一般財団法人 GovTech 東京情報セキュリティ基本方針

2023 年 10 月 3 日決定
2024 年 6 月 14 日改正
2024 年 11 月 26 日改正
2025 年 11 月 4 日改正
GovTech 東京情報セキュリティ委員会決定

1　目的

本基本方針は、一般財団法人 GovTech 東京（以下「財団」という。）が実施する情報セキュリティ対策に関する基本的な事項を定め、すべてのステークホルダーの期待に応えるためにサイバー攻撃等の様々な脅威から、財団が保有する情報資産の機密性、完全性及び可用性を維持し、財団を取り巻く環境の変化を踏まえ、継続的改善に財団を挙げて取り組むことを目的とする。

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
財団の運営に必要な情報の収集、蓄積、処理、伝達及び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。

(4) 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。

(5) 職員等
職員、契約職員、非常勤職員及びインターンシップや派遣等により財団の業務に従事する職員をいう。

(6) 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。

(7) 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。

(8) 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。

(9) 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（仮想クライアント含む。）及びスマートフォン、タブレット等のモバイル端末等をいう。

(10) 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。

(11) 管理区域

サーバ室（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。

(12) 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。

(13) 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。

(14) クラウドサービス

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。なお、本基本方針におけるクラウドサービスは、財団外の一般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であって、当該サービスにおいて財団の情報が取り扱われる場合に限るものとする。

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、情報セキュリティ対策を実施するほか、事業中断・阻害要因となりうる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、財団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) 財団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 適用範囲

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

5 職員等の遵守義務

職員等は、財団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、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。

6 情報セキュリティ対策

３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制の確立

財団の情報資産について情報セキュリティ対策を推進する全体的な組織体制を確立する。

(2) 役割及び責任

組織内における情報セキュリティに関する役割と責任を明確にし、組織全体での情報セキュリティの維持と向上を図る。

(3) 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、情報セキュリティ対策を講じる。

(4) 物理的セキュリティ対策

サーバ、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。

(5) 人的セキュリティ対策

情報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。

(6) 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。

(7) 運用面での対策

情報システムの監視及び情報セキュリティポリシー等の遵守状況の確認のほか、(8)の業務委託及びクラウドサービスを利用する際のセキュリティ確保等、情報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し、効率的かつ効果的な対応を行うために、具体的な手順を定める。

(8) 業務委託及びクラウドサービスの利用に係る対策

財団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。以下「委託事業者」という。）に当該業務を行わせる場合には、財団が定める情報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、財団が定める情報セキュリティ要件を契約等事項に明記し、委託事業者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、クラウド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。

(9) システム開発・導入の管理

システム開発ライフサイクルにおいて、安全で信頼性の高いシステムを提供するため、開発プロセスの各段階で適切なセキュリティ対策を実施する。

また、情報システムの変更管理プロセスを組織内で確立し、徹底することで、変更管理におけるリスクを最小限に抑えるものとする。

(10) 法令、規制の遵守

情報セキュリティに関連する法令、規制および契約上の要求事項を遵守するため、これらの要件を特定し、文書化し、常に最新の状態を維持するものとする。違反が発見された場合は、迅速かつ適切な対応を行い、再発防止策を講じるものとする。

7　リスク評価の実施及び年度計画の策定

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、財団が保有する情報資産の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、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　自己点検及び情報セキュリティに関する監査の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて、自己点検及び情報セキュリティに関する監査を実施する。

9　情報セキュリティポリシーの見直し

自己点検及び情報セキュリティに関する監査の結果、情報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、情報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、情報セキュリティポリシーを見直す。

10　情報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情報セキュリティ対策基準を策定する。

なお、当該対策基準は、財団における情報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、財団の組織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、非公開とする。

11　情報セキュリティ実施手順の策定

10 に定める情報セキュリティ対策基準を踏まえ、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情報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情報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、非公開とする。

附　則

本基本方針は、決定の日から施行する。

附　則

本基本方針は、2024 年６月 14 日から一部改正して施行する。

附　則

本基本方針は、2024 年 11 月 26 日から一部改正して施行する。

附　則

本基本方針は、2025 年 11 月 4 日から一部改正して施行する。