情報セキュリティ基本要綱

（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、管理運用規程に定めるもののほか、次の各号に定めるところによる。

⑴　部局等

部局、地方自治法（昭和 22 年法律第 67 号）第 180 条の５第１項に規定する委員会及び委員の事務局、同法第 180 条の５第２項第２号から第５号に規定する委員会の事務局及び地方自治法第 138 条第１項に規定する議会事務局をいう。

⑵　室課等

部局等における室、課及び出先機関をいう。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　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。

⑼　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。

⑽　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。

⑾　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。

⑿　個人番号利用事務系（マイナンバー利用事務系）

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）又は戸籍事務等に関わる情報システム及びデータをいう。

⒀　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。)。

⒁　インターネット接続系

インターネット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。

⒂　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。

⒃　無害化通信

インターネットメールの添付ファイルの無害化や端末機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ない等、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、以下の脅威を想定し、情報セキュリティ対策を実施する。

⑴　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

⑵　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、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

⑶　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

⑷　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

⑸　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

（適用範囲）

第４条　本情報セキュリティポリシーは、部局等に適用する。

２　本情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。

⑴　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

⑵　ネットワーク及び情報システムで取り扱う情報

⑶　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

（職員の遵守義務）

第５条　職員（非常勤職員及び臨時職員等を含む。以下同じ）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。

（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。

⑴　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。

⑵　情報資産の分類と管理

本府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実施する。

⑶　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・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

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、端末機からの情報持ち出し不可設定や端末機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、本府及び府内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。

⑷　物理的セキュリティ

サーバ、情報システム室、通信回線及び職員のパソコン等の管理について、物理的な対策を講じる。

⑸　人的セキュリティ

情報セキュリティに関し、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。

⑹　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。

⑺　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じるものとする。

⑻　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、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、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　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。

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。

⑼　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。

（情報セキュリティ監査及び自己点検の実施）

第７条　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。

（情報セキュリティポリシーの見直し）

第８条　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、リスクを検討したうえで、情報セキュリティポリシーを見直す。

（情報セキュリティ対策基準の策定）

第９条　前３条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。

（情報セキュリティ実施手順の策定）

第10条　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ものとする。

２　情報セキュリティ実施手順は、公にすることにより本府の行政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。