SOPHOS
Security made simple.

SafeGuard Enterprise
Web Helpdesk

製品バージョン: 7
ドキュメント作成日: 2014年 12月

目次

1 SafeGuard の Web ベースチャレンジ/レスポンス

SafeGuard Enterprise には、社内ワークフローを効率化し、ヘルプデスクの運用コストを削減する Web ベースの復旧ソリューション、Web Helpdesk が用意されています。Web Helpdesk は、ユーザーがコンピュータにログオンできない場合や、暗号化されたデータにアクセスできない場合に、簡単で使いやすいチャレンジ/レスポンス機能でユーザーを支援するシステムです。

また、Web Helpdesk を使って SafeGuard の構成保護ポリシーを一時的に中断することもできます。

チャレンジ/レスポンスの利点

チャレンジ/レスポンス機能は、安全性および効率性の高い緊急事態対応用システムです。

- すべてのプロセスで機密データが交換されるときは、必ず暗号化された状態で交換されます。
- 後でデータを使用したり、他のデバイスで使用したりできないようになっているため、第三者がこの処理を傍受したとしても問題はありません。
- エンドポイントにアクセスするときに、ネットワーク接続は必要ありません。ヘルプデスク用のレスポンス コード ウィザードは、複雑なインフラストラクチャを必要とせず、スタンドアロン PC でも実行できます。
- ユーザーはすばやく作業を再開できます。パスワードを忘れただけなので、暗号化されたデータが失われているわけではありません。

チャレンジ/レスポンスのワークフロー

チャレンジ/レスポンスを実行すると、エンドポイント上にチャレンジ コード (ASCII 文字列) が生成され、ユーザーはこのコードをヘルプデスク担当者に伝えます。ヘルプデスク担当者は、チャレンジコードをもとに、ユーザーにエンドポイントでの特定の操作を許可するレスポンス コードを生成します。

緊急にヘルプデスクの支援を必要とする状況の一般的な例

- ユーザーがログオンのためのパスワードを忘れ、エンドポイントがロックされてしまった場合。
- ユーザーがトークン/スマートカードを忘れた場合/紛失した場合。
- Power-on Authentication のローカル キャッシュが部分的に破損した場合。
- 病気または休暇で持ち主が不在のエンドポイントにあるデータにアクセスする必要がある場合。
- あるユーザーが暗号化されたボリュームにアクセスしたいものの、エンドポイント上に当該の鍵がない場合。

SafeGuard Enterprise Web Helpdesk には、このようなよくある緊急事態が発生した際、ユーザーがエンドポイントへのアクセスを取り戻すための、さまざまな復旧ワークフローが用意されています。

2 Web Helpdesk について

Web Helpdeeskは、Web ベースのインターフェースを通じて SafeGuard Enterprise チャレンジ/レスポンス機能を提供します。このWeb アプリケーションへのアクセスはSSL によって制限できるため、ヘルプデスクのタスクを社内で柔軟に振り分けられます。このとき、ヘルプデスク担当者は、機密性の高い構成設定や、SafeGuard Enterprise が一元管理している情報にアクセスする必要はありません。

Web Helpdesk はインターネット/イントラネット上で利用できます。ヘルプデスク担当者のエンドポイントに SafeGuard Enterprise のソフトウェアをインストールする必要はありません。Web サイトは、SafeGuard Enterprise Server ベースのインターネット インフォメーション サービス (IIS) 上で別個にホストする必要があります。

Web ヘルプデスクは、SafeGuard Management Center と一緒に実行できます。

注: 企業イントラネット上だけで Web Helpdesk を利用できるようにすることをお勧めします。セキュリティ上の理由から、 Web Helpdesk はインターネット上に配置しないでください。

Web Helpdesk で復旧できるクライアント

- SafeGuard で暗号化されたエンドポイント (管理型の SafeGuard Enterprise クライアント)
- 仮想クライアント
- SafeGuard で暗号化されたエンドポイント (集中管理されていない SafeGuard Enterprise クライアント (スタンドアロン型))

3 インストール

Web Helpdesk は、SafeGuard Enterprise Server がインストールされている、IIS ベースの Web サーバーにインストールする必要があります。SafeGuard Enterprise Server が利用できないと、インストールするようメッセージが表示されます。その場合は、Web Helpdesk をインストールしたら Web サーバーを構成する必要があります。

担当者はブラウザを使用して Web Helpdesk を管理します。他にソフトウェアをインストールする必要はありません。

3.1 要件

サーバー要件

詳細なサーバーのシステム要件については、リリースノートを参照してください。

- Windows の管理権限があること。
- Microsoft インターネット インフォメーション サービス (IIS) がインストールされていること。
- .NET Framework 4 と ASP.NET 4 がインストールされていること。
- Windows Server 2012 の場合:ASP.NET のロールがインストールされている必要があります (サーバーの役割 > Web サーバー (IIS) > Web サーバー > アプリケーション開発 > ASP.NET 4.5)。

注: Windows Server 2012 環境での注意事項: ASP.Net のアプリケーションでは、ハンドラーのセクションが web.config で事前に設定されています。これは IIS の機能の委任で読み取り専用に設定されています。IIS マネージャで、サーバー名 > 機能の委任を確認してください。ハンドラーマッピングが読み取り専用に設定されており、使用しているサイトの web.config にハンドラーのセクションがある場合は、値を read/write に変更します。

エンドポイントの要件

Web Helpdesk 担当者のコンピュータには、ブラウザがインストールされている必要があります。Web Helpdesk は次のブラウザに対応しています。

- Microsoft Internet Explorer 7 以降
- Mozilla Firefox 2 以降

3.2 Web Helpdesk のインストール

インストールに必要な SGNWebHelpDesk.msi は製品パッケージに含まれています。

1. SGNWebHelpDesk.msi をダブルクリックします。ウィザードの指示に従ってインストールを行います。可能な限り、デフォルトの値をそのまま選択します。インストール項目について確認があった場合「**完全**」を選択します。

2. インストールが完了すると、再起動するようメッセージが表示されることがあります。「**はい**」または「**完了**」をクリックします。

Web Helpdesk をセットアップするときに、SafeGuard Enterprise Server が IIS Web サーバー上で利用できる状態であるかどうかがチェックされます。利用できない場合は、インストールするようメッセージが表示されます。

3.2.1 SSL による Web サーバーの構成

セキュリティレベルを上げるため、次のように IIS Web サーバーを構成してください。

1. Web Helpdesk をイントラネットだけに展開します。

   Web Helpdesk が社内のイントラネットだけに配置されていることを確認してください。セキュリティ上の理由から、 Web Helpdesk はインターネット上に配置しないでください。

2. SSL 接続を確立します。

   IIS であらかじめ設定されている標準の IIS 構成を使用し、特定のユーザーだけが Web Helpdesk を使用できるよう制限を設けられます。SSL セキュリティ証明書が IIS サーバー上にインストールされていることを確認してください。これにより、Web Helpdesk とのすべての通信が SSL を用いて行われます。

   Web サーバーを SSL 対応にするには、次の一般的な設定を行う必要があります。

   a) SSL 暗号化で使う証明書を発行するための証明機関がインストールされている。

   b) 証明書が発行されており、また、SSL を実装し、発行した証明書を参照するように IIS サーバーが構成されている。

   c) SafeGuard Enterprise Server を構成するときに指定するサーバー名が、SSL 証明書に指定されているサーバー名と同じである。そうでない場合は、クライアントとサーバーは通信できません。SafeGuard Enterprise Server ごとに異なる証明書が必要です。

   d) アプリケーションプール、`SGNWHD-Pool` のワーカープロセスが、デフォルトの値である 1 よりも大きい値に設定されていない。設定されている場合、Web Helpdesk の認証に失敗します。

さらに詳しくはテクニカルサポートにお問い合わせください。または以下を参照してください。

- http://msdn2.microsoft.com/ja-jp/library/ms998300.aspx
- http://support.microsoft.com/default.aspx?scid=kb;ja-jp;316898
- https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx (英語)

3.2.2 SafeGuard Enterprise Server の登録・構成

Web Helpdesk をインストールする前に SafeGuard Enterprise Server がまだインストールおよび登録されていない場合は、SafeGuard Enterprise Server を SafeGuard Management Center 内で登録する必要があります。

1. SafeGuard Management Center を開始します。

2. 「**ツール**」メニューの「**構成パッケージ ツール**」をクリックします。
3. 「**サーバー**」タブを選択し、「**追加...**」をクリックします。
4. 「**サーバーの登録**」で「**...**」をクリックし、サーバーのマシン証明書を選択します。この証明書は SafeGuard Enterprise Server のインストール時に生成されます。デフォルトでは SafeGuard Enterprise Server のインストール先ディレクトリの `MachCert` というディレクトリにあります。ファイル名は <コンピュータ名>`.cer` です。SafeGuard Enterprise Server が SafeGuard Management Center とは異なるコンピュータにインストールされている場合は、ネットワーク経由のアクセスを許可するか、ローカルへコピーするなどして、この `.cer` ファイルがアクセス可能な状態である必要があります。

   MSO 証明書を選択しないでください。

   FQDN (完全修飾ドメイン名、例: `server.mycompany.com`) と証明書情報が表示されます。

   SSL でエンドポイントと SafeGuard Enterprise サーバー間の通信内容を暗号化する場合は、ここで指定するサーバー名は SSL 証明書で指定されているサーバー名と同一である必要があります。同一でない場合、エンドポイントとサーバーは通信できません。

5. 「**OK**」をクリックします。

   サーバーの情報が「**サーバー**」タブに表示されます。

6. 「**サーバー用パッケージ**」タブを選択します。使用可能なパーティションが表示されます。必要なサーバーを選択します。サーバー構成パッケージの出力先を指定します。「**構成パッケージの作成**」をクリックします。

   指定したディレクトリに <サーバー名>.msi というサーバー構成パッケージ (MSI) が作成されます。

7. 成功のメッセージを確認し、「**OK**」をクリックします。
8. 「**サーバー**」タブで「**閉じる**」をクリックします。

SafeGuard Enterprise Server が登録・構成されます。次に、サーバー構成パッケージを SafeGuard Enterprise Server を実行しているコンピュータに展開します。サーバーの構成は「**サーバー**」タブで随時変更できます。

注: 新しいサーバー構成パッケージ (MSI) を SafeGuard Enterpise Server にインストールする場合は、必ず古いサーバー構成パッケージ新しいパッケージをインストールしてください。

3.3 Web Helpdesk のアップデート

Web Helpdesk を最新バージョンに更新するときは、いったん Web Helpdesk をアンインストールしてから、最新バージョンをインストールし直すことをお勧めします。サーバーの設定が更新されている場合は、新しいサーバー構成パッケージを作成するだけでかまいません。

3.4 言語サポート

Web Helpdesk は複数の言語に対応しています。アプリケーションの言語は、Web Helpdesk のログオン画面ですぐに変更できます。表示したい言語をクリックすると、アプリケーションの表示言語が直ちに切り替わります。

4 SafeGuard Enterprise クライアントのないユーザーに Web Helpdesk へのログオンを許可

Web Helpdesk は SafeGuard Enterprise のクライアントがインストールされていないコンピュータでも利用できます。

アクセス許可は、Windows ユーザやグループを追加・削除することで管理できます。

注:

この機能は Windows 認証を利用します。Windows 認証を有効にした場合、Active Directory ユーザーから昇格されたセキュリティ担当者は従来の方法でログインできなくなります。

4.1 SafeGuard Enterprise クライアントを使わないログオンの前提条件

次の前提条件を満たす必要があります。

1. Web Helpdesk へのアクセスを許可するユーザーの属する Windows のユーザーグループが設定されていること (詳細は「**SafeGuard Enterprise 管理者ヘルプ**」を参照してください)。
2. Web Helpdesk の Windows 認証が有効になっていること (**ツール - 構成パッケージツール - 「サーバー」タブ - Windows 認証 WHD**。詳細は「**SafeGuard Enterprise インストールガイド」を参照してください**)。

4.2 SafeGuard Web Helpdesk アプリケーションのための Windows 認証の有効化

1. 「インターネット インフォメーション サービス (IIS) マネージャ」を開きます。
2. 「**サイト** > **既定の Web サイト**」で、SGNWHD などユーザーのノードを選択します。
3. 「**認証**」を選択します。
4. 認証のリストから「**Windows 認証**」という項目を選択します。
5. 画面右側の「**操作**」バーの「**有効**」をクリックします。
6. 「**.NET の承認規則**」を選択し、3つの .NET 承認規則を追加します。

   注: Windows 2008 Server では、IIS に「**.Net 承認規則**」のアイコンは表示されません。「**承認の規則**」というリンクがあります。これらの規則を編集するには、「**URL 承認**」ロールがインストールされている必要があります (「**IIS** > **セキュリティ** > **URL 承認**」)。
7. 「**操作**」バーで「**拒否規則の追加...**」をクリックします。
8. ダイアログが開きます。「**すべての匿名ユーザー**」を有効にしてアクセスを拒否します。「**OK**」をクリックして確定します。

9. 「**操作**」バーに戻り、「**許可規則の追加...**」をクリックします。
10. ダイアログが開きます。「**役割またはユーザーグループの指定**」を有効化します。ドメイン名を含めたユーザーグループ名をフィールドに入力して (例: <ドメイン名>\WHD Users) ユーザーグループに特定のユーザーグループに対するアクセスを許可します。
11. 「**OK**」をクリックして確定します。
12. 「**操作**」バーに戻り、「**拒否規則の追加...**」をクリックします。
13. ダイアログが開きます。「**すべてのユーザー**」を有効にしてすべてのユーザーのアクセスを拒否します。「**OK**」をクリックして確定します。
14. 項目の順序が次のようになっていることを確認します。
    - 拒否 - 匿名ユーザー - ローカル
    - 許可 - <ドメイン名\グループ名> - ローカル
    - 拒否 - すべてのユーザー - ローカル
    - 許可 - すべてのユーザー - 継承

この機能をテストするには、Windows 認証が有効化されているログオン (p. 12) の説明に従ってログオンします。「ようこそ」画面が表示されます。

Active Directory ユーザーから昇格されたセキュリティ担当者が従来の方法でログオンできるように Windows 認証を無効にする必要がある場合は、「**拒否 - すべての匿名ユーザー**」という規則を削除します。

注: Windows 認証は web.config ファイルを編集することでも有効にできます。例:

```
<configuration>
  <system.web>
    <authentication mode="Windows" />
     <authorization>
      <allow roles="HelpDesk" />
      <deny users="*" />
     </authorization>
  </system.web>
</configuration>
```

4.3 Windows 認証が有効化されているログオン

次の手順を実行します。

1. ブラウザを開いて URL を入力します。
2. URL を入力してアプリケーションを起動します。`https://`<ホスト `ID` または `IP` アドレス>`/SGNWHD`
3. 「**復旧**」または「**中断の承認**」など、必要なオプションを選択し、復旧の種類について (p. 16) と以下の説明に従って進めます。

5 認証

セキュリティ担当者が Web ベースの復旧ウィザードを使用するには、Web Helpdesk で SafeGuard Enterprise Server に対して認証を行う必要があります。セキュリティ担当者は自分のユーザー名とパスワード (Windows のログオン情報に相当します) を使って Web Helpdesk にログオンします。

ユーザーの場合、次の 2通りの認証シナリオがあります。

- SafeGuard Management Center でセキュリティ担当者に昇格されたユーザーは、Windows 認証を使わない Web Helpdesk へのログオン (p. 14) の説明に従ってログオンします。
- Windows 認証が有効化されている特定の Web Helpdesk ユーザーグループに属するユーザーは、Windows 認証が有効化されているログオン (p. 12) の説明に従ってログオンします。

5.1 SafeGuard Management Center 内での準備

Windows 認証を有効にせず Web Helpdesk でユーザー認証を行うには、次の前提条件を満たす必要があります。また、SafeGuard Management Center で次の準備を行う必要があります。詳細は、「SafeGuard Enterprise 管理者ヘルプ」を参照してください。

1. Web Helpdesk のユーザーが Active Directory から SafeGuard Enterprise のデータベースにインポートされている必要があります。
2. ユーザー証明書が上記のユーザーに割り当てられているか、またはインポートされていて、これらの証明書 (`.p12` ファイル) がデータベースで利用可能になっている必要があります。
3. その後、Web Helpdesk にアクセスするユーザーを、セキュリティ担当者に昇格する必要があります。

   昇格したセキュリティ担当者は、定義済みのセキュリティ担当者名を使用して Web Helpdesk にログオンできます。この名前は、Windows ユーザー名と、ユーザーに割り当てられているドメインの名前の組み合わせになっています。要求されるパスワードは、証明書を保護している Windows パスワードです。

4. セキュリティ担当者が Web Helpdesk で認証されるには、ヘルプデスク担当者のロールが割り当てられている必要があります。
5. また操作を実行するオブジェクト (ドメインや組織単位など) に対する権限が付与されている必要があります。詳細は「**SafeGuard Enterprise 管理者ヘルプ**」の「**セキュリティ担当者へのディレクトリ オブジェクトの割り当て**」という章を参照してください。

注: Web Helpdesk のセキュリティ担当者は SafeGuard Enterprise Server から認証される必要があるため、トークンによる認証は Web Helpdesk でサポートされていません。

5.2 Windows 認証が有効に設定されていない Web Helpdesk へのログオン

1. ブラウザを起動します。
2. URL を入力してアプリケーションを起動します。`https://<ホスト ID または IP アドレス>/SGNWHD`
3. 「**ようこそ**」ページで、SafeGuard Management Center 内に定義されているセキュリティ担当者名を次の形式で入力します。<ユーザー名>@<ドメイン名> 例: `WHDOfficer@MYDOMAIN`

   ここで大文字小文字は区別されます。ユーザー名が正しいことを確認してください。
4. Windows のパスワードを入力します。
5. [**ログオン**] をクリックします。

Web Helpdesk にログオンされます。

注: ユーザーの昇格時に証明書を作成した場合、ユーザーは SafeGuard Management Center にログオンする際、証明書パスワードを使用する必要があります。Windows パスワードの入力が求められますが、証明書パスワードを入力する必要があります。

6 Web Helpdesk ウィザードの選択

1. 「**ホーム**」ページで次のいずれかを実行します。
   - エンドポイントにおける復旧処理を認証するには、「**復旧**」を選択します。詳細は復旧の種類について (p. 16) を参照してください。
   - エンドポイントの SafeGuard の構成保護ポリシーの中断を認証するには、「**中断の承認** 」を選択します。詳細はSafeGuard の構成保護 (p. 28) を参照してください。

7 復旧の種類について

必要な復旧の種類を選択します。次の種類の復旧が用意されています。

- **SafeGuard Enterprise クライアント (管理型)**

  SafeGuard Management Center が一元管理するエンドポイント用のログオン復旧。管理型エンドポイントは SafeGuard Management Center の「**ユーザーとコンピュータ**」ペインに表示されます。

- **仮想クライアント**

  POA が破損したときなど、一般にチャレンジ/レスポンスがサポートされない状況でも、暗号化されているボリュームを簡単に復旧できます。

  このような状況でチャレンジ/レスポンスを有効にするには、仮想クライアントというファイルを SafeGuard Management Center で作成してユーザーに配布後、チャレンジ/レスポンスセッションを開始します。これらの仮想クライアントと、製品 CD に含まれている鍵復旧ツール `RecoveryKeys.exe` によって、エンドポイント上でチャレンジ/レスポンスを開始できます。ユーザーは、必要な鍵の情報をヘルプデスク担当者に伝え、レスポンスコードを入力するだけで、暗号化されたボリュームに再びアクセスできるようになります。

- **Sophos SafeGuard クライアント (スタンドアロン型)**

  ローカルで管理されているエンドポイント用のログオン復旧。このコンピュータは SafeGuard Enterprise サーバーには接続されません。非管理型の Sophos SafeGuard エンドポイントを構成するときに、復旧ファイル (.xml ファイル) がそれぞれ生成されます。このファイルには、企業証明書を使って暗号化された定義済みのマシン鍵が入っています。この復旧鍵ファイルが USB メモリ上または共有ネットワーク パス上などに存在し、ヘルプデスク担当者がアクセスできる場合は、保護されている非管理型 Sophos SafeGuard コンピュータのチャレンジ/レスポンスが利用できます。

8 管理型エンドポイント (SafeGuard Enterprise クライアント - 管理型) の復旧処理

SafeGuard Enterprise には、さまざまな障害復旧シナリオに基づいた、SafeGuard Enterprise で保護されている管理型エンドポイントを復旧するための機能 (パスワードで復旧したり、外部メディアから起動してデータにアクセスしたりなど) が用意されています。

SafeGuard Enterprise フルディスク暗号化で暗号化されているのか、または BitLocker Drive Encryption が使用されているのかが自動的に判断され、それに応じて復旧ワークフローが調整されます。

8.1 管理型エンドポイントの復旧処理

復旧ワークフローは、どのような種類の SafeGuard Enterprise クライアントの復旧が要求されたかによって異なります。

注: BitLocker で暗号化されたエンドポイントの復旧処理では、特定のボリュームを暗号化するために使用された鍵が復旧されるだけです。パスワードは復旧されません。

8.1.1 POA レベルでのパスワードの復旧

最も一般的な状況の1つは、ユーザーがパスワードを忘れてしまった場合です。SafeGuard Enterprise をインストールすると、デフォルトでは Power-on Authentication (POA) が有効になります。エンドポイントにアクセスするための POA パスワードは、Windows パスワードと同じです。

ユーザーが POA レベルのパスワードを忘れてしまった場合、ヘルプデスク担当者は「**ユーザーログオンありの SGN Client の起動**」用のレスポンスを生成できます。このとき、ユーザーのパスワードは表示されません。ただし、この場合、レスポンスコードを入力した後にオペレーティングシステムが起動するので、ドメインの設定状況に応じて、ユーザーが Windows レベルでパスワードを変更する必要があります。それ以降は、その新しいパスワードを使って Windows と Power-on Authentication にログオンできます。

POA レベルのパスワードを復旧する場合の推奨事項

注: ユーザーがパスワードを忘れた場合は、次の方法を使用することをお勧めします。ヘルプデスク担当者がパスワードをリセットする必要がなくなります。

- **Local Self Help を使用する。** ユーザーは Local Self Help で既存のパスワードを表示でき、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。詳細は、「SafeGuard Enterprise 管理者ヘルプ」を参照してください。

- **SafeGuard Enterprise クライアント (管理型) 用のチャレンジ/レスポンスを使用する。** チャレンジ/レスポンスを行う前に、Active Directory で管理者がパスワードをリセットす

ることは推奨しません。リセットしないことで、Windows と SafeGuard Enterprise の間でパスワードが同期されたままになります。Windows のヘルプデスク担当者にこの情報を伝えてください。

SafeGuard Enterprise ヘルプデスク担当者は、レスポンスに対する処理として「**ユーザーログオンありの SGN Client の起動**」と「**ユーザーパスワードの表示**」を選択してレスポンスコードを生成してください。これにより、Active Directory でユーザーのパスワードをリセットする必要がなくなります。ユーザーが希望している場合は、既存のパスワードをそのまま使用してもらい、後でローカルで変更してもらうこともできます。

8.1.2 ユーザーパスワードの表示

SafeGuard Enterprise には、チャレンジ/レスポンス認証中にユーザーがパスワードを表示できるオプションが備わっています。このオプションの利点は、Active Directory でユーザーのパスワードをリセットする必要がなくなるという点です。このオプションは「**ユーザーログオンありの SGN Client の起動**」が選択されている場合のみに利用できます。

8.1.3 外部メディアから起動してデータにアクセス

チャレンジ/レスポンスを使用して、WinPE などの外部メディアからエンドポイントを起動することもできます。そのためには、POA ログオン ダイアログの「**以下から起動を続行：フロッピー ディスク/外部メディア**」を選択して、チャレンジを開始する必要があります。レスポンスを受け取ったユーザーは、ログオン情報を通常どおり POA に入力すれば、引き続き外部メディアから起動できます。

暗号化されたボリュームにアクセスするための条件は次のとおりです。

- 使用するデバイスに SafeGuard Enterprise のフィルタ ドライバが含まれている必要があります。このドライバー CD の入手方法について、詳細は次のサイトを参照してください。http://www.sophos.com/ja-jp/support/knowledgebase/108805.aspx
- ユーザーは外部メディアからエンドポイントを起動する必要があります。そうするための権限をユーザーに付与するには、SafeGuard Management Center でポリシーを定義し、それをエンドポイントに適用します (「ポリシーの「**認証 - アクセス: ユーザーは内部ハードディスクのみから起動できる**」を「**いいえ**」に設定してください)。
- エンドポイントでは外部メディアからの起動が許可されている必要があります。
- 定義済みのマシン鍵で暗号化されたボリュームだけにアクセスできます。この鍵暗号化タイプは、SafeGuard Management Center 内のデバイス暗号化ポリシーに定義した上で、エンドポイントに割り当てることができます。

注: WinPE などの外部メディアを使って暗号化されたドライブにアクセスすると、一部のボリュームだけにアクセスが許可されます。

8.1.4 SafeGuard Enterprise ポリシーキャッシュの復元

SafeGuard Enterprise ポリシーキャッシュが破損している場合、Power-on Authentication にログオンするときに、チャレンジ/レスポンスを開始するよう自動的にメッセージが表示されます。

8.2 管理型コンピュータ用のレスポンスの作成

管理型コンピュータ (SafeGuard Enterprise クライアント) 用のレスポンスを作成するには、コンピュータ名とドメイン名が必要です。

1. 「**復旧の種類**」ページで「**SafeGuard Enterprise Client**」を選択します。
2. リストから対象のドメイン名を選択します。
3. 目的のコンピュータ名を入力します。これにはいくつかの方法があります。
   - 次の方法で名前を選択する。「**...**」をクリックし、ポップアップウィンドウで「**検索**」をクリックします。コンピュータのリストが表示されます。目的のコンピュータを選択し、「**OK**」をクリックします。コンピュータ名が「ドメイン」の下の「復旧の種類」ウィンドウに表示されます。
   - コンピュータの短い名前を入力します。「**次へ**」をクリックすると、データベースでこの名前が検索されます。見つかった場合は、コンピュータの識別名が表示されます。
   - 次のように、識別名の形式でコンピュータ名を直接入力します。

     ```
     CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=com
     ```

4. 「**次へ**」をクリックします。

コンピュータで SafeGuard Enterprise フルディスク暗号化で暗号化されているのか、または BitLocker Drive Encryption が使用されているのかが自動的に判断され、それに応じて復旧ワークフローが調整されます。

- SafeGuard Enterprise で保護されているコンピュータの場合は、次の手順でユーザー情報を選択する必要があります。
- BitLocker で暗号化されたコンピュータの場合は、アクセスできなくなったボリュームを復旧できる場合があります。次の手順で復号化するボリュームを選択する必要があります。

8.2.1 SafeGuard Enterprise のフルディスク暗号化で保護されるコンピュータ用のレスポンスの作成

1. 「**ドメイン**」でそのユーザーが必要とするドメインを選択します。ローカルユーザーの場合は、「**<コンピュータ名> のローカルユーザー**」を選択します。
2. 目的のユーザー名を検索します。次のいずれか 1つを実行します。
   - 「**表示名で検索**」をクリックします。リストから目的の名前を選択し、「**OK**」をクリックします。
   - 「**ログオン名で検索**」をクリックします。リストから目的の名前を選択し、「**OK**」をクリックします。
   - ユーザー名を直接入力します。つづりが正しいことを確認してください。
3. 「**次へ**」をクリックします。チャレンジコードを入力できるペインが表示されます。
4. ユーザーから伝えられたチャレンジコードを入力し「**次へ**」をクリックします。チャレンジコードが検証されます。入力したコードに誤りがある場合、コードが間違っているブロックの下に「**無効**」と表示されます。

5. 正しいチャレンジコードを入力すると、SafeGuard Enterprise クライアントが要求する復旧処理と、エンドポイント上で実行できる復旧処理が表示されます。レスポンスに対して選択できる処理は、チャレンジコードを呼び出したときにエンドポイントが要求した処理によって異なります。たとえば、「**要求した暗号トークン**」が要求された場合には、レスポンスに表示される処理は「**ユーザーログオンありの SGN クライアントの起動**」と「**ユーザーログオンなしの SGN クライアントの起動**」です。
6. ユーザーが実行する必要のある処理を選択します。
7. 上記の「**ユーザーログオンありの SGN Client の起動**」がレスポンス処理として選択されている場合は「**ユーザーパスワードの表示**」を選択すると、対象のエンドポイント上でパスワードを表示させることができます。
8. 「**次へ**」をクリックします。レスポンス コードが生成されます。
9. 生成されたレスポンスコードをユーザーに伝えます。スペル支援を利用できます。また、レスポンス コードはクリップボードにコピーすることもできます。

ユーザーがレスポンス コードをエンドポイントに入力すると、承認された処理が実行できるようになります。

8.2.2 BitLocker Drive Encryption で保護されるコンピュータ用のレスポンスの作成

1. アクセスするボリュームをリストから選択し、「**次へ**」をクリックします。すると、Web Helpdesk に対応する 48桁の復旧鍵が表示されます。
2. この鍵をユーザーに提供してください。

ユーザーがこの鍵を入力すると、エンドポイント上の BitLocker で暗号化されたボリュームにアクセスできるようになります。

9 仮想クライアントを使用した復旧

SafeGuard Enterprise で仮想クライアントを使って復旧を行うと、復旧が困難な状況でも再び暗号化されたボリュームにアクセスできるようになります。

このタイプの復旧は次のような状況で適用できます。

- Power-on Authentication が破損している場合。
- ボリュームがコンピュータに定義されているマシン鍵ではなく別の鍵で暗号化されている場合。必要な鍵はユーザー環境にはありません。このため、データベース内で鍵を特定してエンドポイントに安全な方法で転送する必要があります。

注: 仮想クライアントの復旧は、複雑な復旧に関する問題を解決する場合にだけ使用してください。前述の両方の問題に該当する場合には、仮想クライアントによる復旧をお勧めします。しかし、ボリュームの復旧に必要な鍵がないだけの場合、ボリュームを復旧する最適な方法は、当該の鍵を各ユーザーの鍵リングに割り当てることです。

このような場合のために、SafeGuard Enterprise には次のソリューションが用意されています。

このような状況でチャレンジ/レスポンスを有効にするには、仮想クライアントという特定のファイルを SafeGuard Management Center で作成し、ユーザーに配布後、チャレンジ/レスポンスセッションを開始します。これらの仮想クライアントファイル、鍵復旧ツール `RecoverKeys.exe`、および SafeGuard Enterprise 向けに変更された WinPE の CD によって、エンドポイント上でチャレンジ/レスポンスを開始できます。その後、ヘルプデスク担当者は目的の鍵を選択してレスポンスコードを生成します。ユーザーがレスポンスコードを入力すると、必要な鍵がレスポンスにより転送され、暗号化されたボリュームにアクセスできるようになります。

注: Web Helpdesk は、仮想クライアントを使った非管理型エンドポイント (Sophos SafeGuard Client スタンドアロン型) の復旧はサポートしません。代わりに SafeGuard Management Center を使用してください。

9.1 仮想クライアントを使用した復旧ワークフロー

詳細は「SafeGuard Enterprise 管理者ヘルプ」を参照してください。

1. ヘルプデスク担当者は、SafeGuard Management Center の「**鍵と証明書**」エリアで仮想クライアントを作成し、それらをファイルにエクスポートします。必ず、このファイル (`recoverytoken.tok`) をユーザーに配布して使用できる状態にしてから、チャレンジ/レスポンス セッションを開始してください。
2. 配布後、ユーザーは SafeGuard Enterprise リカバリ CD または SafeGuard Enterprise 向けに変更された WinPE が含まれるその他の CD をコンピュータ上から POA ログオンなしで起動し、SafeGuard Enterprise 鍵復旧ツールを使用してチャレンジ/レスポンスセッションを開始する必要があります。

   利用できないユーザー/コンピュータ名については、その代わりに SafeGuard Enterprise データベース内で仮想クライアントファイルが使用され、チャレンジに記述されます。

3. 鍵復旧ツールによって、どのボリュームが暗号化されていて、それらのボリュームのためにどの鍵が使用されているかがユーザーに報告されます。ユーザーはこの情報をヘルプデスク担当者に伝えます。
4. ヘルプデスク担当者は、データベース内の仮想クライアントを特定し、暗号化されたボリュームへのアクセスに必要な鍵を選択します。これは、1つの鍵または鍵ファイルにエクスポートされた複数の鍵のいずれかです。そして、ヘルプデスク担当者がレスポンスコードを生成します。
5. ユーザーはレスポンスコードを入力します。レスポンスコード内で必要な鍵が転送されます。ユーザーがレスポンス コードを入力してコンピュータを再起動することによって、再び暗号化されたボリュームにアクセスできるようになります。

9.2 仮想クライアントを使用した復旧処理

ユーザーが使用できない鍵で暗号化されているボリュームにアクセスするには、正しい暗号化鍵をデータベースからユーザー環境に転送する必要があります。

このため、チャレンジ/レスポンスは仮想クライアントを使用する次の 2 つの処理に対応しています。

- 1 つの鍵の転送
- 暗号化された鍵ファイル内の複数の鍵の転送

9.2.1 1つの鍵の転送

暗号化されたボリュームにアクセスするために必要な1つの鍵を復旧するために、チャレンジ/レスポンスを開始できます。ヘルプデスク担当者は、データベース内で必要な鍵を選択し、レスポンス コードを生成する必要があります。レスポンスコードを入力することによって、鍵が暗号化され、エンドポイントに転送されます。レスポンスコードが正しい場合は、転送された鍵がローカル鍵ストアにインポートされます。それ以降は、この鍵を使用して暗号化されているすべてのボリュームにアクセスできるようになります。

9.2.2 暗号化された鍵ファイル内の複数の鍵の転送

暗号化されたボリュームにアクセスするために必要な複数の鍵を復旧するために、チャレンジ/レスポンスを開始できます。鍵は、パスワードで暗号化された 1つのファイルに保存されます。この処理を行うには、ヘルプデスク担当者が保存する 1つ以上の必要な鍵を 1つのファイルにエクスポートする必要があります。このファイルは、データベースに保存されているランダムなパスワードを使用して暗号化されます。このパスワードは作成される鍵ファイルごとに一意です。

暗号化された鍵ファイルをユーザー環境に転送して、ユーザーが使用できる状態にする必要があります。この鍵ファイルを復号化するには、ユーザーは鍵復旧ツール`RecoverKeys.exe`を使用してチャレンジ/レスポンスを開始し、そこでパスワードを目的のコンピュータに転送する必要があります。このセッションの間、対象のエンドポイントにパスワードが転送されます。ヘルプデスク担当者は、レスポンスを生成し、鍵ファイルを復号化するための各パスワードを選択します。パスワードはレスポンス コード内で目的のエンドポイントに転送されます。そのパスワードを使って鍵ファイルを復号化できます。

鍵ファイル内の鍵は、エンドポイント上の鍵記憶域にインポートされます。すると、使用できる鍵で暗号化されたすべてのボリュームに再びアクセスできるようになります。

注: Web Helpdesk では、データベース内の鍵ファイルと対応するパスワードは、チャレンジ/レスポンスセッションで正常に使用された後は削除されます。そのため、チャレンジ/レスポンス セッションが正常に終了するたびに、新しい鍵ファイルとパスワードを作成する必要があります。

9.3 仮想クライアントを使用したレスポンス

9.3.1 前提条件

- 仮想クライアントが SafeGuard Management Center の「**鍵と証明書**」で作成済みである必要があります。詳細は、「SafeGuard Enterprise 管理者ヘルプ」を参照してください。
- ヘルプデスク担当者は、データベース内の仮想クライアントを特定できる必要があります。仮想クライアントは名前によって一意に識別されます。
- 仮想クライアントファイル **recoverytoken.tok** は、ユーザーが使用できる状態でなければなりません。このファイルは、鍵復旧ツールと同じフォルダに保存される必要があります。このファイルは USB メモリに保存することをお勧めします。
- 複数の鍵を復旧することが要求されたときは、ヘルプデスク担当者は事前に SafeGuard Management Center の「**鍵と証明書**」で必要な復旧鍵が含まれる鍵ファイルを作成しておく必要があります。鍵ファイルは、復旧の前にユーザーが利用できる状態でなければなりません。この鍵ファイルを暗号化しているパスワードが、データベースで入手できる状態になっている必要があります。詳細は、「**SafeGuard Enterprise 管理者ヘルプ**」を参照してください。
- ユーザーが鍵復旧ツールを起動して、チャレンジ/レスポンスセッションを開始している必要があります。
- レスポンスは割り当てられた鍵に対してのみ開始できます。鍵が有効ではない場合、つまり鍵が少なくとも 1人のユーザーに割り当てられていない場合は、仮想クライアントのレスポンスは不可能です。このような場合は、無効な鍵を他のユーザーに割り当て直し、この鍵に対するレスポンスを再び生成することができます。

9.3.2 仮想クライアントを使用したレスポンスの作成

1. ヘルプデスク担当者は、「**復旧の種類**」ページで「**仮想クライアント**」を選択します。
2. ユーザーから取得した仮想クライアント名を入力します。これには次の 2種類の方法があります。
   - 一意の名前を直接入力する。
   - 次の方法で名前を選択する。「**...**」をクリックし、ポップアップウィンドウで「**検索**」をクリックします。仮想クライアントのリストが表示されます。対象の名前を選択し、「**OK**」をクリックします。仮想クライアント名が「**復旧の種類**」ウィンドウの「**仮想クライアント**」に表示されます。
3. 「**次へ**」をクリックします。復旧処理を選択できるページが表示されます。

4. ユーザーが実行する復旧処理を選択し、「**次へ**」をクリックします。
   - 1つの復旧鍵だけを転送する必要のある場合は、「**要求された鍵**」を選択します。リストから必要な鍵を選択します。「**...**」をクリックします。鍵は鍵 ID またはシンボリック名で表示できます。「**検索**」をクリックして鍵を選択し、「**OK**」をクリックします。
   - 複数の復旧鍵が入っている鍵ファイルをユーザーが必要としている場合は、「**要求された鍵ファイルのパスワード**」を選択してその暗号化鍵ファイルのパスワードをユーザーに転送します。必要な鍵ファイルを選択します。「**...**」をクリックし、「**検索**」をクリックします。鍵ファイルを選択し、「**OK**」をクリックします。

   「**要求された鍵ファイルのパスワード**」は、鍵ファイルが SafeGuard の「**鍵と証明書**」ですでに作成されていて、鍵ファイルを暗号化しているパスワードがデータベースに保存されていないと選択できません。Web Helpdesk では、データベース内の鍵ファイルと対応するパスワードは、チャレンジ/レスポンスセッションで正常に使用された後は削除されます。このため、チャレンジ/レスポンスセッションが正常に終了するたびに、新しい鍵ファイルとパスワードを作成する必要があります。
5. 「**次へ**」をクリックします。チャレンジコードを入力するページが表示されます。
6. ユーザーから伝えられたチャレンジコードを入力し「**次へ**」をクリックします。チャレンジコードが検証されます。コードが間違って入力された場合、エラー表示の下に「**無効**」と表示されます。
7. チャレンジコードが正しく入力されている場合は、レスポンスコードが生成されます。このレスポンスコードをユーザーに伝えます。スペル支援を利用できます。また、レスポンス コードはクリップボードにコピーすることもできます。
   - 1つの鍵が要求された場合は、生成された鍵がレスポンスコード内で転送されます。
   - 暗号化された鍵ファイルのパスワードが要求された場合は、パスワードがレスポンスコード内で転送されます。鍵ファイルはその後に削除されます。
8. ユーザーはエンドポイントコンピュータ上でレスポンスコードを入力する必要があります。
9. ユーザーが各ボリュームにアクセスするには、コンピュータを再起動してログオンし直す必要があります。

ボリュームに再びアクセスできるようになります。

10 非管理型エンドポイント (Sophos SafeGuard クライアント - スタンドアロン) の復旧処理

SafeGuard Enterprise では、非管理型エンドポイント (Sophos SafeGuard クライアント - スタンドアロン) に対してチャレンジ/レスポンス認証を行うこともできます。スタンドアロンで利用しているエンドポイントは、SafeGuard Enterprise サーバーには接続しません。このようなエンドポイントはスタンドアロン モードで動作し、ローカルで管理されます。SafeGuard Enterprise のデータベースに登録されていないので、チャレンジ/レスポンスに必要なエンドポイントの識別情報は入手できません。

このため、非管理型エンドポイントのチャレンジ/レスポンスは、スタンドアロン クライアントを構成するときに作成された復旧鍵ファイルに基づいて行われます。復旧ファイル (.xml ファイル) は、非管理型エンドポイントごとに生成され、企業証明書を使って暗号化された定義済みのマシン鍵を含みます。このファイルは、ヘルプデスク担当者がチャレンジ/レスポンスの実行中にアクセスできる場所に保存されている必要があります。ヘルプデスク担当者が USB メモリや共有ネットワークパスなどにある各復旧ファイルにアクセスすると、レスポンスコードを生成できる状態になります。

10.1 非管理型エンドポイントの復旧処理

非管理型エンドポイント (Sophos SafeGuard クライアント - スタンドアロン型) のチャレンジ/レスポンスは、次のようなときに開始する必要があります。

- ユーザーが間違ったパスワードを何度も入力した場合。
- ユーザーがパスワードを忘れた場合。
- 破損したローカル キャッシュを修復する必要がある場合。

非管理型エンドポイントの場合、データベースからユーザー鍵を入手することはできません。このため、チャレンジ/レスポンスセッションで実行できる復旧オプションは、「**ユーザー ログオンなしで Sophos SafeGuard クライアントを起動**」だけです。

チャレンジ/レスポンスを実行すると、ユーザーが Power-on Authentication でログオンできるようになります。また、Windows パスワードのリセットが必要な場合でも、ユーザーは Windows にログオンできます。

10.1.1 ユーザーが間違ったパスワードを何度も入力した場合

この場合、パスワードをリセットする必要はありません。ユーザーはチャレンジ/レスポンスで Power-on Authentication にログオンできるようになります。この後、ユーザーが Windows ログインで正しいパスワードを入力すると、再びエンドポイントを使用できるようになります。

10.1.2 ユーザーがパスワードを忘れた場合

注: パスワードを忘れた場合、通常 Local Self Help を使用して復旧することをお勧めします。ユーザーは Local Self Help で既存のパスワードを表示でき、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。詳細は、「SafeGuard Enterprise 管理者ヘルプ」を参照してください。

忘れたパスワードをチャレンジ/レスポンスで復旧するときは、パスワードのリセットが必要です。

1. チャレンジ/レスポンスでは、コンピュータを Power-on Authentication で起動できます。
2. Windows のログオン画面でも、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、SafeGuard Enterprise 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。
   - 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。
   - Windows のパスワード リセット ディスクを使用する。

   ヘルプデスク担当者は、どちらの手続きを使用した方がいいかをユーザに伝えて、追加の Windows ログオン情報または必要なディスクを提供することをお勧めします。
3. ユーザーは、ヘルプデスク担当者から入手した新しいパスワードを Windows のログオン画面で入力します。その後、このパスワードをすぐに自分だけが知っているパスワードに変更します。
4. 新しいパスワードを選択すると、POA で現在使用されている SafeGuard Enterprise パスワードと一致していないことが検出されます。すると、古い SafeGuard Enterprise パスワードの入力を求められます。このパスワードを忘れた場合は、「**キャンセル**」をクリックする必要があります。
5. 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。
6. 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。この結果、ユーザーは再度コンピュータにログオンできるようになり、新しいパスワードを使って Power-on Authentication にログオンできます。

   SafeGuard Data Exchange の鍵

   ユーザーが Windows パスワードを忘れ、リセットした場合、当該のユーザーは、対応するパスフレーズなしで SafeGuard Data Exchange に対して既に作成されている鍵を使用することはできません。既存の SafeGuard Data Exchange のユーザー鍵を引き続き使用できるようにするには、SafeGuard Data Exchange のパスフレーズを思い出して、これらの鍵を再び有効にする必要があります。

10.2 非管理型コンピュータ用のチャレンジ/レスポンス

非管理型コンピュータに対してチャレンジ/レスポンスセッションでレスポンスを生成するには、復旧ファイル (.xml ファイル) の名前が必要です。

1. Web Helpdesk の「**ツール**」メニューから「**復旧**」をクリックします。
2. 「**復旧の種類**」から「**スタンドアロンクライアント**」を選択します。
3. 「**参照**」をクリックし、必要な鍵復旧ファイル (.xml) を参照します。
4. ユーザーから伝えられたチャレンジコードを入力します。
5. ユーザーが行う処理を選択し、「**次へ**」をクリックします。
6. レスポンスコードが生成されます。このレスポンスコードをユーザーに伝えます。スペル支援を利用できます。また、レスポンスコードはクリップボードにコピーすることもできます。

ユーザーは、レスポンス コードを入力し、必要な処理を実行して、作業を再開できます。

11 SafeGuard Configuration Protection

SafeGuard Configuration Protection モジュールは、SafeGuard Enterprise 6.1 より使用できなくなりました。該当するポリシーは、Configuration Protection をインストール済みの SafeGuard Enterprise 6.x クライアントを 6.1 Management Center で管理するため、引き続き SafeGuard Management Center 6.1 に表示されます。

SafeGuard Configuration Protection の詳細は、**SafeGuard Enterprise 6 の Web Helpdesk** マニュアルを参照してください。
(http://www.sophos.com/ja-jp/medialibrary/PDFs/documentation/sgn_60_m_eng_web_helpdesk.pdf)

12 Web Helpdesk のイベントのログ出力

Web Helpdesk のイベントは、Windows イベントビューアや SafeGuard Enterprise データベースでログ出力できます。Web Helpdesk にログオンしたユーザー、チャレンジ要求したユーザー、要求した復旧アクションなど、Helpdesk のアクティビティに関するすべてのイベントをログに記録できます。

Web Helpdesk のイベントログを有効化するには、SafeGuard Management Center でポリシーを構成パッケージに含め、Web Helpdesk サービス上でデプロイする必要があります。

SafeGuard Enterprise のデータベースにログとして記録されたイベントは、SafeGuard Management Center の「イベント ビューア」を使って表示できます。

12.1 Web Helpdesk のイベントログの有効化

Web Helpdesk のログは SafeGuard Management Center で構成します。

ポリシーの作成およびイベントの表示には権限が必要です。

1. SafeGuard Management Center の「**ポリシー**」というナビゲーションペインで、「**ログ**」という種類のポリシーを作成します。ログ出力するイベントを選択します。変更内容を保存します。
2. 新しい「**ポリシーグループ**」を作成します。このグループに作成した「**ログ**」という種類のポリシーを追加します。変更内容を保存します。
3. 「**ツール**」メニューの「**構成パッケージツール**」をクリックします。「**構成パッケージの作成 (管理型)**」を選択し、「**構成パッケージの追加**」をクリックします。作成したポリシー グループを選択し、構成パッケージに含めます。保存先を選択し、「**構成パッケージの作成**」をクリックします。
4. SafeGuard Management Center で、ポリシー グループを Web Helpdesk サーバーのあるドメインに割り当てます。そして、有効化します。詳細は、「**SafeGuard Enterprise 管理者ヘルプ**」の「**ポリシーの割り当て**」という章を参照してください。
5. Web Helpdesk サーバー上に作成した構成パッケージをインストールします。サービスを再起動します。

   Web Helpdesk のイベントログが有効化されます。
6. Web Helpdesk にログオンし、チャレンジ/レスポンスを実行します。
7. SafeGuard Management Center で「**レポート**」タブをクリックします。右側の「**イベント ビューア**」というアクションエリアで、拡大アイコンをクリックし、Web Helpdesk のイベントログを表示します。

13 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。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/
- オンラインでのお問い合せ。
  https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

14 ご利用条件