INSIGHT PAPER

Mythosが示す、継続的なセキュリティ強化の重要性

Tom Stewart
テクノロジーコンサルティング シニアディレクタ

protiviti®
Global Business Consulting

AnthropicのMythosは、サイバーセキュリティの防御側がこれまで前提としてきた制約を変えつつあります。そして、多くの組織はこれから起こる変化に十分に備えられていません。

これまで長い間、サイバー攻撃が大規模に拡大しなかった理由の一つは、十分に高度なスキルを持つ人材が多く存在しなかったことにあります。脆弱性を見つけ、それを攻撃手法に変換し、さらにそれらを組み合わせて成立させるには、専門的な知識と時間が必要でした。Mythosはこの制約を完全に取り除くものではありませんが、確実にそれを緩め始めています。ここに大きな変化の兆しがあります。

攻撃の基本的な流れ自体は変わっていません。依然として以下の3つのステップで構成されます。

- **ディスカバリー（Discovery）**：ソフトウェアや設定上の不備を見つける
- **武器化（Weaponization）**：それらの不備を実際の攻撃手段として使える形にする
- **チェイニング（Chaining）**：複数の弱点を組み合わせ、意味のある攻撃経路を構築する

Mythosはこのプロセス自体を変えるものではありません。しかし、同じ作業をより高速に、より多くの対象に対して、そして人の手に大きく依存せずに実行できるようになります。

また、Mythosによってこの作業が急激に安価になるわけではありません。大規模に実行するには依然としてコストがかかります。

初期の検証では、あるレガシーBSDシステムにおけるサービス不能攻撃（DoS）の問題を特定するために、およそ20,000ドル相当のトークンが消費されました。これは同様の作業を人間の研究者に依頼した場合と同程度のコストです。見つかった最も重要な問題はヌルポインタ参照でしたが、これは通常、リモートからのコード実行にはつながりません。多くの場合、影響はサービス中断にとどまり、システム全体の侵害には至りません。

これは重要なポイントです。現時点でMythosは、低コストで重大な攻撃手法を大量に生み出しているわけではありません。攻撃に関する基本原則は変わっておらず、専門知識の重要性も依然として高いままです。しかしながら、その変化は目立たないようでいて、非常に大きな影響を持っています。これまで分析者の作業時間に依存していたディスカバリーや武器化、

攻撃者の活動範囲は、もはや人員規模によって制約されるのではなく、徐々にコストによって制約されるようになっています。

チェイニングの一部は、現在ではコンピュータの処理能力を用いて並列に実行できるようになっています。その結果、攻撃者の活動範囲は人員ではなくコストによって決まるようになりつつあります。防御側にとって重要なのは、この点です。問題は単に攻撃が速くなることではなく、攻撃対象となる範囲そのものが拡大し、誰がどの程度の頻度でリスクにさらされるかの考え方が変わることにあります。

対象ごとにコストで測定される作業は、時間で測定される作業とは大きく異なる振る舞いをします。時間が制約である場合、拡大はゆっくりとしか進みません。しかし、コストが制約となる場合には、一度に大規模な展開が可能になります。つまり、攻撃者は一件ずつ順番に対応するのではなく、数千の対象に対して同時に処理を分散できるようになります。その結果、多くの組織が一斉に攻撃の対象範囲に入る可能性が高まります。防御側にとっての本質的な問題はここにあります。作業内容自体は変わらないものの、それを実行できる規模が大きく変化しているのです。

注意力がボトルネックとなっていた

これまで多くの組織では、脆弱性管理は比較的単純なモデルに基づいていました。すなわち、見つかった課題を重大度順に並べ、それぞれを個別の問題として対処するという方法です。この方法は完全ではありませんが、実務上は一定の効果を発揮してきました。

なぜなら、従来は攻撃者にも大きな制約があったためです。それは「注意力」です。複数の弱点を組み合わせて意味のある攻撃経路を作るには、時間と集中力が必要であり、攻撃者はその労力を取捨選択せざるを得ませんでした。すべての環境に対して、あらゆる攻撃経路を追うことは現実的ではなかったのです。

しかし、状況は変わり始めている

攻撃経路分析における反復的な作業の多くが、並列処理によって容易に実行できるようになるにつれ、この制約は弱まりつつあります。その結果、リスクの現れ方そのものが変化してきています。

例えば、ドメインコントローラに至る短い経路上にある中程度の脆弱性は、何にもつながらない脆弱性とは同じリスクではありません。この違いは以前から存在していましたが、現在ではそれを特定し、大規模に活用すること

が容易になったため、その重要性が増しています。

そして、そのような分析を行うツールは、防御側だけでなく攻撃側にも広く利用可能になりつつあります。結果として、両者のコスト構造は似通ってきています。

悪用までの時間は短縮している

脆弱性が公開されてから実際に攻撃に利用されるまでの時間は、ここ数年で継続的に短縮してきており、その傾向は今後も続くと見られます。

かつては数週間かかっていたものが、現在では数日で行われることが多くなっています。価値の高い対象に対しては、数時間で悪用される可能性もあります。攻撃手法の自動化が進むにつれて、この時間はさらに短縮されるでしょう。特に、対象が計算コストに見合う価値がある場合は、その傾向が顕著です。

すべての組織がすぐにこの変化の影響を受けるわけではありません。しかし、二極化はすでに明確になりつつあります。

- **価値の高い組織**：自動化による攻撃の高速化と増加
- **価値の低い組織**：少なくとも短期的には比較的安定した攻撃状況

より大きな問題は、防御側がこの変化に追いついていないことです。
多くの組織は依然として以下のようなスケジュールで運用しています。

- 30日間パッチSLAは依然として一般的である
- 四半期ごとのペネトレーションテストは、すでに数週間前の情報しか提供していない
- 年次評価は、テストが終了する前に環境が大きく変化している可能性がある

これにより、攻撃者の対応速度と防御側の対応速度の間には大きな差が生じています。この差は、Mythosのようなツールによってさらに拡大していきます。

情報開示と悪用のタイムラグは縮まりつつある一方で、防衛側の多くは依然として時代遅れのタイムラインに基づいて対応しています。

継続的なセキュリティ強化

この状況に対する当然の対応は、セキュリティの状態をソフトウェアの信頼性と同様に扱うことです。すなわち、年に数回確認するものではなく、常に維持し続けるべきものと捉えるということです。実際には、継続的なセキュリティ強化とは単一のツールや施策を指すものではなく、業務の進め方そのものの変化を意味します。大きく3つの変化に集約されます。

1. テストは最終工程ではなく、開発プロセスの一部として行う

リリース完了を待つのではなく、開発およびデプロイの過程にテストを組み込みます。具体的には、

- 新しいアプリケーションコードの導入時にテストする
- 新しいインフラの構築時に検証する
- 新たな外部連携の接続時に評価する

その目的は明確です。日常的に発生する問題を早期かつ自動的に検知することです。その結果、人の注意力は、従来の自動化では対応が難しい問題、例えば新しい攻撃経路や業務ロジック上の不備、複雑な連鎖的問題に集中できるようになります。

2. 個々の脆弱性ではなく攻撃経路に焦点を当てる

従来は「この脆弱性はどれほど危険か」という問いが中心でした。一方、継続的なセキュリティ強化では、次の問いに変わります。「どの経路を通れば重要な資産に到達できるのか」。そのために、以下の点を定期的に分析します。

- 脆弱性がシステム間でどのようにつながっているか
- どの経路が重要な資産につながるか
- 攻撃者がどの経路に注力する可能性が高いか

このような分析は従来は難しいものでしたが、現在では実現可能性が高まっています。そして重要な点として、攻撃者の活動範囲を拡大する自動化は、防御側にも活用可能であるという点が挙げられます。

3. **対処の優先順位を単なる重大度ではなく実際の露出に基づいて決定する**

同じ重大度スコアであっても、リスクが同じとは限りません。例えば、

- 重要なシステムに直結する中程度の脆弱性
- 孤立しておりアクセスしにくい高重大度の脆弱性

これらは同じリスクではありませんが、ダッシュボード上では同様に見えることがあります。継続的なセキュリティ強化では、この現実を踏まえて優先順位を見直します。

- 攻撃経路上での露出度が主要なインプット
- 資産の重要性がより重視される
- 単純な重大度スコアよりもコンテキストの重要性が増している

これらが単純なスコアよりも重要になります。現在の多くのツールは、初期設定のままではこの考え方に基づいた優先順位付けを行っていませんが、業界の方向性は明確にそちらに進んでいます。

今何をすべきか

この変化に対応するためには、全面的な変革が必要なわけではありませんが、具体的な行動は必要です。まず、基本的な問いから始めます。現在、自社の環境をどの程度の頻度でテストしていますか。

その頻度は今でも十分と言えますか。テストの実施状況を時系列で整理し、検証間隔が数か月単位であれば、それが現在の環境や脅威に適合しているかを見直す必要があります。その上で、重要な領域から改善を進めます。

- 年次テストを四半期に移行する
- 高価値システムの四半期テストを月次に移行する
- リスクの高い領域での検証間隔を短縮する

同時に、既存の仕組みを活用します。

- CI/CD パイプラインへの自動テストの組み込み
- インフラストラクチャー・アズ・コード環境での検証拡張

継続的なセキュリティ強化とは、変更が生じたその時点でテストを行うことを意味し、変更後に時間が経ってから行うことではありません。

- 変更があれば即時にテストされる仕組みの確立

その目的は明確です。変更が起きた時にテストすることであり、後から確認することではありません。また、ツールの限界を正しく理解することも重要です。

自動化が有効な領域：

- 既知の脆弱性
- 繰り返し攻撃される経路
- 標準化された環境

一方で、次のような領域では限界があります。

- 組織固有の業務ロジックの欠陥
- システム運用に組み込まれた前提条件
- 高度な判断を要する複雑な攻撃経路

その意味するところは明らかです。自動化のみに依存する組織は、重大なリスクを見逃してしまいます。一方、次の両方を組み合わせることで、より広範囲のリスクに対応することが可能になります。

- 広範囲をカバーする自動化
- 深い分析を行う専門家の取り組み

これは最悪のシナリオを前提とする必要はありません。現実的な前提として、資金力のある攻撃者は自動化を用いて活動を拡大してくると想定すべきです。最も迅速に適応する組織は、単にテスト回数を増やすのではなく、より賢く、より頻繁に、そして変化に即した形でテストを行う組織です。

最後に

この変化は一夜にして起きるものではありません。また、過去から完全に断絶したものでもありません。攻撃手法の開発はこれまでも高速化しており、脆弱性の組み合わせ分析も自動化が進んできました。Mythosはその延長線上にあるものです。

Mythosは攻撃を極端に低コストにするものでもなく、専門知識を不要にするものでもありません。しかし、反復的な作業に伴う摩擦を取り除き、それら

をこれまで現実的でなかった規模で実行可能にします。

ここに本質的な変化があります。

これらの作業が数千の対象に対して並列に実行されるようになると、攻撃のコスト構造が変化します。その結果、より多くの組織が対象となり、より多くの攻撃経路が成立可能となり、リスク化するスピードが加速します。

変化に追随できる組織とは、事後的に対応する組織ではありません。現在の段階から運用を見直し、セキュリティを定期的に測定する対象ではなく、継続的に維持する対象として扱う組織です。

方向性はすでに明確です。残された問いは、組織がどの程度の速度でこの変化に対応していくかという点です。

著者について

Tom Stewartは、プロティビティの模擬攻撃とペネトレーションテストプラクティスのグローバル提供をリードするシニアディレクタです。Tomとチームは、クライアントがネットワーク・ペネトレーションテスト、ウェブアプリケーション・ペネトレーションテスト、および高度なレッドチームエンゲージメントを実施するのを支援します。彼はネットワークおよびアプリケーションセキュリティに関する豊富な知識と経験を持ち、業界で広く知られた基準や規制要件にも精通しています。

プロティビティLLC　*protiviti.jp*

東京都千代田区大手町 2-6-4 TOKYO TORCH 常盤橋タワー24F

大阪府大阪市北区梅田 3-2-123 イノゲート大阪9F

PJ2607

protiviti®