イントロダクション

私立大学情報教育協会
大学セキュリティ研究講習会運営委員会

目次

1. 2つのインシデント事例から
2. 今回の講習で扱うインシデントモデル
3. 標的型サイバー攻撃の被害調査は大変！
4. 今回の講習における標的型サイバー攻撃への対応フロー
5. 講習の流れ

1. 2つのインシデント事例から

日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告について」

http://www.nenkin.go.jp/n/data/service/press0820.pdf

○○○○大学のパソコンがマルウェアに感染し、
個人情報が流出したことが判明しました。

標的型サイバー攻撃の被害特徴

① マルウェア感染の手法は様々（メール添付ファイル、配布DVD、USBメモリ）

② 攻撃者からマルウェアへの操作命令がなされる

③ 攻撃者はマルウェアを拡散させる

④ 被害は外部通知で発覚することも多い

2. 本講習で扱うインシデントモデル

SJK 大学で起きたインシデント

① ある日、JPCERT/CCより、「SJK大学からの情報流出が疑われる」、との連絡メールが届いた。

② 学内で「一昨日、不審なメールの添付ファイルを開いてしまい、マルウェアに感染した疑いがある」との報告があった。

③ 更に、マスコミよりSJK大学内のプリンタの管理画面がインターネットより閲覧できる状況にあるとの注意を受けた。

講習会で扱うインシデントモデル

	漏洩状況	漏洩源	発覚
①	研究データ	教員所有PC	外部通知
②	ー	事務局所有PC	内部通知
③	印刷ログ	複合機（プリンタ）	マスコミ

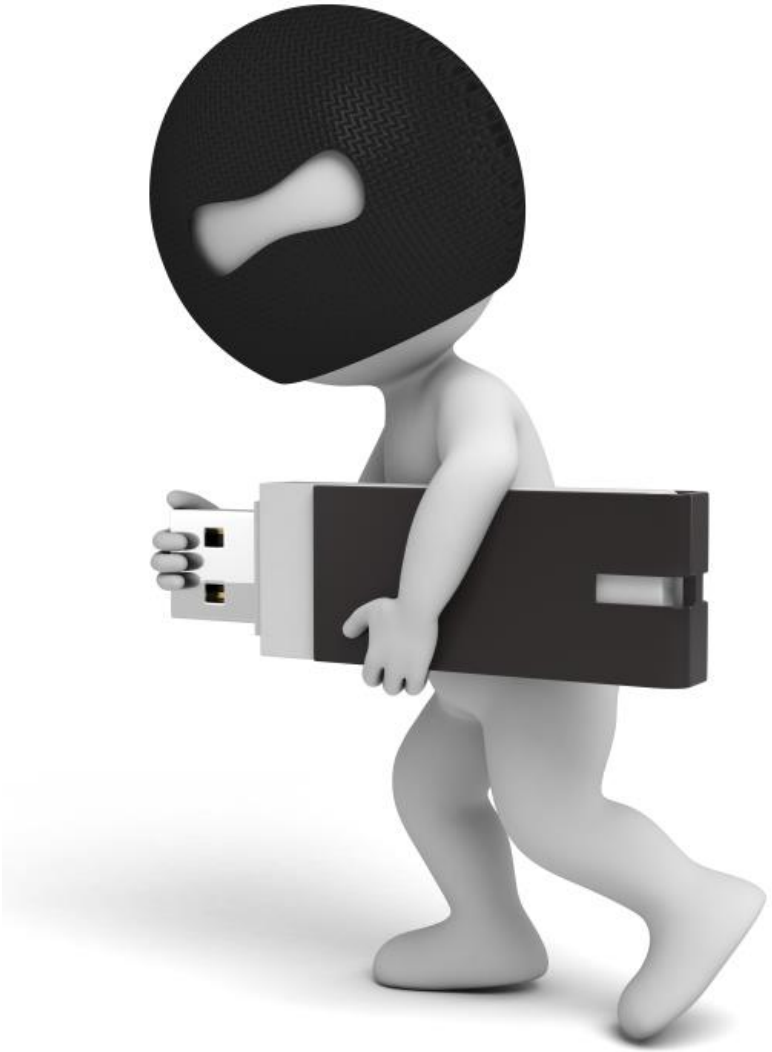
3. 標的型サイバー攻撃の
被害調査は大変！

被害調査のゴール

① 被害範囲の特定

② 侵入経路の特定

③ 窃取データの特定



不審なプロセス・アカウントの調査

不審プロセスの洗い出し

不審なプロセス・アカウントの調査

不審アカウントの操作調査

メモリ上の記録が重要！

感染PCの電源を落とさないこと！

そうは言っても…

【参考】セキュリティ対策製品の価格

	製品名	ハードウェア	保守・ライセンス
①	FireEye(Web)	670万円	130万円
②	FireEye(mail)	（クラウド）	680万円
③	NGFW（10G回線）	120万円	80万円
④	SIEM	2000万円	400万円
⑤	HDD暗号化ソフト		550万円（300名）

マクニカネットワークス調べ

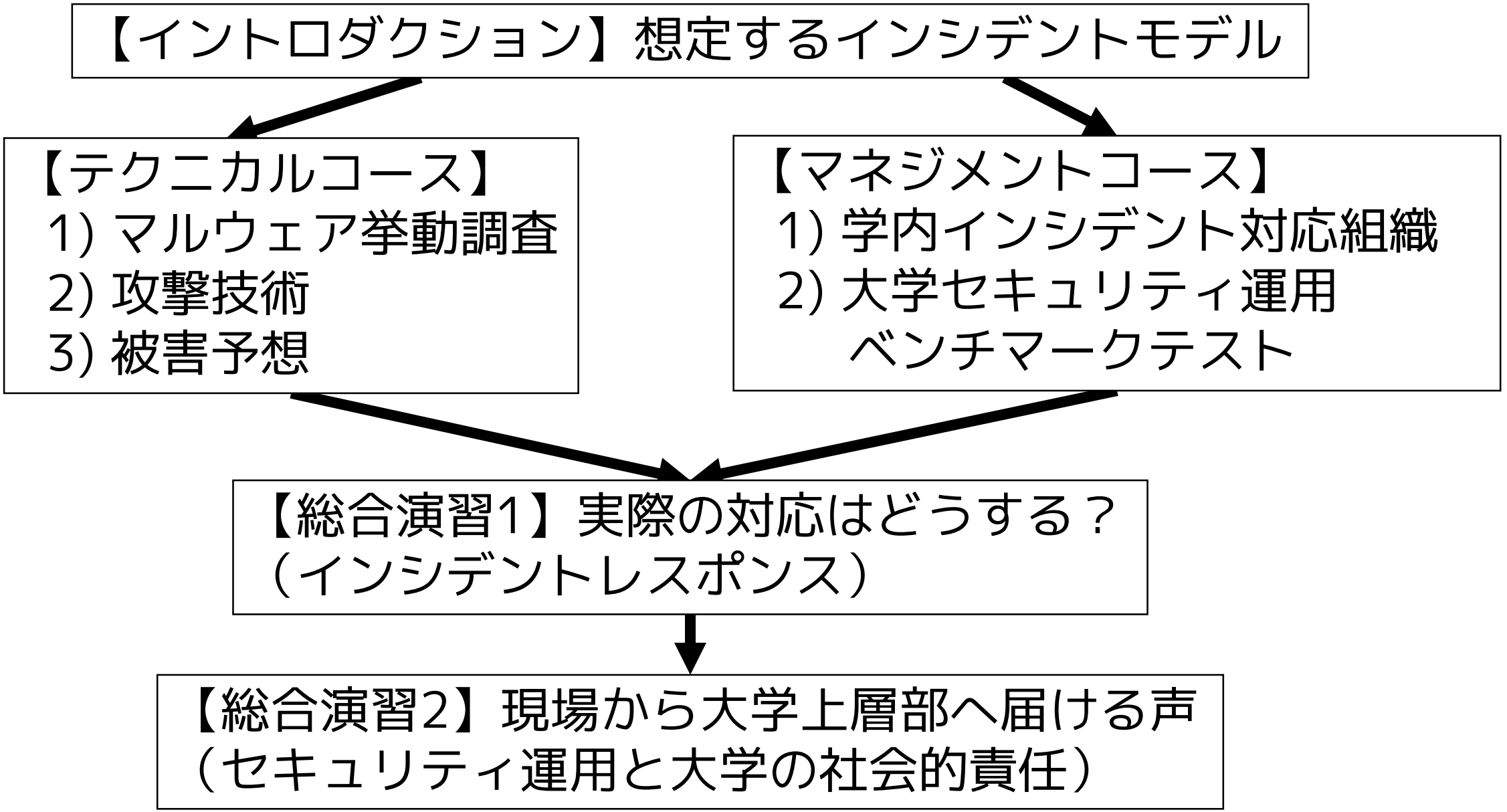
4. 本講習で扱う
標的型サイバー攻撃対応フロー

標的型サイバー攻撃への対応フロー

① ネットワーク・システムの把握
② 被害範囲の予想
③ 報告・連絡・協議
④ 感染拡大防止・緊急対応
⑤ 警察への連絡・セキュリティベンダーへの依頼
⑥ 大学執行部への提言

5. 講習の流れ

午後からの講習会全体の流れ



午後からの講習会の資料と成果物