

HP Data Protector for PCs 7.0 インストール/管理ガイド

HP 部品番号: N/A
2011 年 6 月
第 初 版



© Copyright 2011 Hewlett-Packard Development Company, L.P.

本書で取り扱っているコンピューターソフトウェアは秘密情報であり、その保有、使用、または複製には、Hewlett-Packard Company から許諾を得る必要があります。米国政府の連邦調達規則である FAR 12.211 および 12.212 の規定に従って、コマーシャルコンピューターソフトウェア、コンピューターソフトウェアドキュメンテーションおよびコマーシャルアイテムのテクニカルデータ (Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items) は、ベンダーが提供する標準使用許諾規定に基づいて米国政府に使用許諾が付与されます。

本書の内容は、将来予告なしに変更されることがあります。HP 製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的、編集上の誤り、または欠如について、HP はいかなる責任も負いません。

Microsoft®、Windows®、Windows® XP、Windows NT®、および Windows Vista® は、Microsoft Corporation の米国における登録商標です。

目次

本書について.....	5
対象読者.....	5
表記上の規則およびシンボル.....	5
全般情報.....	6
HP テクニカルサポート.....	6
製品サービスへの登録.....	6
HP の Web サイト.....	6
ご意見、ご感想.....	7
1 概要と要件.....	8
Data Protector for PCs の概要.....	8
Data Vault.....	9
証明書の処理.....	10
自己署名証明書.....	10
インポートされた証明書.....	10
証明書の交換.....	11
Data Protector for PCs のインストールの概要.....	11
要件.....	12
Policy Server.....	12
データベース.....	13
Data Protector for PCs Web Data Vault Server.....	13
Data Protector for PCs Agent.....	13
2 Data Protector for PCs Policy Server のインストール.....	14
クイックインストール.....	14
詳細インストール.....	15
3 Web Data Vault Server のインストール、設定、保守.....	18
Web Data Vault Server のインストールおよび設定.....	18
Web Data Vault の保守.....	19
Windows ファイル共有 Data Vault から Web Data Vault へのデータの移行.....	20
CLI (DvConfig) を使用した Web Data Vault オプションの設定.....	21
4 Data Protector for PCs 保護ポリシーの設定.....	23
Data Protector for PCs インストール後の初期セットアップ.....	23
初回インストール時の設定.....	24
その他のポリシーの設定.....	28
その他の構成タスク.....	30
サポートできる Agent の数の決定.....	31
サイズ決定を左右する要素.....	32
サイズ決定に関する推奨事項.....	32
Data Vault.....	32
Policy Server.....	33
ネットワークに関する検討事項.....	34

5 マルチスレッド クリーンアップの設定.....	35
CLI からの DPNECleanup.exe の使用.....	35
6 Data Protector for PCs Agent のインストール.....	37
個々のクライアント マシンへの Data Protector for PCs Agent のインストール.....	37
要件.....	37
インストール手順.....	37
Data Protector for PCs Agent の組織全体への配置.....	38
Kit の内容.....	38
配置およびインストール手順.....	39
7 Data Protector for PCs の更新.....	42
Policy Server の更新.....	42
Agent の更新.....	42
Agent 更新ポリシーを使用した自動 Agent 更新.....	43
手動 Agent 更新.....	43
8 Data Protector for PCs のサポートへの連絡方法.....	44
用語集.....	45
索引.....	47

本書について

本書では、以下の内容について説明します。

- HP Data Protector for PCs のインストール
- HP Data Protector for PCs のポリシーの設定
- ユーザーのデスクトップおよびノートブック上の HP Data Protector for PCs Agent ソフトウェア
- サポートできる Agent の数の決定
- Data Protector for PCs のサポートへの連絡

対象読者

本書は、HP Data Protector for PCs をインストールおよび構成する管理者を対象としています。次の点に対する理解は有益です。

- Windows の管理

表記上の規則およびシンボル

表記法	項目
ミディアムブルーの語句: 「 本書について 」 (5 ページ)	クロスリファレンスリンクおよび E メールアドレス
ミディアムブルーの下線付き語句: http://www.hp.com	Web サイトアドレス
太字	<ul style="list-style-type: none">• キー名• ボックスなど GUI で入力される文字列• クリックおよび選択される GUI (メニュー、リスト項目、ボタン、タブ、チェックボックスなど)
イタリック体	語句の強調
Monospace フォント	<ul style="list-style-type: none">• ファイル名およびディレクトリ名• システムアウトプット• コード• コマンド、コマンド引数、および引数の値
イタリック体の Monospace フォント	<ul style="list-style-type: none">• コード変数• コマンドライン変数
太字体の Monospace フォント	Monospace フォントの語句の強調

① **重要:** 詳細情報または特定の手順を示します。

注記: 補足情報を示します。

全般情報

Data Protector for PCs の全般情報は、HP の Web サイト <http://www.hp.com/go/dataprotector> (英語) で確認できます。

HP テクニカルサポート

この製品のテクニカルサポートについては、次の HP サポートの Web サイトに記載されています。

<http://www.hp.com/support>

HP にお問い合わせになる前に、次の情報を準備してください。

- 製品のモデル名およびモデル番号
- テクニカルサポートの登録番号 (該当する場合)
- 製品のシリアル番号
- エラーメッセージ
- オペレーティングシステムの種類とリビジョンレベル
- 詳細で具体的な質問

製品サービスへの登録

お使いの製品を、次の Subscriber's Choice for Business の Web サイトで登録することをお勧めします。

<http://www.hp.com/go/e-updates>

登録を済ませると、製品のアップグレード、ドライバーの新しいバージョン、ファームウェア アップグレードなどの製品リソースに関する通知を電子メールで受け取ることができます。

HP の Web サイト

その他の情報については、HP の次の Web サイトを参照してください。

- <http://www.hp.com>
- <http://www.hp.com/go/dataprotector>
- <https://h20230.www2.hp.com/selfsolve/manuals>
- <http://www.hp.com/support/manuals>
- <http://www.hp.com/support/downloads>

ご意見、ご感想

本書に関するご意見、ご感想をお待ちしております。

製品マニュアルについてのご意見、ご感想は、DP.DocFeedback@hp.com に電子メールでご送信ください。お送りいただいたご意見は、HP の資産になります。

1 概要と要件

Data Protector for PCs の概要

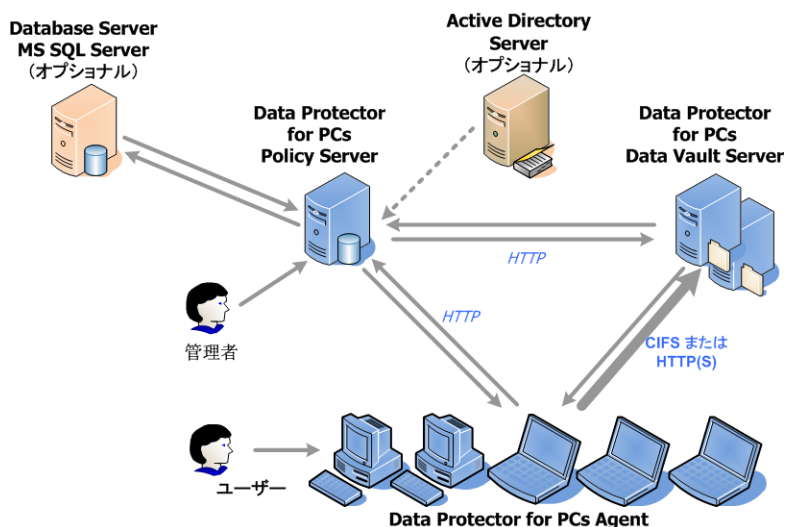
HP Data Protector for PCs は、主に Policy Server と Agent の 2 つのソフトウェアコンポーネントから構成されています。Policy Server は、Windows サーバー上で動作し (サポートされるバージョンについては、サポートマトリクス (<https://h20230.www2.hp.com/selfsolve/manuals>) を参照)、Agent は、各デスクトップ/ノートブック上でバックグラウンドで動作します。

Policy Server は、Active Directory サーバーにあるグループや組織単位にアクセスすることも可能です。

ユーザーのデータは Data Vault にバックアップされます。Data Vault Server は Policy Server とは別の場所に配置する必要があります。推奨される Web Data Vault ではなく Windows ファイル共有 Data Vault を使用している場合、それらはファイルサーバー上の 1 つ以上の Windows ファイル共有に配置されています。

Data Protector for PCs アーキテクチャーを次の図に示します。

図 1 Data Protector for PCs のアーキテクチャー



さまざまなポリシーが、デスクトップおよびラップトップからどのファイルをバックアップするか、さらにこれらのバックアップをどこで保管するかを制御しています。Policy Server Console を使用して、これらのポリシーを定義します。その後、ポリシーは、SOAP プロトコルを使用し、HTTP ポート 80 を介して、Agent に自動的に配信されます。ポリシーは、Policy Server 上で保管されます。

Agent がこれらのポリシーを実行します。ポリシーにより保護されているデータファイルをユーザーが変更すると、ユーザー PC 上のローカルハードディスクに変更前

のバージョンが作成され、かつ変更したファイルが適用される Data Vault すべてにコピーされます。

ファイルがバックアップされると、Agent は必ず、ユーザーによるファイル変更の監査履歴を含む通知を Policy Server に送信します。加えて、各 Agent は定期的に「動作状況」情報を Policy Server に送信します。Policy Server Console で、このデータのレポートを生成できます。

Data Vault は、Data Vault Server 上に保持されます。クライアント データは、CIFS (Windows ファイル共有 Data Vault) または HTTP (Web Data Vault) の 2 つの異なるプロトコルを使用して Data Vault にコピーされます。

Data Vault Server は Policy Server とは別のシステムに配置する必要があります。HTTPS の場合、Web Data Vault Server ソフトウェアが Data Protector for PCs クリーンアップ ソフトウェアと共に実行されます。Windows ファイル共有 Data Vault の場合は、クリーンアップ ソフトウェアのみがインストールされます。

Active Directory をご使用の場合、設定により Policy Server がグループや組織単位にアクセスするようにすることが可能です。あるユーザーに対して、そのユーザーが属するグループや組織単位に基づいて Data Vault を割り当てることができます。レポート閲覧時には、所属グループや組織単位によってユーザーを選択することが可能です。

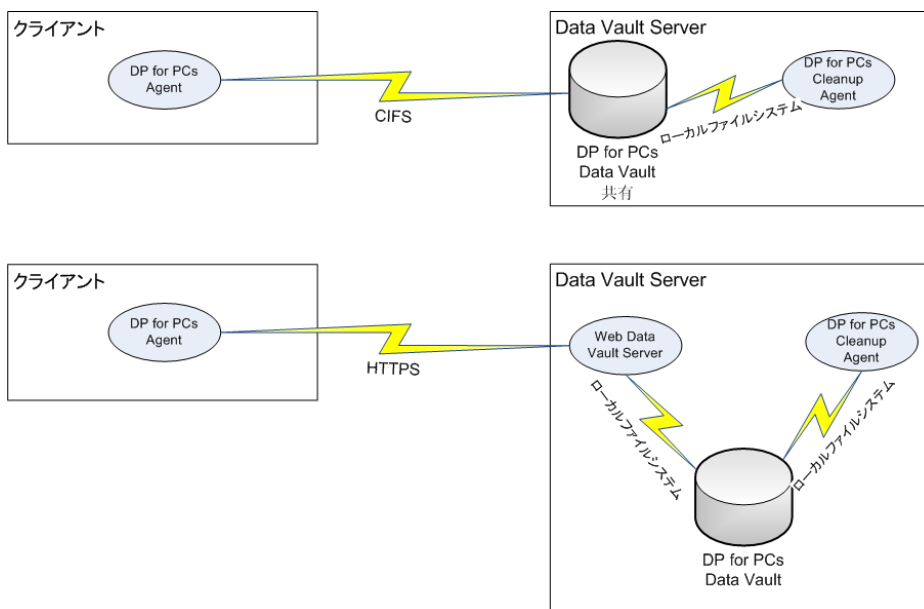
Data Vault

Data Protector for PCs には、次の 2 つのタイプの Data Vault があります。

- HTTPS プロトコルに基づく Web Data Vault。これは、高遅延環境で高いレベルのセキュリティと高いスループットを提供するため、推奨されます。
- 以前のバージョンの Data Protector for PCs で使用され、CIFS プロトコルに基づく Windows ファイル共有 Data Vault。

いずれのタイプの Data Vault のデータ構造も同じなので、既存の Windows ファイル共有 Data Vault は Web Data Vault に変換することができます。

図 2 Windows ファイル共有と Web Data Vault の比較



証明書の処理

Web Data Vault では SSL を必ず使用する必要があります。証明書のタイプは、Web Data Vault のインストール時に決定されます。評価目的での利用などのために、製品をすぐに使用できる状態で提供するには、Web Data Vault Server を自己署名証明書と共にインストールできます。これは認証局 (CA) から発行された証明書と比較すると安全ではありません。完全なセキュリティが必要な場合、環境内の認証局から Data Vault Server 用の証明書をインポートし、サーバー コンポーネントに追加する必要があります。

自己署名証明書

Data Vault ポリシーを作成する際、自己署名証明書を許可するかどうかを定義できます。この場合、Agent 側での処理は必要ありません。インストールから発行された自己署名証明書には 20 年の期限があります。

インポートされた証明書

インポートする際には、秘密キーとそれに一致する公開キーを含む証明書の両方を含む PEM 形式のファイルが 1 つ必要です。このファイルは、Web Data Vault Server の構成ディレクトリにそのままの状態のコピーされます。作成手順によっては、証明書ファイルは暗号化されている場合があります。その場合、Web Data Vault Server を実行する Windows サービス プロセスが複合化パスワードを取得するために対話形式のプロンプトを発行します。これはインストール時と、以降のこのサービスの再開時 (システムの再起動など) のたびに起こります。プロンプトが表示されないようにするには、Web サーバーの構成ファイルにこのパスワードを手動で追加できます。

が、インストール プロセスではこれはサポートされていません。暗号化された証明書ファイルの付近に、そのパスワードが保存されたファイルを置かないようにしてください。

注記:

「認証局」という用語は、Agent を実行するクライアント マシンがこの CA を信頼できるものとみなし、その署名がある証明書を受け入れることを意味します。クライアント マシンの Windows 証明書ストアには、その CA の証明書と、存在する場合はチェーンの他の証明書が追加され、既に正しく設定されていることを想定しています。Agent にはこの信頼を築くためのメカニズムはありません。Windows のメカニズムに依存しています。

証明書の交換

Web Data Vault Server の証明書は、CLI に関して説明している「[「CLI \(DvConfig\) を使用した Web Data Vault オプションの設定」 \(21 ページ\)](#)」の項の DvConfig ユーティリティを使用し、インストール後いつでも交換できます。たとえば、自己署名証明書が当初設定されていたインストールを、インポートした証明書を使用するよう再構成できます。

Data Protector for PCs のインストールの概要

注記: Data Protector for PCs のインストールを更新する場合は、「[Data Protector for PCs の更新](#)」(42 ページ) を参照してください。

Data Protector for PCs のインストールは次の 3 段階に分かれています。

1. **Data Protector for PCs Policy Server をインストールする。**
「[Data Protector for PCs Policy Server のインストール](#)」(14 ページ) を参照してください。
2. **Data Protector for PCs Web Data Vault Server ソフトウェアをインストールする。**
「[Web Data Vault Server のインストール、設定、保守](#)」(18 ページ) を参照してください。
3. **保護ポリシーを設定する。**
「[Data Protector for PCs 保護ポリシーの設定](#)」(23 ページ) を参照してください。
4. **Data Protector for PCs Agent をラップトップおよびデスクトップにインストールする。**
「[Data Protector for PCs Agent のインストール](#)」(37 ページ) を参照してください。

要件

Policy Server

サポートされるオペレーティングシステムについては、サポートマトリックスを参照してください。

注記: Windows 2003 64 ビット オペレーティングシステムへのインストール: Policy Server は、64 ビットの Windows オペレーティングシステム上で 32 ビット互換モードで動作します。このため、インターネット情報サービス (IIS) は、32 ビットモードで動作する必要があります。IIS が 32 ビットモードで動作していない場合、インストールプログラムが前提条件のチェックの際にそのことを検出します。これにより、IIS を 32 ビットモードに設定するためのオプションが表示されます。IIS が 64 ビットモードでなければならない他の Web アプリケーション (Web メールのある Microsoft Exchange 2007-Outlook Web Access など) がサーバーにある場合は、そのサーバーに Policy Server をインストールすることはできません。Policy Server を Windows 2008 上にインストールする場合は、この問題は発生しません。

サーバーには次のものがインストールされている必要があります。

- Internet Information Services 6.0、7.0、7.5 以降、ASP.NET アプリケーションのサポート機能付き。

Windows 2003 では、IIS 6.0 が前提条件であり、このソフトウェアをインストールしていないと Policy Server をインストールできません。Windows 2008 では、IIS 7.0 および 7.5 がインストールされていない場合は、Data Protector for PCs によってインストールされます。

- Microsoft ASP.NET 2.0

また、次のものもサーバーにインストールされている必要があります。

- Microsoft Installer 3.1 以降 (.NET Framework 2.0 SP1 が必要)。
- Microsoft .NET Framework 2.0 SP1 以降。ウィザードは、バージョン 2.0 SP1 をインストールします。
- Microsoft SQL Express (他の SQL バージョンが存在しない場合)

また、Internet Information Services 7.0 および 7.5 についてのみ、以下の IIS コンポーネントが必要です。インストールされていない場合は、ウィザードからインストールすることができます。

- IIS Static Content Web Server — 静的 HTML ファイル、ドキュメント、および画像の提供に必要
- IIS ASP.NET-ASP.NET 2.0 および .NET Framework の配置に必要
- IIS Security - Policy Server Console に使用される統合 Windows 認証を使用するために必要

- IIS 6 Management Compatibility - セットアップによって IIS 6 および IIS 7 をできるだけ同じように設定可能

データベース

Data Protector for PCs は、Microsoft SQL Server データベースにアクセスできる必要があります。サポートされるバージョンについては、サポートマトリックスを参照してください。

Microsoft Enterprise Manager を使用して SQL Server インストールの認証モードを確認 (および変更) できます。

1. SQL Server インスタンスを右クリックし、[プロパティ] を選択し、[セキュリティ] タブをクリックします。
2. [SQL Server and Windows] オプション ([Windows only] オプションではなく) が既に選択されているはずです。選択されていない場合は、選択して [OK] をクリックします。

また、Data Protector for PCs のインストール中に、Microsoft の SQL Server Express Edition のインスタンスをインストールすることもできます。

Data Protector for PCs Web Data Vault Server

- Web Data Vault Server は Policy Server とは別のシステムにインストールされている必要があります (同じシステムにインストールすることも可能ですが、これは評価目的の場合にのみ適しています)。
- Java Runtime Environment バージョン 1.6 以降がインストールされている必要があります。
- 変数 JAVA_HOME と JRE_HOME が、Java Runtime のインストール ディレクトリをポイントしている必要があります。

Data Protector for PCs Agent

Data Protector for PCs Agent ソフトウェアは、Windows を実行するユーザーのデスクトップまたはノートブックにインストールできます。サポートされるプラットフォームについては、サポートマトリックスを参照してください。

2 Data Protector for PCs Policy Server のインストール

注記: 標準的なインストール手順に従うことで、既存の Data Protector for PCs Policy Server のインストールをより新しいバージョンに更新することができます。詳しくは、「[Policy Server の更新](#)」(42 ページ)を参照してください。

クイックインストール

Data Protector for PCs Policy Server の要件については、「[Policy Server](#)」(12 ページ)を参照してください。

1. Data Protector for PCs のインストール用 CD-ROM を挿入します。インストールウィザードが自動的に起動しない場合は、インストール CD-ROM のルートで `setup.hta` をダブルクリックして手動で実行します。
2. 画面上の指示に従います。
3. Data Protector for PCs Policy Server は、Microsoft SQL Server データベースにアクセスできる必要があります。[Microsoft SQL Server Express の既存の Data Protector for PCs インスタンスを使用する] を選択するか、[Microsoft SQL Server の既存のインスタンスを使用する] をクリックします。既存の SQL Server を使用するように選択した場合は、データベースサーバー接続文字列と、新しいデータベースを作成するための十分な権限を持つアカウントの資格情報を入力する必要があります。
4. ウィザードの [Data Protector for PCs Policy Server のインストール] ページで、[インストール] をクリックし、インストールを開始します。
5. インストールが完了したら、[次へ] をクリックします。ここで、Data Protector for PCs Policy Server Console の実行を選択できます。
6. 別のシステムに Web Data Vault Server をインストールします。メインのインストール画面で [Data Vault のインストール] をクリックします。

注記: インストール時に、Web Data Vault Server ソフトウェアと共に常にクリーンアップソフトウェアがインストールされます。Windows ファイル共有 Data Vault のみをホストする Data Vault Server は、最適なパフォーマンスを得るために Data Vault にローカルにインストールすることが推奨されます。

詳細インストール

注記:

Windows 2003 Server のみ: このサーバーの .NET 2.0 Framework ランタイムのセキュリティ ポリシーがローカル イントラネット セキュリティ ゾーンに対して [Full Trust] に設定されている場合、Data Protector for PCs Policy Server は、ネットワーク上で共有されている CD-ROM、またはネットワークファイル共有からのみインストール可能です。サーバーにローカル CD-ROM ドライブがない場合は、管理ツールの .NET Framework 2.0 構成ツールを使用して、ローカル イントラネット セキュリティ ゾーンのランタイムセキュリティ ポリシーを [Full Trust] に変更するか、CD からサーバー上のローカル ディスクに Server フォルダをコピーします。

Data Protector for PCs Policy Server をインストールするには、「管理者」権限を持つアカウントにログインする必要があります。

1. Data Protector for PCs のインストール用 CD-ROM を挿入します。インストールウィザードが自動的に起動しない場合は、インストール CD-ROM のルートで `setup.hta` をダブルクリックして手動で実行します。
2. [Policy Server のインストール] をクリックします。
要求されたら、[このプログラムをディスクに保存] ではなく、[このプログラムを現在の場所から開く] (または [このプログラムを現在の場所から実行]) を選択します。
3. Data Protector for PCs Policy Server には、.NET Framework 2.0 SP1 が必要です。事前にインストールされていない場合は、CD-ROM からそれをインストールするかどうかの確認が求められます。
インストールするには、Windows Installer 3.1 以降が必要です。必要な場合は、CD-ROM から Windows Installer 3.1 をインストールするかどうかの確認が求められます。
4. インストールウィザードは、他の必要なソフトウェアがインストールされていることをチェックします。
 - インターネット インフォメーション サービス (IIS)
 - ASP.NET 2.0いずれかが不足している場合は、リストの該当する要件をクリックすると、そのインストール方法の詳細が表示されます。
[次へ] をクリックします。
5. Microsoft SQL Server をインストールします。

Microsoft SQL Server の既存のインスタンスを使用するには:

- a. [Microsoft SQL Server 2000/2005 の既存のインスタンスを使用する] をクリックします。
- b. [データベースサーバー] フィールドで、既存のデータベースサーバーへの接続文字列を入力します。
- c. [ログイン] フィールドと [パスワード] フィールドで、新しいデータベースを作成するために十分な権限を持つアカウントの資格情報を入力します。通常、これは「sa」アカウントです。
- d. [次へ] をクリックします。入力した接続情報は、既存のデータベースサーバーにテスト接続するために使用されます。接続に成功すると、ウィザードはステップ 6 に進みます。

Microsoft の SQL Server Express Edition の Data Protector for PCs インスタンスをインストールするには:

- a. [Microsoft SQL Server Express の DataProtectorNE インスタンスをインストールする] を選択し、[次へ] をクリックします。
 - b. [インストール] をクリックして、Microsoft SQL Server 2005 Express Edition のインスタンスをインストールし、「DataProtectorNE」という名前を付けます。インストールが完了したら、[次へ] をクリックします。
6. Data Protector for PCs Policy Server ソフトウェアをインストールします。
- a. 初期画面で、[次へ] をクリックして、インストールを開始します。
 - Data Protector for PCs Policy Server Console が、Web アプリケーションとして仮想ディレクトリ `C:\Inetpub\wwwroot\dpnepolicy` にインストールされます。
 - Data Protector for PCs Web サービスは、`C:\Inetpub\wwwroot\dpnepolicyservice` にインストールされます。どちらも、ポート 80 で HTTP プロトコルを使用します。
 - b. Policy Server のインストールが完了したら、[閉じる]、さらに [次へ] をクリックします。
7. ここで、クリーンアッププログラムをインストールする必要があります。[インストール] をクリックし、インストールを開始します。
8. クリーンアップのインストールが終了したら、[次へ] をクリックします。

Data Protector for PCs は、Data Protector for PCs Policy Server Console から集中管理します。コンソールはブラウザベースであるため、(HTTP ポート 80 を使用して) Policy Server へのブラウザ接続を確立できる任意のコンピューターから Data Protector for PCs を管理できます。

Policy Server 上のブラウザから Data Protector for PCs Policy Server Console を実行するには、[Policy Server Console を実行する] チェックボックスをオンのままにして、[終了] をクリックします。

注記: インストール時に、クリーンアップソフトウェアは Policy Server にインストールされます。また、パフォーマンスを最適化するため、クリーンアップソフトウェアを Data Vaults にもインストールすることを推奨します。

注記:

Policy Server Console 用のブラウザ設定: ご使用のブラウザで Policy Server Console のページを正しく表示できない場合は、ブラウザのセキュリティ設定をチェックします。コンソールには、以下の設定が必要です。

- JavaScript を有効にする必要があります。
- dpnepolicy の Web サイトに対してポップアップ ブロックを無効にする必要があります。
- ブラウザーの種類とそのバージョンによっては、システムの動作に制限を加えるこれ以外のセキュリティ設定を変更しなければならない場合があります。

Microsoft SharePoint とのインストール: Policy Server が Microsoft SharePoint の動作するサーバーにインストールされると、Policy Server Console を実行したときに「ページが見つかりません」という 404 エラーが表示されることがあります。Microsoft 社の Web サイト <http://support.microsoft.com/kb/828810> にあるナレッジベースの記事に、この問題と解決策が記述されています。この問題は、Policy Server だけでなく、すべての ASP.NET Web アプリケーションにあてはまることに注意してください。

SharePoint を使用しているサーバーで Policy Server を実行するには、以下の手順に従ってください。

1. SharePoint 管理ツールを使用して、2 つの Policy Server Web アプリケーション、dpnepolicy および dpnepolicyservice に対して除外を作成します。
2. Microsoft 社のナレッジベースの記事の説明に従って、2 つの Policy Server の web.config ファイル (dpnepolicy\web.config および dpnepolicyservice\web.config) を変更して、<httpHandlers> および <trust> XML コードを追加します。

3 Web Data Vault Server のインストール、設定、保守

Web Data Vault Server のインストールおよび設定

注記: Web Data Vault Server を Policy Server とは別のシステムにインストールします。(同じシステムにインストールすることも可能ですが、これは評価目的の場合にのみ適しています)。

1. Data Protector for PCs のインストール用 CD-ROM を挿入します。インストールウィザードが自動的に起動しない場合は、インストール CD-ROM のルートで `setup.hta` をダブルクリックして手動で実行します。
2. [Data Vault のインストール] をクリックします。
3. 以下のいずれかを選択します。
 - **Web Data Vault Server** (推奨)。これによって、サーバーにもクリーンアップソフトウェアがインストールされます。
 - **Windows ファイル共有 Data Vault 用のクリーンアップソフトウェア**。
Windows ファイル共有 Data Vault のみを使用する予定の場合はこれを選択します。

詳細については、「[「Data Vault」\(9 ページ\)](#)」を参照してください。

4. 画面の指示に従って、インストールを完了させます。
5. Policy Server からライセンスを取得した後、Web Data Vault Server をインストールする場合は、Web Data Vault の設定を開始します。
[サーバー設定] 画面で、サーバーの完全修飾ドメイン名 (FQDN) と SSL ポートを入力します。Policy Server に Web Data Vault ポリシーを設定する際、同じ FQDN を使用する必要があります。名前はすべてのクライアント システムが解決可能なものにしないと、このサーバー上の Data Vault に一部バックアップできない場合があります。
6. [証明書設定] 画面で次のいずれかを選択します。
 - 認証局 (CA) から既存の SSL 証明書をインポートする。これは推奨オプションで、最高レベルのセキュリティを提供します。
 - 自己署名 SSL 証明書を作成する。セキュリティ レベルが低いので、評価目的のみに使用します。

注記: Web Data Vault Server の証明書は、DvConfig ユーティリティを使用し、インストール後いつでも交換できます。これには、自己署名証明書が設定されていたインストールを、インポートした証明書を使用するよう再構成することも含まれます。「[CLI \(DvConfig\) を使用した Web Data Vault オプションの設定](#)」(21 ページ) を参照してください。

7. 次の画面では、Web Data Vault Server の以下の 2 タイプのユーザー名の入力が必要と求められます。
- **管理者ユーザー** — Data Vault の作成と削除、およびクライアントのバックアップデータの移行などの管理タスクを行うユーザー。
 - **バックアップユーザー** — ファイルのバックアップやリストアなどのエンドユーザー操作を実行するユーザー。

これらのユーザーは Data Protector for PCs Web Data Vault Server 固有です。このサーバーの Web Data Vault を作成または編集するときには、両方の詳細を入力する必要があります。

注記: パスワードの長さは 8 文字以上とする必要があります。

8. Web Data Vault Server のインストールおよび設定と、クリーンアップソフトウェアのインストールを完了するには、[次へ] をクリックし、[完了] をクリックします。

Web Data Vault の保守

1. [データ ポルト ポリシー] ページで、サーバーの完全修飾ドメイン名と SSL ポート、バックアップユーザーのアカウント情報を入力します。その後、[Data Vault の設定] をクリックします。
2. 管理者ユーザー アカウント情報が送信され、[Web Data Vault Server の保守] ページが表示されます。

ここで、既存の Web Data Vault を選択または削除できます。また、新しい Data Vault を追加することもできます。

注記: 現在別の Data Vault ポリシーに接続されていない既存の Data Vault のみを選択できます。

3. 必ずページ下部の [保存] をクリックして Data Vault ポリシーを保存します。
4. 新しい Data Vault を追加した場合、オプションで Data Vault が存在することと設定が正しいことをテストできます。

Windows ファイル共有 Data Vault から Web Data Vault へのデータの移行

Data Vault 内のデータのレイアウトは、Windows ファイル共有 Data Vault でも HTTPS Web Data Vault でも同一です。これは、既存の DPNE 6.x Data Vault から新しい Web Data Vault へデータを移行することが可能であることを意味します。

注記: データの移行は、同じ Policy Server に属する Data Vault または同じ暗号パスワードを共有する Data Vault からしか実行できません。

データは以下の 2 とおりのシナリオにおいて移行可能です。

- Web Data Vault のホストに、同じシステムを使用します。

注記: 同じディレクトリに Windows ファイル共有と Web Data Vault で同時にアクセスすることはできません。

- Data Vault 全体を別のシステムに移動します。

いずれの場合も、Web Data Vault Server はデータを保持するシステムのローカルにインストールする必要があります。

既存の Windows ファイル共有 Data Vault から Web Data Vault にデータを移行する方法:

注記:

- バックアップの実行の影響を最小限にするには、移行は業務時間外に行ってください。
- Windows のタスク マネージャを参照し、DPNECleanup.exe が現在実行されていないことを確認します。
- Policy Server のクリーンアップ ポリシーを確認し、DPNECleanup.exe の実行スケジュールが移行期間と重なっていないことを確認します。

1. Web Data Vault Server をインストールし、Policy Server および Agent をバージョン 7.0 に更新します。7.0 のインストール後、すべての Agent が再起動されたことを確認します。再起動されている場合のみ、Web Data Vault へのデータのバックアップを開始できます。
2. [Data Vault ポリシー] ページで適切な Windows ファイル共有ポリシーを無効にし、Agent が Data Vault へのデータのコピーを停止するようにします。
3. Web Data Vault で同じディレクトリを使用する場合は、CIFS 経由でのディレクトリの共有は停止してください。
4. Web Data Vault が Windows ファイル共有 Data Vault とは別のサーバーにある場合、データは 67 文字以下のマシンのフォルダーパスにコピーする必要があります。Data Vault が同じサーバー上にある場合、別の理由で意図的に行う場合を除き、新しい場所にデータをコピーする必要はありません。

5. 新しい Web Data Vault を作成する前に、初期更新処理の動作を決定します。すべての Agent で初期更新が行われている場合、既存の Data Vault ではバックアップデータは既に完全であるので初期更新はスキップできます。初期更新をスキップするオプションは Data Vault ポリシーの直接のオプションではなく、参照しているコピー ポリシーのもので、適切なオプションが選択された Data Vault ポリシーが存在することを確認します (つまり、「初期更新」がオフになっており、適切な制限およびスケジュールが設定されています)。このためには、新しいコピー ポリシーを作成するか、既存のポリシーを変更します (この場合、コピー ポリシーを参照するすべての Data Vault ポリシーが影響を受けます)。
6. Web Data Vault の新しい Data Vault ポリシーを作成および保存します。新しい Web Data Vault を作成する際、フォルダー パスを入力する必要があります。これは、移行する Windows ファイル共有 Data Vault の実データがあるパスになります。手順 5 で作成したコピー ポリシーを選択します。Data Vault ポリシーのその他のオプションを、元の Windows ファイル共有 Data Vault ポリシーと同一に設定します (ネットワーク設定、Active Directory 設定など)。
7. Agent が新しい Web Data Vault に正常にファイルをバックアップしていることを確認したら、元の Windows ファイル共有 Data Vault ポリシーを削除します。ポリシーを保存したら、Agent は HTTPS プロトコルを使用し、新しい Web Data Vault へのデータのコピーを再開します。

CLI (DvConfig) を使用した Web Data Vault オプションの設定

CLI からこのユーティリティを使用すると、Web Data Vault のパラメーター (バックアップユーザーや管理者ユーザーおよびそのパスワードなど) の変更、新しい証明書のインポート、SSL の変更、新しい自己署名証明書の作成が可能になります。

パラメータを変更する前に、HP Data Protector for PCs Data Vault Server の Windows サービスを終了して Web Data Vault Server を終了する必要があります。

変更後、Web Data Vault のサービスを再開します。更新したすべてのポリシーは、Agent に再配布されます。

注記: DvConfig を使用し、Web Data Vault Server の SSL ポート、バックアップユーザー名、パスワードを変更した場合、整合性のため Policy Server 上の対応する Data Vault のポリシーも変更する必要があります。

用法:

```
DvConfig [-adminUser login:password -backupUser login:password] [-h] [-i certfile | -s hostname] [-p port] [-v]
```

`-adminUser login:password`

DvAdmin アカウントの資格情報を設定します。login または password を設定しない場合、デフォルトの「DvAdmin」が使用されます。

`-backupUser login:password`

DvAdmin アカウントの資格情報を設定します。login または password を設定しない場合、デフォルトの「DvBackup」が使用されます。

-h

このメッセージを表示します。

-i *certfile*

既存の証明書をインポートします。

-p *portSSL* ポートを設定します。

-s *hostname*

完全修飾されたドメイン名の自己署名証明書を作成します。

-v

バージョン情報を表示し終了します。

4 Data Protector for PCs 保護ポリシーの設定

Data Protector for PCs インストール後の初期セットアップ

Data Protector for PCs のインストール後すぐに、Policy Server Console に [初期セットアップ] ウィンドウが表示されます。Data Protector for PCs のポリシーをセットアップするには、事前に、次の設定手順を正常に完了しておく必要があります。

1. 暗号化パスワードを定義またはインポートする。

セキュリティのため、Data Protector for PCs を使用する前に、暗号化パスワードを定義する必要があります。これによって、すべてのファイルがユーザー コンピューターで暗号化され、暗号化されたファイルがネットワーク経由で送信されるように保証されます。すべてのユーザーからのファイルと、中央で設定されたすべての Data Vaults のファイルの暗号化には、同じパスワードが使用されません。

- 中央で定義された Data Vault (Policy Server Console を通じて定義) は、常に、Data Protector for PCs 暗号化パスワードに基づく暗号化を使用します。
- ローカルで定義された Data Vault の場合 (ユーザーによってそれぞれのコンピューターを使用して定義)、ユーザーはそれぞれについて暗号化を使用するかどうかを選択し、ユーザー専用のパスワードを指定できます。

Data Protector for PCs の初回インストール時には、続行する前にパスワードを**生成**または**インポート**する必要があります。パスワードを生成したら、安全のため、パスワードを**エクスポート**してください。これで、安全な場所に保管します。後でインポートに使用することができます。

パスワードを管理するため、[暗号化ポリシーを設定する] をクリックして、ウィンドウ上の指示に従います。

注記: パスワードを生成またはインポートした後は、それを変更できません。

2. Data Protector for PCs のライセンスを登録する。

Data Protector for PCs を評価する場合は、ライセンスを追加せずに 60 日間使用できます。保護できるユーザー数の制限もありません。Data Protector for PCs を購入する場合は、HP の License Key Delivery Service (<https://webware.hp.com/welcome.asp>) にアクセスしてライセンス キーをダウンロードする必要があります。後の手順でこのライセンス キーを入力できます。購入できるライセンスの種類は次のとおりです。

- TA032AA または TA032AAE (100 個の Agent を使用可能)
- TA033AA または TA033AAE (1000 個の Agent を使用可能)
- TA036AA または TA036AAE (100 個の Agent および HP Data Protector Starter Pack Windows (B6961BA または B6961BAE) 用)

評価期間の終了前に、恒久ライセンスキーを入力する必要があります。ライセンスパスワードを入力しないと、期限の終了日に当たる 60 日目に、Agent がデータを Local Repositories にも Data Vaults にもコピーできなくなります。ただし、以前に保護されたファイルバージョンを復元することはできます。

ライセンスを管理するには、[ライセンス管理]、[Data Protector for PCs ユーザーのライセンス キーを入力する] の順にクリックします。ウィンドウ上の指示に従います。

注記: ライセンスは、Agent のインストール時に、各 Agent に配布されます。

上記の設定手順が正常に完了すると、Policy Server Console は完全に使用可能になります。Data Protector for PCs をインストールしたばかりの場合は、Data Protector for PCs のその他の要素を、次の項で示す順番で設定します。

初回インストール時の設定

Data Protector for PCs には、大半の組織で十分に機能するポリシーが事前に設定されています。最初に Data Vault ポリシー、コピー ポリシー、およびファイル保護ポリシーを設定し、その後、ユーザーのデスクトップおよびノートブックに Data Protector for PCs Agent ソフトウェアをインストールすることを推奨します。

注記: 新しいポリシーを設定する代わりに、Data Protector for PCs に事前設定されているポリシーを変更することができます。各段階で、[新しいポリシーを作成する]ではなく [既存のポリシーを編集する] 選択するだけです。

インストールの保護ポリシーは Policy Server Console から設定します。中央で定義したポリシーは、すべての Data Protector for PCs Agent に配布され、ユーザーのデスクトップおよびラップトップで実行されます。

1. インストールの終わりに、またはブラウザーから次の URL を使用して随時に、Data Protector for PCs Policy Server Console を実行します。

`http://policyserver/dpnepolicy/`

ここで、「`policyserver`」は使用している Data Protector for PCs Policy Server の名前です。サーバーに「管理者」としてログインする必要があります。

2. **Data Vault ポリシーを設定します。**

Data Vault ポリシーは、ポリシーで保護されたユーザー ファイルの継続バックアップの保管先 (Web Data Vault または Windows ファイル共有) を設定します。ファイルが変更された際、編集前のバージョンと編集されたファイルを 1 つまたは複数の保管先に自動的にバックアップできます。各ユーザー グループは 1 つまたは複数の Data Vault に割り当てられます。たとえば、**営業所**という名前の Data Vault ポリシーを定義し、それを**東京営業所**、**大阪営業所**、**札幌営業所**、**名古屋営業所**というユーザー グループに割り当てます。

- 中央で定義された Data Vault (Policy Server Console を通じて定義) は、常に、Data Protector for PCs 暗号化パスワードに基づく暗号化を使用します。

- ローカルで定義された Data Vault の場合 (ユーザーによってそれぞれの Agent ソフトウェアを使用して定義)、ユーザーはそれぞれについて暗号化を使用するかどうかを選択し、ユーザー専用のパスワードを指定できます。

注記: すべての Data Vault の要件:

Data Protector for PCs は、元のファイルと同じファイル サーバーにバックアップされたファイルにアクセス許可 (ACL) を設定します。つまり、ユーザーは、自分のコンピューター上で元のファイルにアクセスできる場合にだけ、バックアップされたファイルを回復できます。

Windows ファイル共有 Data Vault の要件:

標準的な Windows ファイル共有 Data Vault を使用する場合、共有は、Windows ファイルサーバー上に配置する必要があります。このファイルサーバーと Policy Server がインストールされているマシンが同じマシンである必要はありません。ただし、インストールされている Agent の数も少なく Data Protector for PCs を評価しているだけの場合は、Policy Server と Data Vault を同じマシンにすると役立つことがあります。

Data Vault ポリシーを作成するには:

- 左側のナビゲーションペインで、[ポリシー]、[データ ポルト]、[データ ポルト ポリシー] の順にクリックします。
- [新しいデータ ポルト ポリシーを作成する] をクリックします。
- ウィンドウ上の指示に従います。Data Vault のタイプとして、[Web ベース] または [Windows ファイル共有] を選択したかによってこの手順は異なります。

注記: Data Vault を作成する場合、フォルダーまたは共有のパス長は 66 文字以下にする必要があります。

ベストプラクティス:

この時点では、コピー ポリシーは「デフォルト」のままにしておきます。

Windows ファイル共有 Data Vault のクリーンアップ:

- Data Vault がこの Policy Server にある場合は、このマシン名のデフォルト設定のままにします。
- Data Vault が別の Windows ファイルサーバー上にある場合は、そのサーバーに Data Vault クリーンアップ ソフトウェアをインストールし、そのマシンをクリーンアップ マシンとして指定します。

3. コピー ポリシーを設定します。

コピーポリシーは、Data Vault に同時にコピーできるクライアント数の制限を設定します。継続的バックアップを補完するための初期およびスケジュールされた Data Vault の更新も定義します。各コピーポリシーは 1 つまたは複数の Data Vaults に割り当てられます。

コピーポリシーは、次のことを定義します。

- Data Vaults に同時にファイルをコピーできる Agent の数。
- 定期的な更新のスケジュール。ユーザーに関連すると予想されるファイルがすべて Data Vault に存在することを確認し、存在しない場合は、不足しているファイルをコピーします。これにより、すべてのユーザーファイルが Data Vault に適切にコピーされていることをより強力に保証します。
- **初期更新** (またはコピー) を実行する必要があるかどうか。通常の Data Protector for PCs 操作の間は、ユーザーが Data Protector for PCs 継続的保護ファイルを変更するたびに、変更に関する情報しか Data Vault にコピーされないため、初期更新が必要です。

デフォルトのコピーポリシーが、明示的にコピーポリシーが設定されていないすべての Data Vaults に適用されます。デフォルトのコピーポリシーの設定値は変更できますが、削除したり、名前を変更したりすることはできません。

コピーポリシーを作成するには:

- a. 左側のナビゲーション ペインで、[ポリシー] をクリックします。
- b. [コピー ポリシーを設定する] をクリックします。
- c. [新しいコピー ポリシーを作成する] をクリックします。
- d. ウィンドウ上の指示に従います。

ベスト プラクティス:

- 制限: 期間を通常の営業時間に設定し、その他の時間帯の下限を設定します。
- 初期更新: ファイル保護ポリシーによって保護されているすべてのユーザーファイルがバックアップされるように保証するため、初期更新を有効にします。
- 毎週/毎月ファイルを更新する: 更新にはいくつかのファイルコピー (ある場合) が含まれるため、ポリシーで保護されたすべてのユーザーファイルが適切にバックアップされることを保証するために Data Vault 更新を有効にします。

4. ファイル保護ポリシーを設定します。

ファイル保護ポリシーでは、どのファイルを保護し、以前のバージョンをどれだけの期間保持するかを指定できます。たとえば、Word 文書、Excel スプレッドシート、PowerPoint プレゼンテーションに関して、**Office 文書**という名前のファイル保護ポリシーを定義できます。

ローカルディスクドライブ上のファイルは保護することができます。

2つのタイプのポリシーがあります。

- **Continuous File Protection:** ファイルがディスクに保存されたり削除されたりしたときに、いつでもリアルタイムにファイルを保護します。一般に、メ

ニューの [保存] を選択できるファイルや文書は、Continuous File Protection ポリシーで保護できます。

Data Protector for PCs には、各種のサンプル ポリシーが含まれています。インストール後、デフォルトで、**Office 文書**、**ソフトウェア開発**、および **Web 文書** の 3 つが選択されています。これらのポリシーを使用して開始することもできれば、自分専用のポリシーを作成することもできます。

- **Open File Protection:** ファイルの「スナップショット」を定期的 (通常、1 時間に 1 回) とることで、ファイルを保護します。一般的に、とても大きかったり (100 MB 以上)、1 日中ずっと開いていたり、[保存] メニューがないようなファイルはこの方式で保護します。この種のファイルのうち典型的なものとしては、メールやデータベース ファイルがあります。

Data Protector for PCs の 4 つの例: **Microsoft Outlook**、**Microsoft Outlook Express**、**Windows メール**、**Thunderbird** の 4 つの例があります。これらのポリシーを使用して開始することもできれば、自分専用のポリシーを作成することもできます。

注記: Data Protector for PCs は Open File Protection ポリシーのある EFS 暗号化ファイルのバックアップをサポートしないため、.pst のようなファイルは EFS 暗号化してはいけません。

ファイル保護ポリシーの作成方法:

- a. 左側のナビゲーション ペインで、[ポリシー] をクリックします。
- b. [ファイル保護ポリシーを設定する] をクリックします。
- c. [新しいファイル保護ポリシーを作成する] または [新しいオープン ファイル保護ポリシーを作成する] をクリックします。
- d. ウィンドウ上の指示に従います。

注記: ファイル保護ポリシーを作成し除外または追加ルールを設定するとき、ファイル拡張子は、Open File Protection ポリシーの場合は 9 文字、Continuous File Protection ポリシーの場合は 29 文字までにしてください。

Open File Protection ポリシーの追加ルールでは、拡張子を指定せずファイルを選択できます。Continuous File Protection ポリシーでは、これは実行できません。

- ① **重要:** これで、Data Protector for PCs が必要とするすべての基本ポリシーが設定されました。Data Protector for PCs には、大半の組織で十分に機能するその他のポリシーも事前に設定されています。この時点で、ユーザーのデスクトップおよびラップトップで Agent のインストールを開始することを推奨します (「[Data Protector for PCs Agent のインストール](#)」(37 ページ)を参照)。後から、クリーンアップポリシー、ユーザー制御ポリシー、Agent 更新ポリシー、レポート データ保持ポリシーなどの他の Data Protector for PCs ポリシーを見直して、設定することができます。
-

その他のポリシーの設定

1. Active Directory へのアクセスを設定します。

注記: Active Directory グループの Data Vault との関連付け: Data Vault ポリシーで、Data Vault と Active Directory グループを関連付けることができます。関連付けられたグループのすべてのメンバーは、関連付けられた Data Vault にバックアップされます。ただし、個々のユーザーを関連付けることはできません。さらに、組織単位 (OU) を関連付けると、その OU に属するグループだけが関連付けられます。直接 OU 内にあるユーザーは、Data Vault に関連付けられません。Active Directory グループのリストに、誤ってセキュリティグループ以外のグループ (ディストリビューショングループなど) が含まれることがありますが、ただし、実際にはセキュリティグループだけが Data Vault に関連付けられます。

複数ユーザー: 2 人以上のユーザーが 1 台のコンピューターを共有している場合、これらのユーザーは同じ Active Directory グループに属している必要があります。

グループや組織単位ごとに Data Vaults を割り当てる場合や、グループや組織単位別にレポートする場合は、Active Directory にアクセスできるように Policy Server を設定する必要があります。

Active Directory へのアクセスを設定すると、Data Vault の [グループおよび組織単位のメンバー] オプションが有効になります (「[初回インストール時の設定](#)」(24 ページ)を参照)。

Active Directory へのアクセスを設定するには:

- 左側のナビゲーション ペインで、[設定] をクリックします。
- [Active Directory へのアクセスを設定する] をクリックします。
- ウィンドウ上の指示に従います。

2. クリーンアップポリシーを設定します。

ユーザー コンピューターの Data Protector for PCs Local Repository と、Data Vault Server 上の Data Vault は、定期的にクリーンアップして、ファイル保護ポリシーで定義した保持期間の設定を経過している古いバージョンを削除する必要があります。

クリーンアップポリシーを設定するには:

- a. 左側のナビゲーション ペインで、**[ポリシー]** をクリックします。
- b. **[クリーンアップ ポリシーを設定する]** をクリックします。
- c. ウィンドウ上の指示に従います。

Data Vault でサポート可能なユーザー数を増やすには、週末にだけクリーンアップ処理を実行します。金曜の晩または土曜の早朝に開始し、最大限の時間を使用して実行できるようにします。

- a. Policy Server 管理コンソールの **[クリーンアップ ポリシー]** ページを開き、**[データ ボルトのクリーンアップ スケジュール]** を変更します。
- b. 金曜または土曜を除くすべての曜日のチェックボックスをオフにします。
 - 金曜の場合、午後 10 時など晩の遅い時間を選択します。
 - 土曜の場合、午前 1 時など早朝の時間を選択します。

クリーンアップを週末にだけ実行した場合:

- Data Vault から回復するために表示されるファイルのリストは、1 週間後には古くなります。ユーザーは、最新のビューを得るために、Data Vault 上のデータの手動再スキャンをいつでも開始できます。
- クリーンアップは週末にしか実行されないため、バックアップバージョンは、有効期限が切れても最大 1 週間存在し続けます。
- クォータ管理は最新ではありません。ユーザーがクォータを超えた場合、クリーンアップが実行されて Data Vault に空き容量ができるまで待つ必要があります。逆に、容量使用状況レポートはクリーンアップ処理の一部であるため、クォータの超過はすぐには認識されません。

ベスト プラクティス:

- ローカル リポジトリのクリーンアップ スケジュール: デフォルトの 1 時間のままにしておきます。
- データ ボルトのクリーンアップ スケジュール: 大半のインストールでは、「毎日、真夜中にクリーンアップする」デフォルト設定で十分なはずですが。Data Vault の容量の詳細については、「[サイズ決定に関する推奨事項](#)」(32 ページ) を参照してください。
- CPU とディスクを最適に使用して格納するデータ量を増やすため、再使用および拡張可能な方法で複数のスレッドを使用するように DPNECleanup を設定できます。「[マルチスレッド クリーンアップの設定](#)」(35 ページ) を参照してください。

3. ユーザー制御ポリシーを設定します。

ユーザー制御ポリシーは、ユーザーのコンピューターに割り当てられた組織のポリシーに対してユーザーが制御できる範囲を決定します。

ユーザー制御ポリシーを設定する

- a. 左側のナビゲーション ペインで、[ポリシー] をクリックします。
- b. [ユーザー制御ポリシーを設定する] をクリックします。
- c. ウィンドウ上の指示に従います。

ベスト プラクティス:

[ファイルの回復] に [ユーザによる制御を許可する] を設定します。

4. Agent 更新ポリシーを設定します。

ポリシーは、Data Protector for PCs で保護されるすべてのデスクトップとラップトップが使用する Data Protector for PCs Agent のバージョンを指定します。Agent はすべて自動的にこのバージョンに更新されます。

Agent 更新ポリシーを設定するには:

- a. 左側のナビゲーション ペインで、[ポリシー] をクリックします。
- b. [Agent 更新ポリシーを設定する] をクリックします。
- c. ウィンドウ上の指示に従います。

5. レポートデータの保持期間を設定します。

これは、情報の主要なカテゴリごとに、レポート目的でデータを保持しておく期間を設定します。

レポートデータの保持期間を設定する

- a. 左側のナビゲーション ペインで、[設定] をクリックします。
- b. [レポート データの保持期間を設定する] をクリックします。
- c. ウィンドウ上の指示に従います。

その他の構成タスク

次の手順は、通常、Data Protector for PCs の初回インストール時に実行されます。

Data Protector for PCs ソフトウェアのライセンスを登録します。

Data Protector for PCs を評価する場合は、ライセンスを追加せずに 60 日間使用できます。保護できるユーザー数の制限もありません。Data Protector for PCs を購入する場合は、HP の License Key Delivery Service (<https://webware.hp.com/welcome.asp>) にアクセスしてライセンス キーをダウンロードする必要があります。後の手順でこのライセンス キーを入力できます。

ライセンス キーを入力するには、以下の手順に従ってください。

1. 左側のナビゲーション ペインで、[ライセンス管理] をクリックします。
2. [HP Data Protector for PCs ユーザーのライセンス キーを入力する] をクリックします。
3. ウィンドウ上の指示に従います。

複数のライセンスを入力する場合は、行ごとにライセンス キー文字列を 1 つ記述したテキスト ファイルを作成することができます。その後、[ライセンス キーをインポートする] フィールドを使用してファイルをインポートできます。

注記: ライセンスは、Agent のインストール時に、各 Agent に配布されます。

ライセンスの移動

Policy Server の IP アドレスを変更して別のシステムに移動する必要がある場合、またはライセンスを Policy Server 間で移動する必要がある場合は、<https://webware.hp.com/welcome.asp> の HP License Key Delivery Service にアクセスしてください。

暗号化パスワードを設定、インポート、およびエクスポートします。

セキュリティのため、Data Protector for PCs を使用する前に、暗号化パスワードを定義する必要があります。これによって、すべてのファイルがユーザーコンピューターで暗号化され、暗号化されたファイルがネットワーク経由で送信されるように保証されます。すべてのユーザーからのファイルと、中央で設定されたすべての Data Vaults のファイルの暗号化には、同じパスワードが使用されます。

- 中央で定義された Data Vault (Policy Server Console を通じて定義) は、常に、Data Protector for PCs 暗号化パスワードに基づく暗号化を使用します。
- ローカルで定義された Data Vault の場合 (ユーザーによってそれぞれのコンピューターを使用して定義)、ユーザーはそれぞれについて暗号化を使用するかどうかを選択し、ユーザー専用のパスワードを指定できます。

Data Protector for PCs の初回インストール時には、続行する前にパスワードを生成またはインポートする必要があります。パスワードの生成後は、安全のために、パスワードをエクスポートします。これで、安全な場所に保管します。後でインポートに使用することができます。

注記: パスワードを生成またはインポートした後は、それを変更できません。

暗号化パスワードの管理方法:

1. 左側のナビゲーション ペインで、[ポリシー] をクリックします。
2. [暗号化ポリシー] をクリックします。
3. ウィンドウ上の指示に従います。

サポートできる Agent の数の決定

すべての環境で通用する全般的なルールを提案することは困難です。このため、ここではいくつかのケースを挙げ、ここで提示する数が有効になる状況について曖昧さを残さず明快に説明します。

サイズ決定を左右する要素

Data Protector for PCs 環境のサイズ決定は複雑です。ある環境でサポートできるユーザーの数を左右する技術的要素には、次のようなものがあります。

- Data Vault の処理能力 (バックアップデータの夜間統合のため)
- Data Vault サーバーのネットワークおよび I/O 帯域幅
- Data Vault サーバーのディスク容量
- Policy Server 上の SQL データベースのサイズ
- Policy Server のネットワーク帯域幅と処理能力

インストール済みの構成で上記の項目のうちどれがボトルネックの原因になるかは、次に示す Data Protector for PCs のコンフィギュレーション設定および使用パターンの両方によって決まります。

- Data Vault のユーザー数
- 設定された保護ポリシーで保護されるファイルの数とサイズ
- 保護されるファイルの変更頻度
- 保護されるファイルタイプの保持設定

サイズ決定に関する推奨事項

Data Vault

データ特性が平均的に次のようになっている場合、14 TB のディスク容量を持つ Data Vault は、毎日のクリーンアップ スケジュールにより、最大 **3,500** 個の Agent に対応する数のユーザーをサポートできます。

- 保護されるファイルの平均数: 5000
- ローカルディスク上で保護されるファイルの平均総サイズ: 10 GB
- Data Vault の平均総サイズ (圧縮): 4 GB

平均的にこの例よりも保護する必要があるデータの量が多い場合は、Data Vault のディスク容量を単純に増やしてもデータを保存できる余地は増えますが、Data Vault で適切なタイミングでバックアップ データの夜間統合を行えなくなることがあります。次の可能性を検討してください。

- Data Vault クリーンアップを週末にだけ実行します。この方法については、「[その他のポリシーの設定](#)」(28 ページ) の手順 2「クリーンアップ ポリシーを設定します。」を参照してください。これにより、40 TB のディスク容量を持つ Data Vault でサポートできる Agent の数が、10,000 に増えます (平均的なデータ特性が同じである場合)。
- エンドユーザー データの複数の Data Vault への分散を検討してください。

該当する Data Vault のハードウェア仕様は次のとおりです。

Data Vault タイプ	毎日のクリーンアップ (最大 3,500 個の Agent)	毎週のクリーンアップ (最大 10,000 個の Agent)
Windows ファイル共有	3 GHz デュアル コア、4 GB RAM、14 TB のディスク容量	3 GHz デュアル コア、4 GB RAM、40 TB のディスク容量
Web Data Vault	3 GHz クアッド コア、4 GB RAM、14 TB のディスク容量	3 GHz クアッド コア、4 GB RAM、40 TB のディスク容量

ユーザーの所有するデータが平均的に少ない場合は、1 つの Data Vault で 1,000 人を超えるユーザーをサポートできます。

注記: パフォーマンスを最大限に引き出すために、Data Vault のオペレーティングシステムとバックアップデータは別々の物理ディスク上に保存することを強く推奨します。

最適なパフォーマンスのために、Data Vault ディスクは定期的にデフラグする必要があります。

Policy Server

Policy Server 上で生成されるトラフィックの量は、サーバーがサポートする Agent の数に直接左右されます。Data Protector for PCs に付属の MS SQL Server Express Edition を使用する場合は、データベースの最大サイズは 4 GB になります。また、サポートできる Agent の最大数は 5,000¹ です。

ご使用の環境で 5,000 を超す Agent をサポートする必要がある場合は、Policy Server を追加するかまたは MS SQL Express を Microsoft SQL Server の完全版と入れ替えることができます。このようにすれば、最大 50,000 の Agent をサポートするように Policy Server を簡単にスケールアップできます。MS SQL Server の完全版を使用する場合は、Policy Server のメインメモリを 3 GB 以上にアップグレードすることを検討してください。

パフォーマンス上の理由から、Policy Server は Data Vault Server とは別のサーバーで実行する必要があります。同じサーバー上で実行することも可能ですが、これは評価目的の場合にのみ推奨します。

Policy Server は最低 1 つ必要ですが、Policy Server の数と Data Vaults の数が一致する必要はありません。

1. Policy Server 上の「レポートデータの保持期間」のデフォルト設定 (30 日) を使用

ネットワークに関する検討事項

注記: Web Data Vault は、高遅延に影響されません。次の内容は、Windows ファイル共有 Data Vault にのみ適用されます。

Windows ファイル共有 Data Vault では、一般的に、Data Protector for PCs Agent から Data Vault に対する初期更新については、2 つの間のネットワーク遅延が 50 ms を超える場合は推奨されません。低速の WAN 接続で結ばれるホーム オフィスや遠く離れたオフィスでは、通常、ネットワーク遅延が 50 ms を超えます。初期更新は可能ですが、きわめて長い時間がかかります。

ご使用の環境に複数のサイトに点在するオフィスが含まれ、そのうちの一部のネットワーク遅延が 50ms を超える場合、Data Vaults を複数のサイトに設置してすべてのオフィスから少なくとも 1 つの Data Vault に 50ms 以下の遅延でアクセスできるようにすることを検討してください。

初期更新が完了すれば、ホームオフィスを含む、企業ネットワーク上の任意の位置から更新を行うことができます。初期更新以外の更新では更新されるデータのサイズが小さいので、通常、低速のネットワーク接続経由でも十分です。

初期更新を高遅延の接続経由で実行しなければならない状況では、更新の完了までに数日かかりますが、途中で中断しても問題ありません。Data Vault に Data Protector for PCs を再接続すると、停止された時点からただちに更新が再開されます。



ヒント: オフィス間の遅延についての情報がない場合は、1 つのサイトのコンピューターから ping コマンドを実行して別のサイトのコンピューターに ping を送信します。ping が成功すれば、遅延が報告されます。

5 マルチスレッド クリーンアップの設定

DPNECleanup のパフォーマンスにより、Data Vault 上のユーザー データのバックアップ量が制限されます。CPU とディスクを最適に使用して格納するデータ量を増やすため、再使用および拡張可能な方法で複数のスレッドを使用するように DPNECleanup を設定できます。

マルチスレッド クリーンアップでは、スケジューラーの引数である '*-s*' がデフォルトの引数である '*-e -f -u -p -d 1000*' を導き、これによって、マルチスレッド クリーンアップがデフォルトで実行され、Auto-Adjuster の実行前に 1 秒の遅延が発生します。これらのデフォルト設定を使用したくない場合、たとえば、マルチスレッドの実行を無効にする場合や調整する場合は、スケジューラーの呼び出しから '*s*' 引数を削除し、個々の CLI 引数を追加します。

注記:

ある状況下でマルチスレッド クリーンアップを無効化する必要があっても、Data Vault でのクリーンアップの呼び出しには、'*-e -f -u*' を引数として引き続き使用することを推奨します。

CLI からの DPNECleanup.exe の使用

引数 *-p* を DPNECleanup.exe に設定すると、クリーンアップが Parallel Engine を初期化して開始するため、マルチスレッドの実行が有効になります。Parallel Engine は、オプションのコマンドライン引数を提供します。DPNECleanup 実行ファイルはこれらの引数を取得し、Parallel Engine に渡すことができます。

-p が設定されない場合、DPNECleanup はシリアルモードで実行されます。このモードでは、Parallel Engine はまったく使用されません。

dpnecleanup

-a affinity

プロセッサ アフィニティを指定の数に設定します。この数は、スレッドが使用する CPU コアの設定ビットを反映しています。

-d delay

Auto-Adjuster が動作を開始する前の遅延時間をミリ秒単位で設定し、Parallel Engine が大量のスレッドを開始して一部のシステム利用率を作成する時間を提供します。

-s 引数は、デフォルトで、1000 ミリ秒または 1 秒の遅延を導きます。

-m maxCpuUsage

(*affinity* によって定義されたすべてのコア上の) CPU 最大使用率を、Auto-Adjuster が到達可能な *maxCpuUsage%* に設定します。*maxCpuUsage* は 1 ~ 100 の整数に設定する必要があります。デフォルト値は '0' で、制限がないことを意味します (CPU の完全利用)。

-o

一定のリソース。Auto-Adjuster が無効化され、Parallel Engine が並列スレッドの数を変更しないことを意味します。並列スレッドの数を調整するには、`-r` を使用します。引数 `-d`、`-m`、および `-q` は、`-o` を使用して実行されている場合は無視されます。

`-p`

マルチスレッド クリーンアップを有効にします。

`-q maxQueueLength`

Auto-Adjuster が到達可能なディスクの平均待ち行列長の最大値を設定します。値は浮動小数点数に設定する必要があります。デフォルト値は 2.0 です。

`-r resourceCount`

並列リソース (スレッド) の数を指定の数に設定します。デフォルト値とオプション `-o` を組み合わせると、システムでは $2^{\text{CPU 数}}$ の並列スレッドが実行されます。Auto-Adjuster が実行されている場合、指定された値は、スレッドに関する並列リソースの制限を意味します。最大値のデフォルト値が '0' の場合は、制限がないことを意味します。

`-z [Idle|BelowNormal|Normal|AboveNormal|High|Realtime]`

すべてのスレッドに対し、プロセスの優先度を設定します。デフォルト値は Normal です。

`-s`

サーバー クリーンアップ。中央定義やユーザー定義に関わらず、すべての Data Vault に対してクリーンアップを設定します。マルチスレッドの動作は、コマンドの実行時に引数 '`-e -f -u -p -d 1000`' で代替されます。

`-e`

エンタープライズ クリーンアップ。Policy Server のポリシーによって中央定義されたすべての Data Vault に対し、クリーンアップを設定します。

`-f`

迅速なクリーンアップ。通常、Agent のクリーンアップは、システムが休止状態の場合のみ実行されます。このオプションでは、クリーンアップをいつでも開始することができます。

`-u`

ユーザー定義のクリーンアップ。ユーザーが作成したローカル ポリシーによって定義されたすべてのローカル Data Vault に対し、クリーンアップを設定します。

6 Data Protector for PCs Agent のインストール

注記: ライセンスは、Agent のインストール時に、各 Agent に配布されます。

Data Protector for PCs Agent は、次の 2 通りの方法でインストールできます。

- 個別に各クライアントマシンにインストールする。「[個々のクライアントマシンへの Data Protector for PCs Agent のインストール](#)」(37 ページ)を参照してください。
- すべてのクライアントマシンにアクセス可能なファイルサーバーから組織全体に配置する。「[Data Protector for PCs Agent の組織全体への配置](#)」(38 ページ)を参照してください。

個々のクライアントマシンへの Data Protector for PCs Agent のインストール


要件

Data Protector for PCs Agent ソフトウェアは、Windows を実行するユーザーのデスクトップまたはノートブックにインストールできます。サポートされるプラットフォームについては、サポートマトリックスを参照してください。

「管理者」権限を持つアカウントにログインする必要があります。

インストール手順

1. Data Protector for PCs のインストール用 CD-ROM を挿入します。インストールウィザードが自動的に起動します。自動的に起動しない場合は、インストール CD-ROM のルートで setup.hta をダブルクリックして手動で実行します。
2. [Data Protector for PCs Agent ソフトウェアのインストール/更新] をクリックします。[開く] または [保存] ダイアログボックスが表示された場合は、[開く] (または [実行]) を選択します。
3. ユーザーコンピューターに Microsoft Windows Installer 3.1 以降がインストールされていない場合は、ウィザードによってそれをインストールするように指示されます。[Windows Installer の更新] ダイアログボックスが表示されたら、[OK] をクリックしてそれをインストールします。
4. ユーザーコンピューターに Microsoft .NET Framework 2.0 SP1 以降がインストールされていない場合は、ウィザードによってそれをインストールするように指示されます。[Microsoft .NET Framework 2.0 SP1 のインストール] ダイアログボックスが表示されたら、[OK] をクリックしてそれをインストールします。
5. ウィザードが自動的に Data Protector for PCs Agent をインストールします。画面上の指示に従います。インストール中に、Policy Server の詳細情報を入力するように求められます。

6. インストールと設定が完了したら、[終了] をクリックします。Open File Protection ポリシーが Policy Server に設定されている場合は、システムを再起動するように指示されます。
これで、Data Protector for PCs アイコンがシステム トレイに表示されます (保護の状況に応じて、次のいずれか: )。
7. 次の手順を実行して、Data Protector for PCs Agent が適切に動作することをテストします。
 - a. 「デスクトップ」で Word 文書や Excel スプレッドシートなどのテストファイルを選択するか作成します。いくつかの変更を加え、[保存] をクリックします。
 - b. Windows Explorer または [開く] ダイアログボックスで「デスクトップ」にあるテストファイルを右クリックします。メニューに 3 つの Data Protector for PCs エントリが表示されます ([ファイルを検索して回復...]、[バージョンのコピー]、および [XXX... でバージョンを開く])。
 - c. [XXX... でバージョンを開く] を選択すると、作成または編集した文書のタイムスタンプ付きのバージョンのリストが表示されます。いずれかのバージョンを選択すると、適切なアプリケーションで読み取り専用の文書として開かれます。この方法で、ユーザーは以前のバージョンの文書をローカルの Data Protector for PCs 保管領域から回復できます。
8. Data Protector for PCs で保護する他のユーザー デスクトップおよびラップトップに対してもステップ 1 ~ 8 を繰り返します。

Data Protector for PCs Agent の組織全体への配置

インストール CD-ROM に収録された Data Protector for PCs Agent Deployment Kit を使用して、最初に Data Protector for PCs Agent を組織全体に配置できます。

注記: ユーザーアカウント制御 (UAC) が有効になっている Vista PC では、Deployment Kit は使用できません。この問題を解決するには、UAC を無効にするかまたは Agent を対話形式でインストールします。

次に説明する手順では、最初に `CD-ROM:\Agent` にある Data Protector for PCs Agent Deployment Kit を、すべてのユーザーがアクセス可能なファイル サーバー上のディレクトリにコピーします。その後、`SetupConfig.exe` を使用して、そのディレクトリ内でパラメーターファイルを作成します。最後に、各ユーザーのコンピューターから共有ディレクトリにある `StartInstall.exe` を実行するためのメカニズムを確立します。たとえば、ログインスクリプトを使用できます。その後、Data Protector for PCs Policy Server Console から Agent 配置レポートを使用して配置を監視できます。

Kit の内容

Data Protector for PCs Deployment Kit には、次のコンポーネントが含まれています。
`SetupConfig.exe` 初期ファイルを作成および編集します。

StartInstall.exe	権限を持つユーザーとして Setup.exe を起動します。
Setup.exe	要件と DataProtectorNE.ini をインストールします。
DataProtectorNE.msi	Agent ソフトウェアをインストールするための Data Protector for PCs の Windows Installer パッケージ。
DataProtectorNE64.msi	64 ビットマシンに Agent ソフトウェアをインストールするための Data Protector for PCs の Windows Installer パッケージ。
DataProtectorNE*. *.mst	ローカライズされた Agent ソフトウェアをインストールするための Data Protector for PCs の Windows Installer パッケージ。
WindowsInstaller.exe	Windows Installer を更新します (.NET のインストールが必要)。
NetFx20SP1_x64.exe, NetFx20SP1_x86.exe	.NET Framework 2.0 SP1 をインストールします。
Setup.ini	Data Protector for PCs インストール セットアップパラメーター ファイル。このファイルは、SetupConfig.exe を使用して作成されます (以下のステップ 4 を参照)。

配置およびインストール手順

1. 配布 CD-ROM の Agent ディレクトリ内のファイルを、Data Protector for PCs Agent Deployment Kit の使用対象のすべてのユーザーがアクセスできるディレクトリにコピーします。これには、\\yourserver\DPNEDeploy などの共通の netlogon 共有のディレクトリを使用します。
2. 新たに作成したディレクトリに上記のファイルが含まれていることを確認します。それ以外のファイルはすべて削除します。
3. [DOS コマンド] ウィンドウを開き (cmd.exe)、cd を実行してステップ 1 で作成したディレクトリに移動します。
4. SetupConfig.exe を実行して、パラメーターファイル Setup.ini を作成または編集します。SetupConfig.exe の初回実行時には、すべてのパラメーターに値を入力する必要があります。その後は、パラメーターを変更するために、SetupConfig.exe を繰り返し実行できます。パラメーターを変更しない場合は、Enter キーを押すだけです。

必要なパラメーターは次のとおりです。

- **インストールパッケージへの UNC パス** – ステップ 1 でファイルがコピーされた共有ディレクトリへの完全なパス。\\yourserver\DPNEDeploy など。

- **Data Protector for PCs Policy Server** の名前。YOURSERVER のような NetBIOS 名でも、yourserver.yourcompany.com のような完全修飾ドメイン名でも構いません。
 - **ユーザー名** – Domain Admins グループのメンバーなど、Data Protector for PCs Agent Deployment Kit を使用するコンピューター上の管理者権限を持つユーザーのユーザー名。通常は、YOURCOMPANY\JerryAdmin のように、ドメインを含む完全修飾ユーザー名を指定します。
 - **パスワード** – ユーザー名に関連付けられたパスワード。確認のため 2 回入力する必要があります。
5. クライアントコンピューター上で、StartInstall.exe を実行します。たとえば、\\yourserver\DPNEDeploy\StartInstall と指定します。このプログラムは、Setup.ini で指定されたユーザー名とパスワードを使用して、Setup.exe を低い優先度で、バックグラウンドで実行します。これは、ログオンスクリプトの一部として実行できます。マシンアカウントが十分なネットワーク権限を持っていないため、それをスタートアップスクリプトに含めることはできない点に注意してください。
 6. Setup.exe は、クライアントコンピューターが Data Protector for PCs をサポートできるかどうかを判断します。サポートされる Windows プラットフォームについては、サポートマトリックスを参照してください。
 7. Setup.exe は、.NET Framework バージョン 2.0 SP1 がインストールされているかどうかを判断します。インストールされていない場合は、インストールします。その後、コンピューターの再起動が必要となることがあります。
 8. Setup.exe は、Data Protector for PCs がすでにインストールされているかどうかを判断します。インストールされていないか、バージョンが古い場合は、Data Protector for PCs をインストールします。

注記:

ステップ 4～7 でエラーが発生すると、Data Protector for PCs Policy Server と、ローカルコンピューターのアプリケーション イベント ログにメッセージが記録されます。

Data Protector for PCs Policy Server Console を使用して、Agent の配置の進行状況をチェックできます。

1. Data Protector for PCs Policy Server Console にログインします。
2. 左側のナビゲーション ペインにある [レポート] の下の [Agent 配置] を選択します。

最新の初期配置の概要が表示されます。次のことがわかります。

- 配置が正常に **終了**したマシンの数。
- **進行中**の配置の数。
- 配置に **失敗**した数。

3. [コンピューター数]列の数字をクリックすると、選択した配置状態のマシンのリストが表示されます。

各マシンの現在の状態が示されます。たとえば、特定のマシンで配置に失敗した場合、[情報]列に発生したエラーが示されます。NETBIOS名をクリックすると、そのマシンに関するさらに詳細な情報を表示できます。

7 Data Protector for PCs の更新

Data Protector for PCs のバージョン 6.x を 7.0 に更新する場合は、以下の手順に従ってください。

1. Policy Server を 7.0 に更新する。「[Policy Server の更新](#)」(42 ページ) を参照してください。
2. Web Data Vault Server をインストールする。「[Web Data Vault Server のインストール、設定、保守](#)」(18 ページ) の Web のインストールを参照してください。
3. Agent を 7.0 に更新する。
手動更新を使用して手動で更新することも、Agent 更新ポリシーを使用して「ユーザーの操作なしに」更新することもできます。詳しくは、「[Agent の更新](#)」(42 ページ) を参照してください。

Policy Server の更新

標準的なインストール手順に従うことで、既存の Data Protector for PCs Policy Server のインストールをより新しいバージョンに更新することができます。すべての既存の設定 (Data Vault 設定やライセンスなど) は、新しいバージョンでも利用できます。

Policy Server の更新:

1. Data Protector for PCs のインストール用 CD-ROM を挿入します。インストールウィザードが自動的に起動しない場合は、インストール CD-ROM のルートで `setup.hta` をダブルクリックして手動で実行します。
2. ウィザードの [Data Protector for PCs のインストール] ページで、[Policy Server のインストール] をクリックし、更新を開始します。
3. 画面上の指示に従います。
4. インストール手順によって既存の Policy Server のインストールが検出され、更新が行われます。
5. 画面上の指示に従います。
6. インストールが完了したら、[次へ] をクリックします。ここで、Data Protector for PCs Policy Server Console の実行を選択できます。

注記: クリーンアップソフトウェアが Policy Server にインストールされている場合は、クリーンアップソフトウェアも更新する必要があります。手動で、または Agent 更新ポリシーを使用して更新することができます。

Agent の更新

Data Protector for PCs Server のバージョンを更新する場合は、前のバージョンの Data Protector for PCs を使用する既存の Agent は、そのまま使用することができます。Manual Update を使用して手動で更新することも、Agent 更新ポリシーを使用して「ユーザーの操作なしに」更新することもできます。

注記: 更新後は、新しい Web Data Vault を使用できるように、すべての Agent を再起動する必要があります。システムトレイのバルーンメッセージや、PC 上の Data Protector for PCs の [状態] パネルの [概要] タブにも、再起動するように指示が表示されます。

Agent 更新ポリシーを使用した自動 Agent 更新

Agent は、Policy Server の Agent 更新ポリシーを使用して「ユーザーの操作なしに」更新することができます。インストールパッケージは、接続されたクライアントに自動的に配信され、完全に自動化された方法で更新が完了します。エンドユーザーの作業は中断されません。

1. Policy Server Console で、[Policies] -> [Agent Update Policy] を選択します。
2. Policy Server を更新したら、インストール手順によって新しいエージェント更新パッケージがアップロードされています。Policy Server Console では、この新しいバージョンはまだ選択されていません。
新しい Agent バージョンを選択して、使用可能にします。
3. 制限を調整することによって、1 分あたりに可能な最大更新数を調整することができます。
4. [Save Agent Update Policy] をクリックします。
5. これで、Agent は最新バージョンに自動的に更新されます。また、Cleanup Agent も最新バージョンに自動的に更新されます。

注記: Agent 配置レポートを使用して、Agent 更新の進行状況をチェックできます。

手動 Agent 更新

既存の Data Protector for PCs Agent は、標準的なインストール手順を実行することで、より新しいバージョンに更新することができます。

Agent をより新しいバージョンに更新する前に、Agent のバージョンが Data Protector for PCs Policy Server のバージョンに対応することを確認します。

1. Data Protector for PCs のインストール用 CD-ROM を挿入します。インストールウィザードが自動的に起動しない場合は、インストール CD-ROM のルートで setup.hta をダブルクリックして手動で実行します。
2. ウィザードの [Data Protector for PCs のインストール] ページで、[Agent のインストール] をクリックし、更新を開始します。
3. 画面上の指示に従います。
4. インストール手順によって既存の Agent のインストールが検出され、更新が行われます。
5. 画面上の指示に従います。

8 Data Protector for PCs のサポートへの連絡方法

Data Protector for PCs には、1 年間のメンテナンス保証が付いています。次のサービスを利用できます。

- 電話サポート。サポート技術者に問い合わせることができます。
- Data Protector for PCs Server と Data Protector for PCs Agent ソフトウェアの更新。最新バージョンおよび CD-ROM イメージは、Data Protector Web サイトからダウンロードできます。 <http://www.hp.com/go/dataprotector> (英語) を参照してください。

用語集

Active Directory	(Windows 固有の用語) Windows ネットワークのディレクトリサービス。ネットワーク上のリソースに関する情報が含まれ、それらのリソースをユーザーおよびアプリケーションがアクセスできるようにします。ディレクトリサービスは、リソースの存在する物理システムに関係なく、それらのリソースの命名、記述、検出、アクセス、管理を行う一貫性のある方法を提供します。
Agent	各ユーザーのデスクトップ/ラップトップで動作する Data Protector for PCs ソフトウェア。Agent は TCP ポート 80 から Web サービス (SOAP および XML) を介して Policy Server と通信を行います。
Continuous File Protection	Continuous File Protection は、Data Protector for PCs の Continuous Data Protection 方式で、ファイルが保存されるたびに変更内容を自動的に保存します。これは、ユーザーによって保存されるデータ ファイルに適しています (逆に、データベースや Outlook ファイルなどの常に開かれているファイルには適していません)。各 Continuous File Protection ポリシーは、何らかの関係のあるファイルのグループを保護対象とします。Data Protector for PCs には、Office 文書やピクチャなどのよく使われるタイプのファイル用のポリシーが事前構成されています。これらのファイル保護ポリシーを編集することも、自分独自のポリシーを作成することもできます。ポリシーは、保護されているファイルの以前のバージョンをどれだけの期間保持するかも指定します。
Data Vault	Data Vault には、次の 2 つのタイプがあります。 <ul style="list-style-type: none">• Web Data Vault。HTTPS プロトコルを使用してクライアント PC と Data Vault 間のデータ転送に最適なセキュリティを提供し、高遅延環境のスループットを向上させるため、推奨されます。• Windows ファイル共有 Data Vault。これは、Data Vault ポリシーに従ってファイルを保管するファイルサーバー上の共有フォルダーです。ファイルサーバーは、Windows ファイル共有プロトコル (CIFS/SMB) をサポートしている必要があります。待機時間が長いネットワーク環境での使用には推奨されません。 いずれのタイプの Data Vault のデータ構造も同じなので、既存の Windows ファイル共有 Data Vault は Web Data Vault に変換することができます。 ユーザーが属するグループや組織単位に基づいて、1 つ以上の Data Vault ポリシーをユーザーに割り当てることができます。
Local Repository	Local Repository は、保護ファイルやファイル変更分の保管に使用される、Agent コンピューター上の安全な保管場所で、通常はシステム ハード ディスク ドライブ上にあります。これは、隠しシステム ディレクトリです。ユーザーは、以前のバージョンをデスクトップや Windows エクスプローラーから、または [開く] ダイアログボックスでファイルを右クリックすることですばやく回復できます。Continuous File Protection ポリシーで保護されたファイルは、保持期間を満たしている間は、ローカル コンピューターの隠しディレクトリに保管されます。Open File Protection ポリシーで保護されたファイルは、それらが Data Vault にコピーされるまでの間のみローカルの Version Store に保管されます。Local Repository の通常のパスは、 <code>c:\{DPNE}</code> になります。
Open File Protection	Open File Protection は、定期的にファイルレベルのスナップショットを取得することで、Outlook 個人用フォルダーや多数のデータベース ファイルなどの常に開かれているファイルをバックアップします。これは、「近似」継続的データ保護と呼ばれることもあります。Open File Protection ポリシーは、常時使用ファイルの保護を定義します。包含ルールおよび除外ルールのセットで定義されます。たとえば、「『.pst』で終わる」という包含ルールを指定し、「Outlook 個人用フォルダー」という名前のポリシーを定義し、Outlook .pst ファイルに適用することが可

能です。アーカイブした.pst ファイルを除外したいときは、「『archive』を含む」という除外ルールを作成します。保護されているファイルの以前のバージョンをどれだけの期間保持するかも指定します。Open File Protection ポリシーは、すべてのユーザーに適用されます。

Policy Server

Policy Server は、Data Protector for PCs ポリシーの集中管理を行います。また、Agent の状況を収集し、それらの配置と処理のレポートを出力します。

クリーンアップポリシー

ファイル保護ポリシーで設定した保持期間は、定期的に行われるクリーンアップタスクにより処理が行われます。実行頻度は、クリーンアップ ポリシーに定義されています。デフォルトでは、ユーザーの Local Repository は 1 時間ごとにクリーンアップされ、ローカルで定義された Data Vault は 1 日に 1 回クリーンアップされます。中央定義の Windows ファイル共有 Data Vault は、Data Vault ポリシーに定義されるコンピューターによってクリーンアップされ、Web Data Vaults は、Data Vault Server でローカルに実行されるクリーンアップによってクリーンアップされます。クリーンアップポリシーはすべてのユーザーに適用されます。

コピー ポリシー

コピーポリシーは、次のことを定義します。

- Data Vault に同時にファイルをコピーできる Agent の数。
- 定期的な更新のスケジュール。ユーザーに関連すると予想されるファイルがすべて Data Vault に存在することを確認し、存在しない場合は、不足しているファイルをコピーします。これにより、すべてのユーザーファイルが Data Vault に適切にコピーされていることをより強力に保証します。
- **初期更新**を実行する必要があるかどうか。通常の Data Protector for PCs 操作の間は、ユーザーが Data Protector for PCs 継続的保護ファイルを変更するたびに、変更に関する情報しか Data Vault にコピーされないため、初期更新が必要です。

Data Protector for PCs をインストールしたばかりの場合は、ユーザーの保護ファイルすべての初期更新を作成するためのコピー ポリシーを設定する必要があります。

コンソール

ブラウザーベースのコンソールは、Data Protector for PCs ポリシーを集中的に定義する場所です。Administrator のグループのメンバーである必要があります。

バックアップ ユーザー

ファイルのバックアップやリストアなどのエンドユーザー操作を実行する Web Data Vault Server 上のユーザー。

ポリシー

ポリシーとは、Policy Server で集中的に定義され、各デスクトップ/ラップトップ/ノートブックで Agent によって実行されるルールセットです。

ユーザー制御ポリシー

このポリシーは、デスクトップ/ラップトップ/ノートブックで動作している Agent ソフトウェアをユーザーが自分でどこまで制御できるかを決定します。Agent を管理することで、ユーザーからポリシーを完全に隠したり、ポリシーを見せるけれども編集できなくしたり、ユーザー自身がポリシーを追加できるようにしたりすることができます。主要な各 Data Protector for PCs ポリシーに個別に制御レベルを設定することができます。ユーザー制御ポリシーは、すべてのユーザーに適用されます。

管理者ユーザー

Data Vault の作成と削除、クライアントのバックアップ データの移行などの管理タスクを行う Web Data Vault Server 上のユーザー。

初期更新

Data Protector for PCs は、ユーザーが変更内容を保存することによってファイルを継続的に保護します。ユーザーが新しい Data Vault を作成するたびに、Data Protector for PCs は、保管領域に対してすべてのユーザーの保護ファイルの初期更新を行う必要があります。ユーザーは、初期更新をすぐに行うか、バックグラウンドで行うかを選択することができます。

保護されているファイル

保護ファイルとは、Data Protector for PCs によって自動バックアップされるファイルのことです。保護されるファイルタイプは、Continuous File Protection ポリシーおよび Open File Protection ポリシーで定義されます。

索引

記号

- .NET Framework, 15, 37
- 暗号化パスワード, 23, 31
- 暗号化パスワードのインポート, 31
- 暗号化パスワードのエクスポート, 23, 31
- 暗号化パスワードの入力, 31
- 概要, 8
- 管理者ユーザー
 - 作成, 19
 - 変更, 21
- 技術サポート, 6
- 更新
 - Agent, 42
 - Policy Server, 42
- 作成
 - バックアップ ユーザー, 19
 - 管理者ユーザー, 19
- 資料
 - フィードバックの提供, 7
- 自己署名証明書, 10, 18
- 証明書, 10, 18
 - 交換, 11, 21
- 証明書の交換, 11
- 新しい Data Vault へのデータの移行, 20
- 設定
 - Active Directory アクセス, 28
 - Agent 更新ポリシー, 30
 - Continuous File Protection ポリシー, 27
 - Data Vault ポリシー, 24
 - Open File Protection ポリシー, 27
 - Web Data Vault Server, 18
 - クリーンアップポリシー, 29
 - コピー ポリシー, 25
 - ファイル保護ポリシー, 26
 - マルチスレッド クリーンアップ, 35
 - ユーザー制御ポリシー, 30
 - レポート データ保持設定, 30
 - 初回インストール時のポリシー, 24
- 読者, 5
- 認証局, 11
- 配置
 - 手順, 39
 - 進捗状況の確認, 40
- 表記法
 - 文書, 5
- 文書
 - 表記法, 5
- 変更
 - バックアップ ユーザー, 21
 - 管理者ユーザー, 21
- 要件, 12

A

- Active Directory
 - アクセス, 28
 - グループの Data Vault との関連付け, 28
- Active Directory へのアクセス, 28
- Agent, 8
 - 更新, 42
 - 要件, 13
- Agent Deployment Kit の内容, 38
- Agent ソフトウェア
 - インストール, 37
 - 組織全体への配置, 38
- Agent ソフトウェアの配置, 38
 - 手順, 39
 - 進捗状況の確認, 40
- Agent 更新ポリシー, 30
- Agent 配置レポート, 43
- Agents
 - サポートできる数, 31
- ASP.NET, 15

C

- CLI コマンド
 - DPNCCleanup, 35
 - DvConfig, 21
- Continuous File Protection ポリシー, 26

D

- Data Protector for PCs
 - Agent のインストール, 37
 - アーキテクチャー, 8
 - サポートの取得, 44
 - 概要, 8
- Data Protector for PCs の評価, 23, 30
- Data Vault
 - Active Directory グループの関連付け, 28
 - Web, 9
 - Windows ファイル共有, 9
 - サーバーに関する推奨事項, 32
 - データの移行, 20
 - 要件, 25
- Data Vault ポリシー, 24
- DPNCCleanup, 35
- DvConfig, 21

E

- EFS 暗号化ファイル, 27

F

- FQDN, 18

H

HP
技術サポート, 6
HTTPS プロトコル, 9

I

IIS, 15

M

Microsoft SharePoint とのインストール, 17

O

Open File Protection ポリシー, 27

P

Policy Server, 8
インストール, 14
データベースの要件, 13
更新, 42
推奨事項, 33
要件, 12
Policy Server Console
ブラウザー設定, 17
実行, 16
Policy Server Console 用のブラウザー設定, 17
Policy Server Console、実行, 24

S

SharePoint
Policy Server のインストール, 17
SQL Server
インストール, 16
SQL データベース
要件, 13
SSL の変更, 21
SSL ポート
入力, 18
変更, 21
Subscriber's Choice、HP, 6

W

Web Data Vault, 9
へのデータの移行, 20
削除, 19
保守, 19
Web Data Vault Server, 8
インストール, 18
設定, 18
要件, 13
Web Data Vault の削除, 19
Web Data Vault の保守, 19
Web サイト
HP, 6
HP Subscriber's Choice for Business, 6

Windows Installer, 15, 37
Windows ファイル共有 Data Vault
からのデータの移行, 20

い

インストール
Agent, 37
Policy Server, 14
SQL Server, 16
Web Data Vault Server, 18
クリーンアップ ソフトウェア, 18
概要, 11
インターネット インフォメーション サービス, 15
インポートされた証明書, 10

く

クリーンアップ ソフトウェア, 18
クリーンアップポリシー, 29

こ

コピー ポリシー, 25
コンソール
ブラウザー設定, 17
実行, 16
コンソール、実行, 24

さ

サーバー
ファイル, 8
ポリシー, 8
サイズ決定に関する検討事項, 32
Data Vault, 32
Policy Server, 33
ネットワーク, 34
サポート, 44
サポート マトリックス, 8

て

データベースの要件, 13
デスクトップ、要件, 13

ね

ネットワーク、サイズ決定に関する検討事項, 34

の

ノートブック、要件, 13

は

パスワード, 23, 31
バックアップ ユーザー
作成, 19
変更, 21

ふ

- ファイル サーバー, 8
- ファイル共有 Data Vault, 9
- ファイル保護ポリシー, 26
 - オープン, 27
 - 継続的, 27

へ

- ヘルプ
 - 入手, 6

ほ

- ポリシー
 - Agent の更新, 30
 - Continuous File Protection, 26
 - Data Vault, 25
 - Open File Protection, 27
 - クリーンアップ, 29
 - コピー, 25
 - ファイル保護, 26
 - ユーザ制御, 30
 - レポート データ保持設定, 30
 - 初回インストール時の設定, 24
 - 配布, 8

ま

- マルチスレッド クリーンアップ, 35

ゆ

- ユーザー コンピューター、要件, 13
- ユーザー制御ポリシー, 30

ら

- ライセンス, 23, 30
 - 移動, 31
 - 入手可能, 23
- ライセンス キー
 - 入力, 30
- ライセンス キーの入力, 30
- ライセンスの移動, 31

れ

- レポート データ保持設定, 30