総合演習－1
S-1. インシデント対応フロー（モデル）による情報流出インシデント机上演習

文京学院大学　浜　正樹
中部大学　岡部　仁

このセッションの目標

情報流出インシデントに対し、その事実の確認および対応について、SJK大学インシデント対応フローに沿い、

・システム技術担当者（情報部門担当者）
・セキュリティ施策管理者（情報部門管理者）
・CISO

の三者（実務担当・利用者等を除く）の協働作業を机上演習体験する。

＝

・インシデント対応フローで対応ができるものとできないものの状況を確認する。
・大学特有の問題点について洗い出しを行う。

◆ インシデント対応フローでの演習によって得られた問題点を各大学の規程・対応手順の作成・見直しの参考となる。
◆ 対応組織の必要性と各役割を確認する。

セキュリティ対策の机上演習の効果

- セキュリティは変化の速い分野であり、担当関係者（本来は利用者も含む）はそれに追従することは永遠の課題である（**ゴールが無い**）。
- 多くの業務にICTが利用され、その管理、**対策の優先順位**、未知のリスクへの対応も必要となった。
- 入口・出口対策等の限界：　**事故ありき対応**
- 多くの関係者が未経験、**経験したくないが！**
- 多くのメンバーによる思考プロセス、行動、ツールを活用し、検討・議論をかけ、**不備を洗い出せる**。

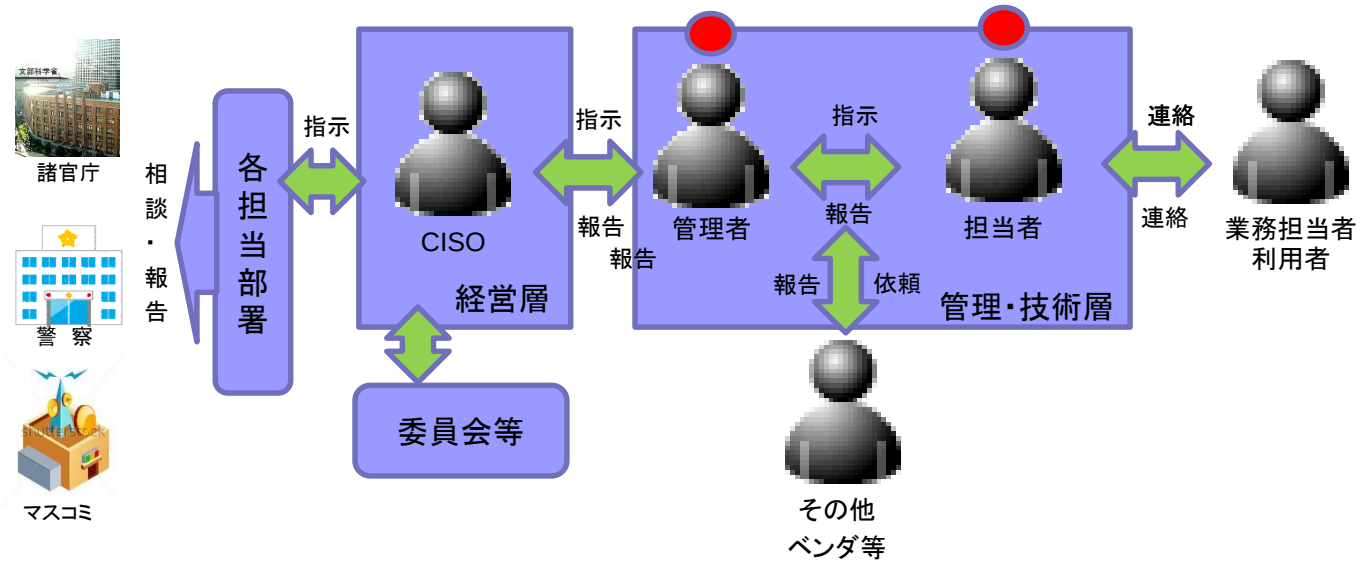
- インシデント対応は、その内容と**対応時間**が問題となる。
- できるだけ**早く検知（認識）**し、**事実を確認**し、これに正確に対応できかである。
- 大学の構成員、管理体制は、集中管理ではなく**分散管理が主流**であり、上記の対応に時間を要する。
- 教育・研究活動を阻害するためではなく、これらを安全に活用するため、また一部の利用者の問題が組織全体に悪影響を与える事態を防ぐため、**安全側に立った規程等による対応**としたい。

インシデント対応机上演習概要

- 想定： SJK大学の学生個人情報の流出対応

外部から電子メールで上記の通知があり、これに対しSJKインシデント対応フローに沿い、対応をする（机上演習）。演習内容をもとに総合演習－2では問題点等について、討議する。

- インシデント対応のプレイヤー



インシデント対応のポイント

- 大学特有の留意点
  - 現況対策の確認自体が必要、非均質な分散管理体制（教員、研究員）
  - 複数種類の構成員（学生、教員・研究員（非常勤）、事務職員、ゲスト）
  - 情報資産種別による対応の違い
    - 学生（受験者、卒業生含む）情報と父兄
    - 研究情報（共同研究、委託研究）と対外組織
    - 組織情報（営業秘密情報）
  - 調査範囲：　情報部門の調査範囲の限界
  - 業者委託（フォレンジック）の判断と予算
- 踏み台（被害者から加害者へ）：教員・研究員の認識と対応
- 被害拡大防止
  - ネットワーク接続：　抜線対応と事前対応
- 謝罪、報告、公表の時期と対象・内容の判断

総合演習-Ｓ１

インシデント対応の机上模擬演習

ワークシート

中部大学　　岡部　仁
文京学院大学　浜　正樹

資料

- インシデント対応の机上模擬演習ワークシート（本項）
- 規程集：　インシデント対応基準
- 通知メール
- 予算書
- フォレンジック調査報告書
- お詫び例文
  - お詫び文郵送版例（情報流出）
  - お詫び文Web版例（情報流出）
- 報告書
  - 【作業1】情報セキュリティ事故発生報告書
  - 【作業2】情報セキュリティ事故経過報告書
  - 【作業4】情報セキュリティ事故経過報告書
  - 【作業5】情報セキュリティ事故最終報告書
- 【作業3】稟議書

フェーズ（1）

フェーズ１：検知（通知・確認）　09:30 ～ 10:10（40分）

フェーズ２：調査および対応　　10:10 ～ 11:20（70分）

休憩（10分）

フェーズ３：回復・復旧　　11:30 ～ 12:00（30分）

昼食（60分）

フェーズ４：事後対応　　13:00 ～ 14:00（60分）

休憩（15分）

フェーズ（２）

フェーズ１：検知（通知・確認）　【作業1】情報セキュリティ事故発生報告書

・説明　⇒　作業　⇒　CISO報告（確認）　⇒　解答例　（以下、各フェーズ同）

フェーズ２：調査および対応　【作業2】情報セキュリティ事故経緯報告書

【作業3】稟議書

フェーズ３：回復・復旧　【作業4】情報セキュリティ事故経緯報告書

フェーズ４：事後対応　【作業5】情報セキュリティ事故最終報告書

登場人物･役割分担

（Ａ）情報部門担当者（インシデント分析コース受講者）

（Ｂ）情報部門管理者（セキュリティ施策・運営コース受講者）

（Ｃ）CISO（講習会運営委員）

利用者、実務担当者および外部組織は除く。この演習では、（Ａ）、（Ｂ）の役割を中心にインシデント対応を行います。また、各フェーズで行った調査および結果については、日時と供に記録すること。

フェーズ１：検知（通知・確認）

インシデントは、自組織の監視での検知が望ましいが、多くは外部からの通知が多い。本例でもメールでの通知として対応します。ただし、そのメール信憑性の確認は必要です。

【参照2】通知メールを参照して下さい。

不正通信の通知メールへの対応1

① 通知内容は、情報部門（センター）で調査すべきか？ （大カッコ内に記述）

(A)と(B)で協議 （インシデント対応基準に沿い、情報部門が調査を行う。）

【参照1】インシデント対応基準を参照して下さい。

② メール・通知内容の真偽判断の方法を列挙しなさい。

(A) （インシデント分析コースでの実習
JPCERT/CCの場合、PGP証明書付メールである。
10.10.19.123 へアクセス内容確認した。）

※ 本演習では情報部門が調査をし、メールの内容が真であることで演習を進めます。

不正通信の通知メールへの対応2

③ 協力を要請するべき部署を検討しなさい。

(A)と(B)で協議

教員・研究員が通信元の場合：

学部・研究組織等の長、支援事務部門

事務系職員が通信元の場合：

非公開情報の主管部署長、事務部門統括者

学生が通信元の場合：

学生支援部

不正通信の通知メールへの対応3

④ CISO への報告内容を検討しなさい。

(B)→(c)

発生日時： 2016年8月22日

通知概要： 学生情報の流出の疑い

リスク： 非公開情報の可能性高くインシデント対応が必要

対応計画： 詳細調査（端末特定、情報確認）、フォレンジック調査可否

事後対応

次回報告予定： 一次報告（詳細調査：早期）、二次報告（フォレンジック調査報告：１週間）

【作業1】事故発生報告書を記載し、CISOに提出してください。

フェーズ1の問題・検討事項

(A)と(B)で協議

◆大学は、縦割り体制でインシデント情報の集約（遅れ）

↓

◆初期対応の遅れ

↓

◆対外（被害者）対応に禍根

◆被害者　⇒　加害者（意識の希薄、好ましくない：隠す）

◆被害者の段階での相談窓口（早期の情報収集）

フェーズ２：　調査および対応

大学情報部門が中心となるSOC注）では、どの程度調査を行い、また専門家によるフォレンジック調査を依頼するかの判断が求められる。なお、対応はできるだけ最悪を想定したものが望ましい。

注）
SOC:　Security Operation Center

端末(利用者)特定と情報収集1

① 調査対象となる端末の通信状況を調査しなさい（カッコ内に記述）。

(A)

通知のあったC&CサーバのIPアドレス（ 10.10.10.2 ）について、F/Wログを参照したところ、学内のIPアドレス（ 192.168.1.? ）との通信が確認された。

IPアドレスから、そのサイトの物理的な場所が正確でないが探索できる。
またそのアドレスが、Blacklist 登録のチェックも有用である。
http://whatismyipaddress.com/blacklist-check

端末（利用者）特定と情報収集２

② 調査対象となる端末を特定しなさい（カッコ内に記述）。

(A)

学内のIPアドレス（192.168.1. ?）は、学内届出データを参照したところ、〇〇学部〇〇学科のD教授研究室が発信元と推測される。管理台帳によると、D教授研究室には、

a. 端末３台
b. サーバ１台
c. プリンタ１台

が設置されていることが判明した。

・IPアドレスの分散管理
・ローカルIPアドレスは、NAT変換ログ、研究室内ルータ管理
・BYOD、共通端末は、認証データ（日時と時間）

【緊急対応】

③ 調査対象の端末へ行う緊急対応とその根拠を記しなさい。

(A)

緊急対応：　ネットワークからの遮断
　LANから切り離す以前の行うべきこと端末調査（原因究明）のためにネットワーク接続が必要な場合がある？

根拠：（インシデント対応基準P-3, (2) 被害拡大防止の応急措置の実施(ア)

ネットワーク遮断のレベル
・学外アクセスの全面的抑止
・学外アクセスの指定サイト（C&Cサー　バ）との抑止
・学内ネットワークとの特定端末のみの抑止
・学内ネットワークとの全研究室端末の抑止
・ネットワーク管理者側での制御
・研究室内の教員による制御（？）

端末（利用者）特定と情報収集3

④ 調査対象端末の感染・操作痕跡の調査方法を挙げなさい。

※ 教員端末を情報部門スタッフが調査することに対する問題点はあるが、
ここでは了承のもと調査を行う。

(A)

イベントログ、監査ログの調査など

端末（利用者）特定と情報収集4

⑤ 調査対象の端末の利用者に聴取すべき内容をまとめなさい。

(A)と(B)で協議

対象利用者は、情報流出（漏えい）に対する管理責任はあるが、犯人ではない。
拡散防止、迅速対応、事後対策を含め、正確な情報（聞き取り）は重要な情報となる。

- **非公開情報の保存の有無、有の場合、その内容（項目）と量**
- 不審なメールの添付ファイルの開封（内容と時期）
- 不審なメールのURLアクセス（内容と時期）
- Web閲覧時の意図しないサイトの表示、その他気づき
- よく閲覧するWebのドメイン、国
- ウイルス対策シフトの管理
- Windows Update、その他ソフトウェアのセキュリティ管理状況
- 端末パスワード管理
- 外部からのアクセス、外部共有利用
- 専用利用／共有利用

端末(利用者)特定と情報収集5

⑥ CISOへの報告内容をまとめなさい（カッコ内に記述）。

(A)と(B)で協議

D教授研究室の教員機のIPアドレス（192.168.1.? ）であると推測される。
緊急対応として、8/24(水)（　）時（　）分に、
（緊急対応：　ネットワークからの遮断（抜線対応））を措置した。
また、教員機の痕跡調査を行ったところ、ファイルサーバ（192.168.1.20?）へのアクセス試行が判明した。
教員機の利用者への聴取の結果、重要情報資産が保存されており、情報流出のリスクが高い。
セキュリティ業者に、（フォレンジック）調査を依頼したい。

【作業2】経過報告書を記載し、CISOに提出してください。

一次報告を受けたCISOが行うべき事項

① フォレンジック調査の指示：　情報流出ありきの対応

② 学内対応関係者（部署）の召集

③ 被害者への一次報告（連絡）

④ 関係外部組織への相談・報告

⑤ その他（上記以外で必要と思われるものを記述する（以下同様）。）

フォレンジック調査依頼

⑦ フォレンジック調査を外注する場合の留意点を記しなさい。

(B)

ベンダー：　　Ｓセキュリティ調査会社

経費／台：　　150万円／台

調査日数：　　早期で２日、長期で一週間以内

秘密保持契約：　発注時に合わせて行う。

【参照3】予算表を参照して下さい。

【作業3】稟議書を作成し、CISOに提出して下さい。

フォレンジック結果

調査対象端末	IPアドレス	マルウェア感染	通信記録（不正通信の疑い）	漏洩の疑いのあるファイル
教員用端末	192.168.1.1	有	10.10.10.2（C&Cサーバ） 192.168.1.200（ファイルサーバ） **10.10.19.123に対するHTTPS通信（分割）**	① 2013～2015年研究室在籍学生個人情報（学籍番号・氏名・住所） ② 2016年担当クラス学生個人情報（学籍番号・氏名・住所）
共用端末１	192.168.1.2	無	無し	
共用端末２	192.168.1.3	無	無し	
ファイルサーバ	192.168.1.200	無	192.168.1.1（教員用端末）	

【参照4】フォレンジック調査結果レポートを参照して下さい。

謝罪（一次報告）

謝罪文（手紙）に掲載する項目を記しなさい。

(B)

- 差出名： 学長
- 標題の明確化
- 現時点判明している事実のみを記載
- 流出した情報の内容（項目）と数（量）
  - 数値は正確にあるいは最大値（可能性）
- 相談（対応）窓口の明記
- 経緯
- 現状での再発防止方針

【参照5】お詫び文（郵送版）を参照して下さい。

(学外)報告

この時点での、インシデントの学外報告先と内容を記しなさい。

(B)

◆監督官庁: 文部科学省私学部私学行政課(付属病院に係わる場合は、医学教育課にも)
同報:情報システム企画課 seijho@mext.go.jp
Web,マスコミ報道の前に報告
◆警察: 都道府県警察本部サイバー犯罪相談窓口:**被害届**
JPCERT/CC(通報者)
インシデント報告: https://www.jpcert.or.jp/form/
03-3518-4600, info@jpcert.or.jp
◆学外情報公開: Web、マスコミ等
◆独立行政法人情報処理推進機構(IPA)

謝罪（二次対応）

謝罪文（Web）に掲載する項目を記しなさい。

(B)

◆謝罪（一次対応）以後、調査状況
◆事後対応での具体的な再発防止
　◆システム系
　◆管理・体制系
◆その他：　更新履歴を明記すること

【参照6】お詫び文（Web版）を参照して下さい。

フェーズ2の問題・検討事項

(A)と(B)で協議

「大学(教員)の特殊性」について

- IPアドレスの分散管理(研究室含む)
- 対象教員への連絡遅延、学部等長への報告
- 教員端末の調査は教員、あるいは情報部門:技術と時間
- ネットワークからの遮断(抜線対応)の徹底
- ウイルス対策ソフトウェアの非集中管理体制、資産管理有無

フェーズ3： 回復･復旧

問題となった端末あるいはシステムをどのような条件で、これまでの状態に回復・復旧されるかを事前に定めていることが望ましい。

回復・復旧1

① 感染端末（教員用）を復旧（調査時も同じ）する場合に必要な作業等を記しなさい。

(A)

調査時
① 抜線のうえ、シャットダウン、再起動せずにしておく。
② セカンドオピニオンとして通常仕様のウイルス対策ソフト以外の対策ソフトで確認
ウイルス確認ができた場合、そのウイルスが原因であるかどうかの判断が難しい。
ウイルス確認ができない場合、外部との不正通信が確認されている事実を
説明するためにフォレンジックが必要になる。
復旧
① 教員にマルウェア感染後の情報漏洩リスクについてレクチャー
② 職員が再インストールのうえ、利用可とする。
ただし、作業は教員が実施する場合は、その確認が必要となる。また、(A)は
F /W等で外部ネットワークと通信をしばらく監視することが必要。

回復・復旧2

② Ｄ教授研究室の措置（抜線対応の場合）の解除判断は？

(B)→(A)　規程でクリーンインストールを明記、クリーンインストールの確認で解除する。

③ ウイルス対策ソフトでマルウェアが検知・駆除されたとしても、しばらく(A)が行うことが必要事項は？

(A)　不正通信が検知されたウイルスに起因するものと判断することは難しい。
　また、Webからマルウェア感染している場合もあるので、検知・駆除後も仕事の都合上、Webサイトの閲覧で再感染する可能性が高い。

【作業4】経過報告書を記載し、CISOに提出してください。

フェーズ3の問題・検討事項

(A)と(B)で協議

大学の場合、大学管理の教員端末は物理的（通常ソフトウェアも含む）には大学資産であるが、保存されている情報については曖昧な部分がある。
企業ではクリーンインストールでの回復・復旧が規程されるが、大学ではこれが適用できるか？　また、その徹底が図られるのか？

フェーズ4： 事後対応

事後対応は、今後同様な事案の再現の防止策、また再現した場合でも迅速に対応するための重要なフェーズであり、これをもって対応の終了となる。

事後対応1： 技術的な改善

例１． F/W,IPSの設定見直し

(A)

その他の改善・問題点あるいは例題の改善点の詳細等を検討する。

◆ネットワーク運用（内部拡散防止）の見直し

◆ウイルス管理ソフトの集中管理

◆ICT資産管理

◆ログ取集設定の確認とログ管理システム (SIEM: Security Information and Event Management)の検討

事後対応2： 管理的な改善

例１． 対応手順の見直し

その他の改善・問題点あるいは例題の改善点の詳細等を検討する。

(B)

◆インシデント対応訓練

◆就業規則とは別にネットワーク利用等に関するペナルティの必要性も議論

ただし、ペナルティはインシデント発生の素早い報告を妨げる風潮を醸成しかねないので、実際に発生したインシデントの事例共有化などが望ましい。

事後対応3： CISOへ提言する事項

例１．インシデント対応組織の整備

その他の提言・問題点あるいは例題の提言の詳細を検討する。

(A)と(B)で協議

◆規程の見直し

◆セキュリティシステムおよび運用経費の確保

「現在導入しているセキュリティ製品が、現在の攻撃に対しどの程度有効製品であるのか？その機能を発揮するような運用となっているのか？」といった事を検討する場合の障壁が経費である。

総括

① 最終報告書の作成

【作業5】 最終報告書を記載し、CISOに提出してください。

② SOCとCSIRT注）の役割等の確認

③ 勤務校におけるインシデント対応体制

注）
SOC:　Security Operation Center
CSIRT: Computer Security Incident Response Team

まとめ（１）

- 訓練として対応（１回／年は）
- 現状の入口・出口対策の見直（現システム・サポート）
  - ポリシーの確認と徹底
  - IPアドレス集中管理、ウイルス対策ソフ集中管理、ICT資産管理
- 個人情報・営業秘密情報の把握、情報レベルの分類（具体的に）
- 規程の見直（学生、教員・研究員、事務職員別）
- インシデント体制（SOC、CSIRT)の必要性
  - 自衛消防団的組織・体制
  - 相談・情報収集窓口と発生時対応

まとめ（2）

- SOC（情報部門）：　複数人対応、機器・ツールの準備
- 誰が、何処まで調査するのか？
- 回復・復帰・事後対応
  - 端末・システムのネットワーク再接続の判断基準と監視の継続
  - 被害者への謝罪・対応
  - 外部報告、外部公表（一次、二次）
  - 学内通知・周知
  - 事後対応のため予算の確保
  - ペナルティ？（職務規程処罰他）