国立国語研究所情報セキュリティ規程

平成２２年　７月１４日
国語研規程第５１号
改正　平成２６年　５月１３日
改正　平成２７年１０月２８日
改正　平成２８年　４月　１日
改正　平成３１年　４月　１日
改正　令和　２年　３月１０日
改正　令和　３年　３月　９日
改正　令和　５年　４月１２日
改正　令和　５年　６月１３日
改正　令和　６年　４月１０日

第１章　総則

（目的）

第１条　この規程は，国立国語研究所（以下「研究所」という。）の情報セキュリティ対策基本方針（令和６年４月１０日所長裁定）に則り，研究所が取り扱う情報資産の機密性，完全性及び可用性を適切に維持するための情報セキュリティ対策基準を定めることを目的とする。

（定義）

第２条　この規程において，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　「情報システム」とは，情報処理及び通信に係るシステムをいう。

二　「情報資産」とは，情報及び情報を管理する仕組み（情報システム並びにシステム開発，運用及び保守のための資料等）の総称をいう。

三　「情報セキュリティ」とは，情報資産の機密性，完全性及び可用性を維持することをいう。

四　「機密性」とは，情報に関して，アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。

五　「完全性」とは，情報が破壊，改竄又は消去されていない状態を確保することをいう。

六　「可用性」とは，情報へのアクセスを認められた者が，必要時に中断することなく，情報及び関連資産にアクセスできる状態を確保することをいう。

（対象とする情報資産）

第３条　この規程で対象とする情報資産は，次のとおりとする。

一　情報システム等については，サーバ（WWWサーバ，メイルサーバ，メイルゲート及びファイルサーバ（ネットワーク接続型ハードディスク）等），ネットワーク機器（ファイアーウォール，ルータ，ハブ，ネットワークケーブル等），コンピュータ端末（役職員等が使用する端末（タブレット等のスマートデバイス含む）），ソフトウエア（基本ソフトウエア及び応用ソフトウエア）及び記憶媒体（ハードディスク及びＣＤ-ＲＯＭ等）等とする。

二　情報システム上で扱われる情報については，設定ファイル，アクセスログ及びユーザが作成する文書等とする。

（適用者）

第４条　この規程は，研究所の情報資産を扱う全ての職員，契約職員，パートタイム職員，派遣職員，総合研究大学院大学学生，連携大学院学生，共同研究員，外来研究員，特別共同利用研究員，

委託業者及び来訪者等（以下「利用者」という。）に適用する。

第２章　情報セキュリティ管理体制

（情報セキュリティ責任者）

第５条　研究所に情報セキュリティ責任者を置き，所長が指名する副所長をもって充てる。

２　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総括的な権限及び責任を有する。

（委員会）

第６条　研究所の情報セキュリティ対策に関する重要事項の審議は，情報セキュリティ委員会（以下「委員会」という。）が行う。

（システム管理者）

第７条　研究所にシステム管理者を置く。

２　システム管理者は，研究所の基幹的な情報システム（以下「基幹システム」という。）及びその利用者の日常的な管理，サポートデスク業務を行う。

（情報セキュリティインシデント対応チーム）

第８条　情報セキュリティインシデント発生時の迅速かつ円滑な対応を図るため，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設置要項（平成２９年３月１３日）に基づき，研究所に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。）を置く。

第３章　基幹システム情報セキュリティ対策

（基幹システムの管理）

第９条　コンピュータ室への不正な立ち入りを制限する。

２　情報システムの重要な機器は，火災，窃盗等からの脅威及び危険等を考慮して設置する。

３　許可なくコンピュータ室にサーバ等の機材を設置してはならない。機材の設置手続きについては別に定める。

４　研究所ネットワークに接続する全てのコンピュータ端末及びサーバ等について，設置場所，管理者及び基本ソフトウエア等を記録した管理簿を作成する。

５　サーバにはＵＰＳ（無停電装置）を使用し，停電による障害を防止する。

６　基本ソフトウエア及び応用ソフトウエアのセキュリティパッチが公開された際には，速やかにこれを適用する。

７　サーバのバックアップは，定期的に実施する。

８　ソフトウェアアップデート，メンテナンス，障害対応等により基幹システムの一部又は全部を停止させる必要がある場合は，原則として情報基盤室長の許可を得るとともに，可能な限り利用者に対して事前通知を行う。

（サーバ等の管理者）

第１０条　外部の一般利用者にサービスを提供するサーバ，外部協力者等にサービスを提供するサーバ及び研究所内部で複数の利用者が使用するサーバ等については，特定のサーバ管理者を定める。

２　ホスティングサービス（レンタルサーバ）又はハウジングサービス（以下「ホスティングサービス等」という。）を利用して研究所ネットワークの外部にサーバを設置する場合は，特定のサーバ管理者を定める。
３　サーバ管理者は，各サーバあたり１名とする。
４　サーバ管理者に対して，必要な情報セキュリティ対策に関する情報等を随時通知する。
５　サーバ管理者からの報告により，各サーバの状況を把握するよう努めるとともに，情報セキュリティ対策に関し必要な措置を講じる。

（ネットワークへの接続制限等）
第１１条　研究所ネットワークには，特別な事情がある場合を除き，研究所の所有物ではないコンピュータ端末を接続させない。
２　特別な事情により研究所の所有物ではないコンピュータ端末を研究所ネットワークに接続させる場合は，接続を制限したネットワークセグメントで使用させる。
３　不特定多数の利用者が使用することを想定したコンピュータ端末は，接続を制限したネットワークセグメントを置き，使用できる機能等を制限する。
４　研究所ネットワークには，特別な事情がある場合を除き，研究所外部からコンピュータ端末を接続させない。特別な事情により接続を認める場合は，接続を制限したＶＰＮ等を経由させ，必要最小限の範囲かつセキュリティが担保された形で接続させる。
５　研究所ネットワークに接続するコンピュータ端末には，必ずウィルスや不正アクセス対策のための適切なセキュリティ設定がなされているようにする。
６　研究所の無線ＬＡＮに対して，不特定のコンピュータ端末が接続できないように，アクセスポイントの接続制限の設定を適切に行う。

（ユーザ管理）
第１２条　基幹システム及び研究所ネットワークの利用者について，ユーザ名及び所属等を記録した管理簿を作成する。
２　利用者が退職等した場合，別に定めるルールに基づきアカウントの削除等を行う。
３　管理簿とシステム上の設定に相違が生じないよう，定期的にアカウントの棚卸を実施する。

（外部との通信）
第１３条　外部ネットワークから研究所ネットワーク内への接続設定は，必要最低限とする。
２　外部との通信は，必要に応じて暗号化等を行う。

（基幹システムの廃棄処理）
第１４条　基幹システムを構成する機器を破棄する際には，適切な方法でデータ消去や破砕処理等を行う。また，記憶装置を有する機器の廃棄を外部に委託する場合は，データ消去に関する証明書の発行を求めるものとする。

（障害の対応）
第１５条　研究所ネットワークに影響のある障害（以下「障害」という。）が発生した場合，被害の拡大を防ぐとともに，障害から復旧するための体制を整備する。また，被害拡大の可能性がある場合，障害が解消されるまで，当該機器を研究所ネットワークから隔離する。
２　障害が発生した場合，障害の内容，原因及び対応について記録する。

（利用者へのサポート及び教育）
第１６条　利用者が情報資産を利用する際や情報セキュリティを維持する際に支援が必要な場合，

情報提供や技術的支援を行う。
２　情報セキュリティ対策に関する情報提供等を随時行い，情報セキュリティに対する意識を高めるよう努める。

（評価・見直し）
第１７条　情報セキュリティ対策の実施状況及び問題点を把握し，より高いセキュリティレベルが維持できるよう改善を行う。
２　情報セキュリティに関わる新たな脅威等の情報収集に努め，必要な対応策を検討する。

第４章　利用者等の情報セキュリティ対策

（法令等の遵守）
第１８条　利用者は，不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号），著作権法（昭和４５年法律第４８号）及び個人情報の保護に関する法律（平成１５年法律第５７号）等の情報資産に関する法令，並びに研究所及び人間文化研究機構が定める規程，ポリシー，マニュアル等を遵守しなければならない。

（申請）
第１９条　利用者は，コンピュータ端末，サーバやプリンタ等を新規に研究所ネットワークに接続する場合は，事前に情報基盤室に申請し，許可を得なければならない。また，許可なく研究所内に研究所ネットワークの構成を改変したり，別のネットワークを構築したりするための機器を設置してはならない。
２　研究所ネットワークへの接続許可を得たコンピュータ端末等であっても，一定の期間，研究所ネットワークの接続実績がない場合は，接続許可を取り消すものとする。

（個人端末）
第２０条　研究所所有のコンピュータ端末で，研究所ネットワーク又はインターネットに接続するものは，必ずセキュリティソフトウエアを導入し，適切なセキュリティ設定がなされていなければならない。
２　基本ソフトウエア及び応用ソフトウエアのセキュリティパッチが公開された際には，速やかにこれを適用する。
３　コンピュータ端末には，ログオン（ログイン）のためのパスワードを必ず設定し，オートログオン等の機能は無効にする。
４　研究所所有ではないコンピュータ端末で研究所の業務に関する情報を扱わざるを得ない場合は，研究所所有のものと同等以上のセキュリティ対策を施す。

（コンピュータ端末及び記憶媒体の持ち出し，研究所外での業務）
第２１条　研究所外に持ち出すコンピュータ端末には，セキュリティソフトウエアを導入するとともに確実にファイアーウォール機能が有効化されていなければならない。また，紛失，盗難により情報が流出することのないよう常時，注意する。
２　第３１条に定める重要情報を記録したコンピュータ端末及び記憶媒体は，研究所外に持ち出すことができない。ただし，その重要情報が,研究所外における研究業務に特に必要な場合で，重要情報の管理者の許可を得た場合はこの限りではない。
３　研究所外に持ち出すコンピュータ端末及び記憶媒体は，情報の重要度に応じて，ファイルの暗号化等の処置を行う。

４　研究所外での業務実施時における情報セキュリティの取扱いについては，別に定める。

（共有設定）

第２２条　ネットワーク上でファイル等を共有する場合には，必要に応じてアクセス権及びパスワードの設定並びに暗号化等を適切に行う。

２　新規にコンピュータ端末を導入する場合，原則として標準で設定された共有機能等は無効にし，共有の必要があるファイル等のみを十分に確認した上で共有設定する。

３　不特定多数でのファイル交換を目的としたファイル交換ソフトウエアは使用しない。

（パスワードの管理）

第２３条　不正アクセス等を防止するため，別に定めるガイドラインに基づき，十分な強度をもつパスワードを設定し，パスワードを他者に知られたり共有されることのないよう適切に管理しなければならない。

（外部との通信）

第２４条　外部との通信は，必要に応じて暗号化等を行う。

（無線ＬＡＮ）

第２５条　無線ＬＡＮを使用する場合には，通信内容が他者に漏えいすることのないよう暗号化等の設定を適切に行う。

（サーバ等の管理）

第２６条　基本ソフトウエア及び応用ソフトウエアのセキュリティパッチが公開された際には，サーバ管理者は，速やかにこれを適用する。

２　研究所ネットワークに影響を及ぼすようなプロトコルの使用及びサービスの提供は行わない。

３　サーバで使用するプロトコル及びサービスは，あらかじめ情報基盤室に報告する。

４　情報基盤室からの求めに応じ，サーバのセキュリティ対策等の報告を行う。また、外部に公開するサーバ，動的コンテンツについては，別に定める手続きにより，情報セキュリティに係る審査又は監査を受けなくてはならない。

５　技術的問題等によりサーバ管理が困難な場合は，情報基盤室に速やかに対応を求める。

６　ホスティングサービス等を利用して研究所ネットワークの外部にサーバを設置する場合は，特定のサーバ管理者を定めるとともに，利用契約の情報をあらかじめ情報基盤室に報告する。

７　管理者が特定されていないサーバを稼働させてはならない。退職等によりサーバ管理者が変更となる場合は，速やかに情報基盤室に報告する。

（情報システムの廃棄処理）

第２７条　記憶装置を有する情報機器を廃棄する際には，必ず適切な方法でデータ消去や破砕処理等を行う。また，廃棄を外部に委託する場合は，データ消去に関する証明書の発行を求めるものとする。

（外部委託時の情報セキュリティ基準）

第２８条　情報システムに係る業務を外部事業者に委託する場合は，別に定める情報セキュリティ基準を満たしていなければならない。

（外部ウェブサービス・クラウドサービスの利用）

第２９条　研究所の業務を実施する上で外部事業者が提供するウェブサービスやクラウドサービ

ス(研究所として契約しているサービスを含む)を利用する場合は,別に定める確認表に基づき,当該サービスの利用条件や利用に係るリスク等を十分に確認の上,利用する。また,アカウント情報の管理に十分に注意する。

(インシデントへの対応)

第３０条　インシデントを発見した場合には,別に定める手順により,インシデント窓口に速やかに報告しなければならない。

２　情報システムを利用する上で情報セキュリティを確保する方法が不明な場合には,情報基盤室に相談又は処置を依頼する。

第５章　情報の分類及び重要情報の取り扱い

(情報の分類)

第３１条　情報は,人間文化研究機構情報格付け基準(平成２９年３月２９日人間文化研究機構情報セキュリティ委員会決定)に基づき,その機密性,完全性及び可用性を踏まえて分類するものとし,機密性３の情報を「重要情報」という。

(重要情報の入手等)

第３２条　催し物の申込み等をホームページ上で受け付ける際には,必要以上の個人情報を収集したり,サーバ上に保持しないようにするとともに,通信を暗号化する。

２　個人情報等の提供を受ける場合には,情報の利用目的,管理方法及び保存期間等を明示する。

３　個人及び機関から重要情報の提供を受ける場合には,提供者と研究所の間で,情報の利用目的,管理方法及び保存期間等を書面で定める。

(重要情報の管理者)

第３３条　重要情報には,管理者(以下「重要情報管理者」という。)を定める。

２　重要情報管理者は,管理する重要情報に対して,その管理方法,保存場所,保存期間及びアクセス権限を記録する。

(重要情報の管理)

第３４条　重要情報を保存する際は,暗号化しなくてはならない。外付けＨＤＤやＵＳＢメモリ等の外部記憶媒体に保存する場合は,当該媒体全体も暗号化しなくてはならない。

２　研究所の所有物ではないコンピュータ端末,外部記憶媒体等で重要情報を扱ってはならない。

(重要情報の共有・複製)

第３５条　利用者は,重要情報管理者の許可なく重要情報の複製を作成してはならない。

２　業務上重要情報を複数の利用者が必要とする場合,重要情報管理者は,重要情報の共有・複製が必要最小限の範囲となるようにするとともに,利用者及び複製・消去等の使用履歴を記録する。

(重要情報の利用)

第３６条　重要情報の利用者は,当該情報のパスワードや複製媒体の管理を適切に行なわなければならない。

２　重要情報の利用者は,当該情報を使用する必要がなくなった場合,重要情報管理者に報告をし,情報媒体の返却等の必要な措置をとるものとする。

３　重要情報管理者は,重要情報の利用者が当該情報を使用する必要がなくなった場合,アクセス

権限の消去や複製媒体の回収・廃棄処理を行い，その旨を記録する。

（業者への委託）

第３７条　業者に委託して重要情報の収集又は利用を行う場合，当該業者及び当該業者が業務を依頼する全ての業者に対して，第１８条に定める法令等を遵守する旨の誓約書を研究所に提出させるか，契約条件に明示する。

２　委託業務終了後，前項に定める業者に対して，適切な方法で情報の消去等を行わせ，処理結果を研究所に提出させる。

（漏えい時の対応）

第３８条　重要情報の漏えい又は漏えいのおそれを認識した場合には，直ちに情報連絡体制により対応をとるものとする。

２　システム管理者は被害の拡大防止又は復旧等のために必要な措置を速やかに講ずるものとする。外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等のネットワーク接続を切断するなど，被害拡大防止のため直ちに行い得る措置を，直ちに行う（職員に行わせることを含む。）ものとする。

第６章　補則

（情報セキュリティの監査）

第３９条　情報セキュリティ責任者は，情報システムがこの規程等に沿って保護されているかの確認を行うため，情報セキュリティの監査を行うことができる。

（罰則等）

第４０条　故意又は重大な過失によりこの規程に違反した場合，又は重大な情報セキュリティの侵害を行った場合は，大学共同利用機関法人人間文化研究機構職員懲戒規程（人間文化研究機構規程第１０２号）及び関連する規則等により処分されることがある。

２　利用者は，研究所に損害を与えた場合又は法律等に違反する行為を行った場合は，損害賠償請求又は告訴されることがある。

（雑則）

第４１条　この規程に定めるもののほか，研究所の情報セキュリティ対策に関し必要な事項は，別に定める。

附　則

この規程は，平成２２年７月１４日から施行し，平成２２年４月１日から適用する。

附　則

この規程は，平成２６年５月１３日から施行し，平成２６年４月１日から適用する。

附　則

この規程は，平成２７年１０月２８日から施行し，平成２７年４月１日から適用する。

附　則

この規程は，平成２８年４月１日から施行し，平成２７年１２月１４日から適用する。

附　則

この規程は，平成３１年４月１日から施行する。

附　則

この規程は，令和２年３月１０日から施行する。

附　則

この規程は，令和３年３月９日から施行する。

附　則

この規程は，令和５年４月１２日から施行し，令和５年４月１日から適用する。

附　則

この規程は，令和５年６月１３日から施行し，令和５年４月１日から適用する。

附　則

この規程は，令和６年４月１０日から施行する。