

レポート

MSP のビジネス展望 2026 年版

サイバーセキュリティサービスの将来の課題と機会について MSP 800 社を対象にした調査結果。

2026 年 9 月



エグゼクティブサマリー

サイバーセキュリティは、リーダーシップの欠落という危機に直面しています。世界では1万組織につきCISOはわずか1人しか存在していません¹。大多数の組織が、専任の責任者を配置しておらず、セキュリティが確保されていることを検証するために必要な体制と戦略がありません。その一方で、この問題をさらに深刻にするように、インシデントは増え続け、セキュリティへの支出は増加し、経営幹部は自社のセキュリティ体制に依然として確信を持てずにいます。組織はこれまで以上にセキュリティへの投資を増やしているものの、多くの組織はいまだに、自社が抱えるリスクやレジリエンス、そしてセキュリティ投資によってどのような成果が得られているのかという基本的な問いに答えられずにいます。

このギャップは、マネージドサービスプロバイダー (MSP) やその他のチャネルパートナーにとって、サービスの提供にとどまらず、信頼されるサイバーセキュリティのリーダーになる大きな機会となります。本レポートの調査結果から、顧客がサイバーセキュリティ対策全般について、技術的な導入から全面的な管理に至るまで、パートナーに助言を求める傾向が強まっていることが明らかになりました。複雑な状況を整理して明確にし、顧客が自社の現状や改善の進捗、リスクが残存する領域を把握できるよう支援するパートナーが、このリーダーシップの空白を埋める存在となるでしょう。

しかし、多くの顧客にサイバーセキュリティのリーダーシップを提供するには、専門知識だけでは不十分です。19ページに示すように、MSPは、セキュリティとコンプライアンスに関する業務を単一の統合プラットフォームで管理できれば、**チームの作業時間を半分以上削減できると見積もっています**。これは、業務効率の重要性を浮き彫りにしています。高まる顧客ニーズに応えるため、プロバイダーには、顧客全体にわたって再現可能な形でセキュリティ戦略を主導し、規模を拡大しながら、その成果を測定できるモデルが必要です。



Scott Barlow
VP、チーフエバンジェリスト
ソフォス

¹ <https://www.sophos.com/ja-jp/resources/report/2026-ciso-report>

はじめに

ソフォスの「MSP のビジネス展望レポート 2026 年版」は、MSP の以下の 3 つの戦略的なビジネス分野について、詳しく分析しています。

- MSP が担うサイバーセキュリティリーダーシップの重要性の高まり
- コンプライアンスを中核とする MSP のサービス提供
- セキュリティとコンプライアンスの大規模な運用

本レポートは、米国 (200 社)、英国 (100 社)、ドイツ (100 社)、フランス (100 社)、シンガポール (100 社)、オーストラリア (100 社)、ブラジル (100 社) の MSP 合計 800 社を対象に実施した、ベンダーに依存しない独立した調査結果に基づいています。回答者は、MSP の上級職から取締役会レベルまでの関係者で構成されています。

この調査は、ソフォスの委託を受けて調査会社の Vanson Bourne が 2026 年 4 月に実施しました。

800 社

MSP

7 つ

注目すべきコンプライアンス領域

7 か国

国の数

主な調査結果の概要

1. MSP は顧客にとって事実上の CISO になっている

- 88% の MSP が、少なくとも **20%** の顧客から CISO としての役割を担うことを期待されていると回答しています。
- **84%** の MSP が、今後 12 か月間で CISO サービスへの需要が増加すると予想しています。

2. コンプライアンスサービスは広く提供されているものの、成熟していない

- **99%** の MSP がコンプライアンスサービスを提供しています。
- 包括的なコンプライアンスサービスを提供している MSP は **6%** に過ぎず、今後さらにサービスを拡充する余地があります。

3. コンプライアンスがセキュリティ投資を後押し

- 顧客の購買決定の **50%** は、コンプライアンス要件によって左右されています。
- 購買決定の平均 **33%** で、コンプライアンス要件が主要な要因として影響しています。

4. 継続的なコンプライアンス対応が徐々に進んでいる

- **62%** の MSP が、複数の顧客にわたってコンプライアンスを継続的に監視、管理、文書化する能力に「非常に自信がある」と回答しています。
- 「完全に自信がある」と回答した MSP は **33%** であり、多くの MSP に改善の余地があることが浮き彫りになっています。

5. ツールを活用したサービス提供が標準に

- **53%** の MSP が、サイバーセキュリティのコンプライアンス対応や CISO 業務に関する活動を一元管理するために、複数のツールやプラットフォームを使用しています。
- 単一のツールやプラットフォームに統合している MSP は **36%** にとどまっており、MSP とその顧客の業務が、複数のツールによって分断され、十分に対応しきれていない可能性のある体制に置かれていることがうかがえます。

6. セキュリティレポートの自動化が進んでいる

- **86%** の MSP が、セキュリティポスチャを統合したレポートを作成するために、完全または半自動化されたプロセスを利用しています。
- 一方、**55%** の MSP では、アクティビティを集約する際に依然として手作業が必要であり、多くのレポート作成プロセスはまだ部分的な自動化にとどまっています。

7. 大幅な効率化を実現する余地がまだ残されている

- 顧客のセキュリティポスチャとコンプライアンスの管理やレポート作成を統合された単一のプラットフォームで行えるようになれば、MSP は作業時間を **53%** 削減できます。
- **81%** の MSP が、こうした業務に現在費やしている時間を **30%** 以上削減できると考えています。

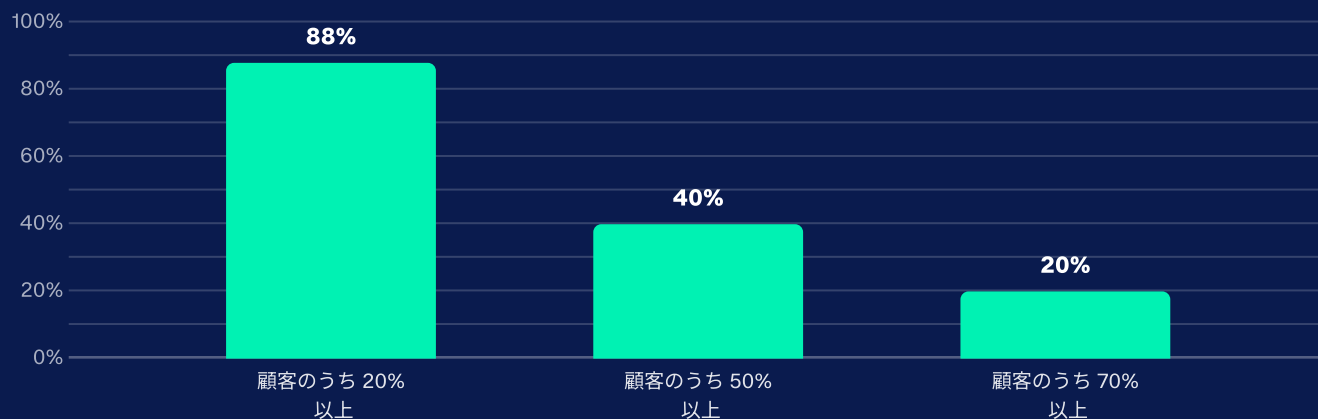
第1部：MSP が担うサイバーセキュリティリーダーシップの重要性の高まり

1.MSP は顧客にとって事実上の CISO になっている

組織は、変化する脅威環境、AI (人工知能) を利用した攻撃、規制の拡大、そしてセキュリティ人材の不足によるプレッシャーの高まりに直面しています。また、多くの組織では、テクノロジーの管理だけにとどまらず、体系的なサイバーセキュリティプログラムを通じてこうした課題に対応するために必要な、リーダーシップも社内でも不足しています。こうした状況を受け、MSP は提供するサービスの価値を高め、戦術的なツールの提供者から戦略的なアドバイザリーパートナーへと進化しています。

本レポートの調査データは、この変化が着実に進んでいることを示しています。MSP は平均して、**顧客の 46%** が現在、このようなサイバーセキュリティにおけるリーダーシップを MSP に頼っていると見積もっています。こうした MSP への依存は広く見られます。**88% の MSP が顧客の 20% 以上に対して CISO としての役割を担っています。**その割合が 50% を超えている MSP は **40%** であり、**70% を超えている MSP は 20%** です。

MSP が提供する CISO サービスへの顧客の依存度



※顧客のうち、CISO としての役割を期待している顧客の割合はどの程度ですか？ (回答者数 = 800)

88%

MSP のうち、20% 以上の顧客に対して CISO としての役割を担っている割合。

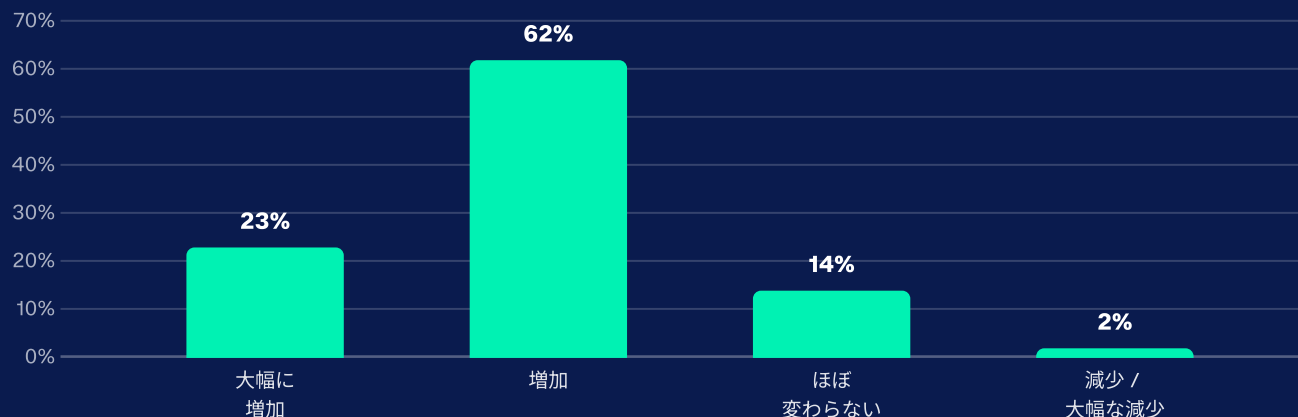
46%

MSP にこの役割を担うことを期待している顧客の割合。

MSP が提供する CISO サービスの需要は増加している

MSP にとってのこのビジネス機会は、今後さらに拡大することが予測されます。**84%** の MSP が今後 12 か月間に CISO サービスの需要が増加すると予想しており、そのうち **23%** が大幅な成長を見込んでいます。減少すると予想している MSP はわずか **2%** です。

CISO サービスに対する需要の予想される変化



今後 12 か月間でこれがどのように変化すると予想していますか (変化がない場合も含む) ? (回答者数 = 800)

MSP の従来の役割の範囲は急速に変化しています。これは、専任のセキュリティ責任者を社内置き、その活動を支えるための専門知識、リソース、資金が不足している組織が直面する課題を反映しています。こうした組織は現在、日々のテクノロジー管理にとどまらず、CISO レベルの戦略的なサイバーセキュリティに関する助言、リスク管理、ガバナンスを MSP に求めています。このギャップを埋め、顧客から真っ先に頼られる存在としての地位を確立できるプロバイダーは、今後高まる需要を取り込む上で有利な立場にあります。

84%

今後 12 か月間で CISO サービスへの需要が増加すると予想している MSP の割合。

23%

大幅に増加すると予想している MSP の割合。

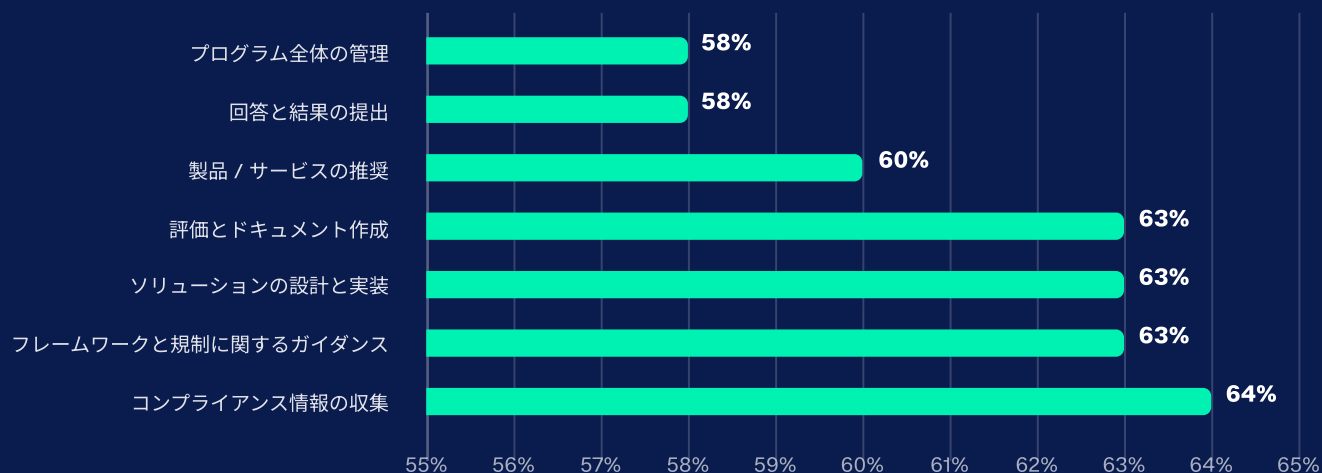
第2部：コンプライアンスを中核とする MSP のサービス提供

1. コンプライアンスサービスは広く提供されているものの、成熟していない

サイバーセキュリティのコンプライアンス対応は今や、MSP が提供する主要な価値となっています。その背景には、専任の体制による継続的なサイバーセキュリティプログラムの管理を求める規制や法律の増加があります。MSP は、こうしたサービスを提供するのに非常に適しています。

調査対象となった7つのコンプライアンス活動全体にわたって、サービス提供は一貫して高い水準にあります。記載された各サービス領域について、**58～64%のMSP**が、すでに該当するサービスを顧客に提供していると回答しています。

現在7つのコンプライアンス領域のそれぞれを提供している MSP の割合



現在および今後において、顧客のサイバーセキュリティのコンプライアンス対応に関する貴社の関与について、最もよく当てはまるものは次のうちどれですか？（回答者数=800）

99%

何らかのレベルのコンプライアンス
サービスを提供している MSP の割合。

58%

プログラム全体を管理している割合。

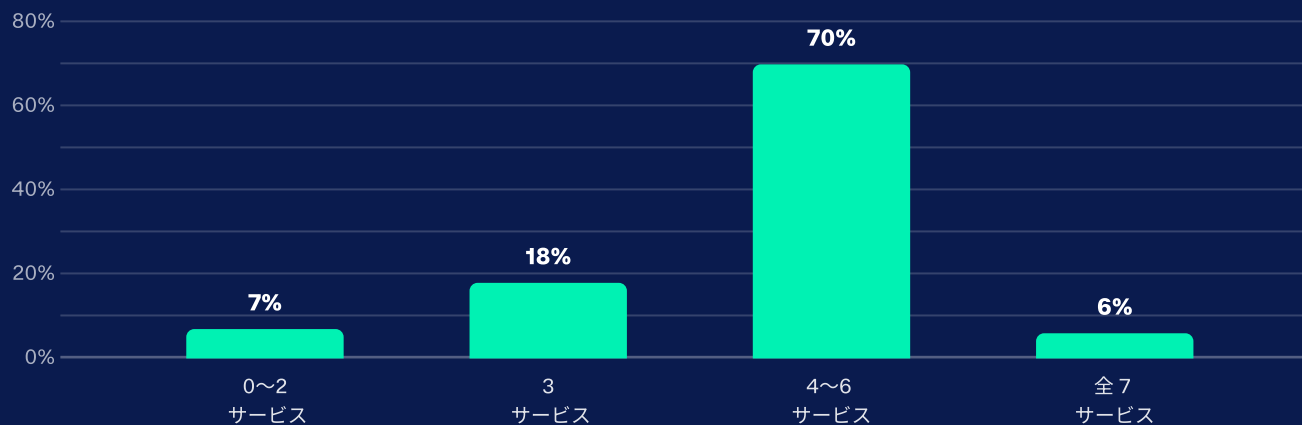
6%

包括的なコンプライアンスサービスを
提供している割合。

包括的なコンプライアンスサービスを提供している MSP はごく少数

個々のコンプライアンスサービスは広く提供されているものの、多くの MSP はコンプライアンスのライフサイクル全体をカバーするまでには至っていません。調査対象となった7つの活動のうち、4～6つを提供している MSP が **70%** を占める一方、7つすべてを提供している MSP はわずか **6%** です。これは、多くの MSP が、提供するサービスをさらに拡充するとともに、これらの機能をエンドツーエンドのコンプライアンスプログラムとして連携させ、顧客が必要とする包括的な管理体制を実現する必要があることを示しています。

提供されるコンプライアンスサービスの深さ

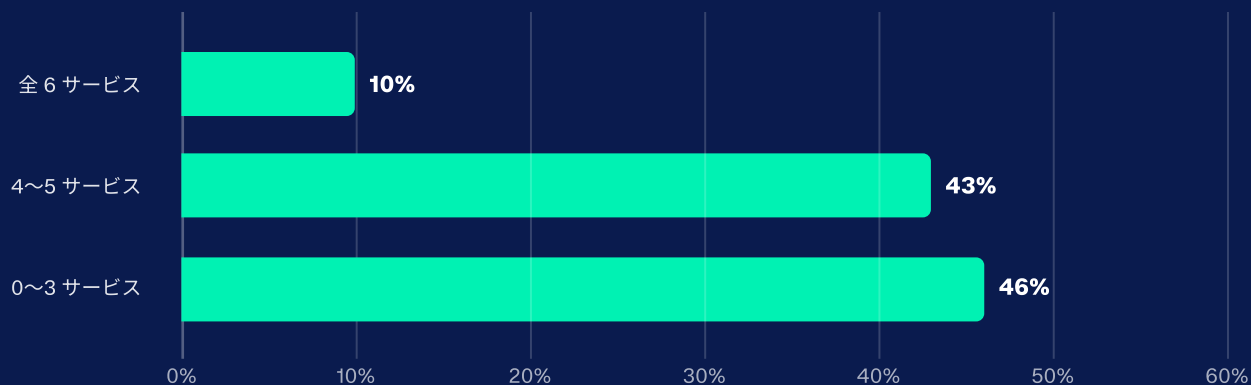


現在および今後において、顧客のサイバーセキュリティのコンプライアンス対応に関する貴社の関与について、最もよく当てはまるものは次のうちどれですか？ (回答者数=800)

コンプライアンスプログラムを管理している MSP でも、必要な支援サービスをすべて提供しているわけではない

顧客のコンプライアンスプログラム全体を管理している MSP だけを見ても、同様のギャップが見られます。これらの **MSP の 58%** のうち、他の 6 つのサービスも提供しているのはわずか **10%** です。これは、多くの MSP が、包括的なコンプライアンスサービスを整備する前に、プログラム全体を管理する責任を担っていることを示しています。実際には、コンプライアンスプログラムの管理には、MSP 自身が各サービスを直接提供するのではなく、顧客や第三者の専門業者が実施する活動を調整することも含まれます。そのため、コンプライアンスプログラム全体を管理する能力と、個々のサービスを提供する能力が必ずしも伴っているとは限りません。

フルプログラム管理を提供する MSP によって提供されるコンプライアンスサービスの数



※なおおよび今後において、顧客のサイバーセキュリティのコンプライアンス対応に関する貴社の関与について、最もよく当てはまるものは次のうちどれですか？ MSP がコンプライアンスプログラム全体を管理 (回答者数 = 465)

MSP はコンプライアンスサービスの拡充を計画している

こうしたサービスへの需要が、今後さらなるサービス拡充を促すと考えられることは、好材料です。現在、コンプライアンスサービスを提供していない MSP の多くが、今後、その提供を開始することを計画しています。最も大きな成長が見込まれるのは、コンプライアンスプログラム全体の管理です。すでに 58% の MSP がこのサービスを提供しており、現在提供していない MSP のうち 40% が今後提供することを予定しています。これは、プログラム管理が MSP の標準的なコンプライアンスサービスになりつつあることを示しています。

サービス	現在提供中	導入予定	合計
製品 / サービスの推奨 コンプライアンス目標をサポートするセキュリティツールやサービスについて助言する。	60%	38%	99%
ソリューションの設計と実装 コンプライアンス要件を効果的に満たすためのセキュリティ制御を構成および展開する。	63%	37%	100%
フレームワークと規制 顧客のコンプライアンスに適用される規制、標準、フレームワークを特定する。	63%	36%	99%
コンプライアンス情報の収集 コンプライアンス要件を満たすために顧客が必要とする証拠を提供する。	64%	35%	99%
評価とドキュメント作成 評価を実施し、コンプライアンスの状況とギャップを示す文書を作成する。	63%	36%	98%
回答と結果の提出 監査への回答、アンケート、コンプライアンス証拠を作成し、提出する。	58%	40%	98%
プログラム全体の管理 継続的なコンプライアンス活動、証拠収集、報告、ガバナンスを監督する。	58%	40%	99%

現在および今後において、顧客のサイバーセキュリティのコンプライアンス対応に関する貴社の関与について、最もよく当てはまるものは次のうちどれですか？「わからない」を除く (回答者数 =800)

割合は四捨五入されています。

コンプライアンスサービスは、規模を問わず MSP が成長を期待できるビジネス

MSP のコンプライアンスサービスの成熟度は、規模によって決まるものではありません。従業員 51 人以上の MSP では、調査対象となった 7 つすべてのコンプライアンスサービスを提供している割合が最も高く **10%** ですが、小規模な MSP も十分に競争力を保っています。従業員数 5 名以下の MSP では、7 つのサービスのうち 4 ～ 6 つを提供している割合が他のどのグループよりも高く **77%** に達しており、提供しているサービス数の平均も最も多くなっています。

コンプライアンスプログラム全体の管理についても、導入率は比較的一貫しており、**54% ～ 62%** の範囲となっています。これは、コンプライアンスが規模を問わず MSP にとって成長分野になりつつあり、競争の軸がサービス提供の可否から、提供のスピード、対応の深さ、成熟度へと移りつつあることを示しています。

MSP の規模	0 ～ 2 つの サービス	3 つの サービス	4 ～ 6 つの サービス	7 つすべて サービス	平均 サービス数	プログラム全体の管理
従業員 1 ～ 5 人	5%	11%	77%	7%	5	62%
従業員 6 ～ 25 人	8%	25%	65%	2%	4	54%
従業員 26 ～ 50 人	8%	17%	70%	6%	4	59%
従業員数 51 名以上	5%	17%	69%	10%	4	59%

割合は四捨五入されています。

現在および今後において、顧客のサイバーセキュリティのコンプライアンス対応に関する貴社の関与について、最もよく当てはまるものは次のうちどれですか？「わからない」を除く（回答者数=800）

MSP はコンプライアンス対応の体制整備で大きく前進しており、現在ではほぼすべての MSP が少なくとも 1 つのコンプライアンスサービスを提供し、大多数がコンプライアンスのライフサイクル全体にわたって複数のサービスを提供しています。コンプライアンスプログラム全体の管理はすでに一般的になりつつあり、今後ほぼすべての MSP が提供するサービスになる見込みです。これは、継続的なコンプライアンス対応への顧客からのニーズが高まっていることを反映しています。

ただし、提供するサービスの幅広さが、そのまま成熟度を意味するわけではありません。多くの MSP が基本的なアドバイザリーサービスの枠を超えてサービスを拡充している一方で、本当に包括的なコンプライアンスサービスを構築している MSP は比較的少数です。多くの MSP は依然として、サービスが部分的にしかそろっていない体制で運用しています。コンプライアンスプログラム全体を管理している MSP でも、それを支えるコンプライアンスサービスをすべて提供しているのはごく少数です。

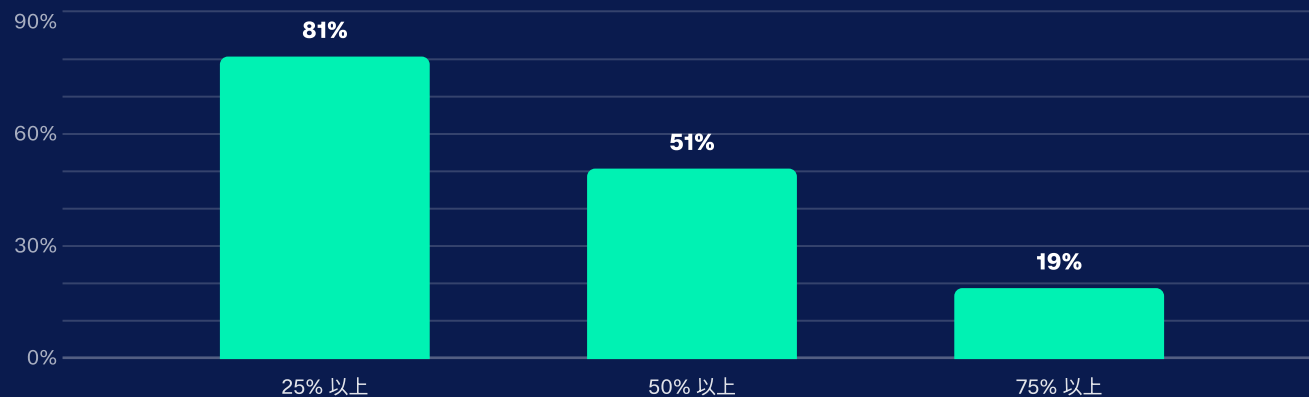
コンプライアンスサービスがより広く提供されるようになるにつれて、競争優位性は、サービスを提供しているかどうかだけでなく、提供のスピード、対応の深さ、品質、そしてシームレスさにますます左右されるようになります。**アドバイザリー、導入、文書化、レポート作成、プログラム管理を一貫したコンプライアンス対応として連携できる MSP は、市場をリードする存在として他社との差別化を図る上で有利な立場にあります。**

2. コンプライアンスがセキュリティ投資を後押し

コンプライアンスは今や、サイバーセキュリティへの投資を促す重要な要因となっています。MSP によると、顧客のサイバーセキュリティ関連の購買決定の平均 **50%** がコンプライアンスの影響を受けており、**33%** の購買決定ではコンプライアンスが「大きい」または「決定的な」影響を及ぼしています。その影響は広範囲に及んでいます。**81% の MSP** が、コンプライアンスが顧客の購買決定の少なくとも **25%** に影響を与えていると回答しており、**51%** の MSP では、その割合が 50% 以上に達しています。つまり、コンプライアンスはもはや単なる報告要件ではなく、顧客のセキュリティ投資の優先順位を左右する要因となっています。

今こそ、その影響をより戦略的に活用する機会です。MSP のうち、コンプライアンスが顧客のサイバーセキュリティ関連の購買決定の大多数 (**75%**) に「大きく」または「決定的に」影響していると回答したのは、わずか **9%** です。これは、MSP にとって、コンプライアンスをきっかけとして、より幅広いアドバイザリー、より高度なサービス、より体系的なセキュリティプログラムへと顧客との対話を広げていく余地があることを示しています。

コンプライアンスに影響を受けた顧客の購入割合



顧客のサイバーセキュリティ関連の購買決定のうち、規制上のコンプライアンス要件によって少なくとも一部が影響を受けている割合はどの程度ですか？影響を受けているものがない場合も含まれます。
(回答者数=800)

50%

コンプライアンス要件によって左右される顧客の購買決定の割合。

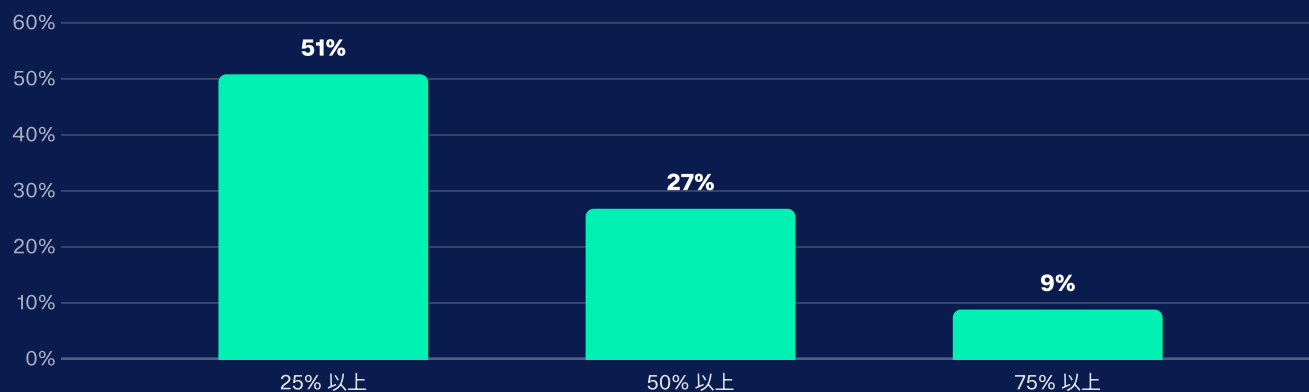
33%

その購買決定のうち、規制上のコンプライアンス要件によって大きな影響を受ける割合。

MSP は、顧客のコンプライアンス対応を戦略的な対話につなげることができます。

これらの調査結果を総合すると、コンプライアンスは規制上の義務から、ビジネスを動かす重要な要因へと変化していることが分かります。すでに顧客のセキュリティ支出に明確な影響を与えています。しかし、コンプライアンスを、より幅広いサイバーセキュリティの提案につなげる収益性の高い機会として活用できている MSP は、まだ少数です。これは、MSP にとって、このギャップを埋め、コンプライアンスを起点とした需要を、より深いアドバイザリー関係や、より付加価値の高い戦略的サービスにつなげる機会となります。

コンプライアンスに「大きく」または「決定的に」影響を受けた顧客の購入割合

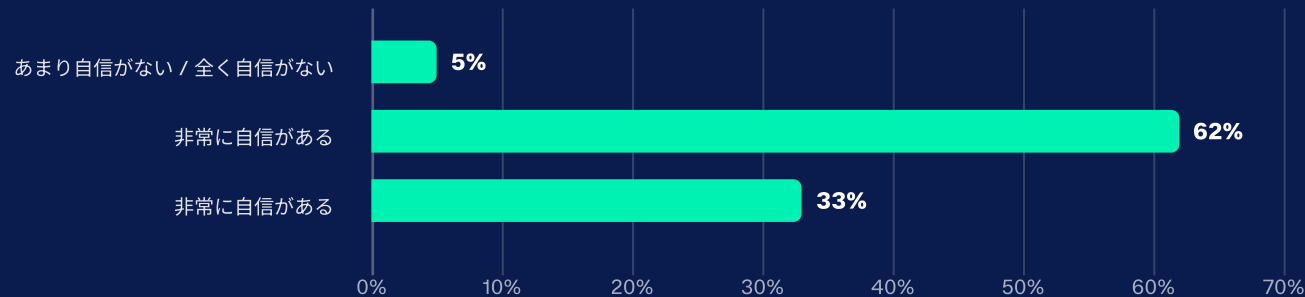


顧客のサイバーセキュリティ関連の購買決定のうち、規制上のコンプライアンス要件によって大きなあるいは決定的な影響を受けている割合はどの程度ですか？ (回答者数=800)

3. 継続的なコンプライアンス対応が徐々に進んでいる

MSP では、コンプライアンス管理を継続的に行うアプローチがますます広がっています。MSP の自信度から、多くのプロバイダーが、コンプライアンス対応が定期的な監査から継続的な監視とガバナンスへと移行する中で、顧客を支援するための十分な体制を整えていると考えていることが伺えます。全体として、**95% の MSP** が、複数の顧客にわたってコンプライアンスを継続的に監視、管理、文書化する能力について「非常に自信がある」または「完全に自信がある」と回答しています。

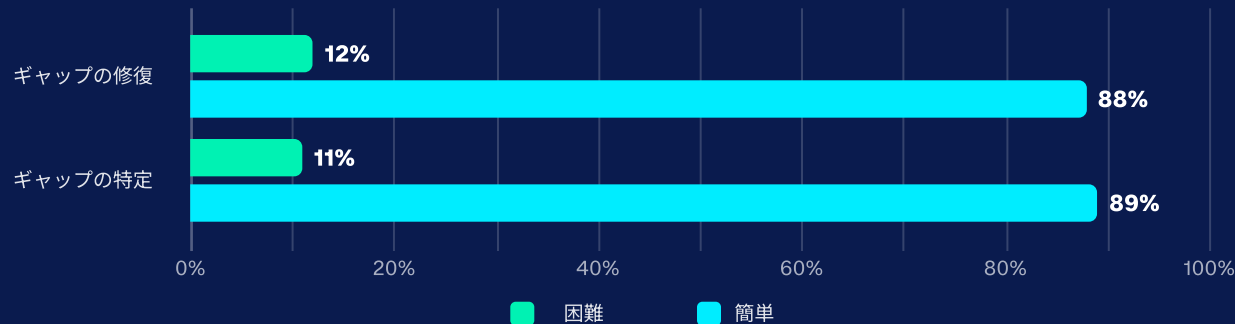
継続的なコンプライアンス管理に対する自信



複数の顧客にわたってコンプライアンス要件を継続的に監視、管理、文書化する現在の自社の能力について、どの程度自信がありますか？ 自信がない場合も含みます。(回答者数=800)

この自信は、顧客のコンプライアンスやセキュリティ制御におけるギャップを特定して是正するための MSP の対応力にも表れており、どちらについても困難を感じていると回答した MSP はごく少数です。

MSP によるコンプライアンスおよび管理ギャップの発見と修復の容易さ



現在、顧客のコンプライアンスやセキュリティ管理策におけるギャップを特定して是正することは、どの程度容易ですか、または困難ですか？ (回答者数=800)

62%

複数の顧客にわたってコンプライアンスを継続的に監視、管理、文書化する能力に「非常に自信がある」と回答した MSP の割合。

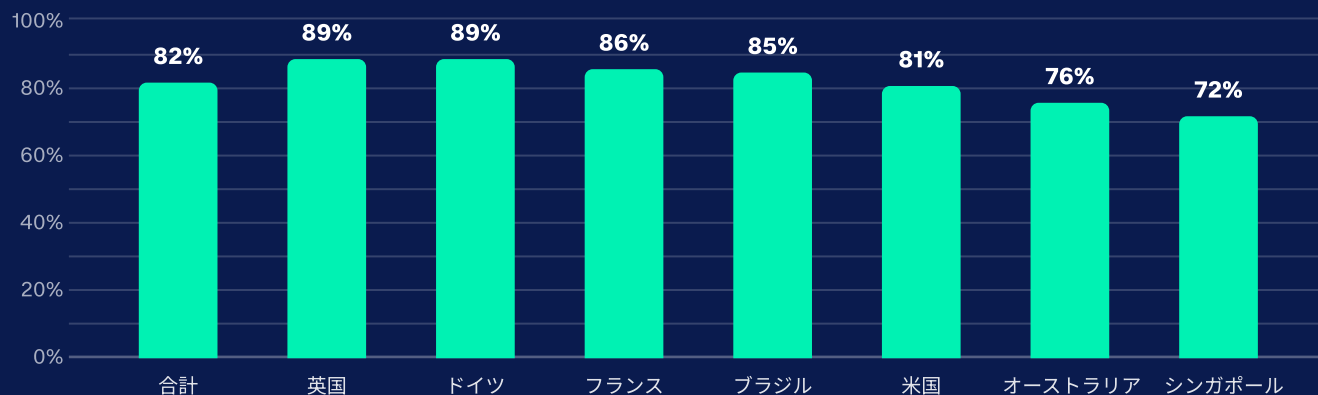
33%

その能力に「完全に自信がある」と回答した MSP の割合。

コンプライアンスと制御のギャップを管理することへの自信は、国によって異なる

コンプライアンスやセキュリティ制御のギャップを管理する能力は、ほとんどの MSP が確立していますが、その自信度には国によって差があります。英国とドイツの MSP は、これらのギャップを容易に特定し修正できると回答する可能性が最も高く (89%)、これに対し米国では 81%、オーストラリアでは 76%、シンガポールでは 72% となっています。こうした違いは、多くのプロバイダーが運用プロセスを整備している一方で、コンプライアンスを維持し、リスクを低減するという実務上の課題は、市場によって大きく異なることを示しています。

コンプライアンスのギャップを特定および是正する容易さは国によって異なる



現在、顧客のコンプライアンスやセキュリティ管理策におけるギャップを特定して是正することは、どの程度容易ですか、または困難ですか？ (回答者数 = 800)

あらゆる規模の MSP が、顧客のコンプライアンスを継続的に管理する能力に自信を持っている

自信度は、MSP の規模を問わず、驚くほど大きな差がありません。小規模なプロバイダーとして最も高い自信を示しており、従業員数 1 ～ 5 人の MSP の **98%** が、継続的なコンプライアンスを管理する能力について「完全に自信がある」または「非常に自信がある」と回答しています。これに対し、従業員数 51 名以上の MSP では **92%** となっています。「完全に自信がある」という回答は、どの規模の MSP でもはるかに低く、**30 ～ 36%** の範囲にとどまっています。「非常に自信がある」と「完全に自信がある」との間に差があることから、MSP 全体で継続的なコンプライアンス対応の体制が整いつつある一方で、多くのプロバイダーには現在の体制を改善する余地があることが分かります。

継続的なコンプライアンス管理に対する自信	合計	1 ～ 5 人の従業員	6 ～ 25 人の従業員	26 ～ 50 人の従業員	51 人以上の従業員
非常に自信がある	33%	36%	34%	30%	31%
非常に自信がある	62%	62%	62%	65%	60%
あまり自信がない	4%	2%	4%	5%	7%
全く自信がない	0%	0%	0%	1%	1%
完全に自信があるまたは非常に自信がある	95%	98%	96%	95%	92%

[※]数の顧客にわたってコンプライアンス要件を継続的に監視、管理、文書化する現在の自社の能力について、どの程度自信がありますか？自信がない場合も含みます。(回答者数 = 800)

サイバーレジリエンスを確保するには、定期的に問題がないことを確認するだけでなく、コンプライアンスを継続的に証明できることが重要です。顧客にとっては、セキュリティ制御が機能し、ギャップが明らかになり、時間の経過とともに改善が進んでいることを示す明確な証拠が必要です。MSP の自信度から、こうした能力が明らかに定着しつつあることが分かります。一方で、「完全に自信がある」とする回答が少ないことは、そこに機会とリスクの両方があることを示しています。このギャップを埋め、安定した、拡張可能で再現性のあるコンプライアンスサービスを提供できるプロバイダーは、より付加価値の高いガバナンスサービスへと事業を拡大する上で有利な立場にあります。一方、こうした対応ができないプロバイダーは、脅威、規制、ビジネスリスクがますます高まる中で、顧客が必要とするレベルの保証を提供することが難しくなる可能性があります。

第3部：セキュリティとコンプライアンスの大規模な運用

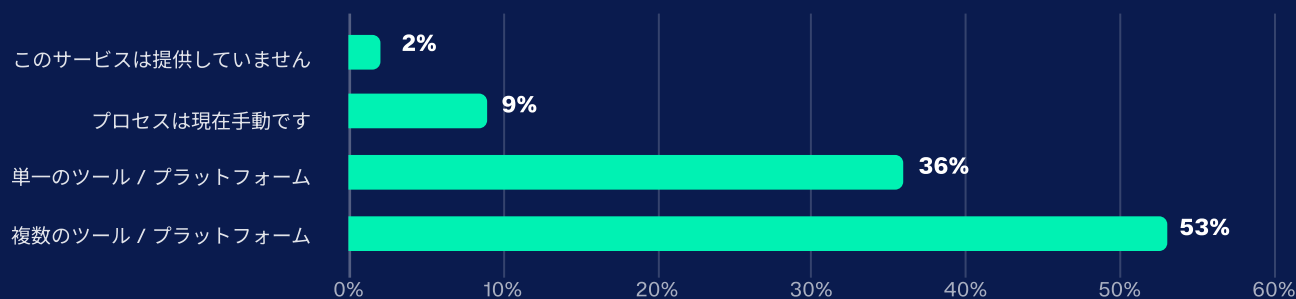
1. ツールを活用したサービス提供が標準に

MSPがサイバーセキュリティのコンプライアンス対応や戦略的なアドバイザリーサービスへとその役割を広げる中、ツールを活用したサービス提供が標準となっています。**89%のMSP**が現在、顧客ベース全体でコンプライアンス対応やCISOとしての活動を一元管理するために、1つ以上のツールやプラットフォームを使用しています。完全に手動のプロセスに依存し続けているMSPはわずか**9%**であり、残りの**2%**はこれらのサービスを全く提供していませんでした。

こうした運用を支援するテクノロジーの導入は進んでいますが、ツールやプラットフォームの集約は十分に進んでいません。単一のソリューション(**36%**)ではなく、複数のツールやプラットフォームを利用しているMSP(**53%**)のほうが多く、単一の統合システムではなく、複数の専門的なプラットフォームを組み合わせるこれらのサービスを提供しているMSPが多いことがうかがえます。

これは、多数の顧客に対してコンプライアンス要件、リスク評価、レポート作成、ガバナンス活動、顧客とのコミュニケーションを管理することが、ますます複雑になっていることを反映している可能性があります。これはまた、共通する課題も浮き彫りにしています。多くのツールではデータを一元的なレポート作成プラットフォームに取り込めないため、複数の業務を手作業で集約し、顧客向けの単一のレポートにまとめる必要があります。この調査結果から、コンプライアンスプログラムの管理とレポート作成を一元化するアプローチへの需要が高まっていることが見えてきます。

コンプライアンス / CISO 活動提供へのプラットフォームアプローチ



現在、顧客全体にわたるサイバーセキュリティのコンプライアンス対応やCISOが担う業務活動を、どのような方法で提供していますか？ (回答者数=800)

53%

サイバーセキュリティのコンプライアンス対応やCISO業務に関する活動を一元管理するために、複数のツールやプラットフォームを使用しているMSPの割合。

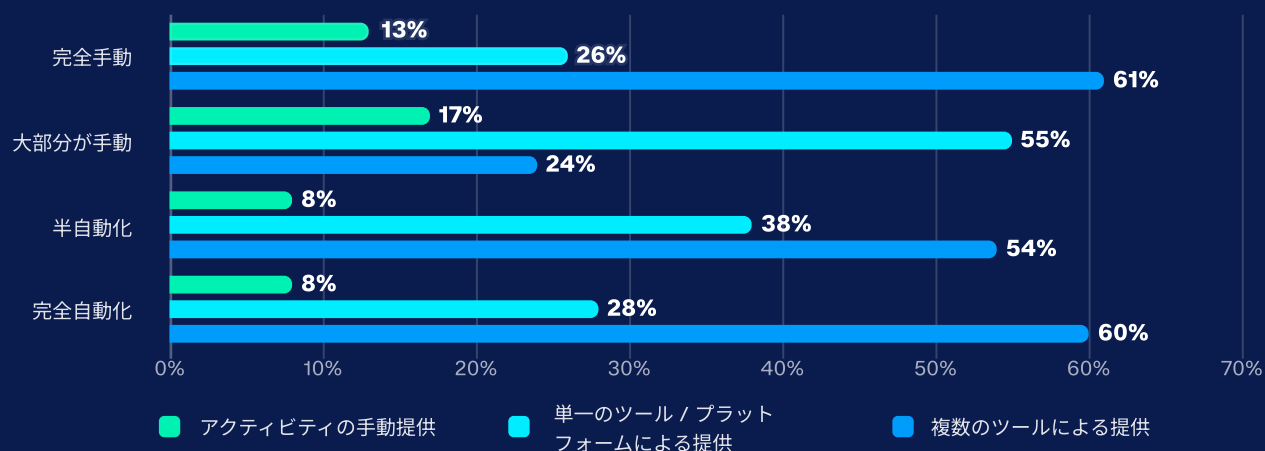
36%

1つのツールまたはプラットフォームのみを利用しているMSPの割合。

2. セキュリティレポートの自動化が進んでいる

多くの MSP が完全な手作業によるレポート作成から移行しており、**86%** が、セキュリティポスチャを総合的に把握するレポートを作成するために、完全または半自動化された方法を利用しています。しかし、完全な自動化はまだ標準化されていません。わずか **31%** の MSP しか、完全に自動化されたプロセスによってレポートを迅速に作成できておらず、**55%** は依然として、データの集約、コンテキストの追加、レポートの仕上げに何らかの手作業を必要としています。

提供アプローチ別のレポート自動化レベル



顧客全体にわたるサイバーセキュリティのコンプライアンス対応や CISO が担う業務活動の提供方法と、サイバーセキュリティの状況、リスク、推奨事項を示す顧客向けのセキュリティポスチャレポートの作成プロセスの自動化レベルはどのくらいですか？ (回答者数 = 800)

これは、プラットフォームを活用する戦略だけで、自動化の成熟度が決まるわけではないことを示しています。自動化のレベルにかかわらず、MSP は複数のツールを使用していますが、これは業務プロセスが分断されているためか、より幅広いツール群にわたって自動化されたワークフローを構築しているためと考えられます。いずれにしても、自動化の必要性は広く認識されており、MSP にとって自動化がもたらす価値も大きなものとなっています。

86%

セキュリティ体制を統合したレポートを作成するために、完全または半自動化されたプロセスを利用している MSP の割合。

31%

自動化をサポートしレポートを迅速に生成できる MSP の割合。

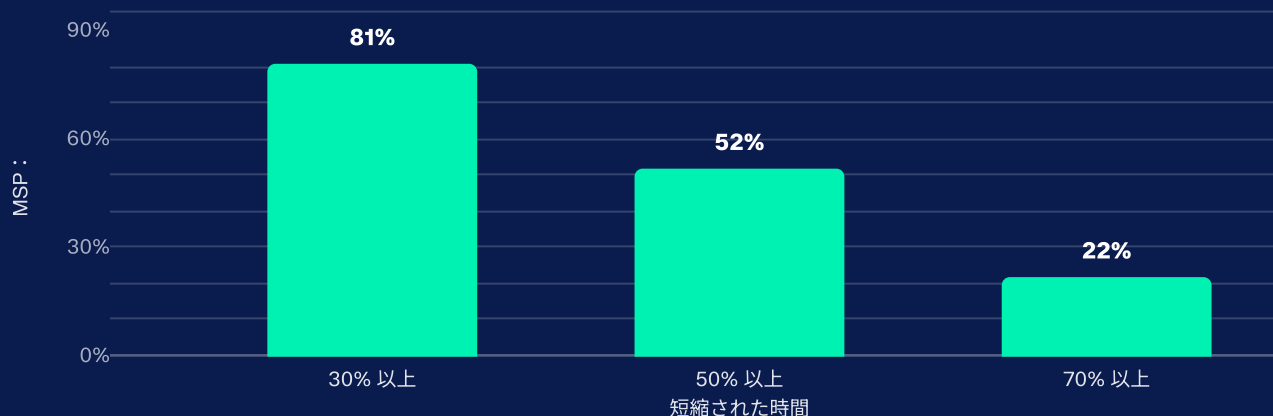
55%

アクティビティを統合するために依然として手作業を必要としている MSP の割合。

3. 大幅な効率化を実現する余地がまだ残されている

プラットフォームの集約により、MSP は大幅な効率化を実現できる可能性があります。MSP は平均して、単一の完全に統合されたプラットフォームを利用することで、顧客のセキュリティポスチャとコンプライアンスの管理とレポート作成にチームが費やす時間を **53%** 削減できると見積もっています。全体では、**81% の MSP が 30% を超える時間削減を見込んでおり**、52% が 50% 超、22% が 70% 超の削減を見込んでいます。

統合プラットフォームによる推定時間短縮効果



顧客のセキュリティポスチャとコンプライアンスの管理やレポート作成を単一の完全に統合されたプラットフォームで行えるようになった場合、チームの作業時間をどの程度削減できると思いますか？ (回答者数=800)

特に、コンプライアンスプログラム全体の管理をすでに提供している MSP は、削減できる時間が大きいことを認識しています。このサービスを提供している **MSP の 84% が、30% を超える時間削減を実現できると回答しているのに対し**、このサービスを提供しておらず、今後提供する予定もない MSP では **64% にとどまっています**。これは、包括的または統合されたコンプライアンス対応を管理している MSP ほど、プラットフォームの集約によって大きなメリットを得られる可能性があることを示しています。

これらの調査結果は、多くの MSP が依然として、複数のプラットフォームやワークフローにわたってレポート作成、コンプライアンス対応、アドバイザリーサービスを管理する際に、大きな業務負担を抱えていることを浮き彫りにしています。コンプライアンス管理や CISO に相当するアドバイザリーなど、より付加価値の高いサービスへの需要が高まる中、サイバーセキュリティプログラムを大規模に管理する方法を再構築することが、ますます重要になっています。

この調査結果から、MSP は、コンプライアンスプログラム全体を一元化して管理することで大きな価値を得られると考えていることが分かります。つまり、チームは情報の集約に費やす時間を減らし、顧客に戦略的な成果をもたらすことに、より多くの時間を費やせるようになります。

53%

顧客のセキュリティポスチャとコンプライアンスの管理やレポート作成を統合された単一のプラットフォームで行えるようになる場合に、MSP が作業時間を削減できる割合。

81%

統合されたアプローチによってチームの時間の 30% 以上を節約できると回答した MSP の割合。

22%

チームの作業時間の 70% 以上を節約できると回答した MSP の割合。

まとめ

MSPを取り巻く環境は、大きく変化しています。顧客は、MSPに対して、テクノロジーの管理に加えて、戦略的なサイバーセキュリティを主導することも、より期待するようになっていきます。このような環境の中でMSPは、コンプライアンス管理、サイバーセキュリティに関するアドバイザリーサービス、その他のCISOに相当する役割へと業務を拡大しています。**調査対象となったMSPの84%が、今後1年間でCISOサービスへの需要が高まると見込んでおり**、こうした高付加価値サービスは、事業の成長と差別化につながる機会としてますます重要になっています。

同時に、セキュリティポスチャ、コンプライアンス、顧客へのレポート作成を大規模に管理することは、依然として運用上の課題として残されています。多くのMSPがプラットフォームや自動化されたプロセスを導入している一方で、こうしたサービスを提供するために、依然として複数のツールや手作業に頼っているMSPも少なくありません。これはある意味で、CISOやセキュリティチームが直面している複雑な状況と似ています。その結果、MSP自身も、顧客が克服しようとしているのと同じ課題に悩まされることになります。

拡張性のあるサイバーセキュリティリーダーシップ、継続的なプログラム管理、測定可能なセキュリティ成果を、安定して効率的に提供できるMSPは、顧客との関係を強化し、売上を拡大するとともに、新たなビジネス機会を最大限に活かす上で有利な立場にあります。

Sophos CISO Advantage

[Sophos CISO Advantage](#) は、これまでとは異なるサイバーセキュリティの対話を MSP が主導する機会をもたらします。成果、ビジネスリスク、継続的なコンプライアンス、そして測定可能な改善に焦点を当てた顧客との対話を実現できます。

ソフォスの AI ネイティブサイバーセキュリティ防衛システムである [Sophos Fusion](#) を通じて提供されるこのサービスは、多くの MSP がすでに担っている CISO の役割を、体系化され、拡張可能で、収益化できるサイバーセキュリティプログラム管理サービスへと転換します。

エージェント型 AI によって評価、レポート作成、ロードマップ策定のワークフローを高速化することで、MSP は、顧客全体にわたって、経営幹部への報告に適した知見、フレームワークとの対応関係を明確にした証跡、優先順位付けされたアクションプランを、再現性のある形で提供できるようになります。

また、既存の顧客との取り組みを起点として、新たな継続収益や成長機会を生み出し、顧客との関係を強化する明確な道筋もつくります。評価を行うたびにセキュリティ上のギャップが明らかになり、そのギャップが改善に向けたロードマップにつながるため、MSP は、その後の対策を提供できる有利な立場を築くことができます。

Sophos CISO Advantage は、セキュリティ業界が長年指摘してきたニーズに応えるものです。MSP はいち早く導入することで、顧客が必要としているサイバーセキュリティリーダーシップの役割を完全に担うことができます。

Sophos CISO Advantage の詳細については、[パートナーポータル](#)をご覧ください。

ソフォスのパートナーとして成功を収めましょう。[ご登録はこちらから。](#)

ソフォス株式会社営業部

Email: sales@sophos.co.jp

© Copyright 2026.Sophos Ltd.All rights reserved.

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK.
Sophos は、Sophos Ltd. の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。
2026-09-14 JA (TA) CRE-6170

