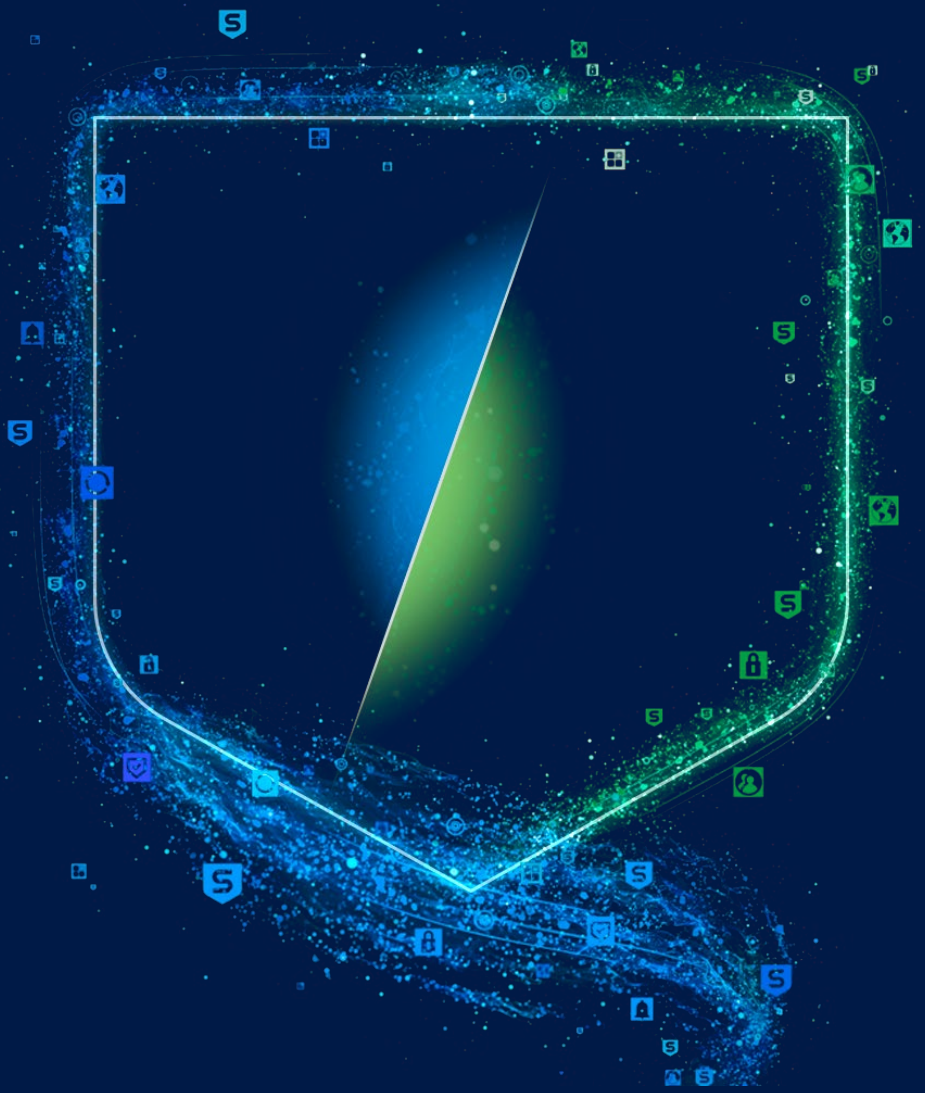
SOPHOS

AI を取り入れた
ソフォスのサイバー防御ソリューション

ソフォスは、適応型の AI ネイティブプラットフォームから、AI テクノロジーと人間の専門知識を組み合わせた、実環境で成果が実証された堅牢な製品とサービスを提供しています。



SOPHOS

ソフォスは 2017 年以来、サイバーセキュリティにおける AI の限界に挑戦し続けており、AI テクノロジーと人間のサイバーセキュリティの専門知識を組み合わせ、あらゆる場所で発生する幅広い脅威を防いでいます。セキュリティアナリストはより迅速に優れた判断を下すことができ、組織はソフォスの堅牢で実績のある AI ソリューションに常に守られながら、自信をもってセキュリティを運用できます。

ディープラーニングと生成 AI の機能は、ソフォスのソリューションに組み込まれており、業界最大の AI ネイティブプラットフォームを通じて提供され、お客様の最も重要な課題を解決します。ソフォスの適応型 AI ネイティブプラットフォームは、60 万社以上のさまざまな顧客環境における攻撃データに基づいて訓練されており、ソフォスの顧客のために比類のない防御機能を提供し、防御力を強化します。

AI の能力

AI は、規模や目的が異なるさまざまなテクノロジーを幅広く網羅しています。Microsoft Copilot や Google Gemini のような生成 AI モデルが注目されることが多くありますが、これらは AI 全体の一端を担っているに過ぎません。
ソフォスでは、進化するサイバーセキュリティに迅速に対応するため、幅広い AI モデルを使用しています。

タイプ

ディープラーニング AI（適用）

人工ニューラルネットワークを使い、人間の脳を模倣した方法でパターンを認識し、意思決定を行います。学習した内容を適用してタスクを実行します。

例：

ソフォスの URL セキュリティモデル
悪意のある URL、フィッシングサイト、その他の Web 関連の脅威を検出します。

展開される製品：
Sophos Endpoint、Sophos Firewall、Sophos Email、Sophos Mobile

生成 AI（作成）

既存のデータ構造やパターンに基づいて、まったく新しいコンテンツを生成します。

例：

Sophos AI ケースサマリーツール
脅威の活動をわかりやすくまとめ次のステップを推奨します。

展開される製品：
Sophos XDR と Sophos MDR

規模

大規模 AI モデル

ユーザーの幅広いタスクを支援します。

例：

Microsoft Copilot、Google Gemini
これらの大規模言語モデル (LLM) は、非常に幅広いユーザーのタスクを支援できます。これらのモデルは一般に公開されている膨大な量のデータに基づいて訓練されています。

小規模 AI モデル

特定のユースケースのために設計、訓練、構築されています。

例：

ソフォスの Android DL モデル
Android に特化したマルウェアを検出するために、ソフォス独自の Android データを使用して訓練されています。

展開される製品：
Sophos Mobile

防御のあらゆるポイントで AI を活用

ソフォスのソリューションには、50 種類以上 (現在も拡大中) のディープラーニングと生成 AI モデルが搭載されており、サイバー脅威がどこで発生しても組織をすばやく効果的に保護します。AI を活用したソフォスのサイバーセキュリティソリューションは、脅威にさらされるリスクを軽減し、脅威を自動的に阻止し、セキュリティアナリストが迅速かつ正確な判断を下せるように支援します。

ソフォスの製品およびサービスにおける AI の活用例

脅威リスクの軽減
脅威にさらされるリスクの軽減

Sophos Managed Risk
Tenable の脆弱性優先度評価 (VPR) の AI モデルを使用し、28 日以内に CVE が攻撃される可能性を予測します。

脅威の自動防止
攻撃の実行を阻止

Sophos Endpoint
複数のディープラーニングモデルによって、Microsoft Office ソリューション、PDF、リッチテキスト形式 (RTF) ファイルの脅威など、既知の攻撃や未知の新たな攻撃から保護します。

Sophos Firewall
AI を活用したゼロデイ脅威のインテリジェンスを SophosLabs Intelix から提供します。

Sophos Endpoint と Sophos Firewall
Web プロテクションモデルが、悪意のある URL、フィッシング Web サイト、その他の Web 関連の脅威を検出します。

Sophos Email
ディープラーニングを活用した自然言語処理 (NLP) によってなりすましを特定します。

Sophos Mobile
Android DL モデルは、Android に特化したマルウェアを検出するために、ソフォス独自の Android データを使用して訓練されています。

ハンティング、調査、対応
脅威を特定して無効化

Sophos XDR と Sophos MDR
AI が生成する脅威スコアは、アナリストが時間と労力を優先的に費やすべき脅威を特定するのに役立ちます。

Sophos XDR、Sophos MDR
AI ケースサマリーは、検出した脅威の概要を明確に示し、次に実施すべき対策を推奨します。

Sophos MDR
AI を活用したケーストリアージによって調査を迅速に進め、重複するケースを除外できます。

Sophos XDR と Sophos MDR
AI コマンド解析は、検出された脅威に関連するコマンドを調査し、攻撃者の行動に関する洞察を提供します。

Sophos XDR と Sophos MDR
AI 検索は、アナリストが自然言語を使用してデータを検索し、調査をスピードアップします。

ソフォスの適応型 AI ネイティブプラットフォームを通じて提供されます。

Sophos Central は AI ネイティブの適応型プラットフォームであり、比類のない保護機能を提供し、防御者の能力を強化します。動的な防御、実環境における優れた効果が実証されている AI、さまざまな製品やサービスと統合できるオープンなエコシステムが、業界最大のソフォスの AI ネイティブプラットフォームに集約されています。

Sophos Central

動的

- 保護機能は、世界中の 60 万社以上の多様な顧客環境で検出された攻撃から収集された脅威インテリジェンスに基づいて常に更新されます。
- 適応型の防御が、自動的に脅威に対応します。
- AI モデルは、300 名のセキュリティオペレーションを専門とするスタッフからリアルタイムでインプットを取り込みながら、継続的に強化されています。

オープン

- ソフォス製品、他のベンダーの製品、またはそれらの両方の組み合わせに対応し、複数の OS 環境にわたって動作します。
- 一元化されたデータと統合されたワークフローにより、セキュリティタスクが最適化され、ユーザーの生産性を向上して、セキュリティの成果を迅速に達成します。

業界最大

- 広範なテレメトリの活用：世界中のさまざまな規模と業種の 60 万社以上の顧客に対する攻撃から得られたテレメトリを活用します。
- 詳細なデータの活用：ソフォスやソフォス以外のテクノロジーおよび Windows、iOS、Linux OS を実行するデバイスのデータなど、IT 環境全体のデータを使用します。

相乗効果：人間の専門知識と AI テクノロジー

AI を活用したサイバーセキュリティソリューションの中核では、ソフォスの従業員が重要な役割を担っており、開発プロセスのあらゆる領域で専門知識を発揮しています。

- 部門横断的なタスクフォースである Sophos X-Ops は、**脅威やサイバー攻撃者の行動について深い知識を持っており、**AI が最も効果的となる方法とタイミングを特定できるように支援しています。
- Sophos の AI チームは、**AI の豊富な専門知識**を活用し、サイバーセキュリティに特化した 50 以上の AI モデルを設計、構築、維持しています。
- ソフォスは、30 年以上にわたって**サイバーセキュリティ工学の領域で専門知識を蓄積しており、**AI モデルをソフォス製品およびサービスに緊密に統合し、安全に機能を展開しています。

AI の導入から得た知己は人間の専門知識をさらに向上させ、AI モデルの継続的な改善、新たな応用分野の特定、ソフォスのテクノロジーの進化を可能にします。

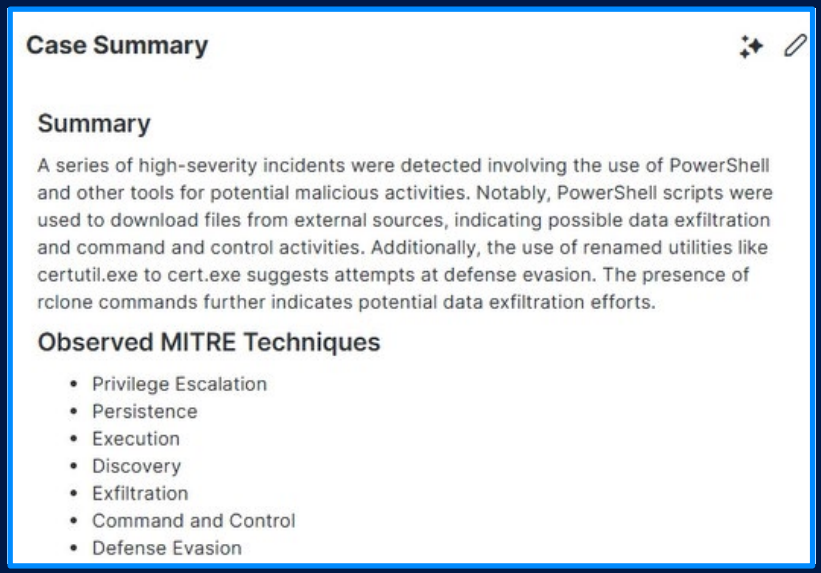
Sophos AI ユースケース

生成 AI によるセキュリティオペレーションの加速

Sophos Extended Detection and Response (XDR) の生成 AI はセキュリティアナリストにとって頼れるツールであり、攻撃をすばやく無効化するために役立ち、アナリストと企業の両方の自信を高めます。

- **AI ケースサマリー**は、検出の概要や推奨の対応方法などをわかりやすく示し、アナリストの迅速かつ的確な判断を助けます。
- **AI コマンド解析**は、悪意の下で実行されている可能性があるコマンドを調査し、攻撃者の行動に関する洞察を提供します。
- **AI 検索**は、自然言語検索を使用して、日々の作業効率を高めるとともに、技術的に高度な知識がない場合でも的確なセキュリティオペレーションを実行できるように支援します。
- **AI ケースアシスタント**は、アナリストがケースを処理する際にサポートとアドバイスを提供し、熟練したアナリストも経験の浅いアナリストも同じように、サイバー攻撃を迅速に無力化できるように支援します (2025 年第 1 四半期提供予定)。

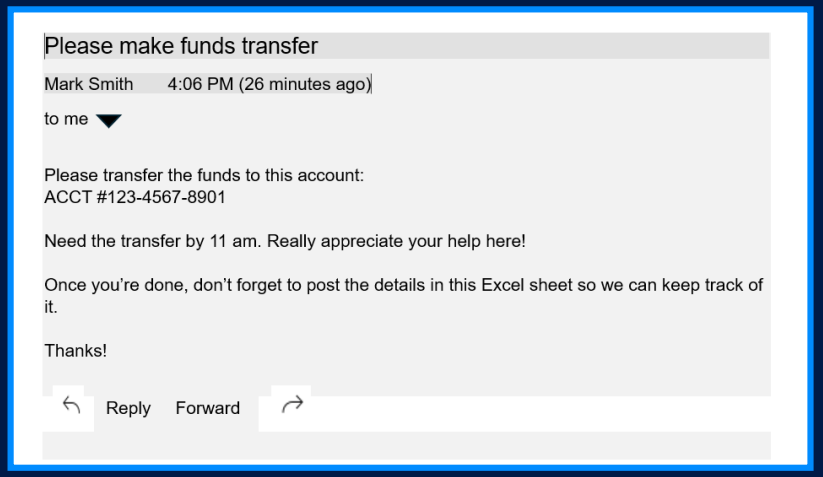
ソフォスの生成 AI の機能は、オプトイン方式で利用できるため、自社で完全にコントロールすることができます。



ディープラーニングによるビジネスメール詐欺 (BEC) の阻止

Sophos Email では、ディープラーニングを活用した自然言語処理 (NLP) が使用されており、詐欺メールやフィッシングメールが正規のメールのように装って、ユーザーを騙す「なりすまし」を特定します。

Sophos Email は、AI を使用してメールの件名と本文のトーンと文言の両方を分析し、詐欺が疑われる会話を特定します。なりすましの試みは自動的にブロックされ、攻撃が防止され、管理者に通知されます。



豊富な経験から生まれる信頼

ソフォスは 2017 年からサイバーセキュリティを加速させるために AI を積極的に活用し、成功を収めてきました。ソフォスが提供する AI はお客様の組織にリスクではなく利益をもたらすことができ、お客様は自社のビジネスに注力できます。

リスク	ソフォスのアプローチ
AI への投資で約束された利益を得ることができない。	**成果重視の AI** ソフォスは AI に関する専門知識を長年にわたって蓄積しており、実環境で優れた成果を発揮させる方法を熟知しています。
AI ソリューションの開発、訓練、展開の方法が不十分である場合、深刻な損害を引き起こす可能性がある。	**セキュリティファーストのプロセス** ソフォスは堅牢な開発プロセスを採用しており、お客様は安心してソフォスの AI を利用できます。
ベンダーは AI そのものに焦点を当てており、AI がもたらす利益には注力していない。	**実世界で発揮される利点** 実環境で優れた成果を実証しているソフォスの堅牢な AI ソリューションは、脅威を迅速に無力化し、アナリストが適切な判断を下せるように支援し、大きな違いをもたらします。

ソフォスの AI チーム

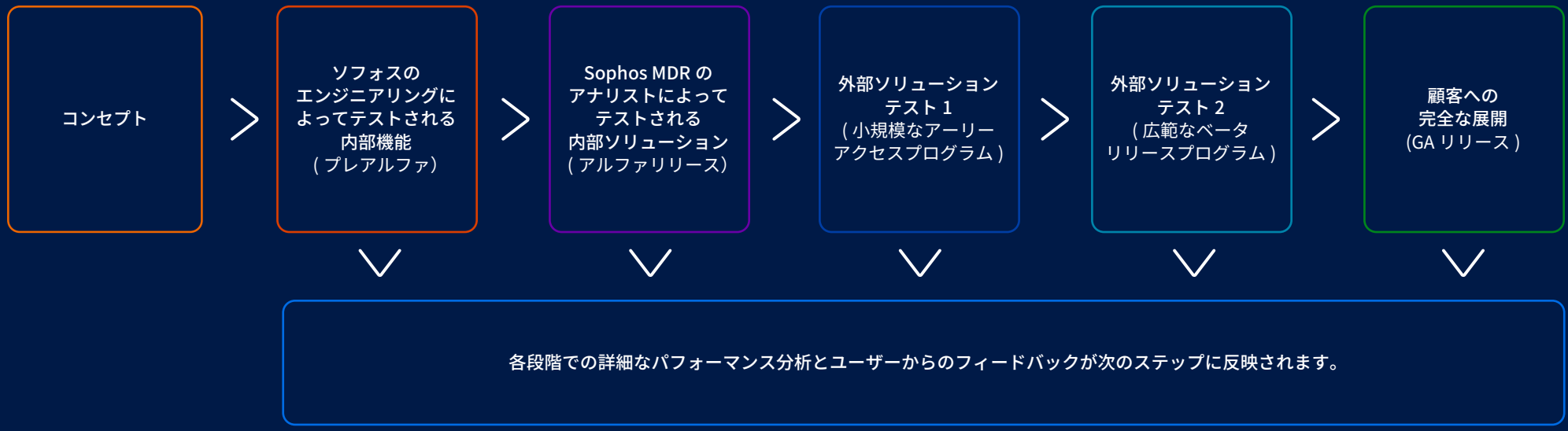
ソフォスの AI チームは、AI を活用してサイバーセキュリティの成果を加速する方法に習熟した専門家から構成されています。この専門的なグローバルなグループは、主に以下の 2 つの分野に主に取り組んでいます。

- AI の開発とソフォスのソリューションでの応用
- サイバーセキュリティのための AI を進歩させる新たな研究

ソフォスの AI チームは、レポートを公開したり、イベントを開催したりして、研究成果を広く共有しています。Sophos AI ブログのサイトで最新の発行物をご覧ください。

堅牢で生成 AI の開発プロセス

サイバーセキュリティのための生成 AI には大きな利点がありますが、同じように危険性も潜在しています。ソフォスは、生成 AI ツールのコンセプトの作成から完全な導入に至るまで厳格なプロセスを採用しています。各段階での詳細なパフォーマンス分析とユーザーからのフィードバックは、開発プロセスの次のステップに反映されています。



AI の誇大宣伝に
惑わされない

AI を活用したソフォスのサイバーセキュリティソリューションの詳細と、
自社の目標達成にこれらのソリューションがどのように役立つのかについては、
www.sophos.com を参照いただくか、ソフォスのパートナーまたは担当者にお問い合わせください。

SOPHOS

2025-01-14 SG-EN (MP)