福島県情報セキュリティポリシー

（令和５年６月５日　福島県デジタル社会形成推進本部決定）

第１部 情報セキュリティ基本方針

今日、県民生活の場に情報通信技術が急速に普及し、電子メールのやり取りや、ホームページの閲覧、電子商取引などが広く行われるようになり、経済面や生活面において様々な変化が起きています。

一方で、情報通信技術の利用に係る事故や犯罪、操作ミス、さらには、自然災害による情報システムの障害が発生すれば県民生活に多大な影響を与えます。

本県でも、行政サービスを提供するため、多くの業務において情報通信技術を活用しており、個人情報や行政運営上重要な情報などの多数の情報資産を保有しています。

これらの情報資産を様々な脅威から防ぐことは、県民の権利及び利益を守り、行政サービスを継続して提供するために必要不可欠です。

そこで、本県は、情報セキュリティ対策に以下のとおり取り組むことを宣言します。

１　情報セキュリティを確保するため、全庁的な組織体制を整備します。

２　情報セキュリティ対策の統一的な基準として「情報セキュリティ対策基準」を定め、それぞれの情報システムごとに「情報セキュリティ実施手順」を定めます。

３　保有する情報資産について、管理者を定め、適正に管理します。

４　情報セキュリティ対策の重要性を認識させるため、職員等に対して必要な教育を実施します。

５　情報セキュリティに関する事故が発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定めます。

６　情報セキュリティポリシーが遵守されていることを検証するため、監査及び自己点検を実施します。

７　情報セキュリティを取り巻く状況の変化及び監査結果を踏まえて、情報セキュリティポリシーを見直します。

８　公社等外郭団体においては、本対策基準等を参考に、各団体において情報セキュリティ対策に係る基本方針を策定するなど、必要な情報セキュリティ対策を実施するよう、所管部局は適正に助言等を行うこととする。

９　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、業務の遂行において、情報セキュリティの関係法令並びに情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守します。

第２部 情報セキュリティ対策基準

目　　次

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

第１　対象範囲

１　適用範囲

この対策基準は、(1)から(3)に該当する者（以下「職員等」という。）に適用する。

(1) 知事、副知事、会計管理者及び病院事業管理者並びに以下の組織に属する職員

ア　知事部局
イ　企業局
ウ　病院局
エ　議会事務局
オ　教育庁、図書館、美術館及び博物館
カ　県立学校、教育センター、特別支援教育センターの別に定める事務部門
キ　警察本部の福島県情報通信ネットワークシステムを使用する事務部門
ク　選挙管理委員会事務局
ケ　監査委員事務局
コ　人事委員会事務局
サ　労働委員会事務局
シ　収用委員会
ス　福島海区漁業調整委員会事務局
セ　内水面漁場管理委員会

(2) 以下の組織に属する委員

ア　教育委員会
イ　選挙管理委員会
ウ　人事委員会
エ　労働委員会
オ　収用委員会
カ　福島海区漁業調整委員会
キ　内水面漁場管理委員会

(3) 監査委員

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。（警察本部における福島県情報通信ネットワークシステム以外のもの並びに教育委員会における教育分野に係るものを除く。以下同様とする。）

(1) ネットワーク

通信回線、ルーター等の通信機器

(2) 情報システム及びこれらに関する設備

ア　パソコン、タブレット、スマートフォン等（以下「端末」という。）、サーバ、ソフトウェア等で構成され情報処理を行うシステム（単体で情報処理を行うシステムを含む。）

イ　配電盤、電源ケーブル、通信ケーブル等の設備

(3) 記録媒体

通信機器や情報システム等に内蔵された記録媒体、ＵＳＢメモリ、ＤＶＤ，ブルーレイディスク、デジカメ等の外部記録媒体

(4) ネットワーク及び情報システムで取扱う情報（これらを印刷した文書を含む。）
(5) 情報システムの仕様書及びネットワーク図等のシステム関連文書

第２　組織及び体制

県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。（別紙１参照）

１　最高情報セキュリティ責任者（CISO：Chief Information Security Officer）

(1) 知事の職務を代理する副知事の順序を定める規則で定める第１順位副知事を、最高情報セキュリティ責任者（以下「CISO」という。）とする。

(2) CISO は、県における情報資産の情報セキュリティ対策を統括し、ネットワーク、情報システム及び端末に係る開発、設定の変更、運用及び更新を行う最終的な権限及び責任を有する。

(3) CISO は、情報セキュリティの統一的な窓口として、情報セキュリティ対策チーム（CSIRT：Computer Security Incident Response Team）を整備し、役割を明確化して、情報セキュリティに関する事案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。

(4) CISO は、必要に応じ、情報セキュリティ対策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くことができる。

２　ネットワーク管理者（CISO 補佐）

(1) 企画調整部次長（情報統計担当）を、CISO を補佐するネットワーク管理者（以下「CISO 補佐」という。）とする。

(2) CISO 補佐は、県における情報資産の情報セキュリティ対策に係る権限及び責任を有する。

(3) CISO 補佐は、県におけるネットワーク、情報システム及び端末に係る開発、設定の変更、運用及び更新を行う権限及び責任を有する。

(4) CISO 補佐は、職員等に対して情報セキュリティ対策に係る指導及び助言を行う権限及び責任を有する。

(5) CISO 補佐は、県の情報資産の情報セキュリティが侵害された場合、又は侵害のおそれのある場合は、軽微なものを除き、CISO に速やかに報告するとともにその指示に従い、必要な対策を講じなければならない。

(6) CISO 補佐は、CISO が不在等の場合は、CISO の職務を代行する。

(7) CISO 補佐は、県の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権限及び責任を有する。

(8) CISO 補佐は、緊急時等における円滑な情報共有を図るため、CISO、CISO 補佐、統括情報セキュリティ管理者、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を網羅する連絡体制を整備しなければならない。

３　情報セキュリティ対策チーム（CSIRT:Computer Security Incident Response Team）

(1) 情報セキュリティ対策チーム（以下「CSIRT」という。）は、CSIRT 責任者、CSIRT 管理者及び CSIRT 要員をもって構成する。

(2) CSIRT 責任者は、CISO 補佐をもって充てる。

(3) CSIRT 管理者は、デジタル変革課長をもって充てることとし、CSIRT 要員は、CSIRT 管理者が指名する。

(4) CSIRT は、CISO による情報セキュリティ対策の意思決定が行われた際には、その内容を４に規定する統括情報セキュリティ管理者等に提供する。

(5) CSIRT は、情報セキュリティに関する事案を発見した場合又は報告を受けた場合には、総務省等へ報告するとともに、事案を事例としてとりまとめ、５に規定する情報セキュリティ管理者及び７に規定する情報システム管理者に情報提供する。

(6) CSIRT は、情報セキュリティに関する事案を発見した場合又は報告を受けた場合には、その重要度や影響範囲等を勘案し、７に規定する情報システム管理者の対策を支援する。
(7) CSIRT は、情報セキュリティ対策に関して、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機能を有する部署、外部の事業者等との情報共有を行う。

4　統括情報セキュリティ管理者
(1) 各部局長、議会事務局長、教育長及び各委員（会）事務局長を、その部局等の統括情報セキュリティ管理者とする。
(2) 警察本部においては、警察本部長が指名した者を統括情報セキュリティ管理者とする。
(3) 統括情報セキュリティ管理者は、所管する部局等における情報セキュリティ対策に係る統括的な権限及び責任を有する。
(4) 統括情報セキュリティ管理者は、所管する部局等における情報システムの開発、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。
(5) 統括情報セキュリティ管理者は、所管する部局等における情報セキュリティポリシーの遵守に係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権限及び責任を有する。
(6) 統括情報セキュリティ管理者は、所管す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を行わなければならない。

5　情報セキュリティ管理者
(1) 知事公室長、各部局の政策監及び次長、議会事務局次長、教育庁の政策監及び教育次長及び各委員（会）事務局次長を、その所管する総室等の情報セキュリティ管理者（総括担当）とする。
(2) 地方振興局においては、局長を情報セキュリティ管理者（総括担当）とする。
(3) 各部局の課長、県議会事務局の課長、教育庁の課長、各委員（会）事務局の課長、各振興局の部（室）長、各出先機関の長を、その所管組織の情報セキュリティ管理者とする。
(4) 警察本部においては、統括情報セキュリティ管理者が指名した者を情報セキュリティ管理者とする。
(5) 情報セキュリティ管理者（総括担当）は、統括情報セキュリティ管理者の下、所管総室等における情報セキュリティ対策に係る総括的な権限及び責任を有する。
(6) 情報セキュリティ管理者は、統括情報セキュリティ管理者の下、所管組織内における情報セキュリティ対策に係る権限及び責任を有する。
(7) 情報セキュリティ管理者は、所管する情報資産に対するセキュリティ侵害又はそのおそれのある場合は、CSIRT 責任者へ速やかに報告を行い、指示を受けなければならない。
(8) 情報セキュリティ管理者は、(7)について CSIRT 責任者に報告した後、軽微なものを除き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。

6　情報化テクニカルリーダー（ITL）
(1) 各所属長は、所属の職員の中から情報化テクニカルリーダー(以下、「ITL」という。)を指名する。
(2) ITL は、情報セキュリティ管理者を補佐し、所属における情報セキュリティ対策及び情報リテラシー向上を推進する。
(3) ITL は、情報セキュリティ管理者の下、所属における情報セキュリティポリシー等の遵守に関して職員等に対する教育、訓練、助言及び指示を行う。

7　情報システム管理者

(1) 各情報システムを所管する各部局の課長、県議会事務局の課長、教育庁の課長、各委員（会）事務局の課長、各振興局の部（室）長、各出先機関の長を当該情報システムに係る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の情報セキュリティ対策に係る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（ファイルサーバ、無線ＬＡＮシステムなど単体動作の機器のみで構成された情報システムを含む。）に係る開発、設定の変更、運用及び更新を行う権限及び責任を有する。

(4) 情報システム管理者は、著しく不適切な利用者を発見した場合は、利用を制限し、又は停止することができる。

(5) 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を策定し、職員等に周知徹底を図らなければならない。

(6) 情報システム管理者は、情報セキュリティ実施手順を策定又は見直した場合、CISO 補佐に報告しなければならない。

8　情報システム担当者

情報システム管理者の指示に従い、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。

9　情報セキュリティ監査統括責任者

(1) 企画調整部次長（情報統計担当）を、情報セキュリティ監査統括責任者とする。

(2) 情報セキュリティ監査統括責任者は、福島県情報セキュリティ監査実施要綱を定め、監査実施計画を立案し、定期的に又は必要に応じて監査を実施する。

(3) 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は、被監査部門から独立した十分な専門的知識を有する者に対して、監査の実施を依頼することとする。

10　情報セキュリティ専門検討会

情報セキュリティ対策のうち重要な事項について調査検討するため、情報セキュリティ専門検討会を設置する。

11　兼務の禁止

(1) 情報セキュリティ対策の実施に係る、承認又は許可の申請を行う者とその承認又は許可を行う者は、やむを得ない場合を除き、同一人が兼務してはならない。

(2) 監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同一人が兼務してはならない。

第３　情報資産の分類及び管理

１　情報資産の分類

情報資産については、事業、業務、機能等の単位で、情報の機密性、完全性及び可用性の観点から、別紙２に定める基準に従い分類し、必要に応じて取扱制限を行った上で管理するものとする。

２　情報資産の管理責任

(1) 情報セキュリティ管理者は、その所掌する情報資産を管理する責任を有する。

(2) 情報システム管理者は、所掌する情報システムを管理する責任を有する。

３　情報資産の分類の表記

職員等は、別紙２の基準に従いファイル、記録媒体等に情報資産の分類を表示し、又は情報資産の分類一覧表を作成するほか、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。

４　情報システムで取り扱う情報資産の範囲

(1) 情報システムで取り扱う情報資産の範囲の明確化

ア　情報システム管理者は、所管する情報システムに登録することができる情報資産を定めなければならない。

イ　情報システム管理者は、所管する情報システムに登録された情報資産を閲覧することができる者を定めなければならない。

(2) 取り扱う情報資産の範囲の確認

職員等は、情報システムに機密性２以上、完全性２又は可用性２以上の情報資産を登録する場合は、(1)の情報システムで取り扱う情報資産の範囲を確認しなければならない。

５　情報資産の作成、編集

(1) 職員等は、業務上必要のない情報資産を作成し、又は編集してはならない。

(2) 情報資産を作成する者は、その作成時に別紙２の基準に従い当該情報資産の分類を定めなければならない。

(3) 情報資産を作成し、又は編集する者は、作成又は編集途上の情報資産についても、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。

６　情報資産の入手、複写

(1) 情報資産を入手し、又は複写する者は、入手後又は複写後の情報資産の機密性については入手元又は複写元の情報資産の機密性の分類に従い、完全性と可用性については新たに情報資産の分類を定めなければならない。

(2) 情報資産の分類の表示がない情報資産を入手し、又は複写した場合は、別紙２の基準に従い当該情報資産の分類を定めなければならない。

(3) 入手し、又は複写した情報資産の分類が不明な場合は、情報セキュリティ管理者又は情報システム管理者に判断を仰がなければならない。

７　情報資産の利用

(1) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

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

(3) 記録媒体を扱う者は、当該記録媒体に保管されている情報資産のうち、機密性、完全性、可用性の最も高い分類に従い記録媒体を扱わなければならない。

8　情報資産の保管

(1) 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い、情報資産を適正に保管しなければならない。

(2) 機密性２以上、完全性２又は可用性２以上の情報資産を記録した外部記録媒体を保管する場合は、施錠するなどの安全対策を講じた場所に保管しなければならない。

(3) 完全性２又は可用性２以上の情報資産を記録した外部記録媒体を保管する場合は、火災、異常発熱、漏水、結露及び静電気の安全対策を講じた場所に保管しなければならない。

9　情報の送信及び情報資産の運搬

(1) 業務上必要のない相手に情報を送信してはならない。また、誤送信しないように宛先について細心の注意を払わなければならない。

(2) インターネット等安全ではないネットワークを用いて機密性２以上の情報を送信する者は、パスワード等による暗号化等により、第三者に入手されても解読できないような安全措置を講じた上で送信しなければならない。

(3) 車両等により機密性２以上の情報資産を運搬する場合は、鍵付きのケース等への格納又はパスワード等による暗号化等により、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。

(4) 機密性２以上の情報資産を運搬する場合は、所管する情報セキュリティ管理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。

10　情報資産の提供及び公表

(1) 機密性２以上の情報資産を外部に提供する者は、提供する相手方のシステムの運用方針及びセキュリティ対策が当該情報資産の機密性と合致していることを確認の上、提供しなければならない。

(2) 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等を行わなければならない。

(3) 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又は情報システム管理者の許可を得なければならない。

(4) 情報セキュリティ管理者及び情報システム管理者は、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。

11　情報資産の廃棄等

(1) 情報資産が不要となった場合は、記録媒体の初期化など情報を復元できないように消去した上で、廃棄又は返却若しくは他の部局等への移管を行わなければならない。

(2) 重要な情報資産を扱ったことがある記録媒体の廃棄等については、情報セキュリティ管理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。なお、廃棄等に係る日時、担当者及び処理内容を記録しなければならない。

(3) 機密性３の情報資産を扱ったことがある記録媒体が不要になった場合は、その記録を保持しているディスクそのもの又は記憶素子を物理的に破壊し、又は記録媒体完全消去用のソフトウェア等で、データの復活が不可能になるよう処理した上で廃棄等を行わなければならない。

(4) 端末、サーバ、接続機器、記録媒体等を廃棄する場合は、関連法に従い適正に廃棄処理

を行わなければならない。

第４　ネットワークの強靭性の向上

１　ネットワークの分離

県の基幹ネットワークである福島県情報通信ネットワークシステムについて、所管する情報システム管理者は、次の三つのネットワークに分離した上でネットワークごとの対策を講じる。

(1) マイナンバー利用事務系（個人番号利用事務系）

ア　マイナンバー利用事務系（個人番号利用事務系）とは、個人番号利用事務（社会保障、地方税若しくは防災に関する事務）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。

イ　マイナンバー利用事務系においては、原則として、(2)及び(3)のネットワークとの通信をできないようにしなければならない。

ウ　やむを得ず、マイナンバー利用事務系と LGWAN 接続系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。

エ　マイナンバー利用事務系においては、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。

オ　USB メモリ等の電磁的記録媒体を使用してマイナンバー利用事務系から、情報を持ち出す場合は、情報セキュリティ管理者の許可を得なければならない。

(2) LGWAN（※）接続系

ア　LGWAN（※）接続系とは、県庁グループウェア（ファイル共有、掲示板等を使用するシステム）や、人事給与、財務会計及び文書管理等の LGWAN（※）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。

※LGWAN：地方公共団体間のコミュニケーションの円滑化、情報の共有による情報の高度利用を図ることを目的とし、国関係機関及び地方公共団体間との閉域網で高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク）

イ　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、次の方法により実施しなければならない。

(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

(3) インターネット接続系

ア　インターネット接続系は、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。

イ　インターネット接続系においては、県内市町村と共同でインターネット接続口を集約する自治体情報セキュリティクラウドを設置し、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、情報セキュリティに関する事案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。

第５　物理的セキュリティ対策

１　サーバ等の設置条件

(1) 情報システム管理者は、ファイルの保管、入出力、集中処理及び通信制御などのサービスを提供する機器（以下「サーバ等」という。）を、火災、水害、埃、振動、温度、湿度及び静電気の影響を可能な限り排除した場所に設置し、かつ、容易に取り外すことができないよう、固定するなどの適正な措置を講じなければならない。

(2) 情報システム管理者は、可用性２以上の情報を格納するサーバ、セキュリティサーバ、住民サービスに関するサーバ等重要なサーバ等を多重化し、同一データを複数保持しなければならない。

(3) 情報システム管理者は、可用性３の情報を格納しているサーバ等については、必要に応じ、移設できるように設置するものとする。

２　電源

(1) 可用性２以上のサーバ等の機器については、電源の停止時に自動的にサーバ等を停止する機能を備えた予備電源を設置することとし、予備電源の容量は、当該機器を安全に停止するまでの間、十分に電力を供給することができるものとする。

(2) 情報システム管理者は、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るものとする。

３　配線

(1) 各情報システム管理者及び情報セキュリティ管理者は、配線が損傷等を受けることがないよう、配線収納管の使用等適正な措置を講じるものとする。

(2) 情報システム管理者は、担当する主要な箇所の配線について、損傷がないかどうか適宜点検を行わなければならない。

(3) 情報セキュリティ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。

(4) 配線の変更や追加は、該当する情報システム管理者、情報セキュリティ管理者及び契約により操作等を認められた事業者に限り行うものとし、それ以外の者が変更又は追加を行うことがないよう、必要な措置を講じなければならない。

４　機器の定期保守及び修理

(1) 情報システム管理者は、可用性２以上のサーバ等の機器について、重要性に応じ定期保守を実施しなければならない。

(2) 情報システム管理者は、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、当該事業者と守秘義務契約を締結する等、秘密保持の対策を講じなければならない。

５　県が所管する施設以外の場所に設置する情報システム

(1) 県が所管する施設以外の場所（以下「外部の場所」という。）に情報システムを設置する場合は、CISO 補佐の許可を得なければならない。

(2) 情報システム管理者は、定期的に当該情報システムの情報セキュリティの水準について確認し、それが求められる水準を下回らないようにしなければならない。

(3) 外部の場所に持ち出す情報資産については、利用箇所及び利用方法を明確にし、管理簿を設けるなど適正に管理しなければならない。

6　情報システム室

情報システム及び記録媒体の保管庫を執務室以外に設置するための施設（以下「情報システム室」という。）を設ける場合、以下のセキュリティ対策を講じなければならない。

(1) 情報システム室は、出入口を限定し、鍵、監視機能、警報装置等により、許可されていない者の立入りを防止し、許可無く出入りすることを禁止すること。

(2) 情報システム管理者は、IC カード、指紋認証等の生体認証又は入退室管理簿の記載により情報システム室への入退室管理を行うこと。

(3) 職員等及び契約により立ち入りを認められた事業者は常に身分を証明できるものを携帯し、求めがあった場合にはこれを提示すること。

(4) 情報システム管理者は、情報システム室に新たに機器等を搬入する場合には、あらかじめ職員等又は委託した業者に当該機器等の既存情報システムに対する影響の有無を確認すること。

(5) 情報システム管理者は、機器等の搬入に職員が立ち会うなど、当該情報システムの設置に必要な措置を講じること。

(6) 情報システム管理者は、外部からの訪問者が情報システム室に入る場合には、必要に応じて立ち入り区域を制限した上で、職員を付き添わせること。

(7) 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、防火対策、防水対策等を講じること。

(8) 情報システム管理者は、情報システム室に配置する消火薬剤や消防用設備等が機器等及び記録媒体に影響を与えないように配備すること。

(9) 情報システム管理者は、可用性３の情報資産に係るサーバ等については、耐震対策が講じられた建物に設置すること。

(10) 情報システム管理者は、当該情報システムに関連しない、または個人所有である端末、通信回線装置、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。

7　ネットワーク

(1) 情報システム管理者は、庁内の通信回線及び通信回線装置を適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

(2) 情報システム管理者は、外部の場所とのネットワーク接続は必要最小限に限定し、かつ、できる限り接続ポイントを減らさなければならない。また、外部の場所とのネットワーク接続について CISO 補佐へ報告しなければならない。

(3) 情報システム管理者は、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。

(4) 情報システム管理者は、ネットワークに使用する回線について、伝送途中に情報の破壊、盗聴、改ざん、消去等が生じないよう、十分なセキュリティ対策を講じなければならない。

(5) 情報システム管理者は、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　盗難の防止

(1) 情報システム管理者及び情報セキュリティ管理者は、情報資産の盗難防止のため、執務室等で利用する端末のワイヤーによる固定、モバイル端末及び記録媒体の使用時以外の施錠保管、執務室等に施錠するなどの対策を講じなければならない。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、端末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。同様に、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。

9　サーバ等の画面の管理

情報システム管理者は、サーバ等の設置に当たっては、情報が漏えいしないよう、必要なときのみ画面を表示することとする。

10　職員等の使用する端末の管理

情報セキュリティ管理者又は情報システム管理者は、所管する端末を職員等が利用するときは、認証を必要とするように設定しなければならない。

第６　人的セキュリティ対策

１　職員等の遵守事項

(1) すべての職員等は、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。この場合において、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、指示を受けなければならない。

(2) 職員等は、職務の遂行においては、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　地方公務員法(昭和２５年法律第２６１号)

イ　著作権法（昭和４５年法律第４８号）

ウ　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）

エ　個人情報の保護に関する法律（平成１５年法律第５７号）

オ　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）

カ　サイバーセキュリティ基本法（平成２６年法律第１０４号）

キ　福島県個人情報保護条例（平成６年福島県条例第７１号）

(3) 業務目的外での利用等の禁止

ア　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。

イ　職員等は、利用する権限のない情報資産を利用してはならない。

ウ　職員等は、電子データの不当な変更又は消去若しくは虚偽情報の作成を行ってはならない。

(4) 可用性２以上である情報の処理を行う職員等は、ネットワークが長期に停止した場合を想定し、手作業での処理方法を参照できるよう準備しなければならない。

(5) データ入出力時の正確性の確認

職員等は、情報システムに入出力する場合はデータが正確であることをその都度確認しなければならない。

(6) 端末の持ち出し及び外部における情報処理作業の制限

ア　情報システム管理者は、所管の情報システムで使用する機密性２以上、可用性２以上又は完全性２の情報資産を外部で使用又は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　CISO 補佐は、特定の情報システム以外で使用する機密性２以上、可用性２以上又は完全性２の情報資産を外部で使用する場合における、安全管理措置を定めなければならない。

ウ　職員等は、情報資産を外部に持ち出す場合は、情報セキュリティ管理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。

エ　職員等は、外部で情報処理作業を行う際、県が管理していない情報機器を用いる場合には、事前に情報セキュリティ管理者又は情報システム管理者の許可を得、かつ、該当する安全管理措置に関する規定を遵守しなければならない。また、機密性３の情報資産については、秘密保守契約を結んだ業者によるもの以外、県が管理していない情報機器による情報処理を行ってはならない。

(7) 端末の接続

職員等は、県が管理していない情報機器及び記録媒体を県の管理するネットワーク及び情報機器に接続してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者

の許可を得て、これらを接続することができる。また、業務が特定の情報システムにかかわる場合は、所管の情報システム管理者の許可も得なければならない。

(8) 異なるネットワークへの接続

職員等は、県が管理している情報機器及び記録媒体を、有線・無線を問わず、当該情報機器及び記録媒体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。

(9) 持ち出し及び持ち込みの記録

情報セキュリティ管理者及び情報システム管理者は、業務上必要な場合において、端末や記録媒体等の持ち出し及び持ち込みを許可する場合について、記録を作成し、保管しなければならない。

(10) 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。

(11) 机上の端末等の管理

職員等は、席を離れるときは、端末をロックし、及びディスプレイを消去し、並びに記録媒体、文書等を容易に閲覧されない場所へ保管するなどの適正な措置を講じなければならない。

(12) 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外部へ漏らしてはならない。

2　非常勤職員及び会計年度任用職員への対応

(1) 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び会計年度任用職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

(2) インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤職員及び会計年度任用職員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等一部の機能を業務で使用しないときは、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

情報システム管理者及び情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び情報セキュリティ実施手順を閲覧できるようにしなければならない。

4　委託事業者に対する説明

情報システム管理者又は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、保守等を事業者に委託する場合は、委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち委託事業者が遵守しなければならない事項を説明しなければならない。

5　教育及び訓練

(1) CISO 補佐は、説明会の開催等により、すべての職員等及び関係者に対し、セキュリティ対策について周知徹底しなければならない。

(2) 情報システム管理者は、最新の技術力を維持するため、情報システム担当者に研修を受

けさせなければならない。
(3) 情報システム管理者は、所管の情報システムについて、説明会の開催等により、職員等及び関係者に対しセキュリティ対策を周知徹底しなければならない。
(4) CISO 補佐は、緊急時におけるセキュリティ対策について、すべての職員等及び関係者に周知しなければならない。また、必要に応じて、緊急時対応を想定した訓練を実施することとする。
(5) CISO 補佐は、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。
(6) 情報セキュリティ管理者は、新規採用の職員等を対象に、業務上必要となる情報資産の取り扱いに関し、情報セキュリティ対策について事前に研修を実施しなければならない。
(7) 研修は、各職員等それぞれの役割、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。
(8) 幹部を含めたすべての職員等は、定められた研修及び訓練に参加しなければならない。
(9) 情報システム管理者は、所管の情報システムが長期にわたり停止することを念頭に置き、手作業での処理方法を明示しておかなければならない。

6　情報セキュリティに関する事案の報告
(1) 庁内からの情報セキュリティに関する事案の報告
ア　職員等は、不正アクセスやコンピュータウイルス等、情報セキュリティに関する事案を発見した場合、速やかに情報セキュリティ管理者及び当該事案の影響を受ける又は受けるおそれのある情報システムの情報システム担当者に報告しなければならない。
イ　職員等は、利用する情報システムの異常及び故障を発見した場合、速やかに情報システム担当者に報告しなければならない。
ウ　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、速やかに情報セキュリティ管理者及び当該違反行為の影響を受ける又は受けるおそれのある情報システムの情報システム担当者に報告しなければならない。
エ　ア～ウの職員等の報告について、ITL は職員等の状況把握等を支援しなければならない。
オ　ア～ウの報告を受けた情報システム担当者は速やかに情報システム管理者に報告しなければならない。
カ　情報システム管理者は、報告のあった事案のうち、県民等や業務に影響が生じたものについて、CSIRT に報告しなければならない。
キ　情報システム管理者は、報告のあった事案について、必要に応じて CISO 及び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。
ク　事案のうち重大なものは「第９　緊急時におけるセキュリティ対策」により対処する。
(2) 県民等外部からの事案の報告
ア　職員等は、県が管理するネットワーク、情報システム等の情報資産に関する事故又は不具合について、県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及び事故又は不具合の報告があった情報システムの情報システム担当者に報告しなければならない。
イ　アの職員等の報告について、ITL は職員等の状況把握等を支援しなければならない。
ウ　アの報告を受けた情報システム担当者は速やかに情報システム管理者に報告しなければならない。
エ　情報システム管理者は、報告のあった事案のうち、県民等や業務に影響が生じたものについて、CSIRT に報告しなければならない。

オ　報告を受けた情報システム管理者は、必要に応じて CISO 及び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。

カ　事案のうち重大なものは「第９　緊急時におけるセキュリティ対策」により対処する。

(3) 事案の分析・記録等

ア　CSIRT は、事案が起きた部門の情報セキュリティ管理者及び情報システム管理者と連携し、これらの事案を分析し、記録を保存しなければならない。また、情報セキュリティに関する事案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。

イ　CISO は、CSIRT から、情報セキュリティに関する事案について報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

第７　技術的セキュリティ対策

１　コンピュータ及びネットワークの管理

(1) 所属内のファイルサーバ

ア　情報システム管理者は、所属の複数の職員等が共同で利用するファイルサーバを適正に管理しなければならない。

イ　情報システム管理者は、他の所属の職員等が利用できないような設定をしなければならない。

ウ　情報システム管理者は、個人情報、人事記録等の特定の情報については、担当以外の職員等が利用できないような設定をしなければならない。

(2) バックアップの実施

情報セキュリティ管理者又は情報システム管理者は、サーバ及び端末に記録された情報について、情報システムの多重化措置にかかわらず、その重要性に応じ、期間を設定し、定期的にバックアップを行うこととする。

(3) 無許可でのソフトウェアの導入、利用及び機器構成の変更の禁止

ア　汎用 OS で動作する端末ハードウェアを管理する情報システム管理者は、端末で利用を認めるソフトウェアと機器（以下「利用許可ソフトウェア等」という。）及び利用を禁止するソフトウェアと機器（以下「利用禁止ソフトウェア等」という。）を定めなければならない。

イ　職員等が業務上の必要から新たなソフトウェアを端末に導入する場合又は端末若しくはネットワークについて機器の増設若しくは交換を行う場合は、情報セキュリティ管理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。

ウ　情報セキュリティ管理者又は情報システム管理者は、イの許可を行う場合には、利用許可ソフトウェア等を除いて、CISO 補佐に協議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、ソフトウェアを導入する場合は、メーカー等のサポートが利用期間において継続していることを確認し、かつ、ソフトウェアのライセンスを管理しなければならない。

オ　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。

カ　職員等は、利用禁止ソフトウェア等が導入されている場合は削除しなければならない。

(4) 業務以外の目的でのシステムの利用の禁止

CISO 補佐は、アクセス記録等から職員等が明らかに業務に関係のないシステムの利用や外部サイトの閲覧を行っていることを発見した場合は、統括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。

(5) 端末の取扱い

ア　職員等は、ユーザ ID 及びパスワードの入力後、システムが利用可能な状態で端末を放置してはならない。

イ　職員等は、ディスプレイ上に表示を残したまま、端末を放置してはならない。

(6) 持ち出した端末の取扱い

情報セキュリティ管理者又は情報システム管理者は、執務室外に持ち出すことを前提に導入した端末については、盗難等の際に第三者により情報が窃取されることを防止するための端末のデータの暗号化、著しい回数認証に失敗した場合のデータの自動消去、機密性２以上の情報は端末ではなくサーバ等に保存するなどの対策を講じなければならない。

(7) 複合機、特定の用途に使用される端末の取扱い

ア　情報システム管理者は、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器（以下「複合機」という。）を導入する場合、適正

なセキュリティ機能要件を満たしたものを選定しなければならない。

イ　複合機がリモートメンテナンス等の目的でインターネットを介して外部と通信する場合は、CISO 補佐の許可を得なければならない。

ウ　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、測定機器等の特定の用途に使用される端末の導入については、CISO 補佐と協議し利用環境に応じた適正なセキュリティ設定を実施しなければならない。

(8) ソフトウェアの管理

情報セキュリティ管理者又は情報システム管理者は、サーバ等、端末にインストールされたソフトウェアについて、以下の管理を行わなければならない。

ア　利用しているソフトウェアのバージョンについて、脆弱性を解消するアップデートが配布されていないか随時調査し、配布されている場合は、アップデートを適用しソフトウェアの利用を継続するか、又はアップデートせずにソフトウェアを削除する。

イ　利用しているソフトウェアのバージョンについて、サポートが継続されているか随時調査し、サポートが終了している場合は、ソフトウェアを削除する。

2　情報システムの仕様書、作業記録等の管理

(1) 情報システム仕様書等の管理

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、操作マニュアル等について、記録媒体に関わらず、権限のない者が閲覧したり、紛失することがないよう、適正に管理しなければならない。

(2) 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仕様書等又はプロトタイプを含むソフトウェアなどの情報を交換する場合、その用途等を明確にして、目的外利用や紛失、改ざん等が起こらないよう、その取扱いに関する事項をあらかじめ定め、CISO 補佐の許可を得なければならない。

(3) 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設定又は構成の変更を行った場合は、その記録を残し、詐取、改ざん等をされないように適正に管理しなければならない。

イ　情報システム管理者は、所管する情報システムの変更を行う場合は、手順書を作成し、当該手順書のとおり、職員等に行わせなければならない。

ウ　情報システム担当者又は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名以上で作業を行わなければならない。ただし、１名で作業する場合において、作業直後に他の担当者が確認できるような作業詳細を記録し、複数人でその作業結果を確認するときはこの限りでない。

(4) アクセス記録の取得等

ア　情報システム管理者は、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（以下「アクセス記録等」という。）を取得し、一定の期間保存しなければならない。

イ　情報システム管理者は、アクセス記録等が詐取、改ざん、誤消去等をされないように必要な措置を講じなければならない。

ウ　情報システム管理者は、システムから自動出力したアクセス記録等について、誤消去等に備えて、外部記録媒体にバックアップしなければならない。

エ　情報システム管理者は、必要に応じてアクセス記録等を点検、分析できるように管理しなければならない。

(5) 障害記録

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、システム障害に係る処理結

果及び課題について、記録し、適正に保存しなければならない。

3　アクセス制御等

(1) アクセス制御

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できる者を定め、アクセスする権限のない職員等がアクセスしないように、システム上制限しなければならない。

(2) 無線 LAN 及びネットワークの盗聴対策

ア　情報システム管理者は、無線 LAN や機密性の低いネットワークを利用したシステムを構築する場合、CISO 補佐の許可を得なければならない。

イ　情報システム管理者は、無線 LAN を利用する場合、解読が困難な暗号及び認証技術を使用しなければならない。

ウ　情報システム管理者は、機密性の低いネットワークで機密性の高い情報を扱う場合、情報の盗聴等を防ぐため、解読が困難な暗号及び認証技術を使用しなければならない。

(3) 外部ネットワークとのネットワーク間接続制限等

ア　情報システム管理者は、所管するネットワークを県の基幹ネットワークである福島県情報通信ネットワークシステム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、CISO 補佐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、庁内のすべてのネットワーク、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、CISO 補佐へ報告しなければならない。また、この確認は定期的に行わなければならない。

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等により県の情報資産の漏洩、破壊、改ざん又はシステムの停止等による業務への影響が生じた場合に対処するため、外部ネットワークの管理者による損害賠償責任を契約書上に担保しておかなければならない。

エ　情報システム管理者は、外部の場所から県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、ファイアウォールなどの、アクセス制御可能な装置を介することとし、直接県のネットワークに接続できない措置を講じなければならない。

オ　情報システム管理者は、通信の手順や方式（プロトコル）は、業務上必要最小限のものに限定する。

カ　情報システム管理者は、利用者の真正性が確保できるよう、必要な措置を講じなければならない。

キ　情報システム管理者は、接続した相手先のセキュリティに問題が認められ、県の情報資産に脅威が生じることが想定される場合には、CISO 補佐の判断に従い、速やかに当該外部ネットワークとの接続を切断しなければならない。

(4) 職員等による外部からのアクセス等の制限

ア　職員等が外部から県の情報システムにアクセスする場合は、CISO 補佐及び所管の情報システム管理者の許可を得なければならない。

イ　CISO 補佐及び情報システム管理者は、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て、県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認めるものとする。

ウ　情報システム管理者は、利用者の真正性が確保できるよう、必要な措置を講じることとし、CISO 補佐に確認を求めなければならない。

エ　情報システム管理者は、外部からのアクセスを認める場合、アクセスに使用する端末

の安全性を検証し、通信途上の情報漏えいを防止するために暗号化等の措置を講じ、CISO 補佐に確認を求めなければならない。

オ　情報システム管理者は、外部からのアクセスに利用する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、CISO 補佐に確認を求めなければならない。

カ　情報セキュリティ管理者又は情報システム管理者は、職員等が外部から持ち帰った端末を県のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

(5) 情報システム間の接続制御及び経路制御並びに停止の連絡

ア　情報システム同士の接続を行う情報システム管理者は、お互いに、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

イ　情報システム管理者は、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　お互いのシステムを接続する各情報システム管理者又は情報セキュリティ管理者は、停電等により相手方ネットワークシステムに影響を与えるおそれがある場合は、接続相手の情報システム管理者へ、連絡しなければならない。

(6) 外部の者が利用できるシステム

情報システム管理者は、外部の者が利用できるシステムについては、不正利用が発生しないように、アクセスを制御する機器の設置又は論理的な回線の分割など、情報セキュリティについて特に強固な対策を講じ、CISO 補佐の許可を得なければならない。

(7) 公衆無線 LAN の利用

ア　公衆無線 LAN を利用する場合は、あらかじめ、使用する回線事業者について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　公衆無線 LAN を利用する場合は、情報セキュリティ管理者の許可を受けた回線事業者の回線以外の回線を使用してはならない。

ウ　公衆無線 LAN を利用する場合は、利用者の ID 及びパスワード、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。

4　電子メール、クラウドサービス等の管理

(1) 電子メールシステムのセキュリティ管理

ア　電子メールシステムを運用する情報システム管理者は、権限のない利用者による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　電子メールシステムを運用する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た場合、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。

ウ　電子メールシステムを運用する情報システム管理者と各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が電子メールアドレスの利用を行う場合、委託事業者を含めた三者で利用方法を取り決めなければならない。

エ　電子メールシステムを運用する情報システム管理者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出したことを検出できるようシステムを構築しなければならない。

オ　電子メールシステムを運用する情報システム管理者は、迷惑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。

(2) 電子メール、クラウドサービスの利用制限

ア　職員等は、業務の都合上、職場の電子メールを自動転送する場合は、情報セキュリティ管理者の許可を得なければならない。この場合において、転送の必要が無くなったときは、即座に転送の設定を解除しなければならない。

イ　情報セキュリティ管理者は、電子メールの自動転送を許可した場合は、CISO 補佐に報告しなければならない。

ウ　職員等は、業務上必要のない相手方に電子メールを送信してはならない。

エ　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。

オ　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。

カ　職員等は、インターネットから利用できるメールサービス、ネットワークストレージサービス等を使用する場合は CISO 補佐の許可を得なければならない。

キ　職員等は、インターネットから利用できるメールサービス、ネットワークストレージサービス等を使用する場合は２段階認証又はこれ以上の強度を持つ認証方法を必ず使用しなければならない。

ク　職員等は、機密性２以上又は完全性２の電子データを外部へ送信する場合は、パスワード等による暗号化等を行わなければならない。

ケ　職員等は、電子メール等で可用性２以上の電子データを送信する場合は、送信先へ着信したことを確認しなければならない。

5　ソーシャルメディアサービスの利用

(1) 情報セキュリティ管理者は、県が管理するアカウントでブログ、ソーシャルネットワーキングサービス、動画共有サイト等の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　ソーシャルメディアサービスで発信できる情報を規定する。

イ　庁内で管理しているウェブサイト内において、利用するソーシャルメディアサービスのサービス名と当該アカウントページへのハイパーリンクを明記するページを設ける。

ウ　運用しているソーシャルメディアサービスの自由記述欄において、庁内ウェブサイト上のページの URL を記載する。

エ　ソーシャルメディアサービスの提供事業者が、「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合は、これを利用する。

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

(2) 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。

(3) 利用するソーシャルメディアサービスごとの責任者を定めなければならない。

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

(5) 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、本県の自己管理 Web サイトに当該情報を掲載して参照可能としなければならない。

6　ユーザ ID の管理

(1) 情報システム管理者によるユーザ ID の管理

情報システム管理者は、ユーザ ID の管理に関し、以下の事項を遵守しなければならない。

ア　情報システムのユーザ ID 登録は、必要な者に限定し、必要最小限の操作が可能となるように設定すること。

イ　ユーザ ID は、個人単位に割り当てること。

ウ　パスワードを情報システム管理者が設定した場合は、利用者本人のみに通知すること。

エ　ユーザ ID の登録及び削除の申出があった場合は、速やかに対応すること。

オ　ユーザ ID は、使用されぬまま放置されないよう、人事管理部門と連携し、点検すること。

カ　上記に掲げるほか、利用者の登録、変更、抹消等の情報管理、職員等の異動、派遣、退職に伴うユーザ ID の取扱いの方法を定めること。

(2) 情報システム管理者による特権を付与されたユーザ ID の管理等

ア　情報システム管理者は、情報システムの管理用ユーザ ID を必要最小限の者にのみ発行し、厳重に管理しなければならない。

イ　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と比較して必要に応じて適宜変更するとともに、入力回数制限等によりセキュリティ対策を強化しなければならない。

ウ　情報システム管理者は、特権を付与された ID による情報システムへの接続は、必要最小限の接続時間に制限しなければならない。

エ　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　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。

(3) 職員等によるユーザ ID の取扱い

職員等は、自己の保有するユーザ ID に関し、次の事項を遵守しなければならない。

ア　ユーザ ID による情報システムへの接続については、必ずパスワード等を併用し、本人であることを認証する設定を行うこと。

イ　自己が利用しているユーザ ID は、他人に利用させないこと。

ウ　職員等間でユーザ ID を共有しないこと。

エ　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、情報システム管理者に通知すること。

(4) 職員等のパスワードの取扱い

職員等は、自己の保有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すること。また、パスワードの照会には一切応じないこと。

イ　パスワードの長さは十分な長さとし、文字列は使用者の名前、誕生日、ユーザ ID など容易に推測可能なものは避け、想像しにくいものとすること。

ウ　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すること。

エ　パスワードは必要に応じて適宜変更し、古いパスワードは再利用しないこと。

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ないこと。

カ　仮のパスワード（初期パスワードを含む）は、最初のログイン後直ちに変更すること。
キ　サーバ、ネットワーク機器及び端末にパスワードを記憶させないこと。
ク　職員等間でパスワードを共有しないこと（ただし、共用 ID に対するパスワードは除く。）。

(5) 情報システム管理者による認証情報の管理

ア　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。また、暗号化なしにパスワードファイルを保存してはならない。
イ　情報システム管理者は、職員等にパスワードを発行する際、仮のパスワードを発行した場合は、最初の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　情報システム管理者は、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用しなければならない。
エ　情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外にＩＣカード、生体認証等の二要素認証を併用しなければならない。
オ　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。
カ　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) IC カード等の取扱い

ア　職員等は、自己の管理する IC カード等は、職員等間で共有してはならない。
イ　職員等は、業務上必要のないときは、IC カード等をカードリーダ若しく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　職員等は、IC カード等を紛失した場合、速やかに情報セキュリティ管理者及び情報システム管理者に報告し、その指示に従わなければならない。
エ　情報システム管理者は IC カード等の紛失の報告があり次第、速やかに当該 IC カード等を使用した情報システムの利用を停止しなければならない。
オ　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。

7　情報システムの調達及び保守等

(1) 情報システムの調達

ア　情報システム管理者は、情報システムの開発、導入、保守等に当たっては、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　情報システム管理者は、機器及びソフトウェアを調達する場合、入手先の信頼性を調査すると共に、誓約書を提出させる等、当該製品が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。
ウ　情報システム管理者は、調達仕様書を一般に公開する場合、それが情報セキュリティ確保の上で秘匿すべき情報を含んでいないことを確認しなければならない。
エ　情報システム管理者は、調達仕様書を CISO 補佐に報告しなければならない。
オ　情報システム管理者は、開発及び導入用の情報セキュリティ実施手順を作成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。

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。

ウ　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。

エ　情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

オ　情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

(3) 情報システムの導入

ア　情報システム管理者は、システムの開発保守及びテストの環境からシステムの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。

イ　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、情報システムの停止等の影響を最小限に抑えなければならない。

ウ　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。

エ　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際、十分な試験を行わなければならない。

オ　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動作確認を行わなければならない。

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

(4) システム開発保守に関連する資料等の保管

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文書を適正な方法で保管しなければならない。

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。

(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、範囲及び妥当性をチェックする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、故意又は過失により情報が改ざんされ又は漏えいさせられるおそれがある場合、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) ソフトウェアの更新等

情報システム管理者は、ソフトウェアの修正及び更新に際しては、不具合及び他のシステムとの不整合の有無を事前に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、システムの更新又は統合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又は統合後の業務運営体制の検証を行わなければならない。

8　不正プログラム対策

(1) CISO 補佐の措置事項

コンピュータウイルス等の不正プログラム対策として、次の事項の措置を講じなければならない。

ア　外部ネットワークから受信したファイルについて、外部ネットワークとの接続点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、システムへの侵入を防止する措置が講じられていることを確認すること。

イ　外部ネットワークへ送信するファイルは、外部ネットワークとの接続点において一元的に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、外部へのウィルス拡散を防止する措置が講じられていることを確認すること。

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すること。

エ　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、運用を行っていることを確認すること。

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が最新の状態に保たれていることを確認すること。

カ　不正プログラム対策のソフトウェアが最新の状態に保たれていることを確認すること。

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いないことを確認すること。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すること。

(2) 情報システム管理者の措置事項

各情報システム管理者は、コンピュータウイルス等の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　外部ネットワークとの接続点を持つ情報システムを管理する場合、福島県情報通信ネットワーク以外のネットワークから受信したファイルについて、外部ネットワークとの接続点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、システムへの侵入を防止すること。また、不正プログラムのチェックを行う構成について CISO 補佐に報告すること。

イ　外部ネットワークとの接続点を持つ情報システムを管理する場合、福島県情報通信ネットワーク以外のネットワークへ送信するファイルについて、外部ネットワークとの接続点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、外部へのウィルス拡散を防止すること。また、不正プログラムのチェックを行う構成について CISO 補佐に報告すること。

ウ　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常駐させ、ファイルを利用する時及び定時にすべてのファイルをチェックするように設定すること。

エ　不正プログラム対策ソフトウェアのパターンファイルを常に最新の状態に保つこと。

オ　不正プログラム対策のソフトウェアを常に最新の状態に保つこと。

カ　不正プログラム対策のソフトウェアが常駐されていないか又は不正プログラム対策のソフトウェア及びそのパターンファイルが最新ではない端末の利用を停止すること。

キ　不正プログラムの検出状況について、CISO 補佐に報告すること。

(3) 職員等の遵守事項

職員等は、不正プログラム対策として、次の事項を遵守しなければならない。

ア　端末において、導入されている不正プログラム対策ソフトウェアの設定を変更しないこと。なお、新規導入端末に不正プログラム対策ソフトウェアがインストールされていない場合は、これをインストールすること。

イ　差出人が不明の電子メールに添付されたファイルや、差出人が分かっていても不自然に添付されたファイルは開封せずに、情報セキュリティ管理者又は電子メールシステムを管理する情報システム管理者の指示に従うこと。

ウ　CISO 補佐が提供する不正プログラム情報を、常に確認し、CISO 補佐から不正プログラムチェックの指示があった場合は、速やかにこれを実施すること。

エ　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処理等 CISO 補佐から指示のあった方法により処理しなければならない。

オ　県が管理していない記録媒体を利用する場合は、福島県情報通信ネットワークへの接続の有無にかかわらず、情報セキュリティ管理者又は所管の情報システム管理者の許可を得て、手動で不正プログラム対策ソフトウェアによるチェックを行ってから利用すること。

カ　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は、速やかに情報セキュリティ管理者及び CISO 補佐に報告すること。

(4) 専門家の支援体制

CISO 補佐は、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。

9　不正アクセス対策

(1) 情報システム管理者は、使用されていないポートを閉鎖しなければならない。

(2) 情報システム管理者は、不要なサービスについて、機能を削除又は停止しなければならない。

(3) 情報システム管理者は、所管するシステムについて、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、データの書換えを検出できるよう設定しなければならない。

(4) 情報システム管理者は、重要なシステムの設定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。

(5) CISO 補佐又は情報システム管理者は、サーバ等に攻撃を受ける可能性が高くなった場合、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、関係機関と連絡を密にして情報の収集に努めなければならない。

(6) CISO 補佐又は情報システム管理者は、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の下に対処しなければならない。

(7) CISO 補佐又は情報システム管理者は、職員等又は委託事業者が使用している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。

(8) CISO 補佐又は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、所管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。

(9) CISO 補佐又は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。

(10) CISO 補佐又は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　セキュリティ情報の収集

(1) 情報システム管理者は、不正プログラム、セキュリティホールに関する情報、ソフトウェアの更新等セキュリティに関する情報の収集に努め、所管する情報システムについて、緊急度に応じて、セキュリティ対策計画を作成し、これに基づいてセキュリティ対策上適正な措置を講じなければならない。

(2) CISO 補佐は、(1)の情報を定期的に取りまとめ、関係部局等に通知し、必要に応じ対応方法を職員等に周知するとともに、セキュリティポリシー等の改定につながる情報については、CISO に報告しなければならない。 情報システム管理者は、情報セキュリティに関する社会環境や技術環境の変化によって新たな脅威を発見した場合、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第８　運用におけるセキュリティ対策

１　情報システムの監視

(1) 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、常に所管する情報システムの監視を行わなければならない。

(2) 情報システム管理者は、記録の正確性を確保するため、サーバ等に関しては正確な時刻の設定を行わなければならない。

(3) 情報システム管理者は、外部と常時接続するサーバ等について、24 時間監視を行わなければならない。

(4) 情報システム管理者は、監視により得られた結果については、消去や改ざんをされないように必要な措置を講じ、安全な場所に保管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) 情報セキュリティ管理者は、情報セキュリティポリシーが遵守されているか常に確認を行い、問題が発生した場合には、速やかに CISO 補佐及び所管の情報システム管理者に報告しなければならない。

(2) 統括情報セキュリティ管理者は、CISO 補佐の指示に従い、発生した問題に適正かつ速やかに対処しなければならない。

(3) 情報セキュリティ管理者は、CISO 補佐又は所管の情報システム管理者の指示に従い、発生した問題に適正かつ速やかに対処しなければならない。

(4) 情報システム管理者は、所管する情報システムの設定及び構成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、問題を発見した場合には速やかに対処しなければならない。

(5) CISO 及び CISO 補佐は、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記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

第９　緊急時におけるセキュリティ対策

１　体制の整備

(1) 情報システム管理者は、情報セキュリティに関する事案、情報セキュリティポリシーの違反等により情報資産への侵害が発生した場合又は発生するおそれがある場合に備えて、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行うため、所管の情報システムに係る情報セキュリティ実施手順において緊急時対応計画を定め、緊急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事項

ウ　発生した事案への対応措置

エ　大規模障害時等において優先的に復旧させる必要がある業務とその対応方法

オ　大規模障害時等において可用性の確保のために緩和する必要がある制限とその対応方法

(3) 情報システム管理者は、緊急時対応計画を、CISO 補佐及び所管の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。

(4) 情報システム管理者は、可用性３の情報システムにあっては、自然災害等により情報システム、電源及びネットワークが被災した場合並びに情報システム担当者及び委託事業者が被災して、活動できない場合に備えて、所管の情報システムに係る業務継続計画を定めなければならない。

２　発生した事案に係る報告事項

情報セキュリティに関する事案を発見した者は、次の項目について、速やかに情報セキュリティ管理者及び、所管の情報システム管理者に報告しなければならない。この場合、情報システム管理者は、緊急時対応計画に定める連絡先に、速やかに連絡しなければならない。

(1) 情報資産への侵害状況

(2) 事案が発生した原因

３　発生した事案への対応措置

(1) 情報システム管理者は、次の情報セキュリティに関する事案が発生したときは、CSIRT 及び関係者の連絡先へ連絡しなければならない。

ア　サイバーテロその他県民に重大な被害を与えるおそれのあるとき

イ　不正アクセスその他犯罪があったと思われるとき

ウ　不正に操作されて他者に被害を与えるおそれがあるとき

(2) CSIRT 責任者は、次の場合、情報資産を保護するためにネットワークを遮断することができる。

ア　異常なアクセス又は不正アクセスが継続しているとき

イ　コンピュータウイルス等の不正プログラムがネットワーク経由で拡散しているとき

ウ　情報資産に係る重大な被害が想定されるとき

(3) 情報システム管理者は、次の場合、情報資産を保護するために情報システムを停止することができる。

ア　コンピュータウイルス等の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

イ　災害等により電源を供給することが困難なとき

ウ　情報資産に係る重大な被害が想定されるとき

(4) 情報システム管理者は、以下の手順に従い、速やかに緊急事案に対し対処しなければならない。

ア　事案に係るアクセス記録及び現状を保存する。

イ　事案への対処経過を記録する。

ウ　事案に係る証拠を保全し、暫定措置を検討する。

エ　暫定措置を講じた後、復旧する。

オ　復旧後、再発の監視を行う。

4　再発防止の措置

情報システム管理者は、情報資産の侵害に係る再発防止計画を策定し、CISO 補佐及び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。

5　業務継続計画との整合性確保

情報システム管理者は、自然災害、新型伝染病等の発生に備え、情報システムに係る業務継続計画を策定する場合、情報セキュリティポリシーとの整合性を確保しなければならない。

6　緊急時対応計画の見直し

(1) 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、行政組織の見直し等に応じ、緊急時対応計画を見直さなければならない。

(2) 情報システム管理者は、緊急時対応計画を見直した場合、CISO 補佐に報告しなければならない。

第10　業務委託と外部サービスの利用及び職員等以外による情報システムの利用

1　業務委託

(1) 委託先の選定基準

情報システム管理者又は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情報セキュリティが確保されることを確認の上、情報システムに係る委託先の事業者を選定しなければならない。

(2) 委託における契約項目

情報システムの運用、保守等を事業者に委託する場合は、必要に応じ、次の情報セキュリティ要件を明記した上で、事業者と契約を締結しなければならない。

ア　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
イ　委託先の責任者、委託内容、作業者の所属及び作業場所の特定
ウ　提供されるサービスレベルの保証
エ　従業員に対する教育の実施
オ　提供された情報の目的外利用及び受託者以外の者への提供の禁止
カ　業務上知り得た情報の守秘義務
キ　再委託に関する制限事項の遵守
ク　委託業務終了時の情報資産の返還、廃棄等
ケ　委託業務の定期報告及び緊急時報告義務
コ　県による監査又は検査
サ　県による事案の公表
シ　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)
ス　可用性２以上のシステムに係る災害時及び原子力発電所事故時の対応
セ　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
ソ　サービス拠点及びサービス拠点で使用する外部回線に係る災害時及び原子力発電所事故時のサービスレベル
タ　クラウドサービス基盤提供業者等の第三者が提供するサービス
チ　入力又は保存された情報は、クラウドサービス基盤提供業者等の第三者によって、どのように利用されるか
ツ　入力又は保存された情報は、削除することが可能か

(3) 委託における確認、措置等

① 情報システム管理者は、委託事業者が必要なセキュリティ対策を講じていることを定期的に確認し、必要に応じ、CISO 補佐に報告しなければならない。

② 情報システム管理者は、クラウドサービスを利用する場合は、サービスの内容及び入力又は保存された情報に係るクラウドサービス基盤提供業者等による利用状況を定期的に確認し、サービスの利用を継続するかどうか判断しなければならない。

2　外部サービスの利用（機密性２以上の情報を取り扱う場合）

(1) 約款による外部サービスを利用し、機密性２以上の情報資産を扱ってはならない。

(2) 外部サービスの選定

①　情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、次の判断基準に従って、外部サービスの利用を検討しなければならない。

ア　外部サービスを利用する目的の明確化
イ　外部サービスを利用する業務範囲の明確化
ウ　外部サービスを利用する際におけるリスク対策

(ｱ)　外部サービス提供者の運用詳細等が公開されない場合に、利用者が情報セキュリティ対策を行うことが困難となるリスク
(ｲ)　利用者が、利用する外部サービスを自組織のセキュリティポリシーに見合うサービスかどうか評価が適切に出来ない場合、セキュリティに対する影響が発生するリスク
(ｳ)　外部サービス提供者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムを一つの外部サービス基盤で共用することにより、情報が漏えいするリスク
(ｴ)　外部サービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスク
(ｵ)　サーバ装置等機器の整備環境が外部サービス提供者の都合で急変する場合、サプライチェーン・リスクへの対策が容易に確認できないリスク
エ　外部サービスで個人情報（特定個人情報を含む）を扱う場合は、個人情報保護法で定められた安全管理措置及び特定個人情報保護評価（PIA）の実施

②　情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、以下に示す事項について基本契約又はサービスレベル契約（SLA）で定めることが出来る外部サービス提供者を選定しなければならない。
ア　日本の裁判管轄、法令が適用される。海外への機密情報の流出リスクを考慮し、外部サービスを提供するリージョン（国・地域）を国内に指定する。国内の外部サービスにおいて、利用者のデータが、海外に保存されないこと。これらの事項を基本契約に定める
イ　外部サービスの中断時の復旧要件について基本契約又はサービスレベル契約（SLA）に定める
ウ　外部サービスの終了又は変更時における事前の通知等の取り決めや情報資産の移行方法について基本契約に定める
エ　稼動率、目標復旧時間、目標復旧ポイント、バックアップの保管方法などの可用性に関する事項をサービスレベル契約（SLA）に定める
オ　外部サービス提供者が、利用者の情報資産へ目的外のアクセスや利用を行わないように基本契約に定める
カ　外部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について、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）の内容を確認する
キ　外部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、利用者の意図しない変更が加えられないための管理体制について、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）の内容を確認する
ク　情報セキュリティインシデントへの対処方法について、外部サービス提供者との責任分担や連絡方法を取り決め、基本契約又はサービスレベル契約（SLA）に定める
ケ　脅威に対する外部サービス提供者の情報セキュリティ対策（なりすまし、情報漏えい、情報の改ざん、否認防止、権限昇格への対応、サービス拒否・停止等）の実施状況やその他契約の履行状況の確認方法を基本契約又はサービスレベル契約（SLA）に定める
コ　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について、基本契約又はサービスレベル契約（SLA）に定める
サ　外部サービス提供者により、利用規約、各種設定が変更される可能性があるため、変更内容の確認方法や連絡方法を基本契約又はサービスレベル契約（SLA）に定める

③　情報セキュリティ管理者は、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めなければならない。

ア　外部サービスの利用を通じて取り扱う情報の外部サービス提供者における目的外利用の禁止

イ　外部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　外部サービスの提供に当たり、外部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、意図しない変更が加えられないための管理体制

エ　外部サービス提供者の資本関係・役員等の情報、外部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

④　情報セキュリティ管理者は、外部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、外部サービス提供者の選定条件に含めなければならない。

⑤　情報セキュリティ管理者は、外部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外部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

⑥　情報セキュリティ管理者は、外部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外部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。

⑦　情報セキュリティ管理者は、外部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、外部サービス提供者の選定条件で求める内容を外部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、県の承認を受けるよう、外部サービス提供者の選定条件に含めなければならない。

⑧　情報セキュリティ管理者は、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、外部サービスを選定しなければならない。また、外部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。（ISO/IEC 27017（クラウドサービスに関する情報セキュリティ管理策のガイドライン規格。「情報マネジメントシステム認証センター」が取得組織を公開）や、ISMAP（政府情報システムのためのセキュリティ評価制度。「サービスリスト」（事業者一覧）を公開）の基準等を満たしていること。）

⑨　情報セキュリティ管理者は、外部サービスの特性を考慮した上で、外部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、セキュリティ要件を定めなければならない。

⑩　情報セキュリティ管理者は、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、外部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。

(3) 外部サービスの利用に係る調達・契約

① 情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部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。

② 情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めなければならない。

(4) 外部サービスの利用承認

① 情報セキュリティ管理者は、外部サービスを利用する場合には、情報セキュリティ管理者（総括担当）の許可を得なければならない。

② 情報セキュリティ管理者（総括担当）は、外部サービスの利用を許可した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名しなければならない。

(5) 外部サービスを利用した情報システムの導入・構築時の対策

① 情報セキュリティ管理者又は情報システム管理者は、外部サービスを利用して情報システムを構築する際に以下のセキュリティ対策を実施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

② 外部サービス管理者は、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。

(6) 外部サービスを利用した情報システムの運用・保守時の対策

① 情報セキュリティ管理者又は情報システム管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスを利用して情報システムを運用する際は以下のセキュリティ対策を実施しなければならない。

ア 外部サービス利用に必要な教育

イ 取り扱う資産の管理

ウ 不正アクセスを防止するためのアクセス制御

エ 取り扱う情報の機密性保護のための暗号化

オ 外部サービス内の通信の制御

カ 設計・設定時の誤りの防止

キ 外部サービスを利用した情報システムの事業継続

② 情報セキュリティ管理者又は情報システム管理者は、外部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。

③ 外部サービス管理者は、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。

(7) 外部サービスを利用した情報システムの更改・廃棄時の対策

① 情報セキュリティ管理者又は情報システム管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスの利用を終了する際に以下のセキュリティ対策を実施しなければならない。

ア 外部サービスで取り扱った情報の廃棄

イ 外部サービスの利用のために作成したアカウントの廃棄

② 外部サービス管理者は、前項において定める規定に対し、外部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　外部サービスの利用（機密性２以上の情報を取り扱わない場合）

(1) 外部サービスの利用における対策の実施

①　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、情報セキュリティ管理者の許可を得なければならない。

②　情報セキュリティ管理者は、外部サービスの利用を許可した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名しなければならない。

③　承認時に指名された外部サービス管理者は、当該外部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。

4　職員等以外による情報システムの利用

情報システム管理者又は情報セキュリティ管理者は、次の要件をすべて満たす場合、事前にCISO補佐の許可を得て職員等以外の者に情報システムを利用させることとする。

(1) 不正利用が発生しないように、アクセスを制御する機器の設置又は論理的な回線の分割などの技術的な情報セキュリティ対策が講じられ、目的外の情報資産へ接続できないこと。

(2) 利用者が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すること。

第11　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において、行政事務を継続する必要がある緊急事態においては、CISO 補佐の許可を得て、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、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに CISO 補佐に報告しなければならない。

3　例外措置の記録

CISO 補佐は、例外措置を記録して適正に保管し、定期的に状況を確認しなければならない。

第12　違反時の対応

1　違反時の措置

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は、速やかに次の措置を講じなければならない。

(1) CISO 補佐が違反を確認した場合は、当該職員等が所属する部局の統括情報セキュリティ管理者及び所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めること。

(2) 情報システム管理者が違反を確認した場合は、速やかに CISO 補佐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、適正な措置を求めること。

(3) CISO 補佐は、情報セキュリティポリシーに違反した職員等が再び違反した場合、ネットワークへの接続を停止し、又は情報システムを利用させないことができる。この場合、CISO 補佐は、当該職員等が所属する部局の統括情報セキュリティ管理者及び所属する課室等の情報セキュリティ管理者に通知すること。

2　懲戒処分等

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じ、懲戒処分等の対象とする。

第13　評価

1　監査

(1) 情報セキュリティ監査統括責任者は、ネットワーク及び情報システムの情報資産における情報セキュリティ対策の実施状況について、毎年度、監査実施計画を立案し、監査を実施しなければならない。

(2) 情報セキュリティ監査統括責任者は、監査実施計画を立案するに当たり、CISO 補佐が取りまとめた自己点検結果を参考にしなければならない。

(3) 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は、被監査部門から独立した者に、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。

(4) 被監査部門は、監査の実施に協力しなければならない。

(5) 情報セキュリティ監査統括責任者は、事業者に業務委託している場合、再委託事業者も含めて、情報セキュリティポリシーの遵守に係る監査を実施しなければならない。

(6) 情報セキュリティ監査統括責任者は、監査結果をとりまとめ、CISO に報告しなければならない。

(7) 情報セキュリティ監査統括責任者は、監査の実施により収集した証拠及び監査調書を、適正に保管しなければならない。

(8) CISO は、監査の結果、指摘事項があった場合、CISO 補佐及び指摘事項を所管する情報セキュリティ管理者又は情報システム管理者に対し、当該事項への対処を指示しなければならない。また、所管外の情報セキュリティ管理者及び情報システム管理者に対しても、同種の課題及び問題点の有無を確認させなければならない。

(9) CISO は、監査結果を情報セキュリティポリシー及びその他の情報セキュリティ対策の見直しに活用しなければならない。

2　自己点検

(1)CISO 補佐は、毎年度最低限必要な自己点検事項を定めなければならない。

(2) 情報システム管理者は、所管する情報システムについて、毎年度自己点検を実施しなければならない。

(3) 情報セキュリティ管理者は、所属等における情報セキュリティポリシーの実施状況について、毎年度自己点検を行わなければならない。

(4) 情報システム管理者及び情報セキュリティ管理者は、自己点検結果とそれに基づく改善策を取りまとめ、CISO 補佐に報告しなければならない。

(5) 職員等は、自己点検の結果に基づき、改善を図らなければならない。

(6) CISO 補佐は、点検結果を取りまとめ、CISO 及び情報セキュリティ監査統括責任者へ報告しなければならない。

(7)CISO は、自己点検の結果を情報セキュリティポリシー及びその他の情報セキュリティ対策の見直しに活用しなければならない。

第14　見直し

1　情報セキュリティポリシー

新たな対策が必要となった場合又は監査若しくは自己点検の結果必要がある場合は、福島県デジタル社会形成推進本部において情報セキュリティポリシーの実効性を評価し、適正な見直しを行う。

2　情報セキュリティ実施手順

情報システム管理者は、新たな対策が必要となった場合及び監査又は自己点検の結果必要がある場合並びに情報セキュリティポリシーの見直しが行われた場合、情報セキュリティ実施手順の見直しを行う。

第15　その他

この対策基準に定めるほか、情報セキュリティ対策に関して必要な事項は、CISO が別に定める。

附　則

この対策基準は、平成２５年１月１日から施行する。

附　則

この対策基準は、平成２６年４月２１日から施行する。

附　則

この対策基準は、平成２８年４月２５日から施行する。

附　則

この対策基準は、令和元年７月１１日から施行する。

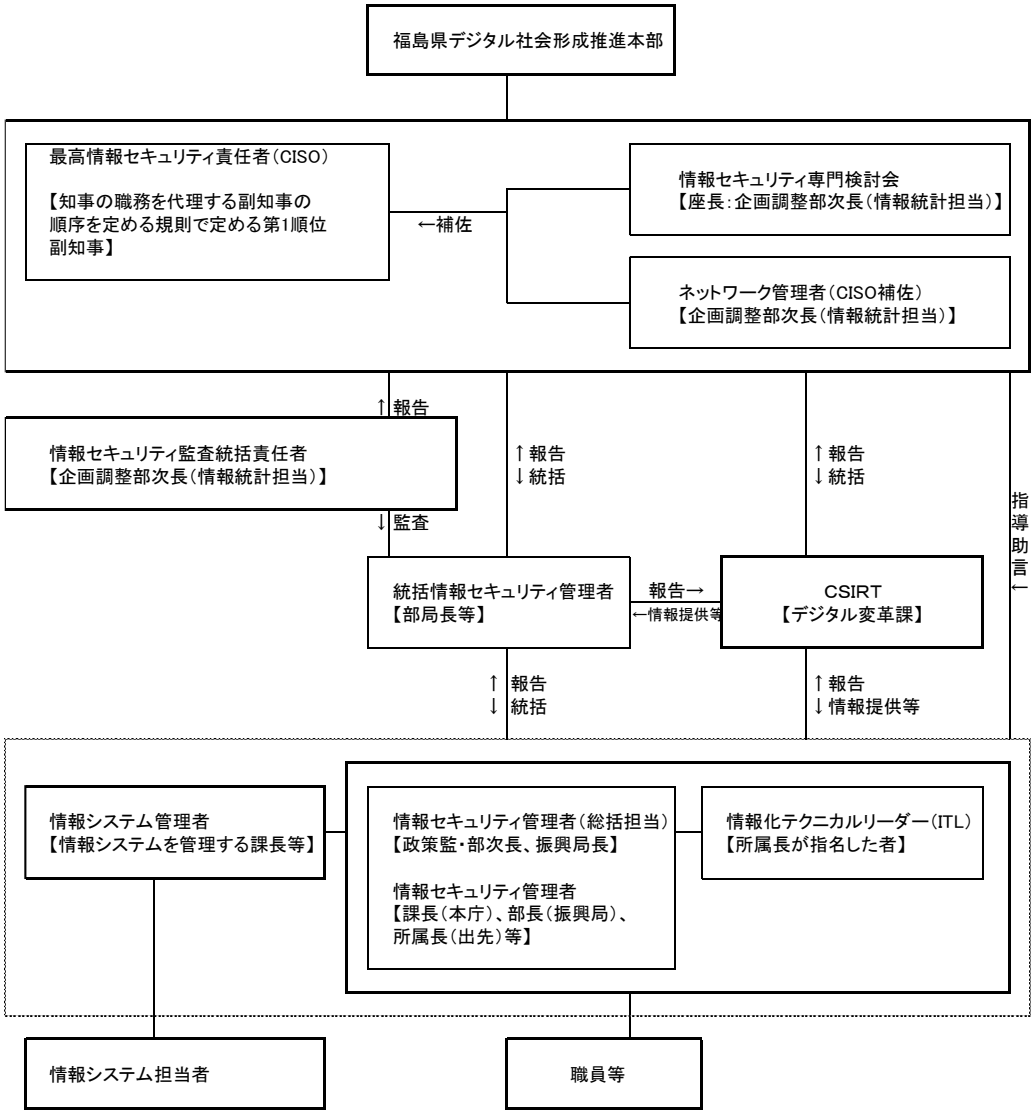
附　則

この対策基準は、令和３年４月１日から施行する。

附　則

この対策基準は、令和５年６月５日から施行する。

別紙1



別紙２

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	個人情報を含むもの又は秘密の取扱いを必要とするもの	・県が管理する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記録媒体の持ち込み禁止 ・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 ・記録媒体の施錠可能な場所への保管
機密性２	機密性３以外の情報資産のうち、直ちに一般に公表することを前提としていないもの	
機密性１	機密性２又は機密性３以外のもの	

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	改ざん、誤びゅう又は破損により、個人の権利が侵害され、又は行政事務の的確な遂行に支障（軽微なものを除く）を及ぼすおそれがあるもの	・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 ・記録媒体の施錠可能な場所への保管
完全性１	完全性２以外のもの（複写であることが明らかな文書を含めてもよい）	

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３	利用不能になった場合、県の経済に大きな損失を与え、又は行政事務全体に影響を与えるもの	・バックアップ、指定する時間以内の復旧 ・記録媒体の施錠可能な場所への保管
可用性２	可用性３以外の情報資産のうち、滅失、紛失又は利用不能により、個人の権利が侵害され、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もの	
可用性１	可用性２又は可用性３以外のもの（複写であることが明らかな文書を含めてもよい）	