大口町

情報セキュリティ対策基準

令和８年一部改定

内容

内容 1
大口町情報セキュリティ対策基準 ..... - 1 -
1. 趣旨 ..... - 1 -
2. 範囲 ..... - 1 -
3. 組織体制 ..... - 1 -
4. 情報資産の分類と管理方法 ..... - 5 -
5. 情報システム全体の強靭性の向上 ..... - 10 -
6. 物理的セキュリティ ..... - 12 -
6.1. サーバ等の管理 ..... - 12 -
6.2. 管理区域（情報システム室等）の管理 ..... - 14 -
6.3. 通信回線及び通信回線装置の管理 ..... - 15 -
6.4. 職員等のパソコン等の管理 ..... - 16 -
7. 人的セキュリティ ..... - 17 -
7.1. 職員等の遵守事項 ..... - 17 -
7.2. 研修・訓練 ..... - 20 -
7.3. 情報セキュリティインシデントの報告 ..... - 21 -
7.4. ＩＤ及びパスワード等の管理 ..... - 22 -
8. 技術的セキュリティ ..... - 24 -
8.1. コンピュータ及びネットワークの管理 ..... - 24 -
8.2. アクセス制御 ..... - 33 -
8.3. システム開発、導入、保守等 ..... - 36 -
8.4. 不正プログラム対策 ..... - 40 -
8.5. 不正アクセス対策 ..... - 43 -
8.6. セキュリティ情報の収集 ..... - 45 -
9. 運用 ..... - 46 -
9.1. 情報システムの監視 ..... - 46 -
9.2. 情報セキュリティポリシーの遵守状況の確認 ..... - 46 -
9.3 侵害時の対応等 ..... - 47 -
9.4. 例外措置 ..... - 48 -
9.5. 法令遵守 ..... - 48 -
9.6. 懲戒処分等 ..... - 49 -
10. 外部サービスの利用 ..... - 50 -
10.1. 外部委託 ..... - 50 -

10.2. 約款による外部サービスの利用 - 51 -
10.3. ソーシャルメディアサービスの利用 - 51 -
10.4. 生成 AI の利用における留意点 - 52 -
11. 評価・見直し - 54 -
11.1. 監査 - 54 -
11.2. 自己点検 - 56 -
11.3. 情報セキュリティポリシー及び関係規程等の見直し - 57 -

大口町情報セキュリティ対策基準

1.　趣旨

大口町情報セキュリティ基本方針（以下「基本方針」という。）第９の規定に基づき、情報セキュリティ対策基準（以下「対策基準」という。）を定める。

2.　範囲

(1) 行政機関の範囲

この対策基準が適用される行政機関(以下｢行政機関｣という。) は、基本方針第４(1)に定めるところによる。

(2) 情報資産の範囲

この対策基準が対象とする情報資産は、基本方針第４(2)に定めるところによる。

(3) 範囲の除外

学校教育に係るシステム全般のうち、大口町 GIGA スクール及び大口町スクールネット、並びにそれら関連システムについては、この対策基準の対象から除外するものとし、この対策基準に準じて別に教育長が定めるものとする。

3.　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。）

ア　副町長をＣＩＳＯとする。ＣＩＳＯは、本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。

イ　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

して置き、その業務内容を定めることができる。

ウ　ＣＩＳＯは、情報セキュリティインシデントに対処するための体制（ＣＳＩＲＴ：Computer Security Incident Response Team、以下「ＣＳＩＲＴ」という。）を整備し、役割を明確化する。

(2) 統括情報セキュリティ責任者

ア　総務部長を、ＣＩＳＯ直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、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、本町の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ　統括情報セキュリティ責任者は、本町の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

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（各部局長）、情報セキュリティ管理者、情報システム管理者（各システム担当課長）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、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。

カ　統括情報セキュリティ責任者は、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情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

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、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。

(3) 情報セキュリティ責任者

ア　行政機関の部局室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、当該部局室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、その所管する部局室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、その所管する部局室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及び職員等（職員、非常勤職員及び会計年度任用職員をいう。以下同じ。）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

ア　行政機関の課長等を、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。

(5) 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・管理を行う。

(6) 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。

(7) 情報セキュリティ委員会

ア　本町の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

イ　情報セキュリティ委員会の機能は、大口町電子計算機運営委員会が兼ねて行うものとする。

ウ　情報セキュリティ委員会は、必要に応じ、本町における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

(8) 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。

(9) ＣＳＩＲＴの設置・役割

ア　ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化する。

イ　ＣＩＳＯは、ＣＳＩＲＴに所属する職員を選任し、その中からＣＳＩＲＴ責任者を置く。

ウ　ＣＩＳＯは、情報セキュリティインシデントの統一的な窓口を整備し、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。

エ　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。

オ　情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、総務省、都道府県等へ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、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。

キ　統括情報セキュリティ責任者は、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。

4.　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、機密性、完全性及び可用性により、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。

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の情報資産に対して)

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	・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
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適確な遂	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可

	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	能な場所への保管
完全性1	完全性2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、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性1	可用性2の情報資産以外の情報資産	

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

(ｳ) 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。

イ　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。

ウ　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。

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) 外部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、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

(ｴ) 情報セキュリティ管理者又は情報システム管理者は、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。

ク　情報資産の運搬

(ｱ) 車両等により機密性２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。

(ｲ) 機密性２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・公表

(ｱ) 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) 機密性２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) 機密性２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、情報セキュリティ管理者の許可を得なければならない。

5.　情報システム全体の強靭性の向上

(1) マイナンバー利用事務系

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)及びアプリケーションプロトコル(ポート番号)のレベルでの限定を行わなければならない。また、その外部接続先もインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、ＬＧＷＡＮを経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

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うち、二つ以上を併用する認証（多要素認証）を利用しなければならない。ま

た、業務ごとに専用端末を設置することが望ましい。

(ｲ)情報の持ち出し不可設定

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

(2) ＬＧＷＡＮ接続系

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。なお、メールやデータをＬＧＷＡＮ接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

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

(ｲ) 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をテキスト化し、添付ファイルはマクロ除去等のサニタイズ(無害化)処理を行った上で、ＬＧＷＡＮ接続系へ転送する方式

(ｳ) 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

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

(3) インターネット接続系

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　愛知県内の市町村のインターネット接続口を集約するあいち情報セキュリティクラウドに参加するとともに、関係省庁や愛知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。

6. 物理的セキュリティ

6.1. サーバ等の管理

(1) 機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、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

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。

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。

(3) 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。

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

イ　情報システム管理者は、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などを行わなければならない。

(6) 外部への機器の設置

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、外部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

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。

6.2.　管理区域（情報システム室等）の管理

(1) 管理区域の構造等

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「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、管理区域を地階に設けてはならない。また、外部からの侵入が容易にできないように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、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、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。

カ　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。

(2) 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　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等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

エ　情報システム管理者は、機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、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てはならない。ただし、職務遂行上やむを得ない場合は、その用途を確認し、情報セキュリティ管理者の許可を得て、持ち込ませることができる。

(3) 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。

6.3.　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。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。

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

ウ　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。

エ　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。

オ　統括情報セキュリティ責任者は、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、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。

カ　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不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

キ　統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

ク　統括情報セキュリティ責任者は、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。

6.4.　職員等のパソコン等の管理

(1) 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。

(2) 情報システム管理者は、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、或いは生体認証等複数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。

(3) 情報システム管理者は、端末の電源起動時のパスワード（ＢＩＯＳパスワード、ハードディスクパスワード等）を併用しなければならな

い。ただし、端末に個人情報等のデータが保存されない場合はこの限りでない。

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

(5) 情報システム管理者は、パソコン及びモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。ただし、端末に個人情報等のデータが保存されない場合はこの限りでない。

(6) 情報システム管理者は、電磁的記録媒体を利用する場合は、データ暗号化機能を備える媒体を使用しなければならない。

7. 人的セキュリティ

7.1. 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　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

(ｱ) ＣＩＳＯは、機密性２以上、可用性２、完全性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。

(ｲ) 職員等は、本町のモバイル端末、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、機密性３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、モバイル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、モバイル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、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、外部で情報処理作業を行う際に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　パソコン及びモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコン及び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、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、非常勤及び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、非常勤及び会計年度任用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

情報セキュリティ管理者は、非常勤及び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、非常勤及び会計年度任用職員にパソコン及び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、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

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。

7.2.　研修・訓練

(1) 情報セキュリティに関する研修・訓練

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

(2) 研修計画の策定及び実施

ア　ＣＩＳＯ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の構築を定期的に行い、情報セキュリティ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、職員等は毎年度最低１回、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。

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及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

オ　ＣＩＳＯは、毎年度１回、情報セキュリティ委員会に対して、職員等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。

(3) 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、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。

7.3. 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。

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

(2) 住民等外部からの情報セキュリティインシデントの報告

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、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、必要に応じ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。

(3) 情報セキュリティインシデントの原因究明、記録、再発防止等

ア　ＣＳＩＲＴは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

イ　ＣＳＩＲＴは、情報セキュリティインシデントであると評価した場合、ＣＩＳＯに速やかに報告しなければならない。

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

エ　ＣＳＩＲＴは、これらの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。

オ　ＣＩＳＯは、ＣＳＩＲＴ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。

7.4.　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。ただし、当該ＩＣカード等に固有の情報が格納されておらず、当該ＩＣを利用するシステムからＩＣカード情報の登録を解除した場合はこの限りでない。

(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　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。

カ　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。

キ　職員等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。

8.　技術的セキュリティ

8.1.　コンピュータ及びネットワークの管理

(1) 文書サーバの設定等

ア　情報システム管理者は、職員等が使用できる文書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　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　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

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、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。

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

情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得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、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

(3) 他団体との情報システムに関する情報等の交換

情報システム管理者は、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。

(4) 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、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、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

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。

(5) 情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書等について、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、紛失等することがないよう、適

切に管理しなければならない。

(6) ログの取得等

ア　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

統括情報セキュリティ責任者及び情報システム管理者は、職員等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　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。

ウ　統括情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により見直さなければならない。

(9) 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。

(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、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るデータの漏えい、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、次のセキュリティ対策を実施しなければならない。

(ｱ) 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。

(ｲ) 脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。

(ｳ) ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。

(ｴ) 情報システム管理者は、ウェブコンテンツの編集作業を行う主

体を限定しなければならない。

(ｵ) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じなければならない。

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。

(11) 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　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

ア　統括情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

(13) 無線ＬＡＮ及びネットワークの盗聴対策

ア　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。

(14) 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、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がいる場合、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。

オ　統括情報セキュリティ責任者は、職員等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。

(15) 電子メールの利用制限

ア　職員等は、情報システム管理者の許可を得ないで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、情報セキュリティ管理者に報告しなければならない。

オ　職員等は、情報システム管理者の許可を得ないで、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、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　職員等は、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。また、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。

(17) 無許可ソフトウェアの導入等の禁止

ア　職員等は、パソコン及び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　職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

ウ　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

ア　職員等は、パソコン及びモバイル端末に対し機器の改造及び増設並びに交換を行ってはならない。

イ　職員等は、業務上、パソコン及びモバイル端末に対し機器の改造

及び増設並びに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。

(19) 無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なくパソコン及びモバイル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、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、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、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。

(21)ウェブ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、ウェブ会議を適切に利用するために必要な情報セキュリティ対策を実施しなければならない。

イ　職員等は、ウェブ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じなければならない。

(22) ソーシャルメディアサービスの利用時の対策

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

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

(ｲ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USB メモリ、紙等）等を適正に管理す

るなどの方法で、不正アクセス対策を実施しなければならない。

イ　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。

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　可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本町の自己管理ウェブサイトに当該情報を掲載して参照可能としなければならない。

(23) 生成 AI の利用時の対策

ア　機密性２以上の情報は生成 AI に与えてはならない。

イ　情報セキュリティ管理者は、所管する課室等における最高 AI 責任者（ＣＡＩＯ：Chief AI Officer）として、本町が所掌するパソコン等の端末で業務のために生成 AI を利用するにあたり、次の事項を管理しなければならない。

(ｱ) 所管する課室等において生成 AI を利用する職員。

(ｲ) 生成 AI を利用できる業務の範囲とその目的。

(ｳ) 生成 AI に与えてよい情報の種類。

(ｴ) 生成 AI が出力した生成物の最新性、正確性、妥当性、一貫性、及び説明可能性。

ウ　生成 AI の利用は、その目的のための必要最小限の利用又は提供でなければならず、法令規則等を踏まえて、情報セキュリティ管理者がそのリスクを総合的に判断し、意思決定の最終的な責任を負うものとする。

エ　生成 AI が出力した生成物を公表する場合、生成 AI が出力した生成物であることを表記しなければならない。

オ　利用する生成 AI は日本国内リージョン（データセンターが日本国

内に配置されているもの）に限る。

8.2.　アクセス制御

(1) 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等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

イ　利用者ＩＤの取扱い

(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、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) 情報システム管理者は、業務上必要がなくなった場合は、利用者登録を遅滞なく抹消するとともに、その旨を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。

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

ウ　特権を付与されたＩＤの管理等

(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、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

(ｲ) 統括情報セキュリティ責任者及び情報システム管理者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意

ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。

(ｳ) 統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、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。

(ｴ) 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。

(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、特権を付与されたＩＤ及びパスワードの変更について、外部委託事業者に行わせてはならない。

(ｶ) 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。

(ｷ) 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤを初期設定以外のものに変更しなければならない。

(2) 職員等による外部からのアクセス等の制限

ア　職員等が外部から庁内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、庁内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、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）の外部通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等、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。

(3) 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。

(4) 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、ログイン・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等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。

(5) 認証情報の管理

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、職員等の認証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認証情報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、初回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。

(6) 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。

8.3.　システム開発、導入、保守等

(1) 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。

(2) 情報システムの開発

ア　システム開発における責任者及び作業者の特定

情報システム管理者は、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。また、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、作業者のＩＤの管理

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

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

ウ　システム開発に用いるハードウェア及びソフトウェアの管理

(ｱ) 情報システム管理者は、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。

(ｲ) 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。

エ　アプリケーション・コンテンツの開発時の対策

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

(3) 情報システムの導入

ア　開発環境と運用環境の分離及び移行手順の明確化

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

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

(ｳ) 情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

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

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

(ｴ) 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。

(ｵ) 情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない

ウ　機器等の納入時又は情報システムの受入れ時

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

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

(4) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

ア　情報システム管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じなければならない。

イ　情報システム管理者は、利用するソフトウェアの特性を踏まえ、以下の実施手順を整備しなければならない。

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

(ｲ) 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

(5) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

ア　情報システム管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施しなければならない。

(ｱ) 情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策

(ｲ) 脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

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

(6) システム開発・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・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

イ　情報システム管理者は、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。

(7) 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恐れがある場合に、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。

(8) 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。

(9) 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・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。

(10) システム更新又は統合時の検証等

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

(11) 情報システムについての対策の見直し

情報システム管理者は、情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本町内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。

8.4.　不正プログラム対策

(1) 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の

事項を措置しなければならない。

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。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

(2) 情報システム管理者の措置事項

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

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　情報システム管理者（各システム担当課長）は、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。

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等に当該権限を付与してはならない。

(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　パソコン及び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　差出人が不明なメールを受信した場合、又は、不自然にファイルが添付されたメー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、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ケーブルを即時に取り外すこと。また、無線ＬＡＮにより情報系ＬＡＮに接続している場合においては、直ちに無線ＬＡＮをＯＦＦにすること。

(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変更すること。

(4) 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。

8.5.　不正アクセス対策

(1) 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正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　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　重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

オ　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禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

(4) 内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) 職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、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

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、第三者からの攻撃により、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(7) 標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、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、職員教育、自動再生無効化等の人的対策及び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。

8.6. 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

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。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

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、職員等に周知しなければならない。

(3) 情報セキュリティに関する情報の収集及び共有

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

9. 運用

9.1. 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。

9.2. 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。

(2) パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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、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。

(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。

9.3　侵害時の対応等

(1) 緊急時対応計画の策定

ＣＩＳＯ又は情報セキュリティ委員会は、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) 業務継続計画との整合性確保

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

(4) 緊急時対応計画の見直し

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

9.4.　例外措置

(1) 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。

(2) 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。

(3) 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、定期的に申請状況を確認しなければならない。

9.5.　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。

ア　地方自治法（昭和２２年法律第６７号）

イ　地方公務員法(昭和２５年法律第２６１号)

ウ　著作権法（昭和４５年法律第４８号）

エ　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）

オ　個人情報の保護に関する法律（平成１５年法律第５７号）

カ　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）

キ　サイバーセキュリティ基本法（平成２８年法律第１０４号）

ク　重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第４２号）

ケ　人工知能関連技術の研究開発及び活用の推進に関する法律（令和７年法律第５３号）

コ　大口町個人情報の保護に関する法律施行条例（令和４年大口町条例第３８号）

9.6.　懲戒処分等

(1) 懲戒処分

情報セキュリティポリシーに違反した職員等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、地方公務員法による懲戒処分の対象とする。

(2) 違反時の対応

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

ア　統括情報セキュリティ責任者が違反を確認した場合は、当該違反職員等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、速やかに統括情報セキュリティ責任者に通知するとともに、適切な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。この場合、統括情報セキュリティ責任者は、その旨をＣＩＳＯ及び当該職員等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。

10.　外部サービスの利用

10.1.　外部委託

(1) 外部委託事業者の選定基準

ア　情報セキュリティ管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

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

ウ　情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用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及び情報セキュリティ実施手順の遵守
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め
・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
・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
・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。

10.2. 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、機密性２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

ア 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。

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

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

(ｲ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（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

イ　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。

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。

10.4.　生成 AI の利用における留意点

ディープラーニング等により、「画像認識」、「自然言語処理(翻訳等)」、「音声認識」を活用して、画像や文章等を生成する AI を用いたサービスを業務で利用するにあたっては、次の事項に留意する。

ア　データ入力に関する事項

(ｱ) 第三者が著作権を有しているデータ（他人が作成した文章等）

単に生成 AI に他者の著作物を入力するだけの行為は原則として著作権侵害に該当しないものの、当該入力対象となった他者の著作物と同一・類似する AI 生成物を生成する目的がある場合には、入力行為自体が著作権侵害になる可能性があること。

また、生成されたデータが入力したデータや既存のデータ（著作物）と同一・類似している場合は、当該生成物の利用が当該著作物の著作権侵害になる可能性があること。

(ｲ) 登録商標・意匠（ロゴやデザイン）

商標や意匠として登録されているロゴ・デザイン等を生成 AI に入力することは商標権侵害や意匠権侵害に該当しないものの、故

意に、あるいは偶然生成された、他者の登録商標・意匠と同一・類似の商標・意匠を利用する行為は商標権侵害や意匠権侵害に該当すること。

(ｳ) 著名人の顔写真や氏名

著名人の顔写真や氏名を生成 AI に入力する行為は、当該著名人が有しているパブリシティ権の侵害には該当しないものの、生成 AI を利用して生成物された著名人の氏名、肖像等については、それらの氏名や肖像等を利用する行為はパブリシティ権侵害に該当すること。

(ｴ) 個人情報

生成 AI においては、入力したデータが当該生成 AI のモデルの学習に利用されることがあるため、生成 AI に個人情報（氏名・住所等）を入力してはならない。ただし、当該個人情報により特定される本人の同意が取得できているのであればこの限りではない。

(ｵ) 秘密保持義務を課されて開示された秘密情報及び本町の機密情報

生成 AI に情報を入力する行為は、生成 AI 提供者という「第三者」に情報を「開示」することになるため、他者との間で秘密保持契約などを締結して取得した秘密情報及び本町の機密情報は入力してはならない。

イ　生成物の利用に関する事項

(ｱ) 生成物の内容に虚偽が含まれている可能性

大規模言語モデル（LLM）の原理は、「ある単語の次に用いられる可能性が確率的に最も高い単語」を出力することであり、もっともらしい文章を作成していくものであるため、書かれている内容には虚偽が含まれている可能性があること。

生成 AI のこのような限界を知り、その生成物の内容を盲信せず、必ず根拠や裏付けを自ら確認すること。

(ｲ) 生成物を利用する行為が他者の既存の権利を侵害する可能性

生成 AI を利用して出力された生成物が、既存の著作物と同一・類似している場合は、当該生成物を利用（複製や配信等）する行為が著作権侵害に該当する可能性があること。

また、画像生成 AI を利用して生成した画像や、文章生成 AI を利用して生成したキャッチコピー等を商品ロゴや広告宣伝等に使う行為は、他者が権利を持っている登録商標権や登録意匠権を侵害する可能性があるため、生成物が既存著作物に類似していないかの調査に加えて、登録商標・登録意匠の調査を行うこと。

加えて、生成 AI は、個人に関する虚偽の情報を生成する可能性があることから、虚偽の個人情報を生成して利用・提供する行為は、個人情報保護法違反や、名誉毀損・信用毀損に該当する可能性があるため、そのような行為を行ってはならない。

(ｳ) 生成物に著作権が発生しない可能性

生成 AI が自律的に生成した生成物は「著作物」に該当しない場合があるため、生成物はそのまま利用せず、必ず加筆・修正すること。

(ｴ) 生成物を商用利用できない可能性

利用する生成 AI の利用規約によっては、当該生成 AI の生成物の権利が本町に帰属しない場合があるため、生成物はそのまま利用せず、必ず加筆・修正すること。

(ｵ) 生成 AI の利用規約上の制限について

利用する生成 AI においては、法令上の制限以外にも、各サービスの利用規約にて独自の制限を設けている場合があるため、利用前に必ず利用規約を確認すること。

11. 評価・見直し

11.1. 監査

(1) 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。

(2) 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。

(3) 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、情報セキュリティ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。

(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定期的に又は必要に応じて行わなければならない。

(5) 報告

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

(6) 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

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。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

情報セキュリティ委員会は、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。

11.2. 自己点検

(1) 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。

(2) 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、情報セキュリティ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 情報セキュリティ委員会は、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。

11.3.　情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、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。

参考

(1) CISO：副町長

(2) 統括情報セキュリティ責任者：総務部長

(3) 情報セキュリティ責任者：部局室長

(4) 情報セキュリティ管理者：課長等

(5) 情報システム管理者：システムを保有している部署の課長等

(6) 情報システム担当者：システムを保有している部署の担当者

(7) 情報セキュリティポリシー：大口町情報セキュリティ基本方針及び大口町情報セキュリティ対策基準の総称

(8) 情報セキュリティ委員会：本町の情報セキュリティ対策を統一的に行うための、情報セキュリティに関する重要な事項を決定する組織であり、大口町電子計算機運営委員会を以て充てる。