文中のハイパーリンクは英文のサイトとなっております、日本語をご希望される場合はブラウザの翻訳機能等をご使用ください。

# 最前線にあるネットワークデバイス

サイバー攻撃の脅威アクターは、企業の防御が最も弱いところ、そして攻撃が最もダメージを与えることができるところを見つけるために、常に進化を続けています。この2年間、あらゆる種類の脅威アクターが、その両方に当てはまる新しいタイプのターゲット、すなわち企業のネットワーク機器に焦点を当ててきました。

VPN、スイッチ、ファイアウォール、ルーター、そしてさまざまなトラフィックコンセントレータ、ゲートウェイ、配信コントローラはすべて、ランサムウェアグループや国家レベルの脅威アクターによって大きな標的とされています。皮肉なことに、企業を保護するために信頼されている同じデバイスの多くが、現在ではそれ自体が最初の攻撃ポイントになっています。

企業のセキュリティ担当者は、自らを守るために、このようなトレンドの背景にあるものを理解し、どのようにリスクを軽減できるかを理解する必要があります。本書では、実際に起きている攻撃の最新の分析結果に基づいて、ネットワーク・デバイスのセキュリティについて詳しく説明します。最新の攻撃手法とその理由、そして企業の安全性を確保するための具体的な要件とベストプラクティスを取り上げます。具体的には、本書により以下を学ぶことができます：

- 現代の攻撃におけるネットワークデバイスの台頭
- ネットワークデバイスが狙われる理由
- ゼロ・トラストにおけるネットワークデバイスとファームウェアの重要な役割
- ネットワークデバイスを保護するための主な要件
- エクリプシウムがネットワークデバイスの保護に貢献できること

これらの情報をもとに、セキュリティリーダーや実務担当者は、既存のセキュリティプログラムのどこにギャップがあるのかを特定し、是正措置を講じる方法を決定することができます。

# 企業のシステムインフラを防御する

## 現代の攻撃におけるネットワークデバイスの台頭

ネットワーク機器に対する攻撃の急増は、ここ数年におけるサイバーセキュリティの最も大きな進展の一つです。2019年に入り、業界の観測筋は、脅威アクターがVPNなどの企業向けデバイスの脆弱性を狙うパターンが増えていることを確認しはじめました。2020年初頭には、CISAのアラートが、CitrixおよびPulse Secure VPNの脆弱性が、すでにAPTグループのトップターゲットの1つになっていると警告しました。

これは、より多くの国家やランサムウェアベースのグループが同じ手法を採用し、Citrix、F5、Fortinet、Palo Alto Networks、SonicWallなどの追加のエンタープライズベンダーに拡大したため、より大きなトレンドの始まりにすぎないことが判明することになりました。

その後、サイバーセキュリティ機関は、ロシア、中国、イランの国家を基盤とする脅威アクターが、さまざまな企業ネットワーク機器やベンダーをターゲットにしていることを詳細に伝える警告を繰り返し発表しています。特に、ロシアの SVR の手法を取り上げた最新のアラートでは、標的となった上位 11 件の脆弱性のうち5件がネットワーク機器に影響(PDF)を及ぼしていました。

この戦略は、最も広範で有害なランサムウェア・キャンペーンでもすぐに採用されるようになりました。Netwalkerは、ネットワーク・デバイスを標的とした最初のランサムウェアの1つで、この傾向はDoppelPaymer、Maze、Ragnarokなどの最も人気のあるランサムウェア・グループに急速に広まりました。この傾向は、製造工場に対する攻撃でF5デバイスを標的としたCringランサムウェアによって、さらに加速しています。直近では、アクセリオン製デバイスのゼロデイの脆弱性を悪用したランサムウェア「Cl0p」が高い標的となっています。

合計すると、上位5つのランサムウェアグループのすべてと、合計20以上のランサムウェアグループが、企業のネットワークデバイスやインフラを標的としていることが確認されています。下表は、さまざまなグループが企業のテクノロジーベンダーをどのように標的にしているかをまとめたものです。

| Vendor/Product | APT Groups | China | DPRK | Iran | Russia | Unknown | Ransomware | Conti | DoppelPaymer | Maze | Netwalker | REvil |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Atlassian | | | | | | | | | | | | ⚠ |
| Cisco | | | | | ⚠ | ⚠ | | | | | | |
| Citrix | | ⚠ | | ⚠ | ⚠ | | | | ⚠ | ⚠ | | ⚠ |
| F5 | | ⚠ | | ⚠ | ⚠ | | | | | | | |
| Fortinet | | ⚠ | | ⚠ | ⚠ | ⚠ | | ⚠ | | | | ⚠ |
| Juniper | | | | | | ⚠ | | | | | | |
| MobileIron | | ⚠ | | | | ⚠ | | | | | | |
| Oracle | | ⚠ | | | ⚠ | | | | | | | ⚠ |
| Pulse Secure | | ⚠ | | ⚠ | ⚠ | | | | | ⚠ | ⚠ | ⚠ |
| VMware | | | | | ⚠ | | | | | | | |

# 企業のシステムインフラを防御する

## ネットワークデバイスが狙われる理由

ネットワーク機器には、攻撃者にとって特に魅力的ないくつかの特徴があります。ネットワーク機器は、組織内で最も強力かつ戦略的に重要な機器であり、サイバー攻撃という文脈においては、他に類を見ないほど貴重な存在となっています。また、一般に公開されているため、サーバーやノートパソコンなどの従来の資産を保護するためのセキュリティ・プロセスやツールが適用されないことがよくあります。

ネットワーク機器が攻撃される主な理由は以下のとおりです。

### 公衆網からのアクセス

ネットワーク機器は、その機能を発揮するために、一般にアクセス可能でなければならないことが多い。例えば、VPNは、リモート・ユーザーにサービスを提供するため、当然ながら公開される必要があります。このようなデバイスの脆弱性を悪用することで、攻撃者は、フィッシングやその他のユーザー依存の感染方法を用いることなく、企業内への極めて戦略的な足がかりを得ることができます。

このため、企業ネットワークへのアクセスを専門とするInitial Access Broker（IAB）は、ネットワーク機器を最優先事項とし、そのアクセス権を他の脅威アクターに転売しています。IABは、特定のベンダーや種類のデバイスを攻撃することに特化しており、ほとんどのIABは、競争上有利となる新しい脆弱性を積極的に探し求めています。

さらに、Covid-19の大流行により、多くの組織がリモートワーク・モデルへの移行を余儀なくされました。このため、企業内VPNへの依存度がさらに高まり、攻撃者はすぐにこれを利用することができるようになりました。

### 高い戦略的価値

ネットワーク機器は、いったん侵入されると、サイバー攻撃のその後の局面で壊滅的な役割を果たすことがあります。企業の中枢神経系であるネットワーク機器は、組織内のほぼすべてのものと自然に接続されているため、横方向の動きや持続性に最適です。

例えば、エンドユーザ・デバイスへの経路を提供することで、攻撃者は追加のマルウェアやペイロードを送り込むことが可能になります。同様に、ネットワーク・デバイスは、接続された他の内部資産への足掛かりとして使用することができます。ネットワーク機器のネットワーク機能を悪用して、攻撃者がトラフィックを監視したり、コピーしたり、リダイレクトしたりすることも可能です。デバイスによっては、攻撃者がDHCP設定を変更したり、DNSポイズニングを実行したりして、ユーザーを悪意のあるサイトに誘導したり、マシン・イン・ザ・ミドルを確立したりすることができます。

また、ネットワーク・インフラストラクチャを侵害することで、IT/OTと企業内の他の高価値なエリアとの間の境界を破壊することもできます。また、攻撃者は、企業の業務を停止させるために、ネットワークデバイスを単に「壊す」こともできます。

### 暴露された脆弱性

ネットワーク機器もまた、攻撃者にとって潜在的な脆弱性の宝庫でもあります。長年にわたり、業界はWindowsベースのノートパソコンのような従来のデバイスの保護という点で大きな進歩を遂げてきました。保護機能の向上、ソフトウェアやオペレーティングシステムの自動更新により、このようなデバイスの攻撃対象は減少しています。このため、攻撃者はより安全な代替ターゲットを探すようになり、ネットワークデバイスが理想的な標的となりました。

多くのネットワーク機器は、Linuxオペレーティングシステムをベースにしていますが、特定のベンダーのニーズに合わせて大幅にカスタマイズされています。このため、独自の脆弱性を持つ多種多様なカスタムOSが存在することとなりました。しかし、これらのカスタムOSは、一般的なOSに見られるような業界全体の監視や更新プロセスを受けず、重大な脆弱性に気付かないままになってしまうことがあります。

これらの脆弱性の多くは、ネットワーク機器のファームウェアや統合コードに直接的に関連していることに留意することが重要です。例えば、APTやランサムウェアによって最もよく攻撃される33のネットワークデバイスのCVEのうち12は、影響を受けるコンポーネントとしてファームウェアを具体的に挙げています。これには、企業向けVPN、Ciscoルーター、Citrix アプリケーション・デリバリー・コントローラー、SonicWall VPN、その他のセキュリティ・デバイスが含まれます。

### 従来のセキュリティツールやプロセスでは保護されない

ネットワーク機器は、企業のセキュリティツールの死角になりがちです。例えば、前述した低レベルの脆弱性の多くは、従来のパッシブなソフトウェア脆弱性スキャンでは発見されません。脆弱性管理チームの多くは、従来のデバイスへのパッチ適用に追われ、ネットワーク・デバイスの脆弱性をスキャンすることができず、脆弱性が検出されたとしてもその重要性を認識できない場合があります。

脅威に関して言えば、問題はさらに深刻です。また、ネットワーク機器は通常、ノートパソコンやサーバーに適用される従来のセキュリティ・エージェントに対応していません。これはIoTデバイスに共通する問題ですが、ネットワークデバイスはより高い価値を持ち、より高いリスクを伴います。

その結果、ほとんどのセキュリティ・チームは、ネットワーク・デバイスの整合性を検証したり、侵害されたデバイスを特定したりする一貫した方法を持ち合わせていないのが現状です。また、利用可能なツールは、特定の脅威に対応するためにベンダーが提供する単発のツールであることがほとんどです。最後に、多くの組織では、デバイスを保護する責任を最初に負うのが誰なのかが明確ではありません。ネットワーキング・チームがある程度の責任を負うかもしれませんが、セキュリティ・チームはルールと設定を最新の状態に保つ必要があるかもしれません。また、脆弱性管理チームが担当する場合もあれば、担当しない場合もあります。このような曖昧さは、運用上のギャップや場当たり的なセキュリティ・プロセスを生み出し、デバイスを無防備な状態にする可能性があります。

## ゼロトラスト戦略は、ネットワークデバイスとそのファームウェアに依存する

ゼロ・トラストは、急速に現代のサイバーセキュリティの基礎となる概念の1つになっています。最近の「国家のサイバーセキュリティの改善に関する大統領令」では、連邦政府機関にゼロトラストアーキテクチャへの移行を義務付けることで、ゼロトラストの重要性がさらに体系化されました。NISTの特別な出版物であるSP 800-207は、ゼロ・トラストを次のように定義するのに役立っています：

> “ゼロトラスト（ZT）とは、進化するサイバーセキュリティのパラダイムを表す用語で、防御を静的なネットワークベースの境界線から、ユーザー、資産、リソースに焦点を当てるようにする...」とあります。"
>
> "ゼロ・トラストは、物理的な場所やネットワークの場所（ローカルエリアネットワークとインターネットなど）、資産の所有権（企業所有と個人所有）に基づくだけで、資産やユーザーアカウントに暗黙の信頼が与えられていないことを前提としています。"
>
> "ゼロトラストは、ネットワークセグメントではなく、リソース（資産、サービス、ワークフロー、ネットワークアカウントなど）の保護に焦点を当て、ネットワークの位置がリソースのセキュリティ態勢に対する主要な構成要素とは見なされなくなったからです。"

この定義は、サイバーセキュリティの戦略家、実装者、実務者に、業界がこれまで現代のネットワーク全体でエンドポイント、サーバ、デバイスに置いてきた固有の、暗黙の、そしてますます弱くなっている信頼について再考するように促しています。これらの概念は、ネットワーク・デバイスという文脈では、さらに重要な意味を持ちます。

## ファームウェアとデバイスレベルのコードを検証する必要がある

デバイス内のファームウェアは、デバイスの中で最初に実行されるコードであり、最も特権的なコードの一部でもあります。従来のラップトップやサーバーの場合、ファームウェア内の悪意のあるコードは、攻撃者がより上位のオペレーティングシステムやアプリケーションレベルで実行されている他の制御を事実上破壊することを可能にすることができます。TrickBot/TrickBootのようなファームウェアベースの脅威の台頭により、セキュリティチームは、デバイスのファームウェアの完全性を検証し、それが侵害されていないことを確認できるようにする必要があります。この検証なしには、より高度なセキュリティ制御を、暗黙のうちに信頼することはできません。

この必要性は、ファームウェアとデバイスのオペレーティングシステムがはるかに統合されているネットワークデバイスにおいて、より顕著になります。もし、攻撃者がファームウェアやマシンレベルのコードを侵害することができれば、そのデバイスを制御できる可能性が高くなります。

## ゼロ・トラストはネットワーク・デバイスの完全性に依存する

ネットワーク機器とセキュリティ機器は、ゼロ・トラスト・アーキテクチャにおいて、非常に重要な役割を担っています。多くの場合、これらのデバイスは、トラフィックを配信、分析し、最終的にゼロ・トラスト・ポリシーを実施するデバイスです。これらのデバイスに対する攻撃の増加に伴い、攻撃者は、まさに文字通り組織のゼロ・トラスト戦略を定義するテクノロジーを弱体化させようとしています。

これらの組織は、スイッチの言う通信が実際に通信しているものであることを「信頼」できる必要があります。ファイアウォールやIPSがトラフィックを正確に分析し、脅威や不正アクセスをブロックすることを信頼できなければなりません。トラフィックの機密性が保持され、意図した宛先にのみ送信されることを信頼できなければならないのです。

ほとんどの組織は、これらのデバイスがその役割を果たすことを暗黙のうちに信頼しています。しかし、ゼロ・トラストは、セキュリティ・チームに、ITとOTのスタックの中で暗黙のうちに信頼されている領域を探し出すよう求めています。ゼロ・トラストにおけるネットワーク・デバイスの基本的な役割を考えると、これらのデバイスの完全性を検証することが不可欠です。

## データプレーンとコントロールプレーンの分離

NISTのSP 800-207は、データと制御の論理的分離を維持することの重要性を広範囲にカバーしています。
ゼロトラストアーキテクチャーでは、プレーン ネットワークデバイスの場合、コントロールプレーンは管理者がデバイスを管理し、ポリシーを更新し、その他の設定を管理するための独立した経路を提供し、データプレーンはエンドポイント間のアプリケーショントラフィックを提供します。コントロールプレーンを分離することで、企業はデバイスへのアクセスを制限し、ポリシーの変更が有効かつ承認されていることを確認するための厳格な制御を適用することができます。

しかし、ネットワーク機器では、データプレーンとコントロールプレーンを論理的に分離することは可能ですが、その基盤となるファームウェアを共有することが多くなります。このため、ファームウェアが侵害されると、攻撃者は両方のプレーンにアクセスすることができるようになります。サーバのベースボード管理コントローラ（BMC）のように、デバイスが別々の物理的なファームウェアを持っている場合でさえ、データまたは管理ハードウェアのいずれかが侵害されると、攻撃者はもう一方のプレーンにピボットできることが調査で明らかになっています。このことは、ネットワークデバイス上のすべてのファームウェアとデバイスコードの姿勢と完全性を 検証することの重要性を、改めて浮き彫りにしています。

## ネットワークデバイスを保護するための重要な要件

ネットワークデバイスのセキュリティは、セキュリティのベストプラクティスと運用を新しいクラスのデバイスに拡張することを組織に要求します。しかし、従来のセキュリティツールは、汎用的なオペレーティングシステムやソフトウェアを保護するように設計されており、ネットワークデバイスのデバイスコード、ファームウェア、ハードウェアが密接に統合された独自のリスクや脅威に対処することはできませんでした。このため、組織で最も価値の高いデバイスの一部が最も保護されていない「リスク・ギャップ」が生じています。

以下の要件は、セキュリティリーダー、アーキテクト、実務者がこのギャップに対処し、ネットワークデバイスが相応の保護と運用の厳しさを受けられるようにするために役立ちます。

### サプライチェーンの検証

組織のセキュリティ対策は、ネットワーク・デバイスが物理的または仮想的に納品される前から始める必要があります。セキュリティ・チームは、ベンダーの選定段階における評価プロセスの標準的な部分として、見込みのあるネットワーク・デバイスに脆弱性や設定ミスがないかどうかをスキャンする必要があります。

現代のテクノロジー・サプライ・チェーンは、メーカーがコスト削減や供給不足の解消を図る中で、常に変化しています。このような変化に対応するため、企業はベンダーに対して、すべてのデバイスソフトウェアとファームウェアを含む最新のソフトウェア部品表（SBOM）を提供するよう求める必要があります。また、新しく受け取ったデバイスをスキャンし、デバイス内の実際のコードがSBOMと一致し、脆弱性がないことを確認する必要があります。

サプライチェーンの問題は、デバイスが配備された後にも、アップデート中に生じたミスや脅威によって発生する可能性があります。ネットワークデバイスは、アップデート後にスキャンと監視を行い、すべてのセキュリティ設定が適切に有効になっていることを確認し、異常や脅威の兆候を検出する必要があります。

### ディスカバリーと可視化の自動化

組織は、ネットワークデバイスを可視化する必要があり、可能であれば、内部コンポーネントを可視化する必要があります。多くの企業では、従来のセキュリティ・エージェントをサポートしない多数のネットワーク・デバイスが存在するため、これは困難な課題となっています。

そのため、企業は、ネットワーク・デバイス自体にエージェントを展開することなく、分散した企業内のあらゆる場所のネットワーク・デバイスを自動的に検出するツールを用意する必要があります。どのような検出プロセスも、ユーザーのプライバシーを保護し、企業以外の環境が不用意に分析されないように、厳密に制御する必要があります。

### 脆弱性とリスク管理

セキュリティ・チームは、ネットワーク・デバイスのセキュリティ・ポストをプロアクティブに可視化する必要があります。これには、ネットワーク機器に固有の脆弱性や機器の設定ミスをスキャンする機能も含まれます。ファームウェアレベルの脆弱性の多くは、認証されていない単純な脆弱性スキャンでは検出されません。そのため、可能な限り、認証されたスキャンをサポートするツールを使用する必要がある。デバイスが通常の認証済みスキャンをサポートできない場合、脆弱なデバイスを特定するために、API のような代替手段を介して、デバイスのフィンガープリントやデータ収集ができるようにする必要があります。

また、多くのベンダーやデバイスの種類にまたがって一貫性のある脆弱性管理プログラムを確立するよう努力する必要があります。ほとんどの企業では、複数のネットワーク・セキュリティ・ベンダーが存在するため、ベンダー固有の定期的なスキャンに頼ると、重大なリスクをすぐに見逃してしまうことになります。攻撃対象領域を包括的かつ確実に可視化するには、ベンダーにとらわれない自動化されたアプローチが重要です。

セキュリティ・チームは、ネットワーク・デバイスの脆弱性が検出された場合に、優先順位を付けるための適切なツールとプロセスを導入しておく必要があります。従来のネットワークベースのスキャンで検出される数千の脆弱性の中から脆弱性を見逃すことがないよう、ネットワークデバイスの専用ビューを検討するのもよいでしょう。また、実際に悪用されている CVE を自動的に優先順位付けできるようにする必要があります。

# 企業のシステムインフラを防御する

### デバイスのパッチとアップデート

チームは、できるだけ少ない労力で、迅速に脆弱性に対処する必要があります。例えば、新しいファームウェア・バージョンのチェック、適切なパッケージのダウンロードと検証、さらにはアップデートの適用など、アップデートの手動ステップの多くを自動化するツールを検討するとよいでしょう。

### 整合性監視と脅威の検出

セキュリティチームは、アクティブな脅威や侵害の兆候をプロアクティブに特定するための武装をする必要があります。これは、ネットワーク・デバイスに適用する場合、さまざまな形で行うことができます。まず、デバイス上の実際のコードと、ベンダーが提供する有効な公開コードを暗号化して比較し、デバイスのファームウェアとコードの整合性を検証する必要があります。デバイス上のファームウェアは、従来のデバイス上の他のコードよりもはるかに安定し、予測可能であるため、このホワイトリストのアプローチは強力な最初のステップとなります。

次に、既知の脅威の存在や侵害の兆候をスキャンする必要があります。攻撃者は、インプラントやバックドアを開発する際に、定期的に過去の脅威のコンポーネントを再利用し、再目的化しています。多くの脅威は、デバイスに微妙な設定変更を加えるため、デバイスの詳細なスキャンが重要になります。

最後に、企業は、デバイス上のコードの動作を監視できるようにする必要があります。ファームウェアは、やはり従来のソフトウェアよりもはるかに予測しやすく、比較的狭い範囲の動作に適合します。この基準値からの逸脱は、脅威が未知のものであったり、ベンダーの正当な更新の一部として導入されたものであったりする場合でも、脅威の兆候を特定するのに役立ちます。

### エクリプシウムの紹介

エクリプシウムは、サーバ、ノートPC、幅広いネットワーク機器など、組織の最も重要なレイヤーのセキュリティをシンプルかつ自動で提供します。エクリプシウムは、クラウドベースのファームウェアセキュリティソリューションで、デバイス自体にエージェントをインストールすることなく、ネットワークデバイスとネットワークインフラの完全な可視化と制御をチームに提供することが可能です。主な機能は以下のとおりです。

識別 - ネットワークデバイスを自動的に検出し、ファームウェア、ハードウェア構成、およびネットワークデバイスとインフラ内の数十のコンポーネントを継続的に可視化します。セキュリティに影響を与える可能性のある重要なデバイス、コンポーネント、属性、または変更に素早く対応します。

検証 - 古くなったファームウェアや脆弱なファームウェア、デバイスの誤設定によるリスクを事前に特定します。すべてのファームウェアの整合性を検証し、ルートキット、インプラント、バックドアなど、既知および未知のファームウェアの脅威を検出します。

強化 - パッチやアップデートをリモートで適用し、デバイスのリスクをプロアクティブに軽減します。主要なSIEM、脆弱性管理、デバイス管理ツールとあらかじめ統合されているため、既存のITおよびセキュリティ・ツールとの統合により、ファームウェアの完全性の変更に対する自動アラートを受信し、自動応答を実行します。

### 今後の展望と次のステップ

ネットワーク機器は、サイバーセキュリティにおいて最も活発な分野の1つであり続けています。この数カ月で状況は急速に進化しており、あらゆる兆候から、攻撃者は今後もネットワーク機器への攻撃を加速させることが予想されます。大規模なランサムウェアや金銭的動機のあるグループは、APT脅威行為者によって以前実証された技術を採用し、前例のない規模で運用を続けています。初期アクセスブローカー（IAB）は、競合する犯罪グループに対して優位に立とうと、新たな脆弱性を特定し、悪用し続けています。

エクリプシウムは、これらの重要なデバイスが可能な限り安全であることを保証するために、セキュリティ研究と制御によって業界を前進させることに専心しています。私たちのプラットフォームは、セキュリティ・チームがネットワーク・デバイスを可能な限り安全に保つために必要なツールを提供します。

エクリプシウムがどのようにお客様の組織を保護するか、ファームウェア・セキュリティについて、より詳しくお知りになりたい場合は、jp-info@eclypsium.comまでお問い合わせください。