国立研究開発法人 情報通信研究機構

プレスリリース

平成 27 年 6 月 8 日

サイバー攻撃統合分析プラットフォーム“NIRVANA 改”を機能強化！

～ エンドホスト連携機能と自動防御機能を開発 ～

国立研究開発法人 情報通信研究機構（NICT、理事長：坂内 正夫）は、株式会社 FFRI（代表取締役社長：鵜飼 裕司）及び株式会社ディアイティ（代表取締役社長：三橋 薫）の協力を得て、標的型攻撃等のサイバー攻撃に対抗するための統合分析プラットフォーム“NIRVANA 改”（ニルヴァーナ・カイ）の新機能として、エンドホスト（PC）の集中制御やマルウェア感染プロセスの特定が可能な「エンドホスト連携機能」、ネットワーク機器と連動して異常な通信の遮断や感染ホストの隔離が可能な「自動防御機能」を開発しました。これにより、ネットワーク系とエンドホスト系の 2 系統のセキュリティ対策が統合されるとともに、自動的な防御策の展開が可能となり、組織内における情報セキュリティインシデントの詳細な原因究明と迅速な対応の実現が期待できます。

“NIRVANA 改”及びエンドホスト連携機能、自動防御機能については、2015 年 6 月 10 日（水）～12 日（金）に幕張メッセで開催される「INTEROP Tokyo 2015」で動態展示を行います。
（http://www.interop.jp/2015/index2.html）

【背景】

標的型攻撃に代表される特定組織を執拗に狙ったサイバー攻撃によって、ファイアウォールや侵入検知システム等、従来型の「境界防御」が突破される情報セキュリティインシデント[*1] が多発し、社会問題となっています。

また、境界防御によるネットワーク系のセキュリティ対策と、アンチウイルスソフトウェア等のエンドホスト（PC）系のセキュリティ対策は独立に運用されることが多く、例えばネットワーク系で組織内に異常な通信が発見された場合、その通信を行っているプロセスをエンドホスト内で特定することは容易ではありませんでした。

さらに、インシデント発生時には、担当者が物理的に感染ホストをネットワークから隔離する等、人手を要する現場対応に迫られることが多く、迅速な対応の妨げや、人的コストの増大に繋がっていました。

図 1 エンドホスト情報と自動防御状況の可視化

中央のモノリスにエンドホストの情報一覧を、周回軌道にエンドホスト内のプロセス群を表示（青：正常プロセス、橙：マルウェアプロセス）、インターネットを表す最外縁の球体表面に自動防御状況を赤色の六角形で表示

【今回の成果】

NICT はこれまで、組織内ネットワークを流れる通信のリアルタイムな観測・分析や、各種セキュリティ機器からのアラート集約を実現するサイバー攻撃統合分析プラットフォーム“NIRVANA 改”を開発してきました。

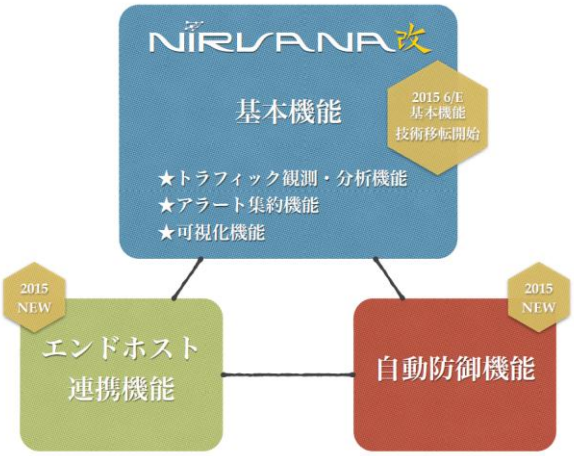

図 2 “NIRVANA 改”の新機能

今回、“NIRVANA 改”の新機能として「エンドホスト連携機能」と「自動防御機能」を開発しました（図 1、図 2）。

エンドホスト連携機能 [#1]

国産の標的型攻撃対策ソフトウェア“FFR yarai”と連動し、組織内のエンドホスト群の各種情報を収集するとともに、マルウェアプロセスを特定し、そのプロセスの親子関係や通信履歴等をリアルタイムに導出します。また、エンドホスト群のマルウェア検出感度を一斉変更するなどの、集中制御も可能です（図 3）。

[#1] 株式会社FFRI（http://www.ffri.jp/）の協力による開発

自動防御機能 [#2]

インシデント発生時に、事前定義したアクチュエーション（動作）ルールに従って、ファイアウォールやスイッチ等のネットワーク機器を自動的に制御し、感染ホストの隔離や異常通信の遮断等が可能です。また、エンドホスト連携機能と連動し、エンドホスト内の特定プロセスの停止等の精緻な制御も可能です（図 4）。

[#2] 株式会社ディアイティ（http://www.dit.co.jp/）の協力による開発

これにより、ネットワーク系とエンドホスト系の 2 系統のセキュリティ対策が統合されるとともに、防御策の自動展開が可能となり、組織内における情報セキュリティインシデントの詳細な原因究明と迅速な対応の実現が期待できます。

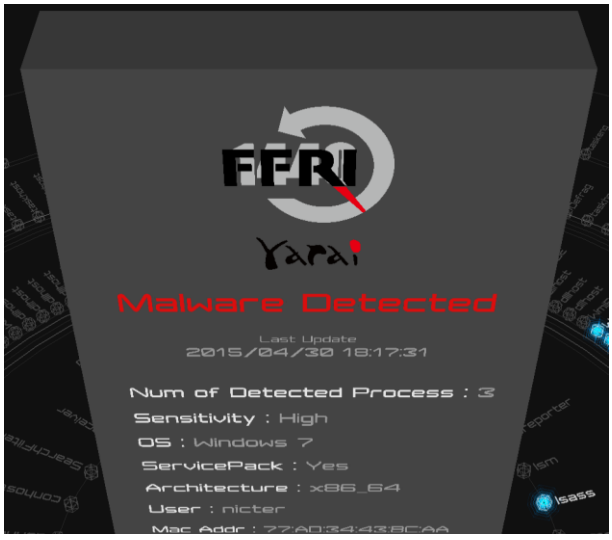

図 3 エンドホスト連携機能

モノリス表面にマルウェア検出等の情報を表示

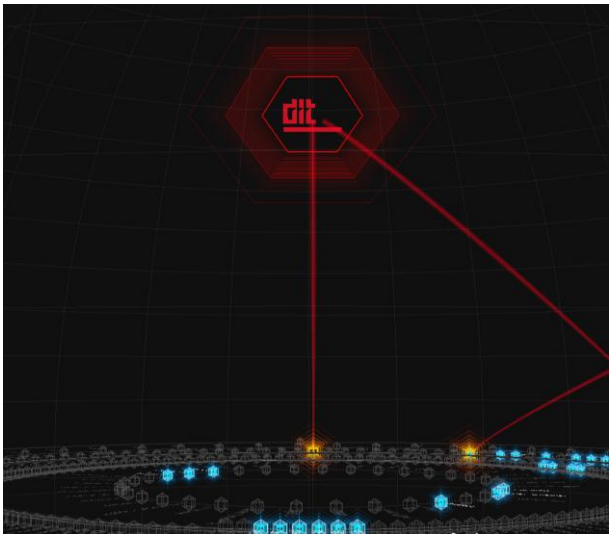

図 4 自動防御機能

マルウェアプロセスからの異常通信が自動遮断されている様子

さらに、“NIRVANA 改”の可視化機能も強化し、ネットワーク系のドリルダウン（全体から詳細への分析機能）に加え、エンドホスト内部にまでシームレスに没入できるようになり、セキュリティオペレーションがより円滑になります（図 5）。

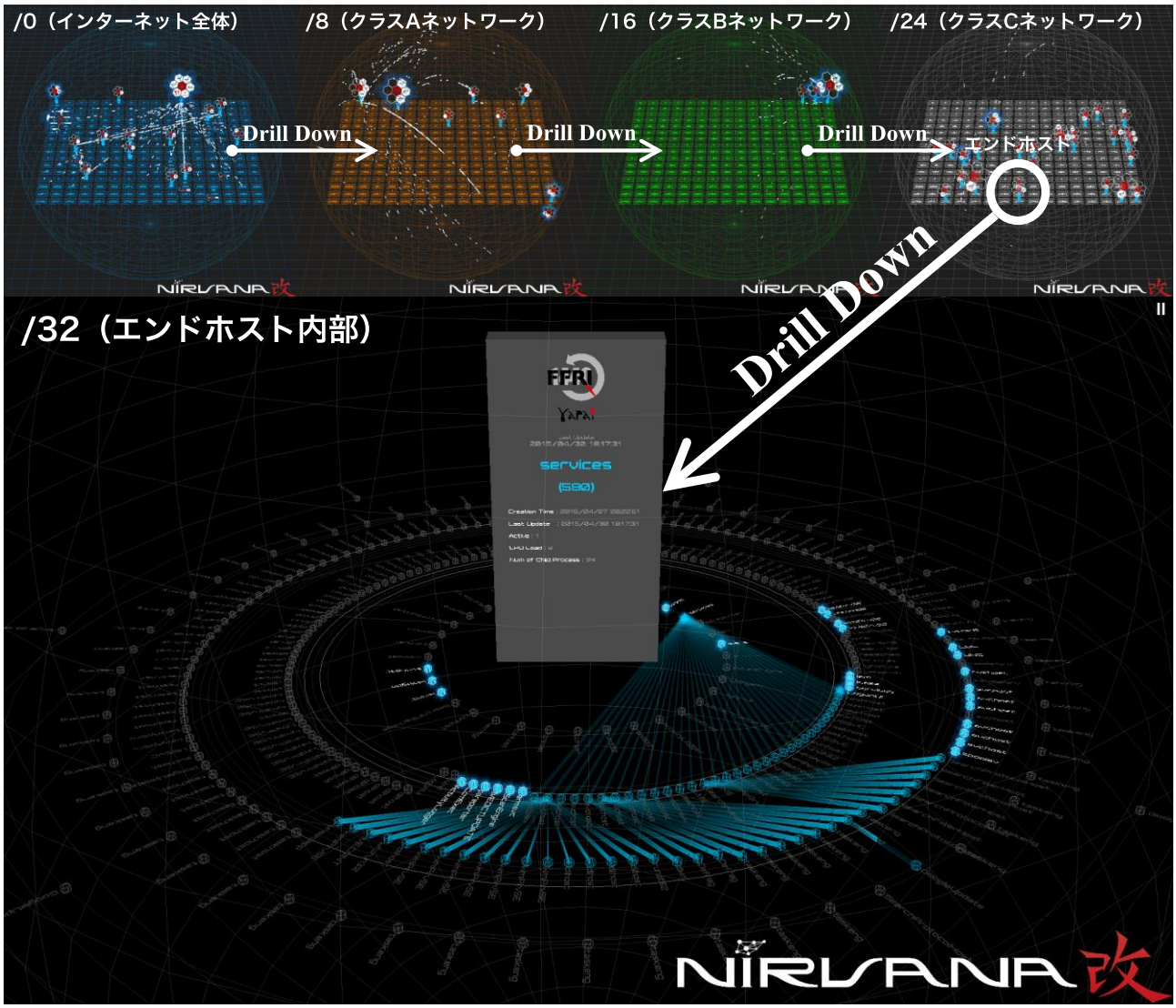

図 5 シームレスなドリルダウンとエンドホスト内のプロセス情報

インターネット全体（左上部）からエンドホスト内部（下部）までをシームレスにドリルダウン可能、エンドホスト内ではモノリス直近に最上位の親プロセスを配置、軌道半径が広がるにつれプロセスツリーの階層が深まる、青線はプロセスの親子関係を表示

【今後の展望】

“NIRVANA 改”の基本機能（トラフィック観測・分析機能、アラート集約機能、可視化機能）は、2015 年 6 月末に技術移転開始予定です。

なお、“NIRVANA 改”及びエンドホスト連携機能、自動防御機能については、2015 年 6 月 10 日（水）～12 日（金）に幕張メッセで開催される「INTEROP Tokyo 2015」（http://www.interop.jp/2015/index2.html）で動態展示を行います。

＜ 本件に関する問い合わせ先 ＞

ネットワークセキュリティ研究所 サイバーセキュリティ研究室
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
井上 大介
Tel: 042-327-6225
Fax: 042-327-6640
E-mail: nicter-interop@ml.nict.go.jp

＜広報＞

広報部 報道担当
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp

補足資料

＜用語解説＞

***1 情報セキュリティインシデント**

企業や大学等、組織の情報通信ネットワークにおける情報漏えいやデータ改ざん、Web サービスの妨害などの情報セキュリティに関する事故を意味する。

＜参考＞

これまでの“NIRVANA 改”関連の報道発表

- 2013 年 6 月 10 日
  「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）を開発 」
  （http://www.nict.go.jp/press/2013/06/10-1.html）

- 2011 年 6 月 2 日
  「リアルトラフィックの可視化ツール “NIRVANA” を開発 ～通信の「見える化」でネットワーク管理を簡単に～」
  （http://www.nict.go.jp/press/2011/06/02-1.html）