富良野市議会
情報セキュリティポリシー
（情報セキュリティ基本方針）

令和８年４月

富良野市議会

（目次）

情報セキュリティ基本方針

第１章　情報セキュリティ基本方針

１．目的

本基本方針は、富良野市議会（以下、「議会」という。）が保有する情報資産の機密性、安全性及び可用性の維持の確保を図ること並びに信頼性を確保するため、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とする。

２．定義

（１）機器

ハードウェア及びソフトウェアをいう。

（２）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、それを構成する富良野市議会タブレット端末等使用基準第２条第１項第１号及び富良野市議会グループウェア運用管理に関する基準第８条に規定する機器をいう。

（３）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。

（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う。

（５）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等をいう。

（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。

（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。

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（DoS 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、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）本基本方針及び情報セキュリティ対策基準等が適用される範囲は、富良野市議会議員（以下、「議員」という。）とし、本基本方針及び情報セキュリティ対策基準等が対象とする情報資産を議会事務局職員が取り扱う場合は、当該職員にも適用があるものとする。
（２）本基本方針及び情報セキュリティ対策基準等が対象とする情報資産は、次のとおりとする。
①議会の活動及び運営に当たって使用する情報システム並びにこれらに関する設備及び電磁的記録媒体
②①で取り扱う情報（これらを印刷した文書を含む。）
③①に関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
４．適用範囲（１）に規定される者は、情報セキュリティの重要性について共通の認識を持ち、議会の活動及び運営に当たって本基本方針及び情報セキュリティ対策基準等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の推進を議長が統括する組織体制において実施する。
（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じん性の向上
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適切な対策を講ずる。
（４）物理的セキュリティ
通信回線、機器及び記録媒体の管理について、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、４．適用範囲（１）に規定される者が遵守すべき事項を定めるとともに、十分な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
機器の管理、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

情報システムの管理、本基本方針及び情報セキュリティ対策基準等に基づき定められる対策の遵守状況の確認、本基本方針及び情報セキュリティ対策基準等の対象となる情報資産に携わる第三者の情報セキュリティの確保等、本基本方針及び情報セキュリティ対策基準等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、必要に応じ、緊急時対応計画を策定する。

（８）業務委託と外部サービス（クラウドサービス）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。

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。

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で発信できる情報資産の範囲も規定し、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

本基本方針及び情報セキュリティ対策基準等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。新たに対策が必要となった場合は、適宜見直しを行う。

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情報セキュリティ対策基準を必要に応じ、策定するものとする。なお、情報セキュリティ対策基準は、公にすることにより議会の活動及び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．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必要に応じ、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活動及び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。