国立研究開発法人
情報通信研究機構

プレスリリース
2021 年 4 月 12 日
国立研究開発法人情報通信研究機構

サイバー攻撃統合分析プラットフォーム“NIRVANA 改”が IPv6 に対応

～世界初！IPv6 の膨大なアドレス空間を流れるパケットのリアルタイム可視化に成功～

【ポイント】

- サイバー攻撃統合分析プラットフォーム“NIRVANA 改”が新たに IPv6 に対応、機能強化
- IPv6 通信の観測、IPv6 関連アラートの収集、IPv6 ネットワークのリアルタイム可視化を実現
- IPv6 ネットワークにおけるセキュリティオペレーションの簡易化に期待

国立研究開発法人情報通信研究機構（NICT、理事長: 徳田 英幸）サイバーセキュリティ研究室は、サイバー攻撃統合分析プラットフォーム「NIRVANA 改[*1]」（ニルヴァーナ・カイ）を機能強化し、インターネットの通信プロトコル IPv4 の後継規格である IPv6 への対応を完了しました。今回、IPv6 の膨大なアドレス空間を流れるパケットのリアルタイム可視化に世界で初めて成功しました。これまで NIRVANA 改は、IPv4 通信のみを観測・分析の対象にしていましたが、新たに IPv6 通信に対応することで、より多様で広範なネットワークのセキュリティ対策に役立てられることが期待できます。

IPv6 に対応した NIRVANA 改は、2021 年 4 月 14 日（水）～16 日（金）に幕張メッセで開催される「Interop Tokyo 2021」（https://www.interop.jp/）で動態展示を行います。

【背景】

インターネットの通信方法を定めた通信プロトコルとして IPv4 が 1981 年に規格が制定されて以来使われてきましたが、その後継規格である IPv6 の普及が急速に進んでいます[*2]。IPv4 では地球の人口よりも少ない約 43 億（2 の 32 乗）個[*3] の IP アドレスしか扱えませんでしたが、IPv6 では約 340 澗（2 の 128 乗）個[*4] という膨大な数の IP アドレスを扱うことができます。

NICT がこれまで研究開発を進めてきたサイバー攻撃統合分析プラットフォーム「NIRVANA 改」は IPv4 のみに対応しており、膨大な IP アドレスを有する IPv6 への対応が課題でした。

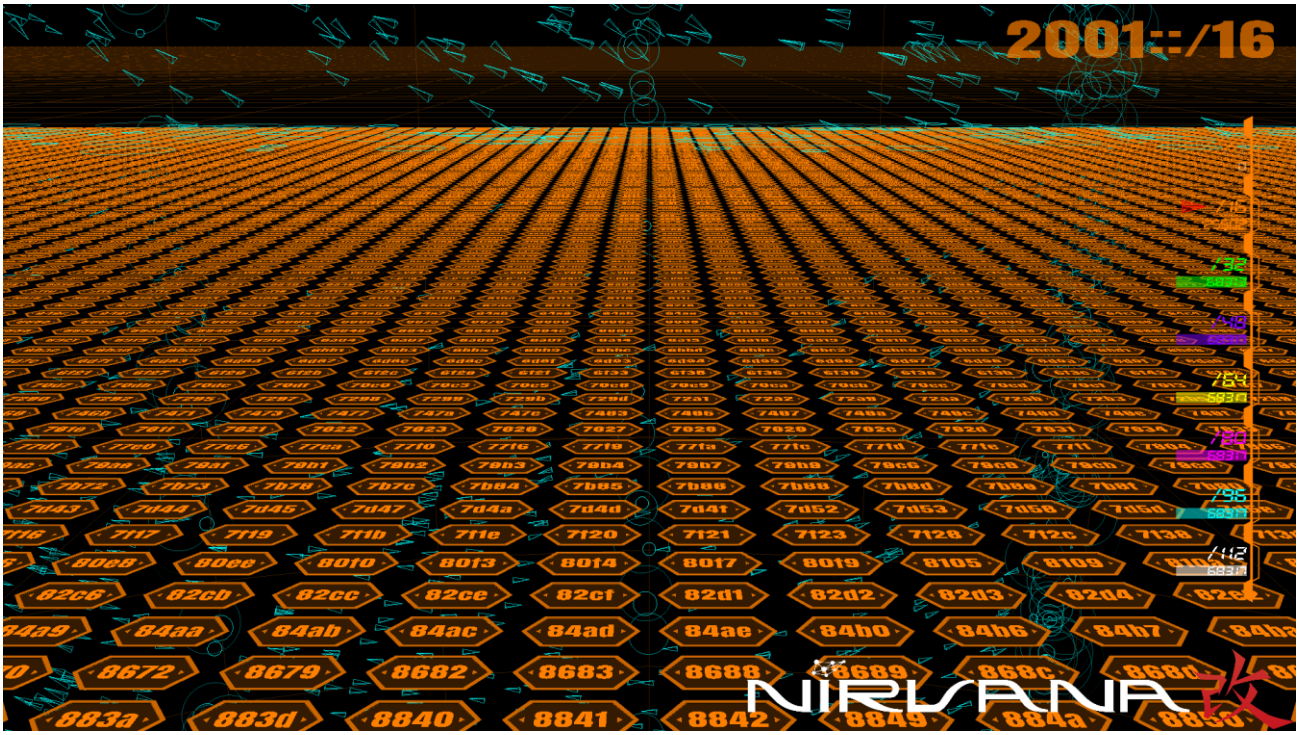


図 1 IPv6 対応版 NIRVANA 改による IPv6 空間の可視化

縦横に並んでいるオレンジ色の各パネルは、IPv6 による通信が観測されたアクティブな IP アドレスブロックを示している（この図では /16）。水色の三角錐のオブジェクトは IPv6 パケットを表しており、1 パケットごとのリアルタイム表示や、IP アドレス/ポート番号でのフィルタリング等の柔軟な可視化設定が可能。

【今回の成果】

NIRVANA 改を機能強化し、システム各部（通信観測部、アラート収集部、可視化部、等）が IPv6 に対応しました。特に可視化部では、通信が観測されたアクティブな IP アドレスブロックを動的に逐次追加していくことで、膨大な IPv6 のアドレス空間を効率的に可視化することに成功しました（図 1～4 参照）。また、IPv6 のアドレス空間の階層構造[*5]における現在位置の視認性を上げるため、インディケータを新たに実装しました（図 2 右端参照）。さらに、セキュリティ機器から発報された IPv6 関連のアラート情報にも対応し、IPv6 アドレスによるフィルタリング等も可能になりました（図 2 参照）。

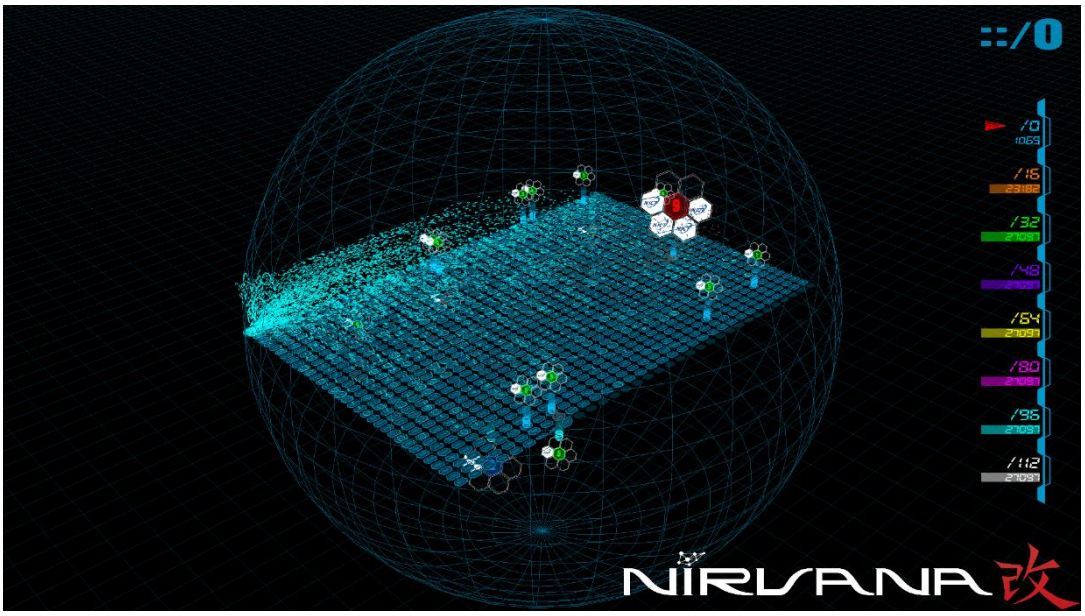


図 2 IPv6 アドレス空間の全景とインディケータ

中央のパネル群は IPv6 のアドレス空間の全景（/0）であり、六角形のアイコンはセキュリティ機器から発報されたアラートを示している。画面右端のインディケータは IPv6 空間の階層構造における現在位置（赤矢印）と、各階層に含まれるアドレスブロック数を示している。

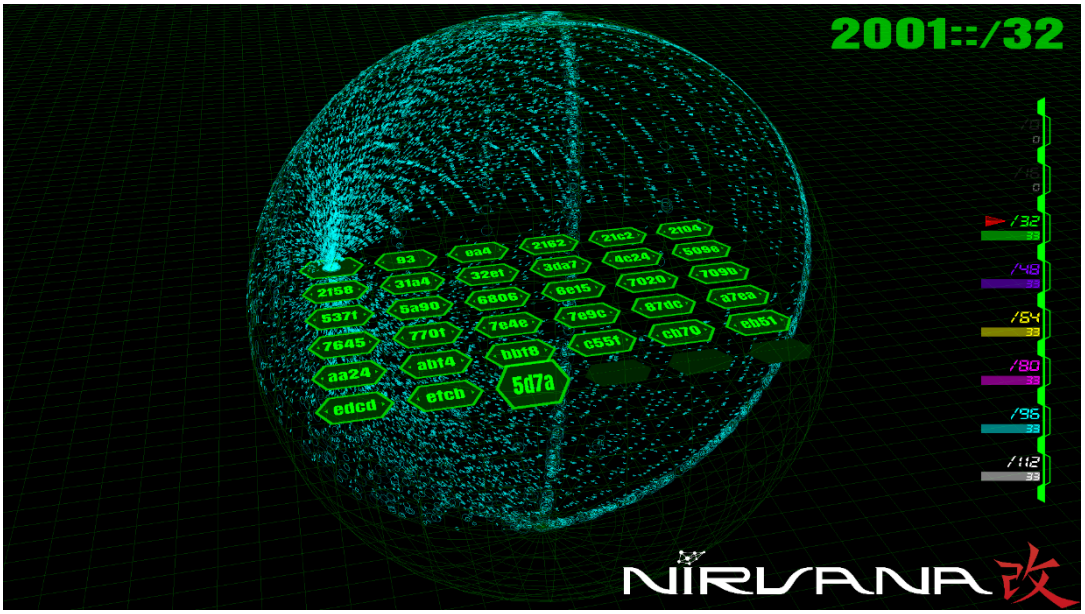


図 3 IP アドレスブロックの動的追加

あるセグメントの中で新たな IP アドレスからの通信が観測されると、そのアドレスを含む IP アドレスブロックが動的に追加される。この図では 2001:0:5d7a::/48 のパネルが回転モーションと共に追加されている。なお、追加されたパネルは自動でソートすることも可能。

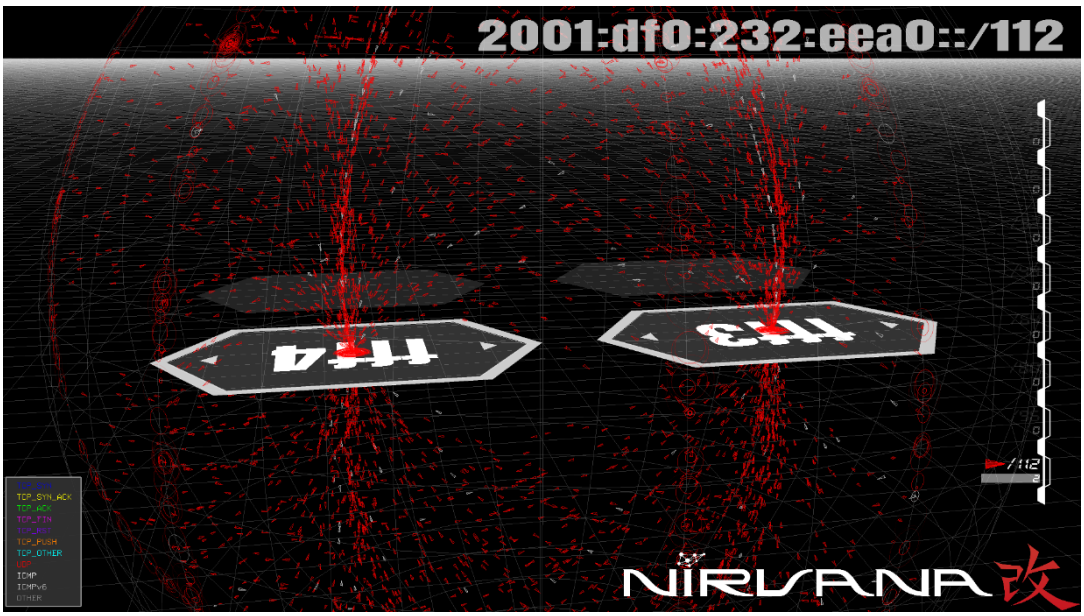


図 4 NICT の時刻サーバの IPv6 通信

NICT が運用している時刻サーバ（ntp.nict.jp）における IPv6 通信を可視化したものである。広範な送信元 IP アドレスから大量の UDP（赤）パケットが 2 つの IPv6 アドレスに去来している様子が分かる。

【今後の展望】

NIRVANA 改が IPv6 通信に対応したことによって、システムの適用範囲が大きく広がり、IPv6 ネットワークにおけるセキュリティオペレーションの簡易化が期待できます。

IPv6 に対応した NIRVANA 改は、既に民間企業への技術移転が進められています。また、2021 年 4 月 14 日（水）～16 日（金）に幕張メッセで開催される「Interop Tokyo 2021」（https://www.interop.jp/）で動態展示を行います。

＜ 本件に関する問合せ先 ＞
国立研究開発法人情報通信研究機構
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
井上 大介、鈴木 宏栄、平田 真由美
Tel: 042-327-6225
E-mail: nicter@ml.nict.go.jp

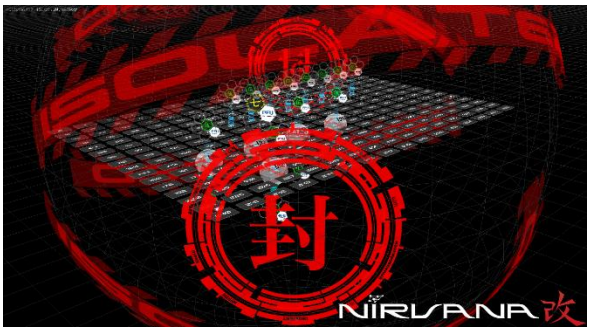
＜ 広報 （取材受付） ＞
広報部 報道室
Tel: 042-327-6923
E-mail: publicity@nict.go.jp

＜用語解説＞

***1 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）**

NIRVANA 改は、組織内の各種セキュリティ機器が発報するアラートを集約・分類・相関分析することで、アラートのトリアージ（優先順位付け）や、異常な通信を遮断するアクチュエーション（自動対処）等を可能にするサイバー攻撃統合分析プラットフォーム

報道発表「NIRVANA 改が更にバージョンアップ！」
2016 年 6 月 7 日
https://www.nict.go.jp/press/2016/06/07-1.html



NIRVANA 改

***2 IPv6 の普及状況**

IPv6 普及・高度化推進協議会「日本における IPv6 の普及状況」
https://v6pc.jp/jp/spread/ipv6spread_03.phtml

***3 IPv4 における IP アドレス数**

2^{32} = 4,294,967,296（約 43 億）

***4 IPv6 における IP アドレス数**

2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456（約 340 澗）
澗（かん）は、10 の 36 乗を示す。

***5 IPv6 のアドレス空間の階層構造**

/0, /16, /32, /48, /64, /80, /96, /112 の 8 階層