SOPHOS
Cybersecurity evolved.

# Sophos Adaptive Cybersecurity Ecosystem

Sophos Adaptive Cybersecurity Ecosystem (ACE) は、予防、検出、対応を最適化するために構築された幅広いシステムです。このシステムは、相互接続したビジネスシステムであるこの新たな現実を保護し、自動化と実際の人間によるハッキングを組み合わせた変化するサイバー攻撃の状況から保護します。

Sophos ACE は、自動化と解析、さらにソフォス製品、パートナー、顧客、開発者からの総合的な情報を活用して、継続的に改善する保護を提供します。常に学習し、改善することで、好循環を生み出します。最大の特長は小規模構成からはじめて、拡張できる点です。まず、ソフォスのエンドポイントまたはファイアウォールテクノロジーを導入し、その後、その上に築き上げていくことができます。

ソフォスホワイトペーパー2021年 5月

# 変遷する状況

サイバーセキュリティが運用される状況は常に進化しており、近年、ビジネス環境と攻撃の特徴の両方に大きな変化が生じています。

## ビジネスの変遷：相互接続性

生産性と効率性を向上させる方法を常に模索するなかで、組織は相互接続したサプライチェーン、およびそれを支えるインフラとテクノロジーを構築してきました。データとアプリケーションをクラウドに移行することで、場所を問わず業務を遂行できること、運用コストの削減、パフォーマンスと拡張性の向上など多くのメリットが提供されました。同時に、グローバルなデジタルサプライチェーンの成長を促進しています。

それと並行して、新型コロナウイルスの影響で在宅業務やリモートワークが急速に浸透し、その結果、組織の境界に関する従来の見解が破綻しました。従業員、アプリケーション、デバイス、データが、どこにでも存在するのが現状です。

このような相互接続し、分散したシステムは大きなメリットをもたらしますが、セキュリティ上の新たな課題も発生しています。多くの組織は、社内のネットワーク範囲を把握するのに苦戦し、接続されているシステムすべてを保護することはもちろん困難に感じています。

高性能かつ適応型の攻撃は、最小限の努力でスケールする機会を求めて、このようなシステムを何度もターゲットにします。他にも例はありますが、これを証明したのは 2020年 12月に発生した SolarWinds 攻撃です。この攻撃は、主要テクノロジーベンダーや小規模企業から、最高レベルの公共機関に及ぶまで、広範囲の組織に被害を与えました。

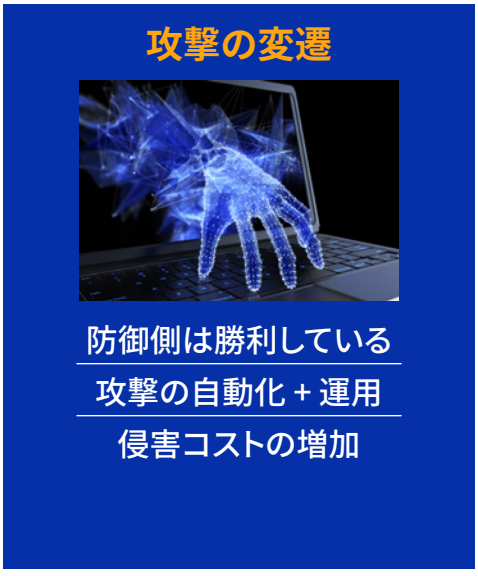

## 攻撃の変遷：自動化から運用へ

サイバーセキュリティ業界に身を置いていると、「重要なシステムやデータをめぐる戦いでは、防御側が勝利している」という重要な事実を見落としてしまいがちです。

新しいセキュリティ侵害を報告する日々のニュースの見出しは、予防措置を講じ、警戒を怠らずに注意することを警告する重要な役割を果たします。しかし、このようなニュースは例外です。毎日何千ものセキュリティ侵害から身を守ることに成功している企業が、ニュースに取り上げられることはありません。

サイバーセキュリティの有効性が劇的に向上しただけでなく、最新のツールやマネージド セキュリティ サービスはより簡単にアクセス可能で、コスト効率もこれまで以上に向上しています。ランサムウェア対策、エクスプロイト対策、動作検知、フィッシング対策などのテクノロジーは、誰もが利用できます。

これらの機能は、AI と機械学習によって促進、改善、加速化され、MITRE ATT&CK フレームワークに記載されている既知の攻撃戦術、手法、手順に対応しています。また、未知の新しい攻撃にも対処します。セキュリティホールやパスの閉鎖、手法のブロックなど、対策の改善によって、非常にコストがかかる攻撃もあり、適応するために攻撃者は手段の変更を余儀なくされています。セキュリティ機能は大幅に改善されたため、「攻撃者は 1回正しければよい」という古い格言はもはや通用しません。攻撃者は収益を得るために、1回の攻撃中に何度も正しい選択をする必要があります。



実際、自動化されたマルウェアから、自動化と実践的なハッキングを組み合わせた、より包括的なアプローチに移行しています。攻撃者の主な目的は、検出されない状態を維持することで、そのためには、ローカルツール、ローカルデバイス、および典型的なトラフィックパターンを使用して、従業員のように行動することが最善の方法です。

このような高度な攻撃には多大な人的投資が必要であり、同時に被害者側にとってもよりコストがかかります。攻撃者は、被害者の環境に関する深い知識を悪用して、最大限の損害をもたらすことができ、最大限の利益を得ることができます。

## IT セキュリティのセキュリティ運用への移行

このようなビジネスの変遷と攻撃の変遷によって、IT セキュリティの進化が必要となります。組織が直面するインテリジェントな攻撃者は、常に調整しながら目標に向かって進んでおり、IT セキュリティチームは、勝利の可能性を高める対策を講じる必要があります。

まず、**セキュリティ管理からセキュリティ運用へ**の変革的な移行が必要です。セキュリティポリシーを「設定して忘れてしまう」時代は終わりました。攻撃者がキーボードで実際に攻撃を操作するようになるなか、IT セキュリティチームも同様にアナリストの力を活用し、疑わしい動作やイベントを追跡・検出して侵害を未然に防ぐ必要があります。


セキュリティチームは、攻撃チェーンのできるだけ早い段階で疑わしいアクティビティを検索して、防御側が被害を受ける前に対応できるようにする必要があります。ステルス攻撃でさえ攻撃の痕跡を残すので、セキュリティチームは、早い段階で攻撃を阻止するために、そのトレイル検出し、追跡する必要があります。もはや、膨大なデータの中から疑わしい痕跡を検出することだけではなく、強力なシグナルになる前に、重要な攻撃の弱いシグナルを特定することが重要になっています。シグナルが強いほど、侵害の発生する可能性が高くなります。適切なツールを使用することで、攻撃者が検出して悪用する前に、IT の問題を事前に検出して修復できます。

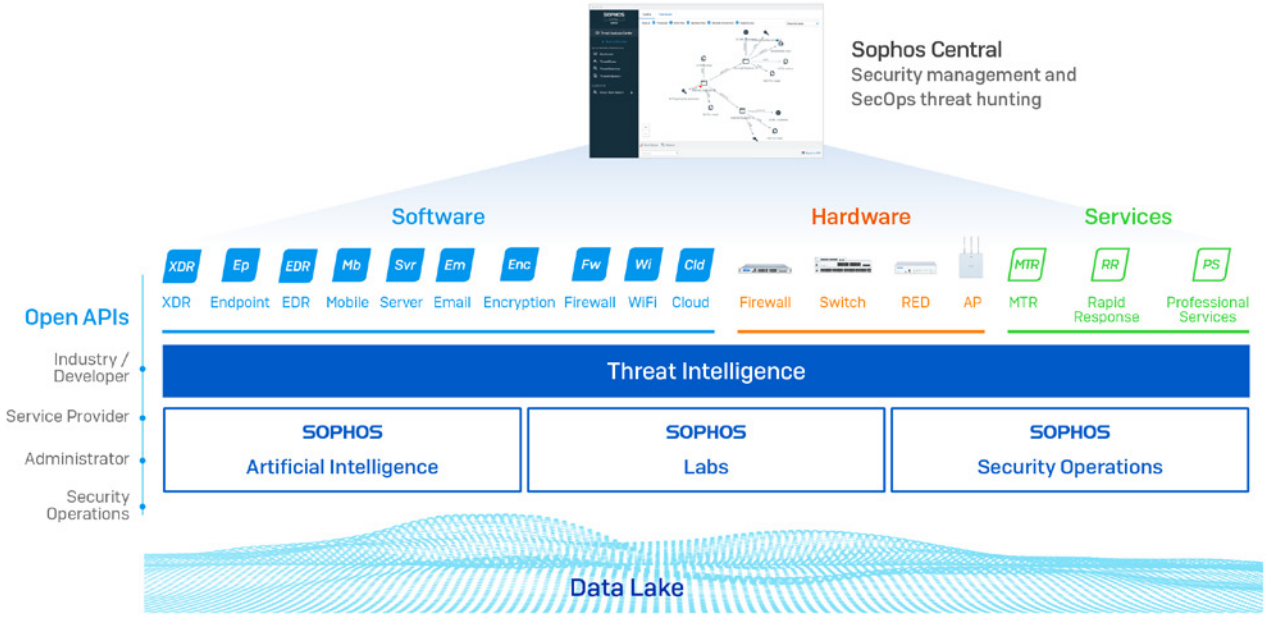
ビジネスが相互接続している現在、セキュリティ対策も同様に提供する必要があります。IT セキュリティチームは、統合されていないセキュリティポイント製品から、可能な限り自動的に防止する**適応型セキュリティシステム**に移行する必要があります。同時に、オペレータは疑わしい動作やイベントなどの弱いシグナルを検索・検出して、侵害の発生を防止する必要があります。

ビジネス環境と攻撃は常に進化しています。IT セキュリティの未来の姿は、独自のフィードバックループを実現して、**常に学習し、改善**できるようにするシステムです。運用チームによって検出された新しい情報とイベントを自動化することで、防御を改善し、システムに侵入する新しい攻撃の数を減らすことができます。同様に、自動化ソフトウェアが改善されるにつれ、オペレーターは疑わしい動作やイベントをより迅速に見つけることができ、インシデントをさらに減少させることができます。この好循環により、組織と接続しているビジネスの全体的なセキュリティは常に向上します。

# Sophos Adaptive Cybersecurity Ecosystem

幸い、このようなシステムは既に存在します。Sophos Adaptive Cybersecurity Ecosystem (ACE) は、この新しい現実に対応しています。自動化とアナリストの力を活用して、セキュリティ管理からセキュリティ運用への移行を実現します。自動化により、動作やイベントを迅速に解析して対応することができ、一方、アナリストは、複数の疑わしいシグナルを関連付けて、その意味を解釈することができます。

Sophos ACE は、ビジネスとオンライン世界の相互接続性を保護するために構築されました。場所を問わずシステムやデータを保護し、常に学習して改善し、テクノロジーや攻撃の将来の変遷を保護します。




Sophos ACE は、SophosLabs、Sophos Security Operations (Managed Threat Response サービスとして、何千もの顧客環境で高度な脅威ハンティングを実行するアナリストチーム)、Sophos Artificial Intelligence (AI) グループの総合的な**脅威インテリジェンス**を基盤としています。このようなリアルタイムのインテリジェンスは、世界をリードするソフォスの**ソフトウェア**および**ハードウェア**製品の次世代テクノロジーを常に改善しています。

単一の統合された **Data Lake** は、ソフォス製品と脅威インテリジェンスソースからの情報すべてを取得し、リアルタイムな分析を行います。これにより、防御側はノイズの中から疑わしい信号を積極的に見つけることで、侵害を防止できます。同時に**オープン API** を活用して、顧客、パートナー、開発者はシステムと連携するツールやソリューションを構築できます。これらはすべて、**Sophos Central の管理プラットフォーム**から管理されます。すべてのセキュリティを 1か所にまとめ、比類のない効率性を実現します。

脅威インテリジェンス、次世代型テクノロジー、Data Lake、API、一括管理の 5つの要素は連携して、常に学習および改善する適応型サイバーセキュリティエコシステムを構築します。また、包括的なエコシステムの力は広範囲に及びますが、必要な要素だけ使用することもできます。多くのお客様は、エンドポイント保護やファイアウォールの導入からはじめ、その後、各自のペースで拡張しています。

この 1年間で、セキュリティ オペレーション センターの多くは、バーチャル化 (VSOC) されました。セキュリティ担当者は、Sophos ACE をあらゆる場所から管理できるため、各組織は最高のグローバルセキュリティ人材を確保することができます。または、ソフォスの専門家が脅威検出と対応をサービスとして管理することもできます。

# Snchronized Scurity の進化

ソフォス製品が Security Heartbeat™ を介してリアルタイム情報を共有し、インシデント対応を自動化することを可能にする Synchronized Security は、長年にわたりソフォスの保護の基盤となってきました。2015年のリリース当時 Synchronized Security は業界唯一のソリューションで、以後、製品間のより深い洞察を備えたあらゆるセキュリティベンダーの最も広範な統合を提供し続けています。

「ソフォスは、ファイアウォールとエンドポイントセキュリティ製品間の XDR 機能で業界をリードし続けています。」

ガートナー社
Gartner Magic Quadrant for Enterprise Network Firewalls、
アナリスト: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 2020年 11月 9日

Sophos Adaptive Cybersecurity Ecosystem は、Synchronized Security の自動化と統合に基づいて構築されており、ソフォスのサイバーセキュリティシステムをさらに拡張します。

## 可視性の向上

次の攻撃の発生元を把握することは不可能で、オペレーターがすべての動作を監視することはできません。代わりに、すべてを監視するシステムが必要で、それを活用して新たな脅威に迅速に対応ことができます。このため、ソフォスはエコシステムを拡張して、新しい Sophos Extended Detection and Response (XDR) や API など、さらに幅広いテクノロジーを追加しました。ソフォス製品は、疑わしいイベント、動作、検出すべてを環境全体で検出、記録するため、必要な情報をすぐに入手できます。

## より多くのデータ

Data Lake は、このようなすべてのセンサーからの情報を組み合わせて関連付け、製品間のより深い洞察を提供します。オペレーターは、Sophos Intercept X with EDR および Sophos XDR を使用して Data Lake を直接クエリできます。これにより、環境全体で疑わしい動作やイベントを特定し、侵害の発生を防止できます。

## より多くのインテリジェンス

MTR (Managed Threat Response) サービスの急速な成長に伴い、ソフォスは、エキスパート脅威ハンターからのリアルタイムのデータを追加して、検出データを補完することができます。並行して、AI モデルと SophosLabs からの脅威検出情報もさらに進化させ続けています。

## 統合性の向上

SophosLabs、Sophos AI、および Sophos Security Operations は連携して、専門知識を統合し、すべてのお客様にメリットをもたらす好循環を生み出しています。たとえば、PowerShell は、多くの優れた用途を持つ正当なツールですが、攻撃者によって広く悪用されています。MTR オペレーターは実環境の使用経験に基づいて AI モデルを訓練し、PowerShell の「正規」の用途と「不正」な用途を区別できるようにします。その後、システム全体が AI 学習で更新され、お客様の保護が強化されます。

# Sophos Adaptive Cybersecurity Ecosystem の動作

Sophos ACE は、実環境で既に保護を強化し、拡張しているライブシステムです。2021年 3月、Hafnium という攻撃グループが Microsoft Exchange の ProxyLogon の脆弱性を悪用しました。これはゼロデイ脆弱性で、攻撃者は Exchange の設計上の本来の弱点を悪用して、即時の検出を回避しました。

この脆弱性が判明するとすぐに、ProxyLogon に関連する動作が検出されるように、Sophos Managed Threat Response (MTR) サービスのセンサーモニタリングが更新されました。Sophos MTR は、Data Lake に既に存在する情報を活用して、この脆弱性に関連する悪意のあるアクティビティを特定・修復するために必要な情報すべてに即座にアクセスできました。

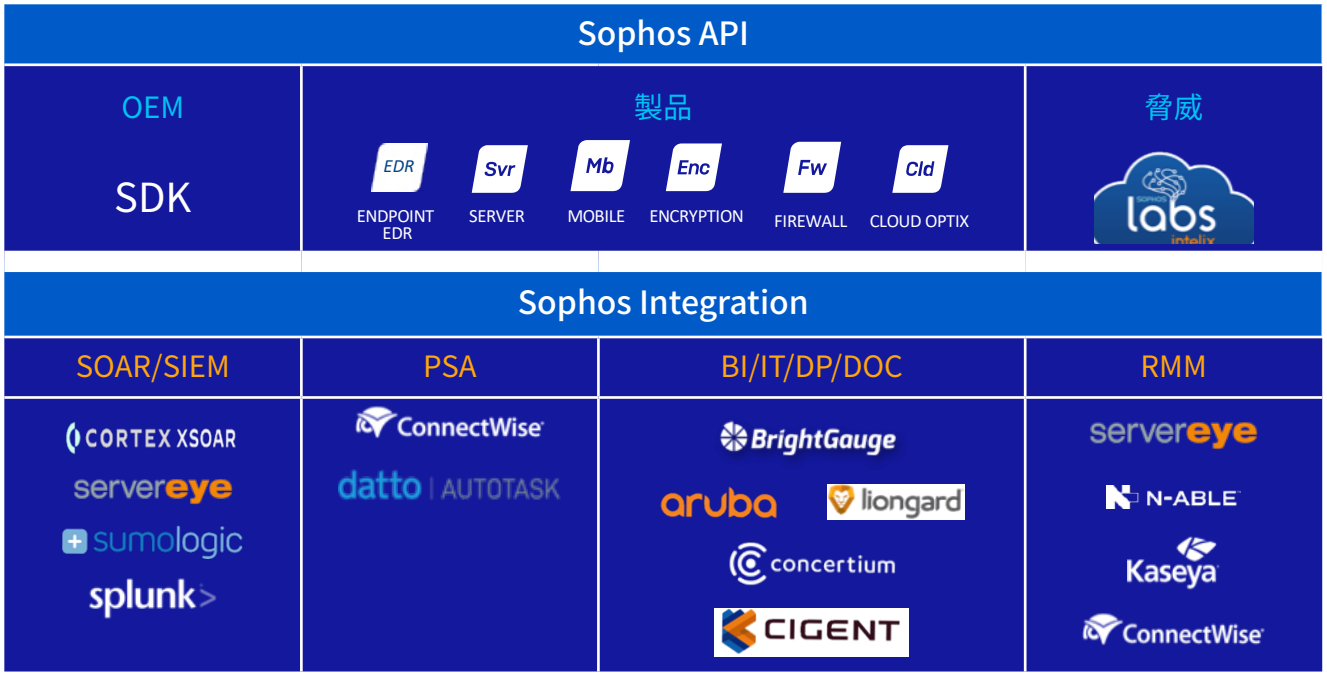
さらに、脅威ハンティング機能と Sophos EDR テクノロジーを組み合わせて、攻撃に関連する新たなアーティファクトや感染の痕跡 (IoC) を検出しました。このような痕跡は、SophosLabs と直接共有され、SophosLabs はそれを使用して Exchange の脆弱性に関連する追加の IoC を公開し、ソフォスのお客様すべてに保護が追加されました。

# 強力な統合とオープン API を備えたオープンプラットフォーム

現在の相互接続された世界では、サイバーセキュリティをより広範なビジネス環境と統合できることは不可欠です。サイバーセキュリティには多面的な対策が必要で、Sophos Adaptive Cybersecurity Ecosystem は、次のようなさまざまなセキュリティニーズをサポートします。

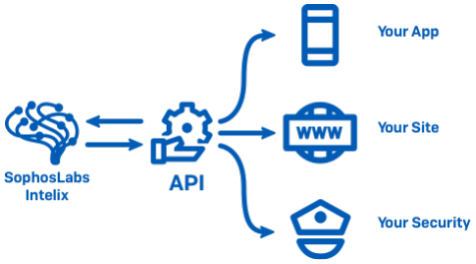
- MSSP – お客様への高度なサイバー防御の提供をサポートします
- チャネルパートナー – ビジネスプロセスを合理化します
- ISP – 提供するインターネットサービスのセキュリティを確保できるようにします
- 中小企業 – セキュリティの制御および有効化を実現するカスタムツールの作成を容易にします

Sophos ACE では、多数の API と統合が既に導入されています。毎日 500万件以上の API リクエストを処理しており、今後もこの導入は続きます。



### API の紹介：SophosLabs Intelix™

Intelix は、シンプルで迅速な応答を可能にする RESTful API スイートで、アプリが脅威を識別、分類、防止し、セキュリティを強化できるようにします。ソフォスのエコシステムをご利用のお客様、パートナー、および開発者は、これらの API を使用して、クラウドの脅威検索、静的なファイル分析、および動的ファイル分析を実行できます。SophosLabs Intelix API の詳細は、次のサイトを参照してください: https://www.sophos.com/ja-jp/labs/intelix.aspx




## Sophos ACE: ビジネスに真の影響を与える

Sophos Adaptive Cybersecurity Ecosystem のメリットは積み重なります。次世代型テクノロジー (SophosLabs、Sophos AI、Sophos Security Operations からの脅威インテリジェンス)、統合された適応型常時学習システム、およびSophos Central プラットフォームによる一括管理を組み合わせることで、保護と効率性の両方に大きな影響を与えます。

| | | | | | | |
|---|---|---|---|---|---|---|
| **次世代型テクノロジー** | + | **脅威インテリジェンス** | + | **統合された適応型システム** | + | **一元管理** |

Sophos Firewall と Sophos Intercept X と同時に実行しているお客様からは、ソフォスのサイバーセキュリティ システムがなければ、同じレベルの保護を維持するのにセキュリティの人員を 2倍にする必要があるとの声が既に寄せられています。また、セキュリティインシデントの発生回数が減り、発生した問題をより迅速に特定して対応できるとしています。Sophos ACE はこれを基盤として、サイバーセキュリティの TCO と保護をさらに変革しています。

# 作業の開始

Sophos Cybersecurity Ecosystem は非常に柔軟性があり、ソフォスの保護製品やサービスのいずれかを導入することで開始できます。組織は、Sophos AI、SophosLabs、Sophos Security Operations の脅威インテリジェンスの専門知識を組み合わせることで、すぐにメリットを享受できます。エコシステムは、ビジネスのニーズに合わせていつでも拡張できます。最も一般的な開始点は次のとおりです。

エンドポイントまたはサーバー用の Sophos Intercept X (EDR または XDR 機能を追加するオプションあり)

Sophos Firewall – ハードウェア、ソフトウェア、または仮想

Sophos Managed Threat Response (MTR) サービス

詳細は、ソフォス営業部にお問い合わせいただくか、ソフォス Web サイトをご覧ください。または、無償評価も開始できます。

Gartner Magic Quadrant for Enterprise Network Firewalls、
アナリスト: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 2020年 11月 9日

ガートナーは、ガートナー・リサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また最高の評価を得たベンダーのみを選択するようテクノロジーの利用者に助言するものではありません。ガートナー・リサーチの発行物は、ガートナー・リサーチの見解を表したものであり、事実を表現したものではありません。ガートナーは、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の保証を行うものではありません。

ランサムウェアの詳細と、ソフォス製品が組織の防御にどのように役立つかをご覧ください。

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。



2021-04-26 (SB-NP)

SOPHOS