大分市における情報セキュリティの基本的な考え方

１．目的

大分市における情報セキュリティの基本的な考え方（以下、「基本方針」という。）は、本市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、本市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しています。

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）をいいます。

（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います。

（３）情報資産

本基本方針が対象とする情報資産は、次のとおりです。

①ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

②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。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

④職員が職務上作成し、又は取得した文書等

（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います。

①機密性

情報にアクセスすることが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います。

②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います。

③可用性

情報にアクセスすることが認められた者が、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います。

（５）情報セキュリティポリシー

本基本方針及び大分市情報セキュリティ対策基準のことをいいます。

（６）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います。

（７）ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等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います。

（８）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います。

（９）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が許可できるようにすることをいいます。

（１０）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無い等、安全が確保された通信をいいます。

３．適用範囲

市長事務部局、教育委員会、選挙管理委員会、公平委員会、農業委員会、固定資産評価審査委員会、上下水道局、消防局、監査事務局及び議会事務局

４．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します。

（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、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、火災等の災害によるサービス及び業務の停止等

（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

５．職員等の責務

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ます。

６．情報セキュリティ対策

脅威から情報資産を保護するために、以下の情報セキュリティ対策を実施します。

（１）　組織・体制

本市における情報セキュリティ対策は、責任や役割を明確にした組織・体制のもとに行うものとします。

（２）　情報の分類と管理

本市の保有する情報資産について、重要度に応じた情報分類の定義を行い、情報の管理責任及び管理方法を明確にします。

（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実施します。

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ぎます。

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します。なお、両システム間で通信する場合には、無害化通信を実施します。

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します。高度な情報セキュリティ対策として、大分県と市区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します。

（４）　物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を実施します。

（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実施します。

（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実施します。

（７）　運用

情報システムの監視、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実施します。

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します。

（８）　委託

外部委託する場合には、外部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行います。

約款による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ます。

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ます。

（９）　評価・見直し

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し、運用改善を行い情報セキュリティの向上を図ります。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行います。

７．情報セキュリティポリシーの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します。

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、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、情報セキュリティポリシーを見直します。

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します。

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市の行政運営に重大な支障を及ぼすおそれがありますので非公開とします。

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します。

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市の行政運営に重大な支障を及ぼすおそれがありますので非公開とします。

１１．公開範囲

本「基本方針」は、職員等に対して大分市の情報セキュリティ対策への指針を示すため、また市民・団体等に対して大分市の情報セキュリティ対策への理解を得るため、広く公開を行うものとします。

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 19 年４月１日から施行する。

附　則

この基本方針は、令和元年７月１日から施行する。

附　則

この基本方針は、令和２年４月１日から施行する。