2-2-4　セキュリティ情報融合基盤 CURE
2-2-4　CURE: Cybersecurity Universal REpository

海崎 光宏　鈴木 宏栄　田中 秀一　井野 毅也
UMIZAKI Mitsuhiro, SUZUKI Koei, TANAKA Hidekazu, and INO Takeya

組織のセキュリティ強化のためには、自組織内での適切なセキュリティ対策によりサイバー攻撃の監視や分析を行うことが不可欠である。加えて、最近では外部組織から提供される脅威情報（threat intelligence）などを定期的に収集し、それらを自組織のセキュリティ戦略に組み込むことも必要とされている。しかし、組織内外から生じる多種多様なサイバーセキュリティ情報を定常的に収集し分析することは、大きな人的コストを要するため、このような活動は多くの組織にとって重荷となり、実施が困難な状況にある。我々は、組織内外から発生する様々なサイバーセキュリティ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 CURE（キュア : Cybersecurity Universal REpository）の研究開発を行っている。本稿では CURE の仕組みについて述べるとともに CURE の社会展開状況についても報告する。

To enhance an organization's security, it is crucial to monitor and analyze cyber attacks by implementing appropriate security measures internally. Moreover, in recent times, there is a growing need to continuously gather threat intelligence and other relevant information from external sources, and to leverage this information for internal security measures. However, the significant human resources required to routinely collect and analyze such cybersecurity information, generated both internally and externally, impose a substantial burden on many organizations, making it challenging to put these measures into practice. We are currently engaged in the research and development of CURE (Cybersecurity Universal REpository), a security information fusion infrastructure that facilitates the centralized collection and cross-analysis of various types of cybersecurity information generated both inside and outside an organization. This paper outlines the mechanism of CURE and provides an update on its societal implementation status.

1　背景

マルウェアの感染拡大といった無差別型攻撃や、特定の組織を対象とした標的型攻撃など、サイバー攻撃の手法は多岐にわたる。これらのサイバー攻撃に対抗するために、多種多様な観測データが収集され、組織のセキュリティ向上に活用される。一方で、現在ではサイバーセキュリティに関連する情報がインターネット上で広く公開されている。これらの情報を適切に活用することで、サイバー攻撃の最新動向を把握でき、組織のセキュリティを一層強化するための知見を得ることが可能となる。しかしながら、組織内外の様々な情報の定常的な収集、分析には高い人的コストを要することから、これまで多くの組織ではサイバーセキュリティ関連情報を容易に利活用できなかった。

我々は、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: Cybersecurity Universal REpository）[1] の研究開発を行っている。CURE は、多種多様で散在するサイバーセキュリティ関連情報の中から、その関連性を自動的かつ高速に発見するためのシステムであり、全てのデータをインメモリ DB に搭載し、高速な検索と横断分析を実現する。加えて、複数のデータベースを横断的に分析し、情報を紐づけていくことにより、これまでに発見できなかったサイバー攻撃に対する新たな知見を得る可能性がある。

本稿では CURE の仕組みや社会展開などの状況について報告する。以下、**2** で CURE の仕組みを説明し、**3** で CURE の可視化システム、**4** で社会展開の状況についてそれぞれ述べ、**5** でまとめる。

2　セキュリティ情報融合基盤 CURE

2.1　システム概要

図 1 に CURE のシステム概要を示す。CURE では Pub/Sub 型メッセージングシステムを参考にし、データを発信する CURE Publisher、データを利用する CURE Subscriber、そして、CURE Publisher と Subscriber を仲介し、データの横断分析機能を持つ CURE Hub を主な要素とする。

CURE Publisher は観測データを扱うシステムと観測データに意味付け（分析情報を付与）するシステムの 2 つで構成される。各 Publisher は、CURE Hub が定めたトピック（IP アドレス、ドメイン名、ファイルハッシュ値、メールアドレス、意味付けデータなどのサイバーセキュリティ関連情報の注目すべき事柄）へのデータ発信を唯一の役割とする。CURE Subscriber は、セキュリティ監視や脅威分析を行う自動化システム（例：SIEM（Security Information and Event Management）や脅威情報プラットフォーム）またはセキュリティ・オペレータによる手動での利用を想定する。CURE は、これら 3 つの要素がそれぞれ独立して動作する疎結合なシステム構造を持っている。

2.2　CURE の情報源 : CURE Publisher

以下に、CURE の情報源である CURE Publisher を示す。観測層 Publisher として情報通信研究機構（以下 NICT）が定常運用するシステム、意味付け層 Publisher としてインターネット上のサービスやセキュリティレポートなどが実装されている。

ハニーポット群（観測層 Publisher）
無差別型攻撃観測。3 種のハニーポット（Dionaea、Cowrie、Glastopf）で観測したサイバー攻撃関連の通信。扱うトピックは IP アドレス、ファイルハッシュ値。なお、ハニーポットとは、サイバー攻撃をしやすいように意図的にぜい弱性を持たせたシステムのことである。

Haguregumo [2][3]（観測層 Publisher）
無差別型攻撃観測。全ポート待ち受け型ハニーポットの観測情報。扱うトピックは IP アドレス。

AmpPot [4][5]（観測層 Publisher）
無差別型攻撃観測。攻撃の一種であるリフレクション攻撃の観測情報。扱うトピックは IP アドレス。なお、リフレクション攻撃とは、IP アドレスを詐称して DNS 等のサーバ群に問い合わせを行い、攻撃対象に大量の応答を返すことでサービス不能に追い込む攻撃手法である。

EXIST [6]（観測層 Publisher）
脅威情報収集。15 種類のオープンソース脅威情報サービスから収集した、危険と判断されたサイトやホストの情報。扱うトピックは IP アドレス、ドメイン名。

NICTER [7]（観測層 Publisher）
無差別型攻撃観測。ダークネット（未使用 IP アドレス）観測で得たパケットを送信元 IP アドレス・宛先ポート番号、プロトコルでグループ化したもの。扱うトピックは IP アドレス。

NIRVANA 改 [8]（観測層 Publisher）
アラート情報統合分析。セキュリティ機器から発報されるアラートを毎分グループ化したもの。扱うトピックは IP アドレス、ドメイン名、ファイルハッシュ値。

STARDUST [9]（観測層 Publisher）
標的型攻撃観測。標的型攻撃関連のマルウェアを介して発生した攻撃者の LAN 内での活動や C2 サーバとの通信。扱うトピックは IP アドレス、ドメイン名、

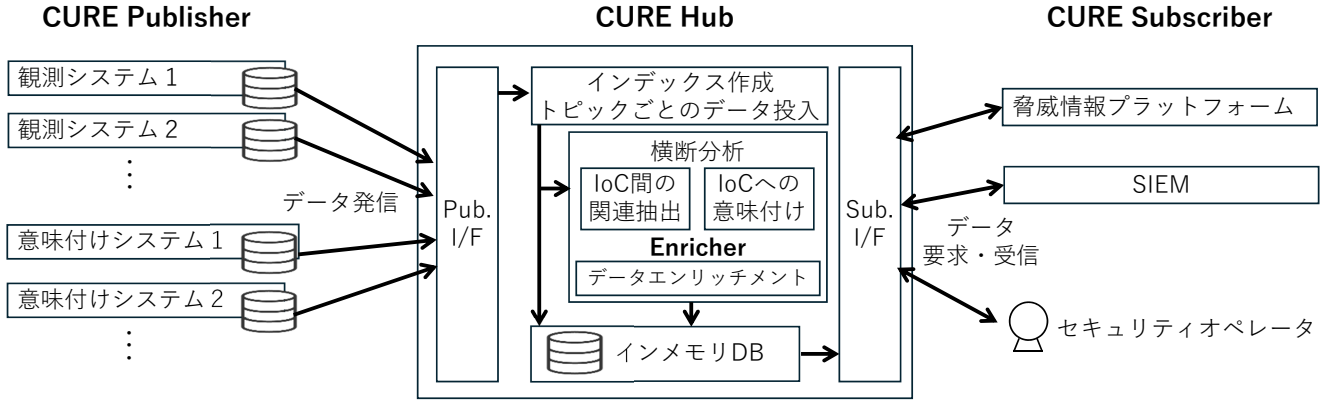

図 1　CURE のシステム概要

ファイルハッシュ値。なお、C2 サーバとは、デバイスに感染したマルウェアにコマンドを送信し、制御するためのサーバのことである。

エンドポイント [10]（観測層 Publisher）
エンドポイント情報収集。端末に導入されたエージェントソフトウェアによって収集された不審プロセス及びそのプロセスによって発生した通信。扱うトピックはファイルハッシュ値。

WarpDrive [11][12]（観測層 Publisher）
Web 媒介型攻撃対策。収集した Web アクセス履歴のうち、WarpDrive が備えるブロックリストと合致したもの。扱うトピックはドメイン名。

CHORUS [13]（観測層 Publisher）
Web 媒介型攻撃対策。マルウェア配布サイトからダウンロードされるマルウェア。扱うトピックはファイルハッシュ値。

Malmail（観測層 Publisher）
攻撃メール観測。各種セキュリティアプライアンスで検出された攻撃メール。扱うトピックはメールアドレス。

SpamDB（観測層 Publisher）
ばらまき型メール観測。NICT のメールサーバでダブルバウンスが発生した際の情報。扱うトピックはメールアドレス。なお、ダブルバウンスとは、メール配信失敗時の送信元への通知（バウンス）が失敗した状態であり、このことは送信元が詐称されている可能性を示唆する。

ATT&CK [14]（意味付け層 Publisher）
サイバー攻撃ナレッジフレームワーク。各 Techniques、Groups、Software を意味付けキーワードとして登録。各詳細ページに記載の参考文献から各種 IoC（Indicator of Compromise）を抽出しキーワードと紐づけて保存。なお、IoC とは、サイバー攻撃を受けた際に残される痕跡情報のことであり、サイバー攻撃に利用されたマルウェアやその通信先の IP アドレスなどがこれにあたる。

Security Reports（意味付け層 Publisher）
セキュリティレポートに記載の脅威情報。セキュリティベンダーなどの解説記事を自然言語処理によって分析。IoC とそれに関連するキーワードを抽出し保存。

Social Media（意味付け層 Publisher）
SNS 上の脅威情報。X（旧 Twitter）などの SNS から情報収集を行い、自然言語処理を用いて分析。IoC とそれに関連するキーワードを抽出し保存。現在は検証中の為、本番環境へのデータ送信は行っていない。

Trouble Ticket（意味付け層 Publisher）
インシデントのタグ情報。NICT で検出したセキュリティアラート情報をアナリストが解析して登録。各種 IoC に紐づけられる。

2.3　データの質の向上 : Enricher

Publisher が投稿した情報は CURE Hub に集約され、横断分析機能により互いに紐づけられる [1]。しかし、サイバー攻撃の実態をより正確に把握するためには、単に紐づけるだけではなく、データの質を継続的に向上させることが肝要である。この実現のために CURE Hub は、データの有用性や信頼性を強化するデータエンリッチメントの仕組みを持っている。

データエンリッチメントはデータの質を高めるために付加情報を与えるという広範なコンセプトである。Enricher を用いて IP アドレスやドメイン名に悪性度スコアを付与することや、解析者によるデータの信頼性評価を付与することなど、多岐にわたる応用が可能であり、情報分析能力を更に強化することに寄与する。

現在、CURE 内の IP アドレスに類似度スコアを付与することで、類似の挙動を示す IP アドレス群を検出する Enricher が実装されている（図 4）。この Enricher により、データの完全一致による関連付けだけでなく、「この IP アドレスと同様の動きを見せる IP アドレス」のように、より柔軟な関連付けができるようになり、データの完全一致だけでは達成できなかった広範な横断分析が可能となる。

3　CURE 可視化エンジン

CURE によって融合された膨大な観測情報や分析情報の関連性を把握することは容易では無い。そのため我々は、CURE に送信された脅威情報とサイバーセキュリティ関連情報との間のつながりや類似 IP アドレスを包括的に把握するための可視化エンジンを開発している。

図 2 に CURE 全体図を示す。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観測情報と分析情報を格納するデータベース（DB）群を表している。桃色の球体は付加情報を与える Enricher で、類似の挙動を示す IP アドレス群を検出する。CURE 本体では IP アドレス、ドメイン、マルウェア、

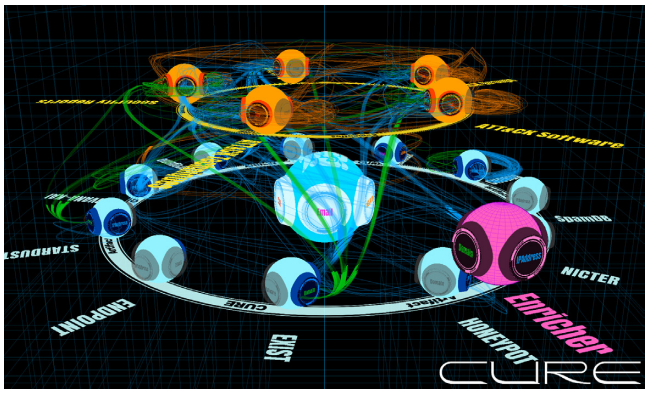

図 2　CURE 全体図

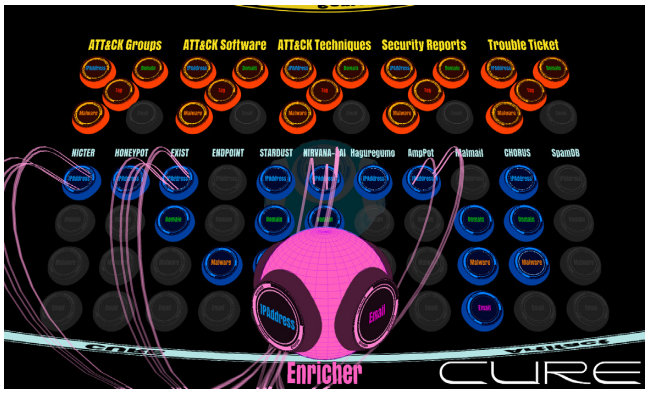

図 4　Enricher による類似 IP アドレスの検出

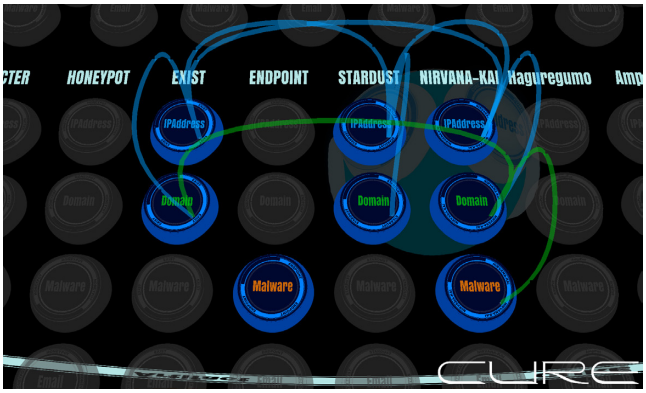

図 3　複数の DB をまたぐ攻撃キャンペーンのハイライト表示

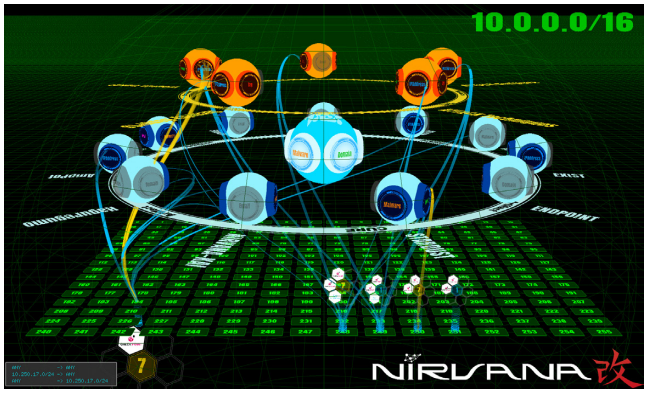

図 5　CURE の NIRVANA 改連携

メールアドレスについて横断分析を行い、同一の情報が見つかると DB 間にリンクを描画する。各 DB から CURE に送られた情報を種別ごとに表示する詳細表示の例として、図3に複数のDBをまたぐ攻撃キャンペーンをハイライトしている様子を、図 4 に Enricher による類似 IP アドレス検出の様子を示す。図5は CURE とサイバー攻撃統合分析プラットフォーム 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を自動的に関連付けている様子を表している。

4　CURE の社会展開状況

CURE は誕生して以来、NICT 内でのみ利用されていた。しかし、2024 年 4 月、国内の産学官の組織が参画する CYNEX（サイネックス）アライアンスにおいて、参画組織を対象に CURE のデータ開放がスタートした。機微情報を含む CURE のようなシステムは、基本的には組織外への開放は行われないが、CURE データに対するリスク分析とデータ格付け、それに基づくアクセス制御機能の実装によりデータ開放が実現した。現時点（2024 年 5 月時点）では計 20 組織に対して CURE データが開放されており、定常的な解析業務の重要な情報源としての CURE 活用が始まっている。

データの開放により、CURE がより広範囲で活用されるようになった。その結果得られるユーザーからのフィードバックは、開発の方向性を示す貴重な情報源だと考える。積極的に収集し、今後の開発に活かしていきたい。

5　まとめ

我々は、これまで、セキュリティオペレーションを効率化するためのひとつとして、CURE の研究開発を行ってきた。CURE は、多種多様かつ大規模なサイバーセキュリティ関連情報を集約・横断分析し、高速な検索を可能にするシステムである。今後は、Publisher/Enricher の拡充によるデータの量と質の向上に取り組むとともに、組織に関連する脅威情報を通知するプッシュ型機能の開発を計画している。さらに、CURE データの分析を実践し、大規模データからのインテリジェンスの創出を目指す。

謝辞

本研究におけるシステムの開発に尽力された津田侑氏に心から感謝申し上げます。その卓越した技術力と献身的な努力により、本研究開発は大いに進展しました。この場を借りて、深く感謝の意を表します。

【参考文献】

1 津田 侑, 井上 大介, 鈴木 宏栄, 高木 彌一郎, 田中 秀一, 金谷 延幸, 竹本 亜希, 古本 啓祐, “セキュリティ情報融合基盤 CURE,” コンピュータセキュリティシンポジウム 2020 論文集, 2020.
2 牧田 大佑, 島村 隼平, 久保 正樹, 井上 大介, ”全ポート待受型の簡易ハニーポットによるサイバー攻撃観測” 電子情報通信学会 2019 年暗号と情報セキュリティシンポジウム (SCIS2019), 2019.
3 牧田 大佑, 島村 隼平, 久保 正樹, 井上 大介, ”全ポート待受型の簡易 TLS ハニーポットにより観測されたサイバー攻撃の分析,” 電子情報通信学会, 第 50 回情報通信システムセキュリティ研究会 (ICSS50), 2020.
4 Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow, “AmpPot: Monitoring and Defending Amplification DDoS Attacks,” Proceedings of the 18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID’15).
5 牧田 大佑, 西添 友美, 吉岡 克成, 松本 勉, 井上 大介, 中尾 康二, “早期インシデント対応を目的とした DRDoS 攻撃アラートシステム,” 情報処理学会論文誌, vol.57, no.9, pp.1974–1985, 2016.
6 nict-csl/exist. https://github.com/nict-csl/exist/.
7 Daisuke Inoue, Katsunari Yoshioka, Masashi Eto, Masaya Yamagata, Eisuke Nishino, Jun’ichi Takeuchi, Kazuya Ohkouchi, and Koji Nakao. “An Incident Analysis System NICTER and Its Analysis Engines Based on Data Mining Techniques. In Advances,” Neuro-Information Processing, pp.579–586, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.
8 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. “NIRVANA 改によるライブネット分析,” 情報通信研究機構研究報告, vol.62, no.2, pp.59–66, 2016.
9 津田 侑, 遠峰 隆史, 金谷 延幸, 牧田 大佑, 丑丸 逸人, 神宮 真人, 高野 祐輝, 安田 真悟, 三浦 良介, 太田 悟史, 宮地 利幸, 神薗 雅紀, 衛藤 将史, 井上 大介, 中尾 康二, “サイバー攻撃誘引基盤 STARDUST,” コンピュータセキュリティシンポジウム 2017 論文集, 2017.
10 Yu Tsuda, Junji Nakazato, Yaichiro Takagi, Daisuke Inoue, Koji Nakao, and Kenjiro Terada, “A LightweightHost-Based Intrusion Detection Based on Process Gen-eration Patterns,” Proceedings of the 13th Asia JointConference on Information Security (AsiaJCIS 2018), pp.102–108, 2018.
11 WarpDrive. https://warpdrive-project.jp/
12 Takeshi Takahashi, Christopher Kruegel, Giovanni Vigna, Katsunari Yoshioka, and Daisuke Inoue, “Tracing and Analyzing Web Access Paths Based on User-Side Data Collection: How Do Users Reach Malicious URLs?,” Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020), 2020.
13 Mitsuhiro Umizaki, Tomohiro Morikawa, Akira Fujita, Takeshi Takahashi, Tsung–Nan Lin, and Daisuke Inoue, “Understanding the Characteristics of Public Blocklist Providers,” Proceedings of the IEEE Symposium on Computers and Communications (ISCC), 2022.
14 MITRE ATT&CK. https://attack.mitre.org/

海崎 光宏 （うみざき みつひろ）
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
博士 (理学)
サイバーセキュリティ

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
上席研究技術員
サイバーセキュリティ

田中 秀一 （たなか ひでかず）
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
サイバーセキュリティ

井野 毅也 （いの たけや）
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