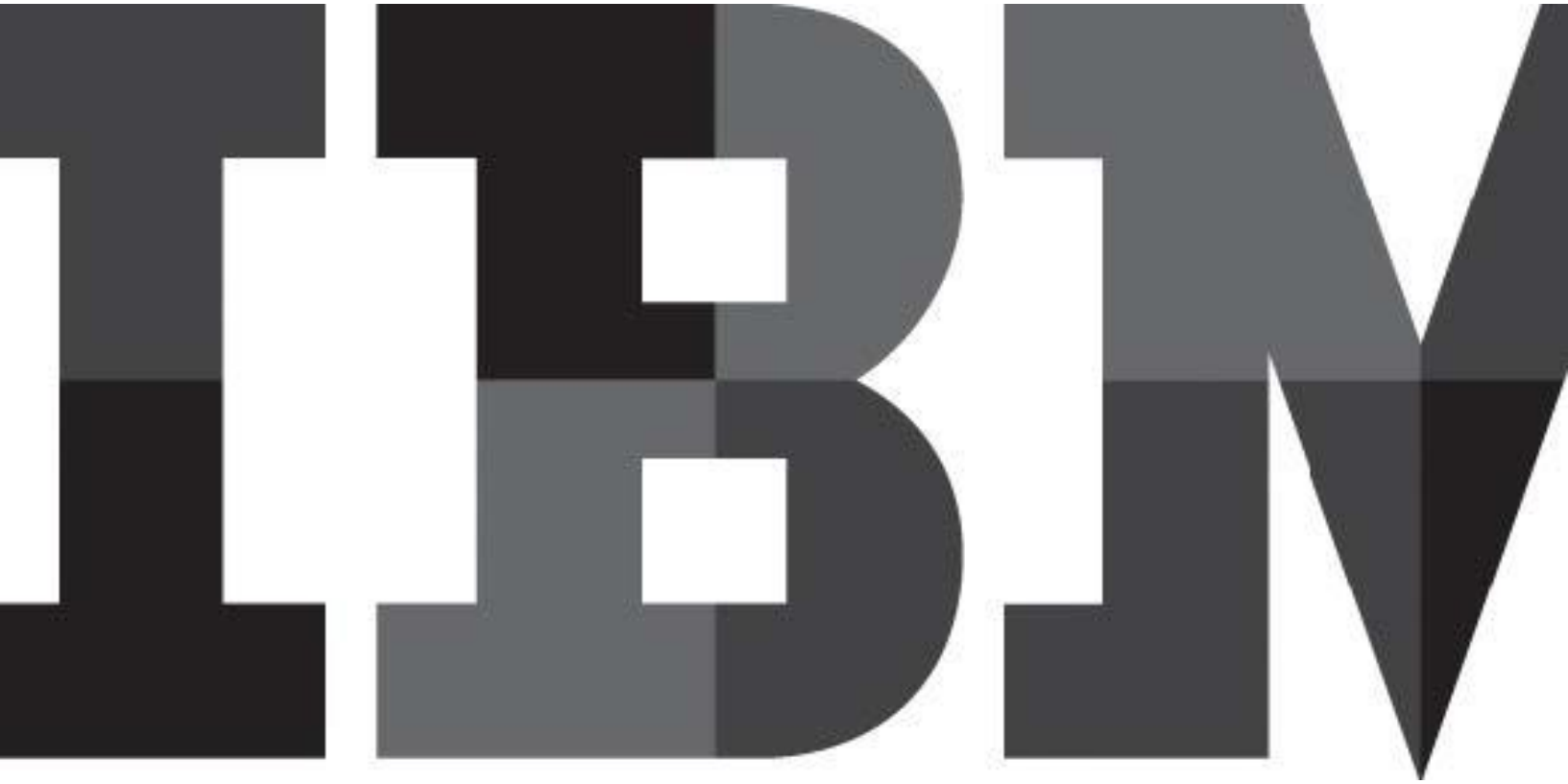
2015 年 4 月

Internet of Things (IoT) のセキュリティーに関する IBM の見解

「モノ」がネットワークに接続するとイノベーションとビジネス・チャンスが生まれる画期的な環境が実現するものの、広範な一連のセキュリティー上の課題と脅威も生まれます。



はじめに

本資料は、Internet of Things (IoT) のシステムに関するセキュリティーとプライバシーに関する IBM® の包括的な見解を記述したものです。2014 年 11 月のアナリストによるレポートでは、2020 年には IoT によって 300 億個のネットワークにつながった「モノ」が発生し、2013 年 の 990 万個から大幅な増加を示します [1]。サーモスタット、医療機器、自動車、工業設備など、私たちの生活、ビジネス、企業を豊かにするモノがあらゆる場面でネットワークにつながることにより、イノベーションと新たなビジネス・チャンスが生まれる画期的な環境が発生します。このような拡張したコンピューティング環境は、さまざまなセキュリティー上の課題と脅威をも生み出します。ネットワークにつながるモノの世界がこのような脅威を発生させ、モノが生成し、使用するデータや、モノを支えるアプリケーションが、悪意のある攻撃者にとっての攻撃ポイントとなる場合があります。発生する可能性のある攻撃には、個人情報や機密情報の取得、デバイスの操作と制御、IoT システム内でデータを使用し、提供するアプリケーションの混乱や停止などがあります。

製造、エネルギー、交通、その他の業種をサポートするビジネスを支える IoT システムが直面するリスクはさらに深刻化します。ビジネスで使用されるモノがインターネットとつながることで、広範な可視化、制御、状況に基づくメンテナンスが実現すると、セキュリティー攻撃に対しても脆弱性を持つことになります。Supervisory Control and Data Acquisition (SCADA) システムや工業制御システム (ICS) がハッキングの被害を受けた例がいくつか報告されています。「2 名のロシアのセキュリティーの専門家がセキュリティー侵害を受けた 6 万以上の制御システムが稼働していることを確認し、脆弱性を活用することで、エネルギー・システム、化学システム、交通システムが稼働するシステムを完全に制御できることを発見しました [2]」

IoT システムは他のデバイス、アプリケーション、サービスとコミュニケーションするデバイス (モノ)で構成され、これらのモノはさまざまなプロトコルを使用し、アプリケーション・プログラミング・インターフェース (API) 経由でインターネット上に存在するデータとサービスにアクセスしています。デバイスには、インターネットに直接つながり、何らかのシンプルなゲートウェイ経由でつながる基本的な個々のセンサーから、自立的な処理を行うことができるより強力かつ先進的な処理ノードまでが含まれます。例えば、ネットワークにつながるクルマは自立的な処理を行うことができるさまざまな電子サブシステムとセンサーで構成される複雑なデバイスであるものの、無線でインターネットに接続することもできます。

セキュア化の対象となるシステムのリスク・プロファイルに基づいて、IoT セキュリティーにはさまざまな要件があります。消費者 IoT システのが庭の植物の水やりシステムを測定し、制御する際のセキュリティー・ニーズは、IoT とつながる弁とポンプが含まれる、企業が使用する複雑でミッション・クリティカルな石油の掘削処理やパイプラインの運用のセキュリティー・ニーズとは異なります。掘削処理とパイプラインの運用には、ビジネス、環境、人間の生命を保護する安全性に配慮したシステムが必要です。不適切な掘削処理によるリスクとコストは、家庭の庭の水やりシステムのリスクとコストに比べはるかに大きくなります。そのため、包括的なセキュリティーに関する手段、専門知識、分析、テスト、管理が必要です。セキュリティー・リスクと複雑度が高い IoT システムを開発しようとする企業にとっては、そのようなシステムの設計と運用に関するアドバイスを提供できる経験豊富な専門家が必要です。IoT のセキュリティーに関する議論は幅広く実施され、多くの人と企業がさまざまな見方と分析を提供しています。IBM がセキュリティーと IoT について初めて言及したのは、2014 年 6 月に発行した IBV による調査 [3] を通じてでした。他の組織も情報と観点を発表しています。最近そのような発表を行った組織には、Open Web Application Security Project (OWASP)[4] に加え、Industrial Internet Consortium (IIC)[5]、Allseen Alliance[6]、および builditsecure.ly[7] などのコンソーシアム・グループが挙げられます。

IoT システム (またはあらゆる IT 環境) のセキュリティーの重要ポイントとは、あらゆるネットワークにつながるデバイスが恒常的に正常に機能することで、システム全体の整合性を常に実現することはできないということです。IoT システムの設計とセキュリティー機能は、前提条件として、個々のデバイスでセキュリティー侵害が発生する可能性があり (すなわち、完全なセキュリティー機能は存在しない)、1 つ以上のデバイスでセキュリティー侵害が発生してもセキュアに機能することができると考えています。

Internet of Things のシステム・アーキテクチャー

IoT システムはさまざまな構成を取ることがあります。一部の IoT システムでは、すべてのデバイスが直接インターネットにつながり、各デバイスは独自にローカルでセキュリティーを実現する必要があります。

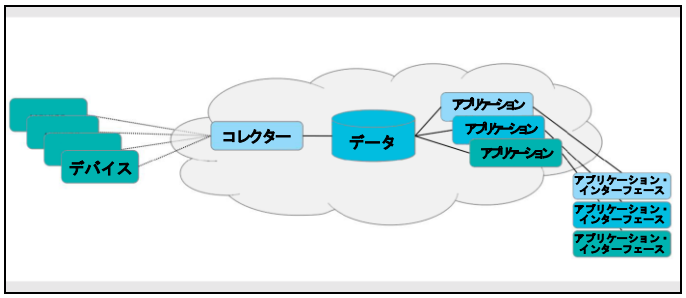


図 1: 直接ネットワークにつながるデバイスで構成される IoT システム

デバイスがローカルで中継デバイスやゲートウェイとしての役割を果たす集約ノードにつながることで、ローカルでつながったデバイスからのデータを集約する場合もあります。ゲートウェイはデータをフィルタリングし、インテリジェントにデータに反応し、インターネットとの間でデータとコマンドの送受信を行います。これまでネットワークにつながっていなかったデバイス、古いデバイス、セキュアでないデバイスと接続するために、ゲートウエイ・デバイスを使用します。これにより、複数のデバイスが共通の接続を使用できるようにすることで、運用を効率化することもできます。

ゲートウエイは外部の世界とつながる他のデバイス用のプロキシーとして、ローカルでネットワークとつながるデバイスのためにセキュリティーを管理する機能を果たす場合があります。ゲートウエイは下流のデバイスへの接続を管理し、当該デバイスの認証を行わなければならないため、ゲートウエイはセキュリティー・システムに不可欠の要素となります。

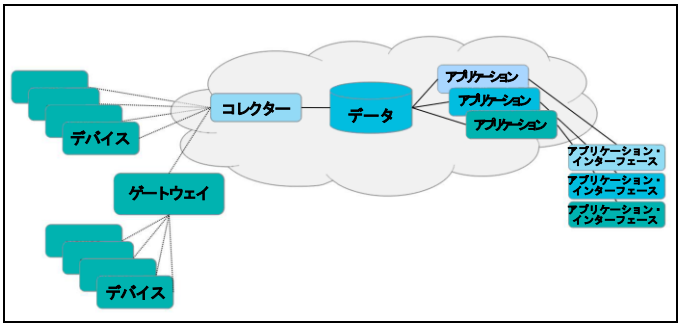


図 2: ゲートウェイ・デバイス経由でネットワークに接続するデバイスによる IoT システム

例えば、ネットワークにつながるクルマには多くのセンサーとプロセッサーが含まれるものの、これら自体はセキュアでなく、クルマ内のローカルのコントローラー・エリア・ネットワーク (CAN バス) にのみ接続します。テレマティクスやインフォテイメントのサブシステムのような単一のサブシステムが、クルマと外部の世界の間の通信ゲートウェイとしての役割を果たします。このサブシステムはクルマの他のサブシステムが提供するデータを集約することでインターネットと通信し、インターネットから受信したコマンドやデータを解析します。このサブシステムはローカルの CAN バス経由でクルマの他のサブシステムにデータとコマンドを再配布します。製造設備のメーカーのような製造環境においては、既存の業界プロトコル (Modbus、Profibus、DeviceNet など) からローカルのゲートウェイ・デバイスにつながるデバイスがよく見られます。ローカルのゲートウェイがデータを集約し、フィルタリングを行い、ローカルで分析を行う場合があります。また、クラウド・サーバーやバックエンド・サーバーに接続することで、より上流のシステムやアナリティクスにデータを配布することもできます。

クラウドにつながるデバイスは単一のエンティティーではなく、複数階層のインターネットにつながったノードで構成される場合があります。スケーラビリティー、パフォーマンス、フォールト・トレランスを実現するためにデバイスをサポートするアプリケーションが複数のハードウエア・ノードに分散しているものの、ネットワークにつながったデバイスからは単一の論理ソースまたは論理ターゲットに見えることがあります。

ピアツーピア・モデルやメッシュ・モデルで通信を行う IoT システムもあります。このようなシステムに関しては、対応すべきリスク、脅威、攻撃に加えて、考慮すべき独自のセキュリティー特性があります。ピアツーピアの運用環境による制限があるため、このような環境は管理が困難です。デバイスは通常低電力で稼働し、ネットワーク通信の能力が低く、コンピュー

ティング、ストレージ、メモリーの能力が比較的低くなっています。デバイスはネットワークにつながらない状態とつながった状態の間で移行し、対象となるデバイスがピアツーピアでつながったあるデバイス群から他のデバイス群に移行する場合があります。

IoT システムは、バックオフィスのシステム、その他の関連する IoT システム、中央政府や地方自治体のシステム、インターネット上の事業者が提供するサービスなどの他のシステムとつながる場合があります。IoT システムのセキュリティーを考える際には、デバイス、ネットワーク、アプリケーション・システムによるエコシステム全体を検討する必要があります。

また、ネットワークにつながるモノを使用する人間 (この場合は、典型的な消費者を指します) の視点についても考慮する必要があります。消費者はモバイル・デバイス経由で多くのモノにアクセスします。デバイスはネットワークにつながるモノで溢れた世界への窓口となり、セキュリティーに脆弱性をもたらすポイントとなる場合があります。

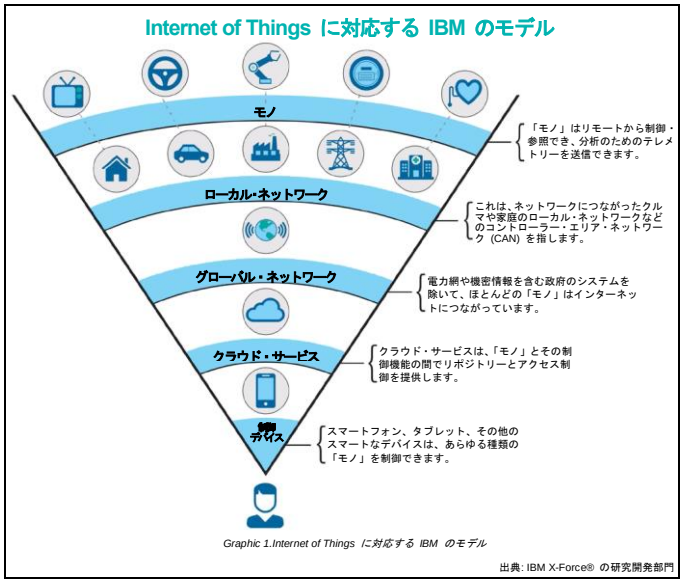


図 3: 人間から見た Internet of Things (出典: X-Force の研究開発部門)[8]

前述のとおり、IoT システムにはさまざまな種類のリスク、脅威、攻撃が発生します。図 4 が示すとおり、このような攻撃は図 2 のシステム・アーキテクチャーの概要図と関連するものです。このような攻撃には、中間者攻撃、アプリケーションの脆弱性、情報の漏えいなどのよく知られた攻撃が含まれます。アプリケーションまたはデバイスで発生するサービス妨害 (DoS) 攻撃も脅威となっています。IoT 環境内の他のシステムに DoS 攻撃を仕掛けるために、悪意のあるプログラムがセキュリティー機能の不十分なデバイスを乗っ取ることもさらなる脅威となっています。

攻撃やエクスプロイトに対抗する防御策も数多く存在し、多くの場合よく知られています。このような方策として、OS の一貫性のチェック、認証と権限の設定、異常の検出、セキュアな開発とデリバリーなどが挙げられます。図 4 にあるとおり、さまざまな種類の防御策が IoT システムのさまざまな領域に対応します。

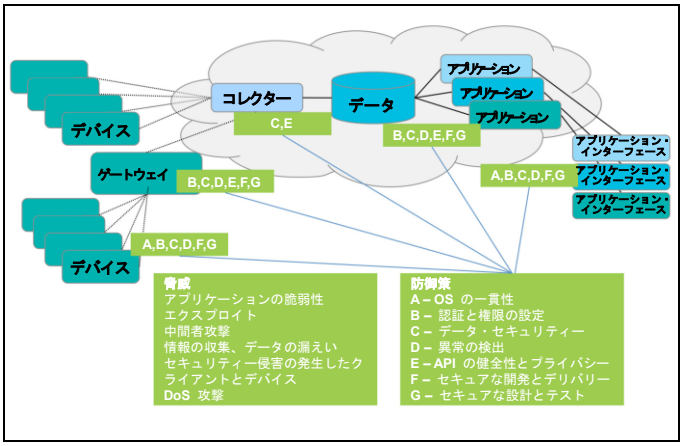


図 4: IoT システムに適用される脅威と防御策

本書を通じて、以下の 2 つの幅広い観点から IoT システムのセキュリティーを管理する際の課題と手法について解説します。

- モノの製造企業がセキュアな IoT システムとデバイスを設計し、製造する
- モノの運用企業が実装した IoT システムをセキュアに運用する

モノの製造企業がセキュアな IoT システムとデバイスを設計し、製造する

設計を通じてセキュリティーを実現する

重要ポイント:

- ネットワークにつながるデバイスとデバイスが稼働する環境の設計にセキュアなエンジニアリングの原則を適用する。
- ソリューションに複数階層の防御機能を含めることで、堅牢な防御体制を確立する。
- デバイスは脅威にさらされ、攻撃対象に含まるようになっている。
- 以前は独立して機能していたデバイスがネットワークにつながることで、あらゆるセキュリティー侵害のリスクが大幅に高まっている。
- デバイスが環境に含まれる他のコンポーネントと通信できなくなったとしても、デバイスでセキュリティー侵害が発生しないモードで運用できるようにする。

IBM はセキュリティー・テクノロジーの領域では幅広い経験を有し、この領域でさまざまなテクノロジーとソート・リーダーシップを提供してきました。IBM は IBM Secure Engineering Framework (SEF)[9] を通じて、ソフトウェアの保全とサイバー・サプライ・チェーンのセキュリティーに関する社内のベストプラクティスを公表しています。IBM の SEF は広範に適用することができ、ソフトウェア・アプリケーションの開発だけでなく、ネットワークにつながるデバイスや IoT システムにも対応します。

IoT デバイスはセキュア化できるよう設計する必要があり、標準状態でセキュアである必要があります。セキュリティーを実現するには、まずデバイスの設計段階で、デバイスに関して発生する可能性のある攻撃面を分析しなくてはなりません。脅威のモデリングを行い、どの脅威をどのように軽減可能か見極めることも、設計プロセスに含まれます。

デバイスで想定される運用条件と必要となる運用条件について、通信特性と運用特性の観点から検討する必要があります。例えば、デバイスのプロセッサーからの電磁場 (EMF) の放射を使用して実行中の計算を推測する場合は、このプロセスにより、使用されているセキュリティー処理の情報が攻撃者に伝わる場合があります。このような外的な運用特性が注意の必要な攻撃ポイントとなることがあります。このような潜在的な攻撃を排除するには、デバイスの設計段階で特別なパッケージングを行う必要があります。または、許容可能な運用条件を定義することで、物理的にデバイスの近くに EMF センサーが存在しないようにして、デバイスを物理的にセキュア化することもできます。

IoT デバイスにはセキュアな通信機能を組み込む必要があります。既存のテスト・分析・更新済みのセキュアな通信プロトコル (SSL/TLS や Diffie-Hellman のキー交換など) を再利用できます。また、Kerberos、既知の共通鍵と公開鍵/秘密鍵による暗号化アルゴリズム、セキュアなハッシュ・アルゴリズムも再利用できます。担当部門は既知の脆弱性に対抗できるセキュアな通信プロトコル (Poodle、Heartbleed、FREAK など) を使用し、タイムリーにこのような実装環境に変更を適用する必要があります。

デバイスの機能が増え、このようなデバイスが生成・送受信・処理・使用する情報も増えると、デバイスにセキュアな処理機能を組み込む重要性も高まります。デバイスが一意性のある ID を示し、その ID に基づいてパートナー (環境内のあらゆるロケーションで稼働する他のデバイスやサービスを含む) との間でセキュアな通信を設定する必要があります。

IBM は、IoT デバイスのライフサイクルをセキュア化する手法に関して、デバイスとプロセッサーのメーカーと協力しています。ライフサイクルの開始時点では、IoT デバイスで使用されるプロセッサーに暗号化情報を挿入し、製造時にセキュアなレジストリーにプロセッサーの ID を挿入します。ライフサイクルの次の段階では、デバイスの製造時に IoT デバイスにプロセッサーを実装する際に、セキュアなレジストリーにデバイスを登録します。次の段階では、ユーザーによる実装時にデバイスの有効化を行います。デバイスが有効な状態でなくなり、使用されなくなると、セキュアなレジストリーによってデバイスの除去と廃棄を行うことができます。セキュアなレジストリー・サービスは適切かつセキュアなアプリケーション・プログラミング・インターフェース (API) を使用するため、プロセッサー・メーカー、デバイス・メーカー、ユーザーはレジストリーをセキュアに使用できます。

IoT の開発部門は適切なセキュリティーのためのコーディング・ガイドラインを採用することで、侵入しやすい環境が生まれないようにする必要があります。セキュアなコーディング・ガイドラインについては多くの参照情報が提供されています。IBM Security AppScan[10] のようなツールを使用すると、ガイドラインを検証し、実行することができます。

担当部門はシステムの設計モデルにセキュリティーに関する視点を組み込み、脅威のモデリング [11] を活用することで、潜在的な脅威ベクトルを予測し、防御策と緩和策を設計することができます。IBM Rational® Rhapsody®[12] (UML/SysML による設計ツール) のような、セキュリティーと脅威のモデリングのプロファイルを持つシステム・モデリング・ツールの使用を検討してください。

API を通じて渡されるデータについては想定を行わず、すべてのデータをチェックしてください。通常セキュリティーを脆弱化させる要因となるのは、コンポーネントのインターフェースで不適切な想定を行うことです。コンポーネントのインターフェースでデータをチェックしないことのリスクを示す 2 つの好例としては、バッファーのオーバーフロー攻撃と SQL インジェクション攻撃があります。いずれの攻撃も、適切な境界やパラメーターに含まれるコンテンツをチェックするなど、インプット・パラメーターを適切にチェックすることで回避できます。

現代の変化の激しい環境では、開発部門の多くがオープン・ソースのコンポーネントを使用して既存の実装環境を再利用し、コア機能の成果物の提供をスピードアップしようとしています。オープン・ソースは迅速な開発には役立つものの、脆弱性の温床にもなります。IoT デバイス上で見つかったセキュリティーを脆弱化させたケースについてはさまざまなものが報告されています。このような脆弱性が発生したのは、既知の脆弱性を持つオープン・ソースのコンポーネント (Heartbleed/OpenSSL など) を使用することによるものです。このような脆弱性についての情報があり、広く実装されているため、ハッカーはデバイス上の脆弱性に対して簡単に攻撃を仕掛けることができます。企業は、すべてのオープン・ソースのコンポーネントとバージョンの依存関係を厳密にトラッキングする必要があります。IBM の X-Force による脆弱性の調査データベース [13] や 米国政府による National Vulnerability Database[14] など、定期的に発行・更新されている既知の脆弱性に関するデータベースもあります。あらゆる IoT アーキテクチャーにおいて、セキュリティー・リスクが判明した際にデバイスを管理し、アップデートする機能を持つことが不可欠です。システムの脆弱性が見つかると、このような脆弱性は、システムのアップデートが困難になることから発生しています。オープン・ソースのコンポーネントは通常迅速にフィックスを提供します。このようなフィックスが提供された時点で、オープン・ソースを実装したすべてのロケーションに配布しなければなりません。

多くの環境では、コーディングを行い、脅威のモデリングを行うことが十分に行われていません。セキュリティー侵害の発生後の環境を監査するには、システムに適用したすべての変更に関する詳細の記録を維持する必要があります。業界と企業によっては、変更記録の管理が義務付けられている場合があります。適切かつ先進的なソフトウェアの変更と構成の管理のための環境とアプリケーションのライフサイクル管理 (ALM) のツールを活用すると、障害やセキュリティー侵害に対応する際に、トレーサビリティーと監査適合性を実現できます。IBM Rational Team Concert[15] は変更をトラッキングするための先進的なモデルを提供するため、精密に監査を実施し、変更をトラッキングできます。

設計を通じてセキュリティーする際には、セキュリティー・ポリシーの要件を定義し、検討し、対応する必要があります。この設計プロセスでは、デバイスと全体的な IoT システムに関する適切な運用環境と運用条件を設定します。また、この設計プロセスでは、必要な条件がそろっていることを確認するために必要な検証メカニズムとチェックも定義します。

障害に強い運用モードを実現するには、特別な点について考慮する必要があります。ネットワークにつながるデバイス、当該デバイスが通信を行うネットワーク、または当該デバイスが通信するその他のデバイスやシステムでセキュリティー侵害が発生している可能性がある場合も、当該デバイスは安全な運用を継続する必要があります。安全に運用を継続しなければならいことは、IoT システムでセキュリティーを設計する際の最も重要なポイントの 1 つとなります。モバイル・デバイスのユーザーが天気や株価を確認できなくなることと、工業用水道ポンプが下流に生息する生物を保護することを目的として、水流スピードを決定するために必要な現在の条件を評価できなくなることの間には大きな違いがあります。

設計に基づいてセキュリティーを実現するには、情報技術 (IT) と運用技術 (OT) の要素についても検討しなくてはなりません。IoT システムの一部は比較的制御された条件下で稼働しているものの、環境の大部分はあまり制御されていない環境下で稼働し、悪天候条件の影響を受けやすく、攻撃に対して弱くなっています。このような条件下では、デバイスをオンサイトで調整することが困難になる可能性が高いため、デバイスのリセットとアップデートは主に無線通信を通じて行うこととなります。

このような環境を考えると、システムをセキュアに維持するには恒常的な努力が必要なことは明らかです。Internet of Things では、当然のことながら、デバイスの脆弱性とデバイスを保護する必要性に着目する必要があります。しかし、デバイスがより大規模な複数階層システムの一部となっているという全体構造を忘れてはいけません。IoT デバイスが脆弱なのは、特に物理的に制御された環境の外でアクセスできるためです。最適な防御策を実施した場合でも、すべてのデバイスが継続的に障害耐性を持ち、恒常的にセキュリティー侵害を受けないことを保証することはできません。個々のデバイス・レベルでセキュリティーを 100% 保証することはできません。1 つ以上のデバイスで最終的にセキュリティー侵害が発生する可能性がゼロではないため、IoT システムの設計者はデバイスでセキュリティー侵害が発生する可能性があることを想定しなければなりません。1 つ以上のデバイスでセキュリティー侵害が発生しも、システムは当該デバイスがもたらす脆弱性を分離し、排除しようとすることで、引き続き正常に機能する必要があります。例えば、あるデバイスを物理的に持ち去り (盗難または家宅侵入を通じて)、リバース・エンジニアリングを行うことで、セキュリティー侵害が発生する場合があります。このような攻撃はハードウェ

アに基づく暗号とハードウェアに組み込んだデジタル証明書と鍵を使用するため、大きな被害を発生させることがあります。しかし、このような攻撃を排除することはできません。そのため、システムの設計とテストの際には、デバイスでセキュリティー侵害が発生するケースを検討し、実行する必要があります。本プロセスにおいては、残りのシステムが稼働し続けたうえで、システムがセキュリティー侵害が発生したデバイスの特定、分離、報告を行う必要があります。

設計を通じてセキュリティーを実現する

重要ポイント:

- データの分離、分類、編集、加工を行うことで、個人情報を除外する。
- 一意性のあるデバイス ID は、個人情報とみなされる場合がある。
- 通信とデータの保存の際に、一時的な ID と別の ID を使用する。一意性のあるデバイス ID と一意性のある個人情報にデータを関連付けることができないようにする。

モノに出入りするデータに加え、モノやモノを制御するデバイスに保存される可能性のあるデータが、機密情報であることがよくあります。ドライバーは自分の携帯電話をクルマに搭載したインフォテイメント・システムにつなぐことがあり、このシステムはドライバーの連絡先情報、E メール・アドレス、テキスト・メッセージにアクセスします。携帯電話で財務アプリケーションを使用すると、クルマからクレジットカード情報がアクセスできる場合があります。また、ホーム・オートメーション・システムや製造制御システムにアクセスするための認証情報を適切に保護しなければ、漏えいする可能性があります。

デバイスから収集した情報を活用すると、どのような人やモノがどこにいつ存在し、どのような処理・タスク・アクションを行っていたのか特定できる場合があります。これほど詳細に何が発生しているのかを確認できることはかつてありませんでした。そのため、どのようにしてこのようなデータを処理し、誰がこのデータにアクセスし、人や企業がこのデータに基づいて何を行うことができるのかについて懸念が生まれるのは当然です。

IT 業界では、長年にわたって医療情報と金融情報に含まれる個人情報 (PII) を取り扱ってきました。データ・プライバシーは新たな課題ではないものの、情報の量と大量の情報がもたらす詳細情報は新たな課題となっています。IBM InfoSphere Guardium[16] と IBM InfoSphere Optim[17] のソリューションは、データ・プライバシーを処理することに特化した機能を提供します。このようなツールは、リアルタイムのデータ・セキュリティーと監視、精密なデータベースの監査、コンプライアンス報告の自動化、データ・レベルのアクセス制御、データベースの脆弱性の管理、機密データの自動検出、オンデマンドによる静的または動的なデータ・マスキングを一元的に制御します。

IoT ソリューションを開発しようとする企業は、ソリューションの開発時にデータ・プライバシーについて検討する必要があります。情報を保存するために使用するデータ・モデルから、パートナー、ユーザー、消費者に提供する外部インターフェースに至るまで、どのデータをどの形式とどの粒度で管理すべきか常に問いかけ、プライバシーに配慮した回答を提供しなければなりません。

情報がデバイスからデータ収集システムに流れると、当該情報を保護する必要があります。データ・センター内では、PII を他のデータ要素と分離することで、この情報が環境全体に広がならないようにする必要があります。情報のプライバシーと関心の分離については、これまで検討と対応が行われてきました。情報への不正アクセスを防止し、個別には特定できないデータを関連付けることによる推定知識を排除するために、マルチレベルのセキュリティー (MLS) のような手法を活用することを検討してください。

複数のデータ・セットからの情報を使用することで、PII が保存されていない場合でも推定できる可能性については、特に配慮する必要があります。医療情報と金融情報の管理に関するセキュリティー対応を通じて、このような課題の検討と対応が既に行われており、IoT システムにも適用することができます。

さらに、Internet of Things を通じて、センサーとデバイスから収集する情報へのアクセスを中継し、提供するための新たなビジネス・モデルも生まれています。データは、RESTful なサービス・インターフェースなどのプログラミング・インターフェースを通過することで通常提供されます。プログラミング・インターフェースは、パラメーターとして提供されるデータ要素と返されるアウトプット・データを定義します。各インターフェースが PII を開示する可能性について検証する必要があります。例えば、ウェアラブル・デバイスを身に着けたユーザーの数を検索して、ユーザーのエクササイズ状況をトラッキングすると、不適切にデバイスの名前を開示する場合があります。この開示の結果、デバイスの名前の付け方 (「Jane Doe's Fitbit®」など) によって、ユーザー名を関連付けることができることがあります。このような場合、不適切な開示を行うことがないよう、特別な防御策を設定しなければなりません。その他の防御策の例としては、集約済みの情報 (十分なサイズのサンプル・セットに基づく平均値や偏差値) のみを返すことや、個人や個別のデバイスを特定する情報を加工し、一般化することが挙げられます。

データ・プライバシーに関してさらに考慮すべきことは、データ保持のポリシーです。収集対象の情報の量が増大するにつれ、将来のある時点でこの情報の一部を使用する可能性が高まります。この状況を回避する 1 つの方法は、適切なデータの保持と

廃棄のポリシーを設定し、必要なくなった情報の除去と削除を積極的に行うことです。法的に可能になった時点で即時に情報を積極的に削除することは理にかなっています。

テストを通じてセキュリティーを実現する

重要ポイント:

- セキュリティーのテスト手法は、他のソフトウェア・システムと同様にデバイスにも適用される。
- コードの分析、倫理的なハッキング、その他の手法をデバイスとデバイス側のコードに適用する。
- 悪意のある環境のテストを行う際は、物理的な悪意のある条件だけでなく、通信とネットワークに関する悪意のある条件にも適用する。
- テストによる検証に基づいてコードが正しい場合は、攻撃面は縮小する。

セキュリティーの脆弱性のテストを行うことは、あらゆる IoT の実装環境に不可欠の要素です。ソフトウェア・システムに通常適用されるセキュリティー・テスト手法は、IoT のデバイスとインフラにも適用できます。

すべての IoT プロジェクトに一連のテストを行うことによって、設計の仕様どおりに機能することを検証しなくてはなりません。このようなテストには、センサー・デバイスに組み込んだセキュリティーのメカニズムとサービスの検証や、このようなデバイスと通信するインフラの検証が挙げられます。

以下をはじめとする複数段階に基づくテストを実施できます。

- 単体テストは、ソリューションのあるコンポーネントが設計どおりに独立した機能を果たすことを検証します。
- 機能検証テストは、複数のコンポーネントから成るソリューションが明記された仕様どおりに稼働することを検証します。
- システム検証テストは、包括的なソリューション環境内のコンポーネントの連携と稼働について検証します。

セキュリティー・テストはすべてのテスト段階で実施できます。セキュリティー・テストでは、IBM Rational® Software Analyzer[18] や IBM Security AppScan[19] などのテスト・ツールが使用される場合があります。また、倫理的なハッキング手法を使用するセキュリティー・テストを行うこともできます。システムがセキュアかどうかを評価するために、幅広い種類のテスト手法を使用できます。製品やソリューションの開発とリリースが行われた後も新たな攻撃が開発されるため、攻撃への耐性を繰り返しテストすることが重要です。開発段階と品質保証段階でのテストに加えて、本番稼働している IoT システムにもテストを行うことをお勧めします。デバイスが過酷な物理的な運用条件にさらされるのと同様に、これらのデバイスは過酷なコンピューティング条件にもさらされています。このような条件には、デバイスの混乱、制圧、無効化を目的としてデバイスに大量の情報が送信される DoS 攻撃やジャミング形式の攻撃への耐性を持つことが挙げられます。

必要に応じて、ソリューションに対して外部による分析とテスト (共通の基準[20] が定義する認証を含む) 実施する場合があります。侵入テストを実施するために、IBM X-Force が提供する資料を活用できます。IBM X-Force は最新のインターネット上の脅威のトレンドの研究と監視を行い、IBM のお客様向けにセキュリティー・コンテンツを開発し、お客様と一般ユーザーに最新の脅威と重要な脅威への対応方法に関するアドバイスを提供しています。

継続的なデリバリー・モデル

重要ポイント:

- デバイスの製造、提供、実装を行った後に、問題と脆弱性が検出される。
- サービスの提供中に、デバイス側のコードをアップデートする必要がある。
- デバイス側のコードを継続的に提供する手法を計画し、実施する。
- アップデートの適用、実行、有効化のタイミングを決定するには、特別なポイントを検証する必要がある。

ソフトウェア業界ではアジャイルな手法と開発と運用 (DevOps) の手法がよく使用され、それには適切な理由があります。このような手法では早期にお客様に有益な機能を提供でき、ユーザーからよりスピーディーなフィードバックが得られ、このような機能をより迅速に調整し、更新することができます。ソフトウェア製品のデリバリーは、低頻度で製品をリリースし、移行計画を提供し、新バージョンの稼働を行うことではなくなり、継続的にデリバリーの流れを提供することを意味するようになっています。サービス・ベースの環境の到来により製品とフィーチャーがサービスとして提供されるようになり、本番稼働中のオファリングに頻繁にアップデートを加えることが当たり前のことになっています。

このような環境にはメリットとデメリットがあります。しかし、機能の更新とデリバリーを継続的に行い、最終的には「当たり前のこと」にすると、提供される製品に含まれるセキュリティー関連の問題に対応できる開発パスとデリバリー・パスを実現できます。

予防、検出、反応、対応など、あらゆる形態でセキュリティーに関心を払うことが重要です。継続的なデリバリーを行うと、製品のリリース、パッチ、フィックス・パックのような過去に行われていたメカニズムに比べ、反応と対応がはるかに簡単になります。

ソフトウェア開発におけるアジャイルな手法と DevOps の手法で使用されるものと同じ手法の多くは、IoT システムの開発とデリバリーに適用できます。重要な相違点は、稼働中でアップデートが必要なコードが制御されたデータ・センターやサーバー環境に存在しないということです。それどころか、コードは現場、ルーター、ゲートウェイ、センサー、その他のデバイスで稼働しています。このようなデバイスは他の場所に移動することもあれば特定の場所に常に存在することもあり、ネットワークと常時つながることもあれば時折つながることもあり、さまざまなストレージ能力とコンピューティング能力を持っています。しかし、このようなデバイス内で稼働しているのはやはりコードであり、製品が現場で実装された後に発見される問題や脆弱性がコードに含まれています。このような問題を 100% 防止することはできないため、発見された問題に対応するためにシステムを無線通信を通じてアップデートする必要があります。

デバイス上で稼働するコードについて継続的なデリバリーのモデルを実現するタイミングが早ければ早いほど、頻繁にアップデートとフィーチャーの追加を行うことで、より早期かつより迅速に自社の顧客に機能を提供することができるようになります。この仕組みを実現するには、無線で受信するアップデートを検証する必要があります。そのためには、コードの署名手法と検証手法を使用することも必要です。このような技術は取り立てて新しいものではないものの、システムのデバイスの開発と実装のために適用する必要があります。

現場のデバイスを無線でアップデートするためには、独自の課題が存在します。特に、アップデートの適用中も、デバイスは使用可能である必要があります。もしくは、デバイスにアップデートを適用できる適切な場所、時間、環境になるまで、アップデートの処理と適用を遅らせる適切なロジックをデバイスが持つ必要があります。デバイスは、障害に対して強いフォールバック・メカニズム (稼働中のシステムをチェックし、一貫性のない動きをすることが判明した変更を取り消す機能を含む) を持つ必要があります。

多くのデバイスで稼働するコードには、オープン・ソースのソフトウェアが含まれています。デバイス・メーカーは使用中のオープン・ソースのコンポーネントの一覧を管理する必要があります。そうすることで、コンポーネントのうちの 1 つで脆弱性が見つかった場合、デバイスのオーナーとオペレーターに迅速にアップデートを提供できます。また、脆弱性が見つかった場合に迅速に対応できるよう、デバイス・メーカーはデバイスのオーナーとオペレーターとの間で連絡プロセスを設定する必要があります。このような脆弱性を公表し、対応を行うために既存の手段としては、US-CERT[21] や Common Vulnerability and Exposures[22] による形式があります。

一貫性のある製造とデリバリーを行う

重要ポイント:

- デバイスのデリバリーには、サプライ・チェーン全体が関係する。
- デバイスの製造に関するサプライ・チェーンをセキュア化するための既存のガイドラインに従う。

信頼性の高いサプライ・チェーンでは、設計、製造、配送、フルフィルメント、インポート、エクスポート、知的財産の管理、サポート、メンテナンスを効果的に管理しなければならない。IBM はグローバル規模でサプライ・チェーンのセキュリティーを支援し、Electronic Industry Supplier Code of Conduct (電子業界サプライヤーの行動規範) の創設メンバーでもあります。IBM は、サプライ・チェーンのセキュリティーに関する Open Group[23] の基準の構築に
協力しています。

信頼性の高いサプライ・チェーンでは、サプライヤーは以下のガイドラインに従う必要があります。

- サプライヤーの行動とセキュリティーに関して設定された原則に準拠する。
- 定期的に評価結果を提出する。
- 準拠していないことが判明した場合は、是正策を実施する。
- コンポーネントの堅牢性、安定性、パフォーマンス、セキュリティーを保証する。
- ソフトウェアとファームウェアの開発ライブラリーと資料に対する適切なアクセス制御を設定する。
- 提供されたすべてのコンポーネントのソースを明記することで、オリジナルのコンポーネントであることの証明を行う。

サプライヤーの評価プロセスの重要な要素として、セキュリティー・リスクの評価があります。セキュリティー・リスクの評価の目的は、サプライヤーのリスク全体を構成するすべてのコンポーネント (オファリング、プロセス、ビジネスのリスクを含む) を特定することです。セキュリティー・リスクのレベルを評価するために、リスクの特徴を見極めます。評価プロセスの一貫として、移行戦略を評価することもできます。

製造とデリバリーをセキュア化するには、プロセス、手続き、サプライ・チェーンをセキュア化する必要があります。製造のセキュア化とは、デバイスとシステムを製造する本番環境の物理的なセキュリティーを確保することでもあります。このようなシステムの本番環境は必ずセキュア化する必要があります。組み立てラインと製造ラインで脆弱性とセキュリティー侵害が発生することで、IoT デバイスに脆弱性が組み込まれる場合があります。これまで、電子機器に脆弱性が組み込まれたケースが発見されています。製造中にこのような脆弱性が組み込まれ

た理由としては、一部の製造システムそのもので脆弱性が発生し、セキュリティー侵害が起きたためです。

IBM Global Business Services は、多くの業種のサプライ・チェーンの最適化、監査、セキュア化を行うサービスを提供します。

モノの運用企業が実装した IoT システムをセキュアに運用する

デバイスを堅牢化する

重要ポイント:

- ソリューションに複数階層の防御機能を含めることで、堅牢な防御体制を確立する。
- ソリューション全体の可用性を実現するため、セキュリティー侵害が発生したサブシステムを分離する手段を設定する。

デバイスの開発部門、テスト部門、製造部門はデバイスで問題を防止するためにあらゆる施策を実施することができるものの、過去の事例を見ると、防止のためにどれだけの労力をかけても、脆弱性が見つかり、攻撃が実施される可能性は常に存在します。攻撃に対して効果的な防御を行うには、徹底的な防御を行うための手法を採用する必要があります。データ・センターでファイアウォールを設置する場合であれ、家庭用のルーターにフィルタリング機能を設定する場合であれ、このような手法は徹底的な防御機能を実現します。複数階層の防御を行うとさらに強固な防御を行うことができ、セキュリティー侵害の発生したデバイスやシステムを分離することもできます。

デバイス (より適切にはデバイスが稼働する環境) を堅牢化するには、ゲートウェイとルーターを使用して、脆弱性が発生している可能性のあるデバイスをネットワークの他の要素から分離する必要があります。このようなルーターとゲートウェイを使用して、脆弱な部分と脆弱でない部分を独立させることができます。例えば、ゲートウェイの外側でセキュリティー侵害が発生した場合、このゲートウェイを使用することで、当該デバイスから提供される情報、データ、ノイズを遮断することができます。また、ゲートウェイやルーターを活用すると、ゲートウェイやルーターの外側で稼働するデバイスで発生している可能性のあるネットワーク通信の大半をブロックすることもできます。

ゲートウェイやルーターがこのような環境の攻撃ポイントになる場合もあります。保護され、情報通信が行われる経由ポイントであるデバイスと同様に、ゲートウェイやルーターにも、同じ堅牢化要件、継続的なデリバリーの要件、無線通信によるアップデート要件を適用する必要があります。

また、ゲートウェイやルーターは、センサー・データのフィードを利用して、デバイスとサービス・ベースのアプリケーションの間の通信の健全性を評価するための、ネットワーク上の監視ポイントにもなります。

適切なアクセスと不適切なアクセスを定義したうえで (インバウンド・アクセスとアウトバウンド・アクセスを含む)、デバイスへのアクセス権に関するポリシーを設定し、更新することが役に立ちます。IBM の Unified Endpoint Management[24] など、デバイスのセキュリティー・ポリシーを制御できるエンドポイント管理ソリューションの導入を検討してください。エンドポイント管理システムは、サイズが小さく低電力の組み込み型デバイスでは機能しない場合があるため、システムのできるだけ下流でエンドポイントの管理を行う必要があります。少なくとも、ゲートウェイ上ではエンドポイントの管理を実施する必要があります。

通信チャネルをセキュア化する

重要ポイント:

- デバイスとシステムの間の通信パスをセキュア化する必要がある。
- ネットワークのタイプと接続方法の信頼性が低い場合がある。
- 使用する各プロトコルについて、設定したガイドラインに従う必要がある。
- IP 通信を保護する際には、通常 SSL/TLS を使用する。

IoT システムでは、幅広い種類のネットワーク通信メカニズムを使用します。このメカニズムには、Bluetooth、Bluetooth Low Energy (BTLE)、6LoPAN、Zigbee などの低電力・低レンジの手法を使用するローカル・エリア・ネットワーク機能が含まれます。また、WiFi を使用したローカル・エリア・ネットワーク機能や、2G、3G、4G の LTE によるワイド・エリア・ネットワーク機能も含まれます。

デバイスが物理環境を移動する際に接するネットワークのセキュリティー機能が異なるのと同様に、さまざまなネットワーク・モデルが提供する防御機能のレベルは大きく異なります。ネットワーク・メカニズムが大きく異なる場合でも、IoT システムはセキュアな通信を行うことができなければなりません。

IoT システムの通信機能は、通常 TCP ネットワーク接続に基づく HTTP ベースの通信 (REST 形式の呼び出し) か、IP ネットワーク・スタックを使用した何らかのイベント・ベースの通信のいずれかの形式を取ります。イベント・ベースの通信モデルとしては、DDS、CoAP、MQTT による形式があります。イベント・ベースの通信モデルは通常 TCP モデルではなく UDP モデルを使用することで、ネットワークにより発生する接続と

データ転送のレイテンシーを削減します。

HTTP ベースのモデルとイベント・ベースのモデルでは、通信をセキュア化するために SSL/TLS が広範に使用されます。このモデルは複数の暗号化アルゴリズムを組み合わせることで、セキュアな通信チャネルを設定します。これにより、デバイス、ゲートウェイ、クラウドでホストされたシステムで稼働するほとんどのロジックがセキュアな通信チャネルを使用し、デバイスまたはアプリケーションの機能を提供できるようになります。

使用パターンを監査し、分析する

重要ポイント:

- 予防策はすべての問題に対応できるわけではない。
- 対応し、是正が行えるよう、検出が必要となる。
- 既存のログ分析手法を使用して、異常を特定し、対応する。

IT 業界では、システムに対して発生する可能性のある攻撃のすべてを予測し、ましてや防止することはできません。発生する状況を検出し、反応し、対応することは、セキュリティーを念頭に置いてシステムの設計・導入・実装を行うことと同様に重要になっています。この領域においても、IT 業界の既存の機能が IoT 環境に大きく貢献することができます。

コンピューティング環境を管理するには、システムの挙動を管理し、注意すべき状況を見極め、そのような状況に反応しなければなりません。ニアタイムとリアルタイムで実施する対応と長期的な分析とレポーティングの両方を検討する必要があります。実施中の攻撃を検出し、そのような攻撃に対応しなくてはなりません。このような状況は、セキュリティー機能の不十分なデバイス、外部からの DoS 攻撃、環境で稼働中の特定または一連のデバイスに対する継続的な攻撃によって発生します。システムの使用パターンを積極的に監視すると、挙動に関する異常を検出し、適切な対応を行うことができます。システムを監視するツールを効果的に使用するには、このような監視ツールを積極的に使用する必要があります。イベントを監視し、記録するだけでなく、状況を監視し、対応しなくてはなりません。IBM Security QRadar® SIEM[25] (Security Information and Event Management) のようなツールに含まれる機能を使用すると、このような監査と分析を行うことができます。

長期間にわたって発生する可能性のある脅威も存在します。このような場合、システムの挙動を観察することで、共通の挙動パターンと想定した挙動パターンを検出する必要があります。システムを積極的に監視することで、一連のイベントが異常かどうか見極めなければなりません。異常の検出手法を活用すると、デバイスが正常な稼働状況とは一貫性のない方法で稼働し、機能し、通常とは異なる情報を生成している場合に、セキュリティー侵害が発生している可能性のあるデバイスを検出できます。IBM Operations™ Analytics - Log Analysis[26] のようなツールには、システムが想定される挙動を示しているかどうか見極めるために、一定期間にわたって環境を監視するために必要な機能が含まれています。

ゲートウェイ、デバイス、クラウド、データ・センター上でホストされたサービスなどを通じて、システムで発生しているイベントを積極的に監視する必要があります。さらに、システム全体の運用を監査するためにポリシーを設定する必要があります。このような監査を通じてシステムの「監視機能を監視」することができ、社内からの攻撃を防御できます。監査プロセスを有効化すると、システムを攻撃し、破壊するには、複数の攻撃者が何らかの協力を行い、攻撃を仕掛けなければならなくなります。セキュリティーのレベルを上げるには、監査の回数を増やすかシステムに組み込んだ監査レベルを上げます。システムはすべてのアクセスを定期的に記録します後でフォレンジックが攻撃の程度と潜在的なセキュリティー侵害を把握できるよう、このようなログは合理的な期間保管する必要があります。

最新のセキュリティー環境を維持する

重要ポイント:

- 認証、権限の設定、監査、管理、暗号化と復号化、鍵の管理、一貫性のチェックなど、セキュリティーにはさまざまな側面がある。
- さまざまなテクノロジーとプロセスを組み合わせることで、環境をセキュアに保つことができる。
- データ・センター、クラウド、その他の制御された環境で稼働するシステムに比べて、はるかに制御されない条件でデバイスは稼働している。

IoT アプリケーションに関するセキュアな環境を構築し、維持することは、企業のコンピューティング・システムのすべてにとってセキュアなコンピューティング環境を実現することと一致します。認証、権限の設定 (アクセス制御)、監査、管理に関する要素が適用されます。これまでにない課題として、ユーザー、グループ、モバイル・デバイス、エンドポイントを処理する際に、デバイス数が過去とは桁違いの数に増大していることが挙げられます。エンドポイントは、企業内で働いている人間と関連しています。IoT の世界では、多くのエンドポイントについて考慮しなくてはならず、セキュリティーに関する幅広い機能が関連しています。

ユーザーとデバイスの登録、認証、アクセス制御だけでなく、認証、通信、データの保存を目的として、暗号化と復号化を行うメカニズムを設定するために使用する鍵の管理も行わなくてはなりません。IoT デバイスにも最終的には影響を及ぼす鍵の管理を使用すると、ソースからターゲットまで情報がセキュア

な環境で流れ、ネットワーク上とストレージ上で情報をセキュアに管理できます。IoT デバイス内で Trusted Platform Module (TPM) に事前に組み込んだ秘密鍵のデータを使用すると、鍵の管理を行うことができます。TPM デバイスの仕様については、これまで Trusted Computing Group (TCG)[27] が開発と強化を実施しています。

IBM Identity Management[28] ソリューションの機能 (IBM Bluemix[29] 上で稼働する IBM Identity を使用することを含む) を活用すると、開発中の IoT ソリューションと関連するユーザーとグループを定義するために最新のセキュリティー環境を維持することができます。デバイスの登録とライフサイクルの管理を行う IBM IoT Foundation[30] による追加機能は、デバイスとデバイスを使用するアプリケーションがお互いに通信するためのセキュアな環境を維持するための基本機能となります。この機能には、既に説明したセキュアなデバイスのレジストリー機能が含まれます。

IBM Security Key Lifecycle Manager[31] の機能を使用すると、暗号鍵の管理と配布を行うために必要な一連のコア機能を分析することができます。本オファリングは主に金融サービス業界で使用されているものの、鍵の管理を提供する本機能をデバイス・レベルの暗号化サービスに適用できます。OASIS Key Management Interoperability Protocol (KMIP)[32] に基づく鍵の管理機能は、分散ネットワーク環境で稼働する一連のデバイスに拡張できます。このような環境で稼働した最初のデバイスは、IBM が暗号化したテープ・ドライブでした。KMIP プロトコルは非常に軽量なプロトコルとして設計されています。KMIP プロトコルを使用すると、さまざまなネットワーク・デバイスとコンピューティング・デバイスを実装し、サポートすることができます。

ID と暗号鍵情の報の管理だけでなく、環境に含まれるすべてのデバイスを管理し、維持しなければなりません。すべてのセキュリティー・パッチとフィックスを適用するために、デバイス、ゲートウェイ、ルーター、その他のインフラを定期的にアップデートする必要があります。以前は、ファームウェアやソフトウェアのアップグレード、フィックス、移行を行う際には、デバイス、ゲートウェイ、ルーターを直接操作するために、人間による多大な関与が必要となっていました。今後は、デバイスの数が増え、アップデートの頻度が高まることが予想されるため、人間による積極的な関与は自動化された無線によるアップデート処理へと移行します。人間の関与は提供される各アップデートの処理と対応ではなく、例外処理に限られます。このため、一連の関連するゲートウェイ、ルーター、デバイスに関するアップデート処理の状態と進捗をさらに詳細に監視し、報告できるようになります。

ネットワークにつながるデバイスの価格が下がると、すべてのデバイスを最新に保ち、あらゆる攻撃から防御するだけのコストに見合わなくなります。この状況における最もコスト効果の高い管理手法は、デバイスを管理の対象から外し、デバイスから提供される情報を無視・除外するためにゲートウェイを設定することです。さらに、デバイス・メーカーは「無効化機能」を組み込むことを検討する必要があります。デバイスは障害に強い最低限の機能を提供するネットワークにつながらないモードで稼働を続けるものの、ネットワークと通信しなくなるため、デバイスそのものと環境に含まれる他のコンポーネントを保護することができます。デバイスから提供されるセンサー情報は失われるものの、パッチとフィックスを適用できないデバイスが引き起こす可能性のある攻撃から環境を保護することができるため、脆弱性を排除できます。

本書で既に説明したとおり、最新のセキュリティー環境を管理するには、デバイス・メーカーが、ネットワークにつながった他のコンピューティング・デバイスとに対応するだけでなく、セキュリティーのインシデント・レポートにも積極的に対応する必要があります。

コンピューティング環境のその他のコンポーネントと同様に、環境全体でログイン情報とパスワード情報を積極的に管理し、情報の鮮度を維持するための施策を実施する必要があります。IoT デバイスに組み込まれる可能性のあるこのような情報を積極的に管理することも必要です。鍵のライフサイクルの管理、ID の管理、無線によるアップデート、デバイスの登録、ライフサイクルの管理などが関係します。ネットワークにつながるデバイスに関しては、デバイス・メーカー、デバイスの購入者、オーナー、管理者、ユーザーなどさまざまなステークホルダーが存在します。ネットワーク通信事業者やデバイスのサービスとサポートを行う事業者のようなサード・パーティーも、考慮すべきステークホルダーとなります。

信頼性の高いメンテナンスのエコシステムを構築する

重要ポイント:

- セキュアな環境を設定し、維持するための既存のガイドラインに従う。
- 包括的なインシデント対応プロセスを開発する。

セキュアな IoT システムを運用するには、環境を運用する責任者がセキュアで適切なアクティビティーを実施しなければなりません。詳細情報については、サプライ・チェーン (環境を運用するために使用するサプライヤーを含む) のセキュア化に関するセクションを読んでください。システムのセキュリティーと一貫性を維持するために、適切なメンテナンスの手続きに従う必要があります。

セキュリティーに関連するインシデントの報告を処理するために、インシデント対応プロセスを明確に定義し、通知する必要があります。本プロセスを通じて、インシデントを発見し、検証した時点で、脆弱性を解決するために体系的な是正策を提供しなければなりません。また、本プロセスにより、脆弱性によって影響を受ける他のコンポーネントの責任者が是正策を実行できるよう、情報を提供する必要があります。コンポーネントの再利用とソリューションの開発が複雑に同時進行するなか、インシデント対応プロセスに基づいて、影響を受ける可能性のあるすべてのコンポーネントを迅速に特定し、是正する必要があります。

IoT システム全体の物理セキュリティーが今後も課題となります。IoT デバイスは、その特性ゆえに条件が厳しく困難な運用条件で稼働しなければならず、物理的な要素の影響を受け、さまざまな攻撃を受けます。このようなデバイスは脅威にさらされるなか稼働し、迅速に他の場所に移動し、過酷な条件にさらされることになります。ハイテク電子機器が大規模に実装されるという点ではこれは新たな状況ですが、これまでと全く異なる状況ではありません。軍事アプリケーション、車載システム、航空電子機器、センサーに加え、モバイル・デバイスをセキュア化するためにこれまで開発されたあらゆる機能が先陣を切って、準拠すべき適切なプラクティスを示しています。

まとめ

Internet of Things のテクノロジーに関するテクノロジーは、他の大規模なコンピューティング・インフラのセキュリティーと異なる点もあれば、似ている点もあります。認証 (デバイス、システム、アプリケーション、ユーザーの認証)、権限の設定、監査、管理、暗号化と復号化、データの一貫性、鍵の管理などの点で、解決すべき問題と問題を解決する手法は似ています。しかし、コンピューティング・デバイスの種類と機能が広がり、制御の困難なグローバル環境で運用され、セキュア化すべき攻撃面が広がると、新たな課題が発生します。

IoT のセキュリティーで対応しなければならないいくつかの課題があります。しかし、長年の研究開発により発展を遂げた手法とテクノロジーを適用することでこのような課題に対応し、必要に応じて Internet of Things がもたらす独自の要件にも対応することができるのです。

協力者

「Internet of Things (IoT) のセキュリティーに関する IBM の見解」を作成するにあたって、IBM の各部門の担当者から多大な協力を得ました。本書の発行に協力した以下の担当者に謝意を示します。

Timothy Hahn	IBM Analytics (IoT 担当)、ディスティングイッシュト・エンジニア
Sky Matthews	IBM Analytics (IoT 担当)、CTO
Lisa Wood	IBM Analytics (IoT 担当)、ディレクター
John Cohn	IBM Corporate Technical Strategy、フェロー
Shmulik Regev	IBM Security、シニア・テクニカル・スタッフ
Jim Fletcher	IBM Analytics (IoT 担当)、ディスティングイッシュト・エンジニア
Eric Libow	IBM Analytics (IoT 担当)、ディスティングイッシュト・エンジニア
Chris Poulin	IBM X-Force、リサーチ・ストラテジスト
大西 克美	IBM Security、ディスティングイッシュト・エンジニア

詳細情報

IBM Internet of Things に関する詳細情報を確認するには、http://www.ibm.com/software/info/internet-of-things/ にアクセスしてください。

出典

[1] IDC, ”Worldwide and Regional Internet of Things 2014-2020 Forecast Update by Technology Split,” Doc #252330, Publish date:Nov 2014. http://www.idc.com/getdoc.jsp?containerId=252330

[2] Storm, Darlene, “ Hackers exploit SCADA holes to take full control of critical infrastructure,” Publish date: Jan 2014.Computerworld. http://www.computerworld.com/article/2475789/cybercrime-hacking/hackers-exploit-scada-holes-to-take-full-control-of-critical-infrastructure.html

[3] IBM IBV Driving Security. http://www-935.ibm.com/services/us/gbs/thoughtleadership/automotivesecurity/

[4] Open Web Application Security Project (OWASP) Top 10 IoT Issues. http://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[5] IIC Reference Architecture. http://www.iiconsortium.org/ and IIC Security Working Group Reference Guide – http://www.iiconsortium.org/wc-security.htm

[6] Allseen Alliance. https://allseenalliance.org/

[7] BuildItSecure.Ly. http://builditsecure.ly

[8] X-Force の研究開発部門。“IBM X-Force Threat Intelligence Quarterly 4Q 2014,” Doc # WGL03062USEN, Publish Date:Nov 2014. http://www.ibm.com/security/xforce/downloads.html

[9] IBM Secure Engineering Framework. http://www.redbooks.ibm.com/abstracts/redp4641.html

[10,19] IBM Security AppScan®. http://www.ibm.com/software/products/en/appscan-source

[11] 脅威のモデリング。http://en.wikipedia.org/wiki/Threat_model

[12] IBM Rational® Rhapsody®. http://www.ibm.com/software/products/en/ratirhapfami

[13] X-Force による脆弱性の調査データベース。https://xforce.iss.net/

[14] National Vulnerability Database. http://nvd.nist.gov/

[15] IBM Rational Team Concert. http://www.ibm.com/software/products/en/rtc

[16] IBM Infosphere Guardium Data Security. http://www.ibm.com/software/data/guardium/

[17] IBM Infosphere Optim Data Privacy. http://www.ibm.com/software/data/optim/

[18] IBM Rational® Software Analyzer.http://www.ibm.com/software/products/en/ratisoftanalfami

[20] Common Criteria. http://www.commoncriteriaportal.org

[21] US-Cert. http://www.us-cert.gov/

[22] Common Vulnerability Exposures. http://cve.mitre.org/

[23] Open Group – Supply Chain Security. http://www.opengroup.org/news/press/open-group-releases-global-technology-supply-chain-security-standard

[24] IBM Unified Endpoint Management. http://www.ibm.com/software/tivoli/unified-endpoint-management/

[25] IBM Security QRadar® SIEM. http://www.ibm.com/software/products/en/qradar-siem

[26] IBM Operations™ Analytics – Log Analysis. http://www.ibm.com/software/products/en/ibm-operations-analytics---log-analysis

[27] Trusted Computing Group. http://www.trustedcomputinggroup.org/

[28] IBM Security Identity and Access Manager. http://www.ibm.com/software/products/en/identity-access-manager

[29] IBM Bluemix. http://www.bluemix.net

[30] IBM IoT Foundation. http://internetofthings.ibmcloud.com

[31] IBM Security Key Lifecycle Manager. http://www.ibm.com/software/products/en/key-lifecycle-manager

[32] OASIS Key Management Interoperability Protocal (KMIP). http://www.oasis-open.org/committees/kmip/

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
2015 年 4 月

RAW14382-JPJA-00