越谷・松伏水道企業団情報セキュリティ基本方針

１．趣旨

基本方針は、越谷・松伏水道企業団情報セキュリティポリシー（以下「セキュリティポリシー」という。）の最上位に位置し、情報セキュリティに関する統一的かつ基本的な方針として、企業団における情報セキュリティ対策に対する根本的な考え方及び取組姿勢を示すものである。

２．定義

セキュリティポリシーにおいて使用する用語を以下のとおり定義する。

（１）情報セキュリティ

情報資産の機密性、完全性、可用性を維持すること

（２）情報セキュリティポリシー

情報資産を活用するに当たって、セキュリティ上保護すべき対象範囲と、対策や管理運営等についての方針を明文化したもの

（３）情報システム

ハードウェア、ソフトウェア、ネットワーク、記録媒体等で構成されるものであって、これら全体で業務処理を行うもの

（４）情報資産

紙、電磁媒体、フィルム等の記録媒体に記録されたすべての情報、情報システム及びこれらに関する設備の総称

（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．対象範囲

　セキュリティポリシーの対象範囲は、次のとおりとする。
（１）組織の範囲
　企業団の情報資産を利用する全ての組織及び団体（以下「対象組織」という。）なお、別途最高情報セキュリティ責任者が認めた個別の規程で定める範囲を除く。
（２）人の範囲
　対象組織の職員及び当該組織の業務に携わる全ての者（以下「職員等」という。）
（３）情報資産の範囲
　対象組織で保有する企業団の情報資産

５．職員等の責務

職員等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セキュリティポリシー及び情報セキュリティ共通実施手順等の関連規程をすべて遵守しなければならない。

６．情報セキュリティ対策の実施

３に規定する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）情報セキュリティ管理体制の整備

局長を最高情報セキュリティ責任者（以下「ＣＩＳＯ」という。）とし、ＣＩＳＯのもとに情報セキュリティを確実にする管理体制を整備し、管理責任の所在を明確にする。

（２）情報資産の明確化及び分類

情報セキュリティ対策を確実及び有効にするために、情報資産を明らかにし､かつ機密性・完全性・可用性別に分類する。

（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。

② 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。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。

（４）人的セキュリティ対策

情報セキュリティに関する権限と責任を定めるとともに、職員等にセキュリティポリシーの内容を周知徹底するなど、十分な教育及び啓発を行うための必要な対策を講じる。

（５）物理的セキュリティ対策

情報システムを設置する場所への不正な立ち入り、情報資産への危害及び妨害等から保護するために物理的な対策を講じる。

（６）技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理、コンピュータウイルス対策等の技術的な対策を講じる。

（７）運用に関するセキュリティ対策

情報システムの監視及びセキュリティポリシー遵守状況の確認、業務委託を行う際のセキュリティ確保等の運用面における必要な対策を行うとともに、緊急事態が発生した際に迅速な対応を行うための危機管理対策を講じる。

（８）業務委託と外部サービス（クラウドサービス）の利用

① 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。

② 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。

③ 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

セキュリティポリシーの遵守及び運用の状況を検証するため、定期的又は必要に応じて監査及び自己点検を実施する。

８．評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果等に基づき、情報セキュリティ対策の評価を行うとともに、情報システムの変更、新たな脅威の発生など情報セキュリティを取り巻く状況の変化に対応するために、セキュリティポリシー及び情報セキュリティ共通実施手順等の関連規程の見直しを適宜実施する。

９．情報セキュリティ対策関連規程の整備

情報セキュリティ対策を講じるに当たり遵守すべき事項を体系的かつ効果的に管理するため、以下に示す規程を整備する。なお、情報セキュリティ共通実施手順等の関連規程は、公にすることにより企業団の事業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。

（１）情報セキュリティ対策基準

基本方針に基づき、情報セキュリティの有効性を継続的に維持するための運営･管理体制及び情報セキュリティを確保するために遵守すべき行為及び判断等の基準を示すもの。

（２）情報セキュリティ共通実施手順等の関連規程

情報セキュリティ対策基準に基づき、具体的な業務においてどのような手順に従って実行していくかを示すもの。

10. 違反に対する対応

セキュリティポリシーに違反した者に対しては、その重大性に応じて地方公務員法その他関係法令に基づく厳正な対応を行う。

11. 委任

この方針に定めるもののほか必要な事項は、別に定める。