奈良県
情報セキュリティ対策基準

令和２年４月改正

目次

１　目的

この基準は、「奈良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の具体的な基準を定め、県における情報セキュリティの統一的水準を確保するために必要な事項を定めることを目的とする。

２　適用範囲

（１）組織の範囲

本対策基準が適用される組織は、知事部局、教育委員会、水道局、議会事務局、人事委員会事務局、監査委員事務局、警察本部、労働委員会事務局、選挙管理委員会事務局、収用委員会事務局、及び内水面漁場管理委員会（以下「県」という。）とする。

なお、教育委員会及び警察本部については、知事部局が設置し、かつ管理運用する情報システムを利用する課、室及び出先機関（以下「課室等」という。）のみとする。

（２）情報資産の範囲

本対策基準が対象とする情報資産は、県が管理するもので、次のものをいう。

ア　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

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

３　組織体制

県の情報資産について、情報セキュリティ対策を推進するため、以下の組織を構成する。構成員は別表「情報セキュリティ管理体制」の通りとする。

（１）最高情報セキュリティ責任者

ア　設置

全ての情報資産の情報セキュリティ対策を統括するため、最高情報セキュリティ責

任者（CISO: Chief Information Security Officer）を置く。

イ　権限と責任

最高情報セキュリティ責任者は、県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。

（ア）最高情報セキュリティ責任者は、情報セキュリティインシデントを認知した場合は、その内容を確認し、情報セキュリティ部局責任者に初動対応、二次被害防止、原因調査及び再発防止対策等の実施について指示を行うこと。

（イ）最高情報セキュリティ責任者は、情報セキュリティインシデントを認知した場合は、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応の判断を行い、情報セキュリティ部局責任者へ対応を指示すること。

（ウ）最高情報セキュリティ責任者は、情報セキュリティインシデントに対処するための体制(CSIRT:Computer Security Incident Response Team 以下「CSIRT」という。）を整備し、役割を明確化する。

（２）統括情報セキュリティ責任者

ア　設置

最高情報セキュリティ責任者を補佐するため、直属の統括情報セキュリティ責任者を置く。

イ　権限と責任

統括情報セキュリティ責任者は次に掲げる事務を所掌し、権限及び責任を有する。

（ア）統括情報セキュリティ責任者は、県が管理する全てのネットワーク及び全庁共通基盤における開発、設定の変更、運用、見直し等を行うこと。

（イ）統括情報セキュリティ責任者は、県が管理する全てのネットワーク及び全庁共通基盤における情報セキュリティ対策を行うこと。

（ウ）統括情報セキュリティ責任者は、情報セキュリティ責任者、情報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こと。

（エ）統括情報セキュリティ責任者は、県の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、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こと。

（オ）統括情報セキュリティ責任者は、基本方針１０に規定する情報セキュリティ実施手順の維持・管理を行うこと。

（カ） 統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、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、情報セキュリティ部局責任者、情報セキュリティ責任者、情報システム管理者及び情報システム担当者を網羅する連絡体制を含めた緊急連絡体制を整備すること。

（キ） 統括情報セキュリティ責任者は、緊急時には、最高情報セキュリティ責任者に早急に報告を行うとともに、回復のための措置を講じること。

（３）情報セキュリティ部局責任者及び情報セキュリティ部局主任

ア　設置

各部局等に情報セキュリティ部局責任者及び情報セキュリティ部局主任をそれぞれ１名ずつ置く。

イ　権限と責任

情報セキュリティ部局責任者は次に掲げる事務を所掌し、権限及び責任を有する。

情報セキュリティ部局主任は、情報セキュリティ部局責任者の指示を受け、その事務を補助する。

（ア）所管する部局等の情報セキュリティ対策に関する事務を統括すること。

（イ）所管する部局等において所有している情報システムの情報セキュリティ対策に関する事務を統括すること。

（ウ）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職員及び地方公務員法における臨時的に任用される職員、その他の法律により任期を定めて任用される職員（以下「職員等」という。）に対する教育、訓練、助言及び指示を行うこと。

（エ）情報資産に対する情報セキュリティインシデントが発生した場合又は情報セキュリティインシデント発生のおそれがある場合、再発防止策を含む必要かつ十分な措置を行うこと。

（オ）部局内のセキュリティ対策の実施状況並びに情報セキュリティインシデント及び再発防止策について、統括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（３組織体制（９）に定める窓口をいう。）に報告すること。

（カ）情報セキュリティ部局責任者は、最高情報セキュリティ責任者の指示により、統括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と協力して、情報セキュリティインシデントに関する報道機関への通知・公表対応を行うこと。

（４）情報セキュリティ責任者及び情報セキュリティ主任

ア　設置

（ア）知事部局、教育委員会、水道局、議会事務局及び警察本部
課室等に情報セキュリティ責任者及び情報セキュリティ主任を置く。

（イ）人事委員会事務局、監査委員事務局、労働委員会事務局、選挙管理委員会事務局、収用委員会事務局及び内水面漁場管理委員会
事務局又は委員会に情報セキュリティ責任者及び情報セキュリティ主任を置く。

イ　権限と責任

情報セキュリティ責任者は次に掲げる事務を所掌し、権限及び責任を有する。情報セキュリティ主任は、情報セキュリティ責任者の指示を受け、その事務を補助する。

（ア）所管する課室等の情報資産の情報セキュリティ対策を実施すること。

（イ）所管する情報資産について、必要となる情報資産管理台帳を作成し、又は改正すること。

（ウ）情報セキュリティインシデントが発生した場合の連絡体制及び対応手順を定めること。

（エ）情報セキュリティ対策が適正かつ円滑に行われるよう、所属職員等に対し、情報セキュリティポリシー及び実施手順書等の研修及び周知を図ること。

（オ）所管する情報資産に対するインシデントが発生した場合又はインシデント発生のおそれがある場合は、速やかに情報セキュリティ部局責任者に報告し、その指示を受けると共に、必要かつ十分な措置をとること。

（５）情報システム管理者

ア　設置

情報システムごとに情報システム管理者を置く。

イ　権限と責任

情報システム管理者は次に掲げる事務を所掌し、権限及び責任を有する。

（ア）所管する情報システムにおける開発、設定の変更、運用、見直し及び情報セキュリティ対策を実施すること。

（イ）所管する情報システムに係る情報資産管理台帳又は事務マニュアル等を作成し、又は改正すること。

（ウ）所管する情報システムに係る情報セキュリティ事故が発生した場合の連絡体制及び対応手順を定めること。

（エ）所管する情報システムに係る情報セキュリティ対策が適正かつ円滑に行われ

るよう、システム利用者に対し、実施手順書等の研修及び周知を図ること。

（オ）所管する情報システムに対する事故が発生した場合又は事故発生のおそれがある場合は、速やかに情報セキュリティ部局責任者に報告し、その指示を受けると共に、必要かつ十分な措置をとること。

（６）情報システム担当者

ア　設置

情報システムごとに情報システム担当者を置く。

イ　役割

情報システム担当者は、情報システム管理者の指示を受け、その事務を補助する。

（７）情報セキュリティ委員会

情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

（８）兼務の禁止

ア　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務しないこと。

イ　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、同じ者が兼務しないこと。

（９）CSIRT の設置・役割

ア　最高情報セキュリティ責任者は、CSIRT を整備し、その役割を明確化すること。

イ　最高情報セキュリティ責任者は、CSIRT に所属する職員を選任し、その中から CSIRT 責任者を置くこと。また、CSIRT 内の業務統括及び外部との連絡等を行う職員を定めること。

ウ　最高情報セキュリティ責任者は、情報セキュリティインシデントに関する事故の統一的な窓口の機能を有する組織（以下「情報セキュリティに関する統一的な窓口」という。）を整備し、情報セキュリティインシデントに関する事故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。

エ　CSIRT の運用管理に関し必要な事項は別に定める。

４　情報資産の分類と管理

（１）情報資産の分類

情報セキュリティ責任者は、次のアからウに掲げる情報分類に従い、課室等が保有する情報資産を分類し、管理するよう努めること。

ア　情報分類Ⅰ

奈良県情報公開条例（平成１３年３月奈良県条例第３８号）第７条各号の情報に該当する情報資産

イ　情報分類Ⅱ

アに該当しない情報のうち、当該情報が脅威にさらされた場合に、事務又は事業の公正かつ能率的な遂行に著しい支障を与える情報を取り扱う情報資産

ウ　情報分類Ⅲ

ア又はイに該当しない情報のみを取り扱う情報資産

（２）情報資産の管理

ア　管理責任

（ア）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すること。

イ　情報資産の分類の表示

情報セキュリティ責任者は、情報分類Ⅰ及び情報分類Ⅱの情報資産について、情報資産管理台帳を整備することにより情報分類を明示し、職員等が必要に応じた適正な管理を行えるようにすること。

ウ　情報の作成

（ア）　職員等は、業務上必要のない情報を作成しないこと。

（イ）　情報を作成する者は、情報の作成時に（１）に掲げる情報分類に基づき、当該情報の情報分類を定め、取り扱うこと。

（ウ）　情報を作成する者は、作成途上の情報についても、紛失、流出等を防止するこ

と。また、情報の作成途上で不要になった場合は、当該情報を消去すること。

エ　情報資産の入手

（ア）職員等が庁内で作成された情報資産を入手した場合は、入手元の情報分類に基づき取り扱うこと。

（イ）職員等が庁外で作成された情報資産を入手した場合は、（1）に掲げる情報分類に基づき、当該情報の情報分類を定め、取り扱うこと。

（ウ）職員等は、入手した情報の情報分類が不明な場合、情報セキュリティ責任者に判断を仰ぐこと。

オ　情報資産の利用

（ア）情報資産を利用する者は、業務以外の目的に当該情報資産を利用しないこと。

（イ）情報資産を利用する者は、情報分類に応じ、適正な取扱いを行うこと。

（ウ）情報資産を利用する者は、その情報資産に含まれる情報が複数の情報分類に該当する場合、最高度の情報分類に従って、当該情報資産を取り扱うこと。

カ　情報資産の保管

（ア）情報セキュリティ責任者又は情報システム管理者は、情報分類に従って、情報資産を適切に保管すること。

（イ）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ること。

（ウ）情報セキュリティ責任者又は情報システム管理者は、情報分類Ⅰ及び情報分類Ⅱの情報を記録した電磁的記録媒体を保管する場合、施錠可能な場所に保管すること。

キ　情報の送信

電子メール等により情報分類Ⅰ及び情報分類Ⅱに該当する情報を外部へ送信する者は、暗号化及びパスワード設定を行うこと。

ク　情報資産の運搬

（ア）情報分類Ⅰ及び情報分類Ⅱに該当する情報資産を運搬する者は、暗号化又はパスワードの設定を行うとともに、必要に応じて鍵付きのケース等に格納する等、情報資産の不正利用を防止するための措置を講じること。

（イ）情報分類Ⅰ及び情報分類Ⅱに該当する情報資産を運搬する者は、情報セキュリティ責任者の許可を得ること。

ケ　情報資産の提供・公表

（ア）　情報分類Ⅰ及び情報分類Ⅱに該当する情報資産を外部に提供する者は、暗号化又はパスワードの設定を行うこと。

（イ）　情報分類Ⅰ及び情報分類Ⅱに該当する情報資産を外部に提供する者は、情報セキュリティ責任者の許可を得ること。

（ウ）　情報セキュリティ責任者は、住民に公開する情報資産について、完全性を確保すること。

コ　情報資産の廃棄

（ア）　情報分類Ⅰ及び情報分類Ⅱに該当する情報資産を廃棄する者は、記録媒体の破壊、磁気処理による消去等、情報を復元できないように処置した上で廃棄すること。

（イ）　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しておくこと。

（ウ）　（イ）の情報資産の廃棄を行う者は、情報セキュリティ責任者の許可を得ること。

５　情報システム全体の強靭性の向上

（１）番号ネット系

ア　番号ネット系と他の領域との分離

番号ネット系と他の領域を通信できないようにしなければならない。ただし、番号ネット系と外部との通信をする必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。なお、外部接続先もインターネット等と接続してはならない。

イ　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

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

（２）行政ネット系

ア　行政ネット系とインターネット系の分割

行政ネット系とインターネット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、メールやデータを行政ネット系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

（ア） インターネット環境で受信したインターネットメールの本文のみを行政ネット系に転送する方式

（イ） インターネット系仮想端末から、行政ネット系の端末へ画面を転送する方式

（３）インターネット系

ア　インターネット系においては、通信パケットの監視、ふるまい検知など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行わなければならない。

イ　県及び市区町村のインターネット接続口を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や関係機関等と連携しながら、情報セキュリティ対策を推進しなければならない。

６　物理的セキュリティ

（１）サーバ等の管理

ア　機器の取付け

情報システム管理者は、サーバ、セキュリティサーバ及びその他の基幹サーバ（以下「サーバ等」という。）等の機器の取付けを行う場合、火災、水害、埃、振

動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じること。

イ　サーバ等の冗長化

情報システム管理者は、情報分類Ⅰの情報を格納しているサーバ等を冗長化し、同一データを保持すること。

ウ　機器の電源

（ア）情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、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備え付けること。

（イ）情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じること。

エ　通信ケーブル等の配線

（ア）統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じること。

（イ）統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応すること。

（ウ）統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）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すること。

（エ）統括情報セキュリティ責任者及び情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

オ　機器の定期保守及び修理

（ア）情報システム管理者は、可用性確保のため情報分類Ⅰ及び情報分類Ⅱのサーバ等の機器の定期保守を実施すること。

（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ること。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行うこと。

カ　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、統括情報セキュリティ責任者の承認を得ること。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すること。

キ　機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じること。

（２）管理区域（電子計算機室等）の管理

ア　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「電子計算機室」という。）や電磁的記録媒体の保管庫をいう。

（イ）統括情報セキュリティ責任者は、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。

（ウ）統括情報セキュリティ責任者は、電子計算機室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じること。

（エ）統括情報セキュリティ責任者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにすること。

イ　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うこと。

（イ）職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示すること。

（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ること。

（エ）情報システム管理者は、情報分類Ⅰ及び情報分類Ⅱの情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、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すること。

ウ　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、あらかじめ職員又は委託した業者に確認を行わせること。

（イ）情報システム管理者は、電子計算機室の機器等の搬入出について、職員を立ち会わせること。

（３）通信回線及び通信回線装置の管理

ア　統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適切に管理すること。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すること。

イ　統括情報セキュリティ責任者は、 外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らすこと。

ウ　統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めること。

エ　統括情報セキュリティ責任者は、情報分類Ⅰ及び情報分類Ⅱ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、適正な回線を選択すること。また、必要に応じ、送受信される情報の暗号化を行うこと。

オ　統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施すること。

カ　統括情報セキュリティ責任者は、情報分類Ⅰ及び情報分類Ⅱ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、可用性の観点から継続的な運用を可能とする回線を選択すること。また、必要に応じ、回線を冗長構成にする等の措置を講じること。

（４）職員等のパソコン及びモバイル端末の管理

ア　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ること。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すること。

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、スマートカード、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すること。

ウ　情報システム管理者は、マイナンバー系では「知識」、「所持」、「存在」を利用する認証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、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、端末の電磁的記録媒体に情報が記録されない等の措置を講じること。

７　人的セキュリティ

（１）職員等の遵守事項

ア　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すること。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ責任者に相談し、指示を仰ぐこと。

（イ）業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、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わないこと。

（ウ）職員等遵守規定の遵守

職員等は、次の事項に関して別に定める職員等遵守規定を遵守すること。

a　パソコンやモバイル端末の持出し及び外部における情報処理作業の制限

b　私物パソコン等の持込み

c　持出し及び持込みの記録

d　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

e　机上の端末等の管理

f　退職時の遵守事項

イ　非常勤及び臨時職員への対応

（ア）情報セキュリティポリシー等の遵守

情報セキュリティ責任者は、非常勤及び臨時職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員が守るべき内容を理解させ、また実施及び遵守させること。

（イ）情報セキュリティポリシー等の遵守に対する同意

最高情報セキュリティ責任者は、非常勤及び臨時職員の採用の際、統括情報セキュリティ責任者と協力し、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めること。

（ウ）インターネット接続及び電子メール使用等の制限

情報セキュリティ責任者は、非常勤及び臨時職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにすること。

ウ　情報セキュリティポリシー等の掲示

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すること。

エ　外部委託事業者に対する説明

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・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明すること。

（２）研修・訓練

ア　情報セキュリティ研修・訓練

最高情報セキュリティ責任者 は、定期的に情報セキュリティ研修・訓練を実施すること。

イ　研修計画の策定及び実施

（ア）最高情報セキュリティ責任者 は、幹部を含め全ての職員等に対する情報セキュリティ研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得ること。

（イ）研修計画において、職員等は毎年度最低１回は情報セキュリティ研修を受講できるようにすること。

（ウ）新規採用の職員等を対象とする情報セキュリティ研修を実施すること。

（エ）研修は、統括情報セキュリティ責任者、情報セキュリティ部局責任者、情報セキュリティ責任者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにすること。

（オ）情報システム管理者は、情報システムの利用を許可する前に、情報システムの利用に関する操作手順のほか、情報セキュリティに関する注意点を含めた研修を実施すること。

（カ）最高情報セキュリティ責任者は、毎年度１回、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告すること。

ウ　緊急時対応訓練

最高情報セキュリティ責任者 は、緊急時対応を想定した訓練を定期的に実施すること。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すること。

エ　研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加すること。

（３）情報セキュリティインシデントの報告

ア　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すること。

（イ）報告を受けた情報セキュリティ責任者は、速やかに統括情報セキュリティ責任者及び情報システム管理者へ連絡し、情報セキュリティ部局責任者に報告すること。

（ウ）報告を受けた情報セキュリティ部局責任者は、速やかに統括情報セキュリティ責任者及び情報セキュリティに関する統一的な窓口に報告すること。

イ　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、県が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ責任者に報告すること。

（イ）報告を受けた情報セキュリティ責任者は、速やかに情報システム管理者へ連絡し、情報セキュリティ部局責任者に報告すること。

（ウ）報告を受けた情報セキュリティ部局責任者は、必要に応じて速やかに統括情報セキュリティ責任者及び情報セキュリティに関する統一的な窓口に報告すること。

（４）ＩＤ及びパスワードの管理

職員等は、ＩＤ、パスワード等に関するセキュリティ対策に関して、別に定める職員等遵守規定を遵守すること。

８　技術的セキュリティ

（１）コンピュータ及びネットワークの管理

ア　ファイルサーバの設定等

（ア）統括情報セキュリティ責任者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知すること。

（イ）統括情報セキュリティ責任者は、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、設定すること。

（ウ）統括情報セキュリティ責任者は、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すること。

イ　バックアップの実施

情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施すること。

ウ　他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、情報セキュリティ部局責任者の許可を得た上で、統括情報セキュリティ責任者に報告すること。

エ　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、作業記録を作成すること。

（イ）情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理すること。

（ウ）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外部委託事業者がシステム変更等の作業を行う場合は、2名以上で作業し、互いにその作業を確認すること。

オ　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について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理すること。

カ　ログの取得等

（ア）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、一定の期間保存すること。

（イ）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、適正にログを管理すること。

（ウ）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すること。

キ　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、適正に保存すること。

ク　ネットワークの接続制御、経路制御等

（ア）統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、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すること。

（イ）統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施すこと。

ケ　外部の者が利用できるシステムの分離等

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、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ること。

コ　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外部ネットワークと接続しようとする場合には、統括情報セキュリティ責任者の許可を得ること。

（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すること。

（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すること。

（エ）統括情報セキュリティ責任者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続すること。

（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、速やかに当該外部ネットワークを物理的に遮断し、情報セキュリティ部局責任者に報告すること。また、情報セキュリティ部局責任者は当該外部ネットワークを遮断したことを統括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すること。

サ　複合機のセキュリティ管理

（ア）情報システム管理者は、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すること。

（イ）情報システム管理者は、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ること。

（ウ）情報システム管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じること。

シ　特定用途機器*のセキュリティ管理

（ア）情報システム管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（*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）

ス　無線 LAN 及びネットワークの盗聴対策

（ア）無線 LAN の利用は原則として禁止する。

（イ）統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けること。

（ウ）統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じること。

セ　電子メールのセキュリティ管理

（ア）統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行うこと。

（イ）統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止すること。

（ウ）統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にすること。

（エ）統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知すること。

（オ）統括情報セキュリティ責任者は、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外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めること。

ソ　電子署名・暗号化

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、電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

タ　無許可ソフトウェアの禁止

（ア）職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

（イ）職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ責任者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

（ウ）職員等は、不正にコピーしたソフトウェアを利用してはならない。

チ　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、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

ツ　無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

テ　業務以外の目的でのウェブ閲覧の禁止

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

（２）アクセス制御

ア　アクセス制御

（ア）アクセス制御等

情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限すること。

（イ）利用者 ID の取扱い

a　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ること。

b　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。

c　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、点検すること。

（ウ）特権を付与された ID の管理等

a　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すること。

b　情報システム管理者の特権を代行する者は、情報システム管理者が指名し、情報セキュリティ部局責任者に報告すること。

c　情報セキュリティ部局責任者は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システム管理者に通知すること。

d　情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせないこと。

e　情報システム管理者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化すること。

f　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すること。

イ　職員等による外部からのアクセス等の制限

（ア）職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者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ること。

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

（ウ）統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保すること。

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

（オ）統括情報セキュリティ責任者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じること。

（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すること。

（キ）統括情報セキュリティ責任者は、公衆通信回線（公衆無線 LAN 等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止すること。ただし、やむを得ず接続を許可する場合は、利用者の ID 及びパスワード、生体認証に係る情報等の認証情報及び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ること。

ウ　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すること。

エ　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すること。パスワード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パスワード設定のセキュリティ強化機能がある場合は、これを有効に活用すること。

（イ）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ること。

（ウ）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。

オ　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すること。

（３）システム開発、導入、保守等

ア　情報システムの調達

（ア）情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記すること。

（イ）情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認すること。

イ　情報システムの開発

（ア）システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定すること。また、システム開発のための規則を確立すること。

（イ）システム開発における責任者、作業者のＩＤの管理

a　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を削除すること。

b　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すること。

（ウ）システム開発に用いるハードウェア及びソフトウェアの管理

a　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すること。

b　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すること。

ウ　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

a　情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離すること。

b　情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にすること。

c　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すること。

d　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すること。

（イ）テスト

a　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うこと。

b　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うこと。

c　情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用しないこと。

d　情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行うこと。

エ　システム開発・保守に関連する資料等の整備・保管

（ア）情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管すること。

（イ）情報システム管理者は、テスト結果を一定期間保管すること。

（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すること。

オ　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すること。

（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る又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計すること。

（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すること。

カ　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すること。

キ　開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認すること。

ク　システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行うこと。

（４）不正プログラム対策

ア　統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置すること。

（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、不正プログラムのシステムへの侵入を防止すること。

（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）所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させること。

（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は、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は、常に最新の状態に保つこと。

（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ないこと。

イ　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、次の事項を措置すること。

（ア）情報システム管理者は、その所掌するサーバ、パソコン及びモバイル端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させること。

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

（ウ）不正プログラム対策のソフトウェアは、常に最新の状態に保つこと。

（エ）インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、県が管理している媒体以外を職員等に利用させないこと。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施すること。

ウ　職員等の遵守事項

職員等は、不正プログラム対策に関する次の事項に関して、別に定める職員等遵守規定を遵守すること。

（ア）パソコンやモバイル端末における不正プログラム対策ソフトウェアの取扱い

（イ）外部とのデータ又はソフトウェアの送受信に伴う措置

（ウ）差出人が不明な場合の添付ファイルの削除

（エ）不正プログラム対策ソフトウェアによる定期的チェックの実施

（オ）添付ファイルの付いた電子メールを送受信する場合のチェックの実施

（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の確認

（キ）コンピュータウイルス等の不正プログラム感染時の対応

エ　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くこと。

（５）不正アクセス対策

ア　統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置すること。

（ア）使用されていないポートを閉鎖すること。

（イ）不要なサービスについて、機能を削除又は停止すること。

（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、情報システム管理者へ通報するよう、設定すること。

（エ）統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築すること。

イ　攻撃への対処

最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合、システムの停止を含む必要な措置を講じること。また、総務省等と連絡を密にして情報の収集に努めること。

ウ　記録の保存

最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めること。

エ　内部からの攻撃

情報システム管理者は、職員等及び外部委託事業者が使用しているパソコンやモバイル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すること。

オ　職員等による不正アクセス

情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ責任者に通知し、適切な処置を求めること。

カ　サービス不能攻撃

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ること。

キ　標的型攻撃

統括情報セキュリティ責任者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じること。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じること。

（６）セキュリティ情報の収集

ア　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有すること。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施すること。

イ　不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知すること。

ウ　情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有すること。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じること。

９　運用

（１）情報システムの監視

ア　統括情報セキュリティ責任者及び情報システム管理者は、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すること。

イ　統括情報セキュリティ責任者及び情報システム管理者は、重要な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ること。

ウ　統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視すること。

（２）情報セキュリティポリシーの遵守状況の確認

ア　遵守状況の確認及び対処

（ア）情報セキュリティ部局責任者及び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及び統括情報セキュリティ責任者に報告すること。

（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すること。

（ウ）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すること。

イ　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

統括情報セキュリティ責任者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

ウ　職員等の報告義務

（ア）職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ責任者に報告を行うこと。

（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情報セキュリティ責任者が判断した場合は、事故対応手順に従って適切に対処すること。

（３）侵害時の対応等

ア　事故対応手順の策定

最高情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、事故対応手順を定めておき、セキュリティ侵害時には当該計画に従って適正に対処すること。

イ　事故対応手順に盛り込むべき内容

事故対応手順には、以下の内容を定めること。

（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

ウ　業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保すること。

エ　事故対応手順の見直し

最高情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて事故対応手順の規定を見直すこと。

（４）例外措置

ア　例外措置の許可

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定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、情報セキュリティ部局責任者の許可を得て、例外措置を講じることができる。

イ　緊急時の例外措置

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、事後速やかに情報セキュリティ部局責任者に報告すること。

ウ　例外措置の申請書の管理

情報セキュリティ部局責任者は、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すること。

エ　例外措置の報告

情報セキュリティ部局責任者は、上記例外措置を許可した場合又は緊急時の例外措置の報告を受けた場合は、事後速やかに最高情報セキュリティ責任者に報告すること。

（５）法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従うこと。

ア　地方公務員法(昭和二十五年十二月十三日法律第二百六十一号)

イ　著作権法（昭和四十五年法律第四十八号)

ウ　不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号)

エ　個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号)

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（平成二十五年法律第二十七号)

カ　サイバーセキュリティ基本法（平成２８年法律第３１号)

キ　奈良県個人情報保護条例（平成十二年三月三十日条例第三十二号)

（６）懲戒処分等

ア　懲戒処分

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

イ　違反時の対応

（ア）統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ責任者に通知し、適正な措置を求めること。

（イ）情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに当該職員等が所属する課室等の情報セキュリティ責任者に通知し、適正な措置を求めること。

（ウ）情報セキュリティ責任者が違反を確認した場合、又は統括情報セキュリティ責任者及び情報システム管理者等から違反があった旨の連絡を受けた場合は、速やかに統括情報セキュリティ責任者及び当該職員に通知し、適正な措置を求めること。

（エ）情報セキュリティ責任者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を最高情報セキュリティ責任者 及び当該職員等が所属する課室等の情報セキュリティ責任者に通知すること。

１０　外部サービスの利用

（１）外部委託

ア　外部委託事業者の選定基準

（ア）情報セキュリティ責任者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認すること。

（イ）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は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用すること。

イ　契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結すること。

・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

・外部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

・外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法

・外部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受託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)

・奈良県個人情報保護条例第１０条第１項に規定する個人情報の保護のために必要な措置

ウ　確認・措置等

情報セキュリティ責任者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、イの契約に基づき措置を実施すること。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて最高情報セキュリティ責任者に報告すること。

（２）約款による外部サービスの利用

ア　約款による外部サービスの利用に係る規定の整備

情報セキュリティ責任者は、以下を含む約款による外部サービスの利用に関する規定を整備すること。また、当該サービスの利用において、情報分類Ⅰ及び情報分類Ⅱの情報が取扱われる場合は当該情報が漏えいしないための措置の実施を規定すること。

（ア）約款によるサービスを利用して良い範囲

（イ）業務により利用する約款による外部サービス

（ウ）利用手続及び運用手順

イ　約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適正な措置を講じた上で利用すること。

（３）ソーシャルメディアサービスの利用

ア　情報セキュリティ責任者は、県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ること。

（ア）県のアカウントによる情報発信が、実際の県のものであることを明らかにするために、県の自己管理ウェブサイトに当該情報を掲載して参照可能とする

とともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

（イ）パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ICカード等）等を適切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　情報分類Ⅰ及び情報分類Ⅱの情報はソーシャルメディアサービスで発信しないこと。

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ること。

１１　評価・見直し

（１）監査

ア　実施方法

最高情報セキュリティ責任者は、情報セキュリティ監査実施要領において定める情報セキュリティ監査統括責任者に、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、計画的に及び必要に応じて下記の内容を定めて監査を行わせること。

イ　監査要件

（ア）監査を行う者の要件

（イ）監査実施計画の立案及び実施への協力

（ウ）外部委託事業者に対する監査

（エ）報告

（オ）保管

ウ　監査結果への対応

最高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情報セキュリティ責任者に対し、当該事項への対処を指示すること。また、指摘事項を所

管していない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ること。

エ　情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用すること。

（２）自己点検

ア　実施方法

（ア）情報セキュリティ部局責任者は、情報システム管理者と連携して、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施すること。

（イ）情報セキュリティ部局責任者は、情報セキュリティ責任者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行うこと。

イ　報告

情報セキュリティ部局責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告すること。

ウ　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ること。

（イ）情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用すること。

（３）情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うこと。

附則

この対策基準は平成１５年４月１日より施行する。

附則

この対策基準は平成２３年４月１日より施行する。

附則

この対策基準は平成２７年１０月５日より施行する。

附則

この対策基準は平成２９年４月１日より施行する。

附則

この対策基準は平成３１年４月１日より施行する。

附則

この対策基準は令和２年４月　日より施行する。