○五ヶ瀬町情報セキュリティ対策に関する規則

平成16年12月20日五ヶ瀬町規則第13号

第１章　情報セキュリティ対策基本方針

（趣旨）

第１条　五ヶ瀬町の各情報システムが取り扱う情報には、町民の個人情報のみならず行政運営上重要な情報が多数あり、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御するため五ヶ瀬町情報セキュリティ対策に関する規則を定め、事務の安定的な運営に資するとともに、町民の個人情報の保護に万全の体制を図り、五ヶ瀬町に対する町民からの信頼の向上に寄与することを目的とする。

２　本規則は、地方公共団体情報システムの標準化、ガバメントクラウドの利用その他のクラウドサービスの活用を前提とした情報セキュリティ対策についても適用するものとする。

（定義）

第２条　この規則において、用語の定義は、それぞれ当該各号に定めるところによる。

（１）　ネットワーク　町長その他の町の執行機関及びその他の施設を相互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）並びに記録媒体で構成され、処理を行う仕組みをいう。

（２）　情報システム　電子計算組織（ネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

（３）　情報資産　ネットワーク及び情報システムの開発と運用に係る全てのデータ並びに取り扱う全てのデータをいう。なお、紙等の有体物に出力された情報も含むものとする。

（４）　情報セキュリティ　情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（５）　機密性　対象資産にアクセスすることを認められた者だけが、対象資産にアクセスできる状態を確保することをいう。

（６）　完全性　対象資産が破壊、改ざん、消去又は不正なデータがない状態を維持し、データの正当性、正確性、一貫性等を確保することをいう。

（７）　可用性　対象資産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、対象資産にアクセスできる状態を確保することをいう。

（８）　特定個人情報　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（以下「番号法」という。）第２条に規定する、個人番号をその内容に含む個人情報ファイルを

いう。

（９） 個人番号利用事務　番号法第２条に規定する個人番号を利用して処理する事務をいう。

(10) クラウドサービス　インターネット等のネットワークを通じて、サーバ、ストレージ、ソフトウェアその他の情報処理機能を提供するサービスをいう。

(11) ガバメントクラウド　国が整備する政府共通のクラウドサービス基盤をいう。

（本規則の位置付けと職員等の義務）

第３条　本規則は、五ヶ瀬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であり、情報セキュリティ対策の頂点に位置するものである。

２　五ヶ瀬町長をはじめとして、五ヶ瀬町が所掌する情報資産に関する業務に携わる全ての職員等及び部外委託者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって本規則を遵守する義務を負うものとする。

３　クラウドサービス又は業務委託を利用して情報資産を取り扱う場合であっても、当該情報資産の最終的な管理責任は五ヶ瀬町に帰属するものとする。

（情報セキュリティ管理体制）

第４条　五ヶ瀬町の情報資産について、所属長が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

２　前項の管理体制は、庁内の情報システムに限らず、クラウドサービスを利用して取り扱う情報資産及び業務委託先における取扱いについても適用するものとする。

（情報資産の分類）

第５条　情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に応じた取扱制限を別表第１、別表第２及び別表第３に定める。

２　前項の分類は、庁内に存在する情報資産に限らず、クラウドサービスを利用して保存又は処理される情報資産についても適用するものとする。

（情報資産への脅威）

第６条　情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮し、特に認識すべき脅威は次の各号のとおりである。

（１） 部外者による故意の不正アクセス又は不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難等

（２） 職員等及び部外委託者による意図しない操作、故意の不正アクセス又は不正操作によるデー

タやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難並びに規定外のコンピュータ接続によるデータ漏洩等並びにクラウドサービスの利用又は外部委託に伴う設定不備、権限管理の不十分さその他これらに起因する情報漏洩等

（３） 地震、落雷、火災等の災害及び事故、故障等によるサービス及び業務の停止第７条　前条各号の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

（情報セキュリティ対策）

第７条　前条各号の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

（１） 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するための物理的な対策

（２） 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等に本規則の内容を周知徹底する等、十分な教育及び啓発が講じられるために必要な対策

（３） 技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、クラウドサービスの利用及びシステム開発等の外部委託、ネットワークの監視、本規則の遵守状況の確認等の運用面の対策

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策

（情報セキュリティ対策基準の策定）

第８条　五ヶ瀬町の所掌する情報資産について、前条の情報セキュリティ対策を講ずるに当たっては、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

２　前項の情報セキュリティ対策基準は、クラウドサービスの利用及び業務委託を含む情報資産の取扱いを考慮して策定するものとする。

（情報セキュリティ実施手順の策定）

第９条　情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、所属長が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。（クラウドサービスの利用及び業務委託により取り扱う情報資産を含む。）

２　情報セキュリティ実施手順は、公にすることにより五ヶ瀬町の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。

（監査）

第10条　本規則が遵守されていることを検証するため、定期的に監査を行う。

２　前項の監査は、クラウドサービスの利用及び業務委託を含めて実施するものとする。

（評価及び見直し）

第11条　本規則が遵守されていることを検証するため、定期的に情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、本規則の見直しを行うものとする。

２　前項の評価及び見直しは、クラウドサービスの利用、業務委託の状況その他情報セキュリティを取り巻く環境の変化を踏まえて行うものとする。

第２章　五ヶ瀬町行政全般における情報セキュリティ対策基準（第12条―第24条）

（対象範囲）

第12条　本規則が対象とする行政機関の範囲は、町長部局、各行政委員会、教育委員会、議会事務局及び地方公営企業部局とする。

２　各教育機関における教育のために用いるシステム及び職員室等は、この規則の対象となるシステムと物理的に分けなければならない。

３　本対策基準が対象とする情報資産は、次の各号のとおりとする。これには、クラウドサービスを利用して取り扱う情報資産を含むものとする。

（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図等のシステム関連文書

（組織・体制）

第13条　五ヶ瀬町の情報セキュリティ管理については、以下の組織・体制とする。

（１）　最高統括情報責任者

（２）　統括情報システム管理者

（３）　情報セキュリティ管理者

（４）　情報システム担当者

（情報の分類）

第14条　情報の分類については、対象となる情報システム各々の情報の機密性、完全性及び可用性を踏まえ、重要性によって分類しなければならない。

２　情報システムで扱う情報について、第三者が重要性の識別を容易に認識できないよう留意しつつ、適切な管理を行わなければならない。

（情報の管理）

第15条　情報の管理については、次に定めるとおりとする。

（１）　情報の管理責任

ア　管理責任　情報は、当該情報を作成した所属長が管理責任を有する。

イ　利用者の責任　情報を利用する者は、情報の分類に従い利用する責任を有する。

ウ　重要性の効力　情報が複製又は伝送された場合には、当該複製等も分類に基づき管理しなければならない。

（２）　情報の管理方法

ア　情報の管理及び取扱い

（ア）　情報について、それぞれの分類に従い、クラウドサービスを利用して取り扱う場合を含め、アクセス権限を定めるものとする。

（イ）　職員等は、情報の複製を保管場所へ移動する場合、当該保管場所からバックアップのために情報システムの設置個所に戻す場合及び業務上必要な場合には、情報セキュリティ管理者の許可を得たうえで外部への持出または送付をしなければならない。

イ　記録媒体の管理

（ア）　取り出しが可能な記録媒体は、適切な管理を行わなければならない。

（イ）　最終的に確定した情報を記録した記録媒体は、書込禁止措置を行った上で保管しなければならない。

（ウ）　記録媒体に納められた情報は全て別の記録媒体に複製し、当該記録媒体は自然災害を被る可能性が低い地域に別途保管しなければならない。

（エ）　重要な情報（個人情報等）を記録した記録媒体は、耐火、耐熱、耐水及び耐湿対策を講じた施錠可能な場所に保管しなければならない。

（オ）　記録媒体を送る場合は信頼できる者を選定し、複製の禁止及び記録媒体の物理的保護規定を定め、違反した場合の罰則規定を定めなければならない。

ウ　記録媒体の処分

（ア）　記録媒体が不要となった場合は、当該媒体に含まれる重要な情報（個人情報等）は、記録媒

体の初期化など情報を復元できないように消去を行ったうえで廃棄しなければならない。

（イ） 重要な情報（個人情報等）を記録した記録媒体の廃棄は、情報セキュリティ管理者の許可を得ることとし、行った処理について、日時、担当者及び処理内容を記録し保存しなければならない。

（物理的セキュリティ対策）

第16条 情報システムの物理的セキュリティ対策については、次によるものとする。（１） サーバ等

ア 装置の取付け等

（ア） 情報システムの取付けを行う場合は、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切な固定等必要な措置を施さなければならない。

（イ） 次のサーバは二重化し、バックアップにより常に同一データを保持し、メインサーバに障害が発生した場合には速やかにセカンダリサーバに移行させ、システムの運用が停止しないようにしなければならない。

ａ 重要情報を格納しているサーバ

ｂ 住民サービスに関するサーバ

ｃ その他の基幹サーバ

（ウ） 職員等及び契約により操作を認められた外部委託事業者以外の者が容易に操作できないように、利用者のＩＤ、パスワードの設定等の設置を施さなければならない。パスワードは容易に推測できないものにしなければならず、１年以上同一のパスワードを使用してはならない。

（エ） サーバ等の取付けに当たっては、ディスプレイ、配線等から放射される電磁波により重要な情報（個人情報等）が外部に漏えいすることがないよう措置しなければならない。

イ 電源

（ア） サーバ等の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

（イ） 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施さなければならない。

ウ 配線

（ア） 配線は、傍受又は損傷等を受けることがないように可能な限り必要な措置を施さなければならない。

（イ） 主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。

（ウ） ネットワーク接続口（ハブのポート等）は、他の者が容易に発見できない場所に設置しなければならない。

（エ） 統括情報システム管理者、情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

エ　外部に設置する装置

（ア） 外部に設置する装置は、最高統括情報責任者の承認を受けたものでなければならない。

また、最高統括情報責任者は、定期的に当該装置の情報セキュリティの水準について確認しなければならない。

（イ） 五ヶ瀬町外に持ち出されるコンピュータ、記録媒体等については、五ヶ瀬町外での使用方法を定め、管理簿を設ける等適切に管理しなければならない。

（２） 管理区域

ア　管理区域

（ア） 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「コンピュータ室」という。）は、統括情報システム管理者の属する課室等で管理する。

（イ） コンピュータ室は、水害対策及び確実な入退室管理を行うために、地階又は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物理的構造としなければならない。

（ウ） コンピュータ室内の機器類は、耐震対策を講じた場所に設置するとともに、防火措置等を施さなければならない。なお、コンピュータ室内の機器類の配置は、緊急時に職員等が円滑に避難できるように配慮しなければならない。

（エ） 消火剤は機器及び記録媒体に影響を与えるものであってはならない。

イ　機器等の搬入場所

（ア） コンピュータ室へ機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について、職員による確認を行わなければならない。

（イ） 機器等の搬入には職員が同行する等の必要な措置を施さなければならない。

（３） ネットワーク

外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

（コンピュータ室の入退室管理）

第17条　コンピュータ室の入退室管理については次によるものとする。

（１）　コンピュータ室管理者

コンピュータ室の入退室を管理するため、コンピュータ室管理者を設置する。コンピュータ室管理者は統括情報システム管理者とする。

（２）　入退室の許可

コンピュータ室への入退室は職員等・外部委託事業者を問わず、許可された者のみとし、鍵等により入退室を管理しなければならない。鍵等は情報システム担当者が管理する。

（３）　コンピュータ室入退出管理簿

入退室する者はコンピュータ室入退出管理簿(様式第１号)に必要事項を記入しなければならない。

（人的セキュリティ対策）

第18条　情報の人的セキュリティ対策については、次の各号による。

（１）　役割・責任

ア　最高統括情報責任者

(ア)　五ヶ瀬町副町長を、五ヶ瀬町における全てのネットワーク、情報システム及び情報資産を統括する最高責任者とする。

(イ)　最高統括情報責任者は、五ヶ瀬町における全ての情報資産の情報セキュリティを統括する。

イ　統括情報システム管理者

(ア)　情報政策担当課長を統括情報システム管理者とする。

統括情報システム管理者は、最高統括情報責任者を補佐しなければならない。

(イ)　統括情報システム管理者は、五ヶ瀬町の全てのネットワークにおける開発、設定の変更、運用、更新等（クラウドサービスを利用する場合及び業務委託により実施する場合を含む。）を行う権限及び責任を有する。

(ウ)　統括情報システム管理者は、五ヶ瀬町の全てのネットワークにおける情報セキュリティに関する権限及び責任を有する。

(エ)　統括情報システム管理者は、情報セキュリティ管理者、情報システム担当者に対して情報セキュリティに関する指導及び助言を行う権限を有する。

(オ)　統括情報システム管理者は、五ヶ瀬町の情報資産に対する侵害または侵害の恐れのある場合には、最高統括情報責任者の指示に従い、最高統括情報責任者が不在の場合には自らの判断に基づき必要かつ十分な全ての措置を行う権限及び責任を有する。この場合、全ての職員等は統括情報システム管理者の指示に従わなければならない。

(カ)　統括情報システム管理者は、五ヶ瀬町の全てのネットワーク、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、管理を行い、クラウドサービスの利用及び業務委託を含め緊急時対応計画の策定及び見直しを行う。

ウ　情報セキュリティ管理者

(ア)　所属長、各行政委員会事務局の長等を、その課室等の情報セキュリティに関する総括的な権限及び責任を有する情報セキュリティ管理者とする。

(イ)　情報セキュリティ管理者は、所掌する課室等における情報セキュリティに関する統括的な権限及び責任を有する。

(ウ)　情報セキュリティ管理者は、所掌に属する課室等において担当している情報システム（クラウドサービスを利用するものを含む。）の追加、変更、運用の権限及び責任を有する。

(エ)　情報セキュリティ管理者は、所掌に属する課室等において担当している情報システムの連絡体制の構築並びに本規則の遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

(オ)　情報セキュリティ管理者は､担当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。

エ　情報システム担当者

(ア)　情報政策担当係を、統括情報システム管理者を補佐する情報システム担当者とする。

(イ)　情報システム担当者は、五ヶ瀬町の保有するパスワードに関し、次の事項を遵守し、職員に徹底をはからなければならない。

a　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ないこと。

b　パスワードのメモを作らないこと。

c　職員には情報システム担当者の承認なしにパスワードを設定させないこと。

d　パスワードの長さは十分な長さとし、文字列は想像しにくいものとすること。

e　情報システム又はパスワードに対する危険の恐れがある場合には、パスワードを速やかに変更すること。

f　パスワードは定期的に、若しくはアクセス回数に基づいて変更し、古いパスワードの再利用はしないこと。

g　複数の情報システムを扱う職員等は、パスワードをシステム間で共有しないこと。

h　仮のパスワードは、最初のログイン時点で変更すること。

i　情報セキュリティ対策の実施において、止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。

j 情報セキュリティ監査の実施において、止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。

オ　職員

(ア)　本規則の遵守義務

a　全ての職員は、本規則及び職員向け実施手順に定められている事項を遵守しなければならない。

b　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協議し、指示等を仰がなければならない。

(イ)　その他

a　全ての職員は、使用するコンピュータや記録媒体について、第三者に使用されること、又は許可なく情報を閲覧されることがないように、適切な措置を施さなければならない。

b　全ての職員は、情報セキュリティ管理者の許可を得ず、コンピュータ等を執務室外に持ち出してはならない。又、情報セキュリティ管理者の許可を得ず、コンピュータ等を執務室内に持ち込んではならない。

c　全ての職員は、異動、退職等により業務を離れる場合には、知り得た情報を秘匿しなければならない。

カ　非常勤及び臨時職員

(ア)　情報セキュリティ対策の遵守義務

a　全ての非常勤及び臨時職員は、本規則及び職員向け実施手順に定められている事項を遵守しなければならない。

b　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)　非常勤及び臨時職員の雇用及び契約

a　非常勤及び臨時職員には、雇用及び契約時に必ず本規則のうち、非常勤及び臨時職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

b　非常勤及び臨時職員には、雇用及び契約の際、必要な場合は本規則を遵守する旨の同意書への署名を求めるものとする。

(ウ)　その他

a　全ての非常勤及び臨時職員は、使用するコンピュータや記録媒体について、第三者に使用されること又は許可なく情報を閲覧されることがないように、適切な措置を施さなければならない。

b　全ての非常勤及び臨時職員は、情報セキュリティ管理者の許可を得ず、コンピュータ等を執務

室外に持ち出してはならない。また、情報セキュリティ管理者の許可を得ず、コンピュータ等を執務室内に持ち込んではならない。

ｃ　全ての非常勤及び臨時職員は、異動、退職等により業務を離れる場合には、知り得た情報を秘匿しなければならない。

キ　外部委託に関する管理

(ア)　ネットワーク及び情報システムの開発・保守を外部委託事業者に発注する場合は、クラウドサービスの提供を受ける場合を含め、　　外部委託事業者から下請けとして受託する事業者も含めて、本規則のうち、外部委託事業者が守るべき内容の遵守及びその守秘義務を明記した契約を行わなければならない。

(イ)　外部委託事業者との契約書には、損害賠償等本規則が遵守されなかった場合の規定並びに情報セキュリティ確保に関する責任分担を定めなければならない。

(２)　教育・訓練

ア　最高統括情報責任者は、説明会の実施等により幹部を含め全ての職員等及び関係する者に対し本規則について啓発しなければならない。また、新規採用の職員等を対象とする本規則に関する研修を設けなければならない。

イ　統括情報システム管理者及び情報セキュリティ管理者は、システム管理者向けの研修を受けなければならない。

ウ　統括情報システム管理者は、緊急時対応を想定した訓練を職員等に計画的に行わせなければならない。訓練の計画に当たっては、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適宜定めることとする。また、より効果的に実施できるよう計画を立てることとする。

エ　情報システム担当者は、最新の技術力を維持するための研修を常に受けなければならない。

オ　職員等は、定められた研修に参加し本規則及び実施手順を理解し、情報セキュリティ上の問題が生じないようにしなければならない。

(３)　事故、欠陥に対する報告

ア　職員等は､情報セキュリティに関する事故､システム上の欠陥及び誤動作を発見した場合には、速やかに情報セキュリティ管理者若しくは情報システム担当者に報告し、指示を仰ぎ、必要な措置を講じなければならない。

イ　情報セキュリティ管理者又は情報システム担当者は、職員等からの報告のあった事故等について、統括情報システム管理者に報告しなければならない。

ウ　統括情報システム管理者は、これらの事故等を分析し、再発防止のための必要な対策を講じ、その情報を記録し保存するものとする。

（技術的セキュリティ対策）

第19条　情報の技術的セキュリティ対策については、次の各号による。

（1）　コンピュータ及びネットワークの管理

ア　端末管理者の設置

（ア）　情報政策担当課長を端末管理者とする。

（イ）　端末管理者は、機器管理台帳及びソフトウェア管理台帳を作成管理することで、庁内ネットワークに接続する全ての端末機を厳正に管理するとともに、データが他に漏れないように適正に管理しなければならない。

イ　アクセス記録の取得等

重要な情報を扱う情報システムについて、次の措置を講じる。

（ア）　統括情報システム管理者及び情報システム担当者は、各種アクセス記録及び情報セキュリティの確保に必要な記録を全て取得し、一定の期間保存しなければならない。この記録には、クラウドサービスに係るものを含む。

（イ）　統括情報システム管理者及び情報システム担当者は、アクセス記録等が窃取、改ざん、消去されないように必要な措置を施さなければならない。また、必要に応じて、アクセス記録等の保全のための措置を講じなければならない。

（ウ）　統括情報システム管理者及び情報システム担当者は、定期的にアクセス記録等を分析、監視しなければならない。この分析、監視は、不正アクセスその他の異常の早期検知に資するよう実施するものとする。

ウ　システム管理記録及び作業の確認

（ア）　統括情報システム管理者及び情報システム担当者は、各種情報システムにおいて行ったシステム変更等の処理について、記録を作成しなければならない。この記録には、設定及び構成の変更を含む。

（イ）　統括情報システム管理者及び情報システム担当者が各種情報システムにおいて行った作業は記録し、適切に管理を行わなければならない。

（ウ）　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担当するシステムにおいて作業を行う場合には、情報システム担当者がその作業を確認しなければならない。

エ　障害記録

統括情報システム管理者及び情報システム担当者は、職員等から報告のあった情報、システムの障害に対する処理又は問題等は障害記録として体系的に記録し、常に活用できるよう保存しなければならない。

オ　情報システム仕様書等の管理

統括情報システム管理者及び情報システム担当者は、ネットワーク構成図、情報システム仕様書については、記録媒体に関わらず業務上必要とする者のみが閲覧できる場所に保管しなければならない。また、構築に際して事業者に外部委託した場合、当該事業者に守秘義務を課さなければならない。

カ　情報及びソフトウェアの交換

組織間において、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は、その取扱いに関する事項をあらかじめ定め、統括情報システム管理者及び情報システム担当者の許可を得なければならない。

キ　バックアップ

統括情報システム管理者及び情報システム担当者は、ファイルサーバ等に記録された情報について二重化措置に関わらずその重要度に応じて期間を設定し、定期的にバックアップ用の複製をとらなければならない。このバックアップには、クラウドサービスを利用して取り扱う情報を含むものとし、必要に応じて復旧の確認を行うものとする。

ク　メール

職員等は、メールで重要な情報（個人情報等）を送ってはならない。ただし、暗号化その他町が別に定める方法により送信する場合は、この限りでない。

ケ　外部の者が利用できるシステム

外部の者が利用できるシステムについては、必要に応じ他の情報システムと物理的に分ける等、情報セキュリティ対策について特に強固な対策をとらなければならない。

コ　情報システムの入出力データ

（ア）　情報システムに入力されるデータは、適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

（イ）　エラー又は故意の行為により情報が改ざんされるおそれがある場合、これを検出する手段を講じなければならない。

また、改ざんの有無を検出し、必要な場合は情報の修復を行う手段を講じなければならない。

（ウ）　情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力され

ることを確保しなければならない。

サ　電子署名・暗号化

（ア）　外部に送るデータが完全であることを担保する事が必要な場合には、定められた電子署名方法及び暗号化方法を使用して送信しなければならない。

（イ）　暗号化については、定められた方法以外の方法を用いてはならない。また、暗号のための鍵の管理方法について、定められた方法で管理しなければならない。

シ　業務目的以外の使用の禁止

（ア）　職員等は、業務目的以外での情報システムへのアクセスを行ってはならない。

（イ）　職員等は業務目的以外でウェブページを閲覧及びメールの使用をしてはならない。

ス　無許可ソフトウェアの導入等の禁止

職員等が業務上の必要から次の行為をなす場合には、統括情報システム管理者及び情報システム担当者の許可を必要とする。

（ア）　標準実装以外のアプリケーションソフトのコンピュータへのインストール

セ　機器構成の変更

（ア）　職員等は、コンピュータに対し改造及び機器の増設・交換を行ってはならない。

（イ）　職員等は、コンピュータに対し業務を遂行するために機器の増設・交換を行う必要がある場合は、統括情報システム管理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。

（ウ）　職員等は、モデム等の機器を増設して他の環境へのネットワーク接続を行うことや、外部からのアクセスを可能とする仕組みを構築する場合は、統括情報システム管理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。

ソ　電子取引

電子商取引に関しては、禁止する。

タ　その他

職員等が利用できるプロトコルは、業務上必要最低限のものとする。

（２）　アクセス制御

ア　利用者登録

統括情報システム管理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、登録情報の管理、異動や五ヶ瀬町外への出向等の職員等及び退職者における利用者ＩＤの取扱い等については、定められた方法に従って行わなければならない。

必要な利用者登録・変更は、統括情報システム管理者又は情報セキュリティ管理者に対する申請に

より行う。

イ　管理者権限

（ア）　ネットワークの管理者権限は、情報システム担当者のみに与え厳重に管理しなければならない。

（イ）　情報システムの管理者権限は、情報システム担当者のみに与え、厳重に管理しなければならない。

ウ　強制的な経路制御

統括情報システム管理者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

エ　外部からのアクセス

（ア）　外部からのアクセスの許可は、必要最低限にしなければならない。

外部から五ヶ瀬町の全てのネットワーク及び情報システムにアクセスする場合は、外部アクセスサーバに対してのみ接続を許可することとし、直接内部のネットワークに接続してはならない。

（イ）　五ヶ瀬町における全てのネットワーク及び情報システムへのモバイルコンピュータ等による外部からのアクセスは、禁止する。ただし、業務上必要があり、統括情報システム管理者が認めた場合であって、多要素認証その他必要な技術的対策を講じたときは、この限りでない。

オ　総合行政ネットワークとの接続

総合行政ネットワークは、「総合行政ネットワーク接続仕様書（平成13年５月11日）」に基づき適切な管理をしなければならない。

カ　外部ネットワークとの接続

（ア）　外部ネットワークとの接続に際しては、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を詳細に検討し、五ヶ瀬町の全てのネットワーク、情報システム及び情報資産に影響が生じないと明確に確認したうえで、最高情報統括責任者及び統括情報システム管理者の許可に基づき接続しなければならない。

その利用は情報システム担当者の適切な管理下で行い、庁内ネットワークと外部ネットワークとの境界にファイアウォールを設置する等、情報セキュリティに留意したネットワーク構成を採らなければならない。

この場合、当該外部ネットワークの瑕疵により五ヶ瀬町のデータの漏洩、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。

（イ） 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、五ヶ瀬町の情報資産に脅威が生じることが想定される場合には、情報システム担当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。

キ　自動識別

五ヶ瀬町で使用されるネットワーク機器については、機器固有情報によってアクセスの可否を自動的に判別しなければならない。

ク　ログイン手順

ログイン手順中におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻の表示等、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手順を定めなければならない。

ケ　パスワードの管理方法

（ア） 統括情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードは情報システム担当者から発行させる。

仮のパスワードを発行する場合は、正式パスワード稼動後、直ちに仮のパスワードを使えないようにしなければならない。

（イ） 統括情報システム管理者は、職員等のパスワードについて、定期的にその妥当性について調査を行わなければならない。

コ　接続時間の制限

管理者権限によるネットワーク及び情報システムへの接続については、必要最小限の接続時間に制限しなければならない。

（3） システム開発、導入、保守等

ア　情報システムの調達

（ア） 最高統括情報責任者は応用ソフトウェアの開発、変更及び運用についての手順及び基準を明らかにしなければならない。

（イ） 最高統括情報責任者は機器及び基本ソフトウェアの導入、保守及び撤去についての手順及び基準を明らかにしなければならない。

（ウ） 統括情報システム管理者は、情報システムの調達に当たっては、一般に公開する調達仕様書が情報セキュリティ確保の上で問題のないようにしなければならない。

（エ） 統括情報システム管理者は、機器及びソフトウェアを購入等する場合は、当該製品が情報セキュリティ上問題にならないかどうか、確認しなければならない。クラウドサービスの提供を受

ける場合も、同様とする。

イ　情報システムの変更管理

統括情報システム管理者は、システムを追加、変更、廃棄等した場合は、その際の設定、構成等の履歴を記録し、保存しなければならない。

ウ　情報システムの開発

統括情報システム管理者は、システム開発及び保守時の事故・不正行為対策のため、次の事項を実施しなければならない。

（ア）　責任者及び監督者の選任

（イ）　作業者及び作業範囲の指示

（ウ）　機器の搬出入の際の、情報セキュリティ管理者の許可及び確認

（エ）　マニュアル等の定められた場所への保管

（オ）　開発・保守を行った者の利用者ＩＤ、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消

エ　システムの導入

（ア）　情報システム担当者は、新たにシステムを導入する際には、既に稼動している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）　情報システム担当者は、試験に使用したデータ及びその結果については、厳重に保管しなければならない。

オ　ソフトウェアの保守及び更新

ソフトウェア（独自開発ソフトウェア及び汎用ソフトウェア）等を更新、又は修正プログラムを導入する場合は、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。

情報システム担当者は、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて、速やかな対応を行うこととし、その他のソフトウェアの更新等については、計画的に実施しなければならない。

カ　システムの受託業者への規定

（ア）　新たなシステムの開発を外部の事業者に委託する場合は、信頼のおける業者に委託するために、必要な資格等を定めなければならない。

（イ）　統括情報システム管理者は、作業中に身分証明書の提示を業者に求め、契約で定められた資格を有するものが作業に従事しているか確認を行わなければならない。また、守秘のための契約

を事業者と結ばなければならない。

キ　機器の修理及び廃棄

（ア）　記憶媒体の含まれる機器について、外部の業者に修理させ又は廃棄する場合は、その内容が消去された状態で行わなければならない。

（イ）　故障を外部の業者に修理させる際、情報を消去することが難しい場合は、修理を委託する業者に対し秘密を守ることを契約に定めなければならない。また重要な機器については、復元不可能な廃棄を行わなければならない。

（４）　コンピュータウイルス対策

ア　外部のネットワークから受信したファイルは、ファイアーウォールレベルでウイルスチェックを行いシステムへの侵入を防止する。

イ　外部のネットワークへ送信するファイルは、ファイアーウォールレベルでウイルスチェックを行い外部へのウイルス拡散を防止しなければならない。

ウ　統括情報システム管理者は、次の事項を実施しなければならない。

（ア）　ウイルス情報について職員等に対する注意喚起を行うこと。

（イ）　常時ウイルスに関する情報収集に努めること。

（ウ）　管理するサーバにおいてウイルスチェックを行うこと。

（エ）　コンピュータにおいてウイルスチェックを行うことを情報セキュリティ管理者及び職員に徹底すること。

（オ）　ウイルスチェック用のパターンファイルは常に最新のものに保つことを情報セキュリティ管理者及び職員に徹底すること。

エ　職員等は、次の事項を遵守しなければならない。

（ア）　ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

（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、必ずウイルスチェックを行うこと。

（ウ）　差出人が不明又は不自然に添付されたファイルは速やかに削除すること。

（エ）　ウイルスチェックの実行を途中で止めないこと。

（オ）　統括情報システム管理者が提供するウイルス情報を常に確認すること。

（カ）　添付ファイルのあるメールを送受信する場合は、ウイルスチェックを行うこと。

（５）　不正アクセス対策

ア　統括情報システム管理者は、次の事項を実施しなければならない。

（ア）　使用終了若しくは使用される予定のないポートを長時間空けた状態のままにしてはならない。

（イ） セキュリティホールの発見に努め、メーカー等からパッチの提供があり次第速やかにパッチをあてなければならない。また、脆弱性情報の収集及び必要な更新を計画的に行うものとする。

（ウ） 不正アクセスによるウェブページ書き換え防止を確実にするために、担当職員等によるものであるか否かに関わりなくデータの書き換えを検出し、統括情報システム管理者及び情報セキュリティ管理者へ通報する設定を施さなければならない。

（エ） 重要なシステムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。

イ　攻撃を受けることが明確な場合には、統括情報システム管理者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、各機関との連絡を密にして情報の収集に努めなければならない。

ウ　攻撃を受け、当該攻撃が不正アクセス禁止法違反等犯罪の可能性がある場合には記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなければならない。

エ　攻撃の可能性が明確であるにもかかわらず職員等の怠惰が原因でデータの漏洩、破壊、改ざん又はシステムダウン等により行政業務に深刻な影響をもたらした場合、当該職員は懲戒の対象とする。

オ　職員等による不正アクセスがあった場合、統括情報システム管理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、適切な処置を求めなければならない。

職員等による不正アクセスの結果、データの漏洩、破壊、改ざん又はシステムダウン等により行政業務に深刻な影響をもたらした場合、当該職員等を懲戒の対象とし、悪質な場合には刑事告発の対象とする。

（６） セキュリティ情報の収集

ア　統括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、五ヶ瀬町の全てのネットワーク及び情報システムについてソフトウェアにパッチを当てる等、セキュリティ対策上必要な措置を講じなければならない。

イ　最高統括情報責任者は、これらの情報を定期的に取りまとめ、関係課室等に通知するとともに、本規則の改定につながる情報については統括情報システム管理者に指示しなければならない。

ウ　統括情報システム管理者は、緊急時対応計画に定める緊急に連絡すべき情報を入手した場合は当該計画に定める情報連絡先に連絡しなければならない。

（運用）

第20条　情報システム全般にわたる運用については、次のとおりとする。

（１） 情報システムの監視

ア　セキュリティに関する事案を検知するため、統括情報システム管理者及び情報セキュリティ管理者は、常に情報システムの監視を行わなければならない。

イ　外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し、24時間監視を行わなければならない。

ウ　内部のシステムについて、アクセスコントロール等を行い、異常な運用等の監視を行わなければならない。

エ　監視により得られた結果については、消去や改ざんされないために必要な措置を施し、定期的に安全な場所に保管しなければならない。また、これらの記録の正確性を確保するため、正確な時刻の設定を行わなければならない。あわせて、必要に応じて、記録の保全及び追跡可能性の確保のための措置を講じなければならない。

（２） 情報システムの使用時間

ア　情報システムの使用時間は月曜日から金曜日まで、午前８時30分から午後５時15分までとする。

イ　情報システムを前項に定める時間以外に使用するときは、所属長の承認を得なければならない。（様式第２号）

ウ　情報システムを次の各号に掲げる日に使用するときは、所属長の承認を得なければならない。（様式第２号）

（ア） 土曜日

（イ） 国民の祝日に関する法律（昭和23年法律第178号）で規定する休日

（ウ） １月２日、３日及び12月29日から31日まで

エ　情報システム管理者は、前イ及びウの承認に基づく使用状況を取りまとめ、定期的に統括情報システム管理者に報告しなければならない。

（３） 本規則の遵守状況の確認

ア　統括情報システム管理者は、本規則が遵守されているかどうかについて、また、問題が発生していないかについて常に確認を行い、問題が発生していた場合には速やかに最高統括情報責任者に報告しなければならない。この確認には、クラウドサービスの利用状況及び外部委託に係る運用状況の把握を含むものとする。

イ　最高統括情報責任者は速やかに発生した問題に適切に対処しなければならない。

ウ　職員等は、本規則の違反が発生した場合は、直ちに情報セキュリティ管理者に報告を行わなければならない。違反の発生時には、それ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

があると統括情報システム管理者が判断した場合は、緊急時対応計画に従って連絡を行わなければならない。

エ　統括情報システム管理者及び情報セキュリティ管理者は、サーバ等のシステム設定が本規則を遵守しているかどうかについて、また問題が発生していないか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速やかに適切に対処しなければならない。

（4）　運用管理における留意点

ア　最高統括情報責任者は、アクセス記録、メール等個人のプライバシーに係る情報を閲覧できる権限を有する職員等を予め定めなければならない。ただし、法令で定められた個人情報の保護に関係する情報の閲覧に関しては、当該法令に定められた手続に従う。

イ　情報システム担当者は、職員等が常に本規則及び実施手順を参照できるよう配慮しなければならない。

（5）　侵害時の対応

情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を次のとおり定める。

ア　連絡先

(ア)　五ヶ瀬町長

(イ)　最高統括情報責任者

(ウ)　総括情報システム管理者

(エ)　情報セキュリティ管理者

(オ)　情報システムに係る外部委託事業者

(カ)　宮崎県庁

(キ)　警察

(ク)　関係機関

(ケ)　影響が考えられる個人及び法人

イ　事案の調査

(ア)　セキュリティに関する事案を認めた者は、次の項目について、速やかに情報セキュリティ管理者を通じて統括情報システム管理者に報告しなければならない。

a　事案の内容

b　事案が発生した原因として、想定される行為

c　確認した被害・影響範囲

（イ） 統括情報システム管理者は、事案の詳細な調査を行うとともに、最高統括情報責任者との情報共有を行わなければならない。

ウ　事案への対処

統括情報システム管理者は、事案に対処するために次の項目を実施しなければならない。

（ア） システム管理者は、次の事案が発生した場合、それぞれ定められた連絡先へ連絡しなければならない。

a　サイバーテロその他町民に重大な被害が生じるおそれがあるとき（五ヶ瀬町長、最高情報統括責任者、警察、影響が考えられる個人及び法人、必要と認められる業者等）

b　不正アクセスその他犯罪と思慮されるとき（五ヶ瀬町長、最高統括情報責任者、警察、必要と認められる業者等）

c　踏み台となって他者に被害を与えるおそれがあるとき（五ヶ瀬町長、最高情報統括責任者、警察、必要と認められる業者等）

d　情報システムに関する被害（情報セキュリティ管理者、必要と認められる業者等）

e　その他情報資産に係る被害（関係課室等）

（イ） 統括情報システム管理者は、次の事案が発生し情報資産の防護のためにネットワークの切断がやむを得ない場合は、ネットワークを切断する措置を講ずる。

a　異常なアクセスが継続しているとき、又は不正アクセスが判明したとき

b　システムの運用に著しい支障をきたす攻撃が継続しているとき

c　コンピュータウイルス等不正プログラムがネットワーク経由で拡がっているとき

d　情報資産に係る重大な被害が想定されるとき

（ウ） 情報セキュリティ管理者は、次の事案が発生し情報資産の防護のために情報システムの停止がやむを得ない場合は、情報システムを停止する。

a　コンピュータウイルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき

b　災害等により電源を供給することが危険又は困難なとき

c　その他の情報資産に係る重大な被害が想定されるとき

（エ） 事案に係るシステムのアクセス記録及び現状を保存する。

（オ） 事案に対処した経過を記録する。

（カ） 事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討する。

（キ） 再発防止の暫定措置を講じた後、復旧する。復旧に当たっては、原因の除去及び安全性の確認を行うものとする。

エ　再発防止の措置

（ア）　統括情報システム管理者は、当該事案に係るリスク分析を実施し、本規則及び実施手順の改善に係る再発防止計画を策定し、最高統括情報責任者へ報告しなければならない。

（イ）　最高統括情報責任者は、本規則及び実施手順の改善に係る再発防止計画が有効であると認められる場合は、これを承認する。

オ　外部委託による運用契約

（ア）　運用を外部委託する場合は、委託に関する責任を有する部署を明確にするとともに、委託事業者に対し必要なセキュリティ対策要件を記載した契約書による契約を締結しなければならない。クラウドサービスの提供を受ける場合も同様とし、責任分担を明確にしなければならない。

（イ）　委託に関する責任を有する部署は、委託先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、その内容を統括情報システム管理者に報告するとともに、その重要度に応じて最高統括情報責任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、個人番号利用事務等の全部又は一部を委託する場合には、外部委託事業者（委託の要素を含む賃貸借・修繕等についても同じ）において、番号法に基づく安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。

（法令遵守）

第21条　職員等は、職務の遂行において使用する情報資産について、次の法令等を遵守し、これに従わなければならない。（１）　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）

（２）　著作権法（昭和45年法律第48号）

（３）　行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）

（４）　五ヶ瀬町情報公開条例（平成16年五ヶ瀬町条例第１号）

（５）　個人情報の保護に関する法律（平成15年法律第57号）

（６）　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）並びにこれらに関連する法令及び条例

（情報セキュリティに関する違反に対する対応）

第22条　職員等に情報セキュリティ対策基準に違反する行動がみられた場合には、速やかに次の措置を講じなければならない。

（１）　職員等が違反を確認した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な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等が違反を確認した場合は、速やかに統括情報システム管理者及び

情報システム担当者に通知し、適切な措置を求めなければならない。

（３） 情報システム担当者の指導によっても改善されない場合、統括情報システム管理者は、当該職員等のネットワーク又は情報システムの使用に関する権利を停止あるいは剥奪することができる。その後、速やかに統括情報システム管理者は、職員等の権利を停止あるいは剥奪した旨を最高情報統括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なければならない。この場合において、当該違反が故意又は重大であると認められるときは、関係法令及び条例に基づき、懲戒その他必要な措置を講ずることを妨げない。

（情報セキュリティに関する違反に対する対応）

第22条　職員等に情報セキュリティ対策基準に違反する行動がみられた場合には、速やかに次の措置を講じなければならない。

（１） 職員等が違反を確認した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な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等が違反を確認した場合は、速やかに統括情報システム管理者及び情報システム担当者に通知し、適切な措置を求めなければならない。

（３） 情報システム担当者の指導によっても改善されない場合、統括情報システム管理者は、当該職員等のネットワーク又は情報システムの使用に関する権利を停止あるいは剥奪することができる。その後、速やかに統括情報システム管理者は、職員等の権利を停止あるいは剥奪した旨を最高情報統括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なければならない。この場合において、当該違反が故意又は重大であると認められるときは、関係法令及び条例に基づき、懲戒その他必要な措置を講ずることを妨げない。

（評価・見直し）

第23条　情報セキュリティ対策基準の評価・見直しについては、次によるものとする。

（１） 監査

（ア） 統括情報システム管理者は、ネットワーク及び情報システムの情報セキュリティについて監査を定期的に行わなければならない。

監査を行う者は、十分な専門的知識を有する者でなければならない。

（イ） 外部委託事業者に委託している場合、統括情報システム管理者は外部委託事業者から下請けとして受託している事業者も含めて、本規則の遵守について監査を定期的に行わなければならない。

（ウ） 統括情報システム管理者は点検結果をとりまとめ、最高統括情報責任者に報告する。最高統

括情報責任者は情報セキュリティ対策基準の見直しの際に参照する情報資産として活用しなければならない。この際、情報システムの利用形態の変化及び外部委託の状況に留意するものとする。

（２） 点検

統括情報システム担当者は、情報セキュリティ対策基準に沿った情報セキュリティ対策が実施されているかどうかについて職員等にアンケート等を行い、また自己点検を行わなければならない。統括情報システム担当者はこれをとりまとめ、最高統括情報責任者に報告する。最高統括情報責任者は、この報告結果を情報セキュリティ対策基準の更新の際に参照する情報資産として活用することとする。

（３） 更新

最高統括情報責任者は、新たに必要な対策が発生した場合又は点検の結果を踏まえ、情報セキュリティ対策基準の実効性を評価し、必要な部分を見直し、内容、時期について決定を行い、情報セキュリティ対策基準の更新を実施する。

（補則）

第24条　この規則に定めるもののほか、住民基本台帳ネットワークシステムの情報セキュリティ対策については別に定める。

附　則

この規則は、公布の日から施行し、平成16年11月１日から適用する。

附　則

この規則は、公布の日から施行し、平成18年７月１日から適用する。

附　則

この規則は、平成19年４月１日から施行する。

附　則

この規則は、公布の日から施行し、平成22年４月１日から適用する。

附　則

（施行期日）

１　この規則は、平成27年４月１日から施行する。

附　則

この規則は、公布の日から施行し、平成27年10月５日から適用する。

附　則

この規則は、公布の日から施行する。

附　則

この規則は、令和５年４月１日から施行する。

附　則

この規則は、令和６年４月１日から施行する。

附　則

この規則は、令和８年４月１日から施行する。

別表第１（第５条関係）

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	・行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産 ・特定個人情報	２に掲げる制限の他、以下に掲げる事項 ・支給以外の端末での作業の原則禁止 特定個人情報においては、上記に掲げる対策の他、以下に掲げる事項 ・法令で定める以外の事務での取扱いの禁止 ・インターネットに接続したコンピュータへの作成、保管、複製
機密性２	・行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管

機密性１	機密性２又は機密性３の情報資産以外の情報資産	

別表第２（第５条関係）

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情報資産以外の情報資産	

別表第３（第５条関係）

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	

様式第１号（第 17 条関係）

コンピュータ室入退出管理簿

入退室日時		入室者			入室目的
年月日	在室時間	所属	氏名	連絡先	
年　月　日	：　～　：				
年　月　日	：　～　：				
年　月　日	：　～　：				
年　月　日	：　～　：				
年　月　日	：　～　：				
年　月　日	：　～　：				
年　月　日	：　～　：				
年　月　日	：　～　：				
年　月　日	：　～　：				

様式第２号（第20条関係）

システム管理者記入欄	
月分	No.

課		係
課長	係長	申請者

電算処理依頼書（時間外端末操作）

令和　　年　　月　　日

統括情報システム管理者　殿

課名＿＿＿＿＿＿　係名＿＿＿＿＿＿

職名＿＿＿＿＿＿　氏名＿＿＿＿＿＿

下記のとおり、端末を時間外（休日）に操作してよろしいか。

職員番号	
使用目的	
使用月日時	月　　日　　：　　～　　：

- 依頼書は、操作員１名につき１枚提出してください。
- 使用目的は、具体的に記載してください。
  例）◎補正予算入力、◎仮課税前事前処理、◎調査表検査、…
  ×統計関係業務、
- 使用月日時は、各日毎に記載してください。
  例）◎４月１２日　１７：３０～１９：００
  ◎４月１３日　１７：３０～１９：３０
  ◎４月１８日　８：３０～１７：１５
  ×４月１２日～１３日　１７：３０～１９：３０
  ×４月１２日　１７：３０～　４月１３日　１９：３０

処理結果
令和　年　月　日