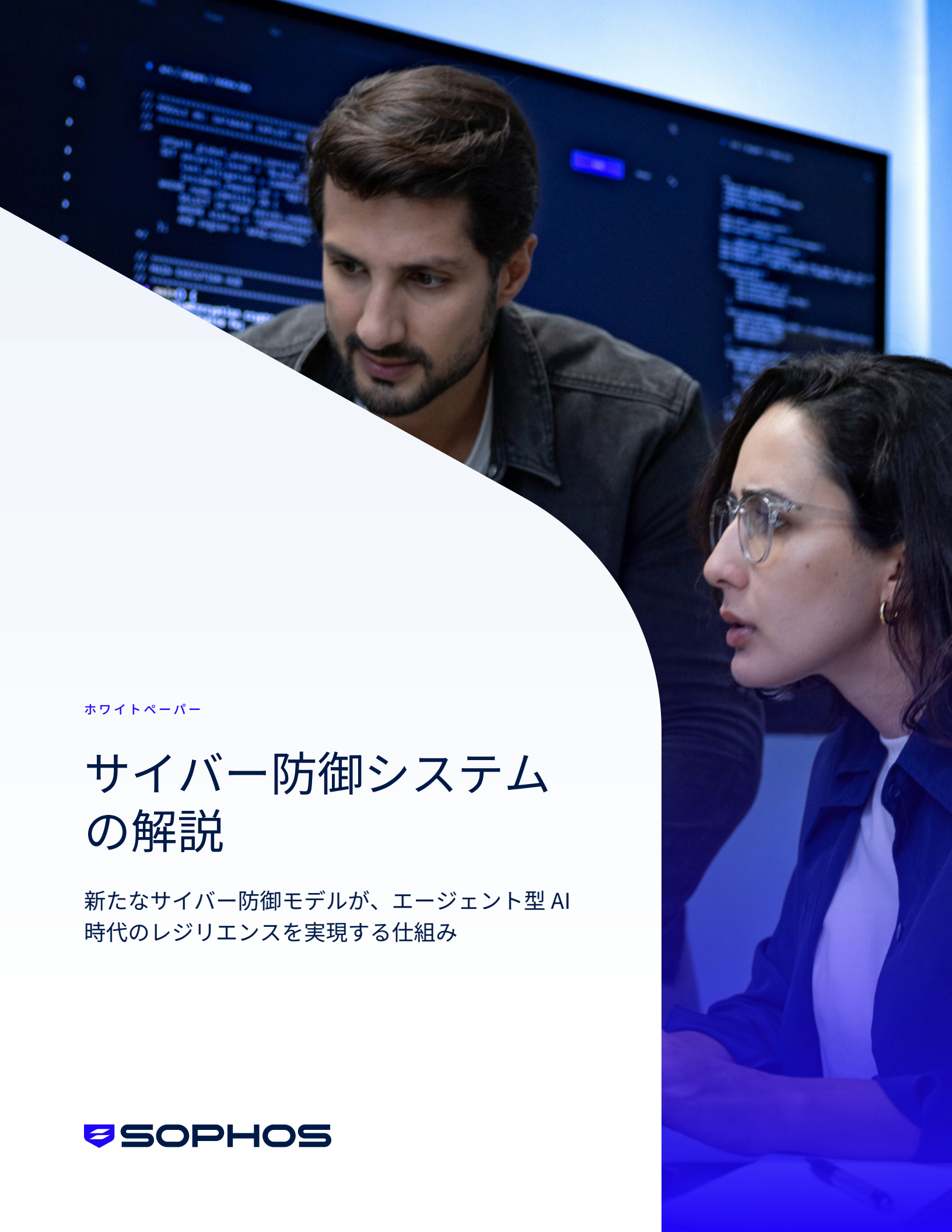


ホワイトペーパー

サイバー防御システムの解説

新たなサイバー防御モデルが、エージェント型 AI 時代のレジリエンスを実現する仕組み

SOPHOS

エグゼクティブサマリー

表面的には、多くの組織でセキュリティ対策は十分に整っているように見えます。長年にわたり、数十種類ものセキュリティ製品を積み重ねてきたからです。しかし、ガートナーによると、「組織は平均して 45 ものセキュリティツールを導入していますが、それらは往々にして個別に運用 (サイロ化) されています。その結果、複雑さや死角、さらには攻撃者に狙われる未把握の脆弱性が生み出されています。」と指摘しています[1]。つまり、ツールが不足しているわけではなく、足りないのは、ツール同士の連携だとソフォスは認識しています。

攻撃者はすでに、ツール間のギャップを悪用し、わずか数分のうちにメール、アイデンティティ、エンドポイント、ネットワークを横断して攻撃を進めます。AI によって、サイバー脅威のスピード、規模、範囲はかつてない速さで拡大しており、高度で多層的な攻撃を広範囲に実行できるようになっています。

現在では、監査機関、規制当局、サイバー保険会社も、断片化したサイバーセキュリティ製品では提示することが難しい、さまざまな証拠を組み合わせた包括的な証跡を求めるようになっています。多くの組織は今なお、自社は十分に保護されているのか、最大のリスクはどこにあるのか、セキュリティへの投資は成果を上げているのか、という 3 つの基本的な問いに明確に答えることができずにいます。

このような環境の中で、AI 時代に自社を守るための新たなサイバー防御モデルが形になりつつあります。セキュリティプラットフォームは、サイバー防御システムへと進化しつつあります。サイバー防御システムの特徴は次のとおりです。

- **あらゆるベンダーの制御ポイントから情報を集約し、**環境全体をリアルタイムに一元的に把握します。
- **メール、アイデンティティ、エンドポイント、ネットワークなど、**複数の制御ポイントにまたがる対応を自動的に連携させます。
- **エージェント型 AI が、現代の攻撃のスピードと規模に対応し、**人間の専門家が AI の行動範囲を定め、その結果に対する責任を担います。
- **新たな知見や、ユーザーベース全体にわたって阻止された脅威から継続的に学習し、**その成果を生かして、あらゆる場所の防御を自動的に強化します。
- **防御の要は、個々の製品から、それらをつなぐアーキテクチャへと変わります。**そこにはテクノロジーのアーキテクチャだけでなく、人間の専門知識を結ぶネットワークも含まれます。

エージェント型 AI 時代の脅威は、すでに始まっている。

2025 年後半、研究者は、人間ではなく主に AI によって実行されたことが確認された初のサイバースパイキャンペーンを確認しました。AI は、この作戦の 80 ～ 90% を自律的に実行したと推定されています。その速度と規模は、人間のチームでは到底及ばないものでした。

出典：Anthropic、2025 年 11 月

サイバー防御システムとは何か

すべての制御ポイントがリアルタイムで情報を共有し、一体となって対応し、継続的に学習しながら、人間の責任のもとでマシンスピードで動作する、統合されたセキュリティアーキテクチャです。

1. *1 出典 Gartner, "Tech FutureSight : Protect the Global Attack Surface With an Autonomous Cyber Defense System," Neil MacDonald, December 12, 2025*

AI 時代におけるセキュリティ上の課題

脅威が発生するたびに、その脅威に対応するための製品を慎重に導入してきた結果、長年の積み重ねによって環境は非常に複雑になり、今やその複雑さ自体がリスクになっています。今や、連携していない製品を積み重ねただけのセキュリティ環境では、AI によって加速する攻撃者に対抗できず、そのスピードについていけなくなっています。なぜこのような状況に陥ってしまったのでしょうか？

プラットフォームアプローチの限界

ほぼすべての大手サイバーセキュリティベンダーが、自社のプラットフォームですべてのニーズに対応できると主張しています。実際には、脅威が発生するたびに個別の製品を導入する顧客向けに、単一のプラットフォームとして連携して機能することを目指したポイントソリューションを販売しています。

統合されたシステムを構築するというプラットフォームの考え方自体は正しい方向を目指していました。しかし実際に販売されているのは、ブームに乗るため、あるいは株価を押し上げるために、急ごしらえされたり買収されたりしたツールを寄せ集めたものにすぎない場合が少なくありません。そして、期待された成果は得られていません。

- **「単一の画面ですべてを把握できる」と主張していますが、**実際の環境では、対応担当者は依然として複数のコンソールを行き来しなければなりません。
- **「データを共有できる」と主張していますが、**プラットフォームを構成する製品は、それらのデータを断続的に分析しているため、アイデンティティ、クラウド、エンドポイントにまたがる攻撃を検知することができません。
- **「統合されている」と主張していますが、**製品ごとに独自のデータモデルを使い続けているため、対応アクションも領域ごとに分断されたままです。

プラットフォームを統合して機能させるための作業、つまり設定やカスタマイズ、すべての製品を連携させて一つのワークフローを構築する作業は、すべて顧客に委ねられています。

Gartner® は、「単にツールをスタックに追加するだけでは、Anthropic 社が最近特定したような AI 主導の攻撃を軽減するために組織が必要とする、インテリジェントなサイバー防御ファブリックを実現することはできない」と指摘しています。

Neil MacDonald
Gartner | VP, Distinguished Analyst and Gartner Fellow Emeritus

Gartner, Tech FutureSight:Protect the Global Attack Surface With an Autonomous Cyber Defense System, Neil MacDonald, 12 December 2025

ドメイン横断型の攻撃が、断片化した防御を出し抜く

プラットフォーム製品でデータモデルや分析が分断されていることは、攻撃者にとって格好の条件となります。以下の攻撃シナリオは、その理由を示しています。

- **ステップ 1：**巧妙なメールが受信トレイに入り込む。
- **ステップ 2：**受信者が偽のサインインページにパスワードを入力する。
- **ステップ 3：**攻撃者が見慣れない場所からログインする。
- **ステップ 4：**攻撃者が気づかれないようにメールボックスにルールを追加し、メールを監視する。
- **ステップ 5:**攻撃者がユーザーのアクセス権を利用してファイル共有にアクセスし、データを外部に持ち出す。

5 つのステップがあり、それぞれ異なるドメインにまたがっています。

- **メール セキュリティ**がメールを検知する。
- **アイデンティティソリューション**が不審なログインを検知する。
- **エンドポイント保護機能が**小さな異常を指摘する。
- **ファイアウォールが**外部への接続をログに記録する。

各製品はそれぞれ担当した部分を記録し、どの製品も技術的には自らの役割を果たしています。しかし、**どの製品も全体像を把握することはできません。**攻撃が進行している間に、それぞれが把握した情報を他の製品と共有していないからです。それぞれが単なるノイズに見え、一つの攻撃シナリオとしては捉えられません。一連の攻撃のつながりが明らかになるのは、手遅れになってからです。

このようなラテラルムーブメントは、現代のサイバー攻撃では珍しくありません。しかし、こうした動きは見落とされることも少なくありません。ソフォスの「ランサムウェアの現状 2026 年版」によると、ファイアウォールが攻撃を検知した場合でも、サイバー犯罪者の 55% がデータの暗号化に成功していることが明らかになっています。

攻撃はマシンスピード、対応は人間の速度

では、先ほどのドメイン横断型の攻撃が、数日ではなく数分で進むとしたらどうなるでしょうか。それを実現したのが AI です。ある製品のアラートに人が気づくのを待ち、別の製品の情報と照合して対応するような防御では、すでに手遅れです。問題なのは、防御側の対応が遅いことではありません。各ツールごとに対応するために、プロセスそのものが遅くなっていることです。手作業に大きく依存するワークフローでは、自動化された攻撃に対応しきれません。オペレーターが対応策を検討し終える頃には、攻撃者はすでに次の段階へ移っています。

専門知識は限られているのに、ノイズはあふれている。

この問題に人員を増して対応するという選択肢も、現実的ではありません。そもそも、人材が不足しているからです。サイバーセキュリティ人材の不足は深刻であり、解消される兆しは見られません。ISC2 が実施した 2025 年のサイバーセキュリティ人材に関する調査によると、95% のセキュリティチームが少なくとも 1 つのスキルギャップを抱えていると回答し、59% がそれを「重大」または「深刻」と評価しました。これは前年の 44% から上昇しています。

その一方で、業務量は増え続けています。少人数のチームが、現実的には到底監視しきれないほど多くの製品、アラート、ダッシュボードを担当することになりかねません。その大半はノイズにすぎませんが、その中に埋もれた本当の脅威の兆候を誰かが見つけなければなりません。

AI はその負担を軽減するはずでしたが、環境によっては、むしろ逆の結果を招いています。

AI をまた別の後付け製品として追加しても、同じ問題が生じます。プラットフォーム内の他の製品とネイティブに連携するよう設計されていないため、ノイズやアラートがさらに増えてしまうのです。今や、サイバーセキュリティチームは誤検知を見極めるだけでなく、AI のハルシネーションにも対処しなければなりません。

サイバーセキュリティに存在する「貧困線」

サイバーセキュリティの「貧困線」とは、このラインを下回ると、組織を効果的に保護することができなくなる境界線です。これは、組織の規模や予算、CISO の有無によって決まるものではありません。実際、十分な予算を持つ組織でも、この水準を下回っているケースは少なくありません。

サイバーセキュリティの「貧困線」とは、戦略的なセキュリティ能力の最低水準です。

組織は、セキュリティテクノロジーを保有しているだけでしょうか。それとも、それらを一つのシステムとして運用できているでしょうか?大規模なチームでも、運用できる専門知識を持つ人材がいないツールに多額の投資をしていることがあります。一方で、規律ある体制を整えた従業員 200 人規模の製造業企業が、はるかに大規模な組織を上回る高度な防御システムを運用しているケースもあります。多くの組織は、セキュリティをシステムとして運用する能力が社内にすでに備わっていると思い込んでいるため、気づかないうちに「貧困線」を下回っています。

こうした組織にとって、最大のギャップはツールの不足ではありません。不足しているのは、明確な戦略と、既存のセキュリティ対策を連携させ、AI によって加速する脅威に一体となって対抗するためのオーケストレーションです。多くの組織は投資を続けているにもかかわらず、依然として次の 3 つの基本的な問いに答えられずにいます。

- 自社は適切に保護されているか?
- 最大のリスクはどこにあるのか?
- 投資は実際に効果を上げているか?

規制当局は、レジリエンスを実証するための証拠をより多く求めている

規制当局やサイバー保険会社が重視するのは、適切な製品を保有しているかどうかではありません。むしろ、組織に次のことを示すよう求めるケースが増えています。

- 複数の領域にわたる協調的な制御。
- 監査可能な証拠の保管。
- 一貫性のある、タイムリーな情報開示。
- 検証された、実環境でのレジリエンス。

こうした新たな規制は、数十もの製品に分散したセキュリティ環境を依然として抱えている組織にとって、大きな負担となります。製品ごとにデータモデルもデータの保存期間も異なるためです。監査人や保険会社から求められる証跡を作成するだけで、フルタイムの仕事になりかねません。別々のシステムからログをエクスポートし、それらを手作業でつなぎ合わせ、最終的に一貫した全体像を示せていることを願うことになります。実証できないセキュリティ対策は、コンプライアンス上、対策として認められません。

共通する要素

こうした問題は、製品をもう一つ増やしたり、コンソールに新しいボタンを追加したりするだけでは解決できません。これらの問題には、共通する根本原因があります。防御は分断されているのに、脅威は連携していています。そのために、防御は破られるのです。このギャップを埋めるには、これまでとは異なるアプローチが必要です。新しい製品をさらに追加することではありません。

サイバー防御システム：セキュリティへの現代的なアプローチ

問題が分断化にあるとしても、ただ統合すればよいというわけではありません。何でもこなそうとして結局うまくいかない 1 つの製品を導入しても、優れた複数の製品がうまく連携できていない状態と何ら変わりません。

組織は、サイバー防御システムを目指すべきです。サイバー防御システムは、セキュリティ製品とサービスを組み合わせ、1 つの統合されたシステムとして機能するよう設計されています。すべての制御ポイントが環境の全体像の把握に貢献し、連携した全体の一部として対応できなければなりません。システムは、緊密に連携し、同期および自動化され、インテリジェントで、適応性を備えている必要があります。それが実際にどのようなものになるのかを、5 つの原則で説明します。

1 同期して自律的に動作する制御ポイント

サイバー防御システムの起点となるのが、制御ポイントです。これらは、セキュリティテレメトリを収集および監視し、セキュリティルールを適用するテクノロジーやサービスです。制御ポイントは、何が起きているかを把握し、それに応じて対応できます。ンドポイント、ファイアウォール、メール、アイデンティティ、生産性ツールなどは、すべて制御ポイントです。

2 リアルタイムで共有する、1 つの全体像

防御システムがプラットフォームと異なるのは、環境全体で何が起きているのかを 1 つの共通認識として把握できる点です。各制御ポイントが捉えた情報を、コピーによる遅延や後からのデータ突合を発生させることなく、リアルタイムで共通のデータレイヤーに取り込みます。これにより、システム全体がイベントをリアルタイムで把握できる、単一の共通ビューが実現します。死角もなければ、対応に漏れもありません。

3 あらゆるレイヤーで連携した対応

連携した対応は、あるレイヤーでの検知を起点に、アナリストがコンソールから別のコンソールへシグナルを伝達しなくても、他のレイヤーで自動的にアクションを起こせることから始まります。

不審なサインインを検知すると、エンドポイントとメールの両方のレイヤーで追加の監視を行うことができます。デバイス上で悪意のあるファイルが検知されると、ファイアウォールやネットワークが、そのファイルが試みる通信をブロックできます。攻撃を一つのものとして捉えるからこそ、システムも一体となって対応できます。そして、攻撃が高速化するほど、こうした連携が重要になります。

4 人間が責任を担う、エージェント型 AI

決め手となるのは、スピードです。数分で展開される攻撃は、人間が異変に気づくのを待つ防御では阻止できません。だからこそ、AI はシステムの周辺に置くのではなく、中核に据える必要があります。

サイバー防御システムでは、AI がアーキテクチャそのものです。後付けするのではなく、最初から組み込まれています。AI は、あらゆるレイヤーのシグナルを相関分析し、攻撃が形を現し始めた段階でその全体像を捉え、検知、調査、対応をマシンスピードで実行します。この AI ネイティブなシステムは、単一の製品に後付けされ、その製品のデータしか把握できない AI とは異なります。

防御システムに組み込まれた AI は、システム全体が捉える情報を横断して推論できます。しかし、人間の責任を伴わないマシンスピードでの対応は、強みではなくリスクになります。サイバー防御システムは、セキュリティにおける人間の役割をなくすものではありません。むしろ、人間の判断が最も重要となる領域に、人の力を振り向けます。具体的には、対応の境界を設定し、未知の脅威や高リスクな判断に対応し、インシデントをレビューし、結果に対する責任を担います。

AI がスピードと規模を支えます。そして、定型的なトリアージや、高速かつ確度の高い対応を担います。

人間の専門家が AI の信頼境界を定めます。つまり、AI が自律的に判断してよい範囲と、人間の判断を仰ぐべき状況を決めます。人間は、未知の状況や、重大な影響を伴う判断が必要な場面で介入します。

システムが信頼を積み重ねるにつれて、その境界を広げることができます。ただし、最終的な責任は常に人間の専門家が担います。

AI がスピードと規模を支えます。

信頼の境界に関わる判断は、人間の専門家が担います。

5 相乗的に進化するインテリジェンス

防御システムは学習します。どこかで検知した脅威が、システム全体の集合知になります。エンドポイントは、ファイアウォールが捉えた情報を把握します。メールゲートウェイは、検知した情報をアイデンティティレイヤーに伝えます。すべてのツールが互いに学び合い、これまでの知識を積み重ねていきます。これらはすべて、手動で設定することなく実現されます。防御システムのインテリジェンスは、ユーザー数と観測するパターンが増えるほど相乗的に強化され、AI による攻撃と同じ速さで進化できるようになります。

プラットフォームからサイバー防御システムへ

この 5 つの原則を備えることで、独自のカテゴリが形成されます。防御システムは、AI 時代に最適化されたプラットフォームの進化形です。プラットフォームとは通常、共通のコンソールから複数の製品を利用できるようにしたもので、製品同士を設計段階から統合するのではなく、共通のログインとライセンス契約でつないでいるにすぎません。

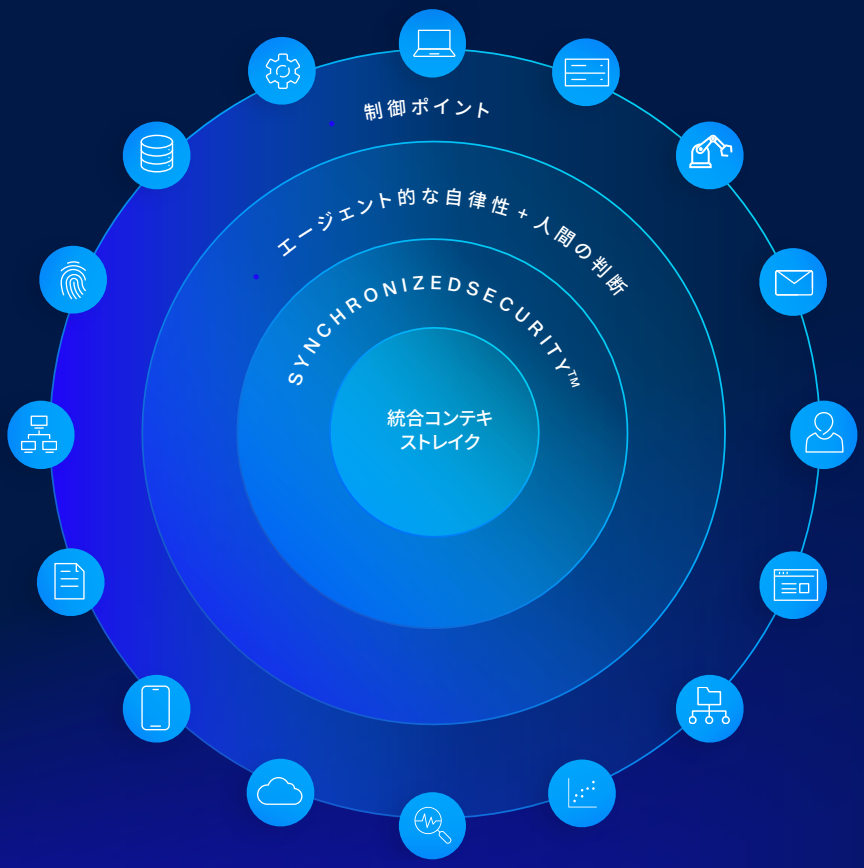
サイバー防御システムはプラットフォームとは異なります。データを共有し、AI を組み込み、対応を連携させ、人間の専門家が主導権を握ります。複数の製品を一つに見せるために組み合わせたものではなく、1 つの製品として機能するよう設計されたアーキテクチャです。

Sophos Fusion：ソフォスのサイバー防御システム

Sophos Fusion は、脅威が AI のスピードで進行する世界を想定して設計された、業界で最も包括的なサイバー防御システムです。Sophos AI-Native Cybersecurity Defense System のアーキテクチャと 500 以上のソフォスおよびサードパーティシステムとの統合により、あらゆる情報を可視化し、あらゆる要素をつなぎ、防御を 1 つのシステムとして機能させます。

Sophos Fusion は、サイバー防御システムの原則を実践に移します。単一のオープンなアーキテクチャのもとで、すべての制御ポイントが一体となって機能し、エージェント型 AI がそれを支えます。そして、人間の判断を組み合わせることで、攻撃者が防御側の対応を上回るスピードで仕掛ける AI を利用した脅威から組織を守ります。

お客様がソフォスのポートフォリオをより多く活用するほど、Sophos Fusion が提供する価値も高まります。



すでに所有している各制御ポイントは、リアルタイムの脅威インテリジェンスを継続的に提供し、対応アクションを実行します。このアーキテクチャは完全にオープンです。ソフォス製品だけでなく、500 以上のサードパーティテクノロジーともネイティブに統合できるため、すでに導入している製品への投資を、孤立させることなく、連携した統合型の防御の一部として活用できます。

また、市場でも最も深いレベルの Microsoft セキュリティ統合を実現しており、最上位プランだけでなく、Microsoft のすべてのプランに対応しています。そのため、エントリーレベルの Microsoft ライセンスを利用している組織でも、そのテレメトリを活用して防御を強化できます。

リアルタイムで共有する、1 つの全体像

すべての制御ポイントから得られるテレメトリが、統合されたコンテキストレイクにリアルタイムで流れ込みます。このコンテキストレイクは、すべての制御ポイントで共有される単一のデータレイヤーです。データの集約による遅延はなく、各制御ポイントに個別のデータストアを置く必要もありません。これは、共有される神経系のようなものです。すべての制御ポイントが、他のすべての制御ポイントが捉えた情報を、発生した瞬間に把握します。この共通認識こそが、連携を可能にします。

あらゆるレイヤーで連携した対応：Synchronized Security ™

Synchronized Security ™ は、Sophos Fusion 全体で共有された共通認識を、連携したアクションへとつなぐ役割を果たします。ソフォス製品とソフォス以外ベンダーの制御ポイントが、脅威に対して自動的に連携して対応できるようにします。

エンドポイントで検知された脅威が、ファイアウォールでの対応アクションをトリガーすることがあります。アイデンティティが侵害された場合、環境全体へのアクセスをロックダウンすることもできます。不審なメールが届いた場合、あらゆる段階で監視を強化することができます。ソフォスのソリューションを多く導入するほど、Synchronized Security ™ のメリットをより多く享受できます。

現代的な建物の消火システムをイメージしてください。ある部屋のセンサーは、警報を鳴らすだけではありません。防火扉を閉じ、空調の気流を切り替え、近くの階のスプリンクラーを作動させます。Sophos Fusion も同様に、連携した一つのシステムとして機能します。これが可能なのは、データがすでに統合されているからです。追加の設定や操作は必要ありません。

人間が責任を担う、エージェント型 AI

Sophos Fusion は、マシンスピードで検知、調査、対応を行います。ただし、人間による監督なしに実行することはありません。すべてのアクションは、人間の専門家が定め、継続的に調整する境界の範囲内で実行されます。これこそがエージェント型 AI です。固定されたプレイブックに従うだけでなく、新たな状況を推論して対応できる AI です。

これは、航空機のオートパイロットに例えると分かりやすいでしょう。システムが航空機を操縦しますが、パイロットは飛行条件を設定し、計器を監視し、想定外の状況に遭遇したりリスクの高い状況が発生したりした場合には操縦を引き継ぎます。

Sophos Fusion では、このエージェント機能を、ソフォスネイティブのエージェント型 AI である Fusion AI が提供します。ソフォスの防御機能には 50 以上の AI モデルが組み込まれており、すべてのモデルがリアルタイムの脅威インテリジェンスによって継続的に改善されています。例えば、Sophos Email では 20 種類以上のモデルが使用されています。その中には、メールのテキスト、トーン、文脈、構造を分析して、フィッシングやビジネスメール詐欺 (BEC) を特定する、独自開発の自然言語処理 (NLP) モデルも含まれています。

Sophos MDR は、ソフォスの専門家がお客様に代わって監視と対応を行う 24 時間 365 日のサービスであり、ソフォスのサイバー防御システムを使用して世界最大のエージェント型 SOC (セキュリティオペレーションセンター) を運用しています。業界最大規模の MDR (Managed Detection and Response) を運用しており、4 万以上の組織を保護しています。AI によってインシデントの 52% をエンドツーエンドで解決しており、アラートから自動対応までの平均時間は 89 秒です。一方で、組織にリスクをもたらす判断については、人間の専門家が引き続き責任を担います。

相乗的に進化するインテリジェンス

ソフォスのサイバー防御システムは、自社への攻撃だけでなく、あらゆる攻撃から学習します。ソフォスが保護する 62 万 5,000 以上の組織で遭遇したあらゆる脅威が、アナリストが解決したすべての例外的なケースや、新たに稼働を開始した環境から得られる情報とともに、Sophos Fusion にフィードバックされます。Sophos X-Ops は、こうした仕組みを、独自の高度な専門知識とリアルタイムの脅威インテリジェンスによってさらに強化します。得られた情報は、すべてのソフォス製品とすべてのお客様に自動的に提供され、防御機能の向上に役立てられます。

これは、生体の免疫システムとよく似た仕組みです。身体が遭遇した脅威は、そのすべてが恒久的な記憶として蓄積され、記録・理解され、次に現れたときに備えられます。Sophos Fusion も同様に動作します。新しいお客様は、これまで遭遇したことのない脅威からも導入初日から保護されます。システムはすでにその脅威を知っているからです。

だからこそ、62 万 5,000 以上という数字には大きな意味があります。これは、防御とインテリジェンスを相乗的に強化する、幅広い経験の蓄積を示しています。システムがより多くの脅威を捉えるほど、システム内のすべての組織をより効果的に守れるようになります。

Sophos Fusion：サイバー防御システムを体験できる場所

Sophos AI-Native Cybersecurity Defense System こそが、そのアーキテクチャです。Sophos Fusion は、それを実際に体験できる場所です。ソフォスの制御ポイントを一元管理し、接続されたすべての制御ポイントから得られる情報を 1 つの全体像として把握し、対応を実行できます。

つまり、追加の製品を購入したり有効化したりする必要はなく、現在の業務の進め方を変える必要もありません。すべてのソフォスの制御ポイントは、すでに Sophos Fusion の一部です。つまり、いずれか 1 つを導入した瞬間から、このアーキテクチャの中で運用できます。ソフォスやサードパーティの制御ポイントを追加するほど、システム全体の機能がさらに活性化し、共有される情報も拡充されます。その結果、すでに運用している環境全体で、より大きな価値が生まれます。

Sophos Fusion から見た攻撃

ここで、先ほどの多段階攻撃の例に戻りましょう。悪意のあるメール、窃取された認証情報、通常とは異なるサインイン、メールボックスの転送ルール、そして機密データへのラテラルムーブメントが実行されていました。Sophos Fusion では、Sophos Email とお客様の Microsoft 環境から得られるテレメトリが、統合されたコンテキストレイクに流れ込みます。Sophos XDR は、これらのシグナルを受信するとすぐに相関分析し、5 つの無関係なアラートとしてではなく、1 つのつながった攻撃として一連の動きを認識します。

そこから、Synchronized Security ™ は、メール、アイデンティティ、エンドポイント、ネットワーク全体にわたる対応を調整します。エージェント型 AI はマシンスピードで動作する一方、Sophos MDR のアナリストは直接行動し、リスクの高い判断を下します。個々の製品が孤立していれば見逃しかねない攻撃も、全体像を把握するシステムなら見逃しません。

Sophos Fusion が組織にもたらすもの

Sophos Fusion は、ビジネスにとって重要な 4 つの領域で、エージェント型 AI 時代のサイバーレジリエンスを実現します。

- **防御側の対応を上回るスピードで進化する、AI によって加速された脅威から組織を保護します。**AI が攻撃のスピードと規模を加速しても、すべての制御ポイントがコンテキストを共有し、それぞれが単独で対応するのではなく連携して動くことで、多段階攻撃を早期に検知して封じ込めます。

- **人材と投資の価値を最大化します。**エージェント型 AI によって、ノイズが吸収され、トリアージおよび対応に関する日常的な業務が行われるため、人員を増やすことなく、複雑化も回避しながら、既存のチームや制御ポイントによってより多くの成果を達成できます。ソフォス製品でもソフォス以外の製品でも、接続されるすべてのツールが、一体となって防御を支援します。

- **コンプライアンスとサイバー保険への対応力を強化します。**24 時間 365 日の監視、レイヤー間のコンテキスト保持、連携対応といった機能が、監査人、規制当局、保険会社が求める証跡を、手作業でログをエクスポートして集めるのではなく、検索可能な 1 つのレコードから提示できます。つまり、防御力を高めるためのアーキテクチャが、証明にも役立ちます。

- **ビジネスに合わせたサイバーセキュリティ戦略**防御をつなぎ合わせて連携させることで、Sophos Fusion は、個々のダッシュボードを管理するだけの運用から、組織全体の防御状況を把握し、確信を持ってセキュリティを運用できる状態へと導きます。どこに防御のギャップや最大のリスクがあるのか、そしてセキュリティへの投資が実際に効果を上げているのかを明確に把握できます。CISO がいる組織でもいない組織でも、規模を問わず、これまで描いてきたセキュリティ戦略をついに実行できるようになります。

ソフォスの顧客はすべて、ソフォスの防御システムである Sophos Fusion にすでに参加しています。自動かつシームレスにアップグレードされ、AI 時代の脅威から組織を守ります。

Sophos Fusion の導入について

すべてのソフォスソリューションは Sophos Fusion の一部であり、単独で完結するツールではなく、統合された防御システムへの入口となります。ソフォスの製品やサービスを 1 つ導入するだけで簡単に利用を開始できます。Sophos MDR、Sophos XDR、Sophos Endpoint、Sophos Firewall、Sophos Email など、いずれかの製品やサービスから始められます。ソリューションを追加すればするほど、アーキテクチャの可能性が広がります。

現在ご利用いただいている他のサードパーティの制御ポイントを変更する必要はありません。これらを Sophos Fusion に統合することで、継続的なリアルタイムの脅威インテリジェンスを提供し、対応アクションを実行できます。最もリスクの高い領域から導入し、自社のペースで拡大してください。

今すぐ始めましょう。まずはソフォスのエキスパートにご相談ください。お客様の環境に最適な始め方をご提案いたします。また、sophos.com/fusion で詳細をご覧ください。

まとめ

長年、新たな脅威が現れるたびに別の製品を追加することが、当たり前になっていました。その結果生まれた分断を、今では攻撃者が悪用しています。AI によって、この問題はさらに深刻になっています。攻撃の進行速度と、コンソールごとに個別対応する方法で追いつける速度との間のギャップが、ますます広がっているためです。製品を増やしても、そのギャップは埋まりません。サイバー防御システムなら、そのギャップを埋められます。

サイバー防御システムは、防御の単位を個々の製品から、それらをつなぐアーキテクチャへと変えます。

- 一元化されたビュー
- あらゆるレイヤーで連携した対応
- マシンスピードで動作するように設計された AI
- 人間の専門家が判断と責任を担う

AI 時代のセキュリティとは、すでに導入しているすべての製品を一体となって機能させることです。Sophos AI-Native Cybersecurity Defense System である Sophos Fusion なら、現在導入している製品を置き換えることなく、このモデルを実際の防御に取り入れることができます。

AI 時代におけるサイバー防御のニーズについてぜひご相談ください。

ソフォスの専門家にご相談ください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp