Actian Audit for Zen 簡易操作ガイド

株式会社エージーテック

2022 年 10 月 20 日

免責事項

株式会社エージーテックは本書の使用を、利用者またはその会社に対して「現状のまま」でのみ許諾するものです。株式会社エージーテックは、いかなる場合にも本書に記載された内容に関するその他の一切の保証を、明示的にも黙示的にも行いません。本書の内容は予告なく変更される場合があります。

商標

すべての Pervasive ブランド名および製品名は、Pervasive Software Inc. の米国およびその他の国における登録商標または商標です。また、すべての Actian のブランド名は、Actian Corporation の米国およびその他の国における登録商標または商標です。

文中の社名、商品名等は各社の商標または登録商標である場合があります。

Actian Audit for Zen 簡易操作ガイド

最終更新:2022 年 10 月 20 日

目次

はじめに

Actian Audit for Zen は、誰が、いつ、どのデータを作成／更新したかといった監査情報を記録するために Actian Zen のデータベース エンジンを拡張するツールで、海外では「Audit Master」という名称で販売されています（商標の関係で日本では「Audit for Zen」としてリリースされています）。

Audit for Zen がインストールされると、監査データを監査ログに保存するためにログ イベントハンドラーが Zen データベース エンジンに追加されます。

監視中のデータベース テーブルに変更があった場合、イベントハンドラーは同時に変更前の情報も記録していくため、Audit for Zen を使用することで監査データを閲覧だけでなく、データを変更前の状態に戻すこともワンアクションで可能になっています。

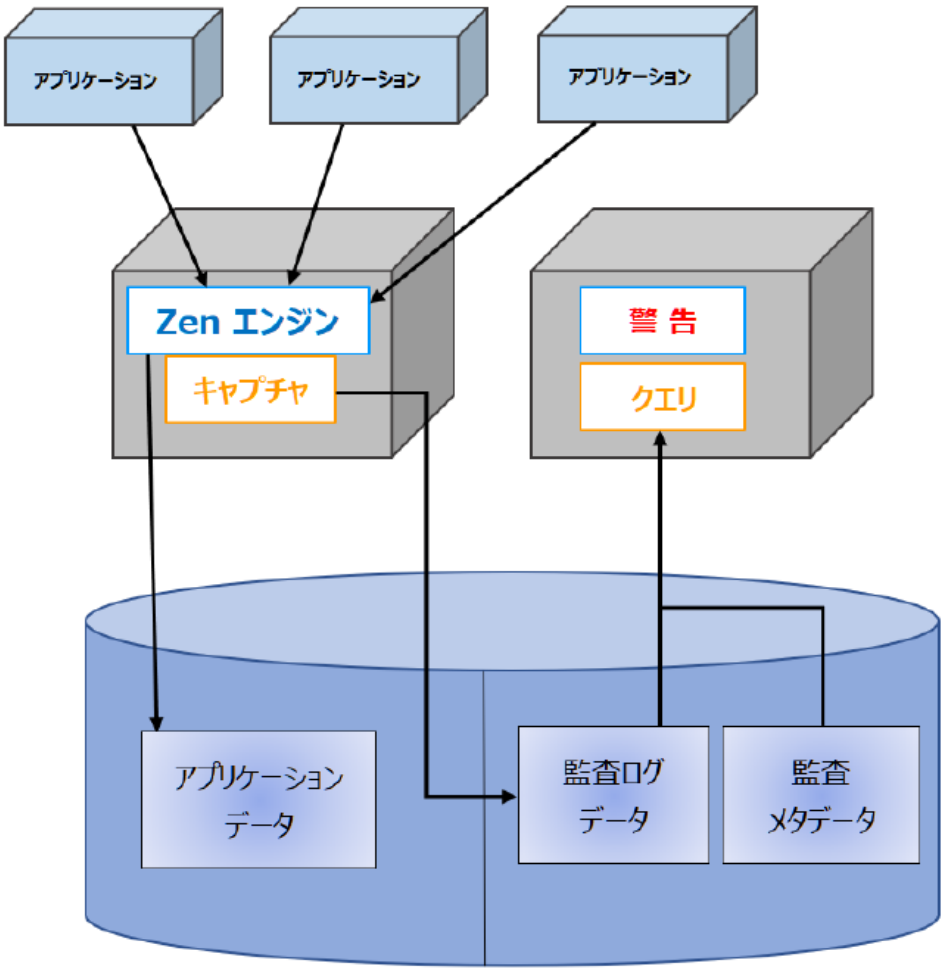
その他、特定のステータス コードをエラーの発生として記録したり、データの変更を Windows のイベント ログに出力したりすることもできるため、何か問題があった場合に即座に管理者にメールで通知するような設定も可能です。

Audit for Zen の使用方法の詳細はマニュアルに記載されていますが、本稿では手早く製品を使いこなすための情報をまとめています。
Audit for Zen の機能を評価する際にご参考にしていただければ幸いです。

DEMODATA を例とした設定方法と手順

Audit for Zen をインストールすると Zen データベース サーバーには、ログ イベントハンドラーがインストールされます。

ログ イベントハンドラーはテーブル監視条件に一致したレコードをキャプチャし、監査ログに記録していきます。

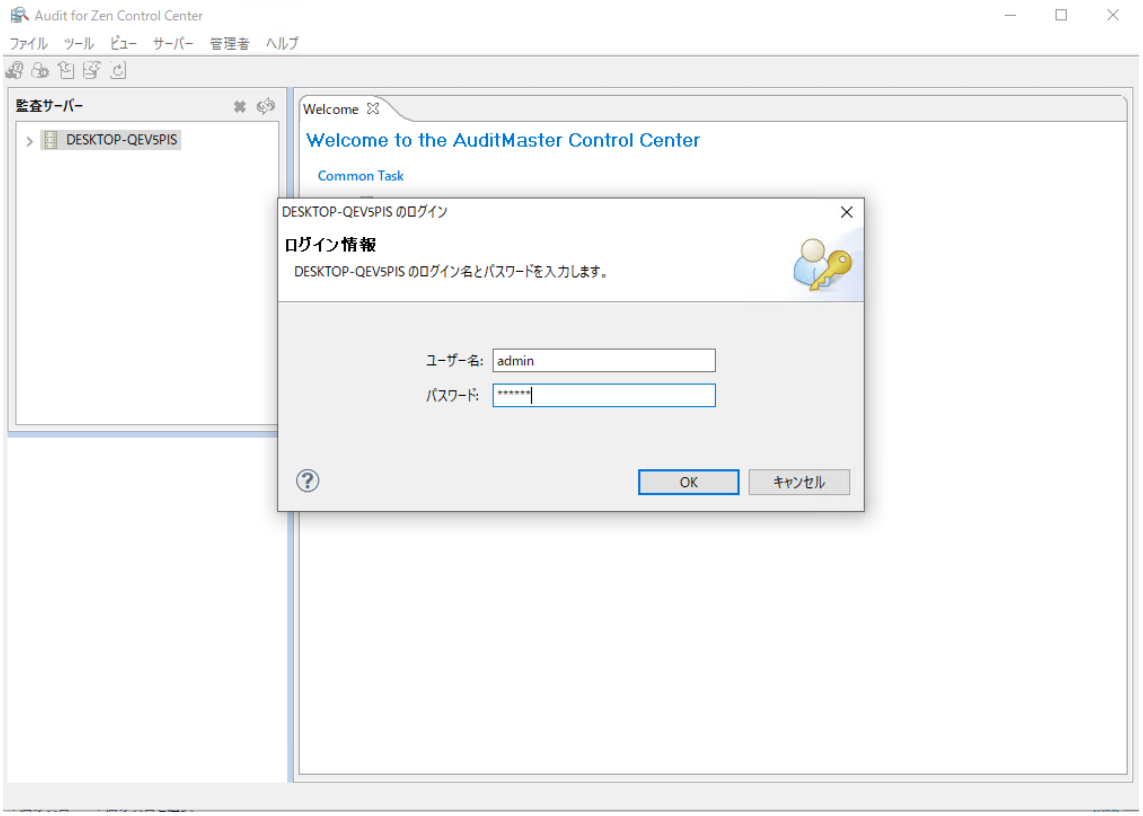


記録されたログの内容は、クエリおよび表示用のビュー ファイルに移動されます。さらに所定の条件になると、ビュー ファイルの内容はアーカイブ ファイルへ移動されます。

それでは、Audit for Zen 付属のサンプル データベース DEMODATA を例として設定・手順の説明をしていきましょう。

AZ Control Center の起動

Audit for Zen をインストールすると AZ Control Center がスタート メニューに登録されます。
AZ Control Center を使用すると監査条件の設定、監査データの確認などができます。
まずはこのツールを起動してみましょう。



設定手順

1. AZ Control Center 左上の[**監査サーバー**]にサーバー名が表示されます。マウスで右クリックして[**ログイン**]を選択してください。ログイン ダイアログが表示されます。

2. 次のユーザーでログインします(パスワードのみ大文字小文字を区別します)。

   ユーザー名：admin

   パスワード：MASTER

   このユーザーは、Zen 本体とは直接関係しない Audit for Zen 自体の管理アカウントです。管理アカウントはログイン後に設定により変更可能です。

監視対象の指定

監視対象のデータを指定する場合、「**テーブル**」と「**Btrieve ファイル**」の 2 種類の設定方法があります。

テーブル

Actian Zen では、テーブル構造を表すスキーマは DDF と呼ばれるデータ ファイルとは別のファイル内に格納され、主に SQL で使用されています。

「**テーブル**」は DDF ファイルが存在するテーブル データに対して監査設定するための項目です。

スキーマを Audit for Zen に読み込むことによるメリットは、以下の 2 点です。

- データを人間が読みやすいように表示する
- 特定のフィールドの変更に基づいて警告を行える

詳細は追って説明しますが、スキーマがあれば、1 レコード内のどのフィールドがどう変化したか分かりやすくユーザーに表示することができます。

Btrieve ファイル

一方「**Btrieve ファイル**」は、DDF のないデータ ファイルに対して設定を行うための項目となります。

Actian Zen では、Btrieve API のみを使用すれば、必ずしも DDF を必要としません。
その場合、アプリケーションがレコード内のフィールド位置を管理しています。

このため SQL を使用してないアプリケーションでは DDF が作成されていない場合があります。

Btrieve API でアクセスしているファイルでも DDF を作成している場合は、「**テーブル**」を使用して設定を行ってください。

Room テーブルを監視する

それでは、監査対象として Demodata の Room テーブルを監視するよう設定していきましょう。

AZ Control Center 左下の[**監査の設定**]のエリアでこれらの設定を行います。

Demodata のスキーマをインポートする

Audit for Zen では最初にデータベースのスキーマをインポートする必要があります。

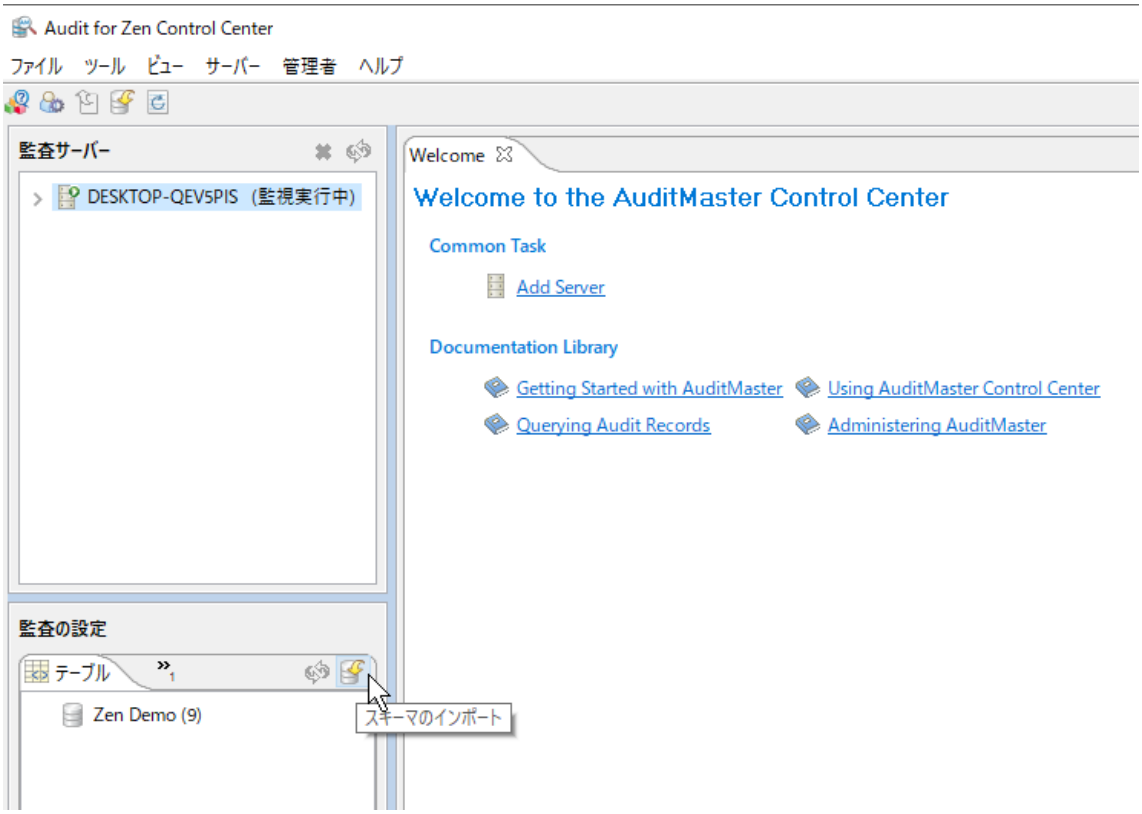
Audit for Zen は DDF ファイルを直接操作しません。最初に監視対象を設定するときに、既存のデータベース情報をインポートして、以降はその情報を元に各種設定を行っていきます。

> **注意：**
>
> **スキーマのインポート後にテーブルの構造を変更したような場合、再度スキーマをインポートし監視対象を再定義する必要があります。**

インストール直後は「Zen Demo(9)」というサンプル スキーマが定義されていますが、今回は最初から設定していくので無視してください。

設定手順

1. ［**スキーマのインポート**］アイコンをクリックしてください。



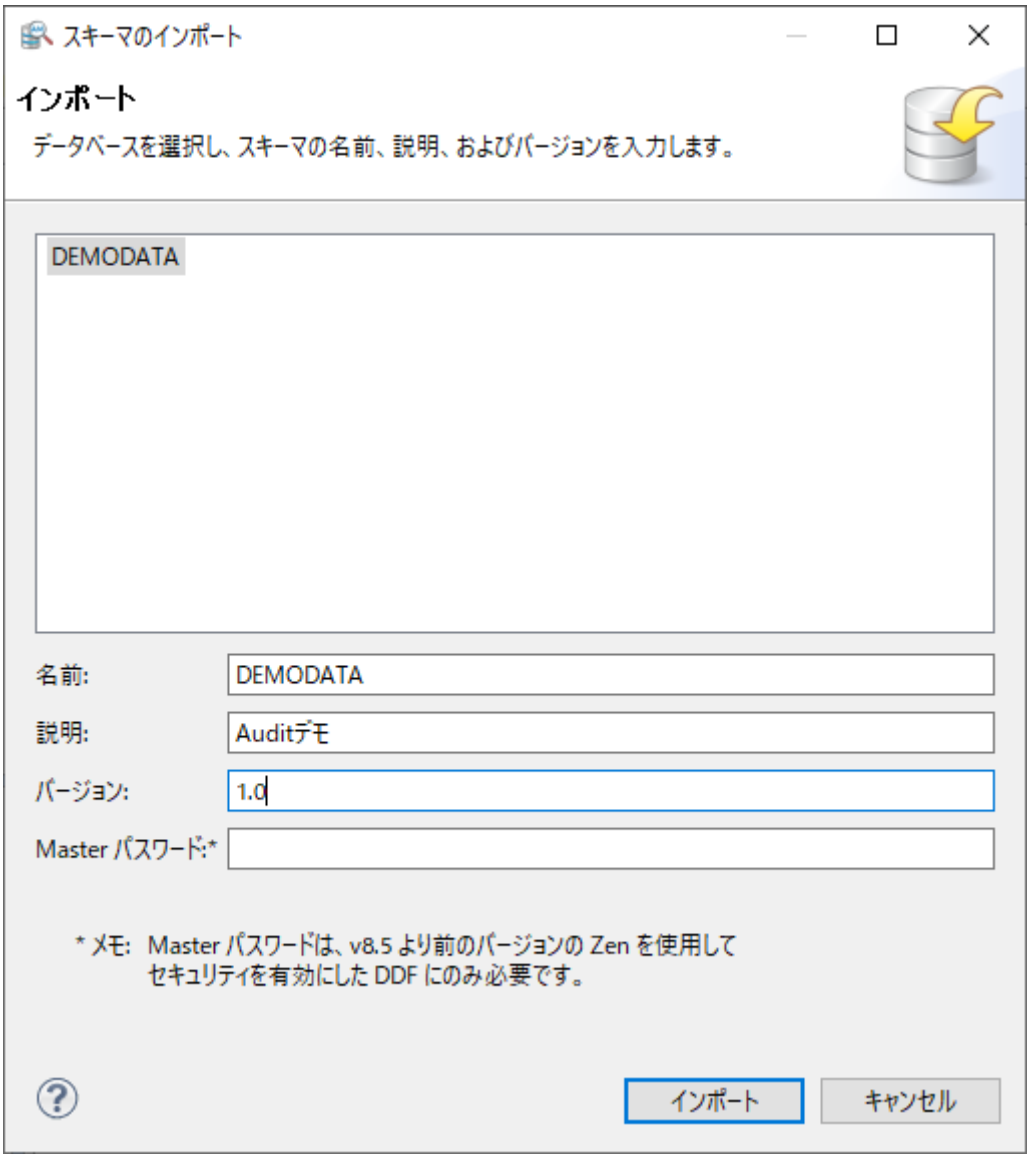
2. ［**スキーマのインポート**］ダイアログが開くので DEMODATA を選択し、次のように入力します。

説明：Audit デモ

バージョン：1.0

［Master パスワード］は何も入力しません。

［**バージョン番号**］は、Audit for Zen 管理者が自由に数値を設定して構いません。アプリケーションのリリース バージョンを特定したり、対象となる Btrieve ファイルのファイル形式を明示したりする用途でご利用ください。



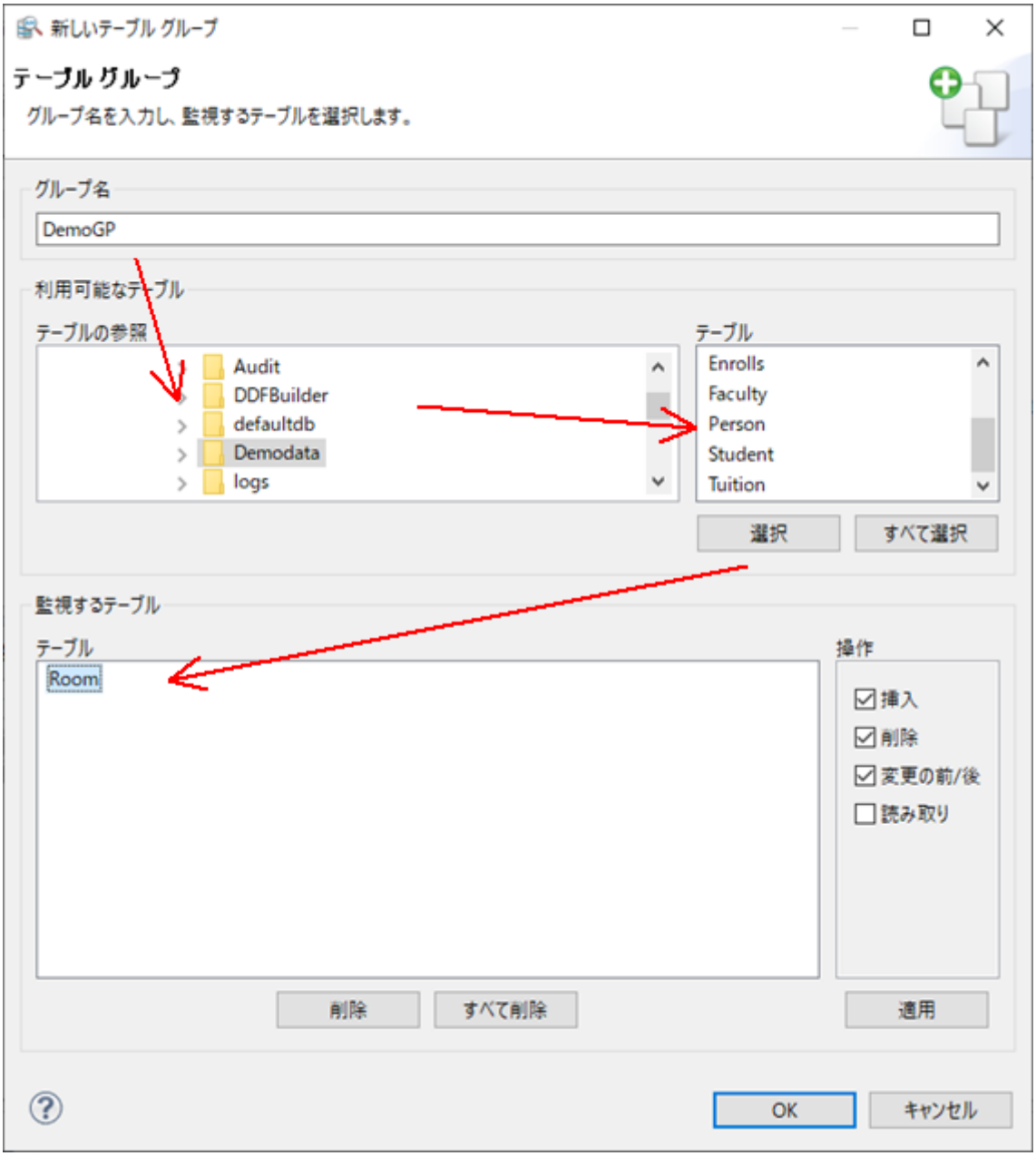
スキーマをインポートしたら、次に監視対象のテーブルをグループとして登録します。

3. 作成した DEMODATA を右クリックし、[**グループの追加**]を選択します。

   グループ名:DemoGP

   テーブルの参照:c:¥ProgramData¥Actian¥Zen¥Demodata

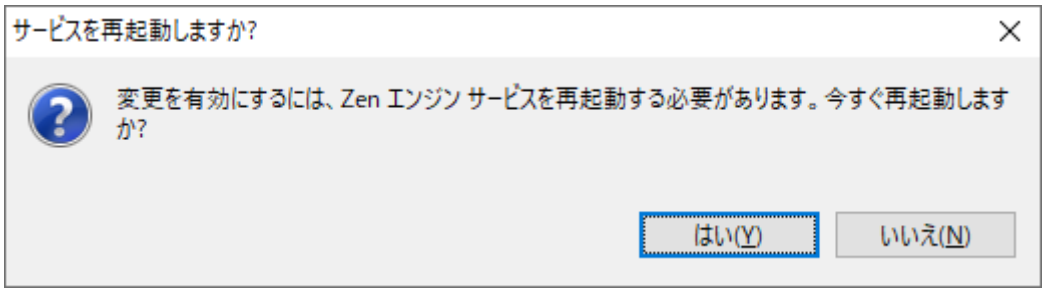
4. [**テーブル**]で "Room" を選択し、[**選択**]ボタンを押すと Room は画面下部の[**監視するテーブル**]に表示されます。



5. [**監視するテーブル**]内の "Room" を選択し、[**操作**]欄で監視する条件が指定されていることを確認します。デフォルトでは[**挿入**]、[**削除**]、[**変更の前/後**]が選択されています。

6. [OK]を押して設定を確定します。

監視の設定をした後、ログ イベントハンドラーに設定情報を反映するため Zen エンジンの再起動が必要になります。再起動を指示するメッセージが表示されるので、指示に従って Zen のエンジンを再起動します。



（AZ Control Center が **"管理者として実行"** で起動されていない場合、エンジンの停止と起動のそれぞれに管理者昇格の確認が表示されます。）

以上で、Room テーブルに対するレコードの作成、削除、変更は、監査ログに記録されるようになりました。

監査ログの確認

それでは、実際に Room テーブルにレコードの作成、削除、変更を行って、監査ログが記録されている様子を確認してみましょう。

作業手順

1. Zen Control Center を起動し、次の SQL を実行します。

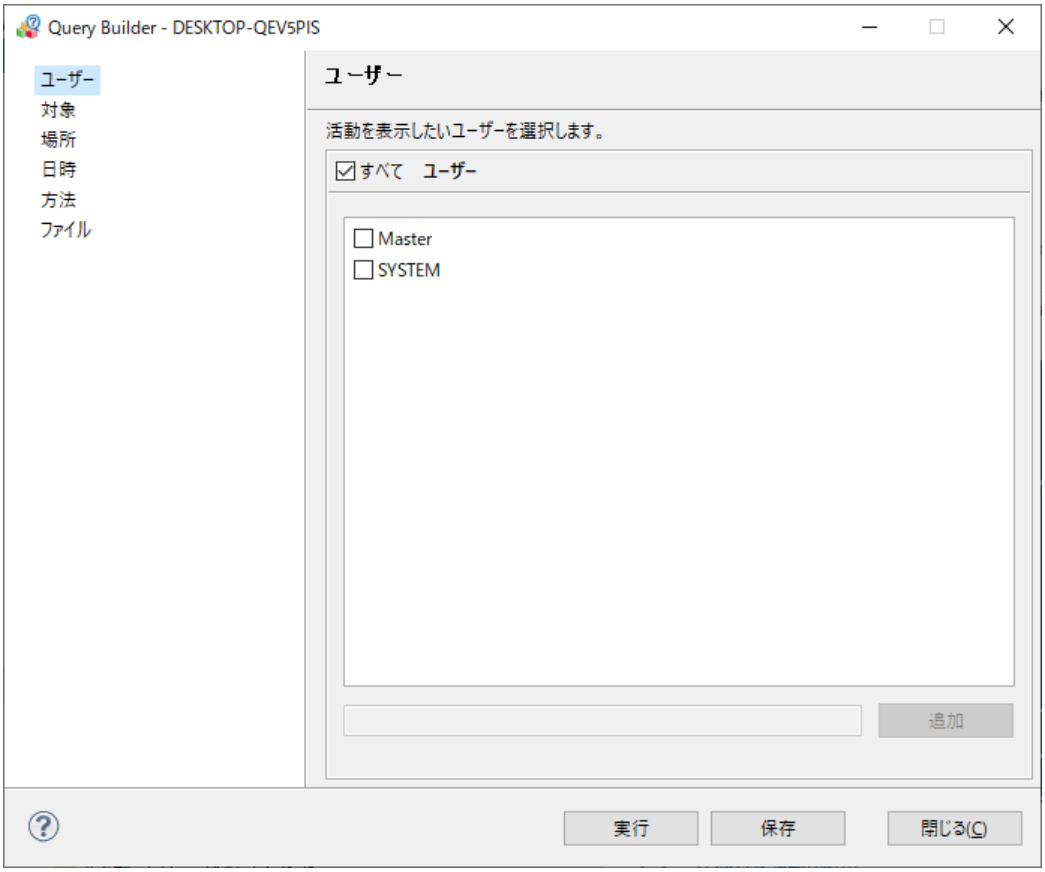
```
INSERT INTO Room VALUES('Zen ビルディング',1111,2222,'管理室');
UPDATE ROOM SET Number = 2011 where Building_Name = 'Roscart Building' and Number = 201;
DELETE ROOM where Building_Name = 'Roscart Building' and Number = 205;
```

   これらの変更は、監査ログファイル（C:¥ProgramData¥Actian¥Zen¥Audit¥DATA¥amview）に保存されます。

   Audit for Zen で監査データを表示するには、この保存されたデータに対して指定条件による絞り込みを行い、結果を「現在のビューファイル」に表示させます。

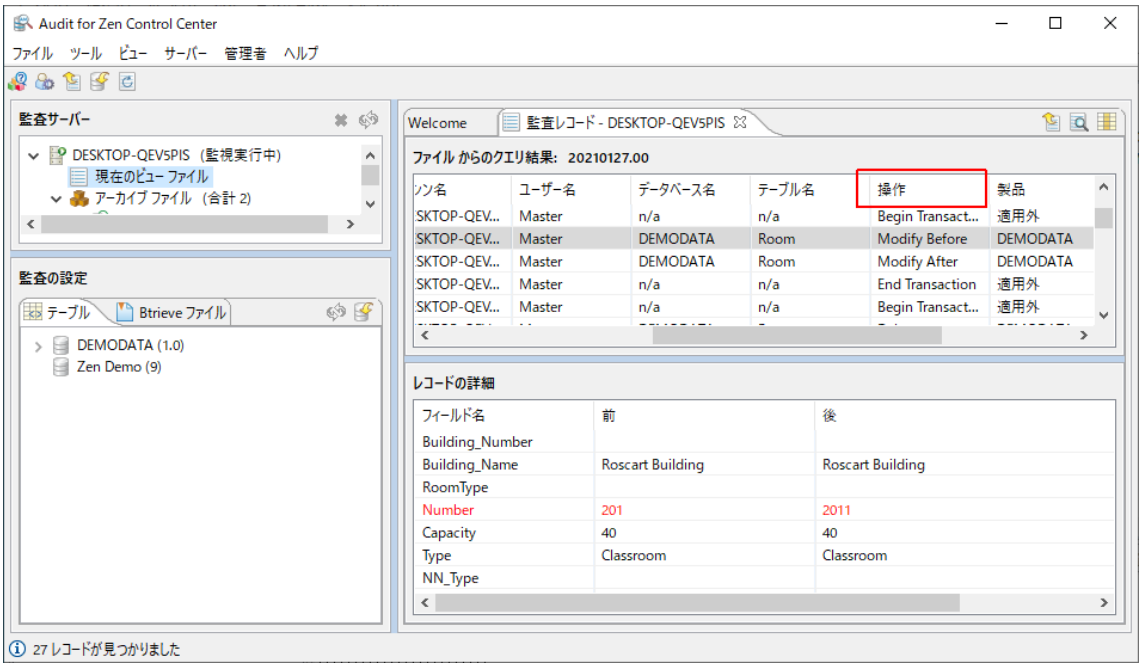
2. AZ Control Center を起動して、再度 admin/MASTER でログインしてください。

3. ［現在のビューファイル］を選択した状態でメニューから［**ファイル**］＞［**クエリ...**］を実行すると、クエリ ビルダが起動します（ダブルクリックでも可）。このツールで、抽出するデータ範囲を制限します。ここでは、特に何も制限を加えず［**実行**］ボタンを押します。

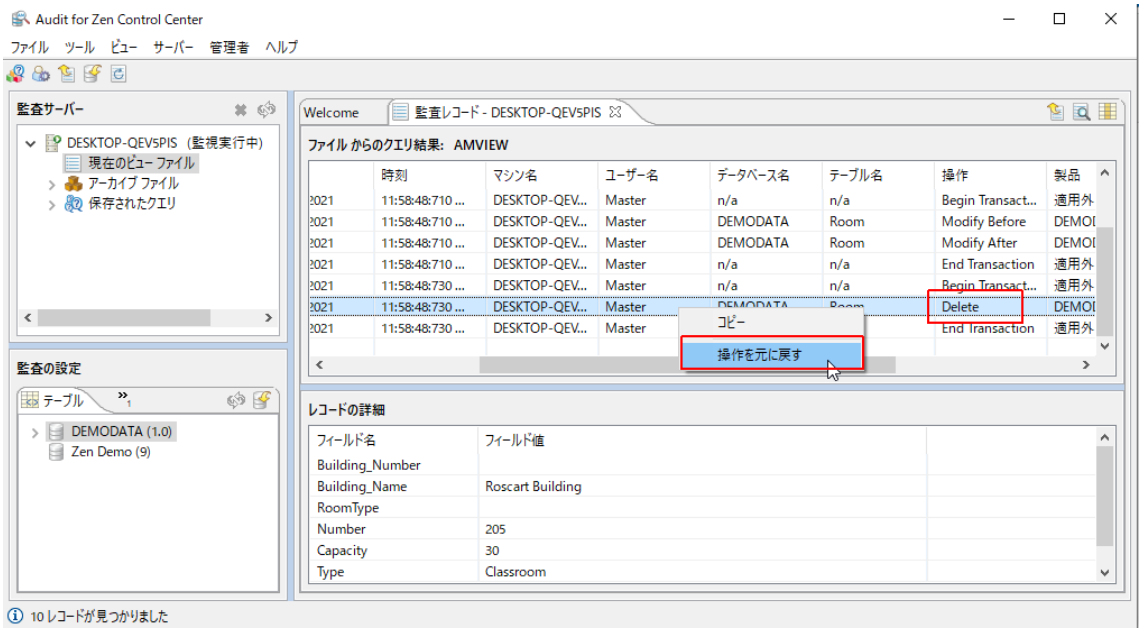


Room テーブルは監視対象に設定しているので、先ほど SQL で操作した内容は監査記録として保管されています。

4. グリッド表示内の[**操作**]列の中で Insert, Delete, Modify Before / Modify After の各レコードを確認してください。

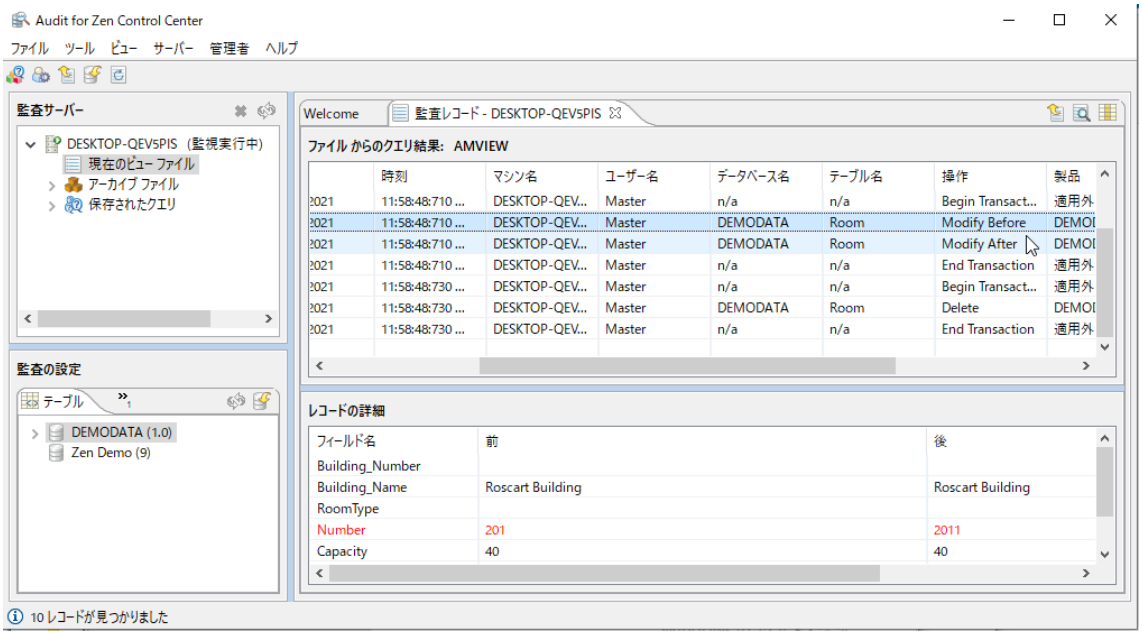


監査結果よりデータを元の状態に戻すことも可能です。



5. Delete が記録されているオペレーション行を右クリックして、[**操作を元に戻す**]を実行してください。確認ダイアログで[**はい**]ボタンをクリックすれば、削除したレコードが復活します(削除した内容が Insert で再作成されます)。

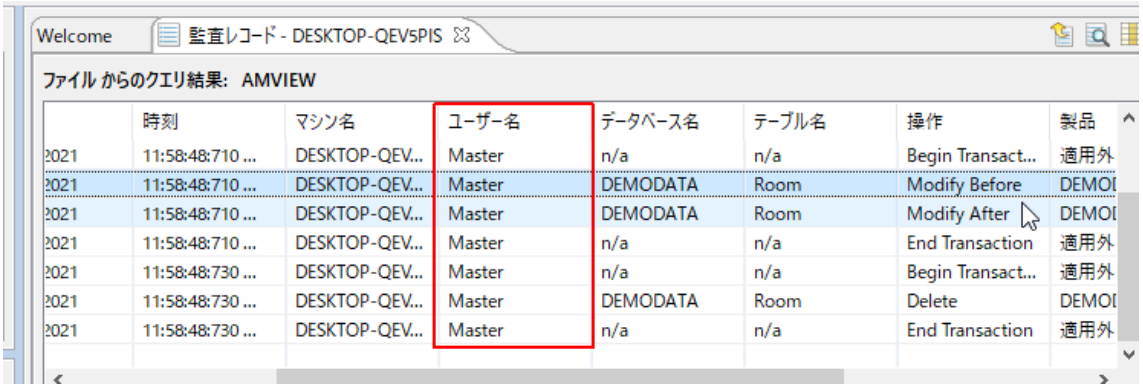
値の変更は "Modify Before"、"Modify After" として記録されています。



変更の場合、元のデータと変更後の 2 種類のデータを保存するため、2 つのオペレーションが記録されていますが、グリッドの表示は両者を組み合わせて表示します。[**操作を元に戻す**]処理はどちらのレコードに対して実行しても有効です。

データベースにユーザーを登録して確認

サンプル データベース DEMODATA にはユーザー権限の設定が特に行われていないため、Audit for Zen の［**ユーザー名**］欄には Zen のデータベース管理者アカウントである「Master」がデータを操作したユーザーとして表示されていました。



	時刻	マシン名	ユーザー名	データベース名	テーブル名	操作	製品
2021	11:58:48:710 ...	DESKTOP-QEV...	Master	n/a	n/a	Begin Transact...	適用外
2021	11:58:48:710 ...	DESKTOP-QEV...	Master	DEMODATA	Room	Modify Before	DEMOI
2021	11:58:48:710 ...	DESKTOP-QEV...	Master	DEMODATA	Room	Modify After	DEMOI
2021	11:58:48:710 ...	DESKTOP-QEV...	Master	n/a	n/a	End Transaction	適用外
2021	11:58:48:730 ...	DESKTOP-QEV...	Master	n/a	n/a	Begin Transact...	適用外
2021	11:58:48:730 ...	DESKTOP-QEV...	Master	DEMODATA	Room	Delete	DEMOI
2021	11:58:48:730 ...	DESKTOP-QEV...	Master	n/a	n/a	End Transaction	適用外

今回は DEMODATA にユーザーを新規に定義して、テーブルを変更したユーザーの名前が記録される様子を確認してみましょう。

DEMODATA へのユーザー追加

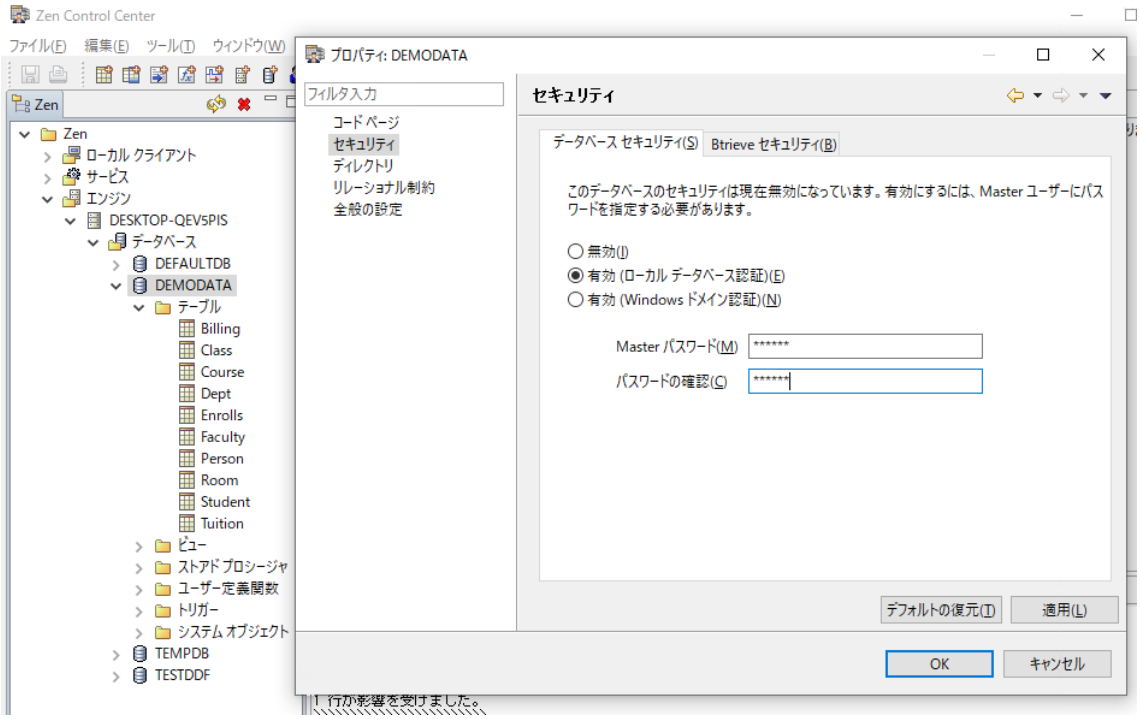
Zen データベースでユーザーを管理するには、データベースのセキュリティ機能を有効にする必要があります。

1. Zen Control Centerを起動しDEMODATAのプロパティを開き、[**セキュリティ**]設定内の[**データベース セキュリティ**]タブを選択し、データベース セキュリティを有効にします。

   ここでは、

   - [**有効(ローカル データベース認証)**]オプションを選択
   - [**Master のパスワード**]:MASTER

   とします。



Master ユーザーは該当データベースへのフルアクセス権限を持った管理者です。Master ユーザーのパスワード設定は対象のデータベースごとに個別に設定する必要があります。

ここではDEMODATAに対して設定しますが、他のデータベースにセキュリティが必要な場合は、それぞれのデータベースで同様の作業を行います。

なお、Zen のセキュリティ モデルには、以下の 2 種類があります。

- **ローカル データベース**
- Windows **ドメイン**

Windows **ドメイン**の場合、各ユーザー単位の権限は設定できず、**グループ**または PUBLIC（全ユーザーに適用されるデフォルトの権限）の権限のみが指定できます。

各ユーザーに権限を割り当てたい場合には、セキュリティ モデルとして **"ローカル データベース"** を選択してください。

2. 次に［Btrieve **セキュリティ**］タブをクリックし、次のオプションを選択してください。

- **データベース（DB 認証及び許可）**

これで、データベースに対してセキュリティが有効になりました。

Zen では Audit for Zen とは異なりユーザー、パスワード共に大文字小文字を区別します。

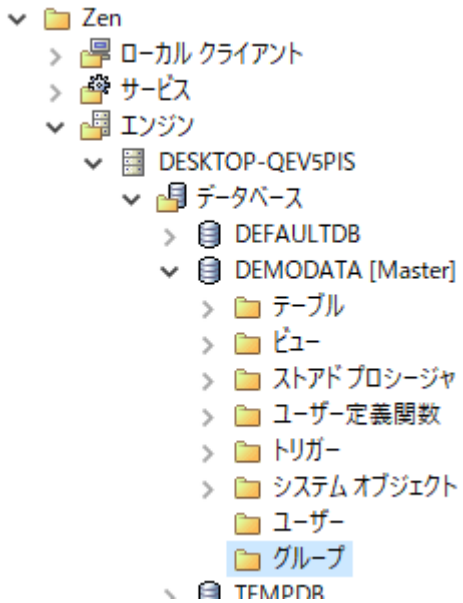
今後 Zen Control Center で DEMODATA を設定・管理する場合、ここで設定した

ユーザー名：Master

パスワード：MASTER

でログインしてください。

セキュリティ設定後、DEMODATA にログインする**ユーザー**、**グループ**の項目が DEMODATA 内に表示されます。



ユーザーは特定のグループに所属する必要はありませんが、グループに所属している場合、個人の権限は持てません。また、ユーザーは複数のグループに所属することはできません（PUBLIC は例外で、全員が PUBLIC にも所属しているとみなされます）。

今回はユーザーを DEMODATA に新規に登録します。

作業手順

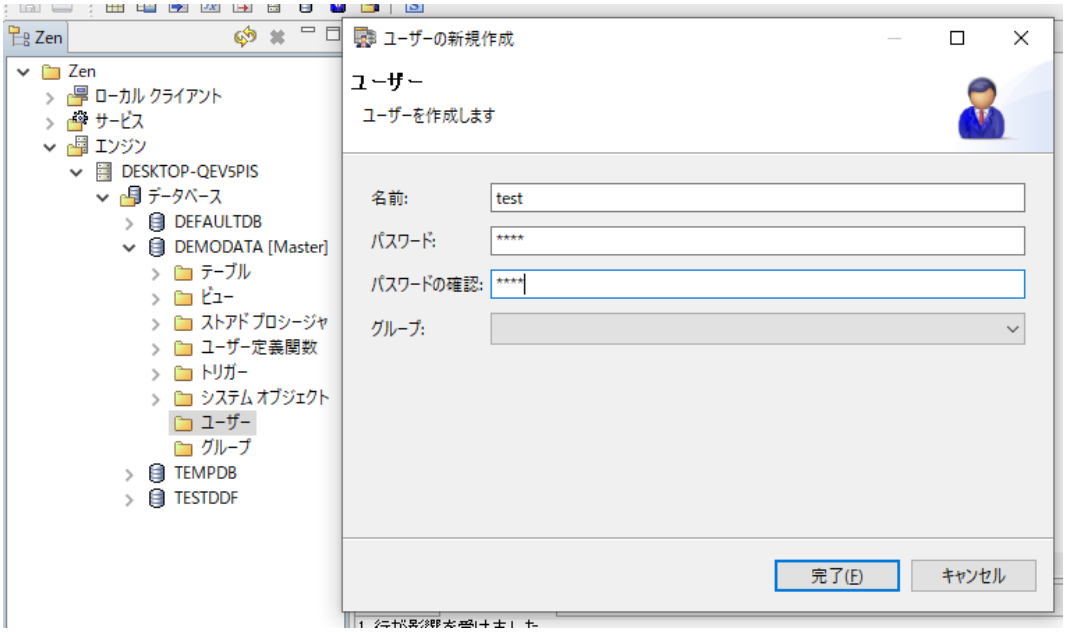
1. Zen Control Center のツリーで、DEMODATA の**ユーザー**を右クリックして[**新規作成**]＞[**ユーザー**]を選んでください。

2. 表示されたダイアログで次のユーザー、パスワードを入力します。

   ユーザー名：test

   パスワード：test

3. [**完了**]ボタンをクリックします。



次に作成したユーザーに権限を設定します。

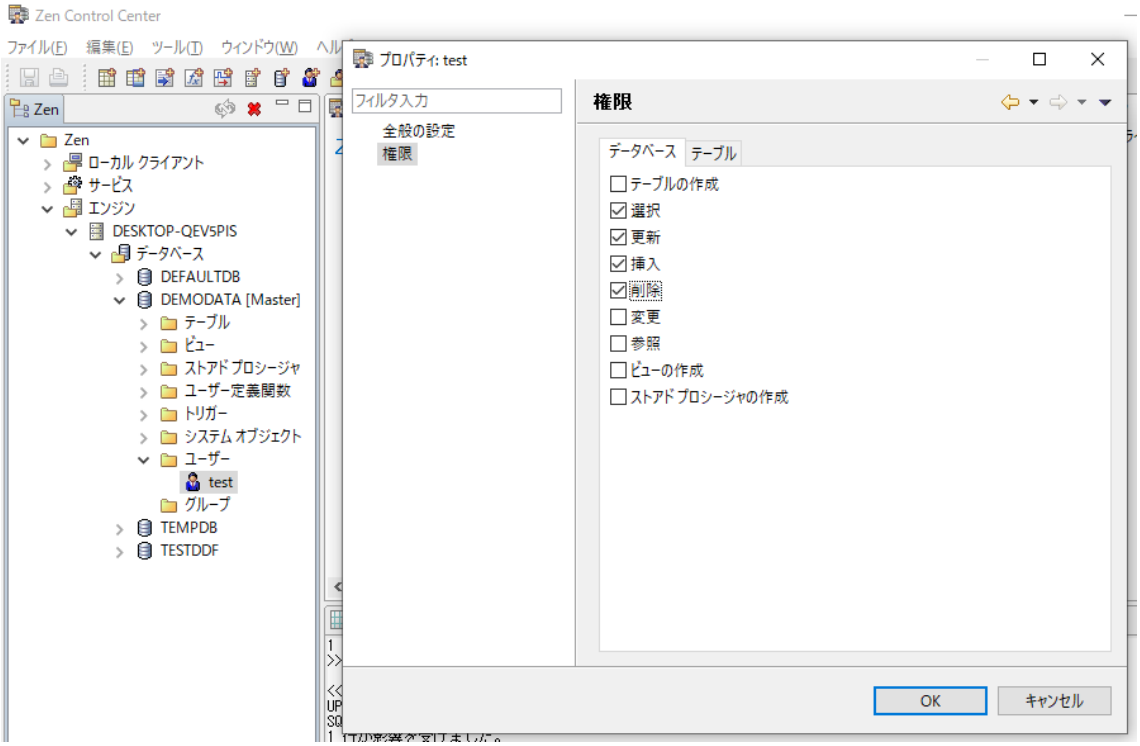
作業手順

1. ツリーに表示されるユーザー test をダブルクリックします。

2. データベースに対する権限として次の項目のチェックをオンにします。

   ・選択
   ・更新
   ・挿入
   ・削除

3. [OK]ボタンをクリックして権限設定を完了します。



ユーザー操作による監査データの確認

Zen Control Centerを一度ログアウトし、testユーザーでDEMODATAにログインしテーブルを変更します。

作業手順

1. ツリー内の DEMODATA を右クリック、[**ログアウト MASTER**]を選択します。
2. 再度 DEMODATA を右クリック、[**ログイン...**]を選択します。
3. ユーザー test、パスワード test でログインします。
4. 次の SQL でテーブルを変更します。

```
INSERT INTO Room VALUES('Actian ビルジング',3333,4444,'購買部');
UPDATE ROOM SET Number = 1103 where Building_Name = 'Vander Stoep Hall' and Number = 110;
DELETE ROOM where Building_Name = 'Vander Stoep Hall' and Number = 115;
```

AZ Control Centerに戻って、一連の変更内容がtestユーザーの操作として記録されているか監査ログの確認をしてみてください。

Btrieve API によるアクセスの監査記録を取得

今までの監査確認は、SQL によるデータベース アクセスに対して確認しました。今回は、Btrieve API を使用したアクセスに対して監査データを確認していきます。

Zen Function Executor を起動して Room.mkd を Btrieve ファイルとして直接書き換えた場合、データベースは DefaultDB、ユーザーは OS のログイン ユーザーとして記録されます。

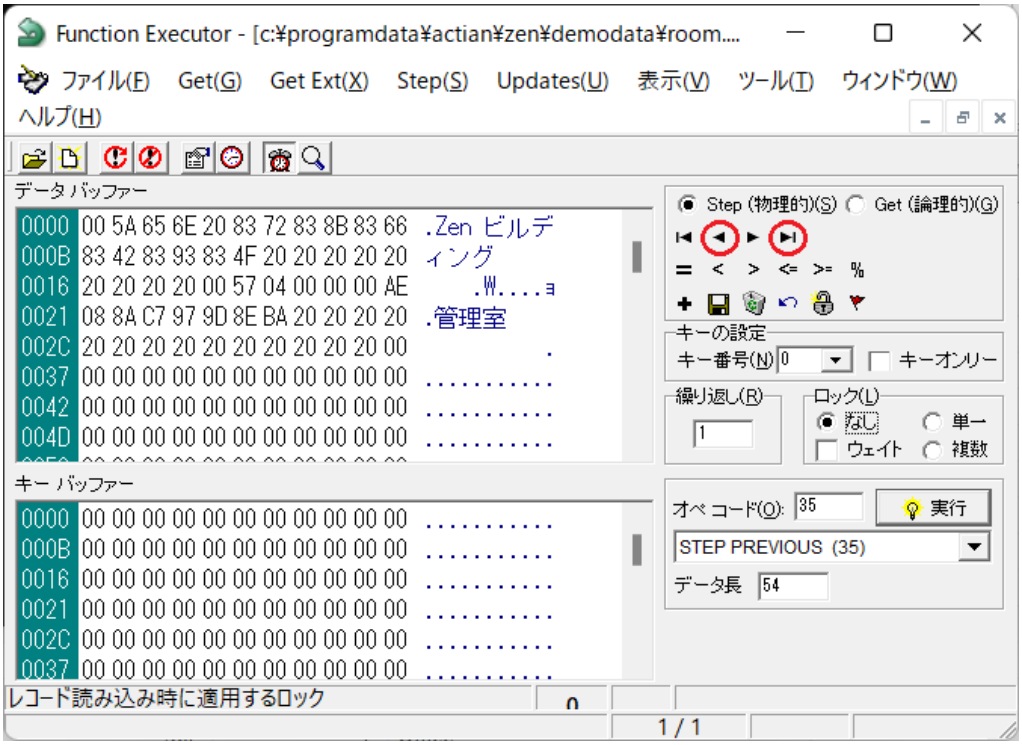
このドキュメントの最初に、MASTER ユーザーとして Room テーブルへ「Zen ビルディング」の値を持つレコードを追加しました。このレコードを Btrieve API レベルで削除して、どのような結果が監査データとして記録されるか確認してみます。

作業手順

1. Zen Function Executor を起動します。
2. C:¥ProgramData¥Actian¥Zen¥Demodata¥Room.mkd を開きます。
   （C:¥ProgramData は隠しフォルダーとなっています。アクセスするにはエクスプローラーの表示設定で隠しファイルのチェックをオフにするか、入力ボックスに直接パスを入力してください。）

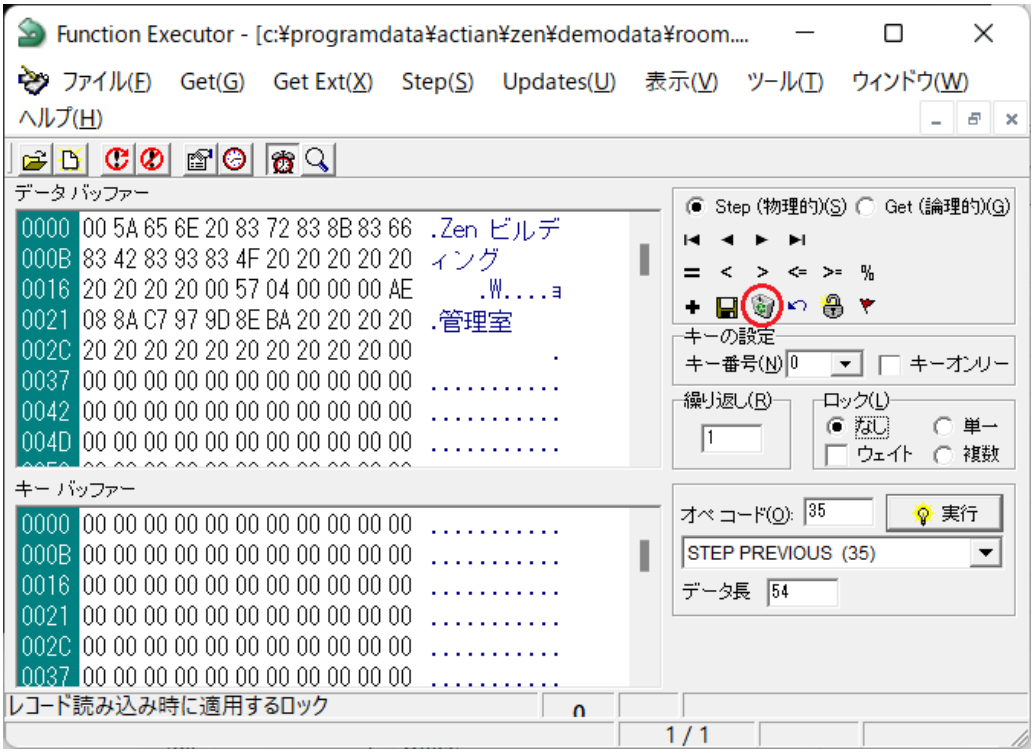
3. 「Zen ビルディング」が記録されているレコードを探します。

（下図の赤丸で示したアイコン（STEP LAST）とその後（STEP PREVIOUS）で探すとすぐに見つかります。）



4. DELETE オペレーションを実行します。

（下図の赤丸で示したごみ箱アイコンが DELETE になります。）



5. Function Executor を終了します。

これで該当のレコードが削除されました。

AZ Control Center に戻って、一連の削除操作が記録されているか確認してください。

またその際、以下の点に注意し、確認してください。

- どのユーザーがレコードを削除したことになっているか
- Room テーブルの所属データベースが何になっているか

DDF の無い Btrieve ファイルの場合

これまでの操作ではスキーマが最初から定義されている DEMODATA データベースのファイルを使用してきました。

ここではスキーマが定義されていない Btrieve ファイルの監視方法を説明します。

事前準備

最初にテスト用に Btrieve ファイルが単独で存在する状況を作ります。

1. コマンドプロンプトで次のコマンドを実行して c:¥testAudit フォルダーに Room.mkd のコピーを用意します。その際ファイル名も「Test.mkd」と変更します。

```
mkdir c:¥testAudit
copy C:¥ProgramData¥Actian¥Zen¥Demodata¥Room.mkd  c:¥testAudit¥Test.mkd
```

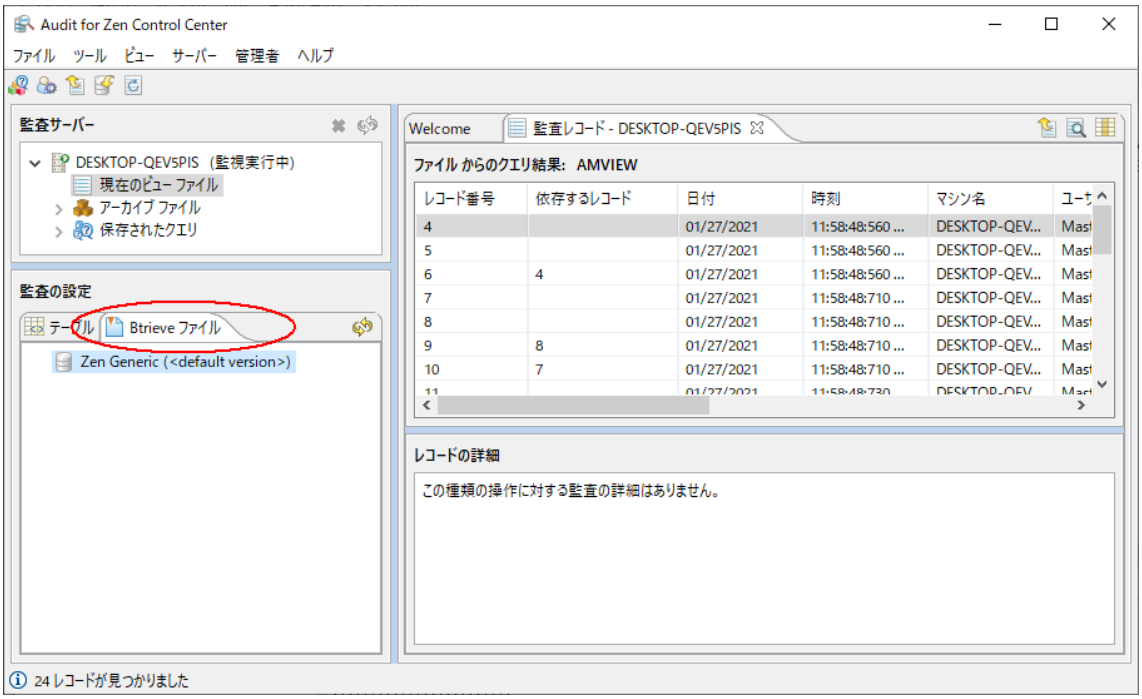
DDF の無いファイルへの監査条件設定

Test.mkd ファイルを監視するために、Audit for Zen の設定を行っていきましょう。

作業手順

1. AZ Control Center を起動し、ユーザー admin、パスワード MASTER でログインします。

   今回は、DDF がない Btrieve ファイルを扱うため、Audit for Zen 左下の[**監査の設定**]では[**Btrieve ファイル**]のタブを選択してください。



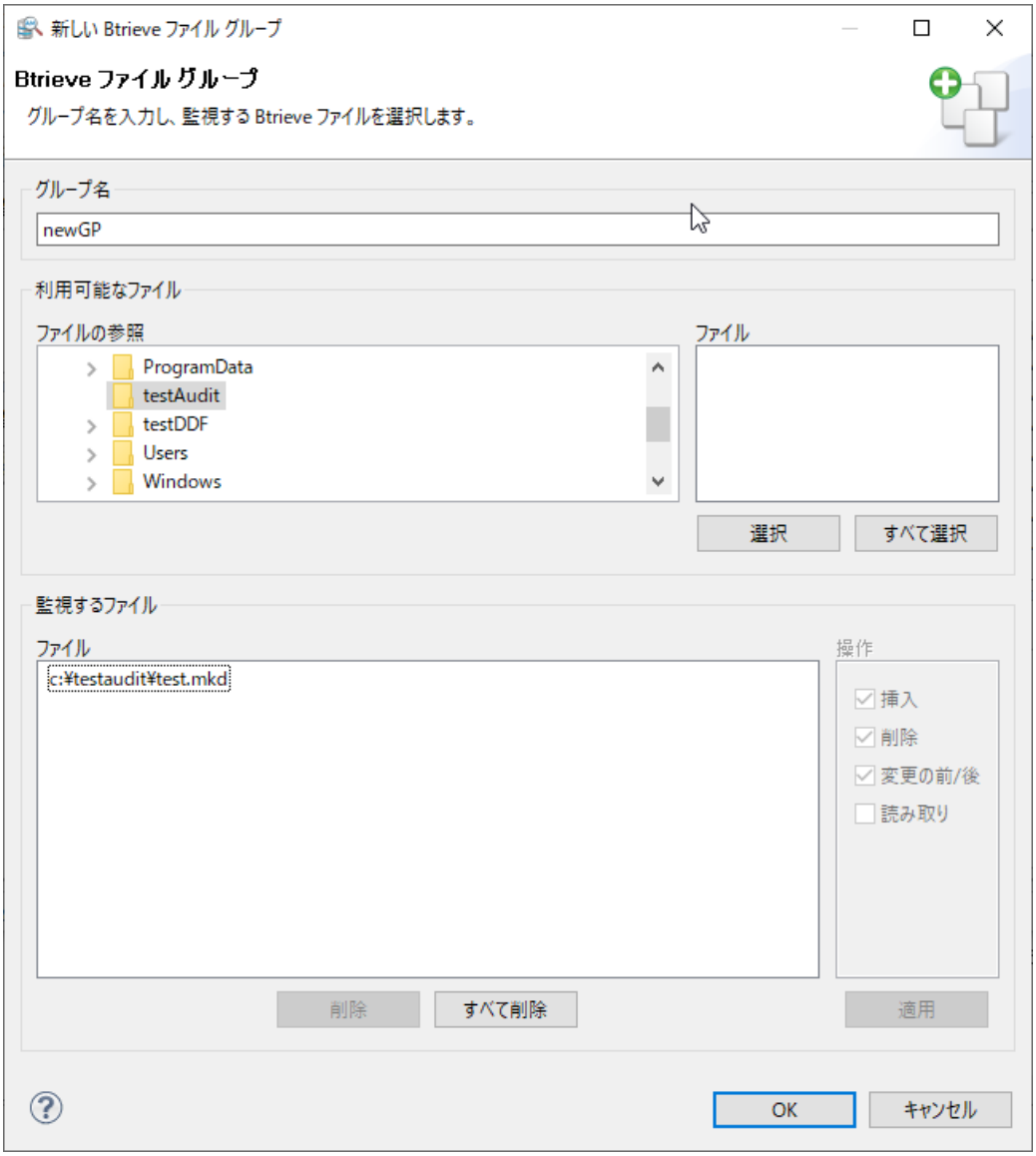
2. [Zen Generic (<default version>)]を選択し、マウス右クリックで[**グループの追加**]を選択します。

3. 次のグループ情報を入力します。

   グループ名：newGP

   ファイルの参照：c:¥testAudit

4. ［**ファイル**］で "test.mkd" を選択し、［**選択**］ボタンを押すと［**監視するファイル**］にファイルが登録されます。



5. 監視する操作が［**挿入**］、［**削除**］、［**変更の前/後**］であることを確認して［OK］を押します。

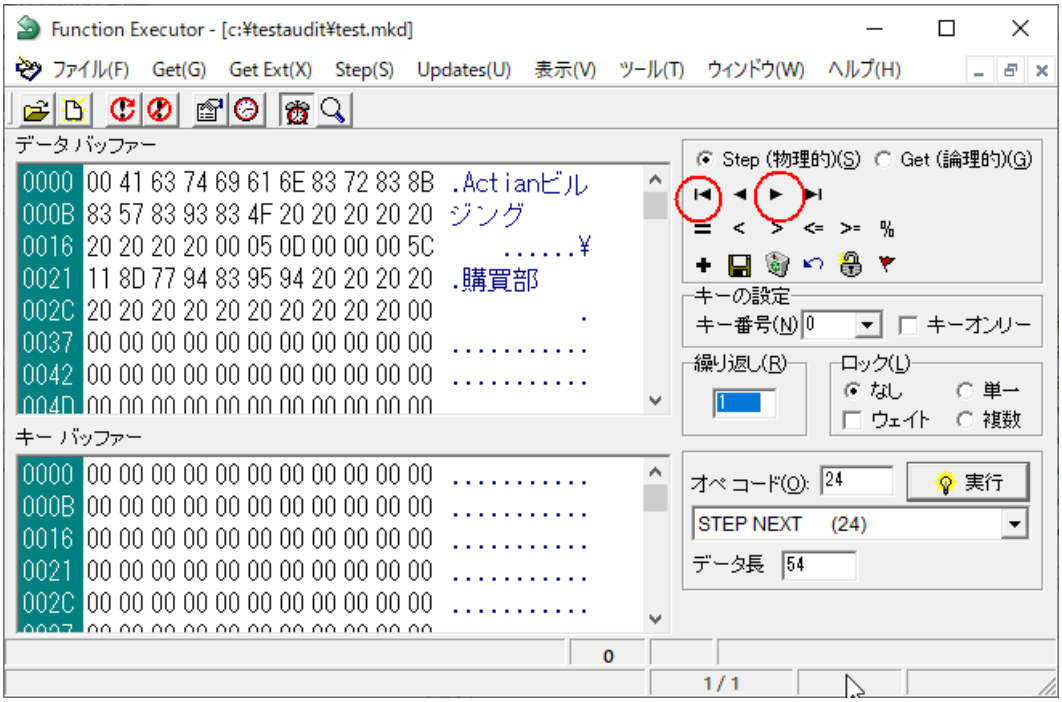
6. メッセージに従い、Zen エンジンを再起動します。

DDF の無いファイルの変更と監査情報の確認

先の作業で変更した「Actianビルジング」のレコードを探し「ACTIANビルジング」に書き換えます。

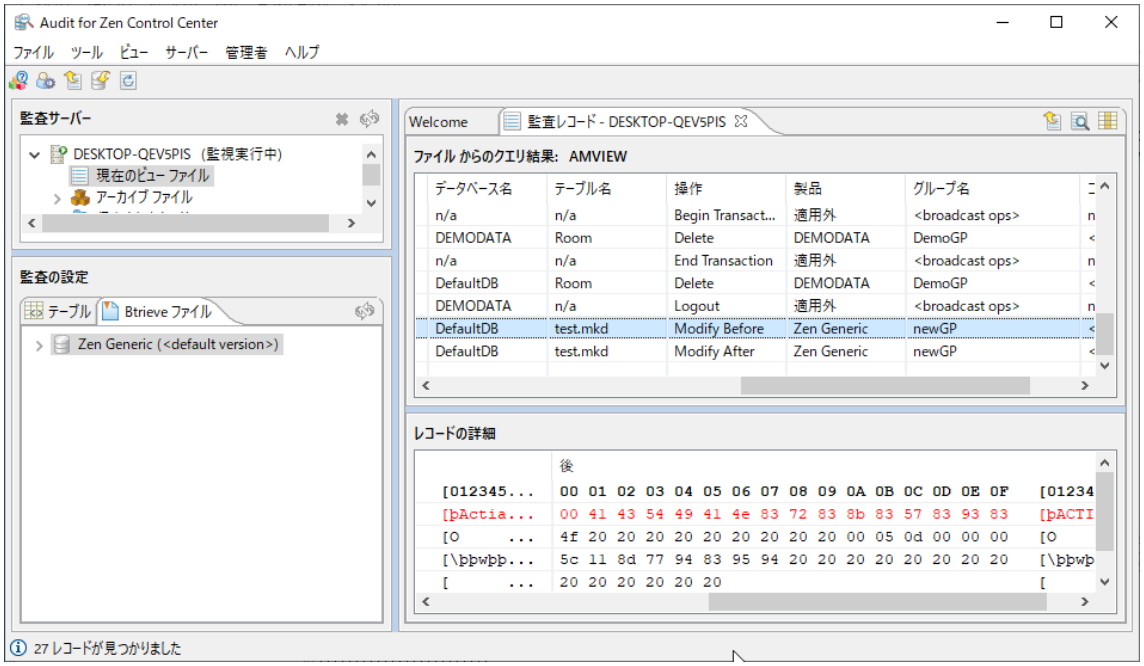
作業手順

1. Function Executor を起動し、c:¥testAudit¥Test.mkd を開きます。
2. Step First / Step Next（下図の赤丸で示したアイコン）を使って、「Actian ビルジング」のレコードを見つけます。



3. 文字列「Actian」の先頭をマウスでクリックし、「ACTIAN」と入力し直します。
4. フロッピー アイコン（UPDATE）をクリックし、書き換え内容を保存します。
5. Function Executor を終了します。
6. Audit for Zen で「現在のビューファイル」を［**クエリ…**］で更新します。

[製品]列が "Zen Generic"、[操作]列が "Modify Before" または "Modify After" のレコードを探し、監査データの内容を確認してください。



次にようになっているはずです。

[ユーザー名]列:OS のユーザー名

[データベース名]列:DefaultDB

[グループ名]列:newGP

また、DDF が定義されている場合と異なり、変更があった部分はバイナリ データとして表示されるので、詳しい内容は一目では判断ができない状態になっていることが確認できます。

先に確認したように、Btrieve ファイルであっても DDF がある場合、「テーブル」を使って監査設定すれば、より詳細な情報を得ることができます。

DDF が存在しない Btrieve ファイルの場合も、DDF Builder を使用すればテーブル スキーマの定義が可能です。

より詳細に監査データを確認できるよう、DDF を作成してから監査記録を取得することをお勧めします。

以上で Audit for Zen の基本的な操作説明は終わりです。

お疲れ様でした。

なお一部、説明を省略した箇所もありますので、以下に補足として記載をしてあります。

また、より詳しい Audit for Zen の利用法につきましては、製品のマニュアルをご参照ください。

補足

DefaultDB について

「デフォルトのデータベース」（DefaultDB）とは、Btrieve ファイルに対して強化されたセキュリティモデルをサポートするために追加されたシステム データベースです。

従来の Btrieve ファイルはデータ ファイル単独で扱うことができ、OS のファイル アクセス権を利用したセキュリティを使用していました。つまりデータベースが独自に管理するアクセス権は持っていない状況でした。

このため、既存の Btrieve ファイルに対して互換性を維持したまま新しいセキュリティ モデルを導入にするために、「デフォルトのデータベース」という概念が導入されました。これが「DefaultDB」です。

特にセキュリティを設定していない場合も、DefaultDB はグローバルに有効になっておりその設定が適用されます。

Btrieve アクセスは DDF を必ずしも必要としないため、DDF の無い Btrieve ファイルのセキュリティ設定は DefaultDB の設定が反映されます。

その他、データベース名の明示的な指定が無い場合も DefaultDB の設定が使用されます。

DefaultDB は Audit for Zen の内部 DB としても使用されています。

amserver ファイル

Zen のデータベース ファイルで Audit for Zen が接続情報の管理で使用しているファイルで、監査レコード情報、ユーザー情報、設定情報はこのファイルに保存されています。

デフォルトでは C:¥ProgramData¥Actian¥Zen¥Audit¥data フォルダー内に存在していますが、このファイルの場所は設定で変更が可能です。

AZ Control Center に登録されているサーバーを削除しても、本ファイルが削除されていなければ再度登録し直すことができます。またデータもそのまま残っています。