情報セキュリティガイドライン

2012 年4月

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。以下「ポリシー」という。）第14条の規定に基づき、国立遺伝学研究所が情報セキュリティ対策を実施するに当たり、作成することとされてい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。

本文書はガイドラインとして作成し強制力を持たせていないが、上記のポリシーのほか特に明記していない情報及び情報システムの取扱いに関する関係法令等を遵守しなければならないのは当然である。

もし、職員等が、故意もしくは重大な過失により著しくポリシー等に違反した場合、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においては、ポリシーの規定に基づき処分等が行われることとなるので注意すること。

第 1 部 情報システム運用・管理実施手順

第 1 章 総則

1-1-1 （目的）

第 1 部は、情報・システム研究機構（以下「機構」という。）が定める情報セキュリティポリシーに基づき、情報・システム研究機構国立遺伝学研究所（以下「研究所」という。）における情報システムの運用及び管理に関する事項を定めることにより、研究所の有する情報資産を適正に保護、活用し、並びに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。

1-1-2 （定義）

本文書において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

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情報をいう。ただし、別に定める場合を除き、情報は電磁的記録（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た記録をいう。）に限るものとする。

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、電子計算機により情報ネットワーク上を送受信される情報の制御を行うための装置（ファイアウォール、ルータ、ハブ、情報コンセント又は無線ネットワークアクセスポイントを含む。）をいう。

三 電子計算機 コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。

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をいう。

五 利用者等 本文書第 3 部において定める利用者のほか、研究所情報資産および情報システムを取扱う者をいう。

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をいう。識別符号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利用者等又は電子計算機等を正当な権限を有するものとして認識する。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をいう。代表的な識別符号として、ユーザ ID が挙げられる。

八　主体認証情報　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。代表的な主体認証情報として、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をいう。

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をいう。

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をいう。

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をいう。

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いう

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。

1-1-3 （適用範囲）

このガイドラインは、情報資産及び情報システムを運用・管理する者に適用する。

1-1-4 （組織体制）

研究所情報システムの運用・管理は、ポリシーに従い、情報セキュリティ責任者の下、情報システムセキュリティ責任者（以下、「システム責任者」）、情報システムセキュリティ管理者（以下、「システム管理者」）等からなる電子計算機委員会が執り行うものとする。

2　情報基盤ユニットは、研究所情報システムの運用・管理について、システム責任者、情報セキュリティ管理者及び電子計算機委員会と連携し執り行うものとする。

1-1-5 （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ずにセキュリティ上の脆弱性を検知する行為

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　管理者権限を濫用する行為

七　上記の行為を助長する行為

第 2 章　情報システムのライフサイクル

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、各段階において遵守すべき事項を定め、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。

第1節　設置時

1-2-1 （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、書面として整備すること。

2 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の構築又は運用開始時に，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セキュリティホールの対策を実施すること。

1-2-2 （不正プログラム対策）

情報セキュリティ責任者は、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ること。

2 システム責任者は、不正プログラムから電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。以下この項において同じ。）を保護するため、アンチウイルスソフトウェアを導入する等の対策を実施すること。

3 システム責任者は、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アンチウイルスソフトウェア等により不正プログラム対策を実施すること。

1-2-3 （サービス不能攻撃対策）

システム責任者は、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電子計算機、情報ネットワーク機器又は通信回線を有する情報システム。）については、サービス提供に必要な電子計算機及び情報ネットワーク機器が装備している機能を

サービス不能攻撃対策に活用すること。

1-2-4 （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こと。

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こと。

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こと。ただし、モバイル PC 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こと。

1-2-5 （規定及び文書の整備）

システム責任者は、電子計算機のセキュリティ維持に関する規定を整備すること。

2 システム責任者は、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規定を整備すること。

3 システム責任者は、すべての電子計算機に対して、電子計算機を管理する利用者等を特定するための文書を整備すること。

4 システム責任者は、電子計算機関連文書を整備すること。

5 システム責任者は、通信回線及び情報ネットワーク機器関連文書を整備すること。

1-2-6 （主体認証と権限管理）

システム責任者は、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こと。

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

1-2-7 （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ソフトウェアを定めること。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙、または両者を併用することができる。

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、確保すること。

3 システム責任者は、要保護情報を取り扱うモバイルPCについては、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が有効に機能するように構成すること。

1－2－8 （サーバ装置の対策）

システム責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、暗号化

を行う必要性の有無を検討し、必要があると認めたときは、送受信される情報を暗号化すること。

2　システム責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めること。

3　システム責任者は、利用が定められたソフトウエアに該当しないサーバアプリケーションが稼動している場合には、当該サーバアプリケーションを停止すること。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能を無効化して稼動すること。

1－2－9 （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、通信回線を構築すること。

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、確保すること。

3 システム責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離すること。

4 システム責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って情報ネットワーク機器を利用しアクセス制御及び経路制御を行うこと。

5 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、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、必要があると認めたときは、情報を暗号化すること。

6 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、通信回線に利用する物理的な回線のセキュリティを検討し、選択すること。

7 システム責任者は、遠隔地から情報ネットワーク機器に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保すること。

8 システム責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。

9 システム責任者は、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こと。

1－2－10 （VPN、無線LAN、リモートアクセス）

システム責任者は、VPN 環境を構築する場合には、次の各号に掲げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。

一　利用開始及び利用停止時の申請手続の整備

二　通信内容の暗号化

三　通信を行う電子計算機の識別又は職員等の主体認証

四 主体認証記録の取得及び管理
五 VPN 経由でアクセスすることが可能な通信回線の範囲の制限
六 VPN 接続方法の機密性の確保
七 VPN を利用する電子計算機の管理

2 システム責任者は、無線LAN 環境を構築する場合には、次の各号に掲げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずること。
一 利用開始及び利用停止時の申請手続の整備
二 通信内容の暗号化
三 通信を行う電子計算機の識別又は職員等の主体認証
四 主体認証記録の取得及び管理
五 無線LAN 経由でアクセスすることが可能な通信回線の範囲の制限
六 無線LAN に接続中に他の通信回線との接続の禁止
七 無線LAN 接続方法の機密性の確保
八 無線 LAN に接続する電子計算機の管理

1－2－11 （上流ネットワークとの関係）

システム責任者は、研究所情報ネットワークを構築し運用するにあたっては、研究所情報ネットワークと接続される上流ネットワークとの整合性に留意すること。

第 2 節 運用時

1－2－12 （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の構成に変更があった場合には、セキュリティホール対策に必要となる機器情報を記載した書面を更新すること。

2 システム管理者は、管理対象となる電子計算機及び情報ネットワーク機器上で利用しているソフトウェアに関連する公開されたセキュリティホールに関連する情報を適宜入手すること。

3 システム責任者は、入手したセキュリティホールに関連する情報から、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を作成すること。
一 対策の必要性
二 対策方法
三 対策方法が存在しない場合の一時的な回避方法
四 対策方法又は回避方法が情報システムに与える影響
五 対策の実施予定
六 対策試験の必要性

七 対策試験の方法

八 対策試験の実施予定

4 システム管理者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。

5 システム管理者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者を含む事項を記録すること。

6 システム管理者は、信頼できる方法で対策用ファイルを入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

7 システム管理者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び情報ネットワーク機器が確認された場合の対処を行うこと。

1－2－13 （不正プログラム対策）

システム管理者は、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、特段の対処が必要な場合には、職員等にその対処の実施に関する指示を行うこと。

2 情報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、その見直しを行うこと。

1－2－14 （脆弱性診断）

システム責任者及びシステム管理者は、情報システムに関する脆弱性の診断を定期的に実施し、セキュリティの維持に努めること。

1－2－15 （規定及び文書の見直し、変更）

システム責任者は、適宜、電子計算機のセキュリティ維持に関する規定の見直しを行うこと。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こと。

2 システム責任者は、適宜、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規定の見直しを行うこと。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こと。

3 システム責任者は、電子計算機を管理する利用者等を変更した場合には、当該変更の内容を、電子計算機を管理する利用者等を特定するための文書へ反映すること。また、当該変更の記録を保存すること。

4 システム管理者は、電子計算機の構成を変更した場合には、当該変更の内容を電子計算機関連文書へ反映すること。また、当該変更の記録を保存すること。

5 システム管理者は、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には、当該変更の内容を通信回線及び情報ネットワーク機器関連文書へ反映すること。また、当該変更の記録を保存すること。

1－2－16 （運用管理）

システム管理者は、電子計算機のセキュリティ維持に関する規定等に基づいて、電子計算機の運用管理を行うこと。

2 システム管理者は、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のため、関連規定に基づいて、日常的及び定期的に運用管理を実施すること。

1－2－17 （接続の管理）

情報セキュリティ責任者は、情報ネットワークに関する接続の申請を受けた場合は、研究所コンピュータ・ネットワーク基準に従い、申請者に対して接続の諾否を通知し必要な指示を行うこと。

1－2－18 （資源の管理）

システム責任者は、電子計算機の CPU 資源、ディスク資源並びに情報ネットワーク帯域資源等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こと。

1－2－19 （ネットワーク情報の管理）

システム責任者は、研究所情報ネットワークで使用するドメイン名やIPアドレス等のネットワーク情報について、利用者等からの利用形態に応じて適切に分配し管理すること。

1－2－20 （サーバ装置の対策）

システム責任者は、定期的にサーバ装置の構成の変更を確認すること。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対応すること。

2 システム管理者は、要安定情報を取り扱うサーバ装置に保存されている情報について、定期的にバックアップを取得すること。また、取得した情報を記録した媒体は、安全に管理すること。

3 システム管理者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期すること。

第 3 節 運用終了時

1－2－21 （電子計算機の対策）

システム責任者は、電子計算機の運用を終了する場合に、データ消去ソフトウェアもしくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊等の方法を用いて、すべての情報を復元が困難な状態にすること。

1－2－22 （情報ネットワーク機器の対策）

システム責任者は、情報ネットワーク機器の利用を終了する場合には、情報ネットワーク機器の内蔵記録媒体のすべての情報を復元が困難な状態にすること。

第 4 節　情報システムの構築と運用

1－2－23 （情報システムの計画・設計）

システム責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を、所長に求めること。

2 システム責任者は、情報システムのセキュリティ要件を決定すること。

3 システム責任者は、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。

4 システム責任者は、構築した情報システムを運用するに当たって、情報セキュリティの観点から実施する手順及び運用環境を定めること。

1－2－24 （情報システムの構築・運用・監視）

システム責任者は、情報システムの構築、運用及び監視に際しては、必要に応じて情報セキュリティ対策を行うこと。

1－2－25 （情報システムの移行・廃棄）

システム責任者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存、並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置をとること。

1－2－26 （情報システムの見直し）

システム責任者は、情報システムの情報セキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。

第 3 章　情報の格付けと取扱い

1－3－1 （情報の作成又は入手）

教職員等は、情報システムに係る情報を作成し又は入手する場合は、研究所の研究教育事務の遂行の目的に十分留意すること。

1－3－2 （情報の作成又は入手時における格付けの決定と取扱制限の検討）

教職員等は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

2 教職員等は、研究所外の者が作成した情報を入手し、管理を開始する時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。

1－3－3 （格付けと取扱制限の明示）

教職員等は、情報の格付けを、当該情報の参照が許されている者が認識できる方法を用いて明示し、必要に応じて取扱制限についても明示すること。

1－3－4 （格付けと取扱制限の継承）

教職員等は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること。

1－3－5 （格付けと取扱制限の変更）

教職員等は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと。

2 教職員等は、情報の取扱制限を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定すること。

1－3－6 （格付けに応じた情報の保存）

システム責任者は、電子計算機に保存された要保護情報について、適切なアクセス制御を行うこと。

2 システム責任者は、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複写の保管について、災害等への対策の必要性を検討し、必要があると認めたときは、同時被災等しないための適切な措置を講ずること。

第 4 章　主体認証

1－4－1 （主体認証機能の導入）

　システム責任者は、すべての情報システムについて、主体認証を行う必要性の有無を検討すること。

2 システム責任者は、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、識別及び主体認証を行う機能を設けること。

3 システム管理者は、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、主体認証情報を秘密にする必要がある場合には、当該主体認証情報が明らかにならないように管理すること。

4 システム責任者は、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、利用者等に対して定期的な変更を促す機能を設けること。

5 システム責任者は、生体情報による主体認証方式を用いる場合には、当該生体情報を本人から事前に同意を得た目的以外の目的で使用しないこと。また、当該生体情報について、本人のプライバシーを侵害しないように留意すること。

6 システム責任者は、セキュリティ侵害又はその可能性が認められる場合、主体認証情報の変更を求め又はアカウントを失効させることができる。

第 5 章　アクセス制御

1－5－1 （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こと。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、アクセス制御を行う必要があると判断すること。

2 システム責任者は、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こと。

1－5－2 （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こと。

2 利用者等は、情報システムに装備された機能を用いて、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って、必要なアクセス制御の設定をすること。

1－5－3 （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こと。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こと。

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こと。

第 6 章 アカウント管理

1－6－1 （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と。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こと。

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機能を設けること。

1－6－2 （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こと。

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こと。

1－6－3 （共用アカウント）

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、共用アカウントの利用許可については、情報システムごとにその必要性を判断すること。

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、アカウントを発行する際に、それが共用アカウントか、共用ではないアカウントかの区別を利用者等に通知すること。

1－6－4 （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こと。

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、アカウントを発行すること。

3 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、管理者権限を持つアカウントを、業務又は業務上の責務に即した場合に限定して付与すること。

4 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、業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス制御に係る設定をすること。

1－6－5 （管理者権限を持つアカウントの利用）

管理者権限を持つアカウントを付与された者は、管理者としての業務遂行時に限定して、当該アカウントを利用すること。

第 7 章 証跡管理

1－7－1 （証跡管理機能の導入）

システム責任者は、すべての情報システムについて、証跡管理を行う必要性の有無を検討すること。

2 システム責任者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けること。

3 システム責任者は、証跡を取得する必要があると認めた情報システムにおいては、事象を証跡として記録するに当たり、事象ごとに必要な情報項目を記録するように情報システムの設定をすること。

4 システム責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方針を整備し、必要に応じ、これらの場合に対応するための機能を情報システムに設けること。

5 システム責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行い、外部記録媒体等その他の装置・媒体に記録した証跡についてはこれを適正に管理すること。

1－7－2 （システム管理者による証跡の取得と保存）

システム管理者は、証跡を取得する必要があると認めた情報システムにおいては、システム責任者が情報システムに設けた機能を利用して、証跡を記録すること。

2 システム管理者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡の保存期間を定め、当該保存期間が満了する日まで証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。

3 システム管理者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が

取得できない場合又は取得できなくなるおそれがある場合は、定められた対処を行うこと。

1－7－3 （証跡管理に関する利用者等への周知）

情報セキュリティ責任者又はシステム責任者は、証跡を取得する必要があると認めた情報システムにおいては、システム管理者及び利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明すること。

1－7－4 （通信の監視）

利用者等によるネットワークを通じて行われる通信の傍受を禁止すること。ただし、情報セキュリティ責任者は、セキュリティ確保のため、あらかじめ指定した者に、ネットワークを通じて行われる通信の監視（以下「監視」という。）を行わせることができる。

2 情報セキュリティ責任者は、監視の範囲をあらかじめ具体的に定めておかなければならない。ただし、不正アクセス行為又はこれに類する重大なセキュリティ侵害に対処するために特に必要と認められる場合、情報セキュリティ責任者は、セキュリティ侵害の緊急性、内容及び程度に応じて、対処のために不可欠と認められる情報について、監視を行うよう命ずることができる。

3 監視を行う者は、監視によって知った通信の内容又は個人情報を、他の者に伝達してはならない。ただし、前項ただし書きに定める情報については、情報セキュリティ責任者及び電子計算機委員会に伝達することができる。

4 監視を行わせる者は、監視を行う者に対して、監視記録を保存する期間をあらかじめ指示するものとする。監視を行う者は、指示された期間を経過した監視記録を直ちに破棄しなければならない。ただし、監視記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。

5 監視を行う者及び監視記録の伝達を受けた者は、ネットワーク運用・管理のために必要な限りで、これを閲覧し、かつ、保存することができる。監視を行う者及び監視記録の伝達を受けた者は、監視記録を不必要に閲覧してはならない。不必要となった監視記録は、直ちに破棄しなければならない。監視記録の内容を、法令に基づく場合等を除き、他の者に伝達してはならない。

1－7－5 （利用記録）

複数の者が利用する情報機器の管理者は、当該機器に係る利用記録（以下「利用記録」という。）をあらかじめ定めた目的の範囲でのみ採取することができる。当該目的との関連で必要性の認められない利用記録を採取することはできない。

2 前項に規定する目的は、法令の遵守、情報セキュリティの確保、課金その他当該情報機器の利用に必要なものに限られる。個人情報の取得を目的とすることはできない。

3 当該情報機器の管理者は、第 1 項の目的のために必要な限りで、利用記録を閲覧することができる。他人の個人情報及び通信内容を不必要に閲覧してはならない。

4 当該情報機器の管理者は、第 2 項に規定する目的のために必要な限りで、利用記録を他の者に伝達することができる。
5 第 1 項の規定により情報機器の利用を記録しようとする者は、第 2 項の目的、これによって採取しようとする利用記録の範囲及び前項により利用記録を伝達する者を、あらかじめ情報セキュリティ責任者に申告し、かつ、当該機器の利用者等に開示しなければならない。情報セキュリティ責任者は、申告の内容を不適切と認めるときは、これを修正させるものとする。
6 当該情報機器の管理者又は利用記録の伝達を受けた者は、第 1 項の目的のために必要な限りで、これを保有することができる。不要となった利用記録は、直ちに破棄しなければならない。ただし、当該情報機器の管理者は、利用記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。

1－7－6 （個人情報の取得と管理）

電子的に個人情報の提供を求める場合は、提供を求める情報の範囲、利用の目的、その情報が伝達される範囲を、あらかじめ相手方に示さなければならない。
2 前項の個人情報は、当人の請求により開示、訂正又は削除をしなければならない。また、そのための手続を示さなければならない。

1－7－7 （利用者等が保有する情報の保護）

利用者等が保有する情報は、ネットワーク運用に不可欠な範囲又はインシデント対応に不可欠な範囲において、閲覧、複製又は提供することができる。

第 8 章 暗号と電子署名

1－8－1 （暗号化機能及び電子署名の付与機能の導入）

システム責任者は、要機密情報（書面を除く。以下この項において同じ。）を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討すること。
2 システム責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けること。
3 システム責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与を行う機能を付加する必要性の有無を検討すること。
4 システム責任者は、電子署名の付与を行う必要があると認めた情報システムには、電子署名の付与を行う機能を設けること。
5 システム責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性につい

て検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リスト又は、研究所における検証済み暗号リストがあればその中から選択すること。なお、複数のアルゴリズムを選択可能な構造となっている場合には、少なくとも一つをそれらのリストの中から選択すること。

1－8－2 （暗号化及び電子署名の付与に係る管理）

システム責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、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、鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対応手順等を定めること。

2 システム責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、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、鍵の保存媒体及び保存場所を定めること。

3 システム責任者は、電子署名の付与を行う必要があると認めた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提供すること。

第 9 章 違反と例外措置

1－9－1 （違反への対応）

このガイドラインの規定に反する違反への対応については、ポリシー第15条に基づき行うものとする。

1－9－2 （例外措置）

このガイドラインの規定に対する例外措置については、ポリシー第16条に基づき行うものとする。

第 10章 インシデント対応

1－10－1 （インシデントの発生に備えた事前準備）

インシデントの発生に備えた事前準備については、ポリシー第18条第1項から第4項に基づき行うものとする。

1－10－2 （インシデントの原因調査と再発防止策）

インシデントの原因調査と再発防止策については、ポリシー第 18 条第 5 項から第 8 項に基づき行うものとする。

第 11 章　所外の情報セキュリティ水準の低下を招く行為の禁止

1－11－1 （所外の情報セキュリティ水準の低下を招く行為の防止）

情報セキュリティ責任者は、所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措置についての規定を整備すること。

第 12 章　教育・研修

1－12－1 （情報セキュリティ対策の教育）

情報セキュリティ対策の教育については、ポリシー第17条に基づき行うものとする。

第 13 章　評価

1－13－1 （自己点検に関する年度計画の策定）

自己点検に関する年度計画の策定については、ポリシー第20条第1項に基づき行うものとする。

1－13－2 （自己点検の実施に関する準備及び実施）

自己点検の実施に関する準備及び実施については、ポリシー第20条第2項に基づき行うものとする。

1－13－3 （自己点検結果の評価）

自己点検結果の評価については、ポリシー第 20条第 4 項に基づき行うものとする。

1－13－4 （自己点検に基づく改善）

自己点検に基づく改善についてはポリシー第 20条第 3 項及び第 4 項に定められた規定に基づき行うものとする。

1－13－5 （監査）

監査については、ポリシー第 21 条に基づき行うものとする。

第 2 部　情報システム障害等管理実施手順

第 2 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講じることを定めることを目的とする。

第 1 章　情報システム非常時行動計画

2－1－1 （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。

2－1－2 （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し、非常時対策本部の設置を提案する。

2－1－3 （非常時対策本部）

情報セキュリティ責任者は、非常事態が発生しまたは発生するおそれが特に高いと認められる場合に、被害の拡大防止、被害からの早急な復旧その他非常事態の対策等を実施するために非常時対策本部を設置する。

2　非常時対策本部は次の各号に定める委員をもって構成する。

一　情報セキュリティ責任者

二　システム責任者

三　システム管理者

3　情報セキュリティ責任者は、非常時対策本部の本部長となる。

4　情報セキュリティ責任者が必要と認めたときは、委員以外の者を出席させて意見を聞くことができる。

2－1－4 （非常時連絡網）

非常時対策本部には、緊急連絡及び情報共有等を行うために非常時連絡窓口を設置し、

関係者に周知徹底する。

2 非常時連絡窓口は、非常時対策本部長の指示に基づき、通報者や捜査当局、クレームの相手方、報道関係者等、外部との対応を直接または広報窓口を通じて行う。

3 非常時連絡窓口は、非常時対策本部長の指示に基づき、所内関係者からの情報の受付および収集、被害拡大防止や復旧のための緊急対策等の伝達を直接行う。

4 情報セキュリティ責任者は、非常時連絡窓口を中心とする非常時連絡網を整備する。

5 非常時連絡網の連絡先には、非常時対策本部委員の他、必要に応じて法律専門家、広報部門を設定する。

2－1－5 （インシデント対応手順）

具体的なインシデント対応は、別途定める「インシデント対応手順」に基づき対処する。

2 非常事態においては、非常時対策本部の指示がインシデント対応手順に優先する。

2－1－6 （再発防止策の検討）

情報セキュリティ責任者は、非常事態への対応が終了した場合、再発防止策を策定し、最高情報セキュリティ責任者への報告書の提出をもって、非常時対策本部を解散する。

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たものである。

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 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
④ 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
⑤ 利用規程により禁止されている形態での P2P ソフトウェアの利用
⑥ 禁止された方法による所外接続
⑦ 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

（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

本文書第 3 部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、公表するものとする。
Email: lan-info@nig.ac.jp （仮）

（3） 所外への連絡・通報、対外クレームに当たっては、所外窓口及び関係部署との連絡を密にし、無断で行わないものとする。

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ものとする。

（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ものとする。

（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ものとする。
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し、対策結果を情報セキュリティ責任者に報告するものとする。
ii） ｉ）以外の場合、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状況報告をし、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ものとする。
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を通じて最高情報セキュリティ責任者に報告をし、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ものとする。

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最高情報セキュリティ責任者に結果報告をするものとする。

（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に報告し、指示を受けることとする。

（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、所外クレーム対応プロセスを併せて実施するものとする。

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ものとする。

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ものとする。

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) 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に報告する。
② 情報セキュリティ責任者は、被害拡大防止措置が所内ネットワークに影響が及ぶと判断する時は所内窓口（情報基盤ユニットに指示して、緊急措置の実施により影響を受ける利用者等へ連絡するとともに、必要に応じ非常時対策本部を組織する。
③ 所外窓口は、情報セキュリティ責任者又は非常時対策本部の指示に基づき、関係するネットワークへの連絡、外部広報などを行う。
④ 非常時対策本部が設置された場合、システム責任者及びシステム管理者及び利用者等は、その指示に従うものとする。

(4) 復旧計画
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。

(5) 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ものとする。

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、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させるものとする。

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に報告する。

② 情報セキュリティ責任者は、被害拡大防止措置が所内ネットワークに影響する場合は、所内窓口(情報基盤ユニットに指示して、緊急措置の実施により影響を受ける利用者等に被害拡大防止措置を連絡するとともに、必要に応じ非常時対策本部を組織する。

③ 所外窓口は、情報セキュリティ責任者または非常時対策本部の指示に基づき、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 への連絡等を指揮する。

④ 非常時対策本部が設置された場合、システム責任者、システム管理者及び利用者等は、その指示に従うものとする。

(4) 復旧計画

① システム管理者もしくは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 システム管理者もしくは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ものとする。

(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ものとする。

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に報告する。

③ 所外クレームについての報告を受けた情報セキュリティ責任者は、必要に応じ非常時対策本部を設置する。

④ 情報セキュリティ責任者または非常時対策本部は、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 への連絡等を指揮し、システム責任者、システム管理者及び利用者等は、その指示に従うものとする。

(2) 利用者等のコンテンツの違法性を主張した送信中止・削除の要求

① 発信元利用者等の特定所外クレームが利用者等により不特定多数宛てに情報発信されたコンテンツの違法性及び情報発信による権利侵害を主張してコンテンツの送信中止や削除の要求が被害を主張する者またはその代理人からなされたものである場合、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、発信元職員等を特定する。

②（通常手続き）コンテンツを発信した職員等への通知と削除

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 条第 2 項第 2 号に基づき職員等に請求があった旨通知し、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ものとする。

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ものとする。

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疑いもなく明らかと判断できる場合、一旦利用者等のコンテンツの送信を保留し、その旨を利用者等に伝えるものとする。有効な反論があればコンテンツ送信を復活するものとする。

ⅱ） 本手続きの対象は、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、緊急な救済の必要性がある場合のみとする。

ⅲ） 本緊急手続が適用されることもあることを具体的に利用規程として明示する等、利用者等に周知するものとする。

（3） 職員等の発信したコンテンツの刑事的違法性の指摘及び送信中止・削除の要求

① 利用者等の発信したコンテンツが刑事法上違法な可能性の高い旨を指摘された場合で、名誉毀損や、著作権侵害等、被害者が存在する犯罪については、前号と同様の手順を取るものとする。

② わいせつ物陳列罪等、被害者のいない犯罪が外部クレームにより指摘された場合、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、発信元利用者等を特定する。

③ 発信元利用者等に犯罪であるとする指摘があった旨通知し、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。

（4） 利用者等の行為（コンテンツ以外）の違法性を主張した送信中止・アカウント削除等の要求

①（通常の対応）通信を発信した利用者等への通知とアカウント停止

ⅰ） 所外クレームが利用者等による１対１の情報発信による権利侵害等による被害を主張して情報発信の中止を要求するものである場合、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、発信元利用者等を特定する。

ⅱ） システム管理者もしくは情報基盤ユニットは、事実確認を行い、特定できた利用者等に対し、問題の通信の発信を中止するよう通知する。これには、同様の通知を再度行った場合には、関連するアカウントを停止する旨を警告する事を含む。

ⅲ） 利用者等から有効な反証があれば、関連する一時停止を解除する。

ⅳ） 念書を取るなどに対応の後、アカウントの復活手続きを行う。

ⅴ） 同様の手順を経て再発が確認できた場合には、本機構の処罰の手順に移行する。

②（セキュリティインシデント対応）利用者等のアカウントの一時停止

ⅰ） 所外クレームが職員等による一対一の情報発信によるセキュリティインシデントによる被害を主張して情報発信の中止を要求するものである場合、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、発信元利用者等を特定する。

ⅱ） システム管理者もしくは情報基盤ユニットは、利用者等の行為がセキュリティインシデントの原因であると判断するのに十分な理由がある場合には、システム責任者に報告し、その判断を求めるものとする。

ⅲ） システム管理者もしくは情報基盤ユニットからの報告を受けたシステム責任者は、必要な場合、利用者等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。

ⅳ） 請求者が連絡を要求しているときには、一時停止した旨を連絡する。

ⅴ） アカウントを一時停止した旨を利用者等に通知するとともに、再度行った場合には、関連するアカウントを停止する旨を警告する。

ⅵ） 利用者等から有効な反論があった場合は、関連するアカウントの一時停止を解除する。

ⅶ） 念書をとるなどの対応の後、アカウントの復活手続きを行う。

ⅷ） 同様の手順を経て再発が確認できた場合には、本機構の処罰の手順に移行すする。

（5） 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の上、対応するものとする。

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。

（6） 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開示請求があった場合であって、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ものとし、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ものとする。

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ものとする。

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ものとする。

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ものとする。

ⅴ） 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すれば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ので、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。

（7） 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、下記の手順をとるものとする。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。

（8） 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ものとする。

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ものとする。

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ものとする。

(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、情報公開等委員会への報告をすることができる。また、情報公開等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、情報セキュリティの確保と円滑な情報システムの利用に資することを目的とする。

総則

3-1-1 （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。

3-1-2 （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。

3-1-3 （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。

3-1-4 （アカウントの申請）

研究所情報システムを利用する者は、別に定めるメイルアカウント申請（仮称）、スーパーコンピュータ利用に関する申請（仮称）等を情報基盤ユニットに提出し、所長からアカウントの交付を得なければならない。

3-1-5 （アカウントの管理）

利用者は、アカウントの管理に際して次の各号を遵守しなければならない。

一　利用者は、自分のアカウントを他の者に使用させたり、他の者のアカウントを使用してはならない。

二　利用者は、他の者の主体認証情報を聞き出したり使用したりしてはならない。

三　利用者は、パスワードを「利用者パスワードガイドライン」に基づいて適切に管理しなければならない。

四　利用者は、使用中のコンピュータをロック又はログオフせずに長時間自らの席を離れてはならない。

五 利用者は、所外のインターネットカフェなどに設置されているような不特定多数の人が操作（利用）可能な端末を用いての研究所内の情報システムへのアクセスを行ってはならない。

六 利用者は、アカウントを他者に使用されまたはその危険が発生した場合には、直ちに責任者（課室等責任者および情報基盤ユニットもしくはシステム責任者）に報告しなければならない。

七 利用者は、研究所情報システムを利用する必要がなくなった場合は、別に定める中止・終了届により遅滞なく所長に届け出なければならない。

3-1-6 （自己点検の実施）

利用者は、研究所自己点検基準に基づいて自己点検を実施しなければならない。

3-1-7 （情報の格付け）

教職員等は、「第１部　情報システム運用・管理実施手順」に従い、情報の格付け及び取扱いを行わなければならない。

3-1-8 （禁止事項）

利用者は、情報システムについて、次の各号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 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

十一 過度な負荷等により円滑な情報システムの運用を妨げる行為

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

十三 上記の行為を助長する行為

十四 システム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

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。

3-1-9 （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、次の各号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

3-1-10 （PC の利用）

利用者は、PC の利用にあたっては、別途定める「パーソナルコンピュータ取扱ガイドライン」に従い、これらの情報及び端末の適切な保護に注意しなければならない。

3-1-11 （電子メールの利用）

利用者は、電子メールの利用にあたっては、別途定める「電子メール利用ガイドライン」及び「所外情報セキュリティ水準低下防止ガイドライン」に従い、規則の遵守のみならずマナーにも配慮しなければならない。

3-1-12 （ウェブの利用及び公開）

利用者は、ウェブブラウザを利用したウェブサイトの閲覧、情報の送信、ファイルのダウンロード等を行う際には、別途定める「ウェブブラウザ利用ガイドライン」及び「所外情報セキュリティ水準低下防止ガイドライン」に従い、不正プログラムの感染、情報の漏えい、誤った相手への情報の送信等の脅威に注意するとともに、私的目的でのウェブの閲覧、掲示板への無断書き込みその他業務効率の低下や研究所の社会的信用を失わせることのないよう注意しなければならない。

2 利用者は、ウェブページの公開にあたって、「ウェブ公開ガイドライン」及び「所外情報セキュリティ水準低下防止ガイドライン」に従い、セキュリティや著作権等の問題及び研究所の

社会的信用を失わせることのないように注意しなければならない。

3 利用者は、研究室等で研究所外からアクセス可能なウェブサーバ等を運用しようとする場合は、事前に研究所コンピュータ・ネットワーク利用基準に従い、情報基盤ユニットに申請し許可を得るとともに、情報セキュリティに充分留意してサーバの運用をしなければならない。

4 ウェブページ及びウェブサーバ運用に関して、本文書及びガイドラインに違反する行為が認められた場合には、電子計算機委員会は、公開の許可の取り消しやウェブコンテンツの削除を行うことがある。

3-1-13 （モバイル PC の利用）

利用者は、モバイル PC その他の情報システムの所外での利用にあたっては、以下の手順を遵守しなければならない。

一 要保護情報及び要安定情報を記録したモバイル PC 等の情報システムを課室等情報セキュリティ責任者（以下「課室等責任者」という。）の許可なく所外に持ち出してはならない。業務上の必要性からこれらの情報を所外に持ち出すには、保護レベルに応じた管理（暗号化、パスワード保護、作業中の覗き見防止等）が必要である。

二 モバイル PC は可能な限り強固な認証システムを備え、ログ機能を持っていなければならない。また、それらの機能が設定され動作していなければならない。アンチウィルスソフトウェアが提供されているシステムでは、その機能が最新の状態でシステムを保護可能でなければならない。

三 モバイル PC の画面を他者から見える状態で利用してはならない。また、当該システムを他者が支配もしくは操作可能な状態にしてはならない（不正操作、情報漏えい及び盗難防止等）。

四 モバイル PC を研究所情報システムに再接続する場合は、接続に先だってアンチウィルスソフトウェア等でスキャンを実行し、問題のあるソフトウェアが検出されないことを確認しなければならない。

五 モバイル PC 等の情報システムの紛失及び盗難があった場合は、速やかに情報セキュリティ責任者に報告しなければならない。

3-1-14 （所外からの利用及び持ち込み）

利用者は、所外の情報システムからの研究所情報システムの利用及び所外の情報システムの研究所内の持ち込みにおいて、次の各号に掲げる手順を遵守しなければならない。

一 利用者は、所外の情報システムを用いて非公開の研究所情報システムへアクセスし、あるいは所外の情報システムを持ち込んで研究所情報システムへ接続する場合、事前にシステム責任者の許可を得なければならない。

二 前項により許可を得た所外の情報システムは可能な限り強固な認証システムを備え、ログ機能を持っていなければならない。また、それらの機能が設定され動作していなけ

ればならない。アンチウィルスソフトウェアが提供されているシステムでは、その機能が最新の状態であって、システムを保護可能な状態でなければならない。

三　利用者は、これらの情報システムを許可された者以外に利用させてはならない。また、当該システムを他者が支配もしくは操作可能な状態にしてはならない。

四　課室等責任者の許可なく、所外の情報システムに要保護情報及び要安定情報を複製保持してはならない。

3-1-15 （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を導入しないように注意しなければならない。

一　アンチウィルスソフトウェア等により不正プログラムとして検知される実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。

二　アンチウィルスソフトウェア等にかかわ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こと。

三　アンチウィルス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こと。

四　アンチウィルスソフトウェア等により定期的にすべての電子ファイルに対して、不正プログラムの有無を確認すること。

五　外部からデータやソフトウェアを電子計算機等に取り込む場合また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こと。

六　ソフトウェアのセキュリティ機能を活用し、不正プログラム感染の予防に努めること。

2　利用者は、研究所情報ネットワーク及びシステムの利用に際して、インシデントを発見したときは、インシデント対応手順に基づいて行動するものとする。

3-1-16 （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。

パーソナルコンピュータ取扱ガイドライン

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)で利用されるパーソナルコンピュータ(以下、PC)の適切な利用手順に関して述べる。

2. （セキュリティの維持）

利用者等は、自らが管理するPCについて下記の事項を遵守しなければならない。

一 情報基盤ユニットが設定した PC のウイルス対策ソフトの変更をしないこと。

二 利用している OS 及びアプリケーションの脆弱性情報をはじめとする情報に留意し、ソフトウェアの不具合を迅速に修正すること。

三 ウイルス対策ソフトウェアをインストールするとともに、ウイルス情報データベースを常に最新に保っておくこと。

3.（アプリケーションソフトの利用）

利用者等がアプリケーションをインストール、利用する際には、以下の各号を遵守しなければならない。

一 研究・教育及び事務に関する目的及びそれらを支援する目的に合致しないアプリケーションをインストール、使用してはならない。

二 インストール、使用しようとするアプリケーションの利用条件に従って利用すること。

三 アプリケーションをインストールする前に、ウイルスチェックソフトウェア等により、ウイルスやスパイウェア等、有害ソフトウェアが含まれていないことを確認すること。

四 出所の定かでないソフトウェアをインストール、使用しないこと。

五 P2P（ファイル交換ソフトウェア）をインストールしてはならない。

六 その他、ポリシー、研究所情報セキュリティガイドライン及びその他の規定等に反するアプリケーションをインストール、利用してはならない。

4.（PCの管理）

利用者等は、自らが管理するPCに関して、下記の各号に掲げる事項を遵守すること。

一 当該PCを認証なしで利用できるようにしてはならない。

二 ネットワークを経由して、不特定多数の第三者がPCにアクセスできないようにすること。

三 当該PCにアカウントを有さない者にPCを使用させないこと。ただし、教育・研究上必要な場合など、管理者が特に認める場合を除く。

四 PCを廃棄、あるいは譲渡する場合は、内部ハードディスクや不揮発性メモリに、要管理

情報やその他重要な情報が残留することのないように、専用ツールを用いて完全に消去するか、物理的に破壊すること。また、その作業が完了したことを課室等責任者に報告すること。

5. （所外からのアクセス）

利用者等は、自らが管理するPCに関して、所外のネットワークからアクセスできるようにする場合は、次の各号に掲げる事項を遵守すること。

一 アクセスに使用するポート番号、VPN ソフトウェア名等を情報基盤ユニットに届け出ること。

二 通信内容は全て暗号化されるようにすること。

三 パスワードのみ（ワンタイムパスワードを除く）による認証方式は原則として避けること。パスワードによる認証を用いる場合は、パスワードの選定に関して十分な注意を行うこと。

四 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こと。

五 研究所が提供するネットワーク以外の方法（電話回線など）でアクセスできるようにしてはならない。

6. （モバイル PC 等の所外への携行）

モバイル PC 等の情報機器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。

一 情報機器を所外へ携行する際は下記に掲げる情報セキュリティ対策を行うこと。

ⅰ） モバイル PC 等

1） ログインパスワードの設定を行うこと。また、サスペンド及び休止状態からの復帰時にはパスワード入力を行う設定とすること。

2） 一定時間使用しない状態が継続したら自動ロックする設定を行うこと。また、使用しないときはロックすること。

3） 用務に必要のない要保護情報（個人情報を含む）を格納しないこと。また、できる限り要保護情報を格納したことのないものとすること。

4） 用務の都合でやむを得ず要保護情報を格納するときは暗号化を行うこと。

5） 研究所の情報システムへアクセスするための設定については、次のような不正アクセス防止対策を行うこと。

・パスワードは保存せずに、接続の都度入力するようにすること（Web メールでのアクセスを行う場合も同様）。

・公開鍵認証を用いる場合は、パスフレーズを設定すること。

ⅱ） メモリデバイス（SD カード、USB メモリなど）

1） 用務に必要のない要保護情報（個人情報を含む）を格納しないこと。また、携行す

る機器は、できる限り要保護情報を格納したことのないものとすること。

2） 用務の都合でやむを得ず要保護情報を格納するときは暗号化を行うこと。

ⅲ） 情報機器を紛失した場合は下記に掲げる対処を行うこと。

1)研究所への連絡

直ちに情報基盤ユニットに連絡を取り指示に従うこと。

2)研究所への不正アクセス防止対策

直ちにパスワードの変更、公開鍵の削除（SSH の場合）等を行うとともに、アクセスログ等により不正アクセスがなかったことを確認すること。もし不正アクセスの可能性が発見された場合は、安全が確認されるまで当該サーバをネットワークから遮断する等の処置を行うこと。なお、出張中等のために直ちにこれらの対策が実施できない場合は、情報基盤ユニットに相談すること。

7．（監査の実施）

利用者等が管理する PC 端末に関して、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のための手順を提供する。

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を利用する利用者を対象とする。

3.（電子メールソフトの設定）

3.1 電子メール受信に係る設定

(1) 利用者は、受信した電子メールをテキスト（リッチテキストを含む。）として表示することとし、偽のホームページへの誘導や不正なスクリプトの実行を未然に防ぐ目的から HTML メールの利用は避けること。

(2) 利用者は、アンチウイルスソフトウェアに加えて、電子メールソフトウェア側においてもウイルス対策が設定可能であれば、これを実施すること。

3.2 電子メール送信に係る設定

(1) 利用者は、原則として、HTML 形式の電子メールを送信しないこと。これは、当方より HTML 形式の電子メールを送信した場合、それを受信した側のセキュリティ水準の低下を招く恐れがあるからである。

4. （電子メールに係る全般的な注意事項）

4.1 電子メールの私的利用の禁止

(1) 利用者は、電子メールシステムを、教育・研究活動を遂行する上で必要な場合のみ使用することとし、私的目的のために使用しないこと。

4.2 電子メールの自動転送の禁止

(1) 利用者は、教育・研究活動を遂行する上で必要な場合を除き要保護情報を含む電子メールを研究所外へ自動転送することを禁止する。電子メールを研究所外へ自動転送する

必要がある場合には、メール転送先・理由・期間・セキュリティ対策などを明確にした上で事前に課室等情報セキュリティ責任者の了解を得ること。

(2) 利用者は、電子メールを研究所外へ自動転送する必要性がなくなった場合には、その旨を課室等情報セキュリティ責任者に報告すること。

4.3 研究所が整備した電子メールシステム以外の情報システム利用の禁止

(1) 利用者は、学習・教育・研究活動遂行にかかわる情報を含む電子メールを送受信する場合には、研究所が整備した電子メールシステムを利用することを原則とする。

(2) 利用者は、研究所が整備した電子メールシステム以外の情報システム(個人所有の電子メールアドレス等)を用いて電子メールを送受信する場合には、セキュリティ対策ソフトを導入するなど安全管理措置を講ずること。

4.4 電子メールの監視

(1) 電子メールシステムの適正な利用のため、その利用状況(あて先、内容、添付ファイル等)について証跡の取得、保存、点検及び分析が行われる可能性がある。利用者は、その趣旨を理解の上、電子メールの内容に関するモニタリング及び監査を実施していることを認識すること。

4.5 電子メール ID 及び電子メールアドレスの管理

(1) 利用者は、他人の電子メール ID (電子メールサーバへのログイン ID。以下同じ。) 及び電子メールアドレスを使用しないこと。

(2) 利用者は、電子メール ID 及び電子メールアドレスを他人と共用しないこと。ただし、特定のサービス、職位、部門単位に付与される電子メール ID 及び電子メールアドレスのように、複数の関係者で共用するあるいは担当者が引き継いで使用する必要がある場合には、利用者はその許可及び設定について情報基盤ユニットに相談すること。

(3) 利用者は、自己に付与された電子メール ID を、それを知る必要のない者に知られるような状態で放置しないこと。

(4) 利用者は、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。

4.6 ニュースグループ、メーリングリスト等の発信機関への電子メールアドレス登録の制限

(1) 利用者は、ニュースグループ、メーリングリスト等 (メールマガジン、Web マガジン、フリーメール)への電子メールアドレス登録は、情報セキュリティ情報のメール配信サービスなど、教育・研究活動上必要なものに限定すること。

5. (電子メールパスワードの管理)

(1) 利用者はパスワードを設定すること。
(2) 利用者は、パスワードの管理にあたっては「利用者パスワードガイドライン」に従うこと。
(3) 利用者は、パスワードを電子メールソフトに永続的に保存しないこと。ただし、電子メールの受信のたびにパスワード入力を行うことが過度に煩雑である場合には、電子メールソフトに一時保存し、クライアント PC 起動後のみパスワード入力とする仕組みを利用してもよい。
(4) 利用者は、パスワードを電子メールソフトに一時保存する場合には、当該パスワードを一時保存するクライアント PC を「主体認証情報格納装置」とみなして、以下の点に配慮して安全に取り扱うこと。
・パスワードを保存したクライアント PC を本人が意図せずに使用されることのないように安全措置を講じること。
・パスワードを保存したクライアント PC を他者に付与及び貸与しないこと。
・パスワードを保存したクライアント PC を紛失しないように管理すること。紛失した場合には、直ちにシステム管理者にその旨を報告すること。

6. （電子メールの受信）

6.1 電子メールの受信確認

(1) 利用者は、定期的に、電子メールの受信確認を行うこと。

6.2 電子メール添付ファイルのウイルスチェック

(1) 利用者は、アンチウイルスソフトウェアによる自動ウイルスチェックを実施すること。
(2)利用者は、受信した電子メールの添付ファイルに対して、随時、ウイルスチェックを行うこと。これは、新種のウイルスに対応したパターンファイルの提供が間に合わず、ファイル受信時のウイルスチェックにおいてウイルスが発見されなかった場合を考慮し、最新のパターンファイルを用いて過去に受信した電子メールの添付ファイルに対してもウイルスの有無を確認するための対策である。
(3) 利用者は、緊急時対応が必要な時には、システム管理者または情報基盤ユニットからの指示に従うこと。

6.3 あて先間違いの電子メールを受信したときの対処

(1) 利用者は、あて先間違いの電子メールを受信し、送信者から正しい受信者へ再度送信する必要がある場合には、可能な範囲で送信者へあて先が間違っていたことを通知すること。
(2)利用者は、あて先間違いの電子メールを受信した場合には、これを削除すること。

6.4 不審な電子メールを受信したときの対処

(1) 利用者は、不審な電子メールを受信した場合には、電子メールを開かず、必要に応じて情報基盤ユニットに連絡・相談し、指示を仰ぐこと。

(2) 利用者は、電子メールに不審なファイルが添付されていた場合には、当該ファイルを開くことなく必要に応じて情報基盤ユニットに連絡・相談し、指示を仰ぐこと。

6.5 ウイルスに感染したときの対処

(1) 利用者は、クライアント PC がウイルスに感染した場合、または感染した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。 ネットワークからの分離は,具体的には,ネットワークケーブル、無線 LAN カード、USB キー型 LAN アダプタなどを取り外す。または、無線 LAN アダプタが PC に内蔵されている場合には無線 LAN 機能を停止させる。

6.6 迷惑メールの対処

(1) 利用者は、必要以上に電子メールアドレスを公表し又は通知しないこと。

(2) 利用者は、ネットワークを経由して電子メールアドレスを開示し又は通知する場合には、アドレスを自動収集されないように、工夫を施すことが望ましい。(画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に接続する等)

(3) 利用者は、送信される迷惑メールに対しては、これを無視することが望ましい。送信者へ停止要求を出した場合、その電子メールアドレスが使用されている事実を伝えてしまう結果となり、かえって迷惑メールが増加してしまう可能性もあるからである。

7. (電子メールの作成)

7.1 To、Cc 及び Bcc の制限

(1) 利用者は、To(あて先)、Cc(カーボンコピー)及び Bcc(ブラインドカーボンコピー)の総あて先件数は必要最低限とすること。

(2) 利用者は、同時に多数の人へ電子メールを送信する場合、 Bcc を利用するか、あるいは各自に個別送信する等配慮すること。これは、その場合に電子メールアドレスを To、Cc に列記してしまうと、当該電子メールを受信した者に、他の者の電子メールアドレスが露呈することになるからである。

7.2 電子メール1件当たりのファイルの総容量

(1) 利用者は、電子メール本体と添付するファイルを含めた総容量が膨大とならないよう注意すること

（2）利用者は、電子メール本体と添付するファイルを含めた総容量が 膨大になる場合、別手段による情報提供や分割送信などについて検討の上、情報基盤ユニットに相談し、指示を仰ぐこと。

7.3　電子メールの内容

(1)利用者は、要機密情報を電子メールで送信する場合には、課室等責任者に届け出の上、安全確保に留意して送信手段を決定すること。例えば以下の手段が挙げられる。

・外部を経由しないネットワーク（専用線等）
・暗号化された通信路（VPN 等）
・暗号メール（S/MIME 等）

利用者は情報を検討の上決定された送信手段について課室等システムセキュリティ責任者へ届け出ること。利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、以下の保護対策の必要性を検討し、必要があると認めたときには、これを実施すること。

・添付ファイルに対するパスワード保護
・添付ファイルの暗号化（暗号化ソフトの使用等）

(2) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。

(3) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

(4) 利用者は、他人になりすまして電子メールを作成しないこと。

(5) 利用者は、電子メールを転送する際に、作成者の許可なく内容の変更をしないこと。

(6) 利用者は、個人情報やプライバシーの保護を考慮すること。

(7) 利用者は、次の事項に該当する電子メールの送信を行わないこと。

・機密保護違反（研究所の機密保護に関連する方針・規程等を遵守）
・権利違反（知的財産権、著作権、商標権、肖像権、ライセンス権利等）
・セクシャルハラスメント及び人種問題に関わる内容
・無礼及び誹謗中傷
・ねずみ講に相当する内容
・脅迫、個人的な儲け話や勧誘に相当する内容
・その他、公序良俗に反するもの

7.4 電子メール利用時のマナー

(1) 利用者は、チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）の送信・転送を行わないこと。

(2)利用者は、スパムメール（ダイレクトメール等営利目的を主とした無差別に発信された電子メール）、ジャンクメール（役に立たない情報が書かれている電子メール）等を送信しないこと。

(3) 利用者は、電子メールに題名を付けること。また、題名は電子メールの内容が分かるように具体的かつ簡潔に書くこと。
(4) 利用者は、機種依存文字コードを使用しないこと。
(5) 利用者は、電子メールを作成する際、各行とも適当な長さで改行を入れること。
(6) 利用者は、To と Cc との使い分けを意識し、送信する電子メールに対する返事を要求する時には、To(あて先)を使用すること。

8. (電子メールの送信)

8.1 送信時の注意

(1) 利用者は、To(あて先)の記述に誤りがないかを確認してから送信すること。
(2) 利用者は、電子メールにファイルを添付し送信する際に、当該ファイルのウイルスチェックを行うこと。

8.2 電子メールの暗号化

(1) 利用者は、要機密情報を電子メールで送信する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。
(2) 利用者は、暗号化された情報の復号に用いる鍵を適切に管理すること。
(3) 利用者は、暗号化された情報の復号に用いる鍵のバックアップを取得しておくこと。

8.3 添付ファイルのパスワード保護

(1) 利用者は、要機密情報を含む添付ファイルを電子メールで送信する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、添付ファイルにパスワードを設定すること。
(2) 利用者は、保護に用いたパスワードについては、あらかじめ受信者と合意した文字列を用いるかあるいは、電子メールで送信せずに電話などの別手段を用いて伝達すること。

8.4 電子メール送信時における情報漏えい防止の確認事項

(1) 利用者は、添付ファイルを電子メールで送信する場合には、当該電子ファイルの付加情報等から不用意に情報が漏えいすることがないか確認すること。

8.5 電子メールへの署名付与

(1) 利用者は、要保全情報を電子メールで送信する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときには、情報に電子署名を付与すること。
(2) 利用者は、電子署名の付与に用いた鍵を適切に管理すること。

8.6 電子メール送信時の受信確認機能の使用制限

(1) 利用者は、トラフィック増を防止するため、電子メール送信時の受信確認は必要最低限の使用とすること。

8.7 電子メールを誤って送信したときの対処

(1) 利用者は、電子メールを誤って送信した場合、相手先（受信者）へのフォローは発信者責任で実施すること。

8.8 ウイルスを送信したときの対処

(1) 利用者は、誤ってウイルスを送信したことが判明した場合、直ちに情報基盤ユニットに連絡・相談し、指示を仰ぐこと。

9. （電子メールの保存・削除）

9.1 メールボックス（サーバ側）における電子メールの保存・削除

(1) 利用者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、メールボックスから不要な電子メールを削除すること。

(2) 利用者は、サーバの個人別メールボックスに格納される電子メールの保存期限や最大容量、バックアップ状況等を考慮の上、適宜、クライアント PC への保存を行うこと。

9.2 メールボックス（クライアント PC 側）における電子メールの保存・削除

(1) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを保存する場合には、暗号化等の措置を講じた上で保存することが望ましい。

(2) 利用者は、本文や添付ファイルに要保全情報が含まれている電子メールについては、適宜バックアップすること。

(3) 利用者は、不要なメッセージは速やかにクライアント PC から削除すること。

(4) 利用者は、本文や添付ファイルに要機密情報が含まれている電子メールを削除する場合には、その機密性に配慮し、復元が困難な状態にすること。

10. （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。

ウェブブラウザ利用ガイドライン

1. （目的）

ウェブは、情報の伝達や共有に必要不可欠なツールとなっている。一方で、私的目的でのウェブの閲覧、掲示板への無断書き込み等は研究所の社会的信用を失わせる要因となる可能性もある。

本文書は、このようなリスクを軽減し、情報資産を保護し、利用者がウェブを安心・安全に利用するために必要な事項を定めることを目的とする。

2.（対象者）

本ガイドラインはウェブブラウザを利用する,すべての利用者を対象とする。

3. ウェブの利用に係る全般的な注意事項

ウェブブラウザを利用したウェブサイトの閲覧、各種情報システムの利用等、ウェブの利用において、利用者の安全性を確保するために、ウェブの利用に係る全般的な注意事項を記述する。

3.1 目的外利用の禁止

(1) 利用者は研究や教育及びそれらの支援等、研究所で活動する上で必要な範囲でウェブを利用するものとし、それ以外で利用しないこと。営利目的での利用は禁止する。

(2) 利用者は研究所内から任意のウェブサイトを閲覧することにより、閲覧先のサーバに研究所のドメイン名及び IP アドレス等が記録されることに留意すること。記録された情報をもとに、閲覧先等より研究所に対して不当な要求が行われ、あるいは閲覧者の個人情報の開示が要求される場合がある。また、掲示板等に名前やメールアドレスを記入した場合、不正請求をされることもある。

3.2 外部のウェブサイトで提供されているサービスの利用等の注意事項

(1) 利用者は、研究所外の掲示板、ブログ等への書き込み等にあたっては、情報漏えいの可能性に十分に注意すること。

(2) 利用者は、公序良俗に反する不適切な書き込みや利用を行わないこと。掲示板等への単純な書き込みであっても、内容によっては研究所や研究所構成員の良識が疑われる場合がある。特に、他人への誹謗中傷と誤解されるような記事や、プライバシーや著作権等の侵害と疑われかねない書き込みをしてはならない。

(3) 不正なサイトへの誘導を狙ったリンクや、ウイルス等の不正なソフトウェアをダウンロー

ドさせることを目的としたリンクはインターネット上に多数存在する。有名なサイトであっても決して安全ではないので、不用意にリンクをクリックしないこと。

3.5 ウェブサイト閲覧の監視

(1) 適正なウェブ利用を維持するため、その利用状況（いつ、誰が、どのウェブサイトを閲覧したか等）について監査証跡の取得、保存、点検及び分析を行う可能性がある。利用者は、その趣旨を理解の上、自身のウェブサイトの閲覧がモニタリング及び監査されていることを認識すること。

4. （ウェブサイトの閲覧）

ウェブサイトの閲覧に使用するウェブブラウザの利用方法、ウェブサイトを閲覧する場合に想定される脅威を回避するための注意事項等について記述する。

4.1 ウェブサイト閲覧時の一般的な注意事項

（1）利用者は、ウェブサイトを閲覧する場合には、以下の事項に留意すること。

- ・有名サイトであってもバナーを安易にクリックしないこと（有害サイトへ誘導、ウイルス感染）
- ・電子メール内のウェブリンクを安易にクリックしないこと（フィッシング詐欺、ウイルス感染）
- ・セキュリティ警告表示のあったファイル等のダウンロードをしないこと（ウイルス感染、不正プログラムの格納）

4.2 SSL/TLS 通信の確認

SSL/TLS 通信とは、通信内容の暗号化及び通信相手が確認できる安全な通信であり、重要な情報等を送受信するウェブサイトで標準的に利用されている技術である。利用者は、閲覧しているウェブサイトと個人情報、重要な情報等を送受信する可能性がある場合には、SSL/TLS 通信が利用されていることを確認すること。ただし、その際提示される証明書が正当なものであることを確認すること。

4.3 確認・警告等のダイアログへの対応

セキュリティ機能に係るウェブブラウザの設定等により、確認のためのダイアログ等が表示される可能性がある。当該ダイアログに関して安易に ActiveX、Java 等のスクリプトの実行を許可すると、不正プログラムの感染、情報漏えい等の危険性がある。利用者は、確認のためのダイアログが表示された場合には、内容を確認せずに安易に実行を許可してはいけない。

4.4 ウェブブラウザの設定変更を要求するウェブサイトの閲覧

（1） 利用者は、ウェブサイトから閲覧のためにプラグイン、スクリプト等の実行に関するウェブブラウザの設定変更を要求された場合であっても、ウェブブラウザのセキュリティレベルが低下し不正プログラムに感染する危険性等があるため、当該要求に従ってウェブブラウザの設定を安易に変更しないこと。

5. ウェブサイトへの情報送信（フォームへ入力した情報の送信、ファイルのアップロード等）

送信する情報の盗聴、なりすましによる誤った通信相手への情報送信等、ウェブサイトに情報を送信する場合に想定される脅威を回避するための注意事項等について記述する。

(1) 重要な情報のやりとりには SSL/TLS 等の安全な通信を利用すること。その際、証明書の正当性を確認すること。

(2) 情報の書き込みにあたっては、本物と見分けがつかない偽装サイトへの誘導（クロスサイトスクリプティング）等の危険性に留意し、正しいサイトを利用していることを確認すること。入力の必要なページは、中継しているポータル等を経由せずに直接参照すること。

6. ファイルのダウンロード

不正プログラムの感染等、ウェブサイトからダウンロードしたファイルを実行又は開く場合に想定される脅威を回避するための注意事項等について記述する。

6.1 ウェブブラウザから直接的に、実行ファイルを実行する行為及び文書ファイル等を開く行為の制限

(1) ウェブブラウザから実行ファイルを直接的に実行した場合でもアンチウイルスソフトウェア等の自動検査機能によりウイルスを検出することが可能であるが、利用者は、実行ファイルをダウンロードする場合には、電子署名及び不正プログラムの有無を確認し、また問題が生じた場合に原因となったファイルの特定を容易にするため、ウェブブラウザから直接実行するのではなく、端末上に一旦ダウンロードすることが望ましい。

(2) ウェブブラウザから文書ファイルを直接的に開いた場合でもアンチウイルスソフトウェア等の自動検査機能によりウイルスを検出することが可能であるが、利用者は、ウェブサイト上にある文書ファイル等を開こうとする（利用しようとする）場合には、不正プログラムの有無を確認し、また問題が生じた場合に原因となったファイルの特定を容易にするため、ウェブブラウザから直接開くのではなく、端末上に一旦ダウンロードすることが望ましい。ただし、信頼できるウェブサイト上にある文書ファイル等を開こうとする（利用しようとする）場合、この限りではない。

6.2 不正プログラムに感染した時の対処

(1) 利用者は、ダウンロードしたファイルを実行または開いたことにより、不正プログラムに感染したか又は感染の疑いがある場合には、直ちに LAN ケーブルを抜き、無線 LAN 機能を停止することにより当該 PC をネットワークから分離し、ウィルスチェックを実施の上、システム管理者または情報基盤ユニットに連絡・相談し、指示を仰ぐこと。

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ない用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）

研究所からウェブによって情報発信を行うことはもはや必要不可欠といえる。一方で、各種権利侵害を伴うようなウェブコンテンツの公開や掲示板等の開設は、そのためのトラブル対応による業務効率の低下や、研究所の社会的信用を失わせる要因となる可能性もある。本文書は、このようなリスクを軽減し、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、研究所内よりウェブページ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、コンテンツの内容に関する責任は研究所にも帰するので注意が必要である。

3. （ウェブの公開にかかわる全般的な注意事項）

ウェブを用いた各種情報の公開においては、各種法令を遵守することはもちろんのこと、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。

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。情報発信者の責任として、その意義と危険性についての十分な認識が求められる。ネットワークの世界は、自己責任の原則によって成り立っていることを忘れてはならない。

3.1 著作権等の知的財産権の遵守

他人が保有する知的財産権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。

3.2 肖像権・パブリシティー権などの侵害の禁止

3.3 他人に迷惑をかけるような情報発信の禁止

3.4 研究成果や研究途中の情報を掲載する際の注意

研究成果や研究途中の情報を掲載する際には、公開に問題がないか十分留意すること。

3.5 企業名やロゴなどの扱い

学会やシンポジウム等で協賛企業のロゴを貼るときは、事前に相手側と協議すること。

3.6 顔写真の掲載によるリスク

自身の肖像写真を掲載する場合にも、顔を露出する際のリスクを十分に考慮すること。

3.7 その他（公序良俗に反する情報発信の禁止など）

違法な情報はもちろんのこと、公序良俗に反する情報や有害情報を発信してはならない。

4.（デジタルアーカイブを行う際の注意事項）

デジタルアーカイブをウェブで公開する際には、各種権利処理が済んでいるかをきちんと確認すること。

5.（リンクの際の留意点）

リンクの設定自体は、慣習上、相手の許諾を得ることなしに自由に行えるものとされている。しかし、トップページ以外の他の階層に直接リンクを張る場合においては、必ずしもその限りではないため、リンクはトップページに設定するように心がけること。

6.（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なければならない。また、研究所の定めるネットワーク利用目的外の利用をしてはならない。

研究所の情報設備及び SINET は、もっぱら教育・研究の推進と職務・支援業務遂行のために提供されている。そのため、情報発信者は、設置目的にそぐわない情報を公開しないように注意することが求められる。

7.（システムの安全性の確保）

7. 1. 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こととし、十分な安全性を確保すること。また、ウェブページを作成す

るときにも、セキュリティの確保に十分注意すること。ページの作成を外部の業者に委託すると際も同様である。

7.2 サーバ容量やネットワーク資源への配慮

ウェブページを公開するためのサーバを設置する際には、必要十分なサーバ容量やネットワーク資源を確保すること。

8.（ウェブサーバや掲示板の管理者等の責任の及ぶ範囲）

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、研究所内外に対してそれなりの責任と義務を負うことを十分承知して運用すること。特に「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」と見なしているため、これらの管理を行う者は、同法上の責任と義務を負うので十分に注意すること。

9.（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。

利用者パスワードガイドライン

1.（目的）

本文書は、研究所情報システムのアカウントを利用する際のパスワードに関し、利用者が予め理解しておくべき事項を示し、安全なパスワードの設定をさせることを目的とする。

2.（パスワードにかかわる全般的な注意事項）

2.1 初期パスワードの変更

利用者は、アカウントが発行されたら速やかに初期パスワードを自己のものに変更すること。初期パスワードのまま情報システムの利用を継続してはならない。

2.2 パスワードに使用する文字列

利用者が設定するパスワード文字列は、以下の条件を全て満足するものが推奨される。

・最低限6文字以上の長さを持つ。

・以下ア～エの文字集合から各最低1文字以上を含む。

ア）英大文字（A～Z）

イ）英小文字（a～z）

ウ）数字（0～9）

エ）システムで使用可能な特殊文字（@!#$%&=-+*/.、:;[]|）

また、以下の文字列は容易に推察可能であるため、パスワードとして設定してはならない。

・利用者のアカウント情報から容易に推測できる文字列（名前、ユーザ ID 等）

・上記を並べ替えたもの、上記に数字や記号を追加したもの

・辞書の見出し語

・著名人の名前等

2.3 パスワードの定期的な変更

利用者は、アカウント発行者（個別システムについてはシステム管理者）からパスワードの変更の指示を受けた場合には遅滞なくパスワードを変更しなければならない。変更後のパスワードは変更前のパスワードと類似のものであってはならない。

2.4 パスワードの管理

利用者は、自己のパスワードを厳重に管理しなければならない。パスワードをメモしたり、端末にそのメモを貼り付けたりしてはならない。利用者は、他の者にパスワードを教えたり、不注意でパスワードが他の者に知られたりしてしまうことがないよう最大限の注意を払わなけ

ればならない。

2.5　パスワードの詐取の可能性のある場所での利用の禁止

　パスワードやアカウントを詐取される可能性があるので、利用者は研究所外のインターネットカフェなどに設置されているような不特定多数の人が操作（利用）可能な端末を用いての研究所内情報システムへのアクセスを行ってはならない。

2.6 パスワードによるロックの励行

　利用者は、使用中のコンピュータにログインしたまま離席する場合は、他者が画面を閲覧したり操作することができないよう、画面のロック操作を行うこと。

2.7　パスワードの事故の報告

　利用者は、アカウントを他者に使用され又はその危険が発生した場合には、直ちに当該システム責任者にその旨を報告しなければならない。

所外情報セキュリティ水準低下防止手順

1. （目的）

研究所は、所内の情報セキュリティ水準の低下を招くような行為を防止するだけでなく、所外の情報セキュリティ水準の低下を招くような行為をしないことは当然である。また、所外のセキュリティ水準を低下させることは、研究所を取り巻く情報セキュリティ環境を悪化させることにもなる。

本文書は、情報セキュリティ対策の適所において講ずべき措置を定め、もって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ことを目的とする。

2. （適用範囲）

ポリシーに定める範囲とする。

3.（所外の情報セキュリティ水準の低下を招く行為の防止）

3.1　措置の整備

システム責任者は、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具体的措置を例示すること。

＊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措置の例示。

(1) 提供する電磁的記録の内容、形式等による影響

所外へ電磁的記録を提供する際に、当該電磁的記録の内容、形式等によって、研究所外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

・提供する電磁的記録が不正プログラムを含まないこと。
・実行プログラムの形式以外に電磁的記録を提供する手段がある場合は、実行プログラムの形式で電磁的記録を提供しないこと。
・提供する電磁的記録に改ざん等がないことを知りえる機会を、提供先の者に与えること。
・提供先の者が警告等に慣れて無視しないように、提供する電磁的記録の参照時に警告等が出ないようにすること。

(2) 提供する電磁的記録を処理することによる直接的な影響

所外へ提供した電磁的記録を提供先の者が参照等する際に、利用する端末等の設定変更を要求することによって、研究所外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

・研究所外の者が利用している端末のオペレーティングシステム、ソフトウェア等のセキュリティ設定変更を不用意に指示しないこと。

・やむを得ずセキュリティ設定変更を指示する場合には、後に元の設定に戻す方法を、参照しやすい形式で紹介すること。

(3) 提供する電磁的記録を処理することによる間接的な影響

所外へ提供した電磁的記録を提供先の者が参照等する際に、明示的に利用する端末等の設定変更を要求するわけでないが、電磁的記録を参照できる設定であることを想定することは、暗黙に設定変更を指示したと考えられる。暗黙に指示した設定変更により、研究所外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

・研究所外の者にセキュリティ上の問題を生じさせるような設定変更を暗黙に指示する電磁的記録を不用意に提供しないこと。

・やむを得ず当該電磁的記録を提供する場合には、後に元の設定に戻す方法を、参照しやすい形式で紹介すること。