サイバー攻撃解析･防御モデル実践演習の実証実験①

概要

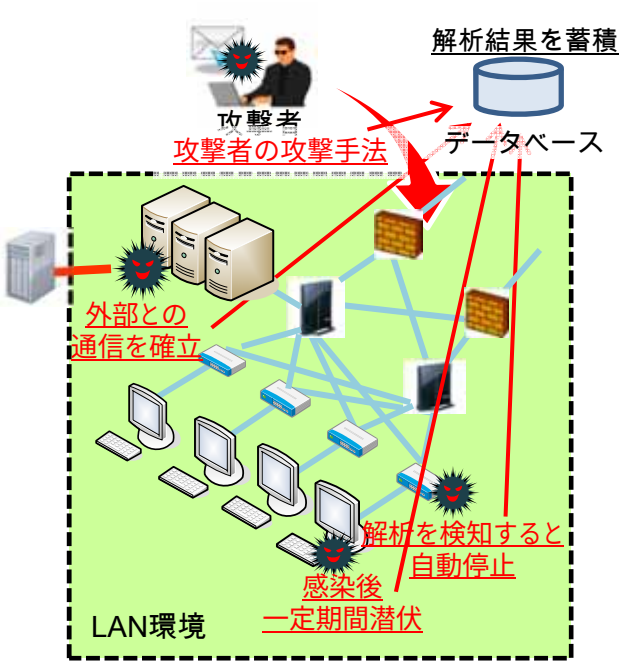
■ 国会、政府機関、民間企業等に対する標的型攻撃※による機密情報の窃取等の被害が頻発している。標的型攻撃は手口が巧妙かつ複雑であるから、当該攻撃に対応可能な環境を実現することが必要。

※標的型攻撃：特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃。

■ 標的型攻撃等の新たなサイバー攻撃に対応可能な環境を実現するため、攻撃の解析及び防御モデルの検討を行い、官民参加型のサイバー攻撃に対する実践的な防御演習を実施する。

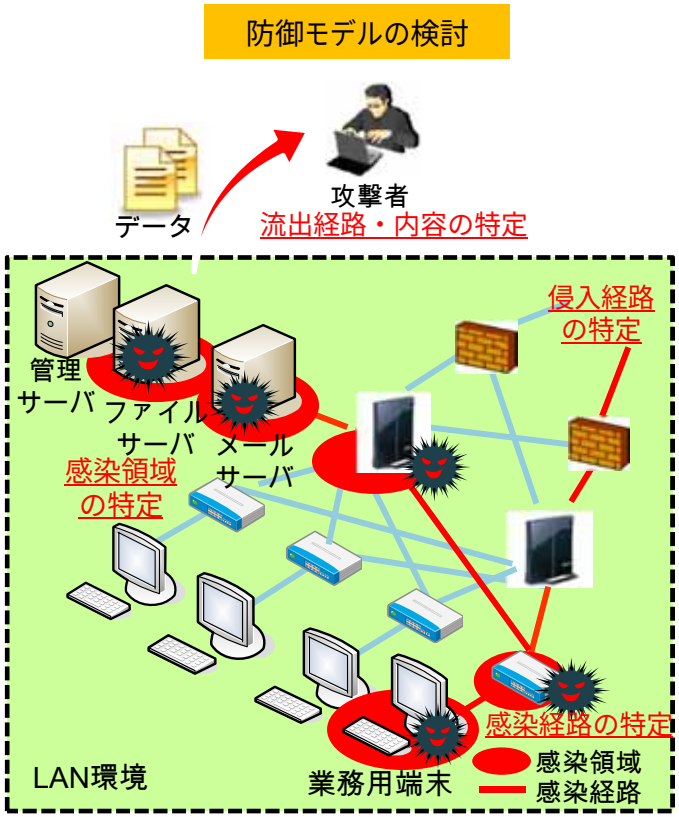
具体的内容

サイバー攻撃の解析



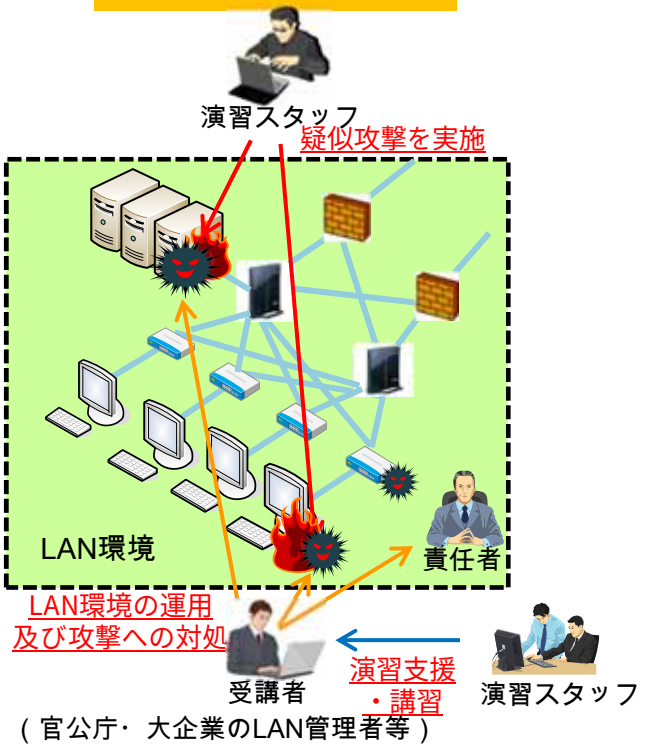
サイバー攻撃の情報収集･解析手法の確立

防御モデルの検討



サイバー攻撃の被害状況の分析･特定

実践的防御演習の実施



一連のインシデント対応プロセスを通じて受講者のサイバー攻撃対処能力を高める

サイバー攻撃解析･防御モデル実践演習の実証実験②

有識者からの指摘事項

1.「サイバー攻撃の解析」の具体的な協力先と体制を構築すべき。

2.「実習の実施」が人材育成のみでは、不十分である。

3. 実証実験の次を提案して頂きたい。

対応

1. サイバー攻撃の解析においては、**アンチウイルスベンダ等とマルウェア検体の提供などの連携体制を構築**し、解析の高度化に努めているところ。

2. 実践的防御演習における検証を通じて、標的型攻撃等の**サイバー攻撃に対するインシデントレスポンスにおいて、LAN管理者等が習得すべきスキルセットを策定**することにより、人材育成にとどまらず関係機関へ成果の共有･展開を図っていく。

3. 本事業について、**実践的防御演習の運営に必要となる事項についてまとめた「演習プログラム運営ガイドライン」を策定**するなど民間企業等における成果の転用を図る。加えて、**ものづくりの原動力である中小企業向けの防御モデルを平成26年度より新たに検討･実証**し、実証実験の次の具体的な実装･事業展開を強化していく。