国立研究開発法人
情報通信研究機構

プレスリリース
2024年6月11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”のカスタム通知機能を開発

～『Watcher』（ウォッチャ）による通知で自組織のセキュリティ向上に貢献～

【ポイント】

- セキュリティ情報融合基盤 CURE のカスタム通知機能『Watcher』を新規開発
- IP アドレスやドメイン名など自組織に関連した情報を CURE の通知対象として設定
- CURE から自組織関連の攻撃情報が通知可能となり、自組織のセキュリティ向上に貢献

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、セキュリティ情報融合基盤“CURE”[*1]（キュア）の新機能として、カスタム通知機能『Watcher』（ウォッチャ）を開発しました。Watcher に IP アドレスやドメイン名など、自組織に関連した情報を通知対象として設定することで、CURE の保有する膨大な情報の中から自組織関連の攻撃情報などが通知可能となり、CURE を活用した自組織のセキュリティ向上が期待できます。

CURE Watcher について、2024 年 6 月 12 日（水）～14 日（金）に幕張メッセで開催される「Interop Tokyo 2024」で動態展示を行います。また今後、サイバーセキュリティ分野の産学官連携拠点「CYNEX[*2] アライアンス」の参画組織への機能提供も予定しています。

【背景】

NICT はサイバー攻撃の実態把握のため、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を行ってきました。CURE は膨大な観測情報（Artifact）や分析情報（Semantics）を蓄積していますが、それらの情報を様々な組織がどのようにしてセキュリティ向上にいかすかが課題でした。

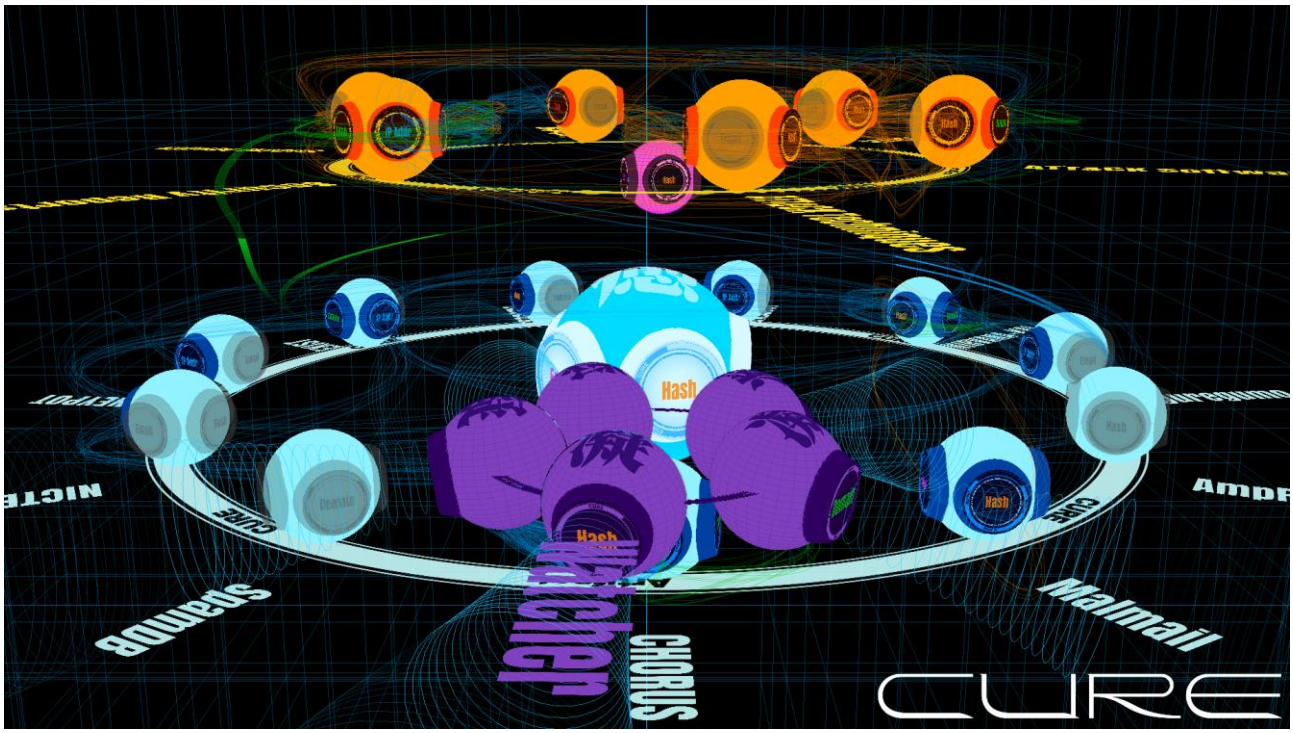


図 1 CURE 全体図（『Watcher』による通知対象の観測）

中央水色の球体が CURE 本体、青色と橙色の小球体はそれぞれ観測情報（Artifact）と分析情報（Semantics）を格納するデータベース。CURE Watcher は紫色の 5 つの小球体で構成され、それぞれが異なる通知対象を観測している。

【今回の成果】

今回、CURE の新機能としてカスタム通知機能『Watcher』(ウォッチャ)を開発しました(図 1 参照)。Watcher に IP アドレスやドメイン名など自組織に関連した情報を通知対象として設定しておくと、それらの情報が CURE の中に現れた際に自組織宛てに即時通知が行われます。

Watcher の通知対象として設定できる情報は、IP アドレス(IP Addr)、ドメイン名(Domain)、ハッシュ値(Hash)、メールアドレス(Email)、キーワード(Tag)の 5 種類です(図 2 参照)。

例えば、Watcher に自組織が使用している IP アドレスの範囲を設定しておくと、そのうちの 1 つが CURE の収集している悪性 IP アドレスリストに載った際に、自組織に通知が行われます(図 3 参照)。これは、自組織の IP アドレスが何らかの原因でサイバー攻撃に加担させられた結果、悪性判定された可能性があり、その IP アドレスについて自組織内で早急な調査が必要となります。

また、Watcherに自組織のドメイン名を設定しておくと、CURE の情報源の AmpPot[*3] がそのドメイン宛ての DRDoS 攻撃[*4] を検知した際に、自組織(＝被害組織)に通知が行われます(図 4 参照)。DRDoS 攻撃のような大量通信による攻撃は被害組織単体では原因の切分けが難しいため、外部からの通知は攻撃の早期検知と対処方針の決定に役立ちます。

これ以外にも、ハッシュ値は自組織に届いたマルウェアが CURE の情報源のハニーポットで捕獲されているかどうかや、セキュリティベンダのレポートに掲載されていないかの確認などに使えます。メールアドレスは自組織で使用しているメールアドレスが、外部サービスからの漏えい情報に含まれていた際の検知などに役立ちます。タグは攻撃グループによる SNS での自組織への DDoS 攻撃宣言の検知や、自組織の製品やサービスがセキュリティレポートで言及されていないかの確認などに使えます。

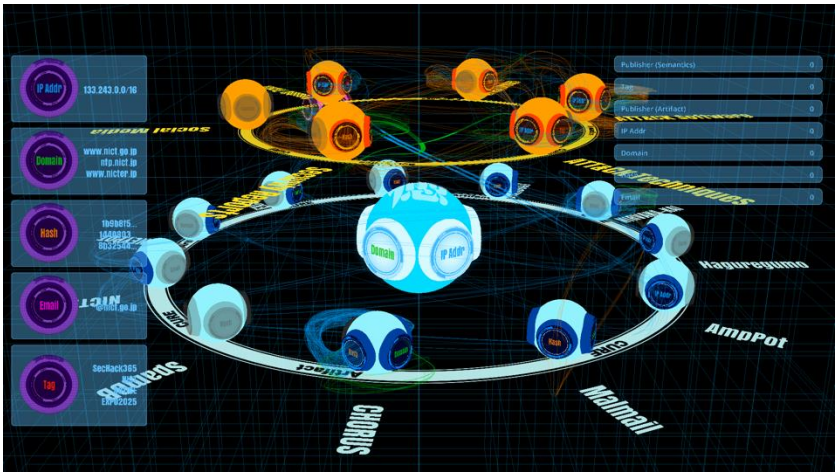


図 2 CURE Watcher の通知対象表示

Watcher の 5 つの小球体が散開し、左側のウィンドウ内で各 Watcher の通知対象として設定されている情報が表示されている。

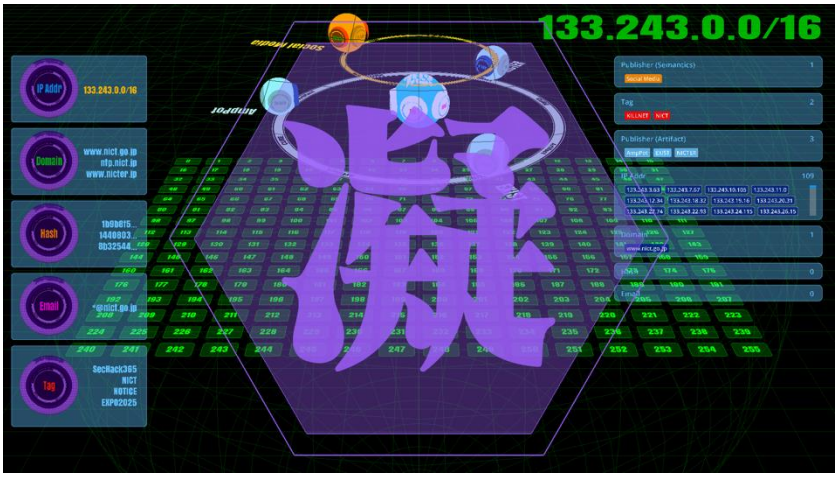


図 3 CURE Watcher による通知

通知対象に合致した情報が CURE に新たに登録されると「凝」アイコンが表示され、右側のウィンドウに検知された情報が表示される。

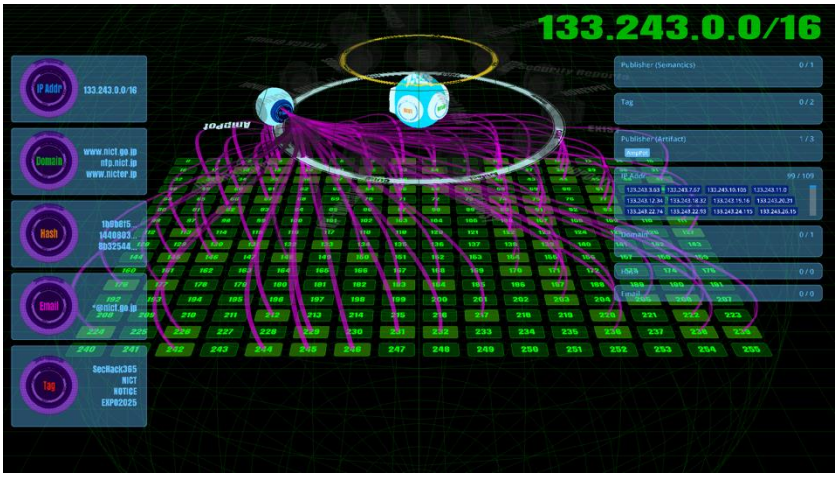


図 4 CURE Watcher による DRDoS 攻撃の検知

AmpPot によって自組織のドメインに対する DRDoS 攻撃を検知した様子。多数の IP アドレス宛てに絨毯爆撃型攻撃[*5] が仕掛けられていることが分かる。

CURE Watcher によって、CURE に蓄積された膨大な情報の中から、自組織関連の攻撃情報などが通知可能となり、CURE を活用した自組織のセキュリティ向上が期待できます。

CURE Watcher について、2024 年 6 月 12 日（水）～14 日（金）に幕張メッセで開催される「Interop Tokyo 2024」で動態展示を行います。

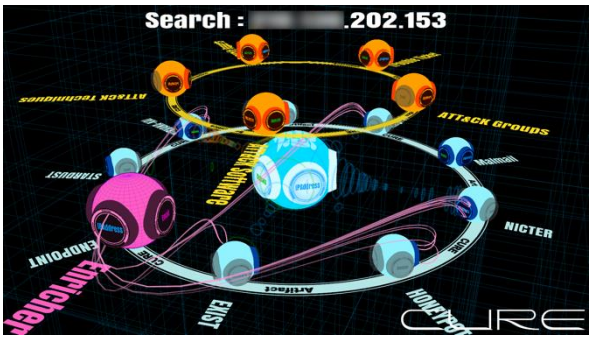
【今後の展望】

CURE はサイバーセキュリティ分野の産学官連携拠点「CYNEX アライアンス」の参画組織向けに開放されており、新機能 CURE Watcher も順次利用可能にしていく予定です。

＜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

報道発表「セキュリティ情報融合基盤 “CURE” を機能強化！」 2020 年 10 月 27 日
https://www.nict.go.jp/press/2020/10/27-1.html

報道発表「セキュリティ情報融合基盤 “CURE” のデータエンリッチメント機能を開発」 2022 年 6 月 14 日
https://www.nict.go.jp/press/2022/06/14-1.html

***2 サイバーセキュリティネクサス（CYNEX: Cybersecurity Nexus）**

サイバーセキュリティ分野の産学官の結節点（ネクサス）となる先端的基盤の構築を目指して、NICT 内に 2021 年 4 月 1 日に創設された組織。サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を開放することで、日本のサイバーセキュリティの対応能力向上を目指す。2023 年 10 月 1 日に産学官の参画組織を集めた CYNEX アライアンスを発足させ、本格稼働を開始した。

***3 AmpPot**

リフレクション攻撃（DRDoS: Distributed Reflection Denial-of-Service）を観測するハニーポット。横浜国立大学吉岡研究室と NICT サイバーセキュリティ研究室との共同研究・共同運用を行っている。

***4 DRDoS 攻撃**

DRDoS 攻撃（Distributed Reflection Denial-of-Service Attack）とは、インターネット上の DNS や NTP 等のサーバを悪用して攻撃対象に大量のパケットを送付し、攻撃対象のネットワーク帯域を圧迫する DDoS 攻撃の一種のこと。

***5 絨毯爆撃型攻撃**

単一の IP アドレスではなく主に同一ネットワーク内の広い範囲の IP アドレスに対して行われる攻撃。

＜ 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、川村慎太郎
E-mail: nicter@ml.nict.go.jp

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