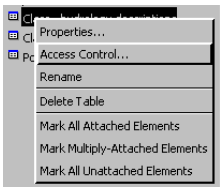
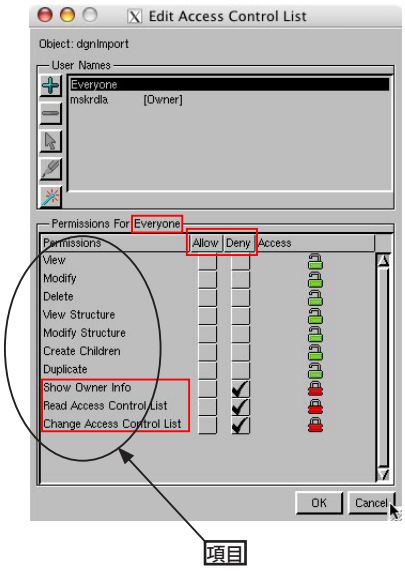
2006 年 5 月 18 日

アクセスコントロールリスト

大勢の人が関わるような企業環境では、地理空間データやデータベースフィールドの情報を誰が表示できて、誰が変更までできるかを制限したい場合があります。あるいは企業環境と関わりなく、TNT SDK を使って開発したカスタム製品がある場合に、開発した製品と一緒に配布したデータを第三者がどの程度操作できるかをコントロールしたいこともあるでしょう。このような管理の問題は、**資格認証** (Credentials) や**アクセスコントロールリスト**によって解決することができます。資格認証はユーザ名とパスワードによって行われます。アクセスコントロールリストは、プロジェクトファイルやオブジェクト、サブオブジェクト等のコンテンツへのアクセスに必要な資格認証を様々な**項目**に対して決めるもので、その項目の種類には要素の表示や変更、削除、データベース構造の表示や変更、サブオブジェクトの作成やコピーがあります。個々のデータベーステーブルやデータベースフィールドへアクセスできるユーザについてもコントロール可能です。ゆえに、ユーザによってテーブル内の一部のフィールドが表示できなかったり、表示できても特定のフィールドは変更できなかったり、他のフィールドについては表示、変更ができたりします。アクセスコントロールリストによってファイルやオブジェクトのオーナー (所有者) 情報を閲覧できるユーザを決めることができ、アクセスコントロールリストの読み込みや変更ができるユーザを決めることも可能です。



アクセスコントロールは「プロジェクトファイルの管理 (Project File Maintenance)」プロセスで設定します。データベーステーブルやフィールドに関しては、データベースが表示できる場所であればどこにでもアクセスコントロールを設定できます。[アクセスコントロールの編集 (Edit Access Control)] アイコンをクリックするか、テーブルでマウスの右ボタンメニューから [アクセスコントロール (Access Control)] を選択すると、ユーザ名とパスワードの入力を促されます。そのレベルでファイルやオブジェクト、サブオブジェクトがまだアクセスコントロールリストを持っていない場合は、あなたがデフォルトの設定によりオーナーになります。デフォルトで設定される許可には「オーナー」に対するものと、「全員」の 2 つがあります。ここで言う「全員」とは、リストに特に名前のない全てのユーザを指します。オーナーは、常にオーナー情報の表示やアクセスコントロールリストの読み込みおよび変更を行うことができます。これら 3 つの許可 (オーナー情報の表示、アクセスコントロールの読み込みと変更) は、「全員」はデフォルトではオフに設定されていますが、許可することも可能です。[オーナー情報の表示 (Show Owner Info)] がカレントユーザに許可されている場合、＜オーナー情報の編集 (Edit Owner Information) ＞ウィンドウに入力された情報は「プロジェクトファイルの管理」のファイルやオブジェクトで [情報 (Info)] ボタンをクリックした際に表示される他の情報に含まれます。

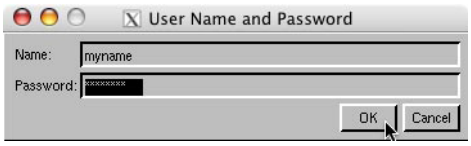


アクセス許可には以下のようにチェックボックスで示される 3 つの状態があります:①許可 (Allow)、②非許可 (Deny)、③あいまい (①、②のいずれもチェックされていない状態)。ある個別のユーザに対する許可状況があいまいな場合は、「全員」に対して設定されている許可状態が調べられます。それでもまだ許可状況があいまいな場合は、親オブジェクトに対する許可が最高のファイル**レベル**まで順に調べられます。例えば、データベースフィールドに対する許可の設定が何もなされていない (特定ユーザおよび全員に対して) 場合、テーブルに対しての許可が調べられ、もしこれも設定されていない場合はデータベース、次にベクタに対する許可状態が調べられます。それでもなお許可状況があいまいな時は、ファイルに関して調べられます。この許可もあいまいな場合は、その項目の操作が許可されます。許可チェックボックスの右側にある鍵の色は、各項目の許可が明白なものかあいまいなものかを示しています。同じレベルで変更は許可するが表示は許可しないなど、許可の組み合わせによっては無意味なものもあります。しかし、ベクタの表示は許可しないがデータベーステーブルの変更は許可するといった、異なるレベルでの許可は便利かもしれません。

アクセスコントロールの使用は自由であり、上述した状況下でデータへのアクセス制限を行いたくない場合は特に使用する必要はありません。アクセスコントロールリストは TNTmips の全ユーザが表示できますが、アクセスコントロールリストの編集はマイクロイメージ社に要求しなければ使用できません。この機能を入手しない限り、OK ボタンはクリックできないようになっています。

どのレベルでも構いませんが、アクセスコントロールリストを持ったファイルを処理のために選択する場合、ユーザはアクセスコントロールリストの編集時のようにユーザ名とパスワードの入力を催促されます。アクセスコントロールリストを持ったファイルが、ある処理で最後に選択するファイルの場合でも、何らかの選択の時点で名前とパスワードの入力を促されます。

SML および SDK におけるアクセスコントロール　データ所有者は、TNTmips の SDK を使って開発したカスタムスクリプトやカスタムプロセスにおいてどのデータをアクセスするか、またどこに書かれているかをコントロールするために、資格認証 (ユーザ名とパスワード) を要求するように設定できます (要求しないでパスするようにも設定できます)。資格認証をパスするように設定すると、スクリプトやプロセスを実行するどのユーザもスクリプト内に明記されたユーザと同じアクセス権を持ちます。もし資格認証をパスせず必要とする場合には、open や create 関数がユーザ名やパスワードを催促してきます。資格認証が必要なオブジェクトやファイルにそのスクリプトがアクセスしようとしてしまった場合に、このダイアログが開くのを防ぐ関数もあります。



資格認証を使ってラスタを開く簡単なスクリプトで、＜コンソール＞ウィンドウにラスタタイプを報告するスクリプトを下に示します。

```
class RASTER R;
class RVC_CREDENTIALS credentials;
credentials.Set("myname","password");
OpenRaster(R,"E:/test/credtesting/creds.rvc","_24BIT_BGR", credentials);
typ$=R.$Info.Type;"print(typ$);
```

このラインが省略されると、実行時に必要に応じてユーザ名とパスワードの入力を促されます。

資格認証をパスし、ファイルやオブジェクトが SDK で開発されたプロセスやスクリプトによって作成されると、そのファイルやオブジェクトに名前を付けたユーザがファイルのオーナーとなります。追加的な許可については 1 ページ目に説明があります。DisableCredentialsPopup() という関数は、資格認証をパスしていない場合にユーザ名やパスワードの入力を促さないようにするためのものです。この関数を使ったスクリプトは、制限的な許可セットのあるファイルやオブジェクトが使われたとしても資格認証の入力を促すことなく「ユーザはこの操作を完了する許可を持っていません」というエラーを出して操作を実行しません。このエラーは、入力またはパスした資格認証がそのファイルやオブジェクトに対するアクセスを提供しない場合に表示されるエラーと同じものです。

アクセスコントロールリスト (ACL) の機能は、デフォルトでは使用できません。
ACL の機能を有効にするためには、ライセンスキーの認証が必要です。