丹波篠山市情報セキュリティ基本方針

平成３０年３月３０日
訓令第１号

（目的）

第１条　この基本方針は、本市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　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)　情報セキュリティポリシー　この基本方針及び情報セキュリティ対策基準をいう。

(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。

(6)　完全性　情報が破壊、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。

(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)　マイナンバー利用事務系（個人番号利用事務系）　個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(9)　ＬＧＷＡＮ接続系　ＬＧＷＡＮ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（マイナンバー利用事務系を除く。）。

(10)　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。

(11)　通信経路の分割　ＬＧＷＡＮ接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(12)　無害化通信　インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、

安全が確保された通信をいう。

（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　この基本方針が適用される実施機関は、市長、教育委員会、選挙管理委員会、監査委員、公平委員会、農業委員会、固定資産評価審査委員会、消防長及び議会とする。ただし、実施機関（市長及び消防長を除く。）が別に定める場合を除く。

２　この基本方針が対象とする情報資産は、本市が保有するもので、次に掲げるとおりとする。

(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

（職員等の遵守義務）

第５条　職員、非常勤職員及び臨時職員（以下「職員等」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情報セキュリティポリシー及び情報セキュリティ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　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、次の各号に掲げる区分に応じ、当該各号に定める次の各号に掲げる区分に応じ、当該各号に定める情報セキュリティ対策を講ずるものとする。

(1)　組織体制　本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立すること。

(2)　情報資産の分類及び管理　本市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こと。

(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、次の三段階の対策を講ずることをいう。

ア　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等を行うこと。

イ　ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割すること。この場合において、両システム間で通信する場合には、無害化通信を実施すること。

ウ　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こと及び高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施すること。

(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職員等のパソコン等の管理について、物理的な対策を講ずること。

(5)　人的セキュリティ　情報セキュリティに関し、職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ずること。

(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ずること。

(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ずるものとする。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切に対応するため、緊急時対応計画を策定すること。

(8)　業務委託、外部サービスの利用及びソーシャルメディアサービス　次に掲げる場合に応じ、次に定める対策を講ずることをいう。

ア　業務委託を行う場合　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ずること。

イ　外部サービスを利用する場合　利用に係る規定を整備し対策を講ずること。

ウ　ソーシャルメディアサービスを利用する場合　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、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。

(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、定期的に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又は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、リスクを検討した上で、情報セキュリティポリシーの見直しを行うものとする。

（情報セキュリティ対策基準の策定）

第９条　前３条に規定する対策等を実施するため、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準（以下「対策基準」という。）を策定するものとする。

（情報セキュリティ実施手順の策定）

第１０条　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（以下「実施手順」という。）を策定するものとする。なお、実施手順は、公にすることにより本市の行政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。

（その他）

第１１条　この基本方針に定めるもののほか、必要な事項は、別に定める。

附　則

（施行期日）

１　この訓令は、平成３０年４月１日から施行する。

（篠山市情報セキュリティ運用管理要領の廃止）

２　篠山市情報セキュリティ運用管理要領（平成１７年篠山市訓令第１２号）は、廃止する。

附　則

この訓令は、公布の日から施行する。

附　則（令和８年３月３１日訓令第１号）

この訓令は、公布の日から施行する。