

SiteMinder

ポリシー サーバ管理ガイド

12.52 SP1



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。

本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし、CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負いません。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- SiteMinder
- eTrust SOA Security Manager (以前の CA SOA Security Manager)
- CA IdentityMinder® (旧 CA Identity Manager)
- CA Security Compliance Manager

CA への連絡先

テクニカルサポートの詳細については、弊社テクニカルサポートの Web サイト (<http://www.ca.com/jp/support/>) をご覧ください。

マニュアルの変更点

以下のドキュメントの更新は、本書の最新のリリース以降に行われたものです。

- [CA SiteMinder イベント マネージャの設定](#) (P. 233) - イベント ライブラリ ファイル (178452) の設定に関する情報が追加されました。
- [LDAP 検索タイムアウト問題の解決](#) (P. 333) - SearchTimeout レジストリ設定を設定するために、別のユース ケースが追加されました。CQ169864 および STAR イシュー番号 20130617 の解決
- [r12.x ポリシー ストア暗号化キーのリセット](#) (P. 135) - CQ171497、CQ171365 を解決するために暗号化キーをリセットする前に、ポリシー サーバを停止する手順が追加されました。
- [MySQL セッションストアタイムアウトエラーの解決](#) (P. 338) - MySQL データベースのセッションストアタイムアウトエラーのトラブルシューティングを行う方法について説明するトピックが追加されました。CQ 177929 を解決します。
- [一部の LDAP ユーザディレクトリでの VLM インデックスによって SiteMinder エージェントグループのロックアップが失敗する](#) (P. 358) - VLV インデックスが原因で発生するエージェントグループロックアップエラーのトラブルシューティングを行う方法について説明するトピックが追加されました。CQ 176247 および STAR イシュー 20397633-1 を解決します。
- [SM--管理 UI が応答しなくなる](#) (P. 334) - スタンドアロンの管理 UI インストール (JBoss アプリケーションサーバが組み込まれている) で管理 UI が応答しなくなるという状況のトラブルシューティングを行う方法について説明するトピックが追加されました。CQ 175819 および STAR イシュー 21529036-1 を解決します。
- [r12.x のポリシー ストア暗号化キーのリセット](#) (P. 135) - 指示が更新されました。CQ 171365/178999 を解決します。
- [監査データの ODBC データベースへのインポート](#) (P. 56) - -b オプションを使用して監査データを Oracle データベースに追加する際に、[ODBC Oracle Wire Protocol Driver Setup] ダイアログ ボックスで [Enable bulk load] オプションを設定しないように指示する注が追加されました。CQ 159529 および STAR イシュー 21045785-2 を解決します。

目次

第 1 章: ポリシー サーバの管理	15
ポリシー サーバ管理の概要	15
ポリシー サーバのコンポーネント	15
ポリシー サーバの処理	16
ポリシー サーバ管理	18
ポリシー サーバの管理タスク	19
ポリシー サーバ管理コンソール	20
ポリシー サーバユーザ インターフェース	21
第 2 章: ポリシー サーバの起動と終了	25
サービスとプロセスの概要	25
Windows システムでのポリシー サーバ サービスの開始と終了	26
UNIX システムでのポリシー サーバ プロセスの開始と終了	26
ポリシー サーバ シャットダウン中のスレッド終了ウィンドウ	28
ポリシー サーバ エグゼクティブの設定	29
Windows エグゼクティブの設定	29
UNIX エグゼクティブの設定	29
第 3 章: ポリシー サーバのデータ ストレージ オプションの設定	31
データ ストレージ オプション設定の概要	31
ポリシー ストア データベースの設定	33
ポリシー ストア データベースを使用するためのキー ストアまたは監査ログの設定	33
キー ストア用の個別のデータベースの設定	34
監査ログ用の個別のデータベースの設定	35
セッション ストアの設定	37
高負荷環境でのセッション ストア タイムアウトの設定	37
LDAP ストレージ オプションの設定	38
LDAP データベースの設定	38
LDAP フェールオーバーの設定	39
拡張 LDAP リフェラル処理の設定	39
大きな LDAP ポリシー ストアのサポートの設定	41
SSL サポートを設定する方法	43
ODBC ストレージ オプションの設定	51

ODBC データソースの設定	51
ODBC フェールオーバーの設定	52
SQL クエリによって返されるレコードの最大数の設定	52
タイムアウト用の ODBC レジストリ設定の設定	53
テキスト ファイルストレージ オプションの設定	54
ODBC の監査データ インポート ツール	54
テキスト ファイルへのより多くの監査データ ログの記録	55
ODBC の監査データ インポートの前提条件	56
ODBC データベースへの監査データのインポート	56
Netscape 証明書データベース ファイルの指定	58

第 4 章: ポリシー サーバの一般的な設定 61

ポリシー サーバの設定の概要	61
ポリシー サーバの設定	61
アクセス制御の設定	62
ポリシー サーバ管理の設定	62
ポリシー サーバの接続オプションの設定	62
ポリシー サーバのパフォーマンスの設定	62
RADIUS の設定	63
OneView モニタの設定	63
SiteMinder ポリシー データ同期の再スケジュール	63
ログ ファイルおよびコマンドライン ヘルプの別の言語への設定	65

第 5 章: 証明書データストアの管理 71

証明書廃棄リスト (CRL) の更新	71
デフォルトの CRL 更新間隔の変更	73
OCSP の更新	73
OCSP と CRL チェックとの間のフェールオーバー	74
OCSP の更新スケジュール	75
OCSP 更新のための SMocsp.conf ファイルの変更	76
OCSP の無効化	83
証明書のキャッシュ リフレッシュ間隔	84
デフォルトの廃棄猶予期間	84

第 6 章: ポリシー サーバのスーパーユーザ パスワードの変更 87

スーパーユーザ パスワードの概要	87
ポリシー サーバのスーパーユーザ パスワードの変更	87

第 7 章: ポリシー サーバログの設定 89

ポリシー サーバによるロギングの概要	89
ポリシー サーバログの設定	89
ポリシー ストア オブジェクトに対して管理者が行った変更の記録	90
古いログ ファイルを自動的に処理する方法	93
SiteMinder 管理監査イベントをレポートに含める方法	94
Windows で ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする	96
Solaris で ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする	97
システム ログへの問題記録のレポート	97
証明書データ ストアのログ設定	98
syslog にイベントを記録する方法	100
コンソールを開く	101
syslog オプションの設定	102
UNIX ポリシー サーバの停止	104
UNIX ポリシー サーバの起動	105
Windows オペレーティング環境でアサーション属性のログ記録を有効にする方法	105
Windows レジストリ エディタを開く	106
レジストリ キーの値の変更	107
Windows ポリシー サーバの停止	108
Windows ポリシー サーバの起動	109
UNIX または Linux オペレーティング環境でアサーション属性のログ記録を有効にする方法	109
sm.registry ファイルをテキストエディタで開く	111
レジストリ ファイル内の行の値の変更	112
UNIX ポリシー サーバの停止	113
UNIX ポリシー サーバの起動	114

第 8 章: 暗号化キーの設定と管理 115

ポリシー サーバの暗号化キーの概要	116
キー管理の概要	117
FIPS 140-2 アルゴリズム	118
導入されたエージェント キー	119
ダイナミック エージェント キーのロールオーバー	120
ダイナミック エージェント キーのロールオーバー	121
ダイナミック キーのロールオーバーで使用するエージェント キー	121
エージェント キーのロールオーバー間隔	122
スタティック キー	123
セッションチケット キー	124
キー管理のシナリオ	125

キー管理に関する注意事項.....	126
共通のポリシーストアとキーストア.....	128
共通のキーストアがある複数のポリシーストア.....	129
個別のキーストアがある複数のポリシーストア.....	130
r6.x ポリシー ストア暗号化キーのリセット.....	131
r12.x ポリシー ストア暗号化キーのリセット.....	135
エージェント キー生成の設定.....	136
エージェント キーの管理.....	137
定期的なキー ロールオーバーの設定.....	137
キーの手動ロールオーバー.....	138
エージェント キー管理とセッション タイムアウトの調整.....	139
スタティック キーの変更.....	140
セッション チケット キーの管理.....	141
セッション チケット キーの生成.....	141
手動によるセッション チケット キーの入力.....	142
EnableKeyUpdate レジストリ キーの設定.....	142
トラステッドホストの共有秘密キー.....	144
トラステッドホストの共有秘密キーのロールオーバー設定.....	145

第 9 章: ポリシー サーバ プロファイラの設定 147

ポリシー サーバ プロファイラの設定.....	147
プロファイラ設定の変更.....	149
Windows 環境でのプロファイラ コンソールの出力に関する問題の回避.....	150
プロファイラ トレース ファイルの保持ポリシーの設定.....	151
プロファイラ トレース ログ ファイルの手動によるロールオーバー.....	151
指定された間隔でのトレース ファイルの動的なロールオーバー.....	153

第 10 章: 管理ジャーナルとイベントハンドラの設定 155

管理ジャーナルとイベントハンドラの概要.....	155
ポリシー サーバの高度な設定.....	155
イベントハンドラ ライブラリの追加.....	156

第 11 章: グローバル設定の調整 159

ユーザ追跡の有効化.....	159
ネストされたセキュリティの有効化.....	160
拡張された Active Directory 統合を有効にする方法.....	160
IgnoreADpwdLastSet レジストリキーの作成.....	161
Active Directory 統合の拡張の有効化.....	161

ユーザディレクトリ接続の設定.....	163
第 12 章: キャッシュ管理	167
キャッシュ管理の概要.....	167
キャッシュ更新の管理.....	168
管理 UI を使用したキャッシュ更新の管理.....	168
smpolycysrv コマンドを使用したキャッシュ更新の管理.....	169
キャッシュのクリア.....	170
すべてのキャッシュのクリア.....	170
ユーザセッション キャッシュのクリア.....	171
リソース キャッシュのクリア.....	172
ポリシー サーバのリクエスト キューのクリア.....	173
第 13 章: ユーザセッションとユーザアカウントの管理	175
ユーザセッションとユーザアカウントの管理の前提条件.....	175
ユーザの有効化と無効化.....	176
ユーザパスワードを管理する方法.....	177
ユーザ許可の監査.....	178
第 14 章: ハードウェア ロード バランサを使用した SiteMinder エージェント とポリシー サーバ間の通信の設定	179
ハードウェア ロード バランシング.....	179
SiteMinder エージェントとポリシー サーバ間の接続の有効期間の設定.....	181
ハードウェア ロード バランシング設定の状態の監視.....	183
アクティブ モニタ.....	184
パッシブ モニタ.....	185
第 15 章: ポリシー サーバのクラスタ化	187
クラスタ化されたポリシー サーバの導入.....	187
フェイルオーバーのしきい値.....	189
ハードウェア ロード バランシングの考慮事項.....	190
ポリシー サーバクラスタの設定.....	191
クラスタの集中監視用のポリシー サーバ設定.....	192
クラスタ化されているポリシー サーバを集中監視用のポリシー サーバの監視対象にする.....	193

第 16 章: OneView モニタの使用 195

第 17 章: OneView モニタの概要 197

ポリシー サーバのデータ	199
Web エージェントのデータ	203
OneView モニタの設定	211
クラスタ化された環境の監視	213
OneView ビューアへのアクセス	214

第 18 章: SNMP による SiteMinder の監視 219

SNMP 監視	219
SNMP の概要	219
SiteMinder SNMP モジュールのコンポーネント	220
依存関係	221
SNMP コンポーネントのアーキテクチャとデータフロー	222
SiteMinder MIB	223
MIB の概要	223
SiteMinder MIB 階層	224
MIB オブジェクトの参照リスト	224
イベントのデータ	231
SiteMinder イベント マネージャの設定	233
イベント設定ファイルの構文	233
イベント設定ファイルの例	234
SiteMinder SNMP サポートの開始と終了	235
Windows 環境の Netegrity SNMP エージェント サービスの開始と終了	235
UNIX 環境のポリシー サーバでの SNMP サポートの開始と終了	236
SiteMinder SNMP モジュールのトラブルシューティング	237
イベントが発生しても SNMP トラップが受信されない	237

第 19 章: SiteMinder レポート 239

レポートの説明	239
SiteMinder レポートのスケジュール	241
SiteMinder レポートの表示	241
SiteMinder レポートの削除	242

第 20 章: ポリシー サーバのツール 243

ポリシー サーバツールの導入	243
----------------------	-----

Windows 2008 ポリシー サーバ ツール要件	246
Linux Red Hat 上でポリシー サーバのツールを使用する場合の要件	246
smobjimport によるポリシー データのインポート	247
XML ベースのデータ形式の概要	248
XPSExport	250
ポリシー データの追加	255
ポリシー データの上書き	257
ポリシー データの置換	259
ポリシー データのマージ	261
XPSImport	262
ポリシー データ転送のトラブルシューティング	264
smkeyexport	265
SiteMinder キー ツール	266
秘密キーと証明書のペアの追加	267
証明書の追加	269
破棄情報の追加	270
破棄情報の削除	271
証明書データの削除	271
証明書の削除	272
証明書または秘密キーのエクスポート	272
エイリアスの検索	273
デフォルトの CA 証明書のインポート	274
すべての証明書のメタデータ リスト	274
破棄情報リスト	275
証明書メタデータの表示	276
エイリアス名の変更	276
証明書の検証	277
OCSP 設定ファイルのロード	277
smldapsetup	278
smldapsetup のモード	280
smldapsetup の引数	282
smldapsetup と Sun Java System Directory Server Enterprise Edition	286
smldapsetup による SiteMinder ポリシー ストアの削除	288
ODBC データベース内の SiteMinder データの削除	289
smpatchcheck	291
SiteMinder テストツール	292
smreg	292
XPSCounter	293
Active Directory の inetOrgPerson 属性のマッピング	293
SiteMinder ポリシーに関連付けられているユーザの数の確認	294

XPConfig	296
XPSEvaluate.....	300
XPExplorer	302
ポリシー ストア データのサブセットのエクスポート	304
XCart 管理.....	306
XPSSecurity.....	313
管理者をスーパーユーザにする	314
-XPSSweeper	316
バッチ ジョブとしての XPSSweeper の実行	317
XPConfig を使用した 24 時間間隔で実行する Autosweep の設定	319

第 21 章: ポリシー サーバ設定ファイル 321

CA Compliance Security Manager 設定ファイル	321
Connection API 設定ファイル	322
OneView モニタ設定ファイル	322
SiteMinder 設定ファイル	323
SNMP 設定ファイル.....	323
SNMP イベント トラップ設定ファイル	324
ポリシー サーバレジストリ キー	324

付録 A: SiteMinder と CA Security Compliance Manager 327

SiteMinder と CA Security Compliance Manager の統合のしくみ.....	327
コンプライアンス レポートの生成	329
使用可能なコンプライアンス レポートまたはそのフィールドのリストの表示.....	330
新しいコンプライアンス レポートの追加	331
既存のコンプライアンス レポートの内容の変更	332

付録 B: SiteMinder の一般的なトラブルシューティング 333

LDAP 検索タイムアウトの問題を解決する	333
管理 UI が無応答になる.....	334
MySQL セッションストア タイムアウト エラーの解決	338
ポリシー サーバが LDAP 管理者制限を超過したエラーで終了する	338
コマンドラインからのポリシー サーバのトラブルシューティング	340
デバッグの動的な開始または停止	344
トレースの動的な開始または停止	345
Web エージェント通信失敗後にポリシー サーバがハングする	346
インストールされている JDK のバージョンの確認.....	347
ポリシー サーバログのローカル時間設定の無効化	348

システム アプリケーション ログの確認	348
LDAP SDK 層によって処理される LDAP リフェラル	348
LDAP リフェラルの無効化	349
バインド操作での LDAP リフェラルの処理	350
アイドルタイムアウトとステートフルインスペクションデバイス	352
エラー -- Optional Feature Not Implemented	353
管理者アクティビティの記録時に発生するエラーまたはパフォーマンスの低下	354
ポリシー ストアを共有するポリシー サーバが一貫して更新されない	354
キャッシュ失敗タイムアウト	355
キー ロールオーバー ログ メッセージ	356
キャッシュ更新ログ メッセージ	356
ポリシー サーバ管理コンソールを開くときの、イベントハンドラ リスト設定に関する警告	357
SiteMinder ポリシー サーバの起動イベント ログ	357
LDAP ユーザディレクトリ上の VLV インデックスにより SiteMinder エージェント グループの検索 が失敗する (174279)	358

付録 C: ログファイルの説明 359

smaccesslog4	359
smobjlog4	364

付録 D: 診断情報の発行 369

診断情報の概要	369
コマンドラインインターフェースを使用します。	369
発行される情報の保存場所の指定	370
データの発行	371
発行されるポリシー サーバ情報	371
発行されるオブジェクトストア情報	376
発行されるユーザディレクトリ情報	379
発行されるエージェント情報	381
発行されるカスタム モジュール情報	384

付録 E: エラー メッセージ 387

認証	387
許可	404
サーバ	407
Java API	428
LDAP	437
ODBC	471

ディレクトリ アクセス	474
トンネル	481

第 1 章: ポリシー サーバの管理

このセクションには、以下のトピックが含まれています。

[ポリシー サーバ管理の概要 \(P. 15\)](#)

[ポリシー サーバの管理タスク \(P. 19\)](#)

ポリシー サーバ管理の概要

ポリシー サーバは、以下のような CA 製品と連携して動作するアクセス制御プラットフォームになります。

- SiteMinder - ポリシー サーバと SiteMinder エージェントとを統合して、Web サーバのアクセス制御を行います。
- eTrust SOA Security Manager - ポリシー サーバと [set AGENT value for your book]とを統合して、XML ベースの Web サービスのアクセス制御を行います。この製品をご購入済みの場合、詳細については「*eTrust SOA Security Manager Policy Configuration Guide*」を参照してください。
- CA Identity Manager - ID 管理サービスを提供します。詳細については、「*CA Identity Manager Administration Guide*」を参照してください。

注: SiteMinder およびポリシーベースのリソース管理については、「*ポリシー サーバ設定ガイド*」を参照してください。

ポリシー サーバのコンポーネント

ポリシー サーバ環境は、次の 2 つのコアコンポーネントによって構成されます。

- **ポリシー サーバ** - ポリシー管理、認証、許可、および監査の各サービスを提供します。
- **ポリシー ストア** - すべてのポリシー サーバデータが格納されます。

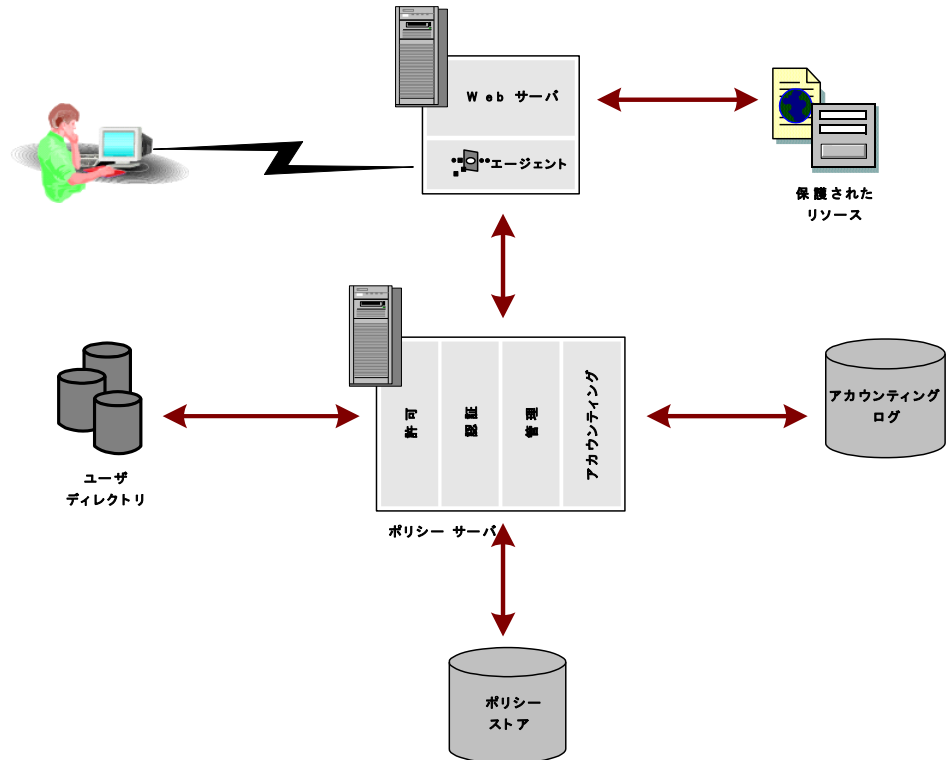
追加のコンポーネントとして、さまざまな CA 製品（SiteMinder エージェントなど）が含まれます。SiteMinder エージェントは、標準の Web サーバまたはアプリケーションサーバに統合されます。エージェントによって、SiteMinder では、事前定義されたセキュリティポリシーに基づいて Web アプリケーションおよびコンテンツへのアクセスを管理できるようになります。そのほかにも、SiteMinder エージェントには、SiteMinder が Web 以外のエンティティへのアクセスを制御することを可能にするタイプもあります。たとえば、SiteMinder RADIUS エージェントは RADIUS デバイスへのアクセスを管理し、SiteMinder アフィリエイト エージェントはポータルサイトからアフィリエイトの Web サイトに渡された情報を管理します。

ポリシー サーバの処理

ポリシー サーバでは、アクセス制御とシングルサインオンが可能です。通常、個別の Windows または UNIX システム上で稼働し、以下の重要なセキュリティ処理を実行します。

- **認証** - ポリシー サーバはさまざまな認証方法をサポートします。ユーザ名とパスワード、トークン、フォームベースの認証、あるいは公開キー証明書などに基づいてユーザを認証します。
- **許可** - ポリシー サーバは、ポリシー サーバ管理者により作成されたアクセス制御ルールの管理、実行を行います。これらのルールは、保護された各リソースに対して許可された操作が定義されています。
- **管理** - ポリシー サーバは、管理 UI を使用して設定できます。UI を使用して設定情報をポリシーストアに記録することを可能にしているのが、ポリシーストアの管理サービスです。ポリシーストアとは、権限付与情報が保存されているデータベースです。
- **監査** - ポリシー サーバは、システム内で発生するイベントの監査情報を記録するログファイルを生成します。これらのログは、あらかじめ定義されたレポート形式で印刷して、セキュリティイベントや異常の分析に使用できます。
- **状態監視** - ポリシー サーバには、状態監視コンポーネントが用意されています。

以下の図は、SiteMinder Web エージェントを 1 つ含む SiteMinder 環境でのポリシーサーバの単純な実装を示しています。

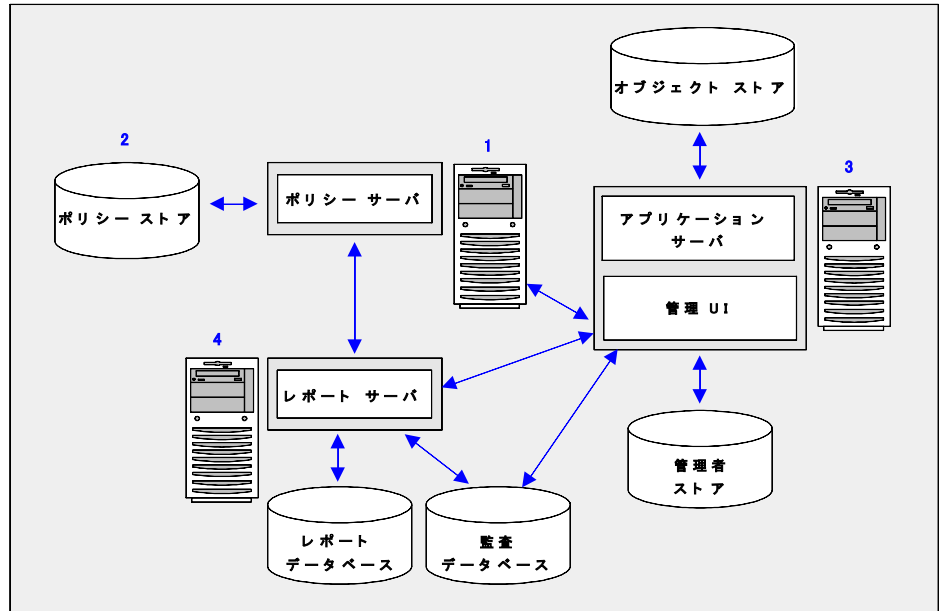


実際の Web 環境では、ユーザはブラウザを介してリソースをリクエストします。リクエストは、Web サーバが受信し、SiteMinder Web エージェントがインターセプトします。Web エージェントは、リソースが保護されているかどうかを判別し、保護されている場合は、ユーザのクレデンシャルを収集してポリシーサーバに渡します。ポリシーサーバは、ユーザ固有のディレクトリに照らし合わせてユーザを認証します。次に、ポリシーストア内のルールとポリシーに基づいて、リクエストしたリソースへのアクセスが認証されたユーザに許可されているかどうかを確認します。ユーザが認証され、許可されると、ポリシーサーバは保護されたリソースへのアクセス許可を付与し、権限と資格に関する情報を配信します。

注: カスタム エージェントは、SiteMinder エージェント API を使用して作成できます。詳細については、「*Programming Guide for C*」を参照してください。

ポリシー サーバ管理

以下の図は、ポリシー サーバの管理モデルを示しています。



1. **ポリシー サーバ** - ポリシー管理、認証、許可、および監査の各種サービスを提供します。
2. **ポリシー ストア** - ポリシー サーバのすべてのデータを格納します。ポリシー ストアの設定は、サポートされている LDAP またはリレーショナルデータベース内で行うことができます。
3. **管理 UI** - ポリシー サーバを介して、SiteMinder 管理者アカウント、オブジェクト、およびポリシー データを管理できます。管理 UI をインストールするときは、ディレクトリ XML ファイル、管理者ユーザストア、およびオブジェクトストアを設定します。
 - **オブジェクトストア** - 管理 UI はイベントベースおよびタスクベースの非同期アプリケーションです。オブジェクトストアはこの情報を格納します。オブジェクトストアの設定は、Microsoft SQL Server または Oracle データベース内で行います。

- **管理者ユーザストア** - 管理 UI は管理者ユーザストアを使用して、SiteMinder 管理者アカウントを認証します。すべての管理者アカウントは1つの管理者ユーザストアに格納する必要があります。管理 UI をインストールするときは、サポートされている LDAP ディレクトリ サーバまたは ODBC データベース内で管理者ユーザストアを設定します。
4. **レポートサーバおよびレポートデータベース** - SiteMinder の一連のポリシー分析および監査レポートを管理 UI から作成し、管理できます。レポートサーバとレポートデータベースは、レポート機能を使用するために必要になります。また、ポリシー分析レポートの実行にも必要です。レポートサーバと監査データベースは、監査ベースのレポートを実行するために必要になります。

ポリシー サーバの管理タスク

ポリシー サーバ管理者は、ユーザやユーザセッションの管理だけではなく、必要に応じて、SiteMinder 環境のシステムレベルの設定や調整と、そのパフォーマンスの監視や維持作業を行う必要があります。

基本的なシステム構成タスクと管理タスクのほとんどは、ポリシー サーバ管理コンソールで行います。その他のタスクは、管理 UI を使用して実行します。

ポリシー サーバの管理タスクには、以下が含まれます。

- ポリシー サーバの起動と終了
- ポリシー サーバ エグゼクティブの設定
- キャッシュ管理
- 暗号化キーの設定と管理
- ユーザセッションとユーザアカウントの管理
- SiteMinder 環境の状態の監視
- レポートの実行

ポリシー サーバ管理コンソール

ポリシー サーバ管理コンソール（略して「管理コンソール」）には、ポリシー サーバ設定とシステム管理のための一連のオプションが備わっています。管理コンソールは、タブベースのユーザ インターフェイスです。この UI では、情報や制御項目が機能ごとにグループ分けされて、1つのウィンドウの各タブに表示されます。

重要: ポリシー サーバ管理コンソールを実行するのは、Microsoft Windows における管理者グループのメンバユーザに限定する必要があります。

管理コンソールの起動

以下の手順に従います。

- **Windows**

SiteMinder プログラム グループ内の [ポリシー サーバ管理コンソール] アイコンを選択します。

重要: Windows Server 2008 上でこのグラフィカルユーザ インターフェイスにアクセスしている場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントの「リリース ノート」を参照してください。

- **UNIX**

`installation_directory/siteminder/bin/smconsole` を実行します。

注: UNIX 上でポリシー サーバ管理コンソールを実行するには、以下が必要です。

- Xディスプレイ サーバが実行されている必要があります。
- 以下を指定してディスプレイを有効にします。

```
export DISPLAY=n.n.n.n:0.0
```

```
n.n.n.n
```

ポリシー サーバのホスト システムの IP アドレスを指定します。

管理コンソール設定の変更内容の保存

管理コンソールのどのタブでも、次の操作を行うことができます。

- [適用] をクリックすると、設定は保存されますが、管理コンソールは開いたままになります。
- [OK] をクリックすると、設定が保存され、管理コンソールが閉じます。

注: 管理コンソール設定の変更内容を有効にするには、認証および許可プロセスを終了して再起動する必要があります。これらのサービスが再起動するまでは、ポリシー サーバで新しい設定を使用できません。

ポリシー サーバ ユーザ インターフェース

ブラウザ ベースの CA SiteMinder 管理 UI の主な用途は、ポリシー サーバ オブジェクトの管理ですが、いくつかのシステム管理機能も備えています。

管理 UI にアクセスする方法

1. 以下のいずれかを実行します。

- 管理 UI をホストしているコンピュータから、[スタート] - [プログラム] - [CA] - [SiteMinder] - [SiteMinder 管理 UI] をクリックします。
- ブラウザで以下の URL を開きます。

```
http://fqdn:port/iam/siteminder/adminui
```

fqdn

管理 UI ホスト システムの完全修飾ドメイン名を指定します。

ポート

管理 UI をホストしているアプリケーション サーバがリスンするポートを指定します。スタンドアロン オプションを使用して管理 UI をインストールした場合は、「8080」と入力します。

例: `http://somehost@example.com:8080/iam/siteminder/adminui`

管理 UI のログインページが表示されます。

2. 有効なユーザ名とパスワードを入力します。

ポリシー サーバに初めてアクセスするときは、ポリシー サーバのインストール中に作成したデフォルトのスーパーユーザ管理者アカウントを使用します。

3. [ログイン] をクリックします。

管理 UI が開きます。

ウィンドウの表示内容は、ログイン時に使用した管理者アカウントの権限に応じて変わります。アカウントにアクセス許可がある項目のみが表示されます。

XPS ツールへのアクセス許可の付与

SiteMinder に含まれる XPS ツールへのアクセス許可は、管理者が管理 UI を使用して個々のユーザに付与する必要があります。

次の手順に従ってください:

1. 管理 UI にログインします。
2. [管理] - [管理者] - [管理者] をクリックします。
3. 以下のいずれかを実行します。
 - 新しい管理者を追加するには、[管理者の作成] をクリックします。
 - 既存の管理者のアクセスを変更するには、ユーザを検索しレコードにアクセスするユーザの名前をクリックします。
4. 管理者の名前と説明(省略可)をそれぞれのフィールドに入力します。
5. ユーザパスを入力するか、[検索] をクリックし、既存のユーザパスを選択します。

注: XPS ツールによって制御される任意の設定への書き込みアクセスを行うには、ユーザパス (管理者が管理 UI または XPSecurity ツールで指定) が必要です。ユーザパスの形式は以下のとおりです。

namespace://directory_server/DN または *Login_for_OS*

6. (オプション) スーパーユーザの権限を付与するには、[スーパーユーザ] オプションを選択します。

7. [アクセス方法]セクション内の以下のコマンドラインツールのいずれかを選択します。

XPSEvaluate Allowed

XPS 式評価ツールへのアクセス許可を付与します。

XPSExplorer Allowed

XPS データベースを編集するツールへのアクセス許可を付与します。

XPSRegClient Allowed

Web Access Manager サーバまたは Reports サーバを権限のあるクライアントとして登録する XPS ツールへのアクセス許可を付与します。

XPSConfig Allowed

XPS 対応製品の XPS 設定を検査および設定するツールへのアクセス許可を付与します。XPSecurity Allowed

XPS ユーザを作成し、XPS 関連の権限を指定するセキュリティツールへのアクセス許可を付与します。

8. [サブミット] をクリックします。

これで管理者は、選択された XPS ツールを使用する許可が得られました。

詳細情報:

[イベントハンドラ ライブラリの追加 \(P. 156\)](#)

第 2 章: ポリシー サーバの起動と終了

このセクションには、以下のトピックが含まれています。

[サービスとプロセスの概要 \(P. 25\)](#)

[Windows システムでのポリシー サーバ サービスの開始と終了 \(P. 26\)](#)

[UNIX システムでのポリシー サーバ プロセスの開始と終了 \(P. 26\)](#)

[ポリシー サーバ シャットダウン中のスレッド終了ウインドウ \(P. 28\)](#)

[ポリシー サーバ エグゼクティブの設定 \(P. 29\)](#)

サービスとプロセスの概要

ポリシー サーバは、Windows 環境では 2 つのサービスを、UNIX 環境では 2 つのプロセスを実行します。ポリシー サーバのインストールプロセスでは、ポリシー サーバプロセスおよび監視プロセスを起動して、将来、システム起動時に自動的にプロセスを実行するようにエグゼクティブアプリケーションを設定します。

Windows の主なポリシー サーバプロセスを以下に示します。

ポリシー サーバ

認証、許可、監査/ログ、および管理 (有効になっている場合) のエージェントリクエストを処理します。

SiteMinder 状態監視サービス

認証サーバ、許可サーバ、および Web エージェントを監視するワンビュー モニタです。

UNIX の主なポリシー サーバプロセスを以下に示します。

smpolicysrv

認証、許可、監査/ログ、および管理 (有効になっている場合) のエージェントリクエストを処理します。

smmon

認証サーバ、許可サーバ、および Web エージェントを監視するワンビュー モニタです。

Windows システムでのポリシー サーバ サービスの開始と終了

Windows システムでポリシー サーバ サービスを開始または終了する方法

- 管理コンソールの [ステータス] タブで、[開始] ボタンまたは [停止] ボタンをクリックします。
- Windows の [スタート] - [設定] - [コントロール パネル] - [サービス] の順にクリックすると表示される [Windows サービス] ダイアログ ボックスを使用します。ポリシー サーバプロセスを起動または終了すると、関連するエグゼクティブも起動または終了します。
- `smppolycysrv` を使用すると、コマンドラインからポリシー サーバを停止できます。

```
installation_path%siteminder%bin%smppolycysrv -stop
```

注: Windows システムでは、リモートデスクトップまたはターミナル サービス ウィンドウから `smppolycysrv` コマンドを実行しないでください。

`smppolycysrv` コマンドはプロセス間通信に依存します。この通信は、リモートデスクトップまたは [ターミナル サービス] ウィンドウから `smppolycysrv` プロセスを実行した場合には機能しません。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

UNIX システムでのポリシー サーバ プロセスの開始と終了

UNIX システムでポリシー サーバのプロセスを開始または終了するには、次のいずれかの操作を行います。

- 管理コンソールの [ステータス] タブで、対応する [開始] ボタンまたは [停止] ボタンをクリックします。
- 用意されているスクリプトを使用します。ポリシー サーバプロセスの起動と終了には、2つのスクリプトが用意されています。ポリシー サーバプロセスが再起動されないように、これらのスクリプトによって UNIX エグゼクティブも終了されます。

```
installation_path/siteminder/start-all  
installation_path/siteminder/stop-all
```

さらに、次のスクリプトをポリシー サーバプロセスの起動と終了に使用できます。スクリプトを実行したときに UNIX エグゼクティブが起動されていなかった場合は、プロセスだけでなくエグゼクティブも起動されます。また、スクリプトは、以下のような同じコマンドラインオプションで呼び出せます。

`installation_path/siteminder/smpolsrv`

コマンドラインオプション:

-stop

プロセスを終了します。

-start

プロセスを起動します。

-status

プロセスが起動されているかどうかを示します。

ポリシー サーバは、UNIX エグゼクティブの全アクティビティのログを `installation_directory/log/smexec.log` ファイルに記録します。ログのエントリは、常に既存のログファイルに追加されます。

詳細情報:

[コマンドラインからのポリシー サーバのトラブルシューティング \(P. 340\)](#)

ポリシー サーバシャットダウン中のスレッド終了ウィンドウ

デフォルトでは、ポリシー サーバは、シャットダウンする前にすべてのスレッドの終了を 3 分間待機します。スレッドのいずれかが終了しない場合でも、ポリシー サーバは終了します。

レジストリ キーを作成することによって、ポリシー サーバがスレッドの終了を待機する最大の時間を変更することができます。

レジストリ キーを作成する方法

1. ポリシー サーバ ホスト システムにアクセスし、以下のいずれかを実行します。
 - (Windows) レジストリ エディタを開き、`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer` に移動します。
 - (UNIX) `sm.registry` ファイルを開きます。このファイルのデフォルトの場所は `siteminder_home/registry` です。

siteminder_home

ポリシー サーバのインストールパスを指定します。

2. `MaxShutDownTime` を作成し、レジストリ値のタイプは `REG_DWORD` にします。

測定単位：秒

デフォルト値：180

最小値：30

最大値：1800

3. 以下のいずれかを実行します。
 - (Windows) レジストリ エディタを終了します。
 - (UNIX) `sm.registry` ファイルを保存します。
4. ポリシー サーバを再起動します。

重要: シャットダウン中にポリシー サーバスレッドが適切に終了しない場合は、SiteMinder サポートにお問い合わせください。

ポリシー サーバ エグゼクティブの設定

UNIX や Windows にポリシー サーバをインストールする場合、1つまたは複数のエグゼクティブアプリケーションによってポリシー サーバプロセスのステータスが監視され、エラーが発生したプロセスは自動的に再起動されます。以下のセクションでは、お使いのプラットフォームに基づいてポリシー サーバプロセスを開始および停止する方法、UNIX と Windows の実行ファイルを設定、無効化、有効化する方法について説明します。

Windows エグゼクティブの設定

Windows では、各ポリシー サーバプロセスは別々のエグゼクティブで監視されます。それぞれのエグゼクティブは、`Policy_Server_installation_path¥config¥siteminder.conf` 設定ファイルから、次のしきい値を読み込みます。

SMEEXEC_UPTIME_THRESHOLD

ポリシー サーバサービスの起動後、頻繁にエラーが発生するため関連するエグゼクティブが監視を停止するまでの間、ポリシー サーバサービスを実行する必要最小時間を秒単位で指定します。このパラメータのデフォルト値は 60 秒です。

SMEEXEC_RESTART_THRESHOLD

SMEEXEC_UPTIME_THRESHOLD パラメータで指定した時間内に、エグゼクティブがサービスの再起動を試行する回数の最大値を指定します。このパラメータで指定した回数を超えるエラーがサービスで発生した場合、エグゼクティブはサービスの再起動を中止します。この試行回数のパラメータのデフォルト値は 5 回です。

しきい値パラメータを変更するには、`siteminder.conf` ファイルを編集し、ポリシー サーバプロセスを再起動してください。

UNIX エグゼクティブの設定

UNIX では、ポリシー サーバプロセスと状態監視プロセスが 1つのエグゼクティブで監視されます。エグゼクティブは、次の設定ファイルから設定を読み込みます。

```
installation_path/config/siteminder.conf
```

このファイルを編集すると、次の設定を変更できます。

POLICYSERVER_ENABLED

エグゼクティブの実行開始時の、ポリシー サーバプロセスのステータスを指定します。エグゼクティブの起動時にプロセスを有効にするには、このパラメータを「YES」に設定します。

MONITOR_ENABLED

エグゼクティブの実行開始時の、状態監視プロセスのステータスを指定します。エグゼクティブの起動時にプロセスを有効にするには、このパラメータを「YES」に設定します。

SMEEXEC_UPTIME_THRESHOLD

ポリシー サーバ サービスの起動後、頻繁にエラーが発生するため関連するエグゼクティブが監視を停止するまでの間、ポリシー サーバ サービスを実行する必要最小時間を秒単位で指定します。このパラメータのデフォルト値は 60 です。

SMEEXEC_RESTART_THRESHOLD

SMEEXEC_UPTIME_THRESHOLD パラメータで指定した時間内に、エグゼクティブがサービスの再起動を試行する回数の最大値を指定します。このパラメータで指定した回数を超えるエラーがサービスで発生した場合、エグゼクティブはサービスの再起動を中止します。この試行回数のパラメータのデフォルト値は 5 回です。

UNIX エグゼクティブのパラメータを変更する方法

1. `installation_path/config/siteminder.conf` ファイルを編集します。
2. コマンドラインで、次のスクリプトを実行します。

```
installation_path/siteminder/bin/stop-all
```

ポリシー サーバ プロセスが終了します。

3. コマンドラインで、次のスクリプトを実行します。

```
installation_path/siteminder/bin/start-all
```

UNIX エグゼクティブが、`siteminder.conf` ファイルの新しい設定を使用して再起動されます。

第 3 章: ポリシー サーバのデータ ストレージ オプションの設定

このセクションには、以下のトピックが含まれています。

[データ ストレージ オプション 設定の概要 \(P. 31\)](#)

[ポリシー ストア データベース の設定 \(P. 33\)](#)

[ポリシー ストア データベース を使用するための キー ストア または 監査 ログ の設定 \(P. 33\)](#)

[キー ストア 用の 個別の データベース の設定 \(P. 34\)](#)

[監査 ログ 用の 個別の データベース の設定 \(P. 35\)](#)

[セッション ストア の設定 \(P. 37\)](#)

[LDAP ストレージ オプション の設定 \(P. 38\)](#)

[ODBC ストレージ オプション の設定 \(P. 51\)](#)

[テキスト ファイル ストレージ オプション の設定 \(P. 54\)](#)

[ODBC の 監査 データ インポート ツール \(P. 54\)](#)

[Netscape 証明書 データベース ファイル の指定 \(P. 58\)](#)

データ ストレージ オプション 設定の概要

ポリシー サーバ 管理 コンソールの [データ] タブから、SiteMinder データ ストア 用の ストレージ 場所 を設定 します。

次の手順に従ってください:

1. ポリシー サーバ 管理 コンソール を起動 します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用 します。詳細については、お使いの SiteMinder コンポーネントのリリース ノート を参照 してください。

2. [データ] タブ をクリック します。

注: このタブの設定 および コントロール の詳細については、[ヘルプ] - [管理 コンソール ヘルプ] をクリック してください。

3. [データベース] から設定するデータストアを選択します。選択したデータストアによって、利用可能なストレージ機能が決まります。

注: 以下の表では、設定できるデータストアおよびそれぞれのストレージオプションをリストします。これらの設定の組み合わせによって、利用可能になる状況依存コントロールに表示される設定が決定されます。

4. [ストレージ] から選択したデータストア用のストレージタイプを選択します。
5. 必要な情報を設定します。
6. [OK] をクリックして設定を保存します。

以下の表に、SiteMinder データストアおよび使用できるストレージオプションをリストします。 **注:** これらのストアの詳細については、「SiteMinder 実装ガイド」を参照してください。

データベース	使用可能なストレージ
ポリシーストア	LDAP ODBC
キーストア	LDAP ODBC
監査ログ	ODBC テキストファイル
セッションストア	ODBC CA Directory

ポリシーストアデータベースの設定

ポリシーストアは、すべてのポリシーサーバオブジェクトが格納されるデータベースです。

ポリシーストアデータベースを設定する方法

1. [データベース] ドロップダウンリストから [ポリシーストア] を選択します。
2. 使用可能なストレージタイプ (LDAP または ODBC) を [ストレージ] ドロップダウンリストから選択します。
3. 選択したストレージタイプに合わせてストレージオプションを指定します。
4. [適用] をクリックして設定を保存するか、[OK] をクリックして設定を保存し、コンソールを終了します。
5. (オプション) ポリシーストアデータベースのストレージタイプを LDAP に変更し、そのポリシーストアをキーストアとして使用する場合は、「[ポリシーストアデータベースを使用するためのキーストアまたは監査ログの設定 \(P. 33\)](#)」で説明されている手順に従います。

注: LDAP 対応のポリシーストアと通信するポリシーサーバが 1 台以上ある場合は、各ポリシーサーバシステムの管理コンソールの設定を同じにする必要があります。

ポリシーストアデータベースを使用するためのキーストアまたは監査ログの設定

ポリシーストアを設定した後、任意でデータベースを設定できます。ポリシーストアが互換ストレージタイプの場合 (つまり、ポリシーストアを、他のデータベースにも有効なストレージオプションであるデータベースに格納されるように設定している場合)、ポリシーストアデータベースを使用して以下を保持するように、ポリシーサーバを設定できます。

- キーストア
- 監査ログ

重要: LDAP データベースをポリシー ストアとして使用している場合は、ポリシー ストア データベースを監査ログに使用しないでください。監査ログは LDAP データベースに書き込むことができません。SiteMinder サンプルデータ ソース (SmSampleUsers) をポリシー ストアとして使用している場合は、ポリシー ストア データベースを監査ログに使用しないでください。監査ログは、このサンプル ポリシー ストアではサポートされていません。

別のデータベースがポリシー ストア データベースに格納されるように設定するには、[ポリシー ストアを使用] オプションをオンにします。このオプションは、[データベース] ドロップダウン リストからポリシー ストア以外のデータベースを選択すると、[データベース] ドロップダウン リストとストレージ オプション領域の間に表示されます。

[ポリシー ストアを使用] オプションをオンにすると、[ストレージ] ドロップダウン リストとコンテキスト依存型のストレージ オプションが淡色表示になります。

キーストア用の個別のデータベースの設定

キー ストアは、SiteMinder エージェントによって作成された cookie の暗号化に使用するキーをポリシー サーバが格納する場所です。

キー ストア用の個別のデータベースを設定する方法

1. [データベース] ドロップダウン リストから、[キーストア] を選択します。
2. [ストレージ] ドロップダウン リストから、使用可能なストレージタイプ ([LDAP] または [ODBC]) を選択します。

注: ポリシー サーバは、LDAP/ODBC 混合のポリシー ストアとキー ストアをサポートしています。ポリシー ストアは ODBC データベースに格納でき、キー ストアは LDAP ディレクトリ サーバに格納できます。また、その逆も可能です。サポートされているデータベースのリストについては、テクニカル サポート [サイト](#)にある SiteMinder プラットフォーム マトリックスを参照してください。

3. 選択したストレージタイプに合わせてストレージ オプションを指定します。
4. [適用] をクリックして設定を保存するか、[OK] をクリックして設定を保存し、コンソールを終了します。

監査ログ用の個別のデータベースの設定

監査ログ データベースは、イベント情報を含む監査ログをポリシー サーバが格納する場所です。

データベースに監査ログを格納すると、環境内で遅延が発生する可能性があります。この遅延は、ポリシー サーバとデータベースの間のトラフィックが増加するために発生します。トランザクション量が増加すると、このデータベースの遅延は、ポリシー サーバのパフォーマンスに影響を与える場合があります。データベースが遅くなると、ポリシー サーバの速度も遅くなります。

データベースのパフォーマンスに問題がある場合は、回避策として、テキスト ファイルにログを記録してエクスポートすることを検討してください。

次の手順に従ってください:

1. [データベース] ドロップダウンリストから [監査ログ] を選択します。
2. [ストレージ] ドロップダウンリストから、使用可能なストレージタイプを選択します。
3. 選択したストレージタイプに合わせてストレージ オプションを指定します。
4. [適用] をクリックして設定を保存するか、[OK] をクリックして設定を保存し、コンソールを終了します。

ポリシー サーバの監査ログの格納先を ODBC データベースまたはテキスト ファイルのいずれにするかを決める際は、以下を考慮してください。

- SiteMinder レポートでは、監査ログが ODBC データベースに書き込まれる必要があります。レポートは、テキスト ファイルへのログ記録をサポートしていません。
- ODBC データベースおよびテキスト ファイルへの SiteMinder 監査ロギングでは、国際化 (I18N) がサポートされます。

- デフォルトでは、ポリシーストアオブジェクトへの SiteMinder 管理者変更は監査データベースに書き込まれません。これらのオブジェクト変更は、`siteminder_home¥audit` にあるテキストファイルに書き込まれます。レポートにこれらのイベントを含めるように SiteMinder を設定できます。
- 同期ログ記録は、非同期ログ記録よりもポリシーサーバのパフォーマンスに影響を与えます。
- ODBC データベースにログ記録する場合、`HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder ¥CurrentVersion¥Database¥` にある以下のレジストリ値を設定してください。この設定により、高負荷による監査データの損失を防ぐことができます。

ConnectionHangwaitTime

高負荷に備えて 60 秒に設定することをお勧めします。デフォルトは 30 秒です。

QueryTimeout

高負荷に備えて 30 秒に設定することをお勧めします。デフォルトは 15 秒です。

LoginTimeout

高負荷に備えて 30 秒に設定することをお勧めします。デフォルトは 15 秒です。

注: ConnectionHangwaitTime の値は常に、QueryTimeout と LoginTimeout の値の 2 倍以上である必要があります。

詳細情報:

[ポリシーストアオブジェクトに対して管理者が行った変更の記録 \(P. 90\)](#)
[SiteMinder 管理監査イベントをレポートに含める方法 \(P. 94\)](#)

セッションストアの設定

セッションストアはポリシーサーバが永続セッションデータを格納する場所です。

以下の手順に従います。

1. [データベース] からセッションサーバを選択します。
2. [ストレージ] から利用可能なストレージタイプを選択します。
3. [セッションサーバの有効化] オプションをオンにします。

1つ以上のレルムで永続セッションを使用する場合は、セッションストアを有効にします。セッションストアを有効にするとポリシーサーバのパフォーマンスに影響します。

注: 以下のオプションは無効化されます。

ポリシー ストア データベースの使用

パフォーマンス上の理由から、セッションストアをポリシーストアと同じデータベース上で動作させることはできません。

4. 必要なストレージオプションを指定します。
5. [OK] をクリックして設定を保存し、コンソールを終了します。

高負荷環境でのセッションストアタイムアウトの設定

高負荷環境では、アイドルタイムアウトしたセッションや期限切れになったセッションの削除など、セッションストアの保守タスクに必要な、実行時間の長いクエリがタイムアウトになる可能性があります。

MaintenanceQueryTimeout レジストリ設定の値を増加させることにより、セッションストアの保守タスクのタイムアウト（デフォルトでは 60 秒）を調節します。メンテナンススレッドがタスクを正常に完了できるように、値を増やします、

MaintenanceQueryTimeout レジストリ設定は次の場所にあります。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder¥CurrentVersion¥SessionServer
```

LDAP ストレージ オプションの設定

LDAP 状況依存ストレージコントロールを使用して、以下のように設定される LDAP ディレクトリ サーバを SiteMinder が参照するように指定します。

- ポリシー ストア
- セッション ストア

以下の点を考慮します。

- CA Directory は、SiteMinder がセッション ストアとしてサポートする唯一の LDAP ディレクトリ サーバです。詳細については、**12.52 SP1SiteMinder プラットフォーム サポート マトリックス**を参照してください。
- ポリシー サーバ管理コンソールの LDAP 設定を更新した後にポリシー サーバを再起動します。ポリシー サーバを再起動するまで、パラメータは有効になりません。

LDAP データベースの設定

LDAP データベースを設定する方法

1. [LDAP IP アドレス] フィールドで、LDAP サーバのサーバ名または IP アドレスを指定します。パフォーマンス上の理由から、IP アドレスを入力することをお勧めします。

注: LDAP サーバをフェールオーバー構成にするために、このフィールドには複数のサーバを指定することができます。

2. [ルート DN] フィールドで、SiteMinder スキーマを配下に持つ LDAP ブランチを指定します (o=myorg.org など)。
3. ポリシー サーバが SSL を介して LDAP ディレクトリと通信する場合は、[SSL を使用] チェック ボックスをオンにします。

注: このオプションをオンにした場合は、[Netscape 証明書データベース ファイル] フィールドで証明書データベースを指定する必要があります。

4. [管理ユーザ名] フィールドで、LDAP ディレクトリ管理者の DN を指定します (cn=Directory Manager など)。

5. [管理者のパスワード] フィールドに、LDAP ディレクトリの管理パスワードを入力します。
6. [パスワードの確認入力] フィールドで、LDAP ディレクトリの管理パスワードを確認します。
7. [LDAP 接続のテスト] をクリックして、入力したパラメータが正しいかどうか、および接続が作成できたかどうかを確認します。

LDAP フェールオーバーの設定

複数の LDAP ディレクトリを使用する場合、ディレクトリをフェールオーバー構成に設定できます。フェールオーバーを有効にするには、[LDAP IP アドレス] フィールドに LDAP サーバの IP アドレスとポート番号を入力します。LDAP サーバのアドレスは、それぞれスペース（空白）で区切って入力します。サーバごとに固有のポートを指定できます。使用している LDAP サーバが標準ポート以外のポート（SSL 以外は 389、SSL は 636）で稼働している場合、コロン（「:」）を区切り文字として使用し、最後に指定されているサーバの IP アドレスにポート番号を追加します。たとえば、サーバがポート 511 とポート 512 で稼働している場合は、次のように入力できます。

```
123.123.12.11:511 123.123.12.22:512
```

ポート 511 の LDAP サーバ 123.123.12.11 がリクエストに応答しない場合、リクエストは自動的にポート 512 の 123.123.12.22 に渡されます。

使用しているすべての LDAP サーバが同じポートで稼働している場合は、最後に指定されているサーバの後ろにポート番号を追加できます。たとえば、サーバがポート 511 で稼働している場合は、次のように入力できます。

```
123.123.12.11 123.123.12.22:511
```

拡張 LDAP リフェラル処理の設定

SiteMinder の LDAP リフェラル処理は強化され、パフォーマンスと冗長性が向上しました。旧バージョンの SiteMinder がサポートしていたのは、LDAP SDK 層による自動 LDAP リフェラル処理でした。LDAP リフェラルが発生すると、これまでは LDAP SDK 層が、参照先サーバへのリクエストの実行を、ポリシー サーバと通信せずに処理していました。

現行バージョンの SiteMinder は、非自動（拡張）LDAP リフェラル処理をサポートしています。非自動リフェラル処理では、LDAP リフェラルは、LDAP SDK 層ではなくポリシー サーバに返されます。リフェラルには、リフェラルの処理に必要なすべての情報が含まれています。ポリシー サーバは、リフェラルで指定されている LDAP ディレクトリが使用できるかどうかを調べて、該当する LDAP ディレクトリが機能していない場合は、リクエストを中断させることができます。この機能により、オフラインのシステムへの LDAP リフェラルによってリクエスト待ち時間が恒常的に増加することによるパフォーマンスの低下が解消されます。このような待ち時間の増加は、SiteMinder でリクエストの飽和状態を発生させることがあります。

LDAP リフェラル処理を設定する方法

1. ポリシー サーバ管理コンソールを開きます。

重要： Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [データ] タブを選択します。

機能強化型リフェラルの有効化

このチェック ボックスをオンにすると、LDAP SDK 層による LDAP リフェラル処理を有効にせずに、ポリシー サーバで LDAP リフェラルの機能強化処理を実行できるようになります。

最大リフェラル ホップ数

元のリクエストの処理試行で許可する連続リフェラルの最大数を指定します。リフェラルは、追加のリフェラルを必要とする位置を示すことができるため、この制限は、不適切な複製設定によってリフェラルループが発生するような場合に役立ちます。

3. 必要に応じて、値を変更します。
4. ポリシー サーバを再起動します。

大きな LDAP ポリシー ストアのサポートの設定

LDAP ポリシー ストアが大きいと、管理 UI のパフォーマンスに問題が生じる可能性があります。

そのような問題を防ぐため、以下のレジストリ設定の値を変更できます。

Max AdmComm Buffer Size

管理 UI のバッファ サイズを指定します（ポリシー サーバから 管理 UI に渡されるデータの 1 パケットあたりの最大データ量をバイト単位で表したもの）。

この設定はレジストリの以下の場所で行います。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion  
¥PolicyServ¥
```

この値を設定する場合は、注意してください。より大きなバッファを割り当てると、全体的なパフォーマンスが低下します。

範囲： 256 KB ~ 2,097,000 KB

デフォルト： 256 KB（このレジストリ設定が存在しない場合にも適用される）。

SearchTimeout

LDAP ポリシー ストアの検索タイムアウトを秒単位で指定します。

この設定はレジストリの以下の場所で行います。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion
\LdapPolicyStore\SearchTimeout
```

この設定に合った適切な値に影響を及ぼす要因の例には以下の項目があります（ただしこれらに限定されません）。

- ネットワーク速度
- LDAP 検索クエリ レスポンスのサイズ
- LDAP 接続の状態
- LDAP サーバの負荷

大量のポリシー ストア データを取得する場合、十分に大きな値を設定すると、すべての LDAP タイムアウトを防ぐことができます。

制限：16 進数を使用します。

デフォルト：0x14（20 秒）。レジストリ設定が存在しない場合にも、この値が使用されます。

例：0x78（120 秒）

詳細情報：

[ポリシー ストア データベースの設定 \(P. 33\)](#)

[キーストア用の個別のデータベースの設定 \(P. 34\)](#)

SSL サポートを設定する方法

SSL を介した LDAP 接続を設定するには、証明書データベース ファイルを使用するように SiteMinder を設定する必要があります。

SSL 接続を設定するには、以下の手順に従います。

1. SSL 接続前提条件を確認します。
2. NSS ユーティリティをインストールします。
3. 証明書データベース ファイルを作成します。
4. 証明書データベースに証明機関 (CA) を追加します。
5. 証明書データベースにサーバ証明書を追加します。サーバ証明書が認証局によって署名された場合は、各認証局からのルート証明書も証明書データベースに追加します。
6. 証明書データベース内の証明書を一覧表示します。
7. ポリシー サーバが証明書データベースを参照するようにします。

SSL に関する要件

以下の SSL 前提条件を考慮します。

- ディレクトリ サーバが SSL 有効になっていることを確認します。
注: 詳細については、ベンダー固有のドキュメントを参照してください。
- SiteMinder では、LDAP ディレクトリと通信するために Mozilla LDAP SDK を使用し、データベース ファイルが Netscape バージョン ファイル形式 (cert8.db) になっている必要があります。

重要: cert8.db データベース ファイルへの証明書のインストールに Microsoft Internet Explorer を使用しないでください。

証明書データベース ファイルの作成

証明書データベース ファイルを作成するには、ポリシー サーバに含まれている Mozilla Network Security Services (NSS) certutil アプリケーションを使用します。

注: 以下の手順では、タスクを実行するための具体的なオプションおよび引数について詳しく説明します。NSS ユーティリティのオプションおよび引数の全リストについては、[NSS プロジェクト ページ](#)にある Mozilla マニュアルを参照してください。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

次の手順に従ってください:

1. コマンドプロンプトから、インストール bin ディレクトリに移動します。

例: C:\Program Files\CA\SiteMinder\bin

注: Windows には固有の certutil ユーティリティがあります。ポリシーサーバ bin ディレクトリから作業していることを確認してください。そうしないと、間違えて Windows certutil ユーティリティを実行する場合があります。

2. 以下のコマンドを入力します。

```
certutil -N -d certificate_database_directory
```

-N

cert8.db、key3.db、および secmod.db の証明書データベース ファイルを作成します。

-d *certificate_database_directory*

certutil ツールが証明書データベース ファイルを作成するディレクトリを指定します。

注: ファイルパスにスペースがある場合は、そのパスを引用符で囲んでください。

このユーティリティは、データベース キーを暗号化するためにパスワードの入力を求めます。

3. パスワードを入力および確認します。

NSS は、必要な証明書データベース ファイルを作成します。

- cert8.db
- key3.db
- secmod.db

例: 証明書データベースファイルの作成

```
certutil -N -d C:%certdatabase
```

ルート認証機関の証明書データベースへの追加

ルート認証機関 (CA) を追加するには、Mozilla Network Security Services (NSS) certutil アプリケーションを使用します。これはポリシー サーバにあります。

注: 以下の手順では、タスクを実行するための具体的なオプションおよび引数について詳しく説明します。NSS ユーティリティのオプションおよび引数の全リストについては、[NSS プロジェクトページ](#)にある Mozilla マニュアルを参照してください。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

次の手順に従ってください:

1. コマンドプロンプトから、ポリシー サーバインストール bin ディレクトリに移動します。

例: C:%Program Files%CA%SiteMinder%bin

注: Windows には固有の certutil ユーティリティがあります。NSS ユーティリティの bin ディレクトリから作業するようにしてください。誤って Windows certutil ユーティリティを実行していることがあります。

- 以下のコマンドを実行します。

```
certutil -A -n alias -t trust_arguments -i root_CA_path -d  
certificate_database_directory
```

-A

証明書データベースに証明書を追加します。

-n *alias*

証明書の別名を指定します。

注: 別名にスペースがある場合は、その別名を引用符で囲んでください。

-t *trust_arguments*

証明書に適用する信頼属性を指定します。使用可能な 3 つの信頼カテゴリは、「SSL、電子メール、オブジェクト署名」の順番で表記されます。それぞれのカテゴリ位置に、以下の属性引数を 0 個以上使用することができます。

p

有効なピア。

P

信頼されたピア。この引数は **p** を意味します。

c

有効な CA。

T

クライアント証明書を発行する信頼された CA。この引数は **c** を意味します。

C

サーバ証明書を発行する信頼された CA (SSL のみ)。この引数は **c** を意味します。

重要: これは SSL 信頼カテゴリに必須の引数です。

u

証明書は認証または署名に使用できます。

-i root_CA_path

ルート CA ファイルのパスを指定します。パスには証明書名も含める必要があります。証明書の有効な拡張子には、.cert、.cer、.pem などがあります。

注: ファイルパスにスペースがある場合は、そのパスを引用符で囲んでください。

-d certificate_database_directory

証明書データベースが入っているディレクトリのパスを指定します。

注: ファイルパスにスペースがある場合は、そのパスを引用符で囲んでください。

例: 証明書データベースへのルート CA の追加

```
certutil -A -n "My Root CA" -t "C,," -i C:\certificates\cacert.cer -d C:\certdatabase
```

証明書データベースへのサーバ証明書の追加

SSL を使用した通信を有効にするには、サーバ証明書を証明書に追加します。Mozilla Network Security Services (NSS) certutil アプリケーションを使用します。これはポリシー サーバで使用できます。

注: 以下の手順では、タスクを実行するための具体的なオプションおよび引数について詳しく説明します。NSS ユーティリティのオプションおよび引数の全リストについては、[NSS プロジェクト ページ](#)にある Mozilla マニュアルを参照してください。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

次の手順に従ってください:

1. コマンドプロンプトから、ポリシー サーバインストール bin ディレクトリに移動します。

例 : `C:\Program Files\CA\SiteMinder\bin`

注: Windows には固有の `certutil` ユーティリティがあります。NSS ユーティリティの `bin` ディレクトリから作業するようにしてください。誤って Windows `certutil` ユーティリティを実行していることがあります。

2. 以下のコマンドを実行します。

```
certutil -A -n alias -t trust_arguments -i server_certificate_path -d
certificate_database_directory
```

-A

証明書データベースに証明書を追加します。

-n alias

証明書の別名を指定します。

注: 別名にスペースがある場合は、その別名を引用符で囲んでください。

-t trust_arguments

信頼指数を指定します。各証明書には、3つの使用可能な信頼カテゴリがあります。これらのカテゴリを表記する順番は、「SSL、電子メール、オブジェクト署名」です。それぞれのカテゴリ位置に、以下の属性指数を0個以上使用することができます。

p

有効なピア。

P

信頼されたピア。この指数は **p** を意味します。

重要: これは SSL 信頼カテゴリに必須の指数です。

-i server_certificate_path

サーバ証明書のパスを指定します。パスには証明書名も含める必要があります。証明書の有効な拡張子には、`.cert`、`.cer`、`.pem` などがあります。

注: ファイルパスにスペースがある場合は、そのパスを引用符で囲んでください。

`-d certificate_database_directory`

証明書データベースが入っているディレクトリのパスを指定します。

注: ファイルパスにスペースがある場合は、そのパスを引用符で囲んでください。

NSS によって、証明書データベースにサーバ証明書が追加されます。

例: 証明書データベースへのサーバ証明書の追加

```
certutil -A -n "My Server Certificate" -t "P,," -i C:%certificates%servercert.cer -d C:%certdatabase
```

証明書データベース内の証明書の一覧表示

証明書が証明書データベースにあることを確認するには、**Mozilla Network Security Services (NSS)** certutil アプリケーションを使用します。ポリシーサーバにはこのツールが含まれています。

注: 以下の手順では、タスクを実行するための具体的なオプションおよび引数について詳しく説明します。NSS ユーティリティのオプションおよび引数の全リストについては、[NSS プロジェクト ページ](#)にある **Mozilla** マニュアルを参照してください。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドラインウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドラインウィンドウを開きます。

次の手順に従ってください:

1. コマンドプロンプトから、ポリシー サーバインストール bin ディレクトリに移動します。

例: `C:%Program Files%CA%SiteMinder%bin`

注: Windows には固有の certutil ユーティリティがあります。NSS ユーティリティの bin ディレクトリから作業するようにしてください。誤って Windows certutil ユーティリティを実行していることがあります。

2. 以下のコマンドを実行します。

```
certutil -L -d certificate_database_directory
```

-L

証明書データベース内のすべての証明書を一覧表示します。

-d *certificate_database_directory*

証明書データベースが入っているディレクトリのパスを指定します。

注: ファイルパスにスペースがある場合は、そのパスを引用符で囲んでください。

このコマンドによって、証明書を証明書データベースに追加する際に指定した、ルート CA の別名、サーバ証明書の別名、および信頼属性が表示されます。

例: 証明書データベース内の証明書の一覧表示

```
certutil -L -d C:¥certdatabase
```

ポリシー サーバから証明書データベースへの参照の設定

SSL を使用してユーザ ディレクトリと通信するには、証明書データベースを参照するようにポリシー サーバを設定します。

次の手順に従ってください:

1. ポリシーサーバ管理コンソールを起動します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [データ] タブをクリックします。
3. Netscape 証明書データベース ファイルのフィールドに、証明書データベース ファイルへのパスを入力します。

例: C:¥certdatabase¥cert8.db

注: key3.db ファイルは、cert8.db ファイルと同じディレクトリ内にある引数があります。

4. ポリシー サーバを再起動します。

ポリシー サーバは、SSL を使用してユーザ ディレクトリと通信できません。

ODBC ストレージ オプションの設定

以下に対して ODBC データ ソースを設定するには、ODBC コンテキスト依存ストレージコントロールを使用します。

- ポリシーストア
- キーストア
- 監査ログ
- セッションストア

注: ODBC データ ソースの設定の詳細については、「ポリシー サーバインストールガイド」を参照してください。

ODBC データソースの設定

ODBC データソースを設定する方法

1. [データ ソース情報] フィールドで、ODBC データ ソースの名前を指定します。このフィールドには、ODBC フェールオーバーを有効にする複数のデータ ソースの名前を入力できます。

データソース情報

ODBC データソースの名前を入力します。このフィールドには、フェールオーバーを有効にする複数のデータ ソースの名前を入力できます。

ユーザ名

必要に応じて、そのデータベースにアクセスするすべての権限を付与されたデータベースアカウントのユーザ名を入力します。

パスワード

データベースアカウントのパスワードを入力します。

パスワードの確認入力

確認のために、データベースアカウントのパスワードをもう一度入力します。

最大接続数

同時に使用できる、データベースごとの ODBC 接続の最大数を入力します。

2. [ODBC 接続のテスト] をクリックして、入力したパラメータが正しいかどうか、および接続が作成できたかどうかを確認します。

ODBC フェールオーバーの設定

複数の ODBC データソースを使用していて、フェールオーバーを設定する場合は、データソース名をカンマで区切って [データソース情報] フィールドに入力します。たとえば、「SiteMinder Data Source1,SiteMinder Data Source2」と入力すると、ポリシー サーバは Data Source1 を最初に検索します。SiteMinder Data Source1 が応答しない場合は、自動的に SiteMinder Data Source2 を検索します。

注: 上記の方法を使用して、ポリシー ストア、キー ストア、セッション ストア、監査ログとして使用されているデータ ソースのフェールオーバーを設定できます。

SQL クエリによって返されるレコードの最大数の設定

多くのレコード数を返す SQL クエリによって、ポリシー サーバがハングまたはクラッシュする場合があります。この状況を管理するため、返されるレコードの数が指定した最大値を超過した場合に SMPS ログに警告メッセージを出力することができます。

最大数を設定するには、レジストリ キー **MaxResults** を追加して、その値を 1 以上に設定します。クエリによって返されるレコードの数が **MaxResults** によって指定された上限値以上である場合、ポリシー サーバは警告を SMPS ログに出力します。**MaxResults** がゼロに設定されるか定義されなかった場合、警告メッセージは出力されません。

レジストリ キー **MaxResults** を追加しても、返されるレコードの数が変更されるわけではありません。このキーを追加することによって、結果の数が指定した上限を超えた場合にユーザに警告されます。このフィードバックを使用して、必要に応じて SQL クエリを修正し、返されるレコードの数を調整できます。

SQL クエリによって返されるレコード数の制限を設定する方法

1. レジストリ キー MaxResults を手動で追加します。

Windows

レジストリ キー MaxResults を以下の場所に追加します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds
\ODBCProvider
```

Solaris

以下の行を sm.registry ファイルに追加します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds
\ODBCProvider=35921
MaxResults=0x1; REG_DWORD
```

2. MaxResults に 1 以上の値を割り当てます。

タイムアウト用の ODBC レジストリ設定の設定

さまざまな状況での ODBC データベースおよびポリシー サーバ間の接続に対するコントロール タイムアウトに基づいてリストされるパラメータ。Windows と UNIX 上のキーは以下の場所から入手できます。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Database
```

"LoginTimeout"

データベースに接続するのに許可されている時間。

"QueryTimeout"

クエリが完了するまで 30 秒間待ちます。クエリがこの時間内に完了しないとき、キャンセルのリクエストがデータベースに送信されます。ODBC ユーザディレクトリについては、クエリ タイムアウトはユーザディレクトリ オブジェクト Searchtimeout で上書きされます。この値は XPSExplorer を使用して設定します。

"ConnectionHangWaitTime"

ポリシー サーバが接続をハングしたとしてマークする前の秒数。この値は、QueryTimeout または SearchTimeout の値の 2 倍より大きくする必要があります。

"ConnectionTimeout"

接続上の最大の待機時間。クエリ タイムアウトまたはログイン タイムアウトが適用される場合、それらの値は接続タイムアウトに優先されます。

テキスト ファイル ストレージ オプションの設定

テキスト ファイル ストレージ オプションを使用すると、ポリシー ストア 監査ログの格納先となるテキスト ファイルを設定できます。

テキスト ファイルを指定するには、[ファイル名] フィールドにファイルのフルパスを入力するか、[参照] ボタンをクリックして必要なディレクトリを参照し、希望するファイルをクリックするか、そのファイルの名前を入力します。

ODBC の監査データ インポート ツール

ポリシー サーバは、監査データを ODBC データベースに格納したり、ファイルに出力したりできます。smauditimport ツールは、SiteMinder 監査データ テキスト ファイルを読み取り、ODBC データベースにそのデータをインポートします。データベースは、5.x または 6.x 方式で監査ストアとして設定されています。

また、認証、許可、および管理データを、ODBC データベース内の対応するテーブルにインポートします。ODBC データベースに正常にインポートされた行の数はログに記録されます。ODBC データベースにインポートできない行については、その行番号がログに記録されます。

ポリシーまたはユーザ ストア内のフィールドに表示される文字 '['、']' または '¥' は、手前にエスケープ文字 '\¥'(円記号) を必要とします。これらの文字は、ユーザ名、レルム名などのフィールドで使用されているために出現します。

以下のレジストリ キーを設定して、これらの文字を自動的にエスケープします。

[HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder¥CurrentVersion¥LogConfig]

値のタイプ : DWORD VALUE

値の名前 : EscapeAuditFields

値のデータ : 1

[値のデータ] が 0 に設定される場合、またはキーが存在しない場合、エスケープはないので、操作は失敗します。

注: SiteMinder の一部のドキュメントでは、「監査」と「ログ記録」という用語はほとんど同じ意味で使われています。

テキストファイルへのより多くの監査データ ログの記録

ポリシー サーバはデフォルトで、監査データ ログをテキスト ファイルよりも ODBC データベースに多く記録します。デフォルトより多くの監査データ ログをテキスト ファイルに記録することで、ODBC データベースのデータ量に合わせるすることができます。そのためには、レジストリ キー "Enable Enhance Tracing" を追加し、その値を 1 に設定します。"Enable Enhance Tracing" を無効にするには、値をゼロ (デフォルト) に設定します。

テキストファイルにより多くの監査データ ログを記録する方法

1. レジストリ キー "Enable Enhance Tracing" を手動で追加します。

Windows

以下のキーを追加します。

```
TYPE=DWORD
¥netegrity¥SiteMinder¥CurrentVersion¥Reports
¥"Enable Enhance Tracing"
```

Solaris

以下の手順に従います。

- a. ファイル .../siteminder/registry/sm.registry を開きます。.
- b. 以下の行を検索します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder
¥CurrentVersion¥Reports=25089
```

c. この行の下に、以下を追加します。

```
"Enable Enhance Tracing"=0x1;    REG_DWORD
```

d. ファイルを保存して閉じます。

2. "Enable Enhance Tracing" を 1 に設定します。

注: "Enable Enhance Tracing" の値は、Entitlement Management Services (EMS) イベントのログ記録には影響しません。

ODBC の監査データインポートの前提条件

smauditimport ツールを実行する前に、以下の前提条件が満たされていることを確認してください。

- ポリシー サーバが Windows、Solaris、または Linux オペレーティング環境にインストールされている。

注: Solaris および Linux プラットフォームの場合は、smauditimport ツールを実行する前に nete_ps_env.ksh を実行します。

- ODBC データベースが 5.x または 6.x 方式で監査 (ログ) ストアとして設定されている。

注: ODBC データベースを監査 (ロギング) ストアとして設定する方法の詳細については、「ポリシー サーバインストールガイド」を参照してください。

- レジストリ キー "Enable Enhance Tracing" が 1 に設定されている。

ODBC データベースへの監査データのインポート

smauditimport ツールは、SiteMinder 監査データ テキスト ファイルを読み取り、ODBC データベースにインポートします。このツールは、ポリシー サーバインストールディレクトリ下の `¥bin` ディレクトリ内にあります。

重要: 監査データを ODBC データベースにインポートする前に、SiteMinder 5.x または 6.x 方式でデータベースを監査ストアとして設定する必要があります。SiteMinder スキーマを使用して ODBC データベースを設定する方法の詳細については、「ポリシー サーバインストールガイド」を参照してください。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

次の手順に従ってください:

1. ポリシー サーバがインストールされているコンピュータで、`siteminder_installation\bin` に移動します。

siteminder_installation

ポリシー サーバのインストールパスを指定します。

2. 以下のコマンドを実行します。

```
smauditimport audit_file dsn user_name user_password -f -v  
-bbulk_load_size -s5 | -s6 -anumber
```

audit_file

監査データを含むテキスト ファイルのパスと名前を指定します。

注: `smauditimport` ツールでは、監査データ テキスト ファイルの完全パス名を指定する必要があります。

dsn

ODBC データベースのデータ ソース名 (DSN) を指定します。

user_name

ODBC データベース管理者の名前を指定します。

user_password

ODBC データベース管理者のパスワードを指定します。

-a

(必須) ポリシー サーバの Enable Enhance Tracing レジストリ設定の値を指定します。この設定は、

`HKEY_LOCAL_MACHINE\Software\Netegrity\SiteMinder\Currentversion\Reports` に存在します。Windows オペレーティング環境では、この設定は Windows レジストリにあります。UNIX または Linux オペレーティング環境では、この設定は `sm.registry` ファイルにあります。この設定値は、このオプションで使用されている値に一致する必要があります。

例: `-a2` (Enable Enhance Tracing レジストリ設定に 2 を指定します)。

-f

(オプション) 監査データのインポート中にエラーが発生した場合に、行番号をログに記録し、処理を続行します。

デフォルト: -f オプションを指定しない場合、行番号をログに記録しますが、処理を停止します。

-v

(オプション) テキストファイル内のフィールドの数、数値フィールドの値が指定の範囲内にあるかどうか、およびデータベースへの接続を検証し、エラーを出力します。

注: `smauditimport` ツールを検証モードで実行するとき、データはデータベースにインポートされません。

-b `bulk_load_size`

(オプション) 読み取って ODBC データベースにインポートする行の数を指定します。

デフォルト: 100

注: -b オプションを使用して、Oracle データベースへ監査データをインポートするために `smauditimport` ツールを使用する場合は、[ODBC Oracle Wire Protocol Driver Setup] ダイアログで [Enable bulk load] オプションを設定しないでください。 [ODBC Oracle Wire Protocol Driver Setup] で [Enable bulk load] オプションが設定されている場合、一括ロード中に予期しない動作が発生します。

-s5 | -s6

(オプション) 5.x または 6.x スキーマのいずれかで監査ストアとして設定された ODBC データベースをサポートします。

デフォルト: 6.x スキーマで監査ストアとして設定された ODBC データベースをサポートします。

Netscape 証明書データベース ファイルの指定

LDAP ディレクトリを使用して、SSL 接続を介してポリシーやユーザ情報を保存している場合は、ポリシー サーバに、Netscape 証明書データベースファイルが含まれているディレクトリを示す必要があります。ディレクトリには、`cert8.db` ファイルと `key3.db` ファイルが含まれている必要があります。

証明書データベース ファイルをインストールする前に、そのコピーを作ります。オリジナルファイルの代わりに証明書データベース コピーを使用してください。また、現在 Netscape Communicator で cert8.db が使用されている場合には、その使用を中止してください。

[Netscape 証明書データベースファイル] フィールドに証明書データベースの名前を入力するか、ディレクトリツリーを検索して保存先のデータベースを選択します。このフィールドには、Active Directory ネームスペースを使用して管理 UI 内で設定される AD ユーザストアの値を入力する必要はありません。SSL 接続を確立する場合、AD ユーザストアではネイティブの Windows 証明書リポジトリが使用されます。

詳細情報:

[監査ログ用の個別のデータベースの設定 \(P. 35\)](#)

第 4 章: ポリシー サーバの一般的な設定

このセクションには、以下のトピックが含まれています。

[ポリシー サーバの設定の概要 \(P. 61\)](#)

[ポリシー サーバの設定 \(P. 61\)](#)

ポリシー サーバの設定の概要

ポリシー サーバでは、その動作と実行の方法を決定するための多くの一般的な設定を、管理コンソールの [設定] タブで行うことができます。

- アクセス制御用の TCP ポート
- TCP ポートなどの管理設定と、アクティブでない状態時のタイムアウト
- 接続の設定
- RADIUS 設定
- パフォーマンスの設定
- OneView モニタの設定

ポリシー サーバの設定

ポリシー サーバの一般的な設定方法

1. ポリシーサーバー管理コンソールを起動します。

重要: Windows Server 2008 上でこのグラフィカル ユーザー インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [設定] タブをクリックします。

注: このタブ上での設定およびコントロールの詳細については、[ヘルプ] - [管理コンソールヘルプ] をクリックしてください。

3. 希望する設定を調整します。
4. 設定が完了したら、[適用] をクリックして設定を保存するか、[OK] をクリックして設定を保存し、管理コンソールを終了します。

アクセス制御の設定

ポリシー サーバは、認証、許可、および監査の目的で SiteMinder エージェントと通信する際に 3 つの異なる TCP ポートを使用します。

これらのエージェント通信ポートを有効または無効にしたり、各機能で使用する TCP ポートの番号を変更したりするには、[管理コンソールの設定] タブの [アクセス制御] グループ ボックスにあるコントロールを使用します。

ポリシー サーバ管理の設定

ポリシー サーバは、ブラウザベースのポリシー管理を可能にするため、TCP ポートを使用して管理 UI と通信します。

管理 UI との通信で使用する TCP ポート番号を有効化、無効化、または変更したり、管理がアクティブでないときのタイムアウト値を指定したりするには、[管理コンソールの設定] タブの [管理] グループ ボックスにあるコントロールを使用します。

ポリシー サーバの接続オプションの設定

ポリシー サーバスレッドの最大数と、ポリシー サーバへの接続のアイドルタイムアウトを指定するには、[管理コンソールの設定] タブの [接続オプション] グループ ボックスにあるコントロールを使用します。

ポリシー サーバのパフォーマンスの設定

ポリシー サーバのパフォーマンスを調整するキャッシュとスレッドを設定するには、[管理コンソールの設定] タブの [パフォーマンス] グループ ボックスを使用します。

RADIUS の設定

環境内の RADIUS コンポーネントのサポートを有効にする設定を指定するには、[管理コンソールの設定] タブの [RADIUS] グループ ボックスを使用します。

OneView モニタの設定

OneView モニタはデフォルトで、監視対象となるポリシー サーバ上でローカルに実行されます。

リモートで監視される他のポリシー サーバからの接続を受け入れるようにモニタを設定したり、クラスタ内のすべてのポリシー サーバを監視する集中監視用のリモートポリシー サーバを指定したりするには、[管理コンソールの設定] タブの [OneView モニタ] グループ ボックスを使用します。

SiteMinder ポリシー データ同期の再スケジュール

SiteMinder は、XPSSweeper ツールを使用してポリシー データを自動的に同期します。このツールの実行頻度を変更するには、以下のパラメータを設定します。

AutosweepSchedule

XPSSweeper プロセスを実行する日付と時刻 (時間と分) を指定します。

デフォルト : 月曜日の 08:30

制限 : 24 時間形式の GMT タイム ゾーン。エントリが複数ある場合は、カンマまたは空白で区切ります。

例 : Mon@13:30,Tue@14:00

注 : SiteMinder バイナリ ファイル (XPS.dll、libXPS.so、libXPS.sl) への書き込みアクセス許可がユーザにない場合は、管理者が管理 UI または XPSSecurity ツールを使用して、関連する XPS コマンドライン ツールを使用する権限を付与する必要があります。

次の手順に従ってください:

1. ポリシー サーバでコマンドラインを開き、以下のコマンドを入力します。

```
xpsconfig
```

ツールが起動し、このセッションのログ ファイルの名前が表示されます。また、選択項目のメニューが開きます。

2. 以下のコマンドを入力します。

```
xps
```

オプションのリストが表示されます。

3. 以下のコマンドを入力します。

```
8 (AutosweepSchedule)
```

XPSSweeper ツールの現在のスケジュールが表示されます。

4. 「C」と入力し、希望する日付と時刻を入力します。複数の日付または時刻を入力する場合は、それらをカンマまたは空白で区切ります。以下の形式を使用します。

```
Mon@13:30,Tue@14:00
```

新しい設定と古い設定が表示されます。追加した値は「保留中の値」として設定の下に表示されます。

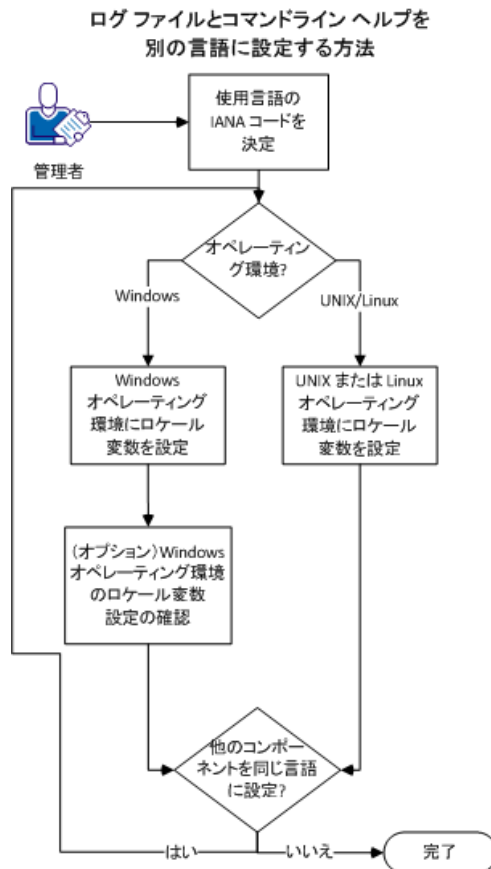
5. 以下の手順を実行します。
 - a. 2回「Q」と入力します。
 - b. 「L」と入力します。
 - c. 「Q」と入力して XPS セッションを終了します。変更が保存され、コマンドプロンプトが表示されます。

ログ ファイルおよびコマンドライン ヘルプの別の言語への設定

以下のコンポーネントは、ログ ファイル、およびその他の言語でのコマンドライン ヘルプをサポートします。

- ポリシー サーバ
- Web エージェント
- レポート サーバ
- CA SiteMinder Agent for SharePoint
- CA SiteMinder for Secure Proxy Server
- <エージェント>
- SiteMinder SDK で作成される任意のカスタム ソフトウェア。

以下の図は、ログ ファイル設定のワークフローおよび、別の言語へのコマンドライン ヘルプについて説明しています。



次の手順に従ってください:

1. [言語の IANA コードを決定します](#) (P. 66)。
2. 以下のいずれかの手順を使用して、オペレーティング環境用の環境変数を作成します。
 - [Windows オペレーティング環境上でロケール変数を設定します](#) (P. 68)。
 - [UNIX または Linux オペレーティング環境で、ロケール変数を設定します](#) (P. 70)。
3. (オプション) [ウィンドウ オペレーティング環境で、ロケール変数の設定を確認します](#) (P. 69)。
4. (オプション) 手順 1 ~ 3 を繰り返して、ユーザの環境内の他のコンポーネントを同じ言語に設定します。

ユーザの言語の IANA コードを決定します。

各言語にはそれぞれ一意のコードがあります。IANA (インターネット番号割当機関) は、これらの言語コードを割り当てます。言語コードをロケール変数に追加することで、ソフトウェアが表示する言語を変更します。ロケール変数を作成する前に、目的の言語に該当するコードを決定します。

以下の表は、このソフトウェアでサポートされている言語に対応する IANA コードのリストを示しています。

言語	IANA コード
ポルトガル語 (ブラジル)	pt_BR
フランス語	fr
ドイツ語	de
イタリア語	it
日本語	ja
韓国語	ko
中国語 (簡体字)	zh-Hans
スペイン語	es

注: IANA 言語コードのリストは、この[サードパーティ Web サイト](#)から利用可能です。

環境変数

環境変数は、ユーザのニーズに適合するように、ユーザがコンピュータをカスタマイズできる設定です。この環境変数の例には、以下のような項目があります。

- ダウンロードされたファイルを検索または格納するためのデフォルトディレクトリ。
- ユーザ名。
- 実行可能ファイルを検索する場所のリスト (パス)。

Windows オペレーティング環境ではグローバル環境変数を設定でき、これはコンピュータのすべてのユーザに適用されます。UNIX または Linux オペレーティング環境での環境変数は、各ユーザまたはプログラムに対して設定する必要があります。

ロケール変数を設定するには、以下のリストからユーザのオペレーティング環境用の手順を選択します。

- [Windows オペレーティング環境上でロケール変数を設定します \(P. 68\)](#)。
- [UNIX または Linux オペレーティング環境で、ロケール変数を設定します \(P. 70\)](#)。

Windows オペレーティング環境でのロケール変数の設定

以下のロケール変数は、ソフトウェアの言語設定を指定します。

`SM_ADMIN_LOCALE`

この変数を作成し、それを目的の言語に設定します。別の言語を使用する各コンポーネントで、この変数を設定します。たとえば、ポリシー サーバ、およびフランス語に設定されているエージェントがあると仮定します。それらのコンポーネントの両方で、この変数をフランス語に設定します。

注: インストールまたは設定プログラムでは、この変数は設定されません。

次の手順に従ってください:

1. [スタート] - [コントロールパネル] - [システム] - [システムの詳細設定] をクリックします。

[システムのプロパティ] ダイアログ ボックスが表示されます。

2. [詳細設定] タブをクリックします。
3. [環境変数] をクリックします。
4. [システム変数] セクションを見つけてから、[新規] をクリックします。

[新しいシステム変数] ダイアログ ボックスが、カーソルが [変数名] フィールドにある状態が表示されます。

5. 以下のテキストを入力します。

`SM_ADMIN_LOCALE`

6. [変数名] フィールドをクリックしてから、目的の [IANA 言語コード](#) (P. 66) を入力します。

7. [OK] をクリックします。

[新しいシステム変数] ダイアログ ボックスが閉じ、`SM_ADMIN_LOCALE` 変数がリストに表示されます。

8. [OK] を 2 回クリックします。

ロケール変数が設定されます。

9. (オプション) 手順 1 ~ 8 を繰り返して、他のコンポーネントを同じ言語に設定します。

Windows オペレーティング環境でのロケール変数値の確認

ロケール変数が設定される値は、随時変更できます。この手順は、変数を設定して、それが適切に設定されていることを確認した後に実行できます。

注: UNIX および Linux での変数の検証手順は、「[プロシージャの設定 \(P. 70\)](#)」にあります。

次の手順に従ってください:

1. 以下の手順で、コマンドライン ウィンドウを開きます。
 - a. [スタート] - [ファイル名を指定して実行] をクリックします。
 - b. 以下のコマンドを入力します。

```
cmd
```

- c. [OK] をクリックします。

コマンドライン ウィンドウが開きます。

2. 以下のコマンドを入力します。

```
echo %SM_ADMIN_LOCALE%
```

ロケールが次の行に表示されます。たとえば、言語がドイツ語に設定される場合、以下のコードが表示されます。

```
de
```

ロケール変数の値が確認されます。

UNIX または Linux オペレーティング環境でのロケール変数の設定

以下のロケール変数は、ソフトウェアの言語設定を指定します。

SM_ADMIN_LOCALE

この変数を作成し、それを目的の言語に設定します。別の言語を使用する各コンポーネントで、この変数を設定します。たとえば、ポリシー サーバ、およびフランス語に設定されているエージェントがあると仮定します。それらのコンポーネントの両方で、この変数をフランス語に設定します。

注: インストールまたは設定プログラムでは、この変数は設定されません。

次の手順に従ってください:

1. 目的のコンポーネントを実行しているコンピュータにログインします。
2. コンソール（コマンドライン）ウィンドウを開きます。
3. 以下のコマンドを入力します。

```
export SM_ADMIN_LOCALE=IANA_language_code
```

以下の例のコマンドは、言語をフランス語に設定します。

```
export SM_ADMIN_LOCALE=fr
```

ロケール変数が設定されます。

4. （オプション）以下のコマンドを入力して、ロケール変数が適切に設定されていることを確認します。

```
echo $SM_ADMIN_LOCALE
```

ロケールが次の行に表示されます。たとえば、言語がドイツ語に設定される場合、以下のコードが表示されます。

```
de
```

5. （オプション）手順 1 ~ 4 を繰り返して、他のコンポーネントを同じ言語に設定します。

第 5 章: 証明書データストアの管理

このセクションには、以下のトピックが含まれています。

[証明書廃棄リスト \(CRL\) の更新 \(P. 71\)](#)

[OCSP の更新 \(P. 73\)](#)

[証明書のキャッシュリフレッシュ間隔 \(P. 84\)](#)

[デフォルトの廃棄猶予期間 \(P. 84\)](#)

証明書廃棄リスト(CRL)の更新

SiteMinder は、証明書データストア内の証明書に対する証明書検証を必要とする機能を提供します。12.52 SP1 では、フェデレーション機能は証明書データストアを使用します。これらの機能には HTTP-Artifact バックチャンネルの保護、SAML メッセージの確認、および SAML メッセージの暗号化が含まれます。証明書データストアは証明書廃棄リスト (CRL) を使用して、有効性チェックを実装できます。

証明書データストアは、CRL の場所を参照します。デフォルトでは、SiteMinder は CRL の更新を確認しません。更新を確認するには、CRL 更新プログラム (CRLUpdater) を有効にします。

以下の点を考慮します。

- SiteMinder は各 CRL の NextUpdate 日付を使用して、格納された場所を参照する時間と CRL を再ロードする時間を決定します。SiteMinder はまた、その日付を使用して証明書を無効にすべきかどうかを決定します。
- デフォルトでは、SiteMinder は 1 時間に 1 回、更新を確認します。デフォルトの頻度を増やすことができます。
- CRL 更新の有効化は、ローカルのポリシーサーバ管理設定です。環境内で 1 つのポリシーサーバに対してのみ CRL 更新を有効にします。
- CRL のロードが失敗した場合、CRL が正常にロードするまで、すべての証明書が無効としてマーキングされます。

以下の手順に従います。

1. ポリシー サーバ ホスト システムにログインします。
2. XPSConfig ユーティリティを起動します。
3. 「CDS」と入力し、Enter キーを押します。
4. EnableCRLUpdater の番号を入力し、Enter キーを押します。
5. 「C」と入力して Enter キーを押します。
6. 「yes」と入力して Enter キーを押します。
7. 「Q」を入力します。
8. 以下のいずれかの操作を実行します。
 - 以下の手順に従って、SiteMinder による更新確認の頻度を変更します。
 - a. DefaultCRLUpdaterSleepPeriod の番号を入力し、Enter キーを押します。
 - b. 「C」と入力して Enter キーを押します。
 - c. 新規の値を入力し、Enter キーを押します。
 - d. ユーティリティを終了します。
 - ユーティリティを終了して、デフォルトの頻度のままにします。
9. ポリシー サーバを再起動します。

CRL リストの更新がスケジューリングされます。

デフォルトの CRL 更新間隔の変更

更新間隔は証明書データストアが CRL を再ロードする頻度です。格納された CRL ファイルに NextUpdate 値が含まれない場合は、更新間隔を設定します。データストアは、CRL ファイルを SiteMinder 設定に追加したときに指定した場所で、更新された CRL を検索します。

次の手順に従ってください:

1. 管理 UI にログインします。
2. [インフラストラクチャ] - [X509 証明書管理] - [CDS 設定] を選択します。
3. 更新間隔の新しい値を入力します。デフォルトは 1 日です。
4. [保存] をクリックします。

新しい値は、更新と更新の間の更新間隔の時間です。

OCSP の更新

SiteMinder は、証明書データストア内の証明書に対する証明書検証を必要とする機能を提供します。12.52 SP1 では、フェデレーション機能は証明書データストアを使用します。これらの機能には HTTP-Artifact バックチャンネルの保護、SAML メッセージの確認、および SAML メッセージの暗号化が含まれます。

証明書の有効性を確認するために、証明書データストアは OCSP サービスを使用できます。OCSP は、証明書検証を要求に応じて提供するために証明機関 (CA) が提供する HTTP サービスを使用します。

デフォルトでは、SiteMinder は、証明書データストア内の証明書の取り消しステータスを確認しません。OCSP レスポンドャによって取り消しステータスを確認するには、OCSP アップデータユーティリティ (OCSPUpdater) を使用します。有効にすると、OCSPUpdater は設定された OCSP レスポンドャの取り消しステータスを 5 分おきに確認します。このデフォルトの頻度は設定可能です。

OCSPUpdater の設定は以下のコンポーネントに依存します。

- SMocsp.conf ファイル

OCSPUpdater は、OCSP レスポンダ設定に関する SMocsp.conf ファイルを使用します。証明書を発行する各証明機関 (CA) には、それぞれ独自の OCSP レスポンダがあります。SMocsp.conf ファイルで、証明書データストアに各 CA 証明書に対するすべての OCSP レスポンダを含めます。

SMocsp.conf ファイルは OCSPUpdater を使用するために必要となります。

注: SMocsp.conf ファイルは、SiteMinderX.509 証明書認証方式がそれ独自の OCSP 実装を設定するために使用するファイルと同じです。

- XPSConfig ユーティリティ

XPSConfig によって、OCSPUpdater の動作をカスタマイズできます。たとえば、それを有効にしたり、更新の頻度を設定することができます。そのカスタマイズは OCSPUpdater を実行するポリシー サーバに固有のもので、SiteMinder の展開において 1 つのポリシー サーバ上のみで OCSPUpdater を有効にします。

OCSP と CRL チェックとの間のフェールオーバー

証明書データストアは OCSP から CRL 検証へのフェールオーバーをサポートします。CRL と OCSP チェックを設定した場合、両者の間のフェールオーバーを有効にすることが可能です。

SiteMinder フェデレーション機能は、拡張が証明書内にあっても、フェールオーバーを設定して証明書の配布ポイントの拡張をサポートしません。

フェールオーバーの詳細については、「[ポリシー サーバ設定ガイド](#)」の証明書の有効性チェックのセクションを参照してください。

OCSP の更新スケジュール

OCSP の更新は XPSConfig を使用してスケジュールされます。

重要: OCSP 更新の有効化は、ローカルのポリシー サーバ管理設定です。SiteMinder の展開においては、1 つのポリシー サーバ上のみで OCSPUpdater を有効にします。

OCSP の更新をスケジュールする方法

1. ポリシー サーバ ホスト システムにログインします。
2. XPSConfig ユーティリティを起動します。
3. 「CDS」と入力し、Enter キーを押します。
4. EnableOCSPUpdater の番号を入力し、Enter キーを押します。
5. 「C」と入力して Enter キーを押します。
6. 「yes」と入力して Enter キーを押します。
7. 「Q」を入力します。
8. 以下のタスクのいずれかを実行します。
 - SiteMinder が更新をチェックする頻度を変更します。
 - a. DefaultOCSPUpdaterSleepPeriod の番号を入力し、Enter キーを押します。
 - b. 「C」と入力して Enter キーを押します。
 - c. 新規の値を入力し、Enter キーを押します。
 - d. ユーティリティを終了します。
 - ユーティリティを終了して頻度をデフォルト値のままにします。
9. ポリシー サーバを再起動します。

OCSP の廃棄ステータスの更新がこれでスケジュールされました。更新を開始するには、フェデレーション シングル サインオン トランザクションが発生する必要があります。OCSPUpdater が有効になっているポリシー サーバで、この最初のトランザクションを実行します。展開内の他のポリシー サーバは後のトランザクションを作成できます。

OCSP 更新のための SMocsp.conf ファイルの変更

OCSPUpdater は、レスポンス設定値に対して SMocsp.conf ファイルを使用します。このファイルは、X.509 証明書認証方式がそれ自体の OCSP 実装を設定するために使用するファイルと同じものです。ただし、認証方式用のすべての設定がフェデレーションに適用されるとは限りません。

SMocsp.conf ファイルは `siteminder_home/config` ディレクトリに存在する必要があります。

重要: SMocsp.conf ファイル内の指定された CA のエントリは、OCSP が有効であることを意味しません。EnableOCSPUpdater 設定を「Yes」に設定する必要もあります。

ファイルを編集する方法

1. `siteminder_home/config` に移動します。
2. テキストエディタでファイルを開きます。
3. 以下のタスクのいずれかを実行します。
 - 既存の OCSPResponder エントリの変更
 - 証明書マッピングにおいて IssuerDN と一致する IssuerDN ごとに一意の OCSPResponder エントリを追加します。

重要: [発行者 DN] にレスポンスレコードがない場合、または設定が無効な場合は、ポリシーサーバは証明書の有効性を確認せずに、証明書操作を実行します。

4. 更新に影響するファイル設定を編集します。

重要: OCSP が有効になっている 1 つのポリシーサーバで、1 つのファイルのみ存在できます。
5. ファイルを保存します。
6. OCSPUpdater がすでに有効になっている場合は、ポリシーサーバを再起動します。それ以外の場合は、以下の `smkeytool` コマンドを使用して、編集された SMocsp.conf ファイルをロードできます。

```
smkeytool -loadOCSPConfigFile
```

詳細情報:

[フェデレーションによって使用される SMocsp.conf 設定 \(P. 77\)](#)

フェデレーションによって使用される SMocsp.conf 設定

SMocsp.conf ファイルを変更する際のガイドラインを以下に示します。

- 設定の名前はすべて大文字と小文字が区別されるわけではありません。エントリの大文字と小文字が区別されるかどうかは特定の設定によって決まります。
- ファイル内の設定が空白のままの場合、ポリシー サーバはエラーメッセージを送信します。メッセージは、エントリが無効であることを示します。ポリシー サーバは設定を無視します。設定が意図的に空白になっている場合は、メッセージを無視してかまいません。
- 設定の名前の先頭にスペースを含めることはしないでください。

SMocsp.conf ファイルで、フェデレーションに対して以下の設定を指定できます。

OCSPResponder

必須です。エントリが OCSP レスポンダレコードであることを示します。各 OCSP レスポンダレコードは、OCSPResponder で始まる必要があります。

IssuerDN

必須です。証明書発行者の DN を指定します。この値は、ファイル内の各 OCSP レスポンダレコードのラベルとなります。

エントリ：証明書内の発行者 DN 値。

AlternateIssuerDN

任意です。セカンダリ IssuerDN または逆の DN を指定します。

ResponderLocation

任意です。OCSP レスポンダ サーバの場所を示します。

ResponderLocation 設定または AIAExtension 設定を使用できますが、以下の点に注意してください。

- ResponderLocation 設定が空白のままか、または SMocsp.conf ファイルにない場合、AIAExtension 設定は「YES」に設定します。また、AIA 拡張が証明書に含まれている必要があります。
- ResponderLocation 設定に値があり、AIAExtension が YES に設定されている場合、ポリシー サーバは検証に ResponderLocation を使用します。ResponderLocation 設定は AIAExtension より優先されます。
- この設定に指定された OCSP レスポンダがダウンしており、AIAExtension が YES に設定されている場合、認証は失敗します。ポリシー サーバは、この証明書の AIA 拡張で指定されたレスポンダの使用は試しません。

場所を入力する際は、*responder_server_url:port_number* の形式で入力します。

レスポンダ サーバの URL およびポート番号を入力します。

AIAExtension

任意です。ポリシー サーバが検証情報を見つけるために証明書の Authority Information Access (AIA) 拡張を使用するかどうかを指定します。

AIAExtension または ResponderLocation の設定を使用できますが、以下の警告に注意してください。

- AIAExtension が「YES」に設定され、ResponderLocation が設定されていない場合、ポリシー サーバは検証用に証明書の AIA 拡張を使用します。この拡張は、証明書内に存在する必要があります。
- AIAExtension が YES に設定され、ResponderLocation 設定にも値がある場合、ポリシー サーバは検証に ResponderLocation を使用します。ResponderLocation 設定は AIAExtension より優先されます。
- AIAExtension が「NO」に設定される場合、ポリシー サーバは ResponderLocation 設定を使用します。AIAExtension の値が存在しても、ポリシー サーバはそれを無視します。

「YES」または「NO」を入力します。

デフォルト：NO

HttpProxyEnabled

任意です。Web サーバではなくプロキシサーバに OCSP リクエストを送信するようにポリシーサーバに指示します。

「YES」または「NO」を入力します。

デフォルト：NO

HttpProxyLocation

任意です。プロキシサーバの URL を指定します。この値は、HttpProxyEnabled が YES に設定されている場合のみ必須です。

http://で始まる URL を入力します。

注：https://で始まる URL は入力しないでください。

HttpProxyUserName

任意です。プロキシサーバに対するログイン認証情報のユーザ名を指定します。このユーザ名はプロキシサーバの有効なユーザの名前である必要があります。この値は、HttpProxyEnabled が YES に設定されている場合のみ必須です。

英数字の文字列を入力します。

HttpProxyPassword

任意です。プロキシサーバユーザ名に対応するパスワードを指定します。この値はクリアテキストで表示されます。この値は、HttpProxyEnabled が YES に設定されている場合のみ必須です。

英数字の文字列を入力します。

SignRequestEnabled

任意です。生成された OCSP リクエストに署名するようポリシーサーバに指示します。署名機能を使用する場合はこの値を Yes に設定します。

この値は、ユーザ証明書の署名とは関係がなく、OCSP リクエストにのみ関係があります。

注：この設定は、OCSP レスポンダで署名されたリクエストが必要とされる場合のみ必須です。

「YES」または「NO」を入力します。

デフォルト：NO

SignDigest

任意です。OCSP リクエストを署名するときにポリシー サーバが使用するアルゴリズムを指定します。この設定では大文字と小文字は区別されません。この設定は、SignRequestEnabled 設定が YES に設定された場合のみ必須です。

次のいずれかのオプションを入力します：SHA1、SHA224、SHA256、SHA384、SHA512

デフォルト：SHA1

エイリアス

任意です。OCSP リクエストに署名するキー/証明書ペアのエイリアスを指定します。OCSP リクエストは、OCSP レスポンダに送信されます。このキー/証明書ペアは、SiteMinder 証明書データ ストア内にある必要があります。

注：このエイリアスは、SignRequestEnabled 設定が YES に設定された場合のみ必須です。

小文字の ASCII 英数文字を使用してエイリアスを入力します。

IgnoreNonceExtension

任意です。OCSP リクエストに乱数を含めないようにポリシー サーバに指示します。乱数（一度使用される数字）は、レスポンスの再利用を防ぐため認証リクエスト内に含まれることがある一意の数です。このパラメータを Yes に設定すると、OCSP リクエストに乱数が含まれないようになります。

「YES」または「NO」を入力します。

デフォルト：NO

PrimaryValidationMethod

任意です。ポリシー サーバで証明書の検証に使用するプライマリ検証方法が OCSP または CRL であるかを示します。この設定は、EnableFailover 設定が YES に設定された場合のみ必須です。

「OCSP」または「CRL」を入力します。

デフォルト：OCSP

EnableFailover

OCSP と CRL の証明書検証方法間でフェールオーバーするように、ポリシー サーバに指示します。

「YES」または「NO」を入力します。

デフォルト： NO

ResponderCertAlias

フェデレーションに対してのみ必須です。OCSP レスポンスの署名を検証する証明書のエイリアスを指定します。ポリシー サーバによってレスポンスの署名の検証を実行するには、この設定のエイリアスを指定してください。指定しない場合、CA 発行者には利用できる OCSP 設定がありません。

注: ポリシー サーバは、X.509 証明書の認証に対してこの設定を使用しません。

エイリアスを指定する文字列を入力します。

SMocsp.conf ファイルがロードされると、それぞれの発行者に OCSP 設定があるかどうかを確認できます。以下のメッセージはステータスメッセージの一例です。

SMocsp.conf ファイルがロードされました。

以下の発行者エイリアスに対して OCSP 設定が追加されました:

```
ocspcert  
ocspcert1  
ocspcert2
```

ステータス メッセージ内の発行者エイリアスは、CA 証明書をデータストアに追加するときに、管理 UI で指定したエイリアスを参照します。発行者エイリアスがリストにない場合は、SMocsp.conf および cds.log ファイルを確認します。ログ ファイルは `siteminder_home¥log` にあります。

RevocationGracePeriod

フェデレーションに対してのみオプションです。失効した後の証明書の無効化を遅らせるための期間（日数）を指定します。OCSP 猶予期間によって、設定が突然機能しなくならないように証明書を更新する時間が与えられます。値 0 は、証明書が失効すると直ちに無効になることを示します。

このフィールドに値を指定しない場合、ポリシー サーバは管理 UI で設定するデフォルトの廃棄猶予期間を使用します。デフォルトの設定は、[インフラストラクチャ] - [X509 証明書管理] - [証明書管理] を選択して確認できます。

デフォルト : 0

OCSP の無効化

SMocsp.conf ファイルから発行者エントリを削除することにより、特定の CA に対する OCSP 設定を無効にします。OCSPUpdater を無効にする場合は、以前に有効にされたファイルからエントリをすべて削除します。

次の手順に従ってください:

1. テキストエディタで SMocsp.conf ファイルを開きます。SMocsp.conf ファイルは `siteminder_home/config` ディレクトリに存在します。
2. SMocsp.conf ファイルから関連する発行者エントリを削除します。
3. `smkeytool` ユーティリティを使用して、以下のコマンドを入力します。

```
smkeytool -loadOCSPConfigFile
```

特定の CA 発行者のための OCSP は無効です。

OCSP が無効の場合の CA 証明書の追加

OCSPUpdater を無効にした場合、指定した発行者が SMocsp.conf ファイル内にエントリがあっても、ポリシーサーバではその同じ発行者の証明書が追加されません。証明書を追加しようとした場合、ポリシーサーバはエラーメッセージを記録します。OCSP は発行者に対して設定されるのでエラーが発生しますが、OCSPUpdater は有効になりません。そのため、廃棄ステータスの確認を実行できません。同じ発行者で証明書を追加しようとした場合、追加は失敗します。

エラーを引き起こさずに CA 証明書を追加する方法

1. テキストエディタで SMocsp.conf ファイルを開きます。SMocsp.conf ファイルは `siteminder_home/config` ディレクトリに存在します。
2. 関連する CA の設定を削除します。
3. `XPConfig` を使用して、`EnableOCSPUpdater` を「Yes」に設定し、再度 OCSP を有効にします。
4. コマンドラインで以下のコマンドを入力して、SMocsp.conf ファイルをロードします。

```
smkeytool -loadOCSPConfigFile
```
5. `EnableOCSPUpdater` パラメータを、元の「No」にリセットします。

証明書のキャッシュリフレッシュ間隔

証明書のキャッシュリフレッシュ間隔は、証明書データストアがポリシーストアの証明書データを更新する頻度を示します。証明書データはメモリにキャッシュされ、SiteMinder のパフォーマンスを向上させます。データが現在のものになるようにメモリ内の情報をリフレッシュします。

次の手順に従ってください:

1. 管理 UI にログインします。
2. [インフラストラクチャ] - [X509 証明書管理] - [CDS 設定] を選択します。
3. 証明書のキャッシュリフレッシュ間隔の新しい値を秒単位で入力します。デフォルトは 300 秒です。
4. [保存] をクリックします。

リフレッシュ間隔が設定されます。

デフォルトの廃棄猶予期間

デフォルトの廃棄猶予期間は、証明書が廃棄されたときから、証明書が無効になるときまでの遅延日数です。猶予期間中 SiteMinder では、廃棄された証明書をそれが無効になるまで使用できます。証明書が無効になった後は、それはアクティブではなくなり、SiteMinder ではそれを使用できません。

このデフォルト猶予期間は CRL および OCSP レスポンダに適用されます。システムに CRL を追加するときに CRL の猶予期間の値を指定しない場合、SiteMinder ではデフォルトの猶予期間を使用します。SMocsp.conf ファイル内の OCSP 猶予期間を設定しない場合、SiteMinder ではデフォルトの猶予期間を使用します。CRL または OCSP 用にそれぞれ猶予期間を設定した場合、それがこのデフォルト猶予期間値より優先されます。

次の手順に従ってください:

1. 管理 UI にログインします。
2. [インフラストラクチャ] - [X509 証明書管理] - [CDS 設定] を選択します。

3. 廃棄猶予期間の新しい値を入力します。デフォルトは0です。それは証明書が廃棄にされると直ちに無効になることを意味します。
4. [保存] をクリックします。

取り消し猶予期間が定義されました。

第 6 章: ポリシー サーバのスーパーユーザ パスワードの変更

このセクションには、以下のトピックが含まれています。

[スーパーユーザパスワードの概要 \(P. 87\)](#)

[ポリシー サーバのスーパーユーザパスワードの変更 \(P. 87\)](#)

スーパーユーザパスワードの概要

スーパーユーザとは、ポリシー サーバのインストール処理で自動的に設定される管理者アカウントです。スーパーユーザのパスワードは管理コンソールの [スーパーユーザ] タブから変更できます。

注: 以前に管理 UI を使用してスーパーユーザを無効にした場合は、このダイアログ ボックスの [スーパーユーザ アカウント] グループ ボックスでパスワードを変更しても、スーパーユーザは有効になりません。

ポリシー サーバのスーパーユーザパスワードの変更

スーパーユーザ アカウントのパスワードを変更する方法

1. ポリシーサーバー管理コンソールを起動します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [スーパーユーザ] タブをクリックします。

注: このタブ上での設定およびコントロールの詳細については、[ヘルプ] - [管理コンソールヘルプ] をクリックしてください。

3. [古いパスワード] フィールドに、スーパーユーザの現在のパスワードを入力します。

4. [新しいパスワード]フィールドに、スーパーユーザの新しいパスワードを入力します。

注: SiteMinder のスーパーユーザ管理者のパスワードには、パイプ記号（「|」）や不等号記号（「>」または「<」）は使用できません。

5. [パスワードの確認入力] フィールドに、新しいパスワードをもう一度入力します。

6. [適用] をクリックしてスーパーユーザに対する変更を保存するか、[OK] をクリックして設定を保存し、コンソールを終了します。

注: スーパーユーザアカウントのパスワードの変更は、ポリシー サーバプロセスを再起動しなくても有効になります。

第 7 章: ポリシー サーバ ログの設定

このセクションには、以下のトピックが含まれています。

[ポリシー サーバによるロギングの概要 \(P. 89\)](#)

[ポリシー サーバ ログの設定 \(P. 89\)](#)

[システム ログへの問題記録のレポート \(P. 97\)](#)

[証明書データストアのログ設定 \(P. 98\)](#)

[syslog にイベントを記録する方法 \(P. 100\)](#)

[Windows オペレーティング環境でアサーション属性のログ記録を有効にする方法 \(P. 105\)](#)

[UNIX または Linux オペレーティング環境でアサーション属性のログ記録を有効にする方法 \(P. 109\)](#)

ポリシー サーバによるロギングの概要

ポリシー サーバのログ ファイルには、ポリシー サーバのステータスに関する情報が記録されます。また、オプションで、ログ ファイル内の認証 イベント、許可 イベント、およびその他のイベントに関する、レベル設定可能な監査情報が記録されます。ポリシー サーバを RADIUS サーバとして設定している場合は、RADIUS アクティビティのログが RADIUS ログ ファイルに記録されます。

これらのログは管理コンソールの [ログ] タブで設定します。

ポリシー サーバ ログの設定

ポリシー サーバ ログを設定する方法

1. ポリシーサーバ管理コンソールを起動します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [ログ] タブをクリックします。

注: このタブ上での設定およびコントロールの詳細については、[ヘルプ] - [管理コンソールヘルプ] をクリックしてください。

3. [ポリシー サーバ ログ] および [ポリシー サーバの監査ログ] グループボックスに示されている設定を調整して、ポリシー サーバ ログの場所、ロールオーバー特性、および監査ログに必要なレベルを設定します。
4. ポリシー サーバを RADIUS サーバとして設定している場合は、[RADIUS ログ] グループボックスに示されている設定を調整します。
5. [適用] をクリックして、変更内容を保存します。

ポリシー ストア オブジェクトに対して管理者が行った変更の記録

デフォルトでは、ポリシー ストア オブジェクトへの SiteMinder 管理者変更は、`siteminder_home\audit` にある XPS テキスト ファイルのセットに書き込まれます。

以下の例に示すとおり、監査ログはテキスト ファイルとして保存されます。

```
policy_server_home/audit/xps-process_id-start_time-audit_sequence.file_type
```

各監査ログ ファイルの名前には、以下の情報が含まれます。

process_id

監査対象イベントに関連付けられているプロセスの数を示します。

開始時間

トランザクションが開始された時刻を以下の形式で示します。

YYYYMMDDHHMMSS

年が 4 桁、時刻が 24 時間形式で表記されます。

例：20061204133000

audit_sequence

監査対象イベントのシーケンス番号を示します。

file_type

以下のいずれかのイベント タイプを示します。

access

以下のアクセス イベントを含む監査ログ ファイルを示します。

- 管理 UI またはレポート サーバが登録される
- 管理 UI またはレポート サーバが他のユーザの代わりにプロキシとして動作する
- リクエストしたアクションについて管理者がアクセスを拒否される

audit

以下のイベントを含む監査ログ ファイルを示します。

- オブジェクトが変更される (XPS ツールまたは 管理 UI を使用して)
- 管理者レコードが作成、変更、または削除される

txn

以下のトランザクション イベントを含む監査ログ ファイルを示します。

- XPS ツールが、オブジェクトへの変更を開始、コミット、または拒否する

注: SiteMinder バイナリ ファイル (XPS.dll、libXPS.so、libXPS.sl) への書き込みアクセス許可がユーザにない場合は、管理者が 管理 UI または XPSecurity ツールを使用して、関連する XPS コマンドライン ツールを使用する権限を付与する必要があります。

デフォルトの動作を変更する方法

1. ポリシー サーバ ホスト システムにアクセスします。
2. コマンドラインセッションを開き、以下のコマンドを入力します。

```
xpsconfig
```

ツールが起動し、このセッションのログ ファイルの名前が表示されます。また、選択項目のメニューが開きます。

3. 以下のコマンドを入力します。

```
xps
```

オプションのリストが表示されます。

4. 以下のコマンドを入力します。

```
1
```

現在のポリシー ストア 監査設定が表示されます。

5. 「C」と入力します。

注: このパラメータは、**TRUE** または **FALSE** の値を使用します。値を変更すると、2つの状態が切り替わります。

更新されたポリシー ストア 監査設定が表示されます。新しい値は「保留中の値」としてリストの下部に表示されます。

6. 以下の手順を実行します。
 - a. 2回「Q」と入力します。
 - b. 「Q」と入力して XPS セッションを終了します。
変更が保存され、コマンドプロンプトが表示されます。

古いログ ファイルを自動的に処理する方法

SiteMinder ポリシー サーバでは、以下のいずれかのスクリプトをカスタマイズすることによって、古いログ ファイルが自動的に処理されるように設定できます。

- Harvest.bat (Windows)
- Harvest.sh (UNIX または Linux)

以下のいずれかのイベントが発生すると、スクリプトが実行されます。

- XPSAudit プロセスが開始するとき (以下のオプションを使用して)

CLEANUP

ディレクトリ内のログ ファイルを一度にすべて処理します。

- ログ ファイルがロールオーバーされるとき常に
- XPSAudit プロセスが終了するとき

ロールオーバーまたは終了中、ファイルは名前別に 1 つずつ処理されます。

ファイルを処理するスクリプトは自由にカスタマイズできます。たとえば、ファイルを削除したり、データベースに移動したり、別の場所へアーカイブしたりするようにスクリプトを変更することもできます。

注: このスクリプトはあくまでも例として提示しています。CA ではサポートされていません。

古いログ ファイルを自動的に処理するには、以下の手順に従います。

1. ポリシー サーバで以下のディレクトリを開きます。

```
policy_server_home/audit/samples
```

2. 使用しているオペレーティング システムに合ったスクリプトをテキスト エディタで開き、コピーを以下のディレクトリに保存します。

```
policy_server_home/audit/Harvest.extension
```

注: ファイルの名前を変更したり、指定とは異なる場所にファイルを保存したりしないでください。

3. 自分のニーズに沿ってスクリプトをカスタマイズするためのガイドとして、スクリプトの中で注釈を使用してください。
4. カスタマイズしたスクリプトを保存し、テキスト エディタを終了します。

SiteMinder 管理監査イベントをレポートに含める方法

SiteMinder レポートサーバと監査データベースがある場合、管理監査イベントを収集するようにポリシーサーバを設定できます。このデータは、監査データベースにインポートします。これにより、生成するあらゆるレポートに含めることができます。

SiteMinder ポリシーサーバにはサンプルの Perl プログラムがインストールされており、ニーズに合わせてカスタマイズできます。

SiteMinder レポートに管理監査イベントを含めるには、以下の手順に従います。

1. 以下の方法で、ポリシーサーバ上のサンプルスクリプトをコピーします。

- a. 以下のディレクトリを開きます。

`policy_server_home¥audit¥samples`

注: 以下のディレクトリが `policy_server_home` 変数のデフォルトの場所です。

- C:¥Program Files¥ca¥siteminder (Windows)
 - /opt/ca/siteminder (UNIX、Linux)
- b. 以下のファイルを探します。
 - Harvest.bat (Windows 用)
 - Harvest.sh (UNIX、Linux 用)
 - ProcessAudit.pl
 - Categories.txt

- c. 上記のファイルを以下のディレクトリにコピーします。

`policy_server_home¥audit`

2. (オプション) ProcessAudit.pl スクリプトをカスタマイズします。

3. 次回にスケジュールされた XPSAudit コマンドの実行の後に、監査ログのコピーがカンマ区切り値 (CSV) 形式で作成され、.TMP ファイルとして以下のディレクトリに格納されます。

`policy_server_home¥audit_R6tmp`

注: .tmp ファイルに手動で生成される必要があるイベントがある場合は、`policy_server_home¥audit` ディレクトリで以下のコマンドを実行します。

`ProcessAudit.pl <Transaction id>`

smobjlog4 データベース テーブルには、以下の 11 の属性と値が含まれています。最初の 8 つのみが .TMP ファイルに生成されます。

<code>sm_timestamp</code>	DATE DEFAULT SYSDATE NOT NULL,
<code>sm_categoryid</code>	INTEGER DEFAULT 0 NOT NULL,
<code>sm_eventid</code>	INTEGER DEFAULT 0 NOT NULL,
<code>sm_hostname</code>	VARCHAR2(255) NULL,
<code>sm_sessionid</code>	VARCHAR2(255) NULL,
<code>sm_username</code>	VARCHAR2(512) NULL,
<code>sm_objname</code>	VARCHAR2(512) NULL,
<code>sm_objoid</code>	VARCHAR2(64) NULL,
<code>sm_fielddesc</code>	VARCHAR2(1024) NULL,
<code>sm_domainoid</code>	VARCHAR2(64) NULL,
<code>sm_status</code>	VARCHAR2(1024) NULL

4. ポリシー サーバの上記のディレクトリから、監査データベースをホストしているサーバに .TMP ファイルをコピーします。
5. .TMP ファイルの CSV 形式の内容をデータベース スキーマにマップするため、以下のファイルのいずれか 1 つを作成します。
 - `control_file_name.ctl` (Oracle データベースの制御ファイル)
 - `format_file_name.fmt` (SQL Server データベースの形式ファイル)

注: 詳細については、データベース ベンダーが提供するマニュアルまたはオンライン ヘルプを参照してください。

6. 監査データベースをホストしているサーバで、以下のコマンドのうち、データベースのタイプに適したほうのコマンドを実行します。

- sqlldr (Oracle データベース用)
- bcp (SQL Server データベース用)

注: 詳細については、データベースベンダーが提供するマニュアルまたはオンラインヘルプを参照してください。

7. コマンドが完了したら、レポートサーバを使用して、管理イベントのレポートを生成します。

管理監査イベントはレポートの中に表示されます。

Windows で ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする

SiteMinder 監査ログをテキストファイルとして保存する場合、それらのファイルにはデフォルトで、利用可能なフィールドの部分的なリストが含まれます。監査ログが記録されるテキストファイルに利用可能なフィールドをすべて含める場合は (ODBC 監査データベースと同じように)、ポリシーサーバにレジストリキーを追加できます。

ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする方法

1. レジストリエディタを開きます。
2. 以下の場所を展開します。
`HKEY_LOCAL_MACHINE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Reports\`
3. 以下の名前を持つ新しい DWORD 値を作成します。
`Enable Enhance Tracing`
4. この値を 1 に設定します。この設定を将来無効にする場合は、値を 0 に戻します。
5. ポリシーサーバを再起動します。

ODBC 監査ログの内容が、テキストベースの監査ログに表示されます。

Solaris で ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする

SiteMinder 監査ログをテキスト ファイルとして保存する場合、それらのファイルにはデフォルトで、利用可能なフィールドの部分的なリストが含まれます。監査ログが記録されるテキスト ファイルに利用可能なフィールドをすべて含める場合は（ODBC 監査データベースと同じように）、ポリシー サーバにレジストリ キーを追加できます。

ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする方法

1. 以下のファイルを開きます。

```
sm.registry
```

2. 次の行を検索します。

```
-  
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Re  
ports=25089
```

3. この行の下に、以下のテキストで構成される新しい行を追加します。

```
- Enable Enhance Tracing= 0x1; REG_DWORD
```

注: この機能を将来無効にする場合は、0x1 を 0x0 に変更します。

4. ポリシー サーバを再起動します。

ODBC 監査ログの内容が、テキストベースの監査ログに表示されます。

システム ログへの問題記録のレポート

監査ログを準備または実行しているときに発生する可能性のある例外について、その情報を Windows イベント ログ ビューアに記録するようポリシー サーバを設定できます。この設定により、デバッグ ログが無効になっている場合に、本稼働環境でそのような情報を見逃さないようにすることができます。この機能を設定するには、CategoryCount レジストリ キーの値を 7 に設定します。

CategoryCount レジストリ キーは次の場所にあります。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application  
\SiteMinder
```

これらのイベントは、イベント ログ カテゴリの ObjAuditLog および AccessAuditLog の下に記録されます。

オブジェクトが作成、更新、または削除されると、SiteMinder はオブジェクト イベントをコールします。SiteMinder オブジェクト監査ログを準備/実行する際に発生した例外は、Windows イベント ビューアの「ObjAuditLog」カテゴリ下に記録されます。

アクセス イベントはユーザ関連アクティビティによって発生し、認証、許可、管理、アフィリエイトのアクティビティのコンテキストで呼び出されます。SiteMinder アクセス監査ログを準備/実行する際に発生した例外は、Windows イベント ビューアの「AccessAuditLog」カテゴリ下に記録されます。

証明書データストアのログ設定

証明書データストア ログを設定して、デフォルトの設定を変更します。デフォルトのログは、以下のように設定されています。

- ログ情報は以下のファイルに記録されます。

`cds.log`

このログは `siteminder_home¥log` にあります。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- 情報およびエラー メッセージが含まれます。
- ファイルサイズが 500 KB に達した時点で、ロールオーバーし、バックアップを作成します。
- 最も古いものが消去される前に、10 個のバックアップ コピーを保存します。

次の手順に従ってください:

1. `siteminder_home¥config¥properties` に移動し、以下のファイルを開きます。

`cdslog4j.properties`

注: log4j の詳細については、Apache の Web サイトを参照してください。

2. 以下の1つ以上の処理を実行します。

- ログインレベルを変更するには、以下のパラメータの終わりで値を更新します。

```
log4j.logger.com.ca.CertificateDataStore=
```

重要: パラメータから以下を削除しないでください。さもないとログインが失敗します。

```
, CertificateDataStore
```

- 出力場所またはログ名を変更するには、以下のパラメータの終わりでファイルパスを更新します。

```
log4j.appender.CertificateDataStore.File=
```

- ファイルがロールオーバーし、バックアップが作成されるサイズを変更するには、以下のパラメータの終わりで値を更新します。

```
log4j.appender.CertificateDataStore.MaxFileSize=
```

- 最も古いものが消去される前に保存されるバックアップコピーの数を変更するには、以下のパラメータの終わりで値を更新します。

```
log4j.appender.CertificateDataStore.MaxBackupIndex=
```

注: SiteMinder サポートから要請がない限り、[ClientDispatcher] セクション内の設定は変更しないでください。これらの設定はデバッグ時にのみ使用されます。

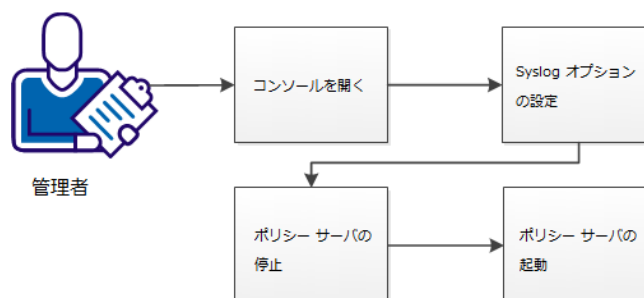
3. ファイルを保存します。

証明書データストアのログが設定されました。

syslog にイベントを記録する方法

管理者は、サポートされているオペレーティング環境で **syslog** にポリシーサーバのイベントを記録できます。以下の図は、**syslog** にイベントを記録する方法を示しています。

Syslog にイベントを記録する方法



次の手順に従ってください:

1. [コンソールを開きます](#) (P. 101)。
2. [syslog オプションを設定します](#) (P. 102)。
3. 以下の手順でポリシー サーバを再起動します。
 - [ポリシー サーバを停止します](#) (P. 104)。
 - [ポリシー サーバを起動します](#) (P. 105)。

コンソールを開く

設定を変更するためにコンソールを開きます。

次の手順に従ってください:

1. システムで X ウィンドウ サーバが実行されていることを確認します。
2. ターミナル ウィンドウを開きます。
3. 以下のコマンドを使用して DISPLAY 変数を設定します。

```
export DISPLAY=IP_address:0.0
```

IP_address

コンソール ウィンドウが表示される場所の IP アドレスを指定します。コンソールへの接続に使用しているシステムの IP アドレスを使用します。

例： (IPV4) 192.168.1.1

例： (IPV6) 2001:DB8::/32

4. コンソールをホストしているシステムにログインします。
5. 以下のディレクトリに移動します

```
installation_directory/siteminder/bin
```

installation_directory

ポリシー サーバがインストールされているファイル システム上の場所を指定します。

デフォルト： /opt/CA/siteminder

6. 以下のコマンドを実行してコンソールを開きます。

```
./smconsole
```

syslog オプションの設定

コンソールで **syslog** オプションを設定して、どのイベントを **syslog** に記録するかを指定します。

注: **syslog** とその設定の詳細については、この [Web サイト](#) を参照してください。

次の手順に従ってください:

1. 以下の手順に従って、**syslog** への記録を有効にします。
 - a. [データ] タブをクリックします。
 - b. [データベース] ドロップダウンリストをクリックし、[監査ログ] を選択します。
 - c. [ストレージ] ドロップダウンリストをクリックし、[Syslog] を選択します。
2. [優先順位] フィールドのテキストを選択し、以下のリストから目的の値を入力します。

優先度

syslog に記録されたイベント優先度を指定します。以下のいずれかの値を指定します。

- LOG_EMERG
- LOG_ALERT
- LOG_CRIT
- LOG_ERR
- LOG_WARNING
- LOG_NOTICE
- LOG_INFO
- LOG_DEBUG

デフォルト : LOG_INFO

3. [機能] フィールドのテキストを選択し、以下のリストから目的の値を入力します。

ファシリティ

オペレーティング環境内のどのイベントを **syslog** に記録するかを指定します。以下のいずれかの値を指定します。

- LOG_AUTH
- LOG_AUTHPRI
- LOG_CRON
- LOG_DAEMON
- LOG_FTP
- LOG_KERN
- LOG_LPR
- LOG_MAIL
- LOG_NEWS
- LOG_SYSLOG
- LOG_USER
- LOG_UUCP
- LOG_LOCAL0
- LOG_LOCAL1
- LOG_LOCAL2
- LOG_LOCAL3
- LOG_LOCAL4
- LOG_LOCAL5
- LOG_LOCAL6
- LOG_LOCAL7

デフォルト : LOG_AUTH

- (オプション) 以下のフィールドのテキストを置換します。

テキスト

syslog に記録するイベントに含まれるテキストを指定します。たとえば、**tiger** という単語を指定すると、**tiger** という単語が含まれるイベントがすべて syslog に記録されます。

デフォルト : Siteminder

- [OK] をクリックします。

コンソールが閉じられ、syslog オプションが設定されます。

UNIX ポリシー サーバの停止

ポリシー サーバを停止すると、以下の結果になります。

- ポリシー サーバが、環境から一時的に削除されます。
- 許可または認証の判断が必要なエージェントは、停止されているポリシー サーバにコンタクトできません。それらのエージェントは、引き続き利用可能なほかのポリシー サーバに接続できます。
- すべてのログ記録アクティビティは停止します。

次の手順に従ってください:

- ポリシー サーバをホストしているシステムに、最初にポリシー サーバをインストールしたのと同じユーザアカウントでログインします。
- 以下のいずれかのアクションを実行して、すべてのポリシー サーバプロセスを停止します。
 - 管理コンソールを開き、[ステータス] タブをクリックし、[停止] ボタンをクリックします。
 - 以下のスクリプトを使用します。 バプロセスが自動的に再起動されないように、このスクリプトによって UNIX エグゼクティブも停止されます。

```
installation_path/siteminder/stop-all
```

ポリシー サーバは、UNIX エグゼクティブの全アクティビティのログを `installation_directory/log/smexec.log` ファイルに記録します。ログのエントリは、常に既存のログファイルに追加されます。

UNIX ポリシー サーバの起動

ポリシー サーバを開始すると、以下のような結果になります。

- エージェントはポリシー サーバに許可または認証の決定を問い合わせます。
- ログ記録が開始されます。

以下のいずれかのアクションを実行して、すべてのポリシー サーバプロセスを開始します。

- 管理コンソールを開き、[ステータス] タブをクリックし、[開始] ボタンをクリックします。
- 以下のスクリプトを使用します。このスクリプトは、UNIX エグゼクティブも開始します。

```
installation_path/siteminder/start-all
```

ポリシー サーバは、UNIX エグゼクティブの全アクティビティのログを `installation_directory/log/smexec.log` ファイルに記録します。ログのエントリは、常に既存のログファイルに追加されます。

Windows オペレーティング環境でアサーション属性のログ記録を有効にする方法

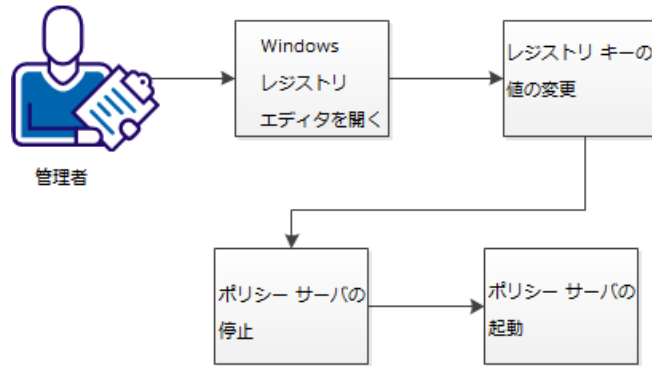
アサーション属性に関する情報を監査ログに記録できます。これらのログはセキュリティ監査、または調査時に使用します。イベントのタイプによって、ログに記録される情報が決まります。アサーション属性のログ記録を有効にすると、以下のイベントが記録されます。-

- すべてのアサーション生成
- すべてのアサーション消費
- 成功したすべての認証
- 失敗したすべての認証
- 試行されたすべての認証
- すべてのアプリケーション アクセス

アサーション属性のログ記録は、デフォルトでは無効になっています。ポリシー サーバでアサーション属性のログ記録を有効にします。-

以下の図は、アサーション属性のログ記録を有効にする方法を示しています。

アサーション属性のログ記録を有効にする方法



次の手順に従ってください：

1. [Windows レジストリ エディタを開きます](#) (P. 106)。
2. レジストリ キーの値を変更します。
3. 以下の手順でポリシー サーバを再起動します。
 - a. [ポリシー サーバを停止します](#) (P. 108)。
 - b. [ポリシー サーバを起動します](#) (P. 109)。

Windows レジストリ エディタを開く

ポリシー サーバをホストするシステム上で Windows レジストリ エディタを開くことにより、この設定を変更します。

次の手順に従ってください：

1. [スタート] - [ファイル名を指定して実行] をクリックします。
2. [名前:] フィールドに以下のテキストを入力します。
`regedit`
3. [OK] をクリックします。

Windows のレジストリ エディタが開きます。

レジストリ キーの値の変更

以下のレジストリ キーは、属性アサーション ログ記録を制御します。

拡張トレースの有効化

属性アサーションが監査ログに記録されるかどうかを示します。値 2 はログ記録を有効にします。値 3 はログ記録を有効にし、ユーザの認証方式を記録します。値 4 は、DeviceDNA™ による拡張セッションのログ記録を有効にします。

制限： 0、2、3、4

デフォルト： 0（ログ記録無効）

次の手順に従ってください：

1. レジストリ エディタで、以下の項目を展開します。

HKEY_LOCAL_MACHINE

2. [Software] - [Netegrity] - [SiteMinder] - [Currentversion] - [Reports] の順にクリックします。

3. 以下のレジストリ キーを見つけます。

Enable Enhance Tracing

4. キーを右クリックしてから、[Modify] を選択します。

5. 以下のタスクのいずれかを実行します。

- アサーション属性のログ記録を有効にするには、値を 2 に変更します。
- アサーション属性および使用する認証方式のログ記録を有効にするには、値を 3 に変更します。
- DeviceDNA™ による拡張セッションのログ記録を有効にするには、値を 4 に変更します。
- アサーション属性のログ記録を無効にするには、値を 0 に変更します。

6. [OK] をクリックします。

7. レジストリ エディタを閉じます。

Enable Enhance Tracing レジストリ キーの値が変更されます。

Windows ポリシー サーバの停止

続行前にポリシー サーバを停止します。ポリシー サーバを停止すると、以下の結果になります。

- ポリシー サーバが、環境から一時的に削除されます。
- 許可または認証の判断が必要なエージェントは、停止されているポリシー サーバにコンタクトできません。それらのエージェントは、引き続き利用可能なほかのポリシー サーバに接続できます。
- すべてのログ記録アクティビティは停止します。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
注: 管理者権限を持ったアカウントを使用します。
2. [スタート] - [プログラム] - [SiteMinder] - [SiteMinder ポリシー サーバ管理コンソール] をクリックします。
3. [停止] ボタンをクリックします。
4. [OK] をクリックします。
ポリシー サーバは停止し、コンソールは閉じます。

Windows ポリシー サーバの起動

ポリシー サーバを起動します。ポリシー サーバを起動すると、以下の結果になります。

- エージェントは、許可または認証のためにポリシー サーバに接続します。
- ログ記録が開始されます。

次の手順に従ってください：

1. [スタート] - [すべてのプログラム] - [SiteMinder] - [SiteMinder ポリシー サーバ管理コンソール] をクリックします。
[ステータス] タブが選択された状態でコンソールが開きます。
2. [開始] ボタンをクリックします。
3. [OK] をクリックします。
ポリシー サーバが起動します。

UNIX または Linux オペレーティング環境でアサーション属性のログ記録を有効にする方法

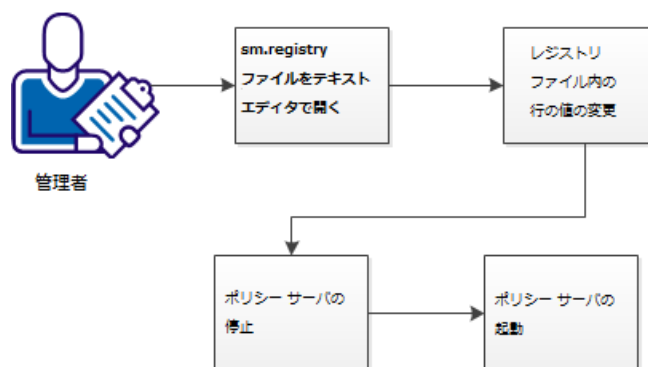
アサーション属性に関する情報を監査ログに記録できます。これらのログはセキュリティ監査、または調査時に使用します。イベントのタイプによって、ログに記録される情報が決まります。アサーション属性のログ記録を有効にすると、以下のイベントが記録されます。 -

- すべてのアサーション生成
- すべてのアサーション消費
- 成功したすべての認証
- 失敗したすべての認証
- 試行されたすべての認証
- すべてのアプリケーション アクセス

アサーション属性のログ記録は、デフォルトでは無効になっています。ポリシー サーバでアサーション属性のログ記録を有効にします。 -

以下の図は、アサーション-属性のログ記録を有効にする方法を説明しています。

アサーション属性のログ記録を有効にする方法



次の手順に従ってください:

1. [sm.registry ファイルをテキストエディタで開きます](#) (P. 111)。
2. レジストリ ファイル内の行の値が変更されます。
3. 以下の手順でポリシー サーバを再起動します。
 - a. [ポリシー サーバを停止します](#) (P. 104)。
 - b. [ポリシー サーバを起動します](#)。(P. 105)

sm.registry ファイルをテキスト エディタで開く

テキスト エディタを使用して `sm.registry` ファイルを開くことにより、UNIX または Linux オペレーティング環境で、この設定を変更します。`sm.registry` ファイルはポリシー サーバに格納されます。

次の手順に従ってください:

1. 以下のディレクトリに移動します。

`Installation_Directory/registry`

`installation_directory`

ポリシー サーバがインストールされているファイル システム上の場所を指定します。

デフォルト : `/opt/CA/siteminder`

2. テキスト エディタで以下のファイルを開きます。

`sm.registry`

設定を変更できます。

レジストリ ファイル内の行の値の変更

sm.registry ファイル内の以下のエントリは、属性アサーションのログ記録を制御します。

拡張トレースの有効化

属性アサーションが監査ログに記録されるかどうかを示します。値 2 はログ記録を有効にします。値 3 はログ記録を有効にし、ユーザの認証方式を記録します。値 4 は、DeviceDNA™ による拡張セッションのログ記録を有効にします。

制限：0、2、3、4

デフォルト：0（ログ記録無効）

次の手順に従ってください：

1. sm.registry ファイルで以下のセクションを見つけます。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Reports=
```

2. Reports セクションで以下の行を見つけます。

```
Enable Enhance Tracing= 0; REG_DWORD
```

3. 値を 0 から以下のいずれかの値に変更します。
 - 2（ログ記録を有効にします）
 - 3（ログ記録を有効にし、認証方式を記録します）
 - 4（DeviceDNA™ による拡張されたセッション保証のログ記録を有効にします）
4. sm.registry ファイル内の行が、以下の例のいずれかと一致することを確認します。

```
Enable Enhance Tracing= 2; REG_DWORD
```

```
Enable Enhance Tracing= 3; REG_DWORD
```

```
Enable Enhance Tracing= 4; REG_DWORD
```

5. sm.registry ファイルへの変更を保存し、テキスト エディタを閉じます。レジストリ ファイル内の行の値が変更されます。

UNIX ポリシー サーバの停止

ポリシー サーバを停止すると、以下の結果になります。

- ポリシー サーバが、環境から一時的に削除されます。
- 許可または認証の判断が必要なエージェントは、停止されているポリシー サーバにコンタクトできません。それらのエージェントは、引き続き利用可能なほかのポリシー サーバに接続できます。
- すべてのログ記録アクティビティは停止します。

次の手順に従ってください:

1. ポリシー サーバをホストしているシステムに、最初にポリシー サーバをインストールしたのと同じユーザ アカウントでログインします。
2. 以下のいずれかのアクションを実行して、すべてのポリシー サーバプロセスを停止します。
 - 管理コンソールを開き、[ステータス] タブをクリックし、[停止] ボタンをクリックします。
 - 以下のスクリプトを使用します。 バプロセスが自動的に再起動されないように、このスクリプトによって UNIX エグゼクティブも停止されます。

```
installation_path/siteminder/stop-all
```

ポリシー サーバは、UNIX エグゼクティブの全アクティビティのログを `installation_directory/log/smexec.log` ファイルに記録します。ログのエントリは、常に既存のログファイルに追加されます。

UNIX ポリシー サーバの起動

ポリシー サーバを開始すると、以下のような結果になります。

- エージェントはポリシー サーバに許可または認証の決定を問い合わせます。
- ログ記録が開始されます。

以下のいずれかのアクションを実行して、すべてのポリシー サーバプロセスを開始します。

- 管理コンソールを開き、[ステータス] タブをクリックし、[開始] ボタンをクリックします。
- 以下のスクリプトを使用します。このスクリプトは、UNIX エグゼクティブも開始します。

```
installation_path/siteminder/start-all
```

ポリシー サーバは、UNIX エグゼクティブの全アクティビティのログを `installation_directory/log/smexec.log` ファイルに記録します。ログのエントリは、常に既存のログファイルに追加されます。

第 8 章：暗号化キーの設定と管理

このセクションには、以下のトピックが含まれています。

[ポリシー サーバの暗号化キーの概要 \(P. 116\)](#)

[キー管理の概要 \(P. 117\)](#)

[FIPS 140-2 アルゴリズム \(P. 118\)](#)

[導入されたエージェント キー \(P. 119\)](#)

[ダイナミック エージェント キーのロールオーバー \(P. 120\)](#)

[ダイナミック エージェント キーのロールオーバー \(P. 121\)](#)

[スタティック キー \(P. 123\)](#)

[セッションチケットキー \(P. 124\)](#)

[キー管理のシナリオ \(P. 125\)](#)

[r6.x ポリシーストア暗号化キーのリセット \(P. 131\)](#)

[r12.x ポリシーストア暗号化キーのリセット \(P. 135\)](#)

[エージェント キー生成の設定 \(P. 136\)](#)

[エージェント キーの管理 \(P. 137\)](#)

[セッションチケットキーの管理 \(P. 141\)](#)

[トラステッドホストの共有秘密キー \(P. 144\)](#)

ポリシー サーバの暗号化キーの概要

ポリシー サーバとエージェントは、暗号化キーを使用して、SiteMinder 環境のポリシー サーバとエージェントの間で転送される重要なデータの暗号化と復号化を行います。

- エージェントキーは、シングルサインオン環境のすべてのエージェントが読み込む SiteMinder cookie を暗号化するために使用されます。各エージェントは、他のエージェントによって暗号化された cookie を復号化する必要があるため、シングルサインオン環境のすべてのエージェントがエージェントキーを共有します。エージェントキーは、ポリシーサーバによって管理され、エージェントに定期的に配信されます。
- セッションチケットキーは、ポリシーサーバがセッションチケットを暗号化するために使用します。セッションチケットには、認証情報と、セッションに関連する他の情報（ユーザ認証情報など）が含まれています。エージェントは、セッションチケットを SiteMinder cookie に埋め込みますが、その内容にアクセスすることはできません。これは、エージェントが、ポリシーサーバの外に出ることがないセッションチケットキーにアクセスできないためです。

どちらのタイプのキーも、ポリシーサーバのキーストアに保存され、実行時にエージェントに配信されます。デフォルトでは、キーストアはポリシーサーバの一部ですが、必要に応じて、個別のキーストアデータベースを作成することもできます。

これらのキー以外に、次の特別なキーがあります。

- ポリシーストアキー - ポリシーストア内にある特定のデータを暗号化するために使用されます。ポリシーストアキーは、ディスク上のファイルに暗号化されて格納されます。ポリシーサーバが独自の技術を使用してポリシーストアキーを暗号化します。ポリシーストアキーは、ポリシーサーバのインストール時に指定した暗号化キーから取得されます。
- キーストアキー - 個別に設定されるキーストア内にあるエージェントキーやセッションチケットキーを暗号化するために使用されます。キーストアキーは、ポリシーストアキーを使用して暗号化されたレジストリ (または UNIX の同様の機能を持つ位置) に保存されます。

キー管理の概要

大規模な環境全体でキー情報を最新の状態に保つために、ポリシー サーバは、自動キー ロールオーバーメカニズムを提供します。同じキーストアを共有するポリシー サーバ環境でキーを自動的に更新することができます。自動キー変換により、キーの整合性も確保されます。

シングルサインオンに設定される SiteMinder エージェントに対して以下を実行します。

- キーストアを複製します。
- シングルサインオン環境内のすべての SiteMinder 環境にわたって複製ストアを共有します。

スタンドアロン キーストアが使用できないとポリシー サーバが判断した場合、使用可能かどうかを確認するためにキーストアへの再接続を試みます。接続が失敗する場合、ポリシー サーバは以下のことを行います。

- 一時停止の状態になり、キーストアがオンラインに戻るまで、確立された接続に対する新規リクエストをすべて拒否します。

一時停止された状態のポリシー サーバは、**SuspendTimeout** で指定された期間そのままの状態になります。その後、ポリシー サーバは正常にシャットダウンされます。**SuspendTimeout** がゼロの場合、キーストア接続が再確立されるまで、ポリシー サーバは一時停止の状態になります。

- エラーステータスを返し、**Web** エージェントが別のポリシー サーバにフェールオーバーできるようにします。
- 適切なエラーメッセージをログに記録します。

また、ポリシー サーバの起動時にキーストアが使用不可能である場合、そのポリシー サーバは正常にシャットダウンします。

キーを管理するには管理 UI を使用します。

FIPS 140-2 アルゴリズム

FIPS (Federal Information Processing Standards) 140-2 は、機密性は高いが機密扱いではないデータを保護するセキュリティシステム内で暗号化アルゴリズムを使用するための要件を規定します。SiteMinder には RSA の CryptoC ME v2.0 暗号化ライブラリが組み込まれています。このライブラリは、FIPS 140-2 (暗号化モジュールに関するセキュリティ要件) に適合していることが確認されています。このモジュールの認証証明書番号は 608 です。

SiteMinder の Java ベースの API は、FIPS 準拠の CryptoJ 暗号化ライブラリを使用しています。

SiteMinder は、FIPS 以前のモードまたは FIPS 専用モードで動作できます。暗号化の相違点として、SiteMinder が暗号化を適用する方法は両方のモードで同じですが、アルゴリズムが異なります。

FIPS 専用モードの SiteMinder は以下のアルゴリズムを使用します。

- キーを暗号化する AES キー ラップ
- チャンネルを暗号化する OFB モード (HMAC-SHA 256) の AES
- シングルサインオンを簡易化するために使用するトークンを暗号化する CBC モード (HMAC-SHA 224) の AES

SiteMinder のコア コンポーネントでは、暗号化されたデータが幅広く利用されます。

- Web エージェントは以下のものを暗号化します。
 - ポリシー サーバから取得したエージェント キーを使用する cookie
 - セッション キーを使用してポリシー サーバに送信されるデータ
 - ホスト キーを使用する共有秘密キー。暗号化された共有秘密キーはホスト設定ファイルに格納されます。

- ポリシー サーバは以下のものを暗号化します。
 - セッション キーを使用して Web エージェントに送信されるデータ
 - ホスト キーを使用するポリシー ストア キー
 - ポリシー ストア キーを使用するポリシー ストア内の機密データ
 - セッション チケット キーを使用するセッション仕様
 - セッション キーを使用して 管理 UI に送信されるデータ
 - セッション チケット キーを使用する、ユーザ ディレクトリ内のパスワード サービス データ

ポリシー ストアに格納される機密データの暗号化には、ポリシー ストア キーを使用します。このキーは、ポリシー ストアのインストール時に入力されるシード文字列から取得されます。ポリシー ストアもホスト キーで暗号化され、システムのローカル ファイルに格納されます。自動操作をサポートするため、ホスト キーはポリシー ストア コードに埋め込まれる固定キーです。エージェントは、この同じホスト キー メカニズムを使用して、それぞれの共有秘密キーのコピーを暗号化し、格納します。

セッション チケット キー（認証トークンを生成するためにポリシー サーバによって使用される）およびエージェント キー（cookie データを暗号化するために、主に Web エージェントによって使用される）は、ポリシー ストア（SiteMinder の設定によってはキー ストア）に暗号化された形で格納される暗号化キーです。これらのキーはポリシー ストア キーまたはキー ストア キーで暗号化されます。キー ストア キーはポリシー ストア内で暗号化されます。エージェントの共有秘密キー（エージェント認証および TLI ハンドシェイクで使用）も、その他の機密データと共に、ポリシー ストア キーで暗号化され、ポリシー ストアに格納されます。

導入されたエージェント キー

SiteMinder Web エージェントはエージェント キーを使用して、ユーザのブラウザに渡す前に cookie を暗号化します。SiteMinder cookie を受信すると、Web エージェントはエージェント キーを使用して cookie の内容を復号化します。キーは、ポリシー サーバと通信するすべての Web エージェントで、同じ値に設定してください。

ポリシー サーバは、次のタイプのエージェント キーを提供します。

- **ダイナミック キー**-ダイナミック キーはポリシー サーバのアルゴリズムにより生成され、接続されたポリシー サーバや関連する **SiteMinder Web** エージェントに配信されます。ダイナミック キーのロールオーバーは、定期的な実行や、管理 UI の [キー管理] ダイアログ ボックスを使用した実行が可能です。セキュリティ上の理由から、エージェント キーはこのタイプのキーにすることを勧めます。
- **スタティック キー**-スタティック キーは不変です。ポリシー サーバのアルゴリズムによる生成や、手動での入力が可能です。SiteMinder 環境では、ユーザのマシン上の **cookie** に長期間保存される情報を必要とする機能のサブセットに対して、このタイプのキーが使用されます。

注: スタティック エージェント キーは、常にインストール時に生成されます。また、エージェント キーとして使用する場合もしない場合も、スタティック キーは特定の他の製品機能 (ユーザ管理など) で使用されます。

詳細情報:

[ダイナミック エージェント キーのロールオーバー \(P. 120\)](#)

ダイナミック エージェント キーのロールオーバー

ダイナミック エージェント キーのロールオーバーは、FSS 管理 UI の [キー管理] ダイアログ ボックスで設定します。Web エージェントはキーの更新を確認するため、ポリシー サーバに定期的にポーリングします。キーが更新されている場合、Web エージェントはポーリング時に変更内容を取得します。デフォルトのポーリング間隔は 30 秒ですが、Web エージェントの **pspollinterval** パラメータを変更して設定することもできます。

注: Web エージェントのパラメータを変更する方法については、「[SiteMinder Web エージェント設定ガイド](#)」を参照してください。

ポリシー サーバでは、ダイナミック キーを定期的に生成するアルゴリズムを使用しています。これらのキーはキー ストアに保存されます。Web エージェントは、新しいキーを検出すると、それらをキー ストアから取得します。

ダイナミック エージェント キーのロールオーバー

管理 UI 内の動的なエージェント キー ロールオーバーを設定します。Web エージェントはキーの更新を確認するため、ポリシー サーバに定期的にポーリングします。キーが更新されている場合、Web エージェントはポーリング時に変更内容を取得します。デフォルト ポーリング時間は 30 秒ですが、Web エージェントの `pspollinterval` パラメータの変更によりデフォルトを変更できます。

注: Web エージェントのパラメータを変更する方法については、「[SiteMinder Web エージェント設定ガイド](#)」を参照してください。

ポリシー サーバでは、ダイナミック キーを定期的に生成するアルゴリズムを使用しています。これらのキーはキー ストアに保存されます。Web エージェントは、新しいキーを検出するとそれをキー ストアから取得します。

ダイナミック キーのロールオーバーで使用するエージェント キー

SiteMinder 環境では、以下のキーをダイナミック キーのロールオーバーで使用し、キー ストアで管理します。

- 前回キーは、現在の値の前にエージェント キーが使用していた、直前の値を持つダイナミック キーです。
- 現在キーは、現在のエージェント キーの値を持つダイナミック キーです。
- 予定キーは、エージェント キーのロールオーバーで現在キーとして使用される予定の、次回の値を持つダイナミック キーです。
- スタティック キー

ポリシー サーバがダイナミック エージェント キーのロールオーバーを処理すると、前回キーの値が現在キーの値に置き換えられます。また、現在キーの値は予定キーの値と置き換えられ、ポリシー サーバは予定キーの新しい値を生成します。

クライアントのブラウザから **cookie** を受信すると、**Web** エージェントはキーストアの現在キーを使用して **cookie** を復号化します。復号化された値が有効でなかった場合、**Web** エージェントは前回キーを使用し、必要に応じて予定キーも使用します。また、まだ更新されていないエージェントからの **cookie** を復号化したり、クライアントのブラウザから既存の **cookie** を復号化したりする際に、前回キーが必要な場合があります。更新されたエージェントが作成した **cookie** の場合でも、まだキーの更新をキーストアにポーリングしていないエージェントがその **cookie** を読み込む場合は、予定キーが必要です。

エージェント キーのロールオーバー間隔

指定した時間になると、エージェント キーのロールオーバー プロセスが開始されます。複数のポリシー サーバから複数のロールオーバーが実行されないようにするには、各サーバのロールオーバー待機時間を **30 分**以内に設定します。待機時間が過ぎても更新が実行されなかった場合、ポリシー サーバはキーを更新します。

すべてのポリシー サーバは、キーの更新を待ってからエージェントに対して新しいキーを処理します。単一のポリシー サーバでも、更新時間はロールオーバー用に指定した時間より長くなります (**30 分**以内)。

エージェント キーのロールオーバー プロセスは、**SiteMinder** の [エージェント キー管理] ダイアログ ボックスで指定した時間に開始され、**3 分**以内に終了します。この時間内に、ポリシー サーバに接続されたすべての **Web** エージェントが更新されたキーを受け取ります。

注: 複数の複製ポリシー サーバがある環境の場合、エージェント キーの配布には最大 **30 分**かかる場合があります。

スタティック キー

スタティック キーは、一定で変化しないデータを暗号化するために使用される文字列です。エージェントキーのロールオーバー機能を使用する SiteMinder 環境では、スタティック キーを使用して、長期間にわたってユーザ情報を管理できます。

以下のような SiteMinder の機能および状況で、スタティック キーを使用します。

- HTML フォーム認証方式におけるユーザの認証情報の保存

HTML フォーム認証方式を使用してユーザがその認証情報を保存できるように設定されている場合、ポリシー サーバはスタティック キーを使用してユーザの認証情報を暗号化します。

- ユーザ追跡

ユーザ追跡がオンになっている場合、ポリシー サーバはスタティック キーを使用してユーザ識別情報を暗号化します。

- 複数のキー ストアでのシングル サインオン

複数のキー ストアがある SiteMinder 環境では、スタティック キーをシングル サインオンに使用できます。この場合、SiteMinder エージェントはすべての cookie の暗号化にスタティック キーを使用します。

注: スタティック キーを変更した場合、変更する前のスタティック キーで作成された Cookie はすべて無効になります。このとき、ユーザは強制的に再認証され、ユーザの追跡情報は無効になります。また、シングル サインオンにスタティック キーを使用している場合、ユーザが別の cookie ドメインのリソースにアクセスしようとする、クレデンシャルが要求されます。

詳細情報:

[個別のキーストアがある複数のポリシーストア \(P. 130\)](#)

セッション チケット キー

ユーザが、保護されたリソースへ正常にログインした場合、ポリシー サーバはセッション チケットを作成します。セッション チケットは、ユーザ認証の有効期間を決定するためにポリシー サーバによって使用されます。セッション チケットはセッション チケット キーで暗号化され、エージェント ユーザ キャッシュ内にキャッシュされます。

アルゴリズムを使用してポリシー サーバにセッション チケット キーを生成させるか、あるいは SiteMinder の[キー管理]ダイアログ ボックスでセッション チケット キーを入力します。セキュリティ上の理由から、キーはランダムに生成することをお勧めします。

ただし、シングル サインオン環境で SiteMinder 実装に複数のキー ストアがある場合は、すべてのキー ストアに対して同一のセッション チケット キーを使用する必要があります。

詳細情報:

[セッション チケット キーの管理](#) (P. 141)

[キャッシュ管理の概要](#) (P. 167)

キー管理のシナリオ

シングルサインオンが必要な環境で、ポリシーサーバ、ポリシーストア、およびキーストアをどのように実装するかによって、キー管理には3つのシナリオがあります。以下にそのシナリオを示します。

- 共通のポリシーストアとキーストア

このシナリオでは、ポリシーサーバグループが1つのポリシーストアとキーストアを共有して、単一 cookie ドメインでアクセス制御とシングルサインオンを実現します。

ポリシーストアデータは、1つのポリシーストアに格納されます。キーデータは、1つのキーストアに格納されます。キーストアは、ポリシーストアの一部とすることも、個別のストアとすることもできます。

ポリシーストアとストアデータは、どちらもフェールオーバーのために複製することができます。複製は、ポリシーストア用に選択したデータベースまたはディレクトリタイプに基づいて設定する必要があります。複製方式については、使用しているデータベースまたはディレクトリのベンダーから提供されているマニュアルを参照してください。

- 共通のキーストアがある複数のポリシーストア

このシナリオでは、ポリシーサーバグループが別々のポリシーストアに接続し、1つのキーストアを共有して、複数の cookie ドメイン間のアクセス制御とシングルサインオンを実現します。

各ポリシーサーバグループのポリシーストアデータは、1つのポリシーストアに格納されます。すべてのポリシーサーバグループのキーデータは、1つのキーストアに格納されます。個別のキーストアにより、すべてのポリシーサーバに関連付けられたエージェントがキーを共有できるため、複数の個別 cookie ドメイン間のシングルサインオンが可能になります。

ポリシーストアとストアデータは、どちらもフェールオーバーのために複製することができます。複製は、ポリシーストア用に選択したデータベースまたはディレクトリタイプに基づいて設定する必要があります。複製方式については、使用しているデータベースまたはディレクトリのベンダーから提供されているマニュアルを参照してください。

- 複数のポリシーストアと複数のキーストア

このシナリオでは、各ポリシーサーバグループが1つのポリシーストアとキーストアを共有して、(各 cookie ドメインのポリシーサーバに個別のキーストアを実装することが望ましい) 複数の cookie ドメイン間のアクセス制御とシングルサインオンを実現します。

各ポリシーサーバグループのポリシーストアデータは、1つのポリシーストアに格納されます。各ポリシーサーバグループのキーデータは、1つのキーストアに格納されます。キーストアは、ポリシーストアの一部とすることも、個別のストアとすることもできます。同一のスタティックキーセットを使用することによって、すべての Web エージェント間でのシングルサインオンが実現されます。

ポリシーストアとストアデータは、どちらもフェールオーバーのために複製することができます。複製は、ポリシーストア用に選択したデータベースまたはディレクトリタイプに基づいて設定する必要があります。複製方式については、使用しているデータベースまたはディレクトリのベンダーから提供されているマニュアルを参照してください。

詳細情報:

[LDAP フェールオーバーの設定 \(P. 39\)](#)

[ODBC フェールオーバーの設定 \(P. 52\)](#)

キー管理に関する注意事項

企業のキー管理のシナリオを決定する際には、以下の点に注意してください。

- 複数のポリシーサーバが共通のキーストアを共有する環境でダイナミックキーを設定する場合は、エージェントキーを生成する単一のポリシーサーバを指定する必要があります。他のすべてのポリシーサーバでは、必ずキー生成を無効にしてください。
- 複数のポリシーサーバが含まれるネットワーク構成では、ポリシーサーバ管理コンソールを使用して、各ポリシーサーバのポリシーストアを指定できます。ポリシーストアは、SiteMinder オブジェクトとポリシー情報の主な格納場所であるマスタポリシーストアにしたり、マスタポリシーストアからコピーされるデータを使用する複製ポリシーストアにしたりできます。

- マスタ/スレーブディレクトリまたはデータベースは、ディレクトリまたはデータベースのプロバイダの指定に従って設定する必要があります。ポリシーサーバでは、ポリシーストアのフェールオーバー順序を指定できますが、データ複製は制御されません。複製方式については、使用しているデータベースまたはディレクトリのプロバイダから提供されているマニュアルを参照してください。
- ダイナミック キーのロールオーバーを使用するネットワークの場合、ポリシーサーバのポリシーストアは必ずマスタ キーストア、または複製されたスレーブ キーストアのいずれかになります。マスタ キーストアは、キーを生成するポリシー サーバプロセスから直接キーを受け取ります。またスレーブ キーストアは、マスタ キーストアにあるキーのコピーを受け取ります。
- マスタ/スレーブ環境では、ポリシーサーバからマスタ ポリシー ストアおよびキーストアにキーが生成されるように設定する必要があります。マスタ ポリシー ストアおよびキーストアのデータは、その後、フェールオーバー順の設定に含まれる他のすべてのポリシーストアおよびキーストアに複製される必要があります。
- 複数の cookie ドメインがあるシングルサインオン環境では、マスタ キーストアが 1 つある場合か、1 つのマスタ キーストアから複製されたキーを持つスレーブ キーストアがある場合のみ、ダイナミック キーを使用できます。
- ポリシーストアとキーストアは、LDAP と ODBC の混合ディレクトリにインストールできます。ポリシーストアは ODBC データベースに格納でき、キーストアは LDAP ディレクトリ サーバに格納できます。また、その逆も可能です。サポートされているデータベースのリストについては、[テクニカル サポート サイト](#)に移動し、SiteMinder 12.52 SP1 プラットフォーム サポート マトリックスを検索してください。

詳細情報:

[エージェント キー生成の設定](#) (P. 136)

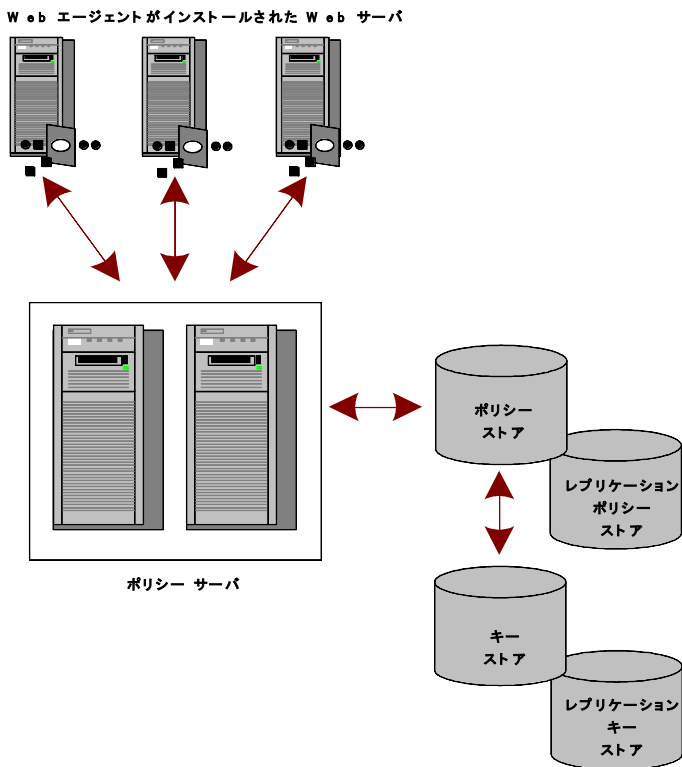
[LDAP フェールオーバーの設定](#) (P. 39)

[ODBC フェールオーバーの設定](#) (P. 52)

共通のポリシーストアとキーストア

キーのロールオーバーを使用する SiteMinder 設定の最も簡単なシナリオは、複数のポリシー サーバが 1つのキーストアと共に、1つのポリシー ストア (および関連するフェールオーバー ポリシー ストア) を使用する場合があります。

以下の図は、1つのポリシー ストアを使用している複数のポリシー サーバを示しています。



このタイプの設定では、ポリシー サーバはキー ストアからダイナミック キーを取得します。ポリシー サーバに関連付けられた Web エージェントは、ポリシー サーバから新しいキーを収集します。

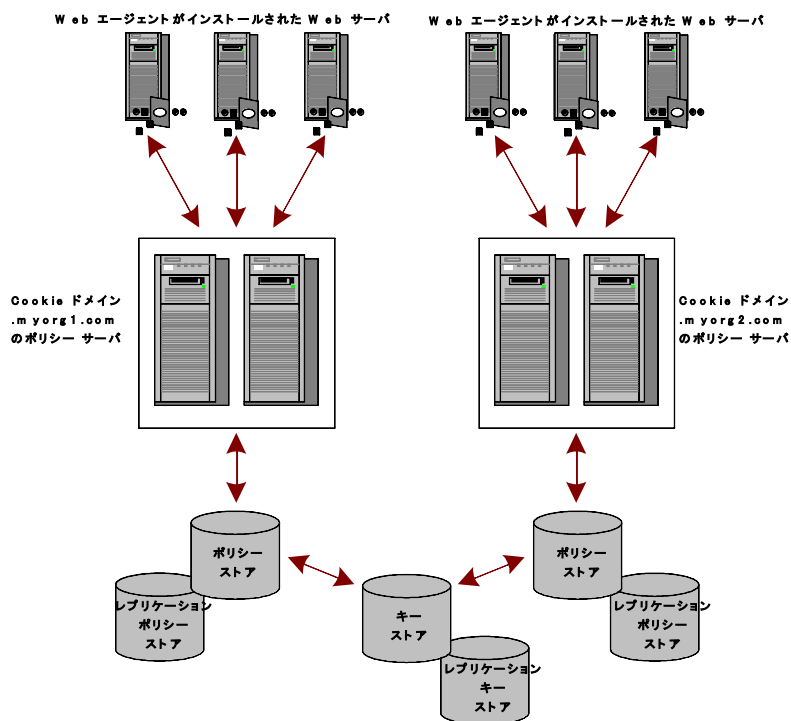
詳細情報:

[キー管理に関する注意事項 \(P. 126\)](#)

共通のキーストアがある複数のポリシーストア

シングルサインオン環境において、個別のポリシーストアを持つ複数ポリシーサーバで構成されるネットワークを設定する場合、すべてのポリシーサーバがキーのロールオーバーで使用する共通のキーストアを持つことができます。

以下の図は、共通のキーストアを使用している複数のポリシーサーバを示しています。



1つのポリシーサーバがダイナミックキーを生成し、それを中央のキーストアに格納します。各ポリシーサーバは、中央のキーストアを使用するように、ポリシーサーバ管理コンソールで設定されています。他のすべてのポリシーサーバでは、エージェントキーの生成を無効にする必要があります。エージェントは新しいキーを取得するために、各自のポリシーサーバをポーリングします。ポリシーサーバは共通のキーストアから新しいキーを取得し、それを SiteMinder エージェントに渡します。

注: このシナリオでは、キーを生成していないポリシーサーバがキーの更新をキーストアにポーリングするように、追加のレジストリ設定が必要です。

詳細情報:

[キー管理に関する注意事項 \(P. 126\)](#)

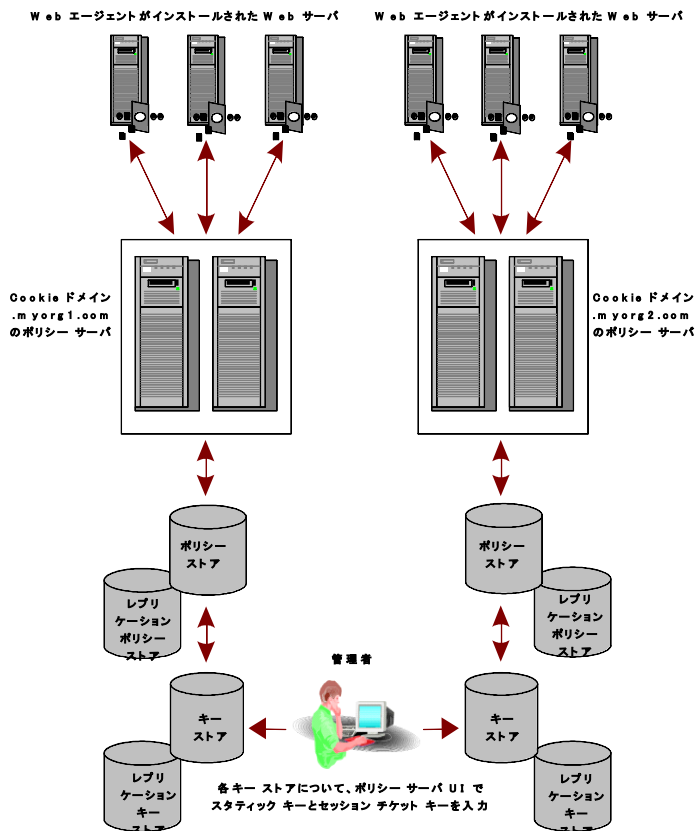
[EnableKeyUpdate レジストリ キーの設定 \(P. 142\)](#)

個別のキーストアがある複数のポリシーストア

複数のポリシーサーバ、ポリシーストア、およびマスタキーストアで構成されるネットワークを設定する場合、適切な権限を持つ管理者は、次のどちらかまたは両方を容易にするために、各ポリシーストアに対して同一のスタティックキーとセッションチケットキーを指定できます。

- すべてのエージェント間でのシングルサインオン
- 共通のユーザディレクトリによるパスワードサービス

以下の図は、複数のポリシーサーバとポリシーストアが含まれる環境を示しています。



前の例では、SiteMinder Web エージェントが作成したすべての cookie の暗号化に、同じスタティック キーが使用されています。

詳細情報:

[キー管理に関する注意事項 \(P. 126\)](#)

r6.x ポリシー ストア暗号化キーのリセット

r6.x ポリシー ストア暗号化キーをリセットする方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

```
smobjexport -dsiteminder_administrator -wpassword -ofile_name -c  
-dsiteminder_administrator
```

SiteMinder 管理者アカウントの名前を指定します。

注: この管理者は、SiteMinder のすべてのドメイン オブジェクトを管理できる必要があります。

```
-wpassword
```

SiteMinder 管理者アカウントのパスワードを指定します。

```
-ofile_name
```

以下を指定します。

- 出力場所のパス
- ユーティリティによって作成される `smdif` ファイルの名前

注: この引数を指定しない場合、デフォルトの出力ファイル名は `stdout.smdif` と `stdout.cfg` になります。

```
-c
```

機密データをクリアテキストとしてエクスポートします。

ポリシー ストア データが `smdif` ファイルにエクスポートされます。

3. smreg ユーティリティが *policy_server_home*¥bin にあることを確認します。

policy_server_home

ポリシー サーバのインストールパスを指定します。

注: ユーティリティがない場合は、サポート サイトで提供されているポリシー サーバインストール メディアから入手できます。

4. 以下のコマンドを実行します。

```
smreg -key encryption_key
```

encryption_key

新しい暗号化鍵を指定します。

制限: 6 ~ 24 文字

ポリシー ストア暗号化キーが変更されます。

5. ポリシー サーバ管理コンソールを起動し、[データ] タブを開きます。
6. ポリシー ストア管理者パスワードを再入力し、[更新] をクリックします。

管理者パスワードが新しい暗号化キーで暗号化されます。

7. 以下のコマンドを実行します。

```
smreg -su password
```

パスワード

SiteMinder スーパーユーザ パスワードを指定します。

スーパーユーザ パスワードが設定され、新しい暗号化キーで暗号化されます。

8. 以下のコマンドを実行します。

```
smobjimport -dsiteminder_administrator -wpassword -ifile_name -r -f -c  
-dsiteminder_administrator
```

SiteMinder 管理者アカウントの名前を指定します。

注: この管理者は、SiteMinder のすべてのドメイン オブジェクトを管理できる必要があります。

-wpassword

SiteMinder 管理者アカウントのパスワードを指定します。

-ifile_name

以下を指定します。

- smdif ファイルのパス
- smdif ファイルの名前

注: この引数を指定しない場合、デフォルトの入力ファイル名は `stdout.smdif` と `stdout.cfg` になります。

-r

インポート中、重複するポリシー ストア情報を上書きできることを明示します。

-f

オブジェクトの名前の自動変更機能をオフにします。デフォルトでは、ターゲット ポリシー ストア内に存在する名前を持つオブジェクトをインポートしようとする時、重複するオブジェクトが作成されます。オブジェクトの名前は *nameoid* です。

name

オブジェクトの名前を指定します。

oid

新しい重複オブジェクトのオブジェクト ID を指定します。

ネーミングの競合が原因で作成できなかったすべてのオブジェクトに対しては、エラーメッセージが返されます

-c

入力ファイルに機密データをクリアテキストで格納することを明示します。

9. 以下のコマンドを実行します。

```
smreg -su password
```

パスワード

SiteMinder スーパーユーザ パスワードを指定します。

スーパーユーザ パスワードが設定されます。

ポリシー ストア暗号化キーがリセットされます。

r12.x ポリシー ストア暗号化キーのリセット

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. ポリシー サーバを停止します。

注: 暗号化キーを変更する前に、ポリシー ストアをポイントしているすべてのポリシー サーバを停止します。

3. XPSExport を使用して、ポリシー ストア コンテンツのフルバックアップをエクスポートします。

```
xpsexport <ファイル名> -xb -npass
```

または (暗号化された出力の場合)

```
xpsexport <ファイル名> -xb -pass <パスワード>
```

4. smkeyexport を使用してエージェント キーをエクスポートします (クリア テキスト オプションが必要)。

```
smkeyexport -o <ファイル名> -d<sm admin 名> -w<smadmin パスワード> -c
```

5. ポリシー ストアの暗号化キーを変更します。

```
smreg -key <新しいキー>
```

6. SmConsole を使用してポリシー ストア パスワードをリセットし、テストします。

SmConsole の [データ] タブを使用して、以前に設定されたパスワードを再入力し、変更を適用して、[テスト接続] ボタンを使用して確認します。

7. 手順 3 でエクスポートしたバックアップを使用し、XPSImport を実行してポリシー ストアのコンテンツをインポートします。

```
xpsimport <ファイル名> -fo -pass <パスワード>
```

または (エクスポート ファイルを作成するときにパスワードを使用しなかった場合) :

```
xpsimport <ファイル名> -fo -npass
```

8. 手順 4 でエクスポートしたエージェント キーを使用し、smkeyimport (クリア テキスト オプションを指定) を実行してエージェント キーをインポートします。

```
smkeyimport -i<ファイル名> -d<sm admin 名> -w<sm admin パスワード>
-c
```

9. ポリシー サーバを再起動します。

ポリシー ストア暗号化キーがリセットされます。

エージェント キー生成の設定

ポリシー サーバ管理コンソールの [キー] タブでは、ポリシー サーバにおけるエージェント キー生成の方法を設定します。

注: キー生成を有効にするのは、エージェント キーを生成させるポリシー サーバのみにしてください。

次の手順に従ってください:

1. ポリシーサーバ管理コンソールを起動します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [キー] タブをクリックします。

注: このタブの設定およびコントロールの詳細については、[ヘルプ] - [管理コンソールヘルプ] をクリックしてください。

3. [キー] タブに示されるフィールドとコントロールに値を入力して、エージェント キー生成を設定します。
4. 入力が終わったら、[適用] をクリックして変更内容を保存します。

エージェント キーの管理

管理 UI からアクセスできる [SiteMinder キー管理] ダイアログ ボックスでは、エージェント キーの定期的なロールオーバーの設定、手動によるロールオーバーの実行、およびスタティック キーの変更ができます。また、セッションチケットキーの管理も可能です。

注: キーを管理するには、キーとパスワード ポリシーの管理権限を持つアカウントを使用して、管理 UI にログインしてください。詳細については、「ポリシー サーバ設定ガイド」を参照してください。

詳細情報:

[セッションチケットキーの管理 \(P. 141\)](#)

定期的なキー ロールオーバーの設定

ポリシー サーバは以下の間隔で定期的なエージェント キー ロールオーバーをサポートします。

- 毎週
- 毎日
- 1 日で決められた間隔

ロールオーバー間隔の最小設定時間は 1 時間です。

注: 使用しているオペレーティング システムが、サマータイム用のシステム時間を調整するよう設定する必要があります。サマータイム用に設定されていないシステムは 1 時間ずつキー ロールオーバーを相殺できます。

以下の手順に従います。

1. ポリシー サーバ管理コンソールにアクセスし、[キー] タブを開きます。
2. [エージェント キー生成を有効にする] を選択し [OK] をクリックします。
3. 管理 UI にログインします。
4. [管理] - [ポリシー サーバ] をクリックします。

5. [キー管理] - [エージェント キー管理] をクリックします。
6. [エージェント キー] セクション内の [ダイナミック エージェント キーを使用] を選択します。

重要: [ダイナミック エージェント キーを使用] を選択した後は、定期的なキー ロールオーバー設定を保存するまで、[今すぐロールオーバーを実行] をクリックできません。

7. [ダイナミック キーの詳細] セクション内の [自動キー ロールオーバー] を選択します。
8. [ロールオーバー間隔の設定] をクリックします。
9. ロールオーバーが発生する間隔を指定します。
10. [OK] をクリックします。
11. [サブミット] をクリックします。

エージェント キー ロールオーバーが設定されます。

キーの手動ロールオーバー

ダイナミック エージェント キーを手動でロールオーバーできます。この機能は、

- 追加されたセキュリティを提供します。いつでもロールオーバーを実行できます。
- 柔軟性が提供されます。ダイナミック キーを生成するためにポリシー サーバを設定できますが、ロールオーバーの間隔を指定する必要はありません。

以下の手順に従います。

1. ポリシー サーバ管理コンソールにアクセスし、[キー] タブを開きます。
2. [エージェント キー生成を有効にする] を選択し [OK] をクリックします。
3. 管理 UI にログインします。
4. [管理] - [ポリシー サーバ] をクリックします。

5. [キー管理] - [エージェント キー管理] をクリックします。
6. [エージェント キー] セクション内の [ダイナミック エージェント キーを使用] を選択します。
7. [ダイナミック キーの詳細] セクション内の [手動キー ロールオーバー] を選択します。
8. [今すぐロールオーバーを実行] をクリックします。

これを選択すると、ポリシー サーバが直ちに新しいエージェント キーを生成します。エージェント キーのロールオーバーを手動で実行しない限り、ポリシー サーバは新しいダイナミック キーを自動的に生成しません。

注: キーのロールオーバーを複数回実行する場合以外は、このボタンを何度もクリックしないでください。

Web エージェントは、次のポリシー サーバへのポーリング時に新しいキーを受け取ります。このアクションには、キャッシュ同期のため最大 3 分かかる場合があります。セキュリティ上の理由からまったく新しいキーセットを使用する場合は、ダイナミック キーを 2 回ロールオーバーします。このアクションにより、キー ストアから古いキーと現在のキーが削除されます。

エージェント キー管理とセッション タイムアウトの調整

エージェント キーの更新とセッション タイムアウトを調整しないと、セッション情報を含む **cookie** が無効になる場合があります。企業のポリシー設計の担当者とダイナミックキーロールオーバーの設定の担当者が異なる場合があるので、この調整は重要です。

セッション タイムアウトは、エージェント キーのロールオーバー間隔の 2 倍以下に設定してください。セッション タイムアウトの前にエージェント キーのロールオーバーが 2 回実行されるように設定すると、1 回目のキー ロールオーバーの前に **Web** エージェントによって書き込まれた **cookie** は、セッションが終了する前に無効になり、ユーザは再度 ID の入力を求められます。

たとえば、3 時間ごとにキー ロールオーバーが実行されるように設定すると、複数のキー ロールオーバーによってセッション **cookie** が無効にならないように、最大セッション タイムアウトを 6 時間以下に設定する必要があります。

スタティック キーの変更

特定の機能の識別情報を暗号化するために Web エージェントが使用するスタティック エージェント キーを変更できます。

重要: スタティック キーを変更することは推奨しません。スタティック キーの変更は、セキュリティ侵害などのやむを得ない状況においてのみ行ってください。このアクションは、いくつかの SiteMinder 機能が正しく動作するために必要なデータを失う原因になります。この場合、永続的な Cookie に格納されている情報を組み立てて使用する機能が動作しなくなります。シングルサインオンが複数の SiteMinder インストール環境で機能する前に、認証されたユーザは強制的に再ログインを要求される可能性があります。

スタティック キーもまた、複数のポリシー サーバと複数のマスタ キー ストアが必要なシングルサインオン環境を維持するために使用されることがあります。

以下の手順に従います。

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] をクリックします。
3. [キー管理] - [エージェント キー管理] をクリックします。
4. [エージェント キー] セクション内 [スタティック エージェント キーを使用] を選択します。
5. 以下のいずれかを実行します。
 - [ランダム エージェント キーを生成] セクション内の [今すぐロールオーバーを実行] をクリックします。
ポリシー サーバが新しいランダムなスタティック キーを生成します。
 - [エージェント キーの指定] セクションでスタティック エージェント キーを入力します。
このオプションは、シングルサインオンを維持するために 2 つのキー ストアがスタティック キーを使用する必要がある場合に使用します。

6. [今すぐロールオーバーを実行] をクリックします。
7. [サブミット] をクリックします。

スタティック キーのロールオーバーは3分以内に終了します。

セッション チケット キーの管理

ポリシー サーバでは、アルゴリズムを使用したセッション チケット キーの生成や、手動によるセッション チケット キーの入力が可能です。セッション チケットは、ユーザの認証が正常に行われるたびに作成され、これによってポリシー サーバがユーザセッションの継続時間を判断できるようになります。

注: セッション チケット キーを手動で割り当てる必要がある環境は、複数の独立したキー ストアがある環境だけです。ポリシー サーバは、自動的に生成したキーを複数の独立したキー ストアに配信することができません。他のいかなる場合でも、ポリシー サーバのアルゴリズムによって生成されるセッション チケット キーを使用することをお勧めします。

セッション チケット キーの生成

ポリシー サーバでは、ダイナミック エージェント キーを生成するのと同様の方法で、セッション チケット キーを生成できます。セッション チケット キーをランダムに生成する場合、ポリシー サーバはアルゴリズムを使用して、暗号化と復号化に使用するキーを作成します。

以下の手順に従います。

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] をクリックします。
3. [キー管理] - [セッション キー管理] をクリックします。
4. 以下のいずれかを実行します。
 - [ランダム セッション チケット キーを生成] セクション内の [今すぐロールオーバーを実行] をクリックします。

ポリシー サーバが新しいセッション チケット キーを生成します。セッション チケットの暗号化と復号化に使用されているキーが、直ちにこのキーと置き換えられます。

- [セッション チケット キーの指定] セクションでセッション チケットを指定し、[今すぐロールオーバーを実行] をクリックします。

ポリシー サーバが、セッション チケット キーを直ちに入力した値に置き換えます。

5. [サブミット] をクリックします。

手動によるセッション チケット キーの入力

使用しているポリシー サーバが複数のキーストアの存在する環境に置かれている場合は、セッション チケット キーを手動で入力できます。

以下の手順に従います。

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] をクリックします。
3. [キー管理] - [セッション キー管理] をクリックします。
4. [セッション チケット キーの指定] セクションでキーを指定します。
5. [今すぐロールオーバーを実行] をクリックします。

ポリシー サーバが、セッション チケット キーを直ちに入力した値に置き換えます。

6. [サブミット] をクリックします。

EnableKeyUpdate レジストリ キーの設定

個別のポリシー ストアに接続し、中央のキー ストアを共有する複数のポリシー サーバが存在する環境で1つのポリシー サーバが暗号化キーを生成している場合は、追加のレジストリ設定が必要です。このレジストリ設定は、各ポリシー サーバが共通のキー ストアをポーリングし、新しい暗号化キーを定期的を取得するようにします。

Windows のポリシー サーバで EnableKeyUpdate レジストリ キーを設定する方法

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択します。
2. [ファイル名を指定して実行] ダイアログボックスで「regedit」と入力し、[OK] をクリックします。
3. レジストリエディタで、次のレジストリ設定を確認します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\
CurrentVersion\ObjectStore
```

4. 以下のレジストリ値を変更します。
"EnableKeyUpdate"=0
変更後
"EnableKeyUpdate"=1
5. ポリシー サーバを再起動します。

UNIX のポリシー サーバで EnableKeyUpdate レジストリ キーを設定する方法

1. 次のディレクトリに移動します。
install_directory/siteminder/registry
2. テキストエディタを使用して *sm.registry* を開きます。
3. ファイル内にある次のテキストを確認します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\
CurrentVersion\ObjectStore
```

4. 以下のレジストリ値を変更します。
"EnableKeyUpdate"=0
変更後
"EnableKeyUpdate"=1
5. ポリシー サーバを再起動します。

詳細情報:

[共通のキーストアがある複数のポリシーストア \(P. 129\)](#)

トラステッド ホストの共有秘密キー

トラステッドホストを登録する場合、インストールプロセスは以下を実行します。

- Web エージェントに対して共有秘密キーを自動生成します。
- ホスト設定ファイル (SmHost.conf) 内に共有秘密キーを格納します。

トラステッドホストの登録時に共有秘密キーのロールオーバーを有効にすると、トラステッドホストの共有秘密キーを手動でまたは周期的にロールオーバーできるようになります。

共有秘密キーの手動によるまたは定期的なロールオーバーの実行時には、共有秘密キーは、インストール時にロールオーバーの有効化を設定したエージェントについてのみロールオーバーされます。

注: Web エージェントのインストールとトラステッドホストの登録については、「*SiteMinder Web エージェントインストールガイド*」を参照してください。

共有秘密キーのロールオーバーが自動的に行われるのは、エージェントキーの生成を有効にするように設定されているサーバのみです。エージェントキーの生成を有効にするには、ポリシーサーバ管理コンソールの[キー]タブにある[エージェントキー生成を有効にする]チェックボックスをオンにします。この設定は、デフォルトでは有効になっています。

重要: キーを生成するためにポリシーサーバを1つのみ有効にすることをお勧めします。環境内に複数のポリシーストアがあるが、共有キーストアが1つのみの場合、すべての共有秘密キーが自動的にロールオーバーされるとは限りません。共有秘密キーはポリシーストアが設定されるポリシーサーバがキー生成に対して有効にされる場合にのみ、自動的にロールオーバーされます。他のすべてのポリシーストアは、ユーザがロールオーバーを手動で実行することを必要とします。

共有秘密キーを手動でロールオーバーするには、以下のいずれかを実行します。

- 管理 UI。
- ターゲット ポリシー ストアで設定されたポリシー サーバ上で実行される C ポリシー管理 API。

注: 共有秘密キー ポリシー オブジェクトは、キー ストアで維持されます。同じキー ストアを共有するポリシー ストアはすべて、同じ秘密キーを共有しています。共有秘密キーそのものは、ポリシー ストアの一部であるトラステッドホストオブジェクト内に保持されます。

トラステッド ホストの共有秘密キーのロールオーバー設定

ポリシー サーバは、トラステッドホストの共有秘密キーの手動によるロールオーバーおよび定期的なロールオーバーをサポートしています。

定期的なロールオーバーは、時間、日、週、または月単位で設定できます。ロールオーバーの設定可能な最短間隔は 1 時間です。ポリシー サーバは、日次、週次、または月次の特定の時間にロールオーバーを開始するのではなく、各トラステッドホストの共有秘密キーの有効期限に基づいてロールオーバーを開始します。各共有秘密キーの有効期限が切れたときにそのキーをロールオーバーすることによって、ロールオーバー関連の処理が時間的に分散されるので、ポリシー サーバに大きな処理負荷がかかることを避けることができます。

手動ロールオーバー機能を使用すると、共有秘密キーのロールオーバーが有効になっているすべてのトラステッドホストに対して新しい共有秘密キーが設定されるため、一般に、その後の定期的なロールオーバーは、すべてのトラステッドホストに対して集中的に実行されることとなります。

重要: 単一のポリシー ストアに関連付けられた複数のポリシー サーバでキーの生成を有効にすると、オブジェクトストアの伝播遅延のために、同じ共有秘密キーが短期間に何回もロールオーバーされることがあります。その結果、ホストの新しい共有秘密キーが破棄され、ホストが孤立する場合があります。この潜在的な問題を解決するために、ポリシー ストアごとに 1 つのポリシー サーバについてのみ共有秘密キーのロールオーバーを有効にするようにしてください。

次の手順に従ってください:

1. ポリシー サーバ管理コンソールの [キー] タブにある [エージェントキー生成を有効にする] チェック ボックスがオンになっていることを確認します。
2. 管理 UI にログインします。
3. [管理] - [ポリシー サーバ] - [共有秘密キーのロールオーバー] をクリックします。
4. [共有秘密キーのロールオーバー] グループ ボックスで、以下の操作のいずれかを実行します。
 - ロールオーバーをただちに実行するには、[今すぐロールオーバーを実行] をクリックします。
 - 共有秘密キーがロールオーバーされないようにするには、[共有秘密キーのロールオーバーなし] を選択します。
 - 定期的なロールオーバーを指定するには、[指定周期による共有秘密キーのロールオーバー] を選択し、以下のフィールドに値を入力します。

ロールオーバー間隔

ロールオーバーを実行する回数を整数で入力します。この数値はロールオーバー期間の値と連動します。

ロールオーバー期間

プルダウン リストから、ロールオーバーを実行する時間、日、週、または月を選択します。

ポリシー サーバは、共有秘密キーのロールオーバーの有効化が設定されているすべてのトラステッドホストについて、共有秘密キーのロールオーバーのプロセスを開始します。環境内のトラステッドホストの数によっては、ロールオーバーに多少時間がかかる場合があります。

5. [サブミット] をクリックして、変更を保存します。

第 9 章: ポリシー サーバ プロファイラの設定

このセクションには、以下のトピックが含まれています。

[ポリシー サーバ プロファイラの設定 \(P. 147\)](#)

[プロファイラ トレース ログ ファイルの手動によるロールオーバー \(P. 151\)](#)

ポリシー サーバ プロファイラの設定

ポリシー サーバ プロファイラを使用すると、ポリシー サーバの内部診断と処理機能をトレースできます。

次の手順に従ってください:

1. ポリシーサーバ管理コンソールを起動します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [プロファイラ] タブをクリックします。
3. [プロファイリングの有効化] オプションを設定して、プロファイリングを有効にします。
4. プロファイラの設定を選択するには、以下のいずれかを実行します。
 - [設定ファイル] ドロップダウン リストに示されるデフォルトの smtracedefault.txt ファイルによって指定されるプロファイラ設定を受け入れます。
 - この管理セッションですでに選択されている別の設定ファイルを [設定ファイル] ドロップダウン リストから選択します。
 - [参照] ボタンをクリックして、別の設定ファイルを選択します。

5. プロファイラの設定ファイルに格納されているプロファイラ設定を変更し、その変更内容を同じファイルまたは新しいファイルに保存するには、[環境設定] ボタンをクリックして [ポリシー サーバ プロファイラ] ダイアログ ボックスを開きます。
6. [出力] グループ ボックスに示されている設定を調整して、ポリシー サーバ プロファイラによって生成される情報の出力形式を指定します。
7. [適用] をクリックして、変更内容を保存します。

注:

プロファイラ設定に対する変更は自動的に有効になります。ただし、ポリシー サーバを再起動すると、新しい出力ファイル（プロファイラでファイル出力が設定されている場合）が作成されます。既存のプロファイラ出力ファイルは、バージョン番号と共に自動的に保存されます。例：

`smtracedefault.log.1`

ロギング機能またはトレース機能の設定に対する変更がプロファイラ出力ファイルに関係がない場合（Windows でのコンソール ロギングの有効化または無効化など）、既存のファイルには新しい出力が追加され、そのバージョンは保存されません。

ポリシー サーバはデフォルトで、最大 10 個の出力ファイルを保持します（現在のファイルと 9 個のバックアップファイル）。10 個のファイル制限を超えると、古いファイルは新しいファイルに自動的に置き換えられます。保持するファイルの数を変更するには、`TraceFilesToKeep` DWORD レジストリ設定で希望する 10 進数を指定します。`TraceFilesToKeep` レジストリ設定は、以下の場所で作成される必要があります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
LogConfig\TraceFilesToKeep
```

[プロファイラ] タブには [バッファトレッシング] オプションがあります。このオプションは、デフォルトでポリシー サーバのパフォーマンスを向上させるように設定されています。このオプションは、Solaris システムのみにあります。

プロファイラ設定の変更

ポリシー サーバがトレースするコンポーネントやデータ フィールドを指定することができます。その後、トレースの出力にフィルタを適用してプロファイラが特定のコンポーネントまたはデータ フィールドの特定の値だけを取得するように設定できます。

次の手順に従ってください:

1. ポリシーサーバ管理コンソールを起動します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [プロファイラ] タブをクリックします。

注: このタブの設定およびコントロールの詳細については、[ヘルプ] - [管理コンソールヘルプ] をクリックしてください。

3. [環境設定] ボタンをクリックします。

注: このボタンは、[プロファイリングの有効化] チェック ボックスをオンにしたときだけ有効になります。

[ポリシー サーバプロファイラ] ダイアログ ボックスが開きます。

4. オプションで、特定のトレース タスクに適したコンポーネントおよびデータ フィールドの事前定義済みセットを含むプロファイラ テンプレート ファイルを [テンプレート] ドロップダウン リストから選択します。

general_trace.template

全般的な広範囲のトレース用オプションを提供します。

authentication_trace.template

ユーザ認証のトレース用オプションを提供します。

authorization_trace.template

ユーザ許可のトレース用オプションを提供します。

samlidp_trace.template

SAML アイデンティティ プロバイダ アサーションのトレース用オプションを提供します。

samlsp_trace.template

SAML サービス プロバイダ 認証のトレース用オプションを提供します。

プロファイラ テンプレートは、プロファイラ設定の出発点として使用することもできます。テンプレートをロードしたら、テンプレートによって指定されるコンポーネントとデータ フィールドを手動で変更したり、データ フィルタを適用したりすることができます。

5. トレース オプションを確認または設定するには、以下の 1 つ以上の操作を行います。
 - コンポーネントの選択 -- [コンポーネント] タブで、トレースするコンポーネント (ポリシー サーバによって実行されるアクション) を指定します。
 - データ フィールドの選択 -- [データ] タブで、トレースするデータ フィールド (タスク完了のためにポリシー サーバによって使用される実際のデータ) を指定します。
 - フィルタの追加 -- [フィルタ] タブで、トレース処理に情報を追加する、またはトレース処理から情報を除外するデータ フィルタを指定します。
6. 新しい設定を保存するには、以下のいずれかを実行します。
 - 現在選択している設定ファイルに設定を保存するには、[OK] をクリックします。
 - 新しい設定ファイルに設定を保存するには、[ファイル] - [名前を付けて保存] を選択し、新しいテキスト ファイルを指定します。
7. [ファイル]-[閉じる]を選択してプロファイラを閉じ、ポリシー サーバ管理コンソールに戻ります。
8. [構成ファイル] フィールドの右にある [参照] ボタンをクリックします。

Windows 環境でのプロファイラ コンソールの出力に関する問題の回避

Windows 環境のポリシー サーバでは、コンソールのデバッグを有効にしたときに発生する問題を回避するために、簡易編集モードと挿入モードを無効にする必要があります。簡易編集モードと挿入モードは、Windows のコマンドプロンプトウィンドウで有効にできる機能です。

簡易編集モードと挿入モードを無効にする方法

1. コマンドプロンプトウィンドウを起動します。
2. ウィンドウのタイトルバーを右クリックして、プルダウンメニューを表示します。
3. [プロパティ] を選択します。
4. [簡易編集モード] または [挿入モード] がオンになっていたら、どちらもオフにします。
5. [OK] をクリックします。

プロファイラトレース ファイルの保持ポリシーの設定

ポリシー サーバはデフォルトで、最大 10 個の出力ファイルを保持します（現在のファイルと 9 個のバックアップファイル）。10 個のファイル制限を超えると、古いファイルは新しいファイルに自動的に置き換えられます。保持するファイルの数を変更するには、TraceFilesToKeep DWORD レジストリ設定で希望する 10 進数を指定します。TraceFilesToKeep レジストリ設定は、次の場所で行う必要があります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\LogConfig\TraceFilesToKeep
```

プロファイラトレース ログ ファイルの手動によるロールオーバー

ポリシー サーバでは、smpolicysrv コマンドを使用して、ポリシー サーバプロファイラのトレース ログ ファイルを手動でロールオーバーできます。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

ファイルへのトレース ログgingを開始するには、以下のコマンドを実行します。

```
smpolicysrv -starttrace
```

このコマンドは、トレース ファイルへのログの記録を開始し、コンソールへのトレース ログgingには影響しません。ポリシー サーバが稼働していない場合は、エラーを発行します。

ポリシー サーバがすでにトレース データのログを記録している場合に `-starttrace` コマンドを実行すると、現在のトレース ファイルの名前が変更され（ファイル名の最後にタイム スタンプを付けて `file_name.YYYYMMDD_HHmms.extension` の形式で）、元の名前を持つ新しいトレース ファイルが作成されます。たとえば、ポリシー サーバ管理コンソールの [プロファイラ] タブでのトレース ファイル名が `C:¥temp¥smtrace.log` である場合、新しいファイルが生成されると、古いファイルは `c:¥temp¥smtrace.20051007_121807.log` として保存されます。タイム スタンプは、ファイルが 2005 年 10 月 7 日の午後 12:18 に作成されたことを示しています。

ポリシー サーバ管理コンソールの [プロファイラ] タブでファイルのトレース機能を有効にしていない場合は、このコマンドを実行しても何も起こりません。

ファイルへのトレース ログgingを中止するには、以下のコマンドを実行します。

```
smpolicysrv -stoptrace
```

このコマンドは、ファイルへのログの記録を中止し、コンソールへのトレース ログgingには影響しません。ポリシー サーバが稼働していない場合は、エラーを発行します。

注: Windows システムでは、リモート デスクトップまたはターミナル サービス ウィンドウから `smpolicysr` コマンドを実行しないでください。`smpolicysrv` コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは [ターミナル サービス] ウィンドウから `smpolicysrv` プロセスを実行した場合には機能しません。

指定された間隔でのトレース ファイルの動的なロールオーバー

指定された間隔でトレース ファイルをロールオーバーするためのスクリプトを作成することもできます。たとえば、新しいトレース ファイルを毎時間作成するには、以下のようなスクリプトを作成します。

```
smpolicysrv --starttrace
repeat forever
wait 1 hour
smpolicysrv --starttrace
end repeat
```

これは、ポリシー サーバ管理コンソールの [ログ] タブにある時間単位のロールオーバー オプションに似ています。

第 10 章：管理ジャーナルとイベントハンドラの設定

管理ジャーナルとイベントハンドラの概要

ポリシー サーバの管理ジャーナルの設定では、管理上の変更をポリシー サーバに適用する頻度、および適用した変更のリストがポリシー サーバによって保持される期間を指定できます。

イベントハンドラは、特定のイベントを処理するためにポリシー サーバに追加できる共有ライブラリです。

ポリシー サーバの高度な設定

次の手順に従ってください：

1. ポリシーサーバ管理コンソールを起動します。

重要： Windows Server 2008 上でこのグラフィカルユーザインターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [詳細設定] タブをクリックします。

注： このタブの設定およびコントロールの詳細については、[ヘルプ] - [管理コンソールヘルプ] をクリックしてください。

3. [管理ジャーナル] グループ ボックスに示される設定を調整して、管理上の変更をポリシー サーバに適用する頻度、および適用した変更のリストがポリシー サーバによって保持される期間を設定します。
4. [適用] をクリックして、変更内容を保存します。

イベントハンドラ ライブラリの追加

SiteMinder ポリシー サーバにはイベントハンドラ ライブラリを追加できます。

注: SiteMinder バイナリ ファイル (XPS.dll、libXPS.so、libXPS.sl) への書き込みアクセス許可がユーザにない場合は、管理者が管理 UI または XPSecurity ツールを使用して、関連する XPS コマンドライン ツールを使用する権限を付与する必要があります。

次の手順に従ってください:

1. ポリシー サーバでコマンドラインを開き、以下のコマンドを入力します。

```
xpsconfig
```

ツールが起動し、このセッションのログ ファイルの名前が表示されます。また、選択項目のメニューが開きます。

2. 以下のコマンドを入力します。

```
xps
```

オプションのリストが表示されます。

3. 以下のコマンドを入力します。

```
5 (AuditSMHandlers)
```

イベントハンドラ ライブラリの設定が表示されます。

4. 「C」と入力し、追加するイベントハンドラ ライブラリのパスとファイル名を入力します。ライブラリの場所が複数ある場合はカンマで区切ります。

イベントハンドラ ライブラリの設定が表示されます。追加した値は「保留中の値」として設定の下に表示されます。

5. 以下の手順を実行します。

- a. 2回「Q」と入力します。

- b. 「L」と入力します。

- c. 「Q」と入力して XPS セッションを終了します。

変更が保存され、コマンドプロンプトが表示されます。

詳細情報:

[ポリシー サーバ管理コンソールを開くときの、イベントハンドラ リスト設定に関する警告 \(P. 357\)](#)

第 11 章: グローバル設定の調整

このセクションには、以下のトピックが含まれています。

[ユーザ追跡の有効化 \(P. 159\)](#)

[ネストされたセキュリティの有効化 \(P. 160\)](#)

[拡張された Active Directory 統合を有効にする方法 \(P. 160\)](#)

ユーザ追跡の有効化

[ポリシー サーバ] - [グローバル ツール] から、ユーザ追跡を有効または無効にすることができます。ユーザ追跡を有効にすると、SiteMinder Web エージェントは GUID (グローバルな固有識別子) を cookie に保存します。匿名認証方式によって保護されているリソースにユーザが初めてアクセスするとき、Web エージェントはユーザの GUID を含む cookie を作成します。各 GUID は一意の値であるため、匿名ユーザの追跡および Web コンテンツのカスタマイズに利用できます。

アフィリエイトエージェントにはユーザ追跡が必要です。アフィリエイトエージェントを含むネットワークで SiteMinder を使用している場合は、次に説明する手順に従ってユーザ追跡を有効にしてください。

ユーザ追跡を有効にする方法

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] - [グローバル ツール] をクリックします。
[グローバル ツール] ペインが開きます。
3. [グローバル設定] グループ ボックスの [ユーザ追跡を有効にする] を選択します。
4. [サブミット] をクリックします。

これで、ポリシー サーバのユーザ追跡が有効になりました。

ネストされたセキュリティの有効化

ネストされたセキュリティを有効および無効にできます。それは、SiteMinder の古いバージョンの下位互換性を提供します。

ネストされたセキュリティオプションを有効にする方法

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] - [グローバル ツール] をクリックします。
[グローバル ツール] ペインが開きます。
3. [ネストされたセキュリティを有効にする] チェック ボックスをオンにします。
4. [サブミット] をクリックします。
ネストされたセキュリティが有効になります。

拡張された Active Directory 統合を有効にする方法

拡張された Active Directory の統合を有効にするプロセスには以下の 3 つの手順が含まれます。

1. IgnoreADpwdLastSet レジストリキーの作成
2. 拡張された Active Directory 統合の有効化
3. ユーザ ディレクトリ接続の設定

IgnoreADpwdLastSet レジストリキーの作成

使用中の Active Directory のバージョンに `pwdLastSet` 属性が含まれない場合、ポリシー サーバ レジストリ キーの `IgnoreADpwdLastSet` を作成します。

重要: `IgnoreADpwdLastSet` レジストリ キーを作成し、`pwdLastSet` 属性が定義されていないインストールに対してのみ値 **1** を設定します。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにアクセスし、以下のいずれかの手順を実行します。
 - (Windows) レジストリ エディタを開き、以下の場所に移動します:
`SiteMinder¥CurrentVersion¥Ds¥LDAPProvider`
 - (UNIX) `sm.registry` ファイルを開きます。このファイルのデフォルトの場所は `siteminder_home/registry` です。
`siteminder_home`
ポリシー サーバのインストールパスを指定します。
2. `IgnoreADpwdLastSet` を作成し、レジストリ値のタイプは `REG_DWORD` にします。
値: 1
3. 以下のいずれかを実行します。
 - (Windows) レジストリ エディタを終了します。
 - (UNIX) `sm.registry` ファイルを保存します。
4. ポリシー サーバを再起動します。

Active Directory 統合の拡張の有効化

Active Directory 2008 には、Windows ネットワーク オペレーティング システム (NOS) に特有で、LDAP 標準によって必要とされない、ユーザ属性とドメイン属性がいくつかあります。属性は以下のとおりです。

- `accountExpires`
- `userAccountControl`
- `pwdLastSet`

- unicodePwd
- lastLogon
- lastLogonTimestamp
- badPasswordTime
- badPwdCount
- lockoutTime
- lockoutDuration
- pwdMaxAge

Active Directory をユーザストアとして使用するようポリシー サーバを設定する場合は、管理 UI の [ポリシー サーバ] - [グローバル ツール] にある [Active Directory 統合を拡張] を有効にします。このオプションでは、Active Directory のユーザ属性と、SiteMinder でマップされるユーザ属性を同期することによって、ポリシー サーバのユーザ管理機能と Active Directory のパスワード サービスとの間の統合を強化します。

次の手順に従ってください:

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] - [グローバル ツール] をクリックします。
[グローバル ツール] ペインが開きます。
3. [Active Directory 統合を拡張] を選択します。デフォルトでは、この機能は無効になっています。
注: この機能を有効にした後、AD ユーザストアを変更するには管理者認証情報が、AD 属性を更新するには管理者権限がそれぞれ必要になります。これらの認証情報および権限を持っていない場合は、エラーメッセージが返されます。
4. [サブミット] をクリックします。
Active Directory 統合の拡張が有効になります。
5. [インフラストラクチャ] タブの [ユーザ ディレクトリ] ダイアログボックスに移動します。
6. 編集する Active Directory オブジェクトを開きます。

7. [ルート] フィールドに、ユーザディレクトリルートとして Windows ドメインのデフォルトの DN を入力します。例：

dc=WindowsDomain,dc=com

注： [ルート] フィールドに別の値が設定されている場合、AD 固有の機能が動作しない可能性があります。

8. [サブミット] をクリックします。

ユーザディレクトリ接続の設定

拡張されたアクティブなディレクトリ統合を有効にした後、ユーザディレクトリ接続を設定します。

次の手順に従ってください：

1. [インフラストラクチャ] - [ディレクトリ] をクリックします。
2. [ユーザディレクトリ] をクリックします。
3. [ユーザディレクトリの作成] をクリックします。

[ユーザディレクトリの作成] ページが LDAP 接続を設定するために必要な設定で表示されます。

4. [一般] および [ディレクトリのセットアップ] のセクションで必要な接続情報を入力します。

注：ポリシーサーバが FIPS モードで動作し、ポリシーサーバと通信する際にディレクトリ接続に安全な SSL 接続を使用する場合、ポリシーサーバとディレクトリストアが使用する証明書は FIPS 準拠である必要があります。

5. (オプション) [管理者認証情報] セクションで以下の手順を実行します。
 1. [認証情報が必要] を選択します。
 2. 管理者アカウントの認証情報を入力します。

6. [LDAP 設定] セクションで LDAP 検索および LDAP ユーザ DN 検索設定を設定します。

LDAP ユーザ DN 検索

LDAP ユーザストアでユーザを検出するためのパラメータを指定します。

先頭

LDAP 検索式またはユーザ DN の先頭部分として使用するテキスト文字列を指定します。ユーザがログインしようとするとき、ポリシーサーバがユーザ名の最初にこの文字列を付加します。

値：(sAMAccountName=

7. [ユーザ属性] セクションで以下の属性に対して指定された値を設定します。

ユニバーサル ID

SiteMinder がユニバーサル ID として使用する属性の名前を指定します。

値：sAMAccountName

無効フラグ

ユーザの無効状態が格納されるユーザディレクトリ属性の名前を指定します。

値：carLicense (または任意の整数属性)

パスワード

SiteMinder がユーザパスワードの認証に使用するユーザディレクトリ属性の名前を指定します。

値：unicodePwd

パスワードデータ

SiteMinder がパスワードサービス用のデータとして使用できるユーザディレクトリ属性の名前を指定します。

値：audio

[パスワードデータ] には任意の大型のバイナリ属性を値として使用できます。値は基本パスワードサービスを使用している場合にのみ必要です。

注: 他のフィールドに関する情報の詳細は、「[管理 UI ヘルプ](#)」を参照してください。

8. (オプション) ユーザ属性マッピングを設定するには [属性マッピングリスト] セクションで [作成] をクリックします。
9. [サブミット] をクリックします。
ユーザディレクトリ接続が作成されます。

第 12 章: キャッシュ管理

このセクションには、以下のトピックが含まれています。

[キャッシュ管理の概要](#) (P. 167)

[キャッシュ更新の管理](#) (P. 168)

[キャッシュのクリア](#) (P. 170)

キャッシュ管理の概要

SiteMinder には、いくつかのキャッシュがあります。最近アクセスしたデータ（ユーザ許可など）のコピーを保持するようにキャッシュを設定して、システムのパフォーマンスを向上させることができます。これらのキャッシュは、使用している環境のデータの特性に合わせて設定する必要がありますが、定期的に手動でクリアすることが必要になる場合もあります。

SiteMinder 環境では、ポリシー サーバの以下のキャッシュを保持するように設定できます。

- ユーザ許可キャッシュ - ポリシーのユーザ部分を基にしたユーザ識別名 (DN) を格納します。ユーザのグループメンバシップも含まれます。

また、SiteMinder は、各 SiteMinder エージェント マシン上にエージェント キャッシュ を保持します。エージェントキャッシュには、次の 2 つのコンポーネントがあります。

- エージェント リソース キャッシュ - さまざまなレルムによって保護されているリソースへのアクセス記録を格納します。エージェントが既に処理したリクエストのリソースに関する情報を持っているため、このキャッシュによってエージェントとポリシーサーバの通信がスピードアップします。
- エージェント ユーザ キャッシュ - ユーザの暗号化されたセッションチケットを保持します。ユーザ、レルム、リソース情報を格納し、セッションキャッシュとして動作します。ユーザがアクセスするレルムに指定されたタイムアウト値に基づいて、このキャッシュのエントリが無効になります。

キャッシュ更新の管理

ポリシー評価問題を解決するためにキャッシュのクリアの更新を一時停止し再開できます。管理 UI または `smpolicy` コマンドを使用してキャッシュ更新を管理します。

キャッシュ更新ステータスを変更する場合、中央管理ポリシー サーバは、すべてのセカンダリ ポリシー サーバに対してコマンドを発行します。

注: ポリシー サーバ コマンドはスレッド マネジメント モデルに基づいて処理されます。その結果、キャッシュ ステータスへの変更は、`smps.log` ファイルですぐには表示されません。

管理 UI を使用したキャッシュ更新の管理

管理 UI を使用して、ポリシー サーバのキャッシュ クリア更新の状態を確認し、それを有効または無効にします。

次の手順に従ってください:

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] - [キャッシュ管理] をクリックします。
3. [キャッシュの更新] セクションでキャッシュ ステータスを確認します。

キャッシュの更新は無効です: キャッシュのフラッシュは無効です。

キャッシュの更新は有効です: キャッシュのフラッシュは有効です。

4. (オプション) キャッシュの更新を切り替えるには [有効/無効] ボタンをクリックします。

smpolicysrv コマンドを使用したキャッシュ更新の管理

smpolicysrv コマンドを使用して、ポリシー サーバのキャッシュ クリア更新の状態を確認し、それを有効または無効にします。

次の手順に従ってください:

1. コマンドプロンプトを開きます。

Windows システムでは以下のポイントを考慮します。

- リモート デスクトップまたはターミナル サービス ウィンドウから smpolicysrv コマンドを実行しないでください。コマンドはプロセス間通信に応じます。リモート デスクトップまたはターミナル サービス ウィンドウから smpolicysrv プロセスを実行する場合、これらの通信は動作しません。
- 必ず管理者権限を使用してコマンドライン ウィンドウを開いてください。管理者としてシステムにログインしている場合でも、これらの権限を使用します。詳細については、お使いの SiteMinder コンポーネントの「リリース ノート」を参照してください。

2. 以下のいずれかのコマンドを入力します。

smpolicysrv -disablecacheupdates

キャッシュのフラッシュを無効にします。

smpolicysrv -enablecacheupdates

キャッシュのフラッシュを有効にします。

smpolicysrv -statuscacheupdates

ポリシー サーバ キャッシュのリフレッシュ ステータスをログ ファイル `smpls.log` に報告します。

無効: キャッシュのフラッシュは無効です。

有効: キャッシュのフラッシュは有効です。

キャッシュのクリア

SiteMinder オブジェクトを変更すると、適切なキャッシュ エントリが自動的にクリアされます。キャッシュ設定では、管理変更の適用間隔も指定します。非常に重要な変更（機密情報に対するアクセス権限の変更など）を行う場合は、SiteMinder キャッシュを手動でクリアするオプションがあります。この手動の手順により、キャッシュに格納されている情報に基づき、許可されていないユーザは保護されたリソースにアクセスできないようにすることができます。

キャッシュ管理の機能は、管理 UI の [ポリシー サーバ]-[グローバル ツール] ペインからアクセスできます。この機能は、以下のキャッシュを手動でクリアすることにより、SiteMinder データの更新を強制します。

すべてのキャッシュ

ユーザセッション、リソース情報、ユーザ ディレクトリのキャッシュ（CRL を含む）など、すべてのキャッシュをクリアできます。

ユーザ セッションのキャッシュ

保護されたリソースにユーザがアクセスしようとするときに再認証を強制できます。

リソース キャッシュ

リソースに関するキャッシュ情報をクリアできます。

すべてのキャッシュのクリア

管理者は、キャッシュ管理のオプションを使用して、すべてのキャッシュの内容をクリアすることができます。すべてのキャッシュをクリアすると、Web サイトのパフォーマンスが低下する可能性があります。これは、キャッシュをクリアした直後に、すべてのリクエストがユーザ ディレクトリとポリシー ストアから情報を取得するためです。ただし、重要なユーザ権限とポリシーの変更内容を即時に有効にする場合は、このアクションが必要となります。

キャッシュ管理の機能を使用できるのは、ユーザの管理権限またはシステムとドメイン オブジェクトの管理権限のどちらかを持っている管理者だけです。[すべてクリア] ボタンは、システムとドメインオブジェクトの管理権限を持つ管理者だけが使用できます。このメニュー選択内容は、ログインに使用したアカウントに、キャッシュ機能にアクセスするための十分な権限がある場合のみ表示されます。

すべてのキャッシュをクリアする方法

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] - [キャッシュ管理] をクリックします。
3. [すべてのキャッシュ] グループ ボックスで、[すべてクリア] をクリックします。

注: [すべてクリア] ボタンは、ユーザの管理権限と SiteMinder オブジェクトの管理権限の両方を持つ管理者だけが使用できます。

ポリシー サーバと関連する SiteMinder エージェントがすべてのキャッシュをクリアします。この処理にはポリシー サーバのポーリング間隔の時間の 2 倍近くかかり、その間にポリシー サーバはキャッシュを同期させます。

4. [サブミット] をクリックします。
キャッシュがすべてクリアされます。

ユーザ セッション キャッシュのクリア

ユーザ認証が正常に終了すると、ポリシー サーバは認証されたユーザに対してセッションを開始します。ユーザのセッション中、Web エージェントは許可情報をユーザ キャッシュに保存します。

以下の点について考慮してください。

- ユーザのアクセス権限を変更する場合は、ポリシー サーバで Web エージェント キャッシュ内のユーザ セッション情報を強制的にクリアする必要があります。
- ユーザ キャッシュをクリアするオプションは、ユーザの管理権限を持つ管理者だけが使用できます。

以下の手順に従います。

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] - [キャッシュ管理] をクリックします。

3. [ユーザセッションのキャッシュ] セクションで以下のオプションのいずれかを選択します。

すべて

ユーザ キャッシュからすべてのユーザセッションをクリアします。

特定のユーザ DN

ユーザ キャッシュから特定の DN をクリアします。

このオプションを選択する場合

- a. 削除する DN が含まれるディレクトリ リストからユーザ ディレクトリを選択します。
 - b. [DN] フィールドに識別名を入力します。グループの DN ではなくユーザ DN を指定します。DN がわからない場合は、[検索] をクリックして DN を検索します。
4. [クリア] をクリックします。

SiteMinder はユーザ キャッシュからそれぞれのユーザをクリアします。この処理にはポリシー サーバのポーリング間隔で指定した時間の 2 倍近くかかり、その間にポリシー サーバはキャッシュの同期をとっています。

5. [サブミット] をクリックします。

ユーザセッションのキャッシュがクリアされます。

リソース キャッシュのクリア

SiteMinder Web エージェントは、ユーザがアクセスした特定のリソースに関する情報をリソース キャッシュに格納します。リソース キャッシュには以下の情報が記録されます。

- ユーザがアクセスしたリソースの記録
- リソースが SiteMinder によって保護されているかどうか
- リソースが保護されている場合の保護方法

ルールやレلمを変更すると、その変更をすぐに有効にする必要が生じることがあります。そのような場合は、リソースキャッシュをクリアしてください。

注: レルムまたは特定ポリシーのリソース キャッシュのクリアについては、「[ポリシー サーバ設定ガイド](#)」を参照してください。

リソース キャッシュをクリアする方法

1. 管理 UI にログインします。
2. [管理] - [ポリシー サーバ] - [キャッシュ管理] をクリックします。
3. [リソース キャッシュ] グループ ボックスで、[クリア] をクリックします。

すべてのリソースキャッシュをクリアすると、強制的に Web エージェントからポリシー サーバへ許可リクエストが送信されます。この処理にはポリシー サーバのポーリング間隔で指定した時間の 2 倍近くかかり、その間にポリシー サーバはキャッシュの同期をとっています。

注: 特定のポリシー ドメインに対してドメイン オブジェクトの管理権限を持つ管理者がすべてのリソース キャッシュをクリアすると、そのポリシー ドメイン内のレルムに対するキャッシュだけがクリアされます。

4. [サブミット] をクリックします。
リソース キャッシュがクリアされます。

ポリシー サーバのリクエスト キューのクリア

SiteMinder エージェントからのリクエストは、一定の期間が経過するとタイムアウトに設定されます。ただし、ポリシー サーバでは、タイムアウトになったリクエストを含むキュー内のすべてのエージェント リクエストを、受信した順序で処理します。以下の状況が発生した場合、ポリシー サーバが処理するよりも早く、キューがエージェント リクエストでいっぱいになる可能性があります。

- ポリシー サーバとポリシー ストア間またはポリシー サーバとユーザストア データベース間のネットワーク遅延
- ポリシー ストアまたはユーザストア データベースに対する高い負荷
- ポリシー サーバのパフォーマンスの問題

ポリシー サーバのリクエスト キューがエージェント リクエストでいっぱいになった場合は、タイムアウトになったエージェント リクエストをキューからクリアして、現在のエージェント リクエストだけを残すことができます。この手順を使用するのは、以下の場合に限られます。

1. ポリシー サーバ キュー内で待機しているエージェント リクエストがタイムアウトになった。
2. 1 つ以上のエージェントがタイムアウトしたリクエストを再送信して、キューがいっぱいになった。

重要: 通常の動作条件下では `-flushrequests` を使用しないでください。

ポリシー サーバのリクエスト キューをクリアする方法

1. ポリシー サーバでコマンド プロンプトを開きます。
2. 以下のコマンドを実行します。

```
smpolicysrv -flushrequests
```

リクエスト キューがクリアされます。

注: Windows システムでは、リモート デスクトップまたはターミナル サービス ウィンドウから `smpolicysr` コマンドを実行しないでください。`smpolicysrv` コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは [ターミナル サービス] ウィンドウから `smpolicysrv` プロセスを実行した場合には機能しません。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンド ライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンド ライン ウィンドウを開きます。

第 13 章: ユーザセッションとユーザアカウントの管理

このセクションには、以下のトピックが含まれています。

[ユーザセッションとユーザアカウントの管理の前提条件](#) (P. 175)

[ユーザの有効化と無効化](#) (P. 176)

[ユーザパスワードを管理する方法](#) (P. 177)

[ユーザ許可の監査](#) (P. 178)

ユーザセッションとユーザアカウントの管理の前提条件

ポリシーサーバは、ユーザセッションとユーザアカウントを管理する機能を備えています。この機能を使用すると、セッションキャッシュをクリアしたり、ユーザを有効および無効にしたり、ユーザごとにパスワードを管理したりできます。

ユーザセッションとユーザアカウントを管理するには、以下の前提条件を満たす必要があります。

- ユーザの管理権限を持つ管理者アカウントを所有していること。
- ユーザアカウントを有効または無効にする場合は、ユーザ情報を含むユーザディレクトリのユーザの無効化に関する属性が設定されていること。
- パスワードの変更またはパスワード変更の強制を行う場合は、ポリシーサーバでパスワードポリシーが設定されており、ユーザ情報を含むユーザディレクトリのパスワードデータに関する属性が設定されていること。

注: 管理者権限、ユーザディレクトリ、およびパスワードポリシーの設定の詳細については、「[ポリシーサーバ設定ガイド](#)」を参照してください。

ユーザの有効化と無効化

ユーザがログインして認証されると、SiteMinder は、ユーザセッションを開始します。SiteMinder は、ユーザ属性をユーザセッション キャッシュに格納します。ユーザを無効にすると、エージェントは、セッション キャッシュをクリアして、ユーザ ID およびセッション情報を削除します。

ユーザが現在のセッションで追加のリソースにアクセスしようとする場合、Web エージェントのキャッシュからはユーザのデータがなくなっているため、エージェントはポリシー サーバと通信して、ユーザの再認証を試みます。ポリシー サーバは、このユーザがユーザ ディレクトリで無効になっていることを確認して、エージェントの認証リクエストを拒否するため、セッションが終了します。

次の手順に従ってください:

1. 管理 UI にログインします。
2. [管理] - [ユーザ] - [ユーザ アカウントの管理] をクリックします。
[ユーザ アカウントの管理] ペインが開きます。
3. 有効または無効にするユーザを含むディレクトリのユーザ ディレクトリ接続を選択します。
4. [検索] ボタンをクリックします。
[ディレクトリ ユーザ] ペインが表示されます。
5. [ユーザ/グループ] グループ ボックスに検索条件を入力し、[実行] をクリックして、有効または無効にするユーザの検索を行います。検索条件は、選択したユーザ ディレクトリのタイプによって決まります。属性と値を入力するか、式を入力できます。検索条件をクリアするには、[リセット] をクリックします。
[ユーザ/グループ] ダイアログ ボックスに検索結果が表示されます。
6. 検索結果のリストからユーザを 1 人選択します。
[ユーザの状態の変更] グループ ボックスにはボタンが含まれます。このボタンのラベルは、ユーザが無効になっている場合は [有効] と、ユーザが有効になっている場合は [無効] と表示されています。
7. [有効] または [無効] をクリックします。
選択したユーザのプロファイルの値が変更されて、ユーザが無効または有効にされます。

ユーザパスワードを管理する方法

管理 UI の [ユーザアカウントの管理] ペインでは、ユーザにパスワードの変更を強制したり、ユーザパスワードを新しい値に変更したりできます。

ユーザにパスワードの変更を強制する前に、パスワードポリシーが存在していることを確認してください。パスワードポリシーが定義されていないと、ユーザは自分自身のパスワードを変更できません。また、保護されたリソースにもアクセスできません。

ユーザにパスワードの変更を強制するとき、ユーザが SSL 接続を使用していないエージェントを経由してリソースにアクセスしている場合は、ユーザの新しいパスワード情報は、安全性の低い接続を経由して受信されます。パスワードを安全に変更するには、パスワード変更時に SSL 接続を経由してユーザをリダイレクトするようにパスワードポリシーを設定します。

次の手順に従ってください:

1. 管理 UI にログインします。
2. [管理] - [ユーザ] - [ユーザアカウントの管理] をクリックします。
[ユーザアカウントの管理] ペインが開きます。
3. パスワード管理の対象となるユーザを含むディレクトリのユーザディレクトリ接続を選択します。
4. [検索] ボタンをクリックします。

[ディレクトリ] ドロップダウンリストから選択したディレクトリタイプに関連した、ユーザディレクトリの検索ダイアログボックスが表示されます。

5. [ユーザ/グループ] グループボックスに検索条件を入力し、[実行] をクリックして、有効または無効にするユーザの検索を行います。検索条件は、選択したユーザディレクトリのタイプによって決まります。属性と値を入力するか、式を入力できます。検索条件をクリアするには、[リセット] をクリックします。

[ユーザ/グループ] ダイアログボックスに検索結果が表示されます。

6. 検索結果のリストからユーザを 1 人選択します。
7. 選択したユーザの次のログイン時にパスワードの変更を強制するには、[ユーザのパスワードをリセット] グループボックスの [パスワードの変更を強制] をクリックします。

- ユーザのパスワードを新しい値に変更するには、[ユーザのパスワードの変更] グループボックスに新しいパスワードを入力します。確認のためにパスワードを再入力します。

注: 指定するパスワードは、パスワードポリシーによって制限されることはありませんが、ユーザのパスワード履歴に記録されます。

ユーザ許可の監査

Web エージェントの監査機能を使用して、ユーザセッションキャッシュに格納されている正常に行われたユーザ許可を追跡し、記録することができます。これにより、ユーザの動作を追跡し、Web サイトでアプリケーションが使用される頻度を計測することができます。

このオプションを選択すると、Web エージェントは、ユーザがリソースへのアクセスをキャッシュから許可されるたびに、ポリシーサーバにメッセージを送信します。後で、ログレポートを実行して、各 SiteMinder セッションでのユーザの動作を表示させることができます。

監査が有効になっていない場合、Web エージェントは、認証と最初の許可のみを監査します。

注: 監査を有効にする方法については、「[Web エージェント設定ガイド](#)」を参照してください。

ユーザがリソースにアクセスすると、Web エージェントは、ユーザ名とアクセス情報を Web サーバのネイティブログファイルに自動的に記録します。監査ログには、ユーザ許可リクエストが成功するたびに Web エージェントが自動的に生成する固有のトランザクション ID が含まれています。また、SiteMinder がリソースへのユーザのアクセスを許可すると、エージェントは、この ID を HTTP ヘッダーに追加します。この後、トランザクション ID は、Web サーバ上のすべてのアプリケーションで利用できます。トランザクション ID は、Web サーバの監査ログにも記録されます。この ID を使用すると、ログを照合して、特定のアプリケーションに関するユーザの動作を調べることができます。

監査機能の出力を表示するには、管理 UI から SiteMinder レポートを実行します。

第 14 章: ハードウェア ロード バランサを使用した SiteMinder エージェントとポリシー サーバ間の通信の設定

このセクションには、以下のトピックが含まれています。

[ハードウェア ロード バランシング \(P. 179\)](#)

[SiteMinder エージェントとポリシー サーバ間の接続の有効期間の設定 \(P. 181\)](#)

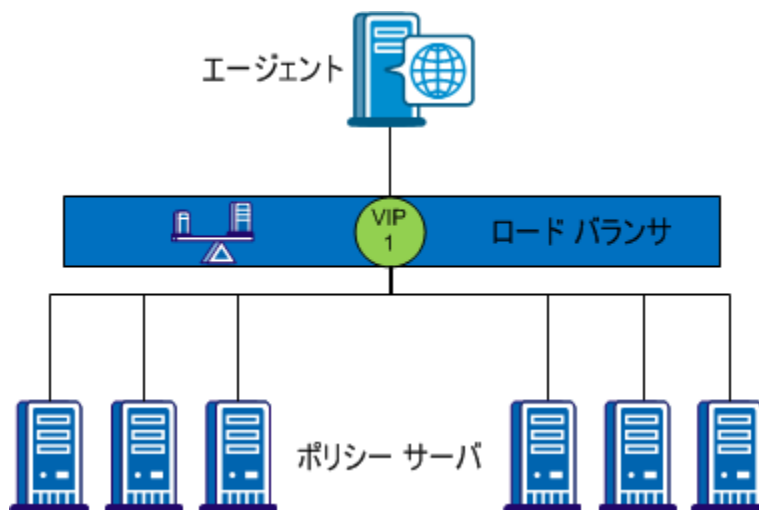
[ハードウェア ロード バランシング設定の状態の監視 \(P. 183\)](#)

ハードウェア ロード バランシング

SiteMinder では、1 つ以上の仮想 IP アドレス (VIPs) によって複数のポリシー サーバを表示するように設定されたハードウェア ロード バランサを使用できます。ハードウェア ロード バランサは、その VIP と関連付けられたすべてのポリシー サーバ間でリクエストの負荷を動的に分散させます。以下のハードウェア ロード バランシング設定がサポートされています。

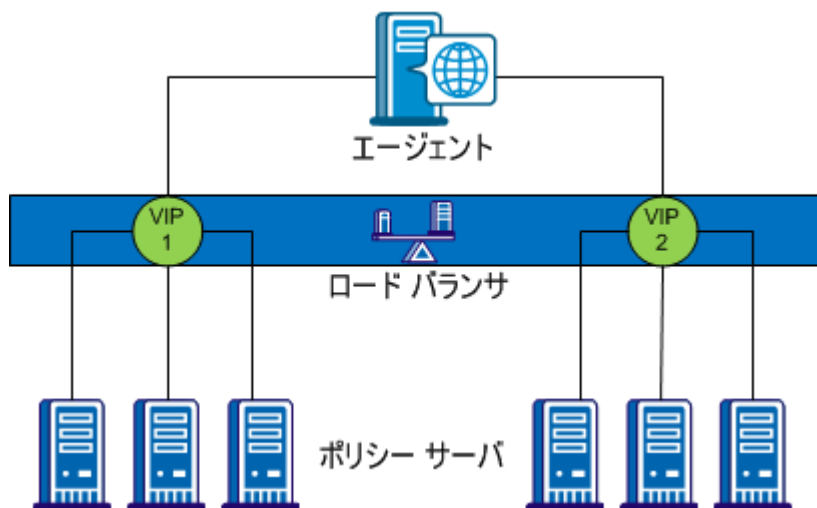
- 単一の VIP と各 VIP によって表示される複数のポリシー サーバ
- 複数の VIP と各 VIP によって表示される複数のポリシー サーバ

単一の VIP と VIP ごとの複数のポリシー サーバ



前の図に示した設定で、ロードバランサは単一のVIPを使用して、複数のポリシーサーバを表示します。このシナリオは、VIPを処理するロードバランサが失敗した場合の単一障害点を示しています。

複数のVIPとVIPごとの複数のポリシーサーバ



前の図に示した設定で、ポリシー サーバのグループは 1 つ以上のロード バランサによって個別の VIP として表示されます。複数のロード バランサが使用される場合は、ロード バランサ間のフェールオーバーになるため、単一障害点は除去されます。ただし、主要なすべてのハードウェア ロード バランサ ベンダーは、単一の VIP のみが必要となるように、複数の同様なロード バランサ間のフェールオーバーを内部的に処理しています。したがって、同じベンダーからの冗長なロード バランサを使用している場合は、単一の VIP でエージェントとポリシー サーバ間の通信を設定して、堅牢なロード バランシングとフェールオーバーを維持できます。

注: ハードウェア ロード バランサを使用して複数の仮想 IP アドレス (VIP) としてポリシー サーバを公開している場合は、それらの VIP をフェールオーバー設定に設定することを推奨します。ハードウェア ロード バランサが同じ機能をより効率よく実行するため、ラウンドロビン負荷分散は不必要です。

SiteMinder エージェントとポリシー サーバ間の接続の有効期間の設定

確立後、エージェントとポリシー サーバ間の接続はセッションの期間にわたって維持されます。したがって、ハードウェア ロード バランサは初期の接続リクエストのみを処理します。その接続が終了し、新しいエージェント接続が確立されるまで、同じ接続での後続のトラフィックはすべて同じポリシー サーバに移動します。

デフォルトでは、ポリシー サーバの接続有効期間は 360 分です。通常の場合、これはハードウェア ロード バランサを使用して効果を示すには長すぎます。すべてのエージェント接続が効果的なロード バランシングのために頻繁に更新されるようにするには、ポリシー サーバ上で最大エージェント接続有効期間を設定します。

ポリシー サーバ用の最大接続有効期間を設定するには、以下のパラメータを設定します。

AgentConnectionMaxLifetime

分単位で最大エージェント接続有効期間を指定します。

デフォルト： 0 特定の値を設定しません。SiteMinder デフォルト接続有効期間（360 分）制限のみが適用されます。

制限： 0 ～ 360

例： 15

注： SiteMinder バイナリ ファイル（XPS.dll、libXPS.so、libXPS.sl）への書き込みアクセス許可がユーザにない場合は、管理者が管理 UI または XPSecurity ツールを使用して、関連する XPS コマンドライン ツールを使用する権限を付与する必要があります。

AgentConnectionMaxLifetime パラメータは動的です。ポリシー サーバを再起動せずに、その値を変更できます。

ハードウェア ロード バランサ用の最大エージェント接続有効期間を設定する方法

1. ポリシー サーバでコマンドラインを開き、以下のコマンドを入力します。

```
xpsconfig
```

ツールが起動し、このセッションのログ ファイルの名前が表示されます。また、選択項目のメニューが開きます。

2. 以下のコマンドを入力します。

```
sm
```

オプションのリストが表示されます。

3. AgentConnectionMaxLifetime パラメータに対応する、「4」などの数値を入力します。

[AgentConnectionMaxLifetime パラメータ] メニューが開きます。

4. 「c」と入力して、パラメータ値を変更します。
ツールは変更をローカルまたはグローバルに適用するかどうかを確認するメッセージを表示します。
5. 以下のいずれかを入力します。
 - 「l」 -- パラメータ値はグローバル値を無視して、ローカル ポリシー サーバのみに対して変更されます。
 - 「g」 -- パラメータ値は、同じポリシー ストアを使用して、すべてのポリシー サーバ(ローカル値上書き設定がない)に対してグローバルに変更されます。
6. たとえば、以下のように分単位で新しい最大エージェント接続有効期間を入力します。

30

[AgentConnectionMaxLifetime パラメータ] メニューが再表示されて、新しい値が示されます。 ローカル上書き値が設定されている場合は、グローバルとローカルの両方の値が表示されます。

7. 「Q」と3回入力して XPSConfig セッションを終了します。
変更が保存され、コマンドプロンプトが表示されます。

詳細情報

[XPSConfig \(P. 296\)](#)

ハードウェア ロード バランシング設定の状態の監視

それぞれのハードウェア ロード バランサは、対応するハードウェアおよびアプリケーションの状態を判定するさまざまな方法を提供します。このセクションでは、ベンダー固有のケースではなく一般的な推奨事項について説明します。

サーバの状態を判定する場合に問題となるのは、SiteMinder の状態と負荷のみがロード バランサでの考慮事項ではない場合があるということです。たとえば、比較的負荷が小さいポリシー サーバがシステムで実行されていても、別のプロセスでは負荷が生じる場合があります。そのため、ロード バランサでは、サーバ自体(CPU、メモリ使用量およびディスク アクティビティ)の状態も考慮に入れる必要があります。

アクティブ モニタ

ハードウェア ロード バランサでは、ステータス情報用のハードウェアまたはアプリケーションをポーリングするためにアクティブ モニタを使用できます。それぞれの主要ベンダーはさまざまなアクティブ モニタをサポートしています。このトピックでは、最も一般的なモニタとポリシー サーバを監視するためのそれらの適合性について説明します。

TCP Half Open

TCP Half Open モニタは、ポリシー サーバとの部分的な TCP/IP ハンドシェイクを実行します。このモニタは、ポリシー サーバに SYN パケットを送信します。ポリシー サーバが起動すると、その状態が良好であることを示すためにモニタに SYN-ACK が返送されます。

Simple Network Management Protocol (SNMP)

SNMP モニタは、ポリシー サーバの状態を判定するために、SiteMinder MIB に対しクエリを実行できます。高度な実装では、MIB 内の値をクエリして、キューの階層数、ソケット数、使用中のスレッド、利用可能なスレッドなどを判定できます。したがって、SNMP 監視は、ポリシー サーバの状態の詳細を取得するのに最もふさわしいメソッドです。

SNMP 監視を有効にするには、各ポリシー サーバ上の SiteMinder OneView モニタおよび SNMP エージェントを設定します。詳細については、「SNMP を介した OneView モニタの使用と SiteMinder の監視」を参照してください。

注: すべてのハードウェア ロード バランサですぐに SNMP 監視を利用できるとは限りません。

Internet Control Message Protocol (ICMP)

ICMP 状態モニタは、ほとんどのネットワーク ハードウェアの ICMP ポートに対して ping を実行してそのオンライン状態を確認します。ICMP モニタはポリシー サーバが良好であることを示すにはほとんど効果を発揮しないため、ポリシー サーバの状態の監視には推奨されません。

TCP Open

TCP Open モニタは、ネットワーク化されたアプリケーションとの完全な TCP/IP ハンドシェイクを実行します。モニタはネットワーク化されたアプリケーションに既知のテキストを送信します。アプリケーションはその後に応答して起動していることを示す必要があります。ポリシー サーバでは TCP/IP 接続のエンドツーエンドの暗号化と独自のメッセージプロトコルを使用するため、TCP Open 監視は、ポリシーサーバの状態監視には適していません。

詳細情報:

[SNMP 監視 \(P. 219\)](#)

[OneView モニタの概要 \(P. 197\)](#)

パッシブ モニタ

インバンド状態モニタは、ハードウェア ロード バランサ上で実行され、その中のトラフィック フローを分析します。このモニタはアクティブ モニタよりも影響度が低く、ロード バランサにほとんどオーバーヘッドを生じさせません。

インバンド モニタは、フェールオーバの前の特定の故障率を検出するように設定できます。一部のロード バランサ上のインバンド モニタは、アプリケーションの問題を検出すると共に、問題がいつ解決されてサーバが再度利用可能になるかを判定するアクティブ モニタを指定できます。

第 15 章: ポリシー サーバのクラスタ化

このセクションには、以下のトピックが含まれています。

[クラスタ化されたポリシー サーバの導入 \(P. 187\)](#)

[ポリシー サーバ クラスタの設定 \(P. 191\)](#)

[クラスタの集中監視用のポリシー サーバ設定 \(P. 192\)](#)

[クラスタ化されているポリシー サーバを集中監視用のポリシー サーバの監視対象にする \(P. 193\)](#)

クラスタ化されたポリシー サーバの導入

SiteMinder 環境の負荷分散機能とフェールオーバー機能は、高レベルのシステム可用性を実現し、SiteMinder エージェントからポリシー サーバへのリクエストの分散によってレスポンス時間を短縮させます。これらの機能にクラスタの定義を組み合わせることによって、システムの可用性とレスポンス時間はさらに向上します。

クラスタを使用しない従来のラウンドロビン方式の負荷分散では、リクエストが一連のサーバに均等に分散されます。ただし、この方法では、すべてのサーバが処理能力に関係なく同じ数のリクエストを受信するため、サーバの処理能力が異なる異機種環境では、最も効率的な方法であるとはいえません。

また、データセンターが地理的に離れた場所にあると、さらに効率が悪くなる場合があります。離れた場所にあるサーバへのリクエストの送信によって、ネットワーク通信のオーバーヘッドが増加することがあり、場合によっては、ネットワークの輻輳が発生します。

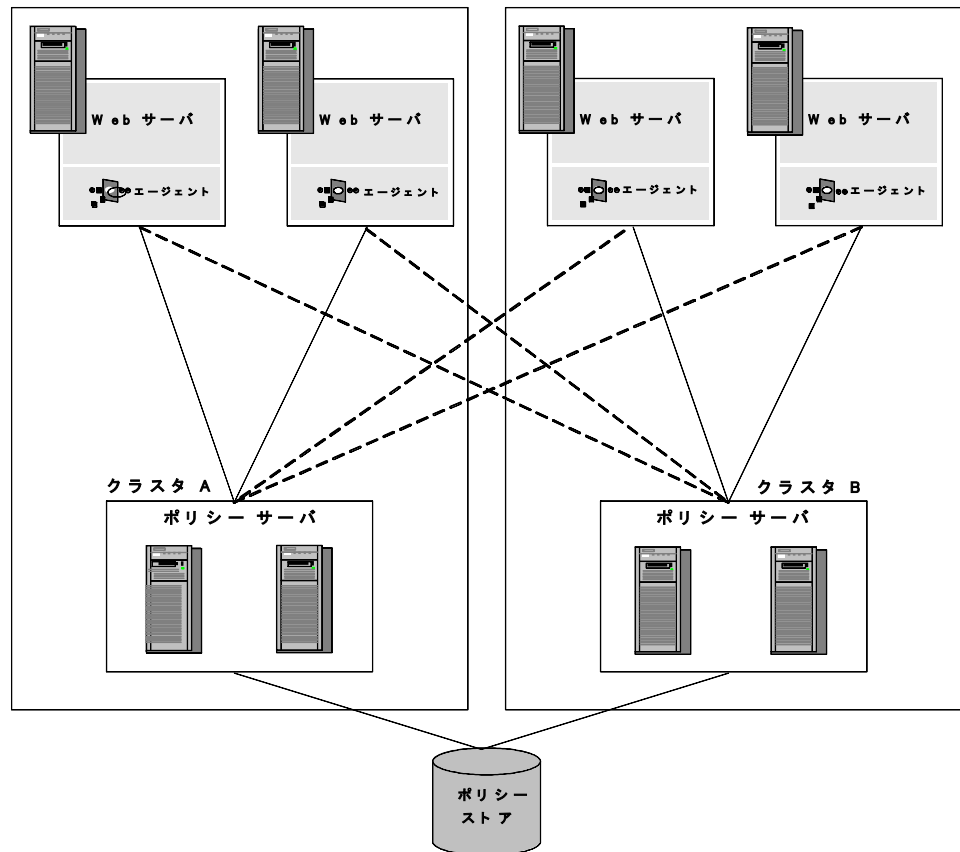
これらの問題を回避し、システムの可用性とレスポンス時間を向上させるために、ポリシー サーバと、ロードバランシングとフェールオーバーを (ソフトウェアベースで) 実行するように設定された関連する SiteMinder エージェントのクラスタを定義することができます。

ポリシー サーバクラスタには、従来の負荷分散/フェールオーバー方式にはない次のような利点があります。

- 負荷は、サーバのレスポンス時間に基づいて、クラスタ内のサーバ間に動的に分散されます。
- クラスタは、クラスタ内の使用可能なサーバの数がしきい値（設定可能）を下回ったときに他のクラスタにフェールオーバーするように設定できます。

注: ポリシー サーバクラスタは、ポリシー サーバがハードウェア ロード バランサを通じてエージェントと通信する環境に適していないため必要ではありません。

以下の図は、2つのクラスタを使用した単純な SiteMinder 環境を示しています。



クラスタ A とクラスタ B は、タイムゾーンの異なる離れた場所に配置されているものとします。独立したクラスタのそれぞれに Web エージェントとポリシー サーバを配置すると、離れた地域の間での負荷分散によるネットワークオーバーヘッドは、一方のクラスタのポリシー サーバがダウンし、もう一方のクラスタへのフェイルオーバーが必要になった場合にだけ発生します。

詳細情報:

[フェイルオーバーのしきい値](#) (P. 189)

[クラスタ化された環境の監視](#) (P. 213)

フェイルオーバーのしきい値

クラスタ化されたあらゆる SiteMinder 環境では、フェイルオーバーのしきい値を設定する必要があります。使用可能なポリシー サーバの数が、指定されたしきい値を下回ると、障害の発生したポリシー サーバクラスタで処理されることになっていたすべてのリクエストが、別のクラスタに転送されます。

フェイルオーバーのしきい値は、クラスタ内のポリシー サーバの割合 (%) で表されます。たとえば、4 つのポリシー サーバによるクラスタで、クラスタのフェイルオーバーのしきい値が 50% に設定されている場合、3 つのポリシー サーバがダウンすると、クラスタ障害となり、すべてのリクエストが次のクラスタにフェイルオーバーされます。

フェイルオーバーのしきい値のデフォルト設定は 0 です。この設定では、クラスタ内のすべてのサーバがダウンした場合にのみ、フェイルオーバーが発生します。

ハードウェア ロード バランシングの考慮事項

SiteMinder ポリシー サーバと Web エージェントの間でハードウェア ロード バランサを展開している場合は、以下の点を考慮します。

- ポリシー サーバ TCP ポートに対して TCP ハートビートまたはヘルス チェックを直接設定することはしません。ポリシー サーバの TCP ポートに対して直接適用されたハートビートおよびヘルス チェックは、その操作に悪影響を及ぼす可能性があります。
- ポリシー サーバの運用状況をテストするため、ロード バランサの包括的な機能を設計します。
- フェイルオーバーのアルゴリズムとして、Web エージェント上に 1 つのポリシー サーバを設定する場合、および複数のポリシー サーバを設定する場合の影響を比較します。
- Web エージェントとポリシー サーバのチューニングおよびモニタリングにおけるパフォーマンスと障害のシナリオを考慮します。
- プロキシエージェントからポリシー サーバへの接続に対してロード バランサが設定されている場合、ロード バランサのタイムアウトおよびソケット状態を考慮します。

注: Web エージェントとポリシー サーバの間にハードウェア ロード バランサを展開する詳細については、サポート サイト上で関連するナレッジ ベース記事 (TEC511443) を参照してください。

詳細情報:

[CA への連絡先 \(P. 3\)](#)

ポリシー サーバクラスタの設定

ポリシー サーバクラスタは、ホスト設定オブジェクトの一部として定義されます。SiteMinder エージェントが初期化されると、ホスト設定オブジェクトの設定を使用してポリシー サーバとの通信が設定されます。

注: ホスト設定オブジェクトの詳細については、「[Web エージェント設定ガイド](#)」および「[ポリシー サーバ設定ガイド](#)」を参照してください。

次の手順に従ってください:

1. [インフラストラクチャ] - [ホスト] をクリックします。 - [ホスト設定オブジェクト] を選択します。
2. [ホスト設定の作成] をクリックします。
3. [クラスタ] セクションで、[追加] をクリックします。
[クラスタのセットアップ] セクションが開きます。

注: フィールド、コントロール、およびそれぞれの要件については、[\[ヘルプ\]](#) をクリックしてください。

4. [ホスト] フィールドと [ポート] フィールドに、ポリシー サーバの IP アドレスとポート番号をそれぞれ入力します。
5. [クラスタへ追加] をクリックします。
ポリシー サーバが [現在の設定] セクションのサーバリストに表示されます。
6. 他のポリシー サーバをクラスタに追加するには、同じ手順を繰り返します。
7. [OK] をクリックして、変更を保存します。

ホスト設定ダイアログボックスに戻ると、ポリシー サーバクラスタがテーブルにリスト表示されます。

8. [フェールオーバーのしきい値パーセント] フィールドに、アクティブである必要のあるポリシー サーバの割合 (%) を入力し、[適用] をクリックします。

クラスタ内のアクティブなサーバの割合が、指定した割合を下回ると、クラスタは、クラスタのリスト内の次に使用可能なクラスタにフェールオーバーします。この設定は、ホスト設定オブジェクトを使用するすべてのクラスタに適用されます。

重要: [設定値] セクションで指定されたポリシー サーバは、クラスタ内で指定されたポリシー サーバによって上書きされます。クラスタを設定すると、[設定値] グループ ボックスで指定されたポリシー サーバは使用されなくなります。[設定値] セクション内のポリシー サーバパラメータに適用する値について、クラスタ内のポリシー サーバは指定しないでください。クラスタが設定され、単純なフェールオーバー設定を優先しクラスタを削除する場合は、クラスタからポリシー サーバ情報をすべて削除してください。

9. [サブミット] をクリックして、変更を保存します。

クラスタの集中監視用のポリシー サーバ設定

OneView モニタは、ポリシー サーバクラスタを監視するように設定できます。この設定を有効にするには、1つのポリシー サーバを集中監視用に設定し、クラスタ化されている他のポリシー サーバがこのサーバの監視対象となるように設定する必要があります。

次の手順に従ってください:

1. ポリシーサーバ管理コンソールを起動します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [設定] タブで [着信リモート接続を許可] をオンにします。

注: このタブ上での設定およびコントロールの詳細については、[ヘルプ] - [管理コンソール ヘルプ] をクリックしてください。

3. [OK] をクリックして変更内容を保存し、ポリシー サーバ管理コンソールを閉じます。
4. OneView モニタを再起動します。

この設定により、集中監視用のポリシー サーバは、クラスタ化されている他のポリシー サーバからのリモート接続を受け入れることができるようになります。

注: ポリシー サーバと監視プロセス間の通信には、セキュリティ保護されていないネットワーク チャネルが使用されます。

ポリシー サーバを集中監視用に設定した後、ポリシー サーバ管理コンソールを使用して、そのサーバをクラスタ化されている他のポリシー サーバが参照するよう設定する必要があります。

詳細情報:

[OneView モニタのポート番号の設定 \(P. 212\)](#)

クラスタ化されているポリシー サーバを集中監視用のポリシー サーバの監視対象にする

次の手順に従ってください:

1. 監視サービスの対象となる各ポリシー サーバについて、ポリシー サーバ管理コンソールを開きます。

重要: Windows Server 2008 上でこのグラフィカルユーザインターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [設定] タブで、OneView モニタの下の [リモート モニタに接続] をオンにします。

注: このタブ上での設定およびコントロールの詳細については、[ヘルプ] - [管理コンソールヘルプ] をクリックしてください。

3. その下にあるフィールドに、監視サービスが設定されているシステムのホスト名と TCP ポート番号を入力します。例：
`server.company.com:44449`
4. [OK] をクリックして変更内容を保存し、ポリシー サーバ管理コンソールを閉じます。
5. ポリシー サーバを再起動します。

第 16 章: OneView モニタの使用

このセクションには、以下のトピックが含まれています。

[OneView モニタの概要 \(P. 197\)](#)

第 17 章: OneView モニタの概要

SiteMinder OneView モニタは、SiteMinder 環境のパフォーマンス ボトルネックを特定し、リソースの利用状況に関する情報を提供します。また、特定のイベント（コンポーネント障害など）が発生した場合に、アラートを表示します。この機能は、以下の SiteMinder コンポーネントから動作データを収集することによって実現されます。

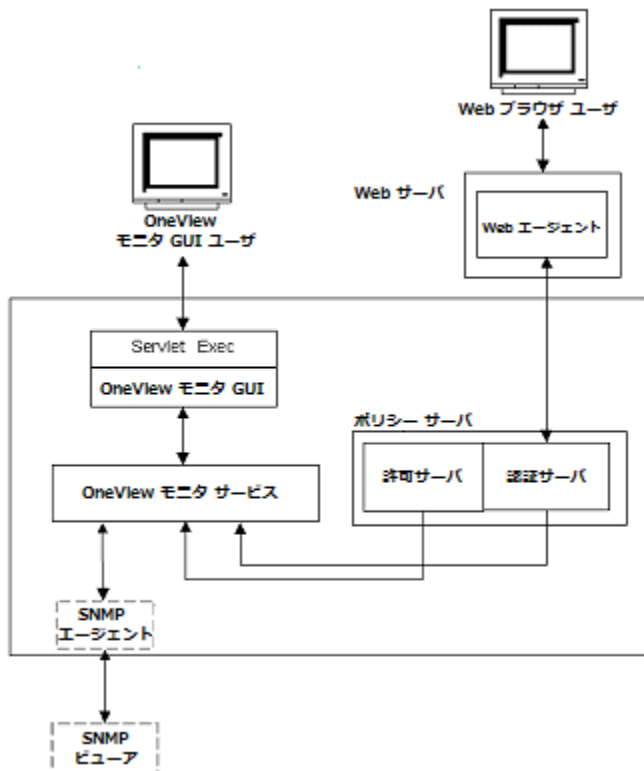
- ポリシー サーバ
- SiteMinder Web エージェント

これらのコンポーネントを SiteMinder 環境に追加すると、OneView モニタに自動的に登録されます。これらのコンポーネントを監視するように OneView モニタを設定する必要はありません。

監視対象のコンポーネントが存在する各マシンでは、OneView エージェントが動作します。このエージェントは、ポリシー サーバがインストールされているマシンに存在する OneView モニタに、動作データを送信します。OneView モニタは、動作データを Web ブラウザまたは必要に応じて SNMP エージェントに送信します。SNMP エージェントは、そのデータを SNMP マネージャに送信します。

OneView モニタのデータには、Web ブラウザやサードパーティ製の SNMP 監視アプリケーションからアクセスできます。

以下は、OneView モニタが統合された SiteMinder 環境を示しています。



OneView モニタは、プロパティ（コンポーネントのホストマシンの IP アドレスなど）と、コンポーネントのアクティビティを示すカウンタ（ユーザがサイトにログインした回数など）を収集します。カウンタは、コンピュータを再起動するとリセットされます。

Web ベースの OneView ビューアを使用すると、管理者は、特定のコンポーネントの一部またはすべてのデータを表示するテーブルを定義できます。データのリフレッシュ間隔も設定できます。

SNMP がサポートされているため、監視アプリケーションが OneView モニタから動作データを取得できます。SNMP サポートには、MIB (Management Information Base) と SNMP エージェントが含まれています。

注: クラスタ化されたポリシー サーバを含む環境では、1 つの OneView モニタを指定して、そこからクラスタ内のすべてのポリシー サーバのアクティビティを監視することができます。集中監視モニタを設定するには、クラスタ内の各ポリシー サーバについて、ポリシー サーバ管理コンソールで OneView モニタの設定を調整する必要があります。

詳細情報:

[SNMP 監視 \(P. 219\)](#)

[OneView データのリフレッシュ間隔とハートビートの設定 \(P. 211\)](#)

ポリシー サーバのデータ

ポリシー サーバデータのリストとその説明を以下に示します。

AgentTable

このサーバに接続されているエージェントのテーブル。

注: AgentTable は、SNMP を使用して利用することはできません。

AuthAcceptCount

成功した認証の数。

AuthRejectCount

失敗した認証試行の回数。これらの試行は、認証情報が無効であったために失敗しました。

AzAcceptCount

成功した許可試行の回数。

AzRejectCount

拒否された許可試行の回数。これらの試行は、必要なアクセス権限がなかったために拒否されました。

CacheFindCount

許可キャッシュ内での検索操作の回数。ユーザがポリシーに属するかどうかを許可プロセスが確認することに更新されます。

CacheFindCount/sec

毎秒あたり発生する許可キャッシュ検索操作の回数。

CacheHitCount

許可キャッシュでのヒット数。ユーザがポリシーに属するかどうかを許可プロセスが確認し、結果が真であるごとに更新されます。

CacheHitCount/sec

許可キャッシュでの毎秒あたりのヒット数。

CacheTTLMissCount

キャッシュ内に要素は見つかったものの古すぎるという理由で発生した、許可キャッシュ ミスの回数。

Component Path

ポリシー サーバのパス。これにより、サーバを一意に特定できます。**Component Path** には、次の情報が含まれています。

- ホストの IP アドレス
- コンポーネントのタイプ
- コンポーネントのインスタンス ID

注: **Component Path** は、SNMP を使用して利用することはできません。

Crypto bits

Web エージェントとポリシー サーバの間で送信されるデータの暗号化/復号化に使用される暗号化キーの長さ。

HitRate

許可検索操作に対する許可キャッシュ ヒットの比率。これは、許可キャッシュの有効性を示すインジケータです。

Host

認証サーバがインストールされているマシンの IP アドレス。

注: ホストの IP アドレスは、**Component Path** に含まれています。

IsProtectedCount

エージェントから受信した **IsProtected** コールの数。

Label

ポリシー サーバのビルド番号。

LastActivity

ポリシー サーバがワンビュー モニターと最後に通信した日時。

MaxSockets

ポリシー サーバへの同時リクエストをサブミットするために使用できる Web エージェント ソケットの最大数。

MaxThreads

スレッド プール内のワーカー スレッドの最大数。

MaximumThreadsEverUser

これまで使用された、スレッド プール内のワーカー スレッドの最大数。

PriorityQueueLength

優先キュー内のエントリ数。優先キューは優先度の高いエントリを保持します。「ServerQueueLength」を参照してください。

Platform

ポリシー サーバがインストールされているマシンのオペレーティング システム。

PolicyCacheEnabled

ポリシー キャッシュが有効になっているかどうかを示します。

Port

ポリシー サーバのポート番号。

Product

ポリシー サーバの製品名。

ServerQueueLength

標準キュー内のエントリ数。標準キューは優先度が標準のエントリを保持します。「PriorityQueueLength」を参照してください。

SocketCount

開いているソケットの数。この数は、ポリシー サーバと Web エージェントの間の開いている接続の数に対応します。

Status

ポリシー サーバのステータス。値は、Active または Inactive です。

Inactive は、指定された期間にわたってポリシー サーバとワンビュー モニターの間に通信がなかったことを示します。この期間は、ハート ビート間隔によって決まります。

ThreadsAvailable

現在使用できる、スレッドプール内のワーカー スレッドの数。リクエストを処理するすべてのワーカー スレッドは、スレッドプールの中に整理されます。すべてのスレッドがただちにビジー状態になるとは限りません。十分な負荷が適用された場合に限られます。この値は、現在ビジー状態にないスレッドの数を示します。

ThreadsInUse

現在使用されている、スレッドプール内のワーカー スレッドの数。

Time Zone

ポリシー サーバがインストールされているマシンの設置場所のタイムゾーン。

Type

ポリシー サーバのタイプ

Universal Coordinated Time

ポリシー サーバが起動した日時。

UserAzCacheEnabled

ユーザ許可キャッシュが有効になっているかどうかを示します。

Update

最後に適用された更新ファイルのバージョン番号。

Version

ポリシー サーバのバージョン番号。

Web エージェントのデータ

Web エージェント データのリストとその説明を以下に示します。

AuthorizeAvgTime

ユーザの許可にかかった平均時間 (ミリ秒単位)。

AuthorizeCount

このエージェントによる許可試行の回数。許可試行は、ユーザが保護されたリソースにアクセスするためにポリシー サーバに認証情報を提示すると発生します。

AuthorizeErrors

この Web エージェントによる許可試行の際にエラーが発生した回数。エラーは、許可呼び出し時に Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。

AuthorizeFailures

失敗した許可試行の回数。ユーザがリソースへのアクセスに必要な権限を持っていないと、許可試行は失敗します。

BadCookieHitsCount

Web エージェントが復号できなかった cookie の数。

BadURLcharsHits

URL の文字が無効であったためにエージェントが拒否したリクエストの数。Web クライアントが SiteMinder ルールに反することを防ぐために、無効な URL 文字は、明示的にブロックされます。これらの文字は、Web エージェントの設定で指定します。

Component Path

Web エージェントのパス。Component Path には、次の情報が含まれています。

- ホストの IP アドレス
- コンポーネントのタイプ
- コンポーネントのインスタンス ID

注: Component Path は、SNMP を使用して利用することはできません。

CrosssiteScriptHits

クロスサイトスクリプティングを検出した回数。これは、サイトのページに埋め込まれた不正コードの数を示しています。

注: クロスサイトスクリプティングの詳細については、「[Web エージェント設定ガイド](#)」を参照してください。

Crypto bits

Web エージェントとポリシー サーバの間で送信されるデータの暗号化/復号化に使用される暗号化キーの長さ。

ExpiredCookieHitsCount

有効期限の切れた cookie を含んでいたリクエストの数。

Host

Web エージェントがインストールされているマシンの IP アドレス。

注: ホストの IP アドレスは、Component Path に含まれています。

IsProtectedAvgTime

リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認するためにかかる平均時間 (ミリ秒単位)。

IsProtectedCount

リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認した回数。

注: リソース キャッシュが 0 に設定されている場合、OneView モニタは、ログイン試行のたびに複数の IsProtected 呼び出しを記録することがあります。Web エージェントが情報をキャッシュしていない場合、Web エージェントは、Web サーバにリクエストがあるたびに、リソースが保護されているかどうかをポリシー サーバに確認する必要があります。

リソースキャッシュが 0 に設定されていない場合、OneView モニタは、1 回の IsProtected 呼び出しだけを記録します。この場合、Web エージェントは、ポリシー サーバに IsProtected 呼び出しを 1 回だけ実行します。同じリソースに関するその後の Web サーバへのリクエストは、Web エージェントのリソース キャッシュの有効期限が切れていないか、キャッシュがクリアされていない限り、キャッシュされた情報を使用して処理されます。

IsProtectedErrors

リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認する際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。

Label

Web エージェントのビルド番号。

直前のアクティビティ

Web エージェントの直前のアクティビティの日時。

LoginAvgTime

ユーザがログインするためにかかった平均時間。

LoginCount

この Web エージェントからのログイン試行の回数。

LoginErrors

ログイン試行の際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。

LoginFailures

失敗したログイン試行の回数。ログインは、ユーザが無効な認証情報を提示すると失敗します。

Name

Web エージェントの名前。

Platform

Web エージェントがインストールされているマシンのオペレーティングシステム。

Product

Web エージェントの製品名。

ResourceCacheCount

リソースキャッシュのエントリ数。リソースキャッシュには、最近アクセスされたリソースに関する情報が保存されます。これにより、同じリソースに関するその後のリクエストの処理速度が向上します。

リソース キャッシュ内のエントリ数は、0～ n になります。 n は、Web エージェントの設定で指定される最大キャッシュ サイズです。

ResourceCacheHits

Web エージェントがリソースキャッシュ内でリソースを検出した回数。この数は、SiteMinder がキャッシュされたリソースを使用する頻度を示しています。

ResourceCacheMax

リソースキャッシュが保持可能なエントリの最大数。この数は、Web エージェントの設定で指定します。

注: リソース キャッシュ サイズの設定の詳細については、「Web エージェント設定ガイド」を参照してください。

ResourceCacheMisses

- Web エージェントがリソースキャッシュ内でリソースを検出できなかった回数。次のような場合には、リソースを検出できません。
- そのリソースにまだ一度もアクセスしていない場合
- キャッシュされた情報の有効期限が切れた場合

SocketCount

開いているソケットの数。この数は、ポリシー サーバと Web エージェントの間の開いている接続の数に対応します。

注: Web エージェントアーキテクチャが変わったので、SocketCount には値がありません。

Status

Web エージェントのステータス。値は、Active または Inactive です。

Inactive は、指定された期間にわたって Web エージェントとワンビューモニターの間に通信がなかったことを示します。この期間は、ハートビート間隔によって決まります。

Time Zone

Web エージェントがインストールされているマシンの設置場所のタイムゾーン。

Type

監視対象のコンポーネントのタイプ。この場合は、**Web** エージェントです。

Universal Coordinated Time

Web エージェントがインストールされている **Web** サーバが起動した日時。

Update

最後に適用された更新ファイルのバージョン番号。

UserSessionCacheCount

ユーザセッション キャッシュのエントリ数。ユーザセッション キャッシュには、リソースに最近アクセスしたユーザに関する情報が保存されます。ユーザ情報を保存することによって、リソースリクエストの処理速度が向上します。

ユーザセッション キャッシュ内のエントリ数は、0 ～ n になります。 n は、Web エージェントの設定で指定される最大キャッシュサイズです。ユーザセッション キャッシュ サイズの設定については、「[Web エージェント設定ガイド](#)」を参照してください。

注: ユーザセッション キャッシュ数は、セッション キャッシュが存在する Web サーバによって異なります。

マルチスレッドキャッシュを使用する Web エージェント (Windows オペレーティングシステム環境で動作する IIS Web エージェント、iPlanet 4.x/6.0 Web エージェント、Windows および UNIX オペレーティングシステム環境で動作する Domino Web エージェントなど) の場合、OneView モニタは、ユーザが正常に認証され、Web エージェントからセッション cookie を受信したときに、ユーザセッション キャッシュ数を増やします。

UNIX オペレーティングシステム環境で動作し、マルチプロセスキャッシュを使用する Apache および iPlanet 4.x/6.0 Web エージェントでは、セッションのカウント方法が異なります。ユーザがセッション cookie を Web エージェントに提示するまでは、ユーザのセッションはセッション キャッシュに追加されません。Web エージェントは、ユーザが正常に認証された後に、ユーザのセッション cookie を作成します。SiteMinder は、ユーザから追加のリソース要求があると、この cookie を使用してユーザを認証します。つまり、ユーザの最初のログインは、ユーザセッション キャッシュ数には含まれません。ユーザがもう一度リクエストし、SiteMinder がセッション cookie を使用してそのユーザを認証すると、ユーザセッション キャッシュ数が増えます。

どの Web エージェントの場合でも、ユーザセッションは、1つのレルム内のリソースに対して有効です。ユーザがセッション cookie を使用して異なるレルムのリソースにアクセスすると、ユーザには別のユーザセッションが与えられ、ユーザセッション キャッシュ数が増えます。

UserSessionCacheHits

Web エージェントがユーザセッション キャッシュにアクセスした回数。

UserSessionCacheMax

ユーザセッション キャッシュが保持可能なエントリの最大数。この数は、Web エージェントの設定で指定します。

注: ユーザセッション キャッシュ サイズの設定の詳細については、「Web エージェント設定ガイド」を参照してください。

UserSessionCacheMisses

Web エージェントがユーザセッション キャッシュ内でユーザセッション情報を検出できなかった回数。次のような場合には、リソースを検出できません。

- そのリソースにまだ一度もアクセスしていない場合
- キャッシュされた情報の有効期限が切れた場合

ValidationAvgTime

ユーザの認証に使用される cookie の正当性の検証にかかった平均時間 (ミリ秒単位)。シングルサインオン環境では、ユーザの認証に cookie が使用される場合があります。

ValidationCount

特定の Web エージェントが、ユーザを認証するために、ユーザのクレデンシャルをユーザ ディレクトリ エントリと照合する代わりに、ポリシー サーバに対してセッション cookie の正当性の検証を試行した回数（Web エージェントは、ユーザが正常に認証されたときにユーザのブラウザ上にセッション cookie を作成し、その cookie を使用して、新しいリソースに対するその後のリクエストでユーザを認証します）。

ValidationCount には、次の条件が影響します。

ユーザ セッション キャッシュのサイズ

Web エージェントのユーザ セッション キャッシュが 0 よりも大きい値に設定されている場合は、ユーザのセッション情報がキャッシュに保存されます。Web エージェントは、ポリシー サーバではなくセッション キャッシュに対してセッションの正当性を検証するため、ValidationCount は増えません。ユーザセッション キャッシュが 0 に設定されている場合は、Web エージェントがポリシー サーバに対してセッションの正当性を検証するため、保護されているリソースをユーザがリクエストするたびに ValidationCount が増えます。

マルチスレッド キャッシュとマルチプロセス キャッシュ

マルチスレッド キャッシュを使用する Web エージェント（Windows オペレーティング システム環境で動作する IIS Web エージェント、iPlanet 4.x/6.0 Web エージェント、Windows および UNIX オペレーティング システム環境で動作する Domino Web エージェントなど）は、ユーザが正常に認証されたときに、セッションをセッション キャッシュに追加します（セッション キャッシュ サイズが 0 よりも大きい場合）。認証されたユーザが同じレルムから追加のリソースをリクエストする場合は、Web エージェントがセッション キャッシュに対してユーザの正当性を検証するため、ValidationCount は増えません。

UNIX オペレーティングシステム環境で動作し、マルチプロセス キャッシュを使用する Apache および iPlanet 4.x/6.0 Web エージェントは、ユーザが、以前に認証されたレルムの別のリソースをリクエストするときに cookie を Web エージェントに提示するまで、セッション cookie をセッション キャッシュに追加しません。Web エージェントは、セッション cookie による最初のリクエストの正当性をポリシー サーバに対して検証します。このとき、ValidationCount が増えます。その後のリクエストの正当性は、キャッシュに対して検証されます。

ValidationErrors

Web エージェントによるユーザセッションの正当性の検証試行の際にエラーが発生した回数。エラーは、Web エージェントとポリシーサーバの間で通信障害が発生したことを示しています。

ValidationFailures

セッション cookie が無効であったために Web エージェントがユーザセッションの正当性を検証できなかった回数。

Version

Web エージェントのバージョン番号。

OneView モニタの設定

OneView モニタの設定には、以下が含まれます。

- データのリフレッシュ間隔とハートビートの設定
- ポート番号の設定

OneView データのリフレッシュ間隔とハートビートの設定

次の設定を修正することによって、OneView モニタと監視対象のコンポーネントの間でデータが送信される間隔を変更できます。

- リフレッシュ間隔 - OneView モニタが認証サーバと許可サーバにデータをリクエストする間隔を指定します。デフォルトの間隔は 5 秒です。
- ハートビート - 監視対象のコンポーネントがワンビュー モニターにハートビートを送信する間隔を指定します。認証サーバおよび許可サーバに対しては、ハートビートはコンポーネントがアクティブかどうかを示します。Web エージェントに対しては、ハートビートはワンビュー モニターが Web エージェントの動作データを受信する間隔を指定します。デフォルト値は 30 秒です。

デフォルト値を変更する方法

1. `Policy_Server_installation/monitor/mon.conf` を開きます。
2. 必要に応じて、次のプロパティとペアになっている値を変更します。
 - リフレッシュ間隔： `nete.mon.refreshPeriod`
 - ハートビート： `nete.mon.hbPeriod`

注：これらのプロパティの値は秒単位で指定します。

3. `mon.conf` を保存して閉じます。
4. OneView モニタを再起動します。

詳細情報:

[Windows システムでのポリシー サーバサービスの開始と終了 \(P. 26\)](#)

[UNIX システムでのポリシー サーバプロセスの開始と終了 \(P. 26\)](#)

OneView モニタのポート番号の設定

OneView モニタは、以下のデフォルト ポート番号を使用します。

- OneView エージェント -- 44449

注: デフォルト ポートが使用されている場合、OneView エージェントでは、そのポート上でのみリスンします。デフォルト ポートが変更された場合、OneView エージェントは、指定したポート上でリスンし、指定したリモート ホスト上で同じポートに接続します。たとえば、ポートを 55555 に変更した場合、OneView エージェントはポート 55555 上でリスンし、リモート ホスト上でポート 55555 に接続します。

- OneView モニタ -- 44450

デフォルトのポート番号を変更する方法

1. `Policy_Server_installation_directory/config/conapi.conf` ファイルをテキスト エディタで開きます。
2. 必要に応じて、以下の OneView エージェント プロパティの値を変更します。

```
nete.conapi.service.monagn.port=port_number
```

```
nete.conapi.service.monagn.host=fully_qualified_domain_name_of_remote_host
```

3. 必要に応じて、以下の OneView モニタ プロパティの値を変更します。

```
nete.conapi.service.mon.port=port_number
```

4. `conapi.conf` ファイルを保存して閉じます。

注: `conapi.conf` 内のプロパティの詳細については、`conapi.conf` ファイルの注記を参照してください。

5. OneView モニタを再起動します。

詳細情報:

[Windows システムでのポリシー サーバサービスの開始と終了 \(P. 26\)](#)

[UNIX システムでのポリシー サーバプロセスの開始と終了 \(P. 26\)](#)

[クラスタの集中監視用のポリシー サーバ設定 \(P. 192\)](#)

クラスタ化された環境の監視

クラスタ化されていない SiteMinder 環境では、監視プロセスは、ポリシー サーバと同じシステムに配置されます。監視ユーザインタフェースと SNMP によって、単一のポリシー サーバの情報が提供されます。クラスタを監視するには、単一の監視プロセスで処理されるようクラスタ内のポリシー サーバを設定する必要があります。ポリシー サーバ管理コンソールを使用すると、監視プロセス ホストを指定できます。

クラスタ化された環境で監視機能を実装する場合は、以下の点を考慮します。

- ポリシー サーバと監視プロセスの間の通信には、セキュリティ保護されていないネットワークチャネルが使用されます。
- 監視プロセスに障害が発生すると、すべての監視作業が中断されます。また、監視ホストとの接続が切れると、監視作業が中断されます。
- クラスタでは、SNMP による監視がサポートされています。

注: クラスタ化を有効にしないことによって、すべてのサーバはデフォルトクラスタに含まれます。クラスタ化されていない環境に対しては、集中監視を有効にすることができます。

詳細情報:

[クラスタ化されているポリシー サーバを集中監視用のポリシー サーバの監視対象にする \(P. 193\)](#)

OneView ビューアへのアクセス

OneView ビューアにアクセスする前に、OneView モニタ サービスが動作していることを確認してください。

OneView ビューアにアクセスするには、ブラウザで次の URL を入力します。

`http://your_server.your_company.org:port/sitemindermonitor`

ここで、`your_server.your_company.org:port` は、ホスト名または IP アドレス、および OneView モニタ用に Web サーバで設定されているポート番号です。

注: OneView モニタ用に Web サーバを設定する方法については、「ポリシー サーバインストールガイド」を参照してください。

OneView ビューアの保護

OneView ビューアを保護するには、`sitemindermonitor` のリソースを保護する SiteMinder ポリシーを作成します。

監視対象コンポーネントの表示

OneView モニタには、次のデフォルト テーブルが用意されています。

- すべてのコンポーネント (表示済み)
- ポリシー サーバ
- エージェント

OneView を開くと、[全コンポーネント] テーブルが表示されます。

注: Apache または iPlanet 6.0 Web サーバにインストールされている Web エージェントは、その Web エージェントがポリシー サーバにリソースが保護されているかどうかを確認するまでは、ワンビュー ビューアに表示されません。Web エージェントがポリシー サーバに情報をリクエストすると、Web エージェントが OneView モニタに登録されます。

OneView ビューアは、設定可能なテーブルに動作データを表示します。テーブルには、[詳細] 列を含めることができます。[詳細] 列のアイコンをクリックすると、特定のコンポーネントのすべての監視対象データを表示するウィンドウが開きます。

OneView の表示をカスタマイズする方法

OneView の表示のカスタマイズには、以下が含まれます。

- [テーブルのセットアップ](#) (P. 215)
- [アラートの設定](#) (P. 216)
- [テーブルの表示](#) (P. 216)
- [テーブルの並べ替え](#) (P. 217)
- [データ更新の設定](#) (P. 217)
- [設定の保存](#) (P. 217)
- [デフォルトの表示の変更](#) (P. 218)
- [設定のロード](#) (P. 218)

テーブルのセットアップ

テーブルをセットアップする方法

1. [設定] をクリックします。
テーブル設定ダイアログ ボックスが表示されます。
2. 以下のいずれかのオプションを実行します。
 - [既存のテーブル] を選択します。 リストボックスからテーブルを選択してください。
 - [新しいカスタム テーブル] を選択します。 [テーブル名] フィールドに名前を入力してください。
3. テーブルに表示するコンポーネントを選択します。
4. テーブルに表示するフィールドを選択します。 フィールドを選択し、上下矢印キーでフィールドの位置を変更して、フィールドを表示する順番を指定します。 使用できるフィールドは、選択したコンポーネントのタイプによって決まります。

注: 一部のフィールドの値は、継続的に増加する値 (コンポーネントを再起動するとリセットされる) または平均値 (最終更新時点以降) として表示することができます。 平均値を表示するには、最後に [/sec] の付いているフィールド名を選択してください。
5. [OK] をクリックします。

注: 設定が完了したら、必ずテーブルを保存してください。

詳細情報:

[設定の保存](#) (P. 217)

アラートの設定

アラートを設定する方法

1. [設定] をクリックします。
2. [アラート] タブをクリックします。
3. 左側のリストボックスからフィールドを選択します。このリストボックスには、現在ロードされているテーブルのすべてのフィールドが含まれています。
4. 中央のリストボックスからオペレータを選択します。
5. 手順 3 で選択したフィールドの値を指定します。
6. 必要に応じて、[テーブルセルを強調表示します] をオンにします。これにより、**OneView** では、指定した基準が満たされたときに、指定されたテーブルセルを強調表示します。
7. 必要に応じて、[Pop up a warning message] を選択します。これにより、**OneView** ビューでは、指定した基準が満たされたときに、ポップアップウィンドウを表示します。

テーブルの表示

テーブルを表示するには、ビューアのメインページの [テーブルの表示] リストボックスからテーブルを選択します。このリストからテーブルを選択すると、**OneView** では、選択されたテーブルを既存のテーブルの下に表示します。

テーブルを非表示にするには、[非表示] ボタンをクリックします。

テーブルの並べ替え

テーブルの各列のデータを昇順または降順にソートすることができます。列のソートにより、テーブルの編成が容易になります。たとえば、[ステータス]に基づいてテーブルをソートすると、アクティブでないすべてのコンポーネントをまとめて表示することができます。

注: 列の見出しに表示される矢印は、その列に基づいて並べ替えが行われたことを示しています。

データ更新の設定

デフォルトでは、OneView は、30 秒ごとにデータを更新します。以下の操作を行うことができます。

- 自動更新の間隔を変更
- ブラウザの表示を更新したときにだけデータを更新するように OneView を設定

データ更新を設定する方法

1. [更新] をクリックします。
[更新] ダイアログ ボックスが表示されます。
2. 以下のいずれかを選択します。
 - 自動更新 -- 指定した時間ごとにデータを更新します。秒単位で時間間隔を指定します。
 - 手動更新 -- ユーザがページの表示をリフレッシュしたときにデータを更新します。
3. [OK] をクリックします。

設定の保存

設定を保存すると、次の項目が保存されます。

- テーブルの定義
- メインページの表示
- テーブルのソート
- 更新間隔

設定を保存する方法

1. [設定を保存] をクリックします。
設定に名前を付けるためのダイアログ ボックスが表示されます。
2. テキストボックスに名前を入力します。
3. [OK] をクリックします。

デフォルトの表示の変更

デフォルトの表示を変更する方法

1. `siteminder_installation¥monitor¥settings` にある `defaults` ファイルの名前を変更します。
2. OneView モニタ コンソールで、設定を行います。
3. 設定をデフォルトとして保存します。

設定のロード

設定をロードする方法

1. [設定をロード] をクリックします。
ロードする設定を選択するためのダイアログ ボックスが表示されます。
2. リストボックスから設定を選択します。
3. [OK] をクリックします。

第 18 章: SNMP による SiteMinder の監視

このセクションには、以下のトピックが含まれています。

[SNMP 監視 \(P. 219\)](#)

[SiteMinder MIB \(P. 223\)](#)

[SiteMinder イベント マネージャの設定 \(P. 233\)](#)

[SiteMinder SNMP サポートの開始と終了 \(P. 235\)](#)

[SiteMinder SNMP モジュールのトラブルシューティング \(P. 237\)](#)

SNMP 監視

SiteMinder の SNMP モジュールを使用すると、SNMP 対応ネットワーク管理アプリケーションによる SiteMinder 環境のさまざまな動作ステータスの監視が可能になります。

SNMP の概要

ネットワーク管理には、2つのタイプのシステムが関係しています。1つは、制御するシステムで管理システムと呼ばれ、もう1つは、監視され、制御されるシステムで管理対象システムと呼ばれます。管理対象システムには、ホストやサーバ、それらのシステム上で動作するソフトウェアコンポーネント、あるいはネットワークコンポーネント(ルーター、インテリジェントリピータなど)が含まれる場合があります。

相互運用性を向上させるため、連携するシステムでは、業界標準の SNMP (Simple Network Management Protocol) をサポートしています。SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。

完全な SNMP ソリューションには、次の 3 つのコンポーネントが含まれます。

- **SNMP MIB (Management Information Base)** - 管理対象オブジェクトのデータベースです。管理対象オブジェクト (変数) は、管理システムによって読み込まれ、管理対象システムに関する情報を提供します。
- **SNMP エージェント** - 管理対象システムに関する情報にアクセスして、その情報を管理システムが利用できるようにする低負荷のソフトウェアモジュールです。ソフトウェアシステムの場合、エージェント機能は、マスタエージェント (ホストオペレーティングシステムが提供) とサブエージェント (管理対象アプリケーションが提供) に分割される場合があります。

注: SNMP エージェントは、すべての SNMP 実装に含まれる標準コンポーネントです。SiteMinder エージェントと混同しないでください。

- **SNMP マネージャ** - 一般には、HP OpenView などのネットワーク管理システム (NMS) アプリケーションです。

SiteMinder SNMP モジュールは、SiteMinder 環境で SNMP リクエスト処理機能と設定可能なイベントトラップ機能を実現します。その仕組みは、SiteMinder OneView モニタから動作データを収集し、そのデータを SNMP プロトコルをサポートするサードパーティ製 NMS アプリケーション (HP OpenView など) で利用できるように MIB に組み込むことです。

注: 6.0 SNMP エージェントは、SiteMinder 5.x ベースのすべてのエージェントアプリケーションと互換性があります。

SiteMinder SNMP モジュールのコンポーネント

SiteMinder SNMP モジュールは、以下のコンポーネントで構成されます。

- **SiteMinder SNMP MIB** - SNMP 対応ネットワーク管理システムによって監視できる SiteMinder オブジェクトのデータベースです。
- **SiteMinder SNMP サブエージェント** - SNMP マスタ エージェントから受信した SNMP リクエスト (GET および GETNEXT のみ) に応答します。
- **SiteMinder イベント マネージャ** - ポリシー サーバ イベントを取り込み、設定されている場合には SNMP トラップ (一部のイベントの発生を示すために SNMP エージェントが SNMP NMS に送信する非請求メッセージ) を生成します。

詳細情報:

[SiteMinder MIB \(P. 223\)](#)

[SiteMinder SNMP サポートの開始と終了 \(P. 235\)](#)

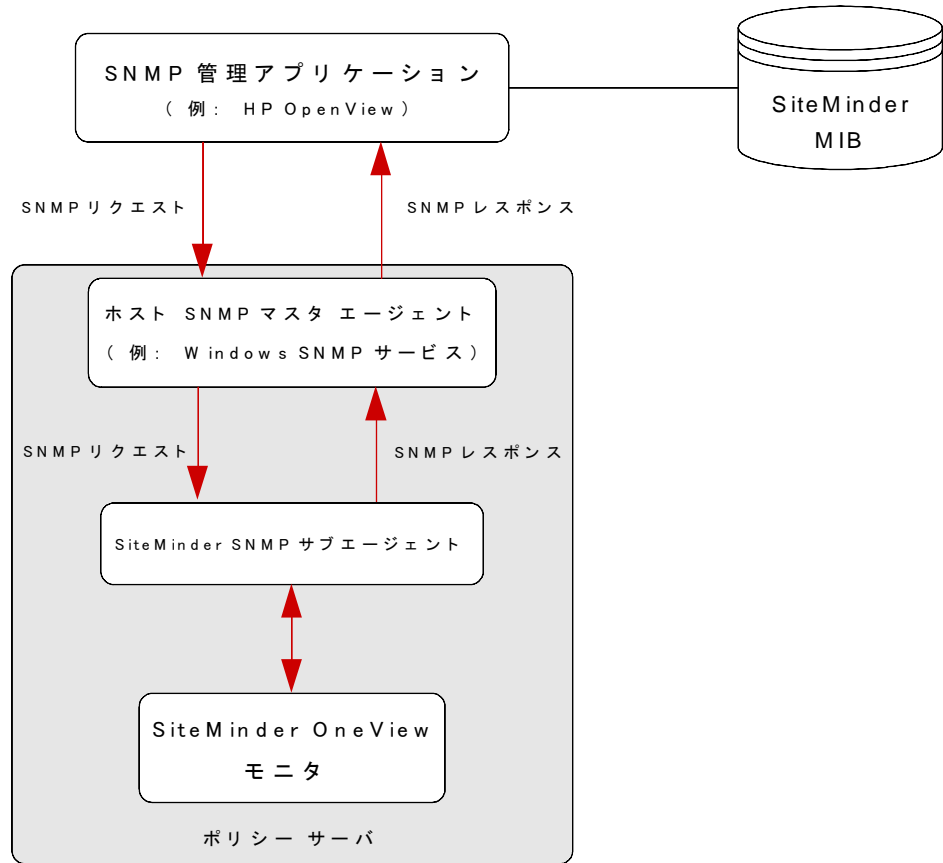
依存関係

SiteMinder SNMP モジュールには、以下の依存関係があります。

- **SiteMinder OneView モニタ** - SiteMinder SNMP モジュールは、OneView モニタから動作情報を取得します。SiteMinder SNMP モジュールを動作させるすべてのポリシー サーバで、OneView モニタも設定し、動作させる必要があります。
- **SNMP マスタ エージェント** - SiteMinder SNMP モジュールは、SNMP マスタ エージェントを提供しません。SiteMinder SNMP モジュールを動作させるポリシー サーバのオペレーティングシステムに適した SNMP マスタ エージェント (Windows SNMP サービスまたは Solstice エンタープライズ マスタ エージェント) がインストールされ、有効になっていることも必ず確認するようにしてください。

SNMP コンポーネントのアーキテクチャとデータフロー

以下の図は、SNMP モジュールのデータフローを示しています。



SiteMinder SNMP のデータフローは以下のとおりです。

1. SNMP マスタエージェントが、管理アプリケーションから SNMP リクエストを受信します。
2. SNMP マスタエージェントが、SNMP リクエストを SNMP サブエージェントに転送します。
3. SiteMinder SNMP サブエージェントが、リクエストされた情報を OneView モニタから取得します。
4. SiteMinder SNMP サブエージェントが、取得した情報を SNMP マスタエージェントに転送します。
5. SNMP マスタエージェントが、SNMP レスポンスを生成して、リクエスト元の管理アプリケーションに送信します。

SiteMinder MIB

SiteMinder MIB は、SiteMinder 環境のすべての監視対象コンポーネントについて、SNMPv2 に準拠したデータ表現を提供します。

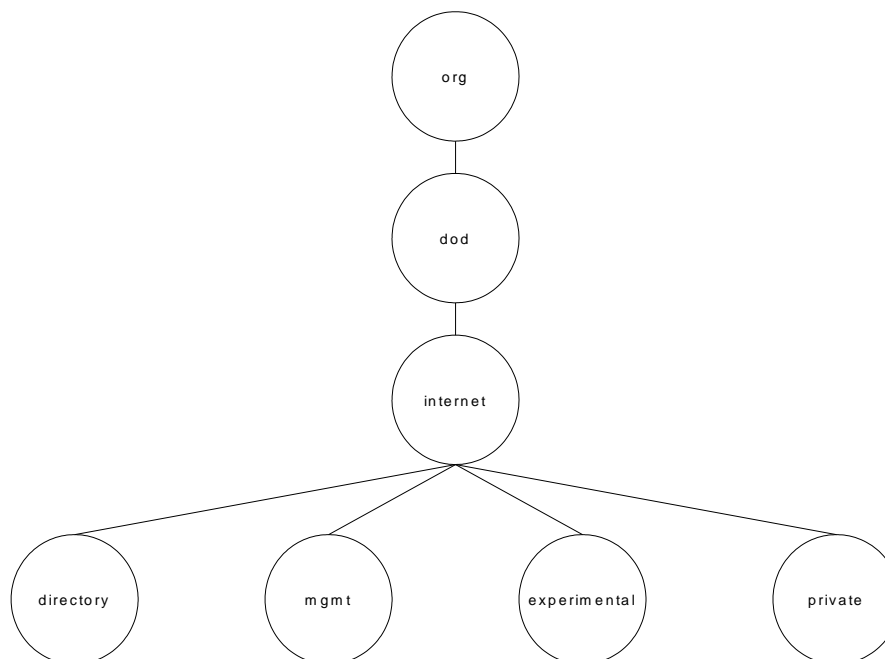
SiteMinder MIB は、次の ASCII テキスト形式のファイルです。

`SiteMinder_Install_Directory\mibs\NetegritySNMP.mib`

MIB の概要

SNMP MIB の構造は、逆ツリー階層によって論理的に表現されます。SiteMinder のようなインターネットに関する製品の MIB は、MIB 階層の ISO メインブランチの下にあります。

以下の図は、ISO ブランチの上部階層を示しています。

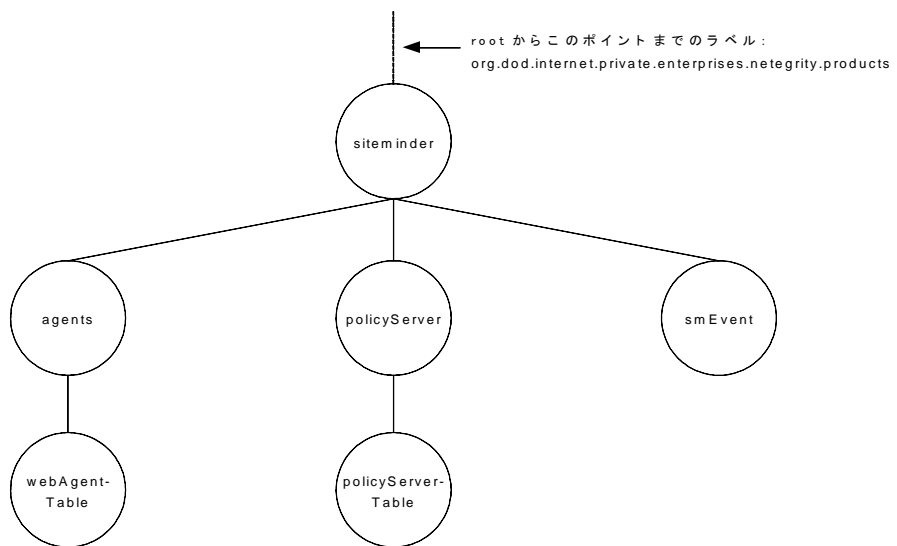


MIB ブランチ、MIB、および MIB 内の管理対象オブジェクトはすべて、短いテキスト文字列によって識別されます。完全な MIB 階層は、ブランチ識別子とオブジェクト識別子を連結して (ピリオド区切り) 表記することができます。たとえば、上の図に示されている `internet` エントリの `private` サブブランチは、`iso.org.dod.internet.private` と表記できます。

SiteMinder MIB 階層

SiteMinder MIB は、*iso.org.dod.internet.private.enterprises.netegrity.products.siteminder* と表記できます。

MIB オブジェクトによって表される、サポートされている管理対象コンポーネントは、ポリシーサーバと Web エージェントです。各コンポーネントの複数のインスタンスが存在する可能性があるため、これらのコンポーネントのそれぞれが持つ管理対象プロパティは、列オブジェクトになります。



STMNDR MIB には、以下の 3 つのサブブランチがあります。

ポリシー サーバ

ポリシーサーバ (`policyServerTable`) オブジェクトが入っています。

エージェント

Web エージェント (`webAgent`) オブジェクトが入っています。

smEvent

システムイベントの SNMP トラップタイプが入っています。

MIB オブジェクトの参照リスト

以下のセクションには、ポリシーサーバ、Web エージェント、およびイベント MIB オブジェクトの詳細を示したリストが含まれています。

認証サーバのデータ

以下の表は、SiteMinder MIB (iso.org.
～.siteminder.policyServer.policyServerTable) にオブジェクトとして示される認証サーバのプロパティのサブセットのリストです。

オブジェクト名	SNMP タイプ	オブジェクトの説明
policyServerIndex	Integer32	現在のポリシー サーバインスタンスの固有識別子。
policyServerHostID	IP アドレス	ポリシー サーバがインストールされているマシンの IP アドレス。
policyServerType	表示可能な文字列	コンポーネントのタイプ。
policyServerStatus	Integer32	ポリシー サーバのステータス。値は、Active または Inactive です。
policyServerPort	Integer32	ポリシー サーバのポート番号。
policyServerProduct	表示可能な文字列	ポリシー サーバの製品名。
policyServerPlatform	表示可能な文字列	ポリシー サーバがインストールされているマシンのオペレーティングシステム。
policyServerVersion	表示可能な文字列	ポリシー サーバのバージョン番号。
policyServerUpdate	表示可能な文字列	最後に適用された更新ファイルのバージョン番号。
policyServerLabel	表示可能な文字列	ポリシー サーバのビルド番号。
policyServerCrypto	Integer32	Web エージェントとポリシー サーバの間で送信されるデータの暗号化/復号化に使用される暗号化キーの長さ。
policyServerUTC	表示可能な文字列	ポリシー サーバがインストールされている Web サーバが起動した日時。日時は、万国標準時形式で示されます。
policyServerTime Zone	Integer32	ポリシー サーバがインストールされているマシンの設置場所のタイムゾーン。

オブジェクト名	SNMP タイプ	オブジェクトの説明
policyServerMaxSockets	Integer32	ポリシー サーバがサポートできる開いているソケットの最大数 (開いているソケットの数はポリシー サーバと Web エージェントの間の開いている接続の数に対応します)。
policyServerSocketCount	Gauge32	開いているソケットの数。この数は、ポリシー サーバと Web エージェントの間の開いている接続の数に対応します。
policyServerAuthAcceptCount	Counter32	成功した認証の数。
policyServerAuthReject-Count	Counter32	失敗した認証試行の回数。これらの試行は、認証情報が無効であったために失敗しました。
policyServerAzAccept-Count	Counter32	成功した許可の数。
policyServerAzReject-Count	Counter32	失敗した許可試行の回数。これらの試行は、認証情報が無効であったために失敗しました。
policyServerPolicy-CacheEnabled	真理値	ポリシー キャッシュが有効になっているかどうかを示す値。
policyServerL2Cache-Enabled	真理値	L2 キャッシュが有効になっているかどうかを示す値。

SiteMinder MIB 内の Web エージェント オブジェクト

以下の表は、SiteMinder MIB (iso.org. ~ siteminder.webAgentTable.webAgentEntry) にオブジェクトとして示される Web エージェントのプロパティのリストです。

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentIndex	Integer32	現在の Web エージェントインスタンスの固有識別子。
webAgentHostID	IP アドレス	Web エージェントサーバがインストールされているマシンの IP アドレス。
webAgentType	表示可能な文字列	コンポーネントのタイプ。

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentStatus	Integer32	Web エージェントのステータス。値は、Active または Inactive です。
webAgentPort	Integer32	Web エージェントのポート番号。
webAgentProduct	表示可能な文字列	Web エージェントの製品名。
webAgentPlatform	表示可能な文字列	Web エージェントがインストールされているマシンのオペレーティングシステム。
webAgentVersion	表示可能な文字列	Web エージェントのバージョン番号。
webAgentUpdate	表示可能な文字列	最後に適用された更新ファイルのバージョン番号。
webAgentLabel	表示可能な文字列	Web エージェントのビルド番号。
webAgentCrypto	Integer32	Web エージェントとポリシー サーバの間で送信されるデータの暗号化/復号化に使用される暗号化キーの長さ。
webAgentUTC	表示可能な文字列	Web エージェントがインストールされている Web サーバが起動した日時。日時は、万国標準時形式で示されます。
webAgentTime Zone	Integer32	Web エージェントがインストールされているマシンの設置場所のタイムゾーン。
webAgentSocketCount	Gauge32	開いているソケットの数。この数は、ポリシー サーバと Web エージェントの間の開いている接続の数に対応します。 注: Web エージェント アーキテクチャが変わったので、SocketCount には値がありません。
webAgentResource-CacheCount	Integer32	リソースキャッシュのエントリ数。リソースキャッシュには、最近アクセスされたリソースに関する情報が保存されます。これにより、同じリソースに関するその後のリクエストの処理速度が向上します。 リソース キャッシュ内のエントリ数は、0 ~ n になります。n は、Web エージェントの設定で指定される最大キャッシュ サイズです。

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentResource-CacheHits	Integer32	リソースキャッシュがアクセスされた回数。この数は、キャッシュされたリソースを SiteMinder が使用する頻度を示しています。
webAgentResource-CacheMisses	Integer32	<p>Web エージェントがリソースキャッシュ内でリソースを検出できなかった回数。次のような場合には、リソースを検出できません。</p> <ul style="list-style-type: none"> ■ そのリソースにまだ一度もアクセスしていない場合 ■ キャッシュされた情報の有効期限が切れた場合
webAgentUserSession-CacheCount	Integer32	<p>ユーザセッションキャッシュのエントリ数。ユーザセッションキャッシュには、リソースに最近アクセスしたユーザに関する情報が保存されます。ユーザ情報を保存することによって、リソースリクエストの処理速度が向上します。</p> <p>ユーザセッションキャッシュ内のエントリ数は、0 ～ n になります。n は、Web エージェントの設定で指定される最大キャッシュサイズです。</p> <p>注: ユーザセッションキャッシュ数は、セッションキャッシュが存在する Web サーバによって異なります。</p>
webAgentUserSession-CacheHits	Integer32	Web エージェントがユーザセッションキャッシュにアクセスした回数。
webAgentUserSession-CacheMisses	Integer32	<p>Web エージェントがユーザセッションキャッシュ内でユーザセッション情報を検出できなかった回数。次のような場合には、リソースを検出できません。</p> <ul style="list-style-type: none"> ■ そのリソースにまだ一度もアクセスしていない場合 ■ キャッシュされた情報の有効期限が切れた場合

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentIsProtected-Count	Integer32	<p>リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認した回数。</p> <p>注: リソースキャッシュが 0 に設定されている場合、ログイン試行のたびに複数の IsProtected 呼び出しが記録されることがあります。Web エージェントが情報をキャッシュしていない場合、Web エージェントは、Web サーバにリクエストがあるたびに、リソースが保護されているかどうかをポリシー サーバに確認する必要があります。</p> <p>リソースキャッシュが 0 に設定されていない場合、1 回の IsProtected 呼び出しだけが記録されます。この場合、Web エージェントは、ポリシー サーバに IsProtected 呼び出しを 1 回だけ実行します。同じリソースに関するその後の Web サーバへのリクエストは、Web エージェントのリソース キャッシュの有効期限が切れていないか、キャッシュがクリアされていない限り、キャッシュされた情報を使用して処理されます。</p>
webAgentIsProtected-Errors	Integer32	<p>リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認する際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。</p>
webAgentIsProtected-AvgTime	Unsigned 32	<p>リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認するためにかかる平均時間。</p>
webAgentLoginCount	Counter 32	<p>この Web エージェントからのログイン試行の回数。</p>
webAgentLoginErrors	Counter 32	<p>ログイン試行の際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。</p>
webAgentLoginFailures	Counter 32	<p>ユーザがポリシー サーバによって認証または許可されていなかったために失敗したログイン試行の回数。</p>
webAgentLoginAvgTime	Unsigned 32	<p>ユーザがリソースにログインするためにかかった平均時間。</p>

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentValidation-Counter	Counter 32	特定の Web エージェントが、ユーザを認証するために、ユーザのクレデンシャルをユーザディレクトリエントリと照合する代わりに、ポリシーサーバに対してセッション cookie の正当性の検証を試行した回数 (Web エージェントは、ユーザが正常に認証されたときにユーザのブラウザ上にセッション cookie を作成し、その cookie を使用して、新しいリソースに対するその後のリクエストでユーザを認証します)。
webAgentValidation-Errors	Counter 32	Web エージェントによるユーザセッションの正当性の検証試行の際にエラーが発生した回数。エラーは、Web エージェントとポリシーサーバの間で通信障害が発生したことを示しています。
webAgentValidation-Failures	Counter 32	セッション cookie が無効であったために Web エージェントがユーザセッションの正当性を検証できなかった回数。
webAgentValidation-AvgTime	Unsigned 32	ユーザの認証に使用される cookie の正当性の検証にかかった平均時間 (ミリ秒単位)。シングルサインオン環境では、ユーザの認証に cookie が使用される場合があります。
webAgentAuthorize-Counter	Counter 32	このエージェントによる許可試行の回数。許可試行は、ユーザが保護されたリソースにアクセスするためにポリシーサーバに認証情報を提示すると発生します。
webAgentAuthorize-Errors	Counter 32	この Web エージェントによる許可試行の際にエラーが発生した回数。エラーは、許可呼び出し時に Web エージェントとポリシーサーバの間で通信障害が発生したことを示しています。
webAgentAuthorize-Failures	Counter 32	失敗した許可試行の回数。許可試行は、ユーザが無効な認証情報を入力すると失敗します。
webAgentAuthorize-AvgTime	Integer32	ユーザの許可にかかった平均時間 (ミリ秒単位)。

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentCrosssite-ScriptHits	Integer32	クロスサイトスクリプティングを検出した回数。これは、サイトのページに埋め込まれた不正コードの数を示しています。クロスサイトスクリプティングの詳細については、「 <i>SiteMinder Web</i> エージェント設定ガイド」を参照してください。
webAgentBadURL-charsHits	Integer32	URL の文字が無効であったためにエージェントが拒否したリクエストの数。Web クライアントが SiteMinder ルールに反することを防ぐために、無効な URL 文字は、明示的にブロックされます。これらの文字は、Web エージェントの設定で指定します。
webAgentBadCookie-HitsCount	Gauge32	Web エージェントが復号できなかった cookie の数。
webAgentExpired-CookieHitsCount	Gauge32	有効期限の切れた cookie を含んでいたリクエストの数。

イベントのデータ

以下の表は、SiteMinder イベント マネージャを使用して SNMP トラップにマップできるシステム イベント用の SiteMinder MIB (iso.org.~.siteminder.smEvents) のオブジェクトのリストです。

イベント名	イベント ID	イベント カテゴリ	イベントカテゴリのタイプ
serverInit	SmLogSystemEvent_ServerInit	サーバアクティビティ	システム
serverUp	SmLogSystemEvent_ServerUP		
serverDown	SmLogSystemEvent_ServerDown		
serverInitFail	SmLogSystemEvent_ServerInitFail		
dbConnectionFailed	SmLogSystemEvent_DbConnectFail		

イベント名	イベント ID	イベント カテゴリ	イベントカテゴリの タイプ
ldapConnection-Failed	SmLogSystemEvent_LDAP-ConnectFail		
logFileOpenFail	SmLogSystemEvent_LogFile-OpenFail	システム アク ティビティ	
agentConnection-Failed	SmLogSystemEvent_Agent-Connectio nFail		
authReject	SmLogAccessEvent_AuthReject	認証	アクセス
validateReject	SmLogAccessEvent_ValidateReject		
azReject	SmLogAccessEvent_AzReject	許可	
adminReject	SmLogAccessEvent_AdminReject	管理	
objectLoginReject	SmLogObjEvent_LoginReject	認証	オブジェクト
objectFailedLogin AttemptsCount	SmLogObjEvent_FailedLogin-Attempts Count		
emsLoginFailed	SmLogEmsEvent_LoginFail	ディレクトリ セッション	EMS
emsAuthFailed	SmLogEmsAuthFail		

SiteMinder イベント マネージャの設定

ポリシー サーバのイベントを取り込むイベント マネージャ アプリケーション (EventSNMP.dll というライブラリ ファイルとして提供) は、そのイベントに対して、設定ファイルの指定に基づいて SNMP トラップを生成する必要があるかどうかを判断し、生成する必要がある場合には、指定された NMS に対して SNMP トラップを生成します。

イベント ライブラリ (EventSNMP.dll) を設定するには、「[イベントハンドラライブラリの追加 \(P. 156\)](#)」を参照してください。

SiteMinder イベント マネージャを設定するには、イベント設定ファイル (`SM_Install_Directory¥config¥snmptrap.conf`) を定義します。このファイルには、処理するイベントと、トラップの送信先となる NMS のアドレスが定義されています。

イベント設定ファイルの構文

snmptrap.conf は、編集可能な ASCII ファイルで、次のような単純な構文 (イベントごとに 1 行) が使用されます。

Event_Name *Destination_Address*

Event_Name

MIB イベントオブジェクトの名前 (またはカンマ区切りのイベントオブジェクト名のグループ)。

例 :

serverUP

serverUp,serverDown

serverUp,serverDown,serverInitFail

Destination_Address

生成したトラップを送信する NMS のアドレス (またはカンマ区切りの NMS のアドレスのグループ)。各アドレスは、*HostID:port:community* という形式で指定する必要があります。

HostID

(必須) ホスト名または IP アドレスを入力します。

Port

(オプション) IP ポート番号。

デフォルト : 162

Community

(オプション) SNMP コミュニティ。コミュニティ名を指定する場合は、必ずポートも指定してください。

デフォルト : 「public」

例 : 100.132.5.166

例 : 100.132.5.166:162

例 : victoria:162:public

注: イベントが重複しないように注意してください。つまり、同じイベントを複数のエントリに割り当てないでください。コメント行を追加することもできます。コメント行の先頭には「#」記号を付けてください。

イベント設定ファイルの例

```
ServerDown,serverUp 111.123.0.234:567:public
```

このエントリによって、イベントマネージャは、SNMP トラップの `serverDown` と `serverUp` を IP アドレス `111.123.0.234`、ポート `567`、コミュニティ名 `public` の NMS に送信するように設定されます。

```
agentConnectionFailed 111.123.0.234,victoria
```

このエントリによって、イベントマネージャは、`agentConnectionFailed` タイプの SNMP トラップを IP アドレス `111.123.0.234`、ポート `567`、コミュニティ名 `public` と、ホスト「`victoria`」、ポート `567`、コミュニティ名 `public` に送信するように設定されます。

azReject

このエントリによって、イベントマネージャは、**azReject** タイプのすべてのイベントを破棄するように設定されます。そのため、トラップは送信されません。

SiteMinder SNMP サポートの開始と終了

ポリシー サーバのインストール時に **SiteMinder SNMP** サポートのインストールを選択すると、ポリシー サーバの初期化のたびに **SiteMinder SNMP** エージェント サービスが自動的に開始されます。

このセクションでは、**Windows** および **UNIX** 環境のポリシー サーバで **SiteMinder SNMP** サブエージェントを手動で開始および終了する方法について説明します。

Windows 環境の Netegrity SNMP エージェント サービスの開始と終了

Windows 環境のポリシー サーバで SiteMinder SNMP サブエージェントを開始する方法

1. コントロールパネルの [サービス] を開きます。
 - (Windows Server) [スタート]、[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。
 - (Windows NT) [スタート]、[設定]、[コントロールパネル]、[サービス] の順に選択します。
2. **Netegrity SNMP Agent** サービスを選択します。
3. [開始] をクリックします。

注: Windows SNMP サービスを再起動した場合、**Netegrity SNMP** エージェント サービスも手動で再起動する必要があります。

Windows 環境のポリシー サーバで SiteMinder SNMP サブエージェントを終了する方法

1. コントロールパネルの [サービス] を開きます。
 - (Windows Server) [スタート]、[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。
 - (Windows NT) [スタート]、[設定]、[コントロール パネル]、[サービス] の順に選択します。

2. Netegrity SNMP Agent サービスを選択します。

3. [停止] をクリックします。

注: Windows SNMP サービスを停止すると、Netegrity SNMP エージェント サービスが全般的に使用できなくなりますが、ポート 801 を使用してアクセスすることは可能です。

UNIX 環境のポリシー サーバでの SNMP サポートの開始と終了

UNIX 環境のポリシー サーバでは、Sun Solstice エンタープライズ マスタ エージェント (snmpdx) デーモンを開始または停止することによってのみ、SiteMinder サービスを開始または終了できます。

UNIX 環境のポリシー サーバで Netegrity SNMP エージェント サービスを開始する方法

1. スーパーユーザ (ルート) としてログインします。
2. `cd /etc/rc3.d` と入力します。
3. `sh SXXsnmpdx (S76snmpdx) stop` と入力します。

UNIX 環境のポリシー サーバで Netegrity SNMP エージェント サービスを終了する方法

1. スーパーユーザ (ルート) としてログインします。
2. `cd /etc/rc3.d` と入力します。
3. `sh SXXsnmpdx (S76snmpdx) start` と入力します。

注: Sun Solstice エンタープライズ マスタ エージェントの動作を停止させると、UNIX ホスト上のすべての SNMP サービスが無効になります。

SiteMinder SNMP モジュールのトラブルシューティング

このセクションでは、SiteMinder への管理接続を確立できない場合や、SiteMinder から SNMP トラップを受信できない場合に、障害の原因を容易に特定できるようにするための手順および SiteMinder で用意されているツールについて説明します。

イベントが発生しても SNMP トラップが受信されない

問題の状況:

SNMP トラップが生成されるはずのイベントが発生しても、SNMP トラップが受信されない。

解決方法:

1. NMS と監視対象ポリシー サーバの間のネットワーク接続を確認します。
2. ポリシー サーバ上で SiteMinder SNMP サブエージェントと SNMP マスタ エージェントが動作していることを確認します。
3. システム環境変数の NETE_SNMPLOG_ENABLED を設定して、トラップログを有効にします。

SiteMinder は、`sminstalldir/log` に以下のログファイルを生成します。

Windows の場合:

```
SmServAuth_snmptrap.log  
SmServAz_snmptrap.log  
SmServAcct_snmptrap.log  
SmServAdm_snmptrap.log
```

UNIX の場合:

```
smservauth_snmptrap.log  
smservaz_snmptrap.log  
smservacct_snmptrap.log  
smservadm_snmptrap.log
```

重要: 生成されるログファイルは、急速に大きくなります。トラップの受信に関する問題が解決したら、すぐにトラップログを無効にして、ファイルを削除してください。

第 19 章: SiteMinder レポート

このセクションには、以下のトピックが含まれています。

[レポートの説明](#) (P. 239)

[SiteMinder レポートのスケジュール](#) (P. 241)

[SiteMinder レポートの表示](#) (P. 241)

[SiteMinder レポートの削除](#) (P. 242)

レポートの説明

SiteMinder レポートは以下の 2 つのグループに分けられます。

- 監査レポート
- 分析レポート

監査レポートは、ポリシー サーバの既存の監査機能から作成されます。データベースへの書き込みを行うようにポリシー サーバを設定する必要があります。

分析レポートは、実行時のポリシー評価に基づいています（どのユーザが何のタスクを実行できるかの評価など）。

SiteMinder 管理 UI を使用すると、以下のレポートを生成できます。

ユーザ別アクティビティ

指定された期間内のユーザ アクティビティをすべてリスト表示します。

管理者による管理上の操作

管理者によって行われるポリシー ストア内の管理操作をすべてリスト表示します。

アプリケーション

ユーザが使用を許可されている設定済みのアプリケーションをすべてリスト表示します。

ユーザ別アプリケーション

指定されたアプリケーションセットのユーザをすべてリスト表示します。

拒否された認可

拒否された認可をすべてリスト表示します。

拒否されたリソース

リクエストされたリソースの拒否をすべてリスト表示します。

ロールごとのポリシー

アプリケーション内の指定されたロールセットのポリシーをすべてリスト表示します。

保護されたリソース

保護されたリソースをすべてリスト表示します（レルムフィルタ + ルールフィルタ）。

リソース アクティビティ

リソース別の認証アクティビティと許可アクティビティをすべてリスト表示します。

ユーザ別リソース

指定されたユーザセットのリソースをすべてリスト表示します。

アプリケーション別ロール

指定された各アプリケーションについて定義されたロールをすべてリスト表示します。

リソース別ロール

指定されたリソースについて定義されたロールをすべてリスト表示します。

リソース別ユーザ

指定された各リソースに関連付けられているユーザをすべてリスト表示します。このレポートを実行するときは、ユーザディレクトリに有効なユニバーサル ID を設定したことを確認します。

ロール別ユーザ

指定されたロールに属するユーザをすべてリスト表示します。

SiteMinder レポートのスケジュール

管理 UI の [レポート] タブでは、SiteMinder の監査レポートまたは分析レポートをスケジュールできます。

次の手順に従ってください:

1. [レポート] タブをクリックし、[監査] または [分析] をクリックします。
2. リクエストするレポートを選択します。
3. 必要なパラメータをすべて入力します。これらのパラメータはレポートのタイプによって異なります。
4. [次へ] をクリックします。
5. ドロップダウンリストからオプションを 1 つ選択します。
6. 説明を入力します。
7. [サブミット] をクリックします。

SiteMinder レポートの表示

管理 UI の [レポート] タブでは、ステータスが [完了] になっているすべての SiteMinder レポートを表示できます。ステータスが [失敗] である場合は、そのステータスの詳細を見ることができます。

SiteMinder レポートを表示する方法

1. [レポート] - [一般] - [SiteMinder レポートの表示] をクリックします。
[SiteMinder レポート検索] ペインが表示されます。
2. 表示するレポートのラジオ ボタンをクリックします。レポートが完了済みであることが [ステータス] フィールドに示されている必要があることに注意してください。
3. [選択] をクリックします。
レポートが画面に表示されます。
4. (オプション) レポートをファイルに保存すれ場合は、ファイルアイコンをクリックします。ドロップダウンリストから出力ファイル形式を選択します。

5. (オプション) レポートを印刷する場合は、プリンタ アイコンをクリックします。
6. (オプション) レポートの各ページを読んだり、検索文字列を入力したりできます。
7. レポートをすべて見たら、[閉じる] をクリックします。

SiteMinder レポートの削除

管理 UI の [レポート] タブでは、1 つ以上の SiteMinder レポートを削除できます。

SiteMinder レポートを削除する方法

1. [レポート] - [一般] - [SiteMinder レポートの削除] をクリックします。
[SiteMinder レポートの削除] ペインが開きます。
2. 削除する SiteMinder レポートをレポート名または説明を条件にして検索するか、すべての SiteMinder レポートを検索します。
3. 削除する 1 つ以上の SiteMinder レポートまたはすべての SiteMinder レポートを選択し、[サブミット] をクリックします。

SiteMinder レポートの削除タスクが処理のためにサブミットされます。

第 20 章: ポリシー サーバのツール

このセクションには、以下のトピックが含まれています。

- [ポリシー サーバツールの導入](#) (P. 243)
- [smobjimport によるポリシーデータのインポート](#) (P. 247)
- [XML ベースのデータ形式の概要](#) (P. 248)
- [XPSExport](#) (P. 250)
- [XPSImport](#) (P. 262)
- [smkeyexport](#) (P. 265)
- [SiteMinder キー ツール](#) (P. 266)
- [smldapsetup](#) (P. 278)
- [ODBC データベース内の SiteMinder データの削除](#) (P. 289)
- [smpatchcheck](#) (P. 291)
- [SiteMinder テストツール](#) (P. 292)
- [smreg](#) (P. 292)
- [XPSCounter](#) (P. 293)
- [XPSConfig](#) (P. 296)
- [XPSEvaluate](#) (P. 300)
- [XPSExplorer](#) (P. 302)
- [XPSSecurity](#) (P. 313)
- [-XPSSweeper](#) (P. 316)

ポリシー サーバツールの導入

SiteMinder には、環境の管理を支援する数多くの管理ツールが用意されています。以下のリストで、各ツールの機能を説明します。

smobjimport

ポリシーデータを SiteMinder ポリシーストアにインポートします。

注: このユーティリティはポリシーストアに既存のバックアップ `smdif` ファイルをインポートする目的のみに使用できます。ポリシーストアを手動で移行するには、`XPSExport` および `XPSImport` ユーティリティを使用します。

smkeyexport

キーストアからキーをエクスポートします。

smkeyimport

キーをキー ストアにインポートします。

smkeytool

証明書データ ストアを管理できます。

また、このユーティリティにアクセス レガシー キー ストア フラグ (accessLegacyKS) を指定して、**12.52 SP1** への移行時に既存の smkeydatabase を管理することもできます。

注: 証明書データ ストアへの smkeydatabase のコンテンツの移行の詳細については、「SiteMinder アップグレードガイド」を参照してください。

smldapsetup

LDAP ディレクトリ内の SiteMinder ポリシー ストアを管理します。

ODBC データベースの SQL スクリプト

ODBC データベースから SiteMinder ポリシー ストア、トークンデータ、およびログ スキーマを削除します。

smpatchcheck

Solaris システムにすべての必要なパッチまたは推奨パッチがインストールされていることを確認します。

smreadclog

ポリシー サーバによって生成された RADIUS ログ ファイルを読み取ります。

smreg

SiteMinder スーパーユーザ パスワードを変更できます。

SiteMinder には、ポリシー データを操作するためのツールもあります。以下のリストに、XPS ツール ファミリーの概要を示します。XPS ツールは、ポリシー ストア データを管理する目的で XPS 管理者が使用できる、プラットフォームに依存しないコマンドラインユーティリティです。特定のツール用のオプションについて学習するには、コマンドラインでツール名を入力し、その後に疑問符を入力します。例：

XPSConfig ?

XPSConfig

ベンダー、製品、製品パラメータなどの設定データを管理します。

注：XPSConfig を使用するには、管理者アカウントに XPSConfig 権限が必要です。

XPSEvaluate

式を評価し、パフォーマンスをテストできるようにします。

注：XPSEvaluate を使用するには、管理者アカウントに XPSEvaluate 権限が必要です。

XPSExplorer

ベンダー、製品、アプリケーションなどのポリシー データを管理します。

注：XPSExplorer を使用するには、管理者アカウントに XPSExplorer 権限が必要です。

XPSExport

ポリシー ストアからデータをエクスポートします。

XPSImport

ポリシー ストアにデータをインポートします。

XPSSecurity

XPS 管理者とその権限を対話形式で作成および編集できます。このツールを使用するには、SiteMinder インストールファイル（サポートからダウンロードしたファイル）の `win32tools` または `/solaris/tools` から、`siteminder_home/bin` にツールをコピーします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

重要: XPSSecurity を使用した後は、不正使用を防ぐため、`siteminder_home/bin` から削除してください。

注: XPSSecurity を使用するには、管理者アカウントに XPSSecurity 権限が必要です。

XPSSweeper

XPS と SiteMinder ポリシー ストアを同期します。

注: XPSSweeper を使用するには、管理者である必要があります。その他の権限は必要はありません。

Windows 2008 ポリシー サーバツール要件

Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合、管理者としてシステムにログインしていても、必ず管理者権限でコマンド ライン ウィンドウを開くようにしてください。詳細については、お使いの SiteMinder コンポーネントの「リリース ノート」を参照してください。

Linux Red Hat 上でポリシー サーバのツールを使用する場合の要件

ポリシー サーバのツールを Linux Red Hat オペレーティング システム上で正しく動作させるには、`/etc/hosts` 内でポリシー サーバのホスト名を定義します。これらのユーティリティは adminoid と OID を生成するので、ホスト名をこの場所で定義します。Linux Red Hat オペレーティング システムでは、これらの OID を生成するとき、Linux 関数の `gethostid()` および `gettimeofday()` が使用されます。

smobjimport によるポリシー データのインポート

smobjimport ツールを使用して、ポリシー ストア全体または 1 つのポリシー ドメインをインポートできます。

注: このユーティリティはポリシー ストアに既存のバックアップ `smdif` ファイルをインポートする目的のみに使用できます。ポリシー ストアを手動で移行するには、`XPSEExport` および `XPSImport` ユーティリティを使用します。

次の手順に従ってください:

1. 次のいずれかのディレクトリに移動します。

- (Windows) `siteminder_home\bin`

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- (Unix) `siteminder_home/bin`

- 以下のコマンドを実行します。

```
smobjimport -ifile_name -dadmin-name -wadmin-pw -v -t [-cf | -cb]
```

例 1 : `smobjimport -ipstore.smdif -dSiteMinder -wpassword -v -t -cf`

例 2 : `smobjimport -ipstore.smdif -dSiteMinder -wpassword -v -t -cb`
`-cf`

(オプション) FIPS 準拠の (AES) 暗号化アルゴリズムを使用して、機密データをインポートします。

注: この引数は、ポリシー サーバが FIPS 専用モードで動作している場合にのみ必要です。

`-cb`

(オプション) RC2 暗号化アルゴリズムを使用して、機密データをインポートします。

重要:

- インポートするファイルに機密データがクリア テキストで含まれる場合、データをインポートするには以下のオプションが必要です。

`-c`

このオプションを使用しないと、ポリシー ストアが破損する場合があります。

- `smobjimport` コマンドを使用して `smdif` ファイルのみを入力します。`smdif` ファイルと `cfg` ファイルが同じディレクトリにある場合、ユーティリティは自動的に両方をインポートします。`cfg` ファイルに格納されている環境プロパティは、`smdif` ファイルに格納されている環境プロパティに優先します。別の `cfg` ファイルで `smdif` ファイルをペアにすることにより、環境のデータに上書きできます。

XML ベースのデータ形式の概要

エンタープライズ環境では、ポリシー ストアデータを環境間で移動しなければならない場合があります (開発環境からステージング環境へ、など)。r12 より前のリリースでは、ポリシー オブジェクトは専用の **SiteMinder Data Interchange Format (SMDIF)** を使用して表現され、データの移行には `smobjimport` および `smobjexport` を使用していました。このエクスポート形式は XML ベースのエクスポート形式に置き換えられ、データ移行ツールは `XPSExport` および `XPSImport` になりました。

XML ベースのエクスポート形式では、以下の基本スキーマを使用します。

XPSDeployment.xsd

トップレベルのスキーマを記述します。この下にその他のスキーマが含まれます。ルート要素とサブ要素を定義します。このスキーマに準拠した XML ファイルは、データディクショナリ、ポリシー、およびセキュリティデータのインスタンスを含むことができます。

XPSDataDictionary.xsd

オブジェクトタイプとそれらのプロパティに関するメタデータ情報を記述します。

XPSPolicyData.xsd

ポリシーストアに格納されるオブジェクト（ドメイン、ポリシー、ルール、アプリケーション、オブジェクト間のリレーションシップなど）に関するメタデータ情報を記述します。

XPSSecurityData.xsd

ポリシーストア管理者および管理者のアクセス権限を表すために使用されるメタデータを記述します。

XPSGeneric.xsd

その他のスキーマ ファイル内で使用される一般的なデータ型の定義が含まれます。

この形式はポリシー データ全体のエクスポートとインポートをサポートしているだけでなく、ポリシー データのサブセットのエクスポートとインポートもサポートしています。オブジェクト単位のエクスポートでは、データのインポート方法に関する知識が要求されます。エクスポート時は、ポリシー データ全体またはデータの一部（オブジェクト識別子を使用）と、オプションで以下の 3 つのエクスポート タイプのいずれかを指定できます。

- **Add** - インポート時に追加のみ実行できることを明示します。
- **Replace** - インポート時に既存のポリシー データを上書きすることを明示します。
- **Overlay** - インポート時にポリシー データを更新することを明示します。

注: XPSExport および XPSImport ツールは、ポリシー サーバが動作している FIPS モードに基づいて機密データを暗号化します。これらのツールには、データ暗号化のために設定する追加パラメータはありません。

XPSExport

XPSExport ツールは、ポリシー ストア データを移行するための以下のタスクをサポートしています。

- 全セキュリティ データのエクスポート
- 全ポリシー データのエクスポート
- 全設定データのエクスポート
- 一部のポリシー データのエクスポート

ルート オブジェクトの識別子を指定すると、ポリシー データのサブセットをエクスポートできます。 コマンドラインまたはファイルで (-xf パラメータを使用して) この識別子を指定します。 親クラスを持たないオブジェクトのみをエクスポートできます。 たとえば、レルム オブジェクトをエクスポートするには、レルムの親ドメインの識別子 (XID) を指定します。

また、XPSExplorer の「ショッピング カート」 (XCart) 機能を使用すれば (XPSExplorer -xf) 、カスタム エクスポート ファイルを作成および編集することもできます。 XCart ファイル内では、個々のオブジェクト単位でインポート モード (ADD、OVERLAY、REPLACE、または DEFAULT) を設定できます。 次に -xf パラメータを使用して、XCart ファイルを XPSExport に渡すことができます。

以下の点を考慮してください。

- XPSExport では、キー ストアからのキーのエクスポートは行いません。 この目的には **smkeyexport** コマンドを使用します。
- ある環境から別の環境にポリシーを移動させる場合、環境に固有の一部のオブジェクトがエクスポート ファイルに含まれます。これらのオブジェクトにはたとえば以下のものがあります。
 - 任意のトラステッド ホスト
 - 任意の HCO ポリシー サーバ設定
 - 任意の認証方式 URL
 - 任意のパスワード サービス リダイレクト
 - 任意のリダイレクト レスポンス

XPSEExport 使用時に選択したモードによって、これらのオブジェクトは新しい環境に追加されるか、または既存の設定を上書きする場合があります。オブジェクトをインポートする際は、環境設定を誤って変更することがないように注意が必要です。

構文

XPSEExport の構文は以下のとおりです。

```
XPSEExport output_file [-xo object_XID] [-xo-add object_XID] [-xo-replace object_XID]
[-xo-overlay object_XID] [-xf file_name] [-xb] [-xe] [-xp] [-xs] [-xc] [-xi] [-xm]
[-f] [-fm] [-q] [-m <number>[%]] [-pass <passphrase>][-npass] [-comment comment]
[-cf commentpath] [-?] [-vT] [-vI] [-vW] [-vE] [-vF] [-l log_file] [-e err_file]
```

パラメータ

output_file

XML 出力ファイル。

-xo object_XID

オブジェクト単位のエクスポートで 1 つ以上のオブジェクトを指定します。以下のエクスポート タイプのいずれかを指定することもできます。

-xo-add object_XID

インポート時に追加のみ行うことを指定します。

-xo-replace object_XID

インポート時にポリシー データを上書きします。

-xo-overlay object_XID

インポート時にポリシー データを更新します。

-xf file_name

(オプション) エクスポートするオブジェクトの XID のリストを含むファイルの絶対名を指定します。

ファイル内のエントリは以下の形式になります。

CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e

ADD = CA.SM::AuthScheme@0d-4afc0e41-ae25-11d1-9cdd-006008aac24b

REPLACE = CA.SM::Agent@01-cb8b3401-a6aa-4794-964e-c569712269c0

OVERLAY = CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634

これらのエントリーは、以下のコマンドラインパラメータに対応します。

```
-xo CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e  
-xo-add CA.SM::AuthScheme@0d-4afc0e41-ae25-11d1-9cdd-006008aac24b  
-xo-replace CA.SM::Agent@01-cb8b3401-a6aa-4794-964e-c569712269c0  
-xo-overlay CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634
```

-xb

(オプション) ポリシーストアの場所を含めて、ポリシーストアのオブジェクトをすべてエクスポートします。ポリシーストアの場所は、ポリシーサーバ管理コンソールの [データ] タブで設定されます。

重要: このデータをインポートするポリシーサーバは、エクスポート時に指定されたポリシーストアを使用します。たとえば、ポリシーストアとして **ODBC** データベースを使用するポリシーサーバ **A** からデータをエクスポートするとします。その後、ポリシーストアとして **Active Directory** を使用するポリシーサーバ **B** へデータをインポートします。ポリシーサーバ **B** 用の **Active Directory** ポリシーストアの場所は、ポリシーサーバ **A** 用の **ODBC** データベース場所と置換されます。

-xe

(オプション) 実行環境に関連付けられるオブジェクトタイプをエクスポートします。

-xp

(オプション) ポリシーに関連付けられるオブジェクトタイプをエクスポートします。

-xe および **-xp** オプションを、**-xo**、**-xo-add**、**-xo-replace**、**-xo-overlay**、または **-xf** と一緒に使用することはできません。

重要: **-xe** および **-xp** オプションは、フェデレーションに関連するオブジェクト以外のポリシーデータをすべて抽出する **-xa** オプションに代わるものです。また、ポリシーストアの場所など、ポリシーサーバの場所に固有のデータを含んだ、ポリシーストアの完全なバックアップを取ることができる **-xb** オプションを使用することもできます。

-xs

(オプション) 全セキュリティデータをエクスポートします。

-xc

(オプション) 全設定データをエクスポートします。

-xi

(オプション) 最初にインストールされたオブジェクトタイプをエクスポートします。

例：AgentType

-xm

(オプション) ExtractManifest オブジェクトで指定されたオブジェクトをエクスポートします。

-f

(オプション) 出力ファイルに上書きします。

-fm

(オプション) メモリの消費量は減りますが、パフォーマンスに影響します。

-q

(オプション) プログレス メッセージを抑制します。

-m <number>[%]

(オプション) プログレス メッセージが <number> 個のオブジェクトごとに出力されるように指定します。

オプションでパーセント記号（「%」）が含まれている場合、<number> は、オブジェクトの数ではなくオブジェクトの合計の割合です。

デフォルト：10%。

-pass <passphrase>

(オプション) 機密データの暗号化に必要なパスフレーズを指定します。パスフレーズは、長さが 8 文字以上で、1 つ以上の数字、1 つ以上の大文字、および 1 つ以上の小文字を含んでいる必要があります。引用符で囲まれた空白を含めることもできます。パスフレーズをコマンドライン オプションとして指定しなかった場合、機密データをエクスポートするとき入力を求められます。

-npass

(オプション) パスフレーズを使用しないことを指定します。

重要: 機密データはクリア テキストとしてエクスポートされます。

-comment

(オプション) 出力ファイルにコメントを追加します。

-cf commentpath

(オプション) <commentpath> からのコメントを取得し、出力ファイルに追加します。

-?

コマンドラインのヘルプを表示します。

-nb

(オプション) エラー時にビープ音を鳴らさないようにします。

-vT

(任意) 詳細レベルを **TRACE** に設定します。

-vI

(任意) 詳細レベルを **INFO** に設定します。

-vW

(オプション) 詳細レベルを **WARNING** に設定します (デフォルト)。

-vE

(任意) 詳細レベルを **ERROR** に設定します。

-vF

(任意) 詳細レベルを **FATAL** に設定します。

-l log_file

(オプション) 指定されたファイルにログを出力します。

-e err_file

(オプション) エラーと例外をログ記録するファイルを指定します。省略した場合、**stderr** が使用されます。

例

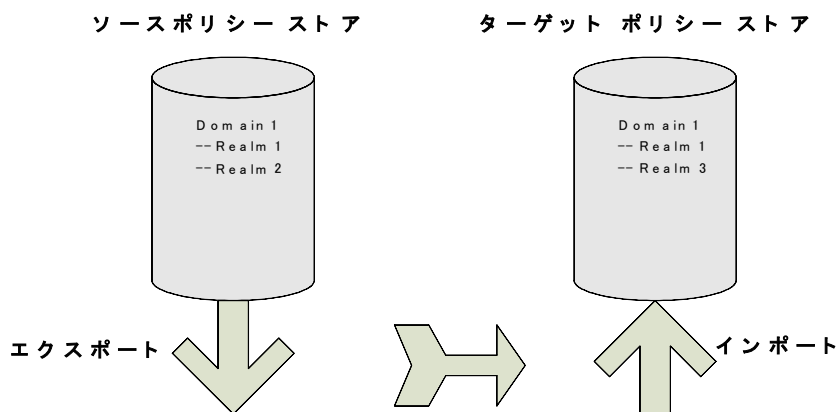
```
XPSEExport PolicyData.xml -xo
CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e
-xo-overlay CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634
```

注: 詳細なエクスポートの場合、エクスポートタイプは、コマンドラインで明示的に指定するか、またはデータディクショナリから取得されます。ダンプエクスポートでは、すべてのオブジェクトのエクスポートタイプ属性は **Replace** です。ポリシーデータのロードインポートは、ポリシーストア内のすべてのポリシーデータを上書きします。

XPSEExport ツールでコマンドラインオプションにエラーが発生した場合、ツールは実行が中止され、例外ファイル（または **stderr**）にエラーが記録されます。任意のオブジェクトのエクスポートが失敗した場合も、エクスポートプロセスは中止されます。該当するエラーが例外ファイル（または **stderr**）に記録され、XML 出力ファイル（作成されている場合）が削除されます。

ポリシーデータの追加

以下の図は、ソースポリシーストア内にある **Domain1** という名前の SiteMinder ポリシードメインを示しています。**Domain1** は、エクスポートして、ターゲットポリシーストアにインポートする必要があります。



ターゲットポリシーストアには同じ名前を持つドメインがすでにありますが、この2つのドメインには以下のような違いがあります。

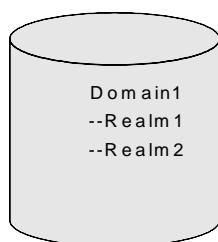
- ソースポリシーストアでは **Realm1** のプロパティが更新されているため、ターゲットポリシーストアの **Realm1** のプロパティとは異なる値を持ちます。
- **Domain1** には、ターゲットポリシーストアには存在しない **Realm2** があります。

ターゲットポリシーストアに1つのオブジェクト (**Realm2**) のみインポートする詳細インポートを指定するための、エクスポート時のコマンドラインは以下ようになります。

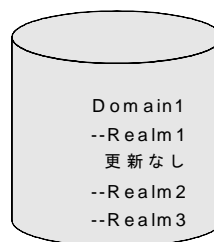
```
XPSExport gran-add.xml -xo-add
CA.SM: :Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

インポートに成功すると、ターゲットポリシーストアの **Domain1** には3つのレルムが含まれます。以下の図に示すとおり、**Realm1** のプロパティは更新されません。

ソースポリシーストア



ターゲットポリシーストア



add メソッドを使用して明示的に指定されたオブジェクト (ドメイン) のターゲットポリシーストアへのエクスポート詳細を指定するには、以下のコマンドを使用します。

```
XPSExport -ma -xo <object_XID>
```

-ma

コマンドラインでこのパラメータの後に表示されるすべてのオブジェクトを追加します。

`add` メソッドを使用して明示的に指定されたオブジェクト（ドメイン）のすべての関連オブジェクトのターゲットポリシーストアへのエクスポート詳細を指定するには、以下のコマンドを使用します。

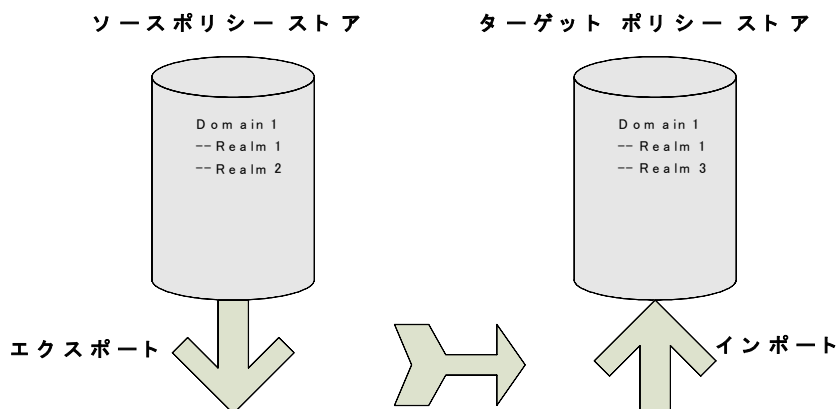
```
XPSEExport -ra -xo <object_XID>
```

`-ra`

コマンドラインでこのパラメータの後に表示されるオブジェクトの関連するシステムオブジェクトを追加します。

ポリシーデータの上書き

以下の図は、ソースポリシーストア内にある **Domain1** という名前の SiteMinder ポリシードメインを示しています。Domain1 は、エクスポートして、ターゲットポリシーストアにインポートする必要があります。



ターゲットポリシーストアには同じ名前を持つドメインがすでにありますが、この2つのドメインには以下のような違いがあります。

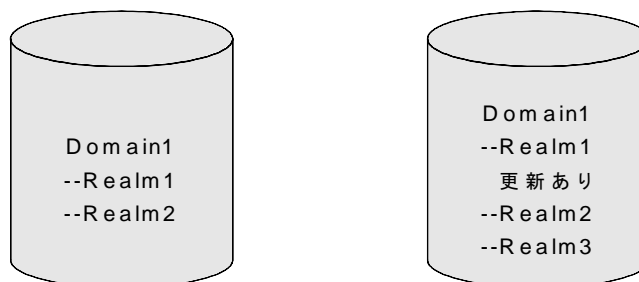
- ソースポリシーストアでは **Realm1** のプロパティが更新されているため、ターゲットポリシーストアの **Realm1** のプロパティとは異なる値を持ちます。
- **Domain1** には、ターゲットポリシーストアには存在しない **Realm2** があります。

ソースポリシーストアの最新の変更内容を使用してターゲットポリシーストアを更新する詳細インポートを指定するための、エクスポート時のコマンドラインは以下ようになります。

```
XPSEExport gran-add.xml -xo-overlay
CA.SM: :Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

以下の図に示すとおり、インポートに成功すると、ターゲットポリシーストアの Realm1 のプロパティが更新されます。

ソースポリシーストア ターゲットポリシーストア



overlay メソッドを使用して明示的に指定されたオブジェクト（ドメイン）のターゲットポリシーストアへのエクスポート詳細を指定するには、以下のコマンドを使用します。

```
XPSExport -mo -xo <object_XID>
```

-mo

コマンドラインでこのパラメータの後に表示されるすべてのオブジェクトをコマンドラインに上書きします。

overlay メソッドを使用して明示的に指定されたオブジェクト（ドメイン）のすべての関連オブジェクトのターゲットポリシーストアへのエクスポート詳細を指定するには、以下のコマンドを使用します。

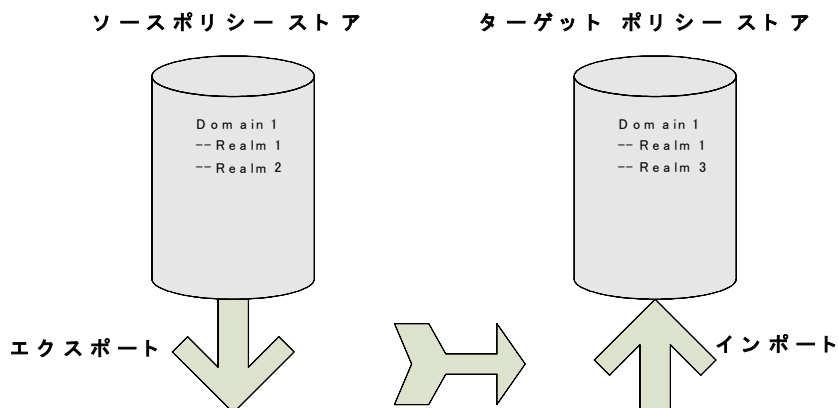
```
XPSExport -ro -xo <object_XID>
```

-ro

コマンドラインでこのパラメータの後に表示されるオブジェクトの関連するシステムオブジェクトを上書きします。

ポリシー データの置換

以下の図は、ソース ポリシー ストア内にある **Domain1** という名前の SiteMinder ポリシー ドメインを示しています。Domain1 は、エクスポートして、ターゲット ポリシー ストアにインポートする必要があります。



ターゲット ポリシー ストアには同じ名前を持つドメインがすでにありますが、この 2 つのドメインには以下のような違いがあります。

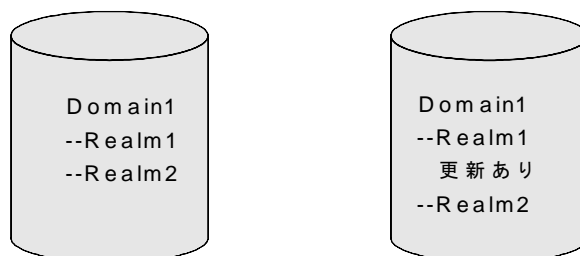
- ソース ポリシー ストアでは **Realm1** のプロパティが更新されているため、ターゲット ポリシー ストアの **Realm1** のプロパティとは異なる値を持ちます。
- **Domain1** には、ターゲット ポリシー ストアには存在しない **Realm2** があります。

ソース ポリシー ストアの内容をターゲット ポリシー ストアに複製するための、エクスポート時のコマンドラインは以下のようになります。

```
XPSExport gran-add.xml -xo-replace
CA.SM: :Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

以下の図に示すとおり、インポートに成功すると、ターゲットポリシーストアの **Domain1** はソースポリシーストアの **Domain1** とまったく同じになります。

ソースポリシーストア ターゲットポリシーストア



replace メソッドを使用して明示的に指定されたオブジェクト（ドメイン）のターゲットポリシーストアへのエクスポート詳細を指定するには、以下のコマンドを使用します。

```
XPSExport -mr -xo <object_XID>
```

-mr

コマンドラインでこのパラメータの後に表示されるオブジェクトをすべて置換します。

replace メソッドを使用して明示的に指定されたオブジェクト（ドメイン）のすべての関連オブジェクトのターゲットポリシーストアへのエクスポート詳細を指定するには、以下のコマンドを使用します。

```
XPSExport -rr -xo <object_XID>
```

-rr

コマンドラインでこのパラメータの後に表示されるオブジェクトの関連するシステムオブジェクトを置換します。

ポリシー データのマージ

あるポリシー ストアから別のストアにドメイン オブジェクトを移行するとき、明示的に指定されたオブジェクト (ドメイン) のみが移行されます。ドメイン (たとえばユーザ ディレクトリ、エージェント、エージェント タイプ) の関連するオブジェクトはすべてターゲット ポリシー ストアに移行されません。関連するシステム オブジェクトがない場合、ドメインをポリシー ストアにインポートできません。

`merge` メソッドを使用して明示的に指定されたオブジェクト (ドメイン) のターゲット ポリシー ストアへのエクスポート詳細を指定するには、以下のコマンドを使用します。

```
XPSEExport -mm -xo <object_XID>>
```

`-mm`

コマンドラインでこのパラメータの後に表示されるオブジェクトをすべてマージします。

`merge` メソッドを使用して明示的に指定されたオブジェクト (ドメイン) のすべての関連オブジェクトのターゲット ポリシー ストアへのエクスポート詳細を指定するには、以下のコマンドを使用します。

```
XPSEExport -rm -xo <object_XID>
```

`-rm`

コマンドラインでこのパラメータの後に表示されるオブジェクトの関連するシステム オブジェクトをマージします。

注: Merge オプションは、Add、Replace、または Overlay オプションの代替策です。Merge オプションは Add オプションに似ていますが、唯一の相違はこのオプションは既存のオブジェクトの不明なオブジェクトを追加するだけでなく、不明な属性も追加することです。

XPSImport

XPSImport ツールは、ポリシー ストア データを移行するための以下のタスクをサポートしています。

- 全ポリシー データのインポート
- 一部のポリシー データのインポート
- 設定データのインポート

注: XPSImport ではキー ストア へのキーのインポートは行いません。キーをインポートするには、`smkeyimport` を使用する必要があります。

構文

XPSImport の構文は以下のとおりです。

```
XPSImport input_file [-pass <passphrase>] [-npass] [-validate] [-fo] [-vT] [-vI] [-vW] [-vE] [-vF] [-e file_name] [-l log_path] [-?]
```

パラメータ

`input_file`

入力 XML ファイルを指定します。

`-q`

(オプション) プログレス メッセージを抑制します。

`-m <number>[%]`

(オプション) プログレス メッセージが `<number>` 個のオブジェクトごとに出力されるように指定します。

オプションでパーセント記号 (「%」) が含まれている場合、`<number>` は、オブジェクトの数ではなくオブジェクトの合計の割合です。

デフォルト: 10%。

`-pass <passphrase>`

(オプション) 機密データの復号化に必要なパスフレーズを指定します。パスフレーズはエクスポート時に指定されたものと同じである必要があります。異なっている場合、復号化は失敗します。

`-npass`

(オプション) パスフレーズが使用できないことを指定します。

重要: 機密データはクリア テキストとしてインポートされます。

-validateOnly

(オプション) データベースを更新せずに、XML 入力ファイルを検証します。

-schemaFile

入力ファイルを検証するためにスキーマ ファイルを指定します。このオプションを指定しないと、入力ファイルは検証されません。

-fo

ダンプ ロードで既存のポリシー ストアの上書きを強制できます。

-?

コマンドラインのヘルプを表示します。

-nb

(オプション) エラー時にビープ音を鳴らさないようにします。

-vT

(任意) 詳細レベルを **TRACE** に設定します。

-vI

(任意) 詳細レベルを **INFO** に設定します。

-vW

(オプション) 詳細レベルを **WARNING** に設定します (デフォルト)。

-vE

(任意) 詳細レベルを **ERROR** に設定します。

-vF

(任意) 詳細レベルを **FATAL** に設定します。

-l log_file

(オプション) 指定されたファイルにログを出力します。

-e err_file

(オプション) エラーと例外をログ記録するファイルを指定します。省略した場合、**stderr** が使用されます。

例

```
XPSImport PolicyData.xml -e C:¥¥tmp¥¥ExceptionLog.txt
```

この例では、**PolicyData.xml** ファイル内で指定されているポリシー データ オブジェクトをインポートします。インポートがダンプロードであるか、オブジェクト単位であるかどうかは、コマンドラインからはすぐにはわかりません。ただし、その情報は、XML 入力ファイル内の **<PolicyData>** 要素の **IsDumpExport** 属性を見ることによって確認できます。この属性が **true** に設定されている場合は、XML 入力ファイルをダンプロードに使用する必要があることを意味します。

ポリシー データ転送のトラブルシューティング

ポリシー ストア データの転送時には、以下の要素が関連してくる可能性があります。

- エラーは、コンソール (stdout/stderr) に出力されるか、ファイルに転送されます。
- ロギングのレベルは以下のようにリスト表示されます。
 - トレース
 - 情報
 - 警告
 - エラー
 - 致命的
- すでにファイルが存在する場合、エクスポートは失敗します。
- XML ファイル内のオブジェクトについて検証が失敗した場合、インポートはロールバックされます。
- 追加タイプによってエクスポートしたオブジェクトがターゲット ポリシー ストア内にすでに存在する場合、詳細インポートは失敗します。

smkeyexport

smkeyexport ツールは、キーストアからキーをエクスポートします。smkeyexport の構文は以下のとおりです。

```
smkeyexport -dadminname -wadminpw [-ooutput_filename] [-f] [-c] [-cb] [-cf] [-l] [-v] [-t] [-?]
```

-d

SiteMinder 管理者の名前を指定します。

-w

SiteMinder 管理者のパスワードを指定します。

-o

(オプション)。出力ファイルを指定します。デフォルトは `stdout.smdif` です。

-f

(オプション) 既存の出力ファイルを上書きします。

-c

(オプション)。暗号化されていない機密データをエクスポートします。

-cb

(オプション)。下位互換の暗号で暗号化された機密データをエクスポートします。

-cf

(オプション)。FIPS 互換の暗号で暗号化された機密データをエクスポートします。

-l

(オプション)。指定されたファイル (`filename.log`) を作成し、エントリのログを記録します。

-v

(オプション)。詳細メッセージングを指定します。

-t

(オプション)。トレースを有効にします。

-?

(オプション)。コマンド オプションを表示します。

SiteMinder キー ツール

SiteMinder キー ツールユーティリティ (`smkeytool`) を使用すると以下の処理が可能です。

- 12.52 SP1 証明書データ ストアを管理できます。
- 12.52 SP1 へのアップグレード時にレガシー `smkeydatabase` にアクセスできます。証明書データ ストアへの移行が失敗した場合、その原因となっているデータ不整合をすべて解決するために、アクセス レガシー キー ストア フラグ (`-accessLegacyKS`) を使用します。
- インストールされている場所は以下のとおりです。

`siteminder_home¥bin`

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

以下の手順に従います。

1. コマンド ラインまたはシェルを開きます。
2. 以下のいずれかのコマンドを実行します。
 - (Windows) `smkeytool.bat -option [-arguments]`
 - (UNIX) `smkeytool.sh -option [-arguments]`

`smkeytool` を使用して、次の操作を実行できます。

- クライアント証明書キーの追加
`smkeydatabase` に含まれていないコンシューマ機関でルートまたはチェーンの認証機関 (CA) を使用している場合、`smkeydatabase` にこれを追加する必要があります。

たとえば、署名された VeriSign の CA サーバ側証明書は、Web エージェント オプションパックでインストールされているプロデューサ側 Web サーバを SSL 対応にするために使用します。SSL を介した基本認証にこの証明書を使用するには、コンシューマ側で `smkeydatabase` への VeriSign 証明書を追加します。証明書の追加は、コンシューマがサーバ側証明書を持つプロデューサと通信していることを確認するのに役立ちます。また、信頼された CA によって証明書が検証されたことを確認するのに役立ちます。

秘密キーと証明書のペアの追加

`addPrivKey` オプションを使用して、秘密キー/証明書ペアのみを証明書データストアにインポートします。以下の点を考慮します。

- データストア内には、複数の秘密キー/証明書ペアを格納できますが、SiteMinder がサポートするのはストア内の RSA キーのみです。
- 秘密キー/証明書のペアのみが、暗号化されたフォームで格納されます。
- 証明書を作成する側のポリシーサーバで、以下を行います。
 - 単一の秘密キー/証明書のペアを使用して SAML アサーションに署名します。
 - 証明書を使用して、証明書を使用する側から受け取る暗号化 SAML アサーションを復号します。

通常、キーは証明書データストアで見つかる最初の秘密キー/証明書ペアです。

- 証明書メタデータは、インポートする前に証明書ファイルから削除します。「--BEGIN CERTIFICATE --」というマーカで始まり、「--END CERTIFICATE --」というマーカで終わるデータのみをインポートします。以下のマーカを必ず含めるようにしてください。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー **smkeydatabase** に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データストアに適用されます。

-alias *alias*

必須です。データベース内の秘密キー/証明書のペアにエイリアスを割り当てます。エイリアスは、英数文字のみを含む一意の文字列である必要があります。

-certfile *cert_file*

秘密キー/証明書ペアに関連付けられている証明書の場所のフルパスを指定します。PKCS1、PKCS5、および PKCS8 の各形式のキーに必須です。

-keyfile *private_key_file*

秘密キー ファイルの場所へのフルパスを指定します。PKCS1、PKCS5、および PKCS8 の各形式のキーに必須です。

-keycertfile *key_cert_file*

秘密キーおよび証明書ペアのデータを含む PKCS12 ファイルの場所へのフルパスを指定します。PKCS12 形式のキーに必須です。

-password *password*

(オプション) 秘密キー/証明書ペアが作成された場合、そのペアの暗号化に使用されたパスワードを指定します。キー/証明書ペアが証明書データストアに書き込まれる前に、そのペアを復号するためにこのパスワードを提供します。

注: このパスワードは証明書データストアには格納されません。

キー/証明書ペアが復号され、証明書データストアに格納された後、SiteMinder はそのペアをそれ自体のパスワードを使用して再び暗号化します。

証明書の追加

`addCert` オプションを使用して、公開証明書または信頼された CA 証明書を証明書データストアに追加します。

以下の点を考慮します。

- 証明書は、秘密キー/証明書ペアと関連付けられる証明書です。ただし、証明書のみが証明書データストアに追加されます。
- 証明書を認証機関 (CA) として信頼する場合、この証明書は常に CA 証明書として処理されます。
- X.509 証明書形式については、V1、V2 および V3 バージョンが SiteMinder ではサポートされています。エンコード形式については、DER および PEM の各形式が SiteMinder ではサポートされています。
- CA 証明書を追加するときは、Web エージェントを再起動してください。
- 証明書メタデータは、インポートする前に証明書ファイルから削除します。「--BEGIN CERTIFICATE --」というマーカで始まり、「--END CERTIFICATE --」というマーカで終わるデータのみをインポートします。以下のマーカを必ず含めるようにしてください。

このオプションに対する引数には、以下が含まれます。

`-accessLegacyKS`

オプションがレガシー `smkeydatabase` に適用されることを指定します。この引数を指定しない場合、オプションは 12.52 SP1 証明書データストアに適用されます。

`-alias alias`

必須です。証明書データストアの秘密キーと関連付けられた証明書のエイリアスを指定します。

制限： 英数文字のみを含む一意の文字列。

`-infile cert_file`

必須です。新しく追加された証明書の場所へのフルパスを指定します。

`-trustcacert`

任意です。追加されるユーザプロバイダ証明書が CA 証明書であることを確認します。ユーティリティにより、証明書にデジタル署名拡張子があり、証明書に同じ `IssuerDN` 値および `SubjectDN` 値があることが確認されます。

-noprompt

(オプション) 証明書の追加の確認を求めるメッセージは表示されません。

破棄情報の追加

addRevocationInfo オプションを使用して、CRL の場所を指定します。証明書データストアは、CRL の場所を参照します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー **smkeydatabase** に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データストアに適用されます。

-issueralias issuer_alias

必須です。CRL を発行する認証機関のエイリアスを指定します。

例： **-issueralias verisignCA**

-type (ldapcrl | filecrl)

必須です。CRL が LDAP ベースかファイルベースかを指定します。

-location location

必須です。CRL の場所を指定します。

- (ファイルベース) ファイルのフルパスを指定します。

例： **-location c:\crls\%siteminder_root_ca.crl**

- (LDAP ディレクトリ サービス) LDAP サーバノードのフルパスを指定します。

例： **-location "http://localhost:880/sn=siteminderroot, dc=crls,dc=com"**

破棄情報の削除

deleteRevocationInfo オプションを使用して、証明書データ ストアから CRL を削除します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー **smkeydatabase** に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データ ストアに適用されます。

-issueralias *issuer_alias*

CRL を発行する認証機関の名前を指定します。

-noprompt

(オプション) CRL の削除の確認を求めるメッセージは表示されません。

証明書データの削除

removeAllCertificateData オプションを使用して、証明書データ ストアから証明書データをすべて削除します。

このオプションに対する引数を以下に示します。

-noprompt

(オプション) 証明書データの削除の確認を求めるメッセージは表示されません。

証明書の削除

削除オプションを使用して、証明書データストアから証明書を削除します。証明書に秘密キーが関連付けられている場合は、そのキーも削除されます。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー **smkeydatabase** に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データストアに適用されます。

-alias <alias>

(必須) 削除する証明書のエイリアスを指定します。

-noprompt

(オプション) 証明書の削除の確認を求めるメッセージは表示されません。

証明書または秘密キーのエクスポート

エクスポートオプションを使用して、証明書または秘密キーをファイルにエクスポートします。

以下の点を考慮します。

- 証明書データは、**PEM** エンコーディングを使用してエクスポートされます。
- 秘密キーデータは、**DER** エンコードによる **PKCS8** 形式でエクスポートされます。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー **smkeydatabase** に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データストアに適用されます。

-alias *alias*

(必須) エクスポートする証明書またはキーを特定します。

-outfile *out_file*

(必須) データがエクスポートされるファイルへのフルパスを指定します。

-type (key|cert)

(オプション) 証明書またはキーのどちらをエクスポートするかを指定します。

デフォルト: 証明書。

-password *password*

秘密キーをエクスポートする場合のみ必須です。エクスポート時に秘密キーの暗号化に使用するパスワードを指定します。公開キーを保持する証明書をエクスポートする場合、パスワードは不要です。これは、証明書はクリアテキストでエクスポートされるためです。

証明書データストアにこの秘密キーを追加するには、このパスワードで **addPrivKey** オプションを使用します。

エイリアスの検索

findAlias オプションを使用して、証明書データストアの証明書と関連付けられるエイリアスを検索します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー **smkeydatabase** に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データストアに適用されます。

-infile *cert_file*

(必須) 検索対象のエイリアスに関連付けられている証明書ファイルへのフルパスを指定します。

-password *password*

パスワードで保護されている **P12** ファイルが証明書ファイルとして指定されている場合にのみ必須。

デフォルトの CA 証明書のインポート

`importDefaultCACerts` オプションを使用して、SiteMinder に含まれるデフォルトの信頼された認証機関の証明書をすべて、証明書データ ストアにインポートします。

このオプションに対する引数を以下に示します。

`-accessLegacyKS`

オプションがレガシー `smkeydatabase` に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データ ストアに適用されます。

すべての証明書のメタデータ リスト

`listCerts` オプションを使用して、証明書データ ストアに格納されたすべての証明書のメタデータの一部を表示します。

このオプションに対する引数には、以下が含まれます。

`-accessLegacyKS`

オプションがレガシー `smkeydatabase` に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データ ストアに適用されます。

`-alias alias`

(オプション) 指定した別名に関連付けられている証明書およびキーのメタデータ情報をリストで表示します。

このオプションは、ワイルドカード文字としてアスタリスク (*) をサポートしています。ワイルドカードの使い方は以下のとおりです。

- エイリアス値の先頭または終わりに挿入する。
- エイリアス値の先頭と終わりに挿入する。

コマンドシェルがワイルドカード文字を解釈しないように、アスタリスクは引用符で囲んでください。

破棄情報リスト

`listRevocationInfo` オプションを使用して、証明書データストア内の証明書廃棄リストの一覧を表示します。以下の項目が表示されます。

- CRL 名。
- CRL はファイルベースか LDAP ベースかを指定します。
- CRL の場所。

このオプションに対する引数には、以下が含まれます。

`-accessLegacyKS`

オプションがレガシー `smkeydatabase` に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データストアに適用されます。

`-issueralias issuer_alias`

(オプション) CRL を発行する認証機関の名前。

このオプションは、ワイルドカード文字としてアスタリスク (*) をサポートしています。ワイルドカードの使い方は以下のとおりです。

- エイリアス値の先頭または終わりに挿入する。
- エイリアス値の先頭と終わりに挿入する。

コマンドシェルがワイルドカード文字を解釈しないように、アスタリスクは引用符で囲んでください。

証明書メタデータの表示

`printCert` オプションを使用して、指定された証明書のメタデータの一部を表示します。このコマンドは、証明書プロパティの表示が難しいシステムで有効です。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー `smkeydatabase` に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データストアに適用されます。

-infile *cert_file*

必須です。証明書ファイルの場所。

-password *password*

パスワードで保護されている **P12** ファイルが証明書ファイルとして指定されている場合にのみパスワードが必須です。

エイリアス名の変更

`renameAlias` オプションを使用して、証明書と関連付けられるエイリアスの名前を変更します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー `smkeydatabase` に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データストアに適用されます。

-alias *current_alias*

(必須) 証明書と関連付けられるエイリアスを指定します。

-newalias *new_alias*

(必須) 新規エイリアスを指定します。

制限： 英数文字のみを含む一意の文字列である必要があります。

証明書の検証

`validateCert` オプションを使用して、証明書を廃棄するかどうかを決定します。

このオプションに対する引数には、以下が含まれます。

`-accessLegacyKS`

オプションがレガシー `smkeydatabase` に適用されることを指定します。この引数を指定しない場合、オプションは **12.52 SP1** 証明書データストアに適用されます。

`-alias alias`

(必須) 証明書データストアの秘密キーと関連付けられた証明書のエイリアスを指定します。

制限：英数文字のみを含む一意の文字列である必要があります。

`-infile crl_file`

(オプション) ユーティリティで、検証する証明書を検索する CRL を指定します。

OCSP 設定ファイルのロード

`loadOCSPConfigFile` オプションを使用して、ポリシー サーバを再起動せずに、証明書データストアに OCSP 設定ファイルを再ロードします。ファイルがロードすると、既存の OCSP 設定がデータストアから削除され、設定はファイルの内容に置き換えられます。OCSPUpdater は、次回起動時に設定の変更をピックアップします。

OCSP 設定ファイルの名前は `SMocsp.conf` です。

Windows のコマンド構文は以下のとおりです。

```
smkeytool.bat -loadOCSPConfigFile
```

UNIX のコマンド構文は以下のとおりです。

```
smkeytool.sh -loadOCSPConfigFile
```

smlldapsetup

smlldapsetup ユーティリティを使用すると、コマンドラインから LDAP ポリシーストアを管理できます。**smlldapsetup** では、LDAP ポリシーストアの設定、LDIF ファイルの生成、およびポリシーストアデータとスキーマの削除が可能です。

smlldapsetup を使用するには、モードを指定します。モードによって、**smlldapsetup** が実行するアクションと、LDAP サーバの設定に使用する値を含む引数が決まります。

以下の表は、**smlldapsetup** で使用できるモードと、各モードで使用される引数を示しています。

モード	引数
reg	-hhost、-pportnumber、-duserdn、 -wuserpw、-rroot、 -ssl1/0、-ccertdb、-k1
ldgen	-hhost、-pportnumber、-duserdn、 -wuserpw、-rroot、 -mn、-ssl1/0、-ccertdb -fldif、-ttool、-ssuffix、-e、-k
ldmod	-hhost、-pportnumber、-duserdn、 -wuserpw、-rroot、 -ssl1/0、-ccertdb、-fldif、 -ssuffix、-e、-k、-i
remove	-hhost、-pportnumber、-duserdn、 -wuserpw、-rroot、-ssl1/0、 -ccertdb、-k
switch	なし
revert	-v
status	-v

smldapsetup を使用する方法

1. 次のいずれかのディレクトリに移動します。

- (Windows) `siteminder_home¥bin`
- (UNIX) `siteminder_home/bin`

`siteminder_home`

SiteMinder のインストール場所を示します。

2. 以下のコマンドを入力します。

`smldapsetup mode arguments`

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドラインウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドラインウィンドウを開きます。

例: `smldapsetup reg -hldapserver.mycompany.com -d"LDAP User" -wMyPassword123 -ro=security.com`

注: `smldapsetup` を実行する場合は、指定する LDAP ユーザが LDAP ディレクトリ サーバ内のスキーマを変更するために適切な管理者権限を持っていることを確認してください。このユーザに適切な権限がない、LDAP サーバでは、ポリシーストアスキーマを生成できず、ポリシーストアデータを更新したり、削除したりできません。`smldapsetup` コマンドを実行した後、このユーザはポリシーサーバ管理コンソールの [データ] タブにある [管理ユーザ名] フィールドに表示されます。

詳細情報:

[smldapsetup のモード](#) (P. 280)

smlldapsetup のモード

モードは `smlldapsetup` が実行するアクションを指定します。LDAP サーバへの接続、LDIF ファイルの生成、LDAP ポリシーストアの設定、およびポリシーデータの削除を行うためのモードを指定できます。

`smlldapsetup` のモードには、以下のものが含まれます。

reg

LDAP サーバへの接続をテストします。接続が成功する場合、`-hhost`、`-pportnumber`、`-duserdn`、`-wuserpw`、`-rroot`、`-ssl1/0`、および `-ccertdb` の各引数を使用して `smlldapsetup` を実行すると、SiteMinder LDAP サーバがそのポリシーストアに設定されます。

ldgen

サポートされている LDAP サーバを自動的に検出し、SiteMinder スキーマを使用して LDIF ファイルを生成します。生成されたファイルを `smlldapsetup ldmod` と共に使用すると、SiteMinder スキーマが作成されます。`-e` 引数を指定して `smlldapsetup ldgen` を実行すると、LDIF ファイルが作成され、この LDIF ファイルを `ldmod` と共に使用すると、SiteMinder スキーマを削除できます。LDAP サーバの自動検出をスキップするには、`-m` スイッチを使用します。以前に `reg` モードで設定されていない場合、`ldgen` モードを使用するには `-f` スイッチが必要です。

ldmod

ポリシーストアにデータを入力せずに、LDAP サーバおよび SiteMinder スキーマに接続します。`ldapmodify` プログラム、および `-fldif` 引数と共に指定する LDIF ファイルが必要になります。`-hhost`、`-pport_number`、`-duserdn`、`-wuserpw`、`-rroot`、`-ssl1/0`、および `-ccertdb` の各引数を指定して `smlldapsetup ldmod` を実行すると、これらの引数によって指定される LDAP ディレクトリが変更されます。`-hhost`、`-pportnumber`、`-duserdn`、`-wuserpw`、`-rroot`、`-ssl1/0`、および `-ccertdb` を指定しないで `smlldapsetup ldmod` を実行すると、`smlldapsetup reg` またはポリシーサーバ管理コンソールで以前に定義した LDAP ディレクトリが使用されます。

remove

LDAP サーバに接続し、現在のバージョンの `smlldapsetup` に対応する SiteMinder LDAP ノード以下に格納されているポリシー データをすべて削除します。 `-hhost`、`-pport_number`、`-duserdn`、`-wuserpw`、`-rroot`、`-ssl1/0`、および `-ccertdb` の各引数を指定して `smlldapsetup remove` を実行すると、これらの引数によって指定される LDAP ディレクトリからデータが削除されます。 `-hhost`、`-pport`、`-duserdn`、`-wuserpw`、`-rroot`、`-ssl1/0`、および `-ccertdb` を指定しないで `smlldapsetup` を実行すると、`smlldapsetup reg` またはポリシー サーバ管理コンソールで以前に定義した LDAP ディレクトリからポリシー データが削除されます。

switch

ODBC の代わりに LDAP を使用するようにポリシー サーバを再設定します。変更を行う前に LDAP ストアまたは LDAP 接続パラメータの準備はしません。

revert

ポリシー ストアを LDAP から ODBC に戻します。このモードで 사용되는唯一の引数は `-v` です。

status

LDAP ポリシー ストアの接続パラメータが正しく設定されていることを確認します。 `-v` 引数が必要です。 `smlldapsetup status` を `-hhost`、`-pport_number`、`-duserdn`、`-wuserpw`、`-rroot`、`-ssl1/0`、および `-ccertdb` の各引数を指定して実行すると、これらの引数によって指定される LDAP ディレクトリへの接続がテストされます。 `-hhost`、`-pport_number`、`-duserdn`、`-wuserpw`、`-rroot`、`-ssl1/0`、および `-ccertdb` を指定しないで `smlldapsetup status` を実行すると、`smlldapsetup reg` またはポリシー サーバ管理コンソールで以前に定義した LDAP ディレクトリへの接続が確認されます。

ポリシー サーバ管理コンソールの [データ] タブでは、`reg`、`switch`、および `revert` 機能を使用して行った設定を GUI インターフェースから表示または変更できます。 `ldgen`、`ldmod`、`remove`、および `status` 機能を実行するには、`smlldapsetup` を使用する必要があります。

smlldapsetup の引数

引数を使用することによって、LDAP ポリシー ストアを管理するための各種モードで使用される情報を指定できます。引数を指定しないで **smlldapsetup** を実行すると、ポリシー サーバ管理コンソールで設定した値が使用されます。

注: **smlldapsetup** の場合、引数とその値との間に空白は使用できません。たとえば、**-h** 引数は以下のように指定する必要があります。

smlldapsetup ldmod -hldapserver.mycompany.com

smlldapsetup のコールで指定できる引数を以下に示します。

-h*host*

LDAP サーバの完全修飾名、マシンが同じドメイン内にある場合は相対名 (**hldapserver**)、または IP アドレス (**-h123.12.12.12**) を指定します。ホストを指定しないで **smlldapsetup** を実行すると、以前に設定した値がデフォルトで使用されます。

例 : **-hldapserver.mycompany.com**

-p*port_number*

非標準の LDAP ポートを指定します。LDAP サーバで非標準のポートを使用している場合、または別のポートを使用する新しいサーバに移行する場合 (SSL を使用しているサーバから、SSL を使用していないサーバへの移行など) は、LDAP ポートを指定する必要があります。ポートを指定しない場合、以前の設定値が使用されます。以前のポート設定が指定されていない場合は、SSL を使用していないときのデフォルトポート **389** か、SSL を使用しているときのデフォルトポート **636** が使用されます。

-d*userdn*

新しい LDAP ディレクトリのスキーマとエントリを作成する権限のあるユーザの LDAP ユーザ名を指定します。必ずしも LDAP サーバ管理者のユーザ名であるとは限りません。ユーザ名を指定しないと、以前に設定した名前がデフォルトで使用されます。

-w*userpw*

-d 引数で指定されたユーザのパスワードを指定します。パスワードを指定しない場合、以前に設定した値が使用されます。

例 : **-wMyPassword123**

-rroot

SiteMinder がポリシー ストア スキーマを検索する LDAP ツリー内のノードの識別名を指定します。ルートを指定しない場合、以前に設定したルートが使用されます。

例：-ro=security.com

-e

smlldapsetup ldgen と共に指定すると、SiteMinder スキーマを削除できる LDIF ファイルが生成されます。スキーマを削除するには、生成されたファイルを smlldapsetup ldmod と共に使用する必要があります。

-mn

LDAP サーバの自動検出をスキップし、LDAP ポリシー ストアのタイプを指定します。*n* は以下のいずれかです。

2

iPlanet v4 LDAP サーバ

3

Active Directory (LDAP) サーバ

4

Oracle インターネットディレクトリ

5

iPlanet v5

6

Sun Directory Server

9

Active Directory アプリケーションモード (ADAM)

-fldif

smlldapsetup の実行場所となるディレクトリから LDIF ファイルへの絶対パスまたは相対パスを指定します。

例：-f../siteminder/db/smlldap.ldif

デフォルト：パスを指定しない場合、現在のディレクトリがデフォルトとして使用されます。

-ttool

ldapmodify コマンドラインユーティリティの絶対パスまたは相対パスを、ファイル名と拡張子を含めて指定します。**ldapmodify** は LDIF 形式のコマンドを使用しているサーバスキーマを設定するために使用します。LDAP サーバおよび SiteMinder には、**ldapmodify** のコピーが用意されています。ユーティリティがデフォルトの場所がない場合は、この引数を使用して場所を指定します。

-ssl1_or_0

LDAP サーバに対して SSL 暗号化された接続を使用するときは **-ssl1**、非 SSL 接続を使用するときは **-ssl0** を指定します。**-ssl** の値を指定しない場合、以前に設定した値が使用されます。LDAP 接続が以前に設定されていない場合、初期デフォルト値は **0** です。

-ccert

SSL 暗号化された (**-ssl1**) LDAP 接続を使用するときは、この引数を指定する必要があります。通常 **cert8.db** と呼ばれる SSL クライアント Netscape 証明書データベースファイルが存在するディレクトリのパスを指定します。

例：**cert8.db** が **/app/siteminder/ssl** 内にある場合は、**-c/app/siteminder/ssl** を指定します (**smlldapsetup ldmod -f/app/siteminder/pstore.ldif -p81 -ssl1 -c/app/siteminder/ssl**)。

注：Sun Java System LDAP に対して SSL 暗号化接続を使用しているポリシーストアの場合は、**cert8.db** と同じディレクトリ内に **key3.db** ファイルがあることを確認してください。

-k-k1

別の LDAP ディレクトリにキー情報を格納する場合に、**smlldapsetup** を使用してキーストアをセットアップまたは変更できます。**-k** を指定すると、ポリシーサーバがキーストアを参照しているかどうか、任意の機能を実行する前に確認されます。ポリシーサーバがキーストアを参照していない場合は、警告が出されます。**ldgen** および新しいポリシーストア用の他の引数と共に **-k1** を指定して **smlldapsetup** を実行すると、指定した場所に別のキーストアが作成されます。**-k** または **-k1** を指定しないと、ポリシーストアが変更されます。

-v

トラブルシューティングの詳細モードを有効にします。**-v** を指定して **smlldapsetup** を実行すると、LDAP 移行の各手順で、コマンドライン引数と設定エントリのログが記録されます。

-iuserDN

ポリシーストアに対する変更を行うために **SiteMinder** によって使用される必要のあるアカウントの識別名を指定します。この引数を使用すると、管理者アカウントで **SiteMinder** スキーマの制御を維持すると同時に、**SiteMinder** データの日常の変更のために使用される別のアカウントを有効にすることができます。管理 UI を使用して変更を行う場合は、この引数によって指定されるアカウントが使用されます。この引数を使用するときは、アカウントの全 **DN** を入力してください。

-q

何も質問が行われない **Quiet** モードを有効にします。

-u

6.x アップグレードスキーマファイル (LDIF) を作成します。

-x

ldmod に **-x** 引数を使用して、別の 5.x Sun Java System Directory Server Enterprise Edition (以前の Sun ONE/iPlanet) LDAP ディレクトリ サーバ用のレプリケーションインデックスを生成します。

-ssuffix

このオプションを使用すると、6.x ポリシー サーバのスキーマを Sun Java System Directory Server Enterprise Edition (以前の Sun ONE/iPlanet) LDAP ディレクトリに設定するときに、デフォルトの親サフィックス以外のサフィックスを指定することができます。

例： 以下のような状況を想定します。

`ou=Apps,o=test.com` はポリシー ストアのルートです。

`o=test.com` はルート サフィックスです。

`ou=netegrity,ou=Apps,o=test.com` はサブ サフィックスです。

`smldapsetup` で `-s` パラメータを使用しない場合、ポリシー サーバは `ou=netegrity,ou=Apps,o=test.com` の親サフィックスとして `ou=Apps,o=test.com` を割り当てます。これを変更し、適切な親サフィックスを設定するには、`-s` パラメータと `o=test.com` を指定して `smldapsetup` を実行します。

-?

ヘルプ メッセージを表示します。

注: 引数に空白が含まれる場合は、引数全体を二重引用符で囲む必要があります。たとえば、SiteMinder 管理者の名前が LDAP ユーザである場合、`smldapsetup` の引数は `-d"LDAP user"` となります。

smldapsetup と Sun Java System Directory Server Enterprise Edition

Sun Java System Directory Server Enterprise Edition (以前の Sun ONE/iPlanet) ディレクトリ サーバでは、`smldapsetup` によって `ou=Netegrity`, `root` サブ サフィックスおよび `PolicySvr4` データベースが作成されます。

root

ポリシー サーバ管理コンソールの [データ] タブ上の [ルート DN] フィールドに指定したディレクトリ ルート。この変数は、既存のルート サフィックスまたはサブ サフィックスのいずれかである必要があります。

例：ルートサフィックスが `dc=netegrity,dc=com` である場合、`smlldapsetup` を実行すると、ディレクトリサーバに以下が生成されます。

- ルートサフィックス、`dc=netegrity,dc=com`、対応する `userRoot` データベース。
- サブサフィックス、`ou=Netegrity,dc=netegrity,dc=com`、対応する `PolicySvr4` データベース。

例：ポリシーストアを `ou=apps,dc=netegrity,dc=com` の下に置く場合、`ou=apps,dc=netegrity,dc=com` は、ルートサフィックス `dc=netegrity,dc=com` のルートまたはサブサフィックスのいずれかである必要があります。

サブサフィックスである場合、`smlldapsetup` を実行すると以下が作成されます。

- ルートサフィックス、`dc=netegrity,dc=com`、対応する `userRoot` データベース。
- サブサフィックス、`ou=apps,dc=netegrity,dc=com`、対応する `Apps` データベース。
- サブサフィックス、`ou=Netegrity,ou=apps,dc=netegrity,dc=com`、対応する `PolicySvr4` データベース。

注：ルートサフィックスとサブサフィックスの詳細については、Sun Microsystems の [ドキュメント](#) を参照してください。

smldapsetup による SiteMinder ポリシー ストアの削除

SiteMinder ポリシー ストア データとスキーマを LDAP ディレクトリから削除するには、最初にデータを削除し、次にスキーマを削除する必要があります。

重要:

- SiteMinder ポリシー ストア データを削除する前に、削除するデータを含むポリシー ストアをポリシー サーバが参照していることを確認してください。smldapsetup は、ポリシー サーバが参照しているポリシー ストアからデータを削除します。また、データを削除する前に、ポリシー ストア データを出力ファイルにエクスポートして、ファイルのバックアップを作成します。
- Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合、管理者としてシステムにログインしていても、必ず管理者権限でコマンドライン ウィンドウを開くようにしてください。詳細については、お使いの SiteMinder コンポーネントの「リリース ノート」を参照してください。

smldapsetup を使用してポリシー ストアを削除する方法

1. 以下の場所へ移動します。

- (Windows) `siteminder_home\bin`
 - (UNIX) `siteminder_home/bin`
- `siteminder_home`

SiteMinder のインストール場所を指定します。

2. 以下コマンドを入力してポリシー ストア データを削除します。

```
smldapsetup remove -hLDAP_IP_Address -pLDAP_Port  
-d LDAP_Admin -wLDAP_Admin_Password -rLDAP_Base_DN  
-v
```

例: `smldapsetup remove -h192.169.125.32 -p552 -d"cn=directory
manager" -wfirewall -rdc=ad,dc=test,dc=com -v`

注: ポリシー ストア データの削除には多少の時間がかかる場合があります。

- 以下のコマンドを入力して、スキーマの削除に使用する LDIF ファイルを生成します。

```
smldapsetup ldgen -e -fldif
```

ldif

生成する LDIF ファイルの名前を指定します。

例：smldapsetup ldgen -e -fdelete.ldif

- 以下のコマンドを実行して、SiteMinder スキーマを削除します。

```
smldapsetup ldmod -fldif
```

ldif

smldapsetup ldgen -e を使用して生成した LDIF ファイルの名前を指定します。

例：smldapsetup ldmod -fdelete.ldif

ODBC データベース内の SiteMinder データの削除

SiteMinder には、ODBC データベースから SiteMinder スキーマを削除する SQL スクリプトが用意されています。以下のリストで各 SQL スクリプトについて説明します。

sm_oracle_ps_delete.sql

Oracle データベースから SiteMinder のポリシーストアおよびデータを削除します。

sm_oracle_logs_delete.sql

sm_oracle_logs.sql を使用してデータベースが作成された場合、Oracle データベースに格納された SiteMinder ログを削除します。

sm_oracle_ss_delete.sql

Oracle データベースから SiteMinder のセッションストアテーブルおよびデータを削除します。

sm_mssql_ps_delete.sql

SQL データベースから SiteMinder のポリシーストアおよびデータを削除します。

sm_mssql_logs_delete.sql

sm_mssql_logs.sql を使用してデータベースが作成された場合、SQL データベースに格納された SiteMinder ログを削除します。

sm_mssql_ss_delete.sql

SQL データベースから SiteMinder のセッションストア テーブルおよびデータを削除します。

sm_db2_ps_delete.sql

DB2 データベースから SiteMinder のポリシーストアとデータを削除します。

sm_db2_logs_delete.sql

sm_db2_logs.sql を使用してデータベースが作成された場合、DB2 データベースに格納された SiteMinder ログを削除します。

sm_db2_ss_delete.sql

DB2 データベースから SiteMinder のセッションストア テーブルおよびデータを削除します。

ODBC データベースの SQL スクリプトは以下の場所にあります。

- (Windows) *siteminder_home*¥db
siteminder_home
ポリシー サーバのインストールパスを指定します。
- (UNIX) *siteminder_home/db*
siteminder_home
ポリシー サーバのインストールパスを指定します。

データベース オブジェクトを削除するには、DB2、SQL Plus for Oracle、または SQL Server クエリ アナライザを使用して、適切な SQL スクリプトを実行します。

注: SQL スクリプト実行の詳細については、お使いのデータベースのマニュアルを参照してください。

smpatchcheck

smpatchcheck ツールでは、お使いのシステムにインストールされたポリシー サーバおよび Web エージェントに必要な Solaris パッチが存在するかどうかを判断することができます。smpatchcheck は、SiteMinder プラットフォーム マトリックスに示されている Solaris バージョンで実行できます。このマトリックスにアクセスするには、[テクニカルサポート](#)に移動し、SiteMinder プラットフォーム サポート マトリックスを検索してください。

smpatchcheck を使用する方法

1. `siteminder_home/bin` に移動します。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

2. 「smpatchcheck」と入力します。

必須のパッチと推奨されるパッチが検索され、そのステータスが表示されます。

例：

```
Testing for Required Patches:  
  Testing for Patch: 106327-09 ... NOT Installed  
Testing for Recommended Patches:  
  Testing for Patch: 106541-08 ... Installed  
  Testing for Patch: 106980-00 ... Installed  
SiteMinder Patch Check: Failed
```

以下のいずれかのメッセージが返されます。

Failed

必須のパッチが 1 つ以上インストールされていません。

一部失敗

推奨されるパッチが 1 つ以上インストールされていません。

Success

必須のパッチと推奨されるパッチがすべてインストールされています。

SiteMinder テストツール

SiteMinder テスト ツールは、エージェントとポリシー サーバの間の対話をシミュレートするユーティリティです。このツールは、ポリシー サーバの機能をテストします。テストツールは、エージェントとしての役割を果たし、実際のエージェントと同じようにポリシー サーバに対して要求を送信します。これにより、SiteMinder の設定を実際に展開する前にテストできます。

注: このツールの詳細については、「[ポリシー サーバ設定ガイド](#)」を参照してください。

smreg

スーパーユーザ パスワードを変更する方法

1. ポリシー サーバが稼働中であり、設定済みのポリシー ストアを参照していることを確認します。
2. smreg ユーティリティが `policy_server_home¥bin` にあることを確認します。

`policy_server_home`

ポリシー サーバのインストールパスを指定します。

注: ユーティリティがない場合は、サポート サイトで提供されているポリシー サーバインストール メディアから入手できます。

3. 以下のコマンドを実行します。

```
smreg -su password
```

```
password
```

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

注: `-su` とパスワードの間に必ず空白を入れてください。

スーパーユーザ アカウント パスワードが変更されます。

4. smreg ユーティリティを削除します。

ユーティリティを削除することで、スーパーユーザ パスワードが他の人によって変更されることを防ぎます。

XPSCounter

SiteMinder ライセンスの条件に準拠するため、SiteMinder 環境内のユーザー数をカウントできます。以下の手順では、ディレクトリの設定方法と、ディレクトリ内に格納されている SiteMinder ユーザのカウント方法を説明します。

1. カウントするユーザディレクトリごとに以下の変更を加えます。

注: 詳細については、「[SiteMinder ポリシー サーバ設定ガイド](#)」を参照してください。

- 管理 UI でディレクトリ管理者のユーザ名とパスワードを入力して、管理者クレデンシャルの使用を強制します。
 - 管理 UI を使用して、ユニバーサル ID および他のユーザ属性のマッピングを定義します。
2. Microsoft Active Directory のユーザストアについては、管理 UI を使用して inetOrgPerson 属性をマップします。
 3. SiteMinder ポリシーに関連付けられているユーザの数の確認

Active Directory の inetOrgPerson 属性のマッピング

SiteMinder ユーザストアが Microsoft Active Directory サーバ上にある場合は、各サーバ内の inetOrgPerson をマップしてから、SiteMinder ユーザをカウントします。

以下の手順に従います。

1. 管理 UI にログインします。
2. [インフラストラクチャ] - [ディレクトリ] をクリックします。
3. [ユーザディレクトリ] をクリックします。
4. 目的のユーザディレクトリを検索し、ディレクトリ名をクリックします。
5. [変更] をクリックします。
6. [属性マッピングリスト] セクションの [作成] をクリックします。
7. オブジェクトを作成するオプションを選択し、[OK] をクリックします。

8. 以下の名前を入力します。
inetOrgPerson
9. 以下の説明を入力します。
Active Directory ユーザをカウントするためのカスタム マッピング
(XPSCounter による)
10. [プロパティ] セクションで以下を行います。
 - a. [エイリアス] オプションが選択されていることを確認します。
 - b. 以下の定義を入力します。
ユーザ
11. [OK] をクリックします。
12. [サブミット] をクリックします。
inetOrgPerson 属性がマップされます。

SiteMinder ポリシーに関連付けられているユーザの数の確認

SiteMinder ライセンスの条件に準拠するため、SiteMinder ポリシーに関連付ける組織内ユーザの数を確認することができます。

注: SiteMinder バイナリ ファイル (XPS.dll、libXPS.so、libXPS.sl) への書き込みアクセス許可がユーザにない場合は、管理者が管理 UI または XPSecurity ツールを使用して、関連する XPS コマンドラインツールを使用する権限を付与する必要があります。

ユーザの数を確認する方法

1. ポリシー サーバのコマンド ウィンドウを開いて、以下のコマンドを入力します。
XPSCounter
ツールが起動し、このセッションのログ ファイルの名前が表示されます。また、[ライセンスのパラメータ] メニューが開きます。
2. 「1」と入力します。
[パラメータ] メニューが表示されます。
3. 「C」と入力します。
[カウンタ] メニューが表示されます。

4. 「I」と入力します。
5. ユーザディレクトリ **XID** を検索するには、「?」と入力します。ポリシーストアで定義されているユーザディレクトリのみがリストに表示されます。
6. カウント対象のユーザを含むディレクトリの数を入力します。
注: このツールは、指定された各ディレクトリ内のユーザオブジェクトの数をカウントします。これには、複数のディレクトリに示される同一のユーザオブジェクトまたは1つのディレクトリ内にある同一ユーザの複数のユーザオブジェクトは含まれません。このツールの実行結果を解釈するときは、このことを考慮する必要があります。
7. (オプション) 結果を説明するコメントを入力します。
ユーザがカウントされ、確認のメッセージが表示されます。
8. (オプション) 別のディレクトリ内のユーザをカウントするには、手順5～8を繰り返します。
9. 「V」と入力します。

カウントしたディレクトリごとに、以下の情報が表示されます。

XID

指定されたユーザディレクトリの一意の識別子を表示します。

例:

CA.SM::UserDirectory@0e-50ea30f0-b5c0-450c-a135-1e317dd25f11

名前

指定されたユーザディレクトリ (管理 UI で定義されている) の名前を表示します。

: count

指定されたユーザディレクトリの最新のユーザ数を表示します。カウンタに保存されている以前の値を削除する必要はありません。この値はカウンタを実行するたびに自動的に更新されます。

例: : 23

総数

カウントしたすべてのユーザディレクトリ内のユーザの合計数を表示します。たとえば、2つの異なるディレクトリのユーザをカウントし、各ディレクトリに23人のユーザがいた場合、表示される合計数は46です。

XPSConfig

XPSConfig は、管理者および運用メンバが製品のパラメータを表示し、許可される場合はその設定を編集できるようにする、対話型のコマンドラインユーティリティです。XPSConfig は必須ツールではないので、XPS プログラミング インターフェースを使用した製品固有の設定ツールを独自に所有する一方で、オプションとして使用できます。

XPSConfig は、ベンダーごとおよびインストールされた製品ごとに、製品のデータ ディクショナリ内で定義されているパラメータまたは指定された設定を管理します。各製品では、独自のパラメータ設定の読み取り、書き込み、および検証が可能です。

XPSConfig を使用するには、XPSConfig の権限を持った管理者である必要があります。

パラメータには以下の属性があります。

Name

パラメータ名を指定します。

制限：

- 名前は、文字またはアンダースコアで始まり、文字、数字、およびアンダースコアのみで構成される必要があります。
- 32 文字まで指定できます。
- 名前では大文字と小文字が区別されません。

Type

パラメータ値の以下のデータ型を指定します。

Logical | Numeric | String

Logical

ブール値 (TRUE または FALSE) を指定します。

Numeric

整数を指定します。

String

文字列を指定します。

Scope

パラメータの以下の値またはスコープを指定します。

Ask | Global | Local | Managed | Overrideable | Read Only

Ask

値が XPS ではなく製品によって管理され、読み取り専用であることを明示します。

Global

値がポリシーストア内に保存され、そのポリシーストアを共有するすべてのポリシーサーバによってアクセス可能であることを明示します。

Local

各ポリシーサーバが独自の値を保存することを明示します。

Managed

値が XPS ではなく製品によって管理され、読み取りと書き込みが可能であることを明示します。

Overrideable

値がポリシーサーバにローカルで保存され、共有ポリシーストアにグローバルに保存されている値を上書きできることを明示します。

Read Only

値がデフォルト値であり、かつ読み取り専用であることを明示します。

Export

このパラメータをポリシーストアのエクスポートに含めるかどうかを指定します。

型：ブール

Report

このパラメータをポリシーサーバの機能レポートに含めるかどうかを指定します。

型：ブール

RemoteAccess

リモート API がパラメータに対して持つアクセス許可のタイプを指定します。

None | Read | ReadWrite

Description

パラメータの目的を説明します。

LicenseType

ライセンス制限のタイプを指定します。

None | SoftLimit | HardLimit | ExpDate

None

パラメータがライセンス制限ではないことを明示します。

SoftLimit

パラメータが厳密でない忠告的なライセンス制限であることを明示します。

HardLimit

パラメータが厳密で絶対的なライセンス制限であることを明示します。

ExpDate

パラメータがライセンスが期限切れになる日付であることを明示します。

Default Value

現在の値が未定義の場合に使用するデフォルト値を指定します。

注: デフォルト値が未定義の場合、その値はデータ型に基づいて指定されます。

文字列

スペース

数値

ゼロ

ブール値

FALSE

Visible

パラメータを XPSConfig で表示するかどうかを指定します。

型：ブール

構文

XPSConfig の形式は以下のとおりです。

```
XPSConfig [-vendor vendor] [-product product]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

パラメータ

XPSConfig には以下のオプションがあります。

-vendor

(オプション) データを表示するベンダーの名前を指定します。

-product

(オプション) データを表示する製品の名前を指定します。

-?

(オプション) このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

(オプション) エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合は、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

-l

(オプション) 指定された場所にロギング情報を出力します。

デフォルト : `stdout`

-e

(オプション) 指定された場所にエラー情報を出力します。

デフォルト : `stderr`

-r

(オプション) 指定された場所にセッションのレコードを出力します。

XPSEvaluate

XPSEvaluate は、管理者およびアプリケーション開発者が式を評価し、パフォーマンスをテストできるようにする、対話型のコマンドラインユーティリティです。XPSEvaluate を使用するには、XPSEvaluate の権限を持った管理者である必要があります。

構文

XPSEvaluate の形式は以下のとおりです。

```
XPSEvaluate [-np] [-trace] [-dbg debuglist]  
[-f DB | formulapath] [-c contextpath] [-u userpath] [-step]  
[-?] [-vT | -vI | -vW | -vE | -vF]  
[-l log_path] [-e err_path] [-r rec_path]
```

パラメータ

XPSEvaluate には以下のオプションがあります。

-np

(オプション) プロンプトを指定しません。

-trace

(オプション) トレースをオンにします。

-dbg

(オプション) デバッグ リストを指定します。

-f

(オプション) 名前付き式の場所を指定します。

注: DB はポリシー ストアを指定します。

-c

(オプション) コンテキスト値の場所を指定します。

-u

(オプション) ユーザ属性の場所を指定します。

-step

(オプション) 評価の手順を表示します。

-?

(オプション) このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

(オプション) エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合は、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

-l

(オプション) 指定された場所にロギング情報を出力します。

デフォルト : stdout

-e

(オプション) 指定された場所にエラー情報を出力します。

デフォルト : stderr

-r

(オプション) 指定された場所にセッションのレコードを出力します。

XPSExplorer

XPSExplorer は、管理者またはアプリケーション開発者がポリシーストアのデータを表示できるようにする、対話型のコマンドラインユーティリティです。XPSExplorer には以下の 2 つの用途があります。

- ドメインまたはレルムのリストを確認することによって、より詳細なレベルでのエクスポートまたはインポート用にオブジェクトの識別子を判別する
- オブジェクトストアが破損し、手動で修復する必要がある場合に、そのストアを修復する。このアクションを実行する場合は、CA サポートの助言のもとでのみ実行する必要があります。

XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

構文

XPSExplorer の形式は以下のとおりです。

```
XPSExplorer [-?] [-vT | -vI | -vW | -vE | -vF]  
[-l log_path] [-e err_path] [-r rec_path]
```

パラメータ

XPSExplorer には以下のオプションがあります。

-?

(オプション) このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

(オプション) エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合は、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

-l

(オプション) 指定された場所にロギング情報を出力します。

デフォルト : stdout

-e

(オプション) 指定された場所にエラー情報を出力します。

デフォルト : stderr

-r

(オプション) 指定された場所にセッションのレコードを出力します。

ポリシーストアデータのサブセットのエクスポート

ポリシーストアデータのサブセットをエクスポートするには、エクスポートするオブジェクトの識別子 (XID) が必要です。オブジェクト識別子の検索には XPSExplorer を使用できます。XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

このユースケースでは、以下の監査アプリケーションをエクスポートします。

- Accounts Payable
- Accounts Receivable
- General Ledger
- 給与計算

ポリシーストアデータのサブセットのエクスポート

1. ポリシーサーバをホストしているマシンでコマンドプロンプトを開きます。
2. 以下のコマンドを入力します。

```
XPSExplorer
```

[メイン] メニューが開き、ベンダー、製品、およびクラスがリスト表示されます。

注: トップレベルのクラスにあるオブジェクトのみエクスポートできます。トップレベルのクラスはアスタリスクで示されます。

3. エクスポートするオブジェクトのクラスに対応する番号を入力します。

[クラス] メニューが開きます。

例: Accounting に対応する番号が 15 番の場合は、「15」を入力します。

4. 「S」と入力してクラス内のオブジェクトを表示します。

[検索] メニューが開き、クラス内のオブジェクトがリスト表示されます。

検索結果の例:

```
1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8
```

```
(I) Name           : "Accounts Payable"
```

```
(C) Desc           : "accounts payable"
```

2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

(I) Name : "Accounts Receivable"

(C) Desc : "accounts receivable"

3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

(I) Name : "General Ledger"

(C) Desc : "general ledger"

4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

(I) Name : "Payroll"

(C) Desc : "payroll"

5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

(I) Name : "Job Costing"

(C) Desc : "job costing"

オブジェクト識別子 (XID) の例 :

CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

5. 3回「Q」と入力して、[検索]、[クラス]、および[メイン]の各メニューを終了し、コマンドプロンプトに戻ります。
6. コマンドプロンプトで、以下のコマンドを入力します。

```
XPSEexport output_file -xo object_XID_1 -xo object_XID_2
-xo object_XID_3 -xo object_XID_4
```

output_file

ポリシーストアデータのエクスポート先となるXMLファイルを指定します。

-xo object_XID

エクスポートする各オブジェクトの識別子を指定します。

注: 検索結果からオブジェクト識別子 (XID) をコピーし、それをコマンドラインに貼り付けることができます。

例：

```
XPSExport accounting.xml
-xo CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8
-xo CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244
-xo CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92
-xo CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b
```

指定された監査アプリケーションのポリシーストアデータが `accounting.xml` にエクスポートされます。

XCart 管理

XPSExplorer には XCart 機能が含まれます。XCart を使用すると、エクスポートするオブジェクトの識別子 (XID) を収集し、後で使用できるようにファイルに保存できます。各 ID を手動でコピーおよび貼り付けする必要はありません。XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

XCart にアクセスするには、XPSExplorer の [メイン] メニューで [XCart Management] の「X」を入力します。[XCart] メニューが開き、XCart 内にあるオブジェクトがすべて表示されます。以下のオプションはコンテキスト依存のため、コンテキストに応じて表示されたり表示されなかったりします。

C - カートのクリア

XCart を空にします。

L - Load cart from file

- 初期ロード - 指定されたファイルの内容を XCart にロードし、指定されたファイル名を XCart ファイルとして記憶します。
- 後続のロード - 指定されたファイルの内容を XCart に追加します。

注: XCart ファイルの名前は変わりません。

S - ファイルへのカートの保存: `xcart_file`

XCart の内容を XCart ファイルに保存します。

重要: S コマンドは、プロンプトを最初に表示せずに、XCart ファイルの内容を上書きします。

N - 新規ファイルへのカートの内容の保存

XCart の内容を指定されたファイルに保存し、指定されたファイル名を XCart ファイルとして記憶します。

注: N コマンドは、指定されたファイルを上書きする前にプロンプトを表示します。

各オブジェクトには、XPS ファイルからポリシーストアへのインポート方法を指定するインポートモードのタグが付けられます。

A - インポートモードの設定: ADD

新規オブジェクトを追加します。既存のオブジェクトは置換しません。

O - インポートモードの設定: OVERLAY

既存のオブジェクトを置換します。新規オブジェクトは追加しません。

R - インポートモードの設定: REPLACE

既存のオブジェクトを置換し、新規オブジェクトを追加します。

D - インポートモードの設定: デフォルト値

デフォルトのインポートモードを指定します。

注: 製品クラスごとに、製品のデータディクショナリで定義されたデフォルトのインポートモードがあります。

Q - 終了

[XCart] メニューを終了し、[メイン] メニューに戻ります。

XCart によるポリシーストアデータのサブセットのエクスポート

ポリシーストアデータのサブセットをエクスポートするには、エクスポートするオブジェクトの識別子 (XID) が必要です。XPSExplorer の XCart 機能を使用すると、オブジェクトを検索し、エクスポートするときは後で使用できるように XCart ファイルに保存できます。たとえば、管理者は、運用のメンバが使用する XCart ファイルを必要に応じて設定できます。XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

このユース ケースでは、以下の 4 つの監査アプリケーションを後で使用できるようにファイルに保存します。

- Accounts Payable
- Accounts Receivable
- General Ledger
- 給与計算

XCart によるポリシー ストア データのサブセットのエクスポート

1. ポリシー サーバをホストしているマシンでコマンドプロンプトを開きます。
2. 以下のコマンドを入力します。

XPSExplorer

[メイン] メニューが開き、ベンダー、製品、およびクラスがリスト表示されます。

注: トップレベルのクラスにあるオブジェクトのみエクスポートできます。トップレベルのクラスはアスタリスクで示されます。

3. [XCart Management] の「X」を入力します。

[XCart] メニューが開きます。

4. テキスト ファイルを作成します。

例: C:\%xcart%\accounting.txt

注: これは XCart の内容を保存する場所です。

5. [Load cart from file] の「L」を入力します。

6. 作成したテキスト ファイルのパスと名前を入力します。

指定したファイル名は XCart ファイルとして記憶されます。

例: C:\%xcart%\accounting.txt

注: ファイルは存在している必要があります。ファイルが存在していない場合、「L」は効果がありません。

7. 「Q」と入力して [メイン] メニューに戻ります。

8. エクスポートするオブジェクトのクラスに対応する番号を入力します。

[クラス] メニューが開きます。

例: Accounting に対応する番号が 15 番の場合は、「15」を入力します。

9. 「S」 と入力してクラス内のオブジェクトを表示します。
[検索] メニューが開き、クラス内のオブジェクトがリスト表示されます。

検索結果の例：

1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

(I) Name : "Accounts Payable"

(C) Desc : "accounts payable"

2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

(I) Name : "Accounts Receivable"

(C) Desc : "accounts receivable"

3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

(I) Name : "General Ledger"

(C) Desc : "general ledger"

4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

(I) Name : "Payroll"

(C) Desc : "payroll"

5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

(I) Name : "Job Costing"

(C) Desc : "job costing"

10. 監査アプリケーション 1～4 について、以下の手順に従います。
- アプリケーションに対応する番号を入力します。
 - [Add to XCart] の「X」を入力します。
 - 「Q」と入力して [XCart] メニューを終了し、[検索] メニューに戻ります。

注：アプリケーション名の先頭にアスタリスクが付いている場合は、そのアプリケーションが XCart 内にあることを意味します。

11. 2回「Q」と入力して [検索] メニューと [クラス] メニューを終了し、[メイン] メニューに戻ります。
12. [XCart Management] の「X」を入力します。
13. 「S」と入力してカートを XCart ファイル (C:¥xcart¥accounting.txt) に保存します。

14. 2回「Q」と入力して [XCart] メニューと [メイン] メニューを終了し、コマンドプロンプトに戻ります。

15. コマンドプロンプトで、以下のコマンドを入力します。

```
XPSExport output_file -xf xcart_file
```

output_file

ポリシーストアデータのエクスポート先となる XML ファイルを指定します。

-xf xcart_file

エクスポートするオブジェクトの識別子 (XID) を含む XCart ファイルのパスと名前を指定します。

例:

```
XPSExport accounting.xml C:¥xcart¥accounting.txt
```

XCart ファイルに保存された監査アプリケーションのポリシーストアデータが `accounting.xml` にエクスポートされます。

XCart ファイルへのアプリケーションの追加

このユースケースでは、XPSExplorer の XCart 機能を使用して、XCart ファイル (`accounting.txt`) 内にすでに存在する以下の 4 つの監査アプリケーションに、5 つ目の監査アプリケーション (Job Costing) を追加します。

- Accounts Payable
- Accounts Receivable
- General Ledger
- 給与計算

注: XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

XCart ファイルへのアプリケーションの追加

1. ポリシー サーバをホストしているマシンでコマンドプロンプトを開きます。

2. 以下のコマンドを入力します。

XPSExplorer

[メイン] メニューが開き、ベンダー、製品、およびクラスがリスト表示されます。

注: トップレベルのクラスにあるオブジェクトのみエクスポートできます。 トップレベルのクラスはアスタリスクで示されます。

3. [XCart Management] の「X」を入力します。

[XCart] メニューが開きます。

4. [Load cart from file] の「L」を入力します。

5. 4 つの監査アプリケーションを含む既存のテキスト ファイルのパスと名前を入力します。

指定したファイル名は XCart ファイルとして記憶されます。

例: C:\xcart\accounting.txt

6. 「Q」と入力して [メイン] メニューに戻ります。

7. XCart ファイルに追加するクラスに対応する番号を入力します。

[クラス] メニューが開きます。

例: Accounting に対応する番号が 15 番の場合は、「15」を入力します。

8. 「S」と入力してクラス内のオブジェクトを表示します。

[検索] メニューが開き、クラス内のオブジェクトがリスト表示されます。

検索結果の例:

1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

(I) Name : "Accounts Payable"

(C) Desc : "accounts payable"

2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

(I) Name : "Accounts Receivable"

(C) Desc : "accounts receivable"

3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

(I) Name : "General Ledger"

(C) Desc : "general ledger"

4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

(I) Name : "Payroll"

(C) Desc : "payroll"

5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

(I) Name : "Job Costing"

(C) Desc : "job costing"

注: アプリケーション名の先頭にアスタリスクが付いている場合は、そのアプリケーションが XCart 内にあることを意味します。

9. XCart ファイルに Job Costing を追加する方法
 - a. Job Costing アプリケーションの「5」を入力します。
 - b. [Add to XCart] の「X」を入力します。
 - c. 「Q」と入力して [XCart] メニューを終了し、[検索] メニューに戻ります。

アプリケーション名の先頭にアスタリスクが付いている場合は、そのアプリケーションが XCart 内にあることを意味します。
 - d. 2回「Q」と入力して [検索] メニューと [クラス] メニューを終了し、[メイン] メニューに戻ります。
 - e. [XCart Management] の「X」を入力します。
 - f. 「S」と入力して XCart を XCart ファイル (C:¥xcart¥accounting.txt) に保存します。

Job Costing が accounting.txt に保存されます。

10. 2回「Q」と入力して [XCart] メニューと [メイン] メニューを終了し、コマンドプロンプトに戻ります。

XPSSecurity

XPSSecurity は、管理者および運用メンバが管理者を作成または削除し、その権限を編集できるようにする、対話型のコマンドラインユーティリティです。XPSSecurity を使用するには、XPSSecurity の権限を持った管理者である必要があります。

構文

XPSSecurity の形式は以下のとおりです。

```
XPSSecurity [-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

パラメータ

XPSSecurity には以下のオプションがあります。

-?

(オプション) このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

(オプション) エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合は、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

- l
(オプション) 指定された場所にロギング情報を出力します。
デフォルト : stdout
- e
(オプション) 指定された場所にエラー情報を出力します。
デフォルト : stderr
- r
(オプション) 指定された場所にセッションのレコードを出力します。

管理者をスーパーユーザにする

スーパーユーザは、外部管理者ストアへの接続を設定するときに定義されます。スーパーユーザを使用して、その他のすべての管理者アカウントを作成し、管理します。スーパーユーザがない場合は、XPSSecurity を使用して外部ストア内の任意のユーザをスーパーユーザにすることができます。

管理者をスーパーユーザにする方法

1. XPSSecurity 権限のある SiteMinder 管理者アカウントを使用して、ポリシー サーバ ホスト システムにログインします。

注: XPSSecurity 権限のある管理者がない場合は、以下のいずれかでログインできます。

- (Windows) システム管理者
- (UNIX) root
- ポリシー サーバをインストールしたユーザ

2. XPSSecurity ユーティリティが *policy_server_home/bin* にあることを確認します。

policy_server_home

ポリシー サーバのインストールパスを指定します。

注: ユーティリティがない場合は、サポートサイトで提供されているポリシー サーバインストールメディアから入手できます。

3. コマンドウィンドウを開き、以下のコマンドを実行します。

XPSSecurity

[メイン] メニューが表示されます。

4. 「A」と入力し、Enter キーを押します。

[管理者] メニューに、外部ストアの SiteMinder 管理者がリスト表示されます。各管理者名の先頭には番号が付いています。

5. 管理者の番号を入力し、Enter キーを押します。

[管理者]メニューに、選択した管理者に固有の属性が表示されます。各属性の先頭には番号が付いています。

6. 「2」と入力し、Enter キーを押します。

[管理者] メニューがフラグ設定によって更新されます。

7. 疑問符 (?) を入力し、Enter キーを押します。

Disabled および Super User フラグが表示されます。各フラグの先頭には番号が付いています。

8. 「2」と入力し、Enter キーを押します。

Super User フラグが選択されます。

9. 「Q」と入力し、Enter キーを押します。

[管理者] メニューに、管理者固有の属性が表示されます。Flags 属性が Super User に設定されます。

10. 「U」と入力し、Enter キーを押します。

管理者レコードが更新されます。

11. 「Q」と入力し、Enter キーを押します。

[管理者] メニューに、外部ストアの SiteMinder 管理者がリスト表示されます。選択した管理者がスーパーユーザとして表示されます。

12. 次の2つのプロンプトで「Q」と入力し、Enter キーを押して、ユーティリティを終了します。

選択した管理者はスーパーユーザです。この管理者を使用して、変更された権限または削除された権限を復元します。

-XPSSweeper

XPSSweeper は、バッチ ジョブとしても実行できるコマンドラインユーティリティです。XPSSweeper を使用して、XPS と SiteMinder ポリシーストアを同期できます。通常、XPS は異なるポリシーストアの同期を行います。ただし、レガシー ツールを使用するときは、XPSSweeper を使用してポリシーストアを再同期しなければならない場合があります。いずれにせよ、XPSSweeper によってポリシーストアが破損することはないので、安全策として実行できます。

構文

XPSSweeper の形式は以下のとおりです。

```
XPSSweeper [-f] [-s seconds] [-m entries]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path]
```

パラメータ

XPSSweeper には以下のオプションがあります。

-f

(オプション) XPSSweeper をループ内で永久に実行します。

注: Ctrl + C キーを押すと終了します。

-s

(オプション) XPSSweeper が反復する間、指定された秒数だけスリープ状態になります。

-m

(オプション) 指定された数のエントリがログに記録されるごとに、マイルストーンメッセージを出力します。

-?

(オプション) このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

(オプション) エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合に、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

-l

(オプション) 指定された場所にロギング情報を出力します。

デフォルト : stdout

-e

(オプション) 指定された場所にエラー情報を出力します。

デフォルト : stderr

バッチ ジョブとしての XPSSweeper の実行

XPSSConfig を使用して以下の 2 つの XPS 設定パラメータを設定することにより、XPSSweeper をバッチ ジョブとして実行できます。

CA.XPS::\$Autosweep

XPSSweeper を Autosweep スケジュールに基づいて実行するか、あるいは XPSSweeper をまったく実行しないかを明示します。

型 : ブール

CA.XPS::\$AutosweepSchedule

Autosweep スケジュール (GMT 時間) を以下の形式で指定します。

DDD@{HH:MM}[,{DDD@{HH:MM}}] ... [{,DDD@{HH:MM}}]

DDD

(オプション) 曜日を指定します。

Sun | Mon | Tue | Wed | Thu | Fri | Sat

HH

時間を指定します。

範囲：00 ~ 23

MM

分を指定します。

範囲：00 ~ 59

例:

Sun@08:30

毎週日曜日の午前 8:30 (GMT)

Tue@14:00

毎週火曜日の午後 2:00 (GMT)

15:15

毎日の午後 3:15 (GMT)

Sun@08:30,Tue@14:00,15:15

毎週日曜日の午前 8:30、毎週火曜日の午後 2:00、および火曜日を
除く毎日の午後 3:15

注: 複数の Autosweep 時間を指定する場合は、カンマ、空白、またはセミコロンで区切ります。

ポリシー サーバは XPSSweeper の Autosweep 時間を以下のように管理します。

- キャッシュ チェックが数分おきに行われるため、XPSSweeper はスケジュールから数分ずれて実行される場合があります。
- XPSSweeper の実行がスケジュールされている時刻にすでに実行している場合は、停止または再起動されることなく、スイーププロセスを完了できます。
- XPSSweeper はたとえスケジュールされたとしても、2 時間未満の間隔で実行されることはありません。

例：XPSSweeper が毎週火曜日の午後 2:00 および毎日の午後 3:15 に実行されるようにスケジュールされた場合、後者のスイープは火曜日には実行されません。

XPSSConfig を使用した 24 時間間隔で実行する Autosweep の設定

24 時間ごとに 1 回実行するように XPSSweeper ユーティリティを設定することをお勧めします。XPSSweeper ユーティリティの実行頻度が十分でない場合、ポリシー サーバの起動に問題が発生する場合があります。ポリシー ストア内にある削除対象オブジェクトが多すぎると、以下のエラーが発生します。

LDAP_SIZELIMIT_EXCEEDED

XPSSweeper ユーティリティを自動的に実行するように設定するには、以下の XPS 設定パラメータを使用します。

- CA.XPS::\$Autosweep
- CA.XPS::\$AutosweepSchedule

次の手順に従ってください:

1. ポリシー サーバをホストしているコンピュータでコマンドライン ウィンドウを開きます。
2. 以下のコマンドを入力します。

XPSSConfig

[製品] メニューが開き、製品がリスト表示されます。

3. 拡張可能ポリシーストアの場合は、「XPS」を入力します。
[パラメータ] メニューが開き、XPS パラメータがリスト表示されます。
4. 自動スイープの場合は「7」を入力します。
[移動スイープのパラメータ] メニューが開きます。
5. Autosweep 値が TRUE に設定されていることを確認するか、「C」と入力して値を TRUE に変更します。
注: この手順によって、XPSSweeper を Autosweep スケジュールに従って実行することを明示します。
6. 「Q」と入力して [Autosweep Parameter] メニューを終了し、[パラメータ] メニューに戻ります。
7. [AutosweepSchedule] の「8」を入力します。
[AutosweepSchedule パラメータ] メニューが開きます。
8. 「C」と入力して AutosweepSchedule パラメータの値を変更します。
9. [新しい値] に必要な時間を入力します。
10. 「Q」を3回入力します。
コマンドプロンプトが表示されます。

第 21 章: ポリシー サーバ設定ファイル

このセクションには、以下のトピックが含まれています。

[CA Compliance Security Manager 設定ファイル](#) (P. 321)

[Connection API 設定ファイル](#) (P. 322)

[OneView モニタ設定ファイル](#) (P. 322)

[SiteMinder 設定ファイル](#) (P. 323)

[SNMP 設定ファイル](#) (P. 323)

[SNMP イベントトラップ設定ファイル](#) (P. 324)

[ポリシーサーバレジストリキー](#) (P. 324)

CA Compliance Security Manager 設定ファイル

SiteMinder には、コマンドライン ツール `smcompliance` が用意されています。このツールによって作成されるコンプライアンス レポートは CA Security Compliance Manager に手動でインポートできます。CA Compliance Security Manager 設定ファイル (`compliance.conf`) を使用すると、コンプライアンス レポートの内容を変更することができます。

場所 : `siteminder_home¥compliance¥config`

`siteminder_home`

ポリシーサーバのインストールパスを指定します。

詳細情報:

[既存のコンプライアンス レポートの内容の変更](#) (P. 332)

[新しいコンプライアンス レポートの追加](#) (P. 331)

Connection API 設定ファイル

Connection API ファイル (conapi.conf) は、Connection API によってサービスを設定するために使用されます。これらのサービスには OneView モニタが含まれます。

場所 : `siteminder_home¥config`

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

詳細情報:

[OneView モニタのポート番号の設定 \(P. 212\)](#)

OneView モニタ設定ファイル

SiteMinder OneView モニタには以下の機能があります。

- SiteMinder 環境においてパフォーマンスのボトルネックを特定し、リソースの使用状況に関する情報を提供します。
- 特定のイベント (コンポーネント障害など) が発生した場合に、アラートを表示します。

OneView モニタ設定ファイル (mon.conf) を使用して以下を指定できます。

- OneView モニタが、登録済みのコンポーネントに対してデータを要求する頻度。
- 登録済みのコンポーネントが、OneView モニタにハートビートイベントを送信する頻度。
- ポリシー サーバ コンポーネントのインデックスが定数かどうか。

場所 : `siteminder_home¥monitor`

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

詳細情報:

[OneView データのリフレッシュ間隔とハートビートの設定 \(P. 211\)](#)

SiteMinder 設定ファイル

SiteMinder 設定ファイル (`siteminder.conf`) は以下の目的で使用されます。

- ポリシー サーバ プロセスの開始および停止
- 実行ファイルの設定、無効化、有効化

1 つ以上の実行のアプリケーションは、ポリシー サーバ プロセスのステータスを監視し、失敗した場合にプロセスを自動的に再起動します。

場所 : `siteminder_home¥config`

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

詳細情報:

[UNIX エグゼクティブの設定 \(P. 29\)](#)

[Windows エグゼクティブの設定 \(P. 29\)](#)

SNMP 設定ファイル

SNMP 準拠のネットワーク管理アプリケーションでは、SiteMinder 環境の多くの運用上の要素を監視できます。SiteMinder SNMP モジュールは、これらのアプリケーションとの情報の交換を可能にします。

SNMP 設定ファイル (`snmp.conf`) は、SiteMinder SNMP モジュールの設定を提供します。

場所 : `siteminder_home¥config`

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

注: このファイルの使用の詳細については、「ポリシー サーバインストールガイド」の「Windows 上での SNMP エージェントの設定」を参照してください。

SNMP イベントトラップ設定ファイル

SNMP イベント トラップ設定ファイル (`snmptrap.conf`) は、以下の設定を提供します。

- SNMP トラップにマップするシステム イベント。
- トラップの送信先のネットワーク管理システムのアドレス。

場所: `siteminder_home¥config`

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

注: このファイルに関連するタスクについては、「ポリシー サーバインストールガイド」の「Windows で SNMP イベント トラップを設定する方法」および「UNIX システムで SNMP イベント トラップを設定する方法」を参照してください。

詳細情報:

[イベントのデータ](#) (P. 231)

[SiteMinder MIB](#) (P. 223)

ポリシー サーバレジストリ キー

ポリシー サーバレジストリ キーは以下のいずれかにあります。

- (Windows)
`HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder ¥CurrentVersion¥PolicyServer.`

- (UNIX) `sm.registry` ファイル

このファイルのデフォルトの場所は `siteminder_home/registry` です。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

以下の点について考慮してください。

- 状況によっては、以下のいずれかを実行する必要があります。
 - 既存のレジストリ キーを変更する。
 - レジストリ キーを作成し、値を割り当てる。

これらの場合、必要な手順は **SiteMinder** ドキュメントに説明されています。

- それ以外の場合は、**SiteMinder** ドキュメントの説明に従って、管理 UI またはポリシー サーバ管理コンソールを使用してポリシー サーバ設定を変更することをお勧めします。**SiteMinder** サポートまたはドキュメントによって指示されない限り、レジストリ キーを使用してポリシー サーバ設定を変更することはしないでください。

付録 A: SiteMinder と CA Security Compliance Manager

このセクションには、以下のトピックが含まれています。

[SiteMinder と CA Security Compliance Manager の統合のしくみ \(P. 327\)](#)

[コンプライアンス レポートの生成 \(P. 329\)](#)

[使用可能なコンプライアンス レポートまたはそのフィールドのリストの表示 \(P. 330\)](#)

SiteMinder と CA Security Compliance Manager の統合のしくみ

CA SiteMinder には、CA Security Compliance Manager に手動でインポートできるコンプライアンス レポートを作成するコマンドラインツール (smcompliance) が用意されています。smcompliance ツールはデフォルトで、以下のタイプのレポートを生成します。

ポリシー

コマンドの実行元となる SiteMinder ポリシー サーバに格納されているポリシーをすべてリスト表示します。

ユーザディレクトリ

ポリシー サーバに関連付けられているポリシー ストア内のユーザディレクトリをすべてリスト表示します。

ユーザリソース

ユーザ、対応するユーザディレクトリ、および関連付けられているポリシーをリスト表示します。

SiteMinder コンプライアンス データを CA Security Compliance Manager にエクスポートするには、以下の手順に従います。

1. (オプション) 以下のいずれかの操作を実行する場合は、コンプライアンス ツールの設定ファイルを更新します。
 - 既存レポートのレポート名またはフィールド名を変更する。
 - 新規レポートを追加する。
 - レポートを削除する。

2. ポリシー サーバ上でコンプライアンス ツールを実行してレポートを生成します。
3. 生成したレポートを組織の CA Security Compliance Manager 管理者に送信します。

コンプライアンスレポートの生成

CA Security Compliance Manager 用の SiteMinder コンプライアンス レポートは、コマンドライン ツールを使用して生成します。 レポートを生成したら、CA Security Compliance Manager にインポートするため、組織の CA Security Compliance Manager 管理者に送信する必要があります。

コンプライアンスレポートを生成する方法

1. ポリシー サーバをホストしているマシンでコマンドライン ウィンドウを開きます。
2. 以下の任意のオプションを指定して `smcompliance` コマンドを実行します。

`-dir directory_name`

生成されたレポートを保存する出力ディレクトリの完全パスを指定します。 このディレクトリがすでに存在する場合、既存のディレクトリはバックアップとして名前が変更されます。

デフォルト : `siteminder_home/compliance/output`

`-conf configuration_file`

レポートの内容と形式を定義する設定ファイルの完全パスを指定します。 デフォルトの設定ファイルには CA Security Compliance Manager の内容が含まれますが、自分のニーズに合わせてカスタマイズできます。

デフォルト : `siteminder_home/compliance/config`

`-log log_file`

ログ ファイルの完全パスを指定します。

デフォルト : `siteminder_home/compliance/output`

`-format format_type`

レポートに使用するファイルのタイプとして、以下のいずれか 1 つを指定します。

- CSV (カンマ区切り値) ファイル
- XML ファイル

デフォルト : `csv`

レポートとログ ファイルが生成されます。 このファイルはすぐに CA Security Compliance Manager 管理者に送信できます。

使用可能なコンプライアンス レポートまたはそのフィールドのリストの表示

SiteMinder コンプライアンス レポート ツール (`smcompliance`) は、デフォルトで作成されるレポートに加えて、他のタイプのレポートも生成できます。

使用可能なコンプライアンス レポートのリストを表示する方法

1. ポリシー サーバでコマンドプロンプトを開きます。
2. 以下のコマンドを入力します。

```
smcompliance -help reports
```

レポート名のリストが表示されます。

3. (オプション) レポートに含まれるフィールドを確認するには、以下のコマンドを入力します。

```
smcompliance -generate report_name
```

`report_name` は、手順 2 のリストの名前に一致する必要があります。たとえば、エージェント レポートに含まれるフィールドを確認するには、以下のように入力します。

```
smcompliance -generate agents
```

レポートに含まれるフィールドのリストは XML 形式で表示されます。XML を設定ファイルに追加すれば、新しいレポートを生成できます。

新しいコンプライアンス レポートの追加

smcompliance ツールによって使用される設定ファイルに新規レポートを追加することによって、他のタイプのコンプライアンス レポートを生成できます。

新しいコンプライアンス レポートを追加する方法

1. 使用可能なコンプライアンス レポートのリストを smcompliance ツールで表示して、追加するレポートの名前を検証します。
2. 追加するレポートのフィールドを表示し、画面から XML 形式のテキストをコピーします。
3. ポリシー サーバの以下のディレクトリに移動します。

```
siteminder_home%compliance%config
```

4. デフォルトの設定ファイル (compliance.conf) をテキストエディタで開きます。
5. デフォルト ファイルのコピーを別の名前で保存します。
6. 既存の <report> セクションをコピーし、設定ファイルの下部にある </reports> タグの上に貼り付けます。
7. <columns> タグ間にある既存のテキストを削除します。
8. 手順 2 のテキストを <columns> タグ間に追加します。
9. <report> タグ内の name 属性の値を、手順 1 のレポートの名前に置き換えます。
10. <table> タグ内の name 属性の値を、新しいレポートの説明となるように変更します。生成されるレポート ファイルでは、この名前が使用されます。
11. 変更を保存し、新しい設定ファイルを閉じます。
新しいレポートが追加されます。
12. smcompliance コマンドを実行し、新しい設定ファイルを指定します。

既存のコンプライアンス レポートの内容の変更

デフォルトの設定ファイルによって生成されたレポートは、CA Security Compliance Manager が必要とする一般的なコンプライアンス情報を提供します。組織内でニーズが異なる場合は、独自のカスタム設定ファイルを作成して、希望する情報を含むレポートを生成できます。

1. ポリシー サーバの以下のディレクトリに移動します。

```
siteminder_home¥compliance¥config
```

2. デフォルトの設定ファイル (`compliance.conf`) をテキストエディタで開きます。
3. デフォルト ファイルのコピーを別の名前で作成して保存します。
4. 新しい設定ファイルのコピーに以下の任意の変更を加えます。
 - レポートを削除するには、削除するレポートが `<report>` タグと `</report>` タグの間にあることを確認し、そのセクションとタグを削除します。
 - レポートの名前を変更するには、`<table>` タグ内の `name` 属性の値を変更します。
 - レポート内のフィールドの名前を変更するには（フィールド内の情報ではなく）、`<column>` タグ内の `name` 属性の値を変更します。
 - 追加する任意の列を、設定ファイルの `<comment>` セクションから `<columns>` セクションへ移動します。

付録 B: SiteMinder の一般的なトラブルシューティング

LDAP 検索タイムアウトの問題を解決する

問題の状況:

LDAP サーバが検索結果を返す前にタイムアウトしていることが、`smps.log` で示されています。タイムアウト間隔を増やす方法を教えてください。

解決方法:

以下の [レジストリ設定](#) (P. 41) の値を変更します。

`SearchTimeout`

管理 UI が無応答になる

問題の状況:

スタンドアロン管理 UI インストール (JBoss アプリケーション サーバが組み込まれている) で、管理 UI は応答しなくなります。つまり、管理 UI サービスは開始されず、通常動作の期間の後にログインできません。

解決方法:

1. 管理 UI アプリケーション サーバを停止します。
2. アプリケーション サーバがダウンしている場合、以下の場所にあるデータ ディレクトリの名前を変更するか削除します。

```
¥adminui¥server¥default
```

3. アプリケーション サーバを再起動します。
4. ポリシー サーバで以下のコマンドを実行します。

```
XPSRegClient client_name[:passphrase] -adminui -t timeout -r retries -c comment  
-cp -l log_path -e error_path  
-vT -vI -vW -vE -vF
```

注: *client_name* と *[:passphrase]* の間にスペースを挿入すると、エラーが発生します。

client_name

登録する 管理 UI を識別します。

制限: この値は一意である必要があります。たとえば、管理 UI の登録にすでに *smui1* を使用している場合は、「*smui2*」と入力します。

注: この値は記録しておいてください。この値は、管理 UI から登録処理を完了するときを使用します。

passphrase

管理 UI の登録の完了に必要なパスワードを指定します。

制限:

- パスフレーズは 6 文字以上にする必要があります。
- パスフレーズには、アンパサンド (&) またはアスタリスク (*) を含めることができません。

- パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。
- 管理 UI をアップグレードの一部として登録する場合、以前のパスフレーズを再利用できます。

注: この手順でパスフレーズを指定しない場合、XPSRegClient でパスフレーズの入力と確認が求められます。

重要: パスフレーズを記録して、後で参照できるようにします。

-adminui

管理 UI の登録を指定します。

-t timeout

(オプション) 管理 UI からの登録処理を完了する必要がある時間を指定します。タイムアウト値に到達すると、ポリシー サーバは登録リクエストを拒否します。

測定単位: 分

デフォルト: 240 (4 時間)

最小制限: 1

最大制限: 1440 (1 日)

-r retries

(オプション) 管理 UI からの登録処理を完了するまでに許容される試行の失敗回数を指定します。登録処理時にポリシー サーバに間違ったクライアント名またはパスフレーズをサブミットすると、登録に失敗することがあります。

デフォルト: 1

最大制限: 5

-c comment

(任意) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(任意) 登録ログ ファイルに複数行のコメントが含まれることを指定します。登録ツールにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log_path*

(オプション)。登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストールパスを指定します。

-e *error_path*

(任意) 例外を指定されたパスに送信します。

デフォルト: *stderr*

-vT

(任意) 詳細レベルを **TRACE** に設定します。

-vI

(任意) 詳細レベルを **INFO** に設定します。

-vW

(任意) 詳細レベルを **WARNING** に設定します。

-vE

(任意) 詳細レベルを **ERROR** に設定します。

-vF

(任意) 詳細レベルを **FATAL** に設定します。

登録ログ ファイルの名前が一覧表示され、パスフレーズが求められます。

5. Enter キーを押します。

登録ツールにより、クライアント名およびパスフレーズの組み合わせが作成されます。

6. ポリシー サーバに 管理 UI を登録するには、管理 UI ホストで以下のいずれかの手順を実行します。

- Windows の場合 :

- (推奨) 管理 UI ショートカットを使用して 管理 UI を開きます。ショートカットを使用するには、SSL を介して 管理 UI を登録します。ショートカットへのアクセス権がない場合は、Web ブラウザを開き以下の場所へ移動します。

`https://host:8443/iam/siteminder/adminui`

注: 10 年間有効な自己署名証明書が作成され、接続に使用されます。証明書は RSA 2048 キーの強度で作成されます。

- Web ブラウザを開き、以下の場所へ移動します。

`http://host:8080/iam/siteminder/adminui`

- UNIX の場合 :

- (推奨) SSL を介して 管理 UI を登録するには、Web ブラウザを開き以下の場所へ移動します。

`https://host:8443/iam/siteminder/adminui`

- ブラウザを開き、以下の場所へ移動します。

`http://host:8080/iam/siteminder/adminui`

注: ホスト システムに Web ブラウザがない場合には、ログイン画面にリモート アクセスすることもできます。

host

管理 UI ホスト システムの完全修飾名を指定します。

SiteMinder 管理 UI のログイン画面が表示されます。

7. [ユーザ名] フィールドに以下の値を入力します。

`siteminder`

8. [パスワード] フィールドに、SiteMinder スーパーユーザアカウントのパスワードを入力します。

MySQL セッション ストア タイムアウト エラーの解決

問題の状況:

MySQL データベースがセッションストアとして設定される場合、以下のタイムアウトメッセージがポリシー サーバ ログに定期的に表示されます。

```
[ERROR][sm-Server-07011] failed.Exception : State = HYT00 Internal Code = 0 - [DataDirect][ODBC MySQL Wire Protocol driver]Timeout expired.. エラー コード -4007
```

解決方法:

以下のレジストリ ロケーションにある `MaintenanceQueryTimeout` レジストリ キーの値を変更して、セッションサーバメンテナンスクエリタイムアウトの値を増やします。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\SessionServer
```

以下の値をお勧めします。

```
MaintenanceQueryTimeout=0x12c
```

ポリシーサーバがLDAP 管理者制限を超過したエラーで終了する

問題の状況:

ポリシーサーバは、ポリシーストア/キーストアのLDAP検索が以下のエラーで失敗する場合に終了します。

```
LDAP_ADMINLIMIT_EXCEEDED (エラー コード 11)
```

解決方法:

以下のオプションのレジストリ キーを有効にします。

```
EnableRetryOnAdminLimitExceededFailure
```

ポリシーサーバが終了する前に検索を1回再試行できるようにします。

値: 0 (無効) または 1 (有効)

デフォルト: 0

Windows

次の手順に従ってください:

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択します。
2. [ファイル名を指定して実行] ダイアログボックスで「regedit」と入力し、[OK] をクリックします。
3. レジストリ エディタで以下の場所に移動します。
`HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder¥CurrentVersion¥ObjectStore`
4. 以下のレジストリ キーの値を変更します。
`EnableRetryOnAdminLimitExceededFailure`
5. ポリシー サーバを再起動します。

UNIX

次の手順に従ってください:

1. 以下の場所に移動します。
`install_directory/siteminder/registry`
2. テキストエディタを使用して `sm.registry` を開きます。
3. ファイル内にある次のテキストを確認します。
`HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder¥CurrentVersion¥ObjectStore`
4. 以下のレジストリ キーの値を変更します。
`EnableRetryOnAdminLimitExceededFailure`
5. ポリシー サーバを再起動します。

コマンドラインからのポリシー サーバのトラブルシューティング

ポリシー サーバのトラブルシューティングを行う場合、デバッグ オプションをオンにすると、ポリシー サーバのプロセスを個別のウィンドウで対話式に実行できます。次のサーバ実行可能ファイルは、コマンドラインから実行できます。

```
install_dir/siteminder/bin/smpolicysrv
```

注: Windows システムでは、リモート デスクトップまたは [ターミナル サービス] ウィンドウから `smpolicysrv` コマンドを実行しないでください。`smpolicysrv` コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは [ターミナル サービス] ウィンドウから `smpolicysrv` プロセスを実行した場合には機能しません。

`smpolicysrv` コマンドでは以下のオプションを使用します。

`-tport_number`

このオプションは、サーバがエージェント接続用にバインドする TCP ポートを変更する場合に使用します。このスイッチが使用されなかった場合、サーバはポリシー サーバ管理コンソールで指定された TCP ポートをデフォルトで使用します。

`-uport_number`

このオプションは、サーバが RADIUS 接続用にバインドする UDP ポートを変更する場合に使用します。このスイッチが使用されなかった場合、サーバはポリシー サーバ管理コンソールで指定された UDP ポートをデフォルトで使用します。このスイッチは認証サーバと監査サーバにのみ適用できます。

`-stop`

このスイッチにより、サーバは可能な限り正式な手順を踏んでから停止します。この方法を使用すると、すべてのデータベース接続とネットワーク接続が適切に閉じられます。

`-abort`

このスイッチにより、サーバはデータベース接続とネットワーク接続を先に閉じるという手順を踏むことなく、ただちに停止します。

`-stats`

このスイッチは、現在のサーバの実行時の統計情報（スレッドプールの限度、スレッドプール メッセージ、接続数など）を生成します。

-resetstats

このスイッチは、ポリシー サーバを再起動せずに、現在のサーバの実行時の統計情報をリセットします。このスイッチは以下のカウンタをリセットします。

- 最大スレッド数は、現在のスレッド数の値にリセットされます。
- メッセージキューの最大階層数は、現在の階層数にリセットされます。
- 最大接続数は、現在の接続数にリセットされます。
- メッセージ数、待機回数、ミス回数、および制限の超過回数はゼロにリセットされます。

このスイッチは以下のカウンタをリセットしません。

- スレッドプールの制限
- 現在のスレッド数
- メッセージキューの現在の階層数
- 現在の接続数
- 接続数の制限

-publish

ポリシー サーバに関する情報を発行します。

-tadmport_number

管理サービス用の TCP ポートを設定します。

-uacport_number

RADIUS 監査用の UDP ポートを設定します。

-uadmport_number

管理サービス用の UDP ポートを設定します。

-uauthport_number

Radius 認証用の UDP ポートを設定します。

-ac

エージェント API リクエストのサービスを有効にします。

-noac

エージェント API リクエストのサービスを無効にします。

-adm

管理リクエストのサービスを有効にします。

-noadm

管理リクエストのサービスを無効にします。

-radius

RADIUS リクエストのサービスを有効にします。

-noradius

RADIUS リクエストのサービスを無効にします。

-onlyadm

以下のオプションを統合して 1 つのオプションにします。

- -adm
- -noac
- -noradius

-starttrace

コマンドの説明

- トレース ファイルへのログの記録を開始し、コンソールへのトレース ロギングには影響しません。
- ポリシー サーバが稼働していない場合は、エラーを発行します。

ポリシー サーバがすでにトレース データのログを記録している場合に `-starttrace` コマンドを実行すると、

- 現在のトレース ファイルの名前が変更され（ファイル名の最後にタイム スタンプを付けて `file_name.YYYYMMDD_HHmss.extension` の形式で）、
- 元の名前を持つ新しいトレース ファイルが作成されます。

たとえば、ポリシー サーバ管理コンソールの [プロファイラ] タブでのトレース ファイル名が `C:¥temp¥smtrace.log` である場合、新しいファイルが生成されると、古いファイルは

`c:¥temp¥smtrace.20051007_121807.log` として保存されます。タイムスタンプは、ファイルが 2005 年 10 月 7 日の午後 12:18 に作成されたことを示しています。ポリシー サーバ管理コンソールの [プロファイラ] タブでファイルのトレース機能を有効にしていない場合は、このコマンドを実行しても何も起こりません。

-stoptrace

コマンドの説明

- ファイルへのログの記録を中止し、コンソールへのトレース ロギングには影響しません。
- ポリシー サーバが稼働していない場合は、エラーを発行します。

smpolicysrv の 2 つのコマンドライン オプション **-dumprequests** および **-flushrequests** を使用すれば、トラブルシューティングを行い、いっぱいになっているポリシー サーバのメッセージ キューの状態から早く回復できます。これらのオプションを使用するのは、以下の場合のみです。

1. ポリシー サーバのメッセージ キューで待機しているエージェント リクエストがタイムアウトになった。
2. タイムアウトになったリクエストが 1 つ以上のエージェントによって再送信され、メッセージ キューがいっぱいになった。

重要: 通常の動作条件下では **-dumprequests** および **-flushrequests** を使用しないでください。

-dumprequests

ポリシー サーバのメッセージ キュー内にある各リクエストの概要を監査ログに出力します。

-flushrequests

ポリシー サーバのメッセージ キュー全体をクリアし、リクエストが残っていない状態にします。

デバッグの動的な開始または停止

一部のコンポーネントのデバッグ機能は、ポリシー サーバを再起動することなく、いつでも開始または停止できます。

注: この機能は、CA Technologies [テクニカルサポート](#) 担当者からの指示があった場合にのみ使用することをお勧めします。

次の手順に従ってください:

1. ポリシー サーバをホストしているマシンでコマンド ウィンドウを開きます。
2. 以下のコマンドを入力します。

```
SmCommand -i SiteMinder
```

オプションのリストが表示されます。

3. CA サポート担当者からの指示に従って、以下のデバッグ オプションのいずれかを選択します。

CA.EPM::EPMObjects_Debug

SiteMinderEPM コンポーネントのデバッグ状態を切り替えます。

CA.XPS::Debug

SiteMinderXPS コンポーネントのデバッグ状態を切り替えます。

CA.XPS::XPSEval_Debug

SiteMinderXPSEvaluate コンポーネントのデバッグ状態を切り替えます。

トレースの動的な開始または停止

一部のコンポーネントのトレース機能は、ポリシー サーバを再起動することなく、いつでも開始または停止できます。

次の手順に従ってください:

1. ポリシー サーバをホストしているマシンでコマンド ウィンドウを開きます。

2. 以下のコマンドを入力します。

```
SmCommand -i SiteMinder
```

3. オプションのリストが表示されます。トレース オプションには、現在の状態の反対の状態が表示されます。たとえば、CA XPS のトレースが現在無効になっている場合は、トレースをオンにするオプションが以下のように表示されます。

```
item_number - CA.XPS::TraceOn
```

4. 希望するオプションの番号を入力して、以下のオプションのいずれかを選択します。

CA.EPM::EPMObjects_TraceState

EPM Objects コンポーネントのトレースをオンまたはオフに切り替えます。

CA.XPS::TraceState

XPS コンポーネントのトレースをオンまたはオフに切り替えます。

CA.XPS::XPSEval_TraceState

XPS Expression Evaluator コンポーネントのトレースをオンまたはオフに切り替えます。

確認メッセージが表示されます。変更が反映されたオプションのリストが再表示されます。

5. (オプション) 別のコンポーネントに対してトレースを開始または停止するには、手順 4 を繰り返します。

6. 「Q」と入力して終了します。

トレースが動的に変更されます。

Web エージェント通信失敗後にポリシー サーバがハングする

問題の状況:

ポリシー サーバリクエストの処理中、たとえばネットワーク停止などで Web エージェントがオフラインになった場合、この通信失敗についてポリシー サーバに通知されないと、ポリシー サーバは、Web エージェント データを待機し続けます。Web エージェントがネットワーク機能を回復してポリシー サーバとの接続を閉じた後も、ポリシー サーバは待機を続けます。

この方法で、1 つまたは複数の Web エージェントから多くのリクエストが失われた場合、リクエストを処理するワーカー スレッドが解放されないため、ポリシー サーバが反応しなくなる可能性があります。

解決方法:

SiteMinder Enable TCP Keep Alive (`SM_ENABLE_TCP_KEEPALIVE`) 環境変数を作成して有効にすると、アイドル状態の Web エージェント接続に対して KeepAlive パケットを送信するようポリシー サーバが設定されます。ポリシー サーバがパケットを送信する間隔は、OS 固有の TCP/IP パラメータに基づいて決まります。

また、Web エージェント、アプリケーションサーバエージェント (ASA)、管理 UI、または SDK によって作成されたカスタム エージェントのロケーションでこの変数を設定できます。

パラメータを設定する場合には、以下の点を考慮します。

- ポリシー サーバがパケット送信をいつ開始する必要があるか。
- ポリシー サーバがパケットを送信する間隔。
- ポリシー サーバがパケットを何回送信したら、Web エージェント接続が失われたと判断されるか。

注: TCP/IP パラメータの設定の詳細については、お使いの OS のドキュメントを参照してください。

アイドル状態の Web エージェント接続に KeepAlive パケットを送信するようポリシー サーバを設定する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のいずれかを実行します。
 - (Windows) 以下のシステム環境変数を作成して値を 1 に設定します。
`SM_ENABLE_TCP_KEEPALIVE`
 - (UNIX)
 - a. 以下のシステム環境変数を作成します。
`SM_ENABLE_TCP_KEEPALIVE=1`
 - b. 環境変数をエクスポートします。

注: 値は 0 (無効) または 1 (有効) である必要があります。0 または 1 以外の値が設定された場合、環境変数は無効になります。環境変数が無効になった場合、ポリシー サーバは、アイドル状態の Web エージェント接続に対して KeepAlive パケットを送信しません。

インストールされている JDK のバージョンの確認

ポリシー サーバの起動に失敗した場合、適切なバージョンの JDK がインストールされているかどうかを確認してください。

ポリシー サーバ ログのローカル時間設定の無効化

ポリシー サーバ ログ ファイル (*install_dir/siteminder/log/smps.log*) には、ポリシー サーバがインストールされているマシンのオペレーティングシステムで指定されているローカルタイムゾーンの時刻が表示されます。

このログファイルの時刻をグリニッジ標準時 (GMT) で表示するには、次の手順に従います。

1. 次のレジストリ設定を確認します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\
CurrentVersion\LogConfig\LogLocalTime
```

2. 値を、1 (デフォルト設定) から 0 に変更します。

システム アプリケーション ログの確認

ポリシー サーバの起動に失敗した場合、イベントログ (Windows NT の場合) または syslog (UNIX の場合) を参照して、ポリシー サーバに関する情報がないかを確認します。

- Windows の場合、イベントビューアを使用してイベントログを参照します。イベントビューアの [ログ] メニューから [アプリケーション] を選択します。
- UNIX の場合、テキストエディタを使用して syslog を参照します。

LDAP SDK 層によって処理される LDAP リフェラル

SiteMinder の LDAP リフェラル処理は強化され、パフォーマンスと冗長性が向上しました。旧バージョンの SiteMinder がサポートしていたのは、LDAP SDK 層による自動 LDAP リフェラル処理でした。LDAP リフェラルが発生すると、これまでは LDAP SDK 層が、参照先サーバへのリクエストの実行を、ポリシー サーバと通信せずに処理していました。

現行バージョンの SiteMinder は、非自動（拡張）LDAP リフェラル処理をサポートしています。非自動リフェラル処理では、LDAP リフェラルは、LDAP SDK 層ではなくポリシー サーバに返されます。リフェラルには、リフェラルの処理に必要なすべての情報が含まれています。ポリシー サーバは、リフェラルで指定されている LDAP ディレクトリが使用できるかどうかを調べて、該当する LDAP ディレクトリが機能していない場合は、リクエストを中断させることができます。この機能により、オフラインのシステムへの LDAP リフェラルによってリクエスト待ち時間が恒常的に増加することによるパフォーマンスの低下が解消されます。このような待ち時間の増加は、SiteMinder でリクエストの飽和状態を発生させることがあります。

LDAP リフェラルの無効化

LDAP リフェラルによってエラーが発生する場合は、すべての LDAP リフェラルを無効にすることができます。LDAP リフェラルを無効にすると、使用しているディレクトリのすべてのリフェラルはエラーを返すようになります。

Windows 環境のポリシー サーバの LDAP リフェラル処理を無効にする方法

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択します。
2. [ファイル名を指定して実行] ダイアログボックスで「regedit」と入力し、[OK] をクリックします。
3. レジストリエディタで、次のレジストリ設定を確認します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\
CurrentVersion\Ds\LDAPProvider
```

4. 次のレジストリ値を変更します。

注: 値は 16 進数で示されます。

```
"EnableReferrals"=dword:00000001
```

LDAP リフェラルをポリシー サーバによって処理するかどうかを決定します。0 に設定すると、LDAP リフェラルはポリシー サーバによって処理されません。1 に設定すると、LDAP リフェラルはポリシー サーバによって処理されます。

LDAP リフェラルは、デフォルトでは有効になっています。この設定は、レジストリを編集するだけで変更できます。

5. ポリシー サーバを再起動します。

Solaris 環境のポリシー サーバの LDAP リフェラル処理を無効にする方法

1. 次のディレクトリに移動します。

```
install_dir/siteminder/registry
```

2. テキストエディタを使用して `sm.registry` を開きます。

3. ファイル内にある次のテキストを確認します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\  
CurrentVersion\Ds\LDAPProvider
```

4. 手順 3 で確認した行の下に次のテキストで始まる行があることを確認します。

```
EnableReferrals
```

5. セミコロンの直前にある値を、次の説明に従って変更します。

注: 値は 16 進数に変換する必要があります。

LDAP リフェラルをポリシー サーバによって処理するかどうかを決定します。0 に設定すると、LDAP リフェラルはポリシー サーバによって処理されません。1 に設定すると、LDAP リフェラルはポリシー サーバによって処理されます。

6. ポリシー サーバを再起動します。

バインド操作での LDAP リフェラルの処理

Windows 環境のポリシー サーバに対してバインド操作での LDAP リフェラルを設定する方法

1. Windows の [スタート] メニューから [ファイル名を指定して実行] を選択します。
2. [ファイル名を指定して実行] ダイアログボックスで「regedit」と入力し、[OK] をクリックします。
3. レジストリエディタで、次のレジストリ設定を確認します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\  
CurrentVersion\Ds\LDAPProvider
```

4. 次のレジストリ値を変更します。

注: 値は 16 進数で示されます。

```
"ChaseReferralsOnBind"=dword:00000001
```

バインド操作での LDAP リフェラルを追跡するかどうかを決定します。ほとんどの LDAP ディレクトリ サーバは、バインド操作での LDAP リフェラルを処理します。使用しているディレクトリ サーバがバインド操作でのリフェラルを処理する場合、ChaseReferralsOnBind は無効です。ただし、ディレクトリ サーバが処理しない場合は、この設定によって、ポリシー サーバがバインドリフェラルを処理するようになります。

使用しているサーバがバインド操作でのリフェラルを処理する場合は、この設定を 0 に変更して、ポリシー サーバのバインドリフェラル処理機能を無効にすることができます。

バインド操作でのリフェラルの追跡は、デフォルトでは有効になっています。この設定は、レジストリを編集するだけで変更できます。

5. ポリシー サーバを再起動します。

Solaris 環境のポリシー サーバに対してバインド操作での LDAP リフェラルを設定する方法

1. 次のディレクトリに移動します。

```
install_dir/siteminder/registry
```

2. テキストエディタを使用して sm.registry を開きます。
3. ファイル内にある次のテキストを確認します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\
CurrentVersion\Ds\LDAPProvider
```

4. 手順 3 で確認した行の下に次のテキストで始まる行があることを確認します。

```
ChaseReferralsOnBind
```

5. セミコロンの直前にある値を、次の説明に従って変更します。

注: 値は 16 進数に変換する必要があります。

バインド操作での LDAP リフェラルを追跡するかどうかを決定します。ほとんどの LDAP ディレクトリ サーバは、バインド操作での LDAP リフェラルを処理します。使用しているディレクトリ サーバがバインド操作でのリフェラルを処理する場合、ChaseReferralsOnBind は無効です。ただし、ディレクトリ サーバが処理しない場合は、この設定によって、ポリシー サーバがバインドリフェラルを処理するようになります。

使用しているサーバがバインド操作でのリフェラルを処理する場合は、この設定を **0** に変更して、ポリシーサーバのバインドリフェラル処理機能を無効にすることができます。

6. ポリシーサーバを再起動します。

アイドルタイムアウトとステートフルインスペクションデバイス

ステートフルインスペクションデバイス (ファイアウォールなど) では、一般に、アイドルタイムアウトを設定できます。ポリシーサーバからエージェントへの SiteMinder 接続でも、アイドルタイムアウトを設定できます。

ポリシーサーバは、サービスに定期的にポーリングします。ポーリング間隔は、最大 5 分間です。つまり、アイドル接続は、設定された値から 5 分以内にタイムアウトになります。たとえば、タイムアウト値を 55 分間に設定すると、アイドル接続は 55 ~ 60 分間でタイムアウトになります。

デフォルトでは、ポリシーサーバと Web エージェントの間の接続は、非アクティブの状態が 10 分間続くとタイムアウトします。ポリシーサーバと Web エージェントの間にファイアウォールなどのステートフルネットワークデバイスがあり、接続のアイドル状態がデバイスのアイドルタイムアウト設定よりも長く続くと、デバイスは、ポリシーサーバや Web エージェントに通知せずに、接続を終了させます。

Web エージェントは、ネットワークデバイスによって終了された接続の使用を試行する際、ネットワークエラーを受信し、接続をリセットして、ブラウザに 500 エラー (20-0003) のメッセージを表示します。また、エージェントは、接続プール内の他の接続で、エラーを受信した接続以前に確立されたものをすべて閉じます。ただし、ポリシーサーバの方では、それらの接続のソケットは確立されたままです。サイトの負荷パターンによっては、ポリシーサーバの正常な動作を妨げるような接続の増加が発生する場合があります。

ファイアウォールなどのステートフル ネットワーク デバイスによるポリシー サーバと Web エージェントの間の接続の終了を防ぐには、ポリシー サーバのアイドル タイムアウトを設定する必要があります。ポリシー サーバは、TCP/IP 接続を閉じると、非アクティブな状態が指定された時間続くのを待ってから、RESET を送信して、サーバ側とクライアント側の両方で接続を適切に閉じます。非アクティブ状態の期間は、ポリシー サーバ管理コンソールの [設定] タブにあるアイドル タイムアウトの [分] フィールドで指定します。

注: アイドル タイムアウトの [分] フィールドは、管理者の総接続時間を制限するためにも使用できます。

インストール時、アイドル タイムアウトの値は 10 分に設定されます。ステートフルネットワークデバイスと共に使用する場合は、この値を、Web エージェントとポリシー サーバの間にあるデバイスの TCP/IP アイドルタイムアウトよりも短い時間に設定してください。ポリシー サーバのタイムアウトが必ず先に発生するように、TCP アイドルセッションタイムアウトを、ステートフルデバイスのアイドルタイムアウトの 60% に設定することをお勧めします。

エラー -- Optional Feature Not Implemented

ポリシー サーバが ODBC データソースの使用を試行する際、データベースに接続できないと、次のエラーメッセージが表示されることがあります。

Optional feature not implemented.. Error code -1

多くの場合、このメッセージは、コンポーネントの不適切な組み合わせ、不適切な設定、または無効な認証情報を示しています。

注: CA の Intersolv または Merant ドライバの設定は、デフォルト設定とは異なります。

ODBC データソースをポリシー ストアとして使用しているとき、またはロギング用に使用しているときにこのメッセージが表示される場合は、「ポリシー サーバインストールガイド」の ODBC データソースの設定に関するセクションを参照してください。

管理者アクティビティの記録時に発生するエラーまたはパフォーマンスの低下

ポリシー サーバ管理コンソールの [監査] タブで、[管理者によるポリシーストアオブジェクトの変更] を [すべてのイベントのログ取得] に設定している場合、ログを ODBC データソースに記録中に、以下のいずれかの状態になることがあります。

- 管理 UI でのオブジェクトの保存時に大きな遅延が発生する。
- 次のエラーメッセージが表示される。

```
Exception occurred while executing audit log insert.
```

このような場合には、ODBC データソースの代わりにテキストファイルにログを記録してください。

ポリシー ストアを共有するポリシー サーバが一貫して更新されない

問題の状況:

複数のポリシー サーバが一つのポリシー ストアを共有している場合、ポリシー ストア内のデータが同期されていない場合があります。同期問題は以下の条件下で発生する場合があります。

- ポリシー サーバ上のシステム時刻が異なっている。
- ネットワーク遅延。

たとえば、ポリシー サーバ A 上のシステム時刻が 10:00 で、ポリシー サーバ B 上のシステム時刻が 10:05 だとします。ポリシー サーバ A は 10:00 にポリシー ストアにデータを送信します。これらのイベントの方が早く発生したように見えるので、ポリシー サーバ B は 10:05 より前にタイムスタンプされたデータの変更を記録しません。

解決方法:

異なるシステム時刻またはネットワーク遅延問題に対応するには以下を実行します。

1. 以下の **DWORD** レジストリ設定を作成します。

```
SiteMinder¥CurrentVersion¥ObjectStore  
キー: ServerCommandTimeDelay
```

2. 時差に相当する秒数のキー値を設定します。たとえば、時差が 5 分の場合はキー値を 300 に設定します。

キャッシュ失敗タイムアウト

ポリシー サーバでは、以下のオブジェクトを削除した後にイベントの処理が失敗する場合があります。

- ポリシー
- ルール
- レルム
- ポリシー ドメイン

キャッシュ失敗タイムアウト機能はこの問題を扱います。

2 次キャッシュ強化が成功しないとき、ポリシー サーバはタイムアウト期間の後に停止します。以下のレジストリ キーを使用して、タイムアウト期間を指定します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder¥CurrentVersion¥ObjectStore¥CacheFailureTimeout
```

このキーの値は秒単位です。デフォルトはタイムアウトが発生しないことを示す 0 です。

ポリシー サーバがシャットダウンした後、smexec は次のプロセス イベントリクエストを即時に提起します。

キー ロールオーバー ログ メッセージ

ポリシー サーバが Web エージェントに対してキーのロールオーバー コマンドを発行した場合、それらのコマンドが正常に処理される場合もあれば、失敗する場合があります。この状況のトラブルシューティングを容易にするため、ポリシー サーバでは、以下の 3 種類のメッセージを SMPS.log に記録します。

[情報]キーのロールオーバーリクエストが手動で開始されました。

このメッセージは、管理者がキーのロールオーバーを手動で開始した場合に記録されます。

[情報]キーのロールオーバーリクエストがポリシー サーバによって自動的に開始されました。

このメッセージは、ポリシー サーバが自動的にキーのロールオーバーを開始した場合に記録されます。

[情報]キーの配布がポリシー サーバによって開始されました。

このメッセージは、キーのロールオーバー リクエストが自動的にまたは手動で開始された場合に記録されます。

キャッシュ更新ログ メッセージ

管理 UI またはコマンドライン インターフェースによって、キャッシュのフラッシュまたは更新を有効化および無効化することができます。トラブルシューティングを容易にするため、ポリシー サーバは、以下の 2 種類のメッセージを SMPS.log に記録します。

[情報]サーバ 'enablecacheupdates' コマンドを受信しました。

このメッセージは、管理 UI またはコマンドライン インターフェースのいずれかによって、キャッシュのフラッシュが有効にされた場合に記録されます。

[情報]サーバ 'disablecacheupdates' コマンドを受信しました。

このメッセージは、管理 UI またはコマンドライン インターフェースのいずれかによって、キャッシュのフラッシュが無効にされた場合に記録されます。

ポリシー サーバ管理コンソールを開くときの、イベントハンドラリスト設定に関する警告

問題の状況:

SiteMinder 12.52 SP1 へのアップグレード後、初めてポリシー サーバ管理コンソールにログインすると、イベントハンドラリストを XPSAudit に設定する必要があることを示す警告メッセージが表示されます。

解決方法:

SiteMinder 12.52 SP1 の場合、ポリシー サーバ管理コンソールを使用してカスタムイベントハンドラライブラリを追加することはできなくなりました。任意のカスタムイベントハンドラライブラリを追加するには、XPSConfig コマンドラインツールを使用します。

詳細情報:

[イベントハンドラライブラリの追加 \(P. 156\)](#)

SiteMinder ポリシー サーバの起動イベント ログ

問題の状況:

ポリシー サーバが起動中にクラッシュしました。ポリシー サーバがクラッシュする前にどのような SiteMinder 起動イベントが発生したのかを知るにはどうしたら良いですか。

解決方法:

ポリシー サーバが起動中にクラッシュした場合は、起動イベントのログが以下のファイルに格納されます。

`policy_server_home/audit/SmStartupEvents.audit`

LDAP ユーザ ディレクトリ上の VLV インデックスにより SiteMinder エージェント グループの検索が失敗する(174279)

問題の状況:

一部の LDAP ユーザ ディレクトリ上の Virtual List View (VLV) 実装の欠陥により、SiteMinder エージェント グループの検索が失敗する可能性があります。返されるエントリーはゼロで、「directory unwilling to perform」というエラーが発生します。

解決方法:

ここに記載されているような SiteMinder エージェント グループの検索の失敗が発生した場合は、ポリシー サーバ上で VLV ルックアップを無効にします。

以下の場所に、DWORD 型のレジストリ キー EnableVLV を作成します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\Siteminder\CurrentVersion\DS\LDAPProvider  
EnableVLV
```

LDAP ディレクトリ ルックアップに対する VLV を無効または有効にします。VLV を無効にするには、EnableVLV を 0 に設定します。VLV を有効にするには、EnableVLV を 1 に設定します。

値: 0 (無効) または 1 (有効)

デフォルト: 1 (有効)

STAR イシュー番号: 20397633-1

付録 C: ログファイルの説明

smaccesslog4

次の表では、認証および許可アクティビティを記録する smaccesslog4 に示されるロギングについて説明します。

フィールド名	説明	NULL/NOT NULL	フィールドタイプ
sm_timestamp	エントリがデータベースに作成された日時をマークします。	NOT NULL	DATE
sm_categoryid	ロギングのタイプを示す識別子です。次のいずれかの値をとります。 <ul style="list-style-type: none">■ 1 = Auth■ 2 = Az■ 3 = Admin■ 4 = Affiliate	NOT NULL	NUMBER(38)

フィールド名	説明	NULL/NOT NULL	フィールドタイプ
sm_eventid	<p>ログインを実行させた個別のイベントを示します。次のいずれかの値をとります。</p> <ul style="list-style-type: none"> ■ 1 = AuthAccept ■ 2 = AuthReject ■ 3 = AuthAttempt ■ 4 = AuthChallenge ■ 5 = AzAccept ■ 6 = AzReject ■ 7 = AdminLogin ■ 8 = AdminLogout ■ 9 = AdminReject ■ 10 = AuthLogout ■ 11 = ValidateAccept ■ 12 = ValidateReject ■ 13 = Visit 	NOT NULL	NUMBER(38)
sm_hostname	サーバが動作しているマシンです。		VARCHAR2(255)
sm_sessionid	このユーザのアクティビティのセッション識別子です。		VARCHAR2(255)
sm_username	このセッションで現在ログインしているユーザのユーザ名です。		VARCHAR2(512)
sm_agentname	ポリシーサーバと共に使用されているエージェントに関連付けられている名前です。		VARCHAR2(255)
sm_realmsname	ユーザが必要としているリソースが現在あるレルムです。		VARCHAR2(255)
sm_realmoid	レルムの固有識別子です。		VARCHAR2(64)
sm_clientip	保護されたリソースを利用しようとしているクライアントマシンのIPアドレスです。		VARCHAR2(255)

フィールド名	説明	NULL/NOT NULL	フィールドタイプ
sm_domainoid	ユーザがアクセスしているレムムおよびリソースが存在するドメインの固有識別子です。		VARCHAR2(64)
sm_authdirname	このフィールドは、レポート生成機能では使用されません。		VARCHAR2(255)
sm_authdirserver	このフィールドは、レポート生成機能では使用されません。		VARCHAR2(512)
sm_authdir-namespace	このフィールドは、レポート生成機能では使用されません。		VARCHAR2(255)
sm_resource	ユーザがリクエストしているリソース (Web ページなど) です。		VARCHAR2(512)
sm_action	HTTP アクション (Get、Post、および Put) です。		VARCHAR2(255)
sm_status	HTTP アクションに関するいくつかの説明文です。		VARCHAR2(1024)

フィールド名	説明	NULL/NOT NULL	フィールドタイプ
sm_reason	<p>ログインを実行する理由です。32000 ユーザが定義します。以下のとおりです。</p> <ul style="list-style-type: none"> ■ 0 = なし ■ 1 = PwMustChange ■ 2 = InvalidSession ■ 3 = RevokedSession ■ 4 = ExpiredSession ■ 5 = AuthLevelTooLow ■ 6 = UnknownUser ■ 7 = UserDisabled ■ 8 = InvalidSessionId ■ 9 = InvalidSessionIp ■ 10 = CertificateRevoked ■ 11 = CRLOutOfDate ■ 12 = CertRevokedKeyCompromised ■ 13 = CertRevokedAffiliationChange ■ 14 = CertOnHold ■ 15 = TokenCardChallenge ■ 16 = ImpersonatedUserNotInDi ■ 17 = Anonymous ■ 18 = PwWillExpire ■ 19 = PwExpired ■ 20 = ImmedPWChangeRequired ■ 21 = PWChangeFailed ■ 22 = BadPWChange ■ 23 = PWChangeAccepted ■ 24 = ExcessiveFailedLoginAttempts ■ 25 = AccountInactivity ■ 26 = NoRedirectConfigured ■ 27 = ErrorMessageIsRedirect 	NOT NULL	NUMBER(38)

フィールド名	説明	NULL/NOT NULL	フィールドタイプ
sm_reason (続き)	<ul style="list-style-type: none"> ■ 28 = Tokencode ■ 29 = New_PIN_Select ■ 30 = New_PIN_Sys_Tokencode ■ 31 = New_User_PIN_Tokencode ■ 32 = New_PIN_Accepted ■ 33 = Guest ■ 34 = PWSelfChange ■ 35 = ServerException ■ 36 = UnknownScheme ■ 37 = UnsupportedScheme ■ 38 = Misconfigured ■ 39 = BufferOverflow 		
sm_transactionid	このフィールドは、レポート生成機能では使用されません。		VARCHAR2(255)
sm_domainname	ユーザがアクセスしているレルムおよびリソースが存在するドメインの名前です。	NULL	VARCHAR2(255)
sm_impersonator-name	別名セッションで別名ユーザとして動作している管理者のログイン名です。	NULL	VARCHAR2(512)
sm_impersonator-dirname	別名ユーザが含まれているディレクトリオブジェクトの名前です。	NULL	VARCHAR2(255)

smobjlog4

次の表では、管理イベントを記録する smobjlog4 に示されるロギングについて説明します。

フィールド名	説明	NULL/NOT NULL	タイプ
sm_timestamp	エントリがデータベースに作成された日時を示します。	NOT NULL	DATE

フィールド名	説明	NULL/NOT NULL	タイプ
sm_categoryid	<p>ログインのタイプを示す識別子です。次のいずれかの値をとります。</p> <ul style="list-style-type: none"> ■ 1 = Auth ■ 2 = Agent ■ 3 = AgentGroup ■ 4 = Domain ■ 5 = Policy ■ 6 = PolicyLink ■ 7 = Realm ■ 8 = Response ■ 9 = ResponseAttr ■ 10 = ResponseGroup ■ 11 = Root ■ 12 = Rule ■ 13 = RuleGroup ■ 14 = Scheme ■ 15 = UserDirectory ■ 16 = UserPolicy ■ 17 = Vendor ■ 18 = VendorAttr ■ 19 = Admin ■ 20 = AuthAzMap ■ 21 = CertMap ■ 22 = ODBCQuery ■ 23 = SelfReg ■ 24 = PasswordPolicy ■ 25 = KeyManagement ■ 26 = AgentKey ■ 27 = ManagementCommand ■ 28 = RootConfig 	NOT NULL	NUMBER(38)

フィールド名	説明	NULL/NOT NULL	タイプ
sm_categoryid (続き)	<ul style="list-style-type: none"> ■ 29 = Variable ■ 30 = VariableType ■ 31 = ActiveExpr ■ 32 = PropertyCollection ■ 33 = PropertySection ■ 34 = Property ■ 35 = TaggedString ■ 36 = TrustedHost ■ 37 = SharedSecretPolicy 	NOT NULL	NUMBER(38)
sm_eventid	<p>ログインを実行させた個別のイベントを示します。次のいずれかの値をとります。</p> <ul style="list-style-type: none"> ■ 1 = Create ■ 2 = Update ■ 3 = UpdateField ■ 4 = Delete ■ 5 = Login ■ 6 = Logout ■ 7 = LoginReject ■ 8 = FlushAll ■ 9 = FlushUser ■ 10 = FlushUsers ■ 11 = FlushRealms ■ 12 = ChangeDynamicKeys ■ 13 = ChangePersistentKey ■ 14 = ChangeDisabledUserState ■ 15 = ChangeUserPassword ■ 16 = FailedLoginAttemptsCount ■ 17 = ChangeSessionKey 	NOT NULL	NUMBER(38)

フィールド名	説明	NULL/NOT NULL	タイプ
sm_hostname	このフィールドは、管理ロギングのレポート生成機能では使用されません。		VARCHAR2(255)
sm_sessionid	このユーザのアクティビティのセッション識別子です。		VARCHAR2(255)
sm_username	この管理者のユーザ名です。		VARCHAR2(512)
sm_objname	管理者内のアクセスされているオブジェクトです。		VARCHAR2(512)
sm_objjoid	管理者内のアクセスされているオブジェクトの固有識別子です。このフィールドは、レポート生成機能では使用されません。		VARCHAR2(64)
sm_fielddesc	管理者のアクションに関するいくつかの説明文です。		VARCHAR2(1024)
sm_domainoid	管理者内の、変更されているオブジェクトが含まれているドメインの固有識別子です。このフィールドは、レポート生成機能では使用されません。		VARCHAR2(64)
sm_status	HTTP アクションに関するいくつかの説明文です。このフィールドは、レポート生成機能では使用されません。		VARCHAR2(1024)

付録 D: 診断情報の発行

診断情報の概要

ポリシー サーバには、SiteMinder 環境に関する診断情報を発行するためのコマンドライン ツールが含まれています。このツールを使用すると、ポリシー サーバ、ポリシー ストア、ユーザ ディレクトリ、エージェント、およびカスタム モジュールに関する情報を発行できます。

コマンドライン インターフェースを使用します。

ポリシー サーバには、情報を発行するための、コマンドラインで実行するコマンドが用意されています。このコマンドは、`installation_dir/siteminder/bin` ディレクトリにあります。

情報を発行するには、`smpolicysrv` コマンドを、`-publish` スイッチを付けて使用します。例：

```
smpolicysrv -publish <optional file_name>
```

注: Windows システムでは、リモート デスクトップまたはターミナル サービス ウィンドウから `smpolicysrv` コマンドを実行しないでください。`smpolicysrv` コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは [ターミナル サービス] ウィンドウから `smpolicysrv` プロセスを実行した場合には機能しません。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

発行される情報の保存場所の指定

発行される情報は、指定したファイルに XML 形式で書き込まれます。指定したファイル名は以下のレジストリ キーに保存されます。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
Publish
```

このキーは、Windows システムではシステム レジストリにあり、UNIX システムでは `install_dir/registry/sm.registry` ファイルにあります。レジストリ設定のデフォルト値は以下のとおりです。

```
policy_server_install_dir>%log%\smpublish.xml
```

コマンドラインから `smpolicysrv -publish` を実行し、パスとファイル名を指定しない場合、発行される XML ファイルの保存場所はレジストリ設定の値によって決まります。

注: Windows システムでは、リモートデスクトップまたはターミナル サービス ウィンドウから `smpolicysrv` コマンドを実行しないでください。`smpolicysrv` コマンドはプロセス間通信に依存します。この通信は、リモートデスクトップまたは [ターミナル サービス] ウィンドウから `smpolicysrv` プロセスを実行した場合には機能しません。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

XML ファイルの保存場所を指定し、XML ファイル内に出力を生成する方法

1. コマンドラインで、次のディレクトリに移動します。

```
installation_dir/siteminder/bin
```

2. 以下のコマンドを入力します。

```
smpolicysrv -publish path_and_file_name
```

Windows 環境では、たとえば、次のように入力します。

```
smpolicysrv -publish c:%netegrity%siteminder%published-data.txt
```

UNIX 環境では、たとえば、次のように入力します。

```
smpolicysrv -publish /netegrity/siteminder/published-data.txt
```

ポリシー サーバにより、指定した場所に XML 出力が生成され、この場所に一致するように

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥
```

```
SiteMinder¥CurrentVersion¥Publish レジストリ キーの値が更新されます。
```

データの発行

このセクションでは、次のコンポーネントに関して発行できる情報の概要を示します。

- ポリシー サーバ
- ポリシー/キーストア
- ユーザ ディレクトリ
- エージェント
- カスタムモジュール

発行されるポリシー サーバ情報

ポリシー サーバ情報には、サーバ名、プラットフォーム、設定、およびサーババージョン情報が含まれます。さらに、ポリシー サーバの設定に使用されている任意のレジストリ設定を発行することもできます。

発行されるポリシー サーバ情報には、次のものが含まれます。

- 基本情報
 - 名前
 - バージョン

- プラットフォーム
- スレッドプールの統計情報
- サーバ設定 (ポリシー サーバ管理コンソールで設定されている値)
 - キー管理
 - ジャーナル
 - キャッシュ
 - イベントハンドラー
 - 追跡ロギング
 - 監査ログ

発行されるポリシー サーバ XML 出力の形式

以下の例は、ポリシー サーバ情報がどのようにフォーマットされるかを示しています。

```
<SERVER>
  < SHORT_NAME>    smpolicysrv </SHORT_NAME>
  <FULL_NAME>     SiteMinder Policy Server </FULL_NAME>
  <PRODUCT_NAME> SiteMinder(tm) </PRODUCT_NAME>
  <VERSION>      6.0 </VERSION>
  <UPDATE>       01 </UPDATE>
  <LABEL>        283 </LABEL>
  <PLATFORM>     Windows (Build 3790)
</PLATFORM>
  <SERVER_PORT>   44442 </SERVER_PORT>
  <RADIUS_PORT>  0 </RADIUS_PORT>
  <THREADPOOL>
    <MSG_TOTALS>  15011 </MSG_TOTALS>
    <MSG_DEPTH>   2 </MSG_DEPTH>
    <THREADS_LIMIT> 8 </THREADS_LIMIT>
    <THREADS_MAX> 3 </THREADS_MAX>
    <THREADS_CURRENT> 3 </THREADS_CURRENT>
  </THREADPOOL>
  <CRYPTO> 128 </CRYPTO>
  <KEYMGT>
    <GENERATION> enabled </GENERATION>
    <UPDATE>    disabled </UPDATE>
  </KEYMGT>
  <JOURNAL>
    <REFRESH> 60 </REFRESH>
    <FLUSH>   60 </FLUSH>
  </JOURNAL>
  <PSCACHE>
    <STATE>      enabled </STATE>
    <PRELOAD>   enabled </PRELOAD>
  </PSCACHE>
  <USERAZCACHE>
    <STATE>     enabled </STATE>
    <MAX>       10 </MAX>
    <LIFETIME> 3600 </LIFETIME>
  </USERAZCACHE>
</SERVER>
```

以下の表に、発行されるポリシー サーバ情報を示します。

タグ	内容	説明	親タグ	必須
SERVER	エレメント	サーバに関する情報であることを示します	SMPUBLSIH	必須
SHORT_NAME	テキスト	サーバの略称	SERVER	必須
FULL_NAME	テキスト	稼働しているサーバのフルネーム	SERVER	必須
PRODUCT_NAME	テキスト	製品名	SERVER	必須
VERSION	テキスト	サーバのバージョン	SERVER	必須
UPDATE	テキスト	サービスパックのバージョン	SERVER	必須
LABEL	テキスト	ビルドまたは CR 番号	SERVER	必須
PLATFORM	テキスト	OS プラットフォーム識別データ	SERVER	必須
THREAD_POOL	エレメント	スレッドプールに関する情報	SERVER	必須
MSG_TOTAL	整数	処理されたスレッドプールメッセージの数	THREAD_POOL	必須
MSG_DEPTH	整数	スレッドプール内のメッセージの最大数	THREAD_POOL	必須
THREADS_LIMIT	整数	スレッドの最大数	THREAD_POOL	必須
THREADS_MAX	整数	使用されているスレッドの最大数	THREAD_POOL	必須
THREADS_CURRENT	整数	現在使用されているスレッドの数	THREAD_POOL	必須
PSCACHE	エレメント	ポリシー サーバ キャッシュ設定に関する情報であることを示します	SERVER	必須
PRELOAD	テキスト	有効か無効かを示します	PSCACHE	必須

タグ	内容	説明	親タグ	必須
JOURNAL	なし	ジャーナル設定（リフレッシュ間隔とクリア間隔）を示します	SERVER	必須
FLUSH	整数	クリア間隔	JOURNAL	必須
REFRESH	整数	リフレッシュ間隔	JOURNAL	必須
KEYMGT	なし	キー管理設定を示します (Generation: 自動キー生成が有効になっているかどうか) (Update: エージェントキーの自動更新が有効になっているかどうか)	SERVER	必須
GENERATION	enabled または disabled	自動キー生成が有効になっているかどうかを示します	KEYMGT	必須
UPDATE	enabled または disabled	エージェントキーの自動更新が有効になっているかどうかを示します	KEYMGT	必須
USERAZCACHE	エレメント	ユーザ許可キャッシュ設定に関する情報であることを示します	SERVER	必須
MAX	整数	キャッシュエントリの最大数	USERAZCACHE	必須
LIFETIME	整数	キャッシュされたオブジェクトの有効期間	USERAZCACHE	必須
PORT	整数	ポート番号	SERVER	必須
RADIUS_PORT	整数	RADIUS ポート番号 (有効になっている場合)	SERVER	必須
STATE	テキスト、enabled または disabled	あるものが有効か無効かを示します	さまざまなタグ	両方

発行されるオブジェクトストア情報

ポリシーサーバは、以下のタイプのオブジェクトストアに情報を格納できます。

- ポリシーストア
- キーストア
- 監査ログストア
- セッションストア

発行されるオブジェクトストア情報には、使用されているオブジェクトストアのタイプ、バックエンドデータベース情報、設定情報、および接続情報が含まれます。

発行されるポリシー/キーストア XML 出力の形式

以下の例は、ポリシー/キーストア情報がどのようにフォーマットされるかを示します。

```
<POLICY_STORE>

  <DATASTORE>
    <NAME> Policy Store </NAME>
    <USE_DEFAULT_STORE> false </USE_DEFAULT_STORE>
    <LOADED> true </LOADED>
    <SERVER_LIST>
      <CONNECTION_INFO>
        <TYPE> ODBC</TYPE>
        <SERVICE_NAME> sm </SERVICE_NAME>
        <USER_NAME> sa </USER_NAME>
        <DBMS_NAME> Microsoft SQL Server <SQL/DBMS_NAME>
        <DRIVER_NAME> Microsoft SQL Server <SQL/DRIVER_NAME>
        <DBMS_VERSION> 08.00.0760 </DBMS_VERSION>
      </CONNECTION_INFO>
    </SERVER_LIST>
  </DATASTORE>

  <DATASTORE>
    <NAME> Key Store </NAME>
    <USE_DEFAULT_STORE> true </USE_DEFAULT_STORE>
    <LOADED> true </LOADED>
  </DATASTORE>

  <DATASTORE>
    <NAME> Audit Log Store </NAME>
    <USE_DEFAULT_STORE> true </USE_DEFAULT_STORE>
    <LOADED> true </LOADED>
  </DATASTORE>

  <DATASTORE>
    <NAME> Session Server Store </NAME>
    <USE_DEFAULT_STORE> false </USE_DEFAULT_STORE>
    <LOADED> false </LOADED>
  </DATASTORE>

</POLICY_STORE>
```

以下の表に、発行されるポリシー/キー ストア情報を示します。

タグ	内容	説明	親タグ	必須
POLICY_STORE	エレメント	すべてのデータストアに関する情報であることを示します	SMPUBLISH	必須
DATASTORE	エレメント	<p>特定のオブジェクトストアに関する情報であることを示します。</p> <ul style="list-style-type: none"> ■ TYPE は、データ ストアのタイプを示します。 ■ USE_DEFAULT_STORE は、そのタイプのデフォルトオブジェクトストアが使用されていることを示します。 ■ LOADED は、そのタイプがロードされているかどうかを示します。 	POLICY_STORE	必須
NAME	テキスト	データストアの名前/タイプ	DATASTORE	必須
USE_DEFAULT_STORE	テキスト	ストレージがデフォルトの「ポリシー ストア」内にあるかどうか (true または false) を示します	DATASTORE	必須
LOADED	テキスト	データ ストアがロードされて、初期化されているかどうか (true または false) を示します	DATASTORE	必須
TYPE	テキスト	ポリシー ストアのタイプ (ODBC または LDAP)	DATASTORE	必須
SERVER_LIST	エレメント	データストア (ODBC) に使用されるフェイルオーバー サーバのリスト	DATASTORE	任意
CONNECTION_INFO	エレメント	サーバ接続のタイプ	SERVER_LIST	任意

タグ	内容	説明	親タグ	必須
DRIVER_NAME	テキスト	ODBC ドライバの名前	CONNECTION	任意
IP	テキスト	IP アドレス	DATASTORE	任意
LDAP_VERSION	テキスト	LDAP のバージョン	DATASTORE	任意
API_VERSION	テキスト	LDAP API のバージョン	DATASTORE	任意
PROTOCOL_VERSION	テキスト	LDAP プロトコルのバージョン	DATASTORE	任意
API_VENDOR	テキスト	API のベンダー	DATASTORE	任意
VENDOR_VERSION	テキスト	ベンダーのバージョン	DATASTORE	任意

発行されるユーザ ディレクトリ情報

ポリシー サーバによってロードおよびアクセスされたユーザ ディレクトリごとに、以下の情報を発行できます。

- 設定
- 接続
- バージョン

発行されるユーザ ディレクトリ XML 出力の形式

ユーザ ディレクトリ情報は、以下の例のような形式で発行されます。

注: 発行される情報は、ユーザ ディレクトリのタイプによって異なります。

```
< USER_DIRECTORIES>

  <DIRECTORY_STORE >
    <TYPE> ODBC </TYPE>
    <NAME> sql5.5sample </NAME>
    <MAX_CONNECTIONS> 15 </MAX_CONNECTIONS>
    <SERVER_LIST>
      <CONNECTION_INFO>
        <TYPE> ODBC</TYPE>
        <SERVICE_NAME> sql5.5sample </SERVICE_NAME>
        <USER_NAME> sa </USER_NAME>
        <DBMS_NAME> Microsoft SQL Server <SQL/DBMS_NAME>
        <DRIVER_NAME> Microsoft SQL Server <SQL/DRIVER_NAME>
        <DBMS_VERSION> 08.00.0760 </DBMS_VERSION>
      </CONNECTION_INFO>
    </SERVER_LIST>
  </DIRECTORY_STORE >
  <DIRECTORY_STORE>
    <TYPE> LDAP: </TYPE>
    <NAME> LDAPsample </NAME>
    <FAILOVER_LIST> 172.26.14.101:12002 </FAILOVER_LIST>
    <VENDOR_NAME> Netscape-Directory/4.12 B00.193.0237
    </VENDOR_NAME>
    <SECURE_CONNECTION> disabled </SECURE_CONNECTION>
    <CREDENTIALS> required </CREDENTIALS>
    <CONNECTION_INFO>
      <PORT_NUMBER> 12002 </PORT_NUMBER>
      <DIR_CONNECTION> 172.26.14.101:12002 </DIR_CONNECTION>
      <USER_CONNECTION> 172.26.14.101:12002 </USER_CONNECTION>
    </CONNECTION_INFO>
    <LDAP_VERSION> 1 </LDAP_VERSION>
    <API_VERSION> 2005 </API_VERSION>
    <PROTOCOL_VERSION> 3 </PROTOCOL_VERSION>
    <API_VENDOR> mozilla.org </API_VENDOR>
    <VENDOR_VERSION> 500 </VENDOR_VERSION>
  </DIRECTORY_STORE>
</USER_DIRECTORIES>
```

以下の表に、発行されるユーザディレクトリ情報を示します。

タグ	内容	説明	親タグ	必須
USER_DIRECTORIES	エレメント	ロードされている一連のディレクトリストアに関する情報であることを示します	SMPUBLISH	必須
DIRECTORY_STORE	エレメント	特定のディレクトリストアに関する情報であることを示します	USER_DIRECTORIES	任意
TYPE	テキスト	ディレクトリストアのタイプ	DIRECTORY_STORE	必須
NAME	テキスト	定義されているディレクトリストアの名前	DIRECTORY_STORE	必須
MAX_CONNECTIONS	整数	定義されている接続の最大数	DIRECTORY_STORE	任意
SERVER_LIST	エレメント	一連のサーバ (ODBC)	DIRECTORY_STORE	任意
FAILOVER_LIST	テキスト			

発行されるエージェント情報

発行されるエージェント情報は、現在ポリシーサーバに接続されているエージェント (IP アドレス、名前など) を示します。

発行されるエージェント XML 出力の形式

エージェント情報は、次の例のような形式で発行されます。

```
< AGENT_CONNECTION_MANAGER>
  <CURRENT>      4 </CURRENT>
  <MAX>          4 </MAX>
  <DROPPED>      0 </DROPPED>
  <IDLE_TIMEOUT> 0 </IDLE_TIMEOUT>
  <ACCEPT_TIMEOUT> 10 </ACCEPT_TIMEOUT>

  <AGENT_CONNECTION>
    <NAME> agent1 </NAME>
    <IP> 172.26.6.43 </IP>
    <API_VERSION> 1024 </API_VERSION>
    <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
  </AGENT_CONNECTION>
  <AGENT_CONNECTION>
    <NAME> agent1 </NAME>
    <IP> 172.26.6.43 </IP>
    <API_VERSION> 1024 </API_VERSION>
    <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
  </AGENT_CONNECTION>
  <AGENT_CONNECTION>
    <NAME> agent1 </NAME>
    <IP> 172.26.6.43 </IP>
    <API_VERSION> 1024 </API_VERSION>
    <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
  </AGENT_CONNECTION>
  <AGENT_CONNECTION>
    <NAME> 940c0728-d405-489c-9a0e-b2f831f78c56 </NAME>
    <IP> 172.26.6.43 </IP>
    <API_VERSION> 1482282902 </API_VERSION>
    <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
  </AGENT_CONNECTION>
</AGENT_CONNECTION_MANAGER>
```

注: エージェント接続情報は <AGENT_CONNECTION_MANAGER> タグ内に含まれています。

以下の表に、発行されるエージェント情報を示します。

タグ	内容	説明	親タグ	必須
AGENT_CONNECTION- _MANAGER	エレメン ト	エージェント接続に関する 情報であることを示します	SM_PUBLISH	必須
CURRENT	整数	現在の接続数	AGENT_CONNECTION- _MANAGER	必須
MAX	整数	接続の最大数	AGENT_CONNECTION- _MANAGER	必須
DROPPED	整数	接続の最大数	AGENT_CONNECTION- _MANAGER	必須
IDLE_TIMEOUT	整数	アイドル接続がタイムアウト するまでの時間	AGENT_CONNECTION- _MANAGER	必須
ACCEPT_TIMEOUT	整数	接続試行がタイムアウト するまでの時間	AGENT_CONNECTION- _MANAGER	必須
AGENT_CONNECTION	エレメン ト	アクティブなエージェント 接続に関する情報であるこ とを示します	AGENT_CONNECTION- _MANAGER	任意
IP	テキスト	エージェントの IP アドレ ス	AGENT_CONNECTION	必須
API_VERSION	整数	接続しているエージェント によって使用 されている API のバージョ ン	AGENT_CONNECTION	必須
NAME	テキスト	エージェントの名前	AGENT_CONNECTION	必須
LAST_MESSAGE_TIME	整数	エージェントから最後に メッセージが送信されてか らの経過時間	AGENT_CONNECTION	必須
AGENT_CONNECTION- _MANAGER	エレメン ト	エージェント接続に関する 情報であることを示します	SM_PUBLISH	必須

発行されるカスタム モジュール情報

カスタム モジュールは、既存のポリシー サーバの機能を拡張するために作成できる DLL またはライブラリです。これには、いくつかのタイプ（イベントハンドラ、認証モジュール、許可モジュール、ディレクトリモジュール、トンネルモジュール）があります。認証モジュールは、一般に、カスタム認証方式と呼ばれ、許可モジュールは、アクティブポリシーと呼ばれます。トンネルモジュールは、エージェントとの安全な接続を定義するために使用されます。イベントモジュールは、イベント通知を受信するためのメカニズムを提供します。ポリシーサーバによってロードされているカスタムモジュールを示す情報を発行することができます。カスタムモジュールの各タイプは、独自の XML タグで定義されます。

発行されるカスタム モジュール XML 出力の形式

以下の表に、発行されるカスタム モジュール情報を示します。

タグ	内容	説明	親タグ	必須
EVENT_LIB	エレメント	イベント API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意
AUTH_LIB	エレメント	認証 API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意
DS_LIB	エレメント	ディレクトリ API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意
TUNNEL_LIB	エレメント	トンネル API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意
AZ_LIB	エレメント	許可 API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意

次のタグは、すべてのタイプのカスタムモジュールに共通です。

タグ	内容	説明	親タグ	必須
FULL_NAME	テキスト	ライブラリまたは DLL のパスを含む完全な名前		必須
CUSTOM_INFO	テキスト	カスタムライブラリによって提供される情報		任意
LIB_NAME	テキスト	ライブラリまたは DLL の名前		任意
VERSION	整数	サポートされている API のバージョン		任意

次のタグは、特定タイプのモジュール専用です。

タグ	内容	説明	API タイプ	必須
ACTIVE_FUNCTION	テキスト	アクティブな式としてコールできるようにロードされている関数の名前	許可 API	任意

付録 E: エラー メッセージ

認証

メッセージ	関数	説明
1) 検証のため新しい PIN を ACE/Server に送信していません	SmLoginLogoutMessage::Send-NewPinForValidation1	情報のみ。 ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
2) 検証 %1s のため新しい PIN を ACE/Server に送信できませんでした	SmLoginLogoutMessage::Send-NewPinForValidation2	情報のみ。 ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
ACE Server --- PIN ポリシーを取得できませんでした	SmLoginLogoutMessage::Sm-AuthorAceGetPinPoliciesFail	SecurID 認証方式において、SecurID/ACE API コールを使用して ACE サーバのバックエンド PIN ポリシーを取得できない場合、このメッセージが表示されます。
ACE Server --- PIN パラメータを取得できませんでした	SmLoginLogoutMessage::Sm-AuthorHtmlPinParamFail	SecurID 認証方式において、SecurID/ACE API コールを使用して ACE の PIN パラメータを取得できない場合、このメッセージが表示されます。
ACE の状態が ACM_NEXT_CODE_REQUIRED ではありません。状態 = %1i	SmLoginLogoutMessage::Ace-NextTokenCodeState	HTML SecurID 認証方式において、ユーザのトークンコード値の期限が切れているため、新しい認証を試行する前に次のコードを待つ必要がある場合、このメッセージが表示されます。
ACE/Server - 新しい PIN が必要です。 isselectable PIN 属性について AceAPI によってあいまいな値が返されました。 ACE 認証を完了できません	SmLoginLogoutMessage::Sm-AuthorHtmlPinRequired	情報のみ。 ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。

メッセージ	関数	説明
ACE/Server - 新しい PIN が必要です。システム PIN を選択または承諾することができます。 Sm_AuthApi_Reject、 Sm_Api_Reason_New_PIN_Select を返します。	SmLoginLogoutMessage::Sm-Ace HtmlChooseNewOrSysPin	SecurID 認証方式において、ACE ユーザが自分で選択した PIN またはシステムによって生成された PIN を使用するように設定されている場合、このメッセージが表示されます。
ACE/Server - 新しい PIN が必要です。システム PIN を承諾する必要があります。 Sm_Api_Reason_New_PIN_Sys_Tokencode が返されました	SmLoginLogoutMessage::Sm-Ace HtmlCannotChoosePin	SecurID 認証方式において、ACE ユーザが常にシステムによって生成された PIN を使用するように設定されている場合、このメッセージが表示されます。
ACE/Server - 新しい PIN が必要です。PIN を選択する必要があります。 Sm_AuthApi_Reject、 Sm_Api_Reason_New_User_PIN_Tokencode を返します	SmLoginLogoutMessage::Sm-Ace HtmlChooseNewPin	SecurID 認証方式において、ACE ユーザが常に自分で選択した PIN を使用するように設定されている場合、このメッセージが表示されます。
ACE/Server : ACM_NEW_PIN_ACCEPTED は aceRetVal%1i で失敗しました	SmLoginLogoutMessage::Ace-Server NewPinAcceptedFailed	HTML SecurID 認証方式で使用されます。新しいユーザ PIN が ACE サーバによって承諾されなかった場合に表示されます。
ACE/Server : ACM_NEW_PIN_ACCEPTED は aceRetVal%1i、 ACE ステータス %2i で失敗しました	SmLoginLogoutMessage::Not-WithinAceServer NewPinAccepted-Failed	HTML SecurID 認証方式で使用されます。新しいユーザ PIN が ACE サーバによって承諾されなかった場合に表示されます。
ACE/Server : ACM_NEW_PIN_ACCEPTED に失敗しました	SmLoginLogoutMessage::NewPinAcceptedFailed	HTML SecurID 認証方式で使用されます。新しいユーザ PIN が ACE サーバによって承諾されなかった場合に表示されます。
ACE/Server によって AceCheck アクセスが拒否されました	SmLoginLogoutMessage::Ace-Check AccessDenied	SecurID 認証方式において、認証リクエストが ACE サーバによって拒否された場合、このメッセージが表示されます。

メッセージ	関数	説明
AceCheck が処理されません。aceRetVal = %1i	SmLoginLogoutMessage::Ace-CheckNotProcessed	SecurID 認証方式において、ACE/SecurID API を使用して ACE 認証プロセスを完了できない場合、このエラーメッセージが表示されます。
AceCheck が ACM_NEW_PIN_REQUIRED ではなく %1i を返しました	SmLoginLogoutMessage::Acm-NewPinRequiredFail	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
AceCheck が ACM_NEW_PIN_REQUIRED ではなく %1i を返しました	SmLoginLogoutMessage::Invalid-ReturnAceCheckNewPin	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
AceCheck : 拒否されました ---aceRetVal = %1i	SmLoginLogoutMessage::Sm-AuthAceCheck-Denial	SecurID 認証方式において、認証リクエストが ACE サーバによって拒否された場合、このメッセージが表示されます。
AceGetMaxPinLen の実行に失敗しました	#REF!	HTML SecurID 認証方式で使用されます。ACE サーバで許可されているユーザ PIN の最大長を取得できなかった場合、このメッセージが表示されます。
AceSendPin の実行に失敗しました	SmLoginLogoutMessage::Ace-SendPinFailed	HTML SecurID 認証方式において、ACE/SecurID API を使用してユーザ PIN を RSA ACE サーバに送信できなかった場合、このエラーメッセージが表示されます。認証方式によってリクエストは拒否されます。
AceServer - PIN を選択できません	SmLoginLogoutMessage::Ace-ServerCannotChoosePin	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。

メッセージ	関数	説明
AceServer - PIN を選択する必要があります	SmLoginLogoutMessage::Ace-ServerMustChoosePin	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
AceServer :: Sm_Api_Reason_New_PIN_Select	SmLoginLogoutMessage::Sm-ApiNewPinSelectReason	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
AceServer が Sm_Api_Reason_New_PIN_Accepted Accepted	SmLoginLogoutMessage::Sm-ApiSuccessReason	HTML SecurID 認証方式で使用されます。ユーザ PIN がユーザによって正常に変更された場合、このメッセージが表示されます。
AceServer が Sm_Api_Reason_New_PIN_Accepted を返しますが、不成功のメッセージが表示される可能性があります。ターゲットが不明です。	SmLoginLogoutMessage::Sm-ApiRejectReasonMessage	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
AceSetPasscode = %1s	SmLoginLogoutMessage::Sm-AuthorAceSetPassCode	SecurID 認証方式において、ACE 認証のパスコードを ACE/SecurID API を使用して登録しようとしている場合、このメッセージが表示されます。
AceSetPasscode は aceRetVal = %1i で失敗しました	SmLoginLogoutMessage::Ace-SetPasscodeFailed	SecurID 認証方式において、ACE 認証のパスコードを ACE/SecurID API を使用して登録できなかった場合、このエラーメッセージが表示されます。認証方式によってリクエストは拒否されます。

メッセージ	関数	説明
AceSetPin の実行に失敗しました	SmLoginLogoutMessage::Ace-SetPinFailed	HTML SecurID 認証方式において、ACE/SecurID API を使用してユーザ PIN を設定できなかった場合、このエラーメッセージが表示されます。認証方式によってリクエストは拒否されます。
AceSetSelectionCode DECRYPT = %1s	SmLoginLogoutMessage::SelectionCodeDecrypt	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
AceSetUsername は aceRetVal = %1i で失敗しました	SmLoginLogoutMessage::Ace-SetUserNameFailed	SecurID 認証方式において、ACE 認証のユーザ名を ACE/SecurID API を使用して登録できなかった場合、このメッセージが表示されず。認証方式によってリクエストは拒否されます。
AddCurrentPWToHistory - パスワード履歴情報を設定できません	SmLoginLogoutMessage::ErrorSettingPassword-History	最新のパスワードのリストに現在のパスワードを追加できませんでした。
AuthenticateUserDir - ユーザ BLOB データを更新できません	SmLoginLogoutMessage::Blob-UpdateFailed	認証プロセス中にパスワード BLOB データを更新できませんでした。
AceAlphanumeric を取得できません	SmLoginLogoutMessage::Get-AceAlphanumericFail	ACE クライアントライブラリ内にメソッドが見つかりませんでした。
AceCancelPin を取得できません	SmLoginLogoutMessage::Get-AceCancelPinFail	ACE クライアントライブラリ内にメソッドが見つかりませんでした。
AceCheck を取得できません	SmLoginLogoutMessage::Get-AceCheckFail	ACE クライアントライブラリ内にメソッドが見つかりませんでした。
AceClientCheck を取得できません	SmLoginLogoutMessage::Get-AceClientCheckFail	ACE クライアントライブラリ内にメソッドが見つかりませんでした。

メッセージ	関数	説明
AceClose を取得できません	SmLoginLogoutMessage::Get-AceCloseFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetAuthenticationStatus を取得できません	SmLoginLogoutMessage::Ace-GetAuthenticationStatusFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetMaxPinLen を取得できません	SmLoginLogoutMessage::Null-AceGetMaxPinLen	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetMinPinLen を取得できません	SmLoginLogoutMessage::Null-AceGetMinPinLen	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetPinParams を取得できません	SmLoginLogoutMessage::Get-AcePinParamFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetShell を取得できません	SmLoginLogoutMessage::Ace-GetShellFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetSystemPin を取得できません	SmLoginLogoutMessage::Ace-GetSystemPinFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetTime を取得できません	SmLoginLogoutMessage::Ace-GetTimeFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetUserData を取得できません	SmLoginLogoutMessage::Ace-GetUserDataFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetUserSelectable を取得できません	SmLoginLogoutMessage::Ace-GetUserSelectable-Fail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceInit を取得できません	SmLoginLogoutMessage::Get-AceInitFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。

メッセージ	関数	説明
AceInitialize を取得できません	SmLoginLogoutMessage::Ace-InitializeFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceLock を取得できません	SmLoginLogoutMessage::Ace-LockFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSendNextPasscode を取得できません	SmLoginLogoutMessage::Ace-SendNextPasscodeFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSendPin を取得できません	SmLoginLogoutMessage::Null-AceSendPin	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSetNextPasscode を取得できません	SmLoginLogoutMessage::Ace-SetNextPasscodeFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSetPasscode を取得できません	SmLoginLogoutMessage::Ace-SetPasscodeFail	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
AceSetPin を取得できません	SmLoginLogoutMessage::Null-AceSetPin	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSetUserClientAddress を取得できません	SmLoginLogoutMessage::Ace-SetUserClientAddressFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSetUsername を取得できません	SmLoginLogoutMessage::Ace-SetUsernameFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
aceInt.dll をロードできません	SmLoginLogoutMessage::Ace-IntDllLoadFail	ACE クライアント ライブラリをロードできませんでした。

メッセージ	関数	説明
パスワードメッセージから新しいパスワードを取得できません	SmLoginLogoutMessage::New-PasswordRetrieveFail	ログインリクエストの処理中、パスワードを新しいものと古いものに分割しているとき、新しいパスワードを取得できませんでした。
パスワードメッセージから古いパスワードを取得できません	SmLoginLogoutMessage::Old-PasswordRetrieveFail	ログインリクエストの処理中、パスワードを新しいものと古いものに分割しているとき、古いパスワードを取得できませんでした。
パスワードメッセージからトークンを取得できません	SmLoginLogoutMessage::Token-RetrieveFail	ログインリクエストの処理中、パスワードを新しいものと古いものに分割しているとき、パスワードトークンを取得できませんでした。
ChangePassword - プロバイダを介してパスワードを変更できません	SmLoginLogoutMessage::Pwd-ChangeFailViaProvider	パスワード変更リクエストの処理中、ユーザディレクトリ内のパスワードを変更できませんでした。
ChangePassword - 新しいパスワードを検証できません	SmLoginLogout-Message::ChangePwdValidation-Fail	パスワード変更リクエストの処理中、ユーザディレクトリ内のパスワードを検証できませんでした。
CheckPasswordPolicies - パスワードポリシーの誤設定のため、認証ステータスが「失敗」に変わりました	SmLoginLogout-Message::CheckPwdFailCause-Misconfig	パスワードポリシーの確認中、ログイン試行を検証できませんでした。パスワードポリシーが誤設定されている可能性があります。
%1s を削除する変数が見つかりませんでした	SmLoginLogout-Message::VariableFindErrorTo-Delete	セッション変数フラグがセッション変数名の前にリクエストの一部として渡されました。
CSmAuthUser - ChangePassword - ユーザ BLOB データを更新できません	SmLoginLogoutMessage::ChangePwdBlobUpdateFail	パスワード変更リクエストの処理中、パスワード BLOB データを更新できませんでした。

メッセージ	関数	説明
DelVariable : 内部エラー : 変数が見つかりませんでした	SmLoginLogoutMessage::Del-VariableFindError	セッションストアから変数名を削除しようとしたとき、その変数名が空でした。
DelVariable が変数 %2s についてエラー %1i を返しました	SmLoginLogoutMessage::Del-VariableReturnError	セッションストアからこの変数を削除できませんでした。
AceSetUsername = %1s が設定されませんでした	SmLoginLogoutMessage::Sm-AuthorNotSetUserId	SecurID 認証方式において、ACE 認証のユーザ名を ACE/SecurID API を使用して登録できなかった場合、このメッセージが表示されます。認証方式によってリクエストは拒否されます。
削除する変数の名前の検索エラー %1s: 無効なインデックス %2i	SmLoginLogout-Message::VariableNameFind-InvalidIndexError	セッション変数フラグが、空の名前を持つセッション変数のリクエストの一部として渡されました。
方式設定パラメータ IpszServerParam 内にエラーがあります	SmLoginLogoutMessage::Error-ServerConfigServerParam	SecurID 認証方式で使用されません。同上。
方式設定パラメータ内にエラーがあります : 空の文字列	SmLoginLogoutMessage::Error-ServerConfigParam	基本的な SecurID 認証方式でも、フォームベースの SecurID 認証方式でも、「ディレクトリ内の ACE ユーザ ID 属性名」パラメータが必要です。このパラメータが見つからないか、間違っていて設定されている場合、このエラーが表示されます。
方式 '%2s' を使用してユーザ '%1s' を認証できませんでした。サポートされていない API バージョンです	SmLoginLogoutMessage::User-AuthFail	認証プロバイダライブラリのバージョンが古いため、認証できませんでした。

メッセージ	関数	説明
認証レルム「%1s」が見つかりませんでした	SmLoginLogoutMessage::Auth-RealmFindFail	Radius 認証リクエストの処理中、指定されたエージェント/エージェント グループによって保護されているレルムが見つかりませんでした。
FindApplicablePassword ポリシー - ルートのフェッチエラー	SmLoginLogoutMessage::Error-FetchingApplicablePolicyRoot	ロギング試行の検証中、ルートオブジェクトをフェッチできませんでした。
FindApplicablePassword ポリシー - 適合するパスワードポリシーの検索エラー	SmLoginLogoutMessage::Error-FindingMatchingPolicies	ロギング試行の検証中、パスワードポリシー オブジェクトをフェッチできませんでした。
FindApplicablePassword ポリシー - ユーザディレクトリ %1s についてパスワードデータ属性が定義されていません	SmLoginLogout-Message::PasswordDataAttrib-NotDefined	使用しているユーザディレクトリで、BLOB の適切な属性が定義されていません。
FindApplicablePassword ポリシー - ユーザまたはディレクトリが NULL です	SmLoginLogoutMessage::Null-ApplicablePwdPolicyDir	ロギング試行の検証中、適用できるパスワードポリシーを検索しているときにユーザオブジェクトとディレクトリオブジェクトが両方とも NULL でした。
GetRandomPassword - 最短長が最大長を超えています	SmLoginLogoutMessage::Long-PwdLength	作成されたランダムパスワードが、許容される最大長を超えています。
GetRedirect - 使用できるパスワードポリシーが見つかりません	SmLoginLogoutMessage::Error-FindingPasswordPolicy	リダイレクト情報を含む最初の適用可能なパスワードポリシーを検索しているとき、適切なポリシーが見つかりませんでした。
GetRedirect - パスワードポリシーを取得できません	SmLoginLogoutMessage::Error-RetrievePasswordPolicy	新しいパスワードの検証中、パスワードポリシーオブジェクトをフェッチできませんでした。

メッセージ	関数	説明
GetVariable : 内部エラー : DelVar %1s が Var : %2s に一致しません	SmLoginLogoutMessage::Get-VariableMatchError	フェッチされたときに削除される変数が、フェッチ用と削除用に異なる名前を持っています。
GetVariable(Del) が変数 %2s についてエラー %1i を返しました	SmLoginLogoutMessage::Get-VariableDelReturnError	セッションストアからこの変数を削除できませんでした。
GetVariable(Fetch) が変数 %2s についてエラー %1i を返しました	SmLoginLogoutMessage::Get-VariableFetchReturnError	セッションストア内にこの変数が見つかりませんでした。
GetVariable : 内部エラー : 変数が見つかりませんでした	SmLoginLogoutMessage::Get-VariableFindError	セッション変数を取得しようとしたとき、変数名が空でした。
SiteMinder が生成したユーザ属性 %1s の形式ができませんでした	SmLoginLogoutMessage::Invalid-SmUserAttribFormat	アプリケーション ロールユーザプロパティの形式に誤りがあります。
新しい PIN が承諾された = %1s	SmLoginLogoutMessage::New-PinAccepted	HTML SecurID 認証方式で使用されます。ユーザ PIN がユーザによって正常に変更された場合、このメッセージが表示されます。
非標準の SelectionCode = %1s	SmLoginLogoutMessage::Ace-ServerNonStandard-Selectioncode	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
パスコードが割り当てられていません	SmLoginLogout-Message::PasscodeNot-Allocated	SecurID 認証方式で使用されます。ユーザパスコード用のバッファが割り当てられていません。
PassCode1 が割り当てられていません	SmLoginLogoutMessage::Mem-AllocPasscode1Fail	SecurID 認証方式で使用されます。ユーザパスコード用のバッファが割り当てられていません。
PassCode1 が割り当てられていません	SmLoginLogout-Message::Passcode1Not-Allocated	SecurID 認証方式で使用されます。次のユーザパスコード用のバッファが割り当てられていません。

メッセージ	関数	説明
PassCode1 が確認されていません。 エラー = %1i	SmLoginLogoutMessage::PassCode1NotChecked	SecurID 認証方式において、ACE/SecurID API を使用して ACE 認証プロセスを完了できない場合、このエラーメッセージが表示されます。
PassCode1 が設定されていません。 エラー = %1i	SmLoginLogoutMessage::PassCode1NotSet	SecurID 認証方式において、ACE 認証のパスコードを ACE/SecurID API を使用して登録しようとしている場合、このメッセージが表示されます。
PassCode1 が設定されていません。 エラー = %1i	SmLoginLogoutMessage::PassCode2NotSet	HTML SecurID 認証方式において、ACE 認証の次回のパスコードを ACE/SecurID API を使用して登録できなかった場合、このエラーメッセージが表示されます。認証方式によってリクエストは拒否されます。
PassCode2 が割り当てられていません	SmLoginLogoutMessage::MemAllocPasscode2Fail	SecurID 認証方式で使用されます。ユーザパスコード用のバッファが割り当てられていません。
PassCode2 が NextPasscode として送信されません。エラー = %1i	SmLoginLogoutMessage::PassCode2NotSentAsNextPasscode	HTML SecurID 認証方式において、ACE/SecurID API を使用して次回のパスコードを ACE サーバに送信できなかった場合、このエラーメッセージが表示されます。認証方式によってリクエストは拒否されます。
パスワードメッセージを解析できませんでした	SmLoginLogoutMessage::PasswordMessage-ParseFail	ログイン リクエストの処理中、パスワードを新しいものと古いものに分割しているとき、パスワード文字列を解析できませんでした。
PIN の割り当てに失敗しました	SmLoginLogoutMessage::Pin-AllocationFailed	HTML SecurID 認証方式で使用されます。ユーザ PIN 用のバッファが割り当てられていません。

メッセージ	関数	説明
pszBuf の割り当てに失敗しました	SmLoginLogoutMessage::pszBuf-AllocFail	SecurID 認証方式で使用されます SiteMinder ユーザ ディレクトリ内のユーザ ID 属性名 RSA SecurID 用のバッファが割り当てられていません。
暗号化されたシステム PIN が UserMsg 経由の Cookie でできませんでした	SmLoginLogoutMessage::ReturningEncrypted-SystemPin	情報のみ。 ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
SelectionCode が割り当てられていません	SmLoginLogoutMessage::SelectionCodeNot-Allocated	情報のみ。 ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
方式 '%2' を使用してユーザ '%1s' を認証しているときに、サーバ例外が発生しました	SmLoginLogoutMessage::User-AuthException	認証プロセス中、不明なエラーが発生しました。 認証プロバイダライブラリ内が最も可能性が高いと思われます。
ユーザ '%1s' の認証を検証しているときに、サーバ例外が発生しました	SmLoginLogoutMessage::Valid-AuthException	認証プロセス中にコールされたとき、高度なパスワードサービス共有ライブラリ内でエラーが発生しました。
ユーザ名の設定エラー = %1i	SmLoginLogoutMessage::Set-UserNameError	SecurID 認証方式において、ACE 認証のユーザ名を ACE/SecurID API を使用して登録できなかった場合、このメッセージが表示されず。 認証方式によってリクエストは拒否されます。
SetVariable : 内部エラー : 変数が見つかりませんでした	SmLoginLogoutMessage::Set-VariableFindError	セッションストア内に変数名を設定しようとしたとき、その変数名が空でした。
SetVariable : 内部エラー : 変数 %1s について NULL の値が見つかりました	SmLoginLogoutMessage::Set-VariableNullValueFound	セッションストア内に変数値を設定しようとしたとき、その変数値が空でした。

メッセージ	関数	説明
SetVariable が変数 %2s についてエラー %1i を返しました	SmLoginLogoutMessage::Set-VariableReturnError	この変数をセッションストアに対して追加または更新できませんでした。
SmAuthenticate : AceInitialization に失敗しました	SmLoginLogoutMessage::Sm-AuthAceInitFail	ACE クライアントライブラリを初期化できませんでした。
SmAuthenticate : イベントを作成できません	SmLoginLogoutMessage::Create-EventFail	SecurID 認証方式で使用されます SecurID 認証方式でイベントオブジェクトが作成されていません。
SmAuthenticate : PIN 用のメモリを割り当てることができませんでした	SmLoginLogoutMessage::Sm-AceHtmlPinMemAllocFail	SecurID 認証方式で使用されます ACE システムによって生成される PIN 用のバッファが割り当てられていません。
SmAuthenticate : AceSetPasscode = %1s が設定されませんでした	SmLoginLogoutMessage::Sm-AuthAceDidNotSetPassCode	SecurID 認証方式において、ACE 認証のパスコードを ACE/SecurID API を使用して登録できなかった場合、このエラーメッセージが表示されます。認証方式によってリクエストは拒否されます。
SmAuthenticate : SM_ACE_FAILOVER_ATTEMPTS 環境変数用の数値が見つかりませんでした。デフォルト値を使用します	SmLoginLogoutMessage::Zero-SmAuthAceFailover	RSA ACE/SecurID フェイルオーバーをサポートするため、SiteMinder ポリシーサーバには環境変数 SM_ACE_FAILOVER_ATTEMPTS があります。この変数はデフォルトで 3 に設定されます。SM_ACE_FAILOVER_ATTEMPTS の値が 0 である場合、このエラーメッセージが表示されます。この場合、SiteMinder で RSA ACE/SecurID フェイルオーバーが正常に動作しない可能性があります。
SmAuthenticate : eventdata用のストレージを割り当てることができません	SmLoginLogoutMessage::EventDataMemAllocFail	SecurID 認証方式で使用されます RSA SecurID API 構造体用のメモリが割り当てられていません。

メッセージ	関数	説明
SmAuthenticate : AceInit に進むことができません -- ACE 処理ではありません。 aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthorizationAceInitProcessingFail	SecurID 認証方式において、ACE/SecurID API を初期化できなかった場合、このメッセージが表示されます。認証方式でリクエストは拒否され、認証は失敗します。
SmAuthenticate : AceCheck に進みませんでした。 aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthorizationAceCheckDidNotContinue	SecurID 認証方式において、ACE/SecurID API を使用して ACE 認証プロセスを完了できない場合、このエラーメッセージが表示されます。
SmAuthenticate : AceInit 完了に進みませんでした。 pEventData->asynchAceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthorizationAceInitCompletionFail	SecurID 認証方式において、ACE/SecurID API を初期化できなかった場合、このメッセージが表示されます。認証方式でリクエストは拒否され、認証は失敗します。
SmAuthenticate : ACE/Server の通信障害によって、名前ロック リクエストが拒否されました	SmLoginLogoutMessage::Sm-AuthorizationNameLockReqDenied	SecurID 認証方式において、ACE/SecurID API を初期化できなかった場合、このメッセージが表示されます。認証方式でリクエストは拒否され、認証は失敗します。
SmAuthenticate : スレッドの同期に失敗しました。 wRet= %1ul	SmLoginLogoutMessage::Sm-AuthorizationThreadSyncFail	Windows プラットフォームの SecurID 認証方式において、非同期 ACE API コールに失敗した場合、このメッセージが表示されます。

メッセージ	関数	説明
SmAuthenticate : ユーザ名をロックできません。 aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthUserNameLockFail	SecurID 認証方式において、ACE サーバのユーザ名をロックできなかった場合、このメッセージが表示されます。この場合、SiteMinder の認証方式で認証リクエストは拒否されます。名前ロック機能は、RSA ACE 製品のバージョン 5.0 以上で使用できます。名前ロック機能の詳細については、RSA ACE 製品のマニュアルを参照してください。
SmAuthUser - 許可レلمをフェッチできませんでした	SmLoginLogoutMessage::Fetch-AuthRealmFailed	アプリケーション ロールユーザ プロパティを取得しているとき、ユーザのレلمが見つかりませんでした。
SmAuthUser - ドメインオブジェクトをフェッチできませんでした。	SmLoginLogoutMessage::Fetch-DomainObjFailed	アプリケーション ロールユーザ プロパティを取得しているとき、ユーザのドメインが見つかりませんでした。
新しい PIN に使用できるのは英数字のみです	SmLoginLogoutMessage::Alpha-NumericOnlyNewPin	HTML SecurID 認証方式において、ユーザが PIN の変更を要求されたときに英数字以外の文字を含む PIN を入力した場合、このメッセージが表示されます。
新しい PIN に使用できるのは数字のみです	SmLoginLogoutMessage::Digit-OnlyNewPin	HTML SecurID 認証方式において、ユーザが PIN の変更を要求されたときに数字が含まれない PIN を入力した場合、このメッセージが表示されます。
新しい PIN が長すぎます	SmLoginLogoutMessage::Long-NewPin	HTML SecurID 認証方式において、ユーザが PIN の変更を要求されたときに新しい PIN が長すぎる場合、このメッセージが表示されます。

メッセージ	関数	説明
新しい PIN が短すぎます	SmLoginLogoutMessage::Short-NewPin	HTML SecurID 認証方式において、ユーザが PIN の変更を要求されたときに新しい PIN が短すぎる場合、このメッセージが表示されます。
PIN の変更を続行できません。不明な PIN タイプです	SmLoginLogoutMessage::Ace-ServerUnableToProceedPin-Change	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカルサポートに連絡してください。
SmPasswordMsg_Change の検索中、予期しないメッセージ ID が見つかりました。 パスワード： %1ul	SmLoginLogout-Message::UnexpectedMessage-ID	ログイン リクエストの処理中、パスワードを新しいものと古いものに分割しているとき、パスワードフィールドに格納されているメッセージ ID が不明でした。
構文： %1s[:AppName]	SmLoginLogoutMessage::Usage-SmUserAttribFormat	アプリケーション ロール ユーザ プロパティの正しい書式設定を補助する文字列です。
UserPIN が割り当てられていません	SmLoginLogoutMessage::User-PinNotAllocated	SecurID 認証方式で使用されます ユーザ PIN 用のバッファが割り当てられていません。
ValidateLoginAttempt - パスワードポリシーの適用エラー	SmLoginLogoutMessage::Error-ApplyingPasswordPolicy	ロギング試行の検証中、パスワードポリシーを適用できませんでした。
ValidateLoginAttempt - パスワードポリシーのフェッチエラー	SmLoginLogoutMessage::Error-FetchingPasswordPolicy	ロギング試行の検証中、パスワードポリシー オブジェクトをフェッチできませんでした。
ValidateLoginAttempt - 使用できるパスワードポリシーの検索エラー	SmLoginLogoutMessage::Error-FindingApplicablePolicy	ロギング試行の検証中、使用できるポリシーが見つかりませんでした。
ValidateNewPassword - パスワード変更情報を設定できません	SmLoginLogoutMessage::Error-PasswordChange	パスワード BLOB データを更新しようとしているときに、パスワード情報を設定できませんでした。
ValidateNewPassword - 一致正規表現のフェッチエラー	SmLoginLogoutMessage::Match-ExprFetchError	パスワードポリシーに必要な正規表現を取得できませんでした。

許可

メッセージ	関数	説明
ValidateNewPassword - 不一致正規表現のフェッチエラー	SmLoginLogoutMessage::No-MatchExprFetchError	パスワードポリシーに必要な正規表現を取得できませんでした。
ValidateNewPassword - パスワードポリシーのフェッチエラー	SmLoginLogoutMessage::Err-FetchingValidPwdPolicy	新しいパスワードの検証中、パスワードポリシーオブジェクトをフェッチできませんでした。
ValidateNewPassword - 使用できるパスワードポリシーの検索エラー	SmLoginLogoutMessage::Err-FindingValidPwdPolicy	新しいパスワードの検証中、適用できるポリシーが見つかりませんでした。
ValidateNewPassword がコールアウト '%1s' をロードできませんでした	SmLoginLogoutMessage::Load-CalloutFail	パスワードを確認するための外部ライブラリをロードできませんでした。
ValidateNewPassword が '%2s' 内の関数 '%1s' を解決できませんでした。エラー: %3s	SmLoginLogoutMessage::Err-ResolveFuncValidPwd	パスワードを確認するための外部ライブラリ内にメソッドが見つかりませんでした。

許可

エラー メッセージの内容	関数	説明
不正な %1s リクエストが検出されました	SmsIsAuthorizedMessage::Bad-RequestDetected	許可リクエストメッセージが適切な形式に準拠していませんでした。
ライセンスされた eTelligent なしでは変数を含むアクティブな式を処理できません	SmsIsAuthorizedMessage::CanNot-ProcessActiveExpr	eTelligent ルール機能のライセンスが見つかりませんでした。アクティブな式は処理されません。
変数の追加中に例外がキャッチされました	SmsIsAuthorizedMessage::Exc-AddingVar	eTelligent ルール変数の解決中、ソフトウェア例外が発生しました。
IsOk で例外が発生しました。	SmsIsAuthorizedMessage::Unk-ExcludesOK	許可の実行中、不明の例外が発生しました。

エラー メッセージの内容	関数	説明
IsOk で例外が発生しました。できませんでした	SmlsAuthorizedMessage::Excln-IsOk	許可の実行中、例外が発生しました。
アクティブな式 %1s をロードできませんでした	SmlsAuthorizedMessage::Failed-FetchActiveExpr	オブジェクトストアからアクティブな式オブジェクトをフェッチできませんでした。
アクティブな式 %1s をロードできませんでした	SmlsAuthorizedMessage::Failed-LoadActiveExpr	アクティブな式をロードできませんでした。
ドメイン %1s をロードできませんでした	SmlsAuthorizedMessage::Failed-LoadDomain	eTelligent ルール変数の処理中、ドメインオブジェクトを取得できませんでした。
変数 %1s をロードできませんでした	SmlsAuthorizedMessage::Failed-LoadVar	指定された eTelligent ルール変数を取得できませんでした。
変数タイプ %1s をロードできませんでした	SmlsAuthorizedMessage::Failed-LoadVarType	指定された変数のタイプを取得できませんでした。
アクティブな式 %1s の変数できませんでした	SmlsAuthorizedMessage::Failed-LoadVarActiveExpr	変数の解決で問題が発生したため、アクティブな式は呼び出されません。
アクティブな式 %1s の変数をロードできませんでした	SmlsAuthorizedMessage::Failed-LoadVarsForActiveExpr	アクティブな式の eTelligent ルール変数をロードできませんでした。
属性 %1s を解決できませんでした	SmlsAuthorizedMessage::FailedToResolveAttr	オブジェクトストアからレスポンス属性オブジェクトをフェッチできませんでした。
ディクショナリ ベンダー属性 %1s を解決できませんでした	SmlsAuthorizedMessage::FailedToResolveDictVendAttr	指定されたベンダー属性がベンダー属性ディクショナリ内に見つかりませんでした。
レスポンス %1s を解決できませんでした	SmlsAuthorizedMessage::FailedToResolveResponse	オブジェクトストアからレスポンス オブジェクトをフェッチできませんでした。

エラー メッセージの内容	関数	説明
レスポンス グループ %1s を解決できませんでした	SmsAuthorizedMessage::FailedToResolveResponseGp	オブジェクトストアからレスポンス グループ オブジェクトをフェッチできませんでした。
ユーザ ポリシー %1u を解決できませんでした	SmsAuthorizedMessage::FailedToResolveUserPolicy	オブジェクトストアからユーザ ポリシー オブジェクトをフェッチできませんでした。
変数レスポンスを無視します - eTelligent オプションのライセンスがありません	SmsAuthorizedMessage::No-eTelligentLicense	eTelligent ルール機能のライセンスが見つかりませんでした。変数は処理されません。
レスポンス属性 %1s が無効です ディクショナリの競合 - 属性がレスポンスになり可能性があります	SmsAuthorizedMessage::Invalid-ResponseAttr	無効なレスポンス属性が許可レスポンスに含まれていませんでした。
IsOk に失敗しました。 できませんでした	SmsAuthorizedMessage::IsOK-Failed	許可を確認できませんでした。

サーバ

メッセージ	関数	説明
TCP サーバソケットを初期化できませんでした：ソケットエラー：%1i	SmServerMessage::TCP-ServerSocketInitFail	ソケットエラーの詳細については、オペレーティングシステムのマニュアルを参照してください（最も一般的なエラーとして、システム上ですでに使用されているソケットを開こうとする場合や、ソケットに対する十分な権限がない場合が挙げられます）。
ポート %1ui 上の UDP サーバソケットを初期化できませんでした。ソケットエラー：%2i	SmServerMessage::UDP-ServerSocketInitFailOnPort	ソケットエラーの詳細については、オペレーティングシステムのマニュアルを参照してください（最も一般的なエラーとして、システム上ですでに使用されているソケットを開こうとする場合や、ソケットに対する十分な権限がない場合が挙げられます）。
WinSock ライブラリを初期化できませんでした	SmServerMessage::WinSock-LibInitFail	(Windows システム) Windows Sockets Library を初期化できませんでした。ライブラリがインストールされていることと、そのバージョンがサポートされていることを確認してください。
TCP サーバソケットでリスンできませんでした。ソケットエラー不明です	SmServerMessage::TCP-ServerSocketListenFail	ソケットエラーの詳細については、オペレーティングシステムのマニュアルを参照してください（最も一般的なエラーとして、システム上ですでに使用されているソケットを開こうとする場合や、ソケットに対する十分な権限がない場合が挙げられます）。

メッセージ	関数	説明
イベントハンドラをロードできませんでした	SmServerMessage::Event-HandlerLoadFail	イベントハンドラ ライブラリをロードできませんでした。設定されたイベントハンドラのパス名とアクセス権限を確認してください。
ライブラリ「%1s」をロードできませんでした。 エラー : %2s	SmServerMessage::FailedTo-LoadLib	レポートされた認証方式ライブラリをロードできませんでした。表示されるエラーテキストの中に問題に関する説明がない場合は、指定されたライブラリが存在することと、ファイルシステムの保護でアクセスが許可されていることを確認してください。
イベントプロバイダ「%1s」内で必要なエントリポイントを特定できませんでした	SmServerMessage::Req-EntryPointInEventProvider-LocateFail	指定されたライブラリは有効なイベント/監視ログプロバイダではありません。
監査ログレコードを書き込めませんでした。レコードは破棄されました	CSmReports::LogAccess	ポリシーサーバから監査ログに書き込めませんでした。監査ログストアのステータスを確認してください。
ホスト名を取得できませんでした。ソケットエラー %1i	SmServerMessage::Host-NameObtainError	監査ロガープロバイダが、ネットワークエラーと思われる原因により、ローカルシステムのネットワークホスト名を取得できませんでした。表示されるエラーコード (UNIX システムの場合は <code>errno</code> 、Windows システムの場合は <code>SOCKET_ERROR</code>) によって、詳細が示される場合があります。

メッセージ	関数	説明
ホスト名を取得できませんでした。ソケットエラー %1i	SmServerMessage::Host-NameObtainFail	ネットワークエラーと思われる原因により、ローカルシステムのネットワークホスト名を取得できませんでした。表示されるエラーコード（UNIX システムの場合は <code>errno</code> 、Windows システムの場合は <code>SOCKET_ERROR</code> ）によって、詳細が示される場合があります。
'%1s' を追加する監査ログファイルを開けませんでした	SmServerMessage::Audit-LogFileAppendFail	監査ロガープロバイダが、エントリ追加のための指定されたファイルを開くことができませんでした。指定したパス名が有効であることと、ファイルアクセス権限が正しいことを確認してください。
RADIUS ログファイルを開けませんでした (ファイルが定義されていません)	SmServerMessage::Radius-LogFileNotDefined	RADIUS ログファイルの名前のエントリがレジストリにないか、名前が空の文字列です。
RADIUS ログファイルを開けませんでした : %1s	SmServerMessage::Radius-LogFileOpenFail	指定された名前を持つ RADIUS ログファイルを、上書き用を開くことができなかったか(すでに存在する場合)、作成できませんでした(存在しない場合)。ディレクトリとファイル(存在する場合)に対するアクセス権限を確認してください。。
認証方式「%1s」を照会できませんでした	SmServerMessage::Fail-QueryAuthScheme	指定された認証方式に対するポリシーサーバのクエリが失敗したため、認証方式を初期化できませんでした。

メッセージ	関数	説明
UDP ソケット上での読み取りに失敗しました。ソケットエラー %1i	SmServerMessage::UDP-SocketReadFail	ポリシー サーバで、管理サービス接続リクエストまたは RADIUS メッセージのいずれかを伝送する UDP パケットを読み取ろうとしているときに、予期しないネットワークエラーが検出されました。表示されるエラーコード (UNIX システムの場合は <code>errno</code> 、Windows システムの場合は <code>SOCKET_ERROR</code>) によって、詳細が示される場合があります。
セッション番号 %1i のリクエストを受信できませんでした : %2s/%3s : %4i。ソケットエラー %5s	SmServerMessage::Request-ReceiveOnSessionFail	ポリシー サーバで、指定されたセッションのエージェントリクエストを読み取ろうとしているときに、予期しないネットワークエラーが検出されました。そのため、接続は閉じられました。表示されるエラーコード (UNIX システムの場合は <code>errno</code> 、Windows システムの場合は <code>SOCKET_ERROR</code>) によって、詳細が示される場合があります。
エージェントキー「%1s」を解決できませんでした	SmServerMessage::Unresolved-AgentKey	エージェントキーの更新中、レポートされたエージェントキーがポリシーストア内に見つかりませんでした。
エージェントキーを解決できませんでした	SmServerMessage::FailTo-ResolveAgentKeys	エージェントキー更新用のポリシーストアの中に、アクセスできるエージェントキーがありませんでした。
エージェントキーを解決できませんでした	SmServerMessage::Agent-KeysResolveFail	エージェントキー更新用のポリシーストアの中に、アクセスできるエージェントキーがありませんでした。

メッセージ	関数	説明
エージェント キー '%1s' を解決できませんでした	SmServerMessage::Fail-ToResolveAgentKey	エージェント キーの更新中、レポートされたエージェント キーがポリシー ストア内に見つかりませんでした。
エージェントまたはエージェント グループ %1s を解決できませんでした	SmServerMessage::Agent-OrAgentGroupResolveFail	指定されたエージェントまたはエージェント グループが存在しないか、そのポリシー ストア レコードが破損しています。
すべてのドメインを解決できませんでした	SmServerMessage::Domain-ResolutionFailed	ポリシー ストア内のドメイン ルート オブジェクト レコードが、見つからないか、破損しています。
すべてのベンダーを解決できませんでした。 ベンダー ディクショナリは作成されません	SmServerMessage::Failed-ToResolveVendors	ポリシー ストア内のベンダー ルート オブジェクト レコードが、見つからないか、破損しています。
認証/許可マッピング %1s を解決できませんでした	SmServerMessage::Fail-ToResolveAuthAzMap	指定された認証/許可マップが存在しないか、そのポリシー ストア レコードが破損しています。
'%2s' 内の関数 '%1s' を解決できませんでした。エラー : %3s	SmServerMessage::Failed-ToResolveFunc	指定された認証方式ライブラリ内のレポートされたエントリ ポイントを解決できませんでした (表示されるエラー テキストを参照)。そのため、ライブラリはロードされませんでした。
トンネル サービス ライブラリ '%2s' 内の関数 '%1s' を解決できませんでした。エラー : %3s	SmServerMessage::Function-ResolveFail	指定された TransactEMS ライブラリ内のレポートされたエントリ ポイントを解決できませんでした (表示されるエラー テキストを参照)。そのため、ライブラリはロードされませんでした。

メッセージ	関数	説明
'%2s' 内の関数 '%1s' を解決できませんでした。エラー : %3s	SmServerMessage::Fail-ToResolveFunction	システム設定情報をレポートする指定のライブラリ内のレポートされたエントリポイントを解決できませんでした (表示されるエラーテキストを参照)。そのため、ライブラリはロードされませんでした。
保存できませんでした	SmServerMessage::Key-ManagementObjResolveFail	ポリシーサーバで、キー管理オブジェクトをポリシーストアから読み取ろうとしたとき、エラーが検出されました。
キー管理オブジェクトを解決できませんでした	SmServerMessage::Resolve-KeyMgmtObjFail	エージェント キー管理オブジェクトをポリシーストアから読み取ることができませんでした。
キー管理オブジェクト '%1s' を解決できませんでした	SmServerMessage::Key-ManagementObjResolve-FailwithVal	エージェント キー管理スレッドで、指定されたキー管理オブジェクトをポリシーストアから読み取ろうとしたとき、エラーが検出されました。
認証/許可マッピングのリストを解決できませんでした	SmServerMessage::Fail-ToResolveAuthAzMapList	ポリシーストア内の認証/許可マッピングオブジェクトレコードが、見つからないか、破損しています。
ログファイル名の解決に失敗しました	SmServerMessage::Log-FileNameRosolveFail	監査ロガープロバイダが、ログファイルの名前をレジストリから取得できませんでした。ファイル名が設定されていることを確認してください。
共有秘密キー ポリシー オブジェクトを解決できませんでした	SmServerMessage::Shared-SecretResolveFail	ポリシーストア内の共有秘密キーのロールオーバーポリシー オブジェクトレコードが、見つからないか、破損しています。

メッセージ	関数	説明
ユーザ識別情報を解決できませんでした	SmServerMessage::Fail-ToResolveUserDir	指定されたユーザディレクトリオブジェクトが存在しないか、そのポリシーストアレコードが破損しています。
ユーザ識別情報を解決できません。アクセスを拒否します	SmServerMessage::User-Identity Fail	適用可能なレールのポリシーを検索しているときにエラーが発生したため、ユーザの識別情報を解決できず、アクセスが拒否されました。
「%2s」内のバージョン 6 関数「%1s」を解決できませんでした。 エラー： %3s	SmServerMessage::Failed-ToResolveVer6Func	指定されたバージョン 6 認証方式ライブラリ内のレポートされたエントリポイントが見つかりませんでした (表示されるエラーテキストを参照)。そのため、ライブラリは使用されません。認証方式のバージョンが古くないことを確認してください。
監査ログのクリア行数を取得できませんでした。無制限に設定します	SmServerMessage::Audit-LogFlushIntervalRetrieveFail	監査ロガー ODBC プロバイダは、クリアの間隔をレジストリから取得できませんでした。間隔が設定されていることを確認してください。
ネームスペース「%1s」の監査ログプロバイダライブラリを取得できませんでした	SmServerMessage::AuditLog-ProviderLibRetrieveFail	指定された監査ログプロバイダネームスペースのライブラリ名エントリがレジストリにありません。
監査ログのクリア行数を取得できませんでした。無制限に設定 1000	SmServerMessage::Audit-LogRowFlushCountRetrieveFail	ODBC 監査ログプロバイダの非同期ロギングでの行のクリア数のエントリがレジストリにありません。そのため、デフォルトの 1000 が使用されます。

メッセージ	関数	説明
メッセージ キューからメッセージを取得できませんでした	SmServerMessage::Retrieve-FromMessageQueueFail	(Windows) ポリシー サーバ プロセスがその Windows アプリケーション キューに関するメッセージを取得しようとしたとき、エラーが発生しました。
トラステッドホストの共有秘密キーをロールオーバーできませんでした	SmServerMessage::Trusted-HostSharedSecretsRolloverFail	トラステッドホストの共有秘密キーをロールオーバーしようとしたとき、エラーが発生しました。ロールオーバー ポリシーが有効であることを確認してください。
セッション キー更新の後、保存できませんでした	SmServerMessage::Save-NewMgmtKeyObjFail	新しい永続キーを保存することになっていたとき、エージェント キー管理オブジェクトをポリシー ストアから読み取ることができませんでした。
セッション キー更新の後、キー管理オブジェクトを保存できませんでした	SmServerMessage::Save-NewMgmtKeyObjAfter-KeyUpdateFail	ポリシー サーバで、ロールオーバー用の新しいエージェント キーが生成されましたが、それらのキーが使用可能であることを記録できませんでした。
セッション キー更新の後、キー管理オブジェクトを保存できませんでした	SmServerMessage::Save-NewMgmtKeyObjAfter-PersistentKeyUpdateFail	新しい永続キーを、ポリシー ストアのエージェント キー管理オブジェクト内に保存できませんでした。
セッション キー更新の後、キー管理オブジェクトを保存できませんでした	SmServerMessage::Save-NewMgmtKeyObjAfterSession-KeyUpdateFail	新しいエージェントセッション キーをポリシー ストア内に保存できませんでした。
新しい永続エージェント キー '%1s' を保存できませんでした	SmServerMessage::Save-NewCurrentAgentKeyFail	指定されたエージェントセッション キーを、エージェントの「現在の」キーとして保存できませんでした。

メッセージ	関数	説明
新しいキー管理オブジェクトを保存できませんでした	SmServerMessage::Agent-KeyManagementObjSaveFail	エージェント キー管理スレッドで、ロールオーバー用の新しいエージェント キーが生成されましたが、それらのキーが使用可能であることを記録できませんでした。
新しい「最後の」エージェント キー '%1s' を保存できませんでした	SmServerMessage::Save-NewLastAgentKeyFail	指定されたエージェントセッション キーを、エージェントの「最終」キーとしてポリシーストア内に保存できませんでした。
新しい「次の」エージェント キー '%1s' を保存できませんでした	SmServerMessage::Save-NewNextAgentKeyFail	指定されたエージェントセッション キーを、エージェントの「次回」キーとしてポリシーストア内に保存できませんでした。
新しい永続エージェント キー '%1s' を保存できませんでした	SmServerMessage::Failed-ToSaveNewPersistentAgentKey	指定された永続エージェント キーをポリシーストア内に保存できませんでした。
セッション番号 %1i でレスポンスを送信できませんでした : %2s/%3s : %4i。ソケットエラー %5i	SmServerMessage::Response-SendOnSessionFail	ネットワーク エラー (あるいはエージェントの障害) が原因で、指定されたセッションでのエージェント リクエストに対するレスポンスを送信できませんでした。表示されるエラー コード (UNIX システムの場合は <code>errno</code> 、Windows システムの場合は <code>SOCKET_ERROR</code>) によって、詳細が示される場合があります。

メッセージ	関数	説明
エージェント コマンド管理のウォッチドッグ スレッドを開始できませんでした	SmServerMessage::Agent-CommandManagementThread-CreationFail	エージェント コマンド管理スレッドが実行されることを保証する「ウォッチドッグ」スレッドが開始されませんでした。オペレーティングシステムで設定されている、スレッドの最大数およびオープンファイル記述子の最大数の、プロセスあたりの制限を確認してください。
ジャーナル管理スレッドを開始できませんでした	SmServerMessage::Journal-ThreadCreateFail	「ウォッチドッグ」スレッドが、ポリシーストア ジャーナルクリーンアップ管理スレッドを開始（再開）できませんでした。オペレーティングシステムで設定されている、スレッドの最大数およびオープンファイル記述子の最大数の、プロセスあたりの制限を確認してください。
ジャーナル管理ウォッチドッグ スレッドを開始できませんでした	SmServerMessage::Journal-ManagementThreadFail	ポリシーストア ジャーナルクリーンアップ管理スレッドが実行されることを保証する「ウォッチドッグ」スレッドが開始されませんでした。オペレーティングシステムで設定されている、スレッドの最大数およびオープンファイル記述子の最大数の、プロセスあたりの制限を確認してください。

メッセージ	関数	説明
キー管理ウォッチドッグ スレッドを開始できませんでした	SmServerMessage::AgentKey-ThreadCreateFail	「ウォッチドッグ」スレッドがエージェント キー管理スレッドを開始（再開）できませんでした。オペレーティングシステムで設定されている、スレッドの最大数およびオープンファイル記述子の最大数の、プロセスあたりの制限を確認してください。
キー管理ウォッチドッグ スレッドを開始できませんでした	SmServerMessage::Key-ManagementThreadCreateFail	エージェント キー管理スレッドが実行されることを保証する「ウォッチドッグ」スレッドが開始されませんでした。オペレーティングシステムで設定されている、スレッドの最大数およびオープンファイル記述子の最大数の、プロセスあたりの制限を確認してください。
メイン応答スレッドを開始できませんでした	SmServerMessage::Main-ReactorThreadStartFail	ネットワーク IO ディスパッチャスレッドが開始されませんでした。オペレーティングシステムで設定されている、スレッドの最大数およびオープンファイル記述子の最大数の、プロセスあたりの制限を確認してください。
オブジェクトストア ジャーナルスレッドを開始できませんでした	SmServerMessage::Journal-StartFailed	「ウォッチドッグ」スレッドが、ポリシーストア ジャーナル管理スレッドを開始（再開）できませんでした。オペレーティングシステムで設定されている、スレッドの最大数およびオープンファイル記述子の最大数の、プロセスあたりの制限を確認してください。

メッセージ	関数	説明
オブジェクトストアウォッチ ドッグスレッドを開始できま せませんでした	SmServerMessage::Watchdog- Failed	ポリシーストアジャーナル管 理スレッドが実行されること を保証する「ウォッチドッグ」 スレッドが開始されませんで した。オペレーティングシス テムで設定されている、スレッ ドの最大数およびオープン ファイル記述子の最大数の、プ ロセスあたりの制限を確認し てください。
管理コマンドチャンネルを開始 できませんでした	SmServerMessage::Stat-MangmC mdChannelFail	(UNIX/Linux) 既存のサーバコ マンド管理パイプ/ファイルの stat () が、予期せずに失敗しま した。サーバコマンド管理ス レッドも開始されない場合は、 他のポリシーサーバプロセス が実行されていないことを確 認し、パイプ/ファイルを手動 で削除してください。
エージェントキーを更新でき ませんでした	SmServerMessage::FailTo-Updat eAgentKeys	キーがエージェントによって 更新される管理者コマンドを ポリシーストア内に保存でき ませんでした。
サーバコマンドからエージェ ントキーを 更新できませんでした	SmServerMessage::Failed-ToUpd ateAgentKeys	エージェントの新しい「現在 の」セッションキーまたは「次 の」セッションキーを、ポリ シーストア内に保存できませ んでした。
エージェントキーへの変更を 更新できませんでした	SmServerMessage::Fail-ToUpdat eChangesToAgentKeys	キーがエージェントによって 更新されるコマンドをポリ シーストア内に保存できませ んでした。
永続キーを更新できませんで した	SmServerMessage::Failed-ToUpd atePersistentKey	エージェントの永続キーをポ リシーストア内に保存できま せませんでした。

メッセージ	関数	説明
UDP ソケット上での書き込みに失敗しました。ソケットエラー %1i	SmServerMessage::UDP-Socket WriteFail	ネットワーク エラー (あるいはエージェントの障害) が原因で、管理 GUI 初期化パケットまたは RADIUS レスポンスパケットを送信できませんでした。表示されるエラーコード (UNIX システムの場合は <code>errno</code> 、Windows システムの場合は <code>SOCKET_ERROR</code>) によって、詳細が示される場合があります。
ファイルが見つかりません	SmServerMessage::File-NotFound	(Windows システム) ワンビュー モニターを開始するサービスが、 <code>bin¥smmon.bat</code> ファイルを読み取ることができませんでした。
プロセッサアフィニティを取得できませんでした	SmServerMessage::Get-ProcessorAffinityFail	(Windows) プロセッサアフィニティのパフォーマンス調整パラメータを処理できませんでした。したがって、既存のアフィニティ設定は変更されません。
ハンドシェイク エラー: hello メッセージ内に不明のクライアント名「%1s」があります	SmServerMessage::Handshake-ErrorUnknownClient	クライアントからの接続試行時、レポート済みの名前が指定されましたが、その名前を持つエージェントはポリシーストア内に見つかりませんでした。また、エージェントが間違っただに共有秘密キーを使用していることも原因です。
エージェント キー マーカー (%1i) が一致していません	SmServerMessage::InconsistentAgent-KeyMarker	ポリシーストア内のエージェント キー レコードに、指定された、未承認のキータイプがあります。
エージェント キーの数 (%1i) が一致していません	SmServerMessage::InconsistentNumberOf-AgentKeys	ポリシーストア内に、エージェント用に指定された不正な数のキーがあります。

メッセージ	関数	説明
レルム リスト計算時の内部エラー。アクセスを拒否します	SmServerMessage::Realm-Corrupt	レルム リストをフェッチしてアクセス許可を実行しようとしたとき、予期しないポリシーストア障害が発生したため、アクセスは拒否されました。
エージェント キー マーカー (%1i) が不正です	SmServerMessage::Invalid-AgentKeyMarker	ポリシー ストア内のエージェント キー レコードに、指定された、未承認のキー タイプがあります。
IP アドレス リソース フィルタが IsOk によってまだサポートされていません	SmServerMessage::IPAddr-ResourceFilterNotSupported	レルム内のアクション ルールが一致しても、IP アドレスまたは範囲の照合はサポートされません。
IsInDictionary - パスワード ディクショナリホルダ %1s に追加できませんでした	SmServerMessage::Add-PasswordDictToHolderFailed	指定されたパスワード ディクショナリをキャッシュできませんでした。100 を超えるディクショナリをキャッシュできません。ディクショナリ内のエントリに対して照合されるパスワードは、一致するものと見なされます。
IsInDictionary - パスワード ディクショナリ %1s を作成できませんでした	SmServerMessage::Create-PasswordDictFailed	指定されたパスワード ディクショナリをキャッシュする準備をしているときに、予期しないエラー (おそらくはメモリ不足) が発生しました。ディクショナリ内のエントリに対して照合されるパスワードは、一致するものと見なされます。
IsInDictionary - パスワード ディクショナリ %1s を設定できませんでした	SmServerMessage::Set-PasswordDictFailed	指定されたパスワード ディクショナリをキャッシュしているときに、エラーが発生しました。ディクショナリ内のエントリに対して照合されるパスワードは、一致するものと見なされます。

メッセージ	関数	説明
IsInDictionary - パスワードディクショナリ %1s が開いていません	SmServerMessage::Open-PasswordDictFailed	指定されたパスワードディクショナリはロードされましたが、予期せず開かれていません。ディクショナリ内のエントリに対して照合されるパスワードは、一致しないものと見なされます。
IsInProfileAttributes - プロパティ名のフェッチエラー	SmServerMessage::Fetching-PropertyNameFail	パスワードをユーザプロファイル属性値と比較しているとき、ユーザ属性名を取得できませんでした。そのため、パスワードは一致するものと見なされます。
IsInProfileAttributes - プロパティ値のフェッチエラー	SmServerMessage::Fetching-PropertyValueFail	パスワードをユーザプロファイル属性値と比較しているとき、属性値を取得できませんでした。そのため、パスワードは一致するものと見なされます。
未記録データの監視リクエスト、Null 値が返されました	SmServerMessage::MonReq-UnrecordedDataNullValue	ポリシーサーバは、監視対象データのリクエストで渡された名前を認識しませんでした。
エージェント暗号化キーが見つかりませんでした	SmServerMessage::Agent-EncryptionKeyNotFound	エージェントのキーセットをポリシーストアからフェッチしたとき、完全なセットが見つかりませんでした。
エージェントキーがキーストア内にありません	SmServerMessage::AgentKey-NotFoundInKeyStore	ポリシーストア内のエージェントキーを更新しようとしたとき、キーが見つかりませんでした。
初期エージェントキーがありません	SmServerMessage::Empty-AgentKeys	ポリシーストア内にエージェントキーが格納されておらず、キー生成が有効になっていません。

メッセージ	関数	説明
初期キー管理オブジェクトが見つかりませんでした。このポリシーサーバは読み取り専用キー管理モードで設定されています。続行できません	SmServerMessage::Key-ManagementObjNotFound	ポリシーストア内に初期エージェントキー管理オブジェクトが格納されておらず、キー生成が有効になっていません。
監査ログプロバイダが使用できる名前空間がありません	SmServerMessage::No-NamespacesAvailForAudit-LogProvider	監査ログプロバイダの namespaces のエントリがレジストリにありません。
ルート設定オブジェクトが見つかりませんでした。 smobjimport を実行して smpolicy.smdif をインポートしてください	SmServerMessage::Root-ConfigObjNotFound	ポリシーストアが正常に初期化されていません。
リクエスト %1s の処理中、セッションポインタが見つかりませんでした	SmServerMessage::Null-SessionPointer	指定されたエージェントリクエストは受信されましたが、対応するエージェントセッションオブジェクトが見つからなかったか、有効ではありませんでした。そのため、リクエストパケットは処理されずに返されました。
ファイルの権限またはパスが有効かどうか確認してください	SmServerMessage::File-PermissionOrPathCheck	ファイルを開くことができませんでした。ファイルのパス名を示すエラーメッセージが、このメッセージの前に表示されるはずです。示されたパス名が有効であることと、ファイルへのアクセス権限が正しいことを確認してください。
ポリシーサーバが ProcessMessage で例外をキャッチしました (メッセージテキストはありません)。	SmServerMessage::Unknown-PolicySrvExcpCaught	ポリシーサーバで、エージェントリクエストの処理中に予期しない例外が発生しました。そのため、空のレスポンスが返されました。

メッセージ	関数	説明
ポリシー サーバが ProcessMessage で 例外をキャッチしました テキスト : %1s	SmServerMessage::PolSrv-ExcpCaught	ポリシー サーバで、エージェント リクエストの処理中に予期しない例外が発生しました。そのため、空のレスポンスが返されました。表示されるテキストに、推奨される修正アクションが示される場合があります。
ポリシー ストアで、オブジェクトタイプ '%2s' の操作 '%1s' に失敗しました。 %3s	SmServerMessage::Policy-StoreObjectFail	ポリシー ストア オブジェクト レイヤで、記述された例外がキャッチされました。
プロセッサ アフィニティがデフォルト設定のままです。アフィニティをゼロに設定することはできません	SmServerMessage::Processor-AffinitySetZeroFail	(Windows) ゼロはプロセッサ アフィニティのパフォーマンス調整パラメータについて無効な値です。したがって、既存のアフィニティ設定は変更されません。
%1s の拒否 : アクセス ログを書き込めませんでした	SmServerMessage::Write-FailInAccessLog	指定された拒否済みの認証または許可リクエストの監査ロギングに失敗しました。
DoManagement() コマンド%1s、リクエスト %2s 内のエージェント名を参照しました	SmServerMessage::Agent-NameInDoManagement	「Do Management」エージェント コマンドは拒否されました。
Logout() コマンド %1s、リクエスト %2s 内のエージェント名を参照しました	SmServerMessage::Agent-NameInLogout	ログアウト リクエストは拒否されました。
プロセッサ アフィニティをできませんでした	SmServerMessage::Set-ProcessorAffinityFail	(Windows) プロセッサ アフィニティのパフォーマンス調整パラメータを処理できませんでした。したがって、既存のアフィニティ設定は変更されません。

メッセージ	関数	説明
初期化中に SM 例外がキャッチされました (%1s)	SmServerMessage::SMExcp-DuringInit	ポリシー サーバ起動時の「GlobalInit」段階で例外がキャッチされたため、ポリシーサーバを起動できませんでした。表示されるテキストに、詳細が示される場合があります。
サーバのシャットダウン中に SM 例外がキャッチされました (%1s)	SmServerMessage::SMExcp-DuringShutdown	ポリシー サーバ停止時の「GlobalRelease」段階で例外がキャッチされました。表示されるテキストに、詳細が示される場合があります。
TCP ポートを初期化できませんでした	SmServerMessage::TCP-PortInitFail	ポリシー サーバの起動中、アクセス制御リクエストまたは管理リクエストについて有効化された TCP ポートを初期化できませんでした。そのため、起動は中止されました。
サービス ローダが %1s を開始できませんでした。エラー %2i %3s	SmServerMessage::SZSERVER_StartFail	(Windows) サービス ローダを開始できませんでした (エラーテキストを参照)。そのため、ポリシー サーバやワンビューモニターを開始できませんでした。
このポリシー サーバにはセッション暗号化キーがありません	SmServerMessage::Session-EncryptKeyNotFound	ポリシー サーバが初期セッションキーを持っておらず、キー生成が有効になっていません。アクセス制御リクエストまたは管理リクエストが処理されるように設定されている場合、起動は中止されます。
スレッドプールスレッドで例外がキャッチされました	SmServerMessage::ExcpIn-ThreadPool	予期しない条件が発生したため、ポリシー サーバのワーカースレッドが終了しました。代替のスレッドがスレッドプールに追加されます。

メッセージ	関数	説明
UDP ポートを初期化できませんでした	SmServerMessage::UDPPort-InitFail	ポリシー サーバの起動中、管理リクエストまたは RADIUS リクエストについて有効化された UDP ポートを初期化できませんでした。そのため、起動は中止されました。
UDP 処理例外	SmServerMessage::UDP-ProcessingExcp	管理 GUI 初期化パケットまたは RADIUS レスポンス パケットの処理中、予期しないエラーが発生しました。 レスポンスは送信されません。
コンソール出力コレクタを作成できません。 トレースは有効になりません	SmServerMessage::Trace-NotEnabledConsoleOutput-CollectCreateFail	ポリシー サーバプロセスが、プロファイラ (トレース) ログの出力先のコンソール (またはターミナル ウィンドウ) にアクセスできませんでした。 コンソールを開くための適切なアクセス権限があることを確認してください。
ファイル出力コレクタを作成できません。 トレースは有効になりません	SmServerMessage::Trace-NotEnabledFileOutput-CollectCreateFail	プロファイラ (トレース) ログ ファイルを、上書き用を開くことができなかつたか (すでに存在する場合)、作成できませんでした (存在しない場合)。 ディレクトリとファイル (存在する場合) に対するアクセス権限を確認してください。。
共有秘密キーのロールオーバー ポリシー オブジェクトを作成できません	SmServerMessage::Shared-SecretCreateFail	ポリシー サーバの起動中、ポリシー ストア内に共有秘密キー ポリシー オブジェクトが見つからず、初期ポリシー オブジェクトを作成できませんでした。そのため、起動は中止されました。

メッセージ	関数	説明
トレースを有効にすることができません	SmServerMessage::Trace-NotEnabled	プロファイラ (トレース) ロギングの初期設定は成功しましたが、それ以外は成功しませんでした。
ロガー オプションを動的にリセットできません	SmServerMessage::Dynamic-LoggerResetFail	ポリシー サーバの実行中にロガー設定オプションの変更を検出するスレッドを開始できませんでした。そのため、ポリシー サーバを再起動するまで、そのような変更は対処されません。
リクエスト %1s のエージェントを解決できません	SmServerMessage::Unresolved-AgentIdentity	エージェント識別情報を含めるにはエージェント リクエストが必要ですが、識別情報を検証できませんでした。 リクエストは拒否されました。
エージェント名 %1s、リクエスト %2s を解決できません	SmServerMessage::AgentName-UnResolved	エージェント識別情報を含めるにはエージェント リクエストが必要ですが、指定されたエージェントの識別情報を検証できませんでした。 リクエストは拒否されました。
パスワード BLOB データを更新できません	SmServerMessage::Blob-UpdateFailed	パスワード サービスのためのユーザの「パスワード BLOB」データをユーザストア内で更新できませんでした。 設定に従って、ポリシー サーバはユーザの認証試行を拒否しました。
許可ライブラリの発行中、予期しない例外が発生しました	SmServerMessage::Unexpected-Exception-PublishingAzLibs	ロードされたカスタム許可モジュールで「発行」の診断情報を照会しているときに、予期しない例外が発生しました。そのため、カスタム許可ライブラリに関する情報は発行されません。

メッセージ	関数	説明
不明のエージェントキータイプ %1i	SmServerMessage::Agent-KeyTypeUnknown	「Do Management」リクエストの処理中、指定された、未承認のキータイプを持つエージェントキーレコードがポリシーストア内で見つかりました。そのため、リクエストは拒否されました。
認証ライブラリの発行中、不明の例外がキャッチされました	SmServerMessage::Unknown-ExceptionPublishAuthLibs	カスタム認証方式ライブラリで「発行」の診断情報を照会しているときに、予期しない例外が発生しました。そのため、ロードされたカスタム認証方式に関する情報は発行されません。
イベントライブラリ情報の発行中、不明の例外がキャッチされました	SmServerMessage::Unknown-ExceptionWhilePublishEventLibInfo	カスタムイベントハンドラライブラリで「発行」の診断情報を照会しているときに、予期しない例外が発生しました。そのため、SiteMinderによってロードされたカスタムイベントライブラリに関する情報は発行されません。
ソケットエラー 104	104 - bind() 関数のコールに失敗しました。	TLI レイヤを介して送信中にエラーが発生したため、このメッセージは返されました。

Java API

エラー メッセージの内容	関数	説明
%1s が管理者ディレクトリをフェッチできませんでした	SmJavaApiMessage::AdministratorDirectory-FetchFail	登録管理者ユーザディレクトリをフェッチできません。ポリシーストアを確認してください。
%1s が登録レلمをフェッチできませんでした	SmJavaApiMessage::RegistrationDirectory-FetchFail	登録ユーザディレクトリをフェッチできません。ポリシーストアを確認してください。
%1s が登録レلمをフェッチできませんでした	SmJavaApiMessage::RegistrationDomain-FetchFail	登録ドメインをフェッチできません。ポリシーストアを確認してください。
%1s が登録レلمをフェッチできませんでした	SmJavaApiMessage::RegistrationRealm-FetchFail	登録レلمをフェッチできません。ポリシーストアを確認してください。
%1s が登録レلمを登録方式	SmJavaApiMessage::RegistrationScheme-FetchFail	登録方式をフェッチできません。ポリシーストアを確認してください。
%1s 無効なレلم OID (NULL)	SmJavaApiMessage::Invalid-RealmOid	レلم OID を取得できません。ユーザがログインに成功したことと、有効なセッション ID が使用可能であることを確認してください。
(CsmEmsCommand::Set-ObjectClasses) プロパティの設定に失敗した後、ディレクトリユーザ %1s のプロパティをロールバックできませんでした	SmJavaApiMessage::Csm-EmsSetObjectClasses-RollBackPropertiesFail	新しい値が拒否された後、ユーザのプロパティをリセットできません。 ユーザストアが正しく動作していることと、ポリシーサーバが接続を確立できることを確認してください。

エラー メッセージの内容	関数	説明
(CSmEmsCommand::Set-Properties) プロパティの設定に失敗した後、ディレクトリ ユーザ %1s のプロパティをロールバックできませんでした	SmJavaApiMessage::CSm-EmsSetPropertiesRollback-PropertiesFail	新しい値が拒否された後、ユーザのプロパティをリセットできません。 ユーザストアが正しく動作していることと、ポリシー サーバが接続を確立できることを確認してください。
(CSmEmsCommandV2::Set-ObjectClasses) プロパティの設定に失敗した後、ディレクトリ ユーザ %1s のプロパティをロールバックできませんでした	SmJavaApiMessage::Set-ObjectClassesDir-UserRollbackFail	新しい値が拒否された後、ユーザのプロパティをリセットできません。 ポリシー ストアで定義されているディレクトリ接続を確認してください。
(CSmEmsCommandV2::Set-Properties) プロパティの設定に失敗した後、ディレクトリ ユーザ %1s のプロパティをロールバックできませんでした	SmJavaApiMessage::Set-PropertiesDirObjRollbackFail	新しい値が拒否された後、オブジェクトのプロパティをリセットできません。 ポリシー ストアで定義されているディレクトリ接続を確認してください。
TransactSessionTimeoutThread で例外が発生しました	SmJavaApiMessage::Unknown-ExcpTransactSessionTimeout-Thread	期限切れセッションの処理中に不明なエラーが発生しました。
TransactSessionTimeoutThread で例外が発生しました メッセージ: %1s	SmJavaApiMessage::Excp-TransactSessionTimeoutThread	期限切れセッションの処理中にエラーが発生しました。
EmsSession タイムアウト スレッドを作成できませんでした	SmJavaApiMessage::Ems-SessionTimeoutThread-CreateFail	新しいスレッドを作成するための十分なシステム リソースがありません。
すべてのドメインを解決できませんでした	SmJavaApiMessage::Domain-ResolveFail	現在の管理者に関連付けられているすべてのドメインを取得しているときに問題が発生しました。ポリシー ストアに破損がないかどうか確認してください。

エラー メッセージの内容	関数	説明
<code>getUsersDelegatedRoles</code> の実行に失敗しました。エラー = %1s	<code>SmJavaApiMessage::IMSgetUsersDelegatedRolesFail</code>	このユーザのロールを取得できません。 <code>smobjims.dll</code> (<code>libsmobjims.so</code>) ライブラリがインストールされていることを確認してください。
<code>getUsersDelegatedRolesInApp</code> の実行に失敗しました。エラー = %1s	<code>SmJavaApiMessage::IMSgetUsersDelegatedRolesInAppFail</code>	アプリケーションのユーザ ロールを取得できません。 <code>smobjims.dll</code> (<code>libsmobjims.so</code>) ライブラリがインストールされていることを確認してください。
<code>getUsersDelegatedTasks</code> の実行に失敗しました。エラー = %1s	<code>SmJavaApiMessage::IMSgetUsersDelegatedTasksFail</code>	このユーザのタスクを取得できません。 <code>smobjims.dll</code> (<code>libsmobjims.so</code>) ライブラリがインストールされていることを確認してください。
<code>getUsersDelegatedTasksInApp</code> の実行に失敗しました。エラー = %1s	<code>SmJavaApiMessage::IMS-getUsersDelegatedTasksIn-AppFail</code>	アプリケーションのユーザ タスクを取得できません。 <code>smobjims.dll</code> (<code>libsmobjims.so</code>) ライブラリがインストールされていることを確認してください。
<code>getUsersRoles</code> の実行に失敗しました。エラー = %1s	<code>SmJavaApiMessage::IMS-getUsersRolesFail</code>	このユーザのロールを取得できません。 <code>smobjims.dll</code> (<code>libsmobjims.so</code>) ライブラリがインストールされていることを確認してください。
<code>getUsersRolesInApp</code> の実行に失敗しました。エラー = %1s	<code>SmJavaApiMessage::IMS-getUsersRolesInAppFail</code>	アプリケーションのユーザ ロールを取得できません。 <code>smobjims.dll</code> (<code>libsmobjims.so</code>) ライブラリがインストールされていることを確認してください。
<code>getUsersTasks</code> の実行に失敗しました。エラー = %1s	<code>SmJavaApiMessage::IMS-getUsersTasksFail</code>	このユーザのタスクを取得できません。 <code>smobjims.dll</code> (<code>libsmobjims.so</code>) ライブラリがインストールされていることを確認してください。

エラー メッセージの内容	関数	説明
getUsersTasksInApp の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMS-getUsersTasksInAppFail	アプリケーションのユーザ タスクを取得できません。 smobjjims.dll (libsmobjjims.so) ライブラリがインストールされていることを確認してください。
IMSObjectProviderFactory: getObjectProvider() - getAddress('%1s') の実行に失敗しました	SmJavaApiMessage::getIMSBaseObjectProvider_getProcAddressFail	smobjjims.dll (libsmobjjims.so) ライブラリがインストールされていることを確認してください。
IMSObjectProviderFactory: getObjectProvider() - プロバイダライブラリのロードエラー	SmJavaApiMessage::IMS_getProviderLib-LoadError	IdentityMinder がインストールされていないか、正しくインストールされていない場合、起動時にこのメッセージが生成されます。
%1s の IMSObjectProviderFactory: getObjectProvider() - getAddress の実行に失敗しました	SmJavaApiMessage::IMS_getProvider_getProcAddressFail	ライブラリが破損しています。あるいは、リソース不足のためポリシー サーバがライブラリをロードできませんでした。
%1s の ImsRBACProviderFactory: getObjectProvider() - getAddress の実行に失敗しました	SmJavaApiMessage::Ims-RBACProvider-Factory_getProviderFail	IdentityMinder がインストールされていないか、正しくインストールされていない場合、起動時にこのメッセージが生成されます。
IsAssociatedWithDirectory の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMSIs-AssociatedWithDirectoryFail	関連する IMS 環境についてユーザ ディレクトリが有効であるかどうかを判断しているときにエラーが発生しました。
IsUserAssignedRole の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMSIs-UserAssignedRoleFail	ユーザがロールに属するかどうかを判断しているときにエラーが発生しました。
IsUserDelegatedRole の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMSIs-UserDelegatedRoleFail	ユーザがロールに属するかどうかを判断しているときにエラーが発生しました。

エラー メッセージの内容	関数	説明
SmJavaAPI : クラス ActiveExpressionContext %1p の検索エラー	SmJavaApiMessage::MSG_E_-FI NDING_CAEClog	結合中、JVM で Active Expression クラスを特定できませんでした。 ポリシー サーバにオプション パックがインストールされてい ることを確認してください。 smjavaapi.jar のクラスパスも確認 してください。
SmJavaAPI : クラス NativeCallbackError %1p の 取得エラー	SmJavaApiMessage::MSG_E_-FI NDING_CNCElog	有効な smjavaapi.jar が存在し、ク ラスパスに含まれていることを 確認してください。JVM バージョ ンがこのリリースについてサ ポートされているかどうかを確 認してください。
SmJavaAPI : クラス SmAuthenticationContext %1p の検索エラー	SmJavaApiMessage::MSG_E_-FI NDING_CAUTHClog	有効な smjavaapi.jar が存在し、ク ラスパスに含まれていることを 確認してください。
SmJavaAPI : クラス Throwable %1p の検索エラー	SmJavaApiMessage::MSG_E_-FI NDING_CTHROWlog	JVM/JRE が正常にインストールさ れていない可能性があります。有 効な rt.jar が存在するかどうかを 確認してください。サポートされ ている JVM バージョンを使用す るように SiteMinder が設定され ていることを確認してください。
SmJavaAPI : クラス TunnelServiceContext %1p の 検索エラー	SmJavaApiMessage::MSG_E_-FI NDING_CTSClog	ポリシー サーバにオプション パックがインストールされてい ることと、有効な smjavaapi.jar が 存在し、クラスパスに含まれてい ることを確認してください。
SmJavaAPI : クラス UserAuthenticationException %1p の検索エラー	SmJavaApiMessage::MSG_E_-FI NDING_CUAElog	有効な smjavaapi.jar が存在し、ク ラスパスに含まれていることを 確認してください。JVM バージョ ンがこのリリースについてサ ポートされているかどうかを確 認してください。

エラー メッセージの内容	関数	説明
SmJavaAPI : メソッド ActiveExpressionContext の検 索エラー。 %1p を呼び出してください	SmJavaApiMessage::MSG_E_-FI ND_MINVOKElog	ポリシー サーバにオプション パックがインストールされてい ることと、有効な smjavaapi.jar が 存在し、クラスパスに含まれてい ることを確認してください。
SmJavaAPI : メソッド ActiveExpressionContext の検 索エラー。 %1p を解放してください	SmJavaApiMessage::MSG_E_-FI ND_MRELEASElog	ポリシー サーバにオプション パックがインストールされてい ることと、有効な smjavaapi.jar が 存在し、クラスパスに含まれてい ることを確認してください。
SmJavaAPI : メソッド SmAuthenticationContext の検 索エラー。 %1p を認証してください	SmJavaApiMessage::MSG_E_-FI ND_MAUTHENTICATElog	有効な smjavaapi.jar が存在し、ク ラスパスに含まれていることを 確認してください。JVM バージョ ンがこのリリースについてサ ポートされているかどうかを確 認してください。
SmJavaAPI : メソッド SmAuthenticationContext の検 索エラー。 %1p を初期化してください	SmJavaApiMessage::MSG_E_-FI ND_MAUTHINITlog	有効な smjavaapi.jar が存在し、ク ラスパスに含まれていることを 確認してください。JVM バージョ ンがこのリリースについてサ ポートされているかどうかを確 認してください。
SmJavaAPI : メソッド SmAuthenticationContext の検 索エラー。 %1p を照会してください	SmJavaApiMessage::MSG_E_-FI ND_MAUTHQUERYlog	有効な smjavaapi.jar が存在し、ク ラスパスに含まれていることを 確認してください。JVM バージョ ンがこのリリースについてサ ポートされているかどうかを確 認してください。
SmJavaAPI : メソッド SmAuthenticationContext の検 索エラー。 %1p を解放してください	SmJavaApiMessage::MSG_E_-FI ND_MAUTHRELEASElog	有効な smjavaapi.jar が存在し、ク ラスパスに含まれていることを 確認してください。JVM バージョ ンがこのリリースについてサ ポートされているかどうかを確 認してください。

エラー メッセージの内容	関数	説明
SmJavaAPI : メソッド Throwable.getLocalizedMessage %1p の検索エラー	SmJavaApiMessage::MSG_E_-FI ND_GLMlog	JVM/JRE が正常にインストールされていない可能性があります。有効な <code>rt.jar</code> が存在するかどうかを確認してください。サポートされている JVM バージョンを使用するように <code>SiteMinder</code> が設定されていることを確認してください。
SmJavaAPI : メソッド TunnelServiceContext.tunnel %1p の検索エラー	SmJavaApiMessage::MSG_E_-FI ND_MTUNNELlog	有効な <code>smjavaapi.jar</code> が存在し、クラスパスに含まれていることを確認してください。
SmJavaAPI : Java のアクティブな式 %1p の初期化エラー	SmJavaApiMessage::MSG_E_-A CTEXPR_INITlog	Active Expression ライブラリをロードできません。 <code>smactiveexpr.jar</code> がクラスパスに含まれていることを確認してください。
SmJavaAPI : SMJavaAPI %1p に対する JNI 参照の初期化エラー	SmJavaApiMessage::MSG_E_-IN IT_JNI_REFSlog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。
SmJavaAPI : クラス TunnelServiceContext %1p に対するグローバル参照の 取得エラー	SmJavaApiMessage::MSG_E_-GL OBAL_CAEClog	アクティブな式のコンテキストを確立しているとき、JVM で内部エラーが発生しました。
SmJavaAPI : クラス TunnelServiceContext %1p に対するグローバル参照の 実行エラー	SmJavaApiMessage::MSG_E_-GL OBAL_CNCElog	有効な <code>smjavaapi.jar</code> が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。
SmJavaAPI : クラス TunnelServiceContext %1p に対するグローバル参照の 取得エラー	SmJavaApiMessage::MSG_E_-GL OBAL_CAUTHClog	認証のコンテキストを確立しているとき、JVM で内部エラーが発生しました。

エラー メッセージの内容	関数	説明
SmJavaAPI : クラス TunnelServiceContext %1p に対するグローバル参照の 実行エラー	SmJavaApiMessage::MSG_E_-GL OBAL_CTHROWlog	JVM/JRE が正常にインストールされていない可能性があります。有効な rt.jar が存在するかどうかを確認してください。サポートされている JVM バージョンを使用するように SiteMinder が設定されていることを確認してください。
SmJavaAPI : クラス TunnelServiceContext %1p に対するグローバル参照の 実行エラー	SmJavaApiMessage::MSG_E_-GL OBAL_CTSClog	トンネル接続を確立しているとき、JVM で内部エラーが発生しました。
SmJavaAPI : クラス TunnelServiceContext %1p に対するグローバル参照の 実行エラー	SmJavaApiMessage::MSG_E_-GL OBAL_CUAEllog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。
SmJavaAPI : Java アクティブ 式 %1p に対する 解放エラー	SmJavaApiMessage::MSG_E_-A CTEXPR_RELEASElog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。
SmJavaAPI : Java アクティブ 式 %1p に対する JNI 参照の初期化エラー	SmJavaApiMessage::MSG_E_-RE L_JNI_REFSlog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。
SmJavaAPI : JVM 環境 %1p を 取得できません	SmJavaApiMessage::MSG_-ERR _GETTING_JVMlog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。
SmJavaAPI : JNI 参照 %1p を 初期化できません	SmJavaApiMessage::MSG_-ERR _INIT_JNI_REFlog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。
SmJavaAPI : JNI 参照 %1p を 解放できません	SmJavaApiMessage::MSG_-ERR _REL_JNI_REFlog	ポリシー サーバは、許可の後またはシャットダウン中に、リソースを完全に解放できませんでした。

エラー メッセージの内容	関数	説明
SmJVMSupport : スレッド %1p への JVM アタッチエラー	SmJavaApiMessage::MSG_E_-ATTACH_TO_THREADlog	JVM が正常に初期化されなかった可能性があります。実行中の迷子の Java プロセスが存在しないことを確認してください。
SmJVMSupport : JVM %1p 作成エラー	SmJavaApiMessage::MSG_E_-CREATE_JVMlog	JVM が正しくインストールされていることと、jvm.dll (libjvm.so) ライブラリが有効であることを確認してください。
SmJVMSupport : JVM %1p の破棄エラー	SmJavaApiMessage::MSG_E_-DESTROYING_JAVA_VMlog	ポリシー サーバでクリーンシャットダウンが実行されませんでした。JVM リソースは解放されませんでした。
SmJVMSupport : スレッド %1p からの JVM 取得エラー	SmJavaApiMessage::MSG_E_-DETACH_THREADlog	ポリシー サーバでクリーンシャットダウンが実行されませんでした。JVM リソースは解放されませんでした。
SmJVMSupport : JVM %1p からリソースを解放するためのクラス System の検索エラー	SmJavaApiMessage::MSG_E_-JM_RR_FSYSlog	ポリシー サーバでクリーンシャットダウンが実行されませんでした。JVM リソースは解放されませんでした。
SmJVMSupport : JVM %1p の作成時における CLASSPATH 環境変数取得エラー	SmJavaApiMessage::MSG_E_-GETENV_CPlog	CLASSPATH 変数が正しく定義されていることを確認してください。
SmJVMSupport : JVM %1p からリソースを解放するための JVM 環境の取得エラー	SmJavaApiMessage::MSG_E_-JM_RR_ENVlog	ポリシー サーバでクリーンシャットダウンが実行されませんでした。JVM リソースは解放されませんでした。
SmJVMSupport : JVM %1p からリソースを解放するためのクラス System 上のメソッド GC の取得エラー	SmJavaApiMessage::MSG_E_-JM_RR_GGClog	JVM がガーベッジコレクションを実行できませんでした。rt.jar の有効性を確認してください。

エラー メッセージの内容	関数	説明
SmJVMSupport : NETE_JVM_OPTION_FILE %1p の 取得エラー	SmJavaApiMessage::MSG_E_-O PEN_JVM_OPTION_FILElog	環境変数 NETE_JVM_OPTION_FILE が設定されていることと、ファイ ルが有効であることを確認して ください。
SmJVMSupport : 作成された JVM %1p の取得エラー	SmJavaApiMessage::MSG_E_-G ET_CREATED_JVM_LOG	JVM が正常に初期化 されなかった可能性があります。 実行中の迷子の Java プロセスが 存在しない ことを確認してください。
SmJVMSupport : JVM %1p の 作成時にキャッチされた 不明のエラー	SmJavaApiMessage::MSG_E_-C AUGHT_CREATE_JVMlog	JVM が正しくインストールされ ていることと、jvm.dll (libjvm.so) ライブラリが有効であることを 確認してください。

LDAP

エラー メッセージの内容	関数	説明
(AddMember) グループ DN : '%1s', ユーザ DN: '%2s'. ステータス: エラー %3i。 %4s	SmLdapMessage::ErrorLdap-Ad dMemberGroupDN	LDAP ユーザディレクトリ内の指 定されたグループに対し、指定さ れたユーザを追加できませんで した。詳細については、LDAP エ ラーメッセージを参照してくだ さい。
(AuthenticateUser) DN : '%1s'。ステータス: エ ラー %2i。 %3s	SmLdapMes-sage::Authenticate UserDNld-Error	ポリシーサーバで、LDAP ユーザ ディレクトリに対してユーザを 認証できませんでした。このエ ラーは、ユーザが正しくないパス ワードを入力するなど、さまざま な理由で発生することがありま す。詳細については、LDAP エラー メッセージを参照してください。

エラー メッセージの内容	関数	説明
(Bind - init) サーバ : '%1s'、ポート : %2ul。ステータス : エラー	SmLdapMessage::ErrorBindInit	ユーザディレクトリ用に設定された LDAP サーバを初期化できませんでした。エラーメッセージの中で示された LDAP サーバをトラブルシューティングしてください。
(Bind - init) サーバ : セキュリティ統合ファイルをロードできませんでした	SmLdapMessage::BindInit-LoadSecurityIntegrationFileFail	(現在使用されていません)
(Bind - init) サーバ : セキュリティ統合秘密キーをロードできませんでした	SmLdapMessage::BindInit-LoadSecurityIntegrationSecret-Fail	(現在使用されていません)
(Bind - ldap_set_option CONNECT_TIMEOUT) 。ステータス : エラー %1i。 %2s	SmLdapMessage::ErrorBind-LdapOptionConnectTimeout	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
(Bind - ldap_set_option LDAP_OPT_PROTOCOL_VERSION) 。ステータス : エラー %1i。 %2s	SmLdapMessage::ErrorBind-LdapOptionProtocolVersion	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
(Bind - ldap_set_option LDAP_OPT_REFERRALS) 。ステータス : エラー %1i。 %2s	SmLdapMessage::ErrorBind-LdapOptionReferrals	自動リフェラル処理の有効化を設定できません。詳細については、エラー文字列を確認してください。
(Bind - ldap_set_option LDAP_VERSION2) 。ステータス : エラー %1i。 %2s	SmLdapMessage::ErrorBind-LdapOptionVersion2	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。使用している LDAP サーバが、サポートされているバージョンのうちの1つであることを確認してください。
(Bind - ldap_set_option SIZELIMIT) 。ステータス : エラー %1i。 %2s	SmLdapMessage::ErrorBind-LdapOptionSizeLimit	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。

エラー メッセージの内容	関数	説明
(Bind - ldap_set_option THREAD_FN_PTRS)。ステータス：エラー %1i。 %2s	SmLdapMessage::ErrorBind-LdapOptionThreadFnPirs	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
(Bind - ldap_set_option TIMELIMIT)。ステータス：エラー %1i。 %2s	SmLdapMessage::ErrorBind-LdapOptionTimeLimit	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
(Bind - LDAP 初期化中、SSL クライアントを初期化できませんでした)サーバ：'%1s'、ポート： %2ul、証明書 DB： '%3s'。ステータス：エラー	SmLdapMessage::BindSSL-LdapClientInitFailed	LDAP サーバに接続できません。LDAP サーバが稼働していることと、LDAP サーバおよびポートが正しいことを確認してください (ポリシー サーバマシンから ping を実行してみてください)。
(Bind - SSL client init) 証明書 DB： '%1s'。ステータス：エラー	SmLdapMessage::BindSSL-ClientCertDBFailed	ユーザディレクトリ用に設定された LDAP サーバへの SSL 接続のクライアント側の初期化に失敗しました。証明書データベースが正しく指定されているかどうかを確認してください。
(Bind - SSL init) サーバ： '%1s'、ポート： %2ul。ステータス：エラー。LDAP サーバおよびポートを確認してください。	SmLdapMessage::BindSSL-InitFailed	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。
(Bind) DN： '%1s'。ステータス：エラー %2i。 %3s	SmLdapMessage::BindDN-RequireCredentialsError	LDAP サーバにバインドできません。認証情報が正しいことを確認してください。SiteMinder 管理コンソールを参照してください。
(Bind) ステータス：エラー %1i。 %2s	SmLdapMessage::Bind-StatusError	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。

エラー メッセージの内容	関数	説明
(ChangeUserPassword) DN : '%1s'。ステータス : エラー %2i。 %3s	SmLdapMessage::Change-User PasswordLdError	指定されたユーザのパスワードを変更できませんでした。そのユーザの古いパスワードを使用して LDAP サーバにバインドできなかったためです。詳細については、エラー メッセージを参照してください。
(ChangeUserPassword) DN : '%1s'。ステータス : エラー %2s	SmLdapMessage::Change-User PasswordDNFail	指定されたユーザのパスワードを変更できませんでした。詳細については、エラー メッセージを参照してください。
(CSmDsLdapProvider::Add-Entry) DN : '%1s'。ステータス : エラー %2i。 %3s	SmLdapMessage::ErrorLdap-AddEntryDN	指定された DN エントリを LDAP ユーザディレクトリに追加できませんでした。詳細については、LDAP エラー メッセージを参照してください。
(GetObjProperties) DN : '%1s'。ステータス : エラー %2i。 %3s	SmLdapMessage::GetObj-PropertiesDNLdError	ポリシー サーバで、LDAP ユーザディレクトリ内にあるリクエストされた DN のリクエストされたプロパティを取得できませんでした。詳細については、LDAP エラー メッセージを参照してください。
(GetUserProp) DN : '%1s'、フィルタ : '%2s'。ステータス : エラー %3i。 %4s	SmLdapMessage::GetUser-Prop DNld-Error	指定された DN を検索しているとき、および取得される属性を指定しているときに、エラーが発生しました。詳細については、LDAP エラー メッセージを参照してください。
(GetUserProp) DN : '%1s'、フィルタ : '%2s'。ステータス : エラー %3i。 %4s	SmLdapMessage::GetUser-Prop sDNldError	指定された DN を検索しているとき、および取得される属性を指定しているときに、エラーが発生しました。詳細については、LDAP エラー メッセージを参照してください。

エラー メッセージの内容	関数	説明
(RemoveEntry) DN : '%1s'。ステータス : エラー %2i。%3s	SmLdapMessage::ErrorLdap-RemoveEntryDN	LDAP ユーザディレクトリから削除する DN エントリが見つかりませんでした。詳細については、LDAP エラーメッセージを参照してください。
(RemoveMember) グループ DN : '%1s'、ユーザ DN : '%2s'。ステータス : エラー %3i。%4s	SmLdapMessage::ErrorLdap-RemoveMemberGroupDN	LDAP ユーザディレクトリ内の指定されたグループから、指定されたユーザを削除できませんでした。詳細については、LDAP エラーメッセージを参照してください。
(SetUserProp) DN : '%1s'、プロパティ名 : '%2s'、プロパティ値 : '%3s'。ステータス : エラー %4i。%5s	SmLdapMessage::SetUser-PropDNError	LDAP ユーザディレクトリ内の指定された DN エントリを変更できませんでした。詳細については、LDAP エラーメッセージを参照してください。
(SetUserProp) DN : '%1s'。ステータス : エラー %2i。%3s	SmLdapMessage::SetUser-Prop sDNLdError	LDAP ユーザディレクトリ内の指定された DN エントリを変更できませんでした。詳細については、LDAP エラーメッセージを参照してください。
(SI Bind - init) サーバ : '%1s'、ポート : %2ul。ステータス : nit エラー	SmLdapMessage::ErrorSI-BindInit	ユーザディレクトリ用に設定された LDAP サーバを初期化できませんでした。エラーメッセージの中で示された LDAP サーバをトラブルシューティングしてください。
(SmDsLdap) サーバを取得できませんでした	SmLdapMessage::SmDs-LdapFailToGetServers	参照先の LDAP サーバに再バインドしているときに、内部エラーが発生しました。データを使用できない場合があります。
(SmDsLdapConnMgr(Bind) : LDAP 初期化中、SSL クライアントを初期化できませんでした) 。サーバ %1s : %2ul、証明書 DB : %3s	SmLdapMessage::Ldap-ConnMgrBindSSLCertDBInit-Fail	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。

エラー メッセージの内容	関数	説明
"ldap_url_parse returns error '%1s' when parsing '%2s'"	SmLdapMessage::Error_ldap_url_parse	内部 LDAP URL を解析できませんでした。この URL は RFC 2255 形式に準拠している必要があります。
(SmDsLdap-LdapAdd) DN : '%1s'。ステータス : リフェラルを受け取りましたが、処理が実装されていません。	SmLdapMessage::SmDsLdap-AddHandlingImplError	リフェラル リクエストを返す Add コールでエラーが発生しました。
(SmDsLdap-LdapDelete) DN : '%1s'。ステータス : リフェラルを受け取りましたが、処理が実装されていません。	SmLdapMessage::SmDs-LdapDeleteHandlingImplError	リフェラル リクエストを返す Delete コールでエラーが発生しました。
(SmDsLdap-LdapModify) DN : '%1s'。ステータス : リフェラルを受け取りましたが、処理が実装されていません。	SmLdapMessage::SmDs-LdapModifyHandlingImplError	リフェラル リクエストを返す Modify コールでエラーが発生しました。
(SmDsLdap-Referral) %1s 解析中のエラー LDAP URL。	SmLdapMessage::Ldap-URLParsingError	ポリシー サーバで、指定された LDAP URL を解析できませんでした。このエラーの一般的な原因は、誤りのある LDAP URL がリフェラルとして渡されたことです。その場合は、LDAP トポロジが正しく定義されていることを確認し、ポリシー サーバ管理コンソールで拡張 LDAP リフェラル処理を無効にしてください。
CSmDsLdapConnMgr (ldap_unbind_s)。サーバ %1s : %2ul	SmLdapMessage::Error-LdapConnMgrUnbind	LDAP サーバからのバインド解除中にエラーが発生しました。
CSmDsLdapConnMgr (ldap_unbind_s)。サーバ %1s : %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrUnbind	LDAP サーバからのバインド解除中に内部エラーが発生しました。
CSmDsLdapProvider::Search() : LDAP 検索フィルタの構文エラー : %1s	SmLdapMessage::Wrong-SyntaxLdapSearchFilter	LDAP 検索フィルタの構文が正しいかどうか確認してください。

エラー メッセージの内容	関数	説明
CsMdsLdapProvider::Search-Binary() : LDAP 検索フィルタの構文エラー : %1s	SmLdapMessage::Wrong-SyntaxLdapSearchBinFilter	LDAP 検索フィルタの構文が正しいかどうか確認してください。
CsMdsLdapProvider::Search-Count() : LDAP 検索フィルタの構文エラー : %1s	SmLdapMessage::Wrong-SyntaxLdapSearchCountFilter	LDAP 検索フィルタの構文が正しいかどうか確認してください。
CsMObjLdapConnMgr 例外 (ldap_unbind_s)。サーバ %1s : %2ul	SmLdapMessage::Excp-CsMObjLdapConn-Mgrldap_unbind_s	SiteMinder ポリシー サーバで、ポリシー ストア用に設定された LDAP サーバからバインド解除できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティングしてください。
ディレクトリの無効フラグ属性が CsMdsLdapProvider::Set-DisabledUserState のパスワード サービス機能について適切ではありません。	SmLdapMessage::DirDisabled-FlagNotProper	ディレクトリには無効フラグを表すユーザ属性があります。この属性はパスワード サービスで機能しません。属性を変更します。
CsMdsLDAPConn::Create-LDAP Controls の例外 (ldap_controls_free)	SmLdapMessage::Unknown-ExceptionFreeLDAPControls	内部オブジェクトを LDAP ライブラリに解放しているときに、予期しないエラーが発生しました。ポリシー サーバシステム上のメモリ エラーまたは設定エラーが原因であると思われます。
CsMdsLdapProvider::Search-Count の例外 (ldap_count_entries)	SmLdapMessage::Unknown-ExceptionLdapCountEntries	ユーザ ディレクトリ プロバイダ レイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CsMdsLdapProvider::Get-GroupMembers の例外 (ldap_explode_dn)	SmLdapMessage::Ldap-Explode-ExceptionGet-GroupMembers	DN をその構成部分に変換しているときに、不明の例外が発生しました。
CsMdsLdapProvider::Bind の例外 (ldap_init)	SmLdapMessage::Unknown-ExceptionLdapInitBind	ユーザ ディレクトリ用に設定された LDAP サーバを初期化しているときに、不明の例外が発生しました。

エラー メッセージの内容	関数	説明
SecurityIntegrationCheck の例外 (ldap_init)	SmLdapMessage::Unknown-ExceptionLdapInit	ユーザディレクトリ用に設定された LDAP サーバを初期化しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Add-Entry の例外 (ldap_modify_s)	SmLdapMessage::Unknown-ExceptionLdapModifyAdd-Entries	LDAP ユーザディレクトリにエントリを追加しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Set-UserProps の例外 (ldap_modify_s)	SmLdapMessage::Unknown-ExceptionLdapModify-SetUserProps	LDAP ユーザディレクトリ内のエントリを変更しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Ping-Server の例外 (ldap_search_ext_s)	SmLdapMessage::Unknown-ExceptionPingServer	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください (ポリシー サーバマシンから ping を実行してみてください)。
CSmDsLdap-Provider::Search の例外 (ldap_search_ext_s)	SmLdapMessage::Unknown-ExceptionLdapSearchExt	ユーザディレクトリ プロバイダレイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmDsLdapProvider::-SearchBinary の例外 (ldap_search_ext_s)	SmLdapMessage::Unknown-ExceptionLdapSearchBinExt	ユーザディレクトリ プロバイダレイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmDsLdapProvider::-SearchCount の例外 (ldap_search_ext_s)	SmLdapMessage::Unknown-ExceptionSearchCount	ユーザディレクトリ プロバイダレイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmObjLdapProvider::Ping-Server の例外 (ldap_search_s)	SmLdapMessage::Unknown-ExceptionLdapSearchGet-ObjProperties	ユーザディレクトリ プロバイダレイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。

エラー メッセージの内容	関数	説明
CSmObjLdapProvider::Ping-Server の例外 (ldap_search_s)	SmLdapMessage::Unknown-ExceptionLdapSearchGet-UserProps	ユーザディレクトリプロバイダレイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmObjLdapProvider::Ping-Server の例外 (ldap_search_s)	SmLdapMessage::Unknown-ExceptionLdapSearchGet-UserProps	ユーザディレクトリプロバイダレイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmObjLdapProvider::Ping-Server の例外 (ldap_search_st)	SmLdapMessage::Excp-Ldap_Search_S	ポリシーストア用に設定された LDAP サーバに対して ping を実行できませんでした。この LDAP サーバが稼働しているかどうかを確認してください。
CSmObjLdapProvider::Ping-Server の例外 (ldap_search_st)	SmLdapMessage::Excpldap_-search_st	ポリシーストア用に設定された LDAP サーバに対し、指定されたタイムアウト値を使って ping を実行できませんでした。この LDAP サーバが稼働しているかどうかを確認してください。
CSmDsLdapProvider::Bind の例外 (ldap_simple_bind_s)	SmLdapMessage::Unknown-Exception-LdapSimpleBind	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください (ポリシーサーバマシンから ping を実行してみてください)。
CSmDsLdapProvider::Add-Entry の例外 (LdapModify)	SmLdapMessage::Unknown-ExceptionLdapModifyAddEntry	LDAP ユーザディレクトリにエンTRIESを追加しているときに、不明の例外が発生しました。拡張リフェラル処理が役に立つかどうか試してみてください。
CSmDsLdapProvider::Add-Member の例外 (LdapModify)	SmLdapMessage::Unknown-ExceptionLdapModifyAdd-Member	LDAP ユーザディレクトリ内のグループにメンバを追加しているときに、不明の例外が発生しました。拡張リフェラル処理が役に立つかどうか試してみてください。

エラー メッセージの内容	関数	説明
CSmDsLdapProvider::Remove-Member の例外 (LdapModify)	SmLdapMessage::Unknown-ExceptionLdapModify-RemoveMember	LDAP ユーザディレクトリ内のグループからメンバを削除しているときに、不明の例外が発生しました。拡張リフェラル処理が役に立つかどうか試してみてください。
CSmDsLdapProvider::Set-UserProp の例外 (LdapModify)	SmLdapMessage::Unknown-ExceptionLdapModifySet-UserProp	LDAP ユーザディレクトリ内のエントリを変更しているときに、不明の例外が発生しました。拡張リフェラル処理が役に立つかどうか試してみてください。
CSmDsLdapProvider::Init-Instance の例外 (ldapssl_client_init)	SmLdapMessage::Unknown-ExceptionLdapSSLClientInit	ユーザディレクトリ用に設定された LDAP サーバへの SSL 接続のクライアント側の初期化に失敗しました。証明書データベースが正しく指定されているかどうかを確認してください。
CSmDsLdapProvider::Bind の例外 (ldapssl_init)	SmLdapMessage::Unknown-ExceptionLdapSSLInitBind	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。
CSmDsLDAPConn::Create-LDAPControls の例外	SmLdapMessage::Unknown-ExceptionCreateLDAPControls	LDAP ライブラリの内部オブジェクトをリクエストしているときに、予期しないエラーが発生しました。ポリシーサーバシステム上のメモリ エラーまたは設定エラーが原因であると思われます。
CSmDsLDAPConn::Free-LDAPControls の例外	SmLdapMessage::Unknown-exceptionCSmDsLDAP-Conn_FreeLDAPControls	LDAP コントロールの解放中に内部エラーが発生しました。
CSmDsLDAPConn::Parse-LDAPControls の例外	SmLdapMessage::Unknown-ExceptionParseLDAPControls	LDAP サーバからのレスポンスを解析できません。LDAP サーバは正常に稼働していますか。

エラー メッセージの内容	関数	説明
CSmDsLdapProvider::Get-ObjProperties の例外	SmLdapMessage::Unknown-ExceptionGetObjProperties	ユーザディレクトリプロバイダレイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Get-UserProp の例外	SmLdapMessage::Unknown-ExceptionGetUserProp	ユーザディレクトリプロバイダレイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Get-UserProps の例外	SmLdapMessage::Unknown-ExceptionGetUserProps	ユーザディレクトリプロバイダレイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Search の例外	SmLdapMessage::Unknown-ExceptionCSmDsLdap-ProviderSearch	ユーザディレクトリプロバイダレイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Search-Binary の例外	SmLdapMessage::Unknown-ExceptionSearchBinary	ユーザディレクトリプロバイダレイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
SecurityIntegrationCheck で例外が発生しました	SmLdapMessage::Unknown-ExceptionSecurityIntegration-Check	ユーザディレクトリ用に設定された LDAP サーバが Security Integration LDAP のインスタンスであるかどうかを確認しているときに、不明の例外が発生しました。
ページング コントロールを作成できませんでした	SmLdapMessage::Create-PagingControlFail	LDAP ライブラリの内部オブジェクトをリクエストしているときに、内部エラーが発生しました。ポリシーサーバシステム上のメモリエラーまたは設定エラーが原因であると思われます。

エラー メッセージの内容	関数	説明
LDAP 並べ替えコントロールを作成できませんでした	SmLdapMessage::Create-SortLdapControlFail	LDAP ライブラリの内部オブジェクトをリクエストしているときに、内部エラーが発生しました。ポリシー サーバシステム上のメモリ エラーまたは設定エラーが原因であると思われます。
DN 「%2s」のユーザプロパティ「%1s」をフェッチできませんでした	SmLdapMessage::FailedTo-FetchUserPropertyForDN	指定された DN が、ユーザディレクトリ用に設定された LDAP サーバ上に存在しないか、指定されたプロパティを持っていません。たとえば、SiteMinderSDK アプリケーションが、存在しないグループに対してユーザを追加しようとすると、このようなエラーが発生する場合があります。
LDAP メッセージを解析できませんでした	SmLdapMessage::Ldap-ParseMsgFail	LDAP サーバから無効なレスポンスを受け取りました。LDAP サーバは正常に稼働していますか。
サーバ側のレスポンス並べ替えコントロールを解析できませんでした	SmLdapMessage::Parsing-ServerSideResponse-ControlFail	LDAP サーバからのレスポンスを解析できません。LDAP サーバは正常に稼働していますか。
レスポンス仮想リスト表示コントロールを解析できませんでした	SmLdapMessage::Virtual-ListViewResponseControlFail	LDAP サーバからのレスポンスを解析できません。LDAP サーバは正常に稼働していますか。
証明書 DB の場所をレジストリから取得できませんでした	SmLdapMessage::Retrieve-CertDBRegFailed	HKLM¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder¥CurrentVersion¥LdapPolicyStore¥CertDbPath レジストリ エントリが見つかりませんでした。そのエントリを作成し、SSL 証明書データベースの適切なパスを入力してください。SSL 接続を使用しない場合は、空のままにします。UNIX システムでは、<install-dir>/registry 内の sm.registry ファイルを使用します。

エラー メッセージの内容	関数	説明
サーバ側の LDAP 並べ替えコントロールを解析できませんでした	SmLdapMessage::Server-SideSortingLdapExecFail	LDAP サーバからのレスポンスを解析できません。LDAP サーバは正常に稼働していますか。
ポリシーストア内のアクティブな式エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchFor-ActiveExpr	ポリシーストア内のアクティブな式の検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内のエージェントエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Device	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のエージェントコマンドエントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AgentCommand	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のエージェントグループエントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_DeviceGroup	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージの内容	関数	説明
ポリシーストア内のエージェントキーエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AgentKey	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のエージェントタイプエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchFor-AgentType	ポリシーストア内のエージェントタイプの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内のエージェントタイプ属性エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-AgentTypeAttr	ポリシーストア内のエージェントタイプ属性の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内の認証/許可マップエントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AuthAzMap	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内の証明書マップエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_CertMap	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージの内容	関数	説明
ポリシーストア内のドメインエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Domain	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のキー管理エントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::LdapAdmin-SizeLimit-Exceeded_KeyManagement	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内の ODBC クエリ エントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_ODBCQuery	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のパスワードポリシーエントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_PasswordPolicy	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージの内容	関数	説明
ポリシーストア内のポリシーエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Policy	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のポリシーリンクエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_PolicyLink	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のプロパティエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchFor-Property	ポリシーストア内のプロパティオブジェクトの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内のプロパティコレクションエントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-PropertyCollection	ポリシーストア内のプロパティコレクションの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内のサーバコマンドエントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::AdminLimit-ExceedSearchForProperty-Section	ポリシーストア内のプロパティセクションの検索で、LDAP インスタンスの設定に使用された検索制限を超過しました LDAP サーバ側の検索制限の値を増やしてください。

エラー メッセージの内容	関数	説明
ポリシー ストア内のレلم エントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Realm	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のレスポンス エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Response	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のレスポンス属性エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForRespAttr	ポリシー ストア内のレスポンス属性の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のレスポンス グループ エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForRespGroup	ポリシー ストア内のレスポンスグループの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のルート設定エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::AdminLimit-ExceedSearchForRootConfig	ポリシー ストアにはルート設定オブジェクトを 1 つしか置くことができないので、このようなエラーが発生してはいけません。ポリシー ストアが破損している可能性があります。

エラー メッセージの内容	関数	説明
ポリシーストア内のルールエントリの検索で LDAP 管理制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForRule	ポリシーストア内のルールの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内のルールグループエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::AdminLimit-ExceedSearchForRuleGroup	ポリシーストア内のルールグループの検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内の方式エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::AdminLimit-ExceedSearchForScheme	ポリシーストア内の認証方式の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内の自己登録エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::AdminLimit-ExceedSearchForSelfReg	ポリシーストア内の登録方式の検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内のサーバコマンドエントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchForServer-Command	ポリシーストア内のサーバコマンドの検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内の共有秘密キーポリシーエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchFor-SharedSecretPolicy	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージの内容	関数	説明
ポリシーストア内のタグ付き文字列エントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchFor-TaggedString	ポリシーストア内のタグ付き文字列の検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内のトラステッドホストエントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchFor-TrustedHost	ポリシーストア内のトラステッドホストの検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内のユーザディレクトリ エントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchForUser-Directory	ポリシーストア内のユーザディレクトリの検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内のユーザポリシーエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchForUser-Policy	ポリシーストア内のユーザポリシーの検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内の変数エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchForVariable	ポリシーストア内の変数の検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシーストア内の変数のタイプエントリの検索で LDAP 管理制限を超過しました	SmLdapMessage::Admin-LimitExceedSearchFor-VariableType	ポリシーストア内の変数のタイプの検索で、LDAP インスタンスの設定に使用された検索制限を超過しました。LDAP サーバ側の検索制限の値を増やしてください。

エラー メッセージの内容	関数	説明
ポリシーストア内の管理者エントリの検索で LDAP 管理サイズ制限を超過しました	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Admin	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
IMSEnvironments の Domain_FetchProperty 内の LDAP エラー - IMS オブジェクトについてサポートされていないポリシーストアバージョン	SmLdapMessage::Error-Domain FetchIMSEnv	ポリシーサーバのバージョンは 5.1 以上である必要があります。
IMSEnvironments の Domain_SaveProperty 内の LDAP エラー - IMS オブジェクトについてサポートされていないポリシーストアバージョン	SmLdapMessage::Error-Domain SaveIMSEnv	ポリシーサーバのバージョンは 5.1 以上である必要があります。
ポリシーストア内のアクティブな式エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceedSearchForActiveExpr	ポリシーストア内のアクティブな式の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内の管理者エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_Admin	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージの内容	関数	説明
ポリシーストア内のエージェントエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_Device	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のエージェントコマンドエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_Agent-Command	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のエージェントグループエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_DeviceGroup	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のエージェントキーエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_AgentKey	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージの内容	関数	説明
ポリシーストア内のエージェントタイプエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceedSearchForAgentType	ポリシーストア内のエージェントタイプの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のエージェントタイプ属性エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceedSearchForAgent-TypeAttr	ポリシーストア内のエージェントタイプ属性の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内の認証/許可マップエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_AuthAzMap	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内の証明書マップエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_CertMap	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のドメインエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_Domain	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージの内容	関数	説明
ポリシーストア内のキー管理エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_KeyManagement	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内の ODBC クエリ エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_ODBCQuery	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のパスワードポリシー エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_PasswordPolicy	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のポリシー エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_Policy	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージの内容	関数	説明
ポリシーストア内のポリシーリンクエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_PolicyLink	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のプロパティエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForProperty	ポリシーストア内のプロパティオブジェクトの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のプロパティコレクションエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForProperty-Collection	ポリシーストア内のプロパティコレクションの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のプロパティセクションエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForProperty-Section	ポリシーストア内のプロパティセクションの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のレルムエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_Realm	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージの内容	関数	説明
ポリシーストア内のレスポンスエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::LdapSize-LimitExceeded_Response	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のレスポンス属性エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForResponse-Attr	ポリシーストア内のレスポンス属性の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のレスポンスグループエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForRespGroup	ポリシーストア内のレスポンスグループの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のルート設定エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForRootConfig	ポリシーストアにはルート設定オブジェクトを1つしか置くことができないので、このようなエラーが発生してはいけません。ポリシーストアが破損している可能性があります。
ポリシーストア内のルールエントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceededSearchForRule	ポリシーストア内のルールの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のルールグループエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForRuleGroup	ポリシーストア内のルールグループの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。

エラー メッセージの内容	関数	説明
ポリシーストア内の方式エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceedSearchForScheme	ポリシーストア内の認証方式の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内の自己登録エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceedSearchForSelfReg	ポリシーストア内の登録方式の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のサーバコマンドエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceedSearchForServer-Command	ポリシーストア内のサーバコマンドの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内の共有秘密キーポリシーエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceedSearchForShared-SecretPolicy	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシーストア内のタグ付き文字列エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceedSearchForTaggedString	ポリシーストア内のタグ付き文字列の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のトラステッドホストエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceedSearchForTrustedHost	ポリシーストア内のトラステッドホストの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。

エラー メッセージの内容	関数	説明
ポリシーストア内のユーザディレクトリエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForUser-Directory	ポリシーストア内のユーザディレクトリの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内のユーザポリシーエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForUserPolicy	ポリシーストア内のユーザポリシーの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内の変数エントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForVariable	ポリシーストア内の変数の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシーストア内の変数のタイプエントリの検索で LDAP サイズ制限を超過しました	SmLdapMessage::SizeLimit-ExceededSearchForVariableType	ポリシーストア内の変数のタイプの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超過しました。LDAP サーバ側のサイズ制限の値を増やしてください。
入力された文字列の長さが、制限を超過しています。詳細については、LDAP ストアのマニュアルを参照してください。	SmLdapMessage::Ldap-LengthConstraint-Violation_CertMap	検索で使用された値が長すぎました。
PingServer 内の SmDsLdapConnMgr (ldap_search_ext_s) : %1s	SmLdapMessage::ErrorLdap-ConnMgrPingServer	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください (ポリシーサーバマシンから ping を実行してみてください)。

エラー メッセージの内容	関数	説明
SmDsLdapConnMgr Bind - init. サーバ %1s : %2ul	SmLdapMessage::LdapConnMgrBindInitFail	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください (ポリシー サーバマシンから ping を実行してみてください)。
SmDsLdapConnMgr Bind - SetOption CONNECT_TIMEOUT %1i. サーバ %2s : %3ul	SmLdapMessage::LdapConnMgrBindSetOptionConnectTimeout	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
SmDsLdapConnMgr Bind - SSL init. サーバ %1s : %2ul	SmLdapMessage::LdapConnMgrBindSSLInitFail	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。
SmDsLdapConnMgr Bind. サーバ %1s : %2ul。エラー %3i - %4s	SmLdapMessage::ErrorLdapConnMgrBind	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください (ポリシー サーバマシンから ping を実行してみてください)。
SmDsLdapConnMgr 例外 (ldap_init)。サーバ %1s : %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrInit	LDAP サーバへの接続中に予期しないエラーが発生しました。LDAP サーバおよびポートの設定を確認してください。
SmDsLdapConnMgr Exception (ldap_simple_bind_s)。サーバ %1s : %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrSimpleBind	LDAP サーバへの接続中に予期しないエラーが発生しました。LDAP サーバおよびポートの設定を確認してください。
SmDsLdapConnMgr Exception (ldapssl_init)。サーバ %1s : %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrSSLInit	SSL を使用して LDAP サーバに接続しているときに、予期しないエラーが発生しました。LDAP サーバおよびポートの設定を確認してください。サーバは SSL 用に設定されていますか。

エラー メッセージの内容	関数	説明
SmObjLdap で LDAP サーバ %1s にバインドできませんでした : %3s としての %2i。 LDAP エラー %4i - %5s	SmLdapMessage::SmObj-LdapFailToBindToLdapServer	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください (ポリシー サーバマシンから ping を実行してみてください)。
SmObjLdap で %1s への LDAP 接続を初期化できません 初期化できませんでした : %2i	SmLdapMessage::SmObj-LdapInitLdapConnFail	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください (ポリシー サーバマシンから ping を実行してみてください)。
SmObjLdap で %1s への SSL LDAP 接続を初期化できませんでした : %2i	SmLdapMessage::SmObj-LdapInitSSLFail	LDAP オプションを設定できません。ポリシー サーバシステム上の設定エラーが原因であると思われる。適切な LDAP ライブラリを使用していますか。
SmObjLdap で %1s を使用して SSL を初期化できませんでした	SmLdapMessage::SmObj-LdapInitSSLFail	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。
SmObjLdap で LDAP CONNECT_TIMEOUT オプションを設定できませんでした	SmLdapMessage::SmObj-LdapConnectTimeoutOptFail	LDAP オプションを設定できません。ポリシー サーバシステム上の設定エラーが原因であると思われる。適切な LDAP ライブラリを使用していますか。
SmObjLdap で LDAP PROTOCOL V3 オプションの設定に失敗しました	SmLdapMessage::SmObj-LdapProtocolV3OptFail	LDAP オプションを設定できません。ポリシー サーバシステム上の設定エラーが原因であると思われる。適切な LDAP ライブラリを使用していますか。

エラー メッセージの内容	関数	説明
SmObjLdap で LDAP RECONNECT オプションを設定できませんでした	SmLdapMessage::SmObj-LdapReconnectOptFail	LDAP オプションを設定できません。ポリシーサーバシステム上の設定エラーが原因であると思われる。適切な LDAP ライブラリを使用していますか。
SmObjLdap で LDAP THREAD_FN オプションを設定できませんでした	SmLdapMessage::SmObjLdap-ThreadFnOptFail	LDAP オプションを設定できません。ポリシーサーバシステム上の設定エラーが原因であると思われる。適切な LDAP ライブラリを使用していますか。
SmObjLdap で LDAP TIMELIMIT オプションを設定できませんでした	SmLdapMessage::SmObjLdap-TimeoutOptFail	LDAP オプションを設定できません。ポリシーサーバシステム上の設定エラーが原因であると思われる。適切な LDAP ライブラリを使用していますか。
SmObjLdap で LDAP_OPT_REFERRALS オプションを設定できませんでした	SmLdapMessage::SmObj-LdapOptReferralsFail	LDAP オプションを設定できません。ポリシーサーバシステム上の設定エラーが原因であると思われる。適切な LDAP ライブラリを使用していますか。
SmObjLdapConnMgr Bind - init。サーバ : %1s : %2ul	SmLdapMessage::SmObj-LdapConnMgrBindInitServer	ポリシーストア用に設定された LDAP サーバを初期化できませんでした。エラーメッセージの中で示された LDAP サーバをトラブルシューティングしてください。
SmObjLdapConnMgr Bind - SetOption CONNECT_TIMEOUT %1i。サーバ %2s : %3ul	SmLdapMessage::SmObj-LdapConnMgrBindSetOption-CONNECT_TIMEOUT	ポリシーストア用に設定された LDAP サーバで、LDAP_X_OPT_CONNECT_TIMEOUT オプション (Microsoft Active Directory SDK を使用しているときは LDAP_OPT_SEND_TIMEOUT) を設定できませんでした。エラーメッセージの中で示された LDAP サーバをトラブルシューティングしてください。

エラー メッセージの内容	関数	説明
SmObjLdapConnMgr Bind - SSL client init。サーバ : %1s : %2ul、証明書 DB : %3s	SmLdapMessage::SmObj-LdapConnMgrBindSSLclientinit	ポリシーストア用に設定された LDAP サーバへの SSL 接続のクライアント側の初期化に失敗しました。証明書データベースが正しく指定されているかどうかを確認してください。
SmObjLdapConnMgr Bind - SSL init。サーバ : %1s : %2ul	SmLdapMessage::SmObj-LdapConnMgrBindSSLinit	ポリシーストア用に設定された LDAP サーバを SSL 接続時に初期化できませんでした。エラーメッセージの中で示された LDAP サーバをトラブルシューティングしてください。
SmObjLdapConnMgr Bind。サーバ %1s : %2ul。エラー %3i - %4s	SmLdapMessage::SmObj-LdapConnMgrBindServerError	SiteMinder ポリシーサーバから、ポリシーストア用に設定された LDAP サーバにバインドできませんでした。詳細については、LDAP エラーメッセージを参照してください。ポリシーサーバで有効な LDAP 管理者認証情報が使用されているかどうかを確認してください。認証情報は、ポリシーサーバ管理コンソールの [データ] タブでリセットできます。
SmObjLdapConnMgr 例外 (ldap_init)。サーバ %1s : %2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap_init	ポリシーストア用に設定された LDAP サーバを初期化できませんでした。エラーメッセージの中で示された LDAP サーバをトラブルシューティングしてください。
SmObjLdapConnMgr 例外 (ldap_simple_bind_s)。サーバ %1s : %2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap_simple_bind_s	SiteMinder ポリシーサーバから、ポリシーストア用に設定された LDAP サーバにバインドできませんでした。ポリシーサーバで有効な LDAP 管理者認証情報が使用されているかどうかを確認してください。認証情報は、ポリシーサーバ管理コンソールの [データ] タブでリセットできます。

エラー メッセージの内容	関数	説明
SmObjLdapConnMgr 例外 (ldapssl_client_init)。 サーバ %1s : %2ul	SmLdapMessage::ExcpSm-ObjL dapConnMgrldap-ssl_client_init	ポリシーストア用に設定された LDAP サーバへの SSL 接続のクラ イアント側の初期化に失敗しま した。証明書データベースが正し く指定されているかどうかを確 認してください。
SmObjLdapConnMgr Exception (ldapssl_init). サーバ %1s : %2ul	SmLdapMessage::ExcpSm-ObjL dapConnMgrldapssl_init	ポリシーストア用に設定された LDAP サーバを SSL 接続時に初期 化できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティン グしてください。
サーバ/プロセスを終了して います.....	SmLdapMes-sage::Terminating Server-Processes	重要な再設定が行われるように、 サーバプロセスをシャットダウ ンします。ログ内の前のエラーを 参照してください。
%1i を超えるデータ エントリ を データストアから フェッチできません。¥n %2s LDAP_SIZELIMIT_EXCEEDED。エ ラーが検出されました。 ¥n %3s ディレクトリサーバ の sizelimit パラメータを再設 定するか、¥n %4s (ディレク トリサーバのマニュアルを 参照) ¥n %5s ディレクトリサーバをルー ト DN にバインドして、この 問題を解決してください。 ¥n %6s 例 : Iplanet / Netscape の場合は、ディレクトリサー バを「cn=Directory Manager」 としてバインドしてくださ い	SmLdapMessage::Unable-ToFet chMoreEntriesFromData-Sourc e	LDAP サーバの sizelimit パラメ ータの値を増やしてください。

エラー メッセージの内容	関数	説明
LDAP ディレクトリ タイプを取得できません	SmLdapMessage::Unable-ToRetrieveLdapDir	LDAP のベンダーとタイプを判別できません。ターゲットサーバはサポートされている LDAP サーバのうちの 1 つですか。処理は続行されますが、予期しないエラーがさらに発生する場合があります。
データ ストアからこれ以上データ エントリを検索してフェッチすることができません。¥n %1s LDAP_SIZELIMIT_EXCEEDED。エラーが検出されました。 ¥n %2s ディレクトリ サーバの sizelimit パラメータを再設定するか ¥n %3s (ディレクトリ サーバのマニュアルを参照)、¥n %4s ディレクトリ サーバをルート DN にバインドして、この問題を解決してください。¥n %5s 例: Iplanet / Netscape の場合は、ディレクトリ サーバを「cn=Directory Manager」としてバインドしてください	SmLdapMessage::Unable-ToSearchFetchMore-EntriesFromDataSource	ポリシー サーバで、ディレクトリ サーバのデータをこれ以上取得できません。可能な設定変更があるかどうか、エラー メッセージ テキストを参照してください。
rebindproc %1i の「arg」引数の値が想定外です	SmLdapMessage::UnexpectedValueArg-Argument	rebindproc コールで「arg」引数として不正な値が渡されています。rebindproc 関数は、自動リフェラル処理のための再バインド コールバックとして設定されます。代わりに、拡張リフェラル処理を有効にしてください。

エラー メッセージの内容	関数	説明
rebindproc_sm %1i の「arg」引数の値が不明です	SmLdapMessage::UnexpectedValueArg-Argument2	rebindproc_sm コールで「arg」引数として不正な値が渡されています。rebindproc_sm 関数は、自動リフェラル処理のための再バインドコールバックとして設定されます。代わりに、拡張リフェラル処理を有効にしてください。
rebindproc_sm %1i の「freeit」引数の値が不明です	SmLdapMessage::UnexpectedValueFreeit-Argument	rebindproc コールで freeit 引数として不正な値が渡されています（許可されるのは 0 または 1 だけです）。rebindproc 関数は、自動リフェラル処理のための再バインドコールバックとして設定されます。代わりに、拡張リフェラル処理を有効にしてください。
rebindproc_sm %1i の「freeit」引数の値が不明です	SmLdapMessage::UnexpectedValue-FreeitArgument2	rebindproc_sm コールで freeit 引数として不正な値が渡されています（許可されるのは 0 または 1 だけです）。rebindproc_sm 関数は、自動リフェラル処理のための再バインドコールバックとして設定されます（Microsoft Active Directory SDK を使用している場合を除きます）。代わりに、拡張リフェラル処理を有効にしてください。

ODBC

エラー メッセージの内容	関数	説明
IMS 環境を保存できませんで した。スキーマ サポートがな い 可能性があります	SmOdbcMessage::IMSSave-Err orMissingSchema	ポリシー サーバ データベースに は IMS をサポートするスキーマ がありません。
クエリ実行時の データベース エラー。不明の 障害です	SmOdbcMessage::Unknown-Fai lureDBExecQuery	指定された SQL ステートメント を実行しようとしているときに、 不明なエラーまたは例外が発生 しました。
クエリ実行時の データベース エラー。不明の 障害です	SmOdbcMessage::Unknown-Fai lureExecODBCQuery	指定された SQL ステートメント を実行しようとしているときに、 不明なエラーまたは例外が発生 しました。
クエリ実行時の データベース エラー。 エ ラー : %2s	SmOdbcMessage::DBError-Exec Query	指定された SQL ステートメント を実行しようとしているときに、 特定のエラーが発生しました。
クエリ実行時の データベース エラー。不明の 障害です	SmOdbcMessage::Unknown-Ex ceptionDBExecQuery	指定された SQL ステートメント を実行しようとしているときに、 不明なエラーまたは例外が発生 しました。
クエリ実行時の データベース エラー。 エ ラー : %1s	SmOdbcMessage::ErrorDB-Exec Query	SQL クエリを実行しようとしてい るときに、特定のエラーが発生し ました。
エスケープ文字取得中の データベース エラー。 エ ラー : %1s	SmOdbcMessage::DBError-Get EscapeChar	データベースで使用するエス ケープ文字を確立しようとして いるとき、エラーが発生しまし た。
エスケープ文字取得中の データベース エラー: 不明の 障害	SmOdbcMessage::Unknown-Ex ceptionDBGetEscapeChar	データベースで使用するエス ケープ文字を確立しようとして いるとき、不明の例外が発生しま した。

エラー メッセージの内容	関数	説明
DB 警告：データ値で切り捨てが行われます： '%1s' 実際の長さ： '%2u' 許可されている最大文字数： '%3u'	SmOdbcMessage::Data-TruncationInfo	指定された入力用のデータ値が、許可されている最大文字数を超えました。値は、指定されている最大文字数に切り捨てられます。
エラー コードは %1i、メッセージは '%2s' です	SmOdbcMessage::ErrorCodeAndMessage	指定されたデータ ソースに接続しようとしているとき、エラーが発生しました。問題を示すエラーコードとエラーメッセージが表示されます。
エラー コードは %1i です	SmOdbcMessage::ErrorCode	指定されたデータ ソースに接続しようとしているとき、エラーが発生しました。問題を示すエラーコードが表示されます。
OID '%1s' でユーザ ディレクトリのクエリをフェッチできませんでした	SmOdbcMessage::FailedTo-AllocMemForUserDir	指定の OID によって指定されるユーザ ディレクトリで使用するクエリを割り当てることができませんでした。
データ ソース '%1s' のいずれにも接続できませんでした	SmOdbcMessage::FailedTo-ConnectToAnyOfDataSources	指定されたユーザ ディレクトリのいずれにも接続できませんでした。
データ ソース '%1s' に接続できませんでした	SmOdbcMessage::FailedTo-ConnectToDataSource	指定されたデータ ソースに接続しようとしているとき、エラーが発生しました。
OID '%1s' でユーザ ディレクトリのクエリをフェッチできませんでした	SmOdbcMessage::FailedTo-FetchQueryForUserDir	指定の OID を使用してユーザ ディレクトリ クエリを検索できませんでした。
OID '%1s' でユーザ ディレクトリをフェッチできませんでした	SmOdbcMessage::FailedTo-FetchUserDir	指定の OID を使用してユーザ ディレクトリを検索できませんでした。
データベース '%1s' のデータソース名が見つかりませんでした	SmOdbcMessage::FailedTo-FindDataSource	指定された SiteMinder データベースの「ProviderNameSpace」レジストリ キーが見つかりませんでした。

エラー メッセージの内容	関数	説明
%1s のクエリ定義が見つかりませんでした	SmOdbcMessage::FailTo-FindQueryDefinition	指定されたクエリのクエリ定義が見つかりませんでした。
DataDirect ODBC ドライバを初期化できませんでした。ライブラリ '%2s' 内の関数 '%1s' をロードできません	DataDirectODBCDriverLoadFail	DataDirect ODBC ライブラリを初期化できませんでした。指定された初期化関数が、指定のライブラリ内に見つかりませんでした。
DataDirect ODBC ドライバを初期化できませんでした。ライブラリ '%1s' をロードできません	SmOdbcMessage::DataDirect-ODBCDriverLibLoadFail	指定された ODBC ライブラリをロードできませんでした。ライブラリパスに SiteMinder ODBC ライブラリ ディレクトリが含まれているかどうかを確認してください。
ODBC ブランド設定ライブラリ '%1s' をロードできませんでした	SmOdbcMessage::ODBC-BrandingLibraryLoadFail	SiteMinder によって使用されるようにブランド設定された ODBC ライブラリをロードできませんでした。
ODBC ブランド設定ライブラリ の名前を解決できませんでした	SmOdbcMessage::ODBC-BrandingLibraryNameResolve-Fail	ブランド設定ライブラリの名前を解決できませんでした。このライブラリ名は、 Netegrity/Siteminder/Database 以下のレジストリ内にある Key OdbcBrandingLib レジストリ キーから指定されます。
データベース「%1s」のデータベース レジストリ キーを取得できませんでした	SmOdbcMessage::FailedTo-RetrieveDBRegKeys	指定された SiteMinder データベースのレジストリ キー (データソース、ユーザ名、またはパスワード) のうちの 1 つが見つかりませんでした。
認証情報が無効であるか、'%1s' サーバ '%2s' に接続を試みているサーバが見つかりません	SmOdbcMessage::Unable-ToConnect	SiteMinderODBC データベースへのアクセスのために入力されたクレデンシャルが無効です。

エラー メッセージの内容	関数	説明
クエリ実行時の ODBC エラー ('%1s')。エラー : %2s	SmOdbcMessage::ErrorExec-ODBCQuery	指定された SQL ステートメントを実行しようとしているときに、特定の ODBC エラーが発生しました。
クエリ実行時の ODBC エラー。エラー : %1s	SmOdbcMessage::Error-ODBCQueryExec	SQL クエリを実行しようとしているときに、特定の ODBC エラーが発生しました。
クエリ実行時の ODBC エラー。不明の障害です	SmOdbcMessage::Unknown-ExceptionExecODBCQuery	ODBC データベースに対して SQL クエリを実行しようとしているときに、不明の例外が発生しました。

ディレクトリアクセス

メッセージ	メッセージ ID	説明
パス '%2s' で %1s に失敗しました	FuncFailForPath	ポリシー サーバで、カスタム プロバイダを使用してディレクトリ情報を取得できませんでした。
ADs EnumContainer に失敗しました。エラー %1xl。 %2s	ADsEnumContainerFailed	ポリシー サーバで、ADSI インターフェースからコンテナメンバを列挙できませんでした。
プロパティ '%1s' について ADs Get に失敗しました。エラー %2xl。 %3s	ADsGetFailForProperty	ポリシー サーバで、ADSI インターフェースからユーザプロパティを取得できませんでした。
ADs GetGroups に失敗しました。エラー %1xl。 %2s	ADsGetGroupsFail	ポリシー サーバで、ユーザグループを取得できませんでした。
プロパティ '%1s' について ADs Put に失敗しました。エラー %2xl。 %3s	ADsPutFailForProperty	ポリシー サーバで、ADSI インターフェースからユーザプロパティを設定できませんでした。
ADs put_Filter に失敗しました。エラー %1xl。 %2s	ADsPutFilterFailed	ポリシー サーバで、ADSI インターフェースから列挙フィルタを作成できませんでした。

メッセージ	メッセージ ID	説明
ADs Search に失敗しました。 エラー %1xl。 %2s	ADsSearchFail	ポリシー サーバで、ADSI インターフェイスから検索できませんでした。
ADsBuildEnumerator に失敗しました。 エラー %1xl。 %2s	ADsBuildEnumeratorFailed	ポリシー サーバで、ADSI インターフェイスからコンテナメンバを列挙できませんでした。
ADsBuildVarArrayStr に失敗しました。 エラー %1xl。 %2s	ADsBuildVarArrayStrFailed	ポリシー サーバで、ADSI インターフェイスから変数の配列を作成できませんでした。
ADsEnumerateNext に失敗しました。 エラー %xl。 %2s	ADsEnumerateNextFailed	ポリシー サーバで、ADSI インターフェイスからコンテナメンバを列挙できませんでした。
ADsGetObject に失敗しました。 エラー %1xl。 %2s	ADsGetObjectFail	ポリシー サーバで、ADSI インターフェイスからオブジェクトプロパティを取得できませんでした。
'%1s' で ADsOpenObject に '%1s'。 ADSI エラー %2xl。 %3s	ADsOpenObjectFailed	ポリシー サーバで、ADSI インターフェイスへのハンドルを作成できませんでした。
アフィリエイトの PropertyCollection が グループ名と一致していません	AffiliatePropertyCollection-GroupNameMismatch	ポリシー サーバで、ポリシーに対するアフィリエイトリレーションシップを検証できませんでした。アフィリエイトのプロパティコレクション名が、指定されたポリシー名に一致していません。
'%1s' 関数を使用してプロパティを フェッチできませんでした	PropertiesFetchFail	ポリシー サーバで、カスタムプロバイダからオブジェクトプロパティをフェッチできませんでした。
SmDsObj で例外が発生しました	SmDsObjUnknownException	ポリシー サーバで、DS プロバイダを検索できませんでした。ポリシー サーバプロセスによってプロバイダ共有ライブラリをロードできるかどうか確認してください。

メッセージ	メッセージ ID	説明
SmDsObj で例外が発生しました : %1s	SmDsObjException	ポリシー サーバで、DS プロバイダを検索できませんでした。ポリシー サーバプロセスによってプロバイダ共有ライブラリにアクセスできるかどうか確認してください。
アフィリエイトの PropertyCollections が見つかりませんでした	AffiliatePropertyCollectionsFail	ポリシー サーバで、アフィリエイト ドメインをフェッチできませんでした。ポリシー ストアの整合性を確認してください。
属性が見つかりませんでした	AttributeFindFail	ポリシー サーバで、指定されたユーザ属性が見つかりませんでした。
パスワードプロパティが見つかりませんでした	PasswordPropertyFindFail	ポリシー サーバで、指定されたアフィリエイトのパスワードが見つかりませんでした。
アフィリエイト ユーザとして機能している PropertySection でプロパティが見つかりませんでした	AffiliateUserPropertyIn-PropertySectionFindFail	ポリシー サーバで、指定されたアフィリエイト プロパティをフェッチできませんでした。
アフィリエイト ユーザ ディレクトリとして機能している Property-Collection が見つかりませんでした	ActingAffiliateUserDirProps-FindFail	ポリシー サーバで、アフィリエイト ドメインをフェッチできませんでした。ポリシー ストアの整合性を確認してください。
アフィリエイト ユーザ ディレクトリに PropertySection が見つかりませんでした	AffiliateUserPropertySection-FindFail	ポリシー サーバで、指定されたアフィリエイトを検索できませんでした。
アフィリエイト ユーザ ディレクトリに PropertySection が ユーザ ディレクトリ	InAffiliateUserDirPropsFindFail	ポリシー サーバで、アフィリエイト ドメインからアフィリエイトをフェッチできませんでした。ポリシー ストアの整合性を確認してください。

メッセージ	メッセージ ID	説明
ルートオブジェクトが見つかりませんでした	RootObjFindFail	ポリシーサーバで、アフィリエイトドメインが見つかりませんでした。SiteMinderの管理UIを使用したときにアフィリエイトオブジェクトが表示されるかどうか確認してください。
アフィリエイトのPropertyCollectionにユーザが見つかりませんでした	AffiliatePropertyCollection-UserFindFail	ポリシーサーバで、指定されたアフィリエイトを検索できませんでした。
カスタムディレクトリ API モジュール '%1s' を初期化できませんでした	CustomDirAPIModInitFail	ポリシーサーバで、カスタムプロバイダライブラリを初期化できませんでした。
カスタムディレクトリ API ライブラリ '%1s' をロードできませんでした。システムエラー： %2s	CustormDirAPILibLoadFail	ポリシーサーバで、カスタムプロバイダライブラリをロードできませんでした。ポリシーサーバプロセスによって適切なカスタムプロバイダライブラリにアクセスできるかどうか確認してください。
トンネルサービスライブラリ '%2s' 内の関数 '%1s' を API ライブラリ '%2s' 内の関数 '%1s' を解決できませんでした。システムエラー： %3s	CustormDirAPILibFuncResovl-Fail	ポリシーサーバで、カスタムプロバイダライブラリを初期化できませんでした。ポリシーサーバプロセスによって適切なカスタムプロバイダライブラリにアクセスできるかどうか確認してください。
ネームスペース ADSI では、Get Disabled State はサポートされていません	ADSIGetDisabledState-Supported	ポリシーサーバでは、ADSI インターフェースからのユーザ無効状態の取得をサポートしていません。

メッセージ	メッセージ ID	説明
カスタム ディレクトリ API ライブラリ「%2s」で関数「%1s」を使用できません。	CustomDirAPILibFuncNotFound	ポリシー サーバで、必要なメソッドの1つがカスタム プロバイダ ライブラリ内に見つかりませんでした。ポリシー サーバプロセスによって適切なカスタム プロバイダ ライブラリにアクセスできるかどうか確認してください。
ネームスペース LanMan では、パスワードの変更がサポートされていません	ADSINoPasswordChange	ポリシー サーバでは、ADSI インターフェースからのユーザパスワードの変更をサポートしていません。
ネームスペース LanMan では、パスワードの変更がサポートされていません	LanManPasswordChangeNotSupported	ポリシー サーバでは、LanMan プロバイダからのユーザパスワードの変更をサポートしていません。
QueryInterface (IID_IADsContainer) に失敗しました。 エラー %1s %2s %3i。 %4s	IID_IADsContainerFail	ポリシー サーバで、ADSI インターフェースからコンテナメンバを列挙できませんでした。
QueryInterface (IID_IADsContainer) に失敗しました。 エラー %1xl。 %2s	QueryInterfaceIID_IADsContainerFail	ポリシー サーバで、ADSI インターフェースからコンテナメンバを列挙できませんでした。
QueryInterface (IID_IADsUser) に失敗しました。エラー %1xl。 %2s	IID_IADsUserFail	ポリシー サーバで、ユーザグループを取得できませんでした。
QueryInterface (IID_IDirectorySearch) に失敗しました。エラー %1xl。 %2s	IID_IDirectorySearchFail	ポリシー サーバで、ADSI インターフェースから検索できませんでした。
ネームスペース ADSI では、Set Disabled State はサポートされていません	ADSISetDisabledState-Supported	ポリシー サーバでは、ADSI インターフェースからのユーザ無効状態の設定をサポートしていません。

メッセージ	メッセージ ID	説明
サポートされていない関数がコールされました： SmDirAddEntry	UnsupportedFuncCallSmDir-AddEntry	SmDirAddEntry 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirAddMemberToGroup	UnsupportedFuncCallSmDir-AddMemberToGroup	SmDirAddMemberToGroup 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirAddMemberToRole	UnsupportedFuncCallSmDir-AddMemberToRole	SmDirAddMemberToRole 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirChangeUserPassword	UnsupportedFuncCallSmDir-ChangeUserPassword	SmDirChangeUserPassword 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirGetGroupMembers	UnsupportedFuncCallSmDir-GetGroupMembers	SmDirGetGroupMembers 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirGetRoleMembers	UnsupportedFuncCallSmDir-GetRoleMembers	SmDirGetRoleMembers 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirGetUserAttrMulti	UnsupportedFuncCallSmDir-GetUserAttrMulti	SmDirGetUserAttrMulti 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirGetUserClasses	UnsupportedFuncCallSmDir-GetUserClasses	SmDirGetUserClasses 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirGetUserGroups	UnsupportedFuncCallSmDir-GetUserGroups	SmDirGetUserGroups 関数はアフィリエイトプロバイダライブラリによってサポートされていません。

メッセージ	メッセージ ID	説明
サポートされていない関数がコールされました： SmDirGetUserProperties	UnsupportedFuncCallSmDir-GetUserProperties	SmDirGetUserProperties 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirGetUserRoles	UnsupportedFuncCallSmDir-GetUserRoles	SmDirGetUserRoles 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirLookup	UnsupportedFuncCallSmDir-Lookup	SmDirLookup 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirRemoveEntry	UnsupportedFuncCallSmDir-RemoveEntry	SmDirRemoveEntry 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirRemoveMemberFromGroup	UnsupportedFuncCallSmDir-RemoveMemberFromGroup	SmDirRemoveMemberFromGroup 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirRemoveMemberFromRole	UnsupportedFuncCallSmDir-RemoveMemberFromRole	SmDirRemoveMemberFromRole 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirSearch	UnsupportedFuncCallSmDir-Search	SmDirSearch 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirSearchCount	UnsupportedFuncCallSmDir-SearchCount	SmDirSearchCount 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirSetUserAttr	UnsupportedFuncCallSmDir-SetUserAttr	SmDirSetUserAttr 関数はアフィリエイトプロバイダライブラリによってサポートされていません。

メッセージ	メッセージ ID	説明
サポートされていない関数がコールされました： SmDirSetUserAttrMulti	UnsupportedFuncCallSmDir-SetUserAttrMulti	SmDirSetUserAttrMulti 関数はアフィリエイトプロバイダライブラリによってサポートされていません。
サポートされていない関数がコールされました： SmDirSetUserDisabledState	UnsupportedFuncCallSmDir-SetUserDisabledState	SmDirSetUserDisabledState 関数はアフィリエイトプロバイダライブラリによってサポートされていません。

トンネル

エラー メッセージの内容	関数	説明
不正なセキュリティハンドシェイクが行われようとなりました。ハンドシェイクエラー： 不明です	SmTunnelMessage::Hand-shakeAttemptError	定義済みのシステムエラーが発生したため、クライアント/サーバセキュリティハンドシェイクに失敗しました。
ハンドシェイク中、クライアントはデータを正常に暗号化できません	SmTunnelMessage::Client-EncryptFail	クライアント/サーバセキュリティハンドシェイクに失敗しました。クライアントはそのハンドシェイクメッセージを適切に暗号化できませんでした。
ハンドシェイク試行中に例外がキャッチされました	SmTunnelMessage::Excpln-HandshakeAttempt	クライアント/サーバセキュリティハンドシェイク中、未定義のエラーが発生しました。
トンネルサービスライブラリ「%1s」をロードできませんでした。 %2s	SmTunnelMessage::Tunnel-ServiceLibInitFail	リクエストされたトンネルサービスライブラリが初期化に失敗しました。
トンネルサービスライブラリ「%1s」をロードできませんでした。システムエラー： %2s	SmTunnelMessage::Tunnel-ServiceLibLoadFail	リクエストされたトンネルサービスライブラリをロードできませんでした。

エラー メッセージの内容	関数	説明
トンネル サービス ライブラリ '%2s' 内の関数 '%1s' を解決できませんでした。システムエラー : %3s	SmTunnelMessage::Tunnel-ServiceLibFuncResolveFail	システムエラーが発生したため、リクエストされた関数が、リクエストされたトンネル サービス ライブラリ内で見つかりませんでした。
ハンドシェイク エラー: hello メッセージ内のホスト名が不正です	SmTunnelMessage::Hand-shake ErrorBadHostname	クライアント/サーバセキュリティ ハンドシェイクに失敗しました。クライアントからサーバへの初期メッセージに不正なホスト名が含まれていました。
ハンドシェイク エラー: hello メッセージ内のバージョン番号が不正です	SmTunnelMessage::Hand-shake ErrorBadVersionNo	クライアント/サーバセキュリティ ハンドシェイクに失敗しました。クライアントからサーバへの初期メッセージに不正なバージョン番号が含まれていました。
ハンドシェイク エラー: クライアントの hello メッセージを受け取れませんでした。ソケットエラー %1i	SmTunnelMessage::Hand-shake ErrorToReceiveClientACK	クライアント/サーバセキュリティ ハンドシェイクに失敗しました。サーバからクライアントへの初期メッセージが、クライアントによって受信確認されませんでした。
ハンドシェイク エラー: クライアントの hello メッセージを受け取れませんでした。クライアントが切断されました	SmTunnelMessage::Hand-shake ErrorClientHelloNot-Receive	クライアント/サーバセキュリティ ハンドシェイクに失敗しました。クライアントが初期メッセージを送信する前に接続を切断しました。
ハンドシェイク エラー: クライアントの hello メッセージを受け取れませんでした。ソケットエラー %1i	SmTunnelMessage::Hand-shake ErrorSocketError	クライアント/サーバセキュリティ ハンドシェイクに失敗しました。クライアントが初期メッセージを送信しませんでした。

エラー メッセージの内容	関数	説明
ハンドシェイク エラー: サーバの hello メッセージを送信できませんでした。ソケット エラー %1i	SmTunnelMessage::Hand-ShakeErrorInSendSocketError	クライアント/サーバセキュリティ ハンドシェイクに失敗しました。通信障害が発生したため、サーバからクライアントへの初期メッセージを送信できませんでした。
ハンドシェイク エラー: このクライアントの共有秘密キーが不正です	SmTunnelMessage::Hand-shakeErrorSharedSecret-Incorrect	クライアント/サーバセキュリティ ハンドシェイクに失敗しました。クライアントからサーバへの初期メッセージに不正な共有秘密キーが含まれていました。
このポリシー サーババージョンは 3.6 エージェントをサポートしていません	SmTunnelMessage::Agent-VersionNotSupported	クライアント/サーバセキュリティ ハンドシェイクに失敗しました。このバージョンのクライアントは、トンネル接続を確立することを許可されていません。
トンネル コーラーはリクエスト %1ul の実行を許可されていません	SmTunnelMessage::Tunnel-CallerExecDenied	トンネル コールで、禁止されているリクエストが行われようとしていました。
予期しないハンドシェイク エラー	SmTunnelMessage::Hand-shakeErrorUnexpected	クライアント/サーバセキュリティ ハンドシェイクが、予期しない理由で失敗しました。
トンネル ライブラリの発行中、予期しない例外がキャッチされました	SmTunnelMessage::Unknown-ExceptionPublishTunnelLibs	トンネル サービス ライブラリがパブリッシング インターフェースを使用してそれ自身を記述しているときに、不明の例外が発生しました。