名古屋港管理組合情報セキュリティポリシー

第１章　情報セキュリティ基本方針

（目的）

第１条　名古屋港管理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。）は、情報セキュリティの確保に関する基本方針及び対策基準を定めることにより、本組合の情報資産を適切に保護することを目的とする。

（定義）

第２条　情報セキュリティポリシーにおいて、次に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1)　通信回線　コンピュータを相互につないで、データを送受信するために使用する回線をいう。

(2)　通信回線装置　ルーター、ＨＵＢ等の通信回線とコンピュータをつなぐ装置をいう。

(3)　ネットワーク　通信回線、通信回線装置等で構成される情報通信網をいう。

(4)　ＮＰＡネットワーク　名古屋港管理組合本庁舎のＬＡＮ及び各事務所のＬＡＮ並びにこれらを結んだＷＡＮ（広域情報連絡網）をいう。

(5)　電磁的記録媒体　ＣＤ－Ｒ、ＤＶＤ－Ｒ、フロッピーディスク、ＭＯ、ＬＴＯ、ＵＳＢメモリ、外付けハードディスクドライブ等をいう。

(6)　モバイル端末　スマートフォン、タブレット型端末等の小型軽量で持ち運ぶことができる情報端末をいう。

(7)　情報システム　コンピュータ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。

(8)　サーバ　情報システムの開発及び処理のために設置されたコンピュータネットワークでサービスを提供する側の機器をいう。

(9)　指定施設　ＮＰＡネットワークを構成する主要な通信機器、サーバ及び業務データを記録した媒体が置かれた室等（区画を含む。）で、第１０条に規定する情報管理者が特に保安措置を要すると認めたものをいう。

(10)　情報資産　次に掲げるものをいう。

ア　ネットワーク及び情報システム並びにこれらに関する機器及び設備並びに電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う全ての電子情報

ウ　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

(11)　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。

(12)　機密性　情報にアクセスすることが許可された者のみがアクセスできることを確実にすることをいう。

(13) 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。

(14) 可用性　情報にアクセスすることが許可された者が必要なときにアクセスできることを確実にすることをいう。

(15) 情報セキュリティインシデント　ウイルス感染、不正アクセス、情報漏えい等の情報管理及びシステム運用に関して保安上の脅威となる事象をいう。

(16) 無線ＬＡＮ　無線通信を利用してデータの送受信を行うＬＡＮシステムをいう。

(17) ネットワークストレージサービス　インターネット上で、ファイル保管用のディスクスペースにデータを保存することができるサービスをいう。

(18) 約款による外部サービス　約款への同意及び簡易なアカウントの登録により、利用可能なインターネット上の情報処理サービスをいう。

(19) ソーシャルメディアサービス　インターネットを利用して情報を発信し、又は相互に情報をやり取りする情報の伝達手段をいう。

(20) ＬＧＷＡＮ接続系　総合行政ネットワーク（以下「ＬＧＷＡＮ」という。）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。

(21) インターネット接続系　電子メール、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。

(22) 危険因子　情報セキュリティインシデントを発生させる可能性のあるデータをいう。

(23) 無害化通信　ファイル中のプログラム除去、情報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。

（適用範囲）

第３条　情報セキュリティポリシーが適用される行政機関は、管理者の事務部局、監査委員事務局及び議会事務局とする。

（職員の義務）

第４条　情報資産に接する全ての職員（非常勤職員及び会計年度任用職員を含む。以下「職員」という。）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、情報セキュリティポリシー及び第８条に規定する実施手順を遵守するものとする。

（管理体制）

第４条の２　本組合の情報資産について、情報セキュリティ対策を推進する全庁的な管理体制を確立するものとする。

（情報システム全体の強靭性の向上）

第４条の３　情報セキュリティの強化を目的とし、業務の効率性及び利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じるものとする。

(1) ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する情報システムと、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し、ＬＧＷＡＮと接続する情報システムとインターネット接続系の情報システムとの間で通信する場合には、無害化通信を実

施する。

(2) 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。

（情報資産の管理）

第５条　本組合の保有する全ての情報資産は、当該情報の重要度を考慮の上、第７条に規定する情報セキュリティ対策を講じる等により適切に管理するものとする。

（対象とする脅威）

第６条　情報セキュリティ対策は、次に掲げる情報資産への脅威に対して、脅威の発生度合及び発生した場合の影響を考慮して、定めるものとする。

(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による情報資産の漏えい、破壊、改ざん、消去等

(2) 部外者の侵入による情報資産の破壊若しくは盗難又は故意の不正アクセス若しくは不正操作による機器若しくは情報資産の破壊、盗聴、改ざん、消去等

(3) 職員又は外部委託事業者による情報資産の持出し若しくは誤操作、アクセスのための認証情報若しくはパスワードの不適切管理、故意の不正アクセス若しくは不正行為による破壊、盗聴、改ざん、消去等、搬送中の事故等による情報資産の破壊、滅失等又は規定外の端末接続によるデータ漏えい等

(4) 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

(5) 大規模、広範囲にわたる疾病による要因不足に伴うシステム運用の機能不全等

(6) 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

（情報セキュリティ対策）

第７条　本組合の情報資産を前条各号に規定する脅威から保護するため、次に掲げる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　情報セキュリティに関し、職員が遵守すべき事項を定めるとともに、全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など教育及び啓発を講じる対策

(2) 物理的セキュリティ対策　情報資産への損傷又は妨害等から保護するための物理的な対策

(3) 技術的セキュリティ対策　情報資産を不正なアクセス等から適切に保護するための情報資産へのアクセス制御及びコンピュータウイルスに対する対策

(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し、情報セキュリティに対する侵害を防ぐためのネットワークの監視等の運用面における対策

（情報セキュリティ実施手順の策定）

第８条　次章に規定する情報システム管理者は、次章に規定する情報セキュリティ対策基準に基づいた情報セキュリティ実施手順（以下「実施手順」という。）を定めるものとす

る。

（評価及び見直し）

第９条　情報セキュリティポリシーに定める事項、情報セキュリティ対策の評価、情報システムの変更及び新たな脅威等の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ポリシーの見直しを行うものとする。

２　情報セキュリティポシリ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行うものとする。