大船渡地区環境衛生組合
大船渡地区環境衛生組合議会
大船渡地区環境衛生組合監査委員
情報セキュリティ基本方針

令和８年３月 31 日

大船渡地区環境衛生組合

大船渡地区環境衛生組合議会

大船渡地区環境衛生組合監査委員

情報セキュリティ基本方針

１　目的

大船渡地区環境衛生組合（以下「組合」という。）、大船渡地区環境衛生組合議会（以下「議会」という。）、大船渡地区環境衛生組合監査委員（以下「監査委員」という。）の情報システムが取り扱う情報資産には、個人情報や行政運営上重要な情報など、外部に漏えいした場合、重大な結果を招く情報が含まれている。

情報システムは、業務の効率化を図るため、行政運営基盤として欠かせないものとなっており、業務執行を今後も円滑に進めるためには、情報システムが安全性を有することが不可欠である。

このことから、組合、議会、監査委員（以下「組合関係機関」という。）の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するため、対象、位置づけ等を規定する情報セキュリティ基本方針（以下「基本方針」という。）を定めることとし、情報セキュリティの確保に取り組むことを目的とする。

機密性 (confidentiality)	情報にアクセスすることが許可された者だけがアクセスできる状態を確保すること。
完全性 (integrity)	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。
可用性 (availability)	情報のアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること。

国際標準化機構(ISO)が定めるもの(ISO7498-2：1989)

２　定義

(1) 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。

(2) 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。

(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) 情報セキュリティインシデント

情報セキュリティに関する障害、事故及びシステム上の欠陥をいう。

３　対象とする脅威

情報資産に対する脅威として以下を想定し、情報セキュリティ対策を実施する。

・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

・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

・地震、津波、落雷、火災等の災害によるサービス及び業務の停止等

・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

・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

⑴　関係職員の範囲

組合関係機関の職員のうち、組合のネットワークにより管理している情報資産を利用できる職員とする。

⑵　情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとし、組合のネットワークにより管理している情報資産以外は、基本方針の対象外とする。

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等のシステム関連文書

５　関係職員の遵守義務

関係職員は、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、基本方針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

情報資産について、情報セキュリティ対策を推進する組織体制を整備し、管理責任の所在を明確にする。

(2) 情報資産の分類と管理

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、当該分類による重要度に応じた情報セキュリティ対策を実施する。

(3) 物理的セキュリティ

情報システム及び情報機器を設置する場所への不正な立ち入り、情報資産の破損・破壊・窃用・盗難等から保護するために物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、関係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。

(5) 技術的セキュリティ

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理、コンピュータウイルス対策等の技術的な対策を講じる。

(6) 運用に関するセキュリティ対策

情報システムの監視、基本方針の遵守状況の確認、外部委託を行う際のセキュリティ確保

等、運用面における必要な対策を行う。

(7) 評価・見直し

基本方針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し、運用改善を行い、情報セキュリティの向上を図る。適宜基本方針の見直しが必要な場合は、その都度見直しを行う。

7　情報セキュリティの監査・自己点検の実施

基本方針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の監査・自己点検を実施する。

8　基本方針の見直し

情報セキュリティの監査・自己点検の結果、基本方針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、基本方針を見直す。

9　違反に対する対応

基本方針に違反した者に対しては、その重大性に応じて、地方公務員法その他関係法令に基づく厳正な対応を行う。