

# ソフォス 総合カタログ

(オンプレミス / SaaS / Sophos UTM / Sophos XG Firewall)





# 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 10万以上の企業と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

クリス ヘイゲルマン Kris Hagerman

### 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 2,300 名以上(全世界)

# ソフォス株式会社

### 代表取締役社長

ニコラス・ポール・シートン・ブレイ

### 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。



### SC Manazine Awards 2016 Europe

**Best UTM Solution** 

WINNER: Sophos UTM SG Series を受賞



Highly Commended: Sophos Cloud Web Gateway を受賞

### **Best Emerging Technology**

Sophos Security Heartbeat にノミネート

引用: http://www.scawardseurope.com/results-2016/

# AV-TEST AWARD BEST PROTECTION 2015

Product: Sophos Mobile Security

引用:

https://www.av-test.org/en/award/2015/best-protection-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。

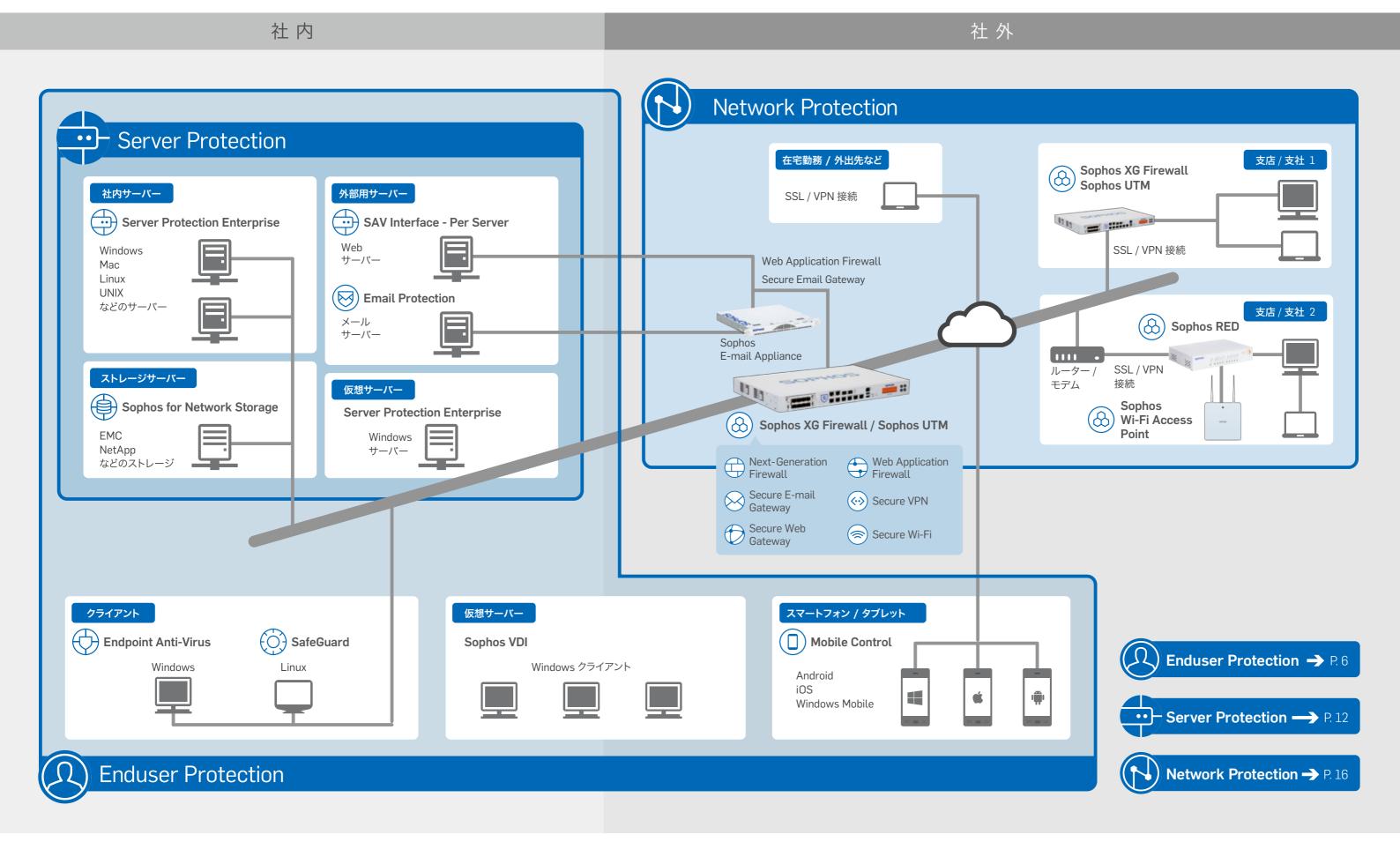
### 国内約 3,500 社以上

岩波書店、大興電子通信、サングループ、講談社、芝浦工業大学、新日鉄ソリューションズ、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、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 Products and Solutions Map



### **Endpoint Protection**

### 主な特長

▲ 合理的なウイルス対策

Linux や UNIX など業界最多 25 種類以上の OS をサポートするウイルス対策ソフト (UNIX 保護は Server Protection Enterprise を別途購入)

2. 異なる OS でも一元管理

Windows / Mac / Linux の セキュリティ状況を一目で把握

3. 未許可ソフトは使用禁止!

アプリケーション コントロール機能で 業務に関係ないソフトの使用を制御

4. データの持出し/持込みを阻止

USB メモリ等のデバイスを種類(型番)や 固有シリアル ID で識別し使用を制御 スマホなどのデバイスへのデータ転送 (MTP/PTP) を制御 り. リアルタイムの脅威対策

定義ファイル反映前のウイルスをクラウド上の データベースで確認 & 危険なサイトへのアクセスを阻止!

6. ストレージサーバーの保護対策

多数のユーザーがアクセスするストレージは、ウイルスの 拡散ポイントにならないように。 また、バックアップ ファイルを信頼できるものにする必要があります。

/ . 社内外問わず安全な Web 閲覧

業務上不適切な Web サイトへのアクセスを阻止し、 ウイルス感染のリスクを軽減

8. 確実なパッチ適用で脆弱性対策

クライアント PC におけるアプリケーションの セキュリティパッチの適応状況を把握(60種類以上)

### 機能紹介

# 

### アプリ・OS の脆弱性

◎アプリケーションコントロール◎パッチアセスメント



### 安全な Web アクセス

◎ Web フィルタリング (URL)◎ Web コンテンツフィルタリング



### ウイルス対策

◎コード実行前 / ランタイム検知◎クラウドベースのウイルス検知

### アプリケーションコントロール

### 未許可アプリは使用禁止!

◎ P2P やインスタントメッセージ、ゲームなど、業務に関係のないアプリケーションの使用による生産性の低下を防ぐ

◎業務に関係ないアプリを使用禁止にすることで、脆弱性自体の数を減らし、データ流出から保護

### パッチアセスメント

### 複雑なパッチ管理作業を効率化

◎ SophosLabs がパッチの重要度評価し、管理画面で簡単に把握可能 **多くのアプリケーションに対応** 

© Adobe、Apple、Microsoft、Oracle など、60 製品以上のパッチに対応

### 確実なパッチ適用で脆弱性対策

◎パッチが適用されていないクライアント PC を検出、管理者に通知

# パッチアセスメント Microsoft Adobe VMware Apple SophosLabs が 60 種以上 の パッチ情報を収集し重要度を評価 パッチの適応状況を把握 クライアント PC をスキャン クライアント PC

### Web コンテンツフィルタリング

### 業務生産性の向上

◎接続場所を問わず、業務上不適切な Web サイトへのアクセスを ブロックまたは警告表示

### マルウェア感染のリスクを軽減

©マルウェアが仕掛けられやすい Web サイト (アダルト、犯罪等) への アクセスをブロック

### シンプルな導入

◎ゲートウェイ製品を使用せずに、エンドポイントだけで実現

### Sophos Live Web フィルタリング

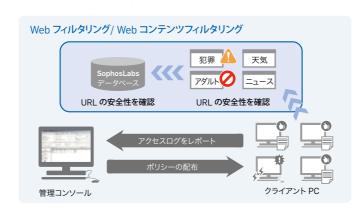
### 有害サイトからの保護

◎ SophosLabs が把握している最新の有害サイトの情報データベースで 瞬時に確認

### 接続場所を問わない保護

◎定義ファイルをアップデートできない環境でも、クラウドで確認 ブラウザを選ばない

◎ IE, Firefox, Safari, Opera, Chrome など主要なブラウザに対応



### **Sophos Live Anti-Virus**

クラウド型のデータベースを参照し最新の脅威から保護

ゼロデイ攻撃を阻止

◎定義ファイル反映前のマルウェアでも瞬時に検出

脅威データベースの充実

◎ユーザーから収集した脅威情報をデータベースに反映

アップデート負担の軽減

◎定義ファイルのアップデートを軽快に

### **Malicious Traffic Detection**

### C&C サーバーとの通信をブロック

◎不正なコマンド & コントロールサーバーが、侵入した不正なプログラムに指示を出す通信をブロック

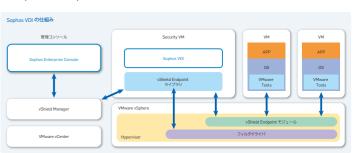
◎これにより、万が一不正なプログラムが侵入した場合でも、外部へのファイルや情報の送信を事前にブロック

### Sophos VDI (個別製品)

VMware vShield Endpoint 利用したエージェントレスマルウェア対策 ◎スキャンストームとアップデートストームの問題を回避し、

集約率をアップ。

◎ Sophos Enterprise Console で一元管理可能



# **②** エンドポイントでの情報漏えい対策

### デバイスコントロール

### データの持出し、持込みを阻止

- ◎ USB メモリ等のデバイスを種類(型番)や固有シリアル ID で識別し、 使用を制限することで情報流出を防ぐ
- ◎ MTP / PTP などのプロトコルを制御し、PC に接続したデバイス等への データの転送をブロックし、情報漏えいを防ぐ
- ◎ オートラン機能を防止し、Conficker のようなリムーバブルストレージを 感染手段とするマルウェアを阻止

### **ライセンス**

機能	Endpoint Protection Advanced	Sophos Clean	Endpoint Protection Standard
ライセンス	サブスクリプション		サブスクリプション
集中管理	•		•
ポリシー策定・配布	•		•
レポート	•		•
マルウェア対策	•		•
対応 OS	Windows / Mac / Linux		Windows / Mac
振る舞い検知 (HIPS) 注(1)	•		•
Sophos Live Antivirus 注(2)	•		•
Sophos Live Web Filtering 注(3)	•		•
クライアントファイアウォール <sup>注(4)</sup>	•		•
アプリケーションコントロール <sup>注(1)</sup>	•		•
デバイスコントロール <sup>注(3)</sup>	•		•
Web コンテンツフィルタリング 注(1)	•		•
Malicious Traffic Detection 注(1)	•		
パッチアセスメント <sup>注(1)</sup>	•		
仮想化対応 注(5)	•		•
Sophos for Network Storage 注(6)	•		
PureMessage for MS Exchange	•		•
自宅使用ライセンス	•		•
シグネチャーレス型マルウェア対策 <sup>注(1)</sup>		•	
ロールバック機能 注(1)		•	
注(1) Windows のみ、 注(2) Windows / Mac / Li	inux、 注(3) Windows / Mac、 注(4) Windows	dows クライアントOS のみ、	

注(1) Windows のみ、注(2) Windows / Mac / Linux、注(3) Windows / Mac、注(4) Windows クライアントOS のみ、注(5) 仮想化上のホストOSにインストールできます。vShield 環境への導入は別売の Sophos VDI (仮想クライアント用) および Server Protection Enterprise (仮想サーバー用) が必要になります。

注(6) EMC / NetApp / ICAP 対応のNAS (SUN Storage や Hitachi Data Systems など) を保護可能。

# 単体ライセンス

Sophos VDI

### バンドルライセンス

バンドルライセンスは、ライセンス一覧をご覧ください。

### 自宅使用ライセンス

契約したライセンス数を上限台数とし、ウイルス対策機能を自宅コンピュータにも拡張してご使用頂けます。

# SafeGuard Enterprise / SafeGuard

### 主な特長

### ▲ 一元管理による管理コストの削減

◎1つの管理コンソールで、各モジュールと鍵を管理◎カスタマイズ可能なレポート

- ◎利用用途に応じた、モジュール導入
- ◎BitLocker / FileVault 2 で暗号化された PC の管理

# 2. 利用形態に合わせた暗号化

◎ファイル/ フォルダベースの暗号化

- ◎ハードディスクの暗号化
- ◎デバイスの暗号化
- ◎BitLocker / FileVault 2 で暗号化

# 3. 緊急時の簡単な復旧

◎チャレンジレスポンス

◎ユーザー自身で復旧できるローカルセルフヘルプ

### 4. 暗号化ポリシーと監査ログ

◎適切な暗号化ポリシーの適用

◎利用状態を把握する監査ログ

# 5. 信頼された暗号化テクノロジー

◎多く政府機関、民間企業に導入 ◎さまざまな暗号化関連の認定を取得

# 6. 暗号化データの安全な共有

- ◎高度な鍵リングによる暗号化データの共有
- ◎クラウド上の情報の保護
- ◎ IT 管理者を含めた全ユーザーのアクセスを管理

### 機能紹介

# ② 暗号化による情報漏えい対策

### 管理とポリシー

◎単一コンソールでの集中管理◎ポリシーの策定と配布



### 盗難•紛失対策

◎ハードディスクの暗号化◎リムーバブルメディアの暗号化

◎仮想ドライブの暗号化



### データの保護

◎ファイルベースの暗号化◎共有ファイルの暗号化

◎クラウド上のデータの暗号化

### 単一コンソールからの集中管理

ハードディスク全体の暗号化

を実現

- ◎複数鍵を効率的に管理
- ◎グループごとのユーザーのポリシーをきめ細かく設定・適用
- ◎すべてのデバイスの最新のセキュリティ状況を把握
- ◎暗号化されたデータを安全に保存、交換、および復旧が可能

◎ノート PC、デスクトップ PC、仮想化マシンのフルディスク暗号化

◎パスワード、トークン、生体認証などを使用する起動前認証が可能

◎ OS 起動時の復号化の認証 と Windows 認証でシングルサインオン

可能 (チャレンジ & レスポンス / ローカルセルフヘルプ)

◎パスワード忘れの際、管理者に依頼することなくユーザー自身で復旧

◎高速の暗号化アルゴリズムを使用し、暗号化 ⇔ 復号化を瞬時に実行

### クラウド上にある情報の暗号化

- ◎ Dropbox、OneDrive、Egnyte、Google Drive などに対応◎認可されたユーザーのみが、暗号化されたドキュメントを閲覧
- Jiぶりされにユーリーのみが、暗ち化されにトキュメントを (サービス提供事業者でも閲覧は不可)
- ◎スマートフォンやスマートデバイスでも、暗号化ドキュメントを閲覧可能◎同機能がインストールされていないデバイスでも、専用のポータブル アプリケーションで暗号化データにアクセス可能

### ファイルの保護

- ◎ IT 管理者によるファイルへのアクセスをブロック
- ◎ファイルの転送や、デバイスへコピーされた場合でも、許可されて いないユーザーによる復号化を防止
- ◎サーバーへアップロードする際の情報流出を防止
- ◎ファイルやディレクトリのアクセスコントロールには依存しない
- ◎暗号化されたファイルに対し、フェイルセーフ リカバリを提供
- ◎独自のキーリング機能で、プロジェクトチームレベルでも全社レベルでも、 データを安全に共有および移動

### リムーバブルメディアの暗号化

◎リムーバブルメディアにファイルをコピーする際に、自動的に暗号化◎共通の暗号化基盤がなくても安全な方法で社外とデータ交換可能

### BitLocker / FileVault 2 で暗号化された PC を管理

- ◎ OS に搭載の暗号化エンジンにより暗号化された PC を管理
- ◎暗号化の状態の把握や鍵の管理、SafeGuard Management Center からの復旧が可能





### ライセンス

# ② 単体ライセンス (パーペチュアル)

SafeGuard Enterprise	Windows	Mac
ハードディスク暗号化	SafeGuard Device Encryption	SafeGuard Disk Encryption for Mac
リムーパブルメディア暗号化	SafeGuard Data Exchange	
共有ファイル暗号化	SafeGuard Encryption for File Shares	SafeGuard File Encryption for Mac
クラウド ストレージ暗号化	SafeGuard Encryption for Cloud Storage	
OS 標準の暗号化エンジンの利用と管理	SafeGuard Native D	Device Encryption *1

※1 BitLocker / FileVault2 で暗号化された PC の管理

# 

オールインワン Sai

SafeGuard Enterprise Encryption (サブスクリプション / パーペチュアル)

ハードディスク暗号化

SafeGuard Disk Encryption Advanced (サブスクリプション)

( SafeGuard Device Encryption  $ext{ } ext{ } ext$ 

ファイル暗号化

SafeGuard File Encryption Standard (サブスクリプション) SafeGuard File Encryption Advanced (サブスクリプション) SafeGuard File Encryption (パーペチュアル)

バンドルライセンスは、ライセンス一覧をご覧ください。

この他 SafeGuard 単体製品もご用意しております。

詳細は ソフォス営業部 03-3568-7550 / sales@sophos.co.jp までお問い合わせください。

# Sophos Mobile Control (オンプレミス / SaaS)

### 主な特長

# 1. Exchange サーバーへのアクセス管理

SMC サーバーを ActiveSync Proxy として利用し、デバイスからの Exchange サーバーへのアクセスを管理

©コンプライアンス準拠のデバイスのみアクセスを許可

©コンプライアンスをチェックJailbreak / root 化検知、パスワード設定、OS バージョン、更新間隔、ブラックリスト/必須アプリ、など

©メールサーバーなどの設定をデバイスに配信

# 2. 盗難・紛失デバイスの管理

◎SIM カード差し替えの通知

デバイスの盗難・紛失の事前対策と事後対応でデータの 安全を確保可能

◎管理デバイスにパスワード、パスコードポリシーを強制◎デバイスの位置情報を取得◎遠隔からデバイスのロックまたは、データ消去

# 3. アプリの管理

導入済みアプリの確認やアプリの配布が可能

◎アプリのインストールを禁止する (iOS)

◎デバイスの棚卸:機種名、OS、キャリア、導入済みアプリなど◎Enterprise App Store による社内アプリの配信◎Android アプリのリモート・インストール/アンインストール

◎必須アプリ・ブラックリストアプリの確認と通知

# 4. IT 部門への負荷を削減

そのままでユーザーへ一部の操作の権限委任と、

一箇所からの端末の管理、状態確認が可能

◎デバイスのユーザーは、セルフサービスポータルから 自分のデバイスの登録、ロック、データの消去が可能

◎ネットワーク経由での管理アプリ、設定、ポリシーの配信が可能 ◎ヘブパイスの情報。コンプライアンス洗料の外沿方

◎全デバイスの情報、コンプライアンス準拠の状況をひとつの管理画面から確認可能

### 機能紹介

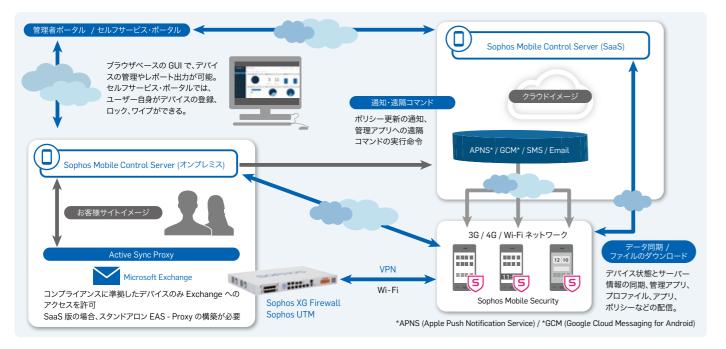
Sophos Mobile Control (SMC) は、スマートフォンやタブレットなどを管理するモバイルデバイス管理\* ソリューションです。

iOS、Android、Windows Mobile などのさまざまなモバイルデバイスを一元管理できます。

※ モバイルデバイス管理 (Mobile Device Management = MDM) ・・・・特に企業・組織で使用するモバイルデバイスを管理システムに登録することで、盗難・紛失時の遠隔消去、利用者やアプリケーション情報収集、パスワード設定強化などを管理できるシステム。

Sophos Mobile Security は、Android 向けのマルウェア対策が可能なモバイルセキュリティソリューションです。

# ② ユーザー自身でセキュリティ管理



### ライセンス

単体ライセンス Sophos Mobile Control Standard (オンプレ版) Sophos Mobile Control as a Service Standard (SaaS 版) Sophos Mobile Control Advanced (オンプレ版) Sophos Mobile Control as a Service Advanced (SaaS 版)

※ Sophos Mobile Control Advanced、および Sophos Mobile Control as a Service Advanced では、Sophos Mobile Security を利用できます。

**バンドルライセンス** バンドルライセンスは、ライセンス一覧をご覧ください。

# Customize Solution

### Sophos Anti-Virus Interface / Sophos Anti-Virus Dynamic Interface / Sophos Anti-Spam Interface

### ソフォス製品 API の紹介

Sophos Anti-Virus Interface (SAVI)
Sophos Anti-Virus Dynamic Interface (SAVDI)
社内の独自アプリケーションに組込み可能な API

### 最新のマルウェア対策技術を提供

- ◎ Behavioral Genotype (振る舞い検出型遺伝子脅威検知)技術で送受信されるすべてのWebトラフィックや電子メールトラフィック (圧縮された添付ファイルを含む)に含まれる脅威をプロアクティブに阻止◎ 万物性のあるゲートウェイ アプリケーショントで、電子メールトラフィック
- ◎互換性のあるゲートウェイ アプリケーション上で、電子メール トラフィック、 Web トラフィック、および FTP トラフィックをリアルタイムで監視

### 高速かつ効率的なパフォーマンス

◎コマンドラインインターフェイスから実行する従来のスキャンアプリケーションに比べ、20~30倍の高速スキャンで、エンドユーザーの生産性を維持◎ソフォスのウイルス検出エンジンはマルチスレッド型であり、1つのインスタンスですべての要求を処理できるため、メモリの効率的な使用が可能

### 簡単な統合と管理

◎自社の IT 環境とスキルに合わせて、統合の方法と使用言語を選択可能 ◎自動化されたレポート機能で、IT 管理者の負担を軽減

# 活用例 1: Web アプリケーションサーバー SophosLabs サードパーティー製品

- 1 クライアントがファイルをアップロードする
- ② マルウェアがないかを SAVI や SAVDI を利用して、アプリケーションサーバー側で スキャンする
- ③ 安全なファイルであれば、アプリケーションサーバーで活用

### Sophos Anti-Spam Interface ( SASI ) 社内の独自アプリケーションに組み込み、スパムチェック

### 多様なゲートウェイ機能を提供

◎ Email セキュリティ、Email 管理、Web フィルタリング、IM フィルタリング、ファイアウォール

### 最新のスパム対策技術

◎プロアクティブな Genotype テクノロジー◎送信者のレピュテーションデータベース照合確認 (ボットネットやゾンビ PC の識別を含む)

◎ SophosLabs による 24 時間 365 日のグローバルな脅威監視体制

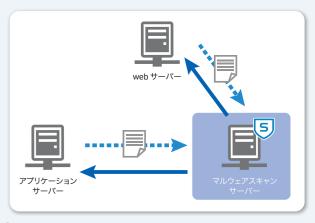
### IP Reputation Service と連動

◎最適なパフォーマンスのために、接続レベルで IP Reputation Service を 導入し、コンテントインスペクションレベルで SASI を導入

### ダブルバイト文字を含め、多言語のメールに対応

◎グローバルに展開する企業でのスパム対策に効果的

# 活用例 2:集中型マルウェアスキャンサービス



- ❶ 各サーバーがファイルやデータのスキャンをスキャンサーバーへ依頼
- ② スキャンサーバーが依頼のあったファイルやデータをスキャンする
- ③ スキャンサーバーからの結果を受け取り、安全なファイルやデータであれば、各サーバーで活用する
- ※ 軽量化に焦点を当てた、リアルタイムチェックを行うエンジンも用意しております。 ※細けも問い合わせ下さい。

# **Server Protection Enterprise**

### 主な特長

# 🗘 サーバーにおけるウイルス対策の必要性

クライアント PC にウイルス対策製品を導入していても、サーバーにマルウェアが潜んでいると、知らないうちにウイルスの感染を 拡大させてしまう(ウイルスの配布ポイント)可能性があります。

また、Windows 系以外のマルウェアも存在し、特にサーバーでは、Linux サーバー上で、Windows 系のウイルスを

見つけるというような異なるプラットフォーム間での検出が重要です。

ソフォスのウイルス対策製品は Windows、Mac、Linux、UNIX で統一した定義ファイルを利用し、さまざまなウイルスからサーバーを保護できます。

# Linux / UNIX サーバーに、ウイルス対策製品を導入していない理由

### 1. Linux や UNIX のウイルスが少ないため

Windows 系のウイルスに比べると数は少ないが、Linux / UNIX 系のウイルスも存在。 Windows 系のウイルスは、Linux サーバーで動作はしませんが、他の Windows シ ステムに配布しないように、ウイルス対策は必要。

### 2. 利用中のウイルス対策ベンダーの製品が対応していない

Server Protection では、業界最多の OS に対応。 ウイルス対策製品が見つからない場合は、ソフォス営業部までご連絡ください。 政府機関の情報セキュリティ対策のための統一基準 (第4版) 2.1.2.2 不正プログラム対策

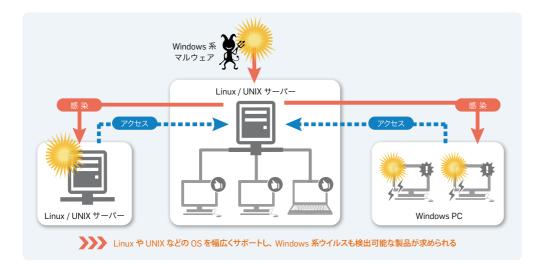
遵守事項

(1) 情報システムの構築時 【基本遵守事項】

- (a) 情報システムセキュリティ責任者は、電子計算機(当該電子計算機で動作可能 なアンチウイルスソフトウェア等が存在しない場合を除く。以下この項において 同じ。)にアンチウイルスソフトウェア等を導入すること。
- (b) 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路のすべ てにおいてアンチウイルスソフトウェア等により不正プログラム対策を実施すること。 出典:http://www.nisc.go.jp/active/general/pdf/K303-081.pdf

# ウイルス対策製品を導入しなかった場合のリスク

社内 / 社外にサービスを提供している Linux や UNIX サーバーに Windows 系 のウイルスが侵入している場合、そのサー ビスを利用している Windows ユーザーの PC に感染させてしまうことも! Windows 系ウイルスは、Linux / UNIX では感染し ないので、管理者は気付きにくい。



# ♀ 標的型攻撃で使われる C&C サーバーとの通信を防ぐには ?

### **Malicious Traffic Detection**

◎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

### ライセンス

### **Server Protection Enterprise**

社内・社外向けの Windows / Linux / UNIX サーバーの保護 VMware vShield で動作する仮想サーバーの保護

### SAV Interface - Per Server

SAV Interface (SAVI) / SAVDI を利用したマルウェア対策保護 (社外向け・不特定多数が利用)

### **SAV Interface**

SAV Interface (SAVI) / SAVDI を利用したマルウェア対策保護

# Sophos VDI

### 主な特長

### ▲ 各仮想マシンには ウイルス対策エージェントは不要

◎導入作業が簡単、素早くセキュアな状態に ◎各仮想マシンのパフォーマンス低下を防止

# 2. Security VM (セントラルスキャナ) が 各 VM のスキャンを実施

- ◎セントラルスキャナを常に最新の状態にしておけば、 各仮想マシンも最新の状態でスキャン
- ◎定義ファイル、エンジンのアップデートを効率化 (アップデートストームを回避)
- ◎自動でスキャンを段階的に実施(スキャンストームを回避)

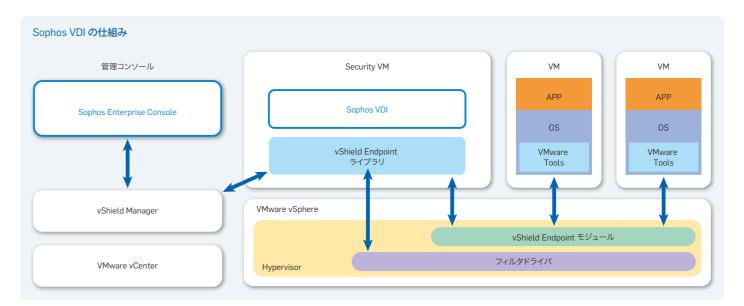
# 3. 仮想環境における リソースの有効活用を実現

◎サーバーのリソース消費を抑制(マシン集約率の向上)

# 4. Sophos Enterprise Console で Security VM を集中管理

- ◎単一の管理コンソールで、すべての仮想 / 物理プラットフォーム
- ◎各仮想マシンのセキュリティステータスを一目で確認

### 機能紹介



### **ライセンス**

### ゲストサーバー用: Sophos VDI が利用できるライセンス

Server Protection Enterprise

### ゲストクライアント用: Sophos VDI が利用できるライセンス

Sophos VDI

※保護対象となるゲスト OS は、VMware Tools が対応する Windows OS のみになります。

### Sophos for Network Storage

### 主な特長

# ストレージにおけるウイルス対策の必要性

### 1. ウイルス拡散ポイントにならないために

多数の社内ユーザーがストレージにアクセスするため、感染したファイルが アップロードされると、そのファイルを経由し全社感染の恐れがあります。



### 3. ガイドラインに準拠するために

政府機関の情報セキュリティ対策のための統一基準 - 内閣官房情報セキュリティセンター 【基本遵守事項】

「情報システムセキュリティ責任者は電子計算機(当該電子計算機で動作可能なアンチウイル スソフトウェア等が存在しない場合を除く)にアンチウイルスソフトウェア等を導入すること」

「電子計算機」とは、コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。

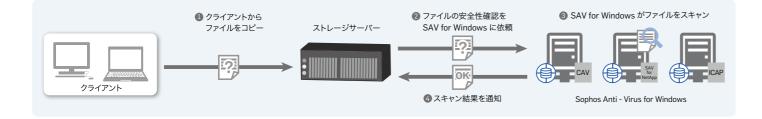
出典:「政府機関の情報セキュリティ対策のための統一基準」 http://www.nisc.go.jp/active/general/kijun01.html

### 2. バックアップデータを信頼できるものに

感染されたファイルを含むバックアップデータは使えなくなり、必要とされる データの復元に影響を与える可能性があります。



### 推奨される利用例



### ライセンス

### Sophos for Network Storage

ストレージサーバーにおけるマルウェア対策と統合管理、自動アップデート。

### ライセンスに含まれるソリューション

O Sophos Anti-Virus for NetApp

NetApp のストレージがスキャン対象のファイルをスキャンサーバー (Sophos Anti-Virus for Windows と Sophos Anti-Virus for NetApp が インストールされたサーバー ) に渡して、ウイルス検索を実行。

◎ EMC Celerra / VNX / VNXe 向けウイルス対策ソリューション FMC のストレージがスキャン対象のファイルをスキャンサーバー

EMC のストレージがスキャン対象のファイルをスキャンサーバー (Sophos Anti-Virus for Windows と CAVA(Celerra Anti Virus Agent が インストールされたサーバー) に渡して、ウイルス検索を実行。

◎ Hitachi Data Systems (ICAP 連携)向けウイルス対策ソリューション ICAP と連携したストレージシステムが、スキャン対象のファイルをスキャンサーバーに渡してウイルス検索を実行



### 主な特長

# → ウイルス、スパムメールを高精度でブロック

- ◎スパム情報をリアルタイムで更新する Sophos Live Anti-Spam によって 99 % 以上のスパムをブロック。
- ◎既知 / 未知のウイルス、トロイの木馬、その他の脅威を阻止
- ◎ Web ベースのコンソールからユーザー自身が隔離アイテムを処理
- ◎ Outlook プラグインを使用してユーザーは簡単にスパムの 報告・提出が可能

# 2. メールの隔離と管理

◎サーバーステータス、レポート、ポリシーの表示◎コンテンツ検閲ルールとセキュリティポリシーの設定◎警告および隔離アイテムの管理

◎ロールベースの管理

◎マルチテナントのグループ構成

### 機能紹介

# **♀** リアルタイムのスパム対策 (PMU のみ)

### Sophos Live Anti-Spam

◎クラウド型サービスを利用して、リアルタイムでスパムを検出◎メールボックスへの侵入を防止◎新しい脅威がメールサーバーに到達する以前に、

◎新しい脅威がメールサーバーに到達する以前に ゲートウェイでブロック

# 

### **Sophos Sender Genotype**

○ IP アドレスやトラフィックに含まれるストリングなどの特性から ボットコンピュータをプロアクティブに検知してブロック○過去に一度もスパムを配信したことのないボットからのメールであって も、ブロックすることが可能

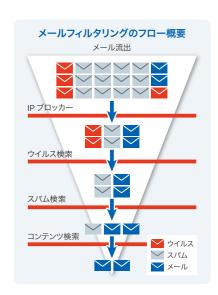
### 製品紹介

### ソフトウェア製品

企業のプラットフォームに合わせて 2 種類から選択。

PureMessage For Exchange

PureMessage For UNIX



### ライセンス

### **Sophos Email Protection Advanced**

メールマルウェア対策、迷惑メール対策、メールポリシー策定、 自動アップデート

スペック	PureMessage For Exchange	PureMessage For UNIX
提供形態	ソフトウェア	ソフトウェア
管理コンソール	•	•
マルウェア対策	•	•
スパム対策(コンテンツ/キーワード)	•	•
スパム対策(SXL)		•
スパム対策(Sender Genotype)		•
ルーティング(ポリシーに基づく)	•	•
データ流出防止(ファイル制御)	•	•
データ流出防止(キーワード制御)	•	•

# Sophos UTM / Sophos RED / Sophos Wi-Fi Access Point

### 主な特長













1. 優れたユーザビリティ

直感的に理解できるブラウザベースの GUI で、 専用のソフトウェアやコマンドラインでの管理が不要

# 2. 優れた防御力

エントリーモデルからハイエンドモデルまで プラットフォームによる機能制限なく様々なセキュリティ機能を提供

# 3. 優れた柔軟性と拡張性

環境にあわせて必要な機能のみ利用できるライセンス体系で提供製品はハードウェア/ソフトウエア/仮想アプライアンスと全てのプラットフォームに対応

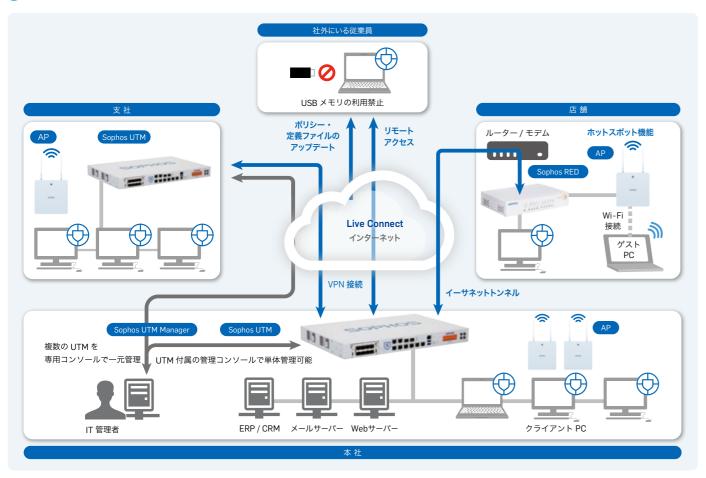
### 管理画面

### Sophos UTM 管理画面



# 機能紹介

# 



### 製品紹介

### 単一アプライアンス製品

ハードウェア / ソフトウェア / 仮想 アプライアンス (VMware, Hyper-V, KVM, Xen, AWS など) からビジネスに最適なプラットフォームを提供。

### Sophos SG シリーズ



### 全てのセキュリティ機能を1台のアプライアンスに集約 ネットワークからエンドポイントまであらゆる場所でユーザーを保護

-----

◎専門知識がなくても、直感的に操作できるブラウザベースの GUI ◎ハードウェア、ソフトウェア、仮想アプライアンスから利用可能

◎必要なセキュリティ機能をモジュール形式で追加可能

◎業界最速のハイパフォーマンス アプライアンス - Miercom 社調べ -

◎拡張できるソケット式の FleXi Port LAN インターフェース

◎ 10 GB イーサネットに対応 (オプション SG210 以上)

◎ホットスワップ冗長電源 (オプション SG450 以上)

◎ SSD 搭載 (SG 230 以上)

### Sophos RED



### ローカルセットアップなしで支社・支店を安全に接続

支社・支店を保護すると同時に、安全なリモートアクセスを実現! Sophos RED をインターネットルーターに接続すると、支社・支店のトラフィックが本社の Sophos UTM に転送され、セキュリティを集中管理することが可能

◎低コストのセキュリティ管理を実現

◎本社から支社に Sophos RED の設定を自動的に配布

◎ Sophos UTM にすべてのトラフィックを転送することで、 最小規模のリモートオフィスやホームオフィスでも完全なセキュリティが実現

◎技術トレーニングやリモートサイトでの継続的なメンテナンスが不要

>>> 総所有コストを最大約 80% 削減

# Sophos Wi-Fi Access Point (Sophos AP)



### 安全で信頼性のある Wi-Fi アクセスポイントを提供 Sophos AP を Sophos UTM に統合し、有線とワイヤレスネットワークを包括的に保護

◎簡単な導入、管理

自動セットアップと設定の機能によって、数分で複数の AP を稼働 Sophos UTM から各 AP を一括管理

◎ゲスト用ホットスポットを簡単に提供

1つの AP で社内ネットワークとゲストネットワークを分割可能 テンプレート型のカスタマイズ可能なログインページやバウチャー

◎最適化されたパフォーマンス

802.11ac および 802.11n を含む最新の高速ワイヤレス基準に対応

各ハードウェアスペックは、別冊の Sophos SG アプライアンスのカタログを参照するか、弊社ホームページをご覧ください。

### Sophos XG Firewall

### 主な特長











# 1. 優れたユーザビリティ

直感的に理解できるブラウザベースの GUI で、 専用のソフトウェアやコマンドラインでの管理が不要

# 2. 優れた防御力

エントリーモデルからハイエンドモデルまで プラットフォームによる機能制限なく様々なセキュリティ機能を提供

# 3. 優れた柔軟性と拡張性

環境にあわせて必要な機能のみ利用できるライセンス体系で提供 製品はハードウェア/ソフトウエア/仮想アプライアンスと 全てのプラットフォームに対応

# 4. Security Heartbeat でエンドポイントと連係して動作

Sophos Central の Endpoint が脅威検出した場合、Security Heartbeat により即座に XG Firewall は通知を受け取り、自動的に該当エンドポイントからの通信を制御、駆除後、自動的に通信制御を解除。

# 5. 特許出願中の Layer 8 Identity Control

ソフォス独自のレイヤー8ユーザー識別に基づいたポリシーを活用して、IPアドレス、ネットワーク、デバイスにもかかわらず、アプリケーション、帯域幅、他のネットワークリソースをユーザーレベルで制御できます。

# 管理画面



### 製品紹介

ハードウェア / ソフトウェア / 仮想 アプライアンス (VMware, Hyper-V, KVM, Xen など) からビジネスに 最適なプラットフォームを提供



### Sophos Firewall Manager (SFM)

### 主な特長

Sophos Firewall Manager (SFM) は、お客様の複数の支社・支店にある複数のすべての Sophos Firewall OS を単一の画面から一括して管理できます。SFM は、時間と経費を節減し、管理を簡単にします。

# 1. 包括的な集中管理

◎単一のコンソールからすべてのファイアウォールポリシーを管理・設定◎一貫したポリシーをすべてのサイトに確実に適用

◎設定テンプレートを再使用して、 新しいファイアウォールを合理的に設定

# 2. 優れた監視機能

◎デバイスとネットワークの状態を一目で確認可能◎警告のしきい値をカスタマイズ可能

# 3. 高度な管理制御

◎地域、モデル、その他のパラメータによって柔軟にデバイスを グループ化。

◎ロールベース管理によって、業務の機能によって制御を委任可能◎変更管理とログ記録による変更の追跡とロールバック

# 4. 柔軟性の高い導入オプション

◎ハードウェア、ソフトウェア、仮想アプライアンスで利用可能 ◎iView に連係して管理ユーザーとデバイスを同期

### SFM ハードウェアモデル

	SFM 200	SFM 300	SFM 400
Sophia Firewall OS デバイスの推奨数	30	150	300
10 / 100 / 1000 RJ45 ポート	6	6	6
コンソールのポート(RJ-45)	1	1	1
USB ポート	2	2	2

### 仮想 / ソフトウェア

	SFM v5 *1	SFM v15	SFM v50	SFM v100	SFM v200	SFM v500	SFM v1000
対応する Sophos Firewall OS デバイスの数	5	15	50	100	200	500	1000
推奨 CPU ※2	デュアルコア	デュアルコア	デュアルコア	デュアルコア	デュアルコア	クアッドコア	クアッドコア
推奨メモリ(vRAM)	2 GB	2 GB	4 GB	4 GB	8 GB	8 GB	16 GB
推奨 HDD	160 GB	160 GB	250 GB	500 GB	500 GB	1 TB	1TB
ネットワーク インターフェース対応(最小 / 最大)	1/4	1/4	1/4	1/4	1/4	1/4	1/4

※1 評価目的の場合は無償 ※2 CPU 周波数は 2.7 GHz またはそれと同等

# Sophos UTM for Amazon Web Services (AWS)

### Amazon Web Services (AWS) 向けの包括的なセキュリティプラットフォーム

Sophos UTM for AWS で AWS EC2 インスタンスと VPC にセキュリティを提供。Amazon クラウド向けに最適化した、次世代ファイアウォール、Web アプリケーション ファイアウォール、業務アプリケーションのセキュリティ、レポート、VPN ゲートウェイ向けの包括的なセキュリティプラットフォーム。

### 機能紹介

### 次世代型ファイアウォールとレポート機能

◎スケールアップ、スケールアウトのどちらの拡張も可能

◎多彩なセキュリティログの取得(侵入防止システム (IPS)、

Web アプリケーションファイアウォール)

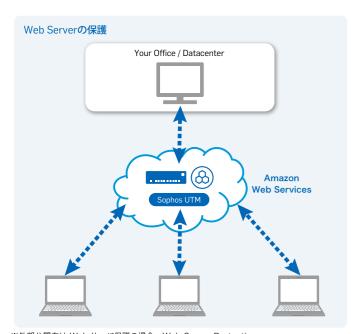
◎送受信国別でトラフィックをブロック可能

### Web アプリケーションファイアウォール

◎ SQL インジェクション、クロスサイトスクリプティングなどの、

Web アプリケーションへの攻撃をブロック

◎アップロード / ダウンロード通信のデュアルアンチウイルスチェック



※外部公開向け Web サーバ保護の場合、Web Server Protection, Unlimited User ライセンスが必要になります。

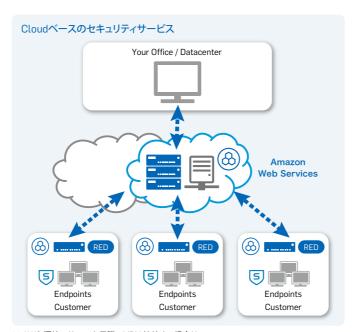
### Secure Access VPN ゲートウェイ

◎データセンタを使わずに簡単に VPN 網を構築

- ◎ RED を使用しゼロ・コンフィグで展開
- ◎ HTML5VPN 対応

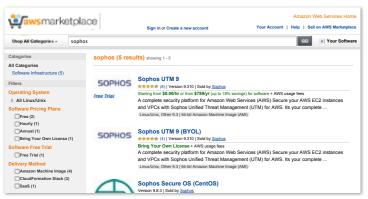
### Auto Scaling への対応

- ◎ Web アプリケーションファイアウォールのスケールアウトに対応
- ◎ VPC および、AWS 経由でインターネットアクセスをおこなうサーバ および、クライアントの入口・出口対策をスケールイン・アウトによる コスト最適化を実現



※ AWS 環境のサーバを保護、VPN 接続する場合は
 Network Protection ライセンスが必要になります。
 詳細は ソフォス営業部 03-3568-7550 / sales@sophos.co.jp までお問い合わせください。

# AWS Marketplace で、今すぐ使用可能



AWS Marketplace にて、Sophos UTM のインストール済みマシーンイメージ (AMI) が登録されており、ユーザーのインストール工数なしに使用が可能。

※ご使用にあたっては、別途 Sophos UTM ライセンスをご購入の上、 BYOL \*を推奨いたします。

※ (Bring Your Own License、クラウドへのライセンス持ち込み)

### Sophos iView (仮想アプライアンス)

### 主な特長

ネットワークの利用状況が一目瞭然

Sophos iView は、すべてのネットワークの利用状況を単一画面から一目で確認できるため、複数のアプライアンスを導入している環境で、まとまったレポート表示やログ管理 / コンプライアンス確認が必要な企業にとっても最適な選択肢です。

# ▲. レポートの統合

- ◎複数のファイアウォールデバイスと所在地の集計レポートを提供◎社内のネットワークのすべてのアクティビティを包括的に参照
- ◎ネットワークの利用状況が単一のダッシュボードで一目瞭然に把握

# 2. ユーザー別のレポートを作成

- ◎従業員のアクティビティを把握
- ◎従業員の P2P やその他のセキュリティ上の 危険度の高いアプリケーションへのアクセス、業務に関係のない Web 閲覧、ATP イベントを発生させるPC、ダウンロードの状況、 消費帯域幅などに関する情報を把握

# 3. 優れたセキュリティ状況の把握

◎iView ではネットワーク全体における潜在的な問題と攻撃を特定

※ATP イベントの原因となるようなマルウェアに感染したホストを特定や疑わしいユーザーや
異常トラフィックを検知するのに役立ちます。

# 4. ログのバックアップと管理

◎高度なインデックス検索機能により、分散した場所の 複数のデバイスのデータをログに記録

### 主な特長

仮想 アプライアンスにて提供。

(VMware, Hyper-V, KVM, Xen など) からビジネスに 最適なプラットフォームを提供

出力可能なレポートについての詳細は、以下をご覧ください。 https://www.sophos.com/ja-jp/medialibrary/PDFs/factsheets/sophos-iview-dsna.pdf



### Sophos iView ライセンス

	ストレージ容量	推奨 CPU **2	推奨メモリ (vRAM)	ネットワーク インターフェース対応 (最小/最大)	処理可能なイベント件数 (概算)(イベント数/秒)
iView Light **1	100 GB	デュアルコア	4 GB	1/4	短期 ※1
iView 500 GB	500 GB	デュアルコア	4 GB	1/4	300人
iView 1 TB	1 TB	デュアルコア	4 GB	1/4	300人
iView 4 TB	4 TB	クアッドコア	4 GB	1/4	600人
iView 8 TB	8 TB	クアッドコア	4 GB	1/4	600人
iView Unlimited	無制限 (推奨 16 TB)	クアッドコア <sup>※3</sup>	8 GB	1/4	2000人

\*\*1 評価目的の場合は無償: 処理可能なイベント件数は CPU およびハードウェアの仕様によって異なる \*\*2 CPU クロック周波数 2.7 GHz またはそれと同等 \*\*3 CPU クロック周波数 3.1 GHz またはそれと同等

### **Email Protection Advanced**

### 主な特長

# 1. メール経由でもたらされる 脅威をかんたんにブロック

- ◎ボットから配信されるメールをブロックする Sender Genotype
- ◎スパムメールをリアルタイムにチェックし、ブロックする SXL
- ◎フィッシングサイトや悪意あるサイトの URL が 含まれているメールをブロック
- © Sender Genotype と Sophos Live Anti-Spam で 99 % のスパムをブロック
- ◎ Behavioral Genotype® Protection により、 マルウェアのゼロデイ攻撃を阻止

# メール内容のフィルタリングや暗号化で、 機密情報の漏えいを防止

- ◎ SPX メール暗号化により、メールをまるごと暗号化◎ DLP (データ流出防止)機能で、ファイル形式、 内容により漏えいを防止
- 3. システムや脅威検知のステータスを 一目で把握できるダッシュボード
  - ◎状況を一目で把握できるダッシュボード・大容量の 隔離エリアを内蔵しているため追加ストレージは不要

### 機能紹介

# ♀ リアルタイムのスパム対策

### **Sophos Live Anti-Spam**

- ◎クラウド型サービスを利用して、リアルタイムでスパムを検出◎メールボックスへの侵入を防止
- ◎新しい脅威がメールサーバーに到達する以前に、 ゲートウェイでブロック

# ♡ ボットからのスパム対策

### **Sophos Sender Genotype**

◎ IP アドレスやトラフィックに含まれるストリングなどの特性から ボットコンピュータをプロアクティブに検知してブロック◎過去に一度もスパムを配信したことのないボットからのメールであって も、ブロックすることが可能

# 

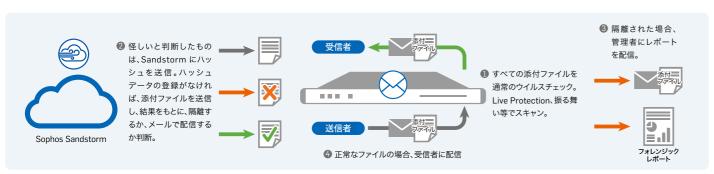
### SPX メール暗号化

◎通常使用しているメールクライアント(Outlook など)からメール送信する際に、ポリシーに準拠してメール本文と添付ファイルを PDF に変換して暗号化! 受信側に特別なソフトウェアのインストールは不要。また、パスワードはアプライアンスが自動生成し提供するため送信者が管理する必要はなく(受信者による設定も可能)、パスワードを忘れた場合でもユーザー自身で復旧や再設定が可能。



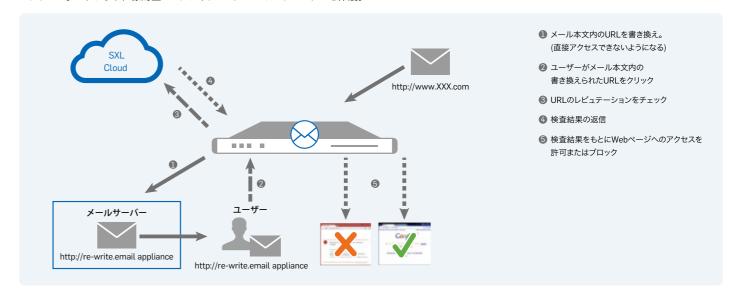
# Sandstorm の仕組み

◎クラウドベースの次世代型サンドボックスで、疑わしいプログラムを安全、隔離されたクラウド上の環境で実行し脅威を検出・ブロック。これにより、従来の脅威解析を回避する脅威を検知し、標的型攻撃からユーザーを保護。



# 

◎ E メール中の URL リンクに常に Email Appliance を経由してアクセスすることにより、アクセス先を毎回 Email Appliance でスキャンした後に アクセス。これにより、標的型スピアフィッシングメールからユーザーを保護。



### 製品紹介

### アプライアンス製品

多様なセキュリティソフトウェアを搭載。企業のニーズに合わせて 2 機種から選択。

### Sophos Email Appliance

# SOPHOS AUTIMITY TO THE TOTAL OF THE TOTAL OF

### E メールセキュリティ機能を 1 台のアプライアンスに集約

SPX メール暗号化、データ流出防止 (DLP)、マルウェア対策、スパム対策などを搭載

- ◎自動化された SPX メール暗号化で、機密データを保護
- ◎搭載済のデータ流出防止 (DLP) 定義で、データ流出のリスクを削減
- ◎既知や未知のゼロデイ脅威を、実証済のマルウェア対策エンジンでブロック
- ◎複雑な設定を必要とせず、99%以上のスパムをブロック
- ◎単一のライセンスで、SPX メール暗号化、データ流出防止 (DLP)、マルウェア対策、スパム対策を提供
- ◎単一のコンソールで、複数のアプライアンスを管理可能
- ◎ハードウェア、ソフトウェア、トラフィック、アップデート状況などのリモート監視で保証される保護
- ◎自動アップグレード、スタンダードサポート (平日 9:00 17:30 / 緊急時は 24 時間 365 日)、 3 年間のハードウェアアドバンス交換保証を提供

スペック	ES1100	ES5000
毎時処理可能なメール件数(理論値)	20 万件	55 万件
プロセッサ	デュアルコア	クアッドコア
ハードドライブ	250GB SATA	160GB SAS (RAID1) (2 台構成、ホットスワップ対応)
電 源	260W 100-240 V	デュアル ホットスワップ 920W 100-240V

### ライセンス

### **Email Protection Advanced**

メールマルウェア対策、迷惑メール対策、メールポリシー策定、SPX メール暗号化<sup>※</sup>、自動アップデート ※SPX メール暗号化を利用するには、メールアプライアンス (別売) あるいは、仮想アプライアンス (VMWare で動作) が必要

# 無償ツールのご紹介

### スクールパックライセンス

### 小学校、中学校、高校、専門学校、幼稚園、保育園、保育所を対象とした、台数無制限で利用可能な包括ライセンス

特 長	包括ライセンスとして提供されるため、契約期間中にユーザー数の増加が生じた場合でも、 追加費用無し。面倒なライセンス管理作業を大幅に軽減します。	スクールパックライ	センス
製品名	Endpoint Protection Advanced (スクールパックライセンス)	学校所有	教職員個人
対 象	文部科学省認可の幼稚園、小学校、中学校、高等学校、専門学校、		
	厚生労働省認可の保育園、保育所		
利用範囲	学内 PC、サーバー、教職員所有の持込み PC、教職員の自宅 PC で利用可		
機能	Endpoint Protection Advanced の使用に準じます。		

価 格	Endpoint Protection Ad	point Protection Advanced (スクールパックライセンス)						
	契約年数	1年契約	2 年契約	3 年契約	4 年契約	5 年契約		
		85.000 円	170.000 円	255.000 円	340.000 円	425.000 円		

<sup>※</sup>一校あたりの単価(消費税別)

### キャンパスライセンス

### 大学を対象とした、台数無制限で利用可能な包括ライセンス

	包括ライセンスとして提供されるため、契約期間中にユーザー数の増加が					
特 長	生じた場合でも、追加費用無し。		キャン	パスライセンス		
	面倒なライセンス管理作業が大幅に軽減されます。					
		学校所有		教職員個人		学生個人
製品名	Enduser Protection and Mail (キャンパスライセンス)		+		+	
対 象	短期大学、大学、その他大学に準じる教育機関など。					
利用範囲	学内 PC / サーバー、教職員の自宅 PC、学生の自宅 PC で利用可					
機能	Enduser Protection and Mail / Server Protection Enterprise の仕様に準じま	す。				
価 格	お問い合わせください。					

### 自治体ライセンス

### 自治体を対象とした、台数無制限で利用可能な包括ライセンス

	特 長	自治体の職員定数による契約で、PC やサーバーを保護。台数無制限で利用でき、コスト削減を実現。		
	製品名	Enduser Protection(自治体ライセンス)		
Endpoint Protection Advanced (自治体ライセンス)				
	対 象 地方自治法で定める都道府県、市町村、特別区(東京 23 区)単位での全導入の場合が対象。			
	利用範囲	自治体の PC や サーバー で利用可		
	機能	Enduser Protection / Endpoint Protection Advanced の仕様に準じます。		
	価 格	お問い合わせください。		

### ライセンスの購入方法 (都道府県及び市区町村の自治体)

	通常の駅	通常の購入方法		
	クライアント	クライアント / サーバー		
該当製品	Enduser Protection	Server Protection Enterprise	Enduser Protection	
購入数	使用するクライアント数	使用するサーバー数	職員定数条例で定めた職員総数 ※	
利用可能な台数	購入数	無制限		

※職員定数条例で定めた職員数で購入できます。カウントが必要なもの(首長部局、議会の職員など)と、任意でカウントできるもの(公営企業の職員、消防職員など)があります。 コンピュータ数が職員定数を超えても、全てのコンピュータで使用可能です。

### Sophos Home - 個人に利用に限り、無償で利用可能

### クラウド型の管理コンソールで、自分の PC だけでなく、離れて暮らす家族の PC も管理可能。

◎ Windows と Mac のマルウェア対策製品

◎管理設定は、直感的に操作でき、どこにいてもクラウドから設定管理可能。 □ 10 台までの Windows や Mac 管理可能

★ https://www.sophos.com/ja-jp/lp/sophos-home.aspx

### Sophos Anti-Virus for Mac Home Edition - 個人利用に限り、無償で利用可能

### ウイルス、トロイの木馬、ワームを検出して駆除

◎ Windows 系のマルウェアなども検出し、利用者自身の Mac だけでなく、他人の Windows PC に送信する Windows 系ファイルもスキャンして保護

### 未知の脅威も含むすべての脅威を阻止

◎定義ファイル反映前の最新の脅威について、SophosLabs が提供するクラウド型のデータベースで瞬時にチェックし、ブロック(Sophos Live Anti-Virus)

### 検出したマルウェアの隔離と駆除

### 簡単なインストールと軽快な動作

★ http://www.sophos.com/ja-jp/products/free-tools/sophos-antivirus-for-mac-home-edition.aspx

### Sophos Mobile Security for Android - Android 向け無償アンチウイルスアプリケーション

### Android スマートフォンおよびタブレットに次の機能を提供

◎インストール済みアプリケーションがデバイスに対して行える パーミッションの確認

◎インストール済みアプリケーションやファイルをスキャンし、脅威の有無を SophosLabs の最新情報と照合

◎紛失または盗難されたデバイスの現在位置の特定

◎盗難されたデバイスのロック、ワイプ、アラーム

★ Google Play Store から "Sophos" で検索、もしくは右の QR コードからダウンロード画面を表示

### Virus Removal Tool - マルウェアを検出して駆除!

### ウイルス、スパイウェア、ルートキット、偽ウイルス対策ソフトを駆除

◎ Windows XP、Vista、7 に対応

◎他社のウイルス対策製品をインストールしている場合でも利用可能 ★ http://www.sophos.com/ja-jp/products/free-tools/virus-removal-tool.aspx ◎簡単なインストール

### Sophos UTM Home Edition - 個人利用に限り、無償 UTM のソフトウェア版

### Sophos UTM ファイアウォールのソフトウェア版で、すべての機能を備えており、自宅利用者に無償で提供

◎全ての機能を備えた Sophos UTM アプライアンスのソフトウェアバージョン

◎ VPN 機能を備えたネットワーク、Web、電子メール、Web アプリケーションの包括的なセキュリティ

◎最大 50 IP アドレスを保護

★ http://www.sophos.com/ja-jp/products/free-tools/sophos-utm-home-edition.aspx

### Sophos XG Firewall Home Edition

# Sophos XG Firewall のソフトウェア・仮想版で、マルウェア対策、Web セキュリティ、URL フィルタリング、アプリケーション コントロール、IPS、トラフィックシェーピング、VPN、レポート、監視など、ホームネットワークに包括的な保護を提供

◎ ホームユーザーとネットワークに対する包括的なセキュリティ対策

○ Linux ベースのセキュアな OS の統合○ Intel 互換ハードウェアで稼動

★ https://www.sophos.com/ja-jp/products/free-tools/sophos-xg-firewall-home-edition.aspx

### Sophos Clean

### ウイルス対策ソフトのセカンドオピニオン製品!

◎ シグネチャーレスの次世代型のマルウェア駆除ツール

◎特に既存のアンチウイルスソフトがマルウェアによって無効にされている場合や、検出を回避しやすいルートキットやランサムウェアなどに有効

◎本製品はインストールの必要がないオンデマンド型のツールで、ソフォスあるいは他社のアンチウイルスソフトウェアと併せて使用することが可能です。

★ https://www.sophos.com/ja-jp/products/sophos-clean.aspx

### Sophos Anti-Virus for Linux Free Edition - 個人利用に限り、無償で料可能

### ミッションクリティカルな Linux サーバーで多数の保護実績あり

◎商用版と同等の機能を利用可能

◎さまざまな Linux ディストリビューション (カスタマイズを含む) とカーネルに対応

◎軽快で使いやすく、Linux サーバーのパフォーマンスを低下させない

この他にも、ソフォスの技術を体験していただくため、さまざまなセキュリティツールを無償でご用意しています。 ホーム > 製品情報 > 無償ツール http://www.sophos.com/ia-jp/products/free-tools

<sup>※</sup>オプションとしてSophos Mobile Controlスクールパックライセンスのアドオンが可能です。

	サブスクリブションライセンス																7			$\rho_6$	q										<i>L</i> .				es					
			þ	/_/							, on	Pao	Pard	Peoo	ard	tion			782		JBD:		rption			d and		tion			yptic	r Mac		/ 6	Share	No.	20			
	パーペチュアルライセンス		'ance	ndarc		rage	Driso	ב ב	Į.	Pag	otect	4dvar	Stand	4dvar	Stand	пслур	ion		on Ag	an St.		Mail	Encr	and '		'ance		ייכיזיי	i / i	e Fn		5	ge	or Pr Filo		on for		ndle	五載()	
			n Adı	n Sta	4	0,50	Enter		Sep	dvan	ail P <sub>ri</sub>	rtrol ,	itrol ;	itrol,	itrol (	ise E.	crypt		,rypti	27.7pti	_	bue (	bue (	' Mai	and ise	7 Ag	ise	oe E	Ench	Devio	crypt	-	chan	tion fe	tion	, rypti	ndle	ıs Bu	標準法	P
		tecti	tectio	, cctio	etwor	5	ction ,	g)	e - Per	tion A	, E				5	rerp.			$^{le}$ $E_{D_{c}}$	$^{le}$ $E_{nc}$	ection	ection	rrotection ar	1000	terti.	ons pa	rd Enterpri	ard File Encr	rd Device Enc	ard Native Devi	sk En	Isy	ata Ex	מעיסי	rage rage	le Enc	rd Bu	rdPlu	wall (	c cua
		Endpoint Proteon:	Endpoint Protect:	Sophos Clean	os for Net <sub>1</sub>	IQA soydos	erver Protection En	CA.	SAV Interface Emc	Sandstorm for a	ed ∫. Mobii	Sophos Mobile Control Adver	Sophos Mobile Control Star	Sophos Mobile C.	SafeGuard E.	SafeGuard Disk Fr.	p.	1	" a File Encryption Advan	ard File Encryption Stand	704	rot d	er Protection an	Prot	pton Enterprise	MC Advanced and	ard Er	ard Fi	$^{3rd}D_{\epsilon}$	ard N	areGuard Disk Encryption	ard Easy	reGuard Data Excha	SafeGuard Encryption for	or Cloud Storage Safegue	TM E	UTM Fulle.	XG Base Fireway	XG Enterprise G.	XG FullGuard
	含まれるライセンス 及び 製品	apoir	dpoir	Soydi	soyd	soyd	irver,	I Int	1 / Int	nall P	sold:	2/ Soft	Sold	Sold Pasies	reGu,	reGu, Vanc		SafeGu		Fnduso.	gnes	duse	duse	orve.	idpoir Jie	10 Ac	$\eta_e G_{U_e}$	nfeGu,	reGu,	"eGu,	"eGu,	rfeGua <sub>l</sub>	neGu,	"eGu,	fec.	IM E.	$^{7}M_{F_L}$	Base	3 Ente	Fully
				S	S	S	8 8		δ <u>Ψ</u>	S. A.	SE	SE	2000	88	လွ	S <sub>o</sub> A		လွ	S	$\vec{\mu}$	Ē	Ē	Ē	E E	ПZ	Q T	လွ	လွ	o c	5 6	8 0	ပို့ လိ	S	, v,	, S	5	5	29	2	*
	Endpoint Protection for Windows		•																	•	•	•		•	•															
エンドポイント	Sophos Anti-Virus for Windows		•																	•	•	•	•	•	•															
	Sophos Anti-Virus for Mac	•	•																	•	•	•	•	•	•															
	Sophos Anti-Virus for Linux	•																		•	•	•		•	•															
	Sophos Anti-Virus (NetApp / EMC / ICAP 連携ストレージ用)	•			•															•	•	•	•	•	•															
	Sophos VDI				(	•																																		
	Sophos Enterprise Console	•	•			•	•*	1 •*	1											•	•	•		•	•															
	Sophos Anti-Virus for Windows					•																																		
	Sophos Clean			•																																				
サー	Sophos Anti-Virus for Mac																																							
八	Sophos Anti-Virus for Linux																																							
· ·	Sophos Anti-Virus for UNIX																																							
	Sophos VDI																																							
	SAV Interface (SAVI)							•																																
	SAV Dynamic Interface (SAVDI)						•	•																																
	PureMessage for MS Exchange	•	•						•											•	•	•	•	•	•															
×	PureMessage for UNIX								•												•		•		•															
メール	Sophos Email Appliance (仮想)								•												•		•		•															
	Sophos Email Appliance (ハードウェア別売)								•												•		•		•															
	Email Sandstorm									•																														
	Sophos Mobile Control Advanced (オンプレミス版)										•													•		•														
モバ	Sophos Mobile Control Standard (オンプレミス版)											•								•	•	•																		
イル	Sophos Mobile Control Advanced (SaaS版)												•																											
	Sophos Mobile Control Standard (SaaS版)													•																										
	Sophos Mobile Security for Android												•										-	•		•	_	_												
	SafeGuard Management Center															•		•	•			•	•	•		•				•		•	•	•	•					
	SafeGuard Device Encryption														•	•							•	•		•	•													
	SafeGuard Native Device Encryption														•	•								•		•	•													
_	SafeGuard Disk Encryption for Mac														•	•										•	•													
データ	SafeGuard Bata Fushages																	•													•									
7	SafeGuard Exeruption for File Shares														•																									
	SafeGuard Encryption for File Shares SafeGuard Encryption for Cloud Storage																																•							
															•																									
	SafeGuard File Encryption for Mac																							-									•							
	Sophos Secure Workspace **2  Network Protection																																							
	Web Protection																																							
ネ	Email Protection																																							
ットワ	Wireless Protection																																							
ワーク	WebServer Protection																																							
ク	Endpoint Protection																																							
	Sandstorm																																							
	Gundstofffi																																							

26

 <sup>※1</sup> SAVI / SAVDI は、エンジンや定義ファイルのアップデートを Sophos Enterprise Console 経由で行えます。
 ※2 Sophos Secure Workspace は、SafeGuard Encryption for File shares や SafeGuard Encryption for Cloud Storage と動作します。
 また、管理するには、Sophos Mobile Control Advanced (オンプレミス版 / SaaS 版 ) が必要です。

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 Tel. 03-3568-7550 Fax. 03-3568-7551 www.sophos.com/ja-jp Email sales@sophos.co.jp

- 技術情報ポータルサイト「ソフォスインサイト」 sophos-insight.jp
- ▶ セキュリティ記事を掲載中 Twitter: @sophosjpmktg / Facebookページ: https://www.facebook.com/sophosjpmktg