3.13.1　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（兼務）　井上大介　ほか 6 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 27 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）の開発を進め、エンドホスト連携機能及び自動防御機能を開発した（図 1、2）。また、NIRVANA 改を Interop Tokyo 2015 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。

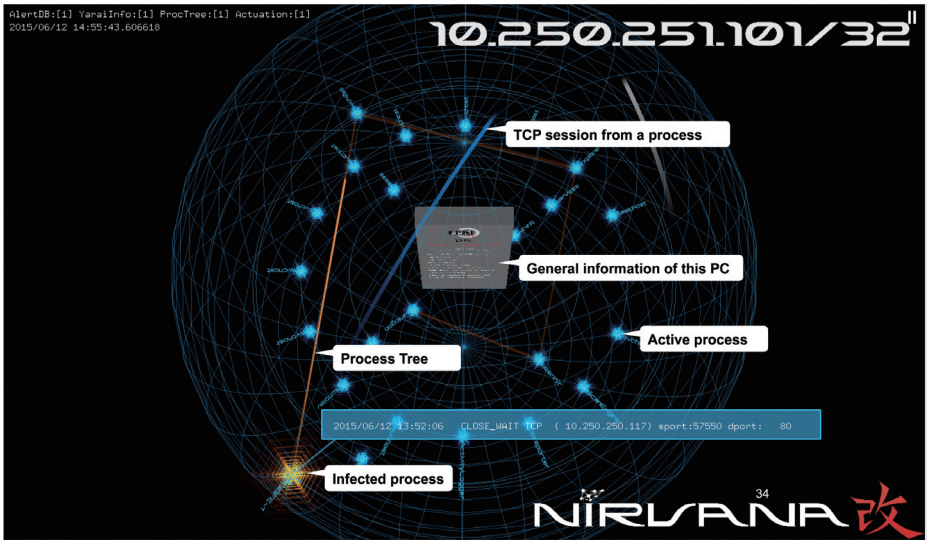

図 1　NIRVANA 改の可視化画面（ホストビュー）

中央にホスト情報の一覧を表示。アラート発生源のプロセスをハイライト表示。マルウェア感染しているプロセスより外部の指令サーバ宛に通信が発生していることを表す。

図 2　NIRVANA 改の自動防御機能

ファイヤーウォール、スイッチ、ルータ、OpenFlow スイッチ等を用いた自動防御の様子。アラートの発見から、通信の遮断までを自動的に処理することが可能。

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開発を進め、大容量オンメモリ処理により NICT のライブネットにおいて 20 万パケット毎秒のリアルタイム処理性能を実証した。また、ブラックリスト方式、ホワイトリスト方式、スロースキャン検知といった、各種ライブネット分析エンジンを開発した。

エンドホスト分析（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] 連携システムの高度化を行い、エンドホスト連携機能及び自動防御機能を開発した。

NIRVANA 改をベースに、サイバー模擬攻防戦“CTF”（Capture The Flag）大会をリアルタイムに視覚化する専用エンジン“AMATERAS[*3]”を開発し、2015 年に日本初の女性限定の CTF 大会である「攻殻 CTF」に導入した（図 3）。

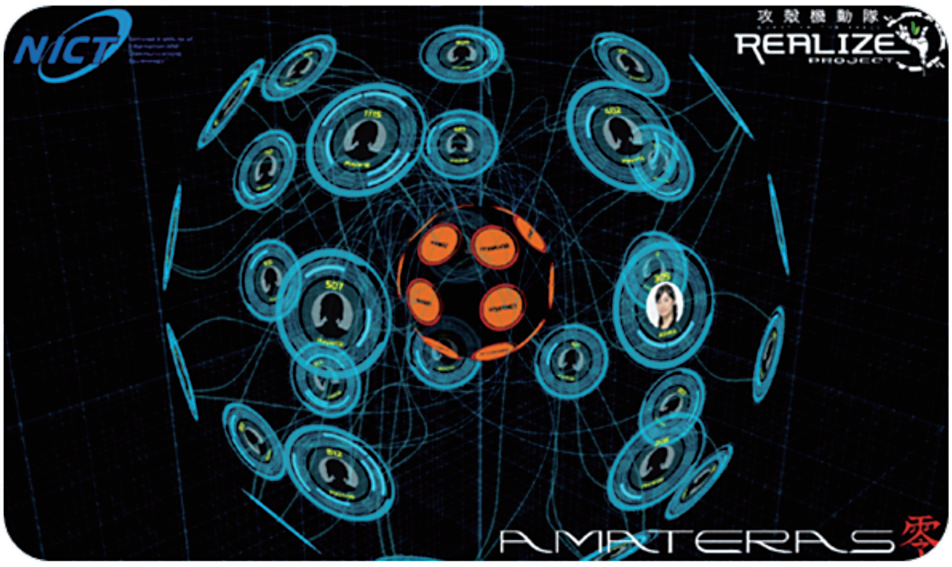

図 3　AMATERAS

中央オレンジ色の球体が CTF の問題サーバ、周囲の青いリングが CTF のプレイヤーを表している。問題サーバの表面にはオレンジ色で問題リングが配置され、各 CTF プレイヤーの得点や回答の正否が、プレイヤーリングにリアルタイムに視覚化されている。

[*1] Network-based Intrusion Detection System

[*2] Host-based Intrusion Detection System

[*3] Advanced Multi-Actor Tactical Exercise Real-time Analysis System: Prototype Version 0