# FortiNAC：セキュリティの自動化 / オーケストレーションプラットフォーム

## 要約

クラウド、IoT（モノのインターネット）、モバイルテクノロジーの普及は、企業における自社ネットワークの保護方法に変化をもたらしました。これまでのセキュリティ対策のままでは、エンドポイントが脆弱になり攻撃の標的となる恐れがあり、重要なデータの保護には次世代のネットワークアクセス制御（NAC）が必要です。FortiNAC は、ポリシーベースのセキュリティの自動化とオーケストレーションのプラットフォームを提供します。エンドポイントやネットワークインフラストラクチャのあらゆるデバイスを検知し、動的なネットワークアクセス制御の実装に必要なコンテキストに基づく識別機能を提供することで、自動化された脅威へのレスポンスが可能となり、サイバーブリーチを封じ込めます。

## FortiNAC：透過的、動的なアクセス制御の自動化

サイバー犯罪者は、エンドポイントデバイスを格好の攻撃ポイントと考え、企業ネットワークへの不正アクセスの足掛かりにしようとしています。このような脅威の対策として、組織はエンドポイントに起因するリスクの検知と封じ込めに毎週 1,156 時間を費やし、週あたり平均で 340 万ドルを投じていることが明らかになっています。[1]

エンドポイントの検知とレスポンスを自動化するソリューションは、自社のエンドポイントを即座に制御したいと考える IT プロフェッショナルの再優先事項となっています。[2] レスポンスとワークフローを自動化することで、検知の高速化と保護の強化が可能になり、リソース不足で過剰な負担を強いられているセキュリティチームの作業を軽減することができます。

フォーティネット セキュリティ ファブリックの一部として統合される FortiNAC は、エンドツーエンドのネットワークの可視化、動的なネットワークアクセス制御、脅威レスポンスの自動化を実現する、次世代の NAC ソリューションです。FortiNAC は、複雑な脅威のトリアージプロセスを自動化してセキュリティアラートへの迅速なレスポンスを可能にすることで、企業の資産や知的財産への不正アクセスのリスクを最小化すると同時に、デバイスに起因する脅威の封じ込めの影響、時間、コストを軽減します。

## ネットワーク全体の可視化

常に変化するネットワークの保護にあたっては、ネットワークの構造を正しく理解することが極めて重要であり、見えないものを保護することはできません。効率的な NAC プラットフォームには、まず最初にすべてのユーザー、アプリケーション、デバイスを検知した後にアクセスのオーケストレーションを実行する能力が求められます。

### エンドポイントとユーザーの識別と分類

FortiNAC は、エージェントレススキャンを実行することで把握した特長やビヘイビア（ふるまい）に基づき、ネットワークの各要素をプロファイリングします。まず、エンドポイントを自動的に検知してプロファイリングし、デバイスをタイプ別に分類して、デバイスが会社所有または従業員所有のどちらであるかを判断します。ユーザーを識別した後にロールベースの適切なネットワークアクセスポリシーが実装されるため、重要なデータや機密性の高い資産が保護されます。

### ゲストアクセスの簡素化

FortiNAC は、ゲストユーザーの安全な登録プロセスを合理化します。ゲストユーザーの適正が確認されると、ユーザーが自分のデバイス（ノート PC、タブレット、またはスマートフォン）を自分で登録できるようになるため、IT スタッフの作業負荷が軽減されます。また、ゲストの初期登録に関するタスクをネットワーク管理者に任せることも可能になります。

## 詳細なアクセス制御

企業ネットワークでは、デバイスの増加と多様化が進んだだけでなく、さまざまな異なるユーザー、グループ、アプリケーションがホストされるようになりました。この複雑さに対処するため、NAC ソリューションに対して動的なアクセス制御とセグメント化の機能が求められるようになりました。

### ネットワークの動的なセグメンテーション

デバイスやユーザーが識別されると、FortiNAC によって適切なレベルのアクセスがデバイスやユーザーに割り当てられて、関連性のないコンテンツの使用が制限されます。このロールベースの動的なネットワーク制御では、アプリケーションや類似データをグループ化することで詳細なネットワークセグメントが論理的に作成され、特定のユーザーのグループのみにアクセスが制限されます。この方法によって、いずれかのデバイスが感染した場合も、ネットワークに感染が拡大したり、他の資産が攻撃されたりするのを防ぎます。

FortiNAC では、セグメンテーションポリシーを実装し、70 以上のベンダーのスイッチや無線製品の構成を変更することができます。これにより、異機種混在環境においても、サードパーティ製品までセキュリティファブリックのカバーする領域が拡大されます。

### 継続的なリスク評価

ネットワークに接続する前にデバイスの整合性が担保されるため、リスクやマルウェアが増加する可能性が最小限に抑制されます。FortiNAC は、ネットワークに参加しようとするデバイスの構成を検証し、コンプライアンスに違反すると判明したデバイスについては、隔離したり限定的な VLAN へのアクセスに制限したりできます。そして、デバイスの構成の修正が必要であることがユーザーに通知されます。適切な修正が行われた後にのみアクセスが許可され、その場合でも FortiNAC がデバイスの詳細情報を連続してスキャンし、接続後の継続的評価を実施します。

## セキュリティの自動化

ポリシーベースの自動化されたセキュリティアクションは、統合セキュリティアーキテクチャの中核とも言うべき要素です。このアクションによって、NAC ソリューションは組織全体でリアルタイムのインテリジェンスを共有可能になり、潜在的な脅威を拡散前に封じ込めることができます。さらに、自動化は作業量の増加やリソース不足に悩むセキュリティチームの負担軽減にも貢献します。

### 脅威の封じ込めに要する時間を大幅に短縮

FortiNAC では、広範でカスタマイズ可能なポリシーが提供されており、セキュリティ ファブリックで観察されたユーザーやデバイスの不正なビヘイビアを瞬時に封じ込めることができます。エンドポイントで感染や脆弱性が確認されると、FortiNAC によって自動レスポンスがトリガーされます。このレスポンスには、接続の強制終了、ネットワークアクセスの制限、検疫による隔離、さまざまな方法での通知などのアクションが含まれます。このような制御機能は、Web ベースの管理ダッシュボードからアクセス可能で、ダッシュボードは高度なカスタマイズおよび容易な活用ができます。FortiNAC は、脅威の封じ込めに要する時間を数日から数秒へと大幅に短縮するだけでなく、厳格化される法規制、標準、およびデータ保護法へのコンプライアンスにも対応します。

### アラートの優先順位付け

FortiNAC は、感染したエンドポイントにユーザー、アプリケーション、ネットワークの接続を相関付けし、そのインテリジェンスをフォーティネット セキュリティ ファブリック全体で共有することでセキュリティアラートの信頼性を向上させます。セキュリティアラートのトリアージが自動的に実行され、セキュリティインシデントの深刻度やビジネスにとっての重要度に基づき、優先順位に応じて 1 つ以上の封じ込めアクションが実行されます。

## 柔軟性と拡張性を兼ね備えた NAC の導入

FortiNAC は、比類のない可視化、制御、自動レスポンスを可能にする、セキュリティの自動化とオーケストレーションのプラットフォームを提供します。このような中核機能だけでなく、FortiNAC はハードウェアアプライアンス、仮想アプライアンス、あるいはクラウドサービスとして導入できるため、あらゆるネットワーク環境の固有のニーズに対応する、柔軟性の高い第 3 世代 NAC ソリューションをセキュリティアーキテクトに提供します。FortiNAC は、拡張性のニーズを念頭に設計されており、配備先各々にサーバーを設置する必要がないため、TCO の削減にも貢献します。既存のディレクトリ、ネットワーク、セキュリティのインフラストラクチャを活用する FortiNAC は、これまでの投資を保護すると同時にシステム運用の中断を最小限に抑制可能な優れた NAC ソリューションです。

[1] 「The Cost of Insecure Endpoints（リスクのあるエンドポイントの代価）」、Ponemon Institute、2017 年 6 月：
https://www.absolute.com/en/go/reports/the-cost-of-insecure-endpoints

[2] 「Endpoint Protection and Response: A SANS Survey（エンドポイントの保護とレスポンス：SANS サーベイ）」、Lee Neely 著、SANS Institute、2018 年 6 月 12 日：
https://www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460

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.co.jp/contact

お問い合わせ