インシデント対応手順

沖縄大学マルチメディア教育研究センター

1. 定義

(1) 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およびその恐れを言う。

(2) 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、またはデータの漏えい、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または他の学内構成員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およびその恐れを言い、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、学内構成員の環境に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学内構成員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センター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
－著作権法、不正アクセス禁止法などに違反する形態での 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
－管理上の過失による秘密情報（個人情報を含む）の漏えい、データの消失または改ざん

(3) 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」という）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また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、下記原因を含む。

－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

ー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

(4) 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またはコンテンツインシデントを言う。

(5) 対外的インシデント

インシデントのうち、学内構成員等による行為であって、外部ネットワーク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

学内構成員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（学内構成員が、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、また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) 運用･管理規程

「沖縄大学マルチメディア教育研究センター規程」と関連規程等に基づく手順、命令、計画等を言う。

(10) 緊急連絡網

規程等に基づき整備されたインシデント／障害等に備え、特に重要と認めた情報システムについて、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。

(11) 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。

(12) 利用規程

「沖縄大学マルチメディア教育研究センター規程」と関連規程等（以下「規程等」という）に基づく手順、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。

(13) 利用規程違反行為

インシデントに係わるかどうかに限らず、利用規程に違反する行為を言い、下記を含む。

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　マルチメディア教育研究センター長（以下、センター長という）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　センター長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　管理者の許可を得ず、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

(14) マルチメディア教育研究センター構成員

マルチメディア教育研究センターは以下のメンバーで構成される。

１　センター長
２　副センター長
３　センター職員
４　センター保守員
５　コンピュータ教室補助員

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・通報窓口は下記のとおりとする。

A.　学内窓口：マルチメディア教育研究センター
B.　学外窓口：マルチメディア教育研究センター／経営企画室

(2) 学外窓口への学外からの e-mail による連絡手段は、以下のメーリングリストとし、公表するものとする。

Email: multimedia@okinawa-u.ac.jp 学

(3) 学外への連絡・通報、対外クレームに当たっては、マルチメディア教育研究センター及び経営企画室との連絡を密にし、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) マルチメディア教育研究センター（以下、センターという）は、インシデントを認知した場合は、センター保守員にインシデントの初期対応を依頼するものとする。

(2) センターは、学内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するものとする。

(3) センターは、インシデントを発見、または内部・外部からの通報を受けることにより認知した場合、ただちに関係者に状況報告するものとする。

(4) センターは、インシデントを自ら認知するか、通報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 学内ネットワークに閉じた技術的問題の場合
i) 物理的インシデントまた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対内的インシデントのいずれでも無く、学内ネットワークにのみ影響が生じている場合、関係者に対策を指示し、対策結果をセンター長に状況報告する。
ii) i)以外の場合、センター長に状況報告をし、物理的インシデントまたはセキュリティインシデント対応のプロセスを実施する。
② コンテンツインシデントの場合
i) コンテンツインシデントの場合、加害者と被害者が学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、原則としてセンター長に報告をし、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、「電話・SNS 等による爆破予告・威力業務妨害等フローチャート」に基づいて対応する。

(5) 学外クレームか、対外クレームか
① センター長は、学外クレームにより認知したインシデントの場合、学外クレーム対応プロセスを併せて実施する。
② センター長は、事務局長及び総務課長に相談しながら、必要に応じて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、通常の技術的対応または利用規程違反対応とする。

4. 物理的インシデント発生時の対応

⑴ 発生から緊急措置決定まで
(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学内構成員は、事実を確認するとともにセンターに報告し、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) 担当者は、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

ィスクのイメージの保存等を行う。

(2) 被害拡大防止の応急措置の実施

(ア) センターは、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、必要に応じて措置を行う。

(イ) 学内構成員等による対処が必要な場合には、その旨命令する。

(3) 緊急連絡及び報告

(ア) センター職員は、緊急の被害拡大防止措置を実施する場合、関係者に報告する。

(イ) センター職員は、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センター長に報告する。

(ウ) センター長はセンター職員を通じて、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、学長の指示を仰いだ上で、必要に応じセンター内にインシデント対応チームを組織する。

(エ) センターは「緊急時広報マニュアル」に基づいて、関係機関等への連絡、取材・問い合わせ対応を行う。

(オ) インシデント対応チームが設置された場合、関係者は、その指示に従うものとする。

(4) 復旧計画

センターは、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・検討し、関係者の承認を得て実施する。

(5) 原因調査と再発防止策

(ア) センター職員は、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) センター長は、学内構成員等への注意喚起等を含めた再発防止策を検討し、策定する。

(ウ) センター職員は、インシデント対応作業の結果をまとめ、センター長は再発防止策とともに必要な会議体に報告し、必要によりポリシーや実施手順の改善提案を行う。

5. セキュリティインシデント発生時の対応

⑴ 発生から緊急措置決定まで

(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センター職員は、事実を確認するとともにセンター長に報告し、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仰ぐものとする。

(イ) センター担当者は、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。

(ウ) 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、センター長の承認を得てセンター職員から相手方サイトへの対処依頼を行う。

⑵ 被害拡大防止の応急措置の実施

(ア) センター長は、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判断し、実施をセンター職員に指示する。

(イ) センター長は、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、直ちに当該アカウントの使用を停止させるものとする。

(ウ) センター長は、学内構成員等による対処が必要な場合には、その旨命令する。

⑶ 緊急連絡及び報告

(ア) センター職員は、緊急の被害拡大防止措置を実施する場合、センター長に報告する。

(イ) センター長は、被害拡大防止措置が全学ネットワークに影響する場合、関係者に連絡する。

(ウ) センター長は、センター職員を通じて、緊急措置の実施により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、学長の指示を仰いだ上で、必要に応じセンター内にインシデント対応チームを組織する。

(エ) センター長は、攻撃元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する。

(オ) インシデント対応チームが設置された場合、学内構成員はその指示に従うものとする。

⑷ 復旧計画

(ア) センター職員は、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) センター長は、復旧計画を検討し、学長の承認を得て実施する。

(5) 原因調査と再発防止策

(ア) センター職員は、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) センター長は、利用者等への注意喚起等を含めた再発防止策を検討し、学長の承認を得て実施する。

(ウ) センター職員はインシデント対応作業の結果をまとめ、センター長が再発防止策とともに学長に報告するとともに、必要によりポリシーや規程の改善提案を行う。

6. コンテンツインシデントに関する緊急対応

(1) センター職員は、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）を発見し、または通報等により認知した場合、センター長の指示によりコンテンツの情報発信元を探知し、その結果を学長に報告するものとする。

(2) センター職員は、センター長にコンテンツの情報発信元の探知結果を報告し、学内緊急連絡についての指示を仰ぐ。

(3) センター長は、学長に学内緊急連絡についての指示を仰ぐ。その際、広報、保護者、警察への連絡等の学内規則に従う。

7. 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、事務局参与または顧問弁護士等の専門家に相談するものとする。

(イ) 学外クレームについては、センター長に報告を行うものとする。

(ウ) 学外クレームについての報告を受けたセンター長は、学長の承認を仰ぎ必要に応じセンター内にインシデント対応チームを設置するものとする。

(エ) インシデント対応チームは、攻撃先サイトや関係するサイトへの連絡、外部広報、及び関係機関への報告などを指揮し、学内構成員は、その指示に従うものとする。

(2) 学内構成員等のコンテンツの違法性を主張した送信中止・削除の要求

(ア) 発信元利用者等の特定

学外クレームが学内構成員等により不特定多数に宛てて発信されたコンテンツの違法性や情報発信による権利侵害を主張してコンテンツの送信中止や削除の要求が、被害を主張する者またはその代理人からなされたものである場合、センター職員は、事実関係を調査し、発信元の学内構成員等を特定する。

(イ)（通常手続き）コンテンツを発信した学内構成員等への通知と削除

a. 指摘されたコンテンツの違法性の判断が困難な場合、プロバイダ責任制限法第 3 条第 2 項第 2 号に基づき学内構成員等に請求があった旨通知し、通知後 7 日以内に学内構成員等から反論がない場合は、送信中止あるいは削除を実施するものとする。

b. 有効と思われる反論があった場合は、その旨、削除請求者に伝えるとともに、当事者間での紛争解決を依頼する。

(ウ)（緊急手続き）学内構成員等への通知前の一時保留

a. 指摘されたコンテンツの違法性が疑いもなく明らかと判断できる場合、一旦学内構成員等のコンテンツ送信を保留し、その旨学内構成員等に伝えるものとする。有効な反論があればコンテンツ送信を復活するものとする。

b. 本手続きの対象は、著名な音楽 CD の丸写しや個人の住所や電話の暴露等、権利侵害の疑いが濃厚である場合、緊急な救済の必要性がある場合のみとする。

c. 本緊急手続は「沖縄大学情報ネットワーク・システム管理運営規程第 7 条」に基づき実施する。

(3) 学内構成員等の発信したコンテンツの刑事的違法性の指摘及び送信中止・削除の要求

(ア) 学内構成員等の発信したコンテンツが刑事法上違法な可能性の高い旨指摘された場合で、名誉毀損や著作権侵害等、被害者が存在する犯罪については、（２）と同様の手順を取るものとする。

(イ) わいせつ物陳列罪等、被害者のいない犯罪が外部クレームにより指摘された場合

a. センター担当者は、事実関係を調査し、発信元学内構成員等を特定する。

b. 発信元学内構成員等に犯罪であるとする指摘があった旨通知し、7 日を経過しても学内構成員等から反論がない場合は、送信中止あるいは削除を実施する。

(4) 学内構成員等の行為（コンテンツ以外）の違法性を主張した送信中止・アカウント削除等の要求

i)（通常の対応）通信を発信した学内構成員等への通知とアカウント停止

- 学外クレームが学内構成員等による１対１の情報発信による権利侵害等による被害を主張して情報発信の中止を要求するものである場合、センター職員は、事実関係を調査し、発信元学内構成員等を特定する。
- 事実確認を行い、特定できた学内構成員等に対し、問題となる通信の発信を中止するよう通知する。この通知には、本行為を再度行った場合、アカウントを停止する旨警告することを含む。
- 学内構成員等から有効な反論があれれば､関連するアカウントの一時停止を解除する。
- 念書をとるなどの対応の後、アカウントの復活手続きを行う。
- 同様の手順を経て再発が確認できた場合には、学生は「沖縄大学学生懲戒処分規程」、教職員は「沖縄大学職員懲戒手続規程」に基づいて処分等を行う。

ii)（セキュリティインシデント対応）学内構成員等のアカウントの一時停止

- 学外クレームが学内構成員等による１対１の情報発信によるセキュリティインシデントによる被害を主張して情報発信の中止を要求するものである場合､センター職員は、事実関係を調査し、発信元学内構成員等を特定する。
- センター職員は、事実を調査し、発信元学内構成員等を特定する。
- センター職員は、学内構成員等の行為がセキュリティインシデントの原因であると判断することに十分な理由がある場合、センター長にその旨を報告し、判断を仰ぐものとする。
- センター担当者からの報告を受けたセンター長は、必要な場合、学内構成員等の関連するアカウントを一時停止するとともに、必要な会議体に報告する。
- 請求者が連絡を要求しているときには一時停止した旨連絡する。
- アカウントを一時停止した旨学内構成員等に通知するとともに、再度行った場合には関連するアカウントを停止する旨警告する。
- 学内構成員等から有効な反論があれれば､関連するアカウントの一時停止を解除する。
- 念書をとるなどの対応の後、アカウントの復活手続きを行う。
- 同様の手順を経て再発が確認された場合、学生は「沖縄大学学生懲戒処分規程」、教職員は「沖縄大学職員懲戒手続規程」に基づいて処分等を行う。

(5) 損害賠償請求等

（ア）学内構成員等の情報発信や学外でのネットワークを利用した行為について損害賠償請求や謝罪請求があった場合、事務局参与または顧問弁護士等と相談の上、対応するものとする。
（イ）学外クレームに対して、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。
（ウ）学内構成員等の発信者情報等、連絡先が特定できている場合、損害賠償を請求する相手方には、学内構成員等との自主的な紛争解決を依頼するものとする。

(6) 発信者情報の開示請求
(ア) プロバイダ責任制限法第 4 条に基づく場合
a. 学内構成員等の情報発信や学外でのネットワークを利用した行為について発信者情報の開示請求があった場合であって､Web ページ等 1 対多の通信によるものの場合、プロバイダ責任制限法の規程に基づき専門家と共に対処するものとし、発信者が開示に同意している場合を除き、発信者情報の開示請求には慎重に対処するものとする。
b. 電子メールアドレス等、事前に学内構成員等から開示の許諾を得ている発信者情報のみが請求されている場合についてはそれを開示してもよい。また、開示と同時に当事者間紛争解決を依頼するものとする。

(7) プロバイダ責任制限法に基づかない発信者情報の照会（民事）
学内構成員等の情報発信や学外でのネットワークを利用した行為について発信者情報の照会があった場合であって、メール等 1 対 1 の通信によるものの場合、下記の手順をとるものとする。なお、警察官、検察官、検察事務官、国税職員、麻薬取締官、弁護士会、裁判所等の法律上照会権限を有する者から照会を受けた場合であっても、原則として発信者情報を開示してはならないので同様の手順となる。
i) 電子メールアドレス等、事前に開示の許諾を得ている発信者情報のみが請求されている場合についてはそれを開示してもよい。また、開示と同時に当事者間紛争解決を依頼する。許諾を得ていない発信者情報の開示については発信者の意見を聴く。
ii) 発信者が開示に同意すれば開示してよい。発信者が開示に同意しない場合は、開示を拒絶する。その場合は、通信の秘密及びプライバシーの保護を理由とする。
iii) 発信者情報の保有の有無、技術的に特定できるか否かの判断をし、開示できる発信者情報がなければ、その旨を請求者に通知する。

(8) 強制捜査による発信者情報の差押え、記録命令等
(ア) センター職員は、発信者情報を含む情報の強制捜査の事前打診があった場合には、発信者情報その他の強制捜査対象の情報を印刷あるいは記録媒体に出力できるよう準備をしておくものとする。
(イ) センター長は、ネットワークの稼動への影響が最小限になるような方法で強制捜査に協力するものとする。

(ウ) 捜査当局から強制捜査の令状の呈示を受けた場合、令状の記載事項等を確認の上、立会いを求められたときは立会い、押収物があるときは押収目録の交付を受けるものとする。

(エ) センター職員は、捜査当局から通信履歴（通信の送信先，送信元，通信日時など。通信内容は含まない。）について、暫定的に残しておくよう警察署長印等のある正式文書にて求められた場合（保全要請）、保全対象の情報を印刷あるいは記録媒体に出力して保管しておくものとする。

8. 通常の利用規程違反行為の対応

(1) 発見また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）

センター職員は発見あるいは通報により利用規程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、発信元学内構成員等を特定した上でセンター長に報告する。

(2) 利用規程違反の該当性判断

センター職員の報告を受けたセンター長は、通常の利用規程違反行為の対応手順にのせることが可能と考える場合、その旨関係者に報告し、確認を得るものとする。

センター長は、技術的事項に関する利用規程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関係者に報告するものとする。

センター長は、技術的事項以外の利用規程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、必要に応じてマルチメディア教育研究センター運営委員会の判断を仰ぐものとする。

(3) 情報発信の一時停止措置

センター職員は、センター長の指示を受けて、利用規程違反に関係する情報発信の一次停止また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

センター職員は、事案に応じて下記内容を発信者に通知するものとする。

- 利用規程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、そのこと、及びその理由・根拠
- 利用規程違反行為の是正、中止の要請
- 利用規程違反行為が是正、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
- 学内構成員等当事者間の紛争解決の要請

(5) 個別の情報発信またはアカウントの停止と復活

(6) センター職員は、(4) の措置を講じたときは、遅滞無くセンター長にその旨を報告し、その後の学内構成員等の対応により、必要に応じマルチメディア教育研究センター運営委員会の承認を得て、下記を実施するものとする。
- 個別の情報発信またはアカウントの停止と復活
- 有効な反論があった場合、また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
- 学内構成員等の当事者間の紛争解決着手の有無の確認

9. 学内処分との関係

センター長は外部クレームの対象となった学内構成員等、利用規程等に違反をした学内構成員等について、関係部署へ報告することができる。また、関係部署による処分の検討に際し、アカウント停止処分やその他ネットワークやシステムの利用を制約する処分の必要性の有無について意見を述べることができる。