

神戸市会情報セキュリティポリシー

令和8年2月16日 制定

(市会運営委員会決定)

令和8年4月1日 施行

神戸市会

改訂履歴

施行年月日	版番号	改定理由・内容
令和8年4月1日	第1.0版	初版発行（令和8年2月16日市会運営委員会決定）

目次

1.	目的.....	1
2.	定義.....	1
2.1.	ネットワーク.....	1
2.2.	情報システム.....	1
2.3.	情報セキュリティ.....	1
2.4.	機密性.....	1
2.5.	完全性.....	1
2.6.	可用性.....	1
2.7.	インターネット接続系.....	1
3.	対象とする脅威.....	1
4.	適用範囲.....	1
4.1.	適用範囲.....	1
4.2.	情報資産の範囲.....	2
5.	議員等の遵守義務.....	2
6.	情報セキュリティ対策.....	2
6.1.	組織体制.....	2
6.2.	情報資産の分類と管理.....	2
6.3.	情報システム全体の強靱性の向上.....	2
6.4.	物理的セキュリティ.....	2
6.6.	技術的セキュリティ.....	2
6.7.	運用.....	2
6.8.	業務委託と外部サービス（クラウドサービス）の利用.....	3
6.9.	評価・見直し.....	3
7.	情報セキュリティ監査及び自己点検の実施.....	3
8.	情報セキュリティポリシーの見直し.....	3

1. 目的

本情報セキュリティポリシーは、神戸市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、神戸市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。なお、本情報セキュリティポリシーは、地方自治法に基づくサイバーセキュリティを確保するための方針として定めるものである。

2. 定義

2.1. 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、その構成機器（ハードウェア及びソフトウェア）をいう。

2.2. 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。

2.3. 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。

2.4. 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。

2.5. 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。

2.6. 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。

2.7. インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

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。

- 3.1. 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
- 3.2. 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の要因による情報資産の漏えい・破壊・消去等
- 3.3. 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
- 3.4. 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
- 3.5. 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

4.1. 適用範囲

本情報セキュリティポリシーの適用範囲は、神戸市会とする。ただし、本市会活動（神戸市会会議規則（昭和31年10月20日市会議決）に定める会議）に従事する場合に限る。

4.2. 情報資産の範囲

本情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。

- ① 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
- ② 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。）
- ③ 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. 議員等の遵守義務

神戸市会議員、会派雇用職員、神戸市会事務局職員等（以下「議員等」という。）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情報セキュリティポリシー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。

6.1. 組織体制

神戸市会の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。最高情報セキュリティ責任者（CISO）を置き、神戸市会の情報セキュリティ対策に関する最終的な責任を負う。

CISOを神戸市会議長とし、CISOを補佐する統括情報セキュリティ責任者を神戸市会事務局次長、統括情報セキュリティ責任者を補佐する情報セキュリティ管理者を神戸市会事務局次長、実務を担当する情報管理者を神戸市会事務局総務課長とする。

6.2. 情報資産の分類と管理

神戸市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。情報資産の分類については、『地方公共団体における情報セキュリティポリシーに関するガイドライン』に準ずる。

6.3. 情報システム全体の強靱性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点から踏まえ、情報システム全体に対し、次の対策を講じる。

インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

6.4. 物理的セキュリティ

サーバ、情報システム室、通信回線及び議員等のパソコン等の管理について、物理的な対策を講じる。

6.5. 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。

- ① 情報資産の利用や持ち出しは、業務目的に限るものとする。
- ② 情報セキュリティインシデントを発見した場合は、速やかに定められた窓口へ報告する義務を負う。

6.6. 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。

6.7. 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、緊急時対応計画を策定する。緊急時対応計画には、以下の内容を定めなければならない。

- ① 関係者の連絡先
- ② 発生した事案に係る報告すべき事項
- ③ 発生した事案への対応措置
- ④ 再発防止措置の策定

6.8. 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。

6.9. 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。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。

7. 情報セキュリティ監査及び自己点検の実施

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。

8. 情報セキュリティポリシーの見直し

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となった場合には、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。