cisco SECURE

セキュリティ

成果

調査

APJC

はじめに

サイバーセキュリティ プログラムを成功に導く要因は何か。セキュリティへの投資によって測定可能な成果が達成されることを示す証拠はあるのか。実際に効果がある要因と効果がない要因を見分けるにはどうすればよいか。これらの質問が 2021 年度シスコセキュリティ成果調査の最重要テーマです。本書は、アジア太平洋・日本・中国（APJC）地域に固有の調査結果のみを取り上げた、セキュリティ成果調査の補足資料です。本書をお読みいただくと、APJC 地域の国・市場においてセキュリティプログラムの成功に寄与する主な要因が何かを知ることができます。

2021 年度シスコセキュリティ成果調査は、IT、セキュリティ、プライバシー分野に従事する世界中の 4,800 人以上の専門家を対象に、（依頼元と回答者名を）完全に匿名にする方式で実施されたアンケート調査です。全回答者のうち 2,110 人が APJC 地域に本社を置く企業に勤めています。調査データの分析と取りまとめは、セキュリティ調査会社の Cyentia Institute 社が独自に行っています。

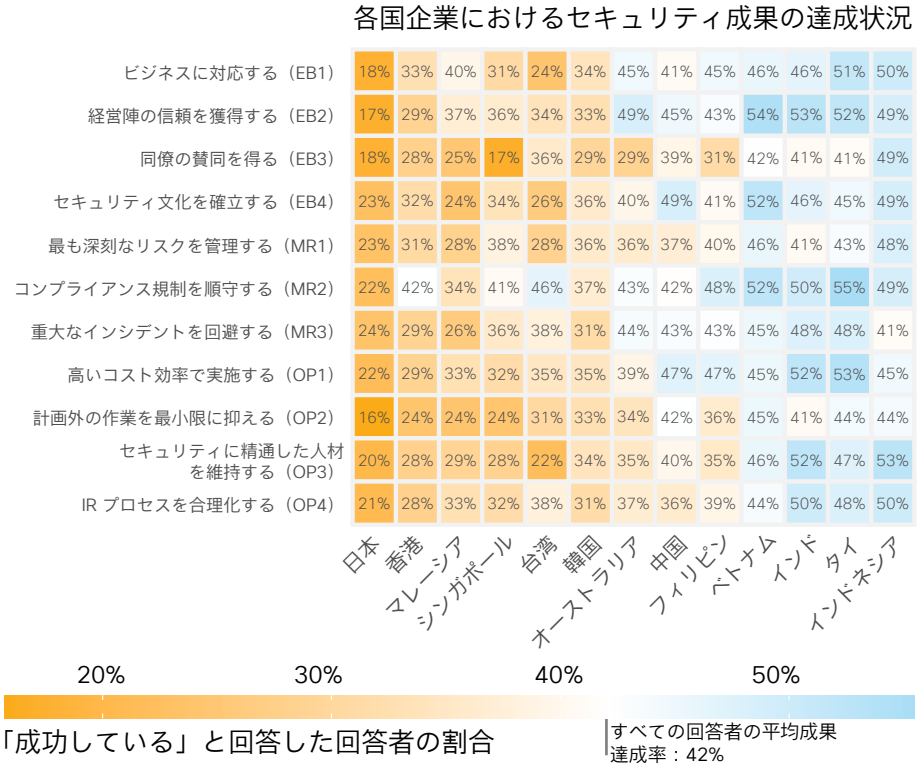
セキュリティプログラムの成果

本調査では、高次のセキュリティ成果 11 種類と主要目標 3 種類（ビジネスの促進、リスク管理、業務の効率化）のすべてにわたって、各企業がどのくらい成功しているのかを回答者に尋ねました。[1] 最終的な目標はこれらの成果の達成に寄与するセキュリティプラクティスを特定することですが、あまり先走るのはよくありません。まずは、APJC 地域の国・市場が、他の地域と比較して、どの点で苦労していて、どの点で勝っているのかをじっくり見ていきましょう。

[1] 2021 年度セキュリティ成果調査の付録 B には、各成果の全文が掲載されています。また、回答者がプログラムの成功度合いを評価する際の目安となる説明と実例も載っています。

図 1 は、セキュリティプログラムの各成果項目をすでに達成できていると回答した企業の割合を国別に示しています。たとえば、日本企業の 18% が、自分の会社のセキュリティプログラムはビジネスに対応できていると回答しており（左上のセル）、インドネシア企業の 50% がインシデント対応(IR) プロセスを合理化できていると回答しています(右下のセル)。また、成功の度合いを相対的に示すために色分けも行っています。オレンジ色のセルはその国の回答者から報告された成功の度合いが世界平均を下回っていることを示し、青いセルは世界平均を上回っていることを示しています。この図からも明らかなように、苦労している分野と成功している分野は国によって異なります。

図 1：　APJC 地域各国におけるセキュリティ成果ごとの成功度の比較



出展：シスコ 2021 年度セキュリティ成果調査

図 1 に示されているすべての国にわたってそれぞれの成果を比較し、コメントすることはできませんが、読者の皆様が自ら結論を導き出すのに役立ちそうなヒントとガイドラインをここでいくつかご紹介します。それでは、詳しく見ていきましょう。

図の各列はその国における成果項目ごとの達成度を示しています。横軸には、すべての成果項目の相対的成功度が低い方から順に、左から右へ国名が並んでいます。このことから、日本の回答者はどの成果項目についても成功していると報告する割合が低い傾向にあることがわかります。一方、インドネシアの回答者は成功していると報告する割合が高くなっています。

前の文で「報告」という言葉を太字にしているのは、これらの調査結果を解釈する上で重要なポイントになるからです。図 1 に示すパーセンテージからは、実際に成功しているのか、ただ成功していると思っているだけなのかは判断できません。ここには各国の文化的要因が大きく影響していると考えられます。「インドネシアのセキュリティプログラムは常に日本のプログラムよりも成功している」といった過度に単純化された結論を出すのは避けましょう。実際には逆かもしれません。日本企業は高いセキュリティ目標を設定し、結果を厳密に測定し、改善点を正確に把握しているために自己採点が厳しくなっている可能性もあります。こうした解釈は、他のビジネス分野における日本企業に対しての評価とも合致しています。

図 1 からはさまざまなことが読み取れます。図の下の部分から関心のある国・市場を選び、その列にある各成果の成功度を確認してみてください。色分けは、その国の企業が苦労している領域（オレンジ色のセル）、成功している領域（青のセル）、世界平均と同等の領域（白のセル）をすばやく把握するのに役立ちます。

図 1 に示す国別の結果をじっくりと比較することが重要です。その国の回答に影響を与えている要因が何かを考え、プログラムの成功に必要なものをより深く理解する上でその考察がどのように役立つかを考えてみましょう。多国籍企業の場合は、各国のセキュリティチームが一体となって共通のプログラムに取り組めるよう、これらの結果を参考にして各国の間にある認識と実態の違いを確認してみるのもよいでしょう。

図 1 は成果の観点からも見ることができます。その場合は、成果項目を選び、その行に並んでいる各国の成功度を比較してみてください。そうすると、多くの国が「コンプライアンス規制の順守」に成功していると報告している（青と白のセルが多い）のに対し、「同僚の賛同を得る」ことには苦労している（オレンジのセルが多い）のが分かります。繰り返しになりますが、これらの調査結果には、成功している（あるいは苦労している）と回答者が思っているだけのケースも含まれる可能性があります。しかし、回答者の間で意見が一致している領域と異なる領域を知ることは、グローバルコミュニティで共有されているセキュリティ上の課題を把握する上で極めて有益と言えます。

図 1 を全体的に見ると、APJC 地域ではセキュリティプログラムの成功度に大きなばらつきがあることがわかります。しかし、この地域の企業におけるこうした状況は改善可能なのでしょうか。データは可能と言っています。以下では、各国の企業においてセキュリティプログラムの成功度の向上に寄与している要因について説明します。

より広範にわたる国レベルのプログラム成果について

幸いなことに、今回の調査では、図 1 に示す APJC 地域諸国の成功度だけでなく、その他の地域の成功度も詳しく確認できるインタラクティブ データ グラフも作成しました。世界平均を基準にして各国の成功度が評価されるため、各国の企業がどの分野のセキュリティ成果を達成するのに苦労していて、どの分野の成果を達成できているのかを一目で確認できます。

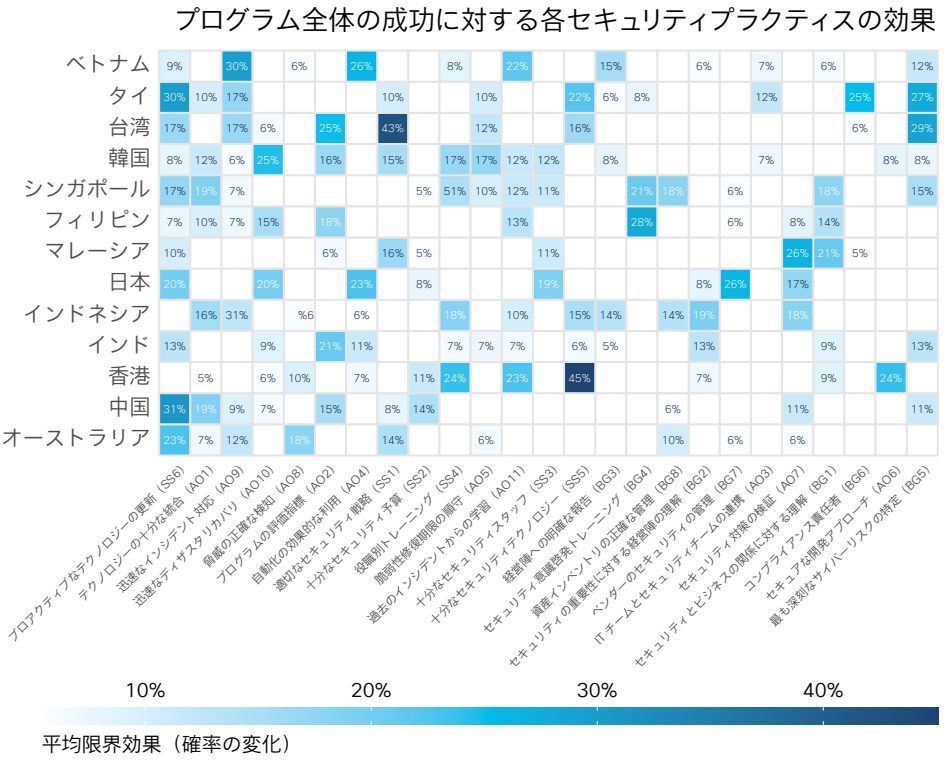
主要な成功要因

本調査では、上記の成果に加え、25 種類の一般的なセキュリティプラクティスをどの程度忠実に実践できているかを回答者に尋ねました。[2] その後、多変量解析を行い、どのプラクティスが各目標の達成に最も大きく寄与しているかを測定しました。言い換えると、APJC 地域の企業にとってセキュリティプログラムの成功に寄与する要因は何なのかを尋ねました。それでは、結果を詳しく見てみましょう。

[2] これらのプラクティスの全文とリストは、2021 年度セキュリティ成果調査の付録 C に掲載されています。

図 2 の数値は、各プラクティスを忠実に実践した場合、プログラム全体の成功度が平均でどのくらい増加する可能性があるかを示しています。たとえば、プロアクティブなテクノロジー更新戦略を実施していると回答したベトナムの企業は、セキュリティプログラムが非常に成功していると報告する可能性が平均で 9% 高くなります（左上のセル）。白または数値が記載されていないセルは、その国において、該当するプラクティスとセキュリティプログラム全体の成功度との間に統計的に有意な相関性が見られなかったことを示しています。ただし、それらのプラクティスが図 1 に示されている特定の成果に影響を及ぼしている場合もあります。

図 2: APJC 地域において各セキュリティプラクティスがセキュリティプログラム全体の成功度にもたらす影響



出展：シスコ 2021 年度セキュリティ成果調査

図 1 と同様に、図 2 も列と行に沿って情報を読み取ることができます。なお、図 1 と同様に図 2 についても、すべての項目について言及することはできませんが、この図からできるだけ多くの洞察を得るためのヒントをご紹介します。

図 2 を最大限に活用するには、図の左側から特定の国または市場を選んで、その行にホットスポット（青いセル）があるかどうかを横に見ていきます。青いセルが見つかった場合は、その列の下に記載されているセキュリティプラクティスを確認します。青が濃くなるほど、該当する国または市場において、そのプラクティスがセキリティプログラムの成功に大きく寄与していることを示しています。そうすることで、セキュリティプログラムの改善に効果がありそうなプラクティスをデータに基づいてすばやく確認できます。

また、列に沿って縦にデータを見ていくと、多くの国でセキュリティプログラムの成功に大きく寄与していそうなプラクティス（プロアクティブなテクノロジーの更新など）や、効果が特定の国に限定されているプラクティス（タイの「コンプライアンス責任者」や、日本の「ベンダーのセキュリティの管理」など）を確認できます。多国籍企業の場合は、このアプローチを取ることにより、それぞれの国で成功に寄与しているプラクティスを特定できます。

図 2 の各行を横に見ていくと、各国のセキュリティプログラムの成功に寄与しているプラクティスを確認できます。たとえば、台湾企業の場合は、セキュリティ戦略の確立に力を入れることで成功度が大きく上がると予想されます（平均上昇率は 43%）。また、香港企業の場合は、適切なセキュリティテクノロジーへの投資に力を入れることで ROI（投資回収率）が大きく向上すると予想されます（平均上昇率は 45%）。その他の国についても同様に見ていくことができます。いずれの国においてもセキュリティプログラムの成功に寄与する要因が 1 つだけでないことがデータに基づいて示されたのは、非常に喜ばしいことと言えるでしょう。

「シスコとのパートナーシップがもたらした最大のメリットは、システム利用者の間に安心感が広がったことです。スタッフの間には常に作業を続けられ、どこにいてもシステムが保護されているという安心感が生まれ、学生の間には最小限の中断で学習を継続できるという信頼感が生まれています」

西オーストラリア大学サイバーセキュリティ & テクノロジー リスク アソシエイト ディレクター、Lee Patterson 氏

Cisco Secure について

シスコは Cisco Secure のポートフォリオと 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。現在、すべてのフォーチュン 100 企業が、世界で最も包括的なシスコの統合型サイバーセキュリティ プラットフォームにより現在と将来の脅威から守られています。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。

https://www.cisco.com/go/secompanies で、シスコのお客様のセキュリティに関する最新事例もぜひご覧ください。

お問い合せ先

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

APJCRPT_12_2020JA 20.12

シスコセキュリティ成果調査

全世界を対象に実施されたセキュリティ成果調査のレポート、インタラクティブ データ グラフ、調査結果の要点をまとめたビデオは、https://cisco.com/jp/go/SecurityOutcomes でご覧いただけます。

セキュリティ成果調査ブログシリーズもぜひご覧ください。ソーシャルチャネルでの会話に進化したい場合は、ハッシュタグ #SecurityOutcomes をご利用ください。

CISCO

SECURE

The bridge to possible