FORESCOUT
Active Defense for the Enterprise of Things™

IoTセキュリティ

新時代のEnterprise of Things(EoT)デバイスを保護する柔軟な選択肢「ゼロトラスト・アプローチ」

Internet of Things (IoT)デバイスは通常、エンタープライズネットワーク上で可視化できません。また、従来型システムと違って簡単に追跡できず、ほとんどのIoTデバイスがソフトウェアエージェントに対応していません。これらが侵害され、脆弱なネットワークへの攻撃の入り口として悪用されると、攻撃対象領域が拡大し、組織のリスクが増大します。エンタープライズ環境には、異種混合ネットワークに存在するすべてのIoTデバイスを継続的に識別・セグメント化し、コンプライアンス設定を実施するためのセキュリティソリューションが必要です。

IoTデバイス：リスクに見合った成果が出ていますか？

IoTデバイスは価値があり、企業の重要資産でもあるため、生産性の向上、製品やサービスの品質向上、純利益の改善に貢献します。実際、企業の63%は「IoTプロジェクトによる投資を3年で回収できる」[2]と見込んでいますが、資金や知恵が豊富な攻撃者はIoTの可視性やセキュリティに抜け穴（ギャップ）がある標的組織を常に探しています。こうしたギャップによるダウンタイム、データ侵害、知的財産の流出、組織の信頼棄損を防止するために、以下をご参照ください。

- Ponemon Instituteによる最近の調査3では、10人中9人近くの回答者が、自分の勤務先について「IoTデバイス/アプリケーションのセキュリティ不備により、2年以内にサイバー攻撃やデータ侵害を受けるだろう」と答えています。
- 2023年時点での平均的なCIOの責任範囲（管理対象エンドポイント数）は、2018年の3倍に拡大することが見込まれます[4]。

ゼロトラストの定義

Forrester社が提唱する「情報セキュリティのゼロトラストモデル」とは、エンタープライズセキュリティの概念/アーキテクチャに関するアプローチです。端的に言うと、デバイス・ユーザー・アクセスすべてが「信頼できる」ことを確認したうえで、接続を確立します。アクセスは、各ユーザーの業務遂行に必要な社内資産のみに限定されます。Forrester社1によると、効果的なゼロトラスト・ポリシーの実装には、以下が必要となります。

- ネットワークの設計変更によるマイクロペリメーターの実装
- 難読化によるデータセキュリティ強化
- 過剰なユーザー権限やアクセスに起因するリスクの抑制
- 分析と自動化によるセキュリティ検知・対応機能の大幅改善

forescout.com/platform/IoT　japan-sales@forescout.com　電話番号: 81 50-1746-6455

今日のEnterprise of Things (EoT)環境には無数のIT、IoT、OT（オペレーショナルテクノロジー）を担うモノ(Thing)が無数に接続しています。こうしたエンタープライズ環境では、IoTデバイス、IP接続デバイスすべてを可視化して制御すると共に、デバイスの侵害や悪用を防止する「ゼロトラスト・ネットワーク」を実現するセキュリティソリューションが求められます

Forescoutのゼロトラスト・アプローチ

IoTセキュリティのベースには、デバイスの完全な可視化、プロアクティブなネットワークセグメンテーション、最小権限にもとづく全デジタル資産へのアクセス制御（デバイス、ユーザー、アプリ、ワークロード）を融合したゼロトラスト・アプローチが必要であると当社は考えています。Forescoutプラットフォームは、EoT環境全体でのサイバー/オペレーショナル/コンプライアンスリスクの効果的な管理を支援します。以下はプラットフォーム機能の一例です。

- 管理対象外のIoT、IoMT（医療分野のIoT）、OTデバイスおよびIP接続システムすべてを完全に可視化
- 工場のデフォルト設定または脆弱な認証情報をもつIoTデバイスを評価・識別し、厳格なパスワードを適用するポリシーアクションを自動実行
- 拡張エンタープライズ環境にまたがるIoTデバイスの通信状況や危険な挙動に関するインサイトをリアルタイムで提供
- ゼロトラスト・ポリシーによる最小権限アクセスを適用し、デバイスを信頼ゾーンにセグメント化
- マルチベンダー環境/マルチネットワークドメイン全体で、ゼロトラストの統合ポリシーオーケストレーションを自動実行
- セキュリティ管理の縦割り分断をなくし、対応を迅速化すると共に、現行セキュリティソリューションへの投資効果を最大化
- 医療機関向け：脆弱性/脅威のプロアクティブな検知・抑制、きめ細かいセグメンテーションやネットワークアクセスルールの実施、Medigateとの緊密な統合による医療機器への脅威の即時ブロックと修復措置の同時進行

Forescoutは、IoT/OTのゼロトラスト・セキュリティを専門とするベンダーです。IoT/OTデバイスのセキュリティは、エンタープライズ環境における難題であり、Forescoutの得意分野です。IoT/OTセキュリティに関するForescoutプラットフォームの対応力は、競合他社をはるかに凌駕しています。

2019年10月版 FORRESTER WAVE「ZERO TRUST EXTENDED ECOSYSTEM PLATFORM PROVIDERS

FORRESTER RESEARCH社

図1：Enterprise of Things(EoT)環境に接続するすべてのモノ(Thing)を識別・セグメント化し、コンプライアンス設定を実施。すべてのデバイスをアクティブ防御します。

IP接続するすべてのデバイスを検出し、分類

異種混合環境全体のIoT、OT、重要インフラのエンドポイントすべてを完全に可視化し、完璧なデバイスコンテキスト情報を得ることは必要不可欠です。Forescoutプラットフォームは以下を実現します。

- IP接続するすべての（物理/仮想）デバイスがネットワークにアクセスした瞬間から、エージェントレス方式で常時検出
- 20以上のアクティブ/パッシブ検出手法、プロファイリング/分類手法を使い分け、すべてのデバイスを細部まで可視化
- デバイスインテリジェンスをクラウド(crowd)ソーシングして蓄積した世界最大のデータレイク「Device Cloud」を活用し、1,200万を超えるデバイスのフィンガープリント、挙動、リスクプロファイルに関する多業種横断的な情報を一元化

ネットワークの動的セグメンテーションおよびコントロールの自動化

異種混合的な今日のEoT環境でゼロトラストモデルを採用する企業は、EoTドメイン全体を網羅するネットワークセグメンテーションおよびインシデント対応のオーケストレーションを実施する必要があります。Forescoutは、以下の観点から皆様を支援します。

- ユーザーの識別情報とアクセスの相関性（どこで誰が、何を、どういう目的で実行しているか）を判定
- ポリシーとリアルタイムコンテキスト情報をもとに、各デバイスを動的ネットワークセグメントに割り当て
- データフローを反映した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る無停止デプロイ
- 自動セグメンテーションによるサイバーリスク、オペレーショナルリスクの低減

セキュリティ・オーケストレーションおよびコンプライアンス設定

多くの組織では、高コスト・単一目的型のセキュリティソリューションが散在し、ナレッジの共有やインシデント対応の連携ができない状況です。当社のソリューションは、こうした非効率性を解消します。当社製品、eyeExtendは、Forescoutプラットフォームと他社製IT/セキュリティツールとの間でデバイスコンテキスト情報を共有し、異種ソリューション全体でワークフローとポリシー適用を自動化します。eyeExtendのオーケストレーション機能は以下を支援します。

- IoTセキュリティと全体的なデバイスコンプライアンスの強化
- 検知・対応の平均所要時間の短縮
- 現行ツールへのROI（投資効果）の拡大
- 構成管理データベース(CMDB)更新処理の自動化により、ミスを招きやすく時間がかかる手作業のインベントリ管理を廃止

「Forescoutによるデバイス分類、適切なVLANセグメントへの割り当て機能のおかげで、プリンタやVoIP電話、監視カメラなどのIoTデバイスを含む当校のネットワーク環境を把握できるようになりました。

– HILLSBOROUGH COMMUNITY COLLEGE
上席ネットワークセキュリティ/インテグレーションエンジニア兼CSO

KEN COMPRES

1. Forrester Research社によるレポート（2018年10月）「Five Steps to a Zero Trust Network, Roadmap Report」
2. Gartner社「Internet of Things: Unlocking True Business Potential」
3. Ponemon Institute Sabine Zimmer氏による調査（2020年6月3日付）「A New Roadmap for Third-Party IoT Risk Management, Benchmark Study」
4. Gartner社による「2023年までのIoT戦略のトップトレンドおよびテクノロジー」（2018年9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/platform/IoT　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