

サイバー攻撃統合分析プラットフォーム NIRVANA 改

サイバーセキュリティ研究所

概要

- リアルタイムに可視化された組織内ネットワークの中から、サイバー攻撃に関連した異常な通信を検知し、その通信の送信元の直上にアラートを表示します。
- 組織内ネットワークは、アドレスブロック単位から IP アドレス単位の表示まで柔軟に変更可能であり、シームレスなドリルダウンが可能です。
- ファイアウォールや侵入検知システムなど、各種セキュリティ検知・防御システムからのアラートも可視化でき、統合的な分析プラットフォームとして機能します。

知財・関連情報

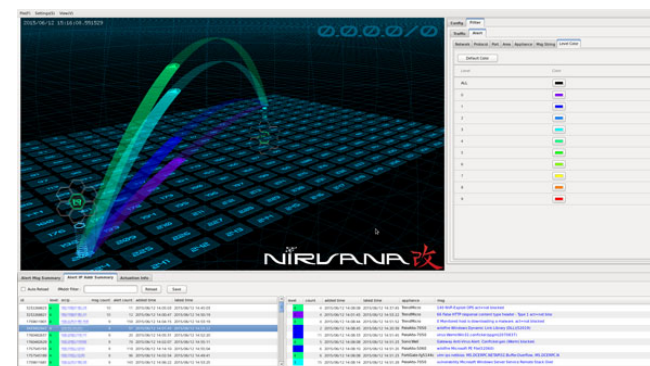
- (1) サイバー攻撃統合分析プラットフォーム NIRVANA 改用センサプログラム
- (2) サイバー攻撃統合分析プラットフォーム NIRVANA 改用ゲートプログラム
- (3) サイバー攻撃統合分析プラットフォーム NIRVANA 改用可視化プログラム
- (4) サイバー攻撃統合分析プラットフォーム NIRVANA 改用アラート情報収集プログラム

報道発表

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 2013 年 6 月 10 日

NIRVANA 改が更にバージョンアップ 2016 年 6 月 7 日

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 2021 年 4 月 12 日



図：（アラート管理画面）画面下部にアラート一覧やアラートの発生源となった IP アドレス一覧等を表示。左下部で IP アドレスを選択すると、その IP アドレスに関連したアラートが右下部に表示される。左上の可視化画面には各アラートの原因となった通信履歴が連動表示される。