

海 部 南 部 水 道 企 業 団
情 報 セ キ ュ リ テ ィ ポ リ シ ー
(情 報 セ キ ュ リ テ ィ 基 本 方 針)

令 和 8 年 4 月

海 部 南 部 水 道 企 業 団
海 部 南 部 水 道 企 業 団 議 会
海 部 南 部 水 道 企 業 団 監 査 委 員

海部南部水道企業団情報セキュリティ基本方針

目 次

第1章 海部南部水道企業団情報セキュリティポリシーの位置づけと構成	
1. はじめに	1
2. 海部南部水道企業団情報セキュリティポリシーの位置づけと構成	1
第2章 情報セキュリティ基本方針	
1. 目的	2
2. 定義	2
3. 対象とする脅威	3
4. 適用範囲	3
5. 職員等の順守義務	4
6. 情報セキュリティ対策	4
7. 情報セキュリティ監査及び自己点検の実施	5
8. 情報セキュリティポリシーの見直し	5
9. 情報セキュリティ対策基準の策定	5
10. 情報セキュリティ実施手順の策定	5

改定履歴

年 月 日	内 容
令和5年4月1日	当初制定
令和8年4月1日	全部改正（企業団・議会・監査委員による共同策定）

<第1章 海部南部水道企業団情報セキュリティポリシーの位置づけと構成>

1. はじめに

海部南部水道企業団企業長、海部南部水道企業団議会及び海部南部水道企業団監査委員は、地方自治法（昭和22年法律第67号）第244条の6第1項に規定するサイバーセキュリティを確保するための方針として、「海部南部水道企業団情報セキュリティポリシー（情報セキュリティ基本方針）」を共同で定めるものである。

2. 海部南部水道企業団情報セキュリティポリシーの位置づけと構成

海部南部水道企業団情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは海部南部水道企業団企業長、海部南部水道企業団議会及び海部南部水道企業団監査委員が保有する情報資産（以下「情報資産」という。）に関する情報セキュリティ対策について、国のガイドラインに基づいて総合的、体系的かつ具体的に取りまとめたものであり、海部南部水道企業団企業長、海部南部水道企業団議会及び海部南部水道企業団監査委員の実施する情報セキュリティ対策の最高位に位置するものである。

情報セキュリティポリシーは、情報資産を取り扱う全ての者に浸透、定着させるものであり、安定的な規範であることが要請される。しかし一方では、情報セキュリティ対策は、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に、柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適正に対応する部分としての「情報セキュリティ対策基準」の2階層から成るものとして策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎に、具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定することとする。

<第2章 情報セキュリティ基本方針>

1. 目的

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。

一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

さらに、昨今、国・地方公共団体・民間企業・住民の間のネットワークを通じた相互接続がますます進展していることに伴い、一つの地方公共団体の情報セキュリティ対策の不備や不適切なシステム利用が、他の地方公共団体や国の機関等の情報セキュリティにも脅威となり、その安全性や信頼性に影響を与える蓋然性が高くなっている。

海部南部水道企業団（以下「企業団」という。）においても、住民の個人情報や行政運営上重要な情報などを多数取り扱っている。また、多くの業務が情報システムやネットワークに依存している。このため、これらの情報資産を様々な脅威から防御することは、住民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも 必要不可欠である。

これらのことを踏まえ、他に定めがあるものを除き、企業団が実施する情報セキュリティ対策についての基本的な事項を定めるための基本方針として、企業団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ことを目的に情報セキュリティ基本方針（以下「基本方針」という。）を定める。

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、情報にアクセスすることが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

インターネット接続系とそれ以外の情報システム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。

(10) 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

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、海部南部水道企業団企業長、海部南部水道企業団議会及び海部南部水道企業団監査委員とする。

(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

企業団に勤務する全ての職員（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庁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靱性の向上

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、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) 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。

(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な対策を講じる。

(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

業務委託する場合には、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。

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。

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。