相良村情報セキュリティポリシー

序　　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、相良村が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、相良村が所掌する情報資産に関する業務に携わる全職員、非常勤及び臨時職員（以下、「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分(対策基準)に分けて策定することとした。

具体的には、情報セキュリティポリシーを、①情報セキュリティ基本方針及び②情報セキュリティ対策基準の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする（下表参照）。

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全ての情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

第１章　情報セキュリティ基本方針

１　目的

相良村の各情報システムが取り扱う情報には、村民の個人情報のみならず行政運営上重要な情報など、部外に漏洩等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、村民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが相良村に対する村民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるＩＴ革命の発展により、電子商取引の発展や電子自治体の実現が期待されているところである。相良村がこれらに積極的に対応するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、相良村の情報資産の機密性、完全性及び可用性(注)を維持するための対策（情報セキュリティ対策）を整備するために相良村情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については相良村の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

(注)：国際標準化機構(IS0)が定めるもの（IS07498-2：1989）

機密性(confidentiality):情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性(integrity)：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性(availability)：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２　定義

（１）　ネットワーク

相良村における内部部局、各行政委員会及び各教育機関（事務室及び職員室のみ）を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

（２）　情報システム

業務系の電子計算機（業務系におけるネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

（３）　情報資産

ネットワーク及び情報システムの開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータをいう。

（４）　情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

３　情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、相良村が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

したがって、相良村長をはじめとして相良村が所掌する情報資産に関する業務に携わる全て

の職員等及び部外委託者は、情報セキュリティの重要性について共通の認識を持つとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

４　情報セキュリティ管理体制

相良村の情報資産について、幹部が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

５　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

６　情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（１）　部外者による故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難等

（２）　職員等及び部外委託者による意図しない操作、故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等

（３）地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

７　情報セキュリティ対策

上記６で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

（１）　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（２）　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が行われるように必要な対策を講ずる。

（３）　技術及び運用におけるセキュリティ対策

情報資産を部外からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

８　情報セキュリティ対策基準の策定

相良村の様々な情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

９　情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、内部部局の長等が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより相良村の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

10　情報セキュリティ監査の実施

情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施する。

11　評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。

第２章　相良村行政全般における情報セキュリティ対策基準

相良村行政全般における情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための相良村行政全般の情報資産に関する情報セキュリティ対策の基準である。

１　対象範囲

この情報セキュリティポリシーが対象とする行政機関の範囲は、村長事務部局、会計室、各委員会及び議会事務局とし、各教育機関（事務室及び職員室を除く）は対象外とする。
なお、各教育機関における教育のために用いるシステム等は、この情報セキュリティポリシーの対象となるシステムと物理的に分けなければならない。

２　組織・体制

相良村の情報セキュリティ管理については、以下の組織・体制とする。

(1)　最高情報統括責任者(CIO)
(2)　ネットワーク管理者
(3)　ネットワーク担当者
(4)　情報セキュリティ管理者
(5)　情報セキュリティ担当者
(6)　情報システム管理者
(7)　情報システム担当者
(8)　相良村情報推進化委員会

３　情報の分類と管理

（１）　情報の管理責任

ア　管理責任

情報は、当該情報を作成した各部局等が情報管理責任者として管理責任を有する。

イ　利用者の責任

情報を利用する者は、情報の分類に従い利用する責任を有する。

ウ　重要性の効力

情報が複製または伝送された場合には、当該複製等も分類に基づき管理しなければならない。

（２）　情報の分類と管理方法

ア　情報の分類

対象となる情報システムの情報は、各々の情報の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

重要性分類
Ⅰ　個人情報並びに相良村の幹部及び業務上必要とする最小限の者のみが扱う情報（極秘の情報を含む）
Ⅱ　公開することを予定していない情報（秘の情報を含む）
Ⅲ　外部に公開する情報のうち業務上重要な情報
Ⅳ　上記以外の情報

イ　情報の管理方法

（ア）　情報の分類の表示

・情報システムで扱う情報について、第三者が重要性の識別を容易に認識できないよう留意しつつ、ファイル名、記録媒体等に情報の分類が分かるように表示をする等適切な管理を行わなければならない。

（イ）　情報の管理及び取扱い

・情報について、それぞれの分類に従い、アクセス権限を定めなければならない。

・職員等は、情報の複製を保管場所へ移動する場合、当該保管場所からバックアップのために情報システムの設置個所に戻す場合及び業務上必要な場合には、最高情報統括責任者の許可を得たうえで外部への持出または送付をしなければならない。

・重要な情報（重要性分類Ⅰ）は暗号化を施して管理するものとし、暗号化に用いた暗号鍵及び暗号化された当該情報は別々に適切な管理を行わなければならない。

（ウ）　記録媒体の管理

・取り出しが可能な記録媒体は、適切な管理を行わなければならない。

・最終的に確定した情報を記録した記録媒体は、書込禁止措置を行った上で保管しなければならない。

・記録媒体に納められた情報は全て別の記録媒体に複製し、当該記録媒体は自然災害を被る可能性が低い地域に別途保管しなければならない。

・重要な情報（重要性分類Ⅱ以上）を記録した記憶媒体は、耐火、耐熱、耐水及び耐湿対策を講じた施錠可能な場所に保管しなければならない。

・記録媒体を送る場合は信頼できる者を選定し、複製の禁止及び記録媒体の物理的保護規定を定なければならない。

（エ）　記録媒体の処分

・記録媒体が不要となった場合は、当該媒体に含まれる重要な情報（重要性分類Ⅱ以上）は、記録媒体の初期化など情報を復元できないように消去を行ったうえで廃棄しなければならない。

・重用な情報（重要性分類Ⅱ以上）を記録した記録媒体の廃棄は、情報セキュリティ担当者の許可を得ることとし、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。

４　物理的セキュリティ

（１）　サーバ等

ア　装置の取り付け等

（ア）　情報システムの取り付けを行う場合は、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切な固定等必要な措置を施さなければならない。

（イ）　次のサーバは二重化し、ミラーリングにより常に同一データを保持し、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に移行させ、システムの運用が停止しないようにしなければならない。

・重要情報を格納しているサーバ

・セキュリティサーバ

・住民サービスに関するサーバ

・その他の基幹サーバ

（ウ）　ネットワーク管理者、情報システム管理者、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容易に操作できないように、利用者のID、パスワードの設定等の措置を施さなければならない。パスワードは可能な限り複雑なものにしなければならず、30日以上同一のパスワードを使用してはならない。また、パスワードの再利用は禁止する。

（エ）　サーバ等の取り付けに当たっては、ディスプレイ、配線等から放射される電磁波により重要な情報（重要性分類Ⅱ以上）が外部に漏洩することがないように措置しなければならない。

イ　電源

（ア）　サーバ等の機器の電源については、当該機器を適切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。

（イ）　落雷時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施さなければならない。

ウ　配線

（ア）　配線は、傍受または損傷等を受けることがないように可能な限り必要な措置を施さなければならない。

（イ）　主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。

（ウ）　ネットワーク接続口（ハブのポート等）は、他の者が容易に発見できない場所に設置しなければならない。

（エ）　ネットワーク管理者、情報システム管理者、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施さなければならない。

エ　外部に設置する装置

（ア）　外部に設置する装置は、最高情報統括責任者の承認を受けたものでなければならない。

　また、最高情報統括責任者は、定期的に当該装置の情報セキュリティの水準について確認しなければならない。

（イ）　相良村外に持ち出される端末、記録媒体等については、相良村外での使用方法を定め、管理簿を設ける等適切に管理しなければならない。

（２）管理区域

ア　管理区域

（ア）　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、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という）は、水害対策及び確実な入退室管理を行わなければならない。また、外部からの侵入を容易にできないように、窓等は開閉できない管理区域としなければならない。

（イ）　管理区域から外部に通ずるドアは１ケ所のみとし、制御機能、鍵、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。

（ウ）　情報システム室には、ビデオカメラ等の監視機能を設置しなければならない。

（エ）　情報システム室内の機器類は、耐震対策を講じた場所に設置するとともに、防火措置等を施さなければならない。なお、情報システム室内の機器類の配置は、緊急時に職員等が円滑に避難できるように配慮しなければならない。

（オ）　管理区域を囲む外壁等の床下開口部は全て塞がなければならない。

（カ）　消化剤は機器及び記録媒体に影響を与えるものであってはならない。

イ　情報システム室の入退室管理

情報システム室の入退室は許可された者のみとし、ＩＣカード等による入退室管理または入退室管理簿の記載を行い、職員等及び外部委託事業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。

ウ　機器等の搬入場所

（ア）　情報システム室へ機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について、職員による確認を行わなければならない。

（イ）　機器等の搬入には職員が同行する等の必要な措置を施さなければならない。

（3）　ネットワーク

（ア）　外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

（イ）　特に行政系のネットワークは総合行政ネットワークに集約するために努めなければならない。

（ウ）　ネットワークに使用する回線は光ファイバによる常時接続専用サービスのみとする。

（4）　職員等の端末等

（ア）　執務室等に職員等がいない場合は、執務室等の施錠等による盗難防止のための措置を施さなければならない。

（イ）　情報システムの執務室等の端末については、盗難防止のためのワイヤーによる固定等、盗難防止のための物理的措置を施さなければならない。また、ディスプレイ、配線等から放射される電磁波により重要な情報が外部に漏洩することがないよう措置しなければならない。

5　人的セキュリティ

（1）　役割・責任

ア　最高情報統括責任者（CIO：Chief Information Officer）

（ア）　相良村助役を、相良村における全てのネットワーク、情報システム及び情報資産を統括する最高情報統括責任者とする。

（イ）　最高情報統括責任者は、相良村における全ての情報資産の情報セキュリティを統括する。

イ　ネットワーク管理者

（ア）　総務課長を、最高情報統括責任者直属のネットワーク管理者とする。

ネットワーク管理者は、最高情報統括責任者を補佐しなければならない。

（イ）　ネットワーク管理者は、相良村全てのネットワークにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

（ウ）　ネットワーク管理者は、相良村全てのネットワーク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。

（エ）　ネットワーク管理者は、情報セキュリティ管理者、情報セキュリティ担当者、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。

（オ）　ネットワーク管理者は、相良村の情報資産に対する侵害または侵害の恐れのある場合には、最高情報統括責任者の指示に従い、最高情報統括責任者が不在の場合には自らの判断に基づき必要かつ十分な全ての措置を行う権限及び責任を有する。

この場合、全ての職員等はネットワーク管理者の指示に従わなければならな

い。

（カ）　ネットワーク管理者は、相良村の全てのネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持、管理を行い、緊急時対応計画の策定及び見直しを行う。

ウ　ネットワーク担当者

（ア）　ネットワーク管理者があらかじめ指定する者を、ネットワーク担当者とする。

（イ）　ネットワーク担当者は、ネットワーク管理者が行う全ての業務においてこれを補佐する。

エ　情報セキュリティ管理者

（ア）　各課、室、事務局の長を、その所管組織の情報セキュリティに関する総括的な権限及び責任を有する情報セキュリティ管理者とする。

（イ）　情報セキュリティ管理者は、情報セキュリティに関する統括的な権限及び責任を有する。

（ウ）　情報セキュリティ管理者は、所掌に属する情報システムの追加・変更の承認等を行う。

（エ）　情報セキュリティ管理者は、所掌に属する情報システムの連絡体制の構築並びに情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

オ　情報セキュリティ担当者

（ア）　各課、室、事務局の係長を、その担当係の情報セキュリティに関する権限及び責任を有する情報セキュリティ担当者とする。

（イ）　情報セキュリティ担当者は、情報セキュリティ管理者の下、担当係における情報セキュリティポリシーの遵守に関する権限と責任を有する。

（ウ）　情報セキュリティ担当者は、所掌に属する係における情報資産に対する侵害または侵害の恐れのある場合には、最高情報統括責任者及びネットワーク管理者へ速やかに報告を行い、指示を仰がなければならない。

　この場合、最高情報統括責任者及びネットワーク管理者に報告した後、速やかに情報セキュリティ管理者に報告しなければならない。

カ　情報システム管理者

（ア）　各課、室、事務局の長を、情報システムに関する情報システム管理者とする。

（イ）　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

（ウ）　情報システム管理者は、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。

（エ）　情報システム管理者は、所管する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。

キ　情報システム担当者

（ア）　各課、室、事務局の係長を、その担当する情報システムに関する権限及び責任を有する情報システム担当者とする。

（イ）　情報システム担当者は、担当する情報システムに関して、情報システム管理者の指示等に従い、開発、設定の変更、運用、更新等の作業を行う。

ク　相良村情報推進化委員会

　相良村の情報セキュリティ維持管理を統一的な視点で行うため、情報推進化委員会において、情報セキュリティポリシー、情報セキュリティ実施手順等の策定など情報セキュリティに関する重要な事項を審議する。

ケ　職員

（ア）　情報セキュリティ対策の遵守義務

・全ての職員は、情報セキュリティポリシー及び職員向け実施手順に定められている事項を遵守しなければならない。

・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については、速やかに情報セキュリティ担当者に相談し、指示等を仰がなければならない。

（イ）　その他

・全ての職員は、使用する端末や記録媒体について、第三者に使用されること、または許可なく情報を閲覧されることがないように、適切な措置を施さなければならない。

・全ての職員は、情報セキュリティ担当者の許可を得ず、端末等を執務室外に持ち出してはならない。

・全ての職員は、異動、退職等により業務を離れる場合には、知り得た情報を秘匿しなければならない。

コ　非常勤及び臨時職員

（ア）　情報セキュリティ対策の遵守業務

・全ての非常勤及び臨時職員は、情報セキュリティポリシー及び職員向け実施手順に定められている事項を遵守しなければならない。

・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については、速やかに情報セキュリティ担当者に相談し、指示等を仰がなければならない。

（イ）　非常勤及び臨時職員の雇用及び契約

・非常勤及び臨時職員には、雇用及び契約時に必ず情報セキュリティポリシーのうち、非常勤及び臨時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。

・非常勤及び臨時職員には、雇用及び契約の際、必要な場合は情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。

・非常勤及び臨時職員に端末による作業を行わせる場合においては、インターネットへの接続及び庁内ＬＡＮのメールの使用が不要の場合には、これを利用できないように設定しなければならない。

（ウ）　その他

・全ての非常勤及び臨時職員は、使用する端末や記録媒体について、第三者に使用されることまたは許可なく情報を閲覧されることがないように、適切な措置を施さなければならない。

・全ての非常勤及び臨時職員は、情報セキュリティ担当者の許可を得ず、端末等を執務室外に持ち出してはならない。

・全ての非常勤及び臨時職員は、異動、退職等により業務を離れる場合には、知り得た情報を秘匿しなければならない。

サ　外部委託に関する管理

（ア）　ネットワーク及び情報システムの開発・保守を外部委託事業者に発注する場合は、外部委託事業者から下請けとして受注する業者も含めて、情報セキュリティポリシーのうち外部委託事業者が守るべき内容の遵守及びその守秘義務を明記した契約を行わなければならない。

（イ）　外部委託事業者との契約書には、損害賠償等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を定めなければならない。

（２）　教育・訓練

ア　最高情報統括責任者は、説明会の実施等により幹部を含めて全ての職員等及び関係する者に対し情報セキュリティポリシーについて啓発しなければならない。また、新規採用の職員等を対象とする情報セキュリティポリシーに関する研修を設けなければならない。

　情報セキュリティポリシーに関する教育・訓練プログラムは、情報推進化委員会で承認されたものを使用する。

イ　ネットワーク管理者は、最新の技術力を維持するための研修を常に受けなければならない。

　ネットワーク管理者は、緊急時対応を想定した訓練を職員等に計画的に行わせなければならない。訓練の計画に当たっては、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を適宜定めることとする。また、より効果的に実施できるよう計画を立てることとする。

ウ　情報システム管理者は、情報システム管理者向けの研修を受けなければならない。

エ　職員等は、定められた研修に参加し情報セキュリティポリシー及び実施手順を理解し、情報セキュリティ上の問題が生じないようにしなければならない。

（３）　事故、欠陥に対する報告

ア　職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合には、速やかにネットワーク管理者に報告し、ネットワーク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。

イ　別途、職員等は、情報セキュリティ担当者に報告し、情報セキュリティ担当者は、報告のあった事故等について全て最高情報統括責任者及び情報セキュリティ管理者に報告しなければならない。

ウ　ネットワーク管理者は、これらの事故等を分析し、再発防止のための情報として記録を保存しなければならない。

（４）　パスワードの管理

職員等は、自己の保有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。

ア　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ないこと。

イ　パスワードのメモを作らないこと。

ウ　パスワードの長さは十分な長さとし、文字列は想像しにくいものとすること。

エ　情報システムまたはパスワードに対する危険の恐れがある場合には、パスワードを速やかに変更すること。

オ　パスワードは定期的に、若しくはアクセス回数に基づいて変更し、古いパスワードの再利用はしないこと。

カ　複数の情報システムを扱う職員等は、パスワードをシステム間で共有しないこと。

キ　仮のパスワードは、最初のログイン時点で変更すること。

ク　端末にパスワードを記憶させないこと。必要に応じて暗号化等を行うことによって他者がパスワードを読めないようにすること。

ケ職員等間でパスワードを共有しないこと。

（５）　ＩＣカード等の管理

ア　ＩＣカード等の認証に用いるカード類は、職員等間で共有してはならない。

イ　ＩＣカード等は、カードリーダ若しくは端末のスロット等に常時挿入してはならない。

ウ　職員等はＩＣカード等を紛失した場合には、速やかにネットワーク管理者及び情報システム管理者に通報し、指示を仰がなければならない。

エ　ネットワーク管理者及び情報システム管理者は通報があり次第速やかに当該ＩＣ

カード等を使用したアクセス等を停止しなければならない。

6　技術的セキュリティ

（1）　コンピュータ及びネットワークの管理

ア　アクセス記録の取得等

重要な情報を扱う情報システムについて、次の措置を講じる。

（ア）　ネットワーク管理者及び情報システム管理者は、各種アクセス記録及び情報セキュリティの確保に必要な記録を全て取得し、一定の期間保存しなければならない。

（イ）　ネットワーク管理者及び情報システム管理者は、アクセス記録等が窃取、改ざん、消去されないように必要な措置を施さなければならない。

（ウ）　ネットワーク管理者及び情報システム管理者は、定期的にアクセス記録等を分析、監視しなければならない。

イ　システム管理記録及び作業の確認

（ア）　ネットワーク管理者及び情報システム管理者は、担当するシステムにおいて行ったシステム変更等の処理について、記録を作成しなければならない。

（イ）　ネットワーク管理者及び情報システム管理者が担当するシステムにおいて行った作業は記録し、適切に管理を行わなければならない。

（ウ）　ネットワーク管理者、情報システム管理者また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担当するシステムにおいて作業を行う場合には、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。

ウ　障害記録

ネットワーク管理者及び情報システム管理者は、職員等から報告のあった情報、システムの障害に対する処理または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しなければならない。

エ　情報システム仕様書等の管理

ネットワーク管理者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書については、記録媒体に関わらず業務上必要とする者のみが閲覧できる場所に保管しなければならない。また、構築に際して事業者に外部委託した場合、当該事業者に守秘義務を課さなければならない。

オ　情報及びソフトウェアの交換

組織間において、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は、その取扱いに関する事項をあらかじめ定め、ネットワーク管理者及び情報セキュリティ管理者の許可を得なければならない。

カ　バックアップ

ネットワーク管理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二重化措置に関わらずその重要度に応じて期間を設定し、定期的にバックアップ用の複製をとらなければならない。

キ　メール

（ア）　ネットワーク管理者は、外部から外部へのメール転送（メールの中継処理）を不可能とする等、情報システム全般に悪影響を与えないような設定を施さなければならない。

（イ）　職員等は、メールの自動転送機能を用いて、職場のメールを転送してはならない。

（ウ）　職員等は、メールで重要な情報（重要性分類Ⅱ以上）を送ってはならない。

（エ）　メールの容量は 10MB を上限とし、10MB を越えるメールの送受信を不可能としなければならない。

（オ）　職員等が使用できるメールボックスの容量は 100MB を上限とし、100MB を越えた場合には職員等が自らメールを削除し、メールの総量が 100MB 未満になるまで一時的にメールの使用を停止するような設定を施さなければならない。

ク　文書サーバ

（ア）　職員等が使用できる文書サーバの容量は職員等１人あたり平均 300MB 以上とする。

（イ）　文書サーバは課室等単位で構成し、他課室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な設定を施さなければならない。

（ウ）　同一課室等であっても、住民の個人データ、人事記録等特定の職員等しか取扱えないデータについては、別途ディレクトリを作成し、担当職員等以外の職員等が閲覧及び使用できないような設定を施さなければならない。

ケ　外部の者が利用できるシステム

外部の者が利用できる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ける等、情報セキュリティ対策について特に強固な対策をとらなければならない。

コ　情報システムの入出力データ

（ア）　情報システムに入力されるデータは、適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

（イ）　エラーまたは故意の行為により情報が改ざんされる恐れがある場合、これを検出する手段を講じなければならない。

また、改ざんの有無を検出し、必要な場合は情報の修復を行う手段を講じなければならない。

（ウ）　情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されることを確保しなければならない。

サ　電子署名・暗号化

（ア）　外部に送るデータが完全であることを担保する事が必要な場合には、定められた電子署名方法及び暗号化方法を使用して送信しなければならない。

（イ）　暗号化については、定められた方法以外の方法を用いてはならない。また、暗号のための鍵の管理方法について、定められた方法で管理しなければならない。

シ　業務目的以外の使用の禁止

（ア）　職員等は、業務目的以外で情報システムへのアクセス及びメールの使用を行ってはならない。

また、職員等は業務目的以外でのウェブページを閲覧してはならない。職員等が業務目的以外でウェブページを閲覧した場合、ネットワーク管理者は当該職員等が所属する課室等の情報セキュリティ担当者に通知し、適切な措置を求めなければならない。

改善されない場合、ネットワーク管理者は、当該職員等のウェブページ閲覧に関する権利を停止あるいは剥奪することができる。

（イ）　ネットワーク管理者は、職員等のウェブページ閲覧に関する権利を停止あるいは剥奪した場合、最高情報統括責任者及び当該職員等が所属する課室等の情報セキュリティ担当者にその旨通知しなければならない。

ス　無許可ソフトウェア導入等の禁止

（ア）　職員等が業務上の必要から次の行為をなす場合には、個別にネットワーク管理者及び該当システム管理者の許可を必要とする。

・標準実装以外のアプリケーションソフトの端末へのインストール
・端末のデスクトップ設定の変更

（イ）　ソフトウェアのインストール及びデスクトップ環境の変更は、サーバにより監視しなければならない。

セ　機器構成の変更

（ア）　職員等は、端末に対し改造及び機器の増設・交換を行ってはならない。

（イ）　職員等は、端末に対し業務を遂行するために機器の増設・交換を行う必要がある場合は、ネットワーク管理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。

（ウ）　職員等は、モデム等の機器を増設して他の環境へのネットワーク接続を行うことや、外部からのアクセスを可能とする仕組みを構築する場合は、ネットワーク管理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。

ソ　電子取引

電子商取引に関しては、原則として禁止する。

タ　その他

職員等が利用できるプロトコルは、業務上必要最低限のものとする。

（２）　アクセス制御

ア　利用者登録

ネットワーク管理者及び情報システム管理者は、利用者の登録、変更、抹消、登録情報の管理、異動や相良村外への出向等の職員等及び退職者における利用者のＩＤ取扱い等については、定められた方法に従って行わなければならない。

必要な利用者登録・変更は、ネットワーク管理者または情報システム管理者に対する申請により行う。

イ　管理者権限

（ア）　ネットワークの管理者権限は、１人の者に与え厳重に管理しなければならない。

ネットワーク管理者の権限を代行する者は、ネットワーク管理者が指名し、最高情報統括責任者が認めた者でなければならない。代行者を認めた場合、最高情報統括責任者は速やかに情報セキュリティ管理者、情報セキュリティ担当者及び情報システム管理者に周知しなければならない。

（イ）　情報システムの管理者権限は、必要最小限の者に与え、厳重に管理しなければならない。

情報システム管理者の権限を代行する者は、情報システム管理者が指名し、最高情報統括責任者が認めた者でなければならない。代行者を認めた場合、最高情報統括責任者は速やかにネットワーク管理者、情報セキュリティ管理者及び情報セキュリティ担当者に周知しなければならない。

ウ　インターネット以外のネットワークにおけるアクセス制御

アクセス可能なネットワーク及びネットワークサービス等についてネットワークごとにアクセスできる者を定めなければならない。

ネットワーク管理者及び情報システム責任者は、ネットワークサービスを使用する権限を有しない職員等が当該サービスを使用できるようにしてはならない。

エ　強制的な経路制御

ネットワーク管理者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

オ　外部からのアクセス

（ア）　外部からのアクセスの許可は、必要最低限にしなければならない。

外部から相良村全てのネットワーク及び情報システムにアクセスする場合は、外部アクセスサーバに対してのみ接続を許可することとし、直接内部のネットワークに接続してはならない。

アクセス方法及び使用方法等は、利用者の真正性の確保が確認できるものでなければならない。

（イ）　相良村における全てのネットワーク及び情報システムへのモバイル端末等による外部からのアクセスは、当分の間禁止する。

カ　総合行政ネットワークとの接続

ネットワーク管理者は、「総合行政ネットワーク接続仕様書(平成１３年5月１１日)」に基づき適切な管理をしなければならない。

キ　外部ネットワークとの接続

（ア）　外部ネットワークとの接続に際しては、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を詳細に検討し、相良村の全てのネットワーク、情報システム及び情報資産に影響が生じないと明確に確認したうえで、最高情報統括責任者及びネットワーク管理者の許可に基づき接続しなければならない。

その利用はネットワーク管理者の適切な管理下で行い、情報セキュリティに留意したネットワーク構成を採らなければならない。

この場合、当該外部ネットワークの瑕疵により相良村のデータの漏洩、破壊、改ざんまたはシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

（イ）　接続した外部ネットワークワークのセキュリティに問題が認められ、相良村の情報資産に脅威が生じることが想定される場合には、ネットワーク管理者の判断に伴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。

ク　自動識別

相良村で使用されるネットワーク機器については、機器固有情報によってアクセスの可否を自動的に判断しなければならない。

ケ　ログイン手順

ログイン手順中におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻の表示等、正当なアクセス権をもつ職員等がログインしたことを確認することができる手順を定めなければならない。

コ　パスワードの管理方法

（ア）　ネットワーク管理者または情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。職員等のパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

（イ）　ネットワーク管理者または情報システム管理者は、パスワードの変更を行わない職員等にパスワード変更する旨勧告し、当該職員等が勧告に従わない場合には速やかに当該職員等のアクセス権を一定期間経過後に停止しなければならない。

（ウ）　ネットワーク管理者または情報システム管理者は、当該職員等からパスワード変更の申告があり次第当該職員等のアクセス権の停止を解除するものとする。

（エ）　ネットワーク管理者及び情報システム管理者は、職員等のパスワードについて定期的にその妥当性について調査を行わなければならない。

（オ）　ネットワーク管理者及び情報システム管理者は第三者に読まれることのないよ

う、暗号化等パスワードを扱う方法を定めなければならない。

サ　接続時間の制限

管理者権限によるネットワーク及び情報システムへの接続については、必要最小限の接続時間に制限しなければならない。

（３）　システム開発、導入、保守等

ア　情報システムの調達

（ア）　最高情報統括責任者は応用ソフトウェアの開発、変更及び運用についての手順及び基準を明らかにしなければならない。

（イ）　最高情報統括責任者は機器及び基本ソフトウェアの導入、保守及び撤去についての手順及び基本を明らかにしなければならない。

（ウ）　ネットワーク管理者及び情報システム管理者は、情報システムの調達にあたっては、一般に公開する調達仕様書が情報セキュリティ確保の上で問題のないようにしなければならない。

（エ）　ネットワーク管理者及び情報システム管理者は、機器及びソフトウェアを購入等する場合は、当該製品が情報セキュリティ上問題にならないかどうか、確認しなければならない。

イ　情報システムの変更管理

情報システム管理者は、システムを追加、変更、廃棄等した場合は、その際の設定、構成等の履歴を記録し、保存しなければならない。

ウ　情報システムの開発

（ア）　最高情報統括責任者はシステム開発及び保守時の事故・不正行為対策のため、次の事項を定めなければならない。

・責任者及び監督者
・作業者及び作業範囲
・システム開発及び保守等の事故・不正行為に係るリスク分析
・開発・保守するシステムと運用システムとの分離
・開発・保守に関するソースコードの提出
・開発・保守の際のセキュリティ上問題となりうる恐れのあるＯＳ、ミドルウェア及びアプリケーションソフトの使用禁止
・開発・保守の際のアクセス制限
・機器の搬出入の際の、情報システム管理者の許可及び確認
・開発・保守記録の提出義務
・マニュアル等の定められた場所への保管
・開発・保守を行った者の利用者ＩＤ、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消

（イ）　情報システム管理者はシステム開発及び保守時の事故・不正行為対策のため、次の事項を実施しなければならない。

・責任者及び監督者
・作業者及び作業範囲
・システム開発及び保守等の事故・不正行為に係るリスク分析
・開発・保守するシステムと運用システムとの分離
・開発・保守に関するソースコードの提出
・開発・保守の際のセキュリティ上問題となりうる恐れのあるＯＳ、ミドルウェア及びアプリケーションソフトの使用禁止
・開発・保守の際のアクセス制限

・機器の搬出入の際の、情報システム管理者の許可及び確認
・開発・保守記録の提出義務
・マニュアル等の定められた場所への保管
・開発・保守を行った者の利用者ＩＤ、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消

エ　システムの導入

（ア）　情報システム管理者は、新たにシステムを導入する際には、既に稼動しているシステムに接続する前に十分な試験を行わなければならない。

（イ）　情報システム管理者は、試験に使用したデータ及びその結果を最高情報統括責任者及びネットワーク管理者へ提出するとともに厳重に保管しなければならない。

オ　ソフトウェアの保守及び更新

ソフトウェア（独自開発ソフトウェア及び汎用ソフトウェア）等を更新、または修正プログラムを導入する場合は、不具合及び他のシステムとの相性の確認を行い、計画的に更新しまたは導入しなければならない。

情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて、速やかな対応を行うこととし、その他のソフトウェアの更新等については、計画的に実施しなければならない。

カ　システム受託業者への規定

（ア）　新たなシステムの開発を外部の事業者に委託する場合は、ソースコードの提出を求め、再委託契約を行う際には再委託先について契約課において経営状況等、契約履行が可能であるか確認をとり、導入前の検査要求事項等を契約に定めなければならない。

（イ）　信頼のおける業者に委託するために、必要な資格等を定めなければならない。

（ウ）　情報システム管理者は、作業中に身分証明書の提示を業者に求め、契約で定められた資格を有するものが作業に従事しているか確認を行わなければならない。また、守秘のための契約を事業者と結ばなければならない。

キ　機器の修理及び廃棄

（ア）　記憶媒体の含まれる機器について、外部の業者に修理させまたは廃棄する場合は、その内容が消去された状態で行わなければならない。

（イ）　故障を外部の業者に修理させる際、情報を消去することが難しい場合は、修理を委託する業者に対し秘密を守ることを契約に定めなければならない。また、重要な機器については、復元不可能な廃棄を行わなければならない。

（４）　コンピュータウィルス対策

ア　外部のネットワークから受信したファイルは、ＦＷレベルでウィルスチェックを行いシステムへの侵入を防止しなければならない。

イ　外部へのネットワークへ送信するファイルは、ＦＷレベルでウィルスチェックを行い外部へのウィルス拡散を防止しなければならない。

ウ　ネットワーク管理者は、次の事項を実施しなければならない。

（ア）　ウィルス情報について職員等に対する注意喚起を行うこと。

（イ）　常時ウィルスに関する情報収集に努めること。

（ウ）　サーバ及び端末において、ウィルスチェックを行うこと。

（エ）　ウィルスチェック用のパターンファイルは常に最新のものに保つこと。

エ　情報システム管理者は、次の事項を実施しなければならない。

（ア）　サーバ及び端末において、ウィルスチェックを行うこと。

（イ）　ウィルスチェック用のパターンファイルは常に最新のものに保つこと。

オ　職員等は、次の事項を遵守しなければならない。

（ア）　外部からデータまたはソフトウェアを取り入れる場合には、必ずウィルスチェックを行うこと

（イ）　差出人が不明または不自然に添付されたファイルは速やかに削除すること。

（ウ）　ウィルスチェックの実行を途中で止めないこと。

（エ）　ネットワーク管理者が提供するウィルス情報を常に確認すること。

（オ）　添付ファイルのあるメールを送受信する場合は、ウィルスチェックを行うこと。

（５）　不正アクセス対策

ア　ネットワーク管理者は、次の事項を実施しなければならない。

（ア）　使用終了若しくは使用される予定のないポートを長時間空けた状態のままにしてはならない。

（イ）　セキュリティホールの発見に努め、メーカー等からパッチの提供があり次第、速やかにパッチをあてなければならない。その際、システム停止等が発生する場合は業務時間外に作業を行うものとする。

（ウ）　不正アクセスによるウェブページ書換防止を確実にするために、担当職員等によるものであるか否かに関わりなくデータの書換を検出し、ネットワーク管理者及び情報システム管理者へ通報する設定を施さなければならない。

（エ）　重要なシステムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。

イ　攻撃を受けることが明確な場合には、ネットワーク管理者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、各機関との連絡を密にして情報の収集に努めなければならない。

ウ　攻撃を受け、当該攻撃が不正アクセス禁止法違反等犯罪の可能性がある場合には記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなければならない。

エ　攻撃の可能性が明確であるにもかかわらず職員等の怠惰が原因でデータの漏洩、破壊、改ざんまたはシステムダウン等により行政業務に深刻な影響をもたらした場合、当該職員は懲戒の対象とする。

オ　職員等による不正アクセスがあった場合、ネットワーク管理者または情報システム管理者は当該職員等が所属する課室等のセキュリティ担当者に通知し、適切な処置を求めなければならない。

（６）　セキュリティ情報の収集

ア　ネットワーク管理者は、情報セキュリティに関する情報を収集し、相良村の全てのネットワーク及び情報システムについてソフトウェアにパッチを当てる等、セキュリティ対策上必要な措置を講じなければならない。

イ　最高情報統括責任者は、これらの情報を定期的に取りまとめ、関係部局等に通知するとともに、情報セキュリティポリシーの改定につながる情報については情報推進化委員会に報告しなければならない。

ウ　ネットワーク管理者は、緊急時対応計画に定める緊急に連絡すべき情報を入手した場合は当該計画に定める情報連絡先に連絡しなければならない。

７　運用

（１）　情報システムの監視

ア　セキュリティに関する事案を検知するため、ネットワーク管理者及び情報システム管理者は、常に情報システムの監視を行わなければならない。

イ　外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し２４時間監視を行わなければならない。

ウ　内部のシステムについて、アクセスコントロール等を行い、異常な運用等の監視を行わなければならない。

エ　監視により得られた結果については、消去や改ざんされないために必要な措置を施し、定期的に安全な場所に保管しなければならない。また、これらの記録の正確性を確保するため、正確な時刻の設定を行わなければならない。

（２）　情報セキュリティポリシーの遵守状況の確認

ア　情報セキュリティ管理者及び情報セキュリティ担当者は、情報セキュリティポリシーが遵守されているかどうかについて、また、問題が発生していないかについて常に確認を行い問題が発生していた場合には速やかに最高情報統括責任者及びネットワーク管理者に報告しなければならない。

イ　最高情報統括責任者は速やかに発生した問題に適切に対処しなければならない。

ウ　職員等は、情報セキュリティポリシーの違反が発生した場合は、直ちにネットワーク管理者及び情報セキュリティ担当者に報告を行わなければならない。違反の発生時には、それ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ネットワーク管理者が判断した場合は、緊急時対応計画に従って連絡を行わなければならない。

エ　ネットワーク管理者及び情報システム管理者は、サーバ等のシステム設定が情報セキュリティポリシーを遵守しているかどうかについて、また問題が発生していないか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速やかに適切に対処しなければならない。

（３）　運用管理における留意点

ア　最高情報統括責任者は、アクセス記録、メール等個人のプライバシーに係る情報を閲覧できる権限を有する職員等を情報セキュリティ実施手順に定めなければならない。ただし、法令で定められた個人情報の保護に関係する情報の閲覧に関しては、当該法令に定められた手順に従う。

イ　情報セキュリティ担当者は、職員等が常に情報セキュリティポリシー及び実施手順を参照できるよう配慮しなければならない。

（４）　侵害時の対応

情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を次のとおり定める。

ア　連絡先

具体的には、各情報システムごとに情報セキュリティ実施手順に明記する。

（ア）　相良村長
（イ）　最高情報統括責任者
（ウ）　ネットワーク管理者
（エ）　情報システム管理者
（オ）　情報システムに係る外部委託事業者
（カ）　熊本県
（キ）　警察
（ク）　関係機関
（ケ）　影響が考えられる個人及び法人

イ　事案の調査

セキュリティに関する事案を認めた者は、次の項目について、すみやかにネットワーク管理者に報告しなければならない。

（ア）　事案の内容

（イ）　事案が発生した原因として、想定される行為

（ウ）　確認した被害・影響範囲

ネットワーク管理者は、事案の詳細な調査を行うとともに、最高情報統括責任者との情報共有及び情報推進化委員会への報告を行わなければならない。

ウ　事案への対処

ネットワーク管理者は、事案に対処するために次の項目を実施しなければならない。

（ア）　ネットワーク管理者は、次の事案が発生した場合、それぞれ定められた連絡先へ連絡しなければならない。

・サイバーテロその他の村民に重大な被害が生じる恐れがあるとき（相良村長、最高情報統括責任者、警察、影響が考えられる個人及び法人）

・不正アクセスその他犯罪と思慮されるとき（相良村長、最高情報統括責任者、警察）

・踏み台となって他者に被害を与える恐れがあるとき（相良村長、最高情報統括責任者、警察）

・情報システムに関する被害（情報システム管理者、必要と認められる業者等）

・その他情報資産に係る被害（関係部局等）

（イ）　ネットワーク管理者は、次の事案が発生し情報資産の防護のためにネットワークの切断がやむを得ない場合は、ネットワークを切断する措置を講ずる。

・異常なアクセスが継続しているとき、または不正アクセスが判明したとき

・システムの運用に著しい支障をきたす攻撃が継続しているとき

・コンピュータウィルス等不正プログラムがネットワーク経由で拡がっているとき

・情報資産に係る重大な被害が想定されるとき

（ウ）　情報システム管理者は、次の事案が発生し情報資産の防護のために情報システムの停止がやむを得ない場合は、情報システムを停止する。

・コンピュータウィルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき

・災害等により電源を供給することが危険または困難なとき

・その他の情報資産に係る重大な被害が想定されるとき

（エ）　個々の端末のネットワークからの切断については、ネットワーク管理者の許可が必要である。ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合には、事後報告とすることができる。

（オ）　事案に係るシステムのアクセス記録及び現状を保存する。

（カ）　事案に対処した経過を記録する。

（キ）　事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討する。

（ク）　再発防止の暫定措置を講じた後、復旧する。

エ　再発防止の措置

（ア）　ネットワーク管理者は、当該事案に係るリスク分析を実施し、情報セキュリティポリシー及び実施手順の改善に係る再発防止計画を策定し、情報推進化委員会へ報告しなければならない。

情報推進化委員会は、情報セキュリティポリシー及び実施手順の改善に係る再発防止計画が有効であると認められる場合は、これを承認する。

（イ）　ネットワーク管理者は、各種セキュリティ対策の改善に係る再発防止計画を策定

し、最高情報統括責任者へ報告しなければならない。最高情報統括責任者は、これらの再発防止計画が有効であると認められる場合は、これを承認する。

オ　外部委託による運用契約

（ア）　運用を外部委託する場合は、委託に関する責任を有する部署を明確にするとともに、委託事業者に対し必要なセキュリティ要件を記載した契約書による契約を締結しなければならない。

（イ）　委託に関する責任を有する部署は、委託先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、その内容をネットワーク管理者に報告するとともに、その重要度に応じて最高情報統括責任者に報告しなければならない。

8　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について、次の法令等を遵守し、これに従わなければならない。

（1）　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）

（2）　著作権法（昭和 45 年法律第 48 号）

（3）　行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）

（4）　相良村個人情報保護条例（平成 17 年条例第6号）

9　情報セキュリティに関する違反に対する対応

情報セキュリティポリシーに違反した者については、その重大性、発生した事案の状況等に応じて対応する。

10　評価・見直し

（1）　監査

（ア）　ネットワーク管理者及び情報システム管理者は、ネットワーク及び情報システムの情報セキュリティについて監査を定期的に行わなければならない。

監査を行う者は、十分な専門的知識を有する者でなければならない。

（イ）　外部委託事業者に委託している場合、ネットワーク管理者及び情報システム管理者は外部委託事業者から下請けとして受託している業者も含めて、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行わなければならない。

（ウ）　最高情報統括責任者は監査結果をとりまとめ、情報推進化委員会に報告する。情報推進化委員会は、この報告結果を情報セキュリティポリシーの更新の際に参照する情報として活用しなければならない。

（2）　点検

情報セキュリティ管理者は、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が実施されているかどうかについて職員等にアンケート等を行い、また自己点検を行わなければならない。情報セキュリティ管理者はこれをとりまとめ、情報推進化委員会に報告する。情報推進化委員会は、この報告結果を情報セキュリティポリシーの更新の際に参照する情報として活用することとする。

（3）　情報セキュリティポリシーの更新

新たに必要な対策が発生した場合または監査の結果及び点検の結果を踏まえ、情報推進化委員会において情報セキュリティポリシーの実効性を評価し、必要な部分を見直し、内容、時期について決定を行う。この決定に基づき、情報セキュリティポリシーの更新を実施する。更新の内容については、情報推進化委員会が決定しなければならない。