

目次

第1編 総則

第1章 本細則の目的・適用範囲（第1条－第4条）

第2章 定義（第5条・第6条）

第2編 情報セキュリティ対策の基本的枠組み

第1章 導入・計画

第1節 組織・体制の整備（第7条－第19条）

第2節 資産管理（第20条）

第3節 情報セキュリティ関係規程の整備（第21条－第23条）

第2章 運用

第1節 情報セキュリティ関係規程の運用（第24条・第25条）

第2節 例外措置（第26条・第27条）

第3節 教育（第28条・第29条）

第4節 情報セキュリティインシデントへの対処（第30条－第33条）

第3章 点検

第1節 情報セキュリティ対策の自己点検（第34条－第36条）

第2節 情報セキュリティ監査（第37条－第39条）

第4章 見直し等（第40条－第43条）

第3編 情報の取扱い

第1章 情報の取扱い（第44条－第51条）

第2章 情報を取り扱う区域の管理（第52条－第54条）

第4編 外部委託

第1章 業務委託

第1節 業務委託（第55条－第58条）

第2節 情報システムに関する業務委託（第59条－第62条）

第2章 クラウドサービス

第1節 クラウドサービスの選定（要機密情報を取り扱う場合）（第63条－第66条）

第2節 クラウドサービスの利用（要機密情報を取り扱う場合）（第67条－第71条）

第3節 クラウドサービスの選定・利用（要機密情報を取り扱わない場合）（第72条・第73条）

第3章 機器等の調達（第74条）

第5編 情報システムのライフサイクル

第1章 情報システムの分類（第75条－第78条）

## 第2章 情報システムのライフサイクルの各段階における対策

第1節 情報システムの企画・要件定義（第79条－第81条）

第2節 情報システムの調達・構築（第82条・第83条）

第3節 情報システムの運用・保守（第84条）

第4節 情報システムの更改・廃棄（第85条）

第5節 情報システムについての対策の見直し（第86条）

## 第3章 情報システムの運用継続計画（第87条）

## 第4章 政府共通利用型システム（第88条－第90条）

## 第6編 情報システムの構成要素

### 第1章 端末

第1節 端末（第91条－第93条）

第2節 要管理対策区域外での端末利用時の対策（第94条・第95条）

第3節 管理運用法人支給以外の端末の導入及び利用時の対策（第96条－第99条）

### 第2章 サーバ装置

第1節 サーバ装置（第100条－第102条）

第2節 電子メール（第103条）

第3節 ウェブ（第104条）

第4節 ドメインネームシステム（DNS）（第105条・第106条）

第5節 データベース（第107条）

### 第3章 複合機・特定用途機器（第108条・第109条）

### 第4章 通信回線

第1節 通信回線（第110条－第112条）

第2節 通信回線装置（第113条－第115条）

第3節 無線LAN（第116条）

第4節 IPv6通信回線（第117条・第118条）

### 第5章 ソフトウェア（第119条・第120条）

### 第6章 アプリケーション・コンテンツ

第1節 アプリケーション・コンテンツの作成・運用時の対策（第121条－第124条）

第2節 アプリケーション・コンテンツ提供時の対策（第125条－第127条）

## 第7編 情報システムのセキュリティ要件

### 第1章 情報システムのセキュリティ機能

第1節 主体認証機能（第128条・第129条）

第2節 アクセス制御機能（第130条）

第3節 権限の管理（第131条）

第4節 ログの取得・管理（第132条）

第5節 暗号・電子署名（第133条・第134条）

第6節 監視機能（第135条）

第2章 情報セキュリティの脅威への対策

第1節 ソフトウェアに関する脆弱性対策（第136条）

第2節 不正プログラム対策（第137条）

第3節 サービス不能攻撃対策（第138条）

第4節 標的型攻撃対策（第139条）

第3章 ゼロトラストアーキテクチャ

第1節 動的なアクセス制御の実装時の対策（第140条－第142条）

第2節 動的なアクセス制御の運用時の対策（第143条・第144条）

第8編 情報システムの利用

第1章 情報システムの利用（第145条－第154条）

第2章 ソーシャルメディアによる情報発信（第155条）

第3章 テレワーク（第156条－第158条）

第9編 雑則（第159条）

附 則

## 第1編 総則

### 第1章 本細則の目的・適用範囲

#### (目的)

第1条 この細則は、政府機関等のサイバーセキュリティ対策のための統一基準群（以下「統一基準群」という。）及び情報セキュリティ管理規程（以下「規程」という。）の規定を実施するため、情報セキュリティ対策の項目ごとに年金積立金管理運用独立行政法人（以下「管理運用法人」という。）が遵守すべき事項を規定することにより、管理運用法人の情報セキュリティ水準の維持向上に資することを目的とする。

#### (適用対象)

第2条 この細則は、全ての役員及び職員（派遣社員を含む。以下「役員等」という。）に対して適用する。

2 この細則の適用対象とする情報は、以下の各号に掲げるものとする。

(1) 役員等が職務上使用することを目的として管理運用法人が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）

(2) 前号に規定するシステム又は外部電磁的記録媒体以外に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）であって、役員等が職務上取り扱う情報

(3) 管理運用法人が調達し、又は開発したシステムの設計又は運用管理に関する情報（前2号に掲げる情報を除く。）

3 この細則の適用対象とする情報システムは、前項に規定する情報を取り扱う全ての情報システムとする。

#### (改正)

第3条 情報セキュリティ水準を適切に維持していくため、統一基準群の改正が行われた場合は、必要に応じ規定内容の追加・修正等の改正を行うものとする。

#### (法令等の遵守)

第4条 役員等は、情報及び情報システムの取扱いに当たって、管理運用法人の情報セキュリティに係る規程類や手順書等を遵守するものとする。情報セキュリティを巡る状況に応じて策定される政府決定等についても同様とする。

### 第2章 定義

(情報の格付の区分・取扱制限)

第5条 情報の格付の区分及び情報の取扱制限については、別表1のとおり定義する。

(用語)

第6条 この細則における用語については、別表2のとおり定義する。

## 第2編 情報セキュリティ対策の基本的枠組み

### 第1章 導入・計画

#### 第1節 組織・体制の整備

(最高情報セキュリティ責任者及び最高情報セキュリティ副責任者)

第7条 組織規程第2条の9第1項に規定する最高情報セキュリティ責任者は、次の各号に掲げる事務のほか、情報セキュリティ関係規程に定める事務を行う。

- (1) 情報セキュリティ対策に関する事務を統括すること。
- (2) 情報セキュリティ対策を適切に実施するための体制を整備すること。
- (3) 情報資産に情報セキュリティインシデントが発生した場合に、再発防止に必要な措置を講ずること。
- (4) その他情報セキュリティ対策に関して必要な調整をすること。

2 管理運用法人は、最高情報セキュリティ責任者を助けて情報セキュリティに関する事務を整理し、統括する最高情報セキュリティ副責任者1人を必要に応じて置くことができる。

(情報セキュリティ委員会)

第8条 組織規程第2条の9第3項に規定する情報セキュリティ委員会（以下「委員会」という。）は、最高情報セキュリティ責任者、審議役、第10条に規定する統括情報セキュリティ責任者及び第11条に規定する情報セキュリティ責任者（監査室長を除く。）により構成する。

2 委員会の委員長は、組織規程第2条の9第4項に基づき最高情報セキュリティ責任者とし、委員長がその議事を進行する。

3 委員長に事故等があるときは、審議役がその職務を代理する。

4 委員長は、コンプライアンス・オフィサー及び監査室長をオブザーバーとして委員会に出席させることができる。

5 委員長は、必要に応じ、説明及び報告を求め、又は事情を聴取するために、委員以外の者を委員会に出席させることができる。

6 委員会は、次に掲げる事項について審議及び議決を行う。

- (1) 対策推進計画に関すること。
- (2) 情報セキュリティ関係規程の整備（軽易なものを除く。）に関すること。
- (3) 規程第14条に規定する情報の格付け及び規程第15条に規定する情報の取扱制限に関すること。

- (4) 規程第7条に規定する例外措置を適用するための対応手順等に関すること。
  - (5) 情報セキュリティインシデントへの対応に関すること。
  - (6) その他委員長が必要と認めること。
- 7 委員会は、委員長が招集する。
  - 8 委員会は、委員長及び委員の半数以上が出席しなければ、委員会を開き、議決することができない。
  - 9 委員会の議事は、出席した委員の過半数をもって決する。可否同数の場合は委員長が決する。
  - 10 前各項に規定するもののほか、委員会の運営に必要な事項は、委員長が別に定めることができる。
  - 11 委員会の事務局は、企画部情報セキュリティ対策課とする。
  - 12 事務局は、委員会の議事概要を作成し、理事長に報告する。
  - 13 委員会の議決事項は、原則として、当該事項の所管部室が起案し、理事長（権限分配細則に基づき、理事長が下位の職位者に権限を委譲している場合には、当該委譲を受けた者）の決裁を得た上で、実施する。
  - 14 議決事項の実施状況は、事務局が確認する。

(情報セキュリティ監査責任者)

第9条 管理運用法人は、規程第11条に規定する情報セキュリティ監査に関する事務を統括する者として情報セキュリティ監査責任者を置く。

- 2 情報セキュリティ監査責任者は、監査室長をもって充てる。

(統括情報セキュリティ責任者)

第10条 管理運用法人は、次条の情報セキュリティ責任者を統括するとともに、最高情報セキュリティ責任者を補佐し情報セキュリティ対策推進体制の責任を担う者として統括情報セキュリティ責任者を置く。

- 2 統括情報セキュリティ責任者は、企画部長をもって充てる。

(情報セキュリティ責任者)

第11条 管理運用法人は、部、室及び事務室における情報セキュリティ対策に関する事務を統括する者として、情報セキュリティ責任者を置く。

- 2 情報セキュリティ責任者は、部、室及び事務室の長をもって充てる。

(区域情報セキュリティ責任者)

第12条 管理運用法人は、情報を取り扱う区域ごとの特性に応じた情報セキュリティ対策に関する事務を統括する者として区域情報セキュリティ責任者を置く。

- 2 区域情報セキュリティ責任者は、全ての区域について総務部長をもって充てる。

(情報セキュリティ管理者)

第13条 管理運用法人は、所管する室、事務室又は課（部の庶務を所掌する課がある場合は、その所属する部とする。）における情報セキュリティ対策に関する事務を行う者として情報セキュリティ管理者を置く。

2 情報セキュリティ管理者は、課長（部の庶務を所掌する課がある部の場合は、当該課の課長とする。）、副室長、副事務室長及びこれに相当する職（これらの職が置かれていない室においては室長、事務室においては事務室長とする。）をもって充てる。

(情報セキュリティ管理補助者)

第14条 情報セキュリティ管理者は、所管する室、事務室又は課に所属する職員のうちから、情報セキュリティ管理補助者を指名し、その事務を担わせることができる。

(情報システムセキュリティ責任者)

第15条 管理運用法人は、部、室及び事務室が所管する情報システムに対する情報セキュリティ対策に関する事務を統括する者として情報システムセキュリティ責任者を置く。

2 情報システムセキュリティ責任者は、情報セキュリティ責任者をもって充てる。

(情報システムセキュリティ管理者)

第16条 管理運用法人は、情報システムセキュリティ責任者を補佐し、所管する情報システムのセキュリティ対策に関する事務を行う者として、情報システムセキュリティ管理者を置く。

2 情報システムセキュリティ管理者は、当該情報システムを所管する情報セキュリティ管理者をもって充てる。

(最高情報セキュリティアドバイザー)

第17条 最高情報セキュリティ責任者は、自らへの助言その他必要な支援を求めるために、情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置くことができる。

(情報セキュリティインシデントに備えた体制の整備)

第18条 管理運用法人は、情報セキュリティインシデントに対処するための体制として、情報セキュリティ委員会の下にS I R Tを置く。

2 S I R Tは、統括情報セキュリティ責任者及び専門的な知識又は適性を有すると認められる職員により構成する。

3 S I R Tに情報セキュリティインシデントに対処するための責任者としてS I R T責任者を置くものとし、統括情報セキュリティ責任者をもって充てる。

4 S I R T責任者は、情報セキュリティインシデントが発生した際には、直ちに最高情報セキュリティ責任者へ報告するものとする。

(兼務を禁止する役割)

第19条 役員等は、情報セキュリティ対策の運用において、以下の役割を兼務することはできない。

- (1) 承認又は許可（以下この条において「承認等」という。）の申請者と当該承認等を行う者（以下「許可権限者」という。）
- (2) 監査を受ける者とその監査を実施する者

2 役員等は、許可権限者が有する職務上の権限等から、当該許可権限者が承認等の可否の判断を行うことが不適切と認められる場合には、当該許可権限者の上司に承認等を申請し、承認を得なければならない。この場合において、当該許可権限者の上司の承認等を得たときは、当該許可権限者の承認等を得ることを要しない。

## 第2節 資産管理

(情報システム台帳の整備)

第20条 統括情報セキュリティ責任者は、全ての情報システムの状況を把握するために、セキュリティ要件に係る事項を含む情報システム台帳を整備しなければならない。

## 第3節 情報セキュリティ関係規程の整備

(リスク評価の実施)

第21条 最高情報セキュリティ責任者は、管理運用法人の目的等を踏まえ、自己点検の結果、情報セキュリティ監査の結果、本部監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを評価するものとする。

(運用規程及び実施手順の策定)

第22条 統括情報セキュリティ責任者は、管理運用法人における情報セキュリティ対策に関する運用規程及び実施手順を整備する。ただし、この細則において整備すべき者を統括情報セキュリティ責任者とは別に定める場合を除く。

- 2 統括情報セキュリティ責任者は、運用規程及び実施手順に関する事務を統括し、整備状況について最高情報セキュリティ責任者に報告するものとする。
- 3 統括情報セキュリティ責任者は、役員等の雇用等の開始、終了及び人事異動時等における情報セキュリティ対策に関する運用規程を整備するものとする。

(対策推進計画の策定)

第23条 最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、対策推進計画を定めるものとする。

## 第2章 運用

### 第1節 情報セキュリティ関係規程の運用

#### (情報セキュリティ対策の運用)

第24条 情報セキュリティ責任者又は情報セキュリティ管理者は、役員等から情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告する。

2 統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて最高情報セキュリティ責任者にその内容を報告する。

#### (違反への対処)

第25条 役員等は、情報セキュリティ関係規程への重大な違反を知った場合は、情報セキュリティ責任者にその旨を報告する。

2 情報セキュリティ責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、統括情報セキュリティ責任者を通じて、最高情報セキュリティ責任者に報告する。

### 第2節 例外措置

#### (例外措置手続の整備)

第26条 最高情報セキュリティ責任者は、例外措置の適用の申請における許可権限者を定めるものとする。

2 統括情報セキュリティ責任者は、例外措置の適用の申請にかかる審査手続を定めるとともに、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求めるとする。

#### (例外措置の運用)

第27条 役員等は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請しなければならない。ただし、業務の遂行に緊急を要し、当該規定の趣旨を十分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出ることとする。

2 許可権限者は、役員等による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定しなければならない。

3 許可権限者は、例外措置の申請状況を台帳に記録し、統括情報セキュリティ責任者に報告するものとする。

- 4 統括情報セキュリティ責任者は、前項の例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告するものとする。

### 第3節 教育

(教育体制の整備・教育実施計画の策定)

第28条 統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備するものとする。なお、教育実施計画については、年度の対策推進計画において計画することで代替できるものとする。

- 2 統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ役員等に対して新たに教育すべき事項が明らかになった場合は、教育実施計画を見直すものとする。

(教育の実施)

第29条 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、教育実施計画に基づき、役員等に対して、情報セキュリティに係る教育を適切に受講させなければならない。

- 2 役員等は、教育実施計画に従って、適切な時期に教育を受講しなければならない。
- 3 統括情報セキュリティ責任者は、情報セキュリティ対策推進体制及びSIRTに属する役員等に教育を適切に受講させなければならない。
- 4 情報セキュリティ管理者は、教育の実施状況を記録し、情報セキュリティ責任者及び統括情報セキュリティ責任者に報告するものとする。
- 5 統括情報セキュリティ責任者は、教育の実施状況を分析、評価し、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告するものとする。

### 第4節 情報セキュリティインシデントへの対処

(情報セキュリティインシデントに備えた事前準備)

第30条 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可能性を認知した際の報告窓口を含む管理運用法人関係者への報告手順を整備し、報告が必要な具体例を含め、役員等に周知するものとする。

- 2 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可能性を認知した際の管理運用法人外との情報共有を含む対処手順を整備するものとする。
- 3 統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段及び連絡内容を含む緊急連絡網を情報システムセキュリティ責任者に整備させるものとする。
- 4 統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、業務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を情報システムセキュリティ責任者に整備させるものとする。

- 5 統括情報セキュリティ責任者は、情報セキュリティインシデントについて管理運用法人外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を管理運用法人外の者に明示するものとする。
- 6 統括情報セキュリティ責任者は、対処手順が適切に機能することを訓練等により確認するものとする。

(情報セキュリティインシデントへの対処)

第31条 役員等は、情報セキュリティインシデントの可能性を認知した場合には、統括情報セキュリティ責任者に報告し、指示に従わなければならない。

- 2 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うものとする。
- 3 S I R T責任者は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責任者に速やかに報告しなければならない。
- 4 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又は勧告を行うものとする。また、S I R T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セキュリティ責任者へ確認を指示するものとする。
- 5 情報システムセキュリティ責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、管理運用法人で定められた対処手順又はS I R Tの指示若しくは勧告に従って、適切に対処しなければならない。
- 6 政府共通利用型システムを利用している情報システムセキュリティ責任者は、認知した情報セキュリティインシデントが政府共通利用型システムに関するものである場合には、当該政府共通利用型システムの情報セキュリティ対策に係る運用管理規程に従い、適切に対処しなければならない。
- 7 S I R Tは、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、警察への通報・連絡等を行うものとする。
- 8 S I R Tは、情報セキュリティインシデントに関する対処状況を把握し、対処全般に関する指示、勧告又は助言を行うものとする。
- 9 S I R Tは、情報セキュリティインシデントに関する対処の内容を記録するものとする。
- 10 S I R Tは、C Y M A Tの支援を受ける場合には、支援を受けるに当たって必要な情報提供を行うものとする。

(情報セキュリティインシデントに係る情報共有)

第32条 S I R T責任者は、管理運用法人の情報システムにおいて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、S I R Tから厚生労働省に連絡させなければならない。ただし、重大な情報セキュリティインシデントと考えられる場合は、直ちに連絡さ

せるものとする。

- 2 SIRTは、情報セキュリティインシデントに関係する可能性がある他の機関等と情報共有を行うものとする。
- 3 SIRT責任者は、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、企画部長に連絡しなければならない。
- 4 企画部長は、前項の連絡を受けた場合、必要に応じて個人情報保護委員会へ報告を行うものとする。

(情報セキュリティインシデントの再発防止・教訓の共有)

第33条 情報セキュリティ責任者は、SIRTから応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として最高情報セキュリティ責任者に報告するものとする。

- 2 最高情報セキュリティ責任者は、情報セキュリティ責任者から情報セキュリティインシデントについての報告を受けた場合には、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するものとする。
- 3 SIRT責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、統括情報セキュリティ責任者、関係する情報セキュリティ責任者等に共有するものとする。

### 第3章 点検

#### 第1節 情報セキュリティ対策の自己点検

(自己点検計画の策定・手順の準備)

第34条 統括情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定するものとする。

- 2 情報セキュリティ責任者は、年度自己点検計画に基づき、役員等ごとの自己点検票及び自己点検の実施手順を整備するものとする。
- 3 統括情報セキュリティ責任者は、情報セキュリティの状況の変化に応じ、役員等に対して新たに点検すべき事項が明らかになった場合は、年度自己点検計画を見直すものとする。

(自己点検の実施)

第35条 情報セキュリティ責任者は、年度自己点検計画に基づき、役員等に自己点検の実施を指示する。

- 2 役員等は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施する。

(自己点検結果の評価・改善)

第36条 情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価する。また、評価結果を統括情報セキュリティ責任者に報告する。

2 統括情報セキュリティ責任者は、管理運用法人に共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価する。また、評価結果を最高情報セキュリティ責任者に報告する。

3 最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、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改善を指示し、改善結果の報告を受けるものとする。

## 第2節 情報セキュリティ監査

### (監査実施計画の策定)

第37条 情報セキュリティ監査責任者は、対策推進計画を踏まえ内部監査実施計画を策定するものとする。

2 情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、内部監査実施計画で計画された以外の監査の実施が必要な場合には、追加の内部監査実施計画を策定するものとする。

### (監査の実施)

第38条 情報セキュリティ監査責任者は、内部監査実施計画に基づき、監査の実施を監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者へ報告する。

### (監査結果に応じた対処)

第39条 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を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指示するものとする。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示するものとする。

2 統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、管理運用法人内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告するものとする。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告するものとする。

3 情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、自らが所管する部、室及び事務室に特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告するものとする。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告するものとする。

## 第4章 見直し等

(情報セキュリティ対策の見直し)

第40条 最高情報セキュリティ責任者は、リスク評価に変化が生じた場合には、情報セキュリティ委員会による審議を経て、この細則又は対策推進計画の必要な見直しを行うものとする。

(情報セキュリティ関係規程等の見直し)

第41条 最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ監査、本部監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、この細則について必要な見直しを行うものとする。

2 統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ監査、本部監査等の結果等を踏まえて情報セキュリティ対策に関する運用規程及び実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告するものとする。

3 統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検、情報セキュリティ監査、本部監査等の結果等を踏まえて管理運用法人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運用見直しについて、管理運用法人内の職制及び職務に応じた措置の実施又は指示をし、措置の結果について最高情報セキュリティ責任者に報告するものとする。

(対策推進計画の見直し)

第42条 最高情報セキュリティ責任者は、情報セキュリティ対策の運用及び自己点検、情報セキュリティ監査、本部監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策推進計画について定期的な見直しを行うものとする。

(情報セキュリティ対策における厚生労働省との連携)

第43条 最高情報セキュリティ責任者は、情報セキュリティ対策を適切に推進するため、厚生労働省と密接な連携を要する事項や専門的知見を要する事項について、厚生労働省へ助言を求めるものとする。

## 第3編 情報の取扱い

### 第1章 情報の取扱い

(情報の取扱いに係る規定の整備)

第44条 統括情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用規程を整備し、役員等へ周知するものとする。

- (1) 情報の格付及び取扱制限についての定義
- (2) 情報の格付及び取扱制限の明示等についての手続
- (3) 情報の格付及び取扱制限の継承、見直しに関する手続

(情報の目的外での利用等の禁止)

第45条 役員等は、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用等しなければならない。

(情報の格付及び取扱制限の決定・明示等)

第46条 役員等は、情報の作成時及び管理運用法人外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等する。

- 2 役員等は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。
- 3 役員等は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下「決定者等」という。）を確認し、その結果に基づき見直す。

(情報の利用・保存)

第47条 役員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱わなければならない。

- 2 役員等は、機密性3情報について要管理対策区域外で情報処理を行う場合は、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なければならない。
- 3 役員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずる。
- 4 役員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理する。
- 5 役員等は、秘密文書（電子文書に限る。次項において同じ。）を保存する場合は、インターネットからの侵入に対する多重防御による情報セキュリティ対策が施された電子計算機において行わなければならない。
- 6 役員等は、秘密文書のうち総括文書管理者が指定するものを機器等に保存する場合は、前項の規定にかかわらず、以下の措置を講じなければならない。
  - (1) インターネット及びインターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用する。
  - (2) 暗号化による保護を行う。
  - (3) 当該文書を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずる。

7 役員等は、USBメモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従う。

#### (情報の提供・公表)

第48条 役員等は、情報を公表する場合には、当該情報が機密性1情報に格付されるものであることを確認しなければならない。

2 役員等は、閲覧制限の範囲外の者に情報を提供する必要がある場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うものとする。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずるものとする。

3 役員等は、機密性3情報を閲覧制限の範囲外の者に提供する場合には、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なければならない。

4 役員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講ずるものとする。

#### (情報の運搬・送信)

第49条 役員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずるものとする。特に、役員等が、機密性3情報を要管理対策区域外に持ち出す場合には、暗号化措置を施した上で、統括情報セキュリティ責任者が指定する方法により運搬しなければならない。ただし、他機関等の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域とみなすことができる。

2 役員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずるものとする。役員等が、機密性3情報を管理運用法人外通信回線（インターネットを除く。）を使用して送信する場合には、暗号化措置を施した上で、統括情報セキュリティ責任者が指定する方法により送信しなければならない。

#### (情報の消去)

第50条 役員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去する。

2 役員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消する。

3 役員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にしなければならない。

(情報のバックアップ)

第51条 役員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施する。

- 2 役員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理する。
- 3 役員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄する。

## 第2章 情報を取り扱う区域の管理

(要管理対策区域における対策の基準の決定)

第52条 統括情報セキュリティ責任者は、要管理対策区域の範囲を定めるものとする。

- 2 統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を全て含む対策の基準を運用規程として定めるものとする。
  - (1) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。
  - (2) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。

(区域ごとの対策の決定)

第53条 区域情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定めるものとする。

- 2 区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定するものとする。

(要管理対策区域における対策の実施)

第54条 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施する。役員等が実施すべき対策については、役員等が認識できる措置を講ずる。

- 2 区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずる。
- 3 役員等は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用する。また、役員等が管理運用法人外の者を立ち入らせる際には、当該管理運用法人外の者にも当該区域で定められた対策に従って利用させる。

## 第4編 外部委託

### 第1章 業務委託

#### 第1節 業務委託

(業務委託に係る運用規程の整備)

第55条 統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備するものとする。

- (1) 委託先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) 委託先の選定基準

(業務委託実施前の対策)

第56条 情報システムセキュリティ責任者又は情報セキュリティ管理者は、業務委託の実施までに、以下に掲げる全ての事項を実施する。

- (1) 委託する業務内容の特定
- (2) 委託先の選定条件を含む仕様の策定
- (3) 仕様に基づく委託先の選定
- (4) 契約の締結
- (5) 委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

2 情報システムセキュリティ責任者又は情報セキュリティ管理者は、業務委託の実施までに、委託の前提条件として、以下に掲げる全ての事項の実施を委託先に求める。

- (1) 仕様に準拠した提案
- (2) 契約の締結
- (3) 委託先において要機密情報を取り扱う場合は、秘密保持契約（NDA）の締結

(業務委託実施期間中の対策)

第57条 情報システムセキュリティ責任者又は情報セキュリティ管理者は、業務委託の実施期間において以下に掲げる全ての対策を実施する。

- (1) 委託判断基準に従った要保護情報の提供
- (2) 契約に基づき委託先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
- (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役員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

2 情報システムセキュリティ責任者又は情報セキュリティ管理者は、業務委託の実施期間において以下に掲げる全ての対策の実施を委託先に求める。

- (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) 契約に基づき委託先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

(業務委託終了時の対策)

第58条 情報システムセキュリティ責任者又は情報セキュリティ管理者は、業務委託の終了に際して以下に掲げる全ての対策を実施する。

- (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) 委託先に提供した情報を含め、委託先において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

2 情報システムセキュリティ責任者又は情報セキュリティ管理者は、契約に基づき、業務委託の終了に際して以下に掲げる全ての対策の実施を委託先に求める。

- (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

## 第2節 情報システムに関する業務委託

(情報システムに関する業務委託における共通的対策)

第59条 情報システムセキュリティ責任者は、情報システムに関する業務委託の実施までに、委託先の選定条件に情報システムに管理運用法人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加え、仕様を策定するものとする。

(情報システムの構築を業務委託する場合の対策)

第60条 情報システムセキュリティ責任者は、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先に求める。

- (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

(情報システムの運用・保守を業務委託する場合の対策)

第61条 情報システムセキュリティ責任者は、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、委託先に実施を求める。

2 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先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、委託先に速やかな報告を求める。

(管理運用法人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)

第62条 情報システムセキュリティ責任者又は情報セキュリティ管理者は、管理運用法人外の一般の者が管理運用法人向けに要機密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、委託先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。

- 2 情報システムセキュリティ責任者又は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に応じてセキュリティ要件を定め、業務委託サービスを選定する。また、業務委託サービスのセキュリティ要件としてセキュリティに係る国際規格（ISO/IEC 27000ファミリーによるISMS認証の国際規格）等と同等以上の水準を求める。
- 3 情報システムセキュリティ責任者又は情報セキュリティ管理者は、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、業務委託先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。
- 4 情報システムセキュリティ責任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へ当該サービスの利用申請を行う。
- 5 統括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、利用の可否を決定する。
- 6 統括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、当該業務委託サービスの責任者として情報セキュリティ責任者を指名する。

## 第2章 クラウドサービス

### 第1節 クラウドサービスの選定（要機密情報を取り扱う場合）

（クラウドサービスの選定に係る運用規程の整備）

第63条 統括情報セキュリティ責任者は、以下を全て含むクラウドサービス（要機密情報を取り扱う場合）の選定に関する運用規程を整備するものとする。

- (1) クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「クラウドサービス利用判断基準」という。）
- (2) クラウドサービスの選定基準
- (3) クラウドサービスの利用申請の許可権限者と利用手続
- (4) クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

（クラウドサービスの選定）

第64条 情報システムセキュリティ責任者又は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、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する。

- 2 情報システムセキュリティ責任者又は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並びにクラウドサービス提供者との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。

- (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
- 3 情報システムセキュリティ責任者又は情報セキュリティ管理者は、特段の理由がない限り、「ISMAP等クラウドサービスリスト」から利用するクラウドサービスを選定する。ただし、リストに記載されていても業務の特性により必要な統制が不足していることも考えられるため、「言明の対象範囲」及び「基本言明要件のうち実施している統制目標の管理策」等に留意する。

(クラウドサービスの利用に係る調達)

第65条 情報システムセキュリティ責任者又は情報セキュリティ管理者は、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る。

- 2 情報システムセキュリティ責任者又は情報セキュリティ管理者は、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締結までに確認し、利用承認を得る。また、調達仕様の内容は、契約に含める。なお、調達仕様の内容を契約に含める際、クラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲が明確になっていることを確認する。

(クラウドサービスの利用承認)

第66条 情報システムセキュリティ責任者又は情報セキュリティ管理者は、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う。

- 2 統括情報セキュリティ責任者は、前項におけるクラウドサービスの利用申請を審査し、利用の可否を決定する。
- 3 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承認した場合は、承認済みクラウドサービスとして記録し、当該クラウドサービスの責任者として情報セキュリティ責任者又は情報セキュリティ管理者を指名する。

## 第2節 クラウドサービスの利用（要機密情報を取り扱う場合）

(クラウドサービスの利用に係る運用規程の整備)

第67条 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導入・構築する際のセキュリティ対策の基本方針を運用規程として整備するものとする。

- 2 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備するものとする。
- 3 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用

規程として整備するものとする。

- (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

(クラウドサービスの利用に係るセキュリティ要件の策定)

第68条 クラウドサービスの責任者に指名された情報セキュリティ責任者又は情報セキュリティ管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、前条各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係る内容を確認する。

- 2 クラウドサービスの責任者に指名された情報セキュリティ責任者又は情報セキュリティ管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、前条各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係るセキュリティ要件を策定する。

(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)

第69条 クラウドサービスの責任者に指名された情報セキュリティ責任者又は情報セキュリティ管理者は、第67条第1項で定めた運用規程を踏まえて、前条第2項において定めるセキュリティ要件に従いクラウドサービス利用における必要な措置を講ずる。また、導入・構築時に実施状況を確認・記録する。

- 2 クラウドサービスの責任者に指名された情報セキュリティ責任者又は情報セキュリティ管理者は、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する。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告する。
- 3 クラウドサービスの責任者に指名された情報セキュリティ責任者又は情報セキュリティ管理者は、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するものとする。
  - (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

(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)

第70条 クラウドサービスの責任者に指名された情報セキュリティ責任者又は情報セキュリティ管理者は、第67条第2項で定めた運用規程を踏まえて、クラウドサービスに係る運用・保守を適切に実施する。また、運用・保守時に実施状況を定期的に確認・記録する。

- 2 クラウドサービスの責任者に指名された情報セキュリティ責任者又は情報セキュリティ管理者

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する。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する。

- 3 クラウドサービスの責任者に指名された情報セキュリティ責任者又は情報セキュリティ管理者は、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、必要な措置を講ずるものとする。

(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)

第71条 クラウドサービスの責任者に指名された情報セキュリティ責任者又は情報セキュリティ管理者は、第67条第3項で定めた運用規程を踏まえて、更改・廃棄時の必要な措置を講ずる。また、クラウドサービスの利用終了時に実施状況を確認・記録する。

### 第3節 クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

(要機密情報を取り扱わない場合のクラウドサービスの利用に係る運用規程の整備)

第72条 統括情報セキュリティ責任者は、以下を全て含むクラウドサービス（要機密情報を取り扱わないものに限る。）の利用に関する運用規程を整備するものとする。

- (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) クラウドサービス管理者の指名とクラウドサービスの利用状況の管理
- (4) クラウドサービスの利用の運用規程

(要機密情報を取り扱わない場合のクラウドサービスの利用における対策の実施)

第73条 役員等は、要機密情報を取り扱わないことを前提としたクラウドサービスを利用する場合、利用するサービスの定型約款、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統括情報セキュリティ責任者へ要機密情報を取り扱わない場合のクラウドサービスの利用を申請する。

- 2 統括情報セキュリティ責任者は、利用するクラウドサービスの定型約款、その他の提供条件等から、役員等による利用に当たってのリスクが許容できることの確認結果を踏まえて、クラウドサービスの利用申請を審査し、利用の可否を決定する。
- 3 統括情報セキュリティ責任者は、要機密情報を取り扱わないクラウドサービスの利用申請を承認した場合は、当該クラウドサービスの責任者として情報セキュリティ管理者を指名し、承認したクラウドサービスを記録する。
- 4 クラウドサービスの責任者に指名された情報セキュリティ管理者は、要機密情報を取り扱わないクラウドサービスを安全に利用するための適切な措置を講ずる。

## 第3章 機器等の調達

(機器等の調達に係る運用規程の整備)

第74条 統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備するものとする。その際、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管理がなされ、その管理を管理運用法人が確認できることを加えるものとする。

2 統括情報セキュリティ責任者は、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・検査手続を整備するものとする。

## 第5編 情報システムのライフサイクル

### 第1章 情報システムの分類

(情報システムにおける分類のための運用規程の整備)

第75条 統括情報セキュリティ責任者は、情報システムの情報セキュリティインシデント発生時の業務影響度等を踏まえ、高度な情報セキュリティ対策が要求される情報システムを判別するための基準である情報システムの分類基準を運用規程として整備するものとする。

(情報システムの分類基準に基づいた情報セキュリティ対策に係る運用規程の整備)

第76条 統括情報セキュリティ責任者は、情報システムに求める分類基準に応じた情報システムのセキュリティ要件及び情報システムの構成要素ごとの情報セキュリティ対策の具体的な対策事項を運用規程として整備するものとする。

(情報システムの分類基準に基づいた分類の実施)

第77条 統括情報セキュリティ責任者は、情報システムの分類基準に基づいた情報システムの分類を情報システムセキュリティ責任者に実施させ、実施した結果を報告させる。情報システムセキュリティ責任者から報告を受けた情報システムの分類結果については、情報セキュリティインシデント発生時の業務影響度や脅威動向等を踏まえて、上位又は下位の情報システムの分類の適用が望ましい場合には修正の指示を行う。

(情報システムの分類基準と情報セキュリティ対策の具体的な対策事項の運用規程の見直し)

第78条 統括情報セキュリティ責任者は、情報システムの分類基準と分類基準に応じた情報セキュリティ対策の具体的な対策事項の運用規程について、定期的な確認による見直しをするものとする。

2 統括情報セキュリティ責任者は、全ての情報システムが分類基準に基づいて適切に分類が行われていることを定期的に確認する。

### 第2章 情報システムのライフサイクルの各段階における対策

## 第1節 情報システムの企画・要件定義

### (実施体制の確保)

第79条 情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、最高情報セキュリティ責任者に求める。

2 最高情報セキュリティ責任者は、前項で求められる体制の確保に際し、組織規程第2条の7に規定するデジタル統括責任者の協力を得ることが必要な場合は、デジタル統括責任者に当該体制の全部又は一部の整備を求める。

### (情報システムの分類基準に基づいた分類の実施)

第80条 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、情報システムの分類基準に基づいて情報システムの分類を行い、統括情報セキュリティ責任者に報告する。

### (情報システムのセキュリティ要件の策定)

第81条 情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等を勘案し情報システムの分類に基づき、情報システムに求める分類基準に応じた具体的な対策事項を踏まえて、以下の全ての事項を含む情報システムのセキュリティ要件を策定する。

- (1) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件
- (2) 情報システム運用時の監視等の運用管理機能要件（監視するデータが暗号化されている場合は、必要に応じて復号する。）
- (3) 情報システムに関連する脆弱性及び不正プログラムについての対策要件
- (4) 情報システムの可用性に関する対策要件
- (5) 情報システムのネットワーク構成に関する要件

2 情報システムセキュリティ責任者は、インターネット回線と接続する情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定する。

3 情報システムセキュリティ責任者は、機器等を調達する場合には、「IT製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定する。

4 情報システムセキュリティ責任者は、構築する情報システムが取り扱う情報や情報システムを利用して行う業務の内容等を踏まえ高度な情報セキュリティ対策を要求する情報システムについては、情報システムの分類に応じて策定したセキュリティ要件について、最高情報セキュリティアドバイザー等へ助言を求め、業務の特性や情報システムの特性を踏まえて、上位の情報セキュ

リティ対策をセキュリティ要件として盛り込む必要性を確認する。

## 第2節 情報システムの調達・構築

(情報システムの構築時の対策)

第82条 情報システムセキュリティ責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずる。

- 2 情報システムセキュリティ責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずる。
- 3 情報システムセキュリティ責任者は、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する。
- 4 情報システムセキュリティ責任者は、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。
  - (1) 情報システムを構成するサーバ装置及び端末関連情報
  - (2) 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
- 5 情報システムセキュリティ責任者は、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する。
  - (1) 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
  - (2) 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) 情報システムが停止した際の復旧手順

(納品検査時の対策)

第83条 情報システムセキュリティ責任者は、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、調達仕様書等に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する。

- 2 情報システムセキュリティ責任者は、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き継がれる項目に、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する。

## 第3節 情報システムの運用・保守

(情報システムの運用・保守時の対策)

第84条 情報システムセキュリティ責任者は、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する。

- 2 情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、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、必要に応じて見直す。

- 3 情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システム台帳及び関連文書の内容に変更が生じた場合、情報システム台帳及び関連文書を更新し、又は修正する。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する。
- 4 情報システムセキュリティ責任者は、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、必要な措置を講ずる。
- 5 情報システムセキュリティ責任者は、要安定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する。

#### 第4節 情報システムの更改・廃棄

(情報システムの更改・廃棄時の対策)

第85条 情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下を全て含む措置を適切に講ずる。

- (1) 情報システム更改時の情報の移行作業における情報セキュリティ対策
- (2) 情報システム廃棄時の不要な情報の抹消

#### 第5節 情報システムについての対策の見直し

(情報システムについての対策の見直し)

第86条 情報システムセキュリティ責任者は、対策推進計画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すものとする。

- 2 情報システムセキュリティ責任者は、管理運用法人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統括情報セキュリティ責任者からの改善指示に基づき、情報セキュリティ対策を適切に見直すものとする。また、措置の結果については、統括情報セキュリティ責任者へ報告するものとする。

### 第3章 情報システムの運用継続計画

(情報システムの運用継続計画の整備・整合的運用の確保)

第87条 統括情報セキュリティ責任者及び情報システムセキュリティ責任者は、管理運用法人において非常時優先業務を支える情報システムの運用継続計画を整備する場合は、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順の整備を検討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セキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順が運用可能であることを定期的に確認しなければならない。
- 3 統括情報セキュリティ責任者及び情報システムセキュリティ責任者は、情報システムの運用継続計画に沿って、危機的事象発生時における情報セキュリティに係る対策事項、運用規程及び実施手順を定期的に見直さなければならない。

#### 第4章 政府共通利用型システム

##### (政府共通利用型システム利用機関における体制の整備)

第88条 情報システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程に応じた体制の確保を、最高情報セキュリティ責任者に求める。

- 2 統括情報セキュリティ責任者は、政府共通利用型システムが提供する機器等の提供を受けこれを管理運用法人の役員等が利用する場合は、当該利用に係る情報セキュリティ対策に関する事務を統括する管理者として、政府共通利用型システムごとに政府共通利用型システム利用管理者を指名する。
- 3 政府共通利用型システム利用管理者は、当該政府共通利用型システムの利用に際し、当該政府共通利用型システム管理機関が定める運用管理規程に応じた体制の確保を、最高情報セキュリティ責任者に求める。

##### (政府共通利用型システム利用機関における情報セキュリティ対策)

第89条 情報システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムの情報セキュリティ水準を低下させることのないように、適切にセキュリティ要件を策定し、運用する。

- 2 情報システムセキュリティ責任者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処する。

##### (政府共通利用型システム利用機関における機器等の管理)

第90条 政府共通利用型システム利用管理者は、政府共通利用型システムが提供する機器等の提供を受けてこれを管理運用法人の役員等が利用する場合は、当該政府共通利用型システムの利用に関する情報セキュリティ対策に係る運用規程及び実施手順を整備するものとする。

- 2 政府共通利用型システム利用管理者は、提供を受けた政府共通利用型システムの機器等を把握するために必要な文書を整備する。
- 3 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が情報システム台帳や情報システム関連文書を整備するために必要な情報について、政府共通利用型システム管理機

関に提供するとともに、当該情報に変更が生じた場合は速やかに通知する。

- 4 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処する。

## 第6編 情報システムの構成要素

### 第1章 端末

#### 第1節 端末

##### (端末の導入時の対策)

- 第91条 情報システムセキュリティ責任者は、要保護情報を取り扱う物理的な端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずるものとする。
- 2 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより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、端末で利用を認めるソフトウェアを定め、それ以外のソフトウェアを役員等に利用させてはならない。
  - 3 情報システムセキュリティ責任者は、端末に接続を認める機器等を定め、接続を認めた機器等以外を役員等には接続させてはならない。
  - 4 情報システム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内容に従い、端末に対して適切なセキュリティ対策を実施するものとする。
  - 5 情報システムセキュリティ責任者は、端末において利用するソフトウェアに関連する公開された脆弱性について対策を実施するものとする。

##### (端末の運用時の対策)

- 第92条 情報システムセキュリティ責任者は、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う。
- 2 情報システムセキュリティ責任者は、その管理する端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図る。

##### (端末の運用終了時の対策)

- 第93条 情報システムセキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消しなければならない。

#### 第2節 要管理対策区域外での端末利用時の対策

##### (役員等が要管理対策区域外で使用する端末の導入及び使用に係る運用規程の整備)

- 第94条 統括情報セキュリティ責任者は、役員等が管理運用法人が支給する物理的な端末を用いて

要保護情報を取り扱う場合（要管理対策区域外で使用する場合に限る。）について、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めるものとする。

- 2 統括情報セキュリティ責任者は、要機密情報を取り扱う管理運用法人が支給する物理的な端末を使用する場合（要管理対策区域外で使用する場合に限る。）について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置に関する運用規程を整備するものとする。
- 3 統括情報セキュリティ責任者は、要管理対策区域外において管理運用法人外通信回線に接続した管理運用法人が支給する物理的な端末を管理運用法人内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から管理運用法人内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた技術的な措置に関する運用規程を定めるものとする。

（役員等が要管理対策区域外で使用する端末の導入及び使用時の対策）

第95条 情報システムセキュリティ責任者は、役員等が管理運用法人が支給する物理的な端末（要管理対策区域外で使用する場合に限る。）を用いて要機密情報を取り扱う場合は、当該端末について前条第2項の技術的な措置を講ずるものとする。

- 2 情報システムセキュリティ責任者は、要管理対策区域外において管理運用法人外通信回線に接続した管理運用法人が支給する物理的な端末を管理運用法人内通信回線に接続させる際、当該端末について前条第3項の技術的な措置を講ずるものとする。

### 第3節 管理運用法人支給以外の端末の導入及び利用時の対策

（管理運用法人支給以外の端末の利用可否の判断）

第96条 最高情報セキュリティ責任者は、管理運用法人支給以外の端末の利用について、取り扱うこととなる情報の格付及び取扱制限、管理運用法人が講じる安全管理措置、当該端末の管理は管理運用法人ではなくその所有者が行うこと等を踏まえ、求められる情報セキュリティの水準の達成の見込みを勘案し、管理運用法人における管理運用法人支給以外の端末の利用の可否を判断しなければならない。

（管理運用法人支給以外の端末の利用に関する運用規程等の整備）

第97条 統括情報セキュリティ責任者は、役員等が管理運用法人支給以外の端末を用いて管理運用法人の業務に係る情報処理を行う場合の許可等の手続を実施手順として定めるものとする。

- 2 統括情報セキュリティ責任者は、役員等が管理運用法人支給以外の端末を用いて要保護情報を取り扱う場合について、盗難、紛失、不正プログラムの感染等により情報窃取されるなどのリスクを踏まえた利用手順及び許可手続を実施手順として定めるものとする。
- 3 統括情報セキュリティ責任者は、要機密情報を取り扱う管理運用法人支給以外の端末につい

て、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置を含めた安全管理措置に関する運用規程を整備するものとする。

- 4 統括情報セキュリティ責任者は、要管理対策区域外において管理運用法人外通信回線に接続した管理運用法人支給以外の端末を管理運用法人内通信回線に接続することについての可否を判断した上で、可と判断する場合は、当該端末から管理運用法人内通信回線を経由して情報システムが不正プログラムに感染するリスクを踏まえた安全管理措置に関する運用規程及び許可手続に関する実施手順を定めるものとする。

(管理運用法人支給以外の端末の利用に関する責任者の策定)

第98条 統括情報セキュリティ責任者は、管理運用法人支給以外の端末を用いた管理運用法人の業務に係る情報処理に関する安全管理措置の実施状況を管理する責任者（以下「端末管理責任者」という。）を定める。

(管理運用法人支給以外の端末の利用時の対策)

第99条 役員等は、管理運用法人支給以外の端末を用いて管理運用法人の業務に係る情報処理を行う場合には、端末管理責任者の許可を得なければならない。

- 2 役員等は、管理運用法人支給以外の端末を用いて要保護情報を取り扱う場合は、第97条第2項で定める利用手順に従うものとする。
- 3 端末管理責任者等は、要機密情報を取り扱う管理運用法人支給以外の端末について、第97条第3項に定める安全管理措置を講じるものとする。
- 4 役員等は、情報処理の目的を完了した場合は、要保護情報を管理運用法人支給以外の端末から消去しなければならない。

## 第2章 サーバ装置

### 第1節 サーバ装置

(サーバ装置の導入時の対策)

第100条 情報システムセキュリティ責任者は、要保護情報を取り扱う物理的なサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずるものとする。

- 2 情報システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保するものとする。
- 3 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより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、サーバ装置で利用を認めるソフトウェアを定め、それ以外のソフトウェアを役員等に利用させてはならない。
- 4 情報システムセキュリティ責任者は、サーバ装置に接続を認めた機器等を定め、接続を認めた

機器等以外を役員等に接続させてはならない。

- 5 情報システム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内容に従い、サーバ装置に対して適切なセキュリティ対策を実施する。
- 6 情報システムセキュリティ責任者は、サーバ装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施する。
- 7 情報システムセキュリティ責任者は、要安定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する。

(サーバ装置の運用時の対策)

第101条 情報システムセキュリティ責任者は、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う。

- 2 情報システムセキュリティ責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図る。
- 3 情報システムセキュリティ責任者は、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ずる。
- 4 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、危機的事象発生時に適切な対処が行えるよう運用をする。

(サーバ装置の運用終了時の対策)

第102条 情報システムセキュリティ責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消しなければならない。

## 第2節 電子メール

(電子メールの導入時の対策)

第103条 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定する。

- 2 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備える。
- 3 情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずる。
- 4 情報システムセキュリティ責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講ずる。

## 第3節 ウェブ

(ウェブサーバの導入・運用時の対策)

第104条 情報システムセキュリティ責任者は、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する。

- 2 情報システムセキュリティ責任者は、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ずる。
- 3 情報システムセキュリティ責任者は、ウェブコンテンツの編集作業を行う主体を限定する。
- 4 情報システムセキュリティ責任者は、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る。

#### 第4節 ドメインネームシステム（DNS）

##### （DNSの導入時の対策）

第105条 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講ずる。

- 2 情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずる。
- 3 情報システムセキュリティ責任者は、コンテンツサーバにおいて、管理運用法人のみで使用する名前解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずる。

##### （DNSの運用時の対策）

第106条 情報システムセキュリティ責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持する。

- 2 情報システムセキュリティ責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的を確認する。
- 3 情報システムセキュリティ責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずる。

#### 第5節 データベース

##### （データベースの導入・運用時の対策）

第107条 情報システムセキュリティ責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行う。

- 2 情報システムセキュリティ責任者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずる。
- 3 情報システムセキュリティ責任者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずる。
- 4 情報システムセキュリティ責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずる。

- 5 情報システムセキュリティ責任者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をする。

### 第3章 複合機・特定用途機器

#### (複合機)

第108条 情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定する。

- 2 情報システムセキュリティ責任者は、複合機が備える機能について適切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ずる。
- 3 情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消しなければならない。

#### (IoT機器を含む特定用途機器)

第109条 情報システムセキュリティ責任者は、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脅威が存在する場合には、当該機器の特性に応じた対策を講ずる。

### 第4章 通信回線

#### 第1節 通信回線

#### (通信回線の導入時の対策)

第110条 情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずる。

- 2 情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設ける。
- 3 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずる。
- 4 情報システムセキュリティ責任者は、役員等が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずる。管理運用法人内通信回線へ管理運用法人支給以外の端末を接続する際も同様とする。
- 5 情報システムセキュリティ責任者は、要安定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、当該通信回線の継続的な運用を可能とするための措置を講ずる。

(管理運用法人外通信回線の接続時の対策)

第111条 情報システムセキュリティ責任者は、管理運用法人内通信回線にインターネット回線、公衆通信回線等の管理運用法人外通信回線を接続する場合には、管理運用法人内通信回線及び当該管理運用法人内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずる。

- 2 情報システムセキュリティ責任者は、管理運用法人内通信回線と管理運用法人外通信回線との間及び管理運用法人内通信回線内の不正な通信の有無を監視するための措置を講ずる。
- 3 情報システムセキュリティ責任者は、保守又は診断のために、管理運用法人外通信回線から管理運用法人内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する。
- 4 情報システムセキュリティ責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておく。

(通信回線の運用時の対策)

第112条 情報システムセキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の確認及び見直しを行う。

- 2 情報システムセキュリティ責任者は、管理運用法人内通信回線と管理運用法人外通信回線との間及び管理運用法人内通信回線内の不正な通信の有無を監視するための監視対象や監視方法等について、定期的な確認による見直しをする。
- 3 情報システムセキュリティ責任者は、保守又は診断のために、管理運用法人外通信回線から管理運用法人内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対策について、定期的な確認による見直しをする。
- 4 情報システムセキュリティ責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更する。

## 第2節 通信回線装置

(通信回線装置の導入時の対策)

第113条 情報システムセキュリティ責任者は、物理的な通信回線装置を設置する場合、第三者による破壊や不正な操作等が行われないようにする。

- 2 情報システム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る。
- 3 情報システム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

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する。

- 4 情報システムセキュリティ責任者は、通信回線装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施する。

(通信回線装置の運用時の対策)

第114条 情報システムセキュリティ責任者は、通信回線装置の運用・保守に関わる作業等により通信回線装置の設定変更等を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管する。

- 2 情報システムセキュリティ責任者は、要安定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。
- 3 情報システム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の状態等を調査し、認識した脆弱性等について対策を講ずる。

(通信回線装置の運用終了時の対策)

第115条 情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずる。

### 第3節 無線LAN

(無線LAN環境導入時の対策)

第116条 情報システムセキュリティ責任者は、無線LAN技術を利用して管理運用法人内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずる。

### 第4節 IPv6通信回線

(IPv6通信を行う情報システムに係る対策)

第117条 情報システムセキュリティ責任者は、IPv6技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Programに基づくPhase-2準拠製品を、可能な限り選択する。

- 2 情報システムセキュリティ責任者は、IPv6通信の特性等を踏まえ、IPv6通信を想定して構築する情報システムにおいて、IPv6通信による情報セキュリティ上の脅威又は脆弱性に対する検討を行い、必要な措置を講ずる。

(意図しない I P v 6 通信の抑止・監視)

第118条 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置を、I P v 6 通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外の I P v 6 通信パケットが到達する脅威等、当該通信回線から受ける不正な I P v 6 通信による情報セキュリティ上の脅威を防止するため、I P v 6 通信を抑止するなどの措置を講ずる。

## 第5章 ソフトウェア

(情報システムの基盤を管理又は制御するソフトウェア導入時の対策)

第119条 情報システムセキュリティ責任者は、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ずる。

2 情報システムセキュリティ責任者は、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する。

- (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の情報セキュリティ水準の維持に関する手順
- (2) 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

(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)

第120条 情報システムセキュリティ責任者は、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する。

- (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のセキュリティを維持するための対策
- (2) 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

## 第6章 アプリケーション・コンテンツ

### 第1節 アプリケーション・コンテンツの作成・運用時の対策

(アプリケーション・コンテンツの作成に係る運用規程の整備)

第121条 統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に管理運用法人外の情報セキュリティ水準の低下を招く行為を防止するための運用規程を整備するものとする。

(アプリケーション・コンテンツのセキュリティ要件の策定)

第122条 情報システムセキュリティ責任者は、管理運用法人外の情報システム利用者の情報セキ

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・コンテンツについてのセキュリティ要件を定め、仕様に含める。

- 2 役員等は、アプリケーション・コンテンツの開発・作成を業務委託する場合において、前項に規定する内容を調達仕様に含める。

(アプリケーション・コンテンツの開発時の対策)

第123条 情報システムセキュリティ責任者は、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ずる。

(アプリケーション・コンテンツの運用時の対策)

第124条 情報システムセキュリティ責任者は、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す。

- 2 情報システムセキュリティ責任者は、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ずる。
- 3 情報システムセキュリティ責任者は、ウェブアプリケーションやウェブコンテンツにおいて、アプリケーションやコンテンツの改ざんを検知するための措置を講ずる。

## 第2節 アプリケーション・コンテンツ提供時の対策

(政府ドメイン名の使用)

第125条 情報システムセキュリティ責任者は、管理運用法人外向けに提供するウェブサイト等が実際の管理運用法人提供のものであることを利用者が確認できるように、政府ドメイン名を取得できない場合を除き政府ドメイン名を情報システムにおいて使用する。

- 2 役員等は、管理運用法人外向けに提供するウェブサイト等の作成を業務委託する場合においては、管理運用法人に適するドメイン名を使用するよう調達仕様に含める。

(不正なウェブサイトへの誘導防止)

第126条 情報システムセキュリティ責任者は、利用者が検索サイト等を経由して管理運用法人のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずる。

(アプリケーション・コンテンツの告知)

第127条 役員等は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずる。

- 2 役員等は、管理運用法人外の者が提供するアプリケーション・コンテンツを告知する場合は、告知するURL等の有効性を保つようにする。

## 第7編 情報システムのセキュリティ要件

### 第1章 情報システムのセキュリティ機能

#### 第1節 主体認証機能

##### (主体認証機能の導入)

第128条 情報システムセキュリティ責任者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設ける。

- 2 情報システムセキュリティ責任者は、国民・企業と管理運用法人との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定する。
- 3 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずる。

##### (識別コード及び主体認証情報の管理)

第129条 情報システムセキュリティ責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずる。

- 2 情報システムセキュリティ責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずる。

#### 第2節 アクセス制御機能

##### (アクセス制御機能の導入)

第130条 情報システムセキュリティ責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設ける。

- 2 情報システムセキュリティ責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用する。

#### 第3節 権限の管理

##### (権限の管理)

第131条 情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を必要最小限の範囲で適切に設定するよう、措置を講ずる。

- 2 情報システムセキュリティ責任者は、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ずる。

- 3 情報システムセキュリティ責任者は、主体から対象に対する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する。

#### 第4節 ログの取得・管理

(ログの取得・管理)

第132条 情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得する。

- 2 情報システムセキュリティ責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法等について定め、適切にログを管理する。
- 3 情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、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する。

#### 第5節 暗号・電子署名

(暗号化機能・電子署名機能の導入)

第133条 情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の全ての措置を講ずる。

- (1) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めるときは、当該機能を設ける。
- (2) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めるときは、当該機能を設ける。
- 2 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された電子政府推奨暗号リストに基づき、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを定めること。また、その運用方法について実施手順を定める。
- 3 情報システムセキュリティ責任者は、管理運用法人における電子署名の運用方法に、電子署名の目的に合致し、かつ適用可能な公的な公開鍵基盤が存在する場合はそれを使用するなど目的に応じた適切な公開鍵基盤を使用するように定める。

(暗号化・電子署名に係る管理)

第134条 情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、

以下の全ての措置を講ずる。

- (1) 電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供する。
- (2) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズム又は鍵長の危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し、必要に応じて、役員等と共有を図る。

## 第6節 監視機能

(監視機能の導入・運用)

第135条 情報システムセキュリティ責任者は、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、監視機能を実装する。

- 2 情報システムセキュリティ責任者は、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する。
- 3 情報システムセキュリティ責任者は、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す。

## 第2章 情報セキュリティの脅威への対策

### 第1節 ソフトウェアに関する脆弱性対策

(ソフトウェアに関する脆弱性対策の実施)

第136条 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施する。

- 2 情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で講じ得る対策がある場合は、当該対策を実施する。
- 3 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的及び適時に確認する。
- 4 情報システムセキュリティ責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずるものとする。

### 第2節 不正プログラム対策

(不正プログラム対策の実施)

第137条 情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入する。

- 2 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずる。
- 3 情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行う。

### 第3節 サービス不能攻撃対策

(サービス不能攻撃対策の実施)

第138条 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下この条において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行う。

- 2 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについて、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築する。
- 3 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視する。

### 第4節 標的型攻撃対策

(標的型攻撃対策の実施)

第139条 情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃を想定した以下の対策を講ずるものとする。

- (1) 標的型攻撃による組織内部への侵入可能性を低減する入口対策
- (2) 標的型攻撃による組織内部への侵入を前提とした横展開（マルウェア等への感染が拡大することをいう。）防止等の内部対策
- (3) 標的型攻撃による組織内部への侵入があった場合における情報流出及び外部通信の阻止等の出口対策

## 第3章 ゼロトラストアーキテクチャ

### 第1節 動的なアクセス制御の実装時の対策

(動的なアクセス制御における責任者の設置)

第140条 統括情報セキュリティ責任者は、複数の情報システム間で動的なアクセス制御を実装する場合は、複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者とし

て、情報システムセキュリティ責任者を選任する。

(動的なアクセス制御の導入方針の検討)

第141条 情報システムセキュリティ責任者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定めるものとする。

(動的なアクセス制御の実装時の対策)

第142条 情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシー（以下「アクセス制御ポリシー」という。）を作成するものとする。

2 情報システムセキュリティ責任者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行う。

## 第2節 動的なアクセス制御の運用時の対策

(動的なアクセス制御の実装方針の見直し)

第143条 情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、情報セキュリティに係る重大な変化等を踏まえ、アクセス制御ポリシーの見直しをするものとする。

(リソースの信用情報に基づく動的なアクセス制御の運用時の対策)

第144条 情報システムセキュリティ責任者は、動的なアクセス制御の運用に際し、リソースの信用情報の収集により検出されたリスクへ対処を行う。

## 第8編 情報システムの利用

### 第1章 情報システムの利用

(情報システムの利用に係る規定の整備)

第145条 統括情報セキュリティ責任者は、管理運用法人の情報システムの利用のうち、情報セキュリティに関する実施手順を整備するものとする。

2 統括情報セキュリティ責任者は、USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する実施手順を定めるものとする。

3 統括情報セキュリティ責任者は、機密性3情報、要保全情報又は要安定情報が記録されたUSBメモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す際の許可手続を定めるものとする。

(情報システム利用者の規定の遵守を支援するための対策)

第146条 情報システムセキュリティ責任者は、役員等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築する。

(情報システムの利用時の基本的対策)

第147条 役員等は、業務の遂行以外の目的で情報システムを利用してはならない。

- 2 役員等は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に管理運用法人の情報システムを接続してはならない。
- 3 役員等は、管理運用法人内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続してはならない。
- 4 役員等は、業務の遂行において、利用が認められていないソフトウェアを利用してはならない。また、当該ソフトウェアを職務上の必要により利用する場合は、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。
- 5 役員等は、接続が許可されていない機器等を情報システムに接続してはならない。
- 6 役員等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずるものとする。
- 7 役員等は、機密性3情報、要保全情報又は要安定情報が記録されたUSBメモリ等の外部電磁的記録媒体を要管理対策区域外に持ち出す場合には、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。
- 8 役員等は、業務の遂行において、利用承認を得ていないクラウドサービスを利用してはならない。

(端末(支給外端末を含む)の利用時の対策)

第148条 役員等は、管理運用法人が支給する端末(要管理対策区域外で使用する場合に限る。)及び管理運用法人支給以外の端末を用いて要保護情報を取り扱う場合は、定められた利用手順に従うものとする。

- 2 役員等は、次の各号に掲げる端末を用いてそれぞれ当該各号に定める情報を取り扱う場合は、情報セキュリティ管理者の許可等を得なければならない。
  - (1) 管理運用法人が支給する端末(要管理対策区域外で使用する場合に限る。) 機密性3情報、要保全情報又は要安定情報
  - (2) 管理運用法人支給以外の端末 要保護情報
- 3 役員等は、要管理対策区域外において管理運用法人外通信回線に接続した端末(支給外端末を含む。)を要管理対策区域で管理運用法人内通信回線に接続する場合には、定められた措置を講ずる。

(電子メール・ウェブの利用時の対策)

第149条 役員等は、職務遂行に係る情報を含む電子メールを送受信する場合には、原則として管

理運用法人が運営する電子メールサーバにより提供される電子メールサービスを利用する。

- 2 役員等は、管理運用法人外の者と電子メールにより情報を送受信する場合は、政府ドメイン名を取得できない場合を除き、当該電子メールのドメイン名に政府ドメイン名を使用する。
- 3 役員等は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処する。
- 4 役員等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わない。
- 5 役員等は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認する。
- 6 役員等は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の全ての事項を確認するものとする。
  - (1) 送信内容が暗号化されること。
  - (2) 当該ウェブサイトが送信先として想定している組織のものであること。

(識別コード・主体認証情報の取扱い)

第150条 役員等は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しない。

- 2 役員等は、自己に付与された識別コードを適切に管理する。
- 3 役員等は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用する。
- 4 役員等は、自己の主体認証情報の管理を徹底する。

(暗号・電子署名の利用時の対策)

第151条 役員等は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム、鍵長及び方法に従う。

- 2 役員等は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理する。
- 3 役員等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行う。

(不正プログラム感染防止)

第152条 役員等は、不正プログラム感染防止に関する措置に努めるものとする。

- 2 役員等は、情報システム（支給外端末を含む。）が不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システム（支給外端末を含む。）の通信回線への接続を速やかに切断し、情報セキュリティ責任者又は情報セキュリティ管理者に連絡するなど、必要な措置を講じなければならない。

(Web会議サービスの利用時の対策)

第153条 役員等は、定められた利用手順に従い、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。

2 役員等は、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。

(クラウドサービスを利用した管理運用法人外の者との情報の共有時の対策)

第154条 役員等は、管理運用法人外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有を行う必要のある者のみがクラウドサービス上に保存した要保護情報にアクセスすることが可能となるための措置を講ずる。

2 役員等は、管理運用法人外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有が不要になった時点で、クラウドサービス上に保存した要保護情報を速やかに削除するものとする。

## 第2章 ソーシャルメディアによる情報発信

(ソーシャルメディアによる情報発信時の対策)

第155条 統括情報セキュリティ責任者は、管理運用法人が管理するアカウントでソーシャルメディアを利用することを前提として、以下を全て含む情報セキュリティ対策を実施する。また、当該サービスの利用において要機密情報が取り扱われないようにする。

(1) 管理運用法人のアカウントによる情報発信が実際の管理運用法人のものであると明らかにするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。

(2) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。

2 役員等は、要安定情報の国民への提供にソーシャルメディアを用いる場合は、管理運用法人の自己管理ウェブサイトにも当該情報を掲載することにより参照可能とする。

## 第3章 テレワーク

(運用規程の整備)

第156条 統括情報セキュリティ責任者は、テレワーク実施時の情報セキュリティ対策に係る運用規程を整備するものとする。当該運用規程においては、原則としてテレワークは管理運用法人が支給する端末で行うよう定めるものとする。

(実施環境における対策)

第157条 情報システムセキュリティ責任者は、テレワークの実施により管理運用法人外通信回線を経由して管理運用法人の情報システムへリモートアクセスする形態となる情報システムを構築

- する場合は、通信経路及びリモートアクセス特有の攻撃に対する情報セキュリティを確保する。
- 2 情報システムセキュリティ責任者は、リモートアクセスに対し多要素主体認証を行う。
  - 3 情報システムセキュリティ責任者は、リモートアクセスする端末を許可された端末に限定する措置を講じる。
  - 4 情報システムセキュリティ責任者は、リモートアクセスする端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定する。

(実施時における対策)

- 第158条 統括情報セキュリティ責任者は、テレワーク実施前及び実施後に役員等が確認すべき項目を定め、役員等に当該項目を確認させるものとする。
- 2 役員等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定する。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意する。
  - 3 役員等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な管理運用法人外通信回線を利用してテレワークを行わないものとする。

## 第9編 雑則

(細則の制定又は改廃等)

- 第159条 この細則の制定、変更又は廃止は理事長が定める。また、必要に応じて理事長はこの細則の下位規定を定める。

附 則 (令和8.3.27制定)

この制定は、令和8年4月1日から施行する。

別表1（第5条関係）

情報の格付の区分・取扱制限の定義

1. 情報の格付の区分

(1) 機密性についての格付の定義

| 格付の区分  | 分類の基準   |
|--------|---|
| 機密性3情報 | 業務で取り扱う情報のうち、国の行政機関における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）に定める秘密文書として取扱いを要する情報に準ずる情報                                       |
| 機密性2情報 | 業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成13年法律第140号。以下「独法等情報公開法」という。）第5条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性3情報」以外の情報 |
| 機密性1情報 | 業務で取り扱う情報のうち、独法等情報公開法第5条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報   |

なお、機密性2情報及び機密性3情報を「要機密情報」という。

(2) 完全性についての格付の定義

| 格付の区分  | 分類の基準  |
|--------|--|
| 完全性2情報 | 業務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され、又は業務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報 |
| 完全性1情報 | 完全性2情報以外の情報（書面を除く。）  |

なお、完全性2情報を「要保全情報」という。

(3) 可用性についての格付の定義

| 格付の区分  | 分類の基準   |
|--------|---|
| 可用性2情報 | 業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され、又は業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 |
| 可用性1情報 | 可用性2情報以外の情報（書面を除く。）   |

なお、可用性2情報を「要安定情報」という。

また、その情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「要保護情報」という。

2. 情報の取扱い制限

|      |   |
|------|---|
| 取扱制限 | 情報の取扱いに関する制限であって、複製禁止、持出禁止、配布禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを役員等に行わせるための手段をいう。役員等は、格付に応じた情報の取扱いを適切に行う必要があるが、その際に、格付に応じた具体的な取扱い方を示す方法として取扱制限を用いる。 |
|------|---|

別表2（第6条関係）

用語定義

|            |  |
|------------|--|
| <p>【あ】</p> | <ul style="list-style-type: none"> <li>● 「アプリケーション・コンテンツ」とは、管理運用法人が開発し提供するアプリケーションプログラム、ウェブコンテンツ等の総称をいう。</li> <li>● 「運用規程」とは、この細則に定められた対策内容を個別の情報システムや業務において運用するため、あらかじめ定める必要のある具体的な規程や基準をいう。</li> </ul>   |
| <p>【か】</p> | <ul style="list-style-type: none"> <li>● 「管理運用法人外通信回線」とは、通信回線のうち、<b>機関等</b>管理運用法人内通信回線以外のものをいう。</li> <li>● 「管理運用法人内通信回線」とは、管理運用法人が管理するサーバ装置又は端末の間の通信の用に供する通信回線であって、管理運用法人の管理下でないサーバ装置又は端末が論理的に接続されていないものをいう。管理運用法人内通信回線には、専用線やVPN等物理的な回線を管理運用法人が管理していないものも含まれる。</li> <li>● 「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。</li> <li>● 「業務委託」とは、管理運用法人の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。委任、準委任、請負といった契約形態を問わず、全て含むものとする。ただし、当該業務において管理運用法人の情報を取り扱わせる場合に限る。</li> <li>● 「国の行政機関」とは、法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成11年法律第89号）第49条第1項若しくは第2項に規定する機関、国家行政組織法（昭和23年法律第120号）第3条第2項に規定する機関又はこれらに置かれる機関をいう。</li> <li>● 「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。なお、この細則におけるクラウドサービスは、管理運用法人外の一般の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービスであって、当該サービスにおいて管理運用法人の情報が取り扱われる場合に限るものとする。</li> <li>● 「クラウドサービス管理者」とは、クラウドサービスの利用における利用申請の許可権限者から利用承認時に指名された当該クラウドサービスに係る管理を行う管理運用法人の役員等をいう。</li> <li>● 「クラウドサービス提供者」とは、クラウドサービスを提供する事業者（クラウドサービスプロバイダ）をいう。</li> </ul> |
| <p>【さ】</p> | <ul style="list-style-type: none"> <li>● 「SIRT（サート）」とは、管理運用法人において発生した情報セキュリティインシデントに対処するため、当該管理運用法人に設置された体制をいう。Security Incident Response Teamの略。</li> <li>● 「サーバ装置」とは、情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス</li> </ul>   |

|     |   |
|-----|---|
|     | <p>等の周辺機器を含む。)をいい、特に断りがない限り、管理運用法人が調達又は開発するもの(政府共通利用型システムが提供するものを含む。)をいう。また、物理的なハードウェアを有するサーバ装置を「物理的なサーバ装置」という。</p> <ul style="list-style-type: none"> <li>● 「CYMAT(サイマツト)」とは、サイバー攻撃等により国の行政機関、独立行政法人及び指定法人の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。Cyber Incident Mobile Assistance Team(情報セキュリティ緊急支援チーム)の略。</li> <li>● 「実施手順」とは、この細則に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順や手続をいう。</li> <li>● 「情報システム」とは、ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、管理運用法人が調達又は開発するもの(管理を外部委託しているシステムや政府共通利用型システムを含む。)をいう。</li> <li>● 「情報セキュリティインシデント」とは、JIS Q 27000:2019における情報セキュリティインシデントをいう。</li> <li>● 「情報セキュリティ関係規程」とは、この細則、運用規程及び実施手順を総称したものをいう。</li> <li>● 「情報セキュリティ対策推進体制」とは、管理運用法人の情報セキュリティ対策の推進に係る事務を遂行するために設置された体制をいう。</li> <li>● 「政府共通利用型システム」とは、他の機関等を含め共通的に利用することを目的として、一つの機関等が管理・運用する情報システムであって、他の機関等が整備する情報システムに対し、当該情報システムと連携して、情報システムのセキュリティ機能を提供する情報システム及び他の機関等に機器等を提供し、他の機関等の職員等が利用する情報システムをいう。なお、政府共通利用型システムを構築・運用する機関等を「政府共通利用型システム管理機関」といい、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築・運用する機関等及び政府共通利用型システムが提供する機器等を利用する機関等を「政府共通利用型システム利用機関」という。</li> <li>● 「政府ドメイン名」とは、.go.jpで終わるドメイン名のことをいう。日本国の政府機関、独立行政法人、特殊法人(特殊会社を除く。)が登録(取得)することができる。</li> </ul> |
| 【た】 | <ul style="list-style-type: none"> <li>● 「対策推進計画」とは、情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画をいう。</li> <li>● 「端末」とは、情報システムの構成要素である機器のうち、役員等が情報処理を行うために直接操作するもの(搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。)をいい、特に断りがない限り、機関等管理運用法人が調達又は開発するもの(政府共通利用型システムが提供するものを含む。)をいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、管理運用法人が調達又は開発するもの以外を指す「管理運用法人支給以外の端末」がある。また、管理運用法人が調達又は開発した端末と管理運用法人支給以外の端末の双方を合わせて「端末(支給外端末を含む。)」という。さらに、物理的なハ</li> </ul>   |

|     |  |
|-----|--|
|     | <p>ードウェアを有する端末を「物理的な端末」という。</p> <ul style="list-style-type: none"> <li>● 「通信回線」とは、複数の情報システム又は機器等（管理運用法人が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、管理運用法人の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、管理運用法人が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。</li> <li>● 「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。また、物理的なハードウェアを有する通信回線装置を「物理的な通信回線装置」という。</li> <li>● 「特定用途機器」とは、テレビ会議システム、IP電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続する機能を備えているもの又は内蔵電磁的記録媒体を備えているものをいう。</li> </ul> |
| 【は】 | <ul style="list-style-type: none"> <li>● 「本部監査」とは、サイバーセキュリティ基本法（平成26年法律第104号）第26条第1項第2号に基づきサイバーセキュリティ戦略本部が実施する監査をいう。</li> </ul>  |
| 【ま】 | <ul style="list-style-type: none"> <li>● 「明示等」とは、情報を取り扱う全ての者が当該情報の格付について共通の認識となるようにする措置をいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。</li> </ul>  |
| 【や】 | <ul style="list-style-type: none"> <li>● 「要管理対策区域」とは、管理運用法人の管理下にある区域（管理運用法人が外部の組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。</li> </ul>  |