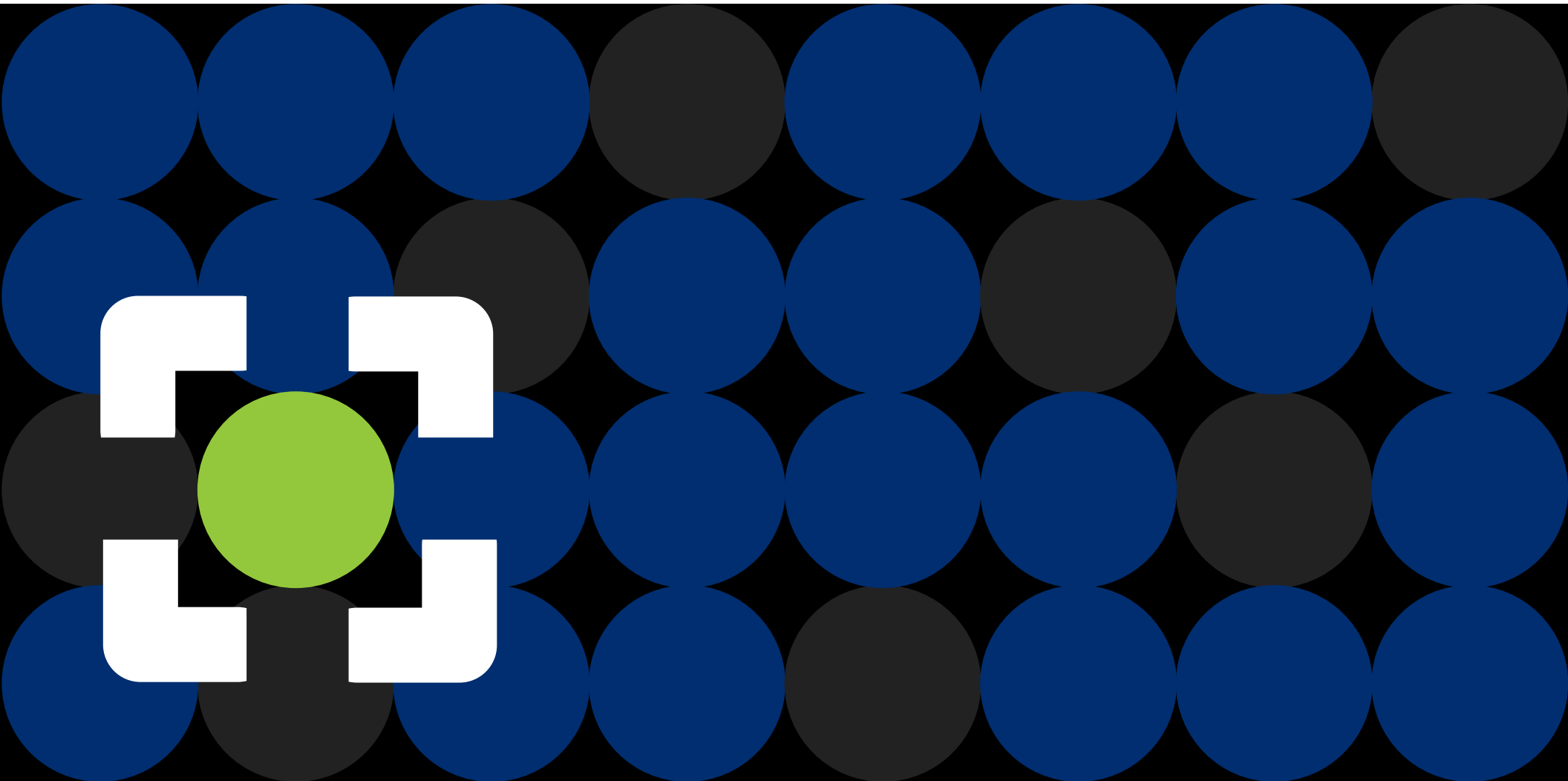
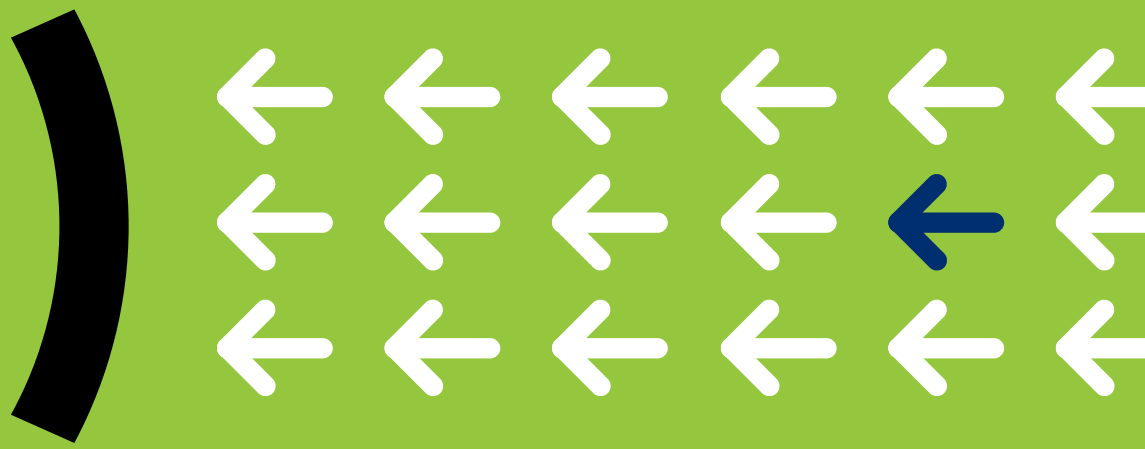
FORESCOUT
Active Defense for the Enterprise of Things™

# Enterprise of Things(EoT)のセキュリティ実現方法
# **5つの課題**



## CONTENTS





## はじめに

今日のエンタープライズネットワーク環境には、制御不能なデバイスが存在します。デバイスの数（数十億個）、種類（IT、OT、IoTデバイスやBYOD）の両方が、爆発的に増えています。既知の管理デバイスもあれば、未知のデバイスとして検知の網をすり抜けるものもあります。また、ユーザーはネットワーク上のあらゆる場所でデバイスを使用します。従業員、請負業者、パートナー、顧客などすべてのユーザーが、あらゆる場所からデータセンターやクラウドに接続します。しかし、セキュリティが万全な接続ばかりではありません。

こうした要因によりそれぞれのネットワーク環境が複雑化し、まさに「Enterprise of Things (EoT)」が形成されています。EoT環境では、慎重な計画および、迷いのないアクションをもとに、デバイスやエンタープライズ全体を保護する必要があります。

本書では、CISOその他のセキュリティ/オペレーション責任者の皆様を対象に、今日のEoT環境における5つの課題および、これらの課題解決に向けた実務的な提言を解説しています。ぜひご検討ください。

## 課 題 1

# 急増する管理対象外デバイスのインベントリ作成・管理方法

> **専門家の予測によると、2020年だけでも世界中で310億個のIoTデバイスがインストールされる見込みです。**
>
> ***2020年1月13日　SECURITY TODAY*** [1]

> **「調査対象者の62%が、成熟した社内セキュリティ態勢を実現できるか否かはIT/OT制御システムの融合状況次第だろう、と答えています。」**
>
> **2019年2月　PONEMON INSTITUTE** [2]

現在、数十億ものIoTデバイスやOT（オペレーショナルテクノロジー）デバイスがエージェントレス方式でネットワークに接続しています。その一方で、セキュリティエージェントが搭載された管理デバイス（社用PC、ラップトップ、スマートフォンなど）は少数派になっています。同時に、IT/OTネットワークの一体化が進んでおり、生産性の向上、ネットワーク管理の効率化というメリットはあるものの、リスクも増大しています。今日の異種混合環境で攻撃対象領域を把握し、対処することはかつてないほど困難になっています。

### 提言：

- 死角のない、完全なデバイス可視化を実現するツールを見極め、選定しましょう
- 候補となるツールを絞り込み、「リアルタイムのデバイスポスチャー評価をエージェントレス方式で実現可能」なソリューションだけを採用しましょう
- セキュリティオペレーションやIT部門の担当者が、リアルタイムの資産インベントリを作成できる機能を提供しましょう

## 課 題 2

# 今日のエンタープライズ環境におけるリスク発生場所

> **「スマートビルディング、医療機器、ネットワーク設備、VoIP電話は、IoTデバイスグループのなかで、最もリスクが高いとみられています。」**
>
> **2020年5月　当社による調査[3]**

> **「IoTやネットワーク対応デバイス技術の台頭により、ネットワークやエンタープライズ環境に、侵害リスクがもたらされました。セキュリティ部門は四六時中、ネットワーク上のあらゆるデバイスを隔離・保護し、コントロールしなければいけません。」**
>
> **2020年6月　FORRESTER RESEARCH[4]**

攻撃対象領域だけでなくリスク分析の概念も変化し、拡大しています。当社が最近行ったEnterprise of Thingsに関する調査では、最もセキュリティリスクが高いデバイスは「IoTデバイス」であることが判明しました。「IoTデバイスは監視・コントロールが大変なだけでなく、これまでは分離されていたサイバー領域と物理領域をつなげる役割を担っているため、新たな脆弱性も発生します。IoTデバイスは、ネットワークに入り込むための秘密のゲートウェイになる、または、標的特化型のマルウェアの主要ターゲットになる恐れがあります。」[3]

### 提言：

- 多要素ベースのリスク分析を実施し、自組織の攻撃対象領域を把握しましょう
- ゼロトラストを取り入れたアクティブ防御戦略に移行しましょう
- リスクレベルに応じたアラートの優先付けにより、脅威対策を加速しましょう
- ここでも、「完全なデバイス可視化」が不可欠です

## 課 題 3

# ネットワーク境界線が消滅した今、注意すべき点

> **「エンタープライズネットワークのエッジを保護するためのベストプラクティスを新たに策定する必要があります。」**
>
> **2020年5月　GARTNER[5]**

オープンかつセキュアな環境の実現：キャンパス、データセンター、クラウド、OT環境にまたがるネットワークで、そんなことが可能でしょうか？エンタープライズネットワークは今や、ワークロードや従業員が存在する世界各地のあらゆる場所に広がっているため、組織全体を防御可能な境界線はありません。もはや、個別の接続デバイスやワークロード単位での境界線が必要な時代になっています。セキュリティの出発点は資産の「エッジ」です。

## 提言：

- ゼロトラストをはじめとする最小権限のアクセスモデルをもとに、企業資産へのアクセスを制限しましょう
- 所在地を問わず、ネットワークにアクセスするデバイスすべてを対象に常時検知・ポスチャー評価を実施しましょう
- ポリシーベースの厳格なコンプライアンス設定をオンプレミス、BYOD、リモート資産に適用しましょう

## 課 題 4

# 必要不可欠なセグメンテーションを、業務オペレーションを止めずに適切に実施するには

> **「取材対象企業の90%が、今年中にセグメンテーションプロジェクトを実施することを予定しています。セグメンテーションの必要性は誰もが認識していても、どこから手を付けて良いのか、どんなリスクが潜んでいるのか、必ずしも明確ではありません。さらに、予算や工数をかけるだけの効果があるのかも未知数です。」**
>
> **2019年1月　当社による調査[6]**

ネットワークセグメンテーションは長年、その重要性を過小評価されていました。つい最近まで、市販のセグメンテーションツールは実装に手間がかかり、ネットワークドメイン横断的な対応もできなかったため、業務の中断やネットワーク環境の分断を招いていました。新規デバイスの追加、ネットワーク環境のさらなる拡張に伴い、この問題がさらに悪化します。しかし今日は、堅牢なセグメンテーションソリューションが入手できるため、脆弱でフラットなネットワークに悩まされ続ける必要はありません。

### 提言：

- セグメンテーションの可視化およびポリシー適用前のシミュレーションにより、不要な業務中断を防止しましょう
- あらゆる場所のあらゆるデバイス（IT、IoT、OTデバイスなど）を対象に、シンプルなゼロトラスト・セグメンテーションを実施できるソリューションをメインに採用しましょう
- エンタープライズ環境全体のゼロトラスト化をスピードアップしましょう
- ネットワークセグメンテーションを効率化する、最新鋭のNACプラットフォームを選定しましょう

## 課 題 5

# 「少ないリソースでより多くを実現」というパラドックスへの対応方法

> **「企業は、散在するネットワーク管理ツールの集約を進めています。しかし、企業の64%がいまだに、ネットワークの監視とトラブルシュート対応に4～10種類の異なるツールを使っています。」**
>
> **2020年4月　ネットワーク管理のメガトレンド2020年版[7]**

> **「取締役層のセキュリティおよびリスク管理への関心は、かつてないほど高まっています。」**
>
> **2019年7月　GARTNERによる調査[8]**

ジョブ単位で分断されたレガシーツールの寄せ集めでセキュリティとネットワーク管理業務に対応している組織のSecOps（セキュリティ・オペレーション）担当部門を考えてみてください。効率的な防波堤、コスト削減の原動力になっているとはとても言えません。一方、変革プランがどんなに素晴らしかったとしても、採用したソリューションの実装に手間がかかる、ROI（投資効果）がすぐに実現しない、習熟が困難、パフォーマンスに不満が残る、などの理由で失敗を招くことはあります。幸い、適切なプラットフォームを選択すれば、CFO（最高財務責任者）を含む利害関係者すべてを満足させることができます。

## 提言：

現行ツールと連携（オーケストレーション）可能で、以下の基準を満たすプラットフォームを採用しましょう

- 業務を止めずに、迅速かつ柔軟に導入展開できること
- 価値および投資効果を早い段階で実現できること
- ベンダーに依存しないこと（既存インフラの活用）
- ソフト/ハードウェアの更新が不要であること
- IT/セキュリティの主力製品と統合・連携できること
- デバイス検知、ポスチャー/リスク評価をエージェントレス方式で実行できること
- 802.1X認証対応による複雑性、導入展開の遅延、コストを回避できること
- 利用拡大に合わせてスケール可能なエンタープライズ規模の拡張性があること
- セキュリティオペレーションの生産性を向上できること
- 可視化、コントロール、セグメンテーション、ゼロトラストをエージェントレス方式で実現できること

## この5つの裏側にある、より大きな課題

本書で解説した5つの課題のそれぞれが、とてつもない難題に思えるかもしれません。しかし、どれか一つでも未解決のまま放置すると、最終的には「サイバー攻撃」につながり、オペレーションの障害、データの窃取、ブランド価値の棄損、多額の罰金、公衆安全の問題をはじめ、数々の問題を引き起こしてしまいます。

鍵となるのは「防御」です。つまり、エージェントレス方式によるデバイスの100%可視化、常時監視、脅威対応の自動化を実現できる効果的なソリューションが必要です。

*注


1. 2020年1月13日付 Security Today記事「The IoT Rundown for 2020: Stats, Risks, and Solutions」
2. Ponemon Instituteによる2019年2月の調査報告「Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT」
3. Forescout Research Labsによる2020年5月の調査報告「The Enterprise of Things Security Report, The State of IoT Security in 2020」
4. Forrester Research社による2020年6月8日付調査報告「Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles and Techniques」
5. Gartnerによる2020年3月27日付レポート「Securing the Enterprise's New Perimeters」
6. 2019年1月　当社ブログ「Network Segmentation」
7. Enterprise Management Associatesによる2020年4月の調査報告「Network Management Megatrends 2020」
8. Gartnerによる2019年7月の調査「Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer」


## 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。

## 当社について

Forescoutは、Enterprise of Things(EoT)セキュリティのリーダーであり、異種混合ネットワーク全体に接続するすべてのモノ(Thing)を継続的に識別・セグメント化し、コンプライアンス対応を実施する包括的プラットフォームを提供します。最も広く採用されている「Forescoutプラットフォーム」は、エージェントレス方式のデバイス可視化・コントロールを実現する、拡張性に優れたエンタープライズ向けソリューションです。既存インフラにエージェントレスで素早く導入展開でき、アップグレードや802.1X認証は不要です。当社は、Fortune 1000掲載企業や政府機関を含むお客様から信頼されるベンダーとして、セキュリティインシデントや侵害による業務中断リスクの軽減、セキュリティコンプライアンスの徹底および実証、セキュリティオペレーションの生産性向上を支援しています。


forescout.com/platform/eyeSight　　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