サイバーセキュリティを確保するための基本方針

令和８年３月31日　策　定

香　川　県

1　目的

本基本方針は、県が保有する情報資産の機密性、完全性及び可用性を維持するため、県が実施する情報セキュリティ対策について、基本的な事項を定めることを目的とする。

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及びその構成機器（ハードウェア及びソフトウェア）をいう。

(2)　情報システム

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

本基本方針及び情報セキュリティ対策基準をいう。

(5)　機密性

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

(6)　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7)　可用性

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

(8)　情報セキュリティインシデント

情報セキュリティに対する脅威として、実際に発生した事案をいう。

(9)　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）に関わる情報を扱うネットワーク環境をいう。

(10)　ＬGWAN接続系

ＬGWANに接続されたネットワーク環境をいう。

(11)　インターネット接続系

インターネットに接続されたネットワーク環境をいう。

(12)　通信経路の分割

ＬGWAN接続系とインターネット接続系の両ネットワーク環境間の通信経路を分離した上で、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。

(13)　無害化通信

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

3　対象とする脅威

情報セキュリティに対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

ア　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図

的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

イ　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規程違反、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

ウ　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

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

オ　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

4　適用範囲

(1)　行政機関の範囲

本基本方針が適用される行政機関は、知事部局（県立大学における学術分野に関する情報システムを除く。）、議会事務局、教育委員会（教育分野に関する情報システムを除く。）、公安委員会（警察本部の所管する情報システムを除く。）、選挙管理委員会、監査委員、人事委員会、労働委員会、収用委員会、海区漁業調整委員会、内水面漁場管理委員会及び病院局（医療分野に関する情報システムを除く。）とする。

(2)　情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

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　アで取り扱う情報（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情報システム関連文書

5　職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6　情報セキュリティ対策

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

(1)　組織体制

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全庁的な組織体制を確立する。

(2)　情報資産の分類と管理

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

(3)　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

ア　マイナンバー利用事務系においては、原則として、他のネットワーク環境との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、情報の漏えいを防ぐ。

イ　ＬGWAN接続系においては、ＬGWANと接続する業務用システムとインターネット接続系との間で通信経路の分割を行い、両接続系の間で通信する場合には、無害化通信を実施する。

ウ　インターネット接続系においては、県と市町のインターネットとの通信を集約した自治体情

報セキュリティクラウドで、高度な情報セキュリティ対策を講じる。

(4) 物理的セキュリティ

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

(5) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7) 運用

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

(8) 業務委託と外部サービス（クラウドサービス）の利用

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

外部サービスを利用する場合には、利用に係る規程を整備し対策を講じる。

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

7 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、毎年度及び必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。

8 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果や、情報セキュリティに関する状況の変化を踏まえ、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーの必要な見直しを行う。

9 情報セキュリティ対策基準の策定

上記 6、7 及び 8 に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10 情報セキュリティ実施手順の策定

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

なお、情報セキュリティ実施手順は、公にすることにより県の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。