www.pwc.com/jp

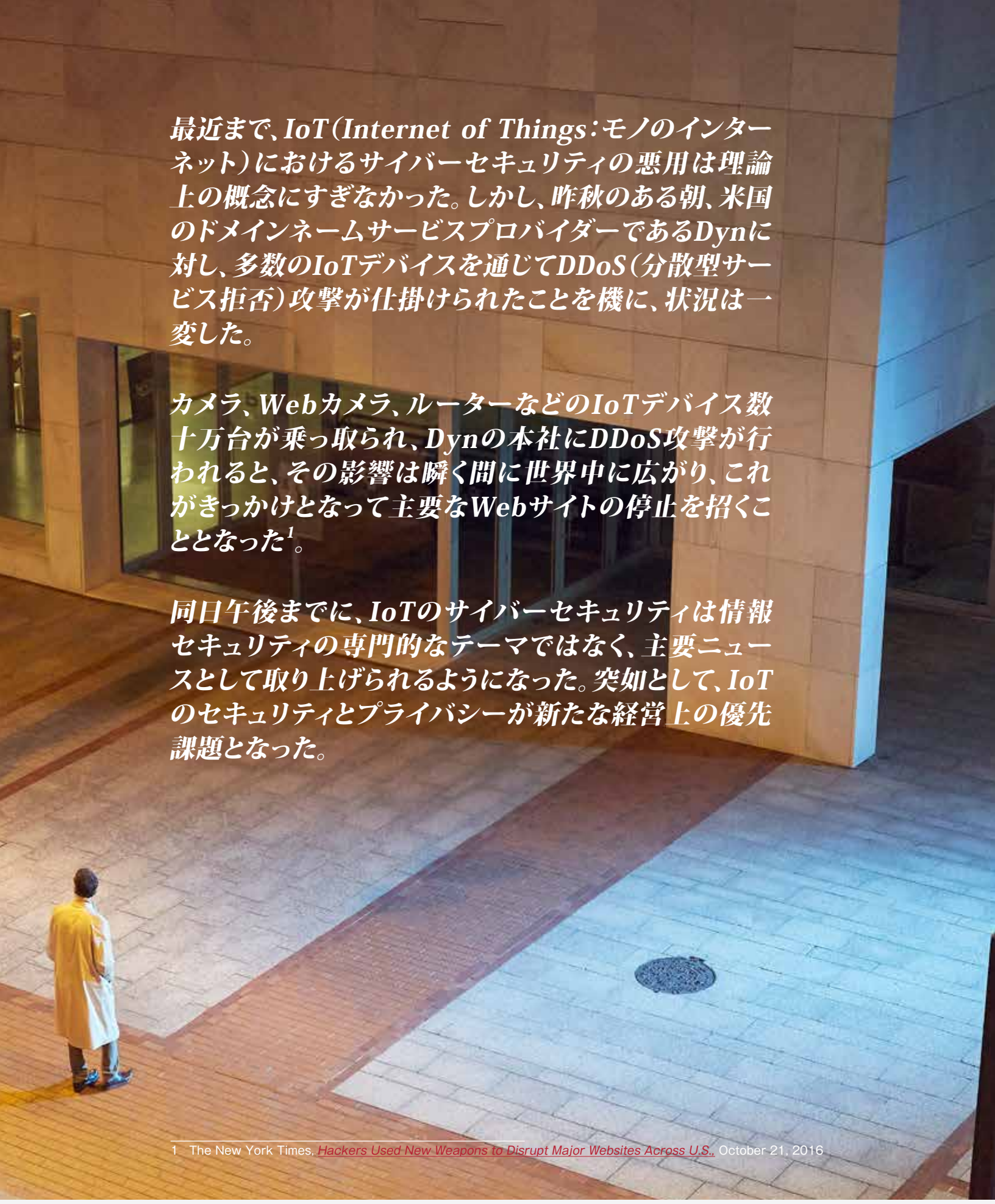
IoTの可能性を探る

サイバーセキュリティ対策は
IoTの未来を具現化できるのか？

グローバル情報
セキュリティ調査2017
The Global State of
Information Security®
Survey 2017 Vol.3

pwc

目次



最近まで、IoT（Internet of Things：モノのインターネット）におけるサイバーセキュリティの悪用は理論上の概念にすぎなかった。しかし、昨秋のある朝、米国のドメインネームサービスプロバイダーであるDynに対し、多数のIoTデバイスを通じてDDoS（分散型サービス拒否）攻撃が仕掛けられたことを機に、状況は一変した。

カメラ、Webカメラ、ルーターなどのIoTデバイス数十万台が乗っ取られ、Dynの本社にDDoS攻撃が行われると、その影響は瞬く間に世界中に広がり、これがきっかけとなって主要なWebサイトの停止を招くこととなった[1]。

同日午後までに、IoTのサイバーセキュリティは情報セキュリティの専門的なテーマではなく、主要ニュースとして取り上げられるようになった。突如として、IoTのセキュリティとプライバシーが新たな経営上の優先課題となった。

1 The New York Times, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, October 21, 2016

今後のコネクテッドデバイスの普及に伴い、セキュリティ侵害リスクの増大が見込まれる。「Gartner, Inc.の予測では、世界で使用されるコネクテッドデバイスの数は2017年までに84億台（2016年の31％増）、2020年までに204億台に達する」[2]。グローバル情報セキュリティ調査2017では、回答者の約4分の1がオペレーショナルテクノロジー（OT）、組み込みシステム、消費者向けデバイスのようなIoTコンポーネントへの侵入を経験したと答えた。

46%

本年、IoTへの投資を計画している回答者の割合

PwC、CIOおよびCSO、*グローバル情報セキュリティ調査2017*、2016年10月5日

IoTがデジタルビジネスの中核へと近づくにつれ、IT、OT、消費者向けテクノロジーといったセキュリティ領域の統合が新たな問題となりそうだ。例えば、コネクテッドデバイス間での情報連携の寸断や、装置との物理的干渉、事業運営への影響、機密情報の窃取、個人データの漏洩、重要インフラストラクチャーの損傷、そして人命の喪失さえ発生するおそれがある。

2 Gartner Press Release, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, February 7, 2017

しかし、統合されたIoTサイバーセキュリティプログラムを提供している企業はまだほとんど存在しない。理由としては、実装標準やフレームワークが遅々として定まらないことが大きい。とはいえ、最近になって指針を示す動きが見られ、DHS（米国国土安全保障省[3]）およびDoC（米国商務省[4]）からIoTガイドラインに関するホワイトペーパーが発表された。

セキュリティのみならず、特にIoTデバイスを使用して取得した情報の収集、保管、使用に関連して、IoTの実装には多くのプライバシーに関する課題がある。企業が収集および使用するIoTデータに個人情報が含まれる場合、または収集した情報によって個人の活動が詳細に把握できる場合、データ処理に伴うリスクを考慮しなければならない。IoTセキュリティやプライバシーは新しいテーマであることから、ほとんどの企業では自社でプログラムを設計、展開、運用する経験やリソースが乏しい。

このような環境にあっても、多くの企業がセキュリティとプライバシーの両方の対策を講じ始めている。本年のグローバル情報セキュリティ調査では、IoTのセキュリティ戦略を立案済みとする回答が35％、また立案中とする回答が28％だった。さらに回答者の46％が今後12カ月でIoTのセキュリティ投資を行うと述べた。その内容は、新しいデータガバナンスポリシーの策定、デバイスおよびシステムの相互接続性および脆弱性の評価、従業員教育、統一されたサイバーセキュリティ標準およびポリシーの策定などである。

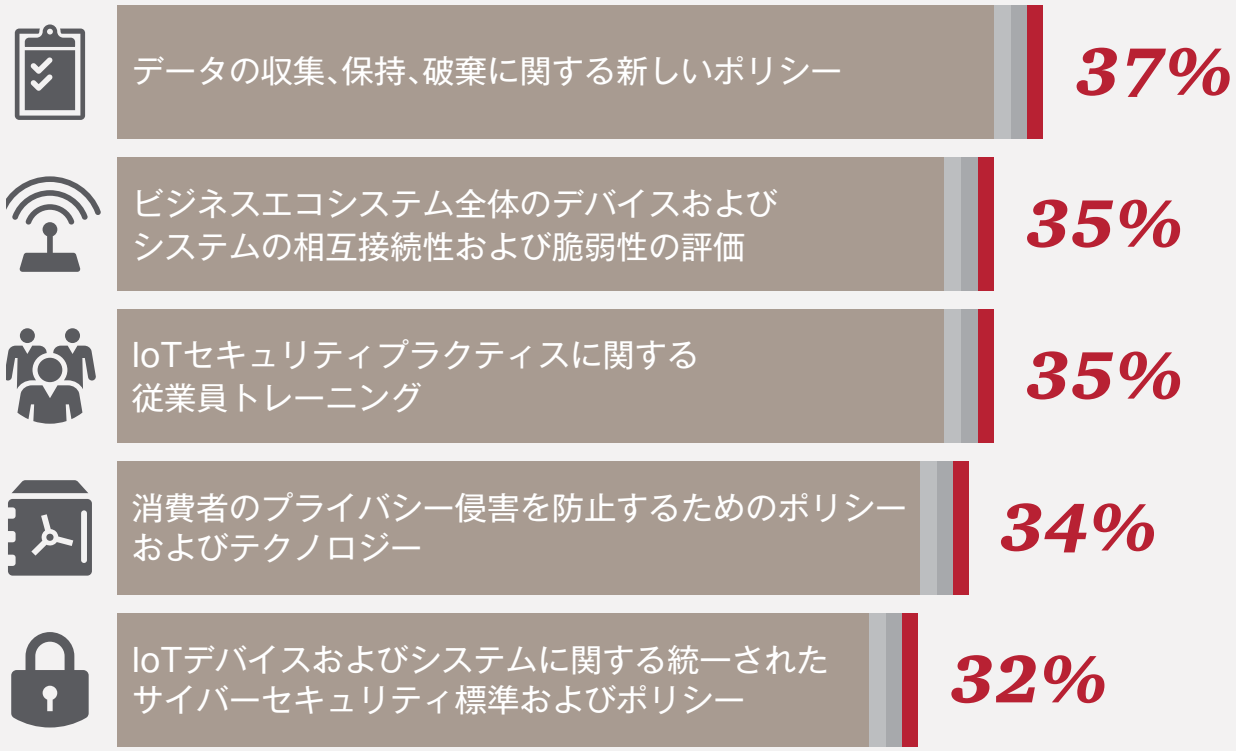
35%

IoTのセキュリティ戦略を立案済みの回答者の割合

PwC、CIOおよびCSO、*グローバル情報セキュリティ調査2017*、2016年10月5日

3 US Department of Homeland Security, Strategic Principles for Securing the Internet of Things, November 2016
4 Department of Commerce, Fostering the Advancement of the Internet of Things, January 2017

今後12カ月に実装する IoTポリシー、テクノロジー、スキル



出典：PwC、CIOおよびCSO、*グローバル情報セキュリティ調査2017*、2016年10月5日

これらのプログラムに加え、組織は新しいソフトウエアやデバイスの設計当初からサイバーセキュリティとプライバシーを考慮する手続きを定める必要もある。既にコネクテッドデバイスのソフトウエア開発戦略を練り直し、より柔軟なサイバーセキュリティ機能に重点的に取り組んでいる企業もある。*「未来志向の企業は、IoTデバイスのコード記述方法を見直している」*と、PwCのGlobal Cybersecurity and Privacy Advisory Leader、David Burgは語る。*「クライアントが求めているのは、製品そのもののサイバーセキュリティ機能の継続的な向上を容易に行えるような、開発環境の構築だ」*

経営陣は、デバイスのみならず、ITシステムのセキュリティの裏で長年後回しにされてきたOTも含め、領域全体の状況や脅威を積極的に監視し、評価できるように準備を整えておくべきである。*「私たちはIoTの三つの領域全体で何が起こっているのかがよく見えるように、クライアントを支援している」*とPwCのBurgは説明する。*「三つのレイヤーの間に亀裂が入る前に、その継ぎ目のひびを発見できなければならない」*

統合されたテクノロジーに対するサイバーセキュリティとプライバシーの取り組みが始まったのは朗報だが、まだ手付かずの領域も多く残っている。IoTサイバーセキュリティとプライバシープログラムを統合して実装することに積極的な企業は、不可避のリスクを管理し、ビジネスモデルを変えるような新製品やサービスを創出できる準備が整えられていると言える。以下では、企業がどのようにIoTのセキュリティ対策を行い、将来のチャンスに備えているかを見ていくこととする。

本書は、4部構成のグローバル情報セキュリティ調査2017の第3部である。第1部の「Moving forward with cybersecurity and privacy」および第2部「Toward new possibilities in threat management」では、デジタル企業がサイバーセキュリティの新しいテクノロジーやプロセスをどのように導入して脅威に対応しているかに注目した。最後の第4部（英語版のみ）では、地政学的脅威の管理を取り上げている。

IoTの競争優位性

IoTがこの10年における大きなかく乱要因であることは間違いないようだ。一般的に、プラットフォームの相互接続によってビジネスモデルが変わり、消費者の暮らしをより快適で安全なものにする革新的な製品やサービスが生まれることが、大きな経済成長につながると考えられている。

潜在的な利点はほぼ無限に広がる。デジタルファーストの世界では、IoTによりオペレーションの改善、消費者との関係の再定義、まったく新しい収益源の創出が起こるとされている。消費者の間では、デジタルとの融合によってこれまでにない生活の利便性が得られ、医療の向上、住宅や自動車の制御が可能となる。政府や地方自治体はIoTテクノロジーを活用し、街灯や交通監視、インテリジェントビルといったインフラストラクチャーをデジタル接続した“スマートシティ”を作り出し、市民の生活の質の向上とコストの削減を目指す。

このような根底からの変化は、ほぼ全ての業界の企業に歓迎され、消費者からは大きな期待が寄せられている。コネクテッドカーを例にとって考えてみよう。完全な自動運転車の登場はまだ数年先のことだが、現時点での新型車両には、車載コンピューターやセンサー、カメラ、ソフトウエアによって可能となった自動運転機能が実装されている。これらのテクノロジーがインターネット接続、死角モニタリング、リアルタイムのナビゲーション、車線逸脱警告、車両診断を可能にしている。未来の自動運転車では、アニメ番組で描かれる未来世界のような利便性、予測ベースのメンテナンスによる維持費の削減、運転の安全性の向上が実現されると考えられている（11ページの関連記事参照）。

46%

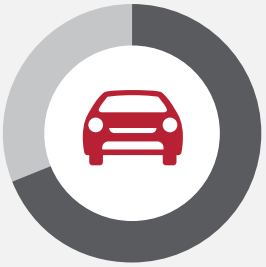
ビジネスモデルの進化に関連する新たなセキュリティニーズへの投資を計画している回答者の割合

PwC、CIOおよびCSO、*グローバル情報セキュリティ調査2017*、2016年10月5日

IoTサイバーセキュリティ戦略の立案に積極的な業界

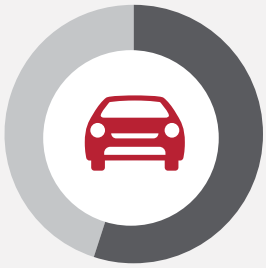
78%
通信

73%
IT



69%
自動車

来年、IoTセキュリティへの投資を計画している



55%
自動車

55%
工業製品

53%
IT

出典：PwC、CIOおよびCSO、*グローバル情報セキュリティ調査2017*、2016年10月5日

また、IoTにより、医療機関がどのように患者を見守り、相互にやりとりし、治療するかも変わるとみられている。現在、医療エコシステムには、医療用モニター、病院用“スマート”ベッド、遠隔医療、ペースメーカー、血糖モニターのような接続された医療用機器が含まれている。これらのコネクテッドデバイスおよび医療用装置は、看護の向上や健康促進、さらには将来の疾病傾向の予測にも役立つとされている（12ページの関連記事参照）。

厄介な点：なぜセキュリティは“動く標的”なのか

IoTは、法律や基準による規制が及んでいない、サイバーセキュリティおよびプライバシーにおける“未開の地”だ。事実、どの組織がプラットフォームの所有者としてセキュリティの最終責任を負うかについて、世界的な合意は形成されていない。

*「IoTが急速に広がるとともに、よく理解されておらず、劇的な影響を及ぼしかねない新たなリスクが生じてきている」*と、PwCのUS Cybersecurity and Privacy Leader、Sean Joyceは警鐘を鳴らす。*「サイバーセキュリティおよびプライバシーのリスク管理は、コネクテッドデバイスの開発や選定が終わった後に考えるものではない。最重要課題として真っ先に取り組むべきものである」*

とはいえ、これは至難の業だ。IoTは全体として見れば、異なるオペレーティングシステム、通信プロトコル、ハードウエア仕様の異なる何十億ものデバイスや設備で構成されている。IoTサイバーセキュリティおよびプライバシーのフレームワーク作成に着手しようとしても、その膨大さと複雑さに二の足を踏まざるを得ない。単純に社内に専門知識がないためである。仮にサードパーティーベンダーがフレームワークやその追加フレームワークを作成したとしても、その多くは相互に連動せず、機能しない。

35%

ビジネスエコシステム全体のデバイスおよびシステムの相互接続性および脆弱性の評価を計画している回答者の割合

PwC、CIOおよびCSO、*グローバル情報セキュリティ調査2017*、2016年10月5日

同様に、既にエコシステムに組み込まれている多くのデバイスに対する標準も存在しない。IT装置とは異なり、コネクテッドデバイスは設計時にセキュリティが考慮されていないため、リスクが野放しのままだ。HPE Fortify on Demandによると、一般的に使用されているコネクテッドデバイス10種を検証した結果、70％に重大な脆弱性が見つかったということだ[5]。多くのデバイスには暗号化や認証、自動パッチ適用のような重要なテクノロジーを処理する能力がないため、このような欠陥に対応するのはたやすいことではない。付け加えるならば、これらのデバイスの多くは、セキュリティを考慮せずに設計、開発されていた。

その一方で、オペレーショナルテクノロジーやインフラストラクチャーシステムの寿命は数十年にも及ぶ。かつて活躍したレガシーシステムの更新が、いまや大きな負担となることもある。仮に更新ができたとしても、そのほとんどは寿命が近づいている。さらに、これらのレガシーシステムには、異なる新しいシステム、ソフトウエア、通信プロトコルとの間に相互運用性もない。

もう一つの問題は、IoTがまったく新しいリスクをもたらすということだ。コネクテッドデバイスは物理装置と頻繁にやりとりしているため、オペレーションが変更されることによって物理的破壊や人的被害を招くおそれがある。人命にもかかわる重大な物理的破壊が電力網や医療用機器、製造工場で使用されているIoTコンポーネントによって引き起こされる可能性について、既に研究者が証明していることを肝に銘じるべきである。

*「IoTデバイスが私たちを取り巻く環境に浸透すれば、付随するリスクも飛躍的に増加する」*とPwCのChris Hallは指摘する。*「企業も個人も、今よりももっとリスクへの対応方法を学ぶ必要がある。デフォルトのパスワードを変更するといった単純な対策もあれば、ネットワークセグメンテーションやデバイス管理などの複雑な対策もある。何も対策をとらないのは、誇張ではなく、もはや生死にかかわる重大な問題となりつつある」*

5 HPE Fortify on Demand, Internet of Things State of the Union Study, July 2014

コネクテッドカーの保護を急ぐ自動車メーカー

IoTに関して何よりも人々の想像を熱くかきたてるのが、自動運転車だ。思い描かれているのは、自動運転車の登場により交通事故が減り、渋滞が緩和され、低燃費でメンテナンスが簡易になることで、毎日の通勤・通学が楽になるような未来図だ。

広く報道されたおかげで、ハッキングのリスクもよく知られるようになった。

熟練したハッカーであればコネクテッドカーを遠隔地から乗っ取り、ブレーキをかけたり、エンジンを停止したり、ハンドルを制御したりすることが可能だということが証明されている。サイバー犯罪者が車載テレマティクスにアクセスし、車両とドライバーに関する機密情報を盗み出す可能性もある。そのようなハッキング事例は現時点では報告されていないが、噂は絶えない。

その一方で、自動車メーカーは他社との競争に勝つために自動運転に取り組んでおり、多くがセキュリティおよびプライバシーを重視するロードマップに従っている。本年の調査では、自動車業界の回答者の半分以上（54％）が車載テレマティクスを可能にする製品やサービスの製造または販売を行っていると答えた。そのうち81％は、サービスの安全な提供に自信を持っている。ほとんどの場合、テレマティクスのセキュリティフレームワークやアーキテクチャの開発は、従来のIT部門に委ねられている。

自動車メーカーやOEMメーカーは、リアルタイムの車両診断データを取り込んで使用できるようにしている。リモート車両診断に資金を投じる企業のうち、既に半数が診断モニタリング機能を導入し、74％がテレマティクスデータのセキュリティ計画を策定している。

テレマティクスデータからは個々の車両やドライバーの詳細を知ることができ、その中には消費者データプライバシーに影響する機密情報も含まれている。回答によれば、約3分の2（65％）がテレマティクスシステムから車両位置情報を、44％がドライバーのデータを収集している。

データを収集して終わりではない。4分の1以上（28％）が既にテレマティクス情報の販売を手掛けており、さらに25％が今後24カ月で販売を計画しているという。買い手は引く手あまただ。保険会社、弁護士、法執行機関、自動車補修部品を扱うOEMメーカーなどは、テレマティクスデータを何としても入手したがっている。

デバイスが患者とより良い医療をつなぐ

誰でも一度くらいは、1日1万歩の健康法について聞いたことがあるだろう。多くの健康を気にしている人々は、このウェアラブルデバイスのメーカーが設定した目標値を達成しようと汗をかいている。

フィットネストラッカーは最も分かりやすい健康のためのコネクテットデバイスであるが、企業も個人も、組み込みの血糖モニターやペースメーカー、高齢者向けモニタリングシステム、院内手術システム、遠隔治療機能など、より洗練された先進的なIoT装置を使い始めている。

本年のセキュリティ調査では、医療従事者や提供者の44％がオペレーショナルシステムおよびウェアラブルデバイスをITインフラストラクチャーに統合したと答えた。IoTを構成する三つの領域が実質的に融合されたことになる。また、そのうち68％はウェアラブルデバイスからデータを収集していると答えている。

多くの回答者がセキュリティおよびプライバシーリスクに対応していると答えたのは喜ばしいことだ。64％がコネクテットデバイスおよびテクノロジーのリスク評価を実施して潜在的なセキュリティ脆弱性を評価し、半数以上（55％）がコネクテッドデバイスのセキュリティ管理策を実装したと回答した。

情報過多のリスク

現在、IoTによって生成されるデータの多くは匿名であり、機械間での意味のないメッセージだ。しかし、IoTエコシステムにデータが蓄積されるにつれて、コネクテッドデバイスを使用する消費者個人の機微情報がそこから取り出される可能性は、徐々に高まってきている。

既にスマートフォンやフィットネストラッカー、車載テレマティクス、住宅監視システムから膨大な量のデータが生み出され、個人の位置や行動がデジタル情報として記録されている。このようなデータを使用して消費者の行動を分析したり、消費者の好みに合わせてサービスをパーソナライズしたりすることで、多くのビジネスチャンスが生まれる。ただし、目的を明示せずに個人データを分析する行為や、適切な通知を行わずに個人データをサードパーティーに提供する行為は、消費者保護および安全に関する規制に違反するリスクを伴う。当該規制には連邦取引委員会（FTC）による規制も含まれる。FTCは消費者を不公正または不正な取引から保護するための広い権限を持ち、プライバシーおよびセキュリティ規制に関する主導的な役割を担っている。

*「企業は、まず初めにIoTデバイスを通じて収集したデータの取得、保存、使用によるプライバシーへの影響を考慮し、その上でオンライン保存する個人情報のセキュリティおよびプライバシーに対応したデータガバナンスを構築すべきだ」*とPwCのPrincipal、Jocelyn Aquaは述べている。

さらに、データの倫理的な使用という新たな規律についても考慮しなければならない。既存のプライバシー規制では、多くの企業がこれに対応できないためである。企業が収集、分析する情報の範囲が拡大するにつれて、許容されるデータ使用の線引きが知らず知らずのうちに曖昧になっていく可能性がある。例えば、職場から住居までの距離を調べるため、採用の判断基準の一つに応募者の住所が含まれているとしよう。それ自体は問題がなくとも、この情報が非倫理的に使用されることにより、人種や性的指向性、宗教に基づいた不採用の判断が行われるおそれもある。一般的にこのような属性は住所からある程度推測できるからだ。

規制当局がIoTで生成されたデータに目をつけ、厳しい罰金と改善義務を課そうとしているのも当然だ。EUの一般データ保護規則（GDPR）では、EUで設立され、個人データを処理し、商品またはサービスの提供やEU居住者の行動をモニターする全ての企業に対し、広範囲に及ぶデータプライバシー要件を定めている。当該保護規則では、個人データの一般的な定義を拡大し、位置情報やIPアドレスといった要素も含めている。2018年5月の施行後、GDPR違反に対する罰金として、最大で年間売上高の4％が科せられる可能性がある。

「企業は、まず初めにIoTデバイスを通じて収集したデータの取得、保存、使用によるプライバシーへの影響を考慮し、その上でオンライン保存する個人情報のセキュリティおよびプライバシーに対応したデータガバナンスを構築すべきだ」（PwC Principal、Jocelyn Aqua）

米国では、FTC（連邦取引委員会）が消費者の許可を得ずに位置情報データを記録したモバイル広告企業と和解に至った[6]。この企業は罰金95万米ドルを科され、明示的な同意を得ることなく消費者から位置情報を収集することを禁じられた。また、今後20年間にわたり、包括的なデータプライバシープログラムを実装し、これに対して2年ごとの独立監査を受けることも義務付けられた。

6 Federal Trade Commission, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission, June 22, 2016

IoTサイバーセキュリティ構築に向けた取り組み

多くの企業にとって、IoTは見逃せないビジネスチャンスだ。新たなプラットフォームが変化のきっかけとなり、競争優位性、運用効率の向上、新たな収益源の創出の手段になるとみられている。

問題は、サイバーセキュリティ対策を実装する前にIoTに飛びつく企業が多いことだ。たしかにIoTの標準がないことは大きな問題だが、乗り越えられないほどではない。既存のベストプラクティスに従い、IoTサイバーセキュリティの基礎を構築することは可能だ、とPwCのShawn Connorsは言う。

「ビジネスエコシステムでサイバーセキュリティに関する技術的対策が統一されず個別に導入されている現状を考えると、IoTで生成または処理されるデータの識別、保護、管理に向けて、テクノロジー製品のパートナーとの話し合いを始めるべきだ」「既にある企業内のテクノロジーが、IoTネットワーク内外でのデータフローの管理と保護にすぐに応用できることに、多くの企業が気づくであろう。ニッチな領域にフォーカスしたベンダーに目を光らせておくことも重要だが、IoTが企業内のデータ管理に問題を起こす可能性があることも踏まえ、まず自社を熟知しているベンダーと、対策について話し合うことから始めるとよいだろう」（Connors）

IoTサイバーセキュリティへの取り組みでは、まずビジネスエコシステム全体で使用されている全データを入念に評価するべきだ。拡張IoTプラットフォーム、サードパーティーパートナー、通信ネットワークも含めてである。データの価値、データ資産の数と種類、データの保存や伝送の場所、アクセス権を持つユーザー、漏洩した場合の影響について、企業が厳密に把握する必要がある。個人情報の使用は、その収集時の目的のみに限定されなければならない。

「ビジネスエコシステムでサイバーセキュリティに関する技術的対策が統一されず個別に導入されている現状を考えると、IoTで生成または処理されるデータの識別、保護、管理に向けて、テクノロジー製品のパートナーとの話し合いを始めるべきだ」（PwC Principal、Shawn Connors）

“プライバシー・バイ・デザイン”の概念はベストプラクティスとみなされているが、GDPRでは義務となる。このアプローチでは、製品およびサービスの開発者は、最初から本当に必要な個人情報を検討し、個人の特定が可能なデータの最小化、匿名化、もしくは曖昧にするような仕組みを実装することが求められる。企業はこのルールを徹底させつつ、製品またはサービスが意図したとおりに動作するために、設計者には、必要最小限の個人情報に対するアクセスのみを許容しなければならない。

多国籍企業の場合、国境を越えた個人情報の移転が規制上の義務に違反しないように、プロセスや管理策を実装する必要がある。そのためには、各地域の最新のデータプライバシー規制、倫理的な情報利用に関する最新の解釈を、常に把握しておくことが不可欠である。GDPRへの対応に加え、企業は法令上のステークホルダーにも適切なプライバシー対策が実装されるよう、慎重に協力していくべきである。

データのほか、コネクテットデバイスのセキュリティ機能の評価も欠かせない。IoTプラットフォームが成熟してコネクテッドデバイスが普及すれば、企業がその全てを評価することは困難だろう。とはいえ、重要でかつリスクにさらされている装置については識別、棚卸しした上で、セキュリティ機能について評価を行うべきである。この評価は、ネットワーク、アプリケーション、データ、物理の各レイヤーで行い、コネクテッドデバイスの弱点と、それをどのようにハッカーが悪用するかを把握するために、倫理的なハッキングによる検証や脆弱性テストも行う必要がある。

サービスとデバイスの間のエントリーポイントの潜在的な脆弱性も慎重に評価する必要がある。サイバー犯罪者は時に、モバイルデバイス、Webインターフェイス、クラウドシステム間のAPIにおける弱点を突いて、ネットワークやシステムへの侵入の足掛かりとするのである。

前述のように、特に懸念されるのはオペレーショナルシステムの寿命だ。OT装置の管理はITシステムの管理と同じルールで行われないことも多く、パッチ適用や更新が何年も行われていないこともある。また、最小限の機能のみを搭載した新しいコネクテッドデバイスは、自動パッチ適用に対応していないことも多い。このような現状にあっても、企業は重要な装置を可能なかぎりアップデートするプロセスを構築し、IoTデバイスに対するソフトウエアパッチの適用を脆弱性管理ポリシーに含めなければならない。システムが古すぎてこのような自動更新ができない場合、社内のセグメント内に置いてリスクを低減することもできるだろう。加えて、当該デバイスを重点的に監視し、システムの健全性同様、異常な動作についても警告が出るようにしておくべきである。

「既にある企業内のテクノロジーが、IoTネットワーク内外でのデータフローの管理と保護にすぐに応用できることに、多くの企業が気づくであろう。ニッチなベンダーに目を光らせておくことも重要だが、IoTが企業内のデータ管理に問題を起こす可能性があることも踏まえ、まず自社を熟知しているベンダーと、対策について話し合うことから始めるとよいだろう」（PwC Principal、Shawn Connors）

ITおよびOTインフラストラクチャーと同様に、IoTコンポーネントにおいても、特権アカウントの悪用による脆弱性があると言える。特権アカウントが悪用されると、機密データ、システム、デジタル資産への侵入をいとも簡単に許してしまうためである。多くの企業では、IT環境においてさえ、特権アカウントのリスクは見過ごされている。そのため、十分なサイバーセキュリティ対策が取られていない特権アカウントが、意図せずIoTデバイスに割り当てられてしまうこともある。基本的な予防策として、特権アカウントが割り当てられているデバイスには強度の高いパスワードを使用する、IT管理者間で特権アカウントの共有を制限する、といったものが挙げられる。

既存テクノロジーを活用したサイバーセキュリティの統合

IoTのサイバーセキュリティ対策のために、必ずしも新規のテクノロジーやソリューションを導入する必要はない。既存のIT環境に対するサイバーセキュリティ対策にIoT基盤を組み込んでいくことから始めることもできるのである。

IDが人間やアプリケーションからコネクテッドデバイスへと移るにつれ、アイデンティティ／アクセス管理（IAM）がますます重要な機能になってくるであろう。IoTエコシステムで使用されるIDが膨大な数に上るにつれ、全てのドメインにわたってセキュリティポリシーをシームレスに適用する機能に加え、データへのアクセス権限の付与、削除についても統一された方法が求められるようになるだろう。

機密データを保存または伝送するコネクテッドデバイスを保護するために、IAMソリューションに強度の高いユーザー認証を組み込むことの重要性が高まってきている。当該認証では、付与する権限の最小化、権限分離による職務分掌担保を原則とすべきである。多要素認証やバイオメトリクスは人間に対してのみ有効であると言えるものの、その技術はインフラストラクチャーのセキュリティ向上にも役立つであろう。

また、暗号化もプライバシーデータの保護に不可欠な技術である。ただし、前述のように、基本的な機能しか備えていないコネクテッドデバイスには、暗号鍵の管理に必要な処理能力がない可能性もある。それでも、可能なかぎり強力なデータ暗号化アルゴリズムを実装し、暗号鍵が平文で表示されないようにする必要がある。また保存時も伝送中も、全ての個人データを可能なかぎり暗号化することが求められる。いかにコストや複雑性を増やさず、データ処理速度を低下させずに実現するかが、今後のチャレンジとなるだろう。

43%

今後12カ月でバイオメトリクスや高度な認証への投資を計画している回答者の割合

PwC、CIOおよびCSO、*グローバル情報セキュリティ調査2017*、2016年10月5日

未来指向の企業はエンタープライズセキュリティアーキテクチャ（ESA）により、あらゆるドメインのコンポーネントに組み込まれたIoTセキュリティの実現に取り組んでいる。ESAは、IoTによって新たにセキュリティスタックに加わるレイヤー（センサー、新たなネットワーク、処理プラットフォーム、サービスプラットフォーム）の統合と保護に特に有用だ。ESAによって、企業はこれらの新たなレイヤーに適切な管理策を適用し、ネットワークレイヤーや通信チャネルといった共通の基準を活用することでエンタープライズスタックに統合することができる。

人材：サイバーセキュリティの“アキレス腱”

サイバーセキュリティの取り組みの強度は、最も弱い部分で決まる。多くの場合、サイバーセキュリティおよびプライバシーに関する手順について十分なトレーニングを受けていない従業員がこの最弱部となる。従業員は昔から、セキュリティインシデントの主因となってきた。悪意を持って故意にインシデントを引き起こす場合もあるが、多くの場合不注意によって、もしくは基本的な注意事項の認識不足によってインシデントが起きている。

従業員トレーニングがサイバーセキュリティプログラムの基本中の基本であるという認識は広まってきているものの、本年の調査でも、従業員認識向上プログラムを整備しているとの回答は半数強（53％）にすぎない。IoTセキュリティのためのトレーニングはまだ多くの組織で当然のものとはなっていないが、本年、IoTサイバーセキュリティに関する従業員トレーニングへの投資を計画していると答えた回答が35％に上ったことは朗報だ。

最大限の効果を得るためには、個々の企業の脅威、対応準備状況、プロセスに合わせたトレーニングを実施すべきだ。経営幹部がセキュアなビジネス環境の重要性を積極的に説いてこそ、セキュリティ文化の醸成が最大の効果を発揮できる。*「組織の風土はトップから作り、セキュリティトレーニングを企業の将来に本当に直結することとして行っていかなければならない」*とPwCのGlobal Cybersecurity and Privacy Assurance Leader、Grant Waterfallは述べる。*「トレーニングを企業の目的と結び付けるべきであり、認識向上プログラムもこれに沿うものとして設計する必要がある」*

35％

今後12カ月でIoTの従業員トレーニングへの投資を計画している回答者の割合

PwC、CIOおよびCSO、*グローバル情報セキュリティ調査2017*、2016年10月5日

従業員のトレーニングとは別に、IoTサイバーセキュリティには、従来のITセキュリティを超える新たなコンピテンシーを持つ専門の人材が必要とされるだろう。例えば、セキュリティの実務にあたる従業員には、組み込みデバイス、センサー、機械間通信の実務的な知識が必要だ。オンプレミスのインフラストラクチャー内とクラウド環境の両方で、データ伝送、通信、ネットワーキングの各種プロトコルを統合した経験を持つことも望ましい。膨大な量のデータから得られる洞察を、ノイズから区別する能力と同じように、さまざまなシステムやドメインから収集したデータの品質を向上させるため、アルゴリズムの専門知識も求められるだろう。

動的なIoTのリスクを管理することは、IoTセキュリティを作り出し、実装し、管理するために必要な人材のいない企業にとって、取り組むべき最優先の課題となるだろう。社内リソースを駆使して包括的なサイバーセキュリティプログラムを開発するよりも、IoTを専門とするセキュリティサービスプロバイダーに委託することを選択する企業もあるだろう。セキュリティサービスプロバイダーは、IoTセキュリティおよびインフラストラクチャーに特化した専門知識を提供することによって、世界規模のセキュリティ人材不足解消に寄与し、さらにセキュリティ予算に対する不満を和らげることにもなるだろう。

未来に向けて点と点をつなぐ

IoTは新しいビジネスモデルを一新し、世界経済を激変させ、社会に前例のない利便性をもたらそうとしている。IoTの潜在的な利点を実現するためのカギとなるのは、統合されたサイバーセキュリティおよびプライバシーの取り組みだ。新しいサイバーセキュリティ標準と既存の対策を用いてIoT製品とシステムの開発を連携させられる企業が、未来の相互接続プラットフォームにおける利点をいち早く享受し、幸先の良いスタートを切ることになるだろう。

日本企業への示唆

本セクションは、The Global State of Information Security® Survey2017にご協力いただいた日本企業205社のデータを、PwC Japanグループが独自に分析し、グローバルとの比較を通じて、日本企業が今後取り組むべきサイバーセキュリティのポイントをまとめたものである。

1.日本におけるIoTセキュリティ戦略の重要度の高まり

2017年6月、「未来投資戦略2017～Society5.0の実現に向けた改革～」が閣議決定された。テクノロジーの発展によって、異なる種類の無数のシステムが相互に結び付くIoTの世界が広がり、そこで生成・収集されたビッグデータを人工知能によって高精度に分析する。日本政府は、このような技術を積極的に活用することで、さまざまな課題を解決するための社会基盤の構築を目指している。そのため、悪意あるサイバー攻撃にも屈しない安定的なシステムを構築することが必達目標であり、もはや国家戦略の一部であると言える。

このような背景を踏まえ、総務省はサイバーセキュリティタスクフォースを組成し、2017年10月に「IoT総合セキュリティ対策[7]」を公表した。本対策は2017年4月に同タスクフォースが取りまとめた「IoTセキュリティ対策に関する提言」に基づき、具体的な施策のありようを整理したものである。ここでは、内閣官房サイバーセキュリティセンター（NISC）などの先行成果に基づいて、IoTを構成する四つの層（サービス層／プラットフォーム層／ネットワーク層／機器層）における諸課題が定義された上で、これらの課題を解決するための具体的な施策群が以下の五つのカテゴリに分類されている。

（1）脆弱性対策に係る体制の整備
（2）研究開発の推進
（3）民間企業などにおけるセキュリティ対策の促進
（4）人材育成の強化
（5）国際連携の推進

7 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000126.html

「IoT総合セキュリティ対策」に記載された内容の大半は、今後、日本政府が中心となって検討・推進すべき諸事項という体裁で整理されている。しかし、これらは単に政府のアジェンダであるだけでなく、今後、IoT機器を生産・供給するメーカーや関連するサービス提供事業者などの民間企業にとっても、製品の品質確保や競争力の高いサービス設計などの面で非常に示唆に富むものとなっている。

一方、本年度のPwCグローバル情報セキュリティ調査では、日本企業の多くは、「ビジネス目標に適したセキュリティ戦略の展開」に意欲的であるが（図1）、政府が掲げる未来投資戦略に直接的に関係する「IoTに関するセキュリティ戦略／投資」については、いまだ本腰が入っているとは言えない（図2）ことが判明した。

図1：今後1年間でビジネス目標に適したセキュリティ戦略の展開に向けた投資を重視すると回答した企業の割合

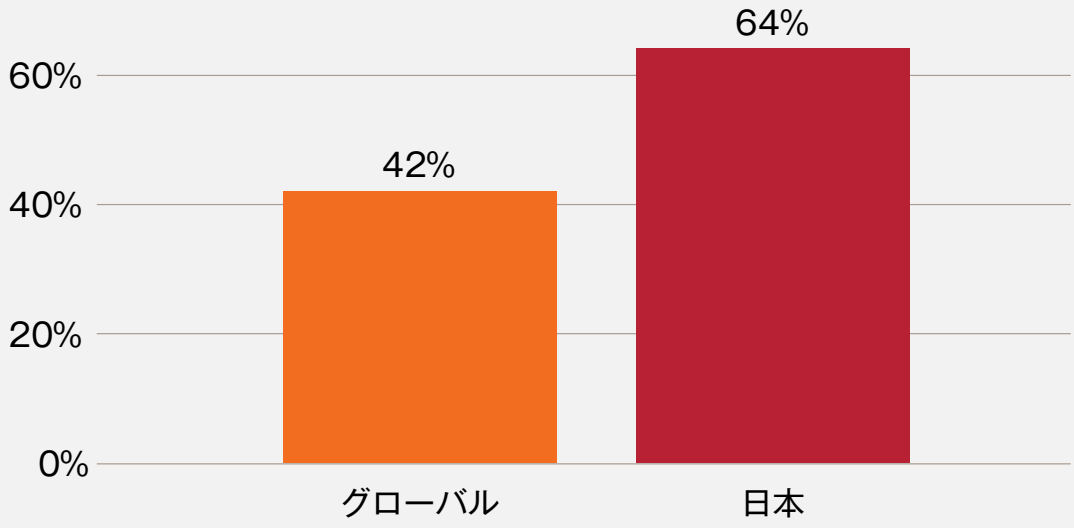


図2：

20%

セキュリティ投資計画にIoTセキュリティを含めていると回答した日本企業の割合

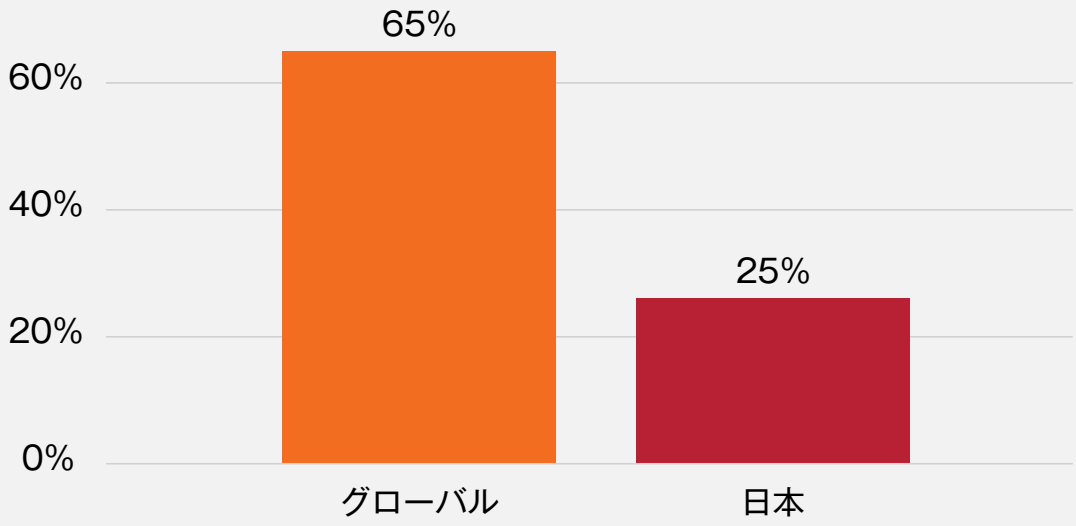
2．グローバル情報セキュリティ調査結果から見る「IoT総合セキュリティ対策」

総務省の「IoT総合セキュリティ対策」では、IoT機器の脆弱性対策を機器のライフサイクルに応じて検討することの重要性が記されている。本報告書では、より具体的なイメージを持っていただくため、機器のライフサイクルを＜研究開発＞、＜製造＞、＜市場利用＞、＜廃棄＞の四つのフェーズに分類した上で、各フェーズにおける重要なポイントを解説する。

①:研究開発フェーズ

研究開発フェーズにおける最も重要な取り組みは、セキュア・バイ・デザインの実践である。つまり、サイバー攻撃の脅威を多角的に分析し、当該IoT機器に求められるサイバーセキュリティ要件を明確にした上で、次工程である製造フェーズにおいて確実に機能を実装できるよう、綿密に設計することである。このような考え方は、情報システムの開発においては従来から常識であるが、本年度の調査結果を見ると、IoT機器の開発においては、同様の取り組みを実践している日本企業の割合は、海外に比して、著しく低い（図3）ことが分かる。

図3:開発サイクルにおけるIoTセキュリティアセスメントを行っているか



セキュア・バイ・デザインは、「IoT総合セキュリティ対策」のなかでも、脆弱性対策における重要な取り組みとして言及されており、ID／パスワード設定、ファームウエアの管理、Wi-Fiの設定などが具体的な着眼点として例示されている。もちろんこれらの着眼点は単なる一例でしかない。このような技術面の設定にとどまらず、IoT機器のライフサイクル全体を想定すること、また初期工程である研究開発フェーズにおいて具体的なセキュリティ要件を識別し、製造フェーズにおいて実装／検証していくことは、機器の継続的な安定性を高めるための重要要素の一つと言える。

「セキュア・バイ・デザイン」と似た概念に「プライバシー・バイ・デザイン」がある。「セキュア・バイ・デザイン」がサイバー攻撃などのセキュリティ上の脅威を想定した取り組みであるのに対し、「プライバシー・バイ・デザイン」は、各国・各地域の個人情報保護規制や消費者のプライバシー意識を想定した設計時の取り組みである。

IoT機器には日々大量の個人情報が蓄積していく。スマートフォンを肌身離さず持ち歩く現代人が、いつどこで誰と会って何をしているのか?プラットフォーマーのクラウドに蓄積されたデータを解析すれば瞬時に判明する。街中には屋内外問わず大量のWebカメラが設置され、人々の生活は映像で記録されている。最近話題のAIスピーカーは、近未来型のスマートホームを実現する機器として注目を集める一方で、しばしば盗聴のリスクとセットで論じられる。それぞれの機器が持つ機能特性を本来の目的とは異なる目的のために悪用されてしまう可能性をどこまで想定できるのか。それが、設計時点の重要な鍵になる。

これらの点は、企業にとってコンプライアンス上のリスクにもなり得る。EU一般データ保護規則（GDPR）では、法律への違反時に売上の4％もしくは2,000万ユーロのどちらか高い方という高額の罰金が科せられる。長期に及ぶブランドの毀損も合わせれば、ダメージはさらに大きくなるだろう。

本年度の調査結果を見ると、日本企業における50％がプライバシー規制に対してコンプライアンスを順守することの重要性を表明しているものの（図4）、そのようなリスクがIoTにも内在していることを認識している企業は、いまだ一握りである（図5）ことが分かる。

図4:プライバシー保護の目的として、「規制・コンプライアンス順守」を重要視すると回答した日本企業の割合

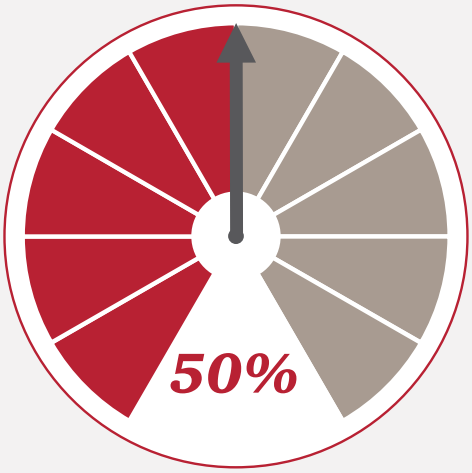
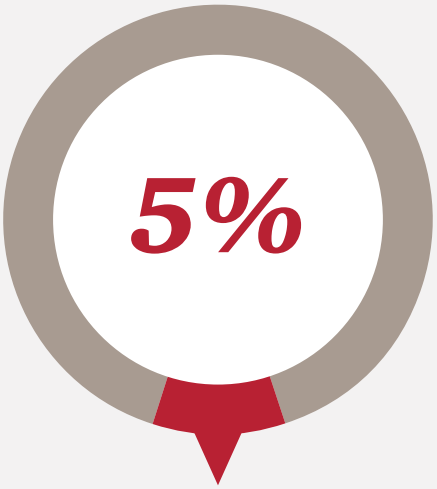


図5:今後1年におけるプライバシーに係る重点施策範囲に「IoT」と回答した日本企業の割合



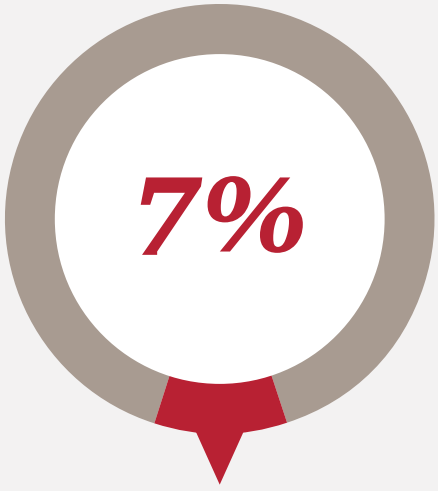
②:製造フェーズ

研究開発フェーズで識別したセキュリティ／プライバシー管理要件に基づいて機器の製造やソフトウエアの開発を行う製造フェーズにおける重要なポイントは、製造環境の信頼性を維持することである。

一般的に、機器の製造は部品メーカーやサプライヤーなど、さまざまな外部事業者と研究開発上のデータを共有するなど、協働して進められることが多い。万が一、製造フェーズに関与する外部事業者の製造環境が、自組織と同等程度のサイバーセキュリティ水準（信頼性）を確保できないとすれば、それは、要求仕様に係るデータの改ざん、あるいはデータの漏洩による機器の市場競争力の低下など、想定外の事態に直面するリスクが存在することを意味する。

しかしながら、本年度の調査結果では、日本企業においては、IoT機器の製造において外部事業者とデータを共有することに伴う、上記のようなリスクに対していまだ無防備である（図6）ことが判明した。研究開発フェーズにおいて実効性のあるセキュリティなどの管理要件を定義できたとしても、その製造環境の信頼性が十分に確保されていなければ、本来あるべきIoT機器のセキュリティは確保できない。

図6:今後1年において、外部の協働業者とのデータ共有に係るリスクに懸念を覚えていると回答した日本企業の割合



③：市場利用フェーズ

「IoT機器」は複数の異なる顔を併せ持つ。機器と言うからには、工業製品として組み立てられ物理的な形を持つハードウエアである。しかし、IoTである以上、その内部にはコンピューターが内蔵されインターネットに接続されるソフトウエアでもある。

これまで機器メーカーの役割は、主に製品を製造して出荷するまでだった。もちろん出荷後の品質保証や故障時の修理などの責任はついて回るが、利用者との接点が生まれるのは、利用者が自らユーザー登録してくれた場合に限られる。そうでなければ、製品がメーカーの手を離れた後、卸売業者や小売業者を巡って最終的に誰の手に渡ったのかを知ることさえ難しい。

従って、製品の欠陥によって一度リコールが発生すれば、メーカーにとっては一大事だ。製品を無償で修理するコストは当然のこと、どこにいるかも分からない利用者に向けて新聞広告を出したり、何年もの間ただ待つだけのお問い合わせ窓口を維持し続けたりするコストは決して看過できない。

一方、ソフトウエア業界はリコールとは無縁だ。元来、生命や健康に害を与える類の不具合が発生しにくいこともあるが、製品の品質追求に向けたアプローチが機器メーカーとはまったく異なる。ソフトウエアの開発において、初期リリース時に完璧な製品を作ることは難しい。その代わりにリリース後にバグを修正し、インターネットを通じて更新版のソフトウエアを配布することが可能だ。原材料が必要な工業製品と違って、無限にコピーできるソフトウエアではコストのインパクトも極めて小さい。大手ソフトウエア会社ともなれば、社外のバグ発見者に対して報奨金を出す制度を導入し、世界中の開発者の協力を得ながら品質の向上に努めており、更新のサイクルも速い。

工業製品を製造していたメーカーがIoTメーカーに生まれ変わるということは、その製品をインターネットに接続させるという単純なことではなく、むしろメーカーにおいてDevOpsを導入することを意味するという見方ができる。つまり、製品の開発・試験・運用やその関連プロセス、製品のライフサイクル、顧客とのコミュニケーション手段や頻度、社外の技術者コミュニティとのかかわり方など、あらゆるものを変革し、製品のライフスタイルを通じたビジネスモデルを作り上げなければならない。

総務省の「IoT総合セキュリティ対策」から市場利用フェーズの対策として読み取れるものは、利用者への意識啓発というボトムアップ型の施策に加え、IoT機器の製造・販売企業、流通企業、保守メーカーなどが一体となり脆弱性情報を集約的に管理し、統括的な対応を図っていくトップダウン型の施策の重要性である。

これらの施策に取り組む上で、各企業は自社が取り扱うIoT機器の脆弱性を網羅的に管理し、利用者に適時に発信するための情報収集・発信の枠組みを整備しなければならない。このような枠組みの整備のもとで初めて、「IoT総合セキュリティ対策」が言及するような、各機器の脆弱性情報を企業横断的に統一管理するためのデータベースの構築に向けた官民の連携が可能となる。

本年度の調査結果を見ると、日本企業の半数以上が、IoTなどの新技術に伴う潜在的なリスクへの低減に向けた同業他社との協力体制に前向きではないと回答している（図7）。しかも、その理由の多くが情報共有フレームワークの未整備にあるという回答（図8）からも、企業間連携や官民連携を加速させるためには、こうしたフレームワークの整備が急務であると言える。

図7:新技術に伴う潜在的なリスク低減／セキュリティ向上に向け、同業他社と公式に協力するかという問いに「いいえ」と応えた企業の割合

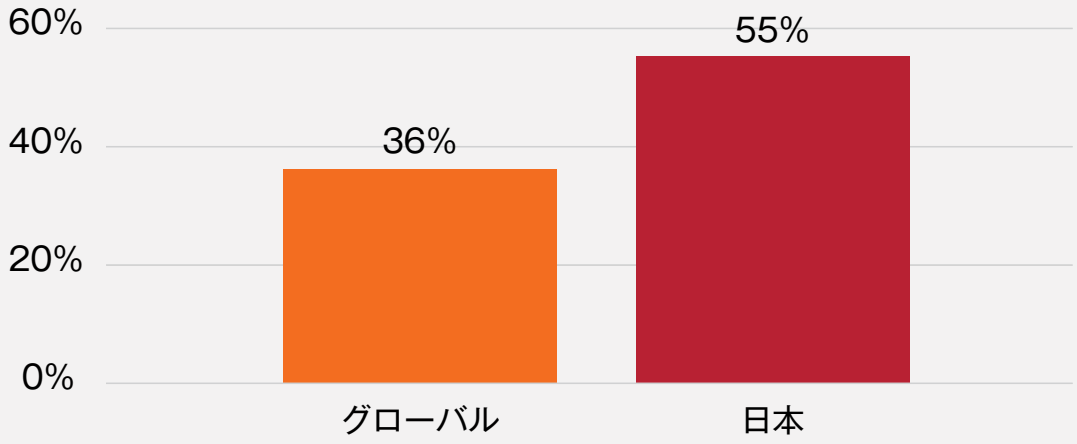
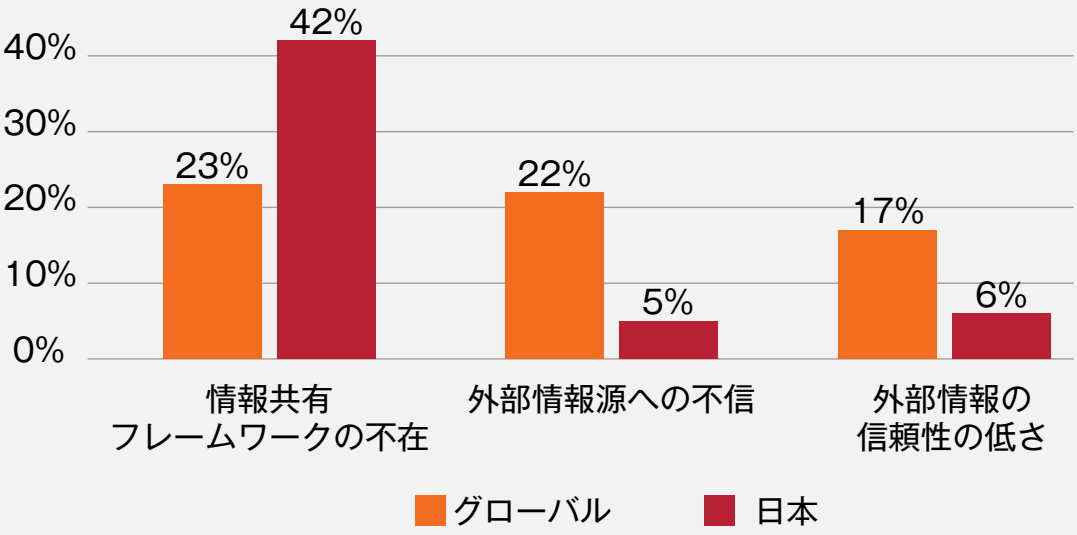


図8:同業他社との公式な協力を阻害する要因



④：廃棄フェーズ

「IoT総合セキュリティ対策」ではフォーカスされていないものの、機器を利用者が廃棄する際の要求事項の整理も、IoTのライフサイクルという観点からは重要である。

IoT機器は、知らず知らずのうちに利用者に関するさまざまなデータを蓄積している場合がある。そのため、当該機器の廃棄時に、後々利用者を特定・識別できないように固有データを確実に消去する手続きが必要となる。こうした手続きが十分に検討されない場合、利用者のプライバシーが侵害されるリスクが考えられるため、機器メーカーや利用者自身に対する意識啓発は不可欠である。

特にIoT機器は情報システムとは異なり、それ自体の再利用（中古品の利用）という局面を持つことにも留意が必要である。今後、機器の再販に際しては、第三者がデータを悪用しないよう、かつての利用者に関する情報を機器メーカーが自らデータを消去するか、再販事業者が確実にデータを消去する仕組みを構築することが求められることになるだろう。

3．IoTセキュリティの実践事例

ここでは、IoTセキュリティの確保に向けてさまざまな取り組みを開始している自動車業界の事例を紹介する。自動車会社は、かつてクルマという機械を製造するメーカーであったが、いまやそのクルマは車輪のついた走るIoTとなり、自動車会社は一種のIoT機器メーカーとして新たなサービスの開発に取り組んでいる。上述してきたIoT機器におけるセキュリティがどのような深度をもって考えられているのかについての具体的なイメージを持っていただこうと思う。

自動車業界を取り巻くIoT環境

コネクテッドカーの技術に関連する市場規模は拡大を続けており、世界各国の自動車メーカーがしのぎを削っている一方で、自動車に対するサイバー攻撃やハッキングについてさまざまな報告がされている。

例えば、あるメーカーのコネクテッドカーでは、携帯電話ネットワーク経由で内部システムへ不正侵入し、システムファームウエアを書き換えることで、ハンドルを遠隔操作可能にする脆弱性が発見された。この発見に伴い、自動車メーカーは数百万台に上るリコールに直面し、大きな損失を抱えることになった。

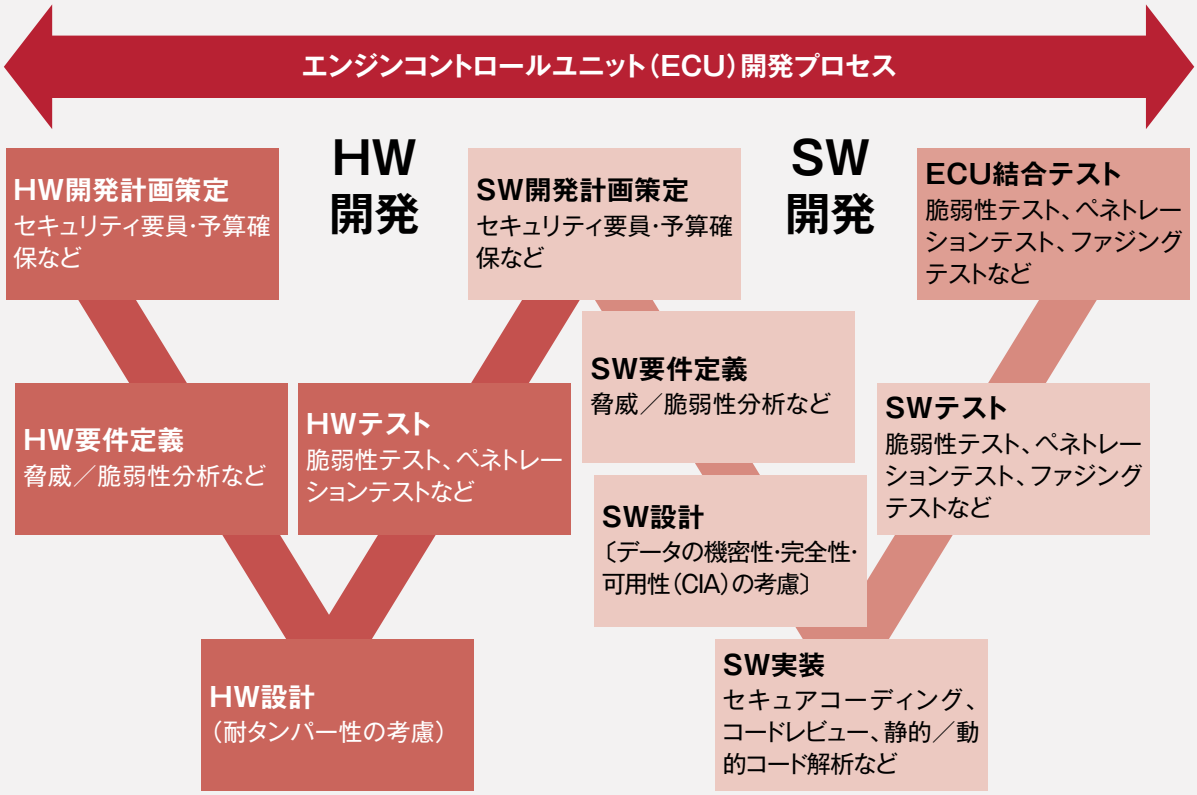
このようなコネクテッドカーに関するセキュリティの抜き差しならない状況のなか、国際機関や業界団体は、自動車のセキュリティ確保に向けてガイドラインの策定を進めているものの、実践的な国際標準規格の発行は2020年とされている。それまでの間、各メーカーは自助努力によって車体システムを構成するIoT機器群のセキュリティを確保し、外部からの攻撃に耐え得るコネクテッドカーを作るための取り組みを進める必要がある。

ある自動車メーカーの例

ある自動車メーカーは、エンジンコントロールユニット（ECU）に係るハードウエア（HW）／ソフトウエア（SW）をセキュアに開発するための、セキュア・バイ・デザインに基づく体系的なコネクテッドカー開発プロセスを運用している。

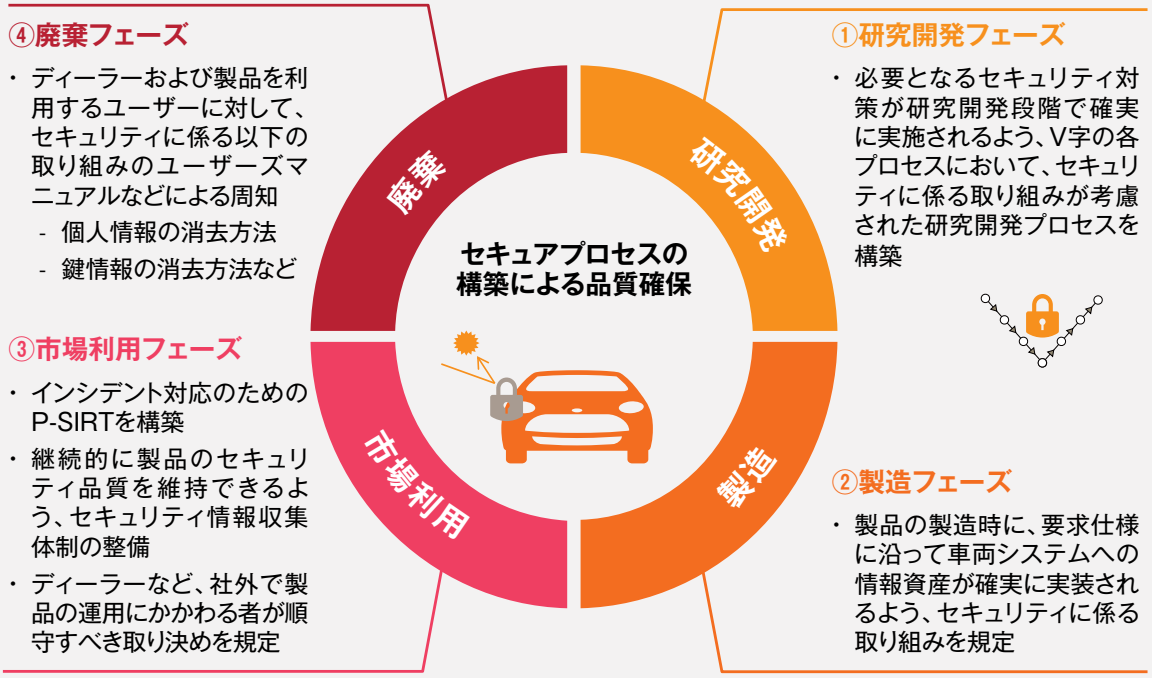
このプロセスにおいては、ハードウエアとソフトウエアが独立して開発されるのでなく、同一のECUをレイヤー別に開発するという観点からプロセス間を連続させている。これにより、ハードウエアに最適化されたソフトウエアセキュリティを実現するとともに、ソフトウエアセキュリティを最大化するハードウエア製造を可能にしている（図9）。

図9:セキュア・バイ・デザイン例



このメーカーでは、コネクテッドカーのライフサイクル(「研究開発」「製造」「市場利用」「廃棄」)を通して実施すべき技術／運用面のセキュリティ対策について、各フェーズに関与するさまざまなステークホルダーを洗い出し、各関係者が実施すべきセキュリティ対策を定義している(図10)。

図10:コネクテッドカーのライフサイクル例



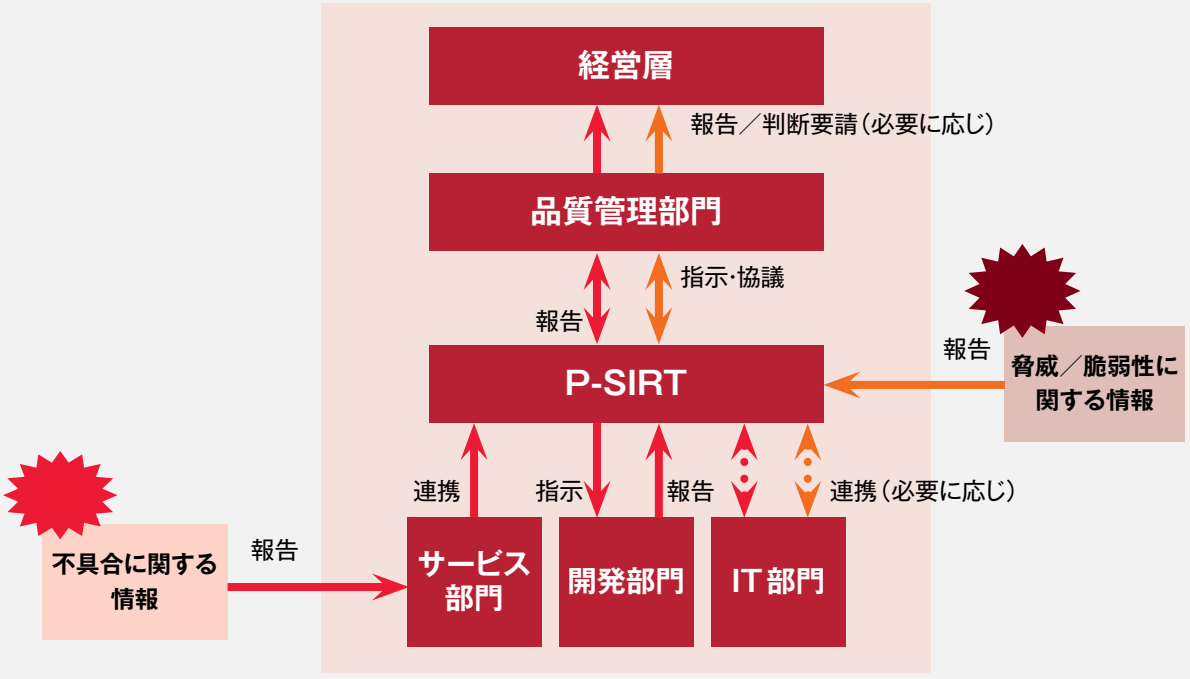
特に着目したい点は、市場利用フェーズにおけるP-SIRT（Product-Security Incident Response Team）である。

このメーカーでは、販売後の製品の安全性（セーフティ）を阻害する不具合はサービス部門が窓口となる一方、製品のセキュリティを危ぶませる脅威や脆弱性情報の窓口としてP-SIRTチームを設置している（図11）。

製品に対するサイバー攻撃への対応は、製品自体の不具合とは異なる対応プロセスが求められる。P-SIRTは問題解決に向けた主導的な役割を担う。また製品の不具合が発見された場合においても品質管理部門からP-SIRTチームへの報告が行われ、当該チームにおいて潜在的な脆弱性の検証が行われている。

ここで重要なポイントは、製品のセーフティ／セキュリティを揺るがす品質懸念上の情報群をP-SIRTが品質管理部門との連携のもとで統括して管理することである。特に、サイバー攻撃の脅威や脆弱性といった技術的なトピックについては、P-SIRTがIT部門と連携しながら機動的な対応を行っている。

図11:IoT製品の品質管理体制例



4．まとめ

日本企業において、IoTにおけるセキュリティ戦略およびそれに基づく具体的な対策は、喫緊の課題である。一部の業界や企業では既にこうした取り組みが先行して進められているものの、海外の企業からは水をあけられていることが今回の調査を通して明らかになった。

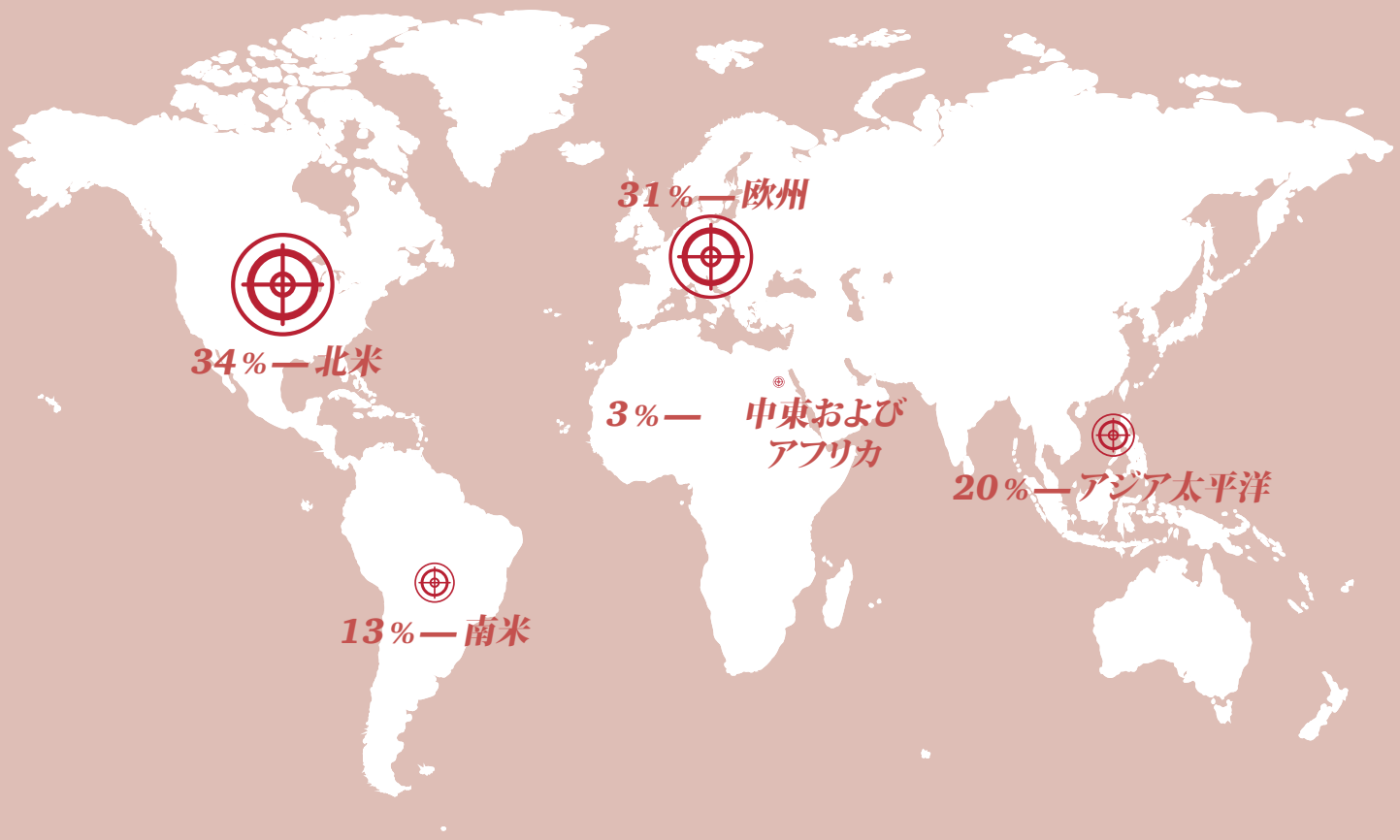
日本政府が目指すデータ主導社会やそれを支えるインフラ基盤の成否は、そこに繋がるIoT機器一つひとつの品質にかかっている。IoT機器を製造するメーカーには、自社の機器の単体でのセキュリティを確保するだけではなく、IoT社会全体の安定性にコミットするといった、高い次元の企業精神が求められているとも言える。

調査方法

グローバル情報セキュリティ調査2017（以下、「本調査」という）は、PwC、CIO、およびCSOが実施した情報セキュリティに関する世界的な調査です。2016年4月4日から6月3日までの期間において、CIOおよびCSOの読者、および全世界のPwCクライアントに対して、電子メールによって調査への協力を依頼し、オンライン調査を実施しました。

本報告書で解説する調査結果は、10,000人以上の最高経営責任者（CEO）、最高財務責任者（CFO）、最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）、最高セキュリティ責任者（CSO）、副社長、ITおよび情報セキュリティ役員からの回答に基づいています。

回答者の地域別では、北米が34％、欧州が31％、アジア太平洋が20％、南米が13％、中東およびアフリカが3％です。



誤差は1％未満です。ここでは四捨五入した数値を使用しているため、数値の合計が100％にならない場合があります。本報告書の全ての図および図形は、調査結果に基づき作成したものです。

サイバーセキュリティおよびプライバシーに関するPwCのお問い合わせ先（国別）

オーストラリア

Richard Bergman
Partner
richard.bergman@au.pwc.com

Andrew Gordon
Partner
andrew.n.gordon@au.pwc.com

Steve Ingram
Partner
steve.ingram@au.pwc.com

オーストリア

Christian Kurz
Senior Manager
christian.kurz@at.pwc.com

ベルギー

Filip De Wolf
Partner
filip.de.wolf@be.pwc.com

ブラジル

Edgar D'Andrea
Partner
edgar.dandrea@br.pwc.com

カナダ

David Craig
Partner
david.craig@ca.pwc.com

Sajith (Saj) Nair
Partner
s.nair@ca.pwc.com

Richard Wilson
Partner
richard.m.wilson@ca.pwc.com

中国

Megan Haas
Partner
megan.l.haas@hk.pwc.com

Ramesh Moosa
Partner
ramesh.moosa@cn.pwc.com

Kenneth Wong
Partner
kenneth.ks.wong@hk.pwc.com

デンマーク

Christian Kjær
Director
christian.x.kjaer@dk.pwc.com

Mads Nørgaard Madsen
Partner
mads.norgaard.madsen@dk.pwc.com

フランス

Philippe Trouchaud
Partner
philippe.trouchaud@fr.pwc.com

ドイツ

Derk Fischer
Partner
derk.fischer@de.pwc.com

インド

Sivarama Krishnan
Partner
sivarama.krishnan@in.pwc.com

イスラエル

Rafael Maman
Partner
rafael.maman@il.pwc.com

イタリア

Fabio Merello
Partner
fabio.merello@it.pwc.com

日本

Yuji Hoshizawa
Partner
yuji.hoshizawa@pwc.com

Sean King
Partner
sean.c.king@pwc.com

Naoki Yamamoto
Partner
naoki.n.yamamoto@pwc.com

Kei Tonomura
Partner
kei.tonomura@pwc.com

Yasuhiro Kishi
Partner
yasuhiro.kishi@pwc.com

韓国

Soyoung Park
Partner
s.park@kr.pwc.com

ルクセンブルク

Vincent Villers
Partner
vincent.villers@lu.pwc.com

メキシコ

Fernando Román Sandoval
Partner
fernando.roman@mx.pwc.com

Yonathan Parada
Partner
yonathan.parada@mx.pwc.com

Juan Carlos Carrillo
Director
carlos.carrillo@mx.pwc.com

中東

Mike Maddison
Partner
mike.maddison@ae.pwc.com

オランダ

Gerwin Naber
Partner
gerwin.naber@nl.pwc.com

Otto Vermeulen
Partner
otto.vermeulen@nl.pwc.com

Bram van Tiel
Director
bram.van.tiel@nl.pwc.com

ニュージーランド

Adrian van Hest
Partner
adrian.p.van.hest@nz.pwc.com

ノルウェー

Lars Erik Fjørtoft
Partner
lars.fjortoft@pwc.com

ポーランド

Rafal Jaczynski
Director
rafal.jaczynski@pl.pwc.com

Jacek Sygutowski
Director
jacek.sygutowski@pl.pwc.com

Piotr Urban
Partner
piotr.urban@pl.pwc.com

ロシア

Tim Clough
Partner
tim.clough@ru.pwc.com

シンガポール

Vincent Loy
Partner
vincent.j.loy@sg.pwc.com

Jimmy Sng
Partner
jimmy.sng@sg.pwc.com

南アフリカ

Sidriaan de Villiers
Partner
sidriaan.de.villiers@za.pwc.com

Elmo Hildebrand
Director/Partner
elmo.hildebrand@za.pwc.com

Busisiwe Mathe
Partner/Director
busisiwe.mathe@za.pwc.com

東南アジア

Jimmy Sng
Partner
jimmy.sng@sg.pwc.com

スペイン

Javier Urtiaga Baonza
Partner
javier.urtiaga@es.pwc.com

Elena Maestre
Partner
elena.maestre@es.pwc.com

スウェーデン

Martin Allen
Director
martin.allen@se.pwc.com

Rolf Rosenvinge
Director
rolf.rosenvinge@se.pwc.com

スイス

Reto Haeni
Partner
reto.haeni@ch.pwc.com

トルコ

Burak Sadic
Director
burak.sadic@tr.pwc.com

英国

Neil Hampson
Partner
neil.r.hampson@uk.pwc.com

Richard Horne
Partner
richard.horne@uk.pwc.com

Alex Petsopoulos
Partner
alex.petsopoulos@uk.pwc.com

米国

David Burg
Principal
david.b.burg@pwc.com

Scott Dillman
Principal
scott.dillman@us.pwc.com

Chris O'Hara
Principal
christopher.ohara@us.pwc.com

Grant Waterfall
Partner
grant.waterfall@us.pwc.com

www.pwc.com/gsiss
www.pwc.com/cybersecurity

参考文献

Framework for Cyber-Physical Systems Release 1.0: *The US National Institute of Standards and Technology (NIST) guidelines for cyber-physical systems.*

Careful Connections: Building Security in the Internet of Things: *The US Federal Trade Commission advice on building security into Internet of Things devices.*

Fostering the Advancement of the Internet of Things: *An overview by the US Department of Commerce on the IoT landscape, infrastructure demands, and cybersecurity and privacy best practices.*

Strategic Principles for Securing the Internet of Things: *Guidance from the US Department of Homeland Security on principles and suggested best practices to build IoT security for devices and systems.*

Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (NIST Special Publication 800-160): *The US National Institute of Standards and Technology (NIST) details an engineering-based approach for the entire life cycle of IoT devices and systems.*

お問い合わせ先

PwCコンサルティング合同会社
〒100-6921 東京都千代田区丸の内2-6-1
丸の内パークビルディング
03-6250-1200（代表）

山本 直樹
パートナー
naoki.n.yamamoto@pwc.com

PwCサイバーサービス合同会社
〒100-0004 東京都千代田区大手町1-1-1
大手町パークビルディング
03-6212-9080（代表）

星澤 裕二
パートナー
yuji.hoshizawa@pwc.com

PwCあらた有限責任監査法人
〒100-0004 東京都千代田区大手町1-1-1
大手町パークビルディング
Tel: 03-6212-6800（代表）

岸 泰弘
パートナー
yasuhiro.kishi@pwc.com

グローバル情報セキュリティ調査2017
日本版レポート執筆委員

PwCコンサルティング合同会社
上村 益永
阿部 耕平
道輪 和也

PwCあらた有限責任監査法人
綾部 泰二
三澤 伴暁
江原 悠介
米山 喜章

www.pwc.com/jp

電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/knowledge/thoughtleadership.html
日本語版発刊年月： 2017年12月　　管理番号： I201710-5