D3103 インシデント対応手順策定に関する解説書

国立情報学研究所 学術研究プラットフォーム運営・連携本部  
高等教育機関における情報セキュリティポリシー推進委員会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年2月15日  A3103 | 新規作成 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2007年10月31日  A3103 | 参考（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）と解説を追加 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2011年3月31日  A3103 | 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）を追加 | 丸橋透（ニフティ） |
| 2015年10月9日  C3102 | 刑法改正等への対応のための修正 | 丸橋透（ニフティ） |
| 2017年10月17日  C3255 | C1101（CSIRT運営規程）との整合性を確保するための修正 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |
| 2021年3月25日  D3103 | A大学CSIRTの仕様への整合性の確保及び  文書の位置付けを解説書に変更 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

　サイバー攻撃や利用者等による規定違反又は過失等により発生したインシデントへの対応については、可能な限り迅速かつ漏れの無い対処が求められることから、あらかじめ実施要領や対応マニュアルに具体的な手順を明記しておかなければならない。一方で、高等教育機関（以下、「本学」という。）におけるインシデント対応体制や報告に関するエスカレーションのルート等は組織ごとに異なることから、それぞれの実情に即して対応手順を個別に定めることになるだろう。

　本文書ではインシデント対応手順（以下、「手順」という。）の策定にあたって、記載の必要性や既存の他規程等との整合性等、考慮することが望ましい内容について解説する。

## 1. 手順の位置付け及び既存の他規程等とのデマケーション

　あらかじめ、手順の位置付けを明確にしておくことが望ましい。次に例示する。

* 本学CSIRTで取り扱うインシデントについての対応を定めるもの。

　なお、手順において扱うインシデントの中には、個人情報漏えい事故のように別規程で取扱が定められているものが存在する。一方で、そのようなインシデントについても、対応は手順に従って行うことが適切な場合があり得る。考慮すべき規程等を例示する。

(1) 個人情報保護規程、特定個人情報保護規程等

　いずれも対応する規程が存在することが前提であり、各規程等において規定されている内容との整合性を考慮する必要がある。

(2) 事業継続計画等

　自然災害、情報セキュリティ事象に該当しないシステムトラブルやネットワークの輻輳等、本学の事業継続計画の対象となっている事業に起因するインシデントについては、同計画において定められている対応手順等との整合性を考慮する必要がある。

(3) 情報サービス利用規程、就業規則、学則等

　以下に例示する事象は、手順で扱うよりも情報サービス利用規程や就業規則、学則等で対応することが適切とも考えられるので、扱いを考慮する必要がある。

* 教職員や学生による、違法性はないが、本学構成員としての社会的責任や倫理性を損なう恐れのある情報発信
* 学内の情報システムやネットワークを用いた他人の名誉・信用の毀損行為

## 2. 対象とするインシデントの種類

　本学におけるインシデントのうち、手順の対象とするインシデントを明確にしておく必要がある。具体的には、次のうち(1)と(2)を対象とすることが考えられるが、他の手順等の整備状況によってはこれとは異なる扱いとすることが適切な場合もあり得る。

(1) 情報セキュリティインシデント

　本学で扱う情報並びに情報システム及びネットワークにおける機密性、可用性、完全性の健全性に影響するインシデントをいう。以下に例示する事象により、具体的な被害が発生しているもの及び今後被害の発生に繋がる恐れのあるものが該当する。

* システムの稼働妨害、またはデータの漏えい、改ざんや消失を起こす行為
* 過失による情報の漏えい、消失、改ざん
* 大量のスパムメールの送信
* マルウェア感染
* ネットワークの帯域やディスク・CPUの浪費で機能不全や障害または利用者の迷惑となる行為
* 利用者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
* 脆弱性や不適切なアカウント管理の利用によるセキュリティ侵害行為
* 不正アクセス禁止法違反行為
* サービス不能攻撃
* P2Pソフトウェアの利用
* 禁止された方法による学外接続

(2) コンテンツインシデント

　本学が管理責任を負う情報システム又はネットワークを用いて保有又は発信される情報（以下、「コンテンツ」という）に係る違法行為又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）によるインシデントをいう。以下に例示する。

* 児童ポルノ画像の所持
* 著作権侵害等の他人の権利を侵害する情報発信行為
* 他人及び本学の名誉・信用毀損にあたる情報の発信
* 他人の個人情報やプライバシーを侵害する情報の発信
* 守秘義務違反情報の発信
* ネットワークを利用したねずみ講
* 差別、侮辱、ハラスメント情報の発信
* 本学情報システムを用いた営業行為

## 3. インシデントの受付と切り分け

(1) インシデントの受付窓口

　問題発生時の対処を迅速・確実に行うためネットワーク運用と利用の問題についての学外・学内の連絡・通報窓口を設定しておくことが必要である。窓口に関する規定例を次に示す。インシデントの種類によっては、CSIRTで扱うことが適切でないものも含まれることから、他の窓口（例：学生課）等との切り分けを明記することが考えられる。

表 1　受付窓口の規定例

|  |
| --- |
| 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。    1. 学内窓口：CSIRT    2. 学外窓口：CSIRT／広報部門 2. 学外窓口への学外からのe-mailによる連絡手段は、[緊急連絡網参加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: abuse@example.ac.jp   1. 学外への連絡・通報に当たっては、CSIRT及び広報部門との連絡を密にし、無断で行わないものとする。 |

　連絡窓口は部署別あるいは機能別に複数設置してもよいが、問題の切り分けが効率的にできるならば、一箇所に集中して設け、関連部門の技術責任者や部局技術担当者等、学内への連絡網を整備し情報を配布することでも対応できよう。対外的連絡・通報については、全学広報部門との役割分担を明確にし、情報共有と意思疎通を密接にする必要がある。

　メーリングリストのアドレスあるいは自動転送をして関係者で同時に情報共有をすることなども考えられるが、いずれにしても一次対応する責任者を明確にしておく必要がある。

　特に、利用者等により違法行為がなされたおそれがあるとする被害者との対応や関連する捜査や取材の対応については、慎重にする必要がある。

　CSIRT以外で検知されたインシデントがCSIRTに報告されるまでの主要なパスを次図に示す。留意すべきは、CSIRTが設置する公式の受付窓口に直接連絡が来るものだけでなく、機関内の他部局や構成員を経由するものが存在することである。ゆえに手順において、これらの部局・構成員からの連絡手順を明示する必要がある。



図 1　インシデントの受付パス一覧

(2) インシデントの切り分け

　インシデントについて、部局技術責任者が発見あるいは通報によって認知した場合の対応手順は、あらかじめ管理者向けマニュアルに明示しておかなければならない。

　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および、当該様式を利用した報告・記録・申請・承認の要領については、「インシデント報告･承認要領」及び別紙を参照すること。

　コンテンツインシデントについては、慎重な法的判断を要することが多く、また通信の秘密あるいはプライバシー保護の観点から、部局技術責任者と部局技術担当者が立ち入ることが適当でない場合が少なくないため、部局技術責任者がコンテンツインシデントと判断した場合は、部局総括責任者に一次判断を求めるものとする。一方、情報セキュリティインシデントに関する問題については、利用規定違反の判断が比較的容易であること、被害の拡大防止のために緊急の技術的対応が必要となる場合も少なくないことなどから、部局技術責任者と部局技術担当者の一次判断が重要となる。なお、コンテンツインシデント及び情報セキュリティインシデントの両方に該当するインシデント（例：秘密保持義務のある情報がサイバー攻撃で漏えい）の場合は、両方のエスカレーション手順に従う必要がある。このとき、インシデント発生時点では原因や影響が明確でないことも多く、確定的な対応ができないことに留意する必要がある。

表 2　インシデントと影響範囲による役割・責任分担例

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| インシデント分類 | | 情報セキュリティインシデント | | コンテンツインシデント | |
| 影響範囲 | | 対外・全学 | 部局 | 対外・全学 | 部局 |
| 全学実施責任者 (非常時対策本部) | | ◎▲ | ------------ | ◎▲ | ◎（定形以外） |
| CSIRT | | ○ | ○ | ○ | ○（定形以外） |
| 情報メディアセンター （非常時窓口） | | ○ | ○ |  |  |
| 部局総括責任者 | |  | ◎ |  | ○(定形のみ◎) |
| 部局技術責任者 | | △ | ▲（定形のみ◎） | △ | △ (定形のみ▲) |
| 部局技術担当者 | | △ | △ | △ | △ |
|  |  |  |  |  |  |
| ◎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 | | | | | |



図 2　インシデントの把握状況に基づく分類

　以下に規定例を示す。

表 3　インシデントの対応判断のエスカレーション手順例

|  |
| --- |
| 1. CSIRTは、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、全学総括責任者、全学実施責任者、部局総括責任者、部局技術責任者、部局技術担当者のうち関係する者にインシデントの初期対応を依頼するものとする。 2. 情報メディアセンターは、CSIRTとの連携のもと、全学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し、部局ネットワークにのみ関連するインシデントについては、部局技術責任者を支援するものとする。 3. 部局技術担当者は、インシデントを発見し、またはCSIRT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、ただちに部局技術責任者に状況報告するものとする。 4. 部局技術責任者は、インシデントを自ら認知するか部局技術担当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. 部局内ネットワークに閉じた技術的問題か   i) 物理的インシデントまたは情報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、部局内ネットワークにのみ影響が生じている場合、部局技術担当者に対策を指示し、対策結果を部局総括責任者に状況報告する。  ii) i)以外の場合、部局総括責任者を通じてCSIRT及び全学実施責任者に状況報告をし、CSIRT及び情報メディアセンターの支援を仰ぎながら、物理的インシデントまたは情報セキュリティインシデント対応のプロセスを実施する。   * + 1. コンテンツインシデントか   i) コンテンツインシデントの場合、加害者と被害者が部局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、原則として部局総括責任者を通じて全学実施責任者に報告をし、CSIRT等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。  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で、部局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、部局総括責任者と全学実施責任者に結果報告をする。   1. 部局技術責任者は、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部局技術担当者に指示を与え、部局総括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部局総括責任者に報告し、指示を受けることとする。 2. 部局技術責任者から報告を受けた部局総括責任者は、コンテンツインシデントについて、部局技術責任者・部局技術担当者を指揮監督する。情報セキュリティインシデント対応については、ポリシーに基づいて全学実施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については、法務担当部門に対応を依頼する。 3. 学外からの申立か、対外クレームか    * 1. 全学実施責任者は、学外からの申立により認知したインシデントの場合、学外からの申立対応プロセスを併せて実施する。      2. 全学実施責任者は、法務担当部門に相談しながら、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定違反対応とする。 |

## 4. インシデント報告のエスカレーション

　文部科学省等への報告が必要なインシデントかどうかは、被害の深刻さによって異なる。次表に示すように、一般に情報の機密性に関わるインシデントの場合は報告の対象となる場合が多く、完全性や可用性に関わるインシデントの場合は、機関の事業運営に深刻な影響を及ぼすものでない限り、報告の必要は無いと考えられるが、機関の状況によって異なる面も存在することから、事前に機関内で検討し、報告基準として手順を含めて規定しておくことが望ましい。

表 4　被害の内容に応じた報告の必要性についての指定例

|  |  |  |  |
| --- | --- | --- | --- |
| 事例 | 報告要件 | | |
| 機密性 | 完全性 | 可用性 |
| 学内サーバのデータ誤消去 |  | △ |  |
| アクセス制限設定ミスで情報漏えい | ● |  |  |
| 大学の秘密情報が学外サーバ上で公開 | ● |  |  |
| 教員のPC紛失 | ● | △ |  |
| 学内サーバ上に違法コンテンツ |  |  |  |
| 大学ホームページの改ざん |  |  |  |
| 学生の成績データベースの改ざん |  | △ |  |
| 学内サーバがランサムウェア感染 |  | △ |  |
| 不審なアクセスログを検知 |  |  |  |
| サークル用無料サイトが乗っ取られて悪用 |  |  |  |
| DDoS攻撃 |  |  | △ |

●＝情報の種類によって報告の有無を決定

△＝被害の深刻さに応じて報告



図 3　報告要否に関する判断のフロー例

## 5. インシデントの種類に応じた対応手順

**5.1 情報セキュリティインシデント発生時の対応**

　情報セキュリティインシデントに対して、技術的対応とともに重要となるのが、事後の対応による見直しである。組織においていかに技術的対応を強固にしても、組織をインターネットに接続する限り常に情報セキュリティ上の脅威は存在しているのであって、潜在的かつ必然的にインシデントに対応しなければならない状況にあることをまず理解しなければならない。

　具体的な手順の策定にあたっては、次の資料を参考にすることができる。

* インシデントハンドリングマニュアル（JPCERT/CC）  
  <https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf>
* ISO/IEC 27035-3:2020  
  Information technology - Information security incident management -  
  Part3: Guidelines for ICT incident response operations

　手順の策定例を示す。

表 5　情報セキュリティインシデントに関する対応手順例

|  |
| --- |
| 1. 発生から緊急措置決定まで    1. 監視システムによる情報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、通報等で情報セキュリティインシデントの可能性を認知した部局技術担当者は、事実を確認するとともに部局技術責任者に報告し、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. 部局技術担当者は、後日の調査に備え、情報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。    3. CSIRT責任者は、情報セキュリティインシデントの原因と見込まれる情報システムや被害を受けていると見込まれる情報システムを所管する部局総括責任者及び部局技術責任者に対し、証拠保全や被害拡大防止のための措置への協力を求めることができる。    4. 情報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、部局総括責任者の承認を得て部局技術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. 部局技術責任者は、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、実施を部局技術担当者に指示する。    2. 部局総括責任者および部局技術責任者は、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. 部局技術責任者は、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. 部局技術責任者は、緊急の被害拡大防止措置を実施する場合は、部局総括責任者に報告する。    2. 部局総括責任者は、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、部局総括責任者は学内窓口を通じて全学実施責任者に連絡する。    3. 全学実施責任者は、CSIRT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、全学総括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. CSIRTは、全学実施責任者また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サイトへの連絡、及び関係機関への報告などを指揮する。    5. 非常時対策本部が設置された場合、CSIRT、部局技術責任者及び部局技術担当者は、その指示に従うものとする。 4. 復旧計画    1. 部局技術担当者は、情報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。    2. 部局技術責任者は、復旧計画を検討し、部局総括責任者（全学ネットワークに影響する場合は全学実施責任者）の承認を得て実施する。   (5) 原因調査と再発防止策   1. 部局技術担当者は、情報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。 2. 部局技術責任者は、利用者等への注意喚起等を含めた再発防止策を検討し、部局総括責任者（全学ネットワークに影響する場合は全学実施責任者）の承認を得て実施する。 3. 部局技術担当者と部局技術責任者は、インシデント対応作業の結果をまとめ、部局総括責任者は、再発防止策とともに全学実施責任者に報告するとともに、必要によりポリシーや実施規程の改善提案を行う。 4. 全学実施責任者は、部局総括責任者から情報セキュリティ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、全学総括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。 |

**5.2 コンテンツインシデントに関する緊急対応**

　コンテンツインシデントのうち、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）が含まれるものを認知した場合の対応について、通常の手順とは別に緊急対応のための手順を定めることが考えられる。以下にその例を示す。

表 6　コンテンツインシデントに関する緊急対応

|  |
| --- |
| 1. CSIRT担当者は、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、または報告等により認知した場合、CSIRT責任者の指示（予め許可を与えておく場合を含む）によりコンテンツの情報発信元を探知し、その結果をCSIRT責任者に報告するものとする。 2. CSIRT責任者は、全学実施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。 |

**5.3 学外からの申立への対応**

　コンテンツインシデントのうち、学内から情報発信されているコンテンツに対する送信中止・削除要求等の申立への対応については、申立内容の妥当性や法的根拠について、法律専門家の助言をもとに判断することが必要な場合も多いことから、これらの取扱に関する手順を定めることが考えられる。以下にその例を示す。

表 7　学外からの申立への対応手順例

|  |
| --- |
| 1. 原則 2. 学外からの申立を受けた場合で、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。 3. 部局技術責任者は、学外からの申立については、部局総括責任者及び全学実施責任者に報告を行ものとする。 4. 学外からの申立についての報告を受けた全学実施責任者は、全学総括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。 5. 全学実施責任者または非常時対策本部は、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、部局技術責任者及び部局技術担当者は、その指示に従うものとする。 6. 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 7. 発信元利用者等の特定   学外からの申立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またはその代理人からなされたものである場合、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。   1. （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    * 1. 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。      2. 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。 2. （緊急手続き）利用者等への通知前の一旦保留    * 1. 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。      2. 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。      3. 本緊急手続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。   解説：「プロバイダ責任制限法ガイドライン等検討協議会」の各ガイドラインを参照。 http://www.telesa.or.jp/consortium/provider   1. 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   (ア) 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。  (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. 部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。  b. 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。  解説：情報内容についての刑事的な違法性判断は困難な場合が多く、基本的には、発信元利用者等の反論を待ってから送信防止措置を講ずることとする。   1. 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   i)（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   * 学外からの申立が利用者等による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、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。 * 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。 * 利用者等から有効な反証があれれば、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、Ａ大学の処罰の手順に移行する。   ii)（情報セキュリティインシデント対応）利用者等のアカウントの一時停止   * 学外からの申立が利用者等による１対１の情報発信による情報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、部局技術担当者は、事実関係を調査し、発信元利用者等を特定する。 * 部局技術担当者は、事実を調査し、発信元利用者等を特定する。 * 部局技術担当者は、利用者等の行為が情報セキュリティ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、部局技術責任者に報告し、その判断を求めるものとする。 * 部局技術担当者からの報告を受けた部局技術責任者は、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、部局情報システム運用委員会に報告する。 * 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。 * 利用者等から有効な反証があれれば、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、Ａ大学の処罰の手順に移行する。   解説：プロバイダ責任制限法第3条は、不特定の者により受信される通信（ウェブサイト、ブログや電子掲示板等によるいわゆる公然性を有する通信）を対象としており、インスタントメッセージやメールのような1対1の通信には適用されない。従って、脅迫メール、特定のメールボックスをターゲットにしたメール爆弾や、特定サーバへのクラッキング等、システムの機能障害を引き起こす通信やコンテンツが問題となる場合であっても特定の者相手の通信には適用がない。 しかし、プロバイダ責任制限法の適用範囲には入らず、免責の対象とはならないとはいえ、学内ネットワークの利用規定が、これらの行為についても手続きを明確にして利用規定違反とし、外部からの送信停止要求についても対応できるようにすることは法律上問題はない。これは学問の自由や表現の自由との関係においても問題が少ないと考えられる。   1. 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. 学外からの申立に対して、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。   解説：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があった場合には、法律の専門家と共に対応する必要がある。 　プロバイダ責任制限法第3条第1項により、損害賠償責任の免責を受けられる場合とそうでない場合がある。都立大学事件判決やニフティ事件第二審判決のように、最終的にネットワーク管理者としての損害賠償責任を負わないこととされた事例、ニフティ事件第一審判決や２ちゃんねる事件のように損害賠償責任を負うとされた事例が存在するため、慎重な判断が求められる。具体的な削除請求が事前または同時になされている場合には、上記(1)または(3)の手続きに従っていることにより作為義務違反が無いとされ、損害賠償責任を負わないとされる有力な根拠となり得る。   1. 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. 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。  b. 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。  解説：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必要がある。プロバイダ責任制限法第4条に基づく手順としては、概ね下記の通りとなる。   1. 発信者情報の保有の有無、技術的に特定できるかどうかの判断   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。   1. 発信者情報開示請求の根拠の確認と違法性の判断   必ず法律の専門家に相談する。   1. 開示について発信者の意見を聞く。 発信者が開示に同意すれば開示してよい。 2. 発信者情報開示をする法律要件を確実には満たしていないと判断すれば開示を拒否する旨通知する。不開示の判断に故意または重過失がなければ責任を問われないので、少しでも法律要件を満たさない事実があれば、不開示判断をすべきである。 3. 発信者情報開示の要件に該当することが確実である場合には開示できる。しかし、開示判断を誤った場合には電気通信事業法や有線電気通信法上の通信の秘密侵害罪やプライバシー侵害による損害賠償責任からは免責されないため、慎重な判断を要する。発信者が開示に同意しない場合、特に慎重な判断を要する。   解説：「プロバイダ責任制限法ガイドライン等検討協議会」の発信者情報開示関係ガイドラインを参照。 http://www.telesa.or.jp/ftp-content/consortium/provider/pdf/ provider\_hguideline\_20160222.pdf   1. 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。  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。   1. 強制捜査による発信者情報の差押え、記録命令等    * + - 1. 部局技術担当者は、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。          2. 部局総括責任者もしくは対外折衝事務担当者は、部局技術担当者の協力を得て、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。          4. 部局技術担当者は、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。   解説：情報処理の高度化等に対処するための刑法等の一部を改正する法律のうち手続法部分の施行（2012年6月22日）により、記録命令付差押え（刑訴法99条の2・218条）、保全要請（刑訴法197条3項）の手続きが新設された。 また、①データではなく、ＰＣやサーバが差押え対象となった時には、リモート接続しているネットストレージにあるデータ等令状に記載された範囲のデータを複写する（刑訴法99条2項・218条2項・219条2項）　②記録媒体（ハードディスク等）が差押え対象となった場合に、記録媒体から必要なデータのみを複写・または移転する（刑訴法110条の2・222条1項）手続きも追加されている。 （ア）の準備作業は、従来手法である差押え（刑訴法99条）と新設の記録命令付差押えに共通するものである。従来から発信者情報等を出力した紙や記録媒体を差押える手続きは行われてきたが、発信者情報等を特定する作業により、利用者の通信の秘密を侵害したとされるリスクが皆無であるとは言い切れなかった。強制的な記録命令の対象となることによりそのリスクは無くなり、従来からの捜査協力手法が正面から認められることとなった。 （イ）の折衝により、サーバ等、サービス稼働に重大な影響を及ぼすハードウェアの差押えを回避すべく努力すべきである。 （ウ）の立会時には、リモートアクセスや、データの複写・移転についてサーバの操作を協力する一方、令状記載の範囲内で複写されたか確認すべきである。 （エ）は将来の通信ログの保存ではなく、要請時に現に残存している通信ログを30日(延長しても最大60日)間消えるままにしないようにすること（保全）を要請するものである。なお、保全したはずのログが消失しても罰則は無いが、セキュアな保管方法を選択すべきである。 |

**5.4 通常の利用規程違反行為の対応**

　本学のD2201（情報サービス利用規程）に対する違反行為についても、頻出行為への効率的な対応を可能にするとともに、担当者による判断のブレなどを防ぐ観点から手順を定めておくことが望ましい。以下にその例を示す。

表 8　利用規程違反行為に関する対応手順例

|  |
| --- |
| 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）   部局技術担当者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部局技術責任者に報告する。   1. 利用規定違反の該当性判断   部局技術担当者の報告を受けた部局技術責任者は、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、その旨部局総括責任者に報告し、確認を得るものとする。  部局技術責任者は、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部局総括責任者に報告するものとする。  部局総括責任者は、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、必要に応じて部局情報システム運用委員会の判断を求めるものとする。   1. 情報発信の一時停止措置   部局技術担当者は、部局総括責任者または部局技術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またはアカウントの一時停止措置等を実施する。   1. 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   部局技術責任者または部局総括責任者は、事案に応じて下記内容を発信者に通知するものとする。   * 利用規定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 * 利用規定違反行為の是正、中止の要請 * 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） * 反論を受け付ける期間とその効果 * 利用者等当事者間の紛争解決の要請  1. 個別の情報発信またはアカウントの停止と復活 2. 部局総括責任者または部局技術責任者は、(4) の措置を講じたときは、遅滞無く全学実施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、必要に応じ部局情報システム運用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、学内処分の開始手続き- * 利用者等の当事者間の紛争解決着手の有無の確認 |

**6. 学内処分との関係**

　部局総括責任者は外部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、本学懲罰委員会への報告をすることができる。また、本学懲罰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。これらの内容を手順に記載してもよい。

**7. 手順策定の参考となる情報源**

**(1) CSIRTマテリアル（JPCERT/CC）**

　組織内CSIRTの構築・運用に係るプロセス等の説明資料が公表されている。

<https://www.jpcert.or.jp/csirt_material/>

**(2) CSIRTスタータキット（日本CSIRT協議会）**

　CSIRT を構築する際に注意し取り組むべき課題や定義すべき事項、組織におけるインシデントレスポンスの計画を構築する際に取るべき手順等について紹介。

<https://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf>

**(3) セキュリティ対応組織の教科書（日本セキュリティオペレーション事業者協議会）**

　セキュリティ対応組織において求められる共通的な機能や役割を書き出した上で、それらをどのように組み合わせ、実行していくべきなのか、セキュリティ対応を専門に実施しているセキュリティオペレーション事業者の知見をエッセンスとして取りまとめたもの。

[https://isog-j.org/output/2023/Textbook\_soc-csirt\_v3.html](https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html)

**(4) ISO/IEC 27035（国際標準化機構, 国際電気標準会議）**

　情報セキュリティインシデント管理に関する国際規格。ただし2023年3月時点で日本語化はされていない。次の３部が標準規格化されている。

* ISO/IEC 27035-1:2023　第１部：原則とプロセス
* ISO/IEC 27035-2:2023　第２部：インシデントレスポンスのための計画と準備に関するガイドライン
* ISO/IEC 27035-2:2020　第３部：ICTインシデントレスポンスの運用に関するガイドライン

# 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Ａ大学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部局技術担当者やCSIRT等の通報先を周知・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、部局技術責任者、部局総括責任者又は全学実施責任者とする。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、部局総括責任者、全学実施責任者または全学総括責任者とする。

**4. 障害等発生から再発防止策実施までの対応**

4.1 障害等発生時における全般的な注意事項

(1) 全学実施責任者又は部局総括責任者は、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。

(2) 部局技術担当者（外部からの通報の場合、CSIRTまたは広報部門）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。

(3) 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】

(4) 部局技術担当者は、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、その旨を部局技術責任者を通じて部局総括責任者（必要により全学実施責任者）に報告し、指示を得ること。

4.2 インシデントの発見報告

(1) 自ら発見、または利用者等からの通報によりインシデントを認知した部局技術担当者（外部からの通報の場合、CSIRTまたは広報部門）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（様式○○）」（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部局技術責任者または部局総括責任者（「**インシデント報告受理者**」）に報告を行うこと。インシデント報告書に記載すべき項目としては、別紙１に示す内容のほか、必要性に応じて次に例示する項目を記載することが考えられる。

・外部報告日時（第何報かを含む）

・CISO報告日時（何報かも含む）

・インシデント発生日時

・インシデント概要

・個人情報・特定個人情報漏えいの恐れがある場合や他社へ被害拡大させるおそれがある場合の対応／措置

・公表／Web掲載への対応状況

・公表内容

・外部機関との連携状況

・その他報告事項

・インシデント発生の原因や要因、想定される攻撃手法

・システム（サービス、サーバ等）のIPアドレス、URL／ドメイン名

・攻撃元（者）IPアドレス、URL／ドメイン名

・インターネットへの接続形態／経路

・感染したウイルス（マルウェア）の名称、利用された脆弱性

・被害システム（端末）のOS／バージョン

・ウイルス（マルウェア）感染経路等

・その他特記事項

(2) 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**の指示により部局技術担当者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。

(3) **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。

(4) **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abuse@example.ac.jp等の連絡網を活用し、部局総括責任者、全学実施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。

(5) 全学実施責任者は、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。

4.3 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、部局総括責任者または全学実施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。

4.4 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からの申立対応時の留意点

**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**

　学外からの申立があった際、C3102に基づき調査の上、対処するが、学外からの申立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（ご指摘ありがとうございます、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、以下のとおりのみ。

(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

・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

・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

・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。

(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、訴訟され反証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. 情報セキュリティインシデントの連絡への対処**

(1) 他機関からの連絡への返信の際には、できるだけ正確な表現となるように努める。

(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、大学として故意に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。