鳥取市
情報セキュリティ対策基準

制定　平成１６年４月

改定　令和６年４月

改定履歴

版	改定日	施行日	改定箇所	改定内容
初	平成１６年４月１日	平成１６年４月１日	全章	初版発行
２	平成２５年４月１日	平成２５年４月１日	第２ほか	組織改正
３	平成２８年１月１日	平成２８年１月１日	全章	社会保障・税番号制度導入等に伴う改正
４	平成２８年４月１日	平成２８年４月１日	第２ほか	組織改正
５	平成２９年４月１日	平成２９年４月１日	別表１	組織改正
６	平成３０年６月４日	平成３０年５月１日	第１ほか	組織改正及び外部記録媒体の取扱いの明確化等に伴う改正
７	平成３１年４月１日	平成３１年４月１日	第２ほか	組織改正
８	令和元年１２月２５日	令和元１２月２５日	全章	本庁舎移転及びガイドライン改定等に伴う改定
９	令和２年３月２３日	令和２年４月１日	別表	組織改編に伴う改正
１０	令和６年３月３１日	令和６年４月１日	全章	地方公共団体における情報セキュリティポリシーに関するガイドライン(令和５年３月版)及び生成ＡＩ等外部サービス利用等に伴う改定

目　次

1　総則

1．1　目的

この対策基準は、鳥取市（以下「本市」という。）の情報資産を適正に保護・管理することを目的に、本市情報セキュリティ基本方針（以下「基本方針」という。）を実行に移し、統一的に情報セキュリティ対策を実施するための基準を定めたものである。

1．2　用語の定義

この情報セキュリティ対策基準における用語の定義は、基本方針に定めるもののほか、次の各号の定めるところによる。

⑴　装置　情報システム及びネットワークに関わる機器をいう。

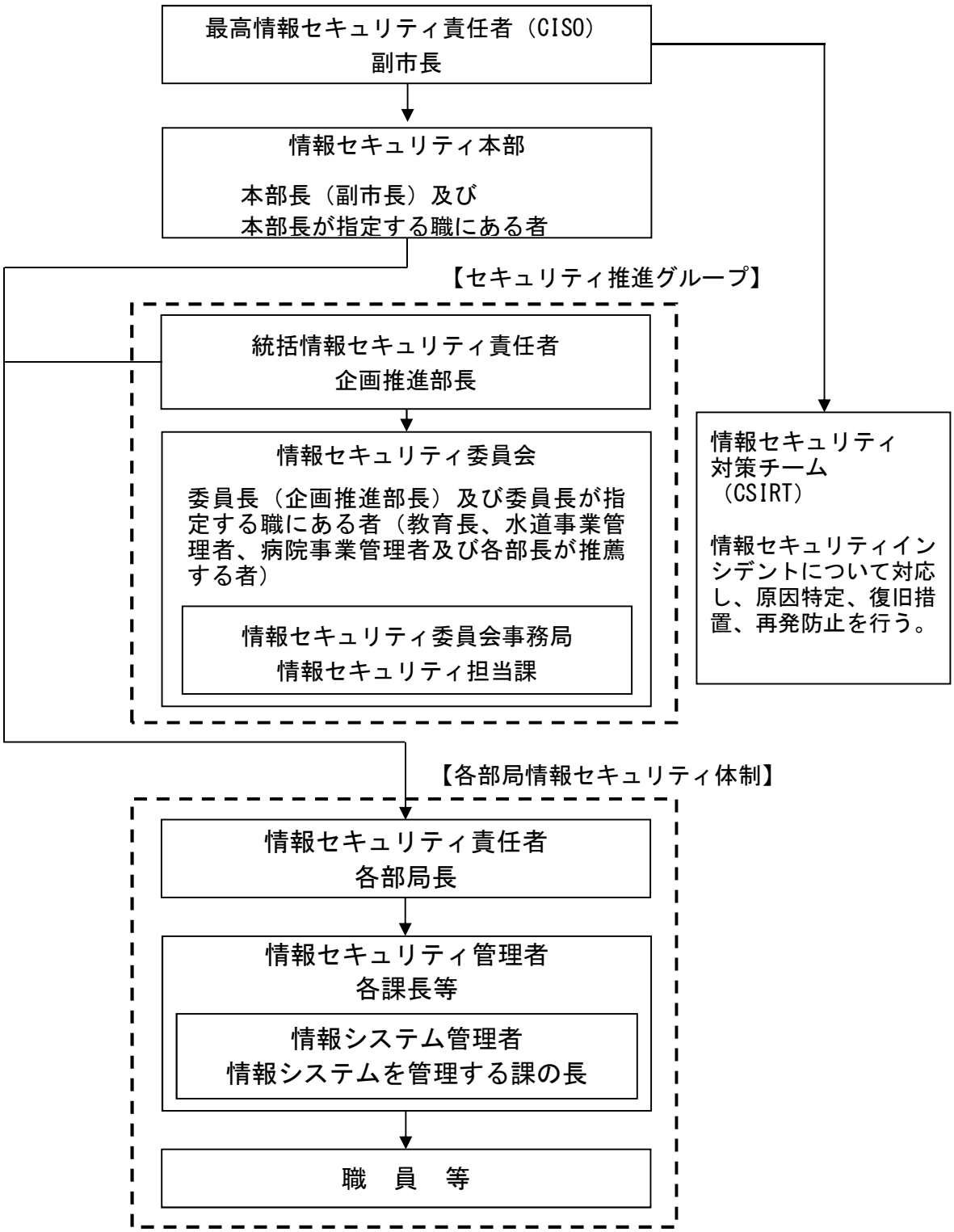
⑵　端末　職員等が、個別に情報システムの情報を処理する装置をいう。

⑶　情報セキュリティインシデント　情報の正常な運営や維持が、セキュリティ上の問題、事故や不正な攻撃等によって妨げられる事象（情報システムの故障、情報漏えい、不正アクセス、不正ソフトウェアの影響等）をいう。

2　組織・体制

2.1　管理体制

本市の情報セキュリティ管理については、下図の情報セキュリティ管理組織に定める組織・体制で推進する。



図：情報セキュリティ管理組織

2.2　役割・責任

⑴　最高情報セキュリティ責任者（CISO：Chief Information Security Officer）

①　CISOは、本市の情報セキュリティを統括する最高責任者とし、副市長をもって充てる。

②　CISOは、情報セキュリティポリシーの範囲でネットワーク、情報システム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　CISOは、情報セキュリティインシデントに対処するため、情報セキュリティ対策チーム（CSIRT：Computer Security Incident Response Team）を整備し、その役割を明確化する。

④　CISOは、CSIRTに所属する職員を選任し、その中からCSIRT責任者を置く。また、CSIRT内の構成、役割及び担当職員を定める。

⑵　情報セキュリティ本部

①　本市の重要なセキュリティ検討事項について審議を行うため、情報セキュリティ本部（以下、「本部」という。）を設置する。

②　本部は、本部長及び本部員をもって組織する。

③　本部長は、CISOをもって充てる。

④　本部員は、CISOが指定する職にある者（別表１）をもって充てる。

⑤　本部会議は、本部長が招集し、本部長が議長となる。

⑥　本部会議の開催は原則年１回とする。ただし、本部長が必要と認めるときは、臨時に会議を開催することができる。

⑶　統括情報セキュリティ責任者

①　情報政策担当部長を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、情報セキュリティポリシーの範囲でネットワークにおける開発、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、情報セキュリティポリシーの範囲でネットワーク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インシデントが発生した場合、又は発生のおそれがある場合、CISOの指示に従い、又は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、情報セキュリティポリシーの範囲でネットワーク、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。

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。

⑨　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CISOにその内容を報告しなければならない。

⑷　情報セキュリティ委員会

①　本市の情報セキュリティに関する事項を審議するため、情報セキュリティ委員会（以下、「委員会」という。）を設置する。

②　委員会は、委員長及び委員をもって組織する。

③　委員長は、統括情報セキュリティ責任者をもって充てる。

④　委員は、委員長が指定する職にある者（教育長、水道事業管理者、病院事業管理者及び各部長等が推薦する者）をもって充てる。

⑤　会議は、委員長が招集し、委員長が議長となる。

⑸　情報セキュリティ委員会事務局

①　情報セキュリティ委員会事務局（以下、「事務局」という。）は、本部及び委員会の庶務を行う。

②　事務局は、情報セキュリティ担当課が行う。

⑹　情報セキュリティ責任者

①　各部局等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、当該部局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、その所管する部局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、その所管する部局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に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行う。

⑺　情報セキュリティ管理者

①　各課室長等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、その所管する課室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CISOへ速やかに報告を行い、指示を仰がなければならない。

⑻　情報システム管理者

①　各情報システムの担当課室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係る情報セキュリティ実施手順の維持・管理を行う。

⑼　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、更新等の作業を行う者を情報システム担当者とする。

⑽　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。

⑾　情報セキュリティ対策チーム（CSIRT）

①　CSIRT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局等より報告を受けた場合には、その状況を確認し、その影響範囲や原因を明確化し、対策及び再発防止策を講じる。

②　CISOによる情報セキュリティインシデントに対する意思決定が行われた際には、その内容を関係各課等に周知する。

③　情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告する。

④　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、必要に応じて報道機関への通知、公表対応を行う。

⑤　情報セキュリティに関して、本部と連携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を有する部署、委託事業者等との情報共有を行う。

⑿　クラウドサービス利用における組織体制

統括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際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築する。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立する。

3　情報資産の分類と管理

3.1　情報資産に対する管理責任

⑴　情報セキュリティ管理者は、各課等内で管理する情報資産の分類を行い、その所在を明らかにして適正に管理しなければならない。

⑵　情報セキュリティ管理者は、機密性３以上の情報資産のリストを整備し、定期的に更新しなければならない。

⑶　情報セキュリティ管理者は、機密性３以上の情報資産のリストを統括情報セキュリティ責任者に提出しなければならない。

3.2　情報資産の分類と管理方法

3.2.1　情報資産の分類

情報セキュリティ管理者は、対象となる情報資産の機密性、完全性、可用性を踏まえ、次の重要性分類基準に従って分類しなければならない。

3.2.2　重要性分類基準

⑴　機密性

４	行政事務で取り扱う情報資産のうち、特に機密性を要するもの ・特定個人情報に関する情報資産
３	行政事務で取り扱う情報資産のうち、機密性を要するもの ・個人情報に関する情報資産 ・法令の規定により秘密を守る義務を課されている情報資産 ・部外に知られることが適当でない法人その他団体に関する情報資産 ・部外に漏れた場合に行政の信頼を著しく害する可能性がある情報資産 ・公開することでセキュリティ侵害が生じる可能性がある情報資産
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３以上には当てはまらないが、広報等は行っていない情報資産
１	機密性２、機密性３又は機密性４以外の情報資産

⑵　完全性

3	行政事務で取り扱う情報資産のうち、特に完全性を要するもの ・改ざん、誤びゅう又は破損が生じると住民の権利が侵害される可能性がある情報資産 ・改ざん、誤びゅう又は破損が生じると行政事務の適確な遂行に著しい支障を及ぼす可能性がある情報資産
2	改ざん、誤びゅう又は破損が生じると行政事務の適確な遂行に支障を及ぼすおそれがある情報資産
1	完全性２又は完全性３以外の情報資産

⑶　可用性

3	行政事務で取り扱う情報資産のうち、特に可用性を要するもの ・利用できないと住民の権利が侵害される可能性がある情報資産 ・利用できないと行政事務の安定的な遂行に著しい支障を及ぼす可能性がある情報資産
2	利用できないと行政事務の安定的な遂行に支障を及ぼすおそれがある情報資産
1	可用性２又は可用性３以外の情報資産

3．2．3　情報資産の管理及び取扱い

⑴　管理責任

①　情報セキュリティ管理者及び情報システム管理者は、それぞれの分類を考慮し、情報システムへのアクセス権限を定めなければならない。

②　情報システム管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

③　職員等は、情報資産が複製又は伝送された場合には、複製物等も分類に基づき管理・取り扱うとともに適正な場所に保管しなければならない。

④　情報セキュリティ管理者は、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）の取扱いを定める。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

⑵　情報の作成

①　職員等は、業務上必要のない情報を作成してはならない。

②　情報を作成する者は、情報の作成時に取扱を定めなければならない。

③　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。

⑶　情報資産の入手

①　職員等は、業務上必要のない情報は入手してはならない。

②　情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

③　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。

⑷　情報資産の利用

①　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

②　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。

③　情報資産を利用する者は、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、当該記録媒体を取り扱わなければならない。

⑸　情報資産の保管

①　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。

②　情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した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。

③　情報セキュリティ管理者又は情報システム管理者は、情報資産の保管を行う場合に、情報資産の完全性を確保するよう努めなければならない。

④　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３以上の情報資産については、定期的にバックアップを実施し、複数の場所で保管しなければならない。

⑤　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３以上、完全性３又は可用性３の情報を記録した記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管することが望ましい。

⑹　情報資産の出力

職員等は、情報資産をプリンター等で必要以上に出力してはならない。また、出力後は、速やかに取り出さなければならない。

⑺　情報資産の運搬

①　車両等により機密性３以上の情報資産を運搬する者は、必要に応じて、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。

②　機密性３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。

⑻　情報資産の提供・公表

①　機密性４の情報資産については、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）及びその他関連する法令の規定で指定する場合以外の提供をしてはならない。

②　機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

③　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に許可を得たうえで、日時、担当者及び提供概要を記録しなければならない。

④　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、完全性を確保するよう努めなければならない。

⑤　市の機関以外の者に提供する場合は、次に掲げる事項をチェックリストなどにより市長と提供先の代表者との間で確認するものとする。

(ア)データの内容に関する事項

(イ)データの利用する業務の根拠法令に関する事項

(ウ)データの利用目的に関する事項

(エ)データの提供方法に関する事項

(オ)データの秘密の保持に 関する事項

(カ)データの目的外の 利用 及び第三者への提供の禁止に関する事項

(キ)データの複写及び複製の禁止に関する事項

(ク)データの取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

(ケ)データの返還又は廃棄が必要な場合にあっては、データの返還又は廃棄に関する事項

(コ)データの利利用又は管理の状況の実地による調査等が必要な場合にあっては、当該調査の実施に関する事項

⑼　情報資産の廃棄等

①　情報システム管理者は、機密性２以上の情報資産（情報システム、装置、端末及び記録媒体等）の廃棄又はリース返却（以下「情報資産の廃棄等」という。）をするときは、事前に情報セキュリティ担当課と協議を行い、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、機密性２以上の情報資産の廃棄等をするときは、当該情報資産の物理的な破壊又は磁気的な破壊等により確実に情報の復元ができないように処置（以下「復元不可能処置」という。）したうえで廃棄又は返却をしなければならない。

③　情報システム管理者は、復元不可能処置の日時、担当者及び処理内容等を廃棄資産管理簿等に記録し、保管しなければならない。

④　情報システム管理者は、機密性２以上の情報資産の廃棄を委託業者に委託する場合、復元不可能処置に職員が立ち会いするなど確実な履行を確認しなければならない。

⑤　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、消去の記録を得なければならない。

4　情報システム全体の強靭化の向上

4．1　住民情報系ネットワーク

⑴　住民情報系と他の領域との分離

住民情報系と他の領域を原則通信できないようにしなければならない。

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

⑵　情報のアクセス及び持ち出しにおける対策

①　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。

②　情報の持ち出し不可設定原則として、USB メモリ等の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。

⑶　住民情報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扱い

住民情報系の端末・サーバ等と専用回線により接続されるクラウド上の情報システムの領域については、住民情報系として扱い、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。

⑷　住民情報系と接続されるクラウドサービス上での情報資産の取扱い

住民情報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、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又は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暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、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。

4．2　LGWAN 系ネットワーク

⑴　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。

①　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

② 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

③ 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

⑵ LGWAN接続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扱い

LGWAN接続系の情報システムをクラウドサービス上へ配置する場合は、その領域をLGWAN 接続系として扱い、住民情報系とネットワークを分離し、専用回線を用いて接続しなければならない。

4.3 インターネット系ネットワーク

⑴ 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。

⑵ 都道府県及び市区町村のインターネットとの通信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。

5 物理的セキュリティ

5.1 装置の管理

5.1.1 装置の設置及び保護

情報システム管理者は、サーバ等の装置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。

5.1.2 サーバの冗長化

⑴ 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サーバを冗長化し、同一データを保持することが望ましい。

⑵ 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小限にすることが望ましい。

5.1.3 装置の電源管理

⑴ 情報システム管理者は、重要なサーバ等の装置を停電等の電源異常から保護するため、無停電電源装置や自家発電装置等を設置するとい

った対策を実施しなければならない。

⑵　情報システム管理者は、落雷等による過電流から、サーバ等の装置を保護するための対策を実施しなければならない。

⑶　可用性３の情報システムを保有する情報システム管理者は、装置の仕様に適合した適切な電力を供給する予備電源を確保しなければならない。また、予備電源が給電可能な時間、燃料等について、定期的に点検、確認を行わなければならない。

5.1.4　配線の管理

⑴　情報システム管理者は、配線・電源ケーブル等を損傷や認められない変更等の脅威から保護し、設置しなければならない。

⑵　情報システム管理者は、主要な箇所の配線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。

5.1.5　装置の定期保守及び修理

⑴　情報システム管理者は、可用性２以上のサーバ等の装置の定期保守を実施しなければならない。

⑵　情報システム管理者は、記録媒体を内蔵する装置を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、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等を行わなければならない。

5.1.6　庁外への装置の設置

情報システム管理者は、庁外にサーバ等の装置を設置する場合、統括情報セキュリティ責任者の承認を得なければならない。また、定期的に当該装置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。

5.1.7　機器の廃棄等

⑴　情報システム管理者は、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、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。

⑵　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）をする者は、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できる。

5．2　区画の管理

5．2．1　区画の分類

統括情報セキュリティ責任者は、庁舎内を区画分類の定義に沿って分類しなければならない。また、必要に応じて新たに区画を設置しなければならない。

5．2．2　区画分類の定義

⑴　高セキュリティ区画

・ネットワークの基幹装置及び重要な情報システムを安全に設置・保護するために、高いセキュリティレベルを保つ区画

・統括情報セキュリティ責任者が許可した者のみが立入りできる区画

⑵　一般セキュリティ区画

・情報システムを利用する事務区画のうち、情報セキュリティ管理者に許可された者のみが立入りできる区画

・第三者の立入りができない区画

⑶　公開区画

・第三者の立入りが可能な区画

5．2．3　高セキュリティ区画の管理

⑴　高セキュリティ区画の物理的管理

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、高セキュリティ区画に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。

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、高セキュリティ区画に耐震対策、防火装置、防水措置等を講じなければならない。

③　高セキュリティ区画に危険物や不要な可燃物の保管をしてはならない。

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、消火剤や消防用設備等が装置等及び記録媒体に影響を与えないようにしなければならない。

⑵　高セキュリティ区画の入退室管理等

①　情報システム管理者は、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による入退室管理を行わなければならない。

②　情報システム管理者は、扉等の施錠を管理しなければならない。

③　職員等及び委託事業者は、高セキュリティ区間に入室する場合、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。
④　委託業者等は、高セキュリティ区間に入る場合、事前に作業内容、作業員名、作業日時等が記載された申請書を提出しなければならない。
⑤　情報システム管理者は、委託業者等が高セキュリティ区画に入る場合、必要に応じて立ち入り区域を制限したうえで、入退室を許可された職員等を立ち会わせなければならない。
⑥　情報システム管理者は、高セキュリティ区間に当該情報システムに関連しない、又は個人所有である端末、装置、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。

5.2.4　一般セキュリティ区画の管理

⑴　一般セキュリティ区画の入退室管理等

①　情報セキュリティ管理者は、一般セキュリティ区画に許可されない者が立ち入りできないようにしなければならない。
②　情報セキュリティ管理者は、扉、書庫等の施錠管理をしなければならない。
③　職員等及び委託事業者は、一般セキュリティ区画に入室する場合、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。
④　委託業者等は、一般セキュリティ区間に入る場合、事前に作業内容、作業員名、作業日時等が記載された申請書を提出しなければならない。
⑤　情報システム管理者は、委託業者等が一般セキュリティ区画に入る場合、必要に応じて立ち入り区域を制限したうえで、入退室を許可された職員等を立ち会わせなければならない。

5.2.5　装置等の搬入出

⑴　情報システム管理者は、搬入する装置等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託した業者に確認を行わせなければならない。
⑵　情報システム管理者は、区画への装置の搬入出について、職員を立ち会わせなければならない。

5.3　通信回線及び通信回線装置の管理

⑴　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。

⑵　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。

⑶　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。

⑷　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総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

⑸　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うえ、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。

⑹　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、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

⑺　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関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

⑻　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るよう努めなければならない。

5．4　職員等の利用する端末や記録媒体等の管理

5．4．1　端末等の管理

⑴　情報セキュリティ管理者は、盗難や紛失防止のため、執務室等で利用する端末及び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。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。

⑵　情報システム管理者は、端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、記録媒体についても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。

⑶　情報システム管理者は、住民情報系では「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認証（多要素認証）を行うよう設定しなければならない。

⑷　職員等は、端末を使用する場合には、庁内 LAN 端末安全管理規定（仮）に基づき、安全な使用に努めなければならない。

5．4．2　記録媒体等の管理

⑴　情報セキュリティ管理者は、記録媒体を利用する場合、公用として登録台帳に登録をしなければならない。また、利用を停止する場合、登録抹消の記録をしなければならない。

⑵　職員等は、記録媒体を使用する場合、使用日時、使用者及び使用目的等を使用台帳に記録し、情報セキュリティ管理者の許可を得なければならない。また、使用が終了した場合、使用台帳に記録し、情報セキュリティ管理者の確認を受けなければならない。

⑶　機密性３以上の情報資産を移動又は保存する記録媒体については、暗号化やウイルス対策の措置が講じられる機器を使用しなければならない。

⑷　情報セキュリティ管理者は、記録媒体を送付する場合、複製の禁止及び記録媒体の物理的保護について規定し、事故等が発生した際の対応策を定めなければならない。

6　人的セキュリティ

6．1　職員等の遵守事項

6.1.1　職員等の遵守事項

⑴　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実施手順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、指示を仰がなくてはならない。

⑵　業務以外の目的での情報資産の使用の禁止

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。

⑶　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発見した場合は、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。

⑷　無許可でのネットワーク接続の禁止

職員等は、情報システム管理者の許可なく端末をネットワークに接続してはならない。

⑸　電子メールの利用制限

①　職員等は、電子メールで機密性３以上の情報資産を送信してはならない。

②　職員等は、電子メールで情報資産を送信する場合は、暗号化を行い、暗号鍵を同時に送信してはならない。

③　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。

④　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。

⑤　職員等は、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、速やかに削除しなければならない。

⑥　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（ＢＣＣを使用）しなければならない。

⑦　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。

⑧　職員等は、業務以外の目的で、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使用してはならない。

⑹　無許可ソフトウェアの導入等の禁止

①　職員等は、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。

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。

⑺　情報資産（端末、記録媒体等）の持ち出し及び外部における情報処理作業の制限

①　CISO は、機密性２以上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。

②　職員等は、機密性２以上の情報資産（端末、記録媒体及びソフトウェア等）を外部に持ち出す場合には、情報セキュリティ責任者の許可を得なければならない。ただし、情報セキュリティ責任者が不在の場合は、情報セキュリティ管理者が代理として許可を行い、別途改めて情報セキュリティ責任者へ報告することとする。

③　職員等は、外部で情報処理業務を行う場合には、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　職員等は、端末を外部で使用する場合には、庁内 LAN パソコン利用要領に基づき、安全な使用に努めなければならない。

⑻　支給以外の端末及び記録媒体等の業務利用

職員等は、公用以外の端末及び記録媒体等を業務に使用してはならない。ただし、業務上必要な場合は、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。

⑼　持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等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。

⑽　端末の適正管理

①　職員等は、庁内 LAN パソコン利用要領に基づき、使用している端末が常に良好な状態で稼働できるよう適正に管理しなければならない。

②　職員等は、端末に影響を及ぼす機器等を利用してはならない。

⑾　端末におけるセキュリティ設定変更の禁止

職員等は、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セキュリティ管理者の許可なく変更してはならない。

⑿　端末構成の変更の制限

①　職員等は、端末の改造及び増設・交換を行ってはならない。

②　職員等は、業務上、端末の改造及び増設・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。

⑬　机上等の管理

①　職員等は、長時間の離席時や帰宅時において、機密性２以上の情報資産を机上等に放置してはならない。

②　職員等は、長時間の離席時や帰宅時において、機密性３以上の情報資産を施錠可能な収納庫等に保管しなければならない。

⑭　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。

⑮　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。

6.1.2　情報セキュリティポリシー等の周知

情報セキュリティ管理者は、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閲覧できるようにしなければならない。

6.1.3　委託事業者に対する説明

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開発・保守等を外部委託事業者に発注する場合、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。

6.2　研修・訓練

⑴　情報セキュリティに関する研修・訓練

CISOは、職員等及び関係する者に対し情報セキュリティに関する勉強会、研修、訓練等を定期的に実施しなければならない。

⑵　研修計画の策定及び実施

①　CISO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、情報セキュリティ本部の承認を得なければならない。

②　研修計画において、職員等は毎年度最低１回、情報セキュリティ研修を受講できるようにしなければならない。

③　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。

④　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。

⑤　情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、統括情報セキュリティ責任者及び情報セキュリティ責任者に対して、報告しなければならない。

⑥　統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、CISOに情報セキュリティ対策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。

⑦　CISOは、毎年度１回、情報セキュリティ本部に対して、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。

⑶　研修・訓練等への参加

職員等は、情報セキュリティに関する定められた研修等に参加し、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。

6.3　情報セキュリティインシデントの報告

⑴　庁内での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、速やかに情報システム管理者及び情報セキュリティ責任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及びCISOに報告しなければならない。

⑵　住民等外部からの情報セキュリティインシデントの報告

①　職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者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、速やかに情報システム管理者及び情報セキュリティ責任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及びCISOに報告しなければならない。

⑶　情報セキュリティインシデントの報告内容

情報管理者等から情報セキュリティ管理者への報告は、以下の内容を含むものとする。

①件名、②判明した日時、③発生した日時、④発見者、⑤対応者、⑥事件事故等の内容、⑦漏えいした情報、⑧予想される影響、⑨想定される原因、⑩事件事故等への対応、⑪復旧方針

⑷　情報セキュリティインシデント原因の究明・記録、再発防止等

①　CSIRT 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。

②　CSIRT 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、CISO に速やかに報告しなければならない。

③　CSIRT 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。また、CSIRT は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。

④　CSIRT は、これらの情報セキュリティインシデント原因を究明し、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。

⑤　CISO 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。

6.4　ＩＤ及びパスワード等の管理

6.4.1　ＩＣカード等の取扱い

⑴　職員等は、自己の管理するＩＣカード等に関し、次の事項を遵守しなければならない。

①　認証に用いるＩＣカード等を、職員等間で共有してはならない。

②　業務上必要のないときは、ＩＣカード等をカードリーダ又は端末のスロット等から抜いておかなければならない。

③　ＩＣカード等を紛失した場合には、速やかに情報システム管理者に通報し、指示に従わなければならない。

⑵　情報システム管理者は、ＩＣカード等の紛失等の通報があり次第、当該ＩＣカード等を使用したアクセス等を速やかに停止しなければならない。

⑶　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うえで廃棄しなければならない。

6.4.2　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。

6.4.3 パスワードの取扱い

⑴ 情報システム管理者は、職員等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。

① 職員等のパスワードの割り当て・管理についての手順を定め、パスワード情報を厳重に管理しなくてはならない。

② 職員等へのパスワード発行時に、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るようにしなければならない。

⑵ 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おそれがある場合には、情報システム管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

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

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

⑦ サーバ、ネットワーク装置及び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（ただし共有アカウントに対するパスワードは除く）。

7　技術的セキュリティ

7．1　情報システムの管理

7．1．1　部門フォルダの設定等

⑴　情報システム管理者は、職員等が使用できる部門フォルダの容量を設定し、職員等に周知しなければならない。

⑵　情報システム管理者は、部門フォルダを課室等の単位で構成し、職員等が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に、設定しなければならない。

⑶　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、同一課室等であっても、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。

7．1．2　情報システムの入出力データ

⑴　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の完全性を確保しなければならない。

⑵　情報システム管理者は、情報システムで処理されたデータに対して、エラー又は故意の行為により情報資産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。

⑶　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の完全性を確保しなければならない。

7．1．3　バックアップ及び二重化

⑴　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、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施し、一定の期間保存しなければならない。特に、完全性３の情報資産については、バックアップを適宜実施しなければならない。

⑵　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、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。

⑶　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、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管することが望ましい。

⑷　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、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなけ

ればならない。また、その機能の仕様が本市の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

7.1.4　他の団体との情報システムに関する情報等の交換

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情報及びソフトウェアを交換する場合、必要に応じてその取扱いに関する事項をあらかじめ定めなければならない。

7.1.5　システム管理記録及び作業の確認

⑴　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。

⑵　情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

⑶　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することが望ましい。

7.1.6　情報システム仕様書等の管理

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、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

7.1.7　ログの取得等

⑴　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。

⑵　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。

⑶　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。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認できることが望ましい。

⑷　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、監査及びデジタルフォレンジック（事実解明及び証拠保存のために必要となる電子データの調査分析）に必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

7.1.8　障害記録

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。

7.1.9　ネットワークの接続制御、経路制御等

⑴　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、ルータ等の通信ソフトウェア等を設定しなければならない。

⑵　情報システム管理者は、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。

⑶　統括情報セキュリティ責任者は、保守又は診断のために、（本市専用の回線を準備するなど）外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保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、定期的な確認により見直さなければならない。

7.1.10　外部の者が利用できるシステムの分離等

⑴　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、必要に応じ他のネットワーク及び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。

⑵　情報システム管理者は、電子申請等の個人情報を取扱うシステムをインターネット上に公開する場合は、不正行為及び情報資産の漏えい、改ざん等の脅威から保護する対策等を講じなければならない。特に厳密な本人確認が必要な申請については、公的個人認証等など、不

正防止の対策を講じなければならない。

⑶　情報システム管理者は、外部の者が利用できるシステムについては、完全性を確保するために、定期的にアクセスログの記録を行わなければならない。

7.1.11　外部ネットワークとの接続制限等

⑴　情報システム管理者は、外部ネットワーク（遠隔保守通信回線等を含む）と接続する際に、情報セキュリティ上の問題が発生しないことを確認し、鳥取市電子計算組織管理運営規程に基づいて接続しなければならない。

⑵　情報システム管理者は、外部へのネットワーク接続は必要最小限とし、できる限り接続ポイントを減らさなければならない。

⑶　情報システム管理者は、外部ネットワークと接続する際には、当該ネットワーク管理組織と情報セキュリティ上適切な契約又は取り決めを結ばなければならない。

⑷　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、次のセキュリティ対策を実施しなければならない。

①　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。

②　脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。

③　職員等のパスワードの割り当て・管理についての手順を定め、パスワード情報を厳重に管理しなくてはならない。

④　職員等へのパスワード発行時に、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るようにしなければならない。

⑸　情報システム管理者は、接続した外部ネットワークにセキュリティ上の問題が発生した際には、統括情報セキュリティ責任者の判断に従い、速やかに当該ネットワークとの接続を物理的に遮断しなければならない。

7.1.12　複合機のセキュリティ管理

⑴　情報セキュリティ管理者は、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。

⑵　情報セキュリティ管理者は、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。

⑶　情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ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。

7.1.13　特定用途装置のセキュリティ管理

情報システム管理者は、特定用途装置について、取扱う情報、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、当該装置の特性に応じた対策を講じなければならない。

7.1.14　無線ＬＡＮ及びネットワークの盗聴対策

⑴　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。

⑵　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。

7.1.15　電子メールのセキュリティ管理

⑴　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。

⑵　統括情報セキュリティ責任者は、スパムメール等の受信又は送信を検知した場合は、メールサーバ運用停止等の措置を講じなければならない。

⑶　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。

⑷　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。

⑸　統括情報セキュリティ責任者は、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事業者の作業員による電子メールアドレス利用について、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。

⑹　統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出したことが分かるように添付ファイルの監視等によりシステム上措置を講じなければならない。

7.1.16　電子メールの利用制限

⑴　職員等は、自動転送機能を用いて、許可なく電子メールを転送してはならない。

⑵　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。

⑶　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。

⑷　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。

7.1.17　電子署名・暗号化

⑴　職員等は、情報資産の分類に従い、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、電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

⑵　情報システム管理者は、必要に応じて情報資産を暗号化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資産は、別々に適切な管理を実施しなければならない。

7.1.18　無許可ソフトウェアの導入等の禁止

⑴　職員等は、端末に無断でソフトウェアを導入してはならない。

⑵　職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者の許可を得て、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。

⑶　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。

7.1.19　機器構成の変更の制限

⑴　職員等は、端末に対し改造及び増設・交換を行ってはならない。

⑵　職員等は、業務上、端末の改造及び増設・交換を行う必要がある場合には、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。

7.1.20　業務外ネットワークへの接続の禁止

⑴　職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

⑵　情報セキュリティ管理者は、支給した端末について、端末に搭載されたOSのポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

7.1.21　業務以外の目的でのウェブ閲覧の禁止

⑴　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。

⑵　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発見した場合は、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。

7.1.22　Web会議サービスの利用時の対策

⑴　統括情報セキュリティ責任者は、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。

⑵　職員等は、本市の定める利用手順に従い、Web会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

⑶　職員等は、Web会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

7.1.23　ソーシャルメディアサービスの利用

⑴　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。

①　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。

②　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の方法で、不正アクセス対策を実施すること。

⑵　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。

⑶　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。

⑷　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。

⑸　可用性２以上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すること。

7.2　アクセス制御

7.2.1　アクセス制御等

⑴　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、必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

⑵　利用者ＩＤの取扱い

①　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、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

②　情報システム管理者は、利用者ＩＤが重複せず、正確であることを確実にしなければならない。

③　情報セキュリティ管理者は、異動や退職等により職員の利用者ＩＤが不要になった場合は、情報システム管理者に速やかに報告しなければならない。

④　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、人事担当課と連携し、点検しなければならない。

⑤　情報システム管理者は、利用停止したＩＤの保存年数を定めなければならない。

⑥　情報システム管理者は、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。

⑶　特権管理

①　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。

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、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。

③　情報システム管理者の特権を代行する者は、情報システム管理者が指名した者でなければならない。

④　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、委託事業者に行わせてはならない。

⑤　情報システム管理者は、特権ＩＤを割り当てる際、通常の利用者ＩＤとは異なるＩＤとして割り当てなければならない。

⑥　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。

7.2.2　職員等による外部からのアクセス等の制限

⑴　職員等が外部から内部のネットワーク又は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当該情報システムを管理する情報システム管理者の許可を得なければならない。

⑵　情報システム管理者は、内部のネットワーク又は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。

⑶　情報システム管理者は、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。

⑷　情報システム管理者は、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。

⑸　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。

⑹　統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、止むを得ず接続を許可する場合は、利用者の ID、パスワードによる認証に加えて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。

7.2.3　自動識別の設定

情報システム管理者は、ネットワークで使用される装置について、装置固有情報によって端末とネットワークとの接続の可否が自動的に識別されるシステムを設定するよう努めなければならない。

7.2.4　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。

7.2.5　認証情報の管理

⑴　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。

⑵　情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回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。

⑶　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。

7.2.6　特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続を必要最小限に制限しなければならない。

7.3　システム開発、導入、保守等

7.3.1　機器等及び情報システムの調達

⑴　情報セキュリティ管理者は、情報システムの開発・導入・変更・廃棄についての管理手順及びセキュリティ要求事項を明確にしなければならない。

⑵　情報システム管理者は、装置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。

⑶　情報システム管理者は、将来情報システムに必要な処理能力や記録容量を予測し、導入又は変更時に反映しなければならない。

7.3.2　情報システムの開発

⑴　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。

⑵　システム開発における責任者、作業者のＩＤの管理

①　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。

② 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。

⑶ 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

① 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。

② 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。

⑷ アプリケーション・コンテンツの開発時の対策

情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

7.3.3 情報システムの導入

⑴ 開発環境と運用環境の分離及び移行手順の明確化

① 情報システム管理者は、新たに情報システムを導入する際、鳥取市電子計算組織管理運営規程に基づいて実施しなければならない。

② 情報システム管理者は、システム開発、保守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。

③ 情報システム管理者は、システム開発・保守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・保守計画の策定時に手順を明確にしなければならない。

④ 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。

⑤ 情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認したうえで導入しなければならない。

⑵ テスト

① 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試験を行わなければならない。

② 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。

③ 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。

④　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が、それぞれ独立したテストを行わなければならない。

⑤　情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

⑶　機器等の納入時又は情報システムの受入れ時

①　情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

②　情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

7.3.4　システム開発・保守に関連する資料等の整備・保管

⑴　情報システム管理者は、システム開発・保守に関連する資料及び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。

①　情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について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。

②　情報システム管理者は、所管する情報システム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、以下を全て含む情報システム関連文書を整備することが望ましい。

・情報システムを構成するサーバ装置及び端末関連情報

・情報システムを構成する通信回線及び通信回線装置関連情報

③　情報システム管理者は、所管する情報システム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、以下を全て含む実施手順を整備しなければならない。

・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

・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

・情報システムが停止した際の復旧手順

⑵　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。

7.3.5　情報システムにおける入出力データの正確性の確保

⑴　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。

⑵　情報システム管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

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

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

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

7.3.6　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。

7.3.7　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等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。

7.3.8　システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時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。

7.4　不正プログラム対策

7.4.1　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。

⑴　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。

⑵　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。

⑶　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。

⑷　所掌する装置及び端末等に、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。

⑸　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。

⑹　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。

⑺　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原則利用してはならない。

⑻　仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

7．4．2　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。

⑴　情報システム管理者は、その所掌する装置及び端末等に、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システムに常駐させなければならない。

⑵　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。

⑶　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。

⑷　インターネットに接続していないシステムにおいて、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、本市が管理している媒体以外を職員等に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。

⑸　不正プログラム対策ソフトウェア等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を除く職員等に当該権限を付与してはならない。

7.4.3　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。

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

7.5　不正アクセス対策

7.5.1　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。

⑴　使用されていないポートを閉鎖しなければならない。

⑵　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。

⑶　不具合に対する修正プログラムの導入、又はソフトウェアの更新等について、全庁的に速やかに対応しなければならない。

⑷　不正アクセスによるウェブページの改ざんを防止する措置を講じなければならない。

⑸　統括情報セキュリティ責任者は、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。

⑹　本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

⑺　クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせることが望ましい。

⑻　パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認することが望ましい。

7.5.2　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。

7.5.3　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禁止法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。

7.5.4　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、職員等及び委託事業者が使用している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。

7.5.5　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発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

7.5.6　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。

7.5.7　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、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、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。

7.6　セキュリティ情報の収集

⑴　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

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、サーバ装置、端末及び通信回線装置等における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　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、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有するデータへの影響について特定する。影響が大きいものと判断される場合、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

⑵　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。

⑶　情報セキュリティに関する情報の収集及び共有

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。

8　運用

8.1　情報システムの監視

8.1.1　情報システムの運用・保守時の対策

⑴　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　システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

⑵　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。

⑶　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、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

8.1.2　情報システムの監視機能

⑴　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、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

⑵　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、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

⑶　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、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

⑷　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、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

8.1.3　情報システムの監視

⑴　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。

⑵　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、監視記録を適正に保管しなければならない。

⑶　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。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

⑷　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。

⑸　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、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

⑹　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、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討することが望ましい。

⑺　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、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

①　サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

②　クラウドサービス利用の終了手順

③　バックアップ及び復旧

8.2　情報セキュリティポリシーの遵守状況の確認

8.2.1　遵守状況の確認及び対処

⑴　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。

⑵　CISOは、発生した問題について、適正かつ速やかに対処しなければならない。

⑶　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。

8.2.2　端末及び記録媒体等の利用状況調査

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端末及び記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

8.2.3　職員等の報告義務

⑴　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に報告を行わなければならない。

⑵　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。

8.3　侵害時の対応等

8.3.1　緊急時対応計画の策定

⑴　CISO 又は情報セキュリティ委員会は、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。

⑵　CISO 又は情報セキュリティ委員会は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した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することが望ましい。

8.3.2　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

8.3.3　業務継続計画との整合性確保

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該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。

8.3.4　緊急時対応計画の見直し

CISO 又は情報セキュリティ委員会は、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の規

定を見直さなければならない。

8．4　例外措置

8．4．1　例外措置の許可

情報セキュリティ管理者及び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。

8．4．2　緊急時の例外措置

情報セキュリティ管理者及び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。

8．4．3　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。

8．5　法令遵守

⑴　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（平成 11 年法律第 128 号)

④　個人情報の保護に関する法律（平成 15 年法律第 57 号)

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

⑥　サイバーセキュリティ基本法（平成 28 年法律第 31 号)

⑦　鳥取市個人情報の保護に関する法律施行条例（令和５年鳥取市条例第 36 号)

⑵　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、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

8．6　懲戒処分等

8.6.1　懲戒処分

情報セキュリティポリシーや関係法令等に違反した職員等は、地方公務員法に基づき、懲戒処分等の対象とする場合がある。また、市が所有する情報資産を侵害した者に対し、その重大性、発生した事案の状況に応じて生じた損害を求償することができる。

8.6.2　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。

⑴　統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室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。

⑵　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通知し、当該職員等に適正な措置を求めなければならない。

⑶　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、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、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室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。

⑷　違反により、本市に損害が生じた場合、違反した職員等に対して、生じた損害を求償することができる。

9　業務委託と外部サービス（クラウドサービス）の利用

9.1　業務委託

9.1.1　業務委託に係る運用規程の整備

⑴　情報セキュリティ管理者は、業務委託に係る以下の内容を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

9.1.2　業務委託実施前の対策

⑴　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、以下の事項を実施しなければならない。

①　委託する業務内容の特定

②　委託事業者の選定条件を含む仕様の策定

③　仕様に基づく委託事業者の選定

④　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り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「システム委託先情報セキュリティ実施状況チェックリスト（外部サービスの利用を含む情報処理業務）（様式第１号)」に記す情報セキュリティ等に係る要件を確認したうえで、契約を締結しなければならない。

9.1.3　業務委託実施期間中の対策

⑴　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、以下の対策を実施しなければならない。

①　委託判断基準に従った重要情報の提供

②　契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

②　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

⑵　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、以下の対策の実施を委託事業者に求めなければならない。

①　情報の適正な取扱いのための情報セキュリティ対策

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

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

9.1.4　業務委託終了時の対策

⑴　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、以下の対策を実施しなければならない。

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

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

⑵　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、以下の対策の実施を委託事業者に求めなければならない。

① 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
② 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

9.1.5 再委託等

再委託（再々委託を含む。以下同様 ）を受ける事業者がある場合、以下（9.2、9.3）に定める事項は再委託を受ける事業者にも適用する。

9.2 情報システムに関する業務委託

9.2.1 情報システムに関する業務委託における共通的対策

情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

9.2.2 情報システムの構築を業務委託する場合の対策

情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めることが望ましい。

⑴ 情報システムのセキュリティ要件の適切な実装
⑵ 情報セキュリティの観点に基づく試験の実施
⑶ 情報システムの開発環境及び開発工程における情報セキュリティ対策

9.2.3 情報システムの運用・保守を業務委託する場合の対策

⑴ 情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。
⑵ 情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

9.2.4 本市向けに情報システムの一部の機能を提供するサービスを利用する

場合の対策

⑴　情報システム管理者又は情報セキュリティ管理者は、外部の一般の者が本市向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えることが望ましい。

⑵　情報システム管理者又は情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

⑶　情報システム管理者又は情報セキュリティ管理者は、委託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。

⑷　情報システム管理者又は情報セキュリティ管理者は業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行わなければならない。

⑸　情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

9．3　外部サービス（クラウドサービス）の利用（機密性２以上の情報を取り扱う場合）

9．3．1　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、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することが望ましい。

⑴　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。）

⑵　クラウドサービス提供者の選定基準

⑶　クラウドサービスの利用申請の許可権限者と利用手続

⑷　情報システム管理者の指名とクラウドサービスの利用状況の管理

9．3．2　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、機密性２以上の情報を取り扱う場合、以下を含むクラウドサービス（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することが望ましい。

⑴　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手順として整備することが望ましい。

9.3.3　クラウドサービスの選定

⑴　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。

⑵　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ることが望ましい。

①　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

②　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

③　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

④　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

⑤　情報セキュリティインシデントへの対処方法

⑥　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

⑦　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

⑶　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ることが望ましい。

⑷　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ることが望ましい。

①　情報セキュリティ監査の受入れ

②　サービスレベルの保証

⑸　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ることが望ましい。

⑹　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。

⑺　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ることが望ましい。

①　クラウドサービスに求める情報セキュリティ対策

②　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

③　クラウドサービスに求めるサービスレベル

⑻　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。

9.3.4　クラウドサービスの利用に係る調達・契約

⑴　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。

⑵　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。

9.3.5　クラウドサービスの利用承認

⑴　情報システム管理者は、クラウドサービスを利用する場合には、統括情報セキュリティ責任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。

⑵　統括情報セキュリティ責任者は、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。

9．3．6　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

⑴　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。

①　不正なアクセスを防止するためのアクセス制御

②　取り扱う情報の機密性保護のための暗号化

③　開発時におけるセキュリティ対策

④　設計・設定時の誤りの防止

⑵　情報システム管理者は、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する場合は、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。

⑶　情報システム管理者は、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。

①　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

②　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

③　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

⑷　情報システム管理者は、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。

9．3．7　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

⑴　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。

①　クラウドサービス利用方針の規定

②　クラウドサービス利用に必要な教育

③　取り扱う資産の管理
④　不正アクセスを防止するためのアクセス制御
⑤　取り扱う情報の機密性保護のための暗号化
⑥　クラウドサービス内の通信の制御
⑦　設計・設定時の誤りの防止
⑧　クラウドサービスを利用した情報システムの事業継続

⑵　情報システム管理者は、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。

⑶　情報システム管理者は、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。

⑷　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。

⑸　情報システム管理者は、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。

9．3．8　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

⑴　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。
①　クラウドサービスの利用終了時における対策
②　クラウドサービスで取り扱った情報の廃棄
③　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

⑵　情報システム管理者は、前項において定める規定に対し、外部サービス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。

9．4　外部サービス（クラウドサービス）の利用（機密性２以上の情報を取り扱わない場合）

9．4．1　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、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（機密性２以上の情報を取り扱わない場合）の利用に関する運用管理規定を整備しなければならない。
①　クラウドサービスを利用可能な業務の範囲

② クラウドサービスの利用申請の許可権限者と利用手続
③ 情報システム管理者の指名とクラウドサービスの利用状況の管理
④ クラウドサービスの利用の運用管理手順

9.4.2 クラウドサービスの利用における対策の実施

⑴ 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機密性２以上の情報を取り扱わない場合の外部サービス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情報システム管理者は、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ずること。

⑵ 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こと。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。

１０ 評価・見直し

10.1 監査

10.1.1 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、ネットワーク及び情報システム等の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。

10.1.2 監査を行う者の要件

⑴ 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、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。

⑵ 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。

10.1.3 監査実施計画の立案及び実施への協力

⑴ 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、原則として監査計画に基づいて実施しなければならない。

⑵ 被監査部門は、監査の実施に協力しなければならない。

10.1.4 委託事業者に対する監査

⑴ 事業者に業務委託している場合、情報セキュリティ監査統括責任者は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の監査を必要に応じて行わなければならない。

⑵　クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

10.1.5　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、CISOに報告しなければならない。

10.1.6　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。

10.1.7　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。

10.1.8　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定等の見直し、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。

10.2　自己点検

10.2.1　実施方法

統括情報セキュリティ責任者は、情報セキュリティ管理者及び情報システム管理者と連携して、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。

10.2.2　報告

統括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、CISO に報告しなければならない。

10.2.3　自己点検結果の活用

⑴　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。

⑵　CISO 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。

10.3　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。

別表１：情報セキュリティ本部構成員

役職名	備　考
本部長	副市長
本部員	教育長
〃	水道事業管理者
〃	病院事業管理者
〃	総務部長
〃	税務・債権管理局長
〃	人権政策局長
〃	危機管理部長
〃	企画推進部長
〃	経営統括監
〃	市民生活部長
〃	環境局長
〃	福祉部長
〃	健康こども部長
〃	こども家庭局長
〃	鳥取市保健所長
〃	経済観光部長
〃	農林水産部長
〃	都市整備部長
〃	下水道部長
〃	会計管理者
〃	市議会事務局長
〃	教育委員会事務局副教育長
〃	監査委員事務局長
〃	選挙管理委員会事務局長
〃	農業委員会事務局長
〃	国府町総合支所長
〃	福部町総合支所長
〃	河原町総合支所長
〃	用瀬町総合支所長
〃	佐治町総合支所長
〃	気高町総合支所長
〃	鹿野町総合支所長
〃	青谷町総合支所長
〃	東部広域事務局長