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

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

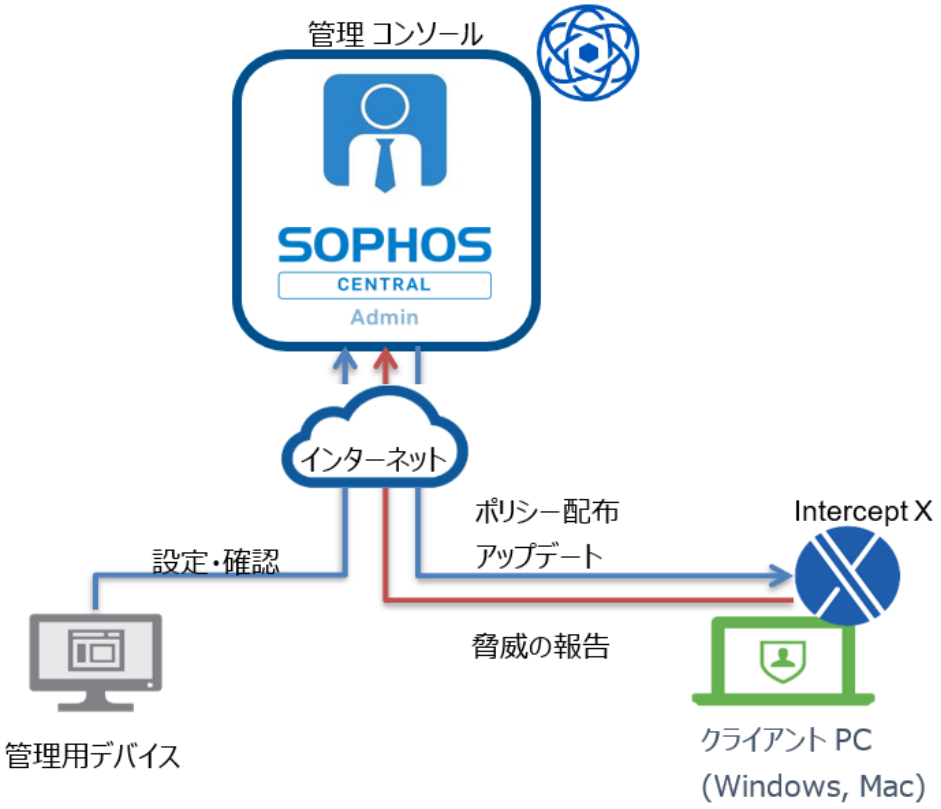
目次

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 と管理サービス 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。



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

❖ 対応プラットフォーム

・ Windows 7*
・ Windows 8.1*
・ Windows 10
・ Windows 11
・ Windows ARM

※Windows7、Windows 8.1 は End of Life のため延長サポートが必要になります。

❖ 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

※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/KB-000035144?language=ja

- Mac

❖ 対応プラットフォーム

・ macOS 11
・ macOS 12
・ macOS 13
・ Intel mac(64 bit)
・ macOS11,12,13(native)
・ Apple Silicon M Series (ARM)

❖ 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/KB-000034670?language=ja

※対応 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/KB-000034756?language=ja#Windows

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)

※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/ManageYourAccount/SupportedBrowsers/index.html

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 80（HTTP）
  - 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/KB-000034570

3 Sophos Central の無償評価登録

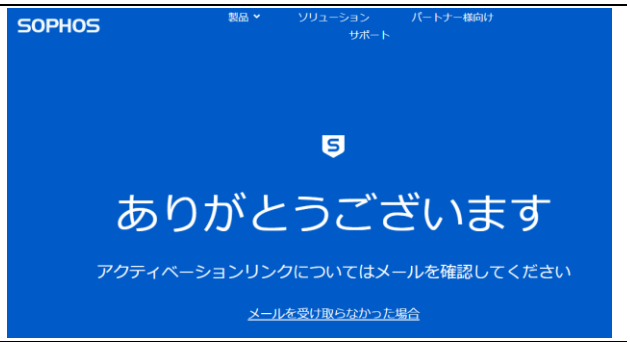
本章では、Sophos Central および Intercept X の評価に必要となる無償評価ライセンスの登録手順を説明します。
ソフォスのホームページよりユーザー情報をご登録いただき、Sophos Central Admin へのログイン ID を作成する手順となります。今まで Sophos Central へ登録したことのない、受信を確認できるメールアドレスアドレスを一つご用意ください。

1. ブラウザにて https://www.sophos.com/ja-jp/products/server-security/free-trial にアクセスします。＊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

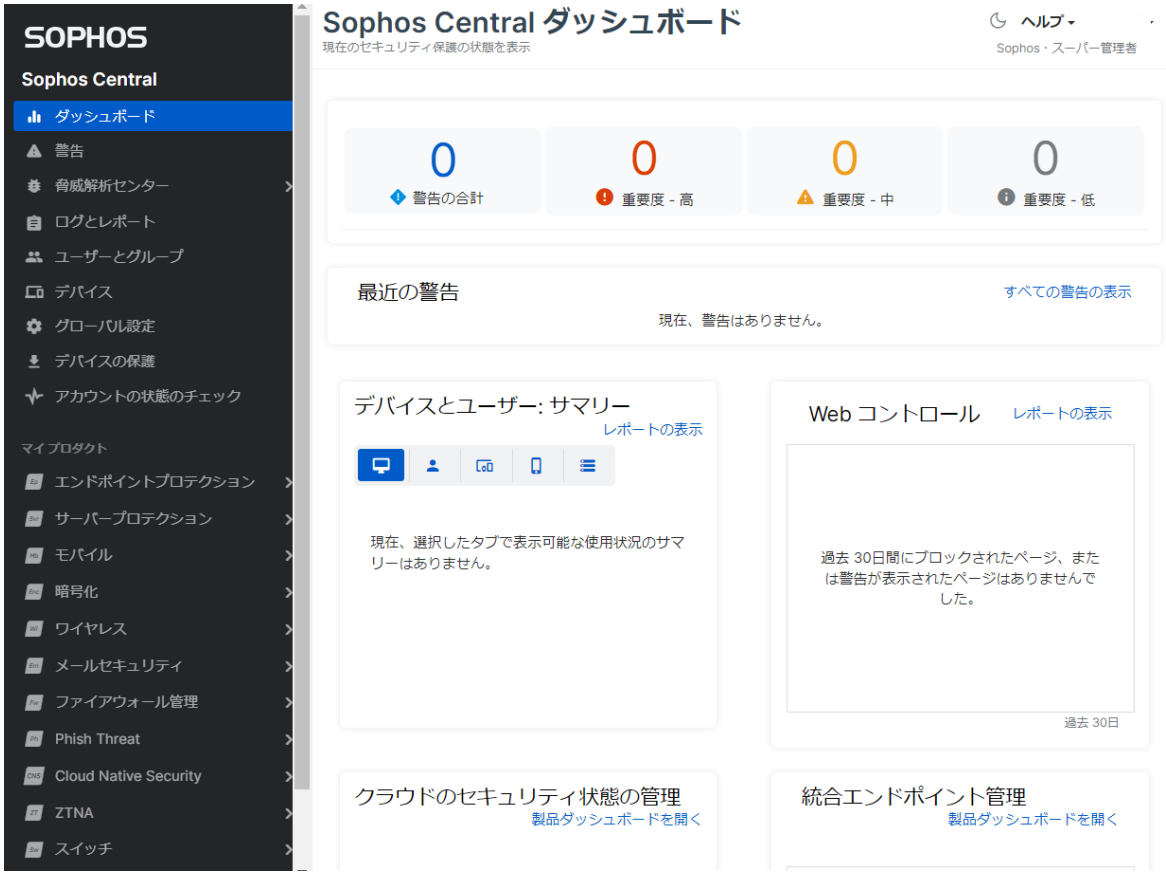
   「パスワードの作成」ボタンを押します。

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。

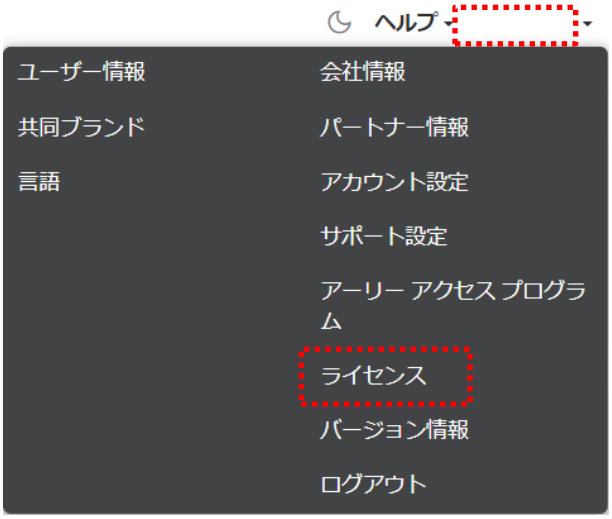
   パスワードを入力、Central Admin ポータルのリージョン選択し、規約へ同意いただける場合、規約への同意を示すチェックボックスにチェックを付け、「アカウントのアクティベーション」をクリックします。

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します。

7. Sophos Central Admin のダッシュボードが表示されます。



8. ダッシュボード画面右上の「ログインユーザー名」→「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。



9. 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。

ライセンス	種類	使用数	制限	開始日	失効日
Phish Threat	評価版	0	100	2022年12月16日	2024年7月12日
Wireless Standard for APX	評価版	0	10	2022年12月16日	2024年7月12日
Device Encryption	評価版	0	100	2022年12月16日	2024年7月12日
Intercept X Advanced with XDR	評価版	0	100	2022年12月16日	2024年7月12日
Mobile Advanced	評価版	0	100	2022年12月16日	2024年7月12日
Cloud Optix Advanced	評価版	0	100	2022年12月16日	2024年7月12日
Sophos Intercept X for Mobile	評価版	0	100	2022年12月16日	2024年7月12日
Intercept X Advanced for Server with XDR	評価版	0	100	2022年12月16日	2024年7月12日
Wireless Standard for AP15	評価版	0	10	2022年12月16日	2024年7月12日
Wireless Standard for AP55/AP100	評価版	0	10	2022年12月16日	2024年7月12日
Email Advanced	評価版	0	100	2022年12月16日	2024年7月12日
Zero Trust Network Access	評価版	0	100	2022年12月16日	2024年7月12日

10. 画面右上の「ログインユーザー名」→「ログアウト」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。

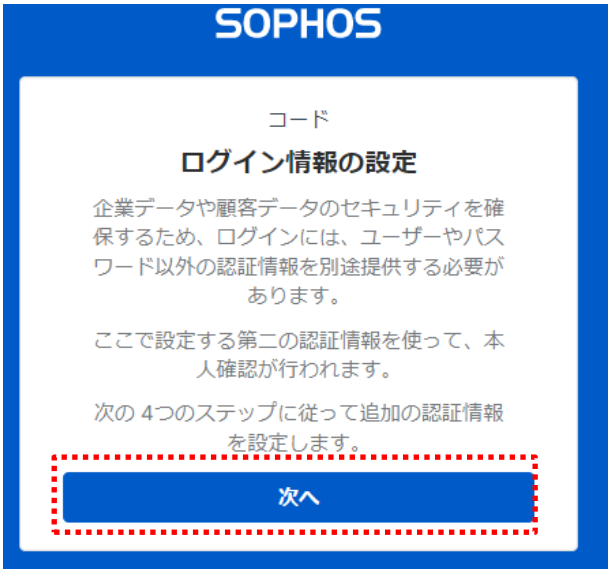
1. ブラウザより https://central.sophos.com のアドレスへアクセスします。
   ログイン画面が表示されますので、
   3 章 2 項で指定したメールアドレスを入力し「Continue」をクリックします。
   3 章 5 項で指定したパスワードを入力し「サインイン」をクリックします。

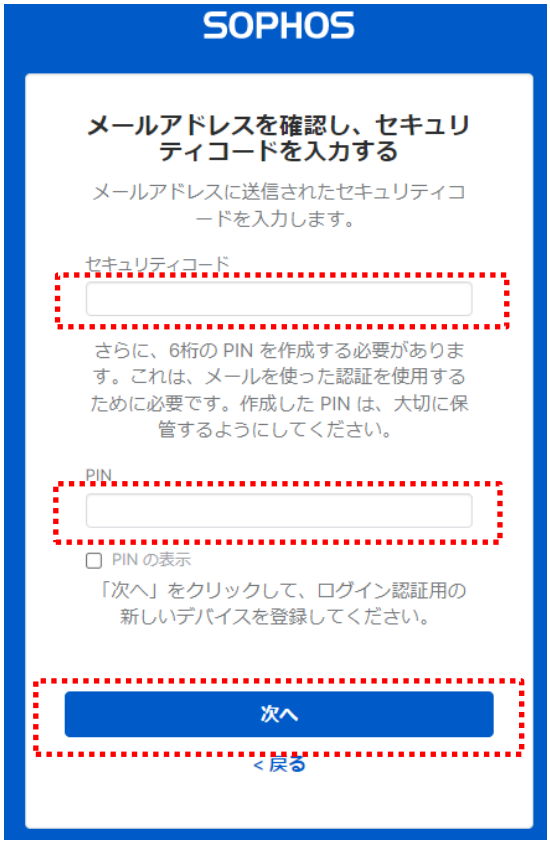
2. 多要素認証を設定するためのログイン情報の設定画面が表示されます。
   「次へ」をクリックします。

   メールアドレスにセキュリティコードが送信されますので、メールを確認してセキュリティコードを入力します。
   6 桁の PIN を入力します。

   「次へ」をクリックします。

   ※紛失、忘れた場合はカスタマケアへお問合せしてリセットしてください





3. 認証方法を選択します。

ここでは、SMS メッセージを選択し
「次へ」をクリックします。

※Sophos/Google Authenticator を利用する場合は以下を参照してください。
https://doc.sophos.com/central/customer/help/ja-jp/ManageYourProducts/GlobalSettings/MultiFactorAuthentication/index.html

4. SMS メッセージを設定します。

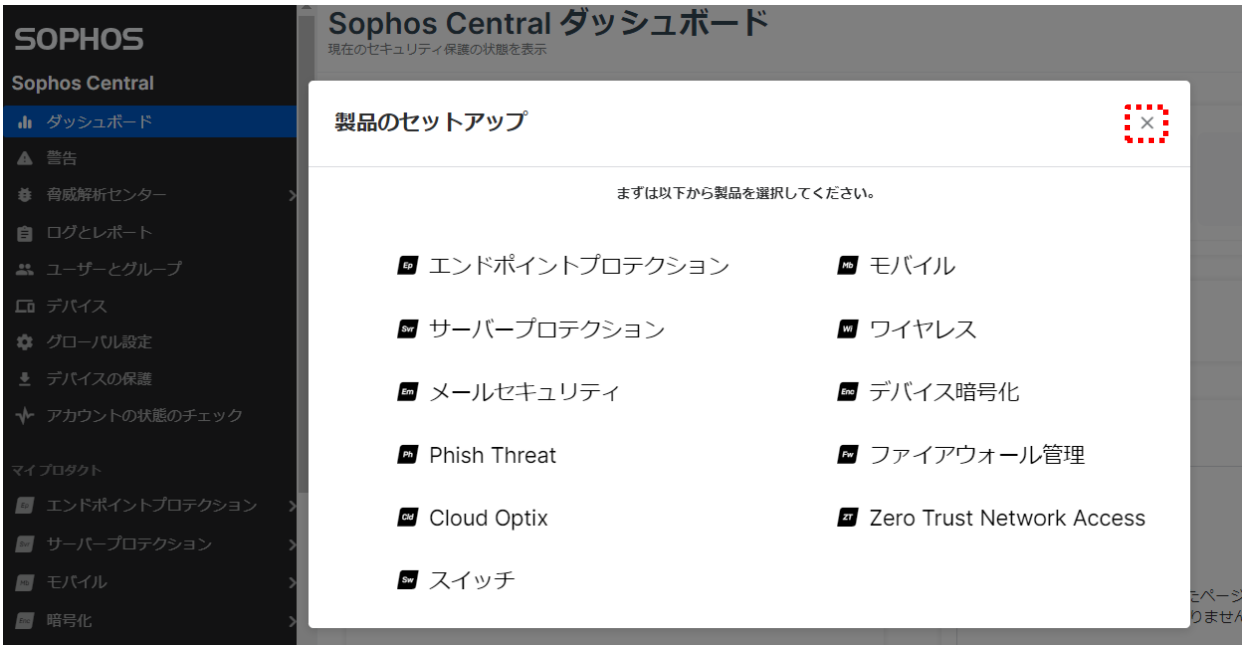
   国名に「Japan」を選択し、携帯電話の電話番号を入力し「次へ」をクリックします。
   ※最初の「 0 」は省略します。
   “ 080-“は、” 80-“のように入力します。

5. 携帯電話に SMS でセキュリティコードが送信されます。

   セキュリティコードを入力し「次へ」ボタンをクリックします。

6. 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 のサポートデーターベースをご参照ください。
https://support.sophos.com/support/s/article/KB-000034831?language=ja

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 の左ペインから「エンドポイントプロテクション」をクリックします。

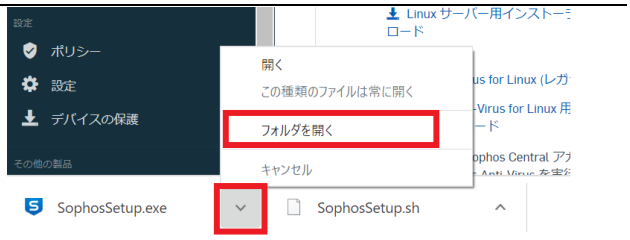
2. エンドポイントプロテクションのダッシュボード画面が表示されますので、左ペインから「デバイスの保護」をクリックします。

3. 右ペインにエンドポイントプロテクションのデバイス保護の画面が表示されます。
Windows 用全機能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。

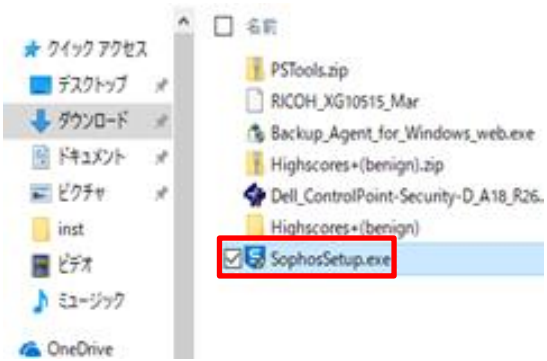
4. デバイスの暗号化のチェックを外した上、「インストーラのダウンロード」をクリックします。

5. Mac の場合も「3」「4」と同様の操作をしてください。

6. 画面の下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）
ファイル名のプルダウンをクリックし、「フォルダを開く」をクリックします。



7. 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。

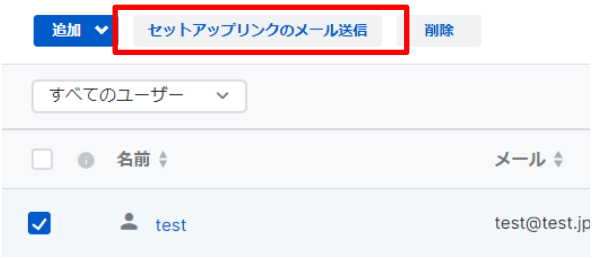


5.2 セットアップリンクを送信する手順

1. 4 章の手順で Sophos Central Admin にログインします。
「エンドポイントプロテクション」-「ユーザーにインストーラ送信」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。

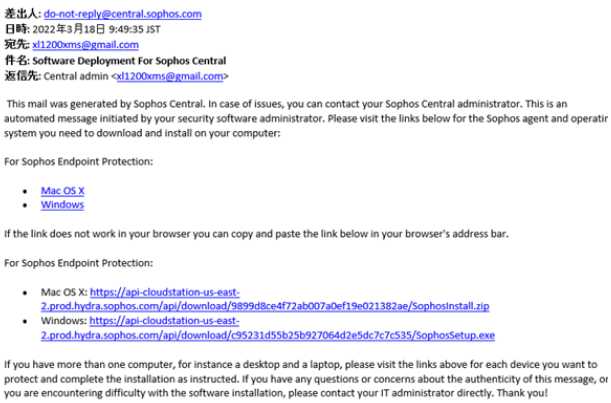
2. ユーザーとグループの画面が表示されます。次に送りたいユーザーのチェックボックスに☑をいれます。

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。



差出人: do-not-reply@central.sophos.com
日時: 2022年3月18日 9:49:35 JST
宛先: xl1200xms@gmail.com
件名: Software Deployment For Sophos Central
返信先: Central admin <xl1200xms@gmail.com>

This mail was generated by Sophos Central. In case of issues, you can contact your Sophos Central administrator. This is an automated message initiated by your security software administrator. Please visit the links below for the Sophos agent and operatir system you need to download and install on your computer:

For Sophos Endpoint Protection:

- Mac OS X
- Windows

If the link does not work in your browser you can copy and paste the link below in your browser's address bar.

For Sophos Endpoint Protection:

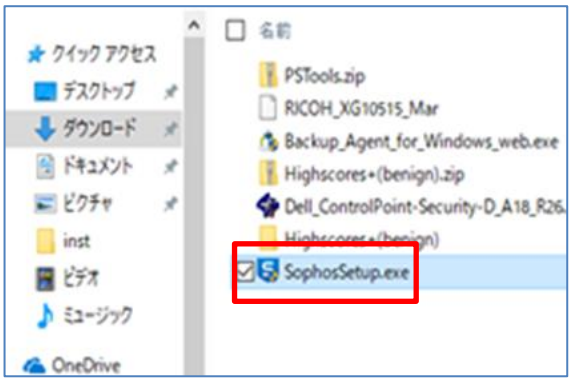
- Mac OS X: https://api-cloudstation-us-east-2.prod.hydra.sophos.com/api/download/9899d8ce4f72ab007a0ef19e021382ae/SophosInstall.zip
- Windows: https://api-cloudstation-us-east-2.prod.hydra.sophos.com/api/download/c95231d55b25b927064d2e5dc7c7c535/SophosSetup.exe

If you have more than one computer, for instance a desktop and a laptop, please visit the links above for each device you want to protect and complete the installation as instructed. If you have any questions or concerns about the authenticity of this message, or you are encountering difficulty with the software installation, please contact your IT administrator directly. Thank you!

5.3 Windows へのインストール

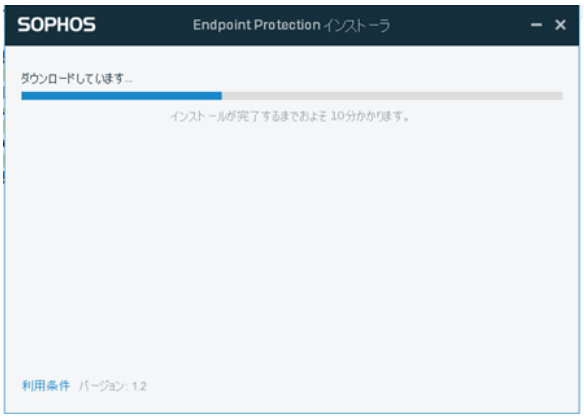
本手順書では、Windows へインストールする手順を説明します。
この操作は Administrator 権限のあるユーザーで行う必要があります。

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。



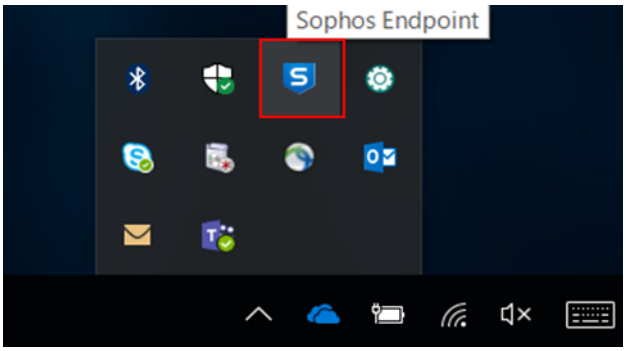
2. インストールウィザードが表示され、インストールされる製品が表示されます。利用する製品に間違いがないことを確認して、「インストール」をクリックします。

3. 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。



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、「完了」をクリックして PC を再起動します。

5. PC 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。



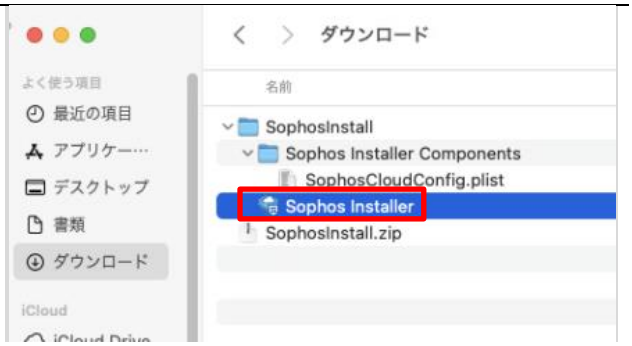
6. コンピューターのステータス画面が表示されます。
この画面でコンピューターが保護されていることを確認します。

7. 以上で Windows へのインストールは終了です。

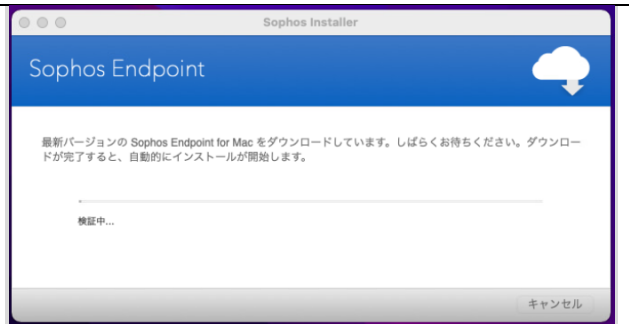
5.4 Mac へのインストール

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。

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。



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。

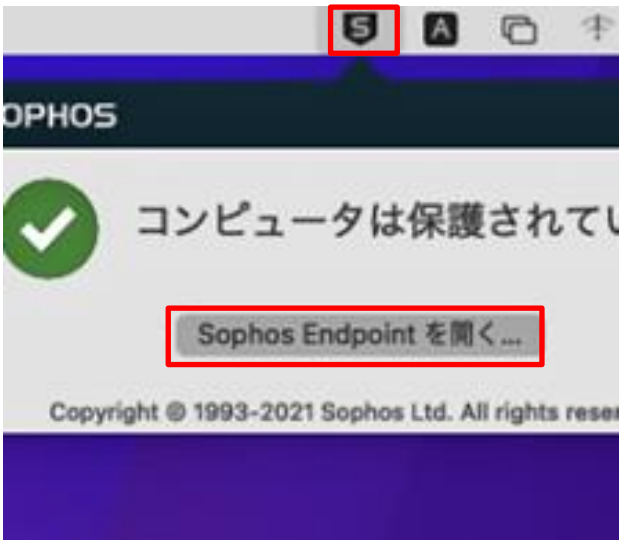


3. 途中で「Sophos scan Extension」や「Network Extension」が許可を求めてきた場合は、「許可」します。

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、PC を再起動します。
PC 再起動後、画面右上のタスクバーから Sophos のアイコンをクリックすると、「コンピューターは保護されてます。」のポップアップが表示されます。

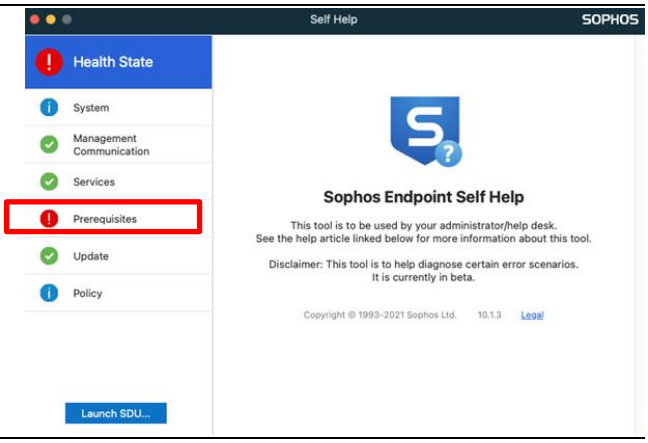
5. 「Sophos Endpoint」を開き、緑色のステータが表示されていれば、インストールは正常に完了となります。

6. 画面右上にあるソフォスアイコンをクリックし、「Sophos Endpoint を開く…」をクリックします。

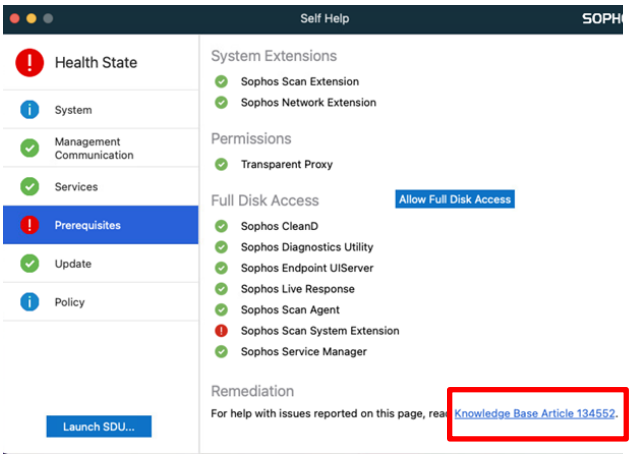


7. 「診断ツールの起動」をクリックします。

8. ヘルスステータスにて、赤い表示がある場合はこれを解決します。
https://support.sophos.com/support/s/article/KB-000039014?language=ja

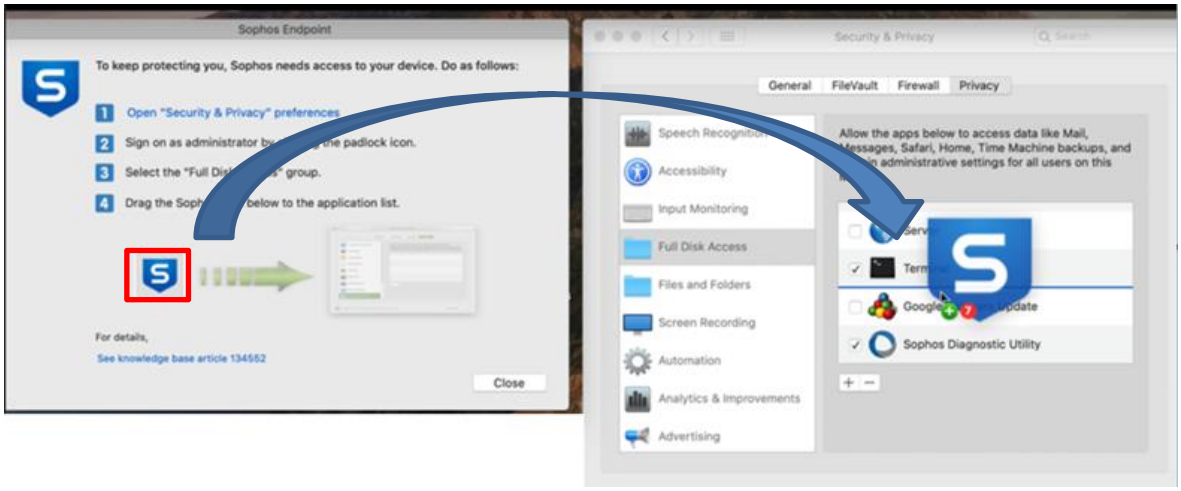


9. ヘルスステータスで赤くなっているタブ内の右下にある KB を参考に対応します。

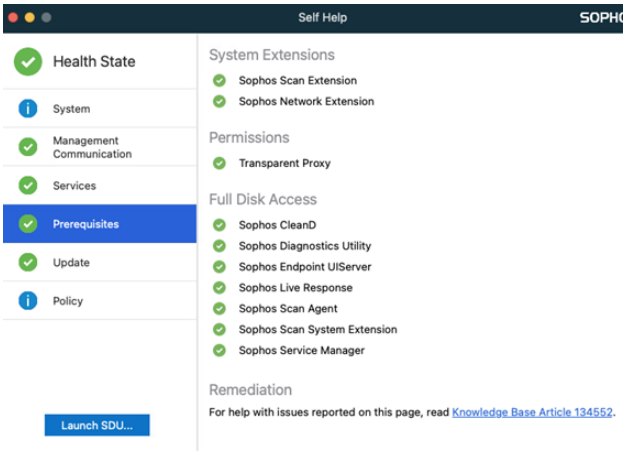


10. KB にてポップアップが表示されたら S のマークを「システム環境設定」-「セキュリティとプライバシー」-「フルディスクアクセス」にドラッグ＆ドロップします。

11.



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。



6. 以上で Mac へのインストールは終了です。

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。「エンドポイントプロテクション」-「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し制御し、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

アップデートポリシーでは、製品アップデートを利用可能な状態にするタイミングを指定できます。設定すると、コンピューター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。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 (コンピューターやサーバーなど) またはデバイスのグループに適用できます。

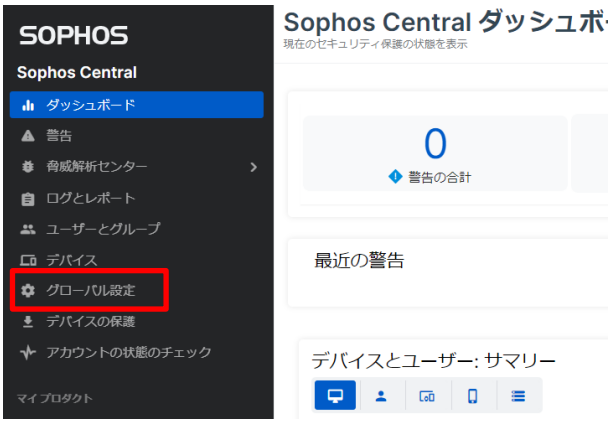
7 タンパープロテクション

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

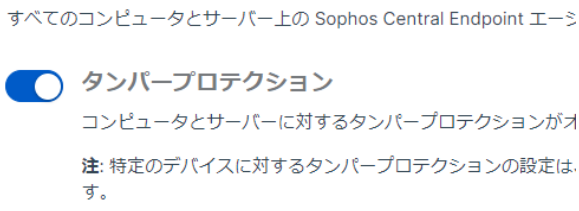
グローバル設定でのタンパープロテクション設定は、Sophos Central 全体の設定となり、全台へのタンパープロテクションの有効、無効を設定します。デフォルトで有効に設定されています。

1. 4 章の手順で Sophos Central Admin にログインします。
   Sophos Central Admin 画面の左ペインの「グローバル設定」をクリックします。



2. 右ペインにグローバル設定の画面が表示されます。
   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。



7.2 タンパープロテクション：コンピューター設定

コンピューター設定でのタンパープロテクション設定は、コンピューター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、コンピューター側の 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 画面の左ペインの「エンドポイントプロテクション」をクリックします。

2. エンドポイントプロテクション画面の左ペインの「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ーが表示されます。
対象の Windows の「コンピューター名」をクリックしサーバーの詳細画面を表示します。

4. コンピューター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。

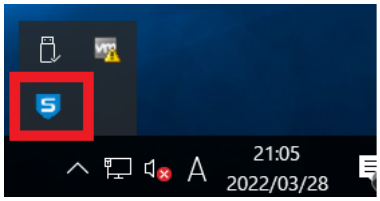
5. サマリータブ画面のサマリー部分にタンパープロテクションの項目が表示され、この「タンパープロテクションを無効化する」をクリックすることで、無効に設定することが可能です。

6. 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、コンピューター側の GUI(Graphical User Interface)で一時的に設定変更が可能となります。

コンピューター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ー側での操作となり、コンピューター側の 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. コンピューター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。

この画面より、各機能の無効設定が一時的に可能となります。

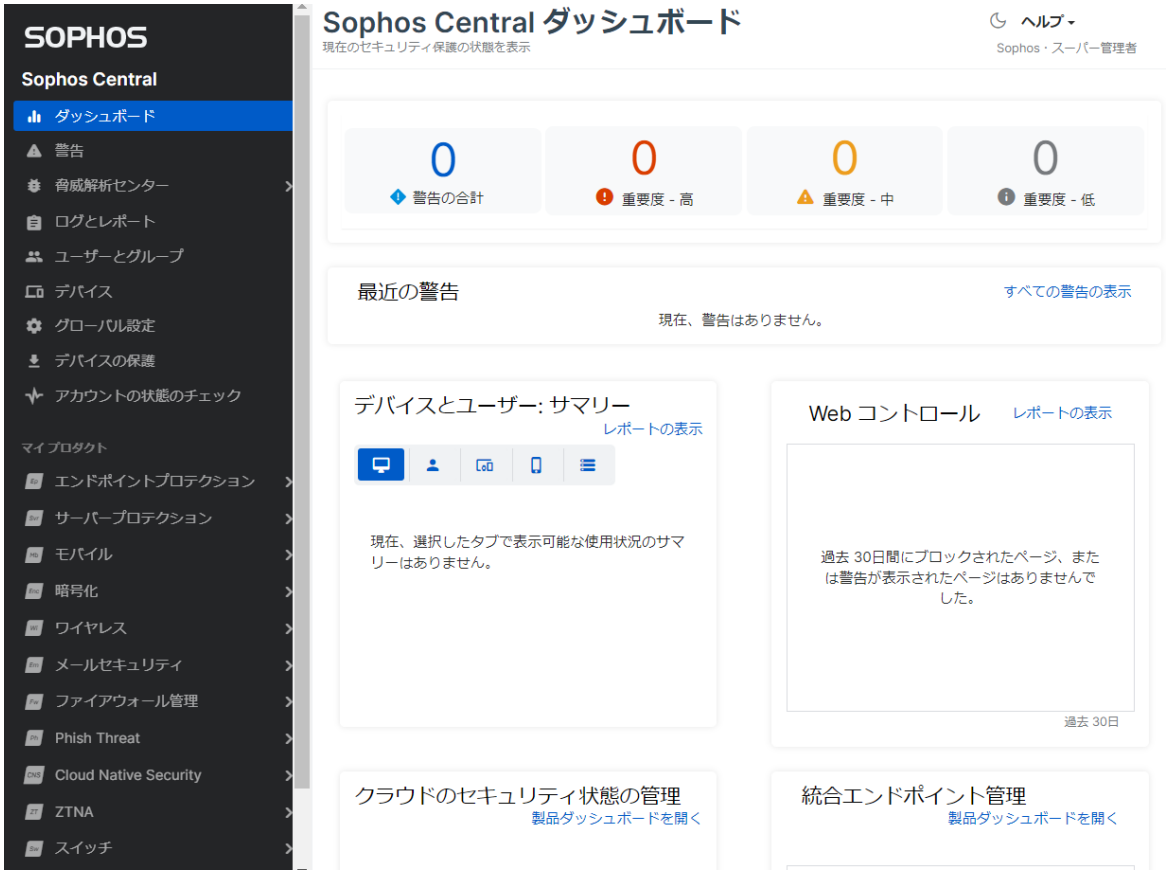
8 Sophos Central の管理

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

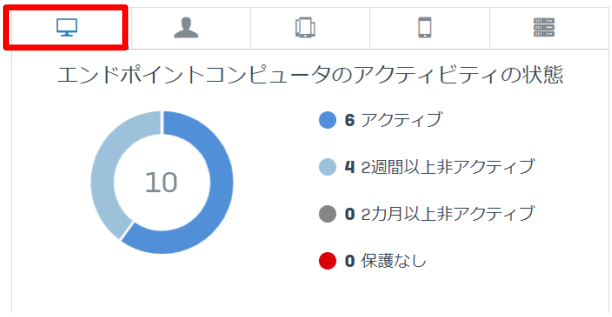
Sophos Central のダッシュボードでは、最新の警告、使用状況のサマリー、Web 利用状況等の情報が表示されます。

1. 4 章の手順で Sophos Central Admin にログインします。
   Sophos Central Admin 画面の左ペインのダッシュボードが選択された状態で右ペインにダッシュボードが表示されます。



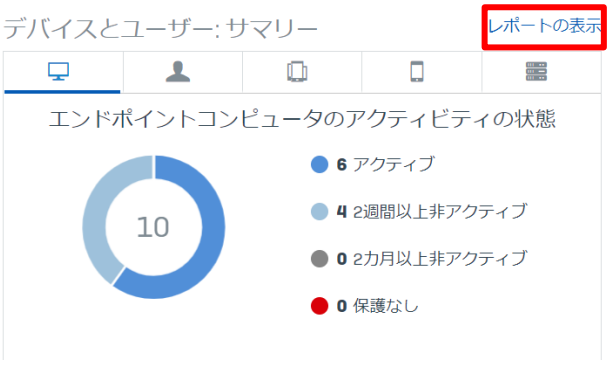
2. 「最新の警告」の表示では、警告発生時にマルウェア名、該当ファイル名情報、検知したコンピューター名の情報が表示されます。
   - 「マルウェア名、該当ファイル名」部分をクリックするとマルウェア詳細情報が記載されている弊社の Web サイトを表示します。（英語表記のみの場合も有ります）
   - 「コンピューター名」部分をクリックするとサマリー、イベント、ステータス情報などサーバーの詳細情報が表示されます。

3. 次に、「使用状況のサマリー」部分で、コンピューターイコンのタグをクリックします。

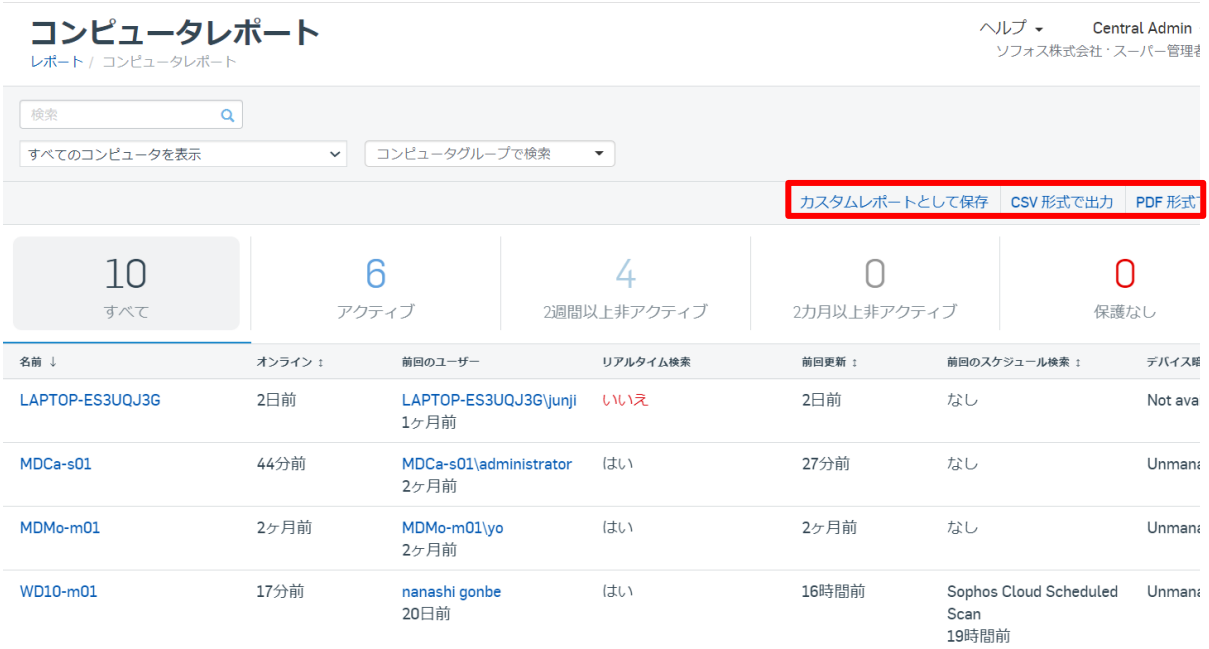


4. コンピューターのアクティビティステータスの画面が表示されます。
   この画面では、現在稼働中のコンピューター（アクティブ）、2 週間以上、2 ヶ月以上、Sophos Central Admin と接続がないコンピューターがグラフで表示されます。

   「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、コンピューター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下部に表示されます。
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. 次に「Web 利用状況」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

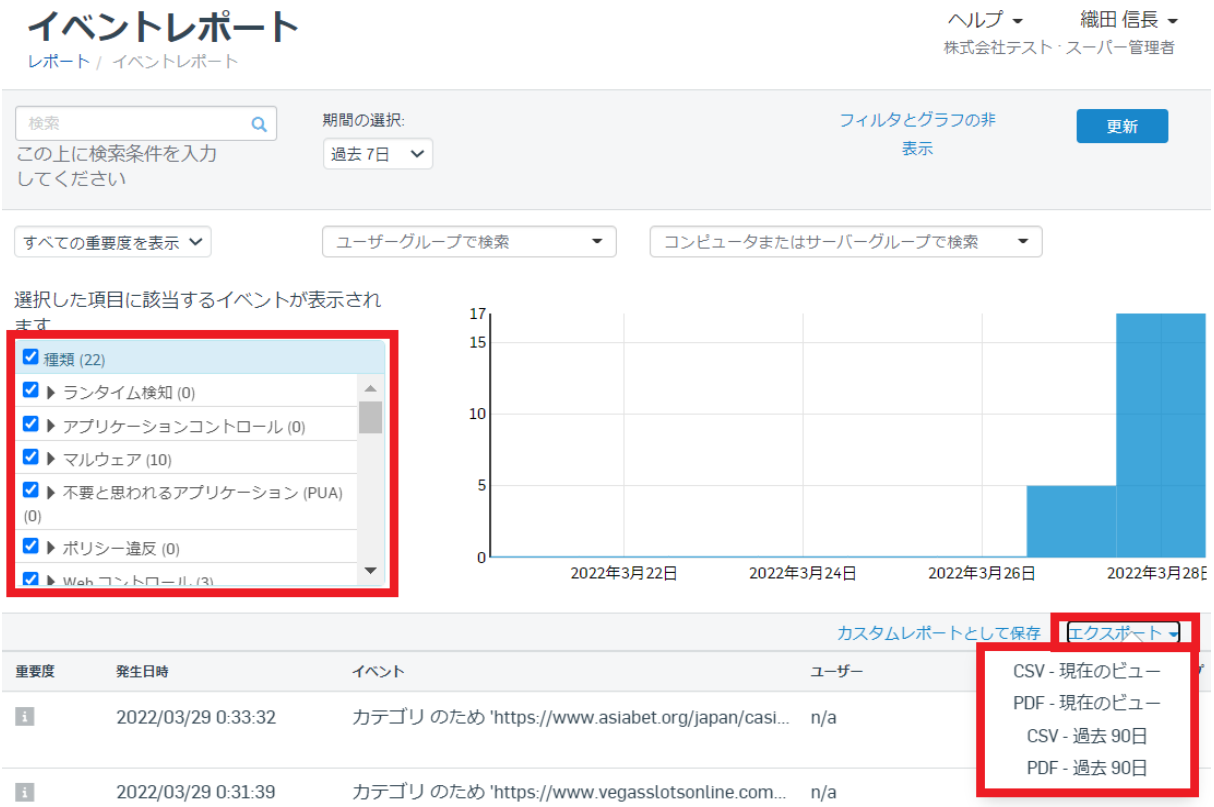
Sophos Central のログとレポートでは、すべてのイベント、監査ログ、コンピューターやサーバー一覧、データ流出防止、アプリケーション コントロール、Web コントロールなどのブロックイベントのレポートが可能となっています。

1. Sophos Central Admin 画面の左ペインより「ログとレポート」をクリックします。右ペインに出力可能なログ、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

[高] Sophos Central で発生した警告 [株式会社テスト]: 手動による脅威のクリーンアップが必要です 受信トレイ ×

do-not-reply@central.sophos.com 3月28日(月) 23:48 (1 時間前)
To 自分

このメール警告は Sophos Central より自動配信されています。このメールには返信しないでください。

SOPHOS CENTRAL

Sophos Central のイベントの詳細: 株式会社テスト

現象: 脅威をクリーンアップできませんでした。

発生場所: ubuntsuTokyo

パス: /home/suzuki/デスクトップ/eicar.sh

検出された項目: EICAR-AV-Test

デバイスに関連付けられているユーザー: n/a

深刻度: 高

ソフォス製品で実行された処理: クリーンアップを試みました (脅威が Linux コンピュータにある場合を除く)。

必要な対応: Sophos Central Admin のコンソールの「**警告**」ページを参照し、該当する脅威の警告を探します。脅威名をクリックし、ソフォスの Web サイトから詳細とクリーンアップのアドバイスを確認します。確認後、感染したコンピュータに移動し、手動で脅威をクリーンアップします。

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

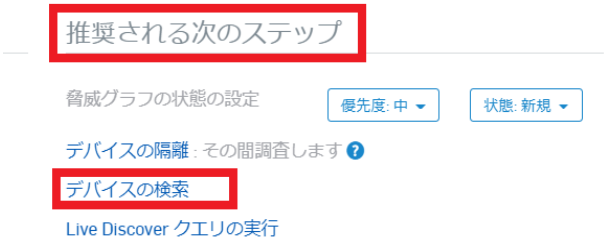
1. Sophos Central Admin 画面の左ペインの「脅威解析センター」をクリックします。

2. Sophos Central Admin 画面の左ペインの「脅威グラフ」をクリックします。

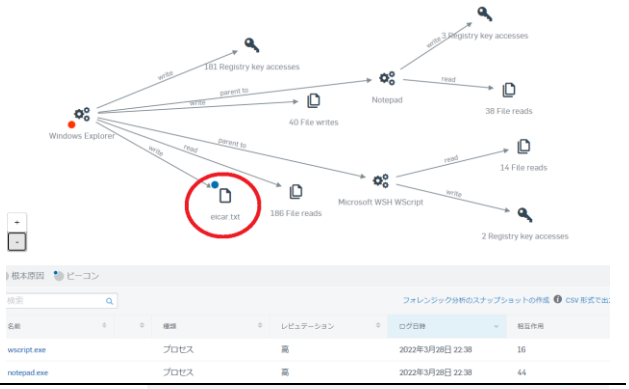
3. 検出された攻撃をクリックします。

4. 攻撃が発生したコンピューターや根本原因、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「細心の解析情報を要求」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

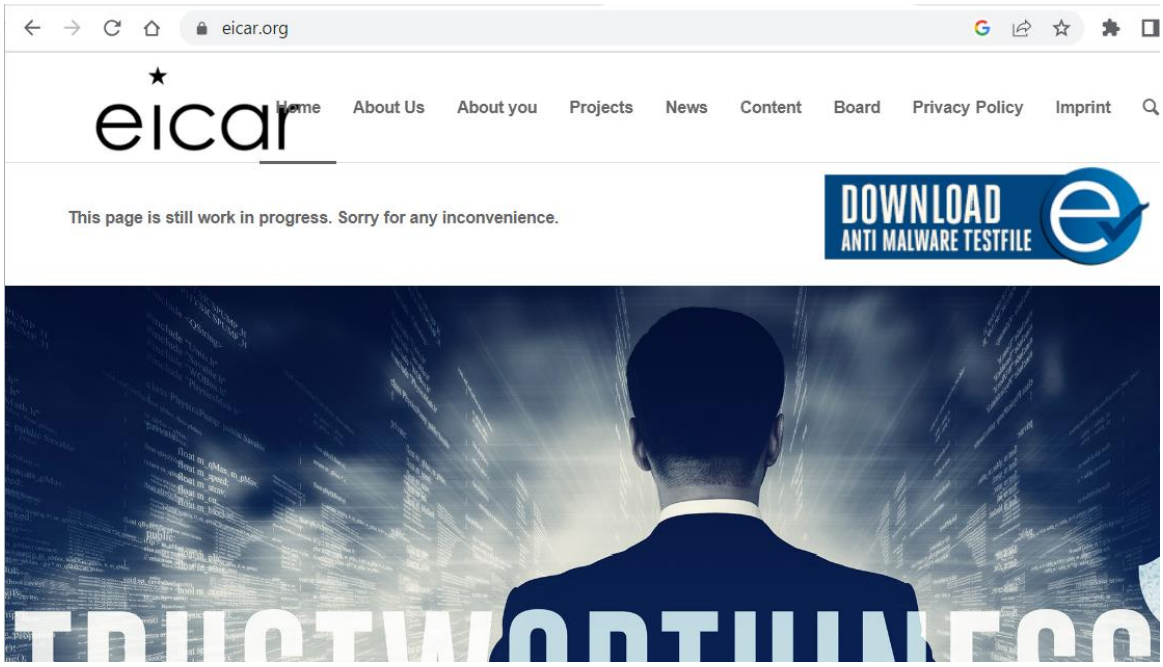
10.1 検出機能をテストする方法

Intercept X Advanced for Server 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/KB-000033289

このテスト方法の内、オンデマンドおよびオンアクセススキャン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。

9. ブラウザにて「https://www.eicar.org/」のサイトを開きます。



10. 画面右上にある「DOWNLOAD ANTI MALWARE TESTFILE」部分をクリックします。

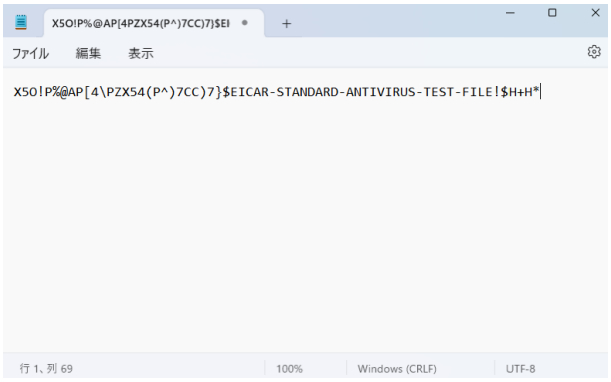
11. 表示された画面の下部に “X5O!” から始まる文字列が表示されています。この文字列をドラックしコピーします。

should detect it in any file providing that the file starts with the following 68 characters, and is exactly 68 bytes long:

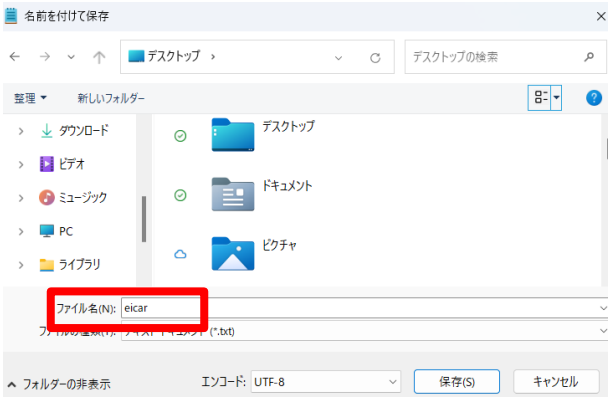
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

The first 68 characters is the known string. It may be optionally appended by any combination o whitespace characters with the total file length not exceeding 128 characters. The only whitespa characters allowed are the space character, tab, LF, CR, CTRL-Z. To keep things simple the file

12. メモ帳を起動し、コピーした文字列を貼り付け、保存します。



13. 保存では、ファイルの種類をすべてのファイル(*.*)に変更し、ファイル名を「eicar.com や eicar.txt」で保存します。



14. Intercept X Advanced With XDR を導入したコンピューターに保存すると、右のポップアップメッセージが表示されます。

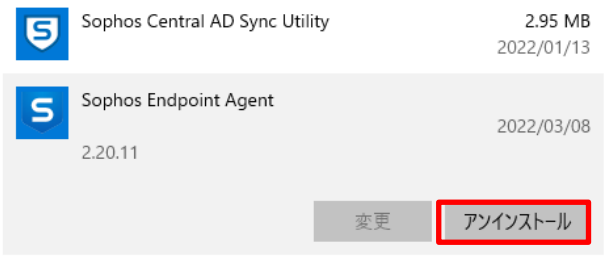
10.2 エージェントのアンインストール（Windows）

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。
「エンドポイントプロテクション」-「コンピューター」をクリックし、アンインストール対象のコンピューターをクリックします。

2. 「タンパープロテクションを無効化する」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、Linux Server 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。 「エンドポイントプロテクション」-「コンピューター」をクリックし、アンインストール対象のコンピューターをクリックします。	
2. 「タンパープロテクションを無効化する」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。	cd /Library/Application¥ Support/Sophos/SaaS/Installer.app /Contents/MacOS/tools/
4. 次に右記コマンドを実行します。	sudo ./InstallationDeployer --remove --tamper_password <タンパーパスワードコード> を実行します。