FORESCOUT
Active Defense for the Enterprise of Things™

次世代のネットワークアクセス制御

エージェントレス方式のデバイス可視化・コントロールが、効果的なサイバーセキュリティに不可欠な理由

デバイスの可視化およびコントロールの重要性

ネットワーク接続するあらゆるデバイスの発見、分類、評価、コントロール機能は**ゼロトラスト・セキュリティ**実現において必要不可欠な条件です。あらゆるセグメントの物理/仮想エンドポイントをリアルタイムで把握し、ポスチャーやセキュリティ状態のきめ細かいインサイト、ポリシーベースの自動修復とアクセス制御を併用することで初めて、システムとデータセキュリティの確実な実現およびインシデントへの迅速かつ正確な対応を実現できるのです。

100%
リアルタイムで可視化

攻撃者は常に、セキュリティが確保されていない管理対象外デバイスを探し求め、組織の死角を見つけるとエクスプロイト攻撃を仕掛けます。エージェントレス方式の可視化・コントロールはセキュリティとコンプライアンス対応の基礎となるだけでなく、業務上の様々な課題を解決するうえでも重要です。たとえば、デバイスを細部にわたって常時可視化することで、正確な**リアルタイムの資産インベントリ**を作成できます。セキュリティ/IT担当者はこの情報をもとに、運用コストを低減しつつ、規制順守や監査対応を徹底できます。

forescout.com/solutions/network-access-control　japan-sales@forescout.com　電話番号: 81 50-1746-6455

可視化・コントロールの難しさ

従来のネットワークエンドポイントは、各デバイスにインストールされたソフトウェアエージェントをベースに管理されてきました。会社所有のPC/サーバーなど、固定エンドポイントが大多数の場合はこの方式で十分ですが、モビリティやデバイスタイプの多様化、仮想化により、コンテキスト情報の可視化とコントロールがかつてないほど複雑になりました。

デバイスの数や種類が爆発的に増え、デバイス環境が一変しました。今ではIoTデバイスやオペレーショナルテクノロジー(OT)システムなどのサイバー・フィジカルシステムが、企業ネットワークに接続しています。多くの従業員が在宅勤務し、その一部はクラウド接続しています。こうしたモダンエンタープライズがあっという間に**Enterprise of Things(EoT)**環境に進化しました。しかし、EoT環境に存在するほとんどのモノ(Thing)が、管理エージェントに対応していません。対応していたとしても、エージェントベースの管理手法は以下の点で問題があります。

- エージェントが欠落/故障している、無効化されている場合は機能しない
- エージェントや802.1X認証ベースの方式ではネットワークに死角が残るため、運用が複雑で、導入展開に不備が発生しやすい
- デバイスコンプライアンスツールが縦割り構成のため、統一ビューに欠け、死角が生まれる
- 多くのネットワークで、管理デバイスの数より管理対象外デバイスのほうが多いため、従来の方法では認証できない
- モバイル、BYOD、ゲスト用/在宅勤務用デバイスのユーザーが増加し、エージェント方式のセキュリティ確保に時間がかかり、効果が薄れる
- マルチベンダー構成が主流の今、ハードウェア/ソフトウェア更新を必要としない、802.1X認証に代わる方法が求められる

> **今日のNACツールは、デバイスや未承認エンティティ(ユーザー、セグメント、デバイスなど)がネットワークに「接触」しないよう、隔離する際に最適な手段です。パッチ適用不備が疑われる未知のアイテムをゼロトラストネットワーク環境から除外するために、-Forescoutなどのベンダーが提供する最新のNAC技術を活用してください。[1]**
>
> **FORRESTER RESEARCH社　主任アナリスト**
> **DR. CHASE CUNNINGHAM**

次世代のNACを実現するForescoutソリューション

Forescout Technologiesは、この分野の先駆者としてエージェントレス方式のネットワークアクセス制御(NAC)を推進し、動的で多様化された今日のネットワーク環境に蔓延する課題に対応してきました。Forescoutプラットフォームは キャンパス、データセンター、クラウド、OTネットワークにまたがるすべてのデバイスの統合ビューを常時提供します。以下の対象を、継続的かつ細部にわたり可視化します。

- キャンパスネットワークのデバイス：ラップトップ、タブレット、スマートフォン、BYOD/ゲストシステム、IoTデバイス
- データセンターインフラ：仮想マシン、ハイパーバイザー、物理サーバーその他の物理/仮想ネットワーク構成機器
- パブリック/プライベートクラウドインフラ：AWS®、Microsoft® Azure® 、VMware® 仮想マシン
- OTおよび産業用制御システム(ICS)：医療機器、産業デバイス、ビルオートメーションデバイス
- 物理ネットワーク、ソフトウェア定義型ネットワーク(SDN)インフラ：スイッチ、ルーター、ファイアウォール、VPN、無線アクセスポイント、コントローラー

死角のない、最も包括的なデバイス可視化

図1：スケール性に優れたForescoutのデバイス可視化機能を拡張エンタープライズ環境全体に適用し、ネットワーク接続するすべてのモノ(Thing)を対象に、詳細かつリアルタイムの資産インベントリを作成できます。

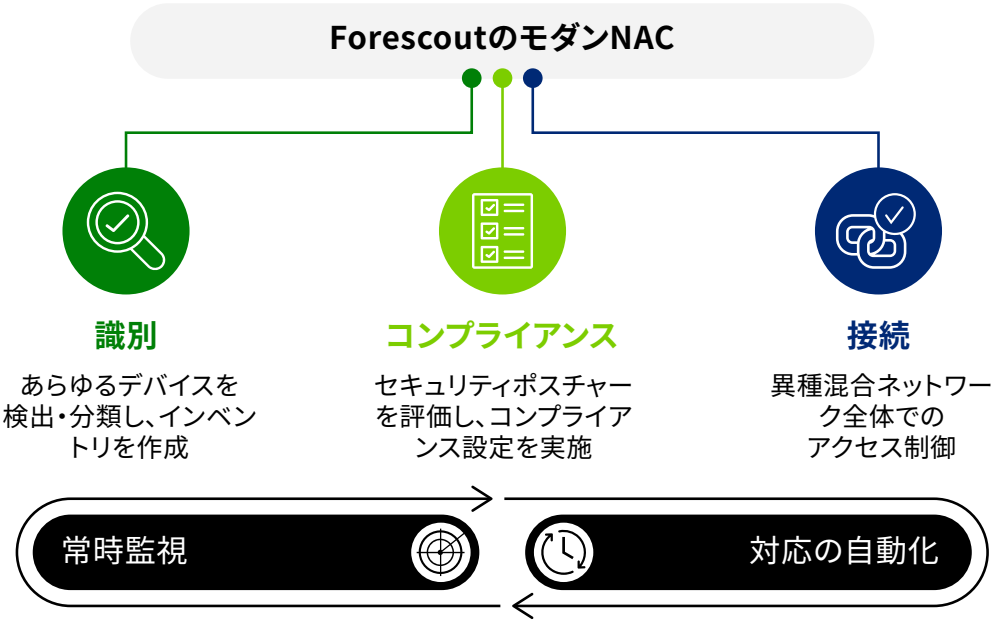


図2：ForescoutのモダンNACソリューションは、あらゆる異種混合環境に不可欠な機能を提供します。ソフトウェアエージェントや802.1X認証は不要です。

当社ソリューションの内容

IT部門の皆様は、ForescoutのモダンNACソリューションで以下を実現できます。

- 20種類以上のアクティブ/パッシブ手法により、あらゆるロケーション、ネットワーク、デバイスタイプをくまなく網羅できる最も包括的な、エージェントレス方式のデバイス検知
- デバイスの機能、OS/バージョン、ベンダー、機種情報にもとづく正確かつ自動化されたデバイス分類
- 拡張ネットワーク上のIP接続デバイスすべてに対するリアルタイムの資産インベントリを自動作成し、維持
- すべてのデバイスのセキュリティポスチャーをエージェントレス方式で評価し、常時監視
- エンドポイントの自動修復によるセキュリティポリシー/業界要件の順守
- 認証、ユーザーの役割、デバイスタイプ、セキュリティポスチャーに応じ、異種混合の有線/無線/VPNネットワーク環境全体を柔軟にコントロール
- 最小権限のアクセス制御によるゼロトラスト・セキュリティの実現

あらゆるネットワークであらゆるデバイスを識別するForescoutの手法

Forescoutプラットフォームは外部ベンダー製品との綿密な統合により、自由に設定可能なデータ収集機能を20種類以上提供します。連携対象は、大手のIT/OTネットワークスイッチ、ルーター、無線アクセスポイント、ファイアウォール、VPNコンセントレータ、データセンター、クラウドソリューションプロバイダーの製品です。Forescoutプラットフォームがネットワークトラフィックをパッシブ状態で監視し、様々なプロトコルストリームを解析します。ネットワークインフラ、エンドポイントの両方とも直接やり取りできます。以下は、当社の可視化手法の一例です。

- **ネットワークとデバイスに対してパッシブ**な手法の例：スイッチや無線コントローラーからのSNMPトラップ受信、SPANポートのモニタリングとトラフィック内のプロトコルストリームの解析（150以上のIT/OTプロトコルに対応するディープパケットインスペクション）、フローデータの収集・分析またはDHCPリクエストとHTTPユーザーエージェントのトラフィック評価など。802.1X認証ありの場合、ビルトインまたは外部サーバーによるRADIUSリクエストも可能。
- **ネットワークとインフラに対してアクティブな**手法の例：スイッチ、VPNコンセントレータ、無線コントローラー、プライベート/パブリッククラウドコントローラーのポーリングによる接続デバイス/VMの一覧作成。Forescoutプラットフォームからディレクトリサービス、Webアプリケーションまたは外部データベースへのクエリ実行によるユーザー/デバイスデータの取得。
- **エンドデバイスに対してアクティブな**手法の例：NMAPによる接続デバイスのネットワークセグメント・スキャン、WMIによるWindowsデバイスのリモート検査、SSHによるMac/Linuxデバイスのリモート検査、SNMPクエリによるエンドポイントプロファイリングなど。

デバイスの可視化手法

パッシブ手法	インフラに対するアクティブ手法	エンドデバイスに対するアクティブ手法
SNMPトラップ	物理ネットワークインフラのポーリング	エージェントレス方式のWindows検査 (WMI、RPC、SMB)
SPANトラフィック • DHCPリクエスト • HTTPユーザーエージェント • TCPフィンガープリント取得 • 医療デバイスのプロトコル解析（20種類に対応） • 産業用制御システム/OTプロトコル解析（70種類以上に対応）	コントローラーによるNWインフラ統合 • Juniper Mist • Cisco ACI, Cisco Meraki	エージェントレス方式のmacOS、Linux検査 (SSH)
フロー解析 • NetFlow • Flexible NetFlow • IPFIX • sFlow	プライベートクラウド（仮想インフラ）との統合 • VMware	Nmap
DHCPリクエスト（ipヘルパー経由）	パブリッククラウドとの統合 • AWS • Azure	エンドポイントへのSNMPクエリ
HTTPユーザーエージェント（URLリダイレクト経由）	ィレクトリサービスのクエリ(LDAP)	エージェントベースの検査 (SecureConnector)
RADIUSリクエスト	Webアプリケーションのクエリ (REST)	
MAC OUI	部データベースのクエリ (SQL)	
	オーケストレーション（ITSM、UEM、EPP、EDR、VA）	

図3：Forescoutのデバイス可視化手法

複数のデバイス可視化手法による優位性

Forescoutプラットフォームには初期設定が簡単で、運用開始後も容易に改修可能な検知手法が数多く搭載されています。これにより当社ならではの柔軟性、効率性、実効性を提供します。

大規模環境への低コストかつシンプルな導入展開：
20以上のアクティブ/パッシブ手法を柔軟に活用し、（複雑性、規模、リモート拠点数にかかわらず）あらゆる異種混合ネットワークのデバイスを完全に可視化します。インフラ（ソフト/ハードウェア）更新や、リモートサイト/オフィス単位でのローカルアプライアンスの導入展開は一切不要です。

死角をなくす：多くのエンタープライズ環境には、追加アプライアンスやSPANトラフィックに対応できないリモート拠点があります。当社は複数のアクティブ/パッシブ手法を使い分け、ネットワーク制限に対処し、死角のない完全なデバイス可視化を提供します。

重要な医療システムやOT/ICSネットワークの発見・分類・評価にはパッシブ手法のみを使用：基幹業務のネットワークは多くの場合、医療システムや工程管理システムを妨げる恐れがあるアクティブプロービングやスキャン手法に適していません。Forescoutプラットフォームは、完全なパッシブ方式（150以上のIT、ヘルスケア、OT特有プロトコルに対応するディープパケットインスペクションによるSPANトラフィック監視など）を組み合わせ、重要なヘルスケア/OTネットワーク全体のデバイスを可視化します。Forescoutソリューションならではの強みは、デバイスを正確に識別した後、アクティブ手法を選択的に適用し、業務を止めずに追加のデバイス評価を実施できることです。

発見にとどまらないインサイト – 分類・評価：
Forescoutプラットフォームはパッシブ/アクティブ型のプロファイリングを多層的に展開できるため、接続先MAC/IPアドレスによる単純なデバイス識別に比べ、はるかに多くのことを実現できます。分類プロセスでは、多数のレイヤーで構成されるコンテキスト情報を取得し、相関性を把握して、各デバイスのきめ細かいプロファイルを作成します。評価プロセスでは、発見したデバイス状態のプロパティをセキュリティポリシーと照合し、アクセスコントロールと修復判断の基準として使用します。どちらも優れた手法です。ぜひ詳細をご確認ください。

インテリジェントな自動分類

きめ細かいポリシーを作成するには、各デバイスの完全なコンテキスト情報が不可欠です。最適な形で保護・管理するには、それぞれの運用目的を把握する必要がありますが、デバイスが増加・多様化した今、手動によるコンテキスト収集はほぼ不可能です。コンテキストが不完全なままポリシーを作成すると、オペレーションがリスクにさらされます。当社は多次元分類をもとに、従来型デバイスおよびIoT/OTデバイスの機能、タイプ、OS/バージョン、ベンダー、機種を識別し、自動分類します。

Forescout プラットフォームは以下を自動分類します。

- 575種類を超えるOSバージョン
- 5,700種類を超えるデバイスベンダーの製品と機種
- 400種類を超える医療システムベンダーの医療機器
- 製造業、エネルギー、石油・ガス、公益セクター、鉱山その他重要インフラ業界で使用される何千種類もの産業用制御・オートメーションデバイス

Forescout Device Cloud：豊富なコンテキスト情報のソースを、デバイスの増加や多様化に合わせて進化できるよう、当社プラットフォームの自動分類にForescout Device Cloud を活用しています。デバイスインテリジェンスをクラウドソーシングして蓄積した世界最大のデータレイク「Device Cloud」は、1,200を超えるエンタープライズ顧客のデバイス分析を通じ、多業種横断的なネットワーク環境に存在する固有の資産すべてのフィンガープリント、挙動、リスクプロファイル情報を一元化します。当社の研究部門Forescout Researchでは新規プロファイルを頻繁に配信し、皆様のデバイス環境全体での分類効率やカバー範囲、スピードの改善を支援します。

エージェントレス方式でのポスチャー評価と自動修復

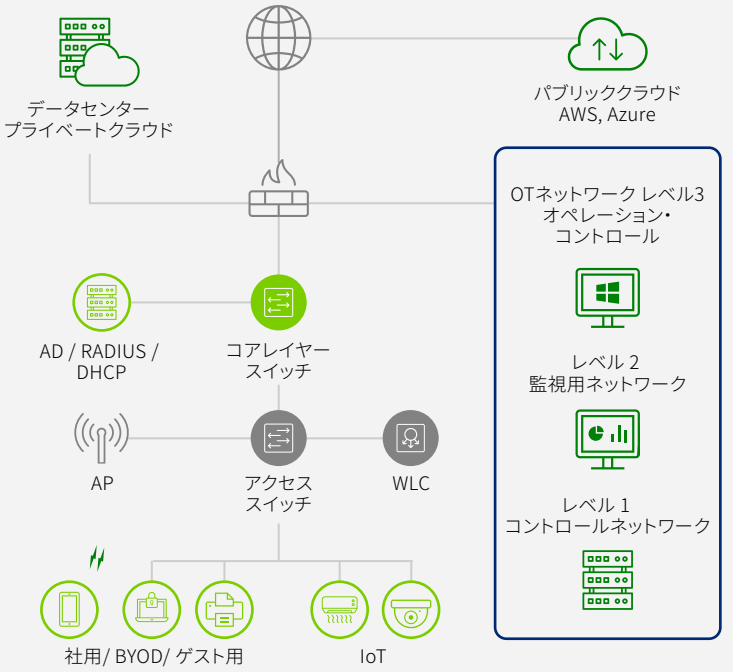
デバイス分類によって、デバイスの用途に関する運用上のコンテキスト、つまり「デバイスの中身」が明らかになります。しかし完全なコンテキストを得るには、各デバイスの健全性とハイジーン（サイバー衛生）の状態を測定する別のレンズ（手段）が必要です。Forescoutはネットワークを常時監視し、接続デバイスの設定、状態、セキュリティポスチャーを評価します。これをもとに、リスクプロファイルを判定し、セキュリティや規制のコンプライアンスポリシーの順守状況を判断します。たとえば、デバイスに関する以下のような重要項目を確認します。

- （最新OSパッチを含む）承認済みのOS上で実行されていること
- セキュリティソフトウェアがインストールされ、正常に動作し、最新パッチで更新されていること
- 無許可のアプリケーションを実行中のデバイス、標準設定に違反しているデバイスがないこと
- デフォルトまたは脆弱なパスワードを使用していないこと（とくに、IoTデバイスでは高リスク）
- 不正デバイスの検出有無（スプーフィングによる正規デバイスへの偽装を含む）
- 接続デバイスのうち、最新の脅威に対する脆弱性がもっとも高いデバイス

Forescoutプラットフォームがこれらの重要項目を確認した後、**デバイスの自動修復により、デバイスコンプライアンス設定を**行います（ネイティブまたは外部のコントロールを適用）。以下は主な機能の一例です。

- エンドポイントが適切に設定されていることを確認し、重大な設定違反（デフォルトまたは脆弱なパスワードなど）の修復を開始
- セキュリティエージェントの運用に問題がないことを継続的に保証（インストール済で、正常に動作し、最新状態であること）
- リスクを招く、またはネットワーク帯域幅やリソースの生産性に無駄な負荷が生じる恐れがある無許可アプリケーションを無効化/ブロック
- 高リスクの脆弱性、重要パッチの適用漏れを特定し、修復アクションを実行
- 必要な修復アクション（セキュリティソフトのインストール、エージェントの更新、セキュリティパッチの適用など）を見極め、プロアクティブに実行
- ポリシーの実装、コントロールの自動化により、クラウド環境(AWS, Azure, VMwareなど)における設定コンプライアンスを順守

デバイス分類と評価



誰が
- ユーザー
- 名前
- Eメール
- 役職
- グループ
- サブスクリプション/アカウント
- IAMオーナー/役割

何を
- 機能
- OS
- ベンダー/機種
- IPアドレス
- ブラウザエージェント
- ポート
- 仮想/物理
- MACアドレス

ポスチャー
- アプリ
- サービス
- プロセス
- バージョン
- レジストリ
- パッチ
- 暗号化
- アンチウィルス

どこで
- スイッチ
- コントローラー
- スイッチポート/SSID/VLAN
- AWS/Azure
- リージョン
- VNet/VPC
- Purdueレベル

図4：Forescoutプラットフォームはデバイスを素早く分類し、デバイスの種類（会社管理、管理対象外、IoT/OTデバイス、物理/仮想の区別）を明確化します。
この情報をデバイスコンプライアンス評価にお役立ていただけます。

「IoTデバイスやネットワーク対応デバイスの技術により、ネットワークとエンタープライズ環境の侵害リスクが増えました。接続するデバイスが増えるたびに、セキュリティ担当者がコードと資産を個別に追跡し、「信頼できないインフラ」として対処しなければなりません。セキュリティ部門は、ネットワーク上のあらゆるデバイスを四六時中、隔離し、安全性の確保およびコントロールを行う必要があります。」[2]

FORRESTER社
2020年6月8日

可視化によるコントロール

ネットワーク環境はお客様の組織ごとに異なるため、要件もそれぞれ違い、セキュリティポリシーも各社各様です。だからこそ、有線/無線/VPNネットワークすべてを保護できる柔軟なソリューションを実装することが不可欠です。たとえば、大規模エンタープライズのお客様環境では通常、有線ネットワーク環境に802.1X 認証なしのForescoutソリューションをデプロイするケースが一般的です。このオプションは簡単にデプロイでき、ハード/ソフトウェアインフラの更新や、スイッチ/エンドポイントの複雑な設定（802.1X対応など）が不要です。

また、単一ベンダー、マルチベンダーのネットワークインフラの両方に対応します。この実装方式は、Gartner社の推奨プラクティス（有線ネットワークでは802.1X認証を使わず、より単純明快なデプロイを実現し、運用コストを低減すること）にも適合しています。ただし無線ネットワークでは、ユーザーベースの会社所有のITデバイスの認証に802.1Xを用いることが標準プラクティスです。当社の柔軟なハイブリッド型の実装オプションは、どちらのベストプラクティスにも対応可能です。

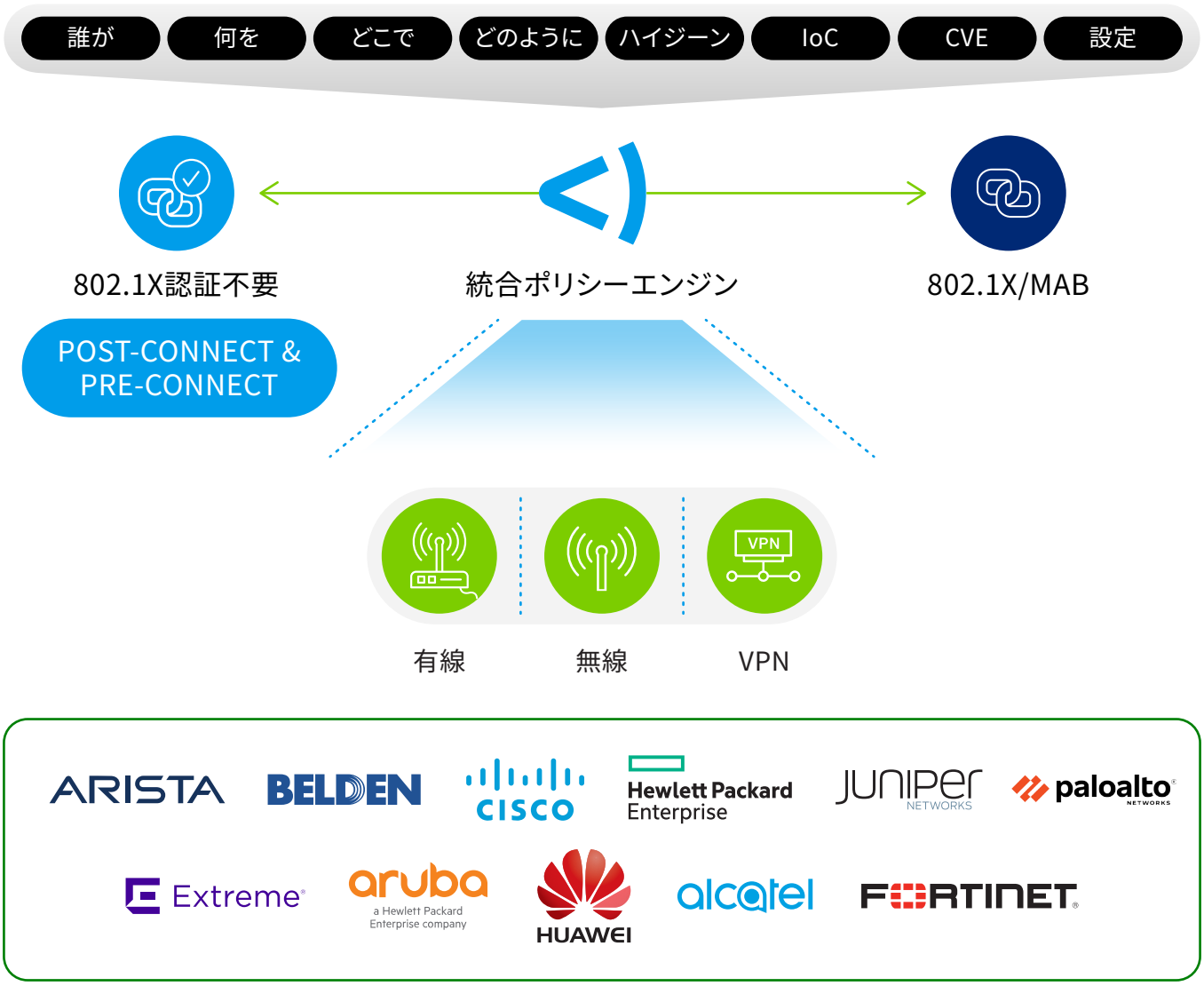


図5：802.1X認証あり/なしの両オプションで、マルチベンダー構成の有線/無線/VPNネットワーク上のエンドポイントを保護します。

ネットワークアクセスのセキュリティ対応にForescoutプラットフォームをご利用いただくと、数々のメリットを実現できます。以下はその一例です。

柔軟性の向上

- 多岐にわたるアクセスコントロール手法（802.1X認証有無を問わず）
- 802.1X認証不要の堅牢なアーキテクチャ：業務の中断をする事なく容易にデプロイ可能、最小限の設定項目、インフラのアップグレード不要、接続後/接続前に使えるオプション、短期間での価値化、ROI（投資効果）の早期実現
- 統合ポリシーエンジンで、デバイス分類（ゲスト用、BYOD、会社所有、IoTデバイス）ごとにセキュアなゼロトラスト・アクセスを実現

アップグレード不要

- 既存インフラ上で運用可能なため、ソフト/ハードウェアのアップグレードは不要
- ご希望のネットワークインフラベンダー製品（スイッチ、無線コントローラー、IaaS）と組み合わせ可能なため、ベンダーロックインの問題を軽減
- 価値およびROIの早期実現

異種混合環境への対応

- 30社以上のネットワークインフラベンダーのスイッチや無線コントローラー製品との直接統合（SNMP、SSH、Telnet、RADIUS経由で、OSバージョンが異なる数百種類の製品と連携）：あらゆるマルチベンダー環境でのネットワークアクセス制御に対応
- デプロイ/保守/運用コストを低減する、柔軟で業務の中断をしないソリューション
- 異種混合環境のサポートにより、M&Aなどで買収した企業のネットワーク資産を素早く可視化し、統合環境としてコントロール可能

エンタープライズ横断的セグメンテーション

- 可視化インサイトをもとに、あらゆる場所のあらゆるデバイスに関するセグメンテーション状態をリアルタイムで把握
- 論理セグメンテーションポリシーの設計・シミュレーションにより、セグメンテーションによる影響を事前に測定
- 拡張エンタープライズ環境全体で、セグメンテーション・ハイジーンをリアルタイムで監視し、ポリシー違反に対応

エンタープライズ横断的セグメンテーションを実現するForescoutソリューションの詳細は、こちらをご参照ください。

NAC実装におけるベストプラクティス

当社が推奨するベストプラクティス：

無線ネットワーク：ユーザーベースの会社所有のITデバイスの認証における標準プラクティスは、802.1X認証です。認証後、ForescoutがWindows、macOS、Linux ベースの端末を識別し、デバイスのコンプライアンス状況をエージェントレスで評価します。Forescoutのポリシーエンジンでデバイスを自動修復し、適切なネットワーク制御を実施することで、セキュリティポリシーにも対応できます。（ユーザーへの通知、修復、ブロック、ブロック、外部ツールとのコンテキスト共有など）

有線ネットワーク： 802.1X認証なしのアーキテクチャを推奨します。有線ネットワークでの802.1XとMABの実装・管理は複雑なため、ほとんどのお客様が802.1X認証なしのオプションを選択されます。デバイスの検出、識別、ポスチャー/コンプライアンス評価からスタートし、異種混合環境で適切なレベルのネットワークアクセスを802.1X認証なしの方式で制御する、という流れが一般的です。注：Forescoutは、有線ネットワーク環境における802.1X認証も完全にサポート可能です。

IT/セキュリティ製品とのオーケストレーション

Forescout はネットワークアクセス制御(NAC)プロセス全体で現行ツールと連携してリアルタイムのデバイスコンテキスト情報を交換し、対応ワークフローを自動化できます。これによりスピーディーなリスク緩和だけでなく、既存のセキュリティとIT管理システムへの投資効果も拡大できます。eyeExtendの標準統合機能およびeyeExtend Connect Appが、縦割り状態のセキュリティ管理を連携し、Enterprise of Things(EoT)のアクティブ防御を実現するエンタープライズ横断的な自動対応システムへの迅速な移行を支援します。

既存セキュリティツールと当社製品のオーケストレーションによって、NACプロセスを効率化できます。以下は、連携の事例です。

デバイスコンテキスト情報の共有

- 既存の資産管理ツールとデバイスコンテキスト情報を共有し、最新かつ正確なインベントリを常に保持(CMDB)
- インシデントの相関分析や優先付けに必要な、リアルタイムのデバイスコンテキスト情報をセキュリティオペレーション部門とアプリケーションに提供

On-Connectワークフローの起動

- 既存ツールの定期スキャンだけではカバーできない一過性デバイスの脆弱性評価に対応：当社製品をセキュリティツールと連携し、デバイス接続(On-Connect)時にリアルタイムの脆弱性スキャンを起動可能
- デバイス接続と同時に、パッチ適用やセキュリティ更新を実施し、攻撃対象領域を縮小

セキュリティポスチャーの評価

- 既存のセキュリティエージェントが問題なく動作していることを確認し、リスクやIoCが示唆されるデバイスを特定
- 接続デバイス上で陳腐化した、または不正な特権アカウントを検知

対応アクションの自動化

- 脆弱なデバイス、侵害されたデバイス、高リスクデバイスの封じ込め、隔離またはブロック
- ポリシーベースの緩和策と修復アクションによるインシデント対応

> **Forescoutは、エージェントレス方式のNAC領域で圧倒的な市場シェア（64.7%）を誇るベンダーです。さらに、ハイブリッド型のNAC実装においても業界で最も豊富な実績があると推定されます。NAC領域では、エージェントレス方式を必要とする「管理対象外デバイス」や「エージェント非対応デバイス」の構成比が高まっています。これらのニーズへの対応を重視した強力な機能群が、同社の成長をけん引しています。**
>
> **IDC社**
> **2020年5月**[3]

単なる可視化だけでない.セキュリティ保護.

Forescoutのモダン NACソリューションは、柔軟かつ業務の中断なくゼロトラスト・セキュリティをエージェントレス方式で実現します。Enterprise of Things(EoT)のアクティブ防御に関する当社のアプローチについて、以下のリソースで詳しく解説しています。ご参照ください。

Gartner社の「Market Guide for NAC」: Gartner社がForescoutを「市場で最も人気の高いNACソリューションのひとつだ」と称する理由を解説します。

当社ウェブサイト: ForescoutのモダンNACソリューションの詳細（対応ユースケース、徹底したデバイスコンプライアンスの支援方法、お客様の声など）をご覧いただけます。

製品体験（テストドライブ）のお申込み:6種類の強力なユースケースを使ったハンズオン形式のテストドライブで、Forescoutプラットフォーム導入前・導入後の違いをご体験ください。

デモのご依頼: 当社サイトの画面から個別デモをお申込みいただけます。また、各種オンデマンド・デモや動画を無料でご視聴いただけます。

1. Forrester Research社「The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook」2019年1月2日付
2. Forrester Research社「Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles And Techniques」2020年6月8日付
3. IDC社による世界全域のNAC市場シェア調査（2019年版）「Diverse Market Demands Expand NAC's Addressable Market」2020年5月

Don't just see it.
Secure it.™

EoT(Enterprise of Things)のアクティブ防御を支援します。今すぐお問合わせください。

forescout.com/solutions/network-access-control　japan-sales@forescout.com　電話番号: 81 50-1746-6455

FORESCOUT
Active Defense for the Enterprise of Things™

〒101-0051
フォアスカウト・テクノロジーズ株式会社
東京都千代田区神田神保町2-11-15
住友商事神保町ビル2階

詳細はForescout.jpをご覧ください