佐賀県情報セキュリティ基本方針

1　目的

「佐賀県情報セキュリティ基本方針（以下「基本方針」という。）」は、県における情報セキュリティ対策の基本的な考え方及び方策を定め、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、電磁的記録媒体等で構成され、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

基本方針及び「佐賀県情報セキュリティ対策基準（以下「対策基準」という。）」のことをいう。

（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データをいう。なお、個人番号利用事務とは、職員が特定の事務処理において、県が保有する特定個人情報ファイルに個人情報を効率的に検索し、又は管理するために、必要な限度で個人番号を利用して処理する事務をいう。

（9）LGWAN[1]接続系

LGWAN に接続されたネットワーク上で稼動する情報システム（職員・給与、財務経営、電子文書決裁システム等）及びその情報システムで取り扱うデータをいう。

（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。

[1] LGWAN(Local Government Wide Area Network)とは、地方公共団体のみが接続することができる、行政専用のインターネットから切り離された閉域ネットワークのこと。

(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のメール本文のテキスト化や端末（LGWAN 接続系）への画面転送、添付ファイルの無害化等により、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。

(13) 各種委員（会）事務局

県の機関のうち、選挙管理委員会事務局、監査委員事務局、人事委員会事務局、労働委員会事務局及び海区漁業調整委員会事務局をいう。

(14) 外部サービス

事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。

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、盗聴等

（2）情報資産の無断持ち出し、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、委託管理の不備、情報資産の管理不備、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、その他内部不正等

（3）地震、落雷、火災等の災害によるサービス、業務の停止等

（4）大規模・広範囲にわたる疾病等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、通信の途絶等のインフラの障害からの波及等

4　適用範囲

（1）適用する対象

基本方針は、以下を対象として適用する。

①　ネットワーク及び情報システムを開発し、運用し、又は利用する職員（知事部局、教育委員会、議会事務局、各種委員（会）事務局及び東部工業用水道局に所属する者とする。以下「職員」という。）

②　ネットワーク及び情報システムの開発、運用等の業務を委託した事業者、機器等のサービス提供者等（以下「委託事業者」という。）

③　情報資産

（2）情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

①　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

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。）

② 情報システムの仕様書及、ネットワーク図等のシステム関連文書

5 職員等の遵守義務

職員及び受託者は、情報セキュリティポリシーの目的を理解し、遵守しなければならない。

6 情報セキュリティ対策

情報資産を３の脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

（１）管理体制

県の情報資産について、情報セキュリティを担保するための全庁的な管理体制を確立する。

（２）情報資産の分類と管理

県の保有する情報資産を重要性分類に応じて分類し、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、情報資産の流出を防ぐ。

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、職員が LGWAN 接続系端末とインターネット接続系端末の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、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対策

サーバ、マシン室、通信回線及び職員のパソコン等の管理について、物理的な対策を講じる。

（５）人的セキュリティ対策

情報セキュリティに関し、職員及び受託者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対策

情報システム及びファイルサーバ等に保管されている情報へのアクセス権の適切な管理、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、外部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インシデント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）業務委託及び外部サービスの利用

① 業務委託を行う場合には、委託事業者と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。

② 外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

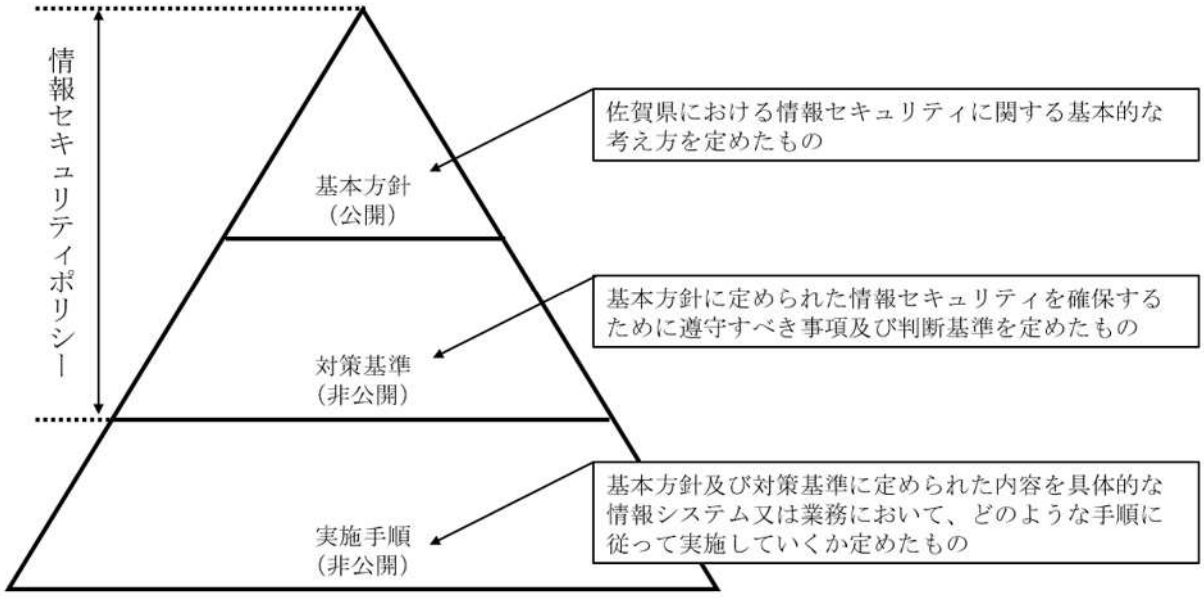
③ ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

7 対策基準及び実施手順の策定

（１）対策基準を別に策定するものとする。

（２）情報セキュリティポリシーに基づき、個々の情報システムについて具体的な手順等を定めた「佐賀県情報セキュリティ実施手順（各種手順及びマニュアルを含む。以下「実施手順」という。）」を別に策定するものとする。

（３）対策基準及び実施手順は、公開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。



8 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。

9 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、情報セキュリティポリシー及び実施手順（以下「情報セキュリティポリシー等」という。）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は情報セキュリティポリシー等を見直す。

附　則

この基本方針は、平成１８年２月２０日から施行する。

附　則

この基本方針は、令和元年１１月２２日から施行する。

附　則

この基本方針は、令和５年４月１日から施行する。