区域の構造等)

第38条　ネットワークの基幹機器及び重要な情報システムの設置、管理及び運用を行うための部屋を管理区域とする。
2　統括責任者は、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。
3　統括責任者は、管理区域内のサーバその他の機器に、転倒及び落下の防止その他の耐震対策及び防火措置を講じなければならない。
4　統括責任者は、管理区域に配置する消火薬剤又は消防用設備が、機器及び記録媒体に影響を与えないようにしなければならない。

(管理区域の入退室管理等)

第39条　統括責任者は、管理区域への入退室を許可された者のみに制限し、指紋認証等の生体認証又はパスワードの認証による入退室管理を行わなければならない。
2　職員等及び外部委託事業者は、管理区域に入室する場合は、身分証明書その他の本人確認書類を携帯し、求めにより提示しなければならない。

(機器等の搬入出)

第40条　統括責任者は、搬入する機器その他の物品が既存の情報システムに与える影響について、あらかじめ正規職員又は委託した業者に確認を行わせなければならない。

２　統括責任者は、管理区域内の機器その他の物品の搬入出について、正規職員を立ち会わせなければならない。

第３款　通信回線及び通信回線装置の管理

(ネットワークのセキュリティ対策)

第41条　統括責任者は、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。

２　統括責任者は、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。

３　統括責任者は、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。

４　統括責任者は、機密性２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は、必要なセキュリティ水準を検討の上、適切な回線を選択するとともに、必要に応じて、送受信される情報の暗号化を行わなければならない。

５　統括責任者は、ネットワークを使用する回線について、伝送途上で情報の破壊、盗聴、改ざん又は消去が生じないように十分な情報セキュリティ対策を実施しなければならない。

６　統括責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

第４款　職員等の端末の管理

(端末及び記録媒体等の管理)

第42条　統括責任者は、情報システムへのログインに際し、パスワード、スマートカード又は生体認証等の認証情報の入力を必要とするように設定しなければならない。

２　統括責任者は、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、モバイル端末及び電磁的記録媒体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。

３　統括責任者は、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。

４　統括責任者は、業務系では多要素認証を行うよう設定しなければならない。

第５節　人的セキュリティ

第１款　職員等の遵守事項

(ポリシー等の遵守)

第43条　職員等は、ポリシー及び実施要領を遵守しなければならない。

２　職員等は、情報セキュリティ対策について不明な点又は遵守することが困難な点がある場合は、速やかに管理者に相談し、指示を仰がなければならない。

３　管理者は、会計年度任用職員に対し、採用時にポリシー及び実施要領のうち、会計年度任用職員が守るべき内容を理解させ、また実施させ、及び遵守させなければならない。

(業務以外の目的での使用の禁止)

第44条　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。

(端末等の持ち出し等)

第45条　最高責任者は、機密性２以上、完全性２及び可用性２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。

２　職員等は、本町のモバイル端末、記録媒体、情報資産及びソフトウエアを外部に持ち出す場合には、管理者の許可を得なければならない。

３　職員等は、外部で情報処理業務を行う場合には、管理者の許可を得なければならない。

(パソコン等の持込みの禁止)

第46条　職員等は、私物のパソコン及び記録媒体を庁舎内又は町の施設内に持ち込み、業務に使用してはならない。ただし、業務上必要な場合は、管理者の許可を得てこれらを持ち込むことができる。

(持ち出し及び持込みの記録)

第47条　管理者は、記録媒体の外部への持ち出し及び外部からの持ち込みについて、記録を作成し、保管しなければならない。

(セキュリティ設定変更の禁止)

第48条　職員等は、端末のソフトウエアに関するセキュリティ機能の設定を統括責任者の許可なく変更してはならない。

(机上の端末等の管理)

第49条　職員等は、端末、記録媒体及び情報が印刷された文書について、第三者に使用されること又は管理者の許可なく情報を閲覧されることがないように、離席時には端末のロックを行うとともに、記録媒体及び文書を容易に閲覧されない場所に保管する等、適切な措置を講じなければならない。

(退職時等の遵守事項)

第50条　職員等は、異動、退職その他の事由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。

２　職員等は、異動又は退職の後も業務上知り得た情報を漏らしてはならない。

(インターネット接続及び電子メール使用等の制限)

第51条　管理者は、会計年度任用職員に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その他の行為が不要の場合は、これを利用できないようにしなければならない。

(ポリシー等の掲示)

第52条　統括責任者は、職員等が常にポリシー及び実施要領を閲覧できるようにグループウエアに掲示しなければならない。

(外部委託事業者に対する説明)

第53条　管理者は、ネットワーク及び情報システムの開発、保守その他の業務を外部委託事業者に発注する場合は、外部委託事業者から再委託を受ける事業者も含めて、ポリシー及び実施要領のうち外部委託事業者が守るべき内容の遵守事項及びその機密事項を説明しなければならない。

第２款　研修及び訓練

(情報セキュリティ対策に関する研修及び訓練)

第54条　最高責任者は、定期的に情報セキュリティ対策に関する研修及び訓練を実施しなければならない。

(研修計画の立案及び実施)

第55条　最高責任者は、幹部を含め全ての職員等に対する情報セキュリティ対策に関する研修計画を定期的に立案しなければならない。

２　最高責任者は、新規採用の職員等を対象とする情報セキュリティ対策に関する研修を実施しなければならない。

３　研修は、統括責任者、管理者、担当者及びその他職員等に対して、それぞれの役割及び情報セキュリティ対策に関する理解度に応じたものにしなければならない。

４　最高責任者は、毎年度１回、委員会に対して、職員等の情報セキュリティ対策研修の実施状況について報告しなければならない。

(緊急時対応訓練)

第56条　最高責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。

２　訓練計画は、ネットワーク及び各情報システムの規模を考慮し、訓練実施の範囲を定め、また、効果的に実施できるようにしなければならない。

３　全ての職員等は、定められた研修及び訓練に参加しなければならない。

第３款　インシデントの報告

(庁内からのインシデントの報告)

第57条　職員等は、情報セキュリティ対策に関する事故、システム上の欠陥及び誤作動並びにそれらにつながりかねない事象(以下「インシデント」という。)を発見した場合は、速やかに管理者に報告しなければならない。

２　報告を受けた管理者は、速やかに統括責任者に報告しなければならない。

３　管理者は、報告のあったインシデントについて、必要に応じて最高責任者に報告しなければならない。

(住民等外部からのインシデントの報告)

第58条　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その他の情報資産に関するインシデントについて、外部から報告を受けた場合は、管理者に報告しなければならない。

２　報告を受けた管理者は、速やかに統括責任者に報告しなければならない。

３　管理者は、報告のあったインシデントについて、必要に応じて最高責任者に報告しなければならない。

(事故等の究明、記録及び再発防止等)

第59条　統括責任者は、報告されたインシデントの可能性について状況を確認し、インシデントであるかの評価を行わなければならない。

2　統括責任者は、インシデントであると評価した場合は、最高責任者に速やかに報告しなければならない。

3　統括責任者は、インシデントに関係する管理者に対し、被害の拡大防止を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

4　統括責任者は、これらのインシデントの原因を究明し、記録を保存しなければならない。また、インシデントの原因究明結果から、再発防止策を検討し、最高責任者に報告しなければならない。

5　最高責任者は、統括責任者から、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。

第４款　ID 及びパスワード等の管理

(ICカードの取扱い)

第60条　職員等は、自己の管理するICカードに関し、次の事項を遵守しなければならない。

(1)　業務上必要のないときは、ICカードをカードリーダ又は端末のスロットから抜いておかなければならない。

(2)　ICカードを紛失した場合には、速やかに管理者に通報し、指示に従わなければならない。

2　管理者は、ICカードの紛失その他の事案の通報があり次第、当該ICカードを使用したアクセスを速やかに停止しなければならない。

3　管理者は、ICカードを切り替える場合は、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。

(IDの取扱い)

第61条　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。

(1)　自己が利用しているIDは、他人に利用させてはならない。

(2)　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。

(パスワードの取扱い)

第62条　職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

(1)　パスワードを秘密にし、パスワードの照会には、一切応じてはならない。

(2)　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。

(3)　パスワードが流出したおそれがある場合には、統括責任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。

(4)　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。

(5)　暫定パスワードは、最初のログイン時点で変更しなければならない。

(6)　端末のパスワードの記憶機能を利用してはならない。
(7)　共用システムを除いて、職員等間でパスワードを共有してはならない。

第６節　技術的セキュリティ

第１款　コンピュータ及びネットワークの管理

(ファイルサーバの設定等)

第63条　統括責任者は、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。

２　統括責任者は、ファイルサーバを課、事務局その他の部署の単位で構成し、職員等が他の部署のフォルダ及びファイルを閲覧及び使用をすることができないように、設定しなければならない。

３　統括責任者は、住民の個人情報又は特定の職員等のみが取り扱う人事記録その他のデータについて、同一部署であっても、担当職員以外の職員等が閲覧及び使用をすることができないようにしなければならない。

４　職員等は、やむを得ない場合を除き、端末で作成した情報を、ファイルサーバに保管しなければならない。

(バックアップの実施)

第64条　統括責任者は、ファイルサーバその他の機器に記録された情報について、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。

(他団体との情報システムに関する情報等の交換)

第65条　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エアを交換する場合は、その取扱いに関する事項をあらかじめ定め、統括責任者の許可を得なければならない。

(システム管理記録)

第66条　統括責任者は、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。

２　統括責任者は、所管するシステムにおいて、システム変更その他の作業を行った場合は、作業内容について記録を作成し、窃取又は改ざんをされないように適切に管理しなければならない。

(情報システム仕様書等の管理)

第67条　統括責任者は、ネットワーク構成図又は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の閲覧又は紛失がないよう、適切に管理しなければならない。

(アクセス記録等の取得等)

第68条　統括責任者は、各種アクセス記録及び情報セキュリティの確保に必要な記録(以下「アクセス記録等」という。)を取得し、７年間保存しなければならない。

２　統括責任者は、アクセス記録等が窃取、改ざん又は誤消去をされないように必要な措置を講じなければならない。

３　統括責任者は、システムから自動出力したアクセス記録等について、必要に応じて、

外部記録媒体にバックアップしなければならない。

(障害記録)

第69条　統括責任者は、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、システム障害に対する問題その他の事項を、障害記録として記録し、適切に保存しなければならない。

(ネットワークの接続制御及び経路制御等)

第70条　統括責任者は、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、ルータその他の機器の通信ソフトウエアを設定しなければならない。

２　統括責任者は、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。

(外部の者が利用できるシステムの分離)

第71条　統括責任者は、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、必要に応じて他のネットワーク及び情報システムと物理的又は論理的に分離する措置を講じなければならない。

(外部ネットワークとの接続制限等)

第72条　統括責任者は、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、最高責任者の許可を得なければならない。

２　統括責任者は、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、セキュリティ技術その他の事項を詳細に調査し、庁内の全てのネットワーク、情報システムその他の情報資産に影響が生じないことを確認しなければならない。

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

４　統括責任者は、ウェブサーバ、メールサーバその他のサーバをインターネットに公開する場合は、庁内ネットワークへの侵入を防御するために、ファイアウォールその他の機器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。

５　統括責任者は、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ずることが想定される場合には、統括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。

(複合機のセキュリティ管理)

第73条　管理者は、複合機を調達する場合は、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

２　管理者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対するインシデントへの対策を講じなければならない。

３　管理者は、複合機の運用を終了する場合は、複合機の持つ電磁的記録媒体の全ての情報を抹消する、又は再利用できないようにする対策を講じなければならない。

(IoT機器を含む特定用途機器のセキュリティ管理)

第74条　統括責任者は、IoT機器を含む特定用途機器について、取り扱う情報、利用方法及び通信回線への接続形態により、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。

(無線LAN及びネットワークの盗聴対策)

第75条　統括責任者は、無線LANの利用を認める場合は、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。

2　統括責任者は、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。

(電子メールのセキュリティ管理)

第76条　統括責任者は、権限のない利用者により、電子メールの中継処理その他の電子メール転送が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

2　統括責任者は、大量のスパムメールの受信又は送信を検知した場合は、メールサーバの運用の停止等の措置を講じなければならない。

3　統括責任者は、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。

4　統括責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

5　統括責任者は、システム開発、システム運用その他の業務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、委託先との間で利用方法を取り決めなければならない。

(電子メールの利用制限)

第77条　職員等は、自動転送機能を用いて、他のメールサーバへ電子メールを転送してはならない。

2　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

3　職員等は、複数人に電子メールを送信する場合は、必要がある場合を除き、BCCメールにより、他の送信先の電子メールアドレスが分からないようにしなければならない。

4　職員等は、重要な電子メールを誤送信した場合は、管理者に報告しなければならない。

5　職員等は、最高責任者が指定するサービス以外のインターネットで利用できるフリーメール及び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。

(電子署名、暗号化及びパスワード設定)

第78条　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、最高責任者が定めた電子署名、暗号化又はパスワード設定の方法を使用して、送信しなければならない。

2　職員等は、暗号化を行う場合に最高責任者が定める以外の方法を用いてはならない。

3　職員等は、最高責任者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。

4　最高責任者は、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。

(無許可ソフトウエアの導入等の禁止)

第79条　職員等は、端末に無断でソフトウエアを導入してはならない。

２　職員等は、業務上の必要がある場合は、統括責任者の許可を得て、ソフトウエアを導入することができる。

３　統括責任者又は管理者は、前項の規定により導入するソフトウエアのライセンスを管理しなければならない。

４　職員等は、不正にコピーしたソフトウエアを利用してはならない。

(機器構成の変更の制限)

第80条　職員等は、端末に対し機器の改造、増設又は交換を行ってはならない。

２　職員等は、業務上、端末に対し機器の改造、増設又は交換を行う必要がある場合には、統括責任者の許可を得なければならない。

(無許可でのネットワーク接続の禁止)

第81条　職員等は、統括責任者の許可なく端末をネットワークに接続してはならない。

２　支給された端末を、有線・無線を問わず、その端末を接続して利用するよう統括責任者によって定められたネットワークと異なるネットワークに接続してはならない。

(業務以外の目的でのウェブ閲覧の禁止)

第82条　職員等は、業務以外の目的でウェブを閲覧してはならない。

２　統括責任者は、職員等のウェブ利用状況を定期的に確認し、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、管理者に通知し適切な措置を求めなければならない。

(ソーシャルメディアサービスの利用)

第83条　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は、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実施すること。

(2)　パスワード、認証のためのコード等の認証情報及びこれを記録した媒体(ハードディスク、USBメモリ、紙等)等を適正に管理する等の方法で、不正アクセス対策を実施すること。

(3)　機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

(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。

(5)　アカウントの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。

第２款　アクセス制御

(アクセス制御)

第84条　統括責任者は、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。
2　統括責任者は、利用者の登録、変更、抹消その他の情報管理並びに職員等の異動、出向及び退職に伴う利用者IDの取扱いの方法を定めなければならない。
3　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、統括責任者又は統括責任者に通知しなければならない。
4　統括責任者は、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。
5　統括責任者は、管理者権限その他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その他の事故が発生しないよう、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。
6　統括責任者の特権を代行する者は、統括責任者が指名し、最高責任者が認めた者でなければならない。
7　最高責任者は、前項の規定により代行者を認めた場合は、速やかに統括責任者及び管理者に通知しなければならない。
8　統括責任者は、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。
(職員等による外部からのアクセス等の制限)
第85条　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、統括責任者の許可を得なければならない。
2　統括責任者は、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。
3　統括責任者は、外部からのアクセスを認める場合は、システム上で利用者の本人確認を行う機能を確保しなければならない。
4　統括責任者は、外部からのアクセスを認める場合は、通信途上の盗聴を防御するために暗号化その他の措置を講じなければならない。
5　統括責任者は、外部からのアクセスに利用する端末を職員等に貸与する場合は、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。
6　職員等は、外部から持ち帰った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、管理者の許可を得るか、又は管理者によって事前に定義されたポリシーに従って接続しなければならない。
7　統括責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを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。
(パスワードに関する情報の管理)
第86条　統括責任者は、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。
2　統括責任者は、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その他のシステム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。
3　統括責任者は、職員等がパスワードを変更することが可能なシステムにおいて、職員等に対してパスワードを発行する場合は、暫定パスワードを発行し、ログイン後直ちに暫定パスワードを変更させなければならない。
4　統括責任者は、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。
(特権による接続時間の制限)
第87条　統括責任者は、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。
第３款　システムの開発、導入、保守等
(情報システムの調達)
第88条　統括責任者は、情報システムの開発、導入、保守その他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。
2　統括責任者は、機器及びソフトウエアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ対策上問題のないことを確認しなければならない。
(情報システムの開発)
第89条　統括責任者は、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。
2　統括責任者は、システム開発の責任者及び作業者が使用するIDを管理しなければならない。
3　統括責任者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。
4　統括責任者は、システム開発の責任者及び作業者が使用するハードウエア及びソフトウエアを特定しなければならない。
5　統括責任者は、利用を認めたソフトウエア以外のソフトウエアが導入されている場合は、当該ソフトウエアをシステムから削除しなければならない。
(情報システムの導入)
第90条　統括責任者は、システムの開発、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、システムの開発又は保守計画の策定時に手順を明確にしなければならない。
2　統括責任者は、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その他の影響が最小限になるよう配慮しなければならない。
3　統括責任者は、導入するシステム及び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。
4　統括責任者は、新たに情報システムを導入する場合は、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。

(システムの開発及び保守に関連する資料等の保管)

第91条　統括責任者は、システムの開発又は保守に関連する資料及び文書を適切な方法で保管しなければならない。

２　統括責任者は、システムの開発に係るテスト結果を一定期間保管しなければならない。

３　統括責任者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

(情報システムにおける入出力データの正確性の確保)

第92条　統括責任者は、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。

２　統括責任者は、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。

３　統括責任者は、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。

(情報システムの変更管理)

第93条　統括責任者は、情報システムを変更した場合は、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。

(開発用又は保守用のソフトウエアの更新等)

第94条　統括責任者は、開発用又は保守用のソフトウエアを更新又はパッチの適用をする場合は、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。

(システムの更新時及び統合時の検証)

第95条　統括責任者は、システムの更新時及び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後及び統合後の業務運営体制の検証を行わなければならない。

第４款　不正プログラム対策

(統括責任者の措置事項)

第96条　統括責任者は、不正プログラム対策として、次に規定する措置をしなければならない。

(1)　外部ネットワークから受信したファイルは、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その他の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

(2)　外部ネットワークに送信するファイルは、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その他の不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

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

(4)　所掌するサーバ及び端末に、コンピュータウイルスその他の不正プログラム対策ソフトウエア(以下「不正プログラム対策ソフトウェア」という。)を常駐させなければ

ならない。

(5)　不正プログラム対策ソフトウエ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。

(6)　不正プログラム対策ソフトウエアは、常に最新の状態に保たなければならない。

(7)　外部ネットワークに接続していないシステムにおいて、記録媒体を使う場合は、コンピュータウイルスその他の感染を防止するために、管理者が許可する媒体以外を職員等に利用させてはならない。

(8)　不正プログラムの感染又は侵入が生ずる可能性が著しく低い場合を除き、不正プログラム対策ソフトウエアを導入し、定期的に当該ソフトウエア及びパターンファイルの更新を実施しなければならない。

(9)　不正プログラム対策ソフトウエア等の設定変更権限については、一括管理し、統括責任者が許可した職員を除く職員等に当該権限を付与してはならない。

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

(職員等の遵守事項)

第97条　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。

(1)　端末において、不正プログラム対策ソフトウエアが導入されている場合は、当該ソフトウエアの設定を変更してはならない。

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

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

(4)　端末に対して、不正プログラム対策ソフトウエアによるフルチェックを定期的に実施しなければならない。

(5)　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウエアでチェックを行わなければならない。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。

(6)　統括責任者が提供するコンピュータウイルス情報を、常に確認しなければならない。

(7)　コンピュータウイルスその他の不正プログラムに感染した場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。

(専門家の支援体制)

第98条　統括責任者は、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。

第５款　不正アクセス対策

(統括責任者の措置事項)

第99条　統括責任者は、次に規定する措置をしなければならない。

(1)　使用されていないポートを閉鎖しなければならない。

(2)　不用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。

(3)　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括責任者へ通報するよう、設定しなければならない。

(4)　統括責任者は、情報セキュリティ対策に関する統一的な窓口と連携し、監視、通知、外部連絡窓口の設置その他の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。

(攻撃の予告)

第100条　最高責任者及び統括責任者は、サーバその他の機器に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ずるとともに、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。また、総務省、県等と連携を密にして情報の収集に努めなければならない。

(記録の保存)

第101条　最高責任者及び統括責任者は、サーバその他の機器に攻撃を受け、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)の違反その他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。

(内部からの攻撃)

第102条　統括責任者は、職員等及び外部委託事業者が使用している端末からの庁内のサーバその他の機器に対する攻撃及び外部のサイトに対する攻撃を防止するための措置を講じなければならない。

(職員等による不正アクセス)

第103条　統括責任者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する部署の管理者に通知し、適切な処置を求めなければならない。

(サービス不能攻撃)

第104条　統括責任者は、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。

(標的型攻撃)

第105条　統括責任者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策(入口対策)並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、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。

第６款　セキュリティ情報の収集

(セキュリティホールの対策)

第106条　統括責任者は、セキュリティホールに関する情報を収集し、必要に応じて、関係者間で共有しなければならない。

２　統括責任者は、セキュリティホールの緊急度に応じて、ソフトウエア更新その他の対策を実施しなければならない。

(不正プログラム等の対策)

第107条　統括責任者は、不正プログラムその他のセキュリティ情報を収集し、必要に応じて対応方法について、職員等に周知しなければならない。

(情報セキュリティ対策に関する情報の収集及び共有)

第108条　統括責任者は、情報セキュリティ対策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。

２　情報セキュリティ対策に関する社会環境、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。

第７節　運用

第１款　情報システムの監視

(監視による事案検知)

第109条　統括責任者は、セキュリティに関する事案を検知するため、情報システムを監視しなければならない。

２　統括責任者は、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　統括責任者は、外部と接続するシステムを常時監視しなければならない。

第２款　ポリシーの遵守状況の確認

(遵守状況の確認及び対処)

第110条　管理者は、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、速やかに最高責任者及び統括責任者に報告しなければならない。

２　最高責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

３　統括責任者は、ネットワーク、サーバその他の機器のシステム設定における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。

(端末及び記録媒体の調査)

第111条　最高責任者及び最高責任者が指名した者は、不正アクセス又は不正プログラムの調査のために、職員等が使用している端末及び記録媒体のアクセス記録及び電子メールの送受信記録を調査することができる。

(職員等の報告義務)

第112条　職員等は、ポリシーに対する違反行為を発見した場合は、直ちに統括責任者及び管理者に報告を行わなければならない。

２　違反行為が直ちに情報セキュリティ対策上重大な影響を及ぼす可能性があると統括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。

第３款　侵害時の対応

(緊急時対応計画の策定)

第113条　委員会は、情報セキュリティ対策に関する事故、ポリシーの違反その他の事案により情報資産への侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止その他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、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。

(緊急時対応計画に盛り込むべき内容)

第114条　緊急時対応計画には、次に掲げる事項を定めなければならない。

(1)　関係者の連絡先

(2)　発生した事案に係る報告すべき事項

(3)　発生した事案への対応措置

(4)　再発防止措置の策定

(事業継続計画との整合性確保)

第115条　本町が自然災害その他の事態に備えて事業継続計画を策定する場合は、委員会は当該計画とポリシーの整合性を確保しなければならない。

(緊急時対応計画の見直し)

第116条　委員会は、情報セキュリティ対策を取り巻く状況の変化及び組織体制の変動に応じ、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。

第４款　外部委託

(外部委託先の選定基準)

第117条　管理者は、外部委託先の選定に当たり、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。

(契約項目)

第118条　情報システムの運用を外部委託する場合には、委託事業者との間で必要に応じて次に掲げる情報セキュリティ対策要件を明記した契約を締結しなければならない。

(1)　ポリシー及び実施要領の遵守

(2)　委託先の責任者、委託内容、作業者及び作業場所の特定

(3)　提供されるサービスレベルの保証

(4)　委託先にアクセスを許可する情報の種類、範囲及びアクセス方法

(5)　従業員に対する教育の実施

(6)　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

(7)　業務上知り得た情報の守秘義務

(8)　再委託に関する制限事項の遵守

(9)　委託業務終了時の情報資産の返還及び廃棄

(10)　委託業務の定期報告及び緊急時報告義務

(11)　町による監査又は検査
(12)　町によるインシデント発生時の公表
(13)　ポリシーが遵守されなかった場合の損害賠償

(確認及び措置等)

第119条　管理者は、外部委託事業者において必要な情報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、必要に応じて、前条に規定する契約に基づき措置しなければならない。

２　管理者は、前項に規定する確認及び措置の内容を統括責任者に報告するとともに、その重要度に応じて最高責任者に報告しなければならない。

第５款　外部サービスの利用(機密性２以上の情報を取り扱う場合)

(外部サービスの選定)

第120条　管理者は、取り扱う情報の分類及び取扱制限を踏まえ、外部サービス(機密性２以上の情報を取扱う場合に限る。以下この款において同じ。)の利用を検討しなければならない。

２　管理者は、外部サービスで取り扱う情報の分類及び取扱制限を踏まえ、外部サービス提供者を選定しなければならない。また、次の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なければならない。

(1)　外部サービスの利用を通じて本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
(2)　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内容及び管理体制
(3)　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、再委託先又はその他の者によって、本町の意図しない変更が加えられないための管理体制
(4)　外部サービス提供者の資本関係、役員等の情報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並びに調達仕様書による施設の場所及びリージョンの指定
(5)　情報セキュリティインシデントへの対処方法
(6)　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
(7)　情報セキュリティ対策の履行が不十分な場合の対処方法

３　管理者は、外部サービスの中断時及び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なければならない。

４　管理者は、外部サービスの利用を通じて本町が取り扱う情報の分類等を勘案し、必要に応じて次の内容を外部サービス提供者の選定条件に含めなければならない。

(1)　情報セキュリティ監査の受入れ
(2)　サービスレベルの保証

５　管理者は、外部サービスの利用を通じて本町が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本町の情報が取り扱われる場所並びに契約に定める準拠法及び裁判管轄を選定条件に含めなければならない。

6　管理者は、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対策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本町に提供し、本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なければならない。また、外部サービス提供者の選定条件に従って再委託の承認の可否を判断しなければならない。

7　管理者は、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、情報セキュリティ対策に関する役割及び責任の範囲を踏まえて、情報セキュリティ対策要件を定めなければならない。

(外部サービスの利用に係る調達及び契約)

第121条　管理者は、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基準及び選定条件並びに外部サービスの選定時に定めた情報セキュリティ対策要件を調達仕様に含めなければならない。

2　管理者は、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、調達仕様の内容を契約に含めなければならない。

(外部サービスを利用した情報システムの導入時及び構築時の対策)

第122条　管理者は、外部サービスの特性及び責任分界点に係る考え方等を踏まえ、次に掲げる事項を含む調達した外部サービスを利用して情報システムを構築する際の情報セキュリティ対策を規定しなければならない。

(1)　不正なアクセスを防止するためのアクセス制御
(2)　取り扱う情報の機密性保護のための暗号化
(3)　開発時における情報セキュリティ対策
(4)　設計時及び設定時の誤りの防止

2　管理者は、前項において定める規定に対し、構築時に実施状況を確認し記録しなければならない。

(外部サービスを利用した情報システムの運用時及び保守時の対策)

第123条　管理者は、外部サービスの特性及び責任分界点に係る考え方を踏まえ、次に掲げる事項を含む調達した外部サービスを利用して情報システムを運用する際の情報セキュリティ対策を規定しなければならない。

(1)　外部サービス利用方針の規定
(2)　外部サービスの利用手続
(3)　外部サービス利用に必要な教育
(4)　取り扱う資産の管理
(5)　不正アクセスを防止するためのアクセス制御
(6)　取り扱う情報の機密性保護のための暗号化

(7)　外部サービス内の通信の制御
(8)　設計時及び設定時の誤りの防止
(9)　外部サービスを利用した情報システムの事業継続

２　管理者は、外部サービスの特性及び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しなければならない。

３　管理者は、前２項において定める規定に対し、運用時及び保守時に実施状況を定期的に確認し記録しなければならない。

(外部サービスを利用した情報システムの更改時及び廃棄時の対策)

第124条　管理者は、外部サービスの特性及び責任分界点に係る考え方を踏まえ、次に掲げる事項を含む調達した外部サービスの利用を終了する際の情報セキュリティ対策を規定しなければならない。

(1)　外部サービスの利用終了時における対策
(2)　外部サービスで取り扱った情報の廃棄
(3)　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

２　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記録しなければならない。

第６款　外部サービスの利用(機密性２以上の情報を取り扱わない場合)

(外部サービスの利用に係る規定の整備)

第125条　管理者は、次に掲げる事項を含む外部サービス(機密性２以上の情報を取り扱わない場合に限る。以下この款において同じ。)の利用に関する規定を整備しなければならない。

(1)　外部サービスを利用可能な業務の範囲
(2)　外部サービスの利用手続
(3)　外部サービスの利用状況の管理
(4)　外部サービスの利用の運用手順

(外部サービスの利用における対策の実施)

第126条　職員等は、利用するサービスの約款その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性２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しなければならない。また、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じなければならない。

２　管理者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定する。また、承認した外部サービスを記録しなければならない。

第７款　例外措置

(例外措置の許可)

第127条　管理者及び統括責任者は、情報セキュリティ対策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、最高責任者の許可を得て、例外措置をとることができる。

(緊急時の例外措置)

第128条　管理者及び統括責任者は、行政事務の遂行に緊急を要する場合であって、例外措置を実施することが不可避のときは、事後速やかに最高責任者に報告しなければならない。

(例外措置の申請書の管理)

第129条　最高責任者は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

第８款　法令遵守

(関係法令の遵守)

第130条　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、次に掲げる法令のほか関係法令を遵守し、これに従わなければならない。

(1)　地方公務員法(昭和25年法律第261号)

(2)　著作権法(昭和45年法律第48号)

(3)　不正アクセス行為の禁止等に関する法律

(4)　個人情報の保護に関する法律(平成15年法律第57号)

(5)　行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年法律第27号)

(6)　サイバーセキュリティ基本法(平成26年法律第104号)

(7)　砥部町個人情報の保護に関する法律施行条例(令和５年砥部町条例第１号)

第９款　懲戒処分等

(懲戒処分)

第131条　ポリシーに違反した職員等及びその監督責任者は、その重大性及び発生した事案の状況に応じて、地方公務員法による懲戒処分の対象とする。

(違反時の対応)

第132条　統括責任者が職員等のポリシー違反を確認した場合は、統括責任者は当該職員等が所属する部署の管理者に通知し、適切な措置を求めなければならない。

２　管理者が職員等のポリシー違反を確認した場合は、速やかに統括責任者に通知するとともに、違反した職員等に対し適切な措置を講じなければならない。

３　管理者の指導によっても改善されない場合は、統括責任者は、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し、又は剥奪することができる。

４　統括責任者は、前項に規定する措置の後速やかに、職員等の権利を停止し、又は剥奪した旨を最高責任者及び当該職員等が所属する部署の管理者に通知しなければならない。

第８節　評価及び見直し

第１款　監査

(実施方法)

第133条　委員会は、情報セキュリティ監査責任者(以下「監査責任者」という。)を指名し、ネットワーク及び情報システムその他の情報資産における情報セキュリティ対策状況について、定期的に、又は必要に応じて監査を行わせなければならない。

(監査を行う者の要件)

第134条　監査責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

(監査実施計画の立案及び実施への協力)

第135条　監査責任者は、監査を行うに当たって、監査実施計画を立案し、委員会の承認を得なければならない。

２　被監査部門は、監査の実施に協力しなければならない。

(外部委託事業者に対する監査)

第136条　外部委託事業者に委託している場合は、監査責任者は、外部委託事業者から下請として受託している事業者も含めて、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。

(報告)

第137条　監査責任者は、監査結果を取りまとめ、委員会に報告しなければならない。

(保管)

第138条　監査責任者は、監査の実施を通して収集した監査証拠及び監査報告書の作成のための監査調書を、紛失その他の事案が発生しないように適切に保管しなければならない。

(監査結果への対応)

第139条　最高責任者は、監査結果を踏まえ、指摘事項を所管する管理者に対し、当該事項への対処を指示しなければならない。

２　最高責任者は、指摘事項を所管していない管理者に対して、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。

３　最高責任者は、庁内で横断的に改善が必要な事項について、統括責任者に対し、当該事項への対処を指示しなければならない。

(ポリシーの見直し等への活用)

第140条　委員会は、監査結果をポリシーの見直しその他情報セキュリティ対策の見直し時に活用しなければならない。

第２款　自己点検

(実施方法)

第141条　統括責任者は、所管するネットワーク及び情報システムについて、定期的に、又は必要に応じて自己点検を実施しなければならない。

(報告)

第142条　統括責任者は、自己点検結果及び自己点検結果に基づく改善策を取りまとめ、委員会に報告しなければならない。

(自己点検結果の活用)

第143条　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。

２　委員会は、この点検結果をポリシーの見直しその他情報セキュリティ対策の見直し時

に活用しなければならない。

第３款　ポリシーの見直し

(委員会によるポリシーの見直し)

第144条　委員会は、ポリシーについて情報セキュリティ監査、自己点検の結果及び情報セキュリティに関する状況の変化を踏まえ、必要があると認めた場合は、その見直しを行うものとする。

附　則

この訓令は、令和８年４月１日から施行する。