情報セキュリティガイドライン

2012 年 4 月　制定
2018 年 2 月 13 日　改訂

情報・システム研究機構
国立遺伝学研究所

目　　　　　　次

はじめに

本文書は、「情報・システム研究機構情報セキュリティポリシー」（平成19年6月22日制定、平成28年12月19日改訂、以下「ポリシー」という。）に基づき、国立遺伝学研究所（以下「研究所」という。）における情報資産の運用管理、情報資産を利用する者の管理、情報資産の障害等の管理についての基準及び実施手順等を定めたものである。

第 1 部 情報資産運用・管理実施手順

第 1 章 総則

1-1 （目的）

本ガイドラインは、研究所の有する情報資産を適正に保護・活用することで、研究所の情報システムの信頼性、安全性及び効率性の向上に資することを目的とする。

1-2 （定義）

本文書における用語は、次のように定める。

一 情報資産 情報システム、情報ネットワークに接続された情報ネットワーク機器並びに電子計算機、及びそこで取り扱われる、有形・無形の資産。

二 情報ネットワーク機器 情報ネットワークの接続のために設置され、送受信される情報の制御を行うための装置。

三 電子計算機 コンピュータ全般を指し、オペレーティングシステム及び接続される周辺機器まで含めた端末（サーバやタブレット等を含む）。

四 安全区域 電子計算機及び情報ネットワーク機器を設置した事務室、研究室、教室又はサーバ室等の内部であって、利用者等以外の者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域。

五 利用者 研究所の情報資産及び情報システムを取扱う者。研究所と雇用関係にある者のみならず、企業・他機関等から出向する者及び外来者、ネットワーク等を通じてリモートアクセスを行う者も全て含む。

六 主体認証 識別符号を提示した利用者等又は電子計算機が、情報システムにアクセスする正当な権限を有するか否かを検証すること。識別符号とともに正しい方法で認証情報が提示された場合に、認証が成立したとみなされる。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、本文書における「主体認証」については、公的又は第三者による証明に限るものではない。

七 識別符号 利用者等又は電子計算機を識別するために、情報システムが認識する符号。代表的な識別符号として、ユーザ ID が挙げられる。

八 認証情報 主体認証を行うために、利用者等又は電子計算機が情報システムに提

示する情報をいう。代表的な認証情報として、パスワードが挙げられる。また、指紋などによる生体認証情報及びICカード、USBメモリーなどの主体情報認証格納装置に格納された認証情報も含まれる。

九　アカウント　主体認証を行う必要があると認めた情報システムにおいて、利用者等又は電子計算機に付与された正当な権限。

十　要機密情報　研究所情報システムで取り扱う情報のうち、秘密文書に相当する機密性を有する情報、もしくは秘密文書に相当する機密性は有しないが,その漏えいにより、利用者の権限が侵害され又は研究所活動の遂行に支障を及ぼす恐れがある情報。

十一　要保全情報　研究所情報システムで取り扱う情報のうち、改ざん、誤びゅう又は破損により、利用者の権限が侵害され、又は研究所活動の的確な遂行に支障を及ぼす恐れがある情報。

十二　要安定情報　研究所情報システムで取り扱う情報のうち、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、利用者の権限が侵害され又は研究所活動の安定的な遂行に支障を及ぼす恐れがある情報。

十三　要保護情報　要機密情報、要保全情報、及び要安定情報を指す。

十四　その他の用語の定義は、ポリシーの定めるところによる。

1-3 （適用範囲）

本ガイドラインは、情報資産及び情報システムの利用者に適用する。

1-4 （組織体制）

研究所の情報システムの運用は、ポリシーに従い、情報セキュリティ責任者（所長）の下、情報システムセキュリティ責任者（情報基盤ユニット長。以下、「システム責任者」という。）、必要業務をおこなう情報システムセキュリティ管理者（各研究室の管理者及び総務企画課長。以下、「システム管理者」という。）、及び情報基盤ユニットが行う。

2　本ガイドラインの策定・変更および研究所における情報資産の管理は、電子計算機委員会がおこなう。

1-5 （禁止事項）

システム責任者及びシステム管理者は、次に掲げる事項を行ってはならない。

一　情報資産の目的外利用

二　守秘義務に違反する情報の開示

三　情報セキュリティ責任者の許可なく情報ネットワーク上の通信内容を監視し、又は情報ネットワーク機器及び電子計算機の利用記録を採取する行為

四　情報セキュリティ責任者の要請に基づかないセキュリティ脆弱性の検知

五　その他法令に基づく処罰の対象となり、又は損害賠償等の民事責任を発生させる情報の発信

六　管理者権限を濫用、またはそれを助長する行為

第 2 章　情報システムの設置と運用

情報システムの設置時、運用時、運用終了時といった情報システムのライフサイクルに着目し、遵守すべき事項と、情報資産及び情報システムを保護するための対策を示す。

2-1 （セキュリティホール対策）

システム管理者は、電子計算機及び情報ネットワーク機器（公開されたセキュリティホールの情報がない電子計算機及び情報ネットワーク機器を除く。以下この項において同じ。）について、セキュリティホール対策に必要となる機器情報を収集し、対策を実施する。

2-2 （不正プログラム対策）

システム管理者は、不正プログラム感染の回避を目的とした実施事項を定め、対策を実施する。また、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、対処が必要な場合には、利用者に対処を指示する。

2-3 （サービス不能攻撃対策）

システム管理者は、要安定情報を取り扱う情報システム（サーバや、情報ネットワーク機器または通信回線等）について、必要情報を収集し、サービス不能攻撃対策を実施する。

2-4 （安全区域）

システム責任者は、情報システムによるリスク（物理的損壊又は情報の漏えいもしくは改ざん等のリスクを含む。）を検討し、安全区域に施設及び環境面からの対策を実施する。

2 システム責任者は、安全区域に不審者を立ち入らせない措置を講ずる。

3 システム責任者は、要保護情報を取り扱う情報システムについては、電子計算機を安全区域に設置する。ただし、モバイル PC やタブレットについては、この限りでない。

4 システム責任者は、情報ネットワーク機器を安全区域に設置する。

2-5 （規定及び文書の整備）

システム責任者は、電子計算機および情報ネットワーク機器のセキュリティ維持に関する規定を整備する。

2-6 （主体認証と権限管理）

システム管理者は、利用者等が電子計算機にログインする場合には主体認証を行うように電子計算機を構成する。

2 システム管理者は、ログオンした利用者等の識別符号に対して、権限管理を行う。

2-7 （電子計算機の対策）

システム責任者は、電子計算機で利用可能な（又は利用不可能な）ソフトウェアを定め、利用者に周知する。

2 システム責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を発揮できる能力を、将来の見通しを含め検討し、確保する。

3 システム管理者は、要保護情報を取り扱うモバイルPCについて、所外で使われる際にも、所内で利用される電子計算機と同等の保護手段を講じる。

2-8 （通信回線の対策）

システム責任者は、通信回線構築によるリスク（物理的損壊又は情報の漏えい若しくは改ざん等のリスクを含む。）を検討して VPN を含む通信回線を構築し、セキュリティ対策をおこなう。

2 システム責任者は、要安定情報を取り扱う情報システムについては、通信回線及び情報ネットワーク機器に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保する。

3 システム管理者は、要保護情報を取り扱う情報システムについては、通信回線を用いて送受信される要保護情報の暗号化を行う必要性の有無を検討し、必要に応じて暗号化する。

4 システム管理者は、情報ネットワーク機器上で証跡管理を行う必要性を検討し、必要と認めた場合には実施する。

2-9 （規定及び文書の見直し、変更）

システム責任者は、適宜、電子計算機および情報サービスのセキュリティ維持に関する規定の見直しを行う。また、当該規定を変更した場合には、当該変更の記録を保存する。

2 システム管理者を変更する場合、システム責任者は変更内容をシステム管理文書へ反映し、変更の記録を保存する。

3 電子計算機の構成を変更する場合、システム管理者、変更内容を関連文書へ反映し、変更の記録を保存する。

4 通信回線の構成、情報ネットワーク機器の設定、アクセス制御の設定又は識別符号を含む事項を変更した場合、システム管理者は、変更内容を関連文書へ反映し、当該変更の記録を保存する。

2-10 （資源の管理）

システム責任者は、情報資源の利用を総合的かつ計画的に推進するため、これらの資源を利用者等の利用形態に応じて適切に分配し管理する。

第 3 章　情報資産の格付けと取扱い

3-1 （情報資産の保護注意義務）

利用者は、情報資産を作成し又は入手する場合は、研究所の研究教育目的に十分留意し、適切に保護するように務める。また同様の管理を学生や外来者に対して尊守させる。

3-2 （情報資産の管理者）

研究所の職員が業務上作成、入手した情報資産については、その者が管理者となる。

2　学生が、遺伝研における教育・研究活動のために作成、入手した情報資産については、主任指導教員が管理者となる。

3　外来者が、遺伝研における教育・研究活動のために作成、入手した情報資産については、受け入れ担当教員が管理者となる。

4　必要に応じて、情報資産の管理者を他の職員等に変更できる。

5　管理者が遺伝研の職員等の地位を失った場合には、情報システムセキュリティ責任者が速やかに当該資産の新しい管理者を割り当てる。

3-3 （格付けと取扱制限の明示等）

研究所における情報の格付け及びその取扱制限については、別に定める「情報・システム研究機構国立遺伝学研究所情報格付け基準」による。

3-4 （格付けに応じた情報の保存と廃棄）

情報資産は、その必要が無くなった時点で速やかに廃棄する。電子媒体は再フォーマットまたは物理的破壊、紙媒体はシュレッダーや溶解処理等の措置をとる。

第 4 章　アクセス制御

4-1 （アクセス制御機能の導入）

システム責任者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討する。その際、要保護情報を取り扱う情報システムは、アクセス制御を行う必要があると判断する。

2　システム管理者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設ける。

4-2 （利用者等による適正なアクセス制御）

システム責任者は、それぞれの情報システムに応じたアクセス制御の措置を講じるよう、利用者等に指示する。

2　利用者等は、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従い、情報システムに装備された機能を用いて、必要なアクセス制御を実施する。

4-3 （無権限のアクセス対策）

システム責任者及びシステム管理者は、無権限のアクセス行為を発見した場合は、速やかに情報セキュリティ責任者に報告する。情報セキュリティ責任者は、上記の報告を受けたときは、遅滞なく最高情報セキュリティ管理者にその旨を報告する。

2　情報セキュリティ責任者は、前項の報告を受けた場合は、新たな防止対策等必要な措置を講じる。

第 5 章　アカウント管理

5-1 （アカウント管理機能の導入）

システム責任者は、すべての情報システムについて、アカウント管理を行う必要性の有無を検討する。この場合、要保護情報を取り扱う情報システムについては、アカウント管理を行う必要があると判断する。

2　システム管理者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理を行う機能を設ける。

5-2 （アカウント管理手続の整備）

システム責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理について、以下の事項を含む手続を明確にする。

一　主体からの申請に基づいてアカウント管理を行う場合には、その申請者が正当な主体であることを確認するための手続

二　主体認証情報の初期配布方法及び変更管理手続

三　アクセス制御情報の設定方法及び変更管理手続

2　システム責任者は、アカウント管理を行う必要があると認めた情報システムにおいて、アカウント管理を行う者を定める。

5-3 （アカウントの発行）

アカウント管理を行う者は、利用者等からのアカウント発行申請を受理したときは、申請者が違反による処分期間中である場合を除き、遅滞無くアカウントを発行する。

2　アカウント管理を行う者は、アカウント管理を行う必要があると認めた情報システムにおいて、情報システムを利用する許可を得た主体に対してのみ、必要最小限のアクセス制御権を有するアカウントを発行する。

第 2 部　情報システム障害等管理実施手順

第 2 部は、研究所の情報システムの運用において非常事態が発生した場合の行動を非常時行動計画として事前に定め、早期発見・早期対応により、事件・事故の影響を最小限に抑え、早急な情報システムの復旧と再発防止に努めるために必要な措置を定める。

1－1 （定義）

本文書において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

一　非常事態　研究所の情報システムの運用に関するインシデントのうち特に緊急性を要するものをいう。

二　その他の用語の定義は、ポリシー及び本文書の第 1 部で定めるところによる。

1－2 （非常事態の報告）

システム責任者は、インシデントについての報告または通報を研究所内または研究所外から受けつけ、迅速に情報を集約する手段を整備し、周知・公表する。

2　システム責任者は、報告または通報を受けたインシデントのうち、非常事態の発生またはそのおそれがある場合には、情報セキュリティ責任者へ報告する。

インシデント対応手順

ここに記載のインシデント対応手順は、災害等によるネットワーク設備の損壊、利用者等による違反行為や所外から所内への攻撃行為などにより発生したインシデントについて、適切な対応によりインシデントの影響が拡大することを防ぐと共に復旧を図るため、インシデントの発見から対処、さらには、再発防止策の実施にいたる手続きを定める。

1．（定義）

本文書において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

（1） 物理的インシデント

地震等の天災、火災、事故、盗難等によるネットワークを構成する機器や回線の物理的損壊及び滅失並びにその他の物理的原因による情報システムやネットワークの機能不全及び障害等、情報セキュリティの確保が困難な事由の発生及びそのおそれをいう。

（2） セキュリティインシデント

ネットワークや情報システムの稼動を妨害しまたはデータの改ざんや消失を起こす行為及び利用行為の形態自体には問題は無いが、ネットワークの帯域やディスクや CPU の資源を浪費するなど、ネットワークやシステムの機能不全や障害または他の利用者の迷惑となる行為による情報セキュリティの確保が困難な事由の発生及びそのおそれをいい、下記原因によるものを含む。

① 大量のスパムメールの送信
② コンピュータウイルスの蔓延及び意図的な頒布
③ 発信者を偽った電子メールへのファイル添付や偽装した URL への誘導などにより、利用者の環境に利用者の意図しないアプリケーション等をインストールさせる行為
④ 情報システムの脆弱性や利用者による不適切なアカウント管理等を利用することにより、 ネットワークや情報システムのセキュリティに影響を及ぼす行為
⑤ 不正アクセス禁止法に定められた特定電子計算機のアクセス制御を免れる行為
⑥ サービス不能攻撃及び情報セキュリティ責任者の要請に基づかずに管理権限のない情報システムのセキュリティ上の脆弱性を検知する行為
⑦ 禁止されている形態や目的での P2P ソフトウェアの利用
⑧ 禁止された方法による所外接続
⑨ 所内ネットワークへの侵入を許すようなアカウントを格納した PC の盗難・紛失
⑩ 過失による秘密情報（個人情報を含む）の漏えい、データの消失または改ざん

（3） コンテンツインシデント

ネットワークを利用した情報発信内容（以下「コンテンツ」という。）が著作権侵害等の他

人の権利侵害や児童ポルノ画像の公開等の違法行為及び公序良俗違反である行為（及びその旨主張する被害者等からの請求）による事故をいい、下記原因を含む。

① 電子掲示板、ブログやウェブページ等での名誉・信用毀損にあたる情報の発信
② 他人の個人情報や肖像の無断公開及び漏えいその他プライバシーを侵害する情報の発信
③ 通信の秘密を侵害する行為
④ 著作物の違法コピーのアップロード等、他人の著作権等の知的財産権を侵害する情報の発信
⑤ 秘密であるデータやプログラムの不正公開等守秘義務に違反する情報の発信
⑥ 児童ポルノやわいせつ画像の公開
⑦ ネットワークを利用したねずみ講
⑧ 差別、侮辱及びハラスメントにあたる情報の発信
⑨ 営業又は商業を目的とした本研究所情報システムの利用行為

（4） インシデント

物理的インシデント、セキュリティインシデント及びコンテンツインシデントをいう。

（5） 対外的インシデント

インシデントのうち、利用者等による行為であって、外部ネットワークにおけるあるいは外部のシステムに対して行われた行為による事故・事件をいう。

（6） 対内的インシデント

インシデントのうち、外部のネットワークから内部に向かって行われた行為による事故・事件をいう。

（7） 所外クレーム

所内の利用者等による情報発信行為（本研究所の業務としてなされたものを除く）の問題を指摘しての連絡・通報及び所外（所内の者が、弁護士等の代理人を立てる場合も含む）からの発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求、及び証拠・証言の収集や犯罪捜査等にかかわる協力要請や強制的命令をいう。

（8） 対外クレーム

対内的インシデントに対し、所外の発信者に対して連絡・通報し、または発信中止を求める要求、損害賠償の請求、謝罪広告の請求、発信者情報の開示請求等の民事的請求及び当局に犯罪捜査の告訴・告発をすることをいう。

(9) 運用･管理規程

ポリシー及び本文書第 1 部とそれにもとづく手順、命令、計画等をいう。

(10) 緊急連絡網

ポリシー及び本文書にもとづき、特に重要と認めた情報システムについて、そのシステム責任者及びシステム管理者の緊急連絡先、連絡手段及び連絡内容を含む連絡網をいう。

(11) 所外窓口

インシデントについて所外から連絡･通報を受け、所外への連絡･通報及び対外クレームをするための窓口をいう。

(12) 利用規程

本文書とそれにもとづく手順、その他研究所の情報ネットワークや情報システムの利用上のルールをいう。

(13) 利用規程違反行為

インシデントに係わるかどうかに限らず、利用規程に違反する行為をいい、下記を含む。

① 情報システム及び情報について定められた目的以外の利用
② 電子掲示板、ブログ及びウェブページ等での名誉･信用毀損にあたる情報の発信
③ 差別、侮辱及びハラスメントにあたる情報の発信
④ 他人の個人情報、肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信
⑤ 守秘義務に違反する情報の発信
⑥ 他人の著作物の違法コピーのアップロード等、他人の著作権等の知的財産権を侵害する情報の発信
⑦ 通信の秘密を侵害する行為
⑧ 営業ないし商業を目的とした研究所情報システムの利用
⑨ 情報セキュリティ責任者の許可（業務上の正当事由）なくネットワーク上の通信を監視及び情報機器の利用情報を取得する行為
⑩ 不正アクセス禁止法に定められたアクセス制御を免れる行為及びそれを助長する行為
⑪ 情報セキュリティ責任者の要請に基づかずに管理権限のないシステムのセキュリティ上の脆弱性を検知する行為
⑫ サービス不能攻撃等、故意に過度な負荷を情報システムに与えることにより研究所の円滑な情報システムの運用を妨げる行為
⑬ その他法令に基づく処罰の対象となり、損害賠償等の民事責任を発生させる情報の発信

⑭ 管理者の許可をえず、ソフトウェアのインストールやコンピュータの設定の変更を行う行為

⑮ 上記の行為を助長する行為

2. （インシデント通報窓口）

（1） インシデント対応のための所外・所内の連絡・通報窓口は次に掲げるとおりとする。

所内窓口：情報基盤ユニット

所外窓口：情報基盤ユニット

（2） 所外窓口への所外からの e-mail による連絡手段は、以下のメーリングリストとし、必要に応じて公表する。

Email: lan-info@nig.ac.jp

（3） 所外への連絡・通報、対外クレームに当たっては、所外窓口及び機構の CSIRT と連絡を密にし、無断で行わない。

3. （インシデントの対応判断の手順）

（1） 情報基盤ユニットは、インシデントを発見し、または、所外クレーム等によりインシデントを認知した場合は、緊急連絡網その他所定の連絡網により、適宜、情報セキュリティ責任者、システム責任者、システム管理者にインシデントの初期対応を依頼するものとする。

（2） 情報基盤ユニットは、研究所ネットワークに関るインシデントについては、必要に応じて自ら技術的対応をする。

（3） システム管理者は、インシデントを発見し、または情報基盤ユニット等を通じて内部・外部からの通報を受けることにより認知した場合、ただちにシステム責任者に状況報告する。

（4） システム責任者は、インシデントを自ら認知するかシステム管理者もしくは情報基盤ユニットから状況報告を受けた場合、下記の基準により一次切り分け判断を行う。

① 所内ネットワークに閉じた問題の場合

ｉ） 物理的インシデント及びセキュリティインシデントの場合で、対外的インシデントでも対内的インシデントでも無く、所内ネットワークにのみ影響が生じている場合、システ

ム管理者もしくは情報基盤ユニットに対策を指示する。

ii） ｉ）以外の場合、情報セキュリティ責任者および機構 CSIRT に状況を報告し、情報基盤ユニットの支援を受けながら、物理的インシデントまたはセキュリティインシデント対応のプロセスを実施する。

② コンテンツインシデントの場合

ｉ） コンテンツインシデントの場合、加害者と被害者が所内に閉じている場合であっても、法律的対策を講じる必要があるため、原則として情報セキュリティ責任者および機構 CSIRT に報告し、情報基盤ユニットの支援を受けながら、ログの保全等、必要な技術的措置を取る。

ii） ただし、爆破予告・自殺予告など、生命・身体への危険等の緊急性がある場合で、所内での対処が可能な場合は、コンテンツに関する緊急対応を実施の上、情報セキュリティ責任者と機構 CSIRT に結果報告をする。

（5） システム責任者は、あらかじめ定められた手順に従って、緊急な技術的対応が必要なときは、システム管理者もしくは情報基盤ユニットに指示して対応を実施し、情報セキュリティ責任者に対応結果を報告する。法的に慎重な判断を要する場合は、対応を実施する前に必ず情報セキュリティ責任者および機構 CSIRT に報告し、指示を受ける。

（6） システム責任者から報告を受けた情報セキュリティ責任者は、コンテンツインシデントについて、システム責任者及びシステム管理者を指揮監督する。セキュリティインシデント対応については、ポリシーに基づいて最高情報セキュリティ責任者に指示や承認を求める。また、法的判断を要する問題のうち、通報者への内容確認や定型回答文書の発信等を情報システム責任者や所外窓口に対して一定の一時的対応を指示または依頼する。

（7） 所外クレームか対外クレームの判断と対応

① 情報セキュリティ責任者は、所外クレームにより認知したインシデントの場合、所外クレーム対応を併せて実施する。

② 情報セキュリティ責任者は、法律専門家に相談しながら、必要に応じて対外クレームを実施する。

③ 所内問題として処理可能であるインシデントは、通常の技術的対応また利用規程違反対応とする。

4. （物理的インシデント発生時の対応）

（1） 発生から緊急措置決定まで

① 通報・発見等で物理的インシデントの可能性を認知したシステム管理者もしくは情報基

盤ユニットは、事実を確認するとともにシステム責任者に報告し、被害拡大防止のための緊急措置の必要性について判断を求める。

② システム管理者もしくは情報基盤ユニットは、後日の調査に備え、物理的インシデント発生時の状況に関する記録を作成し、ネットワーク運用に影響があるおそれがある場合、バックアップデータの作成及びハードディスクのイメージの保存等を行う。

(2) 被害拡大防止の応急措置の実施

① システム責任者は、個別システムの停止やネットワークからの遮断、機器の交換及びネットワークの迂回等の緊急措置の必要性を判断し、実施をシステム管理者もしくは情報基盤ユニットに指示する。

② システム責任者は、利用者等による対処が必要な場合には、その旨を指示する。

(3) 復旧計画

① システム管理者および情報基盤ユニットは、物理的インシデントによる被害や緊急措置の影響を特定し、システムやネットワークの復旧計画を立案する。

② システム責任者は、一で立案した復旧計画を精査し、情報セキュリティ責任者の承認を得て実施する。

(4) 原因調査と再発防止策

① システム管理者もしくは情報基盤ユニットは、物理的インシデント発生の要因を特定し、再発防止策を立案する。

② システム責任者は、利用者等への注意喚起等を含めた再発防止策を検討し、情報セキュリティ責任者は検討結果に基づき再発防止策を策定する。

③ システム責任者及びシステム管理者は、インシデント対応作業の結果をまとめ、情報セキュリティ責任者は、再発防止策とあわせて最高情報セキュリティ責任者に報告するとともに、必要によりポリシーや実施手順の改善提案を行う。

5. (セキュリティインシデント発生時の対応)

(1) 発生から緊急措置決定まで

① 監視システムによるセキュリティインシデントの可能性を示す事象の検知や通報等でセキュリティインシデントの可能性を認知したシステム管理者もしくは情報基盤ユニットは、事実を確認するとともにシステム責任者に報告し、被害拡大防止のための緊急措置の必要性について判断を求める。

② システム管理者および情報基盤ユニットは、後日の調査に備え、セキュリティインシデント発生時の状況、例えばログイン状況、ネットワーク接続や手順の稼働状況に関する

記録を作成し、バックアップデータの作成、ハードディスクのイメージの保存等を行う。

③ セキュリティインシデントが、外部からの継続している攻撃等であって攻撃元ネットワークの管理主体等への対処依頼が必要な場合、情報セキュリティ責任者の承認を得てシステム責任者から相手方サイトへの対処依頼を行う。

(2) 被害拡大防止の応急措置の実施

① システム責任者は、個別システムの停止やネットワークからの遮断(他の情報システムと共有している所内通信回線又は所外通信回線から独立した閉鎖的な通信回線に構成を変更する等)等の緊急措置の必要性を判断し、実施をシステム管理者もしくは情報基盤ユニットに指示する。

② 情報セキュリティ責任者及びシステム責任者は、情報システムのアカウントの不正使用の報告を受けた場合には、直ちに当該アカウントによる使用を停止する。

③ システム責任者は、利用者等による対処が必要な場合には、その旨を指示する。

(3) 緊急連絡及び報告

① システム責任者は、緊急の被害拡大防止措置を実施する場合は、情報セキュリティ責任者と機構 CSIRT に報告する。

② システム責任者と情報基盤ユニットは、情報セキュリティ責任者または機構 CSIRT の指示に基づき、攻撃元サイトや関係するサイトへの連絡、外部広報、及び JPCERT/CC への連絡等をおこなう。

(4) 復旧計画

① システム管理者および情報基盤ユニットは、セキュリティインシデントの被害や緊急措置の影響を特定し、システムやネットワークの復旧計画を立案する。

② システム責任者は、①で立案した復旧計画を検討し、情報セキュリティ責任者の承認を得て実施する。

(5) 原因調査と再発防止策

① システム管理者および情報基盤ユニットは、セキュリティインシデント発生の要因を特定し、再発防止策を立案する。

② システム責任者は、利用者等への注意喚起等を含めた再発防止策を検討し、情報セキュリティ責任者の承認を得て実施する。

③ システム責任者とシステム管理者は、インシデント対応作業の結果をまとめ、情報セキュリティ責任者は、再発防止策とあわせて最高情報セキュリティ責任者に報告するとともに、必要によりポリシーや実施規程の改善提案を行う。

6. （コンテンツインシデントに関する緊急対応）

（1） システム管理者もしくは情報基盤ユニットは、生命・身体への危険の可能性を示唆するコンテンツ（殺人、爆破、自殺の予告等）を発見し、または通報等により認知した場合、システム責任者の指示によりコンテンツの情報発信元を探知し、その結果をシステム責任者に報告する。

（2） システム責任者は、情報セキュリティ責任者にコンテンツの情報発信元の探知結果を報告し、所内緊急連絡についての指示を求める。

7. （所外クレーム対応）

（1） 原則

① 所外クレームを受けた場合で、請求の法律的な効果及び指摘されたコンテンツや行為の違法性の判断を要するときは、あらかじめ対応手順が明確になっていない限り、必ず法律の専門家に相談する。

② システム責任者は、所外クレームの内容を情報セキュリティ責任者および機構 CSIRT に報告する。

③ システム責任者と情報基盤ユニットは、情報セキュリティ責任者または機構 CSIRT の指示に基づき、攻撃先サイトや関係する機関及び個人への連絡、外部広報及び JPCERT/CC への連絡等をおこなう。

（2） コンテンツの違法性を主張した送信中止・削除の要求

① 所内利用者から発信されたコンテンツが違法、権利侵害等であるとして、コンテンツの送信中止や削除の要求がなされた場合、システム管理者もしくは情報基盤ユニットは、事実関係を調査し、発信元利用者を特定する。

② （通常手続き）コンテンツを発信した利用者への通知と削除

ⅰ） 指摘されたコンテンツの違法性の判断が困難な場合、プロバイダ責任制限法第 3 条に基づき当該利用者に請求があった旨を通知する。通知後 7 日以内に利用者等から反論がない場合は、送信中止あるいは削除を実施する。

ⅱ） 有効と思われる反論があった場合は、その旨を削除請求者に伝えるとともに、当事者間での紛争解決を依頼する。

③ （緊急手続き）利用者等への通知前の一旦保留

ⅰ） 指摘されたコンテンツの違法性が明らかな場合、一旦コンテンツの配信を中止し、その旨を当該利用者に伝える。ただし有効な反論があればコンテンツ送信を復活する。

ⅱ） 本手続きは、著作物等の丸写しや個人の住所や電話の暴露等、権利侵害の疑いが濃厚である場合、または緊急性を要する場合にのみ実施する。

ⅲ） 本緊急手続の可能性は、所内研修・教育等を通じて利用者に周知する。

④ （再発防止）利用者が違法な情報発信を繰り返す場合、システム責任者は当該利用者の関連するアカウントを一時停止するとともに、電子計算機委員会に報告する。アカウント復活の手続きをする際には念書を取る。

(3) 損害賠償請求等

① 利用者等の情報発信や所外でのネットワークを利用した行為について損害賠償請求及び謝罪請求があった場合には、法律の専門家と相談する。

② 所外クレームに対して、法律的判断をせずに、謝罪することや、その他の約束をしてはならない。

③ 利用者等の発信者情報等、連絡先が特定できている場合、損害賠償を請求する相手方には、利用者等との自主的な紛争解決を依頼するものとする。

(4) 発信者情報の開示請求

① プロバイダ責任制限法第 4 条に基づく場合

ⅰ） 利用者の情報発信や所外でのネットワークを利用した行為について発信者情報の開示請求があった場合で、Web ページ等一対多の通信によるものの場合、プロバイダ責任制限法の規定に基づき専門家と共に対処する。発信者が開示に同意している場合を除き、発信者情報の開示請求には慎重に対処する。

ⅱ） 電子メールアドレス等、事前に利用者等から開示の許諾を得ている発信者情報のみが請求されている場合についてはそれを開示してもよい。また、開示と同時に当事者間紛争解決を依頼する。

ⅲ） 発信者情報の保有の有無及び技術的に特定できるか否かの判断を行い、開示できる発信者情報がなければ、その旨を請求者に通知する。

ⅳ） 発信者情報開示請求の根拠の確認と違法性の判断については、必ず法律の専門家に相談する。

ⅴ） システム責任者が、発信者情報開示を行う法律要件を確実には満たしていないと判断した場合、開示を拒否する旨を通知する。不開示の判断に故意または重過失がなければ責任を問われないため、少しでも法律要件を満たさない事実があれば、不開示判断をすべきである。

ⅵ） 発信者情報開示の要件に該当することが確実である場合には開示できる。しかし、開示判断を誤った場合には電気通信事業法や有線電気通信法上の通信の秘密侵害罪やプライバシー侵害による損害賠償責任からは免責されないため、慎重な判断を要する。発信者が開示に同意しない場合、特に慎重な判断を要する。

(5) プロバイダ責任制限法に基づかない発信者情報の照会(民事)

利用者等の情報発信や所外でのネットワークを利用した行為について発信者情報の照会があった場合であって、メール等一対一の通信によるものの場合、下記の手順をとる。なお、警察官、検察官、検察事務官、国税職員、麻薬取締官、弁護士会及び裁判所等の法律上照会権限を有する者から照会を受けた場合であっても、原則として発信者情報を開示してはならないので同様の手順とする。

ⅰ) 電子メールアドレス等、事前に開示の許諾を得ている発信者情報のみが請求されている場合については、それを開示してもよい。許諾を得ていない発信者情報の開示については発信者の意見を聴き、発信者が開示に同意すれば開示してよい。また、開示と同時に当事者間紛争解決を依頼する。

ⅱ) 発信者が開示に同意しない場合は、開示を拒絶する。その場合は、通信の秘密及びプライバシーの保護を理由とする。

ⅲ) 発信者情報の保有の有無、技術的に特定できるか否かの判断をし、開示できる発信者情報がなければ、その旨を請求者に通知する。

(6) 強制捜査による発信者情報の差押え、提出命令等

① システム管理者もしくは情報基盤ユニットは、発信者情報を含む情報の強制捜査の事前打診があった場合には、発信者情報その他の強制捜査対象の情報を印刷あるいは記憶媒体に出力できるよう準備をしておく。

② 情報セキュリティ責任者もしくは対外折衝事務担当者は、システム管理者もしくは情報基盤ユニットの協力を得て、ネットワークの稼動への影響が最小限になるような方法で強制捜査に協力する。

③ 捜査当局から強制捜査の令状の呈示を受けた場合、令状の記載事項等を確認の上、立会いを求められたときは立会い、押収物があるときは押収目録の交付を受ける。

④ システム管理者もしくは情報基盤ユニットは、捜査当局から通信履歴(通信の送信先、送信元、通信日時など。通信内容は含まない。)について，暫定的に残しておくよう警察署長印等のある正式文書 にて求められた場合(保全要請)、保全対象の情報を印刷あるいは記録媒体に出力して保管しておくものとする。

8. (通常の利用規程違反行為の対応)

(1) 発見または通報等による認知と事実確認(情報発信者の特定を含む)

システム管理者もしくは情報基盤ユニットは発見あるいは通報により利用規程違反の疑いのある行為を知ったときは、速やかに事実関係を調査し、発信元利用者等を特定した上でシステム責任者に報告する。

（2） 利用規程違反の該当性判断

① システム管理者もしくは情報基盤ユニットの報告を受けたシステム責任者は、通常の利用規程違反行為の対応手順にのせることが可能と考える場合は、その旨情報セキュリティ責任者に報告し、確認を得るものとする。

② システム責任者は、技術的事項に関する利用規程違反に該当するか否かを判断し、該当する場合には情報セキュリティ責任者および機構 CSIRT に報告する。

③ システム責任者は、技術的事項以外の利用規程違反に該当するか否かを判断し、該当する場合には情報発信の一時停止等の措置やアカウントの一時停止等、個別の情報発信の一時停止以上の措置が必要であるかを判断する。判断にあたっては、可能な限り当該行為を行った者の意見を聴取するものとし、必要に応じて電子計算機委員会の判断を求める。

（3） 情報発信の一時停止措置

システム管理者もしくは情報基盤ユニットは、情報セキュリティ責任者またはシステム責任者の指示を受けて、利用規程違反に関係する情報発信の一時停止またはアカウントの一時停止の措置を実施する。

（4） 情報発信者に対する通知・注意・警告・当事者間紛争解決要請

情報セキュリティ責任者またはシステム責任者は、事案に応じて下記内容を発信者に通知するものとする。

ⅰ） 利用規程違反の疑いがあること

ⅱ） アカウントの一時停止措置等の利用を制約する措置を講じた場合は、そのこと、及びその理由・根拠

ⅲ） 利用規程違反行為の是正、中止の要請

ⅳ） 利用規程違反行為が是正、中止されなかった場合の効果（情報の削除やアカウントの停止、所内処分等）

ⅴ） 反論を受け付ける期間とその効果

ⅵ） 利用者等の当事者間の紛争解決の要請

（5） 個別の情報発信またはアカウントの停止と復活

情報セキュリティ責任者及びシステム責任者は、(4)の措置を講じたときは、その後の利用者等の対応により、必要に応じ電子計算機委員会の承認を得て、下記を実施するものとする。

ⅰ） 個別の情報発信及びアカウントの停止と復活

ⅱ） 有効な反論があった場合又は利用行為が是正された場合の個別の情報発信及びアカウントの復活

ⅲ） 利用行為が是正されなかった場合の情報の削除やアカウントの停止及び所内処分の

開始手続き

ⅳ） 利用者等の当事者間の紛争解決着手の有無の確認

9. （所内処分との関係）

情報セキュリティ責任者は、所外クレームの対象となった利用者等、利用規約違反をした利用者等につき、懲罰委員会（事案に応じて臨時に開設）への報告をすることができる。また、懲罰委員会による処分の検討に際し、アカウント停止処分やその他ネットワークやシステムの利用を制約する処分の必要性の有無について意見を述べることができる。

第 3 部　情報システム利用者管理実施手順

第 3 部は、機構が定める情報セキュリティポリシーに基づき、研究所における情報システムの利用に関する事項を定める。

1-1 （定義）

この文書において、用語の定義は、ポリシー、「第 1 部　情報システム運用・管理実施手順」及び「第 2 部　情報システム障害等管理実施手順」で定めるところによる。

1-2 （適用範囲）

この文書は、研究所情報システム及びそれにかかわる情報を利用するすべての者に適用する。

2　研究所の情報システムには、所内のすべての電子計算機及び情報ネットワーク機器が含まれる。

1-3 （遵守事項）

研究所情報システムの利用者等は、この文書及び研究所情報システムの利用に関する規定及び機構個人情報保護規程を遵守しなければならない。

1-4 （禁止事項）

利用者は、情報システムについて、次に掲げる行為を行ってはならない。

一　当該情報システム及び情報について定められた目的以外の利用

二　差別、名誉毀損、侮辱、ハラスメントにあたる情報の発信

三　個人情報やプライバシーを侵害する情報の発信

四　守秘義務に違反する情報の発信

五　著作権等の財産権を侵害する情報の発信

六　通信の秘密を侵害する行為

七　営業等の行為

八　情報セキュリティ責任者の許可（業務上の正当事由）なくネットワーク上の通信を監視し、または情報機器の利用情報を取得する行為

九　不正アクセス禁止法に定められたアクセス制御を免れる行為、またはこれに類する行為

十二　その他法令に基づく処罰の対象となり、または損害賠償等の民事責任を発生させる情報の発信

2　利用者は、ファイルの自動公衆送信機能を持った P2P ソフトウェアについては、これを利用してはならない。ただし、情報セキュリティ責任者が教育・研究目的で特に必要と認めた

場合は、その限りではない。

1-5 （違反行為への対処）

利用者の行為が前項に掲げる事項に違反すると被疑される行為と認められたときは、システム責任者は速やかに調査を行い、事実を確認するものとする。事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取しなければならない。

2 システム責任者は、上記の措置を講じたときは、遅滞無く情報セキュリティ責任者に報告しなければならない。

3 調査によって違反行為が判明したとき、情報セキュリティ責任者は、次に掲げる措置を講ずることができる。

一 当該行為者に対する当該行為の中止命令

二 システム責任者に対する当該行為に係る情報発信の遮断命令

三 システム責任者に対する当該行為者のアカウント停止又は削除命令

四 機構情報公開等委員会への報告

五 ポリシーに定める処罰

六 その他法令に基づく措置

1-6 （安全管理義務）

利用者は、自己の管理するコンピュータについて、研究所情報ネットワークとの接続状況に関わらず、安全性を維持する一次的な担当者となることに留意し、次の各号に掲げるとおり、悪意あるプログラムおよび不正プログラムを導入しないように注意しなければならない。

1-7 （接続の届出）

利用者は、研究所情報ネットワークに新規に情報システムを接続しようとする場合は、研究所コンピュータ・ネットワーク利用基準に従い、情報基盤ユニットの許可を得なければならない。

情報端末取扱ガイドライン

1. （目的）

本文書は、国立遺伝学研究所情報セキュリティガイドラインに準じ、国立遺伝学研究所(以下、研究所)で利用される情報端末（PC、タブレット、スマホ）およびメモリデバイスについて遵守する事項を述べる。

2. （セキュリティの維持）

(1) ウイルス対策ソフトウェアをインストールし、常に最新版に保っておくこと。

(2) 利用している OS 及びアプリケーションの脆弱性情報に留意し、不具合があれば迅速に対応すること。

3. （アクセス管理）

(1) 情報端末にはアクセス認証を設定すること。

(2) 不特定多数の第三者が情報端末にアクセスできないようにすること。

(3) 情報端末を廃棄、あるいは譲渡する場合は、内部に、要管理情報やその他重要な情報を残さないこと。

4. （所外からのアクセス）

自らが管理する情報端末に所外のネットワークからアクセスする場合は、次に掲げる事項を遵守すること。

① アクセスに使用するポート番号等を情報基盤ユニットに届け出る。または、情報基盤ユニットで提供している VPN 接続を利用する。

② 通信内容は全て暗号化する。

③ 特権アカウント（root など）によるリモートアクセスは、原則として行えないように設定する。

5. （所外への携行）

情報端末やメモリデバイスを所外に携行する場合は、場所や保管方法にかかわらず盗難や不正操作に遭う可能性があるため、下記に掲げる事項を遵守すること。

① 要保護情報（個人情報を含む）を格納しない。やむを得ず格納する場合は、所定の書式で持出し許可を届け出ること。

② 紛失や盗難の場合は、直ちに情報基盤ユニットに連絡を取り指示に従うこと。

6. （監査の実施）

適宜、情報セキュリティ責任者の指示に従って情報セキュリティ監査を実施すること。

電子メール利用ガイドライン

1. （目的）

本文書は、電子メール利用に起因する情報セキュリティリスクを軽減し、国立遺伝学研究所(以下「研究所」という)の情報資産の保護と電子メールの安全な利用手順を提供する。

2. （本文書の対象者）

本文書は、研究所が整備・提供する電子メールの利用者を対象とする。

3. （電子メールに係る全般的な注意事項）

(1) 他人の電子メールを使用、または共用しないこと。
(2) 電子メールを利用する必要がなくなった場合は、情報基盤ユニットへ届け出ること。
(3) アルファベットと数字を含み 8 文字以上の、推測しづらいパスワードを設定すること。
(5) パスワードを他人に使用されないように安全措置を講じること。
(6) 定期的に、電子メールの受信確認を行うこと。
(7) あて先間違いの電子メールを受信した場合は、可能な範囲で送信者へ間違いを通知して当該メールを削除すること。
(8) 不審な電子メールは開かず、必要に応じて情報基盤ユニットに連絡・相談すること。

4. （ウイルスに感染した場合）

利用者は、クライアント PC がウイルスに感染、または感染と疑われる場合には、更なる感染を未然に防止するため直ちに当クライアント PC をネットワークから分離し、ウイルスチェックを実施の上、情報基盤ユニットに連絡・相談し、指示を仰ぐこと。

5. （電子メールの内容）

要機密情報を電子メールで送信する場合は、暗号化した添付ファイルにすること。またファイル名に「機密性3」等の名称を入れて重要性を明記すること。

6. （アカウントの削除）

電子メールアカウントは退所後3ヶ月で削除されるため、情報基盤ユニットに相談して必要なバックアップ等を実施すること。希望者には更に3ヶ月の猶予期間を与える。

7. （本手順に関する相談窓口）

利用者は、緊急時の対応及び本文書の内容を超えた対応が必要とされる場合には、情報基盤ユニットに相談し、指示を受けること。

ウェブ公開ガイドライン

1. （目的）

本文書は、情報資産を保護し、利用者がウェブを用いて各種コンテンツや情報を、正確かつ安心・安全に公開するために必要な事項を定めることを目的とする。

2. （本文書の対象者）

本文書は、ウェブページや SNS、電子メール等を用いて情報発信を行う全ての者を対象とする。また、外部業者に委託する場合も、内容に関する責任は研究所に帰することに注意。

3. （ウェブの公開にかかわる全般的な注意事項）

(1) ウェブを用いた各種情報の公開においては、各種法令および、契約 ISP（ホスティングをしている場合など）の利用規約及び関連の所内規則等を守らなければならない。公序良俗に反する行為や社会通念上許されない行為も行ってはならない。

(2) ウェブを用いた情報公開には大きなメリットがある反面、さまざまなリスクを伴うことも承知しておかねばならない。「プロバイダ責任制限法」は、ウェブサイトや掲示板の管理者も「特定電気通信役務提供者」と見なしている。これらの管理を行う者は、同法上の責任と義務を負う。

4. （著作権等、権利の遵守）

他人が保有する知的財産権、肖像権等の諸権利を侵害してはならない。特に、ウェブ公開時には著作権侵害が発生しやすいので、十分に注意すること。 学会やシンポジウム等で協賛企業のロゴを貼るときは、事前に相手側と十分に協議すること。

5. （各種利用規程の遵守と目的外利用の禁止）

ウェブコンテンツ公開者は、本文書以外にも、関連の情報システムの利用に関する規程や規約を守らねばならない。また、研究所の定める利用目的外の利用をしてはならない。

6. （セキュリティの確保）

ウェブサーバは、原則として研究所基幹ネットワークの DMZ ゾーン内に設置するか、外部契約サーバを利用する。

7. （本手順に関する相談窓口）

ウェブサーバ管理者（ウェブサーバシステム管理者及びウェブサーバコンテンツ管理者）は、緊急時の対応及び本文書の内容を超えた対応が必要とされる場合には、情報基盤ユニットに相談し、指示を受けること。