国立研究開発法人国立環境研究所
情報セキュリティポリシー

平成２９年４月１日

国立研究開発法人国立環境研究所

目次

第１部　総　則

1.1　本ポリシーの目的・適用範囲

(1)　本ポリシーの目的

国立研究開発法人国立環境研究所情報セキュリティポリシー（以下「セキュリティポリシー」という。）は、政府機関の情報セキュリティ対策のための統一基準（サイバーセキュリティ戦略本部決定。以下「統一基準」という。）に準拠して、国立研究開発法人国立環境研究所（以下「研究所」という。）が情報セキュリティの確保のために採るべき対策を講じ、その水準を更に高めるための対策を推進することにより、研究所のサイバーセキュリティ対策を含む情報セキュリティの強化・充実を図ることを目的とする。

(2)　本ポリシーの改定

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。

研究所では、「政府機関の情報セキュリティ対策のための統一基準（2005年12月版（全体版初版））」に基づき当所の情報セキュリティポリシーを策定し、以後随時見直しを行ってきたところである。

政府統一基準は、情報技術の進歩に応じて、定期的に点検し、必要に応じ規定内容の追加・修正等の見直しを行うこととされていることから、本ポリシーもその改定等に応じて必要な見直しを行うこととする。

(3)　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、法令及び規則等（以下「関連法令等」という。）においても規定されているため、情報セキュリティ対策を実施する際には、本ポリシーのほか関連法令等を遵守しなければならない。なお、これらの関連法令等は、情報セキュリティ対策にかかわらず当然に遵守すべきものであるため、本ポリシーにおいては、あえて関連法令等の遵守については明記していない。また、情報セキュリティ対策に係る内容について定めた既存の政府決定等についても同様に遵守する必要がある。

(4)　本ポリシーの適用範囲

(a)　本ポリシーにおいて適用範囲とする者は、全ての業務従事者とする。

(b)　本ポリシーにおいて適用範囲とする情報は、以下の情報とする。

（ア）業務従事者が職務上使用することを目的として研究所が調達し、又は開発した情報システム若しく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、業務従事者が職務上取り扱う情報

（ウ）（ア）及び（イ）のほか、研究所が調達し、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)　本ポリシーにおいて適用範囲とする情報システムは、本ポリシーの適用範囲となる情報を取り扱う全ての情報システムとする。

(5)　対策項目の記載事項

本ポリシーでは、研究所が行うべき対策について、目的別に部、節及び項の３階層にて対策項目を分類し、各項に対して目的、趣旨及び遵守事項を示している。遵守事項は、研究所情報セキュリティポリシーにおいて必ず実施すべき対策事項である。内閣官房内閣サイバーセキュリティセンターが別途整備する府省庁対策基準策定のためのガイドライン及び政府機関統一基準適用個別マニュアル群において規定する統一基準の遵守事項に対応した個別具体的な対策実施要件、対策の実施例や解説等も参照し、研究所情報セキュリティポリシーを策定する必要がある。

1.2　情報の格付けの区分・取扱制限

(1)　格付けの区分

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

(a)　機密性についての格付けの定義

格付けの区分	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	独法情報公開法第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３情報及び機密性２情報を「要機密情報」という。

(b)　完全性についての格付けの定義

格付けの区分	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。

(c)　可用性についての格付けの定義

格付けの区分	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) 情報の取扱制限

情報について、機密性、完全性、可用性の３つの観点から区別し、それぞれにつき取扱制限の種類について基本的な定義を定める。「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、配付禁止、暗号化必須、読後廃棄その他の情報の適正な取扱いを業務従事者に確実にするための手段をいう。

業務従事者は、格付け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、格付け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。

1.3 用語定義

【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、外部委託により研究所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、研究所の情報処理業務の一部又は全部について、契約をもって研究所外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、他の機関と共通的に使用する情報システム（一つの機関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。
- 「業務従事者」とは、研究所において業務に従事している職員その他の研究所の指揮命令に服している者であって、研究所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。業務従事者には、個々の勤務条件にもよるが、例えば、派遣労働者等も含まれている。
- 「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。なお、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、DVD-R等の外部電磁的記録媒体がある。

- 「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。
- 「研究所外通信回線」とは、通信回線のうち、研究所内通信回線以外のものをいう。
- 「研究所内通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び研究所管理又は他組織管理）及び通信回線装置を問わず、研究所が管理する電子計算機を接続し、当該電子計算機間の通信に利用する論理的な通信回線をいう。

【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、研究所が調達又は開発するものをいう。
- 「CSIRT」（シーサート）とは、研究所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、研究所に設置された体制をいう。Computer Security Incident Response Teamの略。
- 「実施手順」とは、研究所情報セキュリティポリシー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、「1.1(4) 本ポリシーの適用範囲」の(b)に定めるものをいう。
- 「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、研究所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。
- 「情報セキュリティインシデント」とは、JIS Q 27001:2014における情報セキュリティインシデントをいう。

- 「情報セキュリティ関係規程」とは、本ポリシー及び実施手順を総称したものをいう。
- 「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。

【た】

- 「端末」とは、情報システムの構成要素である機器のうち、業務従事者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、研究所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。
- 「通信回線」とは、複数の情報システム又は機器等（研究所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、研究所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、研究所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、情報を取り扱うすべての者が当該情報の格付け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、情報ごとに格付けを記載することによる明示のほか、当該情報の格付け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、その格付け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すべ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、民間事業者等の研究所外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、研究所が管理する庁舎等（外部の組織から借用している施設等を含む。）研究所の管理下にある区域であって、取り扱う情報を保護するために、施設及び環境に係る対策が必要な区域をいう。

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

目的・趣旨

情報セキュリティ対策は、それに係る全ての業務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。特に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着実に進めるために、自らが組織内を統括し、組織全体として計画的に対策が実施されるよう推進しなければならない。

なお、最高情報セキュリティ責任者は、本ポリシーに定められた自らの担務を、本ポリシーに定める各責任者に担わせることができる。

遵守事項

(1)　最高情報セキュリティ責任者の設置

(a) 研究所における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。

(2)　情報セキュリティ委員会の設置

(a) 最高情報セキュリティ責任者は、研究所情報セキュリティポリシー等の審議を行う機能を持つ組織として、研究所の情報セキュリティを推進する部局及びその他業務を実施する部局の代表者を構成員とする情報セキュリティ委員会を置くこと。

(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、その指示に基づき実施する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。

(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。そのうち、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。

(b) 情報セキュリティ責任者は、遵守事項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

人を置くこと。

(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。

(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こと。

(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こと。

(6) 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、CSIRTを整備し、その役割を明確化すること。

(b) 最高情報セキュリティ責任者は、業務従事者のうちからCSIRTに属する職員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こと。そのうち、研究所における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責任者を置くこと。またCSIRT内の業務統括及び外部との連携等を行う職員を定めること。

(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こと。

(7) 兼務を禁止する役割

(a) 業務従事者は、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。

(ア) 承認又は許可（以下本項において「承認等」という。）の申請者と当該承認等を行う者（以下本項において「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) 業務従事者は、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。

2.1.2 研究所情報セキュリティポリシー・対策推進計画の策定

目的・趣旨

研究所の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に

低減させるためには、研究所として遵守すべき対策の基準を定めるとともに、情報セキュリティに係るリスク評価の結果を踏まえ、計画的に対策を実施することが重要である。

遵守事項

(1) 研究所情報セキュリティポリシーの策定

(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研究所情報セキュリティポリシーを定めること。

(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。）を定めること。また、対策推進計画には、研究所の業務、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こと。

（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）前各号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

目的・趣旨

研究所情報セキュリティポリシーに定められた対策を実施するため、具体的な実施手順を定める必要がある。

実施手順が整備されていない、又はそれらの内容に漏れがあると、対策が実施されないおそれがあることから、最高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に実施手順の整備を指示し、その結果について定期的に報告を受け、状況を適確に把握することが重要である。

遵守事項

(1) 情報セキュリティ対策に関する実施手順の整備・運用

(a) 統括情報セキュリティ責任者は、研究所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（本ポリシーで整備すべき者を別に定める場合を除く。）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こと。

(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こと。

(c) 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、業務従事者より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こと。

(2) 違反への対処

(a) 業務従事者は、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、各規定の実施に責任を持つ情報セキュリティ責任者にその旨を報告すること。

(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こと。

2.2.2 例外措置

目的・趣旨

例外措置はあくまで例外であって、濫用があってはならない。しかしながら、情報セキュリティ関係規程の適用が業務の適正な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、例外措置の手続を定めておく必要がある。

遵守事項

(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、審査手続を定めること。

(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こと。

(2) 例外措置の運用

(a) 業務従事者は、定められた審査手続きに従い、許可権限者に規定の例外措置の適用を申請すること。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こと。

(b) 許可権限者は、業務従事者による例外措置の適用の申請を、定められた審査手

続きに従って審査し、許可の可否を決定すること。

(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こと。

(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こと。

2.2.3　教育

目的・趣旨

情報セキュリティ関係規程が適切に整備されているとしても、その内容が業務従事者に認知されていなければ、当該規定が遵守されないことになり、情報セキュリティ水準の向上を望むことはできない。このため、全ての業務従事者が、情報セキュリティ関係規程への理解を深められるよう、適切に教育を実施することが必要である。

また、政府機関等における近年の情報インシデントの増加等に鑑み、情報セキュリティの専門性を有する人材を育成することも求められる。

遵守事項

(1)　教育体制等の整備

(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こと。

(2)　教育の実施

(a) 課室情報セキュリティ責任者は、業務従事者に対して、情報セキュリティ関係規程に関する教育を適切に受講させること。

(b) 業務従事者は、教育実施計画に従って、適切な時期に教育を受講すること。

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

(d) 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こと。

2.2.4　情報セキュリティインシデントへの対処

目的・趣旨

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、最高情報セキュリティ責任者に早急にその状況を報告するとともに、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、情報セキュリティインシデントの対処が完了した段階においては、原因について調査するなどにより、情報セキュリティインシデントの経験から今

後に生かすべき教訓を導き出し、再発防止や対処手順、体制等の見直しにつなげることが重要である。

遵守事項

(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研究所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、業務従事者に周知すること。

(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研究所外との情報共有を含む対処手順を整備すること。

(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こと。

(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こと。

(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研究所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研究所外の者に明示すること。

(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こと。

(2) 情報セキュリティインシデントへの対処

(a) 業務従事者は、情報セキュリティインシデントの可能性を認知した場合には、研究所の報告窓口に報告し、指示に従うこと。

(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こと。

(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こと。

(d) CSIRTは、認知した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こと。

(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、研究所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、適切に対処すること。

(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、適切に対処すること。

(g) CSIRTは、研究所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、当該事象について環境省を通じて速やかに、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こと。また、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・連絡等を行うこと。さらに、国民の生活、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等においては、「大規模サイバー攻撃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裁）」に基づく報告連絡も行うこと。

(h) 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こと。

(i) 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こと。

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

(k) 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こと。

(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こと。

(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こと。

(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こと。

2.3 点　検

2.3.1 情報セキュリティ対策の自己点検

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ関係規程の遵守状況等を点検し、その結果を把握・分析することが必要である。

自己点検は、業務従事者が自らの役割に応じて実施すべき対策事項を実際に実施しているか否かを確認するだけではなく、組織全体の情報セキュリティ水準を確認する目的もあることから、適切に実施することが重要である。

また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

遵守事項

(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こと。

(b) 情報セキュリティ責任者は、業務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。

(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、業務従事者に自己点検の実施を指示すること。

(b) 業務従事者は、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こと。

(3) 自己点検結果の評価・改善

(a) 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は、業務従事者による自己点検結果を分析し、評価すること。統括情報セキュリティ責任者は評価結果を最高情報セキュリティ責任者に報告すること。

(b) 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こと。

2.3.2 情報セキュリティ監査

目的・趣旨

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要である。

また、監査の結果で明らかになった課題を踏まえ、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に指示し、必要な対策を講じさせることが重要である。

遵守事項

(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こと。

(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の指示を、最高情報セキュリティ責任者から受けた場合には、追加の監査実施計画を定めること。

(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こと。

（ア）研究所情報セキュリティ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こと

（イ）実施手順が研究所情報セキュリティポリシーに準拠していること

（ウ）自己点検の適正性の確認を行うなどにより、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こと

(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情報セキュリティ責任者に指示すること。

(b) 情報セキュリティ責任者は、監査報告書等に基づいて最高情報セキュリティ責任者から改善を指示されたことについて､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こと。

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており､こうした変化に的確に対応しないと、情報セキュリティ水準を維持できなくなる。このため、研究所の情報セキュリティ対策の根幹をなす情報セキュリティ関係規程は、実際の運用において生じた課題、自己点検・監査等の結果や情報セキュリティに係る重大な変化等を踏まえ、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顕在時の損失等を分析し、リスクを評価し、適時見直しを行う必要がある。

また､情報セキュリティに係る取組をより一層推進するためには､上記のリスク評価

の結果を対策推進計画に反映することも重要である。

遵守事項

(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、研究所情報セキュリティポリシーについて必要な見直しを行うこと。

(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こと。

(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こと。

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

目的・趣旨

業務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等（以下、本項において「利用等」という。）を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての業務従事者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、業務従事者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付け及び取扱制限の明示等を行うとともに、情報の格付けや取扱制限に応じた対策を講ずる必要がある。

なお、秘密文書の管理に関しては、文書管理ガイドラインの規定を優先的に適用した上で、当該ガイドラインに定めが無い情報セキュリティ対策に係る事項については、本統一基準の規定に基づき、適切に情報が取り扱われるよう留意すること。

遵守事項

(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、業務従事者へ周知すること。

（ア）情報の格付け及び取扱制限についての定義

（イ）情報の格付け及び取扱制限の明示等についての手続

（ウ）情報の格付け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)　業務従事者は、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、情報を利用等すること。

(3)　情報の格付け及び取扱制限の決定・明示等

(a)　業務従事者は、情報の作成時及び研究所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、格付け及び取扱制限の定義に基づき格付け及び取扱制限を決定し、明示等すること。

(b)　業務従事者は、情報を機密性３情報と決定した場合には、機密性３情報として取り扱う期間を明示等すること。

(c)　業務従事者は、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け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

性に係る格付け及び取扱制限を継承すること。

(d) 業務従事者は、修正、追加、削除その他の理由により、情報の格付け及び取扱制限を見直す必要があると考える場合には、情報の格付け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（以下この項において「決定者等」という。）に確認し、その結果に基づき見直すこと。

(4) 情報の利用・保存

(a) 業務従事者は、利用する情報に明示等された格付け及び取扱制限に従い、当該情報を適切に取り扱うこと。

(b) 業務従事者は、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こと。

(c) 業務従事者は、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こと。

(d) 業務従事者は、保存する情報にアクセス制限を設定するなど、情報の格付け及び取扱制限に従って情報を適切に管理すること。

(e) 業務従事者は、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こと。

(5) 情報の提供・公表

(a) 業務従事者は、情報を公表する場合には、当該情報が機密性１情報に格付けされるものであることを確認すること。

(b) 業務従事者は、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、当該格付け及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付け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こと。

(c) 業務従事者は、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こと。

(d) 業務従事者は、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こと。

(6) 情報の運搬・送信

(a) 業務従事者は、機密性３情報、要保全情報又は要安定情報を、要管理対策区域外に持ち出し他の場所に運搬する場合又は研究所外通信回線を使用して送信する場合には、課室情報セキュリティ責任者の許可を得ること。

(b) 業務従事者は、要機密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、情報の格付け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こと。ただし、環境省その他の府省庁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。

(c) 業務従事者は、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、情報の格付け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こと。

(7) 情報の消去

(a) 業務従事者は、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こと。

(b) 業務従事者は、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、すべての情報を復元できないように抹消すること。

(c) 業務従事者は、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こと。

(8) 情報のバックアップ

(a) 業務従事者は、情報の格付けに応じて、適切な方法で情報のバックアップを実施すること。

(b) 業務従事者は、取得した情報のバックアップについて、格付け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、適切に管理すること。

(c) 業務従事者は、保存期間を過ぎた情報のバックアップについては、本項(7)の規定に従い、適切な方法で消去、抹消又は廃棄すること。

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

目的・趣旨

サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合においては、悪意を持った者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他、設置環境に関する脅威として、災害の発生による情報システムの損傷等もある。

したがって、執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し、当該区域で取り扱う情報や情報システムのセキュリティを確保する必要がある。

遵守事項

(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こと。

(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こと。

（ア）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。

（イ）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。

(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、施設及び環境に係る対策を行う単位ごとの区域を定めること。

(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こと。

(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こと。業務従事者が実施すべき対策については、業務従事者が認識できる措置を講ずること。

(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こと。

(c) 業務従事者は、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こと。また、業務従事者が研究所外の者を立ち入らせる際には、研究所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こと。

第 4 部　外部委託

4.1　外部委託

4.1.1　外部委託

目的・趣旨

研究所外の者に、情報システムの開発、アプリケーションプログラムの開発等を委託する際に、業務従事者が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において研究所情報セキュリティポリシーに適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

外部委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、約款への同意等様々であるが、いずれの場合においても外部委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

なお、クラウドサービスの利用に係る外部委託については、クラウドサービス特有のリスクがあることを理解した上で、4.1.4項「クラウドサービスの利用」についても本項に加えて遵守する必要がある。

また、民間事業者が不特定多数向けに約款に基づきインターネット上で無料で提供する情報処理サービス等、1.3節において「約款による外部サービス」として定義するものを利用し、業務を遂行する場合も外部委託の一つの形態であるが、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、その際は本項に代えて4.1.2項「約款による外部サービスの利用」を適用すること。

＜外部委託の例＞

- 情報システムの開発及び構築業務
- アプリケーション・コンテンツの開発業務
- 情報システムの運用業務
- 業務運用支援業務（統計、集計、データ入力、媒体変換等）
- プロジェクト管理支援業務等
- 調査・研究業務（調査、研究、検査等）
- 情報システム、データセンター、通信回線等の賃貸借

遵守事項

(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こと。

(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

（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、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こと。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こと。

（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、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる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

(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、委託する業務において取り扱う情報の格付け等を勘案し、必要に応じて以下の内容を仕様に含めること。

（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

(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、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(a)(b)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研究所に提供し、研究所の承認を受けるよう、仕様内容に含めること。

(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こと。

(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業務従事者より受けた場合は、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

せること。

(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こと。

(4) 外部委託における情報の取扱い

(a) 業務従事者は、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こと。

（ア）委託先に要保護情報を提供する場合、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こと。

（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こと。

（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こと。

4.1.2 約款による外部サービスの利用

目的・趣旨

外部委託により業務を遂行する場合は、原則として4.1.1項「外部委託」にて規定する事項について、委託先と特約を締結するなどし、情報セキュリティ対策を適切に講ずる必要がある。しかしながら、要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合には、民間事業者が不特定多数の利用者向けに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等、1.3節において「約款による外部サービス」として定義するものを利用することも考えられる。

このような「約款による外部サービス」をやむを得ず利用する場合には、種々の情報を研究所からサービス提供事業者等に送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断し、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

(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こと。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こと。

（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

(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こと。

(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) 業務従事者は、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こと。

4.1.3 ソーシャルメディアサービスによる情報発信

目的・趣旨

インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していく様々なソーシャルメディアサービスが普及している。政府機関においても、積極的な広報活動等を目的に、こうしたサービスが利用されるようになっている。しかし、民間事業者等により提供されているソーシャルメディアサービスは、.go.jpで終わるドメイン名（以下「政府ドメイン名」という。）を使用することができないため、真正なアカウントであることを国民等が確認できるようにする必要がある。また、研究所のアカウントを乗っ取られた場合や、利用しているソーシャルメディアサービスが予告なくサービス停止した際に必要な情報を発信できない事態が生ずる場合も想定される。そのため、要安定情報を広く国民等に提供する際には、研究所の自己管理ウェブサイトに当該情報を掲載した上でソーシャルメディアサービスを併用するなど、当該情報を必要とする国民等が一次情報源を確認できるよう、情報発信方法を考慮する必要がある。加えて、虚偽情報により国民等の混乱が生じることのないよう、発信元は、なりすまし対策等について措置を講じておく必要がある。

このようなソーシャルメディアサービスは機能拡張やサービス追加等の技術進展が著しいことから、常に当該サービスの運用事業者等の動向等外部環境の変化に機敏に対応することが求められる。

なお、ソーシャルメディアサービスの利用は、約款による外部サービスの利用に相当することから、4.1.2項の規定と同様に、要機密情報を取り扱わず、委託先における高いレベルの情報管理を要求する必要が無い場合に限るものとし、本項に定める遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。

遵守事項

(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、研究所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こと。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こと。

（ア）研究所のアカウントによる情報発信が実際の研究所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こと。

（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こと。

(b) 情報セキュリティ責任者は、研究所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こと。

(c) 業務従事者は、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、研究所の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

4.1.4 クラウドサービスの利用

目的・趣旨

業務及び情報システムの高度化・効率化等の理由から、研究所において今後クラウドサービスの利用の拡大が見込まれている。クラウドサービスの利用に当たっては、クラウド基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。

クラウドサービスを利用する際、研究所がクラウドサービスの委託先に取扱いを委ねる情報は、当該委託先において適正に取り扱われなければならないが、クラウドサービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、クラウドサービスでは、複数利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。クラウドサービスの委託先を適正に選択するためには、このようなクラウドサービスの特性を理解し、研究所による委託先へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分考慮することが求められる。

遵守事項

(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、研究所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こと。

(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こと。

(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こと。

(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こと。

(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こと。

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

目的・趣旨

研究所が所管する情報システムの情報セキュリティ水準を維持するとともに、情報セキュリティインシデントに適切かつ迅速に対処するためには、研究所が所管する情報システムの情報セキュリティ対策に係る情報を情報システム台帳で一元的に把握するとともに、情報システムの構成要素に関する調達仕様書や設定情報等が速やかに確認できるように、日頃から文書として整備しておき、その所在を把握しておくことが重要である。

遵守事項

(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、すべ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こと。

（ア）　情報システム名

（イ）　管理課室

（ウ）　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

（エ）　システム構成

（オ）　接続する研究所外通信回線の種別

（カ）　取り扱う情報の格付け及び取扱制限に関する事項

（キ）　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こと。

（ク）情報処理サービス名

（ケ）契約事業者

（コ）契約期間

（サ）情報処理サービスの概要

（シ）ドメイン名（インターネット上で提供されるサービス等を利用する場合）

（ス）取り扱う情報の格付け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こと。

(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こと。

（ア）　当該情報システムを構成する電子計算機関連事項

- ○サーバ装置及び端末を管理する業務従事者及び利用者を特定する情報
- ○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
- ○サーバ装置及び端末の仕様書又は設計書

（イ）　当該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事項

- ○通信回線及び通信回線装置を管理する業務従事者を特定する情報
- ○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
- ○通信回線及び通信回線装置の仕様書又は設計書
- ○通信回線の構成
- ○通信回線装置におけるアクセス制御の設定
- ○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
- ○通信回線の利用部門

（ウ）　情報システムの構成要素のセキュリティ維持に関する手順

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

（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

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。

これらの課題に対応するため、研究所情報セキュリティポリシーに基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

(1)　機器等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こと。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、その管理を研究所が確認できることを加えること。

(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こと。

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

目的・趣旨

情報システムのライフサイクル全般を通じて、情報セキュリティを適切に維持するためには、情報システムの企画段階において、適切にセキュリティ要件を定義する必要がある。

セキュリティ要件の曖昧さや過不足は、過剰な情報セキュリティ対策に伴うコスト増加のおそれ、要件解釈のばらつきによる提案内容の差異からの不公平な競争入札、設計・開発工程での手戻り、運用開始後の情報セキュリティインシデントの発生といった不利益が生じる可能性に繋がる。

そのため、情報システムが対象とする業務、業務において取り扱う情報、情報を取り扱う者、情報を処理するために用いる環境・手段等を考慮した上で、当該情報システムにおいて想定される脅威への対策を検討し、必要十分なセキュリティ要件を仕様に適切に組み込むことが重要となる。

加えて、構築する情報システムへの脆弱性の混入を防止するための対策も、構築前の企画段階で考慮することが重要となる。

また、情報システムの構築、運用・保守を外部委託する場合については、4.1節「外部委託」についても併せて遵守する必要がある。

遵守事項

(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、情報システムを統括する責任者に求めること。

(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組織・部門が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求めること。

(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け等に基づき、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、以下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こと。

（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

（イ）情報システム運用時の監視等の運用管理機能要件

（ウ）情報システムに関連する脆弱性についての対策要件

(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こと。

(c) 情報システムセキュリティ責任者は、国民・企業と研究所との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定すること。

(d) 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こと。

(e) 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こと。

(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、適切に実施させること。

（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

（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

(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等して、適切に実施させること。

5.2.2　情報システムの調達・構築

目的・趣旨

情報システムを調達・構築する際には、策定したセキュリティ要件に基づく情報セキュリティ対策を適切に実施するために、選定基準に適合した機器等の調達や、情報システムの開発工程での情報セキュリティ対策の実施が求められる。

また、機器等の納入時又は情報システムの受け入れ時には、整備された検査手続に従い、当該情報システムが運用される際に取り扱う情報を保護するためのセキュリティ機能及びその管理機能が、適切に情報システムに組み込まれていることを検査することが必要となる。

遵守事項

(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こと。

(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こと。

(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こと。

(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こと。

5.2.3　情報システムの運用・保守

目的・趣旨

情報システムの運用段階に移るに当たり、企画又は調達・構築時に決定したセキュリ

ティ要件が適切に運用されるように、人的な運用体制を整備し、機器等のパラメータが正しく設定されていることの定期的な確認、運用・保守に係る作業記録の管理等を実施する必要がある。

情報システムにおける情報セキュリティインシデントは一般的に運用時に発生することが大半であることから、適宜情報システムの情報セキュリティ対策の実効性を確認するために、情報システムの運用状況を監視することも重要である。

また、情報システムの保守作業においても運用作業と同様に情報セキュリティ対策が適切に実施される必要がある。保守作業を個別に委託する場合等においても、研究所情報セキュリティポリシーに基づく情報セキュリティ対策について適切に措置を講ずることが求められる。

遵守事項

(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こと。

(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、運用管理する組織・部門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こと。

(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こと。

5.2.4　情報システムの更改・廃棄

目的・趣旨

情報システムの更改・廃棄において、情報システムに記録されている機密性の高い情報が廃棄又は再利用の過程において外部に漏えいすることを回避する必要がある。

情報システムに機密性の高い情報が記録されている場合や、格付けや取扱制限を完全に把握できていない場合等においては、記録されている情報の完全な抹消等の措置を講ずることが必要となる。

遵守事項

(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、当該情報の格付け及び取扱制

限を考慮した上で、以下の措置を適切に講ずること。

（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

目的・趣旨

情報セキュリティを取り巻く環境は常時変化しており、新たに発生した脅威等に的確に対応しない場合には、情報セキュリティ水準を維持できなくなる。このため、情報システムの情報セキュリティ対策を定期的に見直し、さらに外部環境の急激な変化等が発生した場合は、適時見直しを行うことが必要となる。

遵守事項

(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こと。

5.3　情報システムの運用継続計画

5.3.1　情報システム運用継続計画の整備・整合的運用の確保

目的・趣旨

非常時に情報システムの運用を継続させる場合には、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し、定めることが重要となる。なお、業務継続計画や情報システムの運用継続計画が定める要求事項と、情報セキュリティ関係規程が定める要求事項とで矛盾がないよう、それぞれの間で整合性を確保する必要がある。

遵守事項

(1)　情報システム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、研究所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に当たり、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こと。

(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こと。

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

目的・趣旨

情報又は情報システムへのアクセス可能な主体を制限するためには、主体認証機能の導入が必要である。その際、アクセス権限のある主体へのなりすましや脆弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講ずることが重要となる。

また、研究所の情報システムにおいて、国民向けのサービスを提供する場合は、国民が情報システムへのアクセスの主体となることにも留意して、主体認証情報を適切に保護しなければならない。

遵守事項

(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こと。

(b) 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こと。

(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こと。

(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こと。

6.1.2　アクセス制御機能

目的・趣旨

アクセス制御とは、情報システム及び情報へのアクセスを許可する主体を制限することである。複数の主体が情報システムを利用する場合、当該情報システムにおいて取り扱う情報へのアクセスを業務上必要な主体のみに限定することによって、情報漏えい等のリスクを軽減することができると考えられる。

遵守事項

(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ことができる機能を設けること。

(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こと。

6.1.3　権限の管理

目的・趣旨

重要システムのアクセス制御機能を適切に運用するためには、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ことが必要である。権限の管理が不適切になると、情報又は情報システムへ不正アクセスされるおそれが生じる。

また、情報システムの管理機能として、一般的に管理者権限にはあらゆる操作が許可される特権が付与されている。当該特権が悪意ある第三者等に入手された場合、主体認証情報等の漏えい、改ざん又は情報システムに係る設定情報等が不正に変更されることによる情報セキュリティ機能の無効化等が懸念されることから、限られた主体のみに管理者権限が付与されることが重要である。

遵守事項

(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、措置を講ずること。

(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こと。

6.1.4　ログの取得・管理

目的・趣旨

情報システムにおけるログとは、システムの動作履歴、利用者のアクセス履歴、通信履歴その他運用管理等に必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の情報セキュリティインシデント及びその予兆を検知するための重要な材料となるものである。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、ま

た、改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。

遵守事項

(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こと。

(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こと。

(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こと。

6.1.5　暗号・電子署名

目的・趣旨

情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装することが求められる。

暗号化機能及び電子署名機能を導入する際は、使用する暗号アルゴリズムに加え、それを用いた暗号プロトコルが適切であること、運用時に当該アルゴリズムが危殆化した場合や当該プロトコルに脆弱性が確認された場合等の対処方法及び関連する鍵情報の適切な管理等を併せて考慮することが必要となる。

遵守事項

(1)　暗号化機能及び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こと。

（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、当該機能を設けること。

（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、当該機能を設けること。

(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こと。

（ア）業務従事者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、それを使用させること。

（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こと。

（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こと。

（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、管理手順を定めること。

(c) 情報システムセキュリティ責任者は、研究所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こと。

(2)　暗号化及び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こと。

（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こと。

（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、業務従事者と共有を図ること。

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

目的・趣旨

公的機関の情報システムに対する脅威としては、第三者が情報システムに侵入し研究所の重要な情報を窃取・破壊する、第三者が過剰な負荷をかけ情報システムを停止させ

るなどの攻撃を受けることが想定される。特に、国民向けに提供するサービスが第三者に侵入され、個人情報等の重要な情報の漏えい等が発生した場合、研究所に対する社会的な信用が失われる。

一般的に、このような攻撃では、情報システムを構成するサーバ装置、端末及び通信回線装置のソフトウェアの脆弱性を悪用されることが想定される。したがって、公的機関の情報システムにおいては、ソフトウェアに関する脆弱性について、迅速かつ適切に対処することが求められる。

なお、情報システムを構成するハードウェアに関しても、同様に脆弱性が存在する場合があるので、5.2.2項「情報システムの調達・構築」の規定も参照し、必要な対策を講ずる必要がある。

遵守事項

(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こと。

(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採り得る対策がある場合は、当該対策を実施すること。

(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、措置を講ずること。

(d) 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及び独自に開発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し、脆弱性対策が講じられていない状態が確認された場合は対処すること。

6.2.2　不正プログラム対策

目的・趣旨

情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは、他の情報システムに感染を拡大させる、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を及ぼす

おそれがある。このような事態を未然に防止するため、不正プログラムへの対策を適切に実施することが必要である。

遵守事項

(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こと。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。

(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すべてにおいて、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こと。

(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、必要な対処を行うこと。

6.2.3　サービス不能攻撃対策

目的・趣旨

インターネットからアクセスを受ける情報システムに対する脅威としては、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることが想定される。このため、政府機関の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。

遵守事項

(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。以下この項において同じ。）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こと。

(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に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こと。

(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、監視すること。

6.2.4　標的型攻撃対策

目的・趣旨

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である

したがって、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）、並びに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）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

遵守事項

(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）を講ずること。

(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）を講ずること。

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

目的・趣旨

研究所では、情報の提供、業務手続、意見募集等のサービスのためにアプリケーション・コンテンツを用意し、広く利用に供している。利用者がこれらのアプリケーション・コンテンツを利用する際に、利用者端末の情報セキュリティ水準の低下を招いてしまうことは避けなければならない。研究所は、アプリケーション・コンテンツの提供に際しても、情報セキュリティ対策を講じておく必要がある。

また、アプリケーション・コンテンツの開発・提供を外部委託する場合については、4.1.1項「外部委託」についても併せて遵守する必要がある。

遵守事項

(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研究所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

こと。

(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、研究所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こと。

（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こと。

（イ）提供するアプリケーションが脆弱性を含まないこと。

（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限り、実行プログラムの形式でコンテンツを提供しないこと。

（エ）電子証明書を利用する等、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がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

（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こと。

（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こと。

(b) 業務従事者は、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、前号に掲げる内容を調達仕様に含めること。

6.3.2　アプリケーション・コンテンツ提供時の対策

目的・趣旨

研究所では、情報の提供、業務手続及び意見募集等のサービスのためにウェブサイト等を用意し、国民等の利用に供している。これらのサービスは通常インターネットを介して利用するものであるため、国民等にとっては、そのサービスが実際の研究所のものであると確認できることが重要である。また、公的機関になりすましたウェブサイトを放置しておくと、公的機関の信用を損なうだけでなく、国民等が不正サイトに誘導され、不正プログラムに感染するおそれがあるため、このような事態への対策を講ずる必要がある。

遵守事項

(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、研究所外向けに提供するウェブサイト等が実際の研究所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よう仕様に含めること。ただし、4.1.3項に掲げる場合を除く。

(b) 業務従事者は、研究所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、前号と同様、政府ドメイン名を使用するよう調達仕様に含めること。

(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研究所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こと。

(3)　アプリケーション・コンテンツの告知

(a) 業務従事者は、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こと。

(b) 事務従事者は、研究所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等の有効性を保つこと。

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

目的・趣旨

端末の利用に当たっては、不正プログラム感染や不正侵入を受けるなどの外的要因により、保存されている情報の漏えい等のおそれがある。また、業務従事者の不適切な利用や過失等の内的要因による不正プログラム感染等の情報セキュリティインシデントが発生するおそれもある。モバイル端末の利用に当たっては、盗難や紛失等による情報漏えいの可能性も高くなる。これらのことを考慮して、対策を講ずる必要がある。

なお、本項の遵守事項のほか、6.1節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1項「ソフトウェアに関する脆弱性対策」、6.2.2項「不正プログラム対策」、7.3.2項「IPv6通信回線」において定める遵守事項のうち端末に関係するものについても併せて遵守する必要がある。

遵守事項

(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こと。

(b) 情報システムセキュリティ責任者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。

(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、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こと。

(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こと。

(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すべ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、改善を図ること。

(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すべての情報を抹消すること。

7.1.2　サーバ装置

目的・趣旨

電子メールサーバやウェブサーバ、ファイルサーバ等の各種サーバ装置には、大量の情報が保存されている場合が多く、当該情報の漏えいや改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入を受けるなどの可能性が高い。仮に政府機関が有するサーバ装置が不正アクセスや迷惑メールの送信の中継地点に利用されるようなことになれば、国民からの信頼を大きく損なう。加えて、サーバ装置は、同時に多くの者が利用するため、その機能が停止した場合に与える影響が大きい。これらのことを考慮して、対策を講ずる必要がある。

なお、本項の遵守事項のほか、6.1節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理等の機能面での対策、6.2.1項「ソフトウェアに関する脆弱性対策」、6.2.2項「不正プログラム対策」、6.2.3項「サービス不能攻撃対策」、7.3.2項「IPv6通信回線」において定める遵守事項のうちサーバ装置に関係するものについても遵守する必要がある。

また、特に電子メールサーバ、ウェブサーバ、DNSサーバ及びデータベースについては、本項での共通的な対策に加え、それぞれ7.2節「電子メール・ウェブ等」において定める遵守事項についても併せて遵守する必要がある。

遵守事項

(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こと。

(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こと。

(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こと。

(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こと。

(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こと。

(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こと。

(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こと。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。

(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こと。

(3)　サーバ装置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、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こと。

7.1.3　複合機・特定用途機器

目的・趣旨

研究所においては、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複合機が利用されている。複合機は、研究所内通信回線や公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、研究所においては、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等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては、汎用的な機器のほか、システム特有の特定用途機器が利用されることがあり、特定用途機器についても、当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。

したがって、複合機や特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして対策を講ずることが重要である。

遵守事項

(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け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こと。

(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こと。

(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こと。

(2)　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こと。

7.2　電子メール・ウェブ等

7.2.1　電子メール

目的・趣旨

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいするなどの機密性に対するリスクの他、悪意ある第三者等によるなりすまし等、電子メールが悪用される不正な行為の被害に電子メールを利用する業務従事者が巻き込まれるリスクもある。これらの問題を回避するためには、適切な電子メールサーバの管理が必要である。

なお、本項の遵守事項のほか、7.1.2項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(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こと。

(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こと。

(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こと。

7.2.2 ウェブ

目的・趣旨

インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ（ウェブページとして公開している情報）の改ざん、ウェブサーバの利用停止、偽サイトへの誘導等の被害が想定されるため、適切な対策を組み合わせて実施することが求められる。

なお、本項の遵守事項のほか、7.1.2項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(1) ウェブサーバの導入時の対策

(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こと。

（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こと。

（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こと。

（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こと。

（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こと。

（オ） サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること。

(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こと。

(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こと。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こと。

7.2.3 ドメインネームシステム（DNS）

目的・趣旨

ドメインネームシステム（DNS：Domain Name System）は、インターネットを使った階層的な分散型システムで、主としてインターネット上のホスト名や電子メールで使わ

れるドメイン名と、IPアドレスとの対応づけ（正引き、逆引き）を管理するために使用されている。DNSでは、端末等のクライアント（DNSクライアント）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等について回答を行う。DNSには、ドメインに関する問合せについて回答を行うコンテンツサーバと、DNSクライアントからの要求に応じてコンテンツサーバに対して問合せを行うキャッシュサーバが存在する。キャッシュサーバの可用性が損なわれた場合は、ホスト名やドメイン名を使ったウェブや電子メール等の利用が不可能となる。また、コンテンツサーバが提供する情報の完全性が損なわれ、誤った情報を提供した場合は、端末等のDNSクライアントが悪意あるサーバに接続させられるなどの被害にあう可能性がある。さらに、DNSが管理するドメインをアドレスとして利用する電子メールのなりすまし対策の一部はDNSで行うため、これに不備があった場合には、なりすまされた電子メールの検知が不可能となる。これらの問題を回避するためには、DNSサーバの適切な管理が必要である。

なお、本項の遵守事項のほか、7.1.2項「サーバ装置」において定めるサーバ装置に係る遵守事項についても併せて遵守する必要がある。

遵守事項

(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こと。

(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こと。

(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、研究所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こと。

(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こと。

(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こと。

(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こと。

7.2.4 データベース

目的・趣旨

本項における「データベース」とは、データベース管理システムとそれによりアクセスされるデータファイルから構成され、体系的に構成されたデータを管理し、容易に検索・抽出等が可能な機能を持つものであって、要保護情報を保管するサーバ装置とする。

要保護情報を保管するデータベースでは、不正プログラム感染や不正アクセス等の外的要因によるリスク及び業務従事者の不適切な利用や過失等の内的要因によるリスクに対して、管理者権限の悪用を防止するための技術的対策等を講ずる必要がある。

特に大量のデータを保管するデータベースの場合、そのデータが漏えい等した際の影響が大きく、また、そのようなデータは攻撃者の標的となりやすい。

なお、本項の遵守事項のほか、6.1節「情報システムのセキュリティ機能」において定める主体認証・アクセス制御・権限管理・ログ管理・暗号・電子署名等の機能面での対策、6.2.1項「ソフトウェアに関する脆弱性対策」、6.2.2項「不正プログラム対策」、7.3.2項「IPv6通信回線」において定める遵守事項のうち、データベースに関係するものについても併せて遵守する必要がある。

遵守事項

(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こと。

(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、措置を講ずること。

(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、対策を講ずること。

(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こと。

(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こと。

7.3 通信回線

7.3.1 通信回線

目的・趣旨

サーバ装置や端末への不正アクセスやサービス不能攻撃等は、当該サーバ装置や端末に接続された通信回線及び通信回線装置を介して行われる場合がほとんどであることから、通信回線及び通信回線装置に対する情報セキュリティ対策については、情報システムの構築時からリスクを十分検討し、必要な対策を実施しておく必要がある。通信回

線の運用主体又は物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し、対策を講ずる必要がある。

また、情報システムの運用開始時と一定期間運用された後とでは、通信回線の構成や接続される情報システムの条件等が異なる場合があり、攻撃手法の変化も想定されることから、情報システムの構築時に想定した対策では十分でなくなる可能性がある。そのため、通信回線の運用時においても、継続的な対策を実施することが重要である。

遵守事項

(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け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こと。

(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こと。

(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こと。

(d) 情報システムセキュリティ責任者は、業務従事者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こと。

(e) 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こと。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等して、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こと。

(f) 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こと。

(g) 情報システムセキュリティ責任者は、研究所内通信回線にインターネット回線や公衆通信回線等の研究所外通信回線を接続する場合には、研究所内通信回線及び当該研究所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こと。

(h) 情報システムセキュリティ責任者は、研究所内通信回線と研究所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こと。

(i) 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こと。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。

(j) 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こと。

(k) 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こと。

(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こと。

(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こと。

(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等、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。

(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こと。

(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、当該の通信回線装置の電磁的記録媒体に記録されているすべての情報を抹消する等適切な措置を講ずること。

(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、業務従事者の業務遂行を目的としたリモートアクセス環境を、研究所外通信回線を経由して研究所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こと。

(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技術を利用して研究所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うえで、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こと。

7.3.2　IPv6 通信回線

目的・趣旨

政府機関において、インターネットの規格であるIPv6通信プロトコルに対応するための取組が進められているが、IPv6通信プロトコルを採用するにあたっては、グローバルIPアドレスによるパケットの直接到達性やIPv4通信プロトコルからIPv6通信プロトコルへの移行過程における共存状態等、考慮すべき事項が多数ある。

近年では、サーバ装置、端末及び通信回線装置等にIPv6技術を利用する通信（以下「IPv6通信」という。）を行う機能が標準で備わっているものが多く出荷され、運用者が意図しないIPv6通信が通信ネットワーク上で動作している可能性があり、結果として、不正アクセスの手口として悪用されるおそれもあることから、必要な対策を講じていく必要がある。

なお、IPv6技術は今後も技術動向の変化が予想されるが、一方で、IPv6技術の普及に伴い情報セキュリティ対策技術の進展も期待されることから、研究所においても、IPv6の情報セキュリティ対策に関する技術動向を十分に注視し、適切に対応していくことが重要である。

遵守事項

(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、IPv6ReadyLogoProgramに基づくPhase-2 準拠製品を選択すること。

(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こと。

（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こと。

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

目的・趣旨

業務従事者は、業務の遂行のため、端末での事務処理のほか電子メール、ウェブ等様々な情報システムを利用している。これらを適切に利用しない場合、情報セキュリティインシデントを引き起こすおそれがある。

このため、情報システムの利用に関する規定を整備し、業務従事者は規定に従って利用することが求められる。

遵守事項

(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、研究所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こと。

(b) 統括情報セキュリティ責任者は、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を想定し、要管理対策区域外に持ち出した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安全管理措置に関する規定及び許可手続を定めること。

(c) 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こと。

(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、業務従事者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こと。

(3)　情報システムの利用時の基本的対策

(a) 業務従事者は、業務の遂行以外の目的で情報システムを利用しないこと。

(b) 業務従事者は、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研究所の情報システムを接続しないこと。

(c) 業務従事者は、研究所内通信回線に、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こと。

(d) 業務従事者は、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こと。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こと。

(e) 業務従事者は、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こと。
(f) 業務従事者は、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こと。
(g) 業務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。
(h) 業務従事者は、機密性３情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、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の許可を得ること。

(4) 電子メール・ウェブの利用時の対策
(a) 業務従事者は、業務で使用するすべての電子メールを送受信する場合には、研究所が運営し、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こと。
(b) 業務従事者は、業務で電子メールにより情報を送信する場合は、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こと。
(c) 業務従事者は、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、対処すること。
(d) 業務従事者は、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こと。
(e) 業務従事者は、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こと。
(f) 業務従事者は、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こと。
（ア）送信内容が暗号化されること
（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こと

(5) 識別コード・主体認証情報の取扱い
(a) 業務従事者は、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こと。
(b) 業務従事者は、自己に付与された識別コードを適切に管理すること。
(c) 業務従事者は、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こと。
(d) 業務従事者は、自己の主体認証情報の管理を徹底すること。

(6) 暗号・電子署名の利用時の対策

(a) 業務従事者は、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こと。

(b) 業務従事者は、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こと。

(c) 業務従事者は、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こと。

(7) 不正プログラム感染防止

(a) 業務従事者は、不正プログラム感染防止に関する措置に努めること。

(b) 業務従事者は、情報システム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こと。

8.2 研究所支給以外の端末の利用

8.2.1 研究所支給以外の端末の利用

目的・趣旨

業務の遂行においては、研究所から支給された端末を用いて業務を遂行すべきである。しかしながら、出張や外出等の際に、やむを得ず研究所支給以外の端末を利用して情報処理を行う必要が生じる場合がある。この際、当該端末は研究所が支給したものではないという理由で、業務従事者へ情報セキュリティ対策の実施を求めなかった場合、当該端末で取り扱われる情報セキュリティ水準が、研究所情報セキュリティポリシーを満たさないおそれがある。

したがって、そのような可能性がある場合は、研究所支給以外の端末を業務従事者が安全に利用するための手続や安全管理措置の規定をあらかじめ整備し、研究所における厳格な管理の下で利用させることが必要である。

また、研究所支給以外の端末であっても、研究所から支給されるモバイル端末と同等の情報セキュリティ水準の確保が求められることから、7.1.1項「端末」も参照し、同等の安全管理が実施されるよう、規定を整備し、業務従事者に安全管理措置を講じさせる必要がある。

遵守事項

(1) 研究所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、研究所支給以外の端末により業務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。

(b) 統括情報セキュリティ責任者は、要保護情報について研究所支給以外の端末によ

り情報処理を行う場合の安全管理措置に関する規定を整備すること。

(c) 情報セキュリティ責任者は、研究所支給以外の端末による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を定めること。

(d) 前号で定める責任者は、要機密情報を取り扱う研究所支給以外の端末について、端末の盗難、紛失や不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、業務従事者に適切に安全管理措置を講じさせること。

(2) 研究所支給以外の端末の利用時の対策

(a) 業務従事者は、研究所支給以外の端末により業務に係る情報処理を行う場合には、遵守事項8.2.1(1)(c)で定める責任者の許可を得ること。

(b) 業務従事者は、要機密情報を研究所支給以外の端末で取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。

(c) 業務従事者は、研究所支給以外の端末により業務に係る情報処理を行う場合には、研究所にて定められた手続き及び安全管理措置に関する規定に従うこと。

(d) 業務従事者は、情報処理の目的を完了した場合は、要機密情報を研究所支給以外の端末から消去すること。

A.1　備考

A.1.1　実施手順、実施要領等の策定

本ポリシーを実現するための実施手順、実施要領等は別途、統括情報セキュリティ責任者が定める。

B.1　情報セキュリティポリシー別添資料

B.1.1　組織・体制図