情報セキュリティ基本方針

４．０版

松　　山　　市

■新規発行／改定記録

発行／改定年月日	版数	文書の新規発行／改定内容	備考
平成 15 年 6 月 16 日	1.0	新規発行	
改定 平成 25 年 4 月 1 日	2.0	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定（平成 22 年 11 月版）に伴う全面改定	施行 平成 26 年 1 月 1 日
改定 平成 26 年 10 月 29 日	2.1	「松山市電子行政組織の管理運営に関する規則」の全部改正に伴う一部改定	
改定 平成 27 年 9 月 1 日	2.2	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定（平成 27 年 3 月版）に伴う一部改定	
改定 平成 28 年 3 月 23 日	3.0	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定（平成 27 年 3 月版）に伴う全面改定	施行 平成 28 年 7 月 1 日
改定 平成 31 年 3 月 22 日	3.1	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定（平成 30 年 9 月版）に伴う一部改定 ・情報セキュリティ対策基準改定による改定版数に合わせる。	施行 平成 31 年 4 月 1 日
改定 令和 2 年 3 月 25 日	3.2	「地方公務員法及び地方自治法の一部を改正する法律（平成 29 年法律第 29 号）」に伴う一部改定 ・情報セキュリティ対策基準改定による改定版数に合わせる。	施行 令和 2 年 4 月 1 日
改定 令和 3 年 3 月 24 日	4.0	「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定（令和 2 年 12 月版）に伴う全面改定	施行 令和 3 年 6 月 1 日

情報セキュリティ基本方針

情報セキュリティ基本方針

1　目的

本市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報及び情報を取り扱うネットワーク及び情報システム等を様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが本市に対する市民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるＩＴ革命の進展により、市民生活においても高度情報化が急速に普及し、電子市役所の実現に対する市民ニーズも高まりをみせてきている。このような状況において本市が電子行政サービスを提供するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、本市の情報資産の機密性、完全性及び可用性を維持するための情報セキュリティ対策を整備するために情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

○機密性（confidentiality）：情報にアクセスすることが認められた者だけが、アクセスできる状態を確保することをいう。
○完全性（integrity）　　：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。
○可用性（avai1ability）　：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。

2　定義

（1）ネットワーク

本市における市長部局、各行政委員会事務局（ただし、教育委員会が管轄する小・中学校は除く）、議会事務局、消防局、公営企業局及び一部事務組合に設置された電子計算機を相互に接続するための通信網その他の機器（ハードウェア及びソフトウェア）で構成された情報伝達を行う仕組みをいう。

（2）情報システム

電子計算機及び記録媒体で構成された事務処理を行う仕組み並びにこれらを相互に接続するための通信網その他の機器をいう。

（３）情報資産

情報システム、これらに関する施設・設備、外部記録媒体、情報システムで取り扱う情報、情報システムの仕様書及びネットワーク構成図等のシステム関連文書をいう。

（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。

３　情報セキュリティポリシーの位置付けと職員及び委託事業者の義務

情報セキュリティポリシーは、本市が所掌する情報資産に関する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取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

したがって、市長をはじめとして本市が所掌する情報資産に関する業務に携わる職員及び委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに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する義務を負うものとする。

４　情報セキュリティ管理体制

本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ため、副市長を最高情報セキュリティ責任者（Chief Information Security Officer）とする管理体制を確立するものとする。

５　情報資産の分類

本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。

６　情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（１）部外者の侵入による情報資産の破壊・盗難、不正プログラム又は不正アクセスによる情報資産の漏洩・破壊・盗聴・改ざん・消去等

（２）職員又は委託事業者による情報資産の持出、誤操作、アクセスのための認証情報又はパスワードの不適切管理、不正アクセス又は不正行為による漏洩・破壊・盗聴・改ざん・消去等、搬送中の事故等による情報資産の盗難、許可外の端末接続によるデータ漏洩等

（３）コンピュータウイルス、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

7　情報セキュリティ対策

上記６で示した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ものとする。

（１）情報資産の管理

機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じて取るべき管理方法を規定し、セキュリティ対策を講じる。

（２）物理的セキュリティ対策

サーバ、情報システム室、通信回線及び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。

（３）人的セキュリティ対策

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。

（４）技術的セキュリティ対策

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な対策を講じる。

（５）運用におけるセキュリティ対策

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、危機管理、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　情報セキュリティ対策基準の策定

本市の様々な情報資産について、上記 7 の情報セキュリティ対策を講じるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

9　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を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定める必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、各課等長が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティポリシー（情報セキュリティ対策基準）及び情報セキュリティ実施手順は、公開することにより本市の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。

１０　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、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。

１１　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及び情報セキュリティに関する状況の変化に対応するため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。