幡多中央消防組合訓令第１号

幡多中央消防組合消防本部情報セキュリティポリシー基本方針に関する規程を次のように定める。

令和８年１月 15 日

幡多中央消防組合長　　山　下　元一郎

幡多中央消防組合消防本部情報セキュリティポリシー基本方針に関する規定

目次

第１章　総則

（目的）

第１条　組合の各情報システムが取り扱う情報（以下「情報資産」という。）の中には、住民の個人情報のみならず組合運営上重要な情報など、部外に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報資産及び情報システムをさまざまな脅威から防御することは、住民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠であり、ひいては、このことが組合に対する住民からの信頼の維持向上に寄与するものである。これらのことから、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠なことから、情報資産の機密性、完全性及び可用性を維持するための対策（以下「情報セキュリティ対策」という。）を整備するために、この幡多中央消防組合消防本部情報セキュリティポリシー（以下「セキュリティポリシー」という。）を定めるものである。

（定義）

第２条

(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（ハードウェアおよびソフトウェア）をいう。

(2) インターネット　共通の通信仕様を用いて全世界の膨大な数のコンピュータや通信機器を相互につないだ巨大なコンピュータネットワークをいう。

(3) 情報システム　業務系の電子計算機（業務系におけるネットワーク、ハードウエア及びソフトウエア）及び記録媒体で構成され、処理を行う仕組みをいう。

(4) 情報セキュリティ　情報資産の機密性、安全性、可用性を維持することをいう。

(5) 不正アクセス　利用する権限のない第三者が、ネットワークを通じて別の場所にあるコンピュータに不正に接続、侵入する行為のこと。

(6) 機密性、完全性及び可用性　国際標準化機構（ISO）がこれらについて定めており、機密性とは、情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること、完全性とは、情報及び処理の方法の正確さ及び完全である状態を安全防護すること、可用性とは、許可された利用者が必要な時に情報にアクセスできることを確実にすること、とそれぞれ定められている。

（位置づけと職員等の責務）

第３条　組合の情報セキュリティ対策における基本的な考え方を定めたものが、「基本方針」である。この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。

管理者をはじめとしてすべての職員及び非常勤職員（以下「職員等」という。）及び外部委託者は、情報セキュリティの重要性について共通の認識をもつとともに、業務の遂行にあたってセキュリティポリシーを遵守する責務を負うこと。

（情報資産の管理）
第４条　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
２　情報資産は、重要度に応じた情報セキュリティ対策を施したうえ、管理すること。
（情報資産の管理体制）
第５条　情報資産について、幹部が率先して情報セキュリティ対策を推進・管理するための体制を確立すること。
（情報資産への脅威）
第６条　情報資産に対する脅威として特に認識すべきものは、以下のとおりである。
(1) 部外者による故意の不正アクセス、または不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難等
(2) 職員等及び部外委託者による意図しない操作、故意の不正アクセス、または不正操作によるデータやプログラムの持ち出し・盗難・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等
(3) 地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止
(4) パンデミック、サイバー攻撃、インフラ障害等不測の事態からの脅威
（情報セキュリティ対策）
第７条　上記で示す脅威から情報資産を保護するため、次の情報セキュリティ対策を講ずること。
（セキュリティ対策のための組織体制の確立、情報資産の重要性の分類と管理、ネットワークのセキュリティ対策が以下の物理的セキュリティ対策等の前提となる。）
(1) 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ち入り、情報資産への損傷・妨害等から保護するために物理的な対策を講じること。
(2) 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、全ての職員等及び外部委託事業者にセキュリティポリシーの内容を周知徹底する等、充分な教育及び啓発が講じられるように必要な対策を講じること。
(3) 技術におけるセキュリティ対策　情報資産を外部からの不正なアクセス等（内部職員からの不正行為も含む）から適切に保護するため、次に掲げる対策を講じること。
ア　情報資産へのアクセス制御
イ　ネットワーク管理等の技術面の対策
(4) 運用面におけるセキュリティ対策　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な対応を可能とするため、緊急時対応計画を策定すること。また、通常時においても、庁内システムの運用にあたり、次に掲げる対策を講ずること。
ア システム開発等の外部委託にあたり、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　ネットワークの監視
ウ　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、セキュリティポリシーの遵守状況を確認する。
（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。
（対策基準の策定）
第９条　情報資産に対し情報セキュリティ対策を講じるにあたり、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、対策基準の策定にあたっては、情報セキュリティ対策を行う上で必要となる基本的な要件、実施手順の策定、監視方法や評価・運用の見直し等の事項について具体的な遵守事項及び判断基準等を明記することとする。
（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本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。

第２章　情報セキュリティ対策基準

（基準の目的・対象範囲）

第11条

(1) この対策基準は、基本方針の規定に基づき、情報資産の機密性、完全性及び可用性を維持するための具体的な対策（以下「情報セキュリティ対策」という。）を示すことで、部外漏洩など情報資産に対するさまざまな脅威から情報資産を守り、業務の安定的運営及び組合に対する住民からの信頼の維持向上を図ることを目的とする。

(2) 対策基準の適用対象範囲を次のとおり定める。

幡多中央消防組合に所属する消防本部及び消防署（以下「本組合」という。）に設置してあるすべての情報システム等の情報資産。

(3) 職員等及びすべての外部委託者は、情報資産を取り扱う場合、対策基準の規定で定める事項を遵守すること。

（組織体制及び情報セキュリティ対策）

第12条　四万十市情報セキュリティ対策基準及び黒潮町情報セキュリティ基本方針を準用する。また、技術的対策基準については、幡多中央消防組合情報ネットワーク運営管理要綱を別に定める。

（セキュリティ事案発生時の報告体制）

第13条　担当者⇒消防責任者⇒四万十市・黒潮町（必要に応じて報告を実施する。）

附　則

この訓令は、令和８年４月１日から施行する。