国立大学法人東京学芸大学
情報セキュリティインシデント
対応手順書

令和６年４月

情報セキュリティインシデント対応手順書

目次

１．定義

（１）インシデント

物理的インシデント，セキュリティインシデント及びコンテンツインシデントを言う。

（２）物理的インシデント

地震等の天災，火災，事故，盗難等によるネットワークを構成する機器や回線の物理的損壊や滅失及びその他の物理的原因による情報システムやネットワークの機能不全や障害等，情報セキュリティの確保が困難な事由の発生及びそのおそれを言う。

（３）セキュリティインシデント

ネットワークや情報システムの稼動を妨害し，又はデータの漏えい，改ざんや消失を起こす行為及び利用行為の形態自体には問題は無いが，ネットワークの帯域やディスクやCPUの資源を浪費するなど，ネットワークやシステムの機能不全や障害又は他の利用者の迷惑となる行為による情報セキュリティの確保が困難な事由の発生及びそのおそれを言い，次の原因によるものを含む。

－大量のスパムメールの送信

－コンピュータウイルス等のマルウェアの蔓延や意図的な頒布

－発信者を偽った電子メールへのファイル添付や偽装したURL への誘導などにより，利用者の環境に利用者の意図しないアプリケーション等をインストールさせる行為

－情報システムの脆弱性や利用者による不適切なアカウント管理等を利用することにより，ネットワークや情報システムのセキュリティに影響を及ぼす行為

－不正アクセス禁止法に定められた特定電子計算機のアクセス制御を免れる行為

－サービス不能攻撃その他部局の長の要請に基づかずに管理権限のない情報システムのセキュリティ上の脆弱性を検知する行為

－利用規則により禁止されている形態でのP2Pソフトウェア（ファイル共有ソフト）の利用

－禁止された方法による学外接続

－学内ネットワークへの侵入を許すようなアカウントを格納したPCの盗難・紛失

－管理上の過失による秘密情報（個人情報を含む。）の漏えい，データの消失又は改ざん

（４）コンテンツインシデント

ネットワークを利用した情報発信内容（以下「コンテンツ」と言う。）が著作権侵害

等の他人の権利侵害や児童ポルノ画像の公開等の違法行為又は公序良俗違反である行為（及びその旨主張する被害者等からの請求）による事故を言い，次の原因によるものを含む。

－ソーシャルネットワーキングサービス（電子掲示板，ブログ等を含む。）やウェブページ等での他人及び本学の名誉・信用毀損にあたる情報の発信

－他人の個人情報や肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信

－通信の秘密を侵害する行為

－他人の著作物の違法コピーのアップロード等，他人の著作権等の知的財産権を侵害する情報の発信

－秘密であるデータやプログラムの不正公開等守秘義務に違反する情報の発信

－児童ポルノやわいせつ画像の公開

－ネットワークを利用したねずみ講

－差別，侮辱，ハラスメントにあたる情報の発信

－営業ないし商業を目的とした本学情報システムの利用行為

（５）対外的インシデント

インシデントのうち，利用者等による行為であって，外部ネットワークにおけるあるいは外部のシステムに対して行われた行為による事故，事件を言う。

（６）対内的インシデント

インシデントのうち，外部のネットワークから内部に向かって行われた行為による事故，事件を言う。

（７）学外クレーム

学内の利用者等による情報発信行為（本学の業務としてなされたものを除く。）の問題を指摘しての連絡・通報及び学外(学内の者が，弁護士等の代理人を立てる場合も含む)からの発信中止を求める要求，損害賠償の請求，謝罪広告の請求，発信者情報の開示請求等の民事的請求及び証拠，証言の収集や犯罪捜査等にかかわる協力要請や強制的命令を言う。

（８）対外クレーム

対内的インシデントに対し，学外の発信者に対して連絡・通報し，又は発信中止を求める要求，損害賠償の請求，謝罪広告の請求，発信者情報の開示請求等の民事的請求及び当局に犯罪捜査の告訴・告発をすることを言う。

（９）緊急連絡網

インシデント及び障害等に備えて，その部局の情報システム管理責任者（以下「部局システム管理責任者」と言う。）及びシステム管理者の緊急連絡先，連絡手段，連絡内容を含む連絡網を言う。

(10) 通報窓口

インシデントについて学内外から連絡・通報を受け，初期対応を行うための窓口を言う。

(11) 利用規則

「国立大学法人東京学芸大学情報セキュリティポリシー」とそれに基づく管理運用規則及び手順，その他本学の情報ネットワークや情報システムの利用上のルールを言う。

(12) 利用規則違反行為

インシデントに係わるかどうかに限らず，利用規則に違反する行為を言い，次を含む。

1 情報システム及び情報について定められた目的以外の利用

2 電子掲示板，ブログやウェブページ等での名誉・信用毀損にあたる情報の発信

3 差別，侮辱，ハラスメントにあたる情報の発信

4 他人の個人情報や肖像の無断公開や漏えいその他プライバシーを侵害する情報の発信

5 守秘義務に違反する情報の発信

6 他人の著作物の違法コピーのアップロード等，他人の著作権等の知的財産権を侵害する情報の発信

7 通信の秘密を侵害する行為

8 営業ないし商業を目的とした本学情報システムの利用

9 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）なくネットワーク上の通信を監視し，又は情報機器の利用情報を取得する行為

10 不正アクセス禁止法に定められたアクセス制御を免れる行為及びそれを助長する行為

11 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

12 サービス不能攻撃等，故意に過度な負荷を情報システムに与えることにより本学の円滑な情報システムの運用を妨げる行為

13 その他法令に基づく処罰の対象となり，又は損害賠償等の民事責任を発生させる情報の発信

14 上記の行為を助長する行為

15 管理者の許可をえず，ソフトウェアのインストールやコンピュータの設定の変更を行う行為

２．インシデント通報窓口

（１）インシデント対応のための学外・学内の連絡・通報窓口は，当該インシデント発生部局システム管理責任者又はシステム管理者のほか，次のとおりとする。

・情報セキュリティインシデント通報窓口→TGU-CSIRT（総務部情報基盤課）

・上記以外のインシデント通報窓口→危機管理会議（総務部総務課）

（２）学外への連絡・通報に当たっては，TGU-CSIRT，総務部総務課等との連絡を密にし，無断で行わないものとする。

３．インシデントの対応・判断のエスカレーション手順

（１） TGU-CSIRTは，インシデントを認知した場合は，緊急連絡網その他所定の連絡網により，適宜，部局情報セキュリティ管理責任者，部局システム管理責任者，システム管理者のうち関係する者にインシデントの初期対応を依頼するものとする。

（２）TGU-CSIRT は，全学ネットワークに関るインシデントについて，必要に応じて自ら技術的対応をするものとし，部局ネットワークにのみ関連するインシデントについては，部局システム管理責任者を支援するものとする。

（３）システム管理者は，インシデントを発見し，又はTGU-CSIRT 等を通じて内部・外部からの通報を受けることにより認知した場合，ただちに部局システム管理責任者に状況報告するものとする。

（４）部局システム管理責任者は，インシデントを自ら認知するかシステム管理者から状況報告を受けた場合，下記の基準により一次切り分け判断を行うものとする。

① 部局内ネットワークに閉じた技術的問題かの判断

i）物理的インシデント又はセキュリティインシデントの場合で，対外的インシデント及び体内的インシデントのいずれでも無く，部局内ネットワークにのみ影響が生じている場合，システム管理者に対策を指示し，対策結果を部局情報セキュリティ管理責任者に状況報告する。

ii）i)以外の場合，部局情報セキュリティ管理責任者を通じて最高情報セキュリティ責任者に状況報告をし，TGU-CSIRT の支援を仰ぎながら，物理的インシデント又はセキュリティインシデント対応を行う。

② コンテンツインシデントかの判断

i）コンテンツインシデントの場合，加害者と被害者が部局内に閉じている場合であっても，法律的対策を講じる必要があるため，原則として部局情報セキュリティ管理責任者を通じて最高情報セキュリティ責任者に報告をし，TGU-CSIRT 等の支援を仰ぎながら，ログの保全等，必要な技術的措置を取るものとする。

ii）ただし，爆破予告・自殺予告など，生命・身体への危険等の緊急性がある場合で，部局内での対処が可能な場合は，コンテンツに関する緊急対応を実施の上，部局情報セキュリティ管理責任者と最高情報セキュリティ責任者に結果報告をする。

（５）部局システム管理責任者は，あらかじめ定められた手順に従って，緊急な技術的対応が必要なときはシステム管理者に指示を与え，部局情報セキュリティ管理責任者に対応結果を報告する。法的に慎重な判断を要する場合は，対応を実施する前に必ず部局情報セキュリティ管理責任者に報告し，指示を受けることとする。

（６）部局システム管理責任者から報告を受けた部局情報セキュリティ管理責任者は，コンテンツインシデントについて，部局システム管理責任者・システム管理者を指揮監督する。セキュリティインシデント対応については，ポリシーに基づいて最高情報セキュリティ責任者に指示や承認を求める。また，法的判断を要する問題については，顧問弁護士等に対応を依頼する。

（７）学外クレームか，対外クレームかの判断

① 最高情報セキュリティ責任者は，学外クレームにより認知したインシデントの場合，関係部局等と連携を行い、学外クレーム対応を行う。

② 最高情報セキュリティ責任者は，必要に応じて顧問弁護士等に相談しながら，関係部局等と連携を行い、対外クレーム対応を実施するものとする。

③ 学内問題として処理可能であるインシデントは，通常の技術的対応又は利用規則違反対応とする。

（８）重大なインシデントが発生した場合，最高情報セキュリティ責任者は，事故等の報告を，文部科学省関係機関における情報セキュリティインシデント発生時の報告・連絡要領により文部科学省担当所管課・関連課に連絡する。また，独立行政法人情報処理推進機構の届出様式に基づき情報処理推進機構セキュリティセンターに届け出る。

４．インシデント発生時の対応

４．１　物理的インシデント発生時の対応

（１）発生時

（ア）通報・発見等で物理的インシデントの可能性を認知したシステム管理者は，事実を確認するとともに部局システム管理責任者に報告し，被害拡大防止のための緊急措置の必要性について判断を求めるものとする。

（イ）システム管理者は，後日の調査に備え，物理的インシデント発生時の状況に関する記録を作成し，ネットワーク運用に影響があるおそれがある場合，バックアップデータの作成，ハードディスクのイメージの保存等を行う。

（２）被害拡大防止の応急措置の実施

（ア）部局システム管理責任者は，早急にシステム復旧措置を講ずるほかに，個別システムの停止やネットワークからの遮断，機器の交換，ネットワークの迂回等の緊急措置の必要性を判断し，実施をシステム管理者に指示する。

（イ）利用者等による対処が必要な場合には，その旨を命令する。

（ウ）保守契約機器においては，保守部品を迅速に確保する。

（３）緊急連絡及び報告

（ア）部局システム管理責任者は，緊急の被害拡大防止措置を実施する場合は，部局情報セキュリティ管理責任者に報告する。

（イ）部局情報セキュリティ管理責任者は，被害拡大防止措置が全学ネットワークに影響が及ぶと判断するときはTGU-CSIRTに連絡する。連絡を受けた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。

（ウ）最高情報セキュリティ責任者は TGU-CSIRTに指示して，緊急措置の実施により影響を受ける利用者等へ連絡するとともに，必要に応じて緊急対策室を組織する。

（エ）本学の情報危機管理体制に従い，最高情報セキュリティ責任者，全学システム管理責任者，TGU-CSIRTは必要に応じて部局システム管理責任者又は部局情報セキュリティ管理責任者と協議し，事態の判断を行う。

・軽微な事案　情報基盤整備推進本部及び情報セキュリティ会議に報告　⇒　学長及び役員会報告

・重大な事案　緊急対策室を設置，招集　⇒　危機管理会議に報告

（オ）TGU-CSIRTは，最高情報セキュリティ責任者又は緊急対策室の指示に基づき，関係するネットワークへの連絡などを行う。

（カ）最高情報セキュリティ責任者は，外部広報を行う必要があると判断した時は，広報戦略を所掌する副学長に連絡する。

（キ）緊急対策室が設置された場合，部局情報セキュリティ管理責任者，部局システム管理責任者及びシステム管理者は，その指示に従うものとする。

（４）　復旧計画

（ア）システム管理者は，物理的インシデントによる被害や緊急措置の影響を特定し，システムやネットワークの復旧計画を立案する。

（イ）部局システム管理責任者は，復旧計画を検討し，部局情報セキュリティ管理責任者の承認を得て復元を実施する。

（５）原因調査と再発防止策

（ア）システム管理者は，物理的インシデント発生の要因を特定し，再発防止策を立案する。

（イ）部局システム管理責任者は，利用者等への注意喚起等を含めた再発防止策を検討し，部局情報セキュリティ管理責任者は検討結果に基づき再発防止策を策定する。

（ウ）システム管理者と部局システム管理責任者は，インシデント対応作業の結果をまとめ，部局情報セキュリティ管理責任者は，再発防止策とともに危機管理会議，情報セキュリティ会議及び情報基盤整備推進本部に報告する。また，必要によりポリシーや実施手順の改善提案を行う。

（エ）最高情報セキュリティ責任者は，TGU-CSIRT責任者から物理的インシデントについての報告を受けた場合には，その内容を検討し，再発防止策を実施するために必要な措置を講ずる。

４－２　セキュリティインシデント発生時の対応

４－２－１　個人情報，特定個人情報又は機密情報（機密性２以上の情報）（以下，個人情報等という。）の漏えい（その可能性がある場合を含む）

（１）発生時

（ア）個人情報等の漏えいの兆候や具体的な事実を確認した場合は，その個人情報等を情報システムで取り扱うシステム管理者，TGU-CSIRT，最高情報セキュリティ責任者及び個人情報保護管理者に報告する。

（イ）報告を受けたシステム管理者は，TGU-CSIRT，部局システム管理責任者，最高情報セキュリティ責任者と対策を協議し，速やかに情報漏洩のための対策をとる。

（ウ）システム管理者は，事実関係の整理を行う。

・事実の発生期日，場所

・紛失，盗難，漏えいの当事者

・紛失，盗難，漏えいの対象物

・対象物に保存（格納）されていた情報（誰の何の情報，いつの情報，件数）

・保存形態（当該情報の暗号化やアクセス制限の有無）

・漏えいの発覚理由

（エ）不正アクセスや不正プログラムなど情報システムからの情報漏えいの可能性がある場合は，不用意な操作をせず，システム上に残された証拠を保存する。

（オ）外部からの通報等による場合は，相手の連絡先等を確認する。

（２）被害拡大防止の応急措置の実施

（ア）紛失物の捜索，回収

（イ）警察への届出

（ウ）ネットワーク接続及びシステムの遮断又は停止

（エ）漏えい・流出したアカウントの停止，パスワードの変更

（３）調査

（ア）本学の情報危機管理体制に従い，最高情報セキュリティ責任者，全学システム管理責任者，TGU-CSIRTは必要に応じて部局システム管理責任者，又は部局情報セキュリティ管理責任者及び当該保有情報等を管理する個人情報保護管理者と協議し，事態の判断を行う。

・軽微な事案　情報基盤整備推進本部及び情報セキュリティ会議に報告　⇒　学長及び役員会報告

・重大な事案　緊急対策室を設置，招集　⇒　危機管理会議に報告

（イ）紛失・盗難等情報の把握により，予想される二次被害の確認

（ウ）盗難機器・媒体の機種・型番，製造番号の確認

（エ）要因の特定

（４）通知・公表等

（ア）文部科学省等関係機関への報告

（イ）個人が特定できる情報の漏えいの恐れがある場合は，本人通知及びお詫び

（ウ）漏えいの規模や影響範囲が大きい場合は，学外公表

（５）システム等の復旧

TGU-CSIRT，部局システム管理責任者，最高情報セキュリティ責任者と協議し，復旧に向けた対策について検討する。

（６）事後対応

情報基盤整備推進本部及び情報セキュリティ会議において，発生した事案（建物への侵入防止，情報資産の保管方法，情報資産の持出し管理，情報の暗号化やアクセス制御及びその徹底，物理面，技術面，管理面，教育面など）の問題点を総合的に検討し，運用体制及び運用手順の改善を実施するとともに，報告書を作成する。

４－２－２　情報システムへの攻撃

（１）発生時

（ア）監視システムによるセキュリティインシデントの可能性を示す事象の検知や通報等でセキュリティインシデントの可能性を認知したシステム管理者は，事実の確認をするとともに部局システム管理責任者，TGU-CSIRT，最高情報セキュリティ責任者に報告する。

（イ）外部からの通報等による場合は，相手の連絡先等を確認するとともに，取得した情報の提供を求める。

（ウ）システム管理者は，後日の調査に備え，セキュリティインシデント発生時の状況，例えばログイン状況，ネットワーク接続や手順の稼働状況に関する記録を作成し，バックアップデータの作成，ハードディスクのイメージの保存等を行う。

（２）被害拡大防止の応急措置の実施

（ア）部局システム管理責任者は，個別システムの停止やネットワークからの遮断（他の情報システムと共有している学内通信回線又は学外通信回線から独立した閉鎖的な通信回線に構成を変更する等）等の緊急措置の必要性を，TGU-CSIRT，部局システム管理責任者，最高情報セキュリティ責任者と協議し，実施をシステム管理者に指示する。

（イ）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，情報システムのアカウントの不正使用の報告を受けた場合には，直ちに当該アカウントによる使用を停止させるものとする。

（ウ）部局システム管理責任者は，利用者等による対処が必要な場合には，その旨を命令する。

（エ）セキュリティインシデントが，外部からの継続している攻撃等であって攻撃元ネットワークの管理主体等への対処依頼が必要な場合，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の承認を得てTGU-CSIRTから相手方サイトへの対処依頼を行う。

（３）緊急連絡及び報告

（ア）部局システム管理責任者は，緊急の被害拡大防止措置を実施する場合は，部局情報セキュリティ管理責任者に報告する。

（イ）部局情報セキュリティ管理責任者は，被害拡大防止措置が全学ネットワークに影響が及ぶと判断するときはTGU-CSIRTに連絡する。連絡を受けた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。

本学の情報危機管理体制に従い，最高情報セキュリティ責任者，全学システム管理責任者，TGU-CSIRTは必要に応じて部局システム管理責任者又は部局情報セキュリティ管理責任者と協議し，事態の判断を行う。

・軽微な事案　情報基盤整備推進本部及び情報セキュリティ会議に報告　⇒　学長及び役員会報告

・重大な事案　緊急対策室を設置，招集　⇒　危機管理会議に報告

（ウ）TGU-CSIRTは，最高情報セキュリティ責任者，全学システム管理責任者又は緊急対策室の指示に基づき，攻撃元サイトや関係するサイトへの連絡及びJPCERT/CCへの連絡などを指揮する。

（エ）最高情報セキュリティ責任者は，外部広報を行う必要があると判断した時は，広報戦略を所掌する副学長に連絡する。

（オ）緊急対策室が設置された場合，部局システム管理責任者及びシステム管理者は，その指示に従うものとする。

（４）復旧計画

（ア）システム管理者は，セキュリティインシデントの被害や緊急措置の影響を特定し，システムやネットワークの復旧計画を立案する。

（イ）部局システム管理責任者は，復旧計画を検討し，部局情報セキュリティ管理責任者（全学ネットワークに影響する場合はTGU-CSIRT責任者）の承認を得て復元を実施する。

（５）原因調査と再発防止策

（ア）システム管理者は，セキュリティインシデント発生の要因を特定し，再発防止策を立案する。

（イ）部局システム管理責任者は，利用者等への注意喚起等を含めた再発防止策を検討し，部局情報セキュリティ管理責任者（全学ネットワークに影響する場合はTGU-CSIRT責任者を通じて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）の承認を得て実施する。

（ウ）システム管理者と部局システム管理責任者は，インシデント対応作業の結果をまとめ，部局情報セキュリティ管理責任者は，再発防止策とともに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。また，必要によりポリシーや実施規程の改善提案を行う。

（エ）TGU-CSIRT責任者は，部局情報セキュリティ管理責任者からセキュリティインシデントについての報告を受けた場合には，その内容を検討し，最高情報セキュリティ責任者の承認を仰ぎ，再発防止策を実施するために必要な措置を講ずる。

４－２－３　情報システムの障害

（１）発生時

（ア）監視システムによるセキュリティインシデントの可能性を示す事象の検知や，通報等でセキュリティインシデントの可能性を認知したシステム管理者は，事実の確認をするとともに部局システム管理責任者，TGU-CSIRT，最高情報セキュリティ責任者に報告する。

（イ）外部からの通報等による場合は，相手の連絡先等を確認するとともに，取得した情報の提供を求める。

（ウ）システム管理者は，後日の調査に備え，セキュリティインシデント発生時の状況，例えばログイン状況，ネットワーク接続や手順の稼働状況に関する記録を作成し，バックアップデータの作成，ハードディスクのイメージの保存等を行う。

（２）被害拡大防止の応急措置の実施

（ア）部局システム管理責任者は，個別システムの停止やネットワークからの遮断（他の情報システムと共有している学内通信回線又は学外通信回線から独立した閉鎖的な通信回線に構成を変更する等）等の緊急措置の必要性を，TGU-CSIRT，全学システム管理責任者，最高情報セキュリティ責任者と協議し，実施をシステム管理者に指示する。

（イ）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，情報システムのアカウントの不正使用の報告を受けた場合には，直ちに当該アカウントによる使用を停止させるものとする。

（ウ）部局システム管理責任者は，利用者等による対処が必要な場合には，その旨を命令する。

（エ）セキュリティインシデントが，外部からの継続している攻撃等であって攻撃元ネットワークの管理主体等への対処依頼が必要な場合，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の承認を得てTGU-CSIRTから相手方サイトへの対処依頼を行う。

（３）緊急連絡及び報告

（ア）部局システム管理責任者は，緊急の被害拡大防止措置を実施する場合は，部局情報セキュリティ管理責任者に報告する。

（イ）部局情報セキュリティ管理責任者は，被害拡大防止措置が全学ネットワークに影響が及ぶと判断するときはTGU-CSIRTに連絡する。連絡を受けた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。

本学の情報危機管理体制に従い，最高情報セキュリティ責任者，全学システム管理責任者，TGU-CSIRTは必要に応じて部局システム管理責任者又は部局情報セキュリティ管理責任者と協議し，事態の判断を行う。

・軽微な事案　情報基盤整備推進本部及び情報セキュリティ会議に報告　⇒　学長及び役員会報告

・重大な事案　緊急対策室を設置，招集　⇒　危機管理会議に報告

（ウ）TGU-CSIRTは，最高情報セキュリティ責任者，全学システム管理責任者又は緊急対策室の指示に基づき，攻撃元サイトや関係するサイトへの連絡及びJPCERT/CCへの連絡などを指揮する。

（エ）最高情報セキュリティ責任者は，外部広報を行う必要があると判断した時は，広報戦略を所掌する副学長に連絡する。

（オ）緊急対策室が設置された場合，部局システム管理責任者及びシステム管理者は，その指示に従うものとする。

（４）復旧計画

（ア）システム管理者は，セキュリティインシデントの被害や緊急措置の影響を特定し，システムやネットワークの復旧計画を立案する。

（イ）部局システム管理責任者は，復旧計画を検討し，部局情報セキュリティ管理責任者（全学ネットワークに影響する場合はTGU-CSIRT責任者）の承認を得て復元を実施する。

（５）原因調査と再発防止策

（ア）システム管理者は，セキュリティインシデント発生の要因を特定し，再発防止策を立案する。

（イ）部局システム管理責任者は，利用者等への注意喚起等を含めた再発防止策を検討し，部局情報セキュリティ管理責任者（全学ネットワークに影響する場合はTGU-CSIRT責任者）の承認を得て実施する。

（ウ）システム管理者と部局システム管理責任者は，インシデント対応作業の結果をまとめ，部局情報セキュリティ管理責任者は，再発防止策とともに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。また，必要によりポリシーや実施規程の改善提案を行う。

（エ）TGU-CSIRT責任者は，部局情報セキュリティ管理責任者からセキュリティインシデントについての報告を受けた場合には，その内容を検討し，最高情報セキュリティ責任者の承認を仰ぎ，再発防止策を実施するために必要な措置を講ずる。

４．３　コンテンツインシデント

（１）発生時

（ア）生命・身体への危険の可能性を示唆するコンテンツ（殺人，爆破，自殺の予告等）や学内ネットワークへの脅威等に対する通報・発見等でインシデントの可能性を認知したシステム管理者又は教職員等は，事実の確認をするとともに部局情報セキュリティ管理責任者，そのコンテンツに関連する部局，TGU-CSIRT，最高情報セキュリティ責任者に報告する。

（イ）外部からの通報等による場合は，相手の連絡先等を確認するとともに，取得した情報の提供を求める。

（ウ）システム管理者等は，後日の調査に備え，インシデント発生時の状況に関する記録を作成し，情報の保全（バックアップデータの作成，ハードディスクのイメージの保存等）を行う。

（２）被害拡大防止の応急措置の実施

（ア）部局情報セキュリティ管理者は，ネットワークを利用した情報発信内容が他人の権利侵害や児童ポルノ画像の公開等の違法行為又は公序良俗違反に関しては，情報公開・個人情報保護会議と連携し，総務課，情報基盤課と対策を協議する。

生命・身体への危険の可能性を示唆するコンテンツに関しては，危機管理会議と連携し，教職員については人事課及びその所属部局，学生等については学生課等，附属学校園児童・生徒等については附属学校課と対策を協議する。

学内ネットワークへの脅威等に対する通報・発見等に関しては，TGU-CSIRT，全学システム管理責任者，最高情報セキュリティ責任者と対策を協議し，速やかに被害防止のための緊急措置をとる。

（イ）システム管理者は，部局システム管理責任者に個別システムの停止やネットワークからの遮断，機器の交換，ネットワークの迂回等の緊急措置の実施の判断を求める。

（ウ）利用者等は，被害の拡大を防止するうえでも，パソコンとネットワークを切り離す（ネットワークケーブルを引き抜く等）等初動対処を実施する。

（３）緊急連絡及び報告

（ア）部局システム管理責任者は，緊急の被害拡大防止措置を実施する場合は，部局情報セキュリティ管理責任者に報告する。

（イ）部局情報セキュリティ管理責任者は，被害拡大防止措置が全学ネットワークに影響が及ぶと判断するときはTGU-CSIRTに連絡する。連絡を受けた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。

（ウ）最高情報セキュリティ責任者は，TGU-CSIRTに指示して緊急措置の実施により影響を受ける利用者等へ連絡する。

（エ）本学の情報危機管理体制に従い，最高情報セキュリティ責任者，全学システム管理責任者，TGU-CSIRTは必要に応じて部局システム管理責任者又は部局情報セキュリティ管理責任者と協議し，事態の判断を行う。

・軽微な事案　情報基盤整備推進本部及び情報セキュリティ会議に報告　⇒　学長及び役員会報告

・重大な事案　緊急対策室を設置，招集　⇒　危機管理会議に報告

（オ）TGU-CSIRTは最高情報セキュリティ責任者，全学システム管理責任者又は緊急対策室の指示に基づき，関係するネットワークへの連絡などを行う。

（カ）最高情報セキュリティ責任者は，外部広報を行う必要があると判断した時は，広報戦略を所掌する副学長に連絡する。

（キ）緊急対策室が設置された場合，当該部局情報セキュリティ管理責任者，部局システム管理責任者及びシステム管理者は，その指示に従うものとする。

（４）復旧計画

（ア）システム管理者は，TGU-CSIRTの協力を得て，インシデントによる被害や緊急措置の影響を特定し，システム，コンテンツやネットワークの復旧計画を立案する。

（イ）部局システム管理責任者は，復旧計画を検討し，部局情報セキュリティ管理責任者　（全学ネットワークに影響する場合はTGU-CSIRT責任者）の確認後，最高情報セキュリティ責任者の承認を得て復元を実施する。

（５）原因調査と再発防止策

（ア）システム管理者は，TGU-CSIRTの協力を得て，インシデント発生の要因を特定し，再発防止策を立案する。

（イ）部局システム管理責任者は，利用者等への注意喚起等を含めた再発防止策を検討し，部局情報セキュリティ管理責任者は検討結果に基づき再発防止策を策定する。

（ウ）システム管理者と部局システム管理責任者は，インシデント対応作業の結果をまとめ，部局情報セキュリティ管理責任者が策定する再発防止策とともに情報基盤整備推進本部及び情報セキュリティ会議に報告し，必要により情報セキュリティポリシーや実施規程の改善提案を行う。

（エ）最高情報セキュリティ責任者は，TGU-CSIRTを通じて部局情報セキュリティ管理責任者からセキュリティインシデントについての報告を受けた場合には，その内容を検討し，再発防止策を実施するために必要な措置を講ずる。

５．通常の利用規則違反行為の対応

（１）発見又は通報等による認知と事実確認（情報発信者の特定を含む）

システム管理者は，発見あるいは通報により利用規則違反の疑いのある行為を知ったときは，すみやかに事実関係を調査し，発信元利用者等を特定した上で部局システム管理責任者に報告する。

（２）利用規則違反の該当性判断

システム管理者の報告を受けた部局システム管理責任者は，通常の利用規則違反行為の対応手順に適用することが可能と考える場合は，その旨部局情報セキュリティ管理責任者に報告し，確認を得るものとする。

部局システム管理責任者は，技術的事項に関する利用規則違反に該当するか否かを判断し，該当する場合には情報発信の一時停止等の措置が必要であるかどうかを部局情報セキュリティ管理責任者及び最高情報セキュリティ管理責任者に報告するものとする。

最高情報セキュリティ管理責任者は，技術的事項以外の利用規則違反に該当するか否かを判断し，該当する場合には，情報発信の一時停止等の措置やアカウントの一時停止等，個別の情報発信の一時停止以上の措置が必要であるかを判断する。判断にあたっては，可能な限り当該行為を行った者の意見を聴取するものとし，必要に応じて情報基盤整備推進本部及び情報セキュリティ会議に判断を求めるものとする。

（３）情報発信の一時停止措置

TGU-CSIRT責任者は，部局情報セキュリティ管理責任者又は最高情報セキュリティ責任者の指示を受けて，利用規則違反に関係する情報発信の一次停止又はアカウントの一時停止措置等を実施する。

（４）情報発信者に対する通知・注意・警告・当事者間紛争解決要請

部局情報セキュリティ管理責任者又は最高情報セキュリティ責任者は，事案に応じて次の内容を発信者に通知するものとする。

・利用規則違反の疑いがあること

・アカウントの一時停止措置等の利用を制約する措置を講じた場合は，その事実及びその理由・根拠

・利用規則違反行為の是正，中止の要請

・利用規則違反行為が是正，中止されなかった場合の効果（情報の削除やアカウントの停止，学内処分等）

・反論を受け付ける期間とその効果

・利用者等当事者間の紛争解決の要請

（５）TGU-CSIRT責任者は，個別の情報発信又はアカウントの停止とアカウントの復活を行う。

（６）部局情報セキュリティ管理責任者又は最高情報システム管理責任者は，（４）の措置を講じたときは，遅滞無くTGU-CSIRT責任者にその旨を報告し，次の事項を実施するものとする。

・個別の情報発信，又はアカウントの停止と復活

・有効な反論があった場合，又は利用行為が是正された場合の個別の情報発信やアカウントの復活

・利用行為が是正されなかった場合の情報の削除やアカウントの停止，学内処分の開始手続き

・利用者等の当事者間の紛争解決着手の有無の確認

６．学外クレーム対応

（１） 原則

（ア） 学外クレームを受けた場合で，請求の法律的な効果や指摘されたコンテンツや行為の違法性の判断を要するときは，あらかじめ対応手順が明確になっていない限り，必ず法律の専門家に相談するものとする。

（イ） 部局システム管理責任者は，学外クレームについては，部局情報セキュリティ管理責任者及び最高情報セキュリティ責任者に報告を行うものとする。

（ウ）最高情報セキュリティ責任者又は緊急対策室は，攻撃先サイトや関係するサイトへの連絡及び関係機関への報告などを指揮し，部局システム管理責任者及びシステム管理者は，その指示に従うものとする。

（エ）具体的な学外クレーム等の対応については，事案に応じて高等教育機関の情報セキュリティ対策のためのサンプル規程集を参考に協議を行う。

附　則

この対応手順書は，令和２年４月１日から施行する。

附　則

この対応手順書は，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

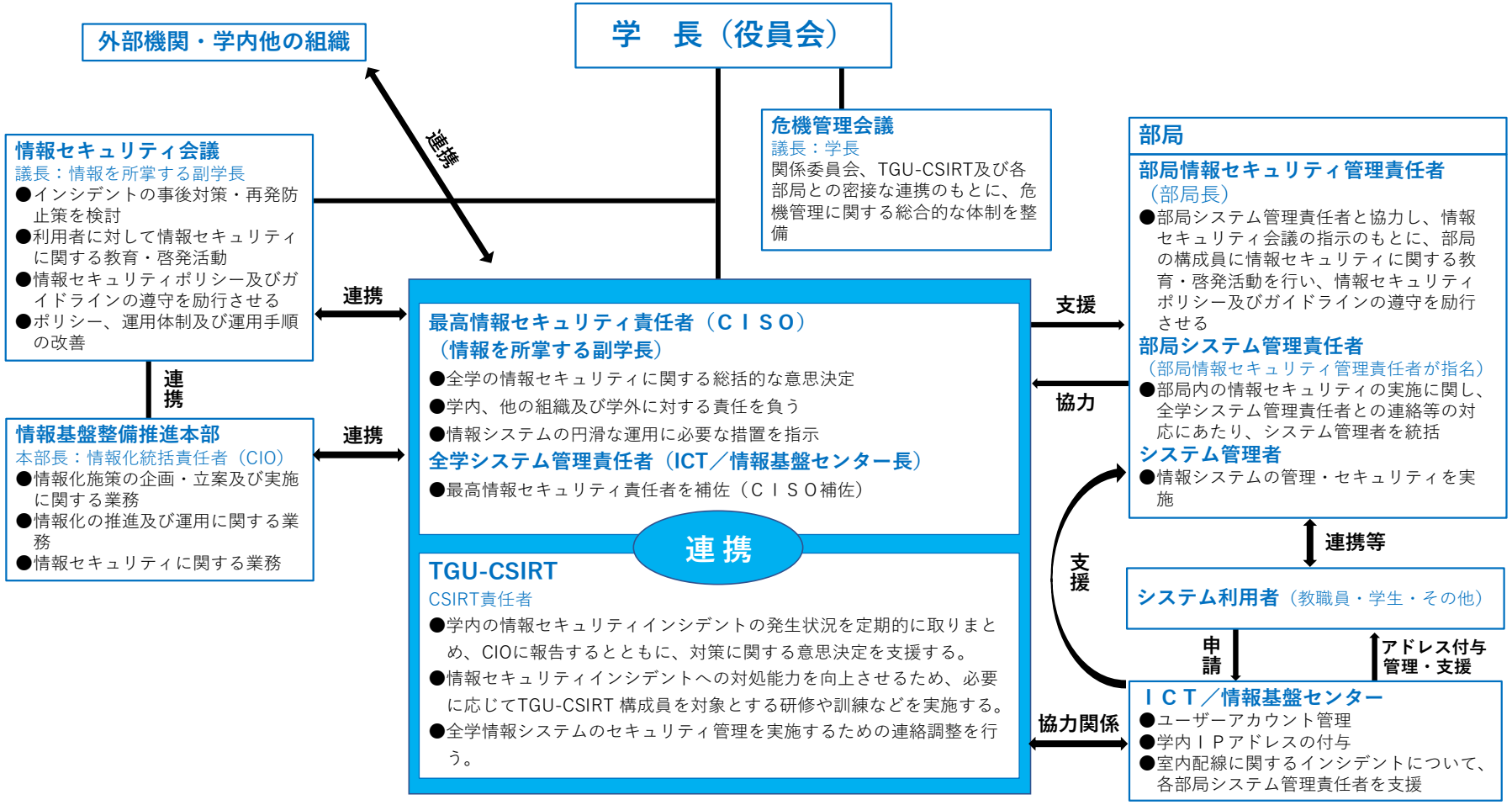
この手順書は，令和５年４月１日から施行する。

附　則

この手順書は，令和６年４月１日から施行する。

別紙１

東京学芸大学情報セキュリティ対応体制



別紙２

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）