情報セキュリティ基本方針

１．目的

真庭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。さらに、αモデルからβ´モデルへの転換により、クラウドサービスの利用を前提としたインターネット接続系のセキュリティを強化していくとともに、総務省が示す『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』に基づいたセキュリティ対策を実施するため、『情報セキュリティ基本方針』および『情報セキュリティ対策基準』を改定する。情報セキュリティが個人の裁量によって左右されることが無いよう、すべての職員は、情報セキュリティの重要性をよく理解し、情報セキュリティに対する意識レベルを共有し、例外なく『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．定義

（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）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

本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。

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。

（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

4．適用範囲

（1）行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

（2）情報資産の範囲

本基本方針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．職員の責務

職員（任期付職員、会計年度任用職員、非常勤職員等も含む）は、情報セキュリティの重要性をよく理解し、情報セキュリティポリシーを遵守し、業務を遂行するものとする。遵守にあたっては例外や個人の裁量による行動があってはならない。

6．情報セキュリティマネジメントの体制

真庭市の情報セキュリティ対策を統括し、管理策の実施、教育訓練等を推進する者として、最高情報セキュリティ責任者（CISO）を定める。

また、真庭市の情報セキュリティを維持していくために、情報管理者会により、全庁的なマネジメント体制を整えるものとする。

7．情報資産の分類・管理

真庭市が保有する情報資産について、機密性・完全性・可用性の重要度について分類し、リスクの大きさと照らし合わせて必要十分のセキュリティ対策を行うものとする。

8．情報セキュリティ管理策

真庭市が保有する情報資産をセキュリティ上の脅威から保護するため、以下の情報

セキュリティ対策を講ずる。

（１）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。

①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。

②LGWAN 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。なお、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。

③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。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。

（２）物理的セキュリティ

サーバ室及び、事務所等、重要な情報資産を保管する場所について、不正な立ち入りや盗難・破壊等から保護するため、入退室や機器管理における物理的な対策を講じる。

（３）人的セキュリティ

情報セキュリティポリシーにおいて、情報資産を取扱う職員の情報セキュリティに関する権限と責任を明確にし、全ての職員がこれに反することがないよう、教育・訓練を行う。

（４）技術的セキュリティ

情報資産を不正アクセスやウイルスによる破壊・漏洩から守るために技術的対策を講ずる。

（５）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。

（6）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。

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。

９．評価・見直し

情報セキュリティ対策は構築した時点では十分であっても、情報資産の価値の変化や、新たなセキュリティ脅威の出現などにより不十分なものとなってしまうことがある。情報セキュリティ環境の変化に対応するため定期的に情報セキュリティ対策基準の評価・見直しを行うこととする。

また、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。

１０．情報セキュリティ対策基準の策定

上記８、９に規定する対策等を実施するために、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を策定する。

１１．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。

以上、真庭市の全職員は、市民情報をはじめとする情報資産の重みをしっかり受け止め、情報セキュリティポリシーを遵守し、市民に対して継続的に安全・安心で、信頼される行政サービスの提供に努めなければならない。

平成１７年　９月　１日

真庭市長

（履歴）

年月日	場所	内容
平成１７年　９月　　１日　策定	－	新規策定
令和　４年　４月　　１日　改定	－	情報セキュリティポリシーの見直しにより改定
令和　８年　４月　　１日　改定	－	「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」の改定と β’モデルへの移行により改定