SOPHOS
Cybersecurity made simple.

ソフォス 総合カタログ

〔クラウド ソリューション〕

Sophos Central

会社概要

ソフォスは法人向け IT セキュリティおよびデータプロテクションにおける世界的なリーディングカンパニーです。
本社をイギリス アビンドン、およびアメリカ サンタクララに構え、コンピュータ、ノート PC 、仮想デスクトップ / サーバー、モバイルデバイス、ネットワーク、Web、E メールゲートウェイなどを保護するセキュリティソリューションを提供しています。世界 5 ヶ所（ アビンドン、バンクーバー、シドニー、アーメダバード、ブダペスト ）にある脅威解析センター、SophosLabs では、経験豊富なアナリストが 24 時間 365 日、さまざまな種類の脅威を統合的に解析し、最新の対策を迅速に提供しています。
ソフォスのソリューションは政府・教育機関・製造・流通・金融その他あらゆる業種で採用され、150 ヶ国 28 万社以上の企業と 1 億人以上のユーザーを保護しています。国内でもすでに、3,500 社以上で導入されています。

Sophos Limited

最高経営責任者 (CEO)
クリス・ヘイゲルマン

本社所在地
イギリス アビンドン
アメリカ サンタクララ

設 立
1985 年 イギリス アビンドンに設立

販売地域
世界 150 ヶ国 (ユーザー数 1 億人以上)

オフィス
イギリス、アメリカ、ドイツ、カナダ、オーストラリア、イタリア、フランス、スペイン、ハンガリー、インド、シンガポール、中国、香港、日本など

従業員数
約 2,900 名以上（全世界）

ソフォス株式会社

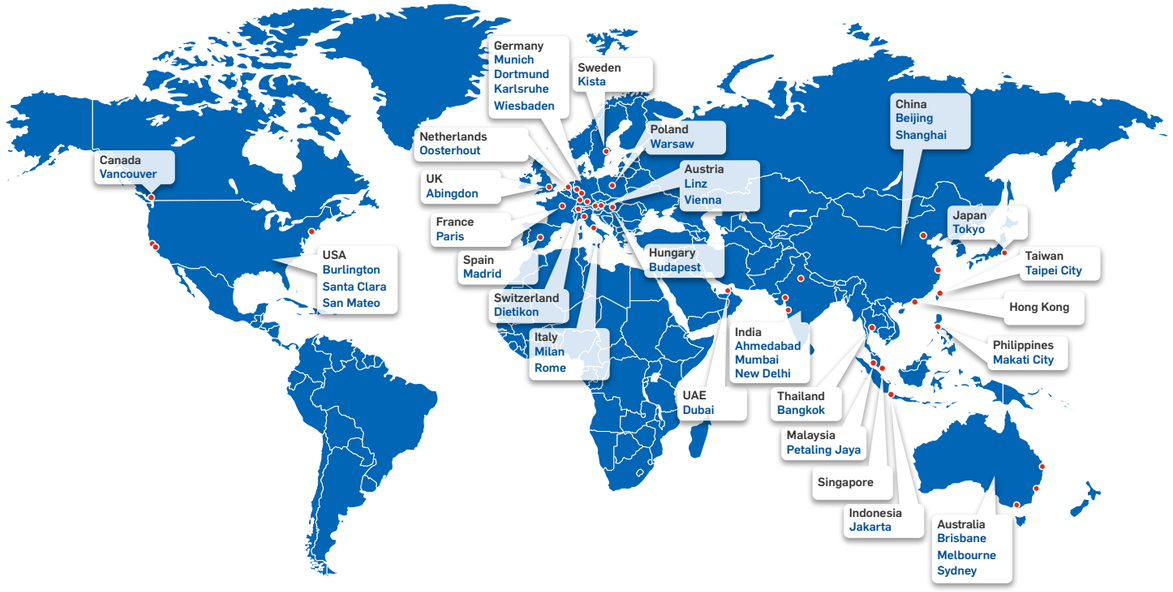
代表取締役
中西智行

所 在 地
東京都港区六本木 1-6-1
泉ガーデンタワー 10F

設 立
1997 年 ソフォス製品国内販売開始
2000 年 ソフォス株式会社 設立

事業内容
法人向け IT セキュリティ関連製品
サービスの開発、販売およびサポート
（日本市場でのソフォスソリューションを販売・サポート）

Global location



ソフォスのテクノロジー

SophosLabs

ソフォスのテクノロジーは、各種アワードを多数受賞しています。
世界 5 ヶ所 [アビンドン、バンクーバー、シドニー、アーメダバード、ブダペスト] にある SophosLabs では、経験豊富なアナリストが 24 時間 365 日、ウイルスやスパムなどさまざまな種類の脅威を統合的に解析しています。SophosLabs が持つ 100 万件以上のマルウェアサンプルと、1 日 4 万件以上更新している有害サイトの URL 情報は、クラウド上のデータベースで共有されているため、最新の脅威対策を即座に提供することが可能です。
ソフォスのテクノロジーは業界でも高く評価されており、多数のセキュリティベンダーやサービスプロバイダが、ソフォスの脅威検出エンジンを採用しています。

アワード
ソフォスのテクノロジーは、さまざまな第三者機関から高評価を得ています。

Gartner Magic Quadrant においてリーダーの評価

- エンドポイント保護プラットフォーム分野 [2007 年から 11 年間 8 度連続リーダーの評価]
- UTM 分野 [2012 年から 7 年間 6 回連続リーダーの評価]

出展：
Gartner "Magic Quadrant for Endpoint Protection Platforms" Eric Ouellet, Ian McShane, Avivah Litan, 30 January 2017
Gartner "Magic Quadrant for Unified Threat Management [SMB Multifunction Firewalls]" Rajpreet Kaur, Claudio Neiva, 20 September 2018

Forrester Wave™ : Endpoint Security Suites, Q2 2018 においてリーダーの評価

出典：: The Forrester Wave™: Endpoint Security Suites, Q2 2018

Sophos Mobile Security が AV-TEST Best Android Security Award を獲得

出典：https://www.av-test.org/en/award/2016/best-android-security-sophos/

ソフォスのお客様

ソフォスのソリューションは政府・教育機関・製造・流通・金融・その他あらゆる業種で採用され、
150 ヶ国以上で 1 億人以上のお客様が、ソフォスのテクノロジーによって保護されています。
国内でも 3,500 社以上のお客様がソフォスを採用しています。

国内約 3,500 社以上
岩波書店、講談社、芝浦工業大学、
新日鉄住金ソリューションズ、早稲田大学、東京大学、朝日新聞社、
テイクアンドギヴ・ニーズ、伊那市、豊川市役所、
デザインフィルホールディングス、シネックスインフォテック、
ビジュアルテクノロジー株式会社、その他、官公庁、
地方自治体、銀行、大学、大手自動車メーカー、電機メーカー 、
コンピュータメーカーなど

海外 150 ヶ国で 1 億人以上のユーザー
Citgo / Deutsche Postbank AG / GE / Gulfstream /
Harvard University / Heinz / Interbrew /
Hong Kong University / Marks & Spencer /
New York University / Orange / Oxford University /
Pulitzer / Sainsbury' s / Siemens / Société Générale /
Toshiba / University of Hamburg / University of Otago /
US Government Agencies / Weleda AG /
Xerox Corporation など

SOPHOS Central Solutions Map

社内

アクセスポイント

Sophos Wireless

仮想サーバー

Central Server Protection

- MS Hyper-V
- VMware ESXi

社内サーバー

Central Server Protection
Central Intercept X for Server

- Windows
- Linux

仮想クライアント

Central Endpoint Protection

Windows クライアント

クライアント

Central Endpoint Protection
Central Intercept X

- Windows
- Mac OS

社外

- Next-Generation Firewall
- Email Protection
- Web Protection
- Web Application Firewall
- Secure VPN
- Secure Wi-Fi
- Secure Wi-Fi

Sophos XG Firewall/ Sophos UTM

お客様用管理コンソール

Sophos Central Admin

Sophos Central Enterprise Dashboard

Sophos Central

Sophos Email　Sophos Phish Threat

パートナー用管理ダッシュボード

Sophos Central Partner

お客様企業の従業員用ポータル

Sophos Central Self Service

スマートフォン/タブレット

Sophos Mobile

- Android
- iOS
- Windows Mobile

SSL/VPN 接続

支店 / 支社 1

Sophos XG Firewall
Sophos UTM

支店 / 支社 2

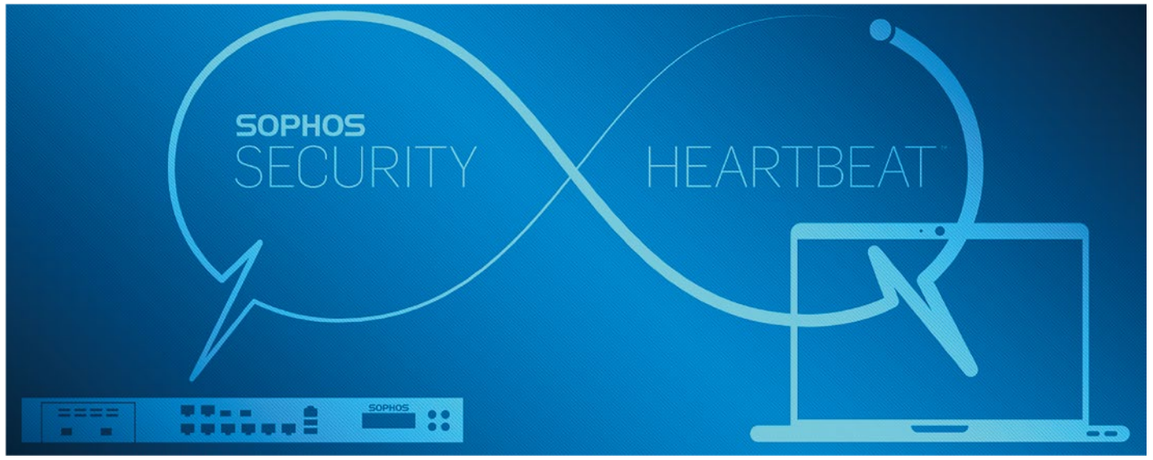
Sophos RED

SSL/VPN 接続

ルーター/モデム

Sophos Wireless

Security Heartbeat™



標的型攻撃やゼロデイ攻撃が高度化・巧妙化するなか、企業は高度なセキュリティ管理体制が求められています。
機密情報、個人情報を扱ういかなる企業も、セキュリティ対策を求められています。今までのファイアウォールとアンチウイルスだけでは、防ぐことはできません。Security Heartbeat は、セキュリティ専任の管理者がいない中堅・中小企業向けに、自動インシデント対応を可能にする画期的なソリューションです。

Security Heartbeat™ ってなに？

Security Heartbeat™ は、エンドポイントとファイアウォールでセキュリティ情報をリアルタイムに共有する仕組み。
これにより、エンドポイントで脅威を見つけると、ファイアウォールはどのエンドポイントが危険なのか瞬時に把握できます。
またファイアウォールも脅威を検出すると、該当するエンドポイントとその情報を共有し、解決に努めます。

セキュリティ管理の悩み

分断された製品管理

エンドポイントとファイアウォールで管理が分断・サイロ化されている。そのため、発見された脅威は、エンドポイントとファイアウォールそれぞれで、個別に解決されて、情報は共有されない。

ログ分析と対応が困難

ログ解析のできるスタッフがおらず、エンドポイントとファイアウォールのログから相関分析ができない・時間がかかる。ログを元に適切な対策ができない、わからない。

発見～復旧までの時間

脅威の高度化やセキュリティ管理の複雑さにより、脅威の発見・隔離・駆除・復旧までに時間がかかる。いざという時にも、スピーディに対応できず、被害が拡大するリスクも高い。

アラートを止めるだけの対応。一体何が起きているのかわからない。予防もできない。

既存の解決策と中堅企業導入時の課題

SOC [セキュリティオペレーションセンター]

セキュリティの集中監視センター。
アラートを 24 時間 365 日監視し、速やかに対応。

→ **高コストで費用対効果が不明確**

SIEM [セキュリティ情報イベント管理ツール]

ログの収集・分析・監視ツール。様々なログを収集。
複数のイベントから、相関分析を行う。

→ **チューニングや分析などに、専門的な知識、スタッフが必要**

運用の負担が大きい、利用しきれない

Sophos Security Heartbeat を試してみませんか？

個別セキュリティ管理をビルの警備に例えると…

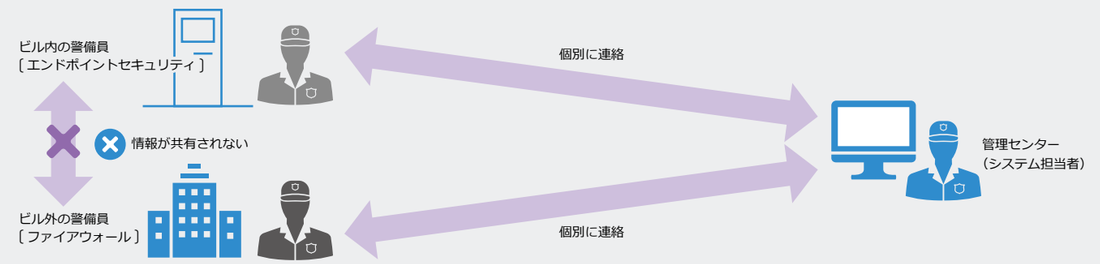
これまでの個別のセキュリティ対策は、ビル内とビル外の警備員が連係していない状態と同じです。このような個別のセキュリティ対策では、管理センターにあたるシステム担当者の業務負荷が重くなります。また、高度化・巧妙化したセキュリティの脅威に対するには限界がありますが、SOC や SIEM といった高度な対策は、中堅企業では人材やコストの面で実現が困難です。

現場の問題

ビル内の警備員とビル外の警備員は、不審者を管理センターにそれぞれ通知 → ビル内と敷地内の警備員同士で情報共有しておらず、管理センターからの指示対応が必要

管理者の問題

- 業務負荷が重く、人手がかかる
- いざという時、対応時間がかかる
- 高度な脅威への対応が困難

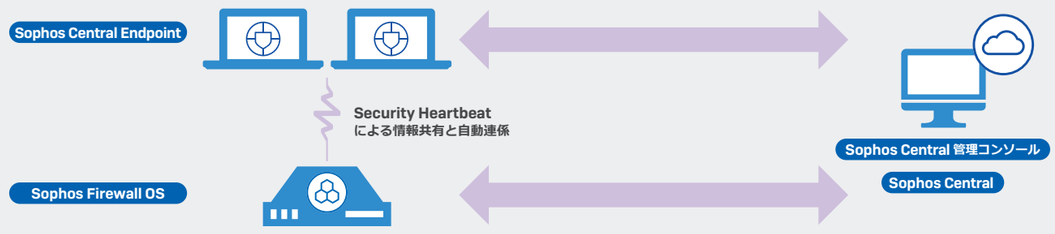


Security Heartbeat は連係プレーで自動対応

Security Heartbeat は、高度なセキュリティ管理体制を実現する機能のひとつです。エンドポイントとファイアウォールとの間で、リアルタイムにセキュリティ情報を共有することで 、「すばやく確実に」「セキュリティ管理者不要」で高度なセキュリティ管理体制を中堅企業に最適なコストで実現します。

問題を解決

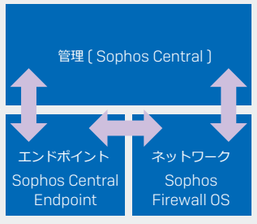
- 自動対応で、人手は不要
- いざという時、スピード対応
- 高度な脅威にも対処可能



Security Heartbeat と SOC / SIEM との違い

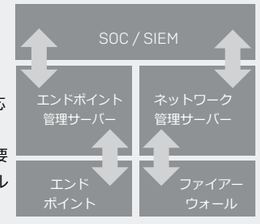
Security Heartbeat

- 低価格なソリューション
- 自動化された相関分析
- SophosLabs のインテリジェンス情報を使った対応
- 自動的な検出・隔離・駆除・復旧
- シンプルなシングル管理



SOC / SIEM

- 高価なサービスや導入コスト
- 人的な相関分析
- 人のスキル・ナレッジに依存した対応
- 手動による検出・隔離・駆除・復旧
- より幅広い機器やソフトウェアが必要
- エンドポイントとファイアウォールの情報共有なし



Synchronized Security

概 要

Synchronized Security とは、Security Heartbeat を利用する高度なセキュリティ対策です。
Security Heartbeat によって、エンドポイント〔サーバー〕とファイアウォール間においてセキュリティ状態を共有し、
エンドポイント〔サーバー〕のセキュリティ状態に応じて、ファイアウォールが自動的に適切な対処を行います。

主な特長

1. 自動化で即座に対応

- Central Endpoint〔Central Server〕と Sophos Firewall OS が情報を共有。SophosLabs の最新の解析結果を元に、状況に応じた適切な対処を自動実行。

2. 専門知識・スタッフは不要

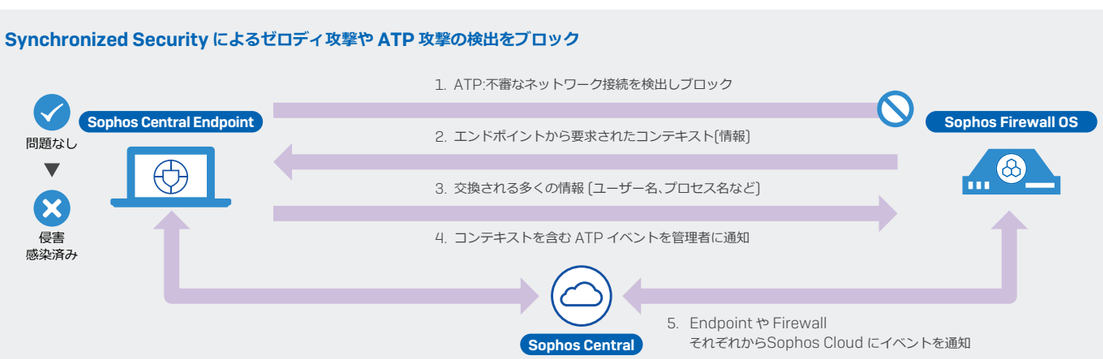
- 高度なスキルや知識を持つセキュリティの専門家がいなくても、高度で巧妙化した攻撃に対応できます。

3. 中小中堅企業がお求めやすい価格設定

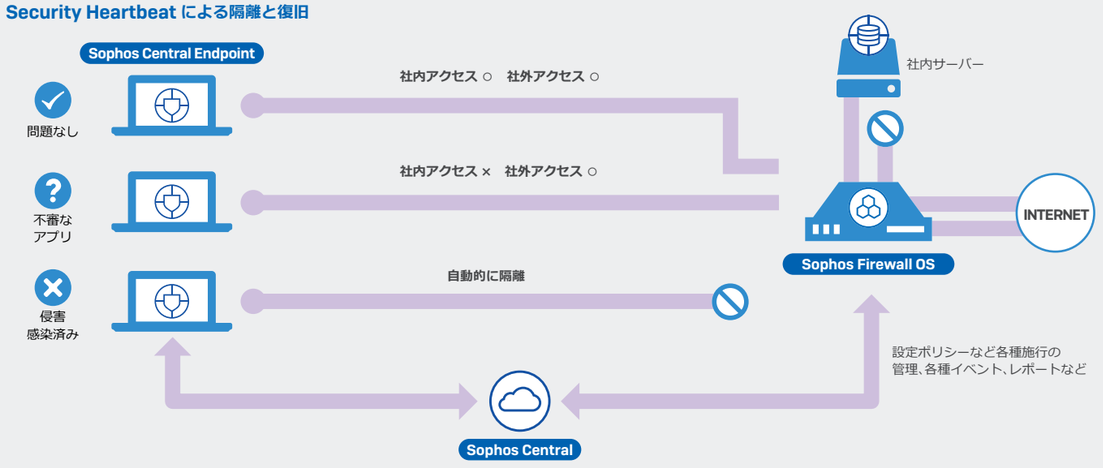
- ファイアウォールとエンドポイントプロテクションだけで実現できるので、中堅企業でも気軽に導入可能です。

動作の仕組み

Synchronized Security によるゼロディ攻撃や ATP 攻撃の検出をブロック



Security Heartbeat による隔離と復旧



Synchronized Encryption

概 要

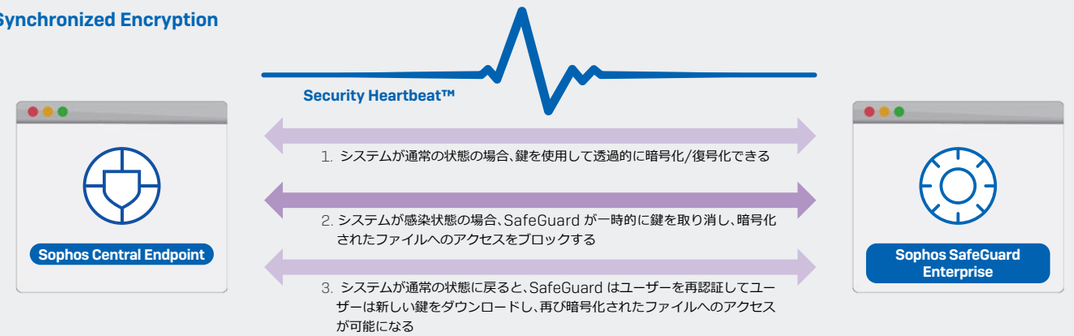
ソフォスは、従業員が作成するデータはすべて重要なものであると考え、ファイルがどこに保存／コピー／移動されても常に暗号化により保護します。また、暗号化されたデータを保護するために、信頼されるデバイス／ユーザー／プロセスからのアクセスのみ許可し、不正なアクセスからデータを守ります。

特 長

- ユーザーが作成するすべてのファイルを Sophos SafeGuard がデフォルトで暗号化
- ファイルがどこに保存／コピー／移動されても常に暗号化状態を維持
- 管理者が設定したアプリケーション以外の信頼されないプロセスから暗号鍵へのアクセスをブロック。
- Sophos Central Endpoint Protection がマルウェアを検出した場合、一時的に暗号鍵をすべて削除し、マルウェアによる暗号化ファイルへのアクセスをブロック。
- 外部のユーザーと安全にファイルを送受信するためのパスワード付 HTML5 ファイルを作成
- Windows、Mac OS、iOS、Android に対応し、ユーザーの生産性を維持

動作の仕組み

Synchronized Encryption



Synchronized Application Control

概 要

Synchronized Application Control は、ネットワークの可視性を飛躍的に高める画期的機能です。
Synchronized Security によってエンドポイントからアプリケーション情報を取得するのが特徴で、これまで識別できなかったアプリケーション、たとえば、シグネチャがないものや、一般的な HTTP や HTTPS 接続を使用するようなものも識別、分類、制御することが可能になりました。

主な特長

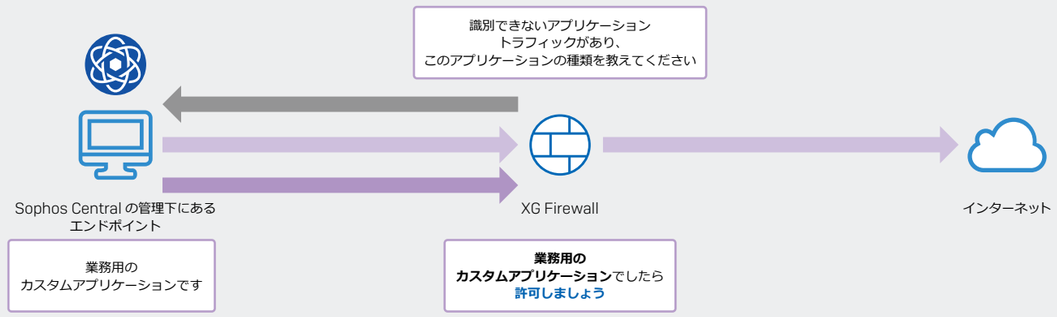
1. 「不明なアプリケーション」問題の解消

- これまでのファイアウォールはシグネチャに基づいてアプリケーションコントロールを行うため、ほとんどのアプリケーションが「不明」、「分類不可能」、「一般的な HTTP」、「SSL」などに分類されていました。Synchronized Application Control では Central Endpoint から詳細なアプリケーション情報を取得するため、すべてのトラフィックの可視化が可能です。

2. きめ細かいアプリケーションコントロールの実現

- 取得したアプリケーションの情報をもとに、自動的に分類し、既存のアプリケーションコントロールルールを適用したり、手動で優先順位を調整したりすることが可能です。また、ユーザー情報と組み合わせることで、よりきめ細かいアプリケーションコントロールが可能になります。

動作の仕組み



Sophos Central Admin / Self Service / Partner / Enterprise Dashboard

概 要

Sophos Central の管理コンソールは、クラウドベースの管理コンソールで、いつでも、どこからでもアクセス！
アップデートなどの煩わしい作業は必要なし！

主な特長

1. クラウドベースの管理コンソール

- いつでもどこからでもアクセス可能
- サーバーの設置やメンテナンスは不要

2. 直感的に操作できる管理コンソール

- ダッシュボードからステータスを即座に把握
- わかりやすいレポート、警告一覧
- グラフィカルな操作画面
- メニュー等は、日本語化済み

3. ユーザー中心のポリシー管理

- あらかじめ用意されたベストプラクティスのポリシー
- Windows と Mac で共通のポリシーの適用

4. 役割に応じたコンソールを用意

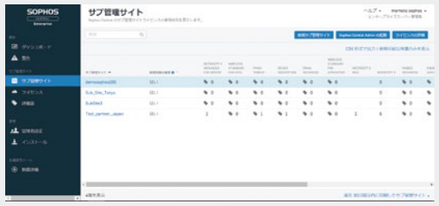
- 管理者用の Central Admin ポリシー設定、ダッシュボード、レポートなど
- 従業員用の Central Self Service
  ヘルプデスクサービスの支援ツール
- パートナー用の Central Partner 販売した顧客の
  Central Admin へアクセス、ライセンス管理が可能
- マルチサイトを管理する Central Enterprise Dashboard

画面紹介

SOPHOS CENTRAL Admin

Sophos Central Admin

ダッシュボード
社内のセキュリティ状態を一目で把握



Central Enterprise Dashboard

SOPHOS CENTRAL Self Service

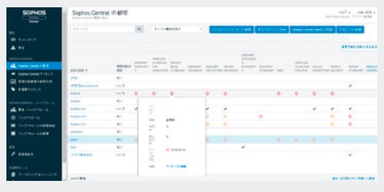
Sophos Central Self Service

メールセキュリティ
従業員が、スパムフィルタによって
隔離されたメールを確認、受信や削除可能

Sophos Central Self Service

デバイス暗号化
従業員が、暗号化のパスワードを忘れた場合でも、
IT部門に連絡せず、自身で復旧可能

SOPHOS CENTRAL Partner



Sophos Central Partner

ダッシュボード
パートナー様が販売したお客様の Sophos Central の
管理コンソールにアクセスしたり、ライセンスの管理などが可能

Sophos Central Endpoint Protection　クラウド管理型エンドポイント保護ソリューション

主な特長

1. 高度な脅威対策機能

- 全世界に配置されたラボから迅速に定義ファイルを配信
- クラウド DB への脅威情報確認、C&C サーバーとの通信の検知、疑わしい動作の検知
- Genotype〔遺伝子〕技術による亜種の検知と駆除
- Decision Caching による検索の高速化

2. 場所を問わない管理

- クラウドベースの管理コンソールには、どこからでもアクセスが可能

3. エンドポイントに必要とされる数々の機能を搭載

- デバイス接続制御、アプリケーション制御、危険な Web サイトへの接続制御、ダウンロードレピュテーション機能
- タンパープロテクション機能
- XG Firewall との連携（Security Heartbeat）

4. シンプルなポリシー管理

- ソフォスがお奨めする設定をベースポリシーとして、テンプレートを用意
- ユーザーベースとデバイスベースのポリシーで、各イベントをユーザー名やデバイス名で調査可能
- Windows と Mac に共通のポリシーを適用

機能紹介

Sophos Live Web Filtering
Web アクセスする際に、接続先の Web サイトが安全かどうか、クラウド上の SophosLabs によって管理されているデータベースに照会してチェック。

デバイス〔周辺機器〕コントロール
PC に接続されるデバイスを詳細に制御。USB メモリなどの持ち出し、持ち込みを制御し、マルウェアの侵入や情報の漏洩を防ぐ。また、MTP / PTP などのプロトコルを制御し、PC に接続したデバイスへのデータの転送をブロック。

Sophos Live Protection
ファイルスキャン時に SophosLabs が管理するクラウド型のデータベースに瞬時に照会をかけて、定義ファイル反映前の脅威から保護。

仮想クライアントの保護
新しい Sophos for Virtual Environments は仮想クライアントを様々な脅威から保護。

ダウンロードレピュテーション
Web からダウンロードする際に、ダウンロードされるファイルのレピュテーション情報を、クラウド上の SophosLabs によって管理されているデータベースに照会してチェックし、ユーザーにダウンロードの許可、不許可を求める。

アプリケーションコントロール
P2P や ゲームなどの業務と関係ないアプリの使用を制御。これにより、従業員の生産性が上がるほか、IT 管理者も管理すべきアプリケーションを限定できるため、管理工数が削減できる。

Malicious Traffic Detection (MTD)
C&C サーバーとの不正な通信を検知・ブロック
万が一不正なプログラムが侵入した場合でも、外部へのファイルや情報の送信をブロック。

マルウェア対策機能

- スキャン
  〔オンアクセス/オンデマンド/スケジュール〕
- クラウド上のデータベースへの照会
  〔Sophos Live Protection / Sophos Live Web Filtering〕
- 疑わしい動作の検知〔HIPS〕
- アドウェア・不要ソフトの検知
- ダウンロードファイルの評価
  〔ダウンロードレピュテーション〕
- 悪質なトラフィックの検知
  〔Malicious Traffic Detection〕

その他の保護機能

- USBメモリなどのデバイス制御
- 危険なアプリケーションの利用制御
- カテゴリ別 Web アクセス制御
- 設定変更やエージェント削除防止機能
  〔タンパープロテクション〕
- ファイアウォールと連携し、自動対応
  〔Security Heartbeat〕

ライセンス

Central Endpoint Protection

Sophos Central Server Protection　クラウド管理型サーバーセキュリティソリューション

主な特長

1. サーバー向けマルウェア対策

- Windows と Linux に対応
- サービスへの影響を考慮したスキャン
- HIPS

2. サーバーロックダウン

- 未認証のソフトウェアの実行を防止
- ワンクリックで、インストール済みソフトウェアのホワイトリストを自動作成
- ホワイトリストにあるソフトウェアのみに実行を許可

3. 自動除外設定

- 自動でサーバー環境を認識
- 動作しているアプリケーションに応じて自動で除外設定

4. 標的型攻撃対策

- 不正なコマンド＆コントロールサーバーが、侵入したプログラムに指示を出す通信をブロック
- 万が一、不正なプログラムが侵入した場合でも、外部へのファイルや情報の送信を事前にブロック

5. ランサムウェアに特化した対策機能

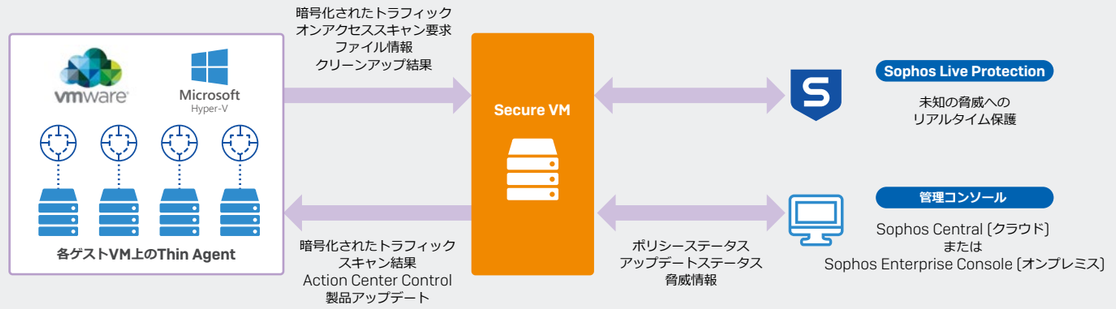
- 悪意ある暗号化の防止と復旧〔CryptoGuard〕
- リモートで実行されるランサムウェアからも防御
- 感染ファイルの自動回復

6. IasS 環境の保護と管理

- AWS および Azure 環境に接続してインスタンス情報を表示
- 保護対象のサーバーの自動検出〔AWS/Azure〕
- Auto Scaling に対応〔AWS〕

機能紹介

Sophos for Virtual Environments



機能紹介

Central Server Protection の AWS/Azure 統合

- Sophos Central から AWS/Azure へアクセスし、設定を確認。
- Sophos Central は AWS から EC2 インスタンスおよび Auto Scaling グループの情報、Azure から Azure VM の情報を取得して Sophos Central Admin 上に表示。

主な特長

- Sophos Central 管理コンソールから終了した AWS EC2 インスタンス／ Azure VM を自動的に削除
- Auto-Scaling Groups に新しいインスタンスが加わると自動的に Server 用ポリシーを適用
- AWS EC2 インスタンス／ Azure VM のメタ情報を表示させることが可能
  - **AWS EC2 インスタンス：**
    インスタンス ID、ライフサイクルの状態、AWS アカウント、AWS リージョン、 Auto Scaling グループ
  - **Azure VM：**
    仮想マシン名、ステータス、サブスクリプション、場所、リソースグループ名

ライセンス

Central Server Protection

Sophos Central Intercept X / Sophos Central Intercept X for Server

主な特長

1. AI による未知の脅威からの保護

- シグネチャを利用せずすべての実行可能ファイルを実行前に評価
- SophosLabs のデータサイエンティストが DARPA ドリブンのテクノロジーを利用して作成したディープラーニングモデル
- データに含まれる重要な特徴をモデル自身で見出して自動的に学習を行い、正常なファイルと悪意のあるファイルを高い精度で判別

2. ランサムウェアに特化した対策機能

- 悪意ある暗号化の防止と復旧 (CryptoGuard)
- 攻撃元の特定
- 感染ファイルの自動回復

3. ハッキング行為の防止

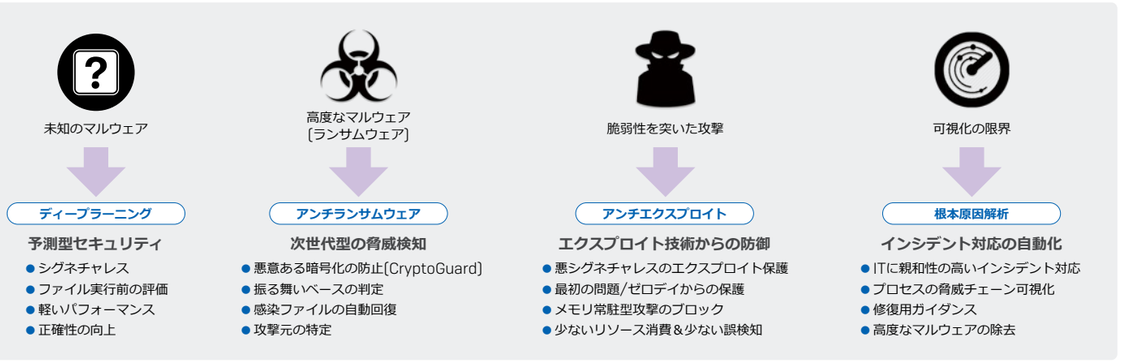
- 脆弱性を突いた攻撃 [エクスプロイト攻撃] を防止 [エクスプロイト防止]
- マルウェアや脆弱性ごとの対処ではなく、攻撃手法ごとの検出

4. 根本原因解析機能により、脅威のチェーンを可視化

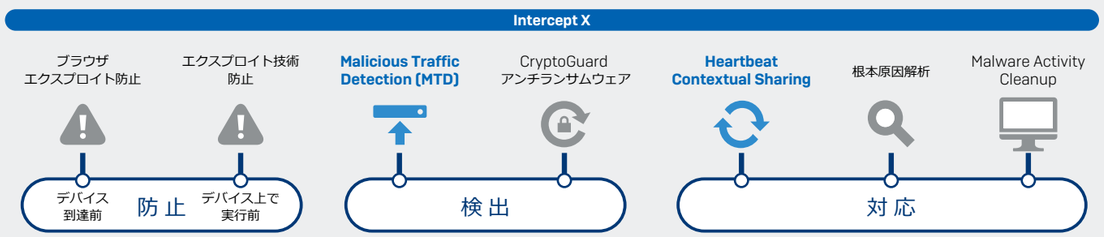
- 発見された脅威の疑わしい振る舞いを可視化
- Sophos Data Recorder によるプロセス、レジストリ、ファイル、ネットワークアクティビティの相関分析

5. 柔軟な運用が可能

- 他社製アンチウィルスと共存可能
- クラウドベースの管理コンソール



ランサムウェアから Intercept X で保護



ディープラーニング

- 生データに含まれる特徴を自動的に見つけ出し、高い精度でデータを認識
- 大量のデータ (ビッグデータ) からセキュリティ脅威情勢を幅広く「暗記」して普遍化し、新種の脅威を検知できるようになるなど、簡単にスケーリングすることが可能
- 検知精度が高く、誤検知率が低いほか、他の機械学習を用いた検知システムに比べ、はるかに少ないメモリ消費量で動作します

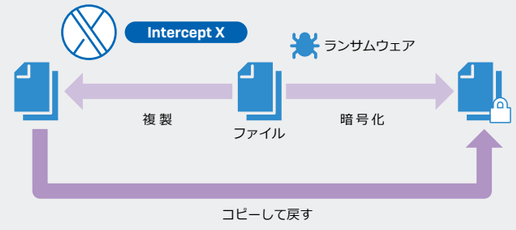
機能紹介

アンチランサムウェア (CryptoGuard)

ランサムウェアが実行された場合

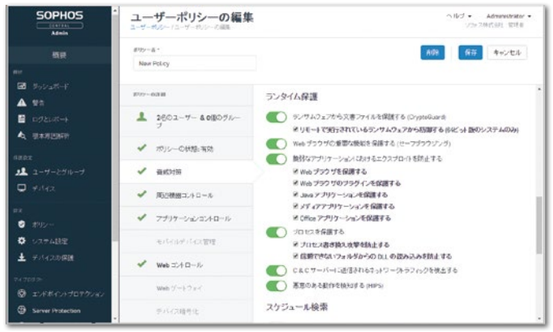
- 暗号化が始まる前にファイルを同時にバックアップ
- 悪意ある暗号化プロセスと判断されると暗号化をブロックし、暗号化されたファイルを復旧

- ランサムウェアの振る舞いを見て検出
- 暗号化が始まる前にファイルをバックアップ
- 悪意ある暗号化と判明した時点でブロックして、バックアップから復旧



アンチエクスプロイト (Exploit Prevention)

- マルウェアのコードを分析してシグネチャとのマッチングによりマルウェアを検出するのではなく、脆弱性を突くエクスプロイト手法を検知し、その手法を使っている攻撃プロセスを停止させる
- 業界トップクラスのエクスプロイト手法数に対応。



根本原因解析 (RCA : Root Cause Analysis)

- Sophos Data Recorder により、プロセスのアクティビティをすべて記録

- 記録されたマルウェアの行動を相関分析し、マルウェアがどのプロセスから起動されたのか、どのようにしてデバイスに侵入してきたのかを可視化

ライセンス

Central Intercept X / Central Intercept X Advanced / Central Intercept X Advanced with EDR / Central Intercept X Advanced for Server

Sophos Central Endpoint Protection / Intercept X 機能表

		ライセンス	ライセンス別対応機能			OS 別対応機能	
		ライセンス名 / OS	Central Endpoint Protection	Central Intercept X	Central Intercept X Advanced ※	Windows	macOS
		ライセンス種類、カウント方法	ライセンス別対応機能				
防 止	攻撃対象領域の削減	Web セキュリティ	◎		◎	◎	◎
		Web フィルタリング [カテゴリ/ファイルベース]	◎		◎	◎	◎
		Sophos Live Web Filtering	◎		◎	◎	◎
		ダウンロードレピュテーション	◎		◎	◎	◎
		周辺機器 [デバイス] コントロール	◎		◎	◎	◎
		アプリケーションコントロール	◎		◎	◎	◎
		ブラウザ エクスプロイト防止		◎	◎	◎	
	デバイス上で実行前	マルウェアスキャン [ファイルスキャン]	◎		◎	◎	◎
		AI によるマルウェアスキャン [ディープラーニング]		◎	◎	◎	
		Sophos Live Protection	◎		◎	◎	
		実行前動作解析 / HIPS	◎		◎	◎	◎
		PUA [業務上不要なアプリケーション] のブロック	◎		◎	◎	◎
		データ流出防止	◎		◎	◎	
		エクスプロイト防止		◎	◎	◎	
検 出	脅威の実行を停止	ランタイム動作解析 / ランタイム HIPS	◎		◎	◎	
		不正な C&C との通信の検知 [MTD]	◎	◎	◎	◎	◎
		敵対行為に対するアクティブな抑止		◎	◎	◎	◎
		CryptoGuard [ランサムウェアによる暗号化防止]		◎	◎	◎	◎
		WipeGuard[ディスクとブートレコードを保護]		◎	◎	◎	
		MITB 保護 [セーフブラウジング]		◎	◎	◎	
対 応	調査と削除	Sophos Clean によるマルウェアの自動削除		◎	◎	◎	
		マルウェアの削除	◎		◎	◎	◎
		Synchronized Security [Security Heartbeat]	◎	◎	◎	◎	◎
		根本原因解析 [RCA]		◎	◎	◎	◎

※ Central Intercept X with Endpoint Advanced [バンドル] にて提供。今後シングルエージェントで提供予定。
注意：仮想クライアント [デスクトップ] の保護は、フルエージェントおよび軽量エージェントを利用できます。軽量エージェントである Sophos for Virtual Environments は、VMware ESXi および Microsoft Hyper-Vをサポートしています。Central Endpoint Protection、Central Intercept X、Central Intercept X Advanced では、サーバーOSは保護対象外となります。

Intercept X のエクスプロイト防止機能およびその他の防止機能の例

エクスプロイト防止	データ実行防止 [DEP：Data Execution Prevention]
	アドレス空間配置のランダム化 / 必須 ASLR
	Bottom-up ASLR [ボトムアップのランダム化]
	Null ページ [Null の間接参照対策]
	ヒープスプレーアロケーション
	ダイナミックヒープスプレー
	スタックピボット
	スタック実行 [MemProt]
	スタックベースの ROP 防止 [Caller]
	ブランチベースの ROP 防止
	SEHOP [Structured Exception Handler Overwrite]
	IAF [Import Address Table Filtering]
	Load Library
	Reflective DLL Injection
	シェルコード
	VBScript God Mode
	Wow64
	Syscall
	プロセス書き換え
	DLL ハイジャック
	Squiblydoo Applocker Bypass
	APC プロテクション [Double Pulsar / AtomBombing]
	プロセスの権限昇格
悪質なプログラムの確実な防止	認証情報盗難防止
	Code Cave 防止
	MITB 攻撃から保護 [セーフブラウジング]
	Meterpreter Shell Detection [Meterpreter シェル検出]

Sophos Central Server Protection / Sophos Central Intercept X Advanced for Server 機能表

		ライセンス	ライセンス別対応機能		OS 別対応機能	
		ライセンス名 / OS	Central Server Protection	Central Intercept X Advanced for Server	Windows	Linux
		ライセンス種類、カウント方法	サブスクリプション / サーバー OS 数			
防 止	攻撃対象領域の削減	アプリケーションのホワイトリスト化 [Server Lockdown]		◎	◎	
		Web セキュリティ	◎	◎	◎	
		Web フィルタリング [カテゴリ/ファイルベース]	◎	◎	◎	
		Windows ファイアウォールの制御	◎	◎	◎	
		ダウンロードレピュテーション	◎	◎	◎	
		周辺機器 [デバイス] コントロール	◎	◎	◎	
		アプリケーションコントロール	◎	◎	◎	
	デバイス上で実行前	マルウェアスキャン [ファイルスキャン]	◎	◎	◎	◎
		AI によるマルウェアスキャン [ディープラーニング]		◎	◎	
		Sophos Live Protection	◎	◎	◎	◎
		実行前動作解析 / HIPS	◎	◎	◎	
		PUA [業務上不要なアプリケーション] のブロック	◎	◎	◎	
		VM のオフボード型検索 [ESXi、Hyper-V 環境]2	◎	◎	◎	
		データ流出防止	◎	◎	◎	
		エクスプロイト防止		◎	◎	
検 出	脅威の実行を停止	不正な C&C との通信の検知 [MTD]	◎	◎	◎	◎
		敵対行為に対するアクティブな抑止		◎	◎	
		CryptoGuard [ランサムウェアによる暗号化防止]		◎	◎	
		WipeGuard[ディスクとブートレコードを保護]		◎	◎	
対 応	調査と削除	Sophos Clean によるマルウェアの自動削除		◎	◎	
		マルウェアの削除	◎	◎	◎	◎
		Synchronized Security [Security Heartbeat]	◎	◎	◎	◎
		根本原因解析 [RCA]	◎	◎	◎	
管 理	制 御	サーバー専用ポリシーの管理	◎	◎	◎	◎
		アップデートキャッシュとメッセージリレー	◎	◎	◎	
		検索から除外する項目を自動検出	◎	◎	◎	
		AWS / Azure との統合	◎	◎	◎	◎
		Synchronized Application Control	◎	◎	◎	
	可 視 化	Azure のワークロードの検出と保護	◎	◎	◎	◎
		AWS のワークロードの検出と保護	◎	◎	◎	◎
		AWS 地図、複数のリージョンの可視化	◎	◎	◎	◎
		Windows リモートデスクトップサービス [ユーザーの可視化]	◎	◎	◎	

攻撃者目線での多層防御

ソフォス製品と組み合わせることでより強固なエンドポイント保護を実現

サイバー キル チェーン [犯罪者の行動]	[内容]	対応する製品
偵察	標的とする企業の調査 [あらゆる情報を調査、特にIT情報]	
武器化	エクスプロイトコード [攻撃コード] と マルウェアの作成	
配送	なりすましメール等へ添付したり、または悪質な Web サイトに誘導し、マルウェアをドライブバイダウンロードさせる	XG Firewall / SG UTM / Email / Endpoint Protection
攻撃	添付のマルウェアを開かせる。または、Web サイトへ誘導し、脆弱性を利用するエクスプロイトコードを実行させる	Endpoint Protection / Intercept X ※
インストール	マルウェアがインストールされる。または、攻撃コードの実行により、インストールされる	Endpoint Protection / Intercept X ※
遠隔操作	C&C サーバーとの通信を確立させて PC を乗っ取る。マルウェア自体のバージョンアップ等も行う。	XG Firewall / SG UTM / Endpoint Protection / Intercept X
侵入拡大	機密情報を探す。また、他の PC やサーバー等にアクセスし、感染を拡大したり、機密情報を探し出す。	Endpoint Protection / Server Protection
目的実行	機密情報を送信する。HTTP / HTTPS / FTP などを利用して外部に送信する。	XG Firewall / SG UTM / Endpoint Protection / Intercept X

※ この段階での Endpoint Protection と Intercept X の機能は異なる検出テクノロジーであり、どちらか一方の製品で対応するわけではなく、2つの製品を組み合わせて利用する必要があります。

Sophos Central Device Encryption　クラウド管理型ディスク暗号化管理ソリューション

主な特長

1. 暗号化管理をシンプルに

- エンドポイントのフルディスク暗号化をシンプルかつ簡単にクラウドから設定／管理

2. OS のネイティブな暗号化機能を使用

- Microsoft BitLocker、Apple FileVault 2 デバイス暗号化
- デバイスの盗難・紛失時のデータ流出を防御

3. コンプライアンス対応のレポート／ダッシュボード機能

- エンドポイントの情報を集約表示するレポート機能
- 警告を表示し現状の管理対象全体の概要を表示するダッシュボード機能

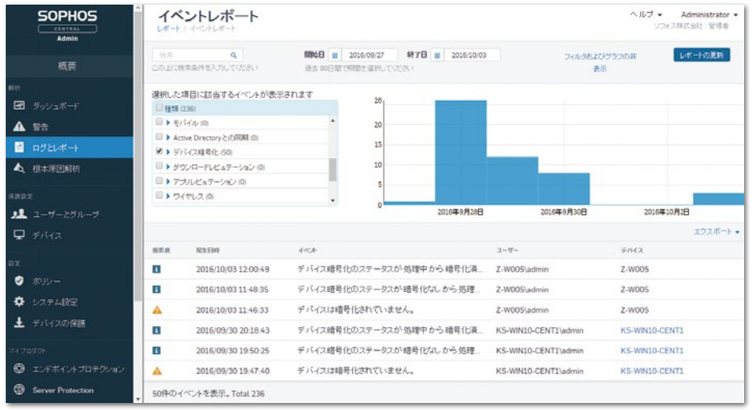
4. Self Service

- ユーザーが PIN/ パスワードを忘れた際に、自分で復旧キーを取得できる Self Service により、TCO を削減

機能紹介

デバイス暗号化ポリシー設定画面

レポート画面



ライセンス

Central Device Encryption

Sophos Mobile クラウド管理型 UEM ソリューション

主な特長

1. モバイルデバイス管理

- わかりやすい管理コンソールとダッシュボード
- インベントリ管理と資産管理
- リモートからポリシー配布
- 紛失および盗難からの保護
- コンプライアンス確認および是正
- セルフサービスポータル
- iOS, Android, Windows 10 Mobile, Windows 10 desktop, macOS をサポート

2. モバイルアプリケーション管理

- リモートからのインストールと削除
- インストール済みアプリ一覧の管理
- ブラックリスト / ホワイトリスト / 必須アプリ設定によるポリシー違反検知
- エンタープライズ アプリ ストア
- アプリケーション コントロール

3. モバイルコンテンツ管理

- 安全な文書ファイルの配布
- 安全な Sophos コンテナ
- ネイティブ OS コンテナの管理
- メールを集中管理
- モバイルデバイス上に「セキュアコンテナ」を作成し、メール、予定表、連絡先を格納

4. モバイルセキュリティ

- フィッシング対策 (Android)
- マルウェア対策 (Android)
- Web コンテンツフィルタリング対策 (Android)
- 危険なサイトへのアクセスブロック (Android)

5. 統合エンドポイント管理

- 単一の管理プラットフォームから MacOS、Windows、その他のモバイル・エンドポイントを管理・保護
- 一貫したセキュリティポリシーを適用でき、リソースへの安全なアクセスが可能
- MacOS の管理と設定、Windows 10 のアプリケーション管理など。

機能紹介

モバイルセキュリティ

ライセンス

ライセンス	Central Mobile Advanced	Central Mobile Standard	Central Mobile Security
モバイルデバイス管理 (MDM)	◎	◎	AV only
モバイルアプリケーション管理 (MAM)	◎	◎	
モバイルコンテンツ管理 (MCM)	◎		
モバイル E-Mail 管理	◎		
モバイルセキュリティ管理	◎		◎
統合エンドポイント管理 (UEM)	◎	◎	
セールスサービスポータル	◎	◎	

Sophos Central Email クラウド管理型 E メールセキュリティソリューション

主な特長

1. セキュリティ管理をシンプルに

- クラウド型の管理コンソールでどこからでもアクセス
- グローバルに配置されたデータセンターで高可用性を実現

2. 実績のあるアンチウイルスエンジン

- 信頼性の高いメールアンチウイルスエンジン。OEM として複数のベンダーも採用
- 最新のマルウエア・スパム対策、フィッシング攻撃対策で、最新型脅威から保護

3. クラウド型メールサービスとの連携

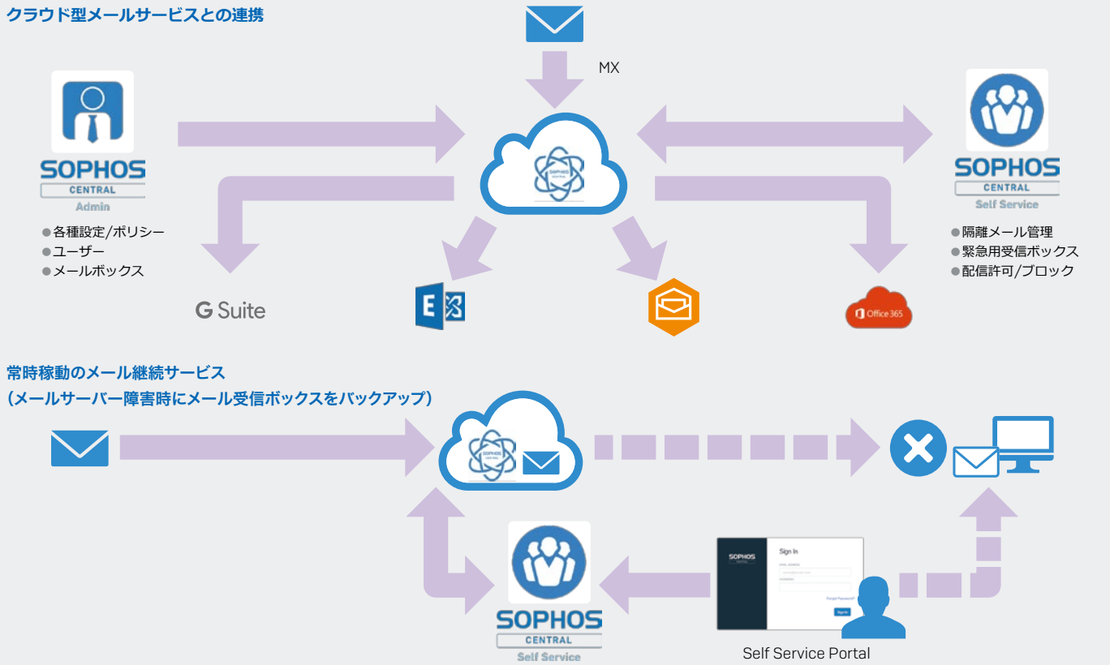
- Office 365 , G Suite などの主要なメールサービスとシームレスな連携
- クラウド型メールサービスのセキュリティを強化

4. 常時稼動のメール継続サービス

- エンドユーザーのセルフサービスポータル画面から隔離メールを管理
- スプーリング機能、緊急用受信ボックス機能で非常時のメールサービスを提供

機能紹介

クラウド型メールサービスとの連携



ライセンス

	Sophos Email Standard	Sophos Email Advanced
Microsoft Exchange 2003 以降、Office 365 、Google Apps 他	○	○
高度なマルチレイヤー スパム フィルタリング	○	○
企業用許可/ブロックリスト	○	○
エンドユーザー向けセルフサービスポータル / メール隔離エリア	○	○
障害時にメールを蓄積、再配信するスプーリング機能	○	○
ユーザーが常時アクセスできる緊急用受信ボックス	○	○
エンドユーザー用許可/ブロックリスト*	○	○
フィッシング URL 検出	○	○
SPF、DKIM によるなりすまし対策	○	○
メール添付ファイルのフィルタリングポリシー		○
Time-of-Click URL Protection		○
Sophos Sandstorm（クラウド型AIサンドボックス）		○

Sophos Phish Threat フィッシングメール攻撃シュミレーション

主な特長

1. クラウド型フィッシングメール攻撃シュミレーション

- スピアフィッシングやソーシャルエンジニアリングなどの多彩な攻撃のシュミレーション
- 組織におけるセキュリティ上の弱点を識別

2. オンデマンドで実施できるフィッシングメール対策トレーニング

- 簡単に作成できるキャンペーン
- 定期的に更新される模擬攻撃用テンプレートを多数用意

3. 模擬攻撃を見分けられなかった従業員個人に合わせたトレーニング

- 安効果的なトレーニングモジュール
- 従業員にとって興味深い特定の脅威について教育できるように設計

4. 模擬攻撃やトレーニング結果のレポートを自動的に作成

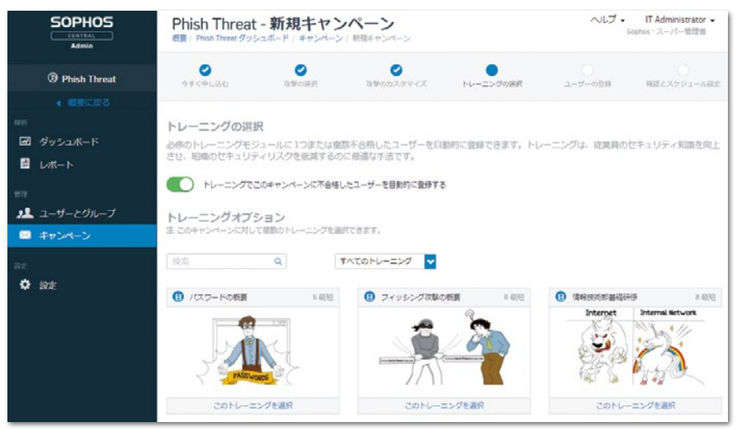
- 包括的なレポート機能
- 会社全体のセキュリティレベルの状況を詳細に把握

機能紹介

フィッシングメールキャンペーンメニュー

トレーニングメニュー

Central Phish Threat



Sophos Wireless クラウド管理型ワイヤレスソリューション

主な特長

1. いつでもシンプルに展開

- アクセスポイントへの設定は不要
- 設置してネットワークに接続後に設定データがクラウドより配信され自動的に適用

2. わかりやすい管理インターフェイス

- ダッシュボードによる状態確認
- Google Map 連携による拠点管理
- 通信カテゴリ別の利用状況の把握

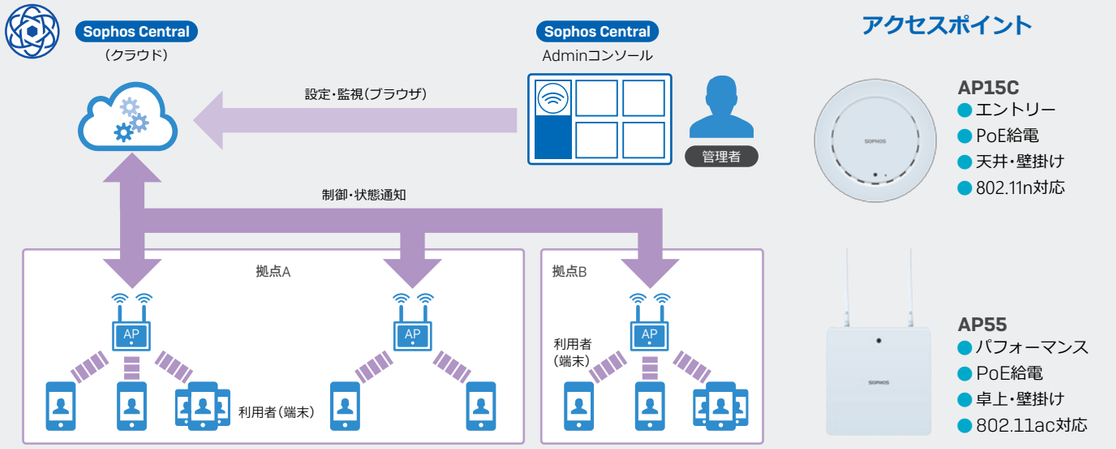
3. AP 設置をシミュレーション

- 設置するフロア図面をアップロード
- アクセスポイントを図面上にドラッグし電波到達範囲等を確認しながらプロット可能

4. 高度なセキュリティ機能

- アプリケーション識別及び制御（将来対応）
- モバイルデバイス管理ソリューションとの連携による高度なアクセス管理（将来対応）

全体構成



アクセスポイント

AP15C
- エントリー
- PoE給電
- 天井・壁掛け
- 802.11n対応

AP55
- パフォーマンス
- PoE給電
- 卓上・壁掛け
- 802.11ac対応

機能紹介

機能名① ダッシュボード・利用状況可視化

機能名② サイトプランニング

ライセンス

Sophos Wireless Standard (for AP15C) / Sophos Wireless Standard (for AP55) / Sophos Wireless Standard (for APX)

販売パートナー

お問い合わせ

ソフォス株式会社

〒106-6010　東京都港区六本木1-6-1 泉ガーデンタワー10F　Email sales@sophos.co.jp

最新の情報はソフォスホームページをご覧ください www.sophos.com/ja-jp

セキュリティ記事を掲載中 Twitter: @sophosjpmktg /　Facebookページ: https://www.facebook.com/sophosjpmktg

1904_CH(09)