S-1. インシデント発生時の対応手順

私情協セキュリティ研究講習会

情報セキュリティ事故等発生時の対応

対応手順		対応内容
１．検知（通知・確認）	1	情報セキュリティ事故等に関する兆候や具体的な事実を確認した場合、あらかじめ定めた連絡体制に従い、責任者に連絡する。
２．初動対応	2	セキュリティ委員会で対応方針を決定する。情報セキュリティ事故等による被害の拡大、二次被害の防止のために必要な応急処置と、適切な対応についての判断を行うために必要に応じて5W1H（いつ、どこで、誰が、何を、なぜ、どうしたのか）の観点で情報の整理を行う。
３．調査	3	被害の重大性や範囲、漏洩した情報の重要度の把握する。事実関係を裏付ける情報や証拠を確保し、予想される二次被害についても確認する。
４.報告・公表	4	漏洩した個人情報の本人、取引先などへの通知、文部科学省、警察、IPA、JPCERT/CCなどへの届出、Webページ等での公表を検討する。
５．2次被害防止と復旧	5	被害拡大の防止（必要に応じて、専用の相談窓口を設置する等）と、被害の内容によっては復旧作業を行う。
６．事後対応	6	根本的な再発防止策を検討し、実施する。調査報告書を作成し、被害者への適切な対応を行う。教職員の責任について、必要に応じて処分等の手続きを行う。必要に応じて、調査報告書等の情報を開示する。

事前準備（対応手順書のポイント）

1. インシデントの種別を列挙し、対応優先度を決めておく
2. 対応フローを作成しておく
3. 連絡先、担当者、作業内容まで決めておくことが望ましい
4. 調査用・復旧用のコマンド一覧を作っておくと漏れを防げる
5. 連絡票や報告書の書式を作っておく

事前準備（対応手順書例）

調査用・復旧用のコマンド一覧	・痕跡・ログ調査用コマンド ・バックアップ/リストア手順
書式類	・学内外への連絡リスト ・報告書式 ・謝罪文例／想定問答集 ・作業一覧
システム関係資料	・システム設定 ・ネットワーク構成図 ・IPアドレス一覧
組織関係資料	・学内組織図 ・業務委託先一覧

【例】標的型攻撃による情報流出

標的型サイバー攻撃の流れ

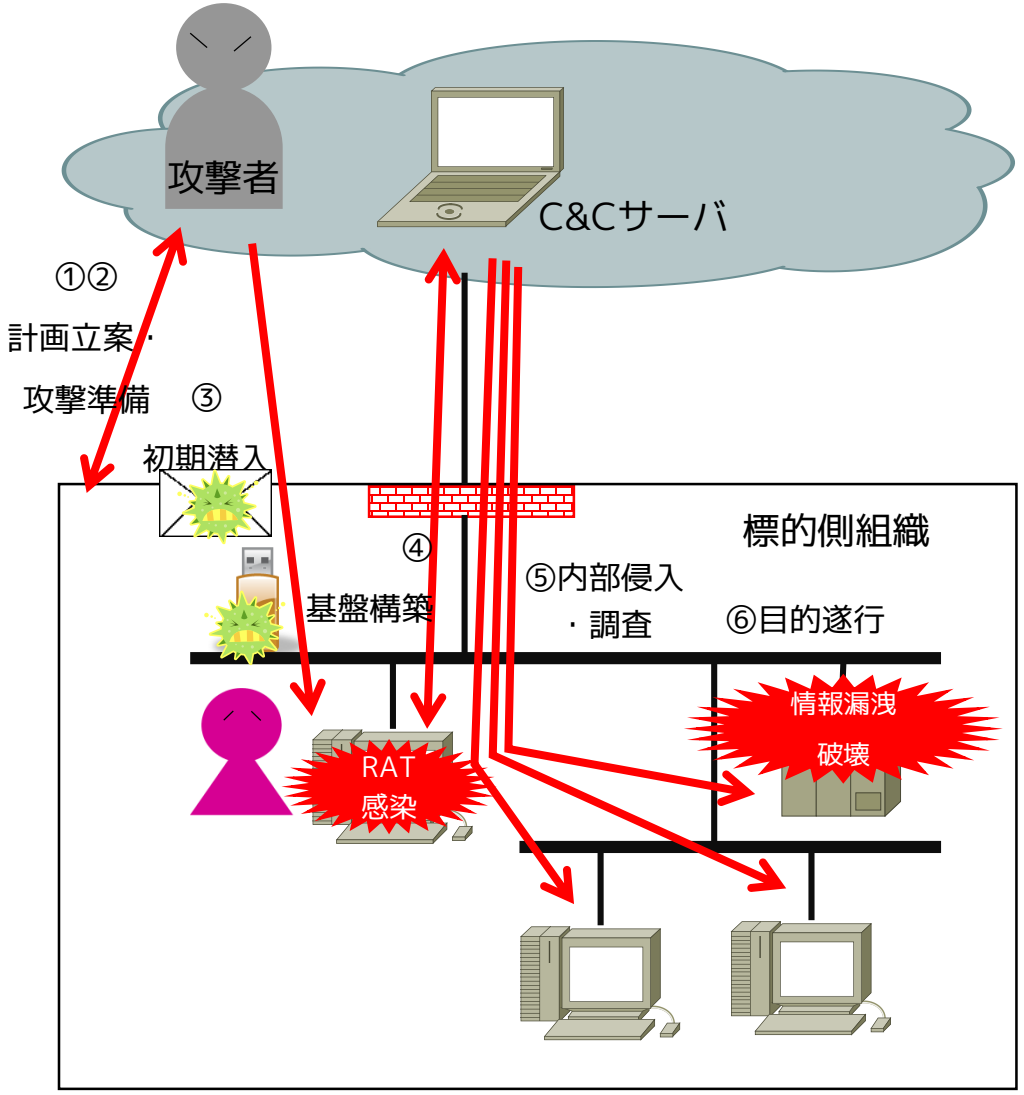
① 計画立案
② 攻撃準備

③ 初期潜入

④ 基盤構築

⑤ 内部侵入
調査

⑥ 目的遂行
⑦ 再侵入



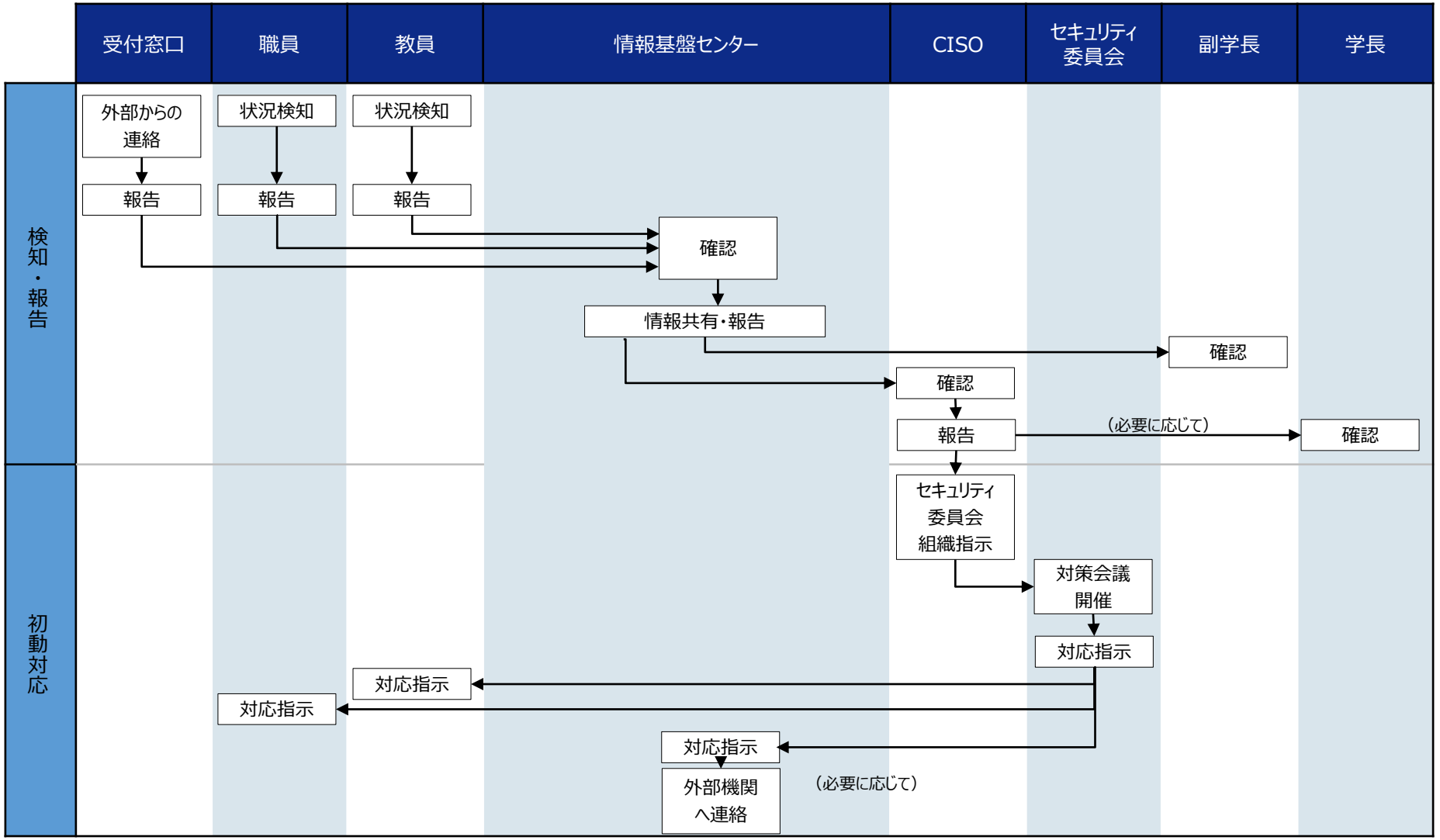
１．検知（通知・確認）

① 教員、職員が情報セキュリティ事故等の発生及びその可能性を検知した場合、速やかに情報基盤センターに連絡する。

② 連絡を受けた情報基盤センター職員は、状況を確認の上、課長およびCISOに連絡する。

③ CISOは情報セキュリティ事故等の重大性を判断し、関連部署へ初動対応・調査を指示する。また、状況により学長に報告する。

１．検知（通知・確認）


受付窓口
職員
教員
情報基盤センター
CISO
セキュリティ委員会
副学長
学長
検知・報告
初動対応
外部からの連絡
状況検知
状況検知
報告
報告
報告
確認
情報共有・報告
確認
確認
報告
（必要に応じて）
確認
セキュリティ委員会組織指示
対策会議開催
対応指示
対応指示
対応指示
対応指示
外部機関へ連絡
（必要に応じて）

【具体例】　通知メール（内容）の信憑性の確認

1. 通知メールの送信元（経路）、場所(時間）の確認
2. 迷惑メール判定（レベル）
3. 日本語文章の表現
4. 添付ファイルの有無
5. その他
   - ①　送信先の情報（Who is確認）、postmaster,abuseでない
   - ②　PGP確認
   - ③　SPF（Pass)確認

※ 送信元に別メール、あるいはメール以外の方法で確認する。

２．初動対応

① CISOは、速やかにセキュリティ委員会による対策会議を開催する。

② 対策会議内で、管理職等の学内関係者間による情報収集・整理を行い、発生した情報セキュリティ事故の重大性、緊急性の度合いを判断する（事前に判断基準を策定しておくと良い）。

③ 情報セキュリティ事故の重大性及び緊急性に応じ、初動対応担当者と初動対応の方針を定める。その後、セキュリティ委員会から初動対応担当者に対し、必要な初動対応を行うよう指示を行う。

④ ウィルス感染や、情報漏洩等（疑いを含む）を起こした当事者、その情報に関わる教職員は、初動対応担当者の指示に従い、初動対応を行う。初動対応担当者は、当事者及びその情報に関わる教職員が、個人の判断による対処を行わないよう留意する。

２．初動対応（不正プログラムへの感染）

初動対応の中で、5W1Hの観点で情報の整理を行う。

事実関係の確認	回答例	情報の確認	回答例
1. ウィルス感染した当事者は誰か。 2. ウィルス感染したのは何か。 3. ウィルス感染により漏洩した情報は何か。 4. いつ、ウィルス感染したのか。 5. どこで、ウィルス感染したのか。 6. なぜ、ウィルス感染したのか。 7. ウィルス感染が発覚した理由は何か。	教職員名 教員PC ｱｶｳﾝﾄ情報 8月19日 学内 メール開封 対策ソフトによる検知	a. 誰の情報か。 b. 何の情報か。 c. いつ頃の情報か。 d. 情報の量（件数）はどのくらいか。 e. どのような形で保存されていたか。	教員本人 ｱｶｳﾝﾄ情報 現時点 1件 パスワード保護

応急処置（例）	留意点
1. ウィルス感染したパソコンの特定を行う。 2. ウィルス感染したパソコンのネットワークからの切り離しを行う。	

２．初動対応（不正アクセス）

初動対応の中で、5W1Hの観点で情報の整理を行う。

事実関係の確認	回答例	情報の確認	回答例
不正アクセスした当事者は誰か。 不正アクセスされたのは何か。 不正アクセスにより漏洩した情報は何か。 いつ、不正アクセスされたのか。 どこから、不正アクセスされたのか。 なぜ、不正アクセスされたのか。 不正アクセスが発覚した理由は何か。	教職員名 学内ｻｰﾊﾞ 学生情報 8月19日 海外 ﾊﾞｯｸﾄﾞｱの存在 ﾛｸﾞ確認	a．誰の情報か。 b．何の情報か。 c．いつ頃の情報か。 d．情報の量（件数）はどのくらいか。 e．どのような形で保存されていたか。	学生 成績証明書 情報 昨年度 600件 暗号化

応急処置（例）	留意点
1．不正アクセスを受けた機器（サイト）のネットワークからの切り離し。 2．不正アクセスを受けた機器（サイト）の停止。 3．代替サイトの立ち上げ。	不正アクセスされた原因、経路を特定せずに代替サイトを立ち上げると、再び不正アクセスされる可能性が高い。

３．調査

① セキュリティ委員会の決定、指示に従い、システム管理者及び関連部署の関係者により事故内容の特定と事故の原因を調査する。

② 情報が漏洩した場合は、漏洩した情報の管理者により、漏洩した情報の特定を行う。

③ 予想される二次被害について、システム管理者及び関連部署の関係者、情報が漏洩した場合は漏洩した情報の管理者により、予想される二次被害について確認する。

被害の重大性や範囲、漏洩情報の重要度を把握するための質問	回答例
1. 漏洩した情報区分は何か。 2. 漏洩した情報の保護策は何を実施していたか。 3. 影響はどこにあるか 4. 管理上の問題点は何か。	1. 個人情報/機密情報/非公開情報等 2. 暗号化の実施/パスワード保護等 3. 個人/本学等 4. 端末持出管理の不備等

【具体例】　インシデントレベル判断と一次対応

1. 調査結果の報告と協議
   ① 対象端末の特定（調査）
   ② 対象端末の状況確認（依頼）
   ③ 通信記録の確認（FW, IPS/IDS, Proxy等）と保管
2. 管理者のインシデントレベル判断例

   レベル3：情報流出有、またはその可能性大

   レベル2：情報流出の実態が確認できないが、通信実態有

   レベル1：指摘端末等、その他で通信実態の確認が早急にできない

【具体例】　インシデントレベル判断と一次対応

1. インシデントレベルと一次対応
   - ① レベル３, ２
     - i. ネットワーク接続の断、端末の電源をOFFしない
     - ii. 端末の状態保持: 可能であればメモリダンプ取得
     - iii. 重要データのバックアップ（端末管理者）：専用デバイスに
   - ② レベル1
     - i. 注意観測
2. 管理者　→　CISO等上層部への報告
   - ① 情報提供・指摘時に一報報告も良
   - ② 一次対応は緊急対応であり、更に詳細調査の継続により、二次対応を検討する。なお、一次対応は安全側に立った対応が必要である。

【具体例】　二次対応

1. 調査継続による詳細情報と二次対応の検討
   ① 内部侵入：影響範囲
   ② 端末のデジタル・フォレンジング調査依頼（可否と範囲）
   ③ 複合機、プリンタ等その他機器の外部通信の確認
2. デジタル・フォレンジックの結果（1週間程度）
   ① 調査結果に基づき、情報流出である場合の外部報告・公表の優先度と内容の検討（ガバナンス）
3. 復旧対応
   ① 対象端末の復旧：クリーンインストール、端末管理の見直
   ② ネットワーク構成・ポリシーの見直
   ③ 保存データ：暗号化対策等

４．報告・公表

個人情報漏洩など学外に影響があるセキュリティ事故が起こり、公表が必要であると判断された場合、Webページでの掲載または記者会見での公表を行う。

① 透明性・開示の原則から、情報流出が発生した場合はなるべく早く公表を行う。

② 公表の前に、被害者や関係者に通知し、公表の意向を確認。

③ 問合わせの窓口は一本化し、対外的な情報に整合性確保。

④ Webページで公表の場合は、公表用資料を掲載する形で実施。

⑤ 掲載場所はトップページからリンクを張る。

４．報告・公表（Webによる公表）

公表用資料に含むべき項目（例）
1.序文（発生した情報漏洩に関するお詫び、学校としての姿勢など） 2.事故発生に関する状況報告 3.事実経緯 4.調査方法及び状況 5.漏洩した情報の内容 6.事故の被害内容（二次被害の影響含む） 7.事故原因 8.当面の対応策 9.再発防止策 10.問い合わせ窓口（事故に対する連絡先）

引用：IPA「情報漏洩発生時の対応ポイント集」

４．一次報告・公表（記者会見）

① 報道機関等から、２～３件以上の取材の依頼が来た場合、記者会見の開催を検討する。

② 報道機関等の取材に応じる場合は、電話ではなく、可能な限り対面での対応を行う。

③ 事前に報道機関にFAXにて情報（開催の概要等）を送付する。

④ 公表用資料の他、事実関係を説明する資料を準備し、正確な情報が伝わるよう配慮する。

⑤ 想定問答集を作成し、事前練習を行う。

⑥ 回答できない質問については、その場で無理に回答しようとせずに、確認の上追って回答を行う旨を伝える。

５．2次被害の防止

① 情報が漏洩した場合で、漏洩した情報に個人の機密情報（ID パスワード等）が含まれている場合は、本人に通知を行い、IDの停止等の処置を行ってもらう。

② Web上に情報が公開されてしまった場合（Webへの誤公開、ブログ、掲示板等への書き込み）は、Web検索サイト（Google等）に依頼し、キャッシュの削除をして、検索結果に表示されなくなるよう対処する。

③ 第三者に情報（ファイル等）が渡った場合は、第三者から情報の回収を行う。

６．事後対応

事故の重大性に応じ、以下の対応を行う。

① 報告書の作成

② 再発防止策の策定と実施

③ 関係者への周知

④ 情報漏洩があった場合、必要な補償等の救済措置の検討と実施

【具体例】　事後対応計画と報告・公表（継続）

1. 再発防止対応

① 全学的な適用に向けた検討および対応

i. 各種規程やセキュリティポリシーの見直し

② 調査・対応体制（組織、チーム）の見直し

③ 監視の強化（継続注意、監視の外部委託、ハニーポット等）

2. 報告・公表等（継続）

① ここまでの内容を網羅し、インシデントレベルに応じた報告・公表を再発防止対応（計画）を含めて行う（CISO）→広報部署