薩摩川内市情報セキュリティポリシー

平成１７年　４　月２５日　制　　定
平成２７年　７　月　１　日　全面改正
平成３０年　６　月２０日　一部改正

薩摩川内市情報セキュリティ委員会

薩摩川内市情報セキュリティポリシーの構成

薩摩川内市情報セキュリティポリシー（以下「セキュリティポリシー」という。）とは、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を総称する。セキュリティポリシーは、本市の情報資産を取り扱う職員、嘱託員、臨時職員（以下「職員等」という。）及び外部委託事業者に浸透・普及・定着させるものであり、安定的な規範であることが要請される。

しかしながら一方では、情報処理・通信技術等の進展に伴う情報セキュリティを取り巻く急速な状況の変化に柔軟に対応することも必要である。

このようなことから、セキュリティポリシーを一定の普遍性を備えた部分である『基本方針』と、情報資産を取り巻く状況の変化に適切に対応する部分『対策基準』に分けて策定することとする。

具体的にはセキュリティポリシーを、

⑴　情報セキュリティ基本方針

⑵　情報セキュリティ対策基準

の２階層から成るものとして策定することとする。また、セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の実施手順（運用マニュアル）として、『情報セキュリティ実施手順』を策定することとする（下表参照）。

文　書　名		内　　容
薩摩川内市情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		ネットワーク及び情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

情報セキュリティ基本方針

１　目的

本市が取り扱う情報資産には、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、情報資産、情報資産を取り扱うネットワーク及び情報システム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及び安定した行政サービスの実施を確保するためにも必要不可欠である。ひいては、このことが本市行政運営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、電子商取引の発展や電子政府・電子自治体の構築が現実のものとなっている。本市が電子自治体の構築を推進するためには、本市の全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』(注)を維持するための対策『情報セキュリティ対策』を整備するために、『薩摩川内市情報セキュリティポリシー』を定めることとし、情報セキュリティ対策に最大限取り組むこととする。このうち、『情報セキュリティ基本方針（以下「基本方針」という。）』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、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。

(注)：国際標準化機構（ＩＳＯ）が定めるもの（ＩＳＯ7498-2：1989）

機密性(confidentiality)：　情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性（integrity）：　情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性（availability）：　許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２　定義

⑴　適用範囲

ア　出先機関を含む市長部局、水道局、消防局、議会事務局、各行政委員会（各教育機関は、事務室及び職員室のみ）及び薩摩川内市公益的法人等への職員の派遣等に関する条例施行規則第２条に定められた法人に適用する。

イ　情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

㈠　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

㈡　ネットワーク及び情報システムで取り扱う情報（これらが記載された文書を含む。）

㈢　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

⑵　ネットワーク

本市における課所等を相互に接続するための通信網、その構成機器（ハードウエア及びソフトウエア）及び記録媒体で構成され、処理を行う仕組みをいう。

⑶　情報システム

業務系の電子計算機（業務系におけるネットワーク、ハードウエア及びソフトウエア）及び記録媒体で構成され、処理を行う仕組みをいう。

⑷　情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。なお、情報資産には紙等の有体物に出力された情報も含まれる。

⑸　情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状

態を維持することをいう。

⑹　用語

ア　副市長　企画政策部を担任する副市長

イ　部局長　薩摩川内市の組織及びその任務に関する条例第２条に定める組織の長及び議会事務局長

ウ　特定職　薩摩川内市事務分掌規則第１３条に定める職

エ　支所長　薩摩川内市支所設置条例別表に定める支所の長

オ　課長等　薩摩川内市の組織及びその任務に関する条例第２条に定める組織に置かれる課及び室の長及び薩摩川内市事務分掌規則第９条に定める課の長並びに会計課長、選挙管理委員会事務局長、監査事務局長、農業委員会事務局長及び議事調査課長

カ　部局総括課長等

薩摩川内市事務分掌規則第１５条に定める部局総括課の長並びに行政改革推進課長、消防総務課長、教育総務課長、水道管理課長、議事調査課長及び文書法制室長

3　セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

セキュリティポリシーは、本市の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、本市の情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たって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、管理職及び各部・支所・課、機関の長が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

5　情報資産の分類と管理

情報資産を、その重要度に応じて分類し、それに応じた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

情報セキュリティ対策を講ずる上で、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。

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、重要情報の搾取、内部不正等

⑵　情報資産の無断持ち出し、無許可ソフトウエアの使用等の既定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンスの不備、内部・外部監査機能の不備、外部委託管理の不備、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

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ずることにより、セキュリティポリシーの実効性を確保するものとする。

⑴　物理的セキュリティ対策

サーバ等、サーバ室等、通信回線等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。

⑵　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等及び外部委託事業者にセキュリティポリシーの内容を周知徹底するため、十分な教育及び啓発が講じられるように必要な対策を講ずる。

⑶　技術的セキュリティ対策

コンピュター等の管理、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。

⑷　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。また、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。

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ずるに当たっては、職員等が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（以下「対策基準」という。)』を策定する。

9　情報セキュリティ実施手順の策定

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は、個々の情報資産の対策手順を具体的に定めていく必要がある。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対策基準の基本的な要件に基づき、『情報セキュリティ実施手順』を策定するものとする。なお、セキュリティポリシーのうち、『対策基準』及び『情報セキュリティ実施手順（以下「実施手順」という。)』は、公に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

セキュリティポリシーが遵守されていることを検証するため、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。

11　評価及び見直しの実施

情報セキュリティ監査の結果等により、セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報システムの変更や新たな脅威等、情報セキュリティを取り巻く状況の変化を踏まえて、適宜セキュリティポリシーの見直しを実施する。