序章 那珂市情報セキュリティポリシー

那珂市（以下「本市」）が取り扱う情報資産には、住民の個人情報をはじめ、行政サービスを安全かつ継続的に提供するために必要な重要情報が含まれる。これらが漏えい・改ざん・滅失・利用不能となった場合、市民生活や行政運営に重大な影響を及ぼすおそれがある。

本市は、情報資産をサイバー攻撃、誤操作、内部不正、災害・障害等の脅威から保護し、機密性（Confidentiality）・完全性（Integrity）・可用性（Availability）を確保するため、本ポリシーを定め、継続的に運用・改善を行う。また本市は、国が示す「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」の考え方に沿い、自治体業務の実態（クラウド利用・遠隔会議・外部との安全なデータ連携等）を踏まえた対策を講じることとする。

本ポリシーは、情報セキュリティ対策の基本的な方針を定める「情報セキュリティ基本方針」と、方針を実行するための全庁共通の対策を定める「情報セキュリティ対策基準」から成る。

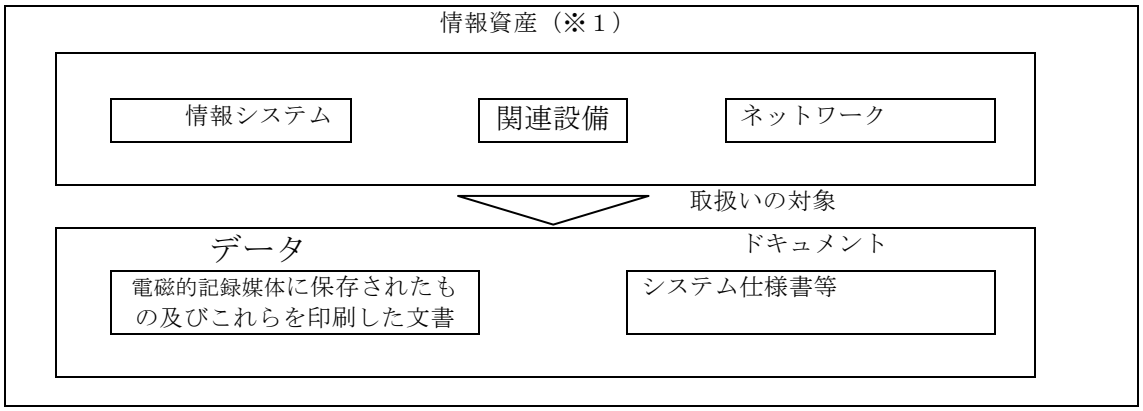
なお、個別の情報システムごとの具体的な設定値・構成・運用手順（例：機器設定、例外経路、監視設定等）は、公開により不正利用を助長するおそれがあるため、別途「情報セキュリティ実施手順」として整備し、原則として非公開で管理する。これにより、本市は情報セキュリティ対策を推進する体制を確立し、情報資産を取り扱う全ての職員等に周知・定着させ、市民の信頼に足る行政運営の継続を実現する。

※　「情報資産」：情報システム（端末・サーバ・ネットワーク及び関連設備）、それらが取り扱う情報（電磁的記録媒体に保存されたもの及び印刷物を含む）、およびシステム関連文書（仕様書・設計書・構成図・手順書等）。

※　機密性（Confidentiality）：許可された者だけが情報にアクセスできる状態を確保すること。

※　完全性（Integrity）：情報及び処理方法が正確・完全な状態であることを保護すること。

※　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状態を確保すること。



情報セキュリティ基本方針

本章では、那珂市（以下「本市」）の情報セキュリティ対策の基本方針として、情報セキュリティポリシーの対象、位置付け等を定める。本市は、三層分離を基本としつつ、業務の実態（Web 会議、クラウド利用、外部連携等）を踏まえ必要となる管理（アクセス制御、記録、監視、例外管理等）を行う。

１　定義

本ポリシーにおいて使用する用語の定義は、次のとおりとする。

(1)　電子計算機器等

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（端末及びサーバ等）をいう。

(2)　電磁的記録媒体

端末・サーバ等に内蔵される記録媒体及び USB メモリ、外付け記録装置、光学媒体等の外部記録媒体をいう。

(3)　ネットワーク

電子計算機器等を相互に接続するための通信網及びその構成機器をいう。

(4)　ドキュメント

情報システムの仕様書、設計書、構成図、ネットワーク図、手順書等のシステム関連文書をいう。

(5)　データ

情報システムで取り扱う情報（印刷物及び電磁的記録媒体に記録された情報を含む）をいう。

(6)　情報資産

本ポリシーが対象とする情報資産は、次のとおりとする。

ア　ネットワーク、情報システム、関連設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（印刷物を含む）

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

(7)　情報セキュリティ

情報資産の機密性・完全性・可用性を維持することをいう。

(8)　個人情報

個人情報の保護に関する法令等に基づき、特定の個人を識別し得る情報をいう。

(9)　マイナンバー利用事務系（個人番号利用事務系）

マイナンバー（個人番号）を利用する事務を行う情報システム及び当該情報システムで取り扱うデータが配置される、他の領域から分離されたネットワーク領域をいう。

(10)　LGWAN 接続系

LGWAN に接続された情報システム及び当該情報システムで取り扱うデータが配置されるネットワーク領域をいう。

(11)　インターネット接続系

インターネットを利用した電子メールやホームページ閲覧等を行う情報システム、公開用サーバ及びこれらで取り扱うデータが配置されるネットワーク領域をいう。

(12)　通信経路の分割

LGWAN 接続系とインターネット接続系の間の通信環境を分離し、安全が確保された通信のみを許可できるようにすることをいう。

(13)　無害化通信

外部から取り込む情報に不正プログラム等の危険因子が付着しないようにした上で行う通信（例：本文のテキスト化、画面転送、危険因子除去等）をいう。

(14)　外部サービス

本市の管理外にある外部事業者が提供するサービス（クラウドサービスを含む）をいう。

(15)　特定クラウドサービス

本市が業務上必要と認め、リスク評価・承認等の手続きを経て利用を認めた外部サービスをいう（利用範囲・条件は別に定める）。

(16)　α’モデル

三層分離を基本としつつ、業務上必要な目的で、LGWAN 接続系の業務端末からインターネット経由で特定クラウドサービスを安全に利用するための対策（アクセス制御等）を適用する考え方をいう。

(17)　動的なアクセス制御

利用者・端末等の状態に応じて、アクセスの可否や追加認証等を制御する考え方をいう（詳細は別に定める）。

２　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、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とする。

また、本ポリシーは本市の情報セキュリティ対策に関する全庁共通の最低限の要件を定めるものであり、各執行機関・議決機関（以下「各機関」という。）が所掌する業務、情報システム又は情報資産の特性、法令・制度要件、外部委託や外部サービスの利用形態等により、本ポリシーのみでは具体的要件を十分に規定できない事項については、各機関は必要に応じて、各機関情報セキュリティポリシー（以下「各機関ポリシー」という。）又はこれに準ずる規程・要領等を定め、当該事項を補完するものとする。

本ポリシーと各機関ポリシーは、二層構造（本市ポリシー＋各機関ポリシー）として整合的に運用するものとし、同一事項について規定が重複する場合又は解釈上の差異が生じる場合は、より厳格な要件を優先して適用するものとする。
ただし、適用関係が不明確で実務運用又は監査対応に支障が生じるおそれがある場合は、所定の管理体制（情報セキュリティ統括部門又は情報セキュリティに係る会議体）において解釈を確定し、必要に応じて本ポリシー又は各機関ポリシーを見直すものとする。

さらに、本市における情報システム間の接続、外部サービスとの連携、他機関・外部機関とのデータ授受等については、三層分離を基本としつつ、業務上必要な外部サービス利用を含め、安全性と追跡可能性を確保し、実務及び監査の双方で整合できるよう、インターフェース管理基準（接続・連携・データ授受の共通ルール）を別に定め、全庁共通で適用するものとする。

インターフェース管理基準は、少なくとも次に掲げる事項を含む。

(1) 対象範囲の明確化（接続・連携・データ授受の類型：API 連携、ファイル授受、メール添付、オンラインストレージ共有、Web 会議連携、リモート保守等）
(2) 事前審査・承認（目的、取扱情報の分類、必要最小化、リスク評価、利用範囲・期限、責任分担、委託・再委託の統制）
(3) 接続方式・経路の統制（許可制、接続先限定、α’モデル適用時の条件、無害化通信等の安全な方式、例外措置の期限管理）
(4) 認証・アクセス制御（証明書等による認証、端末/利用者の状態に応じた制御、最小権限、特権の統制）
(5) データ保護（暗号化、共有範囲の制御、外部共有の原則禁止又は厳格制限、持出・再提供の禁止、保存期間・廃棄）
(6) 記録・監視・追跡可能性（認証・通信・操作ログの取得、保全、突合、監査対応可能な保管）

(7)　変更管理・棚卸し（設定変更の申請・承認・記録、定期棚卸し、利用停止・廃止時の措置）
(8)　証跡管理（監査に提示可能な記録様式、保存先、命名規則、保存期間）

なお、インターフェース管理基準に基づく個別の設定値・構成・運用手順等の技術的詳細は、公開により不正利用を助長するおそれがあるため、必要に応じて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（非公開）において管理する。

3　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの対象範囲は、本市における情報資産に接する許可を受けた全ての者（以下「職員等」という。）とし、次に掲げる執行機関及び議決機関に対し適用するものとする。

(1)　市長（水道事業、下水道事業及び消防本部を含む。）
(2)　教育委員会
(3)　選挙管理委員会
(4)　監査委員
(5)　農業委員会
(6)　固定資産評価審査委員会
(7)　議会
(8)　前各号に掲げる機関に属さない職員等で、本市の情報資産に接するもの及び本市の情報資産を取り扱う外部委託者

4　職員等の義務

職員等は、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、情報資産の利用に当たっては本ポリシーを遵守するものとする。

また、情報セキュリティ上の事故又はそのおそれを認知した場合は、定められた手続きに従い速やかに報告するものとする。

5　情報セキュリティ管理体制

本市は、情報資産について適切に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。

加えて、外部サービスの利用や業務委託に関しては、契約時・契約期間中・終了後の各段階で必要な安全管理措置を確認し、継続的に見直す。

6　情報資産の分類

本市は、情報資産を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。

分類基準は、ガイドラインの考え方（国の分類との対応関係の明確化等）を踏

まえ、必要に応じて見直す。

7　情報資産への脅威

情報セキュリティ対策を講ずるに当たっては、情報資産に対する脅威の発生可能性及び発生した場合の影響を考慮し、リスクに応じて必要な対策を講ずるものとする。

特に認識すべき脅威は次のとおりである。

(1)　権限のない者による、又は権限を不正に取得した者による不正アクセス・不正操作、盗聴等に起因する、データ又はプログラムの漏えい、改ざん、消去、及び機器・電磁的記録媒体の盗難等

(2)　職員等又は外部委託者による、誤操作、手順逸脱、内部不正、又は権限濫用に起因する、データ又はプログラムの漏えい、改ざん、消去、及び規定外の機器操作・外部サービス利用等による情報漏えい等

(3)　サイバー攻撃（マルウェア感染、ランサムウェア、標的型攻撃、サプライチェーン攻撃、DDoS 攻撃等）により生じる、サービス停止、情報漏えい、業務の継続困難等

(4)　地震、落雷、火災、風水害等の災害、事故、故障等による、設備・情報システム・通信の停止又は劣化

(5)　大規模・広範囲にわたる疾病等による、要員不足に伴う運用・対応機能の低下

(6)　電力、通信、水道等のインフラ障害又は外部サービス障害の波及による、行政サービスの停止又は遅延

8　情報セキュリティ対策

本市は、前条の脅威から情報資産を保護するため、次の情報セキュリティ対策を講ずるものとする。

(1)　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性にも配慮しつつ情報システム全体に対し、次の三段階の対策を講じる。

ア　マイナンバー利用事務系

原則として他の領域との通信を行わないようにするとともに、情報の不正持出し防止、強固な認証（多要素認証を含む）、端末管理等により、住民情報等の流出を防止する。

イ　LGWAN 接続系

LGWAN 接続系とインターネット接続系の通信経路を分割し、両系間で通信が必要な場合は、無害化通信等の安全な方式に限定する。

また、三層分離を基本としつつ、業務上必要な場合に限り、LGWAN 接続系の

端末からインターネット経由で特定クラウドサービスを利用する仕組み（α’モデル）を適用する。α’モデルを適用する場合は、少なくとも次を確保する。

① 接続先の限定（許可された特定クラウドサービスのみ利用可とする管理）

② 強固な認証及びアクセス制御（接続先証明書の確認、通信の安全性確保、端末・利用者等に応じた制御を含む）

③ 通信・認証・操作等の記録及び監視（追跡可能性の確保）

④ 例外措置の厳格な管理（期限・範囲・承認・記録）

ウ インターネット接続系

不正通信の検知、通信の可視化等を目的として、自治体情報セキュリティクラウドを活用し、境界防御機能の機能強化及び監視体制の高度化を図る。

(2) 人的セキュリティ対策

職員等の情報セキュリティに関する権限及び責任等を定め、全ての職員等に対して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・訓練を実施する。また、外部委託者に対しても、本市が求める水準の教育・周知及び遵守が確保されるような必要な措置を講じる。

(3) 物理的セキュリティ対策

情報システムを設置する施設等への不正な立入り、情報資産への損傷・妨害等から保護するため、入退室管理、機器の保護、媒体管理等の物理的対策を講ずる。

(4) 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、アクセス制御、認証強化、不正プログラム対策、脆弱性対策、暗号化その他必要な技術的対策を実施する。

(5) 運用におけるセキュリティ対策（監視・継続的改善・レジリエンス）

情報セキュリティポリシーの実効性を確保するため、ネットワーク及び情報システムの監視、ログの取得・保全・分析、セキュリティポリシーの遵守状況確認等の必要な措置を講ずる。

また、サイバー攻撃、障害及び緊急事態が発生した際の迅速な対応、並びに行政サービスの継続及び復旧を可能とするための対策（バックアップ、復旧手順、訓練等）を講ずる。

9 情報セキュリティ対策基準の策定

本市の情報資産について前条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事項及び判断の基準を統一的な水準で定める必要がある。このため、本市は、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、外部サービスの利用及び業務委託に関する要件についても、対策基準において必要な水準を定める。

１０　情報セキュリティ実施手順の策定（非公開）

情報セキュリティ対策を確実に実施するため、個々の情報資産又は情報システムに関する対策の手順を具体的に定める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本市の行政運営に重大な支障を及ぼすおそれがある情報を含むため、原則として非公開とする。

１１　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及び情報セキュリティ実施手順の見直しを実施するものとする。

特に、外部サービスの利用状況、委託先管理状況、監視結果及びインシデント対応結果を踏まえ、継続的に改善を行う。

【改定】

・平成１５年９月策定
・平成２８年３月７日一部改定
・令和６年３月１８日一部改定
・令和８年３月１６日一部改定