

IoT向けのセキュリティ—— 持続可能性をグローバルに 実現する

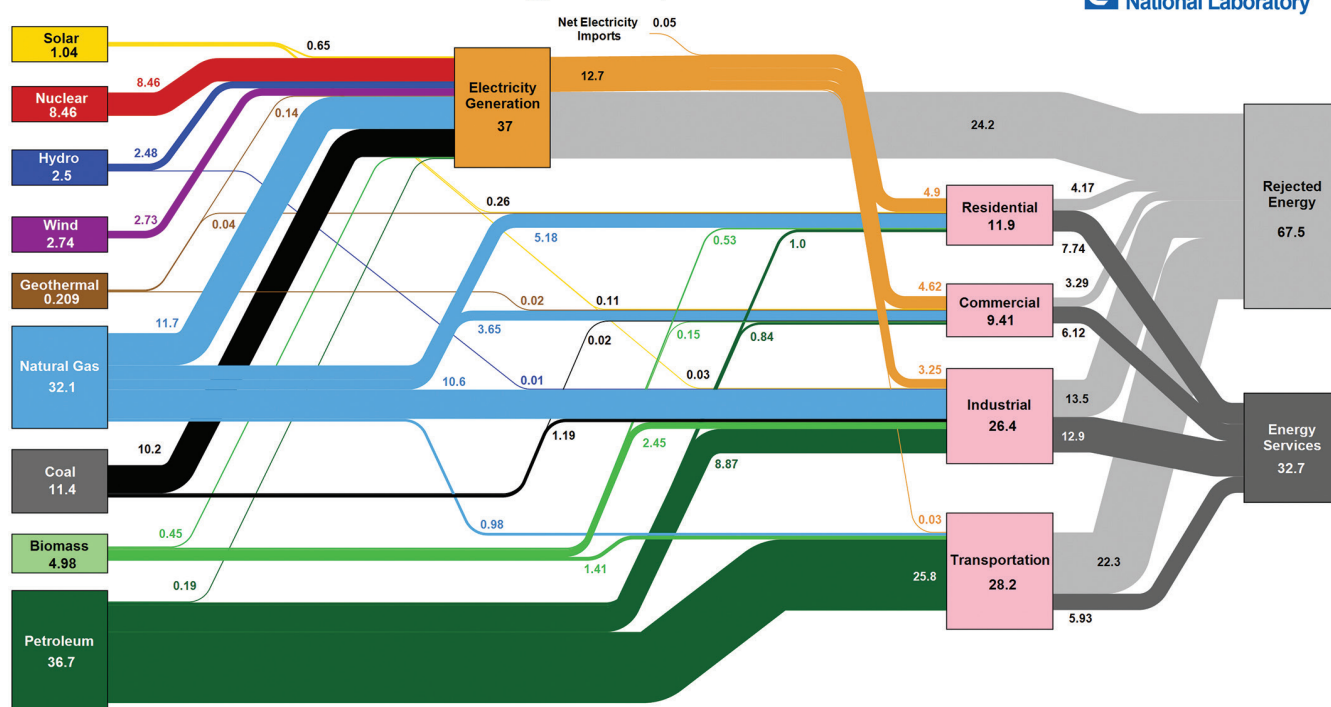
著者：Erik Halthen、プロダクト・マーケティング・マネージャ

IoT向けのセキュリティについては、次の大きな波が押し寄せようとしています。昨今は、最新かつ最高のガジェットを手に入れたとしても、すぐに次のバージョンがリリースされるという状況にあります。それとは異なり、インフラについては、続々と登場する新技術を即座に導入するというわけにはいきません。それには、多大なコストがかかるからです。とはいえ、新たな技術が登場しても何も変化は生じないというわけではありません。例えば、デジタル・トランスフォーメーションにおいては、IoT (Internet of Things) が重要な役割を果たします。インフラにセンサーを組み込むことにより、物理的な移動を抑え、その代わりにデータを移動させるといった具合です。このような仕組みは、より持続可能性の高い社会の構築に大きく貢献します。

今日、私たちはエネルギーについて危機的な状況に直面しています。この問題に対処するには、二酸化炭素の排出量を削減しなければなりません。それにより、社会の持続可能性が高まることとなります。米国のローレンス・リバモア国立研究所によれば、2019年には67.5クワッドものエネルギーが浪費されたといえます¹ (1クワッドのエネルギーは 1.055×10^{18} ジュールに相当)。これは、生成された全エネルギーのうち半分以上が、意味のある使い方をされたわけではなく、熱として消費されたということを示しています。つまり、大量に生成したエネルギーを利用する能力に重大な問題があるということです。IoTは、データを蓄積／活用してエネルギー効率に関する課題に対処する手段になり得ます。

Estimated U.S. Energy Consumption in 2019: 100.2 Quads

Lawrence Livermore
National Laboratory



Source: LLNL March, 2020. Data is based on DOE/EIA MER (2019). If this information or a reproduction of it is used, credit must be given to the Lawrence Livermore National Laboratory and the Department of Energy, under whose auspices the work was performed. Distributed electricity represents only retail electricity sales and does not include self-generation. EIA reports consumption of renewable resources (i.e., hydro, wind, geothermal and solar) for electricity in BTU-equivalent values by assuming a typical fossil fuel plant heat rate. The efficiency of electricity production is calculated as the total retail electricity delivered divided by the primary energy input into electricity generation. End use efficiency is estimated as 65% for the residential sector, 65% for the commercial sector, 21% for the transportation sector and 49% for the industrial sector, which was updated in 2017 to reflect DOE's analysis of manufacturing. Totals may not equal sum of components due to independent rounding. LLNL-MI-415927

図1. 米国におけるエネルギー消費量。2019年における推定値です。

より高度なセンシング技術により、エネルギーがどのように利用されているのかを測定できるようにすることが重要です。これは、効率と持続可能性の改善に向けた第一歩になります。

多くの人々や、組織、政府は、人類が環境に及ぼす影響について深く理解し、より良い未来を築くための変革に参画しようと努めています。その一環として、エネルギーの需要を低減し、既存の資源をより効果的に利用するために、IoTに対応するデバイスが使用されています。現在は、新たな技術が迅速にリリースされ、より速いペースでイノベーションが実現されている状況にあります。そうした技術やイノベーションは、より持続可能性の高い形でエネルギーを生成し、二酸化炭素の排出量を最小限に抑えて社会的な影響を改善するために役立てられます。

より良い未来への道を切り開く

持続可能性に良い影響を与える方法は3つあります。1つは、需要を減らすことです。これは、仮想化とスマート・ソリューションを利用することで実現できます。2つ目は、物事のやり方を改善することによって効率を高める方法です。例えば、エンジンをモータに置き換えたり、石炭を燃やしてエネルギーを生成するのではなく風力のような再生可能エネルギーを利用したりすることです。3つ目の方法は、汚染が生じないように管理を実施するというものです。そのためには、監視と隔離の手段が必要になります。これら3つの方法は、いずれも技術開発やイノベーションを必要とします。

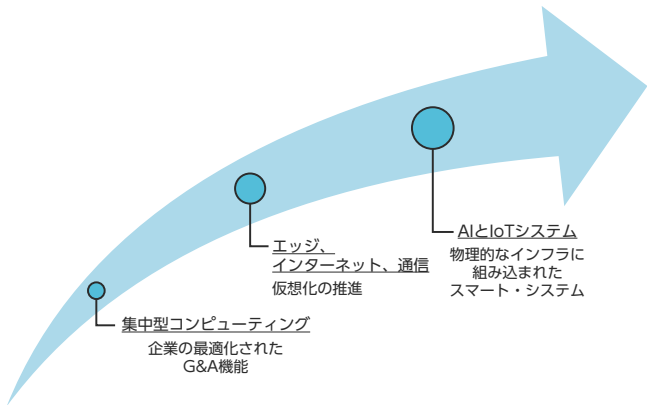
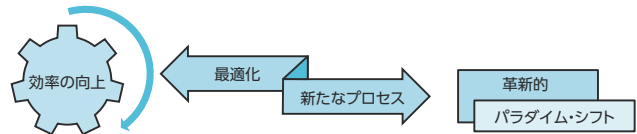


図2. 持続可能性に良い影響を与える3つの方法

エレクトロニクスは、効率に対する要求に応えるために継続的に進化してきました。なかでも、IoTは持続可能性に良い影響を与える最大の機会を迎えていると言えます。

IoTとエッジ・コンピューティングは、データの移動によって物体の移動を抑えるというパラダイム・シフトをもたらしました。それにより、エネルギーの消費量についても良い影響が現れます。物体の移動からデータの移動への移行は、2つの方法で行われます。1つは、IoTを利用し、現行のプロセスを最適化して効率を高めるといったものです。もう1つは、新たなプロセスを導入するというものです。持続可能性に良い影響を与えるためには、両方の方法を採用する必要があります。特に、新たなプロセスを導入する場合には大きな変革がもたらされるはずです。



物体の移動から、データ(情報)の移動に移行すれば、エネルギー消費量を大幅に削減できます。

図3. 物体の移動からデータの移動へのパラダイム・シフト

主要なメガトレンド

IoTをベースとするソリューションは、あらゆる業界で利用されるようになりました。消費財の分野では、家や衣服に装着可能な非常に興味深いガジェットが流通しています。そのようなものとは異なり、IoTは多くの人に認知されているとは言えないかもしれませんが、しかし、IoTは、今日の主要なメガトレンドに組み込まれて持続可能性や社会に大きな影響を与えています。以下、4つの分野における例を示します。

技術的な観点から言えば、5Gは重要なインフラの運用方法を根本的に変革しつつあります。また、5Gを活用すれば、自律走行車のような新たな技術を実現することもできます。あるいは、銅線を敷設することなく、従来のインフラをネットワークに接続することも可能です。その場合、廃棄物の量を大幅に削減することができます。加えて、開発途上の地域にインフラを配備するのも容易になります。つまり、社会を繁栄させるための基盤を構築できるということです。

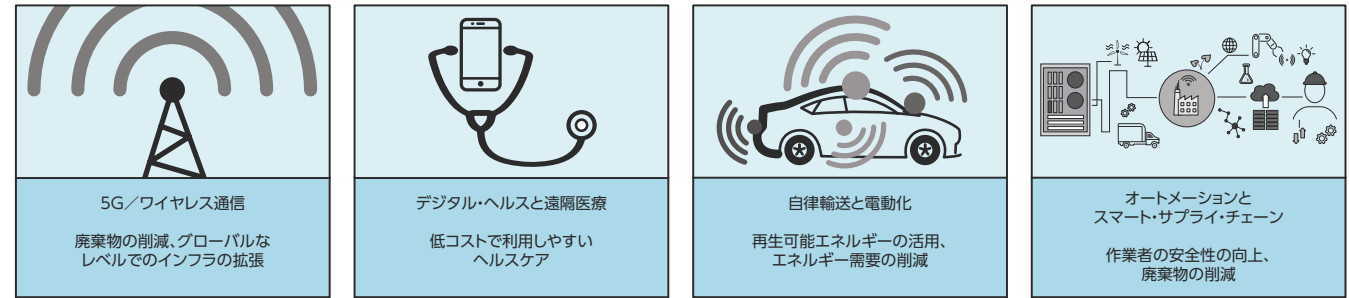


図4. IoTが牽引する市場

2020年、世界は新型コロナウイルスによるパンデミックに見舞われました。このことがきっかけとなり、デジタル・ヘルス向けの新たなソリューションの導入が進んで、遠隔医療がより身近なものになりました。ウェアラブルな医療機器から臨床グレードの家庭用医療機器まで、より効果的／効率的な健康管理を実現するための多様な製品が発売されようとしています。医療費の増加に伴い、健康状態を積極的に監視／管理して臨床医療の負担を軽減することがより重要になっています。予防ケアや在宅ケアによって人々が病院へ行かなくても済むようになれば、コストの上昇を抑えられます。予防ケアや在宅ケアは、生活の質を高めるための非常に効果的な手法だと言えます。

電動自動車や自律走行車は、持続可能性に対して直接的な効果をもたらします。化石燃料の需要を低減させるのは、二酸化炭素の排出量削減を実現するための最も手取り早い方法の1つです。例えば、大規模な自律型ライドシェア・プログラムを展開できるようになった状況を想像してみてください。そうすると、輸送手段をオンデマンドで利用することが可能になります。その結果、交通量や自動車の保有台数を削減することができます。また、ガソリンとエンジンの代わりに再生可能エネルギーとモーターを使用することから、二酸化炭素の排出量を更に抑えられます。

もう1つの主要なメガトレンドは、オートメーションとスマート・サプライ・チェーンです。オートメーション化を実現できれば、人体に大きな負担をかける作業や危険な環境で行わなければならない作業を減らすことができます。つまり、作業者の安全性が大幅に向上します。また、データを活用してサプライ・チェーンの精度／確度を高めれば、エネルギーの消費量と廃棄物を削減することが可能になります。

上述したメガトレンドは、IoTに対応するデバイスとエッジ・コンピューティングによって得られるデータを活用することで実現されます。ただ、それに向けての課題が存在しないわけではありません。市場では、デジタル技術に対する需要に応えるために、より期間が短く、より動的な設計サイクルが求められています。従来の市場では、需要の増加に対応するために、閉ざされていたエコシステムへの扉を開いていくということが行われました。既存／新規のパートナーと共に、設計ソリューションへの貢献度を高めることによって利益を得ていたのです。このような対応を図るために、各種のコンソーシアムやアライアンスが創設され、オープンなアーキテクチャが定義されてきました。

イノベーションの加速、課題の克服

業界標準の規格とアライアンスの構築を促進する主な要因は2つあります。市場では、エコシステムに属するより多くのパートナーが競争力のあるソリューションをタイムリーに提供できるようにするために、設計サイクルを短縮することが求められています。また、IoTに対応するデバイスを物理的なインフラに組み込まなければならないことから、拡張性を備えるオープンなアーキテクチャが必要になります。これらのニーズに応えるために、業界標準の規格が策定され、コンソーシアムやアライアンスが創設されるのです。

O-RANアライアンスはその典型的な例です。同アライアンスは、通信業界の事業者によって立ち上げられました。その目的は、完全な相互運用を実現するモバイル・ネットワークを提供することです。そのネットワークは、インテリジェントで、オープンで、仮想化されたものでなければなりません。同アライアンスには、メンバーとコントリビュータの両方が参画しています。そして、5Gのインフラ向けにホワイト・ボックスのエコシステムを開発し、その導入を促進しています。従来、この市場では、大手の通信会社が独自のブラック・ボックス・ソリューションを展開することによって優位性を保っていました。それに対し、O-RANアライアンスは、オープンなインターフェース規格とホワイト・ボックスのリファレンス設計を提供しています。それらにより、従来は参入できなかった多くの企業がこの市場に関わる事が可能になります。結果として、5Gにおけるイノベーションの実現と多様性への対応が加速されます。

業界標準の規格とコンソーシアムの重要な役割は、信頼性と保守性に優れる開発が行えるように保証しつつ、将来の要件の変化に対応可能な安全策を提供することです。5Gのエコシステムに存在するのと同様のニーズは、他の市場にも存在します。そのため、他の市場でも同様の対応が図られています。また、業界標準の規格とコンソーシアムは、セキュリティに関する要件も定義します。それにより、不注意による攻撃や悪意のある攻撃から未来を守ることが可能になります。セキュリティ向けのコンポーネントは、ワーキング・グループによるリスクの評価と相互運用性に関する定義を踏まえて開発されます。

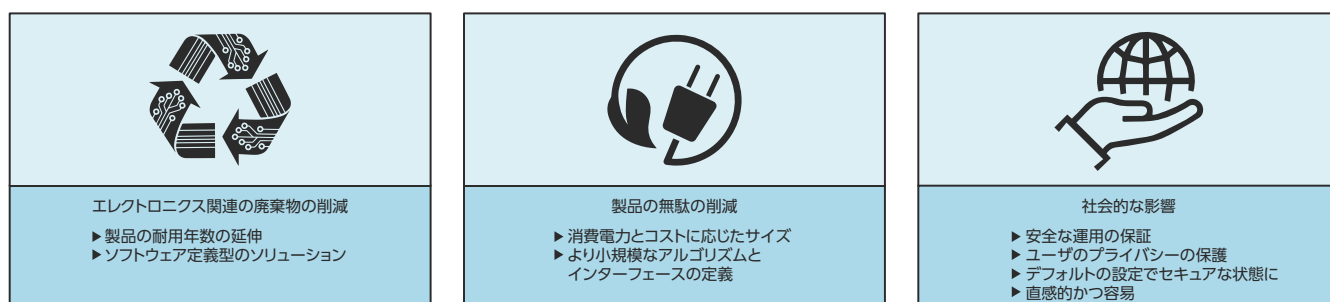


図5. IoT向けのセキュリティが影響を及ぼす3つの分野。
グローバルなレベルで持続可能性を高めることができます。

セキュリティが持続可能性に及ぼす影響

セキュリティについては、いくつかの基本原則が存在します。そのうちの1つは、資産の価値とリスクに応じ、システム内の適切な場所に適切なセキュリティ機構を適用するというものです。旧式か最新式かに関わらず、物理的なデバイスに搭載される接続用ソリューションの開発を続けていけば、セキュリティ上の脅威も増大し続けます。IoTによって、社会的、環境的な要因に意味のある影響を与えるためには、セキュリティを確保することが基本的な要件になります。

コンソーシアム、アライアンス、標準化団体で役割を果たすことにより、セキュリティ対策に対して良い影響を及ぼすことができます。また、セキュリティに対して積極的にアプローチすることにより、持続可能性に対して直接影響を及ぼすことが可能になります。そのための具体的な方法は3つあります。

1つは、エレクトロニクス関連の廃棄物を削減することです。その種の廃棄物が重要な環境問題として取り上げられることは少なくなりました。ただ、この分野には現在でも大きなビジネス・チャンスが存在しています。エレクトロニクス関連の廃棄物には、適切に処分することが求められています。ただ、それらをリサイクルするためには多大なコストがかかります。したがって、優れたリサイクル方法を見出す必要があります。ただ、セキュリティに関する適切なソリューションがあれば、発生する廃棄物の総量を削減することは可能です。そのためには、製品の耐用年数を延ばし、ソフトウェア定義型のソリューションを実現できるハードウェア・プラットフォームを開発しなければなりません。複数種のアプローチに対応可能なセキュリティ向けのサブシステムを組み込み、ハードウェアのライフサイクルを延ばしつつ、セカンド・ライフとして活用するためのソリューションを提供すれば、エレクトロニクス関連の廃棄物を削減することが可能になります。

セキュリティによって持続可能性に影響を与えるもう1つの方法は、運用上の無駄を減らすことです。小規模のIoTアプリケーションにおいて、セキュリティに関する基準を定義すれば、デバイスの全体的なサイズと消費電力を低減することができます。一般に、エッジ・デバイスのインターフェースを定義する際には、データ・センターと同様のアプローチを採用します。すなわち、必要なレベルを超えるアルゴリズムと追加のインターフェースを含むようにセキュリティに関する要件を規定します。逆に、最小限のインターフェースと暗号化処理だけを規定する方法を採用すれば、製品全体のサイズを削減することが可能です。

セキュリティは、安全な運用を保証し、ユーザのプライバシーを保護するための必須の要件です。セキュリティを、エンドユーザと開発チームにとって直感的に理解しやすいものにすることで、社会的にも大きな影響をもたらすことが可能になります。ほとんどの人は、セキュリティの専門家ではありません。また、セキュリティに関する構成や設定の意味も理解していない人がほとんどです。必要なのは、ユーザの観点からセキュリティをシームレスに組み込む方法を見出すことです。それにより、ユーザの生活全般に重要な効果がもたらされます。

今日、イノベーションはより速いペースで実現されるようになりました。そうしたなか、アナログ・デバイセズは持続可能性の向上に貢献する技術を開発し続けています。例えば、当社のワイヤレス・バッテリー・マネージメント・システムを採用すれば、材料にかかるコストを削減しつつ、設計上の柔軟性を高めることができます。それにより、電気自動車を効率的にスケーリングすることが可能になり、業界に変革がもたらされます。また、当社の蓄電システム（ESS：Energy Storage Systems）を利用すれば、風力や太陽光といった再生可能エネルギー源を利用する場合に特有の間欠性の問題を軽減することができます。その結果、主流のエネルギーと再生可能エネルギーの併用が促進されます。あるいは、在席状況の監視ソリューションであるADI EagleEye™を活用すれば、建物をより効率的に管理するための知見を取得／分析できるようになります。これらは、当社のソリューションを利用したアプリケーションの一例にすぎません。意味のある知見を導き出して効率を高めることにより、環境への影響を軽減するアプリケーションは他にも数多く存在します。

当社のセキュリティに対するアプローチは、当社の技術を活用することにより、持続可能性の高いグローバルな環境を実現することを目的としています。それに向けて、速いペースでイノベーションを実現し、無駄を削減べく取り組みを進めています。その際には、業界標準の規格に準拠することが重要な要件になります。一方で、それらの取り組みは、持続可能性の向上に向けたセキュアなエッジ・ソリューションを実現するための新たな業界標準の構築にも役立っています。当社のセキュリティ・ソリューションは、様々なアプリケーションで再利用できるようにするために、業界標準の規格に準拠する形で設計されています。そのため、それらのソリューションを採用すれば、アーキテクチャの設計の堅牢性について確信を持ちつつ、迅速にイノベーションを実現することができます。また、それらのソリューションが採用しているアーキテクチャによって、動的なライフサイクルの実現が可能になります。将来を見据えて設計が行われているため、業界が継続的に潜在的なニーズを掘り起こしている状況下でも、ソフトウェア機能の強化を図ることができます。アナログ・デバイセズは、旧来型のプロセスの効率を高めるための支援を行っています。それだけでなく、お客様が革新的な新ソリューションを導入する際のサポートも提供します。そのような形で、パラダイム・シフトの実現を支援しています。

参考資料

¹ [Estimated U.S. Energy Consumption in 2019: 100.2 Quads(米国における2019年のエネルギー消費量：100.2クワッド（推定値）)] Lawrence Livermore National Laboratory、2020年3月

著者について

Erik Halthen (erik.halthen@analog.com) は、アナログ・デバイスズのプロダクト・マーケティング・マネージャです。サイバー・セキュリティに関する中核的な研究拠点に所属しています。お客様にとって非常に重要な課題であるサイバー・セキュリティに関するニーズを理解し、新たなIPの開発を支援しています。それにより、自律型の未来を実現するソリューションが業界に普及するよう努めています。サイバー・セキュリティに関する脅威に対処してきた豊富な経験を有しており、お客様がIT領域のセキュリティとOT向けのソリューションのギャップを埋められるようサポートしています。執筆した記事や展示会における講演は国際的に評価されており、南フロリダ大学の認定プログラム「Cybersecurity for Executives」の諮問委員会にも参加しています。ネットワークに接続されたインフラに対するサイバー攻撃の脅威を認識するよう呼びかけると共に、「未来を守るためには、環境的／社会的な取り組みと歩調を合わせて進歩していくことが重要である」との提言を行っています。

EngineerZone®

オンライン・サポート・コミュニティ

アナログ・デバイスズのオンライン・サポート・コミュニティに参加すれば、各種の分野を専門とする技術者との連携を図ることができます。難易度の高い設計上の問題について問い合わせを行ったり、FAQを参照したり、ディスカッションに参加したりすることが可能です。



Visit ez.analog.com

* 英語版ソート・リーダーシップ記事は[こちら](#)よりご覧いただけます。