公益財団法人東京 2025 世界陸上財団サイバーセキュリティ基本方針

1　目的

本方針は、公益財団法人東京 2025 世界陸上財団（以下「当法人」という。）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、当法人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、当法人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あらためて認識し、当法人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（ハードウエア及びソフトウエア）をいう。

（2）情報システム

当法人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）情報資産

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

（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、非常勤職員及び臨時職員並びに派遣職員をいう。

（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、改ざん又は消去が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）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、モバイル端末等をいう。

（１１）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。

（１２）管理区域

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区域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。

（１３）準管理区域

事業所の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。

（１４）ＳＭＳ（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。

（１５）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または全部の機能を提供するサービス

等をいう。

（１６）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、当法人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）当法人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、外部委託管理の不備、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　適用範囲

本基本方針が適用される組織の範囲は、公益財団法人東京 2025 世界陸上財団事務局規程第２条に規定する組織とする。

５　職員等の遵守義務

職員等は、当法人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

当法人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組織体制を確立する。

（２）情報資産の分類と管理

当法人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、通信回線及び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）業務委託及び外部サービスの利用に係る対策

当法人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。）に当該業務を行わせる場合には、当法人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、協定等（以下「契約等」という。）の締結時等に、委託事業者等においても当法人が定めるセキュリティポリシーと同等のセキュリティ対策が確保されていることを、契約等事項に明記し、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、外部サービスを利用する場合には、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の規定を整備し、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、（６）の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　リスク評価の実施

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、当法人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。

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、定期的に実施の可否を判断し、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

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、当法人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、当法人の事業運営に重大な支障を及ぼすおそれがあることから非公開とする。

附　則

この基本方針は、令和５年１２月２６日から施行する。

附　則

この基本方針は、令和６年４月１日から施行する。