SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise

ユーザーヘルプ

製品バージョン: 8.3

目次

(2019/11/14)

1 SafeGuard Enterprise について

Sophos SafeGuard は、Windows エンドポイントで実行されるセキュリティ対策ソリューションです。複数のモジュールから構成されています。

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。これは、使用しているライセンス、およびセキュリティ担当者が適用したポリシーに依存します。

Sophos SafeGuard は、Sophos SafeGuard Management Center コンソールから一元的に設定・管理されます。

Sophos SafeGuard に関する全般的な情報を表示するには、Sophos SafeGuard システムトレイ (p. 7)の Sophos SafeGuard アイコンをクリックします。

ファイルの暗号化/復号化に関する最も重要なオプションは、Windows エクスプローラの右クリックメニューからアクセスできます。

このドキュメントは、Windows エンドポイントのみを対象にしています。Mac エンドポイントの詳細は、SafeGuard Enterprise Mac ユーザーヘルプを参照してください。

モジュール:

フルディスク暗号化

- **BitLocker を使用したフルディスク暗号化 (p. 2)**

Synchronized Encryption

- **SafeGuard ファイル暗号化 (アプリケーションベース) (p. 2)**

ファイル暗号化

- **SafeGuard ファイル暗号化 (ロケーションベース) (p. 3)**
- **SafeGuard Cloud Storage (p. 3)**
- **SafeGuard Data Exchange (p. 4)**

2 モジュール

2.1 BitLocker を使用したフルディスク暗号化

BitLocker を使用したフルディスク暗号化は、OS に搭載されている Bitlocker ドライブ暗号化テクノロジーを利用します。ハードディスク全体を暗号化し、コンピュータの盗難や紛失によるデータ漏えいを防止します。

エンドポイントにログオンするたびにログオン情報を入力して、BitLocker のロックを解除する必要があります。詳細は、コンピュータの BitLocker 暗号化 (p. 10)を参照してください。

Sophos SafeGuard を使って、以下のいずれかの OS 環境のエンドポイントの BitLocker を管理することができます。

- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise

2.2 SafeGuard ファイル暗号化 (アプリケーションベース)

アプリケーションベースのファイル暗号化では、指定されたアプリケーション (例: Microsoft Word など) で作成/変更したファイルが暗号化されます。ポリシーでは、このファイル暗号化を自動的に実行するアプリケーションのリストを指定します。これは永続暗号化で、ファイルを別の場所に移動したり、クラウド ストレージ サービスにアップロードしたり、メールで送信したりしても暗号化されたままで残ります。

セキュリティ担当者が、ファイル暗号化をアクティブにするアプリケーションとして Microsoft Word を指定した場合、Microsoft Word で作成/保存されたファイルはすべて、指定された鍵で暗号化されます。鍵リングにこの鍵が含まれている限り、誰でもこのファイルにアクセスできます。

- 指定したアプリで作成した新規ファイルや指定したファイル拡張子のある新規ファイルは、自動的に暗号化されます。
- 暗号化されたファイルに対する鍵がある場合、ファイルの読み取りおよび変更が可能です。
- 暗号化されたファイルに対する鍵がない場合、ファイルの内容を読むことはできません。
- 暗号化されたファイルに、File Encryption がインストールされていないコンピュータからアクセスしても、ファイルの内容を読むことはできません。
- 暗号化対象でないフォルダから、暗号化ルールが適用されるフォルダにコピー/移動したファイルは、暗号化されます。
- 暗号化対象フォルダから暗号化対象でないフォルダにコピー/移動したファイルは、復号化されます。
- 暗号化対象フォルダから、別の暗号化ルールが適用されているフォルダにコピー/移動したファイルは、対象のフォルダに適用されている暗号化ルールに従って暗号化されます。
- ファイルを作成したアプリケーションでファイル暗号化が有効化されていないが、そのファイルの拡張子に対して暗号化ルールが指定されている場合、ファイルは暗号化され、作成に使用されたアプリケーションで開くことができなくなります。具体例としては、OpenOffice で .doc ファイルを作成し、OpenOffice が「**アプリケーションリスト**」で指定されていない場合などです。

重要
ファイルのコピーや移動が、再起動などによって中断された場合、操作は自動的には再開されません。結果として、意図せずに、ファイルが暗号化されない状態で残る可能性があります。常にファイルが適切に暗号化されているようにするには、ポリシーに基づいたすべてのファイルの暗号化 (p. 12)を参照してください。

暗号化対象に指定されているコンピュータ上のパスは、ファイル暗号化の対象の場所の表示 (p. 14)で参照できます。

1つまたは複数のファイルの暗号化の状態を参照するには、ファイル (複数選択可) を右クリックして、「**SafeGuard ファイル暗号化 > 暗号化の状態の表示**」を選択します。

Windows エクスプローラの暗号化されているファイルは、緑色の鍵マーク付きで表示されます。ファイルが暗号化されているにも関わらず、鍵マークが表示されない場合は、ソフォスのサポートデータベースの文章 108784 を参照してください。

2.3 SafeGuard ファイル暗号化 (ロケーションベース)

ロケーションベースのファイル暗号化では、暗号化対象の場所をセキュリティ担当者が定義することができます。例: <**ドキュメント**>。

種類が「**ロケーションベース**」の「**File Encryption**」ポリシーをコンピュータに適用すると、そのポリシーで指定されている場所にあるファイルは、ユーザー介入なしで透過的に暗号化されます。

- 暗号化対象に指定されている場所に新規ファイルを作成すると、ファイルは自動的に暗号化されます。
- 暗号化されたファイルに対する鍵がある場合、ファイルの読み取りおよび変更が可能です。
- 暗号化されたファイルに対する鍵がない場合、ファイルの内容を読むことはできません。
- 暗号化されたファイルに、File Encryption がインストールされていないコンピュータからアクセスしても、ファイルの内容を読むことはできません。

コンピュータで暗号化の対象に指定されている場所は、ファイル暗号化の対象の場所の表示 (p. 14)で参照できます。

1つまたは複数のファイルの暗号化の状態を参照するには、ファイル (複数選択可) を右クリックして、「**SafeGuard ファイル暗号化 > 暗号化の状態の表示**」を選択します。

Windows エクスプローラの暗号化されているファイルは、緑色の鍵マーク付きで表示されます。ファイルが暗号化されているにも関わらず、鍵マークが表示されない場合は、ソフォスのサポートデータベースの文章 108784 を参照してください。

2.4 SafeGuard Cloud Storage

SafeGuard Cloud Storage は、クラウド上に保存されるファイルをロケーションベースで暗号化する機能です。ファイルは従来どおりの方法で利用できますが、クラウド上のデータをローカルにコピーすると、透過的に暗号化が行われ、データをクラウド上に保存した際も暗号化が解除されません。

SafeGuard Cloud Storage は、対応しているクラウド ストレージ サービスを自動的に検出し、暗号化ポリシーを同期フォルダに適用します。

SafeGuard Cloud Storage では、データの初期暗号化は実行されません。SafeGuard Cloud Storage をインストールする前や、ポリシーで有効化する前に保存されたファイルは、暗号化されず、暗号化されないままで残ります。このようなファイルを暗号化するには、まずクラウドから削除した後、再度クラウドに追加するようにしてください。

注
Dropbox フォルダにファイルを追加する際、Windows デスクトップの Dropbox アイコンにファイルをドロップしないでください。ファイルは平文で Dropbox フォルダに保存されます。ファイルが暗号化されるよう、直接 Dropbox フォルダにコピーするようにしてください。

重要
Microsoft Windows 付属のアーカイバを使用して ZIP アーカイブを解凍する際、鍵のない暗号化ファイルが検出されると、ただちに処理が停止されます。ユーザーにはアクセスが拒否されたというメッセージが表示されますが、処理されていないファイル (つまり、存在しないファイル) があることは通知されません。一方、7-Zip のような他のアーカイバは、ZIP アーカイブに暗号化されたファルが含まれていても正常に動作します。

2.5 SafeGuard Data Exchange

SafeGuard Data Exchange は、リムーバブル メディアに保存されているファイルをロケーションベースで暗号化し、ファイルを他のユーザーと交換するために使用されます。対応する鍵を持っているユーザーだけが、暗号化されたデータの内容を読み取ることができます。暗号化と復号化の処理はすべて透過的に実行され、ユーザー介入は最小限で済みます。

日常の作業でユーザーは、データが暗号化されていることを意識しません。しかし、リムーバブル メディアを取り外すと、データは暗号化された状態を維持するため、不正なアクセスから保護されます。権限のないユーザーは、ファイルに物理的にアクセスすることはできても、SafeGuard Data Exchange および適切な鍵がないとファイルを読み取ることはできません。

リムーバブル メディア上のデータ処理方法は、セキュリティ担当者が設定します。たとえば、任意のリムーバブル メディアに保存されるファイルに対して、暗号化を必須と設定することができます。この場合、デバイスに存在する暗号化されていないファイルすべての初期暗号化が行われます。さらに、リムーバブル メディアに新たに保存されるファイルもすべて暗号化されます。既存のファイルを暗号化しない場合は、セキュリティ担当者は、暗号化されていない既存のファイルへのアクセスを許可するよう定義できます。この場合、暗号化されていない既存のファイルは SafeGuard Data Exchange で暗号化されません。ただし、新しいファイルは暗号化されます。したがって、ユーザーは暗号化されていない既存のファイルを読み取ったり編集したりすることはできますが、ファイルの名前を変更するとファイルは直ちに暗号化されます。また、セキュリティ担当者が、暗号化されていないファイルへのアクセスを禁止すると、ファイルは暗号化されていないままになります。

リムーバブル メディアに保存されている暗号化されたファイルの交換方法には次の 2とおりがあります。

- **SafeGuard Enterprise が受け取り側のコンピュータにインストールされている場合**: 両者が使用可能な鍵を使用するか、新しい鍵を作成することができます。新しい鍵を作成する場合は、データの受け取り側に鍵のパスフレーズを通知する必要があります。
- **SafeGuard Enterprise が受け取り側のコンピュータにインストールされていない場合:** SafeGuard Enterprise では、SafeGuard Portable を使用することができます。このユーティリティは、暗号化されたファイルと一緒に自動的にリムーバブル メディアにコピーできます。受け取り側は、SafeGuard Portable と適切なパスフレーズを使用すれば、SafeGuard Data Exchange がコンピュータにインストールされていなくても、暗号化されたファイルを復号化し、再度それを暗号化できます。

重要
Microsoft Windows 付属のアーカイバを使用して ZIP アーカイブを解凍する際、鍵のない暗号化ファイルが検出されると、ただちに処理が停止されます。ユーザーにはアクセスが拒否されたというメッセージが表示されますが、処理されていないファイル (つまり、存在しないファイル) があることは通知されません。一方、7-Zip のような他のアーカイバは、ZIP アーカイブに暗号化されたファルが含まれていても正常に動作します。

2.5.1 オーバーレイアイコン

オーバーレイアイコンは、Windows エクスプローラの項目の上に表示される小さいアイコンです。ファイルの暗号化の状態に関する情報を素早く表示することができます。表示されるアイコンの種類は、インストールしたモジュールによって異なります。

Data Exchange のオーバーレイアイコンは、ファイルとボリュームのみに対して表示されます。

- 赤い色の鍵: ファイルを復号化する鍵がない場合に表示されます。このアイコンは、ファイルのみに対して表示されます。
- 緑色の鍵: 鍵が鍵リングにある暗号化ファイルに対して表示されます。このアイコンは、ファイルのみに対して表示されます。
- 灰色の鍵: 適用可能な暗号化ルールのある暗号化されていないファイルに対して表示されます。このアイコンは、ファイルのみに対して表示されます。
- 黄色の鍵: 定義済みの暗号化ポリシーのあるドライブに対して表示されます。このアイコンは、ドライブのみに対して表示されます。

オーバーレイアイコンは、ブートボリューム以外のボリューム、リムーバブルメディア、および CD/DVD ドライブのみに対して表示されます。ブートボリュームでは、オーバーレイアイコンは、ステージングエリア (Windows で CD/DVD への書き込みを待機しているファイルの保存先フォルダ) に表示されます。 暗号化されていないフォルダを指定すると、そのフォルダおよびサブフォルダ内の暗号化されていないファイルに対して、灰色の鍵は表示されません。一般に、ファイルに暗号化ルールが適用されてない場合、灰色の鍵は表示されません。

注
オーバーレイアイコンが表示されない場合は、ソフォスのサポートデータベースの文章 108784 を参照してください。

2.5.2 透過的な暗号化

リムーバブル メディア上のファイルが暗号化されるよう、ユーザーのコンピュータに対して規定されている場合、暗号化と復号化の処理はすべて透過的に実行されます。

ファイルは、リムーバブル メディアに書き込まれるときに暗号化され、リムーバブル メディアから別の場所にコピーまたは移動されるときに復号化されます。

データは、他の暗号化ポリシーが適用されていない場所にコピーまたは移動される場合のみに復号化されます。このような場合、データはその場所で平文として利用できるようになります。新しい場所に別の暗号化ポリシーが適用されている場合は、それに従ってデータが暗号化されます。

2.5.3 リムーバブル メディア用のメディア パスフレーズ

SafeGuard Data Exchange では、コンピュータに接続されているすべてのリムーバブル デバイスへのアクセスを許可する、シングル メディア パスフレーズを定義できます。これは、個々のファイルを暗号化するために使用した鍵とは関係ありません。

指定すると、1つのメディア パスフレーズを入力するだけで、暗号化されたファイルへのアクセスが許可されます。メディア パスフレーズは、ログオン権限が付与されているコンピュータに結び付けられます。つまり、各コンピュータで同じメディア パスフレーズを使用できます。

メディア パスフレーズの設定方法について、詳細は、メディア パスフレーズの使用 (p. 19)を参照してください。

メディア パスフレーズは変更できます。また、リムーバブル メディアを作業中の各コンピュータに接続するとすぐに、そのコンピュータで自動的に同期されます。

メディア パスフレーズは、次のシナリオの場合に役に立ちます。

- SafeGuard Enterprise がインストールされていないコンピュータにおいて、リムーバブル メディア上の暗号化されたデータを使用する場合 (SafeGuard Data Exchange を SafeGuard Portable と併用)
- データを外部ユーザーと交換する場合: 外部ユーザーにメディア パスフレーズを提供することにより、個々のファイルの暗号化にどの鍵が使用されたかに関係なく、1つのシングル パスフレーズを使用して、リムーバブル メディア上のすべてのファイルへのアクセスを外部ユーザーに許可できます。

また、特定の鍵 (「ローカル鍵」と呼ばれ、SafeGuard Data Exchange ユーザーが作成できる) のパスフレーズだけを外部ユーザーに提供して、すべてのファイルへのアクセスを制限することもできます。この場合、外部ユーザーは、この鍵で暗号化されたファイルのみにアクセスできます。他のファイルを読み取ることはできません。

SafeGuard Enterprise のグループ鍵を使用して、グループのメンバーがそのような鍵を共有するワークグループ内でリムーバブル メディア上のデータを交換する場合は、メディア パスフレーズは必要ありません。この場合 (セキュリティ担当者によってそのように指定されている場合)、リムーバブル メディア上の暗号化されたファイルへのアクセスは完全に透過的になります。パスフレーズやパスワードを入力する必要はありません。これは、リムーバブル メディアのグループ鍵とメディア パスフレーズを同時に使用できるからです。システムによって利用可能なグループ鍵が自動的に検出されるため、この鍵を共有しているユーザーのアクセスは完全に透過的になります。グループ鍵が検出されない場合は、SafeGuard Data Exchange でダイアログが表示され、メディア パスフレーズまたはローカル鍵のパスフレーズを入力するように求められます。

対応メディア

SafeGuard Data Exchange は、次のリムーバブル メディアに対応しています。

- スタートアップ キー
- USB や FireWire を使用して接続される外付けハード ディスク
- CD RW ドライブ (UDF)
- DVD RW ドライブ (UDF)
- USB カード リーダーに挿入されたメモリ カード

ブルーレイディスクおよび 2層 DVD には対応していません。

3 Sophos SafeGuard システムトレイ

ユーザーは、Windows タスクバーの Sophos SafeGuard システム トレイ アイコンを使用して、自分のコンピュータにある Sophos SafeGuard の機能のすべてにアクセスできます。表示される機能は、インストール済みのモジュールによって異なります。

Sophos SafeGuard システム トレイ アイコンを右クリックして、次の項目を表示します。

- **表示**:
  - **鍵リング**: 使用可能なすべての鍵が表示されます。

    注
    これまで集中管理されていなかったエンドポイントが新たに管理下に置かれた場合、SafeGuard Enterprise にログオンし直さないと、ユーザーが定義したローカル鍵が鍵リングに表示されないことがあります。

  - **ユーザー証明書**: ユーザー証明書に関する情報が表示されます。
  - **企業証明書**: 企業証明書に関する情報が表示されます。
- **BitLocker のログオン情報のリセット**: BitLocker の PIN を変更するためのダイアログが開きます。
- **新しい鍵の作成**: SafeGuard Data Exchange (p. 4) や SafeGuard Cloud Storage (p. 3) で使用される新しい鍵を作成するためのダイアログが開きます。いずれかのモジュールがインストールされている場合のみに表示されます。
- **メディア パスフレーズの変更**: メディア パスフレーズを変更するダイアログが開きます。詳細は、SafeGuard Data Exchange (p. 4)を参照してください。
- **同期**: SafeGuard Enterprise Server との同期を開始します。ツールチップに同期の進行状況が表示されます。システム トレイ アイコンをダブルクリックして、同期を開始することもできます。
- **状態**: SafeGuard Enterprise で保護されているコンピュータの現在の状態を示すダイアログが開きます。

フィールド	情報
前回ポリシーを受信した日時	コンピュータが新しいポリシーを前回受信した日時。
前回鍵を受信した日時	コンピュータが新しい鍵を前回受信した日時。
前回証明書を受信した日時	コンピュータが新しい証明書を前回受信した日時。
前回サーバーに接続した日時	サーバーに前回接続した日時。

フィールド	情報
SGN ユーザーの状態	コンピュータにログオンしているユーザー (Windows ログオン) の状態。 — **保留中** POA 実行中のユーザーのレプリケーションが保留中です。これは、初期ユーザー同期がまだ完了していないことを意味します。SafeGuard Enterprise に最初にログオンした後、この情報は特に重要です。これは、初期ユーザー同期が完了して初めて SafeGuard Power-on Authentication でログオンできるためです。 — **SGN ユーザー** Windows にログオンしているユーザーは、SafeGuard Enterprise ユーザーです。SGN ユーザーは SafeGuard Power-on Authentication でログオンすることが可能で、UMA (User Machine Assignment) に追加され、暗号化データにアクセスするためのユーザー証明書と鍵リングが割り当てられます。 — **SGN ユーザー (所有者)** デフォルト設定を変更していない場合、所有者は、他のユーザーがエンドポイントにログオンして、SGN ユーザーになることを許可することができます。 — **SGN ゲスト** SGN ゲストユーザーは、UMA に追加されず、SafeGuard POA でログオンする権限が与えられず、証明書や鍵リングが割り当てられず、データベースに保存されません。 — **SGN ゲスト (サービス アカウント)** Windows にログオンしているユーザーは、管理タスク用のサービス アカウントを使用してログオンした SafeGuard Enterprise ゲスト ユーザーです。 — **SGN Windows ユーザー** SafeGuard Enterprise Windows ユーザーは、SafeGuard POA には追加されませんが、SafeGuard Enterprise ユーザーと同様に、暗号化されたファイルにアクセスするための鍵リングを使用できます。ローカルユーザーは、UMA に追加されます。これは、ユーザーが、そのエンドポイントで Windows にログオンできることを意味します。 — **認証されていないユーザー** 認証されていないユーザーは、次のいずれかの理由で鍵リングにアクセスできません。 – ユーザーが入力したログイン情報が間違っています。 – ローカルユーザーです。 – AD 認証サーバーに接続できませんでした。 – 認証に失敗しました。 – 詳細は、ソフォスのサポートデータベースの文章 124328 も参照してください。 ユーザーが鍵リングにアクセスするには、セキュリティ担当者がユーザーを認証する必要があります。

フィールド	情報
SGN マシンの状態	エンドポイントのセキュリティレベルが表示されます。 — **該当なし** 該当する機能は無効化されています。 — **マシンは安全です** マシンのセキュリティ状態は安全です。 — **マシンは感染しています** マシンのセキュリティ状態は安全ではありません。このため、鍵が無効化され、暗号化ファイルにアクセスできません。
ローカル キャッシュの状態 **転送できるデータ パケット**	SafeGuard Enterprise Server に送信するパッケージがあるかどうかを表示します。
Local Self Help (LSH) の状態 **有効** **アクティブ**	ポリシーで Local Self Help が有効になっているか、また、ローカルコンピュータでアクティブ化されているかを示します。
証明書を変更する準備ができました	このメッセージは、セキュリティ担当者が、トークンでログオンするための新しい証明書をコンピュータに割り当てた場合に表示されます。これで、トークンを使用したログオンの証明書を変更できます。詳細は、SafeGuard Enterprise 8.0 ユーザーヘルプを参照してください。

- **ヘルプ**: SafeGuard Enterprise ユーザーヘルプを開きます。
- **SafeGuard Enterprise のバージョン情報**: SafeGuard Enterprise のバージョン情報が表示されます。

4 操作方法

4.1 コンピュータの BitLocker 暗号化

エンドポイントに対してセキュリティ担当者が指定したログオンモードによって、SafeGuard Enterprise の BitLocker 対応機能は多少異なります。

いずれの場合も、暗号化の実行、または後で実行することを選択するダイアログが表示されます。

保存、再起動または暗号化を選択した場合でも、すぐに暗号化が実行されるわけではありません。SafeGuard Enterprise BitLocker 暗号化の要件を満たすようにハードウェアの検証が実行されます。システムが再起動し、ハードウェア要件が満たされているかどうかチェックされます。たとえば、TPM または USB メモリが利用できない場合や、接続されていない場合は、別のデバイスに外部キーを格納するようメッセージが表示されます。またユーザーが正しいログイン情報を入力できるシステム環境であるかどうかもチェックされます。正しいログイン情報を入力できない場合、コンピュータは起動しますが、暗号化は開始されません。PIN またはパスワードの再入力が求められます。ハードウェアの検証が完了すると、BitLocker 暗号化が開始されます。

「**後で再起動**」を選択すると、暗号化は開始されず、次の条件が満たされるまで、このボリュームの暗号化を促すダイアログは表示されません。

- 新しいポリシーが適用された。
- いずれかのボリュームの BitLocker 暗号化のステータスが変更された。
- システムに再度ログオンした。

4.1.1 スタートアップ キーの保存

ログインモードがセキュリティ担当者によって「**TPM + スタートアップキー**」または「**スタートアップキー**」に設定されている場合、スタートアップキーの保存先を指定する必要があります。スタートアップ キーの保存先として、暗号化されていない USB メモリを推奨します。スタートアップ キーの有効な保存先ドライブの一覧がダイアログに表示されます。保存後、コンピュータを起動するたびに、スタートアップ キーが保存されたストレージデバイスを挿入する必要があります。

対象ドライブを選択して、「**保存＆再起動**」をクリックします。

4.1.2 パスワードの設定

セキュリティ担当者がログオンモードとして「**パスワード**」を指定した場合、新しいパスワードの入力と確認入力が必要です。コンピュータを起動するたびに、このパスワードを入力する必要があります。パスワードの文字数や複雑さの条件は、セキュリティ担当者が設定したグループ ポリシー オブジェクトに依存します。パスワードの条件は、ダイアログに表示されます。

注
PIN や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。

4.1.3 PIN の設定

セキュリティ担当者がログオンモードに「**TPM + PIN**」を設定している場合、新しい PIN の入力と確認入力が必要です。コンピュータを起動するたびに、この PIN を入力する必要があります。文字数や複雑さの条件は、セキュリティ担当者が設定したグループ ポリシー オブジェクトに依存します。PIN の条件は、ダイアログに表示されます。

注
PIN や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。

4.1.4 TPM モードで表示されるダイアログ

セキュリティ担当者がログオンモードとして「**TPM**」を指定した場合、エンドポイントの再起動と暗号化を確認するだけです。

4.2 BitLocker の PIN/パスワードを忘れた場合のリセット

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。復旧鍵をリクエストする方法は次のとおりです。

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。
   「**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 SafeGuard Management Center 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。

再度システムにログオンしたら、ただちに新しい BitLocker のログオン情報を設定します。OS 環境によって異なりますが、ログオン情報のリセットのダイアログが表示されます。このダイアログが自動的に表示されない場合は、タスクバーにある Sophos SafeGuard アイコンを右クリックして、「**BitLocker のログオン情報のリセット**」を選択し、画面に表示される指示に従ってください。

4.3 BitLocker の PIN/パスワードを忘れた場合のリセット (チャレンジ/レスポンスを使用)

チャレンジ/レスポンス

BitLocker の復旧鍵を取得することが必要な場合は、次の手順を実行します。

1. PC を再起動します。再起動後、黄色のメッセージが表示されます。3秒以内に、いずれかのキーを押します。
2. ソフォスのチャレンジ/レスポンス画面が表示されます。
3. ステップ 2 に、ヘルプデスク担当者の連絡先が表示されます。
4. ヘルプデスク担当者に次の情報を提供します。
   - **コンピュータ**: Sophos¥<コンピュータ名> など
   - **チャレンジ** コード: ABC12-3DEF4-56GHO-892UT-Z654K-LM321 など。スペル支援を表示するには、文字の上にマウスを移動します。また、「**F1**」キーを数回押しても表示できます。チャレンジコードは 30分で期限切れになり、PC は自動的にシャットダウンします。
5. ヘルプデスク担当者から入手した「**レスポンス コード**」を入力します (ブロックが 6つあり、各ブロックにテキストフィールドが 2つあります。各フィールドには 5文字ずつ入力します)。
   - 1つのテキストフィールドに 5文字入力したら、フォーカスが自動的に次のテキストフィールドに移ります。
   - ブロックに誤って不正な文字を入力した場合、そのブロックは赤でハイライト表示されます。
6. レスポンス コードの入力に成功したら、「**続行**」をクリックするか、「**Enter**」キーを押して、チャレンジ/レスポンス操作を完了します。

BitLocker のログオン情報のリセット

再度システムにログオンしたら、ただちに新しい BitLocker のログオン情報を設定します。OS 環境によって異なりますが、ログオン情報のリセットのダイアログが表示されます。このダイアログが自動的に表示されない場合は、タスクバーにある Sophos SafeGuard アイコンを右クリックして、「**BitLocker のログオン情報のリセット**」を選択し、画面に表示される指示に従ってください。

4.4 ポリシーに基づいたすべてのファイルの暗号化

File Encryption ポリシーをコンピュータに適用すると、そのポリシーで指定されている場所に以前からあるファイルは自動で暗号化されません。初期暗号化を実行する必要があります。

コンピュータに File Encryption ポリシーが適用されたら、すぐに初期暗号化を実行することを推奨します。なお、この暗号化タスクはセキュリティ担当者が自動的に開始することもあります。

暗号化処理を手動で開始するには、Windows エクスプローラで「**PC**」ノードを右クリックして、「**SafeGuard ファイル暗号化 > ポリシーに基づいて暗号化**」を選択します。SafeGuard ファイル暗号化ウィザード (p. 12) の指示に従って、定義済みの暗号化ルールが適用されているフォルダやサブフォルダ内のファイルすべてを暗号化します。

4.4.1 SafeGuard ファイル暗号化ウィザード

SafeGuard ファイル暗号化のウィザードを開くには、Windows エクスプローラで「**PC**」ノードまたはフォルダを右クリックして、「**SafeGuard ファイル暗号化 > ポリシーに基づいて暗号化**」を選択します。

コンピュータに適用済みの暗号化ルールで指定されているすべてのフォルダがチェックされます。

- 暗号化の対象となっているファイルが平文の場合は、ルールで定義されている鍵を用いて暗号化されます。
- 暗号化済みのファイルが、ルールと異なる鍵を使って暗号化されている場合は、ルールで定義されている鍵を用いて再暗号化されます。
- ユーザーが鍵を所有していない場合はエラーが表示されます。
- 適用されている暗号化ポリシーで暗号化対象外とされているファイルが暗号化されている場合、暗号化は解除されません。

処理のステータスを示す画像は次のように色分けされます。

- **緑色:** 操作が正常に完了した状態です。
- **赤色:** 操作が完了したもののエラーが発生した状態です。
- **黄色:** 操作が進行中の状態です。

処理されたファイルに関する詳細情報は、次の 4つのタブに表示されます。

- **サマリー**: 検出ファイル数または処理済みファイル数が表示されます。「**エクスポート...**」ボタンを使用すると、処理された各ファイルとその結果の一覧を XML 形式のファイルに出力できます。
- **エラー**: 正常に処理できなかったファイルが表示されます。
- **変更済み**: 正常に変更されたファイルが表示されます。
- **すべて**: 処理されたすべてのファイルとその結果が表示されます。

画面右上の「**停止**」ボタンをクリックすると、操作が中止します。「**停止**」ボタンが「**再起動**」に変わるので、処理を開始するときにクリックします。

操作中にエラーが発生した場合は、「**停止**」ボタンが「**再試行**」ボタンに変わります。「**再試行**」ボタンをクリックすると、失敗したファイルに対してのみ処理が再開されます。

4.5 ファイルの手動暗号化/復号化

SafeGuard File Encryption では、個々のファイルを手動で暗号化/復号化できます。ファイルを右クリックし、「**SafeGuard ファイル暗号化**」を選択します。アクセスできる機能は次のとおりです。

- **暗号化の状態の表示**: ファイルが暗号化されているかどうか、および使用された鍵が表示されます。
- **ポリシーに基づいて暗号化**: 詳細は、ポリシーに基づいたすべてのファイルの暗号化 (p. 12)を参照してください。
- **復号化**: (ロケーションベースのファイル暗号化のみ): File Encryption ルールが適用されていないファイルを復号化できます。
- **選択したファイルの復号化** (アプリケーションベースのファイル暗号化のみ): ファイルを復号化して、平文で保存できます。ファイルの復号化は、機密データが含まれていない場合のみに実行することを推奨します。
- **選択したファイルの暗号化** (アプリケーションベースのファイル暗号化のみ): ポリシーで指定されている鍵を使用して、ファイルを手動で暗号化できます。
- **ファイルのパスワード保護**: 個々のファイルに手動でパスワードを設定して暗号化できます。これは、社外のユーザーとファイルを安全に共有する際に便利です。詳細は、暗号化されたファイルのメール送信 (p. 15)を参照してください。

フォルダまたはドライブを右クリックすると、次のオプションが表示されます。

- **暗号化の状態の表示**: フォルダやドライブに含まれるファイル、暗号化の状態を示すアイコン、使用されている鍵を一覧表示します。
- **ポリシーに基づいて暗号化**: 詳細は、ポリシーに基づいたすべてのファイルの暗号化 (p. 12)を参照してください。

以下のオプションは、Cloud Storage および Data Exchange を使用している場合のみに表示されます。

- **デフォルトの鍵**: ボリュームに (保存、コピーまたは移動により) 追加される新規ファイルに対して、現在使用している鍵を示します。デフォルトの鍵は、ボリュームやリムーバブル メディアごとに個別に設定できます。
- **デフォルトの鍵を設定する**: 別のデフォルトの鍵を設定するためのダイアログを開きます。
- **新しい鍵の作成**: ユーザー定義のローカル鍵を作成するためのダイアログを開きます。
- **暗号化の再有効化**: セキュリティ担当者によって許可されている場合は、コンピュータに接続しているリムーバブルメディア上のファイルを暗号化するかどうかをユーザーが選択できます。リムーバブル メディアをコンピュータに接続すると、メディア上のファイルを暗号化するかどうかを確認するメッセージが表示されます。また、セキュリティ担当者によって許可されている場合は、ここでの選択を保存するか確認メッセージが表示されます。「**この設定を保存し、次回からこのダイアログを表示しない**」を選択すると、該当するメディアに対して確認メッセージが再度表示されません。また、Windows エクスプローラで、対象のデバイスを右クリックすると、新しいメニュー「**暗号化の再有効化**」が表示されるようになります。暗号化の設定を元に戻す場合は、このメニューを選択します。デイバイスへの十分な権限がないなどの理由で選択できない場合は、エラーメッセージが表示されます。設定を元に戻すと、当該のデバイスに対する設定を確認するメッセージが再び表示されます。

4.6 ファイル暗号化の対象の場所の表示

コンピュータの暗号化対象の場所、およびファイルの保護に使用されている鍵は、SafeGuard Enterprise FETool ツールを使用して表示できます。

SafeGuard Enterprise FETool ツールを起動するには、コマンドプロンプトを開き、C:¥Program Files (x86)¥Sophos¥SafeGuard Enterprise¥FileEncryption で、fetool rli -a と入力します。

このコマンドを入力すると、コンピュータに適用されている暗号化ルールの一覧が表示されます。リストには、暗号化モード、該当するフォルダへのフルパス、および使用されている鍵が表示されます。

4.7 ファイルのパスワード保護

社外のユーザーにメールを送信する際は、パスワードを使用してファイルを暗号化することを推奨します。この場合、SafeGuard Enterprise がインストールされていなくても、受信者は、暗号化されたファイルにアクセスできます。

以下の手順を実行してください。

1. 送信するファイルを右クリックして、「**ファイルのパスワード保護**」を選択します。
2. 画面上の指示に従って、パスワードを作成します。パスワードは、推測されにくいものを選び、添付ファイルと同じメールで送信しないことを推奨します。
   ファイルは暗号化され、HTML ファイルとして保存されます。この HTML ファイルは、添付ファイルとして安全に送信できます。

注

- 暗号化するためには十分なディスク領域が必要です。
- 暗号化された HTML ファイルのファイルサイズは、元のファイルより大きくなります。
- 対応しているファイルサイズの最大は 50MB です。
- 一度に複数のファイルを送信する場合は、ZIP ファイルとして圧縮した後、その圧縮ファイルを暗号化できます。

3. パスワードは、電話やその他の方法で受信者に通知します。
   受信者は、次のいずれかのブラウザを使用して、パスワード保護された添付ファイルを開くことができます。
   - Mozilla Firefox
   - Google Chrome
   - Microsoft Internet Explorer 11
   - Microsoft Edge
4. ファイルをダブルクリックし、画面に表示される指示に従って、次のいずれかの操作を実行するよう、受信者に伝えます。
   - パスワードを入力し、「**Enter**」をクリックしてファイルにアクセスします。
   - 「**新しいファイルをパスワード保護する**」をクリックして、別のファイルをパスワード保護します。

これで受信者は、パスワード保護されたファイルにアクセスできます。受信者は、返信するファイルをパスワード保護することもできます。その際、同じパスワードを使用するか、または新しいパスワードを作成することができます。さらに、別のファイルをパスワード保護することもできます。

4.8 暗号化されたファイルのメール送信

暗号化されたファイルを社内のユーザーに送信する際、暗号化や復号化を手動で行う必要はありません。適切な鍵がある受信者は、ファイルの内容を読むことができます。

社外のユーザーにメールを送信する際は、SafeGuard Enterprise にある Microsoft Outlook のアドインを使用すると、メールの添付ファイルを簡単に暗号化できます。1つまたは複数のファイルを添付してメールを送信する場合、添付ファイルの送信方法を選択するダイアログが表示されます。表示されるオプションは、メールに添付したファイルの暗号化の状態に依存します。

注
連絡先 (.vcf) またはメール (.msg) など、埋め込まれた項目を添付ファイルとして送信する際、暗号化を促すダイアログは表示されません。暗号化されずに送信されます。

- **パスワード保護する**

  組織外のユーザーに機密ファイルを送信する場合は、このオプションを選択します。

  パスワードを設定後、「送信」をクリックすると、ファイルは暗号化され、HTML ファイルとして保存されます。複数のファイルを一度にパスワード保護すると、各ファイルは同じパスワードで個別に暗号化されます。既に暗号化されているファイルは、まず自動的に復号化され、その後パスワード保護されます。

受信者は、パスワードの通知を受けるとファイルを Web ブラウザで開くことができます。パスワードは、推測されにくいものを選び、添付ファイルと同じメールで送信しないことを推奨します。パスワードは、電話やその他の方法で受信者に通知することを推奨します。

受信者は、次のいずれかのブラウザを使用して、パスワード保護された添付ファイルを開くことができます。

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11
- Microsoft Edge

モバイルサポートなど、これ以外のブラウザを使用できる場合もありますが推奨されません。

受信者は、ファイルを編集後、同じパスワードまたは新しいパスワードを使用して返信できます。さらに、別のファイルをパスワード保護することもできます。操作は、ブラウザのウィザードの指示に従って実行します。詳細は、ソフォスのサポートデータベースの文章 124440 を参照してください。

ファイルを手動でパスワード保護することもできます。詳細は、ファイルのパスワード保護 (p. 14)を参照してください。

- **パスワード保護しない**

  このオプションは、メールの添付ファイルに機密データが含まれていない場合のみに選択することを推奨します。メールの添付ファイルをパスワード保護せずに送信した場合、ログに記録され、セキュリティ担当者によって監視されることがあります。

- **送信する添付ファイルは変更されていません**

  パスワード保護できない添付ファイルがメールに含まれている場合、変更なしで送信するか、メールから削除します。次のいずれかの理由でパスワード保護できないファイルの一覧がダイアログに表示されます。

  - ファイルは既にパスワード保護されています。ファイルを復号化してから新しいパスワードで保護するか、または、変更なしでファイルを送信後、該当するパスワードを受信者に通知します。
  - ファイルは、現在、鍵リングにない鍵で暗号化されています。セキュリティに問題があるか、またはファイルの暗号化に使用された鍵を所有していないため、鍵が一時的に無効になることがあります。この場合は、セキュリティ担当者までお問い合わせください。

社外と社内のユーザーに同時にメールを送信する場合、社外のドメインのみに送信されたものとして処理されます。

4.9 ローカル鍵の作成

ローカル鍵は、リムーバブルデバイスやクラウド ストレージ サービス上の指定されている場所のファイルを暗号化する際に使用します。このようなフォルダは、暗号化ポリシーで事前に指定しておく必要があります。

ローカル鍵を作成する方法は次のとおりです。

1. Windows タスクバーの Sophos SafeGuard のシステムトレイ アイコンを右クリックするか、ボリューム/フォルダ/ファイルを右クリックします。
2. 「**新しい鍵の作成**」をクリックします。
3. 「**鍵の作成**」ダイアログで、鍵の「**名前**」と「**パスフレーズ**」を入力します。

   鍵の内部名が下のフィールドに表示されます。

4. パスフレーズを確認入力します。

   安全でないパスフレーズを入力すると、警告メッセージが表示されます。セキュリティレベルを高めるには、複雑なパスフレーズを使用することを推奨します。警告メッセージを無視して、入力したパスフレーズを使用することもできます。パスフレーズは、社内ポリシーにも準拠している必要があります。そうでない場合は、警告メッセージが表示されます。

5. ショートカットメニューを使用してダイアログを開いた場合は、「**次のパスに対する新しいデフォルトの鍵として使用する**」オプションが表示されます。「**次のパスに対する新しいデフォルトの鍵として使用する**」オプションを選択すると、この新しい鍵を、ボリュームや Cloud Storage の同期フォルダのデフォルトの鍵としてすぐに設定できます。

   ここで指定するデフォルトの鍵は、通常の暗号化処理に使用されます。別の鍵を設定しない限り、この鍵が使用されます。

6. 「**OK**」をクリックします。

   鍵が作成され、データが SafeGuard Enterprise Server と正常に同期されるとすぐに使用可能になります。

   この鍵をデフォルトの鍵として定義した場合、これ以降、リムーバブル ストレージ メディアや Cloud Storage の同期フォルダにコピーされるデータはすべて、この鍵を使用して暗号化されます。

受け取り側がリムーバブル ストレージ メディア上のデータすべてを復号化できるようにするには、ローカルで作成した鍵を使用してデバイス上のデータを再度暗号化する必要があります。これを行うには、Windows エクスプローラでそのデバイスのショートカット メニューから、「**SafeGuard ファイル暗号化 > ポリシーに基づいて暗号化**」を選択します。必要なローカル鍵を選択し、データを暗号化します。メディア パスフレーズを使用する場合、この操作は必要ありません。

4.9.1 ファイルから鍵をインポートする方法

暗号化されたデータを含むリムーバブル メディアを受け取った場合や、ユーザー定義のローカル鍵を使用して暗号化された共有フォルダ内の Cloud Storage データにアクセスする場合、復号化に必要な鍵を自分の秘密鍵リングにインポートできます。

鍵をインポートするには、適切なパスフレーズが必要です。データを暗号化した人から、パスフレーズを入手してください。

1. リムーバブルメディア上のファイルを選択し、「**SafeGuard ファイル暗号化 > ファイルから鍵をインポートする**」をクリックします。
2. 表示されるダイアログで、パスフレーズを入力します。

鍵がインポートされ、ファイルにアクセスできるようになりました。

4.10 SafeGuard Data Exchange を使用したデータの交換

SafeGuard Data Exchange を使用して安全なデータ交換を行う一般的な例は次のとおりです。

- 自分の鍵リングにあるものと同じ鍵を少なくとも 1つ持っている SafeGuard Enterprise ユーザーとデータを交換する場合。

  この場合、受け取り側の (ノート PC などの) 鍵リングにも含まれている鍵を使用して、リムーバブル メディア上のデータを暗号化します。受け取り側はこの鍵を使用して、暗号化されたデータに透過的にアクセスできます。

- 自分と同じ鍵を持っていない SafeGuard Enterprise ユーザーとデータを交換する場合。

この場合は、ローカル鍵を作成し、この鍵を使用してデータを暗号化します。ローカルで作成された鍵は、パスフレーズによって保護され、SafeGuard Enterprise でインポートすることができます。データの受け取り側にパスフレーズを提供します。受け取り側は、パスフレーズを使用して鍵をインポートし、データにアクセスすることができます。

- SafeGuard Enterprise を使用していないユーザーとデータを交換する場合。

  コンピュータに SafeGuard Enterprise がインストールされていないユーザーは、SafeGuard Portable を使用して暗号化されたファイルにアクセスできます。SafeGuard Portable は Mac には対応していません。詳細は、次のリンクを参照してください。

  — リムーバブル メディア上のデータの交換 (SafeGuard Enterprise なし) (p. 20)

  — SafeGuard Portable を使用したファイルの編集 (p. 23)

4.10.1 SafeGuard Data Exchange を使用したリムーバブル メディアの暗号化

リムーバブル メディアにある暗号化されていないデータの暗号化は、メディアをシステムに取り付けるとすぐに自動的に開始されます。開始されない場合は、手動で処理を開始する必要があります。リムーバブル メディア上のファイルを暗号化するかを決定する権限がユーザーにある場合、コンピュータにリムーバブル メディアを取り付けると、暗号化の実行に関するプロンプト指示が表示されます。

暗号化処理を手動で開始する方法は次のとおりです。

1. Windows エクスプローラのショートカット メニューで、「**SafeGuard ファイル暗号化 > ポリシーに基づいて暗号化**」を選択します。特定の鍵が定義されていない場合は、鍵を選択するためのダイアログが表示されます。
2. 鍵を選択し、「**OK**」をクリックします。リムーバブル メディアに含まれているすべてのデータが暗号化されます。

   他の鍵をデフォルトとして設定しない限り、デフォルトの鍵が使用されます。デフォルトの鍵を変更した場合は、変更後にコンピュータに接続するリムーバブルメディアの初期暗号化に対して新しい鍵が使用されます。

注
コンピュータに SafeGuard Enterprise をインストールしているものの、同じ鍵を使用していないユーザーとデータを交換するには、ローカル ユーザーが生成した鍵、またはメディア パスフレーズが必要です。このような鍵は、SafeGuard Enterprise を使用していないユーザーとの安全なデータ交換にも必要です。ローカル鍵は、プレフィックス (Local_) で識別できます。

「**平文ファイルを暗号化し、暗号化されたファイルを更新する**」が選択されている場合、既存の鍵で暗号化されているファイルは復号化され、新しい鍵を使用して再度暗号化されます。

初期暗号化をキャンセルする

初期暗号化が自動的に開始するように設定されている場合は、初期暗号化をキャンセルする権限が与えられていることがあります。この場合、「**キャンセル**」ボタンが有効になっており、「**開始**」ボタンが表示され、暗号化処理の開始が 30秒間遅延されます。この時間内に「**キャンセル**」ボタンをクリックしなければ、30秒後に初期暗号化が自動的に開始されます。「**開始**」ボタンをクリックすると、初期暗号化がすぐに開始されます。

メディア パスフレーズを使用した初期暗号化

メディア パスフレーズの使用がポリシーで指定されている場合は、初期暗号化を行う前にメディア パスフレーズを入力するように求められます。メディア パスフレーズは、ユーザーの使用するリムーバブル メディアすべてに対して有効で、ユーザーのコンピュータやログオン権限のあるコンピュータすべてに結び付けられます。

メディア パスフレーズを入力すると、初期暗号化が自動的に開始します。

メディア パスフレーズを一度入力すると、コンピュータに別のデバイスを接続するたびに初期暗号化が自動的に開始されます。

メディア パスフレーズが指定されていないコンピュータで初期暗号化は開始されません。

4.10.2 メディア パスフレーズの使用

ポリシーによって指定されている場合、SafeGuard Data Exchange の初回インストール後にリムーバブル デバイスを接続すると、メディア パスフレーズを入力するように求められます。

ダイアログが表示されたら、メディア パスフレーズを入力してください。このシングル メディア パスフレーズを使用して、ファイルの暗号化に使用された鍵に関係なく、リムーバブル メディア上の暗号化されたファイルすべてにアクセスできます。

このメディア パスフレーズは、そのコンピュータに接続するデバイスすべてに対して有効です。メディア パスフレーズは、SafeGuard Portable でも使用でき、ファイルの暗号化に使用された鍵に関係なく、すべてのファイルへのアクセスを許可します。

Mac ではメディア パスフレーズを使用できないことに注意してください。

メディア パスフレーズの変更/リセット

システム トレイ アイコンのメニューから「**メディア パスフレーズの変更**」を使用して、いつでもメディア パスフレーズを変更できます。ダイアログが表示され、ここで古いメディア パスフレーズと新しいメディア パスフレーズを入力し、新しいメディア パスフレーズを確認のために再度入力します。

メディア パスフレーズを忘れた場合は、それをリセットするためのオプションがこのダイアログに表示されます。「**メディア パスフレーズをリセットする**」オプションを選択して「**OK**」をクリックすると、次回ログオン時にメディア パスフレーズがリセットされることが通知されます。

今すぐログオフし、再度ログオンしてください。コンピュータ上にメディア パスフレーズがないことが表示され、新しいメディア パスフレーズを入力するように求められます。

メディア パスフレーズの同期

デバイスにあるメディア パスフレーズと、コンピュータにあるメディア パスフレーズは、自動的に同期されます。コンピュータ上のメディア パスフレーズを変更し、まだ古いバージョンのメディア パスフレーズを使用しているデバイスを接続した場合は、メディア パスフレーズが同期されたことが表示されます。これは、ユーザーがログオン権限のあるコンピュータすべてに共通しています。Mac ではメディア パスフレーズを使用できないことに注意してください。

メディア パスフレーズの変更後は、すべてのリムーバブル メディアをコンピュータに接続するようにしてください。これにより、新しいメディア パスフレーズが、すべてのデバイスですぐに使用されること (パスフレーズの同期) が保証されます。

4.10.3 リムーバブル メディア上のデータの交換 (SafeGuard Enterprise なし)

SafeGuard Portable を使用すると、受け取り側のコンピュータに SafeGuard Enterprise がインストールされていない場合でも、リムーバブル メディア上の暗号化されたデータを交換することができます。

注
SafeGuard Portable は Mac、または Sophos SafeGuard がインストールされているコンピュータには対応していません。

SafeGuard Data Exchange で暗号化されたデータは、SafeGuard Portable を使用して暗号化/復号化できます。SGPortable.exe というプログラムが、リムーバブル メディアに自動的にコピーされます。

SafeGuard Portable と関連するメディア パスフレーズを併用することで、どのローカル鍵が暗号化に使用されたかに関係なく、暗号化されたファイルすべてにアクセスできます。ローカル鍵のパスフレーズの場合、その鍵を使用して暗号化されたファイルだけにアクセスできます。

受け取り側は、必要なメディア パスフレーズまたはローカル鍵のパスフレーズを受け取ったら、暗号化されたデータを復号化し、再暗号化できます。SafeGuard Data Exchange で作成された既存の暗号化鍵を使用するか、SafeGuard Portable で新しい鍵を作成することができます (新規ファイルの場合など)。

SafeGuard Portable は、受け取り側のコンピュータにインストールする必要はありません。リムーバブル メディアにある状態で使用できます。

詳細は、SafeGuard Portable を使用したファイルの編集 (p. 23)を参照してください。

4.10.4 SafeGuard Data Exchange で CD/DVD にファイルを書き込む方法

SafeGuard Data Exchange では、Windows の CD 書き込みウィザードを使って、暗号化されたファイルを CD/DVD に書き込むことができます。セキュリティ担当者は、CD ドライブに対して暗号化ルールを指定する必要があります。CD ドライブに対して暗号化ルールが指定されていない場合、ファイルは常に平文で CD に書き込まれます。

CD 書き込みウィザード用の SafeGuard Disc Burning Extension は、**マスタ**形式で CD/DVD に書き込む場合のみに使用できます。ライブ ファイル システム形式の場合、書き込みウィザードは必要ありません。この場合、記録ドライブは他のリムーバブル メディアと同じように使用されます。記録ドライブに対して暗号化ルールが設定されている場合、ファイルは CD/DVD にコピーされるときに自動的に暗号化されます。

CD 書き込みウィザードで、CD へのファイルの書き込み方法 (暗号化または平文) を指定できます。CD の名前を入力した後、「SafeGuard Removable Disk Burning Extension」が表示されます。

「**統計**」の下に、次の情報が表示されます。

- CD に書き込むように選択されたファイルの数
- 選択されたファイルのうち暗号化されているファイルの数
- 選択されたファイルのうち平文ファイルの数

「**状態**」の下に、すでに暗号化されたファイルを暗号化するために使用した鍵が表示されます。

CD に書き込むファイルの暗号化には、CD ドライブの暗号化ルールで指定されている鍵が常に使用されます。

CD ドライブの暗号化ルールが変更された場合は、CD に書き込むファイルが、異なる鍵で暗号化されることがあります。ファイルの追加時に暗号化規則が無効になっていた場合、関連する平文ファイルは CD にコピーされるファイルのフォルダ内にあります。

CD にあるファイルの暗号化

CD にファイルを書き込むとき暗号化する場合は、「**すべてのファイルの (再) 暗号化**」をクリックします。

必要に応じて、すでに暗号化されたファイルは再暗号化され、平文ファイルは暗号化されます。CD 上で、ファイルは CD ドライブの暗号化ルールで指定された鍵を使用して暗号化されます。

CD にファイルを平文として書き込む方法

「**すべてのファイルの復号化**」を選択した場合、ファイルは復号化されてから CD に書き込まれます。

SafeGuard Portable を光学メディアにコピーする方法

このオプションを選択すると、SafeGuard Portable も CD にコピーされます。これにより、SafeGuard Data Exchange がインストールされていなくても、SafeGuard Data Exchange で暗号化されたファイルを読み取り、編集することができるようになります。

4.11 クラウドにあるデータの交換 (SafeGuard Enterprise なし)

SafeGuard Portable を使用すると、受け取り側のコンピュータに SafeGuard Enterprise がインストールされていない場合でも、クラウド上の暗号化されたデータを交換することができます。

SafeGuard Portable を使用すると、コンピュータに SafeGuard Enterprise がインストールされていない場合でも、クラウドストレージ内の暗号化されたデータにアクセスすることができます。SafeGuard Cloud Storage で暗号化されたデータは、SafeGuard Portable を使用して暗号化/復号化できます。SafeGuard Portable の起動には SGPortable.exe が必要ですが、このファイルは同期フォルダに自動的にコピーされます。

ローカル鍵のパスフレーズがある場合、その鍵を使用して暗号化されたファイルだけにアクセスできます。受け取り側は、暗号化されたデータを復号化し、再び暗号化できます。ローカル鍵のパスフレーズは、事前に受け取り側に伝えておく必要があります。

受け取り側は、既存の暗号化鍵を使用するか、SafeGuard Portable で新しい鍵を作成することができます (新規ファイルの場合など)。

SafeGuard Portable は、受け取り側のコンピュータにインストールしたりコピーしたりする必要はありません。クラウドストレージ上に残ります。

SafeGuard Portable の使用方法について、詳細は、SafeGuard Portable を使用したファイルの編集 (p. 23)を参照してください。

ファイルをダブルクリックしたり、「開く」メニューを選択したりしても、ファイルが直ちに復号化されることはありません。これは、クラウドストレージの同期フォルダにある復号化されたファイルは、自動的にクラウドと同期されるためです。このような操作を実行すると、ファイル

の安全な保存場所を選択するダイアログが表示されます。復号化されたファイルは、SafeGuard Portable の終了時に自動的にワイプされません。SafeGuard Portable を使用して復号化した Cloud Storage のファイルに変更を加えた場合、変更内容は元の暗号化ファイルに反映されません。

注
クラウドストレージの同期フォルダは、リムーバブルメディアやネットワークに保存しないでください。そのようにした場合、SafeGuard Portable で暗号化されていないファイルが同期フォルダに保存されます。

4.12 デフォルト鍵の使用

デフォルトの鍵を定義すると、SafeGuard Data Exchange や SafeGuard Cloud Storage の暗号化処理で使用する既定の鍵が指定されます。

セキュリティ担当者は、Cloud Storage に対するデフォルトの鍵の使用を許可する必要があります。許可されている場合、あらかじめ定義されている鍵のリストからデフォルトの鍵を選択して、クラウドストレージ内のフォルダを暗号化する際に使用できます。

次の場所のショートカット メニューからデフォルトの鍵を定義できます。

- リムーバブル メディア
- リムーバブル メディア上のファイル
- Cloud Storage の同期フォルダまたはサブフォルダ
- Cloud Storage の同期フォルダまたはサブフォルダに保存されているファイル
- また、「**鍵の作成**」ダイアログで新しいローカル鍵を作成するときに、ただちにその鍵をデフォルトに指定することもできます。

デフォルトの鍵を定義するには、「**SafeGuard ファイル暗号化 > デフォルトの鍵を設定する**」を選択します。

このダイアログで選択した鍵は、以後、このリムーバブル ストレージ メディア上、または Cloud Storage の同期フォルダ内で行われる暗号化処理すべてに使用されます。別の鍵を使用する場合は、いつでもデフォルトの鍵を新たに設定できます。

Cloud Storage の暗号化にローカル鍵を選択した場合は、SafeGuard Portable が Cloud Storage の同期フォルダにコピーされます。

ここで暗号化したファイルを、Sophos Secure Workspace をインストールした Android デバイスや iOS デバイスで読むためには、暗号化の際、ローカル鍵を使用する必要があります。詳細は、Sophos Secure Workspace ユーザーヘルプを参照してください。

例

たとえば、「Dropbox」を使用して複数の取引先と安全にデータを共有する際、各取引先ごとに特定のサブフォルダ 1つのみにアクセスを許可する場合を想定します。このような場合、サブフォルダごとに異なるデフォルトの鍵を設定するだけでアクセス許可を設定できます。デフォルトの鍵を設定すると、SafeGuard Enterprise によって各サブフォルダに SafeGuard Portable が自動的に追加されるため、取引先は SafeGuard Cloud Storage なしでサブフォルダ内の暗号化データにアクセスできます。取引先には鍵を使用するためのパスフレーズを通知します。SafeGuard Portable とパスフレーズを使用すると、サブフォルダ内に用意されているデータを復号化できます。ただし、サブフォルダごとに異なる鍵で暗号化されているため、他のサブフォルダのデータにはアクセスできません。

4.13 暗号化ファイルの復旧

ファイルの暗号化に使用された鍵が鍵リングに含まれていない場合、そのファイルを開くことはできません。鍵を所有していない理由として、ファイルへのアクセスが企業ポリシーで許可されていないことが考えられます。また、許可されてはいるものの、何らかの理由で、必要な鍵を所有していない可能性もあります。この場合、使用された鍵を特定して、それを鍵リングに割り当てるようセキュリティ担当者に依頼する必要があります。次の手順を実行します。

1. ファイルを右クリックして、「**SafeGuard ファイル暗号化 > 暗号化の状態の表示**」をクリックします。
   このファイルの暗号化に使用された鍵が表示されます。
2. セキュリティ担当者に鍵名を提供します。
3. この鍵を鍵リングに割り当てるようにセキュリティ担当者に依頼します。
4. ユーザーポリシーが更新されたという通知をセキュリティ担当者から受けたら、コンピュータのタスクバーにある Sophos SafeGuard システム トレイ アイコンを右クリックします。
5. 「**同期**」をクリックします。
6. 再びシステム トレイ アイコンを右クリックして、「**状態**」をクリックします。
   コンピュータに前回鍵が転送された日時が表示されます。「**前回鍵を受信した日時**」に、要求した鍵が鍵リングに追加された日時が表示されます。

これでファイルにアクセスできます。

4.14 SafeGuard Enterprise サーバーへの接続の確認

エンドポイントとサーバーの同期で問題が発生している場合は、Client/Server Connectivity Check ツールを使用して、エンドポイントと SafeGuard サーバー間の通信に失敗する原因を解析できます。

SafeGuard Enterprise Client/Server Connectivity Check ツールを起動するには、C:¥Program Files (x86)¥Sophos¥SafeGuard Enterprise¥Client にある SGNCSCC.exe アプリケーションをクリックします。

詳細は、ソフォスのサポートデータベースの文章 109662 を参照してください。

4.15 SafeGuard Portable を使用したファイルの編集

Sophos SafeGuard ユーザーは、SafeGuard Portable を使用する必要はありません。以下の説明は、ユーザーのコンピュータに Sophos SafeGuard がインストールされていないため、暗号化されたデータを SafeGuard Portable を使って編集する必要がある場合を想定しています。

SafeGuard Data Exchange を使用して暗号化されたファイルと、SGPortable というフォルダを受け取りました。このフォルダには SGPortable.exe ファイルが含まれています。

1. SGPortable.exe をダブルクリックして、SafeGuard Portable を起動します。

   SafeGuard Portable を使用して、暗号化されたデータを復号化し、再び暗号化することができます。

SafeGuard Portable には、ファイルの詳細情報の他に、「**鍵**」列が表示されます。この列には、データが暗号化されているかが表示されます。ファイルが暗号化されている場合は、使用された鍵の名前も表示されます。使用された鍵に関連したパスフレーズを知っている場合のみ、ファイルを復号化できます。

2. ファイルを編集するには、ファイルを右クリックして、次のいずれか 1つのコマンドを実行します。

暗号化鍵の設定	「**鍵の入力**」ダイアログを開きます。このダイアログで、SafeGuard Portable を使用して暗号化鍵を生成できます。
暗号化	前回使用された鍵でファイルを暗号化します。
復号化	「**パスフレーズの入力**」ダイアログを開いて、選択したファイルを復号化するためのパスフレーズを入力します。
暗号化の状態	ファイルの暗号化の状態を表示します。
コピー先	選択ファイルを指定した任意のフォルダにコピーし、復号化します。
削除	選択したファイルを削除します。

ツール バーにあるアイコンを使用して、「**開く**」、「**削除**」、「**暗号化**」、「**復号化**」、および「**コピー**」の各コマンドを選択することもできます。

4.15.1 SafeGuard Portable 用の暗号化鍵の設定

SafeGuard Portable 用の暗号化鍵を設定する方法は次のとおりです。

1. ショートカット メニューまたは「**ファイル**」メニューから、「**暗号化鍵の設定**」を選択します。

   「**鍵の入力**」ダイアログが表示されます。
2. 鍵の「**名前**」および「**パスフレーズ**」を入力します。
3. パスフレーズを確認し、「**OK**」をクリックします。

   パスフレーズは、会社のポリシーに準拠している必要があります。そうでない場合は、警告メッセージが表示されます。

鍵が作成され、これ以降の暗号化に使用されます。

4.15.2 SafeGuard Portable を使用したファイルの暗号化

1. SafeGuard Portable で、ファイルを右クリックして「**暗号化**」を選択します。

   ファイルは、前回 SafeGuard Portable によって使用された鍵で暗号化されます。

   ドラッグ アンド ドロップを使用して新しいファイルを保存する際、ファイルを暗号化するかを確認するメッセージが表示されます。

   デフォルトの鍵が設定されていない場合は、鍵を設定するためのダイアログが表示されます。鍵の名前とパスフレーズを入力し、パスフレーズを確認入力し、「**OK**」をクリックします。
2. ここで設定した鍵を使ってさらに別のファイルを暗号化する場合は、ショートカット メニューまたは「**ファイル**」メニューで「**暗号化**」を選択します。
   新しい鍵を設定しないかぎり、前回 SafeGuard Portable によって使用・設定された鍵が、以後、SafeGuard Portable を使用して行う暗号化すべてに使用されます。

4.15.3 SafeGuard Portable を使用したファイルの復号化

1. SafeGuard Portable で、ファイルを右クリックして「**復号化**」を選択します。

   メディア パスフレーズまたはローカル鍵のパスフレーズを入力するためのダイアログが表示されます。
2. 送り側から取得した適切なパスフレーズを入力し、「**OK**」をクリックします。

   ファイルが復号化されます。

メディア パスフレーズは、ファイルの暗号化にどのローカル鍵が使用されたかに関わらず、暗号化されたファイルすべてへのアクセスを許可します。ローカル鍵のパスフレーズだけを持っている場合は、この鍵を使って暗号化されたファイルだけにアクセスできます。

SafeGuard Portable で生成した鍵を使用してファイルが暗号化されている場合 、このファイルは自動的に復号化されます。

ファイルを復号化し、鍵のパスフレーズを入力したら、次回、同じ鍵を使用して暗号化されたファイルを暗号化/復号化する際、再度パスフレーズを入力する必要はありません。

SafeGuard Portable が実行されている間は、パスフレーズを保存します。前回 SafeGuard Portable によって使用された鍵が、暗号化に使用されます。

復号化されたファイルは、SafeGuard Portable を閉じるときに再度暗号化されます。

5 サポート

フルリリース

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/contact-support/support-query.aspx

6 利用条件