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 26 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、複数種のアラートの横断的な分析を実現する相関分析エンジンのプロトタイプ開発を行った（図 1、2）。また、NIRVANA 改を Interop Tokyo 2014 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。

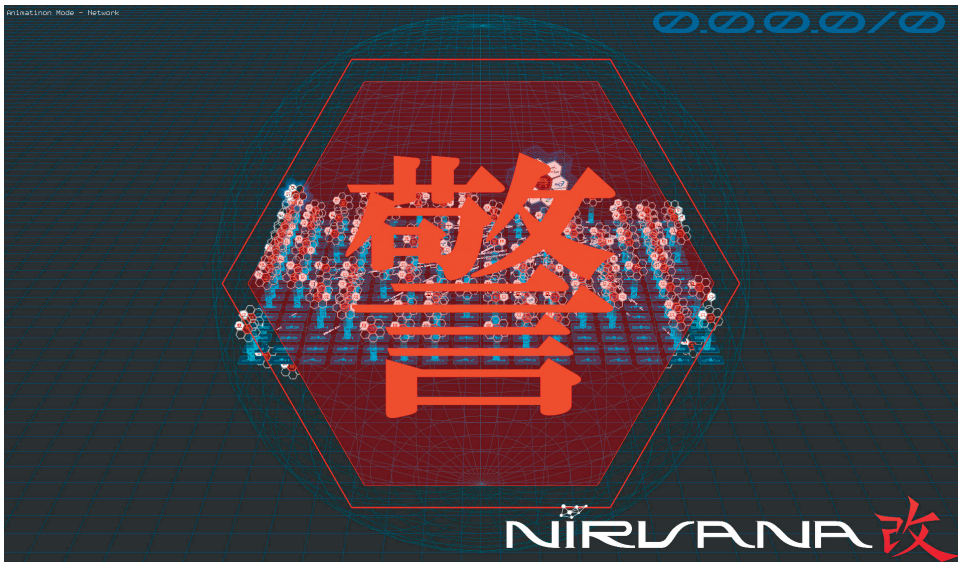

図 1　NIRVANA 改の可視化画面（俯瞰図）

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。画面中央の「警」アイコンは、この瞬間にアラートが発生したことを表す。

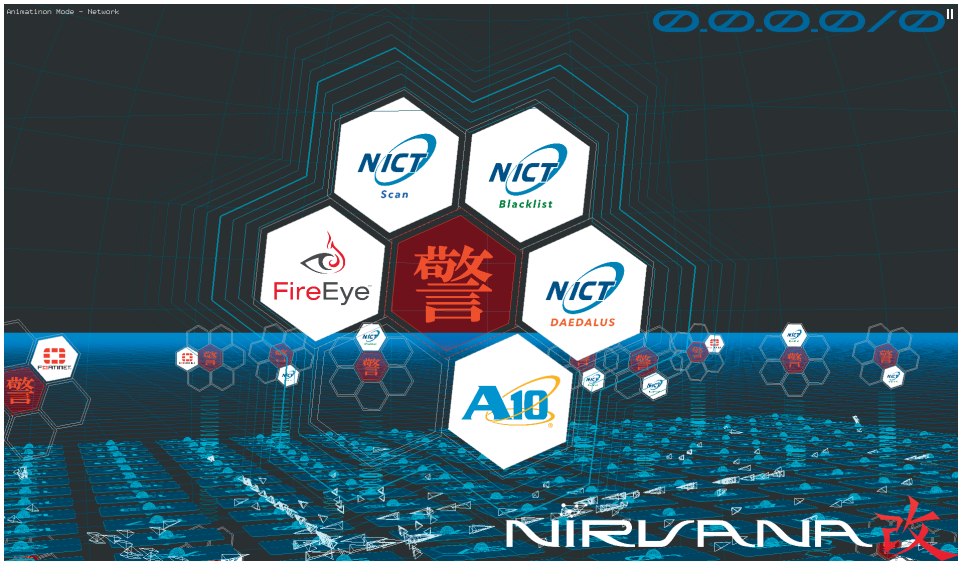

図 2　NIRVANA 改の可視化画面（拡大図）

六角形のアイコンは各種セキュリティ機器からのアラートを表現。相関分析ルールに合致したアラートは、周辺にソニックウェーブが表示される。アラート直下の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、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高度化を行った。

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、エンドホストからの収集情報を拡充するとともに、NICT 内への実験導入を行った。

NIRVANA 改をベースに、サイバー模擬攻防戦“CTF”（Capture The Flag）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 Mk-II”を開発し、日本最大規模の CTF 大会である SECCON CTF 2014 決勝戦に導入、世界各地から集まった CTF のトップチームによる攻防戦をリアルタイムに視覚化した（図 3）。

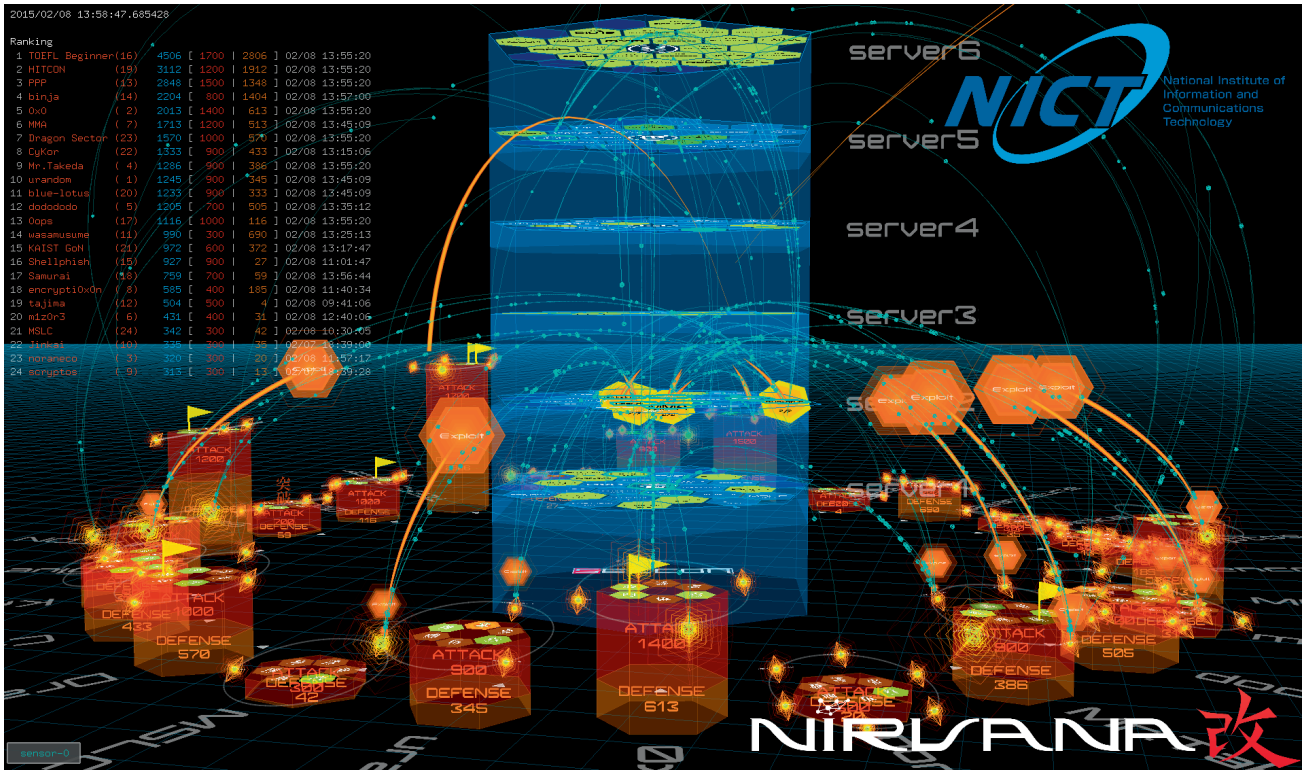

図 3　NIRVANA 改 SECCON カスタム Mk-II

中央青色の六角柱は CTF の問題サーバとその攻略状況（黄色い六角形が正答したチーム）を、その周囲のオレンジ色の六角柱が決勝戦を戦った 24 チームを表している。ポイント数が多いチームほど六角柱の高さが増していく。明るいオレンジ色のエネルギー砲は、各チームから問題サーバに射出されている攻撃（Exploit）を表す。

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