

平成 25 年 12 月 11 日
情報基盤センター運営委員会決定
平成 28 年 2 月 25 日
情報基盤センター運営委員会改正
平成 30 年 2 月 14 日
情報基盤センター運営委員会改正
令和 2 年 2 月 13 日
情報セキュリティ委員会改正

国立大学法人電気通信大学情報システム運用・管理実施手順書

1. 本実施手順書の目的

1.1 本実施手順書の目的

本実施手順書は、国立大学法人電気通信大学情報システム運用基本規程第 28 条及び国立大学法人電気通信大学情報システム運用・管理規程第 40 条の規定に基づき、国立大学法人電気通信大学（以下「本学」という。）における情報システムの適切な運用・管理に関し、具体的な実施手順を定めるものである。

1.2 本実施手順書の適用範囲

本実施手順書は、国立大学法人電気通信大学に所属する情報システムを運用・管理・利用する全ての者を対象とする。

2. 情報ネットワーク及び情報システム管理のための組織

本学において、情報ネットワーク及び情報システムの運用及び管理を行なう管理運営部局は情報基盤センターである。情報基盤センターは情報化統括責任者（以下「CIO」という）の指示に従って本学の情報ネットワーク及び情報システムの運用管理を行なう。

各部局等においては、その長が部局統括責任者となり、以下の者を指名する。

部局運用責任者

その部局等に属する職員のうちから指名される。情報ネットワーク及び情報システムの管理運用の実務的責任者である。部局システム管理者のうちから補佐を指名してよい。

部局システム管理者

その部局等に属する職員のうちから指名される。その部局等に属する情報ネットワーク及び各情報システムの運用担当者である。複数名であってよい。

情報基盤センターからの連絡は基本的には部局運用責任者に対して行なわれる。補佐を指定して複数名の体制で部局等を運用管理する場合は、メーリングリスト等を用いて部局運用責任者とその補佐が全員メールを読めるようにして、緊急対応に備えなければならない。

これらの体制とは別に現在のところ、以下の者が本学の情報ネットワークの運用管理に携わっている。これらの者と各部局等の部局運用責任者及び部局システム管理者は互いに協力して本学の情報ネットワーク及び情報システムの運用管理を行なわなければならない。

IP アドレス管理者

学内ネットワークの論理的 IP アドレスブロックの管理を行なう者。その論理的 IP アドレスブロックを利用する者から選出される。もし、IP アドレス管理者が選出できない場合は、情報基盤センターにて IP アドレスの管理を行うこととす

る。

建物ネットワーク管理者
各建物に設置された物理的ネットワーク（LAN の配線及びネットワーク機器）
の管理を行なう者。

3. アカウントとパスワードに関するマニュアル

3.1 パスワードについて

パスワードは情報システムの利用者を守る最も重要な手段である。そのため、
全てのパスワードは以下の条件を満たしていなければならない。

- ・ パスワード長は十分に長くなければならない。最短で 12 文字、可能ならば
16 文字以上である必要がある。
- ・ パスワードは、大文字、小文字、数字、記号を含まなければならない。
- ・ パスワードは、辞書に掲載されている単語や固有名詞で構成されてはならな
い。

パスワードは十分に複雑であったとしても、定期的に変更することが推奨さ
れる。また、パスワードは暗号化されたパスワード、ハッシュ化されたパスワ
ードであっても、一部の情報が漏洩した場合は、ただちに漏洩したと思われる全
てのパスワードを変更しなければならない。

利用者にパスワードを付与する場合は、仮パスワードを与え一定期間内に利
用者に変更させなければならない。仮パスワードのまま利用させてはならない。

パスワードは、学内外を問わず複数のシステムで同じパスワードを使い回し
てはならない。

されている場合を除き、部局統括責任者の許可を得ること。

3. 大学組織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必要がある場合、利用者は多要素認証やアプリケーションパスワード等による認証情報の保護及び、セキュリティ対策ソフトを導入等による計算機環境の保護等の安全管理措置を講ずること。
4. 大学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必要性がなくなった場合、利用者はその旨を部局統括責任者及び部局運用責任者に報告すること。

4.2 電子メールの自動転送の禁止

1. 大学組織ドメインの電子メール利用者は、要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送することを原則として禁止する。
2. 要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要がある場合、利用者はメール転送先・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申請書を部局システム管理者に提出し、所属する部局統括責任者の了解を得ること。
3. 要保護情報を含む電子メールを大学施設（キャンパス）外へ自動転送する必要性がなくなった場合、利用者はその旨を部局統括責任者及び部局運用責任者に報告すること。

5. IP アドレスの割当・管理・利用について

5.1 IP アドレスの種類

学内ネットワークは以下の4種類のIPアドレスを必要に応じて割り当て利用する。これらのIPアドレスブロックの範囲は情報基盤センターが定めるものとする。

- ・ グローバル IPv4 アドレスブロック
- ・ プライベート IPv4 アドレスブロック
- ・ IPv6 アドレスブロック
- ・ その他特殊用途の IP アドレスブロック

割り当ての基準を以下に示す。

- ・ グローバル IPv4 アドレスブロック

学外と通信可能な IPv4 アドレスブロックである。主に学外に公開する必要のあるサーバや学外と直接通信を行わなければならないクライアントに対して割り当てられる。複合機、プリンタ、NAS アプライアンス、ネットワークカメラ、情報機器の管理インターフェース及び IoT 機器等には割り当ては行われぬ。個人情報保有する機器に対する割り当ては十分に気をつけなければならない。

- ・ プライベート IPv4 アドレスブロック

プライベート IPv4 アドレスブロックは学内にのみ通信可能な IPv4 アドレスブロックと物理セグメント内でのみ利用可能な2種類に分類される。学外と直接通信する必要のないクライアント、複合機、プリンタ、NAS アプライアンス、ネットワークカメラ、情報機器の管理インターフェース及び IoT 機器等に割り当てを行う。

- ・ IPv6 アドレスブロック・その他特殊用途の IP アドレスブロック

これらの IP アドレスブロックは実験及び本学以外の機関との連携や地域連携等に利用される。割り当ては必要に応じて情報基盤センターが行う。

5.2 IP アドレスの割り当て

IP アドレスの割り当て業務は、IP アドレス管理者が行う。以下の手順によって行うこと。

1. IP アドレスの割り当てを希望するシステム管理者は情報基盤センターが用意する申請書を記入し、IP アドレス管理者に申請する。
2. IP アドレス管理者は申請書を精査する。申請に問題がなければ、グローバル IP アドレスの場合は申請書を情報基盤センターに送付する。プライベート IP アドレスの場合は IP アドレスの割当を行う。
3. グローバル IP アドレスの割り当てを申請した場合、申請書は情報基盤センターに送られ、情報基盤センターで再精査を行い、問題がなければ IP アドレス管理者にグローバル IP アドレス割り当ての許可を連絡し、対外接続部のファイアウォールにてそのグローバル IP アドレスが通信可能となるよう設定を行う。
4. システム管理者は申請書に従って情報機器の設定と運用を行い、その結果を帳簿に記録する。
5. 情報基盤センターでは申請書を保存する。

5.3 IP アドレスの利用

システム管理者は IP アドレスの利用を終了したとき、速やかに利用を終了した旨を IP アドレス管理者に報告しなければならない。グローバル IP アドレスの場合、IP アドレス管理者は情報基盤センターに報告しなければならない。情報基盤センターは、IP アドレス管理者よりグローバル IP アドレスの利用終了の連絡を受けた場合は、速やかにファイアウォールの設定を変更して IP アドレスの不正利用を防止しなければならない。

IP アドレスは要求に応じて割り当てられるものである。システム管理者は利用しない IP アドレスを保有してはならない。動的に IP アドレスを割り当てる場合は、割り当てられた IP アドレスとその利用者を合致させる割当システムを利用しログを保存するべきである。

6. 情報システムの導入・利用・廃棄について

6.1 情報システムの導入

情報システムを導入する場合は、以下を検討のうえ計画を立てなければならない。

- ・ 導入する情報システムの管理責任者・管理者は誰か
- ・ 導入する情報システムの利用者は誰か
- ・ 導入する情報システムの利用期間はいつからいつまでか
- ・ 導入する情報システムの利用目的は何か
- ・ なぜその情報システムを導入しなければならないのか
- ・ 導入する情報システムはどこで利用されるか

これらに基づいて情報システムを選定しなければならない。選定の際には、導入する情報システムの以下のサポート期間に注意しなければならない。

- ・ ハードウェア
- ・ オペレーティングシステム、アンチウイルスソフトウェア、情報システム上で動作させる各種ソフトウェア等、情報システムを構成する上で必須のソフトウェア

特にサポート期間を終了したソフトウェアを用いてシステムの運用を行なうてはいけない。導入する情報システムの利用期間よりこれらサポート期間が短い場合は、それらのアップグレードをあらかじめ計画に含めておかねばならない。

可用性が必要とされる情報システムにおいては、多重化やサポート体制の強化等の必要な対策を行なわなければならない。

機密性が必要とされる情報システムは、鍵が厳重に管理された施錠される室内の施錠されるラック等に設置し、管理者以外の者が物理的に接触できないように設置すること。

6.2 情報システムの導入作業

情報システム導入作業は、

1. 必要な情報の収集
2. 管理者アカウント及びパスワード設定
3. オペレーティングシステム・ファームウェアのアップデート及びセキュリティ対策
4. アンチウイルスソフトのインストール及びアップデート
5. 各種ソフトウェアのインストール及びアップデート、カスタマイズ
6. ファイアウォールの設定
7. 動作確認
8. 作業の文書化・帳簿への追加
9. 利用者への開放及びその監視

の順序で行なうこと。マルウェアの侵入のないことを保証できるのであれば、作業順序は入れ替えても構わない。導入作業を終了した時点で、既知のマルウェアや攻撃に対して十分な耐性を持つ情報システムになっていなければならない。個人情報保有する情報システムの場合、学内から学外に対する通信をファイアウォールで制限して、情報漏洩を防がなければならない。

必要に応じて情報システムのバックアップを取得しておくのが望ましい。可用性が必要とされる情報システムにおいては定期的なバックアップの取得は必ず実施しなければならない。

ログを取得可能な機能を持つ情報システムでは必ずログを取得するように設定すること。保存期間は原則1年以上とする。

情報基盤センターでは、全学包括ライセンス契約を締結しているソフトウェアを配布している。利用条件が適合する場合は積極的に全学包括ライセンスを利用し、コストの削減を行なわなければならない。

6.3 情報システム管理業務

情報システムの管理業務として情報システムの利用者は以下の対策を日常的に行なうこと。

6.3.1 セキュリティ対策

オペレーティングシステム・アプリケーションソフトウェアのセキュリティ更新プログラムの適用

自動適用可能なように設定しておくことが望ましい。システム管理者は更新プログラムがリリースされた場合は、利用者に対し適用するよう指示を出さなければならない。

アンチウイルスソフトのウイルス定義ファイル等のアップデート

アップデート頻度が一日一回以上になるように自動適用を設定すること。利用者は情報システムの利用開始時にアンチウイルスソフトを確認し、動作していることと最新のウイルス定義ファイルが適用されていることを確認しなければならない。

利用しているオペレーティングシステム・アプリケーションソフトウェアのセキュリティ情報の取得及び確認

自分が利用しているオペレーティングシステム・アプリケーションソフトウェアの更新プログラム情報を入手できるようにすること。システム管理者は、自分の管理下にある情報システムのオペレーティングシステム・アプリケーションソフトウェアの利用状況を把握し、最新の更新プログラム情報を利用者に提供しなければならない。

6.3.2 ログの確認

ログを確認し不正アクセスや不正侵入、攻撃が発生していないかを確認する。不正アクセス等があった場合は直ちに報告を行ない必要な対策を講じる。攻撃がありそれを遮断している場合はそのログを確認し、必要な追加対策を検討する。

報告に関してはインシデントに対する対応を確認すること。

6.3.3 バックアップ

情報システムの重要度に応じバックアップ計画を策定し、定期的なバックアップを行なうこと。

6.4 情報システムの利用終了・廃棄業務

情報システムを利用終了する場合は以下の作業を行なわなければならない。また、当該情報システムにグローバル IP アドレスの割り当てを行っている場合は、以下の作業について情報基盤センター及び IP アドレス管理者に作業報告書を提出しなければならない。

- ・ 今後必要な情報の移動及びバックアップ
- ・ プライバシー情報・個人情報の削除
- ・ 情報システムが誤って利用されないための安全措置

利用終了した情報システムを再度利用する場合は、以下の作業を行わなければならない。IP アドレスの割り当てについては、新規の情報システムの導入作業と同様に行わなければならない。

- ・ 導入されているオペレーティングシステム・アプリケーション・アンチウイルスソフトウェアのサポート期間の確認。
- ・ オペレーティングシステム・アプリケーション・アンチウイルスソフトウェアのアップデート及びその他のセキュリティ対策
- ・ 利用者が異なる場合は、前の利用者の個人情報等が消去されずに残っていないかを確認する。可能であれば、ハードディスク等の記憶媒体を全て初期化の後オペレーティングシステムから再インストールして利用するのが望ましい。

情報システムを廃棄する場合は以下の作業を行わなければならない。

- ・ インストールされたソフトウェアのライセンスの確認。ライセンス登録の解除が可能なソフトウェアはライセンス登録を解除すること。
- ・ 破棄前にハードディスク等記憶媒体に記録された情報を全て判読が不可能な方法により消去すること。ハードディスクの場合はハードディスク消去機やハードディスク消去プログラムの利用、ハードディスクの物理的破壊を行なうこと。CD-ROM 等の光磁気メディアはシュレッダー等により破壊すること。
- ・ ハードディスク等記憶媒体の消去あるいは破壊を業者に委託する際は、信頼できる業者を選定し、立ち会うか、廃棄写真等付きの廃棄証明書を受け取る等の手段により消去あるいは破壊を確認することが望ましい。また、廃棄業務が再委託される場合には、事前承認の際に、廃棄方法を確認する。
- ・ 情報システムのハードウェアの廃棄に関しては経理調達課の指示に従うこと。
- ・ 破棄した情報システムに関しては帳簿にその旨を記録すること。

7. 情報システムの帳簿の整備

情報システム及びその上で動作するソフトウェアに関しては、研究室あるいは以下を必須とする部局等の単位で帳簿を作成し、記録しなければならない。帳簿の項目は

- ・ 情報システムに関しては以下の通り

ハードウェア名・導入年月日・備品番号・管理責任者名・管理者名・利用者名・利用目的・オペレーティングシステム・IP アドレス・利用場所の項目・廃棄年月日

・

有償ソフトウェアに関しては以下の通り

ソフトウェア名・購入ライセンス数・購入年月日・利用ライセンス数・インストールした情報システム名・メディア保管場所

IP アドレス管理者は、学外と直接接続可能なグローバル IP アドレスを持つ情報システムに関する帳簿を整備しなければならない。これを IP アドレス管理帳簿と呼ぶ。IP アドレス管理帳簿は管理運営部局である情報基盤センターと共有しなければならない。共有手段は情報基盤センターの指示に従うこと。

ハードウェア名・導入年月日・備品番号・管理責任者名・管理者名・利用者名・利用目的・オペレーティングシステム・IP アドレス・利用場所の項目・公開しているポート一覧

情報基盤センターと IP アドレス管理者は、IP アドレス管理帳簿に記載のないグローバル IP アドレスからの発信を観測した場合は、本学情報ネットワークの不正使用があると判定し、部局運用責任者や部局システム管理者と対応に当たる。

帳簿は変更がある度にアップデートすること。利用している情報システムの

実数と帳簿が正しく一致しなければならない。

8. 私物 PC の取扱いについて

職員は私有の PC を本学ネットワークに接続してはならない。また職員は本学の機密性情報を私有の PC にコピーしてはならない。

学生は私有の PC を部局システム管理者によって許可された学内ネットワークに接続することができる。ただし、部局システム管理者は以下を確認しなければならない。

- その PC には十分なセキュリティ対策を行なっていること
- 部局システム管理者はオペレーティングシステム・アプリケーションソフトウェアの更新プログラムの適用状況、アンチウイルスソフトのウイルス定義ファイルの更新状況を確認しなければならない。最新の更新プログラムを適用していない私物 PC は接続させてはならない。
- 利用が禁止されている P2P ファイル共有ソフトウェア等がインストールされていないこと。

匿名性 P2P ファイル共有ソフトウェアの学内での利用は禁止されている。私物 PC にはそれらのソフトウェアがインストールされている場合があり、特にバックグラウンドで自動起動し、利用者すら気が付かないうちにファイル共有を行なっている場合がある。部局システム管理者は注意深く確認しなければならない。

学生の私有 PC を接続するネットワークは、接続が制限されたネットワークであることが望ましい。プライベート IP ネットワークや接続ポートを制限したネットワークへ私有 PC を接続させること。NAT ルータに私物 PC を接続し、学外への接続性を確保する場合は研究等の特別な理由がない限り、学外への通信に対して接続ポートを制限しなければならない。

9. 情報の持ち出し・運搬・保存について

業務及び研究に利用するノート PC 等を学外に持ち出しあるいは運搬する場合は、必ず部局統括責任者の許可を得てから行なうこと。持ち出しあるいは運搬するノート PC は OS の機能等を利用して HDD の暗号化を行なうこと。HDD の暗号化ができないノート PC の持ち出しあるいは運搬は禁止する。

学務情報等機密性を有する情報を学外に持ち出しあるいは運搬してはいけない。特にそれらの必要がある場合は、必ず部局統括責任者の許可を得てから行なうこと。その際には十分な強度を持つ暗号化を施さなければならない。暗号化の手段としては以下等を利用すること。また、完全性を有する情報の場合は、電子署名の利用を検討すること。

- ・ OS の機能としての暗号化フォルダ
- ・ 各種ソフトウェアによるファイルの暗号化・ドライブの暗号化

機密性を有する情報を学内外で保存する場合は、暗号化を施し安全な場所に保管しなければならない。

暗号鍵はこれら暗号済情報とは別に保存・運搬しなければならない。

10. 学内ネットワーク以外の回線の利用について

短期間の携帯電話網及び広域 Wi-Fi 等の移動体通信の利用を除き、研究利用あるいは事務業務のために学内ネットワーク以外の回線を利用する場合は、その旨を部局運用責任者と情報基盤センターまで届け出なければならない。

研究目的の場合であっても、学内情報ネットワークにルーティングを行なってはならない。

11. 情報セキュリティインシデント対応について

情報システムセキュリティ責任者（以下「CISO」という。）と UEC-CSIRT は、情報セキュリティインシデントが発生したことを検出した場合に被害の拡大の防止と原因の究明のために必要な措置を行なうことができる。

- ・ 当該情報システムの学内外の通信の遮断
- ・ 当該情報システムの学内情報ネットワークへの接続の切断
- ・ 当該情報システム管理者への調査と対応依頼
- ・ 当該情報システム管理者への聞き取り調査
- ・ 当該情報システムの実地調査
- ・ 当該情報システムの記憶装置等の調査

学内情報システムに情報セキュリティインシデントが発生した場合は、CISO と UEC-CSIRT が主体となって、部局運用責任者、IP アドレス管理者とともに情報セキュリティインシデントに対応する。

11.1 情報セキュリティインシデント発生の把握

侵入検知システムを含む情報システムのログ情報、学外にある公開情報、学外からの通報等により、インシデントが発生したと確認する。

11.2 情報セキュリティインシデント発生の連絡と初動対応

部局運用責任者は、所管する情報システムにおいて情報セキュリティインシデントの発生を把握した場合は、速やかに UEC-CSIRT に連絡すること。

部局システム管理者は、担当する情報システムにおいて情報セキュリティインシデントが発生した場合は、被害の拡大を防止するため、別に定める【管理者向け】情報セキュリティインシデント発生時の対応マニュアルに従って行動すること。

12. 脆弱性診断について

UEC-CSIRT は、学内の情報システムについて、定期的に脆弱性診断を行ない、情報システムの脆弱性に関する情報収集を行ない、脆弱性のある情報システムが発見された場合は、部局運用責任者と部局システム管理者に対して改善勧告を行なう。当該情報システムの脆弱性が改善されない場合は、情報セキュリティインシデントの発生と同様の措置を行なうことができる。

13. 監査について

情報セキュリティ監査責任者は、定期的に部局運用責任者に対して、情報システムの運用状況とその情報セキュリティ維持に関する内部監査を実施する。

部局運用責任者は、部局システム管理者に対して内部監査に対応するよう指示を出さなければならない。

内部監査の結果は、CISO に報告すること。CISO は、その結果により情報システムの運用状況とその情報セキュリティ維持に関する改善勧告を行ない、本学内の情報システムの情報セキュリティを高水準に維持しなければならない。

14. 情報セキュリティ教育について

CIO は、管理運営部局に対して、本学の構成員に必要な情報セキュリティと情報倫理の定期的な教育に関する計画を立案実行させなければならない。管理運営部局は本学構成員に実行可能な情報セキュリティと情報倫理の教材を用意し、各部局に対して定期的に情報セキュリティと情報倫理の教育を実施するよう依頼すること。

特に 管理運営部局は、学生の新入生に対して情報セキュリティと情報倫理の教育を行なうよう各部局に依頼すること。

管理運営部局は、各部局が定めた情報セキュリティと情報倫理の教育を受講しない利用者に対して、本学情報ネットワークの利用の停止を含めた措置を行なうことができる。