十勝圏複合事務組合情報セキュリティ基本方針

令和８年３月24日制定

（目的）

第１条　十勝圏複合事務組合情報セキュリティ基本方針（以下「基本方針」という。）は、十勝圏複合事務組合（以下「組合」という。）と教育委員会、監査委員、公平委員会及び議会（以下「行政委員会等」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、組合及び行政委員会等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。

（用語の定義）

第２条　情報セキュリティポリシー及び情報セキュリティ実施手順で使用する用語の定義は、次の各号に定めるところによる。

（１）　情報セキュリティとは、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。

（２）　機密性とは、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。

（３）　完全性とは、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。

（４）　可用性とは、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。

（５）　ネットワークとは、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。

（６）　情報システムとは、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。

（７）　情報資産とは、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、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。）又は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をいう。

（８）　情報セキュリティ対策とは、情報セキュリティを維持するための対策をいう。

（９）　情報セキュリティポリシーとは、情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであって、情報セキュリティ基本方針、情報セキュリティ対策基準からなるものの総称をいう。

(10)　情報セキュリティ対策基準とは、情報セキュリティ基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断基準を定めたものをいう。

(11)　インターネット接続系とは、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。

(12)　無害化通信とは、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。

(13)　電磁的記録媒体とは、準用している帯広市電磁的記録取扱規程で定めるものをいう。

(14)　情報セキュリティインシデントとは、不正アクセス、ウイルス感染、ハードウェア・ソフトウェア障害、人為的ミス等により、情報資産の漏えいや破壊、情報システムの停止等が発生すること（その疑いがある場合を含む。）をいう。

（対象とする脅威）

第３条　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、水道供給の途絶等のインフラの障害からの波及等

（適用範囲）

第４条　基本方針が適用される機関及び情報資産の範囲は、次のとおりとする。

（１）　機関の範囲は、組合及び行政委員会等とする。

（２）　情報資産の範囲は、次のとおりとする。

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及びネットワーク図等のシステム関連文書

（職員等の遵守義務）

第５条　基本方針の適用を受ける者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たらなければならない。この場合において、全ての職員（職員、再任用職員、会計年度任用職員、臨時的任用職員をいう。以下「職員等」という。）は、組合の情報セキュリティ対策基準及び情報セキュリティ実施手順（以下「基準等」という。）を遵守しなければならない。ただし、行政委員会等で個別に基準等を定めている場合、行政委員会等の職員等は行政委員会等の基準等の方を遵守しなければならない。

（情報セキュリティ対策）

第６条　第３条で示した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

組合の情報資産について、情報セキュリティ対策を推進及び管理するための組織体制を確立するものとし、行政委員会等の情報資産については、必要に応じて個別に組織体制を定めることができるものとする。

（２）　情報資産の分類と管理

組合及び行政委員会等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靭性の向上

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、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、必要に応じて基本方針の適用を受ける者に対して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、情報セキュリティインシデント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、必要に応じて利用にかかる規定を整備し、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。

（情報セキュリティ監査及び自己点検の実施）

第７条　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。

（情報セキュリティポリシーの見直し）

第８条　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、リスクを検討した上で、情報セキュリティポリシーの見直しを行う。

（情報セキュリティ対策基準の策定）

第９条　組合は、前３条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ものとし、行政委員会等は、必要に応じて個別に情報セキュリティ対策基準を定めることができるものとする。なお、情報セキュリティ対策基準は、公にすることにより組合及び行政委員会等の行政運営等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。

（情報セキュリティ実施手順の策定）

第10条　組合は、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し、行政委員会等は、必要に応じて個別に情報セキュリティ実施手順を定めることができるものとする。なお、情報セキュリティ実施手順は、公にすることにより組合及び行政委員会等の行政運営等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。

附　則

この基本方針は、令和８年４月１日から施行する。