沖縄県情報セキュリティ基本方針

（目的）

第１条　沖縄県情報セキュリティ基本方針（以下「基本方針」という。）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。

（用語の定義）

第２条　この基本方針において、次に掲げる用語の定義は、当該各号に定めるとおりとする。

（１）情報資産　県の保有するネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体並びに、電子データ（印刷した文書を含む。）、システム関連文書のことをいう。

（２） ネットワーク　コンピュータ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。

（３） 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。

（４）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。

（５） 情報セキュリティポリシー　本基本方針及び沖縄県情報セキュリティ対策基準をいう。

（６）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。

（７）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。

（８） 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。

（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）に関わる情報システム及びデータをいう。

(10) 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。）。

(11) 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。

(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。

(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。

（適用範囲）

第３条　この基本方針は、県が保有する情報資産の生成、運用、管理及び利用に携わる以下の者（以下「職員等」という。）に適用する。

（１）地方公務員法第 3 条（昭和 25 年法律第 261 号）に定める本県職員

（２）契約により操作等を認められた者

（情報セキュリティ管理体制）

第４条　情報資産のセキュリティを確保するため、全庁的な組織体制を整備する。

（情報資産の分類）

第５条　情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

（情報資産への脅威）

第６条　次に掲げる情報資産に対する脅威の発生度合や発生した場合の影響を考慮し、情報セキュリティ対策を講ずるものとする。

（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、重要情報の詐取、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、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

（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

（情報セキュリティ対策）

第７条　情報資産を、前条の脅威から守るため、以下の対策を講ずる。

（１）物理的セキュリティ対策　サーバ、情報システムを設置する施設、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。

（２） 人的セキュリティ対策　情報セキュリティに関する権限や責任及び被害の未然防止や抑制のため、職員等が遵守すべき事項を明確に定め、職員等に対する周知及び徹底を図るとともに、十分な教育・啓発が行われるよう必要な対策を講ずる。

（３）技術的セキュリティ対策　情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御、不正プログラム対策、ネットワーク管理等の技術的対策を講ずる。

（４）運用等におけるセキュリティ対策　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。

（５） 緊急時におけるセキュリティ対策　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。

（６）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。

①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、住民情報の流出を防ぐ。

②LGWAN 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。

③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、県と市町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（７）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、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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、利用にかか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。

（情報セキュリティ対策基準の策定）

第８条　この基本方針に基づき、情報セキュリティ対策を実施するに当たっての基本的な基準を明記した沖縄県情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。

（情報セキュリティ実施手順の策定）

第９条　この基本方針及び対策基準に基づき、各部局等の長が所掌する個々の情報システムについて情報セキュリティ対策を具体的に実施するために、情報セキュリティ実施手順（以下「実施手順」という。）を定めるものとする。

（対策基準及び実施手順の扱い）

第 10 条　対策基準及び実施手順は、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のある情報であることから非公開とする。

（職員等の義務）

第 11 条　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つとともに、業務の遂行において、情報セキュリティに関係する法令等及びこの基本方針を遵守する義務を負う。

（情報セキュリティに関する違反への対応）

第 12 条　情報セキュリティポリシーに違反した者については、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なることがある。

（情報セキュリティ監査の実施）

第 13 条　情報セキュリティ対策が遵守されていることを検証するため、定期的に監査を実施するものとする。

（評価及び見直し）

第 14 条　情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項並びに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等を踏まえ、情報セキュリティポリシー及び実施手順の見直しを行うものとする。

附 則

この基本方針は、平成 15 年４月１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 26 年４月１日から施行する。

附 則

この基本方針は、平成 29 年１月 20 日から施行する。

附 則

この基本方針は、令和 ３年 ４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。