○とかち広域消防事務組合情報セキュリティ基本方針

令和３年２月10日制定
令和８年３月27日改正

（目的）

第１条　本基本方針は、とかち広域消防事務組合（以下「組合」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、組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。

（用語の定義）

第２条　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で使用する用語は、とかち広域消防事務組合情報セキュリティ管理規程第２条で定める定義とする。それ以外の用語の定義は、次の各号に定めるところによる。

（１）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。

（２）電磁的記録媒体

電磁的記録媒体とは、とかち広域消防事務組合電磁的記録取扱規程で定めるものをいう。

（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

（適用範囲）

第４条　本基本方針が適用される行政機関及び情報資産の範囲は、次のとおりとする。

（１）行政機関の範囲

組合長の事務部局、消防局、監査委員、公平委員会及び議会とする。

（２）情報資産の範囲

ア　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
イ　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。）
ウ　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

（職員等の遵守義務）

第５条　本基本方針の適用を受ける者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たらなければならない。この場合において、すべての職員（職員、再任用職員、会計年度任用職員及び臨時的任用職員をいう。以下「職員」という。）は、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。

（情報セキュリティ対策）

第６条　第３条で示した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

組合の情報資産について、とかち広域消防事務組合情報セキュリティ管理規程第３条に定める組織体制を確立するものとし、監査委員、公平委員会及び議会（以下「行政委員会等」という。）の情報資産については、必要に応じ、個別に組織体制を定めることができる。

（２）情報資産の分類と管理

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実施する。

（３）情報システムの強靭性の向上

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、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、情報セキュリティインシデント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

ア　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。

イ　外部サービス（クラウドサービス）を利用する場合には、必要に応じて利用に係る規定を整備し対策を講じる。

ウ　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評価・見直しを実施し、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。

（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の見直しを行う。

（情報セキュリティ対策基準の策定）

第９条　前３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ものとし、行政委員会等は、必要に応じ、個別に情報セキュリティ対策基準を定めることができるものとする。なお、情報セキュリティ対策基準は、公にすることにより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。

（情報セキュリティ実施手順の策定）

第10条　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し、行政委員会等は、必要に応じ、個別に情報セキュリティ実施手順を定めることができるものとする。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（令和３年２月10日）

（施行期日）

１　この基本方針は、令和３年４月１日から施行する。

（準備行為）

２　この基本方針を施行するために必要な準備行為は、この基本方針の施行の日前においても行うことができる。

附　則（令和８年３月27日）

（施行期日）

１　この基本方針は、令和８年４月１日から施行する。

（準備行為）

２　この基本方針を施行するために必要な準備行為は、この基本方針の施行の日前においても行うことができる。