

福岡地区水道企業団情報セキュリティに関する基準

1 目的

この基準は、福岡地区水道企業団（以下「企業団」という。）が所管する情報資産の保護及び管理に関する基本的事項を定め、住民及び構成団体（以下「住民等」という。）の財産、プライバシー等を保護するとともに、企業団の適正な運営の確保に資することを目的とする。

2 定義

この規則において、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。

(1) 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、並びに情報資産を定められた範囲で利用可能な状態で維持することをいう。

(2) 情報資産

ネットワーク及び情報システム、これらに関する設備、これらで取り扱う情報、これらを印刷した文書、電磁的記録媒体並びにシステム構成図等の関連する文書をいう。

(3) 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並びにその構成機器であるハードウェア及びソフトウェアをいう。

(4) 情報システム

コンピュータ、ネットワーク、電磁的記録媒体等で構成され、情報処理を行う仕組みをいう。

(5) 部等

福岡地区水道企業団事務分掌規程（昭和 48 年福企管理規程第 8 号）第 2 条に規定する部及び監査委員並びに議会をいう。

(6) 職員

地方公務員法（昭和 25 年法律第 261 号）第 3 条第 2 項に規定する一般職に属する職員及び同 3 項に規定する特別職に属する職員をいう。

(7) 脅威

情報資産に何らかの障害又は影響を与える原因となるものをいう。

(8) 企業団ネットワーク

企業団内のサーバ、パソコン、プリンタ等の機器を相互に接続し、情報の高度利用等を行うためのネットワークをいう。

3 適用範囲

この基準は、企業団が所管する情報資産を利用する全ての職員（以下「職員」という。）に適用する。

4 職員の責務

(1) 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は、この基準を遵守しなければならない。

(2) 職員等は、情報資産の取扱いに当たっては、次に掲げる法令を遵守しなければならない。

① 著作権法（昭和 45 年法律第 48 号）

② 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

- ③ 個人情報の保護に関する法律(平成 15 年法律第 57 号)
- ④ 福岡地区水道企業団個人情報の保護に関する法律施行条例(令和 5 年福企条例第 2 号)
- ⑤ 福岡地区水道企業団議会の個人情報の保護に関する条例(令和 5 年福企条例第 4 号)

5 対象とする脅威

次に掲げる脅威を想定し、脅威から情報資産を保護するための情報セキュリティに関する対策（以下「情報セキュリティ対策」という。）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、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、改ざん又は消去、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又は設計若しくは開発の不備、プログラム上の欠陥、操作若しくは設定ミス、メンテナンス不備、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) 大規模かつ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

6 情報セキュリティ対策

情報セキュリティ対策は、次に掲げるとおりとする。

- (1) 災害、事故等に対する物理的セキュリティ対策
- (2) 情報資産の無断持ち出し、操作ミス等に対する人的セキュリティ対策
- (3) 不正アクセス、データ改ざん等に対する技術的セキュリティ対策
- (4) 情報システム全体の強靱性を向上させる抜本的セキュリティ対策

7 管理体制

情報セキュリティを確保するため、次の各号に掲げる職を置き、当該各号に定める職にある者をもって充てる。

- (1) 情報セキュリティ最高責任者 副企業長
- (2) 情報セキュリティ統括管理者 総務部長
- (3) 情報セキュリティ副統括管理者 総務課長
- (4) 情報セキュリティ管理者 部等の長（監査委員及び議会にあっては、その事務局の長）
- (5) ネットワーク責任者 ネットワークを所管する課（課に相当する組織を含む。以下同じ。）の長
- (6) 情報システム責任者 情報システムを所管する課の長
- (7) 情報セキュリティ責任者 課の長

8 情報セキュリティ最高責任者

情報セキュリティ最高責任者は、情報セキュリティ対策に関する最終決定権限及び責任を有する。

9 情報セキュリティ統括管理者

- (1) 情報セキュリティ統括管理者は、情報セキュリティ対策全般について統括管理する。
- (2) 情報セキュリティ統括管理者は、情報セキュリティ最高責任者を補佐し、情報セキュリティ最高責任者が欠けたときは、その職務を代理する。

10 情報セキュリティ副統括管理者

情報セキュリティ副統括管理者は、情報セキュリティ統括管理者を補佐し、情報セキュリティ統括管理者が欠けたときは、その職務を代理する。

11 情報セキュリティ管理者

情報セキュリティ副統括管理者は、情報セキュリティ統括管理者を補佐し、情報セキュリティ統括管理者が欠けたときは、その職務を代理する。

(1) 情報セキュリティ管理者は、所管する部等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

(2) 情報セキュリティ管理者は、所管する部等の職員等に対して情報セキュリティに関する教育、訓練、助言及び指示を行う。

12 ネットワーク責任者

(1) ネットワーク責任者は、所管するネットワークの敷設、設定の変更、運用及び見直し（以下「敷設等」という。）並びに当該ネットワークの情報セキュリティ対策に関する権限及び責任を有する。

(2) ネットワーク責任者は、所管するネットワークの敷設等に携わる職員等並びに当該ネットワークを利用する所属の情報システム責任者及び情報セキュリティ責任者を指導し、及び監督する。

13 情報システム責任者

(1) 情報システム責任者は、所管する情報システムの開発、設定の変更、運用及び見直し（以下「開発等」という。）並びに当該情報システムの情報セキュリティ対策に関する権限及び責任を有する。

(2) 情報システム責任者は、所管する情報システムの開発等に携わる職員等及び当該情報システムを利用する所属の情報セキュリティ責任者を指導し、及び監督する。

14 情報セキュリティ責任者

(1) 情報セキュリティ責任者は、所管する課の情報セキュリティ対策に関する権限及び責任を有する。

(2) 情報セキュリティ責任者は、所管する情報資産の利用について、所属の職員等を指導し、及び監督する。

15 共通実施手順の策定

情報セキュリティ最高責任者は、企業団共通で行うべき情報セキュリティ対策の詳細を定めた情報セキュリティ共通実施手順（以下「共通実施手順」という。）を策定しなければならない。

16 情報資産の管理

(1) 情報セキュリティ管理者は、所管する部等の情報資産について、この基準及び共通実施手順に従い適正な管理を行うよう、当該部等の職員等を指導し、及び監督しなければならない。

(2) ネットワーク責任者、情報システム責任者及び情報セキュリティ責任者は、共通実施手順に従い所管する情報資産に応じた当該情報資産の管理の具体的な方法を定め、当該方法に従い、情報セキュリティ対策を実施しなければならない。

17 情報資産の利用

- (1) 職員等は、業務以外の目的で情報資産を利用してはならない。
- (2) 職員等は、情報資産を利用する場合には、共通実施手順に従い、適正に取り扱わなければならない。

18 職員への周知等

情報セキュリティ最高責任者は、情報資産を取り扱う全ての職員等を対象とした情報の提供や研修を実施し、情報セキュリティの重要性について周知し、及び啓発しなければならない。

19 情報セキュリティ監査

情報セキュリティ最高責任者は、情報セキュリティ対策の実施状況を検証するため、情報セキュリティに関する監査を実施しなければならない。

20 侵害への対応

- (1) 情報セキュリティ最高責任者は、情報セキュリティに関する事故、障害及び違反行為による情報資産への侵害（以下「侵害」という。）が発生し、又はそのおそれがある場合の対応を定めた手順を策定しなければならない。
- (2) ネットワーク責任者及び情報システム責任者は、侵害が発生し、又はそのおそれがある場合の対応を定めた具体的な手順を策定しなければならない。

21 委任

この基準に定めるもののほか、この基準に関し必要な事項は、情報セキュリティ最高責任者が定める。

附則

この基準は、令和3年4月1日から適用する。

附則

この基準は、令和8年4月1日から適用する。