東京都サイバーセキュリティ基本方針

改正	平成27年10月27日	27総行革行第327号
改正	平成27年10月27日	27共管会第351号
	平成27年10月27日	27交総第841号
	平成27年10月27日	27水総調第316号
	平成27年10月27日	27下総総第567号
	平成27年10月27日	27教総情第283号
改正	平成27年10月27日	27選総第767号
改正	平成27年10月27日	27人委総第529号
改正	平成27年10月27日	27監総第568号
改正	平成27年10月27日	27議調第172号

1　目的

今日、インターネットを始めとする情報通信ネットワークや情報処理システムは、都民生活及び社会経済のあらゆる面で利用が拡大し、必要不可欠な社会基盤となっている。

しかし一方で、世界的規模で生じているサイバーセキュリティに対する脅威が深刻化している。特に、不正アクセスや新たな攻撃手法による重要な情報の漏えい・破壊・改ざんが後を絶たず、サイバー攻撃への対策は重大な課題である。また、操作ミス等によるシステム障害のほか、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全などにも備える必要がある。

東京都では、行政運営上、都民等の個人情報など重要な情報を多数取り扱っており、それらの情報を扱う多くの業務で情報処理システムや情報通信ネットワークの活用は必要不可欠となっている。さらに、東京都は交通、水道及び下水道の公共インフラ事業を行うなど、都民生活及び社会経済活動になくてはならないサービスを提供しており、これらを支える情報システム（以下「制御システム」という。）の安全性の確保も東京都における重大な課題である。

したがって、都民等の権利利益を守るため、また、公正な行政及び公共インフラ事業の安定的、継続的な運営のため、これらの情報資産を様々な脅威から守ることは、東京都に課せられた責務である。

このような状況の中で、東京都は、サイバー攻撃等による事故を未然に防止するとともに、万が一、被害が発生した場合であっても影響を最小限にすべく、都庁全体で発生する事象を統括し、事態に即応した対応を一元的に行う組織を設置するなど、全庁横断的に取り組む必要がある。また、すべての職員等は、情報セキュリティ対策が今日における重大かつ喫緊の課題であることをあらためて認識し、全組織を挙げて、様々な脅威に対応する必要がある。さらに、地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献する必要がある。このため、東京都サイバーセキュリティ基本方針を定め、関係組織との間において緊密な連携と情報共有を行いながら、東京都として総合的、体系的、積極的に情報セキュリティ対策を実施する。

2　セキュリティ対策の体系

東京都は、当サイバーセキュリティ基本方針に基づき、サイバーセキュリティ対策基準、情報セキュリティ安全管理措置及び情報セキュリティ実施手順を定める。

（1）サイバーセキュリティ対策基準

東京都サイバーセキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために、各情報システム等共通の最低限必要な水準として、具体的な遵守事項及び判断基準等を定めたものである。

（2）情報セキュリティ安全管理措置

サイバーセキュリティ対策基準に基づき、各局において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ものである。各局の長は、情報セキュリティ安全管理措置を策定し、これに基づき局における情報セキュリティ対策を遂行する。

（3）情報セキュリティ実施手順

サイバーセキュリティ対策基準に基づき、情報処理システムごとに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ものである。情報システム等を管理する者は、情報セキュリティ実施手順を策定し、これに基づき情報システム等を運用する。

3　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、その構成機器(ハードウエア及びソフトウエア）をいう。

（2）情報処理システム

コンピュータ、端末装置、通信回線等により、電子情報を処理するシステムをいう。

（3）情報資産

以下のものをいう。

ア　ネットワーク、情報処理システム及びこれらに関する設備、電磁的記録媒体（以下「情報システム等」という。）

イ　情報システム等で取り扱う電磁的な情報

ウ　情報システム等の仕様書及びネットワーク図等のシステム関連文書

（4）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することをいう。

ア　機密性とは、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。

イ　完全性とは、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。

ウ　可用性とは、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。

（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。

４　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、情報セキュリティ対策を実施する。

（１）東京都が保有する情報処理システム・制御システムの破壊、停止、誤動作その他の機能不全を起こし得る意図的な行為

（２）東京都が発信する情報の阻害、改ざん、なりすましその他の意図的な不正行為

（３）東京都が保有する機密情報の漏えい、詐取、窃取その他の意図的な不正行為

（４）東京都が保有する情報処理システム・制御システムの停止など機能不全を起こし得る自然災害、疾病等

（５）東京都が保有する情報処理システム・制御システムの停止など機能不全を起こし得る電力、通信などインフラの機能障害

（６）東京都が保有する情報処理システム・制御システムの停止、誤動作等を起こし得る設計・開発における不備、プログラム上の欠陥、操作・設定における誤り、メンテナンスの不備、機器故障等

（７）東京都が保有する機密情報の漏えい、滅失、法令違反等を起こし得る外部委託管理の不備、内部管理の欠陥など職員等による行為

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の監理団体においては、本基本方針を参考に各団体等において情報セキュリティポリシーを策定するなど、必要な情報セキュリティ対策を実施するよう、所管局は適切に指導を行うこととする。

６　職員等の遵守義務

職員、非常勤職員及び臨時職員は、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サイバーセキュリティポリシー及び情報セキュリティ安全管理措置等を遵守しなければならない。

７　外部委託事業者等への対策

東京都の業務を受託する事業者及び派遣職員並びに公の施設の管理を行う指定管理者に当該業務等を行わせる場合においては、セキュリティ対策上遵守させるべき事項を契約又は協定等において明記するとともに、本基本方針及び対策基準と同様の水準での情報セキュリティを確保できるよう、東京都が必要な措置をとるものとする。

８　情報セキュリティ対策

上記４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実施する。

（１）組織体制

東京都の情報資産について、総合的な情報セキュリティ対策を推進するため、東京都サイバーセキュリティ委員会及び情報セキュリティ活動を統括する組織を設置し、

全庁的な組織体制を確立する。また、情報セキュリティ対策に関し、各職層における管理者等の役割、権限及び責任を明確にする。

（２）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、当該分類に基づき情報資産の管理及び取扱い方法等について具体的に定め、実効的な情報セキュリティ対策を行う。

（３）物理的セキュリティ

サーバ、情報システム室、通信回線等及びパソコン等の情報処理機器類の管理について、物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、サイバーセキュリティ対策基準等に職員等が遵守すべき事項を明確かつ具体的に定めるとともに、十分な教育、啓発及び標的型攻撃を想定した訓練等を行うなどの人的な対策を講じる。

（５）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、標的型攻撃やサービス不能攻撃などのサイバー攻撃を含む不正アクセスへの対策等の技術的対策を講じる。

（６）サイバーセキュリティポリシーの運用

情報システム等の監視、サイバーセキュリティポリシーの遵守状況の確認、外部委託等を行う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運用上の対策を講じる。

また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応体制を整備する。

９　リスク評価の実施と年度計画の策定

情報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、情報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、リスク対応方針に基づき、情報セキュリティ活動の年度計画を策定する。

10　サイバーセキュリティポリシーの運用と年度計画の遂行

サイバーセキュリティポリシーを運用するとともに、情報セキュリティ活動の年度計画を遂行し、その進捗状況をモニタリングする。

11　情報セキュリティ監査及び自己点検の実施

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、定期的及び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。

12　サイバーセキュリティポリシーの見直し

情報セキュリティ監査若しくは自己点検の結果に基づく対応又は情報セキュリティに関する状況の変化への対応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。

附　則

この方針は、平成２７年１０月２７日から施行する。