IoTエコシステムとセキュリティ

KPMGジャパン

序文

IoT（モノのインターネット）に関しては、世の中で言われていることがすべて大げさであるとは言い切れません。実際、IoTは大半の人が考えているよりも大きな存在になる可能性さえあります。ただし、IoT分野で成功するには、単に洗練されたアプリケーションやネットワークに接続されたデバイス、高度な分析だけでなく、セキュリティやプライバシー、信頼性に対する確固たるアプローチが必要です。

テクノロジーの分野では、企業や消費者からのメッセージがはっきりしています。それは、革新的であること、大胆であること、安全であることです。

IoTがテクノロジー企業やIoT開発者に飛躍的な成長をもたらし、この拡大する市場で圧倒的な地位を築くことは、疑いの余地がないと言えるでしょう。しかし、成熟しつつある市場と競争の激化に伴って、現在IoTを使用しているユーザーやこれから使用するであろうユーザーは、特にセキュリティ面で大きな懸念を抱いています。

実際、このレポートで提案しているように、テクノロジー企業やIoTサービスプロバイダーは、セキュリティ（デバイスとインフラストラクチャーがどれだけうまく管理されているか）、プライバシー（データの機密性はどのように守られているか）、信頼性（顧客の信頼にどう対処するか）に関する懸念が大きな問題に発展する前に、これらの懸念に素早く、入念に、断固とした態度で取り組む必要があります。その取組みを疎かにする企業は、この新しい環境で成長することは難しいでしょう。

テクノロジー業界は、エコシステム内で水平的、垂直的な関係にある他の組織と協力して、すべての人々が指針とし、ともに成長できるセキュリティや標準に対する統一したアプローチを作る必要があります。現在の標準に対する分裂や競争状態は、さらなるユーザーの混乱とIoT分野の成長を阻害しかねません。

このレポートは、IoTのセキュリティに関する議論を促進し、知識体系を拡大することを目的としています。次ページ以降では、まずIoT分野に影響を及ぼしているセキュリティ、プライバシー、信頼性に関する課題の調査を取り上げ、現在市場で表面化しつつあるいくつかの機会とモデルを掘り下げます。このレポートでは、世界中の100のIoT「ユーザー組織」に対する最新調査と、業界のリーダーや学会およびKPMGのIoT専門家への1対1のインタビュー取材に基づいて、IoTのセキュリティ、プライバシー、信頼性に焦点を合わせ、誕生しつつあるエコシステムのすべてのプレーヤーにとって実用的で実行可能な助言を提供します。

KPMGは今後、継続的にこれらの重要な問題をより深く掘り下げていきます。テクノロジーおよびIoT専門家のグローバルネットワークから得られた知見に基づいて、私たちは、これらの重要な責務が業界、アプリケーション、エコシステムをまたがり、どのように管理されているかを研究していきます。

Gary Matuszak
Global Chair
Technology, Media & Telecommunications

Greg Bell
Principal and Services Leader, KPMG Cyber
KPMG in the US

Danny Le
Partner
KPMG in the US

IoT（モノのインターネット）

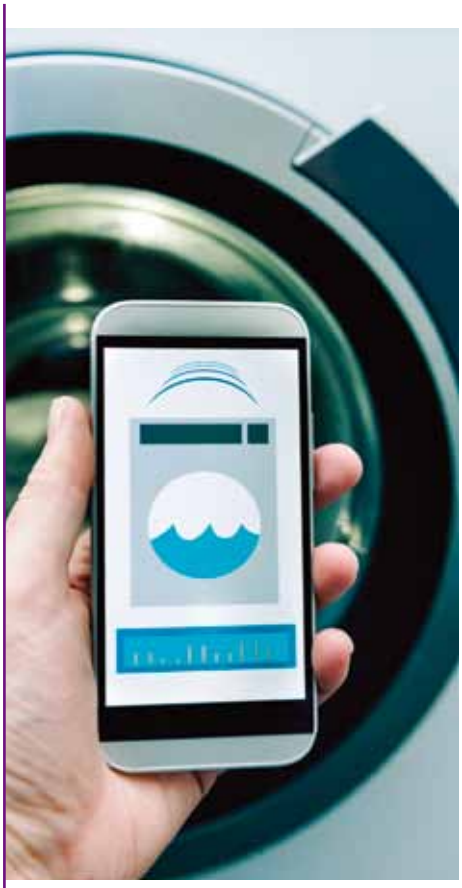
機能と相互作用を向上させるため、身の回りのものにネットワーク接続機能を埋め込んでデータ、クラウド、接続性、アナリティクス、テクノロジーを結び付け、スマートな環境を実現すること。

目次

02

サイバーセキュリティは「必需品」になる

本冊子は、KPMG Internationalが2015年に発行した“Security and the IoT ecosystem”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。



サイバーセキュリティは「必需品」になる

IoTユーザーの
92%
がサイバーセキュリティのことを懸念している

出典：KPMG Cyber Security and IoT Survey

企業のリーダーは、IoTが提供する潜在的な優位性を認識しているかもしれません。しかし、彼らはリスクについて大きな懸念も抱いています。大多数のリーダーが、IoTのもたらすサイバーセキュリティの脅威を完全には把握していないことを認めています。

IoTの顧客は、セキュリティのための追加的な出費には消極的かもしれませんが、顧客データやコンピューターシステムで起きた最近のセキュリティ侵害は、自社のセキュリティ保護に必要な措置を怠ったソリューションプロバイダーが消費者の信頼を失い、見放されてしまう可能性があることを示唆しています。

誰もが新しいIoTソリューションやIoT製品を「世界で初めて」手がけることを望んでいます。私たちの調査回答者の89%が、IoT分野で最初に成功した企業が市場で明確な競争上の優位性を得ると考えています。テクノロジー企業やIoTサービスプロバイダーは自社製品を市場にいち早く投入するために競争しており、この新たに出現した分野の膨大な潜在的成長力から利益を得ようと躍起になっています。

理由は明白です。最初に市場を握ってIoTバリューチェーンで支配的な地位を確立した企業がリーダーシップをさらに強固にし、急速かつ持続可能な成長を遂げる上で有利な立場を得るからです。しかし、実際に過去を振り返れば、内容より市場投入までのスピードを優先した製品やアイデアが、機敏さには欠ける堅実な競合他社に対する優位性を急速に失った例がいくつもあります。要するに、IoTソリューションの開発と運用

には、速度や利便性などの重要な検討事項のほか、セキュリティも優先させる必要があるのです。

それが現実の問題であることは既に実証されています。最近、さまざまな車の最新モデルが抱えるセキュリティの脆弱性が明らかになり、一部の大手メーカーは大量のリコールを余儀なくされました。また、セキュリティの脆弱なソフトウェアシステムを介して車を「ハイジャック」したハッカーのニュースがメディアを賑わせました。

脅威を深刻に受け止める

現在、多くの組織がIoTのセキュリティを高める方法を明確に意識して考えています。「インテルでは、IoTの採用と拡張性の向上を促進するためには、セキュリティをプラットフォームやシリコンに組み込むことが不可欠と考えています。最初からセキュリティを組み込んでおくことがIoTソリューションへの信頼の確立の鍵を握っています」と、インテルのIoTグループ業務執行取締役のBridget Karlin氏は述べています。「当社では、完全

> “IoTのサイバーセキュリティリスクに対する理解が不足しているため、最優先事項としました”
>
> – CEO of a European-based IoT user organization

IoT：急速な成長、膨大な潜在力

IoT（モノのインターネット）が企業、消費者、テクノロジー企業に大きな機会をもたらすことは間違いありません。多くの組織では、まだIoTソリューションで達成できるほんの一部のことに着手し始めた段階です。

デバイスメーカーやアプリケーション開発者は、インストールされるIoTデバイスの爆発的な増大に伴って、IoT対応デバイスの急速な採用が新たな成長と拡大の道を切り開くことを期待しています。IDCリサーチによれば、IoTユニットのインストールベースは毎年17.5%の率で伸びています。5年以内に7兆1000億ドル[1]という途方もない市場規模に成長するという予測もあります。

しかし私たちは、消費者がスマート家電、自動運転車、ウェアラブルデバイスなど、IoTが実現する利便性に慣れるにつれて、セキュリティ、プライバシー、信頼性に関する重大な懸念が増大する可能性があると考えます。

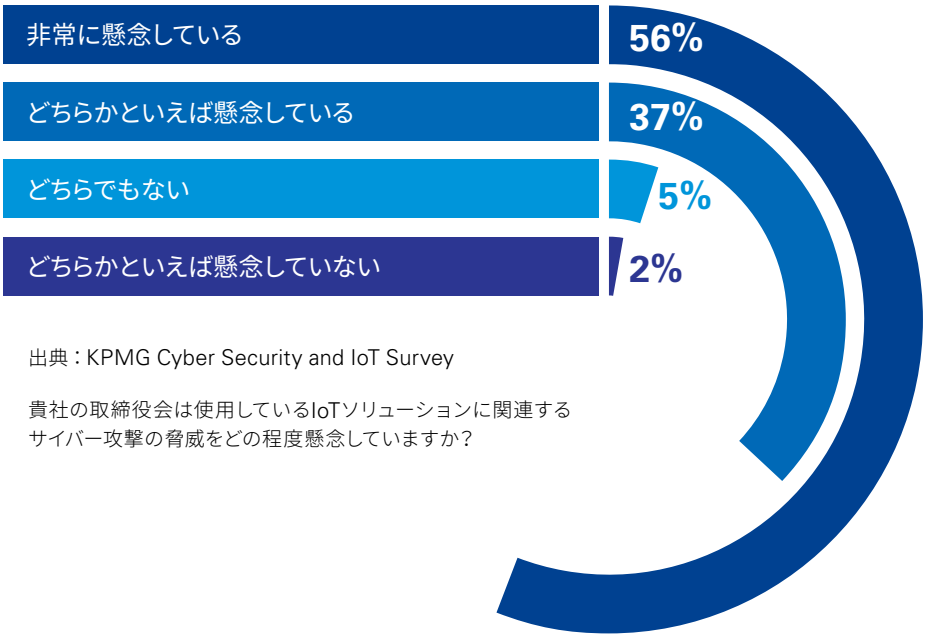
1 Worldwide and Regional Internet of Things 2014–2020 Forecast, IDC Research, 2014

性とデータ機密性が強化されたハードウェアおよびソフトウェアを提供するインテルIoTプラットフォーム参照アーキテクチャーと製品ラインを使用して、安全で拡張性の高いエンドツーエンドのIoTソリューションを実現する製品を市場に出す予定です」。

IoTのユーザー側では、使用しているIoTソリューション内におけるサイバーセキュリティ侵害の潜在的な影響を確かに懸念しています。私たちの調査では、回答者の半数以上である56%が、自社の取締役会がサイバー攻撃の脅威を「非常に懸念している」と回答しています。また、回答者の3分の1以上が自社の取締役会は「どちらかといえば懸念している」と回答しています。

アジア太平洋を本拠地とする企業の最高リスク管理担当役員はこう述べています。「当社の取締役会は、サイバー犯罪の増加とIoTソリューションで利用されている膨大なテクノロジーという観点から、サイバー攻撃の脅威を非常に懸念しています。ITシステム全体が新しいIoTデバイスとともに設計、統合されているため、当然、いかなる脅威も我々の事業の継続性にとって大きな妨げになり得ます」。

IoTユーザーとその企業の取締役会は、利用しているIoTソリューションがサイバー攻撃を受けるリスクに対する懸念を募らせている



出典：KPMG Cyber Security and IoT Survey

貴社の取締役会は使用しているIoTソリューションに関連するサイバー攻撃の脅威をどの程度懸念していますか？

リスクと機会

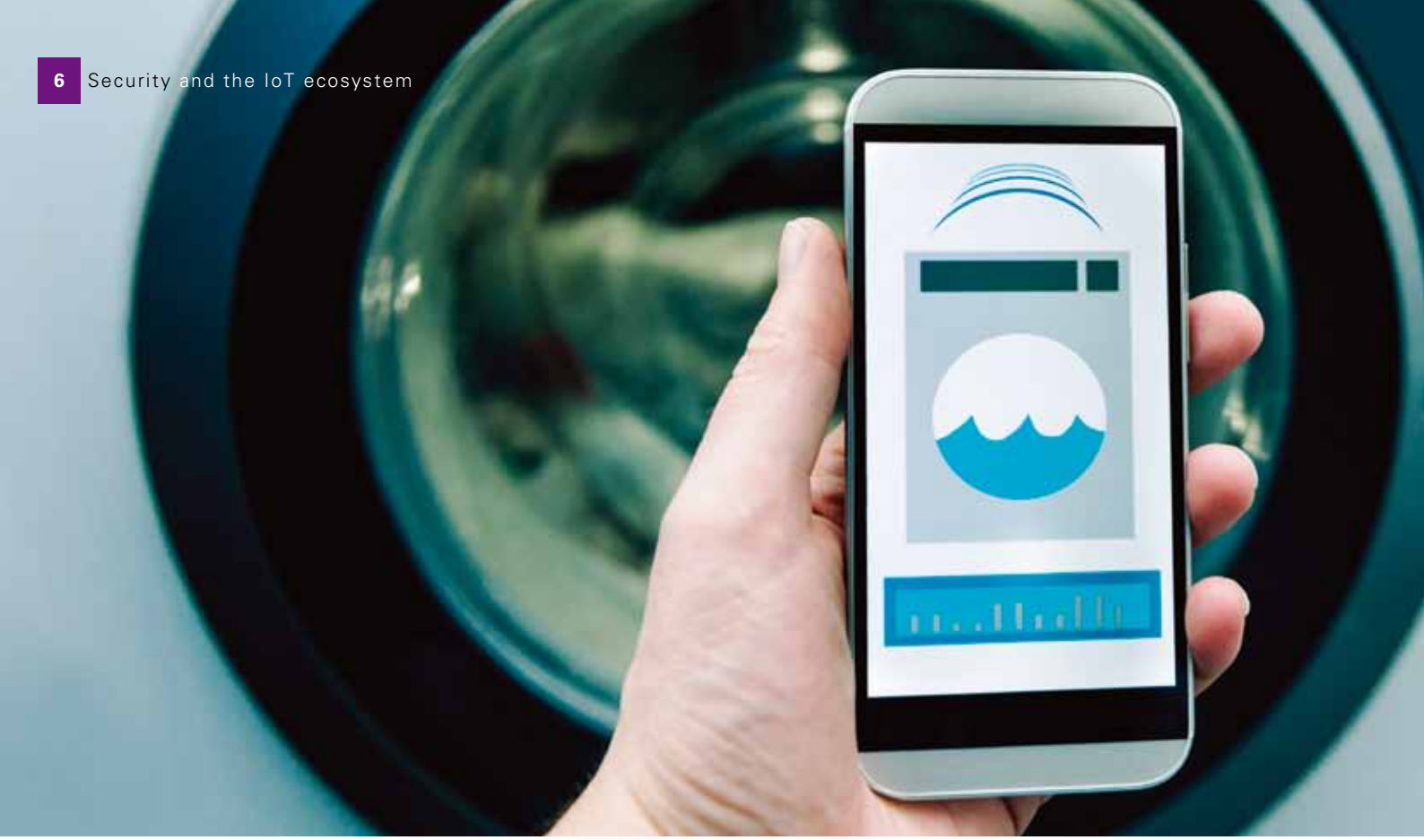
データの損失からサービス妨害攻撃、デバイスの制御不能に至るまで、さまざまな「マイナス面」のリスクがある一方で、IoTのセキュリティ向上は大きな利益をもたらす可能性があります。私たちの経験から、強力で堅固なサイバーセキュリティ体制、広く受け入れられた標準、消費者の信頼を勝ち取るための徹底した行動が、長期的な利益を確保し、最終的に成長を支える鍵になると言えるでしょう。

KPMG米国のパートナーであるDanny Leは次のように述べています。「テクノロジー企業やIoTソリューション開発者は、IoTのセキュリティ、プライバシー、信頼性に関連する重要なコンセプトを中心に据えるべきです。サイバーセキュリティの「プラス面」も見えてきています。実際、私たちは、たとえばアイデンティティや使用パターンを収益化することによって、組織が近い将来、サイバーセキュリティの技術を実際の収入機会に転じるようになると考えています。しかし、そこにも固有のリスクと恩恵があります」。

一部の企業では、既に顧客の個人データを収益化しています。たとえば通信会社は、顧客の地理的な位置データを（顧客の許可を得て）利用し、保険会社や小売業者などのサードパーティベンダーの広告を顧客に合わせ配信しています。顧客の運転パターンに関連した車の「コミュニティ」も形成されています。しかし、この種のモデルを拡張していくには、エコシステムに関わるすべての関係者がそのデータのプライバシー、安全性、機密性を守らなくてはなりません。

IoTソリューションにセキュリティ、プライバシー、信頼性のコンセプトを組み込むことに適切な時間とリソースを費やし、規律あるアプローチをとっているテクノロジー企業やIoTソリューション開発者は、市場投入を急ぐあまり規律をないがしろにする企業に最終的に打ち勝つでしょう。

> 最初からセキュリティをIoTソリューションに組み込んだ設計を行う必要があります。セキュリティをハードウェアレベル、ファームウェアレベル、ソフトウェアレベル、サービスレベルで考える必要があります。そして、継続的にセキュリティを監視し、脅威に対し先手を打つ必要があります
>
> —Florence Hudson, Senior Vice President and Chief Innovation Officer Internet2（formerly with IBM）



業界標準の模索

急速な成長や採用の激増、使用事例の急増が特徴のIoTには、ルールがほとんどなく、規制当局の監視の目が届かないため、あたかも多くの開拓者たちが一山当てようと競争を繰り広げる、バーチャル世界の「西部開拓時代」と言えます。業界、規制当局、ユーザーは連携して、広く受け入れられる標準とエコシステムを形成していく必要があります。

1つにはIoTソリューションの相互運用性を向上させるため、また1つには最小限求められるセキュリティ標準の定義を進めるために、多くの組織が、業界標準の制定がIoTの採用を促進するための最重要ステップであると考えています。実際、大半の新しいイノベーションは、広く受け入れられる標準が制定されるまでは、本格的に主流の技術として採用されないのが常です。

それを知る多くのテクノロジー企業が、規模の大小にかかわらず、新しい標準の制定と商品化に注力するために同じ考えを持つ組織のコンソーシアムを立ち上げはじめています。新しいコンソーシアムと標準が数ヵ月ごとに発表されており、市場の関係者は厳しい競争と大きな不安にさらされています。

たとえば、GoogleのNest製品は、サムスン電子、ARMホールディングス、フリースケール・セミコンダクタ、シリコン・ラボラトリーズなどの企業と提携して、家庭内のIoT通信の標準化を目指す「Thread」ネットワークプロトコルを開発しています。それと同時にインテルは、シスコ、AT&T、GE、IBMと提携して産業用IoT専用の標準を制定しようとしています。シスコは、クアルコムによって形成され、マイクロソフト、LG、HTCなどの大企業も参加している相互運用可能なピア接続と通信のフレームワークの制定を目指すAllSeenアライアンスにも参加しています。2015年8月には、消費者向けIoTデバイスに重点を置いたIoTのメーカー、開発者、小売業者へのガイドラインの提供を計画しているマイクロソフト、シマンテック、ターゲット、ADTなどの企業を含む共同の取組みとしてオンライン・トラスト・アライアンスが立ち上げられました。

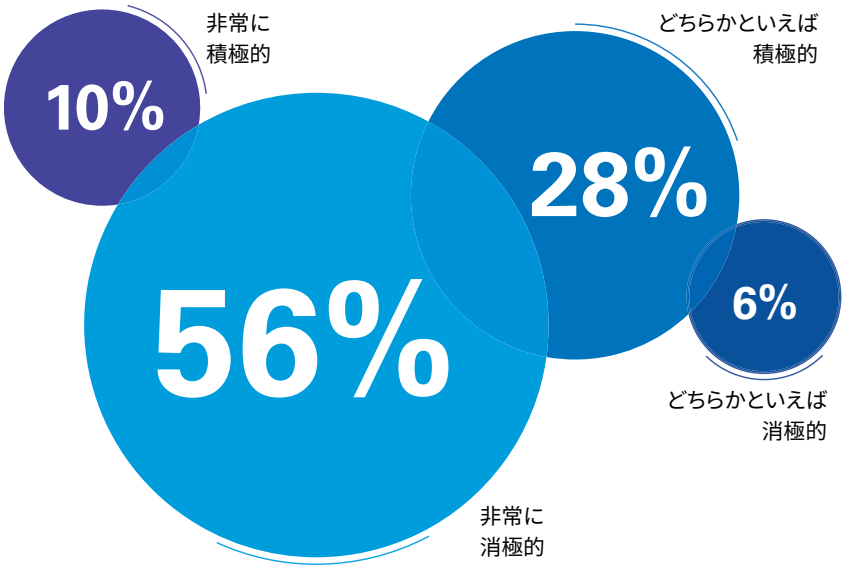
> 企業は規制を管理のためのコストと考えることをやめて、より長期的な見方に切り替える必要があります。企業は規制の制定に自分たちがどのような影響を与えることができるか、それが市場の誕生とビジネスの成功にどのように影響するかを自問する必要があります
>
> —Dr. Michael Geist, Canada Research Chair, Internet and E-commerce Law, University of Ottawa

「この業界は、同様の問題に取り組む標準化団体や準標準化団体がひしめき合ってひどく分裂しているため、業界が同じアプローチや標準に足並みを揃えるには、広範囲にわたる調整と参加が必要です」とシスコの戦略的イノベーション担当副社長、Maciej Kranz氏は述べています。

共同か競争か?

IoTの普及とそのシステムやデータの取扱いの難しさを考えて、この分野に積極的に関与している関係者の誰もが、明確なIoTの規制と標準の必要性を認識しています。JibestreamのCEO、Chris Wiegand氏はこう述べています。「モノのインターネット化

大半のIoTユーザー組織はIoTの議論の促進を様子見している



出典：KPMG Cyber Security and IoT Survey

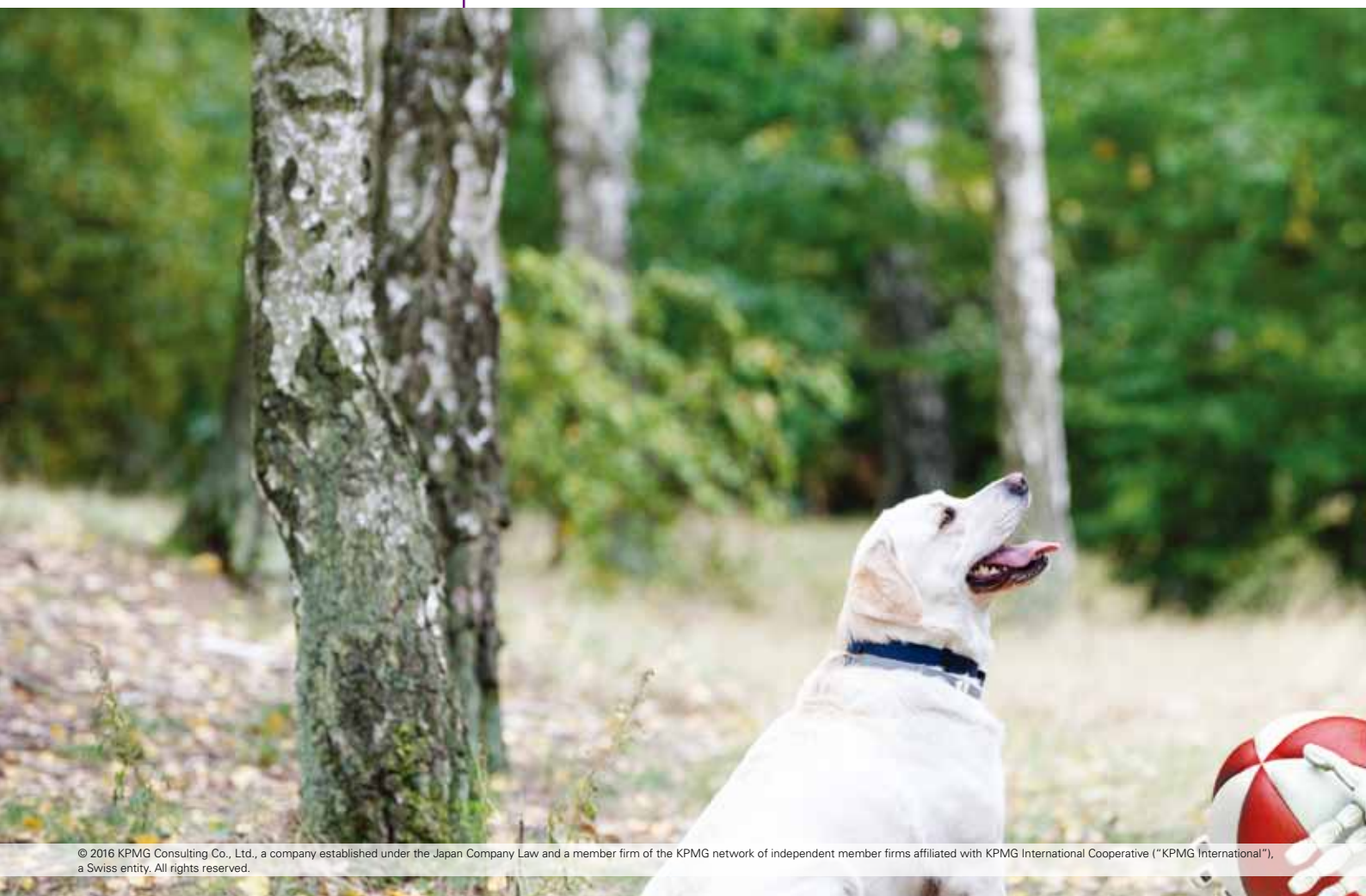
業界内で、貴社はIoTに関する議論にどれだけ積極的な役割を果たしていますか？

を実際に展開しているのは業界であり、我々業界が、IoTが悪用されないような正しい方法でIoTを展開していくことを肝に銘じる必要があります」。

ただし、関係者からは、標準を巡る競争は業界にとって百害あって一利なしという懸念の声も聞かれます。Internet2のFlorence Hudson氏はこう述べています。「誰もがコンソーシアムを形成しようとして分裂が起こり、誰もが勝利を収めようとしています。だから、私は、業界全体のあらゆる部分でセキュリティとプライバシーをテーマとするエコシステムを形成し、そのエコシステムを実践するための手段としてコンソーシアムを使えればよいと思っています」。

規制当局の監視と指導の強化は、標準の採択を促進する効果もあるでしょう。既にIoTソリューションを使用している企業のほぼ3分の1が、既存のルールと規制の欠如がIoTを採用するうえでの足かせになっていると回答しています。たとえば、金融サービス、医療業界、公益事業など厳しい規制を受けている業界では、規制を懸念する特別な理由があります。

「規制当局は新しいイノベーションに追いつくのに苦労することが多く、追いつくまでの間は、多くの場合、業界内部の変化を懐疑的な目で見ます。米国の多くの医療関連業者が米国の医療分野で受け入れられるウェアラブルデバイスについて、FDAの指示を求めていることも驚きではありません」と、KPMGサイバー部門のプリンシパル兼サービスリーダーであるGreg Bellは付け加えています。「規制は両刃の剣です。一方では組織に対してコンプライアンスと報告への投資を要求しながら、同時に許容されるものと許容されないものを明確に示して、組織が投資と計画を押し進めることを認めています」。



しかし、一部の業界では、規制の欠如がIoTソリューションの採用を遅らせている可能性があります。たとえば、現在、多くのテスラ車では、事故を減らし、安全性を向上させる機能である「オートパイロット」を利用できます。この技術が成熟すれば、自動運転によって事故が減るかもしれません。しかし、現在に至るまで、道路規制当局はこの機能の公道での使用許可に慎重であるため、この新しいテクノロジーを通じて得られる競争優位性は著しく限定されています。

もっとやることがある

私たちの経験から言って、標準の制定に積極的に取り組んでいるテクノロジー企業とIoTソリューション開発者はごく少数です。それに輪をかけて少ないのが、将来の規制の方向を理解し、情報提供の面で規制当局に協力している企業です。

「エコシステム内の小規模なテクノロジー企業の多くは、顧客とともに、傍観者の立場から、どの標準や規制が残るのか様子見をしているようです。彼らは大企業にすべての決定を委ねています」とKPMGのサイバーセキュリティグローバルリーダーであるMalcolm Marshallは述べています。「今は消極的な姿勢を取っている場合ではありません。テクノロジー企業は、現在策定中のさまざまな標準を理解し、できればそれに影響を及ぼすために、なるべく多くのコンソーシアムと共同で問題に取り組むべきです」。

しかし、シスコのMaciej Kranz氏は繰り返しこう述べています。「現在、少なくとも10～15の標準化団体がIoTのセキュリティ、プライバシー、信頼性の各要素を検討していますが、個々の業界が独自のベストプラクティスや標準を提案するより、我々がこれらの取組みを集約して全体的なアプローチをとることが重要です」。

セキュリティ、プライバシー、信頼性への取組み

セキュリティの向上、プライバシーの保護、信頼関係の構築をいずれも等しく重視するIoTソリューションプロバイダーとテクノロジー企業が、最も大きな成功を収める可能性が高いでしょう。これら3つの要素はすべて、IoT分野でマーケットシェアを獲得するうえで鍵を握っています。

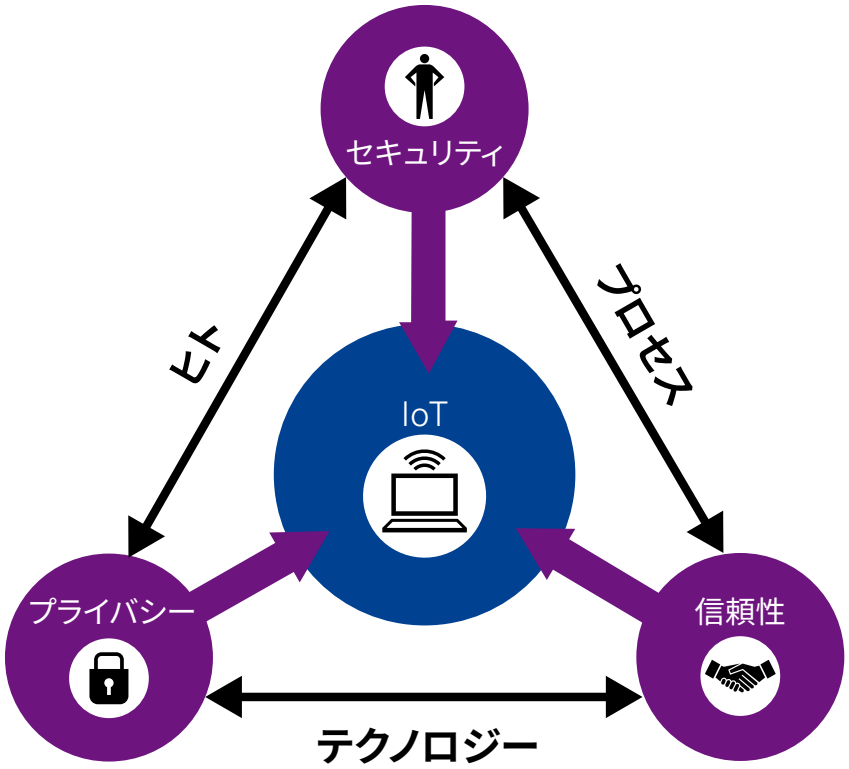
サイバーセキュリティのトピックがIoTユーザーと開発者の両方にとって主要な課題であるように見えるのは確かですが、私たちの経験から、大半の関係者は自分たちの責任に関してやや狭い見方をしていると言えます。堅固な「サイバーセキュリティ」のアプローチでは、システムを支えるデバイスとインフラストラクチャーの保護だけでなく、適正なレベルのデータプライバシーの確保と、顧客や規制当局の信頼の獲得も重視する必要があります。

IoTエコシステムのセキュリティ、プライバシー、信頼性とは何か？

IoTのソリューション、製品、イノベーションを成功させるためには、テクノロジー企業とソリューション開発者が、1つのコンセプトとして混同されがちなセキュリティ、プライバシー、信頼性という3つの重要なコンセプトについて、具体的に考える必要があります。

企業の環境、デバイス、ソフトウェアを管理する能力と定義されることが多いセキュリティは、業界の会議や会合で最も頻繁に論じられる問題であり、多くの場合はプログラムのコードや製造プロセスに埋め込まれ、定期的にアップデートされます。

一方、プライバシーは、機密性とデータの管理に関係しているため、多くの場合、ソリューションや製品に「埋め込む」ことはより難しくなります。



プライバシーは顧客のデータを保護することだけでなく、顧客が自分のデータに対する権利をどのように割り当て、その情報をサードパーティ間でどのように共有し、利用するかということにも関係しています。

（これまで）議論されることが少なかった問題は、IoTの関連性における「信頼性」の影響です。IoTに関わる開発者とテクノロジー企業は、単に「ブランドの信頼度」と評判を守るだけでなく、顧客向けの新しい価値駆動型の機会を創出するために、ユーザー、パートナー、サプライヤー、顧客との間で信頼性、完全性の高い「エコシステム」を構築する必要があります。消費者やユーザーを保護している、既に信頼されているサードパーティの力を活用して信頼関係を構築できることもあります。

私たちの見解

IoTのセキュリティに効果を持たせるには、セキュリティをなるべく資産に近いところでテクノロジーに組み込む必要があります。つまり、デバイスにセキュリティコントロールを、ソフトウェアのコードにセキュリティを、それぞれ埋め込む必要があるのです。実際、セキュリティはフェイルセーフコントロールにすべきで、テクノロジーが「オフライン」のときも安全が確保されなければなりません。「オープンな」デバイスを作ったり、セキュリティが中央管理されるプラットフォームを構築することは推奨できるものではなく、いずれもリスクが高すぎます。

> 「ハッカーは何でもハックしようとします」とIBMのFlorence Hudson氏は警告しています。「私は、医療、自動車等の輸送機関、重大なインフラストラクチャーのセキュリティを最も心配しています」

セキュリティへの取組み

部屋の温度から車の速度に至るまで、すべてを管理するというIoTデバイスが未来の新しい世界で期待されている役割を考えると、IoTユーザーの多くが、現在、市場で使用されている従来型のサイバーセキュリティ対策を導入する動きが鈍いことは驚きです。

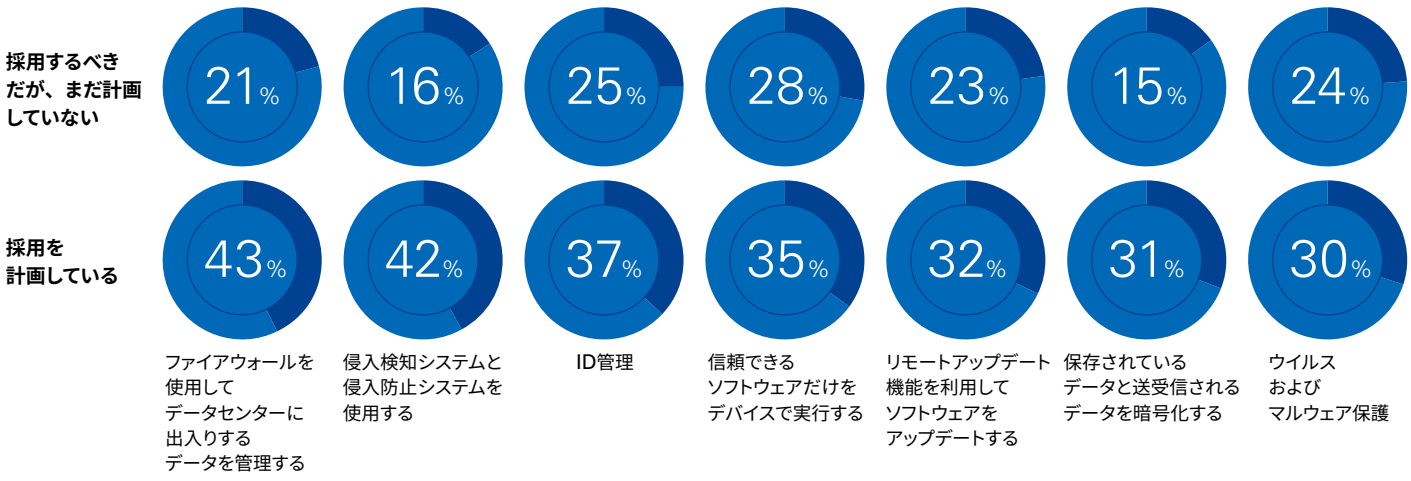
私たちの調査では、現在IoTを使用している企業のうち、ファイアウォール制御の改良やID管理プロセスの強化、侵入検知ソフトウェアの実行など、既にさまざまな対策を講じていると回答したのは、およそ40%に過ぎません。

しかし、攻撃は既に現実のものになっています。2014年にICS-Cert（サイバー脅威を専門とする国土安全保障省の支部）は、制御システム（多くは産業用IoTデバイスが統合され、制御されているプラットフォーム）に関連する245件のインシデントを報告していますが、その55%に、高付加価値ビジネスを標的とすることが多い高度な持続的標的型攻撃（APT）が関わっていました。また、インシデントの42%は通信、水、輸送のインフラストラクチャーを標的にしていました[2]。

オンラインへ移行するデバイスが増えるなか、目的が金銭的利益にせよ、政治的な動機にせよ、単にスキルや能力を磨くことにせよ、脅威を仕掛ける側がIoTセキュリティ対策の裏をかこうと躍起になっていることは目に見えています。また、組織がIoTデータへの依存度を高めていくにつれて、これらの標的は攻撃者にとってますます魅力的になっていきます。

より安全でセキュリティが強固なIoT環境を構築するためには、テクノロジー企業とソリューション開発者が、自分たちのデバイスとソリューションのセキュリティをできる限り強固にして主導的な役割を果たす必要があります。「設計段階からセキュリティを入念に検討し、開発プロセスを通じて継続的にテストを行い、アップデートしていく必要があります」と、KPMGのテクノロジー、メディア、通信部門のグローバルチェアマンであるGary Matuszakは述べています。「製品投入後のアフターマーケットにおいてアップデートやアップグレードを行える企業は、顧客に提供する価値を高めるだけでなく、市場における自社の高い評価も維持するでしょう」。

IoTのユーザーとソリューション開発者は、既存および将来のテクノロジーソリューションの幅広い選択肢を活用して、IoTソリューションに対するサイバー攻撃のリスクに対応したいと考えている



出典：KPMG Cyber Security and IoT Survey
貴社では、IoTソリューションにおけるセキュリティリスクに対応する計画として、何を採用しますか？

2 https://ics-cert.us-cert.gov/monitors/ICS-MM201502

プライバシーへの取組み

今日の消費者は、企業やサービスプロバイダーにとって自分たちの個人情報が持つ価値を認識しており、サービスの向上や値引きを見返りに自分の個人情報を共有するという考え方を、抵抗なく受け入れるようになっています。

しかし、この「価値と引き換えに情報を提供する」という約束が成り立つのは、どのような情報を共有できるか、誰と、どのような目的で情報を共有できるかに関する明確な合意があるからです。たとえば、ネットワークに接続されたウェアラブル心臓モニターを身に付けている消費者は、モニターから得られる情報を医療サービス機関と共有することは望んでいるかもしれませんが、営利企業や保険会社とはその情報を共有したくないと思っているでしょう。

しかし、プライバシーに関する議論は、リスクに関するものにとどまらず、直ちに機会に関する議論に発展していきます。言い換えれば、消費者は自分たちの個人情報（購買記録だけでなく行動データやメタデータも含む）が持つ価値を認識しており、事実上、既に個人情報をより良いサービス、より低い価格、または販売促進活動などと「交換」しています。それがIoT企業に新しい機会や潜在的価値をもたらしています。

「個人情報は急速に消費者にとって新しい形の通貨になっており、適正な環境と適切な見返りがあれば、IoTのユーザーは自分のデータを提供することも考えるでしょう」とKPMG中国のパートナーであるHenry Shekは述べています。「しかし、それはIoTソリューションプロバイダー、プロバイダーの法人顧客、そしてIoTバリューチェーン内のすべての関係者が、どのデータを誰と共有できるかを明確に理解する必要があることを意味しています」。

私たちの見解

組織は、明確な便益と引き換えに、特定の個人情報の利用許可を得るための交渉をユーザーと始めるでしょう。そのような状況のもと、テクノロジー企業やIoT開発者は、許諾の管理とデータを安全に統合・集約するという付加価値サービスを創出し管理するという、またとない機会を得ることになります。

私たちの見解

IoTの普及に伴って、組織は、より完全でシームレスな質の高い体験をエンドユーザーに提供することに注力しており、たとえばトラフィック認識型地図サービスの自動車への組み込みや電話料金の支払アプリケーション開発のような、製品とサービスの統合が進展するでしょう。

信頼性への取組み

個人情報を顧客にとっての価値に変換できるように、信頼性もテクノロジー企業やIoTソリューションプロバイダーにとっての価値に変換することができます。「ブランドの信頼度」、カスタマーエクスペリエンス、売上との間に反論の余地のない関連性を示す資料は数多く存在します。

顧客からの信頼度が高いブランドの製品やサービスは、顧客との間に強力な「関係」を築く傾向があるだけでなく、サービスや製品の組み合わせで販売を幅広く行うことができます。たとえば、テクノロジー企業が1つのサービス分野における既存のブランドと顧客からの信頼を利用して、それまでにほとんど経験も実績もないモバイル支払サービスのようなまったく新しい市場を独占する例を考えてみましょう。当然、顧客からの信頼がIoT分野における長期的な成功の鍵であることは明らかです。

「信頼は、システムのセキュリティを維持する能力と顧客の情報を保護する能力に基づいて構築されますが、その他にはブランドイメージに対する配慮、消費者とコミュニケーションをとる方法、意図しないセキュリティやプライバシーの侵害への対処法も含めなければなりません」とKPMG英国、サイバーセキュリティ部門のシニアマネジャーであるRichard Marriottは付け加えています。「セキュリティさえ確保すれば信頼が生まれると思ったら間違いです。信頼関係の構築に本格的に取り組む必要があります」。

私たちの見解

既存のプレーヤーのなかには、最終的に自身が事業を運営するエコシステム内の実質的な「信頼プロバイダー」になる者もあるでしょう。課題が生じるのは、その「信頼プロバイダー」が、デバイスメーカーやサービスプロバイダーではなく、支配的なブランドになり、エコシステム内で他のプレーヤーの介在を潜在的に必要としなくなったときです。

> 現在、多くの人が気にしていることは、顧客からの信頼の維持とデータのプライバシー、セキュリティ、完全性に関わる問題です
>
> —Danny Le, Partner, KPMG in the US

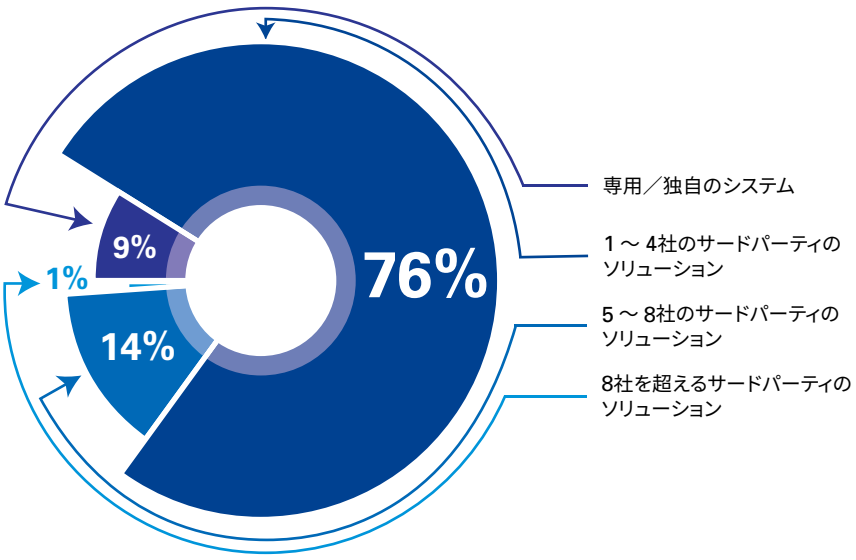
エコシステム全体でセキュリティ、プライバシー、信頼性を追求する

IoT分野で独力で生き残れる企業はありません。成功には、他の組織との提携、バリューチェーンの構築、エコシステムの繁栄が必要です。しかし、IoTユーザーが、より多くの参加者、サービスプロバイダー、サードパーティサプライヤーをバリューチェーンに取り込みはじめると、テクノロジー企業やIoTソリューションプロバイダーは、自社のセキュリティ能力の実証を迫られるというプレッシャーに直面することになるでしょう。

IoTにとって適切なエコシステムを構築するには、デバイスメーカー、インフラ事業者から通信会社やデータウェアハウス事業者に至るまで、多種多様な参加者が連携しなければなりません。既に現在のIoTユーザーの4分の3以上が、自社のIoTソリューションの管理に1社から4社のサードパーティを利用していると回答しています。15％のIoTユーザーは5社以上のサードパーティを利用していると回答しています。

「独力で生き残れる会社は存在しないのが現実です。シスコでは、プラットフォーム能力とソリューションを開発し提供するために水平的関係、垂直的関係両方の多数のパートナーシップを構築しています」とシスコのMaciej Kranz氏は述べています。

IoTエコシステムが成長しており、市場に対して強力にアピールする提案を生み出すには、サードパーティやプロバイダーを頼る必要があるという認識がユーザーの間に広がりつつある



出典：KPMG Cyber Security and IoT Survey

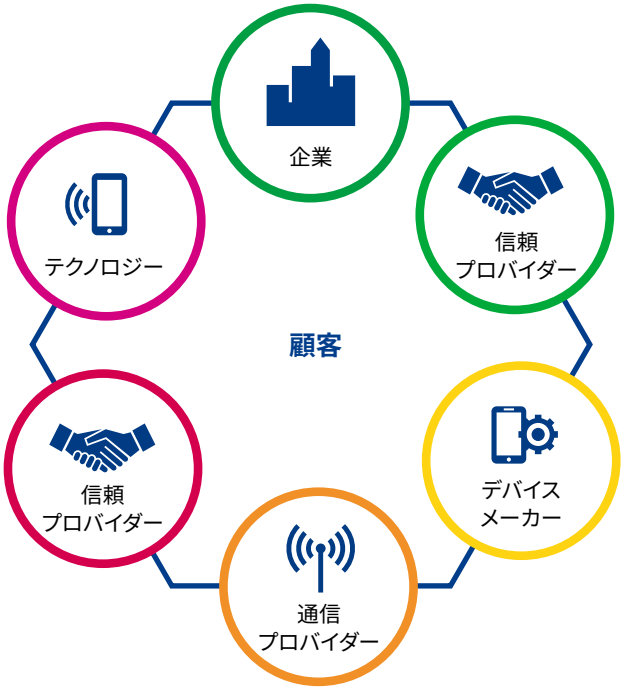
貴社のIoTソリューションには何社のサードパーティが関わっていますか？

私たちの見解

エコシステムは、顧客を終端とする線形モデルから、顧客を中心としてエコシステムのプレーヤーが取り囲むモデルにシフトするでしょう。その環境では、従来の「役割」から変化することが予想され、プレーヤーがエコシステム内および価値提案全体において異なる役割を果たしはじめると考えられます。

これまでのテクノロジーエコシステムは線形だったが...

現在のIoTエコシステムでは、プレーヤーが顧客の周りを「取り囲んで」いる



しかし、私たちのデータは、新しいバリューチェーンがIoTソリューションの全体的なセキュリティに及ぼす影響について、十分に考慮しているIoTユーザーがごく少数にすぎないことを示しています。実際、回答者の44%はサードパーティパートナーがセキュリティリスクをどの程度認識しているかについて、考えたことがないことを認めています。

「デバイスに対するサイバー攻撃は現時点で存在する実際のリスクであり、私たちはある程度の管理またはセキュリティを提供できる能力があるベンダーを選び、現在のIoTの世界を西部開拓時代とみなしているようなベンダーを避けることによって、そのリスクを軽減する必要があります」とJibestreamのChris Wiegand氏は述べています。

しかし、逆に小規模な新興企業や市場でのブランド認知度が低い企業は、エコシステム内のパートナーのおかげで、ごく短期間のうちに顧客の信頼を構築できる可能性があります。

サードパーティを評価する

しかし、IoT市場が成熟し、IoTの採用が増大するにつれて、IoTユーザーがセキュリティ、プライバシー、信頼性の保証を要求しはじめるため、エコシステム内のすべてのサプライヤーも顧客の指針や防御策に合わせて自分たちの指針や防御策を策定するようになるでしょう。組織がリモートプロセスモニタリングなどのテクノロジーやツールを導入して、サプライヤーのパフォーマンスを追跡している例もあります。整合性を確保するために、認証を取得するよう、あるいは監査を受けるようサプライヤーに求める組織もあります。

ある北米企業の最高情報責任者は、「当社では、付加的な責任として認定評価機関に当社の外部パートナーのセキュリティ標準を評価するよう依頼し、外部パートナーは当社の予算に収まる妥当な金額で評価を受けることに同意しています」と述べています。

最近では、サードパーティのセキュリティに対する心構えを評価するために、組織の統制の設計と運用効率をテストし報告する、サービス・オーガニゼーション・コントロール2（SOC2）などのサードパーティのデューデリジェンス評価や、既存の標準および認証プログラムを利用するアプローチが一般的になっています。SOC2は5つの重要な「信頼サービス原則」であるセキュリティ、可用性、処理の整合性、機密性、プライバシーに基づいて評価を行います。たとえば、米国の医療業界では、サードパーティが高レベルのセキュリティ、プライバシー、信頼性を維持しているだけでなく、HIPAAなどの重要なデータセキュリティ規制に準拠していることも確認するためにSOC2を使用することが多くなっています。

私たちの見解

エンドユーザーを保護するために「ハンドシェイク」を機能させるには、エコシステム内のすべてのプレーヤーがソリューションのセキュリティ、プライバシー、信頼性を保護する責任を負う必要があります。

5つの重要なポイント

1 **IoT市場は進化しています。**IoT業界は急速に成長しており、何度か変革を繰り返す可能性が高いと思われます。同様に、市場の進化に伴って、セキュリティ、プライバシー、信頼性に関連する懸念も高まり、変化していくでしょう。このような事情から、セキュリティ戦略は、現在の市場での地位を脅かす可能性がある潜在的な混乱を予期し、それに対応できるような包括的なものにしなければなりません。

2 **IoTエコシステムは、IoTのセキュリティを確保するうえで極めて重要な役割を果たします。**企業はサードパーティサプライヤーを入念に評価し、適格なパートナーを識別し、エコシステム全体にわたるセキュリティ、プライバシー、信頼性の統合に投資する必要があります。企業は、目標達成のために、買収、構築、提携、投資または協力関係形成の可否を含む、エコシステム内で必要とされる能力構築のためのさまざまなアプローチを考える必要があります。

3 **最初から顧客を考慮に入れてセキュリティを組み込む必要があります。**消費者とビジネスパートナーは、セキュリティがシステム内に組み込まれていることを期待するようになります。テクノロジー設計者は、「常時オン」の原則に従い、適切なフェイルセーフを備えた高いレベルの制御を提供する必要があります。IoTの成長の規模と速度を考えれば、セキュリティの脆弱性は企業にとって大きな不利益になる可能性があります。

4 **セキュリティから価値を引き出す機会を求めます。**セキュリティ設計者は、セキュリティの価値を高める可能性を洗い出すためにセキュリティモデルを再考する必要があります。たとえば、セキュリティ、プライバシー、信頼性の対価としてのプレミアムというコンセプトを利用して製品を差別化することを検討します。IoTのセキュリティとは、重要なデータを守ることだけでなく、インテリジェンスを収益化する機会を見出すことでもあります。

5 **IoTの正常化と標準化を加速させるために、業界グループや規制関連グループに参加します。**協力関係は曖昧さが減り、持続可能なビジネスエコシステム内で製品やサービスを立ち上げる企業の能力を加速します。同時に、規制当局も市場と消費者の利益を保護するために業界内の議論に参加する必要があります。テクノロジー企業は、規制当局がIoTをサポートできるように積極的に取り組むべきです。

KPMGサイバーセキュリティアドバイザリーグループ

cybersecurity@jp.kpmg.com
www.kpmg.com/jp/cyber-security

Designed by Evalueserve.

Publication name: Security and the IoT ecosystem

Publication number: 132631-G　Japan 16-1504

Publication date: December 2015