# 新島村情報セキュリティ基本方針に関する規則

平成27年12月10日

規則第11号

（目的）

第１条　この規則は、第４条第１項に定める執行機関等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に当村が実施する、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　この規則において、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)　情報資産　新島村文書管理規則（平成16年規則第９号）第２条第１項第１号に規定される文書のうち、電磁的記録によるものをいう。

(2)　記録媒体　磁気ディスク、フロッピーディスク、光磁気ディスクその他これらに類するもの並びに入出力帳票及び情報システム仕様書等をいう。

(3)　電子計算機　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、周辺機器並びに記録媒体をいう。

(4)　ネットワーク　電子計算機を相互に接続するための通信網及びその構成機器で構成され、情報処理を行う仕組みをいう。

(5)　情報システム　電子計算機及びネットワークにより業務処理を行う仕組みをいう。

(6)　行政情報　行政事務の執行に関わる情報の内、情報システムで取り扱うものをいう。

(7)　情報資産　情報システム及び行政情報をいう。

(8)　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。

(9)　情報セキュリティポリシー　この規則及び第９条の規定に基づき定める情報セキュリティ対策基準の総称をいう。

(10)　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。

(11)　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。

(12)　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。

(13)　マイナンバー利用事務系（個人番号利用事務系）　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。

(14) 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。）。

(15) 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。

（対象とする脅威）

第３条　セキュリティポリシーの対象とする脅威は、次に掲げるものとし、それぞれの発生頻度、被害の程度等を考慮して対策を講じるものとする。

(1) サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、外部委託管理の不備、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提供サービスの障害からの波及等

（適用範囲）

第４条　この規則が適用される機関は、内部課、行政委員会、議会事務局及び地方公営企業管理者とし、その職員（定年前再任用短時間勤務職員、非常勤嘱託職員及び臨時職員を含む。以下同じ。）並びに各機関が所管する情報システム及び情報資産とする。

（職員等の遵守義務）

第５条　職員は、情報セキュリティの重要性について共通の認識を持ち、情報資産の取扱いに当たっては、個人情報の保護に関する法律（平成15年法律第57号）、新島村個人情報保護法施行条例（令和５年新島村条例第７号）、新島村議会の個人情報の保護に関する条例（令和５年新島村条例第10号）その他の関係法令等並びにこの基本方針、対策基準及び実施手順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、次の情報セキュリティ対策を講じる。

(1)　組織体制

当村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組織体制を確立する。

(2)　情報資産の分類と管理

当村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行う。

(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３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。

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導入等をいう。）を実施する。

(4)　物理的セキュリティ

情報機器類を設置する場所の安全性の確保、当該場所への入退室の管理等の物理的な対策を講じる。

(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。

(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な対策を講じる。

(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、外部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ものとする。また、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、緊急時対応計画を策定する。

(8)　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。

（情報セキュリティ監査及び自己点検の実施）

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する。

（情報セキュリティポリシーの見直し）

第８条　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となっ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になった場合には、情報セキュリティポリシーを見直す。

（情報セキュリティ対策基準の策定）

第９条　この規則に基づき、情報セキュリティ対策を具体的に実施するに当たっての遵守すべき事項や、判断等の基本的な基準として、情報セキュリティ対策基準（以下「対策基準」という。）を策定するものとする。

（情報セキュリティ実施手順の策定）

第10条　基本方針及び対策基準に基づき、情報セキュリティ対策を実施するため、個々の情報システムについて、具体的な実施手順を明記した情報セキュリティ実施手順（以下「実施手順」という。）を策定するものとする。実施手順は、公開することにより村の行政運営に支障を及ぼす可能性がある情報であることから非公開とする。

附　則

この規則は、平成27年12月10日から施行する。