久御山町情報セキュリティの管理運営及び対策基準に関する規程

目　次

第１章　総則

（趣旨）

第１条　この規程は、久御山町（以下「本町」という。）における情報セキュリティ基本方針に基づき、本町が所有す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るものとする。

第２章　管理運営体制

（最高情報セキュリティ責任者）

第２条　副町長を最高情報セキュリティ責任者（ＣＩＳＯ: Chief Information Security Officer、以下「ＣＩＳＯ」という。）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：Computer Security Incident Response Team、以下「ＣＳＩＲＴ」（シーサート）という。）を整備し、役割を明確化する。

３　ＣＩＳＯは、ＣＩＳＯを助けて本町における情報セキュリティに関する事務を整理し、ＣＩＳＯの命を受けて本町の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副ＣＩＳＯ」という。）１人を必要に応じて置く。

４　ＣＩＳＯは、本規程に定められた自らの担務を、副ＣＩＳＯその他の本規程に定める責任者に担わせることができる。

（統括情報セキュリティ責任者）

第３条　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及び副ＣＩＳＯを補佐しなければならない。

２　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、見直し等を行う統括的な権限及び責任を有する。

３　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統括的な権限及び責任を有する。

４　統括情報セキュリティ責任者は、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　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。

６　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。
7　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及び情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。
8　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。
9　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。

（情報セキュリティ責任者）

第４条　各部等の長を情報セキュリティ責任者とする。
2　情報セキュリティ責任者は、所管する部署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。
3　情報セキュリティ責任者は、所管する部署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。
4　情報セキュリティ責任者は、その所管する部署において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約、並びに職員等に対する教育、訓練、助言及び指示を行う。

（情報セキュリティ管理者）

第５条　各課等の長を情報セキュリティ管理者とする。
2　情報セキュリティ管理者は、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。
3　情報セキュリティ管理者の所掌する事務は、次の各号に掲げるとおりとする。
(1)　情報システムの開発、導入、運用及び保守に関すること。
(2)　所管する情報システムの追加又は変更の承認に関すること。
(3)　所管する情報資産に係る情報セキュリティ対策の実施及び周知に関すること。
(4)　所管する情報システムに係る事件・事故の発生に備えた訓練の実施に関すること。
(5)　情報セキュリティに係る事件・事故発生時の対応に関すること。
(6)　所管する情報システムに係る実施手順の策定及び評価・見直しに関すること。

（情報システム担当者）

第６条　情報セキュリティ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、更新等の作業を行い、所管する情報資産に係る情報セキュリティ対策の実施等を補佐する者を情報システム担当者とする。

（兼務の禁止）

第７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　情報セキュリティ監査の実施において、やむを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

（ＣＳＩＲＴの設置・役割）

第８条　ＣＩＳＯは、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、ＣＳＩＲＴに所属する職員等を選任し、その中からＣＳＩＲＴ責任者を置かなければならない。また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員等を定めなければならない。

３　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部課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しなければならない。

４　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、その内容を関係部課等に提供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、ＣＩＳＯ、総務省、京都府等へ報告しなければならない。

６　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。

７　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わなければならない。

第３章　情報資産の分類と管理

（情報資産の分類）

第９条　本町における情報資産は、情報の機密性、完全性及び可用性を踏まえ、次の各号に掲げるとおり分類し、必要に応じ取扱制限を行うものとする。

(1)　重要性分類Ａ　個人情報及び情報セキュリティの侵害が住民の生命、財産等へ重大な影響を及ぼす情報を含むもの

(2)　重要性分類Ｂ　公開することを予定していない情報及び情報セキュリティの侵害が行政事務の執行等に重大な影響を及ぼす情報を含むもの

(3)　重要性分類Ｃ　外部に公開する情報のうち、情報セキュリティの侵害が行政事務の執行等に軽微な影響を及ぼす情報を含むもの

(4)　重要性分類Ｄ　上記以外の情報を含むもの

（情報資産の管理責任）

第10条　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。

２　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前条の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11条　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。

（情報の作成）

第12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９条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
３　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。
（情報資産の入手）
第13条　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。
２　庁外の者が作成した情報資産を入手した者は、第９条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
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、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。
（情報資産の利用）
第14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、適正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、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。
（情報資産の保管）
第15条　情報セキュリティ管理者は、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。
２　情報セキュリティ管理者は、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。
３　情報セキュリティ管理者は、重要性分類Ｂ以上（重要性分類Ｂ及びＡ、以下同じ。）の情報を記録した電磁的記録媒体を保管する場合は、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。
（情報の送信）
第16条　電子メール等により重要性分類Ｂ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17条　車両等により重要性分類Ｂ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。
２　重要性分類Ｂ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。
（情報資産の提供・公表）

第18条　重要性分類Ｂ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。

２　重要性分類Ｂ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。

３　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。

（情報資産の廃棄）

第19条　重要性分類Ｂ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。

２　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。

３　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。

第４章　情報システム全体の強靭性の向上

（マイナンバー利用事務系と他の領域との分離）

第20条　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。ただし、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。なお、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、インターネット等からＬＧＷＡＮ－ＡＳＰを経由してマイナンバー利用事務系にデータの取り込みを可能とする。

（情報のアクセス及び持ち出しにおける対策）

第21条　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）を利用するよう努めなければならない。また、可能な限り業務ごとに専用端末を設置することとする。

２　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。

（ＬＧＷＡＮ接続系とインターネット接続系の分割）

第22条　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、次の各号に掲げるいずれかの方法により、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）

第23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　市区町村のインターネット接続口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章　物理的セキュリティ

第１節　サーバ等の管理

（機器の取付け）

第24条　情報セキュリティ管理者は、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正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25条　情報セキュリティ管理者は、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、当該機器が適正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　情報セキュリティ管理者は、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。

（通信ケーブル等の配線）

第26条　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、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。

３　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、自ら又は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できないように必要な措置を講じなければならない。

（機器の定期保守及び修理）

第27条　情報セキュリティ管理者は、重要性分類Ｂ以上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　情報セキュリティ管理者は、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、情報セキュリティ管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

（庁外への機器の設置）

第28条　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。

（機器の廃棄等）

第29条　情報セキュリティ管理者は、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。

第２節　管理区域の管理

（管理区域の構造等）

第30条　情報セキュリティ管理者は、情報システムを構成する基幹機器の設置や電磁的記録媒体を、防犯及び防災について十分な対策を講じた部屋（情報システム室等）又は保管庫等（以下「管理区域」という。）に保管するよう努めなければならない。

２　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。

３　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は、管理区域内の機器等に、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。

４　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。

（管理区域の入退室管理等）

第31条　情報セキュリティ管理者は、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。

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、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　情報セキュリティ管理者は、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。

４　情報セキュリティ管理者は、重要性分類Ｂ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、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなけ

ればならない。

（機器等の搬入出）

第32条　情報セキュリティ管理者は、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。

２　情報セキュリティ管理者は、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。

第３節　通信回線及び通信回線装置の管理

（通信回線及び通信回線装置の管理）

第33条　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、適正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正に保管しなければならない。

２　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。

３　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。

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

６　統括情報セキュリティ責任者は、重要性分類Ｂ以上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節　職員等の利用する端末や電磁的記録媒体等の管理

（職員等の利用する端末や電磁的記録媒体等の管理）

第34条　情報セキュリティ管理者は、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るよう努めなければならない。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　情報セキュリティ管理者は、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、生体認証等複数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。

３　情報セキュリティ管理者は、マイナンバー利用事務系では知識、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（多要素認証）を行うよう設定しなければならない。

第６章　人的セキュリティ

第１節　職員等の遵守事項

（情報セキュリティポリシー等の遵守）

第35条　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。

（業務以外の目的での使用の禁止）

第36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。

（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）

第37条　ＣＩＳＯは、重要性分類Ｂ以上の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

２　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。

３　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。

（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）

第38条　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統括情報セキュリティ責任者が行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得て利用することができる。

２　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に関する規定を遵守しなければならない。

（持ち出し及び持ち込みの記録）

第39条　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。

（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）

第40条　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管理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41条　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、適正な措置を講じなければならない。

（退職時等の遵守事項）

第42条　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。

（会計年度任用職員等への対応）

第43条　情報セキュリティ管理者は、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、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　情報セキュリティ管理者は、会計年度任用職員等の採用の際、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。

３　情報セキュリティ管理者は、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。

（情報セキュリティポリシー等の掲示）

第44条　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。

（外部委託事業者に対する説明）

第45条　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。

第２節　研修・訓練

（情報セキュリティに関する研修・訓練）

第46条　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。

（研修計画の策定及び実施）

第47条　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、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。

（緊急時対応訓練）

第48条　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。

第３節　情報セキュリティインシデントの報告

（庁内での情報セキュリティインシデントの報告）

第49条　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の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管理者は、速やかに統括情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。

３　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に報告しなければならない。

（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）

第50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。

２　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セキュリティ責任者に報告しなければならない。

３　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に報告しなければならない。

（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）

第51条　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。

第４節　ＩＤ及びパスワード等の管理

（ＩＣカード等の取扱い）

第52条　職員等は、自己の管理するＩＣカード等に関し、次の各号に掲げる事項を遵守しなければならない。

(1)　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。

(2)　業務上必要のないときは、ＩＣカード等をカードリーダ又はパソコン等の端末のスロット等から抜いておかなければならない。

(3)　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セキュリティ管理者に通報し、指示に従わなければならない。

２　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。

３　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。

（ＩＤの取扱い）

第53条　職員等は、自己の管理するＩＤに関し、次の各号に掲げる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54条　職員等は、自己の管理するパスワードに関し、次の各号に掲げる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。

(4)　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。

(5)　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。

(6)　仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

(7)　サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

(8)　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。）

第７章　技術的セキュリティ

第１節　コンピュータ及びネットワークの管理

（文書サーバの設定等）

第55条　情報セキュリティ管理者は、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。

２　情報セキュリティ管理者は、文書サーバを課等の単位で構成し、職員等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。

３　情報セキュリティ管理者は、住民の個人情報、人事記録等、特定の職員等しか取り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。

（バックアップの実施）

第56条　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。

（他団体との情報システムに関する情報等の交換）

第57条　情報セキュリティ管理者は、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。

（システム管理記録及び作業の確認）

第58条　情報セキュリティ管理者は、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。

２　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正に管理しなければならない。

３　統括情報セキュリティ責任者、情報セキュリティ管理者及び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。

（情報システム仕様書等の管理）

第59条　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、適正に管理しなければならない。

（ログの取得等）

第60条　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。

２　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、適正にログを管理しなければならない。

３　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。

（障害記録）

第61条　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、適正に保存しなければならない。

（ネットワークの接続制御、経路制御等）

第62条　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。

２　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、ネットワークに適正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等）

第63条　情報セキュリティ管理者は、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。

（外部ネットワークとの接続制限等）

第64条　情報セキュリティ管理者は、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。

２　情報セキュリティ管理者は、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。

３　情報セキュリティ管理者は、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。

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

５　情報セキュリティ管理者は、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。

（複合機のセキュリティ管理）

第65条　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、適正なセキュリティ要件を策定しなければならない。

２　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正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。

３　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66条　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講じなければならない。

（無線ＬＡＮ及びネットワークの盗聴対策）

第67条　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。

２　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。

（電子メールのセキュリティ管理）

第68条　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。
２　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。
３　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。
４　統括情報セキュリティ責任者は、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。
（電子メールの利用制限）
第69条　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。
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、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。
４　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。
５　職員等は、ウェブで利用できる電子メール、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。
（電子署名・暗号化）
第70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、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。
２　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。
３　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。
（無許可ソフトウェアの導入等の禁止）
第71条　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。
２　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セキュリティ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。
３　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。
（機器構成の変更の制限）
第72条　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。
２　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、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73条　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やモバイル端末を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74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正な措置を求めなければならない。

第２節　アクセス制御

（アクセス制御）

第75条　統括情報セキュリティ責任者又は情報セキュリティ管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

（利用者ＩＤの取扱い）

第76条　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。

２　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、統括情報セキュリティ責任者又は情報セキュリティ管理者に通知しなければならない。

３　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。

（特権を付与されたＩＤの管理等）

第77条　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。

２　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セキュリティ管理者が指名し、ＣＩＳＯが認めた者でなければならない。

３　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及び情報セキュリティ管理者に通知しなければならない。

４　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。

５　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。

６　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。

（職員等による外部からのアクセス等の制限）

第78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セキュリティ管理者の許可を得なければならない。

2　統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

3　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。

4　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。

5　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。

6　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、情報セキュリティ管理者の許可を得るか、若しくは情報セキュリティ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　統括情報セキュリティ責任者は、公衆通信回線（公衆無線ＬＡＮ等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（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。

（ログイン時の表示等）

第79条　情報セキュリティ管理者は、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及びログイン・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。

（認証情報の管理）

第80条　統括情報セキュリティ責任者又は情報セキュリティ管理者は、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　統括情報セキュリティ責任者又は情報セキュリティ管理者は、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。

3　統括情報セキュリティ責任者又は情報セキュリティ管理者は、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。

（特権による接続時間の制限）

第81条　情報セキュリティ管理者は、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。

第３節　システム開発、導入、保守等

（情報システムの調達）

第82条　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　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。

（システム開発における責任者及び作業者の特定）

第83条　情報セキュリティ管理者は、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。

（システム開発における責任者及び作業者のＩＤの管理）

第84条　情報セキュリティ管理者は、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。

２　情報セキュリティ管理者は、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。

（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）

第85条　情報セキュリティ管理者は、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。

２　情報セキュリティ管理者は、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。

（開発環境と運用環境の分離及び移行手順の明確化）

第86条　情報セキュリティ管理者は、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。

２　情報セキュリティ管理者は、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。

３　情報セキュリティ管理者は、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。

（テスト）

第87条　情報セキュリティ管理者は、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。

２　情報セキュリティ管理者は、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。

３　情報セキュリティ管理者は、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。

４　情報セキュリティ管理者は、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。

（システム開発・保守に関連する資料等の整備・保管）

第88条　情報セキュリティ管理者は、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正に整備・保管しなければならない。

２　情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

３　情報セキュリティ管理者は、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89条　情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲及び妥当性のチェック機能並びに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　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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。

（情報システムの変更管理）

第90条　情報セキュリティ管理者は、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。

（開発・保守用のソフトウェアの更新等）

第91条　情報セキュリティ管理者は、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。

（システム更新又は統合時の検証等）

第92条　情報セキュリティ管理者は、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。

第４節　不正プログラム対策

（統括情報セキュリティ責任者の措置事項）

第93条　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、次の各号に掲げる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)　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。
(5)　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。
(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ない。
(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。

（情報セキュリティ管理者の措置事項）

第94条　情報セキュリティ管理者は、不正プログラム対策に関し、次の各号に掲げる事項を措置しなければならない。
(1)　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及び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。

（職員等の遵守事項）

第95条　職員等は、不正プログラム対策に関し、次の各号に掲げる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、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。
(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、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)　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。
(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、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。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてＬＡＮケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

（専門家の支援体制）

第96条　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。

第５節　不正アクセス対策

（統括情報セキュリティ責任者の措置事項）

第97条　統括情報セキュリティ責任者は、不正アクセス対策として、次の各号に掲げる事項を措置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セキュリティ管理者へ通報するよう、設定しなければならない。

(4)　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正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。

（攻撃への対処）

第98条　ＣＩＳＯ及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、国、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。

（記録の保存）

第99条　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。

（内部からの攻撃）

第100条　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。

（職員等による不正アクセス）

第101条　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等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

（サービス不能攻撃）

第102条　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103条　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は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

第６節　セキュリティ情報の収集

（不正プログラム等のセキュリティ情報の収集・周知）

第104条　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　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　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章　運用

第１節　情報システムの監視

（情報システムの監視）

第105条　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。

２　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、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。

第２節　情報セキュリティポリシーの遵守状況の確認

（遵守状況の確認及び対処）

第106条　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。

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　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。

（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）

第107条　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。

第３節　侵害時の対応等

（事件・事故発生時の報告）

第108条　職員等は、情報資産に関する事件・事故（システム上の欠陥及び誤動作を含む。）を発見した場合、速やかに情報セキュリティ管理者に報告しなければならない。

２　情報セキュリティ管理者は、事件・事故の内容を統括情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない。

３　統括情報セキュリティ責任者は、前項の報告に情報セキュリティの侵害を認めた場合、ＣＩＳＯに報告しなければならない。

４　ＣＩＳＯは、情報セキュリティに係る重大な判断が必要であると認めた場合、必要に応じ警察等の関係機関と連携を図るものとする。

（事件・事故発生時の対応）

第109条　職員等は、情報資産に関する事件・事故を発見した場合、次の各号に掲げる措置を講じなければならない。

(1)　現状の維持及び関係者への連絡

(2)　証拠の保全及び被害拡大の防止

２　情報セキュリティ管理者は、前条第１項の報告を受けた場合、次の各号に掲げる措置を講じなければならない。

(1)　事件・事故の原因及び被害状況の調査

(2)　証拠の収集

(3)　被害への対応及び復旧

(4)　事件・事故の経過の記録

(5)　再発防止策の検討及び実施

（事件・事故発生時の手順）

第110条　情報セキュリティ管理者は、事件・事故発生時における必要な措置を迅速かつ円滑に実施するため、所管する情報システムに係る実施手順に次の各号に掲げる事項を定めなければならない。

(1)　事件・事故発生時の連絡先及び報告経路に関すること。

(2)　事件・事故発生時の対応に関すること。

(3)　情報システムの緊急停止に関すること。

(4)　ネットワークに接続された情報システムの緊急切断に関すること。

(5)　事件・事故の記録及び報告に関すること。

第４節　例外措置

（例外措置の許可）

第111条　情報セキュリティ管理者は、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、例外措置を講じることができる。

（緊急時の例外措置）

第112条　情報セキュリティ管理者は、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。

（例外措置の申請書の管理）

第113条　ＣＩＳＯは、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

第９章　法令遵守

（法令の遵守）

第114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、次の各号に掲げる法令のほか関係法令等を遵守し、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)　久御山町個人情報保護条例（平成13年久御山町条例第12号）
(8)　久御山町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に基づく個人番号の利用及び特定個人情報の提供に関する条例（平成27年久御山町条例第23号）

第10章　情報セキュリティに関する違反に対する対応

（懲戒処分）

第115条　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。

（違反時の対応）

第116条　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、速やかに次の各号に掲げる措置を講じなければならない。

(1)　統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
(2)　情報セキュリティ管理者が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ管理者

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若しくは情報システムを使用する権利を停止又は剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止又は剥奪した旨をＣＩＳＯ及び当該職員等が所属する課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。

第11章　外部サービスの利用

第１節　外部委託

（外部委託事業者の選定基準）

第117条　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。

２　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。

（契約項目）

第118条　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各号に掲げる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。

(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)　外部委託事業者の責任者、委託内容、作業者の所属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)　外部委託事業者にアクセスを許可する情報の種類と範囲及びアクセス方法

(5)　外部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)　町による監査及び検査

(12)　町による情報セキュリティ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）

（確認・措置等）

第119条　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、前条の契約に基づき措置を実施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。

第２節　約款による外部サービスの利用

（約款による外部サービスの利用に係る規定の整備）

第120条　情報セキュリティ管理者は、次の各号に掲げる事項を含む約款による外部サービ

スの利用に関する規定を整備しなければならない。また、当該サービスの利用において、重要性分類Ｂ以上の情報が取り扱われないように規定しなければならない。

(1)　約款によるサービスを利用して良い範囲

(2)　業務により利用する約款による外部サービス

(3)　利用手続及び運用手順

（約款による外部サービスの利用における対策の実施）

第121条　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、適正な措置を講じた上で利用しなければならない。

第３節　ソーシャルメディアサービスの利用

（ソーシャルメディアサービスの利用）

第122条　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、次の各号に掲げる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によるなりすまし対策を実施すること。

(2)　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ＩＣカード等）等を適正に管理するなどの方法での不正アクセス対策を実施すること。

２　重要性分類Ｂ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。

３　情報セキュリティ管理者は、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。

４　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。

第４節　クラウドサービスの利用

（クラウドサービスの利用）

第123条　情報セキュリティ管理者は、クラウドサービス（民間事業者が提供するものに限らず、本町が自ら提供するもの等を含む。以下同じ。）を利用するに当たり、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。

２　情報セキュリティ管理者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。

３　情報セキュリティ管理者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件としなければならない。

４　情報セキュリティ管理者は、クラウドサービスの特性を考慮した上で、クラウドサービス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セキュリティ要件を定めなければならない。

５　情報セキュリティ管理者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

第12章　評価・見直し

第１節　監査

（監査）

第124条　ＣＩＳＯは、情報セキュリティポリシーの遵守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　監査の結果発見された問題点は、情報セキュリティポリシーに基づき是正しなければならない。

３　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。

４　ＣＩＳＯ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。

第２節　自己点検

第125条　情報セキュリティ管理者は、必要に応じて情報セキュリティポリシーの遵守状況を自ら点検し、その結果を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。

２　点検の際に問題点を発見した場合は、情報セキュリティポリシーに基づき是正しなければならない。

第３節　情報セキュリティポリシー及び関係規程等の見直し

（情報セキュリティポリシー及び関係規程等の見直し）

第126条　ＣＩＳＯは、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、関係規程等について定期的に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。