SOPHOS

Cybersecurity made simple.

Sophos Endpoint for Windows

ヘルプ

目次

(2020/08/24)

1 Sophos Endpoint for Windows について

本ヘルプファイルでは、Sophos Endpoint for Windows の詳細や操作手順について説明しています。

2 Sophos Endpoint

Sophos Endpoint は、コンピュータおよびサーバーで実行されるセキュリティ対策ソリューションです。

制約事項
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。

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

ただし、次の操作はコンピュータやサーバーでも実行できます。

- コンピュータのステータスの確認。
- ファイル、コンピュータ、またはサーバーの脅威検索。
- コンピュータやサーバーで発生したイベント (例: 検出された脅威など) の詳細を表示。
- 脅威のクリーンアップ。
- セキュリティ設定の変更。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。
- アップデート。
- トラブルシューティング。

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、「**管理モードサインイン**」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。

関連概念

ステータス (p. 3)
セキュリティ状態を確認したり、コンピュータやサーバーを検索したりできます。

イベント (p. 5)
「**イベント**」ページには、検出された脅威など、コンピュータやサーバーで発生したイベントが表示されます。

関連タスク

ファイルの検索 (p. 9)
個々のファイルを検索できます。

コンピュータやサーバーの検索 (p. 9)
ここにある手順に従って、コンピュータやサーバーを検索できます。

脅威のクリーンアップ (p. 9)
ここにある手順に従って、検出された脅威をクリーンアップできます。

セキュリティ設定の変更 (p. 9)
ここにある手順に従って、セキュリティ設定を変更できます。

今すぐアップデート (p. 10)
ここにある手順に従って、ウイルス定義をアップデートできます。

トラブルシューティング (p. 10)
問題のトラブルシューティングを行うには、次の手順に従います。

3 ステータス

セキュリティ状態を確認したり、コンピュータやサーバーを検索したりできます。

制約事項
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。

- コンピュータやサーバーのセキュリティステータスを表示する。
- コンピュータやサーバー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
画面右下の「**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。

設定	説明
 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。
 赤色:	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。

コンピュータの検索

コンピュータやサーバー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、「**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。

4 イベント

「**イベント**」ページには、検出された脅威など、コンピュータやサーバーで発生したイベントが表示されます。

制約事項
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

リストには次の項目が表示されます。

- 重要度。リストの一番左側に表示されるアイコン。イベントの重要度 (高、中、通知) を示します。
- 発生元。リストの左側に表示されるアイコン。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。

各イベントの詳細を表示するには、右側にある矢印をクリックして展開します。

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

イベントは、次の種類で絞り込み表示できます。

イベントの種類	説明
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。

イベントの種類	説明
Web 脅威	Web 脅威とは、悪意のある Web サイト、未分類の Web サイト、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。これらのサイトはブロックすることができます。
悪意のある動作	悪意のある動作とは、コンピュータやサーバーで実行中のソフトウェアで検知される不審な振る舞いを指します。 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。
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、コンピュータやサーバー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。
エクスプロイト	ソフォス製品で防御できるエクスプロイトには、アプリケーションハイジャックをはじめ、ブラウザやブラウザ用プラグイン、Java アプリケーション、メディアアプリケーション、Microsoft Office アプリケーションなどに存在する脆弱性を突くエクスプロイトがあります。

5 設定

ここでは、ローカルコンピュータやサーバー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、コンピュータ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。

制約事項
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。

制約事項
「**設定**」ページは、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。

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**」チェックボックスにチェックを入れます。

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 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。

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。元に戻すには、各機能のスイッチを切り替えるのではなく、「**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**」をオフにします。

ディープラーニング

ディープラーニングは高度な機械学習を利用して脅威を検出します。この機能では、シグネチャを使用することなく、マルウェアや不要と思われるアプリケーションを検出することができます。

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します。
- **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するアプリケーションを検出し、ブロックします。
- **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。
- **データ流出防止**: 機密データを含むファイルの転送を監視・制御します。
- **タンパープロテクション**: 設定の変更を制限します。これがオンになっていると、ローカル管理者がセキュリティ設定を変更したり、Sophos Endpoint をアンインストールしたりするには、該当するパスワードが必要になります。

ランタイム保護

ランタイム保護は、エンドポイント上の不審な動作や、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。

- **ランサムウェアの検知**: 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。
- **セーフブラウジング**: マルウェアによる Web ブラウザの悪用を防止します。
- **エクスプロイト防止**: Java アプリケーションなど、最もマルウェアに悪用されやすいアプリケーションを保護します。
- **ネットワーク脅威対策**: エンドポイントコンピュータとエンドポイントコンピュータ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。この機能にはパケットインスペクションも含まれ、ネットワーク通信をスキャンして、OS またはアプリケーションに影響を与える前に脅威を検出してブロックします。

  注
  ネットワーク脅威対策をオフにすると、EDR、隔離、および感染拡大防止の各機能もオフになります。

- **悪意のある動作の検知**: 悪意のあることが確認されている動作や疑わしい動作を検知し、ブロックします。

コンピュータの制御

コンピュータやサーバーにある Windows ファイアウォール (および他の登録済みファイアウォール) を監視できます。

6 操作方法

6.1 ファイルの検索

個々のファイルを検索できます。

ファイルを検索するには、次の手順を実行します。

- エクスプローラで、ファイルを右クリックして「**検索**」を選択します。

6.2 コンピュータやサーバーの検索

ここにある手順に従って、コンピュータやサーバーを検索できます。

コンピュータやサーバー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. 「**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

ここにある手順に従って、検出された脅威をクリーンアップできます。

脅威のクリーンアップを行うには、次の手順を実行します。

1. 「**管理モードサインイン**」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。
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 で実行できるアクションと同じものです。詳細は、Sophos Central Admin 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

ここにある手順に従って、セキュリティ設定を変更できます。

セキュリティ設定を変更する方法は次のとおりです。

1. 画面右上の「**管理モードサインイン**」をクリックします。
2. 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。
   メニューバーに「**設定**」というリンクが表示されます。
3. 「**設定**」ページを開きます。
4. 「**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**」チェックボックスにチェックを入れます。

5. 各セキュリティ機能のスイッチを切り替え、機能を無効化します。

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。元に戻すには、各機能のスイッチを切り替えるのではなく、「**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**」チェックボックスのチェックを外します。

6.5 今すぐアップデート

ここにある手順に従って、ウイルス定義をアップデートできます。

アップデートするには、次の手順を実行します。

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

問題のトラブルシューティングを行うには、次の手順に従います。

問題のトラブルシューティングを行うには、次の手順を実行します。

1. 「**バージョン情報**」をクリックします。
2. 「**Endpoint Self Help ツールを開く**」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。または「**ユーザーフォーラム**」というリンクをクリックします。

6.7 コンピュータの暗号化

ここにある手順に従って、コンピュータを暗号化できます。

制約事項
デバイス暗号化は、エンドポイントコンピュータのみで実行できます。

デバイス暗号化は、Windows BitLocker テクノロジーを使用して、コンピュータのハードディスクを暗号化します。コンピュータにアクセスするたびに認証が必要かどうかは、管理者が指定します。

認証が不要な場合は、Sophos Central ポリシーの適用後、コンピュータを再起動すると、ただちにハードディスクの暗号化が自動的に開始されます。この場合、操作は何も必要ありません。

認証が必要な場合は、次の手順を実行します。

1. 「**Sophos Device Encryption**」ダイアログが表示されたら、画面の指示に従います。表示される指示は、使用しているシステムや、管理者が定義したポリシーによって異なります。
   - PIN やパスワードを使用した認証がデバイス暗号化ポリシーで設定されている場合は、画面の指示に従って PIN やパスワードを作成します。

注
PIN やパスワードを作成する際は注意が必要です。プリブート環境は、「EN-US」キーボードのみに対応しています。記号を含む PIN やパスワードを作成した場合は、サインインする際に、キーボード上の実際の配置と異なるキーを押さなくてはならないことがあります。

- USB キーを使用した認証がデバイス暗号化ポリシーで設定されている場合は、コンピュータに USB メモリを接続する必要があります。NTFS、FAT、または FAT32 でフォーマットされている USB メモリを使用する必要があります。

2. 「**再起動＆暗号化**」をクリックすると、コンピュータが再起動し、ハードディスクの暗号化が開始されます。暗号化中も、通常通りコンピュータを使用できます。

注
「**後で作成**」を選択して、ダイアログを閉じることができます。次回サインインすると、再びダイアログが表示されます。

Sophos Central によるシステムボリュームの暗号化が完了すると、データボリュームの暗号化が開始されます。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。

以後、コンピュータにサインインする際、システムボリュームのロックを解除するために、PIN、パスワード、または USB キーが必要になる場合があります。データボリュームは、自動的に復号化されます。

6.8 パスワードを忘れた場合のコンピュータへのアクセス

ここにある手順に従って、コンピュータへのアクセスを復旧できます。

PIN、パスワード、または USB キーを忘れたため、コンピュータ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 にサインインして、ヘルプにある指示に従います。
- 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。

関連タスク
BitLocker 回復の使用 (p. 11)
ここにある手順に従って、コンピュータを復旧できます。

6.8.1 BitLocker 回復の使用

ここにある手順に従って、コンピュータを復旧できます。

コンピュータを復旧するには、次の手順を実行します。

1. コンピュータを再起動して、「**BitLocker**」のログオン画面で「Esc」キーを押します。
2. 「**BitLocker 回復**」画面で、「**回復キー ID**」を参照します。

「**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、コンピュータを再起動する必要があります。

3. 管理者に「**復旧鍵 ID**」を提供します。
   管理者は、ユーザーのコンピュータ用の復旧鍵を Sophos Central で探して、ユーザーに通知します。
4. ユーザーは、「**BitLocker 回復**」画面で復旧鍵を入力します。
   次にコンピュータを起動します。
5. 画面上の指示に従い、新しい BitLocker PIN やパスワードを作成します。

   Windows 7 コンピュータでは、何も指示は表示されません。PIN/パスワードを手動でリセットする必要があります。

これで、コンピュータにアクセスできるようになりました。

注
復旧鍵は一度のみ使用できます。後でもう一度コンピュータの復旧が必要になった場合は、新しい復旧鍵を取得する必要があります。

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。

メッセージ	説明
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

ソフォス製品のテクニカルサポートは、次のような形でご提供しております。

- 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
- 製品ドキュメントのダウンロード。www.sophos.com/ja-jp/support/documentation.aspx
- オンラインでのお問い合わせ。https://secure2.sophos.com/ja-jp/support/open-a-support-case.aspx

9 利用条件