strategy&
Part of the PwC Network

Strategy& Foresight vol.19
2019 - II -

特集

データの重要性とそのセキュリティ

- Security as an Infrastructure -

vol. 19

2019
- II -

Strategy& Foresight

ストラテジーアンド・フォーサイトは、
PwCネットワークの
戦略コンサルティングチーム
Strategy&が、
経営戦略についての
さまざまな課題をテーマに、
経営の基幹を担われている皆様に
向けて発行する定期刊行物です。

Contents

巻頭言

データエコノミー時代の経営資源

樋崎 充

データが生み出す価値について疑う企業はもはや少ないのではないか。さまざまな企業が自社ビジネスに対し有利に展開するデータ収集の仕組みを他社とのアライアンスを含めて強力に推進し、データビジネス空間の陣取り合戦を繰り広げている。インターネットの普及に伴いウェブ上で生まれたデータに目を付けた企業が、広告や小売業界を中心にビジネスモデル変革を起こした。データビジネス空間の戦いがリアル世界にも影響を及ぼすことは、米系IT企業が大成功した姿を見れば言うまでもない事実である。今後は、AIやAPI[1]などの普及により、今までデータが存在していなかった領域において新たなデータが生まれ、業界をまたいだデータ流通が加速することが予想される。

一方で、個人情報に利用停止権を導入するよう政府の個人情報保護委員会が検討をしているという報道[2]にあるように、データとはそもそも誰のものなのか、そのようなデータから企業側が得た情報の扱いと個人プライバシーの在り方について議論されているというのも事実である。これらはプライバシーの問題として語られるだけではなく、同時にデータセキュリティの在り方自体にも影響を及ぼす。毎日生み出される膨大なデータは単にインターネットを活用した取引の足跡ではなくなり、データ提供者の「財」とみなされ始めている。サービス提供による利便性の提供だけではなく、「財」を最大化し「財」を保障するということがデータビジネス市場に参入する上で考慮しなければならない前提となりつつある。現時点においても既にセキュリティリスクへの対応能力が市場参入障壁になっているというのが実情ではないであろうか。

今号においては、個人データのコントロール支援やサプライチェーンに潜むセキュリティリスクなどについて言及する。これらはデータビジネスに関連した課題ではあるが、単なるビジネス上の課題ではなく、社会課題として解決が望まれるテーマでもある。まだ主流となる解決策は見いだされていないが、イノベーションを起こした企業こそが米系IT企業が制するデータ市場で大きな力を持つ可能性もあり得る領域ではないだろうか。経営者の方々には、たかがセキュリティという見方ではなく、データエコノミー時代における競争優位性を生む源泉としてセキュリティを経営資源の一つとして再定義してもらいたい。

樋崎 充（といざき・みつる）
mitsuru.toizaki@pwc.com

Strategy&のパートナー。約15年にわたり、IT関連企業、総合電機メーカー、電子部品メーカー、製薬会社に対し、事業戦略、組織戦略、M&A戦略、SCM戦略の立案および実行支援などのプロジェクトを手がけてきた。

1：Application Programming Interface、ほかのシステムと連携するためのプログラムインターフェース
2：2019年4月3日付 日本経済新聞「個人情報、本人に利用停止権　企業の乱用防止 政府検討、来年法改正へ」, https://www.nikkei.com/paper/article/?b=20190403&ng=DGKKZO43234840S9A400C1MM8000

データプラットフォームの覇者

**通信会社は、今日のデジタル業界において収益力のある事業を見つけるのに苦労している。
そこで、個人データのコントロールを支援するというのはどうだろうか。**

著者：フロリアン・グローン、ピエール・ペレードー、ライア・アブドル・サマド
監訳：坂野 孔一

通信会社、特に携帯キャリアにとって通信トラフィックに依存しない非通信分野の収益向上は、この十数年、至上命題であった。携帯キャリアは、ヘルスケア、金融サービス（銀行、保険、決済、カード）、eコマース、コンテンツ配信（音楽、動画）などの非通信分野への取り組みを強化してきたが、異業種への後発参入ということもあり、大きな収益源には育っていないのが現状である。本稿で紹介するビジネスモデルは、携帯キャリアのコアコンピタンスに近く、現有のアセットを活用できる点で一つの有力な選択肢と考えられる。また、小売りや保険、自動車など多くのB2C企業にとって、パートナーとしての参画を検討する余地があるのではないだろうか。（坂野 孔一）

時は2025年、アレックスは辟易していた。アナログ生活とデジタル生活の間には、もはやいかなる区別もない。彼女のあらゆる行く先や購入したもの、例えばジムでのエクササイズやネットサーフィンに至る行動など全ての情報に対し、おびただしい量のデータが生成される。不気味なほどにターゲティングされ、パーソナライズされた広告メッセージで爆撃されているようなものである。街を歩けば、通りかかった店に関する広告メッセージがスマートフォン（スマホ）に表示される。スマホに限らず、タブレット、PCにもポップアップ広告が現れ、軽い体調不良向けの薬を勧めてくる。翌日、症状が現れるまで自分が患っていたと気づかない程度の体調不良にも関わらずだ。さらにひどいことに、最近彼女は職場で配置転換されることを知った。AIが、彼女の現在の仕事をマスターしてしまったのだ。彼女が会社のソフトウェアをどのように使うか、AIが分析したのである。

まるでアレックス自身よりも会社のコンピュータアルゴリズムの方が彼女のことを知っているかのようだ。そして、おそらくそれは真実だろう。一体どうやって彼女の一つ一つの行動や会話、さらには彼女の考えた内容までをも、データストアに蓄積できたのだろうか。何しろ「彼女自身」のデータなのである。彼女の好き嫌い、興味、友人関係、購買時の選択、アクティビティ、居場所、つまり彼女のアイデンティティそのものが収集・分析され、儲けの源泉とされ、さらには彼女を管理するのにまで使用されていたのだ。これらの企業は、こうした情報を売買して利益を上げていたようだ。彼女が生み出すデータを彼女自身がある程度コントロールできて何がいけないだろうか。そして場合によっては、そうしたデータを長年にわたり無料で収集してきた企業へデータを売ることでいくらか収入を得て何が問題だろうか。

そこでアレックスは、プライバシーとアイデンティティをコントロールできる新たなサービス「パーソナル・データ・マネージャー」を契約した。このサービスは、米国に拠点を置くコネクティビティ会社（本稿ではDigiLifeと呼ぶが、2025年の時点でインターネットサービスを提供する、いずれの電話会社もこれに当てはまる可能性がある）が提供するものである。ここ数年でDigiLifeは、オンライン上でのメディアやインターネットサービスの利用、情報のやり取りの管理や記録をもっと容易にしたプラットフォームである「コネクティビティ基盤」に変貌してい

フロリアン・グローン

Strategy&のプリンシパルでニューヨークを拠点とする。通信、デジタル、ソフトウェアといった業種における経営陣のアドバイザーを務める。デジタル時代における経営・テクノロジー戦略の策定の面で企業を支援する。

ピエール・ペレードー

Strategy&のパートナーでパリを拠点とする。通信・ハイテク業界、さらにはデジタル変革を担当。通信、テクノロジー、エネルギー、公益事業、航空宇宙、小売業界においてデジタル戦略の策定に取り組む経営陣を支援する。

ライア・アブドル・サマド

Strategy&のマネージャーでボストンに拠点をおく。テクノロジーとメディア業界を担当し、デジタル時代における成長・テクノロジー戦略について企業を支援する。

坂野 孔一 (ばんの・こういち)
koichi.banno@pwc.com

PwCコンサルティング、Strategy&のシニアアソシエイト。通信、製造業を中心に全社戦略、事業戦略、ビジネスデューデリジェンスなど幅広いプロジェクトに携わる。

た。「忘れ去られる権利」などデジタルアイデンティティやデータ管理に関する成立したばかりの法律のおかげで、DigiLifeの「パーソナル・データ・マネージャー」は単なる見せかけにとどまらない存在になっていた。同サービスは、ユーザーに分かりやすい選択肢をいくつか提示しており、全てのインターネットサービスプロバイダーが、法によってユーザーのその選択を尊重することを義務付けられている。

まず、新サービスの助言に従い、アレックスはメディアやインターネットサービスプロバイダーが彼女についてそれまでに蓄積していたデータを消去するよう要請し、まっさらな状態で始められるようにした。それから、DigiLifeのデータ管理アプリにログインした。このアプリは、今後、彼女のデバイスからインターネットへ流れるあらゆる情報のゲートキーパー（門番）の役割を担う。

同アプリはアレックスに対し、彼女がメディアやインターネットサービスプロバイダー、その他の機関にどの程度情報を提供するかについて、いくつか選択肢を示した。彼女のユーザープロファイルを用いて彼女のニーズや意思を効果的に予測するAIが搭載された同アプリにより、サイトごとのプライバシーおよび開示の程度が選びやすくなったほか、彼女が生み出すデータの金銭的価値を容易に見積もれるようになった。

例えばアレックスは、オンラインで買い物や銀行取引ができるように、特定の限られたeコマース企業と金融サービス企業に対して本人認証データベースへのアクセスを認めるという選択をした。しかしながら、それらの企業が彼女の位置情報へアクセスすることや、彼女の買い物データを他の企業からのデータと組み合わせることは禁止した。また、彼女の携帯電話が生成する位置情報を地図アプリのプロバイダーへ開示することと、健康状態を観察してくれるリストバンドのデータを彼女の主治医に送信することは承諾したが、保険会社へ送信することは禁止した。そして最後に、いくつかの限られたeコマース企業、ソーシャルメディア、保険会社、製薬会社などが彼女の関心、嗜好、ライフスタイル上の選択に関するデータを収集することを承諾した。その代わりにこれらの事業者はそれぞれ、自動車保険と医療保険の割引や彼女のDigiLifeのアカウントへの少額の払い戻しなど、金銭的なインセンティブを彼女に与えた。その後何カ月かの間、彼女は同アプリを頻繁に開き、新たなウェブサイトの追加や個人データに関する設定の変更を行った。

今日、2019年、アレックスが使用したような個人データを管理するアプリケーションは未熟なものしか存在せず、消費者がこれらのサービスを信頼しているという域にはまだ達していない。あるいは、自分のデータを売って利益を得ることもできない。ただ、巨大なニーズが存在しており、そのニーズを満たせる企業にとっては絶好の機会が存在する。現在構築されているようなデータエコノミーの価値は2025年までに総額4,000億ドル余りに膨れ上がると考えられ、消費者は自らが生み出す膨大な量のデータをマネタイズすることで、その総額の4分の1もの額を取り戻せる可能性がある。

デジタルエコノミーにおいて通信会社が担う重大な役割、すなわちデータネットワークの中心的存在、ネットワーク構築機能、顧客との関係性、行政への対応における経験などを踏まえると、通信会社はこうしたビジネス機会をつかむうえで優位な立場にある。ただ、単独では実現できないと考えられ、インターネットサービスプロバイダーやその他デジタル分野のパートナーとコンソーシアムを形成することが見込まれる。それでも、旧来のコネクティビティ会社にとっては、この種のサービス

の提供が最も持続可能な事業上の選択肢になるかもしれない。また、人々が自らの個人データであふれるデジタル世界において個人データをコントロールする力を保持しようとするなか、私たちにとっても最適な選択肢になるかもしれない。

データの価値の試算

各種データを見ると、ここ数年でデータエコノミーがいかに大きく成長したか、そしてどれだけ収益力をつけたか、さらには今後どれだけ速いペースで成長するかが分かる。IDC[1]によると、2018年、世界中のあらゆるデータソースから生成されたデータは、33ゼタバイトに達した。わずか5年前、これは4.4ゼタバイトだった。これは、年平均成長率50%に相当し、こうした情報の大海原は2025年までに175ゼタバイトにまで増加し、2018年比で5倍を超える水準にまで膨れ上がると予想されている（ゼタバイトとは10億テラバイト、すなわち10の21乗バイトに相当する。データサイエンティストのリザ・ベルカンは、1ゼタバイトのデータを印刷した本にすると、地球と太陽を5往復するまで積み上げる必要があると試算している）。

データのやり取りの圧倒的多数が機械と機械の間で行われている。それらの多くがオンライン上で行われているが、特にIoTを通じて行われるデータのやり取りが増えている。確かに、ほとんどのデータは保管されて数ミリ秒で消去される。それでも、1年間で約3.7ゼタバイトのデータが、人々によって生成され保管されている。インターネットユーザー一人当たりが生成するデータは、平均すると約117ギガバイトに達する。その約25%がGoogleによって保管されており（単一企業が保管するユーザーのデータとしては、ずば抜けて大きな割合である）、さらに1%をFacebookが保管している。2025年までに、一人当たりのデータ生成量の平均は300ギガバイト近くに達すると予想されている。Seagate社が委託したIDCのレポートでは、平均的な人が1日当たりに生み出すデータのやり取りは4,900件余りに達すると見積もられている。つまり18秒ごとに1件のデータがやり取りされ、そのうち約20%は日常生活に欠かせないものになると試算されている。こうしたデータの約90%が、不正なデータの取得またはサイバー窃盗の危険にさらされるものの、セキュリティが確保されるのはその半分に満たないと考えられている。

誕生からたった20年で急速に成長し続けている、こうした巨大な世界規模のアルゴリズムエコシステムに保管・分析されている全データの、途方もない規模と細かさを考えると気が遠くなる。さらに私たちの試算によると、これらの情報は、最新の解析技術と組み合わさって、毎年2,500億ドル近くの経済価値を創造している。このうち、個人にもたらされている価値はゼロである。個人の行動こそが、データの源泉であるにもかかわらずだ。的を絞った広告を可能にするために個人データを用いている会社（GoogleやFacebookなど、検索エンジンやSNSを提供している会社）は2018年、約1,780億ドルの収益をあげた。データブローカー（仲介業者）は約210億ドルの収益を得た。そして、自身の価値を向上させるために消費者のデータを用いている企業（通信会社や決済会社、自動車メーカーなど）も280億ドルを生成した（図表1参照、「収益源別データ価値」では「直接販売・分析」として表示）。

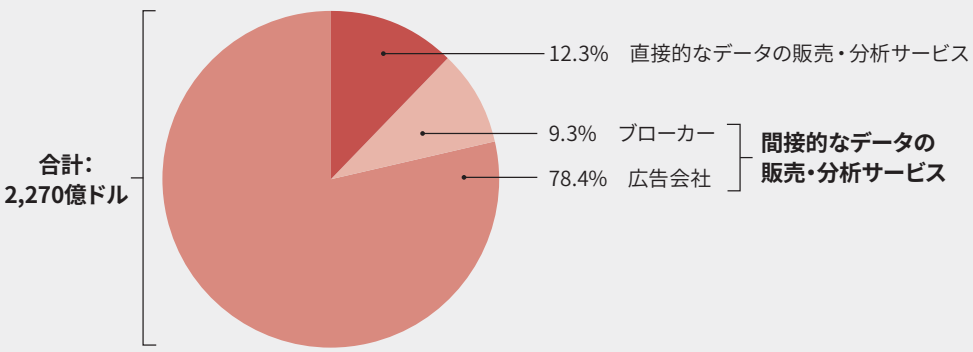
現在、データエコノミーにおける価値の創造は、オンライン広告が圧倒的割合を占めている。オンライン広告は2018年、オンライン市場の収益の80%近くを生み出し、その大半をGoogleとFacebookが占めた。しかしながら、やがて、価値の創造に占める広告の割合は低下すると考えられる。実質的に全ての広告がデジタル化されると、広告がどれだけ的を絞ったとしても、その成長は限界に達する。さらにデータブローカーによる個人データの販売は、規制当局が情報の拡散に制約を課し、そしてユーザーもその収集を制限し始めると、苦労するようになると考えられる。

そこで、自動車メーカーや小売企業、決済会社、通信会社など企業への直接販売から成長が生まれるようになると見込まれる。これらは全て、売上の増加と事業運営の改善を模索している。持続可能な商業的データエコシステムが創造され、それを通じてサービスプロバイダーやユーザーを含む全ての関係者がデータの売買・取引を行い、そしてデータから利益をあげられるようになると、新しい種類のデータをベースとするエ

1：IDC White Paper (November, 2018) “The Digitization of the World – From Edge to Core”

図表1
収益源別データ価値

現在、データエコノミーにて生み出されている価値の大半を広告が占めている。直接販売が出現し、企業が製品やサービス、プロセスの開発に使用する消費者データに対して料金を払うようになるなか、そうした状態に変化が生じると予想される。



出所:IDC『Global DataSphere』(2018年11月)、IDC and Open Evidence『European Data Market Smart 2013/0063 Final Report』、Strategy&分析

コノミーが成立する条件が整うだろう。そうしたエコノミーは種々の画期的なサービスから成り、ヘルスケアや銀行、保険、メディア、娯楽など既存の分野における新たなサービスもあれば、まだ想像もつかないようなサービスも生まれるだろう。

ユーザーのデータにはどのくらいの価値があるのだろうか。Strategy&の分析によると、平均的なインターネット利用者の個人データは、現在1カ月当たり約1.18ドルの値が付けられている。そして、オンライン広告市場が他の国や地域よりはるかに大きい米国では、1カ月当たり4.91ドルにのぼる値が付けられている。例えば、自家用車にテレマティクス装置を設置(加入している保険会社へリアルタイムで運転データを提供)しても構わないという人は、もちろん安全運転を実践しなければならないが、自動車保険の保険料が最大50%割り引かれる。完全なデータエコシステムが生まれれば、消費者行動のデータの価値は高まると見込まれる。とりわけ、保険やヘルスケア、eコマース企業は自らの顧客データを集計し、それをより効率的な事業運営とより確実な新商品・サービスの導入に生かすようになるだろう。これだけでも、値下げや現金の支給という形で個人に一人当たり年間数百ドルがもたらされる可能性がある(図表2参照)。

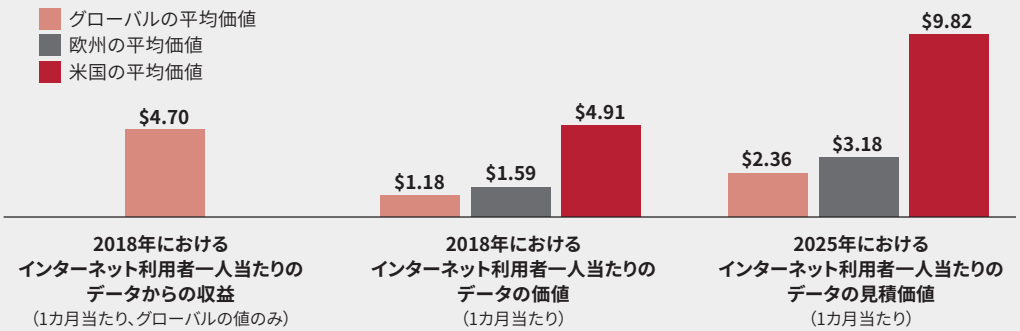
権利と期待

データエコノミーの巨大さと複雑さに鑑みると、そもそもそれが機能しているのか不思議である。しかしながら、大部分は機能している。図表3にユーザーとサービスプロバイダー双方の具体的な権利とニーズを、「プライバシー」「セキュリティ」「認証」「データの所有権」「関連性」「スムーズな体験」という六つの主要分野に分けてまとめた。プライバシーの向上および、生成されたデータの使用方法に関する透明性へのユーザーの期待は、時間の経過とともに強まると考えられる一方、個人データを収集・分析・販売する企業はおそらく、今よりも一層厳しいプライバシー規制の遵守を迫られるようになるだろう。

2: Secure Telephone Identity Revisited/Signature-based Handling of Asserted information using toKENs

図表2
あなたのデータの将来価値

米国では2025年までに、一人当たりのオンラインおよびオフラインでの行動に関する情報の金銭的価値は1カ月当たり10ドルに達する可能性がある。データ活用型サービスへの直接販売（図表には表示なし）も含めた場合、その金額はさらに高くなる可能性がある。



出所：IDC『Global DataSphere』（2018年11月）、『Facebook Annual Report 2017』、Strategy&分析

通信会社が機会に乗じプライバシーの向上に寄与できる方法の一例として、STIR/SHAKEN[2]と呼ばれる規格を考えてみよう。この規格は、着信電話番号の認証をすることでロボコール（自動音声による営業などの電話）によるストレスを減らすための暗号化システムである。米国で2019年に導入されたSTIR/SHAKENでは、同規格を採用する会社は正真正銘の発信者かどうかを確認する共通の管理システムを採用する必要がある。STIR/SHAKENは、コネクティビティ会社が将来使用する認証・プライバシー保護システムの原型になる可能性を秘めている。

ユーザーはまた、オンライン上での本人確認についても、より簡単なシステムを求めている。おそらくこれには、ブロックチェーン技術が組み込まれるだろう。そうしたシステムが、ユーザーが現在のところ頼りにしているユーザー名とパスワードの組み合わせに取って代わると考えられる。AIと機械学習が、ウェブサイトの紹介やアクセスに一役買うようになるほか、各ユーザーのインターネットサービスの質、帯域幅、スループット、通信の遅延、およびセキュリティの最適な水準の決定にも資するようになるだろう。5G時代の幕開けにおいてユーザーが要求するコネクティビティの種類は、ユーザーが使うインターネットサービスに左右されることになると考えられる。

データ会社の中には、これらのニーズの一つまたはそれ以上への対応を図っている会社もあるが、全てのニーズへの対応を実現した会社はまだ存在しない。おそらく、現時点で最も近いところまで到達しているのはVerimiである。さまざまなサービスへのシングルサインオンをユーザーに提供する業界横断型のユーザー認証・データサービスである。2018年5月にドイツにて導入されたVerimiを用いれば、ユーザーは、どのサービスプロバイダーがどのデータへアクセスできるかを決めることができる。このサービスには、アリアンツやアクセル・シュプリンガー、ダイムラー、ドイツテレコム、ルフトハンザ航空などがパートナーとして参加している。

より規模の小さい会社やスタートアップも同じような活動に加わりつつある。その一例がSolidである。1989年にワールド・ワイド・ウェブ（www）のプロトコルを開発したティム・バーナーズ＝リーによって2015年に設立されたSolidは、ユーザーが「pods」や自身のPC、またはクラウドに自らのデータを保管することを可能にし、ウェブの「再分散化」を図るという取り組みである。ユーザーは、どのアプリやウェブサイトが自身の個人データへアクセスできるかを選択する。

2017年に立ち上げられた、香港拠点のDatumも同様に、

ユーザーが自らの意志でデータを共有したり売ったりできるマーケットプレイスの創造に取り組んでいる。ブロックチェーン台帳によってバックアップされたそのデータベースが、SNS上のデータやウェアラブル機器からのデータ、スマートホームその他IoT機器からのデータを安全かつ非公開、そして匿名で保管することを可能にする。

通信会社の役割

通信会社にとっての機会は、利用者のプライバシーやコネクティビティの権利を含む、利用者によるインターネット体験の管理・サポートにある。新データエコノミーにおいて通信会社が果たす役割は、ネットワークの構築とコネクティビティという事業者の中核機能、あらゆるデジタルトラフィックのキャリアとしての中心的立場および大きな顧客基盤に立脚する。既に多くの大手通信会社が自己の中核事業を強化し、生来備わっている固有の力を発揮できる分野で価値を向上させる覚悟を固めている。

データエコノミーと深い関わりがある通信会社のさまざまなアセットを考えてみよう。

ネットワーク： 物理的なインフラはデジタル通信にとって今も欠かせない存在であり、将来的には今よりも強力なアセットになる可能性を秘めている。通信網は、サービスエリア・容量・機能の強化が急速に進んでいる。2020年の本格開始が予想されている高速の5Gへの移行は、通信会社がより多くの顧客データを顧客の同意のもと収集できるようにし、通信会社をコネクテッドエクスペリエンスを可能にする欠かせない存在に押し上げると考えられる。しかしながら、通信会社は世界展開していないところが多い。よって他国の同業と協力して、国内市場以外にも影響力を広げ、世界的な基盤を構築する必要があるだろう。

顧客データ： 通信会社が現在アクセスできる、ユーザーとサービスプロバイダーの間を流れる個人データの種類は限られているが、顧客に関する貴重なデータを大量に保管している。通信会社は通信市場に大きな顧客基盤を構築しており、利用者の支払いや決済に関するデータ、住所、電話番号やeメールのアクセスポイントの情報にアクセスできる。ネットワーク層では、通信会社は移動通信に用いられた無線アクセスネット

図表3
データエコノミーにおけるユーザーのニーズ

ユーザーのニーズ	データ生成者（検索エンジンおよびソーシャルメディアを含む）ができること	データ集約型サービスプロバイダー（通信会社を含む）ができること
プライバシー	ユーザーによるプライバシー設定管理のサポート、個人データの利用状況の可視化、簡単にオプトイン・オプトアウトができる機能の提供	プライバシー規制の遵守と透明性の確保
セキュリティ	データの破損、漏洩や紛失の防止	サイバー攻撃に対する防御
認証	本人確認・認証手続の簡素化	簡単で安全な方法でのユーザーIDの照合と規制の遵守
所有権	ユーザーがデータの価値の恩恵を享受することを目的とする、ユーザーによるデータの所有および収益化のサポート	新しいサービス、ビジネスモデル、およびパートナーシップを通じた、データの収益化
関連性	ユーザーが自分に関連のあるパーソナライズされた情報およびサービスへのアクセスを可能にするサポート	顧客のニーズに基づくサービスのカスタマイズとパーソナライズ
スムーズな体験	シームレスなトランザクションと目的に適したネットワークの品質の提供	チェックアウトプロセスの簡素化、手数料の最小化、ユーザーの体験の保証

出所：Strategy&分析

ワークを基に利用者の位置を追跡できる。ユーザーが所有する各機器を個別のアカウントへ関連付け、機器レベルの情報も把握できる。これにより例えば、SMSで送信されるパスコードを使った認証に頼るのではなくバックグラウンドでユーザー認証を行える。また、こうしたデータを用いて社会的相互作用や人口動態、地域社会の動向を深く知ることもできる。

ブランドと顧客関係： 自国内の通信会社に対する消費者の意識は市場によって著しく異なるが、全般的にユーザーは、通信会社はユーザーのデータを安全に扱っていると信頼している。大手通信会社は、強力なブランド認知度と、自国政府とのつながり（多くの場合、確立されている）を武器に、おのおのの市場で安定した基盤を築いている。そして、それらの通信会社がここ数年で被害に遭ったセキュリティ侵害事案は、たとえあったとしてもごくわずかであり、特に数多くのOTT[3]と比較すると、その数は極めて少ない。

規制への対応力： OTTなど潜在的な競合と異なり、通信会社は既に厳しい規制の対象となっており、規制当局（日本では総務省）の要求に応えるうえで必要な作法をわきまえている。通信会社はそうしたポジションを足掛かりにして、「規制当局認定という信頼感」をユーザーおよびサービスプロバイダーへ一様に与え、競争優位を得ることができる。ロビイストと規制関連のスペシャリストから成るよく組織されたチームが、不可避的に訪れる政府関連の難題や事業機会の中でうまくかじ取りする上で力になる。

データプラットフォームの構築

以上の貴重なアセットのおかげで通信会社は、データエコノミー関連事業における重要な機能を提供できるはずである。つまり、ユーザーとデータ集約型サービスプロバイダーの両方が自身のオンライン作業を非公開で安全に行い、かつ、自身の個人データを誰にどのような条件で開示するかについて選択できるようにするデータプラットフォームを構築できるに違いない（図表4参照）。

現在、通信ネットワークは主に、ユーザーとサービスプロバイダー間のデータのやり取りを受動的に可能にするという「ダムパイプ（土管）」の機能を果たしているにすぎない。各サービスプロバイダーは、サービスの提供内容、トランザクションおよびパーソナライゼーションまわりの取り決めを各ユーザーと直接決めなければならない。

これはデータプラットフォームにより一変する。データプラットフォームは、プライバシーやセキュリティ、アイデンティティ管理など、ユーザーおよびユーザーがやり取りをするオンライン企業の、データに関する数多くのニーズをカバーする機能群と、ユーザーが生成するデータについてユーザーが所有権を取得し収益化することを可能にするソフトウェアやアプリで構成されることになる。通信会社と、ヘルスケアや金融サービス、メディアなどシステムにつながるその他のサービスプロバイダーは、ユーザーのデータプラットフォームに接続でき、自社のサービスを提供する。そしてユーザーは、アプリを使用して各サービスプロバイダーとのつながりを一元管理する。

業界はこれをB2B2Cプロセスと呼んでいる。エコシステムの一方では、システムを構築するプラットフォーマーがサービスプロバイダーと契約を結ぶ。そして他方では、プラットフォーマーは消費者を取り込む。システムの成否はプラットフォーマーに対する信頼に大きく左右される。消費者へのアクセス獲得と信頼性に関するブランドの評判向上を呼び水にサービスプロバイダーに参加してもらう一方で、プラットフォームのアクセス性、信頼性、安全性が常に担保されると消費者に信じてもらわなければならない。

このような針路を取るプラットフォーマーは、こうしたプラットフォームの構築に求められる技術的要件に加え、「パートナーシップ」と「行政への対応」という2つの重要なケイパビリティも磨かなければならない。

パートナーシップ： データプラットフォームの導入には、他のコネクティビティ会社およびさまざまな業界における各種サービスプロバイダーとの協力が求められる。パートナー企業の中には、同時に規模の拡大を模索する企業もあるだろう。例えば、国内ベースの通信会社は国内外の他の固定電話・携帯電話・ケーブルテレビ事業者と提携し、最大限のエリアを網羅す

3：動画コンテンツや音声通話、SNSなどインターネット経由でサービスを提供する事業者、オーバー・ザ・トップ

るデータプラットフォームを提供しようとするかもしれない。また、企業価値を追求するパートナーシップもあるだろう。その場合、成否は提供するサービスの種類に大きく左右されることになる。こうしたパートナーシップを構築する際、通信会社はさまざまな障害を乗り越えなければならない。例えば、独占禁止法に関する問題、戦略の不一致、テクノロジーおよびネットワークの統合に伴うハードル、求められる変化のペースに対する見方の相違、それぞれのリスク回避文化、そして有能な人材確保の難しさといった障害が待ち受けている。パートナーシップを成功させるためには、オープンイノベーションと入念なコラボレーションを促すことでこうした障害を乗り越える必要がある。

行政への対応： データプラットフォームの構築においてプラットフォーマーはまた、政治にも大きな役割を担ってもらうよう働きかける必要がある。つまり、何もしなければ完全民間型データエコシステムの立ち上げを阻害しかねない公共政策や規制を動かす必要がある。事業者は、「デジタルアイデンティティに対する権利」や「忘れ去られる権利」などデジタルまわりの権利を総合的に整備するよう働きかける必要があるだろう。現在、ほとんどの法域がデジタルまわりの各種権利を明確に定めていない（コネクティビティへのアクセスに関する権利を定めている国や、プライバシーに関し一定の規制を整備している国もあるが、それ以外のものについて）。企業による個人データの収集・使用・転売のあり方を規定し、かつそれら企業のデータまわりの業務について高い可視性を求める、より厳格な規制を要求しなければならないだろう。そして、大量の個人データを保管する企業間の公正な競争に関するルールを確立させる必要もあるだろう。

機会の核心

ユーザー、サービスプロバイダー、そして通信会社はみな、新たなデータプラットフォームについて行動を決定する重要な機会を有する。ユーザーによっては、個人データの流れをほぼ完全に制限する設定をするだろう。そうしたユーザーは、必要最低限の本人認証データしかオンライン上で共有することを承認しない。その場合も共有する相手を基本的に、定期的な取引のある銀行やeコマース企業に限定するだろう。

他方、見返りに何か価値のあるものが得られると見越し、個人データの使用についてもっと自由度が高いユーザーもい

図表4
未来のデータプラットフォーム

通信会社が設計・管理するインフラを通じて、データは黒色の矢印でここに示すように流れる。
つまり、ユーザーから通信会社のネットワークを経由して、データがサービスプロバイダーへ流れるようになる。

出所：Strategy&分析

るだろう。eコマース企業は、購買傾向に関するデータを収集・購入させてくれる顧客に対しては特典を与えるかもしれない。消費者はまた、自分の行動を追跡し匿名化された大量のデータの中でそれを使用する権利を企業に売るようになるだろう。2025年までには大半のインターネット利用者が数千にのぼるデータポイントを生成するようになると考えられるため、販売できるデータはかなりの量に達する。

通信会社は、自身のプラットフォームを利用するユーザーとサービスプロバイダーとの間で取引が行われるごとに少額の手数料を徴収し、現在のクレジットカード会社とよく似た機能を果たせる可能性がある。AIを活用してユーザーのデータを独自に予測分析し、取引先へ提供することもできる。または、各種手数料ベースのサービスをユーザーと企業へ一様に提供することもできる。不正防止やデジタルプライバシーの管理、本人認証、デジタルトランザクションの保証、加盟サービスプロバイダー向けの予測分析などを提供できるだろう。最終的には、消費者向けのコンテンツやアプリ、広告、eコマース関連のお得な情報などデジタルエクスペリエンスをユーザーのために整理するパーソナライズキュレーションの提供までも検討できるだろう。

確かに、通信会社がテクノロジーを牽引したという例はこれまで少なかった。この機会をつかむためには大胆な企業文化の変革が求められる。しかしながら、こうした方向に進み始めれば、成長への明瞭な道筋が目の前に現れ、顧客に信頼される透明性の高いパートナーとなる。そしてデジタル世界へのアクセスとデジタル世界をコントロールする力を顧客に与えることで、あらゆる価値と評判の向上を実現できると期待できるであろう。

"Tomorrow's Data Heroes" by Florian Gröne, Pierre Péladeau and Rawia Abdel Samad, strategy+business, February 19, 2019

データ保護の強化に、いかに対処するか

著者：ジョー・ノセラ
監訳：米本 和希

欧州を中心に、個人データ保護に向けた動きが加速している。2018年5月にEU一般データ保護規則（GDPR）が施行され、企業が個人データの侵害を認識してから、原則72時間以内に監督機関へ通知する義務が発生するなど、個人データ保護にかかる企業への要求は年々高まっている。しかしながら、複雑化するデジタル社会において、新たなサイバーリスクの把握と管理に悪戦苦闘している企業も少なくない。本稿では、重要性が増すデータセキュリティについて企業がどのように対応すればよいか、サイバー攻撃に耐え得る危機対応力の構築に向けて考慮すべきポイントについて紹介する。（米本 和希）

消費者は自分の個人情報の扱いについて誰を信じればよいか分からないと感じている。PwCの最新の調査であるConsumer Intelligence Series: Protect.meによれば、自分の個人情報を企業が責任を持って扱ってくれると思うと回答したのはわずか25%で、政府による個人情報の保護について信頼できると答えたのはわずか17%だった。同時に69%の消費者は、企業はハッキングやサイバー攻撃に脆弱であると感じており、85%は情報セキュリティへの取り組み方に不安な点がある企業とは取引をしないと答えている。消費者がこれらを行動に移すかどうかは別としても、本調査結果は消費者が企業や政府のサイバーセキュリティ対策に抱く信頼感が低いという現状を浮き彫りにしている。

しかし、米国の消費者2,000人を調査したProtect.meでは、行動を起こせる企業にとってはチャンスとなる、前向きないくつかの情報も得られた。回答者の72%は、政府よりも企業の方がデータ保護の体制が整っていると感じており、81%は政府よりも企業に自身の個人情報の保護を行ってもらいたいと思っている。もちろん政府による規制は役立っている（回答者の82%が、企業によるデータ利用は政府が規制すべきだと答えている）。既に金融サービス業界とヘルスケア業界では政府による規制が行われており、それらの業界に関しては消費者の信頼が高いことがPwCの調査でも分かっている。しかし、データセキュリティについていえば、消費者は企業に高い期待を抱いていること、そしてその期待に添える企業は自社の利益を保護しながら信頼を築けることは明らかである。

多くの企業にとってこの目標への道のりは長い。122カ国9,500人のエグゼクティブの考えを調査したPwCのグローバル情報セキュリティ調査2018（GSISS）では、回答者の44%が包括的な情報セキュリティ戦略を策定していないと回答している。さらに多くの回答者（48%）が従業員に対するセキュリティ意識啓発のトレーニングプログラムを用意していないと回答しており、54%がインシデントレスポンスにかかわるプロセスが未策定と回答している。消費者から求められる今、企業は以下の手順を踏みサイバー攻撃に耐え得る危機対応力を構築する必要がある。

1. 取締役会を含む経営幹部メンバーを巻き込む。GSISSでは、自社の取締役会がセキュリティ戦略に積極的に参加しているという回答はわずか44%にすぎなかった。これは一部の企業がサイバーセキュリティを単にITの問題ととらえているからだと考えられる。しかし取締役会がサイバーセキュリティ戦略に関与すると、経営幹部はサイバーセキュリティ戦略を優先課

ジョー・ノセラ

PwCのプリンシパルで、シカゴを拠点とする。金融サービス業界向けのサイバーセキュリティおよびプライバシーサービス業務におけるリーダーを務める。

米本 和希（よねもと・かずき）
kazuki.yonemoto@pwc.com

PwCコンサルティング、Strategy&のシニアアソシエイト。電子機器メーカー、自動車メーカー、IT関連企業などに対し、事業戦略の立案および実行支援などのプロジェクトに数多く従事している。

題ととらえる傾向が高まることをこれまでの事例が示唆している。取締役会が関与すると、サイバーリスクはIT部門の単なる日常的な懸念事項からその企業の全社的な戦略計画の一部へと格上げされ、大規模なセキュリティ侵害にかかわるリスクと同程度の重要度が付与される。

情報セキュリティ戦略と予算のレビューに経営幹部を関与させると、サイバーセキュリティの優先度をさらに高められるだろう。これにより、特定のシステムやデータに障害が発生した場合に何が危険にさらされるのかが明確に把握でき、また最も緊急のリスクを軽減するための確実な計画を整えることもできる。企業が最高情報セキュリティ責任者（CISO）の権限をITの枠を超えて引き上げ始めていることがGSISSで明らかになったのは良い傾向だ。回答によればCISOがCIOの直属ではなく、CEO（40%）または取締役会（27%）の直属であることが一般的になってきている。

2. ネットワークの相互依存性を評価する。企業は自社のネットワークが依存するさまざまなネットワークを注意深く見ていく必要がある。これには会社の機密データが短期・長期で収容される可能性のある公共の送電網から第三者ネットワークやクラウドベースのネットワークまで含まれる。脆弱性は企業が所有するネットワークから何層か隔てたところに存在する。しかし停電になるまで自分がいかに電気に依存していたかに気が付かないように、ネットワークの相互依存性にも大惨事が起きてからでないと気が付かないことが多い。

例えば、サイバー攻撃が発生した際に、多くの企業は犯人を明確に特定できないという。GSISSでも攻撃元を特定する能力に強い自信を持っていると回答したのはわずか39%にすぎない。このギャップを埋めるために、企業幹部はサイバー攻撃を想定したシナリオで相互依存に対するストレステストを行う必要がある。また企業は、例えばIoTなどネットワーク上にあるシステムを悪用しようとする新しい技術について調査することも重要である。しかし、自社にビジネスエコシステム全体のIoTのリスクを評価する計画があると答えたGSISS回答者は比較的少数だった。IoTのセキュリティにおける責任の所在は企業によってさまざまで、29%がCISO、20%がエンジニアリングスタッフ、17%がCRO（最高リスク管理責任者）であるとしている。

3. データ操作とデータ破壊に注目する。サイバー攻撃が高度化するのに合わせて、企業のサイバーセキュリティの優先課題も常に適応させていかなければならない。企業はかつてデータの盗難を最も恐れていた。しかし、最近はハッカーが企業のITシステムやITアーキテクチャを、企業および社会全体に対してどのように悪用し得るかを企業幹部は知っておかなければならない。サイバー攻撃をする人たちの主な目的にはクレジットカード番号を盗むといった金銭目的だけではなく、データ操作によりその企業や個人に害を与えることも含まれるかもしれない。例えばもし犯人が病院のカルテにアクセスしデータ操作をしたり、航空管制システムを書き換えたりした場合、多大な被害が生じるだけでなく、人命が危ぶまれる事態にまで発展する可能性がある。

ハッカーは、いかにしてITシステムやITアーキテクチャを企業および社会全体に向けて悪用し得るか。企業幹部は知っておかなければならない。

組織はサイバーセキュリティ評価に際し、インサイドアウトのアプローチを取る必要がある。すなわち、自社において脆弱性がある領域を探し、攻撃を受ければ人の命や安全にかかわるシステムを優先して防護していく必要がある。そしてシナリオ・プランニングを行い「考えられないことを考える」と同時に、シミュレーションを行い自社がそれらの攻撃に耐え得る準備が

できているかを確認するべきである。また万一セキュリティ侵害が発生した際にはすぐに対応できるよう態勢を整えておかなければならない。金融分野のシェルタード・ハーバー（守られた港）イニシアチブ[1]では、他分野でのこうした新たなデータ破壊リスクへの対応に役立つモデルを提供できる可能性がある。この取り組みでは、銀行が大規模なサイバー攻撃を受けた際に口座データを復元・復旧するために役立つ標準が策定されている。

サイバー脅威は常に変化している。これら三つのステップに沿って対策を始めた企業は、進化するサイバー脅威をより深く理解できるようになると同時に、企業幹部が自らサイバー脅威に対する危機対応力の向上に最優先で取り組むような環境を醸成することができる。この危機対応力は大規模なサイバー攻撃により引き起こされる金銭的、風評的、法的大損害から企業を守ることができる。消費者はそこに注目している。

"How Companies Can Respond to Consumers' Demands for Better Data Protection" by Joe Nocera, strategy+business, December 19, 2017

1：米国の金融業界は、2017年にこの取り組みを開始。金融機関がハッキングやDDos攻撃を受けた際、他行が代理で顧客向け業務を継続できるようデータをそれぞれバックアップする

セキュリティベンダーの重要性と影響力の増大

著者：樋崎 充、大塚 悠也

AI、IoTなどのテクノロジーの進展に伴いセキュリティは、社内システムを守るものだけではなく、顧客への製品・サービス提供においてもキーファクターとなる。本稿では、サイバーセキュリティが経営にどのような影響を与えるのか、少し先の未来を想像した上で論じてみたい。

欧米に遅れる日本の経営

近年、サイバー攻撃が増加している。パソコン、インターネットが普及し始めた当初は各種システムへの侵入目的は腕試し、興味本位が主だったが、徐々に金銭や企業の機密情報奪取へと目的が移りかわっている。一説には、セキュリティ産業のグローバルの市場規模が8〜9兆円弱に対し、サイバー攻撃のブラックマーケットは12兆円を超えるともいわれる。さらには水面下では国家間のサイバー攻撃も激しさを増しているといわれている。そのため政府は、サイバー防衛隊を2023年度までに約500人と現状の3倍超に増やすことを計画している[1]。しかし、米国のサイバー攻撃に対応する部隊は約6,000人、予算は約2.2兆円（2017年、日本の予算は632億円）、北朝鮮のサイバー部隊は約7,000人、中国は数万人規模ともいわれ文字通り桁が違う状況である。

以前はパソコンのセキュリティを担保することが中心であったが、スマートフォンやIoT機器の普及に伴いさまざまなデバイスでセキュリティ侵害のリスクが増加している。総務省も家庭用のIoT機器の調査および利用者への注意喚起の取り組みを2019年2月から開始した。

企業においてもさまざまなサイバー攻撃による被害が起きている。世界150カ国・地域でデータを暗号化し身代金を要求するランサムウェア（WannaCryなど）や航空会社の経理担当者に向けた詐欺メールによる金銭奪取などが記憶に新しい。

サイバーセキュリティはもはや経営の問題として捉えなおすべきだという論調もある中、日本はいまだ意識が低い状況にある。経営との橋渡しが期待されるCISO（情報セキュリティ最高責任者）の任命率も欧米と比較すると20ポイント以上の差があり、専任のCISOも少ない（図表1参照）。また、日本のCISOに求められるものは技術・スキル面に片寄っており、経営との橋渡しや事業目標との整合を期待する向きも少ない（図表2参照）。

サイバーセキュリティは自社の防衛とともに顧客へセキュアな製品を届けるという守りと攻めの両側面があり、テクノロジーの進展に伴い両側面ともますます強化する必要性が高まる。

守りを重ねる日本、重要な資産を守り抜く米国

これまで日本の企業は、被害を発生させないためにも「防御」することに注力してきた。その結果、さまざまな製品を組み合わせた多層防御が築かれている。ファイアウォールを設置し、アンチウイルスソフトを入れ、ソフトウェアにパッチを当てるといった対策を行い、さらにIPS（不正侵入防止）やWAF（WEBアプリケーションに特化したファイアウォール）などのセキュリティ製品を重ねて、複数の防御策を組み合わせている企業が多数存在する。

これに対し米国では多層防御にとどまらず、侵入されることを前提とした上で、対処するという考えが浸透している。具体

1：2019年2月20日付 日本経済新聞 「防衛省、サイバー反撃で専門人材」，https://www.nikkei.com/article/DGKKZO41466640Z10C19A2MM8000 ［2019年3月25日閲覧］

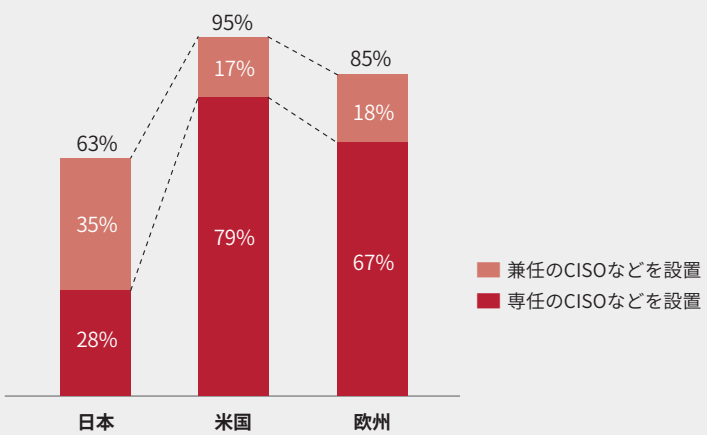
樋崎 充（といざき・みつる）
mitsuru.toizaki@pwc.com

PwCコンサルティング、Strategy&のパートナー。約15年にわたり、IT関連企業、総合電機メーカー、電子部品メーカー、製薬会社に対し、事業戦略、組織戦略、M&A戦略、SCM戦略の立案および実行支援などのプロジェクトを手がけてきた。

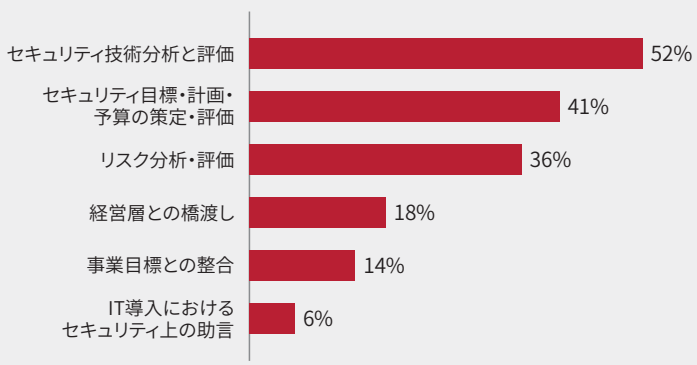
大塚 悠也（おおつか・ゆうや）
yuya.otsuka@pwc.com

PwCコンサルティング、Strategy&のシニアアソシエイト。事業会社を経て戦略コンサルティングに約7年従事。ハイテク業界を中心に製造、サービス、金融など幅広いクライアントに対する、全社、事業戦略の立案および実行支援などのプロジェクトに取り組む。

図表1
CISO任命率



図表2
日本において重要視されているCISOの役割



出所：IPA「企業のCISOやCSIRTに関する実態調査2017」（小数点以下は四捨五入）

的には、組織において守るべき資産（システム・データなど）を「特定」し、そのための「防御」策を施し、防御策が突破された場合に「検知」し、隔離などの「対応」を行い、「復旧」させるという考え方である。これは2014年に重要インフラ向けのベストプラクティスのセキュリティ対策フレームワークとして米国国立標準技術研究所（NIST）が提示をしたものであるが、重要インフラだけではなく、どの企業においても取り入れられる考え方である。

「攻められないためにも多重の守りを重ねに重ねる日本」と「攻められても重要な資産だけは守り抜くことを考える米国」。恒常的にリアルな戦争に直面し、まことしやかに国家間でのサイバー戦争を繰り広げているといわれる米国に比べると、言語のバリアーなどもあり、まだサイバー被害が比較的少ない平和な日本との間で思想の違いがあらわれているように思われる。

現実的には、完璧に防御しきることは困難であるため、攻められる/侵入されることを前提に対策を考える必要があるだろう。日本企業も重要な資産を守り抜く発想に切り替えていく必要がある。しかし、重要な資産を守り抜くためには、そもそも自社の資産を把握しきることが必要であるが、自社の守るべき資産を把握しきれていない企業が大半ではないだろうか。特に日本企業は外部のシステムベンダーにさまざまなシステム構築を依頼しているため、ベンダー各社は構築部分を把握しているが、発注企業側が全体を把握しきれていないなどということは往々にしてある。Strategy&で重要インフラを運営する企業を含む複数社に独自にヒアリングしたところ、資産を把握し、どのシステムが攻撃されるとどこにどれだけ影響があるかをサイバーセキュリティの観点から検討しきれている企業は、皆無に等しかった。

2019年は20カ国・地域（G20）首脳会合、ラグビーワールドカップ、2020年には東京オリンピック・パラリンピックなどと国際イベントが目白押しであり、ハッカーにとっては自身の攻撃能力をアピールする絶好の機会である。2012年のロンドンオリンピックでは、電力システムへのDDoS攻撃（分散型サービス妨害攻撃）などがあり、2016年リオデジャネイロオリンピックでは、情報漏洩が発生し、2018年平昌オリンピックでは、不正プログラムなどによりITシステムが停止している。また、近隣の複数のスキーリゾート施設でもゲートとリフトの操作を行えなくなったなど、オリンピック会場だけではなく、その周辺や関与した関係者など、さまざまな場所・人が狙われた。

無差別な攻撃の中に、政府機関、公共施設、研究・教育機関、交通機関、ライフライン、化学・石油などの重要産業やその取引先を狙った一点突破の攻撃が今後1〜2年で行われる可能性が高まっている。さらには、最悪のシナリオとして想定されるのは2020年を境に日本語を活用した標的型攻撃の精度が高まることである。今までは同じ攻撃を行うなら、経済大国とはいえ日本語という言語バリアーを有する日本に対してサイバー攻撃を行うよりは、英語を使用して欧米中心に標的型攻撃を行う方が確率論的には攻撃者にとって効率的であったが、東京オリンピックなどを契機に経験を積んだ攻撃者が日本語のバリアーも突破することも想定されるのではないか。今後、日本においても深刻化するであろうサイバー攻撃には、侵入を前提とした上で、本当に守るべきものは何かを検討すること、そして、まず資産の把握から始める必要があるだろう。

セキュアな製品を届けるという視点

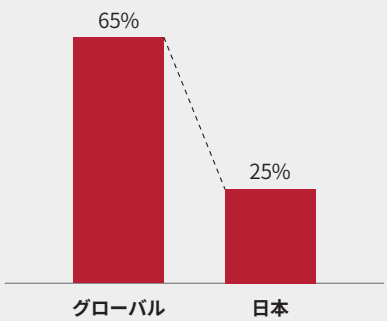
一方、セキュリティは自社防衛だけでは足りず、顧客への製品提供でも必須になっていく。

近年消費者の嗜好が多様になる中、モノを売って終わりではなく、顧客を継続的にサポートしながらその満足を追求するいわゆるas a Serviceモデルへとビジネスを転換しようとする動きが各社に見られる。そのための効果的な手段としてコネクテッド、主にインターネットを介して繋がり続けるサービスが模索されている。

しかし、インターネット空間と繋がるということは、一方でサイバー攻撃の脅威にもさらされ続けていることになる。近年では、さまざまなデバイスがコネクテッド/繋がる製品として発売される中、同時にハッキングの事例も増え続けている。

例えば、2015年には米国のセキュリティ研究者が遠隔からカーナビシステムを経由して自動車へ侵入。エンジン制御などに関わるシステムを不正に作動させる実験に成功した。この結果、開発自動車メーカーは140万台のリコールを行う必要

図表3
開発におけるセキュリティアセスメント実施企業の割合



出所：PwC「グローバル情報セキュリティ調査2017 Vol.3：IoTの可能性を探る」

が生じた。

また、同じく米国での医療機器ハッキング事例として、体内に埋め込んだペースメーカーで取得したデータをサーバーに送信し、ペースメーカーのファームウェアのアップデートを行う機器がハッキング可能であったケースが存在する。

製品・サービスをコネクテッドにすることは、上記のようなリスクがあることも理解しなければならない。この点、PwCのグローバルセキュリティ調査によると、研究開発フェーズからサイバー攻撃の脅威を多角的に分析し、当該コネクテッドな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、次工程の製造フェーズに受け渡すといった綿密な設計（セキュリティアセスメント）をできている日本企業は海外に比べて著しく低いことがわかる（図表3参照）。

一部の大企業では、このようなリスクに対処するため、製品の開発から販売後のアフターフォローまでをセキュリティの観点から一貫して責任を持つ社内組織（PSIRT）の設置を行う企業も出てきているものの、実運用に至っている企業は殆どなく、緒に就いたところである。

拡大するセキュリティベンダーの影響力

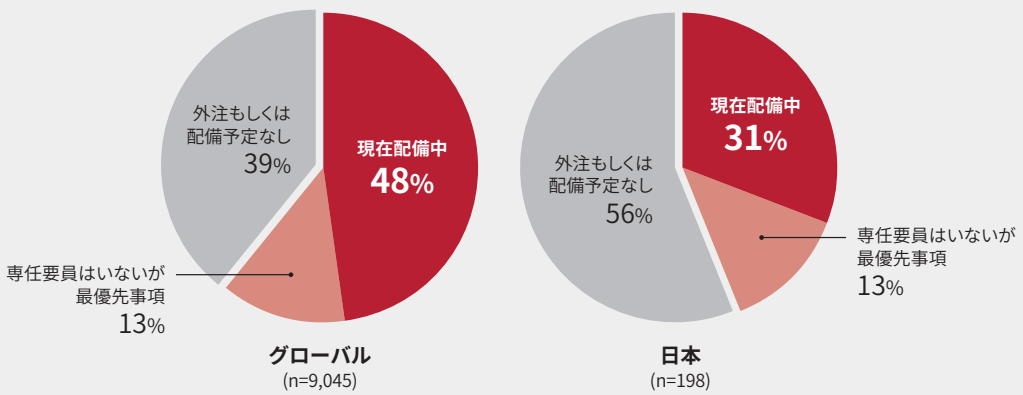
さらに未来に目を向けると、IoTやAIなどが今後進展していくことに疑いの余地はないだろう。コネクテッドカーとして自動車が制御され、スマートホームとして住宅が繋がり、政府や地方自治体も巻き込み街灯、信号、交通監視や各種建物、インテリジェントビルディングなどが繋がるスマートシティーが作り出され、消費者の利便性と生活の質の向上、また行政のコスト削減が果たされていくだろう。

そして、一部の大手企業がセキュアな製品を提供すれば良いのではなく、全ての会社に今以上にセキュアな製品が求められる日がくる。たとえ大手自動車メーカーが、コネクテッドカーに万全のセキュリティ対策を行って発売したとしても、それと繋がる自社製品に万が一にも脆弱性があり、そこからコネクテッドカーがハッキングされたとしたら、社会にも自社にも甚大な被害を及ぼすかもしれない。

大企業・中小企業問わず、自社の製品がさまざまなモノと繋がる世界では、自社の根幹となる業務システムや工場/プラントだけではなく、顧客への提供製品・サービスにもサイバーセキュリティ対策が必須となる。

図表4

社内ビジネス部門をサポートする専任セキュリティ要員を雇っているか



出所：PwC「グローバル情報セキュリティ調査2017 先進的サイバーセキュリティおよびプライバシーの実現」

このような未来に対応していくためにセキュリティベンダーは、各製品にマルウェア[2]が侵入してきた際に悪さの前兆を検知する仕組みを提供していくだろう（当然、侵入されないことが最良ではあるが、100%侵入を防ぐことは不可能に等しい）。彼らは、膨大な数のマルウェアの挙動、振る舞いをデータベース化しており、既知/未知のマルウェア問わず、被害を起こす直接的なアクションよりも前にその予兆を検知し、対処をするための技術を日々ビッグデータ解析により磨いている。自社製品の挙動とこの仕組みを突き合わして異常を検知するためには、セキュリティベンダーが製品の挙動を理解する必要があり、そのためにもログやプログラムや開発過程を公開する必要が出てくる恐れがある。セキュリティベンダーに対し自社の製品を丸裸にせざるを得ない日が来るかもしれない。

これだけでも、十分リスクではあるが、仮にセキュリティベンダーが使用許諾を突然停止したら発売済みの製品が安全に使えなくなってしまう恐れもある。また政府の意向で特定メーカーの通信機器を排除したように諸外国のセキュリティ製品が急に使えなくなることもあるかもしれない。米国系大手ITベンダーがさまざまなデータをおさえたことが各国で問題となっているが、セキュリティレイヤーもまた米国系が強固になると、設計・開発から発売、その後のフォローまで一連の仕組みや製品のログ、プログラムなども実質的におさえられてしまうことになるのではないか。せめてもの対策として国内のセキュリティベンダーを活用することも考えられるが、残念なことに日本のセキュリティベンダーでグローバルスタンダードになれているものはほとんどないのが実情である。セキュリティ製品を思い浮かべていただいた際に、純国産企業が浮かぶ方は多くはいないのではないか。

上記リスクに対処する一つの方法としては、自社でセキュリティ対策を内製化していくことが考えられる。自社製品に最も詳しいのは自社であるため、自社製品の平常状態からの外れ値を異常と規定してマルウェアの異常な挙動を捉えにいくことにより対処ができるかもしれない。

しかし、セキュアな開発を行うための人材確保が今後大き

2：マルウェアとは悪意のあるソフトウェアや悪質なコードの総称。コンピューターウイルスはマルウェアの一種

な問題となるだろう。もともと日本はIT構築を外に発注する傾向にあり、セキュリティにおいても同様である。日本は諸外国と比べても自社専任のセキュリティ要員を確保できていない状態にある（図表4参照）。さらには、数十万人の単位でセキュリティ人材が不足するという試算もある。

平成の時代30年はインターネットとともに急激なスピードで変化した。このスピードは、今後ますます加速していく中、企業の5年、10年先を見据えて、セキュリティを自社のビジネスの中にどのように取り込むべきなのか。今まさに経営者が真剣に考える時期に来ているのではないだろうか。

サプライチェーンセキュリティにおけるビジネスの可能性

著者：樋崎 充、鈴木 裕士

近年高まりを見せているサプライチェーン攻撃の脅威に対応するためには、グローバルでの議論が必要となる。この議論の先には新たなビジネスの出現、既存ビジネスモデルの変貌の可能性が垣間見えるが、これらのビジネスを積極的に取り込むためには、議論を先導していく姿勢が必要となるだろう。

サプライチェーン攻撃に対する脅威の高まり

近年、サプライチェーン上のサイバーセキュリティに対する脅威が高まってきている。サプライチェーンの一連の過程でマルウェアに感染させる攻撃はサプライチェーン攻撃と呼ばれており、いくつかの事例も公表されている。

2017年、ウクライナの税務会計パッケージソフトMEDocの正規更新システムに何者かが管理者権限でログインし、ルート権限を取得、更新プログラムを改ざんすることでバックドアが埋め込まれた。バックドアはマルウェアの一種で、バックドアが存在するとサイバー攻撃者が容易にシステムに侵入できるようになってしまう。改ざんされた更新プログラムをインストールしたユーザーはバックドア型マルウェアに感染してしまい、ネットワークを通じて別のユーザーにも感染が広がっていった。ユーザーはその多くがウクライナの国内企業や組織、また同国と取引のある多国籍企業で、被害はウクライナから欧州全域に広がった。

また、同年には別の深刻な事例も報告されている。世界で数百社の大手企業にサーバー管理ツールを提供している、韓国のNetSarangが配信したソフトウェアのアップデートに、バックドアが埋め込まれていることが発見された。このバックドアは、NetSarangの正規ソフトウェアの更新プログラムが改ざんされて仕込まれており、この更新プログラムをインストールすると、攻撃者によるデータの窃取、外部送信が可能な状況となっていた。ロシアのセキュリティベンダーであるKaspersky社からの連絡を受けたNetSarangは、直ちにバックドアを削除した更新プログラムをリリースすることで解決した。これまでのサプライチェーン攻撃の中でも最大規模の一つと言われており、素早く検知、解決していなければ、世界中の数百もの組織が攻撃の被害に遭っていた可能性があった。

これらの事例も受け、Kaspersky社は、2018年脅威予測レポートにおいてサプライチェーン攻撃の増加を予測し、世間の認識が高まる契機となった。公表されている事例以外にもサプライチェーン攻撃は多く存在していると考えられており、実際に、2018年にセキュリティベンダーのCrowdStrike社が行ったアンケート調査によると、回答企業の3分の2がサプライチェーン攻撃を受けた経験があり、そのうちの半分（全体の3割超）が直近1年以内に攻撃を受けていた（図表1参照）。また、Kaspersky社による2019年の脅威予測レポートにおいても、サプライチェーン攻撃は継続され、引き続き注意が必要であると警告されている。

米国では、疑わしい企業を排除することでサプライチェーン上のセキュリティを確保しようとしており、中国ハイテク企業に対して強硬姿勢を打ち出している。その根拠となっているのが2018年8月に可決された「2019年度米国防権限法（NDAA2019）」で、同法は2019年8月13日以降、政府機関・軍・政府所有企業が中国ハイテク5社（ファーウェイ、ZTEなど）の製品や部品を組み込んだ他社製品を調達することを禁じている。さらに、2020年8月13日以降に適用される規制では、当

樋崎 充（といざき・みつる）
mitsuru.toizaki@pwc.com

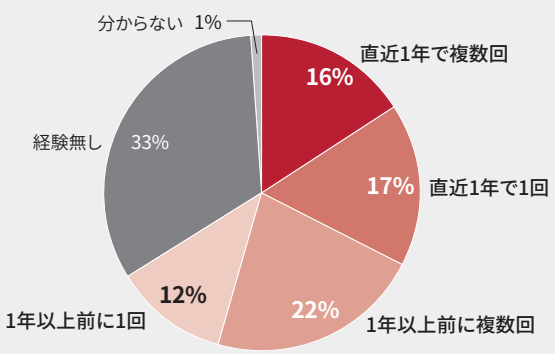
PwCコンサルティング、Strategy&のパートナー。約15年にわたり、IT関連企業、総合電機メーカー、電子部品メーカー、製薬会社に対し、事業戦略、組織戦略、M&A戦略、SCM戦略の立案および実行支援などのプロジェクトを手がけてきた。

鈴木 裕士（すずき・ひろし）
hiroshi.suzuki@pwc.com

PwCコンサルティング、Strategy&のアソシエイト。製造業・商社などのクライアントに対するセキュリティ技術調査支援、新市場参入戦略策定などのプロジェクトに取り組む。

図表1
ソフトウェアサプライチェーン攻撃の経験時期・回数

（n=1,300）



出所：CrowdStrike Supply Chain Survey 2018（July, 2018）

該5社の製品を社内で使用しているだけで、米政府機関と取引ができなくなる。このような強硬策を打ち出している理由の一つに、これらの企業の製品にバックドアが仕込まれ、機密情報の漏洩や、有事の際に製品の性能低下・無力化が行われるのではないかという懸念がある。日本においても、企業の名指しはしないものの、安全保障上の脅威がある場合は、政府調達で制限できる仕組みの導入が発表された。

米国のように疑わしい調達先を排除することでセキュリティを高めることも可能ではあるが、外交上の問題が生じることもあり、簡単ではない。また、調達の代替先も完全に安全とは言い切れないため、実際には別途対策をとる必要がある。

製品の調達時にセキュリティを検査する技術として、静的解析や動的解析が存在する。静的解析では主にソースコード検査が行われ、セキュリティ上のリスクがある既知のコードを検出する。動的解析では主にファジングと呼ばれる検査が行われ、検査対象に問題が起きそうなさまざまなデータを入力して異常な動作が起きないかを確認することで、問題を検出する。実務的にはこれらの手法を組み合わせて効率的・効果的な検査を試みている。また、外部接続されたネットワークを通じて疑似的な侵入テストを行いシステムやネットワークのセキュリティをチェックする、ペネトレーションテストも存在する。しかし、個々の企業では、これらの検査技術は開発工程には組み込まれている場合はあるものの、調達時にはほとんど実施できていないのが現状である。

図表2
開発プロセス内でのセキュリティ評価・検証方法

プロセス	セキュリティ評価・検証	概要
製品企画・設計（要件定義）	• 脅威分析	• 守るべき資産の想定、想定される脅威とビジネスインパクトの分析、対策方針と設計方針決定
	• セキュアプログラミング	• 必要なセキュリティ対策が設計書に含まれているか確認
調達	• 受け入れ検査	• 一般的な手法が確立されておらず、受け入れチェックは ほぼできていない
実装	• ソースコード検査	• コーディング規約に基づく実装が行われているかどうかや、脆弱性*を検証
テスト	• ファジング	• 不正データを検査対象に送信、挙動から脆弱性を検出
	• 脆弱性スキャン/ペネトレーションテスト	• ツールを用いて脆弱性を検出し、脆弱性からシステムに侵入が可能か、侵入された場合の影響の大きさを検証
運用	• 運用時対策/脆弱性対策	• 脅威や脆弱性情報の収集、定期的な修正プログラムの適用など

* 脆弱性：プログラムの不具合や設計上のミスが原因となって発生したセキュリティ上の欠陥

出所：IPA「ファジング活用の手引き」（2018年7月）を基にStrategy&が作成

セキュリティリスクに対する海外の取り組み

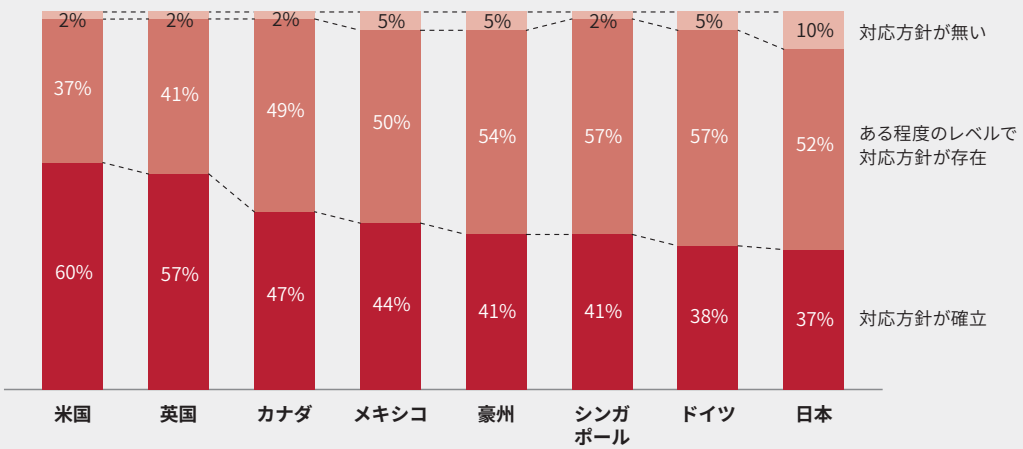
図表3は、ソフトウェアサプライチェーン攻撃を受けた際の対応方針の有無の企業割合を、国別に示している。いずれの国も日本より対応方針が確立されている割合が大きく、特に米国で、サプライチェーン上のリスク認識が高いように見受けられる。

米国では、米国国立標準技術研究所（NIST）により、Cybersecurity FrameworkやNIST SP800-171のような、サプライチェーンリスクに対応したフレームワークが制定されている。2014年2月にVersion 1.0が策定されたCybersecurity Frameworkでは、サイバーセキュリティ対策の全体像が示されており、「特定」「防御」「検知」「対応」「復旧」に分類して対策が記載されている。Version 1.1が2018年4月に策定され、そこではサプライチェーンのリスク管理の重要性が説かれており、サプライチェーン全体でセキュリティ対策を実施することが要求されている。NIST SP800-171は2015年6月に発表され、2018年6月にはアップデート版が発表されている。米国政府機関が調達する製品や技術を開発・製造する企業に対して求められるセキュリティを担保するためのものであり、既に米国防総省は取引事業者に準拠を求めている。

さらに、IoT機器のサイバーセキュリティについて、米国政府が第三者認証を準備していることが確認されている。2016年2月に発行されたCybersecurity National Action Plan にて、米国土安全保障省（DHS）がIoT環境下でつながる機器を試験・認証するためのサイバーセキュリティ保証プログラムの開発において、民間の第三者認証機関であるUL社や産業界

図表3
ソフトウェアサプライチェーン攻撃を受けた際の対応方針の有無

(n=1,300)



出所：CrowdStrike Supply Chain Survey 2018 (July, 2018)

と協力をしているとの記述がある。UL社は2015年よりCyber Assurance Program (CAP) というサイバーセキュリティ認証プログラムを開発しており、一部はANSI (米国国家規格協会) 規格となっている。今後、ISO (国際標準化機構) やIEC (国際電気標準会議) において標準化される可能性も考えられる。

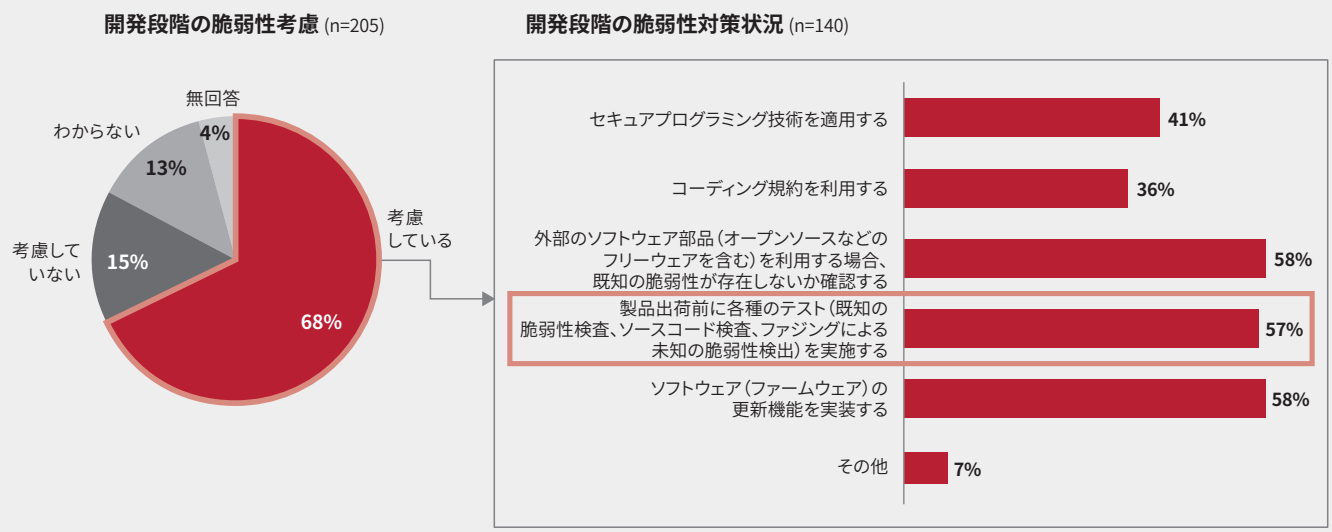
また、サプライチェーン上のセキュリティ向上のために、米国商務省電気通信情報局 (NTIA) 主導で、ソフトウェアコンポーネントの透明性向上への議論も進められている。ここでは、ソフトウェアの構成要素リストであるSBOM (Software Bill of Materials) の構造・共有方法・活用方法の標準化、ユースケース策定などが目的とされている。

日本の現状と課題

一方、日本に目を向けてみると、図表3に示した通り、サプライチェーン攻撃に対する認識が他国に比べて低い。IPA (独立行政法人情報処理推進機構) のアンケート調査によると、ITシステム・サービスの調達側が、開発側 (委託先) が実施すべき具体的な情報セキュリティ対策を仕様書などで明記できているのは30%程度でしかない。また、IPAの別の調査によると、開発段階でセキュリティを考慮している企業は68%程度であり、そのうち製品出荷前にテストを行っているのは57% (全体に対しては39%) にとどまっている (図表4参照)。開発側で十分なセキュリティ検査が行えていないため、調達側で製品受け入れ時に検査を実施する必要があるが、実際には調達側でもできていない状況にある。防衛省の備品や自動車のようなセキュリティが重要なものですらできていないといわれている。不正なプログラムが組み込まれてしまった場合でも、調達時にはチェックができておらず、運用中に偶然に発見されているのが現状である。

各企業でサプライチェーンセキュリティへの取り組みが進んでいない理由として、日本の制度作りが遅く、取り組み意義や実施すべき内容が不明確であることが一因と考えられる。最近になって制度作りへの取り組みが進められるようにはなっ

図表4
開発段階の脆弱性考慮・対策状況



出所：IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」（2018年3月）。小数点以下は四捨五入

たが、他国の後を追うような状況となっている。日本ではサプライチェーンリスクに関するフレームワークがなかったため、米国から日本政府に、サプライチェーンリスクに対応するよう働きかけられていた。2017～2018年度にかけて、経済産業省主体のワーキンググループにより、サイバーセキュリティに関するフレームワークの検討が進められた。本フレームワークにより米国のCybersecurity FrameworkやNIST SP800-171などへの対応がとられることとなったが、米国での規制内容・範囲が変更されれば、それに準じて日本でも再び対応を迫られることになると考えられる。議論が遅れたことから対応が後手に回り、日本企業も今後のビジネス環境を見通しづらい状況となっている。

今後の議論の展望とビジネスの可能性

これまで見てきた通り、他国（特に米国）ではサプライチェーンセキュリティに関する制度化・ルール化が進められており、ソフトウェアコンポーネントの透明性向上に向けた新たな議論も進められている。このような中、今後日本での議論が遅れると、再び他国で決められた枠組みへの対応を迫られることになりかねない。その場合、日本企業には不都合な枠組みにより既存のビジネス環境が悪化、あるいは最悪の場合グローバルサプライチェーンからはじき出されてしまうことも考えられる。他国から取り残されないために、さらにはグローバルのビジネスを先導していくために、今後必要となる議論を日本主導でも進めていくべきではないだろうか。

そして、今後必要となる議論として、サプライチェーンの透明

性向上があると考えられる。昨今ではサプライチェーンが複雑化しており、ソフトウェアにどのようなパッケージやコードが含まれているのか、誰が開発に関わったのかが分かりづらい状況であることが、サプライチェーン攻撃が発生する下地となっており、この不透明性の解消が必要と考えられる。

サプライチェーンの透明性向上のためには、製品自体の情報（ソースコード情報、コンポーネント情報など）、開発者の情報（誰がいつ、どの部分の開発に関わったのかなど）について、サプライチェーン関係者間で共有したり、第三者認証機関を設置して認証を取得する仕組みを作ったりするなどの方向性が考えられる。製品自体の情報が開示されることで調達側（もしくは第三者認証機関）でもセキュリティの検査ができるようになり、さらに開発者の情報が開示されることで、問題が生じた際に原因を追究することが可能となる。また、このような透明性の向上は、不正プログラム混入に対する抑止力にもなりうると考えられる。

このような議論が進んだ場合、新たなビジネスとして、製品情報や開発者情報の開示に用いる共通プラットフォームの提供や、第三者認証機関としてのサービス提供などが考えられる。当初からルール作りの議論に関わることで、このようなビジネスチャンスの取り込みが可能になるだろう。参入できればソフトウェアに関するデータが大量に集まるようになり、独占的なポジションが確立され、新たなデータビジネスへの道も開かれるのではないだろうか。一企業による独占は難しいかもしれないが、複数企業により運営企業を共同設立するという方向性も考えられる。

また、プラットフォームにソースコード情報やコンポーネント情報が集まるようになれば、今までは個別に行われていたソースコード検査や、コンポーネントのバージョンチェックなどが、プラットフォーム上で実施できるようになるかもしれない。その場合、個別に提供されていたサービスがプラットフォーム上に統合されていき、これらのサービスもプラットフォームと相まって強固なポジションを築くことになると想定される。ここでの統合に乗り遅れた場合、市場でのポジションを失うことになりかねない。第三者認証機関を設置した場合でも、同様な事象が生じると考えられる。

プラットフォームビジネスの獲得、あるいはプラットフォームに統合するサービスの提供、いずれにしてもサプライチェーン透明性向上の議論に当初から関わり、ビジネス獲得に有利なポジションを築いていくことが今後重要となるのではないだろうか。

サイバーセキュリティが定義する自動車の将来

著者：赤路 陽太

法規制により照らされる道

ここ数年、IoTやAIなどのエマージングテクノロジーに導かれ、自動車産業およびその周辺産業においては、コネクテッドサービス、自動運転、モビリティサービス、EVなどに関する議論が数多く行われてきた。

自動車メーカーにおいてはもちろんのこと、自動車部品メーカーや周辺産業のプレイヤーにおいても多くのプロジェクトが立ち上がり、巨額の予算と工数が費やされてきた。

世界中の企業においてスマートデバイス経由で利用するモビリティサービスが検討され、シェアリングサービスやロボットタクシーが新車販売台数とタクシードライバーの雇用を奪うというシナリオが描かれている。

PoC（Proof of Concept）と呼ばれる実証実験も多数行われ、その結果報告書が山のように積み上げられている。

市場はまだ立ち上がってもいないにもかかわらず既にレッドオーシャンの様相を呈しており、なかなか見えない「宝探し」に企画・開発担当者が焦り、疲弊し始めている状況もある。

いつの時代においてもエマージングテクノロジーは企業に不安と期待を与え、混乱と進化をもたらしてきた。

自動車産業は今まさにその状況にある。

しかし最近、そうした状況に変化が起こりつつある。変化をもたらしているのは自動運転などに関する国際機関や国による法やガイドラインの整備の進展である。

国際機関や国が定める法やガイドラインは、企画・開発担当者たちの道を照らす明かりとなり、「どこに行けば良いか」「どこまで行けば良いか」「何は許されて何は許されないのか」などの指針を与え始めている。

その結果、これまでのコンセプチュアルな議論に道しるべが立ち、より現実的で具体的な議論が始まりつつある。

サイバーセキュリティも、そうした明かりが灯されたテーマの一つである。そしてその明かりは、今後の自動車の在り方を示唆するものとなっている。

データより大切なもの

海外におけるセキュリティイベントなどで実車へのハッキングが可能と証明されたことは記憶に新しい。大規模リコールに発展した事例もある。だが、自動車産業各社はそれらがきっかけで動き出したわけではない。各社はかなり以前からサイバーセキュリティの必要性を認識しており、その取り組みは既に長期にわたっている。自動車メーカー複数社が参画するサイバーセキュリティプロジェクトの発足や、自動車部品メーカーによるサイバーセキュリティソリューションベンダー買収などが示すように、各社は少なくとも2000年代から取り組みを開始し、国際基準・国際標準がない中で仕様を模索し続けてきた。

そうした長期にわたる研究・開発の結果、自動車のサイバーセキュリティについては、開発段階から生産・販売・使用・再販・廃棄に至るまで、そしてコンセプトからオフィス、工場、生産ライン、ディーラー、クラウド、通信、車両、通信ユニット、車載ネットワーク、ECU、ソフトウェアに至るまでをさまざまなソリューションで包括的かつ多層的に防御する必要があると認識されている。

Strategy&ではこれを「Holistic Multilayer Security」と呼称し、図表1に簡略イメージを提示する。

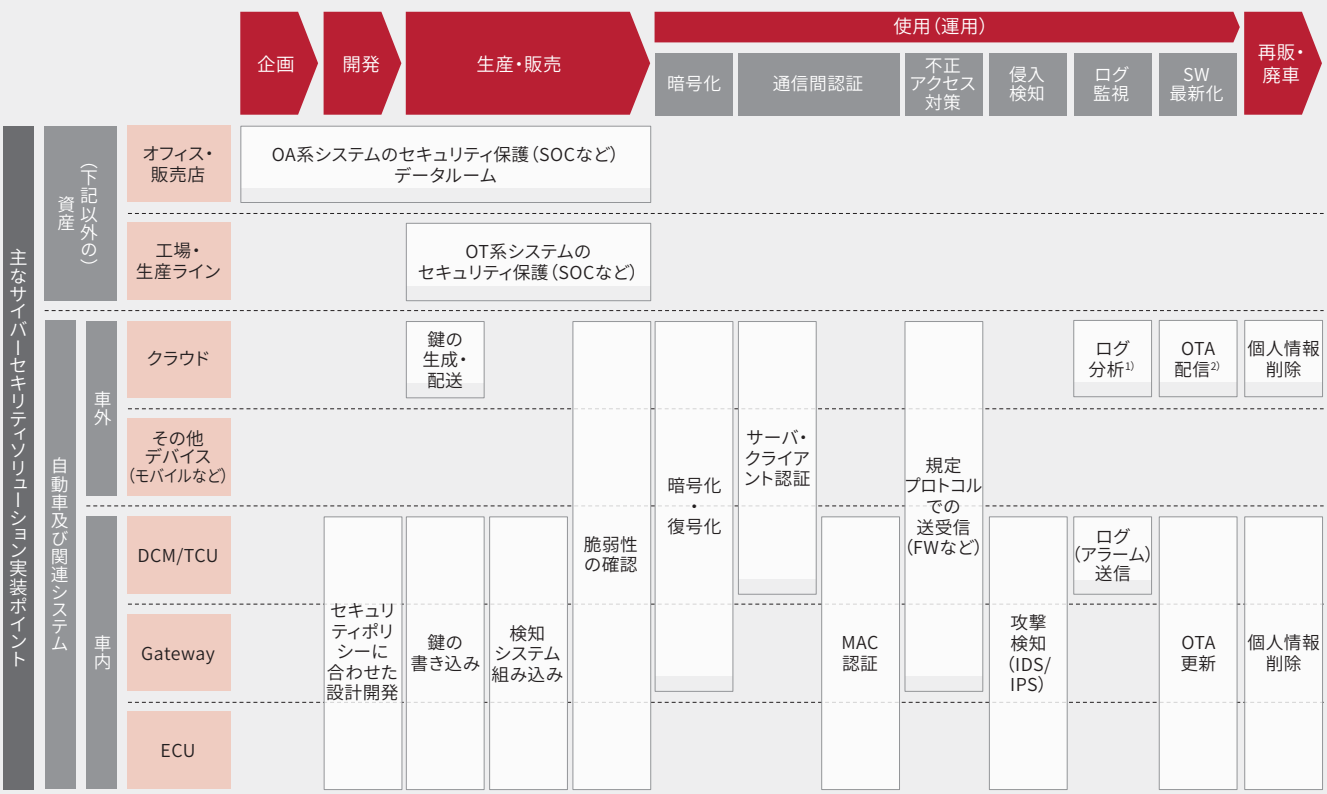
これほど多岐にわたるソリューションが必要と認識されるのは、自動車におけるサイバーセキュリティリスクが、「車両盗難」「個人情報漏洩」「技術情報漏洩」「漏洩情報悪用による二次被害」「それらがもたらす風評被害や損害賠償などの経営リ

赤路 陽太（あかじ・ようた）
yota.akaji@pwc.com

PwCコンサルティング、Strategy&のシニアマネージャー。自動車産業および情報サービス産業を中心に、イノベーション、新事業開発、成長戦略、事業変革、マーケティングなどのテーマについて豊富なコンサルティング実績を有し、次世代のモビリティに関するコンサルティングを多く手掛けている。

なお、本稿の執筆にあたっては、Strategy&のシニアアソシエイトの米本 和希、アソシエイトの長山 東哲の協力を得た。

図表1
Holistic Multilayer Security（簡略イメージ）



1）ログ分析はクラウド（SOC）上で監視しているホワイトハッカーにより実施される
2）OTA配信は、通常更新の他、SOC上での分析結果や脆弱性情報収集の結果行われる

出所：Strategy&分析

スク」はもちろんのこと、「自動車を踏み台にした企業サーバー攻撃」、そして「事故による人命毀損」「周囲の巻き込みによる甚大被害」にまで及びうるからである。

一昔前に「クルマのスマホ化」という言葉が多用された時期があったが、サイバーセキュリティの観点では、残念ながら自動車とスマートフォンが置かれている状況は大いに異なる。

スマートフォンの場合、ハッキングされたアプリケーションが使用者本人や他人に被害をもたらすことはあっても、スマートフォン自体が使用者本人や他人の生命を奪うことはほぼない（バッテリーを熱暴走させるなどはあるかもしれないが）。

一方、自動車の場合、特に制御系のECUがハッキングされると、使用者本人に加え、歩行者ら、他人の生命まで奪ってしまうリスクがある。さらにそれが保険会社も対応しきれない規模の損害になるリスクがある。そのため万が一のリスクも発生しないよう、徹底的なソリューションが必要と考えられている。

ガイドラインが示唆する未来

ところが、これほどまでに時間をかけて検討されてきたにもかかわらず、これまでのところこれらの内容はあくまでも自動車産業各社の研究の域を脱していなかった。

準拠すべきルールが存在していなかったため、結局どこまで実装しなくてはならないのか個社では判断がつかず、研究のみが延々と続けられる状況に陥っていたのである。

しかし、ここ1～2年で国際機関や国によるガイドラインなどの整備が進展し、状況が変わり始めている。

レギュレーションの整備にはもうしばらく時間を要する見込みであるが、これまで先行するICT産業の規格などを参考にしながら個別に検討を進めてきた自動車産業各社にとっては十分なよりどころが整備されつつあり、いよいよ実装に向けての判断が可能な状況が整い始めている。

同時にこれらのガイドラインなどは「今後の自動車の姿」も示している。

図表2にそうしたガイドラインなどから主なものを抜粋して例示する。これらのガイドラインなどにおけるポイントは以下の2点である。

①通信が絡む自動運転技術を搭載する車両は、徹底的なサイバーセキュリティソリューションの実装が必須になる

②サイバー攻撃は防ぎきれないことが前提となる

ポイント①は、言うまでもないことであるが、これまで曖昧で個社に対応が委ねられていたものがルール化されることにより、「必要なサイバーセキュリティソリューションを実装していなければ通信が絡む自動運転技術搭載車両を販売できない」「サイバーセキュリティソリューションの実装によるコストアップに対する解決策を見いださなくてはならない」という新たな課題が自動車メーカーにもたらされることを意味している。

前述のHolistic Multilayer Securityを実装するためには、多額のシステム開発費、ソフトウェア開発費、部品費、組み込み加工費、運用費などが必要になる。これらは従来なかった新規のコストになるため、自動車メーカーとしては回収方法を考える必要がある。単純に車両販価に上乗せしたり所有者にサブスクリプション型で請求したりすると、所有者は当然のことながら嫌がるだろう。「自動運転なんてなくて良いから安くしてほしい」と言う消費者も現れることが想定される。無理に強制しようものなら、買い替えを見送る所有者や、そもそも所有を諦める消費者が現れ、新車販売台数を押し下げるリスクが想定される。

ポイント②は、WP.29/2017/46 Guideline on cybersecurity and data protectionにおける「サイバー攻撃による不正な操作を自動運転システムが検知した時は、ドライバーに警告の上、自動車を安全にコントロールすること」という要件や、Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVAにおける「自動車での攻撃が検知された際は、システムは適切にインシデントレスポンスが行われるように設計すべき」という要件がそれに相当する。

これらの要件の存在は、「工場出荷時に実装された暗号化や相互認証などのサイバーセキュリティソリューションでは防ぎきれないサイバー攻撃の存在」を示唆している。

パソコンやスマートフォンにおいてセキュリティソフトの更新が必要であるように、自動車においてもサイバー攻撃は日々進化している。それらのサイバー攻撃はいつしか工場出荷時に実装されたサイバーセキュリティソリューションでは防げないレベルに進化し、車載ネットワークに侵入し、ドライバーの意志とは異なる挙動を引き起こすことで重大事故を生むリスクがある。

さらに最近はハッキングAIも台頭し始めており、多層防御の脆弱性を機械学習により自動的に見いだし、脆弱性が解消される前にゼロデイ攻撃を仕掛けてくるリスクがある。

そのようなリスクを回避するためには、まずもって自動車のセキュリティソフトを常に最新版にアップデートし続ける必要があり、方法としてはOTA（無線通信）によるセキュリティソフト

図表2
主なガイドラインなどの例

ガイドラインなど	概要（一部抜粋）
WP.29/2017/46 Guideline on cybersecurity and data protection (UN)	❖ **コネクテッド車両および自動運転車両は以下の要件を満たすこと** ★ コネクテッド車両または自動運転技術（ADT）装備車両が適用範囲。コネクテッド車両とは、外部の装置、車、ネットワークまたはサービスとの間で自動運転テクノロジーに関係する可能性がある無線接続または通信を行えるように設計された装置が搭載されている車両を指す ★ 一般要件 • 自動車製造者らは、コネクテッド車両および自動運転車両において、データの操作、誤用などに対して適切な保護を確実にすること • 自動車製造者らは、コネクテッド車両および自動運転車両において、世界標準の通信技術などによるデータおよび通信の暗号化を実施すること ★ データ保護にかかる要件 • コネクテッド車両および自動運転車両におけるデータの収集および処理を行う際は、以下を満たすこと - データ主体（例、運転手）に、どのようなデータが収集・処理されているのかなど、包括的な情報を提供すること - これらの説明を受けたデータ主体による、データの収集および処理に対する同意を得ること • 個人情報については、自動運転に関わる情報の収集および処理に関連するものに限定し、場合によって情報主体は同意を取り下げる権利を持つ ★ 安全性にかかる要件 • コネクテッド車両および自動運転車両は、接続および通信の安全確保のため、以下を満たすこと - 車外のネットワークから車内の制御系ネットワークが影響を受けないこと - 無線インターフェイス、故障診断ポートを介した不正アクセスを回避するよう設計されていること - システムの機能不全時の「セーフモード」を備えること • サイバー攻撃による不正な操作を自動運転システムが検知した時は、ドライバーに警告の上、自動車を安全にコントロールすること ★ セキュリティにかかる要件 • コネクテッド車両および自動運転車両は以下のものが装備されていること - 完全性保護措置（例として、セキュアなソフトウェアアップデート） - 暗号鍵を管理するための適切な措置 • コネクテッド車両および自動運転車両へのリモートアクセスに関わるオンラインサービスについては、強力な相互認証を有すること
Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA （UN、次ページに続く）	❖ **車両へのサイバー攻撃に対するリスクを軽減するために、考慮されるべきサイバーセキュリティ対策を示す。必須事項は「しなければならない（Shall）」、推奨事項は「すべき（Should）」とした** 1. インサイダー攻撃（内部者による攻撃）のリスクを最小限にするため、セキュリティコントロールをバックエンドシステムにも適用しなければならない 2. 不正アクセスを最小限にするため、セキュリティコントロールをバックエンドシステムにも適用しなければならない 3. バックエンドサーバーがサービスの提供に不可欠な場合、システム停止に備えて回復措置を設けなければならない 4. クラウドコンピューティングに関連するリスクを最小限に抑えるため、セキュリティコントロールを適用しなければならない 5. 情報漏洩を防止するため、セキュリティコントロールをバックエンドシステムにも適用しなければならない 6. 車両への攻撃の影響を最小限に抑えるため、設計によるセキュリティ（Security by Design）の原則を採用しなければならない 7. システムデータ/コードを保護するため、アクセス制御技術および設計を適用しなければならない 8. 不正な担当者が重要なデータにアクセス可能なシステム設計およびアクセス制御にすべきではない 9. 不正アクセスを防止し、検出するための措置が採用されなければならない 10. 車両は、受信したメッセージの信頼性と整合性を検証しなければならない 11. 暗号鍵を格納するためのセキュリティコントロールが実装されなければならない

ガイドラインなど	概要（一部抜粋）
Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA (UN)	12. 自動車に対し機密データが送受信される場合は保護しなければならない 13. DoS攻撃に対する検知・回復するための措置を検討すべき 14. 組み込まれたウイルス・マルウェアからシステムを保護するための措置を検討すべき 15. 悪意のある内部メッセージまたは活動を検知するための措置を検討すべき 16. セキュアなソフトウェアアップデート手順を採用しなければならない 17. 保守手順を統制するための手段を講じなければならない 18. ユーザーロールとアクセス権限は、必要最小限な形で統制するための手段を講じなければならない 19. セキュリティ手順が実行されるような組織を定義し、維持しなければならない 20. リモートアクセスを持つシステムに対し、セキュリティコントロールを適用しなければならない 21. ソフトウェアはセキュリティ観点で評価・認証され、完全性を保護しなければならない 22. セキュリティコントロールは、外部インターフェイスに対しても適用しなければならない 23. ソフトウェアとハードウェア開発におけるサイバーセキュリティのベストプラクティスを守らなければならない 24. 個人情報・機密情報を格納する際はデータ保護のベストプラクティスを守らなければならない 25. 自動車での攻撃が検知された際は、システムは適切にインシデントレスポンスが行われるように設計すべき
自動運転車の安全技術ガイドライン（国土交通省）	❖ サイバーセキュリティの要件 ★ 自動車製作者などまたは自動運転車を用いた移動サービスのシステム提供者は、サイバーセキュリティに関する国連（WP29）などの最新の要件を踏まえ、自動運転車のハッキング対策などのサイバーセキュリティを考慮した車両の設計・開発を行うこと ★ 2017年3月にWP29で成立したサイバーセキュリティガイドラインなどで示されている要件（抜粋） • 自動運転車の接続および通信の安全確保 - 車外のネットワークから車内の制御系ネットワークが影響を受けないこと - システムの機能不全時の「セーフモード」を備えること • 不正操作を検知した時は、運転者に警告の上、車両を安全にコントロールすること ❖ 自動運転システムの安全性要件 ★ レベル3の自動運転車については、次の要件を満たす自動運転システムであること • 設定されたODD（運行設計領域）の範囲外となった場合や自動運転車に障害が発生した場合など、自動運転の継続が困難であるとシステムが判断した場合において、運転者に対し介入のための警告（運転権限の委譲）を行うこと • 運転者に運転権限が委譲されるまでの間、システムの機能を維持またはシステムの機能を制限した状態でシステムの稼働を継続させるフォールバック（縮退運転）を行うことにより、安全に自動運転を継続すること • システムから運転者に運転が引き継がれたか否かを判別することができること • システムから運転者に運転が引き継がれない場合において、車両を自動で安全に停止させるミニマル・リスク・マヌーバー（MRM）を設定すること - 車両を路肩などの安全な場所に自動で移動して停止させることが望ましい - 自動運転車の MRM の設定は、周囲への警報を行いつつ、車線を維持、または車線を変更しながら自動で安全に停止させる措置が想定されるが、今後の技術開発の動向および国際的な基準の検討状況を踏まえ具体的要件を検討する

出所：Strategy&分析

のアップデートが考えられる。しかしOTAの実行は基本的に所有者の許可が必要になるため、所有者が許可しなければ永遠に古いセキュリティソフトのままになってしまう。

そのため自動車メーカーは車載ネットワーク上のイベントを常時監視し、それらを分析することによってインシデントと考えられる兆候を検知し、阻止する必要もある。また、車載検知システムでは検知しきれない新たな攻撃を特定すべく、車載ネットワークのログを車外のSOC（Security Operation Center）に送信し、SOCが保有するSIEM（Security Information and Event Management）と呼ばれるログの集約・蓄積・管理・分析を行う仕組みによる相関分析およびセキュリティ専門家による詳細分析にかけることでインシデントを特定し、阻止する必要もある。しかし車載検知ソフトウェアは100%正確に検知を行うことができない。検知精度を高くし過ぎると問題の無いイベントまでインシデントと誤検知してしまい運転に支障が出てしまうため、検知精度に幅を持たせてあるからだ。そうした状況でもインシデントの見逃しがないようにSOCでのバックアップがあるわけだが、残念ながらSOCでの相関分析およびセキュリティ専門家による詳細分析には時間を要するという問題がある。サイバー攻撃の方が早かった場合、このソリューションは効果を発揮することができない。

つまり、「防ぎきれないサイバー攻撃が存在しうる」ということである。

「セキュリティソフトのアップデートをしないのは所有者の責任ではないか」という意見もあるだろうが、そこの責任分担はこれから議論されるところであろう。少なくとも現時点においては自動車メーカーが安全な自動車をつくることが求められているし、そもそもハッキングAIにとってはセキュリティソフトのバージョンは関係ない可能性もある。

こうした状況が想定されてか、ガイドラインなどにおいては、通信が絡む自動運転技術搭載車両について「サイバー攻撃による不正な操作を自動運転システムが検知した時は、ドライバーに警告の上、自動車を安全にコントロールすること」と要件が定義されている。

もしサイバーセキュリティ技術の進化や徹底的な機能・装置追加により上述のソリューションが有効になったとしても、実装するためには相当な仕組みとコストが必要になる。

まず、検知する仕組みを車両に組み込まなければならない。これは従来なかった仕組みのため、検知ソフトウェアやデバイスの開発費、それらの組み込み加工費などが必要になる。

検知したログをSOCに送信するための通信費も必要になる。車両の自動化が進み高度ADAS（先進運転支援システム）や自動運転が搭載されると、車載ネットワークを流れるデータ量は膨大になる。某半導体企業は1台の車両で1日あたり数テラのデータが生成されると予測しているが、それらに基づくログをSOCに送信するとなると、かなりの通信費が必要になるであろう。

通信費を抑制するためにログの送信頻度や送信量を抑制するというアイデアもあるが、そうするとリアルタイムでのインシデント特定ができなくなってしまうため、本末転倒になってしまう（通信量についてはそもそも自動運転技術やストリーミング配信などの方が大きくなるからサイバーセキュリティだけ抑制しても意味がないという意見もあるであろうが、それはいったん置いておこう）。

ログ送信先のSOCも従来なかった仕組みのため、新たなコストが発生する。SIEMの開発費や、セキュリティ専門家の人件費などを含む運用費が必要になる。

インシデントを特定した場合は、所有者に通知するとともにセキュリティパッチを生成し、配信する必要がある。これにも費用が発生する。

ただしこれでも完璧ではなく、セキュリティパッチの生成に時間を要することを想定すると、攻撃を検知した瞬間に車外および車内の通信を遮断し、なんらかのバックアップシステムにより強制的に安全に路肩に停車させるなどの機能安全の仕組みも搭載している必要がある。

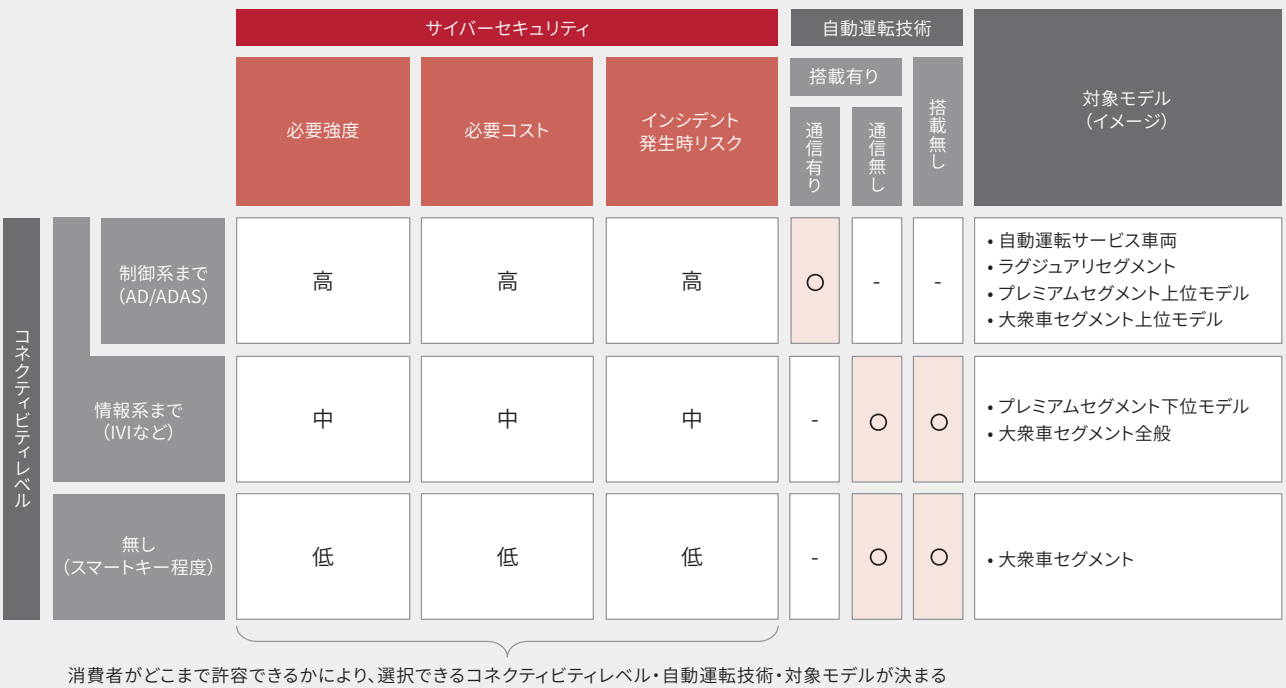
そして最終的にはこれらを自社の車両が走行する世界中の国で対応可能にする必要がある。

1台あたりに換算すると、通信費・運用費・部材費がかさみ、前述のHolistic Multilayer Securityの実装費用も含め、かなりのコストアップになることが容易に想定される。

提示されているガイドラインは、そうした未来の到来を示唆している。

図表3

サイバーセキュリティにより規定されるコネクティビティレベル・自動運転技術搭載動向・対象モデルイメージ



出所：Strategy&分析

サイバーセキュリティにより規定される車両

こうした状況を踏まえると、「これ以上、車にお金を払えない」「せっかく高いお金を払ってもリスクがあるなら、通信が絡む自動運転技術は要らない」という消費者が現れてもおかしくないだろう。

もし「セキュリティソフトのアップデート忘れによるハッキングに起因する事故は所有者責任」ということになれば、そういう消費者がますます増える可能性もある。

つまり、サイバーセキュリティが消費者の費用対効果判断の軸となり、許容できる「サイバーセキュリティコスト」や「インシデント発生時のリスク」により、選択できるコネクティビティレベルおよび自動運転技術が決まる（コスト要因により対象モデルも決まる）ようになる可能性がある。

その結果、昨今のCASE（Connected, Autonomous, Shared, Electric）ブームにより世の中の全車両がすべからく完全自動運転になるかのような見方がある中で、実際はサイバーセキュリティ起点で複数の車両バリエーションが求められる可能性が想定される。

自動車産業各社および関連産業各社は、こうしたバリエーション展開の可能性を認識し、準備を進めておく必要があるだろう。

おわりに

自動車のサイバーセキュリティもエマージングテクノロジーの一つである。よって今後も進化する可能性があり、現時点で全てを結論づけるのは難しい。もしかするとHolistic Multilayer Securityをより多層化することでハッキングを完全に防御できる状態を作り出せるかもしれないし、ゼロデイ攻撃に対するソリューションが開発されるかもしれない。

一方、「万が一のリスクがありえる」状態で販売する自動車メーカーが出てくる可能性がないとも言い切れない。しかしながら自動車は人の命がかかわる製品であることを忘れてはならず、サイバーセキュリティの特性、想定されるリスク、自動車産業が社会で果たさなくてはならない責任、消費者の安全・安心・予算などを総合的に考えれば、安易に予想された未来の実現難度がいかに高いか、遅かれ早かれ気付くであろう。

通信が絡む自動運転技術の開発が進む今、サイバーセキュリティがキーテクノロジーの一つになり、自動車開発において重要な役割を担っていくのは間違いない。

今後サイバーセキュリティは、パワートレイン構成を左右する燃費・排ガス規制のような位置づけになる可能性がある。

よって自動車産業各社および関連産業各社は早急に「サイバーセキュリティが定義する自動車の将来」を勘案し、開発予算・工数の適切な差配と競争力のある商品・サービスポートフォリオを実現していくべきであり、それが「全ての人の自由な移動」を実現することにもつながっていくであろう。

MEDIA HIGHLIGHTS

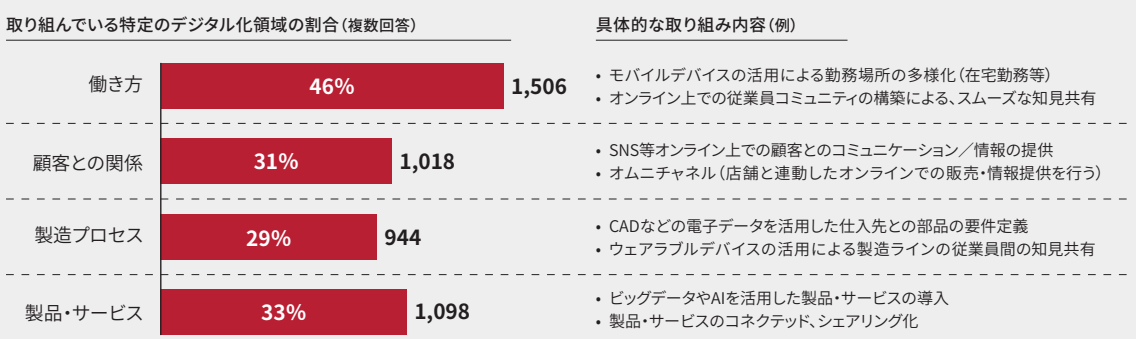
最新レポートのご案内

2018年Chief Digital Officer調査結果を発表

Strategy&は2019年4月、「日本企業のデジタル化の成功に向けて：2018年Chief Digital Officer（チーフ・デジタル・オフィサー：最高デジタル責任者、以下CDO）調査」を発行しました。

今回の調査で約5割の回答者は、自社が働き方改革のためにデジタル化[1]の推進に取り組んでいると回答しました。日本企業におけるデジタル化の取り組みを「働き方」「顧客との関係」「製造プロセス」「製品・サービス」の4領域の変革活動に分類し、取り組んでいる特定のデジタル化領域について複数回答で調査したところ、約5割と最も多くの回答割合となったのが「働き方」でした。

デジタル化の取り組み領域



出所：Strategy& CDO調査（日本）2018年6月

◆『日本企業のデジタル化の成功に向けて：2018年CDO調査』 https://www.strategyand.pwc.com/jp/home/publications/report

グローバルの調査結果[2]は、以下をご覧ください。

◆『The 2019 Chief Digital Officer Study Global Findings』 https://www.strategyand.pwc.com/cdo

1：デジタルによる事業環境や消費者・顧客のマインド、行動の変化に企業が対応するための変革活動
2：ブルームバーグのデータに基づく2018年3月31日現在で全世界の時価総額トップ2,500社のCDOの有無、バックグラウンドなどの分析

Strategy&について

Strategy&は、他にはないポジションから、クライアントにとって最適な将来を実現するための支援を行う、グローバルな戦略コンサルティングチームです。そのポジションは他社にはない差別化の上に成り立っており、支援内容はクライアントのニーズに応じたテイラーメイドなものです。PwCの一員として、私たちは日々、成長の中核である、勝つための仕組みを提供しています。圧倒的な先見力と、具体性の高いノウハウ、テクノロジー、そしてグローバルな規模を融合させ、クライアントが、これまで以上に変革力に富み、即座に実行に移せる戦略を策定できるよう支援しています。

経営課題に関するご相談はこちらまで

info.japan@strategyand.jp.pwc.com

問い合わせ先
PwCコンサルティング合同会社 ストラテジーコンサルティング（Strategy&）
〒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 21 階
電話：03-6250-1209 Fax：03-6250-1201
http://www.strategyand.pwc.com/jp

strategy&

Part of the PwC Network

www.strategyand.pwc.com/jp/