制定:平成16年 4月 1日
改正:令和 8年 4月 1日

王寺町情報セキュリティ基本方針

目 次

1　目的

本基本方針は、本町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、本町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。

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（基幹系）

マイナンバー利用事務（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

人事給与、財務会計及び文書管理等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。

（１３）その他の用語

【か】「外部委託事業者」

システム開発職務等を委託する外部の民間機関等の総称をいう。

「ゲートウェイ」

異なるネットワーク同士を接続するネットワーク機器の事です。 単語本来の「玄関」という意味の通り、他のネットワークと通信する際に必ず通らなければいけない「接続ポイント」であると言えます。 ゲートウェイはプロトコル（通信のルール・規格）を変換し、異なるプロトコルを用いたネットワークを繋げる役割があります。

「脅威」

自然の脅威（地震、火災、風水害等）、情報システムの脅威（情報システムの故障、誤動作等）及び人的な脅威（不正行為、誤操作等）をいう。

【さ】「情報」

職務の遂行に伴ってコンピュータ及び記録媒体に記録されたデータ並びに記録されたデータが処理され出力されたもの全てをいう。

「情報システム」

コンピュータシステム（ハードウェア、ソフトウェア、ネットワーク及び記録媒体）をいう。

「情報資産」

情報及び情報システムをいう。

項	情報資産の種類	情報資産の例
A	ネットワーク	通信回線、ルータ等の通信機器
B	情報システム	サーバ、パソコン、オペレーティングシステム、ソフトウェア等
C	これらに関する施設・設備	情報管理室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
D	電磁的記録媒体	CD-R、DVD-R、フロッピーディスク、MO、USB フラッシュメモリ、SD カード、デジタルカメラ等
E	ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱う情報（全ての文書と電磁的データを含む。）
F	システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

「情報セキュリティポリシー」

基本方針及び情報セキュリティ対策基準をいう。

「情報セキュリティ対策」

情報セキュリティを維持するための管理策をいう。

「職員」

地方公務員法で規定された特別職、一般職の中で町に勤務する者の総称をいう。

「職員等」
　職員、会計年度任用職員及び派遣職員をいう。

「情報セキュリティインシデント」
　「情報セキュリティインシデント」とは、望まない単独若しくは一連の情報セキュリティ事象又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

「冗長化」
　システムの一部に何らかの障害が発生した場合に備えて、障害発生後でもシステム全体の機能を維持し続けられるように予備装置を平常時からバックアップとして配置し運用しておくこと。 冗長化によって得られる安全性は冗長性と呼ばれます。

「ソーシャルメディアサービス」
　「ソーシャルメディアサービス」とは、インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったWeb サイトやネットサービスなどを総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。

「情報機器」
　「情報機器」とは、情報システムの構成要素である機器のうち、職員が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りが無い限り、本町が調達するものをいう。

「セキュリティホール」
　コンピュータのＯＳやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを言います。 セキュリティホールが残された状態でコンピュータを利用していると、ハッキングに利用されたり、ウイルスに感染したりする危険性があります。

【た】「多要素認証」
　「多要素認証」とは、システムが正規の利用者かどうかを判断する際の信頼性を高めるために、複数の認証手段を組み合わせて認証する方式をいう。認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。それぞれの認証手段には各々異なった利点と欠点があり、複数の認証方式を組み合わせることが利用者認証の信頼性を高める意味でも有効である。

「庁内ネットワーク」
　「庁内ネットワーク」とは、地方公共団体の庁舎・出先機関を含めた団体が管理主体となるネットワーク及び同ネットワークを外部委託データセンターに設置している情報システムをいう。

「ディレクトリ」
　エクスプローラのフォルダに相当するものです。 コンピュータの記憶メディア

（ハードディスクなどファイルシステム）のファイルを整理・管理するための、階層構造（ツリー構造）を持つグループ名。初心者向けの解説書などではファイルの入れ物（容器）などと表現されることもあります。

【な】「ネットワークストレージサービス」
　ネットワーク（オンライン）ストレージサービスとは、インターネット上で、データやファイルを格納するディスクスペースを提供するサービスのこと。
　例えば、Dropbox、Googleドライブ、マイクロソフトOne Drive、Yahoo!ボックス、Sugar Sync等が挙げられます。

【は】「汎用受付システム」
　一つのポータルサイト上で、住民や企業がインターネットを通して提出する各種電子申請届出の受付や、行政機関からの結果通知など複数の手続きができるシステムのことを汎用受付システムと言います。この汎用受付システムは総務省により仕様が策定され、各省庁の電子申請システムに採用されています。また、統一された仕様で構築されていることから、複数の自治体が共同でシステムを構築/利用することが可能になり、経費削減や早期の電子申請実現に寄与すると期待されている。

「パッチ」
　コンピュータにおいてプログラムの一部分を更新してバグ修正や機能変更を行なうためのデータのこと。「修正プログラム」や「アップデート（プログラム)」などとも呼ばれます。実際に変更を施す際は「パッチを当てる」、「パッチを適用する」と言います。

「標的型攻撃」
　「標的型攻撃」とは、明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種です。

「フィルタリング」
　インターネット利用における情報閲覧の制限や受発信を制限することを言います。企業や地方自治体でもＷｅｂから生じる情報漏えいを防ぎ、業務効率を向上させるために閲覧できるサイトにフィルタをかけることが出来ます。フィルタリングを導入することで、インターネットを使える時間の制限や見せたい、見てもいい、見たくないページのコントロールをユーザー指定し設定できます。

【や】「約款による外部サービス」
　「約款による外部サービス」とは、民間事業者等の庁外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものを言います。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。

【ら】「ルーティング」
　ルーティングあるいは経路制御（けいろせいぎょ）とは、データを目的地まで送信するために、コンピュータネットワーク上のデータ配送経路を決定する制御の事を言います。宛先となるホストまでパケットを送信する時に最適な経路を選択して転送することです。 このルーティングは、ルータやL3スイッチなどのレイヤ3で動作す

るネットワーク機器によって行われます。

【Ａ～Ｚ】

「CSIRT（Computer Security Incident Response Team)」

「CSIRT」とは、コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行ったりする組織の総称。

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、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、町長部局、教育委員会、選挙管理委員会、農業委員会、固定資産評価審査委員会、水道事業管理者及び議会事務局とする。

（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　職員等の遵守義務

職員、会計年度任用職員等（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、業務の遂行に当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。

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。

（１）組織体制

本町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

本町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。

（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。

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。

（４）物理的セキュリティ

サーバ、情報管理室、通信回線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。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。

（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。

（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になった場合には、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。

9　情報セキュリティ対策基準の策定

上記6、7及び8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。

なお、情報セキュリティ対策基準は、公にすることにより本町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。

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町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。