

シスコ サイバーセキュリティ レポート シリーズ 2020
CISO ベンチマーク調査

サイバーセキュリティの 現在、今後

2020 年—考慮すべき 20 の事項



目次

はじめに	3
2020 年のサイバーセキュリティに関する 20 の考慮事項	4
1. お客様の組織の重点ポイントを明確にし、エグゼクティブをサポート している人は誰ですか？	4
2. 最も重要な基準を判断するにはどうすればよいでしょうか？	5
3. 限られた予算を最適に利用するための主な考慮事項は何でしょうか？	6
4. 信頼性の検証と脅威の検出にどのようにコストを配分するのが最適 ですか？	8
5. セキュリティ侵害によるビジネスへの影響を測定することで何 がわかりますか？	9
6. 侵害を自発的に公表する組織の割合が一貫して高いのはなぜでしょ うか？	11
7. ネットワークチームとセキュリティチームのコラボレーションによる メリットを定量化できますか？	11
8. アウトソーシングする要因は、コスト削減以外に何がありますか？	11
9. 準備することで効果はありますか？	13
10. 侵害防御におけるパッチ適用はどの程度重要ですか？	13
11. ダウンタイムの原因は何ですか？	14
12. モバイルワーカーを保護するにはどのような課題がありますか？	14
13. アプリケーションの保護にまでゼロトラストを拡張するにはどうす ればよいですか？	14
14. ネットワーク インフラストラクチャの防御は依然として困難で すか？	16
15. ベンダー統合の影響を評価できますか？	17
16. サイバーセキュリティ対応に疲弊してしまう原因は何ですか？	18
17. クラウドでインフラストラクチャをホスティングすることで セキュリティ上どんなメリットがありますか？	19
18. 将来どのような課題に直面すると考えていますか？	20
19. インシデント対応にどの程度重点を置くべきでしょうか？	21
20. セキュリティポスチャを改善するために、今何ができるでしょ うか？	22
現在も今後もセキュアに	23
シスコ サイバーセキュリティ レポート シリーズ概要	24

はじめに

企業のセキュリティリーダーは、ビジネスの拡大とデジタル トランスフォーメーションをサポートしながら、多くの課題にも対処する必要があります。シスコは、お客様との日々の会話や年次ベンチマーク調査からお客様の状況を把握してきました。課題のいくつかはセキュリティに関するもので、優れた可視性の確保や自動化、セキュリティに関する管理や対応のシンプル化などがあります。また、ビジネスの成功に関連する課題には、必要なクラウドアプリケーションや使用されているモバイルデバイスにかかわらず、ビジネスの拡大やトランスフォーメーションを促進することなどがあります。その他の課題は、将来組織が変化しても対応できるように今から投資を行うことに関連しています。

これらすべての課題に加えて、高度な脅威を検出してブロックするといった日常業務もあります。高度なセキュリティ犯罪者と、拡大し続ける攻撃対象領域に同時に対応することは困難です。お客様は、限られた予算でさらに多くのことを実施する以外にもさまざまな課題に直面しています。たとえば、ブランドの評価および取締役会や株主の信頼を維持する、サイバー攻撃の戦術、手法、手順（TTP）に対応できる専門家を採用する、といったことがあります。

セキュリティに関するこのような要件、複雑さ、予算の制約に対応しながら、ユーザが求めるアクセス手段を提供する必要があります。また、テクノロジーのオーバーヘッドを削減する、大規模な侵害を回避する、ネットワークに侵入されてデータが窃取される前に脅威を検出する、セキュリティ予算を効率的に利用する、より多くの顧客を獲得するといった課題もあります。

世界経済フォーラムによると、サイバー攻撃は、先進国のビジネスリーダーの懸念事項において、財政危機に次ぐ 2 番目に大きなテーマとして認識されています。¹

シスコは、13 カ国 2,800 人の IT に関する意思決定者に対して 6 回目の年次調査を実施し、例年どおりお客様の状況を詳細に調査して、重要なベンチマークに関する統計情報をまとめました。² また、2020 年における 20 件の考慮事項リストを作成し、CISO の皆様に対して調査結果の分析内容を詳細に説明しました。このレポートは、最高責任者や取締役会のメンバーに価値ある分析結果やデータを説明し、組織のセキュリティポスチャを改善するための具体的な提案をする際に役立ちます。

セキュリティ業界で唯一確かなのは、「すべて不確実だ」ということです。そのためレポートの各セクションは断定を避け、今後の準備に向けて重要なポイントを問いかける形式を取っています。これらの問いかけに共感いただけた場合や、別の分野に関してご質問がある場合は、ぜひ security-reports@cisco.external.com までご意見をお寄せください。今年のセキュリティ課題に対応する上で、レポートがよい指針になることを願っております。

サイバーセキュリティ レポート シリーズのすべてのレポートをご覧になるには、cisco.com/jp/go/securityreports にアクセスしてください。

¹ 「[This is what CEOs around the world see as the biggest risks to business](#)（世界中の CEO がビジネスにとっての最大のリスクと捉えていること）」、2019 年世界経済フォーラム

² 調査対象国：オーストラリア、ブラジル、カナダ、中国、フランス、ドイツ、インド、イタリア、日本、メキシコ、スペイン、英国、米国

2020 年のサイバーセキュリティに関する 20 の考慮事項

1. お客様の組織の重点ポイントを明確にし、エグゼクティブをサポートしている人は誰ですか？

シスコでは、エグゼクティブとセキュリティ部門の関係を良好に保つための 4 つの重要な対策について継続的に調査してきました。こうした調査では、トップダウンでのセキュリティソリューションの導入について評価しています。この項目に関しては、昨年からわずかに減少傾向にあり、以下のような結果となっています。

- ・ 回答者の 89% は、「**エグゼクティブリーダーは依然としてセキュリティを最優先事項と考えている**」と回答していますが、この割合は過去 4 年間でわずかに (7%) 減少しています。
- ・ **エグゼクティブチームにおけるセキュリティ担当者と責任が明確になっている組織**の割合は、ここ数年で変動しています。今年は 89% でした。サイバーセキュリティに対する認識が高まり、トップレベルのセキュリティリーダーが切実に求められていることを考慮すると、担当者と責任を明確にすることは変わらず重要です。
- ・ サイバーリスク評価を全体的なリスク評価プロセスに組み込んでいた回答者の割合は、昨年から 5% 減少していますが、依然として 91% という高い値を維持しています。
- ・ エグゼクティブチームが、セキュリティプログラムの有効性を評価するための明確な基準を確立していると回答した人の割合は昨年から 6% 減少していますが、今年も 90% と高い値を示しています。

過去 4 年間で上記の回答はわずかに減少しています。このことから、1) セキュリティの責任範囲が変化している、2) エグゼクティブチームとのコミュニケーションが以前ほど明確に行われていない、3) エグゼクティブ管理者にその他のビジネス上の優先事項がある、4) CISO とエグゼクティブが基準を再評価している、のいずれかである可能性があります。

また、これらの数値は低下していますが、非常に高い値を維持していることも事実です。それは、セキュリティが業務として定着していても、エグゼクティブの大きなテーマであることに変わりはないからだと思われます。さらに、これらの数値の高さは、エグゼクティブとセキュリティ プロフェッショナルの間で強い関係が維持されていることも示しています。

エグゼクティブの特徴は組織ごとに異なります。エグゼクティブのリーダーシップにも、さまざまなスタイルがあります。CISO の目的は、適切に設計されたセキュリティがビジネスに有益であることを実証することで、セキュリティ強化を呼びかけていくことです。

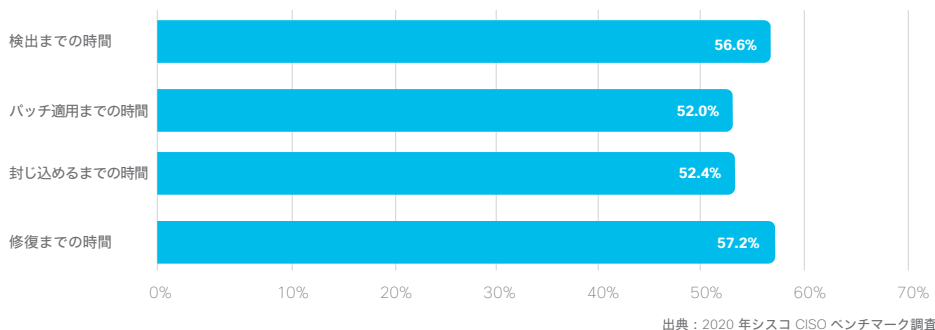
ブルネル大学ロンドン CISO Mick Jenkins 氏 (MBE)

2. 最も重要な基準を判断するにはどうすればよいのでしょうか？

前述のように、組織のエグゼクティブが自社のセキュリティプログラムの有効性を評価する明確な基準を確立している、と回答した人の割合は 90% に達しています。明確な基準を確立することは、セキュリティフレームワークにとって不可欠なアクティビティですが、運用の改善状況やセキュリティの成果を評価する基準を、複数のエグゼクティブやセキュリティチーム全体で同意することは簡単な作業ではありません。

今回の調査において、IT に関する意思決定者は、**重要業績評価指標 (KPI)** として**検出時間を最も重視すると回答しています**。一方、**C スイート (最高責任者) や取締役会に報告する場合は、修復までの時間を重視しています**。修復までの時間には、システムのダウンタイム、影響を受けたレコード数、調査コスト、収益喪失額、顧客喪失数、販売機会喪失額、自己負担コストなどの影響がすべて集約されているからです。また、この指標は、IT 組織の全体的な有効性を表す基準にもなり得ます。修復するには、部門全体で多くの共同作業が必要となる場合があるからです。

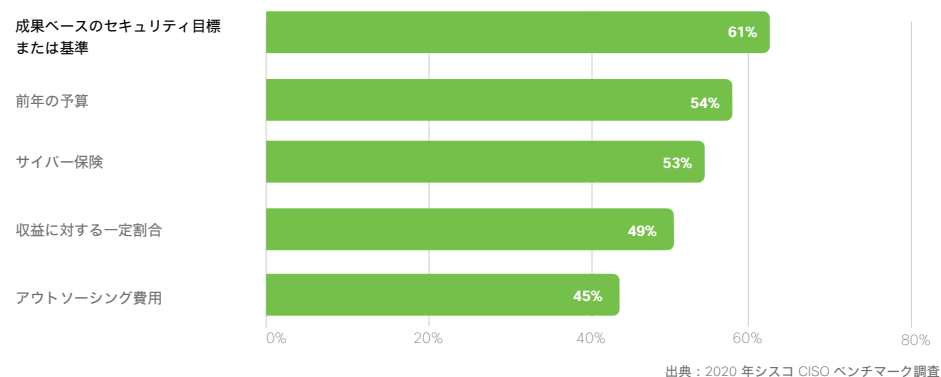
図 1： 影響の大きな侵害を内部の C スイートまたは取締役会に報告する際に使用する基準 (N=2800)



3. 限られた予算を最適に利用するための主な考慮事項は何でしょうか？

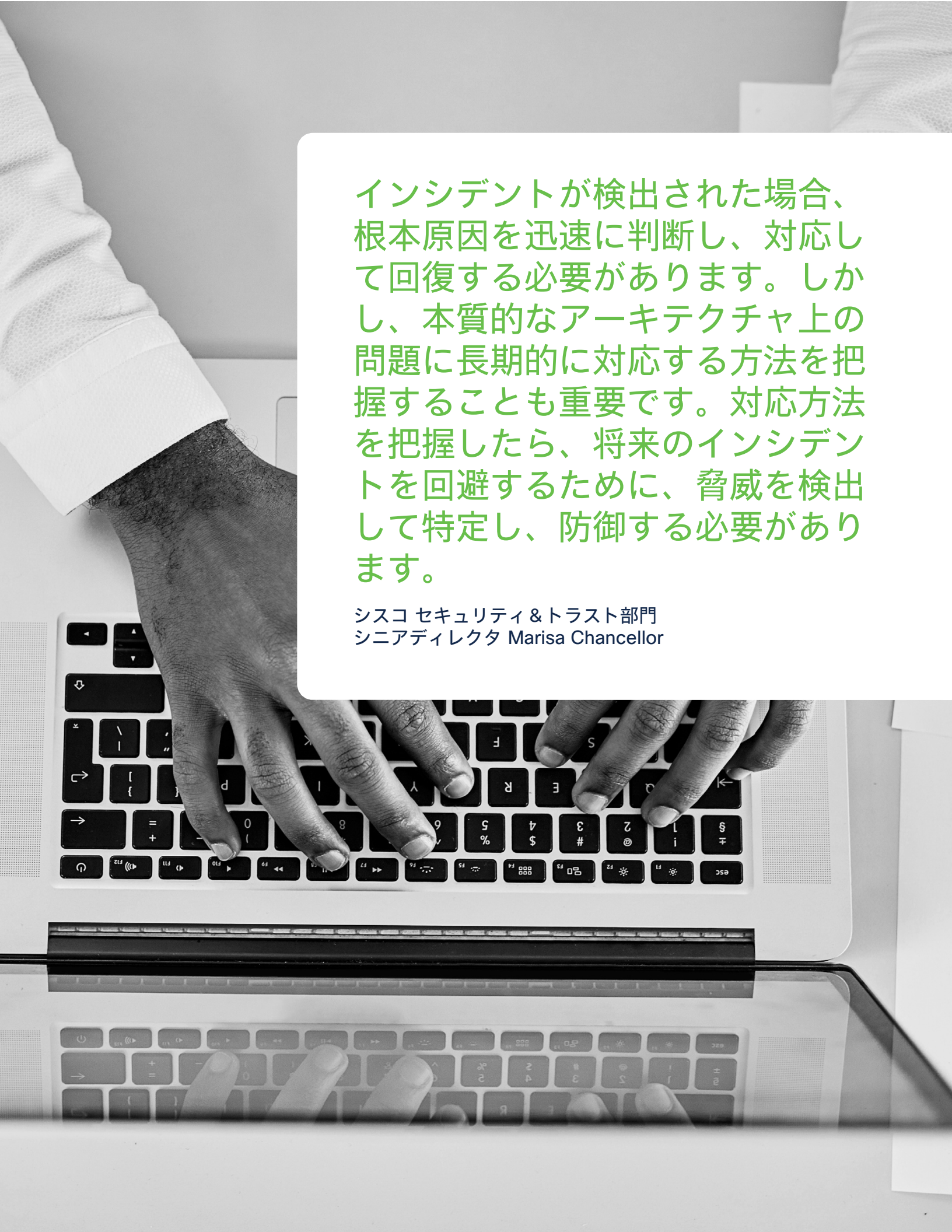
一般的にセキュリティ支出を最適に配分する方法は、成果ベースの目標と基準に応じ
て行うことだと言われています。回答者の 61% がこの計画方式を採用しています。
この割合は増加傾向にあり、前年比 10% 増加しています（図 2）。

図 2： 組織がセキュリティ支出を決定/管理する際に利用している基準（N=2799）。パーセン
テージは四捨五入されています。



「収益に対する一定割合」と「アウトソーシング費用」がセキュリティ予算を決定する要因と回答した人の割合は最も低く、前年の予算を基準とすると回答した人の割合は 54% でした。前年の予算を基準とする方式では、セキュリティコストを正確に定量化できるとは言えないかもしれませんが（特に世界でのデータ漏洩の平均コスト（392 万ドル）がほとんど考慮されていない場合）、予算が前年から変わっていない場合や、コストを予測可能な SaaS サブスクリプションを使用している場合は、セキュリティコストの算定額はおそらくほぼ同じ金額になるでしょう。³

³ [2019 年の侵害によるコストに関するレポート](#)、Ponemon Institute

A black and white photograph of a person's hand typing on a laptop keyboard. The hand is positioned on the left side of the keyboard, with fingers pressing down on the keys. The laptop is open, and the keyboard is visible. The background is a plain, light-colored surface.

インシデントが検出された場合、根本原因を迅速に判断し、対応して回復する必要があります。しかし、本質的なアーキテクチャ上の問題に長期的に対応する方法を把握することも重要です。対応方法を把握したら、将来のインシデントを回避するために、脅威を検出して特定し、防御する必要があります。

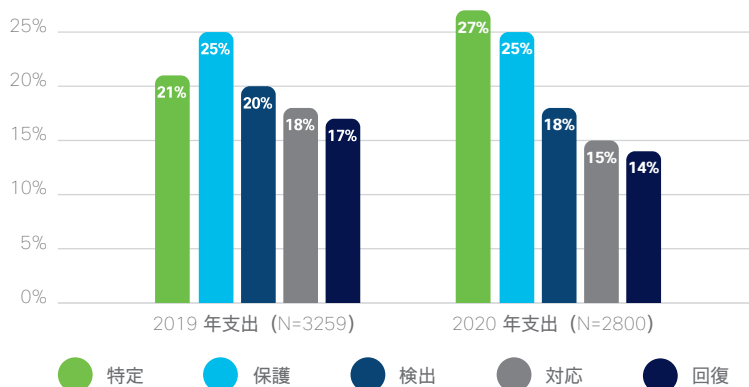
シスコ セキュリティ&トラスト部門
シニアディレクタ Marisa Chancellor

4. 信頼性の検証と脅威の検出にどのようにコストを配分するのが最適ですか？

セキュリティ予算の利用方法に関して、サイバーセキュリティの防御および侵害管理ライフサイクルにおける 5 つのカテゴリ（特定、保護、検出、対応、回復）に分けて調査しました。

- ・ **特定カテゴリ**では、2019 年から 2020 にかけて支出が 21% から 27% に増加しました。
- ・ **保護および検出カテゴリ**は、それぞれ 25% と 18% で基本的に変わりませんでした。
- ・ **対応および回復カテゴリ**の支出は、同じ期間でそれぞれ 15% と 14% に若干減少しました。

図 3： ライフサイクルカテゴリ別のセキュリティ支出。パーセンテージは四捨五入されています。



出典：2020 年シスコ CISO ベンチマーク調査

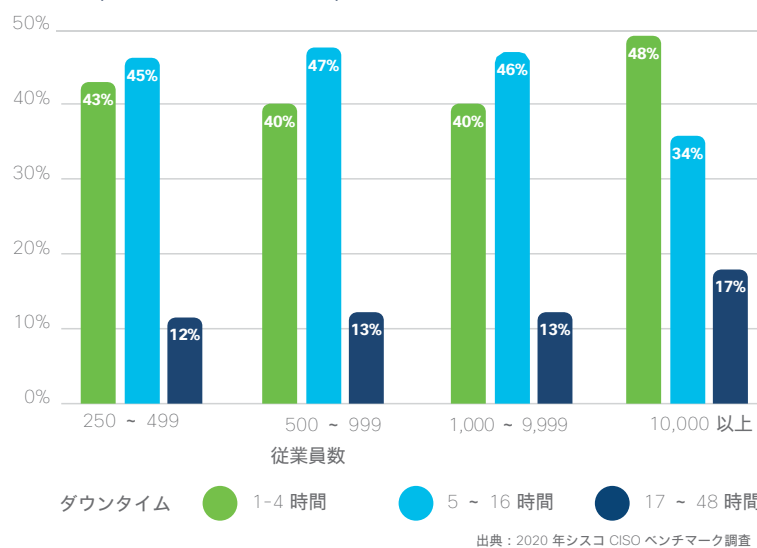
この傾向から、サイバーセキュリティ対応方針において、**組織が事後的な対応よりも予防により多く支出していることがわかります**。企業は、プロアクティブな対応への支出と、対応力と復元力の強化への支出に関して最適なバランスを見つけようと常に模索しており、毎年振り子のように揺れ動いています。昨年組織は、基本的な取り組み（資産の棚卸し、検出など）に注力していたと思われます。理論的には、事前の特定、保護、検出に適切に支出すれば、対応や回復作業が必要な機会が少なくなるため、支出も減少するはずです。

5. セキュリティ侵害によるビジネスへの影響を測定することで何がわかりますか？

今回の調査では、ダウンタイム、レコード数、財務コストなど、侵害によるさまざまな影響について尋ねました。

大規模な侵害によるダウンタイムの影響度合いについて調査し、さまざまな規模の組織を比較したところ、結果はすべての規模でほとんど同じでした。大規模企業（従業員 1 万人以上）は、対応や回復作業を担当するリソースが豊富な場合が多いため、ダウンタイムが短い（0 ～ 4 時間）傾向にあります。小規模から中規模の組織では、回復に 5 ～ 16 時間かかっている割合が高く、17 ～ 48 時間の壊滅的なダウンタイムは、すべての規模の組織で一様に低い割合でした（図 4）。

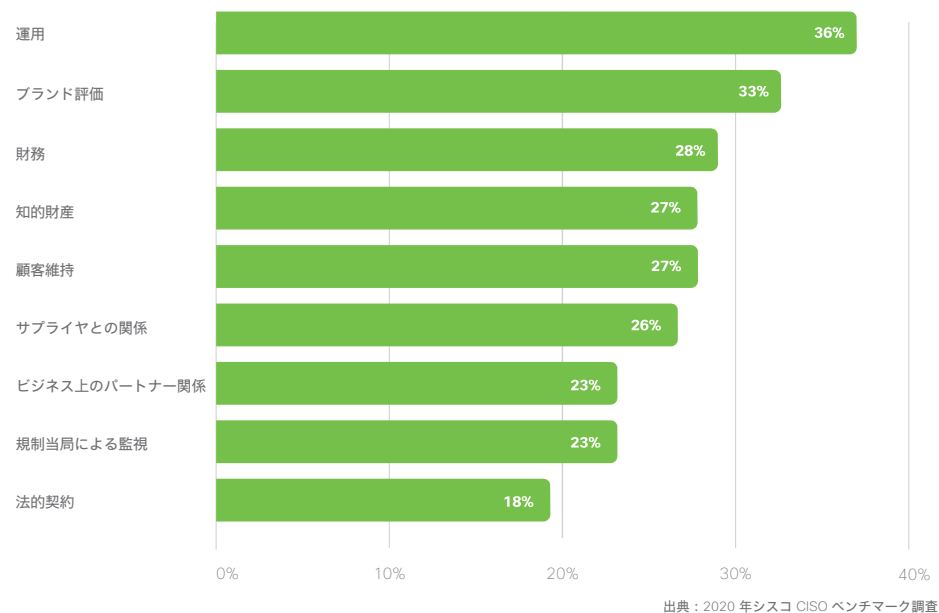
図 4： 過去 1 年間に対応された最も深刻なセキュリティ侵害によるシステムのダウンタイム（組織の規模別。N=2265）。パーセンテージは四捨五入されています。



最も深刻なデータ侵害によって 10 万件を超えるレコードが影響を受けたことのある組織は、昨年の 15% から今年は 19% を超えるまでに増大しています。

さらに図 5 に示すように、重大な侵害によって、1 つの組織で 9 つの重要な分野に影響が及ぶ可能性があります。**最も影響を受けたビジネス分野は、運用とブランド評価で、次に財務、知的財産、顧客維持が続きます。**

図 5： 侵害によってマイナスの影響を受けたビジネス分野の割合（N=2121）。パーセンテージは四捨五入されています。



過去の状況を調べてみると、大規模な侵害によってブランド評価に影響を受けたことがあると回答している人の割合は、3 年間で 26% から 33% に増加しています。運用に影響があった割合は、36 ~ 38% の間で変わっていません。また、財務に影響があった割合は過去 3 年間で年間 1 ポイントの減少にとどまっているため、こちらも比較的变化が少ないと言えます。ブランド全体への影響度が高まる中、インシデント対応の全体計画に危機時のコミュニケーション計画を含めることが重要です。

6. 侵害を自発的に公表する組織の割合が一貫して高いのはなぜでしょうか？

昨年自発的に侵害を公表したと回答した人の割合は 61% で、過去 4 年間で最も高くなっています。この結果から、おそらく新たな法律が制定された結果、または社会的意識の高まりや顧客の信頼を維持したいという思いから、全体としては、組織が積極的に侵害を報告しようとしていることがわかります。

このことの良い面は、侵害が 17 時間以上続いた経験のある組織において、侵害を自発的に公表した組織の数が、報告要件などの他からの要請によって侵害を公表した組織の 2 倍以上になっていることです。

侵害を受けたすべての組織の半数以上 (51%) が、防御を重視するようになり、侵害に伴う世間の監視に対応しようとしています。しかし、政府が定めた報告義務が拡大している一方で、自発的に公表していない組織の割合はほぼ変わらず、侵害を受けた組織の 4 分の 1 を若干上回っている程度です (27%)。また、回答者の 61% が、重大な侵害を自発的に公表することで信頼性が増し、ブランド評価が維持されることに気づいています。

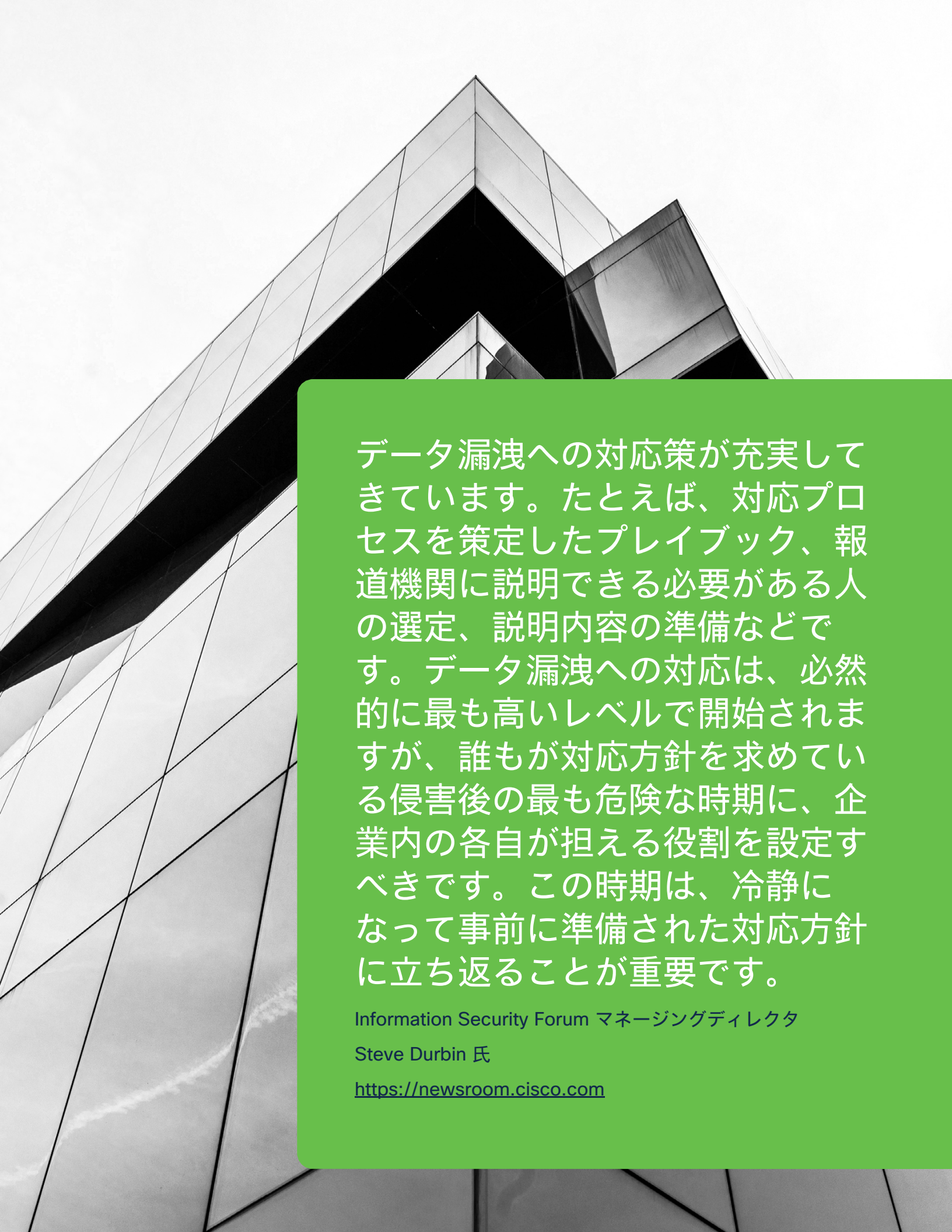
7. ネットワークチームとセキュリティチームのコラボレーションによるメリットを定量化できますか？

ネットワークチームとセキュリティチームでコラボレーションしている割合は依然として高く、今年の調査では、「かなり」または「非常に」協力的であると回答している人の割合が 91% を超えています。エンドポイント担当チームとセキュリティチーム間のコラボレーションも 87% と高いままです。これらの分野ではいくつかの指標が下がっていますが、全体的な傾向としては、単独の組織だけで対応している割合が少なくなっています。

8. アウトソーシングする要因は、コスト削減以外に何がありますか？

昨年のレポートと比較するとアウトソーシングが大幅に増加しています。社内で管理するにはあまりにもベンダーの状況が複雑になっていることで、この傾向が長く続いている可能性があります。しかし興味深いことに、組織は、アウトソーシングの割合が今後減少すると想定しています。

今回の調査の回答者は、コスト以外のさまざまな理由からアウトソーシングしています。コスト効率を理由として挙げる割合は 55% で、わずかな差で第 1 位ですが、「セキュリティチームがインシデントにタイムリーに対応できるようにするため」が、53% ですぐに続いています。



データ漏洩への対応策が充実してきています。たとえば、対応プロセスを策定したプレイブック、報道機関に説明できる必要がある人の選定、説明内容の準備などです。データ漏洩への対応は、必然的に最も高いレベルで開始されますが、誰もが対応方針を求めている侵害後の最も危険な時期に、企業内の各自が担える役割を設定すべきです。この時期は、冷静になって事前に準備された対応方針に立ち返ることが重要です。

Information Security Forum マネージングディレクタ

Steve Durbin 氏

<https://newsroom.cisco.com>

9. 準備することで効果はありますか？

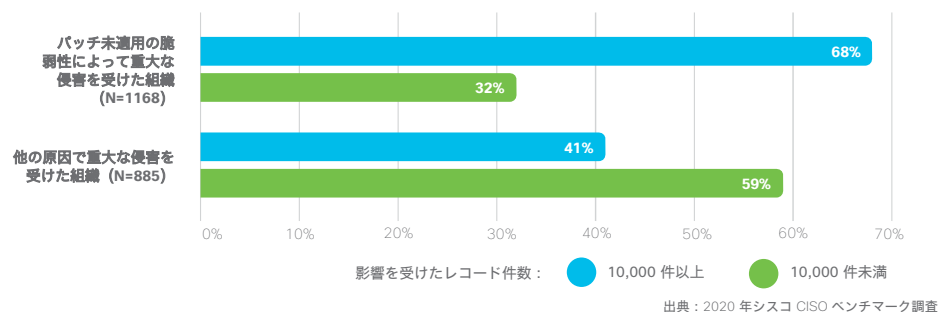
組織に適用されているセキュリティ対策またはポリシーについて尋ねたところ、以下の項目を実践している組織が、大規模な侵害によるコストを削減できている割合が高いことがわかりました。つまり、セキュリティプログラムに次の 6 つの対策を含めることで、侵害によるコストが 10 万ドル未満に収まる可能性が高くなるということです。

- ・ セキュリティ対策を継続して定期的に確認し、正式な対策として戦略的に改善している
- ・ ネットワークに対する接続状況を定期的にチェックし、セキュリティ対策が意図したとおりに機能していることを確認している
- ・ セキュリティを組織の目標と事業の遂行能力に適切に組み込んでいる
- ・ セキュリティインシデントを日常的かつ体系的に調査している
- ・ セキュリティテクノロジーが高度に統合され、連携して効果的に機能している
- ・ 脅威を検出してブロックする機能が最新に保たれている

10. 侵害防御におけるパッチ適用はどの程度重要ですか？

2020 年の重要な懸念事項は、組織の 46%（昨年のレポートの 30% から増加）で、脆弱性にパッチを適用していないためにインシデントが発生していることです。さらに、脆弱性にパッチを適用していないことで昨年重大な侵害を受けた組織は、より深刻なデータ漏洩を経験しています（図 6）。たとえば、パッチ未適用の脆弱性によって侵害された組織の 68% で、昨年 1 万件以上のデータレコードが漏洩しています。他の原因によって侵害を受けたと回答した組織の内、同じ期間に 1 万件以上のレコードが漏洩した組織は 41% のみでした。

図 6： 昨年経験したセキュリティインシデントがパッチ未適用の脆弱性に起因するものかその他の原因によるものか、およびその際のデータ漏洩レコード件数に関する調査（N=2053）。パーセンテージは四捨五入されています。



パッチ適用は困難であり、システムの中断を招く可能性があることはよく知られています。ただしこれらの結果から、リリースされた最新のパッチに関して最低限のベースラインポリシーを導入することで、明確な投資対効果があることがわかります。組織は、パッチを適用しないことによるリスクを分析し、自社環境内の全デバイスのインベントリを最新に維持する必要があります。また、変更管理プロセスを策定し、バージョン管理と文書化を実施することも重要です。

11. ダウンタイムの原因は何ですか？

前述のように、今回の調査では、ダウンタイムの範囲に関して回答を得ています。ダウンタイムの最も一般的な原因を尋ねると、マルウェアと悪意のあるスパムが第1位と第2位に挙げられています。興味深いことに、3番目の原因は、ダウンタイムの長さによって異なっています。ダウンタイムが0～4時間の場合は、フィッシングが最も一般的な原因の3番目です。5～24時間の場合はスパイウェアで、24時間を超える場合は、[ランサムウェア](#)となっています。

重要なポイントは、ランサムウェアの場合、ダウンタイムに関しては組織の規模は関係なく、中小規模企業の組織でも大規模企業の組織でも、最も深刻な脅威だったということです。ダウンタイムが長期化する原因は、被害の評価、バックアップの復元、侵入ベクトルの修正に必要な調査の詳細度に関係している場合があります。

さまざまなタイプの攻撃への対応方法の詳細については、シスコの [Talos 脅威インテリジェンスのブログ](#) をご覧ください。

12. モバイルワーカーを保護するにはどのような課題がありますか？

調査の回答者に、インフラストラクチャのさまざまな側面を保護することがどの程度困難であるかを説明してもらいました。半数以上（52%）が、**防御においてモバイルデバイスが「かなり」または「非常に」課題になっていると回答しています**。昨年の最大の課題はユーザの振る舞いでしたが、今年はモバイルデバイスが上回りました。

[ゼロトラストフレームワーク](#)を使用すると、自社のインフラストラクチャにアクセスしようとしているすべてのユーザとデバイスを特定して確認できます。ゼロトラストは、アーキテクチャ全体にわたって効果的なセキュリティを実現できる、将来を見据えた実用的なフレームワークとして、ワークフォース、ワークロード、ワークプレイスすべてをカバーします。

ゼロトラストフレームワークによって、特に次の3つの成功基準が達成されます。

- ・ ユーザは既知で認証されている
- ・ デバイスはチェックされ、適切であることが確認されている
- ・ ユーザが環境内でアクセスできる場所が限定されている

ゼロトラストフレームワークを導入することで推定での作業は不要になり、モバイルデバイスを含むすべての潜在的な脅威からインフラストラクチャが確実に保護されます。

13. アプリケーションの保護にまでゼロトラストを拡張するにはどうすればよいですか？

ワークロードセキュリティとは、ネットワーク全体のすべてのユーザ接続とデバイス接続を保護することです。ゼロトラストフレームワークを利用すれば、データベースとアプリケーションの内部での依存関係および周辺機能との依存関係を特定し、マイクロセグメンテーションを適用して水平移動（内部での感染拡大）を封じ込めることができます。

調査対象組織の41%が、データセンターの防御は「かなり」または「非常に」困難であると回答し、39%が、アプリケーションの保護に非常に苦慮していると答えています。保護するのが最も難しいのは、パブリッククラウドに保存されているデータであり、52%が「かなり」または「非常に」困難であると回答しています。

ゼロトラストフレームワークにより、ネットワーク全体でポリシーを特定して適用することで、何が実行されていて、何が重要なかを可視化できます。また、継続的にモニタリングして侵害の兆候に対応することで、ポリシー違反が発生した場合にもアラートが表示されます。



脅威インテリジェンスにより、ビジネスが実際に直面している現実の脅威を理解することで、ビジネスに及ぶ可能性のある影響を把握できます。事実に基づいたインテリジェンスを利用して、このような現実のリスクに優先順位を設定することで、ビジネスオーナーは、直面する現実の問題に限られた資本を割り当てることができます。

Talos エンジニアリング担当 VP Matt Watchinski

14. ネットワーク インフラストラクチャの防御は依然として困難ですか？

プライベート クラウド インフラストラクチャは、組織にとって最も重要なセキュリティ課題です（組織の 50% が、防御が「かなり」または「非常に」困難であると回答しています）。ネットワーク インフラストラクチャに関しては、組織の 41% が同様の回答をしています。

ゼロトラストフレームワークが価値を発揮するのはこのような場合です。ゼロトラストフレームワークには、アプリケーション内およびマルチクラウド環境全体のすべての接続に対するソフトウェア定義型アクセス制御機能が含まれています。アクセス制御は、場所ではなく、ユーザ、デバイス、およびアプリケーションのコンテキストに基づいて行われます。このモデルにより、ディストリビューションや場所に関係なく、インフラストラクチャ全体のリスクを検出して対応し、軽減できます。次に示すのは、ゼロトラストセキュリティの成熟度を示すために定義されたフレームワークの各ステージです。

ゼロトラストセキュリティ成熟度モデルの開発

シスコでは、お客様が組織にゼロトラストフレームワークを導入するための構造として、5 つの段階的ステップを採用しています。

ステージ 1：お客様のビジネスニーズに沿った明確なアイデンティティおよびアクセス管理（IAM）戦略が策定され、リスクベースのポリシーでサポートされる多要素認証（MFA）統合ソリューションが導入されている。

ステージ 2：管理対象デバイスと管理対象外デバイスを区別した最新の資産インベントリを作成し、IT とセキュリティの統合機能の一部として、デバイスの状態をチェックしている。

ステージ 3：管理されたプロセス内で、評価済み脆弱性に関してデバイスを更新するようにユーザに指示し、ポリシーに違反しているデバイスをレポートする、信頼できるデバイスポリシーを設定している。

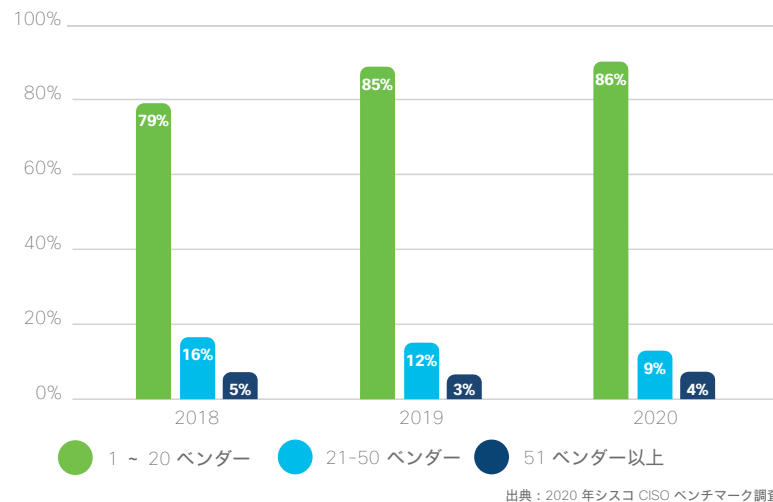
ステージ 4：例外を特定し、例外を考慮して機能する、一元管理されたポリシーに基づいてユーザアクセスを制御している。

ステージ 5：ユーザがオンプレミスとクラウドの両方のアプリケーションにシームレスにアクセスできるアーキテクチャと一連のプロセスを備えた、ビジネスに即したゼロトラスト戦略を構築している。

15. ベンダー統合の影響を評価できますか？

ベンダーを統合することでシンプルにしようとする傾向は続いており、**使用しているベンダー数が1～20社の組織の割合は86%で安定しています**。一方、**20社を超えるベンダーを使用している組織はわずか13%でした**（図7）。

図7： 回答者のセキュリティ環境内で使用されているセキュリティベンダー（ブランド、メーカー）の数（N=2800）。パーセンテージは四捨五入されています。



2017 年以降、マルチベンダー戦略への対応に関して認識が変化しています。**28% がマルチベンダー環境の管理は「非常に困難」だと感じていて、2017 年以来 8% 増加しています**。また、**53% が「やや困難」と回答しています**。一方、マルチベンダー環境の管理が容易だと感じている組織は減少しています（26% から 17% に減少）。ほとんどの組織は、「マルチベンダー環境の管理は困難」というカテゴリに分類されています（81%）。その結果、管理すべきベンダー数を減らしたか、複数の異なるツールから送信されるアラートを統合するために、分析エンジンなどのツールを使い始めたと思われます。

また、マルチベンダー環境におけるアラート数と、それによってサイバーセキュリティ対策に疲弊する度合いの関係についても傾向を調査しました（次のトピックでさらに詳しく調べています）。**回答者の 42% は、サイバーセキュリティ対応に疲弊し、悪意のある攻撃者をプロアクティブに防御することを事実上あきらめていると定義されています**。

シスコのデータから、サイバーセキュリティ対応に疲弊している組織では、マルチベンダー環境が困難であると感じている割合が非常に高いことがわかりました。対応に必要なアラートがあまりに多く、複雑なベンダー混在環境に苦慮しているのに加え、（ダウンタイムの面で）影響の大きな侵害が増加していることで、疲弊度がさらに増していることもわかっています。一方、マルチベンダー環境を管理することが困難だと回答している疲弊した組織は 96% を超え、**マルチベンダー環境の複雑さが、疲弊する主な原因の 1 つであると考えられます**。

セキュリティ製品の統合に費やす時間はありません。セキュリティを確保したいだけなのです。新製品を検討する際には、次の3つのことを確認するようチームに伝えています。

- ・ 確実に機能すること
- ・ すべて可視化でき、見えない部分がないこと
- ・ シスコのセキュリティエコシステムの他の製品と統合されていること

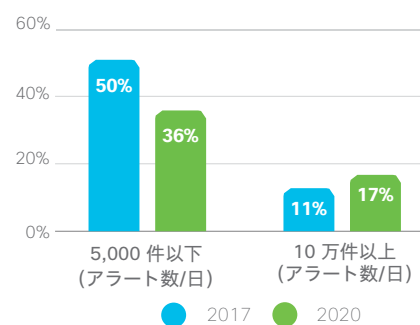
シスコ最高情報セキュリティ責任者 Steve Martino

16. サイバーセキュリティ対応に疲弊しきってしまう原因は何ですか？

前のセクションでは、マルチベンダー環境とサイバー疲弊度の増加の関係を確認しました。ここでは、組織が毎日受信するセキュリティアラートの平均量について確認します。

毎日対応しているアラートの総数は、これまでよりも増加しています。2017年には、1日に受信するアラート数が5,000件以下の組織が50%ありましたが、現在はわずか36%に減少しています。また、1日あたり10万件以上のアラートを受信している組織の数は、2017年の11%から2020年には17%に増加しています（図8）。

図8： 受信したアラートの数（N=2800）。パーセンテージは四捨五入されています。



出典：2020年シスコ CISO ベンチマーク調査

調査したアラートの割合は、過去4年間で最も低い、わずか48%未満となっており、おそらく、アラート数の増加と必要な処理リソースが原因だと思われます（2017年は56%でしたが、それ以降年々減少しています）。正当なインシデントの割合は26%で前年と変わらず、多くの調査で誤検知が起きていることがわかります。

プラスの面を挙げると、正当に修復された脅威の数は昨年のレポート時点から改善され、2017 年時点のレベルと同じ 50% に戻りました。ただし、依然として実際のインシデントの半分以上が放置されていることになります。

特に、膨大なアラート数が、サイバーセキュリティに対する疲弊の要因になっています。サイバーセキュリティに疲弊していると回答した組織の 93% が、毎日 5,000 件を超えるアラートを受信しています。

増加するアラート数と誤検知に対処するために、シスコは、自動化を中心としたアプローチを提唱しています。自動化により、ポリシーを迅速かつ効率的に一貫して適用できるようになります。デバイスが感染している、またはデバイスに脆弱性が存在していると判断した場合、自動的に検疫するか、アクセスを拒否します。管理者の操作は不要です。

17. クラウドでインフラストラクチャをホスティングすることでセキュリティ上どんなメリットがありますか？

シスコの調査では、組織がセキュリティ（88%）およびインフラストラクチャ（89%）をクラウドに移行する主な要因として、有効性、効率性、可視性の向上が挙げられています。86% がクラウドセキュリティを活用することでネットワークの可視性が向上したと回答しているということは、驚くことではありません。2020 年も、クラウド（内部または外部のいずれか）で 20% を超える IT インフラストラクチャを管理している組織が引き続き 83% を超えています。

クライアントは、インシデントを詳細に分析し、高度な分析結果と詳細な調査レポートを作成することに関して、ますますベンダーに頼っています。そのため IR プロバイダーは、製品とプロセスを非常に高度に組み合わせることで、平均被害拡大防止時間（MTTC）およびアクティブなインシデントの平均修復時間（MTTR）を短縮する必要があります。

『Market Guide for Digital Forensics and Incident Response Services（デジタルフォレンジックおよびインシデント対応サービスに関するマーケットガイド）』、Gartner 社、2019 年 12 月⁴

⁴ Brian Reed, Toby Bussa, 『Market Guide for Digital Forensics and Incident Response Services（デジタルフォレンジックおよびインシデント対応サービスに関するマーケットガイド）』、Gartner 社、2019 年 12 月 11 日

18. 将来どのような課題に直面すると考えていますか？

デジタル トランスフォーメーションによって、導入が困難になるかもしれないほどインフラストラクチャが大きく変革されますが、IT リーダーおよびセキュリティリーダーにとっては、イノベーションを推進し、競争優位性を獲得する機会であることに変わりはありません。

セキュリティ担当者は、人工知能と機械学習から高度なテクノロジーとアプローチを取り入れ、DevOps とマイクロセグメンテーションを安全に導入しようとしています。また、周知のとおり、マルチクラウド環境の普及は続いています。

このように環境が激しく変化することを考えると、セキュリティ プロフェッショナルは、基本を習得するだけでなく、最新のテクノロジーにも対応できるようになる必要があります。おそらくこれらの最新テクノロジーのうちいくつかは、現在は主流でなくても、セキュリティエコシステムに不可欠なものになるはずです。

たとえば、デジタル化が普及した現在でも、**多要素認証 (MFA) を使用している組織は 27% に過ぎません**。この値は、価値の高いゼロトラストテクノロジーにとっては低いと言えます。調査対象者の国のうち、MFA の導入率が最も高い国は、順に米国、中国、イタリア、インド、ドイツ、英国でした。導入率が最も高い業界は、ソフトウェア開発、金融サービス、政府、小売、製造、通信でした（率の高い順）。

デジタル トランスフォーメーションにおいては、クラウドの他に、自動化の導入が大きく進んでいます。セキュリティ担当者の多くは、優れた[機械学習機能と人工知能](#)を備えたソリューションを採用しているため、自動化によるスキル不足解消のメリットを得ています。

図 9 に示すように、**回答者の大多数 (77%) が、自動化をさらに進めることでセキュリティエコシステムにおける対応をシンプルにし、応答時間を短縮することを計画しています**。自動化を計画する際には、自動化が最も効果を発揮するエリアを戦略的に定義し、組織内で最も高い ROI を実現する必要があります。

図 9： 2020 年に、組織のセキュリティエコシステム全体で自動化をさらに推進する計画がある組織 (N=2800)。パーセンテージは四捨五入されています。



出典：2020 年シスコ CISO ベンチマーク調査

19. インシデント対応にどの程度重点を置くべきでしょうか？

脅威の状況は進化を続け、あらゆる組織の環境で複雑さを増し、大きな課題となっています。人材不足とインシデントの増加が相まって、ほとんどの組織のセキュリティ体制は全般的に脆弱になっています。座してアラートを待っているだけでは、厳しい罰金、監視の強化、知的財産の喪失、[データプライバシーの侵害](#)、ビジネスの喪失に直面する可能性があります。可視化、脅威ハンティングの実施、ゼロトラストフレームワークの確立を実現して防御することは、インフラストラクチャを保護する上で不可欠になっています。

IT に関する意思決定者に対するシスコの調査では、**76% がインシデント対応に「非常に精通している」と評価し、23% が「ある程度精通している」と回答していて、合計で 99% を占めています。**これはよい状態ですが、シスコの調査によると、セキュリティの複雑さによって貴重なリソースに負担をかけ、サイバーセキュリティに対する疲弊を招いています。アウトソーシングが有効なのはこのような状況です。

図 10：インシデント対応について「非常に」または「ある程度」精通していると回答した人の割合は、合計で 99%（N=2800）。パーセンテージは四捨五入されています。



組織の 34% がインシデント対応サービスをアウトソーシングし、36% が外部/サードパーティサービスを使用して侵害されたシステムを分析していることがわかっています。この割合は、昨年から増加しています。インシデント対応サービスを利用することで、資産の保護、リスクの軽減、コンプライアンスの維持に関するアプローチが効率的になっています。またこのようなサービスは、専門知識を活用しながら事前に計画を策定し、対応を調整した上で実施することで、組織が未知の脅威を防御できるようサポートします。

自分自身や自分のスタッフがサイバーセキュリティに関してキャリアを伸ばす方法を知りたいですか？

こちらをご覧ください：[シスコセキュリティ認定](#)

20. セキュリティポスチャを改善するために、今何ができるでしょうか？

組織は、豊富な資金を備え、果てしなく忍耐強い積極的なセキュリティ犯罪者に直面しています。また、ユーザ、アプリケーション、デバイスの正確なインベントリを維持するなど、決して終わることなく常に繰り返される課題にも対応しています。さらに、チームが迅速に行動できるようにサポートしながら、セキュリティリスクとビジネスリスクに備えています。しかし、ビジネス上の方針は、セキュリティのことが考慮されずに決定されています。新しい規制、取締役からの指示、厳しい予算、リスク管理、セキュリティ人材の入れ替わりなど、

組織を防御する上での課題はますます増え、とどまることを知りません。今こそスマートに取り組んで防御を効率化し、脅威を検出して修復するだけでなく、予防にも注力すべき時です。このレポートでは、組織をより安全に運営するために考慮すべき20の領域について説明しました。そして、これらの各領域において、次のような事項を推奨しています。

- ・ MFA（多要素認証）、ネットワーク セグメンテーション、エンドポイント保護などの階層型防御を採用する
- ・ 最高レベルで可視化し、データガバナンスの強化、リスクの軽減、コンプライアンスの向上を実現する
- ・ 防御の強化、デバイスの更新とパッチ適用、訓練とトレーニングに基づく重点的なサイバーセキュリティ対策を実施する
- ・ ゼロトラストフレームワークを構築し、セキュリティ成熟度を高める（図 11）

図 11：ゼロトラスト戦略により、ワークフォース、ワークロード、ワークプレイスを保護する



ワークフォースの保護
アプリケーションに接続するユーザおよびデバイスのアクセスを保護する



ワークロードの保護環境
境全体のアプリケーションにおけるすべての接続を保護する



ワークプレイスの保護
ネットワーク全体の接続を保護する

シスコは、今こそセキュリティ業界が進化する時だと考えています。セキュリティソリューションは、1つのチームのように機能する必要があります。チームメンバーはリアルタイムにコミュニケーションを行い、相互に学習し、調整された1つのユニットとして対応します。組織のエンドポイントセキュリティは、ネットワークセキュリティとクラウドセキュリティと連携しなければなりません。また、アイデンティティとアクセスをカバーする MFA が必要です。シスコは、お客様のビジネスを確実に保護するには、セキュリティ上のすべてのギャップを埋めるプラットフォームアプローチが最適だと考えています。

現在も今後も セキュアに

シスコのビジョンは、お客様がセキュリティをシスコに任せ、コアとなるミッションに注力できるように、現在も今後も脅威からお客様を保護することです。

非常に優れたセキュリティチームが構築したシスコ セキュリティ プラットフォーム、[SecureX](#) を導入することで、お客様のビジネスの進め方に応じた保護を実現できます。以下のような特長があります。

- ・ まずは、ネットワーク、エンドポイント、アプリケーション、クラウドを保護する、**最適な製品を組み合わせることから始めます。**
- ・ **信頼性検証機能**を利用し、適切なユーザのみがアクセスできるように制御します。
- ・ 各製品は、業界をリードする [Talos 脅威インテリジェンス](#)を活用し、より多くの脅威をブロックして組織を保護します。
- ・ **高度な脅威に自動的に対応し、ポートフォリオ全体で統合された脅威管理機能およびセキュリティ管理機能で運用を効率化します。**
- ・ セキュリティ対応を統合するために、**お客様がすでに導入しているシスコ以外のテクノロジーとも連携できるようにソリューションを構築しています。**

SecureX は、可視化、アクションの自動化、セキュリティポスチャの改善を実現します。カスタマイズされたクラウド配信型アプリケーションも **SecureX プラットフォーム**に組み込まれているため、セキュリティ対応がシンプルになります。シスコの統合セキュリティポートフォリオとお客様環境のサードパーティ製品を、一貫したインターフェイスで利用できます。また、シスコのプラットフォームレベルのイノベーションによって、非常に優れた統合分析機能が実現されています。すべては連携して機能します。

- ・ [SecureX](#) は、セキュリティ、ネットワーク、IT 運用チームをコラボレーションワークフローに統合することで、生産性を向上させます。
- ・ [Cisco Threat Response](#) により、脅威の調査と修復作業がシンプルになり、SecOps の効率性が向上します。
- ・ **分析機能**により、未知の脅威の検出が容易になるため、効果的にポリシーを決定して脅威に対応し、応答時間を短縮できます。

シスコの統合型製品と業界トップクラスの脅威インテリジェンスにより、多くの脅威や複雑さにも対応できる見識、スケール、そして能力を得られます。また、セキュリティを最優先させることで、資産を保護しながらイノベーションを促進できます。シスコにとってセキュリティは最優先です。進化を続ける脅威に対処可能な、効果的なネットワークセキュリティを実現できるのはシスコだけです。シスコのプラットフォームアプローチの詳細については、cisco.com/jp/go/security をご覧ください。

シスコ サイバー セキュリティレポート シリーズ概要

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

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

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



2019 データプライバシー



2019 脅威レポート



2019 CISO ベンチマーク



電子メール：クリックは慎重に



セキュリティの最低ライン



脅威ハンティング



コンシューマプライバシー調査



2019 年の脅威



2020 データプライバシー



2020 CISO ベンチマーク

©2020 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

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

この資料の記載内容は2020年3月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



お問い合わせ先

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>

