3.13.2　サイバー攻撃対策総合研究センター　サイバー攻撃検証研究室

室長（事務取扱）　　平　和昌　ほか５名

新たな脅威へ対抗する技術を効率よく検証するために

【概　要】

サイバー攻撃検証研究室では、同じくサイバー攻撃対策総合研究センターに属するサイバー防御戦術研究室で開発されたサイバー攻撃への対応技術の有効性を検証するために、現実世界に近似した環境を提供することを目指している。現実世界で実用に耐える対応技術であるかどうかを見極めるためには、高精細に現実環境を模倣し、そして、その環境内で発生したイベント内容を保存、観測できる仕組みが必要となる。また、必要なときに必要な環境を迅速に構築することも重要な要素である。これらの要求を満たすため、図１に示した４つの課題をあげ、研究開発を推進している。1.「高精細 ICT 環境の再現・模擬技術」サイバー防御戦術研究室で開発した標的型攻撃対策技術を動作させるための基本技術であり、マルウェアや対抗技術の容易な導入や、マルウェアなどにそこが検証環境であることを感づかせない技術の構築が必要となる。2.「実験データの観測・保存技術」環境内で起こった事象を詳細に保存し、後日でもさかのぼって検証を行えるだけの情報を保存しておくための技術が要求される。3.「検証環境の基盤技術」近年の多様な攻撃に対応するためには、環境を構築できるだけでは不十分であり、検証に必要だと思われる環境を迅速かつ容易に構築でき、更に利用しやすいインタフェイスの提供が重要である。4.「摸倣環境の人材育成への応用技術」サイバー攻撃に対応するためには一部の専門家のみで必要な技術を共有するだけでは不足しており、一般の企業や官庁、大学といった組織内にセキュリティのスペシャリストを配置する必要がある。我々が開発する検証環境はカリキュラムと統合して提供することでセキュリティ演習を実施することができる。

平成 27 年度は検証環境の基盤技術の開発を継続し、サイバー検証環境構築のため開発したツール間での連携を可能とするとともに、実験環境をより現実的とするための利用者摸倣などの技術を開発、現実世界により近い実験環境の統合的な構築を可能とした。また、サイバー人材育成のためのいくつかのプロジェクトに我々の開発してきた技術を提供し、イベントの実施及び実践的評価を行った。

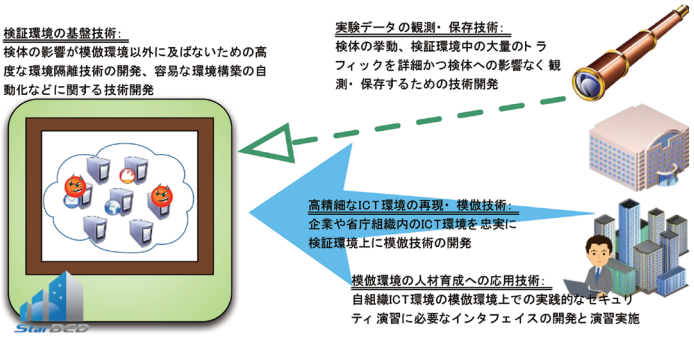

図１　サイバー攻撃検証研究室のミッション

【平成 27 年度の成果】

1.　高精細な ICT 環境の再現・模擬技術

サイバー検証環境内には企業内ネットワークに近似した環境を構築する必要があり、さらに、これらのシステムの利用者の挙動を摸倣する必要がある。より環境に存在する利用者を摸倣するため、摸倣環境の Web サーバにリアルタイムでログを作成するための組織外ユーザの Web 挙動摸倣クローラを作成し、メール模擬システムを構築した（図 2）。これにより、あたかも外部に実際のユーザが存在し、通信を行っているかのような挙動が可能となった。また、HTTP を解析することにより、Web グラフの生成・可視化機構 CHAKRA を開発し、公告事業者や SNS サイトによるプライバシ情報収集状態を可視化とした（図 3）。

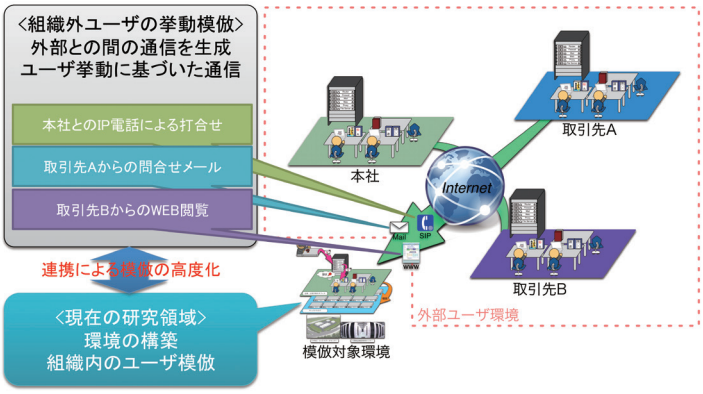

図２　組織外ユーザの Web とメール挙動の摸倣

2.　実験データの観測・保存技術

検証環境で何が起こっているのか、そして過去に何が起こっていたのかを検証するためには、広帯域なネットワークトラフィックをリアルタイムに解析する技術、そしてあるポイントを流れていたトラフィックをすべて保存する技術が必要である。既存の高価なネットワークトラフィック処理装置と比較して、昨年度開発した、安価な PC を利用しセキュリティ解析に重要なレイヤ 7 での解析機構を提供するソフトウェア SF-TAP（図 4）を利用し、HTTP/DNS のリアルタイム解析エンジンを開発した。

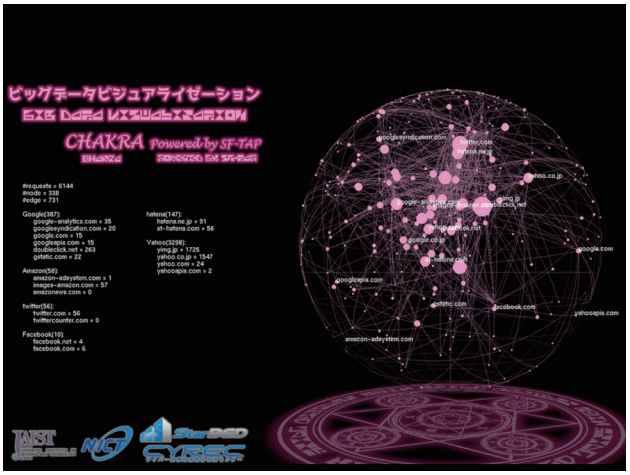

図 3　プライバシ情報の収集状態の可視化
（元となるデータは、利用者に了解済みの仮説ネットワークにて取得）

3.　検証環境の基盤技術

平成 25 年度より開発を継続している、セキュリティ実験環境構築のための機構 Alfons が、前もって生成した OS のイメージとアプリケーションや利用履歴といった追加要素を組み合わせることで任意のノード環境を構築できることを示した。

前年度は、任意のハイパーバイザへの対応、実験途中でのトポロジの変更、作成した実験環境の情報の設定ファイル出力などを開発したが、平成 27 年度は Alfons を複数のセキュリティイベントの環境構築のため投入し実践的評価を行った。実験環境の環境構築の様子を図 5 に示す。

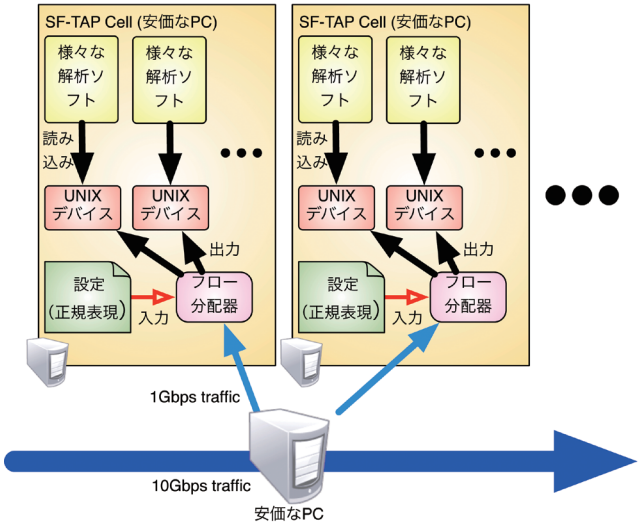

図 4　SF-TAP 概念図

4.　摸倣環境の人材育成への応用技術

前年度と同様に本年度も Hardening や CYDER、enPiT Security といったサイバー人材育成プログラムに我々の技術や知見を提供するなどの協力を行った。Alfons などの技術を検証する場としても有用であり、フィードバックを随時適用しているだけでなく、それぞれのイベントのスタッフと協調したシナリオ作成や環境定義、環境構築を通して、最新の攻撃手法に関する知見などを取得し、新たな課題の整理や既存技術への応用を行った。

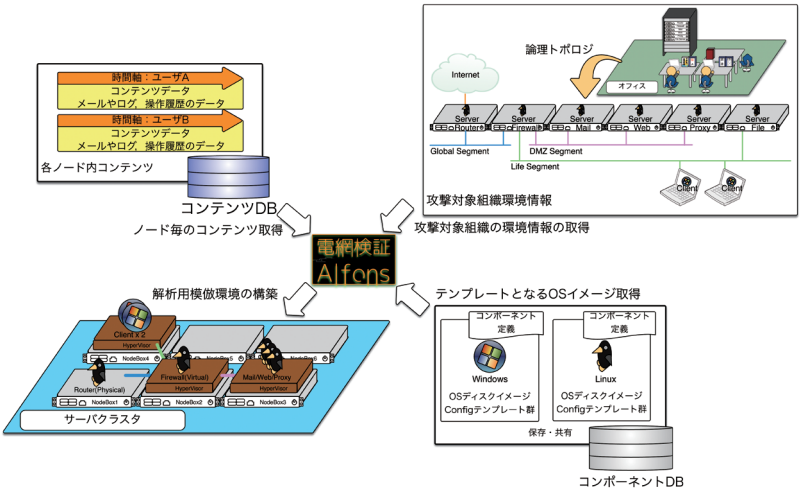

図 5　Alfons を用いた環境構築