

情報セキュリティに関する基本要綱

大阪府の情報セキュリティに関する基準（平成14年4月1日制定）の全部を改正する。

第1部 基本方針

（目的）

第1条 この要綱は、大阪府電子計算機、情報通信ネットワーク及び情報システム管理運用規程（平成8年大阪府訓令第38号。以下「管理運用規程」という。）第3条及び第6条並びに大阪府行政情報化推進基本要綱（以下「推進基本要綱」という。）第3条の規定に基づき、情報セキュリティを確保するために遵守すべき基本的事項を定める。

（定義）

第2条 この要綱における用語の意義は、管理運用規程及び推進基本要綱に定めるもののほか、次の各号に定めるところによる。

- (1) 事業者 府との委託契約等により情報システム又は情報通信ネットワーク（以下「情報システム等」という。）の開発等を行う者をいう。
- (2) 端末機 事務処理等を行うために職員や室課等に配備された電子計算機等をいう。
- (3) ID 情報システム等の利用者を識別するための文字列情報をいう。
- (4) パスワード 情報システム等の利用者がIDによる認証を得るため入力する文字列情報をいう。
- (5) 不正アクセス 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）第2条第4項による不正アクセス行為をいう。
- (6) 不正プログラム 情報システム等に対して不正かつ有害な動作を行う意図で作成されたプログラムをいう。
- (7) 情報資産 情報及び情報の管理や運用を行う仕組みをいう。
- (8) 情報セキュリティ 情報資産の機密性（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。）、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。）及び可用性（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。）を維持することをいう。
- (9) 個人番号利用事務系 個人番号利用事務（社会保障、地方税若しくは防災に関する事務）に関わる情報システム及びその情報システムで取り扱うデータをいう。
- (10) LGWAN接続系 LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう（個人番号利用事務系を除く。）。
- (11) インターネット接続系 個人番号利用事務系、LGWAN接続系以外の情報システム及びその情報システムで取り扱うデータをいう。
- (12) 通信経路の分割 LGWAN接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。
- (13) 無害化通信 危険因子を除去、端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

（対象とする脅威）

第3条 情報資産に対する脅威として、次の各号を想定する。

- (1) 情報システム等の不正利用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、情報システム等の設計・開発・運用・保守等の不備、情報システム等に関する内部・外部監査機能や委託管理の不備、機器故障等の非意図的な要因による情報

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情報システム等の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴う情報システム等の運用不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等による情報システム等の停止等

(適用範囲)

第4条 この要綱は、部局等に適用する。

(職員の遵守義務)

第5条 職員は、情報セキュリティ対策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はこの要綱を遵守しなければならない。

(情報セキュリティ対策)

第6条 第3条で想定する脅威から情報資産を保護するために、次の各号に掲げる対策を講じる。

- (1) 組織体制 本府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庁的な組織体制を確立する。
- (2) 情報資産の分類と管理 本府の保有する情報資産を重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。
- (3) 情報システム全体の強靱性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。
 - イ 個人番号利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。
 - ロ LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。
 - ハ インターネット接続系においては、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。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。
- (4) 物理的セキュリティ対策 情報システム等が稼動する機器等の管理について、物理的な対策を講じる。
- (5) 人的セキュリティ対策 情報セキュリティ対策に関し、職員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 不正アクセス対策等の技術的対策を講じる。
- (7) 運用 情報システムの監視、この要綱の遵守状況の確認、外部委託を行う際のセキュリティ確保等、この要綱の運用面の対策を講じるものとする。
- (8) 外部サービスの利用 外部委託する場合には、外部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、外部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し、必要に応じて契約に基づき措置を講じる。
 - イ 約款による外部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。
 - ロ 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。

(情報セキュリティ対策に関する監査及び自己点検の実施)

第7条 この要綱の遵守状況を検証するため、必要に応じて情報セキュリティ対策に関する監査及び自己点検を実施する。