LUMEN®

BLACK LOTUS LABS®
by Lumen

2026年版Lumen Defender 脅威情勢レポート

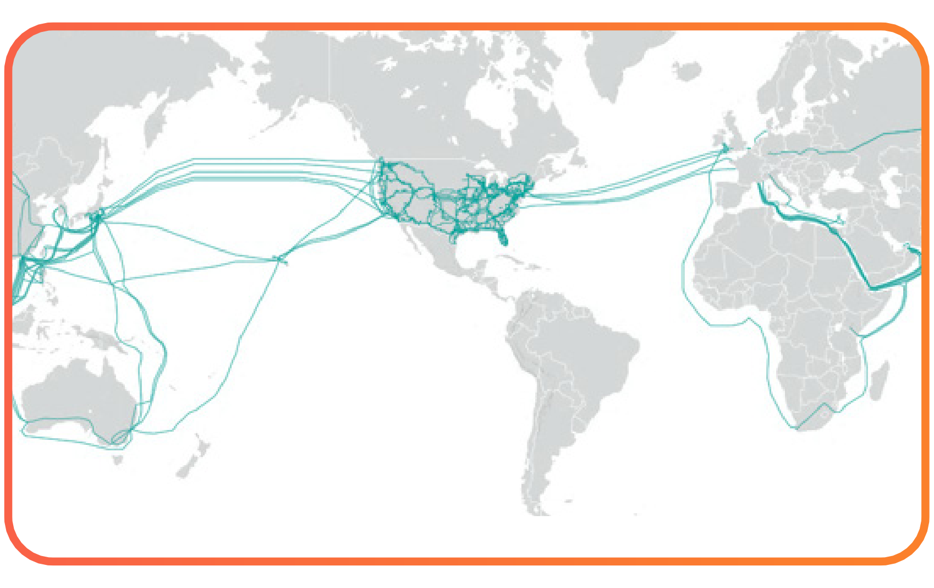
侵害発生時の可視性では全体像を捉えきれない理由

Lumenは、当社の脅威調査・運用部門であるBlack Lotus Labs®のインテリジェンスと、グローバル・インターネット・バックボーン内部からの独自の視点に基づき、2026年に向けた大きな変化を特定しました。**最新のサイバー攻撃は、外部に公開された状態を起点とする傾向がますます強まっており、脅威アクターは脆弱なエッジ・デバイスやサービスを狙うよう、標的選定を最適化しています。**

Lumenのインターネット・バックボーン内部

Lumenは、世界でも最大級で、最も接続性が高く、最も広範にピアリングされたネットワークの1つを管理・運用しています[1]。Black Lotus Labsは以下を提供・実施しています。

- パブリックIPv4アドレスの99%に対する可視性
- 2,000億件以上のNetFlowセッションとDNSクエリ、46,000件のC2を毎日監視
- 230万件の固有の脅威を毎日追跡
- 5,000件以上のC2を無力化(2025年)

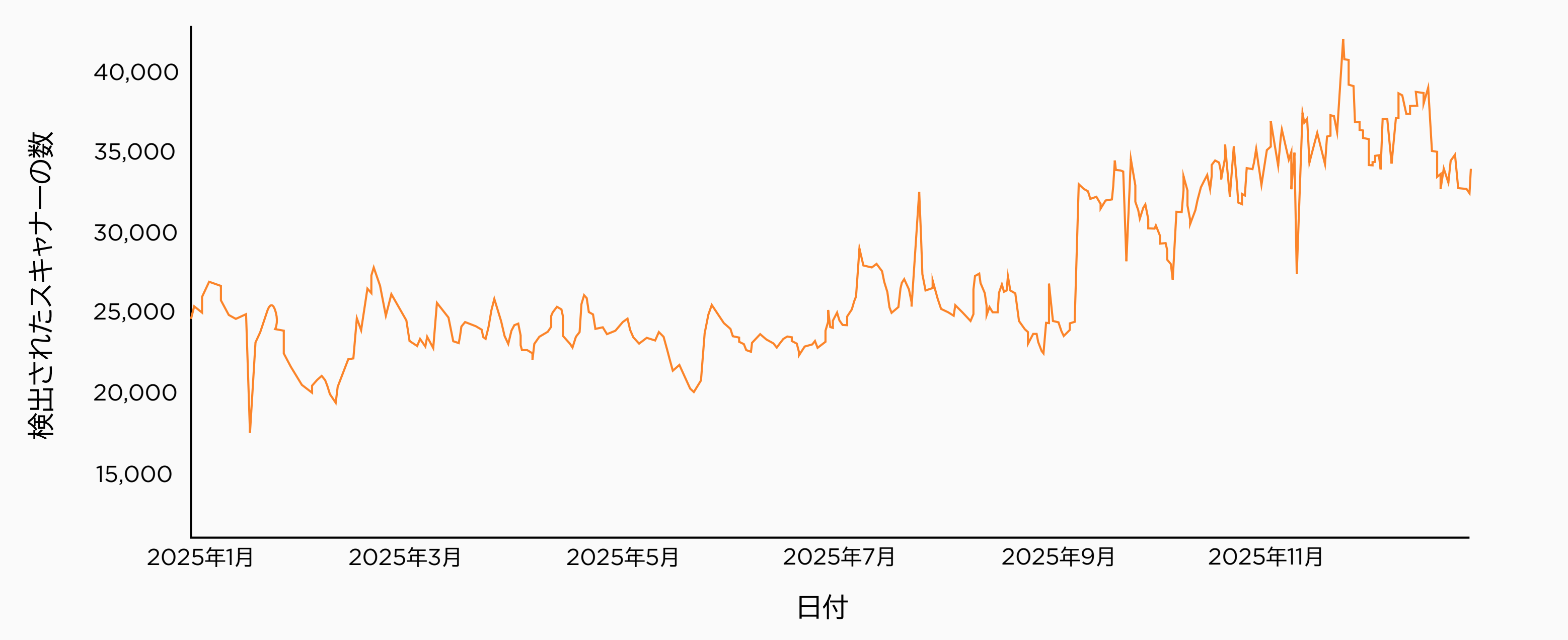


2025年の主要トレンド

1 生成AIがテンポを変え、攻撃は機械並みの速度に

脅威アクターは、生成AIを活用した新たな攻撃ベクトルを取り入れるだけでなく、自動化されたタスク実行、スキャン、インフラの切り替え、C2管理も採用していました。

悪意あるスキャナーの1日あたりの総検出数(2025年)



ボットネット運営者、イニシャル・アクセス・ブローカー、高度な攻撃者は、悪意ある継続的スキャンを用いて、インターネットに公開されたデバイスやサービスを事前に洗い出しています。

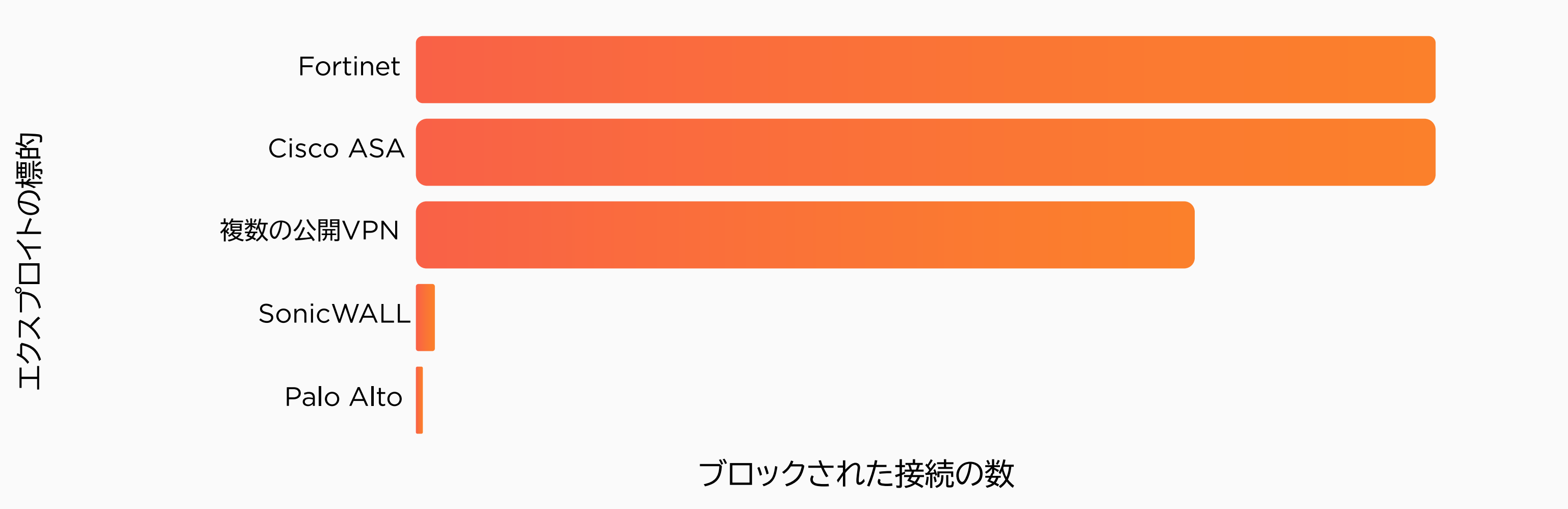
2 攻撃者がネットワークそのものの奥深くに入り込み、インフラに潜伏

攻撃者は、脆弱なエッジ・デバイスを狙って「通信の中間」に入り込み、認証情報を盗んで保護された情報にアクセスしながら、自らの活動をインターネットの接続基盤の中に紛れ込ませていました。

3 マルウェア基盤のプロキシ・ネットワークが、偽装を支える本格的な経済圏に

侵害された住宅用ルーター、IoTデバイス、大容量VPSホストは、攻撃者が信頼されたリモート従業員を装い、ジオフェンシング、ASNベースのブロック、IPレピュテーション・チェック、さらには多くのゼロ・トラストの位置情報シグナルを回避するために利用されました。

Black Lotus Labsの追跡に基づく、ブルート・フォース事象の多かった主な企業向けエッジ・デバイス(2025年10月～12月)



Lumen Defender EssentialsおよびPlusは、エンタープライズ・デバイスへの攻撃試行に起因する大量のトラフィックを検知しました。このグラフは、そうした攻撃で最も頻繁に狙われた上位5つのデバイスを示しています。

Lumen Defender EssentialsおよびPlusがブロックした悪意あるトラフィック全体の33%は、悪意ある継続的スキャンによるものです。

4 犯罪エコシステムがプロ化し、正規のSaaSさながらの洗練さを帯びる

攻撃者は、アクセスの拡大、悪用の自動化、サイバー犯罪への参入障壁の引き下げを目的に、カスタマー・サポートやサブスクリプション・プランまで備えた洗練されたプラットフォームを構築しています。

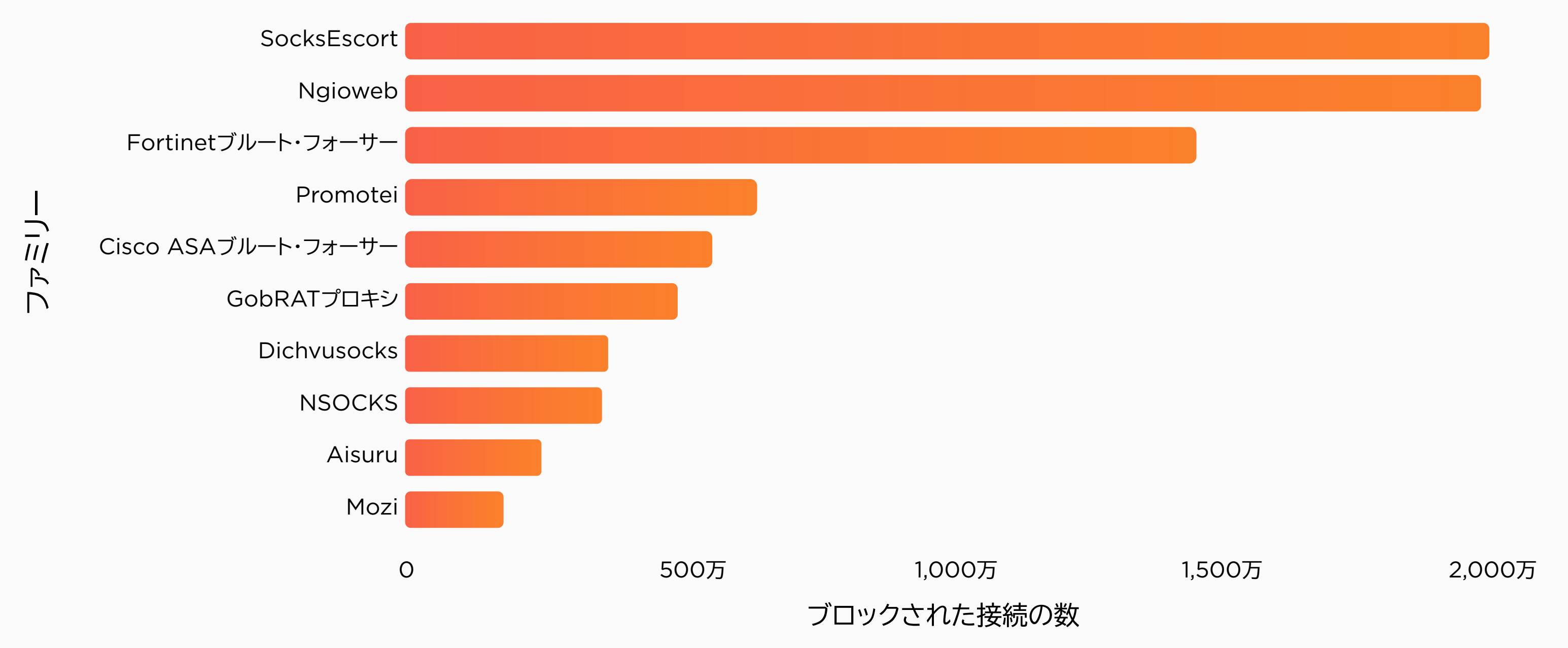
5 共有インフラ上で国家主体と犯罪集団の境界が曖昧に

国家主体が犯罪インフラに便乗し、サイバー犯罪者は情報機関が生み出したツールを再利用するようになったことで、攻撃の帰属を見極めるうえで、所有者よりも犯罪意図の方が強いシグナルとなりました。

6 グローバル・バックボーンが単なる通信経路から早期警戒システムへと変化

攻撃者がルーター、アプライアンス、管理プレーンを武器化するにつれ、グローバル・インターネット・バックボーンは、脅威アクターの移動を支える「目に見えない高速道路」から、検出と無力化に欠かせない重要なレイヤーへと進化しました。

Black Lotus Labsの追跡に基づく、Lumen Defenderがブロックした脅威トップ10 (2025年)



このグラフには、悪意あるスキャナーによるブロックは含まれていません。

2026年の脅威予測

生成AIとエージェントの普及で攻撃準備が高速化

エッジ・デバイスやインターネットに公開された管理インターフェースを標的とする、AI活用型の連鎖的なエクスプロイト経路が急速に増えると予想されます。これには、AIエージェントを用いて次のことを行うケースが含まれます。

- 権限レベルを評価する
- 隣接する信頼関係を特定する
- 最適なエクスプロイト経路を選択する
- 遂行中の戦術を状況に応じて調整する

攻撃の照準はエッジにある好機に集中

公開されたエッジのデバイスやサービスは、今後も攻撃者による継続的かつ無差別なスキャンにさらされます。到達可能なデバイス、特に認証が弱いものやパッチ未適用のものが見つかると、攻撃者は迅速に動き、アクセスの獲得と維持に最も効果的な手法やCVEを用います。

真のシグナルはネットワークにある

2026年には、最初期のシグナルはデバイスのテレメトリではなく、次のようなインフラ全体の挙動から現れるでしょう。

- C2の急速な切り替え
- 突然のプロキシ・レイヤーの出現
- オーケストレーション・トラフィックのパターン
- 複数地域にまたがる連携

最良の偽装は正規のインフラ

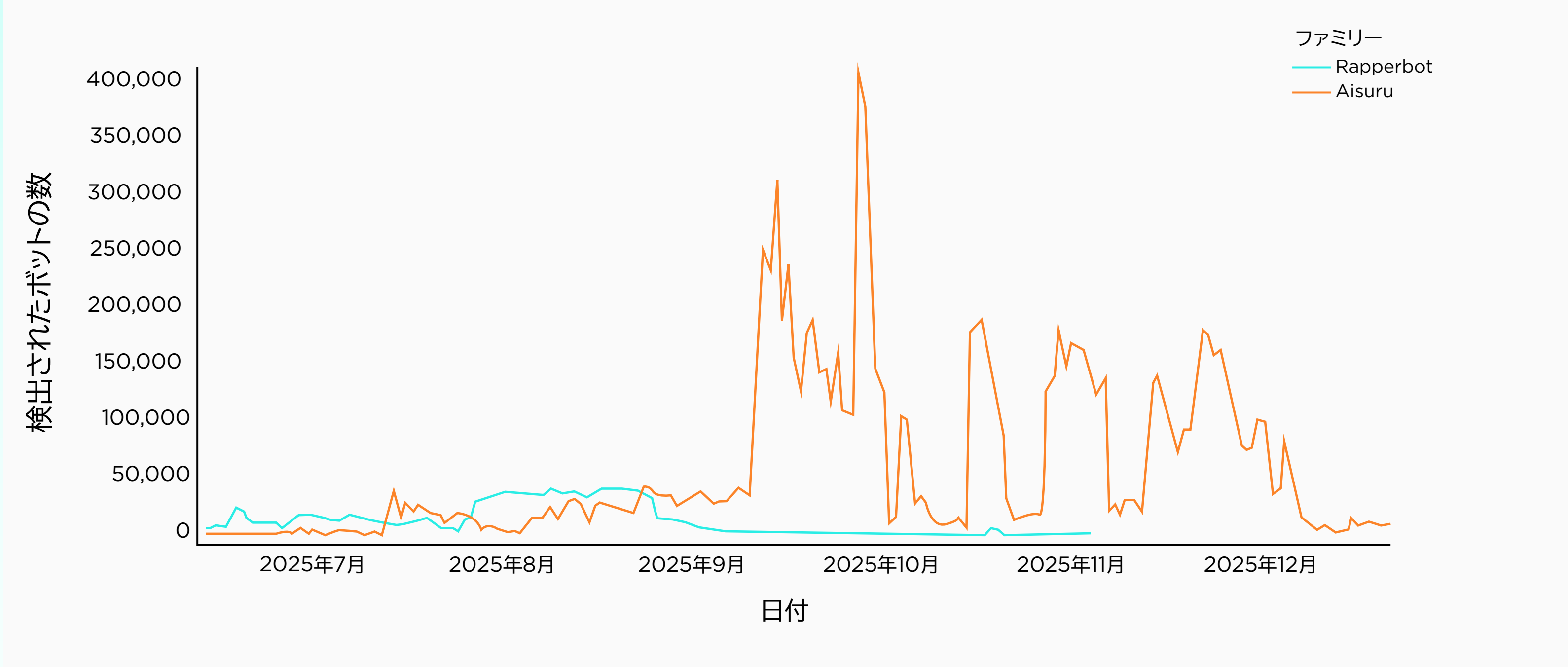
攻撃者は今後、マルウェア基盤のプロキシ・ネットワーク、SOHO基盤のボットネット、乗っ取られたVPSインフラ、「一見無害な」住宅用IPアドレス空間への依存をさらに強め、以下を行うようになります。

- 攻撃の帰属を曖昧にする
- 複数のキャンペーンにまたがってインフラを共有する
- 機能を大規模にレンタル、取引、再利用する

注目のキャンペーン: Kimwolf/Aisuru

Kimwolfは、当時インターネット上で最も強力なDDoS (分散型サービス拒否)ボットネットだったAisuruから分派した活動として、2025年後半に登場しました。Kimwolfは、ボット、急速に切り替わるドメインやIP、マルウェア配布ノードから成る多層型アーキテクチャーを採用していました。

RapperbotおよびAisuruボットの1日あたりの検出数(2025年)



2025年8月に別の有力ボットネットRapperbotが法執行機関によって無力化された後、Aisuruはローカルエリア・ネットワークを悪用する機能を、大規模なマルウェア基盤のプロキシ・ネットワークに対して用い、活動を急速に拡大しました。9月下旬にはKimwolfが登場し、Aisuruボットネット内のデバイスのより広い到達範囲を活用して規模を拡大しました。

上記のAisuru/Kimwolfボットの検出数グラフに見られる急増と急減は、最新のDDoSボットネットの特徴である、継続的な発見、Nullルーティング、再成長というサイクルを示しています。

重要ポイント: Kimwolfは、ボットネットがステルス性だけでなく、主要な生存特性として再生成速度を優先する方向へ移行していることを示しています。Kimwolfを見極めるうえで最も早い警告シグナルは、攻撃ペイロードではなく、プロキシ・サービスのプロービング、急激なトラフィック集中、大量のマルウェア再展開といったインフラの動きでした。これらのシグナルは、上流の可視性なくしては捉えられません。

結論

最新のサイバー脅威は、実際に攻撃が仕掛けられるずっと前から構築されています。攻撃者は、次の要素を基盤とするインフラのエコシステムを急速に構築しています。

- 生成AI
- 耐障害性の高いプロキシ・ネットワーク
- 侵害されたエッジ・デバイス
- 犯罪組織と国家主体が共有するプラットフォーム

強固なサイバー・セキュリティの基礎を上流の可視性やインフラ・インテリジェンスと組み合わせた組織こそが、攻撃者の潜伏時間を短縮し、悪意あるシステムを早期にブロックし、重要資産に到達する前に攻撃活動を阻止するうえで、最も有利な立場に立つことができます。

Lumenのグローバルなインターネット・トラフィックの可視性が、どのように早期検出を可能にするのかをご覧ください。

レポートをダウンロード

LUMEN®

BLACK LOTUS LABS®
by Lumen

脚注

1. 2025年1月 AS Rank、The Center for Applied Internet Data Analysis (CAIDA)