平成30年　№13

○国立大学法人東京学芸大学情報システム管理運用規則の制定について

制定理由

国立大学法人東京学芸大学情報セキュリティポリシーに基づき，情報システムの管理及び運用に関する事項を定めるものである。

承認経過

平成30年２月８日　情報基盤整備推進本部会議　　審議・承認

平成30年３月14日　情報セキュリティ委員会　　審議・承認

国立大学法人東京学芸大学情報システム管理運用規則を次のように制定する。

平成30年３月15日

国立大学法人東京学芸大学長

出　口　利　定

平成30年規則第９号

国立大学法人東京学芸大学情報システム管理運用規則

国立大学法人東京学芸大学情報システム管理運用規則を別紙のとおり制定する。

国立大学法人東京学芸大学情報システム管理運用規則

（平成30年３月15日
規　則　第　９　号）

第１章　総則

（目的）

第１条　この規則は，国立大学法人東京学芸大学情報セキュリティポリシー（平成17年12月21日制定。以下「ポリシー」という）に基づき，情報システムの管理及び運用に関する事項を定めることにより，国立大学法人東京学芸大学（以下「本学」という）が有する情報資産を適正に保護・管理及び活用し，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。

（用語の定義）

第２条　この規則における用語の定義は，次に掲げるとおりとする。

(1) 利用者等　本学の教職員（非常勤職員を含む。），学生，研究生，附属学校の幼児，児童，生徒のほか，許可を受けて本学の情報資産及び情報システムを取り扱う者をいう。

(2) 主体認証　識別符号（ユーザID）を提示した利用者等又はクライアント機器が，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（ユーザID）とともに正しい方法で主体認証情報（パスワード）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クライアント機器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，この規則における「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。

(3) 識別符号（ユーザID）　主体認証を行うために，利用者等又はクライアント機器が提示する符号のうち，情報システムが利用者等又はクライアント機器を特定して認識する符号をいう。

(4) 主体認証情報（パスワード）　主体認証を行うために，利用者等又はクライアント機器が提示する情報のうち，情報システムが利用者等又はクライアント機器を正当な権限を有するものとして認識する情報をいう。

(5) 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，利用者等又はクライアント機器に付与された正当な権限をいう。

２　その他の用語の定義は，ポリシーの定めるところによる。

（適用範囲）

第３条　この規則は，本学の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ものとする。

（組織・体制）

第４条　情報システムの運用・管理は，ポリシー及び関係規程・手順等に従い，最高情報セキュリティ責任者の下，システム管理部会が連絡調整を行うものとする。

２　全学情報システムの管理責任は，全学システム管理責任者が負うものとする。

３　部局の情報システムの管理責任は，当該情報システムを管理し，又は運用する部局のシステム管理者が負うものとする。

（禁止事項）

第５条　部局システム管理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。

(1) 情報資産の目的以外の利用

(2) 守秘義務に違反する行為

(3) 部局情報セキュリティ管理責任者の許可（業務上の正当事由）なく情報ネットワーク上の通信を監視し，又はネットワーク機器及びクライアント機器の利用情報を取得する行為

(4) 部局情報セキュリティ管理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

(5) 管理者権限を濫用する行為

(6) 情報システムによる対外的不適切行為

(7) その他法令に基づく処罰の対象となる，又は損害賠償等の民事責任を発生させる行為

(8) 上記の行為を助長する行為

第２章　部局情報システムのライフサイクル

第１節　設置時

（管理者の設置）

第６条　情報システムを設置しようとする場合は，当該情報システムの管理・権限を有する者としてシステム管理者を定め，部局情報セキュリティ管理責任者の承認を得なければならない。

（セキュリティ対策の確保）

第７条　情報システムの設置時には，ポリシー及び関係規程・手順等に従い，情報システムのセキュリティを確保しなければならない。

（安全区域）

第８条　システム管理者は，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若しくは改ざん等のリスクを含む。）を把握し，サーバ機器及びネットワーク機器を設置した事務室，研究室，教室又はサーバルーム等において，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安全区域を設定しなければならない。

２　システム管理者は，安全区域に不審者を立ち入らせない措置を講じなければならない。

３　システム管理者は，情報の機密性を加味して，サーバ機器を安全区域に設置しなければならない。

４　システム管理者は，ネットワーク機器及び通信ケーブルを安全区域に設置しなければならない。

（文書の整備）

第９条　システム管理者は，所管する情報システムについて必要に応じて次に掲げる文書を整備し，業務上必要とする者のみ閲覧できる場所に保管する。また，利用者等に対し関連する項目について周知しなければならない。

(1) 当該情報システムの利用者等を特定するための文書

(2) 当該情報システム関連文書

(3) 当該通信回線及びネットワーク機器関連文書

（主体認証と権限管理）

第１０条　システム管理者は，利用者等が情報システムにログインする場合には主体認証を行うようにクライアント機器を構成しなければならない。

２　システム管理者は，ログオンした利用者等の識別符号（ユーザID）に対して，権限管理を行わなければならない。

（クライアント機器等の対策）

第１１条　システム管理者は，次に掲げる項目に対し，ポリシー及び関係規程・手順等に従い対策を取らなければならない。

(1) クライアント機器

(2) サーバ機器

(3) ネットワーク機器（端末機器）

（学内ネットワーク(GARNet)接続）

第１２条　システム管理者は，情報ネットワークを構築し運用するにあたっては，学内ネットワークとの整合性に留意しなければならない。

第２節　運用時

（管理・対策）

第１３条　システム管理者は，次に掲げる項目に対し，ポリシー及び関係規程・手順等に従い管理・対策を行なければならない。

(1) 情報コンテンツの管理

(2) 物理的セキュリティ対策

(3) 人的セキュリティ対策

(4) 技術的セキュリティ対策

（文書の見直し及び変更）

第１４条　システム管理者は，適宜，第９条に定める文書の見直しを行わなければならない。当該文書を改正した場合には，当該変更の記録を保存し，速やかに利用者等に周知しなければならない。

（運用管理）

第１５条　部局情報セキュリティ管理責任者及び部局システム管理責任者は，ポリシー及び関連規程・手順等に基づいて，当該情報システムの運用管理を行わなければならない。

（サーバ機器の対策）

第１６条　部局システム管理責任者は，定期的にサーバ機器の構成の変更を確認しなければならない。また，当該変更によって生ずるサーバ機器のセキュリティへの影響を特定し，対応しなければならない。

２　システム管理者は，安定性を必要とする情報を取り扱うサーバ機器に保存されている情報コンテンツを定期的にバックアップしなければならない。また，取得した情報を記録した媒体は，安全に管理しなければならない。ただし，事務情報システムについては，別に定める。

３　システム管理者は，サーバ機器の運用管理について，作業日，作業を行ったサーバ機器，作業内容及び作業者を含む事項を記録しなければならない。

４　システム管理者は，サーバ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しなければならない。

５　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，サーバ機器の時刻を同期しなければならない。

（情報システムの見直し）

第１７条　部局システム管理責任者は，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，必要な措置を講じなければならない。

第３節　運用終了時

（サーバ機器，ネットワーク機器の対策）

第１８条　システム管理者は，運用終了時にはポリシー及び関係規程・手順等に従い，全ての情報を復元が困難な状態にしなければならない。

第３章　アクセス制御

（アクセス制御等）

第１９条　システム管理者は，次に掲げる項目に対し，ポリシー及び関係規程・手順等に従い対応しなければならない。

(1) 主体認証

(2) アクセス制御

(3) アカウント管理

(4) 証跡管理

（証跡管理に関わる個人情報の取得及び管理）

第２０条　システム管理者は，証跡管理に関わる個人情報の取得及び管理に対し，ポリシー及び関係規程・手順等に従い対応しなければならない。

第４章　違反と例外措置

（違反行為の発見・報告）

第２１条　情報システムの利用規則に違反する行為（以下「違反行為」という。）を発見又はその報告を受けた者は，本学情報セキュリティインシデント対応手順書，及び情報セキュリティ委員会が定めた緊急時対応に従い対応しなければならない。

（違反行為への対応）

第２２条　最高情報セキュリティ責任者は，違反行為の報告を受けた場合及び自らが違反行為を知った場合には，速やかに調査を行い，事実を確認しなければならない。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　最高情報セキュリティ責任者は，調査によって違反行為が判明したときには，次に掲げる措置を講ずることができる。措置を講じるかの判断にあたっては，必要に応じて情報セキュリティ委員会の判断を求めるものとする。

(1) 当該行為者に対する当該行為の中止命令

(2) 部局システム管理責任者に対する当該行為に係る情報発信の遮断命令

(3) システム管理者に対する当該行為者のアカウント停止命令又は削除命令

(4) キャンパス情報ネットワークに対する緊急遮断措置

(5) その他法令に基づく措置

３　当該行為を行った者が前項の措置に従わない場合には，本学学則及び本学職員就業規則等に基づき対応しなければならない。

４　最高情報セキュリティ責任者は，第２項第２号及び第３号については，部局情報セキュリティ管理責任者を通じて同等の措置を依頼することができる。

５　部局情報セキュリティ管理責任者は，第２項と同等の措置を講じた場合は，遅滞なく最高情報セキュリティ責任者にその旨を報告しなければならない。

（例外措置）

第２３条　利用者等は，やむを得ない理由により例外措置の適用を受けようとする場合は，最高情報セキュリティ責任者に申請することができる。

２　最高情報セキュリティ責任者は，利用者等による例外措置の適用の申請があった場合，情報セキュリティ委員会の議を経て，適用の可否を決定しなければならない。また，決定の際に，次の項目を含む例外措置の適用審査記録を作成する。

(1) 決定を審査した者の情報（氏名，役職名，所属，連絡先）

(2) 申請内容

イ　申請者の情報（氏名，所属，連絡先）

ロ　例外措置の適用を申請する情報セキュリティ関係規程等の該当箇所（規程等名と条項等）

ハ　例外措置の適用を申請する期間

ニ　例外措置の適用を申請する理由

ホ　例外措置の適用を申請する措置内容（講ずる代替手段等）

ヘ　例外措置の適用を終了した旨の報告方法

(3) 審査結果の内容

イ 許可又は不許可の別

ロ　例外措置の適用を許可した情報セキュリティ関係規程等の適用箇所（規程等名と条項等）

ハ　許可又は不許可の理由

ニ　例外措置の適用を許可した期間

ホ　許可した措置内容（講ずるべき代替段等）

ヘ　例外措置を終了した旨の報告方法

３　最高情報セキュリティ責任者は，例外措置の適用を許可した期間の終了日に，許可を受けた者からの報告の有無を確認し，報告がない場合には許可を受けた者に状況を報告させ，必要な対応を講じなければならない。ただし，最高情報セキュリティ責任者が報告を要しないと判断した場合は，この限りでない。

第５章　インシデント対応

（インシデント対応）

第２４条　最高情報セキュリティ責任者は，情報セキュリティインシデントが発生した場合は，セキュリティインシデント対応手順書，及び情報セキュリティ委員会が定めた緊急時対応等に従って対応しなければならない。

第６章　外部に委託し使用する情報システム

（外部に委託し使用する情報システムにかかる安全管理措置の整備）

第２５条　最高情報セキュリティ責任者は，情報システム業務の全て又はその一部を第三者に委託し行う場合は，当該第三者による安全管理措置についての規則を整備しなければならない。

２　部局システム管理責任者又はシステム管理者は，機密性のある情報について，外部委託の情報システムにより情報処理を行う場合に安全管理が確保されるよう必要な措置を講じなければならない。

第７章　教育・研修

（情報セキュリティ対策の教育）

第２６条　最高情報セキュリティ責任者は，教職員等に対し，情報セキュリティ対策の教育を実施しなければならない。

２　情報セキュリティ対策に関する教育については，情報セキュリティ委員会が策定する情報セキュリティ教育計画に従い実施しなければならない。

第８章　評価

（自己点検に関する年度計画の策定）

第２７条　最高情報セキュリティ責任者は，情報セキュリティ委員会の議を経て，自己点検に関する年度計画を策定しなければならない。

（自己点検の実施に関する準備）

第２８条　部局情報セキュリティ管理責任者は，職務従事者ごとの自己点検の実施手順及び自己点検票を整備しなければならない。

（自己点検の実施）

第２９条　部局情報セキュリティ管理責任者は，最高情報セキュリティ責任者が定める自己点検に関する年度計画に基づき，職務従事者等に対して，自己点検の実施を指示しなければならない。

２　職務従事者等は，部局情報セキュリティ管理責任者から指示された自己点検の実施手順及び自己点検票を用いて自己点検を実施しなければならない。

（自己点検結果の評価）

第３０条　部局情報セキュリティ管理責任者は，職務従事者等による自己点検が行われていることを確認し，その結果を評価しなければならない。

２　最高情報セキュリティ責任者は，部局情報セキュリティ管理責任者による自己点検が行われていることを確認し，その結果を評価しなければならない。

（自己点検に基づく改善）

第３１条　職務従事者等は，自らが実施した自己点検の結果に基づき，自己の権限の範囲で改善できると判断したことは改善し，部局情報セキュリティ管理責任者にその旨を報告しなければならない。

２　最高情報セキュリティ責任者は，自己点検の結果を全体として評価し必要があると判断した場合には，部局情報セキュリティ管理責任者に改善を指示しなければならない。

（監査に対する協力）

第３２条　部局情報セキュリティ管理責任者その他の関係者は，最高情報セキュリティ責任者の行う監査の適正かつ円滑な実施に協力しなければならない。

第９章　雑則

（規則の改廃）

第３３条　この規則の改廃は，情報セキュリティ委員会の議を経て学長が定める。

（雑則）

第３４条　この規則に定めるもののほか，情報システムの管理及び運用に関し必要な事項は，別に定める。

附　則

この規則は，平成30年４月１日から施行する。