情報セキュリティインシデント対応手順

平成 27 年 3 月

独立行政法人 国立高等専門学校機構
弓削商船高等専門学校

目次

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おそれをいう。

（2）システムインシデント

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およびそのおそれをいい下記原因によるものを含む。

① 大量のスパムメールの送信
② コンピュータウイルスの蔓延や意図的な頒布
③ 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
④ サービス不能攻撃その他情報セキュリティ責任者又は情報セキュリティ副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
⑤ 利用規定により禁止されている形態でのP2Pソフトウェアの利用
⑥ 禁止された方法による学外接続
⑦ 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又はネットワーク設定が施されたPCの盗難・紛失
⑧ 情報システムのソフトウェアの不具合によるシステムの停止や処理能力の大幅な低下
⑨ 学外に公開されているホームページ上の情報の改ざん
⑩ 教職員への不正な添付ファイル等を含む電子メールの送信によるフィッシング攻撃

（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又は一般的な道徳観念や社会通念に反するような行為（及びその旨主張する被害者等からの請求）による事故をいい，下記原因を含む。

① 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
② 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
③ 通信の秘密を侵害する行為
④ 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
⑤ 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
⑥ 児童ポルノやわいせつ画像の公開
⑦ ネットワークを利用したねずみ講
⑧ 差別，侮辱，ハラスメントにあたる情報の発信
⑨ 営業ないし商業を目的とした本校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，システムインシデント又はコンテンツインシデントをいう。

（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，事件をいう。

（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，事件をいう。

（７）学外クレーム

学内の利用者等による情報発信行為（本校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いう。

（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・告発をすることをいう。

（９）運用・管理規程

「弓削商船高等専門学校情報セキュリティ管理規程」とそれにもとづく手順，命令，計画等をいう。

（１０）緊急連絡網

運用・管理規程に基づき整備されたインシデントや障害等に備え，特に重要と認めた情報システムについて，その情報セキュリティ管理者及び情報セキュリティ推進責任者の緊急連絡先，連絡手段，連絡内容を含む連絡網をいう。

（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いう。

（１２）利用規定

「弓削商船高等専門学校情報セキュリティ教職員規程」，「弓削商船高等専門学校情報セキュリティ利用者規程」とそれにもとづく手順，その他本校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いう。

（１３）利用規定違反行為

インシデントに係わるかどうかに限らず，利用規定に違反する行為をいい，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校情報システムの利用
⑨ 情報セキュリティ責任者又は情報セキュリティ副責任者の許可（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 情報セキュリティ責任者又は情報セキュリティ副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校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 情報セキュリティ推進責任者の許可をえず，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（現時点において，ソフトウェアのインストールについては「弓削商船高等専門学校ソフトウェア管理規則」に則る）

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。

(ア) 学内窓口： 企画広報室 又は 情報処理教育センター
(イ) 学外窓口： 企画広報室 又は 情報処理教育センター

② 学外窓口への学外からの e-mail による連絡手段は，情報処理教育センター関係者全員が受信可能とする以下のメーリングリストとし，公表するものとする。

Email: center@yuge.ac.jp

③ 学外への連絡・通報，対外クレームに当たっては，本校企画広報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 企画広報室又は情報処理教育センターは，インシデントを発見し，又は，学外クレームにより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，情報セキュリティ責任者，情報セキュリティ副責任者，情報セキュリティ管理者，情報セキュリティ推進責任者にインシデントの初期対応を依頼するものとする。

② 情報処理教育センターは，全学ネットワークに関連す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，又は情報セキュリティ責任者を支援するものとする。

③ 情報セキュリティ推進員は，インシデントを発見し，又は企画広報室又は情報処理教育センターを通じて内部・外部からの通報を受けることにより認知した場合，ただちに情報セキュリティ推進責任者に状況報告するものとする。

④ 情報セキュリティ推進責任者は，インシデントを自ら認知するか情報セキュリティ推進員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。

(ア) 学内ネットワークに閉じた物理的インシデント又はシステムインシデント
A) 物理的インシデント又はシステムインシデントの場合で，対外的インシデントでも対内的インシデントでも無く，学内ネットワークにのみ影響が生じている場合，情報セキュリティ推進員に対策を

指示し，対策結果を情報セキュリティ副責任者に状況報告する。

B) A)以外の場合，情報セキュリティ副責任者を通じて情報セキュリティ責任者に状況報告をし，情報処理教育センターの支援を仰ぎながら，物理的インシデント又はシステムインシデント対応のプロセスを実施する。

(イ) コンテンツインシデント

A) 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，原則として情報セキュリティ副責任者を通じて情報セキュリティ責任者に報告をし，情報処理教育センター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。

B) 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，学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，情報セキュリティ責任者と情報セキュリティ副責任者に結果報告をする。

⑤ 情報セキュリティ推進責任者は，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情報セキュリティ推進員に指示を与え，情報セキュリティ副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情報セキュリティ副責任者に報告し，指示を受けることとする。

⑥ 情報セキュリティ推進責任者から報告を受けた情報セキュリティ副責任者は，コンテンツインシデントについて，情報セキュリティ推進責任者・情報セキュリティ推進員を指揮監督する。システムインシデント対応については，ポリシーに基づいて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のうち，通報者への内容確認や定型回答文書の発信等，情報セキュリティ推進責任者や学外窓口に対して一定の一時的対応を指示又は依頼する。

⑦ 学外クレーム，対外クレーム

(ア) 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，学外クレーム対応プロセスを併せて実施する。

(イ) 情報セキュリティ責任者は，法律の専門家に相談しながら，必要に応じて対外クレームを実施するものとする。

(ウ) 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定違反対応とする。

4. 物理的インシデント発生時の対応

（1）発生から緊急措置決定まで

① 通報・発見等で物理的インシデントの可能性を認知した情報セキュリティ推進員は，事実を確認するとともに情報セキュリティ推進責任者に報告し，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。

② 情報セキュリティ推進員は，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

① 情報セキュリティ推進責任者は，個別システムの停止やネットワークからの遮断，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，実施を情報セキュリティ推進員に指示する。
② 利用者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

① 情報セキュリティ推進責任者は，緊急の被害拡大防止措置を実施する場合は，情報セキュリティ副責任者に報告する。
② 情報セキュリティ副責任者は，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学内窓口を通じて情報セキュリティ責任者に報告する。
③ 情報セキュリティ責任者は学内窓口に指示して，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，最高情報セキュリティ責任者の指示を仰いだ上で，必要に応じ非常時対策本部を組織する。
④ 学外窓口は情報セキュリティ責任者又は非常時対策本部の指示に基づき，関係する機関への連絡，機構本部（総務課情報企画係）への連絡，外部広報などを行う。
⑤ 非常時対策本部が設置された場合，情報セキュリティ副責任者，情報セキュリティ管理者，情報セキュリティ推進責任者及び情報セキュリティ推進員は，その指示に従うものとする。

（４）復旧計画

① 情報セキュリティ推進員は，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。
② 情報セキュリティ推進責任者は，復旧計画を検討し，情報セキュリティ副責任者の承認を得て実施する。

（５）原因調査と再発防止策

① 情報セキュリティ推進員は，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。
② 情報セキュリティ推進責任者は，利用者等への注意喚起等を含めた再発防止策を検討し，情報セキュリティ副責任者は検討結果に基づき再発防止策を策定する。
③ 情報セキュリティ推進責任者は，インシデント対応作業の結果をまとめ，情報セキュリティ副責任者は，再発防止策とともに情報セキュリティ管理委員会に報告するとともに，必要によりポリシーや実施手順の改善提案を行う。
④ 情報セキュリティ責任者は，情報セキュリティ副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。

５．システムインシデント発生時の対応

（１）発生から緊急措置決定まで

① 監視システムによるシステムインシデントの可能性を示す事象の検知や，通報等でシステムインシデントの可能性を認知した情報セキュリティ推進員は，事実を確認するとともに情報セキュリティ推進責任者に報告し，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。
② 情報セキュリティ推進員は，後日の調査に備え，システム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。
③ システムインシデントが，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，情報セキュリティ副責任者の承認を得て情報セキュリティ推進責任者から相手方サイトへの対処依頼を行う。

（２）被害拡大防止の応急措置の実施

① 情報セキュリティ推進責任者は，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判断し，実施を情報セキュリティ推進員に指示する。

② 情報セキュリティ副責任者および情報セキュリティ推進責任者は，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。

③ 情報セキュリティ推進責任者は，利用者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

① 情報セキュリティ推進責任者は，緊急の被害拡大防止措置を実施する場合は，情報セキュリティ副責任者に報告する。

② 情報セキュリティ副責任者は，被害拡大防止措置が全学ネットワークに影響する場合は，学内窓口を通じて情報セキュリティ責任者に連絡する。

③ 情報セキュリティ責任者は，学内窓口に指示して，緊急措置の実施により影響を受ける利用者等に被害拡大防止措置を連絡するとともに，最高情報セキュリティ責任者の指示を仰いだ上で，必要に応じ非常時対策本部を組織する。

④ 学外窓口は，情報セキュリティ責任者又は非常時対策本部の指示に基づき，攻撃元サイトや関係する機関への連絡，機構本部（総務課情報企画係） への連絡，外部広報などを指揮する。

⑤ 非常時対策本部が設置された場合，情報セキュリティ推進責任者及び情報セキュリティ推進員は，その指示に従うものとする。

（４）復旧計画

① 情報セキュリティ推進員は，システム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。

② 情報セキュリティ推進責任者は，復旧計画を検討し，情報セキュリティ副責任者（全学ネットワークに影響する場合は情報セキュリティ責任者）の承認を得て実施する。

（５）原因調査と再発防止策

① 情報セキュリティ推進員は，システム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。

② 情報セキュリティ推進責任者は，利用者等への注意喚起等を含めた再発防止策を検討し，情報セキュリティ副責任者（全学ネットワークに影響する場合は情報セキュリティ責任者）の承認を得て実施する。

③ 情報セキュリティ推進員と情報セキュリティ推進責任者は，インシデント対応作業の結果をまとめ，情報セキュリティ副責任者は，再発防止策とともに情報セキュリティ責任者に報告するとともに，必要により実施規程や実施手順の改善提案を行う。

④ 情報セキュリティ責任者は，情報セキュリティ副責任者からシステム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。

６．コンテンツインシデントに関する緊急対応

① 情報セキュリティ推進員は，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）を発見又は通報等により認知した場合，情報セキュリティ推進責任者の指示によりコンテンツの情報発信元を探知し，その結果を情報セキュリティ推進責任者に報告するものとする。

② 情報セキュリティ推進責任者は，情報セキュリティ副責任者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求める。

③ 情報セキュリティ副責任者は，情報セキュリティ責任者に，学内緊急連絡についての指示を仰ぐ。その際，広報，保護者，警察への連絡等については学内規則に従う。

7．学外クレーム対応

（1）原則

① 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。

② 情報セキュリティ推進責任者は，学外クレームについては，情報セキュリティ副責任者及び情報セキュリティ責任者に報告を行ものとする。

③ 学外クレームについての報告を受けた情報セキュリティ責任者は，最高情報セキュリティ責任者の承認を仰ぎ必要に応じ非常時対策本部を設置するものとする。

④ 情報セキュリティ責任者又は非常時対策本部は，攻撃先サイトや関係する機関への連絡，機構本部（総務課情報企画係）への連絡，外部広報などを指揮し，情報セキュリティ推進責任者及び情報セキュリティ推進員は，その指示に従うものとする。

（2）利用者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

① 発信元利用者等の特定

学外クレームが利用者等により不特定多数に宛て情報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又はその代理人からなされたものである場合，情報セキュリティ推進員は，事実関係を調査し，発信元利用者等を特定する。

② （通常手続き）コンテンツを発信した利用者等への通知と削除

(ア) 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号に基づき利用者等に請求があった旨通知し，通知後7日以内に利用者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。

(イ) 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。

③ （緊急手続き）利用者等への通知前の一旦保留

(ア) 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，一旦利用者等のコンテンツの送信を保留し，その旨利用者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。

(イ) 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。

(ウ) 本緊急手続きが適用されることもあることは具体的に利用規定として明示する等，利用者等に周知するものとする。

（3）利用者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

① 利用者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。

② わいせつ物陳列罪等，被害者のいない犯罪が学外クレームにより指摘された場合，

(ア) 情報セキュリティ推進員は，事実関係を調査し，発信元利用者等を特定する。

(イ) 発信元利用者等に犯罪であるとする指摘があった旨通知し，7日を経過しても利用者等から反論

がない場合は，送信中止あるいは削除を実施する。

（４）利用者等の行為（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

①　（通常の対応）通信を発信した利用者等への通知とアカウント停止

(ア) 学外クレームが利用者等による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，情報セキュリティ推進員は，事実関係を調査し，発信元利用者等を特定する。

(イ) 事実確認を行い，特定できた利用者等に対し，問題の通信の発信を中止するよう通知する。これには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ことを含む。

(ウ) 利用者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。

(エ) 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。

(オ) 同様の手順を経て再発が確認できた場合には，本校の処罰の手順に移行する。

②　（システムインシデント対応）利用者等のアカウントの一時停止

(ア) 学外クレームが利用者等による1対1の情報発信によるシステム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，情報セキュリティ推進員は，事実関係を調査し，発信元利用者等を特定する。

(イ) 情報セキュリティ推進員は，事実を調査し，発信元利用者等を特定する。

(ウ) 情報セキュリティ推進員は，利用者等の行為がシステムインシデントの原因であると判断するのに十分な理由がある場合には，情報セキュリティ推進責任者に報告し，その判断を求めるものとする。

(エ) 情報セキュリティ推進員からの報告を受けた情報セキュリティ推進責任者は，必要な場合，利用者等の関連するアカウントを一時停止するとともに，情報セキュリティ管理委員会に報告する。

(オ) 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。

(カ) アカウントを一時停止した旨利用者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。

(キ) 利用者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。

(ク) 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。

(ケ) 同様の手順を経て再発が確認できた場合には，本校の処罰の手順に移行する。

（５）損害賠償請求等

①　利用者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には，法律の専門家と相談の上，対応するものとする。

②　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。

③　利用者等の発信者情報等，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，利用者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

①　プロバイダ責任制限法第4条に基づく場合

(ア) 利用者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定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。

(イ) 電子メールアドレス等，事前に利用者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）

利用者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。

① 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。

② 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。

③ 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，提出命令等

① 情報セキュリティ推進員は，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憶媒体に出力できるよう準備をしておくものとする。

② 情報セキュリティ副責任者もしくは対外折衝事務担当者は，情報セキュリティ推進員の協力を得て，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。

③ 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。

８．通常の利用規定違反行為の対応

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）

情報セキュリティ推進員は発見あるいは通報により利用規定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情報セキュリティ推進責任者に報告する。

② 利用規定違反の該当性判断

情報セキュリティ推進員の報告を受けた情報セキュリティ推進責任者は，通常の利用規定違反行為の対応手順にのせることが可能と考える場合は，その旨情報セキュリティ副責任者に報告し，確認を得るものとする。

情報セキュリティ推進責任者は，技術的事項に関する利用規定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情報セキュリティ副責任者に報告するものとする。

情報セキュリティ副責任者は，技術的事項以外の利用規定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，必要に応じて情報セキュリティ管理委員会の判断を求めるものとする。

③ 情報発信の一時停止措置

情報セキュリティ推進員は，情報セキュリティ副責任者又は情報セキュリティ推進責任者の指示を

受けて，利用規定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

情報セキュリティ推進責任者又は情報セキュリティ副責任者は，事案に応じて下記内容を発信者に通知するものとする。

(ア) 利用規定違反の疑いがあること
(イ) 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
(ウ) 利用規定違反行為の是正，中止の要請
(エ) 利用規定違反行為が是正，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）
(オ) 反論を受け付ける期間とその効果
(カ) 利用者等当事者間の紛争解決の要請

⑤　個別の情報発信又はアカウントの停止と復活

⑥　情報セキュリティ副責任者又は情報セキュリティ推進責任者は，④の措置を講じたときは，遅滞無く情報セキュリティ責任者にその旨を報告し，その後の利用者等の対応により，必要に応じ情報セキュリティ管理委員会の承認を得て，下記を実施するものとする。

(ア) 個別の情報発信又はアカウントの停止と復活
(イ) 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
(ウ) 利用者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

情報セキュリティ副責任者は，学外クレームの対象となった利用者等，利用規約違反をした利用者等につき懲罰委員会等の関連委員会への報告をすることができる。また，懲罰委員会等の関連委員会による学内処分の検討に際し，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。

10. インシデント対応の役割分担

◎:インシデント総括　○:判断・技術支援　▲:技術対応判断　△:技術対応実施

インシデント分類	物理的 インシデント	システム インシデント	コンテンツ インシデント
情報セキュリティ責任者 （非常時対策本部）	◎	◎	◎
情報セキュリティ副責任者	◎	◎	○
情報セキュリティ管理委員会	○	○	○
情報セキュリティ推進責任者	▲	▲	△
情報セキュリティ推進員	△	△	△
企画広報室 又は情報処理教育センター （非常時窓口）	○	○	○

【参考1】インシデント対応手順にもとづくインシデント報告・承認要領

（1）本書の目的

インシデントが発生した場合，適切な対応によりインシデントの影響が拡大することを防ぐと共に復旧を図ることが必要である。このとき対応を誤ると無用な被害の拡大を招くことが懸念されるため，インシデントの発見から対処，さらには再発防止策の実施にいたる手続きを定め，適切な対処を実施することが必要である。

本書では，インシデントが発生した場合の報告・申請等の手続きに利用する様式を定め，様式を利用した報告・記録・申請・承認の要領を定めることにより本校において必要とされるインシデントへの対処を適切に実施することを目的とする。

（2）本書の対象者

本書は，すべての情報システム運用関係者を対象としている。利用者には，インシデントが発生した場合の企画広報室又は情報処理教育センターの通報先を周知・徹底すること。

（3）承認権限者

① インシデントに対する対処方針の適否を審査等する者（「インシデント対処承認権限者」）は，情報セキュリティ推進責任者，情報セキュリティ副責任者又は情報セキュリティ責任者とする。ただし，インシデントの内容に応じて必要がある場合は，その上位者を対処承認権限者とする。

② インシデントの再発防止策の適否を審査等する者（「インシデント再発防止策承認権限者」）は，情報セキュリティ副責任者，情報セキュリティ責任者又は最高情報セキュリティ責任者とする。

（4）障害等発生から再発防止策実施までの対応

① 障害等発生時における全般的な注意事項

(ア) 情報セキュリティ責任者又は情報セキュリティ副責任者は，インシデントが発生した場合において，緊急に対処が必要な場合の遅延を防止し，対処を円滑に実施するため，情報システム，組織等の状況を勘案し事前に詳細な手順を定め，関係者に周知すること。

(イ) 情報セキュリティ推進員（外部からの通報の場合，企画広報室又は情報処理教育センター）は，緊急の対処が必要なインシデントが発生した場合において，報告，審査等の手続が遅延することにより，必要な対処の実施が遅れることのないようにすること。

(ウ) 緊急の対処が必要な場合は，報告書に代わって口頭での報告，審査等を先行することや，発見者に代わって報告受理者が報告書を記入しインシデントの発見者から内容確認を得ること等により，遅滞なく障害等に対する対処を実施する。ただし，このような場合であっても，速やかに報告書を作成して記録を残すこと。

【事業継続計画（BCP：Business Continuity Plan）が策定されている場合】

(エ) 情報セキュリティ推進員は，BCP と情報セキュリティ関係規程が定める要求事項において事前に想定されていない不整合が生じた場合，その旨を情報セキュリティ推進責任者を通じて情報セキュリティ副責任者（必要により情報セキュリティ責任者）に報告し，指示を得ること。

② インシデントの発見報告

(ア) 自ら発見，又は利用者等からの通報によりインシデントを認知した情報セキュリティ推進員（外部からの通報の場合，企画広報室又は情報処理教育センター）は，別紙1「インシデント発生・再発防止策に関する報告・申請書」（以下「インシデント報告書」）により，インシデントの内容に応じて情報セキュリティ推進責任者又は情報セキュリティ副責任者（「インシデント報告受理者」）に報告を行うこと。

(イ) インシデントによる被害の拡大が懸念されるため，インシデント報告受理者の指示により情報セキュ

リティ推進員が応急措置を実施した場合には，すみやかにインシデント報告書に応急措置の内容を記録すること。

(ウ) インシデント報告受理者は，対処を実施する者を選び，対処の指示を与えること。なお，口頭により報告を受けた場合は，インシデント報告書のインシデントの詳細についてすみやかに記録させること。

(エ) インシデント報告受理者は，報告された内容を確認し，必要に応じて center@yuge.ac.jp 等の連絡網を活用し，情報セキュリティ副責任者，情報セキュリティ責任者及び関係部署等に通知させること。また，通知先をインシデント報告書に記録させること。

(オ) 情報セキュリティ責任者は，危機管理，利用者の意識向上に資するインシデント及びその対処の事例について，情報セキュリティ対策上支障のない範囲で学内の広報に努めること。

③ インシデントの対処

インシデントの対処を実施する者は，インシデントの対処方針を提案し，インシデント報告書によりインシデントの内容に応じて対処承認権限者の承認を得ること。ただし，情報セキュリティ副責任者又は情報セキュリティ責任者が定めた詳細な手順において，対処方針が規定されている場合には，承認を受けたものとみなす。なお，対処方針を決定する際には，必要に応じて通知先の関係部署と連携すること。

④ インシデントの再発防止

インシデントの対処を実施する者は，インシデントが発生する前の状態に復旧するだけでは再発するおそれがあると考える場合には，速やかに根本的な再発防止策を提案し，インシデントの内容に応じて，再発防止策承認権限者の承認を受け，記録すること。

【参考2】インシデント対応手順による学外クレーム対応時の留意点

（1）コンテンツインシデントの権利者や被害者への返信の要否

学外クレームがあった際，インシデント対応手順に基づき調査の上対処するが，学外クレームを発した権利者や被害者への返信は不要な場合が多いことに留意する。

また，違法情報についての第三者からの指摘については，法的責任の観点からは，返信は不要である。ただし，地域コミュニティを無視している等の風評を立てられることを回避するため，通報への謝辞（ご指摘ありがとう，学内ルールに基づき対処します等）のみ記して返答するほうが良い場合もある。

権利者や被害者への返信が必要か望ましい場合は，以下のとおり。

① 法律で義務とされている場合
　プロバイダ責任制限法第 4 条の発信者情報開示請求の要件を満たす場合
② 法律で義務とされていないが望ましい場合
　(ア) 発信者情報開示関係ガイドラインに基づき不開示決定を通知する場合
　(イ) 削除請求等のクレームに対して利用者等から有効と思われる反論があった場合
　(ウ) クレーム者と利用者等との当事者間解決を依頼するのが適当な場合
③ 法律専門家の判断による場合
　対処結果を報告する等，連絡することで，その後の交渉ポジションを不利にしないために有用な場合。（海外からの請求の場合，通常はあてはまらない。）

（2）海外の権利者，被害者からのクレームの特徴と対処時の留意点

① そもそも，正式な法的請求といえないものが多い。
② 海外の権利者・被害者からの場合，正式な法的請求をする場合は，弁護士名での書面で送付されるとのが普通。
③ 少なくとも海外からの訴状はメールでは送られてこない。
④ 米国の Digital Milemium Copyright Act（デジタルミレニアム著作権法。以下，「DMCA」という。）に基づく削除請求は，様式や内容が定められており，電子署名のないメールでは様式を満たさない。
　（参考）
　http://en.wikipedia.org/wiki/Online_Copyright_Infringement_Liability_Limitation_Act
⑤ DMCA に基づく削除請求にもとづき削除することにより，免責を受けられるが，返事をするのは義務ではない。
⑥ DMCA にもとづく旨，明記しているかどうかにかかわりなく，著作権侵害通知メールのほとんどは，機械的に発見した結果をとりこんで自動的に処理しているもので，まじめに読んだ相手方がさっさと削除等して，権利侵害が是正されれば儲け物というスタンス。削除結果等を回答することは実は期待されていない。
⑦ なお，DMCA では，アクセスプロバイダーはエンドユーザの（P2P）通信については免責。ただし，常習の権利侵害者の接続を切断する方針を実施する義務があるので，P2P を利用した著作権侵害についての警告が累積した場合には，米国の ISP は回線を切断している，とのこと。
⑧ 削除等の対処がされない場合は，権利者，被害者側は，それを記録し，正式な要求をすることになった場合の有力な証拠の一つとすることになるが，国際的な裁判はコスト面でも準拠法や裁判管轄等の法的側面でも容易ではないので，これまでも裁判例は無い。
⑨ 万が一，訴訟され反論せざるを得ない局面に備え，対利用者に対する警告，利用停止等の措置の記録はきちんと保存しておくほうが良い。

（３）（特に海外からのクレームにおいて）返信をする場合のポイント

① 謝らない。故意の権利侵害を自認したことになる。
② 聞かれていないことには回答しない。
③ 事実を正確に表現する。揚げ足をとられないように。

（４）システムインシデントの連絡への対処

① CERT や学校の機関からの連絡は，揚げ足をとるつもりは無いはずであるが，返信する場合は正確な表現ですべき。
② 法的権利を持っているわけではないが，ブラックリストに登録する権限をもった機関からの連絡は注意を要する。返信をするかどうかは別として，対処しない場合は，対象となる IP アドレスやホストをブラックリストに登録してしまうため，関連するサービス全体が巻き添えを食う恐れがある。（掲示板のアクセス制限も同様。同じアクセスポイントからの全アクセスを制限してしまうので，掲示板へのアクセスや書き込みを許す場合は，原因を取り除いた上で，アクセス制限の解除依頼をせざるを得ない。）
③ 企業や個人が自営するメールサーバや，掲示板に対する SPAM や荒らし等の攻撃についての苦情も取扱いに注意を要するが，学校として故意に SPAM や業務妨害を行っていない限り，法的手段（訴訟や刑事告訴等）に訴えると脅されても攻撃の原因を取り除くことに集中し，淡々と対処してよい。

【別紙１】

インシデント発生・再発防止策に関する報告・申請書

<table>
<tr><td colspan="3">インシデント管理番号：</td><td rowspan="3">受理者確認</td><td rowspan="3">年　月　日
□情報セキュリティ推進責任者
□情報セキュリティ副責任者
□情報セキュリティ責任者
□その他（氏名，役職，連絡先）</td></tr>
<tr><td colspan="2">発見・通報日</td><td>年　月　日</td></tr>
<tr><td colspan="2">被害の範囲</td><td>□（　　）部局内（部署名：　　）
□全学　□学外（相手方名称・サイト）</td></tr>
<tr><td colspan="3">被害の有無：□有　□無（未遂）</td><td rowspan="3">発見者・通報者及び認知経路・発見方法</td><td rowspan="3">学外（氏名，所属，連絡先*1）
□情報センター経由
□総務課経由
申告・請求内容</td></tr>
<tr><td colspan="2">被害を受けた期間</td><td>年　月　日～　年　月　日</td></tr>
<tr><td rowspan="5">被害対象</td><td colspan="2">関連システム／ネットワークの名称・概要</td></tr>
<tr><td>機種</td><td>□IBM PC（含む互換機）　台　□Mac　台
□その他（機種名：　　）　台</td></tr>
<tr><td>OS</td><td>□Windows（バージョン　　）
□Mac（バージョン　　）
□Unix（名称・バージョン　　）
□その他（　　）</td></tr>
<tr><td>利用目的</td><td>□学術研究
□事務
□情報公開（Web 等）
□その他（　　）</td></tr>
<tr><td>情報種別</td><td>□個人情報（　　）
□その他要保護レベル：
（　　）</td></tr>
<tr><td colspan="3" rowspan="2"></td><td rowspan="2">学内（氏名，所属，連絡先*1）
□情報センター
□情報セキュリティ推進員
□その他</td></tr>
<tr><td>権利侵害・違法行為</td><td>□名誉・信用・プライバシー
□著作権
□その他知的財産（　　）
□営業秘密・通信の秘密
□営業・業務妨害
□その他の犯罪・違法行為（　　）</td><td rowspan="2">発見方法
□目視により発見
□アンチウィルスソフトで発見
（ソフト名：　　）
□ツール類のログ
（ツール名称：　　）
□その他疑いを持った状況</td></tr>
<tr><td colspan="3" rowspan="2"></td><td rowspan="2">通知先</td><td rowspan="2">（氏名，所属，連絡先*1）
□center@yuge.ac.jp
□その他の ML（　　）
□情報処理教育センター
□企画広報室
□情報セキュリティ推進責任者
□情報セキュリティ副責任者
□情報セキュリティ責任者/非常時対策本部
□最高情報セキュリティ責任者
□法律専門家
□その他（保護者，警察等）</td></tr>
<tr><td colspan="2">インシデント種別</td><td>□対外的　□対内的
□物理的インシデント
□システムインシデント
□コンテンツインシデント
□その他利用規程違反
（違反内容　　）</td><td>物理的被害状況</td><td></td></tr>
<tr><td rowspan="4">感染／攻撃経路・手口推定</td><td colspan="2">実施していたセキュリティ対策
（　　）</td><td rowspan="4">応急措置・日時</td><td>年　月　日　時　分</td></tr>
<tr><td colspan="2" rowspan="3">□国内　□海外　□不明
□電子メール　□ダウンロードファイル
□Web サイト閲覧　□外部からの媒体
□パスワード盗用
□セキュリティホール悪用・設定不備
（ソフト名・バージョン：　　）
□その他（　　）</td><td rowspan="3">□パッチ・サービスパック適用
□アンチウィルスソフトで駆除または削除
（社名：ソフト名：　　）
□フリーの専用駆除ソフトで駆除
（ソフト名，またはダウンロード先の URL 等）
□ファイル（メール）の削除　□初期化
□情報発信関連サーバ・BBS 等の一時停止
□権利侵害・違法コンテンツ送信の一時停止
□その他（　　）

・回復に要した人日　（　）人・（　）日
（0.5 日単位で記述）</td></tr>
<tr><td rowspan="2">被害状況セキュリティ</td></tr>
<tr><td>攻撃手法・ウィルス名称（不明な場合は症状）

攻撃（未遂）の種別：
□ファイル／データ奪取，改竄，消去，破壊
□不正プログラムの埋込み
（トロイの木馬，ボット，バックドアなど）
□権限取得　□踏み台
□サービス妨害
□資源利用（ファイル，CPU 使用）
□メールの不正中継
□メールアドレス詐称
□その他（　　）</td></tr>
</table>

インシデントへの対応方針		対処方針の承認権限者承認*1　年　月　日
対処実施者	（役割，氏名，所属，日付，連絡先）	（役割，氏名，所属，連絡先）
対処区分	□緊急　□非常時対策本部の設置 □通常　□再現待ち □通常の利用規程違反	□情報セキュリティ推進責任者 □情報セキュリティ責任者 □最高情報セキュリティ責任者
方針の詳細	□情報機器・システム復旧計画 （内容）	
	□学外クレームへの応答　□対外クレームの実施 （内容：　　） □個別システムの停止／ネットワークからの分離　□特定利用者アカウントの停止 □発信者である利用者への通知，注意，警告，当事者間紛争解決要請	

	インシデントへの対処結果	対処結果の審査者確認*1　年　月　日
原因		（役割，氏名，所属，連絡先） □情報セキュリティ推進責任者 □情報セキュリティ責任者 □最高情報セキュリティ責任者
技術的対応	□パッチ・サービスパック適用（パッチ・サービスパックの全てを列挙） □ソフトウェア・プログラム設定変更（ソフトウェア・プログラムの名称，設定作業内容を明記） □ソフトウェア・プログラム更新・削除（改竄されたものを回復した場合も含む） （ソフトウェア・プログラムの名称を明記） □機器撤去（永久使用しない場合のみ） □その他（以下に詳細を明記）	
事務的対処	□利用者の懲罰委員会への報告 □外部機関への連絡・通報・届出（警察，JPCERT,IPA 等） □民事訴訟他の民事手続きの提起・応訴等	

インシデント再発防止策		インシデント報告受理者確認　年　月　日
実施予定日　　年　月　日		再発防止策許可者承認　　年　月　日
実施者	（役割，氏名，所属，連絡先） □情報セキュリティ推進員 □情報セキュリティ推進責任者 □情報セキュリティ副責任者 □情報セキュリティ責任者	（役割，氏名，所属，連絡先） □情報セキュリティ推進責任者 □情報セキュリティ副責任者 □情報セキュリティ責任者 □最高情報セキュリティ責任者
インシデント再発防止策の詳細*2		

【報告・申請経路】インシデントの発見者→受理者（インシデントの内容により情報セキュリティ推進責任者，情報セキュリティ副責任者または情報セキュリティ責任者が受理）→対処実施者→対処方針の承認権限者（インシデントの内容により必要に応じて受理者より上位の承認権限者に回付）→対処結果の審査者（対処方針を与えた者と承認した者と同一）→再発防止策実施者→インシデント報告実施者→再発防止策許可者→最高情報セキュリティ責任者

【注1】　緊急の対処が必要なインシデントが発生した場合において，報告，審査等の手続により必要な対処が遅延することがないように留意すること。

【注2】　記入欄に全てを書き込むことができない場合，適宜添付資料として通し番号を付すこと。

*1：複数の該当者がいる場合は，それぞれ記入する。

*2：再発防止の対処を暫定的な対処から段階的に実施する場合は，途中の段階における対処についても記入する。

別紙2

不正アクセス届出様式 （第 1 報）

宛先： 国立高等専門学校機構 本部事務局 総務課情報企画係 宛

（文部科学省大臣官房政策課情報化推進室へは高専機構本部事務局から送付）

【情報企画係の連絡先】
電 話：042-662-3164
メール：joho@kosen-k.go.jp

（第1報は空欄。第2報以降文部科学省から連絡のあった識別番号を記載）

識別番号：

情報連絡日時： 平成 年 月 日 ：

◆ 情報連絡の内容 （ 別紙の有無： □有 □無 ） ※既に不正アクセスの報道等があった場合はその内容を添付すること

項目		情報の内容
不正アクセスが発生した機関・部署 （発生場所、担当者の連絡先）		住所： 機関名： 届出者氏名： TEL： FAX： E-mail:
不正アクセスが発生した業務（サービス）		
被害の他機関・部署への波及可能性		
不正アクセスの概要等	業務（サービス）への影響 （業務の状況）	
	不正アクセスが発生した日時	平成 年 月 日（ ） 時 分
	不正アクセスが発生したシステムの概要	
	不正アクセスの手法	
	発生した事象	
	復旧状況及び復旧見込み	
	実施した対策の概要	
	その他の概要 （発見方法，高専機構本部以外に連絡を行った先等）	
情報の取扱い（共有範囲等）について留意すべき事項等		

※高専機構本部事務局 記載欄 （高専側での記載は不要）

◆報道発表の有無（□有 □無） ◆警察への通報の有無（□有 □無）

【報道発表及び警察への通報は，当該高専と本部事務局と協議の上決定する】

［様式バージョン Ver.1 20131101］

【別紙３】

****

【不正アクセス届出様式（詳細報告)】

****

年　　月　　日

（届出者）
住所：(都道府県まで)
高専名：
氏名：
TEL:
FAX:
E-mail:

１．届出者の業務種別：

□エンドユーザ　　□システム（ネットワーク、サーバ）管理者
□ネットワークサービス事業者　□ハードウェア・ソフトウェアのベンダ
□その他（　　）

２．被害を受けたシステム構成：

2-1) インターネットへの接続形態：

□常時接続（□専用線　□CATV　□ADSL　□その他（　　））
□ダイアルアップ　　□その他（　　）

2-2) システムの接続形態図（書ききれない場合には別紙）：

３．発見年月日：　　年　　月　　日

４．発見方法：

□届出者自身（所属組織、委託先組織含む）　□他サイト、外部組織等からの連絡

□ツール類のログ（ツール名称：　　）

□その他（　　）

５．発見した内容（疑いを持った状況）：

６．被害状況：

6-1)被害の有無：　□被害有り　□被害無し（未遂）

6-2)被害（未遂）の種別：

□ファイル／データ奪取、改竄、消去、破壊　□権限取得　□サービス妨害

□不正プログラムの埋め込み（トロイの木馬、バックドアなど）　□踏み台

□資源利用（ファイル、ＣＰＵ使用）　□メールの不正中継

□メールアドレス詐称　□その他（　　）

6-3)被害の内容：

７．原因

８．対策

8-1)事前に実施していた対策（自由記入）

8-2)再発防止のための対策（自由記入）

９．その他