# 東京動物園協会サイバーセキュリティ基本方針

改正　令和６年４月１日　５東動協総総第432号

目次

## 1　目的

東京動物園協会（以下「協会」という。）は、都立動物園及び水族園事業の管理運営上、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、クラウドサービスを活用した情報発信の充実や先端技術を活用した来園者サービスの向上に取り組んでいる。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、事業の安定的・継続的な運営を実現するために、協会に課せられた責務である。

そのため、協会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、協会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、協会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、協会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

協会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

協会の施設等の管理を行ううえで重要な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）情報資産

以下のものをいう。

① 情報システム等

② 個人情報のほか、情報システム等で取り扱うデータ

③ 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

（5）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。

（６）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。

（７）職員等

固有職員、東京都派遣職員、再雇用職員、嘱託員、アルバイト職員及び人材派遣をいう。

（８）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。

（９）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。

(10) 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。

(11) 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、タブレット端末等をいう。

(12) 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メモリ等の外部記録媒体をいう。

(13) 管理区域

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。

(14) 準管理区域

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。

(15) ソーシャルメディア

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。

(16) 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。

(17) 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。

## 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、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、協会が保有する情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取のほか、内部管理の欠陥など職員等による不正行為等

（2）協会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、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、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（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　東京都への情報提供

協会は東京都の政策連携団体として、東京都のサイバーセキュリティポリシーを参考に、協会のサイバーセキュリティポリシーを改定するなど、必要なサイバーセキュリティ対策を実施するとともに、改定内容を建設局の所管部署へ報告する。

## 5　職員等の遵守義務

職員等は、協会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。

## 6　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。

（１）組織体制の確立

協会の情報資産についてサイバーセキュリティ対策を４園及び総務部で推進する組織体制を確立する。

（２）情報資産の分類と管理

協会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。

（３）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。

（４）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。

（５）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。

（６）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、（７）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。

（７）業務委託及び外部サービスの利用に係る対策

協会の業務を受託する事業者及びサイバーセキュリティに関する監査を依頼する専門業者等（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、協会が

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、協会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。

## 7　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、協会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。

## 8　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。

## 9　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。

## 10　サイバーセキュリティ対策基準の策定

６から９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、協会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、都立動物園及び水族園事業の管理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は非公開とする。

## 11　サイバーセキュリティ実施手順の策定

10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、外部には非公開とする。

**附　則**

本基本方針は、令和６年４月１日から施行する。