

鹿児島県教育委員会情報セキュリティポリシー

平成22年4月1日施行
平成24年4月1日一部改正
平成26年5月16日一部改正
平成28年4月1日一部改正
令和5年3月30日一部改正

鹿児島県教育委員会

目 次

第1章 情報セキュリティ基本方針

1 目的	1
2 定義	1
3 対象とする脅威	1
4 適用範囲	1
5 職員等の遵守義務	1
6 情報セキュリティ対策	1
7 情報セキュリティ対策基準の策定	2
8 情報セキュリティ実施手順の策定	2

第2章 情報セキュリティ対策基準

1 組織体制	3
2 情報資産の分類と管理	5
3 情報システム全体の強靱性の向上	8
4 物理的セキュリティ	8
5 人的セキュリティ	11
6 技術的セキュリティ	14
7 運用	23
8 業務委託と外部サービスの利用	25
9 評価・見直し	28

第1章 情報セキュリティ基本方針

1 目的

本基本方針は、本県教育委員会が保有する情報資産の機密性、完全性及び可用性を維持するため、本県教育委員会が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2 定義

この情報セキュリティポリシーにおいて使用する用語は、特別な定めのある場合を除き、鹿児島県情報セキュリティポリシー（平成14年4月1日施行。以下「県情報セキュリティポリシー」という。）において使用する用語の例による。

3 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

- (1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等非意図的な要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4 適用範囲

(1) 対象機関の範囲

本基本方針が適用される機関は、鹿児島県教育委員会の行政組織等に関する規則（昭和36年鹿児島県教育委員会規則第6号。以下「規則」という。）第24条第2項に規定する鹿児島県教育庁及び規則第47条に規定する教育機関（県立学校を含む。）とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。ただし、県情報セキュリティポリシーの対象となる情報資産については、対象としない。

- ア ネットワーク及び情報システム並びにこれらに関する設備、電磁的記録媒体
- イ ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- ウ 情報システムの仕様書及びネットワーク図等のシステム関連文書

5 職員等の遵守義務

職員及び会計年度任用職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及びセキュリティ実施手順を遵守しなければならない。また、本県教育委員会の情報資産を教育課程に基づき、県立学校の児童生徒に利用させる場合や職員等以外の者に利用させる場合にあっても、情報セキュリティを確保しなければならない。

6 情報セキュリティ対策

上記3の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じる。

(1) 組織体制

本県教育委員会の情報資産について、情報セキュリティ対策を推進する本県教育委員会の組織体制を確立する。

(2) 情報資産の分類と管理

本県教育委員会の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ、管理区域、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行うなどの人的な対策を講じる。

(5) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(6) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

(7) 業務委託と外部サービスの利用

外部委託を行う場合には、委託業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

(8) 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜、情報セキュリティポリシーの見直しを行う。

7 情報セキュリティ対策基準の策定

上記6に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

8 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に基づき、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。

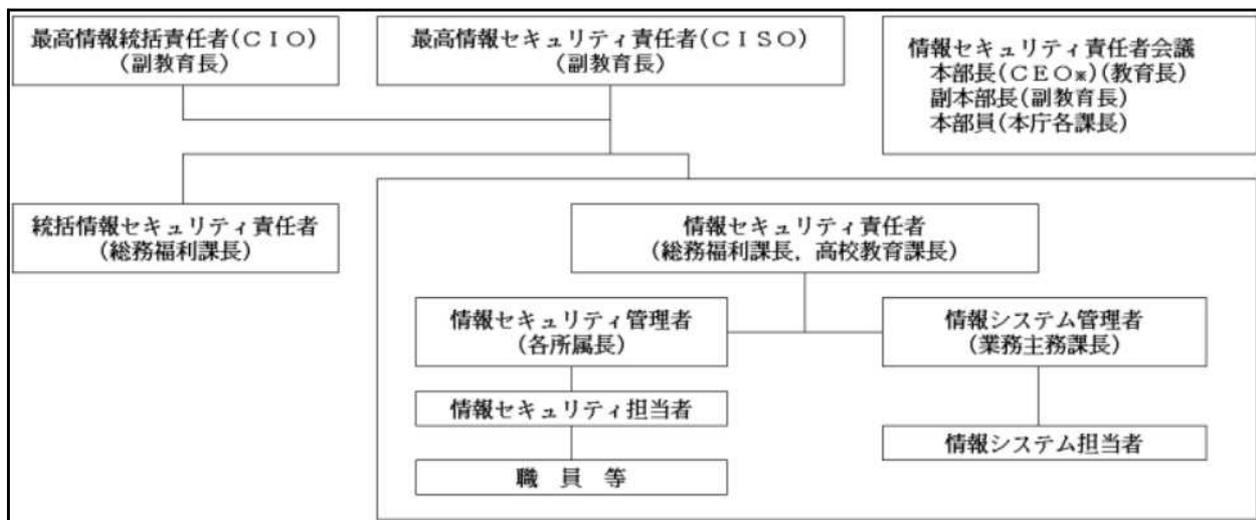
なお、情報セキュリティ実施手順は、公にすることにより本県の教育行政の運営に重大な支障を及ぼすおそれがあることから不開示とする。

第2章 情報セキュリティ対策基準

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本県教育委員会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 組織体制

本県教育委員会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。



※CEO：最高経営責任者（Chief Executive Officer）

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

副教育長を、最高情報統括責任者とする。最高情報統括責任者は、本県教育における情報通信技術の活用による利便性の向上及び教育行政の運営改善等に関する最終決定権限及び責任を有する。

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

ア 副教育長を、CISOとする。CISOは、本県教育委員会における全てのネットワーク、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。

イ CISO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した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

ウ CISOは、情報セキュリティインシデントに対処するための体制（CSIRT：セキュリティインシデントが発生した際に対応する組織（Computer Security Incident Response Team）、以下「CSIRT」という。）を整備し、役割を明確化する。

(3) 統括情報セキュリティ責任者

ア 総務福利課長を、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。

イ 統括情報セキュリティ責任者は、本県教育委員会の全ての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。

ウ 統括情報セキュリティ責任者は、本県教育委員会の全てのネットワークにおける情報セキュリティ対策の実施に関する権限及び責任を有する。

エ 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、情報セキュリティ対策の実施に関する指導及び助言を行う権限を有する。

オ 統括情報セキュリティ責任者は、本県教育委員会の情報資産に対するセキュリティ侵害

が発生した場合又はセキュリティ侵害のおそれがある場合に、C I S Oの指示に従い、C I S O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行う権限及び責任を有する。

カ 統括情報セキュリティ責任者は、本県教育委員会の共通的なネットワーク、情報システムなどの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。

キ 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、C I S O、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。

ク 統括情報セキュリティ責任者は、緊急時にはC I S O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。ケ 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C I S Oにその内容を報告しなければならない。

(4) 情報セキュリティ責任者

ア 情報セキュリティ責任者は、次の表のとおりとする。

責任者	所管する機関
総務福利課長	本庁各課，出先機関，県立学校を除く教育機関
高校教育課長	県立学校

イ 情報セキュリティ責任者は、その所管する機関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。

ウ 情報セキュリティ責任者は、その所管する機関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。

エ 情報セキュリティ責任者は、その所管する機関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。

(5) 情報セキュリティ管理者

ア 各所属長を、情報セキュリティ管理者とする。ただし、これにより難しい場合は、統括情報セキュリティ責任者と協議の上、情報セキュリティ管理者を決定する。

イ 情報セキュリティ管理者はその所管する所属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。

ウ 情報セキュリティ管理者は、その所管する所属において、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C I S Oへ速やかに報告を行い、指示を仰がなければならない。

(6) 情報セキュリティ担当者

ア 情報セキュリティ管理者は、必要に応じてその所管する所属の職員を情報セキュリティ担当者として置くことができる。

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指示に従い、情報資産に係る運用・管理に係る作業を行う。

(7) 情報システム管理者

ア 各情報システムの担当所属長を、当該情報システムに関する情報システム管理者とする。

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、見直

し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。

(8) 情報システム担当者

情報セキュリティ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。

(9) 情報セキュリティ責任者会議

本県教育委員会の情報セキュリティ対策を統一的行うため、情報セキュリティ責任者会議において、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。

(10) 兼務の禁止

ア 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。

イ 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

ア CIOは、CSIRTを整備し、その役割を明確化しなければならない。

イ CIO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内の業務統括及び外部との連携等を行う職員等を定めなければならない。

ウ CISOは、情報セキュリティの統一的な窓口の機能を有する組織を統括情報セキュリティ責任者の下に整備し、情報セキュリティインシデントについて所属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。

エ CISO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、その内容を関係所属に提供しなければならない。

オ 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、CISO、総務省へ報告しなければならない。

カ 統括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を認知した場合には関係所属に対し、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行うよう指示しなければならない。

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

2 情報資産の分類と管理方法

(1) 情報資産の分類

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

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性 3	取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	<ul style="list-style-type: none"> ・支給以外の端末での作業の原則禁止 ・必要以上の複製及び配付禁止 ・情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の暗号化・パスワード設定や施錠可能な場所への保管
機密性 2	取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性 1	機密性 2 又は機密性 3 の情報資産以外の情報資産	—

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性 2	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、県民等の権利が侵害される、又は事務の的確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> ・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
完全性 1	完全性 2 の情報資産以外の情報資産	—

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性 2	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、県民等の権利が侵害される、又は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	<ul style="list-style-type: none"> ・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性 1	可用性 2 の情報資産以外の情報資産	—

(2) 情報資産の管理

ア 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。

イ 情報資産の分類の表示

職員等は、情報資産について、必要に応じてファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類や取扱制限を明示するなど適切な管理を行わなければならない。

ウ 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）情報の作成時は、（１）の分類に基づき、取り扱わなければならない。
- （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。

エ 情報資産の入手

- （ア）庁内（県立学校を含む。以下同じ。）の者が作成した情報資産を入手した者は、必要に応じて入手元に情報資産の分類を確認し、取扱いを引き継がなければならない。
- （イ）庁外の者が作成した情報資産を入手した者は、必要に応じて（１）の分類に基づき、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者は、入手した情報資産の分類が不明な場合、必要に応じて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。

オ 情報資産の利用

- （ア）情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
- （イ）情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。
- （ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

カ 情報資産の保管

- （ア）情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。
- （イ）情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。
- （ウ）情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管するよう努めなければならない。
- （エ）情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合は、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

キ 情報の送信

機密性２以上の情報を庁外に送信する者は、原則として、電子メールに添付する方法を避け、当教育委員会が提供するファイル共有サービス（以下「Webファイル共有システム」という。）を用いなければならない。

ク 情報資産の運搬

- （ア）車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。
- （イ）機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければ

ばならない。

ケ 情報資産の提供・公表

(ア) 機密性2以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

なお、データ送信による場合は、原則として電子メールに添付する方法を避け、Webファイル共有システムを用いなければならない。

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

(ウ) 情報セキュリティ管理者は、県民等に公開する情報資産について、完全性を確保しなければならない。

コ 情報資産の廃棄等

(ア) 情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

(イ) 情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(ウ) 情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

3 情報システム全体の強靱性の向上

(1) 校務内部系

ア 校務内部系と他の領域との分離

校務内部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。校務内部系と外部との通信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。

イ 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、2つ以上を併用する認証(多要素認証)を利用しなければならない。

(イ) 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。

(2) 校務外部系

校務外部系においては、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校務外部系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。

4 物理的セキュリティ

(1) サーバ等の管理

ア 機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定するなど、必要な措置を講じなければならない。

イ サーバ等の冗長化

情報システム管理者は、可用性2の情報資産を格納しているサーバ、セキュリティサーバ、県民サービスに関するサーバ及びその他の基幹サーバを原則として冗長化し、同一データを保持しなければならない。

ウ 機器の電源

- (ア) 情報システム管理者は、施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。
- (イ) 情報システム管理者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

エ 通信ケーブル等の配線

- (ア) 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など必要な措置を講じなければならない。
- (イ) 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。
- (ウ) 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など適正に管理しなければならない。
- (エ) 統括情報セキュリティ責任者及び情報システム管理者は、自ら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以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

オ 機器の定期保守及び修理

- (ア) 情報システム管理者は、必要に応じてサーバ等の機器の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は、電磁的記憶媒体を内蔵する機器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当たり、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。

カ 庁外への機器の設置

情報システム管理者は、庁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承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

キ 機器の廃棄等

情報システム管理者は、機器の廃棄、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。

(2) 管理区域（情報システム室等）の管理

ア 管理区域の構造等

- (ア) 管理区域とは、機密性2以上の情報資産を保有する情報システムのサーバを設置している区域（以下「情報システム室」という。）及び、機密性2以上の情報資産が記録された電磁的記録媒体の保管庫をいう。
- (イ) 情報システム管理者は、原則として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原則として無窓の外壁にしなければならない。
- (ウ) 情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、必要に応じて鍵、監視機能、警報装置等の措置を講じなければならない。
- (エ) 情報システム管理者は、管理区域内の設備に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。
- (オ) 情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電

磁的記録媒体等に影響を与えないようにしなければならない。

イ 管理区域の入退室管理等

(ア) 情報システム管理者は、管理区域への入退室を許可された者のみに制限し、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。

(イ) 職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

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

ウ 機器等の搬入出

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

(イ) 情報システム管理者は、情報システム室の機器等の搬入出について、職員を立ち合わせなければならない。

(3) 通信回線及び通信回線装置の管理

ア 情報システム管理者は、管理する通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

イ 情報システム管理者は、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。

ウ 情報システム管理者は、機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

オ 情報システム管理者は、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十分なセキュリティ対策を実施しなければならない。

カ 情報システム管理者は、可用性2の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

(4) 職員等の利用する端末や電磁的記録媒体等の管理

ア 情報システム管理者及び情報セキュリティ管理者は、執務室等のパソコン等の機器及び電磁的記録媒体について、盗難防止のための必要な措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

イ 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、ICカード、或いは生体認証等複数の認証情報の入力が必要とするように設定しなければならない。

ウ 情報システム管理者及び情報セキュリティ管理者は、パソコンやモバイル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、電磁的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。

エ 情報システム管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

5 人的セキュリティ

(1) 職員等の遵守事項

ア 職員等の遵守事項

(ア) 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、指示を仰がなければならない。

(イ) 業務以外の目的での使用の禁止

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

(ウ) モバイル端末や電磁的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

- ・ C I S Oは、機密性2以上、可用性2、完全性2の情報資産を外部で処理する場合における安全管理措置を定めなければならない。
- ・ 職員等は、本県教育委員会のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。
- ・ 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。
- ・ 職員等は、外部で私物パソコン等により情報処理作業を行う際は、所定の手続きの上、校務用パソコンリモート操作システムにより行うこと。

(エ) 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

- ・ 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等（キーボードやマウス、モニターなど電磁的記録媒体を有しない周辺機器は除く）を原則業務に利用してはならない。ただし、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、利用することができる。
- ・ 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

(オ) 持ち出しの記録

情報セキュリティ管理者は、端末等の持ち出しについて記録を作成し、保管しなければならない。

(カ) パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を統括情報セキュリティ責任者（鹿児島県教育情報ネットワークに接続しないパソコンにあっては、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。

(キ) 机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

(ク) 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。

イ 会計年度任用職員等への対応

(ア) 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、会計年度任用職員等に対し、採用時に情報セキュリティ

ポリシー等のうち、会計年度任用職員等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。

(イ) 情報セキュリティポリシー等の遵守に対する同意

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

(ウ) インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、会計年度任用職員等にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

ウ 情報セキュリティポリシー等の掲示

情報セキュリティ管理者又は情報システム管理者は、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掲示しなければならない。

エ 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。

(2) 研修・訓練

ア 情報セキュリティに関する研修・訓練

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

イ 研修計画の立案及び実施

(ア) 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研修計画の策定とその実施体制の構築を定期的に行わなければならない。

(イ) 研修計画において、職員等は毎年度最低1回は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。

(ウ) 統括情報セキュリティ責任者は、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

(エ) 情報セキュリティ管理者は、所管する機関の研修の実施状況を別に定める自己点検結果表により、統括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。

(オ) 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、C I S O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。

ウ 緊急時対応訓練

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

エ 研修・訓練への参加

全ての職員等は、定められた研修・訓練に参加しなければならない。

(3) 情報セキュリティインシデントの報告

ア 庁内での情報セキュリティインシデントの報告

(ア) 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C S I R Tに報告しなければならない。

(イ) 報告を受けたC S I R T要員は、速やかに統括情報セキュリティ責任者に報告するとともに、その指示に基づき、情報システム管理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インシデントについて、必要に応じてC I S O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。

イ 県民等外部からの情報セキュリティインシデントの報告

(ア) 職員等は、本県教育委員会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事故、欠陥について、県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及びC S I R Tに報告しなければならない。

(イ) 報告を受けたC S I R T要員は、速やかに統括情報セキュリティ責任者に報告するとともに、その指示に基づき、情報システム管理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、当該情報セキュリティインシデントについて、必要に応じてC I S O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。

ウ 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

(ア) C S I R T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。

(イ) C S I R T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、C I S Oに速やかに報告しなければならない。

(ウ) C S I R T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。

(エ) C S I R Tは、これらの情報セキュリティインシデントの原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、C I S Oに報告しなければならない。

(オ) C I S Oは、C S I R T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。

(4) I D及びパスワード等の管理

ア I Cカード等の取扱い

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

- ・ 認証に用いるI Cカード等を、職員等間で共有してはならない。
- ・ 業務上必要のないときは、I Cカード等をカードリーダー又はパソコン等のスロット等から抜き、盗難、紛失、毀損等のないよう管理しなければならない。
- ・ I Cカード等を紛失した場合又は不要となった場合は、速やかに情報システム管理者に報告し、指示に従わなければならない。

(イ) 情報システム管理者は、I Cカード等の紛失等の報告があり次第、当該I C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。

(ウ) 情報システム管理者は、I Cカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

イ I Dの取扱い

職員等は、自己の管理するI Dに関し、次の事項を遵守しなければならない。

(ア) 自己が利用しているI Dは、他人に利用させてはならない。

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

ウ パスワードの取扱い

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

(ア) 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。

(イ) 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。

(ウ) パスワードの文字列は想像しにくいものにしなければならない。

(エ) パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報

- 告し、パスワードを速やかに変更しなければならない。
- (オ) 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情報システム間で用いてはならない（認証用ＩＣカードのログインに係るものを除く。）。
 - (カ) 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。
 - (キ) パスワード及びＩＤを記憶させてはならない（ＩＣカードによる認証に係るものを除く。）。
 - (ク) 職員等間でパスワードを共有してはならない（ただし、共有ＩＤに対するパスワードは除く。）。

6 技術的セキュリティ

(1) コンピュータ及びネットワークの管理

ア ファイルサーバの設定等

- (ア) 情報システム管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。
- (イ) 情報システム管理者は、ファイルサーバを所属の単位で構成し、職員等が他所属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。
ただし、各所属間で各所属長が必要と認めた場合はこの限りではない。
- (ウ) 情報システム管理者は、児童生徒等の個人情報、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、別途ディレクトリを作成するなどの措置を講じ、同一所属であっても、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。

イ バックアップの実施

情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

ウ 他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、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

エ システム管理記録及び作業の確認

- (ア) 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。
- (イ) 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切に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、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しなければならない。

オ 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、適切に管理しなければならない。

カ ログの取得等

- (ア) 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。
- (イ) 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、取得方法及びログが取

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。
(ウ) 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。

キ 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、適切に保存しなければならない。

ク ネットワークの接続制御、経路制御等

(ア) 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。

(イ) 情報システム管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

ケ 外部の者が利用できるネットワーク等の分離等

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、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。

コ 外部ネットワークとの接続制限等

(ア) 情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、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。

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

(ウ) 情報システム管理者は、接続した外部ネットワークのかしによりデータの漏えい、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。

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

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

サ 複合機のセキュリティ管理

(ア) 情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

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

(ウ) 情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する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。

シ IoT機器を含む特定用途機器のセキュリティ管理

情報システム管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を

講じなければならない。

ス 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の利用を認めるに当たっては、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。
- (イ) 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、情報の盗難等を防ぐため、暗号化等の措置を講じなければならない。

セ 電子メールのセキュリティ管理等

(ア) 電子メールのセキュリティ管理

- ・ 情報システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。
- ・ 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、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。
- ・ 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。
- ・ 情報システム管理者は、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。
- ・ 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。

(イ) 電子メールの利用制限

- ・ 職員等は、自動転送機能を用いて、電子メールを外部に転送してはならない。
- ・ 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。
- ・ 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。
- ・ 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。

ソ 電子署名・暗号化

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

タ 無許可ソフトウェアの導入等の禁止

- (ア) 職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
- (イ) 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及び情報セキュリティ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。

チ ソフトウェアのライセンス管理

- (ア) 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。また、ライセンスを超えたインストールを行ってはならない。

(イ) 統括情報セキュリティ責任者、情報セキュリティ管理者又は情報システム管理者は、その調達に係るソフトウェアのライセンスを適正に管理しなければならない。

ツ 機器構成の変更の制限

(ア) 職員等は、パソコンやモバイル端末に対し改造及び構成機器の増設・交換を行ってはならない。

(イ) 職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、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。

テ 業務外ネットワークへの接続の禁止

職員等は、支給された端末を、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。

ト 業務以外の目的でのウェブ閲覧の禁止

(ア) 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。

(イ) 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切な措置を求めなければならない。

ナ 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はWeb会議（専用のアプリケーションやWebブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスのことをいう。なお、テレビ会議システム等特定用途機器同士で通信を行うものは含まない。）を適切に利用するためのセキュリティ確認事項を定めなければならない。

ニ ソーシャルメディアサービスの利用

(ア) 情報セキュリティ管理者は、本県教育委員会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定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。

- ・ 本県教育委員会のアカウントによる情報発信が、実際の本県教育委員会のものであることを明らかにするために、本県教育委員会の自己管理Web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。

- ・ パスワードの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（記憶装置、書類等）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。

(イ) 機密生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) 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) 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。

(オ) 可用性2の情報の提供にソーシャルメディアサービスを用いる場合は、本県教育委員会の自己管理Webサイトに当該情報を掲載して参照可能とすること。

(2) アクセス制御

ア アクセス制御等

(ア) アクセス制御

統括情報セキュリティ責任者又は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、必要に応じてシステム上制限しなければならない。

(イ) 利用者IDの取扱い

- ・ 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。
- ・ 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報システム管理者に届け出なければならない。
- ・ 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、点検しなければならない。

(ウ) 特権を付与されたIDの管理等

- ・ 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。
- ・ 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、CISOが認めた者でなければならない。
- ・ CISOは、代行者を認めた場合、速やかに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及び情報システム管理者に通知しなければならない。
- ・ 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。
- ・ 情報システム管理者は、特権を付与されたID及びパスワードについて、職員等の端末等のパスワードよりも、定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。
- ・ 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。

イ 職員等による外部からのアクセス等の制限

- (ア) 職員等が外部から統括情報セキュリティ責任者の定めた方法により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、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。
- (イ) 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。
- (ウ) 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、情報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。
- (エ) 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。
- (オ) 情報システム管理者は、外部からのアクセスに利用するパソコン等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。
- (カ) 職員等は、外部から持ち帰ったパソコン等の端末を庁内のネットワークに接続する前に、不正プログラム対策ソフトウェアを使用してコンピュータウイルスに感染していないことを確認しなければならない。また、庁内のネットワークに接続し、最新のパッチ及び不正プログラム対策ソフトウェアのパターンファイルを適用後、改めてコンピュータウイルスに感染していないことを確認しなければならない。
- (キ) 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、やむを得ず接続を許可する場合は、利用者のID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（ICカード等）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。

ウ 自動識別の設定

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、ネットワークで使用される機器について、機器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

れるようシステムを設定しなければならない。

エ 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。

オ 認証情報の管理

- (ア) 統括情報セキュリティ責任者又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。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、これを有効に活用しなければならない。
- (イ) 統括情報セキュリティ責任者又は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。
- (ウ) 統括情報セキュリティ責任者又は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。

カ 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時間を必要最小限に制限しなければならない。

(3) 情報システム開発、導入、保守等

ア 情報システムの調達

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

イ 情報システムの開発

- (ア) 情報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、情報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。
- (イ) 情報システム開発における責任者、作業者のIDの管理
 - ・ 情報システム管理者は、情報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。
 - ・ 情報システム管理者は、情報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い。
- (ウ) 情報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
 - ・ 情報システム管理者は、情報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なければならない。
 - ・ 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情報システムから削除しなければならない。

ウ 情報システムの導入

- (ア) 環境開発と運用環境の分離及び移行手順の明確化
 - ・ 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。
 - ・ 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。

ない。

- ・ 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し、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。
- ・ 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上で導入しなければならない。

(イ) テスト

- ・ 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、既に稼動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。
- ・ 情報システム管理者は、運用テストを行う場合、十分な操作確認を行わなければならない。
- ・ 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。
- ・ 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。

エ システム開発・保守に関連する資料等の整備・保管

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

オ 情報システムにおける入出力データの正確性の確保

- (ア) 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。
- (イ) 情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。
- (ウ) 情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

カ 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。

キ 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。

ク 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・統合等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。

ケ リモート保守

情報システム管理者は、所管するシステム等の保守を委託事業者によりリモートで実施させる場合、統括情報セキュリティ責任者に協議の上、セキュリティを担保できる手段（教育情報ネットワークを介した通信、IPアドレスの固定、クライアント認証を用いた二段階認証等）を十分に確保しなければならない。

(4) 不正プログラム対策

ア 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。

- (ア) 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。
- (イ) 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。
- (ウ) 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。
- (エ) 所管するサーバ及びパソコン等に、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。
- (オ) 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。また、ネットワークに接続しないパソコンなど、ネットワーク回線を通じた最新の状態の保持が困難な機器におけるパターンファイルは、1年に1回以上更新しなければならない。

なお、これによりがたい場合に、情報システム管理者から統括情報セキュリティ管理者に対し協議が行われ、ウイルス侵入の恐れがないと認められたものについては、この限りではない。

- (カ) 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。
- (キ) 業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認し、終了が判明した場合は、業務に支障が生じないように、必要に応じて移行期間を設け、速やかな対応を実施しなければならない。

なお、情報システム管理者が業務に支障がないと判断し、統括情報セキュリティ責任者に協議の上、継続使用が認められたものについては、この限りではない。

イ 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として、次の事項を措置しなければならない。

- (ア) 所管するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
- (イ) 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。また、ネットワークに接続しないパソコンなど、ネットワーク回線を通じた最新の状態の保持が困難な機器におけるパターンファイルは、1年に1回以上更新しなければならない。

なお、これによりがたい場合に、情報システム管理者から統括情報セキュリティ管理者に対し協議が行われ、ウイルス侵入の恐れがないと認められたものについては、この限りではない。

- (ウ) 不正プログラム対策ソフトウェアは、常に最新の状態に保たなければならない。
- (エ) ネットワークに接続していない情報システムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、県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物理的に排除されている場合を除き、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。
- (オ) 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

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。

ウ 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。

- (ア) パソコンやモバイル端末において不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
- (イ) 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。
- (ウ) 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。
- (エ) 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実施しなければならない。
- (オ) 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。
- (カ) 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。
- (キ) コンピュータウイルス等の不正プログラムが検出された場合は、情報セキュリティ管理者に報告しなければならない。この場合、情報セキュリティ管理者は直ちに統括情報セキュリティ責任者及び情報システム管理者に報告するとともに、その指示に従わなければならない。

エ 専門家の支援体制

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

(5) 不正アクセス対策

ア 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。

- (ア) 使用されていないポートは閉鎖しなければならない。
- (イ) 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。
- (ウ) 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報セキュリティ管理者へ通報するよう、設定しなければならない。
- (エ) 統括情報セキュリティ責任者は、CSIRT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。

イ 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、関係機関と連絡を密にして情報の収集に努めなければならない。

ウ 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。

エ 内部からの攻撃

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

る攻撃を監視しなければならない。

オ 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、当該職員等の所属するの情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

カ 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。

キ 標的型攻撃

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

(6) セキュリティ情報の収集

ア セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

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

イ 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。

ウ 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、セキュリティ侵害等を未然に防止するための対策を速やかに講じなければならない。

7 運用

(1) 情報システムの監視

ア 統括情報セキュリティ責任者及び情報システム管理者は、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。

イ 統括情報セキュリティ責任者及び情報システム管理者は、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。

ウ 統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続する情報システムを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の遵守状況の確認

ア 遵守状況の確認及び対処

(ア) 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C I S O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。

(イ) C I S O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。

(ウ) 統括情報セキュリティ責任者及び情報システム管理者は、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。

イ パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

C I S O及びC I S Oが指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

ウ 職員等の報告義務

(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。

(イ) 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場合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。

(3) 侵害時の対応

ア 緊急時対応計画の策定

C I S O又は情報セキュリティ責任者会議は、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。

イ 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。

(ア) 関係者の連絡先

(イ) 発生した事案に係る報告すべき事項

(ウ) 発生した事案への対応措置

(エ) 再発防止措置の策定

ウ 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業務継続計画を策定し、C I S O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。

エ 緊急時対応計画の見直し

C I S O又は情報セキュリティ責任者会議は、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。

(4) 例外措置

ア 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、事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、C I S Oの許可を得て、例外措置を取ることができる。

イ 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、事務の遂行に緊急を要するなどの場合であって、例外措置を実施することが回避のときは、事後速やかにC I S Oに報告しなければならない。

ウ 例外措置の申請書の管理

C I S O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。

(5) 法令遵守

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

ア 地方公務員法（昭和25年法律第261号）

イ 著作権法（昭和45年法律第48号）

ウ 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）

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）

カ 鹿児島県個人情報保護条例（令和4年鹿児島県条例第33号）

(6) 懲戒処分等

ア 違反者に対する処分等

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分（戒告、減給、停職又は免職）等の対象とする。

なお、違反の内容と職員等及びその監督責任者の故意又は過失の程度によっては、停職又は免職の対象となり得るものである。

イ 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。

(ア) 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。

(イ) 情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する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。

(ウ) 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C I S O及び当該職員等が所属する情報セキュリティ管理者に通知しなければならない。

8 業務委託と外部サービスの利用

(1) 業務委託

ア 委託事業者の選定基準

(ア) 情報セキュリティ管理者は、委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

(イ) 情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しな

ければならない。

イ 契約項目

情報システムの運用、業務等を外部委託する場合には、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要件を明記した契約を締結しなければならない。

- (ア) 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
- (イ) 委託事業者の責任者、委託内容、作業員、作業場所の特定
- (ウ) 提供されるサービスレベルの保証
- (エ) 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
- (オ) 委託事業者の従業員に対する教育の実施
- (カ) 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
- (キ) 業務上知り得た情報の守秘義務
- (ク) 再委託に関する制限事項の遵守
- (ケ) 委託業務終了時の情報資産の返還、廃棄等
- (コ) 委託業務の定期報告及び緊急時報告義務
- (サ) 県教育委員会による監査、検査
- (シ) 県教育委員会による情報セキュリティインシデント発生時の公表
- (ス) 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）

ウ 確認・措置等

情報セキュリティ管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、イの契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

(2) 外部サービスの利用（機密生2以上の情報を取り扱う場合）

ア 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密生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。なお、当該規定については、当分の間、イからキまでに定めるところによるものとする。

- (ア) 外部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、8（2）において「外部サービス利用判断基準」という。）
- (イ) 外部サービス提供者の選定基準
- (ウ) 外部サービスの利用申請の許可権限者と利用手続
- (エ) 外部サービス管理者の指名と外部サービスの利用状況の管理

イ 外部サービスの選定

(ア) 情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

なお、約款や規約等の同意のみで利用可能となる外部サービス（ただし、電気通信サービスや郵便、運送サービス等は除く）は原則、利用してはならない。

(イ) 情報セキュリティ管理者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部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外部サービス提供者の選定条件に含めること。

- ・ 外部サービスの利用を通じて本県が取り扱う情報の外部サービス提供者における目的外利用の禁止
- ・ 外部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
- ・ 外部サービスの提供に当たり、外部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、本県の意図しない変更が加えられないための管理体制

- ・ 外部サービス提供者の資本関係・役員等の情報、外部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
 - ・ 情報セキュリティインシデントへの対処方法
 - ・ 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
 - ・ 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
- (ウ) 情報セキュリティ管理者は、外部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、外部サービス提供者の選定条件に含めること。
- (エ) 情報セキュリティ管理者は、外部サービスの利用を通じて本県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外部サービス提供者の選定条件に含めること。
- ・ 情報セキュリティ監査の受入れ
 - ・ サービスレベルの保証
- (オ) 情報セキュリティ管理者は、外部サービスの利用を通じて本県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外部サービス提供者を選定し、必要に応じて本県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。
- (カ) 情報セキュリティ管理者は、外部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、外部サービス提供者の選定条件で求める内容を外部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県に提供し、本県の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部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すること。
- (キ) 情報セキュリティ管理者は、外部サービスの特性を考慮した上で、外部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、セキュリティ要件を定めること。
- (ク) 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、外部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すること。

ウ 外部サービスの利用に係る調達・契約

- (ア) 情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部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書に含めること。
- (イ) 情報セキュリティ管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

エ 外部サービスの利用承認

- (ア) 情報セキュリティ管理者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。
- (イ) 統括情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。
- (ウ) 統括情報セキュリティ責任者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

オ 外部サービスを利用した情報システムの導入・構築時の対策

- (ア) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部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

対策を規定すること。

- ・ 不正なアクセスを防止するためのアクセス制御
- ・ 取り扱う情報の機密性保護のための暗号化
- ・ 開発時におけるセキュリティ対策
- ・ 設計・設定時の誤りの防止

(イ) 外部サービス管理者は、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・記録すること。

カ 外部サービスを利用した情報システムの運用・保守時の対策

(ア) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部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すること。

- ・ 外部サービス利用方針の規定
- ・ 外部サービス利用に必要な教育
- ・ 取り扱う資産の管理
- ・ 不正アクセスを防止するためのアクセス制御

(イ) 情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部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すること。

(ウ) 外部サービス管理者は、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・記録すること。

キ 外部サービスを利用した情報システムの更改・廃棄時の対策

(ア) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部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すること。

- ・ 外部サービスの利用終了時における対策
- ・ 外部サービスで取り扱った情報の廃棄
- ・ 外部サービスの利用のために作成したアカウントの廃棄

(イ) 外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。

ク 情報セキュリティ管理者は、緊急を要する場合等においては、イからキまでの定めによらず、統括情報セキュリティ責任者への協議による同意を経て、外部サービスを利用することができる。

(3) 外部サービスの利用（機密性2以上の情報を取り扱わない場合）

ア 外部サービスの利用に係る規定の整備

情報セキュリティ管理者は外部サービス（機密性2以上の情報を取り扱わない場合）を利用する場合、以下を含む外部サービスの利用に関する規定を整備すること。

- (ア) 外部サービスを利用可能な業務の範囲
- (イ) 外部サービスの利用手続
- (ウ) 外部サービス利用における責任者の指名と外部サービスの利用状況の管理
- (エ) 外部サービスの利用の運用手続

イ 外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他の提供条件等から、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を利用すること。

9 評価・見直し

(1) 監査

ア 実施方法

情報セキュリティ監査統括責任者（総務福利課長）は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なければならない。

イ 監査を行う者の要件

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、原則、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。

ウ 監査実施計画の立案及び実施への協力

（ア）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、C I S Oの承認を得なければならない。

（イ）被監査部門は、監査の実施に協力しなければならない。

エ 委託事業者に対する監査

事業者に業務委託を行っている場合、情報セキュリティ監査統括責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

オ 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、C I S Oに報告する。

カ 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切に保管しなければならない。

キ 監査結果への対応

C I S O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。

ク 情報セキュリティポリシー及び関係規定等の見直し等への活用

統括情報セキュリティ責任者は、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。

（2）自己点検

ア 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、統括情報セキュリティ責任者の指示に基づき、自己点検を実施しなければならない。

イ 情報セキュリティ管理者は各所属における情報セキュリティ対策状況について、統括情報セキュリティ責任者の指示に基づき自己点検を行わなければならない。

（3）情報セキュリティポリシー及び関係規程等の見直し

C I S O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。