SOPHOS

Security made simple.

ソフォス 総合カタログ

法人向けセキュリティソリューション

Network Protection

Enduser Protection

Server Protection

Sophos Cloud

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 オックスフォードおよびアメリカ ボストンに構え、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 (オックスフォード、バンクーバー、シドニー、ボストン、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 オックスフォード
アメリカ ボストン

設 立
1985 年 イギリス オックスフォードに設立

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、日本、イタリア、フランス、シンガポールなど

従業員数
約 1,600 名以上（全世界）

ソフォス株式会社

代表取締役社長
纐纈 昌嗣（こうけつ まさつぐ）

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

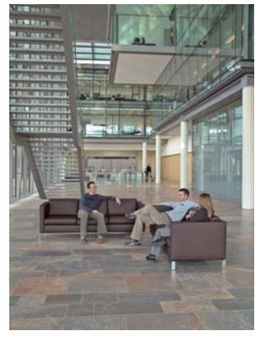
事業内容
法人向け IT セキュリティ関連製品
サービスの開発、販売およびサポート
（日本市場でのソフォスソリューションを販売・サポート）

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 (オックスフォード、バンクーバー、シドニー、ボストン、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 日最大 4 万件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。



アワード受賞

ソフォスラボの迅速な対応と Genotype テクノロジーにより各種アワードを受賞

Virus Bulletin 100% (VB100%) 賞
2014 年 2 月時点

VB100% 受賞回数

ベンダー	ソフォス	A 社	B 社	C 社	D 社	E 社
受賞回数	70 回	16 回	57 回	49 回	52 回	66 回

第三者機関による評価

AV-Test のセキュリティ製品比較調査結果

法人ユーザー Windows 7 2012 年 9 月/ 10 月の調査結果

	ソフォス	A 社	B 社	C 社	D 社	E 社
PROTECTION SCORE（6 点満点）	5.0	3.5	5.5	3.5	5.5	5.5
ゼロデイマルウェアの検出 (%)	92	79	96	79	92	92
既知のマルウェア検出 (%)	100	100	98	99	99	99
拡散してるマルウェアの検出 (%)	100	100	100	100	100	100
REPAIR SCORE（6 点満点）	4.5	2.0	3.5	1.5	5.0	6.0
拡散しているマルウェアの実行中の検出 (%)	100	95	95	83	100	100
拡散しているマルウェアの実行中に関連する悪質なコンポーネントの削除 (%)	90	68	88	75	90	95
悪意のあるコンポーネント削除と重要なシステムの変更を修復 (%)	63	60	65	63	73	83
USABILITY SCORE（6 点満点）	5.0	4.0	5.5	5.0	4.5	5.0
動作中のPCの平均的なスローダウン (秒)	10	18	8	14	11	13
システムスキャン中の誤検出 (件)	0	1	0	0	3	0
特定のアクション時の誤警告 (件)	0	4	0	0	2	0
特定のアクション時の誤ブロック (件)	0	0	0	0	0	0

PROTECTION SCORE ... マルウェア感染の検出率 / REPAIR SCORE...マルウェア感染したコンピュータのクリーニング率
USABILITY SCORE... セキュリティソフトウェア有効時にかかる負荷

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、デザインフィルホールディングスその他、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

社 内

社 外

Server Protection

社内サーバー

Sophos Server Protection

Windows
Mac
Linux
UNIX
などのサーバー

外部用サーバー

Sophos Server Protection

Web
サーバー

Sophos Email Protection

メール
サーバー

ストレージサーバー

Sophos for Network Storage

EMC
NetApp

仮想サーバー

Sophos Anti-Virus for vShield

Windows
サーバー

Network Protection

在宅勤務 / 外出先など

SSL / VPN 接続

Web Application Firewall
Secure Email Gateway

Sophos E-mail Appliance

Sophos UTM

- Next-Generation Firewall
- Web Application Firewall
- Secure E-mail Gateway
- Secure VPN
- Secure Web Gateway
- Secure Wi-Fi

支店 / 支社 1

Sophos UTM

SSL / VPN 接続

支店 / 支社 2

Sophos RED

ルーター /
モデム

SSL / VPN
接続

**Sophos
Wi-Fi Access
Point**

Enduser Protection

クライアント

Sophos Endpoint Anti-Virus **SafeGuard**

Windows Mac Linux

仮想サーバー

Sophos Anti-Virus for vShield - VDI

Windows クライアント

スマートフォン / タブレット

Mobile Control

Android
iPhone
iPad
Windows Phone
Black Berry

すべてのライセンスで、
スタンダードサポート(9:00–17:30)を提供しています。
※土日祝日、弊社指定休業日を除く /
緊急時は 24 時間 365 日

Enduser Protection

- Sophos Enduser Protection
- Sophos Endpoint Protection
- Sophos Mobile Control
- Sophos Mobile Security
- Sophos Anti-Virus for vShield - VDI
- SafeGuard Enterprise
- SafeGuard

→ P. 6

Network Protection

- Sophos UTM
- Sophos RED
- Sophos Wi-Fi Access Point
- Sophos E-mail Appliance

→ P. 14

Server Protection

- Sophos Server Protection
- Sophos for Network Storage
- Sophos E-mail Protection
- Sophos Anti-Virus for vShield

→ P. 18

Sophos Enduser Protection / Sophos Endpoint Protection

主な特長

1. 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

2. 異なる OS でも一元管理
Windows / Mac / Linux / UNIX 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

5. 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. ノート PC の盗難 / 置き忘れ対策
ハードディスク丸ごと暗号化で、PC の盗難、紛失時にデータ流出を防ぐ！

7. 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

エンドポイントでサイバー攻撃に対する多層防御を！

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

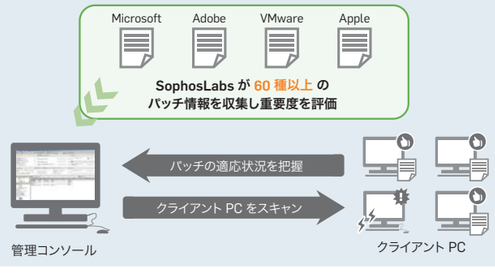
Web コンテンツフィルタリング

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

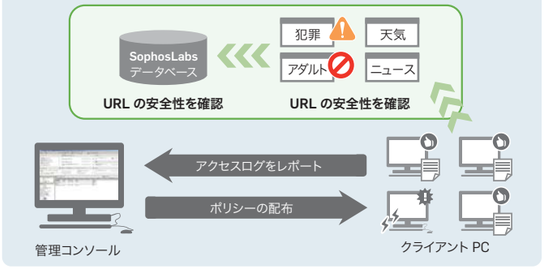
Sophos Live Web フィルタリング

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

パッチアセスメント



Web フィルタリング/ Web コンテンツフィルタリング



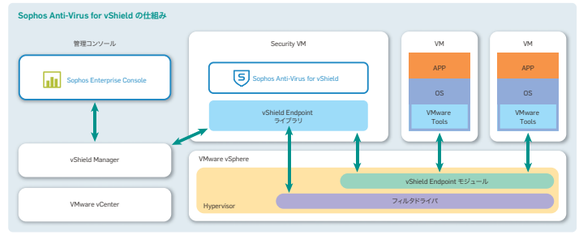
Sophos Live Anti-Virus

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

Sophos Anti-Virus for vShield - 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

Sophos Anti-Virus for vShield の仕組み



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
◎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

フルディスク暗号化

堅牢な暗号化技術で盗難・紛失時の情報漏えい対策
◎ AES-256 bit 暗号化アルゴリズムで高レベルのセキュリティを確保
暗号化状況を管理
◎管理画面から複数の PC に暗号化を導入、状況の把握が可能
導入も簡単な操作性
◎暗号化前と変わらない作業で簡単にログイン。
◎パスワードを忘れてしまった場合、チャレンジレスポンス以外にユーザー自身で復旧可能 (ローカルセルフヘルプ)

ライセンス

機 能	Sophos Enduser Data Suite	Sophos Enduser Protection	Sophos Endpoint Protection - Business	Sophos Anti-Virus - Business 注(8)
クライアント対策	●	●	●	●
サーバー対策	※全社導入の場合は要相談		–	–
集中管理	●	●	●	●
マルウェア対策	●	●	●	●
HIPS 注(1)	●	●	●	●
Sophos Live Anti-Virus 注(2)	●	●	●	●
Sophos Live Web Filtering 注(1)	●	●	●	●
クライアントファイアウォール 注(3)	●	●	●	●
デバイスコントロール 注(1)	●	●	●	–
アプリケーションコントロール 注(1)	●	●	●	●
業務上不要なアプリケーションの検知 注(1)	●	●	●	●
Web コンテンツフィルタリング 注(1)	●	●	●	–
パッチアセスメント(OS, アプリ更新通知) 注(1)	●	●	–	–
自宅使用ライセンス	●	●	–	–
ハードディスク暗号化 注(4)	●	–	–	–
対応プラットフォーム	Windows /Mac /Linux /UNIX / EMC /NetApp / 仮想化環境		Windows / Mac / Linux / 仮想化環境	Windows / Mac / 仮想化環境
ストレージの保護(Sophos for Network Storage)	●	●	–	–
スパム対策	● 注(5)	● 注(6)	● 注(6)	–
メールマルウェア対策	● 注(5)	● 注(6)	● 注(6)	–
メール暗号化(SPX) 注(7)	●	–	–	–
モバイルデバイス管理(Sophos Mobile Control) 注(9)	●	●		
モバイルマルウェア対策(Sophos Mobile Security - Enterprise) 注(10)	●	●		

注(1) Windowsのみ、注(2) Windows / Mac / Linux、注(3) Windows クライアントのみ、注(4) Windows / Mac、注(5) E-mail Protection - Advanced の含まれるものすべて利用可能、
注(6) PureMessage for Microsoft Exchange のみ利用可、注(7) メールアプライアンスが必要(仮想アプライアンスは無料、ハードウェアアプライアンスは別売) 、注(8) 従業員 100 名未満の企業のニーズに合わせて設計、
注(9) Sophos Mobile Control の仕様に準拠、注(10) Sophos Mobile Security - Enterprise の仕様に準拠

単体ライセンス

Sophos Anti-Virus for vShield - VDI

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

1. 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

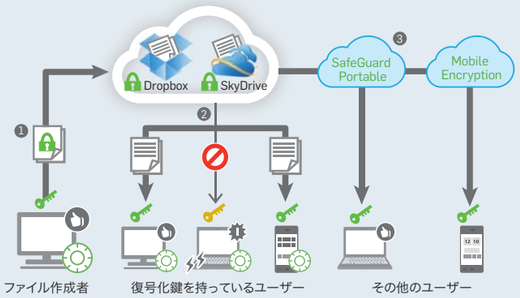
3. 緊急時の簡単な復旧
◎チャレンジレスポンス
◎ユーザー自身で復旧できるローカルセルフヘルプ

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

クラウド上にある情報の暗号化



SafeGuard Encryption for Cloud Storage をインストールしている端末
❶ ファイルをクラウドへ保存する際に自動暗号化（同期フォルダに保存）
❷ 対応する復号化鍵を持っているユーザーのみファイルの閲覧が可能
❸ SafeGuard Encryption for Cloud Storage がインストール されていないデバイスは、専用のアプリケーション（SafeGuard Portable / Sophos Mobile Encryption）にパスフレーズを入力して復号化
※ 現在、Sophos Mobile Encryption は Dropbox、SkeDrive、Egnyte に対応

共有ファイルへの適切なアクセス管理

❶ ファイル作成者が、暗号化したデータをサーバーへ保存
❷ 暗号化した状態でバックアップを取る
❸ IT 管理者が復号化鍵を適切なユーザーに配布
❹ 対応する復号化鍵を持つユーザーのみ閲覧可能
❺ IT 管理者であっても、対応する復号化鍵を持っていなければファイルへアクセスができない

機能紹介

暗号化による情報漏えい対策

管理とポリシー	盗難・紛失対策	データの保護
◎単一コンソールでの集中管理 ◎ポリシーの策定と配布	◎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	◎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
◎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

クラウド上にある情報の暗号化
◎ Dropbox、SkyDrive、Egnyte 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（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

ハードディスク全体の暗号化
◎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
◎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
◎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を実現
◎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可能（チャレンジ & レスポンス / ローカルセルフヘルプ）

共有ファイルの保護
◎ 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

パーペチュアル ライセンス

SafeGuard Enterprise	Windows	Mac
ハードディスク暗号化	SafeGuard Device Encryption	SafeGuard Disk Encryption for Mac
リムーバブルメディア暗号化	SafeGuard Data Exchange	SafeGuard File Encryption for Mac
共有ファイル暗号化	SafeGuard Encryption for File Shares	
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	SafeGuard Native Device Encryption ※1	
一元管理ツール	SafeGuard Management Center ※2	

※1 BitLocker / FileVault2 で暗号化された PC の管理
※2 単独での販売なし。各モジュールに同梱

サブスクリプション ライセンス

スイート型	SafeGuard Enterprise Encryption (上記表のライセンスをすべて利用可能)
ハードディスク 特化型	SafeGuard Disk Encryption Advanced (SafeGuard Device Encryption と SafeGuard Native Device Encryption と SafeGuard Disk Encryption for Mac が利用可能)
ファイル 特化型	SafeGuard File Encryption Standard（SafeGuard Data Exchange が利用可能） SafeGuard File Encryption Advanced （SafeGuard Data Exchange と SafeGuard Encryption for File Shares と SafeGuard Encryption for Cloud Storage と SafeGuard File Encryption for Mac が利用可能）

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

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
◎SIM カード差し替えの通知

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

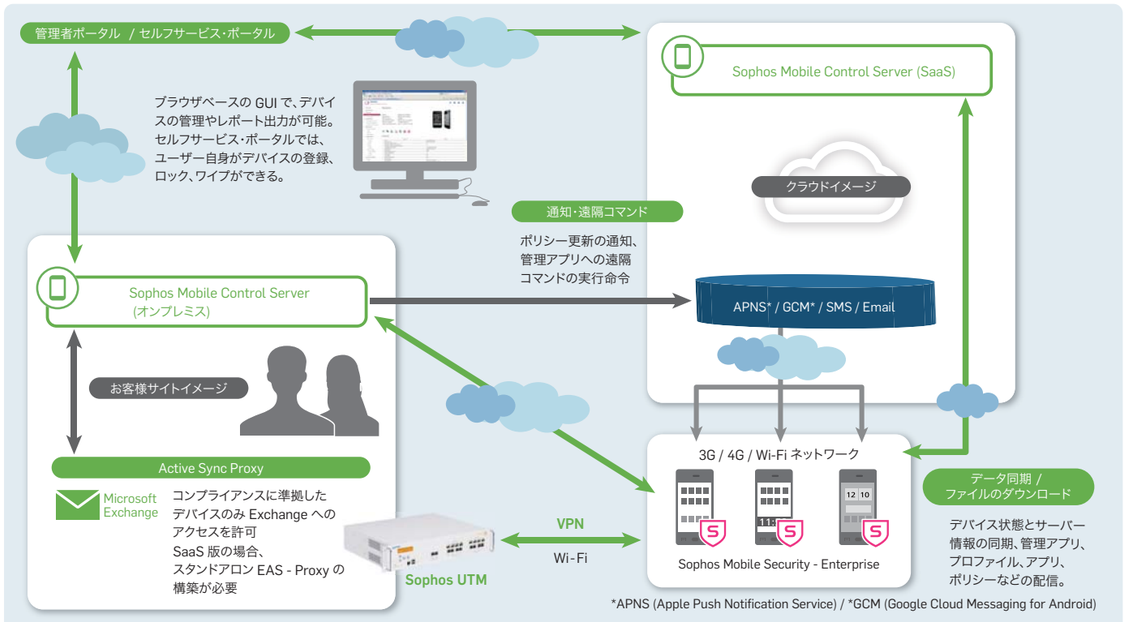
そのままでユーザーへ一部の操作の権限委任と、
一箇所からの端末の管理、状態確認が可能
◎デバイスのユーザーは、セルフサービスポータルから
自分のデバイスの登録、ロック、データの消去が可能
◎ネットワーク経由での管理アプリ、設定、
ポリシーの配信が可能
◎全デバイスの情報、コンプライアンス準拠の状況を
ひとつの管理画面から確認可能

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 (iPhone, iPad)、Android、Windows Mobile、Windows Phone、BlackBerry 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。

ユーザー自身でセキュリティ管理



ライセンス

SMC Standard (オンプレミス)
(Sophos Mobile Control が利用可能)

SMC Advanced (オンプレミス)
(Sophos Mobile Control と Sophos Mobile Security が利用可能)

SMC SaaS

OS 別機能対応表

セキュリティ設定	Apple iOS	Android	Windows Phone 8
SIM カード変更時の通知		●	●
リモートワイプ	●	●	●
リモートロック	●	●	●
リモートによる設定情報のクリア			●
パスワードポリシーの強制	●	●	●
メモリデバイスへのアクセス禁止			●
メモリデバイスのデータ暗号化の有効化			●
データの暗号化の有効化			●
SD カードの禁止		● ※1	
バックアップの禁止		● ※1	
Wi-Fi テザリングの禁止		● ※1	
Bluetooth 接続のブロック		● ※1	
Bluetooth テザリングの禁止		● ※1	
USB 利用の制御(テザリング、デバックモード)		● ※1	
NFC 利用の禁止		● ※1	
Active Sync 接続のブロック	●	●	●
カメラ利用の禁止	●	● ※1	
ユーザーによる設定情報の変更/削除の禁止	●	● ※1	
スクリーンキャプチャの禁止	●	● ※1	
アプリケーションのインストールの許可/禁止	●		●
iTunes、Play store 利用の許可/禁止	●	● ※1	—
YouTube 閲覧の許可/禁止	●		
ブラウザ利用の許可/禁止	●		
不適切なコンテンツの許可/禁止	●		
管理アプリ、プロファイルの削除検知	●	●	—
ローミング中の同期/データ接続/音声通話の禁止		● ※1	
アプリ強制終了のレポートの禁止		● ※1	
ネイティブブラウザの禁止		● ※1	
クリップボードの禁止		● ※1	
マーケット以外のアプリ禁止		● ※1	
ワイプ操作の禁止		● ※1	
スクリーンロック時のカメラ、ウィジェット禁止		● ※3	
Web フィルタ(ブラックリスト、ホワイトリスト)	● ※4		
iOS7 から追加されたプロファイルによる機能制御	● ※4		
SMS/MMS スパムメッセージフィルタ		● ※5	
リモートスクリーン共有(AirPlay デバイスが必要)	● ※4		
Web カテゴリ フィルタリング		●	
モニタリング			
期間内のデータトラフィックの監視		●	

※1 Samsung SAFE 対応デバイスのみサポート
※2 Sophos Mobile Control as a Service では利用不可
※3 Android 4.2 以降でサポート
※4 iOS7 以降でサポート
※5 Sophos Mobile Security のアドオンライセンス利用時のみサポート

コンプライアンスの管理	Apple iOS	Android	Windows Phone 8
パスコードポリシーのチェック	●	●	●
Root 化(Android)、Jailbreak (iOS)のチェック	●	●	—
ステータス同期間隔をチェック	●	●	●
許可する OS バージョン範囲をチェック	●	●	●
禁止、許可、必須アプリのチェック	●	●	
データローミングの設定をチェック	●	●	●
デバイスの暗号化設定をチェック	●	●	●
マルウェアスキャン対策状況のチェック		● ※5	
デバイスの設定			
MS Exchange の設定	●	● ※1	●
IMAP/POP メール設定	●		
LDAP や CalDAV 設定	●		
アクセスポイントの設定	●	● ※1	
Wi-Fi 接続の設定	●	●	
VPN と VPN プロキシの設定	●	● ※1	
アプリ毎のVPN接続	● ※4		
アプリのシングルサインオン	● ※4		
ルート証明書の配布		● ※1	
SCEP によるクライアント証明書の配布 ※2	●		
お気に入り(ブックマーク)の配布	●		●
クライアント証明書の配布		● ※1	
デバイス情報の取得			
内部メモリの使用領域	●		
バッテリーの利用情報	●	●	
SIM カードの識別情報(IMSI)	●	●	●
利用中のキャリア情報	●	●	
ローミングモードの使用情報	●	●	●
OS のバージョン情報	●	●	●
端末の位置情報取得	●	●	●
データのバックアップ取得と復元 ※2		●	
SMC クライアント機能			
メニューによる Enterprise App Store の利用	●	●	●
コンプライアンス違反表示	●	●	●
管理者からの送信メッセージ表示	●	●	●
問合せ先の案内表示	●	●	●
手動操作によるデータ同期	●	●	●
アプリの管理			
アプリの強制インストール	●	●	●
アプリの強制削除	●	●	
インストール済みアプリの一覧表示	●	●	
アプリの有効化/無効化	●		
管理アプリのみを削除	● ※4		
Apple VPP のサポート	●	—	—

Sophos Mobile Security

主な特長

1. Sophos Mobile Control にて一元管理

Sophos Mobile Security がインストールされた Android デバイスを管理可能に。Sophos Mbile Control より、設定の管理、ステータスの管理が可能。
デバイス側から変更は不可にすることも可能。

2. 悪意あるアプリから Android デバイスを保護

通常のスキャンに加え、Sophos Live Protection 機能で、悪意あるアプリをブロック。

3. 悪意ある Web サイトへのアクセスをブロック

SophosLabs が保有するクラウド上の Web 脅威データベースに瞬時にアクセスし、悪意ある Web サイトかどうかを瞬時に確認し、ブロック。

4. Android デバイスの SD カードを監視

Android デバイスの SD カードにマルウェアアプリや危険なファイルが保存される際にリアルタイムで検知。

Sophos Mobile Control 管理画面

Sophos Mobile Security

機能紹介

マルウェアスキャン設定ポリシーを強制

コンプライアンス設定 (通知機能)

SMC 管理コンソールからのオンデマンドスキャン

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

ソフォス製品 API の紹介

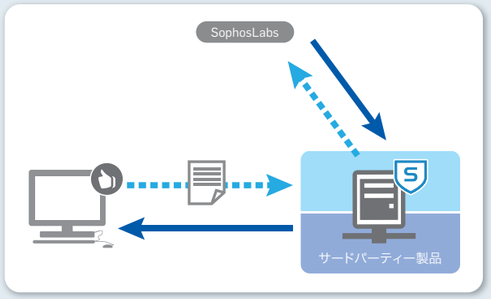
Sophos Anti-Virus Interface (SAVI)
Sophos Anti-Virus Dynamic Interface (SAVDI)
社内の独自アプリケーションに組込み可能な API

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
◎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



❶ クライアントがファイルをアップロードする
❷ 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
❸ 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

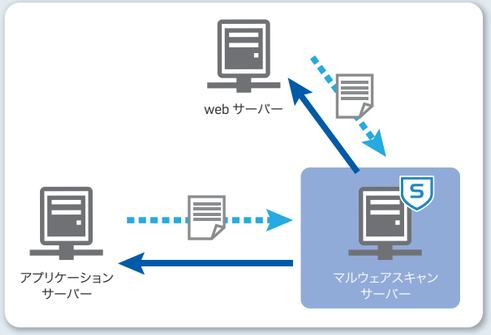
多様なゲートウェイ機能を提供
◎ Email セキュリティ、Email 管理、Web フィルタリング、IM フィルタリング、ファイアウォール

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
❷ 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
❸ 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。
詳細はお問い合わせ下さい。

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

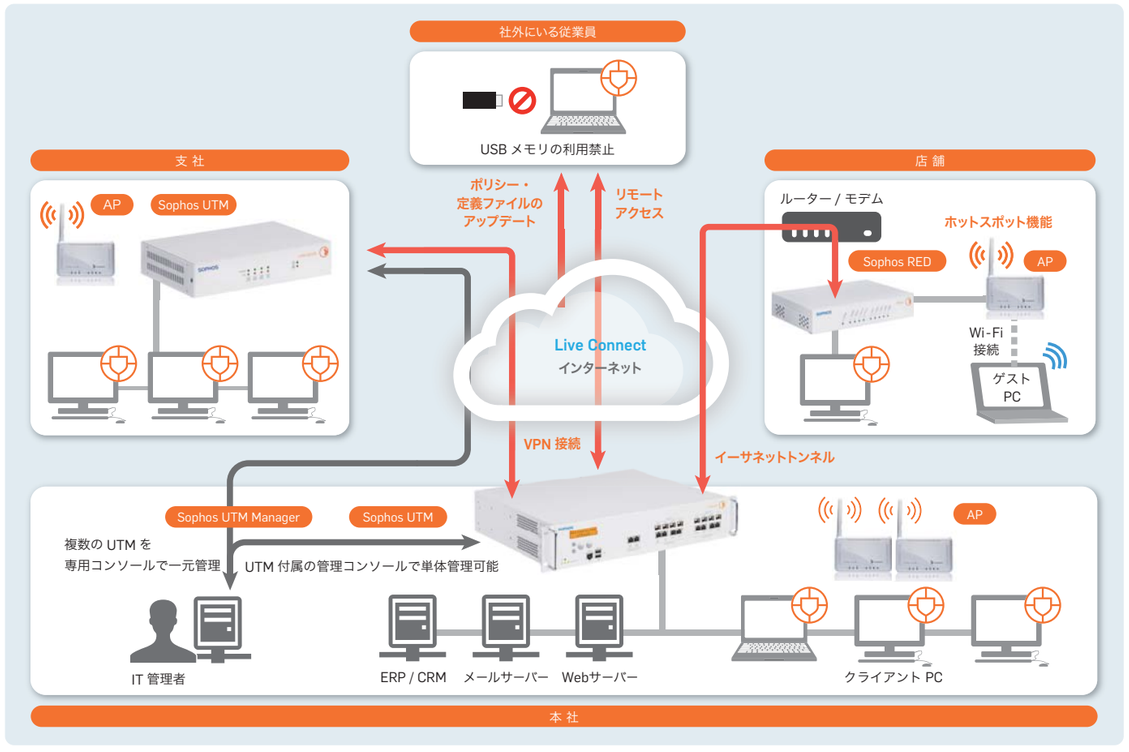
環境にあわせて必要な機能のみ利用できるライセンス体系で提供
製品はハードウェア/ソフトウエア/仮想アプライアンスと
全てのプラットフォームに対応

管理画面

Sophos UTM 管理画面

機能紹介

ネットワークアクセスとセキュリティ



製品紹介

単一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。ハードウェア / ソフトウェア / 仮想アプライアンス (VMware、Citrix、AWS) の中から、
ビジネスに最適なプラットフォームでご提供。

Sophos UTM

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、直感的に使用できるブラウザベースの GUI で製品を簡単に管理
◎単一のモジュール型アプライアンスで、ネットワークからエンドポイントまでカバー
◎ビジネス形態に応じて、ハードウェア、ソフトウェア、または 仮想アプライアンスを選択
◎ファイアウォール、ネットワーキングツール、ルーティングおよびセキュアリモートアクセスなどの基本的なセキュリティ機能を提供
◎各機能がモジュール式になっているため、企業のニーズにあった機能を追加することが可能

スペック	UTM 100	UTM 110	UTM 120	UTM 220	UTM 320	UTM 425	UTM 525	UTM 625
推奨ユーザー数 (人)	10-25	20-50	35-100	81-300	301-800	801-2200	2201-3500	3501-5000
ファイアウォールスループット	250 Mbps	1 Gbps	1.8 Gbps	3 Gbps	3.5 Gbps	6 Gbps	23 Gbps	40 Gbps
VPN スループット	60 Mbps	100 Mbps	180 Mbps	500 Mbps	800 Mbps	2.5 Gbps	4.2 Gbps	5.5 Gbps
IPS スループット	60 Mbps	140 Mbps	420 Mbps	1.2 Gbs	1.9 Gbps	5.5 Gbps	6.8 Gbps	9.1 Gbps
Anti-Virus スループット (Web Proxy)	35 Mbps	50 Mbps	75 Mbps	235 Mbps	375 Mbps	1.4 Gbps	1.7 Gbps	3.8 Gbps
Web Application Firewall スループット	N/A	40 Mbps	85 Mbps	490 Mbps	900 Mbps	1.7 Gbps	2.3 Gbps	2.6 Gbps
Eメールスキャン数	10,000 通/時	20,000 通/時	30,000 通/時	52,000 通/時	78,000 通/時	160,000 通/時	200,000 通/時	250,000 通/時
同時接続数	20,000	40,000	300,000	1,000,000	2,000,000	3,000,000	4,500,000	6,000,000
インターフェース	(4) GE	(4) GE	(4) GE	(8) GE	(8) GE	(6) GE +(2) SFP	(8) GE (+ 拡張スロット 1)	(8) GE (+ 拡張スロット 2)
ストレージ容量	250GB	250GB	250GB	250GB	250GB	320GB	2*500GB	2*450GB

Sophos SG

ミッドレンジ向けアプライアンス製品

◎従来の Sophos UTM に比べて、著しくハードウェアパフォーマンスが向上
◎ソケット式の FleXi Port LAN インターフェースにより、お客様のニーズにより拡張可能
◎ 10 GB イーサネットに対応 (オプション)
◎ホットスワップ冗長電源（オプション SG450 のみ）
◎ SSD 搭載 (SG230/SG310/SG330/SG430/SG450)

スペック	SG 210	SG 230	SG 310	SG 330	SG430	SG450
ファイアウォールスループット	11 Gbps	13 Gbps	17 Gbps	20 Gbps	25Gbps	27Gbps
VPN スループット	1 Gbps	2 Gbps	3 Gbps	4 Gbps	4Gbps	5Gbps
IPS スループット	2 Gbps	3 Gbps	5 Gbps	6 Gbps	7Gbps	8Gbps
Anti-Virus スループット (Web Proxy)	500 Mbps	800 Mbps	1.2 Gbps	1.5 Gbps	2Gbps	2.5Gbps
同時接続数	2,000,000	2,500,000	3,200,000	3,500,000	4,000,000	5,000,000
インターフェース	(6) GE	(6) GE	(8) GE +(2)SFP	(8) GE +(2)SFP	(8) GE	(8) GE
FleXi port slot 数	1	1	1	1	2	2
ストレージ容量	250 GB HDD	120 GB SSD	180 GB SSD	180 GB SSD	240 GB SSD	2*240GB SSD(RAID-1)

製品紹介

アドオン製品

Sophos UTM と組み合せて利用することで、支社・支店等のリモートオフィス環境やワイヤレスネットワーク環境の
セキュリティを簡単に構築できるソリューションをご提供。

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 アプライアンスに転送され、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 アプライアンス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

スペック	RED10	RED50
最大ユーザー数	無制限	無制限
最大スループット	30Mbps	360Mbps
LAN インターフェース	4×10/100 Base-TX	4×10/100/ 1000 Base-TX
WAN インターフェース	1×10/100 Base-TX	2×10/100/ 1000 Base-TX
電 源	110 ～ 240 V、50 ～ 60 Hz、最大 1A	100 ～ 240 V、50 ～ 60 Hz、1.3 A

Sophos Wi-Fi Access Point

安全で信頼性のある Wi-Fi アクセスを提供
Sophos Wi-Fi Access Point 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

◎ローカルの設定が不要なアクセスポイントにより、情報はワイヤレスコントローラに集中され、
最小化
◎中心となる Sophos UTM アプライアンスが提供する完全なセキュリティ機能によって、
すべてのワイヤレスクライアントを速やかに保護
◎アップグレードに費用がかからず、将来的なテクノロジーに簡単に移行することができるため、
無線 LAN の総所有コストが低減

スペック	AP10	AP30	AP50
最大ユーザー数	10 ユーザーまで	30 ユーザーまで	50 ユーザーまで
最大スループット	150Mbps	300Mbps	300Mbps
複数 SSID	8	8	8
LAN インターフェース	1×10/100 Base TX	1×10/100 Base TX	1×10/100 /1000 Base TX
ワイヤレスインターフェース	802.11 b/g/n 2.4GHz	802.11 b/g/n 2.4GHz	802.11 b/g/n 2.4GHz/5GHz
PoE (Power over Ethernet)	ー	802.3af	802.3at (PoE+)
アンテナ数	1 × 外部	3 × 内部	2 × 外部
無線数	1	1	2
電 源	90-240V、50/60Hz	90-240V、50/60Hz	100-240V、50/60Hz

ライセンス

機 能	Essential Firewall	Network Protection	Web Protection	Email Protection	Web Server Protection	Wireless Protection	Endpoint Protection	FullGuard	BasicGuard
Network Firewall	●	●	●	●	●	●		●	●
ネットワークマスカレード/NAT	●	●	●	●	●	●		●	●
ネイティブ Windows リモートアクセス	●	●	●	●	●	●		●	●
DHCP、DNS、NTP サービス	●	●	●	●	●	●		●	●
高可用性（HA構成）		●	●	●	●	●		●	
ディレクトリ認証		●	●	●	●	●		●	●
ユーザーポータル		●	●	●				●	●
侵入防御（IPS）		●						●	●
DoS 防止		●						●	●
SSL & IPSecサイト間VPN		●						●	●
SSL & IPSec リモートアクセス		●						●	●
VoIP セキュリティ		●						●	●
WAN リンク & サーバー負荷分散		●						●	2 リンクのみ
コマンド&コントロール (C&C) 通信の検出		●						●	
ボットネット通信の検出		●						●	
IPS ルールのマニュアル変更		●						●	●
2 要素認証		●						●	
モバイルアクセス制御（VPN）※		●						●	
モバイルアクセス制御（Wi-Fi）※						●		●	
ポリシーテスト機能			●					●	
認証プロキシ & 透過型プロキシ			●					●	●
SEC との Web コントロールポリシー連携			●					●	
URL フィルタリング			●					●	●
スパイウェア防止			●					●	●
HTTP/S スキャン			●					●	●
アプリケーションコントロール			●					●	●
HTTP/S & FTP プロキシ			●					●	●
ユーザー/Web レポート			●					●	●
Dualアンチウィルススキャン			●	●	●			●	SAV のみ
スパム対策				●				●	RBL のみ
SMTP & POP3 プロキシ				●				●	●
フィッシング対策				●				●	●
メール暗号化（S/MIME、OpenPGP、TLS）				●				●	
SPX メール暗号化 (SPX Email Encryption)				●				●	
Web Application Firewall					●			●	
リバースプロキシ & 認証リバースプロキシ					●			●	
ワイヤレスセキュリティ						●		●	1アクセスポイントのみ
クライアントアンチウイルス & HIPS									
デバイスコントロール									

※ Sophos Mobile Control が必要

Essential Firewall (無料)

◎ビジネス用ファイアウォール
◎ネットワークファイアウォール、NAT、ネイティブ Windows
リモートアクセスなど機能を提供

Network Protection

◎支社・支店への柔軟なセットアップ、リモートアクセス VPN 接続が
可能
◎完全統合型の侵入防御システムを通じ、DoS 攻撃や高度なワーム、
ハッカーの侵入を防御

Web Protection

◎ Web サイト閲覧をフィルタリングし、Web を通じた脅威の侵入を
防ぐとともに、社員の Web 閲覧を制御

Email Protection

◎企業のメールをスパムやウイルスから保護すると同時に、
機密情報の漏えいを防ぐ

Web Server Protection

◎ Web サーバーと Web アプリケーションを保護し、
最新の攻撃やデータの流出を防止

Wireless Protection

◎信頼性の高い安全なワイヤレスネットワークを簡単に実現

Endpoint Protection

◎ Windows PC のアンチウイルス、デバイスコントロールを実現
◎ネットワークを介さない脅威からもエンドポイントを保護

FullGuard

◎ Sophos UTM Endpoint Protection を除くすべての機能を提供

BasicGuard

◎小規模向けのエントリーライセンス
◎企業の保護対策に必要な基本的な機能を提供
※ BasicGuard は、Sophos UTM 100 および UTM 110 アプライアンスでのみ利用可能

Sophos 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

2. 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

添付ファイルとメール本文を丸ごと暗号化

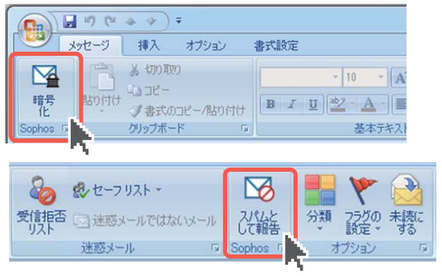
SPX メール暗号化
◎通常使用しているメールクライアント（Outlook など）からメール送信する際に、ポリシーに準拠してメール本文と添付ファイルを PDF に変換して暗号化！受信側に特別なソフトウェアのインストールは不要。また、パスワードはアプライアンスが自動生成し提供するため送信者が管理する必要はなく（受信者による設定も可能）、パスワードを忘れた場合でもユーザー自身で復旧や再設定が可能。

メール環境設定機能

暗号化するメッセージにマーク付け
◎メニューバーに表示されている暗号化ボタンをワンクリックで、SPX メール暗号化で送信するメールにマーク付け可能

スパムメールにフラグを設定
◎フラグを設定されたメッセージは、解析のために、直ちに SophosLabs に送信

※ SPX メール暗号化を利用するには、Sophos Email Appliance (ハードウェア / 仮想) が必要になります。



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

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	38 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

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、SPX メール暗号化※、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

スペック	Sophos Email Appliance
提供形態	ハードウェア (別売) / 仮想アプライアンス
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)	●
DLP	●
SPX メール暗号化	●

Sophos Server Protection

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。

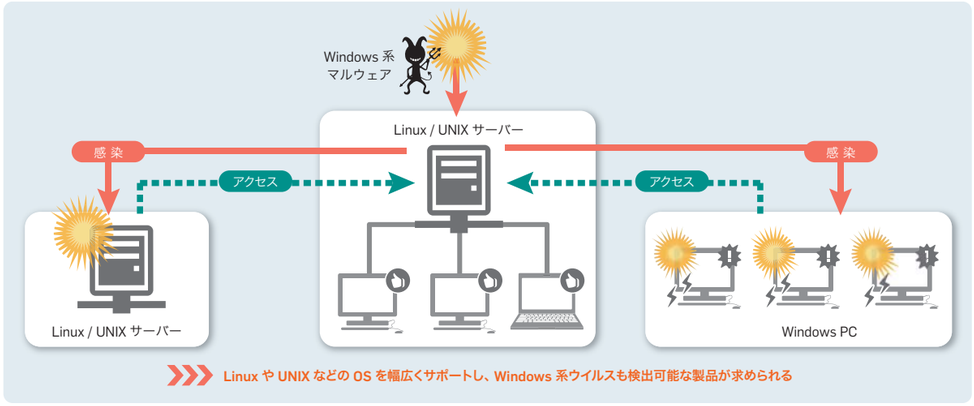
2. 利用中のウイルス対策ベンダーの製品が対応していない

Sophos 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。



まとめ：サーバーをウイルスから保護する理由は？

1. サーバー自体の感染を防ぐ (被害者になることを防ぐ)
2. サーバーにアクセスした PC への感染を防ぐ (加害者になることを防ぐ)

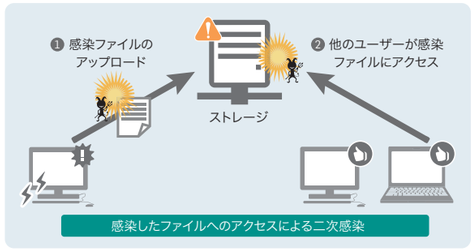
Sophos for Network Storage

主な特長

ストレージにおけるウイルス対策の必要性

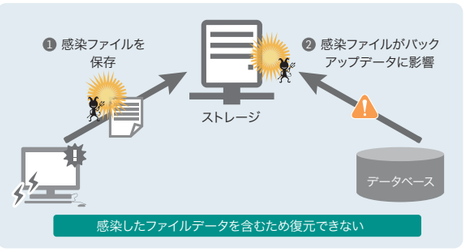
1. ウイルス拡散ポイントにならないために

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。



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。



3. ガイドラインに準拠するために

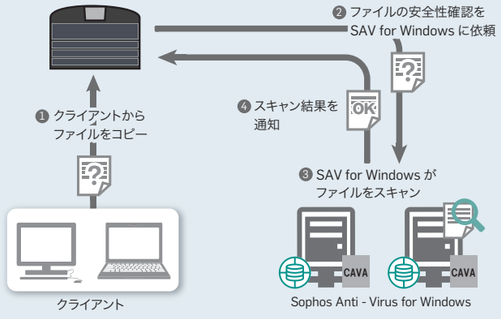
政府機関の情報セキュリティ対策のための統一基準 - 内閣官房情報セキュリティセンター
【基本遵守事項】
「情報システムセキュリティ責任者は電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く）にアンチウイルスソフトウェア等を導入すること」

「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。

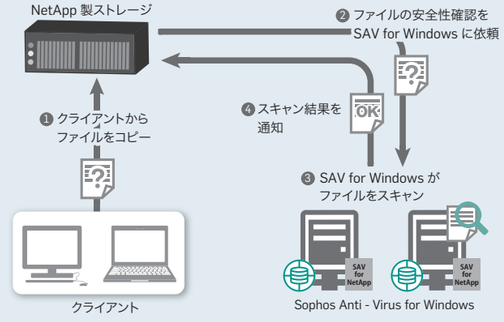
出典：「政府機関の情報セキュリティ対策のための統一基準」
http://www.nisc.go.jp/active/general/kijun01.html

推奨される利用例

EMC Celerra / VNX / VNXe



NetApp Data ONTAP



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
◎ 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
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。

PureMassage

主な特長

1. 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、ゲートウェイでブロック

ボットからのスパム対策（PMU のみ）

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

メールフィルタリングのフロー概要

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 Anti-Virus for vShield

主な特長

1. 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

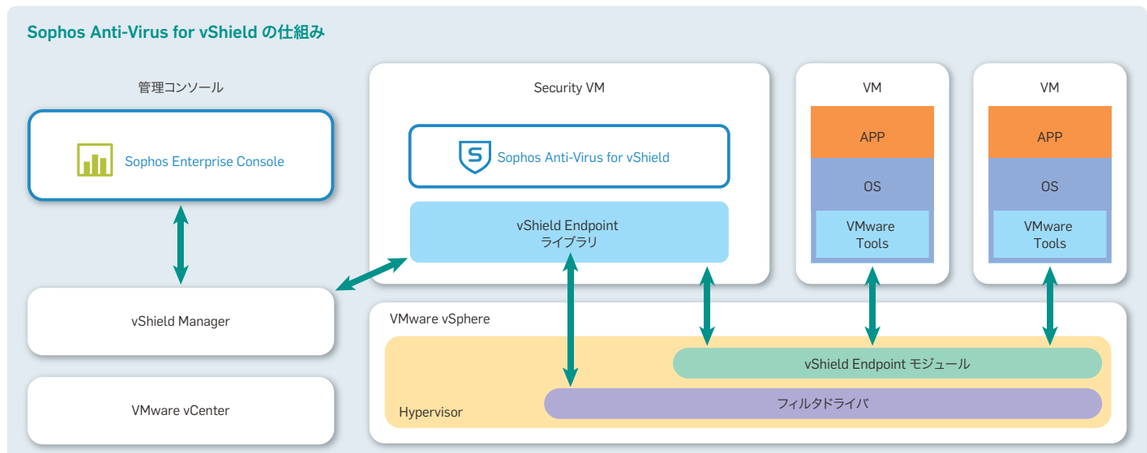
◎サーバーのリソース消費を抑制 (マシン集約率の向上)

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の保護
◎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

Sophos Anti-Virus for vShield の仕組み



ゲストサーバー用：Sophos Anti-Virus for vShield が利用できるライセンス

Sophos Server Protection

ゲストクライアント用： Sophos Anti-Virus for vShield-VDI が利用できるライセンス

Sophos Anti-Virus for vShield - 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 Cloud

主な特長

1. 管理サーバーの設置が不要
◎サーバーを構築や設置が不要なので、初期導入コストを抑えて、
最新のセキュリティ対策が可能。

2. ユーザーベースのポリシー
◎システムやデバイスを問わずに、
ユーザー単位でポリシーを適用可能。

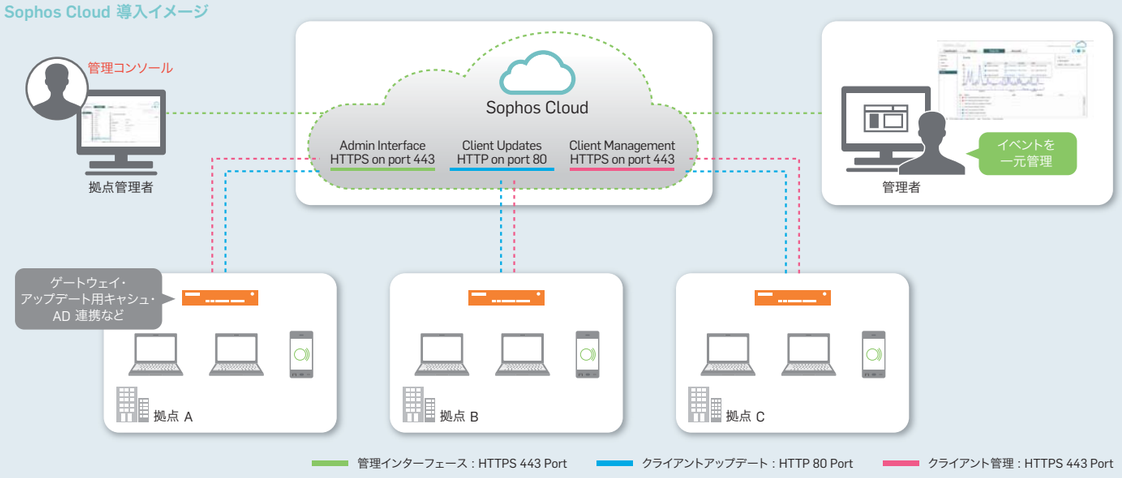
3. Web ベースの統合管理コンソール
◎ Web ベースの管理コンソールで一元管理が可能。
接続場所を問わず、管理コンソールを利用可能。

4. わかりやすいレポート
◎シンプルなダッシュボード、通知システムだけでなく、
わかりやすいレポートで、簡単にセキュリティ状態を把握可能。

5. アップデートの管理が不要
◎管理サーバーやクライアントエージェントは、
ソフォスがアップデート管理を行い、
管理者によるアップデートは不要。

6. 柔軟な拡張性
◎ 今後、様々な機能を統合予定。
(Sophos UTM / Sophos Mobile Control / 暗号化など)

Sophos Cloud 導入イメージ



機能紹介

ウイルス対策
◎ Windows と Mac をサポートし、他の OS (Linux 等) で
動作するマルウェアも検出可能

ライブプロテクション
– Sophos Live Web Filtering
アクセスする URL をクラウド型のデータベースですぐに検索し、
危険な Web サイトへのアクセスをブロック

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

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

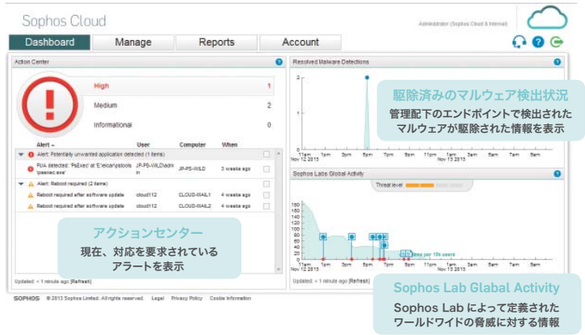
– Sophos Live Anti-Virus
クラウド型のデータベースを参照し最新の脅威から保護

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

Web ベースの管理コンソール



Web 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

簡単に導入
◎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するため、
外出先でも適切に保護

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

◎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	License			
	Sophos Cloud Enduser Protection	Sophos Cloud Endpoint Protection Advanced	Sophos Cloud Endpoint Protection Standard	Sophos Cloud Mobile Management
マルウェア対策	● ※1	● ※1	● ※1	
HIPS	● ※1	● ※1	● ※1	
Sophos Live Antivirus	● ※1	● ※1	● ※1	
Sophos Live Web filtering	● ※1	● ※1	● ※1	
Web フィルタリング (カテゴリ)	● ※2	● ※2		
Web フィルタリング (ファイルタイプ)	● ※2	● ※2		
Web フィルタリング(ホワイトリスト/ブラックリスト)	● ※2	● ※2		
デバイスコントロール	● ※1	● ※1		
Active Directory Sync	●	●		
モバイルデバイス管理	● ※3			● ※3

※ 1 Windows / Mac で利用可能
※ 2 現在 Windows のみ対応。 Mac は今後対応予定
※ 3 iOS で利用可能

お得なサイトライセンスのご紹介 ～台数無制限で利用可能～

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。
製品名	Sophos Endpoint Protection – Advanced（スクールパックライセンス）
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	Sophos Endpoint Protection – Advanced の仕様に準じます。
価 格	

契約年数	1 年契約	2 年契約	3 年契約	4 年契約	5 年契約
単 価※	85,000 円	170,000 円	255,000 円	340,000 円	425,000 円

※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

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が大幅に軽減されます。
製品名	Sophos Enduser Protection（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	Sophos Enduser Protection 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	Sophos Enduser Protection（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	Sophos Enduser Protection 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）

	通常の購入方法		自治体ライセンス
	クライアント	サーバー	クライアント / サーバー
該当製品	Sophos Enduser Protection	Sophos Anti-Virus サーバーライセンス	Sophos 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	購入数が上限		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

医療パックライセンス

病院などの医療機関を対象とした、病床数の数まで利用可能な包括ライセンス

特 長	病床数による契約で、病床数の数まで PC やサーバーを保護。医師、看護師の自宅の PC でも利用でき、コスト削減を実現
製品名	Sophos Enduser Protection (医療パックライセンス)
対 象	病院、診療所、薬局など各地方厚生局・厚生支局へ医療機関として登録されている保険医療機関、保健薬局
利用範囲	院内の PC、サーバー、医師および看護師の自宅 PC で利用可
機 能	Sophos Enduser Protection の仕様に準じます。
価 格(税別)	

病床数	20 床未満	20 – 100 床	101 – 200 床	201 – 300 床	301 – 400 床	401 – 500 床
1 年	19,900 円	150,000 円	300,000 円	495,000 円	700,000 円	900,000 円
5 年	55,000 円	450,000 円	900,000 円	1,485,000 円	2,100,000 円	2,700,000 円

※ 501 床以上、または保護するデバイスの台数が病床数を上回るときは個別見積もりにて対応いたします。
※ 病床がない場合、20 床未満扱いとなります。

無償ツールのご紹介

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
◎簡単なインストール
★ http://www.sophos.com/ja-jp/products/free-tools/virus-removal-tool.aspx

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 UTM Essential Firewall - ビジネス用の無償ファイアウォール

基本的なセキュリティ機能を提供し、どんなビジネスネットワークも保護
◎どんなビジネスにも対応する基本的なネットワークセキュリティ機能を提供
◎ユーザー / IP 数の制限なく、ソフトウェアや仮想アプライアンスとして利用可能
◎全ての機能を備えた Sophos UTM アプライアンスへの簡単なアップグレードが可能
★ http://www.sophos.com/ja-jp/products/free-tools/sophos-utm-essential-firewall.aspx

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/ja-jp/products/free-tools

販売パートナー

お問い合わせ

ソフォス株式会社
www.sophos.com/ja-jp
〒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　Email sales@sophos.co.jp

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

1405_CH(6)