南予水道企業団

情報セキュリティポリシー（基本方針）

令和８年３月

１目的

情報セキュリティポリシー（基本方針）は、南予水道企業団（以下「企業団」という。）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、企業団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

⑴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。

⑵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。

⑶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。

⑷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。

⑸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。

⑹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。

⑺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。

⑻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。

⑼LGWAN 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を除く。）。

⑽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。

⑾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。

⑿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
　情報セキュリティに対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。
⑴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
⑵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
⑶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
⑷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
⑸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
⑴行政機関の範囲
　本基本方針が適用される行政機関は、企業団（議会担当、監査担当含む）とする。
⑵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　①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
　職員等は、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、次の情報セキュリティ対策を講じる。
⑴組織体制
　企業団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。
⑵情報資産の分類と管理

企業団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、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、情報セキュリティ対策を実施する。

⑷物理的セキュリティ

サーバ、情報システム室、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。

⑸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。

⑹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。

⑺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。

⑻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。また、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。加えて、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。

⑼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。また、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、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企業団の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企業団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。