むつ市議会情報セキュリティポリシー

情報セキュリティポリシーとは、むつ市議会（以下「議会」という。）が所掌する情報資産に関する情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。情報セキュリティポリシーは、議会の情報資産に関する業務に携わる議員及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応し、対策レベルを一層強化していくことも必要である。

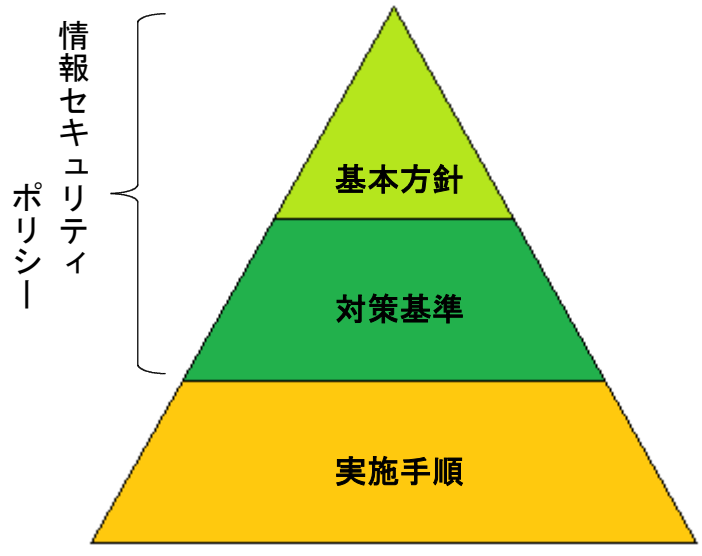
以上のことから、情報セキュリティポリシーを一定の普遍性を備えた部分である「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に対応する部分である「情報セキュリティ対策基準」の２階層に分けて策定することとした。

また、情報セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の実施手順として「情報セキュリティ実施手順」を策定することとする。

令和８年３月３１日　策定

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順



※実施手順は個々のシステムごとに定めるものであり、手順や事項について策定するものである。

情報セキュリティポリシーに関する体系図

情報セキュリティ基本方針

１　目的

本基本方針は、議会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、市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

本基本方針及び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

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。

(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

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、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

４　適用範囲

(1) 適用機関の範囲

本基本方針が適用される機関は、議会とする。

(2) 情報資産の範囲

本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

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

５　議員の遵守義務

議員は、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

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

議会の情報資産について、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

議会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。

(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話経路を分割する。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等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

サーバ等、サーバー室等、通信回線等及び議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

情報セキュリティに関し、議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、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。

(8) 外部サービス（クラウドサービス）の利用

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講じる。

クラウド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。

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。

(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る。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う。

７　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、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

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する。

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。

情報セキュリティ対策基準

１　目的

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための、議会の情報資産に関する情報セキュリティ対策の基準を定めたものである。

２　対象者

本対策基準の対象者は議員とする。

３　用語の定義

（１）　情報資産

文書、電子データ、システム、記録媒体等のうち、議会が議会活動のため保有または管理するものをいう。

（２）　インシデント

情報資産に対する漏えい、紛失、破壊、不正利用、改ざんなどのセキュリティ上の問題が発生、またはそのおそれがある現象のことをいう。

４　組織体制

（１）　統括情報セキュリティ責任者

① 議会に統括情報セキュリティ責任者（以下「統括責任者」という。）を置き、議会事務局長をもってこれに充てる。

② 統括責任者は、議会が保有するネットワーク及び情報システムの開発、設定の変更、運用、見直し等及び情報セキュリティ対策に関する権限及び責任を有し、情報セキュリティの推進及び事故対応の総括を行う。

（２）　情報セキュリティ担当者

議会に情報セキュリティ担当者を置き、統括責任者の指示等に従い、情報システムの開発並びに設定、運用、更新等の日常的な作業及び利用者への周知啓発を行う。

（３）　クラウドサービス利用における組織体制

クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

５　情報資産の分類

議会における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

分　類	分類基準	取扱制限
機密性３	取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止

		・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

完全性による情報資産の分類

分　類	分類基準	取扱制限
完全性２	取り扱う情報資産のうち、改ざん、誤謬又は破損により、住民の権利が侵害される又は行政事務の的確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	

可用性による情報資産の分類

分　類	分類基準	取扱制限
可用性２	取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２情報資産以外の情報資産	

６　保管・廃棄

各分類２以上の情報資産については、適切に保管し不要となった場合は、復元不可能な方法で廃棄する。

７　端末の管理及び運用等

貸与されたタブレット型端末の管理及び運用については、別に定める「むつ市議会情報端末機等使用基準」による。

８　会議システムの管理及び運用

会議システムの管理及び運用は、別に定める情報セキュリティ実施手順による。

９　啓発

統括責任者は、適宜、情報セキュリティに関する研修を実施する。

10　監査・自己点検

定期的に監査・自己点検を実施し、改善が必要な事項を報告・是正する。

11　インシデントへの対応

情報セキュリティインシデントが発生した場合は、直ちに統括責任者に報告し、市の関連部局と連携し、被害拡大防止措置等を講じる。