4　サイバーセキュリティ技術：ライブネット観測・分析技術
4-1　NIRVANA 改によるライブネット分析

津田　侑　金谷延幸　遠峰隆史　神薗雅紀　神宮真人　高木彌一郎　鈴木宏栄

特定組織にねらいを定めたサイバー攻撃である「標的型攻撃」が重大な脅威となっている。標的型攻撃は NICTER のような大規模観測網ではとらえられない。それゆえ、攻撃者に組織内部に侵入されることを前提に、迅速に攻撃を検知し対処することが要求される。本稿では組織内部に流れるトラフィックを観測するとともに各種セキュリティ機器からのアラートを統合して可視化する分析プラットフォーム NIRVANA 改（ニルヴァーナ・カイ）について述べる。

1　はじめに

インターネットを介して様々なサイバー攻撃が発生し、大きな社会問題となっている。たとえば、新たなマルウェアが日々製造されコンピュータへ感染させるように攻撃者によって仕向けられ、感染後には別のコンピュータへと拡大させていく活動もある。さらには、ターゲットをサービス不能に追い込む DoS 攻撃や機密情報の窃取、機器の破壊を目的とするものなど、サイバー攻撃の種類は多岐にわたる。

これまでサイバーセキュリティ研究室では、インターネットの広範囲に影響が及ぼされるサイバー攻撃の活動傾向を大局的に観測・分析するために NICTER（ニクター）を研究開発してきた [1] [2]。NICTER は未使用 IP アドレス空間（ダークネット）を大規模に観測し、ここに達するパケットを観測・分析することによって、自己増殖型のマルウェアが感染拡大を試みる様子や DoS 攻撃の跳ね返り（バックスキャッタ）をとらえることができる。

一方で、特定組織にねらいを定めたサイバー攻撃である「標的型攻撃」が重大な脅威となっている。この種の攻撃は明確なターゲットが存在するために、NICTER のようなダークネット観測網ではその様子をとらえられない。そこで、著者らは NICTER で培った技術を基に組織内部のネットワーク（ライブネット）のトラフィックをリアルタイムに観測・分析・可視化できる NIRVANA 改（ニルヴァーナ・カイ）を開発した。NIRVANA 改はライブネットを流れるトラフィックと組織内部に設置されたセキュリティ機器からのアラートを集約・可視化する統合分析プラットフォームである。

本稿の構成は以下のとおりである。**2** でまず NIRVANA 改の基礎技術のひとつである NIRVANA を説明する。そして **3** では、NIRVANA 改の可視化ユーザインタフェースから NIRVANA 改のバックエンドで動作するコンポーネントについて述べる。**4** では、NICT における NIRVANA 改を活用したセキュリティオペレーションの事例について報告し、最後に **5** に本稿のまとめと今後の展望を述べる。

2　ネットワークリアルタイム可視化システム　NIRVANA

NIRVANA 改の先行技術としてネットワークの管理や運用を支援するための可視化システム NIRVANA[3] がある。NIRVANA はライブネットにおける膨大なネットワークトラフィックをリアルタイムに可視化するシステムである。NIRVANA の可視化ではネットワークトラフィックをパケット単位で描画することや流量を表現することが可能である。さらには、トポロジ図とネットワークの経路情報を用いることでネットワーク機器間をトラフィックが流れていく様子を可視化できる。

NIRVANA ではネットワークの管理・運用を目的として、ネットワーク管理者の負荷を軽減し、管理コストを低減させるための機能が実装されている。しかし、実際にネットワークを管理する上では、組織外からのサイバー攻撃や組織内でのマルウェア感染といったセキュリティインシデントへの迅速でかつ適切な対応が要求される。特に、2010 年代に入ってから社会問題となっている標的型攻撃への対策には、ファイアウォールや侵入検知システムといった組織内外の境界上で防御するセキュリティ機器だけでなく、組織内での攻撃者の活動を素早く発見することが不可欠となる。このような要求から、ライブネットから得られる多種多様な情報を統合、分析、可視化することで迅速なセ

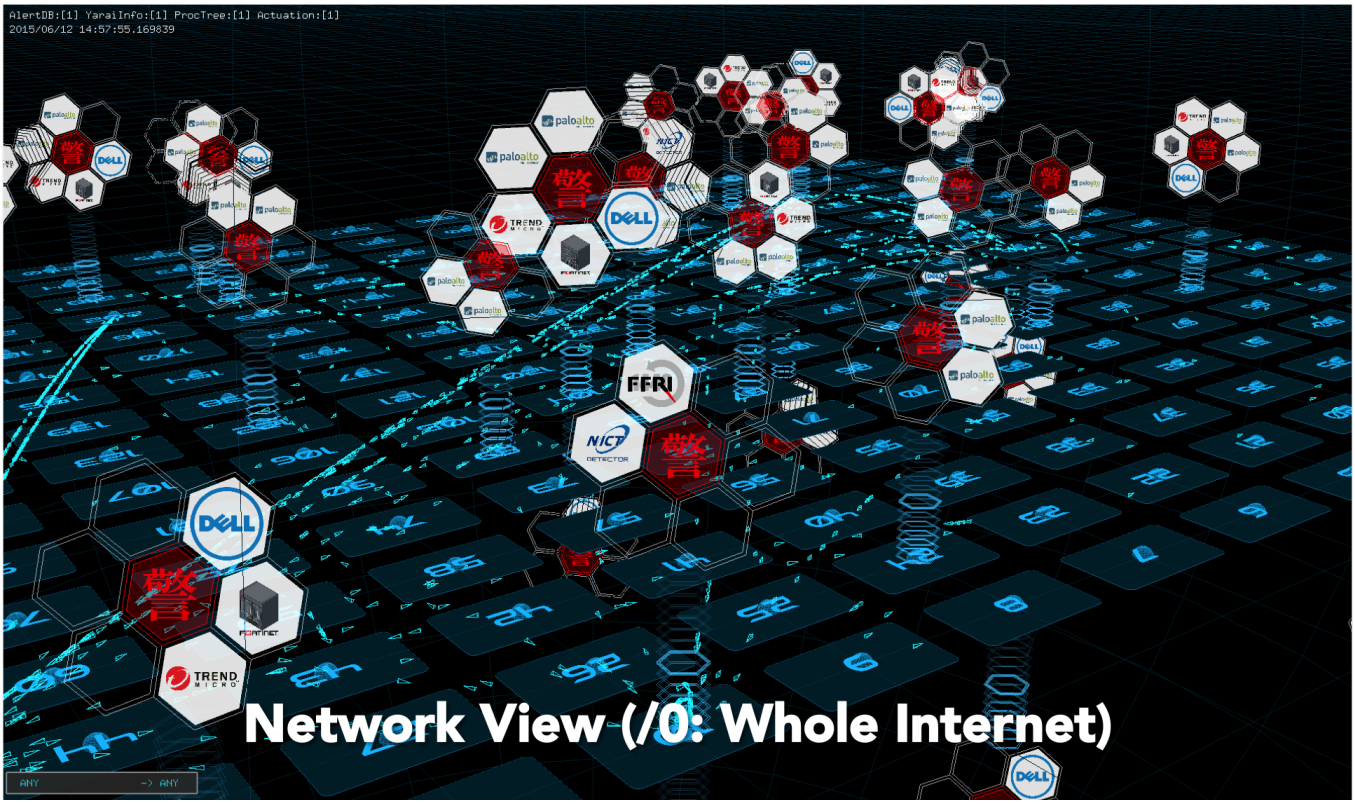

図 1　NIRVANA 改におけるトラフィックとアラートの可視化

キュリティオペレーションを実現するためのプラットフォームである NIRVANA 改の研究開発を進めている。

3　サイバー攻撃統合分析プラットフォーム　NIRVANA 改

3.1　NIRVANA 改の概要

NIRVANA 改は、NIRVANA で培ったネットワークトラフィックの可視化技術と組織内に設置されたセキュリティ機器のアラート情報を統合することで、ネットワーク管理者が迅速にセキュリティインシデントを発見することを支援するプラットフォームである。

図 1 に NIRVANA 改を用いてネットワークの状況を可視化した様子を示す。これは IPv4 のインターネット空間全体（/0 ネットワーク）を表し、0 から 255 までの数値が記載されたパネルはクラス A のアドレスブロックに対応している。パネル間を飛ぶ三角すいのオブジェクトはその間で送受信されるパケットを表している。アドレスブロックのパネル上に表示された花形のオブジェクトでは各種セキュリティ機器から集約されたアラートを可視化している。あたかも花びらのように見える一つひとつがセキュリティ機器と対応し、そのアドレスブロック内部で異常が検知されたことを意味している。

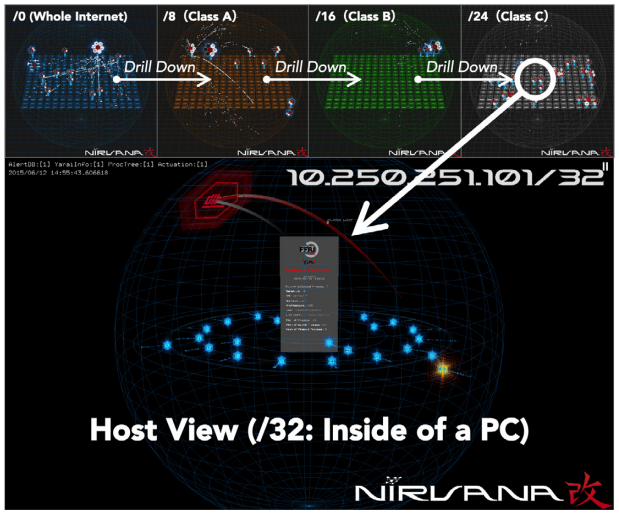

図 2　ドリルダウンの様子

NIRVANA 改では、インターネット空間全体からクラス A アドレス（/8 ネットワーク）、クラス B アドレス（/16 ネットワーク）、クラス C アドレス（/24 ネットワーク）と大きなアドレスブロックからアラート発信源がある小さなアドレスブロックに向かって掘り下げて進んでいく「ドリルダウン機能」があり、最終的にはひとつのホストの内部（/32 ネットワーク）までたどり着ける。ドリルダウンの様子を図 2 に示す。

NIRVANA 改はこれまでに紹介してきた、セキュリティオペレータが操作する可視化ユーザインタ

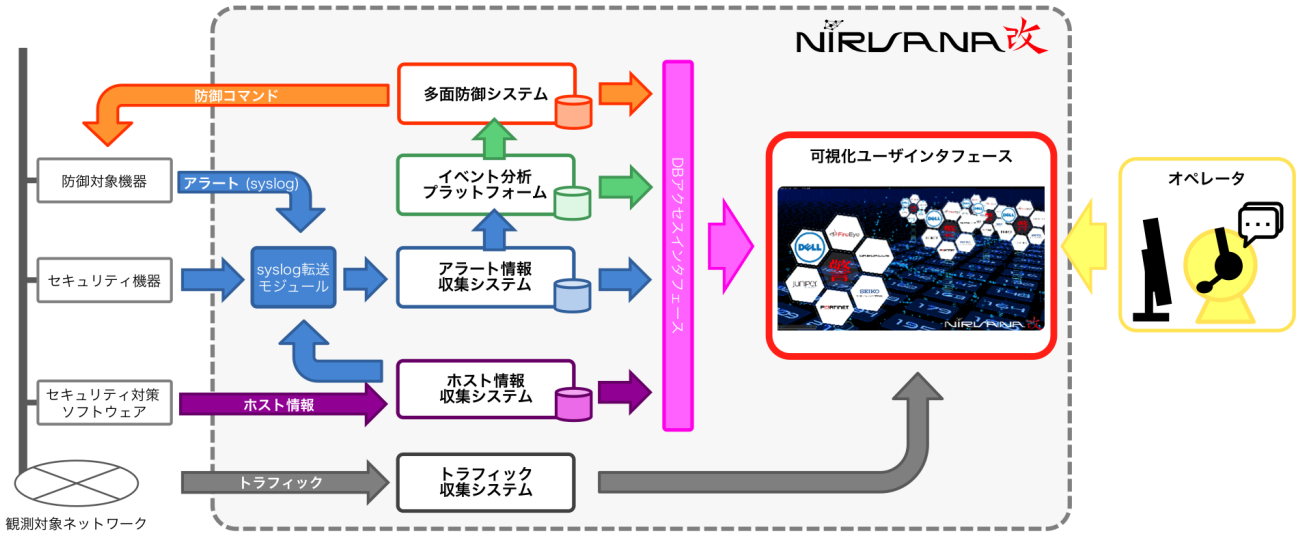

図 3　NIRVANA 改のシステム構成

フェース以外にも、可視化に必要な情報の収集や分析などを実行する以下のコンポーネントがバックエンドで動作している。図 3 に NIRVANA 改のシステム構成を示す。

- トラフィック収集システム
- アラート情報収集システム
- ホスト情報収集システム
- イベント分析プラットフォーム
- 多面防御システム

それぞれのコンポーネントは独立して動作するように実装され、それぞれが持つデータベース（DB）に蓄積された情報を DB アクセスインタフェースを介して取得し、可視化する。これらのコンポーネントのうち、「トラフィック収集システム」は NIRVANA の主機能として既に実装されていたものである。本稿では NIRVANA 改で独自に追加されたコンポーネントである「アラート情報収集システム」、「ホスト情報収集システム」、「イベント分析プラットフォーム」、「多面防御システム」について次節以降で説明する。

3.2　アラート情報収集システム

NIRVANA 改で収集する情報のひとつとして、組織内に導入された機器による攻撃検知情報や、セキュリティ対策ソフトウェアによるマルウェア検知情報といった「アラート情報」がある。NIRVANA 改の「アラート情報収集システム」では、機器のログメッセージを転送するときに標準的に利用される syslog を対象に収集する。

図 4 にアラート情報収集システムの概要を示す。syslog によるログメッセージは機器ごとに異なるフォーマットであるため、受信した syslog のログメッセージを NIRVANA 改で扱えるように整形する必要

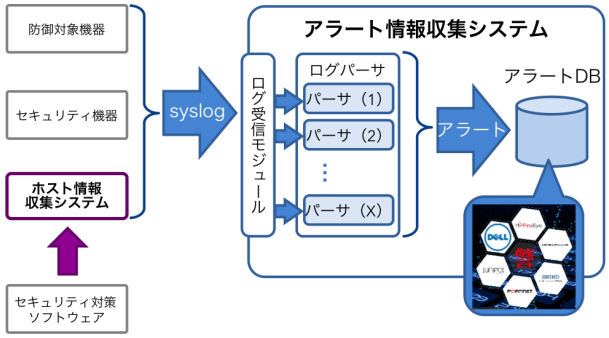

図 4　アラート情報収集システムの概要

がある。まず、syslog で送信されたログメッセージはログ受信モジュールで全て受け取る。ログ受信モジュールは syslog の送信元 IP アドレスを基にログメッセージを機器ごとに振り分け、その機器のログメッセージを整形するためのログパーサを呼び出す。ログパーサでは正規表現を用いて、通信プロトコルや送信元／あて先 IP アドレス、ポート番号、アラートの内容、重大度、発生時刻などのデータを抽出する。そして、抽出されたデータはデータベース（アラート DB）に格納されていく。アラート DB に蓄積された一つひとつのデータは、可視化ユーザインタフェース上で花形のオブジェクトの花びら部分として表示される。

一方で、組織内でのネットワーク管理やセキュリティオペレーションなどの運用を考慮すると syslog のログメッセージを NIRVANA 改以外の機器やサーバに送信したい要求もある。このような場合には、NIRVANA 改の機能の一部として実装されている「syslog 転送モジュール」によって用途に合わせた syslog の転送方法を実現できる。syslog 転送モジュールでは、図 5 に示すような「(1) 複製」、「(2) マルチキャスト」、「(3) ラウンドロビン」の 3 種類の転送方法が実

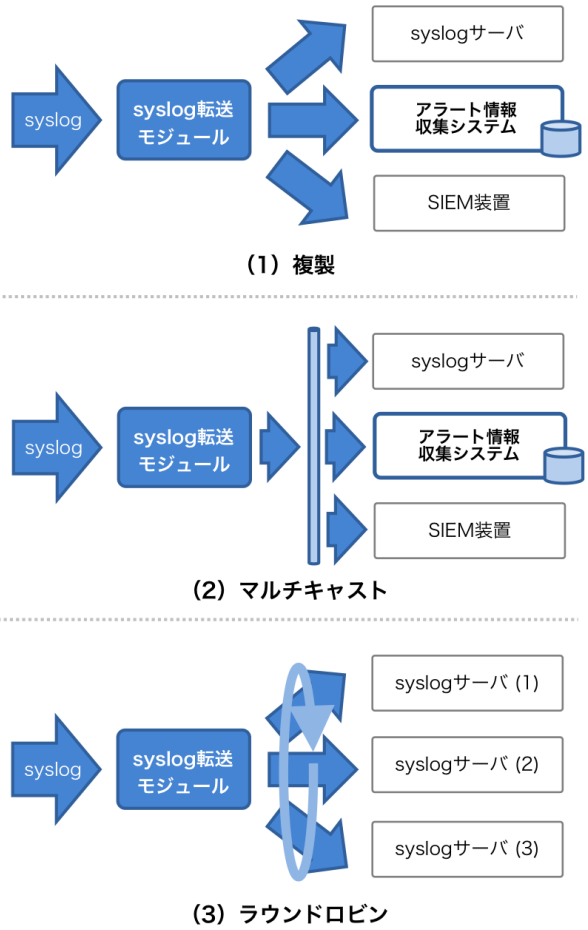

図 5　syslog 転送モジュールの機能

装されている。

これらの転送方法に加え、ログメッセージを任意の文字列でフィルタする機能も備えている。これらの機能を用いると、たとえば、全ログメッセージを syslog サーバへ転送しディスク上に保存し、重大度の高いログメッセージのみをフィルタして NIRVANA 改上で可視化するといった構成を実現できる。

3.3　ホスト情報収集システム

アラート情報以外にも、NIRVANA 改ではホスト内部の情報も収集する。図 6 に「ホスト情報収集システム」[4] [5] の概要を示す。ホストから各種情報を収集するために、セキュリティ対策ソフトウェアと連携したエージェントツールをホストに事前に導入する。このエージェントツールは、セキュリティ対策ソフトウェアによってマルウェアが検知されたときに「ホスト情報収集モジュール」に対してマルウェアと判定されたプロセスと検出理由を通知する。この他に、エージェントツールは OS の種類やバージョン情報やユーザ情報、MAC アドレスといったホストの基本情報や実行中のプロセスの情報、プロセスが発生させる通信の情報をホスト情報収集モジュールへ一定の時間間隔

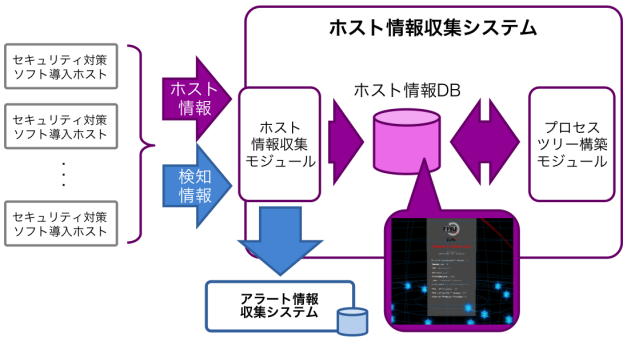

図 6　ホスト情報収集システムの概要

で送信する。その後、マルウェアの検知情報は syslog でアラート情報収集システムへ送信され、その他の情報はデータベース（ホスト情報 DB）へ格納される。

「プロセスツリー構築モジュール」は、ホスト情報 DB に蓄積されたプロセス情報のうち、プロセス ID（PID）や親プロセス ID（PPID）を基にプロセスツリーを構築する。ホスト情報 DB に蓄積されたホストの基本情報やプロセスツリーは「ホストビュー」で可視化される。図 7 にその様子を示す。ホストビューの中央部に位置する石版状のオブジェクト（モノリス）の表面には、このホストの基本情報が記載されている。モノリスを衛星のような軌道で周回しているオブジェクトはホスト内で現在実行されているプロセスを表し、その軌道の半径はプロセスの世代を表している。最も外側を周回しているプロセスでハイライトされているものはマルウェアとして検出されたものである。

プロセスをクリックすると図中のようにプロセスの親子関係が表示され、そのプロセスが生成された経緯を知ることができる。また、マルウェアから外部のネットワークに対しての TCP セッションが確立されている様子も可視化される。この場合、外部ネットワークのとあるホストが C&C（Command & Control）サーバと呼ばれるもので、マルウェアに感染しているこのホストと HTTP 通信で攻撃の命令をやり取りしている。

3.4　イベント分析プラットフォーム

前節までに NIRVANA 改で収集できる情報について述べた。一方で、組織内に導入されたネットワーク機器やセキュリティ機器、動作している PC の規模が大きくなるとアラート情報は増大することが予想され、重大なアラート情報を見逃す要因にもなり得る。そのため、NIRVANA 改では収集したアラート情報を分析し、セキュリティオペレータが対処すべき重大な事柄（イベント）を抽出するための「イベント分析プラットフォーム」[6] が備えられている。図 8 にイベント分析プラットフォームの概要を示す。イベント分析プラットフォームでは、アラート DB に蓄えられた情報

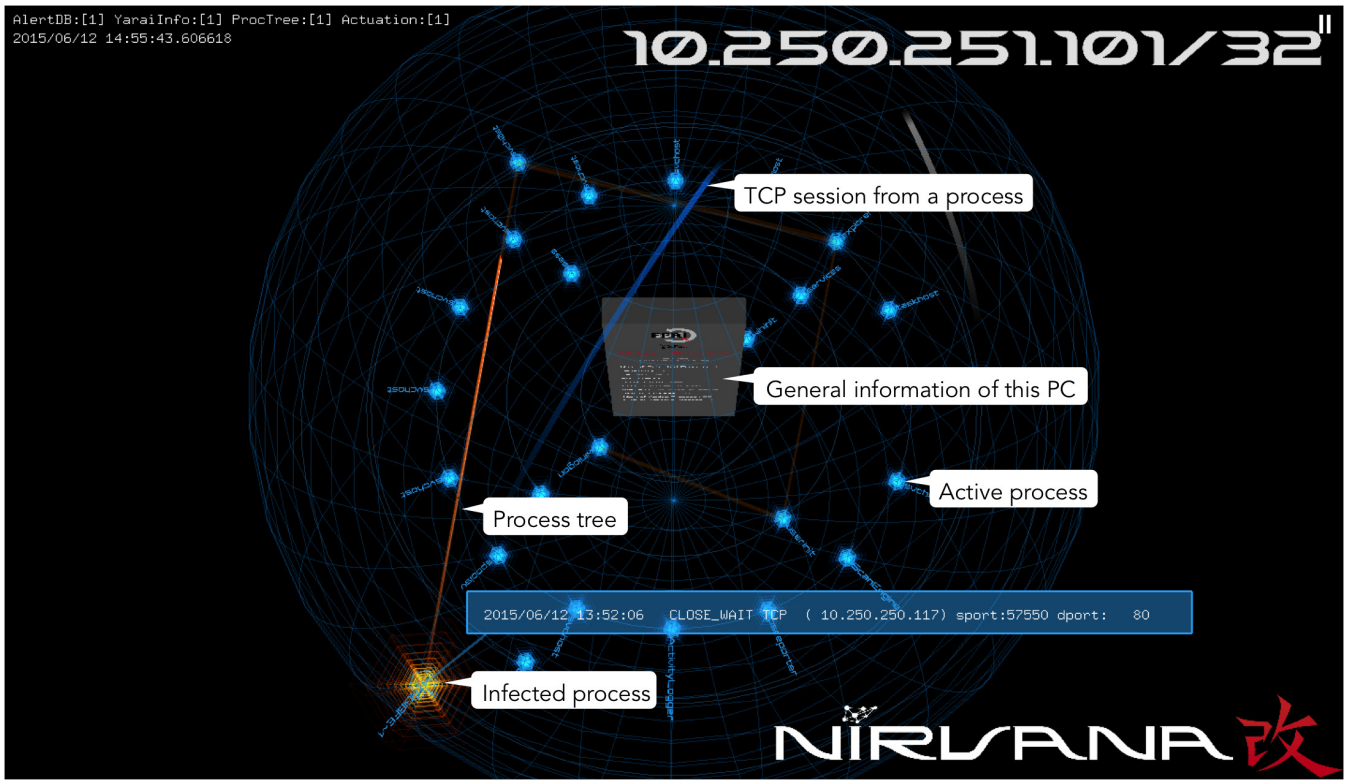

図 7　ホストビュー

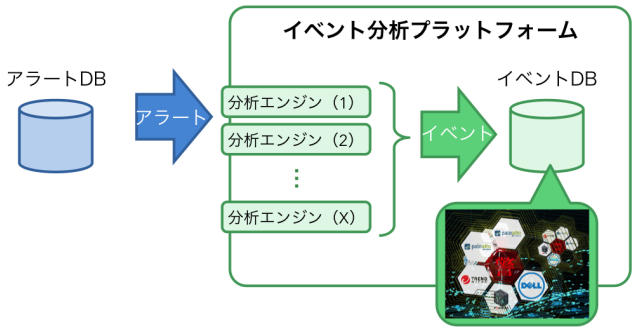

図 8　イベント分析プラットフォームの概要

を分析する「分析エンジン」を容易に実装できる機構を有し、セキュリティオペレータは独自に分析エンジンを追加できる。イベント分析プラットフォームは分析エンジンを記述、動作させるために以下の機構を持つ。

- 分析エンジン実装のためのプラグイン（分析プラグイン）機構
- 分析プラグイン実装のためのテンプレート
- 分析エンジンを記述するためのドメイン特化言語（DSL）

新たな分析エンジンを記述する際には、DSL を記述し複数の分析プラグインを連結する。分析プラグインの種別には、データを入力する input プラグインとデータを加工する filter プラグイン、データを出力する output プラグインがある。イベント分析プラットフォームには表 1 の組み込み分析プラグインがある。分析プラグインはその入出力のフォーマットが規定されており、新たな分析プラグインが必要な場合は用意されたテンプレートに従うことで実装できる。

表 1　イベント分析プラットフォームの組み込み分析プラグイン

種別	分析プラグイン	概要
input	database	MySQL，PostgreSQL，SQLite から入力
	csv	CSV ファイルから入力
	yaml	YAML ファイルから入力
	json	JSON ファイルから入力
filter	match	条件一致
	sort	並べ替え
	group_by	グループ化
	unique	重複排除と数え上げ
	truncate	閾値以下を切り捨て
output	database	MySQL，PostgreSQL，SQLite へ出力
	csv	CSV ファイルへ出力
	yaml	YAML ファイルへ出力
	json	JSON ファイルへ出力
	stdout	標準出力

分析エンジンから抽出されたイベント情報はデータベース（イベント DB）に格納される。可視化ユーザイ

図 9　イベント情報の強調表示

ンタフェース上では、イベント情報はアラート情報である花形のオブジェクトにエフェクトの形で表現される。図 9 はイベント情報を強調表示している様子である。花形のオブジェクトの周囲から発せられた音波がそのアドレスブロックでイベントが発生していることを示している。

3.5　多面防御システム

分析結果から得られたイベントに対して、NIRVANA 改では様々な防御策を講じることができる。図 10 に NIRVANA 改で防御の役割を担う「多面防御システム」の概要を示す。先述の分析エンジンから得られたイベント情報を対象にして、設定された「対

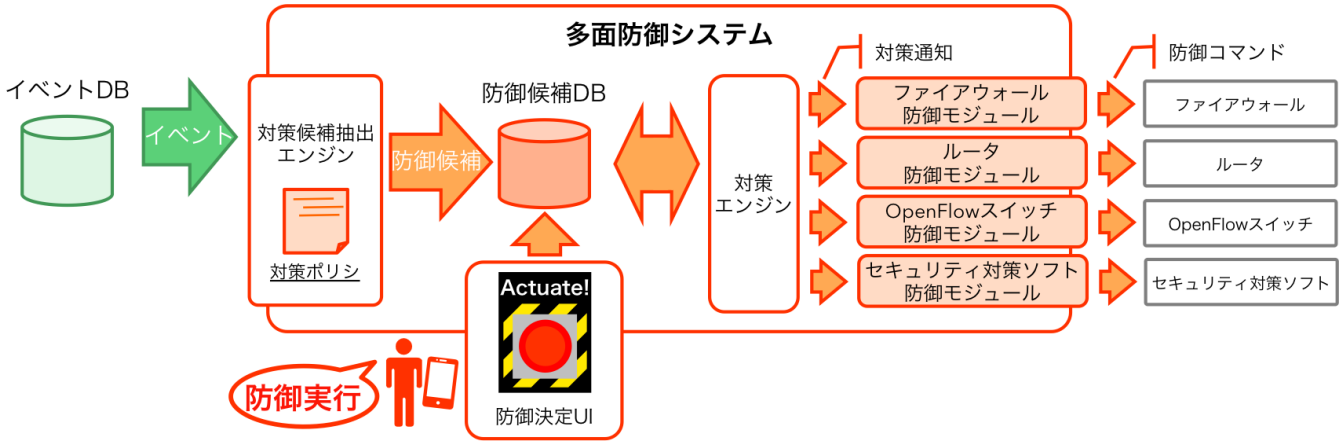

図 10　多面防御システムの概要

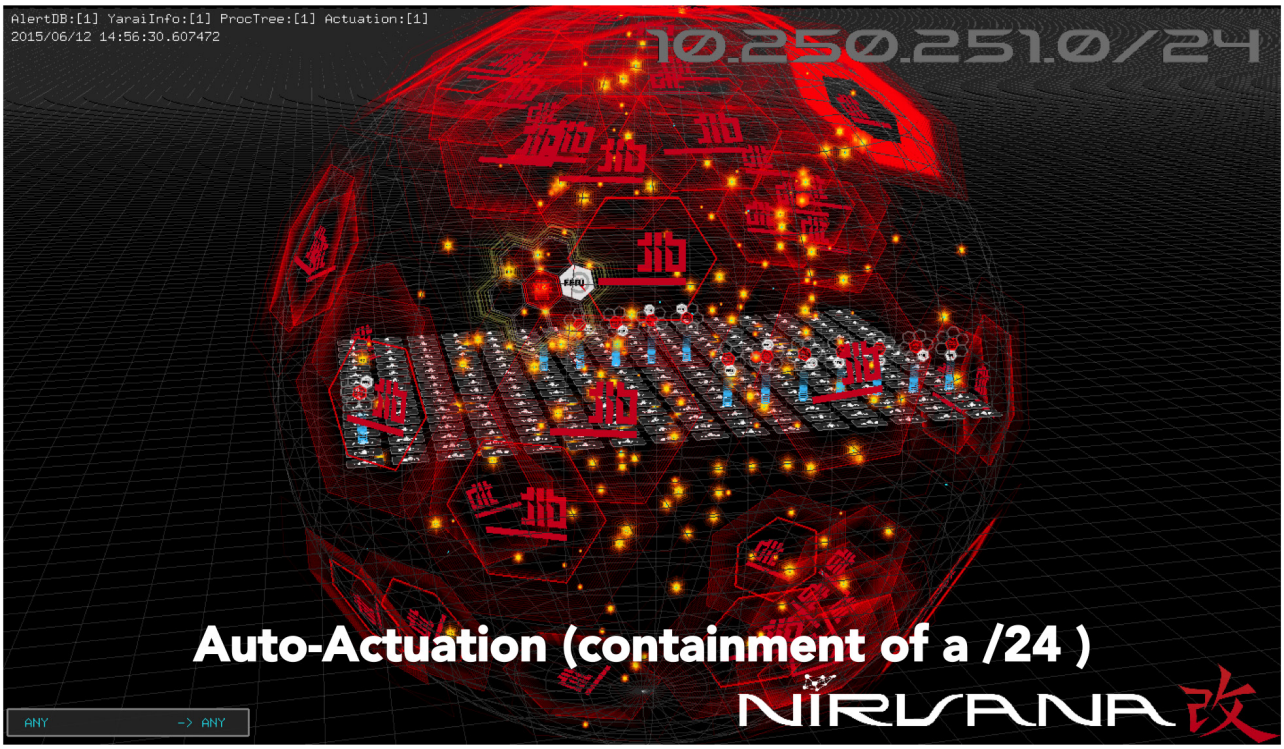

図 11　クラス C アドレスを隔離した様子

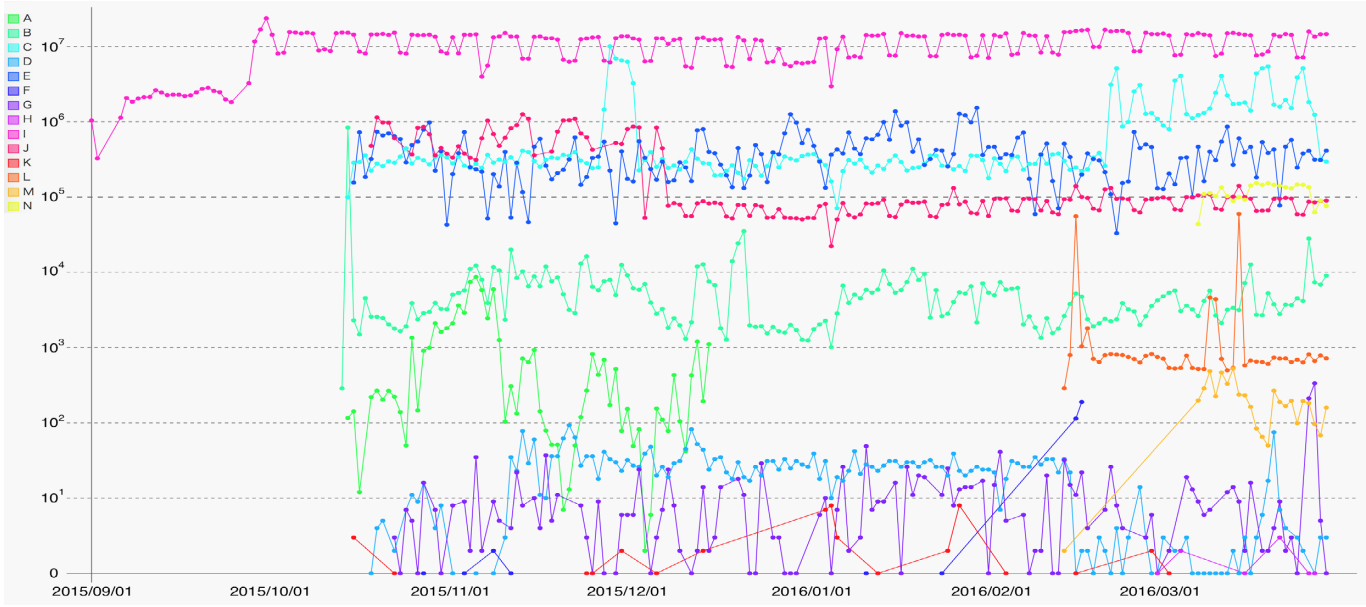

図 12　2015/09/01 から 2016/03/31 までの機器別アラート数

策ポリシ」を適用することで対策候補を抽出する。対策ポリシは任意のプログラミング言語で記述でき、抽出した対策候補とそれに対する防御策を設定しデータベース（防御候補 DB）に格納する。ネットワーク管理者は、防御決定ユーザインタフェース（防御決定 UI）を介して防御策を講じるべきものを選択する。そうすると、「対策エンジン」は設定された防御策を「防御モジュール」に通知し、実際に防御対象機器に防御コマンドが送信される。防御モジュールは適宜追加可能で、NETCONF や REST API といった防御対象機器が備えるプロトコルやインタフェースに合わせて任意のプログラミング言語で防御コマンドを記述すればよい。

また、防御実施中はその状態が NIRVANA 改上で可視化される。防御策の可視化の一例として、図 11 にファイアウォールを用いてクラス C アドレスを隔離している様子を示す。この場合は、当該ネットワーク内でマルウェアの大量感染を確認した場合にファイアウォールへ防御コマンドを送信するように対策ポリシが予め設定されており、挙がってきた防御候補に対してネットワーク管理者が防御決定の判断を下している。この例以外にも、NIRVANA 改では特定のホストをあて先とした通信の遮断や、任意のネットワークの複数ホストに対してセキュリティ対策ソフトウェアを用いたマルウェアのスキャンを一斉に実行させることができ、その様子を可視化できる。

4　NIRVANA 改を活用したセキュリティオペレーション

前章では、NIRVANA 改を用いた情報の収集、分析、

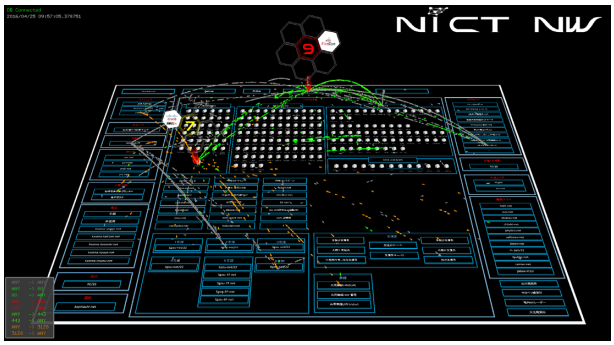

図 13　NICT 内のネットワークに適用した様子

防御の実行の一連の流れとその役割を担う各コンポーネントの概要を述べた。これまでに紹介した NIRVANA 改の各コンポーネントは、日々の NICT 内のセキュリティオペレーションに活用され、実際の運用に即した改善点がフィードバックとして得られている。

NICT では、2015 年 9 月頃からアラート情報を収集する機器を順次拡大し、2016 年 3 月 31 日現在では 14 機器・ソフトウェアを対象とした監視が行われている。図 12 はその期間中の機器別アラート数で、機器・ソフトウェアごとに大きく異なるアラート数やその種類の中から対処すべきものを迅速に発見しなければならない。図 13 は実際の運用の中から挙がったフィードバックを基に開発された可視化ユーザインタフェースの例である。背景に各種機器と地理的な所在が記された画像を設定し、アラートの重大度がひと目で判別できるように花形のオブジェクトの中心に数値と色で可視化している。

より実践的なセキュリティオペレーションの実現に

は、実際の運用に組み込むことは必要不可欠であると考える。これからもNIRVANA改の実運用を重ねていくことで実用面での機能改善を重ね、可視化技術を中心とした実践的なセキュリティオペレーションを確立することが今後の大きな課題となっている。

5　おわりに

本稿では、標的型攻撃に対抗する技術として、サイバー攻撃対策統合分析プラットフォームNIRVANA改のシステム構成とNICTにおける適用事例について述べた。NIRVANA改を用いることで組織内において発生する通信やアラートを集約､分析でき､セキュリティオペレーションに必要となる情報を可視化できる。

標的型攻撃に対する効率的かつ効果的なセキュリティオペレーションには、組織内の状況の変化を迅速にとらえることが要求される。今後はNICT内外でのセキュリティオペレーションを通じて実用面での機能改善を重ね、可視化技術を用いたより実践的なセキュリティオペレーションを確立すべく研究開発に取り組んでいく予定である。

【参考文献】

1　D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka and K. Nakao, “nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis,” WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS '08), pp.58–66, 2008.

2　衛藤将史，高木彌一郎，“インシデント分析センター nicter のシステム実装と社会展開，”情報通信研究機構季報，vol.57, no.3/4, pp.17–26, 2011.

3　鈴木宏栄，衛藤将史，井上大介，“実ネットワークトラフィック可視化システム NIRVANA の開発と評価，”情報通信研究機構季報，vol.57, no.3/4, pp.63–80, 2011.

4　中里純二，津田侑，衛藤将史，井上大介，中尾康二，“プロセスの出現頻度を用いた不審プロセス特定，”電子情報通信学会技術研究報告，vol.115, no.334, pp.61–66, 2015.

5　中里純二，津田侑，衛藤将史，井上大介，中尾康二，“プロセスの出現頻度や通信状態に着目した不審プロセス判定，”電子情報通信学会技術研究報告，vol.115, no.488, pp.77–82, 2016.

6　津田侑，遠峰隆史，神薗雅紀，衛藤将史，井上大介，“プラガブルかつプログラマブルなログ分析フレームワーク，”電子情報通信学会技術研究報告，vol.114, no.489, pp.31–36, 2015.

津田　侑　（つだ　ゆう）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
博士（情報学）
サイバーセキュリティ、標的型攻撃対策

金谷延幸　（かなや　のぶゆき）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
専門研究員
サイバーセキュリティ、web セキュリティ

遠峰隆史　（とおみね　たかし）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究技術員
サイバーセキュリティ、ネットワーク運用管理

神薗雅紀　（かみぞの　まさき）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
協力研究員
サイバーセキュリティ

神宮真人　（じんぐう　まさと）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
専門研究員
サイバーセキュリティ、インシデントレスポンス

高木彌一郎　（たかぎ　やいちろう）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究技術員
ネットワークセキュリティ

鈴木宏栄　（すずき　こうえい）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
主任研究技術員
ネットワークセキュリティ