

Symantec Endpoint Protection Manager データベーススキーマリ ファレンス

Symantec Endpoint Protection
および Symantec Network
Access Control 用



Symantec Endpoint Protection Manager データベーススキーマリファレンス

本書で説明するソフトウェアは、使用許諾契約に基づいて提供され、その内容に同意する場合にのみ使用することができます。

Documentation version 11.00.06.00.00

登録商標

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec、Symantec ロゴ、Bloodhound、Confidence Online、Digital Immune System、LiveUpdate、Norton、Sygate、TruScan は、Symantec Corporation または同社の米国およびその他の国における関連会社の商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

Symantec 製品には、特定のサードパーティ製ソフトウェアが配布、組み込み、または同梱されている場合があります。また、本製品のインストールおよび使用にともない、サードパーティ製ソフトウェアの使用を推奨する場合があります。このライセンス対象ソフトウェアには、オープンソースのフリーウェアライセンスで利用可能なサードパーティのソフトウェアプログラム（「サードパーティプログラム」）を含めることができます。本ソフトウェアに付随する使用許諾契約では、オープンソースのフリーウェアライセンスでお客様が有することのできる権利または義務は変更されないものとします。サードパーティのソフトウェアの著作権に関する情報については、本製品に付属のサードパーティ製ソフトウェアのファイルを参照してください。

本書に記載する製品は、使用、コピー、頒布、逆コンパイルおよびリバース・エンジニアリングを制限するライセンスに基づいて頒布されています。Symantec Corporation からの書面による許可なく本書を複製することはできません。

Symantec Corporation が提供する技術文書は Symantec Corporation の著作物であり、Symantec Corporation が保有するものです。保証の免責: 技術文書は現状有姿で提供され、Symantec Corporation はその正確性や使用について何ら保証いたしません。技術文書またはこれに記載される情報はお客様の責任にてご使用ください。本書には、技術的な誤りやその他不正確な点を含んでいる可能性があります。Symantec は事前の通知なく本書を変更する権利を留保します。

本ソフトウェアは、FAR 12.212 の規定によって商業用コンピュータソフトウェアと見なされ、FAR 52.227-19 「Commercial Computer Software - Restricted Rights」、DFARS 227.7202 「Rights in Commercial Computer Software or Commercial Computer Software Documentation」、その他の後継規制の規定により制限された権利の対象となります。米国政府による本ソフトウェアの使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

弊社製品に関して、当資料で明示的に禁止、あるいは否定されていない利用形態およびシステム構成などについて、これを包括的かつ暗黙的に保証するものではありません。ま

た、弊社製品が稼動するシステムの整合性や処理性能に関しても、これを暗黙的に保証するものではありません。これらの保証がない状態で、弊社製品の導入、稼動、展開した結果として直接的、あるいは間接的に発生した損害等についてこれが補償されることはありません。製品の導入、稼動、展開にあたっては、お客様の利用目的に合致することを事前に十分に検証および確認いただく前提で、計画および準備をお願いします。

スキーマテーブル

この文書では以下の項目について説明しています。

- **Symantec Endpoint Protection Manager** のデータベーススキーマについて
- データベースビューの目的
- 実際の処理のスキーマ (ACTUALACTION テーブル)
- 管理者ユーザーのスキーマ (ADMINUSER テーブル)
- エージェント動作ログのスキーマ (AGENT_BEHAVIOR_LOG_1 テーブルと AGENT_BEHAVIOR_LOG_2 テーブル)
- エージェントパケットログのスキーマ (AGENT_PACKET_LOG_1 テーブルと AGENT_PACKET_LOG_2 テーブル)
- エージェントセキュリティログのスキーマ (AGENT_SECURITY_LOG_1 テーブルと AGENT_SECURITY_LOG_2 テーブル)
- エージェント状態のスキーマ (AGENTSTATUS テーブル)
- エージェントシステムログのスキーマ (AGENT_SYSTEM_LOG_1 テーブルと AGENT_SYSTEM_LOG_2 テーブル)
- エージェントトラフィックログのスキーマ (AGENT_TRAFFIC_LOG_1 テーブルと AGENT_TRAFFIC_LOG_2 テーブル)
- 警告フィルタのスキーマ (ALERTFILTER テーブル)
- 警告メッセージのスキーマ (ALERTMSG テーブル)
- 警告のスキーマ (ALERTS テーブル)
- 異常検出のスキーマ (ANOMALYDETECTION テーブル)
- 異常検出の操作のスキーマ (ANOMALYDETECTIONOPERATION テーブル)
- 異常検出の種類のスキーマ (ANOMALYDETECTIONTYPE テーブル)
- 異常検出のスキーマ (ANOMALYDETECTIONS テーブル)

- 異常修復のスキーマ (ANOMALYREMEDIATION テーブル)
- 異常修復の操作のスキーマ (ANOMALYREMEDIATIONOPERATION テーブル)
- 異常修復の種類スキーマ (ANOMALYREMEDIATIONTYPE テーブル)
- 異常修復のスキーマ (ANOMALYREMEDIATIONS テーブル)
- 監査レポートのスキーマ (AUDIT_REPORT テーブル)
- 基本メタデータのスキーマ (BASIC_METADATA テーブル)
- 動作レポートのスキーマ (BEHAVIOR_REPORT テーブル)
- バイナリファイルのスキーマ (BINARY_FILE テーブル)
- コマンドのスキーマ (COMMAND テーブル)
- コマンドレポートのスキーマ (COMMAND_REPORT テーブル)
- コンプライアンスレポートのスキーマ (COMPLIANCE_REPORT テーブル)
- コンピュータアプリケーションのスキーマ (COMPUTER_APPLICATION テーブル)
- データハンドラのスキーマ (DATA_HANDLER テーブル)
- エンフォーサクライアントログ 1 と 2 のスキーマ (ENFORCER_CLIENT_LOG_1 テーブルと ENFORCER_CLIENT_LOG_2 テーブル)
- エンフォーサシステムログ 1 と 2 のスキーマ (ENFORCER_SYSTEM_LOG_1 テーブルと ENFORCER_SYSTEM_LOG_2 テーブル)
- エンフォーサトラフィックログ 1 と 2 のスキーマ (ENFORCER_TRAFFIC_LOG_1 テーブルと ENFORCER_TRAFFIC_LOG_2 テーブル)
- ファイアウォールレポートのスキーマ (FIREWALL_REPORT テーブル)
- GUI パラメータのスキーマ (GUIPARAMS テーブル)
- GUP リストのスキーマ (GUP_LIST テーブル)
- 履歴のスキーマ (HISTORY テーブル)
- 履歴設定のスキーマ (HISTORYCONFIG テーブル)
- ホームページ設定のスキーマ (HOMEPAGECONFIG テーブル)
- HPP 警告のスキーマ (HPP_ALERTS テーブル)
- HPP アプリケーションのスキーマ (HPP_APPLICATION テーブル)
- ID マップのスキーマ (IDENTITY_MAP テーブル)
- 現在のリスクのインベントリのスキーマ (INVENTORYCURRENTRISK テーブル)
- 現在のウイルスのインベントリのスキーマ (INVENTORYCURRENTVIRUS テーブル)

- SCF インベントリのスキーマ (SCFINVENTORY テーブル)
- インベントリレポートのスキーマ (INVENTORYREPORT テーブル)
- 検出された LAN デバイスのスキーマ (LAN_DEVICE_DETECTED テーブル)
- 除外された LAN デバイスのスキーマ (LAN_DEVICE_EXCLUDED テーブル)
- レガシーエージェントのスキーマ (LEGACY_AGENT テーブル)
- ローカルメタデータのスキーマ (LOCAL_METADATA テーブル)
- ログ設定のスキーマ (LOG_CONFIG テーブル)
- 通知のスキーマ (NOTIFICATION テーブル)
- 通知警告のスキーマ (NOTIFICATIONALERTS テーブル)
- パターンのスキーマ (PATTERN テーブル)
- レポートのスキーマ (REPORTS テーブル)
- スキャンレポートのスキーマ (SCANREPORT テーブル)
- スキャンのスキーマ (SCANS テーブル)
- SE グローバルのスキーマ (SE_GLOBAL テーブル)
- SEM エージェントのスキーマ (SEM_AGENT テーブル)
- SEM アプリケーションのスキーマ (SEM_APPLICATION テーブル)
- SEM クライアントのスキーマ (SEM_CLIENT テーブル)
- SEM コンプライアンス基準のスキーマ (SEM_COMPLIANCE_CRITERIA テーブル)
- SEM コンピュータのスキーマ (SEM_COMPUTER テーブル)
- SEM コンテンツのスキーマ (SEM_CONTENT テーブル)
- SEM ジョブのスキーマ (SEM_JOB テーブル)
- シリアル番号のスキーマ (SERIAL_NUMBERS テーブル)
- サーバー管理ログ 1 と 2 のスキーマ (SERVER_ADMIN_LOG_1 テーブルと SERVER_ADMIN_LOG_2 テーブル)
- サーバークライアントログ 1 と 2 のスキーマ (SERVER_CLIENT_LOG_1 テーブルと SERVER_CLIENT_LOG_2 テーブル)
- サーバーエンフォーサログ 1 と 2 のスキーマ (SERVER_ENFORCER_LOG_1 テーブルと SERVER_ENFORCER_LOG_2 テーブル)
- サーバーポリシーログ 1 と 2 のスキーマ (SERVER_POLICY_LOG_1 テーブルと SERVER_POLICY_LOG_2 テーブル)

- サーバーシステムログ 1 と 2 のスキーマ (SERVER_SYSTEM_LOG_1 テーブルと SERVER_SYSTEM_LOG_2 テーブル)
- システムレポートのスキーマ (SYSTEM_REPORT テーブル)
- システム状態のスキーマ (SYSTEM_STATE テーブル)
- 脅威レポートのスキーマ (THREATREPORT テーブル)
- バージョンのスキーマ (VERSION テーブル)
- ウイルスのスキーマ (VIRUS テーブル)
- ウイルスカテゴリのスキーマ (VIRUSCATEGORY テーブル)

Symantec Endpoint Protection Manager のデータベーススキーマについて

Symantec Endpoint Protection Manager データベースはシマンテック製ソフトウェアと関連付けられたセキュリティ情報にかかわるすべての情報を格納します。情報は一連のテーブル、データベーススキーマに格納されます。

データタイプはデータの物理的構成を表します。

次の種類のデータがデータベースで使われます。

bigint	char
int	varchar
tinyint	nvarchar
datetime	varbinary

一部のデータタイプでは、カッコ内にフィールドの物理的な長さが含まれます。たとえば、char(24) は 24 文字の長さの文字フィールドを示します。

フィールド名に付いたアスタリスクは、そのフィールドがテーブルの主キーとして機能することを示します。主キーはテーブルのすべての行を重複なく識別する 1 つの列または列の組です。主キーはヌル値を含みません。2 つの行が同じ主キーの値を持つことはできません。したがって、主キーの値は常に単一の行を重複なく識別します。複数のキーによってテーブルの行を重複なく識別できます。各キーはそれぞれ候補キーと呼ばれます。1 つの候補キーのみをテーブルの候補キーとして選択でき、ほかの候補キーはすべて代替キーになります。

正規化されたテーブルでは、行のすべてのデータ値は主キーに依存しています。たとえば、主キーとして EmployeeID がある正規化された従業員テーブルでは、すべての列には特定の従業員に関するデータが含まれます。このテーブルに DepartmentName 列は含まれません。部門の名前は Employee ID ではなく、Department ID に依存しているからです。

Symantec Endpoint Protection Manager データベースにはデータテーブルのほかにもビューも含まれており、さまざまな方法でテーブルを表示できます。多くのビューには人が読み取り可能な IP アドレス情報が含まれています。

p.9 の「データベースビューの目的」を参照してください。

データベースビューの目的

Symantec Endpoint Protection Manager データベースにはビューが含まれており、さまざまな方法でデータテーブルを表示できます。ビューには、テーブルと区別するために、名前の先頭に英字 V が付いています。次の表に、ビューと各ビューの目的を示します。

アスタリスク(*)が付いたビューは、人が読み取り可能な IP アドレス情報を提供します。これらのビューには、xxx_TEXT という名前の、人が読み取り可能な列が含まれています。これらの列は、人が読み取り可能でないフィールドに対応しています。たとえば、DNS_SERVER1_TEXT に対応する元のフィールドは、ビュー V_SEM_COMPUTER の人が読み取り可能でないフィールド DNS_SERVER1 です。

表 1-1 データベースビューの目的

表示	目的
V_AGENT_BEHAVIOR_LOG	エージェントのクライアント活動をクエリーする
V_AGENT_PACKET_LOG*	エージェントのパケットトラフィックイベントをクエリーする
V_AGENT_SECURITY_LOG*	エージェントのセキュリティイベントをクエリーする
V_AGENT_SYSTEM_LOG	エージェントのシステムイベントをクエリーする
V_AGENT_TRAFFIC_LOG*	エージェントのトラフィックのイベントをクエリーする
V_ALERTS*	リスクと TruScan のイベントをクエリーする(人が読み取り可能な IP アドレス情報を含む)
V_ENFORCER_CLIENT_LOG	エンフォースアのクライアント活動をクエリーする
V_ENFORCER_SYSTEM_LOG	エンフォースアのシステム活動をクエリーする
V_ENFORCER_TRAFFIC_LOG*	エンフォースアのトラフィック活動をクエリーする
V_LAN_DEVICE_DETECTED*	検出済みデバイスをクエリーする(人が読み取り可能な IP アドレス情報を含む)
V_LAN_DEVICE_EXCLUDED*	既知のデバイスをクエリーする(人が読み取り可能な IP アドレス情報を含む)

表示	目的
V_SECURITY_VIEW	クロステクノロジーのセキュリティイベントをクエリーする
V_SEM_COMPUTER*	コンピュータ情報をクエリーする (人が読み取り可能な IP アドレス情報を含む)
V_SERVER_ADMIN_LOG	サーバーでの管理者活動をクエリーする
V_SERVER_CLIENT_LOG	サーバーでのクライアント活動をクエリーする
V_SERVER_ENFORCER_LOG	サーバーでのエンフォース活動をクエリーする
V_SERVER_POLICY_LOG	サーバーでのポリシー変更活動をクエリーする
V_SERVER_SYSTEM_LOG	サーバーでのシステム活動をクエリーする

実際の処理のスキーマ (ACTUALACTION テーブル)

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_ACTUALACTIONとして機能することを示します。

表 1-2 実際の処理のスキーマ

データベースのフィールド名	コメント	データタイプ
ACTUALACTION_IDX*	主キー (示されている 1 から 500 までのいずれか)	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
ACTUALACTION		varchar(255), NULL

データベースのフィールド名	コメント	データタイプ
	<p>次のルックアップで使用されたハードコードされた英語の文字列:</p> <p>-1 = 処理が無効です</p> <p>1 = 検疫しました</p> <p>2 = 名前を変更しました</p> <p>3 = 削除しました</p> <p>4 = 放置</p> <p>5 = クリーニングしました</p> <p>6 = クリーニングまたはマクロを削除しました</p> <p>7 = 保存しました</p> <p>9 = 元の場所に戻しました</p> <p>10 = 名前を元に戻しました</p> <p>11 = 元に戻しました</p> <p>12 = 不良</p> <p>13 = バックアップ</p> <p>14 = 修復の保留</p> <p>15 = 部分的に修復しました</p> <p>16 = 再起動保留のプロセス終了</p> <p>17 = 除外しました</p> <p>18 = 再起動処理</p> <p>19 = 削除によってクリーニングされました</p> <p>20 = アクセスが拒否されました</p> <p>21 = プロセスを終了</p> <p>22 = 利用可能な修復なし</p> <p>23 = すべての処理が失敗しました</p> <p>98 = 疑いあり</p> <p>99 = 詳細保留</p>	

データベースのフィールド名	コメント	データタイプ
	110 = 商用アプリケーションリスト を使って検出しました	
	111 = ファイル名を使った強制検 出	
	1000 = ファイルハッシュを使った 強制検出	
	500 = 適用可能ではありません	

管理者ユーザーのスキーマ (ADMINUSER テーブル)

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_ADMINUSERとして機能することを示します。

表 1-3 管理者ユーザーのスキーマ

データベースのフィールド名	コメント	データタイプ
USER_ID*	主キー、ログオンユーザー ID	char(32), NOT NULL
USER_NAME	管理者のユーザー名	NVARCHAR(255), varchar(255), NOT NULL
DOMAIN_ID	現在ログインしているドメインのGUID	char(32), NOT NULL
AUTOREFRESH	すべてのログ (コンピュータの状態、通知、スキャンなど) のためのユーザー定義の自動更新の値	int, NOT NULL
LASTCHANGE	ユーザーがコンソールにアクセスした最終日時	int, NOT NULL
LASTSPMTIME	アプリケーションサーバーが正常に稼動していた最終日時	int, NOT NULL

エージェント動作ログのスキーマ (AGENT_BEHAVIOR_LOG_1 テーブルと AGENT_BEHAVIOR_LOG_2 テーブル)

エージェント動作ログのデータテーブルは Symantec Network Access Control で使われません。

表 1-4 はエージェント動作ログのデータベーススキーマを示しています。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

キーは I_AGENT_BEHAVIOR_LOG_1_LOG_IDX または I_AGENT_BEHAVIOR_LOG_2_LOG_IDX です。LOG_IDX フィールドは重複のないテーブルの識別子として機能しますが、テーブルの主キーとしては形式的に分類されません。このフィールドにインデックスがありますが、主キーインデックスではありません。このテーブルに主キーはありません。

表 1-4 エージェント動作ログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	ログが属するドメインの GUID	char(32), NOT NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL
GROUP_ID	ログが属するグループの GUID	char(32), NOT NULL
COMPUTER_ID	エージェントログと関連付けられたクライアントコンピュータの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
EVENT_ID	Symantec Endpoint Protection エージェントからのイベント ID 有効な値は次の通りです。 501 = アプリケーション制御ドライバ 502 = アプリケーション制御ルール 999 = 変更対策	int, NOT NULL
EVENT_TIME	イベント生成された日時(グリニッジ標準時)	bigint, NOT NULL
SEVERITY	イベントの重要性 0 は最も深刻です	int, NOT NULL
AGENT_ID	エージェントの GUID	char(32), NULL
HARDWARE_KEY	コンピュータハードウェアの情報のハッシュ	char(32), NULL
HOST_NAME	クライアントコンピュータのホスト名	nvarchar(256), varchar(256), NULL
ACTION	有効な値には次のものはありません。 0 = 許可する 1 = 遮断 2 = 確認 3 = 続行 4 = 終了	int, NULL
TEST_MODE	このルールがテストモードで動作したか 0 = いいえ、その他 = はい	int, NULL
DESCRIPTION	遮断された動作	nvarchar(256), varchar(256), NULL

データベースのフィールド名	コメント	データタイプ
VAPI_NAME	遮断された API	nvarchar(256), varchar(256), NULL
ENCODED_API_NAME		nvarchar(256), varchar(256), NULL
BEGIN_TIME	セキュリティの問題の開始日時	bigint, NULL
END_TIME	セキュリティの問題の終了日時。 シマンテック社が、UDPなどのトラフィックの厳密な終了日時を検出できない場合があるため、終了日時は省略可能なフィールドです。そのような場合、終了日時は開始日時に等しいです。	bigint, NULL
RULE_ID	イベントによってトリガされるルールのID。ルールIDがセキュリティルールで指定されていなければ常に0です。フィールドはセキュリティルールのトラブルシューティングに有用です。複数のルールが一致すれば、RULE_IDはPacketProcでの最終決定があるルールをログに記録します (pass/block/drop)。	char(32), NULL
RULE_NAME	イベントによってトリガされるルールの名前。ルール名がセキュリティルールで指定されていなければ常に空の文字列です。これもトラブルシューティング用です。理論的には、IDによってIT管理者はルールを区別できます。ただし、名前によってユーザーは、使うことができるルールを直接的に知ることができます。	nvarchar(256), varchar(256), NULL
CALLER_PROCESS_ID	ログ記録をトリガするプロセスのID	bigint, NULL

データベースのフィールド名	コメント	データタイプ
CALLER_PROCESS_NAME	関係するアプリケーションの絶対パス名。アプリケーションが不明、オペレーティングシステムが含まれている、アプリケーションが含まれていない、のいずれかの場合は空になります。同様に、プロファイルが「RAWトラフィックログでアプリケーション名をログに記録しない」になっているような場合は空になります。	nvarchar(256), varchar(256), NULL
CALLER_RETURN_ADDRESS	呼び出し側の戻りアドレス。このフィールドによって、ソフトウェアは API の呼び出しを可能にする呼び出しモジュールの検出が可能です。	bigint, NULL
CALLER_RETURN_MODULE_NAME	呼び出し側のモジュール名。詳しくは「CallerReturnAddress」フィールドを参照してください。	nvarchar(256), varchar(256), NULL
PARAMETER	API の呼び出しで使用されたパラメータ。各パラメータは STRING 形式に変換され、1 つの空白文字で区切られています。文字列内の二重引用符文字はバックスラッシュ (¥) 文字によってエスケープされます。	nvarchar(256), varchar(256), NULL
ALERT	ALERT は、サーバーでの警告通知処理中にこのイベントが数えられるかどうかを示します。イベントが改変対策によってログに記録される場合、ALERT は True です。そうでない場合は false です。 有効な値は次の通りです。 True = 1 False = 0	int, NULL

データベースのフィールド名	コメント	データタイプ
SEND_SNMP_TRAP	SEND_SNMP_TRAP は送信 SNMP トラップ処理を反映します。send が true の場合、SEND_SNMP_TRAP は true です。	tinyint, NULL
USER_NAME	ログオンユーザー名	nvarchar(256), varchar(256), NULL
DOMAIN_NAME	ログオン (Windows) ドメイン名	nvarchar(256), varchar(256), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL
REPETITION	集計 (ダンパー) によるイベントの繰り返し	int, NOT NULL
LOG_IDX*	ログインデックスの重複のない ID	char(32), NULL

エージェントパケットログのスキーマ (AGENT_PACKET_LOG_1 テーブルと AGENT_PACKET_LOG_2 テーブル)

エージェントパケットログのデータテーブルは Symantec Network Access Control で使われません。

表 1-5 はエージェントパケットログのデータベーススキーマを示しています。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理

サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

キーは I_AGENT_PACKET_LOG_1_LOG_IDX または I_AGENT_PACKET_LOG_2_LOG_IDX です。LOG_IDX フィールドは重複のないテーブルの識別子として機能しますが、テーブルの主キーとしては形式的に分類されません。このフィールドにインデックスがありますが、主キーインデックスではありません。このテーブルに主キーはありません。

表 1-5 エージェントパケットログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	ログが属するドメインの GUID	char(32), NOT NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL
GROUP_ID	ログが属するグループの GUID	char(32), NOT NULL
COMPUTER_ID	エージェントパケットログと関連付けられたクライアントコンピュータの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
EVENT_ID	Symantec Endpoint Protection エージェントからのイベント ID 401 = Raw イーサネット	int, NOT NULL
EVENT_TIME	イベント生成された日時(グリニッジ標準時)	bigint, NOT NULL
AGENT_ID	エージェントの GUID	char(32), NULL
HARDWARE_KEY	コンピュータハードウェアの情報のハッシュ	char(32), NULL

データベースのフィールド名	コメント	データタイプ
HOST_NAME	クライアントコンピュータのホスト名	nvarchar(256), varchar(256), NULL
LOCAL_HOST_IP	ローカルコンピュータの IP アドレス (IPv4)	bigint, NULL
REMOTE_HOST_IP	リモートコンピュータの IP アドレス (IPv4)	bigint, NULL
REMOTE_HOST_NAME	リモートコンピュータの名前。名前解決が失敗した場合、空であることがあります。	nvarchar(64), varchar(64), NULL
LOCAL_PORT	ローカルコンピュータの TCP/UDP ポート (ホストバイト順)。TSE_TRAFFIC_TCP と TSE_TRAFFIC_UDP のみで有効です。そうでない場合は、常にゼロです。	int, NULL
REMOTE_PORT	リモートコンピュータの TCP/UDP ポート (ホストバイト順)。TSE_TRAFFIC_TCP と TSE_TRAFFIC_UDP のみで有効です。そうでない場合は、常にゼロです。	int, NULL
TRAFFIC_DIRECTION	トラフィックの方向。Enum (不明 = 0、インバウンド = 1、アウトバウンド = 2)	tinyint, NULL
BLOCKED	トラフィックが遮断されたかどうか。有効な値は次の通りです。 Yes = 1 No = 0	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
APP_NAME	関係するアプリケーションの絶対パス名。不明なアプリケーションが関係するか、アプリケーションが関係しない場合は、空であることがあります。たとえば、 Ping of Death サービス拒否攻撃は、オペレーティングシステムを攻撃するので、 AppName がありません。	nvarchar(256), varchar(256), NULL
ALERT	ALERT はプロファイル処理の警告属性を反映します。サーバー側通知の生成に関してイベントが考慮されるようにネットワーク脅威防止ポリシーで指定される場合、 ALERT フィールドは 1 に設定されます。 有効な値は次の通りです。 Yes = 1 No = 0	int, NULL
SEND_SNMP_TRAP	SEND_SNMP_TRAP は送信 SNMP トラップ処理を反映します。 send が true の場合、 SEND_SNMP_TRAP は true です。 有効な値は次の通りです。 Yes = 1 No = 0	tinyint, NULL
EVENT_DATA	バイナリ形式の追加データ。このフィールドは省略可能です。	varbinary(2000), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL
LOG_IDX*	ログインデックスの重複のない ID	char(32), NULL

エージェントセキュリティログのスキーマ (AGENT_SECURITY_LOG_1 テーブルと AGENT_SECURITY_LOG_2 テーブル)

表 1-6 はエージェントセキュリティログのデータベーススキーマを示しています。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

キーは I_AGENT_SECURITY_LOG_1_AGENT_SECURITY_LOG_IDX または I_AGENT_SECURITY_LOG_2_AGENT_SECURITY_LOG_IDX です。AGENT_SECURITY_LOG_IDX フィールドは重複のないテーブルの識別子として機能しますが、テーブルの主キーとしては形式的に分類されません。このフィールドにインデックスがありますが、主キーインデックスではありません。このテーブルに主キーはありません。

表 1-6 エージェントセキュリティログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	ログが属するドメインの GUID	char(32), NOT NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL

エージェントセキュリティログのスキーマ (AGENT_SECURITY_LOG_1 テーブルと AGENT_SECURITY_LOG_2 テーブル)

データベースのフィールド名	コメント	データタイプ
GROUP_ID	ログが属するグループの GUID	char(32), NOT NULL
COMPUTER_ID	エージェントセキュリティログと関連付けられたクライアントコンピュータの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
EVENT_ID		int, NOT NULL

データベースのフィールド名	コメント	データタイプ
	<p>コンプライアンスのイベント:</p> <p>209 = ホストインテグリティが失敗しました (TSLOG_SEC_NO_AV)</p> <p>210 = ホストインテグリティが成功しました (TSLOG_SEC_AV)</p> <p>221 = ホストインテグリティが失敗しましたが成功として報告されました</p> <p>237 = ホストインテグリティカスタムログエントリ</p> <p>ファイアウォールと IPS イベント:</p> <p>207 = アクティブレスポンス</p> <p>211 = アクティブレスポンスを解除しました</p> <p>219 = アクティブレスポンスを中止しました</p> <p>205 = 実行可能ファイルを変更しました</p> <p>216 = 実行可能ファイルの変更を検出しました</p> <p>217 = 実行可能ファイルの変更を受け入れました</p> <p>218 = 実行可能ファイルの変更を拒否しました</p> <p>220 = アプリケーション乗っ取り</p> <p>201 = ルール別の無効なトラフィック</p> <p>202 = ポートスキャン</p> <p>203 = サービス拒否攻撃</p> <p>204 = トロイの木馬</p> <p>206 = 侵入防止システム (検出された侵入, TSLOG_SEC_INTRUSION_DETECTED)</p>	

データベースのフィールド名	コメント	データタイプ
	<p>208 = MAC 詐称</p> <p>アプリケーションとデバイス制御:</p> <p>238 = デバイス制御がデバイスを無効にしました</p> <p>239 = バッファオーバーフローイベント</p> <p>240 = ソフトウェア保護で例外が発生しました</p>	
EVENT_TIME	イベント生成された日時(グリニッジ標準時)	bigint, NOT NULL
SEVERITY	<p>セキュリティルールで定義される重大度のレベル。</p> <p>有効な値は次の通りです。</p> <p>致命的 = 0 ~ 3</p> <p>重度 = 4 ~ 7</p> <p>軽度 = 8 ~ 11</p> <p>情報 = 12 ~ 15</p>	int, NOT NULL
AGENT_ID	エージェントの GUID	char(32), NULL
HARDWARE_KEY	コンピュータハードウェアの情報のハッシュ	char(32), NULL
HOST_NAME	クライアントコンピュータのホスト名	nvarchar(256), varchar(256), NULL
LOCAL_HOST_IP	ローカルコンピュータの IP アドレス (IPv4)	bigint, NULL
REMOTE_HOST_IP	リモートコンピュータの IP アドレス (IPv4)	bigint, NULL
REMOTE_HOST_NAME	リモートコンピュータの名前。名前解決が失敗した場合、空であることがあります。	nvarchar(64), varchar(64), NULL

データベースのフィールド名	コメント	データタイプ
TRAFFIC_DIRECTION	トラフィックの方向。Enum (不明 = 0、インバウンド = 1、アウトバウンド = 2)	tinyint, NULL
NETWORK_PROTOCOL	プロトコルの種類:Enum (その他 = 1、TCP = 2、UDP = 3、ICMP = 4)	tinyint, NULL
HACK_TYPE	<p>イベント ID が TSLOG_SEC_NO_AV の場合は理由です。</p> <p>イベント ID が TSLOG_SEC_INTRUSION_DETECTED の場合は侵入 ID です。</p> <p>イベント ID が TSLOG_SEC_AV の場合は追加情報です。</p> <p>示される理由:</p> <p>プロセスを実行していません - Bit 0 は 1 です</p> <p>シグネチャが最新ではありません - Bit 1 は 1 です</p> <p>回復を試みました - Bit 2 は 1 です</p>	int, NULL
BEGIN_TIME	セキュリティの問題の開始日時	bigint, NULL
END_TIME	セキュリティの問題の終了日時。ソフトウェアが UDP などのトラフィックの厳密な終了日時を検出できない場合があるため、終了日時は省略可能なフィールドです。そのような場合、終了日時は開始日時に等しいです。	bigint, NULL
REPETITION	攻撃の数。ハッカーが総攻撃を開始すると、ログシステムによって 1 つのイベントにダンプされる場合があります。	int, NULL

データベースのフィールド名	コメント	データタイプ
APP_NAME	関係するアプリケーションの絶対パス。不明なアプリケーションが関係するか、アプリケーションが関係しない場合は、空であることがあります。たとえば、 Ping of Death サービス拒否攻撃は、オペレーティングシステム自体を攻撃するので、 AppName がありません。	nvarchar(256), varchar(256), NULL
EVENT_DESC	イベントの説明。通常、説明の1行目は「概略」として扱われます。	nvarchar(2000), varchar(4000), NULL
EVENT_DATA	バイナリ形式の追加データ。このフィールドは省略可能です。	varbinary(3000), NULL
ALERT	ALERT はプロファイル処理の警告属性を反映します。サーバー側通知の生成に関してイベントが考慮されるようにネットワーク脅威防止ポリシーで指定される場合、ALERT フィールドは 1 に設定されます。 有効な値は次の通りです。 Yes = 1 No = 0	tinyint, NULL
SEND_SNMP_TRAP	SEND_SNMP_TRAP は送信 SNMPトラップ処理を反映します。send が true の場合、SEND_SNMP_TRAP は true です。 有効な値は次の通りです。 Yes = 1 No = 0	tinyint, NULL
LOCAL_HOST_MAC	ローカルコンピュータの MAC アドレス	varchar(18), NULL
REMOTE_HOST_MAC	リモートコンピュータの MAC アドレス	varchar(18), NULL

データベースのフィールド名	コメント	データタイプ
LOCATION_NAME	イベントが起きた場合に使われる場所	nvarchar(256), varchar(256), NULL
USER_NAME	ログオンユーザー名	nvarchar(256), varchar(256), NULL
DOMAIN_NAME	ログオンドメイン名	nvarchar(256), varchar(256), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(1900), NULL
AGENT_SECURITY_LOG_IDX*	ログインデックスの重複のない ID	char(32), NULL

エージェント状態のスキーマ (AGENTSTATUS テーブル)

表 1-7 は、エージェント状態情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_AGENTSTATUS として機能することを示します。

表 1-7 エージェント状態のスキーマ

データベースのフィールド名	コメント	データタイプ
IDX*	主キー。	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
AGENTTYPE	<p>AGENTTYPEの有効な値には次のものがあります。</p> <p>SAV 10.x</p> <p>LogSender</p> <p>ClientInventory</p> <p>SAV 11.x</p> <p>AgentSweepingTask(データベースの保守)</p> <p>TopThreatsTask(最上位と最新の脅威情報の収集)</p> <p>VirusCatTask(ウイルスのプロパティの収集)</p> <p>ThreatCatTask(リスクのプロパティの収集)</p>	varchar(255), NULL
AGENTNAME	<p>エージェントに関連付けられた名前。</p> <p>LogSender エージェント:サーバーグループ名</p> <p>LogSenderSAVSMTP エージェント:メールゲートウェイのホスト名</p> <p>ClientInventory エージェント:親サーバーの名前</p> <p>その他:空白</p>	varchar(255), NULL
LASTRUNGMT	<p>エージェントが最後に実行された日時(グリニッジ標準時で保存)</p>	varchar(50), NULL
REMOTE_TZ_OFFSET	<p>タイムゾーンオフセット</p>	int, NOT NULL
REPORTER_TZ_OFFSET	<p>タイムゾーンオフセット</p>	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
MAIL	電子メールがすでに送信されているかどうかを示すフラグ。 有効な値は次の通りです。 1 = はい 0 = いいえ	int, NOT NULL
VERSION_BUILD	エージェントのバージョンまたはビルド (major.minor.build)	varchar(20), NULL
MACHINE_NAME	クライアントコンピュータのコンピュータ名	NVARCHAR(128), varchar(128), NOT NULL
SERVERGROUP_IDX	IDENTITY_MAP テーブルを指すポイント	char(32), NOT NULL
LASTRUN_DATA	エージェントの実行と関連付けされる追加データ(ある場合)	nvarchar(255), varchar(255), NULL

エージェントシステムログのスキーマ (AGENT_SYSTEM_LOG_1 テーブルと AGENT_SYSTEM_LOG_2 テーブル)

表 1-8 はエージェントシステムログのデータベーススキーマを示しています。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

キーは I_AGENT_SYSTEM_LOG_1_LOG_IDX または I_AGENT_SYSTEM_LOG_2_LOG_IDX です。LOG_IDX フィールドは重複のないテーブルの識別子として機能しますが、テーブルの主キーとしては形式的に分類されません。このフィールドにインデックスがありますが、主キーインデックスではありません。このテーブルに主キーはありません。

表 1-8 エージェントシステムログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	ログが属するドメインの GUID	char(32), NOT NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL
GROUP_ID	ログが属するグループの GUID	char(32), NOT NULL
COMPUTER_ID	エージェントシステムログと関連付けられたクライアントコンピュータの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

エージェントシステムログのスキーマ (AGENT_SYSTEM_LOG_1 テーブルと AGENT_SYSTEM_LOG_2 テーブル)

データベースのフィールド名	コメント	データタイプ
EVENT_ID		int, NOT NULL

データベースのフィールド名	コメント	データタイプ
	<p>Symantec Endpoint Protection エージェントからのイベント ID</p> <p>AGENT_SYSTEM_INSTALL_EVENT_TYPES = インストールイベント: 有効な値には次のものがあります。</p> <p>0x12070001 = 内部エラー</p> <p>0x12070101 = インストールが完了しました</p> <p>0x12070102 = 再起動を推奨</p> <p>0x12070103 = 再起動が必要</p> <p>0x12070104 = インストールが失敗しました</p> <p>0x12070105 = アンインストールが完了しました</p> <p>0x12070106 = アンインストールが失敗しました</p> <p>0x12071037 = Symantec AntiVirus がインストール済みです</p> <p>0x12071038 = シマンテック製ファイアウォールがインストール済みです</p> <p>0x12071039 = アンインストール</p> <p>0x1207103A = アンインストールをロールバックしました</p> <p>AGENT_SYSTEM_SERVICE_EVENT_TYPES = サービスのイベント: 有効な値には次のものがあります。</p> <p>0x12070201 = サービスを開始しています</p> <p>0x12070202 = サービスを開始しました</p> <p>0x12070203 = サービス開始エラー</p> <p>0x12070204 = サービスを停止しました</p> <p>0x12070205 = サービス停止エラー</p> <p>0x1207021A = サービスを停止しようとする試み</p> <p>AGENT_SYSTEM_CONFIG_EVENT_TYPES = 設定のイベント:</p>	

データベースのフィールド名	コメント	データタイプ
	<p>有効な値には次のものがあります。</p> <p>0x12070206 = インポートの設定完了</p> <p>0x12070207 = インポートの設定エラー</p> <p>0x12070208 = エクスポートの設定完了</p> <p>0x12070209 = エクスポートの設定エラー</p> <p>AGENT_SYSTEM_HI_EVENT_TYPES = ホストインテグリティイベント:</p> <p>有効な値には次のものがあります。</p> <p>0x12070210 = ホストインテグリティが無効です</p> <p>0x12070211 = ホストインテグリティが有効です</p> <p>0x12070220 = NAP 統合が有効です</p> <p>AGENT_SYSTEM_IMPORT_EVENT_TYPES = インポートイベント:</p> <p>有効な値には次のものがあります。</p> <p>0x12070214 = 拡張ルールのインポートが正常に完了しました</p> <p>0x12070215 = 拡張ルールをインポートできませんでした</p> <p>0x12070216 = 拡張ルールのエクスポートが正常に完了しました</p> <p>0x12070217 = 拡張ルールをエクスポートできませんでした</p> <p>AGENT_SYSTEM_CLIENT_EVENT_TYPES = クライアントイベント:</p> <p>有効な値には次のものがあります。</p> <p>0x12070218 = クライアントエンジンが有効です</p> <p>0x12070219 = クライアントエンジンが無効です</p> <p>0x12071046 = プロアクティブ脅威スキャンはこのプラットフォーム上でサポート外です</p> <p>0x12071047 = プロアクティブ脅威スキャンロードエラー</p>	

データベースのフィールド名	コメント	データタイプ
	<p>AGENT_SYSTEM_SERVER_EVENT_TYPES = サーバーイベント:</p> <p>有効な値には次のものがあります。</p> <p>0x12070301 = サーバーに接続しました</p> <p>0x12070302 = サーバーレスポンスがありません</p> <p>0x12070303 = サーバー接続が失敗しました</p> <p>0x12070304 = サーバーを切断しました</p> <p>0x120B0001 = サーバーに到達できません</p> <p>0x120B0002 = 再接続したサーバー</p> <p>AGENT_SYSTEM_PROFILE_EVENT_TYPES = ポリシーイベント:</p> <p>有効な値には次のものがあります。</p> <p>0x12070306 = 新しいポリシーを受信しました</p> <p>0x12070307 = 新しいポリシーを適用しました</p> <p>0x12070308 = 新しいポリシーが失敗しました</p> <p>0x12070309 = ポリシーをダウンロードできません</p> <p>0x120B0005 = ポリシーをダウンロードできません</p> <p>0x1207030A = 最新のポリシーがあります</p> <p>0x120B0004 = 最新のポリシーがあります</p> <p>AGENT_SYSTEM_AV_EVENT_TYPES = ウイルス 対策エンジンイベント:</p> <p>有効な値には次のものがあります。</p> <p>0x12071006 = スキャン省略</p> <p>0x1207100B = ウイルス活動を検出しました</p> <p>0x1207100C = 設定が変更されました</p> <p>0x12071010 = ウイルス定義ファイルダウンロード</p> <p>0x12071012 = 検疫サーバーに送信</p> <p>0x12071013 = シマンテック社に配信しました</p>	

データベースのフィールド名	コメント	データタイプ
	<p>0x12071014 = セキュリティレスポンスバックアップ</p> <p>0x12071015 = スキャンを中止しました</p> <p>0x12071016 = Symantec AntiVirus Auto-Protect ロードエラー</p> <p>0x12071017 = Symantec AntiVirus Auto-Protect が有効です</p> <p>0x12071018 = Symantec AntiVirus Auto-Protect が無効です</p> <p>0x1207101A = スキャンを見送りました</p> <p>0x1207101B = 一時停止したスキャンの再開</p> <p>0x12071027 = Symantec AntiVirus が古いウイルス定義を使っています</p> <p>0x12071041 = スキャンを中断しました</p> <p>0x12071042 = スキャンを再開しました</p> <p>0x12071043 = スキャン期間が短すぎます</p> <p>0x12071045 = 拡張スキャンが失敗しました</p> <p>AGENT_SYSTEM_LICENSE_EVENT_TYPES = ライセンスイベント:</p> <p>有効な値には次のものがあります。</p> <p>0x1207101E = ライセンス警告</p> <p>0x1207101F = ライセンスエラー</p> <p>0x12071020 = ライセンスが猶予期間です</p> <p>0x12071023 = ライセンスをインストールしました</p> <p>0x12071025 = ライセンスが最新です</p> <p>AGENT_SYSTEM_SECURITY_EVENT_TYPES = セキュリティイベント:</p> <p>有効な値には次のものがあります。</p> <p>0x1207102B = セキュリティポリシーを順守しないコンピュータ</p>	

データベースのフィールド名	コメント	データタイプ
	<p>0x1207102C = セキュリティポリシーを順守するコンピュータ</p> <p>0x1207102D = 変更の試み</p> <p>AGENT_SYSTEM_OTHER_EVENT_TYPES = その他のイベント:</p> <p>有効な値には次のものがあります。</p> <p>0x1207020A = 電子メール送信 OK</p> <p>0x1207020B = 電子メール送信エラー</p> <p>0x1207020C = 更新完了</p> <p>0x1207020D = 更新エラー</p> <p>0x1207020E = 場所の手動変更</p> <p>0x1207020F = 場所を変更しました</p> <p>0x12070212 = 古い Rasdll を検出しました</p> <p>0x12070213 = 自動更新を延期しました</p> <p>0x12070305 = モードを変更しました</p> <p>0x1207030B = HI スクリプトを適用できません</p> <p>0x12070500 = デバイス制御からのシステムメッセージ</p> <p>0x12070600 = バッファオーバーフロードライバからのシステムメッセージ</p> <p>0x12071021 = アクセス拒否の警告</p> <p>0x12071022 = ログ転送エラー</p> <p>0x12071044 = クライアントを移動しました</p>	
EVENT_TIME	イベント生成された日時(グリニッジ標準時)	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
SEVERITY	イベントの種類。 有効な値は次の通りです。 情報 = 0 警告 = 1 エラー = 2 致命的 = 3	int, NOT NULL
AGENT_ID	エージェントの GUID	char(32), NULL
HARDWARE_KEY	コンピュータハードウェアの情報のハッシュ	char(32), NULL
HOST_NAME	クライアントコンピュータのホスト名	nvarchar(256), varchar(256), NULL
CATEGORY	CATEGORY は今は使われません。	int, NULL
EVENT_SOURCE	NETPORT、NATSRV などのデータソース。	varchar(32), NULL
EVENT_DESC	イベントの説明。通常、説明の 1 行目は「概略」として扱われます。	nvarchar(1024), varchar(2048), NULL
EVENT_DATA	バイナリ形式の追加データ。このフィールドは省略可能です。	varbinary(2000), NULL
SEND_SNMP_TRAP	SEND_SNMP_TRAP は送信 SNMP トラップ処理を反映します。send が true の場合、SEND_SNMP_TRAP は true です。 有効な値は次の通りです。 Yes = 1 No = 0	tinyint, NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL
LOG_IDX*	ログインデックスの重複のない ID	char(32), NULL

エージェントトラフィックログのスキーマ (AGENT_TRAFFIC_LOG_1 テーブルと AGENT_TRAFFIC_LOG_2 テーブル)

表 1-9 はエージェントトラフィックログのデータベーススキーマを示しています。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

キーは I_AGENT_TRAFFIC_LOG_1_LOG_IDX または I_AGENT_TRAFFIC_LOG_2_LOG_IDX です。LOG_IDX フィールドは重複のないテーブルの識別子として機能しますが、テーブルの主キーとしては形式的に分類されません。このフィールドにインデックスがありますが、主キーインデックスではありません。このテーブルに主キーはありません。

表 1-9 エージェントトラフィックログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	ログが属するドメインの GUID	char(32), NOT NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
GROUP_ID	ログが属するグループの GUID	char(32), NOT NULL
COMPUTER_ID	エージェントトラフィックログと関連付けられたクライアントコンピュータの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
EVENT_ID	Symantec Endpoint Protection エージェントからのイベント ID。 有効な値は次の通りです。 301 = TCP を開始しました 302 = UDP データグラム 303 = ping 要求 304 = TCP が完了しました 305 = トラフィック(その他) 306 = ICMP パケット 307 = イーサネットパケット 308 = IP パケット	int, NOT NULL
EVENT_TIME	イベント生成された日時(グリニッジ標準時)	bigint, NOT NULL
SEVERITY	セキュリティルールで定義された重大度。 有効な値は次の通りです。 致命的 = 0 ~ 3 重度 = 4 ~ 7 軽度 = 8 ~ 11 情報 = 12 ~ 15	int, NOT NULL
AGENT_ID	エージェントの GUID	char(32), NULL
HARDWARE_KEY	コンピュータハードウェアの情報のハッシュ	char(32), NULL

データベースのフィールド名	コメント	データタイプ
HOST_NAME	クライアントコンピュータのホスト名	nvarchar(256), varchar(256), NULL
LOCAL_HOST_IP	ローカルコンピュータの IP アドレス (IPv4)	bigint, NULL
REMOTE_HOST_IP	リモートコンピュータの IP アドレス (IPv4)	bigint, NULL
REMOTE_HOST_NAME	リモートコンピュータの名前。名前解決が失敗した場合、空であることがあります。	nvarchar(64), varchar(64), NULL
NETWORK_PROTOCOL	プロトコルの種類:Enum (その他 = 1、TCP = 2、UDP = 3、ICMP = 4)	tinyint, NULL
LOCAL_PORT	ローカルコンピュータの TCP/UDP ポート(ホストバイト順)。TSE_TRAFFIC_TCP と TSE_TRAFFIC_UDP のみで有効です。そうでない場合は、常にゼロです。	int, NULL
REMOTE_PORT	リモートコンピュータの TCP/UDP ポート(ホストバイト順)。TSE_TRAFFIC_TCP と TSE_TRAFFIC_UDP のみで有効です。そうでない場合は、常にゼロです。	int, NULL
TRAFFIC_DIRECTION	トラフィックの方向。Enum (不明 = 0、インバウンド = 1、アウトバウンド = 2)	tinyint, NULL
BEGIN_TIME	セキュリティの問題の開始日時	bigint, NULL
END_TIME	セキュリティの問題の終了日時。UDPなどのトラフィックの厳密な終了日時を検出できない場合があるため、終了日時は省略可能なフィールドです。そのような場合、終了日時は開始日時に等しいです。	bigint, NULL

データベースのフィールド名	コメント	データタイプ
REPETITION	攻撃の数。ハッカーが総攻撃を開始すると、ログシステムによって 1 つのイベントにダンプされる場合があります。	int, NULL
APP_NAME	関係するアプリケーションの絶対パス。不明なアプリケーションが関係するか、アプリケーションが関係しない場合は、空であることがあります。たとえば、Ping of Death サービス拒否攻撃は、オペレーティングシステム自体を攻撃するので、AppName がありません。	nvarchar(256), varchar(256), NULL
BLOCKED	トラフィックが遮断されたかどうか。 有効な値は次の通りです。 Yes = 1 No = 0	tinyint, NOT NULL
RULE_ID	イベントによってトリガされるルールの ID。ルール ID がセキュリティルールで指定されなければ常に 0 です。フィールドはセキュリティルールのトラブルシューティングに有用です。複数のルールが一致すれば、PacketProc での最終決定があるルールをログに記録します (pass/block/drop)。	char(32), NULL
RULE_NAME	イベントによってトリガされるルールの名前。ルール名がセキュリティルールで指定されていない場合は常に空の文字列です。これもトラブルシューティング用です。理論的には、ID によって IT 管理者はルールを区別できます。ただし、名前によってユーザーは、使うことができるルールを直接的に知ることができます。	nvarchar(256), varchar(256), NULL

データベースのフィールド名	コメント	データタイプ
ALERT	<p>ALERT はプロファイル処理の警告属性を反映します。サーバー側通知の生成に関してイベントが考慮されるようにネットワーク脅威防止ポリシーで指定される場合、ALERT フィールドは 1 に設定されます。</p> <p>有効な値は次の通りです。</p> <p>Yes = 1</p> <p>No = 0</p>	tinyint, NULL
SEND_SNMP_TRAP	<p>送信 SNMPトラップ処理を反映します。send が true の場合、SEND_SNMP_TRAP は true です。</p> <p>有効な値は次の通りです。</p> <p>Yes = 1</p> <p>No = 0</p>	tinyint, NULL
LOCAL_HOST_MAC	ローカルコンピュータの MAC アドレス	varchar(18), NULL
REMOTE_HOST_MAC	リモートコンピュータの MAC アドレス	varchar(18), NULL
LOCATION_NAME	イベント発生時に使われた場所	nvarchar(256), varchar(256), NULL
USER_NAME	ログオンユーザー名	nvarchar(256), varchar(256), NULL
DOMAIN_NAME	ログオンドメイン名	nvarchar(256), varchar(256), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL
LOG_IDX*	ログインデックスの重複のない ID	char(32), NULL

警告フィルタのスキーマ (ALERTFILTER テーブル)

表 1-10 は 警告フィルタ情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_ALERTFILTER として機能することを示します。

表 1-10 警告フィルタのスキーマ

データベースのフィールド名	コメント	データタイプ
ALERTFILTER_IDX*	主キー。	char(32), NOT NULL
USER_ID	ユーザー ID	char(32), NOT NULL
FILTERNAME	フィルタのユーザー指定の名前	NVARCHAR(255), varchar(255), NOT NULL
STARTDATEFROM	開始日	datetime, NOT NULL
STARTDATETO	終了日	datetime, NOT NULL

データベースのフィールド名	コメント	データタイプ
RELATIVEDATETYPE	有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = 今月	int, NOT NULL
FILTERACKNOWLEDGED	有効な値は次の通りです。 1 = 対応済み 0 = 未対応	NVARCHAR(255), varchar(255), NOT NULL
FILTERSUBJECT	有効な値は次の通りです。 AF = 認証エラー CL = クライアントリストを変更しました CS = クライアントセキュリティ警告 ED = エンフォース WL = 強制または商用のアプリケーション検出 LA = 新しい学習済みアプリケーション NV = 新種のリスクを検出しました NS = 新しいソフトウェアパッケージ VO = ウイルスアウトブレイク DF = サーバーの健全性 1V = 単一リスクイベント SE = システムイベント UM = 管理外コンピュータ ID = ウイルス定義が最新ではありません	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
FILTERCREATEDBY	警告フィルタを作成した管理者の GUID	NVARCHAR(255), varchar(255), NOT NULL
LASTCOLUMN	使われない。	varchar(255), NULL
SERVERGROUP	使われない。	NVARCHAR(255), varchar(255), NOT NULL
CLIENTGROUP	使われない。	NVARCHAR(255), varchar(255), NOT NULL
PARENTSERVER	使われない。	NVARCHAR(255), varchar(255), NOT NULL
COMPUTER	使われない。	NVARCHAR(255), varchar(255), NOT NULL
THREATNAME	使われない。	NVARCHAR(255), varchar(255), NOT NULL
THREATCATEGORY	使われない。	varchar(255), NULL
SOURCE	使われない。	varchar(255), NULL
ACTUALACTION	使われない。	varchar(255), NULL
LIMITROWS	ページ付けに使う行数	int, NOT NULL
USERRELATIVE	相対日付(「オン」)または絶対日付の使用	char(2), NOT NULL
REPORTINPUTS	特殊なパラメータ(レポートに必要な場合)	NVARCHAR(64), varchar(64), NOT NULL
NOTIFICATIONNAME	選択された通知状態の名前	NVARCHAR(255), varchar(255), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

警告メッセージのスキーマ (ALERTMSG テーブル)

表 1-11 は警告メッセージ情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_ALERTMSG として機能することを示します。

表 1-11 警告メッセージのスキーマ

データベースのフィールド名	コメント	データタイプ
ALERT_IDX*	主キー (1から9までのいずれか)	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
ALERT	<p>ALERTはルックアップに使われるハードコードされた英語の文字列です。Symantec Endpoint Protection エージェントからのイベント ID に対応します。</p> <p>有効な値は次の通りです。</p> <p>1 = ウイルスが見つかりました</p> <p>2 = セキュリティリスクが見つかりました</p> <p>3 は使われません</p> <p>4 は使われません</p> <p>5 = 商用アプリケーションが見つかりました</p> <p>6 = 強制プロアクティブ脅威が見つかりました</p> <p>7 = プロアクティブ検出を許可しました</p> <p>8 = 潜在的なリスクが見つかりました</p> <p>9 = シマンテック社にリスクサンプルを提出しました</p>	varchar(128), NULL

警告のスキーマ (ALERTS テーブル)

表 1-12 は警告情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_ALERTSとして機能することを示します。

表 1-12 警告のスキーマ

データベースのフィールド名	コメント	データタイプ
IDX*	主キー。	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
ALERT_IDX	テーブル ALERTMSG を指すポインタ	int, NOT NULL
COMPUTER_IDX	SEM_COMPUTER.COMPUTER_ID への外部キー	char(32), NOT NULL
SOURCE	次のスキャンの種類のルックアップキーとして使われるハードコードされた英語の文字列: "Scheduled Scan" "Manual Scan" "Real Time Scan" "Integrity Shield" "Definition downloader" "System" "Startup Scan" "DefWatch" "Manual Quarantine" "Reboot Processing" "Heuristic Scan"	varchar(50), NULL
VIRUSNAME_IDX	テーブル VIRUS を指すポインタ	char(32), NOT NULL
NOOFVIRUSES	集計されたイベントレコードのためのイベントの番号。この番号は、クライアント側の集計とサーバー側の圧縮のいずれか、または両方による可能性があります。	int, NOT NULL
FILEPATH	攻撃されたファイルのファイルパス	NVARCHAR(255), varchar(255), NOT NULL
DESCRIPTION	イベントの説明。	NVARCHAR(255), varchar(255), NOT NULL
ACTUALACTION_IDX	テーブル ACTUALACTION を指すポインタ。これはリスクに対するアクションです。	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
REQUESTEDACTION_IDX	テーブル ACTUALACTION を指すポインタ。これはポリシーによって要求されるアクションです。	int, NOT NULL
SECONDARYACTION_IDX	テーブル ACTUALACTION を指すポインタ。これはポリシーによって要求される二次アクションです。	int, NOT NULL
ALERTDATETIME	イベント発生日時	datetime, NOT NULL
ALERTINSERTTIME	イベントがデータベースに挿入された日時	datetime, NOT NULL
SERVERGROUP_IDX	テーブル IDENTITY_MAP を指すポインタ。これは Symantec Endpoint Protection Manager のドメイン GUID です。	char(32), NOT NULL
USER_NAME	イベントが起きたときにコンピュータにログ記録されたユーザーの名前	NVARCHAR(64), varchar(64), NOT NULL
PARENTSERVER_IDX	テーブル IDENTITY_MAP を指すポインタ。これは Symantec Endpoint Protection Manager のサーバー GUID です。	char(32), NOT NULL
CLIENTGROUP_IDX	テーブル IDENTITY_MAP を指すポインタ。これは Symantec Endpoint Protection Manager のグループ GUID です。	char(32), NOT NULL
SOURCE_COMPUTER_NAME	脅威のソース。ウイルス対策とスパイウェア対策のポリシーで脅威トレイサーが有効な場合にログに記録されます。	NVARCHAR(64), varchar(64), NOT NULL
SOURCE_COMPUTER_IP	脅威のソース。ウイルス対策とスパイウェア対策のポリシーで脅威トレイサーが有効な場合にログに記録されます。	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
MOTHER_IDX	ALERTS テーブルでの関連する圧縮イベントを指すポインタ。これはデータベース保守によって作成される圧縮イベントです。ここでの値は、このイベントがサーバー側で集計され、子イベントであることを示します。	char(32), NOT NULL
LAST_LOG_SESSION_GUID	関連する脅威のイベントを追跡するのにクライアントによって使われている ID。	char(32), NOT NULL
ALERTENDDATETIME	イベントが終了した日時。これは集計イベント時間の終わりです。	datetime, NOT NULL
HPP_APP_IDX	テーブル HPP_APPLICATION を指すポインタ	varchar(32), NULL
SITE_IDX	テーブル IDENTITY_MAP を指すポインタ。これは Symantec Endpoint Protection Manager のサイト GUID です。	char(32), NULL
VBIN_ID	検疫された場合、検疫された脅威のクライアント側の ID	bigint, NOT NULL
SCAN_ID	このイベントをピックアップしたスキャンテーブルイベントを指すポインタ	bigint, NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL
LOCAL_HOST_IP	検出が "0.0.0.0" の形で生成されたときのクライアントの IP アドレス。	bigint, NULL

データベースのフィールド名	コメント	データタイプ
AV_PRODUCT	ウイルス対策製品の名前。	varchar(256), NULL
AV_PRODUCT_VERSION	ウイルス対策製品のバージョン番号。	varchar(64), NULL

異常検出のスキーマ(ANOMALYDETECTION テーブル)

表 1-13 は異常検出情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_ANOMALYDETECTIONとして機能することを示します。

表 1-13 異常検出のスキーマ

データベースのフィールド名	コメント	データタイプ
ANOMALY_DETECTION_IDX*	主キー。	char(32), NOT NULL
ANOMALY_DETECTION_OPERATION_ID	テーブル「Anomalydetectionoperation」を指すポインタ	int, NOT NULL
ANOMALY_DETECTION_TYPE_ID	テーブル「Anomalydetectiontype」を指すポインタ	int, NOT NULL
ACTION_OPERAND	このアクションを行ったファイルまたはレジストリキー	NVARCHAR(512), varchar(512), NOT NULL
USN	USN ベースのシリアル番号。このID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
ACTION_OPERAND_HASH	ACTION_OPERAND 列のハッシュ値	char(32), NULL

異常検出の操作のスキーマ (ANOMALYDETECTIONOPERATION テーブル)

表 1-14 は異常検出操作情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_ANOMALYDETECTIONOPERATIONとして機能することを示します。

表 1-14 異常検出の操作のスキーマ

データベースのフィールド名	コメント	データタイプ
DETECTION_OPERATION_ID*	0-8	int, NOT NULL
DETECTION_OPERATION_DESC	Detection_Operation_ID、 Detection_Operation_Desc。 ルックアップで使われるハードコードされた英語の文字列。 有効な値は次の通りです。 0 = 不明 1 = Scan 2 = Present 3 = Not Present 4 = Equal 5 = Not Equal 6 = Equal (大文字と小文字を区別しない) 7 = Not Equal (大文字と小文字を区別しない) 8 = Scan Memory	varchar(255), NULL

異常検出の種類のスキーマ (ANOMALYDETECTIONTYPE テーブル)

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_ANOMALYDETECTIONTYPE として機能することを示します。

表 1-15 異常検出の種類のスキーマ

データベースのフィールド名	コメント	データタイプ
DETECTION_TYPE_ID*	主キー。	int, NOT NULL
DETECTION_TYPE_DESC	Detection_Type_ID、Detection_Type_Desc。ルックアップで使われるハードコードされた英語の文字列。 有効な値は次の通りです。 1000 = Registry 1001 = File 1002 = Process 1003 = Batch File 1004 = INI File 1005 = Service 1006 = Infected File 1007 = COM Object 1008 = Hosts File Entry 1009 = Directory 1010 = Layered Service Provider	varchar(255), NOT NULL

異常検出のスキーマ(ANOMALYDETECTIONS テーブル)

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_ANOMALYDETECTIONSとして機能することを示します。

表 1-16 異常検出のスキーマ

データベースのフィールド名	コメント	データタイプ
ALERT_EVENT_IDX	ALERTS.IDX への外部キー	char(32), NOT NULL
ANOMALY_DETECTION_IDX	テーブル「anomalydetection」を指すポインタ	char(32), NOT NULL
STATUS	スキャン検出の状態。現在は常に「正常に検出が実行されました」を意味する1です。その他の値は今後使用できるように予約されています。	int, NOT NULL
LOG_SESSION_GUID	LOG_SESSION_GUIDは関連する脅威イベントを追跡するためにクライアントによって使われているIDです。	char(32), NOT NULL
USN	USNベースのシリアル番号。このIDは一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL
ID*	主キー (11.0.1 で追加)	char(32), NOT NULL

異常修復のスキーマ (ANOMALYREMEDATION テーブル)

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キーPK_ANOMALYREMEDATIONとして機能することを示します。

表 1-17 異常修復のスキーマ

データベースのフィールド名	コメント	データタイプ
ANOMALY_REMEDIATION_IDX*	主キー。	char(32), NOT NULL
ANOMALY_REMEDIATION_OPERATION_ID	テーブル 「anomalyremediationoperation」 を指すポインタ	int, NOT NULL
ANOMALY_REMEDIATION_TYPE_ID	テーブル 「anomalyremediationtype」を 指すポインタ	int, NOT NULL
ACTION_OPERAND	このアクションを行ったファイルまたはレジストリキー	NVARCHAR(512), varchar(512), NOT NULL
USN	USN ベースのシリアル番号。このID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL
ACTION_OPERAND_HASH	ACTION_OPERAND 列のハッシュ値	char(32), NULL

異常修復の操作のスキーマ (ANOMALYREMIATIONOPERATION テーブル)

表 1-18 は異常修復操作情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_ANOMALYREMIATIONOPERATIONとして機能することを示します。

表 1-18 異常修復の操作のスキーマ

データベースのフィールド名	コメント	データタイプ
REMIATION_OPERATION_ID*	主キー	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
REMIATION_OPERATION_DESC		varchar(255), NULL

データベースのフィールド名	コメント	データタイプ
	<p>Remediation_Operation_ID、 Remediation_Operation_Desc。 ルックアップで使われるハードコー ドされた英語の文字列。 有効な値は次の通りです。</p> <p>0 = Unknown 1 = Delete 2 = Delete Line 3 = Move 4 = Create Empty File 5 = Set 6 = Terminate 7 = Suspend 8 = Stop 9 = Remove 10 = Handle Threat 11 = Set IP Address 12 = Set Domain Name 13 = Deny Access 999 = Invalid 1001 = Move 1002 = Rename 1003 = Delete 1004 = Leave Alone 1005 = Clean 1006 = Remove Macros 1007 = Save As 1008 = Move Back 1010 = Rename Back 1011 = Undo</p>	

データベースのフィールド名	コメント	データタイプ
	1012 = Bad	
	1013 = Backup	
	1014 = Pending	
	1015 = Partial	
	1016 = Terminate	
	1017 = Exclude	
	1018 = Reboot Processing	
	1019 = Clean By Deletion	
	1020 = Access Denied	

異常修復の種類のスキーマ (ANOMALYREMIATIONTYPE テーブル)

表 1-19 は異常修復の種類情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_ANOMALYREMIATIONTYPE として機能することを示します。

表 1-19 異常修復の種類のスキーマ

データベースのフィールド名	コメント	データタイプ
REMIATION_TYPE_ID*	主キー。	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
REMEDIATION_TYPE_DESC	<p>番号は REMEDIATION_TYPE_ID であり、等号の右側の文字列は数字 ID に対応する REMEDIATION_TYPE_DESC です。英語の文字列はルックアップのキーとして使われます。</p> <p>有効な値は次の通りです。</p> <p>2000 = Registry</p> <p>2001 = File</p> <p>2002 = Process</p> <p>2003 = Batch File</p> <p>2004 = INI File</p> <p>2005 = Service</p> <p>2006 = Infected File</p> <p>2007 = COM Object</p> <p>2008 = Hosts File Entry</p> <p>2009 = Directory</p> <p>2010 = Layered Service Provider</p> <p>2011 = Internet Browser Cache</p>	varchar(255), NOT NULL

異常修復のスキーマ (ANOMALYREMEDIATIONS テーブル)

表 1-20 は異常修復情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_ANOMALYREMEDIATIONSとして機能することを示します。

表 1-20 異常修復のスキーマ

データベースのフィールド名	コメント	データタイプ
ALERT_EVENT_IDX	ALERTS.IDX への外部キー	char(32), NOT NULL
ANOMALY_REMEDIATION_IDX	テーブル「anomalyremediation」を指すポインタ	char(32), NOT NULL
STATUS	1 = 修復完了、0 = 修復失敗、デフォルトはありません	int, NOT NULL
LOG_SESSION_GUID	関連する脅威イベントを追跡するためにクライアントによって使われている ID	char(32), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL
ID*	主キー (11.0.1 で追加)	char(32), NOT NULL

監査レポートのスキーマ(AUDIT_REPORT テーブル)

表 1-21 は監査レポート情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されます。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_AUDITREPORT として機能することを示します。

表 1-21 監査レポートのスキーマ

データベースのフィールド名	コメント	データタイプ
AUDITFILTER_IDX*	主キー。	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
USER_ID	フィルタを作成した管理者の GUID	char(32), NOT NULL
FILTERNAME	フィルタの名前	NVARCHAR(255), varchar(255), NOT NULL
STARTDATEFROM	フィルタの開始日時	datetime, NOT NULL
STARTDATETO	フィルタの終了日時	datetime, NOT NULL
RELATIVEDATETYPE	有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = 今月	int, NOT NULL
EVENTTYPE	有効な値は次の通りです。 0 = ポリシーを追加しました 1 = ポリシーを削除しました 2 = ポリシーを編集しました 3 = システムインストール時に共有 ポリシーを追加する 4 = システムアップグレード時に共 有ポリシーを追加する 5 = ドメイン作成時に共有ポリシー を追加する	int, NULL
SERVERGROUPLIST	フィルタ処理するドメイン名(カン マ区切り)。これらの名前にはワイル ドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
PARENTSERVERLIST	フィルタ処理するサーバー名(カン マ区切り)。これらの名前にはワ イルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
USERLIST	フィルタ処理するユーザー名(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
POLICYNAMELIST	フィルタ処理するポリシー名(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
SITELIST	フィルタ処理するサイト名(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
SORTORDER	データをソートする列またはフィールド	varchar(32), NOT NULL
SORTDIR	有効な値は次の通りです。 DESC = 降順のソート ASC = 昇順のソート	varchar(5), NOT NULL
LIMITROWS	ページ付けに使う行数	int, NOT NULL
USERRELATIVE	相対日付(「オン」)または絶対日付の使用	char(2), NOT NULL
REPORT_IDX	使われない。	int, NOT NULL
REPORTINPUTS	特殊なパラメータ(レポートに必要な場合)	NVARCHAR(64), varchar(64), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除されたフラグ: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

基本メタデータのスキーマ(BASIC_METADATA テーブル)

表 1-22 は基本メタデータ情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キー PK_BASIC_METADATA として機能することを示します。

表 1-22 基本メタデータのスキーマ

データベースのフィールド名	コメント	データタイプ
CHECKSUM	XML コンテンツのチェックサム	char(32), NOT NULL
CONTENT	スキーマオブジェクトの XML コンテンツ	image, NOT NULL
DELETED	削除されたフラグ: 0 = 削除された 1 = 削除されていない	tinyint, NOT NULL
ID*	スキーマオブジェクトの GUID	char(32), NOT NULL
OWNER	所有者の GUID。プライベートオブジェクトにのみ適用されます。	char(32), NULL
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL
TYPE	スキーマオブジェクトの種類名	varchar(256), NOT NULL
USN	更新シリアル番号(複製で使用)	bigint, NOT NULL
DOMAIN_ID	オブジェクトが属するドメインの GUID。 SemRootConfig と SemSite には DOMAIN_ID がありません。	char(32), NULL
REF_ID	オブジェクトの参照 ID	varchar(32), NULL

データベースのフィールド名	コメント	データタイプ
NAME	オブジェクト名	nvarchar(2000), varchar(2000), NULL
DESCRIPTION	オブジェクトの説明	nvarchar(256), varchar(256), NULL
LAST_MODIFY_TIME	最終修正日時	bigint, NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

動作レポートのスキーマ (BEHAVIOR_REPORT テーブル)

表 1-23 は動作レポート情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_BEHAVIORREPORT として機能することを示します。

表 1-23 動作レポートのスキーマ

データベースのフィールド名	コメント	データタイプ
BEHAVIORFILTER_IDX*	主キー。	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
USER_ID	このフィルタを作成したユーザーの GUID	char(32), NOT NULL
FILTERNAME	フィルタの名前	NVARCHAR(255), varchar(255), NOT NULL
STARTDATEFROM	フィルタ開始日	datetime, NOT NULL
STARTDATETO	フィルタ終了日	datetime, NOT NULL
RELATIVEDATETYPE	有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = 今月	int, NOT NULL
BEHAVIORTYPE	有効な値は次の通りです。 1 = アプリケーションの種類 2 = デバイス制御の種類	tinyint, NULL
SEVERITY	有効な値は次の通りです。 1 = 致命的 5 = 重度 9 = 軽度 13 = 情報	int, NULL
EVENTTYPE	アプリケーション制御用。 有効な値は次の通りです。 501 = アプリケーション制御ドライバ 502 = アプリケーション制御ルール 999 = 改変対策	int, NULL

データベースのフィールド名	コメント	データタイプ
ACTION	有効な値は次の通りです。 0 = 許可する 1 = 遮断 2 = 確認 3 = 続行 4 = 終了	tinyint, NULL
SERVERGROUPLIST	フィルタ処理するドメイン名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
CLIENTGROUPLIST	フィルタ処理するグループ名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
PARENTSERVERLIST	フィルタ処理するサーバー名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
COMPUTERLIST	フィルタ処理するコンピュータ名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(512), varchar(512), NOT NULL
SITELIST	フィルタ処理するサイト名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
CALLERPROCESSLIST	フィルタ処理するプロセス名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
IPADDRESSLIST	フィルタ処理する IP (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
USERLIST	フィルタ処理するユーザー名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
TEST_MODE	有効な値は次の通りです。 1 = はい 0 = いいえ	tinyint, NULL
SORTORDER	ソートされるテーブルの列	varchar(32), NOT NULL
SORTDIR	有効な値は次の通りです。 DESC = 降順 ASC = 昇順	varchar(5), NOT NULL
LIMITROWS	ページ付けのために表示する行数	int, NOT NULL
USERRELATIVE	相対日付(「オン」)または絶対日付の使用	char(2), NOT NULL
REPORT_IDX	使われない。	int, NOT NULL
REPORTINPUTS	特殊なパラメータ(レポートに必要な場合)	NVARCHAR(64), varchar(64), NOT NULL
USN	USNベースのシリアル番号。このIDは一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970年以降のミリ秒	bigint, NOT NULL
DELETED	削除されたフラグ: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

バイナリファイルのスキーマ(BINARY_FILE テーブル)

表 1-24 はバイナリファイル情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されます。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_BINARY_FILEとして機能することを示します。

表 1-24 バイナリファイルのスキーマ

データベースのフィールド名	コメント	データタイプ
CHECKSUM	XML コンテンツのチェックサム	char(32), NULL
CONTENT	スキーマオブジェクトの XML コンテンツ	image, NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除された 0 = 削除されていない	tinyint, NOT NULL
ID*	スキーマオブジェクトの GUID	char(32), NOT NULL
OWNER	所有者の GUID。プライベートオブジェクトにのみ適用されます	char(32), NULL
TIME_STAMP	データベースレコードが修正された日時 (マージの競合の解決に使用)	bigint, NOT NULL
TYPE	スキーマオブジェクトの種類名	varchar(256), NULL
USN	更新シリアル番号 (複製で使用)	bigint, NOT NULL
DOMAIN_ID	バイナリファイルが属するドメインの GUID	char(32), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

コマンドのスキーマ (COMMAND テーブル)

表 1-25 はコマンド情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_COMMAND として機能することを示します。

表 1-25 コマンドのスキーマ

データベースのフィールド名	コメント	データタイプ
HARDWARE_KEY*	コンピュータハードウェアの情報のハッシュ	char(32), NOT NULL
COMMAND_ID*	コマンドオブジェクトの GUID。この GUID は基本メタデータテーブルの ID に対応します。	char(32), NOT NULL
DOMAIN_ID	コマンド作成時に、現在管理されているドメイン ID	char(32), NOT NULL
USN	更新シリアル番号 (複製で使用)	bigint, NOT NULL
BEGIN_TIME	クライアントでのコマンド起動日時 (グリニッジ標準時)	bigint, NOT NULL
LAST_UPDATE_TIME	クライアントによって報告された最新状態の日時 (グリニッジ標準時)	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
STATE_ID	コマンド状態:次のいずれかの値に対応する数値: 0 = INITIAL 1 = RECEIVED 2 = IN_PROGRESS 3 = COMPLETED 4 = REJECTED 5 = CANCELLED 6 = エラー 最初に作成された場合、コマンドの状態は、INITIAL です。エンドポイントがそれをまだ受信していないことを示します。	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
SUB_STATE_ID	コマンド固有の状態。 有効な値は次の通りです。 0 = 正常に完了 1 = クライアントがコマンドを実行 してませんでした 2 = クライアントが状態を報告し ませんでした 3 = コマンドが重複していて実行 できません 4 = スプールコマンドを再開でき ませんでした 100 = 正常に完了 101 = セキュリティリスクが見つ かりました 102 = スキャンを中断しました 103 = スキャンを中止しました 105 = スキャンが状態を返しま せませんでした 110 = Auto-Protect をオンに できませんでした 120 = LiveUpdate ダウンロードが 進行中です 121 = LiveUpdate ダウンロードが 失敗しました 131 = 検疫削除が失敗しました 132 = 検疫削除が部分的に完了 しました	int, NULL
SUB_STATE_DESC	スキャンされたファイル数やエラー メッセージなどのコマンド固有の追 加情報	nvarchar(260), varchar(260), NULL
ESTIMATED_DURATION	コマンド期間(分単位)のエージェ ント推定。0 = 推定値なし、または わずかな時間	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
PERCENT_COMPLETE	推定期間に基づいたコマンドの進行状況 (0 から 100%)	tinyint, NOT NULL
TIME_STAMP	コマンドがデータベースに追加された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ: 1 = 削除しました 0 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		varchar(260), NULL
RESERVED_BINARY		varbinary(1000), NULL

コマンドレポートのスキーマ (COMMAND_REPORT テーブル)

表 1-26 はコマンドレポート情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キーPK_COMMANDREPORTとして機能することを示します。

表 1-26 コマンドレポートのスキーマ

データベースのフィールド名	コメント	データタイプ
COMMANDFILTER_IDX*	主キー。	char(32), NOT NULL
USER_ID	このフィルタを作成したユーザーの GUID	char(32), NOT NULL
FILTERNAME	フィルタの名前	NVARCHAR(255), varchar(255), NOT NULL
STARTDATEFROM	開始日時	datetime, NOT NULL
STARTDATETO	終了日時	datetime, NOT NULL
RELATIVEDATETYPE	有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = 今月	int, NOT NULL
STATE_ID	コマンドの状態。 有効な値は次の通りです。 0 = 受信していません 1 = 受信しました 2 = 進行中 3 = 完了 4 = 拒否しました 5 = キャンセル 6 = エラー	int, NULL

データベースのフィールド名	コメント	データタイプ
SUB_STATE_ID	<p>状態の詳細。</p> <p>有効な値は次の通りです。</p> <p>0 = 正常に完了</p> <p>1 = クライアントがコマンドを実行しませんでした</p> <p>2 = クライアントが状態を報告しませんでした</p> <p>3 = コマンドが重複していて実行できません</p> <p>4 = スプールコマンドを再開できませんでした</p> <p>101 = セキュリティリスクが見つかりました</p> <p>102 = スキャンを中断しました</p> <p>103 = スキャンを中止しました</p> <p>105 = スキャンが状態を返しませんでした</p> <p>110 = Auto-Protect をオンにできませんでした</p> <p>120 = LiveUpdate ダウンロードが進行中です</p> <p>121 = LiveUpdate ダウンロードが失敗しました</p> <p>131 = 検疫削除が失敗しました</p> <p>132 = 検疫削除が部分的に完了しました</p>	int, NULL
PERCENT_COMPLETE	コマンド進行状況	tinyint, NULL
COMPUTERLIST	フィルタ処理するコンピュータ名のリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(512), varchar(512), NOT NULL
SORTORDER	ソートされるテーブルの列名	varchar(32), NULL

データベースのフィールド名	コメント	データタイプ
SORTDIR	有効な値は次の通りです。 DESC = 降順 ASC = 昇順	varchar(5), NULL
LIMITROWS	ページ付けに使う行数	int, NOT NULL
USERRELATIVE	相対日付(「オン」)または絶対日付の使用	char(2), NOT NULL
REPORT_IDX	使われない。	int, NOT NULL
REPORTINPUTS	特殊なパラメータ(レポートに必要な場合)	NVARCHAR(64), varchar(64), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

コンプライアンスレポートのスキーマ (COMPLIANCE_REPORT テーブル)

表 1-27 はコンプライアンスレポート情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_COMPLIANCEREPORT として機能することを示します。

表 1-27 コンプライアンスレポートのスキーマ

データベースのフィールド名	コメント	データタイプ
COMPLIANCEFILTER_IDX*	主キー。	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
USER_ID	このフィルタを作成したユーザーの GUID	char(32), NOT NULL
FILTERNAME	フィルタ名	NVARCHAR(255), varchar(255), NOT NULL
STARTDATEFROM	開始日	datetime, NOT NULL
STARTDATETO	終了日	datetime, NOT NULL
RELATIVEDATETYPE	有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = 今月	int, NOT NULL
COMPLIANCE_TYPE	有効な値は次の通りです。 1 = エンフォースャサーバー 2 = エンフォースャクライアント 3 = エンフォースャトラフィック 4 = ホストコンプライアンス 5 = 攻撃 (ファイアウォールログ) 6 = デバイス制御	tinyint, NULL

データベースのフィールド名	コメント	データタイプ
SEVERITY	有効な値は次の通りです。 1 = 致命的 (SEVERITY >= 0 かつ SEVERITY <= 3 をフィルタ処理) 5 = 重度 (SEVERITY >= 4 かつ SEVERITY <= 7 をフィルタ処理) 9 = 軽度 (SEVERITY >= 8 かつ SEVERITY <= 11 をフィルタ処理) 13 = 情報 (SEVERITY >= 12 かつ SEVERITY <= 15 をフィルタ処理)	int, NULL

データベースのフィールド名	コメント	データタイプ
EVENT_ID		int, NULL

データベースのフィールド名	コメント	データタイプ
	<p>エンフォースサーバーのイベント。 有効な値は次の通りです。</p> <p>1 = エンフォースを登録しました</p> <p>2 = エンフォースを登録できませんでした</p> <p>5 = エンフォースがポリシーをダウンロードしました</p> <p>7 = エンフォースが <code>sylink.xml</code> をダウンロードしました</p> <p>9 = サーバーがエンフォースログを受信しました</p> <p>12 = サーバーがエンフォース情報を受信しました</p> <p>エンフォーストラフィックのイベント。 有効な値は次の通りです。</p> <p>17 = 着信トラフィックを遮断しました</p> <p>18 = 発信トラフィックを遮断しました</p> <p>33 = 着信トラフィックを許可しました</p> <p>34 = 発信トラフィックを許可しました</p> <p>ホストコンプライアンスのイベント。 有効な値は次の通りです。</p> <p>209 = ホストインテグリティの失敗</p> <p>210 = ホストインテグリティ成功</p> <p>221 = ホストインテグリティが失敗しましたが成功として報告されました</p> <p>237 = ホストインテグリティカスタムログエントリ</p>	

データベースのフィールド名	コメント	データタイプ
	攻撃(ファイアウォール)のイベント。 有効な値は次の通りです。 207 = アクティブレスポンス 211 = アクティブレスポンスを解除しました 219 = アクティブレスポンスを中止しました 217 = 実行可能ファイルの変更を受け入れました 218 = 実行可能ファイルの変更を拒否しました 220 = アプリケーション乗っ取り 201 = 適用なし(ルール別の無効なトラフィック) 202 = ポートスキャン 203 = サービス拒否攻撃 204 = トロイの木馬 206 = 侵入防止 208 = MAC 詐称 デバイス制御のイベント: 238 = デバイス制御がデバイスを無効にしました	
BLOCKED	有効な値は次の通りです。 0 = 遮断された 1 = 遮断されていない	tinyint, NULL
NETWORK_PROTOCOL	有効な値は次の通りです。 1 = その他 2 = TCP 3 = UDP 4 = ICMP	tinyint, NULL

データベースのフィールド名	コメント	データタイプ
TRAFFIC_DIRECTION	有効な値は次の通りです。 1 = インバウンド 2 = アウトバウンド 0 = 不明	tinyint, NULL
SERVERGROUPLIST	フィルタ処理するドメイン名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
CLIENTGROUPLIST	フィルタ処理するグループ名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
PARENTSERVERLIST	フィルタ処理するサーバー名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
COMPUTERLIST	フィルタ処理するコンピュータ名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(512), varchar(512), NOT NULL
IPADDRESSLIST	フィルタ処理する IP リスト (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
USERLIST	フィルタ処理するユーザー名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
SITELIST	フィルタ処理するサイト名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
ENFORCERLIST	フィルタ処理するエンフォーサ名 (カンマ区切り) これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
REMOTEHOSTLIST	フィルタ処理するリモートコンピュータ名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
REMOTEIPLIST	フィルタ処理するリモート IP リスト (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
LOCAL_PORT	ポート番号	int, NULL
HACK_TYPE	有効な値は次の通りです。 0 = プロセスを実行していません 1 = シグネチャが最新ではありません 2 = 回復を試みました	int, NULL
ACTION	エンフォースクライアント用。 有効な値は次の通りです。 認証 切断 成功 拒否 失敗	varchar(32), NULL
ENFORCER_TYPE	エンフォースクライアント用。 有効な値は次の通りです。 0 = ゲートウェイエンフォース 1 = LAN エンフォース 2 = DHCP エンフォース 3 = 統合エンフォース 4 = NAP エンフォース 5 = ピアツーピアエンフォース	tinyint, NULL

データベースのフィールド名	コメント	データタイプ
OS_TYPE	有効な値は次の通りです。 600 = Windows Vista と Windows Server 2008 502 = Windows 2003 と Windows XP 64 ビット 501 = Windows XP 500 = Windows 2000 400 = Windows NT 000 = その他	int, NULL
SORTORDER	ソートされるログ列	varchar(32), NULL
SORTDIR	有効な値は次の通りです。 DESC = 降順 ASC = 昇順	varchar(5), NULL
LIMITROWS	ページ付けに使う行数	int, NOT NULL
USERRELATIVE	相対日付(「オン」)または絶対日付の使用	char(2), NOT NULL
REPORT_IDX	使われない。	int, NOT NULL
REPORTINPUTS	特殊なパラメータ(レポートに必要な場合)	NVARCHAR(64), varchar(64), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除されたエントリ: 0 = 削除されていない 1 = 削除しました	tinyint, NOT NULL
FULL_CHARTS	ネットワーク脅威防止フルレポートに含めるグラフの管理者指定のリスト	varchar(255), NULL

コンピュータアプリケーションのスキーマ (COMPUTER_APPLICATION テーブル)

表 1-28 はコンピュータアプリケーション情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MSSQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_COMPUTER_APPLICATION として機能することを示します。

表 1-28 コンピュータアプリケーションのスキーマ

データベースのフィールド名	コメント	データタイプ
AGENT_ID*	エージェントの GUID	char(32), NOT NULL
DOMAIN_ID*	エージェントが属するドメインの GUID	char(32), NOT NULL
APP_HASH*	学習済みアプリケーションレコードのハッシュ値	char(32), NOT NULL
LOCATION_ID*	場所の GUID	char(32), NOT NULL
COMPUTER_ID	コンピュータの GUID。	char(32), NOT NULL
GROUP_ID	グループ GUID	char(32), NOT NULL
LAST_ACCESS_TIME	コンピュータでのアプリケーションの最終アクセス日時(グリニッジ標準時)	bigint, NULL
USN	更新シリアル番号(複製で使用)	bigint, NOT NULL
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除された 0 = 削除されていない	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

データハンドラのスキーマ (DATA_HANDLER テーブル)

表 1-29 はデータハンドラ情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_DATA_HANDLER として機能することを示します。

表 1-29 データハンドラのスキーマ

データベースのフィールド名	コメント	データタイプ
IDX*	主キー。	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
TECH_ID	技術の拡張子。 有効な値は次の通りです。 AvMan CAvMan LuMan legacy SEP	varchar(255), NULL
LF_EXT	ファイル拡張子。 有効な値は次の通りです。 .dat です。 .AgentStatus .SecurityRisk .VirusScans .VirusLogs .Inventory	varchar(255), NULL
LF_SORT	ソートファイル。 有効な値は次の通りです。 0 = ファイル修正日の昇順 1 = ファイル修正日の降順	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
LF_HANDLER	<p>データファイルを処理するクラス。 有効な値は次の通りです。</p> <p>AvMan = com.sygate.scm.server.logreader.av.LogHandler</p> <p>CAvMan = com.sygate.scm.server.logreader.cav.CommonLogHandler</p> <p>Legacy agentstatus = com.sygate.scm.server.logreader.av.AgentStatusHandler</p> <p>Legacy inventory = com.sygate.scm.server.logreader.av.InventoryHandler</p> <p>Legacy security and virus logs = com.sygate.scm.server.logreader.av.LogHandler</p>	varchar(255), NULL
STATE_HANDLER	<p>状態ファイルを処理するクラス。 有効な値は次の通りです。</p> <p>SEP = com.sygate.scm.server.statereader.sep.StateHandler</p> <p>AvMan = com.sygate.scm.server.statereader.av.StateHandler</p> <p>LuMan = com.sygate.scm.server.statereader.lu.StateHandler</p>	varchar(255), NULL

エンフォーサクライアントログ 1 と 2 のスキーマ (ENFORCER_CLIENT_LOG_1 テーブルと ENFORCER_CLIENT_LOG_2 テーブル)

表 1-30 はエンフォーサクライアントログのデータベーススキーマを示しています。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MSSQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初

エンフォーサクライアントログ 1 と 2 のスキーマ (ENFORCER_CLIENT_LOG_1 テーブルと ENFORCER_CLIENT_LOG_2 テーブル)

の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されま
す。

キーは I_ENFORCER_CLIENT_LOG_1_LOG_IDX または
I_ENFORCER_CLIENT_LOG_2_LOG_IDX です。LOG_IDX フィールドは重複のない
テーブルの識別子として機能しますが、テーブルの主キーとしては形式的に分類されま
せん。このフィールドにインデックスがありますが、主キーインデックスではありません。この
テーブルに主キーはありません。

表 1-30 エンフォーサクライアントログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	使われない (「00000000000000000000000000000000」 としてログに記録)	char(32), NOT NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデー タベースで入力または修正された 日時。1970 年以降のミリ秒	bigint, NOT NULL
EVENT_ID	イベント ID が定義されていない場 合は、0 としてログに記録されます	int, NOT NULL
EVENT_TIME	イベント生成された日時(グリニッ ジ標準時)	bigint, NOT NULL
ENFORCER_ID	エンフォーサの GUID	char(32), NOT NULL
ENFORCER_TYPE	有効な値は次の通りです。 0 = ゲートウェイエンフォーサ 1 = LAN エンフォーサ 2 = DHCP エンフォーサ 3 = 統合エンフォーサ 4 = NAP エンフォーサ 5 = ピアツーピアエンフォーサ	tinyint, NOT NULL
CLIENT_ID	使われない、長さ 0 の文字列とし てログに記録	char(32), NULL

データベースのフィールド名	コメント	データタイプ
REMOTE_HOST	リモートホスト名	varchar(256), NULL
ACTION	<p>クライアントでのエンフォーサの処理。ルックアップに使われるハードコードされた英語の文字列です。</p> <p>有効な値は次の通りです。</p> <p>Authenticated = エージェントの UID は正しい</p> <p>Rejected = エージェントの UID が正しくないか、実行中のエージェントがない</p> <p>Disconnected = エージェントがエンフォーサから切断されたか、エンフォーササービスが停止した</p> <p>Passed = エージェントがホストインテグリティ検査に合格した</p> <p>Failed = エージェントがホストインテグリティ検査に合格しなかった</p>	varchar(256), NULL
PERIOD	<p>エンフォーサがクライアントでアクションをとるまでの期間 (秒単位)。</p> <p>アクションが Rejected と Disconnected に等しい場合にのみ有効です。その他の処理では、このフィールドは 0 になります。</p>	int, NULL
EVENT_DESC	イベントの説明。通常、説明の 1 行目は「概略」として扱われます。	nvarchar(256), varchar(256), NULL
REMOTE_HOST_MAC	リモートホストの MAC アドレス	varchar(17), NULL
REMOTE_HOST_INFO	リモートホスト情報	nvarchar(128), varchar(128), NULL
EXTENDED_INFO		nvarchar(1024), varchar(1024), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1	ピアツーピアエンフォース	nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL
LOG_IDX*		char(32), NULL

エンフォースシステムログ 1 と 2 のスキーマ (ENFORCER_SYSTEM_LOG_1 テーブルと ENFORCER_SYSTEM_LOG_2 テーブル)

表 1-31 はエンフォースシステムログのデータベーススキーマを示しています。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MSSQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

キーは I_ENFORCER_SYSTEM_LOG_1_LOG_IDX または I_ENFORCER_SYSTEM_LOG_2_LOG_IDX です。LOG_IDX フィールドは重複のないテーブルの識別子として機能しますが、テーブルの主キーとしては形式的に分類されません。このフィールドにインデックスがありますが、主キーインデックスではありません。このテーブルに主キーはありません。

表 1-31 エンフォースシステムログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

エンフォースシステムログ 1 と 2 のスキーマ (ENFORCER_SYSTEM_LOG_1 テーブルと ENFORCER_SYSTEM_LOG_2
テーブル)

データベースのフィールド名	コメント	データタイプ
EVENT_ID		int, NULL

データベースのフィールド名	コメント	データタイプ
	<p>Symantec Endpoint Protection クライアントからのイベント ID (16 進数)。</p> <p>有効な値は次の通りです。</p> <p>0x101 = 管理サーバーに接続し ました</p> <p>0x102 = 管理サーバーとの接続 が消失しました</p> <p>0x103 = 管理サーバーからダウン ロードしたポリシーを適用しました</p> <p>0x104 = 管理サーバーからダウン ロードしたポリシーを適用できませ んでした</p> <p>0x107 = 管理サーバーの設定を 適用しました</p> <p>0x108 = 管理サーバー設定を適 用できませんでした</p> <p>0x110 = NAP 管理サーバーに登 録しました</p> <p>0x111 = NAP 管理サーバーから 登録解除しました</p> <p>0x112 = NAP 管理サーバーに登 録できませんでした</p> <p>0x201 = エンフォーサを開始しま した</p> <p>0x202 = エンフォーサを停止しま した</p> <p>0x203 = エンフォーサが一時停止 しました</p> <p>0x204 = エンフォーサが再開しま した</p> <p>0x205 = エンフォーサをサーバー から切断了ました</p> <p>0x301 = エンフォーサフェール</p>	

データベースのフィールド名	コメント	データタイプ
	<p>オーバーが有効です</p> <p>0x302 = エンフォーサフェール オーバーが無効です</p> <p>0x303 = スタンバイモードエン フォーサ</p> <p>0x304 = 一次モードエンフォーサ</p> <p>0x305 = エンフォーサ不足</p> <p>0x306 = エンフォーサループ</p> <p>0x401 = 転送エンジンの一時停 止</p> <p>0x402 = 転送エンジンの開始</p> <p>0x403 = DNS エンフォーサが有 効です</p> <p>0x404 = DNS エンフォーサが無 効です</p> <p>0x405 = DHCP エンフォーサが有 効です</p> <p>0x406 = DHCP エンフォーサが無 効です</p> <p>0x407 = すべての有効化を許可 する</p> <p>0x408 = すべての無効化を許可 する</p> <p>0x501 = ライセンス枠数の変更</p> <p>0x601 = ポリシー解析ルーチンを 作成できませんでした</p> <p>0x602 = 管理サーバーからダウン ロードしたポリシーをインポートで きませんでした</p> <p>0x603 = 管理サーバーからダウン ロードしたポリシーをエクスポート できませんでした</p>	

データベースのフィールド名	コメント	データタイプ
	0x701 = カスタム属性が正しくありません	
EVENT_TIME	イベント生成された日時 (グリニッジ標準時)	bigint, NOT NULL
ENFORCER_ID	エンフォースの GUID	char(32), NOT NULL
ENFORCER_TYPE	有効な値は次の通りです。 0 = ゲートウェイエンフォース 1 = LAN エンフォース 2 = DHCP エンフォース 3 = 統合エンフォース 4 = NAP エンフォース 5 = ピアツーピアエンフォース	tinyint, NOT NULL
SEVERITY	イベントの種類。 有効な値は次の通りです。 0 = 情報 1 = 警告 2 = エラー 3 = 致命的	int, NOT NULL
EVENT_DESC	イベントの説明。通常、説明の 1 行目は「概略」として扱われます。	nvarchar(256), varchar(256), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL

データベースのフィールド名	コメント	データタイプ
EVENT_ID	Symantec Endpoint Protection エージェントからのイベント ID 有効な値は次の通りです。 17 = 着信トラフィックを遮断しました 18 = 発信トラフィックを遮断しました 33 = 着信トラフィックを許可しました 34 = 発信トラフィックを許可しました	int, NULL
EVENT_TIME	イベント生成された日時(グリニッジ標準時)	bigint, NOT NULL
ENFORCER_ID	エンフォースアの GUID	char(32), NOT NULL
ENFORCER_TYPE	有効な値は次の通りです。 0 = ゲートウェイエンフォースア 1 = LAN エンフォースア 2 = DHCP エンフォースア 3 = 統合エンフォースア 4 = NAP エンフォースア 5 = ピアツーピアエンフォースア	tinyint, NOT NULL
CLIENT_ID	使われない、長さ0の文字列としてログに記録	char(32), NULL
LOCAL_HOST_IP	ローカルコンピュータの IP アドレス(IPv4)	bigint, NOT NULL
REMOTE_HOST_IP	リモートコンピュータの IP アドレス(IPv4)	bigint, NOT NULL
NETWORK_PROTOCOL	プロトコルの種類:Enum(その他 = 1、TCP = 2、UDP = 3、ICMP = 4)	tinyint, NOT NULL

エンフォーサトラフィックログ 1 と 2 のスキーマ (ENFORCER_TRAFFIC_LOG_1 テーブルと ENFORCER_TRAFFIC_LOG_2 テーブル)

データベースのフィールド名	コメント	データタイプ
LOCAL_PORT	ローカルコンピュータの TCP/UDP ポート(ホストバイト順)。TSE_TRAFFIC_TCP と TSE_TRAFFIC_UDP のみで有効です。そうでない場合は、常にゼロです。	int, NOT NULL
REMOTE_PORT	リモートコンピュータの TCP/UDP ポート(ホストバイト順)。TSE_TRAFFIC_TCP と TSE_TRAFFIC_UDP のみで有効です。そうでない場合は、常にゼロです。	int, NOT NULL
TRAFFIC_DIRECTION	トラフィックの方向。Enum(不明 = 0、インバウンド = 1、アウトバウンド = 2)	tinyint, NOT NULL
BEGIN_TIME	エンフォーサイベントの開始日時	bigint, NULL
END_TIME	エンフォーサイベントの終了日時	bigint, NULL
BLOCKED	トラフィックが遮断されたかどうか。有効な値は次の通りです。 0 = 遮断された 1 = 遮断されていない メモ: このテーブルの値と AGENT_TRAFFIC_LOG_x テーブルの値は異なります。	tinyint, NOT NULL
TOTAL_BYTES	トラフィックのすべてのパケットの全長	int, NOT NULL
REPETITION	攻撃の数。ハッカーが総攻撃を開始すると、ログシステムによって 1 つのイベントにダンプされる場合があります。	int, NULL
ALERT	予約済み	tinyint, NOT NULL
RESERVED_INT1		int, NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL
LOG_IDX*		char(32), NULL

ファイアウォールレポートのスキーマ (FIREWALL_REPORT テーブル)

表 1-33 はファイアウォールレポート情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_FIREWALLREPORT として機能することを示します。

表 1-33 ファイアウォールレポートのスキーマ

データベースのフィールド名	コメント	データタイプ
FIREWALLFILTER_IDX*	主キー。	char(32), NOT NULL
USER_ID	このフィルタを作成したユーザーの GUID	char(32), NOT NULL
FILTERNAME	フィルタ名	NVARCHAR(255), varchar(255), NOT NULL
STARTDATEFROM	開始日	datetime, NOT NULL
STARTDATETO	終了日	datetime, NOT NULL

データベースのフィールド名	コメント	データタイプ
RELATIVEDATETYPE	有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = 今月	int, NOT NULL
FIREWALLTYPE	有効な値は次の通りです。 1 = トラフィック 2 = パケット	int, NULL
SEVERITY	有効な値は次の通りです。 1 = 致命的 5 = 重度 9 = 軽度 13 = 情報	int, NULL
EVENTTYPE	トラフィックのイベント。 有効な値は次の通りです。 307 = イーサネットパケット 306 = ICMP パケット 308 = IP パケット 303 = ping 要求 301 = TCP を開始しました 304 = TCP が完了しました 302 = UDP データグラム 305 = その他 パケットのイベント: 401 = Raw イーサネット	int, NULL

データベースのフィールド名	コメント	データタイプ
BLOCKED	有効な値は次の通りです。 1 = 遮断された 0 = 遮断されていない	int, NULL
PROTOCOL	有効な値は次の通りです。 1 = その他 2 = TCP 3 = UDP 4 = ICMP	int, NULL
DIRECTION	有効な値は次の通りです。 1 = インバウンド 2 = アウトバウンド 0 = 不明	int, NULL
LOCALPORT	ポート番号	int, NULL
SITELIST	フィルタ処理するサイト名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
SERVERGROUPLIST	フィルタ処理するドメイン名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
CLIENTGROUPLIST	フィルタ処理するグループ名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
PARENTSERVERLIST	フィルタ処理するサーバー名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
COMPUTERLIST	フィルタ処理するコンピュータ名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(512), varchar(512), NOT NULL

データベースのフィールド名	コメント	データタイプ
IPADDRESSLIST	フィルタ処理する IP リスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
REMOTEHOSTLIST	フィルタ処理するリモートコンピュータ名(カンマ区切り)。	NVARCHAR(255), varchar(255), NOT NULL
REMOTEIPADDRLIST	フィルタ処理するリモート IP リスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
USERLIST	フィルタ処理するユーザー名(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
SORTORDER	ソートされるテーブルの列	varchar(32), NOT NULL
SORTDIR	ソートされる方向 有効な値は次の通りです。 DESC = 降順 ASC = 昇順	varchar(5), NOT NULL
LIMITROWS	ページ付けに使う行数	int, NOT NULL
USERRELATIVE	相対日付(「オン」)または絶対日付の使用	char(2), NOT NULL
REPORT_IDX	使われない。	int, NOT NULL
REPORTINPUTS	特殊なパラメータ(レポートに必要な場合)	NVARCHAR(64), varchar(64), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL
FULL_CHARTS	使われない。	varchar(255), NOT NULL

GUI パラメータのスキーマ (GUIPARMS テーブル)

表 1-34 は GUI パラメータ情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_GUIPARMS として機能することを示します。

表 1-34 GUI パラメータのスキーマ

データベースのフィールド名	コメント	データタイプ
GUIPARMS_IDX*	主キー。	int, NOT NULL
PARAMETER	パラメータ名	varchar(255), NOT NULL
VALUE	パラメータ値	NVARCHAR(255), varchar(255), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

GUP リストのスキーマ(GUP_LIST テーブル)

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_GUP_LISTとして機能することを示します。

表 1-35 はグループ更新プロバイダリストのデータベーススキーマを示しています。

表 1-35 GUP リストのスキーマ

データベースのフィールド名	コメント	データタイプ
GUP_ID*	主キー	char(32), NOT NULL
COMPUTER_ID	SEMコンピュータのテーブルからの参照 Computer_ID	char(32), NOT NULL
IP_ADDRESS	グループ更新プロバイダの IP アドレス	bigint, NOT NULL
PORT	グループ更新プロバイダのポート	int, NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません	bigint, NOT NULL
TIME_STAMP	イベントがシステムにログ記録される日時(グリニッジ標準時)。サーバー側の日時です	bigint, NOT NULL
DELETED	削除された行。0 = 削除されていない、1 = 削除された	tinyint, NOT NULL

履歴のスキーマ(HISTORY テーブル)

表 1-36 は履歴情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_HISTORYとして機能することを示します。

表 1-36 履歴のスキーマ

データベースのフィールド名	コメント	データタイプ
HISTORY_IDX*	主キー、インデックス	char(32), NOT NULL
HISTORYCONFIG_IDX	履歴設定テーブルを指すポインタ	char(32), NOT NULL
EVENT_DATETIME	スナップショット日時(グリニッジ標準時)	bigint, NOT NULL
STAT_TYPE	データの種類、ハードコードされた英語のキー	varchar(64), NOT NULL
TARGET	データ	NVARCHAR(256), varchar(256), NOT NULL
STATISTIC	要約統計	NVARCHAR(256), varchar(256), NOT NULL

履歴設定のスキーマ (HISTORYCONFIG テーブル)

表 1-37 は履歴設定情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_HISTORYCONFIG として機能することを示します。

表 1-37 履歴設定のスキーマ

データベースのフィールド名	コメント	データタイプ
HISTORYCONFIG_IDX*	主キー。	char(32), NOT NULL
USER_ID	この定時レポートを作成したユーザーの GUID	char(32), NOT NULL
TZ_OFFSET	データを管理者の現地時間でフォーマットできるように、管理者が定時レポートを作成した時点からのオフセットであるタイムゾーン	int, NOT NULL
FILTERNAME	この定時レポートによって使われるフィルタ	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
REPORT_IDX		varchar(10), NULL

データベースのフィールド名	コメント	データタイプ
	<p>形式は Reporttype-number です。たとえば、I-0 はウイルス定義分布です。</p> <p>有効な値は次の通りです。</p> <p>I = コンピュータ状態レポート</p> <p>0 = ウイルス定義分布</p> <p>1 = サーバーにチェックインしていないコンピュータ</p> <p>2 = Symantec Endpoint Protection 製品のバージョン</p> <p>3 = 侵入防止シグネチャの分布</p> <p>4 = クライアントインベントリ</p> <p>5 = コンプライアンス状態分布</p> <p>6 = クライアントオンライン状態</p> <p>7 = 最新ポリシーを備えたクライアント</p> <p>8 = グループ別のクライアント数</p> <p>9 = セキュリティ状態の概略</p> <p>10 = 保護コンテンツのバージョン</p> <p>11 = クライアント移行</p> <p>100 = クライアントソフトウェアロールアウト(スナップショット)</p> <p>101 = 一定期間にわたってオンライン/オフラインのクライアント(スナップショット)</p> <p>102 = 一定期間にわたって最新ポリシーを備えたクライアント(スナップショット)</p> <p>103 = 一定期間にわたって準拠しないクライアント(スナップショット)</p> <p>104 = ウイルス定義ロールアウトレポート(スナップショット)</p>	

データベースのフィールド名	コメント	データタイプ
	<p>A = 監査レポート</p> <p>0 = 使われるポリシー</p> <p>B = アプリケーションとデバイス制御のレポート</p> <p>0 = 最も警告が多いアプリケーション制御ログを伴う上位グループ</p> <p>1 = 上位を占める遮断した対象</p> <p>2 = 上位を占める遮断したデバイス</p> <p>C = コンプライアンスレポート</p> <p>0 = ネットワークコンプライアンス状態</p> <p>1 = コンプライアンス状態</p> <p>2 = コンプライアンスエラー概略別クライアント</p> <p>3 = コンプライアンスエラーの詳細</p> <p>4 = 場所別の準拠しないクライアント</p> <p>F = ネットワーク脅威防止レポート</p> <p>0 = 上位を占める攻撃の標的</p> <p>1 = 上位を占める攻撃元</p> <p>2 = 上位を占める攻撃の種類</p> <p>3 = 上位を占める遮断したアプリケーション</p> <p>4 = 一定期間にわたる攻撃</p> <p>5 = 重大度別セキュリティイベント</p> <p>6 = 一定期間に遮断したアプリケーション</p> <p>7 = 一定期間にわたるトラフィック通知</p> <p>8 = 上位を占めるトラフィック通知</p> <p>9 = 詳細レポート</p>	

データベースのフィールド名	コメント	データタイプ
	<p>R = リスクレポート</p> <p>0 = 感染コンピュータとリスクを伴うコンピュータ</p> <p>1 = 検出処理の概略</p> <p>2 = リスクの検出数</p> <p>3 = ネットワークで新種のリスクを検出しました</p> <p>4 = 上位のリスク検出相関関係</p> <p>5 = リスク分布の概略</p> <p>6 = 一定期間にわたるリスク分布</p> <p>8 = プロアクティブ脅威検出結果</p> <p>9 = プロアクティブ脅威の分布</p> <p>10 = 一定期間にわたるプロアクティブ脅威検出</p> <p>11 = 上位リスクの処理概略</p> <p>12 = 通知の数</p> <p>14 = 一定期間にわたる通知の数</p> <p>13 = 週次アウトブレイク</p> <p>7 = 総合リスクレポート</p> <p>S = スキャンレポート</p> <p>0 = スキャン統計ヒストグラム</p> <p>1 = 前回のスキャン時間別のコンピュータ</p> <p>2 = スキャンしていないコンピュータ</p> <p>Y = システムレポート</p> <p>0 = エラーを生成する上位クライアント</p> <p>1 = エラーを生成する上位サーバー</p>	

データベースのフィールド名	コメント	データタイプ
	2 = エラーを生成する上位エンフォーサ 3 = 一定期間にわたるデータベース複製エラー 4 = サイト状態レポート	
STARTTIME	レポートの生成を開始する日時。これは繰り返しのスケジュール内の予定時刻を設定します。	datetime, NOT NULL
LASTRUN	レポートが最後に作成された日時 (グリニッジ標準時)	bigint, NOT NULL
RUNHOURS	このレポートの繰り返しのスケジュール (時間単位)。たとえば、次のものがあります。 1 = 1 時間ごと 24 = 毎日 168 = 毎週 720 = 毎月	int, NOT NULL
NAME	この定時レポートの名前	NVARCHAR(255), varchar(255), NOT NULL
EMAIL	レポートを送信する電子メールアドレスのカンマ区切りのリスト	NVARCHAR(255), varchar(255), NOT NULL
DESCRIPTION	このレポートに対して管理者が提供した説明	NVARCHAR(255), varchar(255), NOT NULL
DISABLED	定時レポートが無効であるかどうか。 有効な値は次の通りです。 0 = いいえ 1 = はい	tinyint, NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除しました	tinyint, NOT NULL

ホームページ設定のスキーマ (HOMEPAGECONFIG テーブル)

表 1-38 はホームページ設定情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_HOMEPAGECONFIG として機能することを示します。

表 1-38 ホームページ設定のスキーマ

データベースのフィールド名	コメント	データタイプ
HOMEPAGECONFIG_IDX*	主キー。	char(32), NOT NULL
USER_NAME	管理者 GUID	char(32), NOT NULL
PARAMETER	パラメータ名	varchar(255), NULL
VALUE	パラメータ値	NVARCHAR(255), varchar(255), NOT NULL
USN	USN ベースのシリアル番号。このIDは一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
DELETED	削除された行: 0 = 削除されていない 1 = 削除しました	tinyint, NOT NULL

HPP 警告のスキーマ(HPP_ALERTS テーブル)

表 1-39 は TruScan プロアクティブ脅威スキャンイベント情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値は MSSQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_HPP_ALERTS として機能することを示します。

表 1-39 HPP 警告のスキーマ

データベースのフィールド名	コメント	データタイプ
IDX*	主キー。	char(32), NOT NULL
SENSITIVITY	検出を生成したエンジン感度の設定 (0 から 100 まで)	tinyint, NOT NULL
DETECTION_SCORE	検出のスコア (0 から 100 まで)	tinyint, NOT NULL
COH_ENGINE_VERSION	TruScan エンジンのバージョン	varchar(64), NOT NULL
DIS_SUBMIT	この検出をシマンテック社に提出する必要があるかどうかの推奨。 有効な値は次の通りです。 0 = いいえ 1 = はい	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
WHITELIST_REASON	ホワイトリストの理由。 有効な値は次の通りです。 0 = 許可アプリケーションリストにありません 100 = シマンテック許可アプリケーションリスト 101 = 管理者許可アプリケーションリスト 102 = ユーザー許可アプリケーションリスト	int, NOT NULL
USN	USN ベースのシリアル番号。このID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

HPP アプリケーションのスキーマ(HPP_APPLICATION テーブル)

表 1-40 は TruScan プロアクティブ脅威スキャンが検出するアプリケーションの情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第2の値は埋め込みデータベースに適用されます。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_HPP_APPLICATION として機能することを示します。

表 1-40 HPP アプリケーションのスキーマ

データベースのフィールド名	コメント	データタイプ
APP_IDX*	主キー。	char(32), NOT NULL
APP_HASH	このアプリケーションのためのハッシュ	varchar(64), NOT NULL
HASH_TYPE	使われたハッシュアルゴリズム。 有効な値は次の通りです。 0 = MD5 1 = SHA-1 2 = SHA-256	tinyint, NOT NULL
COMPANY_NAME	会社名	NVARCHAR(260), varchar(260), NOT NULL
APP_NAME	アプリケーション名	NVARCHAR(260), varchar(260), NOT NULL
APP_VERSION	アプリケーションのバージョン	NVARCHAR(256), varchar(256), NOT NULL
APP_TYPE	アプリケーションの種類。 有効な値は次の通りです。 0 = トロイの木馬ワーム 1 = トロイの木馬ワーム 2 = キーロガー 100 = リモート制御	int, NOT NULL
FILE_SIZE	ファイルサイズ	bigint, NOT NULL
DETECTION_TYPE	検出の種類。 有効な値は次の通りです。 0 = ヒューリスティック 1 = 商用アプリケーション	tinyint, NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL
HELP_VIRUS_IDX	シマンテック社のオンライン情報追記のヘルプ ID を提供する、VIRUS テーブルへの外部キー	char(32), NULL

ID マップのスキーマ (IDENTITY_MAP テーブル)

表 1-41 は ID マップ情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_IDENTITY_MAP として機能することを示します。

表 1-41 ID マップのスキーマ

データベースのフィールド名	コメント	データタイプ
ID*	オブジェクトの GUID	char(32), NOT NULL
NAME	オブジェクトの名前	nvarchar(2000), varchar(2000), NULL
TYPE	オブジェクトタイプ名	varchar(256), NULL
DOMAIN_ID	ドメインの GUID	char(32), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL
DELETED	<p>特定のレポートから削除されたクライアントグループを削除します。</p> <p>有効な値は次の通りです。</p> <p>0 or null = Not deleted</p> <p>1 = 削除しました</p>	tinyint, NULL

現在のリスクのインベントリのスキーマ (INVENTORYCURRENTRISK テーブル)

表 1-42 は現在のリスクのインベントリ情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されます。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キーPK_INVENTORYCURRENTRISKとして機能することを示します。

表 1-42 現在のリスクのインベントリのスキーマ

データベースのフィールド名	コメント	データタイプ
COMPUTER_IDX*	SEM_COMPUTER.COMPUTER_ID への外部キー	char(32), NOT NULL
ALERT_EVENT_IDX*	ALERTS.IDX への外部キー	char(32), NOT NULL
USN	USN ベースのシリアル番号。このIDは一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

現在のウイルスのインベントリのスキーマ (INVENTORYCURRENTVIRUS テーブル)

表 1-43 は現在のウイルスのインベントリ情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_PK_INVENTORYCURRENTVIRUSとして機能することを示します。

表 1-43 現在のウイルスのインベントリのスキーマ

データベースのフィールド名	コメント	データタイプ
COMPUTER_IDX*	SEM_COMPUTER.COMPUTER_IDへの外部キー	char(32), NOT NULL
ALERT_EVENT_IDX*	ALERTS.IDXへの外部キー	char(32), NOT NULL
USN	USNベースのシリアル番号。このIDは一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除しました	tinyint, NOT NULL

SCFインベントリのスキーマ(SCFINVENTORYテーブル)

SCFインベントリのデータテーブルは使われません。

表 1-44 は SCF インベントリ情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キーPK_SCFINVENTORYとして機能することを示します。

表 1-44 SCF インベントリのスキーマ(使われない)

データベースのフィールド名	コメント	データタイプ
AGENT_ID*	SEM_AGENT テーブルを指すポインタ	char(32), NOT NULL
IPSSIGDATE	IPS シグネチャの日付	datetime, NULL
IPSSIGREV	IPS シグネチャのリビジョン	int, NULL
SCFVERSION	ファイアウォールのバージョン	varchar(255), NOT NULL
SCFPOLICYFILE		varchar(510), NOT NULL
USN	USN ベースのシリアル番号。このID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

インベントリレポートのスキーマ (INVENTORYREPORT テーブル)

表 1-45 はインベントリレポート情報のデータベーススキーマを示しています。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キーPK_INVENTORYREPORTとして機能することを示します。

表 1-45 インベントリレポートのスキーマ

データベースのフィールド名	コメント	データタイプ
INVENTORYFILTER_IDX*	主キー。	char(32), NOT NULL
USER_ID	管理者 GUID	char(32), NOT NULL
FILTERNAME	この保存されたフィルタのユーザー指定の名前	NVARCHAR(255), varchar(255), NOT NULL
LASTCHECKINTIME	管理サーバーのチェックインの最終日時	datetime, NOT NULL
LASTSCANTIME	コンピュータがスキャンされた最終日時。 有効な値は次の通りです。 <ul style="list-style-type: none"> ■ 0 = 過去 1 週間 ■ 1 = 過去 1 カ月 ■ 2 = 過去 3 カ月 ■ 3 = 過去 1 年 ■ 4 = 過去 24 時間 ■ 5 = 今月 	int, NULL
RELATIVEDATETYPE	前回のチェックイン時間 (関連フィルタが使われた場合) 有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = 今月	int, NOT NULL
OPERATOR	使われない。	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
PATTERN_IDX	<p>キー(ウイルス対策シグネチャのバージョンのフィルタ)として使われるハードコードされた英語の文字列。</p> <p>有効な値は次の通りです。</p> <p>WITHIN_RELATIVE_30 = 過去 30 日以内</p> <p>WITHIN_RELATIVE_90 = 過去 90 日以内</p> <p>OUTSIDE_RELATIVE_30 = 過去 30 日より前</p> <p>OUTSIDE_RELATIVE_90 = 過去 90 日より前</p> <p>または、結果としてリビジョンの < = クエリーになるウイルス定義リビジョン</p>	varchar(255), NULL
PRODUCTVERSION	フィルタ処理する製品のバージョン	varchar(32), NULL
PROFILE_VERSION	フィルタ処理するプロファイルバージョン	varchar(64), NULL
IDS_VERSION	フィルタ処理する侵入検出システムシグネチャのバージョン	varchar(64), NULL
GOOD	使われない。	varchar(5), NULL
LICENSE_STATUS	使われない。	tinyint, NULL
STATUS	<p>有効な値は次の通りです。</p> <p>1 = オンライン</p> <p>0 = オフライン</p> <p>127 = フィルタなし(すべて)</p>	tinyint, NULL

データベースのフィールド名	コメント	データタイプ
ONOFF	Auto-Protect状態。 有効な値は次の通りです。 0 = オフのフィルタ 127 = フィルタなし(すべて)	tinyint, NULL
TAMPER_ONOFF	改変対策の状態。 有効な値は次の通りです。 0 = オフのフィルタ 127 = フィルタなし(すべて)	tinyint, NULL
REBOOT_REQUIRED	再起動が必要な状態。 有効な値は次の通りです。 1 = 再起動が必要なフィルタ 127 = フィルタなし(すべて)	tinyint, NULL
AVENGINE_ONOFF	ウイルス対策エンジンの状態。 有効な値は次の通りです。 0 = オフのフィルタ 127 = フィルタなし(すべて)	tinyint, NULL
TPM_DEVICE	インストール済み TPM デバイス。 有効な値は次の通りです。 1 = インストールされているデバイスのフィルタ 127 = フィルタなし(すべて)	tinyint, NULL
SERVERGROUPLIST	フィルタ処理するドメイン名のリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
CLIENTGROUPLIST	フィルタ処理するグループ名のリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
PARENTSERVERLIST	フィルタ処理するサーバー名のリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
SITELIST	フィルタ処理するサイト名のリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
R_OS_TYPE	有効な値は次の通りです。 0000 = すべて Windows 以外 0001= すべて Windows 0002= すべて Mac 0004= Mac OS X 10.4 0005= Mac OS X 10.5 0006= Mac OS X 10.6 0601 = Windows 7 0600 = Windows Vista 0502 = Windows 2003 および Windows XP 64-bit 0501 = Windows XP 0500 = Windows 2000 0400 = Windows NT 9999 = Windows Server 2008 -1 = フィルタなし(すべて)	int, NULL

データベースのフィールド名	コメント	データタイプ
HI_STATUS	次のコンプライアンス状態のフィルタ: 0 = 失敗 1 = 正常に完了 2 = 保留 3 = 無効 4 = 無視 127 = フィルタなし(すべて)	tinyint, NULL
HI_REASONCODE	次の理由のフィルタ: 0 = 成功 101 = ウイルス対策のバージョンが最新ではありません 102 = ウイルス対策が動作していません 103 = スクリプトが失敗しました 104 = 検査が不完全です 105 = 検査が無効です フィルタ処理するコンピュータ名のワイルドカードリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。 127 = 場所を変更しました -1 = フィルタなし(すべて)	int, NULL
SERVICE_PACK	OS サービスパック、またはフィルタなし(すべて)のときは %	NVARCHAR(64), varchar(64), NOT NULL
WORSTINFECTION_IDX	使われない。	int, NULL
COMPUTERLIST		NVARCHAR(512), varchar(512), NOT NULL

データベースのフィールド名	コメント	データタイプ
IDADDRESSLIST	フィルタ処理する IP アドレスのワイルドカードリスト (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
USERLIST	フィルタ処理するユーザー名のワイルドカードリスト (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
INFECTED	On = 感染したコンピュータのフィルタ	varchar(2), NULL
SORTORDER	コンピュータ状態ログのソートに使う列	varchar(32), NULL
SORTDIR	昇順または降順	varchar(5), NULL
FILVIEW	使われない。	varchar(16), NULL
CLIENTTYPE	使われない。	varchar(32), NULL
LIMITROWS	ページ付けに使う行数	int, NOT NULL
USERRELATIVE	相対日付 (「オン」) または絶対日付の使用	char(2), NOT NULL
REPORT_IDX	使われない。	int, NOT NULL
REPORTINPUTS	特殊なパラメータ (レポートに必要な場合)	NVARCHAR(64), varchar(64), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除しました	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
FIREWALL_ONOFF	ネットワーク脅威防止の状態。 有効な値は次の通りです。 0 = オフのフィルタ 127 = フィルタなし (すべて)	tinyint, NULL

検出された LAN デバイスのスキーマ (LAN_DEVICE_DETECTED テーブル)

検出された LAN デバイスのデータテーブルは Symantec Network Access Control で使われません。

表 1-46 は検出された LAN デバイス情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_LAN_DEVICE_DETECTED として機能することを示します。

表 1-46 検出された LAN デバイスのスキーマ

データベースのフィールド名	コメント	データタイプ
LAN_DEVICE_ID	デバイスの GUID	char(32), NOT NULL
AGENT_ID	エージェントの GUID	char(32), NOT NULL
COMPUTER_ID	クライアントコンピュータの GUID	char(32), NOT NULL
HASH*	コンピュータ HARDWARE_KEY とのリンク、グループ GUID	char(32), NOT NULL
MAC_ADDRESS*	デバイスの MAC アドレス	varchar(18), NOT NULL
IP_ADDRESS	デバイスの IP アドレス	bigint, NOT NULL
DEVICE_DETECTED_TIME	ドメインの GUID	bigint, NULL
ALERT	予約済み	tinyint, NULL

データベースのフィールド名	コメント	データタイプ
SEND_SNMP_TRAP	送信 SNMPトラップ処理を反映します。send が true の場合、SEND_SNMP_TRAP は true です。	tinyint, NULL
USN	更新シリアル番号(複製で使用)	bigint, NOT NULL
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除された 0 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

除外された LAN デバイスのスキーマ (LAN_DEVICE_EXCLUDED テーブル)

除外された LAN デバイスのデータテーブルは Symantec Network Access Control で使われません。

表 1-47 は除外された LAN デバイス情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初

の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されま
す。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー
PK_LAN_DEVICE_EXCLUDED として機能することを示します。

表 1-47 除外された LAN デバイスのスキーマ

データベースのフィールド名	コメント	データタイプ
EXCLUDED_ID*	レコードの GUID	char(32), NOT NULL
HASH	コンピュータ HARDWARE_KEY とのリンク、グループ GUID	char(32), NOT NULL
EXCLUDE_MODE		tinyint, NOT NULL
MAC_ADDRESS	デバイスの MAC アドレス	varchar(18), NULL
IP_ADDRESS	デバイスの IP アドレス	bigint, NULL
SUBNET_MASK	デバイスのサブネットマスク	bigint, NULL
IP_RANGE_START	IP アドレス範囲の開始	bigint, NULL
IP_RANGE_END	IP アドレス範囲の終わり	bigint, NULL
USN	更新シリアル番号 (複製で使用)	bigint, NOT NULL
TIME_STAMP	データベースレコードが修正され た日時 (マージの競合の解決に使用)	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除された フラグ。 有効な値は次の通りです。 0 = 削除された 1 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

レガシーエージェントのスキーマ (LEGACY_AGENT テーブル)

レガシーエージェントのデータテーブルは Symantec Network Access Control で使われません。

表 1-48 は製品の移行のために使われるレガシーエージェント情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MSSQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_LEGACY_AGENT として機能することを示します。

表 1-48 レガシーエージェントのスキーマ

データベースのフィールド名	コメント	データタイプ
LEGACY_AGENT_ID*	バージョン 5.x のエージェントからのエージェント ID。主キー。	char(32), NOT NULL
GROUP_PATH	SEM5 のグループ絶対パス	char(260), NOT NULL
POLICY_MODE	ユーザーモードまたはコンピュータモード	int, NOT NULL
LAN_SENSOR	エージェントが LAN_SENSOR の場合	int, NOT NULL
CLIENT_ID	SEM_CLIENT テーブルの GUID	char(32), NOT NULL
COMPUTER_ID	SEM_COMPUTER テーブルの GUID	char(32), NOT NULL
AGENT_ID	SEM_AGENT テーブルの GUID	char(32), NOT NULL
USN	更新シリアル番号 (複製で使用)	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除された 0 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

ローカルメタデータのスキーマ (LOCAL_METADATA テーブル)

表 1-49 は、ローカルメタデータ情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_LOCAL_METADATA として機能することを示します。

表 1-49 ローカルメタデータのスキーマ

データベースのフィールド名	コメント	データタイプ
ID*	GUID	char(32), NOT NULL
TYPE	local_metadata の種類。 現時点では、SemLocalSettings のみをサポート	varchar(256), NULL
CHECKSUM	XML コンテンツのチェックサム	char(32), NULL
CONTENT	スキーマオブジェクトの XML コンテンツ	image, NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 0 = 削除された 1 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

ログ設定のスキーマ (LOG_CONFIG テーブル)

表 1-50 はログ設定情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MSSQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_LOG_CONFIG として機能することを示します。

表 1-50 ログ設定のスキーマ

データベースのフィールド名	コメント	データタイプ
LOG_TYPE*	ログの種類。 有効な値は次の通りです。 101 = SERVER_SYSTEM_LOG 102 = SERVER_ADMIN_LOG 103 = SERVER_POLICY_LOG 104 = SERVER_CLIENT_LOG 105 = SERVER_ENFORCER_LOG 201 = AGENT_SYSTEM_LOG 202 = AGENT_SECURITY_LOG 203 = AGENT_TRAFFIC_LOG 204 = AGENT_PACKET_LOG 205 = AGENT_BEHAVIOR_LOG 301 = ENFORCER_SYSTEM_LOG 302 = ENFORCER_CLIENT_LOG 303 = ENFORCER_TRAFFIC_LOG	int, NOT NULL
TABLE_LIST	ログを切り替えるテーブルの名前	varchar(250), NOT NULL
THRESHOLD	ログの数のしきい値	int, NOT NULL
EXPIRATION	ログの有効期限	int, NOT NULL
CURRENT_TABLE	現在のログテーブルの名前	varchar(60), NOT NULL
CURRENT_ROWS	ログテーブル内の現在のログの数	int, NOT NULL
SWITCH_TIME	最後にログを切り替えた日時	bigint, NULL
RESERVED_INT1		int, NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

通知のスキーマ (NOTIFICATION テーブル)

表 1-51 は通知情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_NOTIFICATIONとして機能することを示します。

表 1-51 通知のスキーマ

データベースのフィールド名	コメント	データタイプ
NOTAG_IDX*	主キー、通知のインデックス	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
TYPE	<p>有効な値は次の通りです。</p> <p>VO = リスクアウトブレイク</p> <p>SO = 単一コンピュータ上のアウトブレイク</p> <p>VM = コンピュータの台数別のアウトブレイク</p> <p>1V = 単一リスクイベント</p> <p>NV = 新種のリスクを検出しました</p> <p>ID = ウイルス定義が最新ではありません</p> <p>AF = 認証エラー</p> <p>AFS = 単一サーバー上の認証エラー</p> <p>SE = システムイベント</p> <p>CS = クライアントセキュリティ警告</p> <p>CSS = 個々のコンピュータ上のクライアントセキュリティ警告</p> <p>CSM = コンピュータの台数別のクライアントセキュリティ警告</p> <p>LA = 新しい学習済みアプリケーション</p> <p>CL = クライアントリストを変更しました</p> <p>DF = サーバーの健全性</p> <p>UM = 管理外コンピュータ</p> <p>NS = 新しいソフトウェアパッケージ</p> <p>ED = エンフォーサが休止状態です</p> <p>WL = 強制または商用のアプリケーション検出</p>	varchar(30), NULL
USER_ID	管理者 GUID	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
TZ_OFFSET	管理者が通知を作成したタイムゾーン。電子メールで送信されたレポートに、管理者のローカルタイムゾーンの日付を表示できます。	int, NOT NULL
SERVERGROUP	この通知が適用されるサーバーグループの名前。カンマ区切りのリストで、ワイルドカードを使用できます。	NVARCHAR(255), varchar(255), NOT NULL
CLIENTGROUP	この通知が適用されるクライアントグループの名前。カンマ区切りのリストで、ワイルドカードを使用できます。	NVARCHAR(255), varchar(255), NOT NULL
PARENTSERVER	この通知が適用される親サーバーの名前。カンマ区切りのリストで、ワイルドカードを使用できます。	NVARCHAR(255), varchar(255), NOT NULL
COMPUTER	この通知が適用されるコンピュータの名前	NVARCHAR(255), varchar(255), NOT NULL
VIRUS	この通知が適用されるウイルスの名前。カンマ区切りのリストで、ワイルドカードを使用できます。	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
SOURCE	<p>この通知が適用されるスキャン。 ハードコードされた英語の文字列 がキーとして使われます。</p> <p>有効な値は次の通りです。</p> <p>% = すべて</p> <p>Scheduled Scan</p> <p>Manual Scan</p> <p>Real Time Scan</p> <p>Heuristic Scan</p> <p>Console</p> <p>Definition downloader</p> <p>system</p> <p>Startup Scan</p> <p>Idle Scan</p> <p>Manual Quarantine</p>	varchar(255), NULL

データベースのフィールド名	コメント	データタイプ
ACTACTION	有効な値は次の通りです。 % = フィルタなし(すべて) 1 = 検疫しました 3 = 削除しました 4 = 放置 5 = クリーニングしました 6 = クリーニングまたはマクロを削除しました 14 = 修復の保留 15 = 部分的に修復しました 16 = 再起動保留のプロセス終了 17 = 除外しました 19 = 削除によってクリーニングされました 20 = アクセスが拒否されました 21 = プロセスを終了 22 = 利用可能な修復なし 23 = すべての処理が失敗しました 98 = 疑いあり	varchar(255), NULL
HYPERLINK2	レポートの生成に使われるハイパーリンク	NVARCHAR(255), varchar(255), NOT NULL
NTIMES	この通知をトリガする必要がある件数	int, NOT NULL
XMINUTES	通知をトリガするために ntimes イベントが発生する必要のある時間帯	int, NOT NULL
EMAIL	この通知がトリガされる場合に電子メールで送信する、カンマ区切りの送信先リスト	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
LASTRUN	この通知が最後に分析された日時のタイムスタンプ	bigint, NOT NULL
TRIGGERED	警告が最後にトリガされた日時	bigint, NOT NULL
LASTRUN_DATA	通知の電子メールの詳細を示すために必要な追加データ	varchar(50), NULL
CATEGORY	この通知が適用されるウイルスのカテゴリ。 有効な値は次の通りです。 >= -1: フィルタなし(すべて) >= 1: カテゴリ 1(極低レベル)以上用のフィルタ >= 2: カテゴリ 2(低レベル)以上用のフィルタ >= 3: カテゴリ 3(中レベル)以上用のフィルタ >= 4: カテゴリ 4(高レベル)以上用のフィルタ >= 5: カテゴリ 5(非常に深刻)用のフィルタ = -1: 不明なリスク用のフィルタ	varchar(10), NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除しました	tinyint, NOT NULL
SYSTEM_EVENT	システムイベントのグループ	int, NOT NULL
SECURITY_EVENT	セキュリティイベントのグループ	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
DAMPER	警告間の最小静止時間(分)。0 は自動ダンパー (60 分) を意味します。	int, NOT NULL
BATCH_FILE_NAME	通知のトリガ時に実行するバッチファイルまたは実行可能ファイル	NVARCHAR(64), varchar(64), NOT NULL
NAME	通知設定の名前	NVARCHAR(255), varchar(255), NOT NULL

通知警告のスキーマ (NOTIFICATIONALERTS テーブル)

表 1-52 は通知警告情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_NOTIFICATIONALERTS として機能することを示します。

表 1-52 通知警告のスキーマ

データベースのフィールド名	コメント	データタイプ
IDX*	主キー、通知警告のインデックス	char(32), NOT NULL
NOTAG_IDX	この警告をトリガした通知。「notification」テーブルを指すポインタ	char(32), NOT NULL
ALERTDATETIME	警告が生成された日時のタイムスタンプ	datetime, NOT NULL
SUBJECT	警告の件名	NVARCHAR(255), varchar(255), NOT NULL
MSG	通知警告メッセージのテキスト	NVARCHAR(512), varchar(512), NOT NULL
HYPERLINK	警告の詳しい状況が記載されたレポートへのリンク	NVARCHAR(512), varchar(512), NOT NULL

データベースのフィールド名	コメント	データタイプ
ACKNOWLEDGED	警告に対応済みかどうかを示すフラグ	int, NOT NULL
ACKNOWLEDGED_USERID	この通知に対応したユーザーのGUID	char(32), NOT NULL
ACKNOWLEDGED_TIME	通知に対応した日時	datetime, NOT NULL
USN	USN ベースのシリアル番号。このID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

パターンのスキーマ(PATTERN テーブル)

表 1-53 はパターン情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キー PK_PATTERN として機能することを示します。

表 1-53 パターンのスキーマ

データベースのフィールド名	コメント	データタイプ
PATTERN_IDX*	主キー。	char(32), NOT NULL
CLIENT_MONIKER	このコンテンツ用のモニカ	varchar(40), NOT NULL

データベースのフィールド名	コメント	データタイプ
PATTERN_TYPE	ウイルス定義 = VIRUS_DEFS。 有効な値は次の通りです。 DECABI DEUCE_SIG ERASER_ENGINE PTS_CONTENT PTS_ENGINE SYKNAPPS_CAL SYKNAPPS_ENGINE SYKNAPPS_WHITELIST	NVARCHAR(128), varchar(128), NOT NULL
SEQUENCE	この定義と関連付けされるシーケンス番号	int, NOT NULL
PATTERNDATE	このコンテンツがリリースされた日付	datetime, NOT NULL
REVISION	このコンテンツのリビジョン番号	int, NOT NULL
VERSION	このコンテンツのバージョン番号	varchar(255), NOT NULL
INSERTDATETIME	このパターン情報がデータベースに入力された日時	datetime, NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除された	tinyint, NOT NULL

レポートのスキーマ (REPORTS テーブル)

レポートのデータテーブルは使われません。

表 1-54 はレポート情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キー PK_REPORTSとして機能することを示します。

表 1-54 レポートのスキーマ(使われない)

データベースのフィールド名	コメント	データタイプ
ID*	レポートオブジェクトの GUID	char(32), NOT NULL
TYPE	レポートの種類	varchar(256), NOT NULL
REPORT_TIME	レポートのサンプル時間	bigint, NOT NULL
SITE_ID	レポートが生成されたサイトの GUID	char(32), NOT NULL
DOMAIN_ID	レポートが属するドメインの GUID。 システム管理者用のレポートには DOMAIN_ID がありません。	char(32), NULL
CHECKSUM	XML コンテンツのチェックサム	char(32), NOT NULL
CONTENT	スキーマオブジェクトの XML コンテンツ	image, NOT NULL
USN	更新シリアル番号(複製で使用)	bigint, NOT NULL
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除された 0 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

スキャンレポートのスキーマ (SCANREPORT テーブル)

表 1-55 はスキャンレポート情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_SCANREPORTとして機能することを示します。

表 1-55 スキャンレポートのスキーマ

データベースのフィールド名	コメント	データタイプ
SCANFILTER_IDX*	主キー。	char(32), NOT NULL
USER_ID	管理者 GUID	char(32), NOT NULL
FILTERNAME	この保存されたフィルタのユーザー指定の名前	NVARCHAR(255), varchar(255), NOT NULL
STARTTIMEFROM	開始日	datetime, NOT NULL
STARTTIMETO	終了日	datetime, NOT NULL

データベースのフィールド名	コメント	データタイプ
RELATIVEDATETYPE	有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = 今月	int, NOT NULL
DURATION	スキャンの長さ	int, NOT NULL
FILESCANNED	スキャンしたファイルの数	bigint, NOT NULL
THREATS	スキャンにより検出されたリスクの数	int, NOT NULL
FILESINFECTED	スキャンにより検出されたファイルの数	bigint, NOT NULL
SCANSTARTMESSAGE	スキャンの説明	NVARCHAR(255), varchar(255), NOT NULL
STATUS	ハードコードされた英語キーとして表されるスキャン状態。 有効な値は次の通りです。 Completed 、 Cancelled 、 Started 、%(フィルタなし(すべての意味))	varchar(32), NULL
SERVERGROUPLIST	フィルタ処理するサーバーグループのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
CLIENTGROUPLIST	フィルタ処理するクライアントグループのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
PARENTSERVERLIST	フィルタ処理する親サーバーのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
COMPUTERLIST	フィルタ処理するコンピュータのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(512), varchar(512), NOT NULL
IPADDRESSLIST	フィルタ処理するIPアドレスのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
USERLIST	フィルタ処理するユーザーのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
LASTCOLUMN	使われない。	varchar(32), NULL
SORTORDER	有効な値は次の通りです。 'I.Computer' 'P.Parentserver' 'G.Clientgroup' 'C.Clientuser' 'S.Servergroup' 'SC.Startdatetime' 'SC.Duration' SC.Totalfiles(スキャンするすべてのファイル) 'SC.Threats' SC.Infected(感染したすべてのファイル)	varchar(32), NULL

データベースのフィールド名	コメント	データタイプ
SORTDIR	ソート方向。 有効な値は次の通りです。 desc = 降順 asc = 昇順	varchar(5), NULL
LIMITROWS	ページ付けに使う行数	int, NOT NULL
USERRELATIVE	相対日付(「オン」)または絶対日付の使用	char(2), NOT NULL
REPORT_IDX	使われない。	int, NOT NULL
REPORTINPUTS	特殊なパラメータ(レポートに必要な場合)	NVARCHAR(255), varchar(255), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除しました	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
R_OS_TYPE	有効な値は次の通りです。 0000 = すべて Windows 以外 0001=All Windows 0002=All Mac 0004= Mac OS X 10.4 0005= Mac OS X 10.5 0006= Mac OS X 10.6 0601 = Windows 7 0600 = Windows Vista 0502 = Windows 2003 and Windows XP 64-bit 0501 = Windows XP 0500 = Windows 2000 0400 = Windows NT 9999 = Windows Server 2008 -1 = フィルタなし(すべて)	int, NULL

スキャンのスキーマ (SCANS テーブル)

表 1-56 はスキャン情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されます。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_SCANSとして機能することを示します。

表 1-56 スキャンのスキーマ

データベースのフィールド名	コメント	データタイプ
SCAN_IDX*	主キー。	char(32), NOT NULL
SCAN_ID	エージェントによって提供されるスキャン ID	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
STARTDATETIME	スキャンの開始日時	datetime, NOT NULL
STOPDATETIME	スキャンの停止時間	datetime, NOT NULL
STATUS	ハードコードされた英語キーとして表されるスキャン状態。有効な値は次の通りです。 completed = 完了 canceled = キャンセル started = 開始	varchar(20), NULL
DURATION	スキャンの長さ(秒)	int, NOT NULL
COMPUTER_IDX	SEM_COMPUTER.COMPUTER_ID への外部キー	char(32), NOT NULL
CLIENTUSER1	スキャンの開始時にログオンしていたユーザー	NVARCHAR(64), varchar(64), NOT NULL
CLIENTUSER2	スキャンの終了時にログオンしていたユーザー	NVARCHAR(64), varchar(64), NOT NULL
SERVERGROUP_IDX	IDENTITY_MAP テーブル(ドメイン GUID)を指すポインタ	char(32), NOT NULL
PARENTSERVER_IDX	IDENTITY_MAP テーブル(サーバー GUID)を指すポインタ	char(32), NOT NULL
CLIENTGROUP_IDX	IDENTITY_MAP テーブル(グループ GUID)を指すポインタ	char(32), NOT NULL
MESSAGE1	スキャン開始時のスキャンメッセージ	NVARCHAR(255), varchar(255), NOT NULL
MESSAGE2	スキャン終了時のスキャンメッセージ	NVARCHAR(255), varchar(255), NOT NULL
THREATS	スキャンにより検出された脅威の数	bigint, NOT NULL
INFECTED	スキャンにより検出された感染ファイルの数	bigint, NOT NULL
TOTALFILES	スキャンしたファイルの数	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
OMITTED	省略したファイルの数	bigint, NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 0 = 削除されていない 1 = 削除しました	tinyint, NOT NULL
SCAN_TYPE	スキャンの種類。 有効な値は次の通りです。 ScanNow_Quick = アクティブスキャン ScanNow_Full = 完全スキャン ScanNow_Custom = 管理者が定義したスキャン	varchar(64), NULL
COMMAND_ID	SEM_JOB テーブルを指すポインタ。このスキャンを開始したコマンド ID (存在する場合)	varchar(32), NULL

SE グローバルのスキーマ(SE_GLOBAL テーブル)

表 1-57 はシステムシーケンス番号のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

このテーブルには主キーは指定されません。

表 1-57 SE グローバルのスキーマ

データベースのフィールド名	コメント	データタイプ
SEQ_NUM	サイトの最新の USN	bigint, NOT NULL

SEM エージェントのスキーマ (SEM_AGENT テーブル)

表 1-58 はエージェント情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_SEM_AGENTとして機能することを示します。

表 1-58 SEM エージェントのスキーマ

データベースのフィールド名	コメント	データタイプ
AGENT_ID*	エージェントの GUID	char(32), NOT NULL
AGENT_TYPE	インストールされたエージェントの種類。 有効な値は次の通りです。 105 = Symantec Endpoint Protection 151 = Symantec Network Access Control	varchar(64), NULL

データベースのフィールド名	コメント	データタイプ
R_OS_TYPE		int, NULL

データベースのフィールド名	コメント	データタイプ
	<p>クライアントコンピュータのオペレーティングシステムの種類。</p> <p>有効な値は次の通りです。</p> <p>262145 = Windows 95</p> <p>262401 = Windows 95 OSR2</p> <p>264705 = Windows 98</p> <p>264961 = Windows 98SE</p> <p>285185 = Windows Me</p> <p>17039362 = Windows NT 4.0 Workstation</p> <p>17104898 = Windows 2000 Professional</p> <p>17105154 = Windows XP Professional</p> <p>17105170 = Windows XP Home Edition</p> <p>17105186 = Windows XP Home Embedded</p> <p>17170434 = Windows Vista Ultimate Edition</p> <p>17170435 = Windows Vista Home Basic Edition</p> <p>17170436 = Windows Vista Home Premium Edition</p> <p>17170437 = Windows Vista Enterprise Edition</p> <p>17170439 = Windows Vista Business Edition</p> <p>17170444 = Windows Vista Starter Edition</p> <p>17170690 = Windows 7</p> <p>50593794 = Windows NT 4.0 Server</p>	

データベースのフィールド名	コメント	データタイプ
	50593810 = Windows NT 4.0 Server Enterprise Edition 50659330 = Windows 2000 Server 50659346 = Windows 2000 Datacenter Server 50659362 = Windows 2000 Advanced Server 50659842 = Windows Server 2003 Standard Edition 50659858 = Windows Server 2003 Datacenter Edition 50659874 = Windows Server 2003 Enterprise Edition 50659890 = Windows Server 2003 Web Edition 50724882=Windows Server 2008 269091840 = Mac OS X 10.4 269092096 = Mac OS X 10.5 269092352 = Mac OS X 10.6 0 = OS の種類が未指定	
COMPUTER_ID	登録済みコンピュータの GUID	char(32), NULL
DOMAIN_ID	ドメインの GUID	char(32), NULL
GROUP_ID	エージェントの現在のグループ GUID	char(32), NULL
AGENT_VERSION	エージェントソフトウェアのバージョン	nvarchar(64), varchar(64), NULL
PROFILE_VERSION	エージェントの現在のプロファイルバージョン	varchar(64), NULL
PROFILE_SERIAL_NO	エージェントの現在のプロファイルシリアル番号	varchar(64), NULL

データベースのフィールド名	コメント	データタイプ
PROFILE_CHECKSUM	エージェントの現在のプロフィール チェックサム	char(32), NULL
IDS_VERSION	エージェントの現在の IDS バージョン	varchar(64), NULL
IDS_SERIAL_NO	エージェントの現在の IDS シリアル 番号	varchar(64), NULL
IDS_CHECKSUM	エージェントの現在の IDS チェック サム	char(32), NULL
HI_STATUS	ホストインテグリティの状態。 有効な値は次の通りです。 0 = 失敗 1 = 正常に完了 2 = 保留 3 = 無効 4 = 無視	int, NULL
HI_REASONCODE	ホストインテグリティの理由コード。 有効な値は次の通りです。 0 = 成功 101 = ウイルス対策のバージョン が最新ではありません 102 = ウイルス対策が動作して いません 103 = スクリプトが失敗しました 104 = 検査が不完全です 105 = 検査が無効です 127 = 場所を変更しました	int, NULL
HI_REASONDESC	ホストインテグリティの説明	varchar(64), NULL
CREATION_TIME	エージェントの作成日時	bigint, NULL

データベースのフィールド名	コメント	データタイプ
STATUS	エージェントのオンライン状態。 有効な値は次の通りです。 0 = オフライン 1 = オンライン	tinyint, NULL
LAST_UPDATE_TIME	エージェントの最新オンライン日時	bigint, NULL
LAST_SERVER_ID	最後に接続したサーバーのGUID	char(32), NULL
LAST_SITE_ID	最後に接続したサイトの GUID	char(32), NULL
ATTRIBUTE_EXTENSION	使われない。	nvarchar(2000), varchar(2000), NULL
FULL_NAME	従業員のフルネーム	nvarchar(256), varchar(256), NULL
EMAIL	従業員の電子メールアドレス	nvarchar(129), varchar(129), NULL
JOB_TITLE	従業員の役職名	nvarchar(128), varchar(128), NULL
DEPARTMENT	従業員の部署	nvarchar(128), varchar(128), NULL
EMPLOYEE_NUMBER	従業員の番号	varchar(32), NULL
EMPLOYMENT_STATUS	従業員の状態	varchar(16), NULL
OFFICE_PHONE	従業員のオフィスの電話番号	varchar(32), NULL
MOBILE_PHONE	従業員の携帯電話番号	varchar(32), NULL
HOME_PHONE	従業員の自宅電話番号	varchar(32), NULL
USN	更新シリアル番号(複製で使用)	bigint, NOT NULL
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除しました 0 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
PATTERN_IDX	テーブル「pattern」を指すポインタ	char(32), NOT NULL
AP_ONOFF	Auto-Protect 状態。 有効な値は次の通りです。 1 = オン 2 = インストールされていない 0 = オフ 127 = 報告なし	tinyint, NOT NULL
INFECTED	このコンピュータが感染しているかどうか。 有効な値は次の通りです。 0 = 感染していない 1 = 感染している	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
WORSTINFECTION_IDX	<p>最悪の検出。</p> <p>有効な値は次の通りです。</p> <p>0 =(重大度 0) ウイルス性</p> <p>1 =(重大度 1) 非ウイルス性の悪質コード</p> <p>2 =(重大度 2) 悪質コード</p> <p>3 =(重大度 3) ウイルス対策 - ヒューリスティック</p> <p>5 =(重大度 5) ハッキングツール</p> <p>6 =(重大度 6) スパイウェア</p> <p>7 =(重大度 7) トラックウェア</p> <p>8 =(重大度 8) ダイヤラー</p> <p>9 =(重大度 9) リモートアクセス</p> <p>10 =(重大度 10) アドウェア</p> <p>11 =(重大度 11) ジョークプログラム</p> <p>12 =(重大度 12) クライアントコンプライアンス</p> <p>13 =(重大度 13) 汎用ロードポイント</p> <p>14 =(重大度 14) プロアクティブ脅威スキャン - ヒューリスティック</p> <p>15 =(重大度 15) cookie</p> <p>9999 = 検出はありません</p>	int, NOT NULL
LAST_SCAN_TIME	このエージェントの前回のスキャン日時 (グリニッジ標準時)	bigint, NOT NULL
LAST_VIRUS_TIME	前回、クライアントコンピュータでウイルスが検出された日時 (グリニッジ標準時)	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
CONTENT_UPDATE	コンテンツ更新の受け入れ。 有効な値は次の通りです。 1 = はい 0 = いいえ	tinyint, NOT NULL
AVENGINE_ONOFF	RTVScan の状態。 有効な値は次の通りです。 1 = オン 2 = インストールされていない 0 = オフ 127 = 報告なし	tinyint, NOT NULL
TAMPER_ONOFF	改変対策の状態。 有効な値は次の通りです。 1 = オン 2 = インストールされていない 0 = オフ 127 = 状態の報告なし	tinyint, NOT NULL
MAJOR_VERSION	Symantec Endpoint Protection のバージョン: 11.	int, NOT NULL
MINOR_VERSION	マイナーバージョン	int, NOT NULL
REBOOT_REQUIRED	再起動が必要 有効な値は次の通りです。 0 = いいえ 1 = はい	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
REBOOT_REASON	<p>形式は <コンポーネント> = <理由 ID>; <コンポーネント> = <理由 ID>...</p> <p>コンポーネントは次の通りです。</p> <p>AVMAN = ウイルス対策</p> <p>LUMAN = LiveUpdate</p> <p>FW = ネットワーク脅威防止</p> <p>GUP = グループ更新プロバイダ</p> <p>理由は次の通りです。</p> <p>1 = 完了待ちリスク修復</p> <p>2 = 適用待ち製品パッチ</p> <p>3 = 適用待ちコンテンツダウンロード</p>	varchar(128), NULL
LICENSE_STATUS	将来に使用予定。	int, NOT NULL
LICENSE_EXPIRY	将来に使用予定。	bigint, NOT NULL
TIMEZONE	クライアントコンピュータのタイムゾーンオフセット	int, NOT NULL
FIREWALL_ONOFF	<p>ファイアウォールの状態。</p> <p>有効な値は次の通りです。</p> <p>1 = オン</p> <p>2 = インストールされていない</p> <p>0 = オフ</p> <p>127 = 報告なし</p>	tinyint, NOT NULL
FREE_MEM	利用可能な空きメモリ	bigint, NULL
FREE_DISK	利用可能な空きディスク容量	bigint, NULL
LAST_DOWNLOAD_TIME	前回のダウンロード日時	bigint, NOT NULL
CURRENT_CLIENT_ID	このエージェントにログオンしているクライアント。	char(32), NULL

SEM アプリケーションのスキーマ (SEM_APPLICATION テーブル)

表 1-59 はアプリケーション情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_SEM_APPLICATION として機能することを示します。

表 1-59 SEM アプリケーションのスキーマ

データベースのフィールド名	コメント	データタイプ
DOMAIN_ID*	ドメインの GUID	char(32), NOT NULL
APP_HASH*	学習済みアプリケーションのチェックサム(名前、パス、ファイルチェックサム、ファイルサイズなどを含む)	char(32), NOT NULL
APPLICATION_NAME	学習済みアプリケーションの名前	NVARCHAR(260), varchar(260), NOT NULL
APPLICATION_PATH	学習済みアプリケーションのパス	nvarchar(260), varchar(260), NULL
APP_DESCRIPTION	学習済みアプリケーションの説明	nvarchar(1024), varchar(1024), NULL
CHECKSUM	アプリケーションバイナリファイルのチェックサム	char(32), NOT NULL
FILE_SIZE	アプリケーションバイナリファイルのサイズ	bigint, NULL
VERSION	アプリケーションバイナリファイルのバージョン	varchar(256), NULL
LAST_MODIFY_TIME	前回のアプリケーションバイナリファイルの修正日時	bigint, NULL
USN	更新シリアル番号(複製で使用)	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除された 0 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

SEM クライアントのスキーマ(SEM_CLIENT テーブル)

表 1-60 はクライアント情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_SEM_CLIENTとして機能することを示します。

表 1-60 SEM クライアントのスキーマ

データベースのフィールド名	コメント	データタイプ
CLIENT_ID*	クライアントの GUID。主キー。	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
DOMAIN_ID	ドメインの GUID	char(32), NULL
GROUP_ID	グループの GUID	char(32), NULL
GROUP_IS_OU	クライアントが Active Directory からかどうか	tinyint, NULL
OU_GUID	クライアントが Active Directory からであれば、組織単位の GUID	char(32), NULL
POLICY_MODE	Enum {USER_MODE, COMPUTER_MODE}	int, NULL
COMPUTER_ID	登録済みコンピュータの GUID	char(32), NULL
HARDWARE_KEY	コンピュータハードウェアの情報のハッシュ	char(32), NULL
COMPUTER_NAME	コンピュータ名	nvarchar(64), varchar(64), NULL
COMPUTER_DOMAIN_NAME	コンピュータの説明	nvarchar(256), varchar(256), NULL
DESCRIPTION	コンピュータのドメイン名	nvarchar(256), varchar(256), NULL
USER_NAME	ユーザーのログオン名	nvarchar(64), varchar(64), NULL
FULL_NAME	ユーザーの氏名	nvarchar(64), varchar(64), NULL
USER_DOMAIN_NAME	ユーザーのログオンドメイン名	nvarchar(256), varchar(256), NULL
HASH	次のハッシュ: POLICY_MODE COMPUTER_NAME COMPUTER_DOMAIN_NAME USER_NAME USER_DOMAIN_NAME	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
PIN_MARK	このクライアントを Active Directory と同期するかどうかを示すフラグ	tinyint, NULL
EXTRA_FEATURE		int, NULL
CREATOR		tinyint, NULL
CREATION_TIME	クライアントの作成日時	bigint, NULL
USN	更新シリアル番号(複製で使用)	bigint, NOT NULL
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除された 0 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

SEM コンプライアンス基準のスキーマ (SEM_COMPLIANCE_CRITERIA テーブル)

表 1-61 はコンプライアンス基準情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_SEM_COMPLIANCE_CRITERIA として機能することを示します。

表 1-61 SEM コンプライアンス基準のスキーマ

データベースのフィールド名	コメント	データタイプ
CRITERIA_IDX*	主キー。	char(32), NOT NULL
AGENT_SECURITY_LOG_IDX*	V_AGENT_SECURITY.AGENT_SECURITY_LOG_IDX への外部キー	char(32), NOT NULL
ACTION	ACTION はハードコードされた英語キーで、「check」か「remediation」のいずれかの値を指定できます。	varchar(64), NULL
RULE_NAME	管理者がポリシーから指定したルール名	NVARCHAR(256), varchar(256), NOT NULL
RULE_TYPE	RULE_TYPE はハードコードされた英語キーで、次のいずれかの値を指定できます。 antivirus antispysware patch service pack ファイアウォール カスタム unknown - サーバーでのログ処理時にフォールバックし、結果はヌルまたは空白になる	varchar(64), NULL

データベースのフィールド名	コメント	データタイプ
CRITERIA		varchar(256), NULL

データベースのフィールド名	コメント	データタイプ
	<p>CRITERIA はハードコードされた英語キーで、次のいずれかの値を指定できます。</p> <p>as_is_installed</p> <p>as_is_running</p> <p>as_signature_ok</p> <p>av_is_installed</p> <p>av_is_running</p> <p>av_signature_ok</p> <p>file_age_ok</p> <p>file_date_ok</p> <p>file_size_ok</p> <p>file_version_ok</p> <p>file_download</p> <p>file_exists</p> <p>file_checksum_ok</p> <p>file_execute</p> <p>fw_is_installed</p> <p>fw_is_running</p> <p>patch_is_installed</p> <p>reg_value_incr</p> <p>reg_key_exists</p> <p>reg_value_ok</p> <p>reg_value_exists</p> <p>reg_value_set</p> <p>timestamp_ok</p> <p>msg_dlg_ok</p> <p>os_ok</p> <p>os_lang_ok</p>	

データベースのフィールド名	コメント	データタイプ
	<p>process_is_running - ユーザーアプリケーションまたはサービスを意味する</p> <p>file_delete</p> <p>service_pack_ok</p> <p>hi_setup</p> <p>remediation - 修復の全体的な状態を取得する</p> <p>unknown - 基準がヌルまたは空白の場合に、サーバーでフォールバックを実行する</p>	
TARGET	<p>基準の対象。たとえば、ウイルス対策製品名、ファイアウォール製品名、ファイル名、レジストリキー、レジストリ値など。または、パッチのバージョン、OS のバージョン、プロセス名、サービス名など。</p>	<p>NVARCHAR(256), varchar(256), NOT NULL</p>
RESULT	<p>RESULT は次のいずれかの値を取ります。</p> <p>pass</p> <p>fail</p> <p>ignore</p> <p>エラー</p> <p>postponed - 修復基準用</p> <p>unknown - 基準またはルールが最終状態なしで終了する場合に、サーバーでフォールバックを実行する</p>	<p>varchar(64), NULL</p>

データベースのフィールド名	コメント	データタイプ
ERROR		varchar(128), NULL

データベースのフィールド名	コメント	データタイプ
	<p>ERRORは次のいずれかの値を取ります。</p> <p>unknown = 不明</p> <p>product_unknown = 製品が不明です</p> <p>file_notfound = ファイルが見つかりません</p> <p>filename_invalid = 無効なファイル名</p> <p>parameter_invalid = 無効な条件パラメータ</p> <p>parameter_undefined = ポリシーで条件パラメータを指定しませんでした</p> <p>bad_url = URL の形式が無効です</p> <p>filedownload_op_err = URL がアクセス不能か送信先ファイルを作成できませんでした</p> <p>time_out = 処理がタイムアウトになりました</p> <p>connection_lost = 接続が消失しました</p> <p>access_violation = ファイルのアクセス違反</p> <p>access_denied = アクセス拒否</p> <p>remediation_abort = ユーザーが修復を中止しました</p> <p>remediation_postpone = ユーザーが修復を延期しました</p> <p>createdir_failed = ディレクトリ作成が失敗しました</p> <p>system_err = システムエラー</p> <p>runas_noprivilege = 必須の権限</p>	

データベースのフィールド名	コメント	データタイプ
	がクライアントにありません internal_err = 内部エラー os_unknown = オペレーティング システムの種類を検出できません でした	

データベースのフィールド名	コメント	データタイプ
DESCRIPTION		NVARCHAR(256), varchar(256), NOT NULL

データベースのフィールド名	コメント	データタイプ
	<p>追加のコンプライアンス検査の詳細。例外テキスト、または次のいずれか。</p> <p>Checksum_blank = フィンガープリント値が空です</p> <p>Failed_to_get_modification_date = 修正日を取得できませんでした</p> <p>NAN = 数字ではありません</p> <p>Cannot_parse_URL = URL を解析できませんでした</p> <p>URL_not_accessible_or_failed_to_create_destination_file = URL がアクセス不能か送信先ファイルを作成できませんでした</p> <p>Download_exceeded_limit = ダウンロードで限度を超えました</p> <p>Destination = 送信先ファイルアクセス違反</p> <p>By_User = ユーザーが開始した処理</p> <p>Access_denied_by_server = サーバーによるアクセス拒否</p> <p>Download_file = ダウンロードファイルが見つかりません</p> <p>Process_time_out = 処理がタイムアウトになりました</p> <p>Failed_to_detect_OS_type = OS の種類を検出できませんでした</p> <p>Application_name_is_empty = アプリケーション名が空です</p> <p>Probably_software_is_not_installed = おそらくソフトウェアをインストールしていません</p> <p>Signature_age_in_seconds_failed = シグネチャの経過時間を計算で</p>	

データベースのフィールド名	コメント	データタイプ
	<p>きませんでした</p> <p>Failed_to_parse_URL = URL を解析できませんでした</p> <p>Missing_or_no_OS_version_info = バージョン情報が見つからないかありません</p> <p>After_script_file_running = スクリプトファイルの実行後</p> <p>OS_ignore = オペレーティングシステム検査が無視されました</p> <p>Save_failed = 保存が失敗しました</p> <p>No_previous_time = 以前の時間がありません</p> <p>OK_or_YES = ユーザーの応答が OK または「はい」でした</p> <p>= ユーザーの応答が「キャンセル」または「いいえ」でした</p> <p>Fail to get current OS language version = 現在のオペレーティングシステム言語を取り込めませんでした</p>	
USN	更新シリアル番号(複製で使用)	bigint, NOT NULL
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL
DELETED	<p>スキーマオブジェクトの削除されたフラグ。</p> <p>有効な値は次の通りです。</p> <p>1 = 削除しました</p> <p>0 = 削除されていない</p>	tinyint, NOT NULL

SEM コンピュータのスキーマ(SEM_COMPUTER テーブル)

表 1-62 はコンピュータ情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_SEM_COMPUTER として機能することを示します。

表 1-62 SEM コンピュータのスキーマ

データベースのフィールド名	コメント	データタイプ
COMPUTER_ID*	コンピュータの GUID。 コンピュータはコンソールとクライアントの両方から追加できます。 主キー。	char(32), NOT NULL
DOMAIN_ID	ドメインの GUID	char(32), NULL
HARDWARE_KEY	コンピュータハードウェアの情報のハッシュ	char(32), NULL
COMPUTER_NAME	コンピュータ名	nvarchar(64), varchar(64), NULL
COMPUTER_DOMAIN_NAME	コンピュータの説明	nvarchar(256), varchar(256), NULL
COMPUTER_DESCRIPTION	コンピュータのドメイン名	nvarchar(256), varchar(256), NULL
PROCESSOR_TYPE	CPU の種類	nvarchar(64), varchar(64), NULL
PROCESSOR_CLOCK	CPU クロック	bigint, NULL
PROCESSOR_NUM	CPU の数	int, NULL
MEMORY	物理メモリ (KB)	bigint, NULL
BIOS_VERSION	BIOS のバージョン	varchar(128), NULL
TPM_DEVICE	TPM デバイス ID	int, NULL

データベースのフィールド名	コメント	データタイプ
OPERATION_SYSTEM	オペレーティングシステム名	nvarchar(64), varchar(64), NULL
SERVICE_PACK	Service Pack	nvarchar(64), varchar(64), NULL
CURRENT_LOGIN_USER	ログオンしているユーザー	nvarchar(64), varchar(64), NULL
CURRENT_LOGIN_DOMAIN	Windows ドメイン	nvarchar(256), varchar(256), NULL
DNS_SERVER1		bigint, NULL
DNS_SERVER2		bigint, NULL
WINS_SERVER1		bigint, NULL
WINS_SERVER2		bigint, NULL
DHCP_SERVER		bigint, NULL
MAC_ADDR1		varchar(17), NULL
IP_ADDR1		bigint, NULL
GATEWAY1		bigint, NULL
SUBNET_MASK1		bigint, NULL
MAC_ADDR2		varchar(17), NULL
IP_ADDR2		bigint, NULL
GATEWAY2		bigint, NULL
SUBNET_MASK2		bigint, NULL
MAC_ADDR3		varchar(17), NULL
IP_ADDR3		bigint, NULL
GATEWAY3		bigint, NULL
SUBNET_MASK3		bigint, NULL
MAC_ADDR4		varchar(17), NULL

データベースのフィールド名	コメント	データタイプ
IP_ADDR4		bigint, NULL
GATEWAY4		bigint, NULL
SUBNET_MASK4		bigint, NULL
USN	更新シリアル番号 (複製で使用)	bigint, NOT NULL
TIME_STAMP	データベースレコードが修正された日時 (マージの競合の解決に使用)	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除された 0 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL
DISK_TOTAL	ディスク容量の合計	bigint, NULL
DISK_DRIVE	DISK_TOTAL によって参照されるドライブ文字	varchar(3), NULL
OS_LANG	オペレーティングシステムの言語 ID (例: 英語 = 0x09)	int, NULL

SEM コンテンツのスキーマ (SEM_CONTENT テーブル)

表 1-63 はコンテンツ情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されます。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_SEM_CONTENTとして機能することを示します。

表 1-63 SEM コンテンツのスキーマ

データベースのフィールド名	コメント	データタイプ
AGENT_ID*	エージェントの GUID	char(32), NOT NULL
PATTERN_IDX*	pattern テーブルを指すポインタ	char(32), NOT NULL
USN	更新シリアル番号 (複製で使用)	bigint, NOT NULL
TIME_STAMP	データベースレコードが修正された日時 (マージの競合の解決に使用)	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 1 = 削除された 0 = 削除されていない	tinyint, NOT NULL

SEM ジョブのスキーマ (SEM_JOB テーブル)

表 1-64 はジョブ情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されます。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_SEM_JOBとして機能することを示します。

表 1-64 SEM ジョブのスキーマ

データベースのフィールド名	コメント	データタイプ
COMMAND_ID*	コマンドオブジェクトの GUID。この GUID は基本メタデータテーブルの ID に対応します。	char(32), NOT NULL
USN	更新シリアル番号 (複製で使用)	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
COMMAND_NAME	<p>起動したコマンドを示す、ハードコードされた英語の文字列。これは、XML 内に配置される定義済みの名前用の文字列と同じです。有効な値は次の通りです。</p> <p>Update_Now = コンテンツの更新</p> <p>ScanNow_Full = 完全スキャン</p> <p>ScanNow_Quick = アクティブスキャン</p> <p>ScanNow_Custom = カスタムスキャン</p> <p>Update_ScanNow_Full = コンテンツの更新と完全スキャン</p> <p>Update_ScanNow_Quick = コンテンツの更新とクイックスキャン</p> <p>Update_ScanNow_Custom = コンテンツの更新とカスタムスキャン</p> <p>CancelScan = スキャンの中止</p> <p>Reboot = 再起動</p> <p>ApOn = Auto-Protect をオンにする</p> <p>ApOff = Auto-Protect をオフにする</p> <p>FwOn = ファイアウォールをオンにする</p> <p>FwOff = ファイアウォールをオフにする</p> <p>DeleteQuarantine = 検疫から削除</p>	varchar(64), NULL
COMMAND_DESC	コマンドの詳しい説明	nvarchar(350), varchar(350), NULL
SOURCE_SITE_ID	コマンドが生成されたサイトの GUID	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
SOURCE_ADMIN_ID	コマンドを発行した管理者のGUID	char(32), NOT NULL
CREATE_TIME	管理者がコンソールでコマンドを発行した日時	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970年以降のミリ秒	bigint, NOT NULL
DELETED	削除された行: 1 = 削除しました 0 = 削除されていない	tinyint, NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		varchar(260), NULL
RESERVED_BINARY		varbinary(1000), NULL

シリアル番号のスキーマ(SERIAL_NUMBERS テーブル)

表 1-65 はシリアル番号情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

このテーブルには主キーは指定されません。

表 1-65 シリアル番号のスキーマ

データベースのフィールド名	コメント	データタイプ
GROUP_ID	グループの GUID	char(32), NOT NULL
PROFILE_SERIAL_NO	グループのプロファイルシリアル番号	varchar(64), NOT NULL

サーバー管理ログ 1 と 2 のスキーマ (SERVER_ADMIN_LOG_1 テーブルと SERVER_ADMIN_LOG_2 テーブル)

表 1-66 はサーバー管理ログのデータベーススキーマを説明したものです。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

このテーブルには主キーは指定されません。

表 1-66 サーバー管理ログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	ログが属するドメインの GUID	char(32), NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
SEVERITY	Enum (SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST)	int, NOT NULL
ADMIN_NAME	管理者の名前	NVARCHAR(250), varchar(250), NOT NULL

サーバー管理ログ 1 と 2 のスキーマ (SERVER_ADMIN_LOG_1 テーブルと SERVER_ADMIN_LOG_2 テーブル)

データベースのフィールド名	コメント	データタイプ
EVENT_ID		int, NOT NULL

データベースのフィールド名	コメント	データタイプ
	管理イベントの重複のない ID。 有効な値は次の通りです。 0x1001 = ログインが正常に完了 0x1002 = ログイン失敗 0x1003 = ログアウト 0x1004 = アカウントがロック 0x1005 = アカウントがロック解除 0x1006 = アカウントが無効です 0x1007 = アカウントが有効です 0x1008 = 管理者を作成しました 0x1009 = 管理者を削除しました 0x100A = 管理者名を変更しました 0x100B = パスワードを変更しました 0x100C = 管理者のプロパティを変更しました 0x100D = ドメインを作成しました 0x100E = ドメインを削除しました 0x100F = ドメインのプロパティを変更しました 0x1020 = ドメインが無効です 0x1021 = ドメインが有効です 0x1022 = ドメイン名を変更しました 0x2001 = グループを作成しました 0x2002 = グループを削除しました 0x2003 = グループ名を変更しました	

データベースのフィールド名	コメント	データタイプ
	0x2004 = グループを移動しました	
	0x2005 = グループのプロパティを変更しました	
	0x2006 = ユーザーを作成しました	
	0x2007 = ユーザーを削除しました	
	0x2008 = ユーザーを移動しました	
	0x2009 = ユーザーをコピーしました	
	0x200A = ユーザーポリシーモードを切り替えます	
	0x200B = ユーザーのプロパティを変更しました	
	0x200C = コンピュータを作成しました	
	0x200D = コンピュータを削除しました	
	0x200E = コンピュータを移動しました	
	0x200F = コンピュータをコピーしました	
	0x2010 = コンピュータポリシーモードを切り替えました	
	0x2011 = コンピュータのプロパティを変更しました	
	0x2012 = 組織単位をインポートしました	
	0x2013 = ドメインユーザーをインポートしました	
	0x2014 = LDAP ユーザーをインポートしました	

データベースのフィールド名	コメント	データタイプ
	0x3001 = パッケージを作成しました	
	0x3002 = パッケージを削除しました	
	0x3003 = パッケージをエクスポートしました	
	0x3004 = パッケージをごみ箱に移動しました	
	0x3005 = パッケージが最新になりました	
	0x3006 = パッケージを他のドメインに追加しました	
	0x3007 = パッケージのプロパティを変更しました	
	0x3008 = パッケージ配備を作成しました	
	0x3009 = パッケージ配備を削除しました	
	0x300A = パッケージ配備のプロパティを変更しました	
	0x300B = パッケージを更新しました	
	0x4001 = 複製パートナーを登録しました	
	0x4002 = 複製パートナーを削除しました	
	0x4003 = リモートサイトを削除しました	
	0x4004 = サイトのプロパティを変更しました	
	0x4005 = サーバーのプロパティを変更しました	
	0x4006 = データベースのプロパティを変更しました	

データベースのフィールド名	コメント	データタイプ
	<p>0x4007 = パートナーのプロパティを変更しました</p> <p>0x4008 = サイトライセンスを変更しました</p> <p>0x4009 = エンフォーサライセンスを変更しました</p> <p>0x4010 = 今すぐに複製</p> <p>0x4011 = 今すぐにバックアップ</p> <p>0x4012 = 外部ログ記録のプロパティを変更しました</p> <p>0x4013 = サイトのバックアップ設定を変更しました</p> <p>0x4014 = サーバーを削除しました</p> <p>0x4015 = サーバー証明書を変更しました</p> <p>0x4016 = エンフォーサグループのプロパティを変更しました</p>	
EVENT_DESC	イベントの説明。通常、説明の 1 行目は「概略」として扱われます。	nvarchar(256), varchar(256), NULL
MSG_ID	イベントの説明 ID。この ID を使って各国のメッセージをロードします。このイベントに例外が関係する場合にのみ使われます。	int, NULL
ERROR_CODE	ErrorCode はソースコード内のエラーを重複なく識別できます。このイベントに例外が関係する場合にのみ使われます。	int, NULL
STACK_TRACE	例外のスタックトレース。このイベントに例外が関係する場合にのみ使われます。	nvarchar(2000), varchar(2000), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(520), NULL
RESERVED_BINARY		varbinary(2000), NULL

サーバークライアントログ 1 と 2 のスキーマ (SERVER_CLIENT_LOG_1 テーブルと SERVER_CLIENT_LOG_2 テーブル)

表 1-67 はサーバークライアントログのデータベーススキーマを説明したものです。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

キーは I_SERVER_CLIENT_LOG_1_LOG_IDX または I_SERVER_CLIENT_LOG_2_LOG_IDX です。LOG_IDX フィールドは重複のないテーブルの識別子として機能しますが、テーブルの主キーとしては形式的に分類されません。このフィールドにインデックスがありますが、主キーインデックスではありません。このテーブルに主キーはありません。

表 1-67 サーバークライアントログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	ログが属するドメインの GUID	char(32), NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL

サーバークライアントログ 1 と 2 のスキーマ (SERVER_CLIENT_LOG_1 テーブルと SERVER_CLIENT_LOG_2 テーブル)

データベースのフィールド名	コメント	データタイプ
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
EVENT_ID	<p>クライアント活動イベントの重複のない ID。</p> <p>有効な値は次の通りです。</p> <p>1 = 登録が正常に完了しました</p> <p>2 = 登録が失敗しました</p> <p>3 = クライアントが再接続しました</p> <p>4 = クライアントが切断されました</p> <p>5 = ポリシーをダウンロードしました</p> <p>6 = 侵入防止ポリシーをダウンロードしました</p> <p>7 = sylink.xml をダウンロードしました</p> <p>8 = 自動アップグレードファイルをダウンロードしました</p> <p>9 = サーバーがログを受信しました</p> <p>10 = ログ処理が失敗しました</p> <p>11 = サーバーが学習済みアプリケーションを受信しました</p> <p>12 = サーバーがクライアント情報を受信しました</p> <p>13 = クライアント情報の処理が失敗しました</p> <p>14 = ハードウェア ID の変更</p> <p>15 = ファイルフィンガープリントリストをダウンロードしました</p> <p>20 = コンテンツパッケージをダウンロードしました</p> <p>22 = コマンドをダウンロードしました</p>	int, NOT NULL
AGENT_ID	エージェントの GUID	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
HOST_NAME	クライアントのコンピュータ名	nvarchar(256), varchar(256), NULL
USER_NAME	クライアントのログオンユーザー名	nvarchar(256), varchar(256), NULL
DOMAIN_NAME	クライアントのドメイン名	nvarchar(256), varchar(256), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL
LOG_IDX*	ログインデックスの重複のない ID	char(32), NULL

サーバーエンフォースログ 1 と 2 のスキーマ (SERVER_ENFORCER_LOG_1 テーブルと SERVER_ENFORCER_LOG_2 テーブル)

表 1-68 はサーバーエンフォースログのデータベーススキーマを説明したものです。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されま

キーは I_SERVER_ENFORCER_LOG_1_LOG_IDX または I_SERVER_ENFORCER_LOG_2_LOG_IDX です。LOG_IDX フィールドは重複のないテーブルの識別子として機能しますが、テーブルの主キーとしては形式的に分類されません。このフィールドにインデックスがありますが、主キーインデックスではありません。このテーブルに主キーはありません。

表 1-68 サーバーエンフォーサログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

サーバーエンフォースログ 1 と 2 のスキーマ (SERVER_ENFORCER_LOG_1 テーブルと SERVER_ENFORCER_LOG_2 テーブル)

データベースのフィールド名	コメント	データタイプ
EVENT_ID		int, NOT NULL

データベースのフィールド名	コメント	データタイプ
	<p>エンフォーサ活動の重複のない ID。</p> <p>有効な値は次の通りです。</p> <p>0x101 = 管理サーバーに接続しました</p> <p>0x102 = 管理サーバーとの接続が消失しました</p> <p>0x103 = 管理サーバーからダウンロードしたポリシーを適用しました</p> <p>0x104 = 管理サーバーからダウンロードしたポリシーを適用できませんでした</p> <p>0x107 = 管理サーバーの設定を適用しました</p> <p>0x108 = 管理サーバーの設定を適用できませんでした</p> <p>0x201 = エンフォーサを開始しました</p> <p>0x202 = エンフォーサを停止しました</p> <p>0x203 = エンフォーサが一時停止しました</p> <p>0x204 = エンフォーサが再開しました</p> <p>0x205 = エンフォーサをサーバーから切断了ました</p> <p>0x301 = エンフォーサフェールオーバーが有効です</p> <p>0x302 = エンフォーサフェールオーバーが無効です</p> <p>0x303 = スタンバイモードエンフォーサ</p> <p>0x304 = 一次モードエンフォーサ</p> <p>0x305 = エンフォーサ不足</p>	

データベースのフィールド名	コメント	データタイプ
	<p>0x306 = エンフォースループ</p> <p>0x401 = 転送エンジンの一時停止</p> <p>0x402 = 転送エンジンの開始</p> <p>0x403 = DNS エンフォースが有効です</p> <p>0x404 = DNS エンフォースが無効です</p> <p>0x405 = DHCP エンフォースが有効です</p> <p>0x406 = DHCP エンフォースが無効です</p> <p>0x407 = すべての有効化を許可する</p> <p>0x408 = すべての無効化を許可する</p> <p>0x501 = ライセンス枠数の変更</p> <p>0x601 = ポリシー解析ルーチンを作成できませんでした</p> <p>0x602 = 管理サーバーからダウンロードしたポリシーをインポートできませんでした</p> <p>0x602 = 管理サーバーからダウンロードしたポリシーをエクスポートできませんでした</p> <p>0x701 = カスタム属性が正しくありません</p>	
ENFORCER_ID	エンフォースの GUID	char(32), NOT NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(520), NULL
RESERVED_BINARY		varbinary(2000), NULL
LOG_IDX*		char(32), NULL

サーバーポリシーログ 1 と 2 のスキーマ (SERVER_POLICY_LOG_1 テーブルと SERVER_POLICY_LOG_2 テーブル)

表 1-69 はサーバーポリシーログのデータベーススキーマを説明したものです。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

このテーブルには主キーは指定されません。

表 1-69 サーバーポリシーログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	管理されたドメインの GUID	char(32), NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

サーバーポリシーログ 1 と 2 のスキーマ (SERVER_POLICY_LOG_1 テーブルと SERVER_POLICY_LOG_2 テーブル)

データベースのフィールド名	コメント	データタイプ
EVENT_ID	ポリシーイベントの重複のない ID。 有効な値は次の通りです。 0 = ポリシーを追加しました 1 = ポリシーを削除しました 2 = ポリシーを編集しました 3 = システムインストール時に共有ポリシーを追加する 4 = システムアップグレード時に共有ポリシーを追加する 5 = ドメイン作成時に共有ポリシーを追加する	int, NOT NULL
OBJECT_ID	エージェントのポリシーの GUID	char(32), NOT NULL
ADMIN_ID	ポリシーを修正した管理者の GUID	char(32), NOT NULL
EVENT_DESC	イベントの説明。通常、説明の 1 行目は「概略」として扱われます。	nvarchar(512), NULL
EVENT_DATA	バイナリ形式の追加データ。このフィールドは省略可能です。	varbinary(2000), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

サーバーシステムログ 1 と 2 のスキーマ (SERVER_SYSTEM_LOG_1 テーブルと SERVER_SYSTEM_LOG_2 テーブル)

表 1-70 はサーバーシステムログのデータベーススキーマを説明したものです。

このスキーマには 2 つのテーブルがあります。ログを格納するとき、Symantec Endpoint Protection Manager は最初のテーブルをいっぱいになるまで使います。その後、管理サーバーは 2 番目のテーブルを使います。最初のテーブル内のデータは、2 番目のテーブルがいっぱいになるまで維持されます。その後、管理サーバーは最初のテーブルへの入力を再び開始します。このサイクルは連続的です。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

このテーブルには主キーは指定されません。

表 1-70 サーバーシステムログ 1 と 2 のスキーマ

データベースのフィールド名	コメント	データタイプ
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DOMAIN_ID	使われない。長さ 0 の文字列としてログに記録	char(32), NULL
SITE_ID	ログが属するサイトの GUID	char(32), NOT NULL
SERVER_ID	ログが属するサーバーの GUID	char(32), NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
SEVERITY	Enum (SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST): >= 400 = より良好以上 >=500 = 良好以上 >=700 = 設定以上 >=800 = 情報以上 >=900 = 警告以上 >=1000 = 不良以上	int, NOT NULL
EVENT_ID	システムイベントの重複のない ID	int, NOT NULL
EVENT_DESC	イベントの説明。通常、説明の 1 行目は「概略」として扱われます。	nvarchar(2000), varchar(2000), NULL
MSG_ID	イベントの説明 ID。この ID を使って各国のメッセージをロードします。このイベントに例外が関係する場合にのみ使われます。	int, NULL
ERROR_CODE	ErrorCode はソースコード内のエラーを重複なく識別できます。このイベントに例外が関係する場合にのみ使われます。	int, NULL
STACK_TRACE	例外のスタックトレース。このイベントに例外が関係する場合にのみ使われます。	nvarchar(2000), varchar(2000), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL

データベースのフィールド名	コメント	データタイプ
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

システムレポートのスキーマ (SYSTEM_REPORT テーブル)

表 1-71 はレポート情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Server と埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_SYSTEMREPORT として機能することを示します。

表 1-71 システムレポートのスキーマ

データベースフィールド	コメント	データタイプ
SYSTEMFILTER_IDX*	主キー。	char(32), NOT NULL
USER_ID	このフィルタを作成した管理者の GUID。管理者ユーザーテーブル内の user_id の列への外部キー。	char(32), NOT NULL
FILTERNAME	管理者がフィルタの保存操作時に提供したフィルタ名	NVARCHAR(255), varchar(255), NOT NULL
STARTDATEFROM	時間フィルタの開始日	datetime, NOT NULL
STARTDATETO	時間フィルタの終了日	datetime, NOT NULL

データベースフィールド	コメント	データタイプ
RELATIVEDATETYPE	有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = エンフォーサ活動	int, NOT NULL
SYSTEM_TYPE	有効な値は次の通りです。 1 = 管理 2 = クライアント/サーバー活動 3 = サーバー活動 4 = クライアント活動 5 = エンフォーサ活動	tinyint, NULL
SEVERITY	管理、クライアント/サーバー活動、サーバー活動の各ログについて有効な値は次の通りです。 1000 = エラー以上 900 = 警告以上 800 = 情報以上 -1 = フィルタなし(すべて) エンフォーサ活動とクライアント活動について、有効な値は次の通りです。 0 = 情報以上 1 = 警告以上 2 = エラー以上 3 = 致命的 -1 = フィルタなし(すべて)	int,null

データベースフィールド	コメント	データタイプ
EVENT_ID		varchar(32), NULL

データベースフィールド	コメント	データタイプ
	<p>このフィールドが空白または % の場合、フィルタ処理は実行されません。</p> <p>管理システムログ用。この種類のログの場合、このフィールドでは = 記号の左側に値が格納されます (例: ADMIN_ADMIN_TYPES)。これはハードコードされた英語の文字列のキーです。= 記号の右側は、ユーザーがグループを選択するときにクエリーされるイベントです。</p> <p>ADMIN_ADMIN_TYPES = 管理者イベント。 有効な値は次の通りです。</p> <ul style="list-style-type: none"> ■ 4097 = ログインが正常に完了 ■ 4098 = ログイン失敗 ■ 4099 = ログアウト ■ 4050 = アカウントがロック ■ 4101 = アカウントがロック解除 ■ 4102 = アカウントが無効です ■ 4103 = アカウントが有効です ■ 4104 = 管理者を作成しました ■ 4105 = 管理者を削除しました ■ 4106 = 管理者名を変更しました ■ 4107 = パスワードを変更しました ■ 4108 = 管理者のプロパティを変更しました <p>ADMIN_DOMAIN_TYPES = ドメインのイベント。 有効な値は次の通りです。</p> <ul style="list-style-type: none"> ■ 4109 = ドメインを作成しました ■ 4110 = ドメインを削除しました ■ 4111 = ドメインのプロパティを変更しました ■ 4128 = ドメインが無効です ■ 4129 = ドメインが有効です ■ 4130 = ドメイン名を変更しました <p>ADMIN_GROUP_TYPES = グループのイベント。 有効な値は次の通りです。</p> <ul style="list-style-type: none"> 8193 = グループを作成しました 8194 = グループを削除しました 	

データベースフィールド	コメント	データタイプ
	<p>8195 = グループ名を変更しました</p> <p>8196 = グループを移動しました</p> <p>8197 = グループのプロパティを変更しました</p> <p>ADMIN_USER_TYPES = ユーザーイベント。 有効な値は次の通りです。</p> <p>8198 = ユーザーを作成しました</p> <p>8199 = ユーザーを削除しました</p> <p>8200 = ユーザーを移動しました</p> <p>8201 = ユーザーをコピーしました</p> <p>8202 = ユーザーポリシーモードを切り替えます</p> <p>8203 = ユーザーのプロパティを変更しました</p> <p>ADMIN_COMPUTER_TYPES = コンピューターイベント。 有効な値は次の通りです。</p> <p>8204 = コンピュータを作成しました</p> <p>8205 = コンピュータを削除しました</p> <p>8206 = コンピュータを移動しました</p> <p>8207 = コンピュータをコピーしました</p> <p>8208 = コンピュータポリシーモードを切り替えました</p> <p>8209 = コンピュータのプロパティを変更しました</p> <p>ADMIN_IMPORT_TYPES = インポートイベント。 有効な値は次の通りです。</p> <p>8210 = 組織単位をインポートしました</p> <p>8211 = ドメインユーザーをインポートしました</p> <p>8212 = LDAP ユーザーをインポートしました</p> <p>ADMIN_PACKAGE_TYPES = パッケージイベント。 有効な値は次の通りです。</p> <p>12289 = パッケージを作成しました</p>	

データベースフィールド	コメント	データタイプ
	12290 = パッケージを削除しました	
	12291 = パッケージをエクスポートしました	
	12292 = パッケージをごみ箱に移動しました	
	12293 = パッケージが最新になりました	
	12294 = パッケージを他のドメインに追加しました	
	12295 = パッケージのプロパティを変更しました	
	12296 = パッケージ配備を作成しました	
	12297 = パッケージ配備を削除しました	
	12298 = パッケージ配備のプロパティを変更しました	
	12299 = パッケージを更新しました	
	ADMIN_REPLICATION_TYPES = 複製イベント。	
	有効な値は次の通りです。	
	16385 = 複製パートナーを登録しました	
	16386 = 複製パートナーを削除しました	
	16400 = 今すぐに複製	
	ADMIN_OTHER_TYPES = その他のイベント。	
	有効な値は次の通りです。	
	16387 = リモートサイトを削除しました	
	16388 = サイトのプロパティを変更しました	
	16389 = サーバーのプロパティを変更しました	
	16390 = データベースのプロパティを変更しました	
	16391 = パートナーのプロパティを変更しました	
	16392 = サイトライセンスを変更しました	
	16393 = エンフォーサライセンスを変更しました	
	16394 = 今すぐに複製	
	16395 = 今すぐにバックアップ	

データベースフィールド	コメント	データタイプ
	16396 = 外部ログ記録のプロパティを変更しました	
	16397 = サイトのバックアップ設定を変更しました	
	16398 = サーバーを削除しました	
	16399 = サーバー証明書を変更しました	
	16401 = 今すぐにバックアップ	
	16402 = 外部ログ記録のプロパティを変更しました	
	16403 = サイトのバックアップ設定を変更しました	
	16404 = サーバーを削除しました	
	16405 = サーバー証明書を変更しました	
	16406 = エンフォーサグループのプロパティを変更しました	
	クライアント/サーバー活動システムログ用。この種類のログの場合、このフィールドにはクエリーするイベント ID が格納されます。	
	1 = 登録が正常に完了しました	
	2 = 登録が失敗しました	
	3 = クライアントが再接続しました	
	4 = クライアントが切断されました	
	5 = ポリシーをダウンロードしました	
	6 = 侵入防止ポリシーをダウンロードしました	
	7 = symlink.xml をダウンロードしました	
	8 = 自動アップグレードファイルをダウンロードしました	
	9 = サーバーがログを受信しました	
	10 = ログ処理が失敗しました	
	11 = サーバーが学習済みアプリケーションを受信しました	
	12 = サーバーがクライアント情報を受信しました	
	13 = クライアント情報の処理が失敗しました	

データベースフィールド	コメント	データタイプ
	<p>14 = ハードウェア ID の変更</p> <p>15 = ファイルフィンガープリントリストをダウンロードしました</p> <p>20 = コンテンツパッケージをダウンロードしました</p> <p>22 = コマンドをダウンロードしました</p> <p>サーバー活動システムログ用。この種類のログの場合、このフィールドでは = 記号の左側にハードコードされた英語の文字列キーが格納されます。右側には、グループによってクエリーされるイベントがリストされます。</p> <p>SERVER_EVENT_TYPES = サーバーイベント。 有効な値は次の通りです。</p> <p>257 = サーバーの起動が正常に完了しました</p> <p>258 = サーバーを起動できませんでした</p> <p>259 = サーバーの段階的なシャットダウン</p> <p>260 = サーバーを作成しました</p> <p>SERVER_AGENT_EVENT_TYPES = データベース保守イベント。 有効な値は次の通りです。</p> <ul style="list-style-type: none"> ■ 267 = クライアントスイープを開始しました ■ 268 = クライアントスイープの概略 ■ 269 = クライアントスイープが正常に完了しました ■ 270 = クライアントスイープが失敗しました ■ 271 = データベースログをスイープしました <p>SERVER_BACKUP_EVENT_TYPES = バックアップイベント。 有効な値は次の通りです。</p> <p>1025 = バックアップ接続が失敗しました</p> <p>1026 = バックアップデータフェッチが失敗しました</p> <p>1027 = バックアップファイル書き込みが失敗しました</p>	

データベースフィールド	コメント	データタイプ
	<p>1028 = バックアップが不明で失敗しました</p> <p>1029 = バックアップが正常に完了</p> <p>1030 = バックアップを開始しました</p> <p>SERVER_RADIUS_EVENT_TYPES = Radius サーバーイベント。</p> <p>有効な値は次の通りです。</p> <p>1283 = RADIUS サーバーを起動できませんでした。RADIUS ポートを別のプロセスが使っている可能性があります</p> <p>1284 = RADIUS サーバーを起動できませんでした。非ブロック型 I/O ソケットの設定が失敗しました。</p> <p>1285 = RADIUS サーバーを起動できませんでした。ソケットの作成エラー。</p> <p>SERVER_REPLICATION_EVENT_TYPES = 複製イベント。</p> <p>有効な値は次の通りです。</p> <p>769 = リモートサイトから複製を開始しました</p> <p>770 = 複製でリモートサイトにログインできませんでした</p> <p>771 = 変更があったデータをリモートサイトからフェッチできませんでした</p> <p>772 = 複製が正常に終了しました</p> <p>773 = 複製が失敗しました</p> <p>774 = 複製マージが失敗しました</p> <p>775 = リモートサイトに接続できません</p> <p>776 = マージの競合を解決するために名前が変更されました</p> <p>777 = グループの絶対パス名が長すぎて複製できません</p> <p>778 = リモートサイトのローカル変更データの取り込みを開始しました</p>	

データベースフィールド	コメント	データタイプ
	<p>779 = リモートサイトのローカル変更データの取り込みが正常に完了しました</p> <p>780 = リモートサイトのローカル変更データの取り込みが失敗しました</p> <p>781 = データベースはデッドロックを回避するために複製の終了を選択しました</p> <p>782 = 複製データを受信しました</p> <p>SERVER_IMPORT_EVENT_TYPES = インポートイベント。</p> <p>有効な値は次の通りです。</p> <p>264 = 組織のインポートを開始しました</p> <p>265 = 組織のインポートが正常に完了しました</p> <p>266 = 組織のインポートが失敗しました</p> <p>SERVER_INTRUSION_PREVENTION_EVENT_TYPES = ポリシーコンテンツ更新。</p> <p>有効な値は次の通りです。</p> <p>1537 = 侵入防止ライブラリを追加しました</p> <p>1538 = 侵入防止ライブラリを削除しました</p> <p>1539 = 侵入防止ライブラリを更新しました</p> <p>1540 = 侵入防止ライブラリは最新です</p> <p>SERVER_LU_EVENT_TYPES = LiveUpdate イベント。</p> <p>有効な値は次の通りです。</p> <p>1793 = LiveUpdate を開始しました</p> <p>1794 = LiveUpdate が正常に完了しました</p> <p>1795 = LiveUpdate が失敗しました</p> <p>1796 = LiveUpdate 手動タスクが正常に完了しました</p> <p>1797 = LiveUpdate 手動タスクが失敗しました</p> <p>1798 = LiveUpdate 再試行を開始しました</p>	

データベースフィールド	コメント	データタイプ
	1799 = LiveUpdate 再試行が正常に完了しました	
	1800 = LiveUpdate 再試行が失敗して再び試します	
	1801 = LiveUpdate 手動タスクを開始しました	
	1802 = LiveUpdate 再試行の最大時間オーバー	
	1803 = LiveUpdate 再試行が失敗して再び試します	
	1804 = LiveUpdate 再試行の予定日時パス	
	1805 = LiveUpdate で起動したすべての処理	
	1806 = LiveUpdate で異常終了したすべての処理	
	1807 = LiveUpdate で次のサーバー	
	1808 = LiveUpdate ですべての処理が終了しました	
	1809 = LiveUpdate ですべての処理を起動できませんでした	
	1810 = LiveUpdate でコンテンツをアップロード中	
	1811 = LiveUpdate ファイルパスが存在しません	
	1812 = LiveUpdate コンテンツカタログファイルを挿入しました	
	1813 = LiveUpdate コンテンツカタログファイルを更新しました	
	1814 = クライアントパッケージをダウンロードしました	
	1815 = クライアントパッケージのパッチが失敗しました	
	1816 = 新しい LiveUpdate コンテンツをダウンロードしました	
	1817 = LiveUpdate URL パラメータの誤り	

データベースフィールド	コメント	データタイプ
	<p>1824 = ウイルス対策とスパイウェア対策の定義 Win64 11.0 MicroDefsB.CurDefs を更新できませんでした</p> <p>1825 = ダウンロードは最新です</p> <p>1826 = LiveUpdate の再実行はコンテンツカタログ更新によってトリガされます</p> <p>1818 = LiveUpdate コンテンツをダウンロードできませんでした</p> <p>1819 = LiveUpdate コンテンツをクリーンアップしました</p> <p>1820 = ホストインテグリティテンプレートを更新しました</p> <p>1821 = LiveUpdate はタイムアウトになりました</p> <p>1822 = LiveUpdate スケジュールを更新しました</p> <p>SERVER_NET_AUDIT_EVENT_TYPES = 管理外コンピュータイベントを検索。 有効な値は次の通りです。</p> <p>2049 = クライアント不在ホストの検索を開始しました</p> <p>2050 = クライアント不在ホストの検索の正常終了</p> <p>2051 = クライアント不在ホストの検索の異常終了</p> <p>2052 = クライアントリモートを開始しました</p> <p>2053 = クライアントリモートの正常終了</p> <p>2054 = クライアントリモートの異常終了</p> <p>SERVER_OTHER_EVENT_TYPES = その他のイベント。</p>	

データベースフィールド	コメント	データタイプ
	<p>有効な値は次の通りです。</p> <ul style="list-style-type: none"> ■ 261 = サイトを作成しました ■ 262 = パッケージを発行しました ■ 263 = サイトライセンスを超過しました ■ 272 = サーバーアップグレードが正常に完了しました ■ 1282 = 接続メールサーバーが失敗しました ■ 1286 = サーバーエラー <p>クライアント活動システムログ用。このログの場合、このフィールドでは = 記号の左側にハードコードされた英語の文字列キーが格納されます。右側には、グループによってクエリーされるイベントがリストされます。イベント ID は 16 進数。</p> <p>AGENT_SYSTEM_INSTALL_EVENT_TYPES = インストールイベント。</p> <p>有効な値は次の通りです。</p> <p>0x12070001 = 内部エラー</p> <p>0x12070101 = インストールが完了しました</p> <p>0x12070102 = 再起動を推奨</p> <p>0x12070103 = 再起動が必要</p> <p>0x12070104 = インストールが失敗しました</p> <p>0x12070105 = アンインストールが完了しました</p> <p>0x12070106 = アンインストールが失敗しました</p> <p>0x12071037 = Symantec AntiVirus がインストール済みです</p> <p>0x12071038 = シマンテック製ファイアウォールがインストール済みです</p> <p>0x12071039 = アンインストール</p> <p>0x1207103A = アンインストールをロールバックしました</p> <p>AGENT_SYSTEM_SERVICE_EVENT_TYPES = サービスイベント。</p> <p>有効な値は次の通りです。</p>	

データベースフィールド	コメント	データタイプ
	<p>0x12070201 = サービスを開始しています</p> <p>0x12070202 = サービスを開始しました</p> <p>0x12070203 = サービス開始エラー</p> <p>0x12070204 = サービスを停止しました</p> <p>0x12070205 = サービス停止エラー</p> <p>0x1207021A = サービスを停止しようとする試み</p> <p>AGENT_SYSTEM_CONFIG_EVENT_TYPES = 設定イベント。</p> <p>有効な値は次の通りです。</p> <p>0x12070206 = インポートの設定完了</p> <p>0x12070207 = エクスポートの設定エラー</p> <p>0x12070208 = エクスポートの設定完了</p> <p>0x12070209 = エクスポートの設定エラー</p> <p>AGENT_SYSTEM_HI_EVENT_TYPES = ホストインテグリティイベント。</p> <p>有効な値は次の通りです。</p> <p>0x12070210 = ホストインテグリティが無効です</p> <p>0x12070211 = ホストインテグリティが有効です</p> <p>AGENT_SYSTEM_IMPORT_EVENT_TYPES = インポートイベント。</p> <p>有効な値は次の通りです。</p> <p>0x12070214 = 拡張ルールのインポートが正常に完了しました</p> <p>0x12070215 = 拡張ルールをインポートできませんでした</p> <p>0x12070216 = 拡張ルールのエクスポートが正常に完了しました</p> <p>0x12070217 = 拡張ルールをエクスポートできませんでした</p> <p>AGENT_SYSTEM_CLIENT_EVENT_TYPES = クライアントイベント。</p>	

データベースフィールド	コメント	データタイプ
	<p>有効な値は次の通りです。</p> <p>0x12070218 = クライアントエンジンが有効です</p> <p>0x12070219 = クライアントエンジンが無効です</p> <p>0x12071046 = プロアクティブ脅威スキャンはこのプラットフォーム上でサポート外です</p> <p>0x12071047 = プロアクティブ脅威スキャンロードエラー</p> <p>AGENT_SYSTEM_SERVER_EVENT_TYPES = サーバーイベント。</p> <p>有効な値は次の通りです。</p> <p>0x12070301 = サーバーに接続しました</p> <p>0x12070302 = サーバーレスポンスがありません</p> <p>0x12070303 = サーバー接続が失敗しました</p> <p>0x12070304 = サーバーを切断しました</p> <p>0x120B0001 = サーバーに到達できません</p> <p>0x120B0002 = 再接続したサーバー</p> <p>AGENT_SYSTEM_PROFILE_EVENT_TYPES = ポリシーイベント。</p> <p>有効な値は次の通りです。</p> <p>0x12070306 = 新しいポリシーを受信しました</p> <p>0x12070307 = 新しいポリシーを適用しました</p> <p>0x12070308 = 新しいポリシーが失敗しました</p> <p>0x12070309 = ポリシーをダウンロードできません</p> <p>0x120B0005 = ポリシーをダウンロードできません</p> <p>0x1207030A = 最新のポリシーがあります</p> <p>0x120B0004 = 最新のポリシーがあります</p> <p>AGENT_SYSTEM_AV_EVENT_TYPES = ウィルス対策エンジンイベント。</p> <p>有効な値は次の通りです。</p> <p>0x12071006 = スキャン省略</p>	

データベースフィールド	コメント	データタイプ
	0x1207100B = ウイルス活動を検出しました 0x1207100C = 設定が変更されました 0x12071010 = ウイルス定義ファイルダウンロード 0x12071012 = 検疫サーバーに送信 0x12071013 = シマンテック社に配信しました 0x12071014 = セキュリティレスポンスバックアップ 0x12071015 = スキャンを中止しました 0x12071016 = Symantec AntiVirus Auto-Protect ロードエラー 0x12071017 = Symantec AntiVirus Auto-Protect が有効です 0x12071018 = Symantec AntiVirus Auto-Protect が無効です 0x1207101A = スキャンを見送りました 0x1207101B = 一時停止したスキャンの再開 0x12071027 = Symantec AntiVirus が古いウイルス定義を使っています 0x12071041 = スキャンを中断しました 0x12071042 = スキャンを再開しました 0x12071043 = スキャン期間が短すぎます 0x12071045 = 拡張スキャンが失敗しました AGENT_SYSTEM_LICENSE_EVENT_TYPES = ライセンスイベント。 有効な値は次の通りです。 0x1207101E = ライセンス警告 0x1207101F = ライセンスエラー 0x12071020 = ライセンスが猶予期間です 0x12071023 = ライセンスをインストールしました 0x12071025 = ライセンスが最新です	

データベースフィールド	コメント	データタイプ
	<p>AGENT_SYSTEM_SECURITY_EVENT_TYPES = セキュリティイベント。</p> <p>有効な値は次の通りです。</p> <p>0x1207102B = セキュリティポリシーを順守しない コンピュータ</p> <p>0x1207102C = セキュリティポリシーを順守するコ ンピュータ</p> <p>0x1207102D = 変更の試み</p> <p>AGENT_SYSTEM_OTHER_EVENT_TYPES = その他のイベント。</p> <p>有効な値は次の通りです。</p> <p>0x1207020A = 電子メール送信 OK</p> <p>0x1207020B = 電子メール送信エラー</p> <p>0x1207020C = 更新完了</p> <p>0x1207020D = 更新エラー</p> <p>0x1207020E = 場所の手動変更</p> <p>0x1207020F = 場所を変更しました</p> <p>0x12070212 = 古い Rasdll を検出しました</p> <p>0x12070213 = 自動更新を延期しました</p> <p>0x12070305 = モードを変更しました</p> <p>0x1207030B = HI スクリプトを適用できません</p> <p>0x12070500 = デバイス制御からのシステムメッ セージ</p> <p>0x12070600 = バッファオーバーフロードライバか らのシステムメッセージ</p> <p>0x12071021 = アクセス拒否の警告</p> <p>0x12071022 = ログ転送エラー</p> <p>0x12071044 = クライアントを移動しました</p>	

データベースフィールド	コメント	データタイプ
	<p>エンフォース活動システムログ用。このログの場合、このフィールドでは=記号の左側にハードコードされた英語の文字列キーが格納されます。右側には、グループによってクエリーされるイベントがリストされます。イベント ID は 16 進数。</p> <p>ENFORCER_POLICY_MANAGER_EVENT_TY = 管理イベント。</p> <p>有効な値は次の通りです。</p> <p>0x101 = 接続先 > 0x102 = Symantec Endpoint Protection Manager の接続が消失しました</p> <p>0x103 = 管理サーバーからダウンロードしたポリシーを適用しました</p> <p>0x104 = 管理サーバーからダウンロードしたポリシーを適用できませんでした</p> <p>0x107 = 管理サーバーの設定を適用しました</p> <p>0x108 = 管理サーバーの設定を適用できませんでした</p> <p>ENFORCER_ENFORCER_EVENT_TYPES = エンフォースイベント。</p> <p>有効な値は次の通りです。</p> <p>0x201 = エンフォースを開始しました</p> <p>0x202 = エンフォースを停止しました</p> <p>0x203 = エンフォースが一時停止しました</p> <p>0x204 = エンフォースが再開しました</p> <p>0x205 = エンフォースをサーバーから切断しました</p> <p>0x301 = エンフォースフェールオーバーが有効です</p> <p>0x302 = エンフォースフェールオーバーが無効です</p> <p>0x303 = スタンバイモードエンフォース</p> <p>0x304 = 一次モードエンフォース</p> <p>0x305 = エンフォース不足</p>	

データベースフィールド	コメント	データタイプ
	<p>0x306 = エンフォーサループ ENFORCER_ENABLE_EVENT_TYPES = 有効イベント。 有効な値は次の通りです。</p> <p>0x401 = 転送エンジンの一時停止 0x402 = 転送エンジンの開始 0x403 = DNS エンフォーサが有効です 0x404 = DNS エンフォーサが無効です 0x405 = DHCP エンフォーサが有効です 0x406 = DHCP エンフォーサが無効です 0x407 = すべての有効化を許可する 0x408 = すべての無効化を許可する ENFORCER_PROFILE_EVENT_TYPES = ポリシーイベント。 有効な値は次の通りです。</p> <p>0x501 = ライセンス枠数の変更 0x601 = ポリシー解析ルーチンを作成できませんでした 0x602 = Symantec Endpoint Protection Manager からダウンロードしたポリシーをインポートできませんでした 0x603 = ダウンロードしたポリシーをエクスポートできませんでした 0x701 = カスタム属性が正しくありません</p>	
EVENT_DESC		NVARCHAR(255), varchar(255), NOT NULL

データベースフィールド	コメント	データタイプ
MSG_ID		varchar(255), NULL

データベースフィールド	コメント	データタイプ
	<p>このフィールドでは、=記号の左側にハードコードされた英語の文字列のキーが格納されます。右側には、クエリーされるエラーメッセージの種類の説明が表示されます。このフィールドが % または空白の場合、フィルタ処理は実行されません(すべてのレコードを表示)。</p> <p>管理システムログ用。</p> <p>有効な値は次の通りです。</p> <p>ERR_SERVER = サーバーエラーメッセージ</p> <p>ERR_INVALID_PARAMETER = 無効なパラメータエラーメッセージ</p> <p>ERR_GENERAL = 一般エラーメッセージ</p> <p>ERR_ROOT = ルートエラーメッセージ</p> <p>ERR_AUTHENTICATION = ログイン関係のエラーメッセージ</p> <p>ERR_METADATA = メタデータエラーメッセージ</p> <p>ERR_TRANSACTION = トランザクションエラーメッセージ</p> <p>ERR_DATASTORE = データストアエラーメッセージ</p> <p>ERR_LICENSE = ライセンスエラーメッセージ</p> <p>ERR_CERTIFICATE = 証明書エラーメッセージ</p> <p>ERR_GROUP = グループのエラーメッセージ</p> <p>ERR_FILE = ファイル関係のエラーメッセージ</p> <p>ERR_LIVEUPDATE = LiveUpdate エラーメッセージ</p> <p>ERR_OTHER = その他のエラーメッセージ</p> <p>ERR_NONE = なし</p> <p>サーバー活動システムログ用。</p> <p>ERR_SERVER = サーバーエラーメッセージ</p> <p>ERR_INVALID_PARAMETER = 無効なパラメータエラーメッセージ</p>	

データベースフィールド	コメント	データタイプ
	ERR_GENERAL = 一般エラーメッセージ ERR_ROOT = ルートエラーメッセージ ERR_AUTHENTICATION = ログイン関係のエラーメッセージ ERR_METADATA = メタデータエラーメッセージ ERR_TRANSACTION = トランザクションエラーメッセージ ERR_DATASTORE = データストアエラーメッセージ ERR_LICENSE = ライセンスエラーメッセージ ERR_CERTIFICATE = 証明書エラーメッセージ ERR_GROUP = グループのエラーメッセージ ERR_FILE = ファイル関係のエラーメッセージ ERR_LIVEUPDATE = LiveUpdate エラーメッセージ ERR_OTHER = その他のエラーメッセージ ERR_NONE = なし	
ENFORCERLIST	フィルタ処理するエンフォーサ名 (カンマ区切り)	NVARCHAR(255), varchar(255), NOT NULL
ENFORCER_TYPE	有効な値は次の通りです。 0 = ゲートウェイエンフォーサ 1 = LAN エンフォーサ 2 = DHCP エンフォーサ 3 = 統合エンフォーサ 4 = NAP エンフォーサ 5 = ピアツーピアエンフォーサ	int, NULL
SERVERGROUPLIST	フィルタ処理するドメイン名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL

データベースフィールド	コメント	データタイプ
CLIENTGROUPLIST	フィルタ処理するグループ名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
SITELIST	フィルタ処理するサイト名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
PARENTSERVERLIST	フィルタ処理するサーバー名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
COMPUTERLIST	フィルタ処理するコンピュータ名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(512), varchar(512), NOT NULL
IPADDRESSLIST	フィルタ処理するIPアドレス (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(512), varchar(512), NOT NULL
USERLIST	フィルタ処理するユーザー名 (カンマ区切り)。	NVARCHAR(512), varchar(512), NOT NULL
POLICYNAMELIST	フィルタ処理するポリシー名 (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
EVENTSOURCELIST	フィルタ処理するイベント名 (カンマ区切り)	NVARCHAR(255), varchar(255), NOT NULL
SORTORDER	ログ表示用にソートする列	varchar(32), NULL
SORTDIR	ソート方向。 有効な値は次の通りです。 Desc = 降順 Asc = 昇順	varchar(5), NULL
LIMITROWS	ページ付けに使う行数	int, NOT NULL
USERRELATIVE	相対日付 (「オン」) または絶対日付の使用	char(2), NOT NULL

データベースフィールド	コメント	データタイプ
REPORT_IDX	使われない。	int, NOT NULL
REPORTINPUTS	特殊なパラメータ(レポートに必要な場合)	NVARCHAR(64), varchar(64), NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
DELETED	スキーマオブジェクトの削除されたフラグ。 有効な値は次の通りです。 0 = 削除しました 1 = 削除されていない	tinyint, NOT NULL

システム状態のスキーマ (SYSTEM_STATE テーブル)

表 1-72 はシステム状態情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されます。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_SYSTEM_STATE として機能することを示します。

表 1-72 システム状態のスキーマ

データベースのフィールド名	コメント	データタイプ
CHECKSUM	XML コンテンツのチェックサム	char(32), NOT NULL
CONTENT	スキーマオブジェクトの XML コンテンツ	image, NOT NULL
DELETED		tinyint, NOT NULL
ID*	スキーマオブジェクトの GUID	char(32), NOT NULL
OWNER	対応するスキーマオブジェクトの GUID	char(32), NULL

データベースのフィールド名	コメント	データタイプ
TIME_STAMP	データベースレコードが修正された日時(マージの競合の解決に使用)	bigint, NOT NULL
TYPE	スキーマオブジェクトの種類名	varchar(256), NOT NULL
USN	更新シリアル番号(複製で使用)	bigint, NOT NULL
DOMAIN_ID	状態オブジェクトを含むドメインのGUID	char(32), NULL
RESERVED_INT1		int, NULL
RESERVED_INT2		int, NULL
RESERVED_BIGINT1		bigint, NULL
RESERVED_BIGINT2		bigint, NULL
RESERVED_CHAR1		char(32), NULL
RESERVED_CHAR2		char(32), NULL
RESERVED_varchar1		nvarchar(260), varchar(260), NULL
RESERVED_BINARY		varbinary(2000), NULL

脅威レポートのスキーマ (THREATREPORT テーブル)

表 1-73 は脅威レポート情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_THREATREPORTとして機能することを示します。

表 1-73 脅威レポートのスキーマ

データベースのフィールド名	コメント	データタイプ
THREATFILTER_IDX*	主キー。	char(32), NOT NULL

データベースのフィールド名	コメント	データタイプ
USER_ID	管理者 GUID	char(32), NOT NULL
FILTERNAME	この保存されたレポートのユーザー指定の名前	NVARCHAR(255), varchar(255), NOT NULL
STARTDATEFROM	開始日	datetime, NOT NULL
STARTDATETO	終了日	datetime, NOT NULL
RELATIVEDATETYPE	有効な値は次の通りです。 0 = 過去 1 週間 1 = 過去 1 カ月 2 = 過去 3 カ月 3 = 過去 1 年 4 = 過去 24 時間 5 = 今月	int, NOT NULL
FILTER_TYPE	有効な値は次の通りです。 1 = リスク 2 = プロアクティブ脅威防止	tinyint, NULL
PRODUCT	使われない。	varchar(32), NULL
EVENTTYPE	ここで有効な値は ALERTMSG テーブル内にあります。	varchar(32), NULL
ACTUALACTION	ここで有効な値は ACTUALACTION テーブル内にあります。	varchar(32), NULL

データベースのフィールド名	コメント	データタイプ
SOURCE	<p>ハードコードされた英語ルックアップキー。</p> <p>有効な値は次の通りです。</p> <p>定時スキャン</p> <p>Manual Scan</p> <p>Real Time Scan</p> <p>Heuristic Scan</p> <p>コンソール</p> <p>Definition downloader</p> <p>システム</p> <p>起動時スキャン</p> <p>Idle Scan</p> <p>Manual Quarantine</p>	varchar(255), NULL
SORTORDER	ログ表示のソートに使用する列	varchar(32), NULL
SORTDIR	「昇順」または「降順」	varchar(5), NULL
TIMEBASE	非推奨	varchar(32), NULL
TREATCOMPRESSED	非推奨	varchar(32), NULL
SERVERGROUPLIST	フィルタ処理するドメインのリスト (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
SERVERGROUPINCLUDE	リスト内のドメインを含めるか(1)、除外するか(0)。常に1に設定。	int, NOT NULL
CLIENTGROUPLIST	フィルタ処理するクライアントグループのリスト (カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
CLIENTGROUPINCLUDE	リスト内のクライアントグループを含めるか(1)、除外するか(0)。常に1に設定。	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
PARENTSERVERLIST	フィルタ処理する管理サーバーのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
PARENTSERVERINCLUDE	リスト内のサーバーを含めるか(1)、除外するか(0)。(常に 1 に設定)	int, NOT NULL
COMPUTERLIST	フィルタ処理するコンピュータのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(512), varchar(512), NOT NULL
COMPUTERINCLUDE	リスト内のコンピュータを含めるか(1)、除外するか(0)。(常に 1 に設定)	int, NOT NULL
IPADDRESSLIST	フィルタ処理する IP アドレスのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
IPADDRESSINCLUDE	リスト内の IP アドレスを含めるか(1)、除外するか(0)。(常に 1 に設定)	int, NOT NULL
CLIENTUSERLIST	フィルタ処理するユーザーのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
CLIENTUSERINCLUDE	リスト内のユーザーを含めるか(1)、除外するか(0)。(常に 1 に設定)	int, NOT NULL
HPP_APP_LIST	フィルタ処理するヒューリスティックリスクのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL
THREATLIST	フィルタ処理するリスクのリスト(カンマ区切り)。これらの名前にはワイルドカードを使うことができます。	NVARCHAR(255), varchar(255), NOT NULL

データベースのフィールド名	コメント	データタイプ
THREATINCLUDE	リスト内のリスクを含めるか(1)、除外するか(0)。(常に1に設定)	int, NOT NULL
THREATTYPELIST	ここで有効な値は VIRUSCATEGORY テーブル内にあります。現在はリストではなく単一の項目です。	varchar(255), NULL
THREATTYPEINCLUDE	リスト内のリスクの種類を含めるか(1)、除外するか(0)(常に1に設定)。	int, NOT NULL
THREATCATEGORY	有効な値は次の通りです。 = -1 = 不明 >= 1 = 非常に危険度が低いリスク >= 2 = 危険度が低いリスク >= 3 = 中程度のリスク >= 4 = 重大なリスク >= 5 = 非常に重大なリスク	varchar(255), NULL
LIMITROWS	ページ付けに使う行数	int, NOT NULL
USERRELATIVE	相対日付(「オン」)または絶対日付の使用	char(2), NOT NULL
REPORT_IDX	使われない。	int, NOT NULL
REPORTINPUTS	特殊なパラメータ(レポートに必要な場合)	NVARCHAR(255), varchar(255), NOT NULL
FROMUSERLIST	非推奨	NVARCHAR(255), varchar(255), NOT NULL
FROMUSERINCLUDE	非推奨	int, NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL

データベースのフィールド名	コメント	データタイプ
DELETED	削除された行: 0 = 削除されていない 1 = 削除しました	tinyint, NOT NULL
FULL_CHARTS	総合リスクレポートに含める、管理者が指定したグラフのリスト	varchar(255), NULL
R_OS_TYPE	有効な値は次の通りです。 0000 = すべて Windows 以外 0001 = All Windows 0002 = All Mac 0004 = Mac OS X 10.4 0005 = Mac OS X 10.5 0006 = Mac OS X 10.6 0601 = Windows 7 0600 = Windows Vista 0502 = Windows 2003 and Windows XP 64-bit 0501 = Windows XP 0500 = Windows 2000 0400 = Windows NT 9999 = Windows Server 2008 -1 = フィルタなし (すべて)	int, NULL

バージョンのスキーマ (VERSION テーブル)

表 1-74 はバージョン情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キーPK_VERSIONとして機能することを示します。

表 1-74 バージョンのスキーマ

データベースのフィールド名	コメント	データタイプ
PRODUCT*	主キー。	char(20), NOT NULL
VERSION	レポートのバージョン	char(10), NOT NULL
DBSCHEMA	スキーマのバージョン	int, NOT NULL
SR_NONCE	内部使用のみ	char(64), NULL

ウイルスのスキーマ (VIRUS テーブル)

表 1-75 はウイルス情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を1つだけ含んでいる場合、値はMS SQL Serverと埋め込みデータベースの両方に適用されます。2つのデータタイプ値がある場合、最初の値はMS SQL Serverに適用され、第2の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク(*)は、フィールドが主キー PK_VIRUSとして機能することを示します。

表 1-75 ウイルスのスキーマ

データベースのフィールド名	コメント	データタイプ
VIRUSNAME_IDX*	主キー、ウイルス/脅威のインデックス	char(32), NOT NULL
VIRUSNAME	ウイルス/脅威の名前	NVARCHAR(255), varchar(255), NOT NULL
CATEGORY	現在のカテゴリ(シマンテック社のWeb サイトからダウンロードされる)。値は1から5まで(値1は危険度が非常に低く、値5は重大)。値-1は不明または適用不可を意味します。この評価はウイルス性の脅威にのみ適用されます。	int, NOT NULL
MAXCATEGORY	ウイルスが達した最大のカテゴリ。値は1から5。値-1は不明または適用不可を意味します。この評価はウイルス性の脅威にのみ適用されます。	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
TYPE	脅威の種類。 有効な値は次の通りです。 0 = Viral 1 = Non-Viral malicious 2 = Malicious 3 = ウイルス対策 - ヒューリスティック 4 = セキュリティリスク 5 = Hack tool 6 = Spyware 7 = Trackware 8 = Dialer 9 = Remote access 10 = Adware 11 = Jokeware 12 = Client compliancy 13 = Generic load point 14 = プロアクティブ脅威スキャン - ヒューリスティック 15 = Cookie	int, NULL

データベースのフィールド名	コメント	データタイプ
TYPE2	<p>脅威の場所。 有効な値は次の通りです。</p> <p>0 = ブートウイルス 1 = ファイルウイルス 2 = 多形態ウイルス 3 = マクロウイルス 4 = ファイルウイルス 5 = ファイルウイルス 6 = メモリウイルス 7 = メモリ OS ウイルス 8 = メモリ MCB ウイルス 9 = メモリ上位ウイルス 11 = ウイルス動作 12 = ウイルス動作 13 = 圧縮ファイル 14 = Heuristic</p>	int, NULL
DISCOVERED	シマンテック社が最初に脅威を発見した日時(シマンテック社の Web サイトからダウンロードされたとき)	datetime, NOT NULL
VID	セキュリティレスポンスが設定する、ウイルスの重複のない識別子	bigint, NOT NULL
USN	USN ベースのシリアル番号。この ID は一意ではありません。	bigint, NOT NULL
TIME_STAMP	このデータベースレコードがデータベースで入力または修正された日時。1970 年以降のミリ秒	bigint, NOT NULL
DELETED	<p>削除された行:</p> <p>0 = 削除されていない 1 = 削除された</p>	tinyint, NOT NULL

データベースのフィールド名	コメント	データタイプ
PATTERN_IDX	この脅威から保護する pattern テーブルを指すポインタ	char(32), NOT NULL
TOP_THREAT	有効な値は次の通りです。 0 = 上位を占める脅威でない 1 = 上位を占める脅威	tinyint, NOT NULL
LATEST_THREAT	0 = 最近の脅威でない 1 = 最近の脅威	tinyint, NOT NULL
STEALTH	セキュリティリスクがコンピュータに存在するかどうかの判定がどの程度容易かの評価。 有効な値は次の通りです。 0 = 評価なし 1,2 = 低 3 = 中 4 > = 高 -1 は適用不可を意味します。この評価は非ウイルス性の脅威にのみ適用されます。	int, NOT NULL
REMOVAL	指定したコンピュータから脅威を取り除くために必要な技術水準。 有効な値は次の通りです。 0 = 評価なし 1, 2 = 低 3 = 中 4 > = 高 -1 は適用不可を意味します。この評価は非ウイルス性の脅威にのみ適用されます。	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
PERFORMANCE	<p>セキュリティリスクの存在がコンピュータのパフォーマンスに及ぼす悪影響の測定。</p> <p>有効な値は次の通りです。</p> <p>0 = 評価なし</p> <p>1, 2 = 低</p> <p>3 = 中</p> <p>4 > = 高</p> <p>-1は適用不可を意味します。この評価は非ウイルス性の脅威にのみ適用されます。</p>	int, NOT NULL
PRIVACY	<p>コンピュータに存在するセキュリティリスクのために失われたプライバシーのレベル。</p> <p>有効な値は次の通りです。</p> <p>0 = 評価なし</p> <p>1, 2 = 低</p> <p>3 = 中</p> <p>4 > = 高</p> <p>-1は適用不可を意味します。この評価は非ウイルス性の脅威にのみ適用されます。</p>	int, NOT NULL
DEPENDENCY	<p>リスクがインストールする依存コンポーネントの数。</p> <p>有効な値は次の通りです。</p> <p>0 = 評価なし</p> <p>1, 2 = 低</p> <p>3 = 中</p> <p>4 > = 高</p> <p>-1は適用不可を意味します。この評価は非ウイルス性の脅威にのみ適用されます。</p>	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
OVERALL	すべてのセキュリティリスク評価の平均。この評価は非ウイルス性の脅威にのみ適用されます。	int, NOT NULL

ウイルスカテゴリのスキーマ (VIRUSCATEGORY テーブル)

表 1-76 はウイルスカテゴリ情報のデータベーススキーマを説明したものです。

データタイプ列のセルがデータタイプ値を 1 つだけ含んでいる場合、値は MS SQL Server と埋め込みデータベースの両方に適用されます。2 つのデータタイプ値がある場合、最初の値は MS SQL Server に適用され、第 2 の値は埋め込みデータベースに適用されません。

データベースのフィールド名に付いたアスタリスク (*) は、フィールドが主キー PK_VIRUSCATEGORY として機能することを示します。

表 1-76 ウイルスカテゴリのスキーマ

データベースのフィールド名	コメント	データタイプ
CATEGORY*	主キー	int, NOT NULL

データベースのフィールド名	コメント	データタイプ
CATEGORY_DESC	カテゴリ、Category_Desc。ルックアップのために使われる英語文字列キー 有効な値は次の通りです。 0 = Viral 1 = Non-Viral malicious 2 = Malicious 3 = Heuristic 4 は現在使われません 5 = Hack tool 6 = Spyware 7 = Trackware 8 = Dialer 9 = Remote access 10 = Adware 11 = Jokeware 12 = Client compliancy 13 = Generic load point 14 = アプリケーションヒューリスティック 15 = Cookie	varchar(255), NOT NULL