菊陽町

情報セキュリティポリシー

菊陽町

令和７年３月１１日　策定

序 菊陽町情報セキュリティポリシーの構成

菊陽町情報セキュリティポリシーとは、菊陽町が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、菊陽町が所掌する情報資産に関する業務に携わる全職員、会計年度任用職員（以下「職員等」という。)及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と情報資産を取り巻く状況の変化に依存する部分(対策基準)に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

① 情報セキュリティ基本方針

② 情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする(下表参照)。

情報セキュリティポリシーの構成

<table>
<tr><th>文 書 名</th><th></th><th>内 容</th></tr>
<tr><td rowspan="2">情報セキュリティポリシー</td><td>情報セキュリティ基本方針</td><td>情報セキュリティ対策に関する統一的かつ基本的な方針。</td></tr>
<tr><td>情報セキュリティ対策基準</td><td>情報セキュリティ対策基準</td></tr>
<tr><td colspan="2">情報セキュリティ実施手順</td><td>ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。</td></tr>
</table>

目次

情報セキュリティ基本方針

１　目的

本基本方針は、本町が保有する情報資産の機密性、完全性及び可用性を維持するため、本町が実施する情報セキュリティ対策について基本的な事項を定めることにより、町民の財産、プライバシー等を守るとともに、情報システムを活用した住民サービスの向上と行政事務の効率化を図ることを目的とする。

２　定義

（１）　ネットワーク

コンピュータ（以下「端末」という。）等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）　情報システム

端末、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（３）　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（４）　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（５）　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（７）　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（８）　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税又は防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（９）　ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等、総合行政ネットワーク（Local Government Wide Area Network。以下「LGWAN」という。）に接続された情報システム及びその情報システムで取り扱うデータをいう。

（１０）　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１１）　情報経路の分割

ＬＧＷＡＮ接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（１２）　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

（１３）　行政委員会

教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会をいう。

３　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施す

る。

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

（2）情報資産の無断持出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4　適用範囲

（1）行政機関の範囲

本基本方針が適用される行政機関は、町長及び行政委員会とする。ただし、各町立小学校及び中学校（菊陽町立菊陽中部小学校における学校事務センターを除く。）は対象外とする。

（2）情報資産の範囲

本基本方針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、情報システム及びこれらに関する設備、電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

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

5　職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当

たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

６　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

（１）組織体制

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

（２）情報資産の分類と管理

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

（３）情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②ＬGWAN接続系においては、ＬGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、インターネット接続口を熊本県自治体情報セキュリティクラウドとする。ただし、Web会議など、大容量の通信を必要とするものについては、この限りではない。

（４）物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員等の端末等の管理について、物理的な対策を講じる。

（５）人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育

及び啓発を行う等の人的な対策を講じる。

（6）技術的セキュリティ

端末等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（7）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（8）業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づく措置を講じる。

外部サービスを利用する場合には、利用に関わる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

８　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

上記６から８までに規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。

情報セキュリティ対策基準

１　対象範囲

本情報セキュリティ対策基準が適用される範囲は、次のとおりとする。

（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（特別職を含む。）、行政委員会とする。ただし、各町立小学校及び中学校（菊陽町立菊陽中部小学校における学校事務センターを除く。）は対象外とする。

なお、各町立小学校及び中学校における教育のために用いるネットワーク及びシステム等は、この情報セキュリティポリシーの対象となるネットワーク及び情報システムと物理的に分けなければならない。

（２）情報資産の範囲

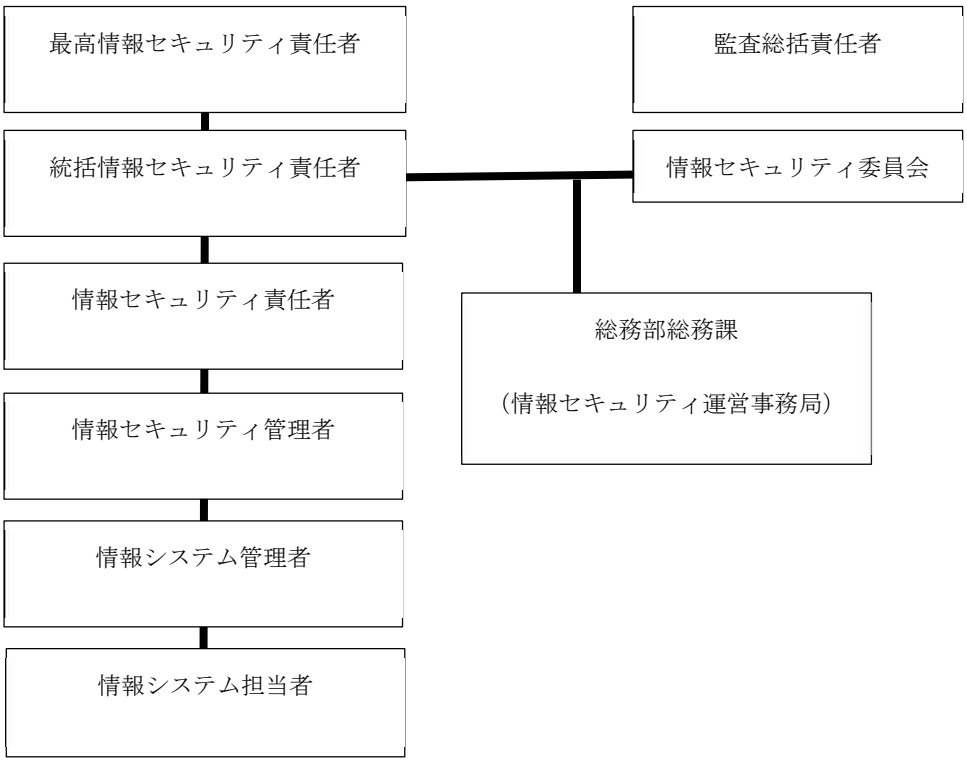
本対策基準が対象とする情報資産は、次のとおりとする。

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ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク構成図等のシステム関連文書

２　組織体制



体制内役職名	該当者
最高情報セキュリティ責任者 （CISO: Chief Information Security Officer、以下「CISO」という。））	副町長
統括情報セキュリティ責任者	総務部長
情報セキュリティ責任者	各部の長、行政委員会の長
情報セキュリティ管理者	各課等の長、行政委員会の課室長等
情報システム管理者	総務課長、総合政策課長、財政課長、町民課長、税務課長、健康・保険課長、こども家庭相談課長、介護保険課長、農政課長、建設課長、下水道課長、施設整備課長、農業委員会事務局長

情報システム担当者	情報システム管理者配下の係長等
情報セキュリティ委員会	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、CISO の指名する者
情報セキュリティ運営事務局	総務部総務課

（1）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。

②CISO 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ものとする。

③CISO 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

①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。

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、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、情報セキュリティ管理者及び情報システム管理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。

（3）情報セキュリティ責任者

①各部の長、行政委員会の長及び会計管理者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、その所管する部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。

③情報セキュリティ責任者は、その所管する部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。

④情報セキュリティ責任者は、その所管する部等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員、会計年度任用職員及び委託事業者（以下「職員等」という。）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

①各課室等の長、行政委員会の課室長等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、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。

③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

①各情報システムの契約担当課室長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対策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。

（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

①情報セキュリティ委員会は、CISOを委員長に、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CISOが指名するメンバーで構成する。

②委員長は、情報セキュリティ委員会に関する一切の事務を統括し情報セキュリ

ティ委員会を代表する。この場合において、委員長に事故がある時は統括情報セキュリティ責任者がその職務を代理する。

③情報セキュリティ委員会に内部監査班を設置し、CISO の指名する者を監査統括責任者とする。情報セキュリティ委員会は、本町の情報セキュリティ対策を統一的に行うため、情報セキュリティポリシーの運用、情報セキュリティ事故・事件への対応等、情報セキュリティに関する重要な事項を審議・決定する。

④情報セキュリティ委員会は、毎年度、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。

⑤情報セキュリティ委員会の庶務は、総務部総務課に設置された情報セキュリティ運営事務局において処理する。

（８）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情報セキュリティ監査において、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。

（９）CSIRT の設置・役割

①CISO は、CSIRT に所属する職員を選任し、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を定めること。

②CISO 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しなければならない。

③CISO 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、熊本県等

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。

⑥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なうこと。

3　情報資産の分類と管理方法

（1）情報資産の分類

対象となるネットワーク及び情報システムの情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

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３A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」(平成 23 年 4 月 1 日内閣総理大臣決定)に定める秘密文書に相当する文書又は漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	・機密性３A、３B の情報資産について、支給されたマイナンバー利用事務系端末以外での作業の原則禁止 ・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収納 ・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。テレワークにて情報資産を扱うときには公共無線の使用禁止 ・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３B	行政事務で取り扱う情報資産のうち、自治体機密性３A に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
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及び機密性３の情報資産以外の情報資産	―

機密性３A 又は３B の資産は鍵付きの書庫に保存する。またデジタル資産の場合は原則マイナンバー利用事務系端末かサーバで取り扱い、取り外し持ち運び可能なリムーバブル

メディアには保管してはならない。

機密性２の資産は来庁者が容易に触れることのない場所に保管する。またデジタル資産の場合はLGWAN系かマイナンバー利用事務系で取り扱う。

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。）を及ぼす恐れがある情報資産	・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の情報資産以外の情報資産	－

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、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	－

機密性２かつ可用性１のデジタル資産は情報セキュリティ管理者の責任の元、各課等の所有するリムーバブルメディアに保管することができる。

（２）情報資産の管理

①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、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　情報セキュリティ管理者は、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、情報資産の重要性分類を表示し、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　職員等が作成した情報資産を入手した者は、本町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　職員等以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、情報セキュリティ管理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、情報資産を適正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、重要な情報資産（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以上の情報資産を送信する者は、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。

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。

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。

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。

⑩情報資産の廃棄等

ア　情報資産の廃棄やリース返却等を行う者は、情報を記載している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

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

ウ　情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の確認を得なければならない。

４　情報システム全体の強靭性の向上

（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。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、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移送を可能とする。

②情報のアクセス及び持出しにおける対策

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。

イ　情報の持出し不可設定

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

①LGWAN 接続系とインターネット接続系の分離

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 への不適正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熊本県自治体情報セキュリティクラウドに参加するとともに、関係省庁や熊本県と連携しながら、情報セキュリティ対策を推進しなければならない。

5　物理的セキュリティ

（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、サーバ等の取付けを行う場合には、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。

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、住民サービスに関するサーバ及びその他の基幹サーバについては、同一データを保持できるよう冗長化することを原則とする。

イ　情報システム管理者は、冗長化した基幹サーバについて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は、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。

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、配線収納管等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、連携し速やかに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）は、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。

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、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当たり、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。

⑥庁外への機器の設置

統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、必要に応じ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、機器の廃棄、リース返却等をする場合には、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。

（２）管理区域（サーバ室等）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「サーバ室」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、管理区域を地下及び１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無窓の外壁にしなければならない。なお、窓がある場合は侵入対策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、サーバ室内の機器等には、転倒及び落下防止等の耐震対策、防火装置、防水装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ものに制限し、ICカード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は、当該情報システムに関連しない端末、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。

③機器等の搬入出

ア　情報システム管理者は、機器等を搬入する場合には、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。

イ　情報システム管理者は、外部委託事業者がサーバ室の機器等の搬入出を行う場合には、職員等を立ち会わせなければならない。

（３）通信回線及び通信回線装置の管理

①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、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、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。

③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は必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

④統括情報セキュリティ責任者は、行政系のネットワークを LGWAN に集約するように努めなければならない。

⑤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。

⑥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。

⑦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に関する事項を含む実施手順を定めなければならない。また、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。

⑧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、回線を冗長構成等の措置を講じなければならない。

（４）職員等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、盗難防止のため、執務室等で利用する端末のワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。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、ある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入力設定を解除してはならない。

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２つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。

⑤情報システム管理者は、端末や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。同様に、電磁的記録媒体についても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。

⑥情報システム管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

６　人的セキュリティ

（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

全ての職員等は、情報セキュリティ管理者の指示に従い、情報セキュリティポリ

シーに定められている事項を遵守しなければならない。

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については、速やかに情報セキュリティ管理者に相談し、指示等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　端末や電磁的記録媒体等の持出し及び外部における情報処理作業の制限

（ア）CISOは、重要な情報資産（機密性２以上、完全性２又は可用性２の情報）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　支給以外の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、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。

（イ）職員等は、支給以外の端末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は安全管理措置に関する規定を遵守しなければならない。

オ　持出し及び持ち込みの記録

情報セキュリティ管理者は、端末及び電磁的記録媒体等の持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　端末におけるセキュリティ設定変更の禁止

職員等は、端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

キ　机上の端末等の管理

職員等は、端末や電磁的記録媒体、情報が印刷された文書等が、第三者に使用又は情報セキュリティ管理者の許可なく情報が閲覧されることがないように、離席時に端末のロックや電磁的記録媒体、文書等が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。

ク　退職時等の遵守事項

異動、退職等により職員等が業務を離籍する場合には、利用していた情報資産を、返却しなければならない。また、業務上知り得た情報はその後も漏らしてはならない。

②会計年度任用職員及び臨時的認証職員等への対応

ア　情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、会計年度任用職員及び臨時的認証職員等に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員及び臨時的認証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。

イ　情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、会計年度認証職員及び臨時的認証職員等の採用の際、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「情報セキュリティポリシー遵守同意書」への署名を求めるものとする。

ウ　インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、会計年度任用職員及び臨時的認証職員等に端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、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、情報セキュリティポリシー及び実施手順は、職員等が常に閲覧できるよう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には、再委託事業者を含めて、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。

（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研修計画の立案及び実施

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、職員等は適時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　新規採用の職員等に対しては、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　情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、統括情報責任者及び情報セキュリティ責任者に対して、報告しなければならない。

カ　統括情報セキュリティ責任者は、所管する課室等の研修の実施状況を分析、評価し、CISO に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

キ　CISO は、毎年度１回、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、必要に応じ緊急時対応を想定した訓練を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、訓練実施の範囲等を定め、効果的に実施できるようにしなければならない。

④研修・訓練への参加

情報セキュリティに関する研修・訓練には、全ての職員等が参加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報告

①庁内で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、「インシデント報告書（IT 障害)」により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。

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。

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処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 は、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。

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。

（4）ID 及びパスワード等の管理

①IC 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又は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。

②ID 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　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。

カ　サーバ、ネットワーク機器にパスワードを記憶させてはならない。端末については情報セキュリティ実施手順に定める。

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。

7　技術的セキュリティ

（1）端末及びネットワークの管理

①ファイルサーバの設定等

ア　情報システム管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。

イ　情報システム管理者は、ファイル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、特定の者しか取り扱えないデータについては、別途ディレクトリを作成する等の措置を講じ、同一部署であっても、担当職員以外の者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は、サーバの冗長化対策にかかわらず、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には、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は、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、作業内容についての記録を作成し、詐取、改ざん等がないように適正に管理し、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について、記録媒体にかかわらず、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。

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ために取得した記録は、詐取、改ざん、誤消去等されないよう適正に管理し、一定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、適正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、適正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、ネットワークに適正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は、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、庁内のネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

イ　情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

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

エ　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。

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。

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。

⑫IoT 機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、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には、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

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）が行われることがないよう、電子メールサーバの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、大量のスパムメール等の受信又は送信を検知

した場合には、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には上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

エ　統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量には上限を設定し、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。

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

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、情報セキュリティ管理者に報告しなければならない。

オ　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。ただし、ネットワークストレージサービスについて、事業者等とデータのやり取りをするなど業務上必要な場合はこの限りではない。

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、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。

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、端末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、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、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、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

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　情報セキュリティ管理者は、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　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。

㉑Web 会議サービスの利用時の対策

ア　統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を

定めなければならない。

イ　職員等は、本町の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

ウ　職員等は、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。

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

㉒ソーシャルメディアサービスの利用

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係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すること。

（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（ハードディスク、USB メモリ、紙等）など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、本町の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

（2）アクセス制御

①アクセス制御等

ア　アクセス制御

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、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・抹消等の情報管理及び職員等の異動・出向・退職者に伴う利用者 ID の取扱等の方法を定めなければならない。

（イ）職員等は、業務上の必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

（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。

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。

（ウ）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。

（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、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。

（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。

（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の定めた方法でのみ行うものとする。

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

ウ　統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

エ　統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

オ　統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、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、持ち込み、又は外部から持ち帰った端末を庁内のネットワークに接続する前に、端末ウイルスに感染していないことを確認した後に接続しなければならない。

キ　統括情報セキュリティ責任者は、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、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。

③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、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。

（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が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　情報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方針、手順等を記載した規則を着手前に策定し開発に適用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、それ以外のものを利用させてはならない。

（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、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可能な限り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　導入前の試験調整

（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稼働試験を行わなければならない。

（イ）情報システム管理者は、稼働試験を行う場合、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の高い生データを、稼働試験用の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稼働試験を行う場合、開発した組織と導入する組織が、それぞれ独立した稼働試験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

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正に整備・保管しなければならない。

イ　情報システム管理者は、稼働試験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正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

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、故意若しくは過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

ウ　情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

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、プログラム仕様書等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ない。

（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端末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害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端末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　端末ウイルス等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端末には、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。

ウ　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

エ　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、町が管理している媒体以外を職員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　端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

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

ウ　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削

除しなければならない。

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

オ　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は無害化しなければならない。

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

キ　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、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。

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。

（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　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。

②攻撃への対処

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

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、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、標的型攻撃による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等の対策（内部対策及び出口対策）を講じなければならない。

（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、セキュリティ侵害等を未然に防止するための対策を速やかに講じなければならない。

８　運用

（１）情報システムの監視

①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。

②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。

③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。

（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、適正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は、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端末及び電磁的記録媒体のログ、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なわなければならない。

イ　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

統括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。

（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。

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。

（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、行政事務の遂行のため緊急を要する場合であって、例外措置を実施することが不可避の場合には、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。

（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 28 年法律第 31 号）

⑦ 菊陽町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 年菊陽町条例第 24 号）

⑧　菊陽町個人情報保護法施行条例（令和 5 年菊陽町条例第 2 号）

（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、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室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。

イ　情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員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、適正な措置を求めなければならない。

ウ　情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員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、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を 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。

9　業務委託とクラウドサービスの利用

（1）業務委託

①業務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当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない

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業務委託実施前の対策

ア　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

（ア）委託する業務内容の特定

（イ）委託事業者の選定条件を含む仕様の策定

（ウ）仕様に基づく委託事業者の選定

（エ）情報セキュリティ要件を明記した契約の締結（契約項目）

重要な情報資産を取り扱う業務を委託する場合には、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等に係る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

・委託事業者の責任者、委託内容、作業者の所属、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、アクセス方法の明確化など、情報のライフサイクル全般での管理方法

・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委託事業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)

（オ）委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

イ　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

（ア）仕様に準拠した提案

（イ）契約の締結

（ウ）委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結

③業務委託実施期間中の対策

ア　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。

（ア）委託判断基準に従った重要情報の提供

（イ）契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

（ウ）統括情報セキュリティ責任者へ措置内容の報告（重要度に応じてCISOに報告）

（エ）委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

イ　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間にお

いて、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア）情報の適正な取扱いのための情報セキュリティ対策

（イ）契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

（ウ）委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

④業務委託終了時の対策

ア　情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

（イ）委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

イ　情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

（イ）提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

（２）クラウドサービスの利用（機密性２以上の情報を取り扱う場合）

①クラウドサービスの選定に係る運用規定の整備

情報セキュリティ管理者は、機密性２以上の情報を取り扱う場合、以下を含む約款による外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。

ア　クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱

いを許可する場所を判断する基準（以下「クラウドサービス利用判断基準」という。）

イ　クラウドサービス提供者の選定基準

ウ　クラウドサービスの利用申請の許可権限者と利用手続

エ　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

②クラウドサービスの利用に係る運用規程の整備

統括情報セキュリティ責任者は、機密性２以上の情報を取り扱う場合、以下を含むクラウドサービス（機密性２以上の情報を取り扱う場合）の利用に関する規程を整備しなければならない。

ア　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

イ　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

ウ　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

(ア)クラウドサービスの利用終了時における対策

(イ)クラウドサービスで取り扱った情報の廃棄

(ウ)クラウドサービスの利用のために作成したアカウントの廃棄

③クラウドサービスの選定

ア　情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。

イ　情報セキュリティ責任者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提

供者を選定すること。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。

（ア）クラウドサービスの利用を通じて本町が取り扱う情報のクラウドサービス提供者における目的外利用の禁止

（イ）クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制

（ウ）クラウドサービスの提供に当たり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、本町の意図しない変更が加えられないための管理体制

（エ）クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

ウ　情報セキュリティ責任者は、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、クラウドサービス提供者の選定条件に含めなければならない。

エ　情報セキュリティ責任者は、クラウドサービスの利用を通じて本町が取り扱う情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めなければならない。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

オ　情報セキュリティ責任者は、クラウドサービスの利用を通じて本町が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し、必要に応じて本町の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

カ　情報セキュリティ責任者は、クラウドサービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保されるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本町に提供し、本町の承認を受けるよう、クラウドサービス提供者の選定条件に含めること。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

キ　情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、クラウドサービスを選定すること。また、原則としてクラウドサービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めることとする。

ク　情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めなければならない。

（ア）クラウドサービスに求める情報セキュリティ対策

（イ）クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

（ウ）クラウドサービスに求めるサービスレベル

ケ　統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況などから、クラウドサービス提供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すること。

④クラウドサービスの利用に係る調達・契約

ア　情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

イ　情報セキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認

し、利用承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。

⑤クラウドサービスの利用承認

ア　情報セキュリティ責任者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。

イ　利用申請の許可権限者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定すること。

ウ　利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名すること。

⑥クラウドサービスを利用した情報システムの導入・構築時の対策

ア　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

（ア）不正なアクセスを防止するためのアクセス制御

（イ）取り扱う情報の機密性保護のための暗号化

（ウ）開発時におけるセキュリティ対策

（エ）設計・設定時の誤りの防止

イ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

（ア）クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

（イ）クラウドサービスを利用した情報システムの運用・監視中における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

（ウ）利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

ウ　クラウドサービス管理者は、前項において定める規定に対し、構築時に実施状

況を確認・記録しなければならない。

⑦クラウドサービスを利用した情報システムの運用・保守時の対策

ア　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

（ア）クラウドサービス利用方針の規定

（イ）クラウドサービス利用に必要な教育

（ウ）取り扱う資産の管理

（エ）不正アクセスを防止するためのアクセス制御

（オ）取り扱う情報の機密性保護のための暗号化

（カ）クラウドサービス内の通信の制御

（キ）設計・設定時の誤りの防止

（ク）クラウドサービスを利用した情報システムの事業継続

イ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な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は、クラウドサービスでの特性や責任分界点に係る考え方を踏まえ、クラウドサービスで発生したインシデントを認知した際の対処手順を整備しなければならない。

エ　クラウドサービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

⑧クラウドサービスを利用した情報システムの更改・廃棄時の対策

ア　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。

（ア）クラウドサービスの利用終了時における対策

（イ）クラウドサービスで取り扱った情報の廃棄

（ウ）クラウドサービスの利用のために作成したアカウントの廃棄

イ　クラウドサービス管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認・記録しなければならない。

（３）クラウドサービスの利用（機密性２以上の情報を取り扱わない場合）

①クラウドサービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含むクラウドサービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定を整備しなければならない。

ア　クラウドサービスを利用可能な業務の範囲

イ　クラウドサービスの利用申請の許可権限者と利用手続

ウ　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

エ　クラウドサービスの利用の運用手順

②クラウド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、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性２以上の情報を取り扱わない場合のクラウドサービスの利用を申請しなければならない。また、承認時に指名されたクラウドサービス管理者は、当該クラウドサービスの利用において適切な措置を講じなければならない。

イ　情報セキュリティ責任者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。また、承認したクラウドサービスを記録しなければならない。

１０　評価・見直し

（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委託事業者に対する監査

事業者に業務委託している場合、情報セキュリティ監査統括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

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正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。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

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。

（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、毎年及び必要に応じて自己点検を実施しなければならない。

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。

（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。