志太広域事務組合
情報セキュリティポリシー

志太広域事務組合

令和８年３月 31 日改正

目　　次

序　章 志太広域事務組合情報セキュリティポリシーの構成

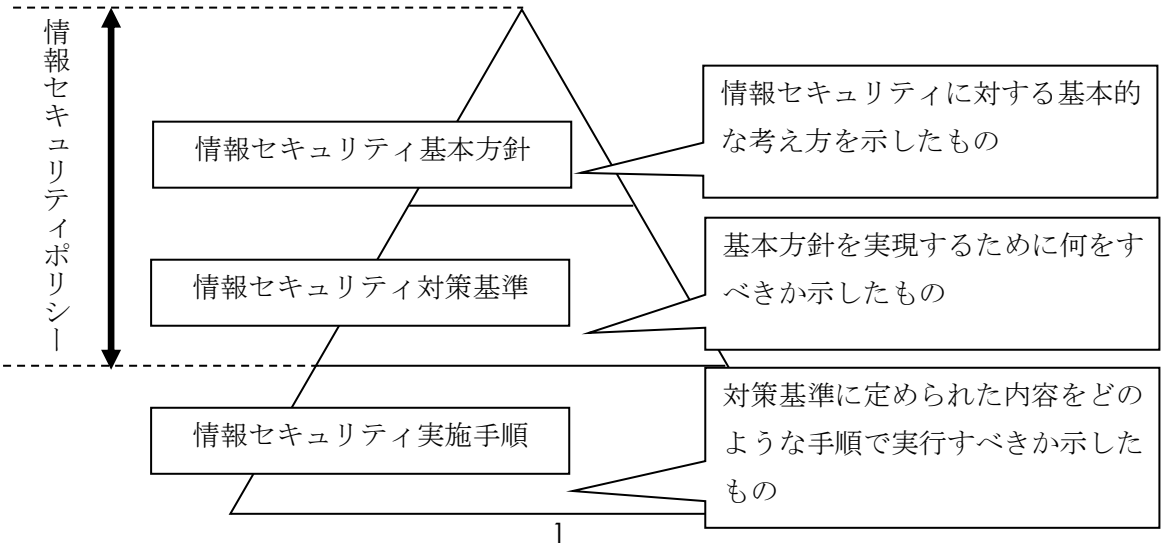
志太広域事務組合情報セキュリティポリシー(以下、「情報セキュリティポリシー」という。)とは、志太広域事務組合(以下、「組合」という)が保有する情報資産に関するセキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

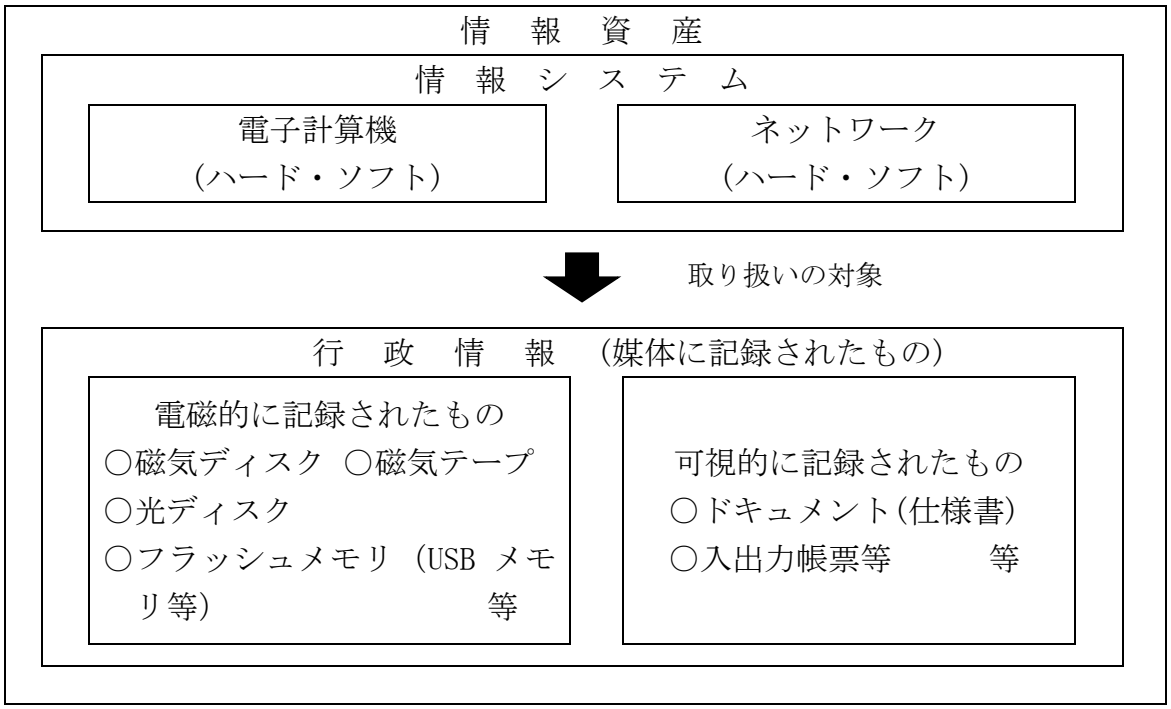
情報セキュリティポリシーは、組合の情報資産を取り扱う全職員に浸透、定着させるものであり、安定的な規範でなければならない。また一方で、情報セキュリティ対策は、情報処理技術や通信技術等の急速な進展に伴う状況の変化に、柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」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としての「情報セキュリティ対策基準」の２階層からなるものとして構成する。また、情報セキュリティポリシーに基づき、情報システムごとに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、整備するものとする。

志太広域事務組合情報セキュリティポリシーの構成

文　書　名		内　容
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するための、全ての情報資産に関する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		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個々の情報資産に関する具体的な対策手順




情　報　資　産
情　報　シ　ス　テ　ム
電子計算機
（ハード・ソフト）
ネットワーク
（ハード・ソフト）
取り扱いの対象
行　政　情　報　（媒体に記録されたもの）
電磁的に記録されたもの
○磁気ディスク　○磁気テープ
○光ディスク
○フラッシュメモリ（USB メモリ等）　等
可視的に記録されたもの
○ドキュメント（仕様書）
○入出力帳票等　等

第１章 情報セキュリティ基本方針

１ 目　的

組合が取り扱う情報資産には、住民の個人情報を始めとし行政運営上重要な情報など、外部に漏えい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おり、これらの情報資産を人的脅威や災害、事故等から防御することは、住民の財産、プライバシーを守るためにも、また、継続的かつ安全・安定的な行政サービスを継続的に確保するためにも必要不可欠である。

また、情報通信技術（以下「ＩＴ」という。）の急激な進展による産業・社会構造の変革と、デジタル社会の形成に向けた政府の戦略は、新しい行政サービスを生みだし、デジタル化が進展する社会へのステップとなっている。組合がこれらに積極的に対応するためには、管理している全ての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となる。

このため、組合の情報資産の情報セキュリティを維持するための対策を整備するため、情報セキュリティポリシーを定めることとし、情報セキュリティの確保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においては、組合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。

２ 定　義

用語の意義は、当該各号に定めるところによる。

（１）情報

紙(メモ等を含む。)、音声、電子データ等のあらゆる形式で保存されている事物、出来事等をいう。

（２）記録媒体

電子計算機に使用される磁気ディスク、磁気テープ、フラッシュメモリ、光ディスク及びその他これらに類する記録用の媒体並びに入出力帳票及び情報システム仕様書等をいう。また、記録媒体のうち、取り外し可能で持ち出しが可能な記録媒体を、外部記録媒体という。

（３）電子計算機

ハードウェア及びソフトウェアで構成するコンピュータ、及び周辺機器並びに記録媒体をいう。

（４）電子計算機室等

電子計算機を運用管理する目的で設置している部屋をいう。

（５）情報処理

収集した多量の情報に、コンピュータなどを使って分類・整理・選択・演算などの

処理を施して、目的に応じた情報を得られるように加工すること。

（６）ネットワーク
　電子計算機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)で構成され、情報処理を行う仕組みをいう。

（７）行政情報
　行政事務の執行に関わる情報で、情報システムで取り扱うものをいう(入出力帳票及び情報システム仕様書を含む)。
　ただし、行政情報を外部へ提供した場合やICカード等に行政情報を記録したものを住民に交付する等により、当該行政情報の管理責任が本組合になくなった場合には対象としない。

（８）情報システム
　電子計算機及びネットワークで構成され、情報処理を行う仕組みをいう。

（９）情報資産
　本組合の情報システム、記録媒体及び行政情報をいう。

(10) 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。

(11) 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をいう。

(12) 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完全保護することをいう。

(13) 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をいう。

(14) 情報セキュリティインシデント
　情報資産の不正使用、業務妨害行為、破壊及びそれらに至るための行為等の情報セキュリティに対する脅威及び脆弱性の事案。そこから発生することを障害という。

(15) 脅威
　自然災害、悪意のある行為等情報資産に被害を与える要因をいう。

（16）脆弱性

情報セキュリティの弱い部分及び情報セキュリティを弱める環境等の脅威を発生しやすくさせる要因をいう。

（17）職員

組合に在職する正職員、会計年度任用職員等をいう。

（18）セキュリティ障害

セキュリティ障害とは、本組合の情報資産に対する脅威が実際に生じることにより、情報資産の機密性、完全性又は可用性が損なわれることであり、以下のものをいう。

（ア）情報システムの故障、停止
（イ）情報システムへの不正アクセス攻撃
（ウ）情報システムの不正な利用
（エ）情報システムにおける入出力内容の誤り
（オ）情報資産の盗難
（カ）情報資産の紛失、滅失
（キ）行政情報の漏えい
（ク）行政情報の改ざん
（ケ）行政情報の誤送付、誤送信
（コ）その他の障害

３ 情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、組合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最高位に位置するものである。

４ 適用範囲

（１）行政機関の範囲

本基本方針が適用される機関は、組合事務局、消防本部、行政委員会及び議会とする。

（２）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。

① ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
③ 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

５ 職員及び外部委託事業者の責務

職員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、情報資産の利用にあたっては情報セキュリティポリシーを遵守しなければなら

ない。

６ 情報セキュリティ管理体制

組合の情報資産に関する情報セキュリティ対策を、適切に推進・管理するための体制を確立するものとする。

７ 情報資産の分類

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。

８ 情報資産への脅威

情報セキュリティポリシーを講ずるうえで、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。

特に以下の認識すべき脅威については、十分な措置を講ずるものとする。

（１）権限外者による故意の不正アクセスまたは不正操作によるデータやプログラムの持ち出し、盗聴、改ざん、消去並びに電子計算機及び外部記録媒体の盗難等

（２）職員及び外部委託者による意図しない操作、故意の不正アクセスまたは不正操作によるデータやプログラムの持ち出し、盗聴、改ざん、消去、電子計算機及び外部記録媒体の盗難、規定外の機器操作によるデータ漏えい等

（３）地震、津波、落雷、火災等の災害や事故、故障、テロ等の破壊活動　等

９ 情報セキュリティ対策

組合の情報資産を上記８の脅威から保護し、又は情報資産の脆弱性を解消するため、次の情報セキュリティ対策を講ずるものとする。

（１）人的セキュリティ対策　（情報セキュリティ組織運営・行動対策）

情報資産に接する職員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、すべての職員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、訓練並びに啓発を行う。

（２）物理的セキュリティ対策　（環境・機器・設備管理対策）

電子計算機、ネットワーク、通信回線、職員のパソコン等の管理及び電子計算機室等の情報資産を有する施設への不正な立ち入り、損傷、盗難等についてから保護するため、入退室や機器管理上の物理的な対策を講ずる。

（３）技術的セキュリティ対策　（情報システム管理対策）

情報資産を不正なアクセス等から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）運用によ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必要な措置を講ずる。

セキュリティ障害が発生した際の迅速な対応と行政事務の円滑な執行を可能とするため、必要な措置を講ずるものとする。

情報資産の管理、セキュリティ対策の遵守状況の確認、緊急事態発生時の危機管理対策等、セキュリティ対策の運用面の対策を講ずる。

（5）ネットワーク管理対策

ネットワークを経由した不正アクセス等から、情報資産を適切に保護するため、ネットワーク構成管理、ネットワークアクセス制御等の必要な対策を講ずる。

（6）情報システム開発対策

情報システムの企画、設計、開発及び導入に関し、情報セキュリティの確保に必要な対策を講ずる。

（7）外部委託対策（クラウドサービス利用を含む）

情報セキュリティポリシーの適用範囲内で行う業務を外部委託する場合、又は指定管理者に実施させる場合には、情報セキュリティ要件を明記した契約を締結する等の必要な措置を講ずる。

また、クラウドサービス等の外部サービスを利用する場合には、その提供事業者に対して情報セキュリティポリシーの遵守を求めるとともに、十分な安全性が確保されたものを選定する等の対策を講ずる。

（8）情報セキュリティインシデント対応対策

情報セキュリティインシデントの発生に対し、事前の対応策及び再発防止策を作成する。

（9）行政業務継続対策

情報サービスの可用性及び代替手段を確保し、行政業務の継続性を高めるため、行政業務継続計画を作成する。

(10) 情報セキュリティポリシーの評価・見直し対策

情報セキュリティを取り巻く状況の変化に対応するため、情報セキュリティポリシーの遵守状況を定期的に監査し、情報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の対策を評価すること等により、情報セキュリティポリシーの見直しを実施するものとする。

(11) 法令等の遵守対策

情報セキュリティポリシーを適切に運用するため、関連法令及び組合条例を遵守させるために必要な対策を講ずる。

(12) 違反への対応対策

情報セキュリティポリシーの違反を防ぐため、情報セキュリティポリシーの遵守状況の確認、遵守違反を発見した場合の報告義務、審議機関の設置等の必要な対策を講ずるものとする。

１０ 情報セキュリティ対策基準の策定

組合の情報資産について、上記９の情報セキュリティ対策を講ずるにあたっては、職員が遵守すべき事項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。

なお、情報セキュリティ対策基準は、公開することにより組合の行政運営に重大な支障を及ぼす恐れがあることから、公開しないものとする。

１１ 情報セキュリティ実施手順(運用マニュアル)の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定、整備するものとする。

なお、情報セキュリティ実施手順は、公開することにより組合の行政運営に重大な支障を及ぼす恐れがあることから、公開しないものとする。

１２ 評価・見直し

情報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、情報システムの変更、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、適宜、情報セキュリティ対策基準の見直しを実施するものとする。

（１）監査及び自主点検の実施

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主点検を実施する。

（２）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主点検の結果、情報セキュリティポリシーの見直しが必要に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。