

## 宮若市情報セキュリティ基本方針

(趣旨)

第1条 この方針は、市が保有する情報資産の機密性、完全性及び可用性を確保し、適正な行政運営及び市民の信頼を維持するため、市が実施する情報セキュリティ対策に関し基本的な事項を定めるものとする。

(この方針の位置付け)

第2条 この方針は、市の情報セキュリティ対策に関する最上位の方針として位置付ける。

(定義)

第3条 この方針において、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) 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その構成機器（ハードウェア及びソフトウェア）をいう。
- (2) 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。
- (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をいう。
- (4) 情報セキュリティポリシー この方針及び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をいう。
- (6) 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。
- (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をいう。
- (8) 実施機関 市長、教育委員会、公平委員会、監査委員、農業委員会、選挙管理委員会、固定資産評価審査委員会、公営企業管理者及び議会事務局をいう。
- (9) 職員等 宮若市職員定数条例（平成18年宮若市条例第24号）第1条に規定する職員及び宮若市会計年度任用職員の給与、費用弁償及び旅費に関する条例（令和元年宮若市条例第20号）第2条に規定する会計年度任用職員並びに本市の業務を受託している事業者のうち、情報資産に関する業務に携わる者をいう。
- (10) 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）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。
- (11) 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。）。

- (12) 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。
- (13) 通信経路の分割 L G W A N接続系とインターネット接続系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。
- (14) 無害化通信 インターネットメール本文のテキスト化、添付ファイルの無害化処理、画面転送その他の方法により、マルウェア等のリスクを除去した通信をいう。

（対象とする脅威）

第4条 情報資産に対する脅威として、次の各号に掲げるものを想定し、情報セキュリティ対策を実施する。

- (1) 不正アクセス、マルウェア感染、サービス不能攻撃その他のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい・破壊・消去等
- (3) 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
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 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

（適用範囲）

第5条 この方針は、実施機関に適用する。

2 この方針が対象とする情報資産は、次に掲げるものとする。

- (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、ネットワーク図その他のシステム関連文書  
（職員等の遵守義務）

第6条 職員等は、情報セキュリティの重要性を十分に理解し、業務の遂行に当たっては、情報セキュリティポリシーを遵守しなければならない。

（情報セキュリティ対策）

第7条 市長は、第4条各号に規定する脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じるものとする。

- (1) 組織体制 市の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をいう。
- (2) 情報資産の分類と管理 市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施することをいう。
- (3) 情報システム全体の強靱性の向上 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、次の三段階の対策を講じることをいう。
  - 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、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、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（自治体情報セキュリティクラウドの活用又はこれと同等以上のセキュリティを確保できる構成により、安全な通信環境を維持すること等をいう。）を実施する。
- (4) 物理的セキュリティ サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じることをいう。
- (5) 人的セキュリティ 情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じることをいう。
- (6) 技術的セキュリティ 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対策を講じることをいう。
- (7) 運用 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、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じることをいう。（情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定するものとする。）
- (8) 業務委託と外部サービスの利用 業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要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ことをいう。（外部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ものとし、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ものとする。)

- (9) 評価・見直し 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、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行うことをいう。

(情報セキュリティ監査及び自己点検の実施)

第8条 情報セキュリティポリシーの遵守状況を確認するため、定期的に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するものとする。また、必要に応じて外部の専門家による公認情報システム監査を実施し、客観的な評価を受けるよう努めるものとする。

- 2 情報セキュリティ監査又は自己点検の結果、改善が必要と認められた事項については、速やかに必要な措置を講ずるものとする。

(情報セキュリティポリシーの見直し)

第9条 情報セキュリティ監査又は自己点検の結果、情報セキュリティポリシーの見直しが必要であると認められ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となった場合には、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、発生時の損失等を分析し、リスクを検討した上で、情報セキュリティポリシーを見直すものとする。

(宮若市情報セキュリティ対策基準の策定)

第10条 第7条、第8条及び第9条に規定する情報セキュリティ対策を実施するため、具体的な遵守事項及び判断基準等を定めた宮若市情報セキュリティ対策基準を策定するものとする。

(宮若市情報セキュリティ実施手順の策定等)

第11条 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定めた宮若市情報セキュリティ実施手順を策定するものとする。

- 2 宮若市情報セキュリティ実施手順は、公にすることにより市の行政運営に重大な支障を及ぼすおそれがある場合には、非公開とする。

(その他)

第12条 この方針の施行に関し必要な事項は、別に定めるものとする。

附 則

この方針は、令和8年4月1日から施行する。