ソリューションショーケース

Forescout: エクステンデッドエンタープライズ全体を見通すビジネス主体のデバイス可視化を実現

日付: 2019 年 4 月 **執筆:** Jon Oltsik (上級主席アナリスト、ESG フェロー)

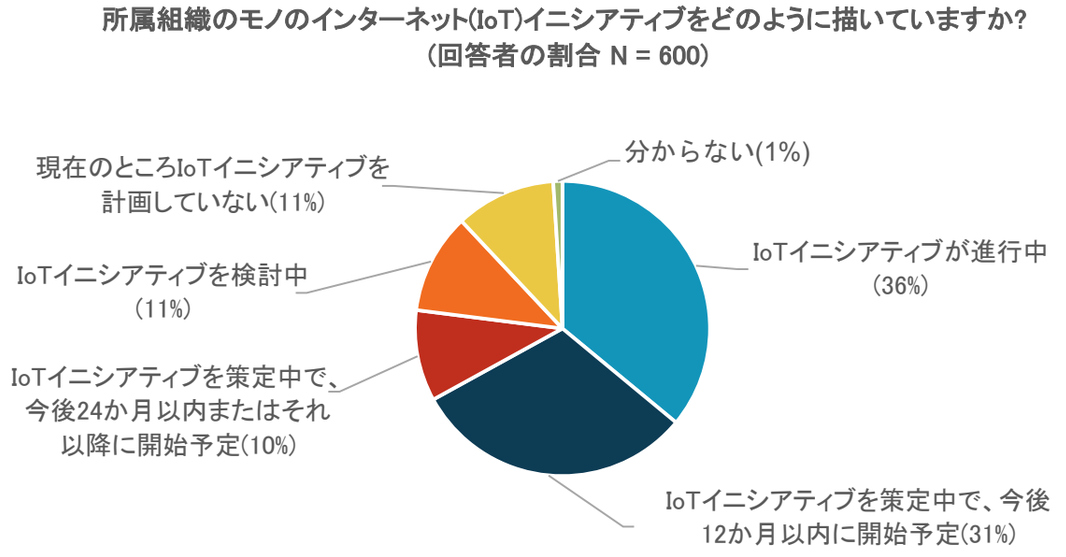
概要: CISO は、さまざまなビジネスイニシアティブをサポートして、デジタルトランスフォーメーション(DX)の優先付けを可能にする役割を担っており、また経営者がビジネス上の意思決定やイノベーションの推進に使用できる、多数の IT および OT ネットワーク(エクステンデッドエンタープライズなど)全体にわたる主要な業務データを把握可能にする役割を担っています。それにもかかわらず、CISO は次のような大きな課題に直面しています。多くの企業が、DX プロジェクトを支えるネットワーク対応デバイスの検出、評価、コントロールに苦戦しています。デバイスに適用すべきポリシーやサイバーセキュリティコントロールを把握するには、技術的コンテキストとビジネスコンテキストの両面から、継続的かつ高度なデバイス可視化が必要です。通常、組織はこの目標を達成するためにさまざまなツールを使用しています。しかし、多くの場合、得ることができるのは、限定的で、一貫性がなく、特定の一時点との関連性しかない可視性です。何が必要なのでしょうか? それは、ビジネス主体の可視化を可能にする詳細な技術的コンテキストとビジネスコンテキストが得られる新しいデバイス可視化ソリューションです。

企業によるデバイス可視化は適切なレベルに達していない

デジタルトランスフォーメーションイニシアティブの普及に伴い、さまざまなテクノロジーがビジネスプロセスの基盤となっています。多くの場合、この移り変わりは、ヘルスケア、小売販売、製造といった業界においてモノのインターネット(IoT)に接続されるデバイスなど、さまざまな新しいデバイスによって支えられています。ESG 調査によると、IT 意思決定者の 36%が所属組織で IoT イニシアティブが進行中で、同 31%が今後 12 か月以内に IoT イニシアティブを策定し、同 10%が今後 24 か月以内またはそれ以降の IoT イニシアティブを計画しています(図 1 参照)。[1]

[1] 出典: ESG 調査レポート「2019 Technology Spending Intentions Survey」(2019 年 2 月)

図 1. IoT イニシアティブプラン



提供 : Enterprise Strategy Group

CISO は、DX イニシアティブや IoT イニシアティブの一環として、コーポレートキャンパス、オンプレミスデータセンター、リモートデータセンター、パブリッククラウド、プライベートクラウド、OT ネットワークといったエクステンデッドエンタープライズ全体にわたる多様な一連のネットワーク対応デバイス(物理、仮想)の保護について監督することを期待されています。これらのネットワーク対応デバイスによる接続や切断の頻度は増加しています。さらに、デバイスポスチャやユーザーロールも変化を続けています。サイバーセキュリティチームは、適切なビジネスコンテキストに対する正確な理解、リスクの緩和、適切なセキュリティコントロールの適用を行うため、非管理の IoT デバイスを含むすべてのデバイスに関する最新の詳細情報を常に把握する必要があります。つまり、新しいビジネス要件や技術要件を満たすのに必要なデバイス機能を細部にわたって取得できるように、継続的な監視が要求されるのです。

基礎的なデバイス可視化では不十分

これまで、エクステンデッドエンタープライズ全体のネットワーク対応デバイスを検出するためにさまざまなツールが使用されてきました。これにより、組織のビジネス上および技術上の可視性が適切なレベルに達したと考える方もいらっしゃるでしょう。ただ実際には、デバイスの急激な多様化によって、モバイル、バーチャル、クラウド、IoT システムの管理に用いる新しいカテゴリーのツールが登場したため、デバイスの可視性はまったく足りていません。管理者にとっては、その多くが不透明なままなのです。

従来のツールは、デバイスを見つけることさえできれば、デバイスを個別に検出、分類、検査するというものでした。その多くは、パケットやデバイスベースのエージェントを使用して各検出デバイスを大まかに理解できますが、正確な状況認識に必要なレベルの詳細情報が得られることはめったにありません。この「ボトムアップ」型のアプローチでは、デバイスやその接続先ネットワークに関する限られたデータしか取得できず、複数のデバイス間の通信に依存するアプリケーションフローやビジネスプロセスなど、ビジネス主体の可視化を実現するデータを得ることができません。

さらには、CISO によるサイバーセキュリティの取り組みが、最新のセキュリティ状況と異なる時点の評価に基づいていることも多いのです。どのデバイスがネットワークに接続されており、どのデバイスが接続されていないのか、それらのデバイスの機能、相互接続されたシステム内でデバイスが果たしている役割、デバイスへの変更が組織全体のセキュリティプロファイルに及ぼす影響について、CISO が把握していないのです。これらの事実は、デバイスデータの適時性とデータの取得元となる資産インベントリの完全性の両方を対象にした、ESG リスクマネジメント調査によって裏付けられています。

- **サイバーリスクマネジメントは継続的な監視ではなく定期的な調査に基づいています。**3 分の 2 に迫る組織が基礎評価を実施しています。しかし、そのデータは特定の時点でのみ効果を発揮します。[2] すなわち、最新のデータではなく過去のデータ(さらには一部が不正確なデータ)に基づいてリスクマネジメントが決定されることも多いのです。この事実は、組織が継続的にデバイスを監視するという前述のニーズに反します。

- **組織には完全なネットワーク上の資産インベントリがありません。**驚くべきことに、63%もの組織がこの資産管理の欠如を抱えています。[3] また、全資産の最新のセキュリティ状況を含む完全で正確なネットワーク上の資産状況を把握しなければ、CISO は精度の高いリスクメトリクスを事業経営者に伝えることができず、事業経営者は効果的なリスク緩和のために必要なセキュリティコントロールを実施できません。

このボトムアップ型アプローチとその取得データでは、とりわけ DX イニシアティブのサポートに使用される新しいデバイスの流入により、良くても限られた結果が得られるのみです。このような限界を考慮すれば、サイバーセキュリティチームは、ネットワーク上にあるものを評価し、各デバイスのデータを収集し、取得データからビジネスリスクを読み取り、そしてどのような種類のサイバーセキュリティコントロールが必要かを推量するために、複数の単独ツールに頼らざるを得ません。動的なビジネスプロセスがエクステンデッドエンタープライズ全体のデバイス通信に依存している場合、この断片的アプローチは適切ではありません。CISO は次のことに注意してください。ツールを連携させてデバイスの状態と役割を推量する場合、組織は強度のサイバーリスクにさらされる可能性が高くなります。

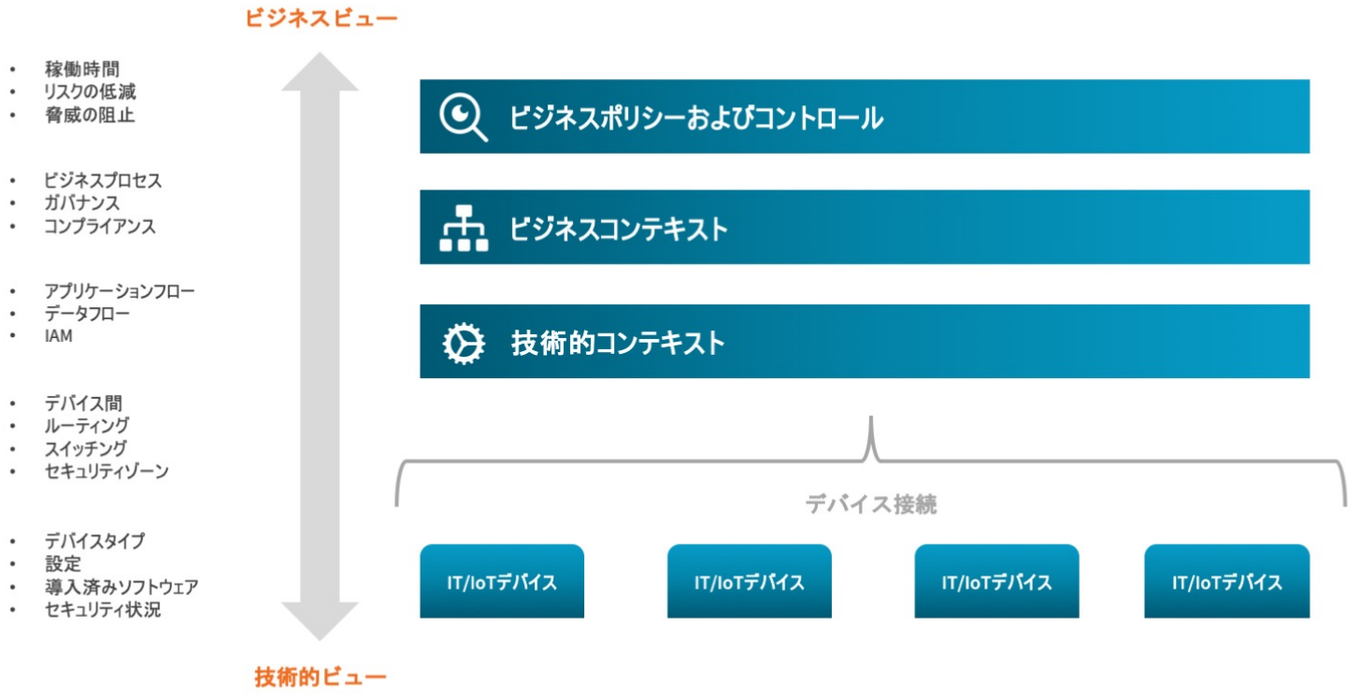
組織が必要とするのはビジネス主体の可視化

多くのデバイス検出ソリューションでは、デバイスを可視化するためにボトムアップ型アプローチまたはトップダウン型アプローチのいずれかを採用しています。前述の通り、ボトムアップ型の可視化モデルはデバイスを起点とします。ソリューションによっては多くの技術的詳細が提供されるものの、ビジネスコンテキストは限られます。これとは逆に、トップダウン型アプローチでは、デバイスが接続されるビジネスプロセスを起点としますが、技術的コンテキストは限られます。

CISO には、ボトムアップ型アプローチで得た技術的コンテキストとトップダウン型アプローチで得たビジネスコンテキストを結合させた新しいソリューションが必要なのです。この結合により、個々のデバイスを DX イニシアティブのサポートに用いるビジネスアプリケーションおよびビジネスプロセスと連携させる、ビジネス主体の可視性が得られます。

[2] 提供: ESG マスター調査結果「*The Pressing Need for Comprehensive Cyber Risk Management*」(2019 年 3 月)
[3] 同上

Figure 2. Business-centric Visibility



提供 : Enterprise Strategy Group

図 2 に示すように、ビジネス主体の可視性には、検出されたデバイス、その接続状況、そして技術的コンテキストとビジネスコンテキストの両方に関する詳細なデータが必要です。このレベルの可視性を用いれば、サイバーリスクの緩和、さらには脅威の防止と稼働時間に対する改善を目的とするビジネスポリシーとサイバーセキュリティコントロールを設けることが可能です。このデバイス情報は、さまざまなマネジメントレポートや技術レポートのサポートも行う中央マネジメントコンソールから入手できるようにすべきです。次のような情報を取得する必要があります。

- **デバイス:** ソフトウェアや OS の更新状況だけでなく、デバイスタイプ(PC、タブレット、IoT、OT、仮想デバイス、クラウドインスタンスなど)とデバイスの衛生状態(インストール済みソフトウェア、利用可能なパッチ、パスワード、設定、電源など)を明らかにする必要があります。言い換えれば、組織はネットワーク上にあるすべてのデバイスについて深く継続的に理解する必要があるのです。

- **デバイス接続:** デバイスの接続先とそのデバイスの場所を理解する必要があります(デバイス間、有線および無線ルーティング/スイッチング、VLAN、セキュリティゾーンなど)。これは、通信が必要なデバイスを論理グループに分割することから着手します。

- **技術的コンテキスト:** 技術的観点からデバイスがどのように使用されているかを理解する必要があります(アプリケーションフロー、データフロー、プロトコル、ID など)。これは、組織がデバイスの通信方法を理解し、ネットワークセグメンテーションやアプリケーションホワイトリストなどのサイバーセキュリティコントロールを検討する際に役立ちます。

- **ビジネスコンテキスト:** ビジネスの観点からデバイスがどのように使用されているかを理解する必要があります(有効なビジネスプロセス、ユーザー/ユニットオーナー、コンプライアンス/ガバナンス、接続先アプリケーションなど)。これは、デバイス通信をビジネスプロセスにマッピングする際に役立ちます。このレベルの可視性があれば、組織が起こり得る事態を理解し、起きてはならない事態を阻止する知識を得ることができます。

- **中央コントロールおよびレポーティング:** すべてのデバイスを一元的に管理およびコントロールできるようにし(デバイスに対するポリシーやパッチの適用機能、セグメントネットワークなど)、リスクマネジメントやコンプライアンスなどのサポートに必要な技術レベルとマネジメントレベルの両方のレポーティングを可能にする必要があります。

CISO とそのスタッフがビジネス主体の可視性を用いることにより、リスク緩和に関する意思決定の優先付けとサイバーセキュリティ予算の賢明な割り当てに役立つリアルタイムデータをビジネスマネージャーに提供できます。この情報は、コンプライアンス機能やガバナンス機能を、単独で実施されるチェックボックス業務ではなく、適切に管理されたサイバーリスクマネジメントプラクティスに含めることにも役立ちます。最終的には、ビジネス主体の可視性によって、活動の優先順位を示し、ベストプラクティスを統制する手引きとしてリアルタイムデータを使用し、セキュリティ業務の生産性を向上させることができます。

ビジネス主体の可視性への道筋: CISO が考慮すべき事項

どのベンダーも可視化の実現を謳っていますが、その定義は一様ではありません。多くの場合、提供されるソリューションによって可能になるのは、限定されたボトムアップ(技術)またはトップダウン(ビジネス)のデータセットの取得と配信のみです。

混乱や失敗を避けるため、CISO (およびその他の責任者)は、デバイスの検出、評価、コントロールに関するソリューションの評価において次の問いを念頭に置くべきです。ここで目指すのは、ビジネスマネジメントに必要なリスク情報に加えて、検出されたデバイスに関する継続的で完全なインベントリと管理を提供することです。CISO は、技術的なソリューションの検討においては次のように尋ねるべきです。

- **すべての接続デバイスに関する十分な詳細情報があるか?** ポリシーやセキュリティコントロールの一貫した適用を可能にする、デバイス全体について適切なレベルの詳細情報を迅速に取得する機能が求められます。

- **デバイス状況の変化など、デバイスの詳細情報が常に最新の状態になっているか**? ビジネスリスクを正確に評価し、管理するには、すでに関連性がなくなった時点のスナップショットではなく、リアルタイムのデバイスコンテキストを把握する必要があります。

- **すべての可視化ツールを集約して共通に視覚化できるか?** 真のデバイス可視化は、すべてのデバイスを同じレベルの詳細とコンテキストで視覚化できる場合にのみ達成できます。

- **ビジネスプロセスのコンテキストとして端から端まで、ネットワーク接続を可視化できるか?** 資産の帰属、システムの帰属、アクセス権や責任に対する、状況に応じた洞察を得ることが不可欠です。これは、セキュリティゾーン全体のネットワーク接続、さらには複数のデバイスが連携するビジネスプロセスを理解するために必要となります。

- **リスク緩和、リアルタイムのガバナンスやコンプライアンス、セキュリティ業務の改善に向けたコントロールを確立するために使える可視性を一元的に得ることができるか?** すべてのデバイスを把握することで技術的コンテキストとビジネスコンテキストの両方を得ることができ、それによってビジネス主体の可視化と広い見識に基づくリスク緩和の意思決定が可能になります。

- **急増する仮想マシン(VM)とクラウドインスタンスを確認できるか?** VM (およびその他の種類のワークロード)の使用は増加し続けています。エクステンデッドエンタープライズ全体に導入されているデバイスへの包括的な監視対象にこれらを含めることが重要です。

ビジネス主体の可視化は、技術的なインテグレーションを通してデータを収集、処理、共有化する際のアーキテクチャを示します。これにより、テクノロジーの単独化を解消し、組織の IT マネジメントとセキュリティ投資全体の可視化によって得られる利益を増大させることが可能です。この推進のためにはオープン API を使ってビジネス主体の可視化ツールを構築することが必要ですが、大手ベンダーはパートナー統合に向けたテクノロジーエコシステムを形成しています。

Forescout の採用

デバイス検出ベンダーは、ネットワーク対応デバイスに対する包括的な可視性の提供を謳っていますが、その多くは、一部のデバイスセットに対する不完全なボトムアップビューやトップダウンビューを提供するにすぎません。この法則の唯一の例外が Forescout であり、Forescout が提供する IT および OT ネットワークを統合したデバイス可視化およびコントロールプラットフォームです。Forescout は、組織が状況の認識とリスクの緩和のためにデバイスを継続的に検出、分類、評価する支援を行うことができます。

Forescout は、大規模、動的、多様な環境におけるエンドポイントの可視化とコントロールの課題に対処できるエージェント不要のアプローチをデバイス検出に取り入れます。Forescout プラットフォームは、アクティブとパッシブの検出技術を組み合わせて使用することにより、デバイスにエージェントをインストールすることなく、キャンパス、データセンター、クラウド、OT ネットワークに接続された IP 対応(有線または無線)デバイスを瞬時に判別できます。管理されたもの、非管理、企業、個人のいずれのデバイスにも対応可能です。デバイスタイプには、従来のコンピュータシステム、モバイルデバイス、IoT デバイス、ネットワーク周辺機器、ネットワークインフラストラクチャコンポーネント、OT デバイスおよびインフラストラクチャコンポーネント、不正ユーザーやハッカーによる偽装ハードウェア、その他のネットワーク対応の物理または仮想デバイスなどがあります。さらに、Forescout は、100 以上の IT/OT プロトコルに対する詳細なパケット取得と検査、さらに多様なリスク評価機能により、エージェント不要の可視化とネットワークベースの状況認識の対象を OT や産業コントロールシステム(ICS)環境にまで拡大しています。

Forescout は、接続デバイスを検出すると、(大規模で拡大中の照合データベースを用いて)デバイスの分類を試み、デバイスタイプ、機能、オペレーティングシステム、ベンダー、モデルに関する詳細情報を収集します。その後、Forescout は、ユーザー、アプリケーション、(パッチレベルを含む)その他の種類のソフトウェアなどを評価して、技術的コンテキストとビジネスコンテキストを取得します。Forescout はエージェント不要の検出アプローチを開発しました。このアプローチにより、デバイスや動作を試みているエコシステムについて詳細な情報を制限なく収集できます。そして、Forescout は、ネイティブ IT および OT の脆弱性検証など、ポリシーに対する各デバイスのセキュリティの状況とコンプライアンス状態を評価します。確立したポリシーと検出されたセキュリティ状況に基づいて、直接、またはセキュリティおよび IT マネジメントテクノロジーの密接な統合により、複数のコントロールオプションを用いた内部ネットワークリソースへのアクセス許可、拒否または制限、通知の発行、修正の開始などを行うことができます。このように、Forescout は、重要なビジネスプロセスを中断することなく、包括的なビジネスインサイトと技術的インサイトの提供が可能です。

The Bigger Truth

デジタルトランスフォーメーションの流れをサポートする多数のネットワーク対応デバイスの導入に伴って、サイバーリスクは増加し続けています。現在の可視化ソリューションでは多様なデバイスタイプを識別できず、また検出されたデバイスについて特定時点の限られた可視性しか得られないため、これらのデバイスの多くは、未知、非管理、または安全性が不十分なままです。この状況は、速やかなサイバーリスクの判定と対策とは相反するものです。

これらの課題に対処するため、CISO は、異種混合な環境、データセンター、ハイブリッドクラウド、OT ネットワーク全体にわたる健全性と衛生状態を継続的に検出、分類、評価できるビジネス主体の可視化ソリューションを採用する必要があります。ソリューションは、すべてのデバイスの検出に対応し、技術的コンテキストとビジネスコンテキストの取得に必要なデータを収集し、そして事業担当者や技術担当者にポリシーマネジメント、設定マネジメント、ポリシー実施、レポーティングのための一元的な指揮統制を提供します。このように、ビジネス主体の可視化によって、セキュリティの有効性、業務効率、ビジネスの実現可能性を向上させることができます。Forescout は、これらの新しい要件に対応可能なソリューションを提供している数少ないベンダーの 1 つです。