滑川市議会告示第１号

滑川市議会情報セキュリティ基本方針を次のように定める。

令和８年３月 19 日

滑川市議会議長　竹　原　正　人

滑川市議会情報セキュリティ基本方針

（目的）

第１条　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。

（定義）

第２条　本基本方針における定義は以下のとおりとする。

(1) 情報資産とは、滑川市議会が保有及び管理する全ての電子的情報、システム、端末機器等をいう。

(2) 情報セキュリティとは、情報資産の機密性、完全性、可用性を確保し、情報漏洩、不正アクセス、改ざん、破壊等の脅威から情報を保護することをいう。

（対象とする脅威）

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

(1) サイバー攻撃（マルウェア、ランサムウェア、不正アクセスなど）

(2) ヒューマンエラー（情報漏洩、誤送信、紛失など）

(3) 内部不正（意図的な情報損壊・漏洩、不適切な利用）

(4) 自然災害や物理的脅威（地震、火災、洪水等による情報資産の損失）

(5) 停電やシステム障害による業務停止

（適用範囲）

第４条　本基本方針は、本市議会に属するすべての議員（以下「議員」という。）及び議会事務局職員（以下「職員」という。）に適用する。

（滑川市情報セキュリティポリシーとの関係）

第５条　本基本方針は、議会活動における情報セキュリティ管理を独自に定めるものであり、滑川市情報セキュリティポリシーとは別の規定として運用されるものである。

２　本基本方針の内容が滑川市情報セキュリティポリシーに定める基準と差異がある場合については、本基本方針の規定を優先して適用するものとする。

３　職員は、その職務において滑川市情報セキュリティポリシーの対象となる場合は、当該規定を遵守するものとする。

（議員及び職員の遵守義務）

第６条　議員及び職員は、情報資産を適切に管理・保護するため、次の事項を遵守しなければならない。

(1) 情報資産にアクセスする際の認証情報の秘密を保持すること。

(2) 機密情報の不正利用や誤送信を防止すること。

(3) 貸与されたタブレット端末（以下「端末」という。）を使用する際は、別に定める使用基準の目的の範囲内で安全に取り扱うこと。

（組織体制）

第７条　本市議会が保有する情報資産について、情報セキュリティ対策を推進するための組織体制を確立するものとする。

（情報資産の分類と管理）

第８条　情報資産は、その機密性、完全性及び可用性により、別表１から別表３までのとおり分類し、必要に応じ取扱制限を行うものとする。

（物理的セキュリティ対策）

第９条　議会事務局（以下「事務局」という。）は、議会施設内の機密情報及び端末機器を管理するため、次の物理的対策を実施するものとする。

(1) 施設内の施錠管理

(2) 関係者以外の立ち入り制限

(3) 機器紛失防止のための指定区域内管理及び持ち出し時の登録

（人的セキュリティ対策）

第 10 条　議長は、情報セキュリティに関する教育及び訓練を実施するものとする。

（技術的セキュリティ対策）

第 11 条　事務局は、技術的セキュリティ対策として次の措置を講じるものとする。

(1) セキュリティソフトウェアの導入並びに定期的な更新

(2) アクセスログの記録監視

(3) 端末のセキュリティ設定及び通信暗号化の徹底

（インシデント管理）

第 12 条　事務局は、インシデント対応手順を別に定めるものとする。

２　情報漏洩、不正アクセス、誤送信等のセキュリティインシデント若しくは端末機器の紛失・盗難、破損等の物理的インシデントが発生した場合、議員又は職員は速やかに議長及び事務局へ報告し、迅速な対応が取れるよう協力するものとする。

３　事務局は、インシデントの発生を確認したとき又インシデント発生の報告を受けたときは、インシデント対応手順に従い必要な措置を講じるものとす

る。

（端末の管理）

第 13 条　議員及び職員は、情報資産を適切に保護するため、端末の利用にあたっては、使用基準に規定する事項を遵守するものとする。

（情報セキュリティ監査）

第 14 条　事務局は、情報資産のリスク評価を定期的に実施し、新しいリスク発生時には必要な管理措置を講じるものとする。

２　事務局は、リスク評価結果の記録を作成・保存し、関係者へ報告するものとする。

（自己点検の実施）

第 15 条　議員及び職員は、本基本方針に係る対策の実施状況を定期的に自己点検し、脆弱性を早期に発見するとともに、速やかに適切な対応を講じるものとする。

（ネットワークの利用）

第 16 条　議会活動において利用するネットワークは、セキュリティリスクを最小化する措置を講じたうえで利用するものとする。

（コミュニケーションツールの利用）

第 17 条　議会で利用するチャットアプリ、メール等のコミュニケーションツールの利用にあっては、次の事項を遵守するものとする。

(1)　各ツールは指定用途に限定し、議会活動および事務局間連絡で必要とされる情報交換にのみ使用する。

(2)　各コミュニケーション手段を利用して送受信する文書、データ等の情報は、その重要度及び機密性に応じて適切に取り扱い、情報漏洩防止を徹底する。

(3)　チャットアプリでやり取りされる情報は、機密性を保持し、必要なセキュリティ設定を適用する。

(4)　メールで送受信する際は不正アクセス防止のため、情報の分類に応じてパスワード付きファイルなどの暗号化措置を講じる。

(5)　メールで送受信する際は、誤送信や第三者閲覧のリスクを回避するため、送信先の確認及び使用場所の注意を徹底する。

２　事務局は、各コミュニケーションツールの運用ルールや責任範囲を整理し、不適切な利用や管理不備によるリスクを最小化するものとする。

（ポリシー改善の方針）

第 18 条　議長は、情報セキュリティ対策の有効性を定期的に確認し、技術の進展や新たな脅威に対応するため、本基本方針を適宜改定するものとする。

附　則

この規程は、公布の日から施行する。

別表１　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	行政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	・支給された端末以外での作業の原則禁止（自治体機密性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
自治体機密性３Ｂ	行政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	行政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	行政事務で取り扱う情報資産のうち、自治体機密性３に相当する機密性は要しないが、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	－

別表２　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	行政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行政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	－

別表３　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	行政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
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	－