SOPHOS
Security made simple.

SafeGuard Enterprise ベストプラクティス ガイド

製品バージョン: 8
ドキュメント作成日: 2016年 7月

目次

1 このガイドについて

このガイドは、以下の 2部で構成されています。

- Synchronized Encryption の導入にあたって (p. 4) : 新モジュール「Synchronized Encryption」の利用開始にあたり最初に行う設定について説明します。

  機能や仕組みのほか、お使いの環境への導入方法を概説します。Synchronized Encryption モジュールの詳細については、SafeGuard Enterprise 管理者ヘルプを参照してください。

- ベストプラクティスと推奨事項 (p. 14) : SafeGuard Enterprise をスムーズに導入展開するためのヒントや推奨される設定、管理、使用方法を紹介します。

  この項目は、すべての手順が網羅されているインストールガイドではありません。本製品を熟知しているユーザーを主な対象としています。インストールと管理の詳細については「SafeGuard Enterprise 管理者ヘルプ」を参照してください。

2 Synchronized Encryption の導入にあたって

Synchronized Encryption は、Sophos SafeGuard Enterprise の新しいファイル暗号化モジュールです。以前のバージョンのファイル暗号化機能と比較した主な変更点は、次のとおりです。

- あらかじめ指定したアプリケーション (IN アプリ) で作成または編集したファイルを自動的に暗号化
- ファイルの復号化は指定したアプリケーションでのみ可能
- ファイルの保存場所にかかわらず暗号化を実行する
- iOS または Android が稼動しているモバイルデバイスとの暗号化鍵の交換が可能

  注: SafeGuard Enterprise と通信するよう Sophos Mobile Control を設定する必要があります。

- セキュリティ脅威の存在が疑われるユーザーのデバイスから自動で暗号化鍵を削除することが可能

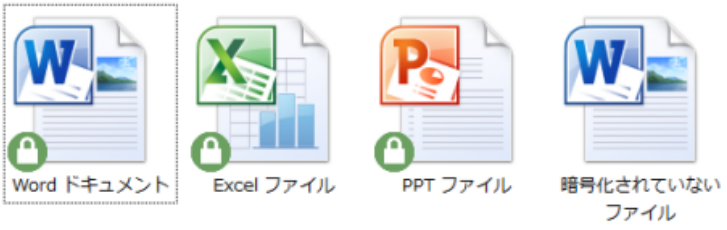
  注: この機能は、SafeGuard Enterprise とクラウド管理型の Sophos Central Endpoint Protection を併用している場合のみに利用できます。SafeGuard Enterprise のポリシーは、暗号化鍵を削除するように設定しておく必要があります。この機能は、Windows エンドポイントと Mac OS X エンドポイントに対して適用することができます。

- ユーザーが自身のモバイルデバイスからボリュームベース暗号化 (Windows の BitLocker ドライブ暗号化または Mac OS X の FileVault2) の復旧鍵を取得することが可能

2.1 標準的なアプリケーションとの連携

Synchronized Encryption では、暗号化を意識する必要がないため、ユーザーは通常どおりに作業ができます。社外のユーザーにファイルを共有する場合にのみ、送信先に応じたセキュリティレベルを考慮する必要があります。

たとえば、Excel や PowerPoint では、通常どおりにファイルを作成できます。作成したファイルは、保存する際に自動的に暗号化されます。暗号化されたファイルのアイコンは小さな鍵マーク付きで表示されます。



2.2 社内でのデータ共有

本バージョンの SafeGuard Enterprise (SGN 8) では、単一の暗号鍵が使用されるので簡単に社内でデータを共有できます。SafeGuard で暗号化されたデータは、SafeGuard Enterprise のユーザーであれば誰でも閲覧できます。

暗号化されたファイルは、メールで送信したり、ネットワーク共有に置いたり、あるいはリムーバブルストレージデバイスにコピーしたりと、通常と同じように共有できます。

Synchronized Encryption モジュールは、社内の共有データへのアクセスが必要なすべてのユーザーのコンピュータにインストールする必要があります。

注: SafeGuard Enterprise は、すべての Windows エンドポイントと Mac OS X エンドポイントにインストールしてください。

2.3 社外とのデータ共有

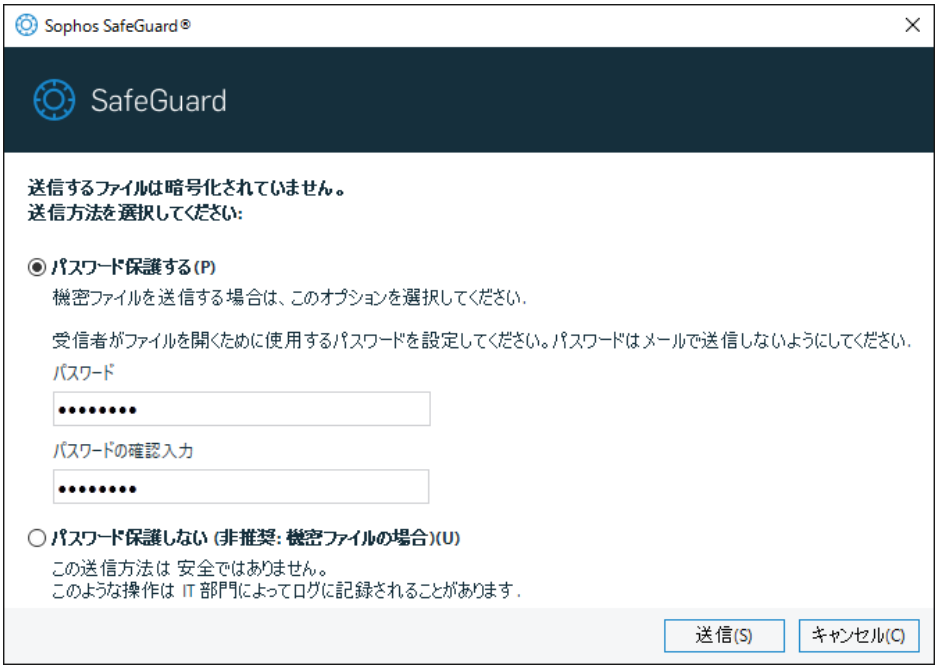
データ暗号化の目的は、機密データへのアクセスを制限することです。たとえば、財務情報や最新の知的財産などは、広く一般に公開するタイプの情報ではありませんが、場合によっては、こういった情報を社外と共有することもあります。暗号化した状態で共有することもあれば、すでに機密性はないと判断することもあります。

処理フローは、Microsoft Outlook を使用している場合と、使用していない場合で異なります。

ヒント: ユーザーには SafeGuard Enterprise ユーザーヘルプを案内してください。

Microsoft Outlook を使用している場合

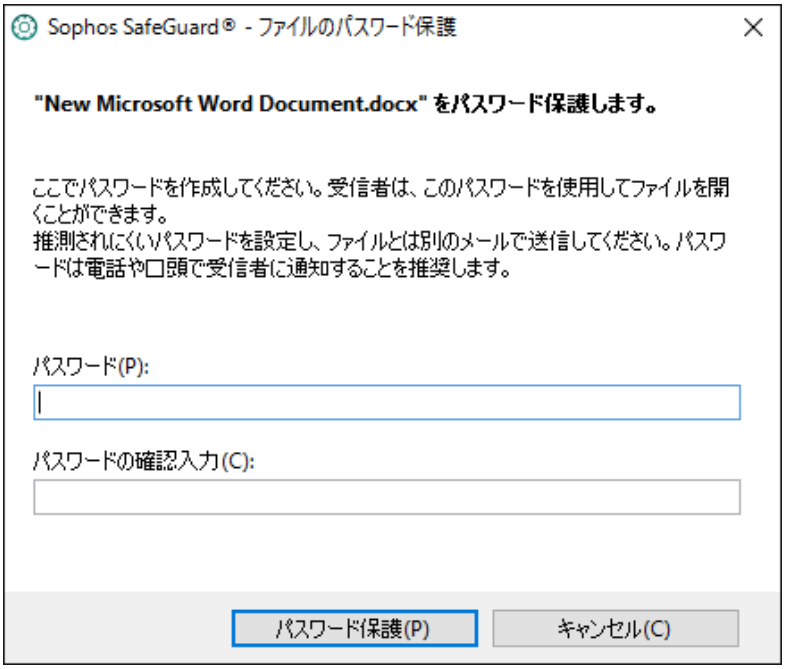
Microsoft Outlook (32ビット版 Office のみ) がインストールされている Windows コンピュータの場合、ユーザーは暗号化を意識する必要はありません。Synchronized Encryption では、ユーザーが少なくとも 1人の社外ユーザーに添付ファイルメールを送信しようとすると、ファイルの処理を確認するメッセージを表示するように設定を行うことができます。



Microsoft Outlook 以外を使用している場合

Windows ユーザーや Mac ユーザーは、ファイルを復号化してから平文で送信したり、ファイルをパスワードで保護してから送信したりします。

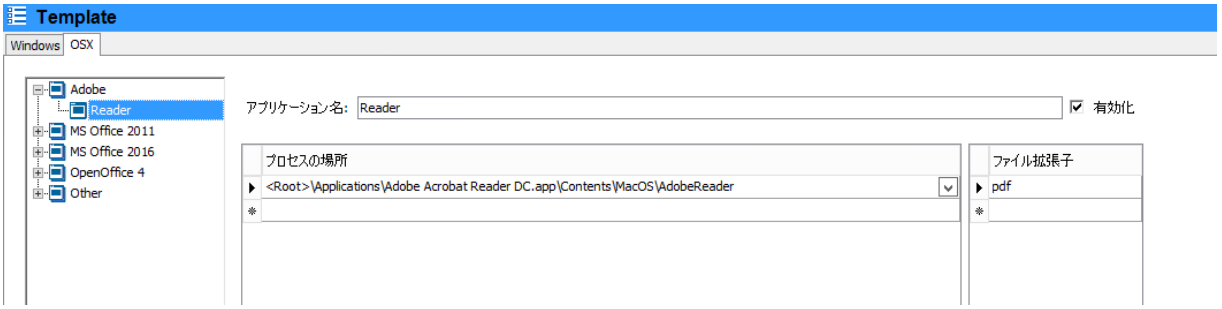
ファイルを右クリックし、「**SafeGuard ファイル暗号化**」、「**選択したファイルの復号化**」の順に選択します。または、ファイルを右クリックし、「**SafeGuard ファイル暗号化**」、「**ファイルのパスワード保護**」の順に選択します。HTML 拡張子を持つ新しいファイルが作成され、受信者は送信者があらかじめ設定したパスワードでファイルを開くことができます。



詳細は、「SafeGuard Enterprise ユーザーヘルプ」のメールの添付ファイルを安全に送信する方法を参照してください。

2.4 IN アプリの指定

IN アプリとは、ファイルを作成・保存時に暗号化し、暗号化されたファイルを閲覧できるアプリケーションを指します。IN アプリを指定するには、SafeGuard Enterprise のセキュリティ担当者が、アプリケーションリストにアプリケーションのフルパスを追加します (Windows と Mac OS X 個別に設定します)。



ヒント: アプリケーションは、すべてのコンピュータで同じ場所にインストールされている必要があります。コンピュータによってインストール先が異なる場合は、すべてのインストール先パスをアプリケーションリストに追加する必要があります。

2.4.1 IN アプリに指定するべきアプリケーション

IN アプリは、ファイルを作成・保存時に自動的に暗号化し、暗号化されたファイルを閲覧できるアプリケーションを指します。ファイルの作成・保存時に暗号化を実行するアプリケーションや、暗号化済ファイルの閲覧に使用するアプリケーションは、すべて IN アプリに指定します。

ファイルの作成に使用するアプリケーションの一般例は次のとおりです。

- オフィススイート (Microsoft Office、OpenOffice、FreeOffice など)
- デザインソフトウェア (Adobe Creative Suite など)

ファイル閲覧アプリケーションの一般例は次のとおりです。

- Office Viewer
- PDF ビューア
- 画像ビューア

注: Windows ストア アプリは、IN アプリとしてアプリケーションリストに追加できません。

ヒント: ファイル作成ソフトウェアで使用されるすべての拡張子を指定します。たとえば、Microsoft Word の場合、.docx のほかに .rtf や .odt なども指定する必要があります。

場合によっては、特定のユーザーのみが使用するアプリケーションも追加します。その場合でも、特定のユーザーのみにポリシーを適用する必要はありません。コンピュータにインストールされていないアプリケーションに関するポリシーを受信した場合、その部分のポリシーは無視されます。

2.4.2 INアプリに指定するべきではないアプリケーション

暗号化の目的は、外部への情報漏えい防止であるため、社外への情報送信に使用する可能性のあるアプリケーションは、IN アプリに指定しないでください。指定した場合、送信する前にすべてのデータが復号化され、データが保護されていない状態になります。

メールクライアント、Web ブラウザ、バックアップ作成ソフトウェアなどは、決して IN アプリに指定しないでください。

注: Mac OS X の場合、Outlook アドインを利用できないため、メールプログラムを追加したほうが便利な場合もあります。詳細は、Mac OS X エンドポイント用ポリシー (p. 17) を参照してください。

2.5 インストールにあたっての注意事項

Synchronized Encryption をインストールする際は、まずは限定したユーザーのみ (テストグループ) にインストールすることを検討してください。それ以外のユーザーに対しては、読み取り専用ポリシーを適用し、社内で暗号化されたファイルの閲覧ができるようにします。詳細は、読み取り専用ポリシーの作成 (p. 10) を参照してください。

Synchronized Encryption のインストールにあたっては、状況に応じて、以降のセクションで説明する事柄を考慮します。

2.5.1 ファイル作成に使用したアプリケーションとは異なるアプリケーションでファイルを開く

アプリケーションの中には、さまざまな形式のファイルを作成できるものがあります。このため、作成されたファイルを開いて閲覧するときに使用するアプリケーションについて考える必要があります。たとえば、PDF 形式のファイルは Microsoft Word でも作成できます。Microsoft Word を IN アプリとして指定すると、Word で PDF 化したファイルは暗号化されます。データに機密情報が含まれる可能性があるので、正しい動作といえます。

しかしながら、出力したファイルを閲覧するアプリケーションを検討する必要があります。この例では、PDF リーダーを使用することにします。一般に、PDF リーダーを使用してファイルを作成することはありませんが、この場合、IN アプリとしてアプリケーションリストに追加する必要があります。リストに追加されていないと、PDF リーダーでファイルを閲覧することができなくなります。このようなことから、SafeGuard 8 Management Center のアプリケーションリストのテンプレートには、あらかじめ一般的な PDF リーダーが含まれています。

その他の同様なアプリケーションの例は次のとおりです。

- 画像を出力するアプリケーション
- TXT、RTF、CSV などさまざまな形式でテキストを出力するアプリケーション

ヒント: IN アプリで作成する、すべてのファイルの閲覧に使用するデフォルトのリーダーをいくつか検討します。これらのリーダーがすべてのコンピュータにインストールされていることを確認し、暗号化されたコンテンツを読み込めるようにアプリケーションリストに追加します。

2.5.1.1 Windows 10 での PDF リーダー

Windows 10 のデフォルトの PDF リーダーは、新しい Web ブラウザ「Edge」です。Edge は IN アプリに指定できますが、指定すると、その後 Edge を使用してインターネットにアップロードするすべてのファイルが復号化されるようになってしまいます。

重要: ビルトインの規定リーダーの Edge 以外に、Adobe Acrobat Reader または Foxit Reader などの PDF リーダーを Windows 10 コンピュータにインストールするようにしてください。

2.5.2 Java アプリケーション

多くの場合、Java アプリケーションの起動には `java.exe` という実行ファイルが使われます。`java.exe` を実行するパスから、現在どの Java アプリケーションが起動しているかを識別することはできません。

java.exe をアプリケーションリストに追加すると、この実行ファイルを使用するすべてのアプリケーションで作成されるコンテンツが暗号化され、また暗号化されたファイルにアクセスできるようになる点を考慮する必要があります。

2.5.3 Web ベースのアプリケーション

複数のユーザーによる作業の効率化にあたって、Web にファイルをアップロードして共有できる Web ベースのアプリケーションがよく利用されます。暗号化されたファイルは、暗号化された状態が保持されるため、サービスの基盤システムではファイルを読み込めません。つまり、以下のとおりとなります。

- ファイルの内容をインデックス化することはできません。
- 社外のユーザーがこれらのファイルにアクセスすることはできません。

このようなファイルを社外のユーザーに共有する場合は、ファイルをアップロードする前に復号化します。または、ファイルを暗号化せず保存できるフォルダを作成します。

こういった暗号化の対象外とするフォルダは、この目的に限ってのみ使用します。ユーザーに対しても明確にその旨を伝えます。

ヒント: 暗号化の除外を設定するには、対象となるフォルダの絶対パス (`c:\unencrypted` など) を指定するか、相対パス (Windows クライアントのみに適用できます) を作成します。相対パスで除外を設定する場合は、相対パスで指定されているフォルダ名と同じ名前のフォルダを作成します。たとえば、除外に指定したフォルダの名前が「`\unencrypted`」の場

合、作成場所にかかわらず、「\unencrypted」という名前のすべてのフォルダ内のファイルとそのサブフォルダが暗号化されるようになります。

2.5.4 SafeGuard の暗号化機能がインストールされていないプラットフォームとのデータ交換

SafeGuard がインストールされている環境で作成したファイルを別の環境で使用することも想定できます。たとえば、Windows や Mac OS X クライアントで作成されたファイルをターミナルサーバー環境で使用する場合などです。SafeGuard Enterprise はターミナルサーバー環境では利用できません。SafeGuard で暗号化されたファイルは、暗号化された状態が保たれるため、ターミナルサーバー環境のアプリケーションで閲覧することはできません。

この問題を回避するには、該当するパスを対象から除外するように暗号化ポリシーを設定します。

2.5.5 プレビュー表示について

Windows エクスプローラや Finder などのファイル閲覧機能では、画像やテキストファイル、表計算ファイル、PDF など、さまざまな種類のファイルをプレビュー表示できます。このようなプレビューは、通常、ファイルを保存したときや変更したときに作成されます。プレビュー表示するには、プレビューを作成するアプリケーションが、ファイルの内容 (暗号化されていない) にアクセスできなくてはなりません。そのためには、該当するアプリケーションを IN アプリとしてアプリケーションリストに追加する必要があります。Mac OS X の場合、このアプリケーションは個別のアプリケーションなので、アプリケーションリストに追加できます (デフォルトで追加されています)。

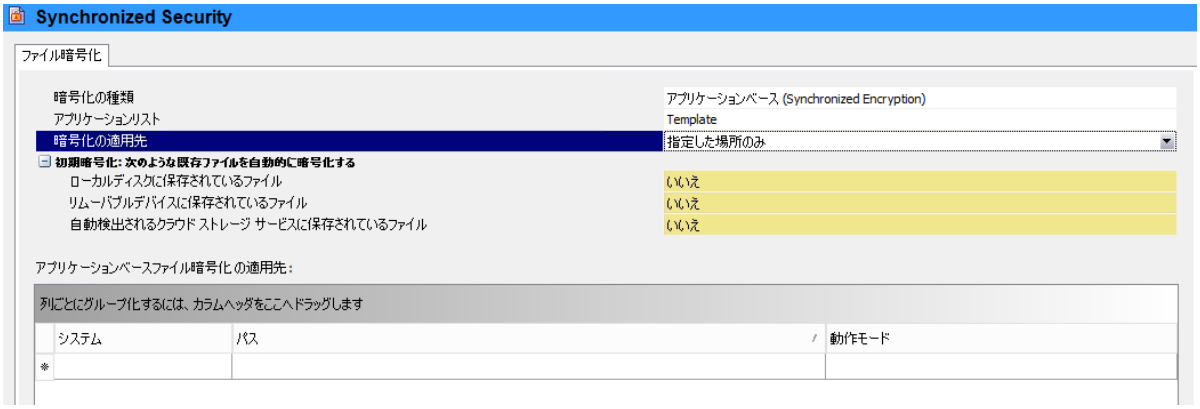
2.6 読み取り専用ポリシーの作成

Synchronized Encryption の段階的インストールを開始する際、まず、ユーザーに対して、暗号化されたファイルの閲覧のみを許可して、ファイルの暗号化はできないように設定します。暗号化機能は、まず特定のグループのみに対して有効化し、次に全ユーザーに対して有効化を行います。

インストールの最初の段階で使用するポリシーが読み取り専用ポリシーです。

Windows

Windows ユーザーの場合、すべてのアプリケーションを含む Synchronized Encryption ポリシーを作成して、「**暗号化の適用先**」を「**指定した場所のみ**」に指定します。ただし、パスは指定しないでください。



詳細については、SafeGuard Enterprise 管理者ヘルプの読み取り専用ポリシーの作成:Windows エンドポイントを参照してください。

Mac OS X

Mac OS X の場合、暗号化は Windows とは異なるかたちで動作します。Mac OS X コンピュータでは、暗号化されたファイルは指定された場所でのみ読み取ることができます。

つまり、Windows ユーザー向けの読み取り専用ポリシーを Mac OS X ユーザーに対して使用することはできません。

Mac OS X の場合、「**ファイル暗号化**」という種類のポリシーを作成して暗号化の種類に「**ロケーションベース**」を選択します。少なくとも1つのパスを追加して、追加したパスを暗号化の対象から「**除外**」し、Mac OS X ユーザーに通知します。たとえば、`<Documents>/Encrypted` といったパスを指定します。暗号化されたファイルを閲覧する必要がある場合、ユーザーは、まず、この場所に閲覧するファイルを移動またはコピーします。

詳細は、SafeGuard Enterprise 管理者ヘルプの読み取り専用ポリシーの作成: Mac エンドポイントを参照してください。

2.7 エンドユーザーへの通知

暗号化製品は、一般に使用経験のあるユーザーがあまり多くないため、暗号化の手順や規則を従業員に案内することを推奨します。特に Synchronized Encryption の場合は、ユーザーが製品の動作を理解していることが重要です。たとえば、ユーザーが IN アプリに指定されているアプリケーションを把握していれば、暗号化対象から漏れている主要アプリケーションがあった場合、即座に気付き、SafeGuard Enterprise のセキュリティ担当者に報告することができます。これを受け、セキュリティ担当者は、漏れているアプリケーションを暗号化の対象としてアプリケーションリストに追加します。

推奨する手順は次のとおりです。

- 新しく導入された暗号化規則とその結果発生する現象について簡単に説明したメールをすべてのユーザーに送信します。可能な場合は、簡単に編集できる社内 Web サイトに新しく指定された IN アプリの情報などを都度掲載し、メールにリンクを含めます。
- メールには問い合わせ用メールアドレスを記載します。

- この時点で、すべてのエンドポイントに SafeGuard Enterprise がインストールされている場合は (読み取り専用モードなどで)、Synchronized Encryption の暗号鍵で暗号化したファイルを添付し、ユーザーがファイルを閲覧できるかどうか確認を求めます。ユーザーが暗号化ファイルを閲覧できなかった場合は、インストールに問題があるか、またはエンドポイントと SafeGuard Enterprise のバックエンドとの通信に問題があるので、問題を修正してから全ユーザーに対して暗号化を有効化します。

2.7.1 ユーザーへの通知文のサンプル

次にユーザーへの通知に使用できるメールの文例を示します。文例には、特に重要な情報が含まれますが、たとえば、「unencrypted」という名前の付いたフォルダすべてを暗号化の対象から除外するルールを設定した場合や、文例に挙げられている以外のアプリケーションを使用している場合など、状況に応じて情報を追加してください。この文例は、Synchronized Encryption の暗号鍵で暗号化されたファイルを添付して送信することを前提に書かれています。

= =
=

各位

このたび、SafeGuard Enterprise の全社へのロールアウトを完了しましたので、お知らせいたします。SafeGuard Enterprise は、社内ドキュメントを保護するためにすべてのユーザーが使用するソフォスの暗号化製品です。暗号化による日々の業務への影響は特にありませんが、いくつか注意していただきたい点があります。

来週より、すべての従業員が、Synchronized Encryption というアプリケーションベースの暗号化機能を使用できるようになります。いったん、この機能が有効になると、お使いのデバイスで作成したファイルは暗号化されるようになります。製品の使用開始にあたって、さまざまなガイドをイントラネット上に用意しましたので、ホームページより暗号化の項目をクリックするか、直接 https://company.internal/encryption 開いてください。

暗号化済ファイルをお使いのコンピュータで閲覧できるかどうか確認するには、添付のファイルを開いてください。

- **Windows および Mac OS X の場合:** 添付のファイルを開き、内容が閲覧できれば、設定は正しく完了しています。ファイルの内容が正しく表示されない場合は、ヘルプデスク担当者にお問い合わせください。

- **iOS および Android の場合:** お使いのデバイスで Sophos Secure Workspace アプリから添付ファイルを開きます。暗号化されているため、システム標準のビューアでファイルを開くことはできません。お使いのモバイル端末上に Sophos Secure Workspace がインストールされていない場合は、ヘルプデスク担当者にお問い合わせください。

使用するアプリケーション

次のアプリケーションで作成する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異なるアプリケーションでアクセスした場合、内容を表示することはできません。

Windows:

- Adobe Reader

- MS Office 2010 (Excel、PowerPoint、Word)

- MS Office 2013 (Excel、PowerPoint、Word)
- MS Office 2016 (Excel、PowerPoint、Word)
- Office Viewer
- Foxit Reader

Mac OS X:

- Adobe Reader
- Apple 仕事効率化アプリ (Keynote、Numbers、Pages、Preview)
- MS Office 2011 (Excel、PowerPoint、Word)
- MS Office 2016 (Excel、PowerPoint、Word)

社外へファイルを送信するには

社外にファイルを送信する際は、ファイルが暗号化された状態で送信されることに注意してください。この場合、社外の受信者はファイルを閲覧できません。機密情報が含まれていない場合は、ファイルを復号化してから送信します。社外秘の場合や、社外秘の可能性がある場合は、ファイルをパスワード保護します。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。「選択したファイルの復号化」または「ファイルのパスワード保護」を選択します。

Windows を使用している場合で、**Microsoft Outlook** でファイルを送信するときは、手動でこれらの作業を行う必要はありません。暗号化されたファイルを社外に送信しようとすると、システムで検知され、ファイルの処理方法を確認するメッセージが表示されます。

Web アプリケーションにファイルをアップロードするには

暗号化されたファイルは、常に暗号化されたままの状態でアップロードされます。つまり、SharePoint やその他の Web アプリケーションでも暗号化された状態が保持されます。状況に応じて、ファイルを手動で復号化してからアップロードします。暗号化されたファイルは、プレビュー機能で表示することも、検索インデックスを作成することもできません。

ご意見やご質問

SafeGuard Enterprise に関する問題や、暗号化機能のインストール後にコンピュータで生じた問題につきましては、ヘルプデスク担当者までお問い合わせください。

よろしくお願いいたします。

3 ベストプラクティスと推奨事項

3.1 ロールアウト

注: SafeGuard Enterprise Server および SafeGuard Management Center をインストールするには、.NET 4.5 が必要です。

一般的な推奨事項

- SafeGuard Enterprise の新しい Synchronized Encryption モジュールと以前の File Encryption モジュールを取り混ぜてロールアウトしないでください。
- 段階的にロールアウトするには、特に AD のグループメンバーシップが複雑に入れ子になっている場合など、各段階でテスト運用や検証が必要となります。
- ユーザートレーニングは円滑な導入/運用の鍵となります。
- ロールアウトの対象部門とその後の作業手順を明確に通知することは重要です。
- IT 部門とサポート部門に十分な人員を配置する必要があります。

前提条件

- すべてのエンドポイントに SafeGuard Enterprise 8 がインストールされている必要があります。インストールされていない場合、透過的に暗号化されたファイルを共有することができなくなり、日常業務に支障をきたします。
- 暗号化されたファイルをモバイルデバイスで閲覧する場合 (SafeGuard Enterprise 8 の新機能)、Sophos Secure Workspace アプリもロールアウトする必要があります。

  注: 暗号化されたファイルをモバイルデバイスで閲覧するには、Sophos Mobile Control で集中管理されている Sophos Secure Workspace を使用する必要があります。
- 外出の多いユーザーは、VPN または Direct Access (Windows) 経由で SafeGuard Enterprise のサーバーに定期的に接続し、最新の暗号化ポリシーが適用されていることを確認します。

3.1.1 Synchronized Encryption を使用するためのエンドポイントの準備

Synchronized Encryption モジュールを正常に動作させるためには、Microsoft Runtime **`vstor-redist.exe`** をインストールする必要があります。このファイルはインストールパッケージに含まれており、Microsoft Visual Studio 2010 Tools for Office Runtime をインストールします。

各コンポーネントは、次の順にインストールすることを推奨します。

1. **`vstor-redist.exe`**

2. **SGNClient.msi**
3. 構成パッケージ

注: 構成パッケージは、**vstor-redist.exe** のインストールが完了するまで、展開できないことに注意してください。

3.1.2 段階的なロールアウト

多くの場合、新機能の **Synchronized Encryption** モジュールは、すべての従業員に短期間で一斉ロールアウトして有効化することはできません。このような場合は、**Synchronized Encryption** を有効化していない SafeGuard Enterprise エンドポイントを使用している場合でも、ユーザーが暗号化済ファイルを閲覧できるようにしておくことが重要です。そのためには読み取り専用のポリシーが必要になります。

ユーザーに読み取り許可を付与するには次の項目が必要です。

- **Synchronized Encryption** 鍵

  この鍵はデフォルトで、Management Center のルートノードに割り当てられており、社内のすべての従業員は、この鍵を自動的に取得します。

- **アプリケーションリスト**と固有の読み取り専用ポリシー

  Synchronized Encryption の段階的ロールアウトの詳細については、SafeGuard Enterprise 管理者ヘルプのSynchronized Encryption の段階的ロールアウトを参照してください。

3.1.3 Synchronized Encryption と SafeGuard Enterprise File Encryption が混在する環境について

注: 用途に応じて Synchronized Encryption と File Encryption の両方を使用する場合は、円滑な導入を図るために次の事柄を考慮してください。

Synchronized Encryption では、1つの暗号鍵を社内全体で使用します。このため、管理やインストールが非常に簡単です。人事や財務など一部の部署では、部署内に限定してデータを共有するために個別の暗号化が必要になることもあります。

このような場合は、SafeGuard Enterprise File Encryption (ファイル暗号化) モジュール (File Share、Cloud Storage、Data Exchange) を使用します。これらのモジュールを使えばファイル暗号化に異なる鍵を使用することができます。Synchronized Encryption モジュールと SafeGuard Enterprise File Encryption モジュールを同じコンピュータにインストールすることはできません。

Synchronized Encryption モジュールと SafeGuard Enterprise File Encryption モジュールの両方を導入するには、別途、次の管理タスクを実行する必要があります。

1. SafeGuard Enterprise のロールアウトにあたり、異なるモジュールのインストールが必要な部署について考慮してください。
2. 特別な要件のある部署には、**Synchronized Encryption** がインストールされているエンドポイントに適用されているポリシーとは異なるポリシーを用意する必要があります。Active Directory のディレクトリ構造をインポートすれば、このようなポリシーを該当するユーザーやコンピュータに簡単に適用できるようになります。

3. SafeGuard Enterprise モジュールは、適用されているポリシーに基づいてロールアウト/インストールする必要があります。すなわち、適切なポリシーを正しいコンピュータに適用してください。

   注: Outlook アドインは、SafeGuard Enterprise File Encryption モジュールでは利用できません。このため、Synchronized Encryption がインストールされているエンドポイントと File Encryption がインストールされているエンドポイントとの間で、暗号化された添付ファイルを透過的に共有することはできません。

推奨事項

- SafeGuard Enterprise File Encryption モジュールのユーザーには、**Synchronized Encryption** の鍵を配布する必要があります。**Synchronized Encryption** の鍵で暗号化されたファイルを透過的に閲覧できるようになります。
- 暗号化済ファイルの共有:

  SafeGuard Enterprise File Encryption モジュールのユーザーを対象に、「転送用」ファイル保存先の共有に対して **Synchronized Encryption** 鍵の使用を指定するポリシーを作成することを推奨します。この共有で作成されたファイルや、この共有に移動されたファイルは、すべて **Synchronized Encryption** 鍵で暗号化されるようになります。**Synchronized Encryption** のユーザーは、これらのファイルを閲覧できます。

- 平文のファイル (暗号化されていないファイル) の共有:

  SafeGuard Enterprise File Encryption モジュールのユーザーには、任意のフォルダを暗号化の対象から除外するよう設定したポリシーを使用できます (「**暗号化の種類**: **ロケーションベース**」、「**動作モード**: **除外**」)。

- SafeGuard Enterprise File Encryption モジュールのユーザーが **Synchronized Encryption** モジュールのユーザーとファイルを共有する場合は、まずはファイルを復号化する必要があります。その後、復号化したファイルを送信するか、または Synchronized Encryption 鍵で暗号化しなおしてファイルを共有します。

3.1.4 ユーザー証明書の有効期限の確認

SafeGuard Enterprise の BitLocker 管理機能のみを使用しており、**Synchronized Encryption** を追加する場合、ユーザー証明書の有効期限を確認することは特に重要です。

証明書は、SafeGuard Management Center の「**鍵と証明書** > **証明書** > **割り当てられた証明書**」で確認できます。

期限切れの証明書や期限が迫っている証明書は、「**有効期限**」カラムの内容が赤で表示されます。期限が迫っている証明書を更新するには、「**更新**」カラムのチェックボックスにチェックを入れます。証明書の有効期限がすでに切れている場合は、新しい証明書を入手する必要があります。失効している証明書は削除してください。削除すると、該当するユーザーは、SafeGuard Enterprise への次回ログオン時に、自動で新しい証明書を受信します。

SafeGuard Enterprise には、このタスクを自動化する `UserCertficateRenewal.vbs` というデータベーススクリプトが用意されています。このスクリプトを SafeGuard Enterprise または Windows の「**タスクスケジューラ**」で使用すれば、証明書が定期的にチェックさ

れ、必要に応じて更新されます。詳細は、ソフォスのサポートデータベースの文章 118878 を参照してください。

3.1.5 すべてのユーザーが認証されていることの確認

SafeGuard Enterprise では、新しいユーザーを SafeGuard Management Center 、または Active Directory のどちらかで認証する必要があります。ほとんどのユーザーは、Active Directory ユーザーであるため、自動的に認証されます。しかし、ローカルユーザーなどの一部のユーザーは手動で認証する必要があります。認証されていないユーザーは、「**SGN ユーザー**」にならないため、Synchronized Encryption 鍵が配信されません。Windows と Mac OS X、どちらのエンドポイントでも同様です。

最初に展開するポリシーは、**読み取り専用**に設定することを推奨します。すべてのエンドポイント/ユーザーが鍵を受信してから、暗号化ポリシーを有効化します。このようにすれば、ユーザーが暗号化ポリシーを受信する前にすべてのユーザーを認証することができます。未認証のユーザーに関する問題を未然に防ぐことができます。

3.1.6 Mac OS X エンドポイント用ポリシー

ファイル暗号化では、暗号化の種類に「**アプリケーションベース (Synchronized Encryption)**」を選択し、「**暗号化の適用先**」を「**指定した場所のみ**」に設定し、まずは数箇所のみを自動暗号化の適用先として指定します。このようにすることで、従業員や日々の業務へ及ぼす影響を最小限に抑えることができます。

ポリシーの管理をするうえで、Windows エンドポイントと Mac OS X エンドポイントを識別しやすくするために、Mac OS X ユーザーとコンピュータに対して個別の Active Directory グループや SafeGuard Enterprise グループを使用します。Mac OS X 用のポリシーは、Mac OS X ユーザーとコンピュータのみに対して有効化します。

3.1.6.1 Mac OS X の Synchronized Encryption ポリシーの推奨事項

IN アプリ

ファイルを作成・保存時に暗号化する必要のあるアプリケーションは、「**アプリケーションリスト**」に追加します。

- メール

  注: Mac OS X の場合、Outlook アドインは利用できません。しかし、Outlook や Apple Mail をアプリケーションリストに追加すれば、暗号化されたファイルを閲覧できないユーザーに、意図せず暗号化済みのファイルを送信することを防止できます。リストに追加したメールアプリは、すべての添付ファイルを暗号化されていない状態で送信し、受信したメールの暗号化された添付ファイルは暗号化された状態で、暗号化されていないファイルは平文で保存します。

  - /Applications/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - /Applications/Microsoft Office 2011/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - Applications/Mail.app/Contents/MacOS/Mail

- Mac OS X のプレビュー、および Finder と Apple Mail のプレビュー機能を有効化するには、次のプロセスを追加する必要があります。
  - /Applications/Preview.app/Contents/MacOS/Preview
  - /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/XPCServices/QuickLookSatellite.xpc/Contents/MacOS/QuickLookSatellite
  - /System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/QuickLookUI.framework/Versions/A/Resources/QuickLookUIHelper.app/Contents/MacOS/QuickLookUIHelper
  - /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/MacOS/quicklookd

暗号化の適用先: **指定した場所のみ** のパス

- 暗号化:
  - <Documents>\Encrypted
- ユーザーがメールクライアントで暗号化済ファイルをダブルクリックして開けるようにするには、Mail などのメールクライアントのアプリケーションをアプリケーションリストに追加し、その一時フォルダのパスを場所の一覧に追加する必要があります。

  リストに追加する Mac のメールクライアントのパスは以下のとおりです。
  - <%TMPDIR%>\com.apple.mail\com.apple.mail
  - <User Profile>\Library\Containers\com.apple.mail\Data\Library\Mail Downloads

  Outlook for Mac の場合は、次のパスを追加します。
  - <User Profile>\Library\Caches\TemporaryItems\Outlook Temp\
  - <%TMPDIR%>com.microsoft.Outlook\Outlook Temp\

3.2 バックエンド

3.2.1 Active Directory との同期に使用する読み取り専用ユーザー

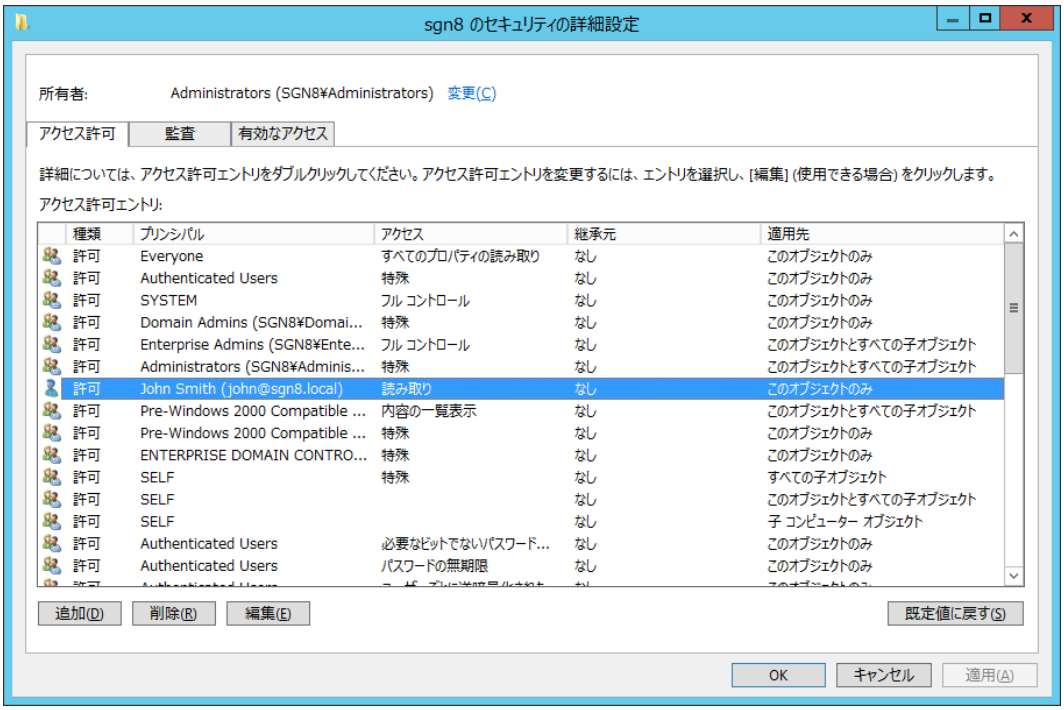
注: 接続のセキュリティを強化するために、Active Directory との同期には SSL 暗号化通信を利用することを推奨します。

Active Directory のインポートと同期には、**読み取り専用**のユーザーアカウントを使用します。ユーザーがドメインとその子オブジェクトにアクセスするには、読み取り権限が必要です。

権限を付与する方法は次のとおりです。

1. 「**Active Directory ユーザーとコンピュータ**」 の管理ウィンドウを開き、「**高度な機能**」に移動します。
2. ドメインを右クリックして「**プロパティ**」をクリックします。
3. ユーザー (またはグループ) を追加して「**読み取り**」権限に対応する「**許可**」チェックボックスを選択します。
4. 「**詳細設定**」をクリックし、ユーザー (またはグループ) を選択して「**編集**」をクリックします。
5. 「**<ドメイン名>のアクセス許可エントリ**」ダイアログで、「**適用先:**」ドロップダウンリストから「**このオブジェクトとすべての子オブジェクト**」を選択します。

   結果は次のようになります。



3.2.2 Management Center に「#」付きで表示されるユーザー

ドメインコントローラを利用せず SafeGuard Enterprise に登録されたユーザーは、「#」付きで Management Center に表示されます。

3.3 ポリシー

3.3.1 暗号化の対象から除外するフォルダ

Synchronized Encryption を使用する場合は、次のパスを暗号化の対象から除外するようにしてください。

Windows

- `<Local Application Data\Temp>`

理由:アプリケーションのなかには、サイズの小さい一時ファイルを多数作成するものがあります。このフォルダを除外しない場合、これらの一時ファイルすべてがポリシーに基づいて暗号化されることになります。パフォーマンスの低下を避けるため、このフォルダを暗号化の対象から除外します。

- `<Local Application Data>\Microsoft and subdirs`

  理由: アプリケーションのなかには、他のアプリケーションを呼び出すものがあります (たとえば、Microsoft PowerPoint に埋め込んだ動画など)。呼び出し元のアプリケーションで作成するファイルが暗号化の対象に指定されている場合、一時ファイル(この場合は動画) は暗号化されます。呼び出されたアプリケーション (この場合はブラウザ) が、暗号化を実行しないアプリケーションの場合 (アプリケーションリストに追加されていない場合)、暗号化されたファイルを実行することはできません。

- `<Program Files>`

  理由: このフォルダへのアクセスには管理者権限が必要です。アクセス権がないため、SafeGuard Initial Encryption でこのフォルダ内のファイルを暗号化することはできません。このフォルダを暗号化の対象から除外しておけば、暗号化に失敗したという大量のイベントメッセージで SafeGuard のデータベースが一杯になることを未然に防止できます。

すべてのシステム

- `<!cloud storage providers!>`

  クラウドストレージは、基本的に暗号化することをお勧めしますが、社外とのデータ共有に使用する特定のクラウドストレージサービスを暗号化の対象から除外することもできます。除外することにより、既知のクラウドストレージの同期フォルダが暗号化されないようになります。このため、クラウドとの同期で問題なく社外とデータをやり取りすることができるようになります。社外とのデータのやり取りにクラウドストレージを使用しない場合は、これらのクラウドストレージフォルダを除外する必要はありません。

- `<Music>`、`<Pictures>`

  理由:通常これらのファイルの暗号化は不要です。これらのフォルダを暗号化の対象から除外したくない場合は、これらのファイルを開く際に使用するアプリケーションを**アプリケーションリスト**に追加する必要があります。

  注: Mac OS X で `<Pictures>` 内のファイルを暗号化する場合、写真アプリケーションと画像ライブラリを使用することはできません。

- `<User Profile>\AppData\Roaming\AppleComputer`

  理由: Windows エンドポイント上の iCloud とのローカルの同期フォルダです。このフォルダは、`<!cloud storage providers!>` を除外するのと同様の理由により、暗号化の対象から除外する必要があります。

3.3.2 ポリシーの推奨設定

「Unencrypted」フォルダを設定する

「Unencrypted」(暗号化対象外) フォルダは、たとえば社内の Linux コンピュータと平文ファイルを共有する際や、部分的に展開する場合に利用できます。詳細は、アプリケーションベースのファイル暗号化ポリシーの作成を参照してください。

- **Windows**

  すべてのエンドポイントで「Unencrypted」フォルダを暗号化の対象から除外するには、ポリシーの「**暗号化の適用先**」を「**すべて**」設定したうえで、相対パスとしてフォルダ名「`Unencrypted`」を除外する場所として指定します。指定すると、保存場所にかかわらず、Unencrypted という名前のフォルダ内のすべてのファイルが暗号化されなくなります。

- **Mac OS X**

  相対パスは、Mac OS X に対しては使用できません。ポリシーの「**暗号化の適用先**」を「**すべて**」に設定したうえで、除外する場所として `<Documents>\Unencrypted` を指定することを推奨します。

Outlook アドイン

「**全般設定**」ポリシーの「**ホワイトリストに登録済みのドメインの暗号化方法**」オプションを「**変更しない**」に設定することを推奨します。

感染マシンの鍵を削除する

SafeGuard Enterprise **Synchronized Encryption** がインストールされているエンドポイントは、Sophos Central Endpoint Protection よりコンピュータの感染ステータスを受信します。

「**感染マシンの鍵を削除する**」オプションは、「**いいえ**」に設定することを推奨します。SafeGuard Management Center の「**レポート**」を開き、問題が発生しているエンドポイントを確認し、対処が必要な項目を見つけます。次に、必要に応じてエンドポイントを確認し、クリーンアップします。最後に、「**感染マシンの鍵を削除する**」オプションを「**はい**」に設定します。

3.3.3 ゲストユーザー

SafeGuard Enterprise の BitLocker 管理のみがインストールされているエンドポイントでは、「**新しい SGN ユーザーの登録を許可する**」オプションが「**所有者**」に設定されている場合があります。

SafeGuard Enterprise の POA を使用しておらず、BitLocker 管理またはファイル暗号化モジュールがインストールされているエンドポイントに対しては、「**新しい SGN ユーザーの登録を許可する**」オプションを「**全員**」に設定する必要があります。このオプションが「**全員**」に設定されていない場合、新しく追加するユーザーのステータスは「**SGN ゲスト**」に

設定されます。SGN ゲストは証明書を取得できないため、**Synchronized Encryption** などの暗号化モジュールをインストールしてもファイルの暗号化ができません。

3.3.4 Mac OSX 用ポリシーと RSOP

Mac OSX では、ユーザーに適用されているポリシーのみが評価されます。コンピュータにポリシーを適用しても Mac OS X のエンドポイントでポリシーが受信されません。

ただし、ポリシーが有効にならないにもかかわらず、Management Center の RSOP タブには現在 Mac に適用されているポリシーが表示されます。

3.3.5 ファイルの追跡

SafeGuard Enterprise のファイル追跡機能は、各国の国内法による規制を受けます。合法的に追跡できる事柄を事前に確認してください。

3.3.6 パスワード変更の通知

SafeGuard Enterprise Credential Provider を使用している場合、ユーザーのパスワードが期限切れに近づくと表示される Windows のポップアップリンドウは、表示されなくなります。

ユーザーにパスワードの変更を通知するには、SafeGuard Enterprise で「**パスワード**」という種類のポリシーを作成して必要な設定を行い、ユーザーに適用する必要があります。詳細は、管理者ヘルプのパスワードの構文ルールを参照してください。

3.4 エンドポイント - すべてのプラットフォーム

3.4.1 エンドポイントのセキュリティステータスが正常に戻らない - クリーンアップに失敗する

Next-Generation Data Protection は、Sophos SafeGuard と Sophos Endpoint Protection との連携を実現します (利用可能な場合)。これは Synchronized Security の拡張の 1つです。Sophos SafeGuard と Endpoint Protection はハートビートを使用してシステムのセキュリティステータスを共有します。

システムがマルウェアに感染すると、機密ファイルを保護するためにシステムがロックダウンされます。

この事態が発生すると、Sophos Endpoint Protection は、セキュリティステータスが危険な状態 (レッド) になっていることをユーザーに通知します。また Sophos SafeGuard は、暗号化済ファイルにアクセスできなくなったことをユーザーに通知します。暗号化済ファイルにアクセスできない状態は、システムのセキュリティステータスが正常な状態 (グリーン) に戻るまで続きます。ステータスが正常な状態に回復すると、Sophos SafeGuard はバックエンドと同期を行い、ユーザーは再び暗号化済ファイルにアクセスすることが許可されます。

このような通知が表示された後、システムのセキュリティステータスがすぐに回復しなければ、ユーザーはシステム管理者に問い合わせる必要があります。

エンドポイントのセキュリティステータスが正常に戻らない場合は、Sophos Anti-Virus がクリーンアップに失敗したことを意味します (Sophos Central でクリーンアップは自動に設定されています)。クリーンアップに失敗する場合は、システム管理者によるマルウェアの駆除など、別途対応が必要となります。詳細は、https://www.sophos.com/ja-jp/support/knowledgebase/112129.aspx を参照してください。

3.5 Windows エンドポイント

3.5.1 ファイルの手動暗号化/復号化

Synchronized 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**: ファイルタイプがアプリケーションリストに追加されており、ファイルの保存場所が暗号化の対象から除外されていない場合は、Synchronized Encryption 鍵でファイルを暗号化します。
- **選択したファイルの復号化** (ファイルが暗号化されている場合のみ): ファイルを復号化して、平文で保存します。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** (ファイルが暗号化されていない場合のみ): Synchronized Encryption 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**: パスワードを定義して、ファイルを手動で暗号化できます。この機能は、社内の Synchronized Encryption 鍵を所有していないユーザーと安全にファイルをやり取りする場合に便利です。ファイルは暗号化され、HTML ファイルとして保存されます。受信者は、送信者から受け取ったパスワードを使用して Web ブラウザからファイルを開きます。

  注: このオプションは、平文のファイル、またはファイルの送信者の鍵リングにある鍵を使用して暗号化されたファイルに対してのみ実行できます。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。

  注: パスワード保護には base64 形式のエンコーディングが使用されるので、元のファイルよりサイズが大きくなります。対応しているファイルの最大サイズは 50MB です。

  注: 個別のファイルに対してのみパスワード保護を実行できます。フォルダやディレクトリはパスワード保護できません。なお、一度に複数のファイルを選択して、暗号化の状態を表示したり、暗号化/復号化したりすることはできます。

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**: すべての暗号化されていないファイルを自動的に検出し、ファイルタイプがアプリケーションリストに追加されており、ファイルの保存場所が暗号化の対象から除外されていない場合は、デフォルトの Synchronized Encryption 鍵で

ファイルを暗号化します。適用されているポリシーによっては、他の鍵で暗号化されているファイルが、Synchronized Encryption 鍵で再暗号化される場合もあります。

3.5.2 自動転送ルールによって送信されるメール

自動転送や転送のルールを**クライアント側で**指定した場合、自動送信されるメールはログに記録されません。

3.6 Mac OS X エンドポイント

3.6.1 デスクトップ上のアイコンの位置

SafeGuard Enterprise for Mac を使用している場合、デスクトップ上のアイコンの位置が正しく記憶されないことがあります。アイコンの位置を変更したにもかかわらず、コンピュータを再起動したり、ログオンしなおしたりすると、アイコンが元の位置に戻ることがあります。

アイコンの位置を正しく記憶させるには、次の手順を実行してください。

1. Mac で Terminal アプリケーションを起動します。
2. 次のコマンドを入力します。

   ```
   defaults write com.sophos.encryption MountDesktopAsNetworkVolume 1
   ```

3. Mac にログオンしなおします。

デスクトップアイコンの位置が正しく記憶されるようになります。

重要: このコマンドを実行すると、ゴミ箱の機能が変更されます。削除したファイルは、ゴミ箱を経由せず、そのまま完全に削除されます。この設定を解除するには、Terminal アプリケーションで次のコマンドを実行します。

```
defaults remove com.sophos.encryption MountDesktopAsNetworkVolume
```

4 テクニカルサポート

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。

- 「Sophos Community」ユーザーフォーラム (英語) (http://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せ。
  https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

5 ご利用条件