上川広域滞納整理機構
サイバーセキュリティを確保するための方針

（上川広域滞納整理機構情報セキュリティポリシー）

初版　令和８年３月１日

目　　次

序章

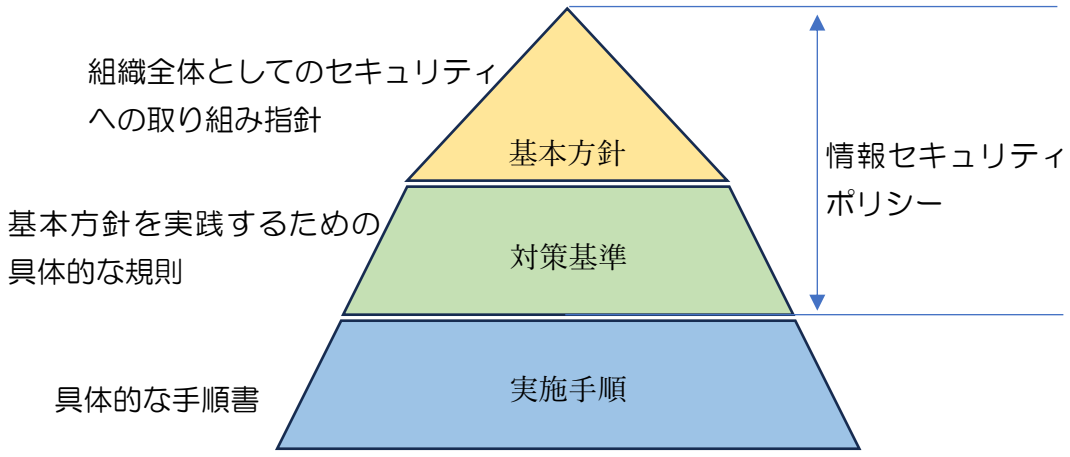
サイバーセキュリティを確保するための方針と情報セキュリティポリシーについて

令和６年6月に地方自治法が改正され、地方自治体はサイバーセキュリティの確保について方針を定め、必要な措置を講じなければならないものとされた。また、方針の策定又は変更については、総務大臣が指針を示すこととされ、令和７年４月に「地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針(案)（以下、「指針」）」が示された。

当機構では情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化してくことが必要と考え、現行の情報セキュリティポリシーのうち「情報セキュリティ方針」について指針を踏まえて見直しを行い、地方自治法第244条の６第１項に規定する方針に位置付ける方針とした。

なお、情報セキュリティポリシーは、機構の情報資産に対する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文書を総称する。機構の情報資産に関する業務に携わる職員等、及び外部委託業者は、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負う。

情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層で構成されている。「情報セキュリティ基本方針」は地方自治法上の方針と位置づけ公表する（地方自治法第244 条の6 第2項）が、「情報セキュリティ対策基準」以下はセキュリティ確保のため公表はしないこととしている。



第１章　情報セキュリティ基本方針

１　目的

この方針は、上川広域滞納整理機構（以下「機構」という。）の各情報システムが取り扱う滞納者の個人情報及び行政運営上重要な情報の破壊、改ざん又は外部への漏えいが生じた場合の被害の重大性にかんがみ、機構の保有する情報資産を様々な脅威から防御し、機構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基本的な事項を定め、もって滞納者の財産及びプライバシーの保全並びに安定的な行政の実現に資することを目的とする。

２　用語の定義

（１）コンピュータ

ハードウェア及びソフトウェアで構成するパーソナルコンピュータ、サーバ及びストレージ等周辺機器をいう。

（２）ネットワーク

情報処理を行う際に利用する通信網、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。

（４）情報セキュリティ対策

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。

（５）機密性

情報へのアクセスを認められた者だけが、その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

情報へのアクセスを認められたものが、必要な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をいう。

（8）特定個人情報

行政手続における特定の個人を識別するための番号の利用に関する法律（以下「番号法」という。）第２条に規定する、個人番号をその内容に含む個人情報ファイルをいう。

（9）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

務等に係る情報システム及びデータをいう。

（10）LGWAN 接続系

LGWAN 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（マイナンバー利用事務系を除く。）。

（11）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。

（12）通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（13）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。

（14）クラウドサービス

クラウドサービスは、ソフトウェア・データ・サーバなどをネットワーク経由で利用する仕組みの総称をいう。

（15）クラウドサービス利用者

クラウドサービスを利用する本機構をいう。本機構は、クラウドサービス事業者との利用における契約を行う。

（16）クラウドサービス事業者

クラウドサービスを提供し、本機構と利用における契約をした組織をいう。また、本機構と契約前のクラウドサービス事業者のことをクラウドサービス提供者という。

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、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）行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局とする。

（２）適用対象者

この方針の適用対象者は、機構に勤務する地方公務員法（昭和25年法律第261号）第３条第２項に規定する一般職の職員及び会計年度任用職員、同条第３項に規定する特別職の職員（以下「職員等」という。）とする。

（３）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

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もち、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

本機構の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（2）情報資産の分類と管理

本機構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）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③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。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（4）物理的セキュリティ

サーバ、電算室、通信回線およ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、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、アクセス制限、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。

（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。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。

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、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、リスクを検討したうえ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を策定する。

１０　情報セキュリティ対策実施手順の策定

　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する。

　なお、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は、公にすることにより、機構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。