# 山形県情報セキュリティ基本方針

本県は、自らＩＴ社会の模範たる構成員となり、ＩＴ社会の健全な発展に寄与するとともに、本県が保有する県基幹高速通信ネットワークをはじめとする情報システム及び電子情報（以下「本県の情報資産」という。）の管理を適正に実施し、県民の権利、利益を守り、行政の安定的継続的な運営を実現するため、ここに山形県情報セキュリティ基本方針を制定する。

１　職員一人一人がＩＴ社会における模範となるよう努める。

２　適切な技術的施策を講じ、本県の情報資産に対する不正な侵入、改ざん、破壊、利用妨害などが発生しないよう、また、これが漏えいなどすることのないよう努める。

３　外部の情報資産に対して不正な侵入、改ざん、破壊、利用妨害などをすることがないよう努める。

４　本県の情報資産にセキュリティ上問題が発生した場合、その原因を迅速に究明し、その被害を最小限に止めるよう努める。

５　本県の情報資産のうち特に重要なものについては、必要なとき確実に利活用できるよう十分な備えに努める。

６　上記の活動を継続的に実施し、かつ、新たな脅威にも対応できるよう、情報セキュリティ管理体制を確立する。

平成 14 年 4 月 1 日　施行

平成 20 年 4 月 1 日　改正施行

# 山形県情報セキュリティ対策基準

目次

## 第１章　総則

１．１　目的

山形県情報セキュリティ対策基準（以下「本対策基準」という。）は、山形県情報セキュリティ基本方針（以下「基本方針」という。）に基づき、本県が保有する情報資産を脅威から保護するための情報セキュリティ対策を実施するにあたっての組織体制、管理方法、遵守すべき事項及び判断基準等について基本的な事項を定めることを目的とする。

１．２　用語の定義

本対策基準における主な用語の定義は以下のとおりとする。

（1）情報セキュリティポリシー

基本方針及び本対策基準をいう。

（2）情報資産

次に掲げるもので、本県が保有又は契約により使用等するものをいう。

① 下記（3）から（7）に掲げるもの

② ①で取り扱う情報（これらを印刷した帳票及び文書を含む。）

③ ①にアクセス又は管理区域へ出入りするために用いる IC カード、USB トークン及びこれらに類するもの（以下「IC カード等」という。）

④ 情報システムの仕様書、ネットワーク構成図及び開発・保守に関する資料等の文書

（3）パソコン等機器

パソコン、モバイルノートパソコン、スマートフォン及びタブレット型コンピュータ等の機器並びにこれらに含まれる電磁的記録媒体をいう。

（4）サーバ等機器

情報を格納しているサーバ及びこれに含まれる電磁的記録媒体並びに通信回線装置等のネットワークを構成する基幹機器をいう。

（5）電磁的記録媒体

磁気ディスク、光学ディスク、磁気テープ及びフラッシュメモリ記憶装置等（スマートフォン及びタブレット型コンピュータ等の機器に含まれるものを含む。）のデータを記録・保持するための媒体又は装置全体をいう。

（6）ネットワーク

パソコン等機器又はサーバ等機器（以下「パソコン・サーバ等」という。）を相互に利用するための通信回線網及びこれを構成する基幹機器をいう。

（7）情報システム

パソコン・サーバ等、電磁的記録媒体、ネットワーク、クラウドサービス（インターネット上で利用できるアプリケーション等のサービスをいう。）及びソフトウェアで構成された情報処理又は通信に用いる機器及び仕組みをいう。

（8）脅威

次に掲げるもの及びこれに類するもので、情報資産に係るものをいう。

① 部外者等の無断侵入、窃取、不正アクセス、不正プログラム（不正かつ有害な動作を行う意図で作成された悪意のあるプログラム等をいう。）による攻撃及び標的型攻撃等の意図的要因並びに委託

事業者等の過失等の非意図的要因による情報資産の漏えい・破壊・改ざん・消去等

② 職員等の情報セキュリティポリシーに係る違反行為等の意図的要因並びにプログラム上の欠陥、人為的ミス（誤操作、電子メールの誤送信、紛失等をいう。）及び故障等の非意図的要因による情報資産の漏えい・破壊・改ざん・消去等

③ 地震、落雷及び火災等の災害並びにサービス不能攻撃等の予期しない大量アクセス等による情報システムの停止等

（9）情報セキュリティ

情報資産について、次に掲げるものを維持することをいう。

① 機密性（Confidentiality）

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

② 完全性（Integrity）

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

③ 可用性（Availability）

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(10) 情報セキュリティインシデント

単独又は一連の脅威のうち、情報セキュリティを脅かす又はその確率が高い事象をいう。

(11) 職員

常勤の職員をいう。

(12) 職員等

職員、非常勤職員をいう。

(13) 事業継続計画

自然災害等の問題発生シナリオに基づいて具体的な作業手順を定め、事業などが停止する時間を可能な限り少なくする目的で作られる管理策や計画をいう。

(14) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(15) LGWAN 接続系

人事給与、財務会計及び文書管理等LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう。

(16) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(17) 通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(18) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピューターウィルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

(19) 標準準拠システム等

地方公共団体情報システムの標準化に関する法律（令和３年法律第40号）第６条第１項及び第7条第１項に規定する標準化基準に適合する基幹業務システム及び関連システム等の業務システムをいう。

(20) 重要情報

住民の個人情報や企業の経営情報等をいう。

１．３　適用範囲

（１）組織の範囲

本対策基準が適用される行政機関は、知事部局、教育委員会、議会事務局、選挙管理委員会、人事委員会、監査委員、公安委員会、警察本部、労働委員会、収用委員会、海区漁業調整委員会、内水面漁場管理委員会、企業局及び病院事業局（以下「各部局」という。）とする。

（２）情報資産の範囲

本対策基準は、各部局が管理する情報資産を対象とする。ただし、第３章以下の規定は、警察本部が管理する情報資産について、及び山形県県立学校教育情報セキュリティ対策基準が対象とする情報資産は、第６章の６．６情報セキュリティインシデントの報告及び対応等を除き適用しない。

## 第２章　組織体制

２．１　組織・管理体制

山形県 DX 推進本部設置要綱により設置された山形県 DX 推進本部（以下「本部」という。）を情報セキュリティポリシーに関する最高意思決定機関として、本県における情報セキュリティに係る方針を決定し、その維持及び向上を図るとともに、次の体制により情報セキュリティ対策を推進する。

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

副知事を、CISO とする。CISO は、次に掲げる権限と責任を有する。

① 本県における情報セキュリティ対策全般に関する統括的な権限と責任を有する。

② 情報セキュリティを含む情報管理全般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ことができる。

③ 本対策基準の改定をすることができる。

④ CISO が不在の場合は、統括情報セキュリティ責任者がその権限を代行する。

（２）統括情報セキュリティ責任者

みらい企画創造部長を、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、次に掲げる権限と責任を有する。

① CISO を補佐する。

② 情報セキュリティ責任者に対して、情報セキュリティに関する指導及び助言を行う。

③ 情報セキュリティインシデント（軽微なものを除く。）が発生した場合は、CISO の指示のもと、必要かつ十分な措置を行う。

（３）副統括情報セキュリティ責任者

みらい企画創造部次長を、副統括情報セキュリティ責任者とする。副統括情報セキュリティ責任者

は、次に掲げる権限と責任を有する。

① 統括情報セキュリティ責任者を補佐する。

② 情報セキュリティインシデント（軽微なものを除く。）が発生した場合において、CISO及び統括情報セキュリティ責任者が不在の場合はこれに代わり必要かつ十分な措置を行う。

（4）情報セキュリティ責任者

本部の本部員（以下「部局長」という。）を、情報セキュリティ責任者とする。情報セキュリティ責任者は、次に掲げる権限と責任を有する。

① 各部局の情報セキュリティに関する統括的な権限と責任を有する。

② 各部局の情報セキュリティ管理者及び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。

（5）情報セキュリティ管理者

各所属長を、各所属における情報セキュリティ管理者とする。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について次に掲げる権限と責任を有する。

① 各所属における情報セキュリティ対策に関して、適切な運用及び管理を行う。

② 所管する情報資産を適正に管理するとともに、情報セキュリティポリシーの適切な運用に関して、所属する職員等に指導を行う。

（6）情報システム管理者

各情報システムを所管する所属の長を、情報システム管理者とする。情報システム管理者は、所管する情報システムについて次に掲げる権限と責任を有する。

① 著しく不適切な利用等が認められる者がある場合は、その者の利用を制限又は停止する事ができる。

② 所管する情報システムの情報セキュリティに関する維持管理を行う。

③ 情報システムに関する実施手順の策定及び維持管理を行うとともに、情報主管課長と連携し、緊急時の連絡体制について利用する職員等に周知徹底を図る。

（7）情報主管課長等

情報セキュリティポリシーの運用を適切に実施するため、情報主管課を定めるものとし、みらい企画創造部ＤＸ推進課を情報主管課とし、同部ＤＸ推進課長を情報主管課長とする。情報主管課長は、次に掲げる権限と責任を有する。

① 県としての情報セキュリティの考え方・取組みを明確にする。

② 情報セキュリティポリシーに基づき、山形県として満たすべき情報セキュリティの基準を明確にし、それを実現し、維持するため、本対策基準に基づき実施手順を整備する。

③ 情報セキュリティインシデントが発生した際に迅速な対応ができるよう、各部局との連携のもとに山形県としての組織体制や連絡網を確立するとともに、山形県全体の情報セキュリティ管理体制の統括事務を所掌する。

④ 軽微な情報セキュリティインシデントが発生した場合は、自らの判断により必要かつ十分な措置を行うことができる。

（8）山形県情報セキュリティ等監査員班

統括情報セキュリティ責任者は、情報資産における情報セキュリティ対策状況について確認するため、山形県情報セキュリティ等監査員班長を指名し、山形県情報セキュリティ等監査員班を組織するものとする。

（9）情報化推進・セキュリティ委員会

情報セキュリティ責任者は、情報セキュリティポリシーを各部局の日常業務の中で具体的に運用するため、各部局、各総合支庁ごと情報化推進・セキュリティ委員会を組織するものとする。

(10)情報セキュリティインシデント対策班(Computer Security Incident Response Team､以下｢CSIRT｣という。)

情報セキュリティインシデントの防止に向けた取組みを行うとともに、発生時において、その状況等を正確に把握し、被害拡大の防止、復旧及び再発防止等の対策を迅速かつ的確に行うため、次に掲げるところによりCSIRTの体制を整備するものとする。

① 統括情報セキュリティ責任者、副統括情報セキュリティ責任者、情報主管課長及び情報主管課をCSIRTとする。

② 統括情報セキュリティ責任者をCSIRT責任者、副統括情報セキュリティ責任者をCSIRT副責任者、情報主管課長をCSIRT管理者とする。

③ CSIRT責任者は、情報セキュリティインシデントに対し必要かつ十分な措置をCSIRT管理者に指示する。

④ CSIRT副責任者は、CSIRT責任者を補佐する。また、情報セキュリティインシデントの公表について、情報セキュリティインシデントが発生した部局（以下「インシデント発生部局」という。）に対し指示及び支援を行う。

⑤ CSIRT管理者は、CSIRT責任者の指示のもと、情報セキュリティインシデントに対し必要かつ十分な措置を行う。

⑥ CSIRT管理者は、情報セキュリティに関して県内市町村、関係機関及び委託事業者等との情報共有を行う。

⑦ CSIRT管理者は、県内市町村から情報セキュリティインシデントの報告を受けた場合は、必要に応じ回復のための支援を行う。

(11) 標準準拠システム等をクラウドサービス上で利用する際の組織体制

情報主管課長及び情報システム管理者は、標準準拠システム等をクラウドサービス上で利用する際には、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しなければならない。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しなければならない。

## 第３章　情報資産の分類と管理

### ３．１　情報資産の管理責任

情報セキュリティ管理者及び情報システム管理者は、所管する情報資産について管理責任を有する。

### ３．２　情報資産の分類

情報セキュリティ管理者及び情報システム管理者は、所管する情報資産について、別に定める実施手順に基づき、表１、表２及び表３に定める機密性、完全性、可用性に関する基準により分類を行うものとする。

表１　機密性による情報資産の分類

| 分類 | 分類基準 |
|---|---|
| 自治体<br>機密性<br>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 |
| 自治体<br>機密性<br>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、取扱いに非常に留意すべき情報資産 |
| 自治体<br>機密性<br>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 |
| 自治体<br>機密性２ | 行政事務で取り扱う情報資産のうち、自治体機密性３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 |
| 自治体<br>機密性１ | 自治体機密性２又は自治体機密性３の情報資産以外の情報資産 |

表２　完全性による情報資産の分類

| 分類 | 分類基準 |
|---|---|
| 自治体<br>完全性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、又は行政事務の適正な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産 |
| 自治体<br>完全性１ | 自治体完全性２の情報資産以外の情報資産 |

表３　可用性による情報資産の分類

| 分類 | 分類基準 |
|---|---|
| 自治体<br>可用性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 |
| 自治体<br>可用性１ | 自治体可用性２の情報資産以外の情報資産 |

３．３　情報資産の管理

情報セキュリティ管理者及び情報システム管理者は、所管する情報資産（クラウドサービスに保存される情報資産も含む。）の取扱いについて管理方法を定め、情報資産の分類又はその内容に応じその取扱いを制限しなければならない。また当該情報資産について、所属する職員等に対し、次に掲げるところ及び別に定める実施手順により取り扱うよう指導しなければならない。

（１）取扱い制限の遵守

取扱い制限のある情報資産を取り扱う場合は、これを遵守すること。

（2）情報の秘匿

情報をパソコン等機器又は電磁的記録媒体に保存する場合は、当該情報の情報資産の分類等に応じて、パスワード等による暗号化又は当該機器等の管理区域への保管等の方法によりこれを秘匿すること。

（3）作成途中の情報の管理

自治体機密性２以上の情報について、作成途中であっても紛失や流出等を防止し、作成途中で不要になった場合は、これを消去すること。

（4）他所属が所管する情報資産の取扱い

他の所属が所管する情報資産について、当該他所属が定めた情報資産の分類に基づき取り扱うこと。

（5）情報資産の廃棄等

情報資産を廃棄やリース返却等を行う場合は、次に掲げるところにより行うこと。

① 当該媒体を所管する情報セキュリティ管理者又は情報システム管理者の許可を得ること。

② 記録されている情報の自治体機密性に応じ、情報資産の情報を復元できないように処置すること。

③ 行った処理について、日時、担当者及び処理内容等を記録すること。

④ 標準準拠システム等のクラウドサービス上での利用におけ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すること。

３．４　パソコン等機器、電磁的記録媒体及びソフトウェアの管理

（1）パソコン等機器、電磁的記録媒体及びソフトウェアの管理

情報セキュリティ管理者及び情報システム管理者は、所管するパソコン等機器、電磁的記録媒体及びソフトウェアの管理について、次に掲げるところにより行うものとする。

① パソコン等機器及び電磁的記録媒体の貸出及び返却について、記録を作成し保管しなければならない。

② ソフトウェアについて、そのライセンスを適切に管理しなければならない。また、開発元のサポートが終了したソフトウェアについては、原則として速やかにその使用を終了しなければならない。さらに、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なければならない。

③ パソコン等機器を情報主管課が所管する山形県基幹高速通信ネットワーク（以下「基幹ネットワーク」という。）に接続しようとする場合は、情報主管課長の承認を得なければならない。

④ マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。

⑤ その他情報セキュリティの確保のために必要な措置を講じなければならない。

## 第４章　情報システム全体の強靭性の向上

## ４．１　マイナンバー利用事務系

### （１）マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。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。

### （２）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。また、業務毎に専用端末を設置することが望ましい。

② 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、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、その情報資産の自治体機密性を考慮し、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 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。

① サニタイズ処理方式（ファイルを一旦分解した上で、ウィルスが潜んでいる可能性のある部分について除去を行った後、ファイルを再構築し分解前と同様のファイル形式に復元する方法）

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又は画面転送と同等以上のセキュリティが確保される方式

### （２）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、マイナンバー利用事務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。

（3）LGWAN 接続系から特定のインターネット接続系へのアクセス

LGWAN 接続系からインターネット経由で特定のクラウドサービスにアクセス可能な構成を採用する場合は、インターネットからのリスクが増加するため、より高度なセキュリティ対策を実施しなければならない。

4．3　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。

## 第５章　物理的セキュリティ

情報システム管理者は、所管する情報システムに係る物理的セキュリティを確保するため、次に掲げるところにより対策を講じるものとする。

5．1　機器等の管理

（1）機器の設置場所

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

（2）サーバの冗長化等

① 自治体可用性２の情報を格納しているサーバについて、仮想基盤上で稼動させる等により、物理サーバに障害が発生した際にも情報システムの運用停止時間を最小限にする措置を講じなければならない。

② 自治体完全性２又は自治体可用性２の情報を格納しているサーバ等機器又は電磁的記録媒体について、ミラーリング（データの複製を別の場所に同期させ保存することをいう。）等により当該情報を保持しなければならない。

（3）機器の電源

サーバ等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源を供給する容量の予備電源を備え、落雷等による過電流に対して情報を保護するための措置を講じなければならない。

（4）通信ケーブル等の配線

① 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、配線収容管を使用する等必要な措置を講じなければならない。

② 主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合は、速やかに修復等の対応を行わなければならない。

（5）機器の定期保守及び修理

① 自治体可用性２の情報を格納しているサーバ等機器については、定期保守を実施しなければならない。

② サーバ等機器又は電磁的記録媒体を事業者等に修理させる場合は、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は、修理にあたり、当該事業者等と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。

（6）庁舎外への機器の設置

庁舎外にサーバ等機器を設置する場合は、情報主管課長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。

（7）機器の廃棄

① サーバ等機器及び電磁的記録媒体の廃棄又はリース返却をする場合は、当該機器等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。また、これに係る廃棄等の記録を作成し保管しなければならない。

② パソコン等機器及びサーバ等機器を廃棄する場合は、山形県財務規則（昭和 39 年山形県規則第９号）のほか、関係法令等を遵守するよう留意すること。

③ 標準準拠システム等のクラウドサービス上での利用における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）をする場合は、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　管理区域の管理

（1）管理区域の構造等

① 管理区域とは、自治体機密性２以上、自治体可用性２又は自治体完全性２の情報を取り扱う情報システムを設置し、管理及び運用を行うための部屋又は自治体機密性２以上の情報が記録された電磁的記録媒体を保管する場所をいう。

② 管理区域の出入り口は必要最小限とし、鍵等によって許可されていない立ち入りを防止しなければならない。

③ 管理区域内のパソコン・サーバ等に、転倒及び落下防止等の措置を講じなければならない。

（2）入退室管理

① 管理区域の出入りについて、IC カード等又は入退室簿への記載等により管理しなければならない。

② 管理区域へ入る者に対し、身分が識別できるよう、ネームプレートの着用等を義務付けなければならない。

③ 自治体機密性２以上の情報を取り扱う情報システムを設置している管理区域について、管理区域へ入る者に対し、当該情報システムに関する業務に不要なパソコン等機器、通信回線装置及び電磁的記録媒体等（当該者が所管するものを含む。）を持ち込ませないようにしなければならない。

（3）機器の搬入出

① 管理区域へ搬入するパソコン・サーバ等が、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に確認を行わせなければならない。

② 管理区域のパソコン・サーバ等及び電磁的記録媒体の搬入出について、職員を立ち会わせなければならない。

## ５．３　ネットワークの管理

（1）関連文書の保管

ネットワークに関連する文書を適切に保管しなければならない。

（2）ネットワーク機器の対策

情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

（3）ネットワーク接続の制限

外部のネットワークへの接続を必要最低限に限定し、可能な限り接続ポイントを減らすよう努めなければならない。

（4）通信回線の選択及び情報の暗号化

自治体機密性２以上の情報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。

（5）自治体機密性及び自治体完全性の確保

自治体機密性２以上又は自治体完全性２の情報を取り扱う情報システムのネットワークに使用する回線について、伝送途上で情報が破壊・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。

（6）調査、認識した脆弱性等への対策

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。

（7）可用性の確保

自治体可用性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、求められる安定性を満たすもの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。

## 第６章　人的セキュリティ

### ６．１　職員の遵守事項

（1）職員の遵守事項

職員は、次に掲げる項目を遵守するものとする。

① 情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたって情報セキュリティポリシー及び実施手順等を遵守するとともに自らの役割及び責任を意識しなければならない。

② 業務上必要のない情報を作成・入手・利用してはならない。

③ 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。

④ 自治体機密性２以上又は自治体完全性２の情報資産を外部に持ち出し、又は送信等する場合は、当該情報資産を所管する情報セキュリティ管理者又は情報システム管理者の承認を得た上で取扱い制限に従うとともに、格納されている情報の暗号化等の処理を行わなければならない。

⑤ 庁舎外で情報処理業務を行う場合は、情報セキュリティ管理者の許可を得なければならない。

⑥ 庁舎外から持ち帰ったパソコン等機器をネットワーク及び情報システムに接続する前に、不正プログラム対策ソフトウェアによるチェックを行なわなければならない。
⑦ 私物のパソコン・サーバ等又は電磁的記録媒体を、ネットワーク及び情報システムに接続してはならない。ただし、在宅勤務職員がリモート接続システムにより接続する場合は、実施手順に従い利用することができる。
⑧ パソコン等機器を公衆無線 LAN 等（不特定多数に利用させることを目的に提供されている無線 LAN 環境をいう。）へ接続してはならない。
⑨ パソコン等機器について、その仕様を変更又はソフトウェアをインストールする場合は、当該機器を所管する情報セキュリティ管理者又は情報システム管理者の許可を得なければならない。
⑩ 情報主管課からパソコン等機器の情報セキュリティに関する修正プログラムが配布された場合は、速やかに当該パソコン等機器へ適用しなければならない。
⑪ ソフトウェアを不正に利用してはならない。
⑫ 電磁的記録媒体等をパソコン・サーバ等に接続する際は、不正プログラム対策ソフトウェアによる当該媒体のチェックを行わなければならない。
⑬ 使用しているパソコン等機器が不正プログラムに感染した場合は、直ちに LAN ケーブルの取り外し又は通信を行わない設定への変更等によりネットワークから切り離すとともに、「6.6.情報セキュリティインシデントの報告及び対応等」に掲げるところにより報告等を行わなければならない。
⑭ 情報資産を第三者に使用閲覧等されることがないよう、離席時にはパソコン等機器のスクリーンセーバー設定及び操作のロックを行わなければならない。また、電磁的記録媒体及び文書等を容易に閲覧等されない場所に保管しなければならない。
⑮ 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当該情報を消去（消去できない場合は当該媒体内の全ての情報について保存される必要がなくなった時点で破棄）しなければならない。
⑯ 入出力した文書をコピー機、ＦＡＸ又はプリンタ等に放置してはならない。
⑰ 差出人が特定できない又は不自然なファイルが添付されている等の不審な電子メールを受信した場合は、「6.6.情報セキュリティインシデントの報告及び対応等」に掲げるところにより報告等を行わなければならない。
⑱ 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。
⑲ 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。
⑳ 複数人に電子メールを送信する場合は、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。
㉑ 異動、退職等により業務を離れる場合は、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。

## ６．２　非常勤職員への対応

（１）非常勤職員への適用

情報セキュリティポリシーは、非常勤職員に対しても適用するものとする。

（２）非常勤職員への対応

情報セキュリティ管理者は、非常勤職員の情報セキュリティポリシーの遵守について、次に掲げるところにより行うものとする。

① 採用の際は、情報セキュリティポリシーのうち、非常勤職員が守るべき内容を理解させなければならない。
② 採用の際は、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なければならない。

６．３　情報セキュリティのポリシー等の掲示

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

６．４　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。

６．５　情報セキュリティに関する研修

（１）研修の実施

① 統括情報セキュリティ責任者は、山形県組織全体の情報セキュリティ向上のため、山形県として必要な教育内容・研修計画を定め、教育・啓発活動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は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施しなければならない。

（２）研修の受講

① 職員等は、情報セキュリティ教育の重要性を認識し、必要と定められた研修を受講しなければならない。
② 情報セキュリティ管理者は、所属職員等に対し、その業務に応じた情報セキュリティ教育・啓発に関する研修等を受講できる環境づくりに努めなければならない。

６．６　情報セキュリティインシデントの報告及び対応等

情報セキュリティインシデントが発生した場合の報告及び対応等は、次に掲げるところにより行うものとする。

（１）情報セキュリティインシデントの報告及び対応

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は速やかに自らが所属する情報セキュリティ管理者に報告し、その指示に従わなければならない。
② 情報セキュリティ管理者は、情報セキュリティインシデントを認知した場合は速やかに情報主管課長に報告するとともに、当該インシデントが情報システムに関連する場合は、速やかにこれを所管する情報システム管理者に報告しその指示に従わなければならない。また、緊急性及び重要性に応じて情報セキュリティ責任者に報告しなければならない。
③ 情報システム管理者は、情報セキュリティインシデントを認知した場合は、速やかに情報主管課長にその旨を報告するとともに、情報主管課長の指示のもと、適切な対応に努めなければならない。また、緊急性及び重要性に応じて情報セキュリティ責任者に報告しなければならない。
④ 情報主管課長は、情報セキュリティインシデントを認知した場合は、その状況を確認し、緊急性及び重要性に応じて統括情報セキュリティ責任者及び副統括情報セキュリティ責任者に報告を行うと

ともに、統括情報セキュリティ責任者の指示又は自らの判断のもと、当該インシデントに係る情報セキュリティ管理者及び情報システム管理者に対し、被害拡大防止及び復旧のための対策を指示し、又は自らこれを講じなければならない。

⑤ 統括情報セキュリティ責任者は、情報セキュリティインシデントの報告を受けた場合はその状況を確認し、被害拡大防止及び復旧のための対策について情報主管課長に対し指示しなければならない。また、その内容についてCISOに報告しなければならない。

⑥ 情報主管課長は、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。

⑦ 情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。

（2）情報セキュリティインシデントの公表

情報セキュリティインシデントについて外部公表を行う場合は、次に掲げるところにより行うものとする。

① 副統括情報セキュリティ責任者は、インシデント発生部局における「山形県広報広聴事務取扱要綱」の規定による広報監（以下「発生部局の広報監」という。）に対し、外部公表に係る指示及び支援を行わなければならない。

② 外部公表は、発生部局の広報監が行うものとし、その内容について副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 副統括情報セキュリティ責任者は、公表した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。

（3）関係機関等との連携

情報主管課長は、当該情報セキュリティインシデント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密接な連携に努めなければならない。

（4）情報セキュリティインシデントの原因究明・記録等

情報主管課長並びに発生した情報セキュリティインシデントに係る情報セキュリティ管理者及び情報システム管理者は、互いに連携して当該インシデントの原因を究明するとともに、その内容、原因、処理結果等を記録し、適切に保存しなければならない。

（5）情報セキュリティインシデントの再発防止

① CISOは、情報セキュリティインシデントの報告を受けた場合は、その内容を確認し、統括情報セキュリティ責任者に対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。

② 統括情報セキュリティ責任者は、CISO の指示のもと、再発防止のための対策について情報セキュリティ責任者に対し指示し、又は自らこれを行わなければならない。また、その内容についてCISOに報告しなければならない。

③ 情報セキュリティ責任者は、再発防止の対策について指示を受けた場合はこれを実施し、その内容について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。

## ６．７　ID及びパスワード等の取扱い

職員等は、ID、パスワード及びICカード等の取扱いについて、次に掲げるところにより行うものとする。

（1）ID及びパスワードの取扱い

① 自己の管理するID及びパスワードを、他人に利用させてはならない。

② 情報システム等でやむを得ずID及びパスワードを共用利用する場合は、共用利用者以外に利用させてはならない。

③ パスワードは秘密にし、パスワードを記載したメモ等を第三者が容易に閲覧できる場所に掲示等してはならない。また、業務上必要がなくなった場合は速やかにこれを廃棄しなければならない。

④ パスワードは十分な長さとし、文字列は他人が容易に想像できないものにしなければならない。

⑤ ID及びこれに係るパスワードが流出した、又はそのおそれがある場合は、速やかにパスワードを変更するとともに、「6.6.情報セキュリティインシデントの報告及び対応等」に掲げるところにより報告等を行わなければならない。

⑥ 情報システム管理者から与えられた仮のパスワード（初期パスワード含む）について、情報システムへ初めてログインした時点で変更しなければならない。

⑦ パソコン等機器のパスワードの記憶機能について、情報主管課より提供された以外のものを使用してはならない。

（2）ICカード等の取扱い

① ICカード等を業務上必要のない者に貸し出してはならない。

② ICカード等をパソコン等機器に接続したまま離席してはならない。

③ ICカード等を紛失した場合は、「6.6.情報セキュリティインシデントの報告及び対応等」に掲げるところにより報告等を行わなければならない。

## 第７章　技術的セキュリティ

### ７．１　機器及びネットワークの管理

（1）機器及びネットワークの管理

情報システム管理者は、所管する情報システムについて、次に掲げるところにより機器及びネットワークの管理等を行うものとする。

① バックアップの実施

（ア）業務システムのデータベースやサーバ等機器に記録された情報について、当該機器の冗長化対策にかかわらず、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。

（イ）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。

（ウ）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しなければならない。

（エ）標準準拠システム等のクラウドサービス上での利用において、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、その機能の仕様が要件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。

② 情報システムの運用において実施した作業について、作業記録を作成し適切に管理しなければならない。

③ 情報システムの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するとともに、これを漏えいし、又は改ざん若しくは消去等されないよう適正に管理し、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。

④ 情報システムの仕様書及びネットワーク構成図について、記録媒体にかかわらず、業務上必要とする者以外の者の閲覧、紛失等がないよう、適正に管理しなければならない。

⑤ 各種ログ及び情報セキュリティの確保に必要な情報を取得するとともに、これを改ざん及び誤消去されないよう必要な措置を講じた上で、一定の期間保管しなければならない。

⑥ ログとして取得する項目、保存期間及び取扱い方法等について定め、適正にログを管理しなければならない。

⑦ 悪意ある第三者等からの不正侵入及び不正操作等の有無について、取得したログを必要に応じて点検又は分析しなければならない。なお、標準準拠システム等をクラウドサービス上での利用の際には、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しなければならない。

⑧ 標準準拠システム等のクラウドサービス上での利用において、情報セキュリティ監査等のために必要となった場合の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。

⑨ 職員等からの情報システムに関する障害の報告及びその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。

⑩ 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の設定情報を管理しなければならない。

⑪ 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。

⑫ 保守又は診断のために、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。

## ７．２　外部ネットワーク等との接続

### （１）外部ネットワーク等との接続

情報システム管理者は、所管する情報システムについて外部のネットワーク及び情報システム（以下「外部ネットワーク等」という。）との接続を行う場合は、次に掲げるところにより行うものとする。

① 基幹ネットワークを外部ネットワーク等と接続する場合は、情報主管課長の承認を得た上でこれを行わなければならない。

② 接続しようとする外部ネットワーク等に係るネットワーク構成、機器構成及び情報セキュリティ

技術等を調査しなければならない。

③ 接続した外部ネットワーク等の管理者の瑕疵によりデータの漏えい・破壊・改ざん・消去等又は情報システムの停止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等の管理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。

④ ウェブサーバ等をインターネット上に公開する場合、次のセキュリティ対策を実施しなければならない。

(ア) 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の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。

(イ) 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。

(ウ) ウェブサーバからの不用意な情報漏えいを防止するため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、ウェブコンテンツの編集作業を行う主体を限定しなければならない。

(オ)インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じなければならない。【推奨事項】

⑤ 接続した外部ネットワーク等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は、速やかに当該外部ネットワークを遮断しなければならない。

### ７．３　無線 LAN の盗聴対策

情報システム管理者は、所管する情報システムにおいて無線 LAN を利用する場合、解読が困難な暗号化及び認証技術を使用しなければならない。

### ７．４　電子メールのセキュリティ管理及び利用制限

情報主管課長が所管する電子メールのセキュリティ管理及び利用制限は、次に掲げるところによるものとする。

（1）電子メールのセキュリティ管理

情報主管課長は、電子メールのセキュリティ管理等について、次に掲げるところにより行うものとする。

① 権限のない利用者により、基幹ネットワークを経由した外部から外部への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、メールサーバの設定を行わなければならない。

② 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、必要に応じてメールサーバの運用を停止しなければならない。

③ 電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④ 所管するドメインについて、外部の者により詐称されないよう送信ドメインの認証を行わなければならない。

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

（2）電子メールの利用制限

情報システムの開発、運用又は保守等のため庁舎内に常駐している委託事業者等による電子メール

アドレスの利用は原則禁止とする。ただし、業務上やむを得ないと情報主管課長が認めた場合はこの限りではない。

７．５　Web 会議サービスの利用時の対策

Web 会議サービスの利用にあたっては、別に定める実施手順に従い、情報セキュリティ対策を実施しなければならない。

７．６　ソーシャルメディアサービスの利用

ソーシャルメディアサービスの利用にあたっては、別に定める実施手順を遵守しなければならない。

７．７　アクセス制御

（１）情報システム管理者によるアクセス制御等

情報システム管理者は、所管する情報システムへのアクセス制御等について、次に掲げるところにより行うものとする。

① 情報システムで取り扱う情報資産の分類又はその内容に応じ、アクセス権限を有する職員等及びその権限の内容を、必要最小限としなければならない。

② 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、IC カード等又はユーザ ID 等によりシステム上制限しなければならない。

③ 利用者の登録、変更及び抹消等の情報管理並びに職員等の異動、出向及び退職等に伴うユーザ ID の取扱い等の方法を定めなければならない。

④ ユーザ ID に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。

⑤ 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 及びこれに係るパスワードの漏えい等が発生しないよう厳重に管理しなければならない。

⑥ 職員等の認証に関する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。

⑦ 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。

⑧ 特権を付与された ID 及びパスワードについて、人事異動の際のパスワードの変更、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。

⑨ 所管する情報システムの情報資産の分類又はその内容に応じて、適正な強度のログインパスワードを設定しなければならない。

⑩ 外部のネットワーク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通信の暗号化等の措置を講じなければならない。

⑪ 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とするよう努めなければならない。

（２）職員等による外部からのアクセス等の制限

情報セキュリティ管理者は、職員等による外部のネットワークからのアクセス等について、次に掲げるところにより行わなければならない。

① 職員等に外部からネットワーク又は情報システムへアクセスさせる場合は、当該システムを所管

する情報システム管理者の承認を得なければならない。

② 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、これを必要とする合理的理由を有する最小限の者に限定しなければならない。

７．８　システム開発・導入・保守等

情報システム管理者は、情報システムの開発・導入・保守等について、次に掲げるところにより行うものとする。

（１）機器等の調達に係る運用規程の整備

① 機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。

② 情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。

（２）機器等及び情報システムの調達

① 情報システムに係る開発・導入・保守等の調達にあたっては、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。また、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、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

② 機器又は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。

（３）情報システムの開発

① 開発に使用するIDを適切に管理し、開発完了後に不要となる場合は、これを消去しなければならない。

② 開発に用いるハードウェア及びソフトウェアを特定し、情報セキュリティ上問題のないことを確認し、それ以外のものを利用させてはならない。

③ 利用を認めた以外のソフトウェアが情報システムに導入されている場合は、これを消去しなければならない。

④ アプリケーション・コンテンツの開発時の対策

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。

（４）情報システムの導入

① 情報システムの開発、保守及びテスト環境と運用環境を可能な限り分離しなければならない。

② 情報システムの開発・保守計画の策定時にシステム運用環境への移行の手順を明確にしなければならない。

③ 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、移行に伴う業務への影響が最小限になるよう配慮しなければならない。

④ 導入する情報システム又はサービスに求められる可用性を満たすことを確認した上で導入しなければならない。

⑤ 導入する情報システム又はサービスを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。またこの場合において、機密性２以上の情報を試験に使用してはならな

い。

⑥ 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。

⑦ 機器等の納入時又は情報システムの受入れ時

（ア）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。

（イ）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。

（5） 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

① 情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じなければならない。【推奨事項】

② 利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。

（ア）情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

（イ）情報システムの基盤を管理又は制御するソフトウェアで発生した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

（6） 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

① 情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施しなければならない。【推奨事項】

（ア）情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策

（イ）脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

② 利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

（7）情報システムの開発・保守に関する資料の保管

情報システムの開発・保守に関する資料を適正に整備・保管しなければならない。

① 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、当該内容について情報主管課長に報告しなければならない。

② 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しなければならない。【推奨事項】

・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 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

（8）入出力データの正当性の確保

① 情報システムに入力されるデータについて、範囲及び妥当性のチェック機能並びに不正な文字列

の入力を除去する機能が組み込まれるよう、情報システムを設計しなければならない。

② 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。

（ア）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。

（イ）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。

（ウ）ウェブアプリケーションやウェブコンテンツにおいて、故意又は過失による情報の漏えい・破壊・改ざん・消去等のおそれがある場合に、これを検出するチェック機能が組み込まれるよう、情報システムを設計しなければならない。

③ 情報システム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、情報システムを設計しなければならない。

（9）変更管理

情報システムの変更をした場合は、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。

(10) 開発・保守用のソフトウェアの更新等

開発・保守用のソフトウェアを更新又はこれにパッチを適用する場合は、関連する他の情報システムへ影響を与えることがないよう、その整合性を確認しなければならない。

(11) システム更新又は統合時の検証等

情報システムを更新又は統合する際は、長時間停止や誤作動による業務への影響が生じないよう、更新等の前にその体制及び計画等について検証等を行わなければならない。

(12) 情報システムについての対策の見直し

対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本県内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、情報主管課長へ報告しなければならない。

7．9　不正プログラム対策

（1）情報主管課長による対策

情報主管課長は、不正プログラム対策について、次に掲げるところにより行うものとする。

① 外部ネットワーク等から送受信するファイルは、基幹ネットワークのゲートウェイにおいて不正プログラムのチェックを行い、これの基幹ネットワークへの侵入及び外部への拡散を防がなければならない。

② 不正プログラムに関する情報を収集し、必要に応じ職員等に対して注意喚起を行わなければならない。

（2）情報システム管理者による対策

情報システム管理者は、所管する情報システムの不正プログラム対策について、以下に掲げるところにより行うものとする。

① ネットワーク接続を要する情報システムにおいて、パソコン・サーバ等に、不正プログラム対策ソフトウェアを常駐させるとともに、不正プログラムのパターンファイル等を常に最新の状態に保たなければならない。

② ネットワークに接続しない情報システムにおける電磁的記録媒体の使用について、使用を認めた

以外のものを職員等に利用させてはならない。

③ ネットワークに接続しない情報システムにおいて、不正プログラムの感染及び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。

④ 不正プログラム対策ソフトウェアを導入しているパソコン・サーバ等に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤ 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。

⑥ 標準準拠システム等のクラウドサービス上での利用において、仮想マシンを設定する際には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。

## 7．10　不正アクセス対策

### （1）基幹ネットワークの不正アクセス対策

情報主管課長は、基幹ネットワークの不正アクセス対策について、次に掲げるところにより行うものとする。

① 使用されていないポートを閉鎖しなければならない。

② 不要なサービスについて、機能を消去又は停止しなければならない。

③ 情報システムに攻撃を受けることが明確になった場合は、「5.6.情報セキュリティインシデントの報告及び対応等」に準じ、報告等及び情報システムの停止を含む必要な措置を講じるとともに、関係機関と連絡を密にして情報の収集、提供を行わなければならない。

④ 基幹ネットワーク内のパソコン・サーバ等に対する攻撃及びこれらからの外部ネットワーク等に対する攻撃を監視しなければならない。

⑤ 標準準拠システム等をクラウドサービス上で利用するにあたって、情報セキュリティポリシーにおける不正アクセス対策に関する事項が、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。

⑥ 標準準拠システム等をクラウドサービス上で利用する際に、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なければならない。

⑦ 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、情報セキュリティポリシーを満たすことを確認しなければならない。

### （2）サービス不能攻撃対策

情報システム管理者は、外部のネットワーク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。

### （3）標的型攻撃対策

電子メールに係る情報システムを所管する情報システム管理者は、所管するネットワークについて、

標的型攻撃による不正プログラムの侵入を防止するために、自動再生無効化等の入口対策を講じなければならない。また、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等の内部対策を講じなければならない。

7．11　セキュリティ情報の収集

（1）セキュリティ情報の収集

情報主管課長及び情報システム管理者は、セキュリティ情報の収集について、次に掲げるところにより行うものとする。

① 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 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知した場合は、情報セキュリティインシデント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。

③ 標準準拠システム等をクラウドサービス上での利用する際には、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、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。そして、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。

（2）不正プログラム情報の収集

情報主管課長は、不正プログラムに関する情報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。

## 第８章　遵守状況の確認

8．1　情報システムの監視

情報システム管理者は、所管する情報システムの監視について、次に掲げるところにより行うものとする。

（1）情報システムの運用・保守時の対策

① 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。

② 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。

③ 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。

（2）情報システムの監視機能

① 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。

② 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。

③ 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。

④ 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。

（3）情報システムの監視

① 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、その記録を保存しなければならない。

② 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。

③ 標準準拠システム等をクラウドサービス上での利用する際には、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。

④ 標準準拠システム等をクラウドサービス上での利用する際には、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しなければならない。

⑤ 標準準拠システム等をクラウドサービス上での利用する際には、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。

（ア）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

（イ）クラウドサービス利用の終了手順

（ウ）バックアップ及び復旧

## 8．2　情報セキュリティポリシー遵守状況の確認

（1）情報セキュリティポリシー遵守状況の確認

① 情報セキュリティ管理者は、定期的又は必要に応じ所属職員等の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、問題を認めた場合は、速やかに情報主管課長に報告しなければならない。

② 情報主管課長は、発生した問題について、適正かつ速やかに対処しなければならない。

③ 情報システム管理者は、ネットワーク及びサーバ等機器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、定期的又は必要に応じ確認を行い、問題がある場合は適正かつ速やかに対処しなければならない。

（2）機器等の利用状況調査

情報主管課長は、不正アクセス及び不正プログラム等の確認のため、パソコン等機器、電磁的記録媒体のログ及び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。

# 第９章　障害時の対応

９．１　緊急時対応計画の策定

情報システム管理者は、緊急時対応計画の策定について、次に掲げるところにより行うものとする。

（1）緊急時対応計画の策定

① 情報セキュリティインシデントが発生した場合において連絡、証拠保全、被害拡大の防止、影響範囲の特定、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、緊急時対応計画を定めておき、発生時には当該計画に従って適正に対処しなければならない。

② 標準準拠システム等をクラウドサービス上での利用する際には、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しなければならない。

（2）緊急時対応計画に定める事項

緊急時対応計画には、次に掲げる内容を定めなければならない。

① 関係者の連絡先

② 発生した事案に係る報告すべき事項

③ 発生した事案への対応措置

④ 再発防止措置の策定

（3）緊急時対応計画の見直し

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対し、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。

９．２　事業継続計画との整合

県が事業継続計画を整備する場合、本部は、当該計画と情報セキュリティポリシー等の整合性を検討し、必要に応じ情報セキュリティポリシーの見直しを行うものとする。

## 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

10．１　業務委託等

情報システム管理者は、業務委託等について、次に掲げるところにより行うものとする。

（1）委託等事業者に係る運用規程の整備

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 委託等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 委託等事業者の選定基準

（2）業務委託実施前の対策

① 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は、委託等事業者との間で必要に応じて次の情報セキュリティ要等に係る要件を契約に含めなければならない。
・山形県情報セキュリティポリシー及び実施手順の遵守
・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
・ 当該事業者の責任者、委託等の内容、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
・ 当該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（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）での管理方法
・ 業務従事者に対する情報セキュリティ教育の実施
・ 提供された情報の目的外利用及び当該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
・ 再委託等に関する制限事項の遵守
・ 業務終了時の情報資産の返還、廃棄等
・ 業務の定期報告及び緊急時報告義務
・ 県による情報セキュリティに関する監査・検査の受け入れ
・ 情報セキュリティインシデント発生時の県による公表に対する同意
・ 情報セキュリティポリシーを遵守しなかったこと及び当該事業者の瑕疵による損害賠償等
（オ）委託事業者又は入札参加者に重要情報を提供する場合は、秘密保持契約（NDA）の締結
② 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（NDA）の締結
（３）業務委託実施期間中の対策
① 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）情報主管課長へ措置内容の報告（重要度に応じてCISO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

（5）セキュリティ教育の実施状況の確認

委託先を含む関係者については委託先等で情報セキュリティに関する教育が行われていることを確認しなければならない。

10. 2　情報システムに関する業務委託

情報システム管理者は、情報システムに関する業務委託について、次に掲げるところにより行うものとする。

（1）　情報システムに関する業務委託における共通的対策

情報システムに関する業務委託の実施までに、情報システムに本県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。

（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なければならない。

① 情報システムのセキュリティ要件の適切な実装

② 情報セキュリティの観点に基づく試験の実施

③ 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

（3）　情報システムの運用・保守を業務委託する場合の対策

① 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。

② 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。

（4）　本県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

① 外部の一般の者が本県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なければならない。

② 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。

③ 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。

④ 業務委託サービスを利用する場合には、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。

⑤ 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。
⑥ 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承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

10. 3　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）

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）にあたっては、別に定める実施手順を遵守しなければならない。

10. 4　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）

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）にあたっては、別に定める実施手順を遵守しなければならない。

## 第 11 章　法令遵守

11. 1　法令遵守

（1）法令遵守

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

① 地方公務員法(昭和 25 年 12 月 13 日法律第 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 5 月 30 日法律第 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 サイバーセキュリィティ基本法（平成 26 年法律第 104 号)
⑦ 個人情報の保護に関する法律施行条例（令和４年 12 月県条例第 37 号)

（2）情報システム管理者は、標準準拠システム等をクラウドサービス上での利用する際に、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。

## 第 12 章　違反時の対応等

12. 1　違反時の対応及び処分等

（1）違反時の処分

職員等の情報セキュリティポリシーに係る違反行為が認められるときは、当該職員等は発生した事案の状況等に応じて、懲戒処分その他の処分の対象となる。

（2）違反時の対応

違反行為への対応は、次に掲げるところによるものとする。

① 職員等は、他の職員等の情報セキュリティポリシーに係る違反行為を認知した場合は、速やかに当該職員等が所属する情報セキュリティ管理者に報告し、適正な措置を求めなければならない。

② 情報セキュリティ管理者は、所属する職員等の情報セキュリティポリシーに係る違反行為を認知した場合は、速やかに情報主管課長及び当該違反行為に係る情報システム管理者に報告するとともに、当該職員等に是正の指導を行わなければならない。

③ 情報主管課長及び当該違反行為に係る情報システム管理者は、所管する情報システムに関して職員等の情報セキュリティポリシーに係る違反行為を認知した場合は、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。

④ 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、情報システム管理者は、所管する情報システムについて、当該職員等の利用を停止することができる。

## 第13章　評価・見直し

13. 1　情報セキュリティ監査

（1）情報セキュリティ監査の実施

情報セキュリティ監査は、次に掲げるところにより行うものとする。

① 山形県情報セキュリティ等監査員班は、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、定期的に又は必要に応じて監査を行わなければならない。

② 山形県情報セキュリティ等監査員班は、情報セキュリティ監査に係る実施要綱を定めなければならない。

③ 被監査所属の情報セキュリティ管理者及び監査対象の情報システムを所管する情報システム管理者は、情報セキュリティ監査の実施に協力しなければならない。

13. 2　自己点検

（1）自己点検の実施

情報セキュリティ対策に関する自己点検は、次に掲げるところにより行うものとする。

① 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運用及び管理状況について、定期的又は必要に応じ自己点検を行わなければならない。

② 情報システム管理者は、所管する情報システムについて、定期又は必要に応じ情報セキュリティ対策状況に関する自己点検を行わなければならない。

③ 情報セキュリティ管理者及び情報システム管理者は、自己点検実施後は点検結果と改善策を取りまとめ、自己の権限の範囲内で改善を図った上で、情報主管課長に報告しなければならない。

④ 情報主管課長は、報告を受けた点検結果について、情報セキュリティポリシーの見直しに活用しなければならない。

13. 3　情報セキュリティポリシーの見直し

本部は、必要があると認めた場合は、情報セキュリティポリシーの運用状況を確認するとともに、その

結果及び情報セキュリティに係る環境の変化等を踏まえ、その見直しを行うものとする。

## 第 14 章　例外措置

14. 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は、統括情報セキュリティ責任者の承認を得て、例外措置を講じることができる。

14. 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、災害対応等行政事務の遂行に緊急を要し、例外措置をとることが避けられない場合は、事後速やかに統括情報セキュリティ責任者に報告しなければならない。

14. 3　例外措置の記録

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又は情報システム管理者により例外措置がとられた場合は、その内容について記録し、一定期間保管しなければならない。

## 第 15 章　実施手順

15. 1　実施手順

本対策基準に定める事項のほか、情報セキュリティポリシーの運用にあたって遵守すべき実施手順のうち情報主管課長が所管するものは、別表のとおりとする。

15. 2　実施手順の公開等

（1）実施手順の公開等

① 実施手順は、公にすることにより本県の行政運営に重大な支障を及ぼすおそれがあることから原則として非公開とする。

② 職員等以外の者がその業務の遂行上実施手順を参照する必要がある場合は、その者に対してのみこれを開示することができ、その者はこれに関して守秘義務を負うものとする。

## 第 16 章　委任

16. 1　情報主管課長への委任

（1）情報主管課長への委任

次に掲げる事項については、情報主管課長に委任する。

① 県の組織に関する条例又は規則の改正に伴う本対策基準の規定の整備及び見直し
② 本対策基準別表の整備及び見直し
③ 本対策基準別表に掲げる実施手順の整備及び見直し

附則
本規程は、平成 20 年４月１日から施行する。
附則
本規程は、平成 21 年４月１日から施行する。
附則
本規程は、平成 22 年４月１日から施行する。
附則
本規程は、平成 23 年４月１日から施行する。
附則
本規定は、平成 28 年４月１日から施行する。
附則
本規定は、平成 29 年４月１日から施行する。
附則
本規定は、平成 31 年４月１日から施行する。
附則
本規定は、令和２年４月１日から施行する。
附則
本規定は、令和３年４月１日から施行する。
附則
本規定は、令和４年 10 月 25 日から施行する。
附則
本規定は、令和５年４月１日から施行する。
附則
本規定は、令和５年 10 月 11 日から施行する。
附則
本規定は、令和７年４月１日から施行する。

別表　実施手順

| 大分類 | 小分類 | 実施手順 |
|---|---|---|
| 情報資産 | 分類管理 | 情報資産の分類と管理に関する実施手順<br>（H23.3.31（R7.4.1 最終改正）） |
| | | 電子情報の持ち出しに係る取扱基準<br>（H20.12.1（R5.4.1 最終改正）） |
| 物理的セキュリティ<br>人的セキュリティ | 端末管理 | 情報系パソコン運用管理手順<br>（H22.8.31（H29.11.6 最終改正）） |
| | | 山形県庁イントラ情報システム利用要綱 |

| | | |
|---|---|---|
| 技術的セキュリティ | イントラ情報システム | (H20.8.14（R2.2.1最終改正)) |
| | | 山形県庁イントラ情報システム「サービス利用者の認証」の利用手順<br>(R2.4.1最終改正) |
| | | 山形県庁イントラ情報システム「電子メール」の利用手順<br>(R2.2.1最終改正) |
| | | 山形県庁イントラ情報システム「インターネット」の利用手順<br>(R4.12.22最終改正) |
| | | 山形県庁イントラ情報システム「文書管理」の利用手順<br>(H26.4.1最終改正) |
| | | 山形県庁イントラ情報システム「共有ワークスペース」の利用手順<br>(R2.2.1最終改正) |
| | | イントラ情報システム「セキュアファイル交換」の利用手順<br>(R2.2.1) |
| | | インターネット接続に係る特定通信の利用手順<br>(R2.2.1) |
| | | 仮想ＰＣ運用管理手順<br>(R2.2.1) |
| | ネットワーク管理 | 山形県基幹高速通信ネットワーク外部機関利用要綱<br>(H16.9.10（R3.4.1最終改正)) |
| | | 山形県基幹高速通信ネットワーク外部機関接続要綱<br>(H17.7.1（R3.4.1最終改正)) |
| | テレワーク | テレワークにおける情報セキュリティ対策実施手順<br>(R2.12.14) |
| | | 在宅勤務制度(試行含む)に係るパソコン貸し出し要綱<br>(H29.8.1（R2.1.1最終改正)) |
| | | 山形県サテライトオフィス（試行含む）に係るパソコン貸し出し要綱<br>(R29.8.1（R2.1.1最終改正)) |
| | | リモート接続システム利用要領<br>(R2.1.1（R5.4.1最終改正)) |
| | | 短期モバイル端末貸出要領<br>(H29.9.14（R5.4.1最終改正)) |
| | | 長期モバイル端末貸出要領<br>(H29.8.1（R5.4.1最終改正)) |
| | Web会議サービス | Web会議ツール「Zoom」利用要領<br>(R2.5.12（R5.4.1最終改正)) |
| 障害時の対応 | 情報システムの対応 | 情報資産に関する危機管理方針<br>(H14.3) |
| | | 山形県基幹高速通信ネットワーク障害対応マニュアル<br>(H22.3.30（R3.4.1最終改正)) |

| | | |
|---|---|---|
| 外部サービスの利用 | 外部サービス | 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）に関する実施手順（R7.4.1） |
| | | 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）に関する実施手順（R7.4.1） |
| 評価・見直し | 情報セキュリティ監査 | 山形県情報セキュリティ監査実施要綱（R4.7.11） |

**（参考資料）情報セキュリティポリシー関連規程について**

情報セキュリティの確保のため特に遵守又は参照すべき主な関連規程について、下記に示す。

（1）関連規程のうち、情報主管課が所管するもの

| 大分類 | 小分類 | 関連規程 |
|---|---|---|
| 組織体制 | | 山形県デジタル化推進本部設置要綱<br>（H12.9.26（R2.11.19最終改正）） |
| 情報資産 | 文書管理 | 山形県行政手続等における情報通信の技術の利用に関する条例<br>（H18.12.19） |
| 物理的セキュリティ<br>人的セキュリティ<br>技術的セキュリティ | システム調達 | 山形県情報システム導入標準ガイドライン<br>（R3.4.1（R4.10.25最終改正）） |

（2）関連規程のうち、情報主管課以外が所管するもの

| 大分類 | 小分類 | 関連規程 |
|---|---|---|
| 情報資産 | 情報公開 | 山形県情報公開条例<br>（H9.12.22（R4.12.23最終改正）、総務部） |
| | 個人情報 | 個人情報の保護に関する法律施行条例<br>（R4.12.23、総務部） |
| | 文書管理 | 山形県公文書管理規程<br>（R2.3.27（R5.4.1最終改正）、総務部） |
| | | 文書事務の手引<br>（H7.3.31（R2.11最終改正）、総務部） |
| | | 総合行政ネットワークにおける電子公文書取扱要領<br>（H16.1.6（R2.4.1最終改正）、総務部） |
| | | 電子メール及び電子掲示板を利用した電子文書取扱要領<br>（H16.1.6（R2.4.1最終改正）、総務部） |
| 物理的セキュリティ<br>人的セキュリティ<br>技術的セキュリティ | インシデント対応 | 山形県広報広聴事務取扱要綱<br>（H9.4.1（R5.4.1最終改正）、総務部） |
| 障害時の対応 | 危機管理 | 山形県危機管理要綱<br>（H17.4.1（R4.4.1最終改正）、防災くらし安心部） |
| | | 山形県大規模災害発生時の災害対策本部事務局活動マニュアル<br>（R4.6最終改正、防災くらし安心部） |
| 外部サービスの利用 | ソーシャルメディアサービス | 山形県ソーシャルメディア広報活用ガイドライン<br>（R7.4.1総務部） |
| 違反時の対応 | 懲戒処分 | 懲戒処分の基準（R2.10.1最終改正、総務部）<br>懲戒処分の基準（R2.7.1最終改正、教育委員会） |