

SOPHOS

simple + secure

Sophos SafeGuard Disk Encryption、Sophos SafeGuard Easy スタートアップガイド

製品バージョン: 5.60

ドキュメント作成日: 2011年 4月



目次

1 このガイドについて.....	3
2 Sophos SafeGuard について.....	3
3 旧バージョンからのアップグレード.....	5
4 インストールするコンポーネント.....	6
5 主な作業項目.....	7
6 SafeGuard Policy Editor のインストール.....	7
7 初期構成の実行.....	8
8 デフォルト ポリシーのコピーと編集.....	10
9 インストール後に実行する管理タスクのためのエンドポイント コンピュータの構成	10
10 構成パッケージへのポリシーの追加.....	11
11 エンドポイント コンピュータへの暗号化ソフトウェアと構成パッケージのインストール.....	12
12 パスワードを忘れた場合の復旧.....	22
13 よく実行するタスクに関する参照資料.....	24
14 テクニカルサポート.....	25
15 ご利用条件.....	25

1 このガイドについて

このガイドでは、不正アクセスから企業のコンピュータを保護するように Sophos SafeGuard を設定する方法について説明します。

このガイドは次の製品を対象にしています。

- Endpoint Security and Data Protection (ESDP) バンドルに付属する Sophos SafeGuard Disk Encryption (SDE) 5.6x。
- Sophos SafeGuard Easy (SGE) 5.6x。バージョン 5.50 から、SafeGuard Enterprise Standalone ソリューションは Sophos SafeGuard Easy に製品名が変わりました。

上記の 2つの製品間で機能や設定が異なる点は、このガイドで説明していません。

その他の情報は、SDE/SGE 管理者ヘルプと SDE/SGE ユーザー ヘルプを参照してください。

2 Sophos SafeGuard について

Sophos SafeGuard は、ユーザー介入なしでデータを暗号化します。どのデータを暗号化したらよいか、ユーザーが考える必要がありません。暗号化と復号化は、バックグラウンドで実行されます。つまり、暗号化を行うことで、認証されていないユーザーによる、データの読み取りや変更を防止することができます。Sophos SafeGuard による暗号化は、ストレージメディアを別のシステムに接続しても同じように実行されます。

Sophos SafeGuard の特長は次のとおりです。

- すばやい導入が可能。
- 機密データの保護。
- FIPS 140 準拠のテクノロジーによるデータの暗号化。

Sophos SafeGuard で保護されているコンピュータでは、プリブート段階 (OS の開始前) で SafeGuard Power-on Authentication (POA) が起動します。POA でユーザー認証に成功すると、OS が起動し、ユーザーが Windows にログオンします。



POA には次のような使いやすく安全性の高い機能が用意されています。

- タンパー プロテクション (Sophos SafeGuard Disk Encryption で提供)。
- ログオン失敗時の待機時間。
- カスタマイズ可能な Windows スタイルのユーザーインターフェース。
- Windows へのパス スルー認証。
- Unicode および多言語対応。

IT 管理作業を支援するアクセス機能

Sophos SafeGuard には、エンドポイントコンピュータでの IT 管理作業を支援する機能がいくつか用意されています。

- Power-on Authentication は、たとえば、Wake-on LAN と併用するように設定し、パッチ管理を容易にすることができます。
- サービスアカウントを使用すると、IT 担当者がインストール後のタスクを実行する際に、Power-on Authentication をアクティブにする必要なく、エンドポイントコンピュータにログオンできます。
- POA アクセス アカウントを使用すると、IT 担当者は、Power-on Authentication がアクティブ化されている暗号化済みのエンドポイントコンピュータにログオンし、管理タスクを実行できます。

Sophos SafeGuard の復旧シナリオ

Sophos SafeGuard には、さまざまな復旧シナリオに合わせて個別のオプションが用意されています。

- Local Self Help によるログオン復旧

Local Self Help を使用すると、パスワードを忘れたユーザーは、ヘルプデスク担当者の手を煩わせることなく自分のコンピュータにログオンできます。電話もネットワーク接続も利用できない状況 (飛行機に乗っている場合など) でも、ユーザーは自分のコンピュータにアクセスできるようになります。ログオンするには、Power-on Authentication で、事前定義済みの複数の質問に答えます。

Local Self Help の使用によって、ログオン復旧に関する問い合わせが削減するため、ヘルプデスク担当者は単純な作業から解放され、より複雑な問題解決に集中できるようになります。

■ チャレンジレスポンスによる復旧

チャレンジレスポンスによる復旧では、ヘルプデスク担当者の支援が必要です。自分のコンピュータにログオンできない場合や、暗号化データにアクセスできない場合に便利です。チャレンジレスポンスでは、エンドポイント コンピュータで生成されたチャレンジコードをユーザーがヘルプデスク担当者に渡すと、ヘルプデスク担当者は、そのコンピュータでの特定の処理の実行を認証するレスポンス コードを生成します。Sophos SafeGuard のチャレンジレスポンスによる復旧では、ヘルプデスク担当者の支援を必要とする一般的な復旧シナリオに応じて、それぞれ異なったワークフローで対処しています。

■ システム復旧

Sophos SafeGuard には、Sophos SafeGuard 用にカスタマイズされた Windows PE 回復ディスクや Lenovo Rescue and Recovery など、システム復旧のための方法・ツールが複数あります。Windows システムおよび Sophos SafeGuard コンポーネントで発生した問題は、これらのツールを使用して対処できます。

復旧は、鍵復旧ファイルに基づいて行われます。鍵復旧ファイルは、Sophos SafeGuard で暗号化されているコンピュータごとに作成され、通常、ネットワーク共有に保存されます。この復旧鍵を使用すると、故意に暗号化システムが迂回されることなく復旧処理を実行できます。また、復旧鍵は暗号化されるため、さらにセキュリティが強化されます。このようなファイルを保存するネットワーク共有とその共有へのアクセス権限は、初期構成時に自動的に作成されます。

3 旧バージョンからのアップグレード

Sophos SafeGuard 5.6 x には、重要な拡張機能が含まれています。

■ バージョン 5.5x からのアップグレード:

すでに SDE 5.5x や SGE 5.5x を使用して暗号化されているコンピュータは、バージョン 5.6x にアップグレードできます。

■ バージョン 4.x からのアップグレード:

すでに SDE 4.6x や SGE 4.3x~4.5x を使用して暗号化されているコンピュータは、Sophos SafeGuard 5.6x にアップグレードできます。

Sophos SafeGuard ではバージョン 5.5x から、SDE 4.x や SGE 4.x と下位互換性のない、新しい管理ツール SafeGuard Policy Editor が使用されています。旧バージョンで暗号化されたボリュームは暗号化されたままになり、暗号化鍵は、バージョン 5.5x と互換性のある形式に変換されます。

Sophos SafeGuard 5.6x では、SafeGuard Policy Editor にインポートする、有効なライセンスファイルが必要です。ライセンスファイルは、セールスパートナーから取得してください。

Sophos SafeGuard 5.6x にアップグレードする前に、SafeGuard Policy Editor を使用して新しい構成パッケージを作成し、Sophos SafeGuard 5.6x ソフトと共に展開してください。

詳細は、管理者ヘルプの「**SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x から Sophos SafeGuard 5.6x へのアップグレード**」の章、および <http://www.sophos.co.jp/support/knowledgebase/article/108561.html> をご覧ください。

4 インストールするコンポーネント

インストールするコンポーネントは次のとおりです。

- SafeGuard Policy Editor: これは、Sophos SafeGuard の管理ツールです。エンドポイント コンピュータ上の暗号化ソフトウェアを管理し、復旧タスクを実行できます。

Sophos SafeGuard ポリシー設定の保存に使用される Microsoft SQL Server 2005 Express は、SQL サーバーのインスタンスが使用できない場合、SafeGuard Policy Editor セットアップ時に自動的にインストールされます。

ヒント:

はじめに、Windows サーバーに SafeGuard Policy Editor をインストールします。後で、それを、サーバー上の一元管理対象の Sophos SafeGuard データベースに接続されている、複数の管理者用コンピュータにインストールできます。

- Sophos SafeGuard 暗号化ソフトウェア: エンドポイント コンピュータ上のデータを暗号化し、不正アクセスから保護します。

ヒント:

この暗号化ソフトウェアは、Sophos SafeGuard の管理に使用している管理者用コンピュータにはインストールしないことをお勧めします。

5 主な作業項目

主な作業項目は次のとおりです。

- SafeGuard Policy Editor をインストールする。
- 初期構成を実行する。デフォルト ポリシーを作成し、ヘルプデスク担当者が復旧作業を実行できるよう設定します。
- デフォルト ポリシーをコピーして、編集する。
- インストール後の管理タスクを実行できるよう、エンドポイント コンピュータを構成する。
- 編集したポリシーを構成パッケージに公開する。
- エンドポイント コンピュータに暗号化ソフトウェアと構成パッケージをインストールする。

6 SafeGuard Policy Editor のインストール

操作を開始する前に次の内容を確認してください。

- SafeGuard Policy Editor のインストール先コンピュータに、.NET Framework 3.0 SP1 がインストール済みであることを確認します。次のサイトから無料でダウンロードできます。 <http://www.microsoft.com/japan/downloads>
- システム要件を確認します。
<http://www.sophos.co.jp/support/knowledgebase/article/112891.html>。
- Windows の管理者権限があることを確認します。

SafeGuard Policy Editor をインストールする方法は次のとおりです。

1. 管理者権限でコンピュータにログオンします。
2. ソフォスの Web サイトを開き、社内のシステム管理者がら入手したアカウント情報で「製品・アップデート版のダウンロード」ページにログオンし、インストーラをダウンロードします。

- 製品のインストールフォルダで、インストールする製品に応じて、次のいずれか1つをダブルクリックします。ウィザードの指示に従って必要な手順を実行します。

Sophos SafeGuard Disk Encryption	SafeGuard Easy
SDEPolicyEditor.msi	SGNPolicyEditor.msi

- これ以降のダイアログではデフォルトの設定をそのまま指定します。

Microsoft SQL Server 2005 Express をインストールするようプロンプト指示されたら、「はい」をクリックします。この場合、使用中の Windows ログオン情報が、SQL のユーザー アカウントとして使用されます。

- 「完了」をクリックして、インストールを完了します。

SafeGuard Policy Editor がインストールされます。次に、SafeGuard Policy Editor で初期構成を実行します。

7 初期構成の実行

Windows の管理者権限があることを確認します。

- 「開始」メニューから、SafeGuard Policy Editor を開始します。構成ウィザードが起動されます。画面の指示に従って必要な手順を実行してください。
- 「ようこそ」ページで、「次へ」をクリックします。
- 「データベース」ページで、「次へ」をクリックします。SafeGuard の設定とポリシーを格納するための SQL データベースが作成されます。
- 「セキュリティ担当者」ページで、SafeGuard Policy Editor のアクセスに必要なパスワードを入力し、確認入力します。「次へ」をクリックします。セキュリティ担当者の証明者が作成されます。

このパスワードは安全な場所に保管してください。パスワードを忘れてしまった場合、以降、SafeGuard Policy Editor にアクセスできなくなります。また、IT ヘルプデスクのスタッフが復旧作業を実行するには、このアカウントにアクセスする必要があります。

セキュリティ担当者の名前が表示されます。

Sophos SafeGuard Disk Encryption	SafeGuard Easy
セキュリティ担当者の名前は常に「Administrator」です。	現在のユーザー名が表示されます。

5. 「**企業**」 ページで、「**次へ**」をクリックします。企業証明書は、データベース内やエンドポイント コンピュータ上のポリシー設定を保護するために作成されます。
6. 「**セキュリティ担当者**と**企業証明書のバックアップ**」 ページで、証明書のバックアップの保存場所を指定します。次に、「**次へ**」をクリックします。

今すぐデフォルトの保存場所に証明書を保存する場合は、復旧が必要なときにアクセスできる場所 (USB メモリスティックなど) に、初期構成後すぐにエクスポートしてください。証明書は、SafeGuard Policy Editor のインストールに失敗したり、データベースが破損したりしたときに必要です。

7. 「**復旧鍵**」 ページで、「**次へ**」をクリックします。IT ヘルプデスク担当者用の十分なアクセス許可のあるネットワーク共有が作成されます。この共有は、復旧に必要な鍵復旧ファイルを、エンドポイント コンピュータから収集するために使用されます。

ヒント:

Sophos SafeGuard 暗号化ソフトウェアは、ネットワーク共有への接続を約4分間試みます。接続できない場合は、接続が確立するか、復旧鍵ファイルが手動でバックアップされるまで、Windows にログオンするたびに接続を再試行します。

8. 「**ライセンス**」 ページで [...] をクリックして、SafeGuard Policy Editor を運用環境で実行するために必要な有効なライセンスファイルを参照します。ライセンスファイルは、セールスパートナーから取得してください。ファイルを選択し、「**開く**」をクリックします。「**次へ**」をクリックします。
9. 「**完了**」をクリックします。

初期構成が完了します。

- 会社規模のセキュリティ ポリシーをエンドポイント コンピュータに実装するためのデフォルト ポリシーが作成されました。

Power-on Authentication が有効になっています。

すべての内蔵ハードディスクで、ボリューム ベースの暗号化が有効になっています。

ユーザーは、パスワードを忘れた場合、Local Self Help で事前に定義された質問に回答して、復旧できます。

ヘルプデスク担当者は、チャレンジ/レスポンスを使用してパスワードを復旧できます。

SafeGuard Easy ユーザーの場合のみ、ファイルベースの暗号化が有効になっています。

- ヘルプデスク担当者が復旧タスクを実行するにあたり必要となる前提条件が、すべて設定されています。
- Sophos SafeGuard を運用環境で実行するため、有効なライセンスファイルがインポートされました。

構成ウィザードが閉じると、SafeGuard Policy Editor が開始します。

8 デフォルト ポリシーのコピーと編集

1. SafeGuard Policy Editor のナビゲーションエリアで、「ポリシー」をクリックします。
2. 「ポリシー」ナビゲーションペインの「ポリシーグループ」で、「デフォルト ポリシー」を右クリックし、「ポリシーのバックアップ」をクリックします。
3. バックアップファイル (XML) の名前と保存場所を入力して、「保存」をクリックします。
4. ナビゲーションペインで「ポリシー グループ」を右クリックし、「ポリシーの復元」をクリックします。
5. 作成したポリシーのコピー (XML) を選択し、「開く」をクリックします。

ポリシー項目すべてを含む、デフォルトポリシーのコピーが SafeGuard Policy Editor に再びインポートされます。

次に、このデフォルトポリシーのコピーをカスタマイズして、インストール後の管理タスクをエンドポイントコンピュータで実行できるように、サービスアカウントのリストを設定します。これによって、サービス担当者は、コンピュータの所有者として指定されることなく、暗号化ソフトウェアがインストール済みのコンピュータにアクセスし、事前に構成することができます。

9 インストール後に実行する管理タスクのためのエンドポイント コンピュータの構成

サービス担当者は、暗号化ソフトウェアをインストールした後も、1カ所から集中的に設定する場合など、エンドポイントコンピュータにアクセスし、事前に構成を行わなくてはならないことがあります。しかし、暗号化ソフトウェアのインストール後、最初にコンピュータにログオンするユーザーは POA をアクティブ化し、Sophos SafeGuard ユーザーとしてコンピュータに追加されてしまいます。これを避けるには、ユーザーをサービスアカウントのリストに追加します。このリストに含まれるサービス担当者は、暗号化ソフトウェアのインストール後、コンピュータの OS にログオンし、Sophos SafeGuard ユーザーとしてコンピュータに追加されたり、POA をアクティブ化したりすることなく、必要な管理タスクを実行することができます。

サービスアカウントのリストを設定する方法は次のとおりです。

1. SafeGuard Policy Editor のナビゲーションエリアで、「ポリシー」をクリックします。
2. 「ポリシー」ナビゲーションペインで「サービスアカウントのリスト」を右クリックし、「新規作成-サービスアカウントのリスト」をクリックします。
3. リストの名前を入力し、「OK」をクリックします。
4. ナビゲーションペインの「サービスアカウントのリスト」で、表示される新しいリストを選択します。
5. 処理ペインの右側を右クリックして、ショートカットメニューから「追加」を選択します。新しいユーザー行が追加されます。
6. 該当する列に Windows の「ユーザー名」と「ドメイン名」を入力し、「Enter」キーを押します。さらにユーザーを追加するには、この手順を繰り返します。詳細は、管理者ヘルプの「ユーザー名およびドメイン名の入力に関する詳細情報」の章を参照してください。
7. ツールバーの「保存」アイコンをクリックし、変更をデータベースに保存します。

これで、サービスアカウントのリストが登録されました。次に説明する手順で、ポリシーに割り当てます。

8. ナビゲーションペインの「ポリシー項目」で、コピーした「認証」ポリシー項目を選択します。
9. 「ログオンオプション」で、「サービスアカウントのリスト」を選択し、新規作成したリストを選択します。
10. ツールバーの「保存」アイコンをクリックし、変更を保存します。

これで、サービスアカウントのリストが設定されました。「認証」ポリシー項目と関連するポリシーグループは、随時アップデートされます。次に、編集したポリシーを構成パッケージに公開します。

ヒント:

POA をカスタマイズする場合や暗号化を構成する場合、または Wake-on-LAN を有効にする場合など、必要に応じてポリシー設定をさらに編集することができます。詳細は、管理者ヘルプの「ポリシー設定」の章を参照してください。

10 構成パッケージへのポリシーの追加

ポリシーをエンドポイントコンピュータに適用するには、まず、適用するポリシーを構成パッケージに追加する必要があります。

1. SafeGuard Policy Editor の「ツール」メニューで、「構成パッケージツール」をクリックします。
2. 「構成パッケージの追加」をクリックします。
3. 構成パッケージに対して任意のパッケージ名を入力します。
4. 前の手順で編集した、エンドポイントコンピュータに適用するための「ポリシーグループ」を選択します。
5. 構成パッケージの保存先を指定します。
6. 「構成パッケージの作成」をクリックします。
7. 「閉じる」をクリックします。

ポリシーは、指定した場所にある構成パッケージ (MSI) に追加されます。次に、エンドポイントコンピュータに Sophos SafeGuard 暗号化ソフトウェアと構成パッケージをインストールします。

11 エンドポイントコンピュータへの暗号化ソフトウェアと構成パッケージのインストール

1. 暗号化にあたってエンドポイント コンピュータを準備します。
2. 製品に関する十分な知識を得るため、まずテスト用コンピュータに Sophos SafeGuard をインストールします。SafeGuard Policy Editor をインストール済みのコンピュータとは別のコンピュータにインストールしてください。
3. 初回のログオンを行います。
4. エンドポイント コンピュータ上の暗号化ソフトウェアを一元的に設定するため、お持ちのツールを使用してインストールパッケージと構成パッケージを作成および配布します。

11.1 暗号化前のエンドポイント コンピュータの準備作業

- ユーザーアカウントが設定済みであること、およびアクティブ化されていることを確認します。ユーザーはパスワードの入力が必要となります。
- データのフルバックアップを作成します。
- 開いているアプリケーションはすべて閉じます。
- Windows の管理者権限があることを確認します。
- ハードディスクに十分な空き容量があることを確認します。

- POA とお使いのコンピュータのハードウェア間で競合する可能性を最小限にするために、ハードウェアの構成リストが用意されています。このリストは、暗号化ソフトウェアのインストールパッケージに含まれています。

Sophos SafeGuard を大規模に展開する前に、ハードウェアの構成リストの最新版をエンドポイント コンピュータにインストールすることをお勧めします。このファイルは毎月更新されます。ダウンロード元は次のとおりです。<ftp://POACFG:POACFG@ftp.ou.utimaco.de>

詳細は、管理者ヘルプの「**POA で使用可能なホットキー**」の章を参照してください。次の文章も参照してください。

<http://www.sophos.co.jp/support/knowledgebase/article/65700.html>

- 次のコマンドを実行してハードディスクにエラーがないかチェックします。

chkdsk %drive% /F /V /X

コンピュータを再起動し、もう一度 **chkdsk** を実行するようメッセージが表示される場合があります。詳細は次の文章を参照してください。

<http://www.sophos.co.jp/support/knowledgebase/article/107081.html>

Windows のイベントビューアで結果 (ログファイル) を確認できます。

Windows XP: 「アプリケーション」を選択し、ソースが「**Winlogon**」の項目を確認します。

Windows 7/Windows Vista: 「**Windows ログ**」、「アプリケーション」の順に展開し、ソースが「**Wininit**」の項目を確認します。

- Windows に付属の **デフラグ** ツールを使用して、ローカル ボリューム上で断片化されているブート ファイル、データ ファイル、およびフォルダを検出し、最適化します。

defrag %drive%

詳細は次の文章を参照してください。

<http://www.sophos.co.jp/support/knowledgebase/article/109226.html>

- 「PROnetworks Boot Pro」や「Boot-US」などの、サードパーティ製ブートマネージャをアンインストールします。
- マスタブートレコード (MBR) を初期状態にすることを推奨します。Sophos SafeGuard をインストールするには、一意で初期状態の MBR が必要です。エンドポイント コンピュータでイメージクローン作成ツールを使用した場合、初期の状態でなくなる可能性があります。

コンピュータを Windows DVD から起動し、Windows 回復コンソール内で **FIXMBR** コマンドを実行します。詳細は次の文章を参照してください。
<http://www.sophos.co.jp/support/knowledgebase/article/108088.html>

- エンドポイント コンピュータのブートパーティションを FAT から NTFS に変換して以来、コンピュータを再起動していない場合は、Sophos SafeGuard をインストールする前に 1 度再起動してください。アクティブ化したときのファイルシステムは NTFS ですが、インストール時のファイルシステムは FAT となるため、再起動しないとインストールが完了しないことがあります。

11.2 テストインストールの実行

暗号化ソフトウェアのテストインストールを実行する場合は、SafeGuard Policy Editor がインストールされていないコンピュータにインストールしてください。

1. エンドポイント コンピュータのインストール前の準備を行います。詳細は、[暗号化するためエンドポイント コンピュータを準備する \(p. 12\)](#) を参照してください。
2. エンドポイント コンピュータに管理者権限でログオンします。
3. プレインストールパッケージ **SGxClientPreinstall.msi** をインストールします。暗号化ソフトウェアを正常にインストールするために必要なコンポーネントが、エンドポイント コンピュータにインストールされます。
4. エンドポイント コンピュータに暗号化ソフトウェアをインストールします。次のいずれか 1 つのパッケージ (MSI) をダブルクリックして、暗号化ソフトウェアのインストールウィザードを開始します。画面の指示に従って必要な手順を実行します。

Sophos SafeGuard Disk Encryption	Sophos SafeGuard Easy
SDEClient.msi (32 ビットの場合)、または SDEClient_x64.msi (64 ビットの場合)。	SGNClient.msi (32 ビットの場合)。 SGNClient_x64.msi (64 ビットの場合)。

5. これ以降のダイアログではデフォルトを指定します。

6. プロンプトに従って、インストールの種類で「すべて」を選択します。

Sophos SafeGuard Easy: SafeGuard Device Encryption および **SafeGuard Data Exchange** がインストールされます。他のクライアントインストールパッケージの詳細については、管理者ヘルプの「インストール」の章をご覧ください。

Sophos SafeGuard Disk Encryption: SafeGuard Device Encryption がインストールされます。**SafeGuard Data Exchange** はインストールされません。

7. これ以降のすべてのダイアログでデフォルト値を受け入れて、インストールウィザードを完了します。
8. 以前作成した構成パッケージ (MSI) の保存場所に移動します。
9. この構成パッケージをエンドポイント コンピュータにインストールします。エンドポイント コンピュータにある古い構成パッケージはすべて削除するようにしてください。

Sophos SafeGuard はエンドポイント コンピュータにインストールされ、事前に作成されたポリシーに基づいて構成されます。次に、インストール後の初回ログオンを行います。インストール後の管理タスクを行う場合は、サービスアカウントを使用してログオンし、コンピュータの所有者になる場合は、通常のユーザーとしてログオンします。

各ハードウェア OS で POA が正常に動作するには、追加の構成が必要になる場合があります。ハードウェア競合の問題のほとんどは、POA に組み込まれている「ホットキー」機能を使用して解決できます。インストール後、ホットキーは、POA で設定したり、追加構成のパラメータとともに `msiexec` 展開ツールを使用して設定したりできます。詳細は、管理者ヘルプの「**POA で使用可能なホットキー**」のセクションをご覧ください。次の文章もご覧ください。

<http://www.sophos.co.jp/support/knowledgebase/article/107781.html>

<http://www.sophos.co.jp/support/knowledgebase/article/107785.html>

11.3 サービス アカウントを使った初回ログオン

コンピュータで、インストール後の管理タスクを行う場合は、サービスアカウントでログオンします。

1. インストール後、エンドポイントコンピュータを再起動します。Windows ログオンが表示されます。

Windows Vista および Windows 7 環境では、ログオンを開始するには、まず「Ctrl + Alt + Del」キーを押す必要があります。管理者は「**Windows の設定 > セキュリティの設定 > ローカル ポリシー > セキュリティ オプションの無効化**」(対話式ログオンの場合: 「Ctrl + Alt + Delete」は不要)の順に選択して、グループ ポリシー オブジェクト エディタの MMC コンソールで、この設定を無効にできます。

2. サービス アカウントを使用して、Windows にログオンします。SafeGuard Policy Editor のサービス アカウント リストで定義済みのドメインとログオン情報を入力します。

ゲストユーザーとして Windows にログオンしました。Power-on Authentication はアクティブ化されず、このコンピュータの所有者には指定されませんでした。これで、インストール後の管理タスクを必要に応じて実行することができます。

11.4 サービス アカウントなしの初回ログオン

1. コンピュータを再起動します。Sophos SafeGuard Autologon が表示された後、Windows ログオンが表示されます。

Windows Vista および Windows 7 環境で、自動ログオン/ログオンを開始するには、まず「Ctrl + Alt + Del」キーを押す必要があります。管理者は、MMC コンソールの「グループ ポリシー オブジェクト エディタ」で、「**Windows の設定 > セキュリティの設定 > ローカル ポリシー > セキュリティ オプション**」を選択し、「対話型ログオン: CTRL+ALT+DEL を必要としない」を「無効」に指定して、この設定を無効にできます。

2. Windows ユーザー名とパスワードを入力します。
3. 再度コンピュータを再起動します。Sophos SafeGuard Power-on Authentication がアクティブ化されます。
4. Windows ユーザー名とパスワードを入力します。ユーザーは自動的に Windows にログオンします。

これで Power-on Authentication がアクティブ化されました。ユーザーは、Sophos SafeGuard ユーザーとして登録されます。これは、ツールチップに表示されます。次回ログオンするときは、Power-on Authentication で Windows ログオン情報を入力するだけです。

初期暗号化が自動的に開始します。ユーザーは作業を継続でき、暗号化が完了してもコンピュータを再起動する必要はありません。暗号化と復号化は透

過的に実行され、ユーザー介入は不要です。詳細は、ユーザー ヘルプ (「Sophos SafeGuardのインストール後の最初のログオン」および「データの暗号化」の章) を参照してください。

11.5 スクリプトによる暗号化ソフトウェアと構成パッケージのインストール

1. エンドポイント コンピュータのインストール前の準備を行います。詳細は、[暗号化前のエンドポイント コンピュータの準備作業](#) (p. 12) を参照してください。
2. 管理者用コンピュータに管理者権限でログオンします。
3. すべてのアプリケーションを一括に格納する **Software** という名前のフォルダを作成します。

4. Microsoft System Center Configuration Manager、IBM Tivoli や Enteo Netinstall などのソフトウェア展開ツールを使用して、エンドポイント コンピュータに一括インストールを行ってください。次のパッケージを上から順にインストールする必要があります。

オプション	説明
パッケージ	説明
プレインストールパッケージ SGxClientPreinstall.msi	暗号化ソフトウェアを正常にインストールするために必要なコンポーネントがエンドポイント コンピュータにインストールされます。 ヒント: このパッケージがインストールされていない場合、暗号化ソフトウェアのインストールは中止されます。
暗号化ソフトウェア インストールパッケージ <Client>*.msi	OS やインストールする製品に応じて、異なるインストールパッケージが用意されています。Windows 7/Vista の場合、*_x64.msi 版のパッケージをインストールできます。必要な <Client> インストールパッケージはすべて製品パッケージ内にあります。 ヒント: クライアントインストールパッケージすべての詳細については、管理者ヘルプの「インストール」の章を参照してください。
エンドポイント コンピュータ用の構成パッケージ	あらかじめ SafeGuard Policy Editor で作成した構成パッケージを使用します。古い構成パッケージは必ず削除するようにしてください。
事前に構成されたインストール用のコマンドを実行するスクリプト	Windows インストーラのコマンドライン ツール、 msiexec を使用してスクリプトを作成することをお勧めします。詳細は、管理者ヘルプの「一括インストールのコマンド」の章、または次のサイト(英語)を参照してください。 http://msdn.microsoft.com/ja-jp/library/aa367988(VS.85).aspx

5. スクリプトを作成するには、コマンドプロンプトを開き、スクリプトのコマンドを入力します。詳細は、[スクリプトで使用するコマンドの例](#)(p.19)を参照してください。

6. プレインストールパッケージ、<Client>パッケージ、構成パッケージ、およびスクリプトを、社内のソフトウェア配布方法を使用してエンドポイントコンピュータに配布します。

パッケージは、エンドポイントコンピュータで実行されます。

Sophos SafeGuard はエンドポイントコンピュータにインストールされ、事前に作成されたポリシー設定に基づいて構成されます。各エンドポイントコンピュータに対し、復旧に必要な鍵復旧ファイルは、SafeGuard Policy Editor 初期構成時に定義した場所に作成されます。

各ハードウェア OS で Power-on Authentication (POA) が適切に機能するには、追加の構成が必要になる場合があります。ハードウェア競合の問題のほとんどは、POA に組み込まれている「ホットキー」を使用して解決できます。インストール後、ホットキーは、POA で設定したり、追加構成のパラメータとともに Windows インストーラ コマンド ツール `msiexec` を使用して設定したりできます。詳細は、管理者ヘルプの「**POA で使用可能なホットキー**」のセクションを参照してください。次の文章も参照してください。

<http://www.sophos.co.jp/support/knowledgebase/article/107781.html>

<http://www.sophos.co.jp/support/knowledgebase/article/107785.html>

11.6 スクリプトで使用するコマンドの例

```
msiexec /i  
F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi /qn
```

```
msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi /qn
```

```
/L*VX
```

```
G:\Temp\Sophos\SafeGuard\%computername%_SDEClient_inst.log
```

```
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard
```

```
msiexec /i F:\Software\Sophos\SafeGuard\SDEClientConfig.msi  
/qn
```

このコマンドは以下の項目を実行します。

```
msiexec /i  
F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
```

Sophos SafeGuard のプレインストールパッケージを、指定された保存場所からデフォルトのインストールディレクトリ **C:\Program Files\Sophos\Sophos SafeGuard** にインストールします。暗号化ソフトウェアを正常にインストールするために必要なコンポーネントがエンドポイント コンピュータにインストールされます。

```
msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi
```

```
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard
```

Power-on Authentication 機能を指定して暗号化ソフトウェア（ここでは SafeGuard Device Encryption）を、指定された保存場所からデフォルトのインストールディレクトリ **C:\Program Files\Sophos\Sophos SafeGuard** にインストールします。

```
msiexec /i  
F:\Software\Sophos\SafeGuard\SDEClientConfig.msi
```

構成パッケージを、その保存場所からデフォルトのインストールディレクトリにインストールします。

```
/L*VX  
G:\Temp\Sophos\SafeGuard\%computername%__SDEClient_inst.log
```

すべての警告およびエラーメッセージをネットワーク上の指定したログファイルに記録します。また、暗号化処理を一括確認できるログファイルも作成します。ログファイルは、Windows インストーラ ツール **wilogutl.exe** を使って分析可能です。

```
/qn
```

ユーザーの介入なしでインストールを実行し、GUI も表示しません。

12 パスワードを忘れた場合の復旧

ユーザーがパスワードを忘れた場合、次の2とおりの方法で復旧することができます。

- ユーザー自身が Local Self Help を使用してパスワードを復旧する。これは推奨方法です。
- ヘルプデスク担当者がチャレンジ/レスポンスを使用してパスワードを復旧する。

12.1 Local Self Help による忘れたパスワードの復旧

1. エンドポイント コンピュータの Power-on Authentication で、ユーザーは自分のユーザー名を入力します。

「復旧」ボタンが有効になります。

2. ユーザーは「復旧」をクリックします。
 - エンドポイント コンピュータでログオン復旧のために Local Self Help だけが有効になっている場合、それは自動的に開始します。
 - ログオン復旧のためにチャレンジ/レスポンスと Local Self Help の両方が使用可能である場合、ユーザーは「**Local Self Help**」をクリックします。

3. 次に表示される5つのダイアログで、ユーザーは、エンドポイント コンピュータに保存されている質問の中から任意に選択された一定の数の質問に回答します。最後の質問に回答した後、ユーザーは、「**OK**」をクリックして回答を確定します。

4. 次に表示されるダイアログで、ユーザーは、「Enter」キーやスペースキーを押すか、青い表示ボックスをクリックして、パスワードを表示できます。

パスワードは最長5秒間表示されます。その後、スタートアップ処理が自動的に続行されます。ユーザーは、「Enter」キーやスペースキーを押すか、青い表示ボックスをクリックして、すぐにパスワードを非表示にすることができます。

5. パスワードの表示後、ユーザーは「**OK**」をクリックします。

これでユーザーは Power-on Authentication および Windows にログオンしました。このパスワードは、今後のログオンでも使用できます。

12.2 チャレンジ/レスポンスによる忘れたパスワードの復旧

前提条件:

ヘルプデスク担当者は、Sophos SafeGuard のインストール時にエンドポイント コンピュータごとに作成される鍵復旧ファイルにアクセス可能で、そのファイル名を知っている必要があります。チャレンジレスポンス機能は、エンドポイント コンピュータ用のポリシーで有効にする必要があります。

ヒント:

パスワードを忘れた場合、まず Local Self Help を使用して復旧することをお勧めします。Local Self Help には現在のパスワードが表示され、ユーザーはそのパスワードを引き続き使用できます。したがって、パスワードの再設定を行ったり、ヘルプデスク担当者に依頼したりする必要がなくなります。

1. エンドポイント コンピュータの Power-on Authentication で、ユーザーは自分のユーザー名を入力します。「復旧」ボタンが有効になります。
2. ユーザーは「復旧」をクリックします。
 - ログオン復旧のためにチャレンジレスポンスだけが有効になっている場合、それは自動的に開始します。
 - ログオン復旧のためにチャレンジレスポンスと Local Self Help の両方が使用可能である場合、ユーザーは「チャレンジレスポンス」をクリックします。

必要な鍵復旧ファイルの名前がダイアログに表示されます。

3. ユーザーは「次へ」をクリックします。任意のチャレンジコードが表示されます。
4. ユーザーはヘルプデスク担当者に連絡を取り、必要な鍵復旧ファイルの名前とチャレンジコードを伝えます。
5. SafeGuard Policy Editor で、ヘルプデスク担当者は「復旧ウィザード」を起動します。
6. ヘルプデスク担当者は、復旧の種類「Sophos SafeGuard Client」を選択し、鍵およびチャレンジコードを確認し、必要な復旧処理「ユーザー ログオンなしの起動」を選択します。

ASCII 文字列形式のレスポンスコードが生成され、表示されます。

7. ヘルプデスク担当者は、電話またはテキストメッセージを使って、ユーザーにレスポンスコードを提供します。
8. ユーザーは、エンドポイント コンピュータのチャレンジレスポンスウィザードで「次へ」をクリックして、レスポンスコードを入力します。コンピュータは、Power-on Authentication で起動できる状態になります。

9. Windows のログオンダイアログでも、ユーザーは正しいパスワードがわからないため、Windows レベルでパスワードを変更する必要があります。変更するには、Sophos SafeGuard 以外に、Windows 標準の方法による復旧処理が必要になります。Windows レベルでパスワードをリセットするときは、以下の方法をお勧めします。
 - エンドポイント コンピュータ上で使用できるサービスまたは管理者アカウントのうち、必要な Windows 権限を持つアカウントを使用する。
 - エンドポイント コンピュータ上で Windows パスワードリセット ディスクを使用する。
10. ユーザーは、ヘルプデスク担当者によって提供された、新しい Windows パスワードを入力します。ユーザーはすぐに、このパスワードを自分だけが知っている値に変更します。
11. Sophos SafeGuard は、新しく設定されたパスワードが、POA で使用されている現在の Sophos SafeGuard パスワードに一致していないことを検出します。このためユーザーは、古い Sophos SafeGuard パスワードの入力を求められます。ユーザーはこれを覚えていないため、「キャンセル」をクリックする必要があります。
12. Sophos SafeGuard では、古いパスワードを入力せずに新しいパスワードを設定するには、新しい証明書が必要になります。この手続きは、ユーザーが確定する必要があります。
13. 新しいユーザー証明書は、新しく設定された Windows パスワードに基づいて作成されます。

ユーザーは、新しく設定したパスワードで Power-on Authentication および Windows にログインすることができます。このパスワードは、今後のログオンでも使用できます。

13 よく実行するタスクに関する参照資料

よく実行するタスクの概要とその操作手順が記載されているドキュメントは次のとおりです。詳細は、Sophos SafeGuard の管理者ヘルプ、ユーザーヘルプ、またはツールガイドを参照してください。

タスク	マニュアル/ヘルプ
SafeGuard Policy Editor の追加インスタンスを構成する。	管理者ヘルプ: 「SafeGuard Policy Editor の追加インスタンスを構成する」
Power-on Authentication が正しく機能していることを確認する。	管理者ヘルプ/ユーザーヘルプ: 「Power-on Authentication で対応しているホットキー」

タスク	マニュアル/ヘルプ
Sophos SafeGuardに固有の情報をエンドポイント コンピュータで表示する。	ユーザー ヘルプ: 「システム 트레이 アイコンとツールチップ」
ポリシーを作成し、グループ化する。	管理者ヘルプ: 「ポリシーの使用について」
証明書をエクスポートする。	管理者ヘルプ: 「企業証明書とセキュリティ担当者の証明書のエクスポート」
エンドポイントコンピュータで管理タスクを実行するためのアカウント (POA アクセスアカウント) を作成する。	管理者ヘルプ: 「エンドポイントコンピュータで管理タスクを実行するためのアカウント」
暗号化データへのアクセスを復旧する。	管理者ヘルプ: 「仮想クライアントを使用したチャレンジ/レスポンス」
破損したマスターブートレコードを復旧する	ツール ガイド: 「破損した MBR を復旧する」
SDE 4.6x や SGE 4.3x~4.5x から Sophos SafeGuard にアップグレードする。	管理者ヘルプ: 「SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x から Sophos SafeGuard 5.6x へのアップグレード」

14 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。

- 「SophosTalk」 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。 <http://www.sophos.co.jp/support/>
- 製品ドキュメントのダウンロード。 <http://www.sophos.co.jp/support/docs/>
- メールによるお問い合わせ。ソフォス製品のバージョン番号、OS および適用しているパッチの種類、エラーメッセージの内容などを、support@sophos.co.jp までお送りください。

15 ご利用条件

Copyright © 1996 - 2011 Sophos Group. All rights reserved. SafeGuard は Sophos Group の登録商標です。

Sophos は Sophos Limited、Sophos Group および ウィテック・セーフウェア AG の登録商標です。その他、記載された製品名および社名は、各社の商標または登録商標です。

この出版物の一部または全部を、電子的、機械的な方法、写真複写、録音、その他いかなる形や方法においても、使用許諾契約の条項に準じてドキュメントを複製することを許可されている、もしくは著作権所有者からの事前の書面による許可がある場合以外、無断に複製、復元できるシステムに保存、または送信することを禁じます。

サードパーティコンポーネントの著作権に関する情報は、製品ディレクトリ内の「Disclaimer and Copyright for 3rd Party Software.rtf」(英語) という名前のファイルをご覧ください。