宮崎県情報セキュリティ基本方針

1　目的

本基本方針は、本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、本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、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) 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

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（マイナンバー利用事務系を除く。）。

(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ない等、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、ウィルス攻撃、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

(2) 情報資産の無断持ち出しや紛失、無許可ソフトウェ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、外部委託管理の不備、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、火災等の災害並びに事故、故障等によるサービス及び業務の停止
(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

(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、企業局、病院局、教育庁、警察本部、議会事務局、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会、海区漁業調整委員会及び内水面漁場管理委員会とする。

ただし、病院局の県立病院、教育庁の県立学校及び警察本部については、知事部局が管理運用する情報システムを利用する部署のみとする。

(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　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　ネットワーク及び情報システムの開発と運用に係る全ての情報

ただし、病院局の県立病院、教育庁の県立学校及び警察本部については、知事部局が管理運用する情報システムの利用にかかる情報資産のみとする。

5　職員等の遵守義務

職員、委員、非常勤職員、会計年度任用職員及び臨時的任用職員（以下「職員等」という。）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で示した脅威から情報資産を保護するために、次のとおりの情報セキュリティ対策を講じる。

(1) 組織体制

本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組織体制を確立する。

(2) 情報資産の分類と管理

本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た重要性で分類し、当該分類に基づき情報セキュリティ対策を行う。

(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、次の三段階の対策を講じる。

ア　マイナンバー利用事務系においては、原則として他の領域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個人情報等の流出を防ぐ。

イ　LGWAN接続系においては、LGWANと接続する業務用情報システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム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、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として本県及び市町村の

インターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(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パソコン等の管理について、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する職員等の責務の明確化、研修の実施及び外部委託の適正な管理など、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

ネットワーク等の監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保など、運用面の対策を講ずる。また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講じる。

(8) 業務委託と外部サービス（クラウドサービス）の利用

情報システムの開発及び運用を業務委託する場合には、情報セキュリティ要件を明記した契約を締結し、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（クラウドサービス）を利用する場合には、利用に係る規定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、定期的又は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する。

8　情報セキュリティポリシーの評価及び見直し

情報セキュリティ監査及び自己点検の結果により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。

9　情報セキュリティ対策基準の策定

上記６、７、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策定するものとする。なお、情報セキュリティ実施手順のうち、公にすることにより本県の行政運営に重大な支障を及ぼすおそれがあるものについては非公開とする。

附　則

この基本方針は、平成１５年３月２９日から施行する。

附　則

この基本方針は、平成１７年４月１日から施行する。

附　則

この基本方針は、平成１８年４月１日から施行する。

附　則

この基本方針は、平成２４年９月１日から施行する。

附　則

この基本方針は、平成２９年７月１日から施行する。

附　則

この基本方針は、令和３年１２月１日から施行する。

附　則

この基本方針は、令和７年４月１日から施行する。

附　則

この基本方針は、令和８年４月１日から施行する。