国立女性教育会館
情報セキュリティポリシー

令和３年３月３０日

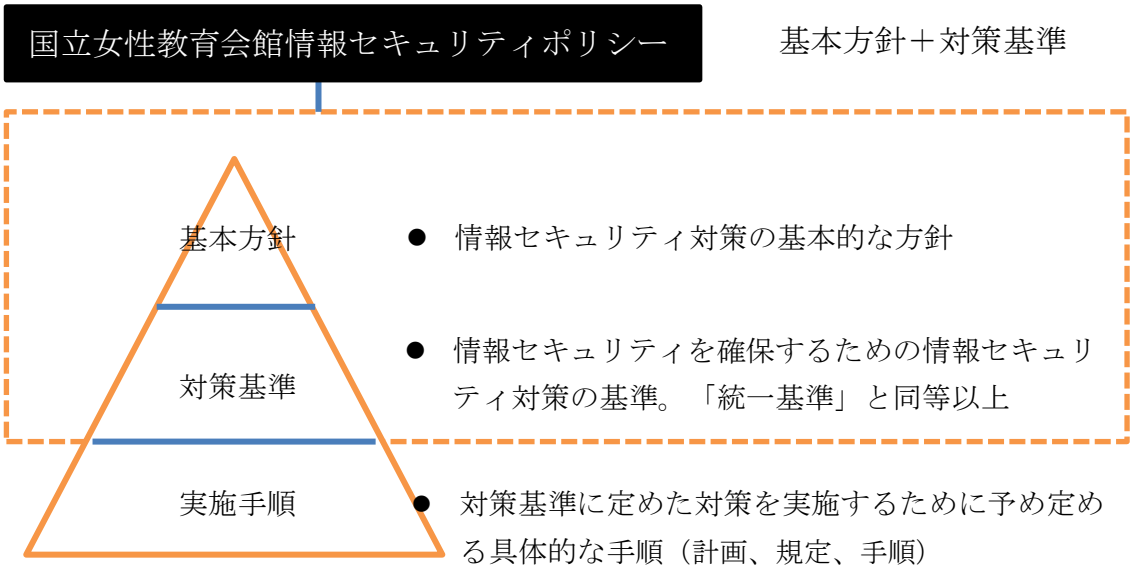
国立女性教育会館

情報セキュリティ委員会

はじめに

独立行政法人国立女性教育会館情報セキュリティポリシー（平成 29 年 10 月 1 日制定）の全部を、内閣サイバーセキュリティセンター「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」に準じて改正する。

【参考】



目次

第1部　総則

1.1 情報セキュリティポリシーの目的・適用範囲

(1) 情報セキュリティポリシーの目的

独立行政法人国立女性教育会館（以下「会館」という。）は、男女共同参画社会の形成の促進に資することを目的としたさまざまな情報の蓄積を行っており、その情報資産は会館の基盤となる非常に重要な資産である。これらの会館の情報資産をあらゆる脅威から守り、社会的責任を保ち、必要な情報セキュリティを確保するため、この情報セキュリティポリシー（以下「ポリシー」という。）を定める。

(2) ポリシーの適用対象

(a)ポリシーにおいて適用対象とする者は、全ての職員等 とする。

(b)ポリシーにおいて適用対象とする情報は、以下の情報とする。

(ア) 職員等が職務上使用することを目的として会館が調達し、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（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

(イ) その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、職員等が職務上取り扱う情報

(ウ) (ア)及び(イ)のほか、会館が調達し又は開発した情報システムの設計又は運用管理に関する情報

(c) ポリシーにおいて適用対象 とする情報システムは、ポリシーの適用対象となる情報を取り扱う全ての情報システムとする。

(3) ポリシーの改定

情報セキュリティ水準を適切に維持していくためには、状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。

このため、情報技術の進歩に応じて、ポリシーを定期的に点検し、必要に応じ規定内容の追加・修正等の改定を行う。

(4) 法令等の遵守

情報及び情報システムの取扱いに関しては、ポリシーのほか法令及び基準等（以下「関連法令等」という。）を遵守しなければならない。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)、著作権法（昭和 45 年法律第 48 号)、独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号)、また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に遵守しなければならない。

(5) 罰則

職員等が故意または重大な過失により著しく基本方針等に違反した場合、またはネットワークに関する法令等の遵守事項の違反行為に該当する場合は、別に定めた職員就業規則等により措置される。

第2部　情報セキュリティ対策の基本的枠組み

2.1 導入・計画

2.1.1　組織・体制の整備

(1) 最高情報セキュリティ責任者の設置

(a) 情報セキュリティに関する事務を統括する最高情報セキュリティ責任者１人を置くことにし、理事をもって充てる。

2.1.1.(1)-1 最高情報セキュリティ責任者は、次に掲げる事務を統括する。

a) 情報セキュリティ対策推進のための組織・体制の整備
b) 対策基準の決定、見直し
c) 対策推進計画の決定、見直し
d) 情報セキュリティインシデントに対処するために必要な指示、その他の措置
e) 前各号に掲げるもののほか、情報セキュリティに関する重要事項

(2) 情報セキュリティ委員会の設置

(a) 対策基準等の審議を行う機能を持つ組織として、情報セキュリティ対策推進体制及びその他業務を実施する課室の代表者を構成員とする情報セキュリティ委員会（以下「委員会」という。）を置く。

委員会の長は、最高情報セキュリティ責任者とする。

a) 委員会は、最高情報セキュリティ責任者、事務局長、総務課長、事業課長、情報課長、研究国際室長及び最高情報セキュリティ責任者が指名する者を持って構成する。

2.1.1(2)-1 情報セキュリティ委員会は、次に掲げる事項を審議する。

a) 対策基準
b) 対策推進計画
c) 前各号に掲げるもののほか、情報セキュリティに関し必要な事項

(3) 情報セキュリティ監査責任者の設置

(a) 最高情報セキュリティ責任者は、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１人を置くことにし、監査室主査をもって充てる。

2.1.1(3)-1 情報セキュリティ監査責任者は、次の事務を統括する。

a) 監査実施計画の策定

b) 監査実施体制の整備
c) 監査の実施指示及び監査結果の最高情報セキュリティ責任者への報告
d) 前各号に掲げるもののほか、情報セキュリティの監査に関する事項

(4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置

(a) 最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、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１人を置くこととする。会館では全体をひとつのまとまりとみて情報課長を充てる。情報セキュリティ責任者を統括し、最高情報セキュリティ責任者を補佐する者として、統括情報セキュリティ責任者１人を選任することとし、総務課長を充てる。

2.1.1(4)-1 統括情報セキュリティ責任者は、次の事務を統括する。

a) 要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定
b) 情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務の取りまとめ
c) 情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備
d) 例外措置の適用審査記録の台帳整備等
e) 情報セキュリティインシデントに対処するための緊急連絡窓口の整備等
f) 前各号に掲げるもののほか、情報セキュリティ対策に係る事務

2.1.1(4)-2 情報セキュリティ責任者は、情報セキュリティ対策を推進するため、次の事務を統括する。

a) 定められた区域ごとの区域情報セキュリティ責任者の設置
b) 各課室の情報セキュリティ責任者の設置
c) 情報システムごとの情報システムセキュリティ責任者の設置
d) 情報セキュリティインシデントの原因調査、再発防止策等の実施
e) 情報セキュリティに係る自己点検計画の策定及び実施手順の整備
f) 前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務

(b) 情報セキュリティ責任者は、3.2.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者 １人を置く。会館の全ての区域に対し区域情報セキュリティ責任者として総務課専門職員（情報システム担当）を充てる。

2.1.1(4)-3 区域情報セキュリティ責任者は、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を統括する。

(c) 情報セキュリティ責任者は、課室ごとに情報セキュリティ対策に関する事務を

統括する課室情報セキュリティ責任者 1 人を置くこととし、各課室長を充てる。

2.1.1(4)-4 課室情報セキュリティ責任者は、課室における情報の取扱いその他の情報セキュリティ対策に関する事務を統括する。

(d) 情報セキュリティ責任者は、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の責任者として、情報システムセキュリティ責任者を、当該情報システムの企画に着手するまでに選任する。会館の事務用電子計算機システムの情報システムセキュリティ責任者として総務課専門職員（情報システム担当）を充てる。

2.1.1(4)-5 情報システムセキュリティ責任者は、情報システムにおける情報セキュリティ対策に関する事務を担う。

2.1.1(4)-6 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管理業務において必要な単位ごとに情報システムセキュリティ管理者を置き、情報システムセキュリティ責任者が兼務する。

(5) 最高情報セキュリティアドバイザーの設置

(a) 最高情報セキュリティ責任者は、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き、自らへの助言を含む最高情報セキュリティアドバイザーの業務内容を定める。最高情報セキュリティアドバイザーとして会館 CIO 補佐を充てる。

2.1.1(5)-1 最高情報セキュリティアドバイザーの主な業務内容は以下の通り。

a) 会館全体の情報セキュリティ対策の推進に係る最高情報セキュリティ責任者への助言
b) 情報セキュリティ関係規程の整備に係る助言
c) 対策推進計画の策定に係る助言
d) 教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
e) 情報システムに係る技術的事項に係る助言
f) 情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言
g) 職員等に対する日常的な相談対応
h) 情報セキュリティインシデントへの対処の支援
i) そのほか、情報セキュリティ対策への助言又は支援

(6) 情報セキュリティ対策推進体制の整備

(a) 最高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を整備し、その役割を規定する。

2.1.1(6)-1 最高情報セキュリティ責任者は、以下を含む情報セキュリティ対策

推進体制の役割を規定する。

a) 情報セキュリティ関係規程及び対策推進計画の策定に係る事務
b) 情報セキュリティ関係規程の運用に係る事務
c) 例外措置に係る事務
d) 情報セキュリティ対策の教育の実施に係る事務
e) 情報セキュリティ対策の自己点検に係る事務
f) 情報セキュリティ関係規程及び対策推進計画の見直しに係る事務
g) 情報セキュリティ委員会の運営にかかわる事務
h) 「本部監査」への対応に係る事務
i) NISC から発出される事務連絡や調査依頼への対応に係る事務

(b) 最高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の責任者を定めることとし、統括情報セキュリティ責任者を充てる。体制の構成員は総務課専門職員（情報システム担当）及び総務課人事・企画係を充てる。

(7) 情報セキュリティインシデントに備えた体制の整備

(a) 最高情報セキュリティ責任者は、会館に CSIRT を整備し（特に断りがない限り、会館の CSIRT）、その役割を明確化する。

2.1.1(7)-1 以下に CSIRT の役割を規定する。

a) 情報セキュリティインシデント発生時の対処の一元管理
- 会館全体における情報セキュリティインシデント対処の管理
- 情報セキュリティインシデント対処の管理
- 情報セキュリティインシデントの可能性の報告受付
- 情報セキュリティインシデントに関する情報の集約
- 情報セキュリティインシデントの最高情報セキュリティ責任者等への報告
- 情報セキュリティインシデントへの対処に関する指示系統の一本化

b) 情報セキュリティインシデントへの迅速かつ的確な対処
- 情報セキュリティインシデントであるかの評価
- 被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
- 所管する国の行政機関（文部科学省）への連絡
- 外部専門機関等からの情報セキュリティインシデントに係る情報の収集
- 情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施

2.1.1(7)-2 最高情報セキュリティ責任者は、実務担当者を含めた実効性のある CSIRT 体制を構築する。

2.1.1(7)-3 最高情報セキュリティ責任者は、情報セキュリティインシデントが

発生した際に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築しておく。

2.1.1(7)-4　最高情報セキュリティ責任者は、会館全体における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者課室及びその他関連課室の役割分担を規定する。

(b) 最高情報セキュリティ責任者は、職員等のうちから CSIRT に属する職員等として専門的な知識又は適性を有すると認められる者を選任する。そのうち、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 CSIRT 責任者を置き、統括情報セキュリティ責任者を充てる。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定める。

(c) 最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

(8) 兼務を禁止する役割

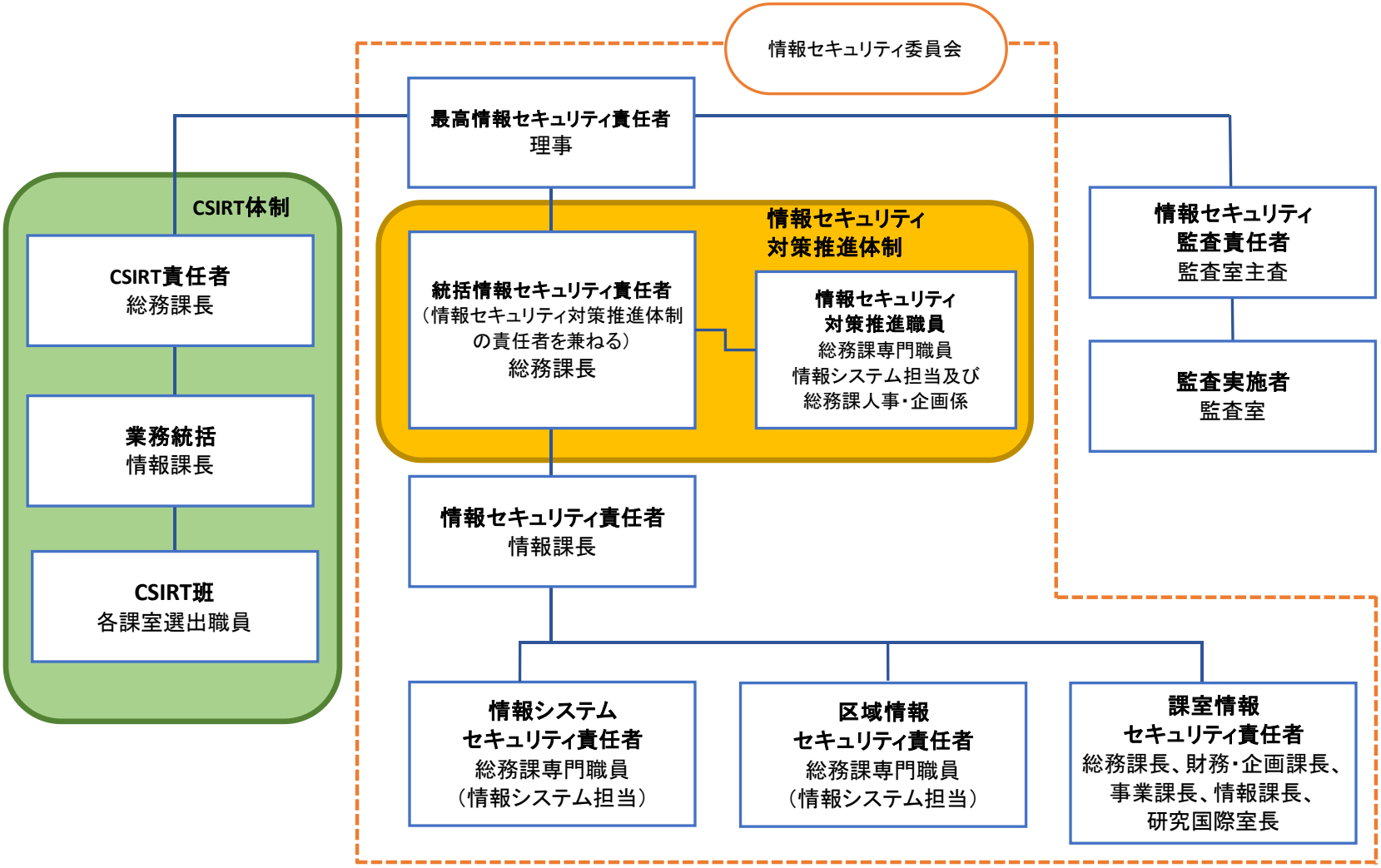
(a) 職員等は、情報セキュリティ対策の運用において、以下の役割を兼務しないこととする。

(ア) 承認又は許可（以下本条において「承認等」という。）の申請者と当該承認等を行う者（以下本条において「承認権限者等」という。）

(イ) 監査を受ける者とその監査を実施する者

(b) 職員等は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ることとする。

国立女性教育会館の情報セキュリティ体制図



国立女性教育会館のCSIRT体制と役割（館内）

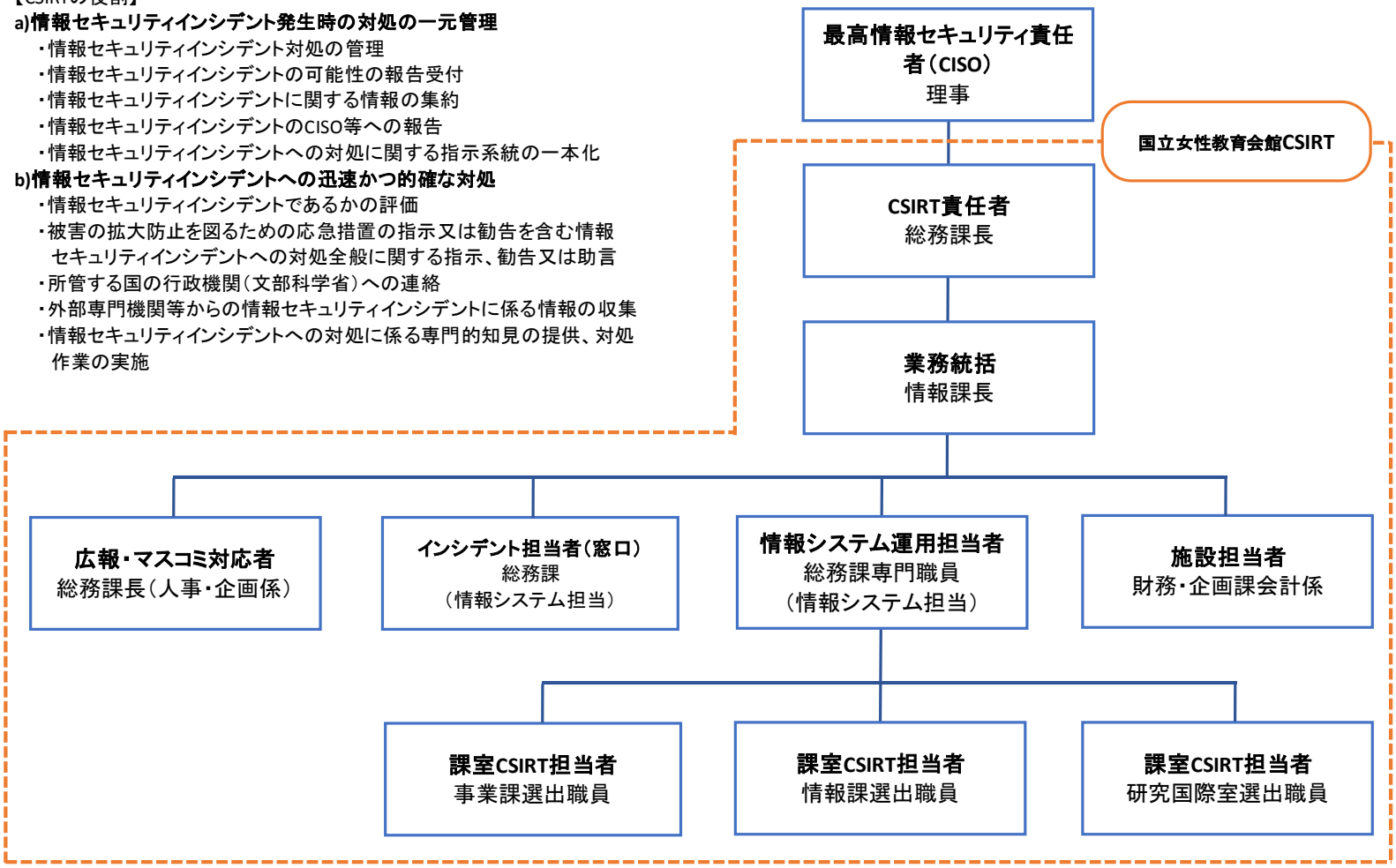
【CSIRTの役割】

a)情報セキュリティインシデント発生時の対処の一元管理

・情報セキュリティインシデント対処の管理
・情報セキュリティインシデントの可能性の報告受付
・情報セキュリティインシデントに関する情報の集約
・情報セキュリティインシデントのCISO等への報告
・情報セキュリティインシデントへの対処に関する指示系統の一本化

b)情報セキュリティインシデントへの迅速かつ的確な対処

・情報セキュリティインシデントであるかの評価
・被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
・所管する国の行政機関（文部科学省）への連絡
・外部専門機関等からの情報セキュリティインシデントに係る情報の収集
・情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施



2.1.2　ポリシー・対策推進計画の策定

(1) ポリシーの策定

(a) 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、統一基準に準拠したポリシーを定める。また、ポリシーは、会館の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定める。

(2) 対策推進計画の策定

(a) 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、情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定める。また、対策推進計画には、会館の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含める。

(ア) 情報セキュリティに関する教育

(イ) 情報セキュリティ対策の自己点検

(ウ) 情報セキュリティ監査

(エ) 情報システムに関する技術的な対策を推進するための取組

(オ) その他に掲げるもののほか、情報セキュリティ対策に関する重要な取組

2.2 運用

2.2.1　情報セキュリティ関係規程の運用

(1) 情報セキュリティ対策の運用

(a) 統括情報セキュリティ責任者は、会館における情報セキュリティ対策に関する実施手順を整備し、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。

(b) 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おける雇用の開始、終了及び人事異動時等に関する管理の規定を整備する。

(c) 情報セキュリティ対策推進体制は、最高情報セキュリティ責任者が規定した当該体制の役割に応じて必要な事務を遂行する。

(d) 情報セキュリティ責任者又は課室情報セキュリティ責任者は、職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。

(e) 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。

(2) 違反への対処

(a) 職員等は、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。

(b) 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。必要な者とは情報システムセキュリティ責任者、課室情報セキュリティ責任者及び区域情報セキュリティ責任者等の当該規程の実施に責任を有する者をいう。

2.2.2 例外措置

例外措置はあくまで例外であって、乱用があってはいけない。しかしながら、情報セキュリティ関係規定の適用が遂行を著しく妨げるなどの理由により、規定された対策の内容と異なる代替の方法を採用すること又は規定された対策を実施しないことを認めざるを得ない場合がある。このような場合に対処するために、例外措置の手続きを定める。

(1) 例外措置手続の整備

(a) 最高情報セキュリティ責任者は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）及び審査手続を定める。許可権限者として統括情報セキュリティ責任者を充てる。例外措置の適用を受ける者は「例外措置適用申請書」を例外措置許可権限者に提出する。

(b) 統括情報セキュリティ責任者は、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。許可権限者は、例外措置の適用審査記録の台帳（例外措置適用審査記録台帳）として保管するとともに、統括情報セキュリティ責任者へ定期的に報告する。

(2) 例外措置の運用

(a) 職員等は、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する。ただし、業務の遂行に緊急を要し、当該規定の趣旨を充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。

(b) 許可権限者は、職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、許可の可否を決定する。

(c) 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。

(d) 統括情報セキュリティ責任者は、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。

2.2.3　教育

(1) 教育体制の整備・教育実施計画の策定

(a) 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。

・ 職員等の役割に応じて教育すべき内容を検討し、教育のための資料を整備する。

・ 職員等が毎年度最低１回は教育を受講できるように、教育実施計画を立案するとともに、その実施体制を整備する。

・ 職員等の着任又は異動後に、3 か月以内に受講できるように、その実施体制を整備する。

(b) 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職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。

(2) 教育の実施

(a) 課室情報セキュリティ責任者は、教育実施計画に基づき、職員等に対して、情報セキュリティ関係規程に係る教育を適切に受講させる。

(b) 職員等は、教育実施計画に従って、適切な時期に教育を受講する。

(c) 課室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 CSIRT に属する職員等に教育を適切に受講させる。課室情報セキュリティ責任者は、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。

(d) 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。

2.2.4　情報セキュリティインシデントへの対処

(1) 情報セキュリティインシデントに備えた事前準備

(a) 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会館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、職員等に周知する。

(b) 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会館外との情報共有を含む対処手順を整備する。

2.2.4(1)-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発生時の対処手順のうち、意思決定の判断基準、判断に応じた対応内容、緊急時

の意思決定方法等をあらかじめ定めておく。

(c) 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、連絡内容を含む緊急連絡網を整備する。

(d) 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整備する。

(e) 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会館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会館外の者に明示する。

(f) 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。

(2) 情報セキュリティインシデントへの対処

(a) 職員等は、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、会館の報告窓口に報告し、指示に従う。

(b) CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行う。

2.2.4(2)-1　CSIRT は、情報セキュリティインシデントではないと評価した場合であっても、注意喚起等が必要と考えられるものについては、関係する者に情報共有を行う。

(c) CSIRT 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する。

(d) CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告を行う。

2.2.4(2)-2　CSIRT 責任者は、認知した情報セキュリティインシデントの種類や規模、影響度合い等を勘案し、必要に応じて、CSIRT、情報セキュリティインシデントの当事者部局、その他関連部局の役割分担を見直す。

(e) 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、会館で定められた対処手順又は CSIRT の指示若しくは勧告に従って、適切に対処する。

(f) 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基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処する。

(g) CSIRT は、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、文部科学省に連絡すること。この連絡を受けた文部科学省における CSIRT は、当該事象について速やかに、内閣官房内閣サイバーセキュリティセンターに連絡する。

(h) CSIRT 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、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行う。

(i) 文部科学省における CSIRT は、認知した情報セキュリティインシデント又は会館から連絡を受けた情報セキュリティインシデントが、国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態又はその可能性がある事態である場合には、「大規模サイバー攻撃事態等への初動対処について（平成 22 年 3 月 19 日内閣危機管理監決済）」に基づく報告連絡を行う。

(j) CSIRT 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、必要に応じて対処全般に関する指示、勧告又は助言を行う。

(k) CSIRT 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。

(l) CSIRT は、情報セキュリティインシデントに関して、会館を含む関係機関と情報共有を行う。

(m) CSIRT は、CYMAT 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。

(3) 情報セキュリティインシデントの再発防止・教訓の共有

(a) 情報セキュリティ責任者は、CSIRT から応急措置の実施及び復旧に係る指示又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。

(b) 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。

(c) CSIRT 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。

2.3 点検

2.3.1 情報セキュリティ対策の自己点検

(1) 自己点検計画の策定・手順の準備

(a) 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。

(b) 情報セキュリティ責任者は、年度自己点検計画に基づき、職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。
(c) 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、職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。

(2) 自己点検の実施
(a) 情報セキュリティ責任者は、年度自己点検計画に基づき、職員等に自己点検の実施を指示する。
(b) 職員等は、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。

(3) 自己点検結果の評価・改善
(a) 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。
(b) 統括情報セキュリティ責任者は、会館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。
(c) 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。

2.3.2 情報セキュリティ監査

(1) 監査実施計画の策定
(a) 情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定める。

2.3.2(1)-1 情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする監査実施計画を策定する。

a) 監査の目的（例：情報セキュリティ対策の実際の運用が情報セキュリティ関係規程に準拠している等）
b) 監査の対象（例：監査の対象となる組織、情報システム、業務等）
c) 監査の方法（例：情報セキュリティ対策の運用状況を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、対策基準及び実施手順とする）
d) 監査の実施体制（例：監査責任者、監査実施者の所属、氏名）
e) 監査の実施時期（例：対象ごとの実施時期）

2.3.2(1)-2　情報セキュリティ監査責任者は、組織内における監査遂行能力が不足している場合等においては、会館外の者に監査の一部を請け負わせる。

(b) 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、対策推進計画で計画された以外の監査の実施が必要な場合には、追加の監査実施計画を定める。

(2) 監査の実施

(a) 情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項を含む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に報告する。

(ア) ポリシーに統一基準を満たすための適切な事項が定められている

(イ) 実施手順がポリシーに準拠している

(ウ) 被監査部門における実際の運用が情報セキュリティ関係規程に準拠している

2.3.2(2)-1 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者に指名する。

(3) 監査結果に応じた対処

(a) 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。

(b) 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、会館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。

(c) 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、自らが担当する組織のまとまり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。

2.4 見直し

2.4.1　情報セキュリティ対策の見直し

(1) 情報セキュリティ関係規程の見直し

(a) 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・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、ポリシーについて必要な

見直しを行う。

(b) 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・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。

(2) 対策推進計画の見直し

(a) 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点検・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。

第3部　情報の取扱い

3.1 情報の取扱い

3.1.1　情報の取扱い

(1) 情報の取扱いに係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を含む情報の取扱いに関する規定を整備し、職員等へ周知する。

(ア) 情報の格付及び取扱制限についての定義

(イ) 情報の格付及び取扱制限の明示等についての手続

(ウ) 情報の格付及び取扱制限の継承、見直しに関する手続

(2) 情報の目的外での利用等の禁止

(a) 職員等は、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、情報を利用等する。

(3) 情報の格付及び取扱制限の決定・明示等

(a) 職員等は、情報の作成時及び会館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。

(b) 職員等は、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。

(c) 職員等は、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（以下本款において「決定者等」という。）に確認し、その結果に基づき見直す。

(4) 情報の利用・保存

(a) 職員等は、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う。

3.1.1(4)-1 職員等は、情報の格付及び取扱制限に応じて、情報を以下のとおり取り扱う。

a) 要保護情報を放置しない。

b) 要機密情報を必要以上に複製しない。

c) 電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化したり、施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずる。

d) 電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずる。

e) 情報の保存方法を変更する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずる。

3.1.1(4)-2 職員等は、入手した情報の格付及び取扱制限が不明な場合には、情報の作成元又は入手元への確認を行う。

(b) 職員等は、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、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得る。

(c) 職員等は、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。

(d) 職員等は、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。なお、会館の職員等は、機密性３情報を機器等に保存する際、以下の措置を講ずる。

(ア) 機器等に保存する場合は、インターネットや、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。

(イ) 当該情報に対し、暗号化による保護を行う。

(ウ) 当該情報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。

(e) 職員等は、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。

(5) 情報の提供・公表

(a) 職員等は、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する。

(b) 職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、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。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。

(c) 会館の職員等は、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、課室情報セキュリティ責任者の許可を得る。

(d) 職員等は、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。

3.1.1(5)-1 職員等は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消する。

(6) 情報の運搬・送信

(a) 職員等は、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。会館の職員等が、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、課室情報セキュリティ責任者が指定する方法により運搬する。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。

(b) 職員等は、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。会館の職員等が、機密性３情報を会館外通信回線（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、課室情報セキュリティ責任者が指定する方法により送信する。

3.1.1(6)-1 職員等は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、セキュアな運送サービスを提供する運送事業者により運搬する。

3.1.1(6)-2 職員等は、要機密情報である電磁的記録を要管理対策区域外に運搬又は会館外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずる。

a) 運搬又は送信する情報を暗号化する。

b) 要機密情報を複数の情報に分割し、それぞれ異なる経路及び手段を用いて運搬又は送信する。

c) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。

3.1.1(6)-3 職員等は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定する。

a) 会館管理の通信回線を用いて送信する。
b) 信頼できる通信回線を使用して送信する。
c) VPN を用いて送信する。
d) S/MIME 等の暗号化された電子メールを使用して送信する。
e) 会館独自で運用するなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する。

(7) 情報の消去

(a) 職員等は、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。

(b) 職員等は、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。

(c) 職員等は、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する。

(8) 情報のバックアップ

(a) 職員等は、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。

3.1.1(8)-1 職員等は、要保全情報又は要安定情報である電磁的記録又は重要な設計書について、バックアップを取得する。

(b) 職員等は、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。

3.1.1(8)-2 職員等は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップについて、災害等により生ずる業務上の支障を考慮し、適切な保管場所を選定する。

(c) 職員等は、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。

3.2 情報を取り扱う区域の管理

3.2.1 情報を取り扱う区域の管理

(1) 要管理対策区域における対策の基準の決定

(a) 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。

(b) 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、以下の観点を含む対策の基準を定める。

(ア) 許可されていない者が容易に立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。

(イ) 許可されていない者の立入りを制限するための、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。

(2) 区域ごとの対策の決定

(a) 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。

(b) 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。

(3) 要管理対策区域における対策の実施

(a) 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。職員等が実施すべき対策については、職員等が認識できる措置を講ずる。

(b) 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。

(c) 職員等は、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、職員等が会館外の者を立ち入らせる際には、当会館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部　外部委託

4.1 外部委託

4.1.1　外部委託

(1) 外部委託に係る規定の整備

(a) 統括情報セキュリティ責任者は、外部委託に係る以下の内容を含む規定を整備する。

(ア) 委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準（以下本款において「委託判断基準」という。）

(イ) 委託先の選定基準

(2) 外部委託に係る契約

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託判断基準に従って外部委託を実施する。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定する。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含める。

(ア) 委託先に提供する情報の委託先における目的外利用の禁止

(イ) 委託先における情報セキュリティ対策の実施内容及び管理体制

(ウ) 委託事業の実施に当たり、委託先企業若しくはその従業員、再委託先又はその他の者によって、会館の意図しない変更が加えられないための管理体

制

(エ) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

(オ) 情報セキュリティインシデントへの対処方法

(カ) 情報セキュリティ対策その他の契約の履行状況の確認方法

(キ) 情報セキュリティ対策の履行が不十分な場合の対処方法

4.1.1(2)-1 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、以下の内容を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させる。また、変更があった場合は、速やかに再提出させる。

a) 当該委託業務に携わる者の特定

b) 当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

4.1.1(2)-2 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取り扱う。

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含める。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

(d) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(b)(c)の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を会館に提供し、会館の承認を受けるよう、仕様内容に含める。また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断する。

(3) 外部委託における対策の実施

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認する。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、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は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく対処を委託先に

講じさせる。

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却又は抹消されたことを確認する。

(4) 外部委託における情報の取扱い

(a) 職員等は、委託先への情報の提供等において、以下の事項を遵守する。

(ア) 委託先に要保護情報を提供する場合は、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供する。

(イ) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させる。

(ウ) 委託業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかに情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告する。

4.1.2 約款による外部サービスの利用

(1) 約款による外部サービスの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を含む約款による外部サービスの利用に関する規定を整備する。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規定する。

(ア) 約款による外部サービスを利用してよい業務の範囲

(イ) 業務に利用できる約款による外部サービス

(ウ) 利用手続及び運用手順

4.1.2(1)-1 統括情報セキュリティ責任者は、会館において約款による外部サービスを業務に利用する場合は、以下を例に利用手続及び運用手順を定める。

a) 利用申請の許可権限者

b) 利用申請時の申請内容

- 利用する組織名
- 利用するサービス
- 利用目的（業務内容）
- 利用期間
- 利用責任者（利用アカウントの責任者）

c) サービス利用中の安全管理に係る運用手順

- サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
- 情報の滅失、破壊等に備えたバックアップの取得
- 利用者への定期的な注意喚起（禁止されている要機密情報の取扱

いの有無の確認等）

d) 情報セキュリティインシデント発生時の連絡体制

(b) 情報セキュリティ責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定める。

(2) 約款による外部サービスの利用における対策の実施

(a) 職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用する。

4.1.3 ソーシャルメディアサービスによる情報発信

(1) ソーシャルメディアサービスによる情報発信時の対策

(a) 統括情報セキュリティ責任者は、会館が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定める。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規定する。

(ア) 会館のアカウントによる情報発信が実際の会館のものであると明らかとするために、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。

(イ) 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。

4.1.3(1)-1 統括情報セキュリティ責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定める。

a) アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている会館の当該ウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。

b) URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。

4.1.3(1)-2 統括情報セキュリティ責任者は、会館のアカウントによる情報発信が実際の会館のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定める。

a) 会館からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、会館が運用していることを利

用者に明示する。

b) 会館からの情報発信であることを明らかにするために、会館が政府ドメイン名を用いて管理している当該ウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設ける。

c) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている会館の当該ウェブサイト上のページの URL を記載する。

d) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得する。

4.1.3(1)-3 統括情報セキュリティ責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定める。

a) パスワードを適切に管理する。具体的には、ログインパスワードには十分な長さと複雑さを持たせた容易に推測されないものを設定するとともに、パスワードを知る担当者を限定し、パスワードの使い回しをしない。

b) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用する。

c) ソーシャルメディアへのログインに利用する端末を紛失したり盗難に遭ったりした場合は、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理を厳重に行う。

d) ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施する。

4.1.3(1)-4 統括情報セキュリティ責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を含む対処手順を定める。

a) 自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していない等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行う。

b) アカウント乗っ取りを確認した場合には、被害を最小限にするため、ロ

グインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、自組織の CSIRT に報告する。報告を受けた CSIRT は遵守事項 2.2.4(2)に従い、内閣官房内閣サイバーセキュリティセンターへの連絡（会館においては文部科学省を経由）を含む適切な対処を行う。

(b) 情報セキュリティ責任者は、会館において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定める。

(c) 職員等は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、会館の自己管理ウェブサイトに当該情報を掲載して参照可能とする。

4.1.4 クラウドサービスの利用

(1) クラウドサービスの利用における対策

(a) 情報システムセキュリティ責任者は、クラウドサービス（民間事業者が提供するものに限らず、会館が自ら提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断する。

(b) 情報システムセキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定する。

(c) 情報システムセキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とする。

4.1.4(1)-1 円滑に業務を移行するための対策として、以下のセキュリティ対策を実施することをクラウドサービスの選定条件とし、仕様内容にも含める。

a) 取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件

b) 取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

(d) 情報システムセキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める。

4.1.4(1)-2 以下のセキュリティ要件をクラウドサービスに求め、契約内容にも含める。特に、運用段階で委託先が変更となる場合、開発段階等で設計したクラウドサービスのセキュリティ要件のうち継承が必須なセキュリティ要件について、変更後の委託先における維持・向上の確実性を事前に確認する。

a) クラウドサービスに係るアクセスログ等の証跡の保存及び提供

b) インターネット回線とクラウド基盤の接続点の通信の監視

c) クラウドサービスの委託先による情報の管理・保管の実施内容の確認
d) クラウドサービス上の脆弱性対策の実施内容の確認
e) クラウドサービス上の情報に係る復旧時点目標（RPO）等の指標
f) クラウドサービス上で取り扱う情報の暗号化
g) 利用者の意思によるクラウドサービス上で取り扱う情報の確実な削除・廃棄
h) 利用者が求める情報開示請求に対する開示項目や範囲の明記

(e) 情報システムセキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの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。

第5部　情報システムのライフサイクル

5.1 情報システムに係る文書等の整備

5.1.1　情報システムに係る台帳等の整備

(1) 情報システム台帳の整備

(a) 統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備する。

5.1.1(1)-1 統括情報セキュリティ責任者は、以下の内容を含む台帳を整備する。

a) 情報システム名
b) 管理課室
c) 当該情報システムセキュリティ責任者の氏名及び連絡先
d) システム構成
e) 接続する会館外通信回線の種別
f) 取り扱う情報の格付及び取扱制限に関する事項
g) 当該情報システムの設計・開発、運用・保守に関する事項

また、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備する。

a) 情報処理サービス名
b) 契約事業者
c) 契約期間
d) 情報処理サービスの概要
e) ドメイン名
f) 取り扱う情報の格付及び取扱制限に関する事項

(b) 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、当該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。

(2) 情報システム関連文書の整備

(a) 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、以下を網羅した情報システム関連文書を整備する。

(ア) 情報システムを構成するサーバ装置及び端末関連情報

5.1.1(2)-1 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を構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備する。

a) サーバ装置及び端末を管理する職員等及び利用者を特定する情報

b) サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン

c) サーバ装置及び端末で利用するソフトウェアを動作させるために用いられる他のソフトウェアであって、以下を含むものの種類及びバージョン

- 動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの
- フレームワーク等、ソフトウェアを実行するための実行環境となるもの
- プラグイン等、ソフトウェアの機能を拡張するもの
- 静的リンクライブラリ等、会館がソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの
- インストーラー作成ソフトウェア等、会館がソフトウェアを開発する際に開発を支援するために使用するもの

d) サーバ装置及び端末の仕様書又は設計書

5.1.1(2)-2 情報システムセキュリティ責任者は、前項 b)及び c)の情報を収集するため、自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェアを導入するなどにより、これら情報を効率的に収集する手法を決定する。

(イ) 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

5.1.1(2)-3 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を構成する通信回線及び通信回線装置関連情報として、以下を含む文書を整備する。

a) 通信回線及び通信回線装置を管理する職員等を特定する情報

b) 通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン

c) 通信回線及び通信回線装置の仕様書又は設計書
d) 通信回線の構成
e) 通信回線装置におけるアクセス制御の設定
f) 通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応
g) 通信回線の利用部門

(ウ) 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

5.1.1(2)-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について、情報システム構成要素ごとのセキュリティ維持に関する以下を含む手順を定める。

a) サーバ装置及び端末のセキュリティの維持に関する手順
b) 通信回線を介して提供するサービスのセキュリティの維持に関する手順
c) 通信回線及び通信回線装置のセキュリティの維持に関する手順

(エ) 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

5.1.2 機器等の調達に係る規定の整備

(1) 機器等の調達に係る規定の整備

(a) 統括情報セキュリティ責任者は、機器等の選定基準を整備する。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、その管理を会館が確認できることを加える。

5.1.2(1)-1 機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を例に規定する。

a) 調達した機器等に不正な変更が見付かったときに、追跡調査や立入検査等、会館と調達先が連携して原因を調査・排除できる体制を整備している。

5.1.2(1)-2 調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408 に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定める。

(b) 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。

5.1.2(1)-3 以下を確認できる手続を定める。

a) 調達時に指定したセキュリティ要件の実装状況
b) 機器等に不正プログラムが混入していない

5.2 情報システムのライフサイクルの各段階における対策

5.2.1　情報システムの企画・要件定義

(1) 実施体制の確保

a) 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。

b) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し運用管理する会館が定める運用管理規程等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。

c) 最高情報セキュリティ責任者は、前二項で求められる体制の確保に際し、情報システムを統括する責任者（情報化統括責任者（CIO））の協力を得ることが必要な場合は、当該情報システムを統括する責任者に当該体制の全部又は一部の整備を求める。

(2) 情報システムのセキュリティ要件の策定

(a) 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に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、情報システムのセキュリティ要件を策定する。

5.2.1(2)-1 情報システムセキュリティ責任者は、NISC「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を活用し、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定する。

5.2.1(2)-2 情報システムセキュリティ責任者は、開発する情報システムが運用される際に想定される脅威の分析結果並びに当該情報システムにおいて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適切に策定し、仕様書等に明記する。

(ア) 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

5.2.1(2)-3 情報システムセキュリティ責任者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書（ST：Security Target）を作成し、ST 確認を受ける。

(イ) 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）

5.2.1(2)-4 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

セキュリティ監視等の運用管理機能要件を明確化し、仕様書等へ適切に反映するために、以下を含む措置を実施する。

a) 情報システム運用時に情報セキュリティ確保のために必要となる管理機能を仕様書等に明記する。

b) 情報セキュリティインシデントの発生を監視する必要があると認めた場合には、監視のために必要な機能について、以下を例とする機能を仕様書等に明記する。

- 会館外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能
- 不正プログラム感染や踏み台に利用される等による会館外への不正な通信を監視する機能
- 端末等の組織内ネットワークの末端に位置する機器及びサーバ装置において不正プログラムの挙動を監視する機能
- 会館内通信回線への端末の接続を監視する機能
- 端末への外部電磁的記録媒体の挿入を監視する機能
- サーバ装置等の機器の動作を監視する機能

c) 暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を仕様書等に明記する。

(ウ) 情報システムに関連する脆弱性についての対策要件

5.2.1(2)-5 情報システムセキュリティ責任者は、開発する情報システムに関連する脆弱性への対策が実施されるよう、以下を含む対策を仕様書等に明記する。

a) 既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としない。

b) 開発時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針。

c) セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施される。

d) ソフトウェアのサポート期間又はサポート打ち切り計画に関する会館への情報提供。

(b) 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。

(c) 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、経済産業省「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。

5.2.1(2)-6 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の構成要素のうち、製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を含む事項を実施する。

a) 「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、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とする。ただし、「IT 製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定する。

b) 「IT 製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する機器等の利用環境において対抗すべき脅威を分析し、必要なセキュリティ要件を策定する。

(d) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体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、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定する。

(3) 情報システムの構築を外部委託する場合の対策

(a) 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外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させる。

(ア) 情報システムのセキュリティ要件の適切な実装

(イ) 情報セキュリティの観点に基づく試験の実施

5.2.1(3)-1 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に基づく試験の実施について、以下を含む事項を実施させる。

a) ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離する。

b) 情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施する。

c) 情報セキュリティの観点から実施した試験の実施記録を保存する。

(ウ) 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

5.2.1(3)-2 情報システムセキュリティ責任者は、開発工程における情報セキュリティ対策として、以下を含む事項を実施させる。

a) ソースコードが不正に変更されることを防ぐために、以下の事項を含むソースコードの管理を適切に行う。
- ソースコードの変更管理
- ソースコードの閲覧制限のためのアクセス制御
- ソースコードの滅失、き損等に備えたバックアップの取得

b) 情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従う。

c) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施する。

(4) 情報システムの運用・保守を外部委託する場合の対策

(a) 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・保守を外部委託する場合は、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、調達仕様書に記載するなどして、適切に実施させる。

5.2.1(4)-1 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・保守を外部委託する場合は、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に、以下を含む要件を調達仕様書に記載するなどして、適切に実施させる。

a) 情報システムの運用環境に課せられるべき条件の整備

b) 情報システムのセキュリティ監視を行う場合の監視手順や連絡方法

c) 情報システムの保守における情報セキュリティ対策

d) 運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策

(b) 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・保守を外部委託する場合は、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、速やかに報告させる。

5.2.2 情報システムの調達・構築

(1) 機器等の選定時の対策

(a) 情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対

する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用する。

(2) 情報システムの構築時の対策

(a) 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。

5.2.2(2)-1 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以下を含む情報セキュリティ対策を行う。

a) 情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対処するために開発環境を整備する。

b) セキュリティ要件が適切に実装されるようにセキュリティ機能を設計する。

c) 情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従う。

d) セキュリティ機能が適切に実装されている及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施する。

e) 脆弱性検査を含む情報セキュリティの観点での試験を実施する。

5.2.2(2)-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段階へ移行するに当たり、以下を含む情報セキュリティ対策を行う。

a) 情報セキュリティに関わる運用保守体制の整備

b) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

c) 情報セキュリティインシデントを認知した際の対処方法の確立

(b) 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) 納品検査時の対策

(a) 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、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する。

(b) 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。

5.2.3 情報システムの運用・保守

(1) 情報システムの運用・保守時の対策

(a) 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セキュリティ機能を適切に運用する。

5.2.3(1)-1 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監視を行う場合は、以下の内容を含む監視手順を定め、適切に監視運用する。

a) 監視するイベントの種類
b) 監視体制
c) 監視状況の報告手順
d) 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の報告手順
e) 監視運用における情報の取扱い（機密性の確保）

5.2.3(1)-2 情報システムセキュリティ責任者は、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ていることを確認する。

5.2.3(1)-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り扱う情報について、当該情報の格付及び取扱制限が適切に守られていることを確認する。

5.2.3(1)-4 情報システムセキュリティ責任者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずる。

(b) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し運用管理する会館との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用する。

(c) 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する。

5.2.4 情報システムの更改・廃棄

(1) 情報システムの更改・廃棄時の対策

(a) 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、以下の措置を適切に講ずる。

(ア) 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
(イ) 情報システム廃棄時の不要な情報の抹消

5.2.5 情報システムについての対策の見直し

(1) 情報システムについての対策の見直し

(a) 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。

5.3 情報システムの運用継続計画

5.3.1　情報システムの運用継続計画の整備・整合的運用の確保

(1) 情報システムの運用継続計画の整備・整合的運用の確保

(a) 統括情報セキュリティ責任者は、会館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必要がある場合は、非常時における情報セキュリティに係る対策事項を検討する。

(b) 統括情報セキュリティ責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認する。

第6部　情報システムのセキュリティ要件

6.1 情報システムのセキュリティ機能

6.1.1　主体認証機能

(1) 主体認証機能の導入

(a) 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。

6.1.1(1)-1 情報システムセキュリティ責任者は、利用者が正当であることを検証するための主体認証機能を設けるに当たっては、以下を例とする主体認証方式を決定し、導入する。この際、認証の強度として２つ以上の方式を組合せる主体認証方式（多要素主体認証方式）が求められる場合には、これを用いる。

a) 知識（パスワード等、利用者本人のみが知り得る情報）による認証

b) 所有（電子証明書を格納する IC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証

c) 生体（指紋や静脈等、本人の生体的な特徴）による認証

6.1.1(1)-2 情報システムセキュリティ責任者は、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、文字の種類や組合せ、桁数等のパスワード設定条件を利用者に守らせる機能を設ける。

(b) 情報システムセキュリティ責任者は、国民・企業と会館との間の申請、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。

(c) 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。

6.1.1(1)-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、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下を例とする機能を設ける。

a) 利用者が定期的に変更しているか否かを確認する機能
b) 利用者が定期的に変更しなければ、情報システムの利用を継続させない機能
c) 利用者が主体認証情報を変更する際に、以前に設定した主体認証情報の再設定を防止する機能

6.1.1(1)-4 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、主体認証情報が第三者に対して明らかにならないよう、以下を含む方法を用いて適切に管理する。

a) 主体認証情報を送信又は保存する場合には、その内容を暗号化する
b) 主体認証情報に対するアクセス制限を設ける

6.1.1(1)-5 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を他の主体に不正に利用され又は利用されるおそれを認識した場合の対策として、以下を例とする機能を設ける。

a) 当該主体認証情報及び対応する識別コードの利用を停止する機能
b) 主体認証情報の再設定を利用者に要求する機能

(2) 識別コード及び主体認証情報の管理

(a) 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。

6.1.1(2)-1 情報システムセキュリティ責任者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下本項において同じ。）する。

6.1.1(2)-2 情報システムセキュリティ責任者は、識別コードの付与に当たっては、以下を例とする措置を講ずる。

a) 単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止
b) 主体への識別コードの付与に関する記録を消去する場合の情報セキュリティ責任者からの事前の許可

6.1.1(2)-3 情報システムセキュリティ責任者は、主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずる。

6.1.1(2)-4 情報システムセキュリティ責任者は、識別コード及び知識による主

体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するように促す。

6.1.1(2)-5 情報システムセキュリティ責任者は、知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促す。

6.1.1(2)-6 情報システムセキュリティ責任者は、情報システムを利用する主体ごとに識別コードを個別に付与する。ただし、情報システムセキュリティ責任者の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与する。

(b) 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。

6.1.1(2)-7 情報システムセキュリティ責任者は、主体認証情報の不正な利用を防止するために、主体が情報システムを利用する必要がなくなった場合には、以下を例とする措置を講ずる。

a) 当該主体の識別コードを無効にする
b) 当該主体に交付した主体認証情報格納装置を返還させる
c) 無効化した識別コードを他の主体に新たに発行することを禁止する

6.1.2 アクセス制御機能

(1) アクセス制御機能の導入

(a) 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ができる機能を設ける。

6.1.2(1)-1 情報システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を定める。また、必要に応じて、以下を例とするアクセス制御機能の要件を定める。

a) 利用時間や利用時間帯によるアクセス制御
b) 同一主体による複数アクセスの制限
c) IP アドレスによる端末の制限
d) ネットワークセグメントの分割によるアクセス制御
e) ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御

(b) 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。

6.1.3　権限の管理

(1) 権限の管理

(a) 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適切に設定するよう、措置を講ずる。

(b) 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。

6.1.3(1)-1 情報システムセキュリティ責任者は、主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、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、以下を例とする措置を講ずる。

a) 業務上必要な場合に限定する

b) 必要最小限の権限のみ付与する

c) 管理者権限を行使できる端末をシステム管理者等の専用の端末とする

6.1.4　ログの取得・管理

(1) ログの取得・管理

(a) 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。

6.1.4(1)-1 情報システムセキュリティ責任者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるように設定する。

(b) 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及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理する。

6.1.4(1)-2 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特性に応じてログを取得する目的を設定し、以下を例とする、ログとして取得する情報項目を定め管理する。

a) 事象の主体（人物又は機器等）を示す識別コード

b) 識別コードの発行等の管理記録

c) 情報システムの操作記録

d) 事象の種類

e) 事象の対象
f) 正確な日付及び時刻
g) 試みられたアクセスに関わる情報
h) 電子メールのヘッダ情報及び送信内容
i) 通信パケットの内容
j) 操作する者、監視する者、保守する者等への通知の内容

6.1.4(1)-3 情報システムセキュリティ責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定める。

6.1.4(1)-4 情報システムセキュリティ責任者は、ログが取得できなくなった場合の対処方法を定める。

(c) 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。

6.1.4(1)-5 情報システムセキュリティ責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、以下を例とする、当該作業を支援する機能を導入する。

a) ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の自動化

6.1.5 暗号・電子署名

(1) 暗号化機能・電子署名機能の導入

(a) 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、以下の措置を講ずる。

(ア) 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、必要があると認めたときは、当該機能を設ける。

(イ) 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、必要があると認めたときは、当該機能を設ける。

6.1.5(1)-1 情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずる。

a) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする
b) 複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とする
c) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の

付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する

d) 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は、耐タンパ性を有する暗号モジュールへ格納する

e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のあるプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する

(b) 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」を参照した上で、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並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定める。

(ア) 職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させる。

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用する。

(ウ) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定める。

(エ) 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、管理手順を定める。

(c) 情報システムセキュリティ責任者は、会館における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、それを使用するように定める。

(2) 暗号化・電子署名に係る管理

(a) 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、以下の措置を講ずる。

(ア) 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。

6.1.5(2)-1 情報システムセキュリティ責任者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする

方法により、当該情報の提供を可能とする。

a) 信頼できる機関による電子証明書の提供

b) 会館の窓口での電子証明書の提供

(イ) 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、職員等と共有を図る。

6.2 情報セキュリティの脅威への対策

6.2.1 ソフトウェアに関する脆弱性対策

(1) ソフトウェアに関する脆弱性対策の実施

(a) 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。

6.2.1(1)-1 情報システムセキュリティ責任者は、対象となるソフトウェアの脆弱性に関して、以下を含む情報を適宜入手する。

a) 脆弱性の原因

b) 影響範囲

c) 対策方法

d) 脆弱性を悪用する不正プログラムの流通状況

6.2.1(1)-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はサポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しない。

6.2.1(1)-3 情報システムセキュリティ責任者は、以下を例とする手段で脆弱性対策の状況を確認する。

a) 構成要素ごとにソフトウェアのバージョン等を把握し、当該ソフトウェア脆弱性の有無を確認する。

b) 脆弱性診断を実施する。

(b) 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とり得る対策がある場合は、当該対策を実施する。

(c) 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に確認する。

6.2.1(1)-4 情報システムセキュリティ責任者は、脆弱性対策の状況を確認する間隔を、可能な範囲で短くする。

(d) 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。

6.2.1(1)-5 情報システムセキュリティ責任者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の事項について判断する。

a) 対策の必要性
b) 対策方法。この際、自動でソフトウェアを更新する機能を有する IT 資産管理ソフトウェアを導入するなどにより、効率的に脆弱性対策を実施する手法を予め決定する
c) 対策方法が存在しないゼロデイと呼ばれる状態の場合又は対策が完了するまでの期間に対する一時的な回避方法
d) 対策方法又は回避方法が情報システムに与える影響
e) 対策の実施予定時期
f) 対策試験の必要性
g) 対策試験の方法
h) 対策試験の実施予定時期

6.2.1(1)-6 情報システムセキュリティ責任者は、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認する。

6.2.1(1)-7 情報システムセキュリティ責任者は、脆弱性対策を実施する場合には、少なくとも以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録する。

a) 実施日
b) 実施内容
c) 実施者

6.2.1(1)-8 情報システムセキュリティ責任者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「対策用ファイル」という。）は、信頼できる方法で入手する。

6.2.2 不正プログラム対策

(1) 不正プログラム対策の実施

(a) 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。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

6.2.2(1)-1 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ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入する。

6.2.2(1)-2 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ソフトウェア等が常に最新の状態となるように構成する。

6.2.2(1)-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ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態なるように構成する。

6.2.2(1)-4 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ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しない。

6.2.2(1)-5 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ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成する。

(b) 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。

6.2.2(1)-6 情報システムセキュリティ責任者は、想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行う。

(c) 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。

6.2.2(1)-7 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実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行う。

a) 不正プログラム対策ソフトウェア等の導入状況
b) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況

6.2.3 サービス不能攻撃対策

(1) サービス不能攻撃対策の実施

(a) 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。以下本条において同じ。）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。

6.2.3(1)-1 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について、以下を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処する。

a) パケットフィルタリング機能
b) 3-way handshake 時のタイムアウトの短縮
c) 各種 Flood 攻撃への防御

d) アプリケーションゲートウェイ機能

(b) 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。

6.2.3(1)-2 情報システムセキュリティ責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する又は通信回線の通信量を制限するなどの手段を有する情報システムを構築する。

6.2.3(1)-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に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、以下を例とする対策を検討する。

a) インターネットに接続している通信回線の提供元となる事業者が別途提供するサービス不能攻撃に係る通信の遮断等の対策

b) サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入

c) サーバ装置、端末及び通信回線装置及び通信回線の冗長化

6.2.3(1)-4 情報システムセキュリティ責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討する。

(c) 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。

6.2.3(1)-5 情報システムセキュリティ責任者は、特定した監視対象について、監視方法及び監視記録の保存期間を定める。

6.2.3(1)-6 情報システムセキュリティ責任者は、監視対象の監視記録を保存する。

6.2.4 標的型攻撃対策

(1) 標的型攻撃対策の実施

(a) 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、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずる。

6.2.4(1)-1 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ついて、組織内部への侵入を低減するため、以下を例とする対策を行う。

a) 不要なサービスについて機能を削除又は停止する。

b) 不審なプログラムが実行されないよう設定する

c) パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する

6.2.4(1)-2 情報システムセキュリティ責任者は、USB メモリ等の外部電磁的記

録媒体を利用した組織内部への侵入を低減するため、以下を例とする対策を行う。

a) 出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させない。接続する外部電磁的記録媒体を事前に特定しておく
b) 外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する
c) サーバ装置及び端末について、自動再生（オートラン）機能を無効化する
d) サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする
e) サーバ装置及び端末について、使用を想定しない USB ポートを無効化する
f) 組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する

(b) 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、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる及び外部との不正通信を検知して対処する対策（内部対策）を講ずる。

6.2.4(1)-3 情報システムセキュリティ責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を例とする対策を行う。

a) 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない
b) 認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずる

6.2.4(1)-4 情報システムセキュリティ責任者は、端末の管理者権限アカウントについて、以下を例とする対策を行う。

a) 不要な管理者権限アカウントを削除する
b) 管理者権限アカウントのパスワードは、容易に推測できないものに設定する

6.2.4(1)-5 情報システムセキュリティ責任者は、重点的に守るべき業務・情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに従って、対策を講ずる。

6.3 アプリケーション・コンテンツの作成・提供

6.3.1 アプリケーション・コンテンツの作成時の対策

(1) アプリケーション・コンテンツの作成に係る規定の整備

(a) 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会館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規定を整備する。

(2) 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

(a) 情報システムセキュリティ責任者は、会館外の情報システム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・コンテンツについて以下の内容を仕様に含める。

(ア) 提供するアプリケーション・コンテンツが不正プログラムを含まない。

6.3.1(2)-1 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を含む対策を行う。

a) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認する。

b) 外部委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させる。

(イ) 提供するアプリケーションが脆弱性を含まない。

(ウ) 実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラムの形式でコンテンツを提供しない。

(エ) 電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与える。

6.3.1(2)-4 情報システムセキュリティ責任者は、改ざん等がなく真正なものであることを確認できる手段として電子証明書を用いた署名を提供する際に、政府認証基盤（GPKI）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施す。

(オ) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発する。

(カ) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発する。

6.3.1(2)-2 情報システムセキュリティ責任者は、提供するアプリケーショ

ン・コンテンツにおいて、会館外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTMLソースを表示させるなどして確認する。必要があって当該機能を含める場合は、当該会館外へのアクセスが情報セキュリティ上安全なものであることを確認する。

6.3.1(2)-3 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツに、本来のサービス提供に必要のない会館外へのアクセスを自動的に発生させる機能を含めない。

(b) 職員等は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前項各号に掲げる内容を調達仕様に含める。

6.3.2 アプリケーション・コンテンツ提供時の対策

(1) 政府ドメイン名の使用

(a) 情報システムセキュリティ責任者は、会館外向けに提供するウェブサイト等が実際の会館提供のものであることを利用者が確認できるように、政府ドメイン名を情報システムにおいて使用する。ただし、4.1.3 に掲げるソーシャルメディアサービスによる情報発信を行う場合。

(b) 職員等は、会館外向けに提供するウェブサイト等の作成を外部委託する場合においては、前項各号列記以外の部分、同項(ア)及び(イ)の規定に則り会館に適するドメイン名を使用するよう調達仕様に含める。

(2) 不正なウェブサイトへの誘導防止

(a) 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会館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。

6.3.2(2)-1 情報システムセキュリティ責任者は、会館外向けに提供するウェブサイトに対して、以下を例とする検索エンジン最適化措置（SEO 対策）を講ずる。

a) クローラからのアクセスを排除しない
b) cookie 機能を無効に設定したブラウザでも正常に閲覧可能とする
c) 適切なタイトルを設定する
d) 不適切な誘導を行わない

6.3.2(2)-2 情報システムセキュリティ責任者は、会館外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト業者へ報告するとともに、不審なサイトへのアクセスを防止するための対策を講ずる。

(3) アプリケーション・コンテンツの告知

(a) 職員等は、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。

6.3.2(3)-1 職員等は、アプリケーション・コンテンツを告知するに当たって、誘導を確実なものとするため、URL 等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、URL 等と一体的に表示する。また、短縮 URL を用いない。

6.3.2(3)-2 職員等は、アプリケーション・コンテンツを告知するに当たって、URL を二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示する。

(b) 職員等は、会館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。

a) 告知するアプリケーション・コンテンツを管理する組織名を明記する

b) 告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記する

第7部　情報システムの構成要素

7.1 端末・サーバ装置等

7.1.1　端末

(1) 端末の導入時の対策

(a) 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。

7.1.1(1)-1 情報システムセキュリティ責任者は、モバイル端末を除く端末について、原則としてクラス２以上の要管理対策区域に設置する。

7.1.1(1)-2 情報システムセキュリティ責任者は、端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずる。モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する。モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意する。

7.1.1(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずる。

一定時間操作が無いと自動的にスクリーンロックするよう設定する。要管理対策区域外で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。

(b) 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及び利用を禁止するソフトウェアを定める。

7.1.1(1)-4 情報システムセキュリティ責任者は、以下を考慮した上で、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める。

a) ソフトウェアベンダ等のサポート状況
b) ソフトウェアと外部との通信の有無及び通信する場合はその通信内容
c) インストール時に同時にインストールされる他のソフトウェア
d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

(2) 端末の運用時の対策

(a) 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及び利用を禁止するソフトウェアについて定期的に見直しを行う。

(b) 情報システムセキュリティ責任者は、所管する範囲の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。

(3) 端末の運用終了時の対策

(a) 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する。

(4) 要機密情報を取り扱う会館が支給する端末（要管理対策区域外で使用する場合に限る）並びに会館支給以外の端末の導入及び利用時の対策

(a) 統括情報セキュリティ責任者は、要機密情報を取り扱う会館が支給する端末（要管理対策区域外で使用する場合に限る）及び会館支給以外の端末について、以下の安全管理措置に関する規定を整備する。

(ア) 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

7.1.1(4)-1　以下を例に、利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を設ける。

a) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする
b) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする
c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する

d) 端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける

e) 上記の各号のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける

f) ハードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により消去する機能を設ける。ただし、この場合は本項 c)～e)を例とする暗号化の機能を組み合わせる

(イ) 会館支給以外の端末において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利用時の措置

7.1.1(4)-2　以下を例に、職員等が講ずるべき利用時の実施手順に係る安全管理措置を設ける。

a) パスワード等による端末ロックの常時設定

b) OS やアプリケーションの最新化

c) 不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（会館として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）

d) 端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある）

e) 会館提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）

f) 以下を例とする禁止事項の遵守

- 端末、OS、アプリケーション等の改造行為
- 安全性が確認できないアプリケーションのインストール及び利用
- 利用が禁止されているソフトウェアのインストール及び利用
- 許可されない通信回線サービスの利用（利用する回線を限定する場合）
- 第三者への端末の貸与

(b) 情報セキュリティ責任者は、会館支給以外の端末を用いた会館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。

(c) 次の各号に掲げる責任者は、職員等が当該各号に定める端末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(a)(ア)の安全管理措置を講ずる。

(ア) 情報システムセキュリティ責任者：会館が支給する端末（要管理対策区域外で使用する場合に限る）

(イ) 端末管理責任者：会館支給以外の端末

(d) 端末管理責任者は、要機密情報を取り扱う会館支給以外の端末について、前項

の規定にかかわらず(a)(ア)に定める安全管理措置のうち自ら講ずることができないもの、及び(a)(イ)に定める安全管理措置を職員等に講じさせる。

(e) 職員等は、要機密情報を取り扱う会館支給以外の端末について、前項において(a)(ア)に定める安全管理措置のうち端末管理責任者が講ずることができないもの、及び(a)(イ)に定める安全管理措置を講ずる。

7.1.2 サーバ装置

(1) サーバ装置の導入時の対策

(a) 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。

7.1.2(1)-1 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サーバ装置については、クラス２以上の要管理対策区域に設置する。

7.1.2(1)-2 情報システムセキュリティ責任者は、サーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずる。

a) 施錠可能なサーバラックに設置して施錠する。

b) 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。

7.1.2(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずる。

a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。

(b) 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。

7.1.2(1)-4 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は、将来の見通しも考慮し、以下を例とする対策を講ずる。

a) 負荷分散装置、DNS ラウンドロビン方式等による負荷分散

b) 同一システムを２系統で構成することによる冗長化

(c) 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及び利用を禁止するソフトウェアを定める。

7.1.2(1)-5 情報システムセキュリティ責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定める。

a) ソフトウェアベンダ等のサポート状況
b) ソフトウェアと外部との通信の有無及び通信する場合はその通信内容
c) インストール時に同時にインストールされる他のソフトウェア
d) その他、ソフトウェアの利用に伴う情報セキュリティリスク

(d) 情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずる。

(2) サーバ装置の運用時の対策

(a) 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及び利用を禁止するソフトウェアについて定期的に見直しを行う。

(b) 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。

7.1.2(2)-1 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する場合は、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録する。

(c) 情報システムセキュリティ責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずる。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

7.1.2(2)-2 情報システムセキュリティ責任者は、サーバ装置への無許可のアクセス等の不正な行為を監視するために、以下を例とする対策を講ずる。

a) アクセスログ等を定期的に確認する
b) IDS/IPS、WAF 等を設置する
c) 不正プログラム対策ソフトウェアを利用する
d) ファイル完全性チェックツールを利用する
e) CPU、メモリ、ディスク I/O 等のシステム状態を確認する

(d) 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、サーバ装置が運用できなくなった場合に正常な運用状態に復元することが可能となるよう、必要な措置を講ずる。

7.1.2(2)-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サーバ装置については、運用状態を復元するために以下を例とする対策を講ずる。

a) サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく
b) 定期的なバックアップを実施する
c) サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する
d) バックアップとして取得した情報からサーバ装置の運用状態を復元する

ための訓練を実施する

(3) サーバ装置の運用終了時の対策

(e) 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する。

7.1.3 複合機・特定用途機器

(1) 複合機

(a) 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。

7.1.3(1)-1 情報システムセキュリティ責任者は、「IT 製品の調達におけるセキュリティ要件リスト」を参照するなどし、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、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記する。

(b) 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。

7.1.3(1)-2 情報システムセキュリティ責任者は、以下を例とする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。

a) 複合機について、利用環境に応じた適切なセキュリティ設定を実施する
b) 複合機が備える機能のうち利用しない機能を停止する
c) 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用する
d) 会館内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにする
e) 複合機をインターネットに直接接続しない
f) リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う
g) 利用者ごとに許可される操作を適切に設定する

(c) 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する。

7.1.3(1)-3 情報システムセキュリティ責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消する。当該機能を備えていない複合機

については、外部委託先との契約時に外部委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずる。

(2) IoT 機器を含む特定用途機器

(a) 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。

7.1.3(2)-1 情報システムセキュリティ責任者は、特定用途機器の特性に応じて、以下を含む対策を講ずる。ただし、使用している特定用途機器の機能上の制約により講ずることができない対策を除く。

a) 特定用途機器について、主体認証情報を初期設定から変更した上で、適切に管理する

b) 特定用途機器にアクセスする主体に応じて必要な権限を割り当て、管理する

c) 特定用途機器が備える機能のうち利用しない機能を停止する

d) インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットや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

e) 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う

f) 特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる

g) 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する

h) 特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消する

7.2 電子メール・ウェブ等

7.2.1 電子メール

(1) 電子メールの導入時の対策

(a) 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。

(b) 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。

7.2.1(1)-1 以下を例とする職員等の主体認証を行う機能を備える。

a) 電子メールの受信時に限らず、送信時においても不正な利用を排除するために SMTP 認証等の主体認証機能を導入する。

(c) 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。

7.2.1(1)-2　以下を例とする電子メールのなりすましの防止策を講ずる。

a) SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）、DMARC （ Domain-based Message Authentication, Reporting &Conformance）等の送信ドメイン認証技術による送信側の対策を行う

b) SPF、DKIM、 DMARC 等の送信ドメイン認証技術による受信側の対策を行う

c) S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用する

(d) 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。

7.2.1(1)-3　以下を例とする電子メールの盗聴及び改ざんの防止策を講ずる。

a) SMTP によるサーバ間通信を TLS（SSL）により保護する

b) S/MIME 等の電子メールにおける暗号化及び電子署名の技術を利用する

7.2.2　ウェブ

(1) ウェブサーバの導入・運用時の対策

(a) 情報システムセキュリティ責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずる。

(ア) ウェブサーバが備える機能のうち、不要な機能を停止又は制限する。

7.2.2(1)-1　以下を例とするウェブサーバの管理や設定を行う。

a) CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とする

b) ディレクトリインデックスの表示を禁止する

c) ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限する

d) ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する

(イ) ウェブコンテンツの編集作業を担当する主体を限定する。

7.2.2(1)-2　以下を例とするウェブサーバの管理や設定を行う。

a) ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコ

ンテンツの作成や更新に必要な者以外に更新権を与えない

b) OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する

(ウ) 公開してはならない又は無意味なウェブコンテンツが公開されないように管理する。

7.2.2(1)-3　以下を例とするウェブサーバの管理や設定を行う。

a) 公開を想定していないファイルをウェブ公開用ディレクトリに置かない

b) 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する

(エ) ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理する。

7.2.2(1)-4　以下を例とするウェブサーバの管理や設定を行う。

a) ウェブコンテンツの更新の際は、専用の端末を使用して行う

b) ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限する

c) ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行う

(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る。

7.2.2(1)-5　以下を含むウェブサーバの実装を行う。

a) TLS（SSL）機能を適切に用いる

b) TLS（SSL）機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる

c) 暗号技術検討会及び関連委員会（CRYPTREC）により作成された「SSL/TLS 暗号設定ガイドライン」に従って、TLS（SSL）サーバを適切に設定する

(b) 情報システムセキュリティ責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認する。

(2) ウェブアプリケーションの開発時・運用時の対策

(a) 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、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。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行う。

7.2.2(2)-1　以下を含むウェブアプリケーションの脆弱性を排除する。

a) SQL インジェクション脆弱性
b) OS コマンドインジェクション脆弱性
c) ディレクトリトラバーサル脆弱性
d) セッション管理の脆弱性
e) アクセス制御欠如と認可処理欠如の脆弱性
f) クロスサイトスクリプティング脆弱性
g) クロスサイトリクエストフォージェリ脆弱性
h) クリックジャッキング脆弱性
i) メールヘッダインジェクション脆弱性
j) HTTP ヘッダインジェクション脆弱性
k) eval インジェクション脆弱性
l) レースコンディション脆弱性
m) バッファオーバーフロー及び整数オーバーフロー脆弱性

7.2.3　ドメインネームシステム（DNS）

(1) DNS の導入時の対策

(a) 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。

7.2.3(1)-1　以下を例とする名前解決を停止させないための措置を講ずる。

a) コンテンツサーバを冗長化する
b) 通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う

(b) 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。

7.2.3(1)-2 情報システムセキュリティ責任者は、会館外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は必要であれば会館内からの名前解決の要求のみに応答をするよう、以下を例とする措置を講ずる。

a) キャッシュサーバの設定でアクセス制御を行う
b) ファイアウォール等でアクセス制御を行う

7.2.3(1)-3 情報システムセキュリティ責任者は、DNS キャッシュポイズニング攻撃から保護するため、以下を例とする措置を講ずる。

a) ソースポートランダマイゼーション機能を導入する
b) DNSSEC を利用する

(c) 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、会館のみで

使用する名前の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。

7.2.3(1)-4　以下を例とする当該コンテンツサーバで管理する情報の漏えいを防止するための措置を講ずる。

a)　外部向けのコンテンツサーバと別々に設置する

b)　ファイアウォール等でアクセス制御を行う

(2) DNS の運用時の対策

(a) 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。

(b) 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に確認する。

(c) 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。

7.2.3(2)-1　ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（３か月に一度程度）に確認し、最新の DNS ルートサーバの情報を維持する。

7.2.4　データベース

(1) データベースの導入・運用時の対策

(a) 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。

7.2.4(1)-1　必要に応じて情報システムの管理者とデータベースの管理者を別にする。

7.2.4(1)-2　データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しない。

7.2.4(1)-3　データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずる。

(b) 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。

(c) 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に対策を講ずる。

7.2.4(1)-4　以下を例とする措置を講ずる。

a)　一定数以上のデータの取得に関するログを記録し、警告を発する

b)　データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する

(d) 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。

7.2.4(1)-5 情報システムセキュリティ責任者は、データベースにアクセスする機器上で動作するプログラムに対して、SQL インジェクションの脆弱性を排除する。

7.2.4(1)-6 情報システムセキュリティ責任者は、データベースにアクセスする機器上で動作するプログラムに対して SQL インジェクションの脆弱性の排除が不十分であると判断した場合、以下を例とする対策の実施を検討する。

a) ウェブアプリケーションファイアウォールの導入
b) データベースファイアウォールの導入

(e) 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。

7.2.4(1)-7 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して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施する。

7.3 通信回線

7.3.1 通信回線

(1) 通信回線の導入時の対策

(a) 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。

7.3.1(1)-1 情報システムセキュリティ責任者は、以下を例とする通信経路の分離を行う。

a) 外部との通信を行うサーバ装置及び通信回線装置のセグメントを DMZ として構築し、内部のセグメントと通信経路を分離する
b) 業務目的や取り扱う情報の格付及び取扱制限に応じて情報システムごとに VLAN により通信経路を分離し、それぞれの通信制御を適切に行う
c) 他の情報システムから独立した専用の通信回線を構築する

(b) 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。

(c) 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。

7.3.1(1)-2 情報システムセキュリティ責任者は、通信回線の秘匿性確保の方法として、TLS（SSL）、IPsec 等による暗号化を行う。また、その際に使用す

る暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定する。

(d) 情報システムセキュリティ責任者は、職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。会館内通信回線へ会館支給以外の端末を接続する際も同様とする。

7.3.1(1)-3 情報システムセキュリティ責任者は、会館内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずる。

a) 情報システムの機器番号等により接続機器を識別する
b) クライアント証明書により接続機器の認証を行う

情報システムセキュリティ責任者は、通信回線装置を要管理対策区域に設置する。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、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。

7.3.1(1)-4 情報システムセキュリティ責任者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策として、以下を例とする措置を講ずる。

a) 通信回線装置を施錠可能なラック等に設置する
b) 会館の施設内に敷設した通信ケーブルを物理的に保護する
c) 通信回線装置の操作ログを取得する

(e) 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措置を講ずる。

7.3.1(1)-5 以下を例とする対策を講ずる。

a) 通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける
b) 通信回線及び通信回線装置を冗長構成にする

(f) 情報システムセキュリティ責任者は、会館内通信回線にインターネット回線、公衆通信回線等の会館外通信回線を接続する場合には、会館内通信回線及び当該会館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。

7.3.1(1)-6　外部からの不正アクセスによる被害を防止するため、以下を例とする対策を講ずる。

a) ファイアウォール、WAF（Web Application Firewall）、リバースプロキシ等により通信制御を行う
b) 通信回線装置による特定の通信プロトコルの利用を制限する
c) IDS/IPS により不正アクセスを検知及び遮断する

(g) 情報システムセキュリティ責任者は、会館内通信回線と会館外通信回線との間で送受信される通信内容を監視するための措置を講ずる。

(h) 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を定め、ソフトウェアを変更する際の許可申請手順を整備する。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。

(i) 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、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保する。

7.3.1(1)-7　以下を例とする対策を講ずる。

a) リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行う

b) 主体認証によりアクセス制御する

c) 通信内容の暗号化により秘匿性を確保する

d) ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにする

(j) 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。

(2) 通信回線の運用時の対策

(a) 情報システム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よる影響を防止するために、通信回線装置の運用時に必要な措置を講ずる。

7.3.1(2)-1 情報システムセキュリティ責任者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施する場合は、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。

7.3.1(2)-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。

(b) 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見直しを行う。

(c) 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を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図る。

(d) 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。

(3) 通信回線の運用終了時の対策

(a) 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。

(4) リモートアクセス環境導入時の対策

(a) 情報システムセキュリティ責任者は、職員等の業務遂行を目的としたリモートアクセス環境を、会館外通信回線を経由して会館の情報システムへリモートアクセスする形態により構築する場合は、VPN 回線を整備するなどして、通信経路及びアクセス先の情報システムのセキュリティを確保する。

7.3.1(4)-1 情報システムセキュリティ責任者は、VPN 回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講ずる。

a) 利用開始及び利用停止時の申請手続の整備
b) 通信を行う端末の識別又は認証
c) 利用者の認証
d) 通信内容の暗号化
e) 主体認証ログの取得及び管理
f) リモートアクセスにおいて利用可能な公衆通信網の制限
g) アクセス可能な情報システムの制限
h) リモートアクセス中の他の通信回線との接続禁止

(5) 無線 LAN 環境導入時の対策

(a) 情報システムセキュリティ責任者は、無線 LAN 技術を利用して会館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。

7.3.1(5)-1 情報システムセキュリティ責任者は、以下を例とする対策を講ずる。

a) SSID の隠ぺい
b) 無線 LAN 通信の暗号化
c) MAC アドレスフィルタリングによる端末の識別
d) 802.1X による無線 LAN へのアクセス主体の認証
e) 無線 LAN 回線利用申請手続の整備
f) 無線 LAN 機器の管理手順の整備

g) 無線 LAN と接続する情報システムにおいて不正プログラム感染を認知した場合の対処手順の整備

7.3.2 IPv6 通信回線

(1) IPv6 通信を行う情報システムに係る対策

(a) 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、可能な場合には選択する。

(b) 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、以下の事項を含む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。

(ア) グローバル IP アドレスによる直接の到達性における脅威

(イ) IPv6 通信環境の設定不備等に起因する不正アクセスの脅威

(ウ) IPv4 通信と IPv6 通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生

(エ) アプリケーションにおける IPv6 アドレスの取扱い考慮漏れに起因する脆弱性の発生

(2) 意図しない IPv6 通信の抑止・監視

(a) 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、IPv6 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 IPv6 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 IPv6 通信による情報セキュリティ上の脅威を防止するため、IPv6 通信を抑止するなどの措置を講ずる。

第8部 情報システムの利用

8.1 情報システムの利用

8.1.1 情報システムの利用

(1) 情報システムの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、会館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規定を整備する。

8.1.1(1)-1 以下を例とする実施手順を定める。

a) 情報システムの基本的な利用のうち、情報セキュリティに関する手順

b) 電子メール及びウェブの利用のうち、情報セキュリティに関する手順

c) 識別コードと主体認証情報の取扱手順

d) 暗号と電子署名の利用に関する手順

e) 不正プログラム感染防止の手順

f) アプリケーション・コンテンツの提供時に会館外の情報セキュリティ水

準の低下を招く行為の防止に関する手順

g) ドメイン名の使用に関する手順

(b) 統括情報セキュリティ責任者は、職員等が、会館が支給する端末（要管理対策区域外で使用する場合に限る）及び会館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、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定める。

8.1.1(1)-2 以下を例として定める。

a) 端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化

b) 盗み見に対する対策（のぞき見防止フィルタの利用等）

c) 盗難・紛失に対する対策（不要な情報を端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど）

d) 利用する場所や時間の限定

e) 端末の盗難・紛失が発生した際の緊急対応手順

8.1.1(1)-3 以下を含む許可手続を定める。

a) 利用時の許可申請手続

b) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線への接続形態等）

c) 利用期間満了時の手続

d) 許可権限者（課室情報セキュリティ責任者）による手続内容の記録

(c) 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会館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会館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（支給外端末を含む）から会館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規定及び許可手続を定める。

8.1.1(1)-4 以下を含む手続を規定し、職員等に遵守させる。

a) 利用時の許可申請手続

b) 手続内容（利用者、目的、利用する情報、端末等）

c) 利用期間満了時の手続

d) 許可権限者（課室情報セキュリティ責任者）による手続内容の記録

(d) 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利用手順を定める。当該手順には、以下の事項を含める。

(ア) 職員等は、会館が支給する外部電磁的記録媒体、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により会館との間で取り決めた会館外の組織から受け取った

外部電磁的記録媒体を使用する。

(イ) 自組織以外の組織から受け取った外部電磁的記録媒体は、自組織と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずる。

8.1.1(1)-5 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利用手順として以下の事項を含めて定める。

a) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する

b) 要機密情報は保存される必要がなくなった時点で速やかに削除する

c) 外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫・駆除を行う

d) 外部電磁的記録媒体の利用者が利用内容を貸出簿等に記録する

(e) 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。

8.1.1(1)-6 以下を含む手続を規定し、職員等に遵守させる。

a) 利用時の許可申請手続

b) 手続内容（利用者、利用期間、主たる利用場所、目的、記録する情報、機器名）

c) 利用期間満了時の手続

d) 許可権限者（課室情報セキュリティ責任者）による手続内容の記録

(2) 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

(a) 情報システムセキュリティ責任者は、職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。

8.1.1(2)-1 情報システムセキュリティ責任者は、会館外のウェブサイトについて、職員等が閲覧できる範囲を制限する機能を情報システムに導入する。具体的には、以下を例とする機能を導入する。また、当該機能に係る設定や条件について定期的に見直す。

a) ウェブサイトフィルタリング機能

b) 事業者が提供するウェブサイトフィルタリングサービスの利用

8.1.1(2)-2 情報システムセキュリティ責任者は、職員等が不審な電子メールを受信することによる被害をシステム的に抑止する機能を情報システムに導入する。具体的には、以下を例とする機能を導入する。また、当該機能に係る設定や条件について定期的に見直す。

a) 受信メールに対するフィルタリング機能

b) 受信メールをテキスト形式で表示する機能
c) スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがない電子メールクライアントの導入
d) 受信メールに添付されている実行プログラム形式のファイルを削除等することで実行させない機能

(3) 情報システムの利用時の基本的対策

(a) 職員等は、業務の遂行以外の目的で情報システムを利用しない。

(b) 職員等は、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会館の情報システムを接続しない。

(c) 職員等は、会館内通信回線に、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ない。

(d) 職員等は、情報システムで利用を禁止するソフトウェアを利用しない。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得る。

(e) 職員等は、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ない。

(f) 職員等は、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。

8.1.1(3)-1 職員等は、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に、以下を例とする措置を講ずる。

a) スクリーンロックの設定
b) 利用後のログアウト徹底
c) 利用後に情報システムを鍵付き保管庫等に格納し施錠

(g) 職員等は、会館が支給する端末（要管理対策区域外で使用する場合に限る）及び会館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。

(h) 職員等は、次の各号に掲げる端末を用いて当該各号に定める情報を取り扱う場合は、課室情報セキュリティ責任者の許可を得る。

(ア) 会館が支給する端末（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

(イ) 会館支給以外の端末 要保護情報

(i) 職員等は、要管理対策区域外において会館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会館内通信回線に接続する場合には、定められた安全管理措置を講ずる。

(j) 職員等は、要管理対策区域外において会館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会館内通信回線に接続する場合には、課室情報セキュリティ責任者の許可を得る。

(k) 職員等は、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、課室情報セキュリティ責任者の許可を得る。

(4) 電子メール・ウェブの利用時の対策

(a) 職員等は、要機密情報を含む電子メールを送受信する場合には、会館が運営し、又は外部委託した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。

(b) 職員等は、会館外の者と電子メールにより情報を送受信する場合は、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。

(c) 職員等は、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。

(d) 職員等は、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。

(e) 職員等は、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。

(f) 職員等は、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、以下の事項を確認する。

(ア) 送信内容が暗号化される

(イ) 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

(5) 識別コード・主体認証情報の取扱い

(a) 職員等は、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。

(b) 職員等は、自己に付与された識別コードを適切に管理する。

8.1.1(5)-1 職員等は、以下を含む措置を講ずる。

a) 知る必要のない者に知られるような状態で放置しない

b) 他者が主体認証に用いるために付与及び貸与しない

c) 識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止する

(c) 職員等は、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。

(d) 職員等は、自己の主体認証情報の管理を徹底する。

8.1.1(5)-2 職員等は、知識による主体認証情報を用いる場合には、以下の管理を徹底する。

a) 自己の主体認証情報を他者に知られないように管理する

b) 自己の主体認証情報を他者に教えない

c) 主体認証情報を忘却しないように努める

d) 主体認証情報を設定するに際しては、推測されないものにする
e) 異なる識別コードに対して、共通の主体認証情報を用いない
f) 異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いない（シングルサインオンの場合を除く。）
g) 情報システムセキュリティ責任者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更する

8.1.1(5)-3 職員等は、所有による主体認証情報を用いる場合には、以下の管理を徹底する。主体認証情報装置の例としては、建物への入退や端末ログインに必要となるICカード等が挙げられる。

a) 主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理する
b) 主体認証情報格納装置を他者に付与及び貸与しない
c) 主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告する
d) 主体認証情報格納装置を利用する必要がなくなった場合には、これを情報システムセキュリティ責任者に返還する

(6) 暗号・電子署名の利用時の対策

(a) 職員等は、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及び方法に従う。

(b) 職員等は、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。

(c) 職員等は、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。

(7) 不正プログラム感染防止

(a) 職員等は、不正プログラム感染防止に関する措置に努める。

8.1.1(7)-1 職員等は、不正プログラム対策ソフトウェア等を活用し、不正プログラム感染を回避するための以下措置に努める。

a) 不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行しない。また、検知されたデータファイルをアプリケーション等で読み込まない
b) 不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持する
c) 不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にする
d) 不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施する

8.1.1(7)-2 職員等は、外部からデータやソフトウェアをサーバ装置及び端末等

に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認する。

8.1.1(7)-3 職員等は、不正プログラムに感染するリスクを低減する情報システム（支給外端末を含む）の利用方法として、以下のうち実施可能な措置を講ずる。

a) 不審なウェブサイトを閲覧しない
b) アプリケーションの利用において、マクロ等の自動実行機能を無効にする
c) プログラム及びスクリプトの実行機能を無効にする
d) 安全性が確実でないプログラムをダウンロードしたり実行したりしない

(b) 職員等は、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するなど、必要な措置を講ずる。

8.2 会館支給以外の端末の利用

8.2.1 会館支給以外の端末の利用

(1) 会館支給以外の端末の利用可否の判断

(a) 最高情報セキュリティ責任者は、会館支給以外の端末の利用について、取り扱うとなる情報の格付及び取扱制限、会館が講じる安全管理措置、当該端末の管理は会館ではなくその所有者が行う等を踏まえ、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、会館における会館支給以外の端末の利用の可否を判断する。

(2) 会館支給以外の端末の利用規定の整備・管理

(a) 統括情報セキュリティ責任者は、職員等が会館支給以外の端末を用いて会館の業務に係る情報処理を行う場合の許可等の手続を定める。

8.2.1(2)-1 以下を含む許可等の手続を整備し、職員等に周知する。

a) 以下を含む会館支給以外の端末利用時の申請内容
- 申請者の氏名、所属、連絡先
- 利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）
- 利用する端末の機種名
- 利用目的、取り扱う情報の概要、要機密情報の利用の有無等
- 主要な利用場所
- 利用する主要な通信回線サービス
- 利用する期間

b) 利用許諾条件
c) 申請手順

d) 利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順
e) 利用期間満了時の利用終了又は利用期間更新の手続方法
f) 許可権限者（端末管理責任者）

(3) 会館支給以外の端末の利用時の対策

(a) 職員等は、会館支給以外の端末を用いて会館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る。

(b) 職員等は、情報処理の目的を完了した場合は、要保護情報を会館支給以外の端末から消去する。

附則

この要領は令和 1 年（2019 年）12 月 1 日から適用する。

用語

[1] 情報の格付の区分の定義

情報について、機密性、完全性及び可用性の３つの観点を区別し、ポリシーの遵守事項で用いる格付の区分の定義を示す。

なお、会館において格付の定義を変更又は追加する場合には、その定義に従って区分された情報が、「政府機関の情報セキュリティ対策のための統一基準」の遵守事項で定めるセキュリティ水準と同等以上の水準で取り扱われるようにしなければならない。

また、他機関等へ情報を提供する場合は、自組織の格付区分とポリシーにおける格付区分の対応について、適切に伝達する必要がある。

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、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。以下「文書管理ガイドライン」という。）に定める秘密文書に相当する機密性を要する情報を含む
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。

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、誤謬又は破損により、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。

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] 統一基準「用語定義」において定義されている用語

【あ】

- 「アプリケーション・コンテンツ」とは、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。
- 「委託先」とは、外部委託により機関等の情報処理業務の一部又は全部を実施する者をいう。

【か】

- 「外部委託」とは、機関等の情報処理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。
- 「機関等外通信回線」とは、通信回線のうち、機関等内通信回線以外のものをいう。
- 「機関等内通信回線」とは、一つの機関等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、当該機関等の管理下に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。機関等内通信回線には、専用線や VPN 等物理的な回線を機関等が管理していないものも含まれる。
- 「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。
- 「基盤となる情報システム」とは、他の機関等と共通的に使用する情報システム（一つの機関等でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。
- 「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディ

スクドライブ、DVDR 等の外部電磁的記録媒体がある。

- 「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（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関をいう。
- 「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。
- 「クラウドサービス事業者」とは、クラウドサービスを提供する事業者又はクラウドサービスを用いて情報システムを開発・運用する事業者をいう。

【さ】

- 「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等の周辺機器を含む。）をいい、特に断りがない限り、機関等が調達又は開発するものをいう。
- 「CYMAT サイマット」とは、サイバー攻撃等により機関等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。

参考：JIS X 9401:2016（抄）
・ クラウドサービス（cloud service）
定義されたインタフェースを使って呼び出されるクラウドコンピューティング経由で提供される一つ以上の能力。
・ クラウドコンピューティング（cloud computing）
セルフサービスのプロビジョニング（provisioning）及びオンデマンド管理を備える，スケーラブルで伸縮自在な共有できる物理的又は仮想的なリソース共用へのネットワークアクセスを可能にするパラダイム。
注記：リソースの例には，サーバ，OS，ネットワーク，ソフトウェア，アプリケーション及びストレージが含まれる。

- 「CSIRT シーサート」とは、機関等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、当該機関等に設置された体制をいう。Computer Security Incident ResponseTeam の略。
- 「実施手順」とは、対策基準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をいう。

- 「情報」とは、統一基準の「1.1(2) 本統一基準の適用対象」の(b)に定めるものをいう。

参考：統一基準の「1.1(2) 本統一基準の適用対象」（抄）
(b) 本統一基準において適用対象とする情報は、以下の情報とする。
(ア) 職員等が職務上使用することを目的として機関等が調達し、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（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）
(イ) その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、職員等が職務上取り扱う情報
(ウ) (ア)及び(イ)のほか、機関等が調達し、又は開発した情報システムの設計又は運用管理に関する情報

- 「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、機関等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を含む。）をいう。

参考：統一基準の「1.1(2) 本統一基準の適用対象」（抄）
(c) 本統一基準において適用対象とする情報システムは、本統一基準の適用対象となる情報を取り扱う全ての情報システムとする。

- 「情報セキュリティインシデント」とは、JIS Q 27000:2014 における情報セキュリティインシデントをいう。

参考：JIS Q 27000:2014（抄）
・ 情報セキュリティインシデント
望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。
・ 情報セキュリティ事象
情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

- 「情報セキュリティ関係規程」とは、対策基準及び実施手順を総称したものをいう。
- 「情報セキュリティ対策推進体制」とは、機関等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、当該機関等に設置された体制をいう。
- 「情報の抹消」とは、電磁的記録媒体に記録された全ての情報を利用不能かつ復元が

困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。

- 「職員等」とは、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、機関等の管理対象である情報及び情報システムを取り扱う者をいう。職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。

【た】

- 「対策基準」とは、機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。
- 「端末」とは、情報システムの構成要素である機器のうち、職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、機関等が調達又は開発するものをいう。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、機関等が調達又は開発するもの以外を指す「機関等支給以外の端末」がある。また、機関等が調達又は開発した端末と機関等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。
- 「通信回線」とは、複数の情報システム又は機器等（機関等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、機関等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、機関等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。
- 「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。
- 「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、通信回線に接続されている又は内蔵電磁的記録媒体を備えているものをいう。

【は】

- 「不正プログラム」とは、コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

【ま】

- 「抹消」→「情報の抹消」を参照。
- 「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。
- 「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

- 「約款による外部サービス」とは、民間事業者等の外部の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする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除く。
- 「要管理対策区域」とは、機関等の管理下にある区域（機関等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。

[3] 一般用語の解説

留意すべき一般用語を以下に解説する。

【あ】

「アクセス制御」とは、情報又は情報システムへのアクセスを許可する主体を制限することをいう。

- 「アプリケーション」とは、OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。
- 「アルゴリズム」とは、ある特定の目的を達成するための演算手順をいう。
- 「暗号化」とは、第三者が復元することができないよう、定められた演算を施しデータを変換することをいう。
- 「暗号モジュール」とは、暗号化及び電子署名の付与に使用するアルゴリズムを実装したソフトウェアの集合体又はハードウェアをいう。
- 「ウェブクライアント」とは、ウェブページを閲覧するためのアプリケーション（いわゆるブラウザ）及び付加的な機能を追加するためのアプリケーションをいう。

【か】

- 「可用性」とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。
- 「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。
- 「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスでき

る特性をいう。

- 「業務継続計画」とは、機関等において策定される、発災時に非常時優先業務を実施するための計画をいう。広義には、平常時からの取組等や復旧に関する計画も含まれる。
- 「共用識別コード」とは、複数の主体が共用するために付与された識別コードをいう。原則として、一つの識別コードは一つの主体のみに対して付与されるものであるが、情報システム上の制約や利用状況等に応じて、識別コードを組織で共用する場合もある。このように共用される識別コードを共用識別コードという。
- 「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

【さ】

- 「サービス不能攻撃」とは、悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。
- 「最小限の特権機能」とは、管理者権限を実行できる範囲を必要最小限に制限する機能をいう。
- 「識別」とは、情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。
- 「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。
- 「主体」とは、情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。
- 「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。
- 「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。
- 「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、IC カード等がある。
- 「セキュリティパッチ」とは、発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルをいう。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。
- 「ソフトウェア」とは、サーバ装置、端末、通信回線装置等を動作させる手順及び命

令を、当該サーバ装置等が理解できる形式で記述したものをいう。OS や OS 上で動作するアプリケーションを含む広義の意味である。

【た】

- 「耐タンパ性」とは、暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。
- 「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。
- 「電子メールクライアント」とは、電子メールサーバにアクセスし、電子メールの送受信を行うアプリケーションをいう。
- 「電子メールサーバ」とは、電子メールの送受信、振り分け、配送等を行うアプリケーション及び当該アプリケーションを動作させるサーバ装置をいう。
- 「ドメインネームシステム（DNS)」とは、クライアント等からの問合せを受けて、ドメイン名やホスト名と IP アドレスとの対応関係について回答を行うシステムである。
- 「ドメイン名」とは、国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.nisc.go.jp というウェブサイトの場合は、nisc.go.jp の部分がこれに該当する。

【な】

- 「名前解決」とは、ドメイン名やホスト名と IP アドレスを変換することをいう。

【は】

- 「複合機」とは、プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。
- 「不正プログラム定義ファイル」とは、不正プログラム対策ソフトウェアが不正プログラムを判別するために利用するデータをいう。
- 「踏み台」とは、悪意ある第三者等によって不正アクセスや迷惑メール配信の中継地点に利用されている情報システムのことをいう。

【ま】

- 「無線 LAN」とは、IEEE802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ad 等の規格により、無線通信で情報を送受信する通信回線をいう。

【ら】

- 「リスク」とは、目的に対する不確かさの影響をいう。ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。
- 「ルートヒントファイル」とは、最初に名前解決を問い合わせる DNS コンテンツサーバ（以下「ルート DNS」という。）の情報をいう。ルートヒントファイルには、ルート DNS のサーバ名と IP アドレスの組が記載されており、ルート DNS の IP アドレスが変更された場合はルートヒントファイルも変更される。ルートヒントファイルは InterNIC（Internet Network Information Center）のサイトから入手可能であ

る。

【A～Z】

- 「CRYPTREC（Cryptography Research and Evaluation Committees）」とは、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。
- 「DNS サーバ」とは、名前解決のサービスを提供するアプリケーション及びそのアプリケーションを動作させるサーバ装置をいう。DNS サーバは、その機能によって、自らが管理するドメイン名等についての名前解決を提供する「コンテンツサーバ」とクライアントからの要求に応じて名前解決を代行する「キャッシュサーバ」の２種類に分けることができる。
- 「IPv6 移行機構」とは、物理的に一つのネットワークにおいて、IPv4 技術を利用する通信と IPv6 を利用する通信の両方を共存させることを可能とする技術の総称である。例えば、サーバ装置及び端末並びに通信回線装置が２つの通信プロトコルを併用するデュアルスタック機構や、相互接続性の無い２つの IPv6 ネットワークを既設の IPv4 ネットワークを使って通信可能とする IPv6-IPv4 トンネル機構等がある。
- 「MAC アドレス（Media Access Control address）」とは、機器等が備える有線 LAN や無線 LAN のネットワークインタフェースに割り当てられる固有の認識番号である。
- 識別番号は、各ハードウェアベンダを示す番号と、ハードウェアベンダが独自に割りてる番号の組合せによって表される。
- 「S/MIME（Secure Multipurpose Internet Mail Extensions）」とは、公開鍵暗号を用いた、電子メールの暗号化と電子署名付与の一方式をいう。
- 「VPN（Virtual Private Network）」とは、暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術をいう。