京田辺市情報セキュリティに関する規程（抜粋）

第１章　総則

（目的）

第１条　この訓令は、市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、市が実施する情報セキュリティ対策の基本的な方針及び対策の基準を定めることを目的とする。

（定義）

第２条　この訓令において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（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で構成され、情報処理を行う仕組みをいう。

（３）　情報資産　情報システムで取り扱う全ての情報（紙等の有体物に出力された情報を含む。）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　この訓令に規定する情報セキュリティ基本方針及び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。

（９）　マイナンバー利用事務系　個人番号利用事務（社会保障、地方税又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。

（１０）　ＬＧＷＡＮ接続系　総合行政ネットワーク（以下「ＬＧＷＡＮ」という。）に接続された情報システム及び当該情報システムで取り扱うデータ（マイナンバー利用事務系を除く。）をいう。

（１１）　インターネット接続系　インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及び当該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接続系及び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　インターネットメール本文のテキスト化、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ない等、安全が確保された通信をいう。

（１４）　職員　地方公務員法（昭和２５年法律第２６１号）第３条第２項に規定する一般職に属する職員並びに同条第３項第１号及び第３号に規定する特別職に属する職員をいう。

（１５）　外部委託事業者　情報資産に関係する開発、導入、保守等により業務を委託した全ての業者をいう。

（１６）　電算室　ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行い、電磁的記録媒体を保管する部屋をいう。

（１７）　情報セキュリティインシデント　情報資産について安全保障上の脅威となる事象をいう。

第２章　情報セキュリティ基本方針

（適用範囲）

第３条　この訓令が対象とする機関の範囲は、市長とする。

（対象とする脅威）

第４条　情報資産に対して想定される脅威は、次のとおりとする。

（１）　不正アクセス、ウイルス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、操作ミス、設定ミス、メンテナンス不備、外部委託管理の不備、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

（４）　大規模又は広範囲にわたる疾病による人員不足に伴うシステム運用の機能不全等

（５）　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

（職員等の遵守義務）

第５条　職員及び本市の業務環境を利用する外部委託事業者（以下「職員等」という。）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　市長は、保有する情報資産を第４条に規定する脅威から保護するため、次に掲げる情報セキュリティ対策を実施する。

（１）　組織体制　市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　市が保有する情報資産を機密性、完全性及び可用性を踏まえてその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じん性の向上　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、次に掲げる３段階の対策を講じる。

ア　マイナンバー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、端末への多要素認証（知識情報、所持情報及び生体情報のうち、２つ以上の要素を利用する認証をいう。）の導入等により、住民情報の流出を防ぐ。

イ　ＬＧＷＡＮ接続系においては、ＬＧＷＡＮに接続する情報システム及びインターネット接続系の情報システム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。

ウ　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、京都府及び京田辺市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　サーバ、電算室、通信回線、情報端末等の管理について、物理的な対策を講じる。

（５）　人的セキュリティ　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。

（６）　技術的セキュリティ　情報システムの管理、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な対策を講じる。

（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、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。

（８）　業務委託　業務委託を行う場合には、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、必要に応じて措置を講じる。

（９）　外部サービスの利用　外部サービス（以下「クラウドサービス」という。）を利用する場合には、利用に係る規定を整備し対策を講じる。

（情報セキュリティ監査及び自己点検の実施）

第７条　市長は、情報セキュリティポリシー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　市長は、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新たに対策が必要になった場合には、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準の策定）

第９条　市長は、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策定する。