（平成 29 年４月１日　策定）
（令和　７年５月１日　全部改正）
（令和　８年３月 31 日　改正）

水戸市情報セキュリティ基本方針

（目的）

第１条　この基本方針は，本市の情報セキュリティに関する基本的な事項を定めることにより，行政の適正かつ円滑な運営を図り，もって市政に対する市民の信頼を確保することを目的とする。

（定義）

第２条　この基本方針において，次の各号に掲げる用語の意義は，当該各号に定めるところによる。

(1) 情報システム　水戸市情報システムの管理運営に関する規則（平成 19 年水戸市規則第 62 号）第２条第１号に規定する情報システムをいう。

(2) 情報資産　情報システム等（パーソナルコンピュータ，サーバ，ストレージ等の機器，コンピュータを相互に接続するための通信網及びその構成機器並びに情報システムをいう。以下同じ。）及び情報システム等において本市が取り扱う情報（情報システムの開発及び運用に係る情報を含む。）をいう。ただし，市立学校（水戸市立小学校，中学校，義務教育学校及び幼稚園設置条例（昭和 39 年水戸市条例第 16 号）に規定する小学校，中学校及び義務教育学校をいう。以下同じ。）において利用し，又は保有するもの及び議会が管理するものを除く。

(3) 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。

(4) 情報セキュリティポリシー　この基本方針及び水戸市情報セキュリティ対策基準をいう。

(5) 機密性　情報にアクセスすることを認められた者だけが，情報にアクセスできる状態を確保すること。

(6) 完全性　情報が破壊，改ざんし，又は消去されていない状態を確保すること。

(7) 可用性　情報にアクセスすることを認められた者が，必要なときに中断されることなく，情報にアクセスできる状態を確保すること。

(8) マイナンバー利用事務系　個人番号利用事務（社会保障，地方税又は防災に関する事務），戸籍事務等に関わる情報システム及びデータをいう。

(9) LGWAN 接続系　LGWAN 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（マイナンバー利用事務系を除く。）。

(10) 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。

(11) 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。

(12) 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。

（情報セキュリティに対する脅威）

第３条　情報セキュリティに対する脅威は，次の各号に掲げる脅威とする。

(1) 人による脅威

ア　不正アクセス，ウイルス攻撃等のサイバー攻撃，機器の盗難，情報資産の不正な操作，持ち出し等による情報資産の漏えい，破壊，改ざん，消去等

イ　情報資産の管理不備，無許可ソフトウェアの使用等，プログラム上の欠陥，誤操作，プログラム，設定又はメンテナンスの不備，外部委託管理の不備等による情報資産の漏えい，破壊，消去等

(2) 災害による脅威

地震，落雷，火災，水害その他の災害（次号において「災害」という。）によるサービス等の停止，情報資産の消失等

(3) 必要資源の不足，故障等による脅威

災害その他の原因による電力，通信，水道の途絶若しくは交通機能の麻痺，大規模若しくは広範囲にわたる疾病の蔓延による要員の不足，機器の故障その他の原因によるサービス若しくは業務の停止又はシステム運用の機能不全等

（適用範囲）

第４条　この基本方針の適用範囲は，次の各号に定めるところによる。

(1) 対象とする行政機関等の範囲

この基本方針が適用される行政機関等は，市長，教育委員会（市立学校を除く。），選挙管理委員会，公平委員会，監査委員，農業委員会，固定資産評価審査委員会，消防長，上下水道事業管理者及び議会事務局とする。

(2) 対象とする職員の範囲

この基本方針は，前号に定める行政機関等が保有する情報資産を扱う全ての職員（地方公務員法（昭和 25 年法律第 261 号）第 22 条の２第１項に規定する会計年度任用職員及び同法第 22 条の３第４項の規定により臨時的に任用される職員を含む。）及び労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和 60 年第 88 号）第２条第３号に規定する労働者派遣事業により派遣された同条第２号に規定する派遣労働者で本市の事務に携わるもの（以下「職員等」という。）並びに本市の事務について委託を受けた者に適用する。

（遵守事項）

第５条　職員等及び市の事務について委託を受けた者は，情報セキュリティの重要性を認識し，業務の遂行に当たってこの基本方針及び情報セキュリティ対策基準を遵守しなければならない。

（情報セキュリティ対策）

第６条　第３条の脅威から情報資産を保護するために，次の各号に掲げる措置（以下「情報セキュリティ対策」という。）を講ずる。

(1) 情報セキュリティ対策を推進する全庁的な組織体制の確立

(2) 情報資産の適切な分類及び管理

(3) 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・利便性の観点を踏まえ，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。

イ　LGWAN 接続系においては，通信経路の分割を行う。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。

ウ　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，都道府県及び市区町村のインターネットとの通信を集約した上で，自治体情報セキュリティクラウドの導入等を実施する。

(4) 次に掲げる情報資産の保護のための措置

ア　情報資産を取り扱う機器の設置及び保管施設の管理に関する物理的な措置

イ　情報セキュリティに関する職員等への研修の開催等

ウ　コンピュータ等の管理，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な措置

(5) 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情報セキュリティの確保等，情報セキュリティポリシーの運用面の対策及び情報資産への侵害が発生した場合等に迅速かつ適切に対応するための緊急時対応計画の策定

(6) 業務委託と外部サービス（クラウドサービス）の利用

ア　業務委託を行う場合には，委託事業者を選定し，情報セキュリティに係る条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。

イ　外部サービス（クラウドサービス）を利用する場合には，利用に係る規定を整備し対策を講じる。

ウ　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。

(7) 情報セキュリティポリシーの遵守状況に関する定期又は随時に行う監査及び点検

（情報セキュリティポリシーの見直し及び改定）

第７条　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己点検を実施し，必要に応じて改正する。

２　前項の規定にかかわらず，前条第５号の規定による監査又は点検の結果，情報セキュリティに関する状況の変化その他情報セキュリティポリシーの改正が必要なときは，保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し，リスクを検討した上で，当該情報セキュリティポリシーの改正を行う。

（情報セキュリティ対策基準等の策定）

第８条　情報セキュリティ対策等の実施のため，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を策定する。