大分県情報セキュリティ基本方針に関する規程

（目的）

第一条　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。

（用語の定義）

第二条　基本方針において掲げる用語は、以下の各号の定義するところによる。

一　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。

二　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。

三　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。

四　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。

五　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。

六　情報資産

県が公務において取り扱うすべての情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）をいう。

七　情報システム

ハードウェア、ソフトウェア、プログラム、ネットワーク及び記録媒体で構成されるもので、これら全体を用いて事務処理を行うための情報処理の仕組みをいう。

八　ネットワーク

電子計算機、関連機器等の多目的利用及び各種オンラインシステムのデータ伝送を目的とした構内及び庁舎間通信網により構築された情報通信基盤をいう。

九　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）又は戸籍事務等に関わる情報システム及びデータをいう。

十　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。）。

十一　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。

十二　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。

十三　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。

（情報資産への脅威）

第三条　県の情報資産に対する脅威として、次の各号の脅威を想定し、情報セキュリティ対策を実施する。

一　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、重要情報の搾取、内部不正等。

二　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。

三　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。

四　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。

五　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。

（適用範囲）

第四条　本基本方針の適用範囲は、知事部局の各部局（大分県部等設置条例（昭和二

十七年大分県条例第七十一号）に規定する部及び大分県行政組織規則（昭和三十一年大分県規則第十号。以下「組織規則」という。）第三条の二第一項に規定する会計管理局をいう。）、議会及び議会事務局、教育委員会、人事委員会、労働委員会、監査委員、選挙管理委員会、海区漁業調整委員会、内水面漁場管理委員会、収用委員会及びそれらの事務局、警察本部、企業局並びに病院局の情報資産に接するすべての者（臨時的任用又は非常勤の職にある者を含む。以下「職員等」という。）とする。

（職員等の義務）

第五条　職員等は、情報セキュリティポリシー及び関連法令等の趣旨を理解・認識し、遵守しなければならない。また、業務委託等により従事する事業者及び外郭団体（下請けを行う者を含む。以下「庁外業者」という。）に対しても、業務委託等により知り得た情報の守秘義務を認識させるため、契約又は別途取決めを行い、情報セキュリティの確保に必要な措置を講じなければならない。

（情報セキュリティ対策）

第六条　第三条に記載した脅威から情報資産を保護するために、次の各号に掲げるセキュリティ対策を講ずるものとする。

一　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全庁的な組織体制を確立する。

二　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。

三　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、次の三層の対策を講じる。

（１）個人番号利用事務系において、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。

（２）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。

四　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、物理的セキュリティ対策を講じる。

五　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セキュリティ対策を講じる。

六　技術的セキュリティ

電子計算機等の管理、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セキュリティ対策を講じる。

七　運用におけるセキュリティ

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等の運用におけるセキュリティ対策を講じる。

八　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、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。

（情報セキュリティ監査及び自己点検の実施）

第七条　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。

（情報セキュリティポリシーの見直し）

第八条　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため

新たに対策が必要になった場合には、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、リスクを検討したうえで、情報セキュリティポリシーを見直す。

（情報セキュリティ対策基準の策定）

第九条　前三条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を定める情報セキュリティ対策基準を策定する。

なお、情報セキュリティ対策基準は、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ことから非公開とする。

（情報セキュリティ実施手順の策定）

第十条　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は、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ことから非公開とする。

附　則

この基本方針は、令和８年３月２日から施行する。