

## 奥能登クリーン組合 情報セキュリティ基本方針

奥能登クリーン組合（以下「組合」という。）は、珠洲市と能登町が共同で設置及び管理運営する一般廃棄物処理を担う広域的な行政組織です。

奥能登地域のごみ処理を効率化し、環境負荷を減らすために、平成12年に発足しました。

組合においては、環境に配慮した安全なごみ処理と資源循環を進めること等を基本理念としています。

### 1 情報セキュリティの目的

組合では、ごみ処理業務・問い合わせ対応・職員管理・行政手続き等に伴い取得する個人情報等の重要な情報資産を取り扱っており、これらの情報資産を様々な脅威から守り、安全性を確保することは、組合に課せられた責務でもある。

そのため、災害や事故に備えた体制を整備する等、組合が実施するセキュリティ対策に関する基本的な事項を定め、様々な脅威から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ことを本基本方針の目的とする。

また、全ての職員等が、組合が保有する情報資産に対する脅威への対応が重大かつ喫緊の課題であることを改めて認識し、組合におけるセキュリティ対策の推進に積極的に取り組むため、具体的対策、措置等をここに定める。

### 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及びその構成機器（ハードウェア及びソフトウェア）をいう。

#### (2) 情報システム

組合の運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

#### (3) セキュリティ（サイバーセキュリティ）

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。

※セキュリティには、サイバーセキュリティを含む。

#### (4) セキュリティポリシー

本基本方針及びセキュリティ対策基準をいう。

- (5) 職員等  
組合長、副組合長、組合議員、会計管理者、監査委員及び事務局長その他の職員をいう。
- (6) 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。
- (7) 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。
- (8) 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。
- (9) インターネット接続の情報システム  
電子メール、Webサイト管理システム、内部事務を取り扱う情報システム等のインターネットに接続された情報システムをいう。
- (10) 業務用端末  
職員等に対し、業務上利用することが許可されたパソコン、スマートフォン及びタブレット等のモバイル端末等をいう。
- (11) 業務用外部記録媒体  
職員等に対し、業務上利用することが許可されたUSBメモリや光ディスク等の外部記録媒体をいう。
- (12) 管理区域  
組合内に設定され、ネットワークの基幹機器及び重要な情報システム等に係る機器等を設置し、管理運用、保管等を行う専用の区域をいう。
- (13) ソーシャルメディアサービス  
インターネット上で展開される情報メディアであって、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通等といった社会的な要素を含んだメディアである、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等のサービスをいう。
- (14) 外部サービス  
組合以外の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービス、Web会議サービス、ソーシャルネットワーキングサービス、検索サービス、翻訳サービス、地図サービス、ホスティングサービス等をいう。
- (15) クラウドサービス  
従来は手元のコンピュータに導入して利用していたソフトウェアやデータ、それらを提供するための技術基盤等を、インターネット等のネットワークを通じて、利用できるサービスをいう。

(16) セキュリティ事象（以下「イベント」という。）

3の脅威により業務の遂行及びセキュリティに影響を与えうる事象の全てをいう。

(17) セキュリティインシデント

イベントのうち、業務の遂行を危うくする確率及びセキュリティを脅かす確率が高い事象をいう。

### 3 対象とする脅威

情報資産に対する脅威として、以下のものを想定し、セキュリティ対策を実施するほか、新たな脅威の発生に備え、最新の脅威動向を確認する等、適切に対応する。

- (1) 不正アクセス、ウイルス攻撃、ランサムウェア攻撃、サービス不能攻撃等のサイバー攻撃及び侵入等の意図的な要因による組合が保有する情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、サービス及び業務の停止のほか、内部管理の欠陥等職員等による不正行為等
- (2) 組合が保有する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、外部サービス設定等の不備、メンテナンスの不備、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、メールの誤送信等の非意図的的要因による情報資産の漏えい・破壊・消去、重要情報の詐取、サービス及び業務の停止、不正行為等
- (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、水道供給の途絶等のインフラの障害からの波及等

### 4 適用範囲

(1) 適用範囲

本基本方針が適用される範囲は、組合執行機関とする。

(2) 情報資産の適用範囲

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 情報システム等

イ 個人情報のほか、情報システム等で取り扱うデータ

ウ 情報システム等に関するシステム設計書、ネットワーク図等のシステム関連文書

エ 紙文書

### 5 職員等の遵守義務

職員等は、組合が保有する情報資産に対する脅威への対応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、セキュリティポリシー及びセキュリティ実施手

順等を遵守しなければならない。

## 6 セキュリティ対策

3の脅威から情報資産を保護するために、以下のセキュリティ対策を講じる。

### (1) 組織体制の確立

組合の情報資産についてセキュリティ対策を推進する組織体制を確立する。

### (2) 情報資産の分類と管理

組合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、セキュリティ対策を講じる。

### (3) 物理的セキュリティ対策

サーバ、管理区域、通信回線、業務用端末等の管理について、物理的な対策を講じる。

### (4) 人的セキュリティ対策

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。

### (5) 技術的セキュリティ対策

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。

### (6) 運用面での対策

情報システムの監視及びセキュリティポリシー等の遵守状況の確認のほか、(7)の業務委託及び外部サービスを利用する際のセキュリティ確保等、セキュリティポリシーの運用面で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、緊急時対応体制を整備する。

### (7) 業務委託及び外部サービスの利用に係る対策

組合の業務を受託する事業者（当該事業者から派遣されている者を含む。）（以下「委託事業者等」という。）に当該業務を行わせる場合には、組合が定めるセキュリティ要件等、セキュリティ対策上、遵守させるべき事項を、委託事業者等の選定要件として提示する。

さらに、契約や協定等（以下「契約等」という。）の締結時等に、組合が定めるセキュリティ要件を契約等事項に明記し、委託事業者等において要件を満たすセキュリティ対策が確保されていることを確認、又は、別途、書面による提出を求める等の措置を講じる。

なお、外部サービスの利用に当たっては、利用に関する手順等を定めるとともに、必要に応じて、当該利用の対象とする情報について定める等、規定を整備し、対策を講じる。

#### 7 リスク評価の実施及び年度計画の策定

セキュリティに係る内部環境及び外部環境の変化を踏まえ、組合が保有する情報資産のセキュリティ上のリスクを評価し、リスク対応方針を策定する。

また、必要に応じて、策定したリスク対応方針に基づきリスク対応計画を策定する。

#### 8 自己点検及びセキュリティに関する監査の実施

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、自己点検及びセキュリティに関する監査を実施する。

#### 9 セキュリティポリシーの見直し

自己点検及びセキュリティに関する監査の結果、セキュリティポリシーの見直しが必要となった場合、又は、セキュリティに関する状況の変化に対応するため、新たに対策が必要となった場合には、セキュリティポリシーを見直す。

#### 10 セキュリティ対策基準の策定

7から9までに示す対策等を実施するため、具体的な遵守事項及び判断基準等定めるセキュリティ対策基準を策定する。

なお、当該対策基準は、組合におけるセキュリティ対策の基準を定めるものであり、公にすることにより、組合の運営に重大な支障を及ぼすおそれがあることから、当該対策基準については、4（1）に定める適用範囲以外に対しては非公開とする。

#### 11 セキュリティ実施手順の策定

10に定めるセキュリティ対策基準を踏まえ、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セキュリティ実施手順を策定するものとする。

なお、当該実施手順は、関連する情報システム等のセキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務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。