公益財団法人特別区協議会情報セキュリティ基本方針

平 成 ２ ４ 年 ３ 月 １ ３ 日
２３協総企第３２１号常務理事決定

公益財団法人特別区協議会情報セキュリティ基本方針（平成23年3月18日常務理事決定）の一部を改正する。

１　目的

公益財団法人特別区協議会情報セキュリティ基本方針は、公益財団法人特別区協議会（以下「この法人」という。）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ため、この法人が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

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

コンピュータ、ネットワーク及び電磁的記録媒体（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法で作られる記録であって電子計算機による情報処理の用に供されるものに係る記録媒体をいう。）で構成され、情報処理を行う仕組みをいう。

（３）　職員等

職員（非常勤職員及び臨時職員を含む）及びその他この法人のネットワークを利用し業務を行う者をいう。

（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。

（５）　情報セキュリティポリシー

この基本方針及び公益財団法人特別区協議会情報セキュリティ対策基準をいう。

（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だけが、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。

３　対象とする脅威

情報セキュリティ対策の対象とする脅威は、次に掲げるものとする。

（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や部外者の侵入等の意図的な要因による情報資産の漏えい、破壊、改ざん、消去、重要情報の詐取、内部不正等

（２）　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又は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
（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

この基本方針が対象とする情報資産は、次のとおりとする。
（1） ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
（2） ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
（3） 情報システムの仕様書及び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、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を遵守しなければならない。

6 情報セキュリティ対策

上記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ずるものとする。
（1） 組織体制
この法人の情報資産について、情報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
この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、当該分類に応じて必要な情報セキュリティ対策を講ずるものとする。
（3） 情報システム全体の強靭性の向上
情報セキュリティの強化を目的とし、業務の効率性及び利便性の観点を踏まえ、情報システム全体に対し不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。
（4） 物理的セキュリティ
サーバ、サーバ室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講ずるものとする。
（5） 人的セキュリティ
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ずるものとする。
（6） 技術的セキュリティ
コンピュータ等の管理、アクセスの制御、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ずるものとする。
（7） 運用
情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託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の運用面の対策を講ずるものとする。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、緊急即応体制を整備する。
（8） 業務委託と外部サービス（クラウドサービス）の利用
業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認する。情報セキュリティインシデントの発生時等は必要に応じて契約に基

づき措置を講じる。
　外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定を整備し対策を講じる。
　ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9）　評価・見直し

　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情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8　情報セキュリティポリシーの見直し

　情報セキュリティ監査又は自己点検の結果、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及び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になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直すものとする。

9　情報セキュリティ対策基準の策定

　上記６から８までに規定する対策等を実施するために、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、情報セキュリティ対策基準は、公にすることによりこの法人の法人運営に重大な支障を及ぼすおそれがあることから非公表とする。

10　情報セキュリティ実施手順の策定

　情報セキュリティ対策基準に基づき、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。
　なお、情報セキュリティ実施手順は、公にすることによりこの法人の法人運営に重大な支障を及ぼすおそれがあることから非公表とする。

11　関係団体への対応

　この法人が所有するコンピュータ等を利用する関係団体（以下「関係団体」という。）対し、関係団体が所掌する情報資産及び情報システムについて、この基本方針の趣旨に即した情報セキュリティを確保するため、必要な措置を講じさせるものとする。
　なお、関係団体へこの法人の情報資産及び情報システムにかかわる業務を委託する場合又は関係団体にこの法人の保有するネットワークの利用を認める場合は、当該業務に関する情報セキュリティ責任者の指定など情報セキュリティに関する協定を締結することとする。

12　その他

　この基本方針に定めるもののほか、基本方針の施行に関し必要な事項は、別に定める。

附　則

この基本方針は、平成２４年４月１日から施行する。

附　則

この基本方針は、令和４年４月１日から施行する。

附　則

この基本方針は、令和８年４月１日から施行する。