

Enterprise Vault™

監査

12.3

Enterprise Vault™: 監査

最終更新日: 2018-03-09。

法的通知と登録商標

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

Veritas、Veritas ロゴ、Enterprise Vault、Compliance Accelerator、Discovery Accelerator は、Veritas Technologies LLC 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。

この製品には、Veritas 社がサードパーティへの帰属を示す必要があるサードパーティソフトウェア (「サードパーティプログラム」) が含まれる場合があります。一部のサードパーティプログラムはオープンソースまたは無償ソフトウェアライセンスの下で利用できます。ソフトウェアに付属している使用許諾契約は、それらのオープンソースまたは無償ソフトウェアライセンスで規定されている権利または義務を変更するものではありません。この Veritas 製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

<https://www.veritas.com/about/legal/license-agreements>

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。Veritas Technologies LLC 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。

文書は「現状有姿のまま」提供され、市販性、特定目的との適合性または権利を侵害していないことを含むすべての明示または黙示の条件、表明および保証は、そのような免責が法的に無効であるとされた場合を除き、免責されます。VERITAS TECHNOLOGIES LLC は本書の供給、実行、または使用に関連した付随的、間接的な損害に対する責任を負わないものとします。本書に含まれる情報は、事前の通知なく変更される場合があります。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商用コンピュータソフトウェアとみなされ、場合に応じて、FAR セクション 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202「Commercial Computer Software and Commercial Computer Software Documentation」、その後継規制の規定により、Veritas がオンプレミスとして提供したか、ホストサービスとして提供したかにかかわらず、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。

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

<https://www.veritas.com>

テクニカルサポート

テクニカルサポートは、世界中にサポートセンターを設けています。すべてのサポートサービスは、サポート契約と、その時点でのエンタープライズテクニカルサポートポリシーに従って提供されます。サポートサービスとテクニカルサポートに連絡する方法について詳しくは、次の当社の Web サイトを参照してください。

https://www.veritas.com/support/ja_JP.html

次の URL で Veritas Account の情報を管理できます。

<https://my.veritas.com>

既存のサポート契約に関して当社に問い合わせる場合は、次に示すご利用の地域のサポート契約管理チームに電子メールでお問い合わせください。

全世界 (日本以外)

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

テクニカルサポートに連絡する前に、Veritas Quick Assist (VQA) ツールを実行して製品のマニュアルに記載されているシステムの必要条件を満たしていることを確認してください。VQA は Veritas サポート Web サイトの次の記事からダウンロードできます。

https://www.veritas.com/support/en_US/vqa

マニュアル

最新版のマニュアルを確認してください。各マニュアルの 2 ページ目に最終更新日が表示されています。最新のマニュアルは Veritas の Web サイトで入手できます。

https://www.veritas.com/support/ja_JP/article.100040095

マニュアルのフィードバック

お客様のフィードバックは当社の財産です。改善点のご指摘やマニュアルの間違い、脱字などのご報告をお願いします。その際、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。フィードバックは次のアドレスに送信してください。

evdocs@veritas.com

次の Veritas コミュニティサイトでマニュアルの情報を参照したり、質問することもできます。

<https://www.veritas.com/community>

目次

第 1 章	本書について	6
	本書について	6
	Enterprise Vault についての詳しい情報の入手先	6
	Enterprise Vault トレーニングモジュール	9
第 2 章	Enterprise Vault の監査の概要	10
	Enterprise Vault の監査について	10
第 3 章	監査の設定	12
	監査の設定	12
	監査データベースの作成	13
	監査カテゴリの設定	14
	監査の開始または停止	17
	監査の調整	18
	監査データベースの移動	18
第 4 章	監査データベースエントリの表示	19
	監査データベースエントリの表示について	19
	Audit Viewer を使用した監査データベースエントリの表示	19
	Audit Viewer による監査データのレポートの実行	19
	Audit Viewer の検索結果のコピー	21
	Audit Viewer の設定の変更	21
	SQL クエリーを使用した監査データベースエントリの表示	21
	ユーザフレンドリな形式でのアーカイブ権限への監査済み変更の 取得	23
第 5 章	データ保護コンプライアンスの監査	24
	一般的な削除操作の監査	24
	一般的なアイテム削除の監査エントリ用のクエリー検索例	26
	権限がある削除操作の監査	28
	権限がある削除の監査エントリ用のクエリー検索例	28

付録 A 監査データベースエントリの形式 30

 監査データベースエントリの形式 30

本書について

この章では以下の項目について説明しています。

- [本書について](#)
- [Enterprise Vault についての詳しい情報の入手先](#)

本書について

このマニュアルでは、Enterprise Vault 監査の設定方法について説明します。

Enterprise Vault の監査は、多くのさまざまなカテゴリのアクティビティを記録します。アクティビティの記録先とするカテゴリを選択し、Enterprise Vault が記録された情報を Enterprise Vault 監査データベースに格納します。監査データベースエントリは、SQL クエリーを使用するか、Audit Viewer ユーティリティを使用して表示できます。

監査は、データ保護規則に準拠していることの証拠を提供する重要なツールです。たとえば、Enterprise Vault 分類を使用して個人識別情報 (PII) をマーク付けし、PII が削除されたときに監査を記録できるように設定できます。

Enterprise Vault についての詳しい情報の入手先

[表 1-1](#) に、Enterprise Vault に付属のマニュアルの一覧を示します。このマニュアルは、Veritas [ドキュメントライブラリ](#)から PDF および HTML 形式でも入手可能です。

表 1-1 Enterprise Vault マニュアルセット

マニュアル	コメント
Veritas Enterprise Vault ドキュメントライブラリ	<p>横断検索の可能な Windows のヘルプ (.chm) 形式の次のドキュメントがすべて含まれています。Acrobat (.pdf) 形式のマニュアルへのリンクも含まれています。</p> <p>このライブラリには、次を含む複数の操作でアクセスできます。</p> <ul style="list-style-type: none"> ■ Windows エクスプローラで Enterprise Vault インストール先フォルダのサブフォルダ Documentation¥language¥Administration Guides を参照し、EV_Help.chm ファイルを開きます。 ■ 管理コンソールの[ヘルプ]メニューで[Enterprise Vault のヘルプ]をクリックします。
導入および計画	Enterprise Vault の機能の概要を説明します。
Deployment Scanner	Enterprise Vault をインストールする前に必要なソフトウェアと設定を確認する方法を説明します。
インストールおよび設定	Enterprise Vault の設定に関する詳細な情報を提供します。
アップグレードの手順	既存の Enterprise Vault インストールを最新バージョンにアップグレードする方法を説明します。
Domino サーバーアーカイブの設定	Domino メールファイルとジャーナルデータベースからアイテムをアーカイブする方法を説明します。
Exchange Server アーカイブの設定	Microsoft Exchange ユーザーメールボックス、ジャーナルメールボックス、パブリックフォルダからアイテムをアーカイブする方法を説明します。
ファイルシステムアーカイブ (FSA) の設定	ネットワークファイルサーバーに保存されているファイルをアーカイブする方法を説明します。
IMAP の設定	Exchange アーカイブとインターネットメールアーカイブへの IMAP クライアントアクセスを設定する方法を説明します。
SharePoint Server アーカイブの設定	Microsoft SharePoint サーバーの文書をアーカイブする方法を説明します。
Skype for Business のアーカイブの設定	Skype For Business のセッションをアーカイブ化する方法を説明します。
SMTP アーカイブの設定	他のメッセージングサーバーから SMTP メッセージをアーカイブする方法を説明します。

マニュアル	コメント
Microsoft ファイル分類インフラストラクチャを使用した分類	Windows Server の新しいエディションに組み込まれた分類エンジンを使用して、新規と既存のすべてのアーカイブ済みコンテンツを分類する方法について説明します。
Veritas Information Classifier を使用した分類	Veritas Information Classifier を使用して、業界標準の分類ポリシーの包括的なセットを基準に新規とアーカイブ済みのすべてのコンテンツを評価する方法について説明します。Enterprise Vault を使用した分類を初めて行う場合は、以前の直観的でないファイル分類インフラストラクチャエンジンではなく、Veritas Information Classifier の使用をお勧めします。
管理者ガイド	日常的な管理を実行する方法を説明します。
PowerShell コマンドレット	Enterprise Vault PowerShell コマンドレットを実行して、さまざまな管理タスクを実行する方法を説明します。
監査	Enterprise Vault サーバー上でイベントの監査情報を収集する方法を説明します。
バックアップと回復	システムエラーが起きた場合にデータ損失を防止する効果的なバックアップ戦略の実装方法や、回復手段を利用する方法を説明します。
レポート	Enterprise Vault サーバー、アーカイブ、アーカイブ済みアイテムの状態に関するレポートを提供する、Enterprise Vault Reporting の実装方法を説明します。FSA レポートを設定すると、ファイルサーバーとそのボリューム用の追加レポートを利用できます。
NSF 移行	Domino ファイルと Notes NSF ファイルから内容を Enterprise Vault アーカイブにインポートする方法を説明します。
PST 移行	Outlook PST ファイルから内容を Enterprise Vault アーカイブに移行する方法を説明します。
ユーティリティ	Enterprise Vault のツールとユーティリティについて説明します。
レジストリ値	レジストリ値を一覧表示している参照用の文書で、さまざまな側面から Enterprise Vault の動作を修正する場合に使うことができます。
管理コンソールのヘルプ	Enterprise Vault 管理コンソールのヘルプ。
Enterprise Vault Operations Manager のヘルプ	Enterprise Vault Operations Manager のヘルプ。

サポートされているデバイスとソフトウェアのバージョンの最新情報について詳しくは、『Enterprise Vault [Compatibility Charts](#)』を参照してください。

Enterprise Vault トレーニングモジュール

Veritas 教育サービスでは、基本的な管理から詳細トピック、トラブルシューティングまで、Enterprise Vault の包括的なトレーニングを提供します。教室でのトレーニングや仮想トレーニングなど、さまざまな形式でトレーニングできます。

Enterprise Vault トレーニング、カリキュラムのパス、認定オプションについて詳しくは、<https://www.veritas.com/services/education-services> を参照してください。

Enterprise Vault の監査の概要

この章では以下の項目について説明しています。

- Enterprise Vault の監査について

Enterprise Vault の監査について

Enterprise Vault には、Enterprise Vault サーバーごとに有効にできる柔軟性の高い監査機能が組み込まれています。監査データは **SQL Server** データベースに書き込まれます。サイトのすべての Enterprise Vault サーバーに対して 1 つの監査データベースを使えます。

Enterprise Vault の監査では次が記録されます。

- イベント発生時刻
- アクティビティを開始したアカウント
- アーカイブされているアイテム
- イベントのカテゴリ (View、Archive、Delete など)

たとえば各種イベントの監査を有効にすることで、次のような詳細情報を取得できます。

- 管理コンソールを使って実行された処理
- 検索
- アイテムの参照
- 削除

大半の種類イベントでは、詳細レベルとして[概略]または[詳細]、あるいはこの両方を指定できます。

- [概略]を指定すると、イベントに関する情報 (日時、使用アカウント、使用ボルトなど) が記録されます。
- [詳細]を指定すると、メッセージの内容の一部 (件名、メールボックスの所有者、フォルダなど) に関する詳細な情報が記録されます。

監査データベースエントリは、SQL クエリーを使用するか、**Audit Viewer** ユーティリティを使用して表示できます。

Enterprise Vault は、Enterprise Vault SQL データベースを管理するための PowerShell コマンドレットを備えています。詳しくは『PowerShell cmdlet』ガイドを参照してください。

監査を有効にすると、パフォーマンスがわずかに低下する点に注意してください。

監査はデフォルトでは無効です。

監査の設定

この章では以下の項目について説明しています。

- [監査の設定](#)
- [監査データベースの作成](#)
- [監査カテゴリの設定](#)
- [監査の開始または停止](#)
- [監査の調整](#)
- [監査データベースの移動](#)

監査の設定

[表 3-1](#)は、監査を設定するのに必要なタスクを要約し、より詳細な情報が見つかるセクションへのリンクを提供します。

表 3-1 **監査を設定する手順**

手順	作業	関連情報
手順 1	監査データベースを作成する	1 つの監査データベースがサイト内のすべての Enterprise Vault サーバーに対して作成されます。 p.13 の「監査データベースの作成」 を参照してください。
手順 2	監査するカテゴリを選択する	サイト内の各 Enterprise Vault サーバーに監査カテゴリを設定します。 p.14 の「監査カテゴリの設定」 を参照してください。

手順	作業	関連情報
手順 3	監査を開始または停止する	サイト内の各 Enterprise Vault サーバーごとに監査を開始または停止する必要があります。 p.17 の「 監査の開始または停止 」を参照してください。
手順 4	必要に応じて、監査を調整します。	Enterprise Vault サービスによる監査データベースに対する接続数を変更することで監査を調整できます。 p.18 の「 監査の調整 」を参照してください。

Enterprise Vault 監査の構成には、関連付けられているレジストリ設定があります。Enterprise Vault 管理コンソールを使用してこれらのレジストリ設定を変更する代わりに、Regedit を使用して直接変更する場合、Enterprise Vault 監査は変更したユーザーに関する情報を取得できません。この情報を記録する場合は、`HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥KVS¥Enterprise Vault¥Admin¥Auditing` 以下の設定に **Windows Registry Auditing** を設定します。

メモ: Enterprise Vault 監査は、常に Enterprise Vault 管理コンソールを使用して設定してください。関連付けられたレジストリ値を直接変更しないでください。

監査データベースの作成

このセクションでは、管理コンソールを使って監査データベースを作成する方法について説明します。

適切なセキュリティを監査データベースに適用することが重要です。データベースへのアクセスをボルトサービスアカウントなどの特別な権限のあるユーザーに制限することを検討してください。たとえば、ボルトサービスアカウントが監査データベースのアーカイブ権限のレコードを削除または修正しないようにすることができます。

Enterprise Vault データベースには、使用環境でデータベースセキュリティを強化するのに使用できるロールがあります。データベースのロールを使用して、監査データベースのセキュリティを強化する方法について詳しくは、『[Using sing SQL Database Roles in Enterprise Vault, Compliance Accelerator, and Discovery Accelerator](#)』を参照してください。

メモ: 監査データベースは大きいサイズになることがあるため、新しいデータベースへのロールオーバーを実行したり、データベースからエントリを削除したりしてディスク容量を再生することが必要になる場合があります。詳しくは、『Enterprise Vault [SQL のベストプラクティスガイド](#)』を参照してください。

監査データベースを作成する方法

- 1 管理コンソールの左ペインの **Enterprise Vault** ディレクトリを右クリックし、コンテキストメニューの[監査の有効化]をクリックします。
- 2 [監査データベースの場所]の下[参照]をクリックして、監査データベースに利用可能な場所を表示します。
- 3 監査データベース用の新しいフォルダを作成する場合は、[新規フォルダ]をクリックします。
- 4 監査データベースに使う場所をクリックして、[OK]をクリックします。
- 5 [トランザクションログの場所]の下[参照]をクリックして、監査データベースのトランザクションログに利用可能な場所を表示します。
- 6 トランザクションログ用の新しいフォルダを作成する場合は、[新規フォルダ]をクリックします。
- 7 ログに使う場所をクリックして、[OK]をクリックします。
- 8 [OK]をクリックして、[監査の設定]ダイアログボックスを閉じます。
- 9 Enterprise Vault がデータベースを作成するまでしばらくお待ちください。
- 10 Enterprise Vault で監査データベースが作成されたことを確認するメッセージが表示されたら、[OK]をクリックしてメッセージを消去します。

監査のデータベースは Enterprise Vault ディレクトリデータベースと同じ SQL Server で作成されます。ただし、必要であれば、別のサーバーに監査データベースを移動できます。

p.18 の「[監査データベースの移動](#)」を参照してください。

監査カテゴリの設定

監査カテゴリは監査で収集可能な情報のさまざまな種類を識別します。監査データベースを作成した後、Enterprise Vault 管理コンソールを使って監査カテゴリを選択できます。すべてのカテゴリで監査の概要データを記録できます。また、一部のカテゴリでは詳細データも記録できます。

監査カテゴリは、管理コンソールの[Enterprise Vault サーバー]コンテナで選択した Enterprise Vault サーバーに適用されます。複数の Enterprise Vault サーバーがある場合、各サーバーを順番に選択して各サーバーの監査カテゴリを設定する必要があります。Enterprise Vault ディレクトリに関連付けられているサイト内のすべての Enterprise

Vault サーバーで一貫した監査カテゴリを設定することを推奨します。これを行えないと、使用環境で一貫性が失われた監査データが生成されます。[アーカイブ権限]カテゴリを選択すると、すべての Enterprise Vault サーバーでこのカテゴリを選択することが特に重要になります。

Enterprise Vault 管理者が監査の設定を変更すると、イベント ID 4288 で、監査が実行中 (有効) か停止状態 (無効) であるか、各監査カテゴリの状態、および変更を行った管理者の ID を報告します。同じ情報で監査データベースエントリも作成されます。

監査が実行中のとき、または停止しているときに監査カテゴリを修正できます。

表 3-2 監査カテゴリ

カテゴリ	説明
管理アクティビティ	Enterprise Vault 管理コンソールまたは管理シェルで行われた設定の変更 (新しいタスクの追加、アーカイブの作成、メールボックスの有効化など)。
詳細検索	検索語や検出アイテム数などの、実行された検索。
アーカイブ	アーカイブされるアイテム (手動またはスケジュール設定された実行)。
アーカイブフォルダの更新	異なるメールボックスフォルダに移動されているアーカイブ済みアイテム。
アーカイブ権限	<p>アーカイブに対するユーザーまたはグループのアクセス権限の手動による変更。アーカイブに手動で権限を設定するには、Enterprise Vault 管理コンソールで[アーカイブプロパティ]ダイアログボックスを使用するか、EVPM (Enterprise Vault Policy Manager) ユーティリティを使用します。このカテゴリを選択する場合は、サイト内のすべての Enterprise Vault サーバーでこれを選択する必要があります。</p> <p>この監査カテゴリは、自動的なアーカイブのアクセス権限への変更をキャプチャしません。自動的なアーカイブ権限は元のコンテンツソース上に設定されている権限で、Enterprise Vault アーカイブに同期します。この情報をキャプチャするには、コンテンツソースのアプリケーションで監査を有効にして設定する必要があります。たとえば、Exchange Server メールボックス上でユーザーが行うアクセス権限の変更は関連付けられた Enterprise Vault アーカイブに自動的に同期します。これらの権限の変更をキャプチャするには、メールボックスをホストする Exchange Server 上の Exchange Server Auditing を有効にして設定する必要があります。</p>
分類	アーカイブ済みアイテムの分類。
削除	保持期間の期限が切れたために削除されたか、ユーザーが削除することを選択したか、データ保護の法律に従ってサードパーティアプリケーションが削除を要求したために削除されるアーカイブ済みアイテム。

カテゴリ	説明
Domino アーカイブ	Domino のアーカイブアクティビティ。
Domino 復元	Domino の復元アクティビティ。
Exchange の同期	Exchange 管理内容の設定の作成、修正、削除の詳細を記録します。Exchange 管理フォルダからアーカイブし、管理内容の設定と同期するように設定されている場合、Enterprise Vault は関連する詳細を記録します。
FS アーカイブ	ファイルシステムのアーカイブアクティビティ。
オンライン XML の取得	SharePoint Portal Server への文書の取り込み。
インデックス操作	インデックスボリュームを管理するためのインデックスサブタスクの開始時および停止時。サブタスクによるインデックスの処理中に発生した重大なエラーも記録します。[インデックス管理]ウィザードを使ってインデックスボリュームを管理できます。
アーカイブの移動	個々のアーカイブ移動操作の詳細。
NSF 移行	NSF ファイルから移行されるアイテム。
PST 移行	PST ファイルから移行されるアイテム。
復元	復元されるアーカイブ済みアイテム。
保持カテゴリの更新	アーカイブ済みアイテムの保持カテゴリへの変更。
SPS アーカイブ	SharePoint アーカイブアクティビティ。
保存セットの状態	(サポート用。)ほとんど使われません。保存セットファイルが利用可能であるかどうかを記録します。
サブタスク制御	アーカイブ移動操作を制御するサブタスクなど、サブタスクの作成と修正。
削除の取り消し	アーカイブのプロパティの[削除済みアイテム]ページにあるオプション [アイテムを回復]を使って回復した削除済みアイテム。FSAUndelete ユーティリティを使って回復したショートカットも記録します。
User	独自の監査エントリ。
表示	アーカイブ済みアイテムの表示 (HTML または元の形式)。
添付ファイルを表示	SharePoint Portal Server 内部からのアーカイブ済みアイテムの表示。

監査カテゴリを設定する方法

- 1 管理コンソールの左ペインで、[Enterprise Vault サーバー]コンテナが表示されるまでツリーを展開します。
- 2 [Enterprise Vault サーバー]コンテナを展開します。
- 3 監査を設定する対象のコンピュータを右クリックして、コンテキストメニューの[プロパティ]をクリックします。
- 4 [監査]タブをクリックします。
- 5 監査カテゴリを選択するか、チェックマークをはずします。

表 3-2

- 6 [OK]をクリックして変更内容を保存します。

監査の開始または停止

監査を開始または停止するには、各 Enterprise Vault サーバーで次の手順を実行する必要があります。

監査が開始または停止されると、イベント ID 42388 で、監査の状態 (実行中 (有効) または停止状態 (無効))、各監査カテゴリの状態、および変更を行った管理者の ID が報告されます。Enterprise Vault 管理サービスが開始すると、監査が実行中の場合はイベント ID 4286 が報告され、監査が停止中の場合はイベント ID 4287 が報告されます。同じ情報で監査データベースエントリも作成されます。

監査を開始または停止する方法

- 1 管理コンソールの左ペインで、[Enterprise Vault サーバー]コンテナが表示されるまでツリーを展開します。
- 2 [Enterprise Vault サーバー]コンテナを展開します。
- 3 監査を開始または停止する対象のコンピュータを右クリックして、コンテキストメニューの[プロパティ]をクリックします。
- 4 [監査]タブをクリックします。
- 5 Enterprise Vault サーバーで監査を開始するには、[以下のカテゴリに基づいてエントリを監査]を選択します。
サーバーでの監査を停止するには、この設定のチェックマークをはずします。
- 6 [OK]をクリックして変更内容を保存します。

監査の調整

監査が有効になっているコンピュータごとに、監査データベースに接続できる数が制限されています。これらの接続は、必要に応じて再使用されます。監査では、監査データベースへの接続のプールが使われます。**Enterprise Vault** 監査レコードをこれらの接続の使用レベルにすることができ、必要に応じて接続数を修正できます。

監査を調整する方法

- 1 管理コンソールの左ペインで、[Enterprise Vault サーバー]コンテナが表示されるまでツリーを展開します。
- 2 [Enterprise Vault サーバー]コンテナを展開します。
- 3 接続情報のログを有効または無効にする対象のコンピュータを右クリックして、コンテキストメニューの[プロパティ]をクリックします。
- 4 [監査]タブをクリックします。
- 5 [詳細設定]をクリックします。
- 6 [データベース情報をログに記録]を選択するか、チェックマークをはずして、ログを有効または無効にします。
- 7 必要に応じて、各 Enterprise Vault サービスの接続数を変更します。
- 8 [OK]をクリックします。
- 9 コンピュータの Enterprise Vault 管理サービスを再起動します。

監査データベースの移動

必要に応じて、たとえばディザスタリカバリの間に、異なる SQL Server に監査データベースを移動できます。データベースを移動したら、監査が有効になる各 Enterprise Vault サーバーで次の手順を完了してください。

監査データベースを移動する方法

- 1 新しい SQL Server に、監査データベースを移動します。
- 2 Enterprise Vault サーバーで、ODBC データソースアドミニストレータを使って EVAudit ODBC データソースで新しい SQL Server を選択します。
- 3 ODBC データソースアドミニストレータでのテストが可能になったら、データソースをテストします。

監査データベースエントリの表示

この章では以下の項目について説明しています。

- [監査データベースエントリの表示について](#)
- [Audit Viewer を使用した監査データベースエントリの表示](#)
- [SQL クエリーを使用した監査データベースエントリの表示](#)

監査データベースエントリの表示について

監査データベースエントリは、SQL クエリーを使って表示およびフィルタ処理できます。スクリプトを使用して、エントリの処理方法と表示方法をカスタマイズすることもできます。

また、Enterprise Vault は、監査エントリを表示およびフィルタ処理できる Audit Viewer ユーティリティを備えています。

Audit Viewer を使用した監査データベースエントリの表示

Audit Viewer を使用すると、Enterprise Vault の監査データベースに記録されているデータを表示してフィルタ処理できます。表示するデータを指定し、データをソートし、Windows のクリップボードにコピーできます。

Audit Viewer による監査データのレポートの実行

このセクションの次の手順に従って Audit Viewer を開き、監査データベースにあるデータのレポートを生成します。

メモ: コンピュータでユーザーアカウント制御 (UAC) が有効になっている場合は、管理者権限でこのユーティリティを実行してください。

Audit Viewer を使って監査データを実行する方法

- 1 Windows エクスプローラで、Enterprise Vault プログラムフォルダ (たとえば、C:\Program Files (x86)\Enterprise Vault) を参照します。
- 2 AuditViewer.exe をダブルクリックします。
- 3 Audit Viewer ウィンドウで、表示するレコードの検索基準を入力するか、選択します。
- 次の表に検索条件について説明します。

ユーザー名	必要なユーザーを domain\username の形式で指定します。
アーカイブ	必要なアーカイブの名前を指定します。Enterprise Vault 管理コンソールを使って名前を決めることができます。
カテゴリ	検索する監査エントリのカテゴリを一覧から選択します。Audit Viewer では、キャプチャしたデータに存在するカテゴリのみが一覧表示されます。
Subcategory	カテゴリを選択した後、一覧からサブカテゴリを選択します。 <div><div>■ [アイテム]を選択すると、カテゴリの概略情報が返されます</div><div>■ カテゴリに[詳細]を選択すると、情報レコードに追加情報が保持されます</div><div>■ [すべて]を選択すると、選択したカテゴリの概略と詳細レコードの両方が返されます</div></div>
Date (From), Date (To)	監査レコードの検索を行う日付範囲と時間範囲を定義します。
Information contains	監査レコードを検索するためのキーワードを入力します。
状態	表示するレコードの状態を一覧から選択します。
サーバー	この検索の対象となる Enterprise Vault サーバーを選択します。
Audit ID	表示する監査レコードを表す数字の範囲を入力します。
Order By	Audit Viewer の結果の表示基準に使う属性と、昇順で一覧表示するか、降順で一覧表示するかを選択します。

Maximum Results 検索で見つかったすべての結果を表示するか、結果の一部を表示するかを選択します。

- 4 [検索]をクリックしてレポートを生成します。

Audit Viewer の検索結果のコピー

Audit Viewer によって、検索基準に一致するレコードが[Search Results]ウィンドウに表示されます。

列のエントリに従ってレコードをソートするには、その列見出しをクリックします。

このウィンドウの内容を表計算アプリケーションなどの他のアプリケーションにコピーできます。

Audit Viewer の検索結果をコピーする方法

- 1 [Search Results]ウィンドウで、コピーするレコードをハイライトします。
- 2 レコードを右クリックして、[コピー]をクリックします。

Ctrl+A と Ctrl+C を押して、すべての検索結果をクリップボードにコピーすることもできます。
- 3 コピー先の文書にレコードを貼り付けます。

Audit Viewer の設定の変更

検索する監査データベースは変更できます。Audit Viewer には、選択したフィールドを[検索結果]ウィンドウで表示/非表示にするオプションも用意されています。

Audit Viewer の設定を変更するには

- 1 Audit Viewer のメインウィンドウで、[設定]をクリックします。
- 2 [設定]ウィンドウで、検索する監査データベースを変更します。表示/非表示にする戻り値フィールドを選択または選択解除することもできます。

SQL クエリーを使用した監査データベースエントリの表示

監査データベースでデータベースビュー EVAuditView を問い合わせることをお勧めします。SQL クエリーは、日付範囲、ユーザー名、ObjectID などの条件に基づいて監査エントリをフィルタ処理できます。監査データベースのエントリの形式および EVAuditView 列の値の監査エントリのさまざまな種類について詳しくは、このドキュメントの付録を参照してください。

p.30 の「[監査データベースエントリの形式](#)」を参照してください。

次の手順では、**SQL Server Management Studio** を使用して SQL クエリーを入力および実行する方法を示します。以降のセクションには、アイテムの削除操作のためのデータベースエントリを検索する SQL クエリーの例が含まれます。このようなクエリーは、アイテムの削除の証拠を取得するなどの目的で実行する必要があります。たとえば、データ保護規制に準拠していることを示す場合です。

p.24 の「[一般的な削除操作の監査](#)」を参照してください。

アーカイブのアクセス権限に対する変更は、セキュリティ記述子定義言語 (SDDL) の文字列として示されます。**Enterprise Vault** には、これらの文字列をユーザーフレンドリな形式の権限の配列に変換するためのスクリプトが同梱されています。

p.23 の「[ユーザーフレンドリな形式でのアーカイブ権限への監査済み変更の取得](#)」を参照してください。

SQL Server Management Studio を使って監査データベースエントリを表示する方法

- 1 SQL Server Management Studio を起動します。
- 2 標準ツールバーで、[新しいクエリ]をクリックします。
- 3 SQL Editor ツールバーで、利用可能なデータベースの一覧から **EnterpriseVaultAudit** を選択します。
- 4 必要な監査エントリを取得する SQL クエリーを入力します。

この簡単なサンプルクエリーでは、データベースビュー **EVAuditView** から日付の順序で監査エントリを取得します。

```
SELECT * FROM EVAuditView ORDER BY AuditDate DESC
```

次に、別のクエリーの例を示します。このクエリーの例では、エントリが日付範囲とユーザー名に基づいてフィルタ処理されます。

```
USE EnterpriseVaultAudit
```

```
DECLARE @StartDateTime datetime
```

```
DECLARE @EndDateTime datetime
```

```
SET @StartDateTime = '2017-10-05 08:00:00'
```

```
SET @EndDateTime = '2017-10-06 08:00:00'
```

```
SELECT * FROM [EnterpriseVaultAudit].[dbo].[EVAuditView]  
WHERE AuditDate BETWEEN @StartDateTime and @EndDateTime  
AND UserName in ('Org¥HSmith', 'Org¥JDoe')  
ORDER BY AuditID
```

- 5 SQL Editor ツールバーで[実行する]をクリックするか、F5 を押してコマンドを実行します。

ユーザーフレンドリな形式でのアーカイブ権限への監査済み変更の取得

管理者は[アーカイブプロパティ]の[権限]タブを使うか、Enterprise Vault Policy Manager (EVPM) ユーティリティを使って、アーカイブに対する手動権限を変更することができます。監査データベースエントリでは、手動によるアーカイブのアクセス権限の変更は、Windows の権限ではセキュリティ記述子定義言語 (SDDL) の文字列として表示され、Domino の権限では XML として表示されます。Enterprise Vault には、これらの文字列をユーザーフレンドリな形式の権限の配列に変換する方法を示す、PowerShell のサンプルスクリプト ExampleEvPermissionsAuditHelper.ps1 が含まれています。スクリプトの出力には、次の情報が含まれています。

- アーカイブの ID の詳細情報
- 権限を変更した Enterprise Vault 管理者の名前
- アーカイブに対する手動権限が設定されている各管理者の新旧の権限リスト

サンプルスクリプトは、Enterprise Vault\installation\Auditing フォルダにあります。監査データベース上でスクリプトを実行するか、監査データベース処理の一環として使うようにスクリプトを変更します。このスクリプトを実行するために Enterprise Vault 管理シェルを使う必要はありません。

サンプルスクリプト内のコメントは、スクリプトの機能、スクリプトを実行するために必要な権限、このサンプルの制限を示しています。使用環境に合わせてスクリプト内の値を変更する必要があります。

[アーカイブプロパティ]ダイアログボックスや EVPM で利用できる権限は、読み取り、書き込み、削除です。これらの権限は、監査データベースエントリ内の詳細な権限と同じです。表 4-1 に、管理者が利用できる権限と、サンプルスクリプトで出力される監査データベースエントリに表示される基本的な権限とのマッピングを示します。

表 4-1 利用可能な権限とスクリプトで出力される権限のマッピング

アーカイブプロパティと EVPM の権限	サンプルスクリプトで出力される権限
読み取り	READ_FOLDER READ_ITEM
書き込み	ADD_FOLDER ADD_ITEM CONTROL_FOLDER
削除	DELETE_FOLDER DELETE_ITEM

データ保護コンプライアンス の監査

この章では以下の項目について説明しています。

- [一般的な削除操作の監査](#)
- [権限がある削除操作の監査](#)

一般的な削除操作の監査

EU 一般データ保護規則 (GDPR) などの一部のデータ保護規則には、「忘れられる権利」が含まれています。この規則は、組織のストレージシステムに保持する必要がなくなった個人情報を削除するための要求に対応します。**Enterprise Vault** 監査は、このような情報が削除された証拠を提供するために使用できます。

このセクションでは、**Enterprise Vault** 内の特定の情報を削除するための要求をサポートするように **Enterprise Vault** を設定する方法について説明します。検索例に、アイテムの削除操作の証拠を提供する監査エントリを取得する方法を示します。このセクションの例は、**Enterprise Vault** での一般的な削除操作に関連します。

権限がある削除機能は、**Discovery Accelerator** で利用可能です。この機能を使用することで、特別な権限を持つ管理者は、データ規制に準拠するためにアイテムを削除できます。類似の機能は、**Enterprise Vault API** を使用するサードパーティのアプリケーションでも利用可能です。これらの操作のための **Enterprise Vault** 監査エントリは、データ規制への準拠の一環として、削除操作が実行されたことを識別します。この理由から、権限がある削除操作のための **SQL** 検索と結果は、一般的な削除操作の場合と若干異なります。

p.28 の「[権限がある削除操作の監査](#)」を参照してください。

[表 5-1](#) に、特定のデータがアーカイブから削除されたことの証拠として監査データベースエントリを提供するための手順の例を示します。

検索を容易にするため、この例には **Enterprise Vault** 分類機能の使用が含まれています。**Enterprise Vault** 分類機能を設定し、アーカイブされるときにさまざまな種類の情報にタグ付けすることができます。たとえば、**Enterprise Vault** 分類は、個人識別情報 (PII) に `evtag.category:PII` タグを適用できます。

表 5-1 アイテム削除の証拠を提供する手順

手順	処理	関連情報
1	[ユーザーが削除したアイテムの回復を有効にする] サイト設定にチェックマークが付いていないことを確認します。	「忘れられる権利」要求の可能性が高い場合は、このサイト設定を有効にしないことが重要です。これにより、「忘れられる権利」要求が実行された後もアイテムは復元されません。
2	監査が有効であり、必要な監査カテゴリが選択されていることを確認します。	Enterprise Vault 監査を有効にします。 Enterprise Vault サーバーのプロパティで、この例のために有効にする必要がある監査カテゴリは[詳細検索]と[削除]です。[削除]カテゴリには概略レベルで十分です。
3	削除する項目を検索します。	この例では、削除するデータを Exchange メールボックスアーカイブから検索するために、 Enterprise Vault 検索を使用します。 検索を実行する前に、検索を実行する管理者が、アイテムを削除するユーザーのアーカイブに対する十分な権限を持っていることを確認します。 入力する検索は <code>'evtag.category:PII'</code> です。 Enterprise Vault 検索が実行する実際の検索は次のとおりです。 <code>' (NOT sens:2) AND (evtag.category:PII) '</code> これは、 Outlook で「Private」としてマーク付けされたすべてのアイテムは検索で返されないことを意味します。 Enterprise Vault 検索は、このフィルタ処理を自動的に行います。
4	Enterprise Vault 検索を使用して、返されたすべての結果を削除します。	検索ポリシーで、アイテムの削除が有効になっていることを確認します。 Enterprise Vault 検索で、削除するアイテムを右クリックし、[削除]を選択します。
5	Enterprise Vault 検索で同じ検索を繰り返します。	正しい項目が削除されたことを示すため、同じ検索を繰り返すことが重要です。

手順	処理	関連情報
6	監査データベースで削除操作エントリを検索します。	適切な SQL クエリーを使って、監査証跡の関連部分を抽出します。検索クエリーは、監査日付、アーカイブ ID などに基づいて実行できます。 p.26 の「一般的なアイテム削除の監査エントリ用のクエリー検索例」 を参照してください。 p.28 の「権限がある削除の監査エントリ用のクエリー検索例」 を参照してください。

一般的なアイテム削除の監査エントリ用のクエリー検索例

次の簡単なクエリーは、指定された期間内のすべての検索と削除エントリを監査データベースから取得します。

```
USE EnterpriseVaultAudit
SELECT * FROM [EnterpriseVaultAudit].[dbo].[EVAuditView]
WHERE CategoryName in ('Search', 'Delete')
AND AuditDate BETWEEN '2017-10-05 08:27:48' and '2017-10-05 08:32:37'
ORDER BY AuditID desc
```

次の SQL クエリーでは、この簡単なクエリーが、アーカイブにもフィルタを適用するように拡張されています。アーカイブの情報は、Enterprise Vault ディレクトリに格納されています。

```
DECLARE @ArchiveId varchar(112)
DECLARE @StartDateTime datetime
DECLARE @EndDateTime datetime

SET @ArchiveId =
'1B29F35DAA512AC47A64558FDF7A614571110000example.local'
SET @StartDateTime = '2017-10-05 08:27:48'
SET @EndDateTime = '2017-10-05 08:28:37'

CREATE TABLE #ArchiveFolders
(
    VaultEntryId varchar(112)
)

INSERT INTO #ArchiveFolders
SELECT VaultEntryId
FROM [EnterpriseVaultDirectory].[dbo].[ArchiveFolderView]
WHERE ArchiveVEID = @ArchiveId
```

```
SELECT * FROM [EnterpriseVaultAudit].[dbo].[EVAuditView]
auditView LEFT JOIN #ArchiveFolders archFolder
ON archFolder.VaultEntryId = auditView.Vault
WHERE AuditDate BETWEEN @StartDateTime and @EndDateTime
AND CategoryName in ('Search', 'Delete')
ORDER BY AuditID

DROP TABLE #ArchiveFolders
```

表 5-2 に、監査データベースの SQL クエリーによって返されるデータの例を示します。列のタイトルは、監査データベースのデータベースビュー **EVAuditView** に関連しています。**[Example values (Search)]** 列の値は、削除するアイテムの最初に検索によって作成された監査エントリを示します。**[Example values (Delete)]** 列の値は、ユーザー **jdoe** がアイテムを削除したときに作成された監査エントリを示します。

表 5-1 の手順に従うと、アイテムが存在しなくなったことを示す最終的な検索の監査エントリもあります。この監査エントリは、表 5-2 には含まれていません。

監査データベースのエントリの形式および **EVAuditView** 列の値の監査エントリのさまざまな種類について詳しくは、このドキュメントの付録を参照してください。

表 5-2 SQL クエリーから返される監査エントリの値の例

EVAuditView 列のタイトル	Example values (Search)	Example values (Delete)
AuditID	3582	3584
Status	SUCCESS	SUCCESS
AuditDate	31/08/2017 10:03:37	31/08/2017 10:03:44
UserName	example¥jdoe 検索操作を実行したユーザーを示します。	example¥jdoe 削除操作を実行したユーザーを示します。
CategoryName	Search	Delete
SubCategoryName	Searches	Item
ObjectID (Saveset および/または Folder ID)		#142\$1610D28B10DB21647B11EEF479 019B70B1110000example.local
Vault (Archive ID または Folder ID)	16454F118169EDE48822DC10CE 69307CA1110000example.local	1610D28B10DB21647B11EEF479019 B70B1110000example.local

EVAuditView 列のタイトル	Example values (Search)	Example values (Delete)
Info	Query '(NOT sens:2) AND (evtag.category:PII)', matching '8' entries, viewing range '1' to '100'	
MachineName	EVServer1	EVServer1

権限がある削除操作の監査

選択した **Discovery Accelerator** クライアントユーザーに規制レビューアの役割を割り当てることによって、**Enterprise Vault** アーカイブから完全にアイテムを削除することを許可できます。役割に関連付けられた「権限がある削除」が許可されると、これらのユーザーは、アーカイブから削除するためにケースレビューセット内のアイテムをマーク付けできるようになります。権限がある削除機能について詳しくは、『**Discovery Accelerator** 管理者ガイド』を参照してください。

コンプライアンス削除機能は、**Enterprise Vault API** を使用するサードパーティのアプリケーションでも利用可能です。サードパーティアプリケーションで実行されるユーザーは、**Enterprise Vault** コンプライアンス削除アプリケーションの役割に割り当てられている必要があります。

Enterprise Vault 監査では、**Discovery Accelerator** で権限がある削除を使用したコンプライアンス削除と、**Enterprise Vault API** を使用するサードパーティアプリケーションでのコンプライアンス削除に関する追加情報が記録されます。

コンプライアンス削除操作に関する情報を取得するため、監査データベースに対して SQL クエリーを実行できます。

権限がある削除の監査エントリ用のクエリー検索例

次のクエリー例は、指定した期間内のアイテム削除操作を監査データベースで検索します。

```
USE EnterpriseVaultAudit
GO
SELECT * FROM EVAuditView WHERE CategoryName = 'Delete' AND
SubCategoryName = 'Information' AND AuditDate BETWEEN
CONVERT(datetime,'mm-dd-yyyy',110) and
CONVERT(datetime,'mm-dd-yyyy',110)
```

表 5-3 に、このクエリーから返される監査エントリの値の例を示します。

表 5-3 SQL クエリーから返される監査エントリの値の例

EVAuditView 列のタイトル	Example values (Delete)
AuditID	4
Status	SUCCESS
AuditDate	2018-02-02 17:01:56.583
UserName	example¥vsa 削除操作を実行したユーザーを示します。Discovery Accelerator の権限がある削除機能で削除されたアイテムの場合、UserName 列にボルトサービスアカウントの名前が表示されます。サードパーティ製のアプリケーションによって削除されたアイテムの場合、これはコンプライアンス削除アプリケーションの役割に割り当てられているユーザーです。
CategoryName	Delete
SubCategoryName	Information
ObjectID	201802017502363~201802011626030000~Z~A158658C6FBE60B76 削除されたアイテムの保存セット ID を示します。
Vault	600B5AA958C24411F9D0B892B91F5E4393B33DB7F88B8E551110000VS1 アイテムが含まれているアーカイブを示します。
Info	<Delete ObjectType="Item" ObjectName="(null)"> <Property Name="EV_API_DELETION_LEVEL"> <Current Value="DELETION_LEVEL_COMPLIANCE"/> </Property> </Delete> 削除レベル DELETION_LEVEL_COMPLIANCE は、そのアイテムが、Discovery Accelerator の権限がある削除や、Enterprise Vault API を使用するサードパーティアプリケーションのコンプライアンス削除を使用して削除されたことを示します。
MachineName	EVServer1

監査データベースエントリの形式

この付録では以下の項目について説明しています。

- [監査データベースエントリの形式](#)

監査データベースエントリの形式

Enterprise Vault 12.3 では、管理アクティビティの監査 ([管理アクティビティ]監査カテゴリ) の機能が強化されました。具体的には、次の領域の管理アクティビティに関連する情報の品質が大幅に向上します。

- Exchange、SMTP、検索ポリシー
- Exchange と SMTP タスク
- Exchange と SMTP ターゲット
- Exchange メッセージクラス
- アーカイブ

役割ベースの管理、ボルトストアとパーティションの管理、詳細設定の監査にも改良が加えられています。

強化された情報は、管理コンソールで、または PowerShell コマンドレットを使用して実行する処理に関して使用できます。

メモ: Veritas はいくつかのリリースにわたって Enterprise Vault 監査を向上してきました。この付録に記載された詳しい情報は、将来のリリースで変更される可能性があります。

監査データベースの EVAuditView データベースビューは、監査エントリの表示に使用でき、次の列で構成されます。

表 A-1 EVAuditView 列の説明

列のタイトル	内容の説明
AuditID	監査エントリの一意の識別子です。
Status	SUCCESS または FAILURE です。操作が正常に完了したか失敗したかを示します。
AuditDate	監査エントリの原因となった処理または操作の日時を示します。
UserName	処理を実行したユーザーを示します。
CategoryName	Enterprise Vault サーバーの[コンピュータプロパティ]で定義されている監査カテゴリを示します。
SubCategoryName	監査エントリの特定の分類を示します。
ObjectID	変更されたエンティティの ID を示します。たとえば Saveset ID、Site ID、Archive ID です。
Vault	大量の監査の場合のみ、これには Archive ID または ArchivePoint ID が含まれることがよくあります。
Info	実行された処理に関する詳細情報が自由形式テキストで提供されます。 Enterprise Vault 12.3 以降では、この列に監査処理に関するより詳しい情報が提供されます。各種監査エントリのこの列の内容が、この付録の主なトピックです。
MachineName	監査エントリが生成されたマシンを示します。

Info 列に新しい形式が導入されました。これにより、監査処理についての情報を構造化された一貫性がある方法で表示することが可能になります。この付録の残りの部分では、さまざまな監査エントリの Info 列の内容について説明します。完全な監査エントリには、日時、処理を実行したユーザー、変更されたエンティティの ID などの前述の情報も含まれることに注意してください。

監査エントリを日付範囲、ユーザー名、ObjectID などの条件に基づいて表示およびフィルタ処理するには、SQL クエリーを使用することをお勧めします。

結果に形成された XML を返すには、次のようなクエリーを使用します。

```
USE EnterpriseVaultAudit
SELECT TOP 50 ObjectID, AuditDate, UserName,
    TRY_CAST(info AS XML) AS infoXML
FROM EVAuditView
ORDER BY auditid DESC
```

単純な監査エントリの Info の内容

次の例に、Exchange メールボックスポリシーの設定が変更されたときに作成された監査エントリの Info 列の内容を示します。表 A-2に、含まれる値について説明します。

```
<Update ObjectType="ExchangePolicyView"
  ObjectName="Exchange Mailbox Policy 2">
  <Property Name="ProcessUnreadMail">
    <Previous Value="0" />
    <Current Value="1" />
  </Property>
  <Property Name="ProcessUnreadMail:TextValue">
    <Previous Value="Off" />
    <Current Value="On" />
  </Property>
</Update>
```

表 A-2 例の XML フィールドの説明

XML フィールド	説明
Update	処理の種類を示します。これは、通常 Create、Update、または Delete です。
ObjectType	この処理の影響を受けるエンティティの種類を示します。多くの場合、変更されたデータベーステーブルまたはビューの名前です。ただし、エントリによってはわかりやすい名前が提供されることがあります。
ObjectName	変更されたエンティティの名前を示します。ObjectName は、該当する値がない場合はボビュレートされないことがあります。
Property Name	エンティティに関連するプロパティの名前を示します。(メモ 1を参照してください)。 Create 操作と Delete 操作の場合、ほとんどのプロパティが値を取得するか失うため、ほとんどのプロパティが一覧表示されます。(メモ 2を参照してください)。 Update 操作の場合、変更されたプロパティのみが含まれます (メモ 3を参照してください)。 Property Name フィールドの末尾の :TextValue は、次の値が設定のテキスト形式の値であることを示します。この例では、値のテキスト形式での値は "0" と "1" が "Off" と "On" を示します。
Previous Value	処理が実行される前のプロパティの値です。
Current Value	処理が実行された後のプロパティの値です。

メモ

- 1 多くの場合、名前はデータベースで使用する名前のため、ユーザーインターフェースの名前と完全には一致しないことがあります。
- 2 監査証跡の不要な膨張を避けるため、**Exchange** メールボックスのサイズなどの非常に頻繁に変更される一部のプロパティは含まれません。
- 3 追加のプロパティがコンテキストに含まれる場合があります。これは、他の種類の監査エントリにも適用されます。

複合プロパティの Info の内容

Enterprise Vault データベースの一部の設定では、複数の設定が単一の値で表されます。監査エントリは、これらの設定を個別のプロパティに分割します。通常 Update エントリには、変更された設定のみが表示されます。

次の例では、Info の内容が、**Exchange** メールボックスポリシーの[ショートカットの内容]タブで[バナーを含める]と[アーカイブされたアイテムへのリンクを含める]という設定の変更後に監査エントリ内で生成されました。これら 2 つの設定は、**Enterprise Vault** データベースに単一の値として保存されます。

```
<Update ObjectType="ExchangePolicyView"
  ObjectName="Exchange Mailbox Policy 2">
  <Property Name="excShortcutDetail">
    <Previous Value="1000005" />
    <Current Value="1000029" />
  </Property>
  <Property Name="excShortcutDetail:IncludeArchivedBanner">
    <Previous Value="False" />
    <Current Value="True" />
  </Property>
  <Property Name="excShortcutDetail:IncludeLinkToArchivedItem">
    <Previous Value="False" />
    <Current Value="True" />
  </Property>
</Update>
```

例からわかるように、[バナーを含める]設定と[アーカイブされたアイテムへのリンクを含める]設定に関する情報は、個別のプロパティとして表示されます。

複数の設定が単一のプロパティに格納されている場合の Info の内容

次の例では、Info の内容は **SMTP** ターゲットが削除されたときに監査エントリ内に生成されました。

```
<Delete ObjectType="SmtptargetViewEx"
  ObjectName="JDoe@example.com">
  <Property Name="TargetId">
    <Current Value="19" />
  </Property>
  <Property Name="Address">
    <Current Value="JDoe@example.com" />
  </Property>
  <Property Name="poName">
    <Current Value="Default SMTP Policy" />
  </Property>
  <Property Name="RetentionCategoryName">
    <Current Value="RetCat01" />
  </Property>
  <Property Name="poPolicyEntryId">
    <Current Value="1781F4D98B1045F438445AC9
      8AD9579331s10000ev.local" />
  </Property>
  <Property Name="RetentionCategoryId">
    <Current Value="141E6B5A255237C4D83BB499
      390F27F091b10000ev.local" />
  </Property>
  <Property Name="ArchivingEnabled">
    <Current Value="1" />
  </Property>
  <Property Name="TargetType">
    <Current Value="1" />
  </Property>
  <Property Name="ArchiveInformation">
    <Current Value="<AI tn="JDoe@example.com" tid="19"
      an="Archive1" at="2049" aid="1868FD2720BFF62
      4483309845BDCCFEDB1110000ev.local" vs="Store1"
      ev="ev.local"/><AI tn="JDoe@example.com" tid=
      "19" an="Archive2" at="2049" aid="151D27
      0BA9638354DBE2B02FBFF7AF25C1110000ev.local" vs="Store1"
      ev="ev.local"/><AI tn="JDoe@example.com" tid="19"
      an="Archive3" at="2049" aid="13C3DC68A1FB836
      479CA542E4AE0CF9761110000ev.local" vs="Store2"
      ev="ev.local"/>" />
  </Property>
</Delete>
```

ArchiveInformation プロパティには、SMTP ターゲットに割り当てられた 3 つのアーカイブの詳細を示す XML が含まれます。

ArchiveInformation プロパティ内の情報をより読みやすくするため、各アーカイブについて個別の監査エントリが作成されます。次の例は、前の ArchiveInformation プロパティ内の Archive3 の監査エントリを示します。

```
<Delete ObjectType="SmtptargetViewEx:ArchiveInformation"
ObjectName="JDoe@example.com">
  <Property Name="TargetAddress">
    <Current Value="JDoe@example.com" />
  </Property>
  <Property Name="TargetId">
    <Current Value="19" />
  </Property>
  <Property Name="ArchiveName">
    <Current Value="Archive3" />
  </Property>
  <Property Name="ArchiveType">
    <Current Value="2049" />
  </Property>
  <Property Name="ArchiveId">
    <Current Value="13C3DC68A1FB836479CA542
      E4AE0CF9761110000ev.local" />
  </Property>
  <Property Name="VaultStoreName">
    <Current Value="Store2" />
  </Property>
  <Property Name="EvServer">
    <Current Value="ev.local" />
  </Property>
</Delete>
```

1 つの監査エントリの複数エントリへの分割は、情報をより明確に示すために使用されません。複数の監査エントリを作成するその他の例として、役割ベースの管理の更新、SMTP ポリシーでの X-Header の管理などがあります。