IoT製品の
セキュリティ保証
レベルを評価

Empowering Trust®

概要

つい最近まで、情報やシステムのほとんどはデジタル化されていませんでした。1989年に遡ってみると、ワールドワイドウェブが発明されたばかりで、自宅からインターネットに実際にアクセスできる人はいませんでした。写真を撮るには、まだフィルムが使われており、デジタル写真は1994年にApple社が世界初のデジタルカメラを発売し、2000年にCanon社のIXUSが登場するまでは、一般に普及していませんでした。1990年代初頭には、大半の人々が携帯電話を持たず、たとえ持っていたとしても、スーツケースに入れて持ち運ばなければならないほど、大きなサイズでした。

そのため、当時の悪意のあるソフトウェアといえば主に、学術研究プロジェクトで作成されたものや、悪戯で作成されたプログラムでしかありませんでした。このようなプログラムでは、家族写真を無断で暗号化し、これを元に戻すために金銭を要求することはありませんでした。また、住居内で音声を無断で録音し、これを基に脅迫したり、ヒーターやドアロックを遠隔操作したり、住居内のデバイスを無断で使用して、世界中のインターネットトラフィックを妨害したりすることもありませんでした。

私たちのデータやシステムの大半がまだアナログであった頃は、このような悪意ある行動を実行することは不可能でした。1989年には、安全性とセキュリティは実質的に同義語と見なされ、いずれも物理的な安全のことを意味していました。

それからわずか30年後の今日では、データの管理や、時には生活そのものが、私たちを取り巻くコンピューターシステムなしでは不可能になっています。物理的な安全だけでなく、データ、預金、財産の安全を確保するには、これらにアクセスし制御するシステム内のソフトウェアのセキュリティを常に考慮する必要があります。

今日では、まさにあらゆるものにソフトウェアが使用されています。

特に、ワールドワイドウェブによってインターネットの使用が急速に普及した1990年代中頃からこれまで、セキュリティは、汎用コンピューターシステムの文脈で理解されてきました。しかしながら、私たちは今や、コネクテッドシステム、つまりIoTの進化の新しい段階に直面しています。このため、セキュリティに関する新しい懸念事項や要件が発生しています。

本書では、IoTの定義について説明するほか、汎用コンピューティングデバイスのセキュリティと比べて、IoTのセキュリティへの対処が困難である理由について取り上げます。さらに、このホワイトペーパーでは、IoTセキュリティに対処するための推奨方法についても詳しく紹介致します。これには、関連するリスクを理解し、IoTシステムに実装されているセキュリティのレーティングを意思決定者への情報提供のために使用し、お客様の製品に適したレーティングを判断することが含まれます。

IoTの定義

IoTとは「モノのインターネット」の略語ですが、IoTの定義に該当するもの、該当しないものを明確に判断することは困難です。スマートデバイスの多くはインターネットに直接接続されていません。ハブなどのプロキシを使用したり、BluetoothやZigbeeワイヤレスを介したローカル接続のみを使用したりします。IoTシステムの大半には、コンパニオンアプリやクラウドサービスが付属しており、デバイス自体の動作を補完したり、その動作に実質的に不可欠な役割を果たしたりします。

本書では、IoTという用語は、スイッチドネットワークまたはワイヤレスネットワーク経由で接続される、1つ以上の物理コンポーネントを備えた機能の集合体を指すものとして考えます。そのため、この範囲にはシステムのすべてのコンポーネントが含まれます。これには、物理コンポーネント、さまざまなコンピューティング要素に含まれる常駐ソフトウェア、およびモバイルアプリやクラウドインスタンスに配置されたソフトウェアなどがあります。

このように捉えることで、通常はインターネットに一切接続されないような、Bluetoothスピーカーやドアロックなどのデバイスも定義に含まれます。これは重要な定義です。ドアロックのセキュリティは明らかに重要ですが、スピーカーのセキュリティはそれほど重視されないでしょう。

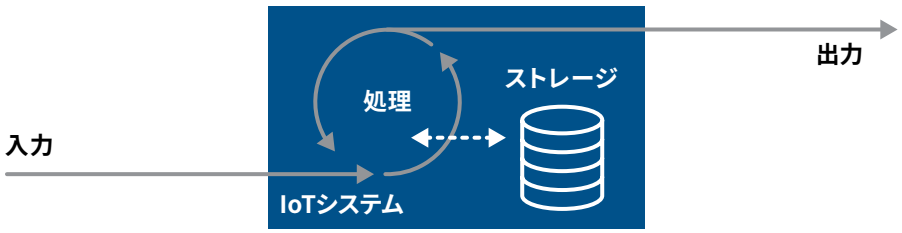
これら2つのデバイスは、同じワイヤレステクノロジーを使用して接続されるにもかかわらず、セキュリティについては異なる見方が必要になるのはなぜでしょうか？すべてのデバイスの種類に適用される脅威を判断するには、どのようなルールに基づくことができるでしょうか？また、このような脅威を考慮すると、デバイスに必要なセキュリティレベルとは、どのようなものになるのでしょうか？

IoTのリスク

IoTシステムで必要とされるセキュリティを評価する際には、このシステムが直面するリスク、発生し得る問題、さらに、悪意のある者がこのシステムに不正アクセスしようとする理由を理解することが重要です。基本的には、これは機会と価値の問題になります。システムにどの程度容易にアクセスできるか、悪意のある者が不正アクセスまたはセキュリティ侵害を行うことで、どの程度の価値を得るか（つまり、攻撃の標的となる資産は何か）ということが重要になります。

最も基本的なレベルでは、IoTをはじめとする、すべてのコンピューティングシステムは、以下の図に示すように入力、出力、ストレージ、処理からなるシステムとして捉えることができます。

多くの場合は、入力、つまりユーザーデータに重点が置かれます。これは、IoTシステムが攻撃される決定的な要因であるためです。



しかし、デバイスのストレージ、処理能力、出力帯域幅、データ、ネットワーク機能、設置場所など、あらゆる側面が攻撃者にとって有益な資産となる可能性があります。たとえば、自宅から外部に向けられたカメラには、価値の低いデータが保存されていると考えられるかもしれません。しかし、このカメラが不正アクセスされた場合には、かつてない規模のボットネットに組み込まれたり、あなたが家から外出するのを犯罪者が確認したり、犯罪者が待ち伏せしているのを隠す為や、通りを歩く他者のプライバシーを侵害したり、より大規模なネットワークでの複数の攻撃の第1段階として攻撃されたりする可能性もあります。以下の表には、攻撃者が標的とする可能性のあるIoTシステムの資産の例と、これらがどのように、何の目的で標的とされるかがまとめられています。

以下の表には、攻撃者が標的とする可能性のあるIoTシステムの資産の例と、これらがどのように、何の目的で標的とされるかがまとめられています。

標的となる資産	攻撃の種類	攻撃の目標/目的の例
保存またはアクセスされるデータ	データの不正入手	収益化/脅迫
	データの改ざん	ランサムウェア
	システム規模のデータまたはコードの抽出	コードのリバースエンジニアリング
処理能力	処理リソースの使用	暗号通貨マイニング パスワードクラッキング
システム処理/機能	処理の無効化	ランサムウェア/脅迫
	処理の変更	セキュリティカメラの映像のループ再生
	処理の確認	在宅中かどうかの判断
	特権操作の悪用	ロックされたドアを開ける
ネットワーク処理/機能	帯域幅の使用	DDoS攻撃
	信頼されるネットワーク機能の悪用	DNSの変更
ネットワークの場所	他のネットワークまたはシステムへのアクセス	他のシステムを攻撃する
	ネットワークトラフィックの取得	他のシステムからデータを不正に入手する

攻撃の種類は多岐にわたるため、残念ながら、特定の種類のIoTデバイスまたはシステムが攻撃者にとって価値があるかどうかを判断することは容易ではありません。この価値は多くの場合、システムの種類ではなく、システムが導入および使用される方法によって決まります。

言い換えれば、IoTシステムのセキュリティでは、システムの種類よりも、その設置場所や、システムがアクセスするデータやリソースが重要になります。システムの「種類」は、データやリソースを判断するためには有用ですが、メインの要素ではありません。スマートスピーカーがインターネットに直接接続されており、内蔵カメラで住居内のビューを提供でき、大量の処理能力と帯域幅リソースを備えている場合は、接続された携帯電話から音楽を再生するだけのBluetoothスピーカーよりも、標的になりやすいでしょう。

IoTセキュリティの問題

このようなIoTセキュリティの多くの側面（脅威の種類やリスク）を考慮すると、これらのシステムでセキュリティ対策を講じることの必要性が理解できるでしょう。しかし、これは必ずしもシンプルなタスクではありません。IoTシステムは多くの場合、さまざまな処理要素で構成されています。このシステムでは、さまざまなコードがあらゆる場所で実行され、さまざまな物理的および論理的なセキュリティが必要になります。システムの「設置場所」が重要になる場合、複数の「場所」に設定されているデバイスでは、さらに状況が複雑になります。

この複雑さは、セキュリティを困難なものにします。

IoTセキュリティの根本的な問題は、多くの場合、セキュリティの実装には大きなコストがかからないものの、コストを伴わずに行うことはできないという点です。優れたセキュリティは、優れた設計があってこそ可能になります。つまり、製品開発の初期段階で、より多くの時間と知識が必要になることを意味します。設計が複雑になるほど、関与する要素やコードの種類が増え、これらすべてを安全なシステムとして統合することが困難になります。

複雑なシステムを維持するにも負担が伴います。時間の経過とともに、パッチやセキュリティアップデートを適用して、システムを最新の状態に維持するには、人員が必要になります。この人員は、現在生産中の製品においてセキュリティが何を意味するかを理解し、セキュリティ調査の最新情報を常にチェックして、将来のセキュリティ要件も把握しながら、この製品の初期収益が達成された後も、製品のセキュリティを維持するために取り組む必要があります。システムが複雑になるにつれて、あらゆるセキュリティ問題に対処することが困難になり、より多くの人員が必要になります。

このようなスキルは世界中で求められており、このような人員を雇うには、多くの場合、高いコストがかかります。したがって、優れた設計と継続的なメンテナンスを行うには、追加の人員と時間を要するため、明らかにコストがかかります。同様に重要な点として、セキュリティ機能の実際の試験や検証にもコストがかかります。「簡易」セキュリティ試験は低コストで実行できる場合もありますが、この場合、試験対象のセキュリティプロパティに対し、低いレベルの保証しか提供できません。より確かな保証を得るためには、より詳細な試験を実行する必要があり、これにはさらに時間とコストがかかります。
このコストは、設計やメンテナンスのコストに上乗せされるため、合計すると、IoTシステムですでに切り詰められているマージンがさらに削減されるか、販売価格が上昇することになります。

このため、根本的にはセキュリティはビジネス上の問題であると言えます。

IoTセキュリティのレーティング

このセキュリティ関連コストには、どのように対処するべきでしょうか？セキュリティ関連コストが、デバイスの総コストで一定の最大限の割合を占める場合（そうでなければ、消費者が他の製品を購入する）、低コストのデバイスでは、より低いレベルのセキュリティで対処することが必要になると考えるのが妥当でしょう。だからといって、どのようなデバイスでも許容される基本的なレベルのセキュリティを設定する必要がないというわけではありません。ただし、この許容レベルを判断するには、デバイスの種類や実装方法を考慮することになります。

しかし、コストのみの観点からセキュリティを考えることはできません。システムが攻撃される可能性は、システムの種類よりも、その設置場所によって左右されるということはすでに説明しました。幸いにも、多くの場合（残念ながら常にとは言えませんが）、システムのアクセスしやすさと、消費者にとってのコストには、相関関係があります。たとえば、IoT電球では多くの場合、Zigbeeなどの短距離ワイヤレス接続が使用されるため、インターネットからは直接アクセスできません。したがって、このようなシステムによって生じるリスクは小さくなります。このようなシステムでは、ユーザーのLANに直接アクセスすることができず、攻撃者はインターネットを介して直接アクセスすることはできません。また、機密データは保存されておらず、処理能力や帯域幅リソースも非常に限られています。

攻撃者は、在宅中であるかを判断するために照明を使用する可能性があるため、これらの製品でもセキュリティは重要になります。ただし、これらのデバイスは多くの場合、ハブを介してアクセスまたはグループ化されるため、追加のセキュリティ機能が提供されます。最後に、これらすべての接続がルーターやファイアウォールで保護されていれば、内部ネットワークに追加のセキュリティ対策が提供されることも期待できます。

したがって、照明には高いレベルのセキュリティ保証は必要ないかもしれませんが、照明が接続されるハブには必要になるでしょう。ルーターやファイアウォールには、最高レベルのセキュリティが必要になります。また、ネットワークの他のセキュリティ機能にもかかわらず、ファイアウォール経由でインターネットに直接アクセスできる他のデバイスも同様です。

このように考えると、自宅、オフィス、その他の環境で必要とされるセキュリティは、階層別に捉えることができます。この階層は、システム自体のアクセスしやすさと価値によって決定されます。以下の図では、このような階層を示しています。

アクセスしにくく、リソースやデータに価値がそれほどないシステムには、低いレベルのセキュリティ、つまり“低いレベルのセキュリティ保証”で対応できます。これに対し、ネットワークの

デバイスに必要となるセキュリティ保証のレベル

高レベルのセキュリティ保証
インターネットから直接アクセス可能なデバイス

インターネット境界またはセキュリティデバイス

製品例
- カメラ
- ベビーモニター/ペットモニター
- ルーター、モデム
- インターネットに接続されたハブ

中～高レベルのセキュリティ保証
「スマートな」安全関連の機能を備えたデバイス（インターネットに直接接続されるかを問わない）

インターネットにアクセスするデバイス

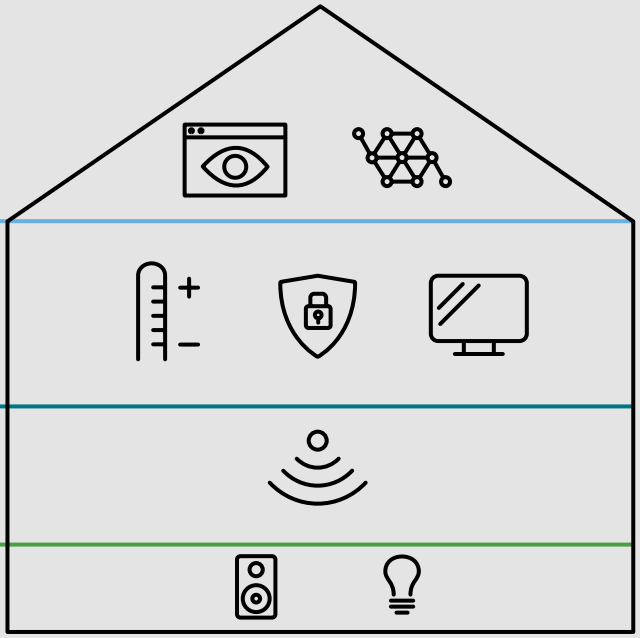
- ヒーター
- ドアロック
- テレビ
- 音声制御スピーカー

低～中レベルのセキュリティ保証
ネットワークをLANにブリッジするが、インターネットには直接接続されないデバイス

- ローカルハブ
- ブリッジ
- アクセスポイント

低レベルのセキュリティ保証
LANに直接接続されないデバイス

- Bluetoothスピーカー
- 照明（Wi-Fi非対応）



周辺にあるデバイスでは、高いレベルのセキュリティ保証が必要になります。もちろん、これらの許容セキュリティレベルは概して、IoTシステムが導入・使用される方法によって決定されます。ただし、これは多くの場合、製造者にとって販売前に把握することは困難です。顧客の中には、Wi-Fi照明を使用して、インターネットに直接接続する人もいるでしょう。この場合には、リスクが高くなるため、高いレベルのセキュリティが必要になります。

しかし、一般的ないくつかの質問をすることで、システムによって生じるリスクと、これによって必要になるセキュリティレベルを判断することができます。右の表には、これらの質問と、低～高レベルのうち、どのセキュリティ保証が推奨されるかが記載されています。システムに該当する最も高いレベルの項目が、推奨されるレベルになります。たとえば、Bluetoothドアロックについて考えてみましょう。これは、インターネット非対応のルーティング可能な接続経由でのみアクセスできます（この点では、低いレベルの保証が推奨されます）。しかし、物理的な安全およびセキュリティに関連する機能を提供するため、高いレベルのセキュリティ保証が適切であると考えられます。

製造者やベンダーは、この表を使用することで、各自の製品で最小限のレベルのセキュリティ保証が何であるかを容易に確認できます。高いレベルが常に推奨されるわけではありません。レベルは高い方が安全になり、市場で製品を差別化するために役立ちます。この表は、製品に適した最小限のレベルを判断するための初期のガイドラインとしてのみ使用してください。

また、時間の経過とともにIoT業界のセキュリティの全体的な成熟度が向上するにつれて、これらの推奨事項や、各レベルの要件および保証内容が変化することが考えられます。これは、Australasian New Car Assessment Program（ANCAP）の車両安全規格に、時間とともに車両の安全性が向上するにつれて、追加の安全性項目が含まれたことと似ています。

どのセキュリティレベルが適切かについてのガイドラインが確認できたら、IoTシステムがどのセキュリティレベルを実際に達成したか、その評価方法、システムの導入においてどの様な意味合いがあるかについて、IoTシステムの購入者に示す方法も必要になります。こうすることで、インターネットに接続したり、機密データの保管や処理に使用したり、重要な他のシステムに接続したりするなど、高いリスクを伴う方法でシステムを導入することを検討している場合には、ユーザーは、価格が高くても、セキュリティレーティングが高いシステムを選択できるようになります。

基準値となるセキュリティを強化し、ニーズに適合したセキュリティオプションを選択できるようにすることが、セキュリティレーティングシステムの役割です。

システムの範囲設定のための質問	推奨される最小限のセキュリティ保証レベル
システムに、HVACコントロール、ネットワーク、物理的なセキュリティなど、安全性またはセキュリティに関連する機能が実装されているか？	高
システムは、インターネットから直接接続することが必要であるか？または、システムに直接接続を構成できるか？	高
システムは、撮影したビデオや録音、支払い詳細などの機密データにアクセスできるか？	中～高
システム（他のシステムを接続するハブを含む）では、インターネットへの直接接続（インターネットからの接続ではなく、インターネットへの接続）が可能か？	中～高
システムは、顧客のLANに対して、さまざまなネットワーク間におけるハブまたはブリッジとして機能しているが、インターネットアクセスは直接提供していないか？	低～中
システムは、帯域幅が低く、インターネット非対応のルーティング可能なネットワーク（Zigbeeなど）またはBluetoothオーディオ経由でのみアクセスできるか？	低

セキュリティ強化への道

システムのセキュリティを評価することは、安全/危険という二元的な判断を下すだけではなく、IoTセキュリティの投資と成長を促進するために役立つという意義もあります。今後発売される製品のすべてが、セキュリティの最高規格に自動的に準拠するようになると期待するのは非現実的です。実際、このような最高レベルの規格を満たすには、設計の完全なやり直しや、製品の設計、構築、出荷、メンテナンスの慣習を大幅に変革することが必要になる可能性があります。

これは、合格/失格だけを判断するセキュリティプログラムのジレンマと言えます。実際に望ましい最終的なレベルではないことを理解した上で、今日の大半の製品で達成可能な最小限のレベルに、要件を引き下げるべきでしょうか？それとも、我々が理想的であると考えるレベルを基準として設定し、業界が追いつくのを待つべきでしょうか？

基準が低すぎる場合には、少なくとも最小限の要件を検証することはできますが、企業がこれらの要件を上回り、顧客への配慮を示すことへの動機付けや認識はなくなります。基準が高すぎる場合には、これらの要件を満たす製品が非常に安全であることに確証を持てるようにはなるが、このレベルを満たす製品がなく、業界全体がこのレベルを達成する意欲をなくしてしまっては意味がありません。

いずれの場合も、さまざまな製品がセキュリティ対策をどのように適用および実装しているかについて、消費者に有用な情報を提供できません。

レーティングでIoTセキュリティに対処する – ビジネス上のソリューション

IoTシステムのセキュリティ成熟度のレベルを向上させるには、IoTの設計と導入を促進するビジネス上の側面だけでなく、さまざまな製品の種類や用途に必要な保証レベルを決定する基準となるリスクについても理解する必要があります。そのリスクは、多数の要素で構成されています。これには、システムがアクセスできるデータの種類、システムが備えている帯域幅と処理能力の程度、アクセスまたは管理する他のシステムの種類、IoTシステムのアクセスやセキュリティ侵害がどの程度容易にできるか、などが含まれます。

IoTセキュリティは、安全/危険という二元的な判断によって客観的に対処することが理想的ですが、これは不可能であり、業界による取り組みを公正に示すことはできません。最高レベルのセキュリティは意図せずに達成できるものではありません。安全な製品設計とセキュリティ試験はいずれも、時間とコストがかかるものです。これにより、製品のビジネスの機会が影響を受け、次世代デバイスの保護に投資する能力が損なわれる可能性もあります。

IoTセキュリティの最低限のレベルを必須とする法規範が導入され、さまざまな業界団体が独自のIoTセキュリティ要件を作成しようとしている中で、コンプライアンスを達成し、市場で競争しながら、ビジネス的に採算がとれる製品群を維持するには、どうするべきでしょうか？

この質問に対して、すべてのシステムで発売当初から最高レベルのセキュリティが提供されることは期待できません。これは、ビジネス上、非現実的なアプローチです。その代わり、IoTセキュリティに段階的なアプローチを採用し、すべてのデバイスで最小限の基準を奨励します。より大きなリスクを伴うシステムでは、セキュリティレベルを引き上げます。

時間の経過とともに、セキュリティのニーズと設計の両方に関する理解が市場で進むにつれて、これらが適用されるレベルとシステムを引き上げることができます。このような認識は、安全なシステムを提供するビジネス上の必要性を増すために有効です。現在では、顧客はIoTセキュリティを完全に諦めているか、セキュリティが内蔵されていると思い込んでいるかのどちらかです。この問題を解決するため、セキュリティを消費者に分かりやすく示す必要があります。しかしながら、複数のレベルを設定しない場合には、一般に達成可能な最低レベルを許容するか、セキュリティ対策にあまりにも急激な変革を求めるセキュリティ規格の採用を阻止するかの、いずれかの選択肢しかなくなります。

セキュリティを強化するには、業界に対抗するのではなく、業界と協力することが必要です。単に問題を列挙するのではなく、ソリューションを提供し、セキュリティのビジネス上の側面にも考慮することが必要です。このために、より多くの時間と労力がセキュリティ対策に費やされている製品がどれであるかを、消費者に容易に示すことができる必要があります。これには、レーティング方式が有効です。

お客様やその製品には、どのレーティングが適しているでしょうか？この質問に回答するには、お客様の市場、顧客、テクノロジーが使用される方法を理解する必要があります。本書でアクセスや資産に関する情報を使って説明した段階的なアプローチは、それを簡単に判断できます。

詳細については、ULまで電子メール（IMSecurity@ul.com）でお問い合わせいただくか、IMS.UL.com/IoT-Security-Ratingにアクセスしてください。

ULサイバーセキュリティ

ULのIoTセキュリティレーティングが、進化し続けるUL IoTセキュリティソリューションのリストに追加されます。これには、UL Supplier Cyber Trust Level、UL Cybersecurity Assurance Program、IEC 62443、およびその他のトレーニング、アドバイザリーサービスが含まれ、エコシステム全体のセキュリティ評価、サプライチェーンの安全性と品質、市場のセキュリティ規制に対応しています。

ULの概要

ULは、科学の活用によって安全、セキュリティ、サステナビリティ（持続可能性）における課題を解決し、よりよい世界の創造に寄与します。そして、先進的製品/技術の安全な導入を実現することで、信頼を高めます。ULのスタッフは世界をより安全な場所にするという情熱を共有しています。第三者調査から規格開発、試験、認証、分析/デジタルソリューションの提供まで、ULは業務を通じて、より健全なグローバル社会の構築を目指します。ULに対する信頼が、企業、メーカー、政府当局、規制機関、人々のスマートな決断を支えます。

詳細は、UL.comをご参照ください。

UL.com

2004UL_V1.0