# WatchGuard Network Discovery

Technical Brief

WatchGuard Technologies, Inc.

発行日: 2016 年 5 月

## はじめに

このテクニカルブリーフでは、Network Discovery 機能について説明します。Network Discovery は、Fireware® オペレーティングシステム　バージョン 11.11 以降を搭載する全ての WatchGuard Firebox® モデルで利用できます。この機能の仕組みと、企業にとってこの機能がセキュリティ上重要である理由について説明します。

**ネットワークの安全を図るためには、ネットワークの状況を把握することが大事。**

情報セキュリティにおけるベストプラクティスでは、ネットワークセキュリティを担当する管理者が最新のネットワーク構成図を作成してセキュリティ維持することが求められます。脆弱性管理プログラムで最初に実行するべきことは、ネットワークにあるすべてのデバイスを検出・特定し、その役割を把握することが、情報セキュリティの担当者は長きにわたって教えられてきました。

たとえば、PCI DSS Requirement 1.1.2 は、「クレジットカード所有者のデータ環境と無線ネットワークを含む他のネットワークとのすべての接続を特定する現在のネットワーク構成を示すこと」を求めています。*1

IT インフラストラクチャは、IT 担当の前任者から引き継がれることが多くあります。自身が始めから設計したネットワークを最初から利用する IT 管理者はほとんどいないでしょう。ネットワークの構成を記した Visio のダイアグラムが存在していれば幸運ですが、特に中小企業ではネットワーク構成が十分に把握されていない場合があります。マネージドサービスプロバイダー（MSP）がクライアントと業務を行うときに最初に行う業務の 1 つは、既存のパートタイムの IT スタッフが導入してきたあらゆるデバイスを検出することです。
ネットワークの維持およびセキュリティの保護に責任を持つ MSP にとって、接続されているすべてのデバイスを検出することは非常に重要な業務の 1 つです。

しかし、デバイス検出プロセスで最も重要なのは、特に企業が把握していない、新しいエンドポイントデバイスの接続を監視することです。把握していないデバイスがネットワークに接続されていた場合には、いくつかの脅威をもたらす恐れがあります。

---

*1 PCI データセキュリティスタンダードの要件とセキュリティ評価手順、バージョン 3.1、2015 年 4 月。PCI Security Standards Council (LLC at www.pcistandards.org) から詳細情報を入手できます。

### 1）社員などの従業員によって接続された許可されていないデバイス

従業員が個人のノート PC を自宅から持ち込む場合、エンタープライズクラスの検知率の高いエンドポイントアンチウイルスによる保護が適用されていない場合が多くあります。従業員が企業のネットワークに有線または無線で接続したりすると、企業の IT 環境全体がセキュリティのリスクにさらされる恐れがあります。
従業員は、Web サーバなどのサーバアプリケーションやソフトウェアを IT 部門の許可なく業務のために勝手にインストールしている場合もあります。これらのソフトウェアをインストールして使用することは簡単ですが、脆弱性を攻撃するコードから保護するために定期的にパッチを適用するなどのベストプラクティスに従っていない場合があります。
従業員の不注意が原因で起こる別の脅威の例：従業員は、職場でより簡単にネットワークアクセスできるように、許可されていないワイヤレスアクセスポイントを導入する場合がありますが、これが企業ネットワークの弱点となり、外部の攻撃者の標的となる恐れがあります。

### 2）攻撃者は、企業ネットワークをハッキングするための方法を模索している

さらに危険なのは、ハッカーがスイッチやルータなどのネットワークポートやネットワークデバイスに不正接続しようとする行為です。
悪意のあるソフトウェアが企業のデバイスにインストールされる場合があります。ボットネットは、通常とは異なる通信手段によって、C&C サーバとやりとりするボットソフトウェアをインストールする場合があります。

## 現在のソリューション

現在のネットワーク管理者は、nmap*2 のようなオープンソースツールを使用して、ネットワーク上のすべてのデバイスをスキャンしています。中堅中小企業は、自社環境にあるすべてのコンピューティングデバイスを追跡・把握することに非常に苦労しています。複雑なデバイス検出システムや脆弱性管理システムを購入する余裕がないため、柔軟で効率的な人気の高いオープンソースユーティリティ nmap などを利用しています。nmap は、Raw IP パケットを使用して、ネットワークで利用可能なホスト、これらのホストが提供しているサービス（アプリケーション名とバージョン）、およびホストで実行されているオペレーティングシステム（およびそのバージョン）を判別します。ウォッチガードの Network Discovery 機能を使用すると、nmap で提供される基本機能よりも優れたスキャン機能を提供します。デバイスの詳細が表示されるビューをインタラクティブに利用でき、ファイアウォールからのリアルタイムのログと脅威情報が統合されて表示されます。

## WatchGuard Firebox と Network Discovery

WatchGuard の統合セキュリティアプライアンス製品　Firebox を使用すると、管理者は特別なツールを購入しなくても、ネットワークに接続するあらゆるデバイスを確認できます。ネットワーク管理者は、スキャンを定義し、即時実行したり、負荷が少ない時間帯に実行するようスケジュールすることもできます。このスキャンでは、nmap のテクノロジと別の手法が組み合わせて使用されます（以下に詳細を示します）。スキャン結果は、インタラクティブなビジュアルマップとして Web ユーザインターフェイスに表示されます。

---

*2: nmap の詳細については、オープソースプロジェクト（https://nmap.org/）を参照してください。

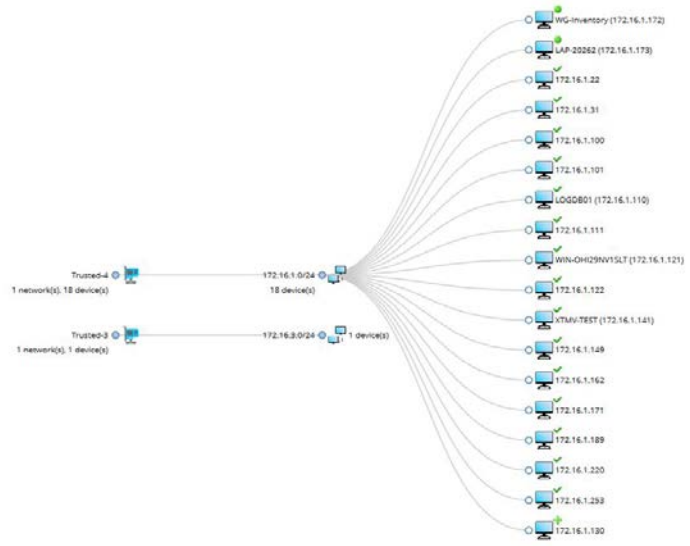


図 *1. Network Discovery* はネットワーク上にあるすべてのノード（デバイス）のネットワークマップ（構成図）を作成

IT 担当者は、Network Discovery を使用すると、ファイアウォールの外側にあるネットワークもマッピングできます。ネットワークにあるデバイスが特定され、次のようなアイコンで表示されます。

- IP アドレス
- MAC アドレス
- デバイスのタイプ - iOS、Android、MAC、Windows など
- オープンしているすべてのポート - IT 管理者は、Web サーバのポートがネットワークに対して開いているかどうかを確認できます。この情報は、ネットワークの潜在的なセキュリティ侵害を示す場合があります。

管理者は、すべてのデバイス情報を検索およびフィルタして、重要な情報を重点的に調査できます。デバイスに「確認済み」（Approved Device）とマークして、分かりやすい名前を割り当てることもできます。新しい不明なデバイスには名前が付けられておらず、把握が簡単にできます。

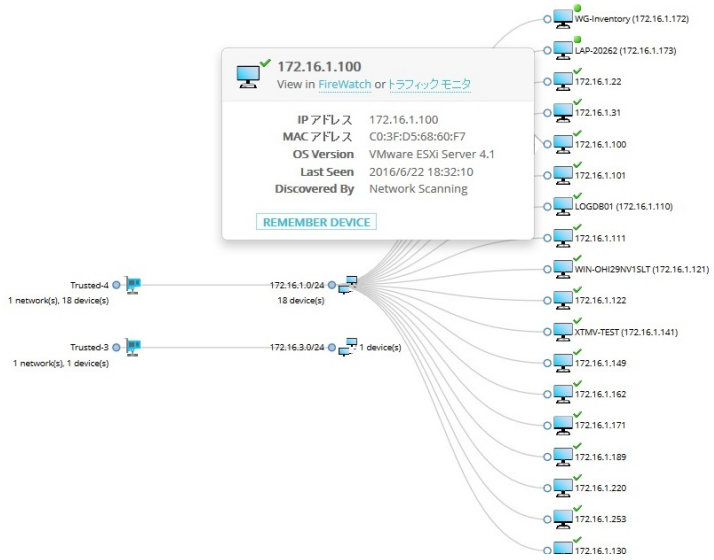


図 *2. WatchGuard FireWatch* と *Traffic Monitor* のワンクリックでの連携

ファイアウォールを管理している担当者は、FireWatch および Traffic Monitor など可視化ツールを組み合わせて、疑わしいデバイスを即座に調査できます。ワンクリックで FireWatch にアクセスし、指定した IP アドレスがどのような通信をしているか視覚化できます。

ネットワークに接続するためにデバイスが使用しているポートの詳細を表示するには、**[Scanned Port]**タブを選択します。デバイスが nmap のネットワークスキャンで検出される場合にのみ、[Scanned Port]タブが表示されます。

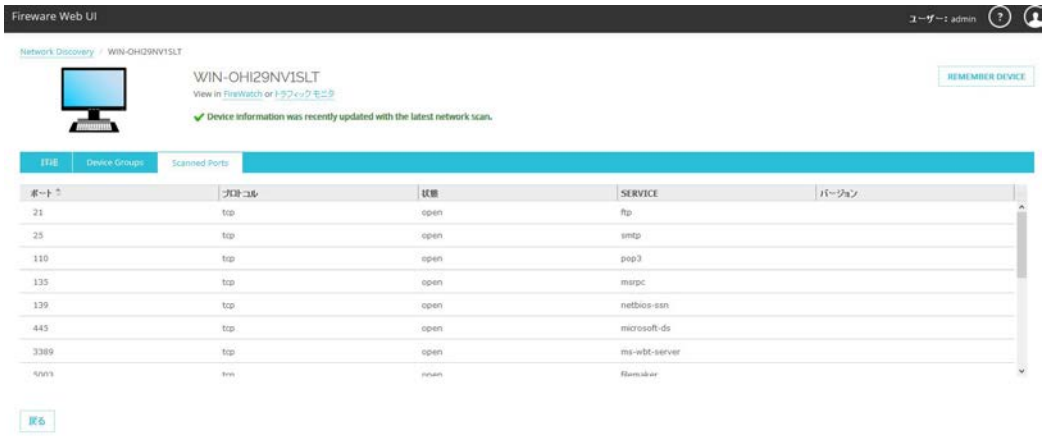


図 *3. Network Discovery* のスキャンによって明確になる詳細情報

各ポートについて次の詳細が表示されます。

- ポート - ポート番号
- プロトコル - TCP や UDP などのポートで使用されているプロトコル
- 状態 - ポートの現在の状態
- サービス - ポートで使用されているサービス名
- バージョン - 利用可能な場合、サービスのバージョンが表示されます

## Network Discovery による資産の把握

ネットワークにあるデバイスを特定するために、多くの手法を利用できます。精度の高い手法の順に、これらを列挙します。Network Discovery は、ネットワークにあるデバイス情報を判別するために利用可能な最も精度の高い オプションを常にデフォルトで使用します。

- iOS および Android デバイスにインストールされるウォッチガードのモバイルセキュリティエージェントである FireClient
- ホットスポットとユーザ認証のための Firebox Web ポータルの HTTP ヘッダ情報
- シングルサインオンで使用される MS Exchange のイベントモニタ
- DHCP Fingerprinting3 は、Firebox が DHCP サーバまたはリレーとして使用されている場合であっても、クライアントが IP アドレスを取得するときに、パケット交換で渡される情報を使用します。パラメータ要求リストの DHCP オプション 55 には、デバイスの OS を特定する情報が含まれます。
- nmap によるアクティブスキャン

## 結論

ネットワーク管理者は、複雑なネットワークにおけるデバイス検出とセキュリティ監査という課題を抱えています。発生した問題についてトラブルシューティングし、新しいまたは不審なアクティビティを特定する必要があります。ウォッチガードの Network Discovery サービスは、IT 担当者が少ない時間でネットワークとデータを安全に維持できるよう効率的かつ柔軟で統合型のサービスを提供します。

Network Discovery は、Firebox T Series から M5600 まで、すべての現行モデルの Firebox シリーズにて利用可能です。個別のサブスクリプションサービスとして利用できますし、ウォッチガードの UTM Security Suite に標準搭載されており、多くの強力なセキュリティ機能と利用できます。

ウォッチガードの Network Discovery やその他のベストインクラスのセキュリティ機能の詳細については、www.watchguard.co.jp をご覧ください。

ウォッチガード・テクノロジー・ジャパン株式会社
東京都港区麻布台 1－11－9　CR 神谷町ビル 5 階　　TEL:　03-5797-7205
WEB: https://www.watchguard.co.jp

ウォッチガードについて

WatchGuard® Technologies, Inc.は、業界標準のハードウェア、最高クラスのセキュリティ機能、およびポリシーベースの管理ツールをインテリジェントに組み合わせた統合型の多機能ビジネスセキュリティソリューションを提供する、グローバルリーダです。WatchGuard は、世界各国の数千の企業に使いやすく優れた保護機能を提供しています。WatchGuard の本社は、米国ワシントン州のシアトルにあり、北米、欧州、アジア太平洋、および南米にオフィスを展開しています。

明示的または黙示的な保証は一切提供されません。すべての仕様は変更される可能性があり、今後新しい製品や機能が利用可能となり提供されることが予測されます。



---

3 http://lets-start-to-learn.blogspot.com/2015/02/dhcp-fingerprinting.html