国立大学法人東京学芸大学
情報セキュリティガイドライン

令和６年４月

目　次

１．はじめに
２．情報コンテンツの管理
　２．１　非公開情報コンテンツ
　２．２　公開情報コンテンツ
　２．３　非公開情報コンテンツの開示
　２．４　原本性の保証
　２．５　記録媒体の管理
　２．６　記録媒体の処分
３．物理的セキュリティ
　３．１　クライアント機器（端末機器）
　３．２　サーバ機器
　３．３　ネットワーク機器
　３．４　災害への対策
４．人的セキュリティ
　４．１　情報の機密保持
　４．２　アカウント及びパスワード管理・ログ管理
　４．３　非常勤職員，臨時職員等の雇用の際の指導
５．技術的セキュリティ
　５．１　コンピュータ及びネットワークの管理
　５．２　情報システムの使用上の留意点
　５．３　アクセス制御
　５．４　システムの開発，導入等
　５．５　情報システム仕様書等の管理
　５．６　コンピュータウイルス対策
　５．７　セキュリティ情報の収集
６．運用
　６．１　情報システムの監視及びポリシーの遵守状況の確認
　６．２　運用管理における留意点
　６．３　外部委託による運用契約
７．インシデント対応

東京学芸大学情報セキュリティインシデント対応体制（緊急時）

１．はじめに

国立大学法人東京学芸大学（以下「本学」という。）の全ての構成員は，本学における情報資産の情報セキュリティを確保するために，国立大学法人東京学芸大学情報セキュリティポリシー（以下「ポリシー」という。）に従わなければならない。

ついては，本学の情報資産に対する情報セキュリティの確保を実現するための具体的対策基準書として，ポリシーに基づき「国立大学法人東京学芸大学情報セキュリティガイドライン」を定める。

特に重要な情報資産を運用する部局においては，このガイドラインに準じて，それぞれの実態に合わせた個別の情報セキュリティガイドライン（以下「個別ガイドライン」という。）を策定しなければならない。

なお，以下に用いる用語は，ポリシーで規定された「用語の定義」に従うものとするが，情報コンテンツは，電磁媒体等に記録された情報に限定する。

２．情報コンテンツの管理

情報コンテンツの漏洩，紛失，盗難，破壊等が起こらないように，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，当該部局の全ての構成員（以下「部局の構成員」という。）に対して，日頃から以下のことに関し適切な指導を行うこと。なお，業務の全部又は一部を外部委託する場合は，委託業者に対しても以下のことに関し適切な指導をすること。

２．１　非公開情報コンテンツ

非公開情報コンテンツとは，個人情報，特定個人情報及び本学の運営にとって重要な機密情報をいい，その情報コンテンツが不正に流出することで，個人のプライバシーに被害を与え，並びに大学運営にとって甚大な損害を被ることになるもので，以下のとおり厳密な管理・運用を行うこと。

１）アクセス制限

非公開情報コンテンツには，許可された者以外がアクセスしてはならない。システム管理者以外は，アプリケーションシステムからのアクセスに限定する。データへのアクセスレベルは厳密に設定する。

非公開情報コンテンツを扱うネットワークは，一般のネットワークとは論理的に分離する。相互に接続する場合は，非公開情報ネットワークからのみアクセス可能とする。

２）複製の禁止

非公開情報コンテンツは，教職員が日常的に使用しているコンピュータ等他の記録媒体に複製してはならない。

３）利用場所の制限

非公開情報コンテンツは，利用する場所を制限する等の対応を行い，利用を許可された場所から外部に持ち出してはならない。

４）暗号化

非公開情報コンテンツを保存する場合には，暗号化することが望ましい。

５）第三者への開示

業務の外注等のため，第三者に開示する必要がある場合は，開示の都度，守秘義務契約を結ぶ。

６）アクセスログの作成及び分析

非公開情報コンテンツへのアクセスログを作成し，一定期間保存する。定期的又は随

意にアクセス記録を分析する。

２．２　公開情報コンテンツ

公開情報コンテンツは，任意の場所からアクセス可能な性質を持つため，情報の改ざん及び破壊が行われないように適切に管理されなければならない。

２．３　非公開情報コンテンツの開示

「独立行政法人等の保有する情報の公開に関する法律」及び「独立行政法人等の保有する個人情報の保護に関する法律」に基づく開示請求等による非公開情報コンテンツを開示する場合には，個人情報の漏洩，プライバシー及び著作権の侵害に十分注意し，開示できる情報コンテンツだけを抽出又は開示してよいかたちに加工する等の措置を講じる。

２．４　原本性の保証

情報コンテンツの原本は，ＣＤ－Ｒ，ＤＶＤ－Ｒ等への書換え，追記不可能な記録媒体に保存する等により原本性を維持する。

情報コンテンツは，複製又は加筆による偽情報の作成及び流布を防止するため，電子署名等により原本性の保証に努める。

２．５　記録媒体の管理

非公開情報コンテンツを記録した記録媒体は，盗難や部外者の持ち出し等を想定し，施錠等により入室が制限された安全な場所で保管する。

非公開情報コンテンツを記録した記録媒体を，部局内から外部に持ち出す場合は，当該情報コンテンツを入手し，又は作成した部局の当該教職員（事務局にあっては，当該課長）の許可を得て行う。

管理責任者の許可のもと，学外へ記録媒体を持ち出す際は，移動中等に紛失，盗難にあわないよう十分に注意する。

記録媒体の紛失，盗難に備え，個人情報等を含むデータにはパスワード，暗号化等のセキュリティ対策を施し，悪意のある第三者が入手しても内容を閲覧，複写できないように対策する。

利用者は，記録媒体の紛失，盗難等が起こらないように，記録媒体の保管状況・管理について使用の都度，確認を行う。

取り外しが可能な記録媒体は，盗難，紛失等に対する安全性を確保するために，適切な管理を行う。

特に，本学の保有する個人情報，入試情報を USB メモリ等に記録し取り扱う際は，以下のセキュリティ対策を行う。

・USB メモリ等にパスワードロック機能を備えたものを使用する。

・その中に格納するファイルにもパスワードを設定する。

セキュリティ対策の行われていない USB メモリ等で本学の保有する重要情報を取り扱ってはならない。

なお，やむを得ず上記セキュリティ対策の行われていない USB メモリ等を使用する場合は，情報セキュリティ会議の承認を得ること。

２．６　記録媒体の処分

情報機器又は記録媒体を廃棄する場合は，当該媒体に記録された情報コンテンツが復元できないように消去又は裁断を行い廃棄する。

非公開情報コンテンツを記録した記録媒体の廃棄は，当該情報コンテンツを入手し，又は作成した部局の当該教職員（事務局にあっては，当該課長）の許可を得て行う。

３．物理的セキュリティ

情報システムの紛失，盗難，破壊等が起こらないように，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，部局の構成員に対して，日頃から以下のことに関し適切な指導を行うこと。なお，業務の全部又は一部を外部委託する場合は，委託業者に対しても以下のことに関し適切な指導をすること。

また，システム管理者は，３．２以下の対策を講じなければならない。

３．１　クライアント機器（端末機器）

１）クライアント機器の使用

クライアント機器として本学のネットワークへ接続するパーソナルコンピュータ等（以下「ＰＣ」という。）は，「５．６ コンピュータウイルス対策」を講じていなければならない。また，ネットワークへ接続する場合は，認証を経ること。

２）盗難防止

教室及び研究室に据置きの情報機器の盗難を防止するため，ワイヤーロックの設置，設置場所の施錠等，盗難防止の措置を講じる。

学生等が携帯するＰＣについては，学生等自ら盗難防止に努めるほか，教職員は，学生等に対しＰＣの管理情報（製品番号等）の記録，ログインパスワードの設定，スクリーンセーバーのパスワードロック，重要ファイルの暗号化等のセキュリティ対策を講じるように指導する。

３．２　サーバ機器

１）設置場所

サーバ及びコンソールは，設定された管理区域内（サーバ類の動作補償範囲内の温度及び湿度が24時間保持され，認証及び入退室記録が残される物理的に隔離された区域）に設置する。

管理区域内の物理的な場所は，当該サーバ機器等のシステム管理者以外には公開してはならない。軽微なサーバ機器類については，必要に応じて，鍵等による入退室管理が行えるようにする。

２）電源

サーバ機器は，電源の二重化又は無停電電源装置により，電源故障，瞬停及び過電流への対応を図る。

３）機器の修理，廃棄等

保守契約又はレンタル期間の終了に伴い情報機器を交換又は撤去する場合は，記録内容の完全消去を実施するか，それを業者に指示する。

また，機器の修理等で外部の業者に依頼する際，記録内容を消去することが困難な場合は，依頼業者に対し守秘義務契約を結ぶ。

完全消去とは，記録媒体を物理的に破壊すること，全記録領域を無作為な数値データで埋める等，いかなる手段を用いても記録内容を復元できないようにすることである。

４）保守

保守においては，保守部品をできるだけ確保する等，迅速に対応できる体制を整える。業者に保守を依頼する場合は，パスワード，システム設定情報等の非公開情報の開示についての守秘義務契約を結ぶ。

３．３　ネットワーク機器

１）設置場所

バックボーンを構成する機器をはじめ，セキュリティ上重要と思われるネットワーク機器については，物理的に隔離した区域に設置しなければならない。設置場所は，当該ネットワーク機器等のシステム管理者以外には公開してはならない。

２）多重化

機器の障害によるネットワーク切断によって，重大な影響を及ぼすようなネットワーク機器については，多重化により信頼性の向上を図る。

３）保守

保守においては，保守部品をできるだけ確保する等，迅速に対応できる体制を整える。業者に保守を依頼する場合は，パスワード，ネットワーク構成情報等の非公開情報の開示についての守秘義務契約を結ぶ。

３．４　災害への対策

サーバ機器及びネットワーク機器については，耐震を考慮した据付けを行う。また，重要管理区域には，火災の一次消火手段を備える。

４．人的セキュリティ

情報資産の適切な管理を行うために，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，部局の構成員に対して，日頃から以下のことに関し適切な指導を行うこと。なお，業務の全部又は一部を外部委託する場合は，委託業者に対しても以下のことに関し適切な指導をすること。

４．１　情報の機密保持

１）認証情報の管理

本学の情報資産にアクセスするために発行されている認証情報（ＩＤ及びパスワード）は，交付を受けた本人だけが使用し，他の者に貸与又は公開してはならない。

２）外部委託

学外の業者等に情報システムの開発又は運用管理を委託する場合は，委託業者に対して，業務を下請負させる場合も含めてポリシー及びこのガイドライン（個別ガイドラインを含む。以下同じ。）を遵守する義務があることを認識させ，遵守されなかった場合の規定を契約書等に明記する。

委託業者は，情報セキュリティを遵守できる技術的能力及び信頼性をもつ業者でなければならない。

３）教職員の異動又は退職時の対応

情報セキュリティに係る教職員等が，異動，退職等で業務を離れる場合，当該職員は，知り得た情報を外部に漏らしてはならない。

４．２　アカウント及びパスワード管理・ログ管理

１）一般利用者

不正アクセスを防止するために，情報システムを利用する全ての者は，厳格にパスワードを管理しなければならない。パスワードについては，以下の点を考慮して設定し，使用する。

(1) 簡単な単語のみをパスワードとしたり，利用者の個人情報から容易に想定できる名前，生年月日等の文字列をパスワードに使用しない。

(2) パスワードの秘密保持に努め，不用意に漏らしたり，メモを作成したりしない。

(3) パスワードは適宜に，又はアクセス回数に基づいて変更する。

(4) 古いパスワードの再利用はしない。

(5) 英（大・小文字）数字・特殊文字のいずれかの組合わせによる８文字以上の適切な長さのパスワードを設定する。

２）共有アカウントの管理者

情報システムのアカウントを一組織（複数の利用者）において共有する場合は，利用対象者の変更や異動に伴い都度パスワードの変更をする。

３）システム管理者

(1) 管理者用のパスワードは，頻繁に変更しなければならない。

(2) 情報資産の重要度に応じて利用資格のレベルを定め，アカウント及びパスワードを設定する。

(3) 情報システムの利用資格を有しない者にアカウント及びパスワードを発行してはならない。また，利用資格を失った場合は，直ちに削除する。

(4) アカウント及びパスワードを漏らしてはならない。

(5) ログ情報及び通信内容の解析等に当たっては，利用者のプライバシーに配慮する。

４．３　非常勤職員，臨時職員等の雇用の際の指導

教職員は，非常勤職員，臨時職員等にも情報セキュリティ確保の観点から，ポリシー及びこのガイドラインの遵守について理解させる。

５．技術的セキュリティ

情報資産の適切な管理を行うために，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，部局の構成員に対して，日頃から以下のことに関し適切な指導を行うこと。なお，業務の全部又は一部を外部委託する場合は，委託業者に対しても以下のことに関し適切な指導をすること。

５．１　コンピュータ及びネットワークの管理

システム管理者は，以下の事項の対策を講じなければならない。

１）ネットワーク管理

ファイアウォール，侵入検知防御その他必要なネットワークセキュリティ機器・システムを導入・運用し，外部からの脅威及び外部への攻撃等に対処する。これらの機器・システムは，ネットワーク性能の向上及び新たな脅威に対応できるように，最新のものを維持する。

２）アクセスログの作成及び分析

サーバ機器及びネットワークセキュリティ機器については，アクセスログを作成し，一定期間（３月以上）保存する。

また，定期的にそれらを分析し，監視する。アクセスログの改ざん，盗難，破壊等を防止するために必要な措置を講じる。

３）ネットワークバックドアの排除

管理上，必要不可欠でない限り，バックドアを設置してはならない。

４）情報のバックアップ

サーバ機器に記録される情報コンテンツは，不測の事態に備えて，定期的にバックアップしなければならない。バックアップのスケジュールは，情報資産の重要度に応じて決定する。情報コンテンツをバックアップした媒体は，認証による入退館管理が行われている管理区域内に保管する。重要な情報コンテンツについては，バックアップを複数作成し，物理的に離れた場所に個々に保管する等の対策を講じる。

５．２　情報システムの使用上の留意点

１）目的以外の使用の原則禁止

部局の構成員は，職務上の目的以外での情報システムへのアクセス，メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

２）業務上のデータの持ち出し禁止

部局の構成員は，分類上，非公開情報コンテンツに該当する業務上のデータを学外に持ち出してはならない。また，サーバ機器等の設置場所に，個人の所有するデータが記録された媒体を持ち込んではならない。ただし，当該構成員が所属する部局の長の許可がある場合は，この限りでない。

３）無許可ソフトウェアの導入の禁止

部局の構成員は，各自に供用されたパソコンに対して，セキュリティ上好ましくないソフトウェアの導入を行ってはならない。特に，ネットワーク上の情報を盗聴するような監視ソフトウェア並びにネットワークの状態を探索するセキュリティ関連のソフトウェア及びハッキングソフトウェアの使用は厳禁する。

４）機器構成の変更の禁止

部局の構成員は，各自に供用されたパソコンに対して，セキュリティ上好ましくない機器の増設及び改造を行ってはならない。特にモデム等の機器を増設して，他の環境（インターネット等）へのネットワーク接続を行うこと及び学外からのアクセスを可能とする仕組みを構築することは禁止する。

５．３　アクセス制御

システム管理者は，情報資産の重要度により，アクセスに係る認証機能（パスワード，ＩＣカード，生体情報等により権限を識別する機能）の設定，不要になったＩＤの速やかな削除等アクセス制御のために必要な措置を講じる。

１）管理者権限

情報システムの管理権限は，必要最小限の者に与え，厳重に管理する。

２）外部からのアクセス

外部からのアクセスの許可は，必要最小限にする。

モバイル端末等からのアクセス方法，使用方法等に関しては，利用者の真正性を確保するための必要な措置を講ずる。

メンテナンスのための外部からの接続口を設ける場合には，十分なセキュリティ対策を講ずる。

外部とのネットワーク接続点には，アクセス制限，サービスの制限，プロトコルの制限等を行い，適切に管理する。

３）自動識別

無線ＬＡＮを利用する場合には，ユーザ又は端末機器の認証及び十分な強度の暗号化を行う。

４）ログイン手順

ログイン手順中におけるメッセージ，ログイン試行回数の制限，アクセスタイムアウトの設定，ログイン・ログアウト時刻の表示等，利用者の適切なログイン手順を定める。

５．４　システムの開発，導入等

新たにシステムの開発，導入及び更新を行う場合は，ポリシー及びこのガイドラインに従い，情報セキュリティ対策として必要な事項をシステム仕様書に記載する。導入の際には，記載した必要事項を満たしているかどうか確認する。

５．５　情報システム仕様書等の管理

システム管理者は，ネットワーク構成図及び情報システム仕様書については，記録媒体に関わらず，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，その閲覧者は，当該資料内容の守秘に努める。

５．６　コンピュータウイルス対策

システム管理者は，コンピュータウイルスに感染することを防止するため，以下の対策を講じる。

(1) システムのセキュリティホール（脆弱性）に対応するために，CERT/JPCERT 等の情報に基づき，最新の状態を保持する。

(2) ウイルス対策の行われていないＰＣをネットワークに接続させてはならない。

(3) セキュリティ上好ましくないソフトウェアの導入を禁止する。

(4) 外部ネットワークからファイル及びソフトウェアをダウンロードする際には，サーバ側及び端末側においてウイルス対策ソフトウェアを実行させるように指導する。

(5) サーバ側及び端末側のウイルス対策ソフトウェアについては，常に最新のものにバージョンアップするとともに，ウイルス情報の更新を頻繁に行う。

(6) 重要なソフトウェア，情報システム及び情報について，その内容を定期的に確認する。

５．７　セキュリティ情報の収集

セキュリティホールは，日々発見されることから，セキュリティに関する情報を積極的に収集し，対策を講じる。

１）情報収集の体制

セキュリティ情報は，情報基盤課が収集・分析し，必要に応じて，利用者に周知する。

２）情報収集先

セキュリティ情報の収集に当たっては，以下の組織から出される注意喚起情報を対象とする。

(1) ＩＰＡセキュリティセンター（http://www.ipa.go.jp/security/）

(2) 文部科学省大臣官房政策課情報化推進室（http://shinko-www.mext.go.jp/）

(3) CERT/CC（http://www.cert.org/）

(4) JPCERT/CC（http://www.jpcert.or.jp/）

６．運用

６．１　情報システムの監視及びポリシーの遵守状況の確認

１）情報セキュリティ会議の指示により，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，情報システム等の運用が，ポリシー及びこのガイドラインに従って，セキュリティ対策が適切に実施されているかどうか，問題が発生していないかについて，定期的に確認する。

２）情報システム等や一般利用者の使用するソフトウェアに重大な問題が確認され，緊急対応として，被害状況等の調査のためにアクセス記録等から個人を特定する必要がある場合は，最高情報セキュリティ責任者の指示のもと，TGU-CSIRT で対応し，情報セキュリティ会議に報告する。

３）情報セキュリティ上重大な問題が発生するおそれのあるポリシー及びこのガイドラインに対する違反が発見された場合は，「情報セキュリティインシデント対応体制（緊急時）」及び「情報セキュリティインシデント対応手順書」に従って処理する。これらの結果は，侵害事案の証拠となるほか，ポリシー及びこのガイドラインの実効性を図

る資料となるので，厳重に保管し，評価・見直しの際に活用する。

６．２　運用管理における留意点

１）個人のプライバシーに係る情報を閲覧する場合は，最高情報セキュリティ責任者又はその指名する者の許可を得なければならない。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きによる。

２）情報セキュリティ上の問題が起こりうる個人のプライバシーに係る情報に対し，最高情報セキュリティ責任者又はその指名する者から閲覧の許可を受けた場合であっても，最高情報セキュリティ責任者又はその指名する者の立会いがない場合には，教職員等個人のプライバシーに係る情報を閲覧してはならない。

３）部局情報セキュリティ管理責任者は，情報システムの活用等を通じ，教職員が常にポリシー及びこのガイドラインを参照できるように配慮する。

６．３　外部委託による運用契約

１）情報システムの開発，管理，保守等及び情報コンテンツの処理，保管等を外部委託する場合は，委託に関する責任を有する部署を明確にする。

２）委託業者に対して，業務を下請負させる場合も含めてポリシー及びこのガイドラインに定める内容を遵守する旨を明記した契約書を締結する。

３）委託に関する責任を有する部署は，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，その内容を部局情報セキュリティ管理責任者に報告する。

７．インシデント対応

事故及び欠陥等を発見、又は通報等により認知した場合は、本学の情報セキュリティインシデント対応体制（緊急時）により関係者に報告するとともに、情報セキュリティインシデント対応手順書により対応する。

特に，重大な事案が発生したときは，TGU-CSIRT 責任者は，最高情報セキュリティ責任者及び全学システム管理責任者に報告する。

最高情報セキュリティ責任者は，緊急対策室を設置し，「コンピュータセキュリティインシデントへの対応」[注)] に準拠して対策を講じる。

注）技術メモ　コンピュータセキュリティインシデントへの対応
初版: 1999-12-09　(Ver.01: JPCERT-E-TEC-99-0002-01)
発 行 日: 2002-06-06　(Ver.04)
最新情報: http://www.jpcert.or.jp/ed/2002/ed020002.txt

附　則

このガイドラインは，平成 17 年 12 月 21 日から施行する。

附　則

このガイドラインは，平成 20 年 4 月 26 日から施行する。

附　則

このガイドラインは，平成 23 年 3 月 31 日から施行する。

附　則

このガイドラインは，平成 27 年 3 月 26 日から施行する。

附　則

このガイドラインは，平成 29 年 3 月 16 日から施行する。

附　則

このガイドラインは，平成 31 年４月 26 日から施行し，平成 31 年４月１日から適用する。

附　則

このガイドラインは，令和２年４月１日から施行する。

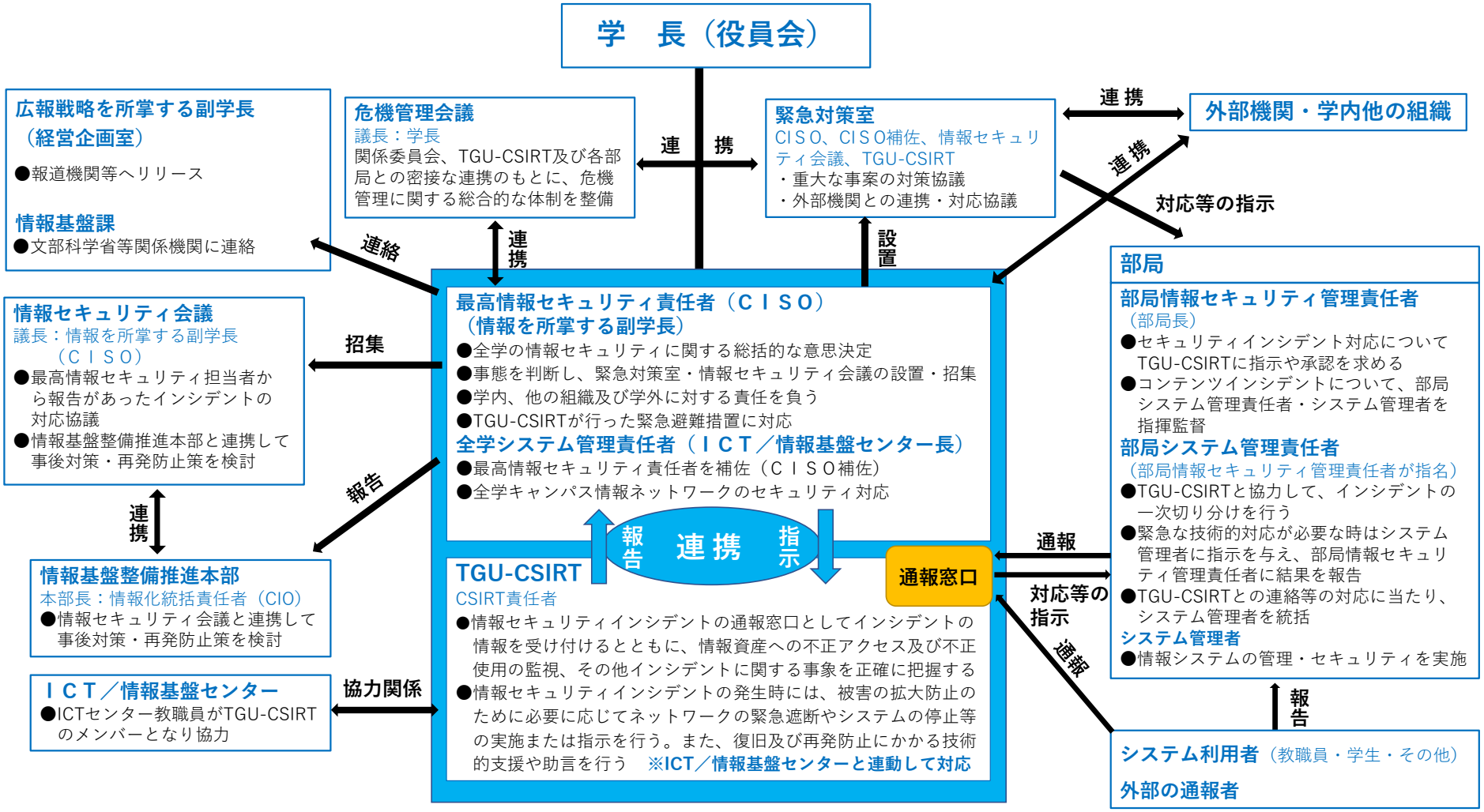
附　則

このガイドラインは，令和２年５月７日から施行し，令和２年４月１日から適用する。

附　則

このガイドラインは，令和５年４月１日から施行する。

附　則

このガイドラインは，令和６年４月１日から施行する。

東京学芸大学情報セキュリティインシデント対応体制（緊急時）