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.「高精細な 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 26 年度はこれまで開発を進めてきた検証環境の基盤技術を更に推し進め、サイバー検証環境構築コストを更に下げるとともに環境の現実性を向上させ、環境中のトラフィックを効率的に保存、解析するための新たなツールの開発、そして、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することでイベントの実施自体を可能とした。

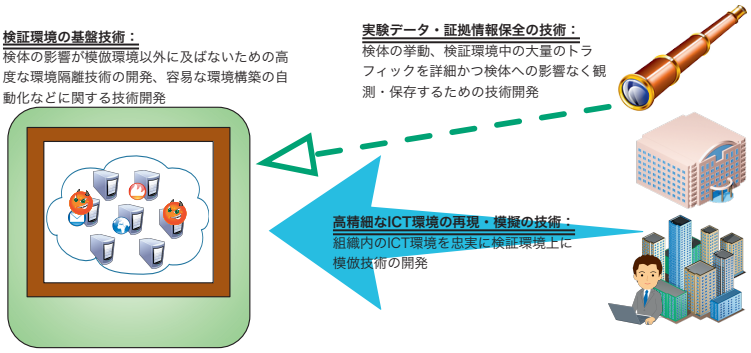

図１　サイバー攻撃検証研究室のミッション

【平成 26 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。一般的な企業では Windows OS が多く利用されており、企業内のシステム利用者を詳細に摸倣するためにはマウスの操作やキーボードの入力の摸倣が必要となる。これを実現するために本年度新たに利用者のマウス及びキーボード入力を“録画”し、その“再生”を可能とする Puppet Master を開発した（図 2）。この際にある程度のブロックごとに作業を保存し、これを任意の順番で組み合わせたフローを作成し実験シナリオとする。さらに“録画”は実際の利用者の操作をそのまま保存するが、このログは簡単な記述方法で保存されているため、直接記述することも可能であり、実際の操作を行わなくてもシナリオ実行が可能である。一般的な作業中はマウスの移動やキーボード入力は人間の動作速度に依存するため、シナリオ上ではイベントごとに動作を停止するといった動作が挿入されている。この動作停止時間を削除することにより高速にイベントを実施することが可能であり、本機能はシナリオ実行だけではなく、Windows OS 上にあたかも利用者が本当に存在するかのような活動履歴を作成することを可能とする。

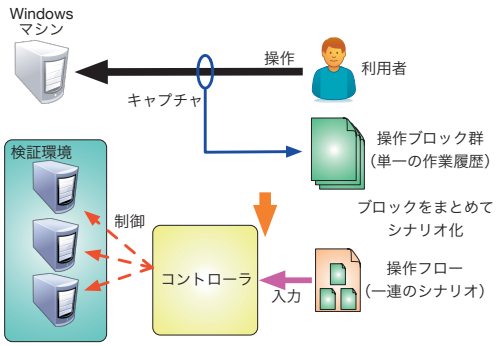

図２　Puppet Master 概念図

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。現在利用されているネットワークトラフィックに対してこのような処理を行うための製品はすでに発表されているが高価なものが多く、実験環境に複数台導入することが難しい。またセキュリティ解析にはレイヤ7での解析が重要となるがそのような機能を提供する製品はそう多くない。そこで安価なPCを利用し、ソフトウェアにより広帯域ネットワークトラフィックのリアルタイム解析とその内容の保存を可能とするSF-TAPを開発した（図3）。SF-TAPは10 Gbpsのネットワークインタフェイスから流入したトラフィックを複製し、さらにフローに分割して複数の1 Gbpsのネットワークインタフェイスに分割する部分と、1 Gbpsのネットワークインタフェイスの先に接続されるPC群からなる。単純に広帯域トラフィックを複数に分けそれを処理するというシンプルな設計であるが、ソフトウェアによる広帯域トラフィック処理の実装には様々なハードルがあり、これを解決している。また、フローの分割部分には正規表現を導入しており利用者が任意のトラフィックを柔軟に指定できる。また、このトラフィックはリーフノードのUNIXデバイスファイルから出力されるため利用者が様々なプログラムで解析を行うことを可能としている。

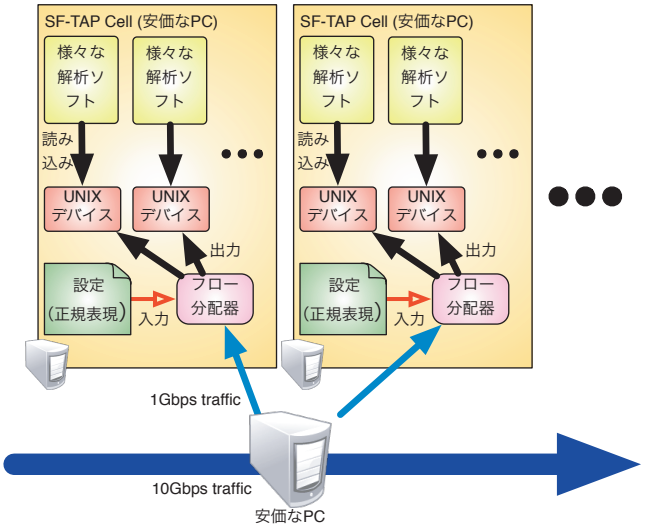

図3　SF-TAP概念図

3. 検証環境の基盤技術

昨年度、開発を進めていたセキュリティ実験環境構築のための機構に機能追加を行いAlfonsと命名した。Alfonsは前もって生成した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する。本年度の開発で、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を設定ファイルとして出力を可能とした。これにより実験環境のより柔軟な構築と構築した環境の再現が行える。Alfonsの概要を図4に示す。

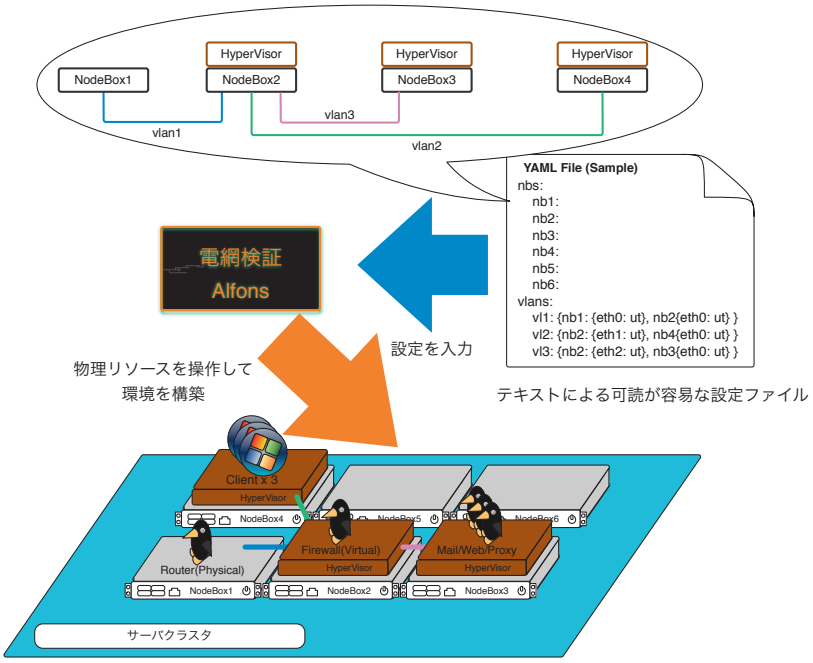

図4　Alfons概念図

4. 摸倣環境の人材育成への応用技術

昨年度と同様に本年度もHardeningやCYDER、SecCap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といった協力を行っている。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ている。