千葉県情報セキュリティ対策基準

平成１４年　３月１５日　策定

令和　８年１１月　４日　改定

千葉県

1．目的 4

2．定義 5

3．対象とする脅威 7

4．適用範囲 8

4．1　適用範囲 8

4．2　職員等の遵守義務 8

5．組織体制・役割 9

5．1　組織体制・役割 9

5．2　兼務の禁止 13

6．情報資産の分類と管理 15

6．1　情報資産の分類 15

6．2　情報資産の管理 18

7．情報システム全体の強靭性の向上 22

7．1　マイナンバー利用事務系 22

7．2　ＬGWAN接続系 23

7．3　インターネット接続系 23

8．物理的セキュリティ 25

8．1　サーバ等の管理 25

8．2　管理区域（情報システム室等）の管理 27

8．3　通信回線及び通信回線装置の管理 28

8．4　職員等の利用する端末や電磁的記録媒体等の管理 29

9．人的セキュリティ 30

9．1　職員等の遵守事項 30

9．2　研修・訓練 32

9．3　情報セキュリティインシデントの報告 33

9．4　ＩD及びパスワード等の管理 35

１０．技術的セキュリティ 37

１０．１　コンピュータ及びネットワークの管理 37

１０．２　アクセス制御 44

１０．３　情報システムの開発、導入、保守等 47

１０．４　不正プログラム対策 52

１０．５　不正アクセス対策 55

１０．６　セキュリティ情報の収集 58

１１．運用 59

１１．１　情報システムの監視 59

１１．２　情報セキュリティポリシーの遵守状況の確認 61

１１．３　侵害時の対応等 62

１１．４　例外措置 63

１１．５　法令の遵守 63

１１．６　情報セキュリティポリシー違反時の対応 64

１２．業務委託及び外部サービス（クラウドサービス）の利用 65

１２．１　業務委託 65

１２．２　情報システムに関する業務委託 67

１２．３　外部サービス（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） 69

１２．４　外部サービス（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） 75

１３．評価・見直し 77

１３．１　監査 77

１３．２　自己点検 78

１３．３　情報セキュリティポリシー及び関係規程等の見直し 79

附　則 80

別表第１　部局情報セキュリティ責任者 82

1. 目的

千葉県情報セキュリティ対策基準（以下「対策基準」という。）は、千葉県情報セキュリティ基本方針（以下「基本方針」という。）に基づき、情報セキュリティ対策を実現するために必要な基本的事項を定める。

2. 定義

（1）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウエア及びソフトウエア）をいう。

（2）情報システム

コンピュータ、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

情報セキュリティ基本方針及び本対策基準をいう。

（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（行政手続き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〕に規定される事務）に関わる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。

（９）ＬGWAN接続系

マイナンバー利用事務系を除き、総合行政ネットワーク（Ｌｏｃａｌ　Ｇｏｖｅｒｎｍｅｎｔ　Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ：「LGWAN：エルジーワン」）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）通信経路の分割

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、端末への画面転送及び危険因子のファイルからの除去等により、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。

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・詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウエ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、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

4．1　適用範囲

（1）県の機関の範囲

本対策基準が適用される県の機関は、知事部局、行政委員会（公安委員会を除く。）、議会事務局及び地方公営企業とする。

（2）情報資産の範囲

ア　本対策基準が対象とする情報資産は、次のとおりとする。

（ア）ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

（イ）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。）

（ウ）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

イ　アに掲げるもののうち、学校教育又は学術研究で用いる次の情報資産は除く。

（ア）教育ネットワーク及び教育情報システム並びにこれらに関する設備及び電磁的記録媒体

（イ）教育ネットワーク及び教育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。）

（ウ）教育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

ウ　監督官庁において個別の業務に対する情報セキュリティガイドライン等が策定されており、マイナンバー利用事務系及びＬＧＷＡＮ接続系から独立した情報システムで取り扱う情報資産は除く。

（3）対象者の範囲

本対策基準が適用される者は、県の機関に従事するすべての職員及び協定等により県の機関の事務に従事する者（以下「職員等」という。）とする。

4．2　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。

５.組織体制・役割

５．１　組織体制・役割

情報セキュリティ管理のための組織体制・役割は、次のとおりとする。

（１）最高情報セキュリティ責任者

ア　総務部長の職にある者を最高情報セキュリティ責任者とする。

イ　最高情報セキュリティ責任者は、適用範囲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。

ウ　最高情報セキュリティ責任者は、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アドバイザーとして置くことができるものとする。

エ　最高情報セキュリティ責任者は、本対策基準に定められた自らの担務を、最高情報セキュリティ副責任者及びその他の本対策基準に定める責任者等に担わせることができる。

（２）最高情報セキュリティ副責任者

ア　総務部次長の職にある者を最高情報セキュリティ副責任者とする。

イ　最高情報セキュリティ副責任者は、最高情報セキュリティ責任者を補佐し、最高情報セキュリティ責任者の命を受け情報セキュリティ対策に係る事務を総括し、最高情報セキュリティ責任者が不在の場合はその役割を代行する。

（３）統括情報セキュリティ責任者

ア　総務部デジタル改革推進局長の職にある者を統括情報セキュリティ責任者とする。

イ　統括情報セキュリティ責任者は、最高情報セキュリティ責任者及び最高情報セキュリティ副責任者を補佐する。

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

エ　統括情報セキュリティ責任者は、本対策基準を適用する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、最高情報セ

キュリティ責任者の指示に従い、最高情報セキュリティ責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する責任を有する。

オ　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、必要に応じて最高情報セキュリティ責任者にその内容を報告しなければならない。

（4）統括情報セキュリティ管理者

ア　総務部デジタル改革推進局デジタル推進課長の職にある者を統括情報セキュリティ管理者とする。

イ　統括情報セキュリティ管理者は、統括ネットワーク管理者、部局情報セキュリティ責任者、所属情報セキュリティ責任者及び情報システム管理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。

ウ　統括情報セキュリティ管理者は、緊急時等の円滑な情報共有を図るため、最高情報セキュリティ責任者、統括情報セキュリティ責任者、統括情報セキュリティ管理者、統括ネットワーク管理者、部局情報セキュリティ責任者、所属情報セキュリティ責任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。

（5）統括ネットワーク管理者

ア　総務部デジタル改革推進局情報システム課長の職にある者を統括ネットワーク管理者とする。

イ　統括ネットワーク管理者は、適用範囲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。

ウ　統括ネットワーク管理者は、緊急時には最高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統括情報セキュリティ管理者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。

（6）部局情報セキュリティ責任者

ア　各部局等に部局情報セキュリティ責任者を置く。

イ　部局情報セキュリティ責任者は別表第１に掲げる者をもって充てる。

ウ　部局情報セキュリティ責任者は、その所管する部局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。

エ　部局情報セキュリティ責任者は、その所管する部局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。

オ　部局情報セキュリティ責任者は、その所管する部局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所属情報セキュリティ責任者に対して情報セキュリティに関する助言及び指示を行うものとする。

（７）所属情報セキュリティ責任者

ア　各所属長を所属情報セキュリティ責任者とする。

イ　所属情報セキュリティ責任者は、その所管する所属において情報セキュリティ対策に関する権限及び責任を有する。

ウ　所属情報セキュリティ責任者は、その所管する所属おいて、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のある場合には、部局情報セキュリティ責任者、統括情報セキュリティ責任者、統括情報セキュリティ管理者、統括ネットワーク管理者及び最高情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

エ　所属情報セキュリティ責任者は、その所管する所属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並びに職員等に対する教育、訓練、助言及び指示を行う。

（８）情報システム管理者

ア　情報システムを所管する所属長を当該情報システムに関する情報システム管理者とする。

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

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

エ　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の

維持・管理を行う。

（9）部局情報セキュリティ担当者

ア　各部局等に部局情報セキュリティ担当者を置く。

イ　部局情報セキュリティ担当者は、部局情報セキュリティ責任者が指名する。

ウ　部局情報セキュリティ担当者は、部局情報セキュリティ責任者の指示等に従い、部局等内に対する情報セキュリティ対策の周知及び連絡調整を行う。

（１０）所属情報セキュリティ担当者

ア　各所属に所属情報セキュリティ担当者を置く。

イ　所属情報セキュリティ担当者は、所属情報セキュリティ責任者が指名する。

ウ　所属情報セキュリティ担当者は、所属情報セキュリティ責任者の指示等に従い、所属内に対する情報セキュリティ対策の周知及び連絡調整を行う。

（１１）情報システム担当者

ア　各情報システムに情報システム担当者を置く。

イ　情報システム担当者は、情報システム管理者が指名する。

ウ　情報システム担当者は、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。

（１２）千葉県情報セキュリティ対策推進委員会

ア　情報セキュリティ対策を統一的に実施するため、千葉県情報セキュリティ対策推進委員会を設置する。

イ　千葉県情報セキュリティ対策推進委員会は統括情報セキュリティ責任者、統括情報セキュリティ管理者、統括ネットワーク管理者及び部局情報セキュリティ責任者で構成する。

ウ　統括情報セキュリティ責任者を千葉県情報セキュリティ対策推進委員会委員長とする。

エ　統括情報セキュリティ管理者を、千葉県情報セキュリティ対策推進委員会事務局長とする。

オ　千葉県情報セキュリティ対策推進委員会事務局長は委員長の監督を受け、その事務

をつかさどる。

カ　千葉県情報セキュリティ対策推進委員会は、情報セキュリティポリシーの見直し等、情報セキュリティに関する重要な事項を審議する。

（１３）情報セキュリティインシデントに対処するための体制

ア　情報セキュリティインシデントに迅速かつ適正に対処するための体制（Computer Security Incident Response Team：「CSIRT：シーサート」）を設置する。

イ　統括情報セキュリティ責任者をCSIRT責任者とする。

ウ　CSIRT責任者は、CSIRTに所属する職員等を指名する。

エ　CSIRT 責任者は、情報セキュリティに関する統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

オ　CSIRT 責任者は、最高情報セキュリティ責任者による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供する。

カ　CSIRT 責任者は、情報セキュリティインシデントを認知した場合には、最高情報セキュリティ責任者及び総務省等へ報告する。

キ　CSIRT 責任者は、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行う。

（１４）クラウドサービス利用における組織体制

統括情報セキュリティ管理者及び情報システム管理者又は所属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際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

５．２　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

13

申請を行う者とその承認者又は許可者は、兼ねてはならない。

（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、情報セキュリティ監査を受ける者とその監査を実施する者は、兼ねてはならない。

６.情報資産の分類と管理

６．１　情報資産の分類

適用範囲における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

（１）機密性による情報資産の分類

ア　機密性３Ａ

（ア）分類基準

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令和７年２月１４日一部改正）に定める秘密文書に相当する文書

（イ）取扱制限

機密性２の取扱制限及び県から配付された端末以外での作業の原則禁止

イ　機密性３Ｂ

（ア）分類基準

行政事務で取り扱う情報資産のうち、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

（イ）取扱制限

機密性２の取扱制限及び県から配付された端末以外での作業の原則禁止

ウ　機密性３Ｃ

（ア）分類基準

行政事務で取り扱う情報資産のうち、機密性３Ｂ 以上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

（イ）取扱制限

機密性２の取扱制限及び県から配付された端末以外での作業の原則禁止

エ　機密性２

（ア）分類基準

行政事務で取り扱う情報資産のうち、機密性３に相当する機密性を要しないが、直ちに一般公表することを前提としていない情報資産

（イ）取扱制限

・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

・電磁的記録媒体の施錠可能な場所への保管

オ　機密性１

（ア）分類基準

機密性２又は機密性３の情報資産以外の情報資産

（２）完全性による情報資産の分類

ア　完全性２

（ア）分類基準

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

（イ）取扱制限

・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

・電磁的記録媒体の施錠可能な場所への保管

イ　完全性１

（ア）分類基準

完全性２の情報資産以外の情報資産

（３）可用性による情報資産の分類

ア　可用性２

（ア）分類基準

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

（イ）取扱制限

・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

イ　可用性１

（ア）分類基準

可用性２の情報資産以外の情報資産

６．２　情報資産の管理

（1）管理責任

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

イ　情報システム管理者は、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　所属情報セキュリティ責任者は、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。

エ　所属情報セキュリティ責任者は、クラウドサービスの環境に保存される情報資産についても「６．１　情報資産の分類」の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定めなければならない。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認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・フッダー等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

（3）情報の作成

ア　職員等は、業務上必要のない情報を作成してはならない。

イ　情報を作成する者は、情報の作成時に「６．１情報資産の分類」の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

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

（４）情報資産の入手

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

イ　庁外の者が作成した情報資産を入手した者は、「６．１情報資産の分類」の分類に基づき、当該情報資産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、所属情報セキュリティ責任者に判断を仰がなければならない。

（５）情報資産の利用

ア　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

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

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

（６）情報資産の保管

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

イ　所属情報セキュリティ責任者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

ウ　所属情報セキュリティ責任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　所属情報セキュリティ責任者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報資産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。

19

（7）情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

（8）情報資産の運搬

ア　車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

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

（9）情報資産の提供・公開

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、所属情報セキュリティ責任者に許可を得なければならない。

ウ　所属情報セキュリティ責任者は、外部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、情報を記録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、所属情報セキュリティ責任者の許可を得なければならない。

エ　クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

（１１）外部での情報処理

ア　外部で情報処理を行う者は、取扱う情報資産について、移動中は常に携行し、紛失、盗難等を防止しなければならない。

イ　外部で情報処理を行う者は、機密性２以上の情報資産を取扱う場合は、業務に関係の無い者からの覗き見等を防止するための措置を講じなければならない。

７. 情報システム全体の強靭性の向上

７．１　マイナンバー利用事務系

（１）マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(ＭＡＣアドレス、ＩＰアドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、ＬＧＷＡＮを経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

（２）情報のアクセス及び持ち出しにおける対策

ア　情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

イ　情報の持ち出し不可設定

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。

（３）マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

ア　マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、他の領域とはネットワークを分離しなければならない。

（４）マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。 また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

７．２　ＬＧＷＡＮ接続系

（１）ＬＧＷＡＮ接続系とインターネット接続系の分割

ＬＧＷＡＮ接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをＬＧＷＡＮ接続系に取り込む場合は、無害化通信を図らなければならない。

（２）ＬＧＷＡＮ 接続系と接続されるクラウドサービス上での情報システムの扱い

ア　ＬＧＷＡＮ 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域をＬＧＷＡＮ 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

７．３　インターネット接続系

（１）不正通信の監視

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）自治体情報セキュリティクラウドへの参加

県及び市町村のインターネットとの通信を集約する自治体情報セキュリティクラ

ウドに参加するとともに、関係省庁や市町村等と連携しながら、情報セキュリティ対策を推進しなければならない。

（3）インターネット接続系への業務端末の設置

業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末を配置する場合、取り扱う情報資産の格付けに応じ、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

８.物理的セキュリティ

８．１　サーバ等の管理

（１）機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、不正持ち出し、傾倒を防止するため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、災害情報等の緊急性が高く、国民の生命や財産に著しく影響を及ぼし得るような重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し同一データを保持しなければならない。

イ　情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

（３）機器の電源

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

イ　情報システム管理者は、統括ネットワーク管理者及び施設管理部門と連携し、落雷等による過電流又は過電圧に対して、必要に応じ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　統括ネットワーク管理者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必

要な措置を講じなければならない。

イ　統括ネットワーク管理者及び情報システム管理者は、主要な個所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

ウ　統括ネットワーク管理者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

エ　統括ネットワーク管理者及び情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

（５）機器の定期保守及び修理

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

イ　情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、事業者に故障を修理させるにあたり、修理を委託する外部の事業者との間で、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

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（委託事業者の施設内に機器を設置し、又は委託事業者の提供する機器を利用する場合を含む。）は、統括情報セキュリティ管理者の許可を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（７）機器の廃棄等

ア　情報システム管理者は、機器を廃棄、リース返却等する場合、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。

イ　クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手

順について確認しなければならない。なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

８．２　管理区域（情報システム室等）の管理

（１）管理区域の構造等

ア　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

イ　統括ネットワーク管理者及び情報システム管理者は、管理区域を地階又は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しなければならない。

ウ　統括ネットワーク管理者及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

エ　統括ネットワーク管理者及び情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

オ　統括ネットワーク管理者及び情報システム管理者は、管理区域内に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

（２）管理区域の入退室管理等

ア　情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ＩＣカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

イ　情報システム管理者は、管理区域に入室する職員等及び委託事業者に対し、身分証明書等を携帯させ、必要に応じ確認しなければならない。

ウ　情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

エ　情報システム管理者は、機密性２以上の情報資産を扱う情報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、また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。

（３）機器等の搬入出

ア　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等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、情報システム室の機器等の搬入出について、職員等を立ち会わせなければならない。

８．３　通信回線及び通信回線装置の管理

ア　統括ネットワーク管理者は、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。

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

ウ　統括ネットワーク管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

エ　統括ネットワーク管理者は、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。

オ　統括ネットワーク管理者は、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、適正な回線及び回線装置を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

カ　統括ネットワーク管理者は、ネットワークに使用する回線について、伝送途上に情報の破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分な情報セキュリティ対策を実施しなければならない。

キ　統括ネットワーク管理者は、通信回線装置が動作するために必要なソフトウエ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、必要なソフトウエアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

ク　統括ネットワーク管理者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

８．４　職員等の利用する端末や電磁的記録媒体等の管理

ア　所属情報セキュリティ責任者又は情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末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。

イ　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、ＩＣカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

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

エ　情報システム管理者は、パソコン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適用しなければならない。

オ　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。

9.人的セキュリティ

9．1　職員等の遵守事項

（1）職員等の遵守事項

ア　情報セキュリティポリシー等の遵守

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

イ　業務以外の目的での利用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

ウ　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

（ア）職員等は、県から配付された情報資産を外部に持ち出す場合には、所属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）職員等は、外部で情報処理業務を行う場合には、所属情報セキュリティ責任者の許可を得なければならない。

エ　県から配付されたパソコン、モバイル端末及び電磁的記録媒体等以外の機器の業務利用

（ア）職員等は、県から配付されたパソコン、モバイル端末及び電磁的記録媒体等以外の機器を原則業務に利用してはならない。ただし、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、所属情報セキュリティ責任者の許可を得て利用することができる。

（イ）職員等は、県から配付されたパソコン、モバイル端末及び電磁的記録媒体等以外の機器を用い、外部で情報処理作業を行う場合には、所属情報セキュリティ責任者の許可を得なければならない。

オ　持ち出し及び持ち込みの記録

所属情報セキュリティ責任者は、端末等の持ち出し及び持ち込みについて、記録を

作成し、保管しなければならない。

カ　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウエアに関するセキュリティ機能の設定を所属情報セキュリティ責任者の許可なく変更してはならない。

キ　机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は所属情報セキュリティ責任者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

ク　退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

ケ　クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

（2）臨時・非常勤職員等への対応

ア　採用時の説明

所属情報セキュリティ責任者は、臨時・非常勤職員等に対し、採用時に情報セキュリティポリシーを説明し、理解させなければならない。

イ　インターネット及び電子メールの利用等の制限

所属情報セキュリティ責任者は、臨時・非常勤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

所属情報セキュリティ責任者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（４）委託事業者に対する説明

所属情報セキュリティ責任者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

９．２　研修・訓練

（１）情報セキュリティに関する研修・訓練

ア　統括情報セキュリティ管理者は、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。

イ　統括情報セキュリティ責任者は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施しなければならない。

ウ　所属情報セキュリティ責任者及び情報システム管理者は、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

（２）研修計画の策定及び実施

ア　統括情報セキュリティ責任者は、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、最高情報セキュリティ責任者の承認を得なければならない。

イ　研修計画において、所属情報セキュリティ担当者が毎年度最低１回は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　統括情報セキュリティ管理者は、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

エ　研修は、部局情報セキュリティ責任者、所属情報セキュリティ責任者、情報システム管理者、部局情報セキュリティ担当者、所属情報セキュリティ担当者、情報システム担当者及びその他の職員等に対して、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　所属情報セキュリティ責任者は、所属する職員等の教育の実施状況を確認しなければならない。

カ　統括情報セキュリティ責任者は、毎年度１回、教育の実施状況を分析、評価し、最高情報セキュリティ責任者に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（３）緊急時対応訓練

統括情報セキュリティ管理者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（４）研修・訓練への参加

職員等は、定められた研修・訓練に参加しなければならない。

９．３　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、速やかに所属情報セキュリティ責任者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

イ　所属情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、速やかに統括情報セキュリティ管理者に報告するとともに、必要に応じて、最高情報セキュリティ責任者、統括情報セキュリティ責任者、統括ネットワーク管理者、部局情報セキュリティ責任者及び情報システム管理者に対しても報告しなければならない。

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

エ　所属情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象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、本対策基準が適用され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、所属情報セキュリティ責任者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

イ　所属情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、速やかに統括情報セキュリティ管理者に報告するとともに、必要に応じて、最高情報セキュリティ責任者、統括情報セキュリティ責任者、統括ネットワーク管理者、部局情報セキュリティ責任者及び情報システム管理者に対しても報告しなければならない。

ウ　最高情報セキュリティ責任者は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。

エ　統括情報セキュリティ責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

（3）情報セキュリティインシデント原因の究明・記録、再発防止等

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、最高情報セキュリティ責任者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所属情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。また、CSIRT 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、最高情報セキュリティ責任者に報告するとともに、必要な措置を実

施しなければならない。

オ　最高情報セキュリティ責任者は、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。

９．４　ＩＤ及びパスワード等の管理

（１）ＩＣカード等の取扱い

ア　職員等は、自己の管理するＩＣカード等に関し、次の事項を遵守しなければならない。

（ア）認証に用いるＩＣカード等を、職員等間で共用してはならない。

（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パソコン等の端末のスロット等から抜いておかなければならない。

（ウ）ＩＣカード等を紛失した場合には、速やかに統括ネットワーク管理者及び情報システム管理者に連絡し、指示に従わなければならない。

イ　統括ネットワーク管理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　統括ネットワーク管理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。

（２）ＩＤの取扱い

職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

ア　自己が利用しているＩＤは、他人に利用させてはならない。

イ　共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

（３）パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア　パスワードは、他者に知られないように管理しなければならない。

イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ　パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）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、所属情報セキュリティ責任者に速やかに報告し、パスワードを速やかに変更しなければならない。

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　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。

キ　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ることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。

ク　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）。

１０.技術的セキュリティ

１０．１　コンピュータ及びネットワークの管理

（1）ファイルサーバの設定等

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、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（2）バックアップの実施

ア　統括ネットワーク管理者及び情報システム管理者は、業務システムのデータベースや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　統括ネットワーク管理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　統括ネットワーク管理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。

エ　統括ネットワーク管理者及び情報システム管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が県の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者から

バックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

（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、他団体と情報システムに関する情報及びソフトウエアを交換する場合、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所属情報セキュリティ責任者の許可を得なければならない。

（４）システム管理記録及び作業の確認

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

イ　統括ネットワーク管理者及び情報システム管理者は、所管する情報システムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理し、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　統括ネットワーク管理者、情報システム管理者又は情報システム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

（５）情報システム仕様書等の管理

統括ネットワーク管理者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書等について、記録媒体にかかわらず、業務上必要とする者以外の者が閲覧し、または紛失すること等がないよう、適正に管理しなければならない。

（６）ログの取得等

ア　統括ネットワーク管理者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

イ　統括ネットワーク管理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　統括ネットワーク管理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。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

エ　統括ネットワーク管理者及び情報システム管理者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

（７）障害記録

統括ネットワーク管理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　統括ネットワーク管理者は、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エア等を設定しなければならない。

イ　統括ネットワーク管理者は、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　統括ネットワーク管理者は、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情報システムの分離等

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情報システムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

（１０）外部ネットワークとの接続制限等

ア　情報システム管理者は、所管するネットワークを適用範囲以外のネットワーク（以下「外部ネットワーク」という。）と接続しようとする場合には、統括情報セキュリティ管理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　統括ネットワーク管理者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。

（ア）庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

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

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

（エ）情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定しなければならない。

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

オ　情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ管理

者の判断に従い、速やかに当該外部ネットワークとの接続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　所属情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ　所属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　所属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、複合機の持つ記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（１２）ＩｏＴ機器を含む特定用途機器のセキュリティ管理

情報システム管理者は、特定用途機器（テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の通信回線に接続して特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているもの）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、特定用途機器の特性に応じた対策を講じなければならない。

（１３）無線ＬＡＮのセキュリティ対策及びネットワークの盗聴対策

ア　統括ネットワーク管理者は、無線ＬＡＮを利用する場合は、解読が困難な暗号化及び認証技術を利用しなければならない。

イ　統括ネットワーク管理者は、機密性の高い情報を扱う無線ＬＡＮ及び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　情報システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバ

の設定を行わなければならない。

イ　情報システム管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

ウ　情報システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

エ　情報システム管理者は、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。

オ　情報システム管理者は、システム開発や運用、保守等のため庁舎内に常駐している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、委託事業者との間で利用方法を取り決めなければならない。

（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、所属情報セキュリティ責任者に報告しなければならない。

（１６）電子署名・暗号化

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、統括情報セキュリティ責任者が定めた電子署名、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統括情報セキュリティ責任者が定める以外の方法を用いてはならない。また、統括情報セキュリティ責任者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　統括ネットワーク管理者は、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）無許可ソフトウエアの導入等の禁止

ア　職員等は、パソコンやモバイル端末に無断でソフトウエ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、統括ネットワーク管理者及び所属情報セキュリティ責任者又は情報システム管理者の許可を得て、ソフトウエアを導入することができる。なお、導入する際は、所属情報セキュリティ責任者又は情報システム管理者は、ソフトウエ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エアを利用してはならない。

（１８）機器構成の変更の制限

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

イ　職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括ネットワーク管理者及び所属情報セキュリティ責任者又は情報システム管理者の許可を得なければならない。

（１９）業務外ネットワークへの接続の禁止

ア　職員等は、配付された端末を、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　情報システム管理者は、配付した端末について、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しなければならない。

（２０）業務以外の目的でのウェブ閲覧の禁止

ア　職員等は、業務以外の目的でウェブを閲覧してはならない。

イ　統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、所属情報セキュリティ責任者に**通知し適正な措置を求めなければならない。**

（２１）　Ｗｅｂ会議サービスの利用時の対策

ア　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、統括情報セキュリティ責任者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しなければならない。

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じなければならない。

エ　職員等は、外部からＷｅｂ会議に招待される場合は、統括情報セキュリティ責任者が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　所属情報セキュリティ責任者は、所属が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

（ア）所属が管理するアカウントによる情報発信が、実際のものであることを明らかにするために、千葉県ホームページ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）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

イ　機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

ウ　利用するソーシャルメディアサービスごとの責任者を定めなければならない。

エ　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

オ　可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、千葉県ホームページに当該情報を掲載して参照可能としなければならない。

１０．２　アクセス制御

（１）アクセス制御等

ア　アクセス制御

統括ネットワーク管理者又は情報システム管理者は、所管するネットワーク又は情

報システムごとにアクセスする権限のない職員等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

イ　利用者ＩＤの取扱い

（ア）統括ネットワーク管理者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

（イ）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、統括ネットワーク管理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）統括ネットワーク管理者及び情報システム管理者は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、点検しなければならない。

（エ）統括ネットワーク管理者及び情報システム管理者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

ウ　特権を付与されたＩＤの管理等

（ア）統括ネットワーク管理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）統括ネットワーク管理者及び情報システム管理者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。

（ウ）統括ネットワーク管理者及び情報システム管理者の特権を代行する者は、統括ネットワーク管理者及び情報システム管理者が指名した者でなければならない。

（エ）統括ネットワーク管理者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードの変更について、委託事業者に行わせてはならない。

（オ）統括ネットワーク管理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、人事異動の際のパスワードの変更、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）統括ネットワーク管理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必要がある場合は、統括ネットワーク管理者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

イ　統括ネットワーク管理者は、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しなければならない。

ウ　統括ネットワーク管理者は、外部からのアクセスを認める場合、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　統括ネットワーク管理者は、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　統括ネットワーク管理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配付する場合、セキュリティ確保のために必要な措置を講じなければならない。

カ　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、所属情報セキュリティ責任者の許可を得るか、又は所属情報セキュリティ責任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。

キ　統括ネットワーク管理者は、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）自動識別の設定

統括ネットワーク管理者及び情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（４）ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・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。

（５）認証情報の管理

ア　統括ネットワーク管理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　統括ネットワーク管理者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

ウ　統括ネットワーク管理者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（６）特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

１０．３　情報システムの開発、導入、保守等

（１）機器等の調達に係る運用規程の整備

ア　統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策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、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。

（２）機器等及び情報システムの調達

ア　統括ネットワーク管理者及び情報システム管理者は、情報システム開発、導入、保守等の調達にあたっては、調達仕様書に必要とするセキュリティ要件を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

イ　統括ネットワーク管理者及び情報システム管理者は、機器及びソフトウエ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。

（３）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、情報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、情報システム開発のための規則を確立しなければならない。

イ　情報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、情報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、情報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い。

ウ　情報システム開発に用いるハードウエア及びソフトウエアの管理

（ア）情報システム管理者は、情報システム開発の責任者及び作業者が使用するハードウエア及びソフトウエアを特定し、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エア以外のソフトウエアが導入されている場合、当該ソフトウエアを情報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。

（４）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、情報システム開発、保守及びテスト環境と情報システム運用環境を分離しなければならない。

（イ）情報システム管理者は、情報システム開発・保守及びテスト環境から情報システム運用環境への移行について、情報システム開発・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、導入する情報システムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

イ　テスト

（ア）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

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

（ウ）情報システム管理者は、個人情報及び機密性２以上の生データを、テストデータに使用してはならない。

（エ）情報システム管理者は、開発した情報システムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

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

ウ　機器等の納入時又は情報システムの受入れ時

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

（イ）情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情

報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

（５）情報システムの基盤を管理又は制御するソフトウエア導入時の対策

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

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

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

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

（６）情報システムの基盤を管理又は制御するソフトウエア運用時の対策

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

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

（イ）脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

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

（７）情報システム開発・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、情報システム開発・保守に関連する資料及び情報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。

（ア）情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ管理者に報告しなければならない。

（イ）情報システム管理者は、所管する情報システム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、以下を全て含む情報システム関連文書を整備し

なければならない。

・情報システムを構成するサーバ装置及び端末関連情報

・情報システムを構成する通信回線及び通信回線装置関連情報

（ウ）情報システム管理者は、所管する情報システム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、以下を全て含む実施手順を整備しなければならない。

・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

・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

・情報システムが停止した際の復旧手順

イ　情報システム管理者は、テスト結果を一定期間保管しなければならない。

ウ　情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。ただし、契約上の条件等で提供されないものは除く。

（８）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、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

（ア）利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直さなければならない。

（イ）運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

（ウ）ウェブアプリケーションやウェブコンテンツにおいて、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等の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。

（９）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。

（１０）開発・保守用のソフトウエアの更新等

情報システム管理者は、開発・保守用のソフトウエ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。

（１１）情報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、情報システム更新・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。

（１２）情報システムについての対策の見直し

情報システム管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、統括情報セキュリティ責任者へ報告しなければならない。

１０．４　不正プログラム対策

（1）統括ネットワーク管理者の措置事項

統括ネットワーク管理者は、不正プログラム対策として、次の事項を措置しなければならない。

ア　外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの情報システムへの侵入を防止しなければならない。

イ　外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

ウ　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

エ　所管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エ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エ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。なお、β モデル又は β‘モデルを採用する場合は、不正プログラム対策ソフトウエアは、未知の不正プログラムに対する対応も可能となるよう対策を講じなければならない。

カ　不正プログラム対策のソフトウエアは、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エアは、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エ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。

ク　仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

（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、その所管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エアをシステムに常駐させなければならない。

イ　不正プログラム対策ソフトウエ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。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。

ウ　不正プログラム対策のソフトウエアは、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情報システムにおいて、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、所属で管理している電磁的記録媒体以外を職員等に使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エアを導入し、定期的に当該ソフトウエ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エ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。

カ　業務で利用するソフトウエアは、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エ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。

（３）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

ア　パソコンやモバイル端末において、不正プログラム対策ソフトウエアが導入されている場合は、当該ソフトウエ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エ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エ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エ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エアでチェックを行わなければならない。また、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。

１０．５　不正アクセス対策

（１）統括ネットワーク管理者の措置事項

統括ネットワーク管理者は、不正アクセス対策として、次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、統括ネットワーク管理者及び情報システム管理者へ通報するよう、設定しなければならない。

エ　重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

オ　統括ネットワーク管理者は、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。

カ　クラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

キ　クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

ク　パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、クラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認しなければならない。

（２）攻撃への対処

最高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統括ネットワーク管理者は、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、情報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、市町村等と連絡を密にして情報の収集に努めなければならない。

（３）記録の保存

最高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統括ネットワーク管理者は、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

統括ネットワーク管理者及び情報システム管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（５）職員等による不正アクセス

統括ネットワーク管理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、ネットワーク及び情報システムについて当該職員等の所属の所属情報セキュリティ責任者に通知し、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

統括ネットワーク管理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

統括ネットワーク管理者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、 侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

１０．６　セキュリティ情報の収集

（１）セキュリティホールに関する情報の収集・共有及びソフトウエアの更新等

ア　統括情報セキュリティ管理者、統括ネットワーク管理者及び情報システム管理者は、サーバ装置、端末及び通信回線装置等における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、ソフトウエア更新等の対策を実施しなければならない。

イ　統括情報セキュリティ管理者、統括ネットワーク管理者及び情報システム管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、業務に対する影響や保有するデータへの影響について特定し、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認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管理者及び統括ネットワーク管理者は、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管理者、統括ネットワーク管理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。

１１.運用

１１．１　情報システムの監視

（1）情報システムの運用・保守時の対策

ア　統括ネットワーク管理者及び情報システム管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

イ　統括ネットワーク管理者及び情報システム管理者は、情報システムの情報セキュリティ対策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　統括ネットワーク管理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について、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

（2）情報システムの監視機能

ア　統括ネットワーク管理者及び情報システム管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

イ　統括ネットワーク管理者及び情報システム管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

ウ　統括ネットワーク管理者及び情報システム管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

エ　統括ネットワーク管理者及び情報システム管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

（３）情報システムの監視

ア　統括ネットワーク管理者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

イ　統括ネットワーク管理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。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

ウ　暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

エ　統括ネットワーク管理者及び情報システム管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

オ　統括ネットワーク管理者及び情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

カ　統括ネットワーク管理者及び情報システム管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

（ア）サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（イ）クラウドサービス利用の終了手順

（ウ）バックアップ及び復旧

１１．２　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　部局情報セキュリティ責任者及び所属情報セキュリティ責任者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに最高情報セキュリティ責任者、統括情報セキュリティ責任者、統括情報セキュリティ管理者及び統括ネットワーク管理者に報告しなければならない。

イ　最高情報セキュリティ責任者は、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　統括ネットワーク管理者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

（２）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

最高情報セキュリティ責任者、統括情報セキュリティ責任者、統括情報セキュリティ管理者、統括ネットワーク管理者、部局情報セキュリティ責任者、所属情報セキュリティ責任者及び情報システム管理者は、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及び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、統括情報セキュリティ管理者及び所属情報セキュリティ責任者に報告を行わなければならない。

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又は統括情報セキュリティ管理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。

１１．３　侵害時の対応等

（１）緊急時対応計画の策定

ア　統括情報セキュリティ責任者、統括情報セキュリティ管理者、統括ネットワーク管理者及び情報システム管理者は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

イ　統括情報セキュリティ責任者、統括情報セキュリティ管理者、統括ネットワーク管理者及び情報システム管理者は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した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

統括情報セキュリティ責任者、統括ネットワーク管理者及び情報システム管理者は、自然災害、大規模・広範囲にわたる疾病等に備えて策定された業務継続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

統括情報セキュリティ責任者、統括情報セキュリティ管理者、統括ネットワーク管理者及び情報システム管理者は、情報セキュリティを取り巻く状況の変化や組織体制

の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

１１．４　例外措置

（１）例外措置の許可

所属情報セキュリティ責任者及び情報システム管理者は、情報セキュリティ関係規程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、統括情報セキュリティ管理者の許可を得て、例外措置を講じることができる。

（２）緊急時の例外措置

所属情報セキュリティ責任者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに統括情報セキュリティ管理者に報告しなければならない。

（３）例外措置の申請書の管理

統括情報セキュリティ管理者は、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。

１１．５　法令の遵守

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

ア　地方自治法（昭和２２年法律第６７号）

イ　地方公務員法（昭和２５年法律第２６１号）

ウ　著作権法（昭和４５年法律第４８号）

エ　不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）

オ　個人情報の保護に関する法律（平成１５年法律第５７号）

カ　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７ 号）

キ　サイバーセキュリティ基本法（平成２６年法律第１０４号）

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

ケ　個人情報の保護に関する法律施行条例（令和４年１２月２７日千葉県条例第３７号）

（２）統括ネットワーク管理者及び情報システム管理者は、クラウドサービスに商用ライセンスのあるソフトウエアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウエアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウエアにおけるライセンス規定に従わなければならない。

１１．６情報セキュリティポリシー違反時の対応

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又は統括情報セキュリティ管理者が違反を確認した場合は、統括ネットワーク管理者、情報システム管理者及び当該職員等の所属の所属情報セキュリティ責任者に通知し、適正な措置を求めなければならない。

イ　統括ネットワーク管理者及び情報システム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統括情報セキュリティ管理者に報告するとともに、当該職員等の所属の所属情報セキュリティ責任者に通知し、適正な措置を求めなければならない。

ウ　所属情報セキュリティ責任者への指導によっても改善されない場合、統括ネットワーク管理者及び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、統括ネットワーク管理者及び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セキュリティ責任者、統括情報セキュリティ責任者、統括情報セキュリティ管理者及び当該職員等の所属の所属情報セキュリティ責任者に通知しなければならない。

１２.業務委託及び外部サービス（クラウドサービス）の利用

１２．１　業務委託

（１）業務委託に係る運用規程の整備

統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備しなければならない。

ア　委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

イ　委託事業者の選定基準

（２）業務委託実施前の対策

ア　所属情報セキュリティ責任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

・データ保護及び管理に関する事項

・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
・県による監査、検査
・県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　所属情報セキュリティ責任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　所属情報セキュリティ責任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管理者へ措置内容の報告（重要度に応じて最高情報セキュリティ責任者に報告）
（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　所属情報セキュリティ責任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　所属情報セキュリティ責任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　所属情報セキュリティ責任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

１２．２　情報システムに関する業務委託

（１）情報システムに関する業務委託における共通的対策

情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに意図しない変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

（２）情報システムの構築を業務委託する場合の対策

情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、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　情報システムのセキュリティ要件の適切な実装

イ　情報セキュリティの観点に基づく試験の実施

ウ　情報システムの開発環境及び開発工程における情報セキュリティ対策

（３）情報システムの運用・保守を業務委託する場合の対策

ア　情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

イ　情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

（４）情報システムの一部の機能を提供するサービスを利用する場合の対策

ア　情報システム管理者又は所属情報セキュリティ責任者は、外部の一般の者が重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

イ　情報システム管理者又は所属情報セキュリティ責任者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

ウ　情報システム管理者又は所属情報セキュリティ責任者は、委託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。

エ　情報システム管理者又は所属情報セキュリティ責任者は業務委託サービスを利用する場合には、統括情報セキュリティ管理者へ当該サービスの利用申請を行わなければならない。

オ　統括情報セキュリティ管理者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

カ　統括情報セキュリティ管理者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

１２．３　外部サービス（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、以下を含む約款による外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定に関する規定を整備しなくてはならない。

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１２．３節において「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）の利用に関する規定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　所属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　所属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しなければならない。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県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、県が取扱う情報に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　所属情報セキュリティ責任者は、イ（ア）から（キ）までの内容を含む情報セキュ

リティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービス（クラウドサービス）が、クラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価しなければならない。

エ　所属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。

オ　所属情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認しなければならない。

カ　所属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。また、クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定め、クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が県によって受容可能か判断しなければならない。

（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

キ　所属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。

ク　所属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せるとともに、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提供し、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なければならない。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。

ケ　所属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しなければならない。また、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なければならない。

コ　所属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正に確保されるよう、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

サ　所属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等から、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しなければならない。

（４）クラウドサービスの利用に係る調達・契約

ア　所属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　所属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　所属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、統括情報セキュリティ管理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　統括情報セキュリティ管理者は、所属情報セキュリティ責任者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。

ウ　統括情報セキュリティ管理者は、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しなければならない。

（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

（オ）クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

イ　クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。また、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ管理者へ報告しなければならない。

ウ　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

エ　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。

オ　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、情報セキュリティ

に配慮した構築の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を確認及び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

（ケ）設計・設定変更時の情報や変更履歴の管理

イ　クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。また、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ管理者へ報告しなければならない。

ウ　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。

エ　所属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。

オ　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。

カ　クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実

践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び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。

ウ　クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

１２．４　外部サービス（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、機密性２以上の情報を取り扱わない場合、以下を含むクラウド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。

（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正な措置を講じなければならない。

イ　所属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。

１３.評価・見直し

１３．１　監査

（１）実施方法

統括情報セキュリティ管理者は、情報セキュリティ監査統括責任者として、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、統括情報セキュリティ責任者の承認を得なければならない。

イ　被監査機関は、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

ア　委託事業者に委託を行っている場合、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。

イ　クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

（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、最高情報セキュリティ責任者に報告する。

（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

ア　統括情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管する所属情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

イ　統括情報セキュリティ責任者は、指摘事項を所管していない所属情報セキュリティ責任者に対しても、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。また、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管理者及び統括ネットワーク管理者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告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

統括情報セキュリティ責任者は、監査結果を情報セキュリティポリシー及び関係規程の見直し、その他情報セキュリティ対策の見直し時に、情報セキュリティ対策推進委員会の意見を踏まえ活用しなければならない。

１３．２　自己点検

（１）実施方法

ア　統括ネットワーク管理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自己点検を実施しなければならない。

イ　部局情報セキュリティ責任者は、所属情報セキュリティ責任者と連携して、所管する部局等における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

（２）報告

統括ネットワーク管理者、情報システム管理者及び部局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、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。

（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　統括情報セキュリティ責任者は、自己点検結果を情報セキュリティポリシー及び関係規程の見直し、その他情報セキュリティ対策の見直し時に、情報セキュリティ対策推進委員会の意見を踏まえ活用しなければならない。

１３．３　情報セキュリティポリシー及び関係規程等の見直し

最高情報セキュリティ責任者は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシーについて定期的及び重大な変化が発生した場合にリスク評価を行い、必要があると認めた場合、情報セキュリティ対策推進委員会の意見を踏まえ改善を行うものとする。

また、統括情報セキュリティ責任者は、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置を実施又は指示し、措置の結果について最高情報セキュリティ責任者に報告しなければならない。

附　則

附　則
　情報セキュリティ対策基準は、平成１４年3月１５日から施行する。
附　則
　情報セキュリティ対策基準は、平成１４年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、平成１６年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、平成１８年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、平成１９年4月１日から施行する。
附　則
　１　情報セキュリティ対策基準は、非公開とする。
　２　情報セキュリティ対策基準は、平成２０年3月２７日から施行する。
附　則
　情報セキュリティ対策基準は、平成２０年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、平成２１年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、平成２３年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、平成２４年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、平成２５年4月１日から施行する。
附　則
　１　情報セキュリティ対策基準は、平成２８年3月２５日から施行する。
　２　ただし、「別表第１」及び「別表第２」の「企業土地管理局経営管理課長」は、
　　平成２８年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、平成２９年4月１日から施行する。
附　則
　１　情報セキュリティ対策基準は、平成３１年4月１日から施行する。
　２　情報セキュリティ対策基準は、公開とする。
附　則
　情報セキュリティ対策基準は、令和３年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、令和４年4月１日から施行する。
附　則
　情報セキュリティ対策基準は、令和４年6月１日から施行する。
附　則
　情報セキュリティ対策基準は、令和６年8月３０日から施行する。

附　則

情報セキュリティ対策基準は、令和７年４月１日から施行する。

附　則

情報セキュリティ対策基準は、令和８年１１月４日から施行する。

別表第１　部局情報セキュリティ責任者

担当部局	役　職　名
総務部	総務課長
総合企画部	政策企画課長
防災危機管理部	危機管理政策課長
健康福祉部	健康福祉政策課長
環境生活部	環境政策課長
商工労働部	経済政策課長
農林水産部	農林水産政策課長
県土整備部	県土整備政策課長
出納局	出納局長
企業局	管理部業務振興課長
病院局	経営管理課長
県議会事務局	総務課長
教育庁	企画管理部教育総務課長
監査委員事務局	調整課長
人事委員会事務局	任用課長
労働委員会事務局	審査調整課長
海区漁業調整委員会事務局	事務局長
収用委員会事務局	事務局長