南あわじ市
情報セキュリティ基本方針

改訂版

＜ 目　　次 ＞

第１編　目的

南あわじ市が取扱う情報資産には、個人のプライバシーに関わる情報を始め、行政運営上重要な情報が多数存在し、毀損、滅失あるいは部外に漏洩等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。このため、南あわじ市の行政サービスの対象となる個人・企業・団体への安心で安全な生活を確保・維持するために、その規模に応じた最適な情報セキュリティ対策が必須となる。

南あわじ市が保有する情報資産の機密性、完全性及び可用性(注)の維持を図るため、物理的脅威、技術的脅威及び人的脅威等、あらゆる脅威に対する予防・抑止・発見・回復のための方策について、組織的かつ計画的に取り組まなければならない。

また、情報セキュリティ対策を確実なものとするため、南あわじ市の行政に関わる関係者全てがこの情報セキュリティ基本方針を理解・遵守しなければならない。これは、行政を安全かつ安定的に継続させることを確実にするためにも必要不可欠である。

本書は、情報セキュリティを実践するにあたり、基本的な考え方及び方針を定め、南あわじ市における情報資産の管理を徹底することを目的とする。

（注）

【機密性：Confidentiality】

アクセスを許可された者だけが、情報にアクセスできることを確実にすること。

【完全性：Integrity】

情報及び処理方法が正確であること及び完全であることを保護すること。

【可用性：Availability】

認可された利用者が、必要なときに情報及び関連する資産にアクセスできることを確実にすること。

第２編　情報セキュリティポリシーの位置付け

基本方針と対策基準から構成される、情報セキュリティポリシーは、南あわじ市が管理する情報資産に関する情報セキュリティ対策の原理、原則を定めるものであり、情報セキュリティ対策の頂点に位置するものである。

第 3 編　用語の定義

以下の用語の定義は、情報セキュリティ管理・運用で使用する全ての文書に適用される。

(1) 情報システム

電子計算機（ハードウェア及びソフトウェアをいう。）、電子計算機を相互に接続するための通信網及び電子記録媒体（磁気ディスク、磁気テープ、光ディスクその他の電子情報を保管する記録媒体をいう。）により構成される情報を処理する仕組みをいう。

(2) 情報資産

情報システム及び情報が保存されているあらゆる形式の媒体をいう。

(3) 情報セキュリティ

情報資産が次に掲げる状態にあるよう維持することをいう。

ア　許可された者のみが、情報にアクセスできること。

イ　情報が破壊、改ざん又は消去されていないこと。

ウ　利用を認められた者のみが、必要なときに中断することなく情報を利用できること。

(4) 職員等

南あわじ市職員、非常勤職員及び臨時職員等のこと。

(5) 脅威

情報資産に何らかの障害又は影響を与える原因となるもの。

(6) 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、住民情報系のネットワークに関わる情報システム及びデータをいう。

(7) LGWAN 接続系

人事給与､財務会計及び文書管理等 LGWAN に接続された内部情報系のネットワークに関わる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。

(8) 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その情報システムで取り扱うデータをいう。

(9) 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。

(10) 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、コンピュータウイ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 4 編　適用範囲

情報セキュリティ基本方針は、南あわじ市の庁内情報ネットワークに接続する情報資産に適用する。

第 5 編　適用対象者とその責務

情報セキュリティ基本方針の適用対象者は南あわじ市の保有する情報資産を利用する全ての職員等であり、情報セキュリティ基本方針の定める事項を理解し、遵守する責務を負う。

(1) 管理責任権限を有する職員等

管理責任権限を有する職員等の意思決定は、情報セキュリティ基本方針に背反するものであってはならず、職員等に対して情報セキュリティ基本方針に違反する行為を命じてはならない。

(2) 職員等の責務

職員等は情報セキュリティポリシーを遵守する責務を負う。

第６編　情報セキュリティ対策の体系

南あわじ市の情報セキュリティの管理・運用で使用する文書・記録の体系は以下のとおりとする。

(1) 情報セキュリティ基本方針

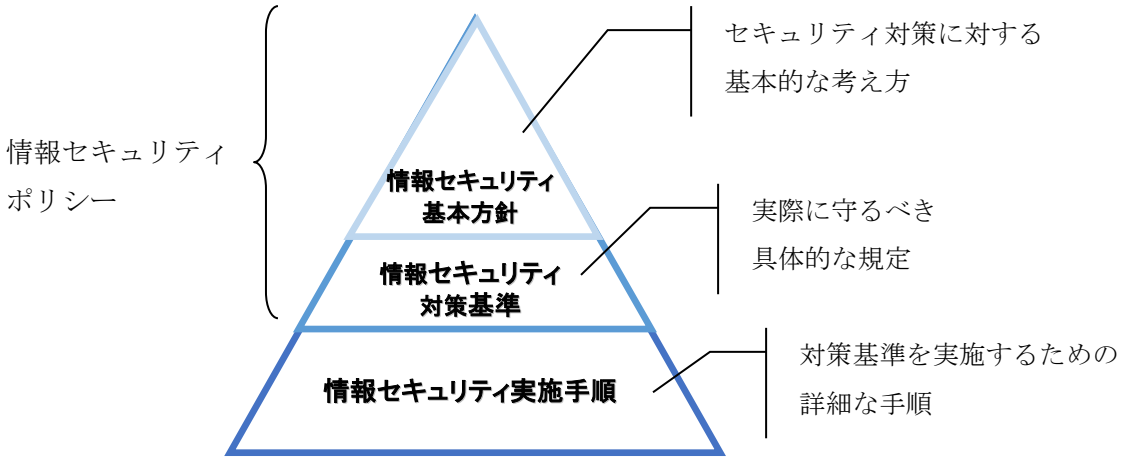
情報セキュリティ基本方針は、文書体系の最上位に位置し、情報セキュリティ管理・運用を実現するための基本方針を定める。

(2) 情報セキュリティ対策基準

情報セキュリティ対策基準は、情報セキュリティ基本方針に基づき、情報セキュリティ対策を実施するにあたって、準拠すべき管理策を定める。

(3) 情報セキュリティ実施手順

情報セキュリティ実施手順は、情報セキュリティ対策基準で定める管理策に基づき、情報セキュリティ管理・運用に関する具体的な内容・方式・手続き・様式等を定める。実施手順に至らない項目については、ガイドライン等で定める。



第７編　情報セキュリティ対策の体制

情報セキュリティ管理・運用の維持改善を目的として、南あわじ市情報セキュリティ委員会を設置する。

第 8 編　情報の管理及び分類

情報資産については、情報の機密性、完全性、可用性を踏まえて重要性分類を定義する。この分類に各情報資産を当てはめてセキュリティ対策を施し、適切に管理する。

第 9 編　情報資産への脅威

情報セキュリティポリシーを講じる上で、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。なお、情報システムや情報ネットワーク等の IT 技術の発展速度は極めて速いため、環境の変化や新たな脅威について、継続的な情報収集をしなければならない。特に認識すべき脅威は以下のとおりである。

(1) 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

(2) 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

(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

第 10 編　情報セキュリティ対策

南あわじ市の情報資産を本書第 9 編で記述した脅威から保護するため、以下のようなセキュリティ対策を講じるとともに、環境の変化や新たな脅威に対応するため継続的に見直しを行っていかなければならない。

(1) 人的セキュリティ対策

情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めるとともに、全ての職員等に情報セキュリティポリシーの内容を周知徹底するため、教育・訓練を行う。

(2) 物理的セキュリティ対策

サーバ室（電子計算機や基幹となる通信制御機器を収納し、運用する室）等について不正な立入りや自然災害等から保護するため、入退室や危機管理上の物理的な対策を講じる。

(3) 技術的セキュリティ対策

情報資産を適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス対策等を実施する。

(4) 運用面におけるセキュリティ対策

情報セキュリティポリシーの実効性を確保するため、また、不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防ぐため、ネットワーク監視等の運用面における情報セキュリティ侵害への必要な措置を講じる。また、障害が発生した際の迅速な対応を可能とするため、障害時の対応を講じる。

(5) 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（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、端末からの情報持ち出し不可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 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。

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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(6) 外部サービスの利用

事業者に業務を委託する場合には、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。

約款による外部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。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。

第 11 編　関連法令の遵守

関連法令を遵守し、必要に応じて南あわじ市独自の管理基準を設定し、継続的な情報セキュリティ対策を講じる。

第 12 編　情報セキュリティに関する違反への対応

情報セキュリティ基本方針・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、その他の関連法令に違反した場合は、地方公務員法に基づき、当該違反により生じた結果の重大性及び当該違反の悪質性等の状況に応じて、懲戒処分等の対象とする場合がある。

第 13 編　監査

情報セキュリティ基本方針、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が遵守されていることを確認するため、必要に応じて情報セキュリティ遵守状況の監査及び自己点検を実施する。

第 14 編　緊急時の対応

災害や障害等の緊急事態の発生時に、障害拡大の防止、二次災害防止等の対策を講じると共に、早期に業務の復旧を図るため、緊急時の対応策を策定し、緊急時に備える。

第 15 編　評価及び見直し

情報資産の適正な保護及び運用において必要があると認めるときは、情報セキュリティ基本方針、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の変更を実施し、その内容を全ての職員等に周知する。

第 16 編　改訂

本書は、情報セキュリティ委員会にて適宜に内容の適切性を審議し、変更が必要な場合は必要部分を変更し、市長の承認を得ることとする。

※但し、軽微な変更については、この限りではない。

改訂履歴

平成 17 年 4 月 1 日	
平成 22 年 10 月 1 日	一部文言等の見直し
平成 26 年 3 月 31 日	副市長 2 名体制、市民交流センターの開設及び情報セキュリティ監査結果に対する是正のための見直し
平成 28 年 4 月 1 日	組織改編による見直し
平成 30 年 4 月 1 日	組織改編等による見直し
令和 2 年 6 月 1 日	・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に伴う見直し ・令和元年度リスク分析結果に基づく見直し
令和 5 年 5 月 31 日	・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に伴う見直し