笠岡市情報セキュリティポリシー

笠岡市情報セキュリティ対策基準

笠岡市

平成29年３月制定
平成31年３月改定
令和元年６月改定
令和５年４月改定
令和６年３月改定
令和７年２月改定

第１章　目的

笠岡市情報セキュリティ対策基準は，笠岡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遵守事項及び判断基準を定めたものである。

第２章　適用範囲

本市が保有する情報資産，情報資産に関する事務に携わる全ての職員，会計年度任用職員，労働者派遣事業により本市の事務に携わる者（以下「職員等」という。)及び委託事業者とする。

第３章　組織体制における役職及びその責任並びに権限

１　最高情報セキュリティ責任者

(1) 副市長を最高情報セキュリティ責任者とする。

(2) 最高情報セキュリティ責任者は，本市における全てのネットワーク，情報システム，データ等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。

(3) 最高情報セキュリティ責任者は，必要に応じ，情報セキュリティに関する専門的な知識及び経験を有する専門家をアドバイザーとして置くものとする。

(4) 最高情報セキュリティ責任者は，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) デジタル政策監を統括情報セキュリティ責任者とする。

(2) 総括情報セキュリティ責任者は，最高情報セキュリティ責任者を補佐する。

(3) 総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) 統括情報セキュリティ責任者は，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統括的な権限及び責任を有する。

(5) 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。

(6) 統括情報セキュリティ責任者は，情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に，最高情報セキュリティ責任者の指示に従い，最高情報セキュリティ責任者が不在の場合には自らの判断に基づき，必要かつ十分な措置を実施する権限及び責任を有する。

(7) 総括情報セキュリティ責任者は，本市の共通的なネットワーク，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・管理を行う権限及び責任を有する。

(8) 統括情報セキュリティ責任者は，緊急時等の円滑な情報提供を図るため，最高情報セキュリティ責任者，総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。

(9) 総括情報セキュリティ責任者は，緊急時には最高情報セキュリティ責任者に早急

に報告を行うとともに，回復のための対策を講じなければならない。

(10)統括情報セキュリティ責任者は，情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し，必要に応じて最高情報責任者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) 各部長，議会事務局長，消防長，市民病院管理局長，会計管理者，監査委員事務局長及び選挙管理委員会事務局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，当該部局等の情報セキュリティ対策に関する総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，所管す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，所管す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に関する意見の集約並びに職員，会計年度任用職員に対する教育，訓練，助言及び指示を行う。

4　情報セキュリティ管理者

(1) 情報資産を取り扱う課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，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)現場や部門において情報セキュリティー対策が必要な情報資産（データ等）を洗い出した上で，それぞれに対する対応策を整理確認する。

(4) 情報セキュリティ管理者は，その所掌する課室等において，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，統括情報セキュリティ責任者及び最高情報セキュリティ責任者へ速やかに報告を行い，指示を仰がなければならない。

5　情報システム管理者

(1) 各情報システムを所管する担当課長等を当該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，所管する情報システムにおける開発，設定の変更，運用，見直し等を行う権限及び責任を有する。

(3) 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。

(4) 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

情報システム担当者は，情報システム管理者の指示等に従い，情報システムにおける開発，設定の変更，運用の見直し等の作業を行う者とする。

７　情報取扱者

情報資産を取扱うすべての者を情報取扱者とし，情報取扱者は情報システム管理者の指示に従う。

８　情報資産管理責任者

情報セキュリティ管理者及び情報システム管理者をいう。

９　情報セキュリティ委員会

(1) 本市の情報セキュリティ対策を統一的に実施するため，情報セキュリティ委員会において，情報セキュリティポリシー等，情報セキュリティに関する重要な事項を決定する。

(2) 情報セキュリティ委員会は，必要に応じて本市における情報セキュリティ対策の改善計画を策定し，その実施状況を確認しなければならない。

１０　兼務の禁止

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

１１　CSIRT の設置・役割

(1) 最高情報セキュリティ責任者は，CSIRT を整備し，その役割を明確化しなければならない。

(2) 最高情報セキュリティ責任者は，CSIRT に所属する職員を選任し，その中からCSIRT 責任者を置かなければならない。また，CSIRT 内の業務統括との連携等を行う職員等を定めなければならない。

(3) 最高情報セキュリティ責任者は，情報セキュリティの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署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。

(4) 最高情報セキュリティ責任者による情報セキュリティ戦略の意思決定が行われた際には，その内容を関係部署等に提供しなければならない。

(5) 個人情報の漏洩など総務省や県等へ報告義務がある情報セキュリティインシデントを認知した場合には，速やかに報告しなければならない。

(6) 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，報道機関へ周知・公表を行わなければならない。

(7) 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機能を有する部署，委託事業者等との情報共有を行わなければならない。

第４章　情報資産の分類と管理

１　情報資産の分類

(1) 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，次の重要性分類に従って分類し，必要に応じて取扱制限を行うものとする。

機密性

分類	分類基準	主な取扱制限等
３Ａ	行政事務で取り扱う情報資産のうち，「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	機密性３Ａ～３Ｃ ・情報資産管理責任者の許可を得た場合，複製・送付・送信を行うことができる。また，権限のある者だけがアクセスできる環境で，保存・利用をしなければならない。 複数の権限ある者でデータを共有したり，所属外にデータを送付・送信したりするときは，パスワード等による情報漏えい対策を施さなければならない。【第４章２（５）ウ】
３Ｂ	行政事務で取り扱う情報資産のうち，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，取扱いの非常に留意すべき情報資産	
３Ｃ	行政事務で取り扱う情報資産のうち，自治体機密性３Ｂ以上に相当する機密性は要しないが，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	機密性３Ａ～３Ｃ・２共通 ・外部に提供するときは，必要に応じ暗号化又はパスワードの設定を行わなければならない。【第４章２（９）ア】 ・外部に提供するときは，情報セキュリティ管理者に事前に許可を得た上で，日時・担当者及び提供概要を記録しなければならない。【第４章２（９）イ】 ・電子記録媒体の搬送にあたっては，必要に応じ鍵付きのケース等に格納し，暗号化又はパスワードの設定を行う等，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。【第４章２（８）ア】 ・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に許可を得なければならない。【第４章２（８）イ】 ・職員は，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。【第７章１（９）】 ・会計年度任用職員が情報資産を取り扱う必要が生じた場合は，情報セキュリティ管理者等管理権限のある者は従事させる事務の範囲を指定する。また，
２	直ちに一般に公表することを前提としていないもの（機密性３ＡからＣには当てはまらないが，広報等は行っていないデータ及びそれらが含まれる電子記録媒体，パーソナルコンピュータ，システム等）	

		会計年度任用職員は前述（１）～（９）に定める事項を守らなければならない。【第７章１（１１）】 【機密性２】 ・電子メールにより機密性２のデータを送信する者は，必要に応じパスワード等による情報漏えい対策を施すものとする。【第４章２（５）エ】
１	機密性２又は機密性３Ａから３Ｃ以外の情報資産	－

完全性

	分類基準	取扱制限
２	行政事務で取り扱う情報資産のうち，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資産	・バックアップ，電子署名付与 ・外部で情報処理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
１	自治体完全性２の情報資産以外の情報資産	－

可用性

	分類基準	取扱制限
２	行政事務で取り扱う情報資産のうち，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，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
１	自治体可用性２の情報資産以外の情報資産	－

(2) 情報資産の機密性，完全性，可用性のいずれかの重要性分類２以上に分類される情報資産は，この対策基準の対象とする。

また，重要性分類１の情報資産も，必要なものはできる限りこの対策基準に準じた対応を講じるものとする。

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１の分類に基づき管理しなければならない。

ウ　クラウドサービスの環境に保存される情報資産についても１の分類に基づき管理しなければならない。また，情報資産におけるライフサイクル（作成，入手，利用，保管，送信，運搬，提供，公表,廃棄等）の取扱いを定めなければならない。

(2) 情報資産の管理方法

情報取扱者は，情報資産について，ファイル（電子を含む。），格納する電磁的記録媒体のラベル，文書の隅等に，１(1)の重要性分類を表示し，必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

(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，作成時に１(1)の重要性分類に基づき，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　職員等が作成した情報資産を入手したときは，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。

イ　職員等以外から情報資産を入手したときは，１ (1)の重要性分類に基づき，当該情報の分類と取扱制限を定めなければならない。

ウ　情報資産を入手したとき，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ときには，業務上の目的以外に情報資産を利用してはならない。

イ　情報資産の利用においては，情報資産の分類に応じ，利用者及びアクセス権限を定めなければならない。

ウ　機密性３Ａから３Ｃの情報は，情報セキュリティ管理者の許可を得た場合，複製・送付・送信を行うことができる。また，権限のある者だけがアクセスできる環境で，保存・利用をしなければならない。複数の権限ある者でデータを共有したり，所属外にデータを送付・送信したりするときは，パスワード等による情報漏えい対策を施さなければならない。

エ　電子メール等により機密性２以上のデータを送信する者は，必要に応じパスワ

ード等による情報漏えい対策を施すものとする。

オ　情報資産を利用するときは，電子記録媒体又は紙媒体に情報資産の分類が異なるデータが複数記録されている場合，最高度の分類に従って，当該媒体を取り扱わなければならない。

(6) 情報資産の保管

ア　情報資産管理責任者は，情報資産の重要性分類に従って，情報資産の保管を適正に行わなければならない。

イ　情報資産管理責任者は，最終的に確定したデータを記録した電子記録媒体を長期保存する場合は，書込禁止の措置を講じなければならない。

ウ　情報資産管理責任者は，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子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への保管を考慮しなければならない。

エ　情報資産管理責任者は，持ち運び可能な電子記録媒体に耐火，耐熱，耐水及び耐湿対策を講じ，施錠可能な場所への保管等適切な管理を行わなければならない。

(7) 情報の送信

機密性２以上の情報を電子メール等により送信する者は，必要に応じ，情報を暗号化し又は情報にパスワードの設定を行う等，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。

(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ときは，必要に応じ鍵付きのケース等に格納し，暗号化又はパスワードの設定を行う等，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に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ときは，必要に応じ暗号化又はパスワードの設定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ときは，情報セキュリティ管理者に事前に許可を得た上で，日時，担当者及び提供概要を記録しなければならない。

ウ　情報資産管理責任者は，住民に公表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

ア　情報資産の廃棄又はリース返却等を行う場合は，当該媒体に含まれる情報の消

去を行った上で裁断等により物理的に破壊し，復元不可能な状態にして廃棄しなければならない。

紙媒体が不要となった場合は，焼却，裁断等により廃棄しなければならない。

イ　情報資産の廃棄又はリース返却等を行うときは，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　情報資産の廃棄又はリース返却等を行うときは，情報資産管理責任者の許可を得なければならない。

エ　クラウドサービスで利用する全ての情報資産について，クラウドサービスの利用終了時期を確認し，クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

第５章　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（以下「基幹系」という。）

(1) 基幹系と他の領域との分離

基幹系と他の領域を通信できないようにしなければならない。ただし，基幹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アドレス等）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。なお，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はなく，ＬＧＷＡＮ（総合行政ネットワーク）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証手段のうち，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

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。

(3) マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの取り扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については，マイナンバー利用事務系として扱い，本市の他の領域とはネットワークを分離しなければならない。

(4) マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取り扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合はその情報資産の機密性を考慮し，暗号等のセキュリティ対策を実施しなければならない。

また，クラウドサービス事業者が提供する情報資産を保護するための機能や情報を入手し，その機能について理解に努め，必要な措置を行わなければならない。

2　ＬＧＷＡＮ（総合行政ネットワーク）接続系

(1) ＬＧＷＡＮ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，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) 岡山県及び市区町村のインターネット接続口を集約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。

第６章　物理的セキュリティ

１　サーバ等の管理

(1) 入退室の管理

情報資産管理責任者は，重要性分類３のデータを取扱う執務区域については，許可された者以外の立入を制限するなどの適正な入退室管理を行わなければならない。

なお，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，当該機器の管理及び運用を行う部屋（以下「管理区域」という。）については，さらに次の事項に従い厳重な管理を行わなければならない。

ア　管理区域を新設する場合は，管理区域を地階又は１階に設けてはならない。また，外部からの侵入が容易にできないようにしなければならない。

イ　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。

ウ　情報取扱者は，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。

エ　管理区域への入退室は，許可された者のみに制限し，入退室管理簿の記載するとともにＩＣカードによる入退室管理を行わなければならない。

オ　外部からの訪問者が管理区域に入室する場合には，必要に応じて立ち入り区域を制限したうえで，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施すものとする。

カ　管理区域については，当該システムに関連しないコンピュータ，通信回線装置，電子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) 装置の取付け等

ア　情報システム管理者は，ネットワーク機器及び情報システム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切な固定を行う等必要な措置を施さなければならない。

イ　情報システム管理者は，システムの停止により，行政事務の執行等に重大な影響を及ぼすおそれがあるものについて二重化等を行い，同一データを保持し，システムの運用が停止しないように努めなければならない。

ウ　権限のある者以外の者が容易に操作できないように，情報システム管理者は，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。

(3) サーバの冗長化

ア　情報システム管理者は，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及びその他の基幹系サーバを冗長化し，同一データを保持しなければならない。

イ　情報システム管理者は，メインサーバに障害が発生した場合に，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低限にしなければならない。

(4) 電源

ア　情報システム管理者は，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　情報システム管理者は，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施さなければならない。

(5) 配線

ア　配線の変更，追加については，情報システム管理者等限られた者と操作を認められた委託事業者の権限とする。

イ　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施さなければならない。

ウ　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。

エ　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切に管理しなければならない。

(6) 機器等の定期保守及び修理

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

イ　情報システム管理者及び情報セキュリティ管理者は，記憶装置を内蔵する機器を外部の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，外部の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他，秘密保持体制の確認等を行わなければならない。

(7) 消火薬剤及び消防用設備

消火薬剤及び消防用設備等は，機器及び電子記録媒体に影響を与えるものであってはならない。

(8) 敷地外への機器の設置

情報システム管理者は，庁舎の敷地外にサーバ等の機器を設置する場合，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。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。

(9) 機器の廃棄等

ア　情報資産管理責任者は，機器を廃棄，リース返却等をする場合，機器内部の記憶装置から，すべてのデータを消去の上，復元不可能な状態にする措置を施さなければならない。

イ　クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をするときは，セキュリティを確保した対応となっているか，クラウドサービス事業者の方針及び手順について確認しなければならない。

なお，当該確認にあたっては，クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には，その監査報告書や認証等を利用する必要がある。

(10) 機器等の搬入出

ア　情報システム管理者は，機器等を搬入する場合，あらかじめ当該機器等の既存情報システムに与える影響について，職員に確認を行わせなければならない。

イ　機器等の搬入出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。

2　ネットワークの管理

(1) 庁舎内の通信回線等の管理

情報システム管理者は，庁舎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，適切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切に保管しなければならない。

(2) 外部ネットワークへの接続

情報システム管理者は，通信回線による外部ネットワークへの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。

(3) ＬＧＷＡＮへの集約

統括情報セキュリティ責任者は，国・県等のネットワークに接続する場合は，ＬＧＷＡＮに集約するように努めなければならない。

(4) 機密を要する情報システムで使用する回線

情報システム管理者は，所管する情報システムにおいて機密性３Ａから３Ｃ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うえ，適切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うものとする。

(5) ネットワークで使用する回線

ア　ネットワークに使用する回線は送信途上においてデータの破壊，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が実施されたものでなければならない。

イ　情報システム管理者は，ネットワークで使用する回線を選択するにあたって，必要な可用性を考慮しなければならない。

3　端末等の管理

(1) 端末等の盗難防止策

情報資産管理責任者及び情報セキュリティ管理者は，執務室等の端末等について，ワイヤーによる固定等盗難防止のための措置を講じなければならない。

(2) ログインパスワード

情報システム管理者は，情報システムへのログインに際し，パスワード，スマートカード又は生体認証等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。また，必要に応じて電源起動時のパスワード（ＢＩＯＳパスワード，ハードディスクパスワード等）を併用するものとする。

(3) 認証の併用

情報システム管理者は，取り扱う情報の重要度に応じて，パスワード以外にＩＤカード，生体認証等を導入し，二要素認証を行うものとする。

(4) 暗号化機能の利用

情報システム管理者は，端末のデータ暗号化等の機能を有効に利用しなければならない。また，電子記録媒体についても，取り扱う情報の重要度に応じて，データ暗号化機能を備える媒体を使用しなければならない。

(5) タブレット端末等の持ち運び可能な端末（モバイル端末）のセキュリティ

モバイル端末を庁外で業務利用する場合は，端末の紛失・盗難対策として，普段からディスク暗号化機能を設定するとともに，パスワードによる端末ロックを設定しておかなければならない。また，紛失・盗難に遭った際の対応として，遠隔消去（リモートワイプ）や自己消去機能などを活用できるときは，それらの機能を活用し，モバイル端末内のデータを消去しなければならない。

(6) 電磁的記録媒体（USB メモリ等）の取扱い

USB メモリ等（持ち運び可能な小型の電磁的記録媒体）の取扱いに当たっては，紛失,盗難,ウイルス感染及びデータ漏えい等を防止するため，次の手段により実施しなければならない。

ア　端末には利用許可された媒体のみ接続可能とすること。

イ　データは暗号化しパスワードを設定すること。

ウ　利用媒体は，全て管理し利用履歴を残せること。

エ　データの受け渡しには，必ず情報セキュリティ管理者の承認と承認記録を残せること。

第７章　人的セキュリティ

1　職員等の責務

(1) 情報セキュリティポリシー等の遵守義務

職員等は，情報セキュリティポリシー及びこれに基づく文書に定められている事項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がある場合には，情報資産管理責任者に相談し，指示を仰がなければならない。

(2) 法令等の遵守義務

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，以下の法令のほか関係法令等を遵守しこれに従わなければならない。

ア　地方公務員法（昭和 25 年法律第 261 号）

イ　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）

ウ　著作権法（昭和 45 年法律第 48 号）

エ　個人情報の保護に関する法律（平成 15 年法律第 57 号）

オ　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）

カ　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）

キ　笠岡市個人情報の保護に関する法律施行条例（令和 5 年笠岡市条例第 1 号）

ク　笠岡市文書取扱規程（平成 10 年笠岡市訓令第 10 号）

(3) 指示に基づいた情報資産の利用等

職員等は，情報資産管理責任者の指示等に従い，情報資産を利用するとともに，開発，設定の変更，運用，更新等の作業を行う。

(4) 支給以外の端末及び電磁的記録媒体等の業務利用

ア　職員等は，管理外のパソコン，モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし，管理外の端末の業務利用の可否判断を統括情報セキュリティ管理者が行った後に，業務上必要な場合は情報セキュリティ管理者の許可を得て利用することができる。また，緊急時又は災害時等で必要とする場合は，統括情報セキュリティ責任者の許可を得て利用することができる。

イ　職員等は，外部で管理外の端末及び電磁的記録媒体等を用い業務作業を行う場合は，情報資産管理責任者の許可を得なければならない。

(5) 情報資産の持ち出し及び持ち込みの記録

ア　職員等は情報資産管理責任者の許可を得た場合に限り，端末，通信回線装置，

電磁的記録媒体等の持出しについて，記録を作成した上で，庁外へ情報資産を持ち出すことができる。

イ　情報資産を持ち込む場合は，情報資産管理責任者の許可を得なければならない。

(6) 業務目的外の利用禁止

職員等は，業務目的外でのパーソナルコンピュータ等の利用，情報システムへのアクセス，電子メールの利用及びインターネットへのアクセス等を行ってはならない。

(7) 端末等の利用

ア　職員等は，端末の設定及び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。

イ　職員等は，端末や電子記録媒体，データが印刷された文書等について，第三者に使用されること，又は情報資産管理責任者の許可なく情報を閲覧されることがないように，離席時の端末のロックや電子記録媒体，文書等の容易に閲覧されない場所への保管等，適切な措置を講じなければならない。

(8) 執務室外における情報処理作業の制限

ア　統括情報セキュリティ責任者は，機密性２以上，可用性３，完全性３の情報資産を執務室外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，執務室外で情報処理作業を行う場合には，情報資産管理責任者の許可を得なければならない。

ウ　職員等は，執務室外で情報処理作業を行う際，個人の所有するパーソナルコンピュータによる情報処理を行ってはならない。

(9) 異動，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。

(10) クラウドサービス利用時等の遵守事項

職員等は，クラウドサービスの利用にあたっても情報セキュリティポリシーを遵守し，クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

(11) 会計年度任用職員

会計年度任用職員が情報資産を取り扱う必要が生じた場合は，情報資産管理責任者は従事させる事務の範囲を指定する。また，会計年度任用職員は前述(1)～(10)に定める事項を守らなければならない。

(12) 職員等

情報セキュリティ管理者は，職員等に対し，採用時のみならず情報セキュリティポリシー等の改変があるごとに，職員等が守るべき内容を理解させ，実施及び遵守させなければならない。

2　研修・訓練

(1) 職員等に対する研修・訓練の実施

最高情報セキュリティ責任者は，定期的に情報取扱者に対する情報セキュリティに関する研修・訓練を実施させなければならない。

(2) 研修計画の策定及び実施

ア　統括情報セキュリティ責任者は，情報取扱者に対する情報セキュリティに関する研修計画を定期的に策定し，最高情報セキュリティ責任者に報告しなければならない。

イ　情報取扱者を対象とする情報セキュリティに関する研修を毎年度最低１回実施しなければならない。

ウ　統括情報セキュリティ責任者は，毎年度１回，情報セキュリティ委員会に対して，情報セキュリティに関する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

最高情報セキュリティ責任者は，緊急時対応を想定した訓練を定期的に実施させるものとする。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，訓練実施の内容等を定め，また，効果的に実施できるようにしなければならない。

(4) 研修等への参加

すべての情報取扱者は，情報セキュリティに関する意識を深め情報セキュリティ上の問題が生じないようにするため，定められた研修・訓練に参加しなければならない。

3　情報セキュリティに関する事件・事故等の報告・分析等

(1) 情報セキュリティに関する事件・事故等の報告

ア　情報取扱者は，情報セキュリティに関する事件・事故等を発見した場合，若しくは住民等外部から報告を受けた場合，速やかに情報システム管理者に報告しなければならない。

イ　報告を受けた情報システム管理者は，速やかに情報資産管理責任者に報告しなければならない。

ウ　情報セキュリティ管理者は，報告のあった情報セキュリティに関する事件・事故等について，国，県等の業務上の関係機関に必要な連絡を行うとともに，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。

エ　情報セキュリティ管理者は，報告のあった情報セキュリティに関する事件・事故等について，統括情報セキュリティ責任者及び最高情報セキュリティ責任者，並びに国，県等の関係機関に報告しなければならない。

オ　情報セキュリティ管理者は，原則，情報セキュリティインシデント対応（侵害時の対応と緊急時対応計画）実施手順書に記載されている情報セキュリティインシデント判定基準のレベル３に該当する事件・事故等が発生した場合はCSIRTを立ち上げ対応するものとする。

カ　最高情報セキュリティ責任者は，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るための窓口を設置し，当該窓口への連絡手段を公表しなければならない。

(2) 事故等の分析・記録等

ア　情報セキュリティに関する事件・事故等を引き起こした部門の情報システム管理者は，情報セキュリティ管理者と連携し，当該情報セキュリティに関する事件・事故等を分析し，記録を保存しなければならない。また，情報セキュリティに関する事件・事故等の原因究明の結果から，再発防止策を検討し，必要に応じて，最高情報セキュリティ責任者に報告するものとする。

イ　最高情報セキュリティ責任者は，情報セキュリティに関する事件・事故等の再発防止策について報告を受けたときは，その内容を確認し，再発防止策を実施するための必要な措置を指示しなければならない。

４　アクセスのための認証情報及びパスワードの管理

(1) アカウント等の管理

ア　情報資産管理責任者はアカウント等の適正な管理を行わなければならない。

イ　情報取扱者は，次の事項を遵守しなければならない。

アカウント等は，情報取扱者間で共有しない。ただし，所属等ごとに配布されたアカウントについては除く。

ウ　情報資産管理責任者は，不正使用等の通報があり次第速やかに当該アカウント等を使用したアクセス等を停止する。

(2) ＩＤの管理

ア　情報取扱者は，他人に自己が利用しているＩＤを利用させてはならない。

イ　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) パスワードの管理

ア　情報取扱者は，自己のパスワードに関し，次の事項を遵守しなければならない。

(ｱ) パスワードは秘密にし，パスワードの照会等には一切応じない。

(ｲ) 情報システム又はパスワードに対する危険のおそれがある場合には，情報資産管理責任者に速やかに報告し，パスワードを速やかに変更する。

(ｳ) パスワードを記載したメモを作成する場合は，特定の場所に施錠して保存する等により，他人が容易に見ることができない措置をとる。

(ｴ) パスワードは十分な長さ（原則として８文字以上）とし，文字列は想像しにくいもの（英字（大文字・小文字区別有），数字，記号を組み合わせたものなど）とする。

(ｵ) パスワードは定期的（概ね１００日以内）又はアクセス回数に基づいて変更し，古いパスワードを再利用しない。

(ｶ) 複数の情報システムを扱う場合は，同一のパスワードを複数のシステムで用いない。

(ｷ) 仮のパスワードは，最初のログイン時点で変更する。

(ｸ) パーソナルコンピュータ等のパスワードの記憶機能を利用しない。

(ｹ) 情報取扱者の間でパスワードを共有しない。

イ　情報システム管理者は，パスワードの照会等には一切応じてはならない。

5　外部委託に関する管理

(1) 委託先事業者の選定

特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は，委託先の選定にあたり，委託内容に応じた情報セキュリティ対策の実施が確保されることを確認しなければならない。

(2) 契約書の記載事項

ア　特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は，当該委託先事業者との間で，下記事項を明記した契約を締結しなければならない。

(ｱ) データその他業務上知り得た情報（以下「データ等」という）の秘密の保持に関する事項

(ｲ) 第三者への委託（以下,「再委託」という。）の禁止又は制限に関する事項

(ｳ) データ等の目的以外の目的のための使用及び第三者への提供の禁止に関する事項

(ｴ) データ等の複写及び複製の禁止に関する事項

(ｵ) データ等の取り扱いに関する事故の発生時における報告義務に関する事項

(ｶ) データ等の取り扱いに関する検査の実施に関する事項

(ｷ) 契約に違反した場合における契約の解除及び損害賠償に関する事項

(ｸ) 委託業務終了時の情報資産の返還，廃棄等に関する事項

(ｹ) 情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項

(ｺ) 事故時等の公表に関する事項

(ｻ) 委託先の責任者，委託内容，従事者，作業場所の特定に関する事項

(ｶ) 委託事業者に重要情報を提供する場合は，秘密保持契約を締結

イ　前項に加えて，次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。

(ｱ) 提供されるサービスレベルの保証に関する事項

(ｲ) 委託業務の定期報告及び緊急時報告義務に関する事項

(ｳ) 外部施設等への情報資産の搬送時における紛失，盗難，不正コピー等の防止に関する事項

(ｴ) 委託先の責任者及び従事者に対する研修の実施に関する事項

(ｵ) 情報セキュリティ確保への取り組みの実施状況に係る報告義務に関する事項

(3) 情報セキュリティ確保への取組みの実施状況等の調査

情報資産管理責任者は，契約締結後においても，当該委託先事業者の情報セキュリティ確保への取組みの実施状況等について，定期的若しくは随時，調査を行い，安全を確保しなければならない。情報セキュリティ責任者から内容の報告を求められた場合には，報告を行わなければならない。

(4) 再委託等

再委託（再々委託を含む。）を受ける事業者がある場合，第７章５（２）及び第７章５（３）に定める事項は再委託（再々委託を含む。）を受ける事業者にも適用する。

(5) 委託事業者に対する説明

情報セキュリティ管理者は，ネットワーク及び情報システムの開発・保守等を事業者に発注する場合，再委託事業者も含めて，情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

第８章　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

(1) データの保存

データの保存については，情報資産管理責任者の定める方法により保存を行わなければならない。

(2) ファイルサーバの設定等

情報システム管理者がデータを共有するためのファイルサーバを設置する場合には，次の事項を守らなければならない。

ア　職員，会計年度任用職員が使用できるファイルサーバの容量を設定し，職員，会計年度任用職員に周知しなければならない。

イ　ファイルサーバを所属等の単位で構成し，職員，会計年度任用職員が他所属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。

ウ　特定の職員，特定の会計年度任用職員のみが取扱う権限を持つデータについては，同一所属であっても，権限のない者が閲覧及び使用できないよう設定しなければならない。

(3) アクセス記録の取得等

ア　情報資産管理責任者は，所管するシステムにおいて，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取得し，窃取，改ざん，誤消去等を防止する措置を施した上で一定期間保存する。また，不正アクセスの兆候を発見するために定期的にそれらを分析することとする。

イ　情報システム管理者は，システムから自動出力したアクセス記録等について，必要に応じ，外部記録媒体にバックアップしなければならない。

(4) 仕様書等の保管

情報資産管理責任者は，所管するシステムのネットワーク構成図，情報システム仕様書等に関し，記録媒体の形態に関わらず，業務上必要とする者以外の者が閲覧したり，紛失したりすることがないよう，適切な保管をしなければならない。

(5) 情報資産のバックアップ

情報資産管理責任者は，所管するシステムにおいて，必要なものはサーバの冗長化対策実施の有無に関わらず，定期的に情報資産のバックアップのための対応を行うものとする。

(6) 他団体との情報システムに関する情報等の交換

情報資産管理責任者は，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，その取り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。

(7) 通信回線によるデータの送信

情報システム管理者は，所管するシステムにおいて，通信回線によりデータを送信する場合，専用通信回線を使用又は送信するデータを必要最小限にする等データの保護のために適切な措置を講じなければならない。

(8) 外部の者が利用するシステム

情報システム管理者は，インターネット等により外部の者が利用できるシステムにおいては，必要に応じ他のネットワーク及び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に対策をとらなければならない。

(9) Ｗｅｂサイトでの情報公開時の注意事項

情報資産管理責任者は，Ｗｅｂサイトにより情報を公開・提供する場合に，所管するサイトに係るシステムにおいて情報の漏えい・改ざん・消去，踏み台，ＤｏＳ攻撃等を防止しなければならない。また，メールシステムを含め各業務システムにおいても，他のシステムに対する攻撃の踏み台とならないようにコンピュータウイルス対策等適切な管理をしなければならない。

(10) 無線ＬＡＮ及びネットワークの盗聴対策

ア　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づけなければならない。

イ　統括情報セキュリティ責任者は，機密性の高い情報を取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。

(11) 無許可ソフトウェアの導入等の禁止

ア　情報取扱者は，各自に供与された端末に対して，無断でソフトウェアを導入してはならない。

イ　情報取扱者は，業務を円滑に遂行するために必要なソフトウェアがある場合，情報システム管理者が定める手続きを行い，必要な許可を得て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。

ウ　情報取扱者は，不正にコピーしたソフトウェア及び個人所有のソフトウェアを導入又は使用してはならない。

(12) 機器構成の変更の禁止

情報取扱者は，ネットワーク及び各自に供与された端末等に対して，端末及びそ

の他機器の接続，増設又は改造を行ってはならない。軽微な機器の増設の場合は，情報資産管理責任者の許可を必要とする。

(13) 電子メール

ア　情報システム管理者は，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。

イ　情報システム管理者は，電子メールに添付されるファイルについて，セキュリティ上問題があると思われるファイルについては，送受信を制限できるようにしなければならない。

ウ　情報システム管理者は，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。

エ　メールアドレス保有者は，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。

オ　メールアドレス保有者は，複数の宛先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わからないようにしなければならない。

カ　メールアドレス保有者は，重要な電子メールを誤送信した場合，情報資産管理責任者に報告しなければならない。

キ　メールアドレス保有者は，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。ただし，業務上やむを得ない場合は，情報資産管理責任者の許可を得た場合に限り転送をすることができる。

ク　情報システム管理者は，システム開発や運用，保守等のため庁舎内に常駐している委託業者の作業員による電子メールアドレスの利用について，委託事業者との間で利用方法を取り決めなければならない。

(14) Ｗｅｂ会議サービスの利用時の対策

ア　統括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，Ｗｅｂ会議を適切に利用するための利用手順を定めなければならない。

イ　職員等は，統括情報セキュリティ責任者及び情報セキュリティ管理者が定める利用手順に従い，Ｗｅｂ会議の参加者や取り扱う情報の機密性に応じた情報セキュリティ対策を実施するよう努めなければならない。

ウ　職員等は，Ｗｅｂ会議を主催する場合は，会議に無関係の者が参加できないよう対策を講じなければならない。

エ　職員等は，外部からＷｅｂ会議に招待される場合は，統括情報セキュリティ責任者及び情報システム管理者が定める利用手順に従い，Ｗｅｂ会議に参加し

なければならない。

(15) ソーシャルメディアサービスの利用

ア　統括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，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しなければならない。

(ｲ) パスワード及び認証のためのコード等の認証情報並びにこれを記録した媒体（ハードディスク，ＵＳＢメモリ，紙等）等を適正に管理するなどし，不正アクセス対策を実施しなければならない。

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

ウ　情報セキュリティ管理者は，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なければならない。

エ　情報セキュリティ管理者は，アカウント乗っ取りを確認した場合のは，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。

オ　情報セキュリティ管理者は，可用性１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。

(16) 電子署名・暗号化

ア　情報取扱者は，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，統括情報セキュリティ責任者が定める電子署名，暗号化又はパスワード設定等の方法を用いて，送信しなければならない。

イ　情報取扱者は，暗号化を行う場合に統括情報セキュリティ責任者が定める以外の方法を用いてはならない。また，統括情報セキュリティ責任者が定める方法で暗号のための鍵を管理しなければならない。

ウ　統括情報セキュリティ責任者は，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) 無許可端末の接続禁止

情報取扱者は，情報資産管理責任者の許可なく端末等をネットワークに接続してはならない。

(18) 利用可能なネットワークプロトコル

情報取扱者が利用できるネットワークプロトコルは，業務上必要最低限のものとする。

(19) 障害記録

情報システム管理者は，システムにおいて，情報取扱者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体系的に記録し，適切に保存しなければならない。

2　アクセス制御

情報システム管理者は，所管するネットワーク又はシステムにおいて，次の事項を実施しなければならない。

(1) 利用者の識別及び認証

情報システム管理者は，所管するネットワーク又はシステムに権限がない情報取扱者がアクセスすることが不可能となるように，利用者の識別及び認証等適切な対応を行わなければならない。

(2) 利用者登録

ア　情報システム管理者は，利用者の登録，変更，抹消，登録した情報資産の管理，異動，出向及び退職時における利用者ＩＤの取り扱い等については，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・抹消は，情報システム管理者に対する申請により行う。ただし，所属等ごとに配布されたＩＤ等については除く。

イ　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。

ウ　情報システム管理者は，ＩＤに割り当てているアクセス権の正当性を確保するために，定められた方法に従って点検しなければならない。

(3) 特権管理等

ア　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　情報システム管理者の特権を代行する者は，当該管理者が指名し，統括情報セキュリティ責任者が認めた者でなければならない。

ウ　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，情報

取扱者の端末等のパスワードと同等あるいはそれ以上のセキュリティ強化を実施しなければならない。

エ　情報システム管理者は，特権によるネットワーク及び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。

(4) ネットワークにおけるアクセス制御

情報システム管理者は，アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセスできる者を定めなければならない。また，ネットワークサービスを利用する権限を有しない情報取扱者が当該サービスを利用できるようにしてはならない。

(5) 強制的な接続制御，経路制御

ア　情報システム管理者は，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。

イ　情報システム管理者は，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，ルータ等に搭載されている通信ソフトウェア等を設定しなければならない。

(6) 無人状態にある装置の管理

情報システム管理者は，サーバ又は端末等の装置が無人の状態になる場合，適切なセキュリティ対策を施さなければならない。

(7) 外部からのアクセス

ア　情報システム管理者は，外部からのアクセスを許可する場合，合理的理由を有する必要最低限のものに限定しなければならない。

イ　内部ネットワーク及び情報システムへのアクセス方法及び利用方法等は，通信途上の機密性及び利用者の真正性が確保できるものでなければならない。

ウ　情報システム管理者は，庁外で利用する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。

(8) 内部ネットワーク間の接続

情報システム管理者は，他の内部ネットワークとの接続については，あらかじめ以下の内容を確認した上で，接続しなければならない。

ア　接続によりそれぞれの情報資産に影響が生じないこと

イ　接続した場合のそれぞれの情報システムの責任範囲

ウ　障害発生時の対応体制

(9) 外部ネットワークとの接続

ア　情報システム管理者は，外部ネットワークとの接続にあたり，当該外部ネット

ワークのネットワーク構成，機器構成，セキュリティ技術等を詳細に調査し，適用範囲における情報資産に影響が生じないことを確認した上で，情報セキュリティ責任者の許可に基づき接続しなければならない。

イ　情報システム管理者は，接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。情報システム管理者は，当該外部ネットワークの瑕疵により本市のデータの漏えい，破壊，改ざん又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応するため，必要に応じて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するよう努めなければならない。

ウ　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，適用範囲における情報資産に脅威が生じるおそれがある場合には，情報システム管理者は当該外部ネットワークとの接続を物理的に遮断することができるものとする。

(10) ネットワーク機器の自動識別

情報システム管理者は，適用範囲におけるネットワークで使用される機器について，機器固有情報等によって端末とネットワークとのアクセスの可否が自動的に識別されるよう必要に応じてシステムを設定するものとする。

(11) ログイン試行回数の制限等

情報システム管理者は，ログイン試行回数の制限及びアクセスタイムアウトの設定等により，正当なアクセス権を持たない情報取扱者が利用できないようにシステムを設定するよう考慮しなければならない。

(12) パスワードに関する情報の管理

ア　情報システム管理者は，情報取扱者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。また，情報取扱者のパスワードを発行する場合において，仮のパスワードを発行する場合，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　情報システム管理者は，パスワード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パスワード設定のセキュリティ強化機能がある場合は，これを活用しなければならない。

ウ　情報システム管理者は，仮のパスワードも含めパスワードを発行する場合，パスワードは十分な長さ（原則として８文字以上）とし，文字列は想像しにくいもの（英字（大文字・小文字区別有），数字，記号を組み合わせたものなど）としなければならない。

エ　情報システム管理者は，原則として，パスワードは定期的（概ね 100 日以内）又はアクセス回数に基づいて変更し，古いパスワードを再利用しないものとする。

3　システム開発，導入，保守等

(1) 情報システムの調達

ア　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。

イ　情報システム管理者は，機器及びソフトウェアの調達にあたっては，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。

ウ　情報セキュリティ管理者は，適切に情報セキュリティ対策を推進・管理するための基礎資料として，情報システム台帳を作成し，整理する。情報セキュリティ管理者は，情報システムを新たに調達したり，既にある情報システムを廃止したりしたときは，情報システム管理者からの求めに応じて，その旨を報告しなければならない。

(2) 情報システムの開発等

ア　情報資産管理責任者は，ネットワーク及び情報システムの開発，導入，更新及び運用保守にあたって，必要に応じて次の事項を定める。

(ｱ) 責任者及び監督者

(ｲ) 従事者及び作業範囲

(ｳ) 開発するシステムと運用中のシステムとの分離

(ｴ) 開発・保守に関する設計仕様等の成果物の提出

(ｵ) セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止

(ｶ) アクセス制限

(ｷ) 機器の搬入出の際の許可及び確認

(ｸ) 記録の提出義務

(ｹ) 仕様書・マニュアル等の定められた場所への保管

(ｺ) 情報システムに係るソースコードの適切な方法での保管

(ｻ) 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

(ｼ) 情報システムセキュリティ実施手順書等の整備

イ　情報資産管理責任者は，ネットワーク及び情報システムの開発，導入，更新及び運用保守にあたって，不正にコピーしたソフトウェア及び個人所有のソフトウェアの導入又は使用等，問題のある行為が発生しないようにしなければならない。

ウ　情報資産管理責任者は，ネットワーク及び情報システムの開発，導入，更新及

び運用保守にあたって，コンピュータウイルス等対策ソフトウェアを導入する等，ウイルス感染による情報漏えい等が発生しないようにしなければならない。

(3) 情報システムの移行

ア　情報資産管理責任者は，システム開発・導入・保守計画の策定時に情報システムの移行手順を明確にしなければならない。また，移行の際，情報システムに記録されているデータ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。

イ　情報資産管理責任者は，新たに情報システムを導入する際には，既に稼働している情報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。また，既存の情報システムを更新する際には，既に稼働している情報システムとの連携において，十分な試験を行わなければならない。

ウ　情報資産管理責任者は，擬似環境による動作確認後に情報システムの移行を行わなければならない。また，作業については，作業経過を確認しながら実施するとともに，作業内容を記録しなければならない。

エ　情報資産管理責任者は，原則として個人情報及び機密性の高い生データを試験データに使用してはならない。ただし，合理的な理由がある場合で，統括情報セキュリティ責任者が許可した場合は，この限りではない。

オ　情報資産管理責任者は，試験に使用したデータ及びその結果を一定期間厳重に管理しなければならない。

(4) 情報システムの入出力データ

ア　情報資産管理責任者は，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必要に応じて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。

イ　情報資産管理責任者は，内部処理において誤ったデータに書き換えられる等の可能性がある場合に，書き換え等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。

ウ　情報資産管理責任者は，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，出力されるように情報システムを設計しなければならない。

(5) ソフトウェアの保守及び更新

情報資産管理責任者は，ソフトウェア等を更新，又は修正プログラムを導入する場合，不具合及び他のシステムとの相性の確認を行い，計画的に更新し又は導入しなければならない。

また，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は，情報システム管理者は，速やかに対応を行わなければない。

(6) 委託業務等従事者の身分確認

情報資産管理責任者は，作業前に委託業務等従事者に対して身分証明書の提示を求め，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することができるようにしておかなければならない。

(7) 作業の確認

契約により操作を認められた委託業務等従事者が重要な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。

(8) 作業管理記録

情報資産管理責任者は，担当するシステムにおいて行ったシステム変更等の作業については，プログラム仕様書等の変更履歴を作成するとともに，作業記録を作成しなければならない。作成した作業記録は，窃取，改ざん等をされないように適切に管理を行わなければならない。

4　コンピュータウイルス等不正プログラム対策

(1) 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　コンピュータウイルス等の情報について情報取扱者に対する注意喚起を行う。

イ　常時コンピュータウイルス等に関する情報収集に努める。

ウ　コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たせるよう指導等を行う。

エ　サーバ及び端末に，コンピュータウイルス等対策ソフトウェアを常駐させる。

オ　情報システムにおいて電子記録媒体を使用する場合，本市が管理しているものを情報取扱者に使用させるとともに，当該媒体の使用にあたり，ウイルスチェックを行わせる。

カ　コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保つ。インターネットに接続していないシステムにおいても，定期的に当該ソフトウェア及び定義ファイルの更新を行う。

(2) 情報取扱者の遵守事項

情報取扱者は，次の事項を遵守しなければならない。

ア　端末において，コンピュータウイルス等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ない。

イ　外部ネットワーク及び電子記録媒体からデータ又はソフトウェアを取り入れる際には，必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

ウ　外部ネットワーク及び電子記録媒体へデータ又はソフトウェアを送信・書き込みする際には，必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

エ　差出人が不明な電子メール又は不自然なファイルが添付された電子メールを受信した場合は速やかに削除する。

オ　端末に対して，コンピュータウイルス等対策ソフトウェアによる完全スキャンを定期的に行い，スキャンの実行を途中で止めない。

カ　情報システム管理者が提供するコンピュータウイルス等の情報を常に確認する。

キ　添付ファイルのあるメールを送受信する場合は，コンピュータウイルス等対策ソフトウェアでチェックを行う。

ク　コンピュータウイルス等に感染したおそれがある場合は，速やかに情報資産管理責任者に報告するとともに，その指示に従い，ＬＡＮケーブルの取り外しや端末の通信機能の停止等，他への感染を防止する措置を講じる。

ケ　端末には，業務に必要なソフトウェアのみをインストールするとともに，端末に導入されているソフトウェアについて，情報システム管理者等から最新版へのアップデートの指示等があったときは，速やかにその指示に従う。

(3) 専門家の支援体制

統括情報セキュリティ責任者は，実施しているコンピュータウイルス等対策では不十分な事態が発生した場合に備え，コンピュータウイルス等対策ソフトのサポート契約を締結する等，必要に応じて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。

5　不正アクセス対策

(1) 使用されていないポートの閉鎖等

統括情報セキュリティ責任者は，全てのシステムにおいて，不正なアクセスによる影響を防止するための必要な措置を講じるものとする。

ア　使用されていないポートを閉鎖する。

イ　サーバ上の不要なサービスを停止する。

ウ　不正アクセスによるデータの書換えを検出する等，Ｗｅｂサイトの改ざんを防止する。

エ　ソフトウェアにセキュリティホールが発見された場合は，速やかに修正プログラムを適用する。

(2) 攻撃の予告等への措置

統括情報セキュリティ責任者は，システムへの攻撃の予告等サーバ等に不正アク

セスを受けることが明白な場合には，システムの停止，他のネットワークとの切断等の必要な措置を講じなければならない。

また，警察・関係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。

(3) 記録の保存

最高情報セキュリティ責任者及び統括情報セキュリティ責任者は，不正アクセス行為の禁止等に関する法律違反等犯罪の可能性がある不正アクセスを受けた場合，不正アクセスの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。

(4) 内部からの不正アクセスの監視

統括情報セキュリティ責任者は，情報取扱者が使用している端末からの庁内のサーバ等に対する不正アクセスや外部のサイトに対する不正アクセスを監視しなければならない。

(5) 情報取扱者による不正アクセス時の措置

情報取扱者による不正アクセスがあった場合，統括情報セキュリティ責任者は当該情報取扱者が所属する課の情報セキュリティ管理者に通知し，適切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に努めなければならない。

(7) 標的型攻撃

統括情報セキュリティ責任者は，情報システムにおいて，標的型攻撃による内部への侵入を防止するために，研修・啓発や自動再生無効化等の人的対策・入口対策を講じたり，内部に侵入した攻撃を早期検知して対処するために，通信をチェックするなどの内部対策を講じたりするなど，必要な対策に努めなければならない。

6　セキュリティ情報の収集

情報セキュリティ管理者は，セキュリティホール等の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情報を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。

第９章　運用面のセキュリティ

１　情報システムの監視

情報資産管理責任者は，所管するシステムにおいて，次の事項を実施しなければならない。

(1) 事象の検知

情報資産管理責任者は，セキュリティに関する事象を検知するため，システムの監視を行わなければならない。

(2) 時刻同期

情報資産管理責任者は，重要なアクセスログ等を取得するサーバの正確な時刻設定又はサーバ間の時刻同期ができる措置を施さなければならない。

(3) 常時監視

情報資産管理責任者は，外部と接続するシステムを稼働中，常時監視しなければならない。

２　情報セキュリティポリシー等の遵守状況の確認及び対処

情報資産管理責任者は，所管の範囲において情報セキュリティポリシー及びこれに基づく文書の遵守状況について常に確認を行い，問題を認めた場合には速やかに情報セキュリティ責任者に報告しなければならない。情報セキュリティ管理者は，発生した問題について，適切かつ速やかに対処しなければならない。

３　運用管理における留意点

(1) 調査権限のある職員の指名

統括情報セキュリティ責任者は，情報漏えい，不正アクセス，コンピュータウイルス等の調査のために，パーソナルコンピュータ，電子記録媒体，アクセス記録及びメール等の情報を調査する権限を有する職員を指名することができる。

(2) 情報セキュリティポリシー等の閲覧

情報資産管理責任者は，職員，会計年度任用職員が常に情報セキュリティポリシー及びこれに基づく文書を参照できるよう配慮しなければならない。

(3) 管理者権限

情報システム管理者及び情報セキュリティ管理者の権限を代行する者は，それぞれが指名する。

(4) 情報取扱者の報告義務

ア　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，直ちに情報資産管理責任者に報告を行わなければならない。

イ　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は，緊急時対応計画に従って適切に対処しなければならない。

4　緊急時の対応

(1) 緊急時対応計画の策定

情報システム管理者は，情報資産への重大な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切に実施するために，緊急時対応計画を策定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，次の内容を定めなければならない。

ア　関係者の連絡先

イ　意思決定の所在

ウ　発生した事象に係る報告すべき事項

エ　発生した事象への対応措置

オ　再発防止措置の策定

(3) 業務継続計画との整合性

自然災害，大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し，情報セキュリティ委員会は当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。

(4) 緊急時対応計画の見直し

情報システム管理者は，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，必要に応じて緊急時対応計画を見直さなければならない。

5　例外措置

(1) 例外措置の許可

情報資産管理責任者は，情報セキュリティポリシー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，最高情報セキュリティ責任者の許可を得て，例外措置を取ることができる。

なお，統括情報セキュリティ責任者が，軽微な例外措置と判断したものについては，当該責任者の許可により，例外措置を取ることができる。

(2) 緊急時の例外措置

情報資産管理責任者は，前項に該当する場合であって，行政事務の遂行に緊急を要し，前項に定める許可を得る時間的な猶予のないときは，例外措置を実施し，実

施後速やかに最高情報セキュリティ責任者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。

(3) 例外措置の報告書等の管理

最高情報セキュリティ責任者は，例外措置の報告書及び審査結果を適切に保管させなければならない。

第 10 章　業務委託と外部サービス（クラウドサービス）の利用

1　業務委託

(1) 業務委託に係る運用規程の整備

統括情報セキュリティ責任者は，業務委託に係る以下の内容を全て含む運用規程を整備しなければならない。

①委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

②委託事業者の選定基準

(2) 業務委託実施前の対策

①情報セキュリティ管理者又は情報システム管理者は，業務委託の実施までに，以下を全て含む事項を実施しなければならない。

（ア）委託する業務内容の特定

（イ）委託事業者の選定条件を含む仕様の策定

（ウ）仕様に基づく委託事業者の選定

（エ）情報セキュリティ要件を明記した契約の締結（契約項目）

重要な情報資産を取扱う業務を委託する場合には，委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件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及び情報セキュリティ実施手順の遵守

・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

・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

・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

・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委託事業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返還，廃棄等

・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）

（オ）委託事業者に重要情報を提供する場合は，秘密保持契約の締結

②情報セキュリティ管理者又は情報システム管理者は，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。

（ア）仕様に準拠した提案

（イ）契約の締結

（ウ）委託事業者において重要情報を取り扱う場合は，秘密保持契約の締結

(3)業務委託実施期間中の対策

①情報セキュリティ管理者又は情報システム管理者は，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。

（ア）委託判断基準に従った重要情報の提供

（イ）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

（ウ）統括情報セキュリティ責任者へ措置内容の報告（重要度に応じて最高情報セキュリティ責任者に報告）

（エ）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等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

②情報セキュリティ管理者又は情報システム管理者は，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。

（ア）情報の適正な取扱いのための情報セキュリティ対策

（イ）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

（ウ）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)業務委託終了時の対策

①情報セキュリティ管理者又は情報システム管理者は，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。

（ア）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

（イ）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

②情報セキュリティ管理者又は情報システム管理者は，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。

（ア）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

（イ）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

2　外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱う場合）

(1) クラウドサービスの選定に係る運用規程の整備

統括情報セキュリティ責任者は，自治体機密性２以上の情報を取り扱う場合，以下を含む外部サービス（クラウドサービス，以下「クラウドサービス」という。）の選定に関する規定を整備しなくてはならない。

①クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「クラウドサービス利用判断基準」という。）

②クラウドサービス提供者の選定基準

③クラウドサービスの利用申請の許可権限者と利用手続

④クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

(2)　クラウドサービスの利用に係る運用規程の整備

統括情報セキュリティ責任者は，自治体機密性２以上の情報を取り扱う場合，以下を含クラウドサービス（自治体機密性２以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。

①統括情報セキュリティ責任者は，クラウドサービスの特性や責任分界点に係る考え方等を踏まえ，クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

②統括情報セキュリティ責任者は，クラウドサービスの特性や責任分界点に係る考え方を踏まえ，クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

③統括情報セキュリティ責任者は，クラウドサービスの特性や責任分界点に係る考え方を踏まえ，以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。

(ア)クラウドサービスの利用終了時における対策

(イ)クラウドサービスで取り扱った情報の廃棄

(ウ)クラウドサービスの利用のために作成したアカウントの廃棄

(3) クラウドサービスの選定

①情報セキュリティ責任者は，取り扱う情報の格付及び取扱制限を踏まえ，クラウドサービス利用判断基準に従って，業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。

②情報セキュリティ責任者は，クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ，クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定すること。また，以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。

（ア）クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止

（イ）クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制

（ウ）クラウドサービスの提供に当たり，クラウドサービス提供者若しくはその従業員，再委託先又はその他の者によって，本市の意図しない変更が加えられないための管理体制

（エ）クラウドサービス提供者の資本関係・役員等の情報，クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

③情報セキュリティ責任者は，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，クラウドサービス提供者の選定条件に含めなければならない。

④情報セキュリティ責任者は，クラウドサービスの利用を通じて本市が取り扱う情報の格付等を勘案し，必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めなければならない。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

⑤情報セキュリティ責任者は，クラウドサービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し，必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

⑥情報セキュリティ責任者は，クラウドサービス提供者がその役務内容を一部再委託する場合は，再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう，クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させるとともに，再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し，本市の承認を受けるよう，クラウドサービス提供者の選定条件に含めなければならない。また，クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

⑦情報セキュリティ責任者は，取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め，クラウドサービスを選定しなければならない。また，クラウドサービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。

⑧情報セキュリティ責任者は，クラウドサービスの特性を考慮した上で，クラウドサービスが提供する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，情報セキュリティに関する役割及び責任の範囲を踏まえて，以下を全て含むセキュリティ要件を定めなければならない。

(ア)クラウドサービスに求める情報セキュリティ対策

(イ)クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(ウ)クラウドサービスに求めるサービスレベル

⑨統括情報セキュリティ責任者は，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，クラウドサービス提供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。

(4) クラウドサービスの利用に係る調達・契約

①情報セキュリティ責任者は，クラウドサービスを調達する場合は，クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

②情報セキュリティ責任者は，クラウドサービスを調達する場合は，クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し，

利用承認を得なければならない。また，調達仕様の内容を契約に含めなければならない。

(5) クラウドサービスの利用承認

①情報セキュリティ責任者は，クラウドサービスを利用する場合には，利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。

②利用申請の許可権限者は，職員等によるクラウドサービスの利用申請を審査し，利用の可否を決定しなければならない。

③利用申請の許可権限者は，クラウドサービスの利用申請を承認した場合は，承認済みクラウドサービスとして記録し，クラウドサービス管理者を指名しなければならない。

(6) クラウドサービスを利用した情報システムの導入・構築時の対策

①統括情報セキュリティ責任者は，クラウドサービスの特性や責任分界点に係る考え方等を踏まえ，以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

（ア）不正なアクセスを防止するためのアクセス制御

（イ）取り扱う情報の機密性保護のための暗号化

（ウ）開発時におけるセキュリティ対策

（エ）設計・設定時の誤りの防止

②クラウドサービス管理者は，情報システムにおいてクラウドサービスを利用する際には，情報システム台帳及び関連文書に記録又は記載しなければならない。なお，情報システム台帳に記録又は記載した場合は，統括情報セキュリティ責任者へ報告しなければならない。

③クラウドサービス管理者は，クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として，クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

（ア）クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

（イ）クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

（ウ）利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

④クラウドサービス管理者は，前項において定める規定に対し，構築時に実施状況を確認・記録しなければならない。

(7) クラウドサービスを利用した情報システムの運用・保守時の対策

①統括情報セキュリティ責任者は，クラウドサービスの特性や責任分界点に係る考え方を踏まえ，以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

（ア）クラウドサービス利用方針の規定

（イ）クラウドサービス利用に必要な教育

（ウ）取り扱う資産の管理

（エ）不正アクセスを防止するためのアクセス制御

（オ）取り扱う情報の機密性保護のための暗号化

（カ）クラウドサービス内の通信の制御

（キ）設計・設定時の誤りの防止

（ク）クラウドサービスを利用した情報システムの事業継続

②クラウドサービス管理者は，クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合，情報システム台帳及び関連文書を更新又は修正しなければならない。なお，情報システム台帳を更新又は修正した場合は，統括情報セキュリティ責任者へ報告しなければならない。

③クラウドサービス管理者は，クラウドサービス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。

④情報セキュリティ責任者は，クラウドサービスの特性や責任分界点に係る考え方を踏まえ，クラウドサービスで発生したインシデントを認知した際の対処手順を整備しなければならない。

⑤クラウドサービス管理者は，前各項において定める規定に対し，運用・保守時に実施状況を定期的に確認・記録しなければならない。

(8) クラウドサービスを利用した情報システムの更改・廃棄時の対策

①統括情報セキュリティ責任者は，クラウドサービスの特性や責任分界点に係る考え方を踏まえ，以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。

（ア）クラウドサービスの利用終了時における対策

（イ）クラウドサービスで取り扱った情報の廃棄

（ウ）クラウドサービスの利用のために作成したアカウントの廃棄

②クラウドサービス管理者は，前項において定める規定に対し，クラウドサービスの利用終了時に実施状況を確認・記録しなければならない。

2　外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱わない場合）

(1) クラウド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，自治体機密性２以上の情報を取り扱わない場合，以下を含むクラウド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。

（ア）クラウドサービスを利用可能な業務の範囲

（イ）クラウドサービスの利用申請の許可権限者と利用手続

（ウ）クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

（エ）クラウドサービスの利用の運用手順

(2) クラウドサービスの利用における対策の実施

①職員等は，利用するサービスの約款，その他の提供条件等から，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自治体機密性２以上の情報を取り扱わない場合のクラウドサービスの利用を申請しなければならない。また，承認時に指名されたクラウドサービス管理者は，当該クラウドサービスの利用において適切な措置を講じなければならない。

②情報セキュリティ責任者は，職員等によるクラウドサービスの利用申請を審査し，利用の可否を決定しなければならない。また，承認したクラウドサービスを記録しなければならない。

第 11 章　情報セキュリティ実施手順の策定

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に基づき，所管するシステム等に対する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情報セキュリティ実施手順を必要に応じて策定させなければならない。

第 12 章　情報セキュリティポリシー等に関する違反に対する対応

1　懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した職員及び会計年度任用職員並びにその監督責任者は，その重大性，発生した事象の状況等に応じて，地方公務員法による懲戒処分の対象となる。

2　再発防止の指導等

情報取扱者に情報セキュリティポリシー及びこれに基づく文書に違反する行為がみられた場合には，情報資産管理責任者は，速やかに次の措置を講じなければならない。

(1) 再発防止の指導その他適切な措置

当該情報取扱者に対して違反する行為の事実を通知し，再発防止の指導その他適切な措置を行う。

(2) 使用権の停止・剥奪

指導等によっても改善されない場合，当該情報取扱者の情報資産の使用権を停止あるいは剥奪する。

(3) 報告

違反する行為が生じた場合，違反する行為の内容，指導内容その他措置の状況について情報セキュリティ責任者に報告する。

第 13 章　評価・改善・見直し

1　監査

(1) 実施方法

最高情報セキュリティ責任者は，情報セキュリティ対策状況について，定期的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

ア　情報システム管理者は，監査を実施する場合には，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。

イ　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) 監査実施計画の策定及び実施への協力

ア　情報システム管理者は，監査を行うにあたって，監査実施計画を策定し，最高情報セキュリティ責任者に報告しなければならない。

イ　被監査部門は，監査の実施に協力しなければならない。

(4) 委託先事業者に対する監査

情報システム管理者は，委託先事業者に対して，委託先事業者からの再委託（再々委託を含む。）の事業者も含めて，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及び必要に応じて行わなければならない。

(5) 監査結果の報告

情報システム管理者は，監査結果を取りまとめ，情報セキュリティ委員会に報告しなければならない。

(6) 監査調書等の保管

情報システム管理者は，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切に保管しなければならない。

(7) 指摘事項への対処

情報システム管理者は，監査結果を踏まえ，指摘事項に関係する情報セキュリティ管理者等に対し，当該事項への対処を指示しなければならない。また，指摘事項に関係しない情報セキュリティ管理者等に対しても，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。

(8) 監査結果の活用

最高情報セキュリティ責任者は，情報セキュリティポリシー等情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

2　自己点検

(1)実施方法

情報セキュリティ責任者及び情報システム管理者は，所管するネットワーク及び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)報告

自己点検の結果報告は，統括情報セキュリティ責任者に報告し，セキュリティ委員会に自己点検結果と改善策を報告しなければならない。

(3)自己点検結果の活用

ア　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。

イ　情報セキュリティ委員会は，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。

3　改善

(1) 是正措置

情報資産管理責任者は，業務上発見された問題，住民からの指摘による問題，監査において指摘された問題等に対する再発防止のため，その原因を除去するための措置を施さなければならない。

(2) 予防措置

情報資産管理責任者は，業務上予見される問題，他の組織で発生したものと同種の情報セキュリティに関する事件・事故等の発生を未然に防止するため，その原因を除去するための措置を施さなければならない。

4　情報セキュリティポリシーの見直し

最高情報セキュリティ責任者は，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，必要があると認めた場合には，情報セキュリティポリシー等情報セキュリティ関連文書の見直しを行う。