人間文化研究機構

情報セキュリティポリシー

平成１８年４月
（令和４年１月改訂）
人間文化研究機構

目　　次

Ⅰ　情報セキュリティの基本方針

１．基本的考え方

高度情報社会において、人間文化研究機構（以下「機構」という。）が学術研究・業務活動を遂行し向上させるためには、情報基盤の整備に加えて、情報資産のセキュリティ確保が不可欠である。情報セキュリティの重要性を機構の全構成員に十分意識させ、情報資産を確固として守るために、「人間文化研究機構情報セキュリティポリシー」（以下「ポリシー」という。）を定める。

ポリシーによって目指すものは、次のとおりとする。

（１）機構の情報セキュリティに対する侵害を阻止
（２）機構内外の情報セキュリティを損ねる加害行為の抑止
（３）情報資産の管理及び使用に関するセキュリティ確保
（４）情報資産の不正使用に関する対処

２．定義

ポリシーの用語の定義については、別添に示すとおりとする。

３．対象範囲

ポリシーの対象範囲は、機構の情報資産に加えて、機構の管理対象以外のコンピュータで、機構の情報ネットワークに一時的に接続されるコンピュータとする（以下「情報資産等」という。）。

ポリシーの対象となる者は、機構に属する役職員（研究員等を含む。）、学生（総合研究大学院大学生等を含む。）、一時的利用者（機構の情報システム等、情報ネットワークを一時的に使用する者）、委託業者などのうち、情報資産等を取り扱う者（以下「機構内利用者」という。）とする。

Ⅱ　対策基準等

本部、国立歴史民俗博物館、国文学研究資料館、国立国語研究所、国際日本文化研究センター、総合地球環境学研究所及び国立民族学博物館（以下「各機関等」という。）においては、ポリシーで定めるもののほか、ポリシー及び情報セキュリティ政策会議の策定する「政府機関の情報セキュリティ対策のための統一規範」等を踏まえ、各機関等における情報システム等又は業務の特性に応じて、情報セキュリティ対策基準及び情報セキュリティ実施手順等を策定しなければならない。

Ⅲ　管理・運営組織等

１．管理・運営組織

1.1　最高情報セキュリティ責任者

機構に最高情報セキュリティ責任者を置き、情報セキュリティ委員会委員長をもって充てる。

最高情報セキュリティ責任者は、機構の情報セキュリティに関する総括的な意思決定と、機構内外に対する責任を負う。

最高情報セキュリティ責任者は、被害を受けたサイバー攻撃に係る情報について、可能な限り速やかに文部科学省へ連絡を行う。

1.2　副最高情報セキュリティ責任者

機構に副最高情報セキュリティ責任者を置き、本部情報セキュリティ責任者をもって充てる。

副最高情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐し、また同責任者が不在の際には、1.1 で規定される全ての事項を代行する。

1.3　情報セキュリティ責任者

各機関等に情報セキュリティ責任者を置き、各機関等の長が指名する副館長相当の職員をもって充てる。

情報セキュリティ責任者は、当該機関等における情報セキュリティに関する総括的な意思決定と、当該機関等の内外に対する責任を負う。ただし、サイバー攻撃その他特に重大と認める事案が発生した場合には、直ちに最高情報セキュリティ責任者に当該事案の内容等について報告しなければならない。

1.4　情報セキュリティアドバイザー

機構に、必要に応じて情報セキュリティアドバイザーを置くことができる。

情報セキュリティアドバイザーは、機構長が情報セキュリティに関する専門的知識及び経験を有する機構外部の専門家に委嘱するものとし、職務内容については機構長が別に定める。

1.5　情報システム管理責任者

各機関等に情報システム管理責任者を置き、各機関等の長が指名する施設長相当の職員をもって充てる。

情報システム管理責任者は、当該機関等における情報システム等の管理の実施に関し、情報セキュリティ責任者との緊急時の連絡など、総括的な対応にあたるとともに情報セキュリティ責任者を補佐する。

1.6　統括システム管理者

各機関等に統括システム管理者を置き、各機関等の長が指名する課長相当の職員をもって充てる。

統括システム管理者は、当該機関等における情報システム等の管理の実施に関し、情報システム管理責任者との連絡などの対応にあたるとともにシステム管理者を統括する。

1.7　システム管理者

各機関等にシステム管理者を置き、各機関等の長が指名する係長相当の職員をもって充てる。

システム管理者は、当該機関等における情報システム等の管理の実施に関し、総括システム管理者との連絡などの対応にあたるとともに各機関等内の利用者を総括する。

1.8　情報セキュリティ監査責任者

機構に情報セキュリティ監査責任者を置き、本部監査室長をもって充てる。

情報セキュリティ監査責任者は、機構の情報セキュリティ対策基準の遵守状況、情報セキュリティ対策について監査する。

1.9　情報セキュリティ委員会

情報セキュリティ委員会は、機構の情報セキュリティに関し、ポリシーの策定及び改訂等の重要事項の決定を行うとともに、機構の情報セキュリティに関する対外的な対応等を行う。

1.10　各機関等情報セキュリティ委員会

各機関等の情報セキュリティに関する委員会（以下、「各機関等情報セキュリティ委員会」という。）は、当該機関等における情報セキュリティ対策基準及び情報セキュリティ実施手順等の策定・改訂を行うとともに、ポリシーの遵守の励行及び情報セキュリティに関する対外的な対応等を行う。

また、機関等情報セキュリティ委員会は、当該機関等の情報セキュリティ対策基準及び情報セキュリティ実施手順等を策定・改訂をした場合には、情報セキュリティ委員会に報告しなければならない。

1.11　システム管理部会

システム管理部会は、各機関等における情報システム等のセキュリティ管理を実施するための連絡調整等を行う。

1.12　管理・運営組織の改編

管理・運営組織については、各機関等における情報システム等の状況に応じて、適宜改編して組織することができる。

1.13　緊急時における体制

情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るため、各機関等に、人間文化研究機構情報セキュリティインシデント対応チーム（以下、「CSIRT」という。）を設置する。CSIRT に関し必要な事項は、別に定める。

２．例外措置

各機関等において、学術研究・業務活動の適正な遂行を継続する上で、ポリシーを遵守することが困難な状況が生じた場合は、各機関等の情報セキュリティ責任者は、情報セキュリティ委員会の許可を得て、例外措置を取ることができる。また、各機関等の情報セキュリティ責任者は、上記例外措置が終了した時に、情報セキュリティ委員会にその旨を報告しなければならない。

ただし、一時的な例外措置及び各機関等における特有の例外措置については、当該機関等で処理する。

３．違反への対応

各機関等の情報セキュリティ責任者は、ポリシーへの違反行為があった場合には、最高情報セキュリティ責任者に当該違反行為に関する報告をしなければならない。

報告を受けた最高情報セキュリティ責任者は、当該情報セキュリティ責任者に対し、情報セキュリティの維持に必要な措置を講じさせなければならない。また、情報セキュリティ委員会において、当該違反行為に対する措置を審議するとともに、機構長及び機関の長に対し、当該違反行為を報告しなければならない。

４．点検・監査及びポリシーの改訂

4.1　点検

4.1.1　最高情報セキュリティ責任者は、別に定める自己点検実施手順に基づき、情報セキュリティ対策の遵守状況を点検し、その結果を把握・分析するため、自己点検計画を整備する。

4.1.2　情報システム管理責任者は、情報セキュリティ責任者が定める自己点検計画に基づき、自己点検の実施を実施するとともに、点検結果を取りまとめ、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。

4.2　監査

4.2.1　情報セキュリティ監査責任者は、別に定める監査実施手順に基づき、対策基準の遵

守状況を検証するため、情報セキュリティ対策について、監査を行い、その結果を最高情報セキュリティ責任者に報告する。

4.2.2　情報セキュリティ監査責任者は、機構外の者に監査の一部を請け負わせる必要性を検討し、必要と判断した場合は、機構外の者に監査の一部を請け負わせることができる。

4.3　改訂

4.3.1　ポリシーの改訂を求める機構に属する役職員（研究員等を含む。）は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、改訂が必要と認めた場合は速やかに改訂の手続きをとり、その内容を機構内利用者に周知しなければならない。

4.3.2　情報セキュリティ委員会は、ポリシーの実効性を定期的に評価し、改訂が必要と認めた場合は速やかに改訂の手続きをとらなければならない。

4.3.3　各機関等で策定する情報セキュリティ対策基準及び情報セキュリティ実施手順の改訂に関することは、各機関等において定める。

附　則

1　ポリシーは、平成１８年４月２５日から実施する。

2　ポリシーの実施前に運用している各機関等の情報セキュリティポリシー（対策基準及び実施手順を含む。）は、ポリシーの基本的考え方に基づき制定されたものとみなし、情報セキュリティの状況の変化に応じて必要な改訂を行う。

附　則

1　ポリシーは、平成２４年９月４日から実施する。

2　ポリシーの実施前に運用している国立国語研究所の情報セキュリティポリシー（情報セキュリティ規程を含む。）は、ポリシーの基本的考え方に基づき制定されたものとみなし、情報セキュリティの状況の変化に応じて必要な改訂を行う。

附　則

ポリシーは、平成２５年９月３日から実施する。

附　則

ポリシーは、平成２９年３月１３日から実施する。

附　則

ポリシーは、令和４年１月３１日から実施する。

（別添）　用語の定義

・情報システム等

「情報システム」並びに「情報」を指す。

「情報システム」とは、情報処理及び通信に係るシステムをいう。

「情報」とは、情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。したがって、作業途中の文書も適用対象であり、書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面）及び情報システムに関する設計書も含まれる。

・情報資産

機構における情報セキュリティ対策の対象となるものであり、次に掲げるものをいう。

（ア）情報

（イ）情報システム及び電磁的記録媒体等

（ウ）ソフトウェア

（エ）組織及び人

・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である。

機密性とは、情報にアクセスすることが認可された者だけがアクセスできることを確実にすること

完全性とは、情報及び処理方法の正確さ及び完全である状態を安全防護すること。

可用性とは、許可された利用者が、必要なときに情報にアクセスできることを確実にすること。

・情報セキュリティポリシー

機構の情報セキュリティ対策について、機構が総合的・体系的かつ具体的にまとめるもので、根本的な考えを示す情報セキュリティ基本方針と、情報セキュリティを確保するために遵守すべき行為及び判断の基準を示す情報セキュリティ対策基準からなる。

・情報セキュリティ実施手順等

情報セキュリティ対策基準に定められた内容を具体的に情報システムにおいて、どのような手順に従って実行していくのかを示すもの。

・情報セキュリティ政策会議

内閣に置かれる「高度情報通信ネットワーク社会推進戦略本部（ＩＴ戦略本部）」の下に設置された我が国の情報セキュリティに関する問題の根幹に係る事項を決定する母体。

・例外措置

機構内利用者が情報セキュリティポリシーを遵守することが困難な状況で、機構の学術研究・業務活動の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。