こうち人づくり広域連合情報セキュリティ基本方針

令和８年４月１日

１．目的

本基本方針は、こうち人づくり広域連合（以下「広域連合」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、広域連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

（１）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。

（２）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。

（３）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。

（４）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。

（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。

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）意図的及び偶発的な人的脅威

不正アクセス・不正操作・操作ミス、意図的・偶発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、情報資産の無断持ち出し・紛失・盗難、無許可ソフトウェアの使用等の規定違反　　等

（２）技術的及び物理的脅威

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、重要情報の詐取、プログラム上の欠陥、情報機器故障や情報システム・ネットワークの不具合等の非意図

的要因による情報資産の漏えい・破壊・消去　　等

（3）災害

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）パンデミック

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）インフラ障害

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の範囲は、広域連合事務局（議会事務局、監査委員事務局、選挙管理委員会事務局を含む。）とする。

（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、任期付職員及び会計年度任用職員（以下「職員等」という。）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。

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ものとする。

（1）組織体制

広域連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組織体制を確立する。

（2）情報資産の分類と管理

広域連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

サーバやパソコン等の情報機器及び通信回線をはじめとする情報資産への不正侵入や盗難・改ざん・破壊等から情報資産を保護するため、情報資産への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

情報資産を外部及び内部からの不正アクセス等から保護するため、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、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。

（7）緊急時における対応

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（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。