CISCO
SECURE

セキュリティ成果調査

Vol. 2

効果的なセキュリティ対策 実践方法
トップ 5

目次

トップ 5 の概要

シスコは 2021 年『シスコ セキュリティ成果調査』を実施し、サイバーセキュリティ管理において最も効果がある手法を探りました。25 種類の一般的なセキュリティプラクティス（対策）を取り上げ、11 種類のプログラムレベルの成果にどの程度寄与するかテストしました。このプラクティスと成果の相関性については、2021 年『シスコ セキュリティ成果調査』の Web サイトに掲載しているインタラクティブな図表でご確認いただけます。またレポート全体をダウンロードすることもできます。

テストの結果、25 種類のプラクティスのうち 5 種類が総合的な寄与度で他を圧倒していることが分かりました。この 5 種類のプラクティスは、測定したすべての成果にわたって満遍なくセキュリティプログラムの成功に寄与していました。

以下のページでは、セキュリティプログラムを成功に導くプラクティス「トップ 5」に焦点を当て、セキュリティ効果を最大限に引き出すための戦略を示します。「トップ 5」は以下のとおりです。

プロアクティブなテクノロジーの更新	プロアクティブなテクノロジーの更新戦略をとることで、最適な IT とセキュリティテクノロジーを常に維持している。
テクノロジーの十分な統合	セキュリティテクノロジーは適切に統合され、相互に連携して効果的に機能している。
タイムリーなインシデント対応	インシデント対応機能で、セキュリティイベントをタイムリーかつ効果的に調査して修復できる。
正確な脅威検出	脅威検出機能に重大な死角がなく、潜在的なセキュリティイベントを正確に把握できている。
迅速なディザスタリカバリ	リカバリ機能で、セキュリティインシデントの影響を最小限に抑え、影響を受けたビジネス機能のレジリエンスを確保できる。

これらのプラクティスがさまざまな側面に寄与することが分かると、次はその理由を知りたくなります。プログラムの成功にこれらが不可欠なのはなぜなのか。効果の高さを左右する要因は何か。これらのプラクティスをどのように実施すれば最大限の成果が得られるのか。今回の『セキュリティ成果調査』ではこれらの疑問を解き明かしていきます。

以下のページでは、セキュリティプログラムを成功に導くプラクティス「トップ 5」に焦点を当て、セキュリティ効果を最大限に引き出すための戦略を示します。シスコは今回の調査手段として 5,100 人を超す世界中の IT 担当者とセキュリティ担当者に対して二重盲検調査を独自に実施しました。得られたデータを詳しく分析して主な調査結果を抽出し、十分に吟味したポイントを紹介していますので、お客様のセキュリティをさらなる高みに押し上げるためにお役立ていただけます。

主な調査結果

27 か国の 5,100 人を超える IT 担当者とセキュリティ担当者に、セキュリティアーキテクチャの更新と統合、脅威の検出と対応、災害時のレジリエンス確保の各側面で採用しているアプローチについて質問しました。おかげさまで多くの方々からさまざまな知見、取り組み、戦略、成功例をお寄せいただきました。すべての回答を複数の方法で分析し、主な調査結果として以下の項目を抽出しました。

アーキテクチャの更新と統合

- 十分に統合された最新の IT は、他のどのセキュリティプラクティスやセキュリティ管理よりもプログラム全体の成功に寄与する。
- クラウドベースの新しいアーキテクチャは、ビジネスの進展に対応するための定期更新がはるかに容易である。
- 単一のベンダーから主に調達している企業は、統合されたテクノロジースタックを構築できる可能性が 2 倍になる。
- セキュリティテクノロジーが統合されていると、プロセスの高度な自動化を実現できる可能性が 7 倍になる。

サイバー脅威の検出と対応

- 強力なリソース（人材、プロセス、テクノロジー）に基づいて構築したセキュリティプログラムは、脆弱なリソースに基づく場合と比べてパフォーマンスが 3.5 倍になる。
- 脅威検出および対応チームは外部委託したほうが高い能力が得られるが、社内チームのほうが平均対応時間が短くなる（13 日間が 6 日間になる）。
- サイバー脅威インテリジェンスを広く活用するチームは、強力な検出機能および対応機能を持っていると回答する割合が 2 倍になる。
- 自動化を行うと、経験の少ない従業員のパフォーマンスは 2 倍以上になり、強力なチームはセキュリティの成果をほぼ確実（95%）に達成するようになる。

災害時のリカバリレジリエンス確保

- 事業継続とディザスタリカバリを取締役会レベルで監督している企業は、強力なプログラムを構築していると回答する割合が最も高い（平均を 11% 上回る）。
- 事業継続およびディザスタリカバリ機能が重要なシステムの 80% 以上をカバーするまで、ビジネスのリカバリレジリエンスを確保できる可能性は向上しない。
- 事業継続およびディザスタリカバリ機能を複数の方法で定期的にテストしている企業は、ビジネスのリカバリレジリエンスを確保できる可能性が 2.5 倍になる。
- カオスエンジニアリングを標準プラクティスにしている企業は、高いレベルのリカバリレジリエンスを得られる可能性が 2 倍になる。

本調査について

サンプリング	回答者	分析
シスコがデータ調査会社 YouGov 社に委託して 2021 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。	27 か国 5,123 人の現役の IT 担当者、セキュリティ担当者、プライバシー担当者から回答を得ました。サンプルの内訳については、付録を参照してください。	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。

5,123 人の現役の IT 担当者、セキュリティ担当者、プライバシー担当者が回答

27 ヵ国が対象

「安全を確保するためにあらゆる対策を実施することが必要です。攻撃は非常に高度になっており、しかも日々進化して新たな手口が生み出されています。デバイス、ユーザ、会社の安全を保てるようにあらゆるセキュリティ侵害を想定して攻撃対象領域を減らしたいと考えています。」

Eric J. Mandela (Allied Beverage グループ、
テクノロジー インフラストラクチャ担当アシスタントディレクター)

詳細はこちら

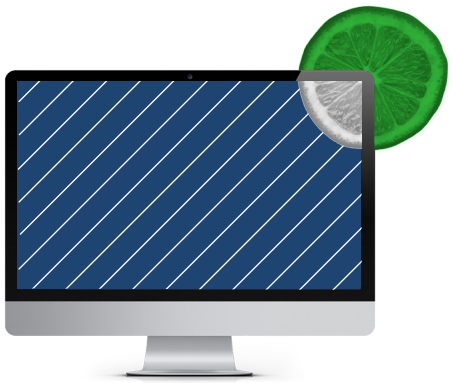
プロアクティブにテクノロジーを更新する戦略

前回の調査では、最適な IT とセキュリティテクノロジーを維持更新していくプロアクティブなアプローチが他のどのプラクティスよりもサイバーセキュリティ プログラムの成功に寄与することが分かりました。テストした 25 種類のプラクティスはいずれも「ベストプラクティス」であると一般に認められていることを考えると、この圧倒的な結果は注目に値します。そこで、このプラクティスが非常に効果的である理由をこの追跡調査で探ることにしました。

テクノロジー更新戦略を詳しく調べていく手始めとして、既存のインフラストラクチャの更新状況を確認しました。使用しているセキュリティテクノロジーのうち古くなっているものの割合を尋ねたところ、平均 39% のセキュリティテクノロジーが古くなっていることが分かりました。使用しているセキュリティツールの 8 割以上が時代遅れになっていると述べた回答者も 13% 近くに上ります。

この結果だけを見ても、プロアクティブなテクノロジーの更新戦略が多くの利点をもたらすことがお分かりいただけると思います。テクノロジーを更新すれば進化を続けるサイバー脅威に対抗できる高度な機能を獲得できる、という利点はよく知られていますが、それだけではありません。それらの点を解き明かす質問をいくつか行いましたので、詳しく見ていきましょう。

平均 39% のセキュリティテクノロジーが古くなっていることが分かりました。



インフラストラクチャの特性は更新イニシアチブに影響を与えるか？

最初の調査では、クラウドベースの最新のアーキテクチャのほうが管理が容易でネイティブのセキュリティ対策も備えているので効果が高くなると推測しました。今回はその仮説を検証するために、使用しているテクノロジー インフラストラクチャについて、次のような記述の中から該当するものを選択してもらいました。

- クラウドかオンプレミスか
- 最新か旧式か
- 統合型か分散型か

こうしたアーキテクチャの特性がテクノロジー更新機能の有効性に寄与しているかどうか調べたところ、図 1 のように明確に寄与していることが分かりました。**クラウドベースの最新の統合型アーキテクチャを使用している企業は、オンプレミスの古い分散型テクノロジーを使用している企業よりも、強力なテクノロジー更新機能があると回答する割合が 2 倍以上高くなります。**ただし、オンプレミス環境を主に使用していても、IT が最新であればパフォーマンスは依然として平均を上回っているわけなので、次のクラウド移行戦略会議でこの図を提示するつもりであれば注意が必要です。

もちろん、クラウドネイティブであればテクノロジー更新戦略を進めやすくなるのは事実です。ただそれよりも、古くなったアーキテクチャを使用していることのほうが問題としては深刻なのです。古いインフラストラクチャの更新が困難になっている場合は、新しいアーキテクチャに移行したほうが古いアーキテクチャを改良していくよりも成果が上がる可能性があります。もちろん、レガシー インフラストラクチャや重要なインフラストラクチャでは移行が不可能であるか費用対効果が低い場合もあるかと思いますが、ここで見た一般原則は同じように適用されます。

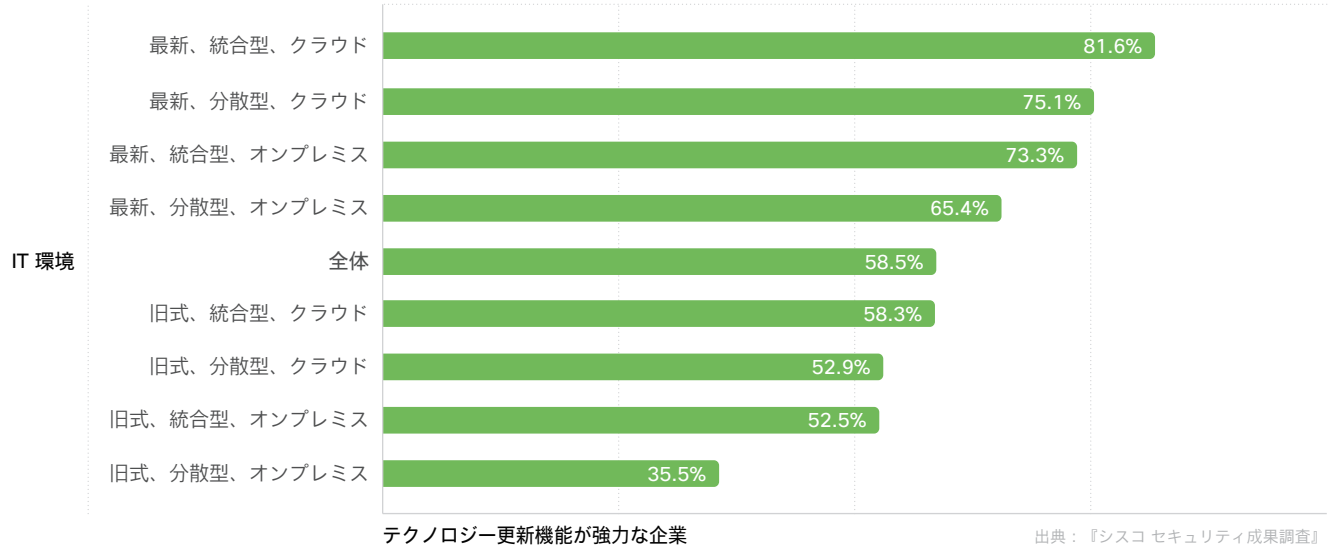


図 1：IT アーキテクチャの特性がテクノロジー更新パフォーマンスに与える影響

81.6% クラウドベースの最新の統合型アーキテクチャを使用している企業の 81.6% が、強力なテクノロジー更新機能があると回答

ビジネスの進展に対応できるセキュリティを獲得する上でアップグレード頻度は重要か？

2021 年『セキュリティ成果調査』によると、プロアクティブなテクノロジー更新戦略と最も相関性の強かった成果は、セキュリティプログラムがビジネスニーズと事業の拡大に対応できることでした。調査全体を見ても、このプラクティスと成果が最も相関性の強い組み合わせとなっていました。

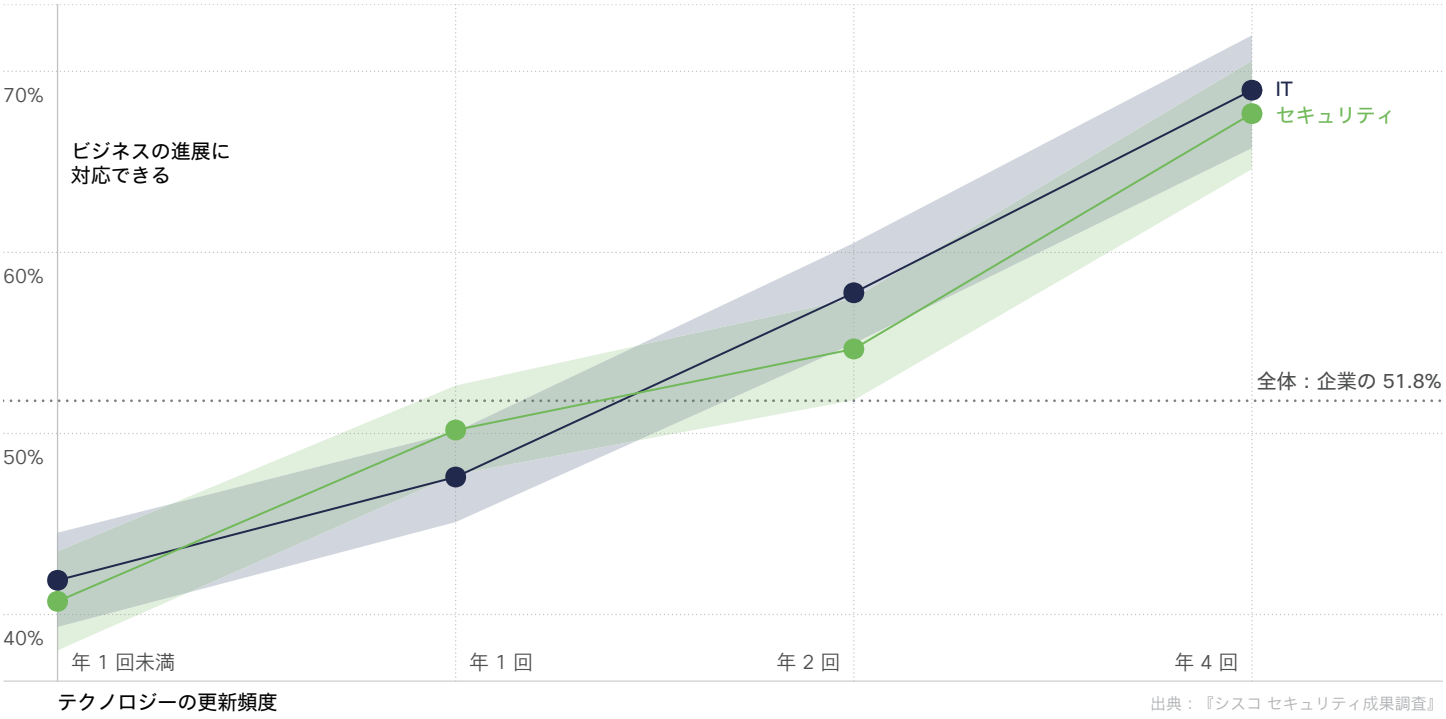


図 2：テクノロジーの更新頻度とビジネスの進展に対応できるセキュリティプログラムの間の関係[1]

そこで、IT とセキュリティのアップグレード頻度を各企業に尋ね、セキュリティプログラムがビジネスの進展に対応できるという回答項目との関係を調べました。すると、この 2 つの変数は互いに関係しており、アップグレード頻度を上げることでこの主要な成果を着実に改善できることが分かりました。IT とセキュリティテクノロジーを四半期ごとにアップグレードする企業は、数年ごとにしかアップグレードしない企業と比べて、**ビジネスの進展に対応できると回答する割合が平均で約 30% 高くなります。**ポスターを作って「常に最新の状態を維持していこう」といった文句を添えれば、苦労が絶えない IT チームの士気が上がりそうです。

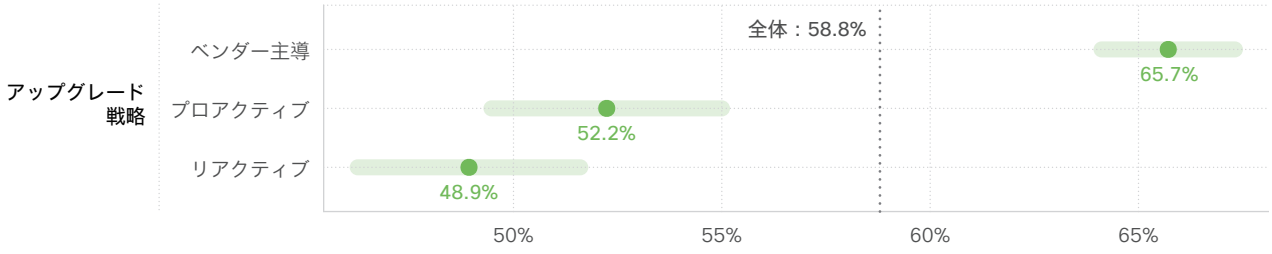
[1] 本レポートでは、それぞれのプラクティスまたは成果における個別の値を「全体」値とともに示しています。この全体値は、各プラクティスまたは成果に関連する一連の質問に回答したすべての回答者の平均値を表します。参考のために提供している値であり、平均を上回っている企業と下回っている企業の実態を理解するのに役立ちます。また、一部の図表ではエラーバーや網掛けで信頼区間を示しています。この信頼区間が「全体」を示す線と重なっている場合、セキュリティプログラムのその側面は該当する成果やプラクティスに影響を与えるとみなすことはできません。

テクノロジーの更新はどのような要因によって主導すべきか？

頻繁なアップグレードがビジネスの進展を支えることが分かりましたが、アップグレードの実行プロセスはどのような要因によって主導すべきなのでしょうか？セキュリティテクノロジーの更新を主導している主な要因を各企業に尋ねたところ、回答は次の 3 つに大別されました。

- **ベンダー主導**：SaaS プロバイダーがスケジュールを決定しているか、大規模なベンダー統合イニシアチブの一環としてスケジュールが組まれている（要因の中で最も一般的）
- **プロアクティブ**：あらかじめ決められたスケジュールに従っているか、新機能や新しいユースケースのためにアップグレードが必要な場合（2 番目に一般的）
- **リアクティブ（事後対応型）**：インシデントが発生した場合、テクノロジーが古くなった場合、またはコンプライアンス要件を満たすため（最も一般的でない）

これらの要因自体にも興味を惹かれますが、ここで知りたいのは、これらがテクノロジー更新アプローチの強化に寄与したかどうかです。その答えは図 3 のとおりです。テクノロジー更新イニシアチブは、ベンダーが管理している（または少なくとも実施に向けて積極的に関与している）場合に成功する可能性が高くなる、というのが基本的な結論です。**強力な更新機能があるとの回答は、リアクティブ（事後対応型）アプローチをとっている企業では半分未満であるのに対し、ベンダーの更新サイクルに基づいている企業では約 3 分の 2 に上ります。**



出典：『シスコ セキュリティ成果調査』

図 3：アップグレードを主導する主な要因がセキュリティテクノロジーの更新パフォーマンスに与える影響

IT 製品とセキュリティ製品を扱うベンダーが発表したレポートでベンダーに都合の良い結果を示されても信ぴょう性に欠けると思われるかもしれませんが、シスコはこの調査結果にまったく影響を与えていません。本調査は信頼できる独立した調査会社によって実施されており、シスコが後援企業であることを回答者は知りませんでした。また、評価の高い Cyentia Institute 社がデータを分析して図 3 の結果を出しています。さらに、これらの結果を解釈する際には最大限の注意を払っています。

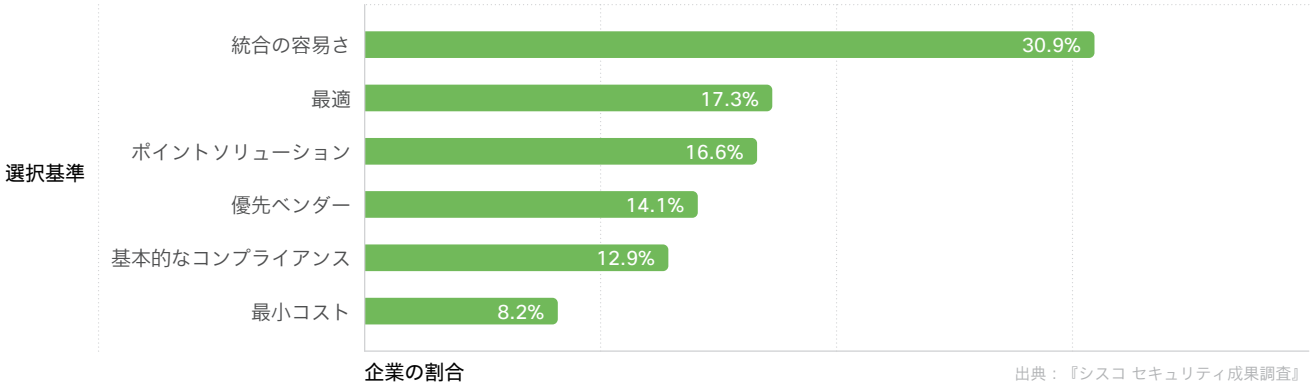
シスコでは、ベンダー主導のアプローチがもたらす改善の多くは、クラウド /SaaS アーキテクチャが頻繁なアップグレードに適していることに関係しているのではないかと考えています。また、ベンダーが優れているからというよりも、ベンダーを利用することで、テクノロジーの更新スケジュールを妨げがちな社内の障害や政治的な問題が避けられるということもあるでしょう。

Rob Base と DJ E-Z Rock の曲に次のような一節があります。「うまくやるなら 2 人でなくちゃ。2 人揃えば最高にクール」。これぞまさにセキュリティアーキテクトの心意気です。テクノロジー ソリューション パートナーとタッグを組めば、ミッションの成果が向上して素晴らしい更新戦略を実現できます。

65.7% ベンダーの更新サイクルに基づいている企業の 65.7% が、強力なテクノロジー更新機能があると回答

アップグレードは機能重視か互換性重視か？

前のセクションではテクノロジーのアップグレードをスムーズに進めるシナリオを調べました。次はソリューションを選択する基準を見ていきます。回答者から寄せられた選択基準をまとめると図 4 のようになりました。既存のテクノロジーとの統合しやすさが圧倒的に重視されています。その次に重視されているのが最適な機能を備えたソリューションや特定のニーズを満たすソリューションです。意外かもしれませんが、コストの最小化は最下位となっています。



出典：『シスコ セキュリティ成果調査』

図 4：セキュリティ製品を更新する際の主要な選択基準

それぞれの選択基準がどの程度重視されているかは分かりましたが、セキュリティプログラムを成功に導く上で重要になる選択基準はあるのでしょうか？この疑問に答えるために、図 4 の選択基準を次の 3 つのカテゴリに分類しました。

- **最小**：最小コストのソリューション、基本的なコンプライアンス
- **統合の容易さ**：既存のテクノロジーとの統合、優先ベンダーの使用
- **機能**：最適、ポイントソリューション

次に、11 種類のセキュリティ成果の達成レベルに基づいた総合スコアを企業ごとに算出して各カテゴリに振り分けました。スコアの絶対値に特別な意味はありませんが、それぞれのテクノロジー更新戦略を比較するのに利用できます。**図 5 に示すように、コストの最小化や基本的なコンプライアンス要件の達成を重視して製品を選択するよりも、統合や機能を重視したほうが成果が上がります。ただし、平均を有意に上回っているのは統合重視のアプローチのみです。**

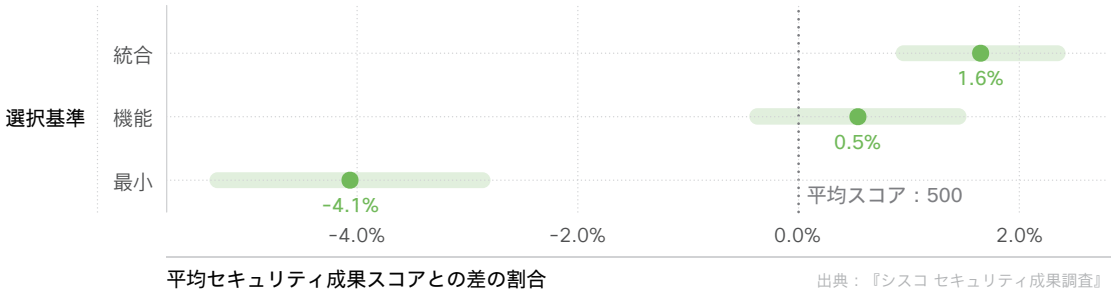


図 5：テクノロジーの選択基準が全体的なセキュリティ成果スコアに与える影響

このようにカテゴリ間の差が示されましたが、プログラムの全体的な成功からすると僅差であることに注意してください。またこの結果はセキュリティプログラムのさまざまな優先事項やプラクティスの一部を垣間見たに過ぎない可能性もあります。しかし、どのような基準で製品を取捨選択するかというソフトな問題も検討に値することが分かります。セキュリティソリューションを更新またはアップグレードする際にどの特徴を重視するか迷っている場合は、この結果を根拠としてコストの最小化よりも互換性や機能を重視してみてください。

セキュリティ成果スコアとは

12 種類のセキュリティプログラム成果に対する各企業の成功レベルについて回答者に尋ねました。詳しい分析は最初の『セキュリティ成果調査』で行いましたが、今回の調査でもいくつか吟味しています。さらに、セキュリティプログラムの全体的なパフォーマンスを測定するために、12 のすべての成果に対する各企業の達成度を示す総合スコアも算出しました。これを「セキュリティ成果スコア」と呼んでおり、このレポートでも何度か言及しています。

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。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。

「CISO はインフルエンサーであると同時に教育者でもある必要があります。影響力を可能な限り高めるには、会社が行う戦略決定の最先端にいる必要があります。セキュリティが重要であること、セキュリティを適切に確保するために適切な投資が必要であること、ビジネスのあらゆる側面に関与する必要があることを分かっていただこうと活動していますが、同時に教育も必要です。ほとんどの経営幹部はセキュリティ分野での経験がないので、それぞれの意思決定が招くかもしれないリスクの種類についてあらゆる段階で情報を提供する必要があります。」

Helen Patton（シスコ、アドバイザリ CISO） @CisoHelen

CISO の進化する役割について Helen が興味深い話を披露していますので、こちらのセキュリティ事例ポッドキャストのエピソードをお聞きください。

テクノロジーの十分な統合を実現

前回の『セキュリティ成果調査』によると、さまざまな IT インフラストラクチャと効果的に連携する十分に統合されたセキュリティテクノロジーは、あらゆるプログラム成果の向上に寄与します。そこで、この素晴らしい効果の背後にある要因を詳しく調べるために一連の質問を行いました。始めにセキュリティテクノロジーを統合する目的を尋ねました。

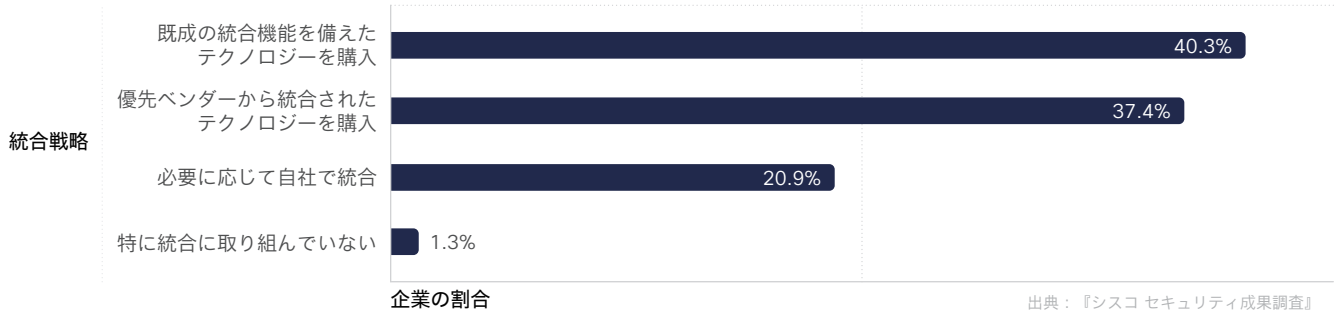
回答者によると、セキュリティテクノロジーを統合する最も一般的な動機はモニタリングや監査の効率向上です。これには共感を覚えます。いくつものコンソールやダッシュボードを確認してネットワークの状況を把握しなければならない苦痛や不満は身にしみて分かります。コラボレーションや自動化が容易になることも、セキュリティテクノロジーを統合する一般的な動機でした（自動化については後で詳しく取り上げます）。これらの動機とテクノロジーの統合レベルやプログラム成果についての回答との関係を調べましたが、それほど強い相関性は見られませんでした。おそらく、セキュリティテクノロジーを統合するときには「動機」よりも「対象」や「方法」のほうが重要になると思われます。以下の質問でこれらの点を掘り下げていくことにしましょう。

回答者によると、セキュリティテクノロジーを統合する最も一般的な動機はモニタリングや監査の効率向上です。

十分に統合されたテクノロジーは購入すべきか構築すべきか？

セキュリティテクノロジーを統合すると成果が向上することは前回の調査で分かりましたが、高度に統合されたテクノロジースタックを実現する最善の方法は何でしょうか？実現できるものを購入すべきか、必要に応じて構築すべきか、特に何もしなくてもよいのか。どの方法が良いか確認することにしましょう。

セキュリティテクノロジーを統合するための一般的なアプローチについて各企業に質問したところ、回答は図 6 のようになりました。**大まかに見ると、4 分の 3 を上回る企業が統合ソリューションは構築するよりも購入したいと考えています。**それらの企業のうちの 40% 強が、既存のインフラストラクチャに簡単に統合できる既成機能を備えたテクノロジーを選択しています。また 37% 超が、単一のベンダーからソリューションを調達するという一歩進んだ選択をしています。ベンダーが 1 社であれば、購入する製品群はネイティブに統合されているか、もっと大きなプラットフォームの中に組み込まれています。20% 強の企業は、ニーズに合った製品であれば自社で統合すると回答していますもれ特に統合に取り組んでいないと回答した企業はほとんどありません。



出典：『シスコ セキュリティ成果調査』

図 6 : 企業がセキュリティテクノロジーを統合する一般的なアプローチ

全体として **3/4** を超える企業が統合型ソリューションを構築ではなく購入

図 7 では、統合アプローチの違いによってパフォーマンスに差が生じるかどうかを評価しています。ベンダーと協力して統合された最新のテクノロジーを維持する利点がここでも示されています。**図のように、優先ベンダーから調達すると、特別な統合アプローチがない場合と比べて、十分に統合されたセキュリティテクノロジーを実現できる可能性が 2 倍以上になります (約 31% に対して約 69%)。**さらに、シスコの調査によると、この調査結果はあらゆる規模の企業に一貫して当てはまります。ただし、優先ベンダーを使用するメリットは大企業よりも中小企業のほうが高いと言えそうです。

ここでも、統合されたセキュリティポートフォリオを広範に展開している企業が都合の良い調査結果を出していると疑いの声が上がるかもしれません。シスコの戦略がこの結果で裏付けられたことはもちろんうれしく思っていますが、これは二重盲検調査であり、シスコは調査結果をまったく操作していないことを念押ししておきたいと思います。

セキュリティテクノロジーの統合に特に取り組まなかった企業は、予想されるとおりの結果になっています。**一方、既成の統合機能を備えた製品を購入する企業と自社で統合を手掛ける企業の間にほとんど差がなかったことは、意外な結果だと思われるかもしれません。**これらのアプローチを採用している企業は、いずれもほぼ半数近く（約 49%）が高い統合レベルを達成していると回答しています。

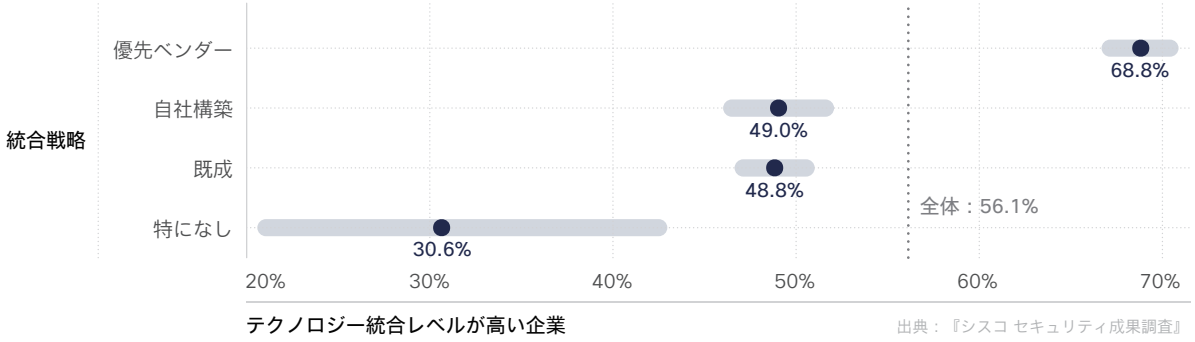


図 7 : 一般的な統合アプローチがセキュリティテクノロジーの統合レベルに与える影響

統合を進めるならクラウドで

セキュリティテクノロジーの統合を始めたい（または拡大したい）のだがクラウド環境とオンプレミス環境のどちらを利用すべきか悩んでいる、という声をお客様からよく聞きます。その決断に役立つデータをご紹介します。オンプレミス環境とクラウド環境のいずれであっても、多くの回答者が良い結果が得られたと回答しています。ただし、テクノロジーの強力な統合はクラウドのほうがはるかに簡単に実現できるようです。

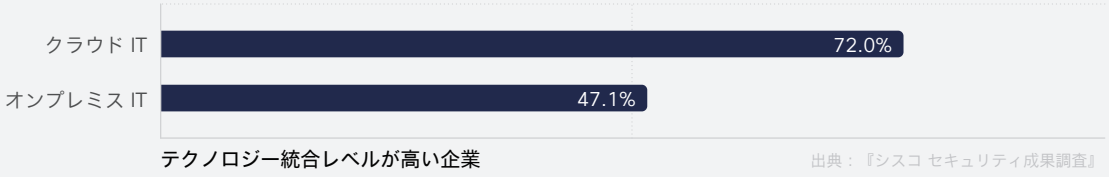


図 8 : クラウド環境 / オンプレミス環境の選択がセキュリティテクノロジーの統合レベルに与える影響

統合は自動化に役立つか？

このセクションの冒頭で説明したように、テクノロジーを統合する最も一般的な動機は自動化ではありませんでしたが、自動化を挙げた企業も 44% に上りました。動機はさておき、テクノロジーが十分に統合されるとセキュリティプロセスの自動化が実際に促進されるという証拠はあるのでしょうか？図 9 のデータがそれを裏付けています。

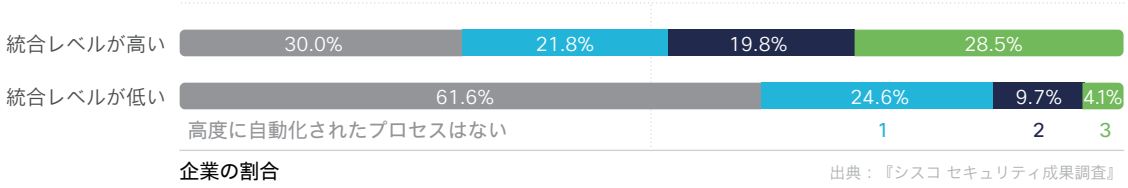


図 9：テクノロジーの統合がセキュリティプロセスの自動化の度合いに与える影響

図 9 の 2 本の横棒は、セキュリティテクノロジーの統合レベルが高い企業と低い企業を表します。色分けされたセグメントは、成熟した自動化によってサポートされている主要なセキュリティプロセス（イベントモニターリング、インシデント分析、インシデント対応）の数を表します。統合レベルが低い企業では、自動化されたプロセスはないと答える割合が 2 倍以上になっています。**逆に、セキュリティテクノロジーが十分に統合されている企業では、3 つのプロセスすべてで高度な自動化を達成する可能性が約 7 倍になっています（4.1% に対して 28.5%）。**自動化は確かに切実な動機と言えるでしょう。

どの機能を統合すべきか？

次に、NIST サイバーセキュリティ フレームワーク（CSF）の 5 つのコア機能をサポートするテクノロジー間の統合レベルについて質問し、非常に断片化している（各テクノロジーがサイロ化してほぼ単独で動作している）から高度に統合されている（テクノロジー間で調整が行われて 1 つの機能ユニットとして動作している）までの尺度で回答してもらいました。その後、各企業の全体的なセキュリティ成果スコアに与えた影響を特定するモデルを作成しました。

図 10 に示すように、5 つのどの機能でもほぼ同じ結果が得られています。**NIST CSF のどの機能領域も、断片化を解消して統合することでセキュリティプログラムの成果が向上します（11 ～ 15% 向上）。**したがって、「どの機能を統合すべきか？」に対する答えは「すべて」になりますが、どこから手を付ければよいか迷う場合は、高度に統合された「識別」機能が向上幅が最も大きいのでお勧めです。

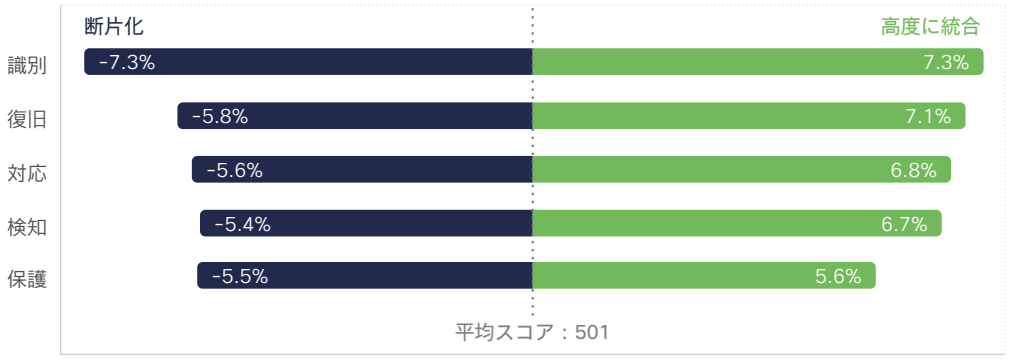


図 10：NIST CSF 機能の統合が全体的なセキュリティ成果スコアに与える影響

テクノロジー統合の最も強い動機がモニタリング、監査、コラボレーションであることを前のセクションで説明しましたが、このセクションの結果にも同様の示唆が含まれているように思えます。つまり、企業全体の可視性を十分に確保することが根本的に重要であることをこれらの結果は示しているのです。「システム、人材、資産、データ、および機能に対するサイバーセキュリティ リスクの管理について組織内の理解を深める」（NIST CSF からの引用）ために断片的なアプローチをとっても、うまくいかないのは当然と言えるでしょう。「脅威の検出とインシデント対応」セクションではこのテーマがさらに重要になっていきます。

統合、識別、情報について

先ほど見た図だけでなく、この調査で示されているデータはどれも統合、識別、情報の間に重要な関係があることを示しています。資産や脅威を識別できなければその存在を知ることはできず、情報を活用した防御体制を整える必要性に気付かないまま手遅れになってしまうのです。

図 11 はこのことをよく示しています。NIST CSF の「識別」機能について各企業が回答した統合レベルと、企業が脅威を正確かつタイムリーに検出する能力を比較してみました。**重要な資産やリスクを識別するためのシステムが高度に統合されている企業は、強力な脅威検出機能を備えている割合が高くなっています (41% 増)。**断片化との戦いを制する者は、敵との戦いも制するのです。

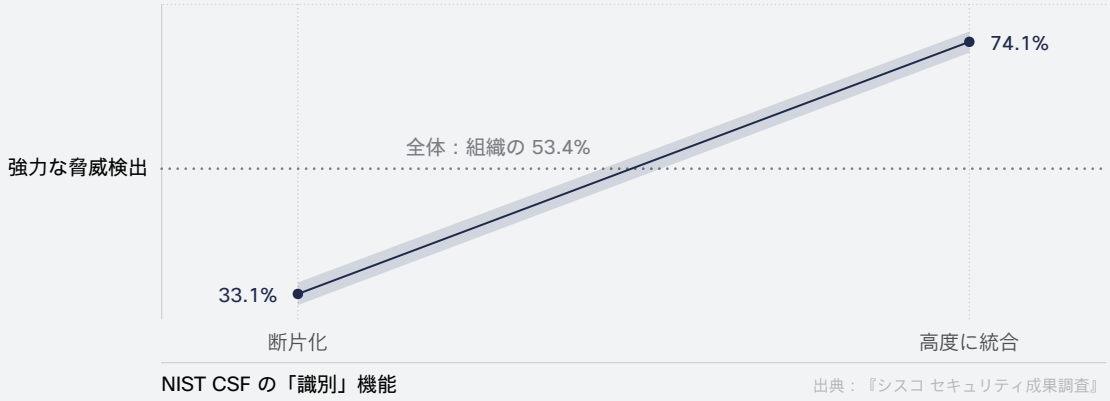


図 11：NIST CSF の識別機能の統合が脅威検出機能に与える影響

重要な資産やリスクを識別するための
システムが高度に統合されている企業は、

+41%

強力な脅威検出機能を
備えている

「自動化のおかげで新しい脅威にエンジニアがタイムリーに対応できるようになりました。ルールを絶えず更新したりネットワークを常時モニタリングしたりする必要がなく、セキュリティのコンセプトを正しく把握することに集中できています。インフラストラクチャをより効果的に保護し維持することができるようになったのは、シスコのソリューションが細部に分け入って必要な情報を抽出してくれるからです。マシンインテリジェンスとヒューマンインテリジェンスの完璧な組み合わせが実現しました。」

- Steve Erzberger (Frankfurter Bankgesellschaft (Schweiz) 社、CTO)

詳細はこちら

脅威検出機能とインシデント対応機能を開発

このセクションでは、「トップ 5」に名を連ねている 2 つのセキュリティプラクティス領域について説明します。脅威検出とインシデント対応はセキュリティ担当部署で人材、プロセス、テクノロジーを共有していることが多いので、この 2 つに共通する質問をいくつか行いました。したがって、この調査ではこの 1 つのセクションで脅威検出とインシデント対応をまとめて分析します。

強力な人材、プロセス、テクノロジーを備えている企業のほぼすべて (約 92%) が高度な脅威検出機能とインシデント対応機能を実現しています。

人材、プロセス、テクノロジーの優先順位は？

まずは人材 (people)、プロセス (process)、テクノロジー (technology)（別名 ppt の三要素）について調べてみましょう。セキュリティ機能、特に脅威検出とインシデント対応の領域に属する機能は、この三大要素の組み合わせであると説明されることが多いようです。しかし、セキュリティの三大要素においてひときわ重要度が高い要素というのはあるのでしょうか？では、さっそく分析に移りましょう。

図 12 を下から見ていくと、三大要素のいずれにも強みがないプログラムでは、セキュリティ機能に自信があると回答する割合が 4 分の 1 ほどにしかなりません。人材、プロセス、テクノロジーのいずれかの領域で強みを獲得すると、その割合が約 60 ～ 64% にまで上昇します。人材に強みがあるほうがわずかに優位のようですが、信頼区間が全体平均を示す線と重なっているので、有意な差があるとは言えません。重要なのは、どの要素であっても優れた検出機能と対応機能を構築するための出発点として適しているということです。

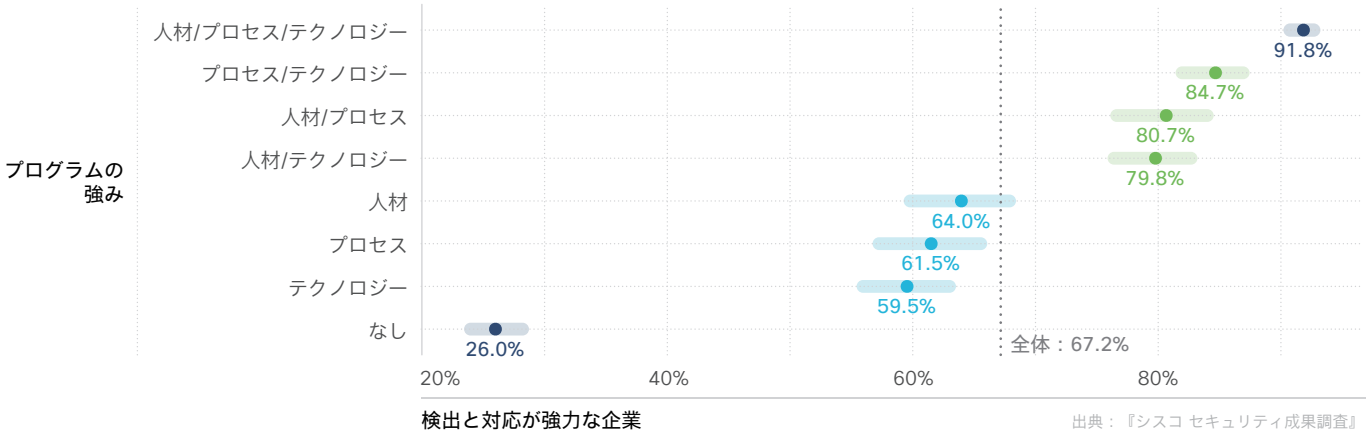


図 12：強力な人材、プロセス、テクノロジーが脅威検出機能とインシデント対応機能に与える影響

図 12 をさらに上に見ていくと、2 つの要素が優れているセキュリティプログラムは平均を大きく上回っており、1 つの要素が優れているプログラムと比べて機能が約 15% ～ 20% 向上しています。ここでも、人材、プロセス、テクノロジーからどの 2 つを選択するかはあまり問題になりません。どれでも構わないので、2 つの要素に強みがあればよいのです。会社のセキュリティロードマップを作るときには選択の自由があることになります。素晴らしいと思いませんか？

図 12 の一番上にはセキュリティの三大要素を達成した優良プログラムがあります。**強力な人材、プロセス、テクノロジーを備えている企業のほぼすべて (約 92%) が高度な脅威検出機能とインシデント対応機能を実現しています。**いずれの要素にも強みがないセキュリティプログラムと比べるとパフォーマンスが 3.5 倍になります。ですから、どこからでも前進しやすいところから取り掛かりましょう。そして、頂点に君臨する人材、プロセス、テクノロジーの三大要素を達成してください。

強力な人材、プロセス、およびテクノロジーを備えている企業では、これらすべての分野で強みがない企業に比べて、脅威の検出と対応のパフォーマンスが **3.5 倍** 向上

ゼロトラストや SASE でセキュリティは向上するか？

前述の調査結果では「強力なテクノロジー」のような抽象的な表現を使用しているので、具体的な実施項目に落とし込むのが難しくなっています。そこで、特定のアーキテクチャについてさらに 2 つの質問を行いました。ゼロトラストとセキュア アクセス サービスエッジ（SASE）の導入について回答者に尋ね、これらのアプローチが脅威検出機能とインシデント対応機能（そしてセキュリティプログラムの成果）に与える影響を探りました。

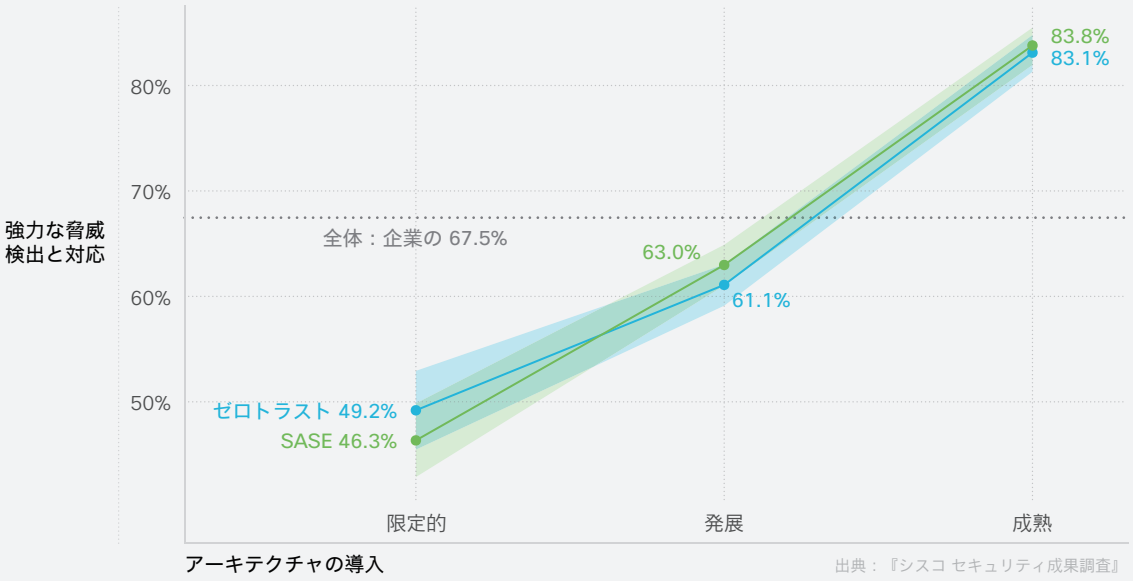


図 13：ゼロトラストおよび SASE アーキテクチャが脅威検出機能とインシデント対応機能に与える影響

ゼロトラストまたは SASE 実装の成熟が進んでいると回答した企業は、実装が初期段階である企業と比べてセキュリティが強力であると回答する割合が約 35% 高くなっています。最新のアーキテクチャがサイバーセキュリティ プログラムにさまざまな利点をもたらすというこれまでの説明がこの結果でも裏付けられました。

頭数が多ければ頭痛の種は減るか？

強力な脅威検出機能とインシデント対応機能を構築するには優秀な人材を揃えることが重要であることが分かりました。しかし、人材を増やしたほうがよいのか、それとも今いる人材のスキルを強化したほうがよいのか、どちらなのでしょうか？もちろん、両方でも構いませんが、疑問は残ります。成功するセキュリティチームを作り上げるときに質と量のどちらが重要になるのか、データから突き止められないものでしょうか？

そこでまず、全従業員に対するセキュリティ担当スタッフの比率をすべての企業で計算しました。次にこの比率を、企業が回答した脅威検出機能とインシデント対応機能の高さと比較しました。図 14 に計算結果を示します。質か量かの疑問に完全に答えているわけではありませんが、いくつか分かることがあります。

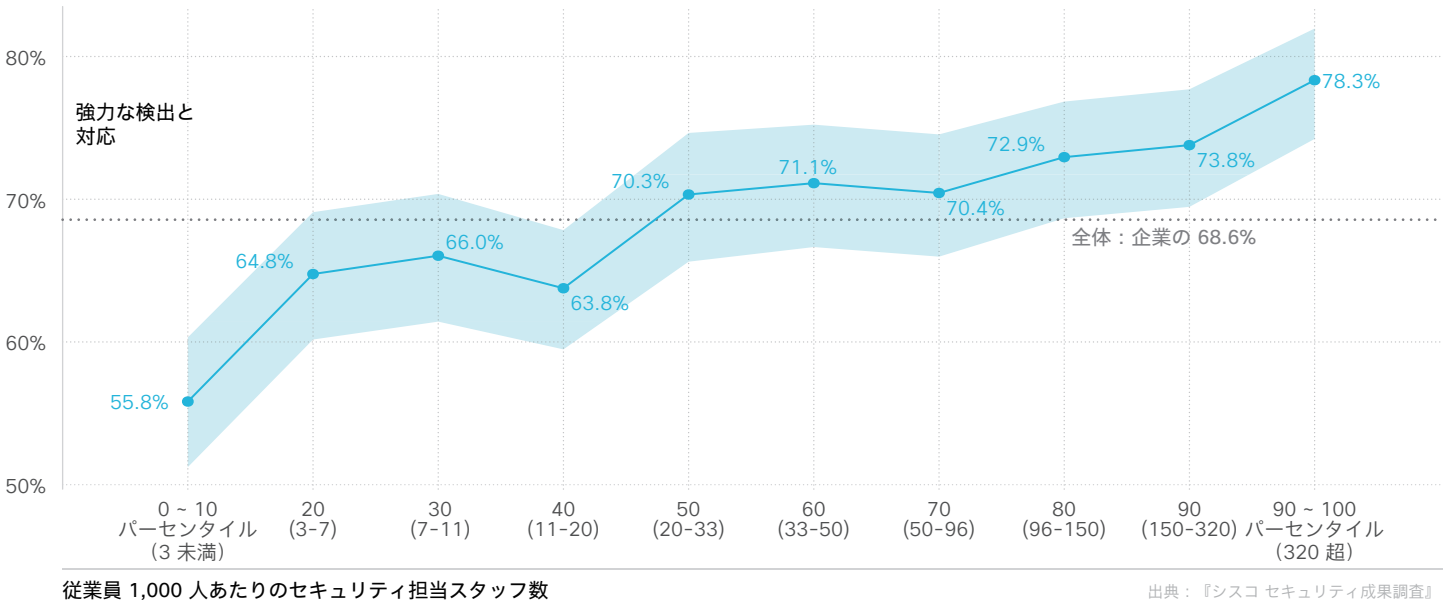


図 14：セキュリティ担当スタッフの比率が脅威検出機能とインシデント対応機能に与える影響

まず、セキュリティ担当スタッフの比率が高くなると脅威検出機能とインシデント対応機能が向上することが分かります。比率が最も高い企業は、最も低い企業と比べて強力な機能を持っていると回答する割合が 20% 以上高くなります。しかし、図 14 では網掛けの信頼区間の大部分が全体平均を示す点線と重なってしまっています。これは、セキュリティ担当スタッフの比率が極端に高いか低い企業を除いて（つまりほとんどの企業で）、強力なセキュリティプログラムを構築していると回答する割合は変わらないことを意味します。

ではこの結果から何が読み取れるのでしょうか？確実に言えるのは、大規模なセキュリティチームを擁する企業は必要最低限のチームしか配置していない企業よりも強力な脅威検出機能とインシデント対応機能を実現する可能性がかなり高くなるということです。しかし、頭数を増やすだけではセキュリティの頭痛の種が消えることも成功が保証されることもありません。さらに、前のセクションで示した強力な人材がもたらすパフォーマンス向上は、人員比率が最小の企業と最大の企業の差をもってしても説明がつきません。**したがって、強力な脅威検出および対応チームを作り上げる際には、質が量と同じくらい重要か、おそらくは量よりも質が重要になると考えられます。**

セキュリティチームの深刻な人手不足は現在も続いています。

縮小するリソースと増大する脅威の中で大きなストレスを抱えて疲れ切っているサイバーセキュリティ担当者が多くなっています。彼らの心身の健康を守るために、事前に打てる手はないのでしょうか？この eBook では、業界リーダーや専門家から心の健康を管理するための知見や事例をお聞きしています。

セキュリティ担当スタッフは社員、外部委託、混合体制？

単に頭数を増やしてもセキュリティは成功しないようですが、人員確保体制は成果に影響を与えるのでしょうか？他の要因がすべて同じであった場合、脅威検出や対応にあたるスタッフは外部委託、社員、混合体制のどれが良いのでしょうか？データを調べて答えを探っていくのですが、今回は互いに矛盾するような結果が出ていますのでご注意ください。

人員確保体制について質問し、脅威検出機能およびインシデント対応機能の評価と比較してみました。図 15 に示すように、**主に社内または外部委託で人員を確保している企業は、混合体制で人員を確保している企業よりも強力なセキュリティプログラムを構築していると回答する割合がかなり高くなりました (それぞれ 20% 増と 30% 増)。**しかし、何らかの形で混合体制を採用している企業がほとんどであったため、この調査結果だけをもって混合体制は劣っていると決めつけずに、別の観点でも調べてみることにしました。

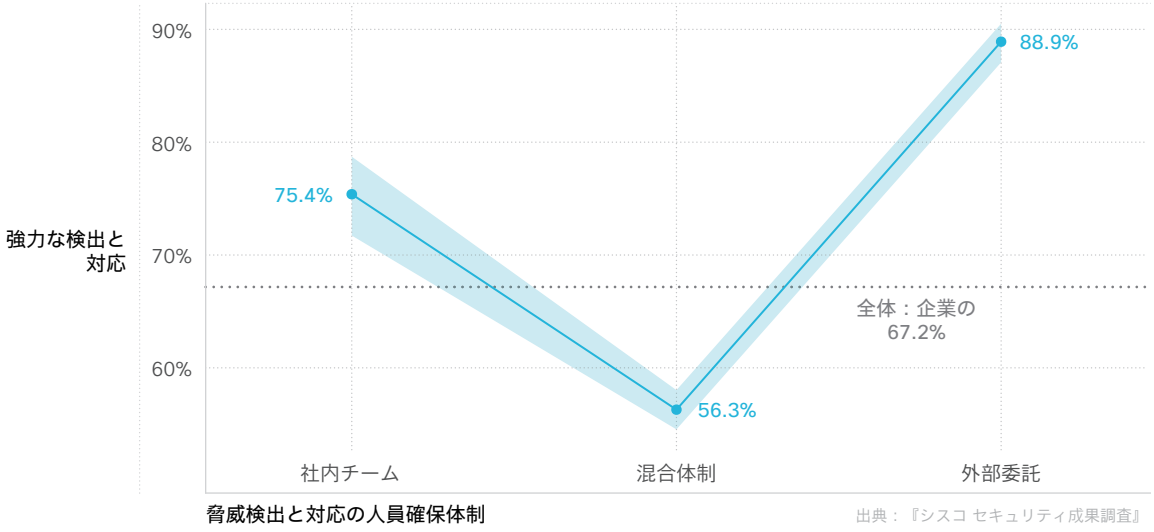


図 15：人員確保体制が脅威検出機能とインシデント対応機能に与える影響

主に社内または外部委託で人員を確保している企業は、混合体制で人員を確保している企業よりも強力なセキュリティプログラムを構築していると回答する割合が

20 ～ 30%

高い

脅威検出機能とインシデント対応機能の高さを回答者に尋ねるとともに、より客観的に比較できる評価基準がないか探しました。その 1 つとして平均対応時間（MTTR）がありました。これはセキュリティインシデントを修復するか抑え込むまでにかかる平均時間です。このレポートとは別に行った事前分析によると、MTTR のような評価基準は主観的評価と方向性が多くの場合一致する傾向があります。しかし、図 16 から明らかなように今回は 2 つの観点が矛盾してしまいました。

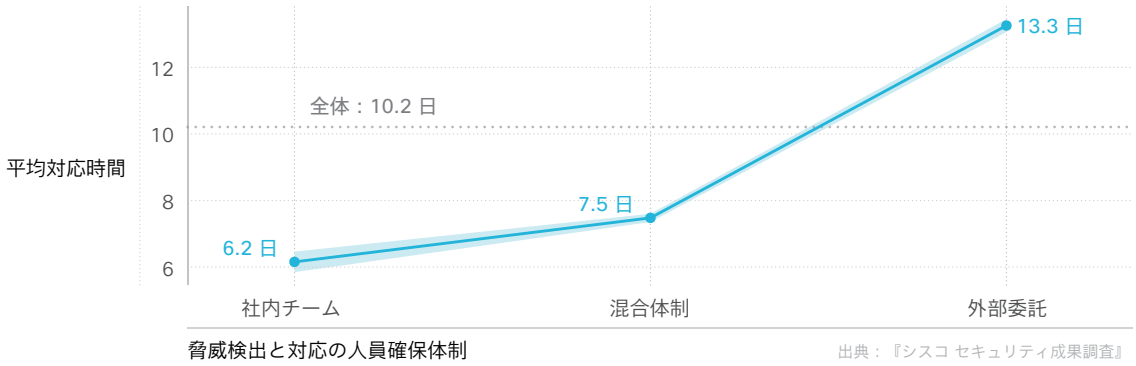


図 16：人員確保体制がセキュリティインシデントの平均対応時間に与える影響 [2]

図 16 を見ると、脅威検出および対応チームを社内に抱えている企業は、外部委託している企業と比べて MTTR が半分以下（約 13 日に対して約 6 日）になっています。混合型の人員確保体制を採用している企業は両者の中間（約 8 日）となっており、社内チームほど迅速ではないものの、主に外部委託しているチームよりはるかに素早く対応しています。

どうやら、あちら立てればこちらが立たぬ困った状況になったようです。主観的評価と評価基準はどちらが正しいのか。そして何より、どちらを信じて人材を確保すべきなのか。ここではあえて結論を出さず、「どちらも正しい」かもしれないし「どちらも間違い」かもしれないと述べておきたいと思います（非難のお気持ちはよく分かりますが、どっちつかずなのは私たちではなくデータのほうなのです）。

一口に「修復」と言っても、そこにはさまざまな要素や依存関係が絡んできます。脆弱性を完全に解決するには、ベンダーに依頼してパッチ（修正プログラム）を発行してもらう必要があるかもしれません。たとえパッチが発行されても、ラボ環境でテストしてからでないと実稼働環境には導入できません。このように、調査結果を左右する要因は大量に存在します。

実際、どのような要因が絡んで前述の調査結果に結びついたのか正確に突き止めるのは困難です。もしかしたら、アンケート調査で評価基準を用いたことで、誤解を招くような結果になったのかもしれません。MTTR と脅威検出および対応機能の評価の間に整合性を求めるのがそもそも間違っていて、脅威検出および対応プログラムが全体として「強力」でありながら、修復には時間がかかるということもあり得ます。徹底的に調査し対応するので時間がかかっている可能性もあります。外部委託のスタッフの場合、調整に時間がかかるのかもしれません。「専門家に金を払って仕事をしてもらっている」という安心感から、外部委託の評価が高くなっていることも考えられます。社内チームの評価の高さはダニング＝クルーガー効果のセキュリティ版なのかもしれません。おそらくここに挙げているすべてが影響したのでしょうし、他の要因も絡んでいたのでしょう。以上のことから、このセクションは意思決定ではなく、ディスカッションの促進に利用していただければ幸いです。

[2] この図では、より「一般的」な値を示すために幾何平均を使用しています。MTTR は 2 ～ 3 週間未満という回答が一般的でしたが、数か月（あるいは数年）という回答も混じっていました。幾何平均を使用すると、こうした極端に大きな値に影響されずにより「一般的」な値を得ることができます。

インテリジェンスを使用するのはスマートか？

ダニング=クルーガー効果が出てきましたが、このセクションを理解するにはまさにうってつけの仮説です。セキュリティプログラムでのサイバー脅威インテリジェンスの使用について回答者に尋ねました。ほとんどの企業（85%）は何らかのレベルでインテリジェンスを使用していると回答しましたが、広く活用していると回答した企業は 3 分の 1 未満(31%) でした。インテリジェンスの活用が進むほど脅威検出と対応が向上し、スマートになり、迅速になっていくように思えますが、実際はどうなのでしょうか？図 17 を見てみましょう。

奇妙なことに、サイバー脅威インテリジェンスをまったく使用していない企業のほとんどは、自らの能力に非常に自信を持っているようです。そしてインテリジェンスをひとたび導入するとこの自信は揺らいでしまうのです（約 84% から 46% に低下）。「知らぬが仏」とはまさにこのことです。**サイバー脅威インテリジェンスを広く活用している企業は、あまり使用していない企業と比べて強力な脅威検出機能とインシデント対応機能を持っていると回答する割合がほぼ 2 倍になります。またインテリジェンスを広く活用する企業は、インテリジェンスを使用しない企業と比べて MTTR が約半分になります。これは機能についての主観的評価と評価基準が一致する例です。**

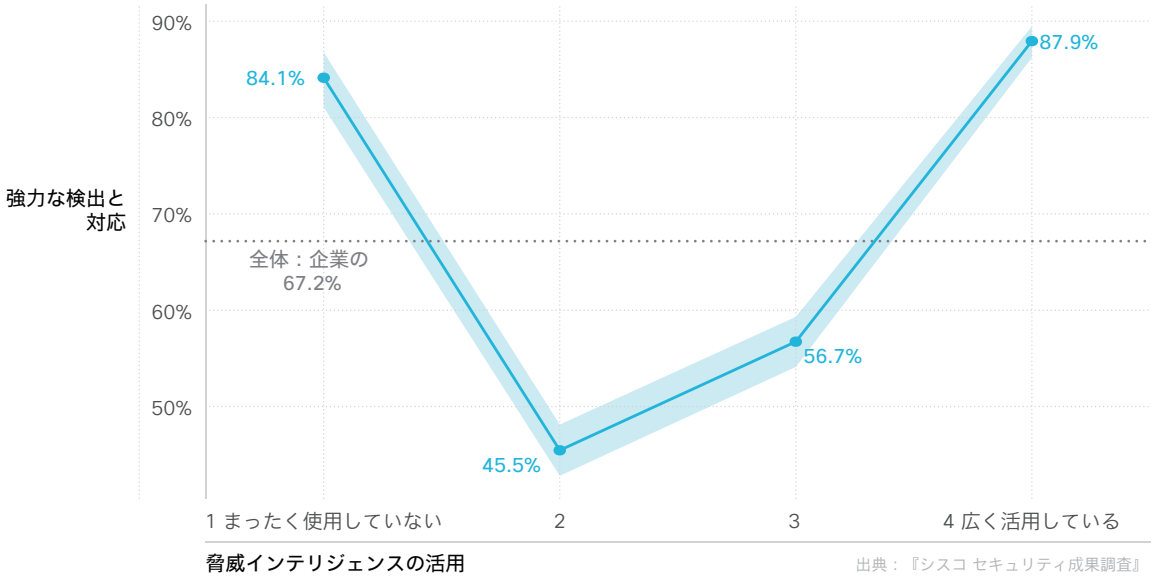


図 17：サイバー脅威インテリジェンスの使用が脅威検出機能とインシデント対応機能に与える影響

心理学者でベストセラーの著者でもある Daniel Kahneman 氏はかつてこう述べています。「人は自分の無知を自覚していません。自分がいかにものを知らないか、ほとんど気付いていないのです」。図 17 を見ると、脅威に取り囲まれていることが少しでも分かれば、自分たちが無知であったことに企業が気付くということが分かります。サイバー脅威インテリジェンスの活用を進めていけば企業は自信を取り戻すことができます。そして今度はもう、それほど無知ではありません。

サイバー脅威インテリジェンスを広く活用している企業は、強力な脅威検出機能とインシデント対応機能を持っていると回答する割合が **2 倍** である

自動化は人間の代わりになるか？

このタイトルを見て、単なるレトリックだと思った方もいらっしゃるかもしれません。早合点は禁物です。セキュリティコミュニティを全員敵に回してしまいそうですが、このセクションではあえて危険を冒して、自動化が実際に人間に取って代わる可能性があることをデータで示したいと思います。このレポートを削除して私たちをブロックリストに追加する前に、落ち着いて最後までお読みいただけますと幸いです。

図 18 は、以前に個別の図で示したセキュリティ担当スタッフと自動化を組み合わせて評価したものです。2 本の線で 2 種類のセキュリティプログラムを比較しています。濃い青色の線は強力な人材を持たない企業、薄い青色の線は強力な人材を持つ企業を表します。どちらのシナリオでも、左から右に見ていくことで、自動化レベルの向上が脅威検出機能とインシデント対応機能に与える影響が分かります。

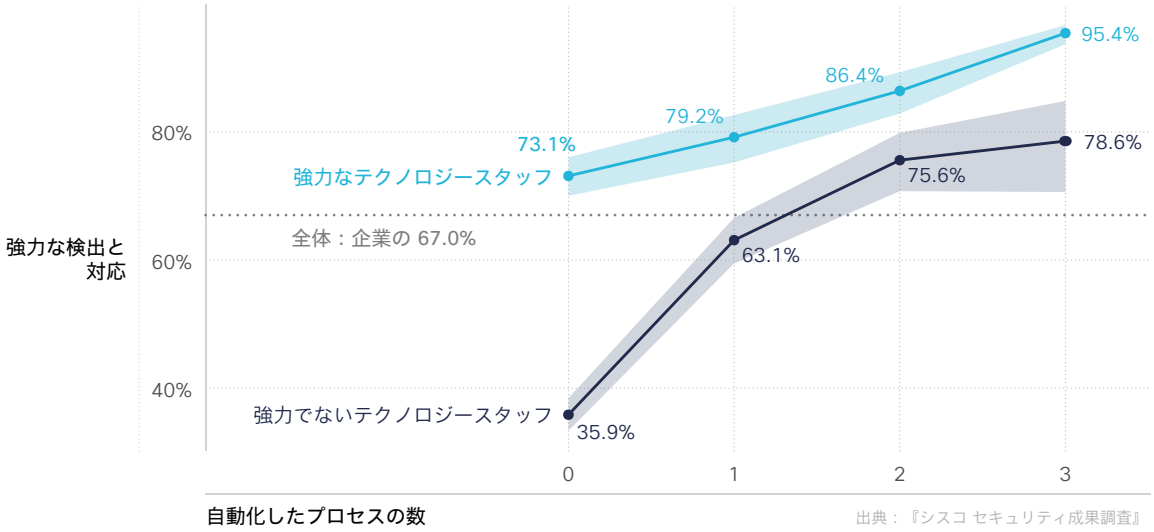


図 18：スタッフおよび自動化のレベルが脅威検出機能とインシデント対応機能に与える影響

まず、強力な人材を持たない企業から見ていきましょう。強力なセキュリティ担当スタッフを持たず、主要なプロセスのいずれも自動化していない企業は、強力な脅威検出機能とインシデント対応機能を持っていると回答する割合が約 3 分の 1 に過ぎませんが、質問で取り上げた 3 つのプロセス領域（脅威モニターリング、イベント分析、インシデント対応）のいずれか 1 つを自動化すると、その割合は大幅に上昇します。2 つを自動化すると割合はさらに上昇し、3 つすべてを自動化すると、経験の少ないスタッフのみの場合と比べてパフォーマンスが 2 倍以上になります。**強力な人材を持っていなくても、高度な自動化を達成すれば 4 分の 3 以上のセキュリティプログラムで堅牢な機能を実現できるのです。**

次に、濃い青色の線の右端の点から薄い青色の線の左端の点まで目か指でなぞってみてください。何が言いたいかお分かりになりましたでしょうか？**スタッフが強力でなくても自動化が進んでいるセキュリティプログラムは、強力なスタッフを備えた自動化が進んでいないセキュリティプログラムにほぼ匹敵するのです。**つまり、最初に申し上げたとおり、強力な自動化は強力なスタッフに取って代わることができるのです。

ですが、人間か機械かという問いは図 18 の重要なテーマではなく、最も重要な結論でもありません。青い線を自動化レベルに沿ってたどっていくと、人と機械の両方を追求すべきである説得力のある証拠が得られます。強力なチームを備えており、かつ主要な脅威検出および対応プロセスを自動化しているセキュリティプログラムは、ほぼ確実に（95% 以上）成功を収めることができます。ですから、自動化するからといって有能な人材を切り捨ててはいけません。自動化のおかげで有能な人材が優先度の高い活動に集中できるようになり、より一層能力を発揮できるようになるのです。

検出ルールの調整、ハッキング演習、脅威ハンティングの頻度は？

日々の活動の中で脅威検出およびインシデント対応プログラムの向上につながりそうなものは無数にありますが、これに関して実施した非公式の調査では、次の 3 つの活動が特に推奨されていました。

- 検出ルールとユースケースをテストし更新する
- 悪意のあるアクティビティの兆候をプロアクティブに捜索する
- レッド / パープルチーム演習に参加する

それぞれの活動の実施頻度を回答者に尋ね、脅威検出機能およびインシデント対応機能の高さと比較してみました。図 19 に示した結果では明確な傾向が見て取れます。

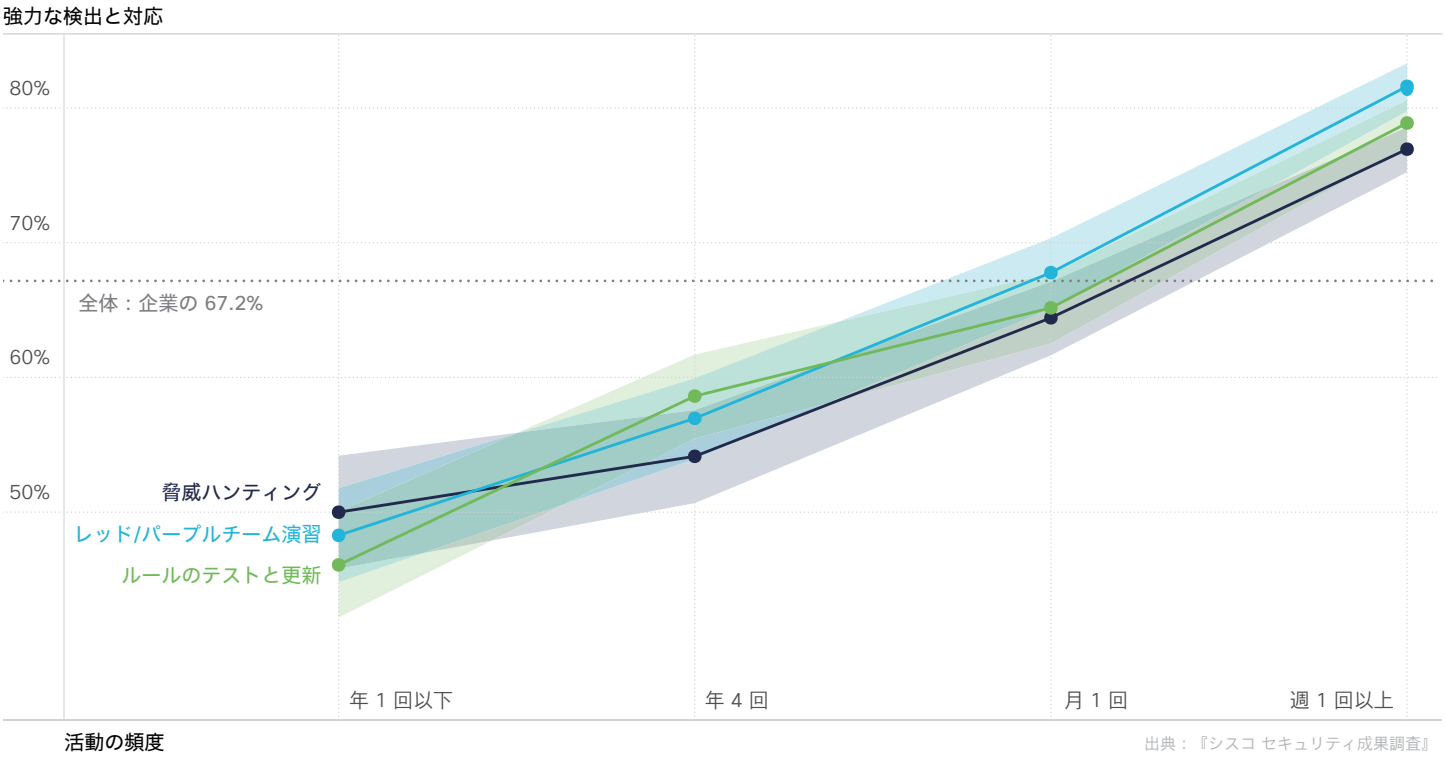


図 19 : 活動の頻度が脅威検出機能とインシデント対応機能に与える影響

検出ルールの調整、レッド / パープルチーム演習、脅威ハンティングはどれも似たような曲線を描いており、頻度が上がるほどセキュリティプログラムの効果が高くなっています。**週に 1 回以上実施する企業は、年に 1 回以下しか実施しない企業と比べてパフォーマンスが約 30% 向上しています。**ではどのくらいの頻度で実施すればよいのでしょうか？答えは「多ければ多いほどよい」です。

これらの活動を週に 1 回以上実施する企業は、パフォーマンスが約 **30%** 向上

「セキュリティは絶えず変化しており、トレンドから外れないようにする必要があります。以前は、セキュリティ問題やセキュリティインシデントの解決に膨大な時間を費やしていました。プロセスがシンプルになり、調査時間が短縮されたことで、新しいセキュリティトレンドに対応できるようになりました。新しいセキュリティソリューションを統合したより安全なインフラストラクチャが私たちの教育ネットワークを支えています。」

Bahruz Ibrahimov (AzEduNet 社、シニア情報セキュリティエンジニア)

詳細はこちら

迅速なディザスタリカバリとレジリエンスを実現

サイバーセキュリティにおいて「最優先」とされる側面が時とともに移り変わっていくのを見ると、興味が掻き立てられます。事業継続およびディザスタリカバリはデータ漏洩やサイバースパイ活動に何年も上位の座を奪われてきましたが、また表舞台に戻ってきました。それには正当な理由があります。ランサムウェアの攻撃、主要なホスティングプロバイダの停止などが相次いでいることから戦略の大幅な見直しが求められており、容赦のない脅威に対抗できるレジリエンスを確保することが必要になっているのです。

2021 年『セキュリティ成果調査』では、効果の高いサイバーセキュリティ プログラムの構築に寄与するプラクティスとして、迅速なディザスタリカバリが第 4 位の評価を獲得しています。このプラクティスは、セキュリティカルチャーを除く 11 種類すべての成果と高い相関性を示しました。以上のことを念頭に置いて、このプラクティスの効果を最大限に高めてレジリエンスを確保するための戦略を見ていきましょう。

ランサムウェアの攻撃、主要なホスティングプロバイダーの停止などが相次いでいることから戦略の大幅な見直しが求められており、容赦のない脅威に対抗できる復元力を確保することが必要になっているのです。

ディザスタリカバリは取締役会レベルで監督すべきか？

ディザスタリカバリ機能を最終的に監督しているのは誰なのか調査してみました。CIO、CISO、その他 IT 以外の最高責任者レベルの経営幹部がほぼ均等にその役割を担っており、それぞれが企業の事業継続およびディザスタリカバリプロセスの約 4 分の 1 を監督していることが分かりました。取締役会レベルでの監督はそれよりも一般的ではありませんが、調査した企業の 18% で行われています。

これらの回答を事業継続およびディザスタリカバリ機能の評価と比較すると、誰が監督するかが重要な問題であることが分かりました。**図 20 に示すように、取締役会レベルで事業継続およびディザスタリカバリを監督している企業は、強力なプログラムを構築していると回答する割合が最も高くなっています (平均を 11% 上回る)。**CIO が事業継続およびディザスタリカバリ機能を監督している企業では、平均を大幅に下回る最低の評価となっています。

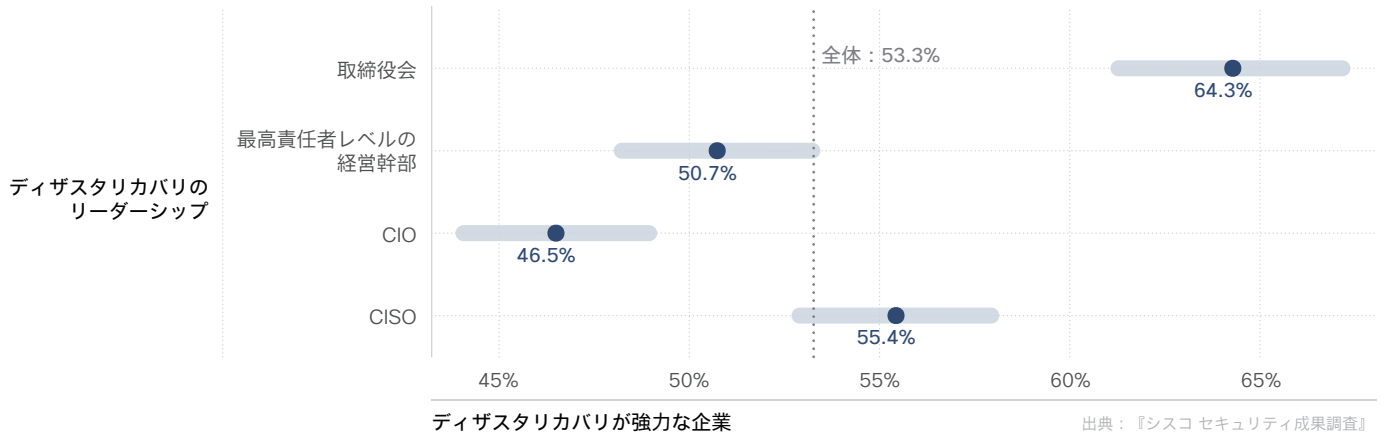


図 20 : 企業でのトップレベルによる監督がディザスタリカバリ機能に与える影響

図 20 のような結果になった理由は多数考えられますが、ディザスタリカバリの問題を取締役会で監督している企業は経営リスクとレジリエンスに対する問題意識が高いのではないかと私たちは考えています。この問題意識が、監督とサポートの強化や予算の増加につながっているものと思われます。したがって、ディザスタリカバリ機能の向上に苦労している企業は、ボトムアップではなくトップダウンで機能を構築してみるとよいかもしれません。

ディザスタリカバリの日々の運用は誰が行うべきか？

最終的な監督責任に加えて、ディザスタリカバリのより戦術的な側面の実行責任者について質問しました。**サイバーセキュリティチームまたは専門の事業継続チームがプログラムを運用している場合に最高のパフォーマンスが得られる傾向があります。**IT 部門がプログラムを運用している場合、ほとんどはそれを下回っています。興味深いことに、取締役会レベルでの監督にはすべての船を持ち上げる上げ潮のような効果があるようです。日々の運用責任がどこにあるかに関係なく、取締役会が最終的に監督していれば成功率は統計的に同等でした。

ディザスタリカバリのカバー率は重要か？

災害は備えがあろうがなかろうが時と場所を選ばず襲ってくる、というのは当然のことだと感じるかと思います。サイバーセキュリティの災害も例外ではありません。したがって、あらゆる不測の事態を想定して最善の準備を整えるのがサイバーセキュリティの常識となっています。しかし、言うは易く行うは難しです。

実際、ディザスタリカバリ機能が重要なシステムの 80% 以上をカバーしていると回答した企業は 3 割未満となっています。半数の企業がカバー率 50 ～ 79% で、それ以下のカバー率の企業が 20% 弱となっています。それほど悪い数字ではないと思った方もいらっしゃるかもしれません。なぜなら、ほとんどの企業が重要なシステムの半分以上をカバーしているからです。しかし、災害は不意を突いてやって来る傾向があることを忘れてはいけません。私たちのデータによると、そのような事例が認めるのも嫌になるくらい多いのです。

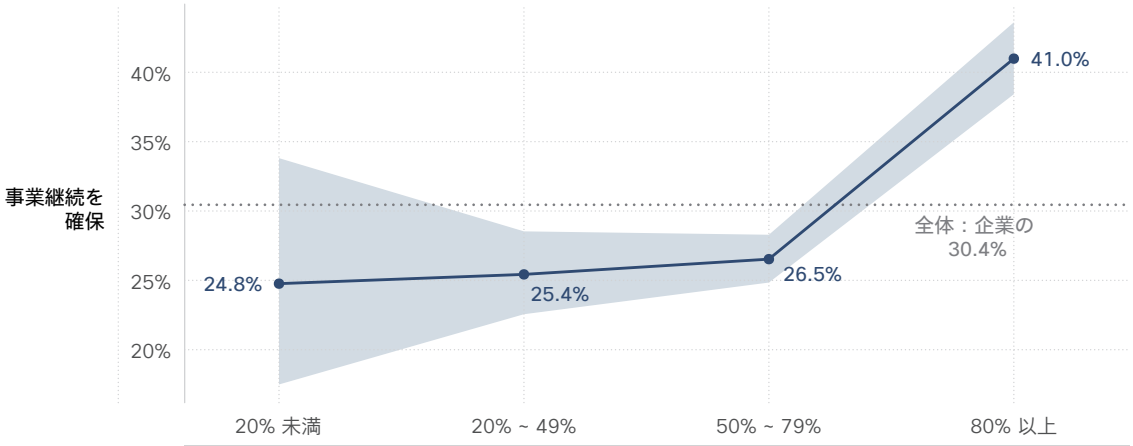


図 21 : 重要な資産のカバー率がディザスタリカバリ機能に与える影響

図 21 は、この調査で追加された新しい成果を測定したものです。目的は、破壊的な出来事に遭遇しても事業継続を確保できる能力を測定することです。これは、最も苦労していると回答者が答えた 3 つの成果のうちの 1 つです。したがって、成功の可能性を高める効果的な方法を見つけることが一層重要になります。

図 21 は、事業継続の確保に関する重要なメッセージを伝えています。**つまり、事業継続およびディザスタリカバリ機能が重要なシステムの 80% 以上をカバーするまで、この成果を達成できる可能性はまったくと言っていいほど向上しないのです。**

これは、災害は不意を突いてやって来ることを如実に物語っています。覚えておいていただきたいのは、事業継続とディザスタリカバリに投資するときはすぐに成果を求めたり投資額に応じた成果を期待したりしてはいけないということです。喜ばしいメッセージではなかったかもしれませんが、甘んじて災害に屈するよりはずっと良いのではないでしょうか？

テストを重ねれば完全なディザスタリカバリを実現できるか？

この質問では答えを先にお教えしましょう。残念ながら実現できません。しかし、まったくテストしない場合に比べれば、かなり良い結果を得られます。どれくらい良い結果になるか見ていくことにしましょう。

「どんな計画も初戦を迎えれば打ち砕かれる」という軍隊の格言はよく知られています。サイバー戦争の世界もこの格言の例外ではなく、事業継続およびディザスタリカバリ機能をテストするためにプランウォークスルー、机上演習、ライブテスト、並行テスト、完全実稼働テストなど、さまざまな手法が使用されています。こうした演習の実施頻度について回答者に尋ね、事業継続を確保できる可能性と比較してみました。

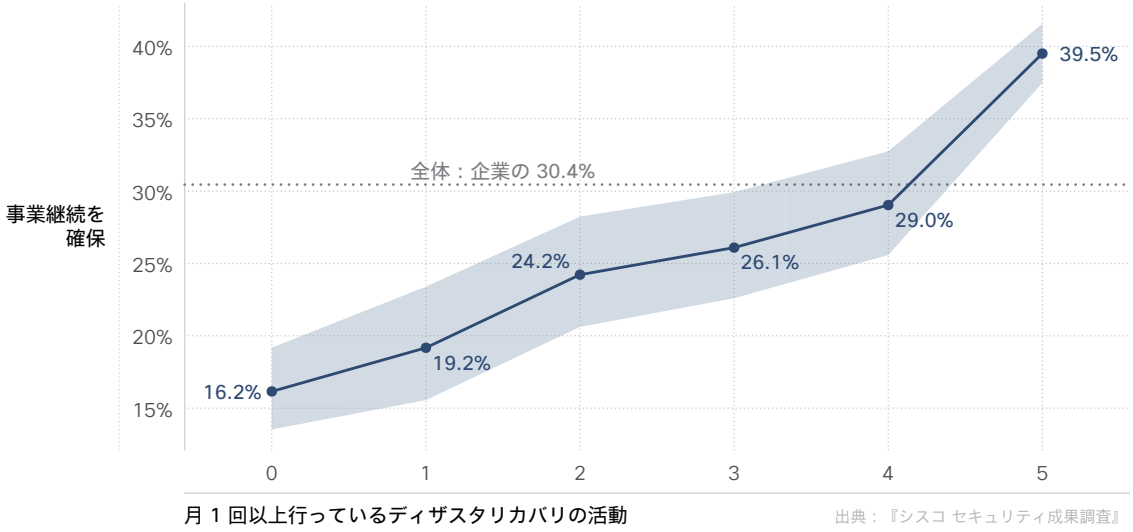


図 22：テストの実施がディザスタリカバリ機能に与える影響

これらのテストは有効性に顕著な違いはなく、すべてが相まってレジリエンスの向上に寄与していました。**5 種類のディザスタリカバリテストをすべて定期的に実施している企業は、1 つも実施していない企業と比べて事業継続を確保できる可能性がほぼ 2.5 倍になりました。**レジリエンスを確保するには成り行き任せではいけないのです。事業継続およびディザスタリカバリ機能に対してさまざまな角度から定期的にストレステストを行ってください。

5 種類のディザスタリカバリテストをすべて定期的に実施している企業は、事業継続を確保できる可能性が 2.5 倍である

カオスモンキーを放つべきか？

ディザスタリカバリ計画のストレステストを行う際は、「ストレス」を最大化するのが効果的です。これはカオスエンジニアリングと呼ばれていて、システムを（意図的に）定期的に混乱させて予期しない状況や出来事に耐える能力をテストする手法です。IT システムやセキュリティシステムにカオスモンキーを放てば企業のレジリエンス向上に役立つのか、以下で詳しく見ていきましょう。

カオスエンジニアリングをどの程度実施しているか回答者に尋ねたところ、予想より普及していることが分かりました。そしてこのプラクティスとテクノロジーの統合の間に注目すべき関係を見つけました。図 23 のように、カオスエンジニアリングを標準プラクティスにしている企業の 3 分の 2 以上が、高度に統合されたテクノロジーでリカバリ機能がサポートされていると回答しています。統合したことでカオスエンジニアリングが必要になったのかそれとも促進されたのかは分かりませんが、この業界でよくあるようにおそらくその両方なのでしょう。高度に統合された複雑な IT 環境で事業継続およびディザスタリカバリを担当している方は特に、この新しい手法に注目してください。

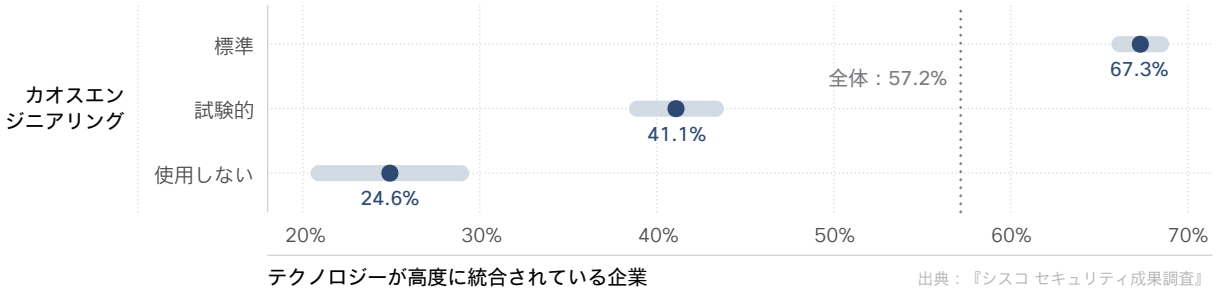


図 23：カオスエンジニアリングと IT 統合レベルの関係

図 24 のようにカオスエンジニアリングの活用度とビジネスレジリエンスの確保における成果を比較すると、ネットワークにカオスモンキーを放つとよいことが分かります。**カオスエンジニアリングを標準プラクティスにしている企業は、そうでない企業と比べて成果が向上する可能性が 2 倍になります。**このサルはなかなかやるじゃないかと驚かれた方は、カオスエンジニアリングを実践してカオスモンキーを使いこなし、サルに一泡吹かせてみてはいかがでしょうか？

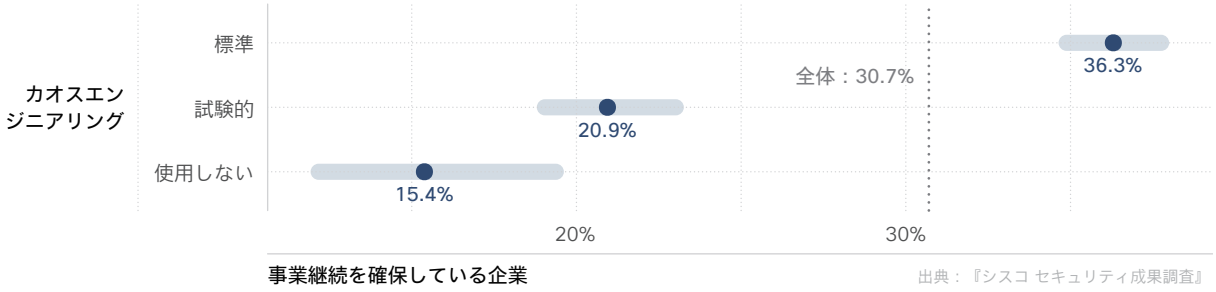


図 24：カオスエンジニアリングがビジネスのレジリエンスの確保に与える影響

まとめと提案

前回の調査で高い効果があると特定されたセキュリティプラクティスに注目し、新しい調査を行ってさらに情報を集め、それらのプラクティスが最も効果的である理由を解き明かして紹介しました。このレポートをご覧になった方が、サイバーセキュリティ プログラムをさらに向上させるための実践的なヒントを得ていただけたとしたら幸いです。

この種の調査結果の振り返りとして、いろいろな方々から感想を聞いてみても損にはなりません。そこで、経験豊富な CISO アドバイザリチームに協力をいただき、今回調査したそれぞれのプラクティス分野について話をうかがいました。以下に、主な提案をご紹介します。詳細な洞察や重要ポイントについては、シスコのセキュリティ成果調査ブログシリーズ、またシスコジャパン セキュリティブログをご覧ください。

プロアクティブな テクノロジーの更新

「古いセキュリティを使い続けてしまうのは深刻な問題です。CISO は『購入、保有、売却』戦略を策定して解決に導いていく必要があります。保有しているものを認識し、適応できるアーキテクチャを定義し、依存関係のリスクを軽減し、今後の更新サイクルのレビューループを導入することが必要です。」

Richard Archdeacon (シスコ、アドバイザリ CISO)

テクノロジーの 十分な統合

「最新の十分に統合された IT がセキュリティプログラム全体の成功に寄与することが分かりました。お客様の環境を改善するためにお勧めしたいのは、クラウドベースのセキュリティソリューションを探すこと、自動化できる分野を見つけること、購入要件にテクノロジー統合機能を含めることです。」

Helen Patton (シスコ、アドバイザリ CISO) @CisoHelen

タイムリーな インシデント対応

「インシデント対応チームが成果を出すには強力なスタッフが必要です。そしてさらに成果を高めるためにその他の要素も向上させていく必要があります。強力な人材、プロセス、テクノロジーを組み合わせることで、高度な脅威検出機能とインシデント対応機能を実現することができます。」

Dave Lewis (シスコ、アドバイザリ CISO) @gattaca

正確な脅威検

「スキルの高い人材をセキュリティチームに配置しましょう。単に頭数を増やすよりも重要なことです。専門知識が必要なレベルに達していない場合は、自動化によって経験の浅いスタッフとのギャップを埋めることができ、経験豊富なスタッフを揃えたときのような強力な結果を得ることができます。」

Wendy Nather（シスコ、アドバイザリ CISO） @wendynather

迅速なディザスタリカバリ

「このレポートの調査結果を見ると事業継続とディザスタリカバリの機能が重要であることが分かりますが、他のセキュリティ機能から切り離して運用してはいけません。リソースの優先順位付けやリスクのランク付けは、他のリスク管理機能と共有する必要があります。同様に、資産管理と脅威管理を緊密に統合することで、すべてのチームが同じ戦略に従って仕事を進められるようになります。」

Wolfgang Goerlich（シスコ、アドバイザリ CISO） @jwgoerlich

Cisco Secure について

シスコは長年にわたりインターネットを支えるテクノロジーの世界的リーダーとしての地位を守り続け、総合的かつオープンなサイバーセキュリティ ソリューションのポートフォリオを構築してきました。セキュリティソリューションは連携して機能するように設計すべきというのがシスコの基本的な考え方です。セキュリティソリューションとは本来、相互に連携して情報を取り入れ、協調的なユニットとして対応するものであるべきです。それが実現すれば、セキュリティはより体系的かつ効果的なものとなります。IT インフラストラクチャとネットワーキングサービスにおける世界最大のプロバイダとして、またエンタープライズ サイバーセキュリティ事業を手掛ける世界最大手として、シスコには長年の信頼と実績があります。

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。シスコは人とお客様を第一に考えて活動しています。また、複雑さとノイズを取り除き、自社のセキュリティに対する自信を高めたいというお客様の声にしっかり向き合い、成果に焦点を当てて開発に取り組んでいます。そのためには極度な単純化を避けつつシンプル化を推し進める必要があります。この目標に向けた大きな布石が、シスコのクラウドネイティブなプラットフォームです。

シスコは Cisco SecureX プラットフォームを通じて、現在および将来の脅威に対する安心感と信頼性をセキュリティのコミュニティに提供しています。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、www.cisco.com/c/ja_jp/products/security/index.html をご覧ください。

付録：調査サンプルの内訳

この付録では、今回の調査に寄せられた 5,123 件の有効な回答からなるサンプルの内訳を示します。調査結果の代表性を判断するための一助となれば幸いです。

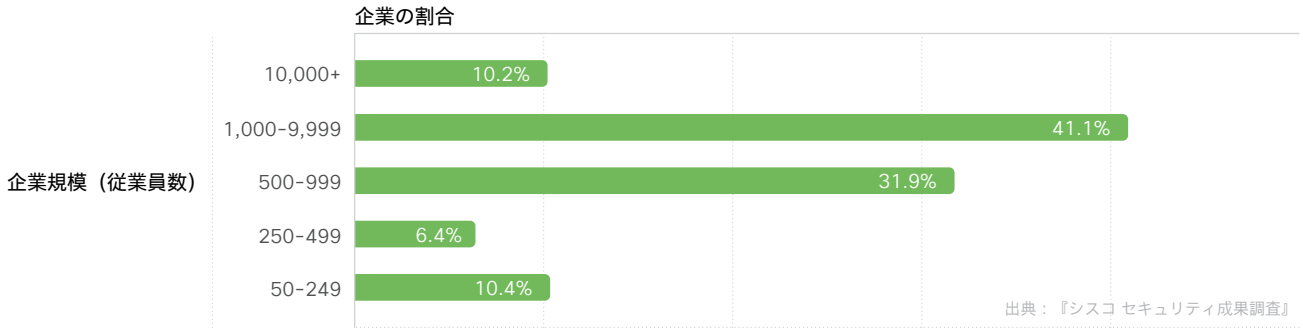


図 A1：参加企業の従業員数

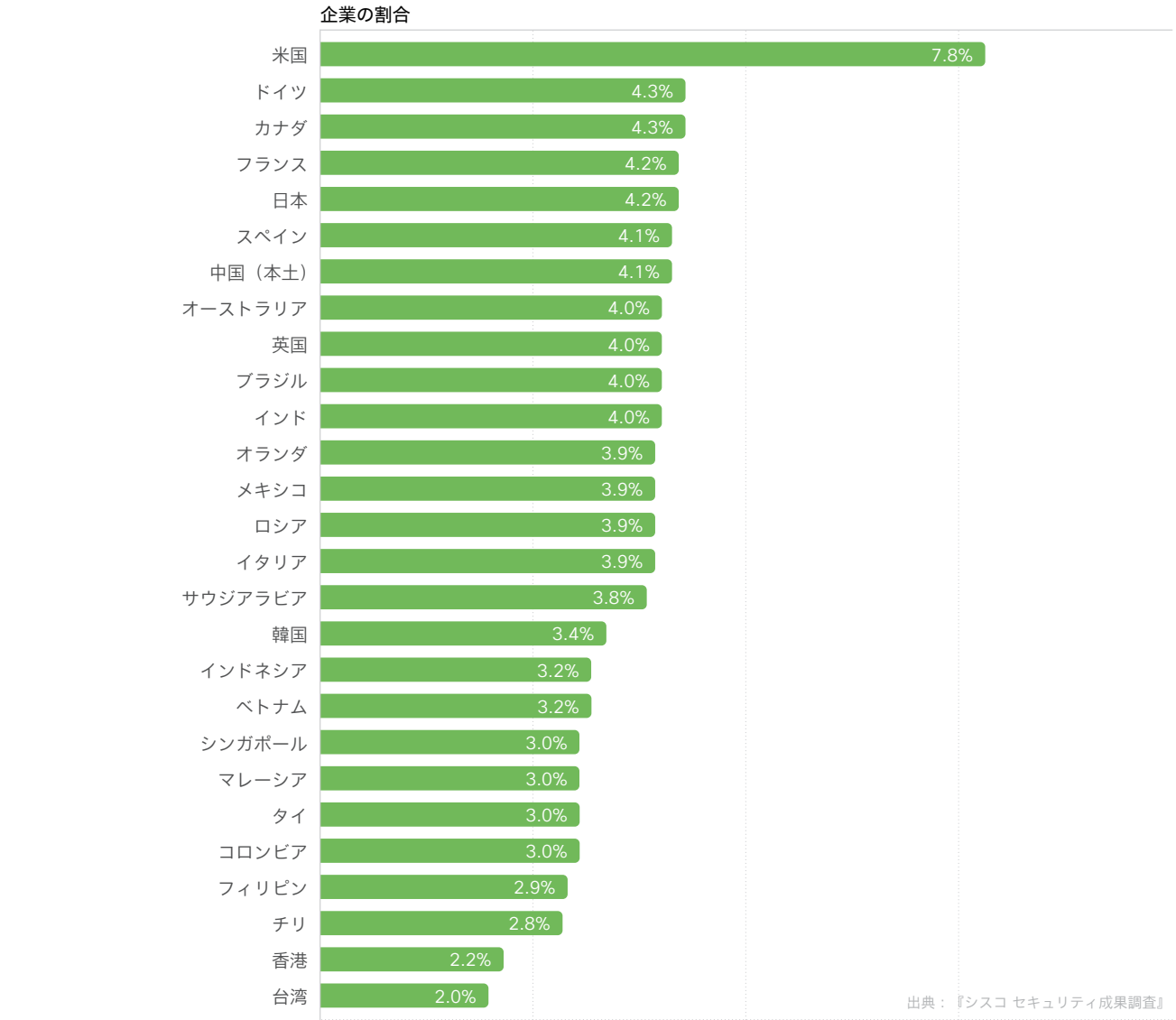


図 A2：参加企業の本社がある市場

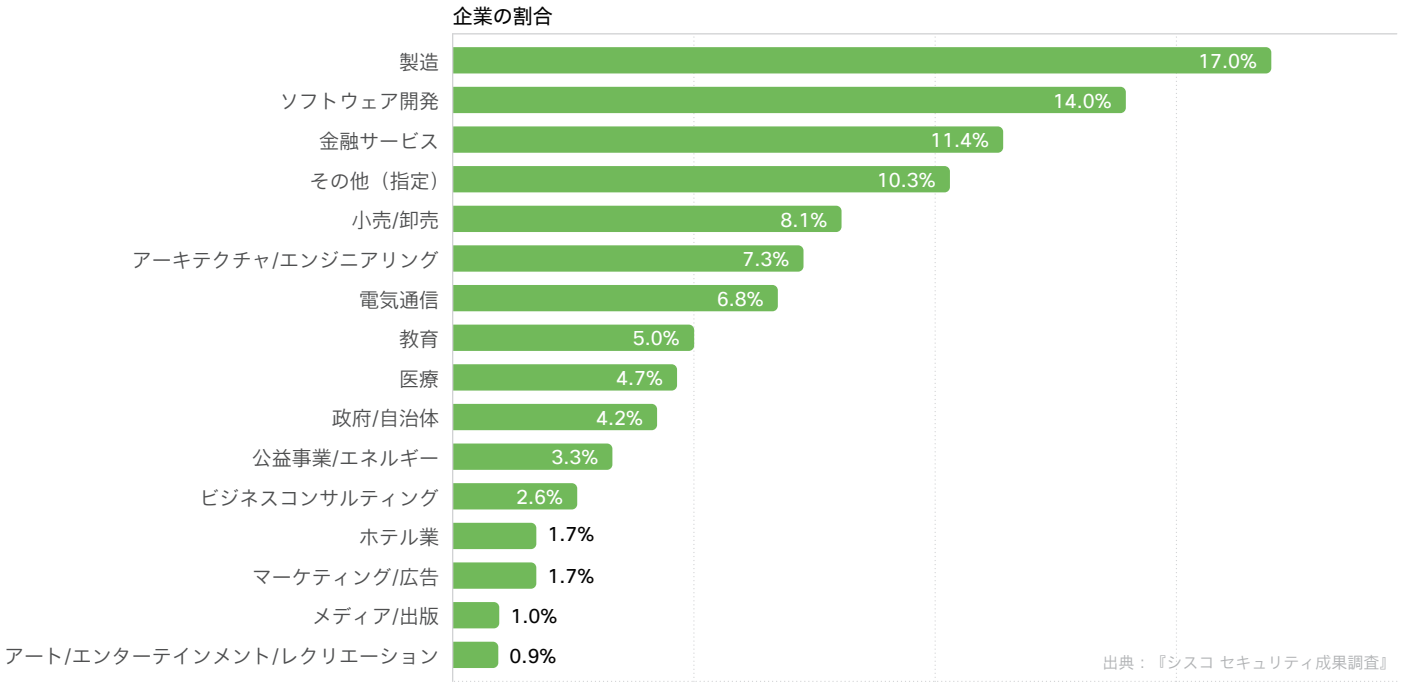


図 A3 : 参加企業の業種

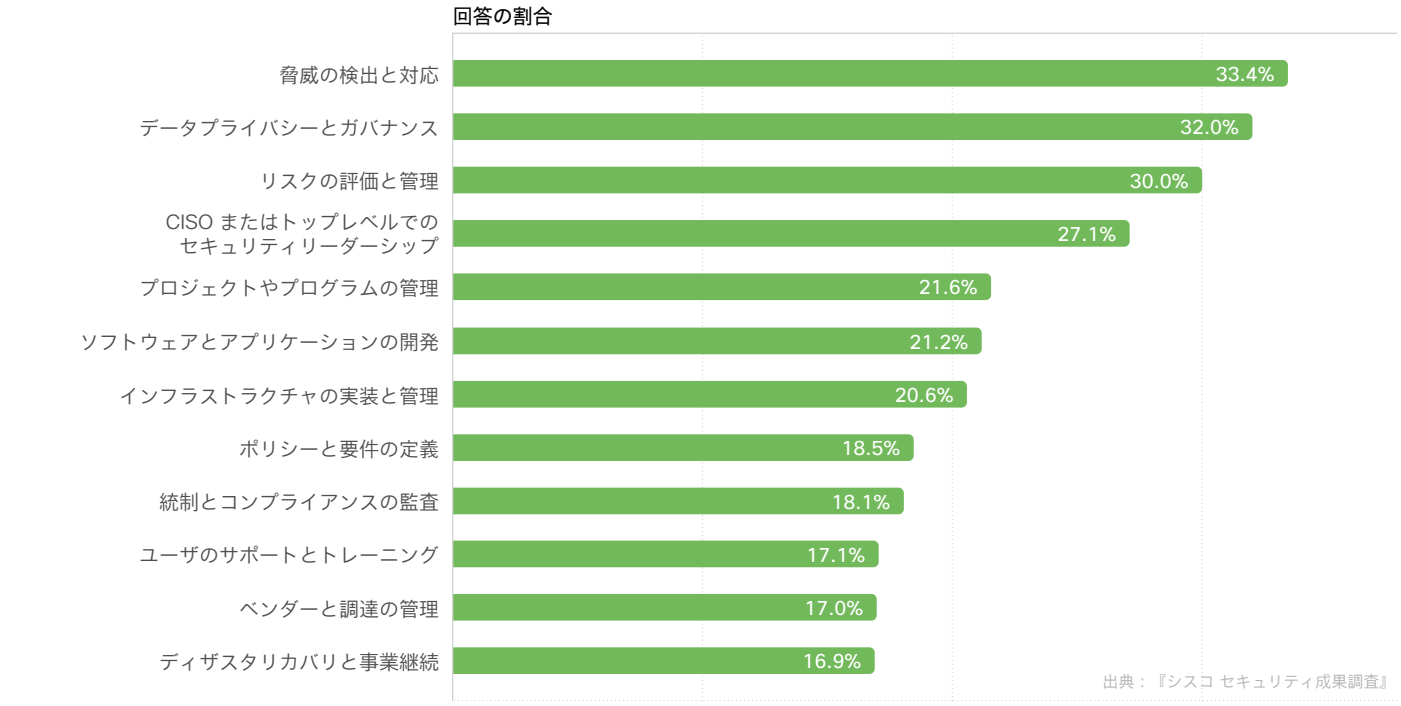


図 A4 : 回答者の主な職責

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

2021 年 12 月発行

The bridge to possible