東京都サイバーセキュリティ基本方針

改正　令和７年３月 28 日　６デ総セ第 489 号
改正　令和７年３月 28 日　６共管会第 734 号
改正　令和７年３月 28 日　６交総第 1557 号
改正　令和７年３月 28 日　６水総企第 560 号
改正　令和７年３月 28 日　６下総企画第 373 号
改正　令和７年３月 28 日　６教総デ第 1493 号
改正　令和７年３月 28 日　６選総第 1546 号
改正　令和７年３月 28 日　６人委総第 968 号
改正　令和７年３月 28 日　６監総第 830 号
改正　令和７年３月 28 日　６議調第 389 号

目次

1　目的

東京都は、行政運営上、個人情報などの重要な情報を多数取り扱っているだけでなく、交通、水道、下水道等の公共インフラ事業を担うことにより、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や制御システム（以下「情報システム等」という。）に加え、これらで取り扱う重要な情報などの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、行政及び公共インフラ事業の安定的・継続的な運営を実現するために、東京都に課せられた責務である。

そのため、東京都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、東京都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、東京都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、東京都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

(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。

(2)　情報システム

東京都の運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

(3)　制御システム

東京都の公共インフラ事業のうち、交通、水道、下水道、公共施設等の管理に関わる制御機器類のハードウェア、ファームウェア（組み込み機器に搭載されるソフトウェアをいう。）、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

(4)　サイバーセキュリティ

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。

(5)　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。

(6)　職員等

常勤職員、非常勤職員及び派遣職員をいう。

(7)　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。

(8)　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。

(9) 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。

(10) マイナンバー利用事務（個人番号利用事務）系の情報システム

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「マイナンバー法」という。）に定められている個人番号利用事務（社会保障、地方税又は防災に関する特定の事務）又は戸籍事務等に関わる情報システムをいう。

(11) ＬＧＷＡＮ接続系の情報システム

マイナンバー利用事務系を除いた情報システムのうち、ＬＧＷＡＮに接続された情報システムをいう。

(12) インターネット接続（内部）系の情報システム

ＬＧＷＡＮ接続系の情報システムで使用する電子メール以外の電子メール、Ｗｅｂサイト管理システム、内部事務を取り扱う情報システム等のインターネットに接続された情報システムをいう。

(13) 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パソコン（仮想クライアント含む。）及びスマートフォン、タブレット等のモバイル端末等をいう。

(14) 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メモリや光ディスク等の外部記録媒体をいう。

(15) 管理区域

情報システム室（ネットワークの基幹機器及び重要な情報システム等に係る機器等を設置し、専ら当該機器等の管理及び運用を行うための部屋）及び業務用外部記録媒体の保管に使用する保管庫を設置している区域をいう。

(16) 準管理区域

庁舎内執務室用フロア内に設定され、情報システムの機器類の設置、管理運用、保管等を行う専用の区域をいう。

(17) 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、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった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。

(18) 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、ホスティングサービス等をいう。

(19) クラウドサービス

従来は手元のコンピュータに導入して利用していたソフトウェアやデータ、それらを提供するための技術基盤等を、インターネットなどのネットワークを通じて、利用できるサービスをいう。

(20) サイバーセキュリティ事象（以下「イベント」という。）

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うる事象の全てをいう。

(21) サイバーセキュリティインシデント

イベントのうち、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ほか、新たな脅威の発生に備え、最新の脅威動向を確認するなど、適切に対応する。

(1)　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侵入等の意図的な要因による東京都が保有す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のほか、内部管理の欠陥など職員等による不正行為等

(2)　東京都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

(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

４　適用範囲

(1)　行政機関の適用範囲

本基本方針が適用される範囲は、東京都組織規程（昭和 27 年東京都規則第 164 号）第８条第１項に規定する本庁の局、室、都民安全総合対策本部、スポーツ推進本部、住宅政策本部、中央卸売市場、スタートアップ戦略推進本部、収用委員会事務局及び労働委員会事務局（以下「知事部局等」という。）並びに東京都公営企業組織条例(昭和 27 年東京都条例第 81 号)第１条に定める局、教育庁、選挙管理委員会事務局、監査事務局、人事委員会事務局、議会局及び東京都職員共

済組合事務局（以下「公営企業局等」という。）とする。

⑵　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。

ア　情報システム等

イ　個人情報のほか、情報システム等で取り扱うデータ

ウ　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文書

5　地方独立行政法人等への指導

東京都が設立した地方独立行政法人及び東京都政策連携団体においては、本基本方針等を参考に、各団体等においてサイバーセキュリティ対策に係る基本方針等を策定するなど、必要なサイバーセキュリティ対策を実施するよう、所管局は適正に指導を行うこととする。

6　職員等の遵守義務

職員等は、東京都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及び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

東京都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

東京都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、マイナンバー利用事務（個人番号利用事務）系の情報システム、ＬＧＷＡＮ接続系の情報システム及びインターネット接続（内部）系の情報システムという三層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、十分な教育及び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。

(7)　運用面での対策

情報システムの監視及び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、(8)の業務委託及び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。

(8)　業務委託及び外部サービスの利用に係る対策

東京都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。）及び公的施設の管理を行う指定管理者等（以下併せて「委託事業者等」という。）に当該業務を行わせる場合には、東京都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、東京都が定めるサイバーセキュリティ要件を契約等事項に明記し、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、又は、別途、書面による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、東京都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、リスク対応計画を毎年度策定する。

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、具体的な遵守事項及び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、東京都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、東京都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、４(1)に定める行政機関の適用範囲以外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、４(1)に定める行政機関の適用範囲以外に対しては非公開とする。

附　則

本基本方針は、令和７年４月１日から施行する。