SOPHOS

Cybersecurity made simple.

Sophos Central Device Encryption

管理者ガイド

目次

1 Sophos Central Device Encryption について

Sophos Central Device Encryption では、Windows エンドポイントに搭載されている BitLocker ドライブ暗号化や、Mac エンドポイントに搭載されている FileVault を Sophos Central から一元管理できます。

ハードディスクの暗号化により、デバイスの盗難・紛失時にもデータを安全に保ちます。

このガイドは、Sophos Central Device Encryption の設定方法や使用方法について説明します。また、セルフサービスポータルを使用して復旧鍵を取得する方法についても説明します。ポリシー設定や警告、および Sophos Central を使用した復旧に関する詳細は、Sophos Central ヘルプを参照してください。

関連情報

Sophos Central ヘルプ

2 BitLocker ドライブ暗号化の管理

このセクションでは、社内ネットワークに接続している Windows エンドポイントの BitLocker ドライブ暗号化を使用するための前提条件や、利用可能な認証方式、該当するポリシーでの認証の設定について説明します。

2.1 Sophos Central Device Encryption への移行

このセクションでは、SafeGuard Enterprise と BitLocker デバイス暗号化、あるいは SafeGuard Enterprise と Sophos Full Disk Encryption を使用して暗号化している環境を Sophos Central Device Encryption に移行する方法について説明します。

対象は以下のとおりです。

- SafeGuard Enterprise と BitLocker を使用している場合
- SafeGuard Enterprise と Sophos Full Disk Encryption を使用している場合
- Mac エンドポイントの移行について詳細は、Sophos Central Device Encryption (Mac) への移行を参照してください。

関連タスク

Sophos Central Device Encryption (Mac) への移行 (p. 14)
Sophos Central を使用して、FileVault で暗号化済みの Mac エンドポイントを管理する場合は、Sophos Central Device Encryption のポリシーをこれらのエンドポイントに適用する必要があります。

2.1.1 SafeGuard Enterprise BitLocker Client からの移行

移行する手順は、次のとおりです。

注

SafeGuard Enterprise バージョン 6.x または 7.x で BitLocker を管理している場合は、まずは最新バージョンの SafeGuard Enterprise にアップグレードすることを推奨します。

SafeGuard Enterprise バージョン 6.x または 7.x を使用している場合は、必ず「SafeGuard Enterprise 管理者ヘルプ」に記載されている手順に従ってシステムディスクを復号化してから、Sophos Central Device Encryption に移行してください。

SafeGuard Enterprise BitLocker Client (バージョン 8.0 以降) から Sophos Central Device Encryption に移行する方法は次のとおりです。

1. 「**コントロールパネル > プログラムのアンインストール**」を開き、「**Sophos SafeGuard Client**」を右クリックします。
2. 右クリックメニューから「**変更**」を選択します。
   Sophos SafeGuard Client Setup ウィザードが開きます。
3. 「BitLocker」というコンポーネントをアンインストールします。

注
「BitLocker」コンポーネントを削除してもボリュームやファイルは復号化されません。

4. Sophos Central Device Encryption のソフトウェアをインストールします。
5. Sophos Central Device Encryption のポリシーがエンドポイントに適用されており、有効になっていることを確認します。

これで、Sophos Central を使用して BitLocker を管理する準備ができました。データを暗号化しなおす必要はありません。Sophos Central Device Encryption のポリシーをエンドポイントに適用すると、復旧鍵が更新され、Sophos Central に送信されます。ファイル暗号化機能に変更はありません。

関連情報
SafeGuard Enterprise 管理者ヘルプ

2.1.2 SafeGuard Enterprise Full Disk Encryption からの移行

移行する手順は、次のとおりです。

SafeGuard Enterprise Full Disk Encryption から移行する方法は次のとおりです。

1. Sophos SafeGuard Client ソフトウェアをアンインストールします。
   暗号化済みのボリュームは、自動的に復号化されます。暗号化済みのファイルは復号化されません。
2. Sophos Central Device Encryption のソフトウェアをインストールします。
3. Sophos Central Device Encryption のポリシーがエンドポイントに適用されており、有効になっていることを確認します。
4. 必要な SafeGuard Enterprise File Encryption モジュール (Synchronized Encryption または Location Based File Encryption) を再インストールします。

これで、Sophos Central を使用して BitLocker を管理する準備ができました。Sophos Central Device Encryption のポリシーをエンドポイントに適用すると、暗号化がバックグラウンドで開始し、復旧鍵が更新され、Sophos Central に送信されます。

2.2 デバイス暗号化の準備

デフォルトでは、ほとんどのシステムドライブは、BitLocker で暗号化できる状態になっています。ドライブの準備ができていない場合は、Sophos Central Device Encryption で、準備に必要なマイクロソフトのコマンドラインツール (BdeHdCfg.exe) が自動的に実行され、ドライブの準備が行われます。

この処理では、システムドライブに BitLocker 専用のパーティションが作成されます。

Sophos Central Device Encryption のセットアップ中に、システムドライブを準備するために再起動が必要であるというメッセージが表示されます。ユーザーは、コンピュータをただちに再起動するか、または後で再起動するかを選択できます。デバイス暗号化は、コンピュータを再起動してシステムドライブの準備が完了している場合のみに実行されます。

デバイス暗号化で必要な .NET Framework バージョンは、エンドポイントに自動的にインストールされます。

2.3 デバイス暗号化の操作手順

デバイスを暗号化する手順は、次のとおりです。

ユーザーが操作を開始する前に、次の事柄を確認します。

- Sophos Central のエージェントソフトウェアがエンドポイントにインストール済みである。
- Sophos Central でデバイス暗号化ポリシーが設定されており、かつ有効になっている。
- ユーザーはエンドポイントに直接ログインして Sophos Central に接続・同期する。リモートログインはサポートされません。
- OS で BitLocker ドライブ暗号化がサポートされている。詳細は、デバイス暗号化の準備およびデバイス暗号化のシステム互換性を参照してください。

エンドポイントに表示されるメッセージと必要な操作は次のとおりです。

1. TPM セキュリティハードウェアがまだ有効化されていない場合、BIOS のセットアップ画面で有効にすることができます。再起動が必要になります。ユーザーは、ただちに再起動するか、または後で再起動するかを選択できます。
   再起動後、TPM の有効化を促す画面が表示されます。TPM を有効化できない場合や、ユーザーが応答しない場合はメッセージが表示されます。
2. TPM がアクティブで有効化されているが、所有者が指定されていない場合、Sophos Central のエージェントソフトウェアによって、TPM の所有者情報が自動的に生成・適用されます。これに失敗すると Sophos Central に警告が送信されます。
3. TPM のエンドースメント鍵がない場合は、Sophos Central のエージェントソフトウェアによって自動的に作成されます。これに失敗すると Sophos Central に警告が送信されます。
4. デバイス暗号化ポリシーで「**起動時に認証が必要**」が指定されなかった場合、ハードディスクの暗号化は自動的に開始されます。この場合、ユーザーによる操作は何も必要ありません。ステップ 8 に進んでください。
5. デバイス暗号化ポリシーで「**起動時に認証が必要**」が指定されている場合、ユーザーに対して「**Sophos Device Encryption**」ダイアログが表示されます。
   - 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、ユーザーは画面の指示に従って PIN やパスワードを定義する必要があります。TPM + PIN を使用すると、システムディスクの暗号鍵は TPM に保存されます。

     注
     パスワードを設定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 やパスワードを設定した場合、ユーザーはログインする際に、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、ユーザーは、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。
6. ユーザーが「**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、デバイス暗号化が動作するかどうかが検証されます。
   ユーザーは「**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。ただし、ユーザーが再ログオンしたり、管理者がデバイス暗号化ポリシーを変更したりすると、再び表示されます。
7. 正しい PIN やパスワードを入力できない場合、ユーザーは「Esc」キーを押すことができます。この段階では、暗号化が適用されていないため、システムは通常どおりに起動します。ログオン後、PIN やパスワードの入力が再び促されます。

8. 管理者は、暗号化の有効化が済んでいないユーザーを確認できます。これは、ユーザーがコンピュータを再起動していない、または画面に表示される操作を完了していないことを意味します。Sophos Central の「**レポート**」を参照してください。
9. プリブートの検証に成功すると、Sophos Central のエージェントソフトウェアによって、ハードディスクの暗号化が開始されます。暗号化はバックグラウンドで実行されるため、ユーザーは通常どおり作業を進めることができます。
   ハードウェアの検証に失敗すると、システムは再起動しますが、暗号化は実行されません。Sophos Central にイベントが送信され、管理者への通知が行われます。
10. Sophos Central のエージェントがシステムボリュームを暗号化した後、データボリュームの暗号化が開始します (ポリシーで指定されている場合)。データボリュームの保護機能はシステムボリュームに保存されているため、システムの起動後、データボリュームは自動的に使用できるようになります。したがって、ユーザーは、コンピュータにログオンすると、追加の操作なしでデータボリュームにアクセスできます。USB メモリなど、リムーバブル データ ボリュームは暗号化されません。

エンドポイントの %ProgramData%¥Sophos¥Sophos Data Protection¥Logs に、CDE.log および CDE_trace.xml というログファイルが出力されます。

関連概念

デバイス暗号化の準備 (p. 3)
デフォルトでは、ほとんどのシステムドライブは、BitLocker で暗号化できる状態になっています。ドライブの準備ができていない場合は、Sophos Central Device Encryption で、準備に必要なマイクロソフトのコマンドラインツール (BdeHdCfg.exe) が自動的に実行され、ドライブの準備が行われます。

デバイス暗号化のシステム互換性 (p. 5)
各 OS でサポートされる保護機能の種類は、以下の一覧を参照してください。利用できる保護機能は、Windows のバージョンや TPM セキュリティチップが搭載されているかどうかによって異なります。

TPM + PIN (p. 7)
「TPM + PIN」モードでは、コンピュータの TPM セキュリティハードウェアと PIN が認証に使用されます。

2.4 デバイス暗号化のシステム互換性

各 OS でサポートされる保護機能の種類は、以下の一覧を参照してください。利用できる保護機能は、Windows のバージョンや TPM セキュリティチップが搭載されているかどうかによって異なります。

括弧内の番号は、各保護機能の優先順位を示します。

(*) 「**起動時に認証が必要**」が有効化されている場合、「TPM のみ」の保護をインストールできないため、「TPM + PIN」が最優先されます。

	Win 7 TPM なし	Win 7 TPM あり	Win 8.1 TPM なし	Win 8.1 TPM あり	Win 10 TPM なし	Win 10 TPM あり
TPM のみ	-	OK (1*)	-	OK (1*)	-	OK (1*)
TPM + PIN	-	OK (2)	-	OK (2)	-	OK (2)
パスフレーズ	-	-	OK (1)	OK (3)	OK (1)	OK (3)

	Win 7 TPM なし	Win 7 TPM あり	Win 8.1 TPM なし	Win 8.1 TPM あり	Win 10 TPM なし	Win 10 TPM あり
USB キー	OK (1)	OK (3)	-	-	-	-

Central Device Encryption を使用している場合、エンドポイントコンピュータで TPM の設定が必要になる場合があります。

TPM 2.0 以降を使用している場合は、ハードドライブを GPT 形式でフォーマットし、BIOS を UEFI モードに設定する必要があります。

TPM 1.2 を使用している場合は、BIOS/UEFI で TPM を有効にし、使用する準備ができている必要があります。これは、TPM.msc を使用して確認できます。

Central Device Encryption をインストールする前に、エンドポイントコンピュータを最新の BIOS/UEFI バージョンにアップデートすることを推奨します。

Windows で FIPS モードが有効になっている場合、BitLocker 暗号化は、Windows 8.1 または Windows 10 のみでサポートされます。Windows 7 の FIPS モードで BitLocker を使用する方法の詳細は、Windows 7 または Windows Server 2008 R2 での BitLocker の FIPS 準拠の回復パスワードを AD DS に保存できませんを参照してください。

暗号化されたハードドライブは、Sophos Central Device Encryption とともに使用できます。詳細は、暗号化されたハードドライブを参照してください。

Sophos Central Device Encryption は、事前プロビジョニングされた BitLocker に対応しています。

関連情報

Windows 7 または Windows Server 2008 R2 での BitLocker の FIPS 準拠の回復パスワードを AD DS に保存できません
暗号化されたハードドライブ

2.5 デバイス暗号化の認証モード

デバイス暗号化の設定画面にある「**起動時に認証が必要**」スイッチを使用して、ユーザーがコンピュータにログオンする際に認証を要求するかどうかを制御できます。

コンピュータにインストールされている認証モードは、システム、BitLocker グループポリシーの設定、および設定済みのデバイス暗号化ポリシーに依存します。デバイス暗号化のシステム互換性に応じて、次のいずれか 1つの認証モードがエンドポイントにインストールされます。

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

既に BitLocker で暗号化されているエンドポイントの場合、必要な手順に関するメッセージがユーザーに表示されます。

「**起動時に認証が必要**」を有効にすると、ユーザーは、PIN/パスフレーズ/USB メモリを定義し、「**適用**」をクリックするよう促されます。ユーザーは今後、コンピュータを起動するたびに、この PIN/パスフレーズ/USB メモリを入力する必要があります。「**起動時に認証が必要**」を無効にすると、「TPM のみ」モードが自動的に適用され、他の認証操作は不要になります。コンピュータの起動時にデバイスのロックが自動的に解除されることが、ユーザーに通知されます。

Sophos Device Encryption では、該当するオプションが「**未構成**」に設定されている場合、すべての認証モードが許可されるように、GPO (グループ ポリシー オブジェクト) を自動設定できます。なお、管理者によって手動で設定された値は、Sophos Device Encryption によって上書きされません。詳細は、BitLocker グループポリシーの設定を参照してください。

ユーザーは、認証モードのインストールを延期できます。この場合、暗号化は実行されません。ユーザーが Windows に再度ログインしたり、新しい暗号化ポリシーが適用されたりするたびに、ユーザーは、コンピュータの再起動を促されます。再起動すると、認証モードがインストールされ、デバイス暗号化が開始されます。今後、ユーザーは自分のデバイスを復号化できなくなります。

関連概念

デバイス暗号化のシステム互換性 (p. 5)
各 OS でサポートされる保護機能の種類は、以下の一覧を参照してください。利用できる保護機能は、Windows のバージョンや TPM セキュリティチップが搭載されているかどうかによって異なります。

BitLocker グループポリシーの設定 (p. 9)
Sophos Central では、一部のグループポリシー設定が自動設定されるため、管理者はデバイス暗号化のためにコンピュータを事前準備する必要はありません。

2.5.1 TPM + PIN

「TPM + PIN」モードでは、コンピュータの TPM セキュリティハードウェアと PIN が認証に使用されます。

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 + PIN」モードには準備済みの TPM が必要で、システムの GPO 設定で「TPM + PIN」モードが許可されている必要があります。

すべての条件が満たされると、「TPM + PIN」の設定ダイアログが表示され、PIN の設定が促されます。ユーザーは「**再起動＆暗号化**」をクリックして、ただちにコンピュータを再起動し、暗号化を開始できます。

GPO の設定「**スタートアップの拡張 PIN を許可する**」が有効化されている場合、数字、英字、および記号を含む PIN を指定することができます。有効化されていない場合は、数字のみを使用できます。

BitLocker 用の PIN の長さは、4～20文字の範囲で指定できます。PIN の最低限の長さは、グループポリシーで 5文字以上に指定することができます。Sophos Central のエージェントソフトウェアにより、拡張 PIN を許可するようグループポリシーが設定されます。ダイアログに、入力できる文字の種類や、許可されている最小・最大の長さが表示されます。

注
1台の Windows コンピュータを複数のユーザーで使用している場合は、全員が同じ PIN を使用してシステムディスクをロック解除する必要があります。ロック解除後、各ユーザーの資格情報で OS にログオンします。Windows コンピュータは、シングル サインオンに対応していません。

2.5.2 パスフレーズ

TPM セキュリティハードウェアのないエンドポイントでは、パスフレーズを使って認証することができます。

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パスフレーズを入力する必要があります。

パスフレーズを使用した認証は、Windows 8.0 以降の環境で可能で、システムの GPO 設定で「パスフレーズ」モードが許可されている必要があります。

すべての条件が満たされると、「パスフレーズ」の設定ダイアログが表示され、8～100文字のパスフレーズの設定が促されます。ユーザーは「**再起動＆暗号化**」をクリックして、ただちにコンピュータを再起動し、暗号化を開始できます。

2.5.3 TPM のみ

「TPM のみ」モードでは、PIN コード認証なしで、コンピュータの TPM セキュリティハードウェアが認証に使用されます。

このため、ユーザーは、Windows のプリブート環境で PIN を入力することなく、コンピュータを起動できます。

「TPM のみ」モードには、準備済みの TPM が必要なほか、デバイス暗号化ポリシーの設定で「**起動時に認証が必要**」を無効に設定する必要があります。さらに、システムの GPO 設定で「TPM のみ」モードが許可されている必要があります。

すべての条件が満たされると、「TPM のみ」の保護インストールダイアログが表示されます。ユーザーは「**再起動＆暗号化**」をクリックして、ただちにコンピュータを再起動し、暗号化を開始できます。

2.5.4 USB キー

「USB キー」モードでは、USB メモリに保存されているキーが認証に使用されます。

コンピュータを起動する際は、USB メモリを挿入する必要があります。

USB キーを使用した保護は、TPM がない場合や GPO によって TPM が無効化されている場合に、Windows 7 環境のエンドポイントで使用できます。

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。exFAT 形式には対応していません。さらに、USB メモリは書き込み可能である必要があります。

すべての条件が満たされると、「USB キー」の保護インストールダイアログが表示され、キーの保存先として、接続した USB メモリの選択が促されます。

ユーザーは「**再起動＆暗号化**」をクリックして、ただちにコンピュータを再起動し、暗号化を開始できます。

2.6 BitLocker グループポリシーの設定

Sophos Central では、一部のグループポリシー設定が自動設定されるため、管理者はデバイス暗号化のためにコンピュータを事前準備する必要はありません。

なお、管理者によって既に設定されている値は、Sophos Central によって上書きされません。

「**ローカル グループ ポリシー エディター**」で、「**コンピュータの構成 > 管理用テンプレート > Windows コンポーネント > BitLocker ドライブ暗号化 > オペレーティング システムのドライブ**」の順に選択します。次のポリシーが表示されます。

ポリシー	設定	Sophos Central によって設定される値	備考
スタートアップ時にネットワーク ロック解除を許可する		有効	あらかじめ BitLocker のネットワークロック解除を許可し、Central Device Encryption を有効にした後も、動作するようにできます。
スタートアップ時に追加の認証を要求する	互換性のある TPM が装備されていない BitLocker を許可する	チェックが入った状態	TPM が装備されていない Windows 8 コンピュータで、スタートアップ時に、パスワードを使用してシステムディスクのロックを解除できるようにします。
スタートアップ時に追加の認証を要求する	TPM スタートアップ PIN の構成	TPM でスタートアップ PIN を許可する	デバイス暗号化ポリシーの設定で「**起動時に認証が必要**」が有効化されていて、システムに TPM が装備されている場合、TPM およびユーザーによる PIN の入力で、システムドライブを保護することが許可されます。
スタートアップの拡張 PIN を許可する	該当なし	有効	TPM が装備されているシステムドライブを、英数字から構成される PIN で保護できるようにします。このオプションを設定できない場合は、数字のみが許可されます。
プリブート回復メッセージと URL を構成する	プリブート回復メッセージのオプションを選択してください	既定の回復メッセージと URL を使用する	デフォルトのソフォスのメッセージと URL を使用する設定になっています。

ポリシー	設定	Sophos Central によって設定される値	備考
プリブート回復メッセージと URL を構成する	カスタム回復メッセージのオプション	復旧鍵を持っていない場合は、社内の IT ヘルプデスクに問い合わせるか、セルフサービスポータルにアクセスしてください: https://sophos.com/ssp	
プリブート回復メッセージと URL を構成する	カスタム回復 URL オプション		
固定データ ドライブに対するハードウェアベースの暗号化の使用を構成する	該当なし	無効	ソフトウェアベースの暗号化が施行される設定になっています。なお、既存の BitLocker グループポリシーの設定でハードウェアベースの暗号化が義務付けられている場合、そのポリシーの設定内容は変更されません。
オペレーティング システム ドライブに対するハードウェアベースの暗号化の使用を構成する	該当なし	無効	ソフトウェアベースの暗号化が施行される設定になっています。なお、既存の BitLocker グループポリシーの設定でハードウェアベースの暗号化が義務付けられている場合、そのポリシーの設定内容は変更されません。

- 使用する暗号化アルゴリズム: Sophos Central Device Encryption は、デフォルトで AES-256 を使用します。なお、グループポリシー設定で AES-128 を選択することもできます。
- PIN/パスワードの要件: グループポリシー設定で、PIN/パスワードの最小文字数を設定したり、複雑なパスワードの使用を指定したりできます。
- すべてのデータ、または使用領域のみの暗号化: ブートボリュームやデータボリューム用のグループポリシーでフルデータ暗号化が指定されている場合、使用領域のみの暗号化を許可する Sophos Central のポリシーはすべてオーバーライドされます。

グループポリシーの設定内容が Sophos Central と競合する場合、暗号化は実行されません。その場合は、Sophos Central にイベントが送信されます。

- スマートカードの使用: BitLocker におけるスマートカードの使用がグループポリシーで指定されていても、これは Sophos Central でサポートされていないため、エラーが生成されます。
- すべてのデータ、または使用領域のみの暗号化: ブートボリュームやデータボリューム用のグループポリシーで使用領域のみの暗号化が指定されている場合、Sophos Central ポリシーでフルデータ暗号化が指定されると、エラーが生成されます。

Microsoft Surface Pro などのタブレット端末を暗号化する場合で、起動時に認証を行うときは、次のグループポリシー設定を有効にする必要があります。

スレートでプリブートキーボード入力が必要な BitLocker 認証を使用できるようにする

詳細は、サポートデータベースの文章 125772 を参照してください。

BitLocker や TPM グループポリシー設定の一般的な情報は、BitLocker グループポリシーの設定およびTrusted Platform Module Services グループポリシー設定を参照してください。

関連概念

暗号化方式およびレポート (p. 11)
ボリュームは、ソフトウェアベースまたはハードウェアベースで暗号化することができます。

関連情報

BitLocker グループポリシーの設定
TPM グループポリシーの設定
サポートデータベースの文章 125772

2.7 制限事項

ダイナミックディスク

BitLocker は、ダイナミックディスクには対応していません。エンドポイントから Sophos Central にイベントが送信され、システム管理者に暗号化の失敗が通知されます。この原因は、ダイナミックディスクのシステムボリュームを暗号化できないことです。ダイナミックディスクのデータボリュームは、単に無視されます。

リモート デスクトップ

リモート デスクトップで、Sophos Central のエージェントソフトウェアがインストールされている Windows エンドポイントを利用すると、ダイアログはまったく表示されず、暗号化ポリシーを適用しても、デバイス暗号化は強制適用されません。暗号化を有効にすると、ハードウェアの互換性の検証を行うために、再起動が必要になります。ユーザーは、プリブート環境で PIN やパスフレーズを入力しなくてはならなくなりますが、リモート デスクトップ環境で、この操作を実行することはできません。

2.8 暗号化方式およびレポート

ボリュームは、ソフトウェアベースまたはハードウェアベースで暗号化することができます。

デバイス暗号化では、ハードウェアベースの暗号化がサポートされているドライブであっても、新しいボリュームに対しては、常にソフトウェアベースの暗号化が用いられます。

ドライブが既にハードウェアベースの暗号化で暗号化されている場合、ドライブは変更されません。

BitLocker グループポリシーの設定で、ハードウェアベースの暗号化が義務付けられている場合、その設定は変更されません。

「**コンピュータ**」ページで、暗号化方式や暗号化されていないコンピュータなど、暗号化状態に応じてコンピュータをフィルタリングできます。

コンピュータの詳細ページには、ボリュームに対して使用される暗号化方式とアルゴリズムが表示されます。

Windows コンピュータの場合は、「**暗号化の実行日**」も表示されます。表示される情報は、デバイスによって異なります。

- Sophos Central Device Encryption で既に暗号化されているコンピュータの場合、Sophos Central Device Encryption バージョン 2.1 にアップグレードされた日時が表示されます。

- 別の暗号化製品を使用して暗号化されたコンピュータの場合、Sophos Central Device Encryption がインストールされた日時が表示されます。
- Sophos Central Encryption 2.1 以降で暗号化された新しいコンピュータの場合、暗号化された日時が表示されます。

「**暗号化の状態**」レポートには、コンピュータの暗号化状態が表示されます。

暗号化されているコンピュータ、暗号化されているボリュームの種類、および暗号化ポリシーに準拠しているコンピュータを確認できます。また、コンピュータの認証方法や暗号化方式も確認できます。

関連概念

BitLocker グループポリシーの設定 (p. 9)
Sophos Central では、一部のグループポリシー設定が自動設定されるため、管理者はデバイス暗号化のためにコンピュータを事前準備する必要はありません。

コンピュータ
コンピュータのサマリー

2.9 復号化について

通常、復号化を行う必要はありません。既に暗号化されているエンドポイントを、暗号化の対象から除外する必要がある場合は、エンドポイントのすべてのユーザーをポリシーから削除した後に暗号化を無効にすると、除外できます。

エンドポイントの Windows エクスプローラで、システムディスクを右クリックして、「**BitLocker の管理**」を選択します。「**BitLocker ドライブ暗号化**」ダイアログで、「**BitLocker を無効にする**」をクリックします。この操作は、Windows 管理者のみが実行できます。

暗号化ポリシーが適用されているコンピュータで、管理者権限を持つユーザーがハードディスクを手動で復号化しようとした場合、ユーザーの操作は Sophos Central によってオーバーライドされ、ハードディスクは暗号化された状態に保たれます。

2.10 Windows エンドポイントの復旧

ユーザーが BitLocker PIN やパスワードを忘れた場合、コンピュータへのアクセスを復旧する方法は２通りあります。

- ユーザーは Sophos Self Service Portal を使用できます。詳細は、セルフサービスポータルを使用した復旧鍵の取得を参照してください。Windows 10 ユーザーに対しては、「**BitLocker 回復**」画面に指示が表示されます。
- 管理者がユーザーを支援してアクセスを復旧できます。ユーザー側で必要な操作は次のとおりです。

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。
3. ユーザーは、管理者に連絡をして「復旧鍵 ID」を伝えます。
   管理者はユーザーに復旧鍵を通知します。ユーザー用に復旧鍵を取得する方法については、Sophos Central ヘルプを参照してください。
4. ユーザーは復旧鍵を入力し、画面に表示される手順に従って新しい PIN またはパスワードを作成する必要があります。

   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、ユーザーはコンピュータにアクセスできるようになります。通常、ユーザーがブートボリュームにアクセスできるようになると、データボリュームは自動でロック解除されます。これに該当しない場合には、ブートボリュームと同じ方法で、Sophos Central からデータボリュームの復旧鍵を取得します。

関連タスク

セルフサービスポータルを使用した復旧鍵の取得 (p. 22)
BitLocker の PIN や macOS のパスワードを忘れるなどして、ユーザーがコンピュータにログオンできない場合、Sophos Self Service Portal を使用して、ユーザー自身で復旧鍵を取得することができます。

関連情報

セルフサービスポータル
Sophos Central ヘルプ

3 FileVault の管理

Sophos Central Device Encryption for Mac では、Mac に搭載されているフルディスク暗号化機能、FileVault を管理できます。

ユーザーは、macOS のログインパスワードだけで、データを暗号化したり、暗号化したデータにアクセスしたりできます。

3.1 Sophos Central Device Encryption (Mac) への移行

Sophos Central を使用して、FileVault で暗号化済みの Mac エンドポイントを管理する場合は、Sophos Central Device Encryption のポリシーをこれらのエンドポイントに適用する必要があります。

注
FileVault を SafeGuard Enterprise で管理している場合は、まずは **Sophos SafeGuard Device Encryption** のソフトウェアをアンインストールします。

ユーザーが操作を開始する前に必要な操作は次のとおりです。

- Sophos Central のエージェントソフトウェアをエンドポイントにインストールする必要がある。
- Sophos Central でデバイス暗号化ポリシーを設定してオンにする必要がある。
- ユーザーはエンドポイントにログオンする必要がある。エンドポイントは Sophos Central に接続され、同期されている必要がある。リモートログオンはサポートされていないことに注意してください。

エンドポイントに表示されるメッセージと必要な操作は次のとおりです。

1. ユーザーがエンドポイントにログオンしたり、ユーザーがログオンしているときに管理者が Sophos Central Device Encryption のポリシーを適用したりすると、コンピュータを保護するために Device Encryption がセットアップされたという内容のメッセージがユーザーに対して表示されます。
2. Sophos Central Device Encryption をオンにするには、ユーザーはログインパスワードを入力して「**鍵の作成**」をクリックする必要があります。
   新しい復旧鍵が作成され、復旧に備えて Sophos Central に鍵が保存されます。他に暗号化されていない内蔵ハードディスクがある場合は、同時に暗号化されます。これらのハードディスクに対して、別のパスワードを設定する必要はありません。
3. ディスクパスワードで暗号化済みの内蔵ハードディスクがある場合、ユーザーはディスクパスワードを入力して「**続ける**」をクリックする必要があります。
   ディスクパスワードが Sophos Central で管理されるようになります。ハードディスクは、システム起動時に自動でロック解除されます。

これで、エンドポイントが Sophos Central Device Encryption で管理されるようになりました。

3.2 デバイス暗号化の操作手順 (Mac)

Mac を暗号化する手順は、次のとおりです。

ユーザーが操作を開始する前に必要な操作は次のとおりです。

- Sophos Central のエージェントソフトウェアをエンドポイントにインストールする必要がある。
- Sophos Central でデバイス暗号化ポリシーを設定してオンにする必要がある。
- ユーザーはエンドポイントにログオンする必要がある。エンドポイントは Sophos Central に接続され、同期されている必要がある。リモートログオンはサポートされていないことに注意してください。

ユーザーに表示されるメッセージと必要な操作は次のとおりです。

1. ユーザーは Mac を起動後、ログインパスワードを入力します。

   これにより、Sophos Device Encryption がオンになります。
2. システムディスクの暗号化をすぐに開始する場合は、「**暗号化**」をクリックします。後で暗号化を開始する場合は、「**延期**」をクリックします。

   ユーザーがログインパスワードを入力して「**暗号化**」をクリックすると、復旧鍵がローカルディスクのキーチェーンと Sophos Central に保存されます。

   エンドポイント上のすべてのユーザーが、自動的に FileVault に追加されます。

   macOS 10.12 以前のバージョンを実行しているエンドポイントの場合は、各ユーザーごとにログインし、FileVault に追加する必要があります。

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は自動的に暗号化されます。暗号化されたディスクは、コンピュータの起動時に自動でロック解除されます。

ユーザーへの通知には、各ディスクの暗号化の状態に関する情報が表示されます。

3.2.1 新しい FileVault ユーザーの追加

ユーザーが FileVault に自動的に追加されない場合、新しいユーザーに表示される情報、および新しいユーザー側で必要な操作は次のとおりです。

次の操作を実行する必要があります。

1. 新しいユーザーのログインパスワードを入力し、「**続ける**」をクリックします。
   ユーザーは通常、macOS のログインパスワードを使用して Mac にアクセスし、FileVault を使用することができます。
2. Sophos Central に復旧鍵が格納されていない場合、新しいユーザーはこのタスクを承認できる既存の FileVault ユーザーを選択する必要があります。
3. 既存の FileVault ユーザーは、ログインパスワードを入力し、「**続ける**」をクリックする必要があります。

これで、新しいユーザーが macOS のログインパスワードを使用して Mac にアクセスし、FileVault を使用することができるようになります。

3.3 Mac エンドポイントの復旧

Mac を復旧する手順は、次のとおりです。

ユーザーがログインパスワードを忘れた場合、コンピュータへのアクセスを復旧する方法は複数あります。

- 対象のコンピュータに最後にログインしたユーザーがパスワードを忘れたユーザーの場合は、ユーザー自身で Sophos Self Service Portal を使用して復旧できます。詳細は、セルフサービスポータルを使用した復旧鍵の取得を参照してください。
- ユーザー自身で、外付けの Mac 起動ディスクを使用してコンピュータを起動し、ターミナルコマンドを実行してディスクをロック解除できます。
- ユーザー自身で、ターゲット ディスク モードでコンピュータを起動し、ターミナルコマンドを実行してディスクをロック解除できます。
- ユーザー自身で、macOS 復元を使用してコンピュータを起動し、ターミナルコマンドを実行してディスクをロック解除できます。

  ターミナルコマンドの詳細は、ターミナルコマンドで HFS+ ボリュームをロック解除およびターミナルコマンドで APFS ボリュームをロック解除を参照してください。

管理者がユーザーを支援してアクセスを復旧できます。ユーザー側で必要な操作は次のとおりです。

1. エンドポイントコンピュータの電源を入れ、「**復旧鍵 ID**」が表示されるまで待ちます。
   復旧鍵 ID は、数分間のみ表示されます。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。
2. ユーザーは、管理者に連絡をして「復旧鍵 ID」を伝えます。
   管理者はユーザーに復旧鍵を通知します。ユーザー用に復旧鍵を取得する方法については、Sophos Central ヘルプを参照してください。
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アイコン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。

   Active Directory からインポートしたユーザーには、次の手順を実行する必要があります。

   - Active Directory で既存のパスワードをリセットします。そして、一時的なパスワードを生成して、ユーザーに通知します。
   - 「**パスワードのリセット**」ダイアログで「**キャンセル**」をクリックして、一時的なパスワードを入力するようユーザーに伝えます。
6. 画面上の指示に従い、新しいパスワードを設定します。
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、ユーザーが起動ボリュームにアクセスできるようになります。

macOS 10.12 以前のバージョンを実行しているエンドポイントでは、新しい復旧鍵が作成され、Sophos Central に保存されます。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。

macOS 10.13 と Apple File System (APFS) が稼働しているエンドポイントでは、新しく復旧鍵が作成されることはありません。既存の復旧鍵を引き続き使用できます。

関連タスク

セルフサービスポータルを使用した復旧鍵の取得 (p. 22)

BitLocker の PIN や macOS のパスワードを忘れるなどして、ユーザーがコンピュータにログオンできない場合、Sophos Self Service Portal を使用して、ユーザー自身で復旧鍵を取得することができます。

ターミナルコマンドで HFS+ ボリュームをロック解除 (p. 17)
ターミナルコマンドを使用して暗号化されたボリュームのロックを解除できます。このセクションに記載されているコマンドは、macOS 10.12 以前のバージョンを実行しており、HFS+ フォーマットのボリュームがあるエンドポイントを対象としています。

ターミナルコマンドで APFS ボリュームをロック解除 (p. 17)
ターミナルコマンドを使用して暗号化されたボリュームのロックを解除できます。このセクションに記載されているコマンドは、macOS 10.13 および Apple File System (APFS) が稼働しているエンドポイントを対象としています。

関連情報

macOS 復元について
別の起動ディスクを選択する方法
Sophos Central ヘルプ

3.3.1 ターミナルコマンドで HFS+ ボリュームをロック解除

ターミナルコマンドを使用して暗号化されたボリュームのロックを解除できます。このセクションに記載されているコマンドは、macOS 10.12 以前のバージョンを実行しており、HFS+ フォーマットのボリュームがあるエンドポイントを対象としています。

ユーザー側で必要な操作は次のとおりです。

1. 「**ターミナル**」アプリケーションを開き、diskutil corestorage list を実行します。
   接続されているすべてのディスクの一覧が表示されます。
2. 復旧するボリュームの名前 (LV Name) を検索し、Logical Volume の ID をメモします。
3. ユーザーは管理者に連絡し、復旧鍵の ID として Logical Volume の ID を管理者に伝え、復旧鍵を要求します。
   管理者はユーザーに復旧鍵を通知します。ユーザー用に復旧鍵を取得する方法については、Sophos Central ヘルプを参照してください。
4. ディスクパスワードの画面に復旧鍵を入力してディスクのロックを解除します。
   または、ユーザーが diskutil corestorage unlockVolume コマンドを実行して「**ターミナル**」アプリケーションに復旧鍵を入力しても、ディスクのロックを解除することができます。

これで、Finder からディスクにアクセスできるようになりました。

関連情報

Sophos Central ヘルプ

3.3.2 ターミナルコマンドで APFS ボリュームをロック解除

ターミナルコマンドを使用して暗号化されたボリュームのロックを解除できます。このセクションに記載されているコマンドは、macOS 10.13 および Apple File System (APFS) が稼働しているエンドポイントを対象としています。

ユーザー側で必要な操作は次のとおりです。

1. 「**ターミナル**」アプリケーションを開き、diskutil apfs list を実行します。
   接続されているすべてのディスクの一覧が表示されます。
2. 復旧するボリューム名を検索し、ボリューム ID をメモします (例: Volume disk1s1)。
3. ユーザーは管理者に連絡し、復旧鍵の ID としてボリューム ID を伝え、復旧鍵を要求します。

管理者はユーザーに復旧鍵を通知します。ユーザー用に復旧鍵を取得する方法については、Sophos Central ヘルプを参照してください。

4. ディスクパスワードの画面に復旧鍵を入力してディスクのロックを解除します。
または、ユーザーが diskutil apfs unlockVolume コマンドを実行して「**ターミナル**」アプリケーションに復旧鍵を入力しても、ディスクのロックを解除することができます。

これで、Finder からディスクにアクセスできるようになりました。

関連情報
Sophos Central ヘルプ

3.3.3 エラー: 復旧鍵を保存できませんでした

ごくまれに、システムがローカルドライブ (キーチェーンに) または Sophos Central に復旧鍵を保存できないことがあります。

この場合、ユーザーがパスワードを忘れてしまうと、コンピュータを復旧できません。この状態を防ぐために、復旧鍵が記載されたエラーメッセージが表示され、ユーザーは復旧鍵を複製するよう促されます。

システムは、Sophos Central への復旧鍵の保存を繰り返し試みます。成功すると、新しい復旧鍵が Sophos Central で管理されるようになったため、複製した復旧鍵を削除できるというメッセージが表示されます。

3.4 デバイス暗号化の状態 (Mac)

暗号化の状態は、「**Sophos Device Encryption**」というアプリケーションを使用して表示できます。このアプリケーションは、「アプリケーション」フォルダにインストールされており、Finder、Launchpad、または Spotlight から起動できます。

「**Sophos Device Encryption**」には次の情報が表示されます。

- ポリシーの状態: 1行目に、エンドポイントが Sophos Device Encryption で管理されているかどうかが表示されます。
- ユーザーの状態: 次の行に、ユーザーが利用できる/できない操作が表示されます。
- ディスクの状態: すべての内蔵ディスクの一覧が表示されます。マウントされていないディスクは、ディスク名がグレーアウト表示されます。ディスク名の横のアイコンは、ディスクのステータスを表します。次のステータスが表示されます。
  - 緑: ディスク全体が暗号化されており、復旧鍵が一元管理機能で保存されています。
  - 黄色: ディスク全体が暗号化されていますが、復旧鍵が Sophos Central に保存されていません。この現象は、Sophos Central が接続できない状態の場合に発生することがあります。ディスクの暗号化が要求されていないために復旧鍵が存在しない可能性もあります。通常この状況に該当するのは、ディスクが Sophos Central Device Encryption で管理されておらず、OS のツールで暗号化されている場合です。
  - 黄色 (感嘆符付き): ディスクが丸ごと暗号化されており、ディスクの暗号化を要求するポリシーも存在しますが、復旧鍵がありません。
  - 赤: ディスクは暗号化されていませんが、ディスクの暗号化を要求するポリシーが有効になっています。
  - グレー: ディスクは暗号化されていません。ポリシーで暗号化が要求されていないか、またはポリシーそのものが存在しません。
  - ステータスバー + **暗号化中**: ディスクの暗号化が進行中です。

— ステータスバー + **復号化中**: ディスクの復号化が進行中です。

注
Mac エンドポイント上の管理者権限を持つユーザーが暗号化ポリシーの適用されているローカルハードディスクを手動で復号化しようとすると、この操作は Sophos Central でオーバーライドできないため、ハードディスクは復号化されます。復号化が完了すると、ユーザーは FileVault を有効にするためにパスワードの入力を促され、ディスクが再び暗号化されます。

- 復旧ステータス: ディスクの復旧鍵が利用可能な状態かどうかが画面下部に表示されます。

また、コマンドラインツールからも Device Encryption のステータスを確認できます。コマンドラインツールは、/usr/local/bin/seadmin にインストールされます。利用できるコマンドは次のとおりです。

- help: 利用できるコマンドの一覧を表示します。
- status: 暗号化ソフトの前回同期と同期間隔を表示します。
- --device-encryption: 現在の暗号化ポリシーや、すべての内蔵ディスクの暗号化ステータスと復旧ステータスを表示します。

4 安全にファイルを共有するためにファイルをパスワード保護する方法

これは、「**デバイス暗号化**」ポリシーでオンにできます。

注
この機能は、Central Device Encryption 2.0 以降のみで使用できます。この機能は、Windows のみに対応しています。

最大 50MB のファイルを保護できます。

コンテキストメニューを有効にする: このオプションをオンにすると、右クリックメニューに「**ファイルのパスワード保護**」オプションが表示されるようになります。ユーザーは、社外に機密情報を送信する際に、ファイルをパスワードで保護してメールに添付することができます。ファイルは、コンテンツが暗号化された新しい HTML ファイルにラップされます。

受信者は、このファイルをダブルクリックしてパスワードを入力することで、ファイルを開くことができます。受信者は、同じパスワードや新しいパスワードを使用して受信したファイルを保護して返送するか、またはパスワード保護されたファイルを新たに作成できます。

Outlook アドインを有効にする: このオプションをオンにすると、メールの添付ファイルの暗号化機能が Outlook に追加されます。ユーザーは、Outlook のリボンにある「**添付ファイルの保護**」を選択することにより、添付ファイルを保護することができます。平文の添付ファイルはすべて、コンテンツが暗号化された新しい HTML 形式の添付ファイルにラップされたうえで、メール送信されます。

添付ファイルの処理について、常にユーザーに確認する: このオプションをオンにすると、メッセージにファイルが添付されているときは、ユーザーは必ず、添付ファイルの送信方法を選択する必要があります。ユーザーは、ファイルをパスワードで保護して送信することも、平文のまま送信することもできます。

社内ドメインなど、「**添付ファイルの処理について、常にユーザーに確認する**」オプションの適用対象から除外するドメインを入力できます。送信先がそういったドメインの場合、添付ファイルの処理方法を確認するメッセージは表示されません。

完全ドメイン名のみを入力し、複数指定する場合は、コンマで区切ってください。

関連情報
デバイス暗号化ポリシー

5 ユーザーにパスワード/PIN の変更を求める方法

ユーザーにパスワードの変更を求めるには、次の 2つの方法があります。

注
このオプションは、Windows のみに対応しています。

- 暗号化ポリシーで「**認証用パスワード/PIN をユーザーがリセットする**」オプションを使用する。

  このオプションはデフォルトでオフになっています。指定された期間後に BitLocker のパスワードまたは PIN の変更を強制します。ユーザーがパスワードまたは PIN を変更すると、イベントがログに記録されます。

  注
  この機能は、Central Device Encryption 2.0 以降のみで使用できます。

- コンピュータの詳細ページの「**サマリー**」タブにある「**パスワード/PIN の変更の実行**」オプションを使用する。

  BitLocker のパスワードまたは PIN を、直ちに変更するようユーザーに要求します。この要求の送信に成功すると、メッセージが表示されます。

BitLocker の新しいパスワードまたは PIN を設定するよう、エンドポイントでユーザーにメッセージが表示されます。ユーザーが新しいパスワードや PIN を入力せずにダイアログを閉じると、30秒後にダイアログが再表示されます。入力すると表示は停止します。パスワードや PIN を変更せずにダイアログを 5回閉じると、警告がログに記録されます。

関連情報
デバイス暗号化ポリシー
コンピュータのサマリー

6 セルフサービスポータルを使用した復旧鍵の取得

BitLocker の PIN や macOS のパスワードを忘れるなどして、ユーザーがコンピュータにログオンできない場合、Sophos Self Service Portal を使用して、ユーザー自身で復旧鍵を取得することができます。

ユーザーは、この復旧鍵を使用してコンピュータに再度アクセスできます。

セルフサービスポータルを使用した復旧をユーザーに許可するには、「**Sophos Central > ユーザーとグループ > ユーザー**」を開き、ユーザーを選択して (複数可)、「**セットアップリンクのメール送信**」ボタンをクリックします。ダイアログが表示されるので、「**Sophos Central Self Service - ようこそ/セットアップ メール**」を選択して、アクティベーションのリンクが記載されたメールをユーザーに送信します。ユーザーはメールに記載されている手順に従い、Sophos Self Service Portal を使用してコンピュータへのアクセスを復旧します。

ユーザー側で必要な操作は次のとおりです。

1. 別のコンピュータから Sophos Self Service Portal にログオンします。
2. 「**デバイス暗号化**」ページを開きます。
   ユーザーが最終ログオンユーザーであるコンピュータの一覧が表示されます。この後に、別のユーザーが復旧するコンピュータにログオンした場合は、セルフサービスポータルを使用してコンピュータへのアクセスを復旧することはできません。
3. 一覧からコンピュータを選択して、「**復旧鍵**」カラムの「**取得**」ボタンをクリックします。
   復旧鍵がダイアログに表示されます。
4. 復旧するコンピュータを起動し、復旧ページを開きます。
   - Windows: 「**Esc**」キーを押して、BitLocker の復旧画面に切り替えます。
   - Mac: 「**パスワード**」フィールドの疑問符のアイコンをクリックし、FileVault の復旧ページを開きます。
5. 復旧鍵を入力します。

これで、ユーザーはコンピュータにアクセスできるようになります。

関連情報

セルフサービスポータル

7 参考資料

Windows

- FAQ: サポートデータベースの文章 124819
- BitLocker よくある質問 (FAQ)
- BitLocker グループポリシーの設定
- TPM の基本情報
- TPM グループポリシーの設定
- TPM の管理に関する技術概要

Mac

- FAQ: サポートデータベースの文章 125982
- FileVault の設定 : FileVault を使って Mac の起動ディスクを暗号化する
- FileVault 復旧キー: 企業、学校、団体等のコンピュータに FileVault 復旧キーを設定する
- パスワードのリセット: macOS ユーザアカウントのパスワードを変更またはリセットする

関連情報

BitLocker よくある質問 (FAQ)
BitLocker グループポリシーの設定
TPM グループポリシーの設定
TPM の基本情報
TPM の管理に関する技術概要
FileVault を使って Mac の起動ディスクを暗号化する
企業、学校、団体等のコンピュータに FileVault 復旧キーを設定する
macOS ユーザアカウントのパスワードを変更またはリセットする
サポートデータベースの文章 124819
サポートデータベースの文章 125982

8 対応している Web ブラウザ

現在対応しているブラウザは次のとおりです。

- Microsoft Internet Explorer 11 および Microsoft Edge。
- Google Chrome。
- Mozilla Firefox。
- Apple Safari (Mac のみ)。

上記のサポート対応ブラウザをインスールまたはアップグレードし、常に最新バージョンを使用することを推奨します。ソフォスでは、Google Chrome、Mozilla Firefox、Apple Safari の最新バージョンとその 1つ前のバージョンに対応するよう努めています。非対応のブラウザが検出されると、https://central.sophos.com/unsupported にリダイレクトされます。

注
Sophos Central Admin は、モバイルデバイスには対応していません。

9 サポートへのお問い合わせ

ソフォスのサポートへは、以下の方法でお問い合わせいただけます。

1. 画面右上の「**ヘルプ**」をクリックし、「**サポートチケットの作成**」を選択します。
2. フォームに必要事項を入力します。お問い合わせに適切に対応できるよう、できる限り詳しい情報を入力してください。
3. 任意で、ソフォスの担当者がお客様の Sophos Central の画面を直接見ながらサポートすることを許可するオプションを選択します。
4. 「**送信**」をクリックします。

ソフォスの担当者が 24時間以内にご連絡します。

注
お客様の Sophos Central セッションへのアクセスをソフォスの担当者に許可するオプションを選択した場合、その機能は「**送信**」をクリックすると有効になります。有効化されたリモートアシスタンスは、72時間後には自動的に無効化されます。これよりも早く無効化するには、画面右上のアカウント名をクリックして、「**アカウントの詳細**」を選択し、「**ソフォスサポート**」タブをクリックします。

フィードバックの送信

製品に関するご意見やご要望をソフォスのサポートに送信する方法は次のとおりです。

1. 画面右上の「**ヘルプ**」をクリックし、「**フィードバックの作成**」を選択します。
2. フォームに必要事項を入力します。
3. 「**送信**」をクリックします。

その他のテクニカルサポート

テクニカルサポートは次のようなかたちでも提供しています。

- 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

10 利用条件