SOPHOS

Cybersecurity made simple.

Sophos Endpoint for Mac ヘルプ

目次

(2020/08/18)

1 Sophos Endpoint

注
お使いの製品によっては、このヘルプで説明するすべての機能が含まれていない場合もあります。利用できる機能は、お持ちのライセンスによって異なります。

Sophos Endpoint は、Sophos Central Admin から一元的に設定・管理されます。

Mac で実行できるタスクは次のとおりです。

- Mac のステータス (p. 2)を確認する。
- ファイルの検索 (p. 8)またはMac の検索 (p. 8)を実行し、脅威を検索する。
- Mac で発生したイベント (p. 3)の詳細を表示する (例: 検出された脅威など)。
- 脅威のクリーンアップ (p. 8)。
- セキュリティ設定の変更 (p. 8)。たとえば、トラブルシューティングを行う目的で一時的に機能を無効化できます。
- 今すぐアップデート (p. 9)。
- トラブルシューティング (p. 9)。

注
脅威をクリーンアップしたり、設定を変更したりするには、「**管理モードログイン**」でタンパープロテクションのパスワードを入力する必要があります。

2 ステータス

注
お使いの製品によっては、ここで説明するすべての機能が含まれていない場合もあります。利用できる機能は、お持ちのライセンスによって異なります。

「**ステータス**」ページでは、次の操作を実行できます。

- Mac のセキュリティステータスを表示する。
- Mac の脅威検索を実行する。
- インストール済みの機能とそのセキュリティ状態を確認する。

注
「**バージョン情報**」というリンクから、ウイルス定義のアップデートや製品のトラブルシューティングを行うことができます。

セキュリティの状態

画面右上のアイコンが状態を表します。


緑色: 警告が発生していない、もしくは発生している場合でも重要度の低い警告しか発生していない状態。


赤: 重要度の高い警告が発生している状態。


黄色: 重要度が中程度の警告が発生している状態。


グレー: ステータスが不明な状態。

この下に、インストール済みのすべての機能がそのセキュリティ状態とともに表示されます。

Mac の検索

Mac 上のすべてのファイルに対して脅威検索を実行するには、「**今すぐ検索**」をクリックします。

注
脅威が検出された場合、「**今すぐ検索**」は使用できません。脅威の詳細を表示する場合は、「**詳細の表示**」をクリックします。

検索が完了すると、検索結果のサマリーが表示されます。脅威が検出された場合は、「**詳細の表示**」または「**イベント**」をクリックして詳細を表示できます。

3 イベント

注
お使いの製品によっては、ここで説明するすべての機能が含まれていない場合もあります。利用できる機能は、お持ちのライセンスによって異なります。

「**イベント**」ページには、検出された脅威など、Mac で発生したイベントが表示されます。

イベントは絞込み表示することができます。たとえば、対処の必要なイベントのみを表示したり、特定の種類のイベントを検索したりすることができます。

イベントリスト

イベントリストには次の項目が表示されます。

- 重要度。アイコンが、イベントの重要度 (高、中、通知) を示します。
- 発生元。アイコンが、イベントを報告したソフォス製品の機能を示します。
- イベントが発生した日付と時刻。
- イベントの説明。
- アクションを実行するためのリンク (対処が必要な場合)。管理モードでサインインしているときのみに表示されます。

イベントの詳細を表示するには、リスト内で該当するエントリをクリックします。

ここで実行できるアクションは、Sophos Central Admin コンソールで実行できるアクションと同じものです。詳細は、Sophos Central ヘルプの「**警告**」ページにある一覧を参照してください。

マルウェア/不要と思われるアプリ

マルウェアは悪意のあるソフトウェアの総称です。ウイルス、ワーム、トロイの木馬、スパイウェアなどが含まれます。

不要と思われるアプリケーション (PUA) は、ダイヤラー、リモート管理ツール、ハッキングツールなど、悪質ではないものの一般的に企業ネットワークには不適切と考えられているアプリです。

Web 脅威

Web 脅威とは、悪意のある Web サイトや危険なダウンロードを指します。

アダルトサイトやソーシャルメディアなど、一部の Web サイトも一般に業務上不適切と考えられています。これはブロックできます。

制御する項目

このカテゴリには次の項目が含まれます。

- セキュリティ脅威ではないものの職場での使用は不適切とされるアプリケーション。
- 周辺機器とリムーバブルメディア。

- 危険なダウンロードまたは職場での閲覧が不適切とされる Web サイト。
- データ漏えい防止対象の機密情報 (個人情報や財務情報など) を含むファイル。

悪質なトラフィック

悪質なトラフィックとは、Mac を制御しようとする兆候がみられる、コンピュータ間のトラフィック (C & C 攻撃: コマンドアンドコントロール攻撃) を指します。

ランサムウェア

ランサムウェアは悪意のあるソフトウェアで、感染したコンピュータのファイルへのアクセスを制限し、制限の解除と引き換えに「身代金」を要求します。

4 検出

Mac を検索して脅威を検出し、ソフォス製品が検出してブロックした脅威を表示できます。

コンピュータの検索

Mac 上のすべてのファイルに対して脅威検索を実行するには、「**今すぐ検索**」をクリックします。

検索が完了すると、検索結果のサマリーが表示されます。脅威が検出された場合は、「**イベント**」ページで詳細を確認できます。

マルウェア/不要と思われるアプリのイベントの履歴

検出されたマルウェアおよび不要と思われるアプリの履歴が表示されます。矢印をクリックして、「**イベント**」ページで詳細を参照できます。

検出履歴

脅威の種類ごとの検出数が表示されます。各種類をクリックすると、「**イベント**」ページが開き、対応する種別の検出された脅威の詳細が表示されます。

サマリーをリセット

「**検出**」ページに表示される検出履歴のカウンターをゼロに戻すには、「**サマリーをリセット**」をクリックします。

5 設定

注
お使いの製品によっては、ここで説明するすべての機能が含まれていない場合もあります。利用できる機能は、お持ちのライセンスによって異なります。

「**設定**」ページは、「**管理モードログイン**」を使用して、タンパープロテクションのパスワード (Sophos Central の管理者から入手できます) を入力した場合のみに表示されます。

ここでは、Mac の設定を一時的に変更することができます。

この操作は、トラブルシューティングを行う際に必要となる場合があります。たとえば、一時的に機能を無効化し、Mac で発生している問題の原因となっていないかどうかを確認することなどができます。

設定の変更方法

「**トラブルシューティングを行うために、最長 4時間 Sophos Central のポリシーをオーバーライドする**」をオンにします。

ページ上の設定が変更できるようになります。ここで行う変更は、管理者が Sophos Central Admin コンソールから適用したポリシーを一時的にオーバーライドします。

変更した設定は、4時間後に、集中管理されているポリシーの設定に自動的に戻ります。

注
必要に応じて、これよりも早くセキュリティ設定を元に戻すこともできます。この操作は、個々の機能ごとに実行することはできません。すべての機能に適用される「**トラブルシューティングを行うために、最長 4時間 Sophos Central のポリシーをオーバーライドする**」をオフにする必要があります。

リアルタイム検索

リアルタイム検索は、ユーザーが項目にアクセスしようとすると同時に検索を実行し、感染していない場合のみにアクセスを許可します。選択できるオプションは次のとおりです。

- **ファイル**: ローカルファイルに対して検索を実行するほか、ポリシーでもこの項目が選択されている場合は、ネットワーク共有に対しても検索を実行します。
- **インターネット**: インターネットのリソースに対して検索を実行します。進行中のダウンロードのスキャン、悪質な Web サイトへのアクセスのブロック、レピュテーションの低い Web サイトの検出などを行うことができます。

ユーザーの制御

- **周辺機器コントロール**: 周辺機器やリムーバブルメディアへのアクセスを制御することができます。
- **アプリケーション コントロール**: セキュリティ脅威ではないものの業務での使用は不適切と判断されるアプリケーションを検出し、ブロックすることができます。

- **Webコントロール**: 危険なダウンロードからの防御、ユーザーが閲覧可能なサイトの制御、データ流出防止などを実行できます。

ランタイム保護

ランタイム保護は、Mac 上の疑わしい動作や、悪意のある動作・トラフィックを検出することにより、脅威から防御する機能です。選択できるオプションは次のとおりです。

- **Malicious Traffic Detection (悪質なトラフィックの検知)**: Mac と Mac を制御しようとしている兆候がみられるサーバーとの間のトラフィックを検知します。
- **ランサムウェアの検知 (CryptoGuard)**: ファイルへのアクセスを制限したうえで、アクセスの復旧と引き換えに支払いを要求するマルウェアから防御します。

6 操作方法

6.1 ファイルの検索

個別のファイルに対して検索を実行する方法は次のとおりです。

Finder でファイルを右クリックして、「**Sophos Endpoint で検索**」を選択します。

「**Finder 項目の検索**」ダイアログが表示され、検索の進行と結果を確認できます。

6.2 Mac の検索

Mac 上のすべてのファイルに対して検索を実行する方法は次のとおりです。

1. 「**ステータス**」ページまたは「**検出**」ページに移動します。
2. 「**今すぐ検索**」をクリックします。
   検索が完了すると、検索結果のサマリーが表示されます。
3. 脅威が検出された場合は、「**イベント**」ページで詳細を確認できます。

6.3 脅威のクリーンアップ

検出された脅威をクリーンアップする方法は次のとおりです。

1. 「**管理モードログイン**」をクリックしてタンパープロテクションのパスワード (Sophos Central の管理者から入手できます) を入力します。
   メニューバーの「**設定**」というリンクがアクティブになります。
2. 「**イベント**」ページを開き、検出された脅威の詳細を確認します。
3. 脅威の詳細の横にあるリンクを参照してアクションを実行します。

ここで実行できるアクションは、Sophos Central Admin コンソールで実行できるアクションと同じものです。詳細は、Sophos Central ヘルプの「**警告**」ページにある一覧を参照してください。

6.4 セキュリティ設定の変更

セキュリティ設定を変更する方法は次のとおりです。

1. 「**管理モードログイン**」をクリックしてタンパープロテクションのパスワード (Sophos Central の管理者から入手できます) を入力します。
   メニューバーの「**設定**」というリンクがアクティブになります。
2. 「**設定**」ページを開きます。
3. 「**トラブルシューティングを行うために、最長 4時間 Sophos Central のポリシーをオーバーライドする**」をオンにします。
4. ページにあるコントロールを使用して、各セキュリティ機能をオンまたはオフにします。

変更した設定は、4時間後に、集中管理されているポリシーの設定に自動的に戻ります。

注
必要に応じて、これよりも早くセキュリティ設定を元に戻すこともできます。この操作は、個々の機能ごとに実行することはできません。すべての機能に適用される「**トラブルシューティングを行うために、最長 4時間 Sophos Central のポリシーをオーバーライドする**」をオフにする必要があります。

6.5 今すぐアップデート

アップデート方法は次のとおりです。

1. 「**バージョン情報**」をクリックします。
2. 「**今すぐアップデート**」をクリックします。

6.6 トラブルシューティング

トラブルシューティングの方法は次のとおりです。

1. 「**バージョン情報**」をクリックします。
2. 「**診断ツールの起動**」をクリックして発生している問題に関するデータを収集します。

「**ユーザーフォーラム**」をクリックして詳細を確認することもできます。

6.7 Mac の暗号化

デバイス暗号化機能は、FileVault 2 テクノロジーを使用して、Mac のハードディスクを暗号化します。管理者が「**Device Encryption**」機能を有効にすると、「**Sophos Device Encryption**」ダイアログが表示されます。

1. 「**Sophos Device Encryption**」ダイアログで、ログインパスワードを入力して「**暗号化**」をクリックします。
   これにより、デバイス暗号化がオンになります。後で暗号化を開始する場合は、「**延期**」をクリックします。
2. 復旧鍵は自動的に Sophos Central に保存されます。

システムディスクが暗号化されると、内蔵のデータボリュームが自動的に暗号化されます。暗号化されたディスクは、Mac の起動時に自動でロック解除されます。なお、USB ドライブなど、リムーバブル データ ボリュームは暗号化されません。

6.8 パスワードを忘れた場合の Mac へのアクセス

ログインパスワードを忘れたため、Mac にログオンできない場合は、復旧鍵が必要になります。

Sophos Device Encryption を使用している場合、復旧鍵は Sophos Central に保存されています。復旧鍵を取得するには、次のいずれかの手順を実行します。

- Sophos Self Service Portal にログオンして、Sophos Central ヘルプにある指示に従います。
- FileVault 回復の使用 (p. 10) の説明に従って、管理者に問い合わせて復旧鍵を取得します。Sophos Self Service Portal を使用できない場合は、こちらの手順を実行してください。

6.8.1 FileVault 回復の使用

管理者に連絡して復旧キーを取得するには、次の手順を実行します。

1. Mac を再起動し、「**復旧鍵 ID**」が表示されるまで待ちます。
   「**回復キー ID**」は短時間、画面に表示されます。もう一度表示するには、Mac を再起動する必要があります。
2. 管理者に連絡して、「**復旧鍵 ID**」を提供します。
   管理者は、ユーザーの Mac 用の復旧鍵を Sophos Central で探して、ユーザーに通知します。
3. 「**パスワード**」フィールドの疑問符マークをクリックします。
   メッセージが表示されます。
4. メッセージの横の矢印をクリックして復旧鍵フィールドを表示します。
5. 復旧鍵を入力します。
6. 画面上の指示に従い、新しいパスワードを設定します。
   Active Directory からインポートしたユーザーアカウントの場合は、「**パスワードのリセット**」ダイアログで「**キャンセル**」をクリックし、管理者に問い合わせてパスワードをリセットしてもらいます。
7. メッセージが表示されたら、「**新しいキーチェーンを作成**」をクリックします。

これで、再び Mac にアクセスできるようになりました。

7 ファイルの転送がブロックされる場合

ファイルのコピーや移動、メール送信などを行うときに、ファイルの転送をブロックしたというメッセージが表示されることがあります。

このメッセージは、機密情報を意図しない宛先に送信することがないよう社内でポリシーが設定されている場合に表示されます。

メッセージには次の 2種類があります。

転送がブロックされた場合

「ファイルの転送がブロックされました」というメッセージが表示された場合、ファイルを転送することはできません。メッセージには、管理者によるアドバイスが追記されている場合もあります。

転送を許可できる場合

「ファイル転送の要求がブロックされました」というメッセージが表示された場合、ファイルを転送するかどうかを選択することができます。メッセージには、管理者によるアドバイスが追記されている場合もあります。続行しても問題がないことが明らかな場合は、「**許可**」をクリックします。

8 サポートへのお問い合わせ

テクニカルサポートは次のようなかたちで提供しています。

- ユーザー コミュニティ サイト「Sophos Community」(英語) (community.sophos.com) のご利用。さまざまな問題に関する情報を検索できます。
- ソフォス サポートデータベースのご利用。www.sophos.com/ja-jp/support.aspx

9 利用条件