愛知工業大学 インシデント対策本部の対応手順

1．目的

本手順は、影響の大きい重大な情報セキュリティインシデントが発生した場合、また、その疑いがある場合、極力速やかに情報を収集して、定められた手順に従って迅速に対応し、情報セキュリティ環境の保持・復旧、及び、対外的な問題の解決を組織的に速やかに行い、被害を最小限に抑え、問題の改善、再発防止策が行われることを目的とし、インシデント対策本部の手順を明確にする。

＜用語定義＞

(1)情報セキュリティ

情報の機密性、完全性、可用性を維持すること

・機密性：情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること

・完全性：情報が破壊、改ざん又は消去されていない状態を確保すること

・可用性：情報へのアクセスを認められた者が、必要なときに情報にアクセスできる状態を確保すること

(2)情報システム

ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成されるものであって情報処理を行う仕組み

(3)部局システム

教育・研究の一環で構築した学科の研究室、実験室、PC 教室等で稼働している情報システム

大学・法人事務局で事務を行うために構築した各部署で稼働している情報システム

(4)情報セキュリティインシデント（以下、インシデントという）

情報セキュリティの確保が困難な事象、その恐れのある事象

(5)インシデント対策本部（以下、対策本部という）

インシデントが発生した場合、愛知工業大学情報セキュリティ対策規程第 10 条の定めにより大学情報セキュリティ責任者が組織的に対策を講じる必要があると判断した際設置する本部

(6)本学構成員

本学の学生、教職員及び学内において業務を行うことが認められている者

(7)CISO

学園の最高情報セキュリティ責任者（法人事務局長）

2．適応対象者

・対策本部を組織する教職員（愛知工業大学情報セキュリティ対策規程第 10 条 2）

対策本部長（大学情報セキュリティ責任者：学長(不在時副学長)）、副学長、
計算センター長、大学事務局長、
情報システム室長、総合企画課長、その他学長の指名した者

・発生した、または、発生する恐れのあるインシデントに関係する教職員等

その内、部局システムのインシデント対応関係者（システム・サーバ所管）を以下の通り定義する。

①部局担当者　　：部局システムの担当者
部局システムを管理運用する教員(非常勤含む)、技術員、研究員・補助員(院生含む)、事務職員等

②部局責任者　　：部局システムの責任者
部局システムの管理運用に責任をもつ教員（部局担当者が兼ねる場合あり）、事務局所属長（課長・事務長等）

③部局統括責任者：学部長・学科長・副学科長、各センター長、事務局事務部長など

3．インシデントの検知と緊急措置

(1)インシデントに関する学内・学外の連絡・通報窓口を設ける。

・学内窓口　：計算センター
メール受付：security@aitech.ac.jp

・学外窓口　：総合企画課　：通報者、クレーム・被害者等
広報課　　：報道機関等
計算センター：情報セキュリティ関連機関等
メール受付：security@aitech.ac.jp

(2)学内・学外の連絡・通報窓口へ連絡のあったインシデントのうち、全学ネットワークに関するインシデントは、計算センターで状況調査・事実確認を行い、インシデントの影響範囲・緊急性・重大性を判断し、必要に応じて該当情報システムの停止やネットワーク接続の遮断を行うと伴に、情報システム室長、計算センター長に報告する。

また、関係する学科・部署、当事者の所属する学科・部署に対しては、状況を連絡して、初期対応を要請する。

4．対策本部の設置

(1) 計算センターより報告を受けた計算センター長は、以下の判断をした場合、対策本部長へ状況を報告する。

・インシデントが学外に影響を及ぼす
・インシデントが全学ネットワークに影響する
・インシデントが本学の業務運営に深刻な影響を及ぼす

(2) 学科・部署で事実確認を行って、部局総括責任者、部局責任者から全学ネットワークに影響すると報告のあったインシデントで重大な被害が想定されるインシデントの場合、計算センター長は、影響を受ける利用者等に被害拡大防止措置を連絡するとともに、対策本部長に状況を報告する。

(3) 対策本部長は、計算センター長より(1)(2)のインシデント発生報告を受けて、組織的に対策を講じる必要があると判断した場合、CISO より対策本部の設置要請を受けた場合、「対策本部」を設置する。

(4) 対策本部長は、設置した対策本部を組織する者を指名する。
(5) 対策本部を組織する者の部署が中心に事務局を編成し、情報収集、調査、対策等の実務を行う。
(6) 対策本部事務局は、本部棟会議室に設置し、情報を集中させる。
(7) 必要に応じて対策本部を組織するメンバーを招集して（会議の開催）、対策の検討・審議を行う。会議の進行は、計算センター長が行う。

5．情報収集・調査

(1) 対策本部は、インシデント発生時の状況（ログイン状況他）、通信ログ・アクセスログ等各種機器のログを解析することによりアクセス状況等を把握して、技術的にインシデントの原因を特定し、被害の影響範囲の調査を行う。
(2) 対策本部は、必要に応じ審議を経て、外部のセキュリティサービス会社に調査の一部を委託する。
(3) 対策本部は、調査に必要な情報が削除されたり、変更されたりする恐れがある場合、バックアップデータの作成、ハードディスクのイメージ保存等を行なって、調査に必要な情報を確保する。
(4) 対策本部は、学内・学外関係者から情報を収集し整理して、発生したインシデントの原因、学内の被害・影響、対外的な影響、重大性、緊急性の度合い等を把握する。
(5) 対策本部は、調査・分析・把握した情報を記録に残す。
(6) 対策本部は、その重大性、緊急性の度合いに応じて、初動対応の方針を定める。初動対応を行うべき部局責任者に対し、必要な初動対応を行うように指示する。

6．対策の決定・実施

(1) 調査・各種対策の重要事項については、対策本部組織にて会議を開催の上、審議し決定する。
例）・調査のための外部のセキュリティサービス会社の利用（費用発生による予算確保）
・対外的な告知（範囲、内容、手段）
漏えいした個人情報の本人、取引先などへの通知
監督官庁、警察、IPA などへの届出
Web ページ、マスコミ（新聞、記者会見他）等による公表
・補償の範囲・費用　　など
(2) 緊急を要することは、計算センター長が指揮をとり応急措置を進める。
(3) 調査によってインシデントによる被害や影響が特定でき、対策が判明したら、情報システムやネットワークの復旧計画を検討・立案し、計算センター長の承認を得て実施する。
(4) 対策本部は、漏えいした情報に個人の機密情報（ID・パスワード等）が含まれる場合、本人に通知を行い、ID の停止等の処理を行ってもらう。
(5) 対策本部は、第三者に重要情報（ファイル等）が渡った場合、第三者から情報の回収を行う。
(6) 対策本部は、攻撃元サイトや関係するサイトに調査・対策要請が必要な場合、該当サイトへ連絡して、解決を図る。例えば、Web 上に個人情報等が公開されてしまった場合、Web 検索サイトに依頼し、Web サイトから個人情報を削除してもらう（キャッシュの削除をして検索結果

に表示されなくなるように対処してもらう)。

(7) 対策本部は、法的な判断を要する問題については、法律の専門家に相談して、解決を図る。

(8) 学外クレームや本学利用者の行為によるインシデントの被害者に対し、法律的判断をせずに、謝罪することや、その他の約束をしてはならない。被害者への謝罪は、法律の専門家に相談の上、謝罪する方法を十分検討して情報を整理し、誠意の伝わる説明、お詫びを行う。

(9) 対策本部は、本学利用者の情報発信行為等に対し損害賠償請求や謝罪要求があった場合、法律の専門家に相談の上、対応する。本学利用者の行為によるインシデントの被害者に対しては、法律の専門家に相談して、補償内容を検討・審議し、被害者の理解を得られる補償を行う。

(10)対策本部は、不正 ID 使用等で本学が被害を受けた場合、損害賠償請求、刑事告訴などを行うかどうか法律の専門家に相談した上、検討・審議し、決定した内容を実施する。

(11)学部・学科・部署で対処した方が良い事項については、対策本部より学部・学科・部署に対応の要請を行う。

7．注意喚起

(1) 対策本部は、同じ事象の再発を防止するため、緊急に必要な注意事項を速やかに案内して、学内への徹底を図る。

(2) 対策本部は、特に注意を要する学科、研究室、個人、部署がある場合、個別に連絡して徹底を図る。

8．報告・公表

(1) 対策本部は、誰にどの範囲まで告知するか、また、どんな手段で告知するか検討・審議する。

(2) 文科省への報告

個人情報の漏えい、標的型サイバー攻撃等による被害は文科省に報告を行う。

・高等教育局 私学部 私学行政課　　03-6734-2527　sigakugy@mext.go.jp

・大臣官房政策課 情報システム企画室　03-5253-4111　seijoho@mext.go.jp

(3) 関係機関への報告

個人情報の漏えい、標的型サイバー攻撃等による被害は状況に応じて以下にも報告を行う。

・警察

特に、紛失・盗難のほか内部犯行・脅迫による不正な金銭要求など犯罪性がある場合

愛知県警察本部 サイバー犯罪対策課 052-951-1611

・IPA（独立行政法人 情報処理推進機構）

https://www.ipa.go.jp/security/todoke/index.html

・JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）

https://www.jpcert.or.jp/form/#contact

(4) Web ページへの掲載・記者会見

個人情報の漏えいなど学外に影響のあるセキュリティ事故が発生し、公表の必要があると判断された場合、Web ページへの掲載または記者会見にて公表を行う。

・透明性・開示の原則から、情報流出が発生した場合はなるべく早く公表を行う。

・公表前に、被害者や関係者に通知し、公表の許可を得る。
・問合せ窓口は一本化し、対外的な情報に整合性を確保する。
・Web ページでの公表の場合、公表用資料を掲載する形で実施。
掲載場所は、トップページからリンクを張る。
・Web による報告・公表は以下の内容を取り入れる。
①序文（お詫び、姿勢)、②事故発生に関する状況報告、③事実経緯、
④調査方法及び状況、⑤漏えいした情報の内容、⑥事故の被害内容、⑦事故原因、
⑧当面の対応策、⑨再発防止策、⑩問い合わせ窓口　等

(5) 報道機関に対する対応
・報道機関から 2〜3 件以上の取材の依頼が来た場合、記者会見の開催を検討する。
・報道機関の取材に応じる場合、電話ではなく、可能な限り対面での対応を行う。
・記者会見する場合、事前に報道機関に FAX 等にて情報（開催概要等）を送付する。
・記者会見では、公表用資料の他、事実関係を説明する資料を準備し、正確な情報が伝わるよう配慮する。
・記者会見では、想定問答集を作成し、事前に練習を行う。
・記者会見にて回答できない質問については、その場で無理に答えようとせずに、確認の上追って回答を行う旨を伝える。

９．事後対応（再発防止）
(1) 対策本部は、同様なインシデントの抜本的な再発防止策を策定して、計画を立てて実施する。
・システム的な対策
・監視、モニタリングの強化
・各種規程やポリシー、手順書の見直し
・調査、対応体制（組織・チーム）の見直し
・本学構成員への教育の実施　　他
(2) 被害者に対して、損害補償等必要な措置を行う。
(3) 本学が被害を受けた場合、加害者に対して、損害賠償請求等必要な措置を行う。
(4) 対策本部で対応したインシデントに対して、検知から事後対応に至る全体をまとめた報告書を作成し、情報セキュリティ対策委員会に報告して今後に活かす。

以上

平成 31 年 4 月 8 日制定

附　則
この規定は、令和 4 年 10 月 1 日から施行する。