3.12.1　サイバー攻撃対策総合研究センター　サイバー防御戦術研究室

室長　　井上大介　ほか 5 名

標的型攻撃等に対する能動的かつ根本的な防御戦術を立案・実現

【概　要】

標的型攻撃対策技術として、マルウェアに感染したコンピュータからの情報流出に対処する技術についてのフレームワークデザインと、一部プロトタイプ開発を行う。

【平成 25 年度の成果】

標的型攻撃への対策技術の確立に向けて、組織内ライブネット（実トラフィック）のリアルタイム観測及び分析と、各種セキュリティアプライアンス群からのアラート集約を行うとともに、リアルタイム可視化インターフェイスからアラート発生源へのドリルダウンを可能にするサイバー攻撃統合分析プラットフォーム“NIRVANA 改”（ニルヴァーナ・カイ）のフレームワークデザインとプロトタイプ開発を行った（図 1、2）。また、NIRVANA 改を Interop Tokyo 2013 に導入し、ShowNet（最先端のネットワーク機器で構築された展示会場ネットワーク）のライブネット観測・分析を行うとともに、国内外のセキュリティ関連企業複数社と連携して、多様なセキュリティアプライアンス群からのアラート集約の実証実験を実施した。

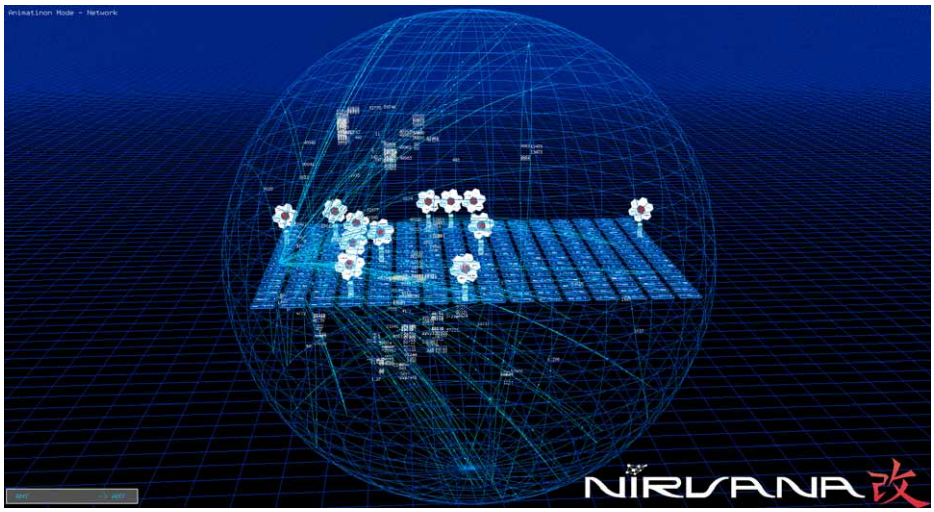

図 1　NIRVANA 改の可視化画面（俯瞰図）

中央の球体表面にインターネット全体の IP アドレス空間をマッピング。球体内部のパネルが組織内ネットワークのアドレスブロックを表現。球体とパネルを行き来する流星状のオブジェクトは、ライブネットトラフィックを示す。

図 2　NIRVANA 改の可視化画面（拡大図）

数字付きパネルが組織内ネットワークの特定のアドレスブロックを示す。パネル直上の六角形のアイコンは各種セキュリティアプライアンスから集約したアラートを表現。パネルをクリックすることでアラート発生源へのドリルダウンが可能。

膨大なライブネットのリアルタイム分析を可能にするライブネット高速分析基盤のプロトタイプ開発を行い、大容量オンメモリ処理により NICT のライブネットを高速に分析可能であることを実証した（図 3）。また、本分析基盤上で動作する分析エンジンとして、ネットワーク境界侵害検出エンジンのプロトタイプ開発を行った。

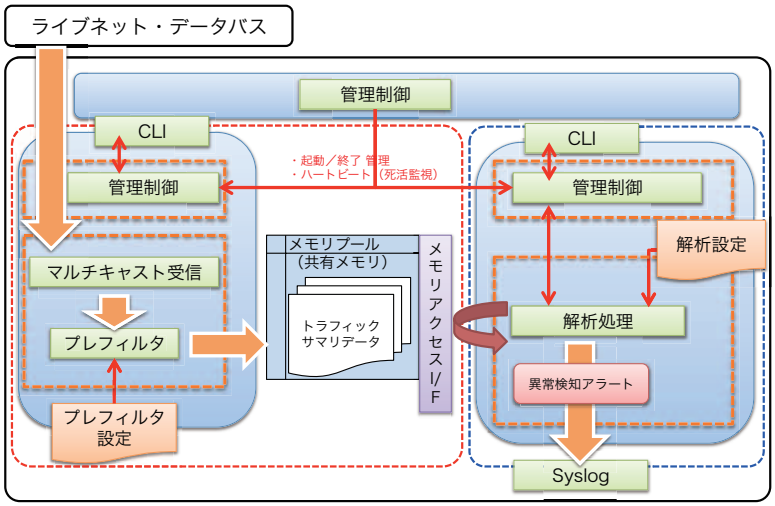

図 3　ライブネット高速分析基盤

アンチウイルスソフト（ホストベースの侵入検知）とライブネット分析（ネットワークベースの侵入検知）を協働させる NIDS[*1]-HIDS[*2] 連携システムの構築を行い、アンチウイルスソフト導入ホスト群のプロセス状態監視やセキュリティレベルの変更等を一元的に行う機構を実現した（図 4）。

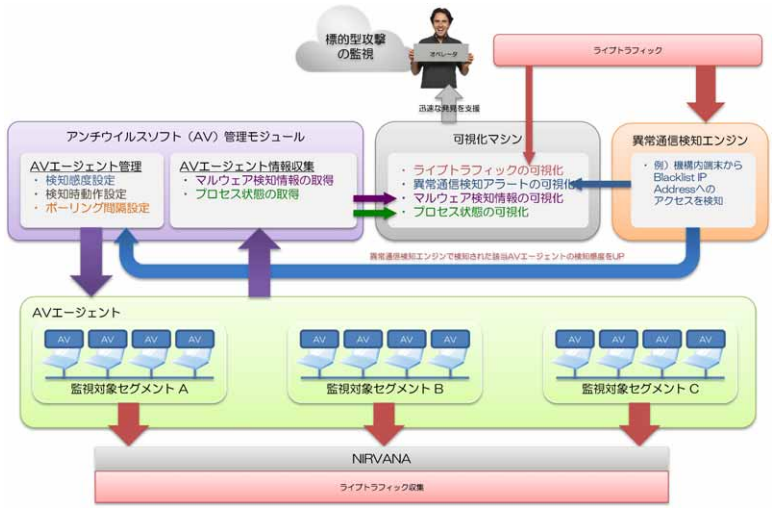

図 4　NIDS-HIDS 連携システム

サイバー攻撃検証研究室と共同で、StarBED 上に組織内ネットワークを簡易的に模擬した模擬ネットワーク環境を構築するとともに、攻撃者が使用する指令サーバ（C&C サーバ）や RAT（リモートアクセスツール）を整備した（図 5）。さらに、本環境内で標的型攻撃の一連の流れを実際に再現する模擬攻防実験を実施し、防御側の攻撃観測・分析技術の検証や、標的型攻撃時に生成される各種ログの検証を行った。

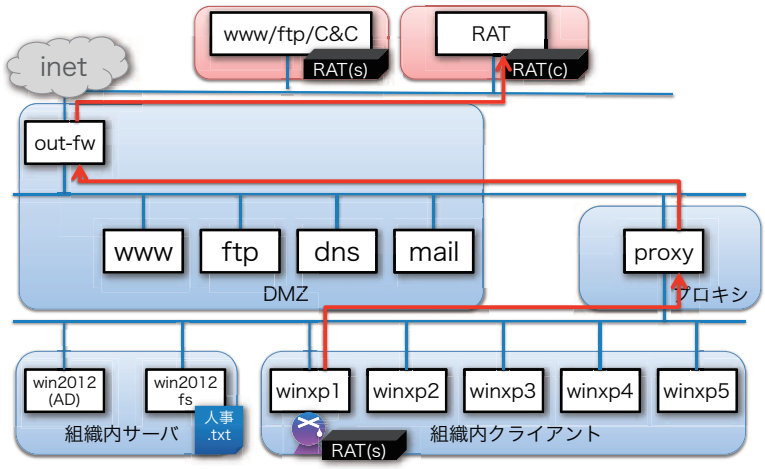

図 5　簡易模擬ネットワーク環境内攻防実験

NICT 内ライブネットトラフィックのリアルタイム観測機構や、ペタバイトクラスの超大規模フォレンジック機構等を設計・構築し、標的型攻撃の研究環境基盤を整備した。

NIRVANA 改をベースに、サイバー攻撃の対処能力の強化を目的とした競技“CTF”（Capture The Flag）の攻防戦をリアルタイムに視覚化する専用エンジン“NIRVANA 改 SECCON カスタム”を開発し、情報セキュリティのコンテストイベントである SECCON 2013 全国大会カンファレンスにおいて CTF 決勝戦のリアルタイム可視化を行った。

[*1] Network-based Intrusion Detection System
[*2] Host-based Intrusion Detection System