東京電子自治体共同運営協議会

情報セキュリティ基本方針

平成２２年２月９日

東京電子自治体共同運営協議会情報セキュリティ基本方針

1　目的

東京都内の地方公共団体は、相互に協力・連携して住民サービスの向上と行政の高度化・効率化を図ることを目的として、東京電子自治体共同運営協議会（以下「協議会」という。）を設置し、電子申請・電子調達サービス等の共同運営事業（以下「共同運営事業」という。）に取り組んでいる。

共同運営事業の実施に当たっては、最新の情報通信技術を活用しつつ、住民の個人情報や事業者の経営情報などの多くの重要な情報を取り扱っている。

一方、情報システム等は、個人情報の漏えい、不正アクセス等による情報資産の破壊・改ざん、操作ミス等の人為的な原因や自然災害によるシステム障害の発生など、様々な脅威にさらされている。

このため、共同運営事業に携わるすべての組織及びその職員（非常勤・臨時職員、派遣職員、受託事業者の従業員等を含む。以下「職員等」という。）は、相互に協力・連携し情報共有を図りながら、こうした脅威から情報資産を防御し、住民の権利・利益を守るとともに共同運営事業の安定的な運営を確保する責務を課せられている。

そこで、共同運営事業における情報セキュリティ対策の基本的事項を定めるため、本基本方針を策定する。

2　情報セキュリティ対策の体系

（1）情報セキュリティポリシー

本基本方針及び（2）により策定する情報セキュリティ対策基準をもって、協議会の情報セキュリティポリシーとする。

（2）情報セキュリティ対策基準

協議会は本基本方針に基づき、協議会及びその会員である東京都、区市町村その他の地方公共団体（以下「会員団体」という。）、並びに会員団体との委託契約に基づき共同運営事業のサービスを提供する者（以下「サービス提供事業者」という。）の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。

（3）情報セキュリティ実施手順

協議会、会員団体及びサービス提供事業者は、情報セキュリティ対策基準に基づき、共同運営事業の実施に当たっての情報セキュリティ対策の具体的な手順を定める情報セキュリティ実施手順を策定し、これに基づき情報システム等を管理・運用する。

3　定義

（1）情報システム等

共同運営事業によるサービスを提供するための情報処理システム及び情報通信ネットワークをいう。

（2）情報資産

情報システム等を構成する設備・機器、記録媒体、情報システム等で取り扱う電磁的な情報、情報システム等の仕様書、ネットワーク構成図その他の関係文書をいう。

（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。

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、情報にアクセスすることができる状態を確保することをいう。

4　対象とする脅威

情報資産に対する脅威として、以下に掲げるものを想定し、情報セキュリティ対策を実施する。

（1）部外者の侵入、不正アクセス、コンピュータウィルス攻撃、サービス不能攻撃等による情報資産の漏えい、破壊、改ざん、消去等

（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、プログラム上の欠陥、操作ミス、故障等による情報資産の漏えい、破壊、消去等

（3）地震、落雷、火災、風水害等の自然災害や停電等によるサービスの停止、情報資産のき損、喪失等

5　職員等の遵守義務

共同運営事業に携わるすべての職員等は、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

（1）組織体制

共同運営事業に関する情報資産について、総合的な情報セキュリティ対策を推進するため、協議会に情報セキュリティ委員会を設置する。また、情報セキュリティ対策に関し、協議会、会員団体及びサービス提供事業者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

共同運営事業に関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行う。

（3）物理的セキュリティ

情報システム等を構成するデータセンター、サーバ、通信回線、端末機等の設備・機器の管理について、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、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

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）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じるものとする。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、障害時・災害時等における対応方針を策定する。

7　情報セキュリティ監査等の実施

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及び自己点検の結果、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となった場合には、協議会は情報セキュリティポリシーを見直す。