

Intercept X Advanced for Server 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いたします。

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	2018/03/08	Central Server Protection 初版
2.0	Sophos	2022/04/01	Intercept X Advanced for Server 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	2023/06/30	画像差替えおよび一部文言を修正

目次

はじめに	5
1 システム要件	7
2.1. Intercept X Advanced for Server with XDR	7
2.2. Sophos Central Admin へ接続するツール	9
2.3. 通信要件	9
2 Sophos Central の無償評価登録	10
3 Sophos Central Admin へのログイン	14
4 エージェントのインストール	18
4.1 Sophos Central Admin からダウンロード	18
4.2 ダウンロードリンクでのダウンロード	20
4.3 Windows Server へのインストール	22
4.4 Linux Server へのインストール	26
5 サーバグループの登録	29
6 ポリシー	33
6.1 脅威対策ポリシー	34
6.2 周辺機器コントロールポリシー	34
6.3 アプリケーションコントロールポリシー	34
6.4 Web コントロールポリシー	34
6.5 データ流出防止ポリシー	34
6.6 アップデートの管理ポリシー	35
6.7 Windows ファイアウォールポリシー	35
6.8 ファイル整合性の監視ポリシー	35
7 サーバロックダウン	36
7.1 サーバロックダウンの事前準備	36
7.2 ロックダウンポリシー	38
7.3 サーバロックダウンのインストール	42
8 タンパープロテクション	45
8.1 タンパープロテクション：グローバル設定	45
8.2 タンパープロテクション：サーバ設定	46
9 Sophos Central の管理	49
9.1 ダッシュボード	49
9.2 ログとレポート	52
9.3 メール通知	53
10 インシデントによる Intercept X Advanced with XDR の利用	55

10.1	脅威解析センター	55
11	補足情報	57
11.1	検出機能をテストする方法	57
11.2	エージェントのアンインストール (Windows Server)	59
11.3	エージェントのアンインストール (Sophos Linux Protection)	63

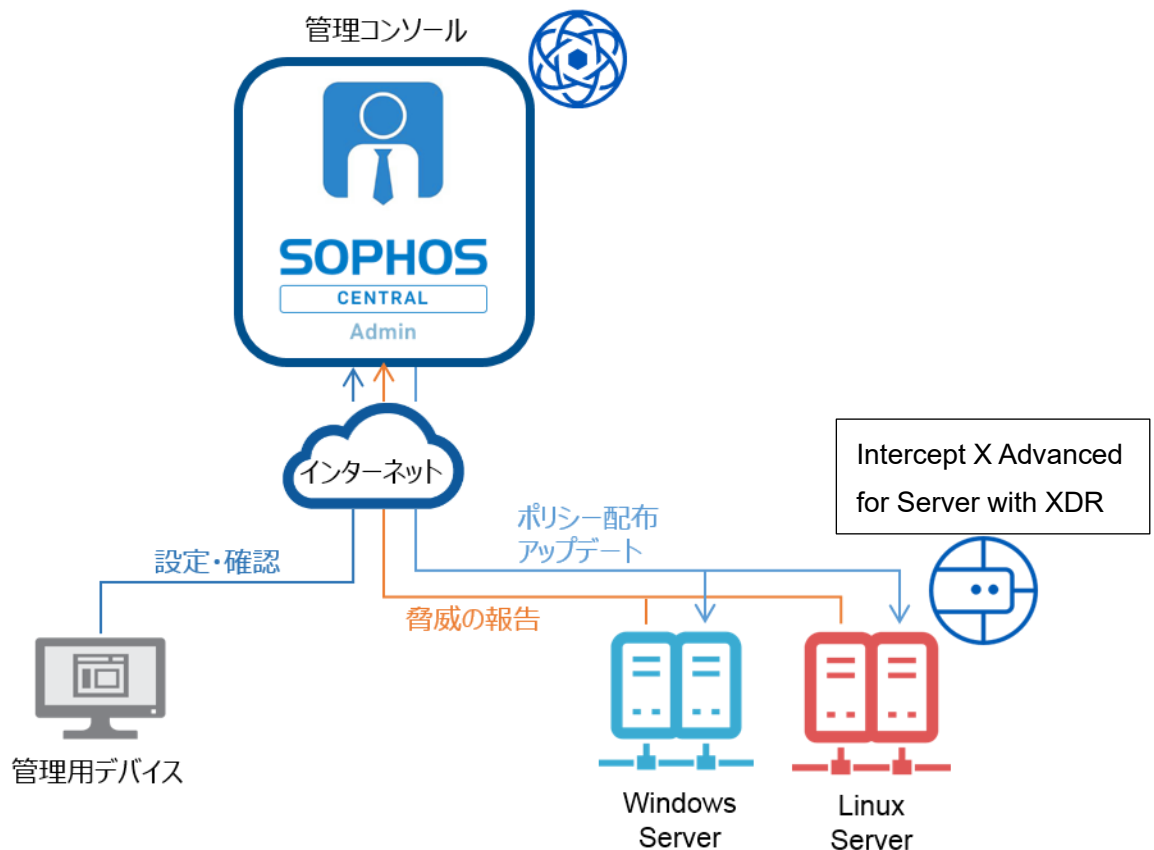
はじめに

このたびは Intercept X Advanced for Server 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 for Server 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 for Server 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サーバ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。

1 システム要件

本章では、Intercept X Advanced for Server 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 for Server with XDR

● Windows Server

❖ 対応プラットフォーム

- ・ Windows Server 2016
- ・ Windows Server 2019
- ・ Windows Server 2022
- ・ ※Windows Server 2008 R2、Windows Server SBS 2011、Windows Server 2012、2012 R2 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 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/KB-000034920?language=ja>

※対応エディションの詳細につきましては、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/KB-000034074?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>

● Linux Server

❖ 対応プラットフォーム

- ・ Amazon Linux 2
- ・ Amazon Linux 2022
- ・ CentOS 7
- ・ CentOS Minimal
- ・ CentOS Stream
- ・ Debian 10
- ・ Debian 11

- Miracle Linux 8
- Oracle 7
- Oracle8
- RHEL 7
- RHEL 8
- RHEL 9
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 15
- Ubuntu 18.04 (LTS)
- Ubuntu 20.04 (LTS)
- Ubuntu 22.04 (LTS)
- Ubuntu Minimal

※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。

❖ システム要件

- 必要メモリ 2GB 以上
- 空きディスク容量 2.5GB 以上
- システムの種類 x64
- systemd がサポートされ、実行されている
- glibc 2.17 以降をサポートするカーネル
- Bash がインストール済み
- pidof および setcap システムコマンドが存在する必要があります※1

※1 [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。

※最新の対応プラットフォーム、システム要件は以下のリンクを参照してください。

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

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?language=ja>

2 Sophos Central の無償評価登録

本章では、Sophos Central および Intercept X の評価に必要な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/server-security/free-trial> にアクセスします。

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。

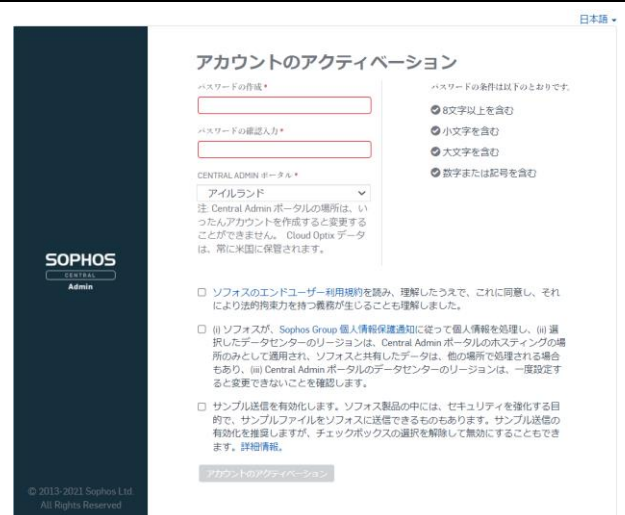
3. 登録が完了すると、右の画面が表示され、数分後に入力したメールアドレスにメールが届きます。



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。
 ※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。特に、モバイル製品やワイヤレス、ZTNA およびスイッチは日本データセンターが未対応ですので、これらの製品を管理する場合はアメリカ、ドイツ、アイルランドから選択ください



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。

The screenshot displays the Sophos Central Admin dashboard. The top navigation bar includes the Sophos logo, the title 'Sophos Central ダッシュボード', and the user name 'Sophos・スーパー管理者'. The main content area is divided into several sections:

- Alerts Summary:** A row of four cards showing the total number of alerts (0) and their severity levels: High (0), Medium (0), and Low (0).
- Recent Alerts:** A section indicating that there are currently no alerts.
- Device and User Summary:** A section with tabs for 'Devices' and 'Users', indicating that no data is currently displayed.
- Web Control:** A section showing that no pages were blocked or alerted over the last 30 days.
- Cloud Security Management:** A section with a link to open the product dashboard.
- Unified Endpoint Management:** A section with a link to open the product dashboard.

The left sidebar contains the following navigation items:

- SOPHOS
- Sophos Central
- ダッシュボード
- 警告
- 脅威解析センター
- ログとレポート
- ユーザーとグループ
- デバイス
- グローバル設定
- デバイスの保護
- アカウントの状態のチェック
- マイプロダクト
- エンドポイントプロテクション
- サーバープロテクション
- モバイル
- 暗号化
- ワイヤレス
- メールセキュリティ
- ファイアウォール管理
- Phish Threat
- Cloud Native Security
- ZTNA
- スイッチ

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。

The screenshot shows the user profile dropdown menu in the Sophos Central Admin dashboard. The menu is open, displaying the following options:

- ヘルプ
- ユーザー情報
- 共同ブランド
- 言語
- 会社情報
- パートナー情報
- アカウント設定
- サポート設定
- アーリー アクセス プログラム
- ライセンス
- バージョン情報
- ログアウト

The 'ヘルプ' menu item is highlighted with a red dashed box, and the 'ライセンス' menu item is also highlighted with a red dashed box.

9. ライセンス画面にて「Intercept X Advanced for Server 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。

ヘルプ

- ユーザー情報
- 会社情報
- 共同ブランド
- パートナー情報
- 言語
- アカウント設定
- サポート設定
- アーリー アクセス プログラム
- ライセンス
- バージョン情報
- ログアウト

3 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「サインイン」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。



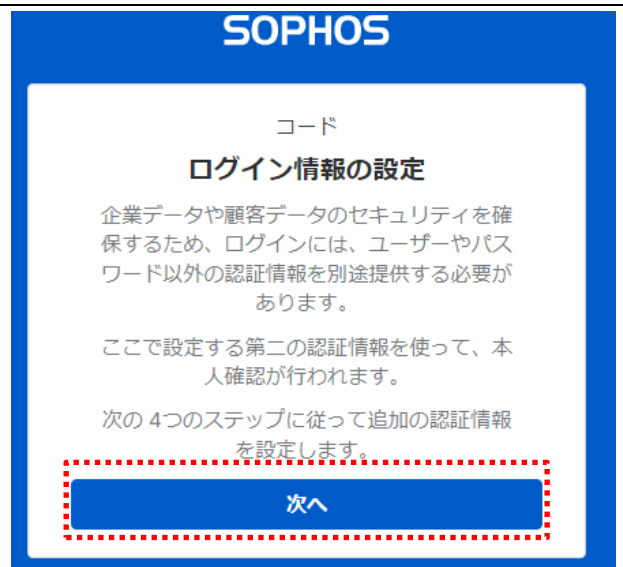
2. 多要素認証を設定するためのログイン情報の設定画面が表示されます。
「次へ」をクリックします。

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



SOPHOS

メールアドレスを確認し、セキュリティコードを入力する

メールアドレスに送信されたセキュリティコードを入力します。

セキュリティコード

さらに、6桁の PIN を作成する必要があります。これは、メールを使った認証を使用するために必要です。作成した PIN は、大切に保管するようにしてください。

PIN

PIN の表示

「次へ」をクリックして、ログイン認証用の新しいデバイスを登録してください。

次へ

< 戻る

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。

※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/customers/help/ja-jp/ManageYourProducts/GlobalSettings/MultiFactorAuthentication/index.html>

SOPHOS

MFA を設定する

サインインするには、第二認証要素を使用して認証する必要があります。使用する方法を選択してください。

モバイルアプリ (推奨)
Google Authenticator や Sophos Authenticator などの認証アプリを使用してセキュリティコードを生成します。

SMS メッセージ
SMS メッセージでセキュリティコードを入手します。

次へ

手順 17/2

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。

SOPHOS

SMSメッセージを設定する

認証に使用するモバイルデバイスの電話番号を入力します。

国:
Japan

電話番号
+81 8012345678

注: SMS 料金が適用されます。テキストメッセージは海外から送信されることがあるため、国際 SMS 料金がかかる場合があります。詳細は、通信会社にお問い合わせください。

次へ

手順 2 / 2

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「完了」ボタンをクリックします。

SOPHOS

デバイスを確認する

モバイルデバイスで受信したばかりのセキュリティコードを入力します。

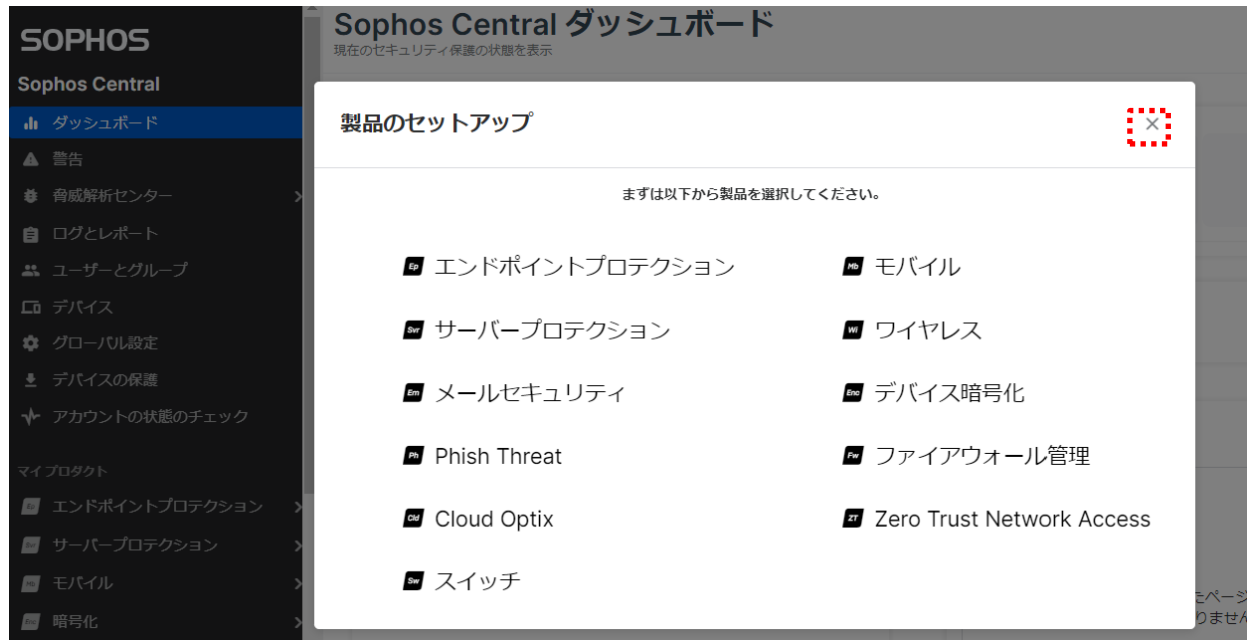
セキュリティコード

次へ

< 戻る

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。



4 エージェントのインストール

本章では、Intercept X Advanced for Server with XDR のエージェントを各サーバー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て、Sophos Central Admin にログインしダウンロードする方法と、ダウンロードリンクにより各サーバーで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。

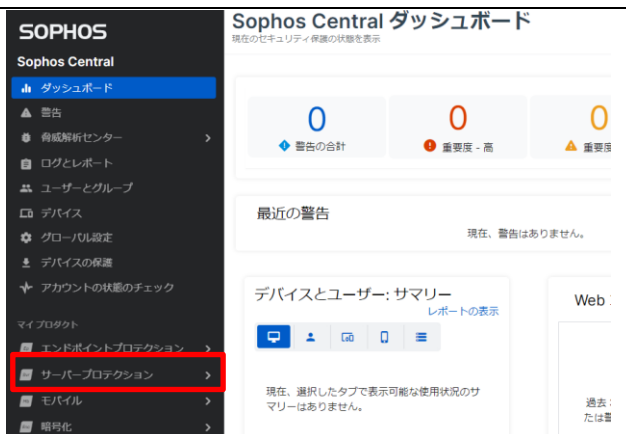
また、本手順書では割愛しますが、スクリプトによる展開、ディスクイメージでの展開方法等があり、こちらは以下 URL のサポートデータベースをご参照ください。

<https://support.sophos.com/support/s/article/KB-000034831?language=ja>

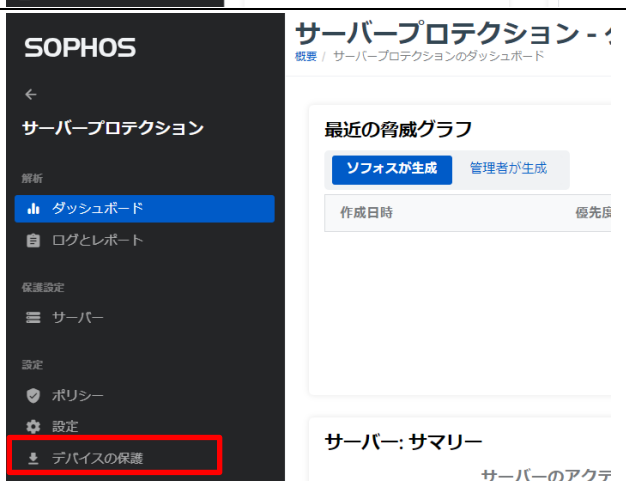
4.1 Sophos Central Admin からダウンロード

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。

- 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「サーバープロテクション」をクリックします。



- 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「デバイスの保護」をクリックします。



3. 右ペインにサーバー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 Server 用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。

続けて、「Linux サーバー用インストーラのダウンロード」をクリックします。



4. 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。

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。



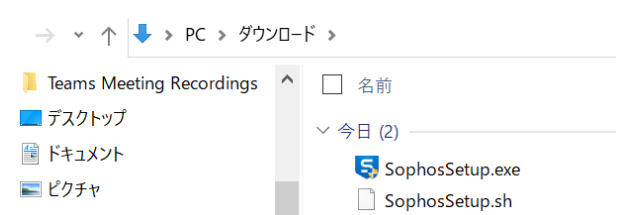
5. エクスプローラが起動されダウンロードしたインストーラが表示されます。

Windows 用 : SophosSetup.exe

Linux 用 : SophosSetup.sh

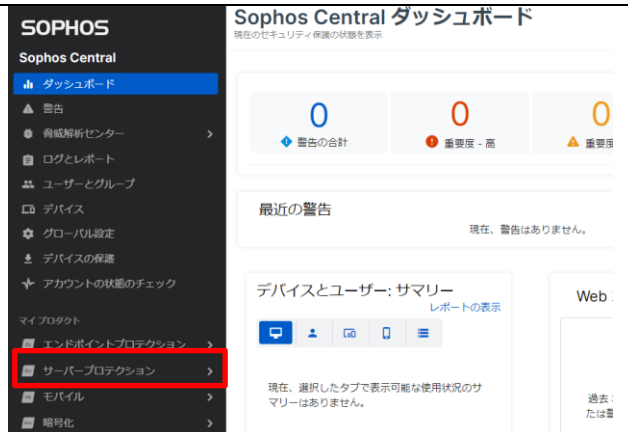
となります。

このインストーラを USB または共有フォルダ等を利用し各サーバーにコピーしてインストールを行います。

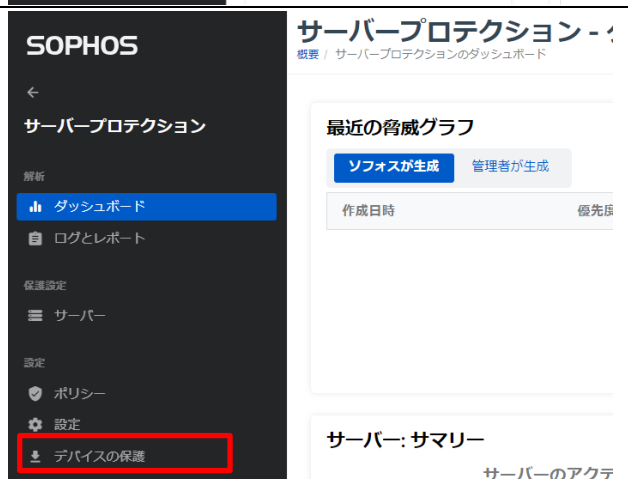


4.2 ダウンロードリンクでのダウンロード

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「サーバープロテクション」をクリックします。



2. 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「デバイスの保護」をクリックします。



3. 右ペインにサーバープロテクションのデバイス保護の画面が表示されます。



4. 「Windows Server 用インストーラのダウンロード」を右クリックし、「リンクのアドレスをコピー」をクリックします。



5. メモ帳を起動し、コピーしたリンクを貼り付けます。



6. 続けて、「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、「リンクのアドレスをコピー」をクリックします。



7. メモ帳にコピーしたリンクを貼り付けます。
このリンクアドレスを利用し、各サーバーにてブラウザ等によりインストーラをダウンロードしインストールを行います。



このリンクアドレスでのダウンロードは、Sophos Central Admin へログインすることなくダウンロードが可能となります。

4.3 Windows 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、Windows 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 Windows Server 上で行い、インストールは Administrator 権限のあるユーザーで行う必要があります。

1. ブラウザにて、前節 5.2 節 4 項でコピーしたアドレスを開きます。（本手順では Google Chrome を利用しています）

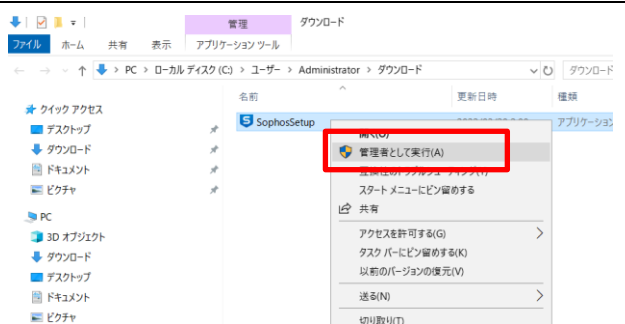
リンクアドレスの末尾が SophosSetup.exe のアドレスです。



2. インストーラがダウンロードされ、画面下部にインストーラが表示されます。ファイル名のプルダウンをクリックし「開く」をクリックします。



3. ファイルを選択して右クリックから「管理者として実行」をクリックします。



4. インストール前の Server の状態チェックが行われます。



5. 状態のチェックが終了するとインストールの確認画面が表示されます。「インストール」ボタンをクリックします。



6. インストールが開始されます。

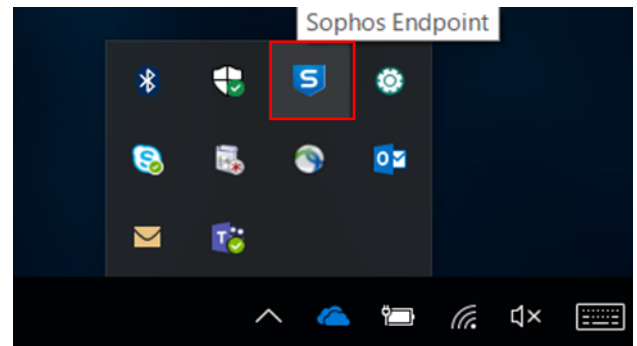
インストールはコンポーネントをダウンロードしながら行われるため、しばらく時間がかかります。



7. 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。



8. PC 再起動後、画面右下のタスクトレイからソフトウェア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することができます。



9. サーバーのステータス画面が表示されます。
この画面で Server が保護されていることを確認します。

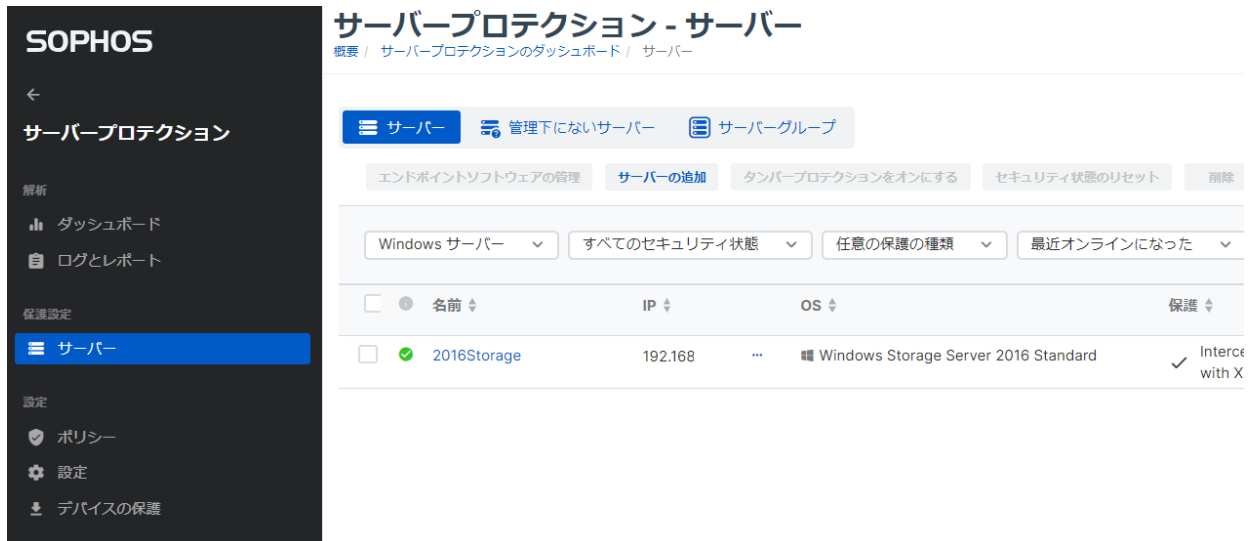


10. 以降の操作は Sophos Central Admin を操作する端末で行います。

11. 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「サーバープロテクション」をクリックします。



12. 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 Windows Server のコンピューター名が表示されていることを確認します。



The screenshot shows the Sophos Server Protection dashboard. On the left is a dark sidebar with the Sophos logo and navigation options: 'サーバープロテクション', '解析' (Dashboard, Log and Report), '保護設定' (Servers), and '設定' (Policies, Settings, Device Protection). The main content area is titled 'サーバープロテクション - サーバー' and shows a list of servers. The list has columns for '名前' (Name), 'IP', 'OS', and '保護' (Protection). One server is listed: '2016Storage' with IP '192.168...' and OS 'Windows Storage Server 2016 Standard'. The protection status is 'Intercept with X'.

名前	IP	OS	保護
2016Storage	192.168...	Windows Storage Server 2016 Standard	Intercept with X

13. 以上で Windows Server へのインストールは終了です。

4.4 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。

<p>1. <code>wget</code> コマンドにより <code>/tmp</code> にインストーラをダウンロードします。</p> <p><code>wget <5.2 節 6 項でコピーしたアドレス> -P ./</code> のコマンドを実行します。</p> <p>リンクアドレスの末尾が <code>SophosSetup.sh</code> のアドレスです。</p>	<pre>cd /tmp/ wget https://api.stn100hnd.ctr.sophos.com/api/download/53f5ba002f9bb09960df0491fe4d835f/SophosSetup.sh -P ./ --2023-06-30 17:43:06-- https://api.stn100hnd.ctr.sophos.com/api/download/53f5ba002f9bb09960df0491fe4d835f/SophosSetup.sh api.stn100hnd.ctr.sophos.com (api.stn100hnd.ctr.sophos.com) を DNS に問い合わせています... 13.230.251.235, 3.115.163.36, 43.207.14.51 api.stn100hnd.ctr.sophos.com (api.stn100hnd.ctr.sophos.com) [13.230.251.235]: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 SophosSetup.sh [<=>] 9.58M 23.4 MB/s in 0.4s 2023-06-30 17:43:08 (23.4 MB/s) - 'SophosSetup.sh' へ保存終了 [10046801]</pre>
<p>2. <code>chmod</code> 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。</p> <p><code>chmod +x /tmp/SophosSetup.sh</code></p>	<pre># #chmod +x /tmp/SophosSetup.sh #</pre>
<p>3. インストーラを実行します。</p> <p><code>/tmp/SophosSetup.sh</code></p> <p>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。</p> <p>“Now managed by Sophos Central”のメッセージが表示されればインストールが終了です。</p>	<pre>root@ubuntsuTokyo:/tmp# ./tmp/SophosSetup.sh This software is governed by the terms and conditions of a licence agreement with Sophos Limited Found existing installation here: /opt/sophos-spl Attempting to register existing installation with Sophos Central Central token is [bbbfdb77def3e00ab0b97ef6ddf760c4afa9f4513f180e69affe50da1d9e026b], Central URL is [https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep] Registering with Sophos Central Now managed by Sophos Central root@ubuntsuTokyo:/tmp#</pre>

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
 osqueryd started

```
root@ubuntuTokyo:~# systemctl status sophos-spl
● sophos-spl.service - Sophos Linux Protection
   Loaded: loaded (/lib/systemd/system/sophos-spl.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-03-30 15:29:07 JST; 3h 15min ago
     Main PID: 840 (sophos_watchdog)
       Tasks: 189 (limit: 2254)
      Memory: 267.1M
     CGroup: /system.slice/sophos-spl.service
            └─ 840 /opt/sophos-spl/base/bin/sophos_watchdog
              └─ 953 /opt/sophos-spl/plugins/runtimedetections/bin/runtimedetections
                └─ 968 /opt/sophos-spl/base/bin/sdu
                  └─ 973 /opt/sophos-spl/base/bin/updatescheduler
                    └─ 993 /opt/sophos-spl/plugins/edr/bin/edr
                      └─ 1004 /opt/sophos-spl/plugins/eventjournaler/bin/eventjournaler
                        └─ 1077 /opt/sophos-spl/plugins/av/bin/av
                          └─ 1104 /opt/sophos-spl/base/bin/python3 -m mcsrouter_mcs_router --no-daemon
                            └─ 1110 /opt/sophos-spl/base/bin/sophos_managementagent
                              └─ 1125 /opt/sophos-spl/plugins/liveresponse/bin/liveresponse
                                └─ 1127 /opt/sophos-spl/base/bin/launcher
                                  └─ 1134 /opt/sophos-spl/base/bin/CommsComponent
                                    └─ 1169 /opt/sophos-spl/base/bin/CommsComponent
                                      └─ 1424 runtimedetections-trigger
                                        └─ 1469 /opt/sophos-spl/plugins/edr/bin/osqueryd --config_path=/opt/sophos-spl/plugins/edr/etc/osquery
                                          └─ 1493 /opt/sophos-spl/plugins/edr/bin/osqueryd
                                            └─ 1494 /opt/sophos-spl/plugins/edr/extensions/SophosMTR_ext --verbose --socket /opt/sophos-spl/plugin
                                              └─ 9114 sophos_threat_detector

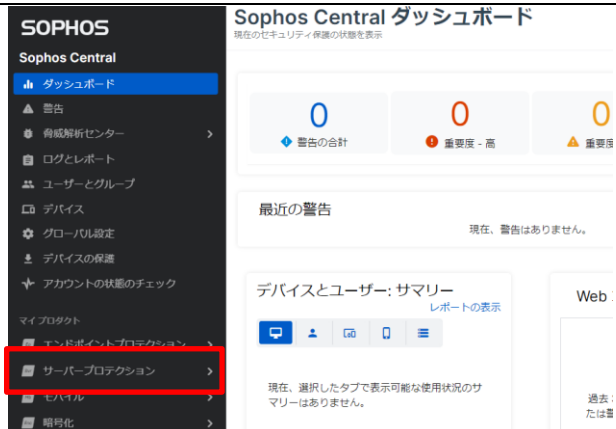
3月 30 15:29:07 ubuntuTokyo systemd[1]: Started Sophos Linux Protection.
3月 30 15:29:13 ubuntuTokyo osqueryd[1469]: osqueryd started | version: 3.1.0
(Lines 1-28/28) (END)
```

5. 次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。

```
root@ubuntuTokyo:/opt/sophos-spl/plugins/av/bin# ./avscanner /tmp
[07:24:03] Logger av configured for level: INFO
[07:24:03] Archive scanning enabled: no
[07:24:03] Following symlinks: no
[07:24:03] Scanning /tmp/.X1024-Lock
[07:24:20] Scanning /tmp/.X1-lock
[07:24:20] Scanning /tmp/.X0-lock
[07:24:20] Scanning /tmp/tmpa0nbuxcp/apt.conf
[07:24:20] Scanning /tmp/.X1025-Lock
[07:24:20] End of Scan Summary:
[07:24:20] 5 files scanned in 17 seconds.
[07:24:20] 0 files out of 5 were infected.
root@ubuntuTokyo:/opt/sophos-spl/plugins/av/bin#
```

4. 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「サーバープロテクション」をクリックします。



5. 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 のコンピューター名が表示されていることを確認します。



The screenshot shows the Sophos Server Protection interface. On the left is a dark sidebar with the Sophos logo and navigation options: < (back), サーバープロテクション (Server Protection), 解析 (Analysis), ダッシュボード (Dashboard), ログとレポート (Logs and Reports), 保護設定 (Protection Settings), サーバー (Servers), 設定 (Settings), ポリシー (Policies), and デバイスの保護 (Device Protection). The main content area is titled 'サーバープロテクション - サーバー' (Server Protection - Servers) and includes a breadcrumb trail: 概要 / サーバープロテクションのダッシュボード / サーバー. Below the title are tabs for 'サーバー' (Servers), '管理下でないサーバー' (Servers not under management), and 'サーバーグループ' (Server Groups). There are also buttons for 'エンドポイントソフトウェアの管理' (Manage endpoint software), 'サーバーの追加' (Add server), 'タンバープロテクションをオンにする' (Turn on tamper protection), and 'セキュリティ状態の' (Security status). A filter bar shows 'Linux サーバー' (Linux servers), 'すべてのセキュリティ状態' (All security states), '任意の保護の種類' (Any protection type), and '最近オンライン' (Recently online). A table lists servers with columns for '名前' (Name), 'IP', and 'OS'. The first row, 'Test-ubuntu' with IP 192.168. and OS Ubuntu 22.04.2 LTS, is highlighted with a red box. The second row is 'localhost' with IP 192.168. and OS CentOS Linux release 7.9.2009 (Core).

6. 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。

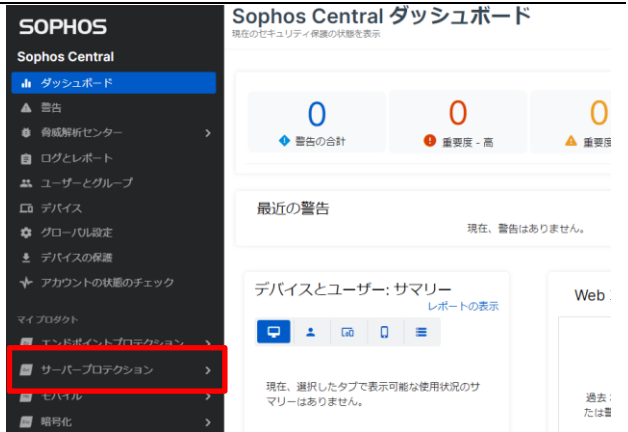
<https://support.sophos.com/support/s/article/KB-000042835?language=ja>

5 サーバークループの登録

本章では、各サーバーをグループ化し、グループ単位でポリシーを適用させるためのサーバークループを作成する手順を説明します。

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「サーバークループ」をクリックします。



2. サーバークループのダッシュボード画面が表示されます。

左ペインの「サーバー」をクリックします。



3. 右ペインに導入された Server の一覧が表示されます。右ペインの画面上部の「サーバーグループ」タブをクリックし、「サーバーグループの追加」をクリックします。



4. サーバーグループ追加の画面が表示されます。

「新しいトップレベルのグループの作成」を選択して「次へ」をクリックします。



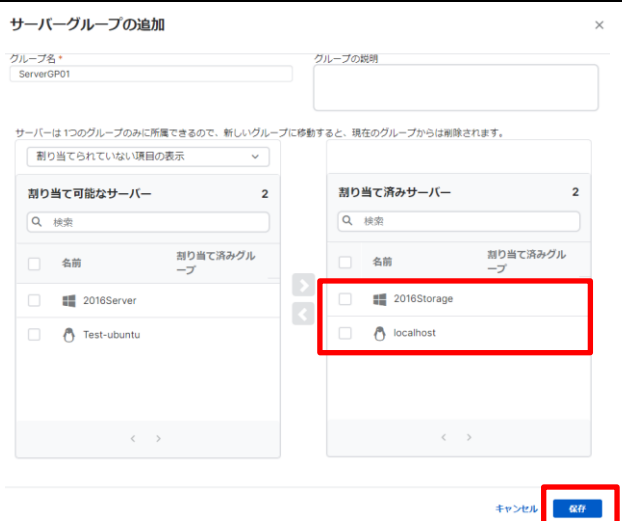
グループ名に任意のグループ名を入力します。（この手順書では“ServerGP01”としています）



- 次に、割り当て可能なサーバーの一覧に 5 章でインストールしたサーバーが表示されていますので、サーバー名の左にあるチェックボックスにチェックを付け、画面中央の右矢印「>」ボタンをクリックします。



- 割り当て済みサーバーにサーバー名が表示されたことを確認し「保存」ボタンをクリックします。



- 作成したサーバーグループが表示されていることを確認します。作成した「グループ名」をクリックします。

サーバープロテクション - サーバーグループ

概要 / サーバープロテクションのダッシュボード / サーバーグループ

🏠 ソフト



8. グループのサマリーが表示され、現在グループのメンバーとなっているサーバー一覧が表示されます。

左ペインに **編集** | **削除** が表示されており、グループメンバーを変更する場合は編集、グループを削除する場合は削除をクリックします。

サーバープロテクション - ServerGP01

概要 / サーバープロテクションのダッシュボード / サーバーグループ / ServerGP01

ServerGP01
編集 | 削除

1 サマリー 2 ポリシー

グループの詳細
グループの説明

グループメンバー

グループメンバー: 2

2016Storage
localhost

9. 右ペイン上部の「ポリシー」をクリックします。グループに割り当てられているポリシーが表示されます。

Sophos Central ではデフォルトポリシーが作成されており、初期状態ではこのデフォルトポリシーが割り当てられています。

サーバープロテクション - ServerGP01

概要 / サーバープロテクションのダッシュボード / サーバーグループ / ServerGP01

ヘルプ
ソフオス

ServerGP01
編集 | 削除

1 サマリー 2 ポリシー

3 Policies below apply to ServerGP01.

種類	名前
サーバープロテクション: 脅威対策	Base Policy - 脅威対策
サーバープロテクション: 周辺機器コントロール	Base Policy - 周辺機器コントロール
サーバープロテクション: アプリケーションコントロール	Base Policy - アプリケーションコントロール
サーバープロテクション: Web コントロール	Base Policy - Web コントロール
サーバープロテクション: データ流出防止 (DLP)	Base Policy - データ流出防止 (DLP)
サーバープロテクション: アップデートの管理	Base Policy - アップデートの管理
サーバープロテクション: Windows ファイアウォール	Base Policy - Windows ファイアウォール
サーバープロテクション: ファイル整合性の監視	Base Policy - ファイル整合性の監視
サーバープロテクション: ロックダウン	Base Policy - ロックダウン

6 ポリシー

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

ポリシーは、ユーザー、またはサーバーを保護するために、Sophos Central で適用するセキュリティ設定の集まりです。「サーバープロテクション」-「ポリシー」にて、管理することが出来ます。



サーバープロテクション - ポリシー

ヘルプ ソファス・スーパ

検索

注:ポリシーはリストの上から下の順番で優先的に適用されます。

脅威対策 (1)	名前	状態	サーバー (個別/グループ)	前回更新日時
	デフォルトポリシー - 脅威対策	✓ 適用済み		2023/03/06

周辺機器コントロール (1)	名前	状態	サーバー (個別/グループ)	前回更新日時
	デフォルトポリシー - 周辺機器コントロール	✓ 適用済み		2022/11/14

アプリケーションコントロール (1)	名前	状態	サーバー (個別/グループ)	前回更新日時
	デフォルトポリシー - アプリケーションコント...	✓ 適用済み		2022/11/14

サーバー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、Web コントロール、ロックダウン、データ流出防止、アップデートの管理、Windows ファイアウォール、ファイル整合性の監視）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ァス推奨のデフォルトポリシーが適用されています。

また、「脅威対策」と「アップデート管理」以外については Windows Server のみ適用されるポリシーとなります。ここでは、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、Web コントロール、ロックダウン、データ流出防止、アップデートの管理のポリシーを説明します。

尚、ロックダウンポリシーについては 8 章に記載いたしますので 8 章をご参照ください。

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。（Windows Server のみの機能です）

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。（Windows Server のみの機能です）

6.4 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 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。（Windows Server のみの機能です）

6.5 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。（Windows Server のみの機能です）

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。（Windows Server のみの機能です）

6.8 ファイル整合性の監視ポリシー

PCI:DSS コンプライアンスの準拠を必要とする場合や、重要なファイルやレジストリキーの監視を必要とする場合に役立ちます。重要な Windows システムファイルへの変更を監視するデフォルトのルールを提供しています。また、監視場所や除外を追加することができます。対象として、ファイル、フォルダ、レジストリキー、レジストリ値を監視します。（Windows Server のみの機能です）

7 サーバーロックダウン

本章では、Intercept X Advanced for Server のサーバーロックダウン機能の設定方法について説明します。サーバーロックダウンは、サーバーでの未認証のソフトウェアの実行を防止する機能です。サーバーにインストールされている安全なソフトウェアをリスト化し、このリストにあるソフトウェアのみに実行を許可する仕組みです。また、サーバーロックダウン機能は、アプリケーション間の信頼関係を設定し、どのアプリケーションが他のアプリケーションを更新できるかを設定します。ソフォスでは、信頼されたアプリケーションにデータフィードを提供し、サーバーがどのアプリケーションをインストールしたかに基づいて自動的に製品を設定します。（Windows Server のみの機能です）

7.1 サーバーロックダウンの事前準備

サーバーロックダウンの設定を行う前に導入対象サーバーで以下の事項を確認してスタートの準備を行います。

- ◇ ダウンロード等を行ったインストーラのうち、今後使用しない不要なインストーラが削除されていること
- ◇ 一時ファイル用のフォルダが消去され、ブラウザのキャッシュがクリアされていること
- ◇ インストールされたすべてのアプリケーションは信頼の置けるものであること
- ◇ サーバーで必要とされている役割および機能がインストールされていること
- ◇ 最新の Windows Update が適用されていること

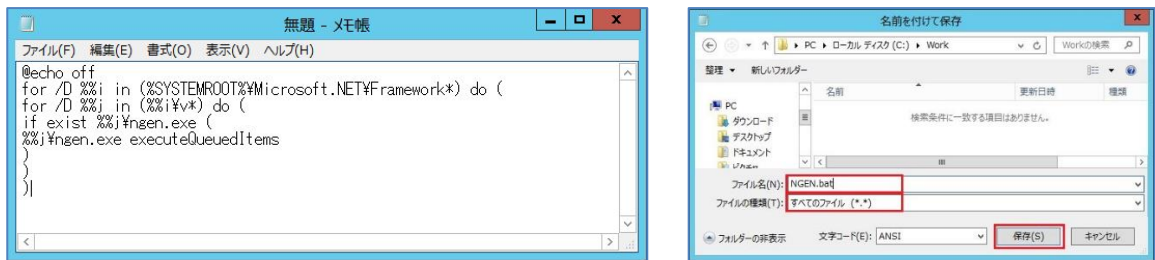
また、サーバーロックダウン設定直前に Windows Update を実施した場合、.NET ネイティブ イメージの生成が未指定の時間で実行される可能性があります。.NET ネイティブ イメージの生成中にロックダウンの処理が発生した場合、ホワイトリストには追加されないため、すべての .NET アプリケーションの実行が阻止されることとなります。詳細については以下 URL のサポートデータベースをご参照ください。

<https://support.sophos.com/support/s/article/KB-000035352?language=ja>

以下の手順を実行し、.NET ネイティブ イメージの操作が実行されているかどうかを確認します。

1. メモ帳を起動し以下の 8 行を “NGEN.bat” として保存します。（本手順書では C:¥Work¥NGEN.bat に保存しています）

```
@echo off
for /D %%i in (%SYSTEMROOT%¥Microsoft.NET¥Framework*) do (
for /D %%j in (%%i¥v*) do (
if exist %%j¥ngen.exe (
%%j¥ngen.exe executeQueuedItems
)
)
)
```

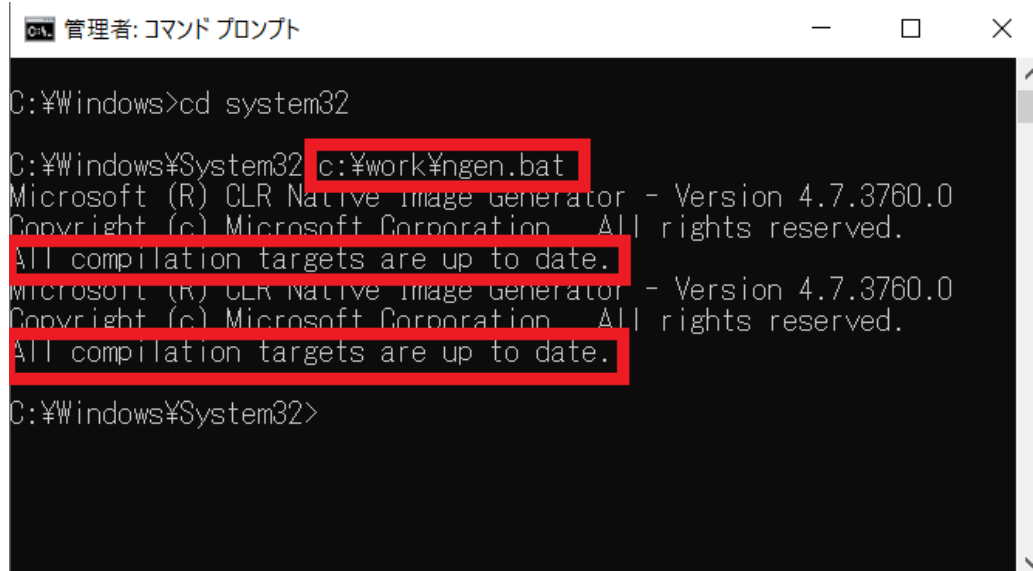


2. コマンドプロンプトを管理者モードで起動し、上記で作成したバッチ“NGEN.bat”を実行します。

バッチは、サーバー上にインストールされている .NET Framework のすべてのバージョンに関するキューにあるすべてのアイテムに対してコマンドの実行を行います。すべてのバージョンに対して次の応答があった場合にロックダウンを開始できることになります。

All compilation targets are up to date.

すべてのバージョンに対してこの応答が確認できない場合には、最新である状態が確認できるまでこの確認処理を繰り返します。



7.2 ロックダウンポリシー

ロックダウンポリシーは、“許可するファイルやフォルダ”、“ブロックするファイルやフォルダ”の設定をおこないます。

サーバーのロックダウン機能を選択する前にポリシーを設定することによって、ブロックするに指定されたファイルやフォルダはスキャン検索の対象にはならず、許可リストにも追加されずに済むという利点があります。これによって許可リストを生成する時間が節減されます。ロックダウンの処理自体は、すべてのローカルドライブをスキャン検索するため、ポリシーを設定する際にはこのことを考慮に入れる必要があります。

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「サーバープロテクション」をクリックします。



2. 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。

左ペインの「ポリシー」をクリックします。



3. 右ペインにポリシーの一覧が表示されます。
画面右上の「ポリシーの追加」をクリックします。

サーバープロテクション - ポリシー

概要 / サーバープロテクションのダッシュボード / ポリシー

ヘルプ
ソフォス・スーパー管理者

検索

ポリシーの追加

注:ポリシーはリストの上から下の順番で優先的に適用されます。

脅威対策 (1)			
名前	状態	サーバー (個別/グループ)	前回更新日時
デフォルトポリシー - 脅威対策	✓ 適用済み		2023/03/06

4. ポリシーの追加画面が表示されます。
プルダウンより、「機能のオプションを選択してください」をクリックし、「ロックダウン」をクリックします。

選択後、「続行」をクリックします。



5. ロックダウンポリシーの新規作成画面が表示されます。
ポリシー名に任意のポリシー名（本手順書では“ロックダウンポリシー 1”としております）を入力します。
次に、割り当て可能なサーバーよりロックダウンを設定する Windows Server のチェックボックスにチェックを付け、画面中央の「>」をクリックします。（本章ではサーバー個別にポリシーを割り当てます）

サーバープロテクション - サーバーポリシーの新規作成

概要 / サーバーポリシー / サーバーポリシーの新規作成

ヘルプ
ソフォス・スーパー管理者

ポリシー名 *

ポリシーの種類

このポリシーを適用するサーバーの指定

! このポリシーはどのサーバーにも適用されません。

割り当て可能なサーバー

- 割り当て可能なサーバー 4
- 2016Server
- 2016Storage
- localhost
- Test-ubuntu

割り当て済みサーバー

- 割り当て済みサーバー 0

6. 割り当て済みサーバーにチェックを付けたサーバーが表示されます。

「設定」タグをクリックします。

ポリシーの種類

このポリシーを適用するサーバーの指定

割り当て可能なサーバー

- 割り当て可能なサーバー 3
- 2016Server
- localhost

割り当て済みサーバー

- 2016Storage

7. ロックダウンポリシーの設定画面が表示されます。
以降、設定項目について説明します。

サーバープロテクション - サーバーポリシーの新規作成

概要 / サーバーポリシー / サーバーポリシーの新規作成

ヘルプ
ソフォス・スーパー管理者

ポリシー名*

保存 キャンセル

ポリシーの種類 ロックダウン

サーバー 0 グループ 設定 ✓ ポリシーの状態: 適用済み

対象

サーバーをロックダウンすると、サーバーにインストールされているソフトウェアがリスト化され、以後リストにあるソフトウェア以外は実行できなくなります。許可するソフトウェアは、サーバーのロックを解除することなく変更できます。

許可するファイルやフォルダ

ソフトウェアの実行や他のファイルの変更を許可します。

許可するファイルやフォルダの追加

パス	種類
現在、信頼するファイルやフォルダはありません	

8. 許可するファイルやフォルダ

許可するファイルおよびフォルダを指定します。
指定したファイルや指定したフォルダに保存した新しいソフトウェアの実行が可能になります。
また、既存のソフトウェア（インストーラやアップデート）を実行して他のアプリケーションを変更することもできます。
信頼されたインストーラを保存にするのに使用しているフォルダなどを設定します。

許可するファイルやフォルダ

ソフトウェアの実行や他のファイルの変更を許可します。

許可するファイルやフォルダの追加

パス	種類
現在、信頼するファイルやフォルダはありません	

許可するファイルやフォルダの追加

種類

パス*

キャンセル 保存

9. ブロックするファイルやフォルダ

ブロックするファイルやフォルダを指定し、現在は実行が許可されているソフトウェアをブロックしたり、インストーラなどに関するフォルダで、ネットワーク上で他の従業員には利用可能にする必要があるが、サーバー上では実行できないようにする必要があるものをブロックできます。

共有フォルダやインストーラの場所などを設定します。

ブロックするファイルやフォルダ

現在実行が許可されているソフトウェアをブロックします。

ブロックするファイルやフォルダの追加

パス	種類
現在、ブロックされたファイルやフォルダはありません	

ブロックするファイルやフォルダの追加

種類

パス*

キャンセル 保存

10. 画面最上段の右側の「保存」ボタンをクリックしてポリシーを作成します。



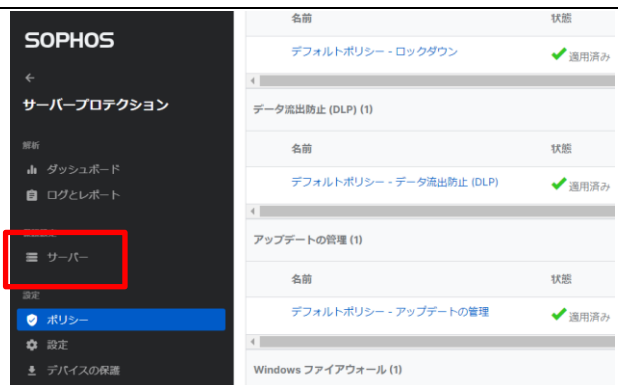
11. デフォルトポリシーの上に新たに作成したロックダウンポリシーが表示されていることを確認します。上段のポリシーが優先され適用されます。

ロックダウン (2)		
名前	状態	サーバー (個別/グループ)
ロックダウンポリシー-1	✓ 適用済み	サーバー (1 / 0)
デフォルトポリシー - ロックダウン	✓ 適用済み	

7.3 サーバーロックダウンのインストール

サーバーロックダウンのインストールは Sophos Central Admin より行い、5.3 節で記載しております Intercept X Advanced for Server エージェントがインストールされている必要があります。

1. サーバープロテクション画面の左ペインの「サーバー」をクリックします。



- 右ペインに Intercept X Advanced for Server がインストールされたサーバー一覧が表示されます。Windows Server の右側、「ロックダウン」をクリックします。

サーバープロテクション - サーバー

ヘルプ ソフトウェア・サーバー管理者

サーバー 管理下でないサーバー サーバークラウド

エンドポイントソフトウェアの管理 サーバーの追加 タンバプロテクションをオンにする セキュリティ状態のリセット 削除 CSV形式で出力

Windows サーバー すべてのセキュリティ状態 任意の保護の種類 最近オンラインになった

名前	IP	OS	保護	前回同期	グループ	ロックダウンの状態
2016Storage	192.168.	Windows Storage Server 2016 Standard	Intercept X Advanced for Server with XDR	2023年6月29日 12:48	ServerGP01	インストール済み ロックダウン

- ロックダウンの警告画面が表示されます。「ロックダウンを開始」をクリックします。

ロックダウンの初期設定ではサーバー上に存在するアプリケーションすべてを検索しリスト化するため終了するまでに時間がかかります。

ロックダウン

ロックダウンの実行中、Sophos Central は現在サーバーにあるすべてのソフトウェアの許可リストを作成します。

この処理には時間がかかることがあります - この処理を実行する間、ソフトウェアをインストールしたり、アップデートしたりしないでください。

サーバーをロックする前に以下の操作を行うことを推奨します:

- サーバーのロールまたは機能をインストールする。
- すべての Windows の更新プログラムをインストールし、必要に応じて再起動を行う。
- 一時ファイル用のフォルダを消去し、ブラウザのキャッシュをクリアする。
- ダウンロードしたインストーラのうち、今後使用しないものを削除する

詳細は、FAQ を参照してください。

キャンセル **ロックダウンを開始**

- ロックダウン開始後、ロックダウンのステータスが「ソフトウェアのインストール中」になります。

ロックダウンの状態

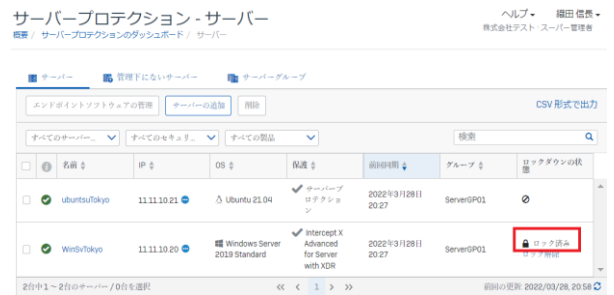
ソフトウェアのインストール中
ロック解除

- インストールが終了するとロックダウンのステータスが「登録中」になります。

ロックダウンの状態

登録中
ロック解除

- ホワイトリストの作成が終了するとロックダウンのステータスが「ロック済み」になりロックダウンのインストールは終了です。



- サーバー側でロックダウンのインストールを確認するには以下の操作を行います。

- 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。



- サーバーのステータス画面が表示されます。画面右下の「バージョン情報」をクリックします。



- 製品部分の“Lockdown”にバージョン番号とロック済みの表示がされている場合、ロックダウンがインストールされていることを示します。



8 タンパープロテクション

本章では、Intercept X Advanced for Server 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。

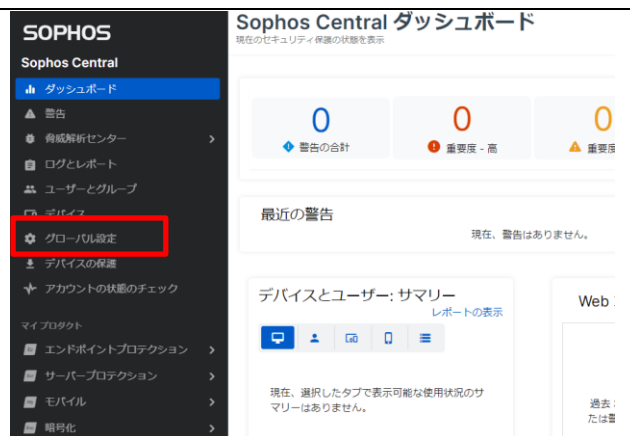
タンパープロテクションは、未承認のユーザーや悪意のあるアプリケーションがソフォスのセキュリティソフトウェアをアンインストールしたり、ソフトウェアの設定を無効設定にしたり、ファイル、レジストリキー、サービス、プロセスの変更を行う動作を阻止する機能です。（Windows Server のみの機能です）

8.1 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。

- 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。



- 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。



- 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。



8.2 タンパープロテクション：サーバー設定

サーバー設定でのタンパープロテクション設定は、サーバ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、サーバー側の 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えます。

1. Sophos Central Admin 画面の左ペインの「サーバープロテクション」をクリックします。



2. サーバープロテクション画面の左ペインの「サーバー」をクリックします。



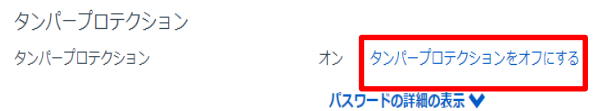
3. 右ペインに Intercept X Advanced for Server がインストールされたサーバー一覧が表示されます。
対象の Windows サーバーの「サーバー名」をクリックしサーバーの詳細画面を表示させます。
(本手順書では 2016Storage をクリック)



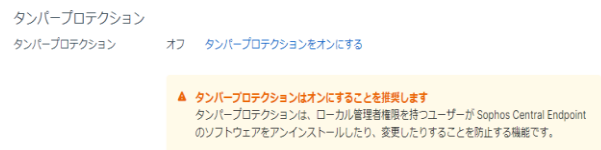
4. サーバーの詳細画面が表示されます。
サマリー、イベント、ステータス等の情報が表示可能になっています。



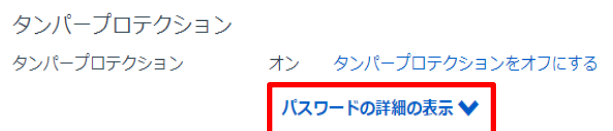
5. サマリータブ画面のサマリー部分にタンパープロテクションの項目が表示され、この「タンパープロテクションを無効化する」をクリックすることで、無効に設定することが可能です。



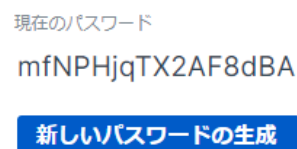
オフにすると「タンパープロテクションはオンにすることを推奨します」と警告が出てきます。



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、サーバー側の GUI(Graphical User Interface)で一時的に設定変更が可能となります。



タンパープロテクションのパスワードの詳細



サーバー側担当者が作業終了後、「新しいパスワードの生成」をクリックすることによってパスワードの再作成が行えます。

7. 以降の操作はサーバー側での操作となり、サーバー側の 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. サーバ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。



9 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。

9.1 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。

- 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。

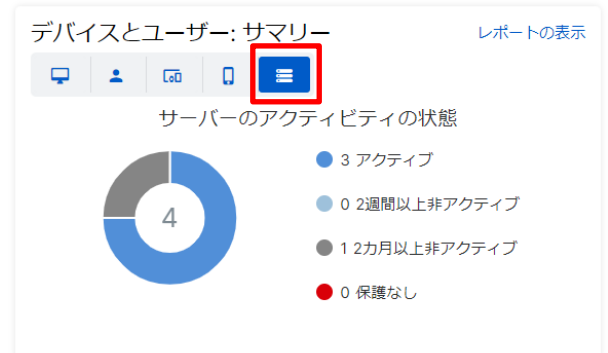
The screenshot shows the Sophos Central Admin dashboard. On the left is a dark sidebar with the 'SOPHOS' logo and a list of navigation items including 'ダッシュボード', '警告', '脅威解析センター', 'ログとレポート', 'ユーザーとグループ', 'デバイス', 'グローバル設定', 'デバイスの保護', 'アカウントの状態のチェック', and various security products like 'エンドポイントプロテクション', 'サーバープロテクション', 'モバイル', '暗号化', 'ワイヤレス', 'メールセキュリティ', 'ファイアウォール管理', 'Phish Threat', 'Cloud Native Security', 'ZTNA', and 'スイッチ'. The main dashboard area is titled 'Sophos Central ダッシュボード' and shows a summary of security status. It features four alert cards: '警告の合計' (0), '重要度 - 高' (0), '重要度 - 中' (0), and '重要度 - 低' (0). Below this is a '最近の警告' section with the message '現在、警告はありません。' and a link to 'すべての警告の表示'. There are also sections for 'デバイスとユーザー: サマリー' (no data) and 'Web コントロール' (no data for the last 30 days). At the bottom, there are links for 'クラウドのセキュリティ状態の管理' and '統合エンドポイント管理'.

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、検知したサーバー名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）
- ・ 「サーバー名」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。



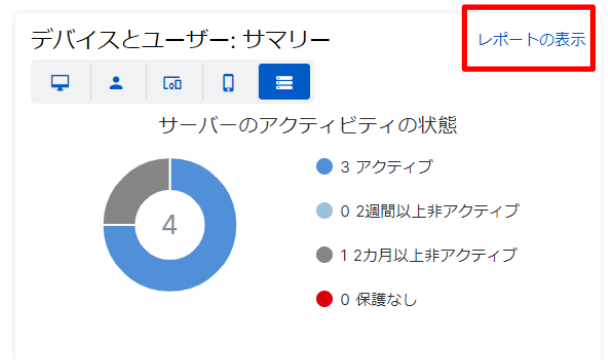
3. 次に、「使用状況のサマリー」部分で、サーバーアイコンのタグをクリックします。



4. サーバ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、現在稼働中のサーバー（アクティブ）、2週間以上、2ヶ月以上、Sophos Central Admin と接続がないサーバーがグラフで表示されます。

「レポートの表示」部分ををクリックします。



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、サーバ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サーバ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」よりサーバー一覧をデータ出力することが可能です。

サーバーレポート ヘルプ
レポート / サーバーレポート ソフォス・スーパー管理者

検索

すべてのサーバーを表示 サーバークラウドで検索

名前 ↓	オンライン ↓	リアルタイム検索	前回更新 ↓	前回のスケジュール検索 ↓	セキュリティ状態	グループ
2016Server	3ヶ月前	はい	3ヶ月前	Sophos Central Scheduled Scan 3ヶ月前	▲	
2016Storage	1時間前	はい	21時間前	Sophos Central Scheduled Scan 1日前	●	ServerGP01

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。

Web コントロール レポートの表示

5 Web 脅威 ブロック数	711 ポリシー違反 ブロック数
6 ポリシー警告 表示数	3 ポリシー警告 続行数

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。

ポリシーに違反したユーザー

レポート / ポリシーに違反したユーザー

期間の選択:
過去 30日 ▼

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

違反者	アクセス数	検出した違反上位5種
WinSvTokyo	711	Chat (158) Chat (48) Chat (48) Chat (32) Chat (16)

9.2 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、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。

SOPHOS

Sophos Central

- ダッシュボード
- 警告
- 脅威解析センター
- ログとレポート
- ユーザーとグループ
- デバイス
- グローバル設定
- デバイスの保護
- アカウントの状態のチェック
- マイプロダクト
- エンドポイントプロテクション
- サーバープロテクション

ログとレポート

セキュリティの解析や改善に役立つログやレポートの表示

フィルタの表示

テンプレート名	レガシー?	送信元	作成者
合計テンプレート数: 0			

ログ

S 一般ログ

イベント

マルウェア検出など、デバイス上のすべてのセキュリティイベントを表示し、それらを絞り込んでレポートを生成できます。

Em メール

Cid Clo

システムで行われたすべてのアクティビティや変更に関する記録です。

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。

イベントレポート
レポート / イベントレポート

ヘルプ ソフォス・スーパー管理者

検索 検索する項目: コンピュータ OR ユーザー OR 脅威

期間の選択: 過去 7日

フィルタとグラフの非表示

更新

すべての重要度を表示 ユーザーグループで検索 コンピュータまたはサーバーグループで検索

選択した項目に該当するイベントが表示されます

- 種類 (17)
- ▶ ランタイム検知 (0)
- ▶ アプリケーションコントロール (0)
- ▶ マルウェア (0)

2023年6月23日 2023年6月25日 2023年6月27日 2023年6月29日

カスタムレポートとして保存 エクスポート

- CSV - 現在のビュー
- PDF - 現在のビュー
- CSV - 過去 90日
- PDF - 過去 90日

重要度	発生日時	イベント	ユーザー
i	2023/06/28 17:47:53	アップデートに成功しました	n/a
i	2023/06/28 17:29:57	検索 'Sophos Central Scheduled Scan' が完了し...	n/a

9.3 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
To 自分

3月28日(月) 23:48 (1 時間前) ☆ ↶ ⋮

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 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: ubuntuTokyo

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が (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。

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

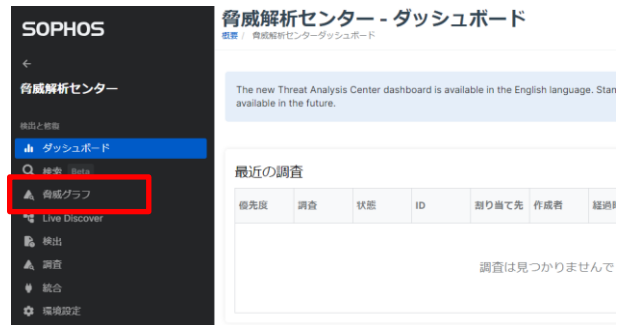
本章では、マルウェア検出後の EDR/XDR の利用方法について説明します。12 章の 12.1 記載のテストマルウェア eicar を用いた疑似マルウェア攻撃の結果を用いて説明します。

10.1 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. 攻撃が発生したサーバーや根本原因、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。

推奨される次のステップ

脅威グラフの状態の設定

優先度: 低

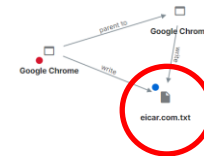
状態: 新規

デバイスの隔離: その間調査します ?

デバイスの検索

Live Discover クエリの実行

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。



名前	種類	レピュテーション	ログ日時	相互作用
chrome.exe	プロセス	悪	2023年6月29日 14:56	246

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 SophosLabs 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。

PDF のダウンロード クリーン&ブロック
この機能の説明

その他のファイル: eicar.com.txt

レポートのサマリー 機械学習分析 ファイルのプロパティ ファイルの内訳

SOPHOSLABS 脅威解析情報
最新レポートの作成日: 2023年6月15日 19:15

最新の解析情報を要求

注: 最新の解析情報を要求すると、ソフォスにファイルが送信され、さらなる解析が行われます。 詳細情報

パス: c:\users\administrator\desktop\eicar.com.txt
名前: eicar.com.txt
SHA256: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

8. 解析が終了したという通知が来ます。

SOPHOSLABS 脅威解析情報
最新レポートの作成日: 2023年6月29日 16:05

最新の解析情報を要求

注: 最新の解析情報を要求すると、ソフォスにファイルが送信され、さらなる解析が行われます。 詳細情報

パス: c:\users\sopho\desktop\test.txt
名前: test.txt
SHA256: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

✓ 解析情報のレポートが生成されました
脅威解析情報のレポート test.txt - WIN10-ZIH2 が生成されました。

11 補足情報

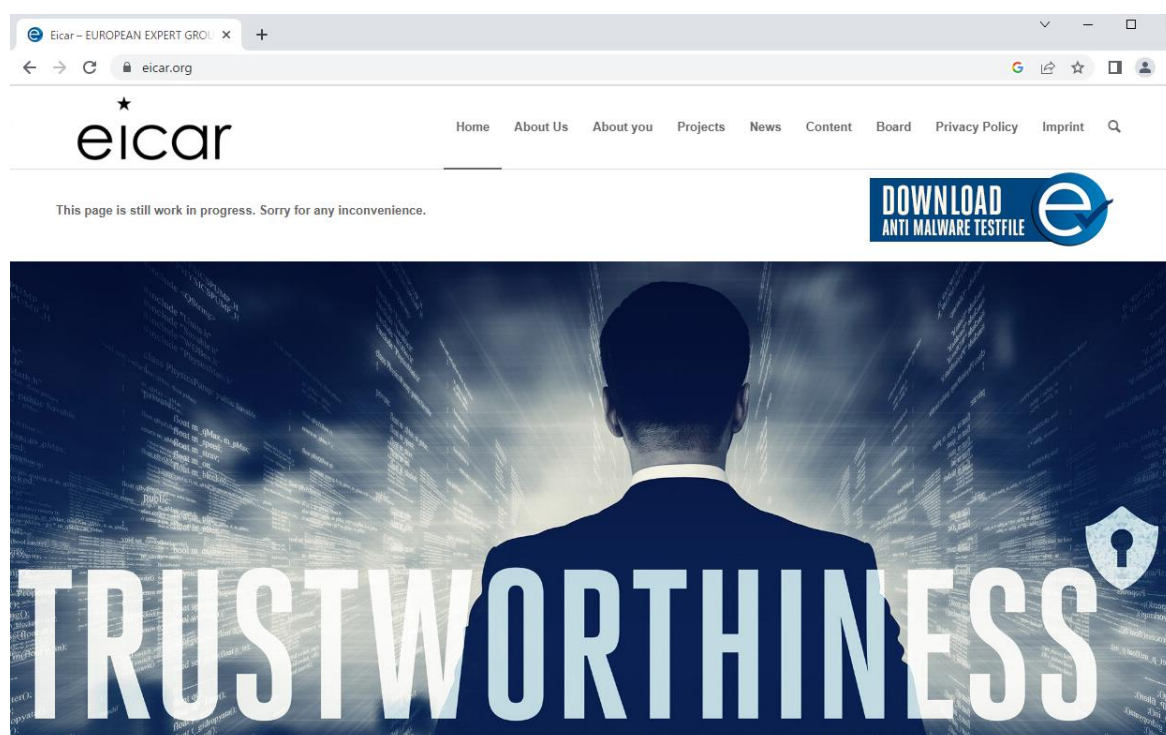
11.1 検出機能をテストする方法

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あります。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?language=ja&_displayLanguage=ja

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。



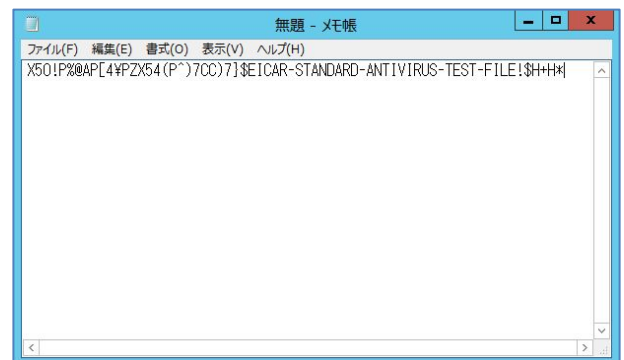
11. 表示された画面の下部に “X5O!” から始まる文字列が表示されています。この文字列をドラックしコピーします。

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

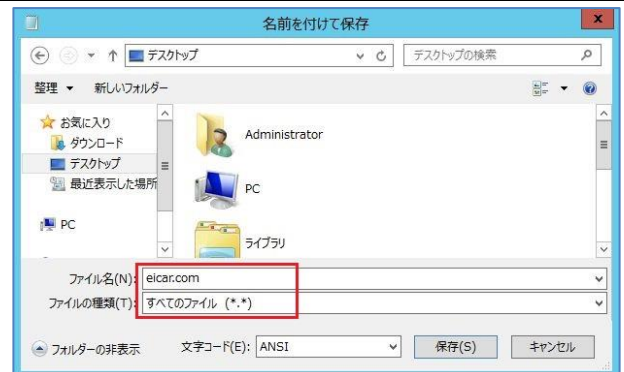
X5O!P%#@AP[4!PZX54(P^)7CC)7]\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

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

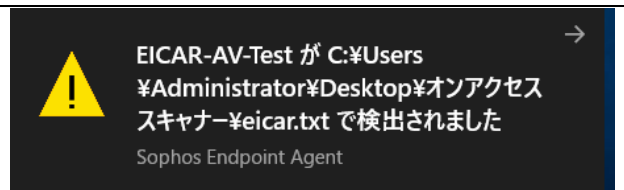
12. メモ帳を起動し、コピーした文字列を貼り付け、保存します。



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 for Server を導入したサーバーに保存すると、右のポップアップメッセージが表示されます。



※検出の詳細は脅威解析センターで確認ができます

<https://support.sophos.com/support/s/article/KB-000036359?language=ja>

11.2 エージェントのアンインストール（Windows Server）

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 Server のアンインストール手順で、サーバーロックダウン機能を導入されている場合の手順となります。サーバーロックダウンを導入されていない場合、タンパープロテクションの解除操作部分より行います。

1. 最初にサーバーロックダウン機能の解除を行います。

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「サーバープロテクション」をクリックします。



2. 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。

左ペインの「サーバー」をクリックします。



3. 右ペインにサーバー一覧が表示されます。アンインストールする対象サーバーの右端の「ロック解除」をクリックします。

サーバープロテクション - サーバー

概要 / サーバープロテクションのダッシュボード / サーバー

ヘルプ
ソフォス・スーパー管理者

サーバー 管理下でないサーバー サーバークラウド

エンドポイントソフトウェアの管理 **サーバーの追加** タンパープロテクションをオンにする セキュリティ状態のリセット 削除 CSV形式で出力

Windows サーバー 全てのセキュリティ状態 任意の保護の種類 最近オンラインになった 検索

名前	保護	前回同期	グループ	ロックダウンの状態
ge Server 2016 Standard	✓ Intercept X Advanced for Server with XDR	2023年6月29日 15:48	ServerGP01	登録中 ロック解除

4. ロック解除の警告画面が表示されますので、「ロック解除」をクリックします。

ロック解除 ×

このサーバーのロックを解除するには「ロック解除」をクリックしてください。

サーバーは未承認のバイナリファイルの実行をブロックしなくなります。

キャンセル **ロック解除**

5. ロックダウンの状態が「ロック解除中」に変わります。（ロック解除には数分時間がかかります）

🔄 **ロック解除中**
ロックダウン

6. ロックダウンの解除が終了すると、ロックダウンの状態が「ロック解除済み」に変わります。

👍 **ロック解除済み**
ロックダウン

7. 次にタンパープロテクションを解除し、エージェントのアンインストールを行います。サーバー一覧に表示されているアンインストールする対象サーバーの「サーバー名」をクリックし、サーバーの詳細画面を表示します。

サーバープロテクション - サーバー

概要 / サーバープロテクションのダッシュボード / サーバー

ヘルプ
ソフォス・スーパー管理者

サーバー 管理下でないサーバー サーバークラウド

エンドポイントソフトウェアの管理 **サーバーの追加** タンパープロテクションをオンにする セキュリティ状態のリセット 削除 CSV形式で出力

Windows サーバー 全てのセキュリティ状態 任意の保護の種類 最近オンラインになった 検索

名前	IP	OS	保護
2016Storage	192.168	Windows Storage Server 2016 Standard	✓ Intercept X Advanced for Server with XDR

8. サーバー詳細画面のサマリー部分に表示されているタンパープロテクションの「パスワードの詳細の表示」をクリックします。

タンパープロテクション

タンパープロテクション

オン [タンパープロテクションをオフにする](#)[パスワードの詳細の表示](#) ▼

9. タンパープロテクションのパスワードの詳細が表示されます。
表示された「現在のパスワード」をメモします。

タンパープロテクションのパスワードの詳細

現在のパスワード

mfNPHjqTX2AF8dBA

[新しいパスワードの生成](#)

10. 以降の操作はエージェントをアンインストールする Windows Server の操作となります。

11. 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。



12. サーバ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。



13. 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 9 項でメモし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。



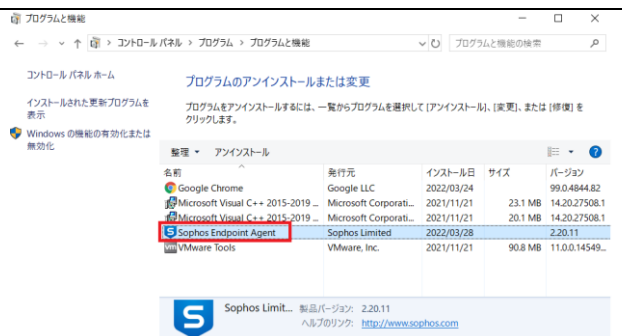
14. 画面上部に表示された「設定」をクリックします。



15. 設定画面が表示されますので、オーバーライトのチェックボックスにチェックを付けます。
チェックを付けることによって設定変更が可能になりますので、タンパープロテクションのボタンを OFF に設定し、画面を閉じます。



16. 次に、コントロールパネルのプログラムと機能より「Sophos Endpoint Agent」を右クリックしアンインストールをクリックします。



17. アンインストールの警告画面が表示されますので「アンインストール」ボタンをクリックします。
Windows OS の状況によりアンインストールには事前に再起動が必要な場合があります。この場合、OS を再起動し、タンパープロテクションを解除し、再度アンインストール操作を行います。



11.3 エージェントのアンインストール (Sophos Linux Protection)

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。

- ターミナルより以下のコマンドを実行します。
Sophos Linux Protection をアンインストールするには、次の手順を実行します。
 - opt/sophos-spl/bin を参照します。
 - アンインストールを起動します。
./uninstall.sh