Veritas Storage Foundation and High Availability Solutions™ クイックスタートガイド Symantec Product Authentication Service

Windows 2000, Windows Server 2003

5.0

11416137

symantec™

Veritas Storage Foundation and HA Solutions クイックスタートガイド Symantec Product Authentication Service

Storage Foundation for Windows HA 5.0

Symantec Corporation
www.symantec.com
Printed in the Singapore

サードパーティ（第三者）製ソフトウェアの権利に関する通知

本製品には、特定のサードパーティ製ソフトウェアが配布、組み込み、または同梱されている場合があります。また、本製品のインストールおよび使用にともない、サードパーティ製ソフトウェアの使用を推奨する場合があります。同サードパーティ製ソフトウェアのライセンスは、著作権の保有者により別途付与されます。サードパーティのソフトウェアの使用に必要なライセンスおよび著作権に関する情報については、本製品リリースノートのサードパーティに関する章を参照してください。

ライセンスと登録

Storage Foundation for Windows および Storage Foundation HA for Windows はライセンスが必要な製品です。ライセンスのインストールについては、『Veritas Storage Foundation and High Availability Solutions インストールおよびアップグレードガイド Windows 2000, Windows Server 2003』を参照してください。

テクニカルサポート

製品のサポートを受けるには、http://entsupport.symantec.com ページへアクセスし「Phone Support」または「E-mail Support」をクリックします。このページから TechNote、Software Alerts、ソフトウェアのダウンロード、ハードウェア互換性リスト、VERITAS Email Notifications サービスなどにアクセスすることもできます。「Knowledge Base Search」機能を使用し、製品ドキュメントのリリースなどの製品情報へアクセスすることができます。

1

Symantec Product Authentication Services の基本操作

このスタートガイドでは、次のトピックを説明します。

- Symantec Product Authentication Service について
- ベストプラクティス
- SFW HA 環境での Symantec Product Authentication Service の計画
- ルートブローカーのインストール
- 既存の Symantec Product Authentication Service ルートブローカーのアップグレード
- セキュリティ保護されていない 4.x SFW HA クラスタからセキュリティ保護された 5.0 SFW HA クラスタへのアップグレード
- Symantec Product Authentication Service のバックアップ
- 用語集

Symantec Product Authentication Service について

Symantec Product Authentication Service を使用することにより、セキュリティ管理者は認証を設定し、Symantec アプリケーションに対してシングルサインオンサービスを提供できます。この場合、1 つの Symantec アプリケーションに 1 回だけログオンすれば、他のアプリケーションは 1 回目のログオンで取得した信用証明を使用できます。

Symantec Product Authentication Service（以前の VxSS（Veritas Security Services））は、認証と SSL にデジタル証明書を使用し、パブリックネットワーク上での通信を暗号化することで、クラスタノードとクライアント（Java コンソールなど）間の通信の安全を確保します。

1 つのルートブローカーをデータセンターに設定し、必要に応じて認証ブローカーを SFW HA クラスタの各ノードなどに設定することをお勧めします。

- ルートブローカー
  ルートブローカーは主要な登録局と認証局として機能します。ルートブローカーは自己署名した証明書を持ち、他のブローカーを認証できます。ルートブローカーは、認証ブローカーの初期作成時にのみ使用されます。
- 認証ブローカー
  認証ブローカーは、中間の登録局と認証局として機能します。認証ブローカーは、ルートにより署名された証明書を保持します。SFW HA クラスタの各ノードは、認証ブローカーとして機能します。

各認証ブローカーは、プライベートドメインリポジトリを持ち、この認証ブローカーを使用するすべての Symantec アプリケーションのサービスやユーザーを格納します。

VCS クラスタ設定ウィザードを使用して、クラスタの認証サービスを設定できます。

認証サービスについて詳しくは、『Symantec Product Authentication Service 管理者ガイド』を参照してください。

ベストプラクティス

Symantec Product Authentication Service は様々な方法で導入できます。ただし、ベストプラクティスを使用することで、セキュリティテクノロジに要する継続的な管理コストを最小限に抑えることができます。

ガイドラインを次に示します。

- ルートブローカーの数を 1 つに制限する
- プライベートドメインリポジトリのバックアップを作成し、安全な場所でそのバックアップファイルを保持する

- プライベートドメインリポジトリのアカウントを Symantec サービスでしか使えないように制限する

ルートブローカーの数を 1 つに制限する

単一のルートブローカーを使用することにより、セキュリティの分散を防ぎ、すべての シマンテック社製品を同一のセキュリティドメインに移行できます。このような統合整理は、シングルサインオンと、様々な製品間のセキュアな通信を円滑にする働きがあります。

ルートブローカーは、信頼関係にある階層内のすべてのホストについての信頼関係を保持します。2 つ以上のルートブローカーを使用している場合、それぞれのルートブローカー間で信頼関係を構築する必要があります。複数のルートブローカー間の信頼関係を維持するには、費用と時間がかかります。

ルートブローカーの数を極力少なくすることは、セキュリティの観点から見ても利点があります。ルートブローカーが危殆化した後の環境の修復は、認証ブローカーのみが危殆化した場合に比べてさらに困難なものとなります。ルートブローカーが危殆化した場合、その影響範囲は、セキュリティドメイン全体にわたります。ルートブローカーの数を少数に留めておくことで、セキュリティドメイン全体が危殆化するリスクを極力抑えられます。

Symantec Product Authentication Service のバックアップ作成の必要性

ルートブローカーと認証ブローカーのプライベートドメインリポジトリには、必要不可欠なデータが格納されます。プライベートドメインリポジトリのバックアップは、その他の重要なデータのバックアップと同じ頻度で実行してください。安全性を考え、コピーはオフラインで管理します。

「Symantec Product Authentication Service のバックアップ」を参照してください。

プライベートドメインリポジトリのアカウントの使用を Symantec サービスのみに制限する

プライベートドメインリポジトリは、Symantec プログラム間で相互認証を必要とする場合に使用されることを想定しています。プライベートドメインリポジトリでは、サイトのヒューマンユーザー認証ドメイン（Windows 2000 の Active Directory など）内で Symantec プログラムの ID 情報を定義または格納する必要がありません。

SFW HA 環境での Symantec Product Authentication Service の計画

Symantec Product Authentication Service は、SFW HA とともに自動的にインストールされます。VCS 設定ウィザードを使用してクラスタを設定する場合、クラスタ内部またはクラスタ外部のルートブローカーを特定して指定できます。

SFW HA のインストールメディアの Product Authentication Service ディレクトリ内にある実行可能ファイルを使用することで、クラスタ外部に Symantec Product Authentication Service ルートブローカーをインストールして設定できます。

次のシナリオを確認し、使用する環境に応じて所定の処理を実行してください。

メモ : SFW HA 5.0 は、クラスタ環境でのルートブローカーの高可用化をサポートしていません。

メモ : 認証ブローカーはスタンドアロン SFW システムには不要であるため、Symantec Product Authentication Service は SFW HA 環境でのみ使用されます。

SFW HA のインストールとクラスタの設定について詳しくは、『Veritas Storage Foundation and High Availability Solutions インストールおよびアップグレードガイド』を参照してください。

シナリオ 1: 1 つ以上のクラスタで、クラスタ外部に 1 つのルートブローカーを設定

環境 : クラスタ外部に設定されたルートブローカーを持つ複数のクラスタ

説明 : ルートブローカーはクラスタ外部の個別のシステムにインストールされており、すべてのクラスタノードは認証ブローカーとして機能します。この Symantec Product Authentication Service では、次の設定をお勧めします。

ユーザーによる操作 :

1. SFW HA のインストールメディアから、Symantec Product Authentication Service 実行可能ファイルを実行し、指定したシステムに Symantec Product Authentication Service のインストールと設定を行って、ルートブローカーを作成します。
   7 ページの「クラスタ外部の専用システムへのルートブローカーのインストール」を参照してください。
2. クラスタ内のノードとなるすべてのシステムに SFW HA をインストールします。

3 VCS 設定ウィザードを使用してクラスタを設定します（スタートメニューの［すべてのプログラム］、［Symantec］、［Veritas Cluster Server］、［設定ウィザード］、［クラスタ設定ウィザード］の順にクリック）。［セキュリティサービスオプションの設定］パネルで、手順 1 で作成したルートブローカーを指定します。クラスタのノードは認証ブローカーとして自動的に設定されます。

メモ : ルートブローカーが必要なのは、新しいクラスタまたは新しいノードをクラスタに追加するときのみです。

シナリオ 2: 単一クラスタで、クラスタ内部に 1 つのルートブローカーを設定

環境 : 単一クラスタ

説明 : クラスタ内部のシステムをルートブローカーとして使用するものと見なします。ルートとして使用されるシステムも、システムクラスタ設定時にはルートブローカーと認証ブローカーになるため、クラスタ内のすべてのシステムが認証ブローカーになります。

メモ : 1 番目のシナリオのように、ルートブローカーを個別にインストールして設定する必要はありません。VCS 設定ウィザードを使用すると、ルートブローカーと認証ブローカーを自動で設定できます。

ユーザーによる操作 :

1 クラスタの設定中にルートブローカーがインストールされるクラスタ内のノードを特定します。

2 クラスタ内のノードとなるすべてのシステムに SFW HA をインストールします

3 VCS 設定ウィザードを実行してルートブローカーの設定を行います。（スタートメニューの［すべてのプログラム］、［Symantec］、［Veritas Cluster Server］、［設定ウィザード］、［クラスタ設定ウィザード］の順にクリック）。［VxSS セキュリティサービスの設定］パネルで、手順 1 で特定したルートブローカーを指定します。クラスタのノードは認証ブローカーとして自動的に設定されます。

シナリオ 3: マルチクラスタで、クラスタ内部に 1 つのルートブローカーを設定

環境 : 同じドメイン内に 2 つ以上のクラスタがある

説明 : 1 つのクラスタ内のノードにルートブローカーを設定します。追加クラスタの設定処理を行うときに、そのルートブローカーを指定します。追加クラスタ内のノードは、認証ブローカーとして機能します。

ユーザーによる操作 :

1. クラスタの設定中にルートブローカーが作成されるシステムを特定します。
2. SFW HA をすべてのシステムにインストールします。
3. VCS 設定ウィザードを実行して 1 番目のクラスタの設定を行います。設定処理中にルートブローカーのホストとなるシステムを指定します。
4. VCS 設定ウィザードを実行して追加のクラスタの設定を行い、1 番目のクラスタのルートブローカーを指定します。追加クラスタ内のノードは、認証ブローカーとして機能します。

注意事項 : VCS 設定ウィザードでは、Windows システムに存在するルートブローカーのみを検出できます。

シナリオ 4: 既存のルートブローカーで、SFW HA を使用

環境 : 別の Symantec 製品用に設定されたルートブローカー

説明 : Windows オペレーティングシステムで動作する既存のルートブローカーを使用するように、SFW HA を設定します。

ユーザーによる操作 :

1. 別の Symantec 製品でルートブローカーとしてすでに設定されているシステムを識別します。
2. 新しいクラスタのノードとなるシステムに SFW HA をインストールします。
3. VCS 設定ウィザードを使ってクラスタを設定します（スタートメニューの［すべてのプログラム］、［Symantec］、［Veritas Cluster Server］、［設定ウィザード］、［クラスタ設定ウィザード］の順にクリック）。
   ［VxSS セキュリティサービスの設定］パネルで、手順 1 で特定したルートブローカーを指定します。クラスタのノードは認証ブローカーとして自動的に設定されます。

シナリオ 5: マルチクラスタで、クラスタごとに 1 つのルートブローカーを設定

メモ : このシナリオはお勧めできません。

環境 : マルチクラスタと複数のルートブローカー

説明 : クラスタの設定中にルートブローカーを設定します。

ユーザーによる操作 :

1 SFW HA をインストールします。

2 VCS 設定ウィザードを使用してクラスタを設定する際に、各クラスタのルートブローカーの設定を行います。

注意事項 : 複数のルートブローカーを使用すると、Symantec Product Authentication Service のフットプリントが増加するので、この方法はお勧めしません。

ルートブローカーのインストール

次の手順で、ユーザーの構成にルートブローカーをインストールします。

クラスタ外部の専用システムへのルートブローカーのインストール

1 番目のシナリオで説明したように、クラスタ外部のセキュリティドメイン内にルートブローカーをインストールするには、Symantec Product Authentication のインストールウィザードを実行する必要があります。

ただし、Symantec Product Authentication Service をインストールする前に、Java Runtime Environment（JRE）バージョン 1.5.02 をインストールする必要があります。JRE パッケージはインストールメディアに含まれています。すでに JRE 1.5 をインストールしている場合、再インストールする必要はありません。

JRE をインストールする方法

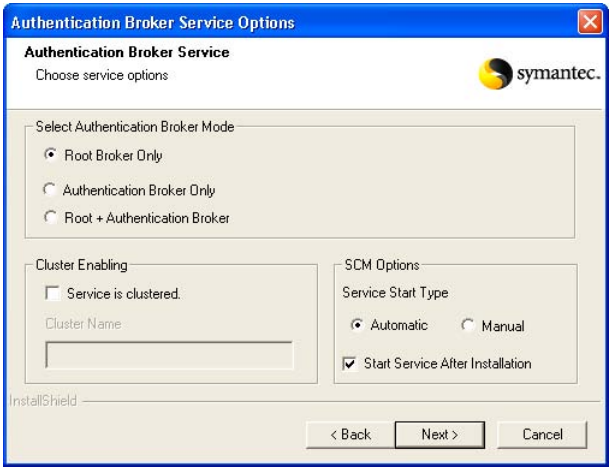
1 インストールメディアのルートディレクトリから、Symantec_Product_Authentication_Service に移動します。

2 VRTSjre.msi をダブルクリックします。

3 Windows インストーラが表示されたら、画面の指示に従って JRE をインストールします。

インストールメディアからルートブローカーをインストールする方法

1. インストールメディアのルートディレクトリから、Symantec_Product_Authentication_Service に移動します。
2. VxSSVRTSatSetup.exe をダブルクリックします。
3. ［Welcome］画面を確認し、［Next］をクリックします。
4. ［Setup Type］ウィンドウで、［Complete］をクリックし、クライアントとサーバーの両方のコンポーネントをインストールします。コンポーネントをデフォルトに指定されたディレクトリ以外にインストールする場合は、［Browse］をクリックします。
5. ［Authentication Broker Service］画面で、次のオプションを選択します。



   - ［Root broker only］
   - ルートブローカーのクラスタ化がサポートされていないため、［Service is clustered］チェックボックスをオンにしないでください。
   - ［Service Start Type］には、［Automatic］を選択します（デフォルトでは［Manual］が選択されています）。
   - ［Start Service After Installation］チェックボックスを選択します。
6. 処理が終了したら、［Next］をクリックします。
7. ［Summary］画面で、選択した設定を確認し、［Next］を選択してインストールを開始します。
8. ［Setup Status］画面にインストールの進行状況が表示されます。

9 ルートブローカーのパスワードをパスワード確認画面のテキストボックスに入力し、［Next］をクリックします。
［Root Broker Only］モードでのインストールを選択しているため、認証ブローカーパスワード用のテキストボックスは表示されません。

10 ［InstallShield Wizard Complete］画面が表示されたら、［Finish］をクリックしてウィザードを終了します。

サービス開始の確認

次の操作で、Windows の［管理ツール］の［サービス］ウィンドウを開くと、Symantec Product Authentication Service が開始したことを確認できます。

スタートメニューで、［設定］、［コントロールパネル］、［管理ツール］、［サービス］の順に選択します。

サービスリストで［Symantec Product Authentication Service］を探し、状態が［開始］になっていることを確認します。

既存の Symantec Product Authentication Service ルートブローカーのアップグレード

インストールメディアを使用して、以前のバージョンの Symantec Product Authentication Service ルートブローカーをアップグレードできます。

メモ : 以前のバージョンの Symantec Product Authentication Service を使用している既存のルートブローカーがある場合は、そのルートブローカーを引き続き使用できます。ルートブローカーのアップグレードはオプションです。

既存のルートブローカーをアップグレードする方法

1 インストールメディアの Symantec Product Authentication Service をクリックするか、または VxSSVRTSatSetup.exe をダブルクリックします。
Windows インストーラの進行状況メーターが表示されます。

2 Symantec Product Authentication Service をアップグレードするかどうか、確認を求める画面が表示されます。アップグレードを続行するには［Yes］を、インストール処理を停止するには［No］をクリックします。

3 ［Welcome］画面を確認し、［Next］をクリックします。

4 ルートブローカーの新しいパスワードを入力します。既存ルートブローカーの古いパスワードを入力しないでください。処理が終了したら、［Next］をクリックします。

5 ［Setup Status］画面にインストールの進行状況が表示されます。

6 ［InstallShield Wizard Complete］画面が表示されたら、［Finish］をクリックしてウィザードを終了します。

セキュリティ保護されていない 4.x SFW HA クラスタからセキュリティ保護された 5.0 SFW HA クラスタへのアップグレード

製品インストーラを使用して、セキュリティ保護されていない 4.x SFW HA クラスタを、セキュリティ保護されていない 5.0 SFW HA クラスタにアップグレードします。セキュリティ保護された通信で Symantec Product Authentication Service を設定する場合は、VCS 設定ウィザードを実行します。［クラスタオペレーション］、［既存のクラスタの編集］、［再設定］、［VxSS セキュリティサービスの設定］の各オプションが選択されていることを確認してください。

詳しくは、『Veritas Cluster Server 5.0 管理者ガイド』を参照してください。

Symantec Product Authentication Service のバックアップ

ルートブローカーと認証ブローカーのプライベートドメインリポジトリには、重要なデータが格納されています。プライベートドメインリポジトリのバックアップは、その他の重要なデータのバックアップと同じ頻度で実行してください。安全性を考え、コピーはオフラインで管理します。

vssat showbackuplist コマンド

`vssat showbackuplist` コマンドを使用すると、バックアップする必要のあるデータが一覧表示されるため、後から必要に応じてブローカーをリストアできます。

注意 : `vssat showbackuplist` コマンドを実行しても、ファイルのリストアは行われません。

`vssat showbackuplist` コマンドでは、次の情報が一覧表示されます。

- バックアップする必要のある重要なブローカーファイル
- バックアップファイルのリストア名（名前がもとのファイルと異なる場合）
- バックアップする必要のあるレジストリキー

Windows でブローカーデータをバックアップする方法

1 コマンドラインから、次の Windows ディレクトリにある vssat showbackuplist コマンドを検索します。
C:¥program files¥veritas¥security¥authentication¥bin

2 次の Windows レジストリキーから、認証の実際のインストールパスを取得します。
HKLM¥Software¥Veritas¥Security¥Authentication¥InstallDir

3 次の構文で改行を入れずにコマンドを実行します。
vssat showbackuplist [--filename < 一覧用のファイル名 >]
vssat showbackuplist コマンドは、重要なファイルのバックアップや一覧表示に使用する管理ツールです。このコマンドでは、ファイルはリストアされません。

4 vssat showbackuplist の出力を確認します。
各ディレクトリまたはファイルは別々の行に表示されます。*--filename* 引数を指定すると、結果はファイルに出力されます。たとえば、list.txt というファイルに一覧を取得するには、次のコマンドを実行します。
vssat showbackuplist *--filename list.txt*
ファイルを要求しない場合、出力は次の標準出力に表示されます。

B| FileOrDirToBeBackedup
R| RestoreAboveFileOrDirToFileOrDir
K| RegistryKey

たとえば、Windows の場合、出力は次のように表示されます。

```
C:¥Program Files¥Veritas¥Security¥Authentication¥bin>vssat
showbackuplist
B|C:¥Program Files¥Veritas¥Security¥Authentication¥
systemprofile¥VRTSatlocal.conf
B|C:¥Program Files¥Veritas¥Security¥Authentication¥
systemprofile¥certstore
B|C:¥Program Files¥Veritas¥Security¥Authentication¥
systemprofile¥RBAuthSource
B|C:¥Program Files¥Veritas¥Security¥Authentication¥
systemprofile¥ABAuthSource
K|HKEY_LOCAL_MACHINE¥SOFTWARE¥Veritas¥Security¥
Authentication
Quiescing ...
Snapshot Directory :C:¥Program
Files¥Veritas¥Security¥Authentication¥Snapshot
```

5 ブローカーの重要なデータをバックアップした後で、次のコマンドを実行して追加のバックアップを実行します。

```
% reg export
HKLM¥SOFTWARE¥Veritas¥Security¥Authentication
<snapshotdir>¥AtKey.reg
```

出力は次のように表示されます。

```
C:¥>reg export HKLM¥SOFTWARE¥Veritas¥Security¥Authentication
"c:¥Program
Files¥Veritas¥Security¥Authentication¥Snapshot¥AtKey.reg"
The operation completed successfully.
```

バックアップのリストア

次の手順では、ブローカーのデータと他の重要なデータを Windows にリストアする方法を説明します。

Windows でバックアップをリストアする方法

1. コマンドラインで次のように入力して、ブローカーをシャットダウンします。

   ```
   net stop vrtsat
   ```

2. 次のコマンドを入力してバックアップ先を確認します。showbackuplist コマンドでも、バックアップ先を表示できます。

   ```
   % vssregctl -l -q
   -b"Security¥Authentication¥Authentication Broker"
   -kSnapShotDirectory
   ```

3. 次のコマンドを実行してバックアップファイルをリストアします。

   ```
   % reg import <snapshortdir>AtKey.reg
   % “xcopy /E <snapshotdir> <installdir>
   ```

   reg import コマンドの出力例を次に示します。

   ```
   C:¥Program Files¥Veritas¥Security¥Authentication¥Snapshot>reg
   import AtKey.reg
   The operation completed successfully.
   ```

   xcopy コマンドの出力例を次に示します。

   ```
   C:¥Program Files¥Veritas¥Security¥Authentication>xcopy
   /ESnapshot
   Snapshot¥systemprofile¥ABAuthSource
   Snapshot¥systemprofile¥RBAuthSource
   Snapshot¥systemprofile¥VRTSatlocal.conf
   Snapshot¥systemprofile¥certstore¥28b9d521.0
   Snapshot¥systemprofile¥certstore¥bb7eb69b.0
   Snapshot¥systemprofile¥certstore¥ef12cf8d.0
   Snapshot¥systemprofile¥certstore¥keystore¥ABPrivKeyFile.pem
   Snapshot¥systemprofile¥certstore¥keystore¥ABPubKeyFile.pem
   Snapshot¥systemprofile¥certstore¥keystore¥DummyWebPrivKeyFile.p
   em
   Snapshot¥systemprofile¥certstore¥keystore¥DummyWebPubKeyFile.pe
   m
   Snapshot¥systemprofile¥certstore¥keystore¥PrivKeyFile.pem
   Snapshot¥systemprofile¥certstore¥keystore¥PubKeyFile.pem
   Snapshot¥systemprofile¥certstore¥keystore¥RBPrivKeyFile.pem
   Snapshot¥systemprofile¥certstore¥keystore¥RBPubKeyFile.pem
   Snapshot¥systemprofile¥certstore¥trusted¥bb7eb69b.0
   Snapshot¥systemprofile¥systruststore¥28b9d521.0
   ```

```
16 File(s) copied
```

4 次のコマンドを実行してブローカーを起動します。

```
net start vrtsat
```

用語集

ここでは、Symantec Product Authentication Service を理解するのに必要な概念について説明します。

Secure Sockets Layer プロトコル（Secure sockets layer protocol）

Secure sockets layer（SSL）は公開キープロトコルです。クライアントとサーバーが Web を介したセキュアな通信を行うために使用されます。たとえば、SSL プロトコルは、インターネットを介したクレジットカード情報やその他の機密データの送信によく使用されます。

SSL テクノロジにより、Symantec アプリケーションクライアント、認証ブローカー、Symantec アプリケーションサービス間でセキュアな通信が可能になります。

認証の際、クライアントは SSL を使って、認証ブローカーとの通信を確立し、製品信用証明を要求します。プリンシパルの認証を 1 回行うと、Symantec アプリケーションクライアントと Symantec アプリケーションサービスとの間で SSL 接続が確立されます。クライアントが通信を停止するまで、必要に応じてメッセージがやり取りされます。

SSPI プラグインを介したシングルサインオン認証（Single sign-on authentication through the SSPI plugin）

Windows の Security Support Provider Interface（SSPI）。Microsoft プラットフォーム上で動作するアプリケーション間の認証と通信に関する一連のセキュリティサービスを提供します。

Symantec Product Authentication Service は、SSPI プラグインと連動して、Microsoft プラットフォームとログインを統合します。ユーザーは、別のパスワードを入力する必要がありません。

たとえば、ユーザーが、Windows ドメインのアカウントとパスワードを使用してすでに Windows コンピュータにログインしているとします。Symantec Product Authentication Service は、信用証明の取得に SSPI を使用します。この SSPI 接続では、Symantec アプリケーションクライアントから認証ブローカーまでがリンクされます。Symantec アプリケーションクライアントから Symantec アプリケーションサービスへの通信は、暗号化されたチャネル上で相互に認証されます。認証ブローカーによる認証において Symantec Product Authentication Service は、プリンシパルが所属する OS グループをすべて取得します。

アプリケーションホスト（Application Host）

Symantec アプリケーションが実行されるマシン。

証明書（Certificate）

証明書は、電子パスポートや ID カードの一種です。所有者の ID 情報を保証し、プリンシパルの名前をユーザーの公開キーにバインドします。

認証局の各階層で、プリンシパルの信頼性を保証する証明書の署名が行われます。ルートの認証局（ルートブローカー上）は、この階層の最上位に位置するエンティティであるため、最も信頼性の高い認証局です。この認証局の証明書は、ルート自身を保証する、自己署名された証明書です。これをルート証明書と呼びます。

アプリケーションプログラム環境には、認証ライブラリにより有効な署名者として受け入れられ、ルート証明書一式が含まれています。この証明書の内容は、事前に設定することも、Symantec アプリケーションサービスから入手することもできます。プリンシパルでは、このルート証明書が、レジストリの設定の一部として格納されます。ただし、実際には、個別のファイルかファイルセットに格納し、次に示す標準形式の小規模コレクションの 1 つに格納する方法が一般的です。

- 標準の PKCS#12
- JKS（Java JSSE で使用）
- PEM（OpenSSL 内、S/MIME 実装用）

信用証明（Credential）

製品信用証明（略して信用証明）とは、認証済みのプリンシパルとして認識される資格を意味します。この製品信用証明には証明書が含まれますが、プリンシパル専用キーも含む必要があります。両方がそろっていないと、信用証明にはなりません。

製品信用証明では、次のものが両方必要となります。

- プリンシパル専用キー
- 特別な拡張子を含む X.509v3 証明書
  証明書は、プリンシパル名を公開キーにバインドするために認証ブローカーまたはルートブローカーのいずれかにより作成、署名されます。

製品信用証明は、シングルサインオンの信用証明に相当します。Symantec Product Authentication Service が使用可能で、Symantec シングルサインオンのセッション内で動作するすべての Symantec アプリケーションに対して、この製品信用証明が有効になります。

製品信用証明を必要とするユーザー

Symantec リソース管理アプリケーションには、2 つのコンポーネントが含まれています。次にこれらのコンポーネントを示します。なお、これらのコンポーネントはいずれも有効な信用証明を使って認証される必要があります。

- Symantec アプリケーションクライアント
  Symantec サービスまたは別のプログラムから提供される機能にアクセスするプログラムです。
- Symantec アプリケーションサービス
  要求されたサービスを提供するプログラムです。

これらのコンポーネントは、認証時はいずれもクライアントとして機能します。信用証明は、それがアプリケーションクライアントに所属するか、アプリケーションサービスに所属するかによって異なります。通常、サービスに付与される信用証明は、クライアントに付与されるものより長い期間有効です。

セキュリティポリシー（Security policy）

セキュリティポリシーとは、次の事柄について十分に検討を行った決定事項のことです。

- 該当する環境で製品を使用する方法
- 製品が誤用される場合の用途と方法
- 製品で施行するアクセスルールの範囲

ポリシーの許容範囲を設定するには、次の項目を考慮します。

- 製品を使用するユーザーまたは機能
- 実行するタスクと使用するリソース。それを実行するユーザーまたは機能

認証（Authentication）

識別情報を検証すること。クライアントは、自分自身を識別することと、本人であることを証明することが求められます。証拠を提示して受け入れられると、クライアントに証明書が与えられます。クライアントは次に、この証明書とクライアントの専用キーを組み合わせて有効な製品信用証明を作成します。

認証ドメイン（Authentication domain）

認証プリンシパルに対して一連の識別情報を定義したもの。また、グループメンバーシップなど、プリンシパルに関連する認可情報を提供します。この種の認可情報には、Active Directory ドメイン内の名前などがあります。特別な形式の認証ドメインとして、Symantec 社製品独自のプライベートドメインがあります。

認証プラグイン（Authentication plugin）

認証ブローカーにより、特定のドメインタイプで識別情報の検証に使用されるコンポーネント。

認証メカニズム（Authentication mechanism）

ドメインで定義された特定の名前空間内のプリンシパルに対して認証を行う方法。たとえば、Kerberos ドメインでは、Kerberos ticket とパスワードが使用されます。認証メカニズムは、認証アルゴリズムの詳細すべて（API、プロトコル、トークン形式、トークンコンテンツの構文、データベースオブジェクト形式など）をカプセル化します。関連する構成要素は、メカニズムごとに異なります。

認証ライブラリ（Authentication library）

Symantec アプリケーションクライアントにリンクするコンポーネント。認証の要求を行うプログラムの呼び出しを実装します。概念上、このライブラリは通信のセキュリティを保護する認証部分から切り離されています。実際には、両方のコンポーネントを 1 つのライブラリにまとめることが可能です。