新島村情報セキュリティ対策基準に関する規則

平成27年12月10日

規則第12号

目次

第１章　総則

（趣旨）

第１条　この規則は、新島村情報セキュリティ基本方針に関する規則（平成27年新島村規則第11号）第９条の規定に基づき、情報セキュリティを確保する上での具体的な措置、遵守すべき行為、判断基準等に関し必要な事項を定めるものとする。

（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　フロッピーディスク、MOディスク、磁気テープ等の取り出し可能な記録媒体をいう。

(3)　ユーザID　情報システムを利用する権利を有する者であることを識別するために割り当てられた文字列をいう。

(4)　パスワード　情報システムを利用する者が本人であることを識別するための暗証文字列をいう。

(5)　ログイン　情報システムを使用可能な状態にする手続をいう。

(6)　プロトコル　ネットワークを介してコンピュータ相互の通信を行うための通信手順

をいう。

(7)　ポート　サーバが他のパソコン等と同時に接続を行うために使われる識別番号をいう。

(8)　アクセス記録　ユーザID、使用した電子情報、使用した日時等の記録をいう。

(9)　データ　電子計算処理（村が管理する電子計算組織による事務の処理をいう。）に係る磁気媒体及び入出力帳票に記載された情報をいう。

2　前項に定めるもののほか、この基準において使用する用語は、新島村情報セキュリティ基本方針に関する規則において使用する用語の例による。

第２章　情報セキュリティ管理体制

（情報セキュリティ管理体制）

第３条　情報セキュリティを総合的、体系的かつ具体的に確保するため、この章に定めるところにより、村の情報セキュリティ管理体制を整備する。

（最高情報セキュリティ責任者）

第４条　当村における全ての情報セキュリティを統括する責任者として、最高情報セキュリティ責任者（以下CISOという。）を置き、副村長をもって充てる。

2　CISOは、当村における重要な情報資産とこれに係る情報システムを総括的に管理し、情報セキュリティ対策を総合的に実施する。

3　CISO は、CISO を助けて当村における情報セキュリティに関する事務を整理し、CISO の命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副 CISO」という。）１人を必要に応じて置く。

4　CISO は、本対策基準に定められた自らの担務を、副 CISO その他の本対策基準に定める責任者に担わせることができる。

（情報セキュリティ管理者）

第５条　各課等における情報セキュリティを統括する責任者として、情報セキュリティ管理者（以下「セキュリティ管理者」という。）を置き、各課長及び課長相当職（議会事務局長を含む。以下「各課長等」という）の職にある者をもって充てる。

2　セキュリティ管理者は、CISOの求めにより情報セキュリティポリシーの実施状況を点検し、報告する。

3　セキュリティ管理者は、課内の情報資産を管理し、当該情報資産に係る情報セキュリティを確保する。

4　セキュリティ管理者は、その所掌する部署において、情報資産に対するセキュリティ侵

害が発生した場合又はセキュリティ侵害のおそれがある場合には、CISO 及び副CISOへ速やかに報告を行い、指示を仰がなければならない。

5　セキュリティ管理者は、所管する部署における情報端末の執務室外での利用及び持込みについて管理するとともに、その管理状況を定期的にシステム管理者に報告しなければならない。

6　セキュリティ管理者は、職員が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（情報システム管理者）

第６条　情報システムの管理運用及び情報システムにおける情報セキュリティの確保に関する責任者として、情報システム管理者（以下「システム管理者」という。）を置き、当該情報システムを運用する課室等の各課長等をもって充てる。

2　システム管理者は、所管する情報システムを適切に管理し、必要に応じて開発、設定の変更、運用、見直し等を行う。

3　システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

4　システム管理者は、システム管理者があらかじめ指定する者を、情報システム担当者(以下「システム担当者」という。）を選任することができる。

5　システム担当者は、システム管理者が行う全ての業務においてこれを補佐する。

（重要事項の協議、調整等）

第７条　情報セキュリティポリシーの策定、運用、評価、見直しその他情報セキュリティに関し重要な事項は、新島村情報化推進委員会設置要綱（平成27年新島村要綱第10号）の規定に基づく新島村情報化推進委員会（以下「委員会」という。）において協議、調整等を行うものとする。

第３章　情報資産の分類と管理

（情報資産の管理者）

第８条　情報資産の管理者は、当該情報資産を作成し、収受し、又は複製した課のセキュリティ管理者とする。

（情報資産の分類と管理）

第９条　情報資産は、新島村文書管理規則に定める取扱いに加え、機密性、完全性及び可用性により、次の各号のとおり分類し、必要に応じ取扱制限を行うものとする。

(1)　機密性による分類

分類	分類基準	取扱制限
自治体機密性3A	行政文書の管理に関するガイドライン（平成23年4月1日内閣総理大臣決定）に定める秘密文書に相当する文書	・指定された端末以外での作業及び持出しの原則禁止
自治体機密性3B	漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体機密性3C	基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産（自治体機密性3B以上に相当するものを除く）	
自治体機密性2	直ちに一般に公表することを前提としていない情報資産（自治体機密性3C以上に相当するものを除く）	・必要以上の複製及び配布禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持込禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・伝送する際には原則として信頼のできるネットワーク回線を選択する ・執務室外等に持ち出す場合は漏えい防止対策を施した上でセキュリティ管理者の許可を得る ・電磁的記録媒体の施錠可能な場所への保管
自治体機密性1	自治体機密性2以上に相当しない情	ー

	報資産	

(2)　完全性による分類

分類	分類基準	取扱制限
自治体完全性2	改ざん、誤り又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ又は電子署名の付与 ・執務室外等に持ち出す、又は持ち込む場合は、改ざん防止対策を施した上でセキュリティ管理者の許可を得る ・電磁的記録媒体の施錠可能な場所への保管
自治体完全性1	自治体完全性2以上に相当しない情報資産	―

(3)　可用性による分類

分類	分類基準	取扱制限
自治体可用性2	滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ及び指定する時間以内の復旧
自治体可用性1	自治体可用性2以上に相当しない情報資産	―

2　前項の分類（以下「重要性分類」という。）は、当該情報資産を所管するセキュリティ管理者が行う。

（重要性分類の表示）

第10条　セキュリティ管理者は、可搬性がある情報システム端末（以下「情報端末」という。）、記録媒体等に重要性分類の表示をする等適切な管理をしなければならない。この場合においては、第三者が重要性分類の識別を容易にすることができないよう留意しなければならない。

（情報資産の取扱い）

第11条　セキュリティ管理者は、情報資産を取り扱う職員（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。）又はその方法を限定する等の措置を講じ、職員に重要性分類に基づいた情報資産の取扱いをさせなければならない。

2　セキュリティ管理者は、自治体機密性２以上又は自治体完全性２以上の情報資産については、施錠が可能な場所への保管等安全な方法で保管しなければならない。

3　セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も前出の分類に基づき管理しなければならない。

4　セキュリティ管理者は、情報資産が業務上の理由なく、定められた場所以外に持ち出され、又は外部に転送されることのないよう措置を講じなければならない。

5　セキュリティ管理者は、重要性分類の区分に応じ、定期的又は随時に情報資産の内容を確認するとともに、データを別の記録媒体に複製してこれを適切に保管する等の措置を講じなければならない。

6　職員等は、業務上必要のない情報を作成してはならない。

7　情報を作成する者は、情報の作成時に前出の分類に基づき、当該情報の分類を定めなければならない。

8　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

9　庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

10　庁外の者が作成した情報資産を入手した者は、前出の分類に基づき、当該情報の分類を定めなければならない。

11　情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

12　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

13　情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

14　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

15　セキュリティ管理者又はシステム管理者は、情報資産の分類に従って、情報資産を適

正に保管しなければならない。

16　セキュリティ管理者又はシステム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

17　セキュリティ管理者又はシステム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

18　セキュリティ管理者又はシステム管理者は、自治体可用性以上の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

19　電子メール等により自治体機密性２以上の情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

20　車輌等により自治体機密性２以上又は自治体完全性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

21　自治体機密性２以上又は自治体完全性２以上の情報資産を運搬する者は、セキュリティ管理者に許可を得なければならない。

22　自治体機密性２以上又は自治体完全性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

23　自治体機密性２以上又は自治体完全性２以上の情報資産を外部に提供する者は、セキュリティ管理者に許可を得なければならない。

24　セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

（情報資産の廃棄）

第12条　職員は、自治体機密性２以上の情報資産を廃棄する場合は、当該情報資産を所管するセキュリティ管理者の許可を受けることとし、行った処理について、日時、担当者及び処理内容を記録しなければならない。

２　職員は、自治体機密性２以上の情報資産を記録した媒体が不要となった場合は、当該情報資産の内容が復元されることがないよう、消去を行った上で廃棄しなければならない。

第４章　物理的セキュリティ対策

（情報システム全体の強靭性の向上）

第13条　マイナンバー利用事務系と他の領域は分離し、基本的に相互通信できないように

しなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

2　マイナンバー利用事務系の情報へのアクセスに当たっては情報システムが正規の利用者かどうかを判断する認証手段のうち、２つ以上を併用する認証（多要素認証）を利用しなければならない。

3　マイナンバー利用事務系の情報については、原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

4　LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをLGWAN 接続系に取り込む場合は、セキュリティ管理者の許可を得て指示された方法でのみ行う。

5　インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及びLGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

（情報システム等の管理）

第14条　セキュリティ管理者は、所管する情報システム及び情報資産の管理に関し、次の各号に掲げる事項について、当該各号に定めるセキュリティ対策を実施し、必要に応じてシステム管理者に報告しなければならない。

(1)　機器の設置

ア　火災、水害、ほこり、振動、温度、湿度、静電気、電磁波等の影響を可能な限り排除した場所に設置し、容易に取り外せないように固定する等の措置を講じること。

イ　自治体可用性２以上の情報資産を格納及び運用しているホストコンピュータ、サーバ等（以下「重要な情報システム」という。）については、二重化、ミラーリング等の措置をとり、システムの運用に支障を来さないよう措置を講じること。

ウ　重要な情報システムのメインサーバに障害が発生した場合には、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にすること。

エ　重要な情報システムについては、システム管理者、職員及び契約により操作を認め

られた委託事業者以外の者が容易に操作できないように、利用者のID及びパスワードの設定等の措置を講じること。

オ　重要な情報システムにおける基幹機器の取付けに当たっては、配線等から放射される電磁波により、情報が漏えいすることのないよう必要な措置を講じること。

カ　村庁舎以外の場所に重要な情報システムを設置する場合は、CISOの承認を受けるとともに、設置後も、情報セキュリティ対策について定期的な点検を行う等、適切に管理すること。

(2)　電源

ア　重要な情報システム及びそれに記録されている情報資産を、落雷等による停電又は過電流から保護するため、必要な措置を講じること。

イ　システム管理者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けること。

(3)　配線

ア　システム管理者及び施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じること。

イ　主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、システム管理者と連携して対応すること。

ウ　システム管理者と連携し、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理すること。

エ　自ら又はシステム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じること。

(4)　機器の保守、修理及び廃棄

ア　電磁的記録媒体を内蔵する機器を事業者に保守又は修理させる場合、委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

イ　記録装置が含まれる情報端末等の機器を廃棄する場合は、当該記録装置に保存されている電子情報の消去、記録装置の破砕等を行い、当該電子情報が復元不可能な状態にしなければならない。

（管理区域の整備）

第15条　セキュリティ管理者は、重要な情報システムの設置又は自治体機密性２以上、自

治体完全性２以上、又は自治体可用性２以上のネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋や電磁的記録媒体の保管庫（以下「管理区域」という。）の整備をする場合は、次の各号に掲げる事項について、当該各号に定めるセキュリティ対策を実施しなければならない。

(1)　管理区域の整備

ア　施設管理部門や外部委託事業者と連携し、水害対策及び確実な入退室管理が行えるよう、設置場所について配慮すること。

イ　施設管理部門や外部委託事業者と連携し、ドア、窓等の開口部は必要最小限にとどめ、鍵、警報装置等を設置して不正な立入りを防止できるようにすること。

ウ　施設管理部門や外部委託事業者と連携し、特に厳重に耐震及び耐火対策を講じること。

エ　施設管理部門や外部委託事業者と連携し、機器及び記録媒体に損傷を与えるおそれのない消火剤を備えること。

オ　施設管理部門や外部委託事業者と連携し、電気容量又は空調能力の不足等により、基幹機器の運用に支障が生じないことを事前に確認すること。

(2)　管理区域の入退室管理

ア　外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された者が付き添うものとし、外見上でそれと分かる措置を講じなければならない。

イ　管理区域内には、当該情報システムに関連しない、又は個人所有である記憶媒体、電子計算機、ネットワーク等を持ち込ませないようにしなければならない。

(3)　通信回線及び通信回線装置の管理

ア　庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

イ　通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

ウ　外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

エ　行政系のネットワークを総合行政ネットワーク(LGWAN)に集約するように努めなければならない。

オ　自治体機密性２以上又は自治体完全性２以上の情報資産を取り扱う情報システム

に通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

カ　ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

キ　自治体可用性２以上の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

２　システム管理者は、前項の各号に加えて、次の各号に掲げる事項について、当該各号に定めるセキュリティ対策を実施しなければならない。

(1)　管理区域の入退室管理

ア　管理区域への入退室を許可された者のみに制限し、IC カード等による施錠・解錠システムや入退室管理簿の記載等による入退室管理を行わなければならない。

イ　外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員が付き添うものとし、外見上職員と区別できる措置を講じなければならない。

ウ　自治体機密性２以上又は自治体完全性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

(2)　機器等の搬入出

ア　搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託事業者に確認を行わせなければならない。

イ　外部からの訪問者等が行う室内への機器等の搬入出について、職員を立ち会わせなければならない。

(3)　職員の利用する端末や電磁的記録媒体等の管理

ア　盗難防止のため、執務室等で利用する情報端末のワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。

イ　電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

ウ　自治体機密性２以上又は自治体完全性２以上の情報を取り扱う情報システムへのログインに際し、パスワードの他に、IDカード、多要素認証アプリ或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

エ　マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち２つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

オ　情報端末等におけるデータの暗号化等の機能を有効に利用しなければならない。

３　管理区域に入室する者は、身分証明書等を携帯し、求めにより提示しなければならない。

第５章　人的セキュリティ対策

（職員の責務）

第16条　職員等は、情報セキュリティポリシー及び情報セキュリティ実施手順並びに本条各項で定めることを遵守しなければならない。

２　職員は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

３　職員は、情報端末等に周辺機器等を接続してはならない。ただし、システム管理者の許可を受けた場合は、この限りでない。

４　職員は、情報端末にソフトウェアをインストールし、又は情報端末からソフトウェアをアンインストールしてはならない。ただし、システム管理者の許可を受けた場合は、この限りでない。

５　情報端末等を執務室外で使用する場合は、セキュリティ管理者の許可を得なければならない。

６　支給又は貸与を受けた以外の情報端末等を業務に使用してはならない。ただし、システム管理者の許可を受けた場合は、この限りでない。

７　情報端末等のセキュリティ機能の設定をシステム管理者(その所管がセキュリティ管理者の場合にあってはセキュリティ管理者）の許可なく変更してはならない。

８　情報端末等及びその情報が印刷された文書等について、第三者に使用されること又はシステム管理者（その所管がセキュリティ管理者の場合にあってはセキュリティ管理者）の許可なく情報を閲覧されることがないように、離席時の情報端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

９　異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、重要性分類の別に関わらず、業務上知り得た情報の一切を漏らしてはならない。

（臨時職員等の任用時の説明等）

第17条　セキュリティ管理者は、その形態を問わず一時的に任用する職員（以下、臨時職員等という）が情報端末等を利用した職務をさせる場合は、任用に当たって、当該職員が遵守すべき情報セキュリティポリシー、実施手順及び関係法令等について説明しなければならない。

2　セキュリティ管理者は、前項の場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（教育及び訓練）

第18条　CISOは、職員に対し、必要に応じて情報セキュリティポリシーに関する説明、研修等を実施し、情報セキュリティポリシーの啓発に努めなければならない。

2　CISO は、必要に応じ、緊急時対応を想定した訓練を実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

3　全て職員（特別職や一時的に任用している職員等を含む）は、定められた研修・訓練に参加しなければならない。

（事故及び欠陥の対処）

第19条　職員は、情報セキュリティに関する事故（データファイルの漏えい、滅失、改ざん、毀損等の事故をいう。）又は情報システム上の欠陥若しくは誤動作（以下「事故等」という。）が発生した場合は、直ちにセキュリティ管理者に報告し、システム管理者の指示に従い、必要な措置を講じなければならない。

2　システム管理者は、事故等の報告を受けた場合において、当該事故等の影響が重大と認められるときは、CISOに報告しなければならない。

3　CISOは、情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。

4　システム管理者及びセキュリティ管理者は、事故等の再発防止のため、発生した事故等を分析し、当該事故等に関する記録を保存しなければならない。

（侵害時の対応）

第20条　システム管理者及びセキュリティ管理者は、情報セキュリティ侵害事件が発生した場合の対応について、緊急連絡体制、証拠保全、被害の拡大防止、復旧等の必要な措置を情報システムごとに実施手順に定めなければならない。

2　職員は、当村が管理するネットワーク及び情報システム等の情報資産に関する情報セキ

ュリティインシデントについて、住民等外部から報告を受けた場合、セキュリティ管理者に報告しなければならない。

3　住民等外部から報告を受けたセキュリティ管理者は、速やかにCISO及びシステム管理者に報告しなければならない。

（教育及び訓練）

第21条　CISOは、職員に対し、情報セキュリティポリシーに関する説明、研修等を実施し、情報セキュリティポリシーの啓発に努めなければならない。

2　システム管理者及びセキュリティ管理者は、情報セキュリティ、情報通信技術等に関する研修を受講するなど、必要な知識の維持及び習得に努めなければならない。

3　セキュリティ管理者は、重要な情報資産を運用している情報システムについて、緊急時対応計画に基づく訓練を情報システムの運用に支障がない範囲で実施し、情報資産の漏えい等の事故が発生した場合に職員が即応できる体制を整えなければならない。

4　職員は、情報セキュリティポリシーに関する研修等を受講し、情報セキュリティポリシー及び実施手順を理解することにより、情報セキュリティに関する支障が生じないようにしなければならない。

（ID及びパスワード等の管理）

第22条　職員は、当村より貸与されたIC カード等に関し、次の事項を遵守しなければならない。

(1)　認証に用いる IC カード等を、セキュリティ管理者の許可なく職員間で共有してはならない。

(2)　業務上必要のないときは、IC カード等をカードリーダ又は情報端末等から抜いておかなければならない。

(3)　IC カード等を紛失した場合には、速やかにセキュリティ管理者及び情報システム管理者に通報し、指示に従わなければならない。

2　セキュリティ管理者及びシステム管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

3　セキュリティ管理者及びシステム管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

4　職員は、自己の管理する ID に関し、次の事項を遵守しなければならない。

(1)　自己が利用している ID は、他人に利用させてはならない。

(2)　共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

5　職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

(1)　パスワードは、他者に知られないように管理しなければならない。

(2)　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

(3)　パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。

(4)　パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

(5)　複数の情報システムを扱う職員は、同一のパスワードをシステム間で用いてはならない。

(6)　仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

(7)　職員間でパスワードを共有してはならない（ただし、共用 ID に対するパスワードは除く）。

第６章　技術的セキュリティ対策

（ネットワーク等の管理）

第23条　システム管理者は、ネットワーク等の管理に関し、次の各号に掲げる事項について、当該各号に定めるセキュリティ対策を実施しなければならない。

(1)　管理記録及び障害記録

ア　情報システムにおいて行った変更等の作業については、記録を作成し、適切な管理を行うこと。

イ　職員から報告のあった情報システムの障害に対する処理及び問題等は、障害記録として体系的に記録し、常に活用できるよう保存すること。

(2)　情報システム仕様書等の管理　情報システム仕様書、ネットワーク構成図等のネットワーク等に関する技術情報については、記録する媒体にかかわりなく業務上必要とする者のみが閲覧できる場所に保管すること。

（アクセス制御）

第24条　システム管理者は、ネットワーク等におけるアクセスの制御に関し、次の各号に掲げる事項について、当該各号に定めるセキュリティ対策を実施しなければならない。

(1)　情報端末及び利用者の登録手続等　情報端末及び利用者の登録、変更又は抹消の手続、登録情報の管理の方法等について、実施手順に定めること。

(2)　管理者権限の付与　管理者権限（サーバの管理を行うための操作権限をいう。以下

同じ。）は、システム管理者があらかじめ指名する必要最小限の者に与えること。

(3)　端末接続の管理

ア　接続された情報端末を機器固有情報等の識別コードで自動的に識別する等の措置を通信機器に講じることにより、不正接続を防止すること。

イ　ルータの設置等により適切なネットワーク経路制御を施すこと。

ウ　情報システムごとにログイン権限を定め､資格のない職員等がシステムにアクセスできないよう制限すること。

(4)　ネットワークの外部からのアクセス　ネットワークの外部からのアクセスを認める情報システムは最小限に限定し､原則として､ネットワークの外側に設置したサーバのみ認めることとし、適正なアクセスであることを確認できる措置をとること。

(5)　外部ネットワークとの接続　外部のネットワークとの接続に当たっては、当該ネットワークの構成､機器､セキュリティレベル等を詳細に確認し､村が管理する情報システム及び情報資産に対する影響の有無を検証した上で統括責任者の許可を得ること。

(6)　ログインに関する設定　ログイン及びログアウト時刻等を記録し、ログインの試行回数を制限する等適切に管理すること。

(7)　接続時間の制限　管理者権限によるアクセス時間は、必要最小限に制限すること。

（不正アクセス対策）

第25条　システム管理者は、不正アクセス対策に関し、次に掲げるセキュリティ対策を実施しなければならない。

(1)　使用が終了し、又は使用される予定のないポートを長時間開放したままの状態にしないこと。

(2)　重要な情報システムの設定に係るファイル等については、当該ファイルが改ざんされていないことを定期的に確認すること。

(3)　ネットワーク内の情報端末からの不正アクセスが発見された場合、システム管理者は､直ちに当該端末を管理するセキュリティ管理者に通知し､接続の切断､不正アクセスを行った者の特定等、適切な処置を求めること。

(4)　不正アクセスによる被害を受けた場合は、その記録を保存するとともに、警察等との緊密な連携に努め、再発の防止を図ること。

（コンピュータウイルス対策）

第26条　システム管理者は、コンピュータウイルス対策として、次に掲げるセキュリティ対策を実施しなければならない。

(1)　外部のネットワークに情報若しくはソフトウェアを送信する場合又は外部のネットワークから情報若しくはソフトウェアを受信する場合は、ネットワークの接続ポイントにおいてウイルスチェックを行うとともに、サーバ及び情報端末において、定期的なウイルスチェックを行うこと。

(2)　ネットワークの外部から情報媒体を使用して情報若しくはソフトウェアを移入する場合又はネットワークの外部に情報媒体を使用して情報若しくはソフトウェアを移出する場合は、事前にウイルスチェックを行うこと。

(3)　ウイルスチェックに用いるパターンファイルは、常に最新のものにすること。

(4)　ウイルスに関する情報の収集に努め、セキュリティ管理者、セキュリティ管理者及び職員に対して、最新の情報を提供すること。

（情報システムの導入）

第27条　システム管理者は、情報システムを新規に導入する場合は、既に稼動している情報システムに接続する前に十分なテストを実施し、情報セキュリティに関する支障の有無を確認しなければならない。

（変更記録の管理）

第28条　システム管理者は、情報システムにおいて行ったシステム変更等の作業について、記録を作成し、適切に管理しなければならない。

（サーバの設定等）

第29条　システム管理者は、サーバを課の単位で構成し、職員が他課のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

2　システム管理者は、住民の個人情報、人事記録等、特定の職員しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同じ課であっても、担当職員以外の職員が閲覧及び使用できないようにしなければならない。

（バックアップの実施）

第30条　セキュリティ管理者及びシステム管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策にかかわらず、必要に応じて定期的にバックアップを実施しなければならない。

2　セキュリティ管理者及びシステム管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。

3　セキュリティ管理者及びシステム管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアッ

プを取得し保管しなければならない。

（他団体との情報システムに関する情報等の交換）

第31条　システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、セキュリティ管理者及び情報セキュリティ責任者の許可を得なければならない。

（システム管理記録及び作業の確認）

第32条　システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

２　セキュリティ管理者及びシステム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

３　セキュリティ管理者、システム管理者又はシステム担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

（情報システム仕様書等の管理）

第33条　セキュリティ管理者及びシステム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体にかかわらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

（外部の者が利用できるシステムの分離等）

第34条　汎用受付システム等の職員以外の者が利用できる情報システムについては、必要に応じ他の情報システムと物理的に分離し、又はファイアウォールを設置する等により、情報の漏えい、村の有する他の情報システムへの侵入等を防止するための措置をとること。

（無線LAN 及びネットワークの盗聴対策）

第35条　システム管理者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

２　システム管理者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（電子メールのセキュリティ管理）

第36条　システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定

を行わなければならない。

2　システム管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

（電子メールの利用制限）

第37条　職員は、業務上必要のない送信先に電子メールを送信してはならない。

2　職員は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

（電子署名・暗号化）

第38条　職員は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

（情報システムにおける入出力データの正確性の確保）

第39条　システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

2　システム管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(1)　利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直ししなければならない。

(2)　運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

(3)　ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

(4)　システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（情報システムの監視）

第40条　セキュリティ管理者及びシステム管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

2　セキュリティ管理者及びシステム管理者は、情報システムの情報セキュリティ対策につ

いて新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

3　セキュリティ管理者及びシステム管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

4　セキュリティ管理者及びシステム管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

5　セキュリティ管理者及びシステム管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

6　セキュリティ管理者及びシステム管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

7　セキュリティ管理者及びシステム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

8　セキュリティ管理者及びシステム管理者は、外部と常時接続するシステムを常時監視しなければならない。

9　暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

（情報セキュリティポリシーの遵守状況の確認）

第41条　情報セキュリティ責任者及びセキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及びセキュリティ管理者に報告しなければならない。

2　CISO は、発生した問題について、適正かつ速やかに対処しなければならない。

3　セキュリティ管理者及びシステム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

4　CISO 及び CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員が使用している情報端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

5　職員は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちにセキュリティ管理者及びセキュリティ管理者に報告を行わなければならない。

6　当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があるとセキュリティ管理者が判断した場合において、職員は、その指示に従い適正に対処しなければならない。

（例外措置）

第42条　セキュリティ管理者及びシステム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、CISOの許可を得て、例外措置を講じることができる。

2　セキュリティ管理者及びシステム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに CISOに報告しなければならない。

3　CISO は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

（法令遵守）

第43条　職員は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

(1)　地方公務員法（昭和25年法律第261号）

(2)　著作権法（昭和45年法律第48号）

(3)　不正アクセス行為の禁止等に関する法律（平成11年法律第128号）

(4)　個人情報の保護に関する法律（平成15年法律第57号）

(5)　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）

(6)　サイバーセキュリティ基本法（平成26年法律第104号）

（懲戒処分等）

第44条　情報セキュリティポリシーに違反した職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

2　職員の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

(1)　セキュリティ管理者が違反を確認した場合は、セキュリティ管理者は当該職員が所属する課室等のセキュリティ管理者に通知し、適正な措置を求めなければならない。

(2)　システム管理者等が違反を確認した場合は、速やかにセキュリティ管理者及び当該

職員が所属する課室等のセキュリティ管理者に通知し、適正な措置を求めなければならない。

(3) セキュリティ管理者の指導によっても改善されない場合、セキュリティ管理者は、当該職員のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、セキュリティ管理者は、職員の権利を停止あるいは剥奪した旨を CISO 及び当該職員が所属する課室等のセキュリティ管理者に通知しなければならない。

（業務委託と外部サービスの利用）

第45条 セキュリティ管理者又はシステム管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

(1) 仕様に準拠した提案

(2) 契約の締結

2 セキュリティ管理者又はシステム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。

(1) 契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

(2) セキュリティ管理者へ措置内容の報告（重要度に応じて CISO に報告）

(3) 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

3 セキュリティ管理者又はシステム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。

(1) 情報の適正な取扱いのための情報セキュリティ対策

(2) 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

(3) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

4 セキュリティ管理者又はシステム管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

(1) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

(2)　委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

5　セキュリティ管理者又はシステム管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。

(1)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

(2)　提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

（情報システムに関する業務委託）

第46条　システム管理者は、情報システムに関する業務委託の実施までに、情報システムに当村の意図せざる変更が加えられないための対策を仕様に加えなければならない。

2　システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

(1)　情報システムのセキュリティ要件の適切な実装

(2)　情報セキュリティの観点に基づく試験の実施

(3)　情報セキュリティの観点に基づく試験の実施

3　システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

4　システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

第７章　監査、評価等

（点検）

第47条　セキュリティ管理者は、情報セキュリティ対策の実施状況について定期的に点検を行い、その結果をシステム管理者に報告しなければならない。

2　システム責任者は、前項の報告内容が情報セキュリティの確保に重大な影響を及ぼすと判断した場合は、速やかにCISO及び委員会に報告しなければならない。

3　委員会は、前項の報告結果を情報セキュリティポリシーの評価及び見直しのための資料として活用するものとする。

4　システム管理者は、所管する情報システムについて定期的に点検を行い、問題を発見し

た場合は速やかに対処しなければならない。

（監査）

第48条　委員会は、情報セキュリティポリシーの実効性を検証するため、必要に応じて監査を実施しなければならない。

２　委員会は、監査の結果を評価し、その内容をCISOに報告しなければならない。

３　委員会は、監査の結果、情報セキュリティポリシーの改定が必要と認められるときは、CISOにその改定を進言するものとする。

（情報セキュリティポリシーの改定等）

第49条　CISOは、システム管理者及びセキュリティ管理者の報告、委員会の監査結果の報告等を踏まえ、情報セキュリティポリシーの改定等が必要と認めるときは、適宜その改定等の措置を講じるものとする。

第８章　補則

（その他）

第50条　この規則に定めるもののほか、必要な事項は、別に定める。

附　則

この規則は、平成27年12月10日から施行する。