

## 米原市議会情報セキュリティ基本方針

令和8年4月1日

### (目的)

第1条 本基本方針は、米原市議会（以下「本市議会」という。）が保有する情報資産の機密性、完全性およ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。

- (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およびその構成機器（ハードウェアおよびソフトウェアを含む。）をいう。
- (2) 情報システム コンピュータ、ネットワークおよ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、完全性および可用性を維持することをいう。
- (4) 議員等 情報システムの運用に関わる議員および事務局職員をいう。
- (5) 機密性 情報にアクセスすることを認められた者のみが、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、改ざんまた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) 利用端末等 議員等に対し、職務上利用することが許可されたパソコン、タブレット等および職務上利用することが許可された外部記録媒体をいう。
- (9) クラウドサービス ソフトウェアやデータ、これらを提供するための技術基盤等をインターネットを通じて利用できるサービスをいう。

### (対象とする脅威)

第3条 情報資産に対する脅威として、次の各号の脅威を想定する。

- (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、操作・設定ミス、メンテナンス不備、マネジメントの欠陥、機器故障等の非意図的な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および業務の停止等
  - (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、通信、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 本基本方針を適用する人的範囲は、議員等とする。

2 本基本方針が対象とする情報資産は、次の各号に掲げるとおりとする。

- (1) ネットワークおよび情報システムならびにこれらに関する設備および電磁的記録媒体
  - (2) ネットワークおよ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および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、業務の遂行に当たって本基本方針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 本市議会は、第3条に規定する脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講じるものとする。

(1) 組織体制

本市議会の情報資産の情報セキュリティ対策を推進するため、組織体制を別表1のとおり確立する。

(2) 情報資産の分類と管理

本市議会の保有する情報資産を機密性、完全性および可用性に応じて別表2のとおり分類し、当該分類に基づく情報セキュリティ対策を実施する。

(3) 物理的セキュリティ

利用端末等の管理における物理的な対策を講じる。

(4) 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、十分な教育および啓発を行う等の人的な対策を講じる。

(5) 技術的セキュリティ

利用端末等の管理、アクセス制御等の技術的な対策を講じる。

(6) 運用

情報システムの運用に当たっては、議員等が遵守すべき運用に係る基準等を定め、これに基づき運用するものとする。

(自己点検の実施)

第7条 本基本方針の遵守状況を検証するため、定期的または必要に応じて、議会における自己点検を実施する。

(本基本方針の見直し)

第8条 自己点検の結果、本基本方針の見直しが必要となった場合およ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は、本基本方針を見直すものとする。

付 則

この基本方針は、令和8年4月1日から施行する。

別表1（第6条関係）

情報セキュリティ責任者	本市議会の情報セキュリティ対策に関する総括的な権限および責任を有する者として、議長をもって充て、当該権限に基づく実務は、議会事務局長が行うものとする。
情報セキュリティ管理者	本市議会の情報セキュリティ対策に関する権限および責任を有する者として、議会事務局長をもって充てる。
情報システム管理者	情報システムに係る設定変更、運用、見直し等を行う権限および責任を有する者として、議会事務局次長をもって充てる。
情報システム担当者	情報システムの処理を適正に行う者として、情報システム担当者を置く。

別表2（第6条関係）

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 B	情報システムで取り扱う情報資産のうち、漏洩等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務また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	<ul style="list-style-type: none"> <li>・支給された利用端末等以外での作業の原則禁止</li> <li>・必要以上の複製および配布禁止</li> <li>・必要以上の電磁的記録媒体等への書込み禁止</li> </ul>
機密性 3 C	情報システムで取り扱う情報資産のうち、機密性3 B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	<ul style="list-style-type: none"> <li>・データの復元不可能な処理をしての廃棄</li> <li>・信頼できるネットワーク回線の選択</li> <li>・外部での情報閲覧等を行う場合の安全管理に係る遵守事項の整備</li> </ul>
機密性 2	情報システムで取り扱う情報資産のうち、機密性3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ない情報資産	<ul style="list-style-type: none"> <li>・電磁的記録媒体の施錠可能な場所への保管</li> </ul>
機密性 1	機密性3または機密性2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	情報システムで取り扱う情報資産のうち、改ざん、誤びゅうまたは破損により、住民の権利が侵害される、または議会運営事務的的確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> <li>・バックアップ</li> <li>・外部での情報閲覧等を行う場合の安全管理に係る遵守事項の整備</li> <li>・電磁的記録媒体の施錠可能な場所への保管</li> </ul>
完全性 1	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
可用性 2	情報システムで取り扱う情報資産のうち、滅失、紛失また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、または議会運営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	<ul style="list-style-type: none"> <li>・バックアップ、指定する時間以内の復旧</li> <li>・電磁的記録媒体の施錠可能な場所への保管</li> </ul>
可用性 1	可用性2の情報資産以外の情報資産	—