

## 岐阜大学における情報セキュリティインシデント対応手順

### 1. 定義

#### (1) 情報セキュリティインシデント

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。）とは、ネットワークや情報システムの稼動を妨害またはデータの改竄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ないが、ネットワークの帯域、ディスクや計算機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また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いい、下記原因によるものを含む。

- －迷惑メールの送信
- －コンピュータウイルスの蔓延や意図的な頒布
- －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(注)
- －サービス不能攻撃その他情報ネットワーク管理責任者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
- －禁止されている形態での P2P ソフトウェアの利用(注)
- －禁止された方法による学外接続(注)
- －学内ネットワークへの侵入を許すようなアカウント情報を格納した情報機器の盗難・紛失

(注) 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、禁止されている形態での P2P ソフトウェア、禁止された方法による学外接続等については、別紙「情報セキュリティインシデントの原因となる不正なアクセスやソフトウェア等について」で説明する。

#### (2) 緊急連絡網

インシデントや障害等に備え、重要と認めた情報システムについて、そのシステム管理責任者及びシステム担当者の緊急連絡先、連絡手段、連絡内容を含む連絡網をいう。

#### (3) 学外窓口

インシデントについて学外から連絡・通報を受け、学外への連絡・通報、対外クレームをすための窓口をいう。

### 2. インシデント連絡等窓口

(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、下記のとおりとする。

- A. 学内窓口：情報管理対策室
- B. 学外窓口：総合企画部総務課及び情報管理対策室

—連絡先—

情報管理対策室

TEL : 090-3158-6600, E-mail : csirt@gifu-u. ac. jp

総合企画部総務課 : 総務課課長補佐

TEL : 058-293-2007, E-mail : gjga01002@jim. gifu-u. ac. jp

(2) 情報管理対策室は、学外への連絡・通報、対外クレームに当たっては、総合企画部総務課等との連絡を密にし、独断で行わないものとする。

### 3. インシデントへの対応・判断の段階的手順

岐阜大学では、文部科学省からの「情報セキュリティインシデント発生時の報告・連絡要領」等に基づき対応することとし、以下の手順により行う。

(1) 総合企画部総務課並びに各部局総務担当者は、学内外を問わずインシデントに係る通報を受けた場合は、速やかに情報管理対策室に、通報の事実及び内容等を連絡する。

電話や電子メールでの第一報の後、情報セキュリティインシデント発生報告書を情報管理対策室に提出するものとする。

(2) 情報管理対策室はインシデントを発見し、または学外クレームや学内からの通報等によりインシデントを認知した場合は、インシデントの緊急性・重大性を判断し、必要に応じて、別途定める全学情報システム等停止マニュアルにより当該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ともに、緊急連絡網その他所定の連絡網により、最高情報責任者（以下、「CIO」という。）、危機管理担当理事、広報担当理事及び当該情報資産の管理責任者へ連絡する。また、必要に応じて、当該情報システムの管理者に対し当該情報システムの停止や、情報の保全（バックアップデータの作成、ログデータの保全、ハードディスクのイメージの保存等）等の初期対応を指示する。

なお、当該インシデントが医学部附属病院に関する場合は、医療情報部へ対応を移管する。

(3) 重大なインシデントについては、CIO はインシデント発生の認知後、速やかに学長等へ報告する。

(4) CIO 及び危機管理担当理事の判断に基づき、情報管理対策室、総務課課長補佐（危機管理担当）、総務課広報係長（広報担当）、当該情報資産の管理担当者、当該情報資産の管理部局の情報セキュリティ技術専門委員等によるインシデント緊急対処チームを設置する。

なお、インシデント緊急対処チームを設置した場合は、速やかに文部科学省に重大なインシデント発生を連絡するものとする。

(5) インシデント緊急対処チームの要請に基づき、情報ネットワーク管理責任者（以下「全学 LAN 管理責任者」という。）は、全学情報ネットワークに関わるインシデントについては、必要に応じて自ら技術的対応を行うものとし、部局情報ネットワークにのみ関連するインシデントについては、部局情報ネットワーク管理責任者（以下「部局 LAN 管理責任者」という。）を支援するものとする。

- (6) 部局等情報ネットワーク管理担当者は、インシデントを発見し、または情報ネットワーク管理責任者等を通じて内部・外部からの通報を受けることにより認知した場合、ただちに部局情報ネットワーク管理責任者へ状況を報告するものとする。
- (7) インシデント緊急対処チーム又はインシデント一般対処チームによりインシデントに対応する。対応内容については、4. インシデント緊急・一般対処チームによる対応のとおりである。
- (8) CIO は、インシデント緊急チーム、インシデント一般対処チームの作業状況を適宜把握するとともに報告内容を確認し、重大なインシデントについては、その状況及び結果等を学長等へ報告するものとする。
- (9) 学長は、本件についての公表の是非を判断するとともに、必要に応じて、文部科学省及び関係省庁への報告を行う。

#### 4. インシデント緊急・一般対処チームによる対応

##### (1) インシデント事実関係の確認

- (ア) 通報・発見等による事案が、インシデントであることをチーム構成員間で共通認識するとともに事案の事実関係を確認する。
- (イ) 当該インシデントの対処に必要なチーム構成であるか確認し、不足する場合は、情報セキュリティ最高責任者（以下「CISO」という。）が必要な措置を講じるものとする。

##### (2) 状況・原因の調査・分析

- (ア) インシデント発生時の状況を記録するとともにアクセスログ等証跡調査に必要な情報を確保・保存する。
- (イ) ネットワーク運用に影響があるおそれがある場合は、バックアップデータの作成やハードディスクのイメージの保存等を行う。
- (ウ) 収集した情報の調査・分析を行い、原因の特定と解明に当たる。必要に応じて、文部科学省へ指導・助言を仰ぐものとする。

##### (3) 被害者等への対応

- (ア) 個人情報や秘匿情報の漏洩等により個人の権利・利益を侵害するおそれがある場合は、被害者等への説明や謝罪等の対応を当該担当部署へ要請する。
- (イ) 被害者への説明や謝罪に必要な情報を整理し、当該担当部署へ報告する。

##### (4) 学外組織との対応・連携

- (ア) 必要に応じて、法律の専門家、捜査当局及び通信事業者等の学外組織と連携してインシデントに対応するものとする。

##### (5) 対応方針・復旧計画・再発防止策の検討及び実施

- (ア) インシデントによる被害や緊急措置の影響が特定されたら、システムやネットワークの復旧計画を検討し、CIO、全学 LAN 管理責任者や部局 LAN 管理責任者等所要の承認を得て実施する。
- (イ) CISO は、必要に応じて CIO や関係部署に再発防止策の検討及び実施を要請する。

(6) 報告書の作成

- (ア) 別添様式による報告書を作成し、CISO から CIO へ報告する。
- (イ) 情報管理対策室は、インシデントの内容や状況に応じて報告書を作成し、CIO, CISO の了解の下、文部科学省へ報告するものとする。
- (ウ) CISO は、報告書の内容について、必要に応じて CIO や関係委員会に情報セキュリティポリシーや実施手順の改善提案を行う。

別紙「情報セキュリティインシデントの原因となる不正なアクセスやソフトウェア等について」

(1. 定義(1)情報セキュリティインシデント 関係)

a. 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

不正アクセス禁止法(不正アクセス行為の禁止等に関する法律)とは、ID やパスワードによりアクセス権限が付されている機器やサービスに対し、ネットワークを通して他人の認証情報や脆弱性を利用して不正に利用する行為を禁ずる法律である。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として認知された例は次のようなものがある。

- ・メールの盗み見等の情報の不正入手
- ・知人になりすましての情報発信
- ・ウェブサイトの改竄・消去

なお、これらの不正アクセスの手口は識別符号窃用型(他人の ID・パスワードの窃取)及びセキュリティホール攻撃(情報システムの脆弱性を利用したもの)に二つに分けられる。

b. 禁止されている形態での P2P ソフトウェア

P2P ソフトウェアとは、ネットワークを介して不特定の相手とファイルを共有(送信・受信)するなどの機能を備えたソフトウェアをいう。

本来、P2P は効率的なファイルの入手・公開を目的の一つとした通信方式であるが、P2P ソフトウェアで共有されているファイルには次のような危険性があるため、岐阜大学では P2P ならびにそれに類するソフトウェアの使用を禁止している。

- ・映画・音楽・市販ソフトウェアなどのように著作権で保護されているにもかかわらず、著作権者に許諾を得ずに共有されているものが多い。
- ・わいせつ物頒布等罪、児童ポルノ禁止法に抵触するものがある。
- ・ウイルスが仕込まれているものがあり、感染すると個人情報の流出、遠隔操作、ボットネットとしての利用など被害への遭遇あるいは犯罪に加担する可能性がある。

なお、禁止されている形態での P2P ソフトウェア及び P2P ソフトウェアの動作を助長するおそれのあるソフトウェアには次のものがある。

Xunlei・Kugoo・BitTorrent・BearShare・QQLive・PPLive・QQDownload・PPStream・FlashGet・baofeng・eMule・Cabos・Winny・Share・VeryCD・P2PTV・WebThunder・Gnutella・WinMX・PerfectDark・Azureus・Ares・Shareaza・BitComet・UPnPJ・μTorrent・eDonkey・FrostWire・Vuze・WebbyFiles・Zultrax・LemonWire ほか
--

c. 禁止された方法による学外接続

禁止された方法による学外接続とは、GU-VPN(岐阜大学常勤教職員向け VPN サービス)以外の、岐阜大学が提供していない方法でのトンネリングや、公衆交換電話網モデムを無許可でキャンパス情報ネットワークに設置して学外から接続するなど、キャンパス情報ネットワークに悪影響を及ぼす可能性のある接続手段をいう。なお、岐阜大学が提供していない方法での接続には以下のようなものがある。

各種 VPN アプリケーション (Freenet, Hamachi, OpenVPN, Packetix VPN ほか)

各種通信匿名化アプリケーション (Tor, Hotspot Shield, SpotFlux ほか)

各種通信制限迂回ツール (Hola Unblocker, Mobility XE ほか)

各種リモートアクセスツール (Chrome Desktop, LogMeIn, TeamViewer ほか)