FortiNAC による
包括的な IoT セキュリティの簡素化

要約

IoT（モノのインターネット）デバイスに起因するリスクは、ネットワークの保護において最も困難な問題の 1 つといえるでしょう。310 億台ものの IoT デバイスが 2020 年までにインターネットに接続されるようになると予測される中[1]、サイバー犯罪者がエクスプロイト可能な新たな脆弱性を次々と発見し、IoT デバイスを標的にする攻撃が急速に進化していることから、ビジネスを継続する上でこれらのデバイスの保護が不可欠となってきています。[2] FortiNAC は、IoT エンドポイントの可視化、ネットワークアクセス制御、脅威への自動レスポンスを可能とし、あらゆる組織のセキュリティに対するニーズを解決します。あらゆるファイアウォールとの機能連携や他のセキュリティソリューションとのシームレスな統合が可能であるため、セキュリティへの既存の投資を有効活用しながら強力なセキュリティ環境を構築できます。

IoT の脆弱性によるデータ侵害の増加

Ponemon Institute による最近の調査では、リスク管理のプロフェッショナルの 97% が、保護されていない IoT デバイスに起因するデータ侵害が自社に壊滅的な被害をもたらす恐れがあると考えていることが報告されています。そのような状況にもかかわらず、自社の IoT デバイスの包括的なインベントリが存在するという回答は、わずか 15% にとどまっています。[3] IoT やその他のヘッドレスデバイスが格好の標的になってしまうのは、ほとんどのファイアウォールがこのようなタイプのエンドポイントの認識や保護が不可能であることが原因です。

これらのデバイスベースのリスクの発生には、主として、次の 2 つの要因があります。

無意識の共犯者とシャドー IT：ほとんどの従業員は、インターネット対応のコーヒーメーカー、冷蔵庫、プリンター、プロジェクターなどの一般的なオフィス機器を使用する際に、ネットワークセキュリティの潜在的なリスクが存在することに未だ気付いていません。しかしながら、これらのデバイスは製造元に情報を自動送信したり、インターネット経由で他のデバイスと情報を共有したりするように設計されており、そのようなデバイスが外部のネットワークに接続していることに持ち主が気付いていない場合もあります。

ビジネスの課題を少しでも解決しようとする従業員の善意からの行為によって、ネットワークに接続する新たなテクノロジーが IT 部門を介在することなしに追加されてしまうことがよくあり、結果としてサイバー攻撃の新たな侵入口が開かれてしまうことがあります。また、組織のセキュリティエキスパートによる承認も監視も受けることなく、ユーザー自身によって管理される、シャドー IT と呼ばれるアプリケーションやエンドポイントにも同じ問題があります。シャドー IT は悪意のある行為ではないものの、大きなトレンドとなったことで、大企業の IT 支出の 50% を占めるまでになりました。[4] そして、そのことによって組織が大きなリスクにさらされることになっています。

保護されていないヘッドレスデバイス：セキュリティカメラ、空調センサー、医療機器、さらにはそれに類似する数千ものネットワーク接続されたデバイスやスマートデバイスが組織で利用されると、その多くが IoT 対応であることから、ビジネス運営の効率化という面では大いに役立つことになるといえます。しかしながら、セキュリティを考慮してこれらのデバイスが設計されることはほとんどありません。ヘッドレスデバイスにはメモリや処理装置がなく、PC や電話のような従来型のインタフェースやオペレーティングシステムがないため、有効性のあるセキュリティ機能を組み込んで実行することはできません。さらには、ファームウェアに PIN がハードコード化されているためにパッチやアップデートを適用できない IoT デバイスも存在します。

また、IoT デバイスにはユーザーが関連付けられていないため、ユーザーベースでアクセスの可否が判断される既存のファイアウォールやその他のセキュリティソリューションで認証し、保護することはできません。多くの場合、セキュリティチームはこのようなデバイスが IoT 対応であることや、既存のセキュリティインフラストラクチャでは保護できないものであることを理解していません。また、ICS（産業用制御システム）や PLC（プログラマブルロジックコントローラ）などの他のヘッドレスデバイスについても、これと同じ問題が存在します。

見えないものは保護できない

接続されているすべてのエンドポイントをリアルタイムで可視化することは、セキュリティギャップの解消に不可欠な第一歩となります。存在することがわかっていないデバイスを保護することはできません。フォーティネット セキュリティ ファブリックの構成要素として統合される FortiNAC は、ネットワークに接続しているすべてのデバイスのライブインベントリによってリアルタイムの可視化を実現します。

FortiNAC は、アクセス制御機能の欠如やレガシーな性能によって生じるセキュリティギャップを解消することを目的に設計された、使いやすいワンストップソリューションです。ネットワークのロックダウンを可能にすることで IoT デバイスのオンボーディング（初期設定）と管理を簡素化すると同時に、デバイスアクセスの制御によって重大なセキュリティギャップを解消します。FortiNAC の主な中核機能は以下のとおりです。

1. エンドポイントのプロファイリングおよび分類：組織内で増加する IoT や BYOD（私的デバイスの活用）のエンドポイントの問題に対処するため、FortiNAC では、デバイスが自動的に検出され、会社所有または個人所有のいずれかに分類されます。すべてのデバイスの詳細と使用場所に関する情報が FortiNAC によって提供され、プロファイリングされたデバイスには、そのデバイスが機能するために必要な資産のみにアクセスが許可されます。たとえば、IP（インターネットプロトコル）カメラの場合であれば、NVR（ネットワークビデオレコーダー）サーバーへのアクセスが許可され、財務や法務の部門サーバーへのアクセスは許可されません。

2. セキュリティ対策の施されていない / ヘッドレスデバイスの制御：FortiNAC では、サードパーティのネットワークデバイスにセグメンテーションポリシーを実装するように構成可能で、70 社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。この動的な制御機能により、異機種混在環境においてセキュリティ ファブリックの網羅する領域が拡大します。また、既存のネットワークインフラストラクチャを使用することで、コストと時間の削減にも貢献します。

IoT デバイスの導入を簡素化

FortiNAC は、スポンサー機能を使用して認証プロセスの多くを自動化することで、IoT デバイスの導入を簡素化します。新しい IoT デバイスがネットワークへの接続を試みると、FortiNAC によって自動的にデバイスが隔離されたネットワークに配置され、プロファイリングが行われます。デバイスの情報や疑わしいデバイスのタイプについては、確認や認証の目的で所定の部門へと送信されます。デバイスの確認が完了すると、デバイスのタイプと配置先が FortiNAC からファイアウォールに通知され、適切なネットワークセグメントに配置されます。このソリューションは、アップグレードと拡張も容易であるため、あらゆる規模、あらゆる業種の組織に導入することが可能です。

あらゆるファイアウォールと機能連携し、他のセキュリティ製品とのシームレスな統合が可能な FortiNAC ソリューションは、既存の投資を最大限に活用し、組織の防御体制の強化を支援します。FortiNAC では、あらゆる組織のニーズに対応する多様な導入オプションが提供されています。

- **FortiNAC Base ライセンス**：IoT / ヘッドレスデバイスの保護とネットワークの簡易的なネットワーク制御を必要とするものの、高度なネットワーク制御や脅威への自動レスポンスを必要としない組織に最適です。
- **FortiNAC Plus ライセンス**：エンドポイントの完全な可視化ときめ細かい制御が可能な柔軟性の高い NAC ソリューションを必要とするものの、脅威への自動レスポンスを必要としない組織に最適です。
- **FortiNAC Pro ライセンス**：エンドポイントの完全な可視化ときめ細かい制御が可能な柔軟な NAC ソリューションに加えて、高精度のイベントのトリアージや脅威に対するリアルタイムの自動レスポンスを必要とする組織に最適です。

製品	要件	可視性	制御	レスポンス
FortiNAC Base ライセンス：デバイスのアクセスに関するセキュリティギャップを解消し、シャドー IT によって生じることの多い監査の回避を排除し、ネットワークの簡易的なネットワーク制御を可能にするよう設計された、エントリーレベルの製品です。	高度なユーザー / ネットワーク制御、常駐エージェント、または脅威への自動レスポンスを必要としない組織に最適です。	◔	◑	○
FortiNAC Plus ライセンス：より高度なネットワークアクセス制御機能が追加され、ユーザー、ゲスト、デバイスの自動的なプロビジョニングと制御が可能になります。ユーザーの役割やデバイスに基づき、決められた範囲のアクセス権だけが付与されます。FortiNAC Plus は、接続前と接続後にスキャンを実行し、ネットワークセキュリティの最小要件を満たしているデバイスだけにアクセスを許可し、特定の問題についてはユーザーに自己減災を指示することも可能です。さらに、コンプライアンス違反のデバイスはもちろん、ネットワーク接続中にコンプライアンス違反になったデバイスについても、ポリシーに基づいて自動隔離することができます。	エンドポイントの完全な可視化ときめ細かい制御が可能な高度な NAC ソリューションを必要とするものの、イベントのトリアージ、イベントの相関付け、あるいは脅威への完全な自動レスポンスを必要としない組織に最適です。	●	●	○
FortiNAC Pro ライセンス：リアルタイムのエンドポイントの可視化、包括的なアクセス制御、脅威に対する自動レスポンスを可能にし、コンテキストに基づく情報とアラートのトリアージ機能を提供します。より広範なフォーティネット セキュリティ ファブリックとの統合によって、他のソリューションからのログやデータの取り込みを可能にします。さらに、相関エンジンを活用した深刻度に基づくアラートのトリアージによってイベントトリアージの精度を向上させ、分析担当者にアラート（およびすべてのコンテキストデータ）を提示します。 FortiNAC は、これらすべての情報を 1 つの包括的なアラートとして提示することで、人手によるセキュリティのレビュープロセスの多くを自動化します。このような自動化によって、IT 分析担当者によるアラートの分類とイベント情報の調査の所要時間が大幅に短縮され、脅威の封じ込めに要する時間が数日からわずか数秒へと大幅に短縮されます。 FortiNAC の自動化されたルールによって、セキュリティアーキテクチャ（FortiGate、FortiSwitch、FortiAP、あるいは統合されたサードパーティのソリューションなど）全体で脅威の封じ込め設定が実行されます。	NAC のすべての機能を 1 つのソリューションで導入したいと考える組織に最適です。FortiNAC の最上位ライセンスである FortiNAC Pro は、最上級の可視化、制御、自動レスポンス機能を提供します。	●	●	●

[1]「The Internet of Things (IoT) units installed base by category from 2014 to 2020（2014 ～ 2020 年のカテゴリ別 IoT 装置インストール数）」、Statista、2017 年 2 月（2018 年 8 月 24 日にアクセス）：https://www.statista.com/statistics/370350/internet-of-things-installed-base-by-category/

[2]「脅威レポート 2018 年第 2 四半期版」、フォーティネット、2018 年 8 月 2 日：https://www.fortinet.co.jp/fortiguard/threat-intelligence/threat-landscape.html

[3]「Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party Risk（IoT に関する第 2 回年次調査：サードパーティリスクの新時代）」、Ponemon Institute、2018 年 3 月：https://sharedassessments.org/wp-content/uploads/2018/04/2018-IoTThirdPartyRiskReport-Final-04APR18.pdf

[4] Peter Bendor-Samuel 著、「How to eliminate enterprise shadow IT（シャドー IT を排除する方法）」、CIO、2017 年 4 月 11 日：https://www.cio.com/article/3188726/it-industry/how-to-eliminate-enterprise-shadow-it.html

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