ホワイト ペーパー

Cisco IoT System Security：リスクの軽減、コンプライアンスの簡素化、信頼の構築

概要

製造業者、エネルギープロバイダー、輸送プロバイダー、およびスマート シティは、Internet of Things（IoT）を利用して競争優位性を獲得しています。しかし、より多くの場所でより多くのモノを接続することにより、新たなセキュリティ上の課題が生じています。リスクを軽減するためには、サイバーセキュリティと物理的なセキュリティを組み合わせる必要があります。このホワイト ペーパーでは、ビジネス マネージャと業務技術担当者を対象に、Cisco® IoT System Security について説明します。IoT System Security は、リスクの軽減、コンプライアンスの簡素化、信頼の構築のための包括的な製品ポートフォリオです。

IoT の保護の課題

IoT のデバイス数は、2015 年の 120 億台から、2020 年には 500 億台に増加する見込みです。それらのデバイスのそれぞれが、インサイダー、ハッカー、犯罪者のネットワーク攻撃の入口となる可能性を秘めています。Forrester が実施した世界中の組織の調査では、IoT を使用している、または使用する予定である産業組織の 47 % が、組織の産業アプリケーションでセキュリティ侵害を経験したことがあると答えています。[1]

IoT の保護は、新しいタイプの課題をもたらします。

- **規模**：セキュリティ ソリューションをコスト効率の高い方法で（場合によっては数十万～数百万エンドポイントまで）拡張できる必要があります。
- **遠隔地**：センサーなどのデバイスは、道路脇、線路、変電所など、アクセスしにくい無人の場所に設置されることがあります。こうしたデバイスは、攻撃者が人目につかずに改ざんすることができます。これらのデバイスを保護するためのサイバーセキュリティ デバイスや物理的セキュリティ デバイスには、過酷な環境条件に耐えられる、狭いスペースに収まる、定期的なアップデートやメンテナンスのためにフィールド技術者が現場に出向く必要がない、などの要件が課されます。
- **可用性**：OT チームは、重要なシステムがダウンすることを恐れて、標準の脅威検出や脅威対応技術の利用を躊躇しています。単純なポート スキャンが原因で IoT デバイスが動作しなくなることもあります。ダウンタイムが発生した場合、そのコストは、あらゆるインシデントにおける修復コストをはるかに上回ることもあります。実際、誤検出による停止のリスクを負うくらいであれば、サイバーセキュリティ保護など**不要だ**という OT チームもいるでしょう。しかしその場合、制御ネットワーク内の脅威を見つける手立てがなくなってしまいます。

Internet of Things のための準備はできていますか

- 73 % のビジネス意思決定者が、IoT によって今後 2 年間でセキュリティに対する脅威がさらに深刻になると予測しています。[2]
- 49 % のビジネス意思決定者が、セキュリティに対する脅威をアプリケーションの最優先課題の 1 つに挙げています。[3]
- 78 % の IT セキュリティ プロフェッショナルが、新しいタイプのネットワーク接続デバイスの保護について確信が持てない、または必要な可視性と管理機能がないと答えています。[4]
- 46 % の IT セキュリティ プロフェッショナルが、現在のポリシーでは IoT デバイスに対応できず、IoT デバイスへの可視性は提供されないと考えています。[5]

[1] Forrester、「Security: The Vital Element of the Internet of Things」、2015 年
[2] シスコの依頼で Lightspeed Research の Global Market Insite（GMI）部門が実施した調査
[3] 同上
[4] SANS Institute、Securing the Internet of Things
[5] 同上

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

包括的な IoT セキュリティ ソリューションには次のような要件があります。

- アプリケーション、ユーザ、プロトコル、異常性が可視化できる。
- 攻撃を受けても重要なシステムの運用を継続できる。
- 業界や政府の規制へのコンプライアンスを簡素化する。
- コスト効率の高い方法で拡張することができ、IoT デバイスやデータの増加に対応できる。
- 状況認識の向上と迅速なインシデント対応を実現する。(状況認識のためには、ビデオ監視、人とデバイスの識別、テレメトリとログの収集および分析を組み合わせる必要があります。)
- IT と OT のプロセスを統合する。(OT システムを IT ネットワークに接続すると、IT セキュリティの既存の資産とポリシーの価値が向上します。)

Cisco IoT System Security

Cisco IoT System Security はこれらの要件を満たしており、大規模なセキュリティの提供、コンプライアンスの簡素化、信頼の構築を実現します。必要なすべてのサイバーセキュリティ ソリューションと物理的セキュリティ ソリューションが 1 つのベンダーによって提供されるというメリットもあります(図 1)。

図 1. シスコの IoT セキュリティ製品ポートフォリオ

センサーおよびエンフォーサとしての IoT ネットワーク

シスコ ネットワーク インフラストラクチャを使用してネットワークに直接セキュリティを組み込むと、異常なネットワーク アクティビティを感知してポリシーを適用することができます。これらのネットワーク デバイスの特長を以下に示します。

- ハードウェア アクセラレーションによる優れた VPN パフォーマンス
- 一貫したポリシーの適用
- 分散型サービス妨害(DDoS)などの攻撃の検出および緩和
- 攻撃者に悪用される設定ミスの防止
- デバイス タイプの識別による適切なアクセス制御
- Cisco Identity Services Engine(ISE)を使用した、ユーザとデバイスの ID に基づく IoT デバイスへのアクセス制御

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

OT 中心のセキュリティ

アプリケーションの可視化、一貫したポリシーの適用、コンプライアンスの簡素化を実現します。Cisco 3000 産業用セキュリティ アプライアンス（ISA）を導入すると、以下のことが実現されます。

- Cisco ASA with FirePOWER™ Services の実績ある脅威管理の活用
- OT のプロトコルとアプリケーションのサポート
- DDoS、使用上の安全性、インサイダー攻撃など、OT 固有の脅威の検出および保護
- 指定したプロトコル、デバイス、アプリケーションへの可視性
- 高性能 VPN、ドメイン ネーム システム（DNS）、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）、およびネットワーク アドレス変換（NAT）によるインターネット接続の保護

ISA 3000 は、コンパクトかつ堅牢で、屋外や過酷な環境での使用に適しています。また、主要な業界認定を受けています。

IoT の物理的セキュリティ

無人の場所にある IoT デバイスの近くでアクティビティが検出されると、すぐにアラートが受信されます。アラートは、ビデオ監視カメラ、物理的アクセス制御、モーション検知用 IoT センサーなど、さまざまなデバイスから送られてきます。このソリューションでは、ワイド ダイナミック レンジ（WDR）技術を搭載した IP カメラにより、逆光や照度の変化にかかわらず有用な画像が得られます。

クラウドとフォグ：Internet of Things のパートナー

フォグは、IoT データを生成したり操作したりするモノの近くまでクラウドを拡張します。コンピューティング、ストレージ、ネットワーク接続を備えたあらゆるデバイスをフォグ ノードにすることができます。たとえば、産業用コントローラ、スイッチ、ルータ、組み込みサーバ、ビデオ監視カメラなどがこれに含まれます。フォグ ノードは、工場フロア、電柱の上、線路脇、車両、石油掘削装置など、ネットワークに接続できるあらゆる場所に導入できます。リスクを軽減するには、シスコのフォグ ノードでフォグ データ サービスを有効にして、ネットワーク エッジでデータを暗号化します。

サービスとパートナー エコシステム

シスコは、テクノロジーだけでなく、IoT の保護に必要なプロフェッショナル サービスとパートナー エコシステムも提供しています。たとえば次のようなサービスがあります。

- Industrial Cyber Security Capability Assessment
- Industrial Cyber Security Reference Architecture
- Industrial Cyber Security Plan, Design, and Implementation
- IoT Physical Security Services

利点

IoT System Security がお客様にもたらす利点には次のようなものがあります。

- **競争優位性の獲得**：データとシステムの保護が確保されると、効率性、安全性、カスタマー エクスペリエンスなどの改善のために IoT を安心して活用できるようになります。サイバー攻撃、設備の停止、危険な状況などのイベントをより素早く検出して、ポリシーに基づく自動的な対応を適用できます。
- **コスト効率の高い方法によるリスクの緩和**：既存のネットワーク インフラストラクチャと OT 中心のセキュリティ アプライアンスを使用して、IoT デバイスの可視化とセキュリティ ポリシーの適用を実現できます。
- **稼働時間の最大化と規制要件への準拠**：IT セキュリティに関する既存の専門知識を OT に応用できます。

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- **コンプライアンスの簡素化**：一貫したポリシーの適用が実現されます。また、コンプライアンスの簡素化と監査範囲の縮小のためにネットワークをセグメント化できます。

シスコが選ばれる理由

IoT 環境の保護のためにシスコを選んだお客様には、ネットワーク セキュリティ リーダーのテクノロジーと専門知識が提供されます。IoT System Security の製品は、過酷な環境でのデバイスの保護、攻撃下における産業用制御システムの継続的な運用など、IoT 固有の要件に合わせて設計されています。

さらに、シスコでは、導入と、ソリューションのライフサイクル全体にわたる継続的なサポートが簡素化されます。サイバーセキュリティ、物理的セキュリティ、プロフェッショナル サービスなど、必要なものすべてを 1 つのベンダーから調達できます。

関連情報

Cisco IoT System Security の詳細については、http://www.cisco.com/jp/go/iotsystemsecurity を参照してください。

©2016 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1602R)
この資料の記載内容は2016年2月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C11-735952-00JA 16.03