SOPHOS

SOPHOS CENTRAL DEVICE ENCRYPTION – 技術概要

ソフォス ホワイトペーパー 2020年 7月

目次

概要

このドキュメントでは、Sophos Central Device Encryption の技術概念 (暗号化プロセス、使用されるプロテクター、鍵の処理方法など) の概要について説明します。暗号化プロセスは、Windows (BitLocker) デバイスと macOS (FileVault) デバイスで異なります。このドキュメントは、Sophos.com にある Central Device Encryption 管理者ガイドを置き換えるものではありません。

Windows

Windows デバイスを暗号化するには、Sophos Central Device Encryption エージェントをコンピュータにインストールし、Sophos Central で暗号化ポリシーを適用する必要があります。デバイスはこのポリシーを受信し、暗号化プロセスを開始します。

暗号化プロセス - Windows

1. デバイスは Sophos Central から暗号化ポリシーを受信します。ポリシーには、デバイス暗号化を有効にする設定が含まれています。

   注: ドライブが BitLocker を使用できる状態になっていない場合、またはマシンの TPM が有効化されていない場合、ユーザーは必要な操作を実行して再起動するように求められます。ほとんどの最新システムでは、この手順は必要ありません。

2. デバイスの復旧鍵が作成されます。これは、一意の ID と 48桁のパスワードで構成されます。

   注: ユーザーの PIN、パスワード、または暗号化鍵が Sophos Central に送信されることはありません。復旧鍵のみが保存されます。

3. 復旧鍵は難読化され、SSL 経由で Sophos Central に安全に送信されます。Sophos Central は、受信した復旧鍵を暗号化し、キーマネージャ仮想アプライアンスに安全に保存します。Sophos Central は、鍵が正常に受信され保存されたことを確認するメッセージをデバイスに送信します。

4. 鍵が保存されたことを確認するメッセージを Sophos Central から受信すると、次にデバイスはログインプロテクターのインストールを実行します。ログインプロテクターには、TPM+PIN、TPM のみ、パスフレーズ、USB キーの 4種類がありますが、そのうちの 1つのみがインストールされます。インストールされるプロテクターは、使用しているソフトウェアとハードウェアの組み合わせによって異なります。詳細は、「BitLocker プロテクター」を参照してください。

5. ログインプロテクターが正常にインストールされると、ユーザーはデバイスを再起動するように求められます。デバイスのバックアップが開始されると、ユーザーは、新しい BitLocker PIN / パスワードを入力するか、USB キーを接続するように求められます (使用しているプロテクターによって異なります)。

   注: 「TPM のみ」を使用した認証方式を使用する場合、ユーザーは PIN / パスワードの入力を求められません。

6. プリブート環境での認証に成功し、Windows にログインすると、ディスク暗号化プロセスが開始されます。ユーザーは、「コントロールパネル - システムとセキュリティ - BitLocker ドライブ暗号化」の順に選択して、暗号化プロセスの状態を確認できます。デバイスはその暗号化状態を Sophos Central に報告し、デバイスは Sophos Central 管理コンソールに表示されます。

BitLocker プロテクター

BitLocker には、別の方法で、暗号化されたデバイスやボリュームにアクセスまたは「ロック解除」する、「プロテクター」という概念があります。

ログインプロテクター

Central Device Encryption は、デバイスの起動プロセスの一環として、以下のプロテクターを利用します。

- TPM + PIN
- TPM のみ
- パスフレーズ
- USB キー

Central Device Encryption では、各デバイスでこれらの方式のいずれか 1つのみが有効になります。使用されるプロテクターは、デバイスハードウェアとソフトウェアの組み合わせに基づいています。詳細は、Central Device Encryption 管理者ガイドを参照してください。

TPM + PIN

このプロテクターは、Trusted Platform Module (TPM) と PIN を使用して認証を行います。ユーザーは、コンピュータを起動するたびに、プリブート環境でこの PIN を入力する必要があります。

TPM のみ

「TPM のみ」プロテクターでは、PIN を使用した認証は必要とせず、TPM チップが使用されます。ユーザーは、プリブート環境で何も入力する必要はありません。

注: Central Device Encryption の「起動時に認証する」ポリシーオプションが有効になっている場合、「TPM のみ」のプロテクターは使用されません。

パスフレーズ

パスフレーズプロテクターは、パスフレーズのみを認証として使用し、TPM が搭載されていないマシンに適しています。ユーザーは、コンピュータを起動するたびに、プリブート環境でパスフレーズを入力する必要があります。パスフレーズプロテクターには Windows 8 以降が必要です。

USB キー

USB プロテクターには、USB デバイスに保存された鍵が必要です。この場合、起動するたびに USB キーをデバイスに接続する必要があります。

注: USB プロテクターは、Windows 7 コンピュータにある Central Device Encryption のみで使用されます。

その他のプロテクター

Sophos Central Device Encryption は、次の BitLocker プロテクターも活用します。

復旧鍵

コンピュータで暗号化を開始する前に、Windows によって復旧鍵が作成されます。復旧鍵は、一意の ID と 48桁のパスワードで構成されます。復旧鍵は Sophos Central に安全に保存され、BitLocker の PIN やパスワードを忘れたユーザーが、自分のマシンにログインし直すことができるようにします。管理者は、BitLocker プリブート認証ページに入力するための 48桁のパスワードをユーザーに付与します。

Sophos Central に復旧鍵のパスワードが表示されると、公開されたため、鍵は期限切れと見なされます。次にデバイスが Sophos Central と同期すると、デバイスは、鍵の有効期限が切れたことを検出し、新しいキーを生成して、新しい復旧鍵を Sophos Central に送信します。したがって、次回のログインが成功した後、元の復旧鍵は無効になります。

注: Sophos Central では、古い復旧鍵は削除されません。その後更新された復旧鍵は、ボリューム ID で検索することによって検出できます。

自動ロック解除
すべての固定データボリュームには、自動ロック解除プロテクターがインストールされます。したがって、ユーザーがデバイスにログオン後、追加のユーザー操作なしでデータボリューム (つまり、OS のボリュームではない) にアクセスできます。

注: Central Device Encryption の「ブートボリュームのみを暗号化する」ポリシー設定が有効になっている場合、固定データボリュームは暗号化されません。

注: リムーバブル データ ボリューム (例: USB キー) は、Central Device Encryption によって暗号化されません。

macOS

macOS デバイスを暗号化するには、Sophos Central Device Encryption エージェントをコンピュータにインストールし、Sophos Central で暗号化ポリシーを適用する必要があります。デバイスはこのポリシーを受信し、暗号化プロセスを開始します。

暗号化プロセス - macOS

1. デバイスは Sophos Central から暗号化ポリシーを受信します。ポリシーには、デバイス暗号化を有効にする設定が含まれています。
2. ユーザーは、デバイスで暗号化を開始するか、後で開始するように求められます。

   注: ディスク暗号化が開始されるまで、FileVault 復旧鍵を Sophos Central に送信することはできません。Sophos Central に復旧鍵を送信できるように、暗号化の実行中にデバイスがインターネットに接続されていることを確認してください。
3. 暗号化はバックグラウンドで実行され、完了するとユーザーに通知が送信されます。デバイス復旧鍵は難読化され、SSL 経由で Sophos Central に安全に送信されます。Sophos Central は、受信した復旧鍵を暗号化し、キーマネージャ仮想アプライアンスに安全に保存します。

   注: ユーザーのパスワードが Sophos Central に送信されることはありません。復旧鍵のみが保存されます。

鍵の保管

Sophos Central は、ユーザーが PIN やパスワードを忘れたり、自身をロックアウトしてしまった場合に対処するために、デバイス復旧鍵を保存します。暗号化プロセスの一環として、デバイスは新しい復旧鍵を生成し、SSL 経由で Sophos Central に送信します。復旧鍵は、仮想キーマネージャに安全に保存されます。

Sophos Central が、ユーザーの実際のプリブート PIN やパスワードの詳細を収集することはなく、復旧鍵のみが保存されることにご注意ください。

復旧プロセス

復旧プロセスによって、ログオン認証情報を忘れた場合でも、ユーザーは自分のマシンに再びアクセスできるようになります。復旧は、管理者の支援を受けて行うか、またはユーザー向けの Sophos Self Service Portal を使用して行うことができます。

管理者の支援による復旧

管理者は、Sophos Central Admin コンソールで、特定のデバイスの復旧鍵を見つけることができます。復旧鍵を見つけるには、次の 2つの方法があります。

1. **直接 Sophos Central コンソールから復旧鍵を取得する。**
   これは、管理者がユーザー名またはコンピュータ名を把握している場合に便利です。Sophos Central の「デバイス」または「コンピュータ」ページで、該当するマシンを見つけて、「デバイス暗号化」セクションに移動します。「復旧鍵の取得」をクリックして復旧鍵を表示します。復旧鍵は 48桁のパスワードで、デバイスへのアクセスを復旧するために、ユーザーが BitLocker プリブート環境で入力するものです。

2. **復旧鍵 ID やボリューム ID を使用して復旧鍵を検索する。**
   この方法は、特定の復旧鍵を手動で検索する際に便利です。復旧鍵 ID は、ユーザーに対してプリブート認証画面に表示され、管理者は、これを使用して検索することで、関連付けられた復旧パスワードを見つけることができます。ボリューム ID による検索は、管理者がディスクの詳細のリストを持っていて、復旧パスワードを見つける必要がある場合などにも便利です。Sophos Central で復旧鍵が削除されることはないため、後日更新された可能性のある復旧鍵は、手動検索で見つけることができます。

注：管理者が復旧鍵を表示したことによって、クライアントデバイスは、新たに復旧鍵を作成して Sophos Central と共有するように指示されます。コンピュータがオフラインの場合は、オンラインに復帰したときに新しい復旧鍵が生成されます。

ユーザーの操作による復旧

Sophos Central Self Service Portal (https://www.sophos.com/ssp) を使用すると、ユーザーは IT 管理者やヘルプデスクに連絡しなくても復旧鍵を取得できます。 Sophos Central のユーザーに対して、Self Service Portal へのアクセスを設定する必要があります。詳細は、Sophos Central ヘルプを参照してください。

Sophos Central Self Service Portal にログイン後、「デバイス暗号化」タブにユーザーのデバイスが一覧表示されます。復旧鍵を取得するには、「復旧鍵」カラムで「取得」ボタンをクリックします。

安全なファイル共有

安全なファイル共有機能を使用すると、ユーザーは、サイズが最大 50MB のファイルを暗号化して、同僚や外部の受信者と共有できます。ユーザーはファイルを暗号化する際にパスワードを指定する必要があり、受信者はファイルアクセスのために、このパスワードが必要になります。ファイルは、256 ビット AES 暗号化を使用して暗号化されます。

注：現在、安全なファイル共有は Windows のみで利用できます。

ソフォス株式会社
営業部
Email: sales@sophos.co.jp

200712 WPEN (NP)