公益財団法人九州先端科学技術研究所
情報セキュリティ実施手順

公益財団法人九州先端科学技術研究所

目次

Ⅰ 目的

本情報セキュリティ実施手順（以下「実施手順」という。）は、「公益財団法人九州先端科学技術研究所情報セキュリティ管理規程」（以下「規程」という。）第 12 条の規定に基づき、公益財団法人九州先端科学技術研究所（以下、「本研究所」という。）が所管する情報資産に関する情報セキュリティ対策に関する実施手順を定め、情報資産の漏洩及び不正使用など防止することを目的とする。

Ⅱ 公益財団法人九州先端科学技術研究所情報セキュリティポリシー

規程及び実施手順をもって本研究所の情報セキュリティポリシー（以下「ポリシー」という。）と総称する。

Ⅲ 脅威

実施手順における情報セキュリティに係る脅威とは、以下に掲げるものを想定する。

（1）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的要因による情報資産の盗難、漏えい、破壊、改ざん、消去、重要情報の詐取、内部不正等

（2）情報資産の無断持ち出し、無許可ソフトウェアの利用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の紛失、漏えい、破壊、消去等

（3）地震、落雷、火災等の環境的要因によるサービス、業務の停止等

（4）通信の途絶等の提供サービスの障害からの波及等

Ⅳ 脅威への対応

上記に掲げる脅威に対する規定の概要を示し、具体的な遵守事項等は各項に示す。

（1）組織体制

情報セキュリティ対策の推進のための組織体制を定める。（参照：1 組織体制）

（2）情報資産の管理

（3）物理的セキュリティ対策

災害や事故、停電、故障、プログラム上の欠陥等の脅威への対策を行う。（参照：3 物理的セキュリティ）

（4）人的セキュリティ対策

操作ミス等の人的ミス、無断持ち出し、ポリシー違反、内部不正行為等の脅威への対策を行う。（参照：4 人的セキュリティ）

（5）技術的セキュリティ対策

部外者の侵入、不正アクセス、ウイルス攻撃、盗難、漏えい、改ざん、消去、詐取等の脅威への対策を行う。（参照：5 技術的セキュリティ）

（6）運用

情報システムの管理・運用上の不備によって生じる内部統制上の脅威への対策を行う。（参照：6 運用）

（7）評価及び見直し

現在の情報セキュリティ対策の定期的な評価・見直しを行う。（参照：7 評価及び見直し）

1 組織体制

本研究所の情報資産管理の組織体制は、以下のとおりとする。

（1）情報セキュリティ最高管理者

情報セキュリティ最高責任者は、以下の役割を担う。

①本研究所の情報セキュリティ対策に関する最終決定権限及び責任を有する。

②実施手順の策定、変更および維持管理を行う。

（2）情報セキュリティ統括管理者

情報セキュリティ統括管理者は、以下の役割を担う。

①所管する各部門の情報セキュリティ対策に関する統括的な権限及び責任を有する。

②所管する各部門の職員及び派遣労働者（以下「職員等」という。）に対して、情報セキュリティに関する教育、訓練、助言及び指示を行う。③所管する各部門の職員等が、情報資産の取扱いを適正に行うよう、指導、監督を行う。

（3）ネットワーク管理者

ネットワーク管理者は、以下の役割を担う。

①本研究所のネットワークの敷設、設定の変更、運用及び見直し等（以下「敷設等」という。）並びに当該ネットワークの情報セキュリティ対策に関する権限及び責任を有する。

②本研究所のネットワークの敷設等に携わる職員等並びに当該ネットワークを利用する職員等を指導し、及び監督する。

（4）情報システム管理者

情報システム管理者は、以下の役割を担う。

①本研究所の情報システムの開発、設定の変更、運用及び見直し等（以下「開発等」という。）並びに当該情報システムの情報セキュリティ対策に関する権限及び責任を有する。

②本研究所の情報システムの開発等に携わる職員等及び当該情報システムを利用する職員等を指導し、及び監督する。

（5）情報セキュリティ管理者

情報セキュリティ管理者は、以下の役割を担う。

①本研究所の情報セキュリティ対策に関する権限及び責任を有する。

②本研究所の情報資産の取扱いについて、本研究所の職員等を指導し、及び監督する。

2 情報資産の管理

情報資産を適正に管理するための対策を以下のとおり講じる。

（1）情報の作成

①職員等は、業務上必要のない電子的なデータ及びファイル（以下「情報」という。）を作成してはならない。

②職員等は、作成中の情報についても紛失や流出等を防止する。また、作成途上で不要になった場合は消去する。

（2）情報資産の利用

①職員等は、情報資産を業務以外の目的で利用してはならない。

②職員等は、契約書や合意書等による特段の合意がない限り、職員等以外の者に本研究所の情報資産を取扱わせてはならない。

③職員等は、情報資産の重要度に応じた適正な取扱いを行う。

（3）情報資産の保管

①ネットワーク管理者、情報システム管理者及び情報セキュリティ管理者は、情報資産の重要度に従って適正に保管する。

②情報資産を含む記録媒体及び文書等については、外部からの脅威にさらされないように施錠ができる場所等の特に安全な場所に保管する。情報資産を含む記録媒体をバックアップ等の必要により長期保管する場合は、書込禁止の措置を講じる。

③情報資産が、本研究所内電子ネットワーク上にある場合には，適切な利用以外のアクセスができないよう措置するなど，前項の趣旨に適合する取扱いを行うものとする。

④ネットワーク管理者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上取扱いを許可されていない者による閲覧及び紛失等がないように適正に管理する。

（4）情報資産の入手及び提供

①情報セキュリティ管理者は、外部から情報資産を入手する場合及び外部へ情報資産を提供する場合、情報セキュリティ統括管理者に事前に申請し承認を受けるものとする。なお、入手した情報資産については、入手元の情報資産の重要度に基づいた取扱いを行う。 また、外部へ提供する情報資産については、本研究所における情報資産の重要度に基づいた取扱いを行うことを条件とする。

②外部から入手した情報資産や本研究所における業務で作成した情報資産が機密情報を含む場合は、秘密表示を行うことする。

③受託研究等の業務においては、委託元（企業等）の定める情報セキュリティ関連規程や秘密情報管理規程等を遵守する。また、再委託を行う場合は委託元の事前承諾を受けたのち、再委託先についても情報セキュリティ関連規程や秘密情報管理規程等を遵守させることとする。

④個人情報を含む情報資産の取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人情報の安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行うこととする。

（5）暗号化

①職員等は、インターネットを通じて利用できる電子メール、ネットワークストレージ、アップロード、掲示板等のサービスを利用して、情報の送信、保存及び公開等を行う場合、機密情報や個人情報を含む場合は、不正に入手した者が容易に復元できないよう暗号化又はパスワード設定等による対策を講じる。

（6）情報資産の持ち出し

①職員等は、機密情報や個人情報を含む情報資産を持ち出す場合、持ち出す情報が適切であることを所属長が確認し承認したのち持ち出すこととし、紙媒体等物理的に難しいものを除き、暗号化又はパスワード設定を行う。なお、暗号化については、（5）の定めるところにより行う。

（7）情報資産の返却又は廃棄

①職員は、情報資産を事業者に返却する場合、廃棄する場合、又は事業者に廃棄させる場合、すべての情報を復元できないように措置等を講じた上で行う。措置等の詳細は以下のとおりとする。

ア　機器及び記録媒体等の情報資産を事業者に返却する場合、データ消去用ソフトを使用する。

イ　機器及び記録媒体等の情報資産を廃棄する場合、データ消去用ソフトを使用又は物理的に破壊を行う。

3 物理的セキュリティ

災害や事故等に対して、以下のとおり物理的な対策を講じる。

（1）機器の設置

①ネットワーク管理者及び情報システム管理者は、サーバ等の機器の取付けを行う場合、地震、落雷、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないように適正に固定する等必要な措置を講じる。

②情報システム管理者は、サーバ等の新規設置又は移設を行う場合、当該施設場所が本研究所の管理する施設以外である際は、定期的に当該サーバ等への情報セキュリティ対策状況について確認する。

（2）通信ケーブル等の配線

①ネットワーク管理者及び情報システム管理者は、通信ケーブル及び電源ケーブルの損傷等を防止するために、本研究所入居施設管理者及び本研究所総務部等（以下、「施設管理者等」という。）と連携し、配線収納管を利用する等必要な措置を講じる。

②ネットワーク管理者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合、施設管理者等と連携し、対応する。

（3）機器の保守又は修理

①情報システム管理者は、サーバ等の機器の保守を定期的に実施する。

②情報システム管理者は、記録媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせる。内容を消去できない場合は、事業者に故障を修理させるにあたり、修理を行う事業者との間で守秘義務契約を締結するほか、秘密保持体制の確認などを行う。

（4）機器の廃棄等

情報システム管理者は、機器の廃棄又は返却にあたっては、２（７）を参照する。

（5）管理区域の構造等

①ネットワーク管理者及び情報システム管理者は、ネットワークの基幹機器及び機密情報を含む情報資産を取扱うサーバ等の機器を設置し、当該機器等の管理及び運用を行うための部屋や大量の記録媒体を保管する場所（以下「管理区域」という。）を設ける。

②ネットワーク管理者及び情報システム管理者は、施設管理者等と連携し、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止する。

③ネットワーク管理者及び情報システム管理者は、施設管理者等と連携し、管理区域内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じる。また、管理区域に配置する消火薬剤や消防用設備等が、機器等及び記録媒体に影響を与えないようにする。

（6）管理区域の入退室管理等

①ネットワーク管理者及び情報システム管理者は、管理区域への入退室を許可された者のみに制限し、管理区域専用の鍵による入退室管理を行う。

②職員等及び事業者は、管理区域に入室する場合、職員証等を携帯し、求めにより提示する。

③ネットワーク管理者及び情報システム管理者は、外部からの訪問者が管理区域に入る場合、必要に応じて立入区域を制限した上で、管理区域への入退室を許可された職員等が付き添い、及び外見上職員等と区別できる措置を講じる。
④ネットワーク管理者及び情報システム管理者は、機密情報を含む情報資産を取扱う機器等を設置している管理区域について、当該管理区域内の機器に関連しないコンピュータ、モバイル端末、通信回線装置、記録媒体等を持ち込ませないようにする。

（7）個人情報を取扱う区域の管理

個人情報を取扱う事務を実施する区域（以下「取扱区域」という。）について、事務を取扱う者以外が容易に閲覧できないよう対策を講じる。

（8）機器等の搬入出

①ネットワーク管理者及び情報システム管理者は、搬入する機器等が既存のネットワーク又は情報システムに与える影響について、あらかじめ職員等又は委託した事業者に確認を行わせる。
②ネットワーク管理者及び情報システム管理者は、管理区域の機器等の搬入出について、受託した事業者が作業を行う場合は、職員を立ち会わせる。

（9）通信回線等の管理

①ネットワーク管理者は、施設管理担当者等と連携し、本研究所内の通信回線及び通信回線装置を適正に管理する。
②ネットワーク管理者は、外部へのネットワーク接続を必要最小限とし、可能な限り接続ポイントを減らす。
③ネットワーク管理者及び情報システム管理者は、機密情報を含む情報資産を取扱う情報システムに通信回線を接続する場合、必要な情報セキュリティ水準を検討の上、適正な通信回線を選択する。また、万一情報が漏洩した際の影響が大きいと考えられる場合等、必要な場合は、送受信される情報の暗号化を行う。暗号化については、２（５）の定めるところにより行う。
④ネットワーク管理者は、ネットワークに利用する通信回線について、伝送途上で情報の破壊、盗聴、改ざん、消去等が生じないように十分な情報セキュリティ対策を講じる。
⑤ネットワーク管理者及び情報システム管理者は、通信回線の性能低下や停止により行政事務の運営に著しく支障を来す情報システムについて、接続する通信回線は継続的な運用を可能とする回線を選択する。また、必要に応じて、回線を冗長構成にする等の措置を講じる。

４ 人的セキュリティ

情報資産の無断持ち出しや操作ミス等に対して、以下のとおり人的な対策を講じる。

（1）端末等の管理

①職員等は、業務で使用するパソコン・スマートデバイス（スマートフォン、タブレット端末）等の端末や記録媒体、情報が印刷された文書等について、情報システム管理者の許可なく、第三者に利用されること又は閲覧されることがないように、記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じる。
②職員等は、不正にコピーしたソフトウェアを利用してはならない。
③私有情報機器（パソコン・スマートデバイス等）や取り外し可能な私有記録媒体については、業務で使用は原則として禁止する。使用する場合は、所属長及び情報システム管理者の承認を得て使用することとし、上記、①、②に定める取扱い方法を遵守するとともに、原則として業務情報を保存しないこととする。

（2）パソコン等の端末における設定変更の禁止

職員等は、パソコン等の端末及びソフトウェアのセキュリティ機能の設定に関して、情報システム管理者及び情報セキュリティ統括責任者（各部門の長）の指示に従うこととし、許可なく変更してはならない。

（3）ＩＤ及びパスワード等の管理

① 職員等は、認証に用いるＩＤ及びパスワード等を職員等間で共有してはならない。

② 職員等は、自己のＩＤやパスワードを他人に利用させてはならない。また、他人のＩＤやパスワードを利用して、情報システムへの不正アクセス等を行ってはならない。

③ 職員等は、共有ＩＤを利用する場合は、共有ＩＤの利用者以外に利用させてはならない。

④ 職員等は、以下のとおり自己のパスワードを適正に管理する。

ア　秘密にし、照会等には一切応じてはならない。

イ　メモに残す場合は、第三者に閲覧されることがないように当該メモを適正に管理する。

ウ　十分な長さとし、文字列は想像しにくいものにする。

エ　パスワードが流出したおそれがある場合には、情報セキュリティ管理者及び情報システム管理者に速やかに報告するとともに、速やかにパスワードを変更する。

（4）業務以外の目的でのインターネット利用等の禁止

①職員等は、業務以外の目的で、情報システム、電子メール及びインターネットの利用並びにファイルのダウンロード等を行ってはならない。

②ネットワーク管理者又は情報システム管理者は、職員等のインターネットの利用にあたり、明らかに業務に関係のないウェブサイトを閲覧していることを発見した場合は、当該職員等が属する部門の情報セキュリティ統括責任者（各部門の長）に通知し、適正な措置を求める。

（5）電子メール、FAX の利用

職員等は、電子メール、FAX の利用にあたり、以下のことを遵守する。

①自動転送機能を用いて、外部に電子メールを転送してはならない。

②業務上必要のない送信先に電子メールを送信してはならない。

③複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにする。

④重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告する。

⑤職員等は、インターネット上で利用できるフリーメールを業務で使用してはならない。

⑥不審なメールを受信した場合はメールヘッダ情報（差出人、宛先等）を確認し、怪しいものは破棄する。

⑦メール添付ファイルについては、メールヘッダ情報（差出人、宛先等）やメール内容確認し、不用意にクリックしない。

⑧電子メール及び FAX の送信時は、正しい宛先であること及び適切な添付ファイル（電子メール）であることを確認したのち送信する。

（6）研修及び訓練

①情報セキュリティ最高責任者は、職員等に対し、情報セキュリティに関する研修及び訓練を実施させる。

②情報セキュリティ管理者は、情報セキュリティ最高責任者の指示に従い、職員等に対する情報セキュリティに関する研修計画を立案し、職員等の役割に応じた研修を実施する。

③職員等は、定められた研修に参加する。
④情報セキュリティ管理者は、職員等が常にポリシーを閲覧できるように掲示する。

（7）事故、欠陥等の報告等

①職員等は、情報セキュリティに関する事故、障害及び違反行為による情報資産への侵害（以下「侵害」という。）を発見した場合又は市民等の外部からその報告を受けた場合、速やかに情報セキュリティ管理者に報告する。
②情報セキュリティ管理者は、当該侵害がネットワークに関連する場合は、ネットワーク管理者に報告し、情報システムに関連する場合は、情報システム管理者に速やかに報告する。なお、情報システム及びネットワークに関連しない場合で、侵害が重大である場合は、各部門の情報セキュリティ統括責任者（各部門の長）に報告する。
③ネットワーク管理者又は情報システム管理者は、侵害が重大である場合は、各部門の情報セキュリティ統括責任者（各部門の長）に報告する。
④ネットワーク管理者、情報システム管理者又は情報セキュリティ管理者は、これらの侵害を分析し、記録を保存する。また当該侵害の原因究明の結果から、再発防止策を検討し、必要と判断した場合は、情報セキュリティ最高責任者に報告する。

（8）退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を情報セキュリティ管理者あるいは情報セキュリティ統括責任者（各部門の長）に返却する。また、業務を離れた後も業務上知り得た情報を漏らしてはならない。

5 技術的セキュリティ

不正アクセス、データ改ざん等に対して、以下のとおり技術的な対策を講じる。

（1） ネットワークの接続制御、経路制御等

①ネットワーク管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定する。
②ネットワーク管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施す。
③情報システム管理者は、情報システムの新規構築等により、当該情報システムを新たにネットワークに接続する必要が生じた場合は、ネットワーク管理者の承認を受ける。
④職員等は、パソコン等の端末を無断でネットワークに接続してはならない。ただし、職員は、ネットワーク管理者の許可があれば接続することができる。
⑤ネットワーク管理者は、承認を受けずに又は承認を受けたものとは異なる状態で、情報システムがネットワークに接続されていることを発見した場合又は許可を受けていないパソコン等の端末がネットワークに接続されていることを発見した場合は、当該情報システム等を切断することができる。
⑥情報セキュリティ管理者は、無線ＬＡＮの利用にあたっては、解読が困難な暗号化及び認証技術を利用する。
⑦ネットワーク管理者は、機密情報を含む情報を扱うネットワークについて、万一情報が盗聴等された際の影響が大きいと考えられる場合等、必要に応じて、通信の暗号化等の措置を講じる。暗号化については２（５）の定めるところにより行う。

（2）アクセス制御

①ネットワーク管理者及び情報システム管理者は、所管するネットワーク又は情報システムごとに、アクセスする権限のない職員等がアクセスできないようにシステム上制限する。

②情報システム管理者は、特定の職員等のみに取扱わせる機密情報を含む情報資産について、特定の職員等以外はアクセスできないように制限する。
③情報システム管理者は、端末の電源起動時又は情報システムログイン時にパスワードの入力を必要とするよう設定する。
④情報セキュリティ管理者は、業務上必要のなくなった職員等の利用者登録を削除するようにネットワーク管理者又は情報システム管理者に通知する。
⑤情報セキュリティ管理者は、利用されていないＩＤが放置されないようにネットワーク管理者又は情報システム管理者と連携し、点検する。
⑥ネットワーク管理者又は情報システム管理者は、管理者権限等の特権（以下「特権」という。）を付与されたＩＤを利用する者を必要最小限とし、当該ＩＤのパスワードの漏えい等が発生しないように当該ＩＤ及びパスワードを厳重に管理する。
⑦情報システム管理者は、職員等に対してパスワードを発行する場合は、原則として仮のパスワードを発行することとし、ログイン後直ちに仮のパスワードを変更させる。
⑧情報システム管理者は、特権により情報システムを利用する場合、その利用時間を必要最小限とする。
⑨ネットワーク管理者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（３）職員等による外部からのアクセス等の制限

①情報セキュリティ管理者は、所管する局等で、職員が外部から内部のネットワーク又は情報システムにアクセスする場合は、あらかじめ情報セキュリティ統括管理者（各部門の長）と協議する。
②ネットワーク管理者又は情報システム管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の職員に限定する。
③ネットワーク管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保する。
④ネットワーク管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じる。
⑤ネットワーク管理者又は情報システム管理者は、外部からのアクセスに利用するパソコン等の端末を職員に貸与する場合、情報セキュリティ確保のために必要な措置を講じる。

（４）情報システムの調達

①ネットワーク管理者又は情報システム管理者は、情報システムの開発、導入、保守等の調達にあたっては、調達仕様書に必要とする技術的なセキュリティ機能を明記する。
②ネットワーク管理者又は情報システム管理者は、機器及びソフトウェアの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題がないことを確認する。

（５）情報システムの開発

①情報システム管理者は、システム開発の責任者及び作業者を特定する。
②情報システム管理者は、システム開発の責任者及び作業者が本研究所の提供する開発環境にて利用するＩＤを管理し、開発完了後、当該ＩＤを削除する。
③情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定する。

④情報システム管理者は、システム開発の責任者及び作業者が本市の提供する開発環境にて利用するハードウェア及びソフトウェアを特定する。
⑤情報システム管理者は、利用を認めていないソフトウェアがインストールされている場合、当該ソフトウェアをシステムから削除する。

（6）情報システムの導入

①情報システム管理者は、情報システムの開発、保守及びテストを行う環境と運用環境を分離する。
②情報システム管理者は、情報システムの開発、保守及びテストを行う環境から運用環境への移行について、開発及び保守計画の策定時に手順を明確にする。
③情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が必要最小限となるように配慮する。
④情報システム管理者は、導入する情報システムやサービスの可用性が確保されていることを確認した上で導入する。
⑤情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分なテストを行う。

（7）情報システムの開発・保守に関する資料等の整備・保管

①情報システム管理者は、情報システムの開発・保守に関連する資料及び情報システムの関連する文書を適正に整備・保管する。

（8）情報システムの運用

①情報システム管理者は、情報システムの開発及び保守用ソフトウェア等を更新する場合又は当該ソフトウェアにパッチを適用する場合、他の情報システムとの整合性を確認する。

（9）ネットワーク及び情報システムの不正プログラム対策

①ネットワーク管理者は、外部ネットワークから受信したファイル及び外部ネットワークに送信するファイルについて、外部ネットワークとのゲートウェイにおいてコンピュータウイルス等の不正プログラムの有無を確認し、それぞれシステムへの侵入及び外部への拡散を防止する。ただし、接続相手が互いに限定されたネットワーク同士の接続で、不正プログラムの感染及び侵入が生じる可能性が著しく低い場合を除く。
②ネットワーク管理者又は情報システム管理者は、添付ファイルが付いた電子メールを送受信する場合、不正プログラム対策ソフトウェアでチェックを行わなければならない。
③ネットワーク管理者又は情報システム管理者は、所管するサーバ及びパソコン等の端末に不正プログラム対策ソフトウェアを常駐させる。
④ネットワーク管理者は、不正プログラム対策ソフトウェアは、常に最新のバージョンに保つとともに、パターンファイルについても、常に最新の状態を維持する。
⑤ネットワーク管理者、情報システム管理者及び情報セキュリティ管理者は、業務上利用するソフトウェアについて、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアは、原則として利用してはならない。
⑥ネットワーク管理者及び情報システム管理者は、不正プログラム情報を収集し、職員等に対して注意喚起を行う。
⑦情報システム管理者は、インターネットに接続したシステムの不正プログラム対策ソフトウェアは、常に最新のバージョンに保つとともに、パターンファイルについても、常に最新の状態を維持する。なお、インターネットに接続していないシステムの

不正プログラム対策ソフトウェアは、当該ソフトウェアのバージョン及びパターンファイルを定期的に最新の状態にする。

⑧情報システム管理者は、インターネットに接続していないシステムにおいて記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、情報セキュリティ管理者の許可を得ていない記録媒体を職員等に利用させてはならない。

⑨職員等は、パソコン等の端末において、不正プログラム対策ソフトウェアがインストールされている場合、当該ソフトウェアの設定を変更してはならない。

⑩職員等は、外部からデータ又はソフトウェアを取り入れる場合には、不正プログラム対策ソフトウェアによる確認を行う。

⑪職員等は、パソコン等の端末を持ち込んだ場合又は外部から持ち帰った場合は、研究所内のネットワークに接続する前に当該端末が不正プログラムに感染していないこと及びパッチの適用状況等を確認する。

⑫職員等は、差出人不明又はファイルが不自然に添付された電子メールを受信した場合は、本研究所への連絡等であることが明らかである場合を除き、速やかに削除する。

⑬職員等は、パソコン等の端末に対して、不正プログラム対策ソフトウェアによるフルスキャンを定期的に実施する。

⑭職員等は、ネットワーク管理者及び情報システム管理者が提供する不正プログラム情報を常に確認する。

⑮職員等は、不正プログラムに感染した場合又は感染が疑われる場合は、次の対応を行う。

ア　パソコン等の端末の場合、ＬＡＮケーブルの即時取り外しを行う。

イ　モバイル端末の場合、直ちに利用を中止し、通信を行わない設定への変更を行う。

（10）ネットワーク及び情報システムの不正アクセス対策

①ネットワーク管理者及び情報システム管理者は、利用しないポートを閉鎖する。ただし、他のネットワークと接続していないネットワークで安全性が確保されている等、ポートの閉鎖が不要である場合を除く。

②ネットワーク管理者及び情報システム管理者は、不要なサービスについて、機能を削除又は停止する。

③ネットワーク管理者及び情報システム管理者は、不正アクセスによるウェブページの書換え防止策を講じる。

④情報セキュリティ統括管理者及び情報セキュリティ管理者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じる。

⑤情報セキュリティ統括管理者及び情報セキュリティ管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努める。

⑥ネットワーク管理者及び情報システム管理者は、職員等による不正アクセスを発見した場合、当該職員等の所属の情報セキュリティ統括管理者（各部門の長）に通知し、適正な措置を求める。

⑦ネットワーク管理者及び情報システム管理者は、セキュリティホールに関する情報を収集し、緊急に対応する必要がある場合等、必要に応じて、関係者間で共有する。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を講じる。

(11) ファイルサーバの管理

①情報システム管理者は、ファイルサーバ（職員等が情報を格納するサーバ）を各所属等の単位で構成し、他所属の職員からの閲覧制限・利用制限することができるように設定する。

②情報セキュリティ管理者は、特定の職員等のみに取り扱わせる機密情報を含む情報資産についてフォルダを分けて格納する等の措置を講じ、特定の職員等以外からの閲覧制限・利用制限することができるように設定する。

③情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの二重化対策に関わらず、消失した際の影響が大きいと考えられる場合等、必要に応じて、定期的にバックアップをとる。

(12) 管理記録及び作業の確認

①ネットワーク管理者及び情報システム管理者は、所管するネットワーク又は情報システムの運用において、職員等又は契約により操作を認められた事業者が設定変更等の作業を行う場合は、作業内容について記録を作成し、窃取、改ざん等をされないように適正に管理する。

(13) 電子メールの管理

①ネットワーク管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることが不可能となるようにメールサーバの設定を行う。

②ネットワーク管理者は、迷惑メール等の受信又は送信に対して適正な対応を行う。

③ネットワーク管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にする。

④ネットワーク管理者は、職員等が利用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知する。

(14) ログ及び障害記録の取得等

①ネットワーク管理者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定期間保存する。

②ネットワーク管理者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理する。

6 運用

情報システムの管理・運用上の不備によって生じる内部統制上の脅威に対して、以下のとおり対策を講じる。

（1）公開範囲等

本実施手順は、公にすることにより本研究所の事業に重大な支障を来すおそれがあることから、規程第２条（３）において定める「職員」以外に公開してはならない。ただし、相手方と秘密保持に関し合意が成立している場合は、必要最小限の範囲に限り公開することができる。

（2）遵守状況の確認及び対処

①情報セキュリティ管理者は、職員等のポリシーの遵守状況について定期的に確認を行い、問題を認めた場合には、情報セキュリティ統括管理者（各部門の長）に報告する。

②ネットワーク管理者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等におけるポリシーの遵守状況について定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処する。

（3）パソコン等の端末及び記録媒体等の利用状況調査

情報セキュリティ管理者（情報セキュリティ管理者が指名した者を含む。）は、不正アクセス、不正プログラム等の調査のために、職員等が利用しているパソコン等の端末及び記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（4）侵害への対応

①ネットワーク管理者及び情報システム管理者は、侵害が発生した場合の個別の対応手順については、以下の事項を記載した手順書を作成する。

・関係者の連絡先
・発生した事案に係る報告すべき事項
・発生した事案への対応措置
・再発防止措置の策定

②それぞれ所管する対応手順は情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、見直さなければならない。

（5）懲戒処分等

①ポリシーに違反した職員等及びその管理監督者は、その重大性、発生した事案の状況等に応じて、本研究所就業規則等による懲戒処分等の対象となる。

②情報セキュリティ統括管理者（各部門の長）は、職員等のポリシーに違反する行動を確認した場合、速やかに当該職員に指導し、違反を改善させる。

③情報セキュリティ管理者は、情報セキュリティ統括管理者（各部門の長）の指導によっても違反が改善されない場合、ネットワーク管理者又は情報システム管理者に指示して、当該職員等のネットワーク又は情報システムの利用を停止することができる。

④情報セキュリティ管理者は、当該職員等のネットワーク又は情報システムの利用を停止した場合、速やかに、情報セキュリティ管理者に周知する。

7 評価委及び見直し

規程及び実施手順からなる ISIT 情報セキュリティポリシーの評価及び見直し等について以下のとおり行う。

（1）情報セキュリティ監査

①情報セキュリティ最高責任者は、ネットワーク、情報システム及び各所属の情報セキュリティ対策の実施状況を検証するため、定期的に又は必要に応じて、監査を実施する。

②情報セキュリティ管理者及び情報セキュリティ統括管理者は、情報セキュリティ最高責任者の指示に従い、監査を行う。

（2）情報セキュリティ自己点検

①ネットワーク管理者、情報システム管理者及び情報セキュリティ管理者は、所管するネットワーク、情報システムの情報セキュリティ対策について、定期的に自己点検を実施する。

②情報セキュリティ最高責任者は、ネットワーク責任者、情報システム責任者又は情報セキュリティ責任者に対して、自己点検の結果及びその結果に基づく改善策について報告を求めることができる。

③職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図る。

（3）実施手順の見直し

情報セキュリティ最高責任者は、情報セキュリティ管理者および情報セキュリティ統括管理者に対し、実施手順について、監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、必要に応じて、その見直しを行わせる。ただし軽易な改定については、情報セキュリティ管理者に行わせる。

附則
本実施手順は、令和２年４月１日から施行する。
附則
本実施手順は、令和３年８月 20 日から施行する。