従来型エンドポイントセキュリティが企業をリスクにさらす理由

概要

今日の分散型ネットワークのあらゆる対象を保護しようとした場合、エンドポイントは最も脆弱性が高いといえます。モビリティにより、企業ネットワークの内外で日々多様なデバイスの利用が増え続けています。公衆回線からのアクセスの増加、エンドポイントにおける従来型の不十分なセキュリティ対策、ユーザー向け自律機能の普及を背景に、このようなデバイスは、マルウェアや組織全体を狙う高度な攻撃の格好の標的になっています。攻撃者は、こうしたデバイスに攻撃を仕掛け、極めて大きな成果を収めています。

ほとんどの組織は、競争力の維持を目的にデジタルトランスフォーメーション（DX）に取り組んでおり、クラウドサービス、IoT（モノのインターネット）のスマートデバイス、モビリティの導入を推進しています。その結果、あらゆるデバイスから重要な情報へ、高速かつシームレスなアクセスが可能になっています。ところが、分散型ネットワークの拡大に伴い管理が追いつかない今、エンドポイントはセキュリティチェーンにおいて脆弱なリンクのまま取り残されています。

攻撃の標的になりやすいエンドポイント

エンドポイントデバイスは、組織内で最も狙われやすい場所です。その理由の 1 つが、ネットワーク接続のデバイスの増加にあります。ユーザーは、ネットワーク上のリソースに対して、ノートパソコン、スマートフォン、タブレット、スマートウォッチといった複数のデバイスからいつでも同時にアクセスできるようになっています。

効果と効率の低いエンドポイント戦略が原因で、年間**6 万ドル**のコストが発生しています [1]。

エンドポイントは、**組織内で最も狙われやすい標的**です。

セキュリティ保護されていないエンドポイントの検知と隔離において、年間**340万ドル**のコストが発生しています[1]。

残念ながら、ほとんどのITチームは、エンドポイントをネットワークの他の構成要素から切り離して捉えています。その理由は、デバイス数があまりに多く、セキュリティ管理にエンドユーザーの協力が必要になるためです。エンドポイントセキュリティは、多くの場合、個別のソリューションとしてデバイスに適用され、通常は、ウイルス対策やエンドポイントセキュリティパッケージとして導入されます。一般的なネットワークセキュリティのスタート地点は、エンドポイントデバイスがネットワークに接続するポイントです。エンドポイントがネットワークに接続すると、そのデバイス（さらには、デバイスの内蔵コンポーネント）は、LANやWANを構成する一部となります。

ところが、上記のような理由から、エンドポイントとネットワークをつなぐ境界ポイントの定義は難しくなり、防御も困難になりつつあります。また、エンドポイントセキュリティの強化を求める要素は他にもあり、状況はさらに深刻化しています。

エンドポイントは、もはや企業ITの延長上に統合されてはいません。これは、運用上でエンドポイントセキュリティの変革が必要な理由の1つになっています。ユーザーは、デバイスの選択やソフトウェアのインストールの多くを自律的に行っており、セキュリティパッチやアップデートを先延ばしにしてしまうこともあります。

また、このようなユーザーの自律性から、シャドーITが発生しています。シャドーITは、ユーザー自身が管理するアプリケーションやエンドポイントであり、組織のIT管理者による承認や監視の対象外です。使いやすさや生産性を優先してエンドユーザーに管理を任せていますが、その結果、セキュリティの問題が浮上しています。特に、シャドーITは広範に拡大する傾向にあり、ユーザーに悪意はないものの、組織を大きなリスクにさらす原因になっています[2]。

また、脅威のリスク増大も、エンドポイントセキュリティの変更が急務とされる理由の1つです。エンドポイント（およびエンドポイントがアクセスするリソース）は、企業ファイアウォールに保護されているとは限りません。ユーザーは商用SaaS（Software-as-a-Service）アプリケーションやクラウドサービス（Dropbox、Boxなど）に、オンサイトや外出先から接続します。また、企業データへのアクセスに、VPN（仮想プライベートネットワーク）を経由することを義務付けていない組織も存在します。公共のネットワークにアクセスするエンドポイントは、直接的な攻撃に対して脆弱になり、感染にさらされ、人為的なミスや不正行為による侵害が起こりやすくなります。

フィッシング攻撃に騙されるユーザーは、平均で**4%**にのぼります[3]。

サイバー犯罪者は、エンドポイントの脆弱性を悪用しています。2018年には、合計で2,216件のデータ侵害が発生したことが確認されています。その73%が、外部からの侵入でした。フィッシングやプリテキスティング（なりすまし）は、セキュリティ侵害の93%を占めます。メールは、最も狙われやすい攻撃対象です（96%）[4]。一般的に、メールを悪用した攻撃は、エンドポイントユーザーとエンドポイントデバイスを標的にします。攻撃が成功すると、組織は非常に多額の被害を被ります。2017年に発生したエンドポイント攻撃の被害額は、1社あたり500万ドルを超えています[5]。

包括的な保護対策を講じるには、現在、エンドポイントデバイスを危険にさらしている環境的な緊急課題に取り組み、体系上の弱点を解消できるエンタープライズセキュリティが必要になります。

拡大し続ける攻撃対象領域

ある調査によると、企業ネットワーク外のエンドポイントデバイスを監視する機能がない組織は63%を占めます。また、過去12カ月でマルウェアに感染したエンドポイントが増加した企業は、全体の53%にのぼります[6]。感染したノートパソコンやスマートフォンを社内ネットワークに接続すると、組織全体が、オフネットワークで感染した脅威（ウイルスやマルウェアなど）のリスクにさらされかねません。

エンドポイントに存在する脅威のタイプによって幅広い範囲に、次のような影響が及ぶことになります。第1に、脅威は、デバイスから移動しなくても、組織に損害を与えることができます。ノートパソコン、タブレット、POSシステムは、価値の高い情報やIPを処理し、ローカルメモリ内に格納する機能を備えています。したがってこのようなデバイスがマルウェアに感染すると、情報は即座に持ち出されてしまいます。

第2に、感染したデバイスを社内ネットワークに接続すると、その脅威は、エンドポイントの認証情報を収集し、社内全体を水平移動し、価値の高いデータがないか探索を開始します。そして、認証情報は密かに収集され、将来的な攻撃のために保管されます。

第3に、この接続パターンがマルウェアの急激な拡散を引き起こすことがあります。1つのマシンに感染したマルウェアは、接続機能とエンドポイントの認証情報を使って、ネットワーク上にある大量のデバイスに感染を広げます。最近発生した大量感染には、WannaCry、Petya / GoldenEye、Bad Rabbitといったマルウェアがあります。このような攻撃では、感染したエンドポイントをロックするのみならず、ワームのような機能を使ってネットワーク上に拡散する能力を持つランサムウェアやクリプトウェアが使用されています。その目的は、被害を最大に拡散し、できるだけ多額の身代金を手に入れることにあります。

日々、攻撃件数や感染速度が増し、巧妙な手法が増えています。先頃フォーティネットが342人のセキュリティリーダーを対象に行った調査によると、サイバーセキュリティの最大の課題は、急速に進化するサイバー脅威への対応であることがわかりました[7]。現在、エンドポイントのウイルス対策はほぼ標準化されているものの、最新の脅威は極めて急速に進化し、感染規模も非常に大規模になり、捕捉が困難であるため、マシンごとに封じ込めを行う個別のローカル対策ではとても太刀打ちできません。

分断したセキュリティ対策では複雑な環境を保護できない

これまでのネットワーク向けに設計された古いセキュリティコントロールでは、変化を続ける脅威に追い付くことはできません。現在、エンドポイントセキュリティソリューションはサイロ化されており、様々なセキュリティアーキテクチャを構成する他の要素と接続し、連携することは不可能です。

このようなエンドポイントは、ゼロデイ脅威インテリジェンスを受信または共有する機能を備えていません。その結果、セキュリティ部門は、攻撃や侵害に迅速、効率的、効果的に対応できなくなっています。現在、多くのセキュリティアーキテクチャでは、非集約型で複雑なネットワークトポロジが採用されているため、エンドポイントを超えてオープンなネットワークにまで攻撃の手を広げる新たな脅威に対応できていません。

企業の IT プロフェッショナルを対象にしたエンドポイントセキュリティに関する調査では、導入と管理の複雑さは、三大課題の 1 つとなっています（他の 2 つは、不十分な保護機能、誤検知の大量発生です）[9]。エンドポイント管理が複雑になった理由はいくつかあります。

第 1 に、エンドポイント管理の複雑さは、より広範なセキュリティをカバーする上での複雑さに起因しています。セキュリティアーキテクチャはポイントソリューションの寄せ集めで構成されているため、ネットワーク全体の効果的な管理と保護に IT チームは苦戦しています。ポイントソリューションは、さまざまな理由で段階的に追加される傾向があります。たとえば、新たに発生したセキュリティギャップ対策のため、増大するネットワークニーズへの対応（SSL / TLS インスペクション、SD-WAN など）のため、ますます厳格になるコンプライアンス標準と法規制要件への対応のためなどがあげられます。

第 2 に、個別の製品を複数のコンソールを使って管理するため、運用作業が格段に複雑になります。これは、人為的なミスを招く原因にもなります。その結果、緊縮予算や人材不足で既に大きな負担を抱えているサイバーセキュリティチームと IT チームの負担は、さらに増大します [10]。

主な攻撃経路[8]

- **74%** が、メールの添付やリンクから侵入
- **48%** が、Web ベースのドライブバイやダウンロードを介したブラウザから侵入
- **30%** が、ユーザーエンドポイントに存在するアプリケーションの脆弱性から侵入
- **26%** が、Web サーバーや Web アプリケーションの脆弱性から侵入

IT プロフェッショナルの 56% が、「エンドポイントデバイスのコンプライアンスを確認できない」（パッチが適用されていない脆弱性のチェックなど）と回答しています。 また、3 分の 1 以上（36%）のデバイスは、コンプライアンステストに合格していません。この 2 つは、エンドポイントが IT セキュリティから漏れていることを実証しています[11]。以上から、エンドポイントは組織内の重大な盲点になっていることがわかります。企業は、脅威にさらされるだけでなく、セキュリティ侵害が発生した場合には、法規制違反による罰金や法的な賠償責任を負う恐れもあります。

把握できないデバイスは保護できない

膨大な数のデバイスがネットワークに接続されているため、IT セキュリティではすべてを把握しきれず、リスクを管理することができません。その結果、問題はますます複雑になっています。多くのネットワーク管理者は、ネットワーク全体を透過的に可視化する機能や、セキュリティポリシーを一元管理する機能を使用していません。

従来のエンドポイントセキュリティには、限られたデバイス可視化機能しか実装されていません。エンドポイント保護を強化するには、サイバーセキュリティチームがすべてを把握できる機能が必要です。ネットワークにアクセスできるユーザー、接続されるデバイスのタイプ、インストールされている OS のバージョン、パッチの非適用による脆弱性、関与するトラフィック、使用されているソフトウェアなど、非常に幅広い情報を把握しなければなりません。

エンドポイントをセキュリティ保護対象に戻す

エンドポイントは、他から切り離された存在で良いわけではありません。ますます危険になる脅威、IT による不十分な監視、複雑化するビジネス環境に直面するエンタープライズセキュリティは、攻撃の標的となるネットワークエッジデバイスの保護に向けて、取り組みを強化する必要があります。

エンドポイントセキュリティの責務は、エンドポイントやデスクトップ IT チームの枠を遙かに超えています。個々のデバイスを保護するだけでなく、攻撃経路を閉じることで、企業データ、ネットワークリソース、情報システムの安全を確保しなければなりません。そして、さらに広範な統合ネットワークセキュリティアーキテクチャの一部として、エンドポイントセキュリティを組み込む必要があります。

企業の 50% は、エンドポイント管理に**35 人以上のフルタイム従業員**を必要としています[12]。

ユーザーアクションは最も一般的な脅威の侵入経路であり、エンドポイントの**セキュリティ侵害や感染を特定**する最も有効な手段でもあります[13]。

1 「The Cost of Insecure Endpoints」、Ponemon Institute、2017 年 6 月（英語）：https://www.absolute.com/en/go/reports/the-cost-of-insecure-endpoints
2 「Don't Let Shadow IT Put Your Business at Risk」、Christy Pettey 著、ガートナー、2016 年 5 月 3 日（英語）：https://www.verizonenterprise.com/verizon-insights-lab/dbir/
3 「2018 Breach Data Investigations Report」、ベライゾン、2018 年 4 月 10 日（英語）：https://www.verizonenterprise.com/verizon-insights-lab/dbir/
4 同上
5 「Fileless attacks surge in 2017, security solutions are not stopping them」、Charlie Osborne 著、ZDNet、2017 年 11 月 5 日（英語）：https://www.zdnet.com/article/fileless-attacks-surge-in-2017-and-security-solutions-are-not-stopping-them/
6 「The Cost of Insecure Endpoints」、Ponemon Institute、2017 年 6 月（英語）：https://www.absolute.com/en/go/reports/the-cost-of-insecure-endpoints
7 「Center Security On Advanced Technology」、Forrester Consulting、2017 年 7 月（英語）：https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/Center-Security-On-Advanced-Technology.pdf
8 「2017 Threat Landscape Survey」、Lee Neely 著、SANS Institute、2017 年 8 月（英語）：https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910
9 「Fileless attacks surge in 2017, security solutions are not stopping them」、Charlie Osborne 著、ZDNet、2017 年 11 月 5 日（英語）：https://www.zdnet.com/article/fileless-attacks-surge-in-2017-and-security-solutions-are-not-stopping-them/
10 「Research suggests cybersecurity skills shortage is getting worse」、Jon Oltsik 著、CSO、2018 年 1 月 11 日（英語）：https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html
11 「The Cost of Insecure Endpoints」、Ponemon Institute、2017 年 6 月（英語）：https://www.absolute.com/en/go/reports/the-cost-of-insecure-endpoints
12 同上
13 「2017 Threat Landscape Survey」、Lee Neely 著、SANS Institute、2017 年 8 月（英語）：https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ