

標的型攻撃の増加と人材育成 CYBER RANGE ENVIRONMENT FOR EDUCATION

標的型攻撃の定義

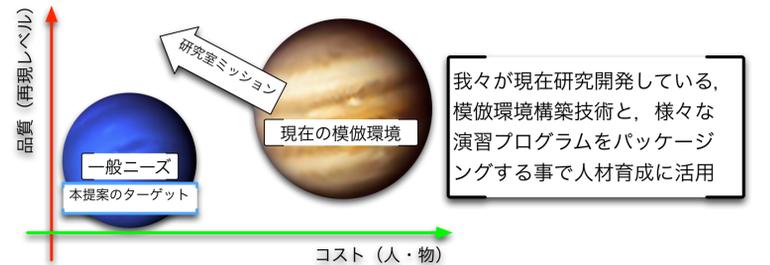
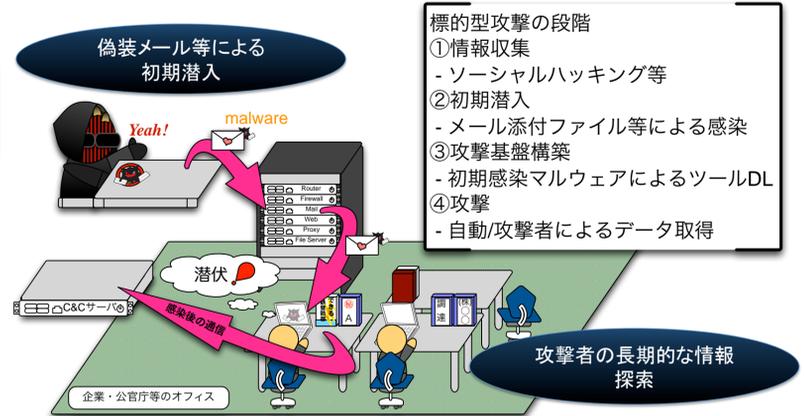
- 特定の相手に狙いを定め、その相手に適合した方法・手段を用いて侵入・潜伏し、場合によっては長期にわたって継続するサイバー攻撃

攻撃の特徴

- ソーシャルハッキング等によるメールアドレスや、各種内部情報の取得し、特定の企業やユーザを攻撃
- 通常のウィルスの様な感染ノードを破壊するような派手な挙動はせず、秘密裏に潜伏すると共に、長期的に情報を収集

セキュリティ人材の不足

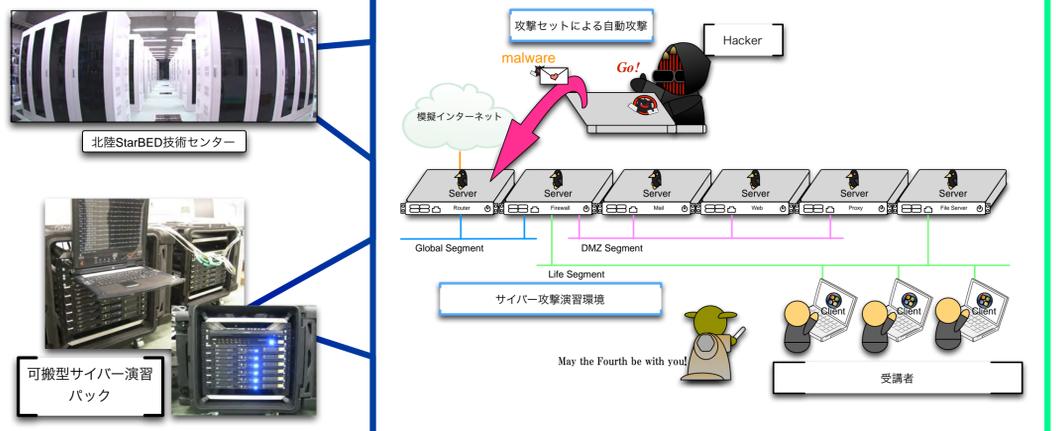
- セキュリティ人材8万人月不足
- 現職のセキュリティ人材の6割がスキル不足
- セキュリティ人材育成が急務
 - 人材育成の裾野を広げ、官民の対応力の底上げ
 - 一般市民への啓蒙活動による社会全体のリテラシーの向上



サイバー攻撃演習環境 CYBER RANGE ENVIRONMENT FOR EDUCATION

セキュリティ演習パッケージ

- 一般的な組織ネットワーク環境とユーザ端末を模擬
- 各種レベルの演習シナリオセット
- 演習レベルにあわせた攻撃セット
- StarBED環境を用いた複雑な環境と高度な攻撃も再現可能



可搬型演習パッケージ

- 環境規模等を縮退する代わりに手軽に演習を行えるパッケージ
- セキュリティ演習パッケージを可搬型機材で実現
- StarBEDへの接続環境が準備出来ない会場でも演習可能
- SDN技術を活用した安価な演習システム

要素技術：電網検証 ALFONS CYBER RANGE ENVIRONMENT CONTRUCTOR

演習環境の自動構築

- 各種組織ネットワークのトポロジの再現
- テンプレートに基づくインスタンス生成
 - 物理・仮想マシンが混在可能
 - 演習シナリオに基づきコンテンツや設定を挿入

逐次的・反復的な環境構築

- 対話的に環境構築するUIも有する
- 構築した模擬環境の保存と再構築が可能
 - 作成した環境情報をXML形式で保存可能
 - 保存したXMLにより、同じ環境を繰り返し構築可能

計測・監視機構 (拡張予定)

- 演習環境のトラフィックの柔軟な計測監視
 - 柔軟なポイント選択
 - 柔軟なフィルタリング
- SDN/NFV技術と環境構築技術の融合
 - 仮想スイッチ制御
 - Hyper Visorからの情報収集
 - フィルタリング

ビルディングブロック型インスタンス作成

