＜重要インフラにおけるヒューマンエラーと情報セキュリティ＞

電力分野におけるサイバーテロ演習

2009年2月20日

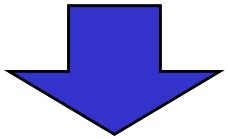
(財)電力中央研究所
システム技術研究所
松井　正一

「人間の特性8箇条」(高橋秀俊)

1. 人間は気まぐれである
2. 人間はなまけものである
3. 人間は不注意である
4. 人間は根気がない
5. 人間は単調を嫌う
6. 人間はのろまである
7. 人間は論理的思考力が弱い
8. 人間は何をするかわからない

背景・目的

- サイバー攻撃を速やかに検知し、事業への影響を最小限に留めるためにはインシデントレスポンスが重要
- 電力会社および関係会社からの演習参加者が、演習用モデルシステム上でサイバー攻撃を実際に体験
- 攻撃に対するインシデントレスポンスを実施



インシデントレスポンス体制や情報セキュリティ対策の検討材料となる知見を獲得

事前調査・検討（1）

- 様々なサイバー攻撃を経験するための攻撃のあり方について調査・検討した
  - 設定・メンテが正しく行なわれていると攻撃はなかなか成功しない
  - 攻撃を成功させるためには，用意周到な準備や実際の攻撃のためにかなりの時間がかかる

限られた時間・設備の中で，様々な攻撃を経験するため，ソーシャルエンジニアリングが成功したという前提条件による情報提示や，攻撃がはかばかしくない際の意図的設定ミス，脆弱性の埋め込み（促進ルール）を実施

事前調査・検討（2）

- 海外におけるサイバーテロ演習や情報セキュリティ対策について実態調査を実施
  - 米国等では机上演習が中心
  - 演習のシナリオ作成段階からの参加が重要
  - 参加者への結果のフィードバックが重要

    ➡ 演習実施の参考に

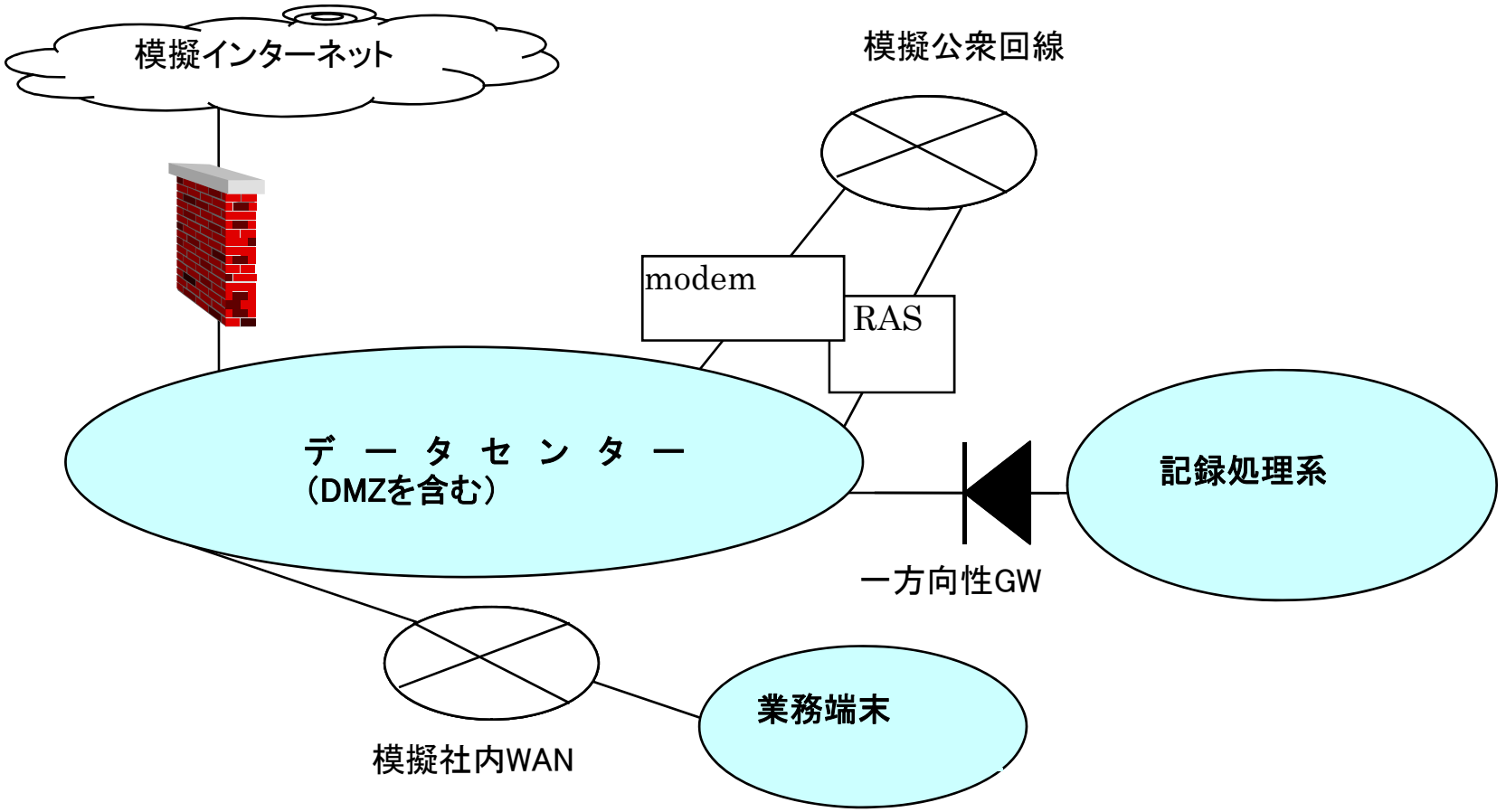
  - 欧米では，演習を実施しても，実施の有無を含め全く公開しないか，公開しても実施の事実程度

    ➡ 演習に係る情報は慎重に取扱うべき

モデルシステム（1）

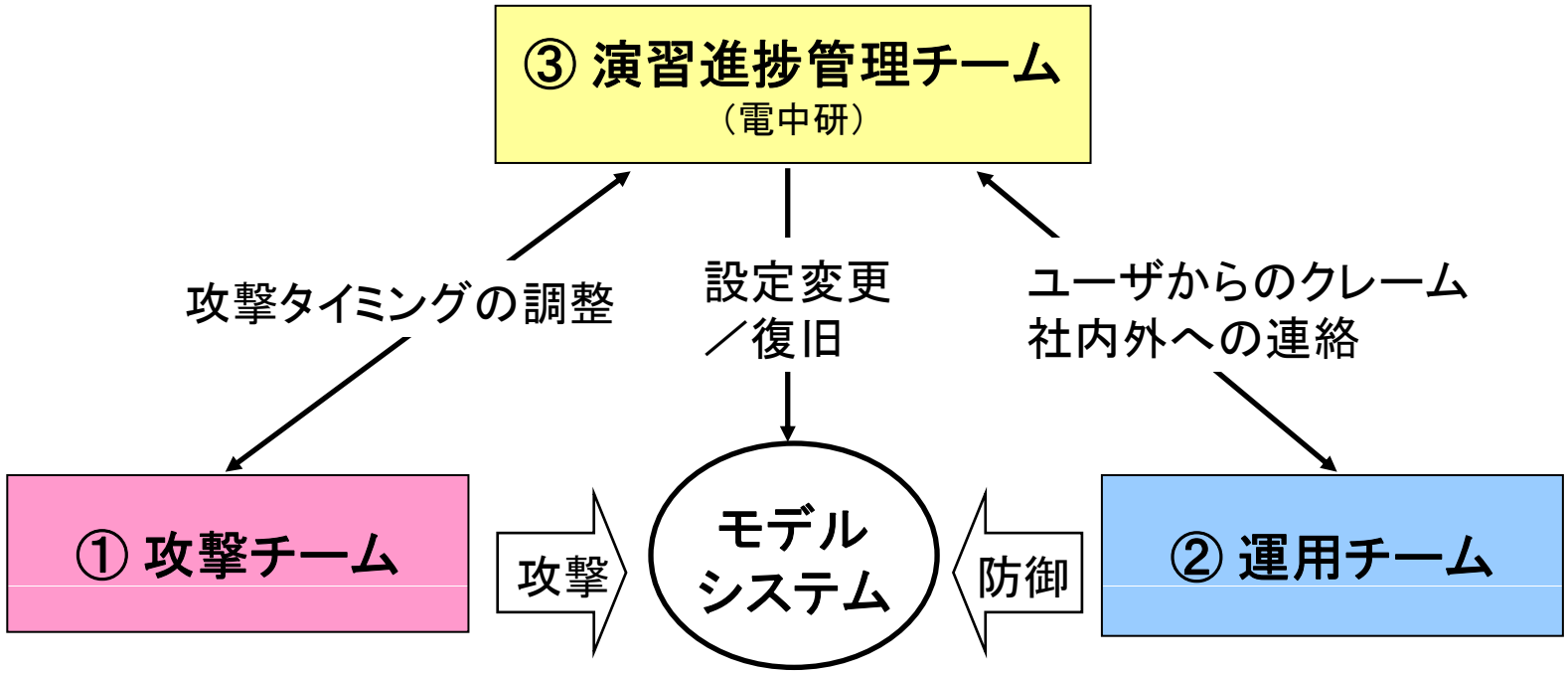
- 外部のネットワークと直接接続されている業務系，および業務系と一方向性のGWで接続されている記録処理系とのインターフェースまでを対象範囲
- 対象範囲における電力の情報ネットワークを概念的に表すため，インターネット，データセンター，支社・支店の業務端末，記録処理系などを模擬

モデルシステム（2）



実施体制

- 参加者は基本的に運用チーム（防御側）で参加
- 電中研が攻撃および進捗管理
- シナリオに沿って攻撃（運用チームは知らない）



攻撃シナリオ，ケース，促進ルール

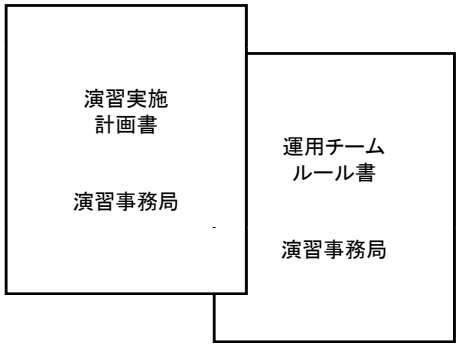
- シナリオは攻撃の状況想定・前提条件等を規定
  - 攻撃目的、侵入経路、攻撃対象、攻撃の種類、・・・
- 攻撃の網羅性を確保するため，ケースを設定
  - ケースの範囲内での具体的な攻撃手法は攻撃者が自由に選択
- 限られた時間内で様々な攻撃を経験するため，前提　条件や促進ルールを適用
  - 前提条件　　：不正端末が接続されていた　等
  - 促進ルール：ユーザーID，パスワードの開示等

攻撃の分類

	攻撃目標	侵入経路	脅威レベル	インシデント
1	DMZのサービスを妨害	インターネット	レベル0 レベル1	Scan Forged Intrusion DoS Other
2	事務系システムの破壊	インターネット RAS 無線LAN データ収集回線 不正接続PC メール	レベル0 レベル1 レベル2	Scan Forged Intrusion DoS Other
3	記録処理系の破壊	インターネット RAS 無線LAN データ収集回線 不正接続PC メール	レベル3 レベル4	Scan Intrusion DoS Other

部門分け

- インシデント対応のあり方をより現実的に経験するため，運用チームをさらに運用部門と情報システム部門に分割
  - 運用部門
    - サイバーテロを検知し，情報システム部門に報告
    - 情報システム部門からの指示に基づき対策を実施
  - 情報システム部門
    - 演習実施にあたって事前に運用チームのルールを策定
    - 運用部門からの報告を受け，①情報を分析，②ルールに基づき対応方針を決定，③運用部門に対する指示を行う。



検討会

- 演習最終日あるいはケース終了時に，演習で経験したことを，より有機的に理解し，ノウハウや知見として習得するため，攻撃チーム，運用チーム，進捗管理チーム合同で検討会を実施

この時，初めて攻撃／運用チームが顔合わせ

- 攻撃者の行為，攻撃の予兆・現象の発生を時間軸で整理
- 各チームがそれぞれの事象に対してお互いに意見交換

実施結果

- 様々な攻撃手法で想定したケースを網羅

限られた期間の中で多種多様な攻撃を実現

- 演習の実施により得られたノウハウと知見を以下の観点からとりまとめることができる
  - 技術
  - セキュリティポリシー
  - 人・組織

参加者の意見・コメント

- 知識として知っていたが、実際に経験すると検討しておくべき点があるのが分かった
- 日常業務とは異なる部門を担当したことで、相手に伝わりやすい報告・指示方法が実感できた
- 状況を整理し、運用チーム内で情報共有しておくことが重要である
- 部門間で電話連絡に齟齬が生じるケースがあった。

まとめ

- モデルシステムを用いてのサイバーテロ演習を実施
- 様々な攻撃手法で想定したケースを網羅

限られた期間の中で多種多様な攻撃を実現

- 演習により得られた知見とノウハウを，技術，セキュリティポリシー，人・組織の観点からとりまとめることができる

ご清聴ありがとうございました

松井 正一
matsui@criepi.denken.or.jp