# 福津市情報セキュリティ基本方針

第1条（目的）

この基本方針は、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について基本的な事項を定め、国の方針に基づくネットワーク構成の見直しを踏まえた情報セキュリティ対策を講じることを目的とする。

第2条（定義）

この基本方針において、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 次に定めるとおりとする。
   （1） ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体（以下「情報システム等」という。）
   （2） 紙文書
   （3） 情報システム等及び紙文書で取り扱う情報
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 この基本方針及び別に定める情報セキュリティ対策基準、情報セキュリティ実施手順、情報セキュリティ運用基準をいう。
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。
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。
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（マイナンバー利用事務系を除く。）。
11. 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。
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うえで、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や端末への画面転送等により、コンピュータウィ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。

第3条（対象とする脅威）

情報資産に対する情報セキュリティ対策の実施に当たり、対象とする脅威は、次の各号に掲げるとおりとする。

1. サイバー攻撃（不正アクセス、ウイルス攻撃、サービス不能攻撃等をいう。）、不正な部外者の侵入、その他の意図的な要因による情報資産の漏えい、破壊、改ざん、消去等

2. 情報資産の無断持ち出し、管理不備、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、保守・管理の不備、機器故障その他の非意図的要因による情報資産の漏えい、破壊、改ざん、消去等

3. 地震、落雷、火災その他の災害によるサービス及び業務の停止、情報資産の消失等

4. 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

5. 電力供給、水道供給及び通信の途絶等のインフラの障害からの波及

6. その他情報セキュリティを脅かす事案

第4条（適用範囲）

この基本方針の適用範囲は、本市が保有する情報資産、情報資産に関する事務に携わる全ての職員、非常勤職員、会計年度職員、任期付き職員、労働者派遣事業等により本市の事務に携わる者（以下「職員等」という。）とする。

第5条

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対策基準及び別に定める情報セキュリティ実施手順並びに情報セキュリティ運用基準を遵守しなければならない。

第6条（委託等に伴う措置）

委託等により、業務において市が保有する情報資産を職員以外の者に利用させる場合は、情報セキュリティポリシーと同等以上の水準での情報セキュリティを確保できるよう、契約等において必要な措置を講じるものとする。 また、業務において市が保有する情報資産を利用する職員等以外の者は、当該業務の範囲において情報セキュリティポリシーを遵守するものとする。

第7条（情報セキュリティ対策）

第3条に規定する脅威から情報資産を保護するために講じる情報セキュリティ対策は、次の各号に掲げる区分に応じ、当該各号に定めるとおりとする。

1. 組織体制　市の保有する情報資産について、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ものとする。

2. 情報資産の分類及び管理　市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行うものとする。

3. 情報システム全体の強靭性の向上　情報システム全体に対し、次の三段階の対策を講じる。

（1）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うえで、端末からの情報持ち出し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。

（2）LGWAN 接続系においては、通信経路の分割を原則とした上で、業務上必要な範囲に限り、適切な認証及びアクセス制御等の措置を講じた場合には、インターネットを経由した外部サービスの利用を認める。

（3）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、県と市区町村のインターネット接続口を集約した、自治体情報セキュリティクラウド等を経由する。

4．物理的セキュリティ　サーバ、情報システム室、通信回線、パソコン等の管理について、物理的な対策を講じるものとする。

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別に定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じるものとする。

6．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ものとする。

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ものとする。この場合において、情報資産に対するセキュリティ侵害が発生した場合等には、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ものとする。

8．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、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、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。外部サービス（クラウドサービス）を利用する場合には、責任分界を踏まえ、市が管理すべき範囲について必要な対策を講じる。

9．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、適宜行う。

第8条（情報セキュリティ監査及び自己点検の実施）

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ものとする。

第9条（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等、必要に応じて見直すものとする。

第10条（情報セキュリティ対策基準の策定）

この基本方針に基づいた情報セキュリティ対策等を実施するために、具体的な遵守事項、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ものとする。情報セキュリティ対策基準は、公にすることにより市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、外部に周知すべき事項を除いて原則非公開とする。

第11条（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ものとする。情報セキュリティ実施手順は、公にすることにより市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、原則非公開とする。

附　則

この基本方針は、令和8年2月2日から施行する