「能動的」な攻撃側への対処が進むことで、現場では何に備えなければならないか

一般社団法人JPCERTコーディネーションセンター　政策担当部長 兼
早期警戒グループマネージャー／脅威アナリスト　**佐々木 勇人**

佐々木 勇人（ささき はやと）●2010年、独立行政法人情報処理推進機構（IPA）勤務。2013年、経済産業省商務情報政策局情報セキュリティ政策室（当時）出向。2016年7月、JPCERT/CC入職。注意喚起等の情報発信のほか、インシデント対応支援や情報共有活動、官民連携活動に従事。研究活動にも取り組み、2023年からサイバーセキュリティ法制学会理事。2024年から防衛研究所政策研究部サイバー安全保障研究室 特任研究員。

■ 2024年の攻撃の傾向から

今年2月7日に「重要電子計算機に対する不正な行為による被害の防止に関する法律案」が閣議決定され、国会での審議に入りました。いわゆる「能動的サイバー防御」を実施するための新法やその関連法案の整備が進められます。これまでもサイバーセキュリティ基本法をはじめ、さまざまな関連法令によりサイバーセキュリティ政策の各施策が取り組まれています。既存の施策以上に、より強力な手段により、攻撃者側に対して対処を行っていく「能動的サイバー防御」を導入する必要性について考えてみたいと思います。

その理由の一つに、安全保障を脅かすレベルのサイバー活動に対しては、各組織の自主的な対策を重視する、平時におけるリスク行政的なアプローチでは対処に限界がある点が挙げられます。図表1は、昨年JPCERT/CCから発信した注意喚起のうち、脆弱性を悪用する攻撃が伴ったものを抜粋し、比較したものです。脆弱性の公表と注意喚起の発行時点では、すでにゼロデイ攻撃に悪用されているだけでなく、これらの直後から複数の攻撃者が当該脆弱性を悪用する、いわゆるNデイ攻撃も広範囲に行われてしまいました。注意喚起を発行した翌日に国内被害が発生してしまったケースも確認されています。

従前、脆弱性の悪用、特にゼロデイ攻撃については、当該脆弱性を把握している攻撃グループだけが先行して悪用することができ、脆弱性公表後、研究者等による脆弱性の詳細開示やPoC（Proof of Concept：概念実証コード）の公表が行われて初めて、他の攻撃者も当該脆弱性を悪用できるようになるのが一般的でした。そのため、仮に先行する攻撃者がゼロデイ攻撃を行っていたとしても、その攻撃者が標的とする攻撃対象に限られるため、影響範囲は限定的であり、脆弱性公表・注意喚起後に可能な限り速やかに脆弱性の修正対応を行えば同様の被害に遭うことはないという認識のもと、各組織で対応が行われてきました。「JPCERT/CCから注意喚起が出たその週末までに修正対応」する組織は比較的対応が早いと評されていたかと思います。

他方で、最近はこのゼロデイ攻撃での悪用状況が変化しています。前述のとおり、クリティカルな脆弱性を複数の攻撃グループが同時並行・広範囲に悪用を行っており、修正対応が間に合わないまま被害に遭う組織が多く発生しています。

こうした脅威動向への変化について、サイバー攻撃や脅威を分析するアナリストからは、これまで観測されることがなかった、攻撃グループ間の連携や未知の脆弱性情報の「融通」が行われている可能性が指摘されていま

（図表1）2024年にJPCERT/CCが発行した注意喚起のうちゼロデイ攻撃／Nデイ攻撃の悪用を伴ったもの

		ゼロデイ攻撃	Nデイ攻撃
2024年1月	Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）	あり	あり ※脆弱性公表直後
2024年2月	Fortinet製FortiOSの境域外書き込みの脆弱性（CVE-2024-21762）	あり ※「悪用の可能性」	
2024年4月	Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起	あり	あり ※脆弱性公表直後
2024年10月	Fortinet製FortiManagerにおける重要な機能に対する認証の欠如の脆弱性（CVE-2024-47575）	あり	あり ※脆弱性公表直後
2024年11月	Palo Alto Networks製PAN-OSの管理インタフェースにおける複数の脆弱性（CVE-2024-0012、CVE-2024-9474）	あり	あり ※脆弱性公表直後

す。さらにITセキュリティ企業がネットワーク機器を入手して未知の脆弱性を発見し、それを攻撃グループの活動に提供していたことが発覚しており、脆弱性を悪用するためのリソースが大幅に増加していること、また、連携等の効率化がなされていることが判明しています。

また、こうした高度な攻撃グループの攻撃被害に遭う“遭遇率”も変化しつつあります。後述のとおり、企業が利用している正規のネットワーク機器を踏み台にして攻撃活動を行うケースが増えており、この「踏み台」となる攻撃インフラ構築のために、広範囲でネットワーク機器の脆弱性を突いた攻撃が盛んに行われています。自組織が高度な攻撃グループに狙われないと想定していても、使用しているネットワーク機器が狙われないわけではないのです。

■ 受動的・自主的なセキュリティ対策の限界

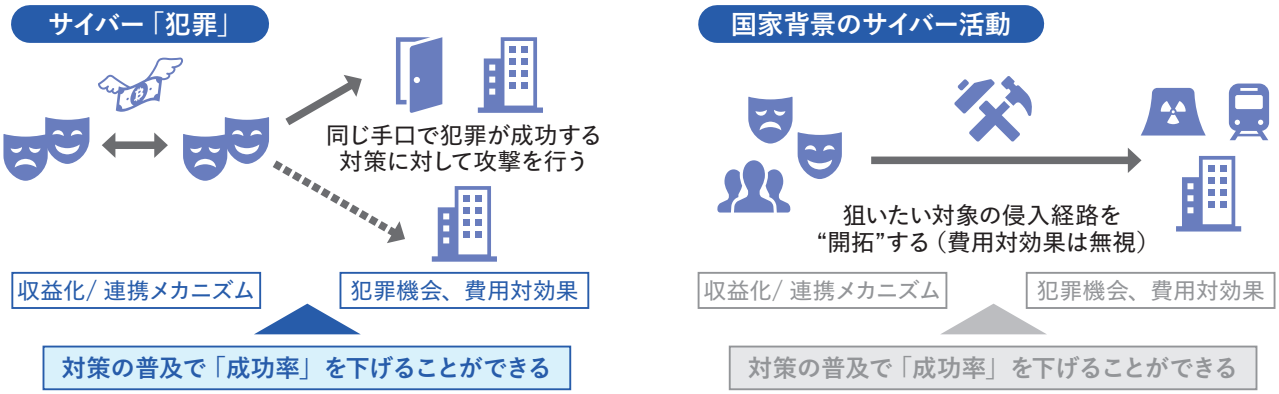
このような攻撃の増加に対し、これらの機器を利用する組織自身の自主的な対策・対応には限界が出てきていると言わざるを得ません。従前のセキュリティ施策は基本的に、ユーザー組織が自ら対策を実施し、この対策に必要な情報が国の施策によりJPCERT/CCなどから提供されるリスク行政的なアプローチが取られていました。このアプローチでは、「攻撃手法はある一定期間、繰り返し使われる」という前提に基づき、過去の被害事案から得た、対策の「原則」的な情報を広く周知することで、繰り返される特定の攻撃手法の有効性を下げていく、というアプローチが中心的でした。対策がある程度・割合まで浸透すれば、攻撃の成功率が下がり、やがて攻撃活動が（一時的に）収束する、という見込みのもとで実施されていました。

他方で、国家的背景を持つ攻撃グループは、目的達成のためには採算度外視で活動を行うこともあり、また、前述のように、脆弱性を見つけるために相当のリソース投入もなされており、さらには、グループ間連携による効率化も進んでいます。こうした活動には従前からの標的となり得る「将来の被害組織」自身の自主的な対策では限界があるのです。

2024年10月にSophos社が同社のファイアウォール製品の脆弱性を悪用した攻撃活動（Pacific Rim）との5年にわたる戦いに関するレポートの公表を行いました。このケースでは中国のITセキュリティ企業が同社製品を何らかの流通経路で入手し、未知の脆弱性を見つけ出し、攻撃活動側に提供していたことが判明しています。一部のネットワーク機器には、機器の状態等を遠隔で調査可能な通信機能である、「テレメトリー」が備わっているものがあり、同社はこの機能を活用して各被害組織での侵害状況を把握し、第２波、第３波の攻撃活動を早期に認知し対応したことを明かしています。また、攻撃サーバーを早期に見つけ出し、海外当局との連携によってこれを押収し、保存されていた情報からも標的組織を割り出し、対処したことが明かされています。

このレポートから読み取れるのは、先述のゼロデイ攻撃のために脆弱性の積極的な「開拓」が相当のリソースを投入して行われているという脅威だけでなく、ネットワーク機器からの通信情報やユーザーとのつながりを活用することで、機器ベンダー自体が攻撃対処の中心的な

（図表2）従前のリスク行政的なものが想定している脅威とサイバー安全保障が想定する脅威



役割を担ったという点です。また、攻撃活動中の攻撃インフラを早期に把握し、攻撃者側の情報を早期に、積極的に得ていく動きも注目されます。

2024年2月に米司法省はVolt Typhoonが用いていたボットネットの一部制圧・攪乱オペレーションを実施したことを公表しました。Volt Typhoonは米国を中心に通信事業者等の重要インフラへ侵入し、将来的な軍事衝突に備えて破壊的な攻撃を行うための長期的な準備活動を行っているとされ、2023年5月以降、米当局等が度々注意と対策を呼び掛けている攻撃グループです。Volt Typhoonが当時使っていた攻撃インフラは主に米国内の企業が使っていたネットワーク機器、ルーターを踏み台にし、巨大な攻撃インフラを構築していました。この攻撃インフラの活動を一時的に麻痺させるだけでなく、再開後の新たな攻撃の動きを早期に捉える活動も行われており、北米のTier1 ISPであるLumen社のセキュリティチームが、自社が提供する回線網の通信情報を分析し、ボットネットの全容解明や新たな攻撃活動の兆候を早期に検出し、被害拡大防止に役立てています。政府当局だけでなく、ISP事業者も通信情報の分析能力により、高度な攻撃活動に対処する重要なプレーヤーとして存在感を示しています。

■ 能動的サイバー防御が実現されたら何が起きるのか？

日本が法整備を進め導入を目指している「能動的サイバー防御」では、通信情報の分析を活用した攻撃の早期認知や、官民間の情報共有強化、攻撃インフラの無害化が主な手段として示されています。先述のPacific RimやVolt Typhoonの事例でも見られるように、海外では、防御側が官民にわたって、さまざまなプラットフォーム、事業者、製品等を活用して、攻撃活動の途中でこれを認知・捕捉し、攻撃者側の最終目的の達成前にこれを妨害・攪乱することが試みられています。能動的サイバー防御の導入にあたって整備される各手段が実際に機能すれば、こうした海外の試みと同様に、攻撃活動の途中で攻撃者を「迎え撃つ」ことが可能になると考えられます。

本稿は能動的サイバー防御の個別の手段・法整備の論点を解説するものではありませんので、各論の解説はさまざまな先行研究等をご覧ください。本稿ではユーザー目線、インシデント対応現場目線での課題を考えてみたいと思います。繰り返し述べたとおり、高度な攻撃グループとの戦いにおいては、攻撃活動の途中でこれを認知・捕捉し、何らかの対抗手段を行うことで活動を中断・攪乱させ、攻撃者側の最終的な目的を達成させないというアプローチがすでに取り組まれ始めています。

先に紹介した2事例のように、攻撃インフラが特定・調査され、途中経路の通信情報が分析・特定されることで、被害組織または被害組織が使うセキュリティ製品・サービス「以外」のソースにより侵害を認知するケースが増えつつあります。攻撃インフラを調査した捜査当局や、ISP事業者経由で被害を知る、というケースが今後増えることが想定されます。

「早く侵害を認知できて、被害が広がる前に攻撃を追い返せたならいいじゃないか」と単純に喜ぶことはできません。一般的な不正アクセス事案では、残念ながら発覚は攻撃からしばらく経過した「事後」であり、インシデント対応・フォレンジック調査というのは「過去の侵害を調査する」、後始末的なものとなります。そこには多くの「アーティファクト」（※被害現場に残るマルウェアやログなどの攻撃「痕跡」情報）が残されており、時間をかけて調査を行えば大体のケースで被害の全容を解明することができます。

他方で、「攻撃活動途中の侵害を認知した場合」というのは、攻撃の途中ですので、被害組織内には断片的なアーティファクトしか残っていません。例えば、「ネットワークアプライアンスが侵害され、バックドアが設置さ

れただけで、そこから先のネットワークまで侵害が拡大していなかった」ということを証明するためには、どれだけの調査を行えばいいのでしょうか。「そこから先へ侵害されてはいなかった」ということを証明するのは、やや「悪魔の証明」的な調査・分析となります。今後、インシデント報告先の行政機関やステークホルダーとの間で「本当にその先に侵害されていないのか？」「なぜそうだと証明できるのか」といったやり取りが発生した場合、ミスコミュニケーションによるトラブルが懸念されます。

ミスコミュニケーションを防ぐためにも、外部から提供される断片的な情報をトリガーとして実効性のある調査・インシデント対応を行い、また、被害が拡大する前に攻撃者を追い出すためにも、基本的なことですが、各種ログの記録・保存と運用がますます重要であると筆者は考えます。これまでの「何かあったときに痕跡を調べられるように」という（時間軸的にも）「後ろ向き」な目的だけでなく、「侵害されても速やかに攻撃者を追い出すために」使い、攻撃を見える化する、「前向き」な目的として整備・運用がされることが望まれています。

JPCERT/CCではインシデント発生時の相談だけでなく、こうした脆弱性を悪用した攻撃を速やかに見つけるための調査方法などの情報も可能な限り注意喚起に掲載し、また、ログ分析のポイントなどを解説したコンテンツも公開していますので、是非ご活用ください。

（図表3）これまでのインシデント対応とこれから想定されるインシデント対応