サイバーセキュリティレポート 1

なぜMITRE ATT&CKが注目されるのか？最新動向の背景とは

なぜMITRE ATT&CKが注目されるのか？最新動向の背景とは

NTT コミュニケーションズ株式会社
エバンジェリスト
竹内 文孝

本連載では、国内外のサイバーセキュリティについて、皆様にお伝えしたい最新のトピックスや事例を解説していく。第1回目はMITRE ATT&CK の最新動向を紹介する。

MITRE ATT&CK（マイター アタック）とは

米国連邦政府が資金を提供する非営利組織で、世界中の脆弱性情報に対して識別子を付ける「CVE」の運用等を行う MITRE は、2013 年から ATT&CK（敵対的な戦術とテクニック、共通知識）を公開している。脆弱性を悪用した実際の攻撃を戦術（Tactics）と技術／手法（Technic）の観点で分類したナレッジベースであり、防御対策のツールとして使用されるものだ。2018 年頃からペネトレーションテスターや SOC アナリストのセキュリティプロフェッショナルから注目されるようになり、2020 年頃からは一般企業においても活用が進んでいる。

MITRE ATT&CKのこれまでの歩み

ATT&CK は四半期に一度もしくは不定期にバージョンアップしており、2021 年 4 月 29 日に最新版「バージョン 9」がリリースされた。ATT&CK における「戦術」は現在、「Enterprise 向け」と「Mobile 向け」「ICS（産業制御システム）向け」に分類されている。今回はこの 3 分野でテクニック、グループ、ソフトウェアがアップデートされたほか、「Cloud」マトリクスにおけるデータソースを刷新した。巧妙化し続ける攻撃手法やその対策技術は日進月歩で進化しており、これらに対応した内容更新が要求されるからである。今回の最新版では、14 の戦術、185 のテクニック、367 のサブテクニックが示された。また、「Cloud」マトリクスのアップデートでは Enterprise マトリクスに掲載されているクラウドベースの戦術と技術／手法が整理されており、2019 年 10 月のリリースより、AWS、Azure、GCP をカバーしてきたが、今回これらを一つの「IaaS」プラットフォームに統合し、同一のテクニックとサブテクニックのセットを共有できるようにした。また、有益なデータソースを増やすため、IaaS、SaaS、Azure AD、Office365 に、Google Workspace プラットフォームを追加している。

このATT&CKフレームワークは、セキュリティ製品の評価などで活用されている点にも注目していただきたい。これを促進するための取り組みの一つが「MITRE Engenuity ATT&CK評価」である。この評価は、セキュリティ対策製品のベンダー等が自社製品の能力を一定の指標で検査し把握することを目的に実施されるもので、検査対象となる製品に対して ATT&CK が定義する攻撃シナリオに沿って実際の攻撃を実行し、それがどのように検知および防御できるかを検証する。2018 年には APT3、2019 年には APT29、そして 2020 年には金融サービスやホスピタリティ企業を侵害した 2 つの脅威アクターである Carbanak や FIN7 という実在する攻撃グループの攻撃手法に基づいて評価が行われた。また上記の他、ATT&CK はサイバー攻撃の流れと手法を体系化したフレームワークとして、一般企業の CSIRT における脅威インテリジェンス、さらには自社の防御態勢のギャップ分析やその対策可否、及び攻撃の成功度合いを測る評価ツールにも活用されている。

なぜ今MITRE ATT&CKが必要なのか？何が起こっているのか？

ATT&CK が注目されている背景には、サイバー攻撃に対する危機感の高まりがある。今年に入って重要インフラを狙ったサイバー攻撃が相次ぎ発生し、2021 年 5 月には米国最大級の石油パイプラインが金銭目的のハッカー集団による外部からの

ランサムウェア（身代金要求型ウィルス）の攻撃により、5日間にわたり操業停止に陥った。この他にも北米に複数の工場をもつブラジルの世界最大の食肉加工会社でもランサムウェアにより工場が操業停止となり、同社は犯行グループに1,100万ドル（約12億円）相当の身代金を仮想通貨で支払ったと発表している。このような攻撃には海外の国から支援を受けている犯罪組織集団の関与も疑われており、攻撃を受ける側も国主導で対応を行っている。アメリカの司法省は連邦捜査局（FBI）が一度はハッカー集団に仮想通貨で支払われた身代金を奪還したことを発表するなど、その攻防がますます激しくなると想定される。一方、日本では警察庁が2022年よりサイバー犯罪捜査の新組織を立ち上げることを表明しており、今後は法整備をはじめ、人材育成や国家間で連携した捜査への貢献等が急速に進むことが期待される。

このような環境下においてATT&CKフレームワークの戦術分類は、攻撃成立後の初期侵入から始まり、悪意あるプログラムの実行、永続性、特権昇格、防御回避、認証情報アクセス、探索、水平展開、情報収集、C&C接続、情報送信、影響までのプロセスに分けられており、加えて攻撃者情報も備えていることから、サイバー攻撃に対するリスク評価を網羅的に行うためのツールとして各所から注目されているのである。

MITRE ATT&CKの今後

以上の状況を踏まえ、2021年6月にサイバーセキュリティ・インフラストラクチャ・セキュリティ庁（CISA）は多くの企業でのATT&CKフレームワークの活用を促すことを目的の一つとして、新たなガイド「Best Practices for MITRE ATT&CK® Mapping」を公開した。図1は当該ガイドに示される作業ステップとその概要をまとめたものである。このガイドによってATT&CK利用者に対する有効性と運用容易性が向上するため、より一層の普及促進が期待されている。

ATT&CKにおいて、「戦術」は攻撃者が何を達成しようとしていたのか、そしてその理由は何かに注目している。また、「手法／技術」はこの目標をどのように達成しようとしていたのかに焦点を合わせている。これらを適切に定義づけてマッピングするには、攻撃者行動の兆候を探し、異常な振る舞いや疑わしい挙動の連鎖を見つけ出す必要があり、一連の攻撃行動における全体像を理解することが最重要であることをこのガイドでは示している。

米国では現在、ATT&CK forCloudマトリクスを活用したサービスプロバイダ等が増加しており、一般企業は自社のセキュリティ運用業務をアウトソースする傾向にあるという調査結果があることから、今後、サービス提供者側と顧客側の多くの企業がATT & CKフレームワークを活用し、セキュリティ対策の成熟度向上やアウトソース先の評価を行っていくことが予見される。本ガイドはこうしたMSSP事業の質的高度化を推進するうえでも大きな役割を果たすものと言えるだろう。

MITREは今後のロードマップとして、2021年10月にATT&CK for ICSのデータソースをアップデートするほか、「クロスドメイン・マッピング」をリリースする予定としている。攻撃者は理論上の境界線を超えた攻撃手法を次々と編み出している。このため、エンタープライズやクラウド、モバイル、ICSなど異なるドメインやテクノロジースタックに跨った攻撃行動をより深く理解することが不可欠になる。MITREは、領域横断的なマッピングにより、ナレッジベースを組み合わせて使えるようにするための準備を進めており、今後もその動向に注目していくべきである。

	作業ステップ	概要
1	攻撃者の行動の兆候を見つける	敵対者が特定のプラットフォームやアプリケーションをどのように操作したかという兆候を探し、異常な動作や疑わしい動作の連鎖を見つけ出す。最初の侵害がどのように行われたか、また侵害後の活動がどのように行われたかを確認する
2	行動全体を調査する	疑わしい敵やソフトウェアの行動を理解するためのコンテキストを得るためには、さらなる調査が必要になる。オリジナルのレポートで挙動がどのように記述されているかを理解し、ATT&CKのウェブサイトでキーワードを検索して、行動を特定する
3	「戦術」を特定する	レポートに目を通し、敵の戦術と攻撃の流れを特定する。戦術（敵対者の目標）を特定するには、敵対者が「何を」達成しようとしていたのか、そしてその「理由」に注目する
4	「テクニック」を特定する	敵が「どのように」目的を達成しようとしたのか、技術的な詳細を確認する。レポートで観察された行動を確認して、考えられるATT&CKテクニックの範囲をドリルダウンする
5	サブテクニックの確認	サブテクニックの説明が、レポートの情報と一致しているかどうかを確認する。ただしレポートの詳細度によっては、サブテクニックを特定できない場合がある
6	結果を他のアナリストと比較・共有する	戦術、テクニック、サブテクニックが注釈されたレポートをピアレビューすることで、マッピングの精度を改善することができる。また、チーム内でのマッピングの一貫性を高めることができる

図1　MITRE ATT&CKマッピングガイドを活用するための作業ステップと概要

●お問い合わせ先●
wideangle-pr@ntt.com

お問い合わせ先

NTTコミュニケーションズ株式会社

Mail：wideangle-pr@ntt.com

●この冊子は「ビジネスコミュニケーション」2021年8月号より抜粋したものです。
●記載の会社名および製品名は、各社の商標または登録商標です。