総合演習－1
S-1. システム管理者とマネージメント部門協働によるインシデント対応演習

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

標的型サイバー攻撃に対し、その事実の確認および対応について、システム（技術）担当者とマネージメント（管理）担当者との協働作業によるインシデント対応実習を体験する

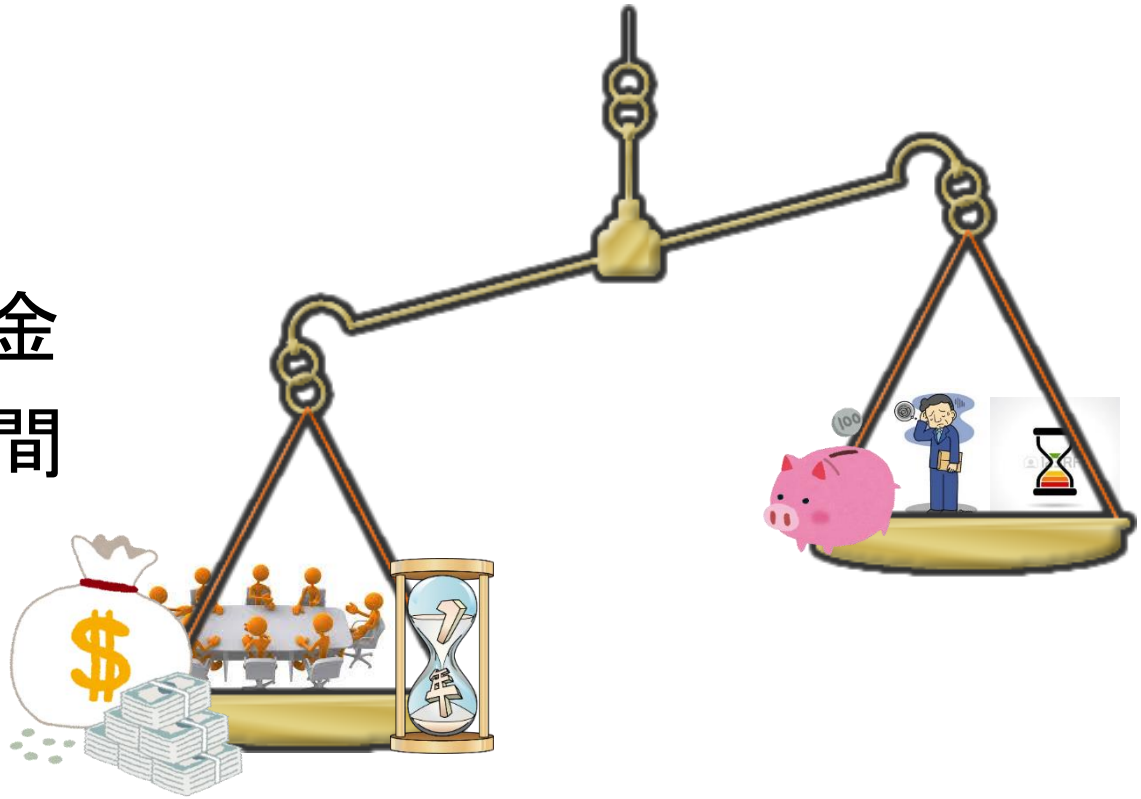
（1） 外部からの情報提供、指摘によるインシデント対応
（2） 内部からの情報提供等によるインシデント対応
（3） 不可抗力による意図しない情報流失対応（対応例）

＝

3種のインシデント対応を各担当者として体験し、自組織におけるインシデント対応および見直しの行動がとれる

標的型サイバー攻撃の攻撃側と防御側のバランス

- 人
- お金
- 時間

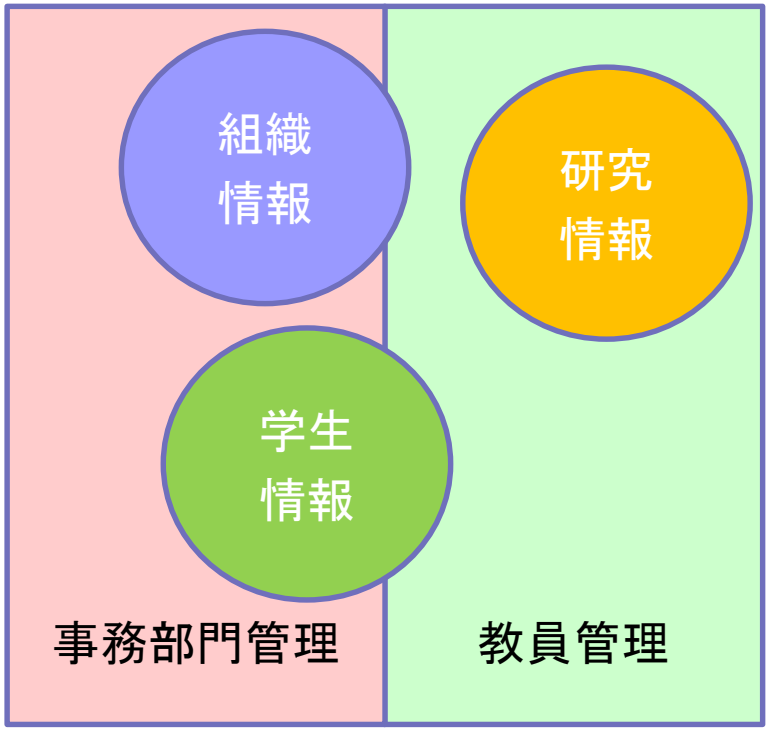


攻撃側

防御側

大学が標的型サイバー攻撃で狙われる情報

- 学生、職員の個人情報
  - 成績、健康診断情報等
  - 住所、家族、学歴情報等
- 研究情報
  - 先進的な研究情報
  - 企業との共同研究情報
  - 国、自治体等外部組織委員会情報
- 組織管理情報
  - 組織管理情報
  - 入試情報
  - 財務、経理情報（マイナンバー）



- 情報漏えい（≠情報流失）
- 不正利用（ホップポイント：踏み台サーバ）

情報提供内容等と対応(要求)の分類

- 外部機関等
  - 警察、裁判所
  - 公的機関、これに準ずる機関 (JPCERT, IPA等)
  - 報道機関(取材)
  - 企業、他大学
  - 個人
- 提供・指摘方法
  - 電話
  - 手紙、メール、Web投稿
  - 本人(対面)
- 依頼、要求内容
  - 捜査、指示
  - クレーム
  - 警告、注意勧告
  - 取材
- 応答の有無
  - 報告指示
  - 報告要請
  - 協力
  - 明記なし
- 報告、公示
  - 監督官庁等
  - 報道機関、ホームページ

インシデント対応時の注記

- 複数人（組織）で確認・対応すること。
- 実施事項、要点については、必ず日付・時間と共にメモあるいは記録すること。
- 数値はできるだけ正確な情報として記録すること。その担保データを保管すること。
- 報告者および指示者の氏名も合わせて記録すること。
- 教員所有の端末調査には、教員および上層部の協力も必要な場合あり

まとめ

- 組織内CSIRT

  情報インシデント対応は、これに対応する組織が必要とされる。これを専門に行う部門が理想的ではあるが、当面は**仮想組織の対応チーム**として組織内にCSIRTを構築し、**学内認知**が必要である。

- 相談窓口

  標的型サイバー攻撃は、その攻撃実態および情報流失の状況把握が難しい。このため、学内構成員の意識付と些細な気づきが相談できる**窓口の公開・公示**が必要である。

- 活動(継続)予算の確保

  CSIRTの活動は継続的なものであり、情報セキュリティ対応に合わせた**運用経費**等の予算確保が重要である。

演習-1

外部からの情報提供、指摘による インシデント対応

- 想定：　研究データ流失の疑い

提供情報

- 提供元: JPCERT/CC（早期警戒グループ）
- 提供方法: 電子メール（添付ファイル無）
- 報告の有無: 協力要請
- 内容

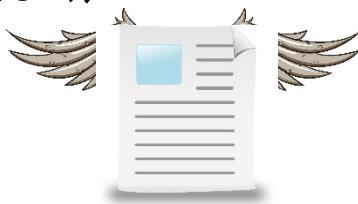
貴学のグローバルIPアドレス(1.2.4.5)を持つ端末と外部の複数のC&Cサーバとの通信が確認されました。第三者による遠隔操作により、外部ホストに対する悪意のある不正通信や複数のファイル（情報）の流失が疑われます。

不正通信先リスト

- 221.214.xx.26
- 220.181.xx.148
- 219.148.xx.3

インシデント対応手順（概要）

1. メールの信憑性の確認
2. 状況の把握：（調査権限を規程に明記しておく）
   - 対象端末の特定と調査：　調査範囲と権限
   - 各種ログの調査
3. 緊急一次対応（手順書に発動の基準を明記しておく）
   - 端末に対する対応
   - ネットワーク接続に関する処置
4. 調査継続による詳細情報等による二次対応の検討
   - 内部侵入の調査
   - 端末の詳細情報（デジタル・フォレンジング）
5. 復旧、事後対応計画の策定と実施
6. 報告、公示（掲示）、学内広報



実習-1 メール(内容)の信憑性の確認

- メールの送信元(経路)、場所(時間)の確認
- 迷惑メール判定(レベル)
- 日本語文章の表現
- 添付ファイルの有無
- その他

- その他の回答例(隠し)
  - 送信先の情報(Who is確認)、postmaster, abuseでない、複数
  - JPCERT PGP確認
  - 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。

実習-2　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(テ：テクニカルコース）⇔（マ：マネージメントコース）
  - 対象端末の特定（調査）
  - 対象端末の状況確認（依頼）
  - 通信記録の確認（FW, IPS/IDS, Proxy等）と保管
  - 管理者として判断に必要な情報の不足？

- 管理者のインシデントレベル判断例（マ）
  - レベル3:　情報漏えい有、またはその可能性大
  - レベル2:　情報の流失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

実習-2　インシデントレベル判断と一次対応（2）

- インシデントレベルと一次対応(マ）　⇔　（テ）
  - レベル3, 2
    - ネットワーク接続の断、端末の電源をOFFしない
    - 端末の状態保持:　可能であればメモリダンプ取得
    - 重要データのバックアップ（端末管理者）:　専用デバイスに
  - レベル2
    - 注意観測
- 管理者（マ）　→　CIO等上層部への報告
  - 情報提供・指摘時に一報報告も良
  - 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。

実習-3 二次対応、復旧・事後対応計画と報告・公示等(1)

- 調査継続による詳細情報と二次対応の検討(テ)、(マ)
  - 内部侵入:　影響範囲(テ)
  - 端末のデジタル・フォレンジング調査依頼(可否と範囲)(マ)
  - 複合機、プリンタ等その他機器の外部通信の確認(テ)
  - その他
- デジタル・フォレンジングの結果(一週間程度)
  - 調査結果に基づき、情報漏えい(流失)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)
- 復旧対応
  - 対象端末の復旧:　クリーンインストール、端末管理の見直
  - ネットワーク構成・ポリシーの見直
  - 保存データ:　　暗号化対策等
  - その他

実習-3 二次対応、復旧・事後対応計画と報告・公示等(2)

- 再発防止対応
  - 全学的な適用に向けた検討および対応
    - 各種規程やセキュリティポリシーの見直し
  - 調査・対応体制（組織、チーム）の見直し
  - 監視の強化（継続注意、監視の外部委託、ハニーポット等）
  - その他

- 報告・公示等
  - 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・公示（掲示）を再発防止対応（計画）を含めて行う（CIO） → 広報部署

演習－２

内部からの情報提供によるインシデント対応

- 想定

　総務部のAさんに「医療費請求メール（添付ファイル）」が届き、添付ファイルを開けてしまった。

　情報センターに連絡があり、調査し、内容に応じインシデント対応を行う。

インシデント対応手順（概要）－１

1. テクニカルコース：　VirtualBoxを用いたマルウェア挙動調査
   - レジストリの変更実行を確認
   - ウイルス対策ソフトでの異常検出無　→　標的型インシデントと判断（テ）　→　（マ）　→　CIO

2. 緊急一次対応
   - 端末の現状保持（メモリダンプ取得）（テ）
   - データのバックアップ（別専用メディアに）（テ）
   - 同等メールの受信および開封の確認調査（テ）

3. テクニカルコース：　内部侵入・調査（テ）
   - 総務課のPC、ネットワークを中心として調査
     - ADサーバ等への侵入の確認

インシデント対応手順（概要）－２

4. 一次対応：「被害範囲予想報告書」より
   - インシデントレベル（高、中、低）を報告（テ） ⇔ 判断（マ）
   - 対応指示（マ） → （テ）
     - ADサーバ等への対応：（管理者）パスワード管理
     - 内部ネットワーク構成、制御の見直し
5. 二次対応
   - 端末の詳細情報（デジタル・フォレンジング）の範囲と可否（マ）
   - 内部侵入の対応（テ） → （マ） → 委員会等
     - ネットワーク、端末、ドメインレベルの監視の強化（テ）
   - その他対応と設定等に関する通知と確認（テ）、（マ）
6. 復旧対応と再発防止計画（教育）
     - 運用規程、内部統制への適用、利用者啓蒙と教育
7. インシデント報告書の作成、提示（テ、マ）と承認（CIO)
8. 報告、掲示等

対応例

不可抗力による意図しない情報流失対応

- 概要： 複合機、プリンタ等（今後のIoE, IoT)の管理

提供情報

- 提供元:　　報道機関（A新聞 特別報道部）
  （後日JPCERT/CC制御システムセキュリティ対策グループ系より）
- 提供方法:　　電子メール（添付ファイル有）
- 協力（取材）要請　一次窓口広報部担当者
- 内容要約(電話とメール）

　貴学の複合機／プリンタ（複数）が外部からWeb閲覧ができる状態にある（添付ファイル）。端末の適切な管理がなされていない状態（工場出荷設定）であり、第三者による設定変更あるいは情報表示が可能である。

　今後IoE、IoTの時代に向け多くの機器がネットワークに接続される。このような状況下において、その代表的な機器（複合機／プリンタ）の管理に対する貴学の対応等について取材をお願いしたい。

インシデント対応手順（概要）－１

1. メールの信憑性の確認（電話連絡もありここでは省略）
   - 状況の報告（CIO等）と取材対応の可否　→　対応
2. 状況の把握（全学的な調査権限を規程に明記しておく）
   - 対象端末の状況調査依頼（数個）
   - その他端末の注意勧告と調査要請（全学的）：対象多
3. 緊急一次対応
   - 対象端末のインターネット接続制限
   - 対象端末の管理（パスワード）設定の確認（個別））
   - 対応端末（複合機）での保存データの内容とその管理調査
4. 調査継続による詳細情報等による二次対応の検討

インシデント対応手順（概要）－２

4. 二次対応
   - ジョブ履歴表示対応（実習、自習環境） → メーカ確認
   - プリンタ管理に関するマニュアルの作成
     - 不要なサービス（Web, telnet/ssh, ftp, SMB等）の停止
     - アクセスコントロール設定
   - 複合機（閉域）ネットワークへの切替
   - 個別複合機導入時の注記（導入業者、学内担当部署）
     - 導入に関するセキュリティチェック（シート）の活用
5. 事後対応計画の策定と実施
   - インターネット接続（HTTP通信）ポリシーの基本閉鎖型への完全実施
6. 取材対応： CIO、事務局管理者、広報部、技術担当者
   - 報道機関の目的の確認
   - 複合機、プリンタメーカーの出荷時セキュリティ対応

まとめ

- 組織内CSIRT

  情報インシデント対応は、これに対応する組織が必要とされる。これを専門に行う部門が理想的ではあるが、当面は仮想組織の対応チームとして組織内にCSIRTを構築し、学内認知が必要である。

- 相談窓口

  標的型サイバー攻撃は、その攻撃実態および情報流失の状況把握が難しい。このため、学内構成員の意識付と些細な気づきが相談できる窓口の公開・公示が必要である。

- 活動(継続)予算の確保

  CSIRTの活動は継続的なものであり、情報セキュリティ対応に合わせた運用経費等の予算確保が重要である。