我孫子市議会情報セキュリティポリシー
情報セキュリティ対策基本方針

我孫子市議会

更新履歴

変更日	項目	変更内容
2026/02/26	―	新規作成

目次

情報セキュリティ対策基本方針

1.目的

本基本方針は、本市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、本市議会が独自に構築・運用する情報システム及びネットワーク、並びにこれらで扱う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。なお、市から貸与されているパソコン等の端末及び接続するネットワークについては、市と市議会による共同策定の情報セキュリティ対策基本方針に準拠することとする。

2.定義

(1) 議会ネットワーク

議会活動及び事務の円滑な遂行を目的として、本市議会が独自に管理するインターネット接続環境をいう。

(2) クラウドサービス

インターネットを通じて提供される外部サービスをいう(ペーパーレス会議システム、議会中継システム、その他将来的に導入される議会活動に資するサービスを含む)。

(3) 端末管理システム(MDM)

ネットワークに接続する端末の設定、利用制限、及び盗難・紛失時の遠隔消去等を一元的に管理する仕組みをいう。

(4) 情報資産

議会ネットワーク及び情報システムで取り扱うデータ、システム関連文書等をいう。

(5) 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。

(6) 機密性・完全性・可用性

①機密性

許可さ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。

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。

③可用性

許可された者が、必要な時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。

3. 対象とする脅威

情報資産に対する脅威として、サイバー攻撃、内部不正、紛失、災害、及びインフラ障害等を想定し、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、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) 行政機関の範囲

議会ネットワークを利用する全ての議員、議会事務局職員、及び議会運営に関わる市職員に適用する。

(2) 情報資産の範囲

議会が管理するネットワーク、情報システム（タブレット端末等を含む）、及びこれらで取り扱うデータや文書を対象とする。

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器等
情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等
ネットワーク・情報システムに関する施設設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体等
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ等（情報システムから印刷した文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

図表 情報資産の種類と例

5. 議員等の遵守義務

本市議会の情報資産に接する全ての議員及び職員（以下「議員等」という。）は、本基本方針を遵守しなければならない。

6. 情報セキュリティ対策

議会ネットワーク及びクラウドサービスを安全に利用するため、以下の対策を講じる 。

(1) 組織体制

情報セキュリティ対策を推進する組織体制を確立する。

① 最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

（ア）議長を CISO とする。CISO は、本市議会における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（イ）CISO は、本基本方針に定められた自らの担務を、情報セキュリティ責任者その他の本基本方針に定める責任者に担わせることができる。

② 情報セキュリティ責任者

（ア）議会事務局長を CISO 直属の情報セキュリティ責任者とする。情報セキュリティ責任者は、CISO を補佐しなければならない。

（イ）情報セキュリティ責任者は、本市議会の情報セキュリティ対策、全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③ 情報セキュリティ・システム管理者

（ア）議会事務局次長を情報セキュリティ・システム管理者とする。

（イ）情報セキュリティ・システム管理者は、市議会の情報セキュリティ対策に関する権限及び責任を有する。

（ウ）情報セキュリティ・システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

④情報システム担当者

情報セキュリティ・システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

(2) 情報資産の分類と管理

本市議会が保有する情報資産を、機密性、完全性及び可用性に応じて以下に分類し、その分類に基づき適切な管理を行う。

機密性による情報資産の分類

分類	分類基準	取扱制限
自治体機密性3A	議会事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年4月1日内閣総理大臣決定）に定める秘密文書に相当する文書	・許可された端末以外での作業の原則禁止 ・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 ・信頼のできるネットワーク回線の選択 （3A・3Bの場合） ・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 ・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
自治体機密性3B	議会事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体機密性3C	議会事務で取り扱う情報資産のうち、自治体機密性3B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体機密性2	議会事務で取り扱う情報資産のうち、秘密文書に相当する自治体機密性3は要しないが、直ちに一般に公表することを前提としていない情報資産	
自治体機密性1	自治体機密性2又は自治体機密性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
自治体完全性2	議会事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は議会事務の適確な遂行に支障（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
自治体完全性1	自治体完全性2の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
自治体可用性2	議会事務で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議会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
自治体可用性1	自治体可用性2の情報資産以外の情報資産	－

(3) 物理的セキュリティ

端末、サーバ、通信回線、及び管理区域（端末の保管場所等）について、物理的な対策を講じる。

(4) 人的セキュリティ

①情報セキュリティに関し、本基本方針等を遵守し、必要な教育及び啓発を行う。

②市議会から貸与されたタブレット端末を使用する際は、別に定める「我孫子市タブレット端末使用基準」を遵守しなければならない。

③支給以外のパソコン、モバイル端末及び電磁的記録媒体等を議会ネットワークへ接続する場合は、情報セキュリティ責任者へ申請し許可を得なくてはならない。

(5) 技術的セキュリティ

MDM（端末管理システム）による一元管理 、アクセス制御、不正アクセス対策等の技術的対策を講じる。

(6) 運用

情報システムの監視、本基本方針の遵守状況の確認、及び事故発生時の緊急時対応計画の策定を行う。

(7) 業務委託及び外部サービス（クラウドサービス）の利用

外部委託やクラウドサービス利用時は、機密保持等を含むセキュリティ要件を契約に明記し、委託先において必要な対策が確保されていることを確認する。

7. 情報セキュリティ監査及び自己点検の実施

遵守状況を検証するため、定期的または必要に応じて点検を実施する。

8. 情報セキュリティポリシーの見直し

状況の変化や点検の結果に基づき、本基本方針を適宜見直す。