ビジネス成長の武器となるサイバーセキュリティ

著者

Joel Barbier
Lauren Buckalew
Jeff Loucks
Robert Moriarty
Kathy O'Connell
Michael Riegel

考察

- かつてないほどの革新が起きている時代において、企業はサイバーセキュリティが単なる「防衛」機能だという従来の見方を改める必要があります。
- Square, Inc のデータ セキュリティおよび業界交渉の責任者である Mike Dahn は、この状況について次のように述べています。「現在セキュリティは、恐れや不安、疑いにつけこんで販売されていますが、そのような防御中心のアプローチとしてセキュリティを扱うことをやめることがとても重要だと思います。セキュリティとは、イノベーションをサポートし、ビジネスを推進するためのイネーブラであると考えるようにしなければなりません」
- シスコの新しい調査結果[1]では、そのような企業が増えていると報告されています。
- 1014 名を対象とした調査では、回答者（財務および基幹業務部門の幹部）の 31 % が、サイバーセキュリティの主要な目的は、**成長の実現**であると考えています。69 % は、現在でもサイバーセキュリティの主な目的をリスク軽減だと考えています。
- 44 % は、サイバーセキュリティは組織にとって**競争上の優位性**になると考えています。56 % は、サイバーセキュリティをビジネス運営上のコストであると見なしています。
- 経営幹部は、サイバーセキュリティと*デジタル化*の間には重要な関連があり、業務、プロセス、ビジネス機能が、1 つのリエンジニアリングされたデジタル運用モデルへと移行すると考えています。
- 多くの経済価値をもたらす可能性があります。シスコは、今後 10 年間に、全世界で 7.6 兆ドルのデジタル経済価値[2]を創出するであろう **414 のユース ケース**を特定しています。
- このうちの 4 分の 3 以上は、**成長のイネーブラとしてサイバーセキュリティが関係するものです。**
- しかし残念なことに、多くの企業がこの可能性に気付いていません。シスコの調査では、71 % が、**サイバーセキュリティにはイノベーションを妨げるリスクがあると回答しています。**さらに、39 % が**サイバーセキュリティへの懸念によって、ミッションクリティカルな取り組みが停滞している**と回答しています。
- サイバーセキュリティに対する不安も、重要なデジタル化への企業の取り組みを遅らせる原因となっています。競争が激化している経済状況において、こうした取り組みが重要な差別化要因となる可能性が高まっています。
- 企業は「**セキュア デジタイザ**」の例にならう必要があります。セキュア デジタイザとは、サイバーセキュリティを重要な基盤として活用し、ビジネス モデルやオファリングをデジタル化することでビジネスの成長に注力している企業のことです。

「デジタル エコノミーは、現在の経済が単にデジタル化されたものではありません。デジタル エコノミーについて検討するにあたり、欠かせないのがサイバーセキュリティです。脅威の面からだけでなく、サイバーセキュリティが何を実現できるかという観点から考える必要があります。」

– dPrism 創業者兼 CEO Adriaan Bouten

はじめに

革新を進める企業は、コストの削減、カスタマー エクスペリエンスの向上、オファリング[3]の拡張を実現する、新たな価値の源泉として、デジタルの力を活用しています。デジタルを活用する革新的な企業は、従来型の企業に対してイノベーションにおける圧倒的な優位性を誇っています。こうした革新的な企業は、新しい機会を見い出し、そうした機会を活用するために素早く変化することに長けているからです。[4]

厳しい競争が続く環境下で、新興企業や俊敏性の高い企業が、デジタル化したビジネス モデル、製品、およびサービスを武器に、既存の企業を凌駕しつつあります。[5]

あらゆる企業が、かつてない変化をもたらし、業界の垣根を取り払う「デジタル化の渦」の中心に向かって引き寄せられています。[6] 適応できない企業は、市場から撤退を迫られるか、ビジネス自体を続けられなくる確率が著しく高くなります。IMD とシスコの取り組みである Global Center for Digital Business Transformation の最新調査では、各業種のリーダー企業の 10 社のうち 4 社が、今後 5 年間にデジタル化した革新的な企業に取って代わられると予測しています。[7]

従来型の企業がデジタル化の渦の中で競争し生き残るためには、「誰も利用していない価値」—デジタル革命をおこせば利用できる市場機会—を見つけ、革新者に対抗できるようなデジタル化戦略を採用するしかありません。[8]

しかし、デジタル変革には、強力なサイバーセキュリティ基盤が必要です。この基盤を構築することで、企業は、イノベーションと成長を促進するデジタル プロセスやテクノロジーを安心して導入できるようになります。この基盤がなければ、企業はデジタル プロジェクトの開始に二の足を踏み、イノベーションの可能性を放棄して、デジタル革命への道を閉ざしてしまうことになります。

取締役や経営幹部の間で高まりつつある懸念

経営幹部クラスのリーダーの多くが、優れたサイバーセキュリティが成長を可能にすることを理解している一方で、脅威の防御についても引き続き懸念を持っています。サイバーセキュリティの侵害は急増しており[9]、何百万ものレコードが外部のハッカーの被害にあうことは、かつては驚くべきことでしたが、今やいたって当たり前のことになっています。

そして、シニア エグゼクティブもこうした状況を認識しています。87 % は、自社にはサイバーセキュリティの侵害に関する懸念があると述べており、約半数が「非常に不安である」と回答しています。また、41 % は、このわずか 3 年の間に「不安度が大幅に高まった」と答えています。

こうした懸念は IT 組織だけの問題ではありません。サイバーセキュリティ関係の大規模なインシデントが発生した場合に、最も責任が大きいと考えられているのは CEO と取締役会ですが（図 1 参照）、企業リスクの管理責任者、最高情報責任者（CISO）、CIO および部門長も、事態が悪化した場合の責任を負うべきだと見なされています。

財務および基幹業務部門の経営幹部は、サイバーセキュリティが取締役会レベルの懸念事項になっていると回答しています。監査機関は、企業のサイバーセキュリティの弱点を、受託者の責任の一部として重点的に調査しています。サイバーセキュリティは、財務リスクおよび安全性/セキュリティのリスクとともに、企業のリスク管理の柱となっています。そのため、監査機関は、CFO[10] や最高リスク責任者など、企業のリスク管理に対して責任を持つ経営幹部がサイバーセキュリティに関する責任を持つべきだと主張しているのです。

ビジネス エグゼクティブは、CIO や、場合によっては CISO など、サイバーリスクの技術面を理解している人の協力を仰いで、信頼できるガイダンスとアドバイスを提供しなければなりません。シスコの調査結果が示すように、現在、IT に関する支出の 46 % は、企業の収益源や重要な業務に対する責任を持つ、基幹業務の幹部が管理しています。[11]企業が新しい製品やモバイ

手法

この調査について

2015 年 10 月、シスコは 1014 名の経営幹部、VP、部門長に対するオンライン調査を実施しました。調査対象者の 3 分の 1 以上が財務を担当し、サイバーセキュリティ関連の投資に影響力を持っています。残りはさまざまな基幹業務部門の関係者です。回答者は、オーストラリア、ブラジル、カナダ、中国、フランス、ドイツ、インド、英国、米国 および日本から選出されています。

加えて、11 名の専門家を対象にした定性調査も実施しました。対象者は全員上級幹部か、過去に上級幹部を務めた経験がある人物で、サイバーセキュリティに関するさまざまな経歴を持っています。また、このうち 2 名はサイバーセキュリティに関するコンサルティングの専門家です。

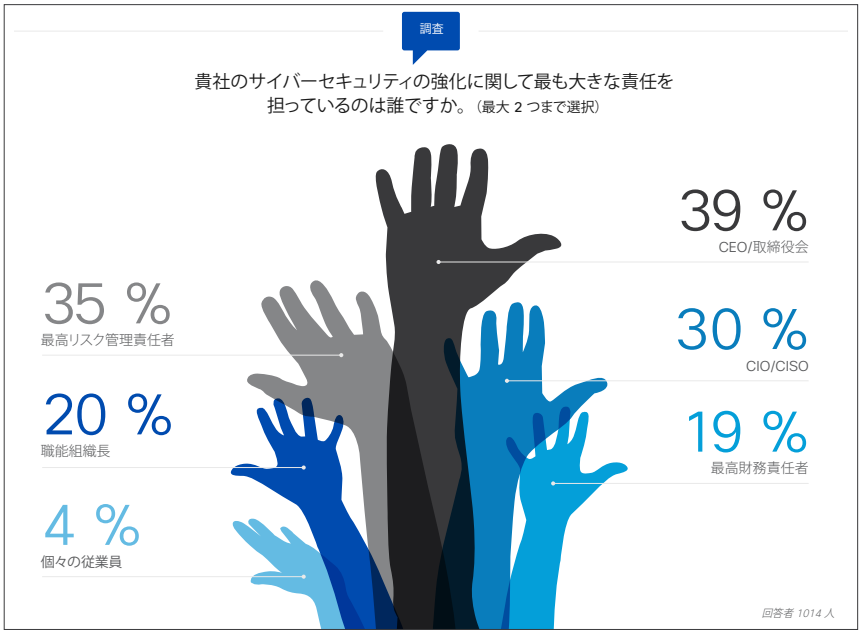

図 1
サイバーセキュリティの責任はトップにまで及ぶ

出典：
シスコ、2016 年

ル アプリケーションをリリースする場合、基幹業務の幹部が開発や業務遂行の最終責任を持つことになるというのは、これらの経営幹部も認識しています。基幹業務の幹部の 54 % が、「顧客などの主要なステークホルダーは、サイバーセキュリティに関する責任を、自分たち経営幹部が「大きく」負うべきだと考えている」、と回答しています。

侵害のダメージが甚大であることから、上級幹部は、侵害を防止する責務は自分たちが負うべきだと考えています。

サイバーセキュリティの侵害による平均被害額は巨額で、さらに増加を続けており、2014 年の 352 万ドルから 2015 年は 379 万ドルに増えています。[12]

侵害の影響は、損害を算出しやすいコストだけにとどまらず、インシデント対応、犯罪調査、内部監査、コミュニケーションなど、多岐に及びます。今回調査した財務経営幹部は、最も恐れるべき影響は、顧客の信頼を損なうことによってビジネスを失うことだ、と回答しています（図 2 参照）。自分のアカウントがサイバー脅威に対して脆弱であることを恐れ、顧客がある企業との取引を停止したら、その企業は多額の収益を失う可能性があります。

図 2
侵害の影響は多方面に及ぶうえに甚大である

出典：
シスコ、2016 年

基幹業務の幹部は、顧客データは最も重要な保護の対象だと答えていますが、その理由は明らかです。顧客データの紛失や侵害は、さまざまな悪影響をもたらす原因となります。企業はビジネスを失うだけでなく、訴訟、罰金、規制の強化、修復費用などの損失を被る可能性があります。経営幹部のほぼ全員（92 %）が、規制機関や金融機関の監視が厳しくなると予測しています。最新の発表では、新たな規制の波がやって来ることを示しています。[13]

顧客情報が侵害されると、その影響は業界全体に波及する可能性があります。たとえば、小売業者がデータ漏洩の被害を受けると、顧客は個人情報の共有に不安を覚えるようになります。その結果小売業者は、購買者が期待するような、分析に基づいて高度にパーソナライズされたエクスペリエンスを、実店舗やオンラインで提供できなくなります。するとその小売業者の顧客は、安全なデータを利用してさらに優れたカスタマー エクスペリエンスを提供できる別の小売業者へと移ることになります。

各地域についての考察

サイバーセキュリティ戦略の責任者は国によって異なる

中国とインドでは、サイバーセキュリティに関する責任は最高リスク管理責任者が負う割合が最も高くなっています（両国の回答者の 44 % が回答）。

ブラジル、カナダ、英国では、CEO/取締役会が最も責任があるとされています。

CIO/CISO がトップ（37 %）となったのは米国のみで、米国で次に多かったのは CEO/取締役会（36 %）でした。

CFO が責任者であると回答したのは、全世界の調査対象企業の 19 % でした。中国では、企業の 29 % が CFO に責任があると回答しています。これは、調査対象となった国の中でトップの比率です。

経営幹部は、知的財産や他の機密情報などの戦略的資産が脆弱である可能性についても危惧しています。データ漏洩による総コストには、企業がイノベーションに費やした金銭面での投資や人的リソースの投資も織り込む必要があります。競合他社によって製品や計画の詳細情報が盗まれた場合に、企業が失う競争力も同様です。

経営幹部は、財務データ、ビジネス プロセス、特殊なノウハウ、サプライヤとの契約などを保護することも重要だと述べています。資産の損失による損害が企業にもたらす影響をよく理解しているのです。さらに、調査対象者の多くは脅威の発生源についても危惧しており、27 % が、最大の懸念として産業スパイをあげています。

不十分なサイバーセキュリティが阻害するイノベーションと競争力

脆弱なサイバーセキュリティについて、非常に重要であるにもかかわらず見逃されていることが多いのが、*企業のイノベーションと成長への影響*です。これは、特にデジタル オファリングとビジネス モデルを開発する場合に当てはまります。

シスコの調査では、71 % もの経営幹部が、サイバーセキュリティに関する懸念が組織のイノベーションを停滞させていると回答しています。また、39 % が、サイバーセキュリティの問題によってミッションクリティカルな取り組みが停止していると回答しています（図 3 参照）。

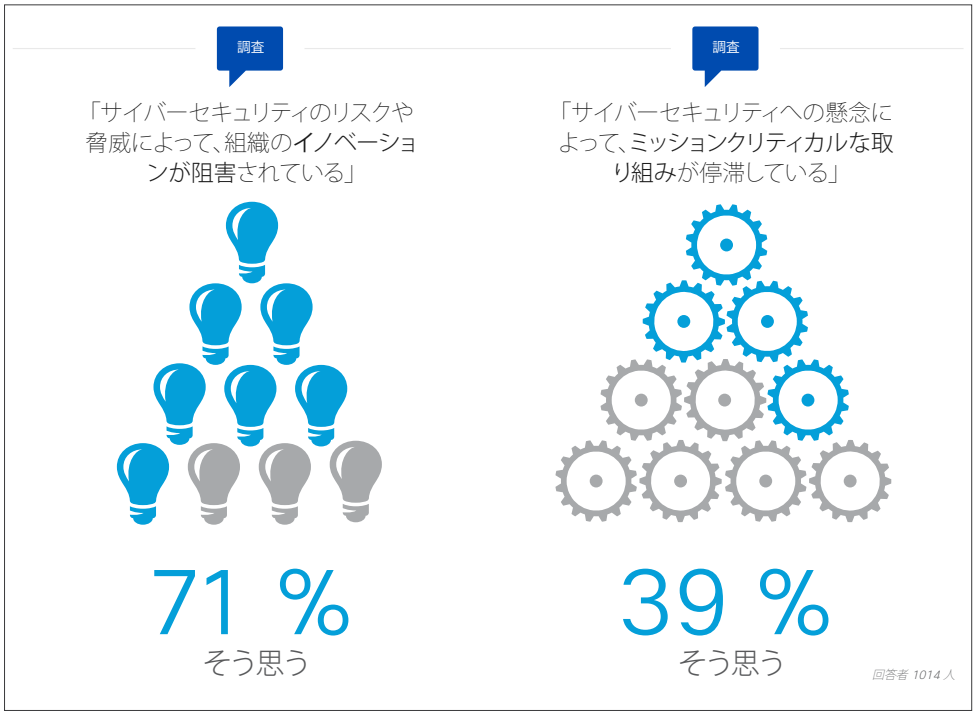

図 3
不十分なサイバーセキュリティはイノベーションを妨げ、ビジネスの速度を低下させる

出典：
シスコ、2016 年

この調査では、サイバーセキュリティに関する懸念がイノベーションに与える影響と、地理的な場所との間には強い相関関係は見られませんでした。サイバーセキュリティの脆弱性に関して認識された脅威がイノベーションに与える影響は、インド、中国、英国、カナダの回答者で高く、米国が最低でした。サイバーセキュリティ上の懸念から、組織がミッションクリティカルな取り組みを停止しているという回答者が最も多かったのはインドとブラジルでした。

業種では、イノベーションに対する脅威の影響が最も高かったのは、技術製品、ビジネス サービス、小売業、金融業でした。一方、最も低かった業種は、サービス業/旅行/娯楽、製造/消費財でした。サイバーセキュリティに関する懸念が原因で、ミッションクリティカルな取り組みを停止している企業が最も多い業界はビジネス サービスで、次いで技術製品および教育でした。

一部の業種は、デジタル革命の影響をすでに大きく受けています。デジタルビジネスのリーダーたちは、デジタル製品やサービスを導入するリスクとメリットを敏感に認識しています。またその多くが、脆弱なセキュリティとイノベーションの喪失の関連を認識しています。

サイバーセキュリティが脆弱だということは「自覚症状のない病」のようなものです。この病にかかると、デジタル化の渦に巻き込まれる直前になってもイノベーションを起こすことができなくなります。デジタル化の渦[14]の中では、デジタル化、革新、急激な変化が「新たな常識」になっています。[15]多くの企業がこの病を患っていますが、そのことを自覚している企業は限られています。脆弱なサイバーセキュリティをそのままにしておくことは、デジタル化の渦の中では致命的です。

このようなデジタル化の渦の中で革新を進める企業は、従来型の企業にはない 3 つの強みを持っています。1) 革新性、2) 高い俊敏性、および 3) 実験的精神の 3 つです (図 4 参照)。従来型の企業が新興企業のスピードと効率性の両方に追い付くには、イノベーションに関する能力を大幅に向上させる必要があります。しかし、回答者の 60 % は、サイバーセキュリティのリ

「サイバーセキュリティの侵害に関する最大の懸念は、財務面への直接的な影響よりはむしろ間接的な影響です。企業の評判という点からはどのような影響があるでしょうか。お客様が当社は信頼に値しないと判断し、離れてしまったらどうなるのでしょうか。」

—Stein Mart CFO
Greg Kleffner

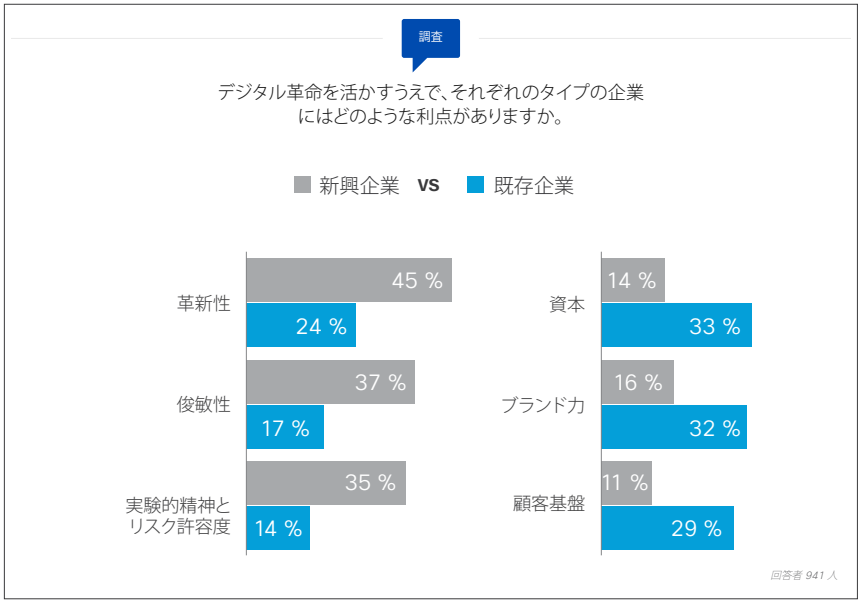

図 4
既存の企業には優位性があるが、新興企業に学ぶべきである

出典:
Global Center for Digital Business Transformation、2015 年

スクを恐れるがゆえに、デジタル製品やデジタル サービスといった分野の開発に消極的であると述べています。[16]残念ながら、革新を進める企業と戦うには、デジタル製品やデジタル サービスが必要です。

サイバーセキュリティがデジタル ビジネス モデルやイノベーションの推進を妨げる可能性がある一方で、多くの企業が、進歩しなければ、デジタル化を進める革新的な企業や俊敏性の高い企業の後れを取ると考えています。実際に、回答者の 73 % は、サイバーセキュリティのリスクがあったとしても、新しいテクノロジーやビジネス プロセスを採用する場合が多いことを認めています。

平均以下のサイバーセキュリティしかない企業は、競争において最悪の立場に置かれることになります。つまり、デジタル イノベーションで後れを取っている上に、競争するスピードも足りず、サイバー攻撃から自社を守るための安全性もないということになります。

さらに詳しい分析については、cs.co/cyberAB にアクセスしてください。

「イノベーションは進展しています。けれども、優れたサイバーセキュリティ ツールがないために、進展はおそらく本来の 70 ～ 80 % 程度に留まっているのでは...」

—CFO Robert Simmons

経営幹部はサイバーセキュリティが成長に貢献することを認めているが、この分野における投資は停滞

上級幹部クラスのビジネス リーダーたちは、製品、サービス、ビジネス モデルのデジタル化が必須であることを明確に認識しています。経営幹部の 69 % は、自社の現在の成長戦略にとってデジタル化が「非常に重要」であると回答しています。また、デジタル成長戦略の基礎としてサイバーセキュリティが不可欠であることも認識しており、64 % が、サイバーセキュリティは製品、サービス、そしてビジネス モデルのデジタル化を成功に導く「重要」な要因になると述べています（図 5 参照）。

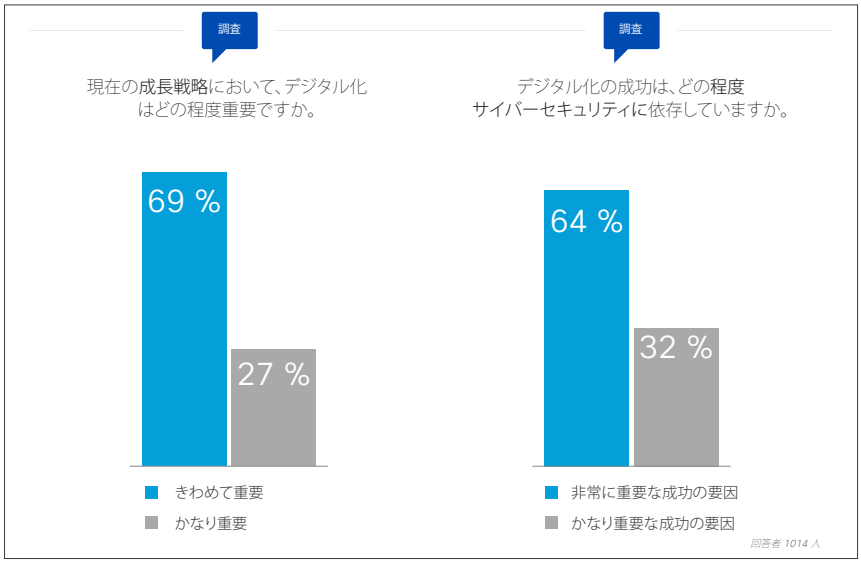

図 5
経営幹部は、サイバーセキュリティと、デジタル化および成長との関係を理解している

出典：
シスコ、2016 年

サイバーセキュリティ、デジタル化、イノベーションの関連が強固であることから、優れたサイバーセキュリティが、ビジネス価値を向上させる原動力であると認識されつつあります。シスコの調査によると、経営幹部の約 3 分の 1（31 %）は、この関係性をすでに認識しており、サイバーセキュリティの*最も重要な*目的を、「成長の実現」であるとしています。その一方で、経営幹部の 69 % は、サイバーセキュリティの主な目的を「リスクの軽減」と考えています。

同様に、44 % の経営幹部が、サイバーセキュリティが自分の組織の「競争優位性」につながると考えているのに対して、56 % は、「ビジネスの遂行に必要なコスト」と考えています。サイバーセキュリティへの投資に対する認識は、「防衛だけのための」投資から、さらに大きなイノベーションを「実現する」投資へと変わりつつあります。この認識の変化によって、企業の競争力が劇的に向上する可能性があります。

各国の中で、「成長を実現する手段」という考え方が最も多く見られたのは、中国、インド、カナダです（図 6 参照）。また、サイバーセキュリティを競争上の優位性と見なす傾向が強いのは、インド、中国、ブラジルです。この結果には、中国、インド、ブラジルという新興国でデジタル化が急速に進んでいる状況が、確実に反映されています。実際に、最新のシスコの分析 [英語] では、2024 年までに、全世界の民間企業におけるデジタル価値の約 3 分の 1 が、新興国によって創出されると予測されています。

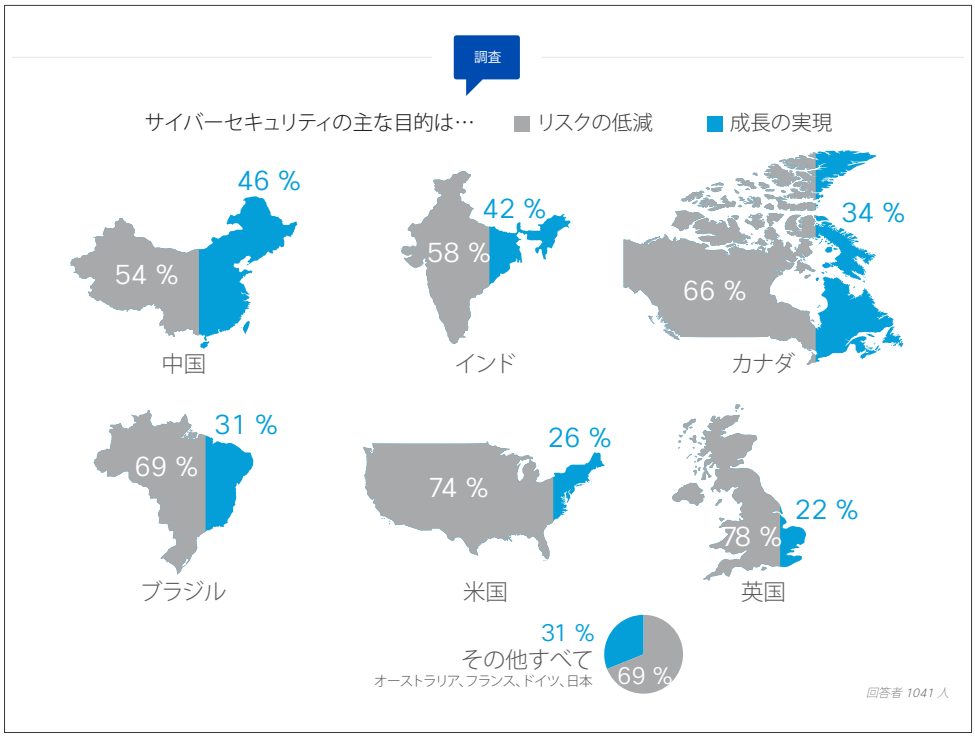

図 6
全世界で、経営幹部の約 3 分の 1 がサイバーセキュリティと成長を関連付けている

出典：
シスコ、2016 年

業種の中で、サイバーセキュリティを成長のイネーブラと見なす回答者が最も多かったのは、鉱業/エネルギー、小売、運輸/物流でした（次ページの図 7 参照）。このことから、ほぼすべての業種の経営幹部が、イノベーションの推進の必要性と、サイバーセキュリティとデジタル製品/サービスとの重要な関連性の両方を理解していることが分かります。

優れたセイバーセキュリティを真の競争優位性へと変換している企業は、イノベーションを高速化し、デジタル変革を完全に実現することが可能です。デジタル変革を

「市場で一歩抜け出すためには、サイバーセキュリティを必要悪と考えるのではなく、戦略的な強みだと考えることが必要です」

—フォーチュン 100 に選ばれた銀行の元人事部担当副社長

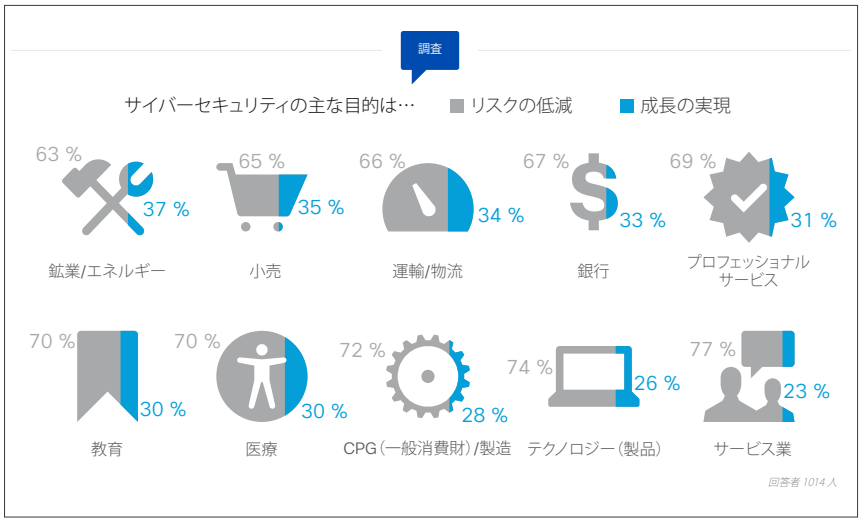

図 7
成長のイネーブラと見なす傾向は、鉱業/エネルギー、小売、運輸/物流の各業界で最も高い

出典：
シスコ、2016 年

実現することで、急速に変化する市場に素早く対応することができます。この俊敏性により、企業は効率性を高め、財務面でのパフォーマンスを改善することができます。

優れたサイバーセキュリティを導入している企業は、顧客から高い信頼を得ていることを示し、自社のブランドを差別化する機会が得られます。見込み客や顧客から、セキュリティ侵害やプライバシー侵害が発生しないと信頼してもらえれば、その信頼性は、品質、コスト、カスタマー エクスペリエンスとあわせて、ブランドの重要な属性の 1 つとなります。企業は、見込み客や顧客に対してその優れたサイバーセキュリティを伝えることにより、競争優位性を確立することができます。[17]

このようなメリットは、財務責任者がセキュリティに投資する際の判断に影響を与え始めています。現在、「ビジネスの成長を実現する能力」は、サイバーセキュリティへの投資を検討する際の決定要因の 3 分の 1 を占めています。残りは、脅威の防御や法令遵守など、防御に関する要因です（次ページの図 8 参照）。優れたサイバーセキュリティは、俊敏性、業務、デジタル化への対応力を向上させると企業に認識されるようになれば、シスコはこの「成長のイネーブラ」が投資判断に大きな影響を与えるようになると予測しています。

Gartner は、2015 年に企業の IT 予算が減少すると予測していましたが、[18] 企業はサイバーセキュリティへの投資を今までになく重視するようになっています。企業の 87 % が、来年はサイバーセキュリティへの支出を増やすとしています。さらに、41 % は「大幅に」増やすとしています。シスコがインタビューした財務部門の幹部は、サイバーセキュリティのメリットについての理解が進んだことから、サイバーセキュリティ プロジェクトの予算を獲得しやすくなっていると述べています。

さらに詳しい分析については、cs.co/cyberMD にアクセスしてください。

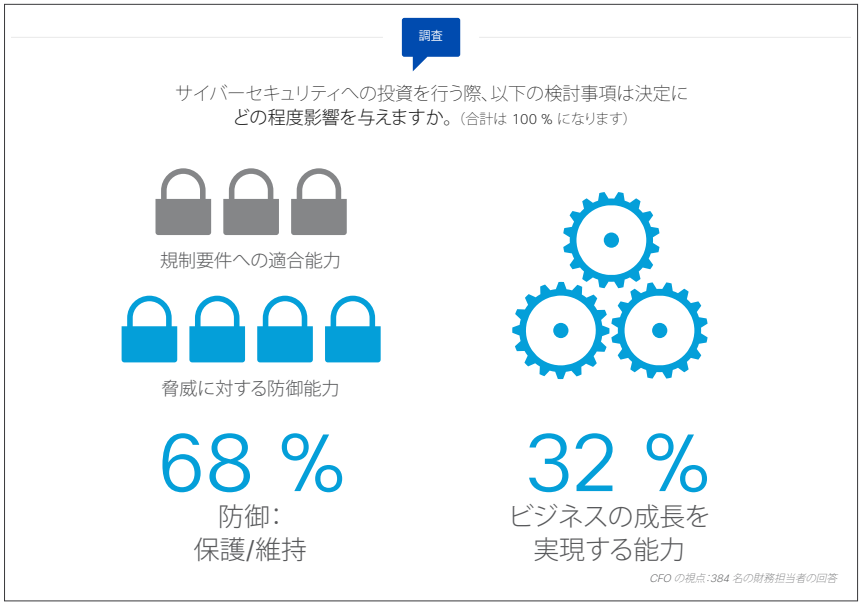

図 8
サイバーセキュリティが成長を牽引する可能性は投資決定の重要な条件

出典：
シスコ、2016 年

「これには教科書はありません…危機的なレベルのリスクの可能性と成長の機会の両方について検討する必要があります。リスクと機会の割合を決める公式を見出すことが課題の 1 つです」

—CFO Robert Simmons

しかし、サイバーセキュリティへの投資によるメリットを定量化できれば、企業の投資はさらに進むはずです。実際に、財務部門の幹部の 81 % が、サイバーセキュリティのビジネス成果を測定できる良い方法が見つかれば、サイバーセキュリティへの支出を「大幅に増やす」か「やや増やす」と回答しています。

調査の回答者は、適切な指標を見つけるのが難しいことを認識しています。「総収入の成長」や「収益性」などの定義済みのメトリックを使用して、サイバーセキュリティがビジネスに与える好影響を測定している企業は 88 % に及びますが、その測定方法が「非常に効果がある」と回答したのは 42 % のみでした。これでは、企業はコストのかかる戦略的な投資について、経営陣やステークホルダーを説得することができません。

その結果、ほとんどの企業がサイバーセキュリティへの投資を控える傾向にあります。実際に、今回の調査の回答者は、サイバーセキュリティへの投資が不足している問題は、急速に進化するデジタル ビジネス環境への対応や、サイバーセキュリティ プロトコルの効果的な適用という課題と同じく、現在直面している最大の経営課題の 1 つであると述べています。[19]

さらに詳しい分析については、cs.co/cyberRS にアクセスしてください。

サイバーセキュリティが実現するイノベーションと成長（400 以上のデジタル ユース ケースより）

シスコは、今後 10 年間に、7.6 兆ドルのデジタル経済価値を創出する 414 のデジタル ユース ケースを特定しています（詳細については、「セキュリティに価値を見出す」を参照してください）。

この経済価値のシェアを獲得するには、まずサイバーセキュリティの防御に関する側面を正しく把握する必要があります。今後 10 年間に、防御に関する 7 つの特定のユース ケースで、1.8 兆ドルのデジタル経済価値が実現されると思われます。これらのユース ケースには、知的財産の保護、データ侵害の削減（内部データと顧客情報の両方）、ビジネスの稼働時間の増加およびネットワーク停止時間の減少、金融資産の保護、行政/国家/政治に関する機密情報の保護、企業の信用の維持が含まれます。

しかし、最大のチャンスは、サイバーセキュリティを重要な基盤として活用し、イノベーションと成長を実現する 407 のデジタル ユース ケースにあります。シスコは、2015 ～ 2024 年の間に、こうしたデジタル ユース ケースによって 5.8 兆ドルのデジタル経済価値が創出されると予測しています（図 9 参照）。

この価値はどうやって算出されたのでしょうか。

シスコの調査では、多くの企業はサイバーセキュリティの脆弱性と懸念から、製品やサービスのデジタル化に消極的な姿勢をとっていることが明らかになっています。場合によっては、サイバーセキュリティを不安視するあまりに、ミッションクリティカルな取り組みが停滞してしまうこともあります。

このようなイノベーションの停滞は、損失として定量化できます。これを定量化するには、いち早くデジタル イノベーションを成し遂げた競合他社に奪われ、民間企業や公的機関が獲得できなかった価値に注目します。ここでは、今後 10 年間（2015 ～ 2024 年）に予想される 400 以上の潜在的なデジタル ユース ケースの価値の実現が、サイバーセキュリティの懸念によってどの程度妨げられるかを測定しました。

セキュリティに価値を見出す

デジタル経済価値は、2 つの要素から構成されます。すなわち、1）デジタル化への投資とデジタル イノベーションから生じる、完全に新しい価値の源泉と、2）企業や業界におけるデジタル機能の活用能力（またはその能力の欠如）に応じて、企業間で発生する価値のシフトの 2 つです。

シスコは、デジタル経済価値を、今後 10 年間（2015 ～ 2024 年）に創出される価値を合計する、「ボトムアップ」方式によって算出しました。計算の対象は、民間企業および公的機関に関する 400 以上のユース ケースです。経済価値は正味価値に基づいており、ユース ケースごとに利点とコストの両方が考慮されています。

これらのユース ケースは、テクノロジーをビジネスに導入することから予測される結果（この場合は、デジタル エコノミー/デジタル化によるビジネスの変革）を反映したものです。一般的な「ケース スタディ」では、テクノロジーを導入したことによる実際の成果を示しますが、それとは異なります。シスコの経済価値の計算には、業界固有のユース ケースと業界共通のユース ケースの両方が含まれています。

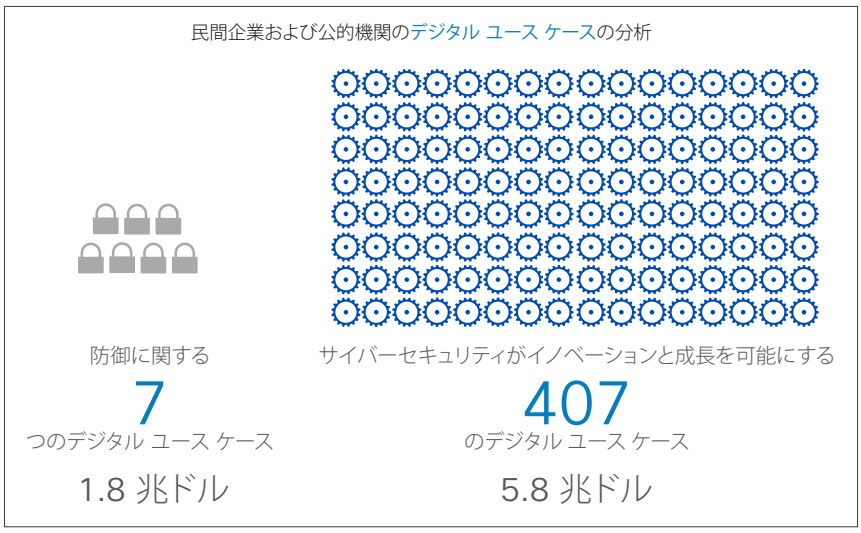

図 9
サイバーセキュリティのデジタル価値の 76 % はイノベーションおよび成長と関係している

出典：
シスコ、2016 年

この分析では、各ユース ケースに関連するサイバー リスクの程度に基づき、導入の遅れの程度を 1 年から 5 年の範囲で想定しました。リスクが大きくなるほど、問題の対処や克服に要する時間が長くなります。このリスクによって、デジタル機能に基づく成長戦略が阻害されたり、イノベーションやデジタル変革のペースが遅れたりする可能性があります。

したがって、企業におけるデジタル プロジェクトの遅延の原因となるサイバーセキュリティの懸念がなければ、控えめに見積もって 5.8 兆ドルの「成長」が、さらに大きくなるはずです。

製造業

たとえば、製造業界について見てみましょう。図 10 は、サイバーセキュリティのリスクが及ぼす可能性のある影響と、製造業における今後 10 年間のデジタル経済価値の大部分を推進すると思われる、7 つのユース ケースに関連する導入の遅れを示しています。これらのユース ケースのすべてで、Internet of Things や分析などに関するデジタル機能を製造現場に導入することを求めています。そのためには、自社のサイバーセキュリティが信頼できるものでなければなりません。そうでなければ、価値を実現する機会を逃すことになります。

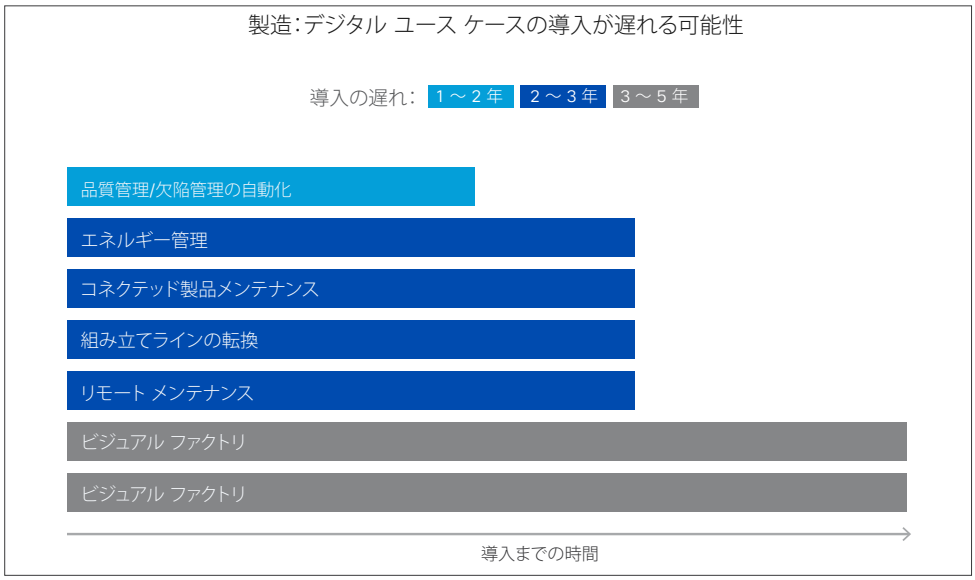

図 10
サイバーセキュリティに関する懸念によりデジタル化の取り組みが遅延すると、成長の可能性と市場での位置付けに悪影響が及ぶ

出典：
シスコ、2016 年

*分析を活用した予測ベースのメンテナンス*は、製造業者が競争力を維持するためには導入が必要不可欠なデジタル ユース ケースです。しかし、ほとんどの製造業者は予測ベースのメンテナンスに必要なアルゴリズムの作成はもちろん、実行の経験もありません。そのため、製造業者はパートナー（機器製作メーカーや制御ベンダーなど）に頼ることになります。これはオンプレミスのオファリングの場合も、クラウドによるオフプレミスのオファリングの場合もあります。オフプレミスのオファリングは、製造業者にとって新しく、馴染みのないコンセプトです。

このユース ケースで認識されるサイバーセキュリティのリスク レベルに基づき、シスコは、この業界では導入が 1 ～ 2 年遅れると推定しています。別の見方をすると、サイバーセキュリティに関する懸念のために製造業者がこの特定のユース ケースを導入できていないのであれば、すでにユース ケースを導入済みの競合他社に追いつくのに 1 ～ 2 年かかるということです。導入が遅れた製造業者は、予測ベースのメンテナンス（分析）によって今後 10 年間に世界中で発生すると思われる、4,180 億ドルのデジタル経済価値のシェアを得る機会を逃すことになります。その結果、こうした製造業者のイノベーションや成長を実現する力が衰えることになります。

導入が最も遅れると思われるのが、*リモート メンテナンス*のユース ケースです。

リモート メンテナンスでは、企業が外部のベンダーに自社のネットワークを開放しなければならない場合があります。リモート メンテナンス ベンダーは、問題を特定して解決するために、依頼企業の機器やデータにアクセスしなければなりません。これまで、こうした機器は内部ネットワークに接続されていませんでした。したがって、インターネットから機器にアクセスできるようにするという考え方は、多くの企業にとって事業運営のパラダイム シフトを意味します。しかし、企業は、リモート メンテナンスの必要性を認識しています。リモート メンテナンスにより、修理の専門家を特定の場所に派遣することなく、ネットワーク経由で問題を解消できるようにすることで、機器のダウンタイムを最小化することができるからです。

一元化されたリモート メンテナンス システムは高いレベルのリスクを抱えています。侵害が発生した場合、非常に長時間のシステム ダウンタイムにつながる可能性があるためです。たとえば、ハッカーが工場の制御システムや自動化システムに大損害を与えているにもかかわらず、それが長期間検出されなかったとすると、その企業は競争の上で大きな問題を抱えることになります。結論として、シスコはリモート メンテナンスのユース ケースについて、脆弱なサイバーセキュリティに関する認識の問題に対処し、克服するのに最大で 5 年かかると予測しています。その結果、市場における立場が弱くなり、成長が滞ります。

以下は、他の業界においてサイバーセキュリティが価値の創出を促進する事例です。

金融サービス：*モバイル決済*

金融機関は顧客からの信頼の上に成り立っています。特に、モバイル決済ビジネスは消費者の信頼に委ねられています。企業はセキュリティ侵害を防止し、万一侵害が発生した場合には素早く検出して修復しなければなりません。モバイル決済でセキュリティ侵害が発生すると、ダウンタイムの発生、収益の損失、ビジネスの信頼性の低下、損害対応費用の発生、財務データの喪失という結果を招く可能性があります。

その反面、適切なサイバーセキュリティ機能が導入されれば、モバイル決済は、2015 ～ 2024 年の間に、全産業で 3,960 億ドルの価値を創出することが見込まれます。

小売業：*店舗分析*

小売業界では、ダッシュボード、リアルタイム情報、運用分析、スタッフ管理ツール、購買分析などを利用した店舗分析によって、店舗スタッフの効率性が向上しています。ここで重要なイネーブラになるのがサイバーセキュリティです。分析情報の発生源を強固なものにし、情報の漏洩を防ぐには、情報の質とプライバシーが重要です。

セキュリティ侵害が発生すると、顧客情報の喪失や、データの汚染という結果を招く可能性があります。顧客も個人データを小売業者に提供することに不安を感じるようになるため、分析に使用する情報の詳細度や範囲が不十分になります。

適切なサイバーセキュリティ基盤があれば、店舗分析は、2015 ～ 2024 年の間に 2,850 億ドルのデジタル価値を創出する可能性があります。

石油/ガス：*原油流出制御*

デジタル化された原油制御システムにアクセスできない場合、原油の流出は長時間にわたって検出されません。これらのリモート システムの多くは、接続されていないか、オンデマンドで接続されるので、問題の発生から解決までに長時間かかる可能性があります。その結果、訴訟、汚染除去、システムのダウンタイムによるコストが増加することになります。

シスコは、サイバーセキュリティが、原油流出制御のユース ケースで「決定的な」役割を果たすと判断しています。そのため、サイバーセキュリティに関する懸念がある場合、導入に 3 ～ 5 年要する可能性があります。

正しく接続され、サイバーセキュリティが適切に導入されていれば、石油/ガスの企業は、これまで「闇に埋もれていた（未接続だった）」資産に「光を当て」、原油流出制御によって、2015 年～ 2024 年に 160 億ドルのデジタル価値を得ることができます。

イノベーション、価値、成長の実現は、組織が、デジタル戦略の*基盤*にセイバーセキュリティを組み込むことができるかどうかにすべてかかっています。シスコの調査では、*セキュア デジタイザ*[20]という新しい市場セグメントの存在が確認されています。セキュア デジタイザは、市場で最も効率的にセイバーセキュリティを導入していると考えられています。

サイバーセキュリティを活用して勝利を目指す*セキュア デジタイザ*

革新を進める組織とさらに効率的に戦い、自社のサイバーセキュリティを向上させるために、従来型の企業はデジタル ビジネスの*変革*を追及する必要があります。

真のデジタル変革とは、デジタル テクノロジーとデジタル ビジネス モデルによって推進される*組織的な変化*を意味します。デジタル変革は、従来型の企業にとって、顧客に価値を提供する方法を再定義し、業務とバリューチェーンをさらに迅速に実行できるように変更する機会をもたらします。企業は、主にビッグデータと分析、IoT、クラウド コンピューティングなどのデジタル テクノロジーを活用して、飛躍的に向上することができます。革新的な企業はそうして市場における圧倒的な優位性を獲得しています。

デジタル変革では、計画の初期段階からサイバーセキュリティを組み込むことが必要です。

たとえば、モバイル決済企業である Square では、製品設計の全段階にサイバーセキュリティの専門家を参加させています。高度なサイバーセキュリティは、製品開発の最後に「付け足す」ものではなく、必要不可欠な条件と考えられています。新しい社内プロセスを設計する場合も同様です。Square では、すべての業務において、サイバーセキュリティの専門家が経営幹部や設計者と積極的に連携しています。つまり、デジタル変革によって、サイバーセキュリティが初期段階から組み込まれた、新たなデジタル化プロセスを構築し、そのプロセスによって業務を改善することが可能になるのです。

調査対象の経営幹部の多くは、ビジネスのデジタル化を進めることで、ビジネス プロセスを再設計して俊敏化し、サイバーセキュリティを強化する機会が得られることを理解しています。実際に、経営幹部の 69 % はサイバーセキュリティに関する懸念のために、デジタル化を推進する意向が強くなったと答えています。

新しい市場セグメント

「セキュア デジタイザ」に学ぶ

シスコの調査に対する回答者の 4 分の 1 以上が、デジタル化を喫緊の課題と見なして取り組んでいます。デジタル化により*サイバーセキュリティを強化できる*と考えているためです。

シスコが「セキュア デジタイザ」と呼ぶこの市場セグメントは、サイバーセキュリティを重要な基盤とし、ビジネス モデルやオファリングをデジタル化することでビジネスの成長に力を注いでいます。そのため、このセグメントは、他の回答者よりサイバーセキュリティをプロアクティブに管理する傾向があります。また、このセグメントは、セキュリティがビジネスに与える影響を複数の分野にわたって測定する傾向が高くなっています。

セキュア デジタイザは、ビッグデータ/分析、クラウド、Internet of Things（IoT）という、3 つの主要なデジタル機能のセキュリティに、より大きな自信を持っています。この自信に基づいて、彼らはデジタル オファリングをさらに積極的に追求し、その結果として、イノベーションを推進し、市場投入までの時間を短縮しています。

セキュア デジタイザを見習うことで、企業はサイバーセキュリティの課題に取り組み、さらに自信を持ってイノベーションを進め、競争力を高めることができます。

「サイバーセキュリティをビジネス プロセスに始めから組み込んでおくことで、デジタル変革によってさらに高い安全性を実現できます」 ―サイバーセキュリティ コンサルティング企業の社長

また、回答者の一部（28 %）は、喫緊の課題としてデジタル化を推進しています。このグループは、デジタル変革によってサイバーセキュリティを改善できることを理解しています。これらの「セキュア デジタイザ」はデジタル変革者に対抗するのに最も有利な位置に着けており、他の従来型の企業をしのぐ力を持っています。なぜなら、セキュア デジタイザは、デジタル ビジネス モデルやデジタル オファリングを利用したビジネスの成長に最も熱心に取り組んでいるためです（図 11 および、前ページの「『セキュア デジタイザ』に学ぶ」を参照）。

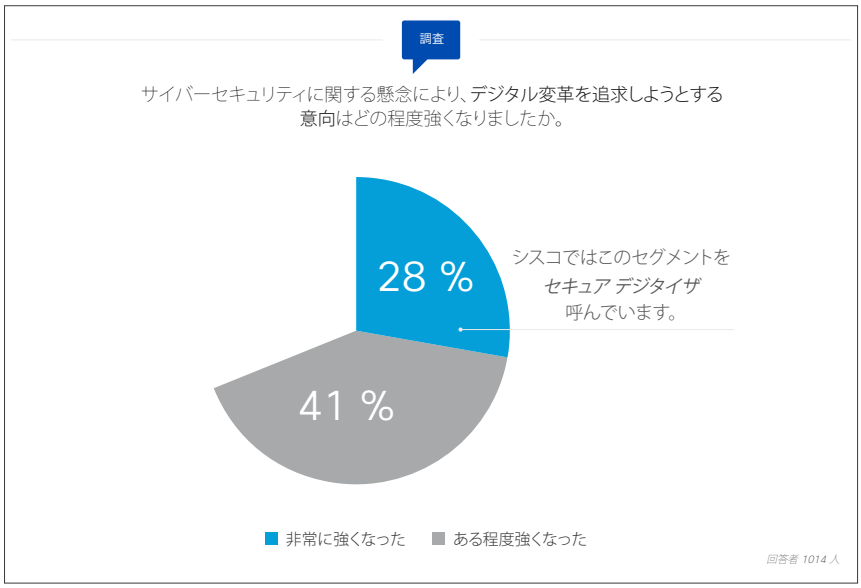

図 11
サイバーセキュリティの必要性が企業のデジタル変革を推進

出典：
シスコ、2016 年

すべてのセキュア デジタイザの *95 %* が、デジタル化は現在の自社の成長戦略において非常に重要だと述べており、89 % が、今後 2 年間に「さらに重要になる」と回答しています。一方、従来型の企業では、同じ質問に対して同様に回答したのは、それぞれ 58 % と 35 % でした。

セキュア デジタイザは、サイバーセキュリティの問題について、同業他社より力を入れて取り組んでおり、66 % がサイバーセキュリティの責任は自社にあるという説明に「非常にそう思う」と回答しています。一方、セキュア デジタイザ以外で「非常にそう思う」と答えたのは 31 % でした。この一因として、CEO や取締役などの主要なステークホルダーが、たとえ IT や技術的な職務を担当していない場合でも、サイバーセキュリティ問題について責任を担っていることが考えられます。

セキュア デジタイザは、自社の成長におけるデジタル ビジネス モデルやデジタル オファリングの果たす役割が大きいため、サイバーセキュリティに関する懸念がイノベーションを妨げ、成長を停滞させることを認識しているのです。そのため、こうした企業では、自社の変革を進めるにあたり、サイバーセキュリティを向上させるために積極的な手段を講じています。

その結果、これらの企業はデジタル化プロジェクトをさらに自信を持って進めることができます。そして、イノベーションを高速化して、デジタル経済価値におけるシェアをさらに増やすことができます。実際に、セキュア デジタイザの 62 % が、新しい製品やサービスの収益において同業他社に勝っていると回答しています。セキュア デジタイザ以外の企業では、同様に回答したのは 33 % のみです。

サイバーセキュリティをデジタル化戦略の基盤にする方法

常に革新が行われイノベーションが続く時代においては、成長の速度を速めたい企業にとって、サイバーセキュリティを活用して戦略面での俊敏性を高め、優れた運用効率を実現できる能力は、重要な差別化要因となり得ます。サイバーセキュリティに関する取り組みを進展させる方法については、セキュア デジタイザのベスト プラクティスが参考になります。

1. **サイバーセキュリティを成長の武器とする。**セキュア デジタイザは、サイバーセキュリティを自社の問題として考えており、80 % がサイバーセキュリティに「強い関心」を持っています（他の企業は 36 %）。83 % がサイバーセキュリティについての責任を「非常に大きく」負うことを想定し（他の企業は 39 %）、66 % が「リーダーとしてサイバーセキュリティを自分の責任と考えている」という説明に「強く同意」しています（他の企業は 31 %）。

   その結果、セキュア デジタイザはサイバーセキュリティに対してさらにプロアクティブに対応しています。たとえば、セキュア デジタイザの 66 % がサイバーセキュリティ専門の要員を採用しており（その他の企業では 42 %）、65 % がサイバーセキュリティの取り組みに対して予算を確保しています（その他の企業では 41 %）。また 65 % は自社の業務にサイバーセキュリティ ツールとベスト プラクティスを積極的に取り入れています（その他の企業では 47 %）（図 12 参照）。

さらに詳しい分析については、cs.co/cyberSD にアクセスしてください。

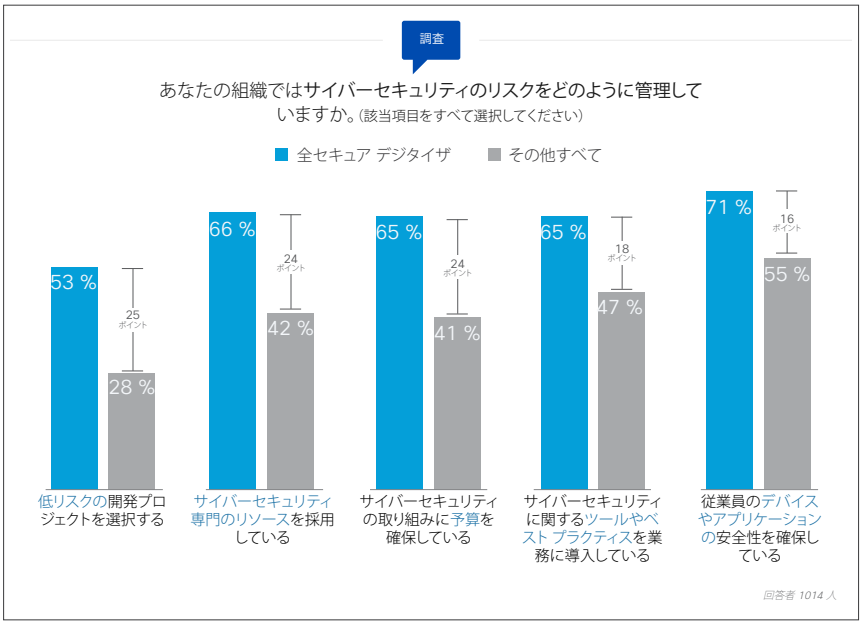

図 12
セキュア デジタイザはサイバーセキュリティをよりプロアクティブに管理

出典：
シスコ、2016 年

2. **低リスクのプロジェクトだけでなく、リスクよりも大きなチャンスが見込めるプロジェクトを選択することでリスクを軽減する。**セキュア デジタイザはより多くのリスクを取っていますが、コストを上回る成果を得ています。

幸いなことに、リスクよりも大きなチャンスが見込めるデジタル ユース ケースが多数あります。サイバーセキュリティ自体がその一例です。すでに価値が実証されている、成熟したデジタル機能には、リモート コラボレーション、Center of Excellence サポート機能、原油回収効率の向上（石油/ガス）、オムニチャネル機能とセールス/サービス転換（金融サービス）、予測ベースのメンテナンス分析（製造）などがあります。

Square のデータ セキュリティ ソリューションの責任者である Mike Dahn は、「私たちはサイバーセキュリティのリスクついて議論することが多いのですが、本当はセキュリティが実現できることについて話し合うべきなのです」と述べています。

「デバイス数の急増に伴い、潜在的なリスクと潜在的な機会の両方が存在するようになっています」と Mike は続けます。「私は、リスクは常に存在するものだと考えています。このことは念頭に置いておくべきです。けれども、私たちはセキュリティに対する考え方を、防御中心の古いモデルから、セキュリティによって実現できるものは何か、という新しいモデルへと変えていかなければなりません。これこそが、イノベーションの本質です。製品について考える際に、『これらの製品を守るには何が必要か』と考えるのではなく、『私たちを守るためにこの製品をどう使うべきか』と考えるのです」

セキュア デジタイザとその他の企業で、サイバーセキュリティの課題への対処に関する意識の差が最も大きかったのは、3 つの主要なデジタル テクノロジーの領域である、分析、IoT、クラウド コンピューティングについてでした。結果として、セキュア デジタイザは、自社のビジネス プロセスやオファリングにデジタル テクノロジーを導入することに、その他の企業よりはるかに自信を持っていることが明らかになりました（図 13 参照）。

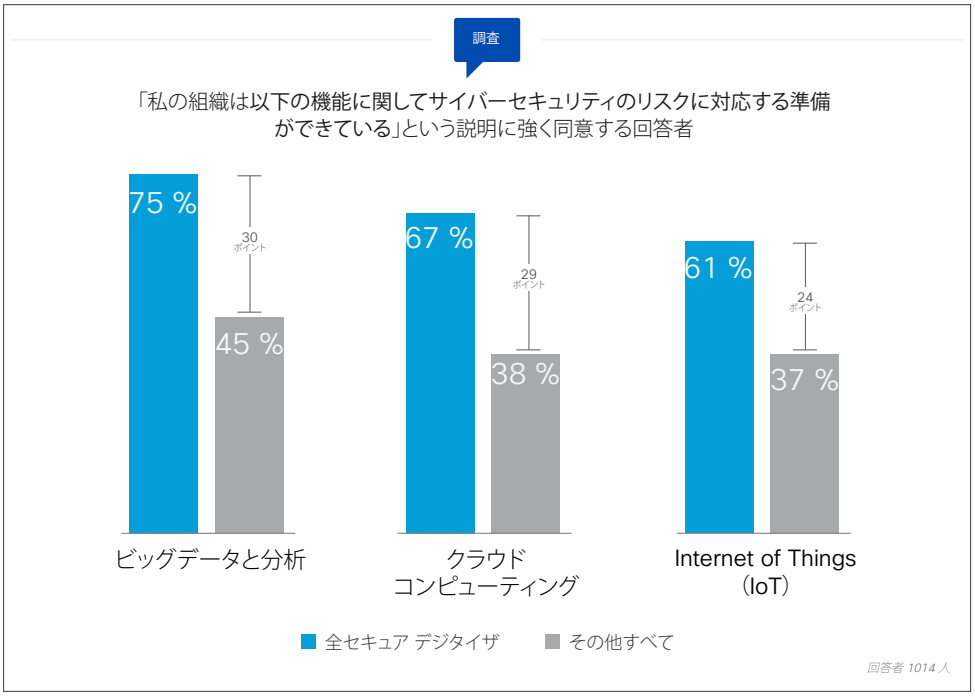

図 13
セキュア デジタイザは、自社のデジタル戦略におけるセキュリティに大きな自信をもっている

出典：
シスコ、2016 年

3. **サイバーセキュリティを基盤としてデジタル プロセスを再構築する。**サイバーセキュリティ自体が、デジタル ビジネス変革のエンジンです。サイバーセキュリティが進化する中、企業は安全性の低いテクノロジーと実現可能なビジネス プロセスを特定し、それらを最初からサイバーセキュリティが統合された新しいテクノロジーやプロセスで置き換える必要があります。この点の対応については、セキュア デジタイザの方が従来型の企業より大幅に優れています（図 14 参照）。dPrism の創業者兼 CEO の Adriaan Bouten は、次のように指摘しています。「サイバーセキュリティに最初から対応しておかなければ、後になって対応する際に「非常に大きな負担」となるでしょう」

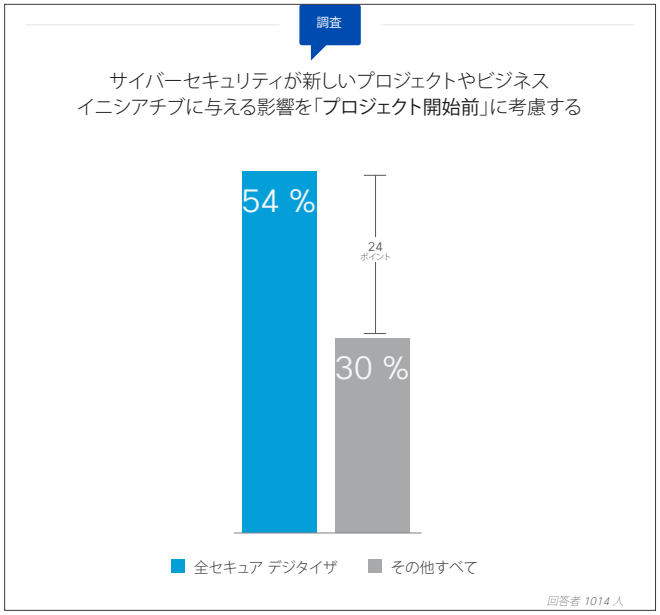

図 14
セキュア デジタイザはサイバーセキュリティが基本であることを理解している

出典：
シスコ、2016 年

4. **企業のあらゆるレベルにサイバーセキュリティの技術を組み込む。**企業による優れたサイバーセキュリティの実現を支援するプロアクティブな手段は、製品開発、リスク耐性、脅威分析、応答性など、ビジネス全体を向上させるのにも役立ちます。これはつまり、サイバーセキュリティの専門家を企業内のさまざまな部門に配置すべきだということを示しています。また、企業の戦略的な計画立案や経営に別の側面があることを知らしめるために、サイバー脅威を予測する心構えが必要だということも示しています。

   CFO の Robert Simmons は、「取締役から清掃スタッフまで、文字通り関与するすべての人が当事者なのです」と説明します。「これはもはや、IT の領域ではありません。この状況を企業が認識するのが早ければ早いほど、企業はこうしたプログラムを実施しやすくなり、今日のデジタル化時代に対応することができるでしょう」

5. **有効性を測定する。**セキュア デジタイザの 75 % は、それぞれの職能組織におけるサイバーセキュリティ戦略の有効性を評価する詳細なプロセスを設けています。一方、その他の企業では 21 % に留まります。こうしたプロセスでは、デジタル資産への影響や、サイバーセキュリティへの適切な投資のレベルなど、多様な情報が評価されます（次ページの図 15 参照）。

   サイバーセキュリティ保護の効果を測定することで、企業の業務や戦略的資産などへの脅威に対する経営幹部の認識を高めることができます。これは、保護を強化するためにさらなる投資を引き出すための根拠として使用できます。

   セキュア デジタイザの 65 % が、「非常に効率的」にビジネス上の利益を測定できると述べています。他の企業の場合、これは 30 % にとどまります。翌年のサイバーセキュリティへの支出を増加させると考えている数が、セキュア デジタイザの方が他の企業の 2 倍を超えているのはこのためです（セキュア デジタイザが 64 % であるのに対して、他の企業は 31 %）。

さらに詳しい分析については、cs.co/cyberMD2 にアクセスしてください。

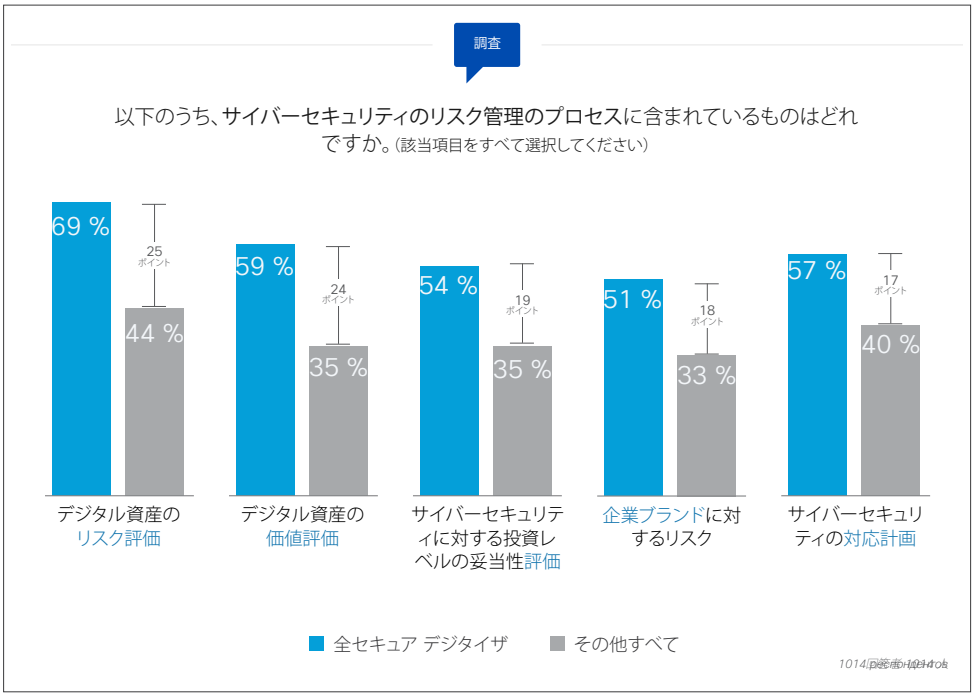

図 15
セキュア デジタイザは、自社のデジタル戦略におけるセキュリティに大きな自信をもっている

出典:
シスコ、2016 年

投資金額を決めるには、企業は自社が保護する対象の価値を測定しなければなりません。

Information Security Forum のマネージング ディレクターである Steve Durbin は、「これは、守るべき情報の保護に関連したリスクを理解するだけでなく、その情報が不適切な相手に渡った場合を想定して、組織における情報の価値を理解するということでもあります」と説明しています。「まず、次のような観点から考えてみることが必要です。つまり、『私たちがある時点でなんらかの情報を失う可能性は非常に大きいが、失った情報にはどれくらいの価値があるだろうか。一方、現在、社外から情報にアクセスできないようにすることはどの程度難しいだろうか』ということです。次に、その情報を保護するのに必要な自社のリソースやコストに換算してみます」

有効な測定を行うには、サイバーセキュリティのメリット/デメリットの両方を定量化する手法が必要です。目標を設定する場合、新しいデジタルビジネス戦略による変化がもたらす望ましいパフォーマンスと、意図しない結果の双方を考慮する必要がありますが、多くの企業が実施できていません。[21]

デジタル革命が進むこの時代では、デジタル製品やデジタル サービスは成長に欠かせないだけでなく、生き残っていく上でも必要なものです。しかし実際には、サイバーセキュリティの実践レベルが平均にも満たない多くの企業が厳しい状況に追い込まれています。勝ち抜くのに必要な速度や信頼性を持ってイノベーションを進めることができず、競争のプレッシャーにさらされ、サイバーセキュリティを正しく実践せずに、実験的な導入を行っていることも原因です。レガシーの IT システムに縛られることなく、成長のイネーブラとしてサイバーセキュリティに投資しやすい、俊敏な革新的企業が、常に先行することになります。

セキュア デジタイザの後を追うことで、デジタル イノベーションを果敢に追求し、デジタル時代において大きく成長することができます。

「新しい取り組みを開始する際には、サイバーセキュリティをビジネス ケースやプロジェクト管理プロセスに含めます。あらゆる手段を講じる必要があります。データセキュリティのマイルストーンを設定し、コンプライアンスを遵守できるように人材を教育します。あらゆる人の関与が必要なのです」

—フォーチュン 100 に選ばれた銀行の元人事部担当副社長

1. 中規模から大規模の企業がサイバーセキュリティをどのようにビジネスに組み込んでいるかを理解するために、2015 年 10 月に 1014 名のディレクター、VP、経営幹部に対してオンライン調査を実施しました。回答者の 3 分の 1（38 %）は財務担当者で、サイバーセキュリティへの投資に影響力を持つ人物です。残りの 62 % は、さまざまな基幹業務の担当者です。回答者は、サイバーセキュリティ戦略や企業の慣習についてかなりあるいは非常に詳しい情報を持っていますが、情報技術部門や情報セキュリティ部門の所属ではありません。調査対象国は、オーストラリア、ブラジル、カナダ、中国、フランス、ドイツ、インド、イギリス、アメリカ、および日本です。さらに、GLG エキスパート ネットワークから抽出した 11 名のエキスパートに対し、電話による 1 時間の定性調査も実施しました。対象者はいずれも、既成企業において広範なサイバーセキュリティの経験を持つ現職のシニア マネージャか、その任にあった人物とし、財務と基幹業務の両方の担当者を対象としました。このうち 2 名はサイバーセキュリティ コンサルティングのエキスパートでした。
2. デジタル経済価値は、2 つの要素から構成されます。すなわち、1）デジタル化への投資とデジタル イノベーションから生じる、完全に新しい価値の源泉と、2）企業や業界におけるデジタル機能の活用能力（またはその能力の欠如）に応じて、企業間や業界内で発生する価値のシフト（つまり、「敗者」から「勝者」への価値の移動）の 2 つです。
3. 「オファリング」という用語は、企業が提供する製品やサービスを意味します。ここで言うオファリングは、製品やサービスの一般的な定義や従来のビジネス モデルとは完全に一致しない場合があります。たとえば、デジタル革命を進める企業は、独自の消費モデルによるオファリングを提供しています。そのビジネス モデルでは、オファリング自体は無料であり、関連するアクティビティにより収益を得るという方式をとっています。デジタル革命を進める企業が創出している価値の源泉や、そうした価値の創出に使用しているビジネス モデルに関する詳細な調査内容については、IMD とシスコの取り組みである 2015 年 11 月の Global Center for Digital Business Transformation（DBT Center）の『New Paths to Customer Value: Disruptive Business Models in the Digital Vortex（顧客価値への新たな道：デジタル化の渦における革新的なビジネス モデル）』（英語）を参照してください。
4. 新興企業やその他の俊敏なデジタル革命企業とは対照的に、「従来型の企業」、または「既存企業」は多数の従業員を抱え、伝統的なバリュー チェーンを保有し、固有の生産的資産を新興企業より多く保有している傾向があります。シスコの調査は従来型の企業のみに焦点を置いて実施され、対象となる企業の従業員数は 500 名以上です。83 % は従業員が 1,000 名以上の企業であり、その内 19 % は従業員が 10,000 名以上でした。
5. 「デジタル」という言葉は、ユビキタスな高速接続によって実現されるテクノロジーに関する複数のイノベーションを集合的に表現しています。こうしたテクノロジーに関するイノベーションには、ビッグデータと分析、クラウド コンピューティング、Internet of Things（IoT）、モビリティ、ソーシャル メディア、機械学習などが含まれます。「デジタル」の定義と関連する用語については、DBT Center 作成の『Defining the Digital Vortex（デジタル化の渦の定義）』（英語）を参照しています。
6. シスコは、「デジタル化」を「デジタル テクノロジーで使用/共有が可能な情報を生成、または変換すること」と定義しています。デジタル化された情報は、デジタル ビジネス プロセスとビジネス モデルの基盤です。DBT Center が 2015 年 12 月に発表した『Defining the Digital Vortex（デジタル化の渦の定義）』を参照してください。
7. 『The Digital Vortex: How Digital Disruption Is Redefining Industries（デジタル化の渦：デジタル革命は産業をいかに再定義するか）』（英語）、Global Center for Digital Business Transformation、2015 年 6 月
8. 『Disruptor and Disrupted: Strategy in the Digital Vortex（革新者と被革新者：デジタル化の渦における戦略）』（英語）Global Center for Digital Business Transformation、2015 年 11 月
9. 2014 年、10 億件を超えるレコードが被害を受けました。対前年比 54 % 増であり、これは小売業における大規模な侵害が主な原因です。2015 年上半期の漏洩の件数は 2014 年上半期より 10 % 増えていますが、被害を受けたレコード自体の件数は 41 % 減少して 2 億 4 千 6 百万レコードとなっています。Gemalto、2015 年 9 月および ZDNet、2016 年 1 月
10. 『Data and Dollars: The Role of the CFO in Cybersecurity（データと収益：サイバーセキュリティにおける CFO の役割）』（英語）Connected Futures Information Security Forum マネージング ディレクター Steve Durbin
11. 『Fast IT: Accelerating Innovation in the Internet of Everything（Fast IT：Internet of Everything 時代におけるイノベーションの推進）』（英語）シスコ、2014 年
12. 『2015 Cost of Data Breach Study: Global Analysis（2015 年データ漏洩のコストに関する調査：グローバル分析）』（英語）Ponemon Institute、2015 年 5 月
13. 『Businesses Braced for Bout of Regulation on Cyber Security（サイバーセキュリティに関する大量の規制に縛られるビジネス）』（英語）Financial Times、および『New York Bank Regulator Details Cybersecurity Regulations（ニューヨークの銀行の取締官が語るサイバーセキュリティに関する規制）』（英語）The Wall Street Journal、2015 年 11 月
14. 『The Digital Vortex: How Digital Disruption Is Redefining Industries（デジタル化の渦：デジタル革命は産業をいかに再定義するか）』（英語）、Global Center for Digital Business Transformation、2015 年 6 月
15. 別の調査では、「組織がイノベーションを進めることを妨げている理由は何ですか」という質問に対して、回答者の 28 % が「イノベーションがセキュリティ リスクを増加すると思うから」と答えています。2015 年 4 月の Ponemon Institute LLC および Lockheed Martin による『Risk & Innovation in Cybersecurity Investments（サイバーセキュリティへの投資におけるリスクとイノベーション』（英語）を参照してください。
16. この結果は、Ping Identity によって実施された最近の調査（『Secure Access for the Digital Enterprise（デジタル企業に対する安全なアクセス）』（英語）Ping Identity、2015 年）とも一致しています。Ping Identity の調査では、企業の 51 % がデジタル テクノロジーの導入における最大の課題はセキュリティだと回答し、78 % がセキュリティに関する懸念が原因でクラウドへの移行が遅れていると回答しています。

謝辞

本書の著者一同、執筆にご協力いただいた以下の方々に心よりお礼を申し上げます。Debbie Abbott、Caroline Ahlquist、Sara Aiello、Kevin Bandy、Ruba Borno、Kristine Briggs、John Choi、Lynne Cox、David Goeckeler、Dan Gould、Gene Hall、Amy Henderson、Lisa Lahde、Rob Lothman、James Macaulay、Melissa Mines、James Mobley、Bryan Palma、Robert Pepper、Caroline Robertson、John Stewart、Ann Swenson、Greg Thomas、Virgil Vidal、Michael Zielenziger、Elisabeth Zornes。

17. 『Seven Ways CEOs Can Apply Digital Business for Competitive Advantage（CEO がデジタル ビジネスを導入して競争優位を獲得する 7 つの方法）』（英語）Gartner Hung LeHong、2015 年 6 月
18. Gartner は、2015 年の全世界における IT 支出は減少したと述べています。
19. シスコの調査では、「サイバーセキュリティの管理とポリシーに関する自社の最大の課題は何か」という質問に対して、回答者の 32 % が「ビジネスが変化するペースに合わせてサイバーセキュリティ ポリシーを更新することができない」を選び、27 % が「サイバーセキュリティの効果を判断するための適切な指標がない」を選択しています。また、26 % が「サイバーセキュリティに対する投資が不十分」を選択し、24 % が「サイバーセキュリティ ポリシーの適用が非効率的」を選択しています。サイバーセキュリティに対する投資を全般的に増やしても、すべての問題が解決するわけではありません。価値を最大化するためには、企業は、成功の指標が定義されている取り組みや、効率的に管理されている取り組みに対して優先的に投資を行う必要があります。
20. セキュア デジタイザとは、シスコがこの調査で発見した新たな市場セグメントです。市場のセグメント化では、広範なターゲット市場を、共通のニーズや関心、行動、優先順位を持つ（または持つと思われる）ビジネス区分に細分化します。
21. 『Using Risk-Adjusted Value Management to Close the Strategy Gap and Gain Competitive Advantage（リスクに応じた価値の管理により、戦略上のギャップを埋め、競争優位を獲得する）』（英語）Gartner Michael Smith および Paul E. Proctor、2015 年 12 月

C45-BCI0416-00　04/16