Intercept X Advanced with XDR

評価導入手順書

本ドキュメントに関する注意事項

このドキュメントは、弊社サービスで使用する一般的な設定を、簡単なステップで構築するための補助資料であり、導入に際して必要な全てのトピックについて網羅・解説することを意図したものではありません。個々のトピックについての詳細は、弊社 Web に公開されております製品マニュアル及びナレッジベース記事をご確認頂くようお願いします。

サービスの仕様は予告なく変更されるため、本ドキュメントに記載した内容と異なる場合がございます。

弊社テクニカルサポートでは、本ドキュメントに関するサポートはいたしません。本ドキュメントに関するご質問は、ご購入前の技術的なお問い合わせ先までご連絡頂くか、該当箇所をマニュアルで確認のうえ、テクニカルサポートまでご質問ください。

ソフォス株式会社

https://www.sophos.com/ja-jp.aspx

Sophos Central Admin ガイド

https://docs.sophos.com/central/Customer/help/ja-jp/index.html

評価導入手順書・オンラインデモ

https://news.sophos.com/ja-jp/2022/04/15/japanese-manual/

ナレッジベース

https://support.sophos.com/support/s/?language=ja

ご購入前の技術的なお問い合わせ

メールアドレス techjp@sophos.co.jp

文書更新履歴

(必要に応じて追記すること – 削除不可)

Version	Name	Date	**Comments**
1.0	Sophos	2017/07/07	Central Intercept X (CIX) 初版
2.0	Sophos	2022/04/01	Intercept X Advanced with XDR に更新
3.0	Sophos	2022/04/19	多要素認証の PIN を 4 桁に更新
4.0	Sophos	2022/07/19	一部リンク切れを修正
5.0	Sophos	2023/06/05	画像差替えおよび一部文言を修正
6.0	Sophos	2024/07/01	サーバーと端末用を統合、仕様変更に沿った修正
7.0	Sophos	2025/01/23	仕様変更に沿った修正

目次

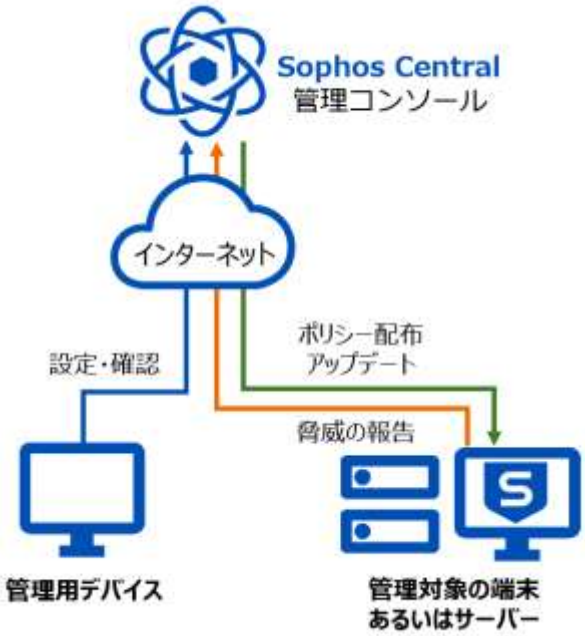
1 はじめに

このたびは Intercept X Advanced with XDR をご評価いただきまして誠にありがとうございます。
本ドキュメントは以下の目的と対象を想定し、内容を作成しております。

目的：Intercept X Advanced with XDR と統合管理コンソールである Sophos Central Admin の基本的な動作、設定、および運用を理解する

対象：運用開始前に設定方法を確認されたい方、およびソフォス製品を学習されたい方

以下は本手順書で想定している構成イメージです。評価導入を想定したインストール方法を記載いたします。



手順書に記載している表記は Sophos Central の表記に沿って記載しております。

Intercept X Advanced with XDR と Sophos Central Admin のご使用にあたり、あらかじめ下記 2 点をご案内いたします。

(1) Sophos Central 管理コンソールにおけるライセンスカウントについて

Sophos Central では、インストール方法等によって、ライセンスの使用状況が実際のユーザー数よりも一時的に多く表示される場合がありますが利用上の問題はありません。

(2) Sophos Central 管理コンソールのデザインについて

Sophos Central は、ユーザービリティ向上のために、予告せず画面デザインを変更することがあります。その場合は、変更された画面に従って操作をお願いします。

2 システム要件

本章では、Intercept X Advanced with XDR の導入に必要なシステム要件を説明します。

2.1. Intercept X Advanced with XDR

- Windows（クライアント OS）

  ❖ システム要件

  ・ 必要メモリ　　4GB 以上
  ・ 空きディスク容量 8GB 以上
  ・ 必要コア数　　2 コア以上
  ・ ディスクの種類　起動ドライブには SSD を使用することを強く推奨します。

  ※最新のシステム要件は以下のリンクを参照してください。

  システム要件

  https://support.sophos.com/support/s/article/KBA-000003229

  ❖ 対応プラットフォーム (コンピュータ)

  対応プラットフォームは以下のリンクを参照ください。

  対応プラットフォーム

  https://support.sophos.com/support/s/article/KBA-000009867

- Mac

  ❖ システム要件

  ・ 必要メモリ　2GB 以上
  ・ 空きディスク容量 2GB 以上

  ※最新のシステム要件は以下のリンクを参照してください。

  https://support.sophos.com/support/s/article/KBA-000002792

  ❖ 対応プラットフォーム

  対応プラットフォームは以下のリンクを参照ください。

  https://support.sophos.com/support/s/article/KBA-000002792

- Windows（サーバーOS）

  ❖ システム要件

  ・ 必要メモリ　　8GB 以上
  ・ 空きディスク容量 10GB 以上
  ・ 必要コア数　　2 コア以上

  ※最新のシステム要件は以下のリンクを参照してください。
  https://support.sophos.com/support/s/article/KBA-000003024

  ❖ 対応プラットフォーム（サーバー）

  対応プラットフォーム、および対応エディションについては以下のリンクの
  エクセルシートを参照してください。
  https://support.sophos.com/support/s/article/KBA-000009867

- Linux Server

  ❖ システム要件

  ・ 空きディスク容量:　2.5GB
  ・ メモリ:　2GB
  ・ システムの種類:　x86_64 および ARM64
  ・ systemd がサポートされ、実行されている
  ・ glibc 2.17 以降
  ・ ARM64: glibc 2.18 以降
  ・ Bash がインストール済み

  ※ARM64 システムでは、5.3 以上のカーネルが必要です。5.3 リリースより前のカーネルプローブ（kprobes）では、ユーザー空間のアクセスモニターがサポートされていないため、対応していません。これは、一部の ARM SoC (System-on-Chip) デバイスに影響を与えます。
  ※Sophos Protection for Linux: SUSE Linux Enterprise Servers にインストールする場合の追加の前提条件を参照してください。
  https://support.sophos.com/support/s/article/KBA-000008293

❖ 対応プラットフォーム

最新の対応プラットフォームは以下のリンクにあります“システム要件” を参照してください。

https://docs.sophos.com/releasenotes/output/ja-jp/esg/linux_protection_rn.html

※テスト済みプラットフォームバージョンの最新の 2 つのマイナーリリースのみが完全にサポートされます。

※対応プラットフォーム（OS）のサポート終了日は以下のリンクを参照してください。

https://support.sophos.com/support/s/article/KBA-000002876

2.2. Sophos Central Admin へ接続するツール

- ブラウザ
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox
  - Apple Safari (Mac のみ)

  ※対応するブラウザについての最新情報は、以下のソフォス Web サイトを参照してください。
  https://docs.sophos.com/central/customer/help/ja-jp/ManageYourAccount/SupportedBrowsers/index.html
  ※Sophos Central は、モバイルデバイスには対応していません。

2.3. 通信要件

- インストール、ポリシー配布、イベント通知、アップデート時等の通信
  - 通信方向
    - サーバー → インターネット
  - 接続先ドメイン

※最新の情報につきましては、以下のソフォス Web サイトを参照してください。
https://docs.sophos.com/central/customer/help/ja-jp/PeopleAndDevices/ProtectDevices/DomainsPorts/index.html

  - ポート
    - TCP 443（HTTPS）
    -

- マルウェア検知機能等での通信

  Live Protection など、利用する機能によってサーバーから Sophos Labs に通信が発生します。通信の詳細につきましては、以下のソフォス Web サイトを参照してください。
  https://support.sophos.com/support/s/article/KBA-000002701

3 Sophos Central の無償評価登録

本章では、Sophos Central および Intercept X の評価に必要となる無償評価ライセンスの登録手順を説明します。

ソフォスのホームページよりユーザー情報をご登録いただき、Sophos Central Admin へのログイン ID を作成する手順となります。今まで Sophos Central へ登録したことのない、受信を確認できるメールアドレスを一つご用意ください。

1. ブラウザにて
   https://www.sophos.com/ja-jp/products/endpoint-antivirus/free-trial
   にアクセスします。
   “無償評価版はこちら”の下にある「登録」ボタンをクリックします。
   ＊販売店経由にてご提供の場合はご担当者にご相談ください。

2. ユーザー情報の入力画面が表示されますので、氏名、メールアドレス、会社情報等を入力し「次へ」を押します。

   入力するメールアドレスが Sophos Central Admin へのログイン ID として登録されます。

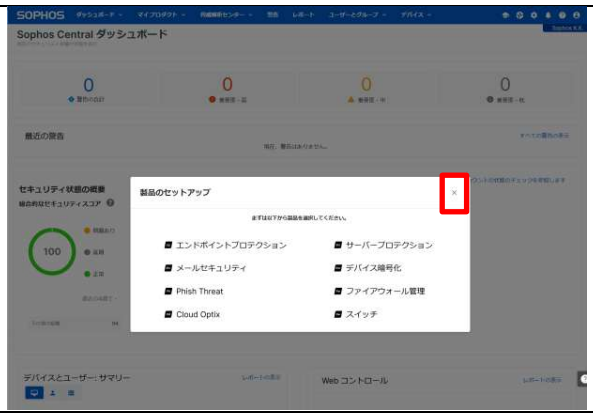
3. 登録が完了すると、右の画面が表示され、数分後に入力したメールアドレスにメールが届きます。

4. メールアカウントに右のようなメールが届きます。
差出人：do-not-reply@central.sophos.com
件名：Sophos Central: アカウントのアクティベーション（有効化）のご案内
または
件名：Activate your Sophos Central account
「パスワードの作成」ボタンを押します。

5. ブラウザが起動され、アカウントのアクティベーション画面が表示されます。右上のプルダウン部分で言語が設定できますので日本語に変更します。
ここで、Sophos Central Admin へログインするためのパスワードと Central Admin ポータルのリージョンを設定します。

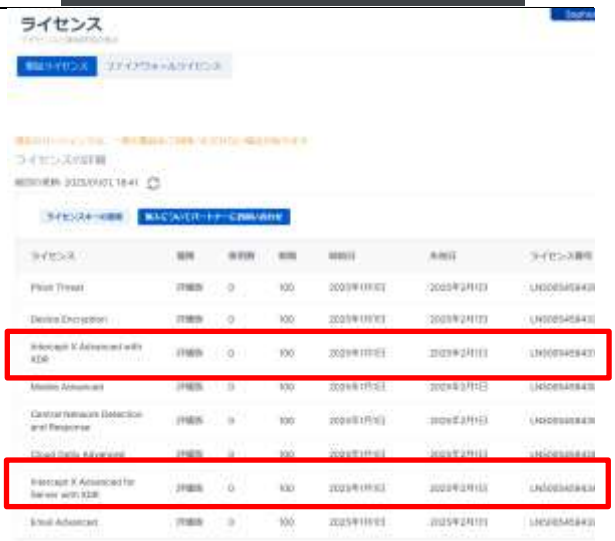
※Central Admin ポータルの場所は、いったんアカウントを作成すると変更することができません。

※データセンターの選択にて“日本”を選択した場合、一部のソフォス製品の管理がで

	きない旨の内容と承認ボタンが表示されます（橙枠）。 該当する製品を利用する場合はデータセンターを**“米国”、“ドイツ”、“アイルランド”から選択**ください。 詳細は以下のソフォス Web サイトを参照ください。 https://support.sophos.com/support/s/article/KBA-000009216 パスワードを入力、Central Admin ポータルのリージョン選択し、規約へ同意いただける場合、規約への同意を示すチェックボックスにチェックを付け「アカウントのアクティベーション」 をクリックします。	
6.	アクティベーションが完了すると、Sophos Central Admin へ自動的にログインされ、Sophos Central Admin のダッシュボードが表示されます。 右図のように「製品のセットアップ」画面が表示された場合は右上の「X」をクリックし、画面を消去します。	

7. ダッシュボード画面右上のアイコン →
「ライセンス」 をクリックし、ライセンス状況の確認を行います。

8. ライセンス画面にて 「Intercept X Advanced with XDR」 が表示されていることを確認します。



9. ダッシュボード画面右上のアイコン →「サインアウト」 をクリックし、ログアウトします。

   以上で、無償評価登録は終了です。

4 Sophos Central Admin へのログイン

本章では、Sophos Central Admin にログインする手順を説明します。

1. ブラウザより
   https://central.sophos.com のアドレスへアクセスします。
   ログイン画面が表示されますので、
   3 章 2 項で指定したメールアドレスを入力し「続行」をクリックします。
   3 章 5 項で指定したパスワードを入力し「サインイン」をクリックします。

2. 多要素認証を設定するための検証コードの入力画面が表示されます。
   また、3 章 2 項で指定したメールアカウントに右下のようなメールが届きます。

   メールの差出人：do-not-reply@central.sophos.com
   件名：Your security code

   メール本文に記載された検証コードを入力し、「続行」をクリックします。

3. 多要素認証（MFA）の設定画面が表示されます。
「今すぐ設定する」をクリックすると QR コードが表示されます。

認証アプリ（Google Authenticator や Microsoft Authenticator など）を用意し、認証アプリの QR コードスキャン機能を利用して、画面に表示された QR コードをスキャンします。

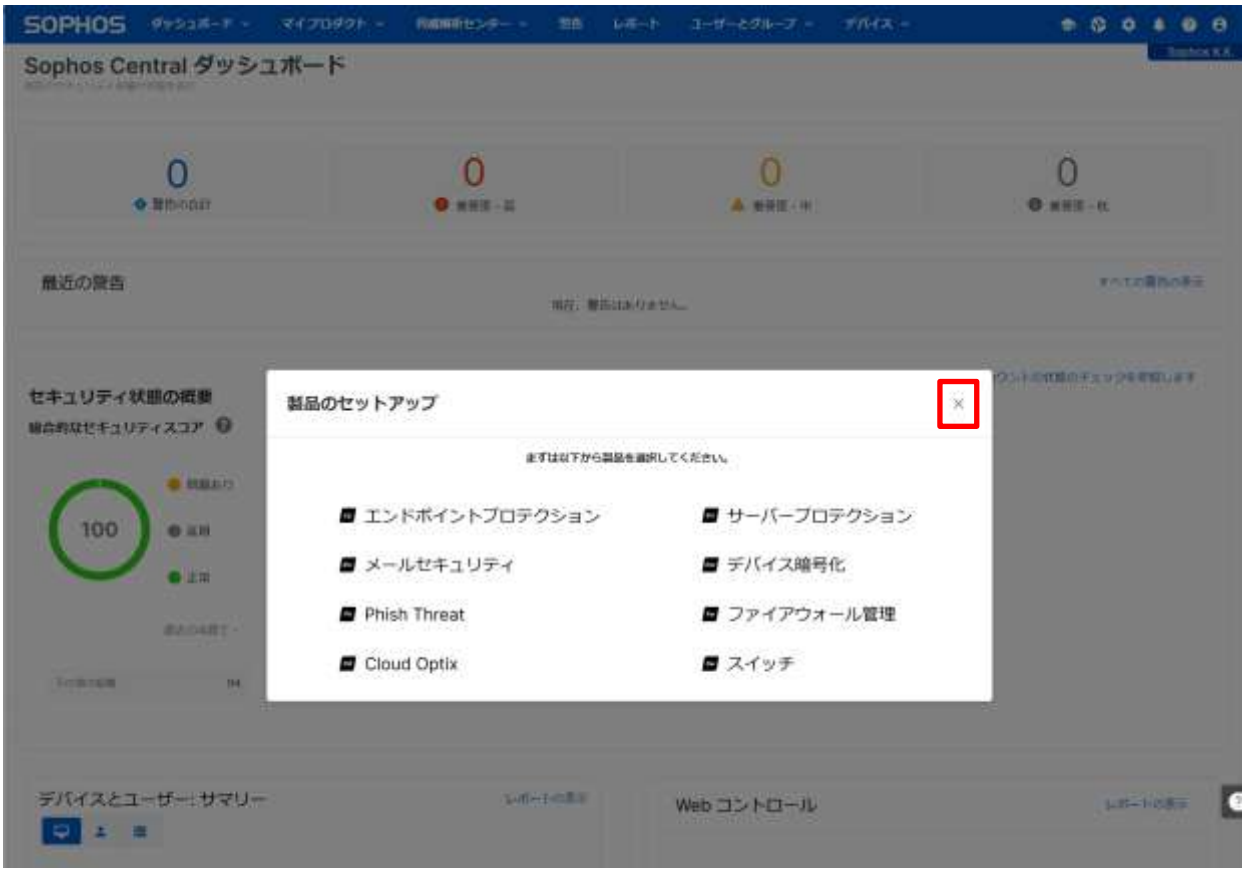
QR コードをスキャンした後、認証アプリにセキュリティコードが表示されますので入力し、「続行」をクリックします。

https://doc.sophos.com/central/customer/help/ja-jp/ManageYourProducts/GlobalSettings/MultiFactorAuthentication/index.html

「登録に成功」の画面が表示されます。
これで多要素認証の設定は完了です。
「続行を」クリックします。

4. Sophos Central Admin へログインされます。

製品のセットアップの右上の「×」をクリックします。



5 エージェントのインストール

本章では、Intercept X Advanced with XDR のエージェントを各エンドポイントへインストールする手順を説明します。
インストールは Sophos Central からインストーラをダウンロードし、インストールする手順となります。ダウンロード方法としまして、Sophos Central Admin にログインしダウンロードする方法と、セットアップリンクを送信し、ダウンロードする方法がありますので、本手順書で説明します。

また、本手順書では割愛しますが、スクリプトによる展開、ディスクイメージでの展開方法等があり、こちらは以下 URL のサポートデータベースをご参照ください。
https://support.sophos.com/support/s/article/KBA-000002941

5.1 Sophos Central Admin からダウンロード

インストーラを管理コンソールからダウンロードして配布します。

1. 4 章の手順で Sophos Central Admin にログインします。
   Sophos Central Admin の画面右上の「デバイス」–「インストーラ」をクリックします。

2. 画面左上にエンドポイントプロテクションに関係するインストーラのリンクが表示されます。

   「Windows 用全機能のインストーラのダウンロード」下部にある「コンポーネントの選択」をクリックします。

3. “デバイスの暗号化”と“ZTNA”のチェックを外した上、「インストーラのダウンロード」をクリックします。

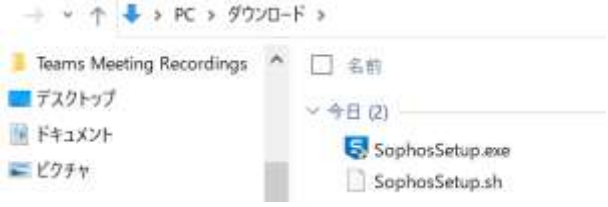
4. Mac の場合も「2」「3」と同様の操作をしてください。

5. 画面の右上部にダウンロードしたファイルが表示されます。（右図は Google Chrome の場合）
フォルダのアイコンをクリックします。

6. エクスプローラが起動されダウンロードしたインストーラが表示されます。
Windows 用：SophosSetup.exe
Mac 用：SophosInstall.zip
となります。

7. Windows Server の場合は画面の中程にある、サーバープロテクションに関係するインストーラのリンクが表示されます。
「Windows Server 用インストーラのダウンロード」をクリックします。

8. エクスプローラが起動されダウンロードしたインストーラが表示されます。
Windows 用：SophosSetup.exe
Linux 用：SophosSetup.sh
となります。



9. Linux Server の場合は、「7」と同じ手順から「Linux サーバー用インストーラのダウンロード」を右クリックし、「リンクアドレスのコピー」をクリックします。このリンクアドレスは Linux Server へのインストール時に利用します。

5.2 セットアップリンクを送信する手順

1. 4 章の手順で Sophos Central Admin にログインします。
   Sophos Central Admin の画面右上の「デバイス」–「インストーラ」に進み、「ユーザーにインストーラーを送信」をクリックすると、指定ユーザーにセットアップのためのメールの送信を行うことが出来ます。そのメール内のリンクへアクセスすることによりインストールができます。

2. ユーザーとグループの画面が表示されます。次に送りたいユーザーのチェックボックスに☑をいれます。

3. 次にセットアップリンクのメール送信をクリックします。

4. セットアップリンクのメール送信のポップアップが表示されます。
チェックボックスに☑を入れて送信をクリックするとセットアップメールが指定のユーザーへ送られます。

5. メールが届いたら Mac または Windows のデバイスのリンクをアクセスするとダウンロードが始まりますので完了後にインストーラを起動してエージェントをインストールします。

5.3 Windows へのインストール

本手順書では、Windows クライアントや Windows サーバーへインストールする手順を説明します。

この操作は Administrator 権限のあるユーザーで行う必要があります。

1. ダウンロードフォルダを開き、インストーラ（Sophos Setup.exe）をダブルクリックします。

2. インストールウィザードが表示され、注意事項が表示されます。右図のような画面が表示されますので、右下の「続行」をクリックします。

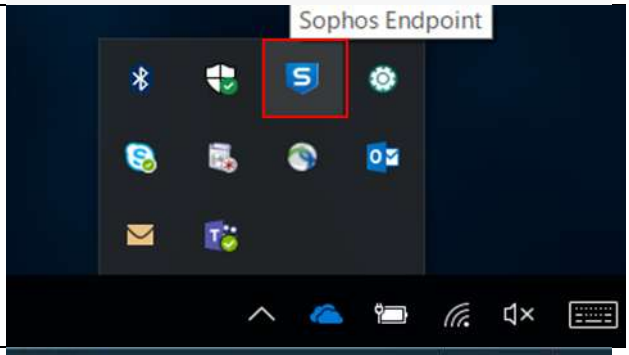
3. インストールされる製品が表示されます。利用する製品に間違いがないことを確認して、「インストール」をクリックします。

4. インストールが自動的に進行します。10 分程度で完了します。

5. インストールが完了したことをお知らせする画面が表示されたら、「完了」をクリックします。

※環境により、コンピュータの再起動を求められる場合があります。

6. コンピュータの再起動後、画面右下のタスクトレイからソフォスのアイコンをクリックします。
エージェントのステータスを確認します。



7. コンピュータのステータス画面が表示されます。
この画面でコンピュータが保護されていることを確認します。
これで Windows へのインストールは終了です、

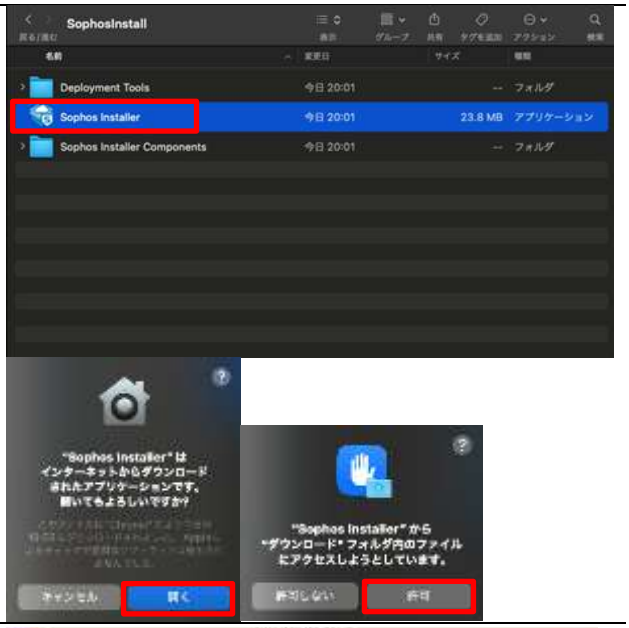
5.4 Mac へのインストール

本手順書では、Mac へインストールする手順を説明します。

この操作は Administrator 権限のあるユーザーで行う必要があります。

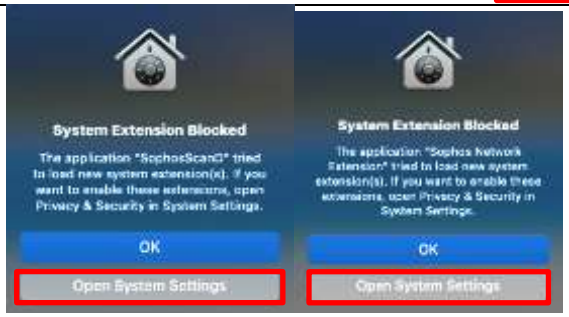
手順は MacOS14 のインストール手順になります。

1. ダウンロードフォルダを開き、インストーラ「SophosInstall.zip」をダブルクリックし、展開します。
   展開された「SophosInstall」のフォルダ配下に「Sophos Installer」があるのでダブルクリックします。
   アクセス許可を求めるポップアップが表示された場合は「許可」をクリックします。



2. インストールウィザードが表示され、インストールされる製品が表示されます。利用する製品に間違いがないことを確認して、「インストール」をクリックします。

3. 途中で「SophosScanD」や「Network Extension」が許可を求めてきた場合は、「システム環境設定を開く」をクリックします。



「プライバシーとセキュリティ」が表示されますので、「詳細」をクリックし、各機能を有効にします。その後、「Network Extension」がネットワークコンテンツのフィルタリングの許可を選択します。

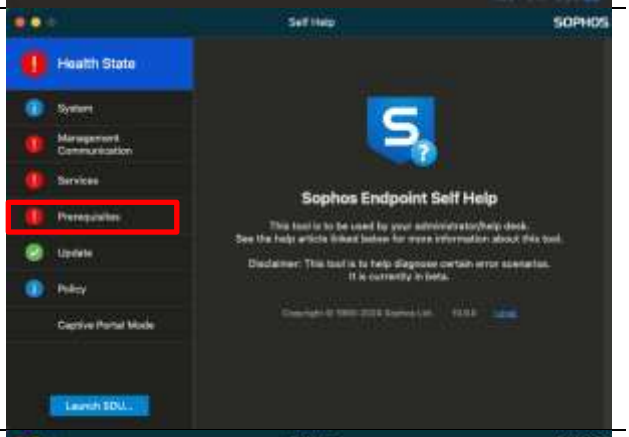
4. インストールが完了したことをお知らせする画面が表示されたら、終了をクリックします。

5. 画面右上にある「Sophos Endpoint」を開き、「一部のソフォスのサービスが実行されていません」と表示される場合は「Sophos Endpoint を開く...」をクリックします。

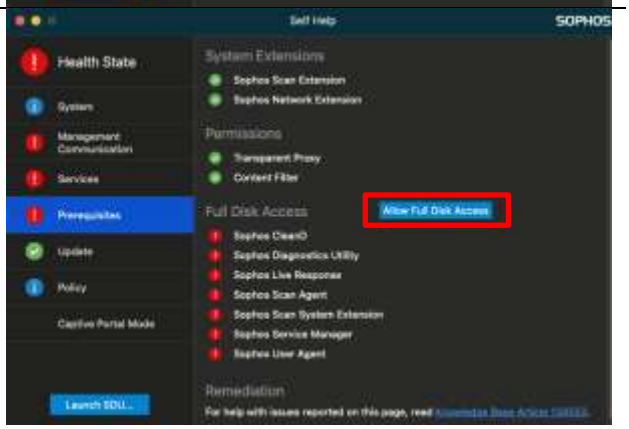
6. Sophos Endpoint 画面が表示されますので、「バージョン情報」をクリックします。

7. 「診断ツールの起動」をクリックします。

8. ヘルスステータスにて、「前提条件（Prerequisites）をクリックします。

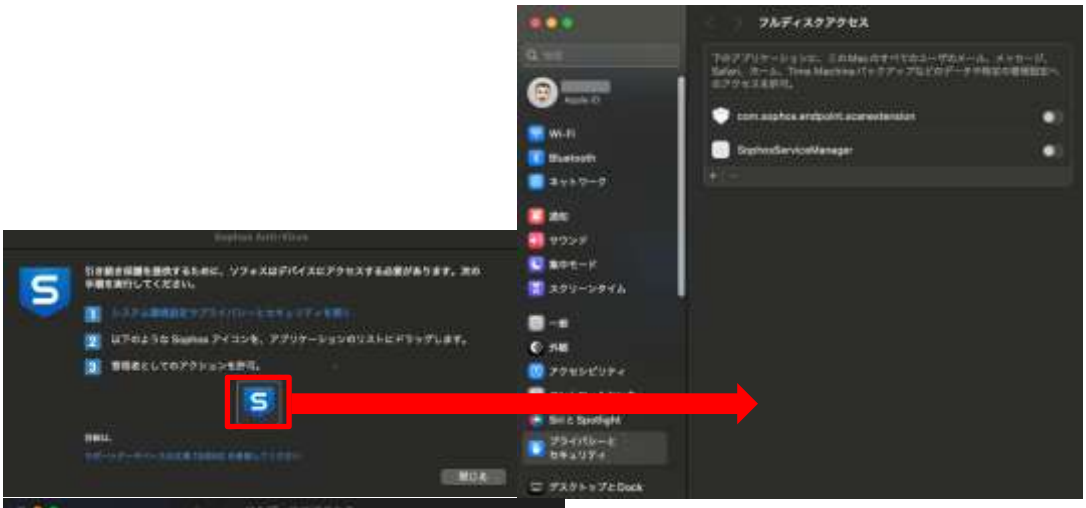


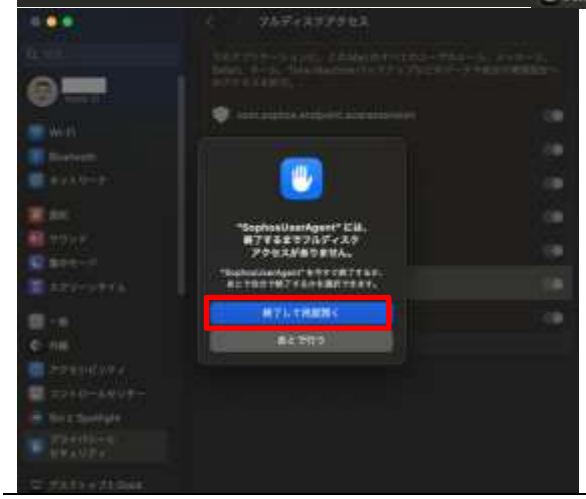
9. 「フルディスクアクセスを許可する（Allow Full Disk Access）をクリックします。



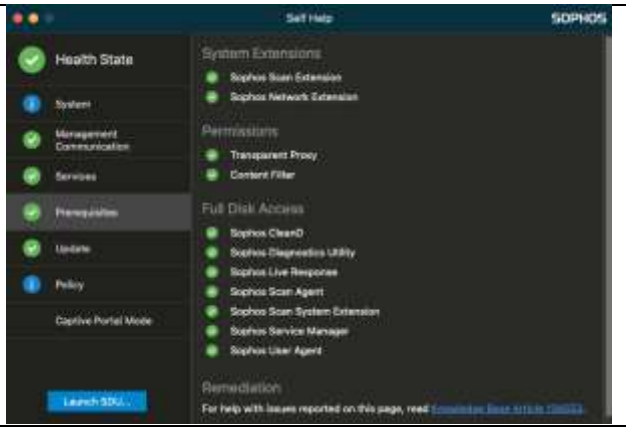
10. 右図のような画面が表示されます。その後、MacOS の「システム設定」から「プライバシーとセキュリティ」―「古ディスクアクセス」を開きます。

11. S アイコンをフルディスクアクセス画面にドラッグ＆ドロップします。設定変更を反映させるためのパスワード入力が求めらますので、入力します。
    また、SophosUserAgent の再起動について聞かれますので許可します。





12. ドラッグ＆ドロップを実行すると赤色のアラートが解消し、インストール完了となります。



13. 以上で Mac へのインストールは終了です。

5.5 Linux Server へのインストール

本手順書では、ダウンロード用リンクアドレスを利用し、Linux Server 側でインストーラをダウンロードしインストールする手順を説明します。

この操作はエージェントをインストールする Linux Server 上で行い、インストールは root 権限のあるユーザーで行う必要があります。

1. wget コマンドにより /tmp にインストーラをダウンロードします。 wget <5.1 節 9 項でコピーしたアドレス> のコマンドを実行します。 リンクアドレスの末尾が SophosSetup.sh のアドレスです。	# cd /tmp/ # wget https://dzr-api-amzn-us-west-2-fa88.api-upe.p.hmr.sophos.com/api/download/<Central の ID>/SophosSetup.sh --2024-06-23 20:36:40-- https://dzr-api-amzn-us-west-2-fa88.api-upe.p.hmr.sophos.com/api/download/7e9743b788dd0b11457d6576d5ba52a4/SophosSetup.sh dzr-api-amzn-us-west-2-fa88.api-upe.p.hmr.sophos.com (dzr-api-amzn-us-west-2-fa88.api-upe.p.hmr.sophos.com) を DNS に問いあわせています... 35.167.137.152, 52.89.5.55, 35.160.231.200 dzr-api-amzn-us-west-2-fa88.api-upe.p.hmr.sophos.com (dzr-api-amzn-us-west-2-fa88.api-upe.p.hmr.sophos.com)|35.167.137.152|:443 に接続しています... 接続しました。 HTTP による接続要求を送信しました、応答を待っています... 200 長さ: 特定できません [application/octet-stream] `SophosSetup.sh' に保存中  [ <=> ] 27,741,322 4.19MB/s 時間 6.8s  2024-06-23 20:36:48 (3.90 MB/s) - `SophosSetup.sh' へ保存終了 [27741322]
2. chmod コマンドでダウンロードしたインストーラに実行権限を付与します。 chmod +x /tmp/SophosSetup.sh	# # chmod +x /tmp/SophosSetup.sh #

3. インストーラを実行します。

   /tmp/SophosSetup.sh

   インストールはコンポーネントをダウンロードしながら行われるため、しばらく時間がかかります。

   “Successfully installed product” のメッセージが表示されればインストールが終了です。

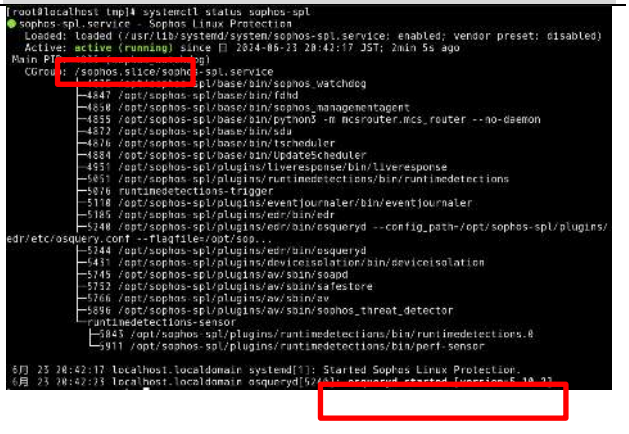
```
# /tmp/SophosSetup.sh
This software is governed by the terms and conditions of a licence agreement with Sophos Limited: https://www.sophos.com/en-us/legal/sophos-end-user-terms-of-use

Performing pre-installation checks to verify whether SPL can be installed on this machine
INFO: Verifying connections to Sophos Central
INFO: Server can connect to Sophos Central directly
INFO: Verifying connections to Sophos Update Service (SUS) server
INFO: Server can connect to the SUS server (https://sus.sophosupd.com) directly
INFO: Verifying connections to the CDN server
INFO: Server can connect to CDN address (https://sdds3.sophosupd.com) directly
INFO: Connection verified to CDN server, server was able to download all SPL packages directly
SPL can be installed on this system based on the pre-installation checks

Installing to /opt/sophos-spl
Installation process for Sophos Protection for Linux started
Attempting to connect to Sophos Central
Successfully verified connection to Sophos Central
Successfully registered with Sophos Central
Downloading and installing Sophos Protection for Linux...
Successfully installed product
```

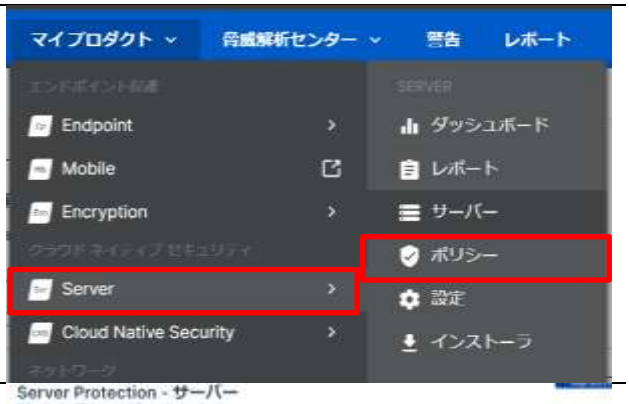
4. root でコマンドを実行します。
   コマンド：systemctl status sophos-spl

   次のメッセージが表示されます。
   active (running)
   Started Sophos Linux Protection
   osquertd started



5. 以下のコマンドを実行します。
   cd /opt/sophos-spl/plugins/av/bin
   ./avscanner /tmp
   tmp 以下がスキャンされます。

6. 4 章の手順で Sophos Central Admin にログインします。
   Sophos Central Admin の画面上部から「マイプロダクト」－「Server」－「サーバー」 と
   クリックします。



7. サーバープロテクションのダッシュボード画面が表示されますので、左ペインから「サーバー」 をクリックします。
   右ペインにサーバーの一覧が表示されます。インストールした Linux Server のコンピュータ名が表示されていることを確認します。

8. 以上で Linux Server へのインストールは終了です。
   ※インストールが正常にされているかを確認するには下記をご参照ください。
   https://support.sophos.com/support/s/article/KBA-000007858

6 ポリシー

本章では、Intercept X Advanced のポリシーの説明をします。

ポリシーは、ユーザー、またはデバイスを保護するために、Sophos Central で適用するセキュリティ設定の集まりです。「Endpoint」-「ポリシー」にて、管理することが出来ます。

エンドポイントのポリシーは各機能（脅威対策、周辺機器コントロール、アプリケーションコントロール、データ流出防止、Web コントロール、アップデートの管理、Windows ファイアウォール）ごとにデフォルトのポリシーが用意されており、エージェントのインストール直後はこのソフォス推奨のデフォルトポリシーが適用されています。

また、Windows ファイアウォールのポリシーについては Windows のみ適用されるポリシーとなります。

6.1 脅威対策ポリシー

脅威対策ポリシーはマルウェア、危険な種類のファイル/Web サイト、および悪質なトラフィック等の脅威に対する設定およびスケジュール検索等の設定が可能です。

6.2 周辺機器コントロールポリシー

周辺機器コントロールは、各サーバーで認証されていない外付けのハードディスク機器、リムーバブル ストレージ メディア、および無線接続機器等の使用をブロックする機能です。リムーバブル ストレージ デバイス、光学ディスクドライブ、およびフロッピーディスクドライブに対しては、読み取り専用の制限を設けることもできます。

6.3 アプリケーションコントロールポリシー

アプリケーションコントロールは、セキュリティ脅威はもたらさないものの、管理者が業務上の使用は不適切と判断する正規のアプリケーションを検知・ブロックする機能です。インスタント メッセージング (IM) クライアント、VoIP クライアント、デジタル画像ソフト、メディアプレーヤー、ブラウザプラグインなど、利用するアプリケーションのコントロールが可能です。

6.4 データ流出防止ポリシー

データ流出防止は、機密情報を含むファイルの転送を監視・制限し、サーバーからのデータ流出事故を防止する機能です。特定の周辺機器 (リムーバブル ストレージ デバイスなど) へのデータ転送や、特定のアプリケーション (メールクライアント、Web ブラウザなど) によるデータ転送を監視・コントロールできます。

6.5 Web コントロールポリシー

Web コントロールは、管理者が従業員の Web 閲覧を制御することを目的にしており、特定のカテゴリのサイト、特定の種類のファイル、特定の Web サイトなどをブロックします。企業を危険にさらす可能性のあるサイトに従業員がアクセスできないように制御し、業務の生産性の確保や使用される帯域幅の制限を行う機能です。Firefox、Google Chrome、Safari、Opera と Microsoft Edge のブラウザをサポートし、他のブラウザでは動作しません。

6.6 アップデートの管理ポリシー

アップデートの管理ポリシーで、ネットワーク上のアップデートを利用可能な状態にする日時を制御できます。設定すると、コンピュータのアップデートは設定した日時になるまで行われません。また、このポリシーでは、長期間アップデートを一時停止することもできます。これを行うには、

カスタムの「ソフトウェアパッケージ」を選択します。
なお、定義ファイルのアップデートについてはこのポリシー設定の有無にかかわらず 60 分に一回、更新データのチェックを行い更新データがある場合、アップデートが実行されます。

6.7 Windows ファイアウォールポリシー

Windows ファイアウォールポリシーを使用して、Windows ファイアウォールを監視・設定 (および他の登録済みファイアウォールを監視) できます。Windows ファイアウォールポリシーは、個別のデバイス (コンピュータやサーバーなど) またはデバイスのグループに適用できます。

7 タンパープロテクション

本章では、Intercept X Advanced のタンパープロテクション機能の設定方法について説明します。

タンパープロテクションは、未承認のユーザーや悪意のあるアプリケーションがソフォスのセキュリティソフトウェアをアンインストールしたり、ソフトウェアの設定を無効設定にしたり、ファイル、レジストリキー、サービス、プロセスの変更を行う動作を阻止する機能です。

7.1 タンパープロテクション：グローバル（全般）設定

グローバル設定でのタンパープロテクション設定は、Sophos Central 全体の設定となり、全台へのタンパープロテクションの有効、無効を設定します。デフォルトで有効に設定されています。

1. 4 章の手順で Sophos Central Admin にログインします。
   Sophos Central Admin 画面上の「マイプロダクト」から 「全般設定」 をクリックします。

2. 各設定項目が表示されます。下へスクロールし、
全般の 「タンパープロテクション」 をクリックします。

3. タンパープロテクションの設定画面が表示されます。
デフォルトで有効に設定されており、ここで OFF にすることにより、サーバー、クライアント全台のタンパープロテクション機能を無効にすることが可能です。
※通常利用時には必ず ON の状態で運用してください。

7.2 タンパープロテクション：コンピュータ設定

コンピュータ設定でのタンパープロテクション設定は、コンピュータ個々にタンパープロテクションを有効、無効にする設定と、コンピュータ側の GUI(Graphical User Interface)にて一時的にリアルタイム検索、ランタイム保護、周辺機器コントロール、アプリケーションコントロール等の設定を変更するためのパスワード表示およびパスワード再作成を行います。

1. Sophos Central Admin 画面上の「マイプロダクト」から 「Endpoint」 をクリックします。

2. Endpoint 画面の左ペインの 「コンピュータ」 をクリックします。

3. 右ペインに Intercept X Advanced がインストールされたコンピュータが表示されます。
対象の Windows の 「コンピュータ名」 をクリックし、コンピュータの詳細画面を表示します。

4. コンピュータの詳細画面が表示されます。
サマリー、イベント、ステータス等の情報が表示可能になります。

5. サマリータブ画面のサマリー部分にタンパープロテクションの項目が表示され、この「タンパープロテクションをオフにする」をクリックすることで、無効に設定することが可能です。

6. 上記以外の方法もございます。
タンパープロテクション項目の 「パスワードの詳細の表示」 をクリックするとパスワ

ードが表示されます。 このパスワードをサーバー側担当者に通知することで、コンピュータ側のGUI(Graphical User Interface)で一時的に設定変更が可能となります。 コンピュータ側担当者が作業終了後、「新しいパスワードの生成」　をクリックしパスワードの再作成を行います。	
7. 以降の操作はコンピュータ側での操作となり、コンピュータ側の GUI(Graphical User Interface)で設定変更する手順となります。	
8. タスクトレイの 「ソフォスのアイコン」をダブルクリックします。	
9. コンピュータのステータス画面が表示されます。 画面右上の 「管理モードサインイン」 をクリックします。	
10. タンパープロテクションのパスワード要求画面が表示されます。 上記 6 項で表示されたパスワードを入力し、「管理モードサインイン」をクリックします。	

11. 画面上部に表示された 「設定」 をクリックすると設定画面が表示されます。

    画面左上のチェックボックスにチェックを入れることで、各機能の無効設定が一時的に可能となります。

    タンパープロテクションの無効はこの画面が設定できます。

    ※通常利用時には必ず ON の状態で運用してください。

8 Sophos Central の管理

本章では、Sophos Central Admin のダッシュボード、ログとレポートについて説明します。

8.1 ダッシュボード

Sophos Central のダッシュボードでは、最新の警告、使用状況のサマリー、Web 利用状況等の情報が表示されます。

1. 4 章の手順で Sophos Central Admin にログインします。
   Sophos Central Admin 画面上部にメニューがあり、クリックすると各項目一覧が表示されます。

2. 「最近の警告」の表示では、警告発生時にマルウェア名、該当ファイル名情報、検知したコンピュータ名の情報が表示されます。
   - 「コンピュータ名」 部分をクリックするとサマリー、イベント、ステータス情報などサーバーの詳細情報が表示されます。
   - 「マルウェア名、該当ファイル名」のリンク部分をクリックするとマルウェア詳細情報が記載されている弊社の Web サイトを表示します。（英語表記のみの場合も有ります）

3. ダッシュボード画面に戻り、「デバイスとユーザー: サマリー」 部分へ進み、コンピュータイコンのタグをクリックします。

4. コンピュータのアクティビティステータスの画面が表示されます。
   この画面では、現在稼働中のコンピュータ（アクティブ）、2 週間以上、2 ヶ月以上、Sophos Central Admin と接続がないコンピュータがグラフで表示されます。
   「レポートの表示」 部分をクリックします。

5. レポートの表示をクリックすることで、サーバーレポート画面が表示され、コンピュータが一覧表示されます。
   画面上段の 「すべて」、「アクティブ」、「2 週間以上非アクティブ」、「2 ヶ月以上非アクティブ」 部分をクリックすることで、クリックした対象のコンピューター一覧が表示されます。
   画面右上の 「カスタムレポートとして保存」、「CSV 形式で出力」、「PDF 形式で出力」 よりコンピューター一覧をデータ出力することが可能です。

6. ダッシュボード画面に戻り、「Web コントロール」 部分に進みます。
   ここでは、Web での脅威検出のブロックおよび Web コントロールポリシーによるブロックと警告の件数が表示されます。

   「ポリシー違反ブロック数」 部分をクリックします。

7. ポリシー違反ブロック数部分をクリックすると詳細の画面が表示されます。
   画面右上の 「カスタムレポートとして保存」、「CSV 形式で出力」、「PDF 形式で出力」 より一覧データ出力することが可能です。

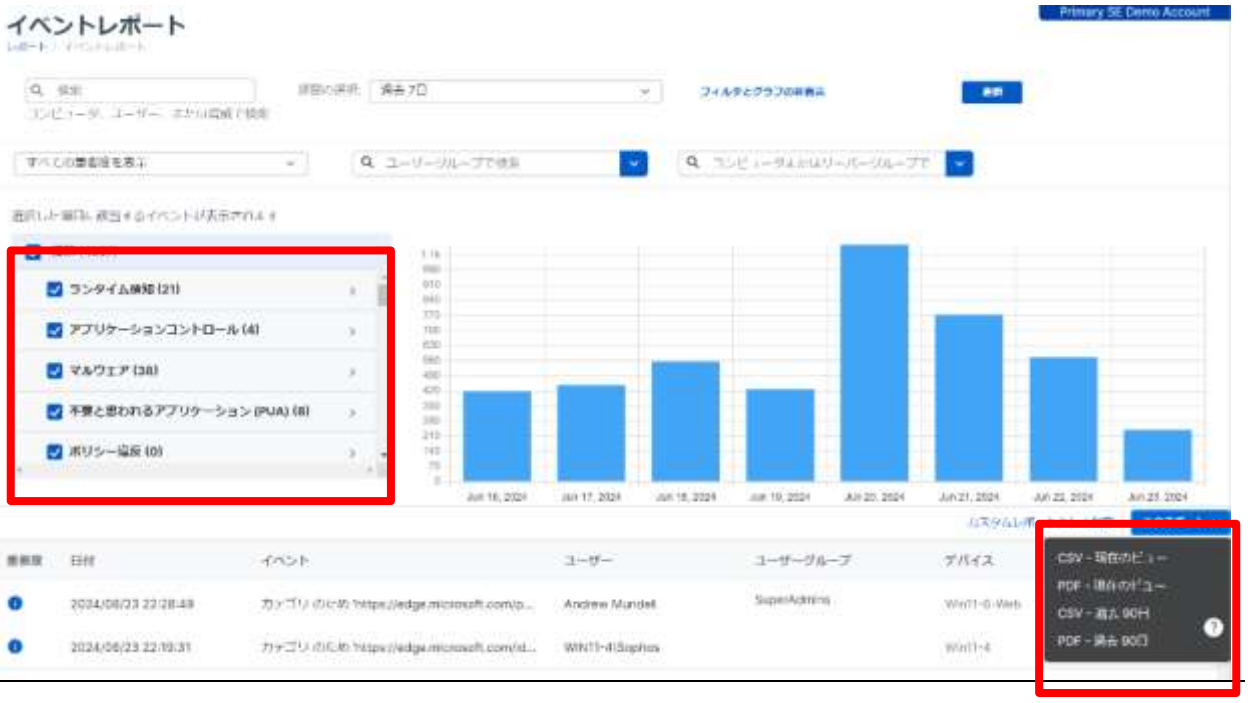
8.2 ログとレポート

Sophos Central のログとレポートでは、すべてのイベント、監査ログ、コンピュータやサーバーの一覧、データ流出防止、アプリケーション コントロール、Web コントロールなどのブロックイベントのレポートが可能となっています。

1. Sophos Central Admin 画面上のメニューより「レポート」をクリックします。クリックすると、出力可能なログ、レポートの一覧が表示されます。

   一般ログの 「イベント」 部分をクリックします。

2. すべてのイベントのグラフ、一覧データが表示されます。
   - 画面左上の 「イベントの種類選択」 により特定のイベントのみを表示することが可能です。(種類選択後、「更新」をクリック)
   - 画面中央右の 「エクスポート」 より CSV または PDF にてデータ出力することが可能です。



8.3 メール通知

Sophos Central ではイベント（「不要と思われるアプリケーション（PUA(Potentially Unwanted Applications)) が検出されました」など）が発生した場合に管理者にメール警告を送信します。尚、同じ種類のイベントに関する警告が、過去 24 時間以内にすでに送信されている場合には警告は送信されません。

1. Sophos Central Admin へのログイン ID（メールアドレス）に警告発生時に右のようなメール通知が行われます。
   この通知後、Sophos Central Admin へログインし詳細を確認します。
   差出人：
   do-not-reply@central.sophos.com

9 インシデントによる Intercept X Advanced with XDR の利用

本章では、マルウェア検出後の EDR/XDR の利用方法について説明します。10 章の 10.1 記載のテストマルウェア eicar を用いた疑似マルウェア攻撃の結果を参考に説明します。

9.1 脅威解析センター

1. Sophos Central Admin 画面上部の「脅威解析センター」 –「ダッシュボード」をクリックします。

2. 「脅威解析センター」画面の左ペインの「脅威グラフ」 をクリックします。

3. 検出された攻撃をクリックします。

4. 攻撃が発生したコンピュータや根本原因、ビーコン（マルウェアなど）、検出日時、クリーンアップ（駆除）されたかどうかを確認します。

5. 推奨されるステップを確認します。
「デバイスの検索」をクリックしてリモートで対象の
端末やサーバーのスキャンを実行します。

6. グラフを確認して攻撃の全体像を把握します。
ビーコンの eicar.txt をクリックしてこのマルウェアの詳細を確認します。

7. 画面右側に eicar.txt の詳細情報が表示されます。新しいマルウェアなどの理由で機械学習分析など詳細な情報が非表示の場合は「最新の解析情報を要求」をクリックすることで Sophos Labs へ解析依頼を行います。
数分後に解析結果が表示できるようになります。

8. 解析が終了したという通知が来ます。

10　補足情報

10.1 検出機能をテストする方法

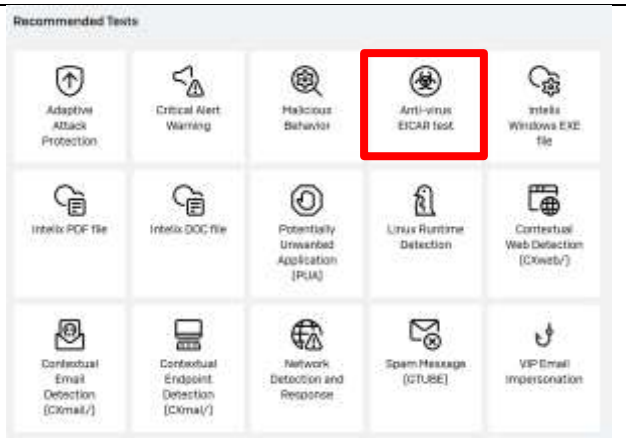
Intercept X Advanced with XDR の検出機能が正常に作動していることをテストするのに使用できるいくつかの方法が有ります。テスト方法の詳細につきましては、以下の URL のご参照をお願いいたします。

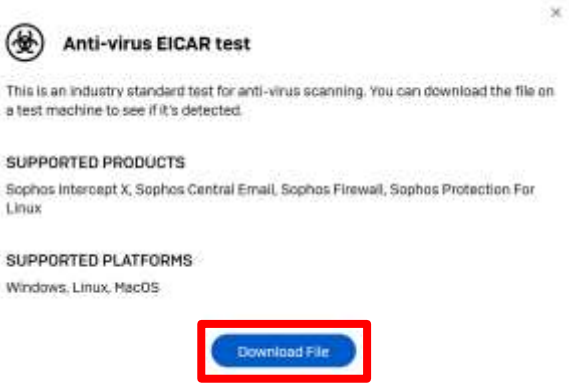
https://support.sophos.com/support/s/article/KBA-000001431

このテスト方法の内、オンアクセススキャン（リアルタイム検索）のテストに利用するテストウィルスの取得方法を以下に説明します。

1. ブラウザにて 「https://sophostest.com/」 のサイトを開きます。

2. 「Recommended Tests」にある「Anti-virus EICAR test」をクリックし、ポップアップされた画面にある「Downloaded File」をクリックし、ファイルをダウンロードします。





3. 右のポップアップメッセージが表示されます。その後、脅威のクリーンアップが完了したことを示すのポップアップメッセージが表示されます。

10.2 エージェントのアンインストール（Windows）

評価終了後のエージェントのアンインストール方法について説明します。以下、Windows のアンインストール手順となります。

1. エージェントをアンインストールする場合は、タンパープロテクションを解除します。 Sophos Central Admin 画面上部の「マイプロダクト」－「Endpoint」-「コンピュータ」をクリックし、アンインストール対象のコンピュータをクリックします。 ※Windows Server の場合は「マイプロダクト」－「Server」－「サーバー」からアンインストール対象のサーバーをクリックします。	
2. 「タンパープロテクションをオフにする」をクリックします。	
3. 次に、Windows にて「Windows の設定」-「アプリと機能」の画面を表示します。 「Sophos Endpoint Agent」を「アンインストール」します。	

10.3 エージェントのアンインストール（Mac）

評価終了後のエージェントのアンインストール方法について説明します。以下 Mac のアンインストール手順です。

1. エージェントをアンインストールする場合は、タンパープロテクションを解除します。 Sophos Central Admin 画面上部の「マイプロダクト」－「Endpoint」-「コンピュータ」をクリックし、アンインストール対象のコンピュータをクリックします。	
2. 「タンパープロテクションをオフにする」をクリックします。	
3. ターミナルを開き、右記コマンドを実行します。 4. 次に右記コマンドを実行します。 パスワード入力を求められた場合はログインパスワードを入力します。	cd /Library/Application¥ Support/Sophos/SaaS/Installer.app /Contents/MacOS/tools/ sudo ./InstallationDeployer --remove

10.4 エージェントのアンインストール（Linux）

評価終了後のエージェントのアンインストール方法について説明します。以下 Linux のアンインストール手順です。

1. ターミナルより以下のコマンドを実行します。 アンインストールには root 権限が必要になります。 1）opt/sophos-spl/bin に移動します 2）./uninstall.sh を実行します	# cd /opt/sophos-spl/bin # ./uninstall.sh Do you want to uninstall Sophos Linux Protection? y #