国立研究開発法人
情報通信研究機構

プレスリリース
2019年6月6日
国立研究開発法人情報通信研究機構

セキュリティ情報融合基盤“CURE”を開発
～サイバーセキュリティ関連情報の大規模集約・横断分析を実現～

【ポイント】

- サイバーセキュリティ関連情報を大規模集約・横断分析する「CURE」を開発
- 散在する多種多様な情報を自動的につなぎ合わせ、サイバー攻撃の隠れた構造を解明
- 自組織内のアラートと外部の脅威情報とを関連付け、組織のセキュリティ・オペレーションを効率化

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、多種多様なサイバーセキュリティ関連情報を大規模集約・横断分析するセキュリティ情報融合基盤「CURE」（キュア）を開発しました。CURE は、サイバー攻撃の観測情報や脅威情報等、異なる情報源から得られるサイバーセキュリティ関連情報を一元的に集約してつなぎ合わせることで、これまで把握が困難であったサイバー攻撃の隠れた構造を解明し、リアルタイムに可視化します。さらに CURE は、自組織内のアラートと外部の脅威情報とを関連付けることで、最新の脅威が組織に及ぼす影響について迅速な把握を可能にし、組織のセキュリティ・オペレーションの効率化が期待できます。

CURE については、2019年6月12日（水）～14日（金）に幕張メッセで開催される「Interop Tokyo 2019」で動態展示を行います。

【背景】

組織のセキュリティを向上するためには、自組織内で適切なセキュリティ対策を講じてサイバー攻撃の観測や分析を行うことが重要ですが、最近では外部組織から発信される脅威情報（threat intelligence）等を定常的に収集し、自組織のセキュリティ対策に活かすことも求められています。しかしながら、そのような組織内外の多種多様なサイバーセキュリティ関連情報を定常的に収集・分析することは高い人的コストを要するため、多くの組織では実現困難でした。

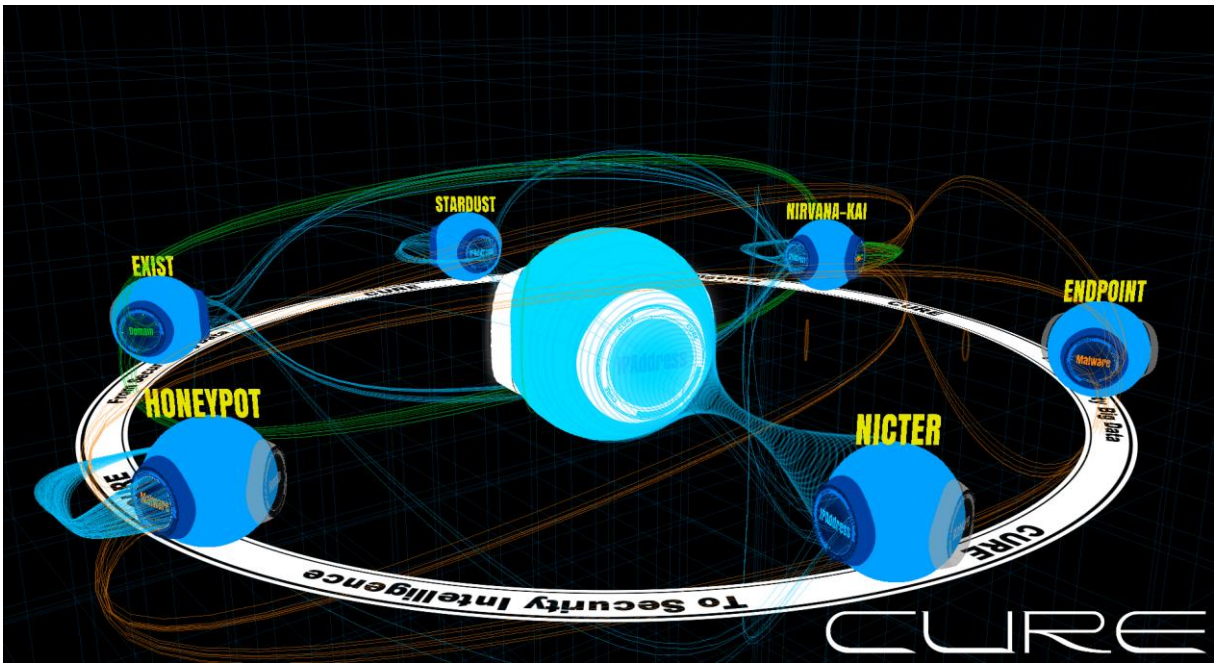


図1　CURE 全体図

中央水色の球体が CURE 本体、外周青色の球体は各種サイバーセキュリティ関連情報を保有するデータベース（DB）群。各 DB は CURE 本体に情報を送る際にリップルレーザを射出。CURE 本体では IP アドレス、ドメイン、マルウェアについて横断分析を行い、同一の情報が見つかると DB 間にリンクを描画（青: IP アドレス、緑: ドメイン、橙: マルウェア）

【今回の成果】

NICT はこれまで、無差別型攻撃の観測（インシデント分析センターNICTER[*1]）や標的型攻撃の観測（サイバー攻撃誘引基盤 STARDUST[*2]）、組織内のアラートやエンドポイント情報の収集（サイバー攻撃統合分析プラットフォーム NIRVANA 改[*3]）、様々な情報源からの脅威情報の取得（サイバー脅威情報集約システム EXIST[*4]）等、多種多様なサイバーセキュリティ関連情報の収集を行ってきました。

今回、NICT が開発した「CURE」（キュア: Cybersecurity Universal REpository）は、これらサイバーセキュリティ関連情報を一元的に集約し、異種情報間の横断分析を可能にするセキュリティ情報融合基盤です。CURE によって、個別に散在していた情報同士を自動的につなぎ合わせることが可能となり、これまで把握が困難であったサイバー攻撃の隠れた構造の解明につながります。

さらに、CURE と NIRVANA 改とを連動させ、外部組織から発信される脅威情報と自組織内のアラートやエンドポイント情報とを関連付けることで、最新の脅威が組織に及ぼす影響について迅速な把握を可能にし、組織のセキュリティ・オペレーションの効率化が期待できます。

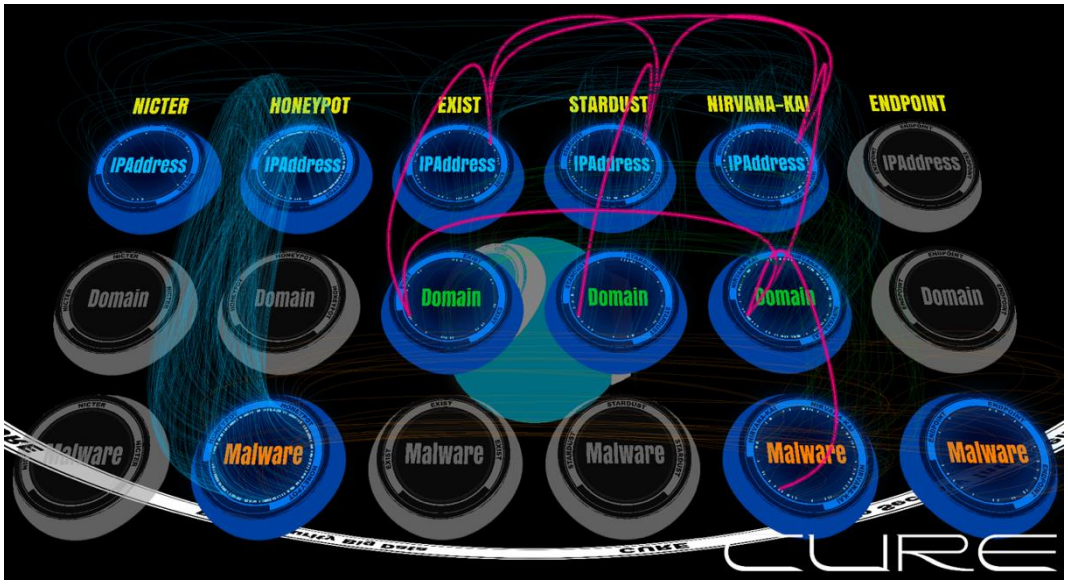


図 2　詳細情報表示

各 DB から CURE に送られた情報を種別ごとに詳細表示。複数の DB をまたぐ攻撃キャンペーンをハイライト表示

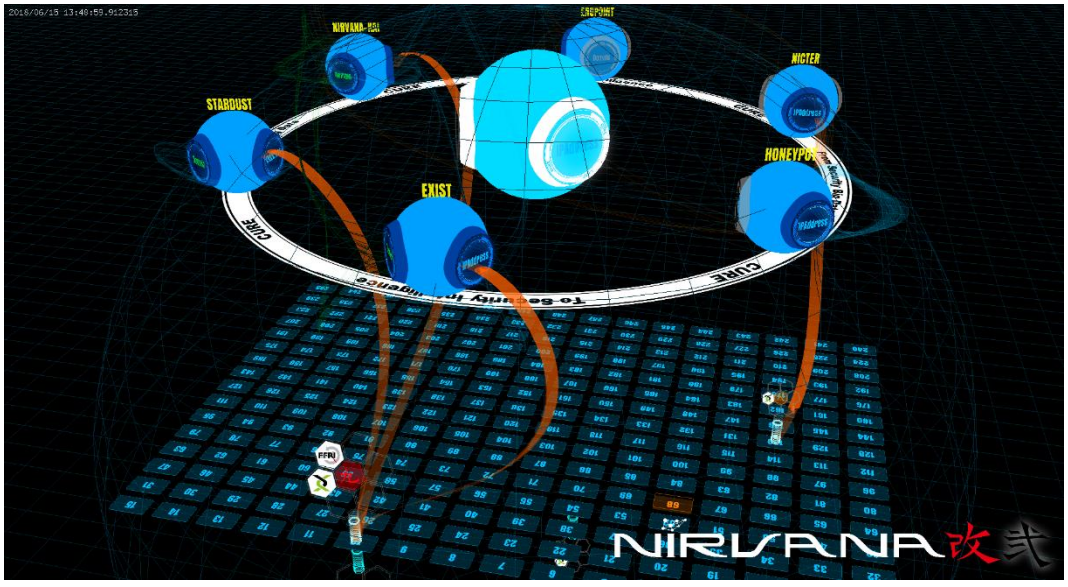


図 3　NIRVANA 改連携

CURE と NIRVANA 改が連動し、自組織内で発報したアラートと各種の脅威情報とを自動的に関連付け

【今後の展望】

CURE によって散在するセキュリティ・ビッグデータを統合し、日本のセキュリティ向上に資するセキュリティ・インテリジェンスの創出を目指します。また、CURE が集約したサイバーセキュリティ関連情報について、更に高度な分析技術の研究開発を推進していきます。

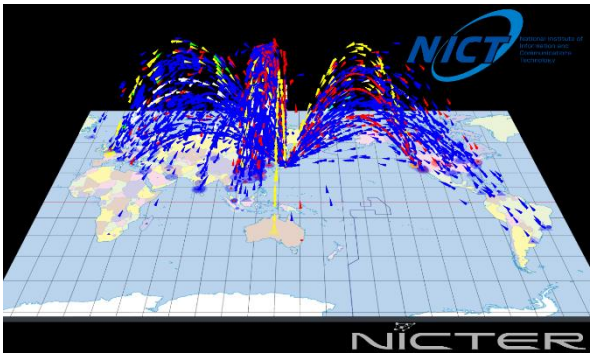
CURE については、2019 年 6 月 12 日（水）～14 日（金）に幕張メッセで開催される「Interop Tokyo 2019」で動態展示を行います。https://www.interop.jp/

＜用語解説＞

*1 **インシデント分析センター NICTER（ニクター）**

NICTER（Network Incident analysis Center for Tactical Emergency Response）は、インターネット上で発生する無差別型攻撃を迅速に把握し、有効な対策を導出するための複合的なシステム。ダークネット（未使用の IP アドレス空間）の大規模観測やマルウェアの収集・分析などによって得られた情報を相関分析し、その原因を究明する機能を持つ。

NICTERWEB
https://www.nicter.jp/

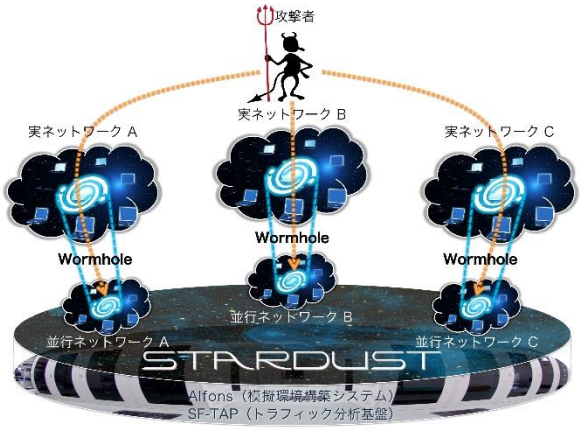


NICTER

*2 **サイバー攻撃誘引基盤 STARDUST（スターダスト）**

STARDUST は、標的型攻撃等の攻撃者の挙動を長期分析するための攻撃誘引基盤。攻撃者を外部から誘引するために、企業サイズの精巧な模擬環境“並行ネットワーク”を自動構築し、標的型攻撃に用いられるマルウェアを実行。模擬環境中でステルス性の高いリアルタイム観測・分析を可能にする。

報道発表「サイバー攻撃誘引基盤“STARDUST”（スターダスト）を開発」 2017 年 5 月 31 日
https://www.nict.go.jp/press/2017/05/31-1.html

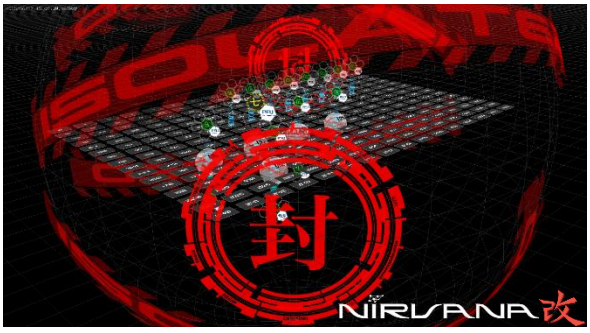


STARDUST

*3 **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

*4 **サイバー脅威情報集約システム EXIST（イグジスト）**

EXIST は、様々な情報源から公開あるいは有償提供されている脅威情報を自動収集し、解析者が WebUI もしくは WebAPI で横断的な検索を行うことを可能にする Web アプリケーション。オープンソースとして公開されている。

NICTER Blog「サイバー脅威情報集約システム EXIST」 2019 年 3 月 15 日
https://blog.nicter.jp/2019/03/exist/

補足資料

NICT サイバーセキュリティ研究室では、サイバー攻撃の観測の広さを横軸として、無差別型攻撃対策のための全域的観測から標的型攻撃対策のための局所的観測まで、また、観測の深さを縦軸として、受動的な観測から能動的な観測まで、サイバーセキュリティについて全方位の研究開発を行っています（図 4 参照）。それら研究開発の中心に位置するのが CURE です。

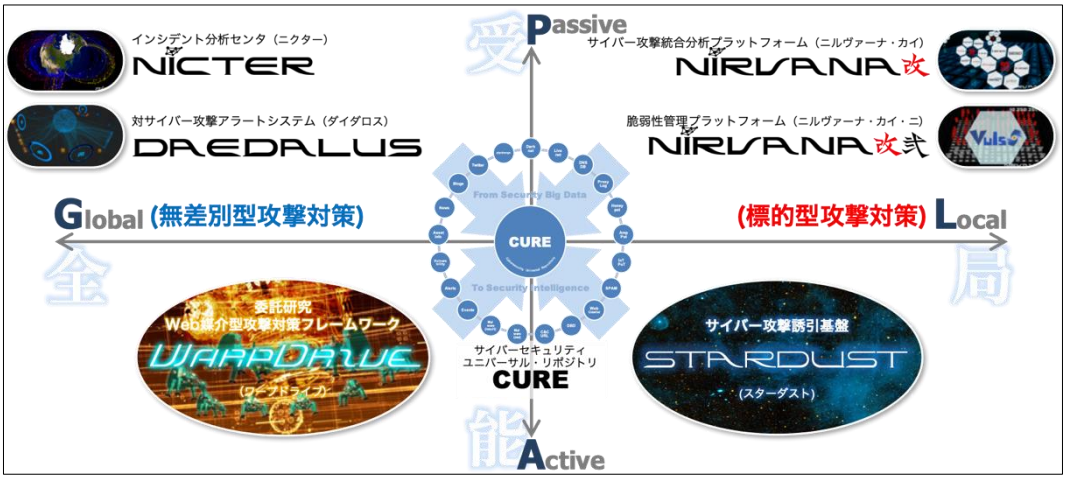


図 4　サイバーセキュリティ研究室 研究マップ

CURE は、サイバー攻撃対策に必要となる多種多様なサイバーセキュリティ関連情報（図 5 外周 参照）を一元的に集約し、横断分析を可能にするセキュリティ情報融合基盤です。CURE は、膨大な量の情報を高速に処理するため、インメモリデータベースを採用し、各種 DB と CURE 本体のメッセージングは Pub/Sub（Publish/Subscribe）モデルに基づいて実装されています。これにより、高速性と高いスケーラビリティを実現します。

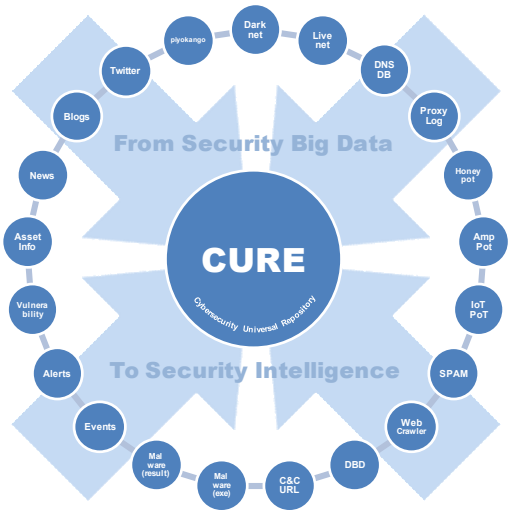


図 5　CURE 概念図

＜ 本件に関する問い合わせ先 ＞
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、津田 侑、鈴木 宏栄
Tel: 042-327-6225
E-mail: nicter@ml.nict.go.jp

＜ 広報 ＞
広報部 報道室
廣田 幸子
Tel: 042-327-6923
E-mail: publicity@nict.go.jp