塩谷広域行政組合
情報セキュリティ基本方針

平成 19 年３月１日　施行
令和８年４月１日　全部改正

1　目的

塩谷広域行政組合情報セキュリティ基本方針（以下「基本方針」という。）は、塩谷広域行政組合（以下「組合」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、組合が実施する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

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　情報セキュリティポリシー

本基本方針及び塩谷広域行政組合情報セキュリティ対策基準をいう。

⑻　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。

⑼　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は、次のとおりとする。

⑴　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

⑵　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

⑶　地震、落雷、火災等の災害によるサービス及び業務等の停止等

⑷　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

⑸　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

⑴　行政機関の範囲

本基本方針が適用される行政機関は、管理者部局、消防部局、監査委員及び議会事務局とする。

⑵　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。

①　ネットワーク、情報システム及びこれらの運用又は管理に必要な設備並びに電磁的記録媒体

②　ネットワーク又は情報システムで取り扱う情報（これらを印刷した文章を含む。）

③　ネットワーク又は情報システムに関する仕様書、図面等のシステム関連文書

5　職員等の遵守義務

職員、非常勤職員、臨時職員及び会計年度任用職員（以下「職員等」という。）は、業務の遂行に当たり情報セキュリティポリシー及塩谷広域行政組合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の対象とする脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

⑴　組織体制

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。

⑵　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、当該分類に基づき情報セキュリティ対策を実施する。

⑶　物理的セキュリティ対策

サーバ、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。

⑷　人的セキュリティ対策

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。

⑸　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、不正アクセス防止等の技術的な対策を講じる。

⑹　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、業務委託を行う場合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｡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。

⑺　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。

7　情報セキュリティの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確認するため、定期的又は必要に応じて情報セキュリティの点検及び監査を実施する。

8　情報セキュリティポリシーの見直し

情報セキュリティの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となった場合には、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、リスクを検討した上で、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（以下「対策基準」という。）を策定する。

１０　情報セキュリティ実施手順の策定

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（以下「実施手順」という。）を策定する。

１１　公表

⑴　この基本方針は、組合ホームページにおいて公開する。

⑵　対策基準及び実施手順は、公にすることにより組合の業務運営に支障を及ぼすおそれがあることから非公開とする。

１２　委任

この基本方針に定めるもののほか必要な事項は、別に定める。