○松本市議会情報セキュリティ基本方針

令和８年３月３０日
議会訓令甲第２号

（目的）

第１条　この基本方針は、松本市議会（以下「議会」という。）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、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　議会は、この基本方針をもって、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定するサイバーセキュリティを確保するための方針に位置付ける。

（定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

⑴　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。

⑵　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。

⑶　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。

⑷　情報セキュリティポリシー　この基本方針及び第９条第１項に規定する情報セキュリティ対策基準をいう。

⑸　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。

⑹　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。

⑺　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。

（対象とする脅威）

第３条　情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。

⑴　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

⑵　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

⑶　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

⑷　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

⑸　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

（適用範囲）

第４条　この基本方針を適用する対象者及び保護すべき情報資産の範囲は、次に掲げると

おりとする。

⑴　対象者の範囲　議員及び議会事務局職員（以下「議員等」という。）

⑵　保護すべき情報資産の範囲　議会活動（これに付随する活動を含む。以下同じ。）のために議会が管理運用する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電磁的記録媒体、当該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。）並びに当該情報システムの仕様書、ネットワーク図等のシステム関連文書

（議員等の遵守義務）

第５条　議員等は、情報セキュリティの重要性について共通の認識を持ち、議会活動及び議員活動の遂行に当たって情報セキュリティポリシー及び第１０条第１項に規定する情報セキュリティ実施手順を遵守しなければならない。

２　議会事務局職員は、業務において松本市の執行機関が管理運用するネットワーク及び情報システムを使用するときは、松本市情報セキュリティ対策基本要綱（平成１６年訓令甲第１号）、松本市情報セキュリティポリシー対策基準及び松本市情報セキュリティポリシー実施手順を遵守しなければならない。

（情報セキュリティ対策）

第６条　議会は、第３条に規定する脅威から第４条第２号に規定する情報資産（以下「対象情報資産」という。）を保護するため、次に掲げる情報セキュリティ対策を講じるものとする。

⑴　組織体制の確立　対象情報資産について、情報セキュリティ対策を推進する組織体制を確立すること。

⑵　情報資産の分類と管理　対象情報資産を機密性、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こと。

⑶　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、議会活動の効率性・利便性の観点を踏まえ、情報システム全体に対し、必要な対策を講じること。

⑷　物理的セキュリティ　サーバ、議員控室及び議会事務局事務室、通信回線、議会のパソコン等の管理について、物理的な対策を講じること。

⑸　人的セキュリティ　情報セキュリティに関し、議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こと。

⑹　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こと。

⑺　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こと。また、対象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こと。

⑻　業務委託に係る情報セキュリティ対策　議会事務局が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こと。

⑼　外部サービス（クラウドサービス）の利用に係る情報セキュリティ対策　議会が外部サービス（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こと。

⑽　ソーシャルメディアサービスの利用に係る情報セキュリティ対策　議会が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、及び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こと。

⑾　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こと。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こと。

２　議員等は、第３条に規定する脅威から対象情報資産を保護するため、自己の統一タブレット端末（議会活動及びこれに必要な調査研究活動に使用するため、松本市において調達し、議会が議員等に配備するタブレット端末をいう。）及び自己の私物端末（議会活動及び議員活動に使用するため、議員等が自己の負担において調達した情報通信端末で、インターネットを通じて対象情報資産に接続するものをいう。）に対し、必要かつ相当な対策を講じるものとする。

（情報セキュリティ監査及び自己点検の実施）

第７条　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ものとする。

（情報セキュリティポリシーの見直し）

第８条　議会は、前条に規定する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、保有する情報及び利用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。

（情報セキュリティ対策基準の策定）

第９条　議会は、前３条に規定する対策等を実施するため、具体的な遵守事項、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ものとする。

２　前項に規定する情報セキュリティ対策基準は、公にすることにより議会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。

（情報セキュリティ実施手順の策定）

第１０条　議会は、前条第１項に規定する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。

２　前項に規定する情報セキュリティ実施手順は、公にすることにより議会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。

（補則）

第１１条　この基本方針に定めるもののほか必要な事項は、議長が別に定める。

附　則

この訓令は、令和８年４月１日から施行する。