

湖北広域行政事務センター情報セキュリティ基本方針に関する規程

(目的)

第1条 この基本方針は、湖北広域行政事務センター（以下「センター」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、センター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。

(定義)

第2条 この基本方針において使用する用語の意義は、次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。
- (8) 実施機関 管理者、監査委員及び議会をいう。
- (9) 職員等 一般職の職員、特別職の職員、非常勤職員、会計年度任用職員、センターと業務委託契約を締結した事業者、センターに派遣された職員等情報を業務上利用する全ての者をいう。
- (10) マイナンバー利用事務系 個人番号利用事務（社会保障、地方税又は防災に関する事務）又はその他個人番号の利用が必要とされる事務に関わる情報システム及びデータの領域をいう。
- (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当該情報システムで取り扱うデータの領域をいう。
- (12) 特定用途機器 センター業務のうち、特定の用途に使用される機器（IoT機器を含む。）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、機械故障等の非意図的な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 この基本方針の適用範囲は、センター全ての実施機関における情報資産及び情報資産に接する職員等とする。

2 この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（職員等の遵守義務）

第5条 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 センター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 センター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靱性の向上 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、次の二段階の対策を講じる。

ア マイナンバー利用事務系においては、原則として、総務課職員以外が閲覧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、人事給与システム及び総務課所管フォルダ内での管理を徹底し、情報の流出を防ぐ。

イ 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、情報システム室、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、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、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。

(8) 業務委託と外部サービスの利用

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。この場合において、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、リスクを検討したうえで、情報セキュリティポリシーを見直す。

(情報セキュリティ対策基準の策定)

第9条 第6条、第7条及び前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。