

東京動物園協会 情報セキュリティ基本方針

改定 平成28年07月01日 28東動協総総第125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、日常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情報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。

東京動物園協会（以下「協会」という。）では、都立動物園の運営上、動物等の情報資産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。

したがって、協会の持つ情報資産を様々な脅威から守り、動物園・水族園の利用者、協会の協力者・理解者の権利利益を守るため、また、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、協会に課せられた責務である。

このような状況の中で、協会は、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、全組織を挙げて発生する事象を統括し、様々な脅威、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、全園横断的に取り組む必要がある。また、東京都との間において緊密な連携と情報共有を行いながら、協会として総合的、体系的、積極的に情報セキュリティ対策を実施する。

そのために、協会は、「情報セキュリティマネジメントシステム」を構築する。運用にあたり、『情報セキュリティポリシー』を策定する。すべての職員は、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、この『情報セキュリティポリシー』を遵守しなければならない。

2 情報セキュリティ対策の体系

『情報セキュリティポリシー』は、3つの階層に分けて策定・管理される。当情報セキュリティ基本方針に基づき、情報セキュリティ対策基準及び情報セキュリティ実施手順を定める。

(1) 情報セキュリティ基本方針

情報セキュリティ基本方針は、情報セキュリティポリシーの最上位に位置する。協会の情報セキュリティマネジメントシステムにおける方針を定めたものである。これに基づいて下層の文章を策定する。

(2) 情報セキュリティ対策基準

情報セキュリティ対策基準は、(1)の下層に位置する。情報セキュリティ対策を実施するために、各情報システム共通の最低限必要な水準として、具体的な遵守事項

及び判断基準等を網羅的に定めたものである。

(3) 情報セキュリティ実施手順

情報セキュリティ実施手順は、(2)の下層に位置する。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。

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(ハードウェア及びソフトウェア)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) 情報セキュリティポリシー

本基本方針及び情報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) 協会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し得る意図的な行為

(2) 協会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) 協会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) 協会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し得る自然災害、疾病等

(5) 協会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し得る電力、通信などインフラの機能障害

(6) 協会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) 協会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 東京都への情報提供

東京都の監理団体として、東京都のサイバーセキュリティポリシーを参考に、協会の情報セキュリティポリシーを改定するなど、必要な情報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適時適切に報告する。

6 職員等の遵守義務

固有職員、都派遣職員、再雇用職員、嘱託職員、人材派遣、アルバイトスタッフは、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情報セキュリティポリシー及び情報セキュリティ実施手順等を遵守しなければならない。(東京都から協会に派遣された者については、就業規則規程第1章第2条に基づき職員とみなす)

7 外部委託事業者等への対策

協会の業務を受託する事業者及び派遣職員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、協会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

協会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、情報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定し、全園の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

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、情報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) 情報セキュリティポリシーの運用

情報システム等の監視、情報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、情報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 情報セキュリティポリシーの運用と年度計画の遂行

情報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 情報セキュリティ自己点検の実施

情報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自己点検を実施する。

12 情報セキュリティポリシーの見直し

情報セキュリティ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、情報セキュリティポリシーを見直す。

附 則

この方針は、平成28年07月01日から施行する。