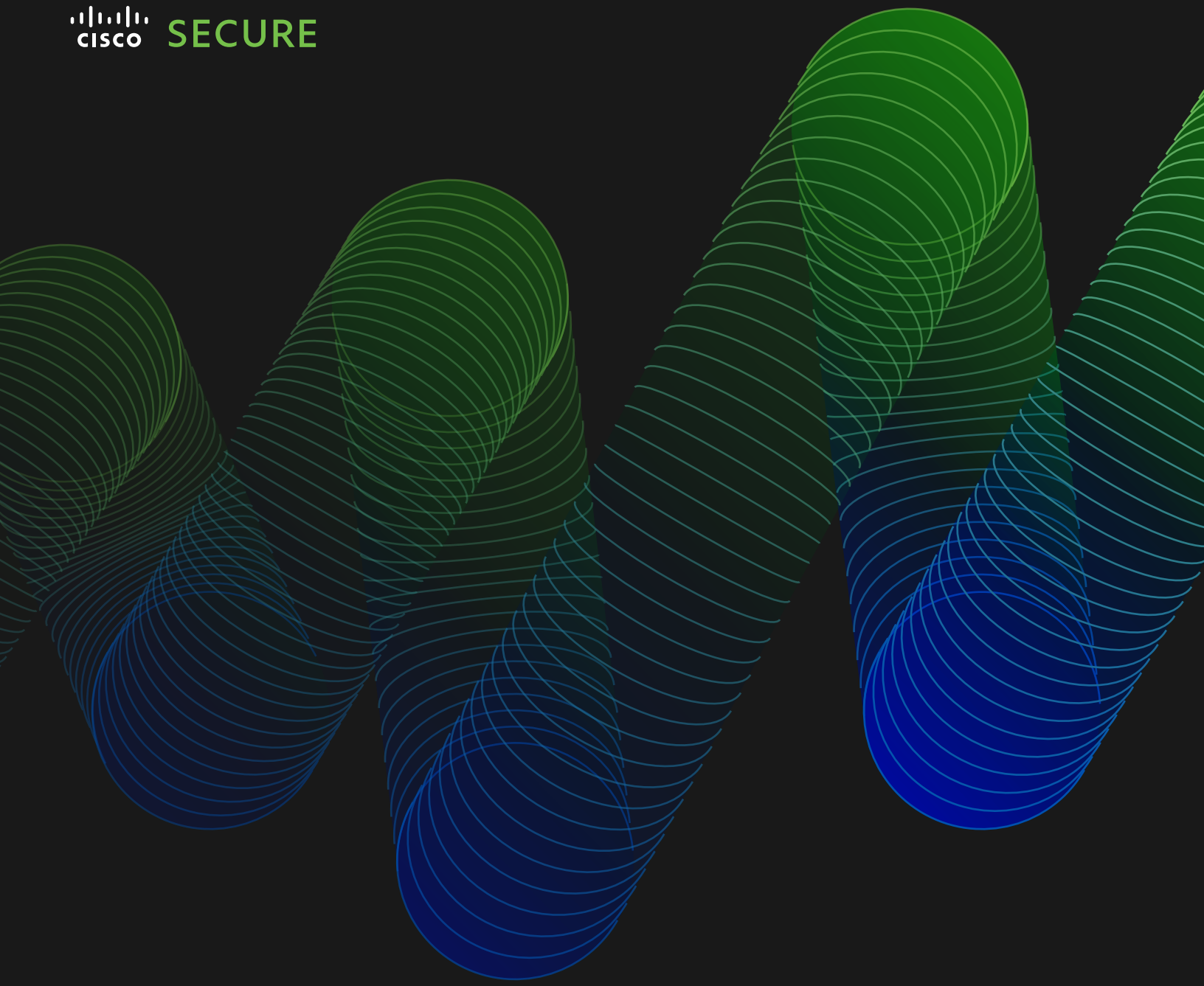
cisco SECURE



セキュリティ成果レポート

Vol. 3

サイバーレジリエンスの達成

目次

序文

レジリエンス（復元力）という言葉から何を思い浮かべますか？シェイクスピアの言葉を借りれば、「非道な運命の矢弾をじっと耐え忍び」ながらも、さらに強くなろうとする不屈の精神と大胆さを思い浮かべるかもしれません。

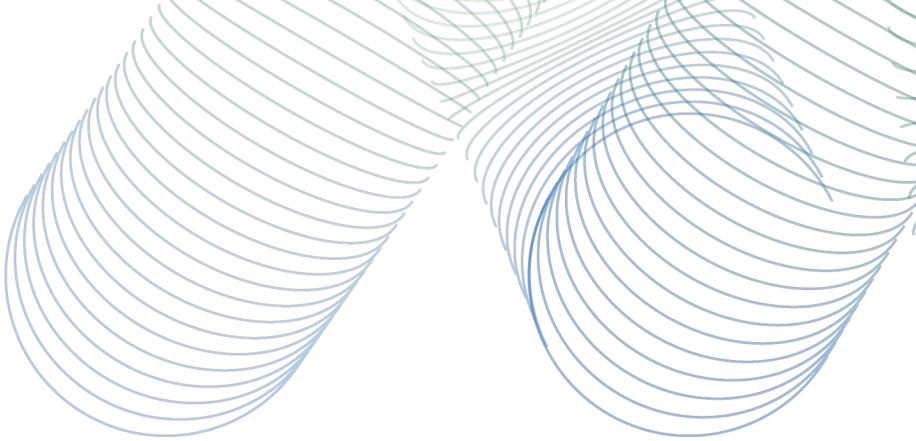
それはまさに納得のいく定義であり、その精神は賞賛されるべきものです。しかし、大小さまざまな企業のセキュリティを確保するという話になると、ダウンした後で立ち直るレジリエンス（復元力）があるだけでは十分ではない場合があります。結局のところ、ランサムウェアや知的財産の盗難などのサイバーセキュリティ侵害が成功すると、企業やその従業員、パートナー、さらには顧客にまで多大な損害を与える可能性があるのです。2021 年のセキュリティ成果レポートでは、調査対象の企業の 41% が、過去 2 年以内に重大なセキュリティインシデントまたは損失を被ったと述べていることから、この問題がいかに広範囲に及んでいるかがわかります。

シスコでは、サイバーレジリエンスを、ビジネスのあらゆる側面の完全性を保護する能力と定義しています。その能力により、ビジネスは存続できるだけでなく、予測不可能な脅威や変化に耐えられるようになり、さらに強固になるのです。この第 3 回セキュリティ成果レポートでわかるように、調査対象となった経営幹部の間では、サイバーレジリエンスを達成することがビジネスにとって重要であるという意見でほぼ同意しています。これは、より多くのビジネスが相互につながっている今日であれば不思議なことではありません。バリューチェーンのどこかが侵害を受けると、他のバリューチェーンにも大きな波及効果をもたらす可能性があります。**経営幹部はだれでも、十分に手を尽くさなかったという評判を立てられることを望まないでしょう。**

このレポートをぜひご活用ください。サイバーレジリエンスの基準を達成するための戦略やソリューションを作成する上で、本書がお役に立てば幸いです。脅威に対するレジリエンス。変化に対するレジリエンス。未知なるものに対するレジリエンス。セキュリティ業界は確かにバズワードに事欠きません。ただ、レジリエンスという言葉は当面よく耳にしそうな気がします。『ハムレット』などの偉大なシェイクスピア劇ほど長くは残らないと思いますが、ある程度長期間におよぶことでしょう。

– Shailaja Shankar
Cisco Secure SVP 兼 GM

出典：シスコ『2021 年セキュリティ成果レポート：エンドポイント版』



「世の中はつらいことで
いっぱいですが、
それに打ち勝つことも
満ちあふれています。」

– ヘレン・ケラー

概要

セキュリティ部門の仕事は決して楽ではありません。しかし、ここ数年、サイバーインシデントからビジネスを保護するための対策は非常に高い水準に達しています。今日のセキュリティ対策は、脅威の増加と攻撃対象領域の拡大を考慮しなければならないだけでなく、戦争、気候変動、金融不安、そしてもちろん、世界的なパンデミックなど、より大局的なリスクについても考慮する必要があります。

この激動の環境において、レジリエンスという概念がほとんどの企業の課題の上位に浮上しています。**このような急速で破壊的な変化に迅速に対応し、より強い企業として生まれ変わるにはどうすればよいでしょうか？**

第 3 回目となるこのセキュリティ成果レポートでは、サイバーレジリエンスを消化しやすく、実行可能な洞察にかみ砕いて説明しています（多くの本来集中すべき業務があるでしょうから、ご自身でレジリエンスについて研究していただく必要はありません）。このような巨大なテーマは、1 つのレポートですべてを網羅することはできません。しかし、今後のサイバーセキュリティ戦略を構築し、改善する際に考慮すべきいくつかのポイントをご紹介します。

26 か国の 4,700 人を超えるセキュリティ専門家から収集したデータを使用して、サイバーレジリエンスを向上させることができる **7 つの成功要因**を明らかにしました。また、このレポートでは、サイバーレジリエンスの意味、重要性、および企業が自社のレジリエンス（復元力）をどのように評価しているかを正確に分析しています。

このデータが参考になり、今後何が起ころうとも成功するような組織を構築する際の自信につながることを願っています。

リスクとレジリエンス（復元力）は橋でつながっています。時として困難な道のりを歩むことになりますが、私たちがお手伝いします。

主な調査結果

サイバーレジリエンスはエグゼクティブの最優先事項です。 **96%** のエグゼクティブはサイバーレジリエンスをビジネスにとって**非常に重要** と考えています。

約 **2/3** の組織が、事業運営を危険にさらす**重大なセキュリティインシデントを経験**していると報告しています。

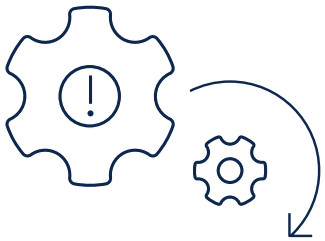
文化は重要です。

セキュリティの文化を育む組織では、レジリエンス（復元力）が 46% 向上しています。

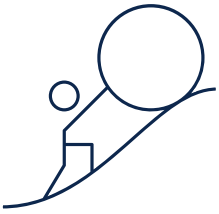
アーキテクチャは重要です。

ゼロトラスト、XDR、SASE の実装が成熟している組織は、いずれもレジリエンススコアが著しく高くなっています。

最優先事項



インシデントの防止と**損失の軽減**は、サイバーレジリエンス全体の最優先事項です。



セキュリティ人材の確保は、レジリエンス（復元力）の優先度が最も低い分野ですが、あらゆる種類の組織にとって**最も困難な課題でもあります。**

優先順位最低

当社では、**7** つの**成功要因**を特定しました。これらを達成すれば、全体的な**サイバーレジリエンス**の測定値が、下位 10 パーセントから上位 10 パーセントに**上昇**します。

本調査について

サンプリング方法	シスコは専門のデータ調査会社に委託して、2022 年半ばに層化無作為抽出法による完全匿名アンケートを実施しました。
調査参加企業	本調査の対象となったのは、情報セキュリティおよびプライバシーの分野に従事する、26 か国、4,751 人の専門家です。サンプルの内訳については、付録を参照してください。
データ分析	調査データの分析と取りまとめは、シスコから委託を受けた Cyentia Institute 社が独自に行っています。

「セキュリティ成果レポートの思慮に
富んだアプローチに感銘を受けました。
セキュリティプログラムの効果を
最大化するためのリソースの最適な
活用方法について、データに基づく
ガイダンスを提供しています。」

– Theresa Payton
Fortalice の CEO
ホワイトハウスの元 CIO

サイバーレジリエンスとは

「レジリエンス（復元力）」がバズワードだと思うかどうかは別として、サイバーセキュリティ分野の内外で多くの人がこの言葉を意識していること、そしておそらく口にしていることは否定できません。しかし、それは正確には何を意味するのでしょうか？シスコはこのテーマについて一定の考えを持っていますが、今回は 4,700 人以上のセキュリティ専門家を対象とした調査であるため、彼らの意見を聞くことにしましょう。

「君は何回もその言葉を使っているけど使い方を間違っていると思うよ。」

– イニゴ・モントーヤ、『*The Princess Bride*（プリンセス・ブライド・ストーリー）』

セキュリティ（またはサイバー）レジリエンスがそれぞれの組織の文脈ではどのような意味があるのかを説明してもらえるよう依頼したところ、幅広い回答が返ってきました。しかし、それらの回答にはいくつかの共通のテーマが見られます。

「耐える」、「回復する」、「予想する」、「適応する」、「不利になる」などの言葉はすべて、回答者が考えるサイバーレジリエンスの概念の中核として際立っています。奇妙なことにそれに聞き覚えがあるとしたら、それは NIST のサイバーレジリエンスの定義をそのまま引用しているからかもしれません。それはまったく問題ありません。このような調査で不正をすることはありませんから。しかし、このことは、多くのセキュリティ専門家が調べなければならないほど、レジリエンス（復元力）の意味が曖昧であることを示唆しています。以降のセクションで、その概念をより明確にしていきましょう。

サイバーレジリエンス：

サイバーリソースを使用する、またはサイバーリソースによって利用可能になるシステムが、困難な状況下、ストレス下、攻撃下にある、もしくは侵害されている状態に陥ったとしても、それを予測し、それに耐えて、そこから回復し、それに適応できる能力。

– 出典：NIST SP 800-172

サイバーレジリエンスが重要な理由

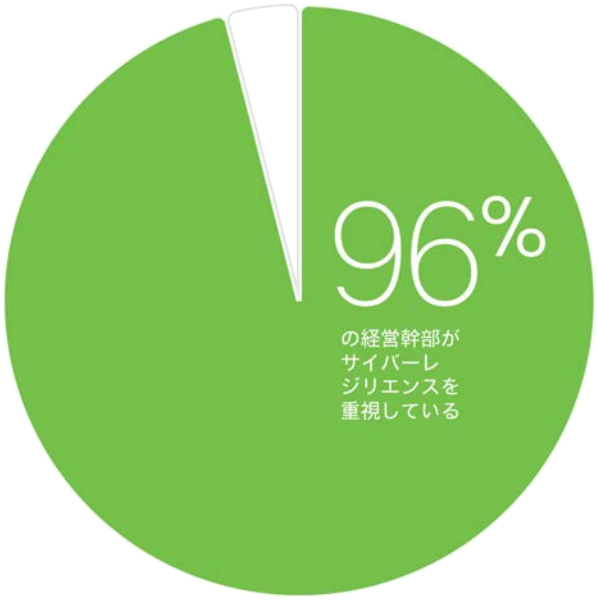
この考えに反対する人たちは、このセクションのタイトルを読み、「サイバーレジリエンスが重要だなんて納得がいかない」と思うかもしれません。それで結構です。無駄な主張をするつもりはありません、最初にそれを裏付ける証拠を述べます。

回答者に、組織の最高幹部がサイバーレジリエンスにどの程度の関心と重要性を抱いているかについて尋ねました。これ以上明確な答えはありません。**経営幹部の 96% が、サイバーレジリエンスを非常に重要視していたのです。**これこそ真の重大事であることの証明です。

経営幹部の間でサイバーレジリエンスが非常に重要視されているのは、彼らの多くがリスクを熟知しているからかもしれません。**回答者の 3 分の 2 近くが、業務を危険にさらす重大なセキュリティインシデントを経験していると報告しています。**

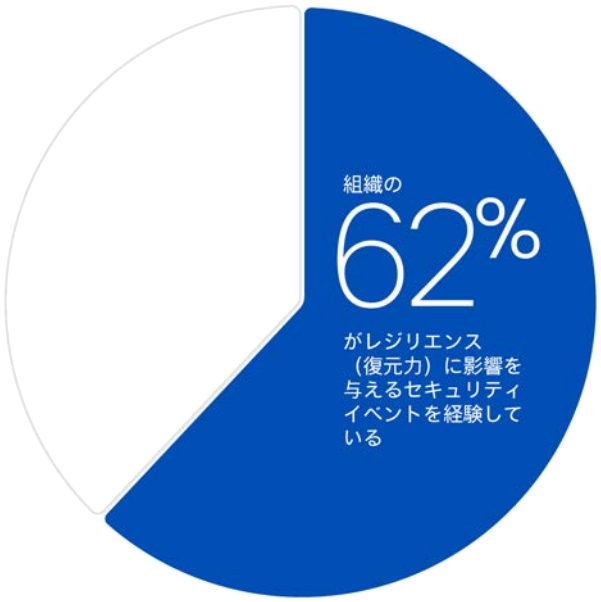
さらに、これらの事象の大半は、過去 2 年以内に発生したと言われています。このことから、サイバーレジリエンスは、思考的指導者の言葉や経営幹部の頭の中だけで重要な問題になっているわけではないと推測されます。これは、世界中の大多数の組織にとって非常に重要な概念です。

図 1：経営幹部はサイバーレジリエンスにどの程度の関心と重要性を抱いているか？



出典：『シスコセキュリティ成果レポート』

図 2：組織はレジリエンス（復元力）に影響を与えるセキュリティインシデントを経験したことがあるか？



出典：『シスコセキュリティ成果レポート』

次に、レジリエンスに影響を与えるインシデントの種類について詳しく説明してもらえるよう回答者に依頼したところ、図 3 に示すように、過去のインシデントを報告した参加企業の半数以上が、ネットワーク / データ侵害とネットワーク / システム停止の両方を挙げました。次に多いのは、ランサムウェアと分散型サービス妨害（DDoS）攻撃で、それぞれ約 46% の組織が影響を受けました。

前述のインシデントの種類のいくつかは、従業員が攻撃ベクトルとして関与していることはほぼ間違いありませんが（フィッシングメールをクリックするなど）、内部関係者によるあからさまで悪質な不正使用が約 38% の組織から報告されました。また、物理的な破壊行為や妨害行為も挙げられていますが、他のインシデントの種類と比べてかなり少ない数になっています。

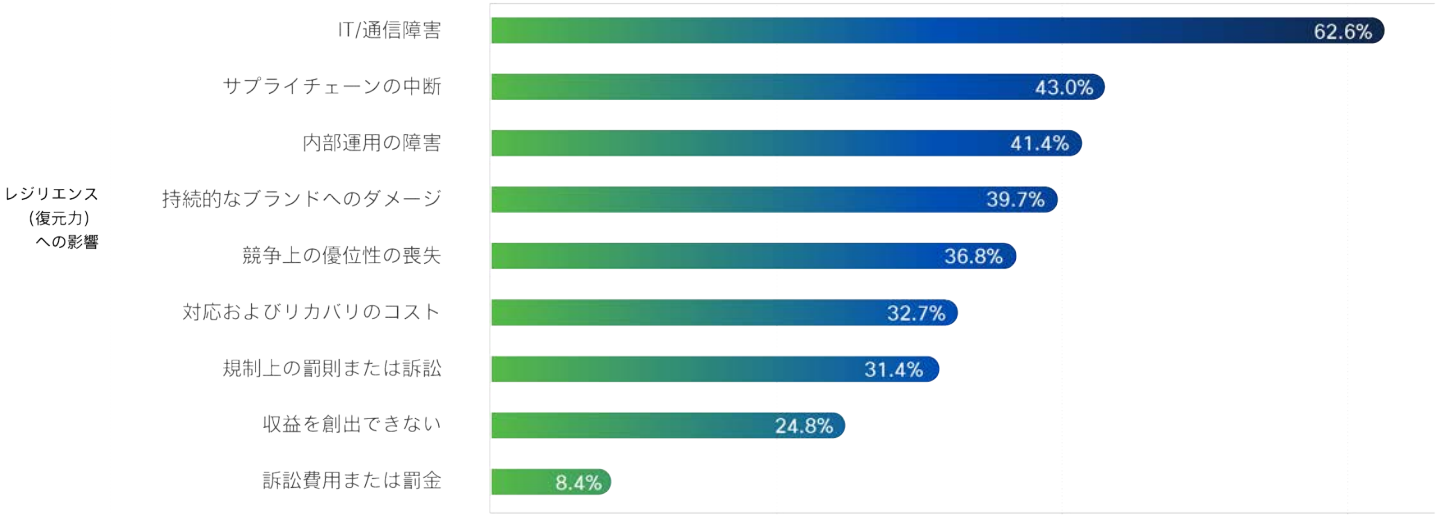
図 3：レジリエンス（復元力）に影響を与えたセキュリティインシデントの種類

出典：『シスコセキュリティ成果レポート』

また、これらの事象が組織にどのような影響を与えたかについても、多くの回答者が見解を述べました（図 4 を参照）。60% 以上が IT と通信の中断とサイバーレジリエンスにおいて ICT が果たす重要な役割をあげています。サプライチェーンの混乱は、ビジネスレベルの影響として 2 位にランクインしています。最近は、私たちの誰もがその不便さを感じながら生活しているため、組織も同じように感じているのは当然のことです。

サプライチェーンの運用への影響は被害組織の外部の組織に影響を及ぼしますが、内部運用の障害（企業の約 41% が報告）は内部に大混乱をもたらします。ブランドへのダメージは、多くの経営幹部が「夜も眠れない原因」の上位に挙げています。つまり、これらのインシデントの約 40% がそのような結果を招いていることを物語っています。さらに別の懸念事項として、競争上の優位性の喪失が上位に挙がっていて、レジリエンス（復元力）への影響の上位 5 つの中にランクインしています。

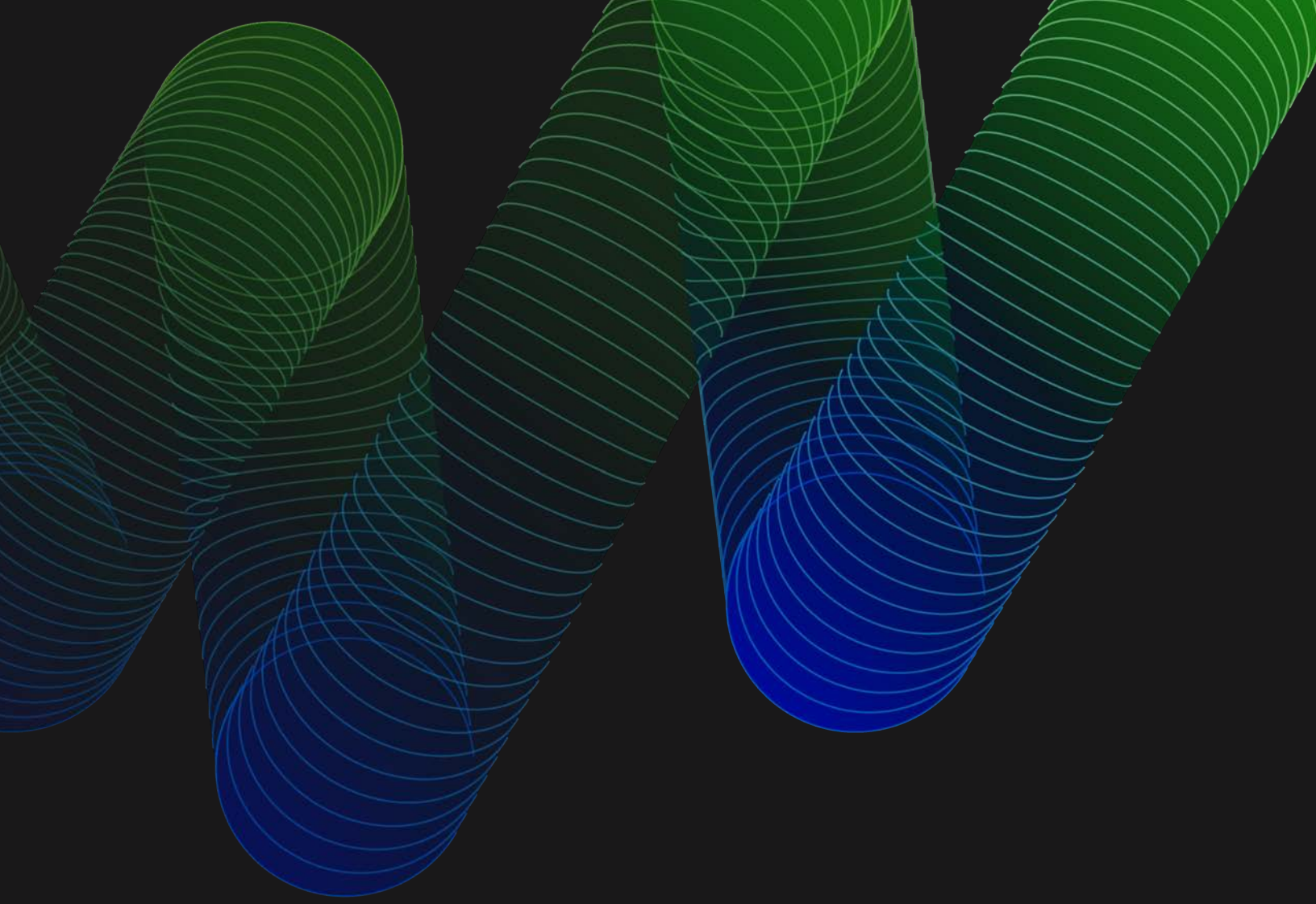
図 4：セキュリティインシデントによって生じるレジリエンス（復元力）への影響の種類



出典：『シスコセキュリティ成果レポート』

このような事象を回避し、サイバーレジリエンスを向上させるために、組織は何ができるでしょうか？それが、このレポートで扱おうとしている主な疑問の 1 つです。まず、組織が何よりも大切にしていることが「お金を使うこと」であるのは、明らかです。驚くべきことに、参加企業の 96% が、昨今の重大なインシデントを受けて、組織がセキュリティへの投資を増やしていると述べています。

お金をつぎ込んでも問題は解決しないことを誰でも知っています。しかし、無料のソリューションはほとんどないことも知ってのとおりです。重要な問題は、どの投資がリターンをもたらし、どの投資がリターンをもたらさないかということです。それに関しては、もう少し後でご紹介します。その前に、サイバーレジリエンスの保護のもとに入る主な目的を調べてみましょう。



「結局のところ、セキュリティはリスクビジネスです。あらゆる場所ですべてを保護することはできませんし、そうでなければビジネスは成り立ちません。しかし、サイバーレジリエンスにより、組織に最大の価値をもたらすビジネスの分野にセキュリティリソースを集中させ、その価値を確実に保護することができます。」

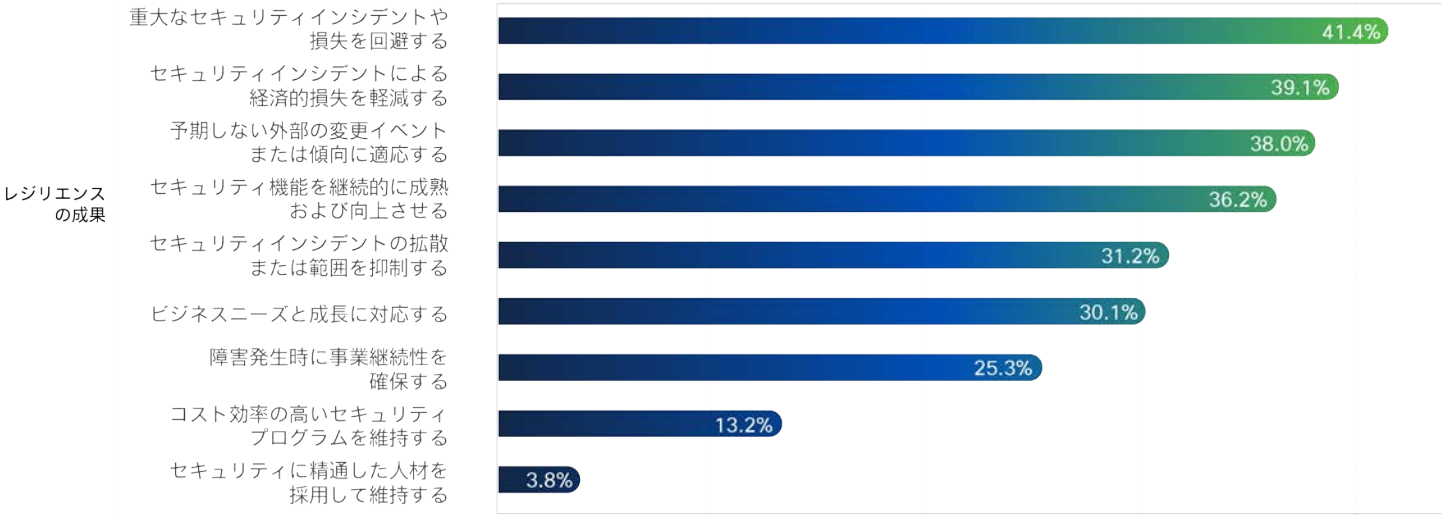
– Helen Patton
シスコ セキュリティ ビジネス グループ CISO

サイバーレジリエンスに含まれるもの

前のセクションからサイバーレジリエンスが経営幹部の間で重要と見なされていることがわかりましたが、実際サイバーレジリエンスには何が含まれるのでしょうか？組織にレジリエンス（復元力）があることを示す特徴や成果とは何ですか？この調査の準備として、セキュリティリーダーたちに、サイバーレジリエンスの目標と目的について質問しました。次に、その回答を検討し、サイバーレジリエンスの主要な成果を 9 つに分類しました。

現在のグローバルに実施された調査に戻って、レジリエンスの 9 つの主要な成果のうち、組織が最も重要であると見なすものはどれかを参加企業に尋ねました（最大 3 つまで選択）。図 5 は、その回答を集計したものです。

図 5：参加企業が選択したサイバーレジリエンスの最も重要な成果



出典：『シスコセキュリティ成果レポート』

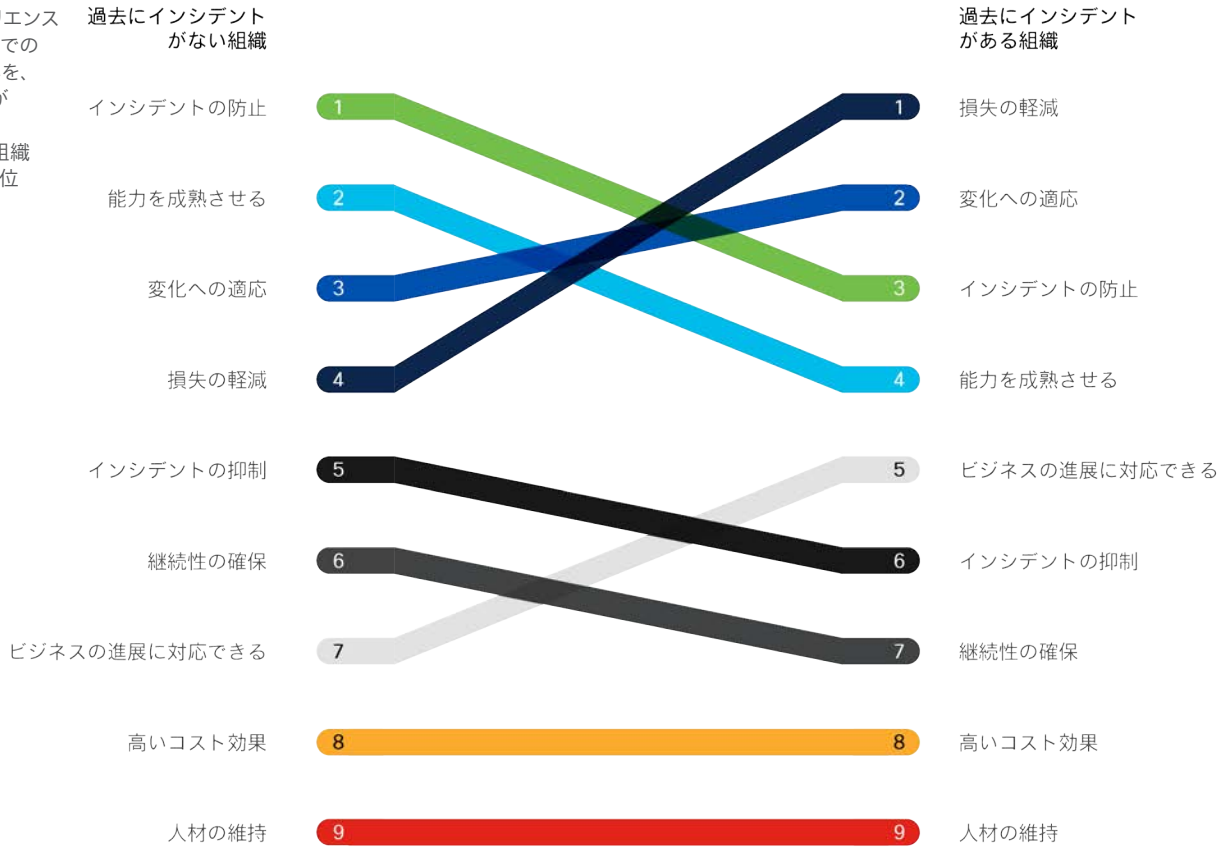
レジリエンスを「災害発生後の対応」の概念と捉えることが一般的であるのを考えると、「インシデントの防止」が上位に選ばれているのは少し意外です。しかし、経済的損失の軽減と合わせると、上位 2 つは、従来のリスクの定義である可能性と影響を対象としています。

次に、予期しない事象への対応ですが、これは先程の自由形式の回答で示されたテーマが思い出されます。近年の新型コロナ感染症の影響もあって、リストの上位にランクインしたのではないかと考えられます。

ここでは、9 つの成果についてのすべてにコメントすることは差し控え、最後の 1 つまでスキップすることにします。セキュリティ人材の採用と維持をサイバーレジリエンスの主要な側面と見なしている回答者は 3.8% にすぎません。おそらく、回答者は人材の維持を、レジリエンス（復元力）に影響を与える事象にとって重要なものというより、人事部門の責任または長期的な目標と見なしているのでしょう。しかし、後で詳しく説明するように、十分な訓練を受けたセキュリティ担当者は、レジリエンス（復元力）のある組織にとって重要な成功要因となります。

ご想像のとおり、サイバーレジリエンスに含まれるものは何かという認識は、経験によって形成されます。先程、回答者の 62% がレジリエンス（復元力）に影響を与えるセキュリティインシデントを経験していると述べたことを思い出してください。図 6 によると、これらの事象がきっかけとなって、優先順位が入れ替わった可能性があります。

図 6：サイバーレジリエンスの成果に対する組織での重要性の認識度合いを、過去にインシデントがない組織と過去にインシデントがある組織で比較した場合の順位

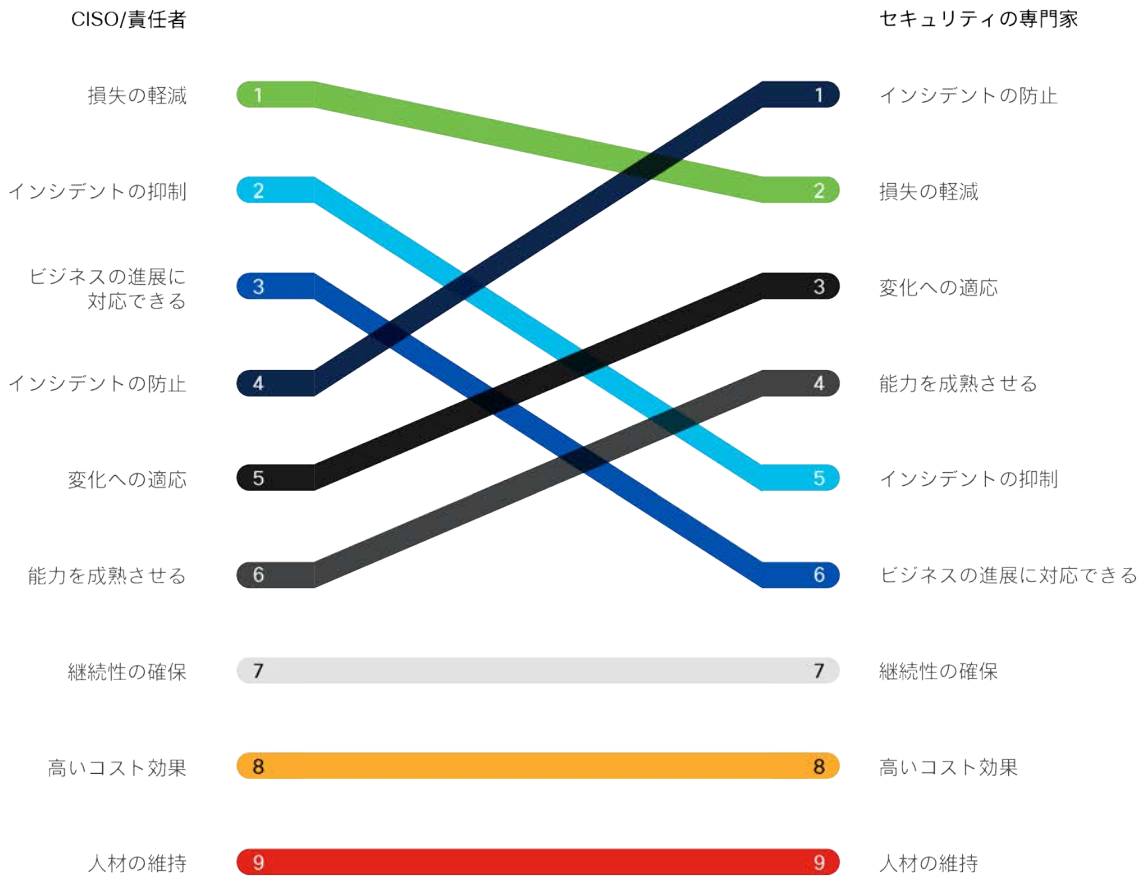


出典：『シスコセキュリティ成果レポート』

損失の軽減は、大きなインシデントが発生していない組織では 4 位でしたが、インシデントを経験した組織では 1 位に上昇しました。変化する事象に適応し、ビジネスの成長についていくことについても上昇しています。インシデントの防止や能力の成熟は後回しにされています。

また、サイバーレジリエンスの認識が人口統計的特性や企業統計的特性によって異なるかどうかも気になるところです。ここでもデータは肯定的な答えを出しています。ここでは、回答者の役割でふるいにかけて、CISO およびセキュリティ責任者と、技術的な役割を持つセキュリティ専門家を比較しています。

図 7 : サイバーレジリエンスの成果の重要性における職務別認識ランキング

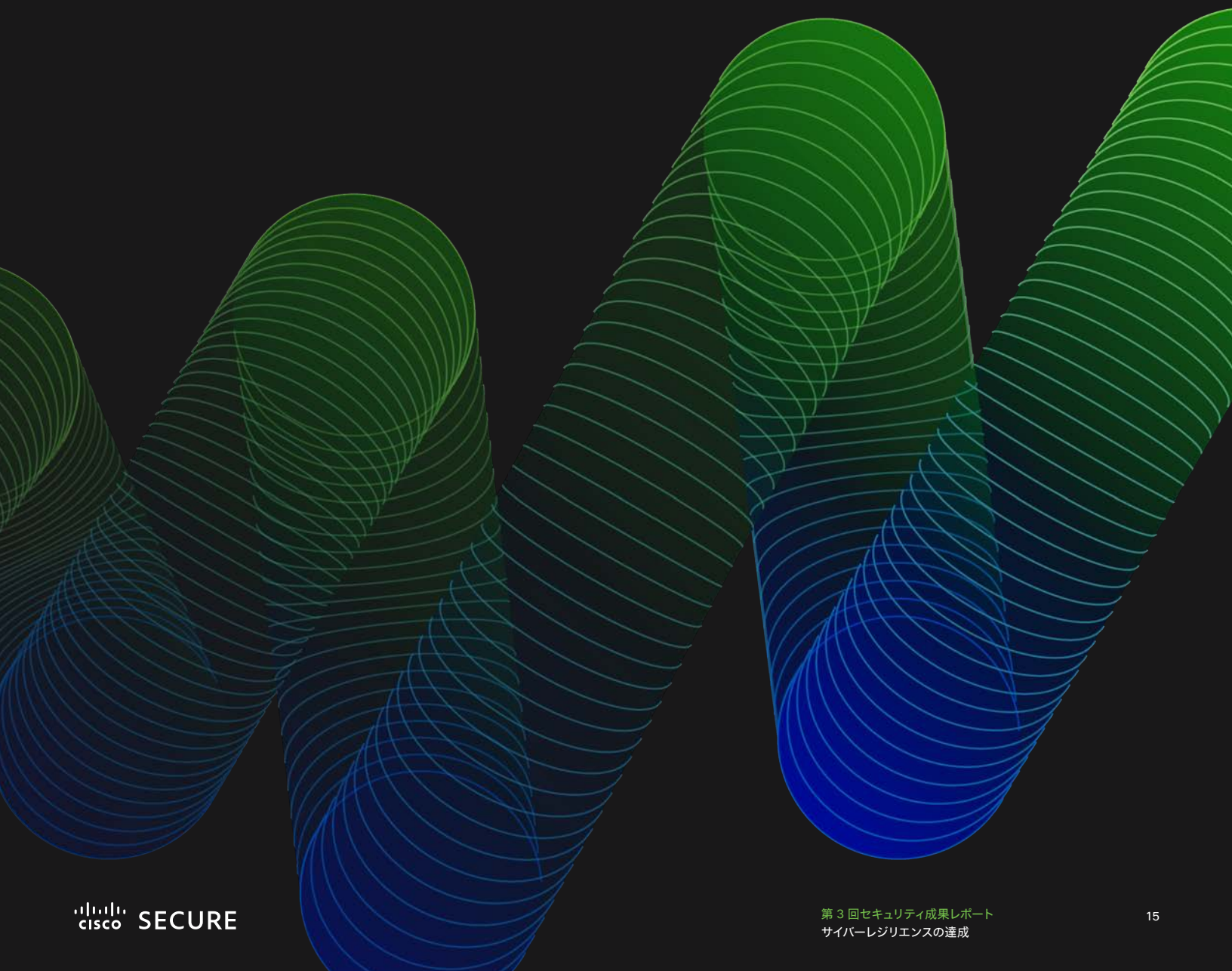


出典：『シスコセキュリティ成果レポート』

最初から意見の違いが見られます。セキュリティリーダーは、経済的損失の軽減、事象の拡大と範囲の抑制、ビジネスを妨げないことを優先します。一方、より技術的および運用上のセキュリティを担当する回答者は、それらをそれぞれ 2 位、5 位、6 位にランク付けし、重大なインシデントの防止を最も重要視しています。どちらのグループが正しいか、間違っているかということではありません。それぞれのグループがサイバーレジリエンスの異なる側面に焦点を当てるのは当然のことです。しかし、より良い成果を達成するために全員がチームとして機能するには、共通の優先順位を確立し、責任を明確にしておくことが適切と言えるでしょう。

「私たちは、ファイブナイン (99.999%) の稼働率を維持するシステムを構築するという、時代遅れの概念を持っています。サイバーレジリエンスについては、システムが失敗しても、技術的な問題があっても稼働し続けるように (システムを) 構築することを目指しています。」

– Dave Lewis
(Cisco Secure アドバイザリ CISO) との対談



サイバーレジリエンスの状態

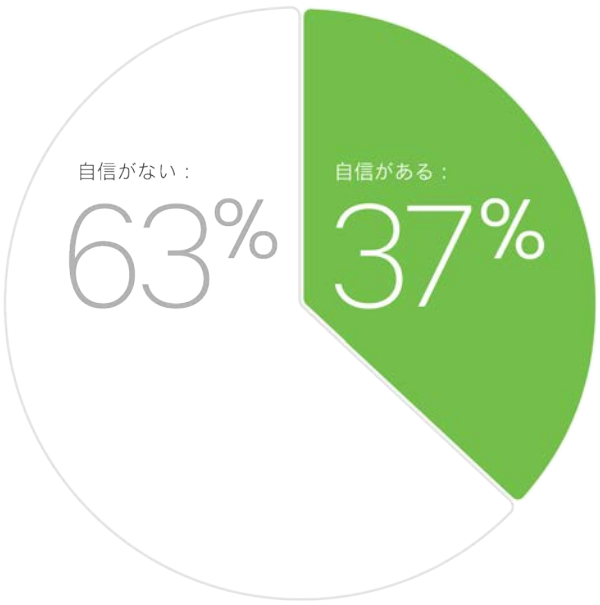
私たちは回答者に、最悪の（とはいえ、起こり得る）サイバー事象が今日発生した場合に、組織にレジリエンス（復元力）を維持できる自信がどの程度あるかを尋ねました。

3 分の 1 強が強い自信を示し、残りの 3 分の 2 は、組織の状態についてある程度の疑念を表しています。

こうした主観的な質問は、サイバーレジリエンスの状態を興味深く状況分析するのに役立ちますが、目標を達成したいのであれば、もっと具体的に評価する必要があります。回答者から、望ましいサイバーレジリエンスの成果に関する情報を得たので、これらの成果の達成という観点から、組織の現状を調べます。

回答者に、各目標に対する組織のパフォーマンスを 4 段階（失敗｜苦労｜順調｜優秀）で評価してもらいました。より客観的に評価できるようにするために、各成果の説明と、失敗例と優秀例も紹介しました。これらの説明と例は付録 B に掲載されていますので、詳細に興味のある方や、これらを組織に適応して使用してみたいと思われる方はご覧ください。

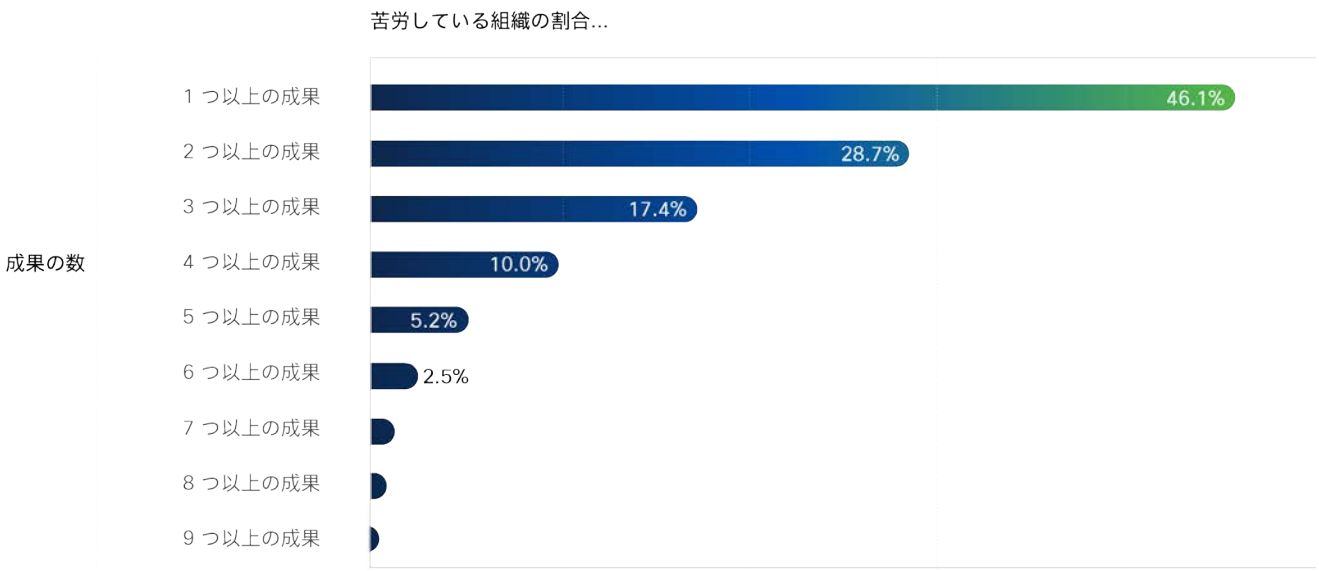
図 8：最悪のサイバー事象に対してレジリエンス（復元力）を維持できるかどうかに対する自信



出典：『シスコセキュリティ成果レポート』

一般に、回答者の大多数は、自分の組織を少なくとも「順調」と評価しています。しかし、だからといって、サイバーレジリエンスの世界ですべてが順調だという意味ではありません。図 9 に示すように、調査参加企業のほぼ半数が、9 つのサイバーレジリエンスの成果のうち少なくとも 1 つを達成するのに苦労しているか、完全に失敗していると述べています。4 分の 1 以上が 2 つ以上の問題を抱え、10% は少なくとも 4 つの成果が問題になっていると報告しています。以上のことから、サイバーレジリエンスの重要な分野で十分な成果を上げていない組織がたくさんあると結論付けられます。

図 9 : サイバーレジリエンスの成果に苦労している組織の割合



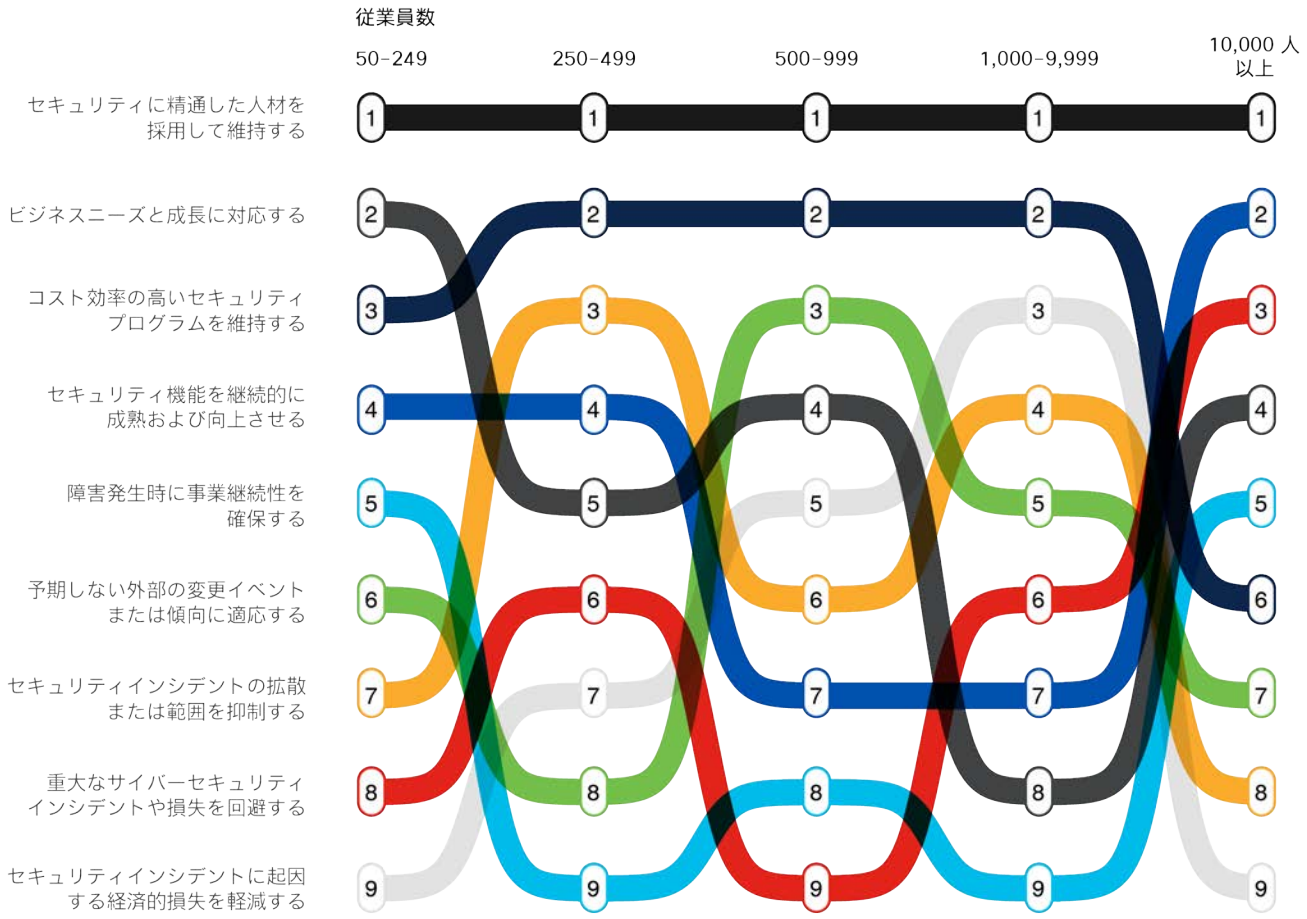
出典：『シスコセキュリティ成果レポート』

これまで見てきたとおり、これらのサイバーレジリエンスの成果の相対的な重要性に関する認識は異なっています。そのため、組織の種類によって状態が異なるのは当然とも言えるのです。たとえば、図 10 では、さまざまな規模の組織で、それぞれの成果に苦労している参加企業の割合を比較しています。セキュリティスタッフの採用と維持が最大の課題であることは、あらゆる規模の企業で共通認識となっていますが、その認識はそこで終わっています。

この見解は、組織が成長するにつれて、苦労する分野が変化するという意味で、特に興味深いと言えます。たとえば、経済的損失の軽減は、小規模な企業にとってはさほど難しくないと言われています（おそらく、損失を出すことよりも倒産することを心配しているからでしょう）。しかし、従業員数が 1,000 ～ 9,999 人の組織では、トップ 3 に次々と入り込んでいます。そして、大企業では最下位に位置しています（おそらく、高収益による余分な経済的保障があるからかもしれません）。

一方で、成長しても変わらないものもあるようです。前述のとおり、どの規模の組織も、セキュリティ人材の採用と維持に最も苦労しているようです。この成果は、サイバーレジリエンスにとって最も優先度の低い成果であると共通で評価されていることから、むしろ皮肉なことです。自己達成しつつある予言ということでしょうか？あるいは極端な実用主義かもしれません。（「優秀な人材を確保するのは大変ですが、それよりも大きなインシデントや損失を回避することの方がはるかに重要です。」）

図 10：組織の規模別にみるサイバーレジリエンスの成果ランキング



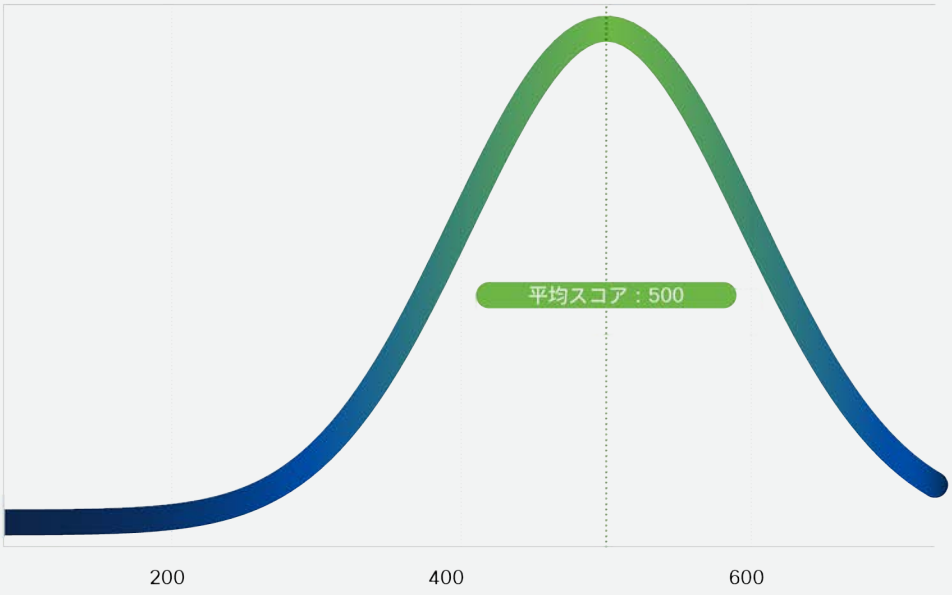
出典：『シスコセキュリティ成果レポート』

私たちは、個々の成果の状態を評価するだけでなく、参加組織ごとにサイバーレジリエンスを総合的に評価しようとしました。そこで、9 つの成果すべてにおける各組織の達成度に基づいて、サイバーレジリエンススコアを作成しました。その方法については、以下の注意事項をご覧ください。要は、スコアが高ければ高いほど、より多くのサイバーレジリエンスの成果において高い評価が得られるということです。次のセクションでは、このスコアを広範囲に使用して、サイバーレジリエンスの向上におけるさまざまな成功要因の有効性を測定します。

全体的なサイバーレジリエンススコアの測定

それぞれの成果を評価することに加えて、組織の全体的なサイバーレジリエンスの指標として、9 つの成果すべてにわたる達成度を把握するための集計スコアを求めることにしました。これは「サイバーレジリエンススコア」と呼び、このレポートでも何度も言及しています。

図 11：参加企業全体のサイバーレジリエンススコアの分布



標準化されたレジリエンススコア

出典：『シスコセキュリティ成果レポート』

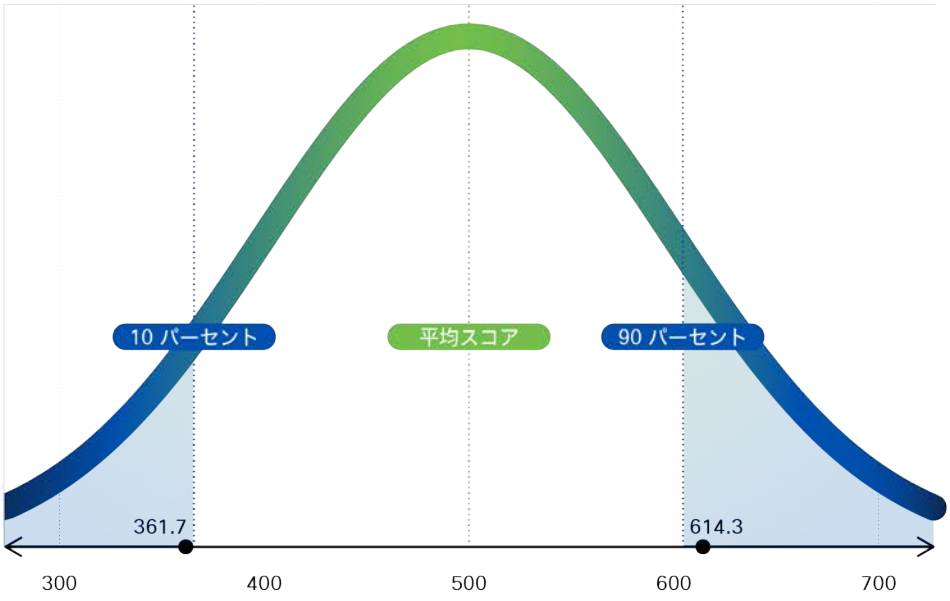
スコアの算出には「項目反応理論」という高度な統計手法を使用しました（前回のセキュリティ成果スコアについても同じことを行いました）。この手法を使用すると、各成果の達成難易度の違いを考慮しながら、すべての成果に対するパフォーマンスに基づいてスコアを算出することができます。標準化されたテストスコアはこの実証された手法によって算出されます。スコアの絶対値に特別な意味はありませんが、それぞれのプログラムを比較するのに利用できます。サイバーレジリエンススコアの分布を図 11 に示します。平均はちょうど 500 です。

レジリエンス（復元力）に必要な 7 つの成功要因

さて、いよいよお待ちかねのテーマになりました。4,700 以上の組織について、それぞれ 9 つの成果に関する総合的なサイバーレジリエンスを表すスコアが揃ったので、それを改善する方法を探っていきます。私たちは、組織、IT、およびセキュリティの潜在的な要因を分析し、それらがサイバーレジリエンスの強化とどのように相関するかをテストすることで、この課題に取り組みました。

そのプロセスを通じて、データに裏付けられたサイバーレジリエンスの 7 つの成功要因を特定しました。どれくらいの差があったのでしょうか？それをご説明します。これらの要因を満たす組織は、レポートの全参加企業で測定されたすべてのサイバーレジリエンススコアの上位 10% 以内に入りました。一方、大部分を満たしていない組織は、下位 10 パーセントに分類されます。誰もそのようなベンチマークを望んでいません。

図 12：7 つの成功要因を遵守することが総合的なサイバーレジリエンススコアに及ぼす影響



出典：『シスコセキュリティ成果レポート』

これらの成功要因を導入している組織では、レジリエンス（復元力）が 10 パーセントから 90 パーセントに急上昇している。

では、サイバーレジリエンスを強化するための幸運な 7 つの要因とは何ですか？また、あなたの組織はこれらの要因からどのような恩恵を受けられるでしょうか？それについては運としか言えません！デンゼル・ワシントンがかつて言ったように、「幸運とは、チャンスが訪れたときに、それに対する準備が整っている」ことです。このセクションの残りの部分が、その準備をする助けとなるはずです。

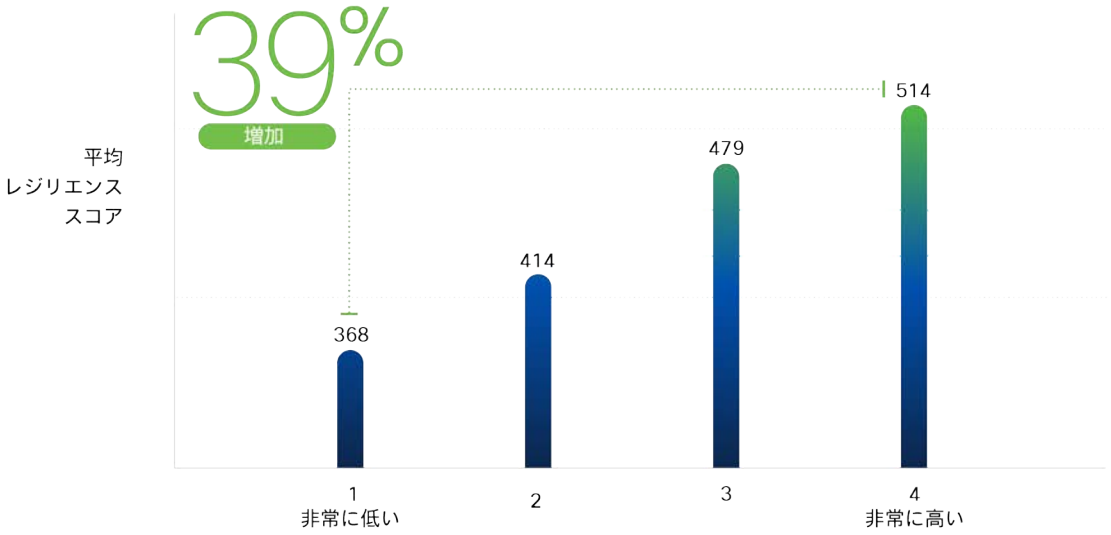
1. エグゼクティブサポートを確立する

確かに、この要因はサイバーセキュリティの世界ではかなり陳腐なものですが、その効果は一概に否定できるものではありません。組織の最高幹部からのサポートが不十分であると報告している組織のサイバーレジリエンススコアは、経営幹部からのサポートが強力な組織よりも 39% 低いという結果が出ています。もちろん、経営幹部のサポートをいかに獲得するかが真の難題です。

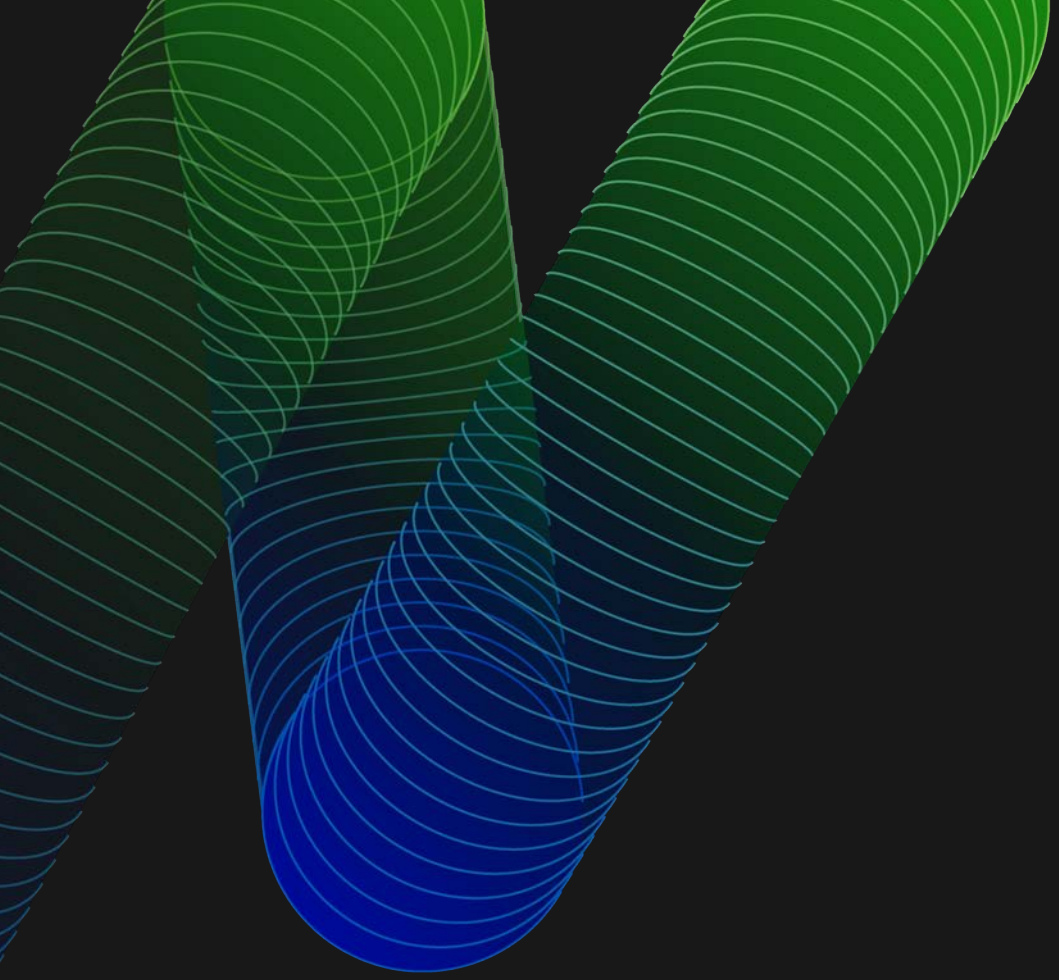
私たちのデータによると、ビジネスの中核的使命と緊密に連携しているセキュリティプログラムの方が経営幹部レベルのサポートが強力で、起動時のレジリエンス（復元力）が向上しています（総合スコアの 32% 増）。このように、ビジネスがどのように機能し、セキュリティイニシアチブがどのようにその機能を向上させるかをしっかりと理解した上で、経営幹部との架け橋が築かれます。結局のところ、どのような関係でもサポートは双方向です。

関係ということで、今回の分析から見えてきた点をもう 1 つ紹介します。サイバーレジリエンスの責任は組織図のどこにあるのかを回答者に尋ねました。そして、ほとんどの場合、レポートラインは大きな違いをもたらさないようです。しかし、CEO、CRO（最高リスク責任者）、CISO が密接に関与している組織は、他の C レベルの幹部（CIO、COO、CTO、CFO など）が全責任を負う組織よりもサイバーレジリエンススコアが大幅に高いことがわかりました。

図 13：サイバーレジリエンスに対するエグゼクティブサポートの効果



出典：『シスコセキュリティ成果レポート』



「CISO は経営陣との関係を強化する必要があります。ビジネスの整合性を高め、予算や人員について経営幹部の同意を得ることで、組織はサイバーレジリエンスを向上させることができます。良い関係は良いセキュリティプログラムにつながり、良いプログラムは素晴らしい関係につながります。」

– Wolfgang Goerlich
シスコ、アドバイザリ CISO

2. セキュリティの文化を育む

サイバーレジリエンスの向上を目指すリーダーは、経営幹部のサポートを確立することから始めるかもしれませんが、それだけにとどまるべきではありません。私たちのデータによると、セキュリティの文化を育むことができる組織では、セキュリティ文化が不十分な組織に比べてレジリエンススコアが 46% も向上することが示されているためです。

±46%
不十分なセキュリティ文化と優れたセキュリティ文化を持つ組織間の平均レジリエンススコアの差

しかしもちろん、言うは易く行うは難しです。そして、強力なセキュリティ文化とは何を意味するのか、そしてそれが私たちのレポートでどのように評価されたのかを尋ねるのは、妥当なことです。回答者が組織のセキュリティ文化の強さを評価し、格付けするために、以下のガイダンスを提供しました。

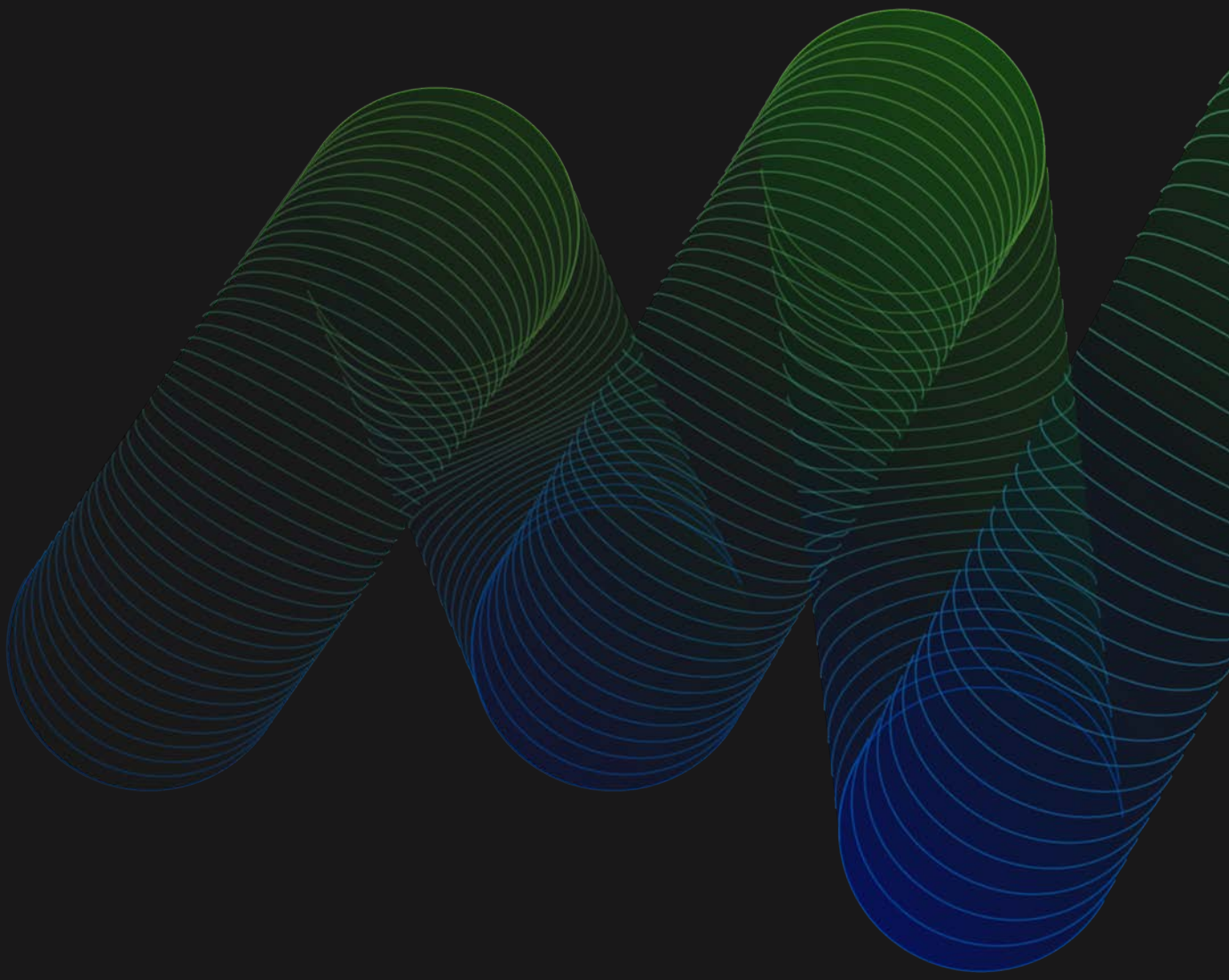
> 強力なセキュリティ文化では、従業員は問題の発生原因としてではなく、ソリューションの一部として扱われています。セキュリティ担当者は、組織の中での自分の役割を理解し、セキュリティ担当者以外のスタッフも自分たちの役割を理解しています。これは、フィッシング詐欺の疑い、潜在的なマルウェア、その他のインシデントを定期的に報告することからわかるかもしれません。従業員満足度調査や退職時のインタビューで、従業員からセキュリティ部門に対する否定的な意見が上がっていない。逆に、セキュリティポリシー違反や回避策が頻繁に生じる場合は、セキュリティ文化が不十分な証拠です。

これは、強力なセキュリティ文化がどのようなものかを徹底的に説明することを意図したものではありません。なぜなら、それは組織ごとに異なるためです。しかし、少なくとも、回答者がセキュリティ文化の強さを評価する際に何を念頭に置いていたかを示しており、うまくいけば、自社のセキュリティ文化を評価するためのアイデアを与えてくれます。

その説明の真意を理解すると、セキュリティプログラムではそのポリシーと理論的根拠を組織の他の部門に明確に伝えることが重要だと思われるかもしれません。その点で組織を高く評価している回答者は、自社のセキュリティプログラムが何をしているのか、なぜそうしているのかを明確に説明できないと答えた回答者に比べて、サイバーレジリエンススコアが 27% 向上しています。全員が異なる設計図を使用しているなら、強力な文化を構築することは困難です。

「セキュリティ意識は、セキュリティ文化を重視することに取って代わられ、トピックとしては消滅しつつあります。そして、組織の DNA を変革し、全従業員を大きなセキュリティファミリーの一員へと変えています。単純なトレーニングは、コンプライアンス実践の単なる確認作業と見なされる一方、組織の価値観を伝え、変革することは、今や多くの CISO によって主要な目標と見なされています。」

– Richard Archdeacon
シスコ、アドバイザリ CISO



3. リソースを確保しておく

これまで見てきたように、優秀なセキュリティ人材の採用と維持は、サイバーレジリエンスの成果としては重要度が最も低いものの、最も困難な課題であると広く認識されていました。過去のセキュリティ成果レポートでは、サイバーセキュリティ プログラムの柱である「人」に関連する測定可能な利点をいくつか指摘してきましたが、今回のレポートも例外ではありません。

意外なことに、組織内の総従業員数をコントロールしたとしても、セキュリティ担当者の全体的な規模とサイバーレジリエンスのレベルとの間に強い相関関係は見つかりませんでした。ただし、予期しないサイバー事象により適切に対応するために、余分な内部スタッフとリソースを確保していることが大きな違いを生んでいるようです。それができる組織は、必要なときに活用できる「柔軟な」リソースを持たない組織と比べて、平均で 15% 高いサイバーレジリエンススコアを達成しています。

では、基本的なセキュリティ人材の採用と維持がすでに困難な状況で、組織はどのように余分な内部リソースを維持すればよいのでしょうか？残念ながら、今回の調査ではその点について尋ねていませんが、今後の研究課題としてリストアップしています。

±15%

インシデント対応のために余剰な内部スタッフを確保している組織としていない組織との平均レジリエンススコアの差

±11%

外部インシデントサービスを利用している組織としていない組織との平均レジリエンススコアの差

予期しない事象に対応するために余分な内部スタッフを維持することが現実的でないとしても、まだ望みは残っています。また、外部のインシデント対応（IR）サービスを利用している企業では、サイバーレジリエンスが平均 11% 向上しているという分析結果も出ています。信頼できる IR サービスプロバイダーと契約を結び、電話一本でサポートを受けられるようにすることを検討してください。

余分な内部リソースにも外部の IR サービスにもそれぞれメリットがあるのだから、組み合わせればもっと良くなるのではないかと思うかもしれません。確かにそのとおりです。大規模なサイバー事象が発生した場合に備えて内部と外部の両方のリソースを準備しておくと、どちらか一方だけを使用する場合と比べて、サイバーレジリエンススコアがさらに 13% 上昇します。

4. ハイブリッドクラウド環境を簡素化する

クラウドアーキテクチャとクラウドへの移行は、IT チームとセキュリティチームの間でかなり以前から大きな話題となっています。インフラストラクチャからソフトウェアに至るまでクラウドに全面的に移行した企業も多くあれば、オンプレミス環境に頑なに固執する企業もあります。では、これらの戦略のうち、サイバーレジリエンスの助けとなるのはどちらでしょうか？答えは両方だと思いますか？

一般的に、IT インフラストラクチャがオンプレミスでホストされているか、それともクラウド（またはさまざまなレベルのハイブリッドモデル）でホストされているかを参加企業に尋ねました。そして、その回答と各組織のサイバーレジリエンススコアを関連付けました。クラウドを多用する組織の平均は 526 で、オンプレミスを多用する組織の平均は 525 でした。言い換えれば、オンプレミスを多用する環境とクラウドを多用する環境のサイバーレジリエンスの成果には差がないことがわかります。

±15%

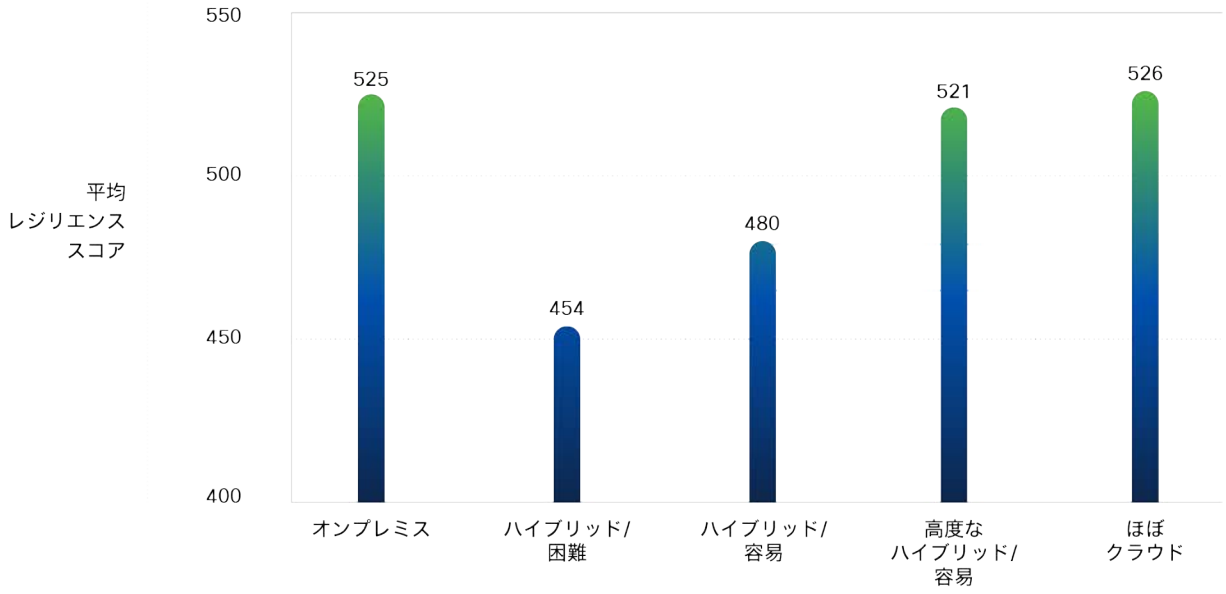
ハイブリッドクラウド環境において、管理しやすい環境と管理しにくい環境での平均レジリエンススコアの差

オンプレミス環境とクラウド環境の中間で差が見られています。ハイブリッドモデルの初期段階にある組織のサイバーレジリエンススコアは、オンプレミスが主流の組織よりも平均 14% 低くなっています。『恋はデジャ・ブ』（原題：Groundhog Day）のネッド・ライアソンが言うとおりです。「（クラウドへの）最初に一歩に気をつけなさい。それが難しいのです！」

しかし、クラウドへの最初の一歩を少しでも楽にできるという証拠もあります。別の質問で、ハイブリッド環境の管理と保護が容易であると評価した組織は、クラウド移行の初期段階にありがちなレジリエンス（復元力）への悪影響を緩和しているようです。レジリエンススコアは 14% ではなく、わずか 8.5% しか低下していません。さらに、クラウドの導入が進むにつれて、ハイブリッド環境の管理を簡素化できるメリットも大きくなります。

より広範なハイブリッド環境を持つ組織は、管理を簡素化できれば、オンプレミス（または完全にクラウド）の基準値と統計的に同等のレジリエンススコアを示しています。そうでなければ、せっかく獲得したレジリエンスも台無しになり、組織は管理が困難なハイブリッド状態に陥ります。全体として、管理が困難な初期のハイブリッドクラウド環境と、管理がより容易な高度なクラウド展開との間には、レジリエンススコアに 15% の差があります。

図 14：クラウドの導入と管理の容易さがサイバーレジリエンスに及ぼす影響

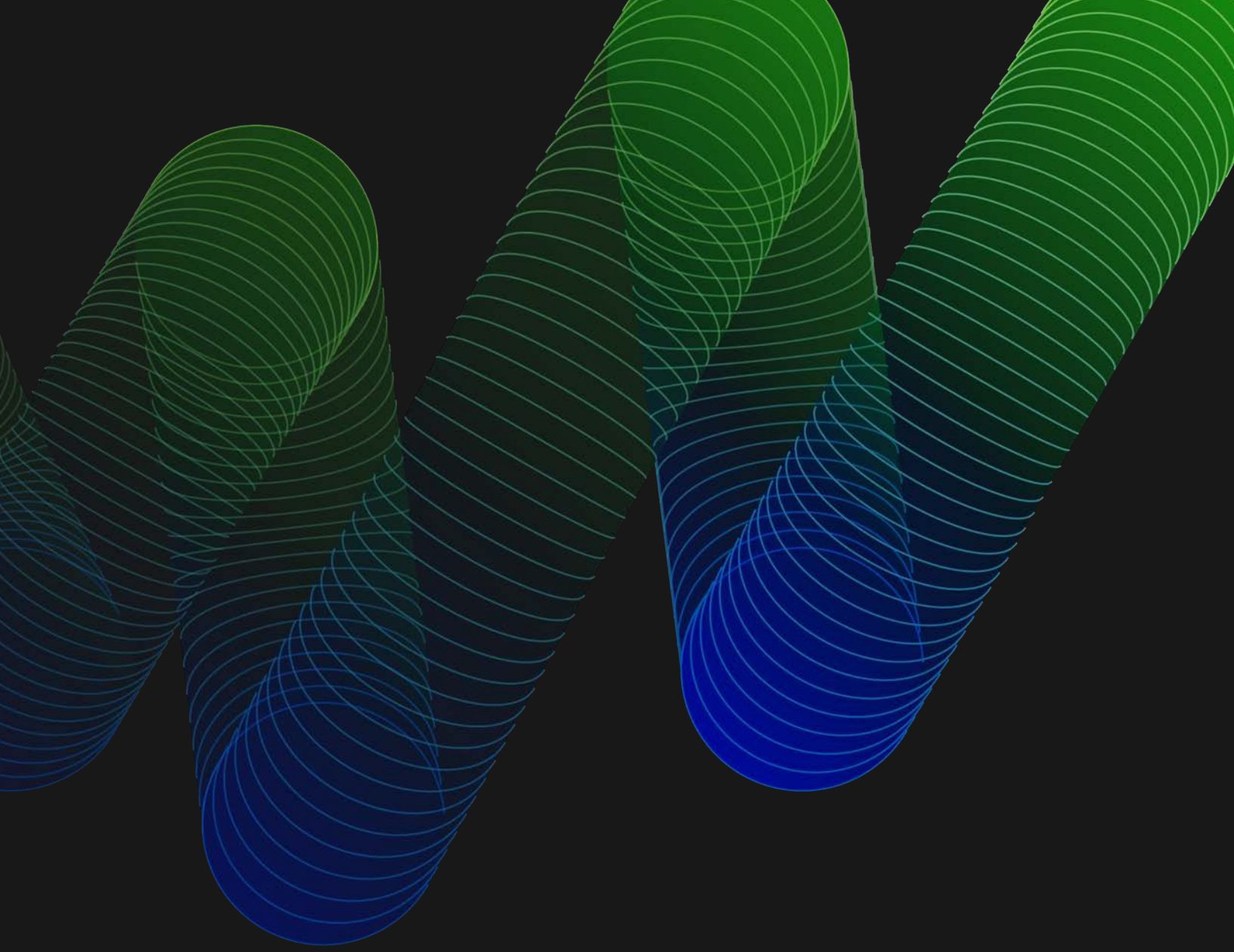


インフラストラクチャ移行のマイルストーン

出典：『シスコセキュリティ成果レポート』

このことから、シンプルで抵抗のない状態を維持することが、クラウドへの移行を成功させる重要な要因であると推測されます。ハイブリッドクラウドの導入はその取り組みの必要な部分であるため、これらの複雑な環境を管理するための適切なツールとサービスを用意することは、組織がその取り組みを通じて安全でレジリエンス（復元力）のある状態を維持するのに役立ちます。

ここで説明する一般的なパターンは、あらゆる規模の組織に適用されることに留意してください。どのような規模の組織であっても、クラウドとオンプレミスの両極端で、サイバーレジリエンスに測定可能な差はそれほどありません。しかし、中小企業も大企業も同様に、ハイブリッド クラウド インフラストラクチャのレジリエンスに苦労しています。1 つの違いは、大規模な組織ほど、自社の環境が複雑で管理が難しいと評価する割合が 3 倍になっていることです。このことは、クラウドへの移行が適切に管理されないと、サイバーレジリエンスに大きな打撃を与える可能性があることを意味しています。



「課題は、ほとんどの場合、セキュリティ（専門家）では組織がオンプレミスからクラウドに移行するスピードを操作することができないということです。
技術を変えられないなら、他に調整できるのは、人とプロセスだけです。」

– Helen Patton
シスコ セキュリティ ビジネス グループ CISO

5. ゼロトラストの導入を最大化する

今日のビジネス環境では、あらゆる場所で仕事を行えます。つまり、ビジネスを完全に保護するには、セキュリティがあらゆる場所に存在する必要があります。企業ネットワーク内のあらゆるもの（デバイス、ユーザー、インフラストラクチャなど）を信頼する従来のセキュリティアプローチでは、そのようなレベルの保護を提供できません。そこで、盲目的な信頼をなくすアプローチが生まれました。それがゼロトラストモデルです。これは、すべてのアプリケーションを保護するカスタム セキュリティ ポリシーにより、各アクセス試行の認証と継続的なモニタリングを通じて、ユーザーとデバイスの信頼を確立するというものです。

ここで、ゼロトラストモデルがサイバーレジリエンスを向上させるという証拠はあるのだろうか、という当然の疑問が生じます。そして、その質問に対しては、はっきり「はい」と答えることができます。成熟したゼロトラストを実装している組織は、その取り組みを開始していない組織と比べて、サイバーレジリエンスの評価が 30% 高くなっています。さらに、ゼロトラストは、先に説明した 9 つのサイバーレジリエンスの成果のうち、8 つの成果で成功率が明らかに高いことと相関していました。

±30%

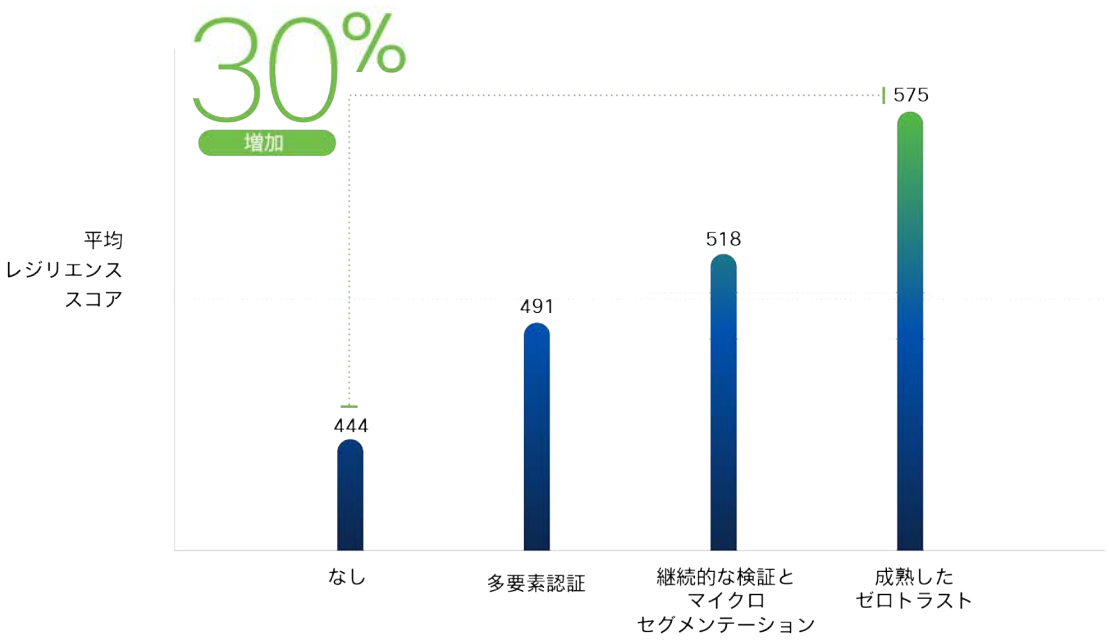
ゼロトラストを実装していない組織と成熟したゼロトラストを実装している組織の間の平均レジリエンススコアの差

成熟したゼロトラストの実装は一夜にして実現するものではありませんし、レジリエンス（復元力）のすべてのメリットを一度に得られるわけでもありません。長い道のりなのです。このレポートでは、その道のりの詳細な地図を作成することはできませんが、これから始めようと関心を寄せている方に役立つリソースがたくさんあります。これから、ゼロトラストの導入を成熟させることで得られる段階的なメリットを実証するために、いくつかの重要なステップに焦点を当てていきます。

多くの組織にとってゼロトラストの取り組みの最初の段階は、多要素認証（MFA）を介してユーザーとデバイスを検証することです。回答者の中で、MFA の導入は、サイバーレジリエンススコアの 11% の向上と相関しています。

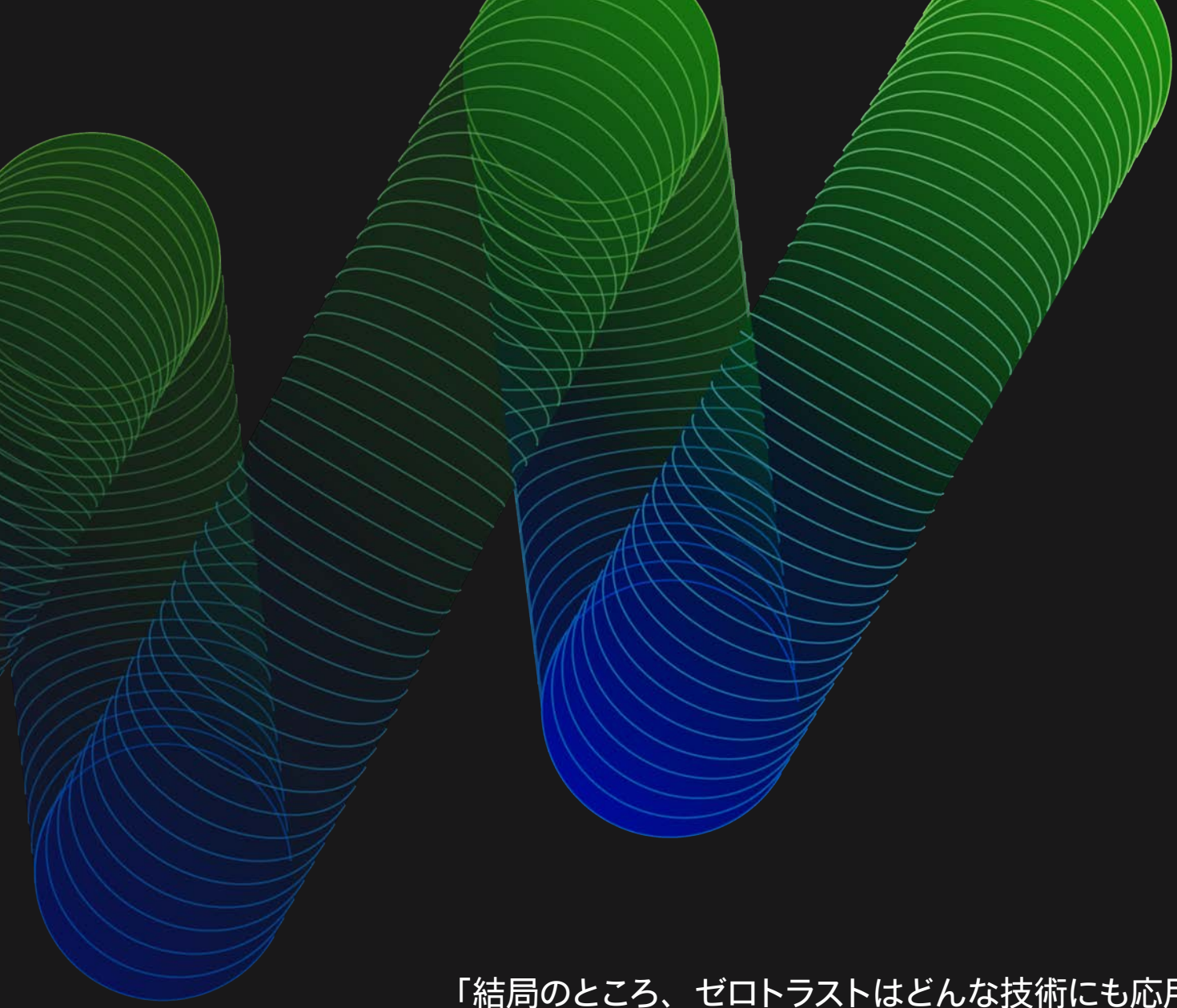
ゼロトラストの取り組みを継続している多くの組織は、ユーザーとデバイスの継続的な検証とともに、ワークロードのマイクロセグメンテーションも実施することにしています。当社のデータによると、そうした組織はサイバーレジリエンススコアがさらに 6% 向上しています。この増加は無視できません。ベーススコアが高くなるほど、大幅な増加率を達成するのが難しくなることに注意してください。

図 15：ゼロトラスト実装のマイルストーンがサイバーレジリエンスに与える影響



出典：『シスコセキュリティ成果レポート』

ゼロトラストの取り組みのもう 1 つのマイルストーンを見てみましょう。これはゴールに近づいています。ここで、組織は、MFA、継続的な検証、およびマイクロセグメンテーションを、適応型ポリシー、幅広いモニタリング、およびユーザーワークフローのオーケストレーションによって強化しています。その結果、ゼロトラストの「成熟した」実装と呼ばれるものが実現し、上記のサイバーレジリエンススコアの 30% の向上を完全に達成するのです。



「結局のところ、ゼロトラストはどんな技術にも応用できる哲学です。技術だけでは十分ではなく、選択した目的地までの道のりも組織によって異なるでしょう。その基本原則を実装するための適切な技術の組み合わせを見つけることが、最終的にはゼロトラストセキュリティのメリットを最大限に引き出し、よりレジリエンス（復元力）のあるビジネスを実現することになります。」

– Wendy Nather
シスコ、アドバイザリ CISO リーダー

6. 検出および対応能力を拡張する

最新の見出しに目を通すだけで、現代のサイバー脅威がさまざまなベクトルから侵入してくることがわかるでしょう。しかし、さらに納得のいく答えが必要な場合は、MITRE ATT&CK フレームワークにリストされている多数の攻撃者の手法（およびサブ手法）に真っ向から取り組むことができます。重要なのは、これらすべての戦術や手法を効果的に検出し、対応するには、複数の視点が必要になるということです。

Extended detection and response（XDR）は、ネットワーク、クラウド、エンドポイント、アプリケーション全体のデータを可視化し、分析と自動化を適用して、現在および将来の脅威を検出、分析、脅威ハンティング、および修復します。この先はどうなるのか、推測できるでしょう。では、検知および対応能力が拡張され、より多くの脅威ベクトルや企業資産を扱うようになったことで、サイバーレジリエンスは測定可能なレベルまで向上しているのでしょうか？それでは、結果を詳しく見てみましょう。

±45%

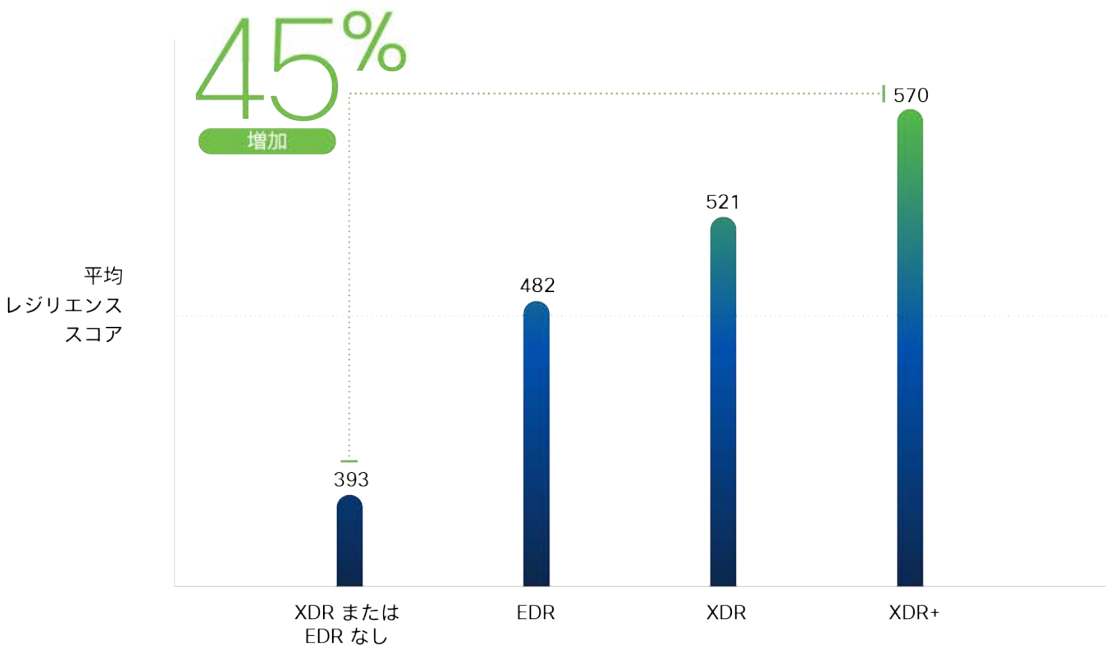
XDR を実装していない組織と導入が進んでいるより成熟した組織の間の平均レジリエンススコアの差

それを検証するために、XDR やその前身である Endpoint Detection and Response（EDR）でさえも進歩していない組織を対象に、基準値を設定します。これらの組織のサイバーレジリエンススコアは、平均 393 です。それを視野に入れると、これは全参加企業の中でサイバーレジリエンスが 14 パーセントに相当することを意味します。ほとんどの組織は現状で満足していないでしょう。

多くの人は EDR を XDR の基本的なコンポーネントと見なしているため、それをこの取り組みのマイルストーン #1 と考えます。EDR を導入したと報告した組織は、総合的なサイバーレジリエンススコアが基準値より 23% 向上しました。全然悪くありません。しかし、実際は XDR ではないので、このまま続けます。

XDR の基本要素を導入していると報告した参加企業は、EDR または XDR を導入していない組織と比べて、サイバーレジリエンススコアがさらに 10 パーセント高くなり、33% 上昇しました。「基本」とは、エンドポイントやネットワークでの検出および対応能力はあるが、まだすべてを統合していないことを意味します。

図 16 : XDR 実装のマイルストーンがサイバーレジリエンスに与える影響



出典：『シスコセキュリティ成果レポート』

機能を拡張することは素晴らしいことですが、セキュリティ運用に携わったことがある人なら誰でも、より広く、より深く可視化することで生じる課題についても理解しています。トリアージや対応が必要な事象が増え続けることで、見出しで目にするような多くのセキュリティインシデントが発生するのです。XDR の基本のコンポーネントを統合し、まとまりのあるソリューションにするためには、サイバー脅威インテリジェンスと自動化 / オーケストレーションという 2 つの主要な要素があると私たちは考えています。

検出および対応能力が最もよく機能するには、何をどのように探すべきかがわかっていなければなりません。そのために、多くの企業は質の高いサイバー脅威インテリジェンスを求めています。セキュリティの自動化とオーケストレーションは、成熟した XDR 実装をつなぎ合わせる役割を果たします。XDR を次のレベルに引き上げるために連携します。これらすべての機能を備えている組織は、9 つのレジリエンスの成果すべてでパフォーマンスが大幅に向上し、XDR に向けて前進していない組織と比べて、総合的なレジリエンススコアが 45% 優れていました。

7. セキュリティをエッジに

モバイルワーカー、デバイスの急増、複数のクラウドプロバイダーへのアプリケーションの超分散化など、ハイブリッドワークの加速により、ヒューマンスケールを超える広範な相互接続性を確保するための課題が増加しています。現在普及している安全な接続モデルでは、これらの課題に対処するには不十分です。その結果、エンドユーザーと IT プロフェッショナルは、自分たちの経験が断片的であり、かつ顕在化しているという現実に同様に直面します。

セキュア アクセス サービス エッジ（SASE）は、ネットワークとセキュリティをクラウド提供サービスに統合し、運用を簡素化し、絶え間なく変化するビジネスニーズに直面しながらレジリエンス（復元力）を維持するための戦略を提供します。当社のレポートから、SASE がレジリエンス（復元力）の向上と実際に相関しているという証拠はあるのでしょうか？もちろん！

±27%

SASE を実装していない組織と導入が進んでいるより成熟した組織の平均レジリエンススコアの差

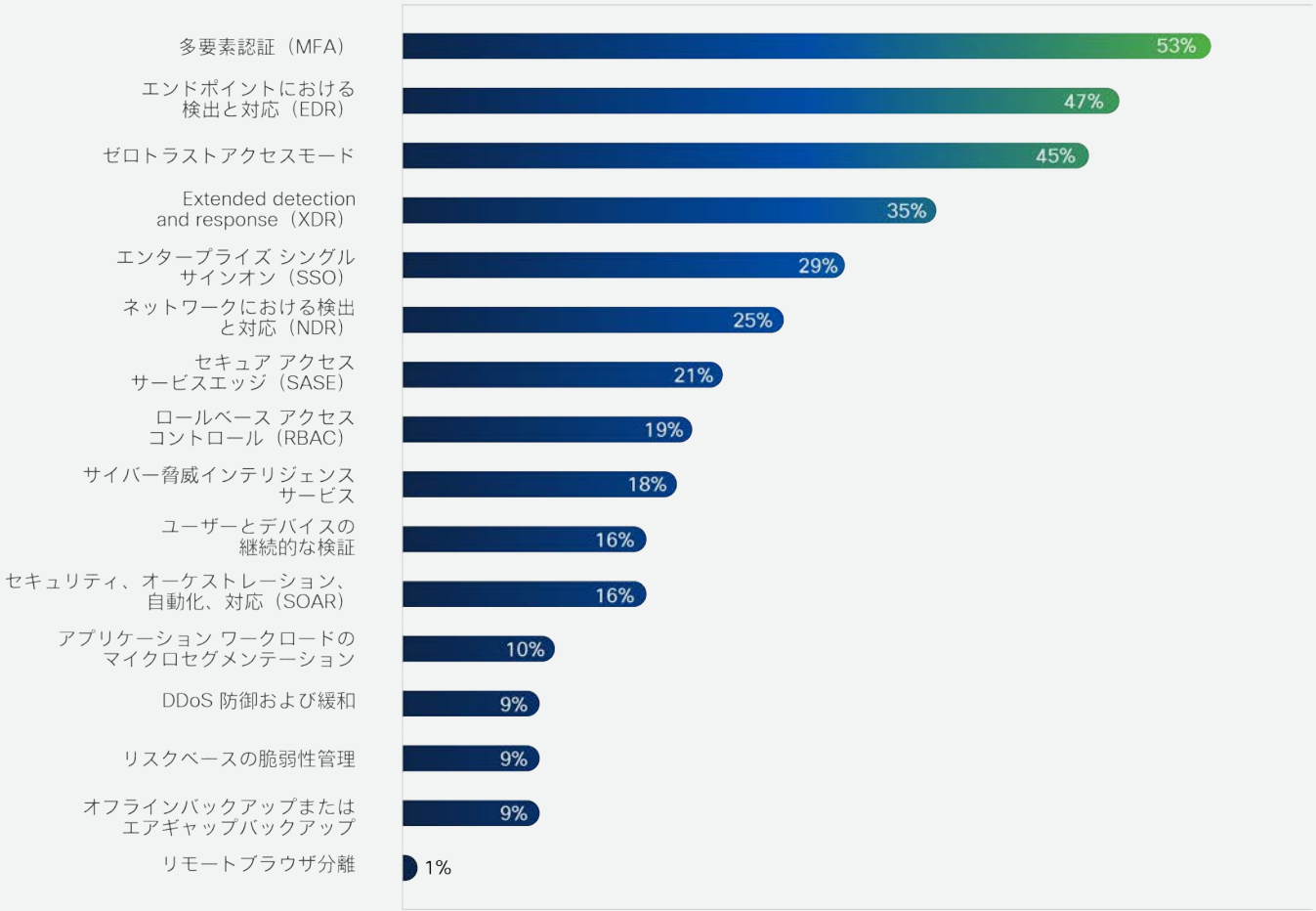
SASE 実装の従来のコンポーネントの具体的な内容については触れませんでしたが（Gartner 社の定義を参照）、実装する方向での一般的な進捗状況について参加企業に問い合わせました。SASE を導入していると回答した組織は、SASE を導入する予定や進展がない組織と比較して、全体的なサイバーレジリエンススコアが平均で 15% 高いことを示しています。また、SASE の実装は、9 つのそれぞれのサイバーレジリエンスの成果のうち 8 つにおいて、高い成功率と相関していることもわかりました。

ただし、シスコは Gartner 社の SASE の定義を拡張して、他のコンポーネントの中でも特に、高度な脅威検出と応答機能を組み込んでいます。これらの機能について尋ねた後、SASE の導入とともにそれらの機能を組み込んだ組織でさらにレジリエンス（復元力）が向上しているかどうかを確認したいと思いました。その結果、SASE を導入していない組織の基準値よりも 27% 高いスコアを獲得し、サイバーレジリエンスの新たな高みに到達したことが判明しました。

イニシアチブの一部を示す

この大規模な調査と並行して、IT およびセキュリティエグゼクティブのフォーカスグループを対象に、組織のサイバーレジリエンスを向上させるために現在取り組んでいるイニシアチブの上位 3 つを調べました。その内容を紹介します。

図 17：サイバーレジリエンスの上位イニシアチブ



出典：『シスコセキュリティ成果レポート』

サイバーセキュリティ（レジリエンス）フレームワーク

NIST サイバーセキュリティ フレームワーク（CSF）は、元々は重要なインフラストラクチャの保護を目的とした 2013 年の米国の行政命令の結果として作成されましたが、現在では世界中のさまざまな種類の組織がサイバーリスクの軽減とレジリエンス（復元力）の向上のために利用しています。このように幅広く利用されていることを踏まえ、サイバーセキュリティ フレームワーク（CSF）で定義されている関連活動が、9 つのサイバーレジリエンスの成果にどのように影響するかを評価することが有用であると考えました。

評価を実施するため、サイバーセキュリティ フレームワーク（CSF）で定義された活動から派生した 13 の能力のサブセットについて、各参加企業に実装レベルの評価を求めました。これらの能力は、サイバーレジリエンスとの潜在的な関連性に基づいて、当社の専門家によって選ばれたものです。次に、それぞれの能力とそれぞれのサイバーレジリエンスの成果との相関関係を判断するために、データを解析しました。その結果は、データ専門家がその才能を遺憾なく発揮した以下の効果マトリックスにまとめられています。

図 18：サイバーレジリエンスの成果と相関する NIST サイバーセキュリティ フレームワーク（CSF）の活動

	重要なシステムデータは追跡され、セキュリティ要件がある (ID.AM)	上位のサイバーリスクシナリオが特定され、評価されている (ID.RA)	応答能力には、セキュリティイベントの拡張が含まれる (RS.MI)	十分なサイバー保険が維持されている (N/A)	回復戦略には、広報の管理が含まれる (RC.CO-1、RC.CO-2)	応答/復旧テストには、サードパーティプロバイダーによるサービスが含まれる (RC.SC-5)	対応/復旧計画が定期的に更新されている (RS.IM、RC.IM)	サイバーイベント発生時/発生後のサービス提供を確保している (ID.BE-5)	対応/復旧計画には、外部関係者との調整が含まれる (RS.CO-4)	脅威検出機能は、潜在的なセキュリティイベントを把握できている (ID.AE)	対応スタッフは、セキュリティイベントに対処するための訓練を受けている (RS.CO-1)	応答機能により、イベントのタイムリーで効果的な調査が可能になる (RS.AN)	インシデント対応および復旧計画が存在している/知られている (RS.RP、RC.RP)
セキュリティインシデントの拡散または範囲を抑制する	10.6%	9.0%	8.6%	5.4%	5.4%	4.9%	5.3%						
セキュリティに精通した人材を採用して維持する	9.7%	7.2%	5.0%	5.8%	6.1%			4.6%				5.1%	
セキュリティインシデントに起因する経済的損失を軽減する	9.9%	8.4%	4.1%	5.0%	6.7%	4.4%	4.1%						4.7%
予期しない外部の変更イベントまたは傾向に適応する	10.7%	6.5%	6.2%	5.1%	5.4%	4.9%	4.6%	4.1%	4.2%			6.5%	
ビジネスニーズと成長に対応する	11.6%	8.3%	4.4%				4.7%	7.4%		8.9%		4.0%	4.7%
セキュリティ機能を継続的に成熟および向上させる	8.1%	6.9%	7.4%	4.9%	6.1%	5.8%	6.6%	4.5%	4.3%				
重大なサイバーセキュリティインシデントや損失を回避する	11.1%	8.2%	7.5%	4.9%				5.3%	4.7%	5.5%	4.3%		5.4%
障害発生時に事業継続性を確保する	7.9%	7.8%	4.0%	4.3%	4.2%	4.8%	4.0%		9.5%		5.2%	4.9%	
コスト効率の高いセキュリティプログラムを維持する	8.3%	6.8%		5.0%	5.7%	8.1%		4.6%	5.0%		5.5%	4.3%	

出典：『シスコセキュリティ成果レポート』

青い四角が表示されている場所は、NIST の能力とサイバーレジリエンスの成果が交差していて、統計的に有意な相関があることを意味します。これらの青い四角の中のパーセンテージは、その能力を最も効果的に実装している組織においてその成果を達成する可能性の高さを表しています。言い換えれば、主要なシステムとデータの追跡に優れている組織は、セキュリティインシデントの拡散と範囲を抑制する効果が優れている可能性が約 11% 高いということです（左上の四角）。その他もすべて同じように解釈できます。

本シリーズの第 1 回で紹介した最初のセキュリティ成果マトリックスと同様に、このチャートも「自分で道を決めるアドベンチャー」のようなものです。レジリエンス（復元力）の成果を向上させる具体的な方法を知りたい場合は、左側の項目を選択し、それを達成するためのデータに基づく選択肢をくまなく調べてください。一方、サイバーセキュリティ フレームワーク（CSF）内の特定の活動が組織のレジリエンス（復元力）を強化する方法について興味がある場合は、一番上の項目を選択し、交差する成果のリストを順に調べてください。

その精神で、私たちはマトリックスを使った独自のアドベンチャーを選び、以下のような考察を導き出しました。これは決して唯一の結論というわけではありません。また、皆さんの探求心を損なったり、偏らせたりするものでもありません。ですから、私たちの見解を知りたくないという場合は、「まとめ」に進んでください。

観察 1

何を防御しているのか、何に対して防御しているのかを知る

これは「システムにパッチを当てれば良い」という方針に沿ったセキュリティの常套句です。そして、この概念は、多くの PowerPoint スライドの「重要資産を保護する」といった言及や、孫氏の兵法の引用に現れています。しかし、それには正当な理由があるのかもしれません。

ここでデータのメッセージを無視することはできません。主要なシステムとデータを追跡することは、全体として最も効果的な活動の第 1 位に該当します。上位のサイバーリスクシナリオを特定することは第 2 位です。つまり、NIST サイバーセキュリティ フレームワーク（CSF）の識別機能に該当する 2 つの活動は、通常、レジリエンス（復元力）に関連付けられている検出、対応、回復などの機能よりも、サイバーレジリエンスを向上させる効果が大きい可能性があるということです。つまり、考える材料（と行動！）です。

観察 2

サイバーレジリエンスは自分だけの問題ではない

サイバーセキュリティ フレームワーク（CSF）の活動のうち、レジリエンス（復元力）の成果と相関するものを見直すと、組織の成功のかなりの部分が外部関係者と結び付いているという印象を受けます。十分なサイバー保険で防御をバックアップすることは、全体の 4 位にランクインしています。インシデント対応および復旧プロセスにおける PR の管理は 5 位にランクインしています。重要なサードパーティサービスのテストは 6 位に入り、サイバー事象中にも継続的なサービス提供を保証することが 8 位です。最後に、外部関係者との対応計画の調整が 9 位に入りました。

ぜひ、予期しない破壊的なサイバー事象に備えて、準備を整えてください。そのときが来ても、無防備でいることがないようにしてください。このデータともに、実際の経験が、サイバーレジリエンスの真の範囲が自社の境界線や人をはるかに超えていることを明確に示しています。

観察 3

人と計画の ROI は高い

最後に「人」について言及しましたが、これは前述のマトリックスから浮かび上がるもう 1 つのテーマにつながっています。つまり、複数のサイバーセキュリティ フレームワーク（CSF）の活動には、人または計画（人を念頭に置いて作成されたもの）が関与しています。

ある活動では、インシデント対応計画を作成し、従業員に周知することを定めています。また、別の活動では、計画を収集しただけで棚（または共有ドライブ）で埃をかぶせておくのではなく、定期的に更新することを必要としています。そして、外部関係者との連携を含めた対応計画の重要性についてはすでに述べたとおりです。もちろん、これらの計画を実行する方法について対応するスタッフが十分に訓練されていなければ、何の意味もありません。

組織がサイバーレジリエンスを向上させるのに役立つ技術的なソリューションは数多くあります。しかし、これらのソリューションの背後には、サイバー危機の際にそれらを設定、保守、および運用する人々がいます。何をすべきか、どのように行うべきかを彼らが理解できるように支援することが、組織を支援することにつながります。

観察 4

お金がすべてではないが …

… セキュリティイベントによる経済的損失を軽減することは、過去に重大なインシデントを経験した CISO や組織にとって最も重要なレジリエンス（復元力）の成果です。したがって、13 のサイバーセキュリティ フレームワーク（CSF）の活動のうち 8 つは、その成果を首尾良く達成する可能性を高めるという分析結果に注目するなら参考になります。

これらの活動をすべて列挙するつもりはありません。各自でそれを行い、NIST のドキュメントを参照して、追加の詳細と実装ガイダンスを確認することができます。マトリックスで強調されている効果的な活動は、ガバナンス、人、プロセス、および技術ベースのコントロールに及ぶということを強調しておきます。これは、損失を最小限に抑え、レジリエンス（復元力）を最大化するには、1 次元のポイントソリューション以上のものが必要だというテーマを裏付けています。

まとめ

おわかりいただけたでしょうか。レジリエンス（復元力）を感じていますか？少なくとも、レジリエンス(復元力) を獲得するための道を歩んでいるでしょうか？サイバーレジリエンスの構築には多大な労力が必要ですが、それは計画から始まります。

どんな事態が起ころうとも成功できるような組織を作るために、私たちは計画の策定と実行をサポートし、混乱を明晰さに変えるお手伝いをします。リスク評価、ランサムウェア、法規制の遵守、対応とリカバリ、またはその他のセキュリティ上の課題に取り組んでいる場合でも、1 人で取り組む必要はありません。

さらに洞察を得る方法：

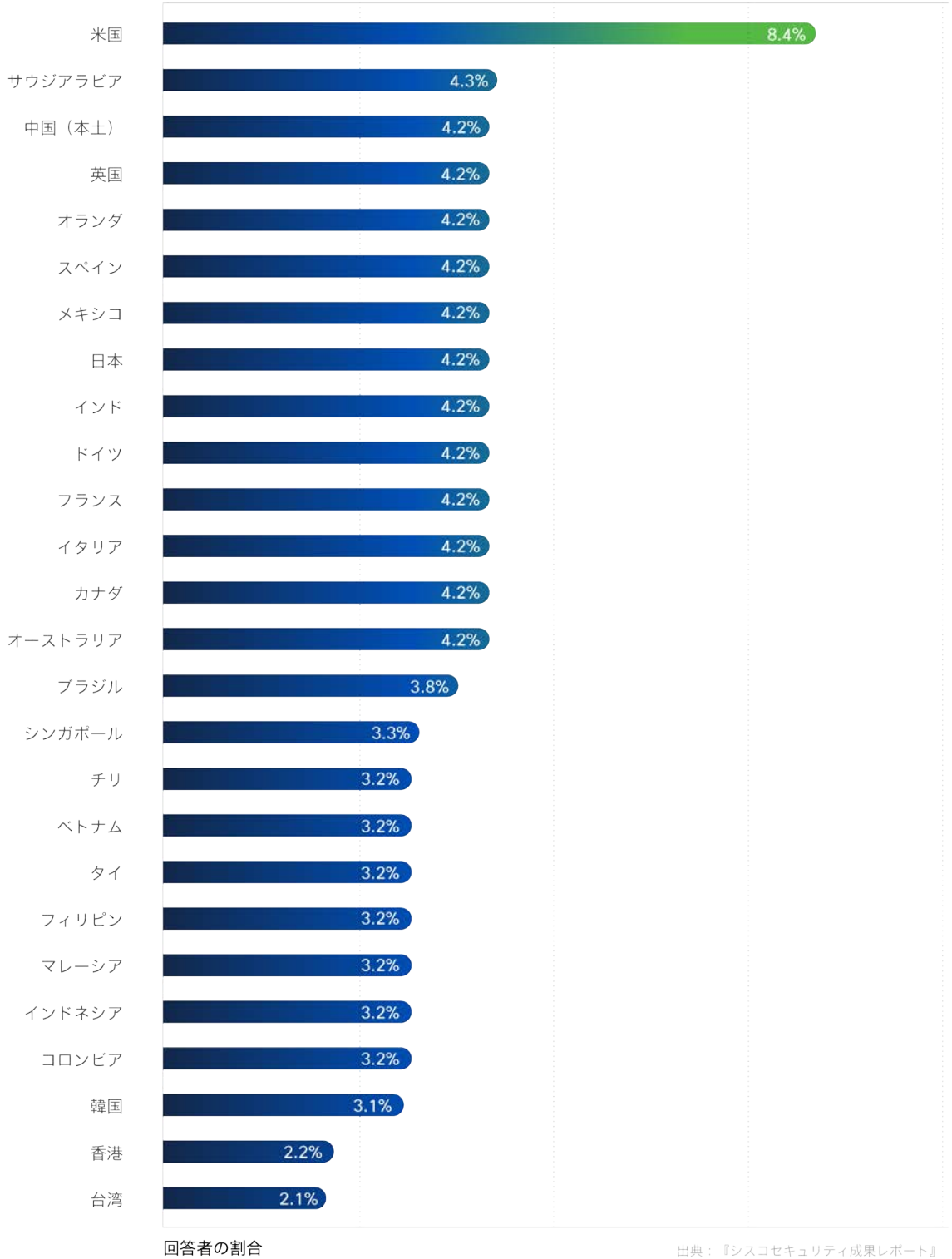
- 一連の調査とそのデータに基づく研究について確認する
- サイバーレジリエンスでビジネスを保護する方法の詳細を調べる

Cisco Secure について

Cisco Secure は、最高水準のセキュリティを目指して開発されています。導入、管理、使用が簡単な、顧客中心の合理化されたアプローチを通じてセキュリティを確保できるだけでなく、すべての要素が連携して機能します。Fortune 100 社のすべての企業に最も包括的で統合されたプラットフォームを提供し、どこにいても安全に仕事が行えるように支援しています。シスコのソリューションがエクスペリエンスをどのようにシンプル化し、成功を加速させ、未来を保護するかについては、cisco.com/go/secure をご覧ください。

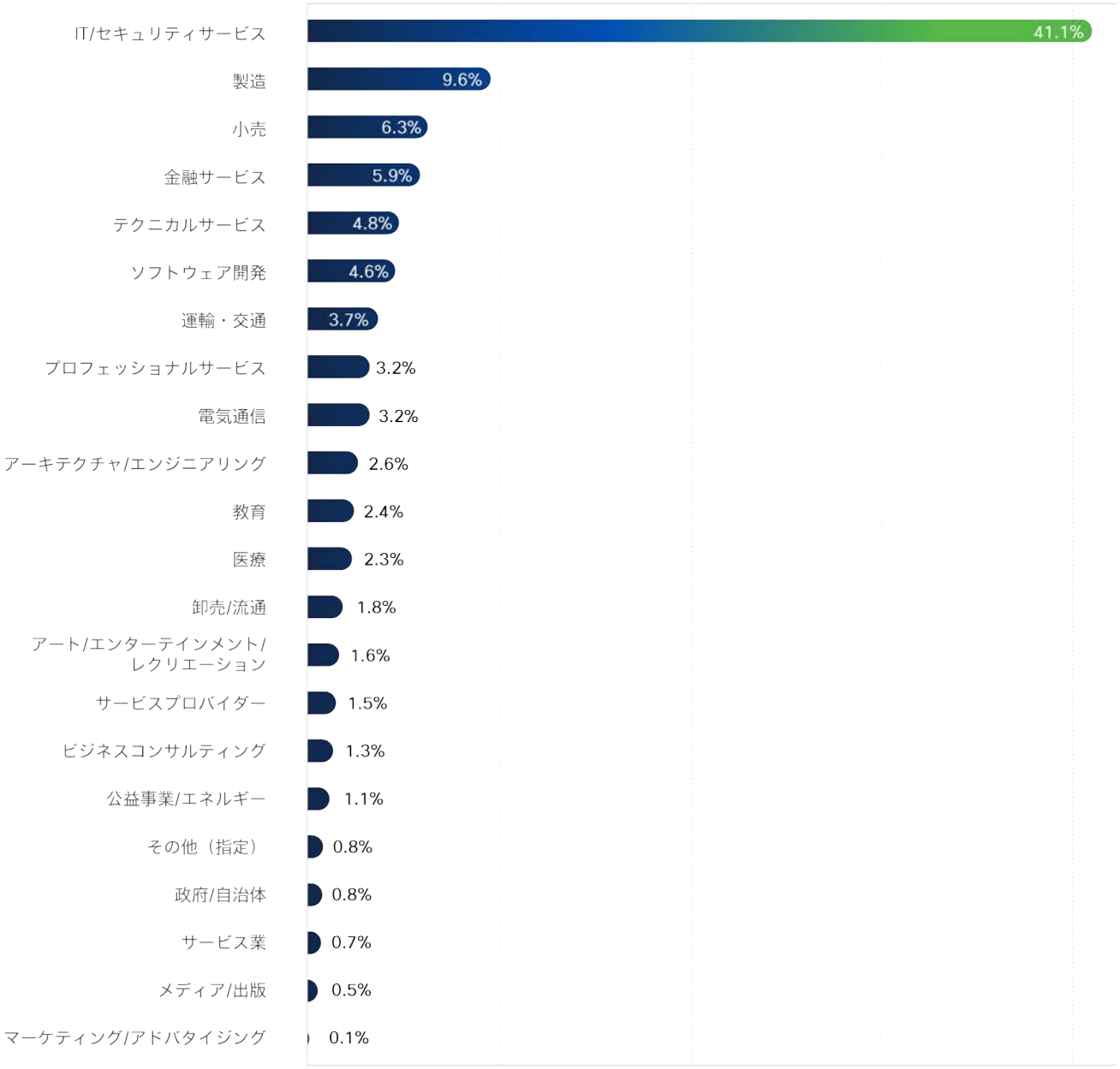
付録 A：
参加企業の内訳

図 A1：参加企業が主に働いている市場



出典：『シスコセキュリティ成果レポート』

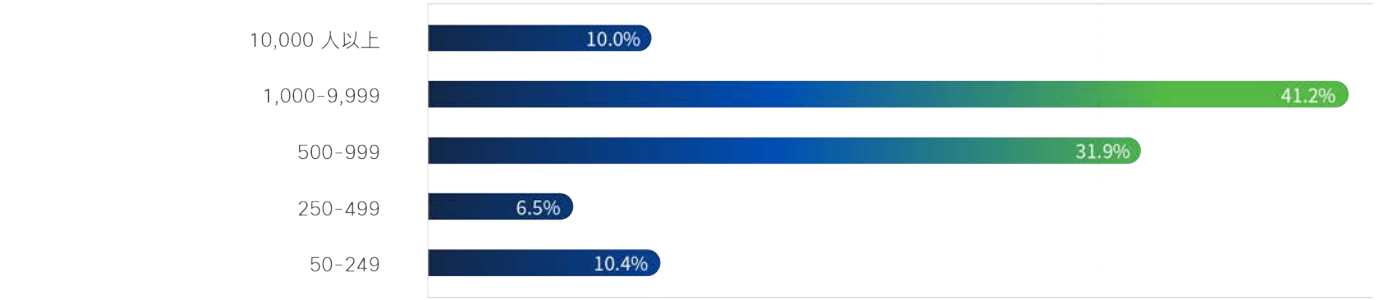
図 A2 : 参加企業の業種



回答者の割合

出典：『シスコセキュリティ成果レポート』

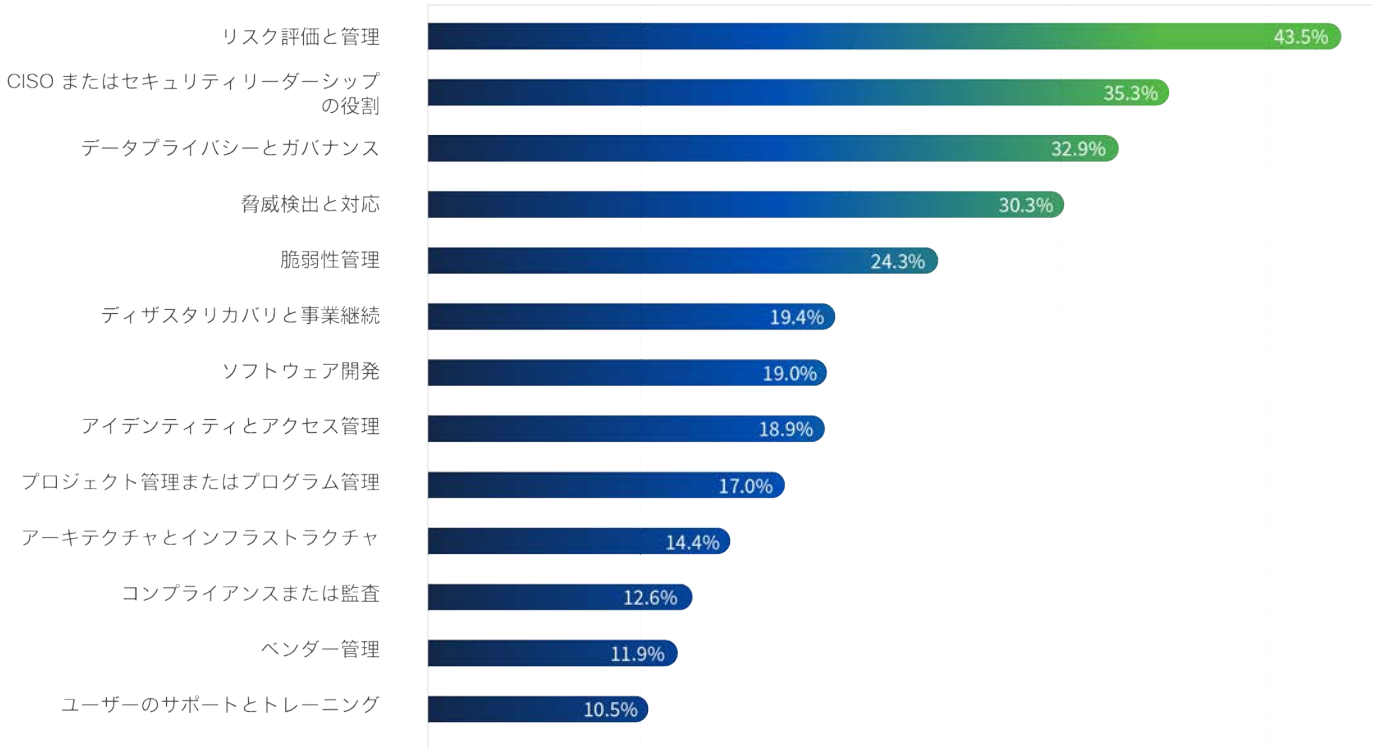
図 A3 : 参加企業の従業員数



回答者の割合

出典：『シスコセキュリティ成果レポート』

図 A4 : 参加企業のセキュリティにおける主な役割と責任



回答者の割合

出典：『シスコセキュリティ成果レポート』

付録 B：
サイバーレジリエンスの成果

1. **セキュリティインシデントの拡散または範囲を抑制する：**セキュリティインシデントが発生した場合、その範囲は、横方向への移動、権限の昇格、滞留時間、他の部門への伝播などを制限するコントロールとプロセスによって抑制される。さらに大きくなっていた可能性のあるインシデントを阻止した実績や、これらの能力を検証する最近のテストは、ここでの成功の指標になる。

2. **セキュリティインシデントに起因する経済的損失を軽減する：**セキュリティインシデントが発生した場合、影響の範囲と関連する損失を軽減するコントロールとプロセスによって、コストが削減される。たとえば、迅速な回復、ブランドへのダメージの抑制、他者に対するダウンストリームの損失の低減、訴訟の回避、サイバー保険によるリスク移転などの計画や手順が含まれる。最良の結果を期待することや「起きるかもしれないことに対処する」という戦略は、この目標の達成に苦労していることの表れである。

3. **予期しない外部の変更イベントまたは傾向に適応する：**セキュリティプログラムは機敏であり、組織外の不測の事態や制御不能な事象によって引き起こされる状況の変化に効果的に対応できる。コロナ禍でのリモートワークフォースへの突然の移行にうまく適応し、その後のハイブリッドワークの傾向に対処し、デジタル トランスフォーメーションを加速していることは、成功の証となる。

4. **ビジネスニーズと成長に対応する：**セキュリティプログラムは変化するビジネスニーズに柔軟に対応できていて、収益向上の妨げになっていない。セキュリティが競争上の優位性を獲得するのに役立ち、セキュリティ自体が収益を生み出す場合もある。経営陣がセキュリティをビジネスの障害と見なしたり、純粋にコストセンターと見なしたりしている場合は、この目標の達成に苦労していることの表れである。

5. **セキュリティ機能を継続的に成熟および向上させる：**セキュリティプログラムは、目標を設定し、進捗状況を追跡し、時間の経過とともにその有効性を継続的に改善することを目指す。プログラムはまだすべての分野で成熟していないかもしれないが、最も改善する必要がある分野を理解し、そこに到達するための計画を立てる必要がある。現代の脅威に遅れをとっている停滞したセキュリティプログラムや、次の対策を実施したら「終わり」という哲学は、この目標の達成に苦労していることの表れである。

6. **重大なサイバーセキュリティ インシデントや損失を回避する：**この目標を高い水準で達成できている組織は、過去数年間に（社内外で大きく取り沙汰された）深刻な、あるいは非常に大きな影響を与えるセキュリティインシデントを経験していない。また、いずれ大規模な漏洩が発生するだろうと考えるに足る理由も存在しない。軽微なインシデントや中規模なインシデントは別として、新聞の見出しになるような大問題が過去に起きておらず、将来も起こらないかどうかを尋ねることがこの質問の意図である。

7. **障害発生時も事業継続性を確保する：**システム障害、ネットワークの停止など、技術的な中断が発生しても、重要な業務への影響は最小限にとどまる。組織は、大規模または急速なアーキテクチャおよび / またはプロセスの変更を余儀なくさせるような突然の予期しない事象をうまく乗り切ることができる。

8. **コスト効率の高いセキュリティプログラムを維持する：**経営幹部は、セキュリティプログラムは ROI が高いと見なしている。セキュリティ関連のコストが高すぎるという不満の声が繰り返し上がっていない。購入後に十分活用されていないセキュリティ製品が少ない。スタッフは少人数だが、不測しているわけではない。経営陣とセキュリティリーダーの間でリスクを増やさずにセキュリティ予算を削減する計画が話し合われている場合は、この目標を達成できていることの表れと言える。

9. **セキュリティに精通した人材を採用して維持する：**セキュリティ プロフェッショナルのコミュニティで、あの会社は働きやすい職場だという評判が上がっている。過度なインセンティブを提示しなくてもセキュリティチームの欠員がたいていすぐに埋まる。有能なスタッフが去って行かずに昇進し、離職率が低い水準で維持されている。従業員満足度が常に高い。

CISCO
SECURE

米国本社
Cisco Systems, Inc.
San Jose, CA

アジア太平洋地域本部
Cisco Systems (USA), Pte. Ltd.
Singapore

ヨーロッパ本社
Cisco Systems International BV
アムステルダム、オランダ

2022 年 12 月発行

The bridge to possible