大船渡地区消防組合・
大船渡地区消防組合議会・
大船渡地区消防組合監査委員
情報セキュリティ基本方針

令和８年４月１日

大船渡地区消防組合
大船渡地区消防組合議会
大船渡地区消防組合監査委員

1　目的

大船渡地区消防組合（以下「消防組合」という。）、大船渡地区消防組合議会（以下「議会」という。）、及び大船渡地区消防組合監査委員（以下「監査委員」という。）の各情報システムが取り扱う情報資産には、個人情報や行政運営上重要な情報など、外部に漏えい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、これらの情報及び情報を取り扱う情報システムを人的脅威や災害、事故等から防御することは、大船渡地区消防組合構成市町の住民（以下「住民」という。）の財産、プライバシー等の保護及び事務の安定的な運営に必要不可欠であり、消防組合、議会及び監査委員（以下「消防組合関係機関」という。）に対する住民からの信頼の維持向上にも寄与するものである。

また、住民サービスの向上と業務の効率化を図るため、情報システムは行政運営基盤として欠かせないものとなっており、消防組合関係機関の業務執行を今後も円滑に進めるためには、消防組合関係機関が管理している情報システムが高度な安全性を有することが不可欠である。

このことから、消防組合関係機関の情報資産の機密性、完全性及び可用性（注）を維持するための対策（情報セキュリティ対策）を整備するため、対象、位置付け等を規定する情報セキュリティ基本方針（以下「基本方針」という。）を定めることとし、情報セキュリティの確保に最大限取り組むこととする。

（注）：国際標準化機構(ISO)が定めるもの(ISO7498-2：1989)

機密性 (confidentiality)	情報にアクセスすることが許可された者だけがアクセスできる状態を確保すること。
完全性 (integrity)	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。
可用性 (availability)	情報のアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること。

2　定義

(1) 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。

(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し、適切に管理することをいう。

(4) 情報セキュリティインシデント

情報セキュリティに関する障害、事故及びシステム上の欠陥をいう。

(5) 消防情報一括管理システム接続系

消防情報一括管理システム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。

(6) インターネット接続系

インターネットメール、ホームページ管理などに関わるインターネットに接続された情報システムで取り扱うデータをいう。

(7) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3　対象とする脅威

情報資産に対する脅威として以下を想定し、情報セキュリティ対策を実施する。

・サイバー攻撃、不正アクセス、ウイルス感染等の意図的な攻撃による情報資産の漏えい、破壊、改ざん又は消去

・内部不正、誤操作、設定不備、委託管理不備等の非意図的要因による情報資産の障害

・地震、津波、火災等の災害による業務停止

・感染症の流行による要員不足

・電力及び通信インフラの障害

4　適用範囲

(1) 職員の範囲

消防組合関係機関の職員（以下「職員」という。）とする。

(2) 情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとし、消防組合のネットワークにより管理している情報資産以外は、基本方針の対象外とする。

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

5　職員の遵守義務

職員は、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基本方針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。

(1) 組織体制

消防組合関係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。

また、情報セキュリティ対策の統括責任者（最高情報セキュリティ責任者：CISO）を設置し、情報セキュリティ対策の推進及び管理を行うものとする。

(2) 情報資産の分類と管理

消防組合関係機関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、当該分類による重要度に応じた情報セキュリティ対策を実施する。

また、情報資産については台帳を整備し、所在、管理責任者、取扱区分等を明確にするものとする。

(3) 情報システム全体の強靭性の向上

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、次の対策を講じる。

ア　消防情報一括管理システム接続系においては、組織及び個人における、２重のログイン認証体制の下、TLS 等の暗号化通信を用いてデータの保護を図る。

また、データセンターにおけるセキュリティ対策を構築し、安全性維持を図る。

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

情報システム及び情報機器を設置する施設への不正な立ち入り、情報資産の破損・破壊・窃用・盗難等から保護するために物理的な対策を講じる。

可搬媒体及び端末の持ち出しについては、許可制とし、紛失防止措置を講じるものとする。

(5) 人的セキュリティ

情報セキュリティに関し、職員及び外部委託事業者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

コンピュータ及びネットワークの管理・監視、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。

重要な情報システムについては、アクセスログ及び操作ログを取得し、一定期間保存するとともに、不正行為の早期発見のため監視を行うものとする。

(7) 運用

情報システムの監視、基本方針の遵守状況の確認、外部委託を行う際のセキュリティ確保等、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。

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) 外部委託とクラウドサービスの利用

外部委託を行う場合には、外部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、外部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。

クラウドサービスを利用する場合には、利用に係る規程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する。

クラウドサービスの利用にあたっては、データの保存場所、管理主体、アクセス権限等を明確にし、必要なセキュリティ対策が確保されていることを確認するものとする。

7　情報セキュリティ監査及び自己点検の実施

基本方針の遵守状況を検証するため、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　基本方針の見直し

情報セキュリティ監査及び自己点検の結果、基本方針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、基本方針を見直す。

9　情報セキュリティ対策基準及び実施手順の策定

(1) 情報セキュリティ対策基準

上記６、７及び８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た情報セキュリティ対策基準を策定するものとする。

(2) 情報セキュリティ実施手順

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事項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。

10　通信指令センター運用に係る情報セキュリティ対策

(1) 通信指令センターに係る基本的事項

通信指令センターは、119 番通報の受理、出動指令、関係機関との連絡調整等を行う消防活動の中枢であり、その機能停止は住民の生命・身体に重大な影響を及ぼす。

このため、通信指令センターにおいては、可用性を最優先としつつ、機密性及び完全性を確保する。

(2) 対象となる情報資産（通信指令センター）

通信指令センターにおいて取り扱う主な情報資産は、次のとおりとする。

ア　指令台設備、指令制御システム
イ　音声通話記録（119 番通報録音データ）
ウ　出動指令データ、活動履歴情報
エ　位置情報（発信位置情報システム等）
オ　無線通信設備及び関連ネットワーク
カ　指令センター運用マニュアル等

(3) 通信指令センター特有の脅威

通信指令センターにおいては、次の脅威を特に考慮する。

ア　指令システム停止による 119 番受理不能
イ　サイバー攻撃による指令遅延・誤指令
ウ　通報情報の漏えい（個人情報・位置情報）
エ　無線通信の妨害・盗聴
オ　災害時の同時多発通報による処理逼迫
カ　長時間停電・回線断による機能停止
キ　映像通報システムを通じた個人情報の漏えい及び不正取得
ク　ランサムウェア等によるシステム停止

(4) 可用性確保対策

通信指令センターの継続運用を確保するため、次の対策を講じる。

ア　指令システムの冗長構成（二重化）
イ　自家発電設備及び無停電電源装置（UPS）の整備
ウ　通信回線の多重化（異なる経路・事業者）
エ　災害時優先通信の確保

(5) アクセス管理及び認証

通信指令センターのシステム利用にあたっては、以下を徹底する。

ア　指令業務従事者ごとの ID 管理
イ　多要素認証またはそれに準ずる厳格な認証
ウ　権限の最小化（必要最小限のアクセス権）
エ　操作ログの取得及び定期的な点検
オ　映像通報システム(Live119)の利用に係る、閲覧期限を限定し、不必要なアクセスの防止

(6) 通信及びデータ保護

通信指令センターにおける情報の保護のため、以下の対策を講じる。

ア　音声・データ通信の暗号化
イ　通報録音データの適切な保存・管理
ウ　外部ネットワークとの接続制御（分離・監視）
エ　無線通信の適切な管理（秘匿性確保）

オ　映像通報システム（Live119）により取得される映像及び音声データについては、通信の暗号化を確保するとともに、保存の要否、保存期間及びアクセス権限を明確にし、適切に管理するものとする。

(7) 物理的セキュリティ（指令室）

通信指令センターの施設については、以下の対策を講じる。

ア　入退室管理（認証・記録）

イ　不正持ち込み・持ち出しの防止

ウ　機器の耐震・防火対策

(8) 運用体制及び教育

安定的な運用のため、次の体制を整備する。

ア　定期的な訓練（大規模災害・システム障害想定）

イ　情報セキュリティ教育（指令員向け）

ウ　インシデント発生時の報告・対応手順の明確化

(9) インシデント対応

通信指令センターにおいてインシデントが発生した場合は、次の対応を行う。

ア　迅速な初動対応（影響範囲の特定）

イ　指令機能の継続確保（代替運用への移行）

ウ　関係機関への速やかな連絡

エ　原因分析及び再発防止策の実施

オ　映像データの漏えい等が発生した場合の迅速な遮断及び影響範囲の特定

カ　インシデントの記録、分析及び再発防止策の実施

(10) 外部連携

通信指令センターは、次の関係機関との連携を考慮する。

ア　通信事業者

イ　システムベンダー

(11) 継続的改善

通信指令センターの情報セキュリティ対策については、以下を実施する。

ア　定期的な監査及び評価

イ　技術進展・脅威動向への対応

ウ　運用実績に基づく見直し