2-2-2　攻撃者の行動を観測するためのサイバー攻撃誘引基盤 STARDUST

2-2-2　STARDUST: Large-scale Infrastructure for Luring Cyber Adversaries

金谷 延幸　鈴木 悦子　中村 大典　梅村 勇貴　佐藤 茂
KANAYA Nobuyuki, SUZUKI Etsuko, NAKAMURA Ohnori, UMEMURA Yuki, and SATO Shigeru

標的型攻撃に代表される政府機関や企業を狙ったサイバー攻撃が身近な社会問題となって久しい。サイバーセキュリティ研究室では、サイバー攻撃に対抗するための手段として、攻撃の手口を解明するための基盤 STARDUST を研究・開発・運用することで、攻撃と対策に関する有益な情報を収集してきた。従来のハニーポットやサンドボックスは単一プログラムの解析が目的であったが、STARDUST は実際の攻撃者を欺瞞（ぎまん）・誘引し攻撃を実演させ、複数 PC に拡散する攻撃者行動の解析を目的とする。このため、STARDUST は典型的な企業ネットワークを模擬した ICT 環境と、秘匿性の高いデータ収集の仕組みを提供する。本稿では、攻撃者の行動観測を実現する STARDUST について説明する。また、2023 年 10 月より提供を開始した新しい STARDUST NxtGen の特徴を説明し、さらに最新の攻撃観測事例について紹介する。

Cyber-attacks targeting government agencies and businesses, as typified by targeted attacks, have long been a more familiar social issue, and NICT has been working on a platform for analyzing attacks as a means of countering these attacks.

Through research and development of STARDUST, NICT has collected useful information on cyber-attacks and their countermeasures. Unlike conventional honeypots and sandboxes that only analyze the behavior of single programs, STARDUST aims to observe the human behavior of attackers. For this purpose, STARDUST has an ICT environment that emulates an actual corporate network and has a mechanism to allow an actual attacker to demonstrate an attack and collect data without the attacker being aware of it. This paper describes the STARDUST mechanism that enables observation of attacker behavior. It also explains the features of the new STARDUST NxtGen, which was launched October 2023, and introduces an actual case of attack observation and analysis.

1　まえがき

政府機関や企業を狙ったサイバー攻撃が身近な社会問題となって久しい。標的型攻撃とは特定の組織を狙い長期間潜伏し行われるサイバー攻撃のことである。標的型攻撃では、まず対象となる組織にマルウェアを送り込み、事務処理 PC 等に感染させ初期侵入を行う。次に、より高度な Remote Access Tool（RAT）を侵入した PC にダウンロード・インストールし、侵入した PC を遠隔操作する。攻撃者は、侵入した PC を踏み台として対象組織のネットワーク内を探索し、次の侵入先 PC に感染を広げつつ重要なサーバを探し出し、最後に目的とするファイルを盗み出す。このように、高度なサイバー攻撃では、攻撃の開始から目的の達成まで長期にわたり潜伏し、様々な手口による試行錯誤を経て実行されることが報告されている [1]–[3]。

サイバー攻撃の対策には、まず攻撃を観測することで攻撃者の手口をよく知り、攻撃に関連したデータを収集し、研究開発の実験・評価に利用する事が必要である。さらに、サイバー攻撃に関連する研究開発には、実際の攻撃で使われる攻撃ツール、攻撃により発生する通信、侵入された PC に残された証跡（メモリ、レジストリ、ファイル等）などのデータが必要とされる。こうした観測とデータ収集の結果から分析される、攻撃者の人間としての行動、例えばどのような名前のファイルに興味があり、RAT 等を使った遠隔操作によって得られるどのような情報によって次の攻撃手段を選択しているか等の知見が特に重要である。一方で、こ

れらの攻撃に関する詳細な情報は、被害組織から外部に提供されることはまれであり、入手することは困難であった。

従来、解析者（サイバー攻撃に関連した情報の収集と分析スキルを有する技術者）は、サンドボックスやハニーポットと呼ばれる単一のプログラムの挙動解析を目的とする技術・ツールを利用してきた。しかしながら、これらの手段では表層的なプログラムの機能と動作しかわからず、攻撃者がマルウェアをどのように活用し、侵入後に活動するかまではわからない。また、PC 間で入先を広げる感染拡大を伴う活動は、単一の PC 上で動作させる解析では観測することができない。さらに、特定の対象を狙った攻撃を観測するためには、攻撃者の目的に合致する環境を用意する必要がある。

そこで、サイバーセキュリティ研究室では、攻撃者の人間的な行動の観測を実現するサイバー攻撃誘引基盤 STARDUST を研究開発した [4]。STARDUST を利用することで、仮想マシンで構成された企業の典型的な ICT 環境に攻撃者を誘引し、秘匿性の高い手段でデータを収集することが可能であり、さらにワンストップの Web UI を介して仮想マシン操作やデータ参照することができる。当研究室では、STARDUST を活用し実際の攻撃者を欺瞞・誘引した複数の事例を解析し、その際のデータを蓄積してきた。STARDUST は内部利用だけでなく、外部の官公庁等を含む共同研究組織に貸与され、研究開発活動に貢献してきた。また、収集されたデータは標的型攻撃のデータセットとして提供され、研究開発に活用されている [5]。

さらに、2023 年度より、サイバーセキュリティネクサス（CYNEX）アライアンスの Co-Nexus A 参画組織へ貸与することが決定され、STARDUST の利用者を大幅に増加させることになった [6]。この需要を満たすため、新たに次期バージョンの STARDUST NxtGen を研究開発した。STARDUST NxtGen は、増加する利用者の需要を満たす計算機資源の増強と、構築・運用管理の省力化を両立させる新たなアーキテクチャにより実現されている。

本稿では、まず **2** で STARDUST の概要と構成を紹介し、**3** で進化した STARDUST NxtGen の新機能とその実現技術について紹介する。さらに **4** で STARDUST による観測事例について紹介する。最後に、CYNEX アライアンスでの提供も含めた今後の予定について説明する。

2　STARDUST の概要とその構成

STARDUST は、攻撃者を欺瞞・誘引し、解析者による観測の事実を秘匿しつつ長期間行動を観測するため必要となる、以下の 4 つの主要な要素で構成されている（図 1）。

1. 典型的な企業 ICT 環境を摸倣した、模擬環境
2. 秘匿性の高い手段でデータを取得する、観測・分析システム
3. 高速にかつ解析目的に合致した構成の模擬環境を提供する、自動構築システム
4. 解析者が容易に STARDUST を利用することを可能にした、ユーザサービス

ここでは、上記 4 つの要素について説明する。

2.1　模擬環境

STARDUST では、解析者は実際の攻撃者を典型的な企業 ICT 環境を摸倣した模擬環境（図 2）に誘引し、攻撃者に対象企業への侵入に成功したと誤認識させ、攻撃者の行動を観測しデータ収集を行う。この模擬環境は、仮想マシン（VM）技術で保護され完全に隔離された環境に構築されている。攻撃者が模擬環境に侵入後に観測の事実を察知したとしても模擬環境の中から STARDUST を構成するサービス用のネットワークや

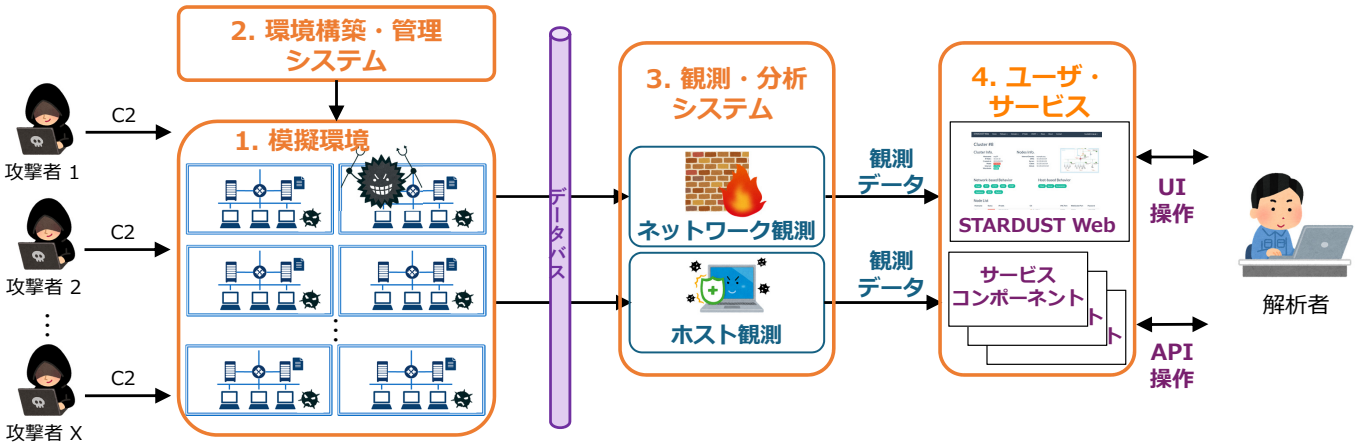

図 1　STARDUST の構成

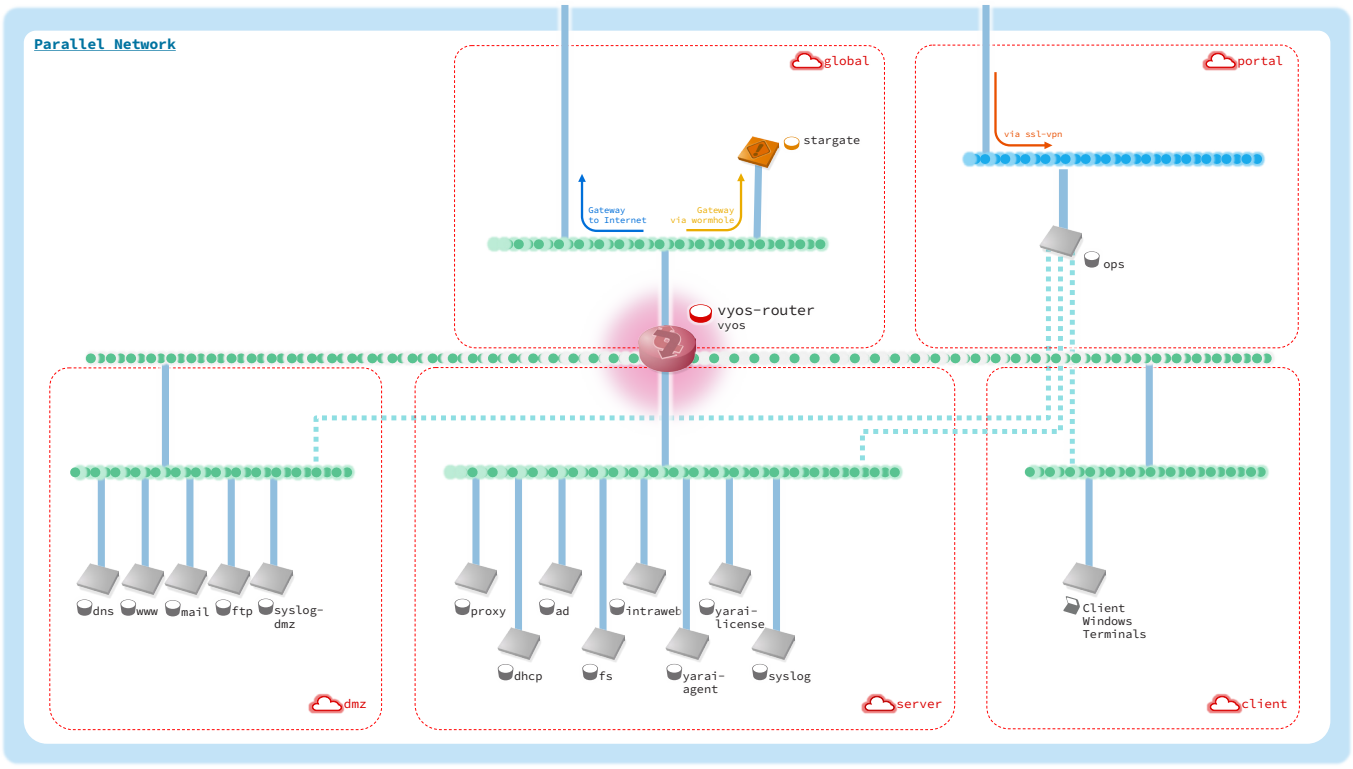

図 2　模擬環境

サーバ群に攻撃することはできない。誘引された攻撃者は、Command & Control サーバ（C&C サーバ）と呼ばれる遠隔操作を仲介するサーバを経由し、感染に成功した（と解析者が偽装した）模擬環境内のオフィス PC で実行した RAT を用いて、模擬環境の探索を始める。模擬環境内に設置された、重要と誤認識したサーバ、例えばファイルサーバや認証サーバを見つけると、それらのサーバの脆弱性（セキュリティ上の欠陥）を悪用した攻撃などを駆使し攻撃を行う。そして、囮として用意された重要ファイルを入手すると、RAT を使ってアップロードし、ファイルの内容を確認する、などの攻撃活動を行う。解析者は、STARDUST を使い観測することで、RAT の通信先、攻撃者の使うツール、悪用する脆弱性、攻撃行動に伴う通信データなど、攻撃活動に伴う情報を得ることができる。

攻撃者の欺瞞に失敗し、観測の事実を攻撃者に察知されてしまうと、攻撃に関する重要な情報を入手することができない。そこで、模擬環境には以下の性質が求められる。

1. ICT 環境が、典型的で自然
2. 用意されたコンテンツが、攻撃者の興味をそそる
3. 上記 ICT 環境とコンテンツの特徴が、攻撃対象組織の特徴に一致

まず、観測専用の偽環境と見破られることを防ぐため、ICT 環境が典型的で自然である必要がある。このため、実企業ネットワークと同等の ICT 環境を用意し、あたかも実業務が行われているかのように偽装したサーバや PC 群を構築する。模擬環境は、インターネットセグメント、DMZ（外部ネットワークと内部ネットワークの中間ネットワーク）セグメント、サーバセグメント、一般的な事務所を想定したクライアントセグメントといった典型的な企業に倣った複数のネットワークセグメントで構成される。模擬環境内には、文書作成ツールやプレゼンテーションツールなどがインストールされた事務処理用 PC 相当の VM を複数台用意する。また、典型的なサーバ群、例えば認証サーバ、ファイルサーバ、メールサーバ、社内用 Web サーバ、社外公開サーバなどの VM を配備する。各々のサーバには実業務でも利用可能な一貫性のある設定を行い、模擬環境内では実際に社内 Web ページの参照やメールの発信も可能である。さらに、実企業を模擬した複数の部署（開発部、営業部、人事部等）で構成される架空の従業員を想定したユーザアカウントを多数用意し、十分な規模の組織を想定した企業システムとして構築する。

次に、攻撃活動を継続させるには、より攻撃者の興味をひくコンテンツを用意することが必要となる。このため、各事務処理相当の PC には囮のファイルが置かれ、メールサーバには囮のメールが蓄積されている。さらに、解析者が Web ブラウザの閲覧履歴などをあらかじめ作成しておくことで、攻撃者の疑念を払拭するような試みを行う事例もある。

最後に、特定の組織を狙った攻撃を観測するには、ICT 環境の特徴やコンテンツの内容が標的組織の特徴と一致させることで、攻撃者に標的組織の ICT 環境とコンテンツであると誤認識させる必要がある。そこで、事前に標的とする企業・組織が判明している場合は、標的企業のネットワーク構成等を摸倣した模擬環境を用意する。例えばドメイン名や IP アドレスを攻撃目標にあわせ、ユーザアカウントやメールアドレスを変更し、必要であればファイルやメールなどのコンテツを標的企業のプロファイルに沿って書き換える。さらに、ワームホールと呼ばれる模擬環境のインターネット出口を実組織のネットワークに接続する技術を用意しており、C&C サーバに模擬環境内のマルウェアが接続した際に、実組織に感染したマルウェアから発信されたと攻撃者を欺瞞することができる。

2.2　観測・分析システム

精巧に作り込んだ模擬環境を用いて攻撃者に行動させることに成功したら、次は攻撃者に察知されずデータ収集し、分析できなければならない。もし、マルウェア分析に使われるバイナリ解析ツールが模擬環境内 PC にインストールされていたら、攻撃者は解析用の環境であると見抜くだろう。

そこで、STARDUST は、隠蔽性の高い 3 つの手法でデータを収集し、分析する。

1. パケットミラーリングによるトラフィックの収集と蓄積
2. VM 上で動作するエージェントによるプロセス情報の収集
3. VM の仮想化された周辺機器からの収集

最初の収集方法として、模擬環境内で発生するすべてのトラフィックはパケットブローカーと呼ばれる専用装置を用いパケットミラーリング（通信されたパケットをコピーすること）し蓄積する。次に、トラフィック解析基盤 SF-TAP [7] を使いリアルタイムで DNS、HTTP、TCP、ICMP といった主要なプロトコルに対する分析を行い、その結果を蓄積する。これらのデータを参照することで、解析者はどこの通信先に対してどのような通信が行われたのかをリアルタイムで参照しながら、必要な対応を行うことが可能である。

2 番目のデータ収集方法として、事務処理 PC を想定した VM には、VM で動作する OS 情報を収集するエージェントが動作している。このエージェントにより、VM 内で動作するマルウェアの情報や、そのプロセスツリー、通信先を収集することが可能である。Linux が動作するサーバ VM の動作情報は、Syslog（システムログを他サーバに転送する仕組みとそのプロトコル）を利用して収集している。

3 番目のデータ収集方法である仮想化された周辺機器からの情報収集としては、VM の仮想コンソールのスクリーンショットを 2 秒に 1 回取得している。この機能を使うと、攻撃者のコンソール上の操作を可視化できる。例えば、攻撃者が感染した PC にリモートデスクトップツールをインストールし、コンソールを乗っ取り、コンソール上でファイルを参照し、ブラウザを起動し攻撃の踏み台に利用する行動を、連続する画像ファイルとして収集することができる。この他の仮想周辺機器からの情報収集機能として、仮想ハードディスクからの証跡収集機能があるが、詳細は **3.3** で説明する。

2.3　自動構築システム

解析者がより有意義な観測を得るためには、攻撃の対象となる組織を模倣した模擬環境を配備し、標的とする組織のプロファイルに沿ったサーバや PC、コンテンツ等の用意が必要である。例えば Windows Active Directory サーバ（Windows のユーザ認証を一括管理するサーバ、AD サーバとも呼ぶ）を狙って探索しているのであれば、その AD サーバを用意し、特定の OS の特定の脆弱性を狙った攻撃が利用されるのであれば、その脆弱性を含む OS を用意する必要がある。また、模擬環境の構成が原因で有意義な結果得られない場合は、その構成の変更が必要となる。さらには、別の新しい攻撃者を観測する場合は、新しい攻撃者の標的に対応した模擬環境を作り直すことになる。このように、常に解析者の要求や攻撃の対象に合わせ細かくカスタマイズされた模擬環境を、必要な時に即座に提供できることが重要となる。

これらのニーズに応えるため、構築する模擬環境の仕様を定義し、仕様を与えると自動構築を行うツールを研究・開発してきた。初期の STARDUST では、NICT にて開発したビルディングブロック型構築システム Alfons [8] を利用していた。Alfons は、テンプレートとなる OS ディスクイメージに差分となる実行ファイルや設定ファイル、ドキュメントファイルなどを挿入することで、ビルディングブロック式に VM を構築するシステムである [9]。この技術により、従来の一律同じ構成のシステムを構築する技術と異なり、カスタマイズされた模擬環境の構築が可能となった。この Alfons をベースとして、解析者が観測に必要な模擬環境の定義を作成し、この定義から目的とする模擬環境全体の構築に必要となる各種の設定やパラメータなどを自動生成することで、解析者が望む模擬環境を自動構築するシステムを研究開発した [10]。この技術により、解析者が望む ICT 環境を記述するだけで、必要な模擬環境が構築され、利用することができる。

さらに、大規模で、より複雑で多様なネットワーク構成に対応し、かつ高速な構築を可能とする新たな構築ツールを研究開発した [11]。この最新の構築システムは、論理構成及び物理構成を表現する 2 つのモデルに基づき模擬環境を定義することで、模擬環境のネットワーク設定や、各 VM のハードディスクに囮ファイルや設定ファイルとして書き込むファイルを自動生成し、自動的にネットワークと VM を作成する。この構築システムはネットワーク仮想化技術に対応し、ネットワークセグメント、ファイアーウォール、ルータなどを自動生成し、さらに NAT（Network Address を変換する技術）やルーティングといったネットワーク設定を自動化する。この構築システムは大規模（数百 VM 規模）な模擬環境に対応するため、十分な構築速度の最適化とスケーラビリティの確保を実現しており、従来のシステムでは完了まで数日が必要であった 100 台規模で構成される模擬環境の構築作業を、わずか数時間で完了させることができる。

最新の構築ツールのもう一つの重要な特徴は、一般的な技術者が行う一般的な手順による標準的な設定と同等の手順と設定を自動化していることである。現在では、多数の自動構築手法やツールが利用されているが、これらの自動化ツールによる構築を行った場合、構築された模擬環境に、自動構築による痕跡が残ることがある。攻撃者は、自動構築エージェントの存在や、あきらかに設定ファイルが自動生成されているような内容であると、攻撃者は観測環境であることに気付き、その特徴を観測環境の識別に利用して、次の攻撃時に避けるようになるかもしれない。そこで、STARDUST の自動構築ツールは、多少のオーバヘッドを許容し、一般的な技術者が行うインストール・設定手順に従ったサーバ設定を行うことで、自然な構築手順を模倣して自然なシステムを構築している。

最新の STARDUST NxtGen では、この構築ツールを更に進化させた、設計・構築・テスト・運用までを一貫して管理する DevOps（DEVelopment and OPerationS）ツールを研究開発し、大規模化したシステムの運用に活用している。この進化したテストと運用については、**3.2** で説明する。

2.4　ユーザサービス

解析者が模擬環境を使い効率的に観測し分析を行うには、マルウェアの設置・実行などの事前準備のための VM を操作する仕組みと、マルウェア実行後に攻撃者の行動を分析するために収集されたデータを即座に参照できる仕組みが必要となる。STARDUST では、解析者に対するワンストップのユーザインタフェースで GUI として動作する STARDUST Web と、解析作業を自動化するための REST（REpresentational State Transfer）API を提供している。

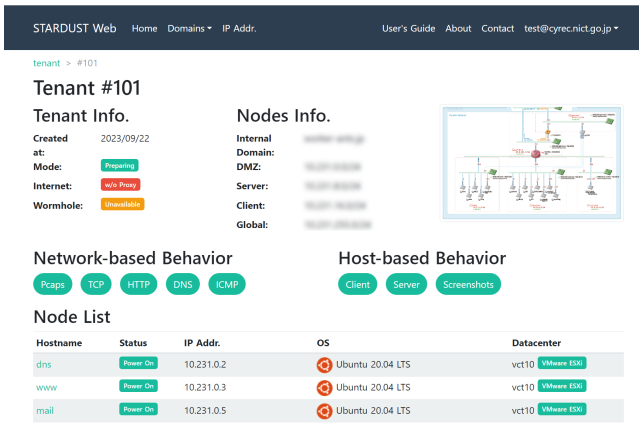

図 3　STARDUST Web

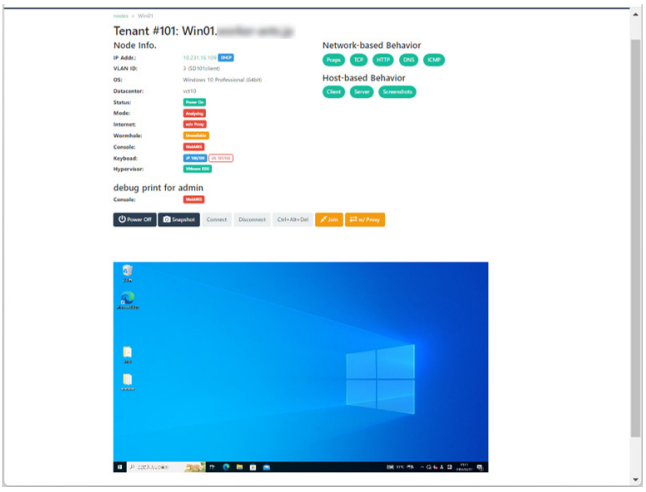

図 4　コンソールからの操作

STARDUST Web は Ruby on Rails フレームワークで実装された Web アプリケーションである。解析者は、STARDUST Web より VM を操作し、収集されたデータを参照することができる（図 3）。VM の電源投入・切断操作、スナップショットの作成・削除等の操作などに加え、VM の仮想コンソールを表示させ仮想マウス・キーボード操作が可能である（図 4）。リモートデスクトップツール経由での接続と違い、対象の VM に侵入した攻撃者からすると、これらの操作はあたかもハードウェア的に接続されたキーボードとマウスから操作しているように見える。

また、STARDUST Web を利用することで、ミラートラフィックのキャプチャ結果の閲覧・ダウンロードや、SF-TAP によるプロトコル解析結果、例えば TCP のデータ（図 5）や HTTP のデータ（図 6）を参照することができる。TCP データ画面では、送信元と送信先の IP アドレスとポート番号及び通信内容を参照することができる。HTTP のデータ画面では、送信元と送信

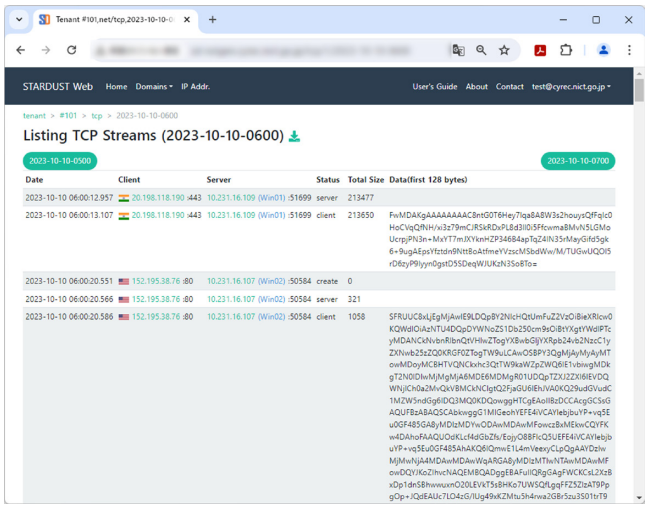

図 5　TCP データの参照

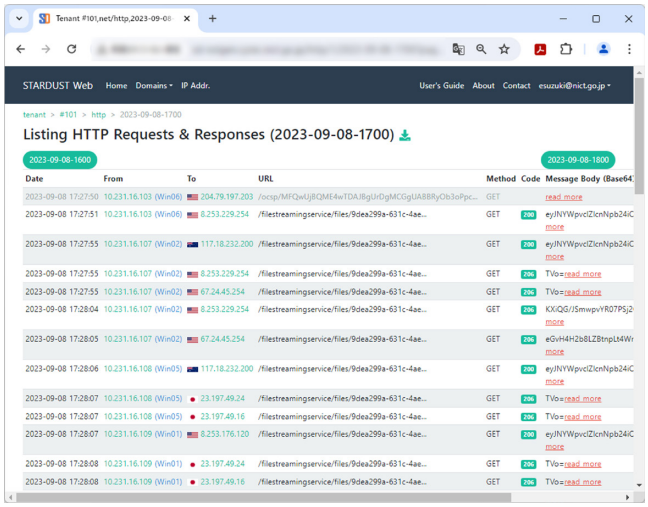

図 6　HTTP データの参照

先の IP アドレスに加え、URL やステータスコードなど HTTP に即した情報が表示され、C&C サーバとの通信内容をリアルタイムに把握することができる。また、収集された Client 情報画面（図 7）では、ゲスト OS 内で動作するプロセスの一覧を参照することができ、各プロセスがどのような通信をしているかが表示される。この情報は、ゲスト OS 内で動作するマルウェアの挙動の把握に使われる。さらに、収集された連続する大量の VM の仮想スクリーンショットから動画を生成し、大きな変化があった画像を抽出しインデックスを作成し表示している。このスクリーンショットのインデックスを作成することで（図 8）、攻撃者が VM の遠隔操作をした際の着目すべき画像に絞り参照することが可能となり攻撃行動の発見を容易にし、さらに動画として表示させることで攻撃者の行動を把握できる。

ユーザインタフェースとしては STARDUST Web のほかに、スクリプト等から STARDUST の

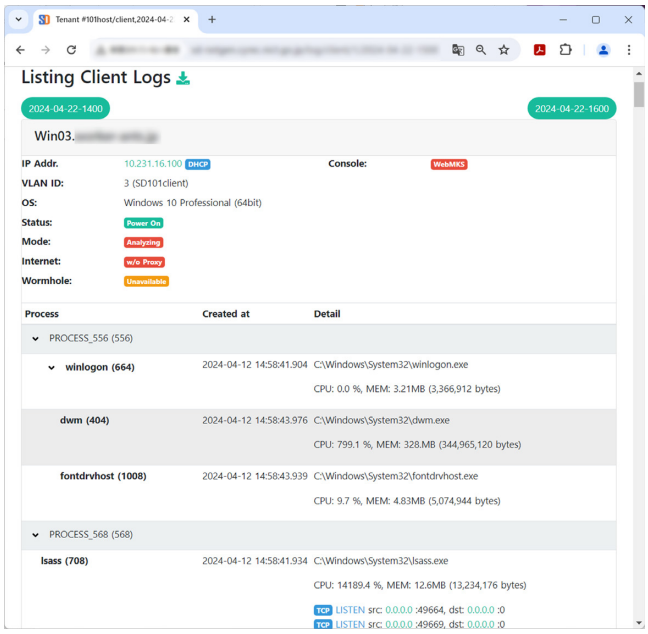

図 7　クライアント情報の参照

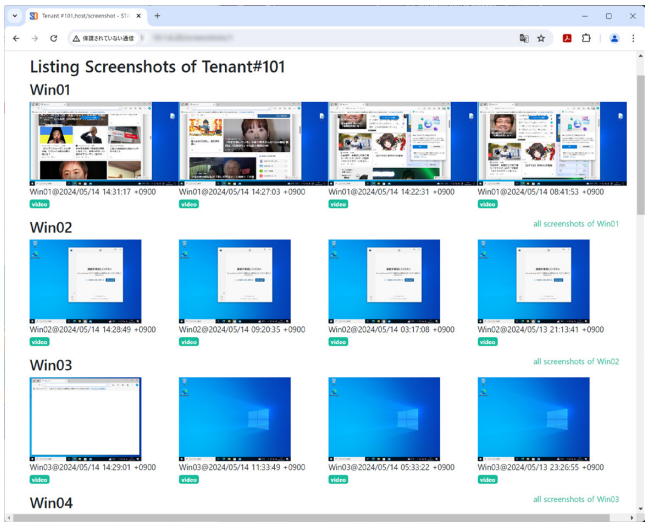

図 8　スクリーンショットの一覧

操作やデータのダウンロードを可能とする REST（REpresentational State Transfer）API を提供している。解析者は、この REST API を使うことで、例えば、観測を開始した時刻から終了時刻までのすべてのトラフィックデータを一括ダウンロードし、それらのデータを処理するスクリプトを作成することができる。また、感染によって汚れた模擬環境内の全ての VM を、REST API を使って感染前の状況にスナップショットのリバート処理を実行することで、環境をクリーンな状態に戻し、次の観測に備えるといった自動化を実現するスクリプトを実装することも可能である。このように、REST API を使い作業を自動化することで解析作業を効率化することができる。

さらに、STARDUST NxtGen では、より先進的な

Web フレームワーク Nuxt.js で実装した新たな Web フロントエンドインタフェースを研究開発し提供した。この新たな Web インタフェースは、利用者の利用体験を向上させることを目的として実装された。Nuxt.js はバックグラウンドで処理される非同期通信による画面作成処理を行うクライアントサイドレンダリングを Web ブラウザ上で行うことが特徴である。大量のデータを表示させる場合、データ全体を受信してから表示すると処理に時間がかかり、遅延が大きい。そこで、データの一部を受信し、その一部分の画面を順次生成し逐次表示することで、見かけ上のレスポンスをデータ量に関係なく高速化させることができる。また、サーバサイドで複数のサービスから取得したデータを使い画面を生成するサーバサイドレンダリングにより、STARDUST Web 本体のサービスだけでなく、他の補助的な観測システムを組み合わせたより高機能な UI を実現している。

3　STARDUST NxtGen の特徴

プロジェクト発足時より 10 年以上継続的な研究開発してきた旧 STARDUST であったが、物理的な機器の老朽化や基盤ソフトウェアの旧式化に伴い、新規にバージョンアップした STARDUST NxtGen の研究開発に着手し 2023 年度より運用を開始した。旧 STARDUST に対してさらに以下 3 つの特徴を実現する。

1. 基盤技術の更新とアーキテクチャの刷新
2. テストと監視の自動化と通知
3. 隔離環境内の VM に対する能動的なデータ収集と操作

ここでは、上記の 3 つの特徴について説明する。

3.1　基盤技術の更新とアーキテクチャの刷新

10 年前に構築された旧 STARDUST のハードウェアの技術的な進歩に伴い、STARDUST NxtGen は、より高性能・大容量のサーバ・ストレージで構成され、より高速なネットワークで接続されている。ハードウェアの高性能化により、より大規模な模擬環境を用いた誘引・観測が可能であり、その模擬環境で発生した大量のデータを漏れなく収集・蓄積し、高速に分析することが可能となった。また、ネットワークストレージの高速化は、頻繁に発生する VM の構築やスナップショットの処理といった、通常のクラウドサービスとは異なる処理を必要とする STARDUST の高速化に大きく貢献しており、解析や運用業務の効率化と利便性の向上に寄与している。

さらに、アーキテクチャも以下の 2 点が変更されている。

1. ネットワーク仮想化技術の導入
2. サービスのコンテナ化

STARDUST NxtGen では、旧来の物理スイッチやルータに変わり、ネットワーク仮想化製品である VMware NSX を用いてネットワークが構成されている。旧 STARDUST では、ネットワークはネットワーク技術者によって手動で静的に作られており、ネットワーク構成は物理的な設置や結線に依存していた。さらにルーティングテーブルや VLAN ID の制約によって、提供可能な模擬環境の規模や数が制限されていた。一方、STARDUST NxtGen では Software Defined Network（従来の物理ルータや物理スイッチなどネットワークを構成する機器をソフトウェアで仮想化し制御する技術）をベースとするネットワーク仮想化プラットフォーム VMware NSX を利用している。VMware NSX が提供するオーバーレイネットワークにより物理的・地理的に離れたホスト間であっても透過的に同一ネットワークとして接続することができ、ホストの構成変更（増設など）や離れたホストとの連携も容易である。また、仮想スイッチや仮想ルータの配備と結線や、ネットワークのセグメント、IP アドレス、外部ネットワークとの接続に使われる VLAN、ネットワークトラフィックのミラーなどの設定や、ルーティング、NAT、ファイアーウォールなどの設定が、すべて動的にかつ自由に設定でき、柔軟なネットワークを物理的な制約を受けず即時に構築できる。この結果、必要な時に指定された設定で、模擬環境の構築ツールと連動しネットワークを自動的に構築することが可能となった。

次に、旧 STARDUST は、10 年近く研究開発を行い機能拡張することで、19 サーバに機能が分散するなど構成が複雑化し、旧サーバ群から新しいサーバ群への移行も困難となっていた。そこで、STARDUST NxtGen では、旧 STARDUST のサービスを実装するソースコードを整理し、コンテナ技術のひとつである Docker コンポーネントとしてリファクタリングすることでアプリケーションと動作環境を整理した（図 9）。すべての STARDUST を構成するサービスを Docker コンポーネント化し各アプリケーション設定（IP アドレスやログ保管ディレクトリ等）を統一することで、新規サービスの構築作業、サービスの起動・停止、ソースコードのアップデート作業等が簡略化され、より安定的な運用が実現できた。このリファクタリングによるコンポーネント化と設定の整理は、次のテスト・監視の自動化を可能とした要素のひとつでもある。

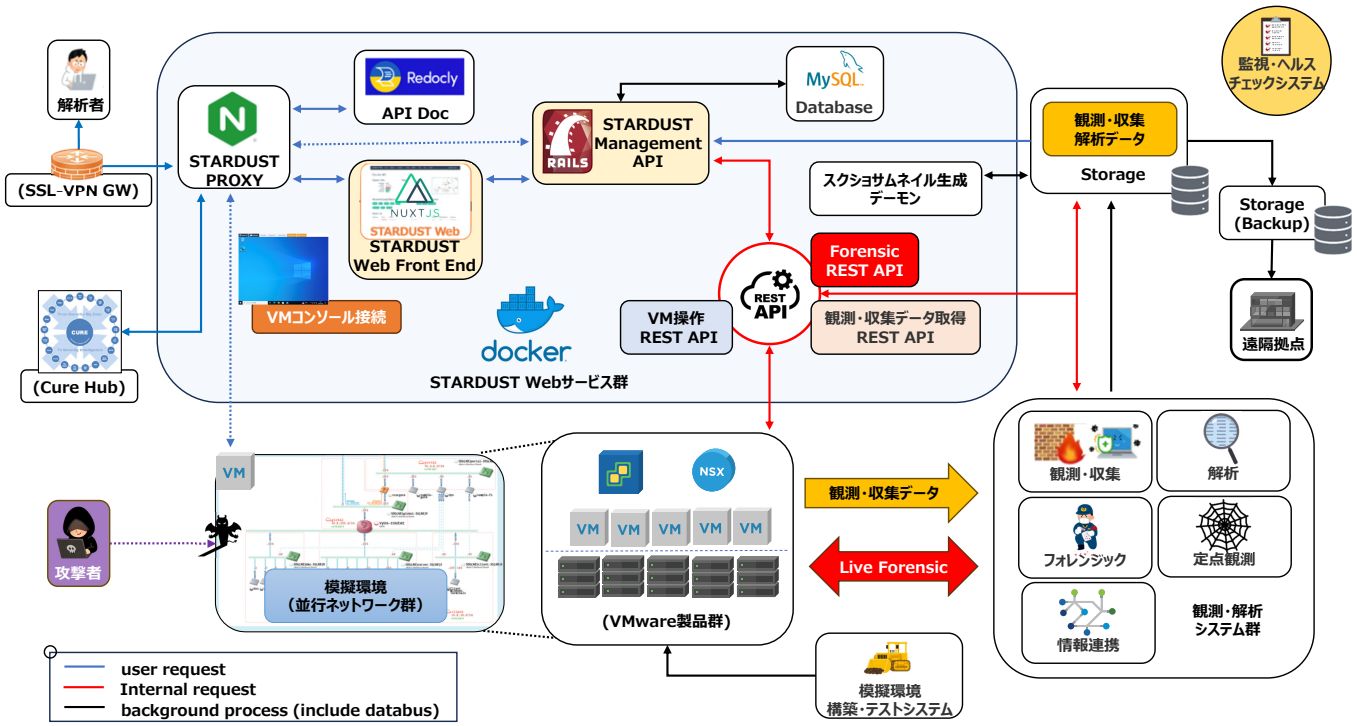

図 9　STARDUST NxtGen の内部構成

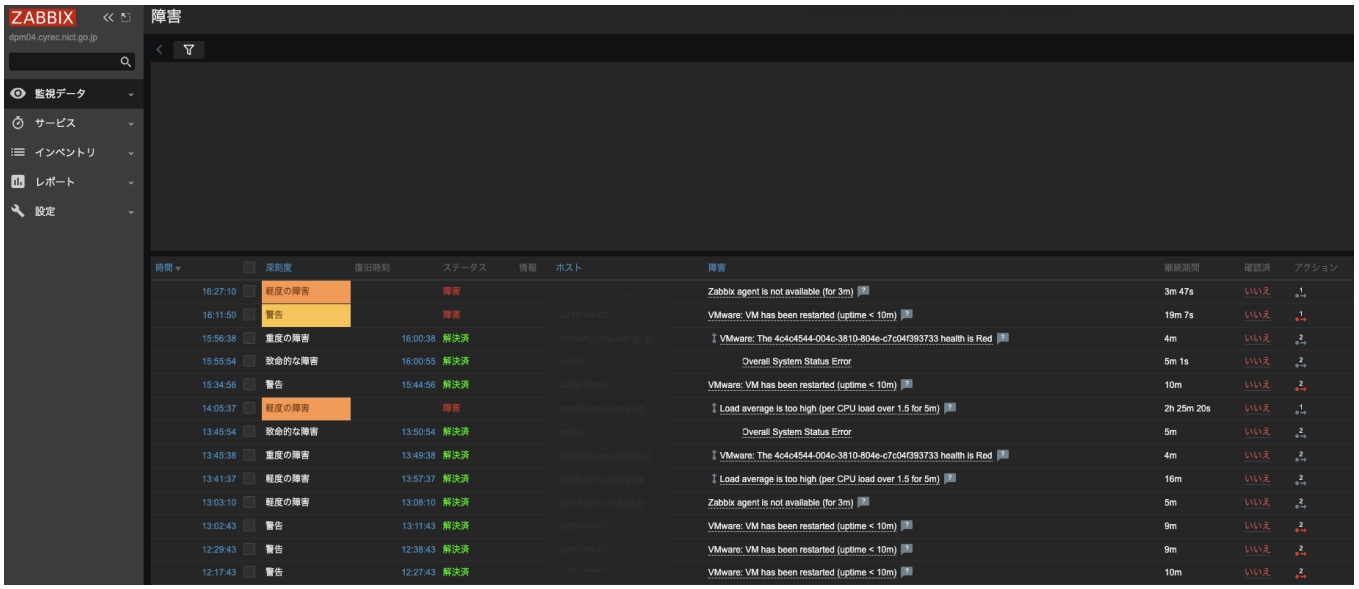

図 10　Zabbix 監視による障害検知

3.2　テストと監視

大規模化しユーザ数が増えた STARDUST NxtGen では、健全性と可用性を担保するため、構築された模擬環境のテストとサービスの監視を自動化し運用監視の強化を実現している。旧 STARDUST においても、統合監視ソフトウェア Zabbix を使ったサーバやネットワーク機器などインフラストラクチャの自動監視を実施していた（図 10）。

しかし、STARDUST は完成されたシステムではなく、常に開発・構築・運用が短いサイクルで繰り返されるシステムである。頻繁に新しい模擬環境が構築・提供され、短いサイクルでサービスの機能強化が行われる。このため、インフラストラクチャの定常的な監視だけでなく、模擬環境に対する提供前のテストや、サービスに対する構築時のテストと定常的な監視が必要となる。

自動構築ツールで模擬環境を作成した時、様々な理由により正しく構築されない場合がある。例えば、模擬環境内のサーバにパッケージをインストールする時、パッケージが壊れていることや、バージョンアップに

表 1　テスト項目概要

大項目	中項目	概要	検査項目数
仮想ネットワーク統合基盤	単体テスト（自動）	模擬環境の仮想ネットワークコンポーネントであるゲートウェイやセグメント、ファイアーウォール等が事前定義通りに構築、設定されているかを検査	9 項目
仮想マシン統合基盤	単体テスト（自動）	事前定義通りに仮想マシンが構築され、正常に起動しているかを検査	20 項目*1
模擬環境	単体テスト（自動）	仮想マシンの IP アドレスやサービスコンポーネントが事前定義通りに設定され、ライセンス認証等の処理が完了しているか等を検査	76 項目*1
	結合テスト（自動）	各仮想マシンの模擬環境内外への通信や各種サーバサービスへのアクセス、並行稼働する他の模擬環境へアクセスできないか等を複合的に検査	34 項目*1
	結合テスト（手動）	SSL-VPN 経由でユーザが模擬環境にアクセスできるか、模擬環境内の GUI 操作等の一部操作を手動で検査	6 項目
	システムテスト（自動）	模擬環境から収集する各種観測データが STARDUST Web から参照、ダウンロードできるか、Web から仮想マシン操作やコンソール表示等ができるかを検査	32 項目

*1 既定仮想マシン台数の模擬環境の場合（仮想マシン台数に応じて増減）

表 2　監視項目概要

大項目	中項目	概要	監視項目数
Zabbix 監視	ハードウェア監視	STARDUST 基盤として稼働するネットワーク、サーバ、ストレージ機器等の正常性を監視し、異常時に通知	*1
アラームチェック	アラーム監視	仮想基盤の統合管理ソフトウェアから報告されるアラームを集約し通知	–
サービスチェック	サービス監視	STARDUST が提供するネットワーク、サーバサービスへの接続性や、サービスコンポーネントのレスポンスや稼働状況、データベースバックアップ等のバックエンド処理等の正常性を確認し、異常時に通知	359 項目*2
リソースチェック	サーバリソース監視	STARDUST サービスを提供するサーバのリソース（CPU や Memory、Disk 使用率等）を常時監視し、事前定義する閾値を超えた場合や、過去データを基準とした単位時間あたりの急激なリソース状況の変動を検知した場合に通知	70 項目*2

*1 機器ごとに設定するテンプレートをもとに各機器あたり数十～数百項目を監視
*2 執筆時点の監視項目数

伴い設定ファイルのフォーマットが変更されて構築ツールが追従していないことがある。また、Windows サーバや PC の構築の際、ライセンス認証に失敗することがまれに発生する。構築の失敗を発見するため、旧 STARDUST では手動で模擬環境の動作テストを行っていた。STARDUST NxtGen では、より高速な VM の生成が可能となり、また大幅に VM 数が増えたため、手動での模擬環境に対するテストはボトルネックとなる。そこで、STARDUST NxtGen では、模擬環境に対して以下の自動化されたテスト（一部手動を含む）が行われる（表 1）。

- 単体テスト：VM のネットワーク設定やインストールされたサービスが正しく動作しているかを検証
- 結合テスト：VM を模擬環境ネットワークに接続し他のサーバのサービスに正しくアクセスできるかなどを検証
- システムテスト：構築された VM のミラートラフィック等のデータが正しく取得されているか、STARDUST Web から正しく VM にアクセスできるかを検証

これらのテストは、構築ツールに与えた模擬環境の定義に基づきテストが行われ、定義に従った模擬環境が構築されているかどうかを検査する。

STARDUST を構成するサービスのテストや監視では、Zabbix を使ったインフラ監視に加えサービス・アプリケーションレベルの監視を行っている。リファクタリングの際に、全サービスコンポーネントの整理を

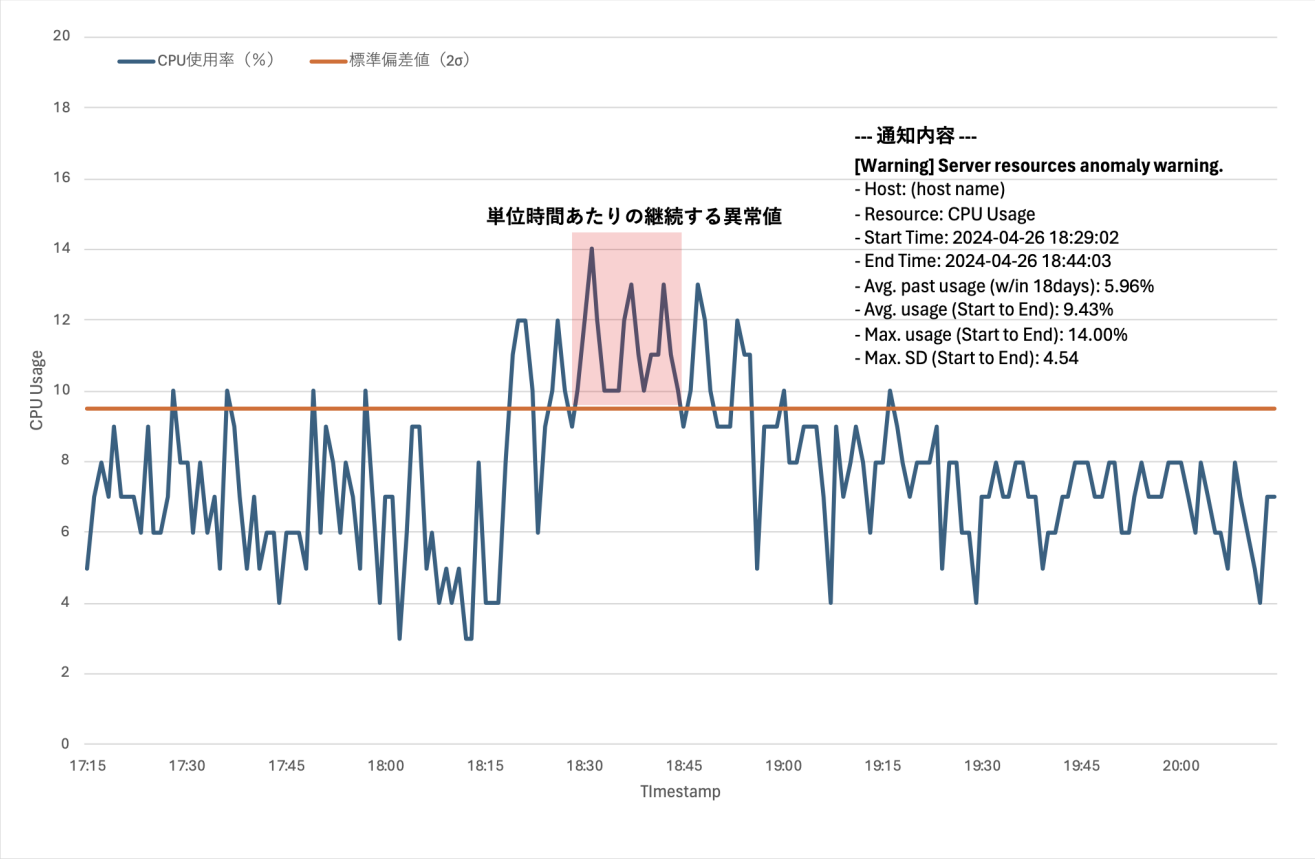

図 11 単位時間あたりの異常値による障害検出

行い、各サービスに必要なテスト・監視項目を抽出し、監視･テスト自動化ツールを設計･実装した（表 2）。例えば、全てのサービスがアクセスできるか、データが正しく取得されているか、ログが正しく記録されているかなどを定常的に監視している。また、サーバやネットワーク機器が故障する、CPU 使用率が極端に増える、メモリの残量が極端に減る、ディスクの消費率が極端に増えるなどのイベント発生に加え、蓄積した監視データを基に単位時間当たりの継続する異常を検出すると、運用者に対して Slack 等のコミュニケーションツールを使って通知される（図 11）。これらのテスト・監視と通知の自動化は、より効率的で確実な運用を実現し、STARDUST の健全性と可用性の確保に貢献している。

3.3　隔離環境内の VM に対する能動的なデータ収集と操作

STARDUST の模擬環境は、攻撃者が侵入した VM からの攻撃を防ぐため、攻撃者誘引を始める前に完全に隔離される。このため、模擬環境内の VM に対し外部から干渉することはできず、環境内で発生するトラフィックや、VM 内のエージェントから定期的に送信されるホスト情報を受動的に収集するだけであった。しかし、より有意義な観測結果を得るためには、解析者が望む適切なタイミングで適切な情報、例えば C&C サーバからコマンドが送られレジストリ書き換えが発生した瞬間のレジストリを取得することや、バッファオーバーフロー攻撃が行われた直後のメモリイメージを取得することが必要となる。もし、これらの情報を定期的に取得すると、データサイズが膨大となるためデータ送信に多くのリソースが消費され、さらに、そのデータ送信の存在により攻撃者に観測事実を察知される危険性がある。

そこで、攻撃者に秘匿性が高く隔離した状態を維持しつつ VM との安全な通信が可能となる技術、VM-Hypervisor 間通信を使って能動的に VM からのデータ収集と VM の操作を実現する機能 Live Forensic API を研究開発した。解析者は、この Live Forensic API を利用すると（図 12）、以下のような操作を隔離された VM に対し任意のタイミングで実行可能である。

1. ファイルのアップロード、ダウンロード
2. 特定のプロセスのメモリダンプ
3. 特定のレジストリの取得、書き換え
4. 任意プログラムの実行と実行結果の取得

一般的なサイバー攻撃のインシデント対応では、侵入された後の調査として、侵入された PC のハードディスクから証跡を収集することが行われる。調査に使われる証跡には、システムディレクトリ、設定ファ

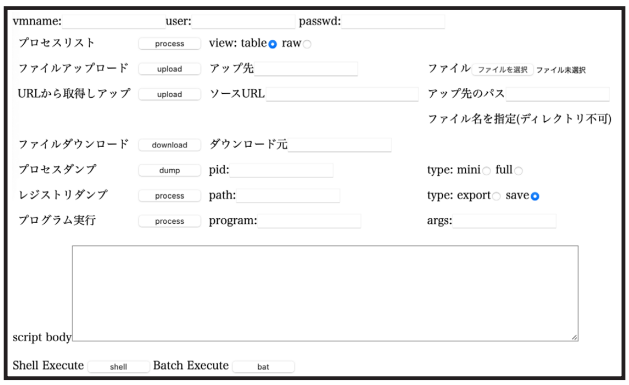

図 12　Live Forensic API の呼び出し画面

イル、自動起動ファイル、テンポラリファイル、ログファイル、レジストリなどが含まれる。STARDUST NxtGen では、隔離中の VM からバックグラウンドで仮想ハードディスクの複製を行い仮想ハードディスクから証跡を収集する機能を有し、攻撃者が活動する VM の動作に全く影響を与えず密かに証跡を取得することができる。

これらの Live Forensic API を使い情報を収集しつつ必要な操作、例えば攻撃者の目的に沿ったより興味を引くファイルをアップロードする、などを行うことで長期の攻撃観測を継続させることができる。

4　観測事例

ここでは、STARDUST で観測したマルウェアの紹介と、観測事例として実際に STARDUST 上での観測事例について述べる。特に、マルウェア単体の解析だけでは得ることが不可能な、STARDUST の特徴を生かした長期的な模擬環境を用いた解析により、実際に観測できた攻撃者の行動について紹介する。

4.1　観測対象マルウェア

当研究室で STARDUST を使用し解析した実績のある主なマルウェアファミリーは下記のとおりである。

- XWorm
- Warzone RAT
- Remcos RAT
- AgentTesla
- GuLoader
- Formbook
- AsyncRAT
- Nanocore
- Ave Maria RAT
- SystemBC
- njRAT
- Quasar RAT

STARDUST では、攻撃者が遠隔で操作できる RAT 系のマルウェアを中心に解析しているが、サンドボックス製品やマルウェア解析者が使用する一般的な動的解析では困難な長期観測が可能であるため、RAT 系以外のマルウェアファミリーも対象にして解析を行っている。

観測の対象とするマルウェアは主に、NICT に実在するメールアドレス宛に届いたメールから抽出できるマルウェアの中から選別している。その中には無差別型攻撃（詐欺等を目的とした広範囲にばらまかれる攻撃）として届いたメールから抽出したマルウェアもあれば、NICT に対する標的型攻撃の初期侵入を意図したと思われるメールから抽出したマルウェアも含まれる。NICT 宛のメールから抽出したマルウェア以外にも、Virus Total [12] や Malware Bazaar [13] といったマルウェアリポジトリに投稿されているマルウェアについても STARDUST の観測対象としている。

STARDUST を利用した解析では、単に入手したマルウェアを STARDUST 上で実行し観測するだけで有意義な結果は得られない。STARDUST 上で有意義な解析結果を得るために、解析者はまずマルウェアの特徴を把握し、攻撃者を知るといった事前準備を行う。例えば、まず一般的な表層解析・動的解析・コード解析を実施し、マルウェアの動作環境（OS のバージョンやライブラリ等）、マルウェアの機能と挙動、接続先の C&C サーバの IP アドレスやドメイン名といった特徴を把握する。解析者は、これらの情報を基に STARDUST に環境を整えた後に、マルウェアを実行し解析活動を行う。

4.2　STARDUST で得られた攻撃者の活動

実際に上記のようなマルウェアの活動を観測した中で、攻撃者の活動が観測できた事例について紹介する。今回紹介する事例は、「AsyncRAT」と呼ばれる RAT 系のマルウェアの観測を実施した際に得られた成果である。

AsyncRAT は、標的型攻撃を行うグループの間で人気の高いマルウェアである。標的型攻撃メールに添付されたファイルをクリックすることによってターゲットとなるホストに感染し、標的のホストを遠隔から自由自在に操作する。AsyncRAT の機能は多岐にわたり、その主な機能はチャット通信やファイルのダウンロード、カメラの利用やデスクトップ画面の録画などが挙げられる。

次に、実際に STARDUST 上に誘引された攻撃者が使用した AsyncRAT の活動について紹介する。

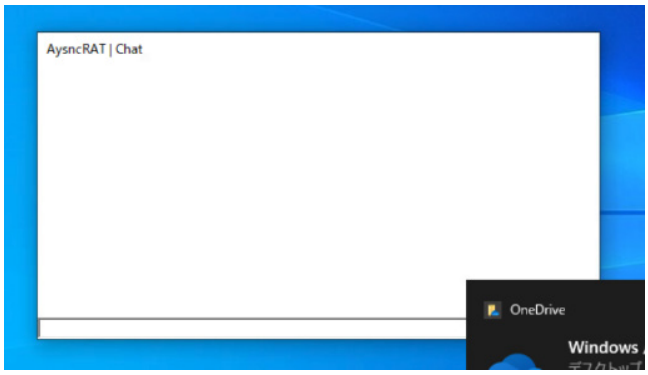

図 13　AsyncRAT のチャット通信機能

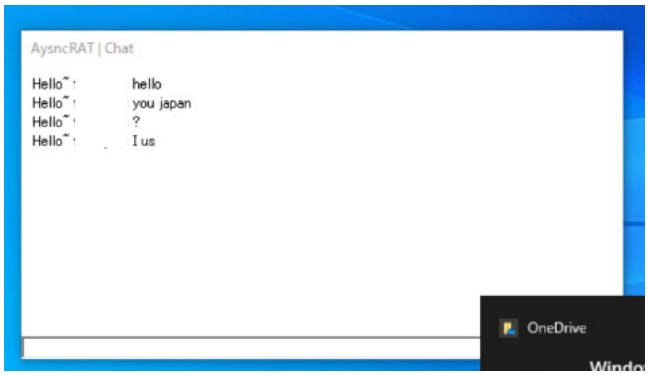

図 14　攻撃者によるチャットメッセージ

4.2.1　チャット通信

STARDUST で誘引に成功した攻撃者は、AsyncRAT のチャット機能を用いた通信を行ってきた（図 13）。

AsyncRAT のチャット機能では、Windows のデスクトップ画面上にチャット用のウィンドウが表示され、遠隔で操作している攻撃者とチャットのやり取りをすることができる。次に、実際に攻撃者が本機能を用いて送信してきたメッセージの一部を示す（図 14）。

攻撃者の送信したメッセージから、攻撃者は感染端末に侵入後その環境がどの国なのかを確認していることが分かる。また、本メッセージに加えてその後次々とメッセージを送信してきた（図 15）。

この解析事例では、攻撃者が何らかの目的をもって、侵入した PC の利用者に対してチャットを用いてコンタクトするという行動を観測することができた。このような観測結果は、攻撃者の行動を観測するという開発目的を STARDUST NxtGen で実現したことにより得られたと考えることができる。

4.2.2　ファイルのダウンロード

チャット通信機能以外にも、EXE ファイルをダウンロードする活動が観測された（図 16）。

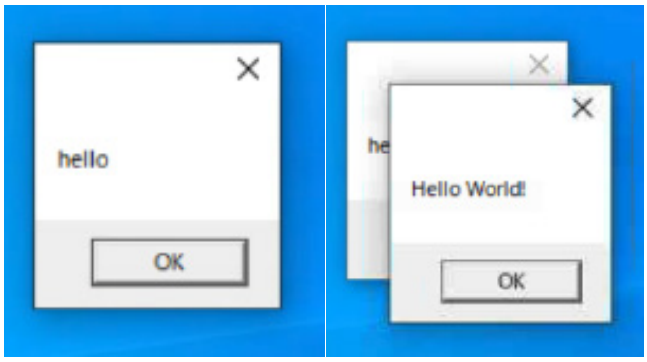

図 15　さらなる攻撃者からのメッセージ

図 16　攻撃者によるファイルダウンロード

5　まとめ

STARDUST は、実際の攻撃者を欺瞞・誘引し、解析者による観測の事実に気付かれずに長期にわたり攻撃者の行動を観測するための基盤である。攻撃者を模擬環境と呼ばれる観測用の ICT 環境に誘引し、秘匿性の高い観測・分析システムによりデータを収集する。解析者が望む適切な模擬環境を自動構築するツールを有し、解析者は STARDUST Web にアクセスして STARDUST を操作する。2023 年度より運用が開始された STARDUST NxtGen は、より多数の解析者に対して大規模で柔軟な模擬環境を提供することができる。大規模化した STARDUST の健全性と可用性を確保するため、テストと監視を強化した。さらに、利便性を高め解析の高度化を実現する VM-Hypervisor 通信を利用した Live Forensic API の研究開発を行い、試行を開始している。

サイバーセキュリティ研究室の行う STARDUST を使った攻撃者誘引による解析により、多数のサイバーセキュリティに関する知見が蓄積されており、セキュリティコミュニティにその知見を提供している。また、そこで得られた通信データは、サイバーセキュリティ研究室にて研究開発されているセキュリティ情報融合基盤 CURE に観測情報として提供し活用されている [14]。

外部機関との連携・共同研究においても、STARDUST を活用した研究成果が得られている。例えば、STARDUST で得られた組織内ネットワークへの侵害活動を観測したデータは、マルウェア対策研究人材育成ワークショップ（MWS）より、BoS データセットとて提供されている [5]。また、サイバーセキュリティ研究室といくつかの企業、大学と共同研究を実施し、STARDUST を利用した共同研究が行われた [15]。

さらに、STARDUST で収集されたデータを匿名化処理し、模擬環境内部に関する情報を秘匿し外部提供し、攻撃者による実データを使った評価に役立てた研究も行われている [16][17]。2023 年の CYNEX アライアンスの発足に伴い [6]、STARDUST NxtGen における模擬環境は既に旧 STARDUST の実績の 2 倍近い提供数となった。また、CYNEX Co-Nexus A で提供するサイバー攻撃観測の用途だけではなく、Co-Nexus E のセキュリティ製品評価の環境としても利用を開始されている。

今後は、スケーラブルで柔軟な ICT 環境を即時に構築できる特性を活かし、より汎用的で利便性の高いセキュリティ実験のインフラを研究開発したいと考えている。このためには、サイバーセキュリティ研究に必要となる様々な機能を STARDUST に取り取り込む必要があると考える。例えば、通信内容の解析機能の充実や、実行中のマルウェアの解析機能との連携を実現することで、より高度な観測・解析が可能となると考える。さらに、これまで STARDUST は高度な技術を有する解析者による高度な解析を主な対象としてきたが、今後は初心者も含めより広いユーザを対象とし利用範囲を拡大したい。このために、よりユーザインタフェースを工夫するとともに、解析ノウハウを蓄積し解析コミュニティに還元できる仕組みについて考えたい。

【参考文献】

1 Mandiant, Mandiant APT1: Exposing One of China's Cyber Espionage Units, 2013.
2 FireEye. Operation Quantum Entanglement, 2014.
3 Kaspersky Lab., New Activity of the Blue Termite APT, 2015.
4 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, pp.472–479, 2017.
5 寺田 真敏, 佐藤 隆行, 青木 翔, 亀川 慧, 清水 努, 津田 侑, "研究用データセット「動的活動観測 2018」," コンピュータセキュリティシンポジウム 2018 論文集, pp.145–150, 2018.
6 国立研究開発法人情報通信研究機構, "日本のサイバーセキュリティの結節点 "CYNEX" アライアンスを発足," 情報通信研究機構ニュースリリース (https://www.nict.go.jp/press/2023/10/02-1.html), 2023 年 10 月 2 日.
7 Yuuki Takano, Ryosuke Miura, Shingo Yasuda, Kunio Akashi, and Tomoya Inoue, "SF-TAP: Scalable and Flexible Traffic Analysis Platform Running on Commodity Hardware," Proceedings of the LISA '15, pp.25–36, 2015.
8 安田 真悟, 三浦 良介, 高野 祐輝, 宮地利幸, "Alfons: マルウェア解析の為の高詳細な環境構築システム," 電子情報通信学会技術研究報告, vol.114, no.523, ICM2014-77, pp.139–144, 2015.
9 安田 真悟, 金谷 延幸, 津田 侑, 太田 悟史, 三浦 良介, 井上 大介, "能動的攻撃観測環境における端末の自動駆動システム," 電子情報通信学会技術研究報告, pp.299–304, 2019.
10 金谷 延幸, 津田 侑, 遠峰 隆史, 安田 真悟, 井上 大介, "環境特徴情報による模擬環境自動構築効率化手法の提案と実装," 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 2018.
11 金谷 延幸, 津田 侑, 遠峰 隆史, 鈴木 悦子, 佐藤 茂, 田中 秀一, 井上 大介, "アジャイル型のサイバー攻撃解析用模擬 ICT 環境構築・管理システム," コンピュータセキュリティシンポジウム 2022 論文集, pp.1163–1170, 2022.
12 VirusTotal, https://www.virustotal.com/
13 Malware Bazaar, https://bazaar.abuse.ch/
14 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, pp.637–644, 2020.
15 細見 勇介, 津田 侑, 鄭 俊俊, 毛利 公一, "標的型マルウェアの通信先情報に基づく C&C サーバ監視による攻撃誘引," 2022 年暗号と情報セキュリティシンポジウム, 2022.
16 海野 由紀, 森永 正信, 及川 孝徳, 古川 和快, 金谷 延幸, 津田 侑, 遠峰 隆史, 井上 大介, 鳥居 悟, 伊豆 哲也, "標的型攻撃の被害範囲を迅速に分析するネットワークフォレンジック手法の提案," コンピュータセキュリティシンポジウム 2018, pp.1170–1177, 2018.
17 海野 由紀, 及川 孝則, 金谷 延幸, 津田 侑, 遠峰 隆史, 井上 大介, 鳥居 悟, "高速フォレンジック技術を利用した標的型攻撃の挙動分析," 2020 年暗号と情報セキュリティシンポジウム, 2021.

金谷 延幸 (かなや のぶゆき)
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
主任研究員
セキュリティ

鈴木 悦子 (すずき えつこ)
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
セキュリティ

中村 大典 (なかむら おおのり)
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
セキュリティ

梅村 勇貴 (うめむら ゆうき)
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
セキュリティ

佐藤 茂 (さとう しげる)
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
セキュリティ