KPMG

止まない IoT規制の雨

IoT製品メーカーに求められる
新たな消費者保護規制への対応

著者紹介

Mike Krajecki

Managing Director, Emerging Technologies
KPMG LLP

マイク・クラジェッキー（Mike Krajecki）は、KPMGのエマージング・テクノロジー部門のマネージングディレクターです。12年を超える専門的な経験を通じて、KPMGのIoTリスクおよびガバナンスのサービス提供・支援フレームワークの開発を主導してきました。専門は、スマート／コネクテッド製品やデジタル資産に関連するリスクを識別、評価、管理できるように組織を支援することです。自動車、消費者向け製品、公共交通、医療機器、産業用機器においてIoTを実現してきた経験があります。また、CPA（公認会計士）とCISA（公認情報システム監査人）の資格を保持しています。

Danny Le

Principal, Cyber Security Services
KPMG LLP

ダニー・リー（Danny Le）は、KPMGのサイバー部門のプリンシパルであり、専門はサイバーセキュリティです。豊富な国際コンサルティングの経験を有し、世界最大級の企業の多数の管轄区域と事業活動においてグローバルなテクノロジーと規制リスクの管理を支援してきました。また、KPMGの情報セキュリティ保護とビジネスにおけるレジリエンスの領域をリードしています。幅広い業界にわたってテクノロジーリスク管理、内部統制、ビジネスプロセス、ガバナンス、レポーティングの先進的事例に深い知見を有しています。

Nick Naddaf

Manager, Emerging Technologies
KPMG LLP

ニック・ナダフ（Nick Naddaf）は、KPMGのエマージング・テクノロジー部門のマネジャーであり、専門はデジタル戦略、ガバナンスおよびエンタープライズIoT／モバイルのリスク、セキュリティ、ならびにIT内部監査です。デジタルリスクを評価し、その管理とガバナンスを向上させるために、製造、医療、医薬、農業、プロフェッショナルサービスなどの業界における米国の主要な組織との連携を実施してきました。

ルールは書き記されている

IoT（Internet of Things）は、私たちの知る世界をすでに作り変えました。そして、IoTは常に拡大を続けています。IHS Markitによると、IoTデバイスは2030年までに1,250億台を超える見通しです。その中でも、スマート家電、コネクテッドカー、パーソナルフィットネス機器、デジタル医療機器のように身近となったコンシューマデバイスが、全体のほぼ3分の2を占めると予測されています[1]。

IoT製品により、有用なデータを絶えず収集して利用することで、人々の生活はより手軽なものとなります。そして、利便性と得られる経験はますます向上し、応答性の高いより良いサービスが提供されます。そうした多くの利点に着目すれば、IoT機器が急速に普及していることも容易に理解できますが、その一方で、それにともなうリスクを見逃しやすくもあります。

しかし、現実には非常に多くのリスクがあります。セキュリティの不十分なコネクテッドデバイスにより、人々の身体的、経済的な状況や、個人のプライバシーなどが晒され、侵害される恐れがあります。そして、物理的な世界と相互作用のない従来のテクノロジーをはるかに超えた損害をもたらします。過去数年にわたり、ハッカーはスマートフォンアプリ、ウェブカメラ、無線ルーター、さらにはインターネットに接続された温度計やBluetoothを搭載した玩具などのさまざまな小型のコネクテッドデバイスを乗っ取ってきましたが、これにより甚大な被害が生じることとなりました。悪意のある攻撃者は、IoTデバイスをハッキングすることによりウェブサイトをダウンさせ、インターネットを広範囲にわたって使用不能にしています[2]。また、会話を盗聴する、自宅にいる人々の様子を盗み見る[3,4]、利益を稼ぐためにクリックベイト（釣り広告や釣り記事）であふれさせる[5]、機密性の高い個人データを詐取するなど[6]、多くの損害を引き起こしています。

これらの侵害によってもたらされる金銭的および評判上の大きな損害を考えると、安全でセキュアな消費者向けコネクテッド製品を製造することは、メーカーにとって大きなインセンティブがあります。これは、製品とブランドに対する消費者の信頼を築くうえで重要なものであり、製品のセキュリティとプライバシーへの取組みが不適切なメーカーは、適切に対処している競合企業に市場シェアを奪われる恐れがあります。

しかし、それでも損害が生じる可能性はあり、政府はそれを阻止したいと考えています。消費者の保護を最終目標として、全世界の政府当局は、先頭に立ってIoTの規制に取り組んでおり、メーカーにその照準を合わせています。現在、州や連邦、そして世界レベルで、消費者向けデバイスのセキュリティに対する責任をメーカーに担わせることを目的としたIoTセキュリティ法案が次々に成立しています。

現在の規制環境から明らかなのは、IoTデバイスの秘匿化と被害防止の責任はメーカーにあるということです。IoTを通じて、より良い消費者体験を提供するだけでなく、消費者の利用において安全で保護された状態を確保するための負担も、メーカーに課されるのです。

1 Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says (IHS Markit, Oct. 24, 2017)

2 The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet (CSO, March 9, 2018)

3 This pretty blond doll could be spying on your family (Washington Post, Feb. 23, 2017)

4 Internet of Babies–When baby monitors fail to be smart (SEC Consult, Feb. 21, 2018)

5 Hackers Take Over IoT Devices to 'Click' on Ads (ThreatPost, May 9, 2019)

6 Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank (Business Insider, April 15, 2018)

KPMG

IoTセキュリティ規制の一端

メーカーに対するIoTセキュリティ規制の波は、連邦と州の両方に到来しています。メーカーに対して、IoTデバイスに最低限必要なセキュリティ基準を組み込むことを義務づけるルールが、すでに米国のいくつかの州で立法化されており、2つの法案がカリフォルニア州とオレゴン州ですでに可決されています。また、多数の法案が州レベルで提出され、現在、各州の立法制度の中で制定に向けた手続きが進んでいます。加えて、連邦議会に対しても非常に多くの法案がすでに提出されています。

コネクテッド製品を世界規模で販売しているメーカー、そして今日のコネクテッドな世界ではほとんどの企業が、可決済み、および審議中の法案だけでなく、法的強制力はないものの将来の法律の先例となりえる自主的で業界横断的な指針や基準を把握する必要があります。EU、英国、中国、日本、オーストラリア、カナダ、ブラジルなど、米国のメーカーが頻繁にビジネスを行う諸外国地域においても、独自の法制を成立、あるいはその手続きを進めています。

一部の製造業界のサブセクターでは、固有のIoTセキュリティ標準を開発することによって、自主規制を導入しています。自動車業界は、コネクテッドビークルを保護するためのベストプラクティスを設計するために協力しており、医療業界では、設計管理、パッチ適用、およびインシデント対応のガイドラインを設定することで、医療機器の全体的なセキュリティを改善するためのパートナーシップを結んでいます。あるエレクトロニクス保安団体は現在、機能と要件のチェックリストに基づいたIoTデバイスのサイバーセキュリティ評価制度の開発を進めています。この評価は、一種の品質保証を示す役割として機能し、消費者がIoT製品の安全性とセキュリティを評価することや、メーカーが自社製品を市場で差別化する機会を提供することに役立っています。

しかし、これらの新しい規制やガイドラインだけがメーカーに影響を及ぼしているわけではありません。規制当局は、セキュリティおよびプライバシーに関する既存の法律もIoTデバイスやIoTプラットフォームに合わせて改正しています。例えば、消費者の健康情報を使用するコネクテッドデバイスのメーカーは、医療保険の携行性と責任に関する法律（HIPAA）のデータプライバシー要件の対象となります。さらに、スマート玩具メーカーは、子供向けオンラインサービスのデータ収集慣行を規制する児童オンラインプライバシー保護法（COPPA）を遵守しなければなりません。

各地におけるIoTセキュリティ規制[7]

米国、連邦レベル

— 米国の上下両院に複数の審議中の法案がある

米国、州レベル

— 情報プライバシー：コネクテッドデバイス（カリフォルニア州）

— インターネットに接続されているデバイスに要求されるセキュリティ対策に関連する規制（オレゴン州）

— 複数の州（イリノイ、メリーランド、マサチューセッツ、ニューヨーク、バーモントなど）の審議中の法案

中国

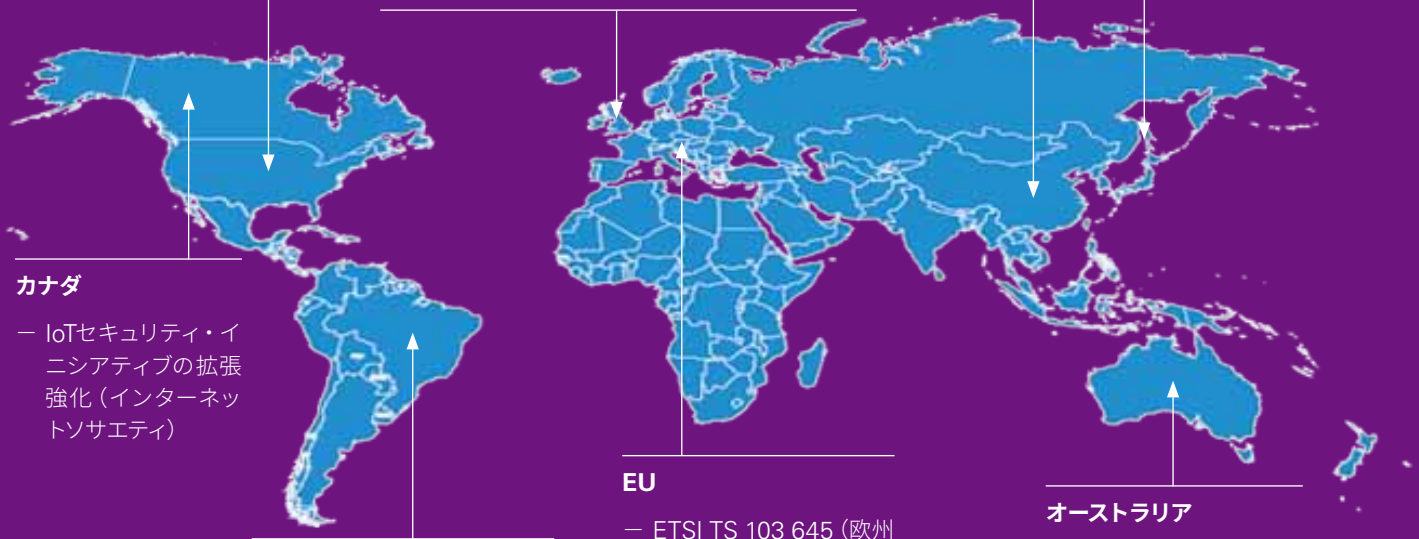
— モバイルIoTの構築および開発の包括的な推進に関する通知（中国工業情報化部）

日本

— IoT推進コンソーシアム（総務省、経済産業省）

英国

— 消費者向けIoTセキュリティに関する行動規範（英国デジタル・文化・メディア・スポーツ省）



カナダ

— IoTセキュリティ・イニシアティブの拡張強化（インターネットソサエティ）

ブラジル

— IoTに関する国家計画（科学技術革新通信省、国家電気通信庁）

EU

— ETSI TS 103 645（欧州電気通信標準化機構）

オーストラリア

— IoTリファレンス・フレームワーク（IoTアライアンス・オーストラリア）

最近の業界固有規制の動きの例

— 自動車サイバーセキュリティ・ベストプラクティス（Auto-ISAC）

— NHTSA先進車両サイバーセキュリティ・ベストプラクティス（米国高速道路交通安全事業団）

— 医療機器安全行動計画（米国食品医薬品局）

— 21 CFR Part 820.30（米国食品医薬品局）

7 KPMGによる調査：IoT製品およびサービスのベースラインセキュリティを改善することを明確な目的とした法案、標準、調査が含まれています。なお、IoTデバイスメーカーに影響を与える可能性があるものの、IoTセキュリティに特にフォーカスしていないサイバーセキュリティや消費者データのプライバシーを改善することを目的としたより広範な法案、標準、調査は含まれません。

規制の展望を理解する

IoTテクノロジーは急速に進化を続けているため、現在の法律と提案の多くは意図的に曖昧さを持たせるように設計されており、将来に向けた柔軟な解釈の余地を残しています。しかし、これらの規制の多くは包括性を欠き、規定が厳密でなく、どの規制のどの側面が個々の企業に適用されるのか、メーカーに対して混乱を生じさせています。規制の全体像を正確に把握することなく、どのようにしてメーカーは規制を遵守する準備を整え、また、いかにして自社にコンプライアンス違反のリスクがあることを知ることができるのでしょうか？

KPMGが、今日のグローバルな規制環境について深く掘り下げ、直近に成立した法案と準備中の法案を分析した結果、規制が重点を置いている8つの中核的な領域が明らかになりました。

この重点領域は、今後数年間、規制の展望がどこに向かっているのかを示唆しており、将来的に優れた製品のセキュリティがどのように進化していくのか、それを予想する判断材料を提供してくれます。その多くは、ごく単純な話に思えるかもしれません。しかし、IoTは本質的に複雑なものです。たとえ最先端のメーカーであっても、ときにはIoTデバイスのエンドユーザー（すなわち消費者）を保護するための基本的な対策を講じ損ねることがあることを、歴史は示しています。IoTセキュリティ規制の重点領域を評価することは、あらゆるメーカーがコンプライアンスを確保し、消費者を保護するためのデバイスセキュリティプログラムに対する投資の優先順位を理解するうえで役立つでしょう。

持続可能なIoTセキュリティ規制のコンプライアンスの8つのテーマ

ガバナンス

ガバナンスは、IoTのライフサイクル全体を通じて、リスクに適切に対処するための組織のポリシーとプロセスによって成り立っています。ガバナンスは、規制に準じたコネクテッドデバイス・セキュリティプログラムを推進し、かつそれを持続可能なプラットフォームへと転じる基盤であり、原動力となります。メーカーは、プログラムの方向性を定め、ステークホルダー間の連携を可能にするとともに、標準化と一貫した対応を推し進め、優れた慣行の提供や規制リスクの継続的な監視を行うために、効果的なガバナンスを導入しなければなりません。

リスクアセスメント

リスクアセスメントは、ガバナンスの中核的な構成要素であり、効果的なIoT製品セキュリティプログラムの計画立案と戦略に必要不可欠です。ビジネスを安全かつ効果的に営むために、メーカーは消費者を含む主要なステークホルダーだけでなく、自社の事業や資産に存在するコネクテッドデバイスがもたらすリスクを理解しておく必要があります。目の前の脅威と今後発生する可能性のある脅威の両方を評価するリスクアセスメントにおける堅牢なアプローチは、安全な製品の設計に踏み出す第一歩であり、どこにセキュリティの取組みの焦点を合わせるべきなのかを理解するのに役立ちます。

サプライチェーン管理

IoTデバイスメーカーには、全ての業務や運用に関与しているサードパーティのセキュリティ体制を認証および検証することが求められます。これには、製品のハードウェア材料およびソフトウェアコンポーネントの設計、開発、調達、および納入に関与するサプライヤーも含まれます。また、組立ラインから、倉庫、積出港に至るまで、事業活動における他のさまざまな場面に関係しているサプライヤーも含まれます。さらに、IoTデバイスのライフサイクルに特有の状況として、工場から出荷されて消費者の手に渡った後も継続してデバイスとのデータのやり取りを行うソフトウェアベンダーを監視することも含まれます。

セキュア開発ライフサイクル

IoT製品は、プロトタイプの作成から、開発、導入展開に至るまで、セキュリティを念頭に置いてエンドツーエンドで設計する必要があります。メーカーは、セキュア開発ライフサイクル（SDL）の技法をコネクテッドデバイスの設計と生産に組み込むことが求められています。SDLは、テクノロジースタックの全てのレイヤーにおいて、ソフトウェアにセキュリティとリスク低減策を組み込むための確立された反復可能なプロセスです。これには、「セキュリティ／プライバシーバイデザイン」の原則、すなわち、開発の初期段階においてセキュリティおよびプライバシーの要件とアーキテクチャを製品に組み込む技術開発アプローチが含まれます。セキュリティとリスクの検証を開発サイクルの後期に行うのではなく、ライフサイクル全体を通じて持続させる文化的原則とするべきです。このSDLの慣行をIoT製品に適用することで、組織は真の長期的なコスト削減と業務効率を達成する体制を整えることが可能となります。

構成管理

事前に設定されたソフトウェアとファームウェアの構成をカスタマイズする機能は、多くのIoT製品の重要な機能であり、消費者がデバイスを所有した後、デバイスの使いやすさ、プライバシー、および相互運用性を向上させることができるものです。これには、パスワードのカスタマイズや、基本的なプライバシーの設定変更といった単純な操作から、デバイスに暗号化を追加するような複雑な操作までが含まれます。しかし、多くのIoTデバイスのインシデントは、デバイスのデフォルト設定の弱点や、（意図の有無は別として）セキュリティを弱めるような方法で設定を変更する機能によって発生していました。メーカーにはIoTデバイスに事前に設定された安全なデフォルトの構成が組み込まれるようにする責任があります。また、誰が構成を変更でき、どのような変更ができるのかを制御可能とする責任もあります。

ID管理、認証、およびアクセス制御

ID管理、認証、およびアクセス制御は、権限のある個人、プロセス、およびデバイスのみにコネクテッドデバイスを使用することができるように確実に制限します。メーカーはこれらの領域のソフトウェアセキュリティのベストプラクティスを採用する必要があります。例えば、簡単に悪用可能な「admin」などのデフォルトパスワードを排除し、各デバイスを一意に識別できるようにすること、ユーザー名やパスワードなどの機密性のあるデータを安全に保存および送信すること、許容されるアクセス試行の回数を制限し、不正アクセスするための不適切な試行を阻止すること、さらに未使用のポートを閉じてサービスを無効化することなどによって、攻撃の標的となり得る対象を最小限に抑えるということです。

データ管理とプライバシー

メーカーには、生成、収集、保管され、そしてコネクテッドデバイスに伝送されるデータを保護する合理的な方法を実装する責任があります。データへの許可されたアクセス、データの使用、および開示のいずれについても、コネクテッドデバイスの機能において適切と見なされるものに限って許可されるようにするべきです。また、メーカーはデバイスを販売した後で、IoTサービスを提供するために必要なデータの可用性、機密性、完全性を確保することも求められています。安全なデータ管理とプライバシーの優れた慣行には、エンドツーエンドの暗号化、安全なストレージメカニズム、保存されたデータを消去する機能、そして明確で透明性の高いデータ利用ポリシーが必要です。重要な点は、効果的なデータ管理とプライバシーへのアプローチが、メーカーが消費者の信頼を築くためだけではなく、規制上のリスクを軽減するためにも必要であるということです。消費者のプライバシー保護は、HIPAA、COPPA、一般データ保護規則（GDPR）、カリフォルニア消費者プライバシー法（CCPA）などの広範な規則とともに、ますます規制当局の焦点となっています。

脆弱性のモニタリング、運用管理、パッチ適用、およびインシデント対応

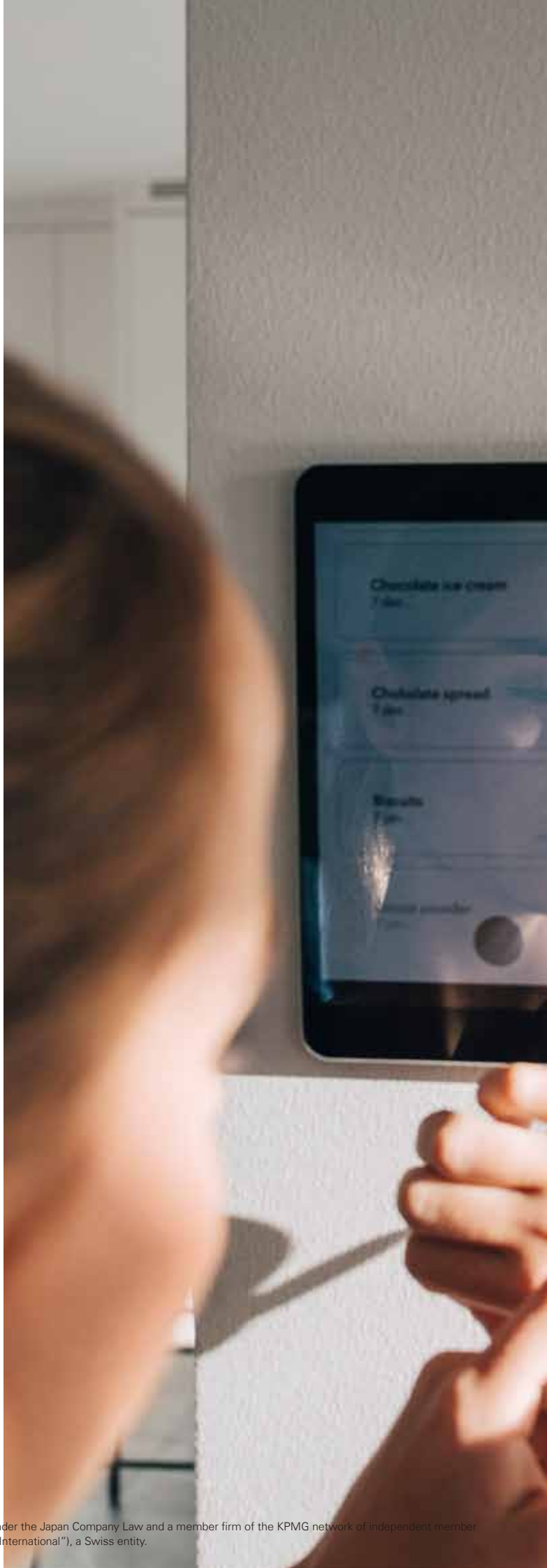
IoT製品のセキュリティは、製品がリリースされた時点で終わるわけではありません。マルウェア、ランサムウェア、そして盗聴まで、悪意のある攻撃者がより高度な攻撃を仕掛けるようになるにつれて、ソフトウェアやハードウェアに対する脅威は日々増してきています。発生するリスクを軽減するために、メーカーは生産や運用の段階での問題を含めて、IoTデバイスのセキュリティインシデントの発生を積極的かつ継続的に監視、特定、修正することが求められます。また、異常なデータの監視、不正侵入のリアルタイムな検出、セキュリティの脆弱性の発見（基本的なデータ監視から、侵入テストや倫理的ハッキングなどの最先端の方法に至るまで）だけでなく、販売前と販売後のデバイスに問題を修正するためのセキュリティプログラムを適用して、既知の脆弱性に関して、その影響を受けるステークホルダーや一般の人々に開示するための正式なプロセスを実装する必要があります。

短期的なコンプライアンスは長期的な価値をもたらさない

おそらく、メーカーが現在の規制に対応する最も容易で明白な方法は、目下のビジネスに適用される特定の要件に基づく組織を準備することです。しかし、これは近視眼的な解決策でしかありません。

大局的な視点で捉えれば、個別のIoTセキュリティ規則の遵守に焦点を当てることは、一時しのぎの対応となるだけであり、将来に向けた準備が十分にできていなければ、メーカーにおける顧客との関係や、潜在的な利益の創出、そして市場での地位までを脅かす恐れがあります。デジタル時代において、信頼できるテクノロジーの重要性はますます高まっています。コネクテッドな世界で、テクノロジーは顧客体験にも、顧客がメーカーに寄せる信頼のレベルにも、前例のない大きな影響を及ぼします。信頼できるテクノロジーは、市場における主要な差別化要因であり、長期的により強力で有利な関係をもたらします。巧妙に設計された安全な製品は、顧客のロイヤルティを獲得しますが、設計が不十分で安全性の低い製品は信頼を損ね、顧客離れを誘発し、メーカーのブランドに深刻なダメージをもたらすことになります。したがって、製品のセキュリティとプライバシーに関して最低限の対策を講じるような対応では、顧客の信頼を獲得し、それを活用して競争上の優位性を築き上げることはできません。

さらに、チェックリストによる確認作業のようにコンプライアンスに取り組むことは、次々と現れる新しいコンプライアンスの要求への対応に、いつまでも追われ続ける一因となります。今日、多くのメーカーは世界規模で製品を販売しています。オンライン通販とデジタル化されたサプライチェーンの急激な増加に伴い、大多数のメーカーは米国全土だけでなく、世界中の多くの地域の消費者が使用するコネクテッドデバイスを製造しています。関連する各規制に対して個別に遵守するやり方では効率が悪く、コスト効果も得られません。特定の州においてのみ販売を行っている比較的小規模なメーカーであっても、現地の規制を遵守するのみでは、将来的に問題を引き起こす可能性があるため、より広範な規制に目を向けることが不可欠です。メーカーが新しい市場に参入する場合や、顧客基盤が変化するような場合において、単発的なコンプライアンス対応は企業の成長を妨げることになるでしょう。



KPMG

コネクテッドな世界の製品セキュリティを変革する

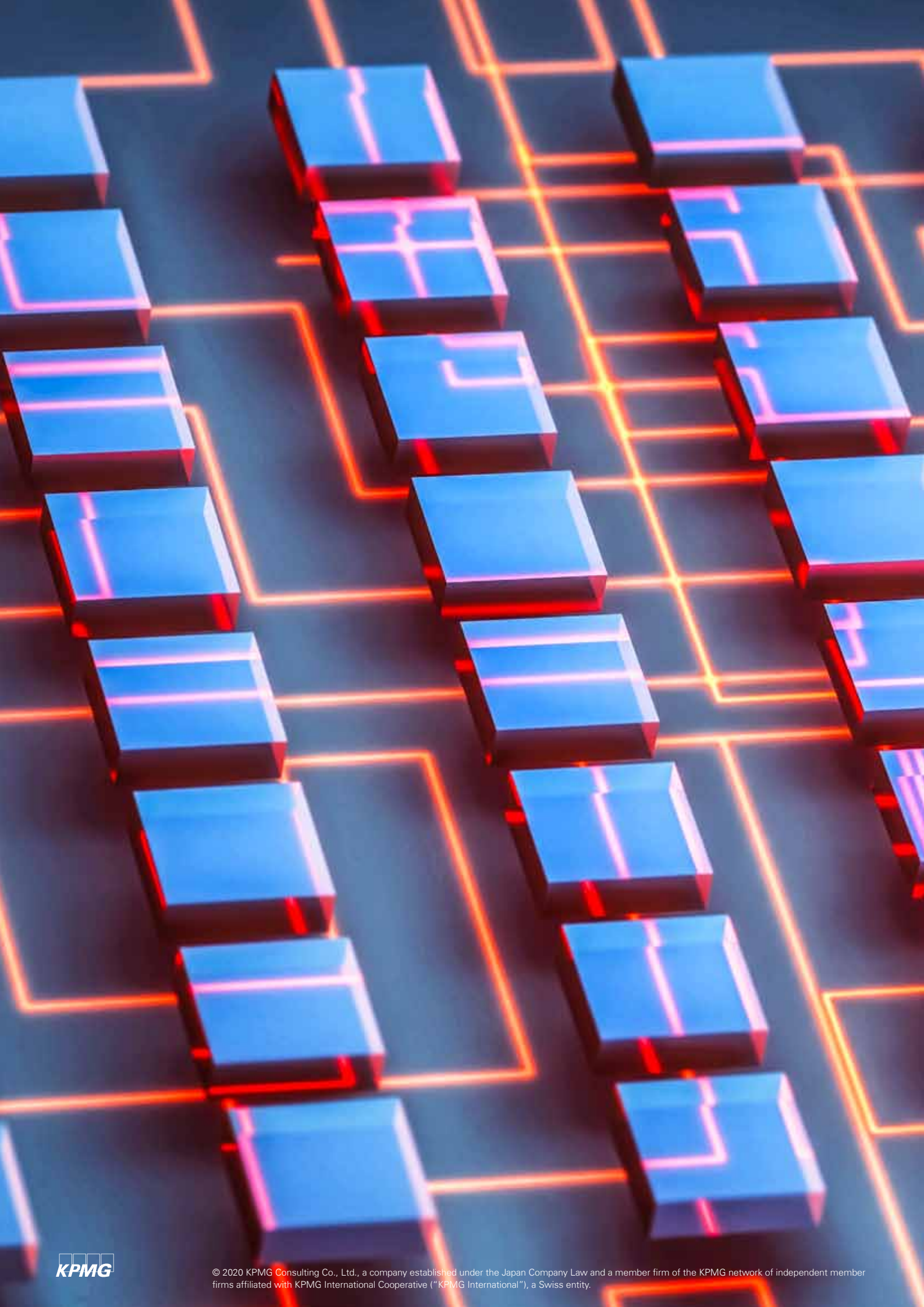
IoTセキュリティ規制の波は単なるコンプライアンスの実践ではありません。これは、すでにメーカーが行動に移さなければならないこと、すなわち、新たに出現したIoTエコシステムに対する製品セキュリティの再構想を促すものと捉えるべきです。

IoTのリスクと複雑性は、メーカーの製品開発のあり方自体を変化させ、セキュリティが果たす役割をより重要なものとしています。コネクテッド製品のセキュリティを工場から所有者の手に渡るまで維持するために、これまで以上の対策が求められています。

財務的な理由だけでも、製品のセキュリティを向上させる有力な動機となります。強力なセキュリティとプライバシー保護が整っていなければ、IoTメーカーは継続的なビジネスを獲得するために必要不可欠な消費者の信頼を失う危険性があります。新しいIoTセキュリティ規制が制定されている今、ルールや規制によって問題が生じるリスクが、セキュリティプログラムの抜本的な変革を一段と強く促す要因となっています。

こうした理由から、次々と到来するIoTセキュリティ規制の波への戦略的対応のあるべき姿は、消費者保護を中心に据えて設計された強力かつ堅牢で持続可能な製品セキュリティプログラムを構築し、実施することであると言えます。信頼できるテクノロジーのベストプラクティスに基づいたインターネット接続製品の効果的なセキュリティプログラムは、製品ライフサイクルのあらゆる要素に消費者の保護を組み込んでいます。安全な製品は消費者によって選択され、企業の成長を支える持続可能な基盤となります。

規制という観点から、包括的な顧客中心の製品セキュリティプログラムは、世界中の現在の規制の8つの重点領域それぞれに対応することで、メーカーの体制を盤石なものとします。技術的な問題が発生することによるリスクを低減することによって、メーカーは自社のコネクテッド製品に対する消費者の信頼を獲得し、維持することも可能になります。さらに、将来的に次々と新しい法律が成立していく状況にも適応することができるようになります。これは、今日の刻々と変化するグローバルな規制環境において、事業継続性と競争優位性の両方を維持するため非常に重要なことなのです。



IoT製品メーカーのための製品セキュリティの青写真

米国では、2020年1月1日にいくつかの新しいセキュリティルールと標準が施行され、メーカーはそれに準拠することを余儀なくされています。準備は今すぐにでも始めなければなりません。しかし、どのように推進するべきなのでしょうか？

ここでは、初期段階に検討すべき3つの項目を示します。メーカーはこれを出発点としてトップレベルのIoTセキュリティプログラムの構築に取り組むことにより、消費者の信頼を獲得してIoT製品およびサービスのビジネス価値を高めながら、今日と将来の規制への遵守を達成することが可能となるでしょう。

- **はじめにガバナンスを確立する：**IoTセキュリティプログラムは、ガバナンスの水準を超えることはできません。強力なガバナンス基盤によりIoTリスク管理の透明性と説明責任が向上することで、メーカーは市場で責任を持って安全なIoT製品を製造、提供、サポートできるようになり、規制の遵守が可能となります。リスクアセスメントはガバナンスの中核要素の1つであり、コネクテッドデバイスメーカーにおいて特に大きな焦点とするべきものです。脅威分析やストレステストのようなリスクアセスメントのアプローチは、セキュリティとプライバシーのリスクが及ぼす製品設計、サプライチェーン、消費者体験、そして収益源に対する広範な影響を理解するのに役立ちます。優れたガバナンスは、IoTセキュリティ規制の遵守を含めた戦略および運用上の目標を達成するために、ビジネスとテクノロジーの両方の利害関係者を含む適切な人々と協力することから始まります。ガバナンス機能は、IoTセキュリティプログラムの全体的な方向性を定め、プロセスの標準化を通じて一貫性をもたせ、IoT製品ライフサイクル全体にわたるセキュリティのベストプラクティスを推進します。ガバナンスモデルには厳密な公式は存在しません。正式なCoE（センターオブエクセレンス）を組織して運営しているメーカーもあれば、より分散性の高いアプローチとして様々なグループからリソースを引き出しているメーカーもあります。メーカーにおけるビジネスとテクノロジーのリーダーは、自社の組織構造の制約の中で最適な方法を判断する必要があります。
- **従来のセキュリティ・ベストプラクティスを優先する：**従来の消費者向けテクノロジー製品と比較して、安全でレジリエンスのあるインターネット対応デバイスを製造するためには、より強化されたセキュリティアプローチと対策が必要となります。しかし、それはITセキュリティとプライバシーの最も重要で基本的な原則と無関係ではなく、むしろ、この原則は信頼性の高いIoT製品の根幹をなすものとして重要視されるべきものです。消費者を保護するために、「セキュリティ／プライバシーバイデザイン」の原則は、コネクテッドデバイスの開発と生産の基本的な要素でなければなりません。データ管理、ID管理、およびリスク管理などの関連領域に従来のセキュリティのベストプラクティスを一貫して適用することによって、メーカーはIoTデバイスセキュリティの強固な基盤を創り出すことができるでしょう。また、それは規制遵守に向かう道へとメーカーを導いていくでしょう。KPMGによるIoT規制状況の分析によって明らかなように、IoTセキュリティのベースラインに対する期待は、サイバーセキュリティに対する期待と大きく異なるわけではありません。
- **リスクの存続期間を確認する：**IoT製品が展開されると、メーカーは消費者にサービスを提供し、消費者体験を継続的に高めていくために、デバイスと価値あるデータの送受信を継続します。信頼できる製品を作り上げることで、消費者に対して貴重なデータの継続した提供を促し、さらに得られたデータを活用して新しいサービスを開始して、新たな収益創出の機会を開拓していきます。このように、IoTエコシステムは、製品がメーカーの手を離れて物理的な統制下から外れた後でも、消費者の安全を確保することをメーカーに要求します。IoT製品メーカーが、販売の前後両方で消費者のセキュリティとプライバシーのリスクを管理することは、消費者の信頼を得るために不可欠であるだけでなく、世界中の規制当局の重要な焦点領域でもあります。規制当局では、消費者の安全に対するメーカーの責任は、IoT製品が機能しなくなる場合や、IoTネットワークから切り離されたときにのみ終了するものであると考えています。そのため、メーカーが実施するリスクアセスメント、ID管理、データ管理、脆弱性監視、インシデント対応などのプロセスは、包括的かつ継続的でなければならず、しかもIoT製品ライフサイクルの各ステージにおいて、絶えず変化する要件に適応する機動性も備えていなければなりません。

KPMGの支援

IoTは急速に拡大しており、消費者向け製品の分野に巨大なチャンスを生み出しています。また同時に、企業と消費者に新しいセキュリティとプライバシーのリスクをもたらしています。

KPMGは高度な技術的専門家とリスク管理の専門家を有しており、あらゆる業界の企業がIoTエコシステムの固有のリスクを管理し、テクノロジーの体制を整備することで、IoTのような破壊的なテクノロジーから価値を引き出すことを支援します。

KPMGは豊富な経験と将来を見据えた視点をもち、セキュリティ、レジリエンス、そして信頼の基盤の上に開発されたIoT製品だけが、消費者を保護するために進化し続ける法規制や業界標準を満たすことができるものであることを理解しています。KPMGは、メーカー各社と開発の初期段階から緊密に連携し、安全で規制に準拠した、混戦状態の市場の中においても際立つIoT製品を開発、提供、サポートできるよう責任をもって支援します。

Strategy

- IoTガバナンス機能と運用モデルの確立
- IoTプログラムでのリスク活動の評価
- コネクテッドデバイスの継続的なリスク監視のためのツールとプロセスの開発
- IoTリスクとガバナンスプログラムのロードマップを定義することによる経営陣の支援

Delivery

- 「セキュリティ／プライバシーバイデザイン」の原則の定義と評価
- コネクテッド製品の品質保証プロセスへのテストの組み込み
- コネクテッドデバイスの識別と分類体系の開発
- 共通のツールと実現手段によるトレーニングと意識向上プログラムの提供

Operations

- コネクテッドデータの接続、伝送、およびストレージの監視と保護
- 正式なデータガバナンスおよびデータ保護プログラムの実行
- 継続的な脆弱性管理と脅威検出アクティビティの実施
- 継続的な改善とリスク軽減のためのデータの管理、保持、分析

お問い合わせ先

KPMGコンサルティング株式会社

T: 03-3548-5111
E: kc@jp.kpmg.com

home.kpmg/jp/kc

home.kpmg/jp/socialmedia

本冊子は、KPMG Internationalが2020年1月に発行した「After the rainfall of IoT regulations: New regulations are making IoT product manufacturers responsible for safeguarding consumers on the IoT. Are they ready?」を翻訳したものです。翻訳と英語原文間に齟齬がある場合には、当該英語原文が優先するものとします。