岡山県広域水道企業団情報セキュリティ基本方針

1　目的

本基本方針は、岡山県広域水道企業団（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の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) 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。

(9) 通信経路の分割

事務系システム及び制御系システムの各環境間の通信環境を物理的又は論理的に分離した上で、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。

(10) 無害化通信

分離された各システム間において、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。

(11) 事務系システム

水道事業の運営に必要不可欠な業務処理を行う情報システムをいう。

(12) 制御系システム

浄水場、配水施設等の水道施設の監視・制御を行う情報システムであって、事務系システム及びインターネット接続系から分離された情報システムをいう。

(13) 重要インフラサービス

構成団体の水道事業運営に必要不可欠な水道用水の供給サービスをいう。

(14)サプライチェーン

水道事業における業務委託事業者、保守事業者、資機材供給事業者、ソフトウェア事業者、クラウドサービス事業者その他の関係者及びこれらの者が運営する情報システムの連鎖をいう。

(15) 構成団体

企業団を組織する別表に掲げる地方公共団体をいう。

(16) 事業継続

災害やサイバー攻撃等の脅威が発生した場合においても、構成団体への水道用水供給を継続し、又は早期に復旧させることをいう。

(17) 重要情報

企業団が保有する機密性の高い情報であって、漏えい等により水道事業の運営に重大な影響を与えるおそれがある情報をいう。

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、通信の途絶等のインフラの障害からの波及等

(6) サプライチェーンを構成する関係者の情報システムへの攻撃や情報セキュリティ事故等による連鎖的な影響及び企業団への波及、関係者を踏み台とした企業団への攻撃等

(7) 分離されたシステム間の不正な通信や、分離機能の迂回・無効化による情報漏えいや不正アクセス等

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、企業団事務局、企業団監査事務局、企業団議会事務局とする。

(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。

ア　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

イ　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。）

ウ　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、臨時・非常勤職員等（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

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体的な組織体制を確立する。

(2) 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・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

ア　事務系システム及び制御系システムの通信経路を分割する。なお、各システム間で通信する場合には、無害化通信を実施する。

イ　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対策を実施する。

ウ　事務系システム及び制御系システムにおいては、水道事業の継続性及び水道施設の安全な運用を確保するため、必要なセキュリティ対策を実

施する。

(4) 物理的セキュリティ

コンピュータ室、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。

(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、利用に係る規定を整備し対策を講じる。

(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。

(10) 構成団体との連携

企業団は、セキュリティインシデント発生時における迅速な情報共有及び水道用水供給の継続を図るため、構成団体との連携体制を整備する。

(11) 経営層の責務

管理者等（以下「経営層」という。）は、重要インフラ事業者として、サイバーセキュリティ確保に関する責任を負い、必要な措置を講じる。

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。

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。

別表

岡山県　岡山市　倉敷市　津山市　井原市　総社市　高梁市　備前市　瀬戸内市　赤磐市　真庭市　和気町　鏡野町　勝央町　奈義町　久米南町　美咲町　吉備中央町