水戸市議会情報セキュリティ基本方針

１　目的

水戸市議会（以下「議会」という。）が管理する情報資産（以下「情報資産」という。）の機密性、完全性及び可用性を維持するため、議会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に水戸市議会情報セキュリティ基本方針（以下「基本方針」という。）を策定する。

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）をいう。

(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

基本方針及び別に定める情報セキュリティ対策基準をいう。

(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（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。

(9) 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。）。

(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。

(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

議会は、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、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、設計又は開発の不備、プログラム上の欠陥、操作又は設定ミス、メンテナンス不備、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業務の停止等

(4) 大規模かつ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、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) 組織の範囲

基本方針は、情報資産を扱う議員及び議会事務局の職員（会計年度任用職員を含む。以下、「議員及び職員」という。）に適用する。

(2) 情報資産の範囲

基本方針の対象となる情報資産は、次のとおりとする。

①　議会が管理する情報システム及びこれらに関する設備

②　議会が管理する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　議会が管理する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　遵守義務

議員及び職員は、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別に定める水戸市議会情報セキュリティ実施手順を遵守しなければならない。

６　情報セキュリティ対策

議会は、上記３に記載する「対象とする脅威」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

情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

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、業務の効率性及び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、端末から情報を持ち出すことができないように設定すること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ものとする。

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。

(4) 物理的セキュリティ

議会が管理する情報システムについて、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、議員及び職員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、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、緊急時の対応を定める。

(8) 業務委託と外部サービス（クラウドサービス）の利用

① 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。

② 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　情報セキュリティ監査及び自己点検の実施

議会は、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。

８　情報セキュリティポリシーの見直し

議会は、以下に記載する場合には、情報資産及び議会が管理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ものとする。

(1) 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

(2) 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

９　情報セキュリティ対策基準の策定

議会は、上記６、７及び８に記載する対策等を実施するため、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別に定める。

10　情報セキュリティ実施手順の策定

議会は、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別に定める。

なお、情報セキュリティ実施手順は、公にすることにより議会の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。