公益財団法人東京観光財団　サイバーセキュリティ基本方針

第１章　総則

（目的）

第１条　この要項は、公益財団法人東京観光財団（以下「財団」という。）が保有および活用する、情報処理システムやインターネット等の情報通信ネットワークにおいて、個人情報の漏えい、人為的原因による情報セキュリティ事故、自然災害等によるシステム障害、システム運用の機能不全などに備えるとともに、不正アクセスや、新たな通信ネットワーク攻撃等による重要な情報の破壊・改ざんといった、サイバーセキュリティに対する脅威を未然に防ぐことを目的とする。

（定義）

第２条　この要項において「ネットワーク」とは、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　この要項において「情報処理システム」とは、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　この要項において「情報資産」とは、以下のものをいう。

（１）　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。）

（２）　情報システム等で取り扱う電磁的な情報

（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

４　この要項において「情報セキュリティ」とは、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。

（１）　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。

（２）　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。

（３）　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　この要項において「サイバーセキュリティポリシー」とは、本基本方針及びサイバーセキュリティ対策基準(別紙：公益財団法人東京観光財団 サイバーセキュリティ対策基準)をいう。

（対象とする脅威）

第３条　財団は、以下のものを情報資産に対する脅威と想定し、情報セキュリティ対策を実施する。

（１）　財団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）　財団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）　財団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）　財団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）　財団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）　財団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）　財団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

（職員等の遵守義務）
第４条　職員、臨時職員及び派遣職員は、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を遵守しなければならない。

（外部委託事業者等への対策）
第５条　財団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また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、必要な措置をとるものとする。

（情報セキュリティ対策）
第６条　上記第３条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
財団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を設置し、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
財団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り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
ホストコンピュータ、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。

（情報セキュリティ自己点検の実施）
第７条　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自己点検を実施する。

（サイバーセキュリティポリシーの見直し）
第８条　情報セキュリティ自己点検の結果、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及びサイバー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

この基本方針は、平成２０年４月１日から施行する。

附 則２

この基本方針の改正は、平成２３年４月１日から施行する。

附 則３

この基本方針の改正は、平成２８年１２月１９日から施行する。