大間町情報セキュリティ対策基準

本対策基準は、情報セキュリティ基本方針を実行に移すための、本町における情報資産に関する情報セキュリティ対策の基準を定めたものである。

第１　対象範囲

（１）　行政機関の範囲

本対策基準が適用される行政機関は、町長部局、各行政委員会、議会事務局及び公営企業局とする。ただし、教育委員会の所管する学校を除く。

（２）　情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

② ネットワークおよび情報システムで取り扱う情報（これらを印刷した文書含む）

③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

第２　組織体制等

（１）　最高情報セキュリティ責任者（CISO）

① 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。

② 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）を整備し、役割を明確化する。

（２）　情報セキュリティ責任者

① 企画経営課長を情報セキュリティ責任者とする。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。

② 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。

③ 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。

④ 情報セキュリティ責任者は、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。

⑤ 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実施する権限及び責任を有する。

⑥ 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。

⑦ 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、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。

⑧　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。

（3）　情報システム管理者

①　各情報システムの担当課長等を情報システム管理者とする。

②　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

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

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

（4）　情報システム担当者

情報システム責任者の指示等に従い、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。

（5）　兼務の禁止

①　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。

（6）　CSIRTの設置・役割

①　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）を整備し、その役割を明確化しなければならない。

②　CISOは、情報セキュリティ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しなければならない。

③　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しなければならない。

④　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。

⑤　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。

第３　情報資産の分類と管理方法

（１）　情報資産の分類

本町における情報資産は、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	・支給以外での端末での作業の原則禁止（機密性３に対して） ・必要以上の複製及び配布禁止 ・保管場所の制限、保管場所への必要以上の電子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、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能な場所への保管
完全性１	完全性２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以外の情報資産	－

（２）　情報資産の管理

①　管理責任

ア　情報セキュリティ責任者は、その所管する情報資産について管理責任を有する。

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

②　情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

③　情報の作成

ア　職員等は、業務上必要のない情報を作成してはならない。

イ　情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④　情報資産の入手

ア　庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

イ　庁外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ　情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ責任者に判断を仰がなければならない。

⑤　情報資産の利用

ア　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

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

ウ　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥　情報資産の保管

ア　情報セキュリティ責任者又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

イ　情報セキュリティ責任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　情報セキュリティ責任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。

⑦　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、パスワード等による暗号化を行わなければならない。

⑧　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、パスワード等による暗号化を行う等、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。ただし、暗号化を施すことができないものについては、２名体制で運搬する等して機密性を確保しなければならない。

イ　機密性２以上の情報資産を運搬する者は、情報セキュリティ責任者に許可を得なければならない。

⑨　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、必要に応じパスワード等による暗号化を行わなければならない。ただし、パスワード設定を施すことができないものについては、別な方法により機密性を確保しなければならない。

イ　機密性２以上の情報資産を外部に提供する者は、情報セキュリティ責任者に許可を得なければならない。

ウ　情報セキュリティ責任者は、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。

⑩　情報資産の廃棄等

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理したう

え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、情報セキュリティ責任者の許可を得なければならない。

第４　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

①　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、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。

②　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、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。

（２）　LGWAN 接続系

①　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

（３）　インターネット接続系

①　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。

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。

第５ 物理的セキュリティ

５．１ 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

① 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。

② 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

① 情報システム管理者は、施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

② 情報システム管理者は、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

① 情報セキュリティ責任者及び情報システム管理者は、通信ケーブル及び電源ケーブルの損傷等を防止するために、主要な箇所について配線収納管を使用する等必要な措置を講じなければならない。

② 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な管理をしなければならない。

③ 情報セキュリティ責任者及び情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた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講じなければならない。

（５） 機器の定期保守及び修理

① 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。

② 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、事業者に故障を修理させるに当り、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わせなければならない。

（6） 庁外への機器の設置

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。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。

５．２ 管理区域（サーバ室）の管理

（1）サーバ室の構造等

① 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や電磁的記録媒体の保管庫をいう。

② CISO は、外部からの侵入が容易にできないよう無窓の外壁にしなければならない。

③ CISO は、サーバ室に通ずるドアを必要最小限とし、施錠管理等によって許可されていない職員の立入りを防止しなければならない。

④ 情報セキュリティ責任者及び情報システム管理者は、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

（2） サーバ室の入退室管理等

① 情報システム管理者は、サーバ室への入退室をする者について、入退室管理簿による入退室管理を行わなければならない。

② 職員及び委託事業者は、サーバ室に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

③ サーバ室に入室する者は、当該情報システムに関連しない、または個人所有であるコンピュータ、パソコン、モバイル端末、通信回線装置、電磁的記録媒体等を必要以上に持ち込んではならない。

（3） 機器等の搬入出

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事業者に確認を行わせなければならない。

５．３ 通信回線及び通信回線装置の管理

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、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しな

ければならない。

（2） 情報セキュリティ責任者は、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。

（3） 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）に集約するよう努めなければならない。

（4） 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、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

（5） 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。

（6） 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。

５．４ 職員の利用する端末や電磁的記録媒体等の管理

（1） 情報システム管理者は、職員の利用する端末についてログインパスワード、或いは生体認証等の認証情報の入力を必要とするよう設定しなければならない。また、盗難防止のため、個人番号利用事務系パソコンをワイヤーによる固定をしなければならない。

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

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

第６ 人的セキュリティ

６．１ 職員等の遵守事項

（1） 職員等の遵守事項

① 情報セキュリティポリシー等の遵守

職員は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに当該情報資産を管理する情報セキュリティ責任者に相談し、指示を仰がなければならない。

② 業務以外の目的での使用禁止

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。

③　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、情報セキュリティ責任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、情報セキュリティ責任者の許可を得なければならない。

④　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、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、情報セキュリティ責任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、情報セキュリティ責任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に関する規定を遵守しなければならない。

⑤　持ち出し及び持ち込みの記録

情報セキュリティ責任者は、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。

⑥　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

職員等は、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責任者の許可なく変更してはならない。

⑦　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責任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、適正な措置を講じなければならない。

⑧　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等への対応

①　情報セキュリティポリシー等の遵守

情報セキュリティ責任者は、非常勤及び会計年度任用職員等に対し、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等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。

② インターネット接続及び電子メール使用等の制限

情報セキュリティ責任者は、非常勤及び会計年度任用職員等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。

（3） 情報セキュリティポリシー等の掲示

情報セキュリティ責任者は、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） 委託事業者に対する説明

情報セキュリティ責任者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち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。

６．２ 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

① 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わなければならない。

② 新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

③ 研修は、情報セキュリティ責任者、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。

（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。

（4） 研修・訓練への参加

職員は、定められた研修・訓練に参加しなければならない。

６．３ 情報セキュリティインシデントの報告

（1） 庁内でのセキュリティインシデントの報告

① 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責任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。

② 報告を受けた情報セキュリティ責任者は、速やかに CISO 及び情報システム管理者に報告しなければならない。

（2） 住民等外部からの情報セキュリティインシデントの報告

① 職員は、本町が管理する情報資産に関するインシデントについて、町民等外部から報告を受けた場合、情報セキュリティ責任者に報告しなければならない。

② 報告を受けた情報セキュリティ責任者は、必要に応じて CISO 及び情報システム管理者に報告しなければならない。

③ 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。

（3）情報セキュリティインシデント原因の究明・記録、再発防止等

① 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。

② 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。

③ 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。

④ CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。

⑤ 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。

６．４　ＩＤ及びパスワード等の管理

（1）　ID の取扱い

職員は、自己の管理する ID に関し、次の事項を遵守しなければならない。

① 自己が利用している ID を他人に利用させてはならない。

② 共用 ID を利用する場合、共用 ID を利用者以外に利用させてはならない。

（2）　パスワードの取扱い

職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

① 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。

② 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。

③ 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 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）。

第７　技術的セキュリティ

７．１　コンピュータ及びネットワークの管理

（1）　コンピュータ及びネットワークの管理

① ファイルサーバの設定

情報システム管理者は、ファイルサーバを課等の単位で構成し、職員が他課等のフォルダ及びファイルを閲覧及び使用できないように設定しなければならない。

② バックアップの実施

情報セキュリティ責任者及び情報システム管理者は、ファイルサーバに記録された情報について、サーバの冗長化対策に関わらず、定期的にバックアップを実施しなければならない。

③ 他団体との情報システムに関する情報等の交換

情報システム管理者は、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、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、管理する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

イ 情報セキュリティ責任者及び情報システム管理者は、管理する情報システムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

ウ 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

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。

⑥ ログの取得等

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。

⑦ 障害記録

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結果又は問題等を障害記録として記録し、一定期間保存しなければならない。

⑧ ネットワークの接続制御、経路制御等

ア 情報セキュリティ責任者は、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 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。

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、管理するネットワークを外部ネットワークに接続しようとする場合には、CISO 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。

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　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、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　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、設置環境並びに取扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

イ　情報セキュリティ責任者は、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インシデントへの対策を講じなければならない。

ウ　情報セキュリティ責任者は、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

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

⑬　無線 LAN 及びネットワークの盗聴対策

ア　情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化さ

れた通信により使用できるものを選定しなければならない。

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

ウ　情報セキュリティ責任者は、機密性の高い情報を取扱うネットワークについて、情報の盗聴を防ぐため、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　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　情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

ウ　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。

⑮　電子メールの利用制限

ア　職員等は、自動転送機能を用いて、電子メールを転送してはならない。

イ　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

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

エ　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ責任者に報告しなければならない。

⑯　電子署名・暗号化

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、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

⑰　無許可ソフトウェアの導入等禁止

ア　職員等は、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　職員等は、業務上の必要がある場合は、情報セキュリティ責任者の許可を得て、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、情報セキュリティ責任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、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

イ　職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、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　業務外ネットワークへの接続の禁止

ア　職員等は、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情報システム管理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。

イ　情報セキュリティ責任者は、支給した端末について、端末に搭載されたOSのポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

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　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、情報セキュリティ責任者に通知し適正な措置を求めなければならない。

㉑　Web会議サービスの利用時の対策

ア　職員等は、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。

イ　職員等は、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。

㉒　ソーシャルメディアサービスの利用

ア　情報セキュリティ責任者は、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。

・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。

・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すること。

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。

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Webサイトに当該情報を掲載して参照可能とすること。

７．２　アクセス制御等

（１）　アクセス制御

①　アクセス制御

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

②　利用者ＩＤの取り扱い

ア　情報セキュリティ責任者及び情報システム管理者は、アクセスを許可した者の利用者 ID を適切に管理しなければならない。

イ　職員等は、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、当該情報資産を管理する情報セキュリティ責任者に申し出なければならない。

ウ　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。

③　特権を付与された ID の管理等

ア　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 を利用する職員等を必要最小限にし、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　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、委託業者に行わせてはならない。

（２）　職員等による外部からのアクセス等の制限

①　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、当該ネットワーク又は当該情報システムを管理する情報システム管理者の許可を得なければならない。

②　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職員等に限定しなければならない。

③　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。

④　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。

⑤　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インターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID 及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化、

情報セキュリティ確保のために必要な措置を講じなければならない。

（3） 認証情報の管理

① 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。

② 情報セキュリティ責任者及び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。

（4） 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。

7．3 システム開発、導入、保守等

（1） 情報システムの調達

① 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。

② 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

① 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。

② 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。

（3） 情報システムの導入

① 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、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。

② 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、あらかじめ疑似環境による操作確認を行わなければならない。

ウ　情報システム管理者は、個人情報及び機密性の高い生データをテストデータに使用してはならない。

エ　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。

（4）　システム開発・保守に関連する資料等の整備・保管

① 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。

② 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。

③ 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。

（5）　情報システムにおける入出力データの正確性の確保

① 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。

② 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。

③ 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。

（6）　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、プログラム仕様書の変更履歴を作成しなければならない。

（7）　開発・保守用のソフトウェアの更新等

情報システム管理者は、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。

（8）　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い。

７．４　不正プログラム対策

（1）　情報セキュリティ責任者の措置事項

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。

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。

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。

③ 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。

④ 管理するサーバ及びパソコン等の端末に、コンピュータウ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。

⑤ 不正プログラム対策のソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥ 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い。

⑦ 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管理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。

① 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。

② 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。

③ 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。

④ インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、本町が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

⑤　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。

①　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。

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

③　差出人が不明又は不自然に添付されたファイルを受信した場合は、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

④　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。

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。

⑥　情報セキュリティ責任者が提供するウィルス情報を、常に確認しなければならない。

⑦　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。

ア　パソコン等の端末の場合 LAN ケーブルの即時取り外しを行わなければならない。

イ　モバイル端末の場合直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

（4）　専門家の支援体制

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。

７．５　不正アクセス

（1）　情報セキュリティ責任者の措置事項

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。

①　使用していないポートを閉鎖しなければならない。

②　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。

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の対策を講じなければならない。

（2）　攻撃への対処

CISO 及び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。また、総務省、都道府県等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

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

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。

（6） サービス不能攻撃

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。

（7） 標的型攻撃

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。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）や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、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。

7．6 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

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、情報セキュリティ責任者にソフトウェア更新等の対策をするよう指示しなければならない。

（2） 不正プログラム等のセキュリティ情報の収集・周知

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。

（3） 情報セキュリティに関する情報の収集及び共有

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。

第８　運用

８．１　情報システムの監視

（１）　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、情報システムを監視しなければならない。

（２）　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。

（３）　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。

８．２　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

①　情報セキュリティ責任者は、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に報告しなければならない。

②　CISOは、発生した問題について、適正かつ速やかに対処しなければならない。

③　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正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

①　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報セキュリティ責任者に報告を行わなければならない。

②　当該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情報セキュリティ責任者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

８．３　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責任者は、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正に実施するために、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正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。

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

（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、情報セキュリティ責任者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 又は情報システム管理者は、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。

８．４ 例外措置

（1） 例外措置の許可

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する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、例外措置を講じることができる。

（2） 緊急時の例外措置

情報セキュリティ責任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。

８．５ 法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

① 地方公務員法(昭和 25 年法律第 261 号)
② 著作権法（昭和 45 年法律第 48 号)
③ 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号)

④　個人情報の保護に関する法律（平成 15 年法律第 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　大間町個人情報保護条例　（平成 17 年条例第５号）

８．６　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。

①　情報セキュリティ責任者が違反を確認した場合は、CISO は適正な措置を講じなければならない。
②　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情報セキュリティ責任者に通知し、適正な措置を求めなければならない。
③　情報セキュリティ責任者の指導によっても改善されない場合、情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、職員等の権利を停止あるいは剥奪した旨を CISO に通知しなければならない。

第９　業務委託と外部サービスの利用

９．１　業務委託

（１）　委託事業者の選定基準

①　情報セキュリティ責任者又は情報システム管理者は、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。
②　情報セキュリティ責任者又は情報システム管理者は、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、委託事業者を選定しなければならない。

（２）　契約項目

情報セキュリティ責任者又は情報システム管理者は、情報システムの運用、保守等を業務委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティポリシー要件を明記した契約を締結しなければならない。

①　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
②　委託事業者の責任者、作業者、委託内容、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
⑤　委託事業者の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事業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、廃棄等
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、検査
⑫　町によるインシデント発生時の公表
⑬　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

情報セキュリティ責任者は、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を実施しなければならない。

９．２　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）

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

（2）　当該外部サービスを利用する情報システム管理者は、その利用に係る情報資産を管理する情報セキュリティ責任者の許可を得なければならない。

（3）　情報セキュリティ責任者は、許可した外部サービスについて記録をとらなければならない。記録する事項としては、サービス提供者、サービス名、利用目的、利用期間、利用する職員名とする。

第１０　評価・見直し

１０．１　監査

（1）　実施方法

CISOは、監査する者（以下「監査実施者」という。）を外部から選任し、本町の情報資産における情報セキュリティ対策の状況について、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

①　被監査部門から独立した者であること。
②　監査及び情報セキュリティに関する専門知識を有する者であること。

（3）　監査の実施への協力

被監査部門は、監査の実施に協力しなければならない。

（4） 委託事業者に対する監査

事業者に業務委託を行っている場合、情報セキュリティ責任者は委託事業者（再委託事業者を含む。）に対して、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

監査実施者は、監査結果を取りまとめ、情報セキュリティ責任者に報告する。

（5） 保管

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

（6） 監査結果への対応

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

１０．２ 自己点検

（1） 実施点検

情報セキュリティ責任者は、管理する情報資産における情報セキュリティ対策の状況について、定期的に自己点検を行わなければならない。

（2） 報告

情報セキュリティ責任者は、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、CISO に報告しなければならない。

（3） 自己点検結果の活用

① 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。

② 情報セキュリティ責任者は、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。

１０．３ 情報セキュリティポリシー及び関連規程等の見直し

情報セキュリティ責任者は、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。