東京消防庁サイバーセキュリティ基本方針

1　目的

当庁は、行政運営上、個人情報等の重要な情報を多数取り扱っているだけでなく、都民の生命、身体、財産を火災から保護することにより、都民生活及び社会経済活動に必要不可欠なサービスを提供している。よって、これらを支える情報システムで取り扱う情報資産を様々な脅威から守り、安全性を確保することは、消防行政の安定的、継続的な運営を実現するために、当庁に課された責務である。

そのため、当庁が実施するサイバーセキュリティ対策に関する基本的な事項を定め、サイバー攻撃等の様々な脅威から、当庁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ことを本基本方針の目的とする。

また、全ての職員等は、当庁が保有する情報資産に対する脅威への対応が重大かつ喫緊の課題であることを改めて認識し、当庁におけるサイバーセキュリティ対策の推進に積極的に取り組むこととする。

2　定義

⑴　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及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑵　情報システム

当庁の運営に必要な情報処理システム及び通信システムをいう。

⑶　アプリケーション

特定の機能、目的のために設計されたソフトウェア

⑷　サイバーセキュリティ

情報資産をサイバー攻撃、情報漏えい等の脅威から保護し、機密性、完全性及び可用性を維持することをいう。

⑸　サイバーセキュリティポリシー

本基本方針及びサイバーセキュリティ対策基準をいう

⑹　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。

⑺　完全性

情報が破壊、改ざん又は消去をされていない状態を確保することをいう。

⑻　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。

⑼　内部事務系の情報システム

当庁職員が総務、警防、予防、救急業務等の内部事務を行うための情報処理システムのうち、通信環境が他の領域と分離又は分割（無害化通信）されたものをいう。

⑽　インターネット接続系の情報システム

⑼を除いた情報処理システムのうち、インターネットに接続されたものをいう。

⑾　業務用端末

職員等に対し、業務上利用することが許可された情報システムの端末装置、パソコン、モバイル端末（スマートフォン、タブレット等）等をいう。

⑿　業務用外部記録媒体

職員等に対し、業務上利用することが許可されたＵＳＢメモリ、光ディスク等の電子記録媒体をいう。

⒀　管理区域

コンピュータ室（情報システムに係る基幹機器等を設置し、専ら当該機器等の管理及び運用を行うための部屋）をいう。

⒁　準管理区域

庁舎内事務室等に設定され、情報システムに係る機器等の設置、管理及び運用を行う区域並びに業務用外部記録媒体の保管に使用される保管庫を設置している区域をいう。

⒂　ソーシャルメディアサービス

インターネット上で展開される情報メディアであって、組織、個人等による情報発信、個人間のコミュニケーション、人の結び付を利用した情報流通等の社会的な要素を含んだメディアであるブログ、ソーシャルネットワーキングサービス、動画共有サイト等のサービスをいう。

⒃　外部サービス

自組織以外の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービス（Ｗｅｂ会議サービス、ソーシャルネットワーキングサービス、検索サービス、翻訳サービス、地図サービス等）をいう。

⒄　サイバーセキュリティ事象

３の脅威により業務の遂行及びサイバーセキュリティに影響を与え得る事象の全てをいう。

⒅　サイバーセキュリティインシデント

サイバーセキュリティ事案のうち、業務の遂行を危うくする確率及びサイバーセキュリティを脅かす確率が高い事象をいう。

３　対象とする脅威

情報資産に対する脅威として、以下のものを想定し、サイバーセキュリティ対策を実施する。

⑴　不正アクセス、ウイルス攻撃、ランサムウェア攻撃、サービス不能攻撃等のサイバー攻撃及び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、サービス及び業務の停止、不正行為等

⑵　当庁が保有する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、外部サービス設定等の不備、メンテナンスの不備、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、メールの誤送信等の非意図的要因による情報資産の漏えい・破壊・消去、重要情報の詐取、サービス及び業務の停止、不正行為等

⑶　地震、落雷、火災等の災害によるサービス、業務の停止等

⑷　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

⑸　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　情報資産の適用範囲

本基本方針が対象とする情報資産は、次のとおりとする。

⑴　情報システム等

⑵　個人情報のほか、情報システム等で取り扱うデータ

⑶　情報システム等に関するシステム設計書、ネットワーク図等のシステム関連データ

5　東京都政策連携団体への指導

当庁の東京都政策連携団体に対しては、本基本方針を参考に、各団体において独自の情報セキュリティ基本方針、情報セキュリティ対策基準等を策定させるなど、必要な情報セキュリティ対策を実施するよう、東京都政策連携団体を指導監督する主管課は適正な指導を行うこととする。

6　職員等の遵守義務

職員等は、当庁が保有する情報資産に対する脅威への対応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、サイバーセキュリティポリシー、サイバーセキュリティ実施手順等を遵守しなければならない。

7　サイバーセキュリティ対策

3の脅威から情報資産を保護するために、以下のサイバーセキュリティ対策を講じる。

⑴　組織体制の確立

当庁の情報資産についてサイバーセキュリティ対策を推進する全庁的な組織体制を確立する。

⑵　情報資産の分類と管理

当庁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、サイバーセキュリティ対策を講じる。

⑶　情報システム全体の強じん性の向上

情報システム全体に対し、内部事務系の情報システム及びインターネット接続系の情報システムからなる強じん性向上対策を講じる。

⑷　物理的セキュリティ対策

サーバ、管理区域、準管理区域、通信回線、業務用端末等の管理について、物理的な

対策を講じる。

⑸　人的セキュリティ対策

サイバー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、啓発を行う等の人的な対策を講じる。

⑹　技術的セキュリティ対策

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。

⑺　運用面での対策

情報システムの監視、サイバーセキュリティポリシー等の遵守状況の確認のほか、⑻の業務委託、外部サービスを利用する際のセキュリティ確保等、サイバーセキュリティポリシーの運用面で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正に対応するため、緊急時対応体制を整備する。

⑻　業務委託及び外部サービスの利用に係る対策

当庁の業務を受託する事業者（当該事業者から派遣されている者を含む。）、公的施設の管理を行う指定管理者等（以下「委託事業者等」という。）に当該業務を行わせる場合には、当庁が定めるサイバーセキュリティ要件等、セキュリティ対策上、遵守させるべき事項を、委託事業者等の選定要件として提示する。

さらに、契約や協定等（以下「契約等」という。）の締結時等に、当庁が定めるサイバーセキュリティ要件を契約等の事項に明記し、委託事業者等において要件を満たすセキュリティ対策が確保されていることを確認し、又は、別に書面の提出を求める等の措置を講じる。

なお、外部サービスの利用に当たっては、利用に関する手順等を定めるとともに、必要に応じて、当該利用の対象とする情報について定める等、規定を整備し、対策を講じる。

8　リスク評価の実施及び年度計画の策定

サイバーセキュリティに係る内部環境及び外部環境の変化を踏まえ、当庁が保有する情報資産のサイバーセキュリティ上のリスクを評価し、リスク対応方針を策定する。

また、策定したリスク対応方針に基づき、リスク対応計画を策定する。

9　自己点検及びサイバーセキュリティに関する監査の実施

サイバーセキュリティポリシーの遵守状況を検証するため、定期的に、又は必要に応じて、自己点検及びサイバーセキュリティに関する監査を実施する。

10　サイバーセキュリティポリシーの見直し

自己点検及びサイバーセキュリティに関する監査の結果、サイバーセキュリティポリシーの見直しが必要となった場合又はサイバーセキュリティに関する状況の変化に対応するため、新たに対策が必要となった場合には、サイバーセキュリティポリシーを見直す。

11　サイバーセキュリティ対策基準の策定

７から10までに示す対策等を実施するため、具体的な遵守事項、判断基準等を定めるサイバーセキュリティ対策基準を策定する。

なお、当該対策基準は、当庁におけるサイバーセキュリティ対策の基準を定めるものであり、公にすることにより、消防行政の運営に重大な支障を及ぼすおそれがあることから、当該対策基準については、外部に対しては非公開とする。

12　サイバーセキュリティ実施手順の策定

11に定めるサイバーセキュリティ対策基準を踏まえ、サイバー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サイバーセキュリティ実施手順を策定するものとする。

なお、当該実施手順は、関連する情報システム等のサイバーセキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務の運営に重大な支障を及ぼすおそれがあることから、外部に対しては非公開とする