# ○矢板市情報セキュリティ基本方針

令和５年４月１日要綱

（目的）

第１条　この基本方針は、市が保有する情報資産の機密性、完全性及び可用性を維持するため、市が実施する情報セキュリティ対策について基本的な事項を定め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。

⑴　ネットワーク　コンピュータ等を相互に接続するための通信網及びこれを構成する情報機器（ハードウェア及びソフトウェアをいう。）をいう。

⑵　情報システム　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑶　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。

⑷　情報セキュリティポリシー　この基本方針及び第１０条第１項の規定により定める情報セキュリティ対策基準をいう。

⑸　機密性　情報にアクセスすることを認められた者のみが情報にアクセスできる状態を確保することをいう。

⑹　完全性　情報が破壊、改ざん又は消去をされていない状態を確保することをいう。

⑺　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をいう。

⑻　マイナンバー利用事務系　個人情報利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

⑼　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。

⑽　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。

⑾　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。

⑿　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を防止する等、安全が確保された通信をいう。

（行政機関の範囲）

第３条　この基本方針が適用される行政機関は、市長部局、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会及び上下水道事務所並びに議会事務局とする。

（情報資産の範囲）

第４条　この基本方針が対象とする情報資産は、次に掲げるとおりとする。

⑴　ネットワーク、情報システム及びこれらの運用又は管理に必要な設備並びに電磁的記録媒体

⑵　ネットワーク又は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。）

⑶　ネットワーク又は情報システムに関する仕様書、図面等のシステム関連文書

（職員等の遵守義務）

第５条　職員、再任用職員、任期付職員及び会計年度任用職員等（以下「職員等」という。）は、業務の遂行に当たり情報セキュリティポリシー及び第１１条第１項の規定により定める情報セキュリティ実施手順を遵守しなければならない。

（情報資産に対する脅威）

第６条　情報資産に対する脅威は、次に掲げるとおりとする。

⑴　情報機器の盗難、不正アクセス、コンピュータウイルスによる攻撃、部外者の侵入等の意図的要因による情報資産の漏えい、破壊、改ざん、消去等

⑵　情報資産の管理の不備、ソフトウェアの無許可での使用、プログラム上の欠陥、誤操作、メンテナンスの不備、情報機器の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

⑶　地震、落雷、火災等の災害、電力供給又は通信の途絶等による情報システムの運用障害等

（情報セキュリティ対策）

第７条　市は、前条に規定する脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講ずるものとする。

⑴　情報セキュリティ対策を推進する全庁的な組織体制を確立すること。

⑵　情報資産を、その重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行うこと。

⑶　情報システム全体の強靭性の向上のため、次の対策を講じること。

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を禁じる設定や多要素認証の導入等により、住民情報の流出を防止する。

イ　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。

ウ　インターネット接続系においては、栃木県セキュリティクラウドを経由することで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。

⑷　コンピュータその他情報機器の設置場所、通信回線等の管理に関する物理的セキュリティ対策を行うこと。

⑸　情報セキュリティに関する職員等への教育、啓発等の人的セキュリティ対策を行うこと。

⑹　情報資産へのアクセスの制御、不正プログラムへの対策、不正アクセスの防止等の技術的セキュリティ対策を行うこと。

⑺　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、外部委託を行う場合のセキュリティの確保等の情報セキュリティポリシーの運用面における対策を行うこと。

⑻　情報資産に対するセキュリティの侵害が発生した場合に、迅速かつ適切に対応できるよう対策を行うこと。

（情報セキュリティの点検及び監査の実施）

第８条　市は、情報セキュリティポリシーの遵守状況を確認するため、定期的又は必要に応じて情報セキュリティの点検及び監査を実施するものとする。

（情報セキュリティポリシーの見直し）

第９条　市は、情報セキュリティの点検若しくは監査の結果又は情報セキュリティに関する状況の変化により、新たに対策が必要になったときは、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準）

第１０条　市は、前３条に規定する事項を実施するための具体的な遵守事項、判断基準等を情報セキュリティ対策基準として定めるものとする。

（情報セキュリティ実施手順）

第１１条　市は、情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を情報セキュリティ実施手順として定めるものとする。

２　情報セキュリティ実施手順は、非公開とする。

（委任）

第１２条　この基本方針に定めるもののほか必要な事項は、別に定める。

附　則

この基本方針は、令和５年４月１日から施行する。