

スモールビジネスにおける セキュリティの重要性

スモールビジネスのサイバーセキュリティにまつわる **10** の神話を覆す



目次

現在のサイバーセキュリティで、組織は想定通りに守られていますか?	3
10の神話の中身を探る	5
スモールビジネスと大規模企業のセキュリティ体制の対比	5
神話その1: 世間の厳しい視線にさらされるのは、業種を問わず大規模な組織に限られる	5
神話その2: 大規模企業は攻撃によるダウンタイムが短く、復旧も早い	7
神話その3: スモールビジネスにはセキュリティに専従できる人員が不足している	8
神話その4: 大規模企業は新しいインフラストラクチャの導入率が高い	9
神話その5: スモールビジネスは大規模企業とは異なるサイバーセキュリティの脅威に直面している	10
神話その6: スモールビジネスは予防手段としての脅威検出を実施していない	12
神話その7: スモールビジネスはインシデント対応計画を訓練や演習でテストしていない	13
神話その8: どのような理由であれ、スモールビジネスのリーダー層はセキュリティとデータプライバシーを重視していない	14
神話その9: 小規模の組織は、脆弱性に対処するパッチを定期的に適用していない	17
神話その10: スモールビジネスは自社のセキュリティ体制の有効性を測定できない	18
セキュリティ最適化の機会を捉える	19
サイバーセキュリティ疲れ	19
従業員によるサイバーセキュリティ啓発プログラムの受け入れ	19
ダウンタイムの短縮	21
ベンダーの複雑さ	22
今後の取り組みを着実に進めるための関連資料	23
リモートワーク環境の保護	24
シスコのエキスパートについて	25
シスコ サイバーセキュリティ レポート シリーズの概要	25

現在のサイバーセキュリティで、組織は想定通りに守られていますか？

スモールビジネスの企業（SMB）の経営者や従業員の皆様は、これまでに大きな課題の克服に携わってきたはずです。事業資金の調達、人材採用のタイミングの判断から、運用コストの管理、規模拡大戦略の立案に至るまで、心が奮い立ち、有意義で、自らの決定が結果に結びつくものではありますが、厳しい局面の連続です。

パンデミックや景気後退の最中にあっても事業を継続するなど、前例のない事態に直面した場合、どのように乗り切ればよいのでしょうか。セキュリティを確保するには、何に重点を置くべきでしょうか。人員を削減して事業を運営する場合、サイバー攻撃から組織をどのように保護するのでしょうか。

このような場面で生きるのが、起業家としての本能です。危機的状況では、新しい働き方に適応していく過程で、必然的に今までにないアイデアが生まれます。つまり、あらゆる難局を乗り越えて、生産性と競争力を維持するための方策が生み出されるのです。

サイバーセキュリティは、検討すべき緊急の課題が他にも数多く存在する昨今の状況で、大きな役割を担うものなのでしょうか。

間違いなく大きな役割を担います。中堅中小企業が生き残りを図るだけでなく、業績を伸ばし、成功を加速する上で、サイバーセキュリティはどのような形で重要な役割を果たせるのでしょうか。今回のレポートでは、この点についての分析情報をお届けします。その手立てとして、広く流布している神話の誤りをデータで検証していきます。それらの神話が、スモールビジネスのセキュリティに関する世間の認識を誤った方向へと導いているのです。

スモールビジネスは、サイバーセキュリティをどの程度の優先事項と捉えているのでしょうか。この点に関して、セキュリティ業界は時に厳しい態度をとっていました。セキュリティベンダーは、スモールビジネスがセキュリティに真摯に取り組んでいないと決め付けて近づき、セキュリティについて説明し始めている（IT 専門家の目線で説明している）ように映ります。

このレポートは、スモールビジネス（ここでは従業員数 250 ~ 499 人の組織としています）約 500 社の調査に基づくものです。スモールビジネスがセキュリティを非常に重視しているだけでなく、セキュリティに対する革新的で起業家精神にあふれるスモールビジネスのアプローチが、実を結びつつあることも明らかにします。スモールビジネスによるサイバーセキュリティ リソースの使用状況をめぐって、いくつかの神話を打ち破るべき時期が訪れたのです。

年次の [CISO ベンチマーク調査](#)の結果と中堅中小企業との対話から得られた結果を活かして、神話の誤りを検証します。たとえば、プロアクティブな脅威の検出に特化した部門を設置しているスモールビジネスの数や、スモールビジネスが直面しているサイバー攻撃の種類といったトピックについてです。

言い換えると、スモールビジネスのサイバーセキュリティを左右する重要な要素を詳細に検証していきます。たとえば、老朽化したインフラストラクチャがセキュリティ侵害に与える影響や、セキュリティ侵害の持続期間について把握しました。また、採用するベンダーの数が多いほど、最も深刻なセキュリティ侵害に起因するダウンタイムが長くなることもわかりました。さらに、スモールビジネスに最も影響力のある戦略を探るとともに、データ漏洩の被害を受けたスモールビジネスの復旧のスピードは、これまで業界で考えられていた水準よりも速いことを実証するデータをご紹介します。

小規模企業であることに伴うすべての重圧に十分に対処できる場合も、外的な圧力の影響を受ける可能性があることは、今となっては明らかでしょう。従業員の一部または全員がいつでもリモートワークに対応できるよう、態勢を整えることを余儀なくされ得るのです。独立系のサイバーセキュリティ アナリストであり、ブロガーでもある [Graham Cluley](#) 氏は、最近のニュースレターで「自宅で仕事をしていても、ハッカーから狙われなくなるわけではありません」と述べています。今までとは違う働き方に適応しなければならないかもしれません。事態が深刻な場合は、優先順位を付けることが不可欠です。

このレポートの目的は、どの戦略が有効であるかを浮き彫りにすることにあります。貴社と従業員が今後どのようにセキュリティを管理するか、またサイバーセキュリティがどのように貴社の成功を促進する力となるかについての意思決定に役立つことを願っています。

「当社において、セキュリティは重要な役割を担っています。米国内の 3 つの信用組合について、当社は合同のコールセンターに加え、バックエンド機能の運営にも携わっていますが、セキュリティは、ビジネスの主要な側面を統合して運用効率を高めるのに役立ちます」

Kevin Hatch 氏 (Open Technology Solutions 社、
ネットワークエンジニア)

10の神話の中身を を探る

スモールビジネスと大規模企業のセキュリティ体制の対比

スモールビジネスのセキュリティ体制について巷で語られている神話の真偽を明らかにするために、スモールビジネス（従業員数 250 ~ 499 人）と大規模企業（従業員数 500 人以上）を対象に、さまざまなサイバーセキュリティ機能に関する調査回答を比較しました。

調査データで明らかになった事実から、いくつかの神話が誤りであることが判明しました。ここでは、これらの神話の実態を調査し、誤りの証明となるデータを提示します。スモールビジネスは、誰もが認識しているよりも優れたセキュリティ環境を保つことができます。

注：

1. 今回の調査では、従業員数が 250 ~ 499 人の企業を中堅中小企業（SMB）としました。調査の結果は、従業員数が 250 人未満の組織では大幅に異なる可能性があります。
2. 百分率の数値はいずれも四捨五入したものです。調査の質問項目に対する「わからない」という少数の回答は、割愛しています。したがって、掲載しているグラフの数値の合計は、必ずしも 100% になりません。調査データの出典は、[シスコの 2020 年版 CISO ベンチマーク調査](#)です。

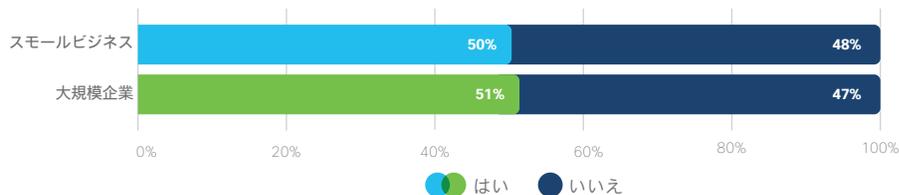
神話その 1：世間の厳しい視線にさらされるのは、業種を問わず大規模な組織に限られる

よく語られる神話の 1 つに、マスメディアが取り上げたいのは、市場を席巻する巨大企業または政府機関のデータ漏洩だけだというものがあります。これでは、スモールビジネスの一部で「たとえサイバー攻撃を受けたとしても、世間の厳しい視線にさらされることはない」という誤認識が生じかねません。

誤り： 昨年の調査によれば、小規模企業に対して世間が向ける視線の厳しさは、大規模企業に匹敵するものでした。

図 1 からは、世間の厳しい視線にさらされるかどうかに関して、スモールビジネスと大規模企業に差があることを示す実質的な証拠はないことがわかります。

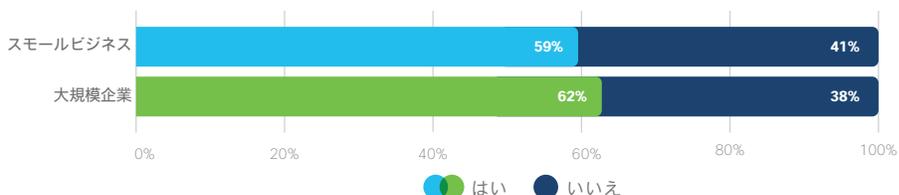
図 1. セキュリティ侵害の発生に伴い、世間の厳しい反応に対処せざるを得なくなったことはありますか？（スモールビジネス 481 社、従業員数 500 人以上の企業 2,319 社）



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

2 番目に、スモールビジネスの 59% は、前年に被った最も深刻なデータ漏洩を自主的に公表しています（大規模企業は 62%）。これは、小規模企業であっても、顧客とパートナーに対するコミットメントを真摯に受け止めていることを示唆しています。

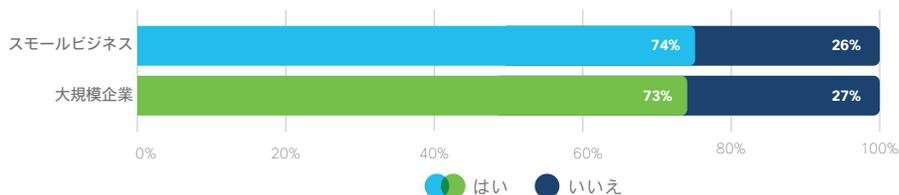
図 2. 世間の厳しい視線を受けながらの対応が必要となった、前年の最も深刻なセキュリティ侵害が明るみに出たのは、貴社の自主的な公表によるものでしたか？（スモールビジネス 241 社、従業員数 500 人以上の企業 1,190 社）



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

3 番目に、スモールビジネスは、顧客データの取り扱いについて顧客から問い合わせを受けない割合よりも、受ける割合のほうが圧倒的に多くなっています。スモールビジネスの 74% が、顧客または見込み客からそのような問い合わせを受けたと回答しています（大規模企業の 73% とほぼ同水準）。これは、顧客が提供先企業の種別にかかわらず個人情報の保護を重視していることや、個人情報の提供先企業への信頼という要素が明らかに重要であること示しています。

図 3. 顧客（または見込み客）から、データのプライバシーと個人情報の取り扱いについて問い合わせを受けることがありますか？（スモールビジネス 432 社、従業員数 500 人以上の企業 2,117 社）



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

スモールビジネスがこのような問い合わせを受ける理由には、諸規制とベンダー（納入業者）のリスク管理が上流から下流に向かって進むことがあります。出発点は大規模企業です。大規模企業は、自社のベンダーである中規模企業を監査します。何年か後、

中規模企業は、自社のベンダーである小規模企業を監査することになります。スモールビジネスは、セキュリティ侵害やデータプライバシーの問題が発生しているため、問い合わせと無縁ではられません。大規模企業と同様に責任を負うことになります。

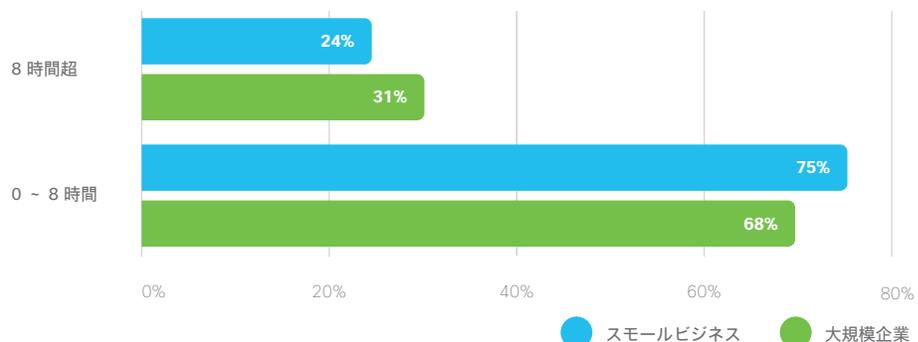
神話その 2：大規模企業は攻撃によるダウンタイムが短く、復旧も早い

神話のとおりであるとする、スモールビジネスがサイバー攻撃を受けて一定のダウンタイム（営業時間の喪失）が生じた際、大規模企業ほど迅速にビジネスを再開できるリソースがないことになります。

誤り：当社のデータによると、スモールビジネスと大規模企業のダウンタイムにはほとんど差がありません。

これらの調査結果の一部を要約すると、スモールビジネスの 24% で、最も深刻なセキュリティ侵害に起因して、昨年 8 時間を超えるダウンタイムが生じていました。これは、大規模企業の 31% をわずかに下回る水準です。

図 4. 前年中の最も深刻なセキュリティ侵害によってシステムが稼働停止となった時間は、どの程度でしょうか？（スモールビジネス 388 社、従業員数 500 人以上の企業 1,877 社）



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

また、これらの数値を 2018 年発行のシスコ スモールビジネス レポート「Small and Mighty」と比較したところ、小規模企業に関しては、この 2 年間で顕著な改善が見られます。2 年前には、最も深刻なセキュリティ侵害を受けた後のダウンタイムが 8 時間を超えたスモールビジネスは 40% にのぼっていました。

ここで認識しておく必要があるのは、企業の規模にかかわらず、深刻なセキュリティ侵害が発生すると、大きな混乱が生じる可能性があるということです。問題は、どのような企業でダウンタイムが長引くかではなく、スモールビジネスがどのような策を講じることができるかにあります。その目的は、自社のリソースが、能力の限界を超えて対処を強いられる事態に至らないようにすることです。このような状況で、早期の警告と迅速な復旧によってダウンタイムを最小限に抑え、不測の事態にあってもビジネスを継続させるための強化策になり得るのが、[自動化](#)です。[2020 年版の CISO ベンチマーク レポート](#)によると、組織の規模を問わず回答者の大多数（77%）が、今後 1 年間にセキュリティエコシステムにおけるレスポンスの簡素化と迅速化のために自動化の拡大を計画しています。

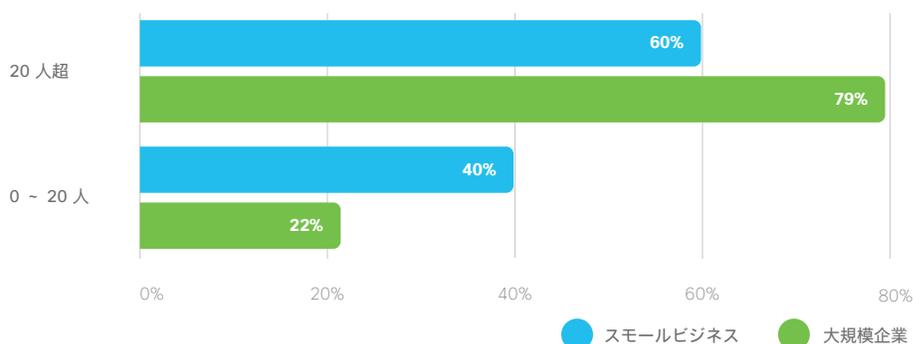
神話その 3：スモールビジネスにはセキュリティに専従できる人員が不足している

スモールビジネスでは、部署にかかわらず、誰もが必要不可欠な職務に従事しているため、サイバーセキュリティは誰かの職務の 1 つの側面にすぎない、という固定観念が世間に存在します。またその担当者は、データセンターの管理や新しいハードウェアの評価など、IT 管理のその他の側面のバランスを取ることも想定されています。つまり、スモールビジネスにはサイバーセキュリティ専従リソースがほとんどない、という神話がまかり通っているのです。

誤り：この神話が当を得ている場合もあるものの、スモールビジネスの圧倒的多数は、サイバーセキュリティ専従の人員を配置していると回答しています。実際、セキュリティ専従の人員がいないと回答したスモールビジネスは 1% 未満でした。さらに驚くべきことに、スモールビジネスの 60% は、セキュリティ専従の人員が 20 人を超えていると回答しています（ただし、専任スタッフによる関与の度合いと、マネージドセキュリティ サービス プロバイダー（MSSP）へのアウトソーシングの有無については、質問項目に明記していません）。

このデータを大規模企業と比較してみます。セキュリティ専従の人員が 20 人を超えていると回答した大規模企業の割合は、非常に高くなっています（79%）。これは誰もが予想し得る結果でしょう。

図 5. セキュリティに専従している従業員は何人いますか？（スモールビジネス 481 社、従業員数 500 人以上の企業 2,319 社）



これらの数値から、スモールビジネスが大方の予想を上回る規模のセキュリティ専従リソースを配置していることがわかります。スモールビジネスでは、サイバーセキュリティ要員の不足はもはや問題となっていないのでしょうか。

そう結論付けるのは、やや早計です。

スモールビジネスによれば、トレーニングを受けた人材の不足は、実際には 3 番目に大きな課題となっています。最大の課題は予算上の制約であり、2 番目はレガシーシステムとの互換性でした。トレーニングを受けた人材の不足と同数で 3 番目に位置しているのは、互いに競合する優先順位です。

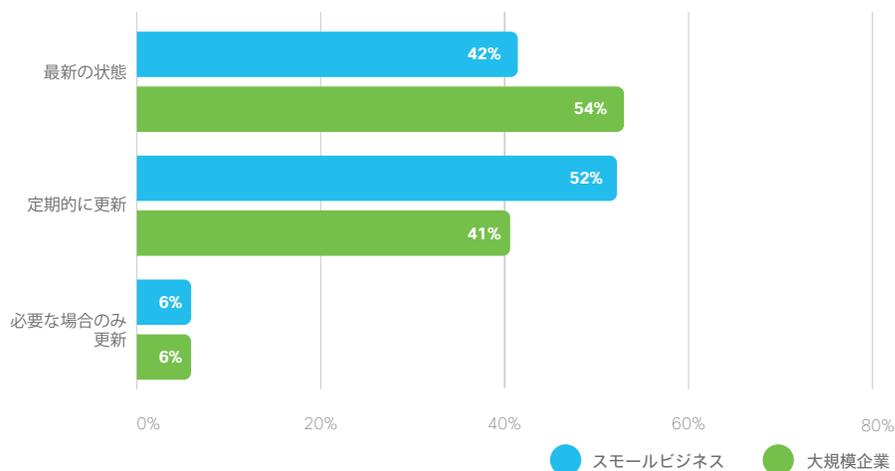
この点は、小規模企業がサイバーセキュリティ上の課題に直面していることの表れであると考えられます。小規模企業は、自社が標的となっていて、攻撃がますます巧妙になっていることを認識しています。この情勢への対策として、小規模企業は、可能な範囲で最善を尽くしています。スモールビジネスの場合、これはしかるべき人材に投資することを意味します。

神話その 4：大規模企業は新しいインフラストラクチャの導入率が高い

消費者が最新のスマートフォンに買い換える頻度を考えてみると、大規模企業は、セキュリティ インフラストラクチャの個々の要素を定期的に置き換える資金的余裕があるようにも映ります。一方、定期的な投資が年間の IT 予算に及ぼす影響が大きくなり得る、小規模企業の場合はどうでしょうか。

部分的に正しい：自社のインフラストラクチャについて、また重要なセキュリティ基盤への投資と置き換えに関する戦略について問われた際、ほぼすべてのスモールビジネスは、インフラストラクチャを最新の状態に維持することに努めていると回答しています。

図 6. 貴社のセキュリティ インフラストラクチャの更新状況を教えてください。（スモールビジネス 481 社、従業員数 500 人以上の企業 2,319 社）



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

スモールビジネスのインフラストラクチャは、大規模企業のものほど最新の状態でないことは事実です（大規模企業の 54% が「最新の状態である」と回答しているのに対して、スモールビジネスの場合は 42%）。ただし、合計で 94% のスモールビジネスは、定期的あるいは頻りにインフラストラクチャを更新していると回答しています。したがって、圧倒的多数のスモールビジネスは、古い設備が陳腐化してセキュリティを維持できなくなる前に更新していることは間違いありません。

スモールビジネスの場合、新たに登場する画期的なセキュリティ製品を追い求めることよりも、既存の環境を最大限に活用することが鍵になります。シスコのスモールビジネスのお客様は、多くの場合、従来の発想の枠組みを打ち破ることによってセキュリティを強化しています。

「当社は小規模の事業者です。したがって、可能な限り少数のシステムから可能な限り多くの情報を獲得して、効率を最大限に高めることが欠かせません。クラウドベースのセキュリティソリューションである Cisco AMP for Endpoints は、インフラストラクチャ全体の運用で実績を挙げていて、不可欠なシステムとなっています。資産の保護に不可欠だけでなく、機器情報、ユーザ環境、レポートに即座にアクセスすることもできるので、ヘルプデスクによるトラブルシューティングで役立っています。結果として、ソフトウェアシステムを別途に導入する必要がなくなりました。現在の形で運用していれば、学びに基づいて絶えず調整できます」

Alan Zaccario 氏 (New Castle Hotels and Resorts 社、IT およびサイバーセキュリティ担当副社長)

神話 5 : スモールビジネスは大規模企業とは異なるサイバーセキュリティの脅威に直面している

サイバー犯罪者の目的は最大限の利益を得ることなので、大規模企業に対して、最も探知されにくく危険な戦術を駆使するのでしょうか。

部分的に正しい : スモールビジネスと大規模企業から、前年 1 年間に受けたと報告のあったサイバー攻撃の種類とともに、攻撃によって生じたダウンタイム (営業時間の喪失) を比較しました。従業員数に基づいて、組織を 4 つのカテゴリに分けて比較し、ダウンタイムが 24 時間を超える可能性の高いイベントをランク付けしました。

図 7. 従業員数と、前年 1 年間の最も深刻なセキュリティ侵害に起因するダウンタイム (1 時間単位) との相関関係および原因となった攻撃の種類 (従業員数 250 ~ 499 人の企業が 388 社、500 ~ 999 人が 746 社、1,000 ~ 9,999 人が 863 社、10,000 人以上が 268 社)



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

どの脅威が最も深刻な被害をもたらしているのかという点で、結果は興味深いものとなっています。結果から見てとれるのは、ランサムウェアの攻撃が無差別であることです。スモールビジネスと大規模企業の双方で、ランサムウェアは 24 時間を超えるシステムダウンタイムにつながりかねない最大の脅威でした。

DDoS 攻撃は、小規模企業に最大の被害をもたらすことはほとんどない一方、従業員数が 10,000 人を超える企業に関しては、ダウンタイムの点で 3 番目に被害の大きい攻撃となっています。これに対して、小規模企業からはフィッシングが大きな問題として挙げられているものの、大規模企業では影響が十分に抑えられています。

ワイパー型マルウェアを拡散する攻撃者の目的は、ただ 1 つしかありません。システムやデータを破壊することか、混乱に陥れることです。スモールビジネスと従業員数 10,000 人を超える企業のどちらについても、ワイパー型マルウェアは昨年 1 年間に 17 ~ 24 時間のダウンタイムを引き起こしていました。身代金目的でデータを抱え込むマルウェア (ランサムウェア) とは異なり、攻撃にワイパーを選択する攻撃者は、金銭が直接の動機となっているわけではありません。この種の攻撃はデータを復元できる見込みがないため、多くの場合、企業にとって最悪の攻撃です。

クレデンシャルの窃取も、スモールビジネスにとっては重大な問題であると考えられます。昨年は、平均で 17 ~ 24 時間のダウンタイムを引き起こしています。

また、攻撃者によっては、特定の規模の企業、業種、または地域に標的を絞っていることも考慮する必要があります。したがって、(前掲の図に示したとおり) 手口が似通っているととしても、攻撃者そのものは異なります。

神話その 6：スモールビジネスは予防手段としての脅威検出を実施していない

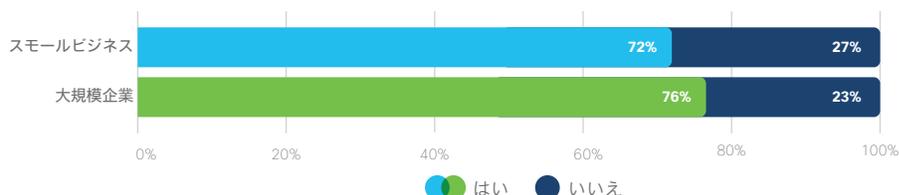
脅威検出は、予防的な手段となるセキュリティ対策です。環境に潜んでいながら、アラートが発行されていない攻撃者を発見し、排除することを目的としています。これは、悪意を持つ可能性のあるアクティビティが検出された後、発行されるアラートに基づいて調査を実施し、対処するという従来の手法とは対照的です。

脅威検出という概念には、その響きと複雑さから、小規模企業が採用できるものではなく、謎めいた犯行現場の捜査を進めるかのような印象があります。スモールビジネスはアラートの調査で手一杯となっていて、その他の脅威の検出に時間を割く余裕はないのでしょうか。

誤り：シスコの調査データによると、スモールビジネスの 72% は脅威検出に専従する人員を配置しています。これは、脅威検出部門を設置している大規模企業の割合にも近い水準です。

スモールビジネスはリソースが限られていることから、人員の成熟度については、大規模企業とは異なる可能性があります。しかし、シスコのデータでは、スモールビジネスはサイバーセキュリティの価値を認識していて、サイバーセキュリティに関する予防的なアプローチの採用を進めていることが示唆されています。

図 8. 脅威検出に専従する部門またはチームを組織内に設置していますか？（スモールビジネス 481 社、従業員数 500 人以上の企業 2,319 社）



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

脅威検出の実践およびさまざまな企業での実施方法については、シスコの最新レポート「[環境に潜む脅威の検出：脅威検出をセキュリティ体制に組み込む \(Hunting for Hidden Threats: Incorporating Threat Hunting Into Your Security Program\)](#)」をご覧ください。

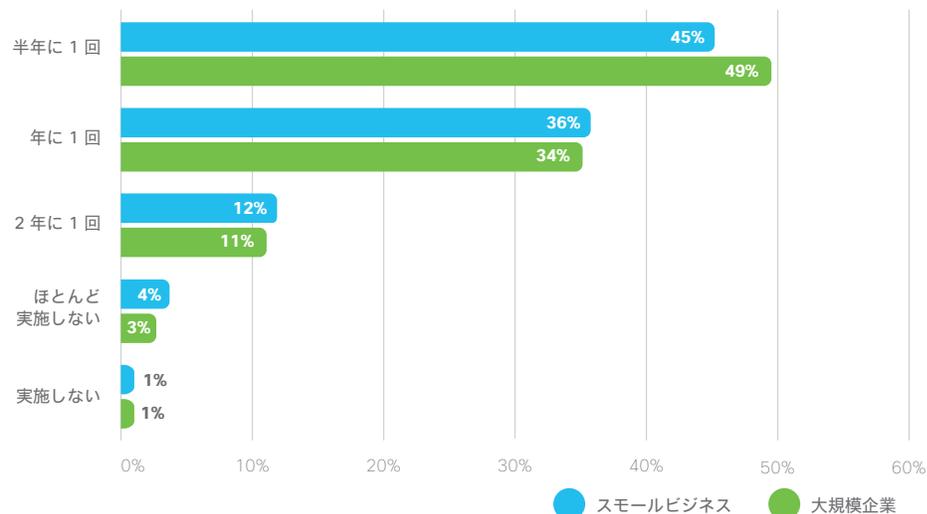
神話その 7：スモールビジネスはインシデント対応計画を訓練や演習でテストしていない

ボクシングの伝説的チャンピオンである Mike Tyson 元選手が「誰もが作戦を持っている。パンチを食らうまでの話だかな。(Everyone has a plan until they get punched in the face.)」とよく口にしていたように、インシデント対応計画は、実際にどのように機能するかを把握するまで、机上の空論にすぎません。

しかし、スモールビジネスには計画をテストする時間や人員の余裕がありません。したがって、割り当てることができたであろう時間や人員の価値を上回る規模の混乱が、確実に発生することになります。

誤り：この神話はまったくの的外れです。計画をテストしたことがないスモールビジネスはわずかに 1% であり、ほとんどテストしていないスモールビジネスは 4% にすぎません。12% が 2 年に 1 回、36% が年に 1 回のテストを実施しています。テストの頻度で最も多いのは、半年に 1 回です (45%)。

図 9. サイバーセキュリティ インシデントに備えた対応計画がある場合、訓練または演習によるテストをどの程度の頻度で実施していますか？ (スモールビジネス 481 社、従業員数 500 人以上の企業 2,319 社)



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

この数字は、大規模企業と比較してどのような状況でしょうか。結果がきわめて接近していることから、スモールビジネスの計画は大規模企業ほどには適切でないという見解は、インシデント対応に関しては誤りです。

神話その 8：どのような理由であれ、スモールビジネスのリーダー層はセキュリティとデータプライバシーを重視していない

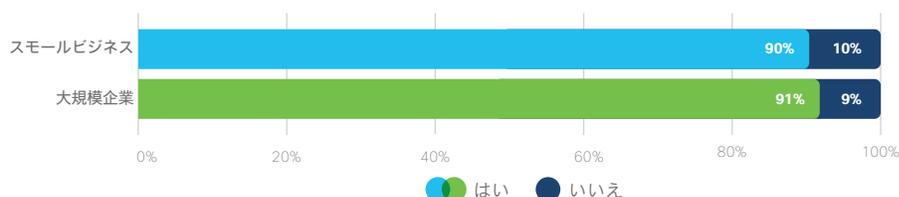
これは、まさに大きな問題となる神話です。残念ながら、業界全体で長年にわたって喧伝されています。スモールビジネスは、どの程度の危険にさらされているのかを把握できていません。また、セキュリティとデータプライバシーに関する組織文化も培われていません。

誤り：この神話は、実情とかけ離れていることがシスコのデータから明らかです。シスコは、さまざまな規模の組織を対象として、IT 意思決定担当者への調査を実施しています。そのデータに基づいて、3つの方法で神話の誤りを証明します。

データプライバシー

まず、シスコのデータによれば、自社のデータプライバシー制度を熟知していると回答したスモールビジネスの IT 意思決定担当者は、実に 90% にのびります。大規模企業の 91% と比較して、大きな差はありません。

図 10. 自社のデータプライバシー制度を熟知していますか？（スモールビジネス 481 社、従業員数 500 人以上の企業 2,319 社）

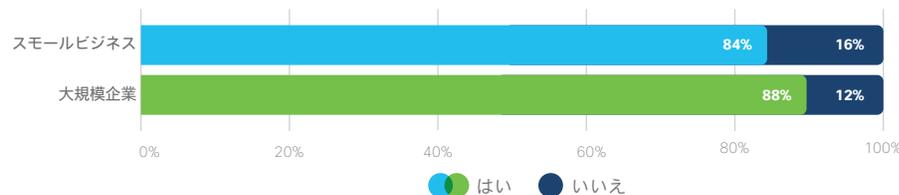


出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

サイバーセキュリティ啓発研修

次に、スモールビジネスの大多数である 84% が、セキュリティ啓発研修を義務付けています。これは、大規模企業の水準をほんのわずかに下回る程度です。

図 11. 貴社の従業員にサイバーセキュリティ啓発研修を義務付けていますか？（スモールビジネス 464 社、従業員数 500 人以上の企業 2,272 社）

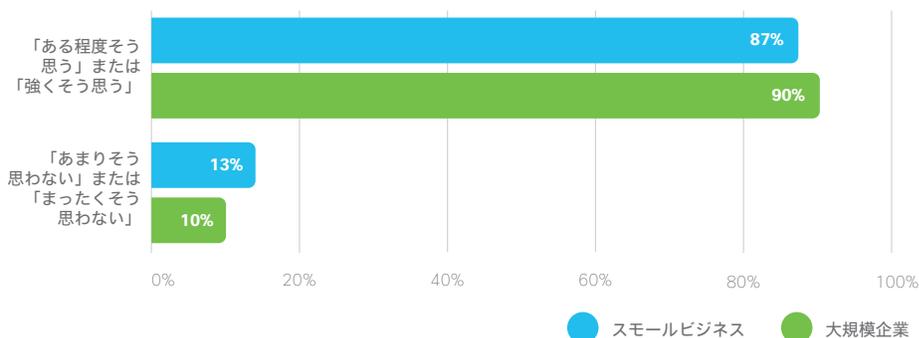


出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

エグゼクティブの賛同

3 番目に、スモールビジネス経営幹部の 87% が、セキュリティは最優先事項であると回答しています。この水準は、大規模企業の水準をわずかに 3 ポイント下回るにすぎません。

図 12. 貴社の経営幹部は、セキュリティを最優先事項と捉えているでしょうか？ (スモールビジネス 481 社、従業員数 500 人以上の企業 2,319 社)

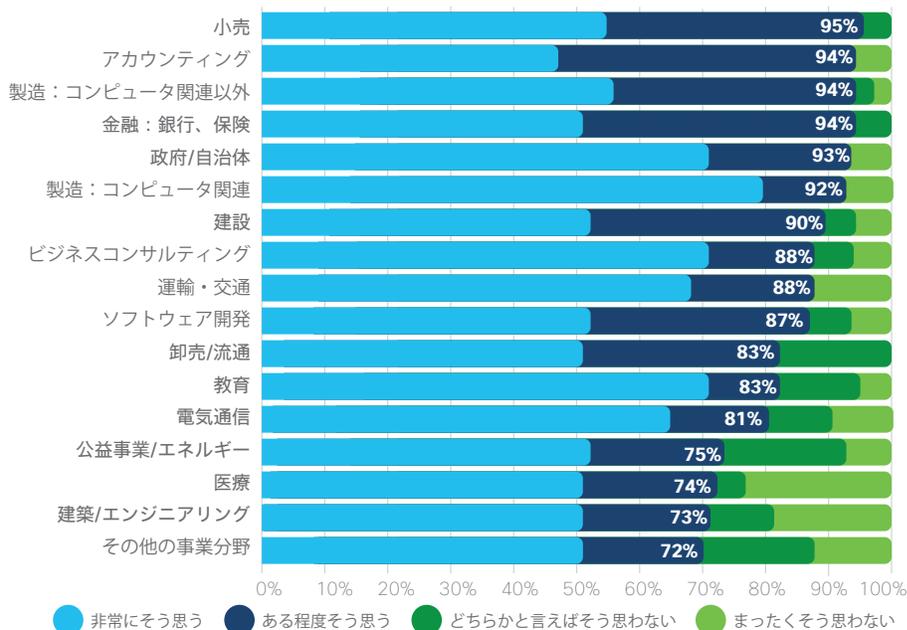


出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

セキュリティが効果を発揮するには、全社規模で浸透させる必要があり、セキュリティを軌道に乗せるには、経営幹部による後押しが欠かせません。これはシスコのお客様からよくお聞きするご意見であり、シスコも同じ見解です。この点は、大規模企業と同様にスモールビジネスにも当てはまります。ほとんどの場合、俊敏性が高いと考えられる環境では達成が容易になります。

これらの 3 つのアンケート調査の結果によると、スモールビジネスでは、セキュリティとデータプライバシーに関する組織文化がすでに根付いていることがわかります。自社の経営幹部がセキュリティを最優先事項と捉えているという回答は、すべての業種で 3 分の 2 を超えています (スモールビジネスの回答のみを掲載した図 13 を参照)。

図 13. 貴社の経営幹部は、セキュリティを最優先事項と捉えているでしょうか？ (スモールビジネス 481 社)



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版



「フィッシングテストで重点としているのは、あらゆる対象について、ユーザがクリックする頻度を洗い出すことではありません。より重要なのは報告です。好ましくないリンクをクリックする可能性は誰にでもあります。しかし、何か想定外の事態が起きた場合に報告を怠れば、自社の被害はあっという間に甚大なものになるのです」

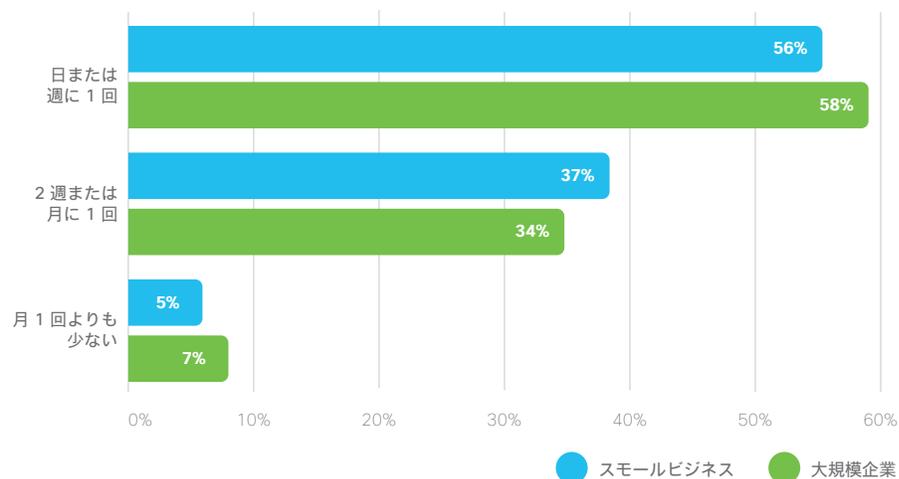
Wouter Hindriks 氏 (Missing Piece 社、ネットワークおよびセキュリティ担当技術チームリーダー)

神話その 9：小規模の組織は、脆弱性に対処するパッチを定期的に適用していない

パッチの適用はサイバーセキュリティの基本とされることが多い一方、実際には実装が困難な場合があります。神話として語られているのは、パッチの適用に伴う中断を最小限に抑えるための手立てを見つけ出すくらいなら、スモールビジネスはそのためのリソースを他の業務に振り向けるだろうというものです。

誤り：スモールビジネスの 56% は、パッチを 1 日または週に 1 回適用しています。大規模企業の場合は 58% です。つまり、きわめて規則的なパッチ適用ルーティンという観点では、どの規模の企業も同じアプローチをとっています。

図 14. 公表されたソフトウェア脆弱性に対処するパッチは、どの程度の頻度で適用していますか？ (スモールビジネス 481 社、従業員数 500 人以上の企業 2,319 社)



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

シスコのデータからわかるのは、従業員数が 500 ~ 999 人の企業または組織の場合、既知の脆弱性に起因するインシデントの発生率が最も高いことです。つまり、スモールビジネスに分類される企業は、既知の脆弱性に対して、一部の大規模企業よりも効果的にパッチを適用できているため、実際にはインシデントの発生率が低くなります。

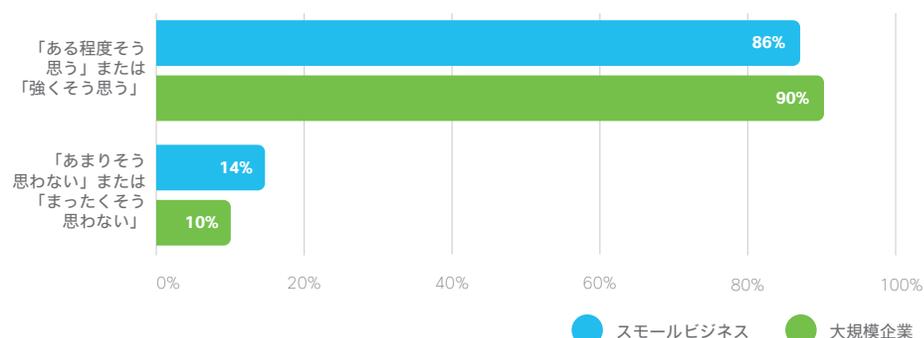
パッチの適用は、米国の [NIST SP 800-53](#) や [Center for Internet Security® \(CIS®\)](#) などによって定義されているとおり、最初の防御として欠かせません。これを実証しているのがスモールビジネスなのです。

神話その 10：スモールビジネスは自社のセキュリティ体制の有効性を測定できない

スモールビジネスは、「数打てば当たる」といったやり方でサイバーセキュリティに臨んでいるという固定観念を持たれています。つまり、取り組みをモニタリングし、何が本当に効果的であるのかを測定するための手段が導入されていないため、現状を最適化できないという見方です。

誤り：実にスモールビジネスの 86% が、セキュリティ体制の有効性を評価するための指標を明確に定めていると回答しています。一方、大規模企業の場合は 90% です。

図 15. 貴社の経営陣は、セキュリティ体制の有効性を評価するための指標を明確に定めていますか？（スモールビジネス 481 社、従業員数 500 人以上の企業 2,319 社）



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

シスコの調査データからわかるのは、組織の規模を問わず、明確な指標の採用に関しては、ごくわずかな差しかないことです。これは、サイバーセキュリティ製品が長年にわたって進化してきたことが一因かもしれません。最も優れた製品は、レポート作成を容易にするために、発見事項とその意味がきわめて明確に示される設計となっています。

ただし、「測定できないものは修正できない」という重要な概念を念頭に置けば、スモールビジネスの取り組みには改善の余地があります。経営幹部が指標を明確に定めているかという質問項目に「強くそう思う」と回答したのは、大規模企業が 53% であるのに対して、46% にすぎないためです。

セキュリティ最適化の機会を捉える

スモールビジネスは強力なセキュリティ対策を実施しているという点で、より高い評価を受けるに値することが実証されました。その一方で、さらに改善したいという要求が今なお存在することも明らかです。ベンダーを取り巻く現状を考慮すると、セキュリティを盤石にすることは容易ではありません。現実味のない、薔薇色の将来像を描くべきではないでしょう。

サイバーセキュリティ疲れ

サイバーセキュリティ疲れとは、攻撃者の機先を制する地道な取り組みを事実上あきらめてしまうことです。意外にも、小規模企業は大規模企業とまったく同じ水準のサイバーセキュリティ疲れに見舞われています。スモールビジネスと大規模企業のいずれも、疲れを経験したことがあるという回答は41%で、経験したことがないという回答は58%です。セキュリティ管理の効率を高めたいという要求や必要性が存在することは、疑いありません。

従業員によるサイバーセキュリティ啓発プログラムの受け入れ

ユーザによるサイバーセキュリティ啓発プログラムの受け入れが進んでいなかったスモールビジネスと大規模企業では、セキュリティ侵害を受けた際のダウンタイムに大きな差はありません。

ユーザは防御の最前線に位置する可能性もあり、ユーザの行動が結果を左右することは明らかです。ただし、ユーザを「最弱リンク」、つまり鎖を構成する中で最も弱い部分と見なすことは、得策ではありません。むしろ、ユーザをセキュリティ戦略の一員として組み入れ、プログラムの受け入れが当たり前となるようにします。

セキュリティの民主化（誰もが取り組みに参加する）は、シスコのCISO アドバイザリボードで責任者を務める Wendy Nather が、RSA Conference 2020 で[魅力的な基調講演](#)を行った際のトピックです。Wendy のインタビューは、[シスコのセキュリティ事例のポッドキャスト](#)でも配信しています。



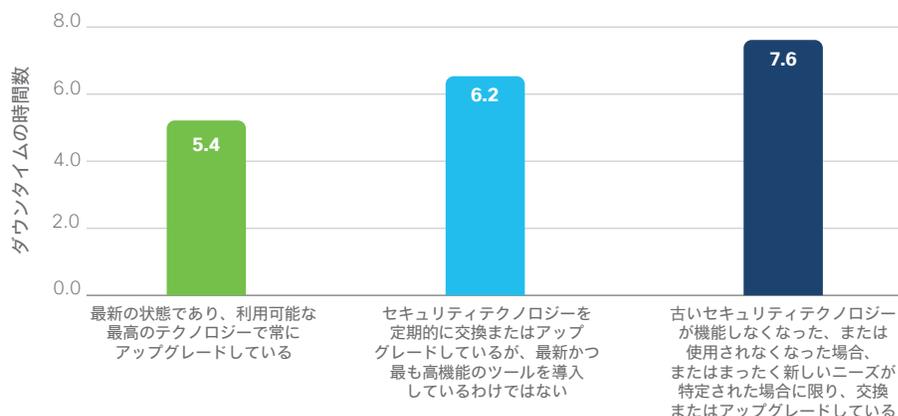
「フィッシング攻撃のシミュレーションの結果、罠にかかってしまった人を糾弾するのではなく、被害を報告してくれた人に謝意を伝えています。奨励したい行動をとったかどうかを、測定の対象とするのです」

Wendy Nather (シスコ、アドバイザー CISO リーダー)

ダウンタイムの短縮

ハードウェアやソフトウェアは古くなるほど、新しく出現する脅威に対する効果が低下するというのは本当でしょうか。この説は、スモールビジネスに関しては、シスコのデータで裏付けられたように思われます。

図 16. 貴社のセキュリティ インフラストラクチャは、前年 1 年間に受けた最も深刻なセキュリティ侵害に起因するダウンタイムの長さを考慮すると、どのような状況にあるでしょうか？（スモールビジネス 481 社）



出典：シスコの「スモールビジネスにおけるセキュリティの重要性」レポート 2020 年版

古いセキュリティテクノロジーが機能しなくなった場合に限り、交換またはアップグレードを実施していると回答したスモールビジネスでは、昨年 1 年間の最も深刻なセキュリティ侵害の発生後、7.6 時間のダウンタイムが発生していました。最新のインフラストラクチャを使用していると回答したスモールビジネスの場合、ダウンタイムは 5.4 時間です。

では、既存の環境をすべて廃棄して、高機能の最新ツールを購入することだけをシスコは奨励しているのでしょうか。いいえ、まったく違います。サイバーセキュリティに関するシスコの経験では、適切に機能する既存の環境が陳腐化するまで何も手を付けずに運用するのではなく、適切に統合を進め、必要に応じて新しいテクノロジーで補完することが重要です。

インフラストラクチャの旧式化が懸念事項となっている場合は、検討すべき側面がいくつかあります。最も重要なのは、変化に対応できる柔軟性を備えていることです。ポリシーとデバイスの管理に役立つ自動化およびアナリティクスの機能が組み込まれていて、未知の脅威が検出され、対応およびポリシー変更に向けて調整を進められることが理想的です。

現在のプラットフォームで、オンプレミスとクラウドのネットワークトラフィックにアナリティクスを適用して、異常な行動を特定できるかどうかを確認してください。この処理は、ポリシーを適用し、セキュリティ侵害を受けたエンドポイントのネットワークおよびアプリケーションへのアクセスを自動的に調整する処理と同時に実行する必要があります。

詳細については、「[セキュリティ プラットフォーム ベンダーへの 5 つの質問 \(5 Questions to Ask Your Security Platform Vendor\)](#)」をご覧ください。

ベンダーの複雑さ

多くの組織にとって、セキュリティのリスクを分散することは、ベンダーを増やすことを意味するように思えるかもしれませんが。しかし、このアプローチを採用した場合、結果はどのようなものになるのでしょうか。マルチベンダー環境を管理する業務の難しさを考えてみてください。採用するベンダーの数を増やせば、保護対象の範囲が拡大し、ダウンタイムが短縮されて、セキュリティが向上するのでしょうか。

驚くべき事実として、調査に回答したスモールビジネスの場合、採用したベンダーの数が多いほど、最も深刻なセキュリティ侵害に伴うものとして報告されたダウンタイムは長くなっています。ダウンタイムの長さは、ベンダーが1社の場合は平均4時間であった一方、50社を超える場合は平均で17時間を超え、4倍を上回る差が生じました。

図 17. セキュリティ環境で採用しているセキュリティベンダーの数と（スモールビジネス 472 社）、前年 1 年間に対処した最も深刻なセキュリティ侵害に伴うシステムダウンタイム（スモールビジネス 388 社）

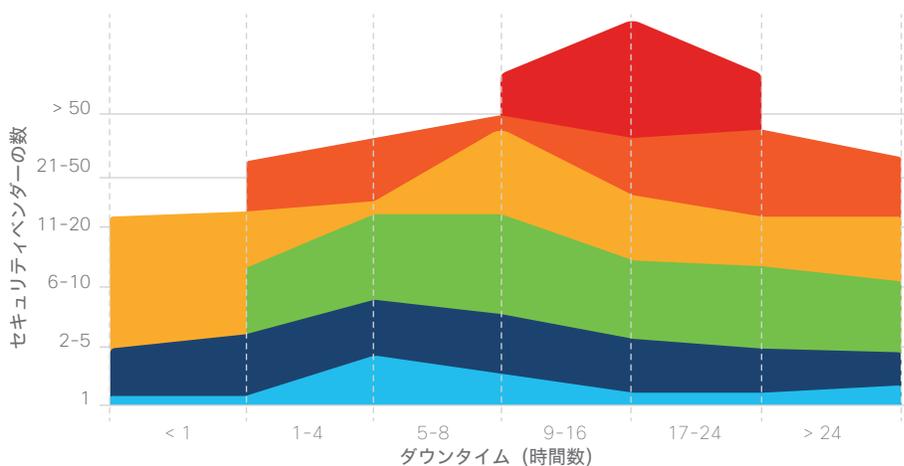


図 17 から明らかなように、採用するベンダーの数が多くなるほど（下から上）、ダウンタイムは長くなっています（左から右）。一般的なスモールビジネスのセキュリティ環境では、ベンダーが無秩序に増加すると、不要な複雑さや非効率的なワークフローが発生するだけでなく、システムのダウンタイムという点で自社の死活問題にもなり得ます。

マルチベンダー環境で生じる複雑さの問題を軽減する上で最適な方策は、オープンかつポートフォリオベースのプラットフォームを採用して、複数のソリューションが連携できるようにすることです。

今後の取り組み を着実に進める ための関連資料

これまでの要点をまとめると、スモールビジネスは、セキュリティの問題を真摯に受け止めた上で、戦略的なプランニングと日々の業務に取り組んでいることをデータが示しています。これはすばらしい傾向です。

一方、[2020年版のCISOベンチマーク調査](#)によれば、新たなセキュリティ課題も日々持ち上がっています。

また、スモールビジネスの場合、事業を維持し、成長させなければならないという重圧は強いものになります。その点に加え、モバイルとリモート環境を利用する従業員も増加しています。私たちは、一歩先も見えない状況の真っ只中にあるのです。

このような状況で取り組みを進めるための一助として、スモールビジネスに特化したシスコのWebサイト ([スモールビジネス向けセキュリティソリューション](#)) をご覧ください。また、サイバーセキュリティを活用して成功を加速する上で有用となる、その他のリソースもいくつかご紹介します。

- ・ [パスワードがその役割を終える日がついに到来 \(The End of the Password... Finally\)](#)
- ・ [ビジネスの未来を見据えたクラウドセキュリティ \(Cloud Security for the Future of Your Business\)](#)
- ・ [スモールビジネス向け製品セレクト \(Small Business Product Selector\)](#)
- ・ [次世代ファイアウォールを選択する際の3つのヒント：中小規模企業向け](#)
- ・ [シスコスモールビジネス向けセキュリティのお客様導入事例 \(Cisco Small Business Security Customer Case Studies\)](#)

シスコは、セキュリティソリューションはひとまとまりのチームとして機能（相互に学び、相手の行動を待ち、応答）するべきであるという考えに基づいて、セキュリティプラットフォームを構築しています。セキュリティの簡素化と有効性の向上をもたらす体系的なアプローチであるとシスコは考えています。

[Cisco SecureX](#) は、既存のインフラストラクチャを統合して、一貫性のあるエクスペリエンスを実現します。可視化の機能が一体化され、自動化を実現するとともに、ネットワーク、エンドポイント、クラウド、アプリケーションの全体にわたってセキュリティを強化します。

リモートワーク 環境の保護

現在は、大量のリモートワーカーをサポートする体制への急激な転換が進んでいる状況です。かつてないほどに一変した環境で組織を運営し続けるために、一連のセキュリティ課題が持ち上がっています。その結果、セキュリティチームと IT チームは、いずれも突然の激務を強いられています。かつてない数のオフサイトワーカーとそのデバイスを対象として、セキュリティを損なうことなく、迅速にサポートを提供するという責務を課せられているのです。

リモートワーク体制への適応を進めているスモールビジネスは、どのようにセキュリティを維持しているのでしょうか。新しい生活様式という現実を考慮すれば、ビジネスの速度と規模に応じて、シンプルかつ容易にリモートワーカーをセキュリティ保護するための手立てが必要です。

シスコは、貴社の従業員がリモートで安全に職務を進められる環境の整備でお役に立ちたいと考えています。シスコがお勧めするのは、以下の手順で取り組むことです。

- ・ **まず、このレポートで取り上げた基本事項を押さえます。**つまり、脆弱性に対処するパッチの適用、従業員向けのトレーニング、多要素認証 (MFA) によるゼロトラストアクセスの実装、およびネットワーク、エンドポイント、クラウド、アプリケーションのセキュリティ保護です。
- ・ **2番目に、セキュリティと使いやすさのバランスを取ることです。**従業員は、セキュリティ専門家の頭にある知識を読み取る能力は必要ありません。それぞれが職務を抱えています。職務の中で、各自がスムーズにセキュリティ対策を実践できるようにします。
- ・ **3番目に、セキュリティ インフラストラクチャを複雑にするのではなくシンプルにするための取り組みで、助力となるセキュリティベンダーと提携します。**シスコのデータによれば、関与するベンダーは数が少ない (かつ、戦略的である) ほど、セキュリティ侵害に伴うダウンタイムが短いという相関関係が存在しています。

安全な接続環境を維持する上で有用となる記事、ウェビナー、ご提案事項については、「[リモートワーカーのセキュリティ保護のためのシスコ製品 \(Cisco Secure Remote Worker\)](#)」をご覧ください。

シスコのエキスパートについて

シスコセキュリティには、CISO の職務経験者で構成される CISO アドバイザリボードが設置されています。メンバーは、サイバーセキュリティに関する知識と各種業界での経験を兼ね備えた人材です。各メンバーがインサイト、ガイダンス、経験を提供し、サイバーセキュリティ レポート シリーズで推奨事項をご紹介します。また、デジタルトランスフォーメーションの着実な遂行から、コンプライアンス、プライバシー、モニタリング、可視化機能、ゼロトラスト、脅威インテリジェンスに至るまで、さまざまな課題について販売代理店、パートナー、お客様へのサポートも行っています。CISO アドバイザリチームのメンバーへのご相談をご希望の場合は、asktheciso@external.cisco.com までお問い合わせください。

シスコ サイバーセキュリティ レポート シリーズの概要

シスコは過去 10 年間にわたって、全世界のサイバーセキュリティ専門家を対象に、セキュリティと脅威インテリジェンスに関する多くの信頼できる情報を公開してきました。これらの包括的なレポートでは、脅威の現状や組織への影響を詳しく解説し、データ漏洩などから組織を守るためのベストプラクティスを紹介しています。

シスコセキュリティは『シスコ サイバーセキュリティ シリーズ』というシリーズ名で、調査データに基づく一連の出版物を発行しています。シスコはシリーズのタイトル数を増やししながら、それぞれに関心の異なるセキュリティ プロフェッショナル向けにさまざまなレポートを提供してきました。セキュリティ業界の脅威研究者やイノベーターからの幅広い専門知識を集めた毎年のレポートには、データ プライバシー ベンチマーク調査、脅威レポート、CISO ベンチマーク調査などがあり、今後も年間を通していくつかのレポートが発表される予定です。

詳しい情報や過去のレポートは、www.cisco.com/go/securityreports をご覧ください。

©2020 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2020 年 7 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
<http://www.cisco.com/jp>

お問い合わせ先

 **Secure**