ホワイト ペーパー

IoT への脅威に関する状況

IoT への脅威に関する状況の概要およびリスク ベースのセキュリティ プログラムの推奨事項

はじめに

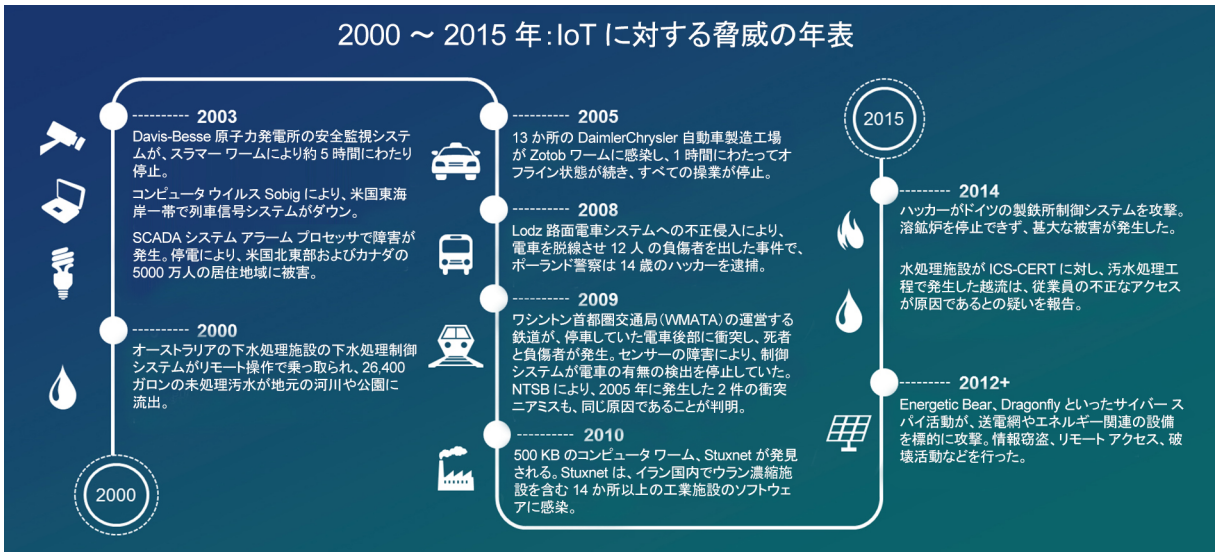
ネットワークは、閉じたシステムからインターネットに対応したオペレーショナル テクノロジー（OT）の接続へと拡大しており、業務部門と運用部門は、それに伴って発生するセキュリティとコンプライアンスの課題に対応しています。テクノロジーによって効率および運用効率を高める新たな機会が生み出される中、施設はますますネットワーク化され、Internet of Things（IoT）エンドポイントが急増しています。しかし既存のシステムの大部分では、セキュリティに対応するよう設計されていない多数のレガシー ハードウェアおよびソフトウェアが使われています。このようなレガシー システムは、セキュリティ要件が主な課題となる前に導入されたもので、多くの場合、新しいセキュリティ コントロールに対応するためのパッチ適用やアップグレードをすぐに行うことができません。このような事情から、エネルギー、製造、スマート シティ、運輸業界は、より高度で広く普及している絶え間ない脅威と、深刻な経済的損害と実際の物理的な影響（工程停止、送電網停止、人身事故など）を被る可能性に直面しています。

本書では、脅威の状況の経験的モデルを確立するため、セキュリティ インシデントと脆弱性の傾向について考慮します。このようなインシデントから得られる教訓、一般的な脅威、および攻撃パターンについて取り上げます。本書では、リスクに基づく脅威モデリング アプローチと、効果的なセキュリティ プログラム管理について説明します。この情報は、重要なセキュリティ リスクの軽減を優先し、かつ法規制への準拠を実現する、コスト効率の高いセキュリティ コントロールの導入に役立ちます。これにより、ビジネス リーダーと OT リーダーはスマート コンプライアンスを実現できます。つまり、コンプライアンスへの投資を活用して、実用的なセキュリティ リスクの軽減を促進することができます。エネルギー、製造、スマート シティ、および運輸の各分野に固有の例と検討事項について考慮します。

インシデントの歴史

2010 年の Stuxnet の発見は、産業ネットワークに対して脅威がもたらす物理的な影響の認識を広げるきっかけとなりました。また、エネルギー業や製造業などのさまざまな市場セグメントで発生する重大なセキュリティ インシデントは、脅威の現実性、影響の大きさ、これらの市場セクターが標的となっているという影響の規模を示唆しています。リスク管理の点では、攻撃の可能性、脅威の継続性、発生する可能性のある影響の深刻さを検討することで、重大なリスクが浮き彫りになります。高度な戦略を使用した外部からの攻撃により、さまざまな業界でセキュリティに対する認識が高まりました。Stuxnet 発生の前後におけるセキュリティ インシデントの例を、図 1「IoT セキュリティ年表」に示します。

図 1. IoT セキュリティ年表



IoT への脅威に関する状況

このようなインシデントは、IoT における影響と脅威のパターンについて何を明らかにしているでしょうか。公開報告情報の不足、発見されていないインシデント、守秘、およびエンタープライズ IT セキュリティ（長期にわたる重大なセキュリティ インシデントの報告の歴史を持つ）に比べて早期の導入サイクルということもあり、報告されている IoT セキュリティ インシデントの数は少数ですが、このようなインシデントのパターンから潜在的な影響が見て取れます。実際に、[9] SANS による 2014 年の調査『Breaches on the Rise in Control Systems』では、IoT への侵入が増加していることが指摘されています。同年に制御システム環境での侵入または感染があったと答えた回答者は 27 % にのぼりました。これは前年よりも 20 % 増です。さらに 13 % の回答者が、違反が発生した疑いがあると回答しました。

影響

IoT ネットワークでは、物理的および経済的な影響は現実問題となります。IoT 事業者、特にエネルギー、製造、スマート シティ、および運送の分野の IoT 事業者にとってこれは重大な影響を及ぼします。ネットワークの不正利用は、人身事故やサプライチェーンの中断につながることもあるからです。

公共の安全

IoT システムは本来、物理システムを制御するもので、公共機関での使用には、当然安全性が懸念されます。公的機関の場合、これは輸送システム、電力供給、水処理、流通、保管に当てはまります。DHS 分析の中で専門家は、次のように述べています。「PTC（ポジティブ列車制御）システムの本質的な自動化および制御のレベルでは、悪意のある攻撃者が脆弱性を悪用できる場合、そのような脆弱性は特に危険となる。システムレベルのアクセスを取得すると、攻撃者はさまざまなコマンドを実行できるようになる。このようなコマンドの多くは、ユーザによる監視がほとんど、またはまったくない状態では自動的なリアクションの連鎖を引き起こす可能性がある。」[10]製造業の場合、この安全の問題は従業員と顧客の両方に関係します。たとえば、最近の例では、運転中の車が不正に遠隔操作される脆弱性の問題が報告されています。

システムのダウンタイム

従来の IT 環境（IoT 導入で要件となる**可用性**と**整合性**よりも**機密性**と**可用性**を重視する）とは対照的に、IoT 環境で最も重要な属性は可用性と安全性です。IoT システムで高可用性が要件の場合、意図しない、悪意のないダウンタイムは、IoT システムのリスクを高めることになります。たとえば、ある天然ガス施設で、セキュリティ コンサルタントが侵入テストの一環として施設のネットワークをスキャンする際、テスト担当者が企業ネットワークから SCADA システムに水平移動し、SCADA システムが停止しました。これにより、この施設は 4 時間にわたってガスをパイプラインに供給できず、この間顧客はガスを利用できませんでした [11]。

コミュニティへの影響：国、州、地方自治体

公共サービスで中断が発生すると、地方自治体、州、および国全体のレベルで大きな経済的影響が発生することがあります。2003 年、米国北東部とカナダで発生した 60 ギガワットの停電と、2015 年 3 月にトルコで発生した数時間にわたる停電（81 県のうち 44 県で停電が発生）では、数十億ドル単位の経済的な被害が発生しました。ただし、より局地的なインシデントが大きな影響を及ぼすこともあります。サンフランシスコでは BART システムのバグが原因で、3 路線が 7 時間以上停止しました。これにより 35,000 人の乗客が取り残されたため、経済的なコストは 10 億ドルと推定されています。DHS によれば、ハッカーは交差点、高速道路入口、料金所、インターチェンジ、および市内の重要なポイントの機能を操作でき、長期にわたって市の交通網に影響を及ぼしました。[10]

ブランドへの打撃

Dow Chemical Company は、ボパールの工場事故から 30 年たった現在でも、ブランドへの打撃を受け続けています。この事故では、インドのボパールにある殺虫剤工場で発生した急激な化学反応が原因で、50 万人が有毒ガスと化学物質にさらされ、数千名の死者と、さらに多くの負傷者が出ました。たとえばロンドン議会は、Dow Chemical がスポンサーとなっている国際オリンピック委員会を、ボパールの事故との関連から批判し、「（スポンサーシップは）2012 年 ロンドン オリンピックの評判を傷つけるものである」と述べています。この事故の原因としては、メンテナンスの遅れ、運用上の誤り、設計不備、破壊活動などさまざまな要因が考えられますが、圧力、温度、およびレベル センサーの故障により、Union Carbide Corporation（UCC）（Dow が 2001 年に買収）の工場で起きた暴走反応を早期に検出できませんでした [13]。

信頼の喪失

DHS の分析では、「システム エラーにより列車の衝突事故、特に死亡事故が起きると、列車旅行に対する社会的な不安は増大する」と述べられています。[10] 原子力産業はこれまでにさまざまな攻撃を受けてきました。昨年にも、国外の不明な攻撃者により引き起こされ、NRC が確認したインシデントがいくつかあります [14]。たとえば、2008 年にジョージア州の原子力発電所で発生したインシデントでは、ソフトウェアのアップグレードが原因で、安全システムがデータの欠落を核燃料棒の冷却水の水位低下と誤って解釈した結果、48 時間にわたり発電所が緊急停止しました [15]。また、2003 年に発生した Davis-Besse 原子力発電所でのインシデント [16] もあります。

原子力発電所でのこうしたインシデントの例は、すでにエネルギー需要と公共の安全認識の間で微妙なバランスを保っている業界に対する、セキュリティ インシデントの影響を示しています。

スマート メーターは、すでに社会的な不信感を引き起こしているテクノロジーであり、一般的な認識における感情と経済的影響の両方のリスクを抱えています。漏えいした 2010 年の FBI の報告書によると、プエルトリコでは公益事業のメーター改ざんによる収益損失額は年間 4 億ドルを超え、スマート メーターのハッキングがさらに拡大するおそれがあることを示しています [17]。

知的財産の窃盗

一部の推定によれば、米国の企業に限っても知的財産のサイバー盗難の規模は、米国からアジア地域への輸出額に匹敵する年間数千億ドルにおよんでいます [18]。FBI は、知的財産のサイバー盗難は今年になり 53 % 増加したと推定しています [19]。こうした数値は見ただけではイメージが湧きにくいものです。では、ある製造業者がハッキングによりどのような影響を受けたか具体的な例をあげましょう。ロイターによれば、金属探知機や採掘テクノロジーを扱うオーストラリア企業の Codan は、金属探知機の設計図を盗まれました。

その結果、ゴールド ラッシュに沸く、需要の高いアフリカの市場で、偽造品が多数出回りました。Codan は金属探知機の価格を約 3000 ドルから 2000 ドル未満に引き下げざるを得ず、その結果、純利益が 80 % 減少しました [20]。

脅威に関与する攻撃者

IoT のセキュリティ インシデントを確認することで、さまざまなパターンが判明します。

高度な技術を持つ攻撃者

脅威に関与する攻撃者の中には、高度な技術を持ち、経済的な動機で活動する人たちがいます。このような攻撃者は一般に、エネルギー分野や公的機関における民族国家やテロリストによる脅威に関連していますが、製造業での競争が動機であることもあります（競合他社がテクノロジー設計や製造工程、価格設定、事業計画、契約、連絡先一覧などの詳細情報を狙っている場合や、サプライ チェーンの分断を目的としている場合など）。どの程度高度な技術であるかは、さまざまなマルウェア活動、ハッキング グループなど、攻撃者とその使用ツールについてここで取り上げた事例からも明らかです（サイドバーに掲載された「高度なマルウェアおよびハッキング活動」を参照）。

内部関係者の脅威

IoT における内部関係者の脅威は、従業員、請負業者、ベンダーが関わる、悪意のある場合と意図的ではない場合の両方のセキュリティ インシデントが関連する多面的な問題です。内部関係者による意図的ではない脅威に多い形態の 1 つは、（これまで悪意のあるネットワーク トラフィックと多様なネットワーク プロトコルから切り離されてきたことに基づく）悪意のあるネットワークに対する IoT システムの敏感さと、IoT の高可用性の要件に起因します。

意図的ではない脅威のもう 1 つのリスクは、自己増殖型マルウェアまたは継続的な攻撃者がエアギャップ ネットワークやその他の隔離されたネットワークに拠点を確立しようとする際に、第三者を攻撃ベクトルとして使う場合です。このドキュメントで説明するインシデントの多くでは、このような攻撃ベクトルの形態が関わっています。例：

- 請負業者がウイルスに感染したラップトップを使ってネットワークを感染させる
- USB ストレージ デバイスによってウイルスに感染させる
- 水飲み場型攻撃（攻撃対象企業の従業員が、トロイの木馬型ウイルスが仕組まれたソフトウェア更新により感染したベンダー サイトから、IoT ソフトウェア更新をダウンロードする）。
- 攻撃対象企業の従業員に対するフィッシング攻撃

IoT 環境での悪意には、従来の内部関係者による脅威に似た特性がありますが、その影響がよりはっきりと分かるという点が異なります（水処理施設の氾濫 [8] や、従業員が電力使用量を実際より少なく報告するために改ざんしたスマートメーター [18] など）。

攻撃パターン

IoT のセキュリティに対する脅威から、さまざまなパターンが明らかになります。

標的型攻撃

IoT では攻撃の多くが継続的かつ標的型であり、攻撃者は複数の攻撃ベクトルを用いてネットワーク内に拠点を確立し、そこから水平に展開します。このような状況では、攻撃者があきらめて別の標的に移っていくことを願い、攻撃されやすい脆弱性だけを取り除くだけというセキュリティ戦略では不十分です。

付随的被害のリスク

増加する IoT 固有のマルウェアでは、標的型攻撃として設計されている場合でも、自己増殖型の感染手法を用いています。そのため、意図しない対象が感染することがよくあります。新しい脆弱性（または、パッチ未適用/未解決の古い脆弱性）やゼロデイ脅威に関する重要な情報開示は、感染の懸念を強めるだけということになります。攻撃対象ではなくても、感染するおそれがあります。

ソーシャル エンジニアリングとフィッシング

従来の IT および運用テクノロジー環境と同様に、従業員はセキュリティ チェーンにおける弱点です。標的型攻撃活動の多くは、従業員を使ってネットワークにおける最初の拠点を確立します。これは、マルウェアで一般的な初期ベクトルでもあります。

リモート アクセス

IoT コントローラの分散的な特性、システム管理にベンダーが使用されるという一般的なシナリオ、そして多数のコンポーネントが新しいセキュリティ コントロールやプロトコルに対応していないという状況から、リモート アクセスが攻撃ベクトルとしてよく利用されます。このドキュメントで説明するインシデントの多くでは、これが主な攻撃方法として使われています。

脆弱性に関する状況

膨大な数のベンダー脆弱性の存在

ICS-CERT が公開している IoT システムに関する勧告の一覧には、セキュリティの問題、脆弱性、エクスプロイト（不正利用）に関する情報が載せられています。

従来の IT/OT ネットワーク環境は、最新の脅威によるリスクを受ける傾向にあり、多くの IoT システムの長い耐用期間と、パッチ適用の難しさから、新たな脅威は追加型、つまり脆弱性の累積に伴ってリスクが増加する傾向にあります。

IoT ネットワーク脆弱性のパターン

ICS-CERT が 2014 年度に実施したセキュリティ評価によれば、同機関が重要なインフラストラクチャ ネットワークで検出した脆弱性の多く（28 %）は、6 つの領域に分類されました（NIST 800-53 コントロール ファミリ）。

コントロール ファミリ	説明
境界保護	IoT ネットワークの不十分なファイアウォール制御（社内 IT/OT ネットワークまたはインターネットからの不十分な論理的分離など）。
情報フローの適用	ポリシーに基づいて IoT ネットワークでの情報フローやネットワーク間の入力/出力を制御する、技術的なアクセス制御メカニズム（ファイアウォール、ルータ、プロキシ、ゲートウェイ、トンネルなど）の欠落。
リモート アクセス	インターネットに直接接続するシステム、ベンダー、および請負業者、VPN 設定、個人デバイスや脆弱な OS の使用など、リモート アクセスのセキュリティ コントロールが弱い状態。
最小限の権限	必要最小限以上の昇格特権を使用したユーザのプロビジョニング（ルーティング機能に管理者アカウントを使用することなど）により、意図しないインシデントまたは悪意のあるインシデントの両方のリスクが発生する。
物理的アクセス制御	IoT 機器への物理アクセスが保護されていない。
セキュリティ機能の分離	多層構造のセキュリティ コントロールを使用せずにフラット ネットワーク トポロジを実装すると、不正な利用が容易になり、信頼度が異なるシステム間の接続のモニタが困難になる。

リスク ベースの IoT セキュリティ プログラムの実装

IoT ネットワークの所有者は、リスク ベースのアプローチを使用して、コスト効率の高い方法でセキュリティ リスクを管理し、かつ短期的なコンプライアンスを実現できます。リスク ベースのアプローチでは、脅威について把握している情報に基づいて、セキュリティ コントロールの導入に関する決定を行います。これにより、最も重大なリスクに最初に取り組むことになります。これらの優先事項をコンプライアンス要件（およびその要件の意図）に対応付けることで、コンプライアンスに対処すると同時に、大幅な支出の重複を解消できます。

ISA-99/IEC-62443、NERC CIP、および NIST SP 800-82 に記述されているガイドラインでは、セキュリティ プログラムの実装プロセスが詳細に説明されていますが、この説明は、このドキュメントで脅威モデルとして説明する影響、脅威の攻撃者、攻撃、および脆弱性の共通パターンに適用されます。また、リスク ベースのアプローチを使用して導入されたコントロールとコンプライアンス目標の相関関係を示すため、一部のコンプライアンス要件にも言及します。このため、推奨される 3 段階のセキュリティ プログラム実装手順を表 2 に示します。

表 1. 3 段階のセキュリティ プログラムの実装手順

ステップ	説明
1.評価	ネットワークのマッピングと IoT 資産のインベントリ作成により、現在のネットワーク環境を理解し把握することを目的としています。
2.実装	このステップでは、ネットワークを階層化し、システムを強化し、各自の脅威モデルに基づいてセキュリティ コントロールを実装します。
3.形式化	ポリシーと手順を文書化し、従業員のトレーニングを実施します。

このライフサイクルは反復的です。セキュリティ プログラムの改善に伴い、システムを再評価してネットワーク環境に新たな脆弱性または変更が発生していないかどうかを確認する作業を、継続的に行う必要があります。これは反復的なプロセスであり、セキュリティ プログラムの成熟レベルの異なるさまざまな組織に適用されますが、各ステップでの重点は異なることがあります。

評価

環境の評価では、IoT ネットワーク環境を構成する資産を明確に定義、マッピング、文書化することで、環境を最初に把握します。これは、サブネット レベル、施設レベル、およびグローバル レベルで実行できます。ただし、どの程度詳細に評価を実施したかに関係なく、ネットワーク境界での信頼の評価を促進するため、他のネットワークに対するすべてのネットワーク インターフェイスを文書化する必要があります。たとえば特定のネットワークを分析する際には、そのゲートウェイがエンタープライズ IT/OT ネットワーク、別の IoT ネットワーク、DMZ またはインターネットのいずれであるかを理解しておくことが重要です。この説明で使用する**ネットワーク**という用語は、分析範囲内の特定のエリアを意味します。ネットワークの評価は次の各作業で構成されています。

資産のインベントリ作成

ネットワーク内のシステム、アプリケーション、データ、セキュリティ コントロールなどの主要なすべての資産のインベントリを作成します。これには、そのネットワーク内のその他のネットワーク、およびそのネットワークと直接接続するその他のネットワークが含まれます。PLC、DCS、SCADA、および HMI システムをすべて特定する必要があります。主要なネットワーク デバイス、特にルーティング可能なデバイス、リモート アクセスを提供するシステム、既存のセキュリティ コントロールをすべて含める必要があります。

ネットワークのマッピング

論理ネットワーク セグメントと物理ネットワーク セグメントを明確に識別するネットワーク構成図に各資産をマッピングし、ネットワーク インターフェイスが明確に示されるようにします。このマッピングにより、各サブネットを、重要度、アクセス要件、およびセキュリティ レベルの面から評価できます。

ネットワーク マップを評価するときには、ネットワーク セグメント内の資産に共通するセキュリティ要件があるかどうかを検討してください。同じセグメントの他のデバイスのセキュリティ要件ほど信頼度の高くないユーザまたはシステムによって、特定のシステムにアクセスが提供されていますか。セグメントまたはゾーン間の接続がファイアウォールによって適切に保護されていますか。不要なポートは閉じていますか。

このような点を考慮することは大切です。セキュリティ ベスト プラクティスとコンプライアンスの両面における主要なアクティビティは、ネットワークを信頼度が異なる個々のシステムにセグメント化し、階層構造のセキュリティによる多層防御戦略を実装することだからです。

リモート アクセスの文書化

ネットワーク マップと資産インベントリにより、リモート アクセス ポイントを明確にする必要があります。これまでリモート アクセスも企業 IT/OT ネットワークの脆弱なポイントであり、非常に多くの IoT セキュリティ インシデントにおける侵入ポイントとなっていました。このようなアクセス ポイントすべてを、アクセス ポイントで許可されるプロトコル、アクセス ポイントを使用する従業員、請負業者、およびベンダー、アカウントの権限、接続後に付与されるアクセス レベル（特定のユーザにとって必ずしも必要ではないアクセス可能なシステムを含む）、ユーザ アカウントのタイプ（共有または個別）などの情報と共に特定する必要があります。

実装

脅威モデルを運用要件に適用し、既存のコントロールと緩和要因を検討し、残存リスクに対処するセキュリティ コントロールを導入します。ここでは、脅威の攻撃者、攻撃、および脆弱性に関して説明した共通パターンを脅威モデル テンプレートとして使用し、一般的なリスク領域を緩和する価値の高いアクティビティをいくつか紹介します。また、特定のコンプライアンス要件について説明し、リスク ベースのセキュリティ アクティビティとコンプライアンス イニシアチブの直接的な相関関係を示します。

ネットワークのセグメント化

ネットワークのセグメント化では、ネットワークを小さな論理サブネットワークに分割し、システムの信頼度と重要度、およびセキュリティ ドメイン内のアクセスに基づいてセキュリティ ドメインを切り離します。小規模組織では、最低限でも IoT ネットワークを IT/OT ネットワークから切り離します。より複雑な環境では、多数の論理 IoT ネットワークを各種カテゴリ（制御ゾーン、HMI ゾーン、エンタープライズ ゾーン、DMZ など）に分類します。セグメント化は、エンタープライズ セキュリティにおける長期的なベスト プラクティスですが、同時に IoT セキュリティの基本原理でもあり、NIST 800-82, Guide to Industrial Control Systems Security（2015 年 5 月）のセキュリティ アーキテクチャの主要コンポーネントです。

NERC CIP モデルに準拠するエネルギー企業にも、このベスト プラクティスが適用されます。NERC CIP のモデルは、エッジで保護されている大規模ネットワークのモノリシック セキュリティ モデルを説明しています。NERC CIP 全体が多重防御戦略を実装するものであり、セグメント分割を具体的に必要としています。セキュリティとコンプライアンスの両方の点で、ネットワークのセグメント化は、インフラストラクチャ保護の重要な部分です。この機能により、侵入者がネットワークの重要な領域にアクセスすることが困難になり、マルウェアの脅威が最小限に抑えられ、内部関係者による偶発的または悪意のある脅威が制限されます。

システムの強化

個々のシステムを強化する必要があります。このためには、不要な機能のアンインストールまたは無効化、サービスのパッチ適用、不要なアカウントの削除、未使用ポートとサービスのクローズ、デフォルト パスワードの変更などを行います。たとえば NERC CIP には、強化に関する特定の要件があります。

リモート アクセスの制御

リモート アクセス ポイントの制御は、セキュリティ リスクを最小限に抑える上で最も重要な要素の 1 つです。リモート アクセス ポイントでは次のようにする必要があります。

- 共有アカウントを使用しない。たとえば、ベンダーは共有アカウントを使用すべきではありません。
- 最小限の権限を使用する。可能であれば、リモート アクセスでは職務の要件を満たすために必要な最小限の機能セットだけにアクセスできるようにします。定期的にアクセス権限を確認する。
- デフォルト パスワードを変更し、新規ユーザとアカウントに対し初期パスワードの変更を義務付ける。
- 取り消しできるようにする。アカウントを定期的に確認し、不要なアカウントを削除する。
- すべてのアクセスをログに記録する。
- リモート アクセスを使用するすべてのユーザが、セキュリティ ポリシーへの準拠に同意する必要がある。
- 強力なパスワードを使用する。
- 総当たり攻撃を防止するため、リモート ログイン試行が繰り返された場合にアカウントを無効にする。

監視

セキュリティを監視するため自動化システムと手動システムを実装します。これには、侵入検知システム（IDS）、侵入防御システム（IPS）、パッチ管理、システム ログ、セキュリティ情報、およびイベント管理（SIEM）（セキュリティ イベントの監視、分析、相関付け）があります。マルウェアおよびウイルス対策システムが最新であることを確認し、必ずユーザ アカウントの監査を定期的に実行します。

形式化

厳格なセキュリティ プログラムを形式化します。これは実質的にすべての標準の主要なコンプライアンス要件であり、実用的なセキュリティ リスク管理ツールとなります。

ポリシーおよび手順の文書化

文書化されたセキュリティ ポリシーでは、組織のセキュリティ要件を明確に定義し、アカウンタビリティを確立し、従業員、請負業者、およびベンダーの基準を確立します。文書化されたポリシーは、セキュリティ プログラムの形式化における主要な要素です。特定のタスクに関するドキュメントも作成します。たとえば、導入前のシステム強化のための必須手順や、各種システムのパッチ管理要件を文書化します。

トレーニング

トレーニングはあらゆる組織で重要ですが、IoT 環境では特にそう言えます。特に第三者によるリスクを考慮すると、従業員、請負業者、ベンダーはいずれも、セキュリティ ポリシーと、システムへの適切なアクセス手順を理解していることを確認する必要があります。

ライフサイクル

これは反復的なプロセスであることに注意してください。脅威に関する状況はダイナミックに変化します。脅威と、脅威に関連するコントロールを継続的に再評価する必要があります。効果的な IoT セキュリティ プログラムとは、技術的なセキュリティ コントロールや 1 回限りの作業ではなく、組織全体で徹底的に制度化する必要があるプロセスです。

まとめ

IoT ネットワークの保護は困難です。リスクの性質を考えると、システムの可用性は優先度の高いセキュリティ属性であり、これは脅威に関する状況が二極化していることを意味しています。IoT ネットワークでは、競合他社や民族国家による高度な標的型攻撃と、従業員、請負業者、ベンダーによる偶発的な誤用の両方を懸念する必要があります。

ただし IoT ネットワーク所有者は、これまでの攻撃パターン、脆弱性、および過去のインシデントから得られた教訓を活かすことで、セキュリティ リスクを効率的に軽減し、かつコンプライアンス要件に対応する脅威モデルを構築できます。このリスク ベースのアプローチはコスト効率が高く実用的であり、最も重要なリスク領域を最初に重視します。これは継続的な情報セキュリティ プログラムのための重要な基盤となります。このプログラムでは、実証された ROI によって示される、強化されたシステム相互接続のメリットを組織が継続的に利用できるようにし、かつ IoT に関連する人的および経済的リスクを最小限に抑えることができます。

付録

参考資料

[1] 米国北東部で発生した停電
http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinalImplementationReport%282%29.pdf [英語]
http://www.oe.energy.gov/DocumentsandMedia/BlackoutFinal-Web.pdf [英語]

[2] Davis-Besse 原子力発電所の事故
http://www.securityfocus.com/news/6767 [英語]

[3] DaimlerChrysler の米国内自動車製造工場における Zotob ワーム感染
http://www.eweek.com/article2/0,1895,1849914,00.asp [英語]
http://www.computerwire.com/industries/research/?pid=750E3094-C77B-4E85-AA27-2C1D26D919C7 [英語]

[4] Wired Magazine、2015 年 1 月 8 日：ドイツの製鉄所への攻撃
http://www.wired.com/2015/01/german-steel-mill-hack-destruction/ [英語]

[5] Maroochy Shire 汚水氾濫
http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/ [英語]

[6] CSX 列車信号システム。2003 年 8 月 Sobig ウイルス
http://www.cbsnews.com/stories/2003/08/21/tech/main569418.shtml [英語]
http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807 [英語]

[7] ポーランド警察、2008 年に Lodz 路面電車システムに侵入した 14 歳のハッカーを逮捕
http://www.computerweekly.com/news/2240084537/Schoolboy-hacker-derails-Polands-tram-network [英語]

[8] 2014 年 5 ～ 8 月 ICS-CERT モニタ水処理施設の制御システムの異常動作
https://ics-cert.us-cert.gov/ [英語]

[9] SANS 2014 年調査：制御システム侵害の増加：SANS 調査
https://www.sans.org/reading-room/whitepapers/analyst/breaches-rise-control-systems-survey-34665 [英語]

[10] スマート シティの将来：サイバー/物理インフラストラクチャのリスク、2015 年 8 月、米国国土安全保障省、サイバーおよびインフラストラクチャ分析局（DHS/OCIA）
https://ics-cert.us-cert.gov/Future-Smart-Cities-Cyber-Physical-Infrastructure-Risk [英語]

[11] 天然ガス施設での侵入テストにおけるインシデント
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf [英語]

[12] セキュリティ研究者による車両ハッキング、リコールに進展
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [英語]

[13] Dow Chemical、1984 年ボパール化学工場事故
http://www.aria.developpement-durable.gouv.fr/wp-content/files_mf/Sensorsindustrialautomation_GB.pdf [英語]
https://en.wikipedia.org/wiki/Bhopal_disaster [英語]
http://www.ibtimes.co.uk/exclusive-30-years-bhopal-gas-tragedy-thousands-victims-still-wait-justice-1475466 [英語]

http://www.telegraph.co.uk/sport/olympics/news/9392569/London-2012-Olympics-Dow-Chemical-partnership-has-damaged-reputation-of-London-Games.html [英語]

[14] 米国原子力規制委員会コンピュータ、数回にわたりハッキングされる。2014 年 8 月報告。
http://www.nextgov.com/cybersecurity/2014/08/exclusive-nuke-regulator-hacked-suspected-foreign-powers/91643/ [英語]

[15] サイバー インシデントによる原子力発電所停止
http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html [英語]

[16] 2003 年、2006 年、および 2008 年の原子力産業でのセキュリティ インシデントの概要
http://www.safetyinengineering.com/FileUploads/Nuclear%20cyber%20security%20incidents_1349551766_2.pdf [英語]
http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdfhttp://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf [英語]

[17] 2010 年のプエルトリコにおけるスマートメーター改ざんに関する FBI の報告（Krebs on Security ブログ）
http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/ [英語]

[18] IP 乗っ取り、Economist Magazine
http://www.economist.com/news/united-states/21578405-it-time-retaliate-against-cyber-thieves-fighting-chinas-hackers [英語]

[19] IP 乗っ取り、FBI 統計、Fortune Magazine
http://fortune.com/2015/09/16/obama-warns-china-on-hacking/ [英語]

[20] IP 乗っ取り、Codan の事例、ロイター
http://www.reuters.com/article/2015/06/25/china-cybersecurity-australia-pix-graphi-idUSL3N0ZB15O20150625 [英語]

[21] ICS-CERT：推奨プラクティス：多層防御戦略による産業制御システム サイバーセキュリティの強化、2009 年
https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf [英語]

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

C11-735871-00JA 16.03