安来市サイバーセキュリティを確保するための方針

策定：令和８年４月１日

安来市議会
安来市長
安来市消防長
安来市病院事業管理者
安来市教育委員会
安来市選挙管理委員会
安来市公平委員会
安来市監査委員
安来市農業委員会
安来市固定資産評価審査委員会

１　目的

安来市（以下「本市」という。）の各情報システムが取り扱う情報には、住民の個人情報のみならず行政運営上重要な情報など、漏えいや改ざん等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、住民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠であり、ひいては、このことが本市に対する住民からの信頼の獲得・維持・向上に寄与するものである。

そのため、本市の情報資産の機密性（情報にアクセスすることが認可された者だけがアクセスできることを確実にすること）、完全性（情報及び処理方法の正確さ及び完全である状態を安全防護すること）及び可用性（許可された利用者が必要なときに情報にアクセスできることを確実にすること）を維持するための対策を整備するため、地方自治法の一部を改正する法律（令和６年法律第６５号）の施行に伴い、総務省が策定した「地方公共団体におけるサイバーセキュリティを確保するための方針又は変更に関する指針」を踏まえて、本市のサイバーセキュリティを確保するための方針（以下「基本方針」という。）として定めるものである。

２　定義

この基本方針の用語の意義は、それぞれ次に定めるとおりとする。

（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）情報資産

次に掲げるものをいう。

ア　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

イ　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。）

ウ　情報システムの仕様書、ネットワーク図等のシステム関連文書

（４）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。

（５）機密性

情報にアクセスすることが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、必要な時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、地方税又は防災に関する事務をいう。以下同じ。）又は戸籍事務等に係る情報システム及びデータをいう。

（９）ＬＧＷＡＮ接続系

財務会計、文書管理その他の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。

（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係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）通信経路の分離

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うえで、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ィ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。

（１３）業務委託

本市の情報を取り扱い、本市の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。

（１４）職員等

本市が所掌する情報資産を取り扱う全職員、臨時・非常勤職員等

３　適用範囲

本基本方針が適用される機関は、安来市情報公開条例（平成１６年安来市条例第８号）第２条第１号に規定する実施機関とする。ただし、本市の情報資産を利用する場合に限る。

４　情報セキュリティポリシーの位置付けと職員等及び委託事業者の義務

情報セキュリティポリシーは、本市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

したがって、本市が保有する情報資産に接する職員等及び委託事業者は、情報

セキュリティの重要性を認識し、業務の遂行に当たって本基本方針及び各機関に適用される情報セキュリティポリシーを遵守する義務を負うものとする。

5　情報資産への脅威

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。

（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

（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

6　情報セキュリティ対策

情報資産を脅威から保護するため、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。

（２）情報資産の分類と管理

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。

（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じる。

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により、住民情報の流出を防ぐ。

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離する。なお、両システム間で通信する場合には無害化通信を行う。

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高度な情報セキュリティ対策を行う。高度な情報セキュリティ対策として、都道府県と市町村のインターネット接続口を集約したうえで自治体情報セキュリティクラウドの導入等を行う。

（４）物理的セキュリティ

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

（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じる。

（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、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、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、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。

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、リスクを検討した上で、

情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

情報セキュリティ対策を講じるに当たっては、具体的な遵守事項及び判断基準等を統一的なレベルで定める必要があるため、職員等及び委託事業者が遵守すべき事項及び判断等の基準となる基本的要件を明記した情報セキュリティ対策基準を策定する。

なお、情報セキュリティ対策基準は、公開することにより本市の行政運営に支障を及ぼす恐れがあることから非公開とする。

１０　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、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等を策定するものとする。

なお、情報セキュリティ実施手順は、公開することにより本市の行政運営に支障を及ぼす恐れがあることから非公開とする。

附　則

この基本方針は、令和８年４月１日から施行する。