大阪広域環境施設組合情報セキュリティ基本方針

令和８年３月31日達第２号

目　次

第１章　総則

（目的）

第１条　この基本方針は、大阪広域環境施設組合通信ネットワークシステム等の運用等に関する規程（令和８年達第１号。以下「通信ネットワークシステム等運用等規程」という。）第２条第１号及び第２号に規定する通信ネットワークシステム、情報システム、通信ネットワークシステム及び情報システムにより伝達又は処理される情報、並びにその他の本組合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、本組合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。

（定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

⑴　情報セキュリティ　情報資産の機密を保持し、情報資産の正確性及び完全性を維持し、並びに定められた範囲での利用可能な状態を維持することをいう。

⑵　情報資産　通信ネットワークシステム及び情報システムの開発及び運用管理に係るファイル（データを記録している電磁的記録をいう。以下同じ。）及びドキュメント（情報システムの設計書、操作手引書、プログラ

ムリスト、ネットワーク構成図その他の電子計算機の運用に関する文書をいう。）、通信ネットワークシステム及び情報システムで取り扱うデータに係るファイル、並びに通信ネットワークシステム及び情報システムを構成する機器をいう。

⑶　情報セキュリティポリシー　この基本方針及び第16条に規定する情報セキュリティ対策基準をいう。

⑷　情報セキュリティ対策　情報セキュリティを確保するために実施する各種の対策をいう。

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　電子計算機処理　電子計算機を使用して行われる情報の入力、蓄積、編集、加工、修正、更新、検索、消去、出力又はこれらに類する処理をいう。

⑼　電磁的記録　電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。

⑽　データ　電子計算機処理に係る情報で媒体に記録されているものをいう。

⑾　課　大阪広域環境施設組合公文書管理条例施行規則（平成26年規則第６号）第７条第４項に規定する課（工場を含む。）をいう。

（対象とする脅威）

第３条　情報資産に対する脅威を以下のとおり想定し、情報セキュリティ対策を実施する。

⑴　不正アクセス、ウイルス及び標的型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、外部委託管理の不備、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、火災等の災害等

⑷　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

⑸　大規模、広範囲にわたる疾病による要員不足に伴う情報システム運用の機能不全等

（適用範囲）

第４条　この基本方針の適用範囲は、本組合の執行機関（監査委員及び公平委員会を含む。）及び議決機関が保有する全ての情報資産とする。

（職員の責務）

第５条　職員は、情報セキュリティの重要性を十分に認識し、情報セキュリティポリシー（以下「ポリシー」という。）を遵守するとともに、大阪広域環境施設組合個人情報の保護に関する法律の施行等に関する条例（令和５年条例第３号）その他の関連する法令等を遵守し、情報資産を適切に管理しなければならない。

第２章　情報セキュリティに係る体制

（統括情報セキュリティ責任者等の設置等）

第６条　本組合に統括情報セキュリティ責任者を置き、事務局長をもって充てる。

２　統括情報セキュリティ責任者は、本組合における情報セキュリティを統括し、情報セキュリティ対策の統一的な実施に必要な指導、助言又は調整を行う。

３　ＩＴ管理者（通信ネットワークシステム等運用等規程第４条第１項に規定

するＩＴ管理者をいう。）は、統括情報セキュリティ責任者の命を受けて、本組合における通信ネットワークシステムの利用状況等、各情報システムの利用状況等、データの管理状況等を把握し、情報セキュリティ対策が適切かつ確実に実施されるよう必要な助言又は調整を行う。

（課情報セキュリティ責任者の設置等）

第７条　課における情報セキュリティ対策の適正な実施を推進するため、課に課情報セキュリティ責任者を置く。

２　課情報セキュリティ責任者は、課の所属長をもって充てる。

３　課情報セキュリティ責任者は、統括情報セキュリティ責任者の命を受けて、その所管に係る情報資産に関し情報セキュリティ対策が適切かつ確実に実施されるよう、必要な措置を講じなければならない。

第３章　情報セキュリティ対策

（体制及び役割）

第８条　本組合の情報資産について、体制及び役割に基づき情報セキュリティ対策を行う。

（情報資産の分類と管理）

第９条　本組合の情報資産を機密性、完全性及び可用性を踏まえ重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（物理的セキュリティ）

第10条　情報資産の管理について、物理的な対策を講じる。

（人的セキュリティ）

第11条　職員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。

（技術的セキュリティ）

第12条　情報資産の管理、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な対策を講じる。

（運用）

第13条　通信ネットワーク及び情報システムの監視、ポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、ポリシーの運用面の対策を講じる。

（業務委託とクラウドサービスの利用）

第14条　業務委託を行う場合には、委託事業者の選定に際し、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情報セキュリティ対策が確保されていることを確認するとともに、必要に応じ契約に基づいた措置を講じる。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、必要な対策を講じる。

（評価及び見直し）

第15条　情報セキュリティ対策に関する点検及び評価を適宜実施し、必要に応じ運用改善及びポリシーの見直しを行う。

（情報セキュリティ対策基準の作成）

第16条　統括情報セキュリティ責任者は、本組合における情報資産の取扱いについて遵守すべき事項及び情報セキュリティ対策の実施に関する統一的な規準を定めるため、情報セキュリティ対策基準を作成しなければならない。

（情報セキュリティ実施手順の作成）

第17条　課情報セキュリティ責任者は、その所管する通信ネットワークシステム及び情報システムにおける情報セキュリティ対策の実施に関し必要となる事項を定めるため、情報セキュリティ実施手順を作成し統括情報セキュリティ責任者の承認を得なければならない。

第４章　検証及び見直し

（情報セキュリティ検査の実施）

第18条　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検査を実施する。

（見直しの実施）

第19条　統括情報セキュリティ責任者は、情報セキュリティをめぐる情勢の動

向、変化等を勘案し、及び情報セキュリティ検査の結果を踏まえ、適宜ポリシーに検討を加え、必要があると認めるときは、これを変更しなければならない。

２　課情報セキュリティ責任者は、前項の規定に準じて、情報セキュリティ実施手順に検討を加え、必要があると認めるときは、これを変更しなければならない。

第５章　雑則

（施行の細目）

第20条　この基本方針の施行に関し必要な事項は、統括情報セキュリティ責任者が定める。

附　則

１　この基本方針は、令和８年４月１日から施行する。

２　大阪広域環境施設組合情報セキュリティ管理規程（平成27年達第３号）は、廃止する。