宮古市
情報セキュリティ
対策基準

令和７年２月

宮古市 総務部 デジタル推進課

目　次

宮古市情報セキュリティ対策基準

本対策基準は、宮古市情報セキュリティ基本方針を実行に移すため、本市における情報資産に関する情報セキュリティ対策の基準を定めることを目的とする。

本対策基準における用語の意義は、宮古市情報セキュリティ基本方針に規定する定義を準用する。

１　組織体制

（１）最高情報セキュリティ責任者（ＣＩＳＯ: Chief Information Security Officer、以下「ＣＩＳＯ」という。）

①副市長を、ＣＩＳＯとする。ＣＩＳＯは、本市における全ての情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

②ＣＩＳＯは、情報セキュリティインシデントに対処するための体制（ＣＳＩＲＴ:Computer Security Incident Response Team、以下「ＣＳＩＲＴ」という。）を整備し、役割を明確化する。

（２）統括情報セキュリティ責任者

①総務部長を、ＣＩＳＯ直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、ＣＩＳＯを補佐しなければならない。

②統括情報セキュリティ責任者は、本市の全ての情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③統括情報セキュリティ責任者は、本市の全ての情報資産における情報セキュリティ対策に関する権限及び責任を有する。

④統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤統括情報セキュリティ責任者は、本市の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、ＣＩＳＯの指示に従い、ＣＩＳＯが不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

⑥統括情報セキュリティ責任者は、本市の情報資産に関する共通的な情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑧統括情報セキュリティ責任者は、緊急時には、ＣＩＳＯに早急にその内容を報告するとともに、回復のための対策を講じなければならない。

⑨統括情報セキュリティ責任者は、情報セキュリティポリシー及び関係規程等に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じてＣＩＳＯにその内容を報告しなければならない。

（３）情報セキュリティ責任者

①市長部局の部及び監、上下水道部、議会事務局並びに教育委員会事務局（以下「部等」という。）の長を、情報セキュリティ責任者とする。

②情報セキュリティ責任者は、その所管する部等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③情報セキュリティ責任者は、その所管する部等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④情報セキュリティ責任者は、その所管する部等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守状況の確認並びに職員及び会計年度任用職員（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

（４）情報セキュリティ管理者

①市長部局の課、センター及び支所、上下水道部の課、議会事務局、教育委員会事務局の課、選挙管理委員会事務局、監査委員事務局並びに農業委員会事務局（以下「課等」という。）の長を、情報セキュリティ管理者とする。

②情報セキュリティ管理者は、その所管する課等の情報セキュリティ対策に関する権限及び責任を有する。

③情報セキュリティ管理者は、その所管する課等において、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、情報セキュリティ責任者及び情報システム管理者に速やかにその内容を報告し、指示を仰がなければならない。

（５）情報システム管理者

①デジタル推進課長を、本市の全ての情報システムに関する情報システム管理者とする。

②情報システム管理者は、本市の全ての情報システム（部等において所有している情報システムを除く）における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③情報システム管理者は、本市の全ての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情報システム管理者は、本市の全ての情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（６）情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、見直し等の作業を行う者を、情報システム担当者とする。

（７）宮古市デジタル戦略推進本部

本市の情報セキュリティ対策を統一的に実施するため、宮古市デジタル戦略推進本部において、情報セキュリティポリシーその他情報セキュリティに関する重要な事項を決定する。

（８）兼務の禁止

①情報セキュリティ対策の実施において、承認又は許可の申請を行う者とその承認者又は許可者は、やむを得ない場合を除き、同じ者が兼務してはならない。

②情報セキュリティ監査の実施において､監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（９）ＣＳＩＲＴの設置・役割

①ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化しなければならない。

②ＣＩＳＯは、ＣＳＩＲＴに所属する職員等を選任し、その中からＣＳＩＲＴ責任者を置かなければならない。また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員等を定めなければならない。

③ＣＩＳＯは、情報セキュリティに関する統一的な窓口を整備し、情報セキュリティインシデントについて部等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

④ＣＳＩＲＴは、ＣＩＳＯによる情報セキュリティインシデントへの対応方針等の意思決定が行われた際には、その内容を関係する部等に周知しなければならない。

⑤ＣＳＩＲＴは､情報セキュリティインシデントを認知した場合には､必要に応じて、ＣＩＳＯ、総務省、岩手県及び個人情報保護委員会へ報告しなければならない。

⑥ＣＳＩＲＴは、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

⑦ＣＳＩＲＴは、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行わなければならない。

２　情報資産の分類と管理

（１）情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	・宮古市情報公開条例（平成17年条例第11号）第５条に規定する不開示情報（以下「不開示情報」という。）のうち、特定の職員その他必要最小限の者のみが扱う情報 ・特定個人情報 ・上記の情報を記録した電磁的記録媒体、紙その他の媒体（以下「記録媒体」という。）	・支給以外（市所有以外をいう。以下同じ。）の端末での作業の原則禁止 ・必要以上の複製及び配付禁止 ・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ち込み禁止 ・情報の送信、情報資産の運搬・提供時におけるパスワード等による暗号化、鍵付きケースへの格納等 ・復元不可能な処理を施しての廃棄等 ・信頼のできるネットワーク回線の選択 ・外部で情報処理作業を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	・不開示情報のうち、機密性３の情報以外の情報 ・上記の情報を記録した記録媒体	
機密性１	・機密性２又は機密性３の情報資産以外の情報資産	

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	・改ざん、誤びゅう又は破損により、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 ・上記の情報を記録した記録媒体	・バックアップ、電子署名付与 ・外部で情報処理作業を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	・完全性２の情報資産以外の情報資産	

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	・滅失、紛失又は当該情報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 ・上記の情報を記録した記録媒体	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	・可用性２の情報資産以外の情報資産	

（２）情報資産の管理

①管理責任

（ア）情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

（イ）情報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情報資産の分類に基づき管理しなければならない。

②情報資産の分類の表示

職員等は、機密性２以上、完全性２又は可用性２の情報資産について、ファイル（ファイル名、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示しなければならない。ただし、次に該当する場合は、この限りでない。

（ア）情報システムを稼働又は監視するためのプログラム、ログ等（システム内部に存在する場合に限る）

（イ）次のシステムで取り扱う場合（システム内部に存在する場合に限る）

・マイナンバー利用事務系のシステム

・ＣＩＳＯが別に定める特定業務システム

（ウ）外部に提供する場合

③情報の作成

（ア）職員等は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、情報の作成時に情報資産の分類基準に基づき、当該情報の分類を定めなければならない。

（ウ）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。

④情報資産の入手

（ア）情報資産を入手した者は、情報資産の分類基準に基づき、当該情報の分類を定め、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。

（イ）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。

⑤情報資産の利用

（ア）情報資産を利用する者は、業務以外の目的で情報資産を利用してはならない。

（イ）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。

（ウ）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。

⑥情報資産の保管

（ア）情報セキュリティ管理者又は情報システム管理者は､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。

（イ）情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報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。

（ウ）情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合は、必要に応じ、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。

⑦情報の送信

電子メール等により機密性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。

⑧情報資産の運搬

（ア）車両等により機密性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。

（イ）機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者の許可を得なければならない。

⑨情報資産の提供・公表

（ア）機密性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。

（イ）機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者の許可を得なければならない。

（ウ）情報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。

⑩情報資産の廃棄等

（ア）機密性２以上の情報を記録した記録媒体の廃棄、リース返却等を行う者は、ソフトウェアによる処理等により情報を復元できないように処置した上で行わなければならない。

（イ）機密性２以上の情報を記録した記録媒体の廃棄、リース返却等を行う者は、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。

（ウ）機密性２以上の情報を記録した記録媒体の廃棄、リース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

３　情報システム全体の強靭性の向上

（１）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系は､他の領域と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。この場合、その外部接続先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でのデータの移送を可能とする。

②情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認定手段は、二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。また、業務毎に専用端末を設置することが望ましい。

（イ）情報の持ち出し不可設定

マイナンバー利用事務系は、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の持ち出しができないように設定しなければならない。

（２）ＬＧＷＡＮ接続系

①ＬＧＷＡＮ接続系とインターネット接続系の分割

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、電子メールやデータをＬＧＷＡＮ接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

（ア）インターネット環境で受信したインターネットメールの本文のみをＬＧＷＡＮ接続系に転送するメールテキスト化方式

（イ）インターネット接続系の端末から、ＬＧＷＡＮ接続系の端末へ画面を転送する方式

（ウ）危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

（３）インターネット接続系

①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。

②インターネット接続系の運用においては、岩手県が整備する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

４　物理的セキュリティ

4.1　執務室等の管理

①ＣＩＳＯは、情報資産の盗難、漏えい等を防止するため、執務室等にセキュリティ区画を設定し、職員等以外の者の執務室等への入退室の制限その他の管理基準を定めなければならない。

②情報セキュリティ管理者は、ＣＩＳＯが定めたセキュリティ区画の管理基準に従って、所管する執務室等を適正に管理しなければならない。

③職員等は、ＣＩＳＯが定めたセキュリティ区画の管理基準を遵守しなければならない。

4.2　サーバ等の管理

（１）機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度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適正に固定する等、必要な措置を講じなければならない。

（２）機器の電源

①情報システム管理者は、統括情報セキュリティ責任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なければならない。

②情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（３）通信ケーブル等の配線

①統括情報セキュリティ責任者及び情報システム管理者は、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なければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、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、連携して対応しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、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しなければならない。

④統括情報セキュリティ責任者及び情報システム管理者は、情報システム担当者及び契約により操作を認められた外部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なければならない。

（４）機器の定期保守及び修理

①情報システム管理者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

②情報システム管理者は、機密性２以上の情報を記録した電磁的記録媒体を内蔵する情報機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を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を行わなければならない。

（５）庁外への機器の設置

統括情報セキュリティ責任者及び情報システム管理者は、庁外に機密性２以上の情報を取り扱うサーバ等の機器を設置する場合、ＣＩＳＯの承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（６）機器の廃棄等

情報システム管理者は、機密性２以上の情報を取り扱うサーバ等の機器の廃棄、リース返却等をする場合、当該機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

4.3　管理区域（サーバ室等）の管理

（１）管理区域の構造等

①管理区域とは、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（以下「サーバ室」という。）並びに機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体の保管庫をいう。

②統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

④統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（２）管理区域の入退室管理等

①情報システム管理者は、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、指紋認証等の生体認証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。

②職員等及び外部委託事業者は、管理区域に入室する場合、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。

③情報システム管理者は、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等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

④情報システム管理者は、機密性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、当該システムに関連しない、又は個人所有であるパソコン、モバイル端末、通信回線装置、電磁的記録媒体その他の情報機器を持ち込ませないようにしなければならない。

（３）機器等の搬入出

①情報システム管理者は、管理区域に搬入する機器等が、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した業者に確認させなければならない。

②情報システム管理者は、サーバ室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。

4.4　通信回線及び通信回線装置の管理

①統括情報セキュリティ責任者は、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。

②統括情報セキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、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。

③統括情報セキュリティ責任者は、 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。

④統括情報セキュリティ責任者は、行政系のネットワークをＬＧＷＡＮに集約するように努めなければならない。

⑤統括情報セキュリティ責任者は、機密性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。

⑥統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報の破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

⑦統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアについて、脆弱性を解決するための修正が含まれているバージョンアップがある場合、適用した際の通信への影響等を十分に考慮した上で、遅滞なく適用しなければならない。

⑧統括情報セキュリティ責任者は、可用性２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。

4.5　職員等が利用する端末等の管理

①情報セキュリティ管理者及び情報システム管理者は、盗難防止のため、その所管する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。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。

②情報セキュリティ管理者及び情報システム管理者は、その所管する情報システムへのログインに際し、ＩＤ、パスワード、ＩＣカード、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。

③情報システム管理者は、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二つ以上を併用する多要素認証を行うよう設定しなければならない。

５　人的セキュリティ

5.1　職員等の遵守事項

（１）職員等の遵守事項

①情報セキュリティポリシー等の遵守

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（以下「情報セキュリティポリシー等」という。）を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

②業務以外の目的での使用の禁止

職員等は、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モバイル端末等の持ち出し及び外部における情報処理作業の制限

（ア）ＣＩＳＯは、機密性２以上、完全性２又は可用性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ）職員等は、本市のモバイル端末、電磁的記録媒体その他の情報機器を外部に持ち出す場合には、当該機器を所管する情報セキュリティ管理者又は情報システム管理者の許可を得なければならない。

（ウ）職員等は、外部で情報処理作業を行う場合には、当該作業で使用する機器を所管する情報セキュリティ管理者又は情報システム管理者の許可を得なければならない。また、作業に当たっては、安全管理措置を遵守しなければならない。

④支給以外のパソコン等の業務利用

職員等は、支給以外のパソコン、モバイル端末、電磁的記録媒体その他の情報機器を原則業務に利用してはならない。ただし、業務上必要な場合は、情報システム管理者の許可を得て利用することができる。

⑤持ち出し及び持ち込みの記録

情報システム管理者は、モバイル端末、電磁的記録媒体その他の情報機器の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報システム管理者の許可なく変更してはならない。

⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び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情報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、離席時のパソコン、モバイル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。

⑧退職時等の遵守事項

職員等は、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、その後も業務上知り得た情報を漏らしてはならない。

（２）会計年度任用職員への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、会計年度任用職員に対し、情報セキュリティポリシー等のうち、会計年度任用職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、会計年度任用職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、会計年度任用職員にパソコンやモバイル端末による作業を行わせる場合において、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。

（３）情報セキュリティポリシー等の掲示

統括情報セキュリティ責任者は、職員等が常に情報セキュリティポリシー等を閲覧できるように掲示しなければならない。

（４）外部委託事業者に対する説明

情報セキュリティ管理者は、機密性２以上、完全性２又は可用性２の情報を取り扱う業務を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等の遵守及び委託業務における機密事項を説明しなければならない。

5.2 研修・訓練

（１）情報セキュリティに関する研修・訓練

ＣＩＳＯは、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（２）研修計画の策定及び実施

①ＣＩＳＯは、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、宮古市デジタル戦略推進本部の承認を得なければならない。

②ＣＩＳＯは、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

③研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

④ＣＩＳＯは、毎年度１回、宮古市デジタル戦略推進本部に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（３）緊急時対応訓練

ＣＩＳＯは、緊急時対応を想定した訓練を定期的に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、効果的に実施できるようにしなければならない。

（４）研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

5.3 情報セキュリティインシデントの報告等

（１）情報セキュリティインシデントの報告

①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③報告を受けた情報セキュリティ責任者は、速やかに統括情報セキュリティ責任者に報告しなければならない。
④報告を受けた統括情報セキュリティ責任者は、速やかにＣＩＳＯに報告しなければならない。

（２）情報セキュリティインシデントの原因究明等
①ＣＳＩＲＴは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。
②ＣＳＩＲＴは、情報セキュリティインシデントであると評価した場合は、ＣＩＳＯに速やかに報告しなければならない。
③ＣＳＩＲＴは、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。
④ＣＳＩＲＴは、報告された情報セキュリティインシデントの原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、ＣＩＳＯに報告しなければならない。
⑤ＣＩＳＯは、ＣＳＩＲＴから、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

5.4　ＩＤ及びパスワード等の管理

（１）ＩＣカード等の取扱い
①職員等は、自己の管理するＩＣカードその他の認証媒体（以下「ＩＣカード等」という。）に関し、次の事項を遵守しなければならない。
（ア）認証に用いるＩＣカード等を、職員等間で共有してはならない。
（イ）業務上必要のないときは、ＩＣカード等をカードリーダ、パソコン等の端末のスロット等から抜いておかなければならない。
（ウ）ＩＣカード等を紛失等した場合には、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告し、指示に従わなければならない。
②情報セキュリティに関する統一的な窓口を通じてＩＣカード等の紛失等の報告を受けた統括情報セキュリティ責任者及び情報システム管理者は、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統括情報セキュリティ責任者及び情報システム管理者は、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。

（２）ＩＤの取扱い
職員等は、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。

（３）パスワードの取扱い

職員等は､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にしなければならない。

④パスワードが流出した場合又は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及び情報セキュリティに関する統一的な窓口に速やかに報告しなければならない。

⑤情報セキュリティに関する統一的な窓口を通じてパスワード流出等の報告を受けた情報システム管理者は、パスワードを速やかに変更しなければならない。

⑥複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

⑦サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

⑧職員等間でパスワードを共有してはならない（ただし、共有ＩＤに対するパスワードは除く)。

６　技術的セキュリティ

6.1　コンピュータ及びネットワークの管理

（１）文書サーバの設定等

①情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

②情報システム管理者は、文書サーバを課等の単位で構成し、職員等が他課等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。

③情報システム管理者は、住民の個人情報、人事記録等、特定の職員等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、同一課等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（２）バックアップの実施

統括情報セキュリティ責任者及び情報システム管理者は、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関わらず、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。

（３）他団体との情報システムに関する情報の交換

情報システム管理者は、他の団体と情報システムに関する機密性２以上の情報を交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者の許可を得なければならない。

（４）システム管理記録及び作業の確認

①情報システム管理者は、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統括情報セキュリティ責任者及び情報システム管理者は、所管する情報システムにおいて、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なければならない。

③統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び契約により操作を認められた外部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。

（５）情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図及び情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者の閲覧、紛失等がないよう、適正に管理しなければならない。

（６）ログの取得等

①統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は､ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（７）障害記録

統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

（８）ネットワークの接続制御、経路制御等

①統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

（９）外部の者が利用できるシステムの分離等

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他の情報システムと物理的に分離する等の措置を講じなければならない。

(10) 外部ネットワークとの接続制限等

①情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、ＣＩＳＯ及び統括情報セキュリティ責任者の許可を得なければならない。

②情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワークその他の情報資産に影響が生じないことを確認しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

④情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(11) 複合機のセキュリティ管理

①統括情報セキュリティ責任者は､情報システムに接続される複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

②統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより、運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

(12) 特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は､情報システムに接続される特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(13) 無線ＬＡＮ及びネットワークの盗聴対策

①統括情報セキュリティ責任者は、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統括情報セキュリティ責任者は、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。

(14) 電子メールのセキュリティ管理

①統括情報セキュリティ責任者は、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統括情報セキュリティ責任者は、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、電子メールサーバの運用を停止しなければならない。

③統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④統括情報セキュリティ責任者は職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

(15) 電子メールの利用制限

①職員等は、自動転送機能を用いて、電子メールを転送してはならない。

②職員等は、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。

③職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

④職員等は、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。

⑤職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等を情報セキュリティ管理者の許可なく使用してはならない。

(16) 電子署名・暗号化

①職員等は、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。

②職員等は、暗号化を行う場合にＣＩＳＯが定める以外の方法を用いてはならない。また、ＣＩＳＯが定めた方法で暗号のための鍵を管理しなければならない。

③ＣＩＳＯは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

(17) 無許可ソフトウェアの導入等の禁止

①職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

②職員等は、業務上の必要がある場合は、情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③職員等は、不正にコピーしたソフトウェアを利用してはならない。

(18) 機器構成の変更の制限

①職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を原則行ってはならない。

②職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報システム管理者の許可を得なければならない。

(19) 無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

(20) 業務以外の目的でのウェブ閲覧の禁止

①職員等は、業務以外の目的でウェブを閲覧してはならない。

②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを認知した場合は、当該職員等が所属する課等の情報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。

6.2 アクセス制御

（1）アクセス制御等

①アクセス制御

統括情報セキュリティ責任者及び情報システム管理者は、所管する情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

②利用者ＩＤの取扱い

（ア）統括情報セキュリティ責任者及び情報システム管理者は､利用者の登録､変更、抹消等の情報管理、職員等の異動、出向、退職等に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

（イ）職員等は、業務上必要がなくなった場合は、利用者登録の抹消について、情報システム管理者に申請しなければならない。

（ウ）統括情報セキュリティ責任者及び情報システム管理者は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、点検しなければならない。

（エ）統括情報セキュリティ責任者及び情報システム管理者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

③特権を付与されたＩＤの管理等

（ア）統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

（イ）統括情報セキュリティ責任者及び情報システム管理者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が悪意ある第三者等によって窃取された際の被害を最小化するための措置及び内部からの不正操作や誤操作を防止するための措置を講じなければならない。

（ウ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードの変更について、外部委託事業者に行わせてはならない。

（エ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードについて、職員等の端末等のパスワードよりも、定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（オ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたＩＤを初期設定以外のものに変更しなければならない。

（２）職員等による外部からのアクセス等の制限

①職員等が外部から内部の情報システムにアクセスする場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

②統括情報セキュリティ責任者は、内部の情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内の情報システムに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

⑦統括情報セキュリティ責任者は、公衆無線ＬＡＮ等の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録したＩＣカード等による認証、通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（３）ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（４）認証情報の管理

①統括情報セキュリティ責任者及び情報システム管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、認証情報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。

（５）特権による接続時間の制限

情報システム管理者は、特権による情報システムへの接続時間を必要最小限に制限しなければならない。

6.3 情報システムの開発、導入、保守等

（１）情報システムの調達

①統括情報セキュリティ責任者及び情報システム管理者は、情報システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（２）情報システムの開発

①システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者及び作業者のＩＤの管理

（ア）情報システム管理者は、システム開発の責任者及び作業者が使用する開発用ＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

（イ）情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

（ア）情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定し、それ以外のものを利用させてはならない。

（イ）情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（３）情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

（ア）情報システム管理者は、システムの開発、変更及びテスト環境とシステム運用環境を分離しなければならない。

（イ）情報システム管理者は、システムの開発、変更及びテスト環境からシステム運用環境への移行について、システム開発・変更計画の策定時に手順を明確にしなければならない。

（ウ）情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（エ）情報システム管理者は、可用性２の情報を取り扱うシステム又はサービスを導入する場合、導入するシステム又はサービスの可用性が確保されていることを確認した上で導入しなければならない。

②テスト

（ア）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分なテストを行わなければならない。

（イ）情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

（ウ）情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（エ）情報システム管理者は､開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織において、それぞれ独立したテストを行わなければならない。

（４）情報システムの開発・変更に関連する資料等の整備・保管

①情報システム管理者は、システムの開発・変更に関連する資料その他のシステム関連文書を適正に整備・保管しなければならない。

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保

①情報システム管理者は、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情報システム管理者は、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。

③情報システム管理者は、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。

（６）情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（7）開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェアを更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（8）システムの更新又は統合時の検証等

情報システム管理者は、システムの更新・統合に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

6.4 不正プログラム対策

（1）統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

①外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

②外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

④所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定があるソフトウェアを利用してはならない。

（2）情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

①所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

②不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

③不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

④インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市が管理している媒体以外を職員等に許可なく利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

⑤不正プログラム対策ソフトウェアの設定変更権限については、一括管理し、情報システム管理者が許可した職員以外の職員等に当該権限を付与してはならない。

（３）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

②外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに情報セキュリティに関する統一的な窓口に報告し、指示を仰がなければならない。

④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをＬＧＷＡＮ接続系に取込む場合は無害化しなければならない。

⑥統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行うとともに、直ちに情報セキュリティに関する統一的な窓口に報告し、指示を仰がなければならない。

（ア）パソコン等の端末の場合

直ちに、無線ＬＡＮ接続を遮断するか、ＬＡＮケーブルの取り外しを行わなければならない。

（イ）モバイル端末の場合

直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

（４）専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

6.5　不正アクセス対策

（1）統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

①使用されていないポートを閉鎖しなければならない。

②不要なサービスについて、機能を削除又は停止しなければならない。

③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定しなければならない。

④情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2）攻撃への対処

ＣＩＳＯ及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、都道府県等と連絡を密にして情報の収集に努めなければならない。

（3）記録の保存

ＣＩＳＯ及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が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）違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（4）内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5）職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを認知した場合は、当該職員等が所属する課等の情報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。

（6）サービス不能攻撃

統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（７）標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

6.6　セキュリティ情報の収集等

（１）セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（２）不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者及び情報システム管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ、対応方法について職員等に周知しなければならない。

（３）情報セキュリティに関する情報の収集・共有

統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

７　運用

7.1　情報システムの監視

①統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、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。

③統括情報セキュリティ責任者及び情報システム管理者は、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。

7.2　情報セキュリティポリシーの遵守状況の確認等

（１）遵守状況の確認及び対処

①情報セキュリティ責任者及び情報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及び統括情報セキュリティ責任者に報告しなければならない。

②ＣＩＳＯ及び統括情報セキュリティ責任者は、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統括情報セキュリティ責任者及び情報システム管理者は、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。

（２）パソコン等の利用状況調査

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、職員等が使用しているパソコン、モバイル端末、電磁的記録媒体その他の情報機器のログ、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。

（３）職員等の報告義務

①職員等は、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、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

②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統括情報セキュリティ責任者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

7.3　セキュリティ侵害時の対応等

（１）緊急時対応計画の策定

ＣＩＳＯは、情報セキュリティインシデント、情報セキュリティポリシーの違反等により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発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

（２）緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

①関係者の連絡先

②発生した事案に係る報告すべき事項

③発生した事案への対応措置

④再発防止措置の策定

（３）業務継続計画との整合性確保

ＣＩＳＯは、地震、津波等に備えて策定された宮古市業務継続計画と情報セキュリティポリシーの整合性を確保しなければならない。

また、各種業務継続計画が策定される際は、情報セキュリティポリシーとの整合性をあらかじめ検討し、必要があれば情報セキュリティポリシーを改定しなければならない。

（４）緊急時対応計画の見直し

ＣＩＳＯは、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、緊急時対応計画の規定を見直さなければならない。

7.4　例外措置

（１）例外措置の許可

情報システム管理者は､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し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）緊急時の例外措置

情報システム管理者は、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）例外措置の申請書の管理

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。

7.5　法令遵守

職員等は、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
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）
⑦宮古市個人情報の保護に関する法律施行条例（令和４年宮古市条例第33号）

7.6　懲戒処分等

（１）懲戒処分

情報セキュリティポリシーに違反した職員等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）違反時の対応

職員等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統括情報セキュリティ責任者が違反を確認した場合は、当該職員等が所属する課等の情報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情報システム管理者が違反を確認した場合は、速やかに統括情報セキュリティ責任者に報告するとともに、当該職員等が所属する課等の情報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情報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、統括情報セキュリティ責任者は、当該職員等の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、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨をＣＩＳＯ及び当該職員等が所属する課等の情報セキュリティ管理者に通知しなければならない。

８　外部サービスの利用

8.1　外部委託

（１）外部委託事業者の選定基準

情報セキュリティ管理者は、機密性２以上、完全性２又は可用性２の情報を取り扱う外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（２）契約項目

機密性２以上、完全性２又は可用性２の情報を取り扱う業務を外部委託する場合には、外部委託事業者との間で、次の情報セキュリティ要件（業務内容に照らして必要のない要件を除く。）を明記した契約を締結しなければならない。

・情報セキュリティポリシー等の遵守
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め
・外部委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・外部委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守

・委託業務終了時の情報資産の廃棄、リース返却等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（３）確認・措置等

情報セキュリティ管理者は、機密性２以上、完全性２又は可用性２の情報を取り扱う外部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定期的に確認し、必要に応じ、委託契約に基づく措置を実施しなければならない。また、その内容を情報セキュリティ責任者に報告するとともに、その重要度に応じてＣＩＳＯ、統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

8.2 約款による外部サービスの利用

（１）約款による外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性２以上の情報が取り扱われないように規定しなければならない。

①約款によるサービスを利用して良い範囲
②業務に利用できる約款による外部サービスの基準
③利用手続及び運用手順

（２）約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

8.3 ソーシャルメディアサービスの利用

①統括情報セキュリティ責任者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

（ア）本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

（イ）パスワードや認証のためのコード等の認証情報及びこれを記録したＩＣカード等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

②職員等は、機密性２以上の情報をソーシャルメディアサービスで発信してはならない。

③ソーシャルメディアサービスを導入する場合は、導入するソーシャルメディアサービスごとの責任者を定めなければならない。
④統括情報セキュリティ責任者は、アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。
⑤職員等は、可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理ウェブサイトに当該情報を掲載して参照可能としなければならない。

8.4 クラウドサービスの利用

①情報システム管理者は、クラウドサービスを利用するに当たり、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。
②情報システム管理者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。
③情報システム管理者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、クラウドサービスを選定する際の要件としなければならない。
④情報システム管理者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、セキュリティ要件を定めなければならない。
⑤情報システム管理者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

９　評価・見直し

9.1 監査

（１）実施方法

ＣＩＳＯは、情報セキュリティ監査統括責任者を指名し、情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

（２）監査を行う者の要件

①情報セキュリティ監査統括責任者は、監査を実施する場合には、やむを得ない場合を除き、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。
②監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（３）監査実施計画の立案及び実施への協力

①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、宮古市デジタル戦略推進本部の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

（４）外部委託事業者に対する監査

情報システムの保守業務を外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は、外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（５）報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、宮古市デジタル戦略推進本部に報告しなければならない。

（６）保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

（７）監査結果への対応

ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

（８）情報セキュリティポリシー及び関係規程等の見直し等への活用

ＣＩＳＯは、監査結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

9.2　自己点検

（１）実施方法

①統括情報セキュリティ責任者及び情報システム管理者は、所管する情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

②情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部等における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

（２）報告

統括情報セキュリティ責任者､情報システム管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、宮古市デジタル戦略推進本部に報告しなければならない。

（３）自己点検結果の活用

①職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②ＣＩＳＯは、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

9.3　情報セキュリティポリシー及び関係規程等の見直し

ＣＩＳＯは、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。