平成２８年９月３０日
最高情報責任者(CIO)決定

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し，またはデータの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，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恐れを言い，下記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
－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
－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

(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言う。

(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，対外クレームをするための窓口を言う。

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：058-293-2057，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。

⑻CIO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。

⑼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

⑴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。

⑵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恐れがある場合は，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。

⑶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・利益を侵害する恐れがある場合は，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。

⑷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。

⑸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。

⑹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。