香取広域市町村圏事務組合情報セキュリティ基本方針

香取広域市町村圏事務組合管理者、香取広域市町村圏事務組合副管理者、香取広域市町村圏事務組合会計管理者、香取広域市町村圏事務組合事務局、香取広域市町村圏事務組合消防本部、香取広域市町村圏事務組合議会及び香取広域市町村圏事務組合監査委員は、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定するサイバーセキュリティを確保するための方針として、香取広域市町村圏事務組合情報セキュリティ基本方針を共同で定める。

令和８年４月１日

香取広域市町村圏事務組合管理者
香取広域市町村圏事務組合副管理者
香取広域市町村圏事務組合会計管理者
香取広域市町村圏事務組合事務局
香取広域市町村圏事務組合消防本部
香取広域市町村圏事務組合議会
香取広域市町村圏事務組合監査委員

１．目的

本基本方針は、実施機関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、実施機関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し、実施機関共同で策定する。

２．定義

（１）実施機関

香取広域市町村圏事務組合（管理者、副管理者、会計管理者、事務局及び消防本部）、香取広域市町村圏事務組合議会及び監査委員をいう。

（２）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。

（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）情報資産

ネットワーク及び情報システムの開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータをいう。

（５）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。

（６）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。

（７）サーバ

電子データを蓄えたり提供したりするための装置のことをいう。

（８）端末

通信回線によってサーバと接続され、又は単独でデータの入力及び出力を行うための装置をいう。

（９）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。

（１０）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。

（１１）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

情報セキュリティ対策を行う上で、特に認識すべき情報資産に対する脅威は、その発生度合や発生した場合の影響を考慮するものとし、次のとおりとする。

（１）不正アクセス、ウィルス攻撃、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、重要情報の搾取、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、洪水等の災害によるサービス及び業務の停止

（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、実施機関とする。

（２）対象者の範囲

本基本方針が適用される対象者は、情報資産に接するすべての職員、会計年度任用職員、非常勤職員、会計管理者、議員及び監査委員（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、以下の情報セキュリティ対策を講じる。

（1）組織体制

実施機関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）物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・盗難等から保護するために施設整備等の物理的な対策を講じる。

（3）人的セキュリティ対策

情報セキュリティに関する権限や責任を定めるとともに、職員等に情報セキュリティポリシーを周知徹底するための教育を実施する等、必要な対策を講じる。

（4）技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、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。

（5）運用

不正なアクセス等から情報セキュリティが侵害されることを防ぐため、ネットワーク監視等の運用面における対策を講じるとともに、緊急事態の発生に備えた危機管理体制を講じる。

（6）業務委託

業務委託を行う場合には、委託事業者と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。

7．情報セキュリティ侵害時のための対策

情報セキュリティが侵害される事態が発生した場合に被害の拡大防止、復旧等を迅速かつ的確に実施するよう備えなければならない。

８．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、定期的また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。

９．情報セキュリティポリシーの評価・見直し

情報システムの変更や新たな脅威の発生等、状況の変化に迅速かつ的確に対応するため、必要に応じて情報セキュリティポリシーの見直しを実施する。