Actian Zen のセキュリティ

株式会社エージーテック

2020 年 3 月 23 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 Zen のセキュリティ
最終更新：2020 年 3 月 23 日

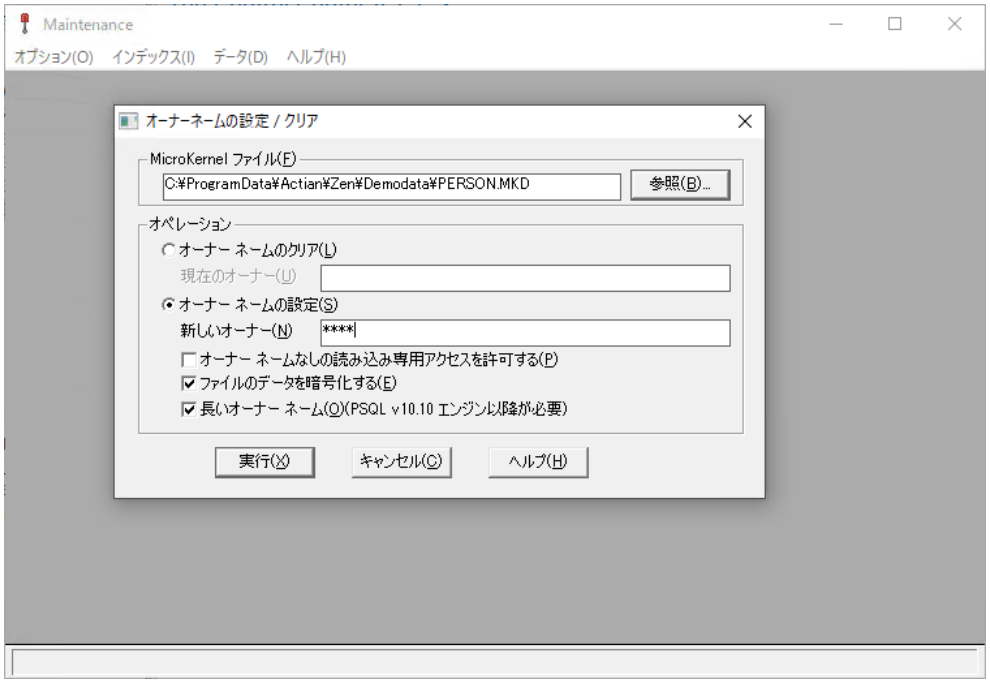
Actian Zen（PSQL）には、次のようなセキュリティ機能があり、重要なデータを保護することが可能です。

- ファイルの暗号化
- ネットワークの暗号化
- データベース URI 使用による、ファイルパスの隠蔽
- アクセス権

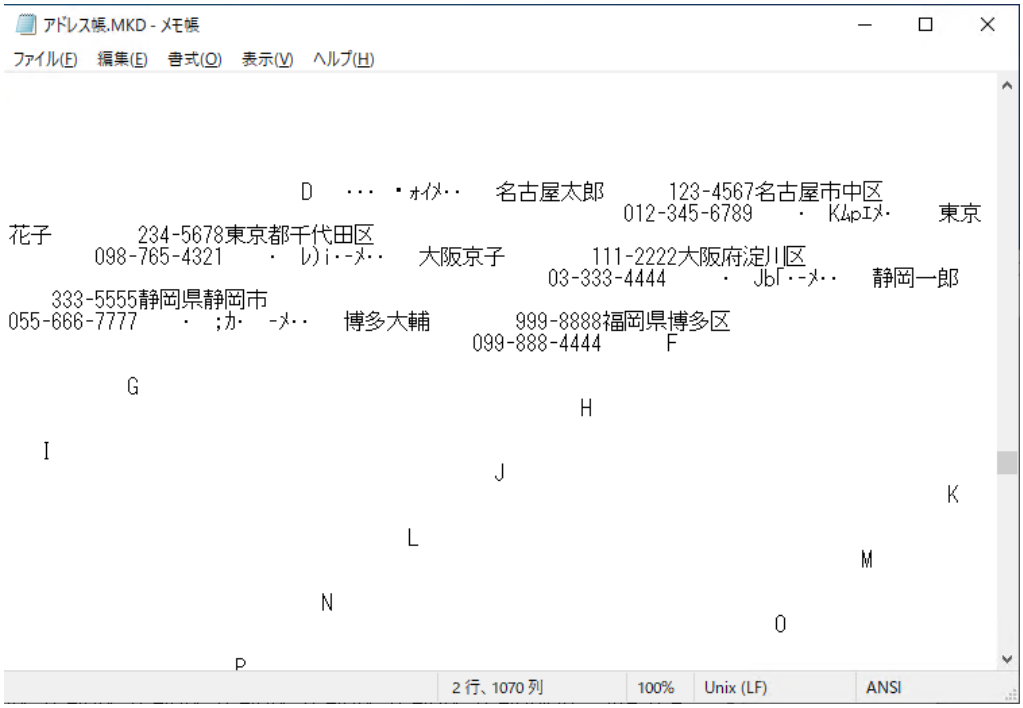
1. ファイルの暗号化

Btrieve ファイルには、オーナーネームと呼ばれるパスワードのようなものを設定する機能があります。
オーナーネームが設定されていると、OPEN を行う際にオーナーネームを指定しないと、OPEN に失敗します。（設定により、読み込みでは指定不要にできます）
また、オーナーネームを指定する際、オプションで暗号化を指定可能です。
オーナーネームには、短いオーナーネームと長いオーナーネームがあり、暗号化の強度が異なります。（長いオーナーネームを設定することで、暗号化強度は強くなります）

オーナーネームは、Maintenance ユーティリティで簡単に設定可能です。
［オプション］－＞［オーナーネームの設定/クリア］をクリックし、表示されるダイアログでオーナーネームを設定するファイルを指定し、「オーナーネームの設定」を選択します。
「ファイルのデータを暗号化する」をチェックして実行することで、暗号化が行われます。
ファイルのサイズによっては、暗号化に時間がかかります。
また、オーナーネームは開発元でも調べることはできません。
忘れてしまうと、アクセスできなくなりますので、十分にご注意ください。



暗号化を行うことで、エディターで Btrieve ファイルを開いたとき、データを見ることができなくなります。
暗号化を行わない場合、メモ帳等のエディターで Btrieve ファイルを開くことで、データが見えてしまいます。



これに対し、暗号化を行うことで、メモ帳等で開いても、データを見ることはできなくなります。

※Btrieve ファイルをエディターで開く場合、破損の恐れがありますので、必ずバックアップを行ってください。

暗号化（オーナーネームを設定した）ファイルにアクセスする場合、Btrieve API ではデータバッファにオーナーネームを指定します。
（OPEN の際に指定します。他のオペレーションでは不要です。）
他には暗号化を意識する必要はありません。
オーナーネームには、以前からのオーナーネームと、PSQL v10 SP1 からの長いオーナーネームの 2 種類があります。
以前からのオーナーネームでは、簡易な暗号化となります。
長いオーナーネームでは、より強力な暗号化となります。
エンジンのバージョンやファイル形式等で暗号強度が変わります。
ファイル形式が 9.5 形式では、128 ビット暗号化を使用します。
ファイル形式が 13 形式で、かつオーナーネームが 24 バイトまででは、AES-192 暗号化を使用します。
ファイル形式が 13 形式で、かつオーナーネームが 24 バイトより長い場合は、AES-256 暗号化を使用します。

SQL でアクセスする際には、セッション毎に SET OWNER ステートメントでオーナーネームを指定してからテーブルにアクセスします。
後述のセキュリティを設定している場合、ログオンするユーザー毎に予めオーナーネームを設定しておくことができます。
この設定は、GRANT ステートメントで行います。

---メモ---
GRANT ステートメントでのオーナーネーム設定は、ユーザーまたはグループ毎に 1 回行います。

例：GRANT ALL ON Person 'オーナーネーム' TO Master

この例では、Person テーブルの全ての操作に対し Master ユーザーにオーナーネームを設定します。
テーブル事にオーナーネームが異なる場合、GRANT ステートメントを複数回実行します。
Zen エンジンは、複数の設定されたオーナーネームで OPEN を試行します。

暗号化（オーナーネームの設定）は、いつでも Maintenance ユーティリティで行えます。

2. ネットワークの暗号化

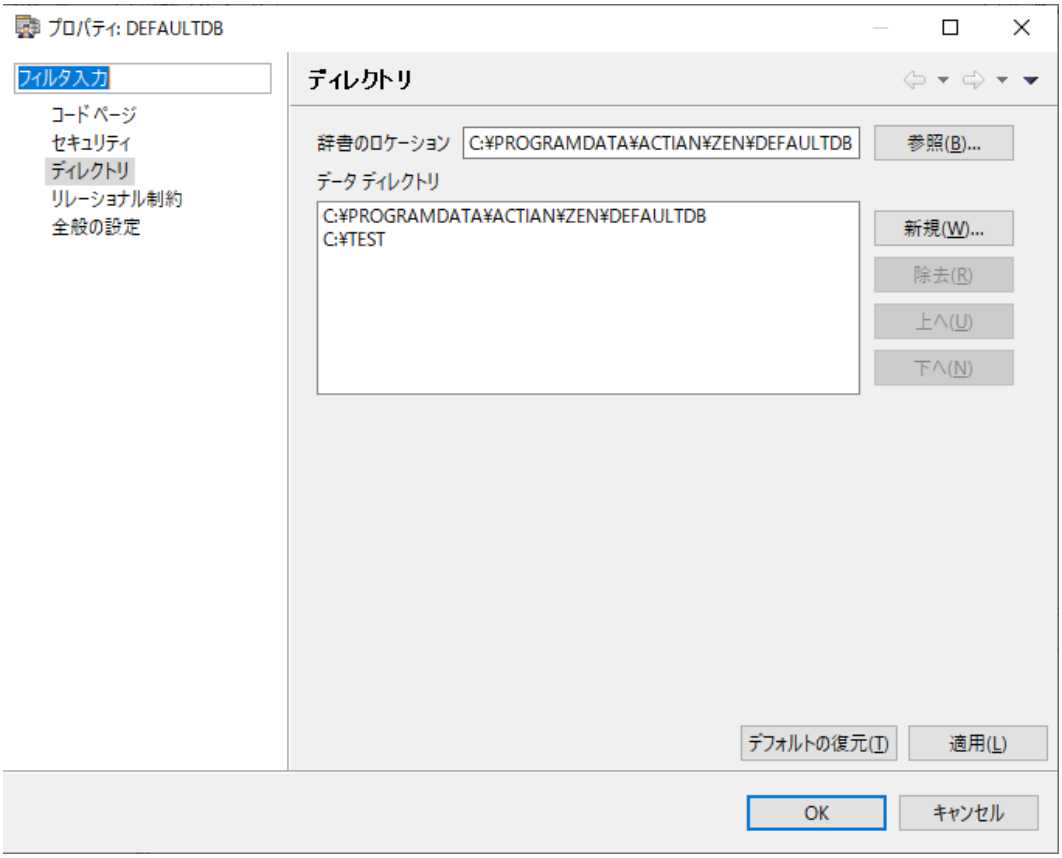
Zen はデフォルトでは通信の暗号化は行いません。
Wireshark 等のパケットキャプチャーツールを使用することで、ネットワークを流れるデータを参照できてしまいます。
これを防止するには、暗号化の設定を行います。
サーバー側とクライアント側双方で暗号化を行う設定をすることで通信時のデータを暗号化できます。
ネットワークの暗号化では、アプリケーションの処理は暗号化を行わない場合と全く同じです。
ネットワークの暗号化にアプリケーションの変更は一切必要ありません。
ただし、ネットワークの暗号化を行う場合、データの暗号化・複合化処理が余分に必要となるため、CPU 負荷が高くなります。
暗号化の強度は低（40 ビット暗号化キーを使用）、中（56 ビット暗号化キーを使用）、高（128 ビット暗号化キーを使用）の 3 段階から選択できます。

3. データベース URI 使用による、ファイルパスの隠蔽

Btrieve API では、ファイルを開く際、ドライブ名から始まるパスや「¥¥サーバー名」から始まる UNC パスを指定しますが、この形式では全ての開発者はファイルがどのフォルダーに存在しているのか解っていることが必要です。
複数の開発会社で開発を行う場合等で、ファイルの存在場所を公開したくないこともあります。
クライアントサーバーで使用する場合、アクセス権の設定も必要です。
また、Named Pipe 等（ポート 137、138、139、445）のポートを解放する必要があり、インターネット上で使用するにはセキュリティホールとなります。
P.SQL V8 SP2 からは､データベース URI 形式でファイルパスを指定することが可能で、これらの問題を解決できます。
データベース URI でファイルパスを指定する場合、ポート 3351 以外にポートを解放する必要はありません。
データベースに登録されている Btrieve ファイルでは、ファイル名では無く、テーブル名で指定可能で、ファイルの格納場所を知る必要はありません。
アクセス権もデータベースに設定されているアクセス権に従います。
OS の共有に対する設定を必要としません。
データベースとして登録されているファイルは、次のような指定でアクセスが可能です。
例：
btrv://Server/demodata?table=person

demodata はデータベース名を、person にはテーブル名を指定します。

データベースに登録されていない Btrieve ファイルを使用する場合、DEFAULTDB データベースのプロパティのデータディレクトリに該当ファイルがあるパスを追加し、データベース URI のデータベース名に DEFAULTDB データベースを指定します。
次の例では、c:¥test をデータディレクトリに追加しています。



テーブルとして登録されていない Btrieve ファイルを指定する場合は、table= では無く、dbfile= で Btrieve ファイルを指定します。

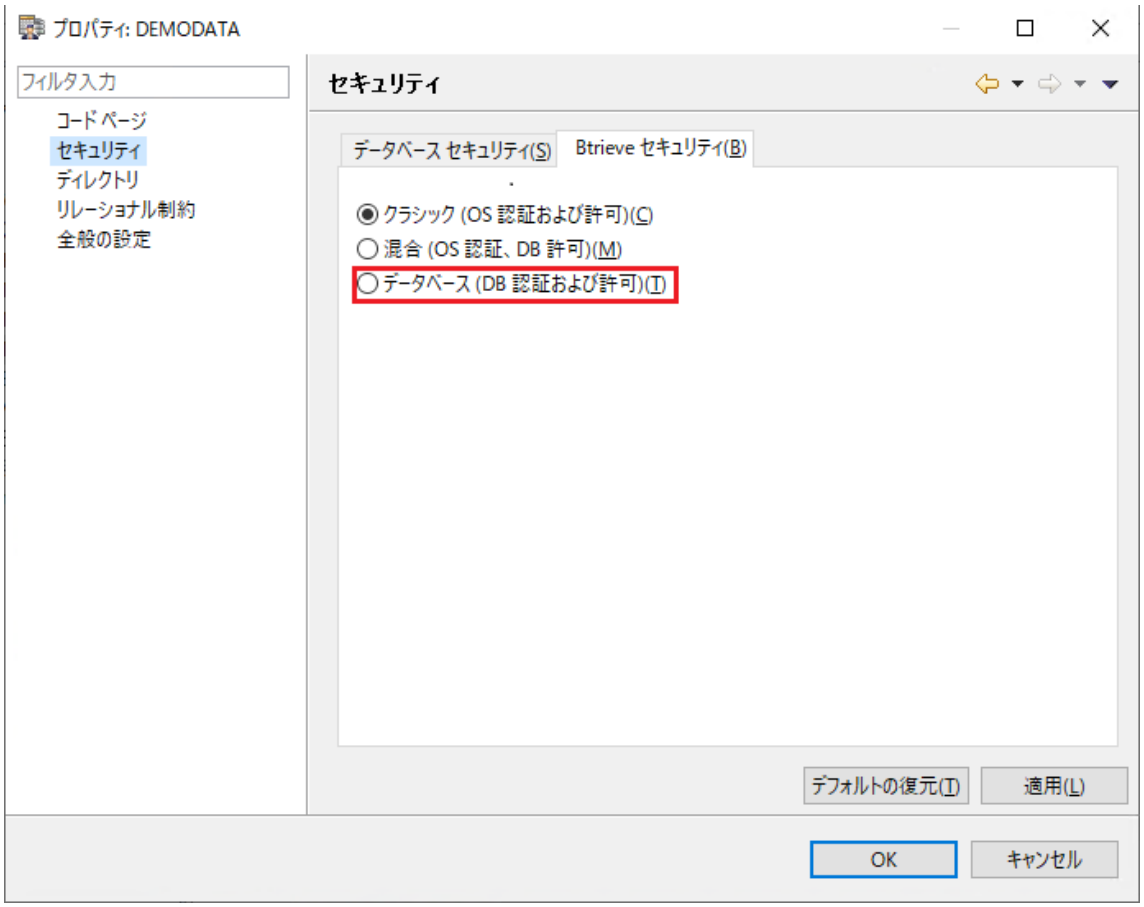
例：
btrv://サーバー名/DEFAULTDB?dbfile=person.mkd

dbfile= には、「データ ディレクトリ」で設定されているフォルダーからの相対パスでファイルを指定します。
ドライブ名から始まる絶対パスでは指定できません。
また、「データ ディレクトリ」に複数のフォルダーを設定した場合で、複数のフォルダーに同名のファイルが存在すると、始めに見つかったファイルがアクセス対象となりますので、同名のファイルの使用はお勧めいたしません。

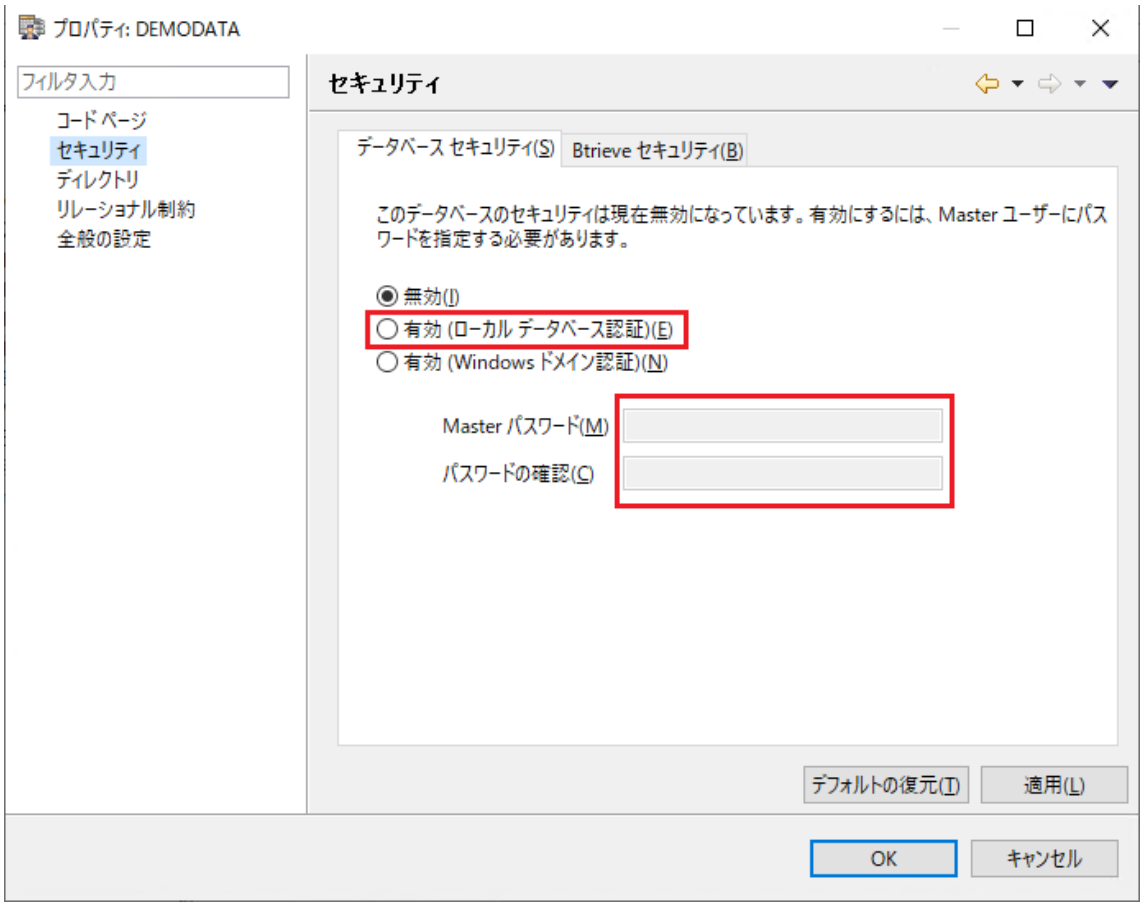
4. アクセス権

Zen では、エンジンでユーザーを管理することも可能で、OS が管理しているアカウントのアクセス権でアクセスすることが可能です。(デフォルトの動作)
(Workgroup は、OS が管理しているアカウントのアクセス権には対応しません)
また、Zen でユーザーやグループを設定し、アクセス権を設定することも可能です。

セキュリティを有効にするには、データベースのプロパティで設定を行います。
まず Btrieve セキュリティを「データベース」に設定します。

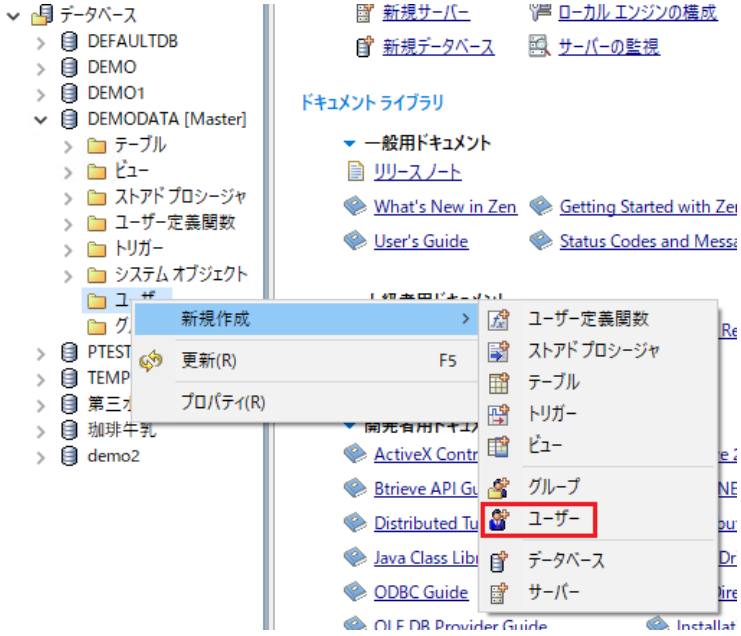


次に、データベースセキュリティを「有効 (ローカルデータベース認証)」を選択し、Master ユーザーのパスワードを設定します。
※Master ユーザーのパスワードを忘れると、セキュリティの有効・無効が変更できなくなりますので、ご注意ください。



テーブル毎に詳細なアクセス権を設定するには、Zen でユーザーまたはグループを設定する必要があります。

ユーザーは、セキュリティを有効にすることで、追加可能となります。



SQL アクセスでは、ユーザーまたはグループ毎に、各テーブルに次のようなアクセス可否が設定可能です。
フィールド毎に設定可能な項目もあります。

- 選択
- 更新
- 挿入
- 削除
- 変更（テーブル構造）
- 参照

データベースに対しても、次のような操作の可否が設定可能です。

- テーブルの作成
- 選択
- 更新
- 挿入
- 削除
- 変更（テーブル構造）
- 参照
- ビューの作成
- ストアドプロシージャの作成

Btrieve アクセスでは､テーブル(ファイル)毎に次のようなアクセス可否が設定可能です。
Btrieve アクセスでは、レコード全体の設定となり、フィールド毎の設定は無視されます。
※レコード全体のアクセスが許可されている事が必要です。

- 選択
- 更新
- 挿入
- 削除

セキュリティを有効にして Btrieve にアクセスするには、予め Logon オペレーションを実行するか、データベース URI にユーザーとパスワードを含めて Open オペレーションを行う必要があります。

例：
btrv://testuser@testserver/defaultdb?dbfile=testfile.mkd&pwd=password

※testuser：ユーザー名、testserver：サーバー名、password：パスワード