第1日目

情報セキュリティ担当者のためのインシデント対応入門

マルウェア感染対応オリエンテーション

2014年12月

セクタンラボ勉強会

はじめに

- この講座では，組織内パソコン（PC）が，マルウェアに感染した場合の対応方法について学習します。

- オリエンテーションでは，学習に先立ち，講座の全体構成や，インシデント対応の基本的な考え方を確認します。

本日の次第

第1章 講座の概要

– 講座の全体構成，学習目標などを確認します。

第2章 インシデント対応のイメージ

– インシデント対応時における基本的な考え方を確認します。

第1章 講座の概要

講座の全体構成

- **各講座の所要時間は，3～4時間（休憩時間含む）で，実機を使った実習も行います。**

講座名称	主な学習内容
フォレンジック基礎編	・感染PCの調査に用いる基本ツールの操作方法
WEB型マルウェア編	・感染源WEBサイトの特定・遮断方法 ・感染PCに潜伏しているマルウェア検体の取得方法
メール型マルウェア編	・特定の不審メールの遮断方法 ・特定の不審メール受信者の把握方法 ・感染PCに潜伏しているマルウェア検体の取得方法
模擬訓練	・机上での模擬訓練により，マルウェア感染状況の把握，ならびに被害拡大防止対応の判断と指示を体験

想定受講者と学習目標

想定受講者

- 組織の情報セキュリティ担当者（インシデント対応未経験者）
- WindowsおよびMicrosoft Officeの基本的な操作ができる

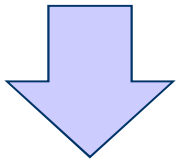
学習目標

- 組織内PCのマルウェア感染時の調査・対応方法を「なんとなく理解したつもり」になる。

「なんとなく理解したつもり」とは？？？

- インシデント対応には，幅広い知識が必要となるため，いきなり机上で教科書を見ながら暗記する勉強法では，（個人的には）とても眠くなってしまいます。

- 本講座では，「まずはやってみよう」を合言葉に，とにかく実習で手を動かしてみます。
- 動作原理を深く理解できていないものの，とりあえずツールを使って調査したり，サーバやネットワーク機器を運用している業者にログ取得や設定変更を依頼できるようになることを，目標としています。



「なんとなく理解したつもり」になることで，
分からないことを自分で調べて学習するキッカケとなることを期待

（参考）インシデント対応とは

- 情報セキュリティ分野における「インシデント」とは，不正アクセス，マルウェア感染，情報流出事故など，情報セキュリティを脅かす事象のことです。
- インシデン対応とは，インシデントが発生した際に，被害を最小限に抑止するための「事後対応」のことを指します。

- 現在の技術では，PCのマルウェア感染を完全に防止することは困難なため，防御策の実施に加えて，万が一インシデントが発生した場合に備え，迅速的確に対応できる体制を整備しておくことが必要です。

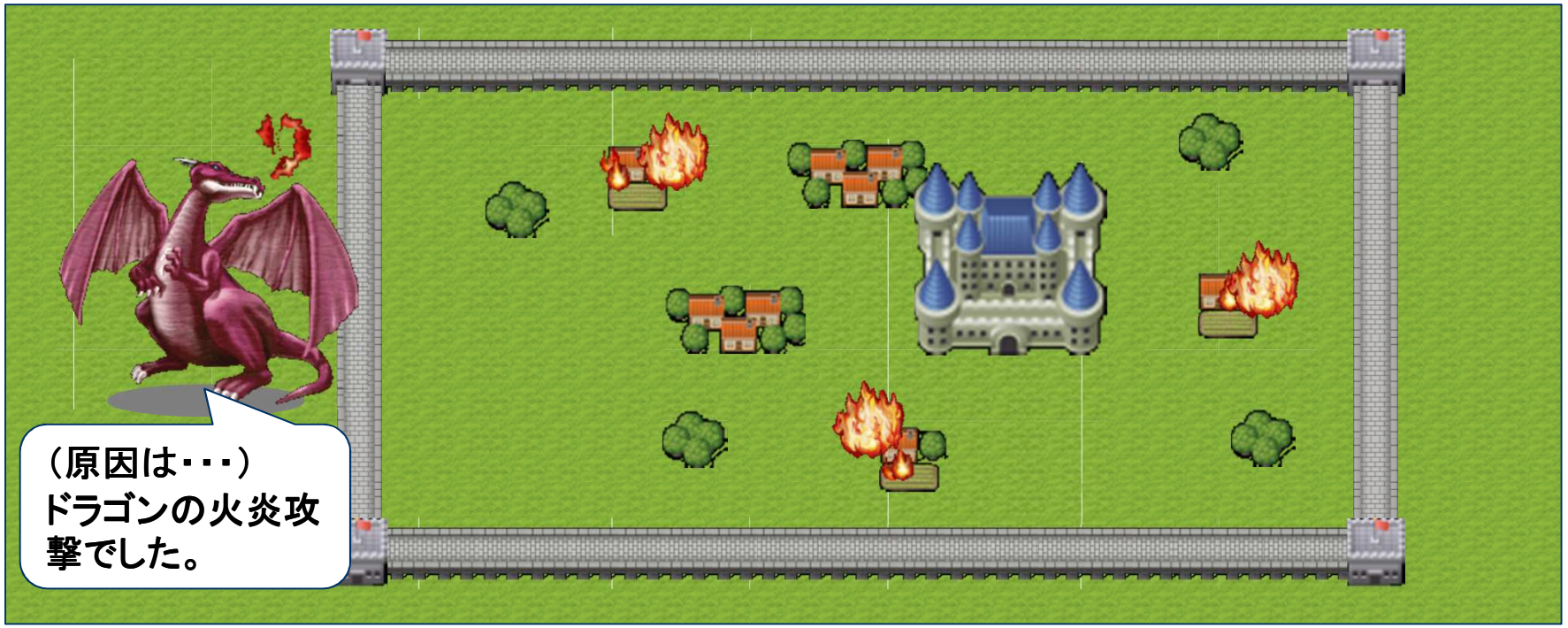
（補足）ISO/IEC 27001では，インシデントは，「望まない、又は予期しない一連の情報セキュリティ事象であって、事業運営や情報セキュリティを脅かす可能性が高いもの」と定義されている。

第2章 インシデント対応のイメージ

インシデント対応のイメージ（1）

- 城壁の中で爆発が発生しました。あなたは警備隊の隊長です。さて，どうしますか？

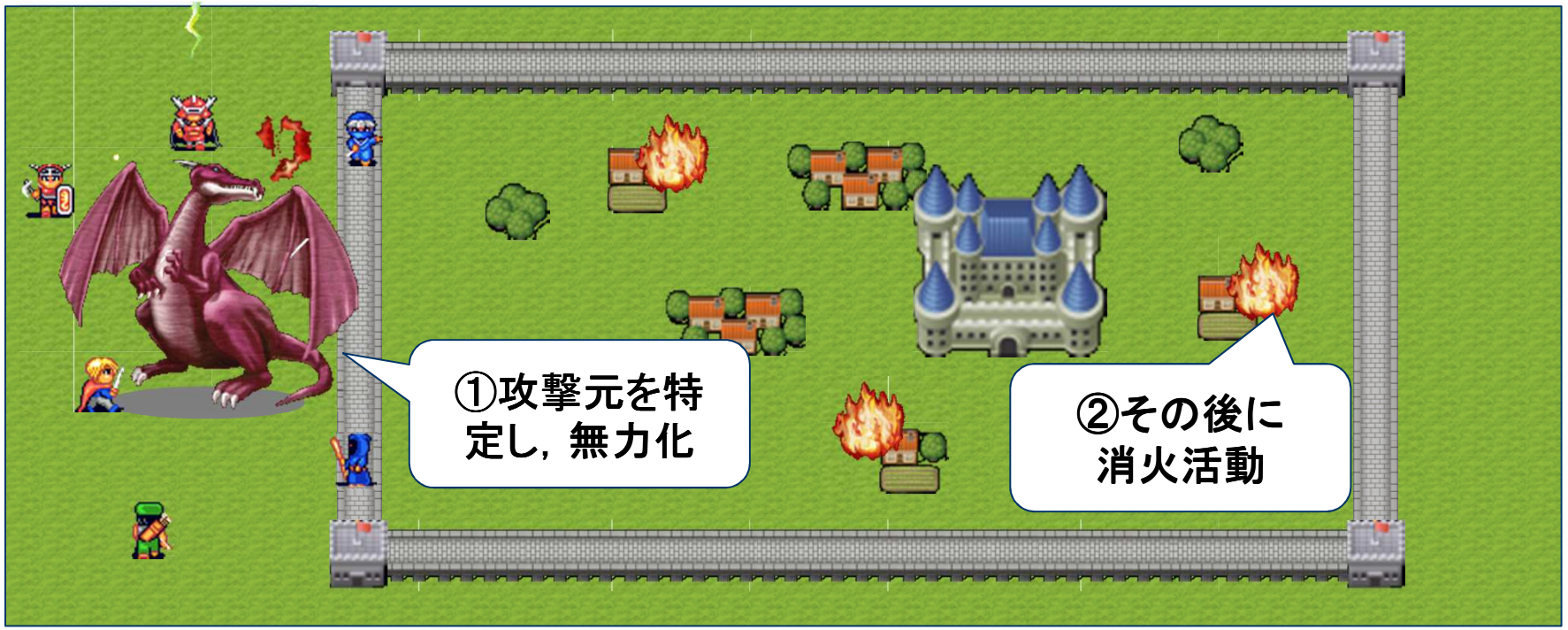
消火 ➡ 新たな爆発 ➡ 消火 ➡ 新たな爆発！
原因が不明なまま闇雲に対処しても，イタチゴッコになる可能性がある。



インシデント対応のイメージ（2）

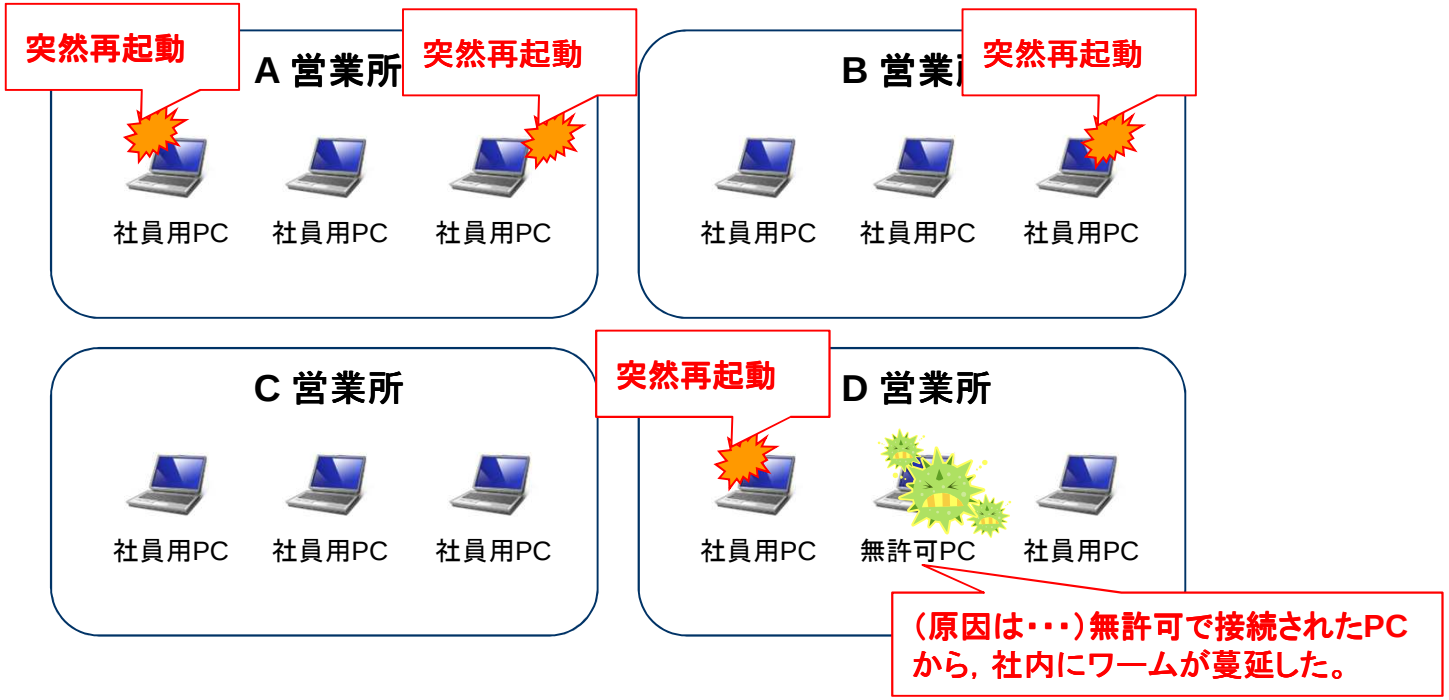
- 現在進行形で被害が拡大している場合は，最初に攻撃元を無力化する。それから復旧（消火）活動，および事後処理を行います。

状況を正しく把握できれば，対応は意外とシンプル
（状況を把握できないと，大きな混乱が生じる）



現実世界のインシデント対応

- 突然，各営業所のPCがブルースクリーンとなり，再起動する事象が発生しました。再起動したPCは，しばらくすると，また再起動してしまいます。
- 時間の経過とともに，被害が拡大しているようです。さて，どうしますか？

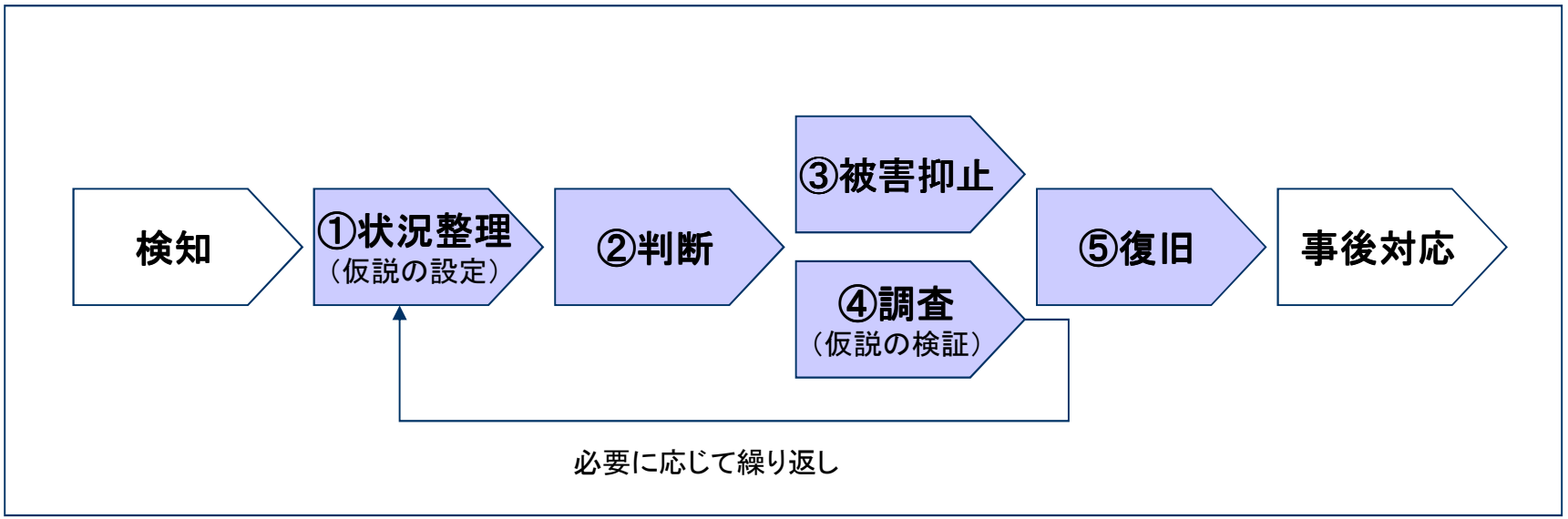


WEB閲覧による感染，メール添付ファイル閲覧による感染など，想定シナリオに応じて，対応手順も変わる

現実世界のインシデント対応の基本手順

- **インシデントが発生した際は，次の①～④の手順を繰り返し，⑤復旧を目指します。**
  - ① 事実と推測を整理し，発生している事象とリスクの「仮説」を設定する。
  - ② リスクの大きさと，対応にかかる労力などを考慮し，対応方針を判断する。
  - ③ 被害抑止のため，仮説で想定したリスクの対策を講じる。
  - ④ 判断に必要な情報が不足している場合は，調査を実施し，仮説の検証を行う。
  - ⑤ 同様の攻撃を受けないよう応急処置を施した上で，復旧作業を実施し，事態を収束させる。
    - ・仮説で想定した被害の抑止対策と，調査による仮説検証を平行実施することで，対応の迅速化を図る。
    - ・各手順の対応状況や対応結果は，関係者と情報共有すること。

◆ インシデント対応の基本手順



課題

- 目に見えないサイバー攻撃の状況を正しく把握することは，簡単ではありません。
（状況を正しく把握できれば，対応の半分以上は終わったようなもの）

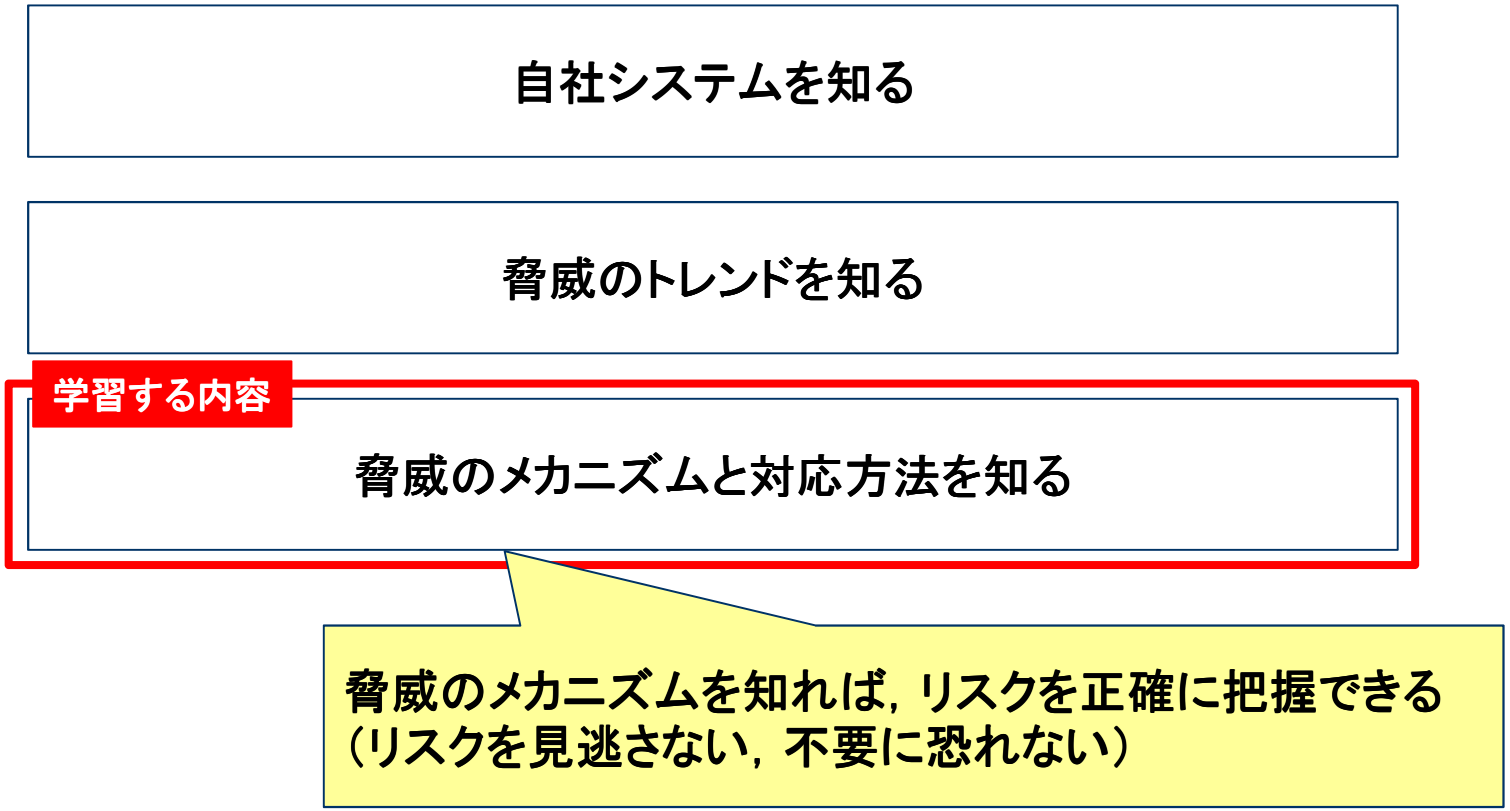
正しい状況把握のためには，事前の準備が必要

◆ 事前の準備

分類	対策の例
技術的対策	• PCのインターネット接続経路をProxy経由に限定する。 • ウィルス対策ソフトの検知アラートを監視する。 • 事後調査に役立つPC操作履歴記録ツールなどを導入する。
組織的対策	• 対応責任個所と権限を明確化する。 • 対応手順書，情報共有ルールを整備する。 • 利用者に，不審な事象に気が付いたらシステム管理者に通報するよう周知する。
人的対策	• システム管理者のスキルアップ

事前の準備 システム管理者のスキルアップ

- 既存の対策をすり抜けた結果としてインシデントが発生するため，「想定外」の出来事が起こり得えます。
- 最後に頼りになるのは，人の知恵。システム管理者のスキルアップを図ることが重要です。



学習のスタート！

分からないことがあっても，
まずは気にせずに，手を動かしてみましょう！