国立研究開発法人
情報通信研究機構

プレスリリース
2020 年 10 月 27 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”を機能強化！

～自然言語で記述された分析情報を融合してセキュリティオペレーションを効率化～

【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」を機能強化
- サイバー攻撃を体系的に自然言語で記述した MITRE 社の ATT&CK などの分析情報を融合
- 外部分析情報と自組織観測情報を自然言語処理で関連付け、セキュリティオペレーション効率化

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するセキュリティ情報融合基盤「CURE[*1]」（キュア）を機能強化し、自然言語で記述された分析情報を融合、迅速に横断分析することに成功しました。これまでの CURE の機能に加え、今回、自然言語処理による関連付け機能を開発することで、米国の MITRE ATT&CK[*2]（マイター アタック）などの自然言語で記述された分析情報を CURE に融合し、横断分析ができるようになりました。これにより、外部の分析情報と自組織の観測情報とを柔軟に関連付けることが可能となり、セキュリティオペレーションの効率化が期待できます。

機能強化した CURE は、2020 年 10 月 28 日（水）～30 日（金）に幕張メッセで開催される「第 10 回 情報セキュリティ EXPO【秋】」で動態展示を行います。また、CURE の技術詳細については 2020 年 10 月 26 日（月）～29 日（木）にオンライン開催されるコンピュータセキュリティシンポジウム 2020（CSS2020）で発表しています。

【背景】

組織のセキュリティ向上のためには、自組織におけるサイバー攻撃の観測情報や、外部機関が公表した分析情報などの多種多様なサイバーセキュリティ関連情報を活用する必要があります。そこで、NICT はセキュリティ情報融合基盤「CURE」を開発し、サイバーセキュリティ関連情報の大規模集約と横断分析の研究を行ってきました。

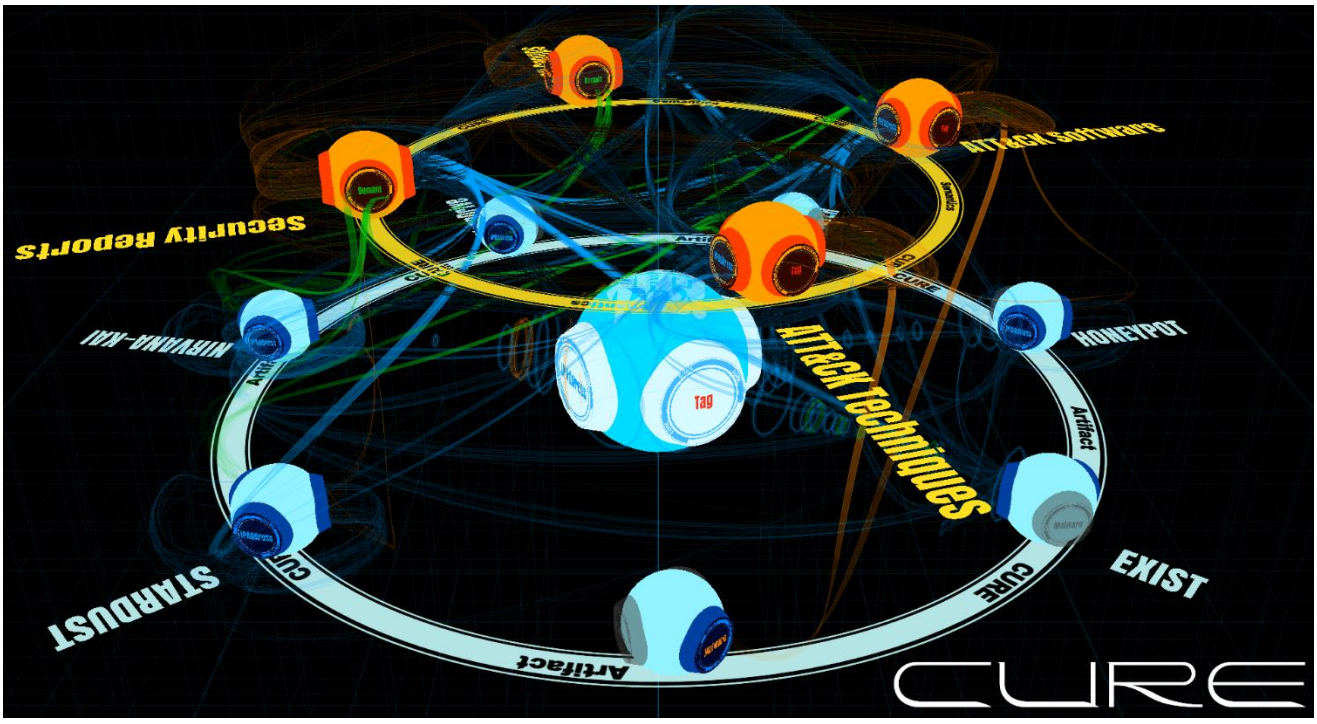


図 1 CURE 全体図

中央水色の球体が CURE 本体、外周青色と橙色の小球体はそれぞれ Artifact（観測情報）と Semantics（分析情報）を格納するデータベース群。CURE 本体では IP アドレス、ドメイン、マルウェア、自然言語のタグにより横断分析を行い、同一の情報が見つかるとデータベース間にリンクを描画（青：IP アドレス、緑：ドメイン、橙：マルウェア、赤：タグ）。

これまで CURE は、サイバー攻撃に使用された IP アドレス、ドメイン名、マルウェアのいずれかの情報が完全一致することで、異なる観測情報の間での関連付けを行っていましたが、セキュリティレポートなどの自然言語で記述された分析情報を、どのようにして統一的に取り扱うかが課題でした。

【今回の成果】

今回、CURE に自然言語処理の機能を加え、自然言語で記述された情報から重要な単語（タグ）を抽出し、タグを用いた異種情報の間での関連付けを可能にしました。これにより、各種のセキュリティレポートや、サイバー攻撃を体系的に記述する米国の MITRE ATT&CK などの自然言語で記述された分析情報を CURE のデータベースに融合し、横断分析ができるようになりました。

また、CURE の構造を Artifact（観測情報）レイヤと Semantics（分析情報）レイヤの 2 階層に分離し、自然言語のタグによって両レイヤ間の関連付けを可能にするとともに、2 階層モデルに対応した可視化機能を開発しました。

図 2 は、観測情報を格納する Artifact レイヤを示しています。

これまで CURE に集約してきたダークネット観測情報（NICTER[*3]）や、組織内のアラート情報（NIRVANA 改[*4]）のデータベースに加え、新たに Web 媒介型攻撃の観測情報（WarpDrive[*5]）を融合しました。

各種データベースの間で、完全一致した情報にリンクが描画されています。

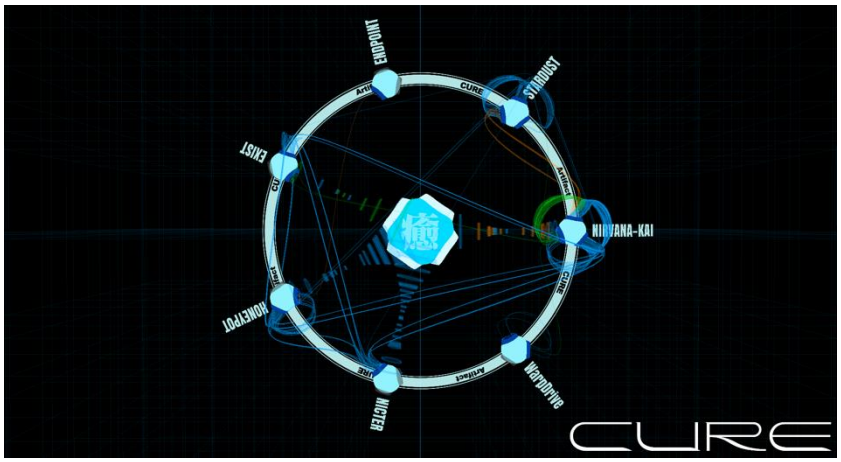


図 2 Artifact（観測情報）レイヤ

図 3 は、今回新たに CURE に加わった、自然言語で記述された分析情報を格納する Semantics レイヤを示しています。

様々なセキュリティベンダによるセキュリティレポート（Security Reports）や、米国の MITRE ATT&CK で公開されている攻撃者グループ（ATT&CK Groups）、攻撃手法（ATT&CK Techniques）、攻撃に用いられるソフトウェア（ATT&CK Software）に関する情報が融合されています。

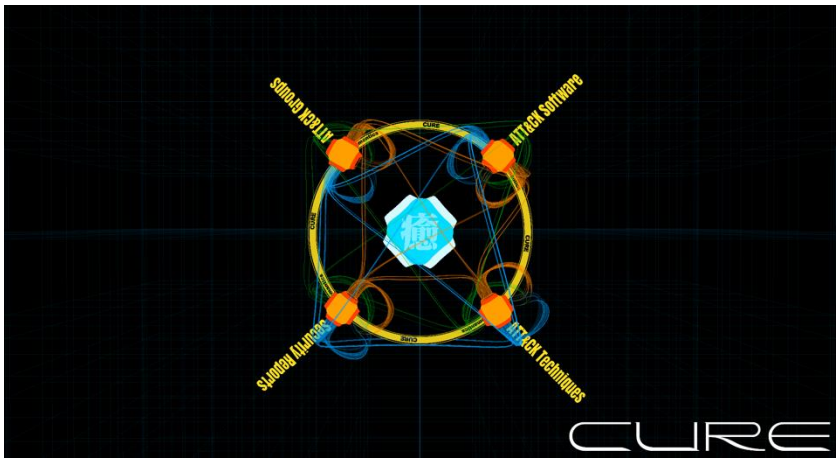


図 3 Semantics（分析情報）レイヤ

図 4 は、Semantics レイヤのデータベースに含まれる自然言語のタグと、タグによる異種情報間のリンクを表しています。

セキュリティレポートなどの文書から、自然言語処理によって、その文章の特徴を表す特徴語を抽出してタグを生成します。文書中の画像などからもタグを抽出できます。

このタグを用いた関連付けによって、Artifact レイヤの観測情報（IP アドレス、ドメイン名、マルウェア）に対して、分析情報による意味付けを行うことができます。

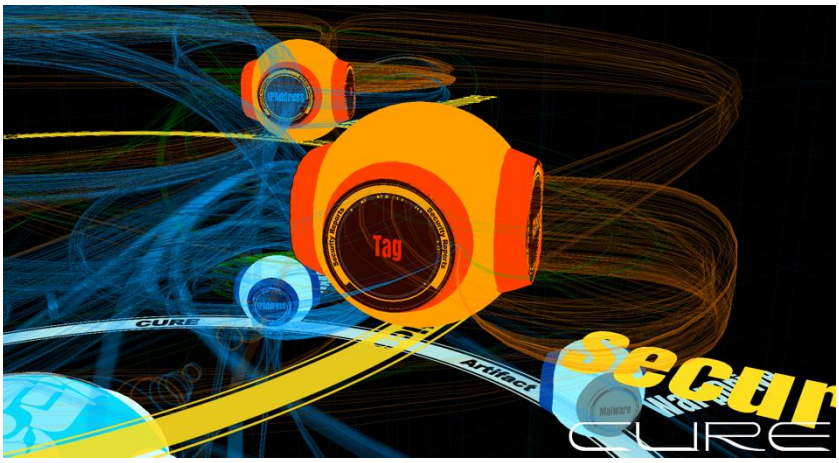


図 4 タグによる関連付け

図 5 は、Emotet と呼ばれるマルウェアが使用する IP アドレスが、外部機関の発行したセキュリティレポートと ATT&CK Software（Semantics レイヤ：橙色小球体）の中に記載されています。さらに、その IP アドレスが NIRVANA 改が集約した自組織内のアラート情報（Artifact レイヤ：青色小球体）に含まれていることが青色のリンクで可視化されています。

この Emotet の例のように、自然言語のタグによる CURE 内の検索も可能になり、世の中で新たに出現したサイバー攻撃について、自組織での発生状況などが容易に調査できます。

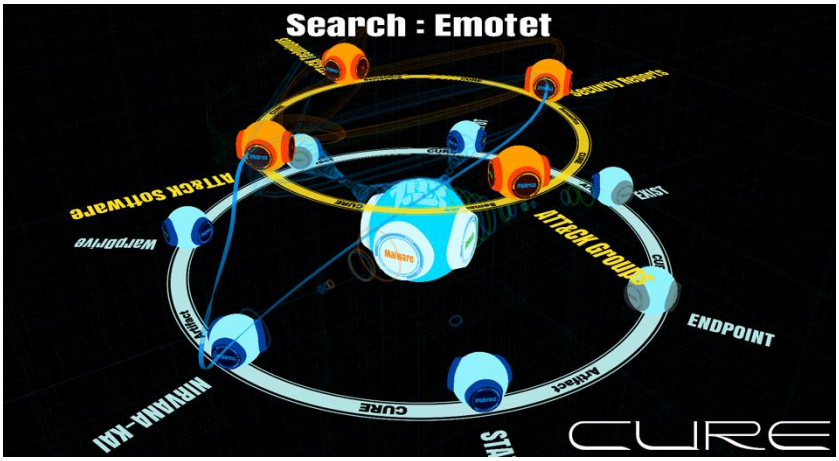


図 5 CURE の検索機能

今回の CURE の機能強化によって、自組織における観測情報と外部機関が公表した分析情報とを柔軟に関連付けることが可能となり、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。

【今後の展望】

CURE によって、多種多様なセキュリティ・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サイバーセキュリティ統合知的基盤の創出を目指します。

機能強化した CURE は、2020 年 10 月 28 日（水）～30 日（金）に幕張メッセで開催される「第 10 回 情報セキュリティ EXPO【秋】」で動態展示を行います。また、CURE の技術詳細については 2020 年 10 月 26 日（月）～29 日（木）にオンライン開催されるコンピュータセキュリティシンポジウム 2020（CSS2020）で発表しています。

＜ 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、津田 侑、鈴木 宏栄
Tel: 042-327-6225
E-mail: nicter@ml.nict.go.jp

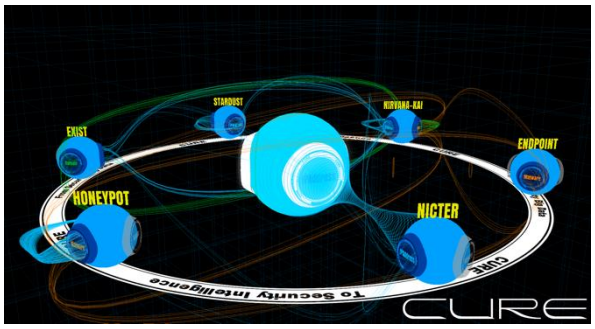
＜ 広報 （取材受付） ＞
広報部 報道室
廣田 幸子
Tel: 042-327-6923
E-mail: publicity@nict.go.jp

＜用語解説＞

*1 CURE（キュア）

CURE（Cybersecurity Universal REpository）は、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。個別に散在していた情報同士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し、リアルタイムに可視化する。

報道発表「セキュリティ情報融合基盤“CURE”を開発」
2019 年 6 月 6 日
https://www.nict.go.jp/press/2019/06/06-1.html



CURE

*2 MITRE ATT&CK（マイター アタック）

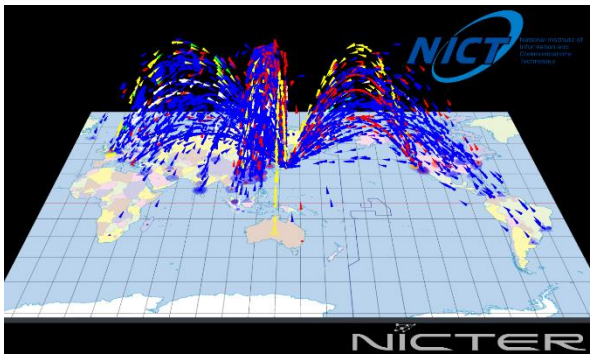
MITRE ATT&CK は、米国 MITRE 社が開発しているサイバー攻撃の戦術や手法等を体系的かつ網羅的に記述するフレームワーク。実際の観測に基づいて記述された ATT&CK 知識ベースを公開している。

MITRE ATT&CK
https://attack.mitre.org

*3 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/

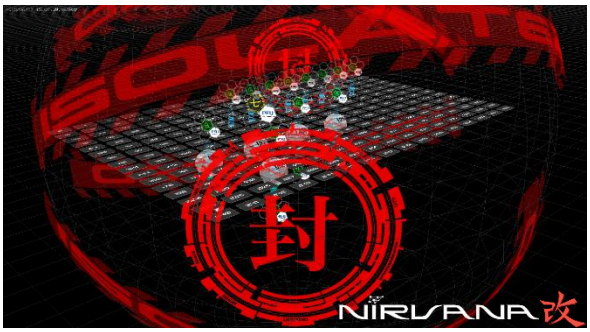


NICTER

*4 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（NICTER Real-network Visual ANAlyzer KAI）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

*5 WarpDrive（ワープ・ドライブ）

WarpDrive（Web-based Attack Response with Practical and Deployable Research InitiatiVE）は Web 媒介型攻撃の実態把握と対策技術の向上を目指したユーザ参加型プロジェクト。「攻殻機動隊 S.A.C.」シリーズに登場するキャラクター「タチコマ」がユーザの PC やスマートフォンの中で Web 媒介型攻撃の観測・分析を行い、悪性サイトへのアクセスを遮断する。

WarpDrive ポータルサイト
https://www.warpdrive-project.jp/

WarpDrive