www.pwc.com/jp

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

デジタル時代における脅威の管理および競争優位性を得るための革新的なセキュリティ対策の導入

グローバル情報セキュリティ調査 2017

The Global State of Information Security® Survey 2017

pwc

目次

今日、経営幹部らは、サイバーセキュリティやプライバシーへの革新的なアプローチを求めている。恐怖、不安、疑念を蒸し返すのではなく、それらを乗り越え、ビジネス、サードパーティーパートナー、カスタマーを保護し実現する者として、サイバーセキュリティおよびプライバシーをより広い視野で捉えようとしているのだ。

これは明らかな変化だ。多くの企業はもはやサイバーセキュリティを、変化を阻む障壁やITコストと考えるのではなく、ビジネスの成長の促進、市場における優位性の獲得、ブランドに対する信頼の構築につながることだと理解している。

この考え方の変化を引き起こした主な要因は、ビジネスのデジタル化だ。今日の企業は製品を作るだけではない。製品に対するソフトウエアを用いたサポートサービスも(時には無料で)提供し、顧客関係の強化と成長の機会を広げている。

59%

ビジネスエコシステムのデジタル化がセキュリティ支出にインパクトを与えたと答えた回答者の割合

PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

ありとあらゆる製品やサービスがインターネットに接続されるようになり、サイバーセキュリティやプライバシーに関するリスクへの積極的な対応がますます必要になった。これは、変化を促す要因であるだけではない。データプライバシーや信頼は、生成・共有される消費者情報やビジネス情報が飛躍的に増えるにつれて、ビジネスの必須要件にもなっているのだ。

この変化を受けて、先進的な企業は新しいサイバーセキュリティモデルへと進路を変えた。目指すのは、分析に基づいた機敏な行動が可能で、リスクや脅威の進化に適応できるサイバーセキュリティモデルである。この新しいアプローチの中核となるものは、データアナリティクスやリアルタイム監視、マネージドセキュリティサービス、高度認証、オープンソースソフトウエアのようなソリューションだ。

全てが新しいテクノロジーというわけではないにしても、提供や管理の方法・頻度はこれまでにないものだ。多くはクラウドベースやマネージドセキュリティサービスといった形態をとっている。オープンソースソフトウエアの採用などは、オンプレミスシステムの開発・稼働方法にも大きな変化をもたらす。

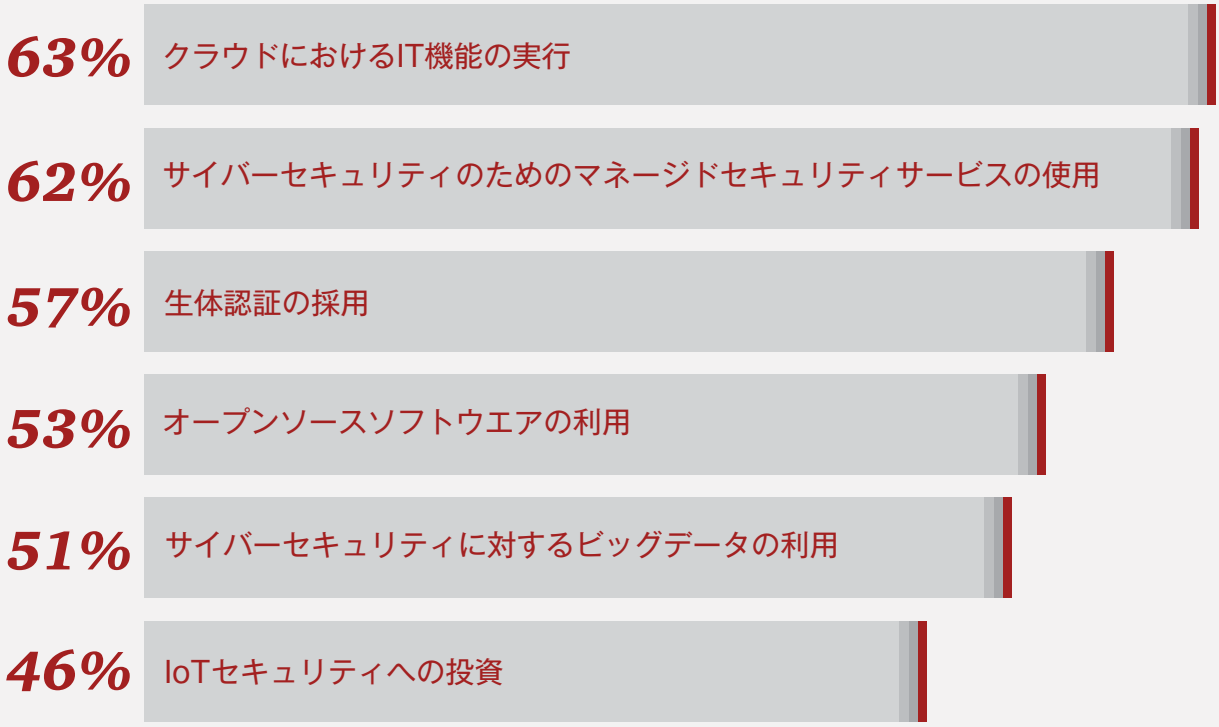
これらを一つにするものがあるとしたら、それはクラウドだ。クラウドベースのプラットフォームの能力と相互運用性を活用すれば、相乗効果のあるテクノロジーをつなぎ合わせることができる。さらに、クラウドアーキテクチャー本来のシンプルさは、セキュアな新製品や新サービスの構築に活用できる。このアーキテクチャーの利点は、サイバーセキュリティとプライバシーにおけるツールの統合と改善が大きく前進する可能性を示している。

インタラクティブタイムラインをご覧ください。
http://pwc.com/gsiss
***Connecting the dots：A* timeline of technologies, threads and regulations that redefined cybersecurity and privacy**

*「企業がイノベーティブに、速やかに活動するための方策として、サイバーセキュリティの重要性が増している」*とPwC米国およびグローバルリーダー、Cybersecurity and Privacy、David Burgは述べている。*「あるデジタルイノベーションでは、新しい製品やサービスの設計と開発に、負担のない認証手段とともに、セキュリティの検討、管理策、機能が不可欠となる」*

また、クラウドで統合されたソリューションにより、データプライバシー機能を強化し、顧客からの信頼とブランドの評判を高めることもできる。消費者が自分の機密データの収集・共有に敏感になり、政府が国境を越えた情報の利用について監視を強化する中、このような保護策はなくてはならないものだ。

脅威への対応と価値創出を目的としたテクノロジーの利用



出典:PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

テクノロジーがサイバーセキュリティやプライバシーのモデルを変えていく中で、一つの不変の真理がある。効果的なプログラムにはセキュリティの基本要素を備えていることが必須条件であるということだ。

サイバーセキュリティへの投資を行い、高度なテクノロジーを活用することによって、攻撃を抑制したり影響を低減したりすることは可能だ。しかし、攻撃者の動機やテクノロジーが進化して新たな手段・手法が生まれ、これからも先回りされる状況は変わらないだろう。

従業員トレーニング、ポリシーと管理策の更新、徹底的な準備とレジリエンスの確保といったサイバーセキュリティの基本を守る企業は、単純な攻撃に対処し、複雑なインシデントに備えてリソースを確保できる可能性が高い。

今回の調査の結果、四つの重要トレンドが浮かび上がった。デジタルビジネスによるサイバーセキュリティの新しいテクノロジーやアプローチの採用、ビジネスにおけるスレットインテリジェンスと情報共有の重要性、IoT（モノのインターネット）に伴うリスクへの対応、地政学的脅威の高まりだ。

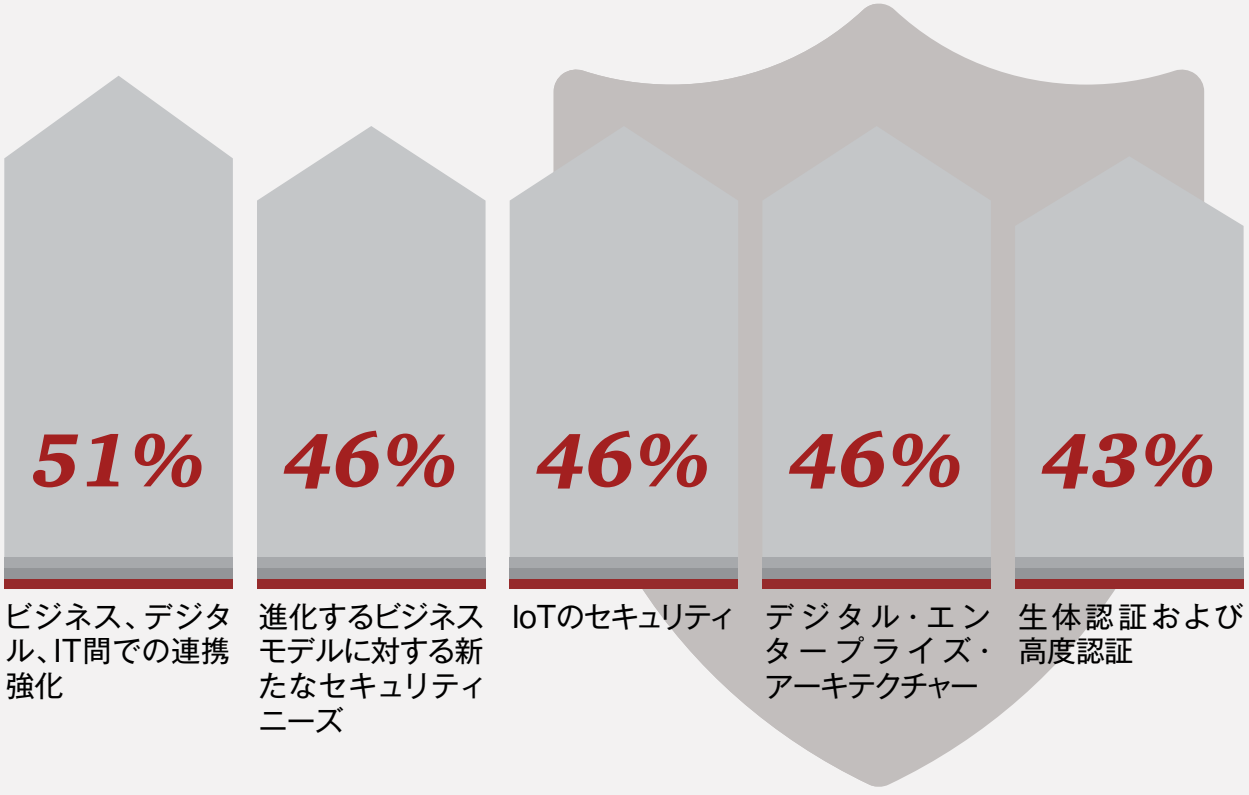
本年の調査結果については、今後数カ月に4回に分けてリリースする。最初のリリースとなる本書では、デジタル企業が、成功に向けて、また真の差別化要因となるよう、サイバーセキュリティおよびプライバシープログラムに、どのようにして新しいテクノロジー対策を活用しているかを探る。

サイバーセキュリティとプライバシーを広い視野で捉える

今日、ほとんどのビジネスは基本的にデジタル化されており、ソフトウエアが運用、製品、サービスの根幹となりつつある。サイバーセキュリティおよびプライバシーとデジタルビジネス戦略を統合することにより、価値や競争優位性を創出する新たな機会を求める動きに拍車がかかっている。

自動車業界を例にとって考えてみよう。かつて自動車の購入で重視された要素は、性能やデザイン、機能、価格だった。現在はこれらに代わって、接続性、車内デジタルコンテンツおよびサービス、自動運転機能に注目が集まっている。ビジネス範囲を拡大する自動車メーカー、通信事業者、ソフトウエアベンダー、家庭用電化製品メーカーは、デジタル化された長期的なアフターサービスを提供している。

今後12カ月で優先されるサイバーセキュリティ支出



出典:PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

これは、製品やサービスはもはや「売って終わり」ではなくなったということを意味する。企業はプロダクトライフサイクルを通して、デジタルによる拡張サービスを提供している。この例がほとんどの業界に見られるようになり、ビジネスモデルにパラダイムシフトが起こっている。

また、デジタルサービス全体で品質と安全性がより重視されるようにもなっている。顧客は直感的で魅力あるデジタルパッケージであると同時に、機密データを保護することも期待している。その結果、非常にセキュアなデジタルエクスペリエンスが不可欠になった。

*「顧客の企業や製品に対する信頼を裏切らないよう、サービスを安全な方法で提供する必要がある」*とPwC米国 Co-leader、Cybersecurity & Privacyの Christopher O'Haraは語る。*「サイバーセキュリティは、企業が提供する製品とサービスの一部であるとともに、顧客の信頼を得るための基本要素となった」*

そのためには、サイバーセキュリティとデジタルを統合するための予算を最初から確保しておく必要がある。多くの企業がこの課題への対応を始めなければならない。今回の調査では、59%の回答者が自社のビジネスエコシステムのデジタル化がサイバーセキュリティ支出にインパクトを与えたと回答した。デジタルビジネスモデルとの統合が行われているテクノロジーには、暗号化、次世代ファイアウォール、ネットワークのセグメント化、IDおよびアクセス管理などがある。セキュリティ制御をよりデータに近づけることも考えるべきである。

費用対効果はあるのだろうか？*「サイバーセキュリティとデジタル戦略を統合している企業は、あらゆる活動において信頼を獲得しやすく、変革も速やかだ」*とPwC's Global Degital Services Leader、Tom Puthiyamadamは述べる。*「トップ企業はサイバーセキュリティ、プライバシー、デジタル戦略を最初から統合し進めている。この取り組みは、既存の顧客を離さず、新規顧客を引き寄せる。また、運用、ビジネスプロセス、IT投資の効率化にも作用する」*

クラウドによる高いシナジー

アプリケーションとデータはクラウドベースストレージに載せる方が、オンプレミスの社内システムよりも安全性が高いことはすでにはっきりしている。機密データや作業をクラウドプロバイダーに預ける企業が増えているのは当然だ。

実際に、財務、運用、カスタマーサービスなどのデータや作業をクラウドで実行している企業は多い。成熟したサイバーセキュリティプログラムを持つ大手金融サービス企業を含む、厳しい法規制に従わなければならないビジネスですら、機密データをクラウドプロバイダーに預けている。

63%

IT 運用にクラウドを利用していると答えた回答の割合

PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

*「会計、財務、運用、人事などの重要なビジネスプロセスや機能にクラウド利用を検討している企業は爆発的に増加している」*とPwCのBurgは指摘する。*「利点がますます明確になっており、クラウドを積極的に活用するトレンドは続くだろう」*

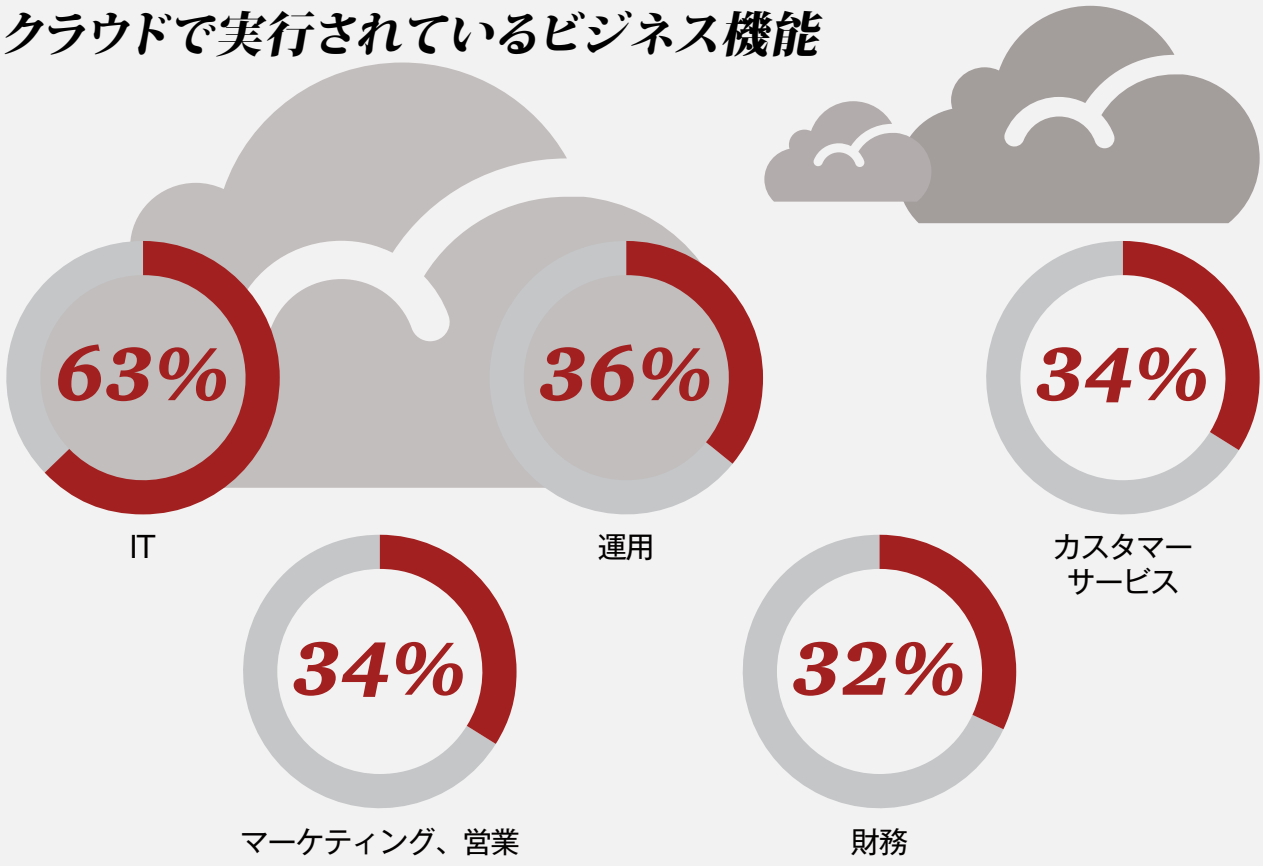
クラウド中心のサイバーセキュリティはリスクへの動的なアプローチであり、ビジネスエコシステム全体と内外の脅威をより深く理解できるようになる。クラウドベースのサイバーセキュリティを機械学習と人工知能で補い、ネットワークアクティビティー、脅威情報とログの統合分析を可能にする。このデータをリアルタイムで解析し、実用的なインテリジェンスを生み出すのだ。

最先端のクラウドプラットフォームは、ヒューリスティック機能も備えている。この計算能力と分析能力は、ネットワークやデータに対する攻撃に、リアルタイムで適応し、さらに能力を増強していく。つまり、クラウドプラットフォームはレジリエンスだけでなく、改良を続けていくのである。

クラウドベースのサイバーセキュリティでは、侵入者を阻止するだけではなく、正規の従業員、サードパーティーパートナー、顧客もモニターし、それぞれの行動から学習する。クラウドベースのサイバーセキュリティをマーケティングやカスタマーサービス、物流と統合すれば、ビジネスエコシステムにかかわる全ての人のアクティビティを追跡できる。顧客の行動を分析し、最終的にエクスペリエンスの向上につなげることも可能だ。

先進テクノロジーとクラウドアーキテクチャーの融合によって、企業は脅威を素早く識別して対応し、顧客やビジネスエコシステムについての理解を深め、最終的にはコストを削減することもできる。要するに、サイバーセキュリティが強みの源泉となり、真の差別化要因となるビジネスを生み出すことができるのだ。

クラウドで実行されているビジネス機能



出典:PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

外部からセキュリティを管理する

サイバーセキュリティおよびプライバシープログラムの設計と実装だけでも労力を要するが、それで終わりではない。プログラムの整備が終わると、各コンポーネントを完全に統合し、専門家によって管理され、継続的に改善を施していく必要がある。

限られたリソースしか持たない企業にとって、これは至難の業だ。多くの企業は、マネージドセキュリティサービスの導入によってこの課題に対応する。実際、今回の調査では、回答者の約3分の2（62％）がサイバーセキュリティプログラムの運用や強化にセキュリティ・サービス・プロバイダーを利用していると答えた。

主な要因は、スキルを備えたサイバーセキュリティスペシャリストの不足だ。Cybersecurity Venturesが最近実施した調査では、既存のサイバーセキュリティ人材と求人の差が2019年までに150万まで拡大すると予測されている[1]。人材不足が続けば、企業はますますサードパーティーにセキュリティプログラムを部分的または全面的に委託することになるだろう。

1　CSO、*Market expansion adds to cybersecurity talent shortage*、2016年7月13日

62%

サイバーセキュリティおよびプライバシーのためにマネージドセキュリティサービスを利用していると答えた回答者の割合

PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

*「テクノロジーの革新が急速に進んでおり、IoTやクラウドコンピューティングなどの新しいテクノロジーに対応する最新のスキルセットを確保していくことはますます困難になる」*と、PwCのGlobal Cybersecurity and Privacy Co-Leader、Grant Waterfallは述べている。*「マネージドセキュリティサービスを利用すれば、サービスプロバイダーからスキルセットを調達でき、自社の能力を補うために必要なニッチなスキルも手に入れることができる」*

もう一つの要因はコストだ。フルタイムのサイバーセキュリティおよびプライバシー専門チームを雇う余裕がない企業もがある。既存のソリューションの拡張が必要でも、比較的簡単な活動のために、高度なスキルを持つ社内スタッフを雇用したがらないケースもある。

マネージドセキュリティサービスの利用

出典: PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

要因が何であれ、企業は認証やデータ損失防止（DLP）、IDおよびアクセス管理、リアルタイムモニタリングなどのさまざまなテクノロジーによる保護策をマネージドセキュリティプロバイダーに外注するようになっている。

マネージドサービスは二つのカテゴリーに大別できる。一つはIDおよびアクセス管理、DLP、特権アクセス管理などの保護および予防のためのテクノロジー、もう一つは高度分析やスレットインテリジェンスなどの検知と対応のためのテクノロジーだ。

大手プロバイダーは二つのカテゴリーのサービスをまとめ、シームレスに提供している。最先端テクノロジーと高度な訓練を受けたスタッフを24時間365日のセキュリティ運用に採用し、新たな脅威を迅速に検知して対応する。また、投資を強化してサイバーセキュリティプロセスを継続的に改善できるように、テクノロジーや人材の管理も支援する。そうすればセキュリティチームは日々の雑務から解放され、脅威への対応やその他の戦略的活動に専念できる。

アナリティクスおよびスレットインテリジェンスを利用したリスク予測

内外の敵の目的や戦術が分からなければ、脅威の予測も検知もできない。

必要なのは、コンテキストに沿ってリスクを認識し、敵の戦術や手法、手順を理解するための高度分析とリアルタイムのスレットインテリジェンスだ。アナリティクスとスレットインテリジェンスをクラウドで同期させれば、シームレスな相関付けとリアルタイムの管理が可能な、企業規模の単一データソースを実現できる。

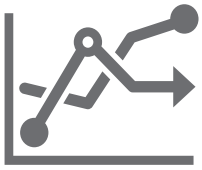
クラウドの計算能力とストレージ能力により、膨大な量のデータと非常に複雑な相互接続アプリケーションを監視し、不審なアクティビティを識別することが可能になる。クラウド中心のアナリティクスでは、ネットワーク全体にわたって全てのアクティビティーと、基準や脅威指標のグローバルリポジトリと比較し、継続的に評価できる。新しい脅威が見つかった場合は、データアセットへのビジネスインパクトに基づいて対応の優先順位を設定できる。

本年の調査では、回答者の半数以上（51％）がサイバーセキュリティ脅威のモデリングとインシデントの識別のためにビッグデータ分析を利用していると答えた。それでも、多くの企業にとってビッグデータは大きな挑戦だ。高度なアルゴリズムや分析アプリケーションの開発には、大量のストレージと処理能力だけではなく、経験豊富なデータサイエンティストが必要だ。前述のように、サイバーセキュリティ専門人材の不足と予算制約がビッグデータソリューションの実装を妨げている可能性がある。

51%

脅威のモデリングと識別のためにビッグデータ分析を利用していると答えた回答者の割合

PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日



このようなリソース不足も、クラウドベースのソリューションの採用が進む理由の一つだ。マネージドセキュリティサービスを利用している回答者の55％は、リアルタイムモニタリングおよび分析にサービスプロバイダーを利用していると答えている。大手マネージドサービスプロバイダーを利用すれば、計算能力、ストレージ能力、技術的ノウハウが得られるだけではなく、グローバルなセキュリティオペレーションセンター（SOC）およびスレットインテリジェンスフュージョンセンターも利用できる。SOCやスレットインテリジェンス融合センターは、データの集約、誤検知の除外、実用的な情報の取得に不可欠だ。

同業他社や業界団体、政府機関とスレットインテリジェンスを共有すれば、モニタリングおよびアナリティクスツールはより絶大な威力を発揮する。クラウドは情報を保存・共有するための安全な単一プラットフォームを実現するのだ。情報共有については、後続のレポートで詳しく取り上げる。

パスワードから高度認証へ

認証において、パスワードは「123456」と同じ程度のものでしかない。誰でも思いつくような数列がいまだにパスワードとして広く使用されている。

推測困難なパスワードの重要性の理解が進まないこともあり、多くの企業は高度認証技術へと舵を切っている。追加のセキュリティレイヤーを設け、顧客やビジネスパートナーからより強い信頼を得るためだ。

認証技術はユーザーの利便性を高めるだけではなく、データセキュリティ全体も強化する。本年の調査では、高度認証を導入している企業の46％がオンライントランザクションのセキュリティが強化されたと答えている。また、認証技術が自社のセキュリティおよびプライバシーの信頼の向上、カスタマーエクスペリエンスの改善、ブランドのレピュテーションの保護に役立ったとも述べている。

57%

生体認証を採用していると答えた回答者の割合

PwC、CIO and CSO、The Global State of Information Security® Survey 2017、2016年10月5日

かつて、高度認証は主に政府システムや大手金融機関で利用されていた。しかし近年、ソーシャルメディアや消費者向けeメールプロバイダーが多要素認証を導入するようになり、多要素認証を幅広く採り入れる業界が増えている。

多要素認証の考え方はシンプルだ。名前とパスワードを入力し、認証を完了するためのコード（第二の要素）が記載されたテキストメッセージをモバイルデバイスで受け取る。多要素よりもさらに進んだオンプレミステクノロジーの開発・実装に取り組んでいる企業もある。このような認証では、ユーザーが入力しなければならないパターンや、アクセスカード、ハードウエアトークン、指紋または虹彩スキャンなどの生体情報を使用する。

新しい認証テクノロジーの実装に伴い、ID管理へのアプローチを見直す必要があるかもしれない。IDに基づく信頼関係を構築し、顧客にとって使いやすいソリューションを設計するためだ。また、アクセスに伴うリスクのレベルに見合った認証を導入することも重要だ。

オープンソースソフトウエアが可能性を開く

オープンソースソフトウエアの採用は、オンプレミスソリューションの開発・稼働、ITサービスの提供方法に大きな変化をもたらす。

この動きは業界を問わず広がっている。ソフトウエア製品の最大手、Microsoft社も含め世界の大手企業がオープンソースへの移行を進めている。同社はSQL Serverのコンポーネントである.NETとPowerShellをLinuxで利用できるようにした[2]。また米国政府も、連邦政府資金によるWebサイト、アプリ、その他のソフトウエアプロジェクトの新規コードの少なくとも20%をオープンソースとしてリリースすることを機関に求めるパイロットプログラムを立ち上げた[3]。

49%

オープンソースソフトウエアの利用によりサイバーセキュリティプログラムを向上したと答えた回答者の割合

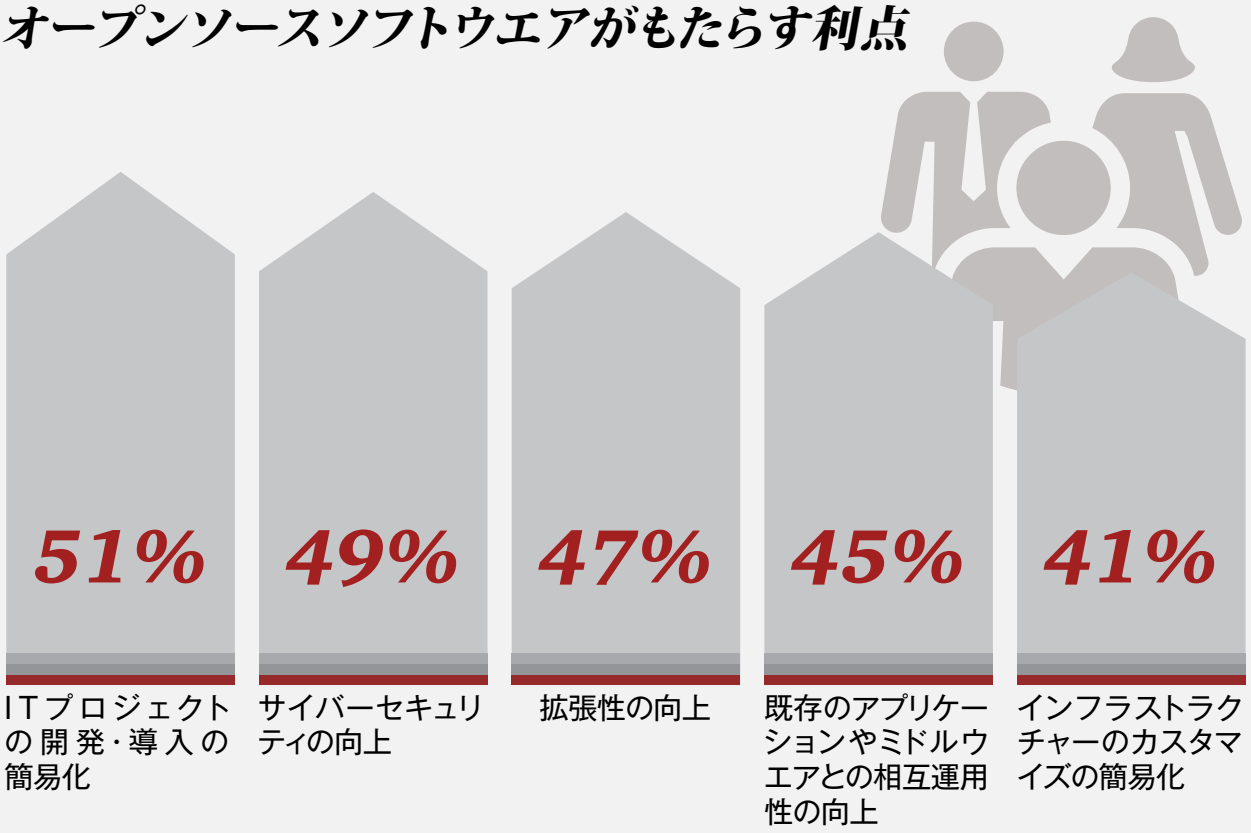
PwC、CIO and CSO、The Global State of Information Security® Survey 2017、2016年10月5日

このような状況を考えると、回答者の半数以上（53%）が何らかの形でオープンソースソフトウエアを利用しているという結果は驚くほどのことではない。しかし、オープンソーステクノロジーを利用している回答者の49%はサイバーセキュリティ態勢が向上したと答えたことはやや予想外であった。

オープンソースソフトウエアが採用されている理由はいくつかある。オープンソースアプリケーションは素早く効果的に拡張できる他、さまざまな業界のセキュリティ人材が協力して開発・テストを行っていることが多い。ソフトウエアのコストがほぼゼロであり、新しいソリューションを低コストで開発できる。クラウドと組み合わることで、オープンソーステクノロジーは増え続けるデバイス、センサー、テクノロジー、IDの間での相互運用性をさらに広げることも可能だ。

2 Microsoft AzureBlog、*PowerShell is open sourced and is available on Linux*、2016年8月18日
3 Federal Source Code Policy、*5. Open Source Software*、2016年9月20日アクセス

オープンソースソフトウエアがもたらす利点



出典:PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

このようにさまざまな利点をもたらすオープンソースは、革新的テクノロジーとなる可能性を秘めている。*「オープンソースを採用する業界はこれからも増えていくだろう」*とPwCのBurgは述べている。*「オープンソースには、優れたアプリケーションやサービスをできるだけ効率的に開発するという集団思考が生かされている」*

データプライバシーに関するグローバルリスクの高まり

相互接続されたデジタルエコシステムとそこから生じる脅威がサイバーセキュリティに変化をもたらす一方、テクノロジーの進化が世界各国の法規制を変化させている。法規制の激変は、位置情報追跡やビッグデータ分析などの新しいテクノロジーに対する強制措置や集団訴訟のかつてないほどの増加、そして規制当局による監視の強化を招いている。

事実、本年は新しい要件の施行・発表が相次いでいる。

特に影響が大きいのは、2018年5月に施行されるEUの一般データ保護規則（GDPR）だ。GDPRによりプライバシーの必要性が波及的に高まり、EU市民に商品やサービスを提供する企業はデータプライバシーへの取り組みを見直さなければならない。GDPRを遵守しなければ、世界年間収益の4％もの罰金が科せられる[4]。欧州の判例から、プライバシーを巡って集団訴訟を起こされる新たなリスクが生じている。

4　欧州連合、*一般データ保護規則（GDPR）*、2016年9月20日

*「GDPRでは、プライバシーの取り扱いについて前例のないレベルでの内部統制が求められる」*と、PwC Cybersecurity and PrivacyのPrincipal Jay Clineは指摘する。*「2018年の春、EU在住の5億人が新しい権利を行使し、多国籍企業の責任を厳しく追求できるようになる」*

GDPRの次の五つの重要要件は、欧州でビジネスを展開する企業に深い影響を及ぼすだろう。

- 欧州住民の個人データのインベントリの作成と全ての処理プロセスの記録の義務付け
- 情報漏えいが発生した場合の、規制当局および当該情報の所有者へのデータ漏えい通知の義務付け
- 忘れられる権利に基づく個人データの消去の要請の受容
- プライバシー影響評価の定期的な実施
- データ保護責任者（DPO）の設置の義務付け

GDPRの遵守は多くの企業にとって課題だ。包括的なリスク評価や、徹底的な新しいセキュリティ強化策を実施しなくてはならない。多くの企業では、データガバナンス戦略の見直し、総合データインベントリを維持するためのプロセスおよびテクノロジーの実装が必要になるだろう。

その準備を整えることができるのは、先を見越して行動した企業だけだ。GDPRに対する準備状況を評価し、GDPRとのギャップを埋めて十分な運用適合性レベルを実現し、継続的なコンプライアンスモニタリングプロセスを策定することで、先行して法規制に対応することができる。

多くの米国企業はGDPRに加え、プライバシーシールドへの対応も迫られる。これはセーフハーバーの後継として、大西洋を横断したEU市民の個人データの転送を管理するフレームワークだ。プライバシーシールドへの参加により、ソーシャルメディアへの投稿から給与支払い処理まで、あらゆる種類のデータの格納・転送が厳しい監視下に置かれることになるのは間違いない。

コンプライアンスは、潜在的に負担を伴うものになりそうだ。例えば、米国企業はEU市民の個人データを共有するサードパーティーの身元を確認する必要がある。EUの個人データを処理するサードパーティーに対してプライバシー適正評価を実施した上で、要求に応じてコンプライアンスの証拠を作成し、責任者が署名しなければならない[5]。

多くの企業では、そこに至るまでに、データインベントリやデータフローマップを最新化し、EUの個人データの取り扱い範囲を検証する作業が必要だ。また、プライバシーシールドを遵守することの費用対効果を分析し、標準契約を設け、その責任についてテストする運用適合性の管理策を整備する必要もある。

新しい法規制や法律が負担となるのは、もちろんEUと米国だけではない。中国、韓国、香港、シンガポールなどのアジア諸国でも、その他の新たな重要規制が導入されている。

中国では、サイバーセキュリティ法案の下、禁止されている反道徳的な情報の拡散の防止が義務となり検閲が強化されるなど、政府がますます法規制を強めている。これは国外企業にとっては潜在的な課題だ[6]。最近のサイバーセキュリティ法では、テクノロジー企業や金融機関に、データを中国国内で保存すること、セキュリティチェックを受けること、要望に応じて復号に協力することを求めている。これを受けて、多くの企業は共同事業を強化するか、中国のパートナーを通じての取引を増やしている。

5 米商務省、*プライバシーシールドフレームワーク参加要件*、2016年9月20日
6 Broader Perspectives、*Chinese Cybersecurity Rules Alter Business Paths*、2016年6月14日

しかし最近になって、中国は態度を軟化させ、外国企業がサイバーセキュリティ標準を定める政府組織の会議に参加することを許可した[7]。中国がグローバルなテクノロジーサプライチェーンに理解を示し、自国の政策を国際的なトレンドに合わせる必要性を認識するようになったのは朗報だ。

サイバーセキュリティおよびプライバシーに関する法律の厳格化は、韓国の個人情報保護法（PIPA）の改正にも表れている。この改正により、1億韓国ウォン以下の罰金もしくは10年もの禁錮刑、またはその両方を含む刑罰が新たに定められる[8]。

香港では、個人情報（プライバシー）条例によって個人データの収集・取り扱いの法規制が強化された。サードパーティーへのデータの転送や国境を越えた転送にも規則が設けられる[9]。刑罰は100万香港ドル以下の罰金と5年以下の懲役だ。

7 SC Magazine、*China allows foreign tech firms to participate in creating cybersecurity standards*、2016年8月31日
8 韓国安全行政部、*個人情報保護法第70条*、2016年10月3日アクセス
9 PwC、*Are you taking action on data privacy?*、2013年1月

香港金融管理局は5月、全ての銀行を対象として、サイバーレジリエンス管理に関する協議のフレームワーク草案として「Cyber Fortification Initiative」を発表した。新たなフレームワークは2016年後半または2017年初めに発表される見込みだ。

またシンガポールでは、2014年7月に施行された個人情報保護法により、個人情報の収集、利用、開示、国境を越えた転送に新しい規制がかけられる。違反した場合は、100万シンガポールドル以下の罰金と3年以下の懲役が科せられる[10]。

データローカリゼーション要件の増加、データ漏えい通知の義務化、ビッグデータ分析の制限といった全体的なトレンドに対応するためには、ビジネスおよびテクノロジーの両分野のリーダーがグローバルなプライバシー戦略の策定に積極的に取り組む必要がある。法令順守にとどまらず、データのグローバルな転送や収益化に関する手順も含め、卓越した戦略を目指すべきだ。

10　シンガポール個人情報保護委員会、*法律およびガイドライン*、2016年9月30日

法規制の変化への対応

データプライバシー規制やインターネット利用規則の進化は、企業にとって新たな課題を生み出す。多くの経営幹部が懸念を抱いていることは明らかだ。PwCが実施した第19回世界CEO意識調査では、本年のビジネス成長を脅かす最大の要因として過剰規制が挙げられた[11]。

グローバル情報セキュリティ調査2017で今後12カ月において優先するプライバシー対応を尋ねたところ、最多回答は「プライバシーに関するトレーニング」であった。僅差で2番目になったのは「プライバシーポリシーおよび手順の更新」だ。

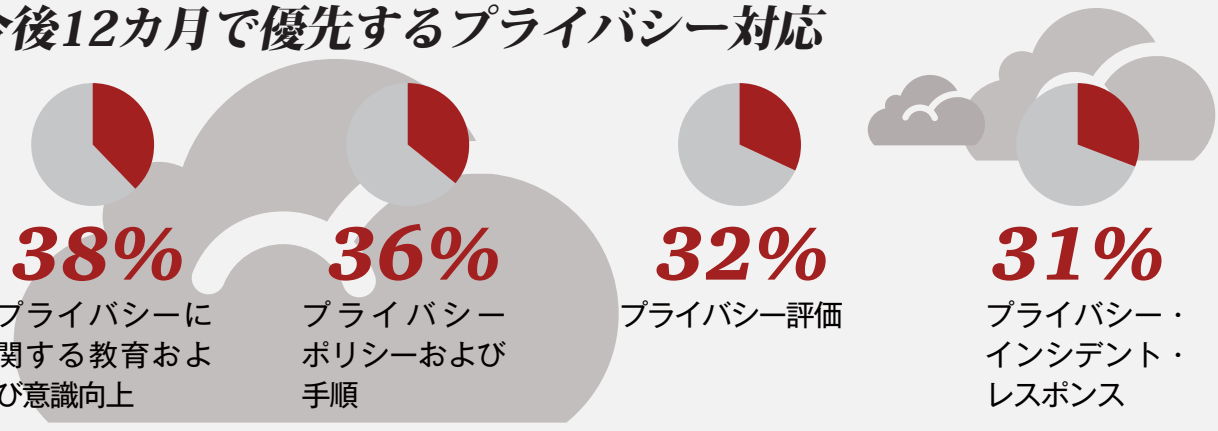
「教育や意識向上プログラムを改善するには経営トップが基調を定め、自社のデジタルによる未来の実現を強調する必要がある」と、PwCのWaterfallは述べている。「企業の目的と結び付け、プログラムを設計すべきだ」

その他にも、プライバシーやコンプライアンスの管理方法の開発・更新、データ利用のガバナンスフレームワークの実装・更新、影響分析の実施、最新のデータプライバシーライフサイクルプログラムの整備状況の確認が必要だ。インフラストラクチャーとテクノロジーを安全に統合してITの冗長性に対応し、状況に応じてそれらのシステムをクラウドに移行すれば、多くの企業が利点を得られる。

収集する顧客情報の種類を慎重に検討し、保存・収集するデータの量を最小限に抑えることの重要性は、かつてないほど高まっている。ビジネス上の利点はリスクに勝る。

11　PwC、第19回世界CEO意識調査、2016年1月

今後12カ月で優先するプライバシー対応



出典: PwC、CIO and CSO、*The Global State of Information Security® Survey 2017*、2016年10月5日

過去、現在、未来の可能性

この10年間、テクノロジーとサイバーセキュリティは急激に発展した。

例えば、Amazonが企業に対してAmazon Web Services（AWS）によるITサービスの提供を開始したのはたった10年前のことだ[12]。現在、世界の企業の過半数（回答者の63％）がITサービスをクラウドで運用していると回答している。

10年前、デジタルビジネスモデルは多くの企業にとって得体の知れないものであった。2007年の時点では、デジタルモデルの実装方法どころか、その利点すら理解されていなかった。考え方に不信感を抱く企業もあった。そのわずか数年後、AOLとTime Warnerが合併し、時価総額3,500億米ドルの巨大企業が誕生したが、結局は失敗に終わったのは周知のことだ[13]。

それから10年経った今、回答者の59％がデジタル化によりセキュリティ支出が増加したと答えている。企業は未来を見据え、デジタル時代に合わせたビジネスモデルの最適化に取り組んでいる。多くの企業がクラウドコンピューティング、先進的データモニタリングおよび分析、オープンソーステクノロジーをはじめとする基本的要素を実装し、デジタル化とサイバーセキュリティ、プライバシーを統合している。

サイバーセキュリティおよびプライバシーが企業にどのような脅威をもたらすのかを理解する能力も身についた。2008年の調査では、回答者の42％が検知されたセキュリティインシデントの原因を把握していなかった[14]。本年の調査では、侵入者（従業員やビジネスパートナー、ハッカー、政治的ハッカー、国家など）を特定できなかった回答者は13％にすぎない。

ついに多くの企業がサイバーセキュリティやプライバシーが単なるITの課題ではなく、サイバーセキュリティがビジネスにおける優位性、信頼、株主価値を生み出すということが理解され常識となった。また、デジタルビジネスモデルとサイバーセキュリティを組み合わせることで、まったく新しいデジタルプラットフォーム、製品、サービスを確信を持って作り出すことも可能となった。

未来は計り知れない。しかし、人工知能や機械学習、高度認証、適応制御などのテクノロジーは発展していくだろう。それらがクラウドにおいて統合されることで、新しいアーキテクチャーモデルや優れたサイバーセキュリティおよびプライバシー機能が登場する可能性は高い。企業はこれらを活用して、複雑な、しかしありふれた、脅威の先を行くことができるようになるだろう。

12 CIO、*10 Cloud Computing Companies to Watch*、2009年5月18日
13 The New York Times、*How the AOL-Time Warner Merger Went So Wrong*、2010年1月10日
14 PwC、CIO and CSO、*The Global State of Information Security® Survey*、October 2008

日本企業への示唆

本セクションは、The Global State of Information Security® Survey 2017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。

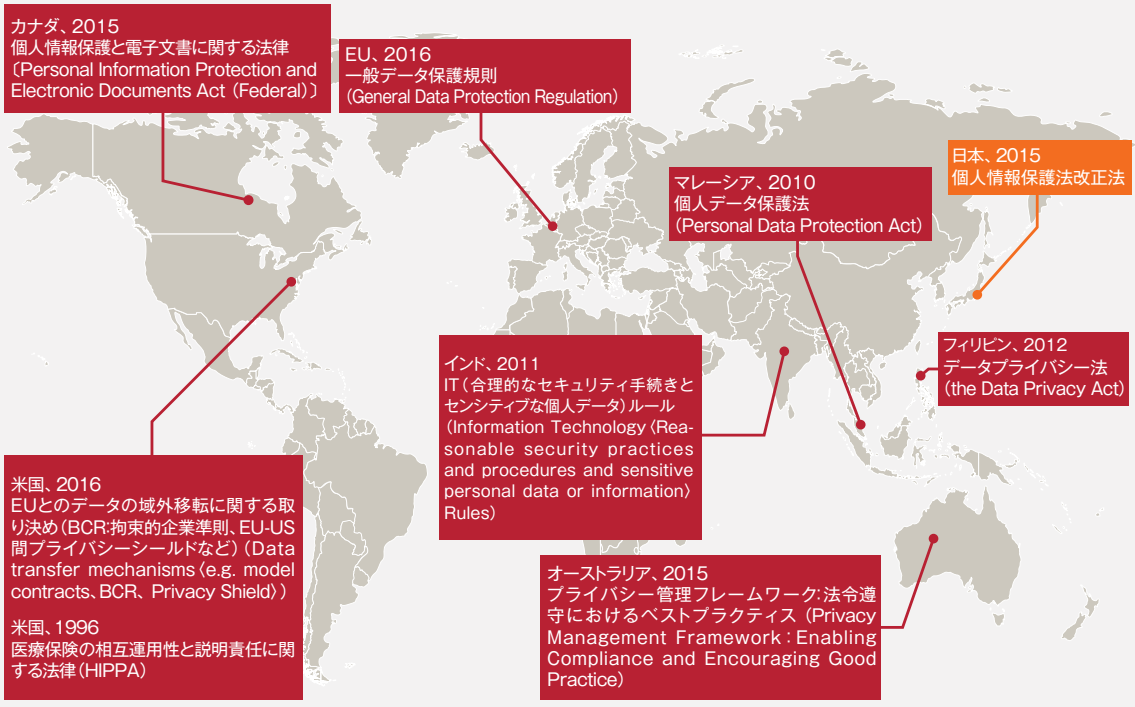
示唆①：世界で高まるデータ保護要件にどのように対応していくのか

～グローバル企業が対応すべき個人データ保護関連法令～

企業活動のグローバリゼーションや情報技術などの発展により、消費者などの個人情報は国境を越えて利活用されるようになった。地理的・時間的な制約にとらわれないユニバーサルなサービスが普及し、ビジネスのデジタル化が急速に拡大している。

一方、流通する情報の量が飛躍的に増えたことで、情報漏えいリスクに対する個人の意識も高まっている。自国の産業を保護する目的もあり、近年、各国では個人情報保護政策の強化を進めている。日本においても、2015年9月9日に個人情報保護法の改正法が公布され、現在、多くの日本企業は、法規制施行までの限られた時間の中での対応に追われている状況である。

図1：個人データ保護関連法令の潮流



～容易にクリアできないGDPRの要求事項～

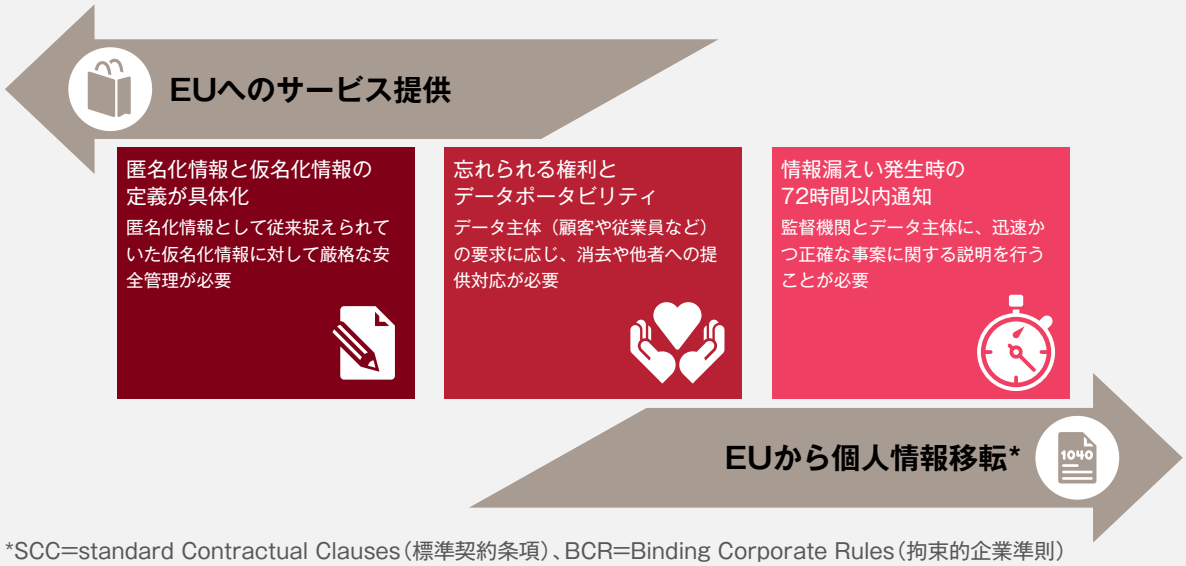
前述のとおり、世界中で個人情報保護の規制が強化され、国外の企業に対しても罰則を含めた監督方針や安全管理措置の見直しが急速に進んでいる。これらの取り組みに大きな影響を与えているのがEUの一般データ保護規則（GDPR：General Data Protection Regulation）である。日本企業もそのビジネスモデルによっては規制の対象となり、違反した場合、「企業の全世界年間売上高の4％以下または2,000万ユーロ以下のいずれか高い方」の罰金を科せられる可能性がある。

日本企業においてGDPRの対象事業者となるケースは、図2のとおり大別すると二通りのパターンが考えられる。一つは、日本企業が直接EUへサービス提供を行うケースである。もう一つは、EUから日本に個人情報を移転するケースだ。対象となる日本企業は、個人情報・データのフローの遵守性を早急に検証する必要がある。

ケース	具体例
EUへのサービス提供	・インターネットを通じた小売業でEUの消費者にサービスを提供する
EUから個人情報移転	・EU域内の支社などが現地顧客の個人データを取得し、日本にあるデータベースに保管する

GDPRの施行により日本企業が特に影響を受けるポイントとして、「匿名化情報と仮名化情報の定義が具体化」、「忘れられる権利とデータポータビリティ」、「情報漏えい発生時の72時間以内通知」などが考えられる。顧客や従業員単位でデータの取得から提供、廃棄まで厳格な安全管理措置が求められる点を考慮していく必要があるのだ。

図2:GDPRの要求事項



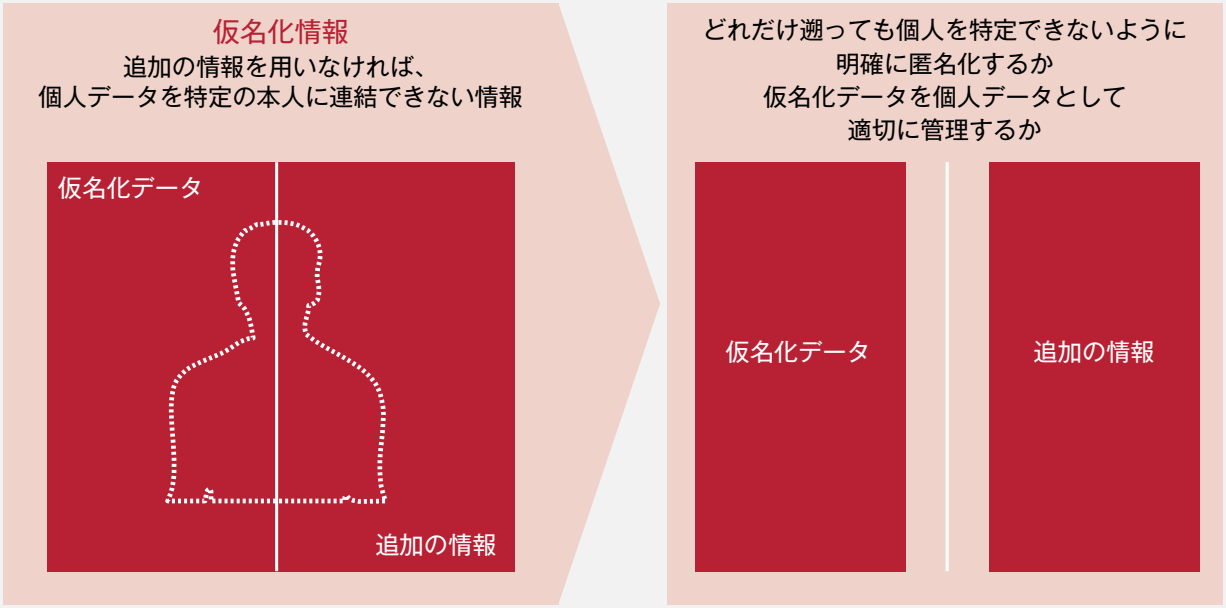
*SCC=standard Contractual Clauses（標準契約条項）、BCR=Binding Corporate Rules（拘束的企業準則）を通じた各加盟国のDPA=Data Protection Authority

～匿名化の落とし穴～

匿名化は、個人データを保護する手法の一つである。GDPRでは、匿名化情報を「特定の、もしくは特定可能な自然人（いわゆる“人”のこと）に関連しない匿名の情報。または、データ主体が特定されない、もしくは特定される可能性のない方法で匿名化された個人データ」と定義している。匿名化された情報は、もはや個人データとはみなされず、GDPR各規則の適用対象外となる。

一方、「追加の情報を用いることよって、個人データを特定のデータ主体に結び付けることができる個人データ」のことを、GDPRでは仮名化情報と定義している。匿名化とは明確に区別しているため注意が必要である。仮名化されたデータは依然として個人データであるためGDPRの適用対象であり、「追加の情報」を別に管理するなど、個人が特定されないよう技術的・組織的措置を講じる必要がある。

図3:GDPRが求める仮名化情報の取り扱い



～個人データを十分に利活用できているか～

図4は、企業において実施済みの情報セキュリティ対策を調査した結果である。図が示すとおり、日本企業における「個人情報取扱規程の整備などプライバシー特化の対策」は、グローバルと比較して15ポイント上回っており、他の対策と比較しても大きくリードしている。日本企業のコンプライアンス意識の高さが見て取れる結果となった。

しかし、この「日本企業のコンプライアンス意識の高さ」は、法令・ガイドラインが求める“適切な”安全管理措置を過度に捉え、時にビジネスの阻害要因にもなりうる。法規制にのっとって顧客の情報を管理することは最低限の要件をクリアしているだけに過ぎず、顧客データに鍵をかけて大切にしまっておくことは、顧客に提供する価値の最大化には直結しない。

図5は、企業のプライバシーを扱う部門が今後取り組む予定のプロジェクトを調査した結果である。ここで挙げたプロジェクトはいずれも、個人情報・個人データを利活用し自社のビジネスが提供する価値を向上するために必要不可欠だと考えられる。しかし、残念ながら現時点では日本企業における意識はまだ低い。

図4:Q.あなたの組織では、どのようなセキュリティ対策を実施していますか

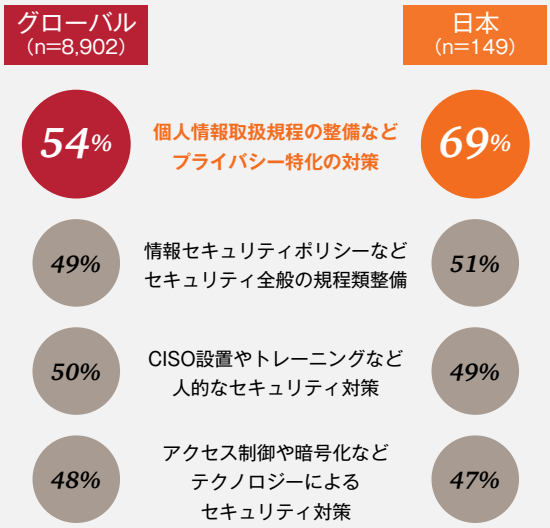
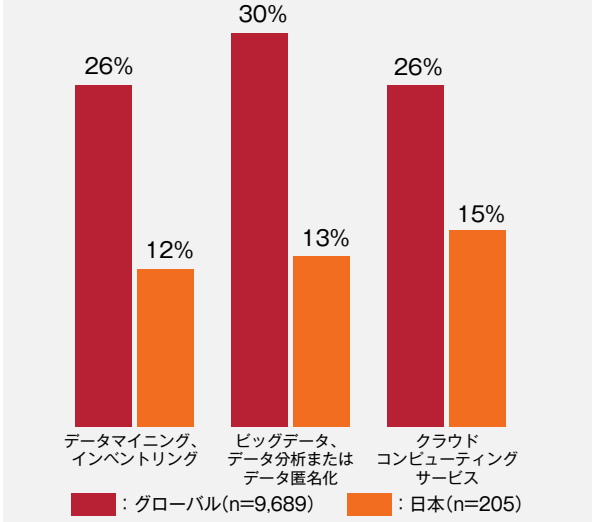


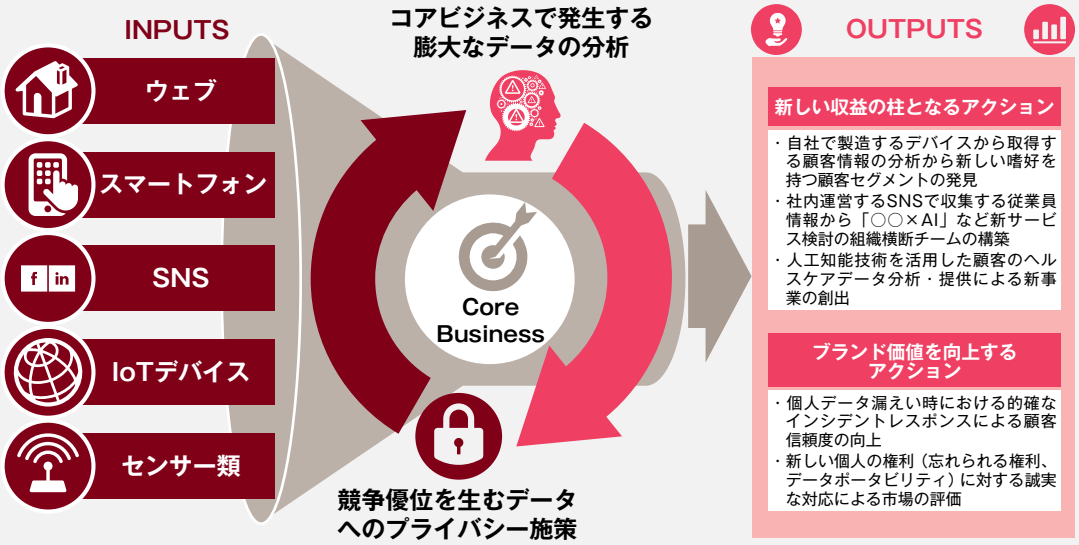
図5:Q.今後1年以内にプライバシー部門が取り組むプロジェクトは何ですか



～新たな価値提供の源泉となるデジタル戦略～

顧客情報や従業員情報を適切に保護することは企業にとって最低限の社会的責任である。しかしその一方で、企業が社会に価値を提供し続けるには、個人データを含むあらゆるデータを最新の技術とともに活用することが欠かせない。自社のコアビジネスで管理するあらゆるデジタルデータの集積・分析を深化させ、既存のものとは異なる新たな価値を創出し、コアビジネスを進化させる戦略が求められる。顧客接点となるデバイスやSNS、製造ライン上のIoTデバイスやセンサー類などあらゆるインプットを整理し、コアビジネスが提供する価値を進化させるデジタル戦略を策定することが求められる。

図6:企業の価値を進化させるデジタル戦略（イメージ）



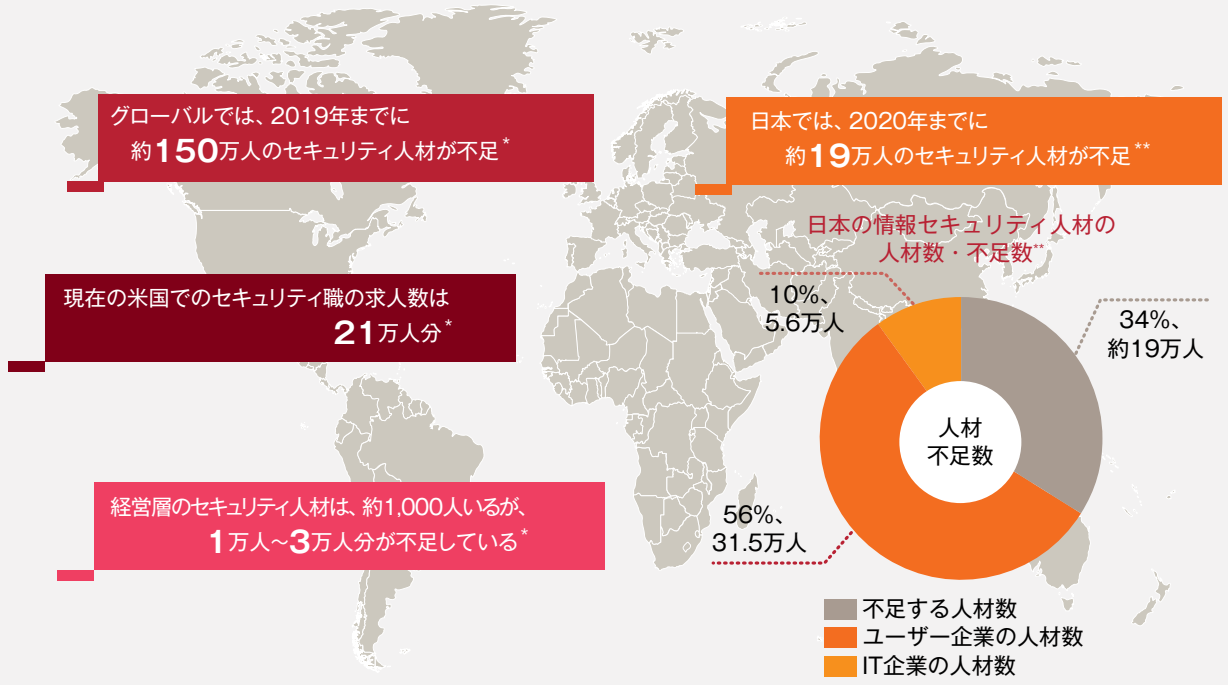
示唆②：人材不足への解決策

～世界中で不足するセキュリティ人材～

サイバー空間における脅威が増している一方で、セキュリティ人材の不足が著しい。人材不足は世界中で発生しており、グローバルでは、2019年に約150万人、日本でも2020年に約19万人のセキュリティ人材が不足すると言われている（図7）。

このように世界中でセキュリティ人材が不足する状況下では、社外から適切な人材を採用することは、ますます困難になっていくだろう。このままでは、本来必要なセキュリティ組織を整備することができず、急激な進化を続ける攻撃者に対応しきれない事態に陥ってしまう。サイバー攻撃への対応が経営課題として認識される昨今、セキュリティ人材の慢性的な不足という状況に手をこまねいていては、物事は何も進まない。

図7：セキュリティ人材の不足状況

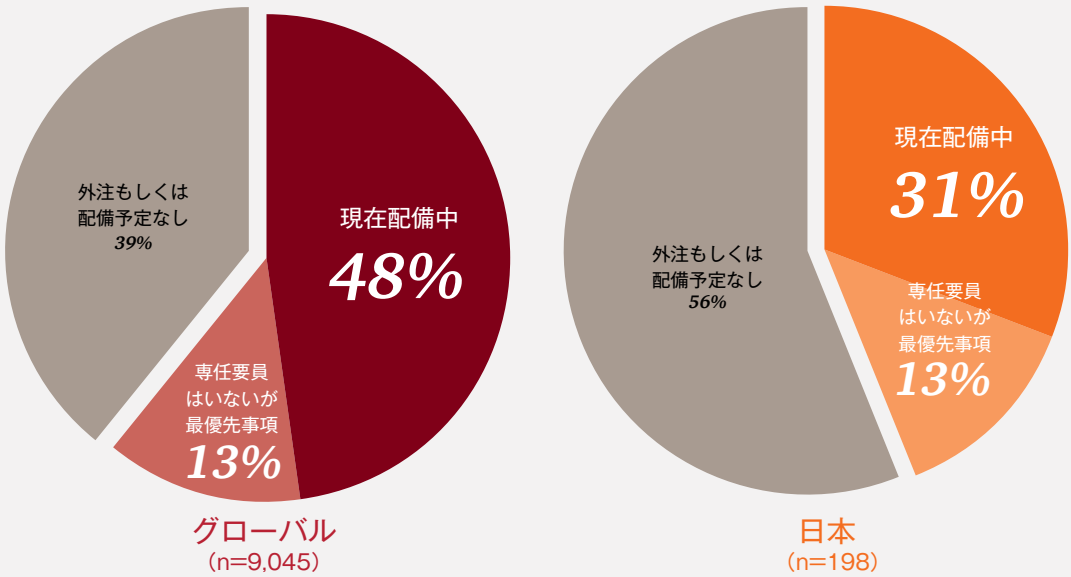


* 出典：「Market expansion adds to cybersecurity talent shortage」（CSO）2016年7月
** 出典：「IT人材の最新動向と将来推計に関する調査結果」（経済産業省）（http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html）（2016年11月1日に利用）

この状況下で、企業はどの程度セキュリティ人材を確保できているのだろうか。今回の調査の結果、実際にセキュリティ人材を雇用できている企業は、グローバルで約5割、日本においては約3割にとどまっていることが分かった（図8）。

今後、さらに増大する脅威への対応にあたり、どのようなセキュリティ組織を考えていくべきだろうか。

図8: 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



～【解決策1】社内人材を育成する～

一つ目の解決策は、社内でセキュリティ人材を育成し、増やしていく方法である。

これは時間を要する施策である。しかし、私たちの経験上、セキュリティ組織強化のために、最も近道だと感じていることでもある。枯渇した人材市場において優良人材を探し求めるより、自組織の中で育成する方が、よほど効率的だろう。また、セキュリティ人材を育成していく過程において、セキュリティ管理の業務内容が整理され、文書化、標準化されるなど、セキュリティ組織にプラスの影響を与えることが多い。

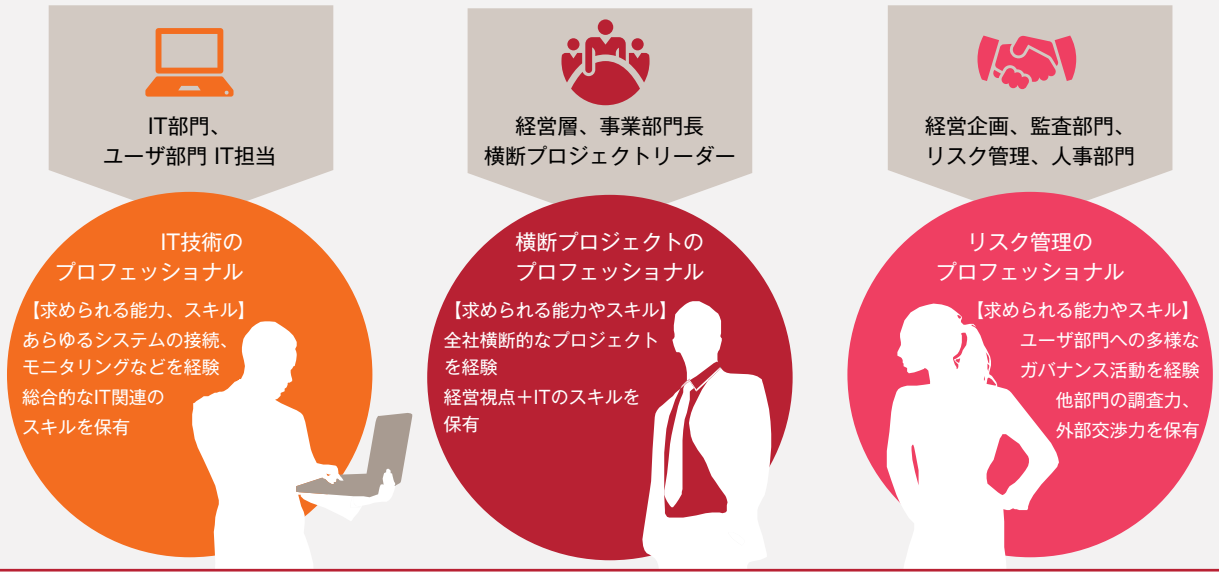
育成の対象は、技術分野の人材だけでない。なぜなら、企業におけるセキュリティ管理業務とは、もっと広範な要素が必要だからだ。例えば、「セキュリティ戦略の立案」、「セキュリティ投資にかかわる予算確保および投資後の効果測定」、「ポリシーや社内規程などの整備」、「国内外の個人情報に係る法規制への対応」、「消費者や株主などステークホルダーへの説明」、「経営層や社内への教育・啓発」、「外部委託先の管理・監視」などさまざまな領域に及ぶ。2016年9月に公開された「産業横断サイバーセキュリティ人材育成検討会

第一期最終報告書」においても、セキュリティ管理業務の多くが、セキュリティに特化したものではなく、複数の役割を掛け持ちで担当している実状について言及されている。

（セキュリティ）機能の多くがサイバーセキュリティに特化したものではなく、（省略）現状の企業組織においては、通常の技術者や数少ないセキュリティ技術者が、複数の部署で複数の役割を掛け持ちで担わされている実態が想起される（産業横断サイバーセキュリティ人材育成検討会「第一期最終報告書」2016年9月）。

IT人材をセキュリティ人材として活用することは容易に考えられるだろう。セキュリティへの取り組みを通し、多様なシステムとの接点を持つことができる。他にも、経営企画やリスク管理部門といったガバナンス活動に特化した人材をセキュリティの分野へ転用することも可能だ。彼らを、リスク管理のプロフェッショナルへと育成していくことは、セキュリティ、リスク管理両方の面で利点がある。また、セキュリティプロジェクトの多くは、経営層から一般の従業員まで、複数の部署にまたがる活動を求められる。全社に影響を与える横断プロジェクトの経験を得る場として、リーダー人材の育成にも有用だろう。経営視点とITスキルを身につけることができる。社内他部署の人材に目を向け、セキュリティ組織を補完するとともに、セキュリティという場を用いてあらゆるプロフェッショナルを育成していくことは、効果的な施策の一つと言える（図9）。

図9:セキュリティ組織に転用可能な人材像

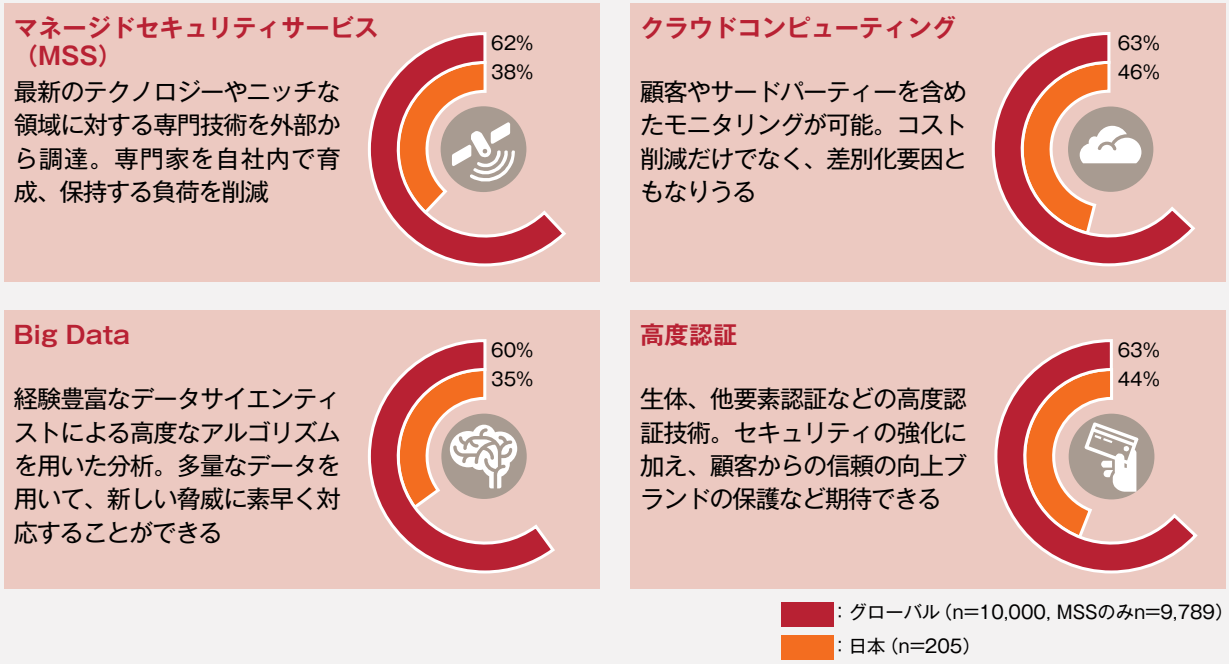


～【解決策2】テクノロジー活用により人材不足をカバーする～

二つ目の解決策は、テクノロジーを活用して技術者不足を補う方法である。

さまざまなテクノロジーを活用することによって、人的リソースに対する負荷低減を目指す。今回の調査の結果、日本とグローバルでは、テクノロジー活用状況に大きな乖離があることが浮き彫りとなった（図10）。マネージドセキュリティサービスや、クラウドコンピューティングなどの活用は、社内で人的に行っていた業務を移管することが可能だ。最近では人工知能を活用したセキュリティ製品も多く市場に投入されるようになった。とりわけ、スレットインテリジェンスを活用したサイバー攻撃の予見機能や即時検知機能など、セキュリティ運用の負荷を下げると同時に精度の向上も期待される。これまでに導入してきたさまざまなセキュリティ施策は、重要な資産の厳守や、法令遵守、インシデント発生後の即時回復などに重きを置いてきた。これらを見直し、最小限の労力で同一の目標達成を目指す、効率的なセキュリティへと舵を切るべきではないだろうか。

図10:日本／グローバルにおけるテクノロジー活用状況の格差



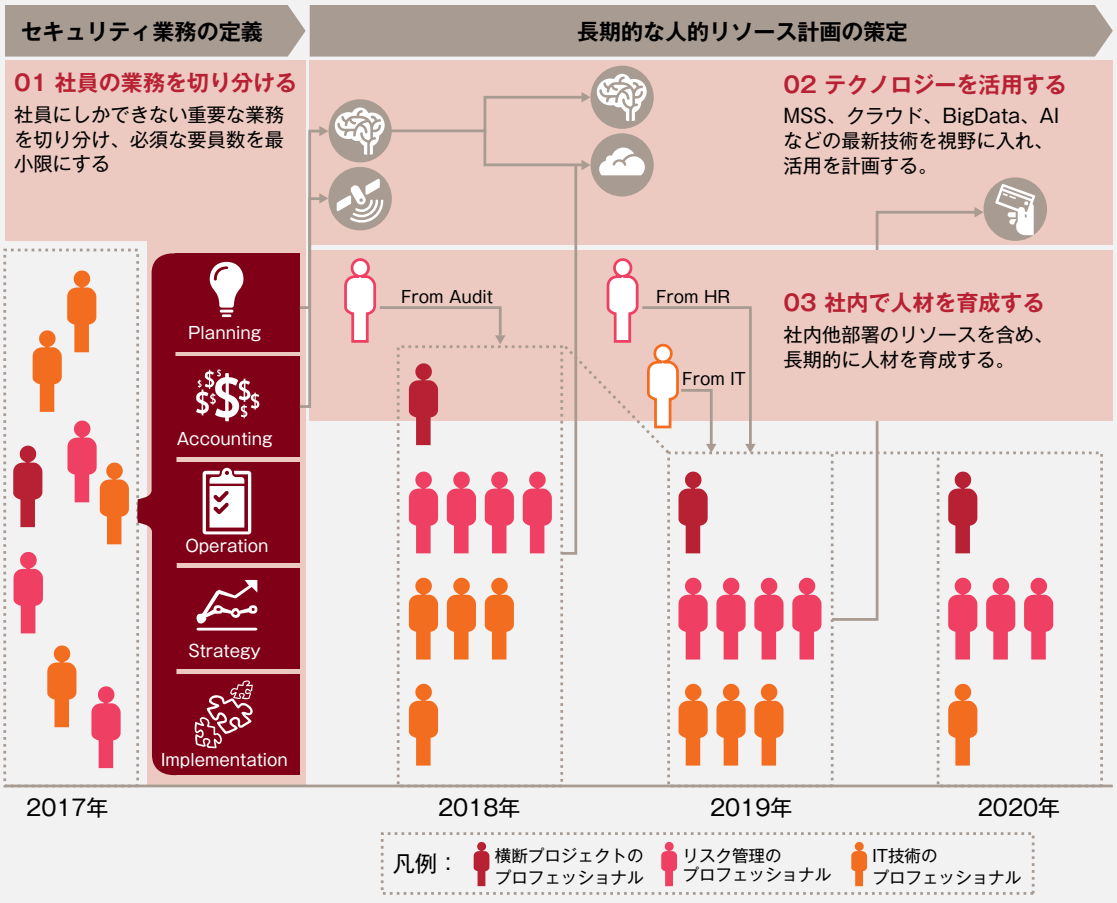
～【推奨アプローチ】セキュリティ組織の長期的な計画を立てる～

社内人材の育成やテクノロジーの活用は、いずれも成果が出るまでに時間を必要とする。長期的な視点から、自社に適したセキュリティ組織を考えていかなくてはならない。

まずは社内のセキュリティ管理業務を専門分野ごとに棚卸し、社員を充てる必要のある重要業務、およびそのボリュームを可視化する。次に、テクノロジーが活用できる業務、外部に移管可能な業務を整理し、導入のロードマップを立てる。最後に、社員が行う重要業務に必要な人材を見極め、他部署の人材の発掘、および育成シナリオを立案する（図11）。

サービス攻撃の脅威はいつ自組織を襲ってくるか分からない。そのため、セキュリティ組織には、常に対応できる態勢の維持が求められる。確実なセキュリティ対応や継続的な能力向上のために、将来を見据えたセキュリティ組織のあるべき姿を描き、長期的な計画を立てることが重要である。

図11:セキュリティ組織の強化計画におけるアプローチの例

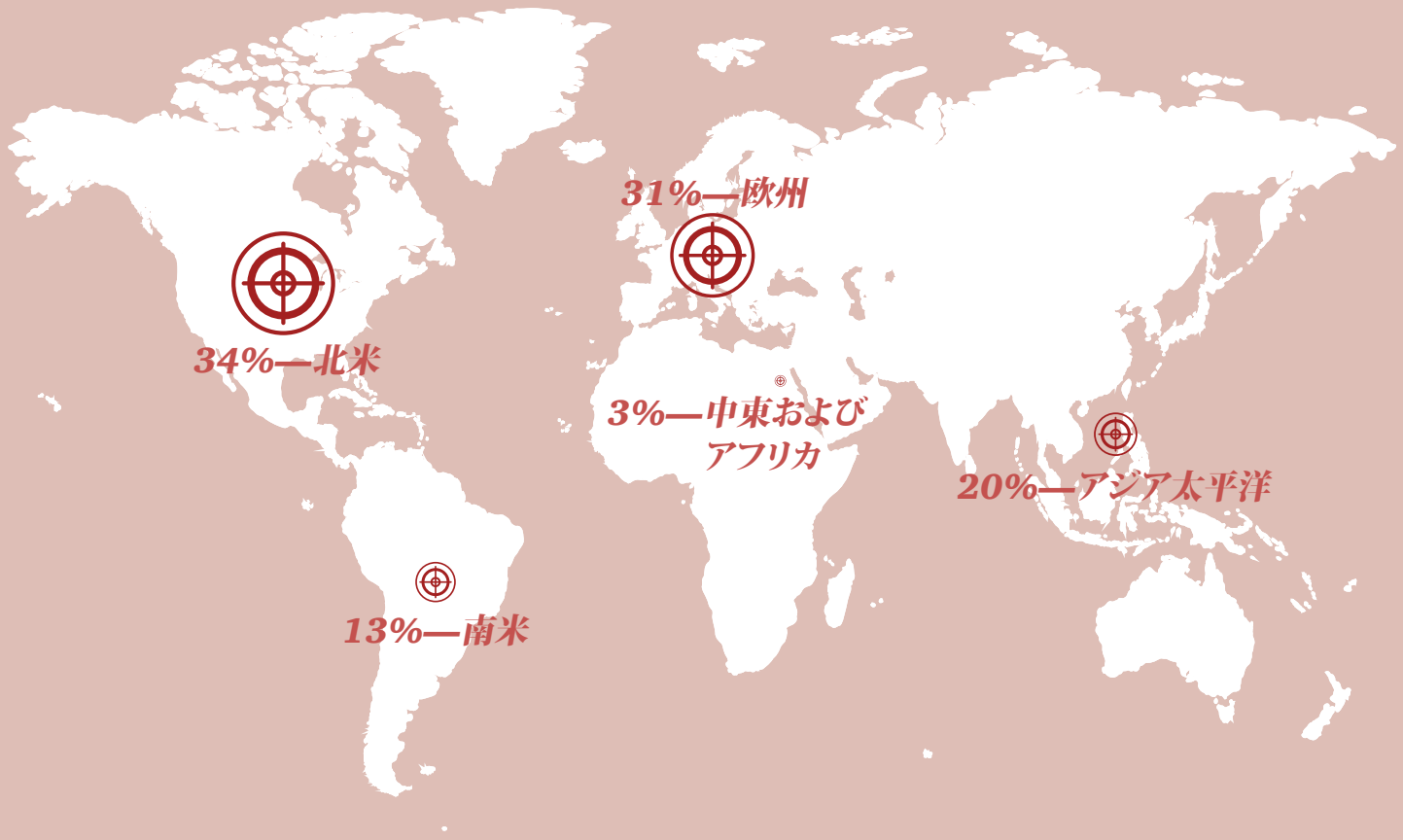


調査方法

The Global State of Information Security® Survey 2017（以下、「本調査」という）は、PwC、『CIO magazine』、および『CSO magazine』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 magazine』および『CSO magazine』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、133カ国の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。

回答者の地域別構成は、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）

Australia

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

Austria

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

Belgium

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

Brazil

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

Canada

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

China

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

Denmark

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

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

France

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

Germany

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

India

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

Israel

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

Italy

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

Japan

Yuji Hoshizawa
Partner
yuji.hoshizawa@pwc.com

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

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

Korea

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

Luxembourg

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

Mexico

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

Middle East

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

Netherlands

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

New Zealand

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

Norway

Lars Erik Fjørtoft
Partner
lars.fjortoft@pwc.com

Poland

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

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

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

Russia

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

Singapore

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

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

South Africa

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

South East Asia

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

Spain

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

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

Sweden

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

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

Switzerland

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

Turkey

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

United Kingdom

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

United States

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

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
上杉 謙二
道輪 和也
篠宮 輝
河崎 玄志
本川 友理
小林 啓将

PwCあらた有限責任監査法人
百歩 路子

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

ショーン キング
パートナー
sean.c.king@pwc.com

PwCサイバーサービス合同会社
〒104-0061 東京都中央区銀座8-21-1
住友不動産汐留浜離宮ビル
03-3546-8480（代表）

星澤 裕二
パートナー
yuji.hoshizawa@pwc.com

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、法務のサービスをクライアントに提供しています。
PwCは、社会における信頼を築き、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界157カ国に及ぶグローバルネットワークに223,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.com をご覧ください。

本報告書は、PwCメンバーファームが2016年10月に発行した『Moving forward with cybersecurity and privacy』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/japan-knowledge/thoughtleadership.html
オリジナル（英語版）はこちらからダウンロードできます。 www.pwc.com/gx/en/industries/financial-services/fintech-survey/insurtech.html
日本語版発刊月： 2017年2月　　管理番号： I201604-5