南那須地区広域行政事務組合
情報セキュリティポリシー

【情報セキュリティ基本方針】

南那須地区広域行政事務組合

平成 19 年４月　策定

令和８年４月　改定

もくじ

１．目的・・・・・・・・・・・・・・・・・・・・・・・・・・・・・1
２．用語の定義・・・・・・・・・・・・・・・・・・・・・・・・・・1
３．対象とする脅威・・・・・・・・・・・・・・・・・・・・・・・・3
４．適用範囲・・・・・・・・・・・・・・・・・・・・・・・・・・・3
５．職員等の遵守義務・・・・・・・・・・・・・・・・・・・・・・・3
６．情報セキュリティ対策・・・・・・・・・・・・・・・・・・・・・3
７．情報セキュリティ監査及び自己点検の実施・・・・・・・・・・・4
８．情報セキュリティポリシーの見直し・・・・・・・・・・・・・・4
９．情報セキュリティ対策基準の策定・・・・・・・・・・・・・・・4
10．情報セキュリティ実施手順の策定・・・・・・・・・・・・・・・4
附　則　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・5

１．目的

南那須地区広域行政事務組合（以下「当組合」。という）の、各情報システムが取り扱う情報には、住民の個人情報や行政運営上重要な情報など、部外者に漏洩等した場合に極めて重大な結果を招くものが多数含まれている。これらの情報及びそれを取り扱う情報システムを様々な脅威から防御することは、住民の財産、プライバシー等を守るためにも、事務の安定的な運営のためにも必要不可欠である。

また、近年の高度情報化の急速な進展により、電子自治体の実現も更に加速すると思われる。

このような状況下において当組合が電子行政サービスを提供するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、当組合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）を整備するために「南那須地区広域行政事務組合情報セキュリティポリシー」を策定することとし、その根本的な考え方として、ここに情報セキュリティ基本方針を定めるものである。

なお、この基本方針は、「サイバーセキュリティを確保するための方針」の内容を含むものである。

２．用語の定義

基本方針において、次の各号に掲げる用語の定義は、それぞれ当該各号に定めるところによる。

（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、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

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。

（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）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（５）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。

（６）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。

（７）可用性

情報にアクセスすることを認められた者が、必要な時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。

（８）マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（９）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。

(10) 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。

(11) 外部要員

当組合関係団体の職員で当組合の所有する情報資産を使用する者及び当組合と業務委託先（システム開発業務等を受託する業者）等との契約に基づいて当組合の所有する情報資産を使用する者をいう。

(12) ネットワークシステム

LAN、WAN及びそれらを構成する制御機器、通信機器、回線、接続するサーバ等の総称をいう。

(13) 記録媒体

持ち運びが可能な電子データの記憶媒体。USBメモリー、外付HD、BL（ブルーレイディスク）、DVD、CD、MT（磁気テープ）等の総称をいう。

(14) 開発環境

プログラムの作成・変更及び開発したプログラム等の試験を行うために設置された開発者のみがアクセスできる仕組みをいう。

(15) 保守

情報システムの点検作業をいう。不備・不具合等があった場合の調整、修復作業も含む。

３．対象とする脅威

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、メンテナンスの不備、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。

（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）当組合の範囲

情報セキュリティポリシーは、当組合が保有する全ての情報資産と、それを取扱う全ての職員及び外部要員（以下「職員等」という。）に適用する。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

② 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。）

③ 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

５．職員等の遵守義務

職員等は、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

当組合の情報資産について、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。

（２）情報資産の分類と管理

当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行う。

（３）物理的セキュリティ

サーバ等、通信回線等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。

（４）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、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

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

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、外部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切に対応するため、緊急時対応計画を策定する。

７．情報セキュリティ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。

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、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を策定する。

なお、情報セキュリティ対策基準は、情報セキュリティの対策に関する具体的な内容が含まれるため、公にすることにより当組合の行政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。

10. 情報セキュリティ実施手順の策定

情報セキュリティ対策基準の策定に基づき、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当組合の行政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。

附　則

この基本方針は、平成 19 年４月１日から実施する。

この基本方針は、令和８年４月１日から実施する。