国立健康・栄養研究所
情報ネットワークセキュリティポリシー

平成２０年３月３１日
改　正　平成２５年６月１３日
改　正　平成２７年４月１日

１．情報セキュリティ基本方針

（１）情報セキュリティの基本方針

①　情報セキュリティの基本方針

国立健康・栄養研究所における情報資産について、「情報セキュリティポリシーに関するガイドライン（平成１２年７月１８日情報セキュリティ対策推進会議決定）」（以下「ガイドライン」という。）における「政府の情報セキュリティの基本的な考え方」を踏まえ、国立健康・栄養研究所における継続的かつ安定的な研究業務の実施を確保するとともに、国民の安全、安心及び信頼の下に電子政府を構築するため、我が国の電子政府の基盤としてふさわしいセキュリティ水準を達成するよう適切な情報セキュリティ対策を実施することが必要不可欠である。

このため、国立健康・栄養研究所においては、「厚生労働省の情報セキュリティポリシー」に則り、国立健康・栄養研究所における研究情報資産のセキュリティの確保に取り組むため、「情報ネットワークセキュリティポリシー（以下「ポリシー」という）」を策定し、国立健康・栄養研究所の情報資産をあらゆる脅威から守るために必要な情報セキュリティの確保に最大限取り組むこととする。

また、国立健康・栄養研究所のネットワーク(NIH-NET)を利用するすべての利用者は、この目的を果たすため、ポリシーの実施に責任を負うとともに、規範を尊重し、遵守しなければならない。

②　組織・体制

情報セキュリティの確保のための組織・体制を定め、その責任及び権限を明確にする。

③　情報の分類と管理

NIH-NET の情報システムにおいて取り扱う情報について、重要な情報を重点管理する考え方から、重要度に応じた情報分類の定義、情報の管理責任、管理の方法を規定する。

④　物理的セキュリティ

情報システムの設置場所について、不正な立入り、損傷及び妨害から情報資産を保護するため、管理区域を設置する等の物理的な対策を規定する。

⑤　人的セキュリティ

情報セキュリティに関する権限や責任を定め、すべてのユーザにポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるよう必要な対策を規定する。

⑥　技術的セキュリティ

NIH-NET の情報資産を外部からの不正アクセス等から適切に保護するため、情報資産への接続及び利用の制限、ネットワーク管理等の必要な対策を規定する。

⑦　運用

ポリシーの実効性を確保するため、また、不正アクセス及び不正アクセスによって他の情報システムに対する攻撃に悪用されることを防ぐため、ポリシーの遵守状況の確認、ネットワークの監視といった運用面に関して必要な措置を規定する。また、緊急事態が発生した際の迅速な対応を可能とするため、緊急時対応計画を規定する。

⑧　評価・見直し

ポリシー及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等を踏まえ、定期的に対策基準の評価・見直しを実施することとし、このための必要な措置を規定する。

（2）定義

このポリシーの用語の定義については、次のとおり定める。

・情報

研究・業務の記録のうち、保管又は公開される目的で電磁的に記録されたもの。

・情報セキュリティ

情報資産の機密性、完全性及び可用性を維持すること。

・情報資産

情報及び情報を管理する仕組み（情報システム及びシステム開発、運用及び保守のための資料等）の総称。

・NIH-NET

NIH-NET とは、国立感染症研究所情報ネットワーク（国立健康・栄養研究所研究情報ネットワークを含む）の略称。研究所の情報資産を繋ぎ、情報を伝達する。

・情報システム

NIH-NET に繋がれた情報資産のうち、特定の研究・業務処理を行うものの集合。ハードウェア、ソフトウェア、ネットワーク及び記録媒体で構成され、開発・運用・保守資料が付帯する。

・部・センター等

国立健康・栄養研究所組織規程（規程第 6 号、）で置かれる組織をいう。　・ユーザ

NIH-NET にユーザ登録を行っている者。

（3）　対象範囲

ポリシーの対象範囲は、NIH-NETを使用するハードウェア、ソフトウェア、ネットワーク、記録媒体等の情報システム等（システム構成図等の文書を含む。）及びすべての情報のうち情報システムに電磁的に記録される情報、並びにすべてのユーザ及び委託事業者とする（ 別表 参照）

２．対策基準

（1）組織体制

① 情報セキュリティ責任者等

（イ）国立健康・栄養研究所の最高情報セキュリティ責任者は、理事長をもって充てるものとする。

（ロ）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として、理事の職責にあるものを指名する。

（ハ）情報セキュリティ責任者は、情報管理委員長をもって充てるものとする。

（ニ）情報システム管理者は、栄養情報技術研究室長をもって充てるものとする。

（ホ）課室情報セキュリティ責任者は、各部・センター長をもって充てるものとする。

（ヘ）課室情報セキュリティ責任者は、課室情報システム管理者を情報管理委員の職責にあるものの中から指名する。

（ト）課室情報システム管理者は、緊急時に置ける予備の連絡担当者を指名する。

（2）情報の管理責任者等及び情報の管理等

① 情報の管理責任等は、以下のとおりとする。

（イ）管理責任

情報は、当該情報を作成等した課室情報セキュリティ責任者が管理責任を有する。ただし、別途、特別の定めがある場合はこの限りでない。

（ロ）利用責任

情報を利用するユーザ及び委託事業者は、情報の分類に従い利用する責任を有する。特に、他に漏えいすることが禁じられている情報については、厳重に管理するとともに守秘しなければならない。

（ハ）重要性の効力

情報が複製又は伝送された場合には、当該複製等も分類に基づき管理しなければならない。

② 情報の分類と管理方法

（イ）情報の分類

このポリシーの対象となる研究所内のすべての情報は、各々の情報の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

■ 重要性分類

Ⅰ 研究所幹部及び業務上必要とする最小限の者のみが扱う情報（極秘の情報を含む。）

Ⅱ 公開することを予定していない情報（極秘の情報を含む。）

Ⅲ 外部に公開する情報のうち業務上重要な情報

Ⅳ 上記以外の情報

（ロ）情報の管理方法

ａ 情報の分類の表示

・第三者が重要性の識別を容易に認識できないよう留意しつつ、情報システムで扱う情報について、ファイル名、記録媒体等に情報の分類が分かるように表示をする等、適切な管理を行わなければならない。

b　情報の管理及び取扱い

・情報について、それぞれの分類に従い、利用権限を定めなければならない。

・ユーザは、課室情報セキュリティ責任者の許可がある場合を除き、重要な情報（重要性分類 II 以上）の外部への送付及び持出しをしてはならない。

・重要な情報（重要性分類 I）は暗号化を施して管理し、暗号化に用いた暗号鍵及び暗号化された当該情報は、必要に応じて別々に適切な管理を行うこととする。

c　記録媒体の管理

・記録媒体は、適切な管理を行わなければならない。

・重要な情報（重要性分類 II 以上）を記録した記録媒体を、部・センター等から外部に持ち出す場合は、部・センター等の課室情報セキュリティ責任者の許可を得なければならない。

・重要な情報（重要性分類 II 以上）を記録した記録媒体は、施錠可能な場所に保管しなければならない。

・重要な情報（重要性分類 II 以上）を記録した記録媒体を送る場合は、信頼できる者を選定し、記録媒体の物理的保護規定を定めなければならない。

d　記録媒体の処分

・記録媒体が不要となった場合は、当該媒体に含まれる重要な情報（重要性分類 II 以上）をいかなる方法によっても復元できないように処理した上で、廃棄しなければならない。

・重要な情報（重要性分類 II 以上）を記録した記録媒体の廃棄は、課室情報セキュリティ責任者の許可を得ることとする。

3．物理的セキュリティ

（1）サーバ等

（イ）管理区域の設置

・ホストあるいはサーバ等を設置する情報処理機器室（以下「情報処理機器室」）は、外部からの侵入が容易にできないよう外壁等に囲まれた管理区域としなければならない。

・管理区域からすべての外部に通ずるドアは、制御機能、鍵、警報装置等によって許可されていない立入りを防止しなければならない。

・情報処理機器室には、必要に応じて、監視機能を設置することとする。

・情報処理機器室内の機器類は、耐震対策を講じた場所に設置するとともに、防火措置等をしなければならない。

（ロ）情報処理機器室の入退室管理

・情報処理機器室の入退室は、許可された者のみとし、入退室管理簿の記載を行い、職員以外の者が入退室を行う場合、身分証明書等がよく見えるように身につけなければならない。

（ハ）機器等の受渡し場所

・サーバ室へ機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について、情報システム管理者による確認を行わなければならない。

・機器等の搬入には職員が同行する等の必要な措置を講じなければならない。

（ニ）装置の取付け等

・情報システムの取付けを行う場合は、火災、水、埃、振動等の影響を可能な限り排除した場所に設置し、必要に応じ容易に取り外せないよう適切な固定等の必要な措置を施すこととする。

・情報システムの取付けに当たっては、必要に応じて画面、配線等から放射される電磁波により重要な情報が外部に漏えいすることがないよう措置することとする。

・情報システム管理者以外の者が容易に操作できないように、利用者ＩＤ、パスワードの設定等の措置を施さなければならない。

（ホ）電源

・サーバ等の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

・落雷等による過電流に対してサーバ等の機器を保護するための措置を施さなければならない。

（ヘ）配線

・配線は、傍受又は損傷等を受けることがないように可能な限り必要な措置を施さなければならない。

・主要な箇所の配線については、損傷等についての定期的な点検を行なわなければならない。

（ト）外部に設置する装置

・外部に設置する装置（外部委託事業者の敷地に置かれるサーバ等）は、最高情報セキュリティ責任者が定めた装置又は課室情報セキュリティ責任者の承認を受けたものでなければならない。また、定期的に当該装置のセキュリティの水準について、確認しなければならない。

・情報セキュリティ責任者は、外部から接続、利用するために所外に持ち出されるモバイルパソコン等が当該情報システムに存在する場合、モバイルパソコン等については、次の点に留意し、庁舎外での使用方法及び内部ネットワーク等への接続方法等を定め、適切に管理しなければならない。

・外部からのモバイルパソコン等からの内部ネットワーク等への接続の許可は、必要最低限にしなければならない。

・外部からのモバイルパソコン等からの内部ネットワーク等への接続方法及び利用方法等は、利用者の真正性の確保が確定できるものでなければならない。

（2）ユーザのクライアントパソコン等

・執務室等にユーザがいない場合は、必要に応じて執務室等の施錠等による盗難防止のための措置を施すこととする。

・執務室等のクライアントパソコン等については、必要に応じて盗難防止のためのワイヤーに

よる固定等、盗難防止のための措置を施すこととする。
・執務室等のクライアントパソコン等については、必要に応じて、画面、配線等から放射される電磁波により重要な情報が外部に漏えいすることがないよう措置することとする。

４．人的セキュリティ

（1）役割・責任

（イ）最高情報セキュリティ責任者

・最高情報セキュリティ責任者は、研究所の情報セキュリティに関する権限と責任を有し、連絡体制の構築並びにポリシーの遵守に関する意見の集約及び職員に対する教育、訓練、助言及び指示を行う。また、部・センター等内で行う外部委託において、適正な委託事業者の管理及び指導を行わなければならない。（情報セキュリティ責任者が行うものを除く。）

（ロ）情報セキュリティ責任者

・情報セキュリティ責任者は、当該情報システムにおける情報セキュリティに関する権限及び責任を有し、ポリシーの具体的実施手順を定め利用者に周知するとともに遵守させなければならない。また、開発や運用等の外部委託を行う場合、適正な委託事業者の管理を行わなければならない。

・情報システム管理者は、情報セキュリティ責任者を補佐し当該情報システムに関する設定の変更、運用及び更新等を行う管理権限を有する。

（ハ）課室情報セキュリティ責任者

・課室情報セキュリティ責任者は、部・センター内における情報セキュリティに関する権限と責任を有する。

・課室情報システム管理者は、課室情報セキュリティ責任者を補佐する。

（ニ）ユーザ

a.　情報セキュリティ対策の遵守義務

・情報システムを利用するすべての者は、ポリシー及び NIH-NET の規約等に定められている事項を遵守しなければならない。

・情報セキュリティ対策について不明な点、遵守することが困難な点等については、すみやかに課室情報システム管理者または課室情報セキュリティ責任者に相談し、指示等を仰がなければならない。

b.　外部委託に関する管理

・情報システムの開発・保守を外部委託事業者に発注する場合は、外部委託事業者から下請けとして受託する業者も含めて、ポリシーのうち外部委託事業者が守るべき内容の遵守を明記した契約を行わなければならない。

・外部委託事業者との契約書には、ポリシーが遵守されなかった場合の規定を定めなければならない。

c.　その他

・ユーザは、使用するクライアントパソコンや記録媒体について、第三者に使用されること又は許可なく情報を閲覧されることがないように、適切な措置を施さなければならない。

・ユーザは、課室情報システム管理者の許可を得ず、クライアントパソコン等を執務室外に持ち出してはならない。

（2）教育・訓練

・説明会の実施等により、幹部を含めすべてのユーザに対しポリシーについて啓発しなければならない。

・新規ユーザには、登録から２ヵ月以内に情報セキュリティ講習会を受講させなければならない。

・情報システム管理者は、システム管理者向けの研修を受けなければならない。

・ユーザは、定められた研修に参加する等し、ポリシー及び規約を理解し、情報セキュリティ上の問題が生じないようにしなければならない。定められた研修に参加しないユーザは、利用停止とすることができる。

（3）ユーザアカウントの管理

ユーザは、自己の保有するユーザアカウントに関し、次の事項を遵守しなければならない。

・パスワードを秘密にしておくこと。

・パスワードのメモを作らないこと。

・パスワードの長さは８文字以上のシステムが許す最大長とし、文字列は英文字と数字若しくは記号を組み合わせ辞書や人名にないものを使用すること。

・情報システム又はパスワードに対する危険のおそれがある場合には、パスワードを変更すること。

・パスワードは定期的若しくは接続回数等に基づいて変更し、古いパスワードの再利用は行わないこと。

・仮のパスワードは、最初の利用時に変更すること。

・クライアントパソコンに、パスワードを記憶させる際は、暗号化等を行うことによって他人がパスワードを読めないようにすること。

・ユーザアカウントを共有しないこと

５．技術的セキュリティ

（1）コンピュータ及びネットワークの管理

（イ）アクセス記録の取得

・情報システム管理者は、アクセス記録及びセキュリティ関連事案に関する記録を取得し、一定の期間保存しなければならない。

・アクセス記録が窃取、改ざん、消去されないように必要な措置を施さなければならない。

・情報システム管理者は、定期的にアクセス記録を分析、監視しなければならない。

（ロ）システム管理記録及び作業の確認

・情報システム管理者は、行ったシステム変更等の処理について、記録を作成しなければならない。

・情報システム管理者の行った作業は記録し、適切に管理を行わなければならない。

・情報システム管理者が当該情報システムの運用に重要な影響が及ぶ作業を行う場合には、必要に応じ２名以上で作業し、互いにその作業を確認しなければならない。

（ハ）情報システム仕様書等の管理

・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については、当該書類に記録されている情報の漏えいが当該情報システムの情報セキュリティに重大な影響を及ぼすと思慮される場合は、記録媒体、紙媒体に関わらず、業務上必要とする者のみが閲覧できる場所に保管しなければならない。

（ニ） 情報及びソフトウェアの交換

・組織間において、情報システムに関する情報（紙媒体及び口頭も含む。）及びソフトウェアを交換する場合は、必要に応じその取扱いに関する事項をあらかじめ定めなければならない。

（ホ）データ保全

・情報システム管理者は、サーバ等に記録された情報について、その重要度に応じて期間を設定し、定期的にデータの待避を行わなければならない。

（ヘ）メール

・情報システム管理者は、情報システムを経由しての外部から外部へのメール転送（メールの中継処理）を不可能とする等、他の情報システムに悪影響を与えないような設定を施さなければならない。

・ユーザは、チェーンメール・メールボム・極端に大きなバイナリメール・規定コード以外のメール等、所内外のメールサーバの動作を不安定にする恐れのあるメールの送信及び転送を行ってはならない。

・ユーザは、メールで重要な情報（重要性分類 II 以上）を送る場合は、暗号化を行わなければならない。

（ト）外部の者が利用できる情報システム

・外部の者が利用できる情報システムについては、情報セキュリティ対策について、特に強固な対策を取らなければならない。

（チ）情報システムの入出力データ

・情報システムに入力されるデータは、適切な検査等を行い、それが正確であることを確実にするための対策を施さなければならない。

・誤びゅう又は故意の行為により情報が改ざんされることがあるため、改ざんを検出する検査システムを導入しなければならない。

・情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されることを確保しなければならない。

（リ）電子署名・暗号化

・暗号化については、情報セキュリティ責任者が定めた方法以外の方法を用いてはならない。また、暗号のための鍵の管理方法について、定めた方法で管理しなければならない。

（ヌ）業務目的以外の使用の禁止

・ユーザは、業務目的以外での情報システムの利用、メールの使用及びインターネットへの接続を行ってはならない。

（ル）無許可ソフトウェアの導入の禁止

・ユーザは、情報システム管理者が設置した機器(ワークステーション等)に対して、情報システム管理者に許可されていないソフトウェアを導入してはならない。

・ユーザは、個々のクライアントパソコンに導入するソフトウェアについて、情報システム管理者がセキュリティ上危険と判断した場合、これを導入してはならない。

（ヲ）機器構成の変更

・ユーザは、クライアントパソコンについて、業務を遂行するために機器の増設・交換を行う必要がある場合は、情報システム管理者の許可を得なければならない。

・ユーザは、情報セキュリティ責任者が定めた方法以外で外部からの接続を行ってはならない。

（2）利用の管理

（イ）利用者登録

・情報システム管理者は、利用者の登録、変更、抹消、登録情報の管理、異動や研究所外への出向等の職員及び退所者におけるユーザアカウントの取扱い等については、情報セキュリティ責任者が定めた方法に従って行わなければならない。

（ロ）管理者権限

・情報システムの管理者権限は、情報セキュリティ責任者の許可した、必要最小限の者に与える。

・情報システム管理者は、管理者権限を使用する場合には、その記録を保存し、情報セキュリティ責任者から報告を求められた場合、速やかに応じなければならない。

（ハ）ネットワークへの接続制御

・情報セキュリティ責任者は、NIH-NET の個々の情報システムに接続可能な他のネットワーク及び情報システムの提供手段等について、各情報システムごとに制限を設けて接続させなければならない。

・情報システム管理者は、業務遂行上必要ないネットワークサービスを、停止しておくとともに、外部からの当該サービスへの問い合わせを不可能にしなければならない。

（ニ）強制的な経路制御

・情報システム管理者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

（ホ）遠隔地にあるシステムへの接続

・保守・点検のため外部からの接続口を設ける場合には、必要十分なセキュリティ対策を講じなければならない。

・情報システム管理者は、遠隔地に情報システムがある場合は、安全な接続が可能となるよう、適切な制御を施さなければならない。

・民間企業等が保有する設備への相互接続が業務上必要となる場合は、情報セキュリティ責任者は、各設備への接続要件を定めなければならない。

(ヘ) 自動識別

・NIH-NET で使用されるネットワーク機器については、技術的に可能な範囲で機器固有情報によって接続の可否を自動的に決定するシステムを導入することとする。

(ト) 利用手順

・情報セキュリティ責任者は、利用者ＩＤ、パスワードの入力時におけるメッセージ及び利用者ＩＤ、パスワードの試行回数の制限、アクセスタイムアウト（一定時間、操作しなければ自動的に接続している情報システムの接続が切断される機能）の設定、情報システムの利用開始から終了までの時刻の表示等、ユーザが情報システムを利用する際の手順を必要に応じて定めることとする。

(チ) パスワードの管理方法

・情報システム管理者は、ユーザのパスワードに関する情報を厳重に管理しなければならない。ユーザのパスワードを発行する場合は、仮のパスワードを発行し、当該情報システムを最初に利用したとき、直ちに仮のパスワードを変更させなければならない。

・情報システム管理者は、定期的にユーザのパスワードの脆弱性を検査しなければならない。脆弱性のあるユーザについては、パスワード変更の勧告を行った後、安全な仮パスワードへの変更を行うことができる。

・情報システム管理者は、第三者に読まれることのないよう、暗号化等パスワードを扱う方法を定めなければならない。

(リ) 接続時間の制限

・管理者権限による情報システムへの接続については、必要最小限の接続時間に制限しなければならない。

（3）．システム開発、導入、保守等

(イ) 情報システムの調達

・課室情報セキュリティ責任者は、NIH-NET に接続される個々の情報システムの調達に当たっては、一般に公開する調達仕様書が情報セキュリティ確保の上で問題のないようにしなければならない。

・課室情報セキュリティ責任者は、機器及びソフトウェアを購入等する場合は、当該製品が情報セキュリティ上問題にならないかどうか、確認しなければならない。

(ロ) 情報システムの変更管理

・情報システム管理者は、重要な情報システムを追加、変更、廃棄等した場合は、その際の設定、構成等の履歴を記録し、保存しなければならない。

(ハ) 情報システムの開発

情報システムの開発及び保守時の事故・不正行為対策のため、次の事項を遵守しなければ

ならない。

・責任者、監督者を定めること。

・作業者及び作業範囲を明確にすること。

・情報システムの開発及び保守等の事故・不正行為に係る危険性の分析を行うこと。

・開発・保守する情報システムは、可能な限り既に運用している情報システムと切り離すこと。

・開発・保守に際しては、可能な限りプログラム言語での提出を求めること。

・開発・保守に際しては、セキュリティ上問題となりうるおそれのあるソフトウェアを使用しないこと。

・開発・保守の際の利用制限を明確にすること。

・機器の搬出入には、情報システム管理者の許可及び確認を得ること。

・開発・保守記録の提出を義務づけること。

・マニュアル等は、定められた場所に保管すること。

・開発・保守を行った者のユーザアカウント、パスワードを当該開発・保守終了後に不要となった時点で速やかに抹消すること。

（ニ）情報システムの導入

・情報システム管理者は、情報システムを導入する際には、原則として既に稼働している情報システムに接続する前に、十分な試験を行わなければならない。ただし、導入前に十分な試験を行うことが困難な場合には、危険性を十分に考慮した上で対処方針を策定しなければならない。

・情報システム管理者は、試験に使用したデータ及びその結果を厳重に保管しなければならない。

（ホ）ソフトウェアの保守及び更新

・情報システム管理者は、ソフトウェア（独自開発ソフトウェア、汎用ソフトウェア）を更新又は修正用のプログラムを導入する場合は、不具合、他の情報システムとの相性の確認を行い、計画的に導入しなければならない。

・情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて、すみやかな対応を行うこととし、その他のソフトウェアの更新等については、計画的に実施しなければならない。

（ヘ）情報システムの外部への委託

・新たな情報システムの開発等を外部の事業者に委託する場合は、可能な限りプログラム言語での提出を求めること。

・外部の事業者に委託する際には、導入前の検査要求事項を契約に定めなければならない。

（ト）下請け業者に対する確認

・委託業者が、当該契約について、下請け業者に対し、再委託契約を行う際には、あらかじめ、再委託先、委託内容等について当所の了承を得ることを契約に定めなければならない。

・信頼のおける業者に委託するために、必要な資格等を定めなければならない。

・必要に応じて守秘のための契約を事業者と結ばなければならない。

（チ）機器の修理及び廃棄

・記録媒体の含まれる機器について、業者に修理させ、又は廃棄する場合は、その内容が消去された状態で行わなければならない。

・故障を業者に修理させる際、情報を消去することが難しい場合は、修理を委託する業者に対し、秘密を守ることを契約に定めなければならない。また重要な機器を廃棄する場合は、情報が復元不可能となる方法で廃棄を行わなければならない。

（4）コンピュータウイルス対策

（イ）情報システム管理者の義務

情報システム管理者は、次の事項を実施しなければならない。

・コンピュータウイルス情報について利用者に対する注意喚起を行うこと。

・定期的にコンピュータウイルスに関する情報収集をすること。

・重要なシステムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。

・サーバ及びクライアントパソコンにおいて、コンピュータウイルスの確認を行うこと。

・コンピュータウイルスの確認用のパターンファイルは常に最新のものに保つこと。

・ 添付ファイルのあるメールを送受信する場合は、コンピュータウイルスの確認を行うような対策を講じること。

（ロ）ユーザの遵守義務

ユーザは、次の事項を遵守しなければならない。

・データ又はソフトウェアを取り入れる場合には、必ずコンピュータウイルスの確認を行うこと。

・差出人が不明、又は不自然に添付されたファイルは開かないこと。

・コンピュータウイルスの確認用プログラムの実行を途中で止めないこと。

・情報システム管理者等が提供するコンピュータウイルス情報を常に確認すること。

（5）セキュリティ情報の収集

情報システム管理者は、所掌する情報システムの版（バージョン）情報を管理し、得られた情報との確認ができるようにしなければならない。

6．運用

（1）情報システムの監視

・セキュリティに関する事案を検知するため、情報システム管理者は、常に情報システムの監視を行わなければならない。

・外部と常時接続する情報システムについては、侵入検知装置を設置し、２４時間監視を行わなければならない。

・内部の情報システムについても、必要に応じ侵入検知装置を設置し、監視を行わなければならない。

・監視により得られた結果については、消去又は改ざんをされないために必要な措置を施し、定期的に安全な場所に保管しなければならない。また、これらの記録の正確性を確保するため、正確な時刻の設定を行わなければならない。

[情報システムの監視項目]

・ファイアウォール、サーバのアクセス記録
・ファイアウォール、サーバのセキュリティ関連事象
・ネットワーク侵入監視装置
・入退室記録
・配線、中継機器への不正な接続
・ネットワーク負荷
・システムの異常停止
・ハードウェアの使用状況
・ファイルの改ざん
・情報システムへの操作
・利用開始及び利用終了の時刻
・利用権限
・パスワードの変更記録

（2）ポリシーの遵守状況の確認

・課室情報システム管理者及び情報システム管理者は、ポリシーが遵守されているかどうかについて、また、問題が発生していないかについて、常に確認を行わなければならない。

・情報システム管理者は、サーバ等のシステムの設定がポリシーを遵守しているか否かについて、又、問題が発生していないかについて、定期的に確認を行わなければならない。

（3）運用管理における留意点

・アクセス記録及びメール等個人のプライバシーに係る情報を閲覧する場合は、情報セキュリティ責任者と情報管理委員会が協議の上行わなければならない。ただし、他の法令等で定められた個人情報の保護に関係する情報の閲覧に関しては、当該法令等に定められた手続に従う。

・前項の場合においても、情報システム管理者及びユーザが所属する課室情報セキュリティ担当者又はその指名する者の立ち会いがない場合には、ユーザ個人のメールを閲覧してはならない。

・情報システム管理者は、情報システムの活用等を通じ、ユーザが常に実施手順を参照できるよう配慮しなければならない。

（4）外部委託による運用契約

・運用を外部委託する課室等は、委託事業者に対しシステム構築時に判明した脆弱性に対する

対応及び、システム運用中に発覚した脆弱性に対する対応を記載した契約書による契約を締結しなければならない。

・外部委託を行う課室等は委託先において必要なセキュリティ対策が確保されていることを確認しなければならない。

７．侵害時等の対応

サイバー攻撃による情報資産への侵害等情報セキュリティに関する事故及び情報システム上の障害等が発生した場合における証拠保全、被害拡大の防止、復旧、連絡等の必要な措置を迅速かつ円滑に実施し、併せて、再発防止策の措置を講じるため、以下のとおり体制を整備するものとする。

（１）緊急連絡対応

（イ）各情報システム

情報セキュリティ責任者が策定する具体的実施手順には、以下の内容の緊急連絡対応を盛り込まなければならない。

a　侵害時等における情報セキュリティ責任者までの連絡体制（情報セキュリティ責任者が不在の場合の体制も含む。）

b　次の事案が発生し、情報資産の防護のためにネットワークの切断や情報システムの停止がやむを得ない場合は、情報セキュリティ責任者（情報セキュリティ責任者が不在の場合、情報セキュリティ責任者の業務を代行するものを含む。）は、ネットワークの切断や情報システムの停止等必要な措置を講じなければならない。

○　インターネットを通じて提供している情報の改ざん等、不正アクセスが継続し、情報資産に影響が発生又は影響が発生するおそれがある場合

○　サービス不能攻撃（ＤｏＳ攻撃）又はメール爆弾等により情報システムの運用に著しい支障をきたす攻撃が継続している場合

○　コンピュータウイルス等の不正プログラムが、情報資産に深刻な被害を発生させている場合又は発生させる恐れがある場合並びにネットワーク経由で広がっている場合

○　災害等により電源を供給することが危険又は困難な場合

○　その他の情報資産に係る重大な被害が発生又は発生するおそれがある場合

c　情報セキュリティ責任者（情報セキュリティ責任者が不在の場合、情報セキュリティ責任者の業務を代行するものを含む。）は「b」及びあらかじめ厚生労働省が報告を求めるべき事項として通知した事案が発生した場合、速やかに、証拠保全、被害拡大の防止、復旧等の措置を講じると同時に厚生労働省に報告することとする。

d　「c」の場合において、所轄の警察にも通報するものとする。（ただし、災害等に係わる事例は除く。）

（ロ）情報システム以外

情報システム以外における情報セキュリティに関する事故等が発生した場合の体制は、次のとおりとする。

a　ユーザは情報セキュリティに関する事故等を発見した場合又はポリシーに違反した場合は、速やかに課室情報システム管理者に報告し、指示を仰がなければならない。

b　課室情報システム管理者は、報告等のあった事故等についてすべて課室情報セキュリティ責任者に報告し、これらの指示の下、必要な措置を講じなければならない。

c　課室情報セキュリティ責任者は、その重要性に応じこれらの事故等を、情報システム管理者、情報セキュリティ責任者、統括情報セキュリティ責任者、及び最高情報セキュリティ責任者に報告しなければならない。

（2）再発防止対応

（イ）（1）の事案を対応した情報セキュリティ責任者は次に掲げる措置を講じなければならない。

a　事案に関する記録の整理

b　当該事案に係る危険性の分析

c　再発防止策の策定

d　a及びcの厚生労働省への報告

e　規約・細則等の改定が必要と認められる場合、当措置事案に関する内容が不正アクセスに関する場合、不正アクセス行為の禁止等に関する法律第6条に基づく都道府県公安委員会に対する援助の申し出

（ロ）情報セキュリティ責任者、統括情報セキュリティ責任者または最高情報セキュリティ責任者は、必要に応じてポリシーの改定を行うこととする。

8．法令遵守

ユーザは、職務の遂行において使用する情報資産について、次の法令を遵守し、これに従わなければならない。

①　不正アクセス行為の禁止等に関する法律

②　著作権法

③　行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律等

9．情報セキュリティに関する違反に対する対応

セキュリティポリシーに違反した者については、その重大性、発生した事案の状況等に応じて懲戒処分等の対象となりうる。

なお、処分の決定に際し、自らの責任において発生した情報セキュリティ上の問題について、その問題について申告した場合は、状況等に応じて考慮されるものである。

１０．評価及び見直し

① 監査

情報セキュリティ責任者は、NIH-NET について、その指名する者による監査を定期的に行う。外部の事業者に委託する場合には、情報システム管理者は、委託事業者を選定する。

② 点検

ユーザは、ポリシーに沿った情報セキュリティ対策が実施されているかどうかについて自己点検を行わなければならない。

③ ポリシーの更新

新たに必要な対策が発生した場合、または監査の結果及び点検の結果を踏まえ、情報管理委員会においてポリシーの実効性を評価し、必要な部分の見直し内容、時期について決定を行う。この決定に基づき、ポリシーの更新を実施する。更新の内容については、情報管理委員会が決定しなければならない。

別表　対象範囲

●情報システム等

範囲：汎用コンピュータ、ファイアウォール、ルータ、各種サーバ（WWW、データベース、グループウェア、メール、ファイル等）、クライアントパソコン、リピータハブ、スイッチ、ルータ、ネットワークケーブル等、ソフトウェア、システム設定情報（パスワードファイル等）、通信機器、記録媒体（MO、FD、CD-ROM、DVD 等）、システム構成図等

●情報システムに記録される情報

範囲：情報、アクセス記録（ログ）、文書及び図面等の電磁的記録

●これらの情報に接するすべての者

範囲：役職員、特別研究員、事務・技術補助員、流動研究員、研修生、客員研究員、協力研究員、派遣職員、委託事業者、情報管理委員会が認めた者