3.12.2　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　　三輪信介　ほか 3 名

高精細なサイバー攻撃防御技術の検証環境の実現を目指して

【概　要】

当研究室では、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の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」: 最も基本的な技術であり、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る。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付かせない技術の構築が必要となる。2.「実験データ・証拠情報保全技術」: 環境内で起こったことを詳細に保存し、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、さらにそれがわかりやすいインタフェイスで利用者が利用できることが重要である。4.「模擬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、大学等の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を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 25 年度は現実的な組織内環境を構築するための第一段階として、一般的な組織内に存在するであろうネットワーク要素とトポロジを持つ単純化した環境を検討し、その環境を仮想マシン、物理マシンを制御し構築するための技術、そして、今後その一連の作業を自動で行うためのプロトコル設計とライブラリの開発を行った。さらには、いくつかの演習イベントと協調し、演習環境の構築と提供を行った。

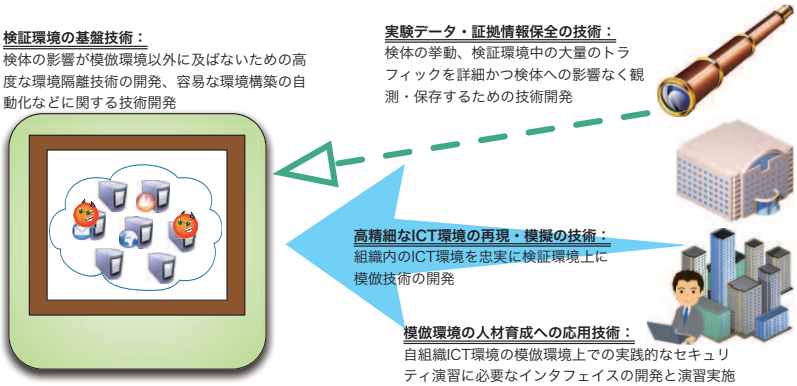

図 1　サイバー攻撃検証研究室のミッション

【平成 25 年度の成果】

- 高精細な ICT 環境の再現・模擬技術

典型的な組織内ネットワーク構築の第一歩として、組織内で一般的に動作していると考えられる Web サーバや Proxy サーバ、ファイアウォールなどの要素とそのトポロジ構成を検討し、実際に仮想ノードを利用して環境を構築、サイバー防御戦術研究室と連携していくつかのマルウェアを動作させその挙動を解析した。また、一部のマルウェアは自身が動作する環境を精査し、観測環境と判断した場合は、一般環境と同様に動作をしなかったり、全く違う挙動を示したりすることがあるため、マルウェアに観測環境だと悟られないよう、各ノードへのメールのやりとりの記録や、Web ブラウザの閲覧履歴などのアプリケーションの利用履歴を導入するためのシステムの設計と開発を行った。本システムは図 2 で示すように、OS やアプリケーションのバイナリデータと、タイムスタンプの付いた各種アプリケーションの履歴データを別々に用意し、対象ノードにバイナリデータを導入した後、利用者から指定された時刻までの履歴データを挿入することで「利用痕跡」を導入するためのシステムである。また本システムは環境構築も同時に行うため、検証環境の基盤技術としての研究開発の側面も持っている。

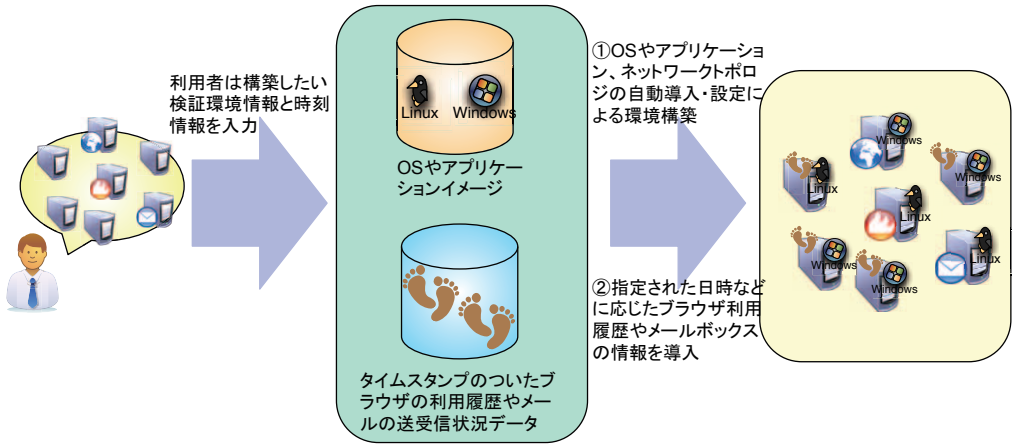

図２　検証環境上へのノードの利用履歴の導入機構プロトタイプ

• 検証環境の基盤技術

サイバーセキュリティのための実証環境に限らず、実験のための環境を自動構築するためには様々な管理モジュールが協調動作し全体的に物理リソースと論理リソースを管理、そして実験シナリオを実行する必要がある。また、環境の観測のためには、現在作成されている環境についての情報が、環境の構築モジュールと観測モジュールの間で共有される必要があるなど、その情報共有が重要となる。NICT では大規模なネットワーク実験環境である StarBED を長年運用し、そのノウハウを蓄積してきた。そのノウハウと既存のモジュールを分析し、サイバーセキュリティ実験にも対応するためのモジュールの検討を行い、まずその間を接続するための通信プロトコルの設計とそれを各プログラムから容易に利用できるライブラリを構築した。これにより、モジュール構築が容易になり、環境構築の迅速化が期待できる。

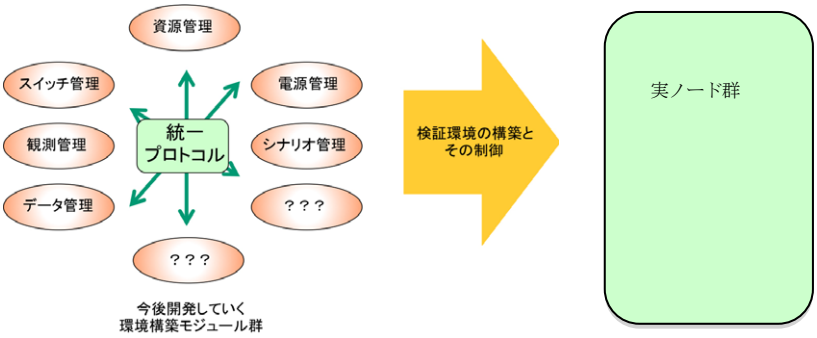

図３　環境管理のための統一プロトコル

• 演習環境の構築と提供

当研究室では、平成 25 年度は 3 つのサイバー演習と協調し、環境構築のためのノウハウの提供や、実際の環境構築を行った。

IT-Keys は大学院生を対象にしたプログラムであり、大学の授業の一環として座学で学習したセキュリティのための各種作業を実際に身をもって体験するため、StarBED 上に環境を構築し、実際に放たれたマルウェアをどう検知し、さらにどう対策をとるかについて学習するための演習である。

Hardening One Remix は一般から参加者を募集し、「守る」技術を競うためのコンペティションである。競技開始時に引き渡された脆弱な環境に対し実行委員が攻撃をしかけ、参加者がそれをどれだけ回避できたのか、また、インシデント発生時の周囲への告知などが適切に行われていたのかなどを総合して順位付けが行われる。過去に Hardening Zero、Hardening One と継続して行われているセキュリティイベントである。

実践的サイバー防御演習（CYDER）は、特に最近多くなっている標的型攻撃を対象とし、標的型攻撃をすでに受けてしまった環境において、どのようにその痕跡を発見するか、またどのように対抗するかを体験するための演習である。

それぞれ 3 つの演習は異なる性質を持っており、外部の実行委員などと協調して環境構築やシナリオを作成するなかで、それぞれに適した環境や攻撃手法に関する知見を取得でき、他の課題への応用が可能となっている。また、我々が開発した技術を外部に提供する非常によい場となっている。