情報セキュリティ基本方針

公益財団法人　神奈川県都市整備技術センター

本　　所　神奈川県茅ヶ崎市汐見台１番７号
県央支所　神奈川県厚木市田村町２の２８

情報セキュリティ基本方針

近年のインターネットをはじめとする情報通信ネットワークの急速な発展は、公益財団法人神奈川県都市整備技術センター（以下「技術センター」という。）の業務の効率化等に大きな変化をもたらしています。

しかしながら、一方では不正アクセスやコンピュータウイルスなどによる情報資産の破壊や改ざん、情報漏えいなどの脅威も顕著になってきており、この様な脅威から情報資産を防御保護することは、技術センターの安定的、継続的な業務運営のために必要不可欠となっています。

そこで、技術センターでは、情報セキュリティポリシーを策定し、そのポリシーに基づき情報セキュリティ対策を積極的に推進してまいります。

１　趣旨

本情報セキュリティ基本方針は、技術センター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に、技術センター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ここに定める。

２　用語の定義

（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、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報資産

情報そのものと情報システムの両方を指すもので、資料等も含まれる。

（３）情報システム

ハードウェア、ソフトウェア、ネットワーク及び電磁的記録媒体で構成される情報を処理するための仕組みをいう。

（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。

①機密性　許可された者だけが情報にアクセスできることを確実にこと。

②完全性　保有する情報が正確で、しかも完全である状態を保持すること。

③可用性　許可された者が必要な時にいつでも情報にアクセスできること。

（５）電磁的記録媒体

情報システムによる情報処理の用に供されるもので、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ等をいう。

（６）情報セキュリティポリシー

技術センターが所有する情報資産の情報セキュリティ対策について、総合的・体系的かつ具体的にとりまとめたもので、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」からなる。

3　対象とする脅威

（1）情報資産への脅威

次の脅威を想定し、情報セキュリティ対策を実施する。

① 誤操作又は故意の不正アクセス（ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報又はプログラムの持出し、盗聴、改ざん及び消去、機器及び電磁的記録媒体の盗難、正規の手続きによらない端末の接続による情報漏えい等）。

② 地震、落雷、火災等の災害及び事故、故障等による業務の停止。

4　適用範囲

（1）範囲

技術センターの全ての部署に本情報セキュリティ基本方針が適用される。

（2）情報資産の範囲

① ネットワーク、情報システム及びこれに関する設備、電磁的記録媒体。

② ネットワーク及び情報システムで取扱う情報（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　情報セキュリティ対策

技術センターは、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じる。なお、（2）～（6）の各対策は、情報セキュリティ関連法案やその他規範に適合するよう定める。

（1）組織体制

情報セキュリティ管理責任者を設置し、情報セキュリティに取組むための体制を構築する。

（2）情報資産の分類と管理

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。

（3）物理的セキュリティ

サーバ等の管理、管理区域の入退管理、ネットワーク・装置の管理、職員等のパソコン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

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、緊急時対応計画を策定する。

６　情報セキュリティ対策基準の策定

上記６のセキュリティ対策を実施するために、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、公表することにより技術センターの業務実施に重大な影響を及ぼす恐れがあることから非公開とする。

７　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、公表することにより技術センターの業務実施に重大な影響を及ぼす恐れがあることから非公開とする。

８　情報セキュリティ監査の実施

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情報セキュリティ監査を実施する。

９　情報セキュリティポリシーの見直し

情報セキュリティに関する状況の変化に対応するため、定期的に情報セキュリティポリシーを見直すものとする。