大牟田市情報セキュリティ基本方針

1 目的

この基本方針は、本市の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の適正な管理運用を組織的かつ計画的に実施するため、本市における情報セキュリティの考え方及び対策に関し必要な事項を定めることを目的とする。

2 定義

（1） 情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準（以下「対策基準」という）をいう。

（2） 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。

（3） 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及びその構成機器をいう。

（4） 情報システム

コンピュータ、ソフトウェア、ネットワーク等で構成され、情報処理を行う仕組みをいう。

（5） 記録媒体

ハードディスク、フロッピーディスク、ＵＳＢメモリ、ＣＤ－ＲＯＭ、磁気テープその他これらに類する媒体をいう。

（6） 機密性

情報にアクセスすることを認められた者のみが、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）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。

（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。

３ 対象とする脅威

情報資産に対する脅威として、以下を想定し、情報セキュリティ対策を講じる。

（１） 部外者の侵入、不正アクセス、ウィルス攻撃、サービス不能攻撃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

４ 対象範囲

（１） 対象部局の範囲

この基本方針が対象とする部局は、大牟田市事務分掌条例（平成１０年条例第３号）第１条に掲げる部、消防本部及び消防署、会計課、企業局、教育委員会事務局及び教育機関（市立学校及び教育研究所を除く。）、市議会、選挙管理委員会、公平委員会、監査委員及び農業委員会の各事務局並びに大牟田市土地開発公社とする。

（２） 対象者の範囲

この基本方針が対象とする者は、本市の職員（地方公務員法（昭和２５年法律第２６１号）第３条第２項に規定する一般職及び同条第３項第３号に規定する特別職をいう。）及び大牟田市土地開発公社の職員（以下「職員等」という。）とする。

（３） 対象情報資産の範囲

この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　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

5 職員等の遵守義務

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、業務の遂行に当たり情報セキュリティに関する法令、情報セキュリティポリシー（以下「ポリシー」という）及び情報セキュリティ実施手順（以下「実施手順」という）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の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講じる。

（1） 組織体制

本市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。

（2） 情報資産の分類と管理

本市の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。

（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の制限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。

イ　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。

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、都道府県及び市区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、ネットワーク、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

情報システムの監視、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、ポリシーの運用面の対策を講じるものとする。

（８） 緊急時セキュリティ

情報資産への侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応マニュアルの策定等、危機管理対策を講じる。

（９） 業務委託と外部サービスの利用

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。

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。

（１０）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る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

７ 情報セキュリティ対策基準の策定

上記６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対策基準を策定する。

なお、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ることから非公開とする。

８ 実施手順の策定

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実施手順を策定するものとする。

なお、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ることから非公開とする。

９ 自己点検及び情報セキュリティ監査の実施

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自己点検及び情報セキ

ュリティ監査を実施する。

１０　ポリシー及び実施手順の見直し

自己点検及び情報セキュリティ監査の結果、ポリシー及び実施手順の見直しが必要と評価された場合又は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と判断された場合には、ポリシー及び実施手順を見直さなければならない。

付則

この基本方針は、平成１５年７月１日から施行する。

付則

この基本方針は、平成２１年１０月１日から施行する。

付則

この基本方針は、令和２年２月１８日から施行する。

付則

この基本方針は、令和４年１２月２６日から施行する。