丹波篠山市議会情報セキュリティポリシー

令和８年４月１日　施行

丹波篠山市議会

丹波篠山市議会情報セキュリティポリシー

（目的）

第１条　本情報セキュリティポリシーは、丹波篠山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、丹波篠山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。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。

（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、それぞれ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及びその構成機器（ハードウェア及びソフトウェア）をいう。

(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。

(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。

(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。

(5)　完全性　情報が破棄、改ざん又は消去をされていない状態を確保することをいう。

(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。

(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。

（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ものとする。

(1)　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃、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

（適用範囲）

第４条　本情報セキュリティポリシーが適用される実施機関は、丹波篠山市議会とする。ただし、本市議会活動（丹波篠山市議会会議規則に定める会議）に従事する場合に限る。

２　本情報セキュリティポリシーが対象とする情報資産は、次にとおりとする。

(1)　ネットワーク、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

（議員等の遵守義務）

第５条　丹波篠山市議会議員、丹波篠山市議会事務局職員等（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、業務の遂行にあたって本情報セキュリティポリシーを遵守しなければならない。

２　丹波篠山市議会事務局職員、会計年度職員（以下「職員等」という）は、本市が管理する情報資産に対しては「丹波篠山市情報セキュリティポリシー」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　第３条各号に規定する脅威から情報資産を保護するため、以下の情報セキュリティ対策を講ずるものとする。

(1)　組織体制　丹波篠山市議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、丹波篠山市議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 を丹波篠山市議会議長とし、CISO を補佐する統括情報セキュリティ責任者を丹波篠山市議会事務局長、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丹波篠山市議会事務局課長とする。

(2)　情報資産の分類及び管理　丹波篠山市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行う。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。

(3)　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、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、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。

(4)　物理的セキュリティ　サーバ等、サーバ室等、ネットワーク等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。

(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)　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。

(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、外部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ずるとともに、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切に対応するため、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。

(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。

（情報セキュリティ監査及び自己点検の実施）

第７条　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　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。