Forrester Consulting
Thought Leadership Paper
（IBMの委託による調査）

2019年5月

2019年 サイバーセキュリティに見られる複雑化に関する報告

複雑化の低減がいかに優れた結果を生むか

FORRESTER®

目次

プロジェクト ディレクター：
Josh Blackborow、Sophia Christakis、マーケットインパクト コンサルタント

リサーチ貢献者：
Forrester社セキュリティ&リスク・リサーチ・グループ

FORRESTER CONSULTINGについて

Forrester Consultingは組織のリーダーがその組織を成功に導けるよう、独自の客観的調査に基づくコンサルティングを提供しています。お客様はそれぞれの事業課題に最適な専門知識と経験を有するリサーチアナリストを通じて、短期の戦略セッションからカスタムメイドのプロジェクトに至るForrester Consultingのサービスを利用することができます。詳細については、forrester.com/consultingをご覧ください。

FORRESTER®

別々に稼働し膨大な量のデータを生み出す、接続されていない個別のセキュリティソリューションが複雑化の危機を引き起こす。

セキュリティエコシステムの簡素化に取り組んだ組織は、セキュリティ脅威に対するレジリエンスの強化などの恩恵を受けている。

エグゼクティブサマリー

セキュリティ脅威の現状は目まぐるしく変化し続け、組織におけるセキュリティはこれまでになくきわめて重要かつ困難な課題となりました。組織はネットワークに接続されていないポイントソリューションに多額の資金を投入し、その都度対処してきましたが、別々に動作し膨大なデータが生成される個別製品を組み合わせた結果、複雑化の危機に陥りました。結局セキュリティ担当チームは投資を最大限に活用できず、確実に環境の安全を確保するにはまたさらに投資しなければならない状況です。複雑化を解消する必要性はこれまでになく明らかです。

このような背景で、Forrester ConsultingはIBM社の委託により、セキュリティの複雑化と複雑化がセキュリティの効率と効果に及ぼす影響を評価しました。このテーマを深く掘り下げるため、Forresterは、セキュリティ戦略またはセキュリティ関連技術の購入を担当する世界中のセキュリティ担当者200人を対象にアンケート調査を実施しました。調査では、回答者のほぼ全員が複雑化に関する懸念があると回答していました。一方、複数のソリューションを単一の管理プラットフォームで一元管理するなど、組織のセキュリティエコシステムを簡素化する手段をとった組織では、有意義なメリットが確認されているようです。

主な調査結果

- **悪化し続けるセキュリティ環境の複雑化。**セキュリティ担当者はサイロ化されたチームで業務を行うことが多く、セキュリティ分野全体でのデータとプロセスの全体像を完全に掌握できることは、不可能ではないにしても、めったにありません。状況をさらに悪化させることに、ロケーション全体のデータ量が、ここ数年間では特にクラウド上で激増し、その傾向は今後も続くと見られています。
- **組織の支出額は増加傾向で、必ずしも賢明な支出ではない。**セキュリティへの経費増大と組織が損害を被るデータ漏洩を回避しようとするプレッシャーによって、組織はネットワークに接続されていないポイントソリューションを過剰に採用しました。当社の調査によれば、ここ2年間で平均して、セキュリティ対策製品では52%、ベンダーでは77%が追加されています。この異常な購買熱は組織のセキュリティの複雑化を激化させたものの、セキュリティプログラムの全体的な成熟度には必ずしも貢献しませんでした。
- **複雑化はROIをも蝕む。**セキュリティの複雑化は、組織がこれ以上無視できないレベルの問題となりました。当社調査によれば、組織の91%が複雑化に対して懸念を表し、そして複雑化が非常に悪化した環境においては、経費に関する課題とテクノロジーとスタッフの非効率性の問題に言及する割合が高かったことが示されています。
- **簡素化によってセキュリティ価値を発見できる可能性がある。**環境の簡素化に効果的に取り組んだ組織では、それまでのセキュリティへの投資を最大限に活かすことができています。そのような組織ではデータとプロセスを接続し、ソリューションの一元管理プラットフォームへの統合が行われています。さらに、脅威の検出・対応そして脅威からの復旧といった恩恵も複数獲得しています。

FORRESTER®

リアクティブな対処が長期化を招いたセキュリティソリューションのもつれ問題

データ漏洩の大々的な報道により、セキュリティ対策は企業幹部に認識されるようになりました。それによってセキュリティ担当の責任者にとって、セキュリティプロジェクトへの投資の予算と幹部の承諾を得やすい状況が生まれました。実際、IT予算におけるセキュリティ関連支出の占める割合は増加傾向にあります。[1]同時に、業界が新たな脅威から身を守るために興味をそそられる大量のソリューションに反応してしまったのも事実です。[2]結果はどうなったでしょうか。リアクティブなセキュリティ支出と非効率性の蔓延です。

当社調査に参加した、セキュリティアセットの最適化と来年の人材獲得を優先課題にしている200人のセキュリティ意思決定者の回答には、2つの強い傾向が確認されました。回答者は「セキュリティ投資のリターンを改善」を「高度な脅威への対応能力を改善」に続く優先事項の1つにあげています。さらに、多くが、環境の簡素化や運用効率の向上を行うことでスタッフの生産性を向上させることに注力しています（図1を参照）。それにも関わらず、下記に示す解決の必要性に迫られている問題のため苦戦を強いられることになります。

- **接続されていないポイントソリューションの数が急上昇。**セキュリティ担当者は、特に漏洩被害を経験した企業に勤務する場合、その増え続ける予算で新しいセキュリティソリューションの購入に及びました。しかしその多くが短絡的な解決策にとどまり、追加ソリューションの一つひとつが及ぼす長期的なセキュリティプログラムの成熟度への影響までは十分に考えられていませんでした。その結果、セキュリティ担当チームは、異種のソリューションで構成された接続されていないポイントソリューションを持て余すことになります。当社調査の回答者の勤務する組織では、13社のベンダーから平均25種類の異なるセキュリティ対策製品やサービスを管理しており、多くの組織ではその数はさらに多くなります。ここ数年の異常な購買熱の兆候として、セキュリティ製品の52%の上乗せと、新規ベンダー77%の上乗せが24ヵ月以内に行われた現象があげられます。
- **データ量の激増。**この2年間でデータは、オンプレミス、エンドポイント、バーチャルサーバ、そして特にクラウドで大幅に増加しました。当社でテストを実施した各ロケーションでは、回答者は少なくとも保存データ55%増を報告し、さらに多くがデータの2倍、3倍、もしくはそれ以上の増加を報告しています（図2を参照）。セキュリティ対策製品のように増やして対応した状況とは異なり、セキュリティ担当チームがデータの増加に対してコントロールできることはほぼ皆無に等しく、その状況は今後も数年ほど続くと見られています。

回答者の組織ではセキュリティベンダーが24ヵ月間に平均77%追加された。

図1

今後12ヵ月のセキュリティ優先事項ランキング

調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
出典：IBMの委託によるForrester Consulting実施の調査2019年1月

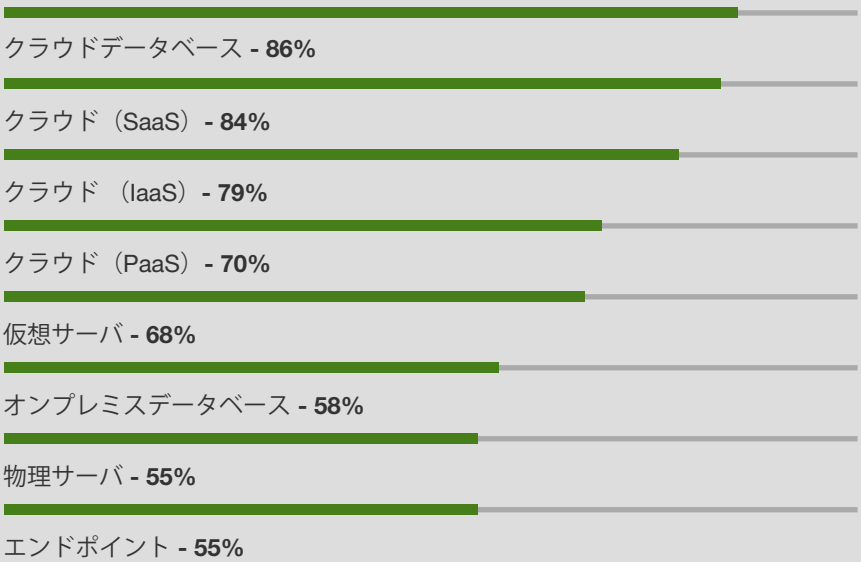
› **異種環境に生息するデータ。**現在、エンドポイントとオンプレミスサーバーから移動されるデータは増加傾向にあり、企業全体のデータ数は激増しています。多くの組織がクラウドファースト戦略を採用した状況に鑑みると、それほどの組織データがクラウドに移行され、セキュリティアセットやプロセスも続いて移動されたのも当然でしょう。実際、回答者は2020年までには、組織のクラウド上のセキュリティアセットとプロセスは2016年時と比較して200%超の増加を予測しています。異種アーキテクチャに分散するデータはセキュリティチームの可視性を脅かします。セキュリティチームの目に触れないと、価値あるデータアセットは守られません。

組織が寄せ集めた数々の幅広いセキュリティ防衛策にもかかわらず、セキュリティ担当者はその投資を最大限に活用することと組織の保護に苦心します。[3] 実際、高度な脅威インテリジェンス機能の開発をはじめ、セキュリティスタッフの増員、データからのインサイト抽出、効率性の推進の支援という観点でセキュリティポートフォリオに完全に満足していると回答しているのは4割未満です。さらに、当社調査に使用したセキュリティテクノロジーの11カテゴリーに関して言えば、任意の1カテゴリーのすべてまたは大半の機能を使用していると回答したのは50%未満でした。同時に、25%が組織のテクノロジーはモノのインターネット（IoT）のセキュリティ、IDとアクセス管理、セキュリティの自動化とオーケストレーション、セキュリティ情報イベント管理（SIEM）で完全に最適化されていると回答していることは特筆すべき事実です。

回答者は、組織のクラウド上のセキュリティアセットとプロセスが2016年時と比較して2020年までに200%超増加することを予測。

図2：複数ロケーションにまたがるデータ量がここ2年で激増

「過去2年間では、貴社が下記のロケーションに保存しているデータの量はどのように変化しましたか？」
（平均増加率を示す）



調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
出典：IBMの委託によるForrester Consulting実施の調査。2019年1月

FORRESTER®

複雑化に脅かされるサイバーセキュリティの効果

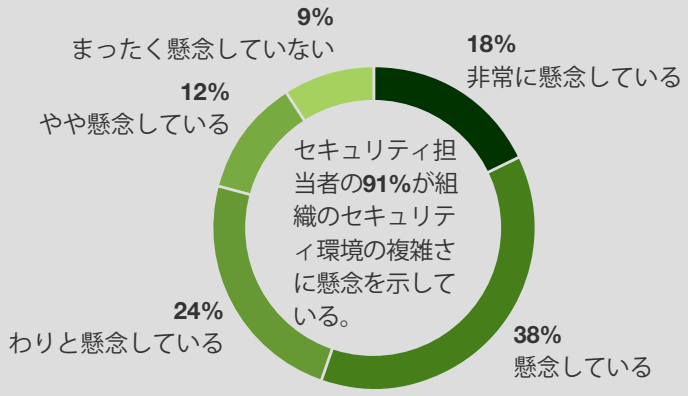
昨今のセキュリティ責任者は複雑化したセキュリティ環境の管理に追われ、接続されていないポイントソリューションを追加することでは複雑化は何も解消されないという痛い教訓を実感しているところです。長時間のデプロイメントサイクル、難しい統合、殺到するソリューションの管理にはテクノロジーへの投資を失敗させるリスクがあります。[4] 回答者はこれを非常に現実的な脅威であると認識しており、91%が組織のセキュリティの複雑化に一定レベルの懸念を示しています（図3参照）。主な懸念点の2番目となり、「変化・進化するという脅威の性質」に僅差で続きます。

ほぼ全員の回答者が環境の複雑化に対しある程度の懸念を示している状態に加え、最高レベルの懸念を示した回答者の回答を見れば、いかに組織が複雑化したかが明確に表れていることがわかります（図4参照）。予想にたやすく、複雑化に関する懸念度の高さに比例して、組織はより多くの製品とデータを所有していました。複雑化への高い懸念度を示した回答者はまた、懸念度の低い回答者に比べ、平均してセキュリティ対策の製品（45%）とベンダーの所有（36%）が多かったことが示されています。さらに、複数ロケーションでより多くのデータを管理していました。実際、分散したセキュリティテクノロジーとデータソースの統合が困難であると回答し、さらにセキュリティ関連のデータとインサイトに対する可視性の獲得に苦労していると回答する割合がほかの組織に比べ2倍になっています（図5参照）。その上、収集したインサイトはどれもその上に構築が困難です。過半数が、セキュリティインサイトについて組織内外の同僚と協働することを障壁であると認識しており、それによって脅威インテリジェンス機能の開発と脆弱性のパターン摘発が困難になっています。

セキュリティ担当者の91%が、組織のセキュリティの複雑化に懸念を示している。

図3：セキュリティ担当者を最も悩ませるのは複雑化に関する懸念

「組織のセキュリティ体制の保護という観点では、下記の項目はどの程度懸念材料になりますか？」
（「所属する組織のセキュリティ環境の複雑さ」に対する回答を表示）



調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
注：値を四捨五入しているため合計が100%にならないことがあります。
出典：IBMの委託によるForrester Consulting実施の調査。2019年1月

セキュリティの複雑化は回答者の懸念事項の上位にランキングし、IT脅威と規制コンプライアンスの変化するという性質に対する懸念度を凌ぐ。

FORRESTER®

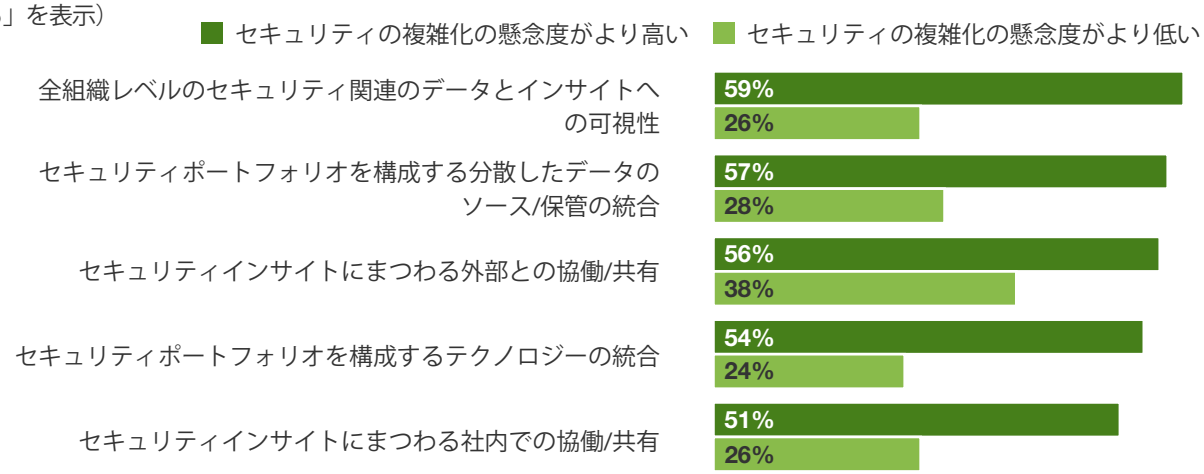
図4：複雑化に対する懸念

「組織のセキュリティ体制の保護という観点では、セキュリティの複雑化はどの程度懸念材料になりますか？」

セキュリティ複雑化の懸念度がより高い (N = 112)	セキュリティの複雑化の懸念度がより低い (N = 88)
「非常に懸念している」または「懸念している」	「わりと懸念している」、「やや懸念している」、「まったく懸念していない」

図5：高度な複雑化により引き起こされた大きな課題

「下記の各項目は、セキュリティ担当チームにとってどの程度困難ですか？」（「困難である」または「きわめて困難である」を表示）



調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
出典：IBMの委託によるForrester Consulting実施の調査。2019年1月

より高い懸念度を示した回答者（当社調査でより高い複雑化を示した回答者）はまた独特な不利を被る状況にあることも示されています。

- **複雑化はROIをも蝕む。**セキュリティの複雑化はただでさえ困難な既存の課題、たとえばセキュリティリソースの最大活用などをさらに深刻化させます。複雑化への懸念度が高い回答者では、その組織のセキュリティ環境の複雑化が高いコストにつながったと回答する割合が高い傾向にあります。さらに同回答者グループでは、セキュリティテクノロジーの活用やセキュリティスタッフの時間の使い方が非効率的で、新しいセキュリティ対策製品のスタッフ研修を困難であると認識している割合が高い傾向が示されています（図6参照）。
- **複雑化はイノベーションを妨げる。**政府機関・競合他社・顧客に起因する市場の不確実性は常に変化します。速く、コネクテッドな環境を持ち、イノベーティブな者のみがこの移りゆく市況で勝ち残ることができます。セキュリティの複雑化を有する場合、必要なアジリティをもって進化することに苦労しています。50%がその複雑化によって旧式のセキュリティテクノロジーを置き換えることが困難であると回答し、37%はさらなる複雑化の悪化を恐れて購入を見合わせているしていると回答しています。さらに困ったことには、29%は特定のベンダーに縛られていると感じています。高度に複雑化したセキュリティ環境をもつ企業は、より能率化されたエコシステムからメリットが得られる可能性がある一方で、近代化への取り組みにおいては、複雑化の低い企業に比べ、苦戦を強いられています。

高度な複雑化が発生している組織ではコスト面での苦労に言及する傾向が強く見られ、テクノロジーやスタッフの非効率性においても同様のことが言える。

FORRESTER®

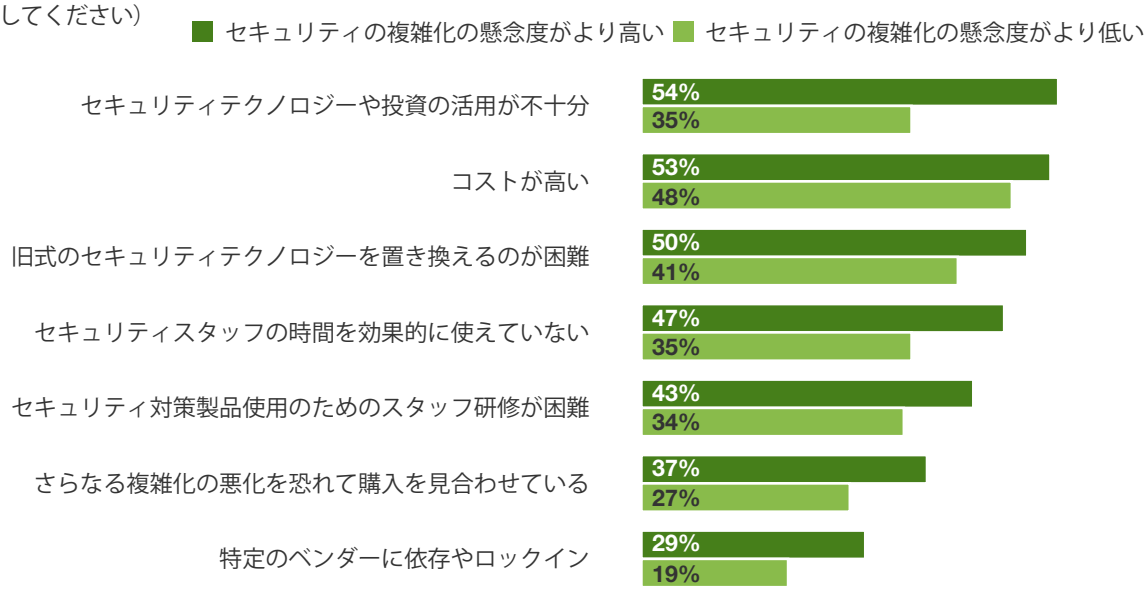
セキュリティの簡素化は投資の価値発見につながる

目前に立ちはだかる複数の課題にもかかわらず、複雑化の懸念度の高い組織には簡素化を価値のある取り組みであると認識している組織もあります。そういった組織では、簡素化された環境に複数のメリットを見出しています。たとえば、データからのインサイト抽出能力の改善をはじめ、脅威インテリジェンス、社内コラボレーション、ユーザーエクスペリエンスなどがあげられます。ここで特筆すべきなのは、72%の回答者が簡素化されていれば「中程度」または「非常に」改善されていただろうと思った事柄に、運用効率とセキュリティスタッフの生産性の改善（68%）そしてセキュリティ投資の利益率の改善（58%）をあげており、それらはいずれも回答者の高優先事項となっていることです。

組織は簡素化された環境が、運用効率、セキュリティスタッフの生産性、セキュリティ投資の利益率の改善につながると考えている。

図6：ROIを減らし、柔軟性を制限し、モダナイゼーションへの取り組みを阻害するセキュリティの複雑化

「貴社のセキュリティ環境が複雑化していることで直面した困難にはどのようなものがありますか？」（該当するものをすべて選択してください）



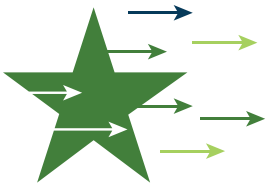
調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
出典：IBMの委託によるForrester Consulting実施の調査。2019年1月

サイバーセキュリティポートフォリオの簡素化こそが解決への道

セキュリティの複雑化にまつわる課題と簡素化のメリットを一旦認識すると、次に「組織がセキュリティの複雑化を低減するには何ができるのか?」という疑問が浮上します。回答者全員が複雑化を低減するために少なくとも何らかの手段をとったと回答しており、半数以下（44%）はその取り組みは効果的であったと回答しています。本調査の目的に沿って、ここではそのような組織を「チャンピオン」と称し、それ以外（取り組みについて「わりと効果的」、「やや効果的」、「まったく効果的でない」と回答した者）を「チャレンジャー」と称します（図7参照）。

チャンピオン組織は簡素化への取り組みではより効果的でも、簡素化への道はまだ続いています。実際、その多くが複雑化を懸念しているという回答をしています。とはいえ、セキュリティの能率化には大きく着手し始めており、現在も苦労している組織の役に立つ教訓がすでにあります。以下、チャンピオンにみられた特徴を記します。

- **簡素化を優先している。**当然のように思われるかもしれませんが、チャンピオンとチャレンジャーの明確な違いは簡素化がどの程度優先されていたかでした。チャンピオンの簡素化を優先させた割合が高かっただけでなく、その取り組み専門に特定のリソースを投入していた割合も高い傾向が示されています（図8参照）。チャンピオンが専門チームを配置した割合は75%で、チャレンジャーでは56%でした。さらに、チャンピオンの63%以上が当社が検証した各簡素化対策を採用していました。



「チャンピオン」とはセキュリティの複雑化の低減において大きく前進した組織を指す。

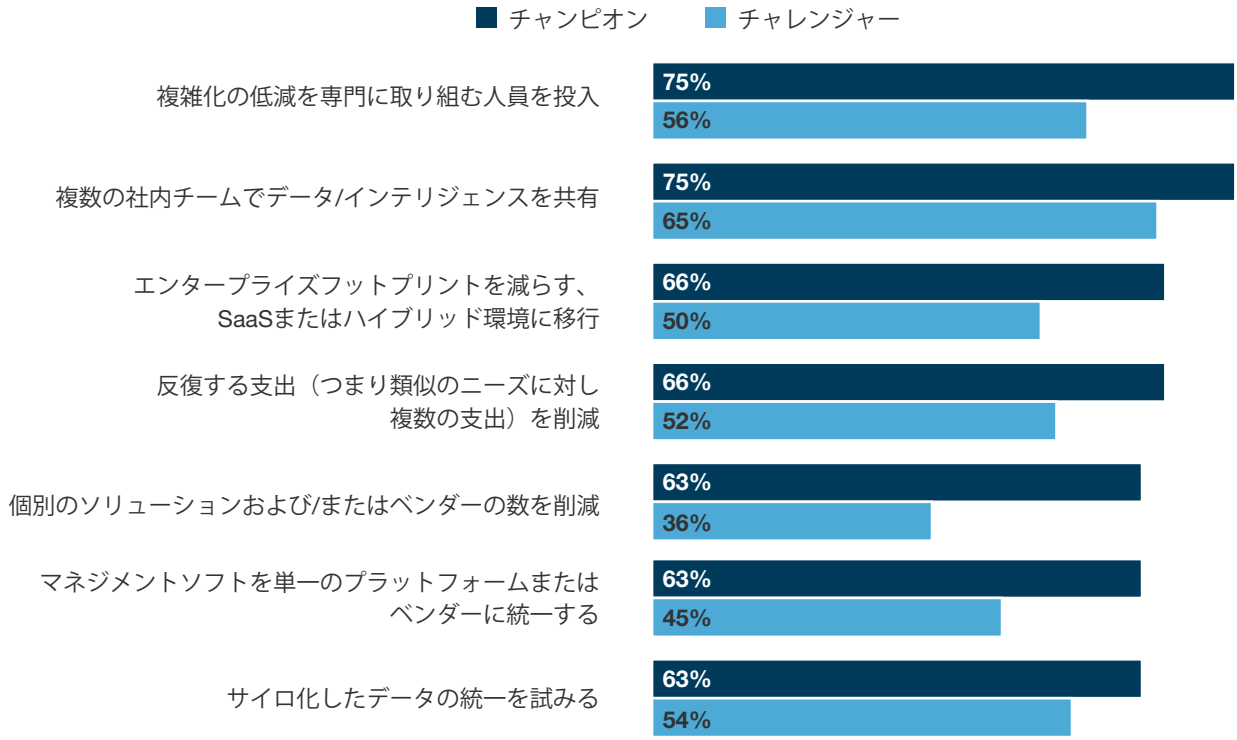
図7：「チャンピオン」と「チャレンジャー」の特徴づけ

「現時点まででは、セキュリティの複雑化を低減する貴社の取り組みはどの程度効果的でしたか？」

チャンピオン (N = 87)	チャレンジャー (N = 113)
「非常に効果的」または「効果的」	「わりと効果的」、「やや効果的」、「まったく効果的でない」、「判断するには時期尚早」

図8：簡素化への取り組みでより前進したのはチャンピオン

「貴社がセキュリティ環境を簡素化するために、下記のアクションのうちどれを実行しましたか？または、実行予定ですか？」



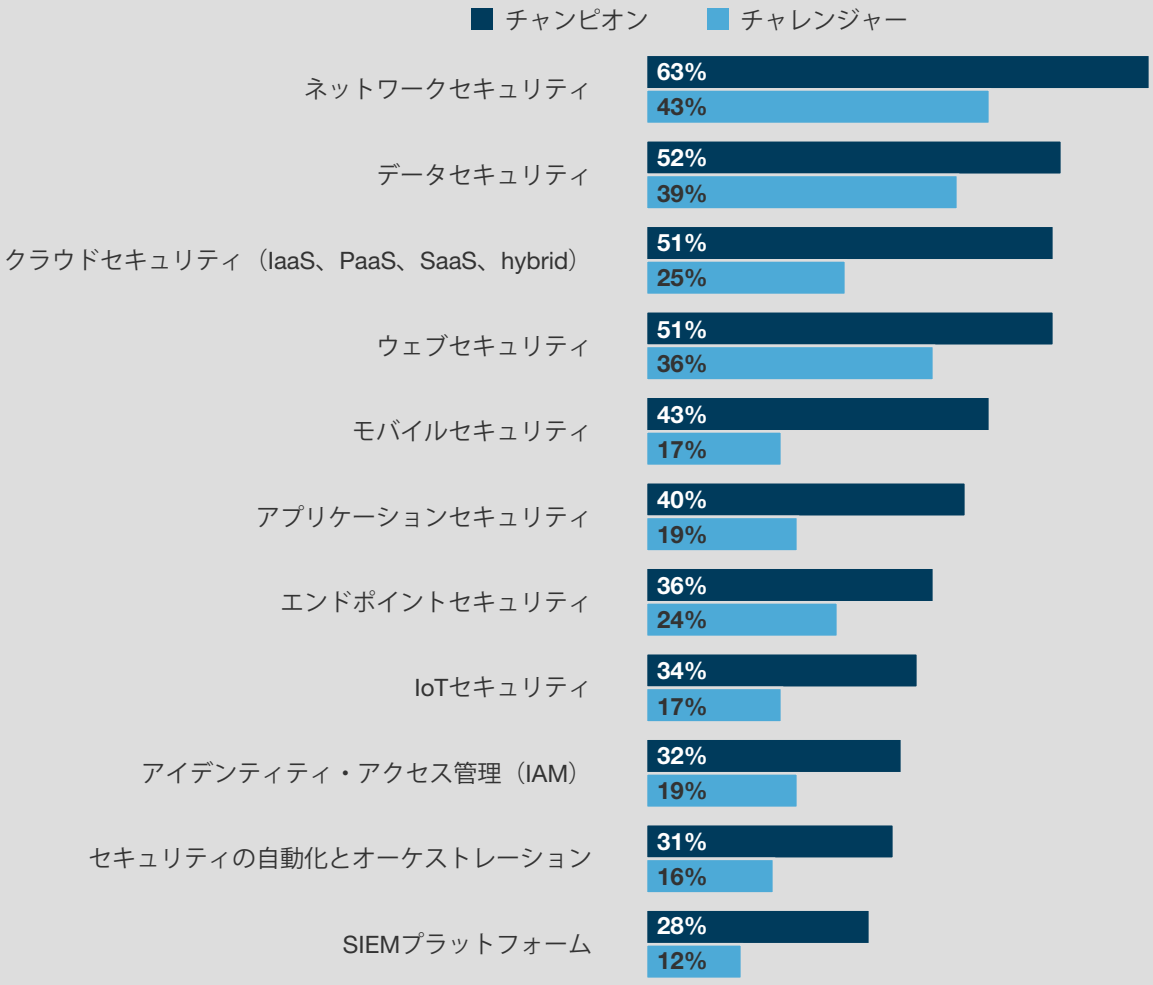
調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
出典：IBMの委託によるForrester Consulting実施の調査。2019年1月

› **既存の投資を最適化する。**既存のテクノロジーを最適化せずに、目新しいポイントソリューションを追いかけてしまうと類似のニーズに複数の個別ツールを使用する状況に陥ります。より効率的なアプローチは、既存ツールを小規模単位にまとめてその使用を最適化し、そこで再編成と再投資が可能な機会を探索することです。[5]チャンピオンはまさにそれを実施しており、63%が接続されていないポイントソリューションの数を減らす努力をしたと回答し、一方チャレンジャーでは36%でした。さらに、チャンピオンは反復する支出を阻止する割合が高い傾向にあります（それぞれ66%、52%）。最後に、チャンピオンは既存のセキュリティツールからより価値を絞り出していました。セキュリティ投資全般においてより高い活用率が確認されています（図9参照）。

チャンピオンはマネジメントソフトを単一のプラットフォームまたはベンダーに統一している割合が高い傾向にある。

図9：チャンピオンは既存のセキュリティ投資からより価値を抽出している

「貴社では、次の領域のセキュリティテクノロジーをどの程度完全に活用していますか？」
（「完全に最適化 - これらのソリューションの機能のすべてまたは大半を利用している」）



調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
出典：IBMの委託によるForrester Consulting実施の調査。2019年1月

› **マネジメントを単一のプラットフォームに統一する。**チャンピオンはマネジメントソフトを単一のプラットフォームまたはベンダーに統一している割合が高い傾向にあります（それぞれ63%、45%）。セキュリティアセットの管理を統一されたプラットフォームで行えば、分散したソリューションをまとまりのある、連携がとれ接続されたセキュリティスイートへと変身させることが可能です。統一オファリングはセキュリティ担当チームにより高い可視性と環境制御レベルを提供します。さらに運用の煩雑さと個別製品を別個に管理するコストも同時に削減し、セキュリティ防衛ツールの自動化とオーケストレーションの基盤を構築します。[6]

複雑化への対応で組織のレジリエンスが強化される

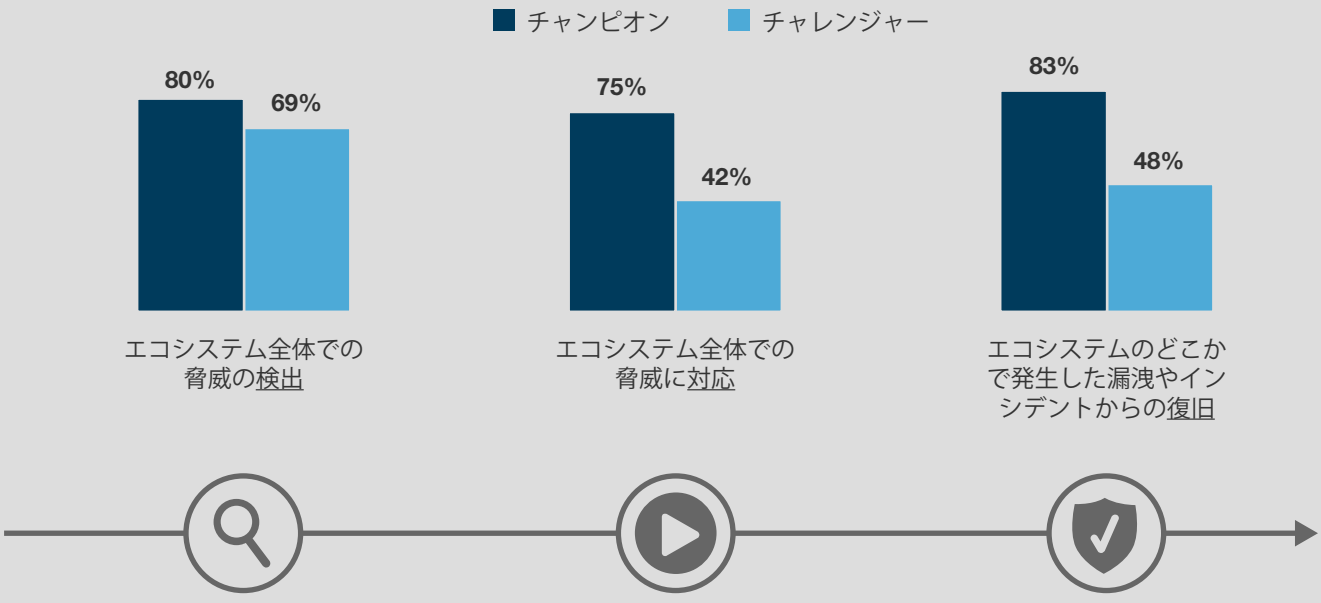
本調査で特に興味深い発見として、チャンピオンは効率性の改善による恩恵を受けただけでなく、サイバーセキュリティ脅威から会社を守ることにも成功していた割合が高かったという点があげられます。

チャンピオンは、効率性の低い組織に比べ、エコシステム全体で脅威を検出する組織のセキュリティポートフォリオに満足していると述べた割合が高く、さらに、セキュリティへの*応答*とセキュリティインシデントからの*復旧*の能力に満足している割合は有意に高く、マージンは33～35ポイントの範囲に設定されていました。チャンピオンにも複雑化を克服するための作業はまだ残っているとは言え、取り組みの優先や、既存の投資を最大活用、マネジメントツールの単一プラットフォームへの統合など、問題にアプローチにすることにより、チャンピオンのセキュリティ破壊から組織を守る準備体制はよりはるかに整っています（図10参照）。

チャンピオンは脅威の検出や脅威への応答、セキュリティインシデントの復旧においてもより効率的。

図10：チャンピオンは脅威によりレジリエンスがある

「下記の項目において、貴社のセキュリティポートフォリオから得られる支援にあなたはどの程度満足していますか？」
（「完全に満足している」または「満足している」を表示）



調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
出典：IBMの委託によるForrester Consulting実施の調査。2019年1月

FORRESTER®

簡素化で重要な役割を担うセキュリティベンダー

多くの組織は、セキュリティエコシステムの簡素化で組織としての進歩はある程度達成しました。とは言え、セキュリティベンダーが組織の取り組みを支援する変化を行わなければ、組織が経験したメリットの寿命は長くは続きません。組織はこの際、ベンダーが非効率性のスパイラルの長期化に加担したことは無視する必要があります。実際、調査に参加した意思決定者の98%は、複雑化の低減にセキュリティベンダーのヘルプを求めています。ベンダーからの提供を希望するソリューション（図11）：

- **使用・統合・購入が簡単なソリューション。**Forresterの調査では、セキュリティ責任者はスタッフとスキルの不足に関する重大な課題に直面していることが示されています。[7] 当社の調査によりその傾向はさらに強固なものとなり、44%のセキュリティ責任者が、会社を守る際の懸念点にスタッフ不足をあげています。過剰な数のテクノロジーの不適切な統合は、人的資本問題を悪化させるばかりです。また組織の問題の対処も困難にします。40%がスキル不足を環境の簡素化への取り組みにおける障壁であると述べています。多くのセキュリティベンダーは現在、使いやすさとシンプルな制御に配慮した新たなプラットフォームを開発しています。[8] 当社調査に参加したセキュリティ担当者は、そういったタイプのツールへの関心、そして統合と購入が簡単なツールへの関心を示しています。
- **すでに配置されているソリューションの最適化と接続。**セキュリティ担当の意思決定者は、ベンダーが既存のセキュリティの現状を理解してくれることを期待しています。ベンダーに期待するのは、既存のセキュリティ投資の価値を拡張し、サイバーセキュリティの長期的な成熟に貢献する機能のみを統合することです。これには、そのベンダーのポートフォリオ内に留まらず、ほかのベンダー製品とのシームレスな統合が可能であることが含まれます。
- **保存場所にかかわらずデータを有効化し接続する。**データ量が増大し、またデータが会社の隅々にまで広がっている状況では、インサイトや分析のために組織が無理なくすべてのデータを一元管理できる場所一つに集約することは至難の業です。これに挑戦するとなると多大なコストがかかります。セキュリティ担当チームは、高い費用と時間のかかる、複雑なマイグレーションプロジェクトの必要性を減らすことで、保存場所に関わらずデータの有効化と接続をヘルプしてくれるベンダーに価値を見出しています。

図11：セキュリティ担当者は、セキュリティ簡素化のための取り組みをサポートしてくれるベンダーを求めている

「セキュリティの複雑化を低減するためにベンダーにヘルプしてほしいのはどのようなことですか？」（該当するものをすべて選択してください）

59% - 使用・統合・購入が簡単なソリューション

57% - すでに配置されているソリューションの最適化をヘルプ

55% - ユースケース全体を隅々まで解決できる統合ソリューション

48% - データと製品をベンダーに関係なく接続することをヘルプ

46% - 保管されているその場所でデータをアクティブにすることをヘルプ（データのマイグレーションの必要性を低減）

調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
出典：IBMの委託によるForrester Consulting実施の調査。2019年1月

主な推奨事項

複雑化は昨今の状況ではますます緊急性が高まっている課題で、対処しなければ問題は大きくなり続けると見られています。このような潜在的な危険を回避することを切望するセキュリティ担当チームは、セキュリティの複雑化を低減することを組織の優先事項とし、重点的に取り組むことが勧められます。下記は実現のための主要アクションです。

ビジネス目標に集中した取り組みができるように機能を統一する。個別のソリューショの数を減らせば、セキュリティエコシステムの円滑な運輸を維持するために必要な管理とメンテナンスの量を減らすことができます。既存のソリューションに再投資・再編成する方法を模索して、組織のスタッフ増員を阻止しとROIを増加できるよう支援します。

データのサイロ化を低減し、セキュリティ担当チームの摩擦を制限する。セキュリティ・情報テクノロジーの統合をし損ねる組織は、さらにアプリケーションのデータも加味すれば、不測のセキュリティ問題の際に迅速で正確な意思決定を行うために必要な情報を持つことはできません。懸念度の高い組織ほどデータの分離が症状として見られます。セキュリティ担当チームに分散したデータソースが届けられ、分析に取り組めるツールやテクノロジーがあれば、チームがためらうことなく行動できるようになります。

エコシステムを簡素化して応答と復旧を強化する。脅威の検出はセキュリティポートフォリオの改善によって比較的良好な改善が期待できることは知られていますが、顧客のエコシステムで発生したインシデントに発生場所に関わらず応答して復旧することで多大な利益につながることが確認されました。セキュリティ責任者にとって「起きるかどうかではなく、いつ起きるか」という格言は真実であり、応答と復旧は重点領域の中心に置くことが必須となります。セキュリティの簡素化こそが、実現のための唯一の確実な方法です。

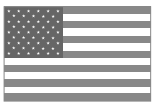
FORRESTER®

付録A：調査方法

本調査では、Forresterは組織のセキュリティ戦略やテクノロジー購入の意思決定者または影響力を持つセキュリティ担当者200人を対象にオンライン調査を実施しました。回答者は米国・カナダ・英国・フランス・ドイツの少なくとも従業員数500人を抱える企業から選出されています。調査では、組織のセキュリティテクノロジーポートフォリオのステージと、複雑化の影響が組織のエフェクティブネスに顕れる時点までの程度を評価しました。参加者に出題したた設問の内容は、セキュリティ戦略を推進する主な目情、成功を妨げる課題、セキュリティの簡素化のために採用した方法、セキュリティアセットとリソースを最適化することで期待できる価値に及びます。回答者には、調査への協力に対する謝礼が贈られています。調査は2018年12月に開始し、2019年1月に完了しました。

付録B：統計

国


米国 **40%**

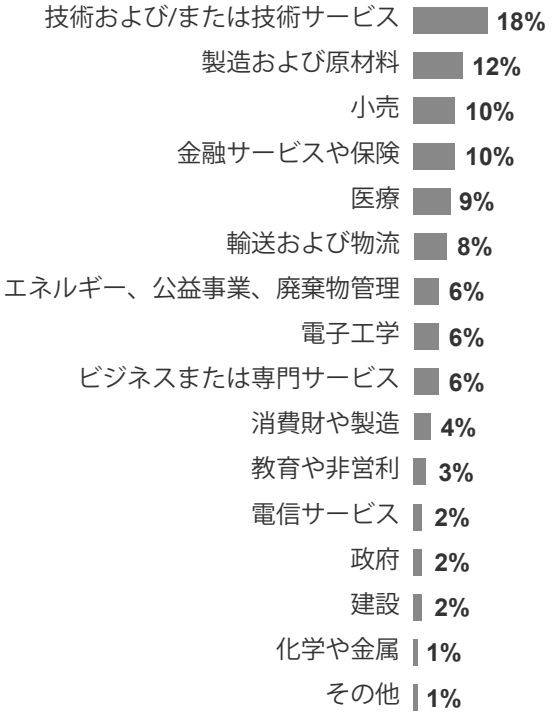

カナダ **10%**


英国 **19%**


仏国 **16%**


独国 **16%**

業種



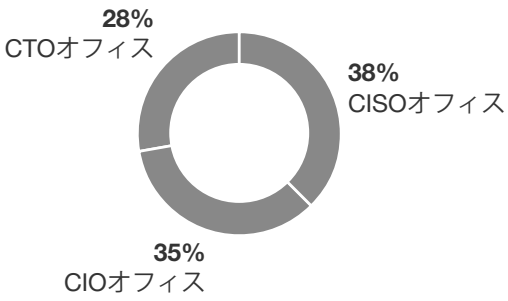
セニョリティ

30% 経営幹部
11% 副社長
60% 取締役

従業員数

40% 500～999人
36% 1,000～4,999人
16% 5,000～19,999人
10% 20,000人以上

部門



調査対象：セキュリティ戦略やセキュリティテクノロジーの購入を担う世界中のセキュリティ担当者200人
注：値を四捨五入しているため合計が100%にならない場合があります。
出典：IBMの委託によるForrester Consulting実施の調査。2019年1月

FORRESTER®

付録C：注釈

[1] 出典：“Security Budgets 2017: Increases Help But Remain Reactionary,”Forrester Research, Inc. 2016年11月23日

[2] 出典：“The Top Security Technology Trends To Watch, 2017,” Forrester Research, Inc. 2017年4月26日

[3] 出典：“The Top Security Technology Trends To Watch, 2017,” Forrester Research, Inc. 2017年4月26日

[4] 出典：“Security Budgets 2019: The Year Of Services Arrives,” Forrester Research, Inc. 2018年12月17日

[5] 出典：“Security Budgets 2019: The Year Of Services Arrives,” Forrester Research, Inc. 2018年12月17日

[6] 出典：“The Zero Trust eXtended（ZTX） Ecosystem,” Forrester Research, Inc. 2018年1月19日

[7] 出典：“The Zero Trust eXtended（ZTX） Ecosystem,” Forrester Research, Inc. 2018年1月19日

[8] 出典：“The Zero Trust eXtended（ZTX） Ecosystem,” Forrester Research, Inc. 2018年1月19日