内容

1　序文

データベースを管理するにあたり、誰がデータベースの内容を参照・更新する権利があるのかを事前に取り決め、不正アクセスを防止する措置を講ずる必要があります。独立した端末にインストール・管理されているデータベースの場合、その端末（或いはデータベースを保存しているディスク）自体を暗号化・パスワード保護することで不正アクセスを未然に防ぐことが可能です。一人のユーザーのみがデータベースを参照・更新するという運用の場合、この様な措置で事足ります。

プロマシスは、複数のユーザーがインターネットを介して同時にアクセスし、参照や更新を行うデータベース管理システムです。プロマシスがインストールされている施設の従業員をはじめ､外部の者にもアクセスを許可することが可能です｡場所を問わずアクセスが可能になると、データの漏えい・不正アクセス対策をより厳重に図る必要があります。具体的には、実施施設外のもの（治験依頼者等）が被験者の氏名・住所等を参照（閲覧）することを防ぎつつ各被験者の治験データへのアクセスを許可することや、データ入力担当が誤ってプロトコルのデザインに変更を加えることを未然に防ぐための措置を講ずる等が必要になってきます。

プロマシスでは、各ユーザーのアクセス権限を詳細に設定できます。アクセス権限を振り分ける操作は全てメインインターフェースで行います｡操作こそ簡単なアクセス権限の設定ですが、誤った設定をしてしまうことの影響が大きいので、アクセス権限の管理者には深い理解力が要求されます。少しでも理解の向上に役立たせるに、本チュートリアルでは、最初にプロマシスでのアクセス権限の設定の全体図を説明します。その後、新規ユーザーを登録する場合に行うアクセス権限の設定を一般的な順番で解説していきます。

2　プロマシスのアクセス権限の基本

プロマシスでは、プロトコル別または機能別に詳細にアクセス権限を設定することが可能です。個々の設定の意義を理解するには、全体の理解が必要です。本章では、プロマシスにおけるアクセス権限の各設定の基本的な情報を記すとともに、全体像での位置づけについて解説します。

プロマシスでのアクセス権限の設定を学んでいく過程で、様々な場所で矛盾・競合する設定が行える様な印象を受ける可能性があります。プロマシスにおけるアクセス権限を理解する上で重要なのが、プロマシスではアクセス権限の競合があった場合、一番低いアクセス権限レベルが適応される、ということです。例えば、ユーザーのある機能（データ入力等）に対する権限レベルが「管理者権限」の場合でも、あるプロトコルに対して読み取り権限のみ付与されている場合、一番低いアクセス権限レベルが適応され、該当プロトコルに対して実質読み取り権限のみ付与される状態になり、データ入力ができない状態になります。矛盾や競合を回避するための措置ですが、これを常に意識していないと「○○へのアクセス権限を付与したのに△△ができない」というエラーへの対処が難しくなります。

2.1　アクセス権限の基本

プロマシスのアクセス権限は基本的に三段階（「無」を含むと四段階）に分かれており、読み取り（レコードの参照）のみが許可される「Read Access」、書き込み（レコードの更新）が許可される「Write Access」と、管理者権限が付与される「Admin Access」があります。書き込み権限には、読み取り権限が全て含まれており、管理者権限には、書き込み権限が全て含まれております。

管理者権限に限定されている操作は、「通常のフローに反する操作」と「データベースへの影響が大きい操作」です。下記 2.2 にて解説しますが、確定されたデータの上書き入力、プロトコルに登録された被験者の登録解除等がそれにあたります。これらの操作の多くでは「変更・更新の理由」（Reason for transaction）の入力を求められます。

アクセス権限	可能な操作
無	一切のアクセスが許可されていない状況です。
読み取り	レコードの参照のみが可能で、一切の更新が行えません。
書き込み	レコードの参照と更新が可能です。基本的な操作が行えますが、通常のフローに反する操作は行えません。
管理者	通常のフローに反する操作も行えます。
全て	特殊なアクセス権限設定で、データベースの内容全てに対して管理者権限が付与されます（下記 3.1 参照）。

2.2　スタディーライフサイクルとの関係

プロマシスには、プロトコルや登録被験者の進行状況に応じて操作を許可したり凍結したりするシステムがあります。スタディーライフサイクルというこのシステムでは、プロトコルが作成段階にあるのか、実施段階にあるのか等によって、操作に必要なアクセス権限レベルが変動します。例えば、パラメーターやアクティビティの作成、並びにタイムテーブルの作成等は、プロトコルが作成段階（DEF）にある場合は書き込み権限で行うことが可能です。プロトコルが実施段階（EXE）にある場合は、これらの操作には管理者権限が必要です。

プロトコルに関するスタディーライフサイクルには、次の段階（フェーズ）が存在します。

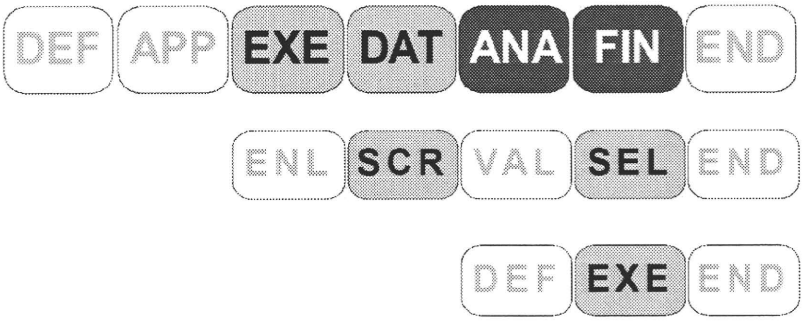
各フェーズで許可されている操作は大まかに以下の通りです。

DEF：　プロトコルのデザイン、タイムテーブル・スケジュール作成等
APP：　プロトコルデザインが凍結されるため、ほとんどの操作が不可
EXE：　被験者の登録・組み入れとデータ入力が全て可能
DAT：　データ入力が全て可能。被験者の登録・組み入れには管理者権限が必要
ANA：　被験者の登録・組み入れとデータ入力の全てに管理者権限が必要
FIN：　ANA と同じ
END：　プロトコル・入力データが完全凍結し、一切の変更が不可

登録被験者もフェーズで管理されており、次の 5 つのフェーズが存在します。プロトコルのフェーズとは異なり、本チュートリアルで説明するアクセス権限の設定と直接的な関係は少ないです。登録被験者のフェーズは、主にデータ入力の可否に影響してくる属性です。フェーズが END に到達した被験者に関しては、一切のデータ入力が不可能です。

最後に、各登録被験者の各オケージョンもフェーズで管理されており、次の 3 つのフェーズが存在します。

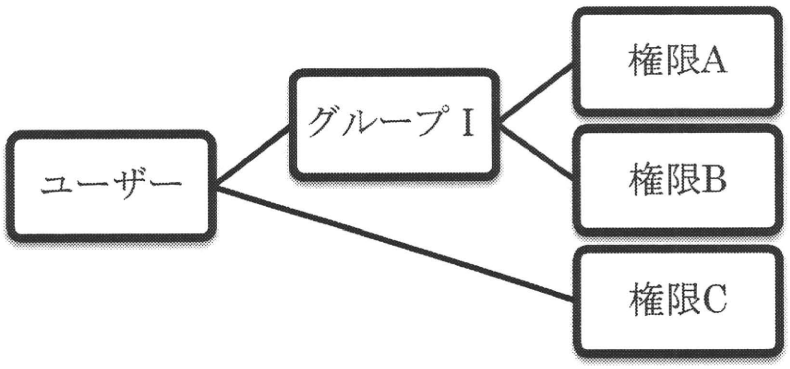
これらのフェーズはプロマシスマニュアルのリファレンスの章で下図の通りに表示されます。モジュール・タブ別に機能を紹介するリファレンスでは、各フェーズにおいてどの操作が可能であるかがカラーコードで示されています。白は更新不可（参照のみ）、緑は書き込み権限以上で更新可、赤は管理者権限でのみ更新可、をそれぞれ意味しています。



上図の例だと、EXE 及び DAT フェーズにおいては書き込み権限以上が付与されている場合に操作が可能で、ANA 及び FIN フェーズにおいては管理者権限が付与されている場合にのみ操作が可能、ということを意味しています。このように、マニュアルのリファレンスを参照することで、必要なアクセス権限を把握することが可能です。

2.3　ユーザーアカウントとユーザーグループ

プロマシスのアクセス権限付与には、二通りの方法があります。ユーザー単位で付与する方法と、ユーザーグループに権限を付与し、その後ユーザーにユーザーグループを割り当てる方法です。ユーザー主体で見た場合、下図の様な構造になっております（詳細については、「ユーザーアカウント」及び「ユーザーグループ」を参照）。



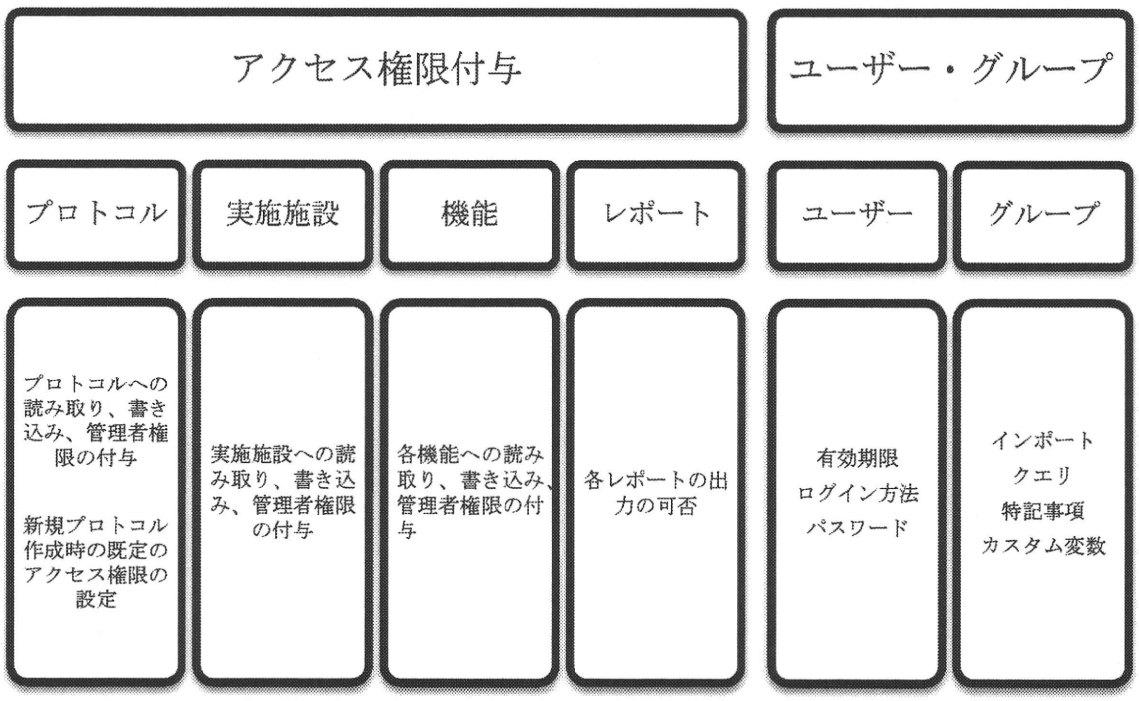
ユーザーグループを作成することで、あらかじめ定められたアクセス権限のセットをまとめて

ユーザーに付与することが可能です。例えば、プロトコルのデザインをプロマシスに入力するユーザーは、複数のモジュール・タブにアクセスできなければいけません。ユーザーを登録する度に、アクセス権限を一個ずつ付与するのは時間がかかる上、手順の多さからミスを招く可能性があります。但し、アクセス権限の付与全般にユーザーグループの使用が適切であるかは、使用環境によって大きく異なります。一般的には、個々のプロトコルへのアクセス権限等は各担当者のユーザーアカウントに付与し、各機能（モジュール・タブ）へのアクセス権限は、ユーザーグループを介して付与します。

2.4　プロトコル、施設、メニュー、レポート、クエリ、特記事項…

プロマシスのアクセス権限は、特定のプロトコル、施設、及び機能（モジュール・タブ）にユーザーアカウント又はユーザーグループを「読み取り」、「書き込み」、「管理者」のいずれかに登録することで該当ユーザー・ユーザーグループに付与されます。プロマシスの各レポートの出力の可否も、同様の方法で制御できます（可否のみのため、「読み取り」、「書き込み」、「管理者」の権限レベルは存在しません）。クエリ、特記事項、カスタム変数、電子署名に関するアクセス権限は特殊で、全てユーザーグループを介しての付与のみが可能です。また、一部ユーザーアカウント単位でのみ付与できるアクセス権限もあります。

詳細な設定が可能なシステムには、当然ながら複雑さも伴います。システム管理者は、各アクセス権限の付与方法を把握しておく必要があります。下図に、**ACCESS CONTROL** モジュールの各タブで設定できるアクセス権限を簡単に示します。

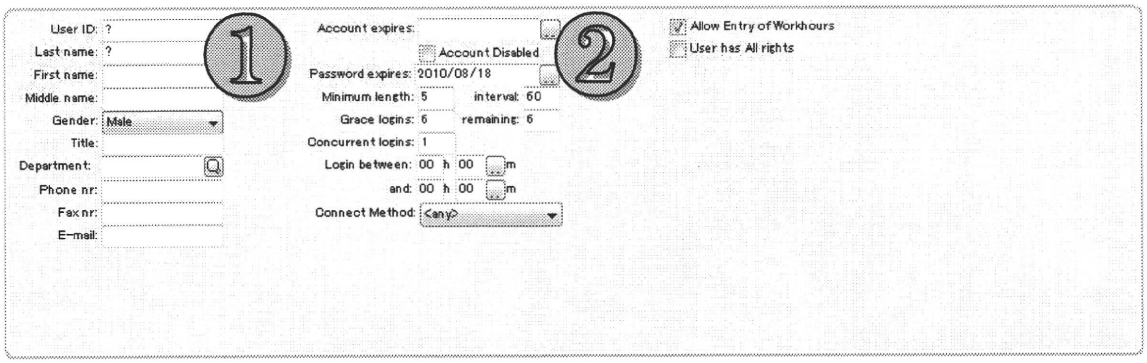


3　ユーザーアカウント

本章では、新規のユーザーを作成する手順と、ユーザーアカウントで設定できるアクセス権限、ログイン方法その他 **ACCESS CONTROL** モジュールの **USERS** タブで行える操作について説明します。一般的には、一人の使用者につきユーザーアカウントが最低一つ準備されます。

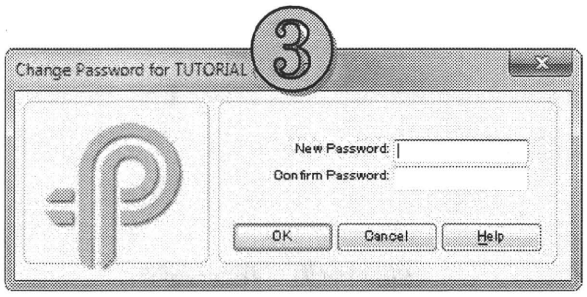
3.1　ユーザーアカウントの作成

新規のユーザーアカウントの作成は、**USERS** タブで画面右下の Add をクリックすることで開始します。既存のユーザーアカウントを変更する場合は、Update をクリックします。画面下部のフィールドが白になり、入力が可能な状態になります。



① User ID にユーザーのアカウント名を入力します。半角英数字のみ、全て大文字で入力します。小文字での入力は可能ですが、システム内では全て大文字に変換されてから処理が行われます。従って、User ID に大文字小文字の区別はありません。初期パスワードには既定で、ここで設定するアカウント名と同じ文字列が設定されます。Last name フィールドに、ユーザーの名前（姓）を入力します。Last name の下にある First name から E-mail のフィールドは、必要に応じて入力します（任意です）。User ID は、ユーザーアカウントの新規作成時に設定し、その後の変更は不可能です。また、データベース内に重複する User ID は存在できません。

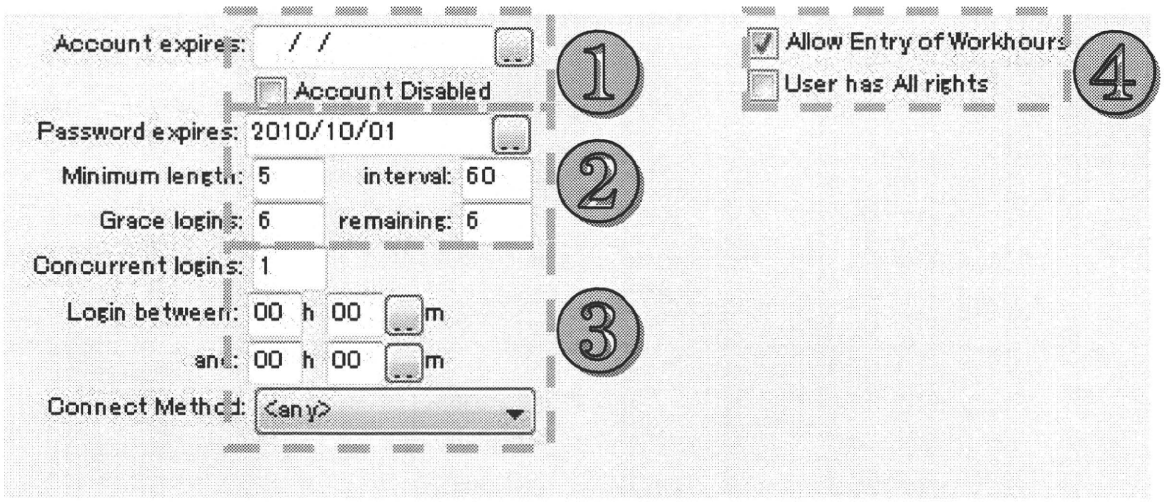
② Account expires から Connect Method のフィールドは、アカウント及びパスワードの有効期限、同アカウントでの同時ログイン可能数、ログイン方法の限定等の設定を行います。詳しくは「ユーザーアカウントの詳細設定」を参照して下さい。一般的には既定の設定で問題ないです。Save をクリックすると、入力内容が確定され、ユーザーアカウントが作成されます。



③ ユーザーアカウントの新規作成時、初期パスワードは User ID と同じものに設定されます。パスワードをすぐに変更する場合は、画面左下の Change Password ボタンをクリックします。「Change Password for...」ウィンドウが表示されるので、新しいパスワードを New Password 及び Confirm Password にそれぞれ入力し、OK をクリックします。ここで変更を行わない場合、初回ログイン時に変更を求められます。

3.2 ユーザーアカウントの詳細設定

アカウントの有効期限や、その他制限を設ける方法について説明します。尚、この設定は、ユーザーアカウント作成時にまとめて行えますが、混乱を避けるため本書では分けて説明しています。本項の手順は、の手順に沿ってユーザーアカウントが既に作成されていることを前提としています。**USERS** タブで画面右下の Update ボタンをクリックします。画面下部のフィールドが白になり、入力が可能な状態になります。



① **アカウントの有効期限に関する設定：** Account expires フィールドに、アカウントの有効期限を設定します。空欄の場合は、アカウントは無期限に使用できます。また、設定されている有効期限に関わらずアカウントを無効化したい場合は、Account Disabled にチェックを入れます。

② **パスワードの有効期限に関する設定：** パスワードの有効期限は Password expires で設

定します。空欄の場合は、パスワードは無期限に使用できます。期限が設定されている場合は、期限を過ぎるとログイン時にパスワードを変更する様に求められます。変更後に、Password expires は、パスワードを変更した日付に interval に設定されている日数を加算した日付に再設定されます。Minimum length では、パスワードの最低文字数を設定します。指定した文字数より短いパスワードは、設定できません。Grace logins では、パスワードの有効期限を超過した状態で、パスワードを変更せずに何度のログオンを許可するかを設定します。Grace logins は最大許可される残り回数で、remaining は現在の残り回数を示します。パスワードを再設定した時点で、remaining の値は Grace logins の値にリセットされます。

③ **ログインの制限に関する設定：**Concurrent logins では、同一アカウントが同時にシステムにログインできる回数を設定します。Concurrent logins が「2」以上に設定されている場合、一つの端末で既にシステムにログインしていても、他の端末でも同時にログインすることが可能です。

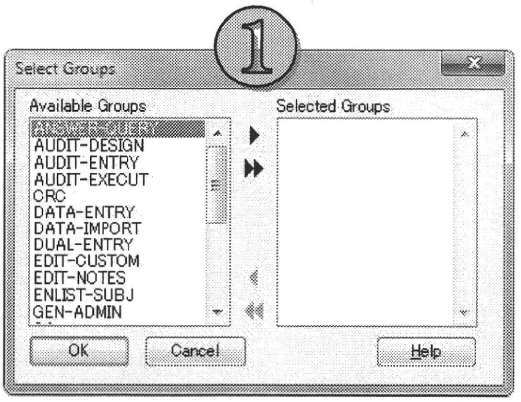
Login between 及び Connect Method で、ユーザーアカウントのログイン時間帯・ロケーションを制限できます。Login between の項目には、二つの入力フィールドがあり、二つのフィールドにそれぞれ時刻を入力することで、ユーザーがシステムにログイン可能な時間帯を設定できます。例えば、ログインを午前 9 時から午後 5 時に制限したい場合は、上のフィールドに 09:00、下のフィールドに 17:00 と入力します。Connect Method では、アカウントのログインロケーションを「<all>」、「Host Based only」、「WebClient only」から選択できます（もう二つオプションがありますが、特殊な環境でのみ使用されるため、割愛します）。

Connect Method が「Host Based only」のアカウントでは、プロマシスのサーバーマシン上でのログインのみが許可されています。一方、Connect Method が「WebClient only」のアカウントでは、端末（プロマシスのクライアントがインストールされているマシン）からのみログインが許可されています。「<all>」に設定した場合には、ロケーションに制限が設けられません。

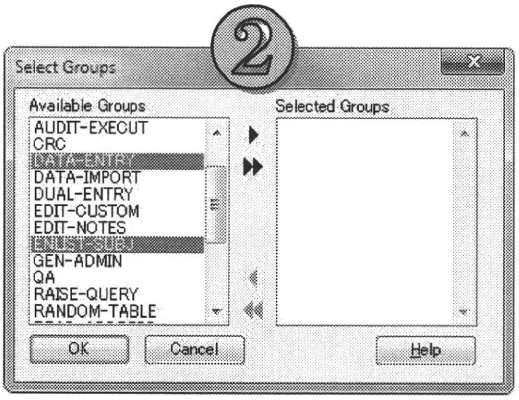
④ 右にある二つのチェックボックスでは、その他のオプションを設定します。Allow Entry of Workhours が有効になっている場合、**USERS > WORKHOURS** で作業時間の入力が許可されます。User has All rights が有効になっている場合は、そのアカウントには、全ての権限が付与されています。このオプションは、一般的にはデーモン用のアカウントにのみ付与され、併せてアカウントの Connect Method を「Host Based only」に設定します。デーモン以外のアカウントに関しては、リスク管理の観点から基本的に User has All rights 属性を無効に設定することが推奨されます。

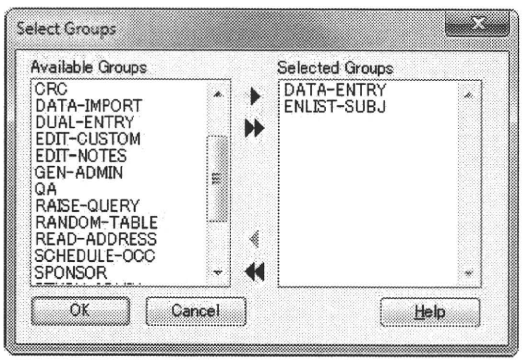
3.3　ユーザーグループの割り当て

ユーザーアカウントの詳細設定が終了したら、次にアカウントにユーザーグループを割り当てます。ユーザーグループは、事前に定義されているアクセス権限のセットであり、一つのアカウントに対して複数割り当てることが可能です。ユーザーグループの作成方法については、下記 4.1 にて解説します。本項では、作成済みユーザーグループをユーザーアカウントに割り当てる方法について解説します。

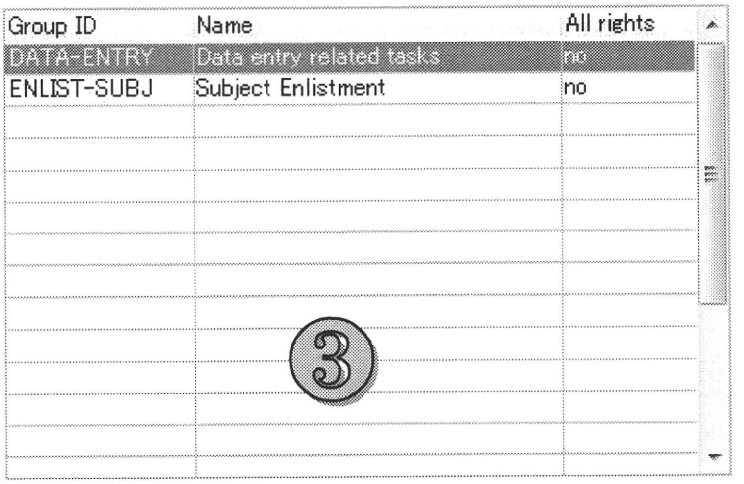


① **ACCESS CONTROL** モジュールの **USERS** タブ、ウィンドウ左下 Group Membership をクリックすると、「Select Groups」ウィンドウが表示されます。ウィンドウ左側選択可能なユーザーグループ（Available Groups）が、ウィンドウ右側に選択済み（Selected Groups）ユーザーグループが表示されます。





② ユーザーアカウントに割り当てるユーザーグループを Available Groups の一覧でクリックしてハイライトします。複数のユーザーグループを同時に割り当てる場合は、キーボードの CTRL キーを押しながら他のユーザーグループをクリックします。▶ボタンをクリックすると、ハイライトされたユーザーグループが Selected Groups へ移動します。ユーザーグループの割り当てを取り消すには、Selected Groups から取り消すユーザーグループを選択し、◀ボタンをクリックします。確定するには、OK をクリックします。



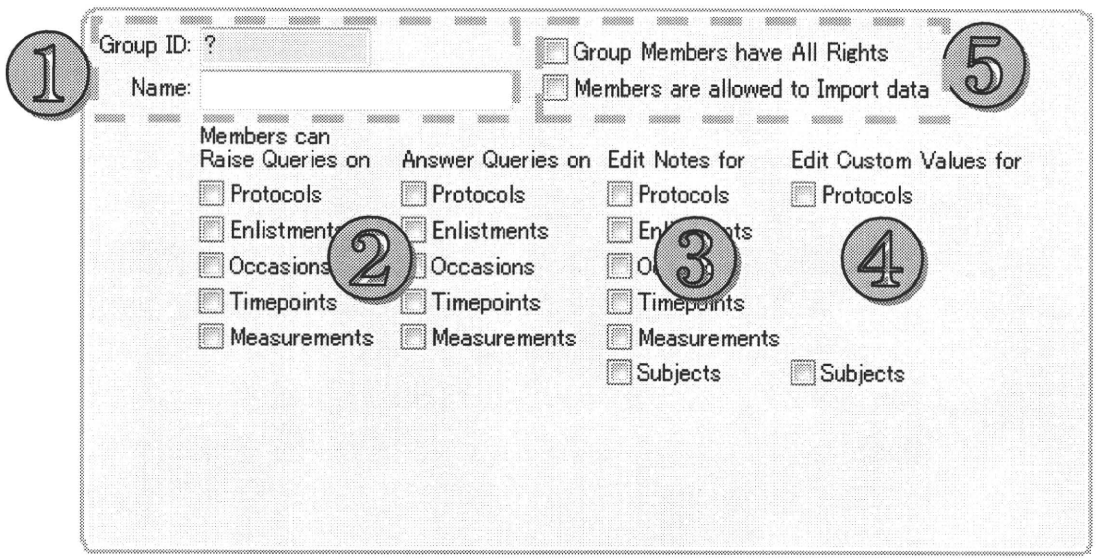
③ インターフェース右側のウィンドウに、ユーザーアカウントに割り当てられたユーザーグループが表示されます。

ACCESS CONTROL モジュールの **USERS** タブでは、上記の手順でユーザーアカウントにユーザーグループを割り当てることができます。同様の手順で、**ACCESS CONTROL** モジュールの **GROUPS** タブでユーザーグループに属するユーザーアカウントを選択できます。**USERS** タブと同様、Group Membership ボタンをクリックして割り当てを行いますが、視点がユーザーグループだということに注意が必要です。

4　ユーザーグループ

本章では、ユーザーグループについて説明します。ユーザーグループには、「データ入力」や「プロトコル管理」等、様々なアクセス権限のセットが既定で存在します。既定のユーザーグループをそのまま、又は若干の修正を加えた状態で、多くの使用環境に適応できます。既定のユーザーグループを変更するには、下記手順で Add ボタンをクリックする代わりに、対象のユーザーグループをクリックした上で Update をクリックします。

4.1　ユーザーグループの新規作成



① **ACCESS CONTROL** モジュールの **GROUPS** タブで、ウィンドウ右下 Add をクリックします。Group ID にユーザーグループの識別子を、Name 欄にユーザーグループの名前を入力します。

② クエリに対するアクセス権限の設定を行います。Raise Queries on 及び Answer Queries on の下に、それぞれ 5 つのチェックボックスが表示されています。左の列では、プロトコル、登録被験者等のそれぞれに対してクエリを新規発行の可否を設定し、右の列では発行済みクエリへの回答の可否を設定します。クエリの新規発行・クエリへの回答の可否をそれぞれ Protocols（プロトコル）、Enlistments（登録被験者）、Occasions（オケージョン）、Timepoints（タイムポイント）、Measurements（メジャーメント）別に設定できます。既定のユーザーグループ「RAISE-QUERY」と「ANSWER-QUERY」では、それぞれクエリの新規発行（全項目）とクエリへの回答（全項目）が一括で付与できます。

③ Edit Notes for の下にある 6 つのチェックボックスで、特記事項の作成・更新の権限を設定します。Protocols（プロトコル）、Enlistments（登録被験者）、Occasions（オケージョン）、Timepoints（タイムポイント）、Measurements（メジャーメント）、Subjects

（被験者パネル）それぞれ個別に、特記事項の作成・更新の可否を設定できます。既定のユーザーグループ「EDIT-NOTES」では、特記事項の作成・更新（全項目）が一括で付与できます。

④ Edit Custom Values for にて、カスタム変数の新規作成・更新の可否を設定できます。カスタム変数は、Protocols（プロトコル）及び Subjects（被験者パネル）のみで設定できます。既定のユーザーグループ「EDIT-CUSTOM」では、カスタム変数の新規作成・更新（全項目）が一括で付与できます。

⑤ ユーザーグループに属するものに、全てのアクセス権限を一括で付与する場合には、Group Members have All Rights を有効にします。特殊なケースを除いて、本オプションを使用することは推奨されません。外部データの読み込み権限を設定したい場合には Members are allowed to Import data を有効にします。外部データの読み込みは、本オプションが有効になっているユーザーグループに属するユーザーアカウントのみです。

ユーザーグループの定義時に行えるのは、クエリ、特記事項等に対するアクセス権限の設定のみです。バージョン 6.1 以降の場合、更に電子署名に関するアクセス権限も設定できます。それ以外の初設定（各プロトコルへのアクセス権限の設定、機能や許可されている操作等）は、**ACCESS CONTROL** モジュールの **PROTOCOLS**、**STUDY CENTRES**、**MENU**、**REPORTS** タブでそれぞれ設定します。これらの設定については、下記第 5 章で解説します。クエリ発行や、特記事項作成等の機能は、作業対象のプロトコルに書き込み以上の権限が付与されている必要があります。書き込み以上の権限が付与されていない場合は、クエリの発行及び回答、特記事項の作成及び更新、外部データの読み込みがいずれも行えない状態になります。

4.2 既定のユーザーグループ

プロマシスには、既定で 21 のユーザーグループが定義されております。下記に、各ユーザーグループでどの様な権限が付与されるのかを簡潔に示します。権限が付与される仕組みはユーザーグループによって異なり、**GROUPS** タブで付与できるアクセス権限もあれば、**MENU** タブを用いて付与するアクセス権限もあります（後者の設定方法は次章の 0 で解説します）。

ACCESS CONTROL > GROUPS で設定できるアクセス権限：

RAISE-QUERY：	クエリの新規発行が許可されている
ANSWER-QUERY：	発行済みクエリへの回答が許可されている
EDIT-NOTES：	特記事項の作成・更新が許可されている
EDIT-CUSTOM：	カスタム変数の作成・更新が許可されている
DATA-IMPORT：	外部データの読み込みが許可されている

ACCESS CONTROL > MENU で設定できるアクセス権限：

AUDIT-DESIGN：	プロトコルの作成に関する管理者権限
AUDIT-ENTRY：	データ入力に関する管理者権限
AUDIT-EXECUT：	被験者登録に関する管理者権限
DATA-ENTRY：	データ入力に関する書き込み権限
ENLIST-SUBJ：	被験者登録に関する書き込み権限
GEN-ADMIN：	プロトコルの作成及びマイルストーンに関する管理者権限
QA：	標準業務手順書の管理に関する書き込み権限
RANDOM-TABLE：	二重盲検デザインの処置群に関する管理者権限
READ-ADDRESS：	被験者パネルの個人情報の読み取り権限
SCHEDULE-OCC：	オケージョンのスケジュリングに関する書き込み権限
STUDY-ADMIN：	経理に関する機能への管理者権限
STUDY-DESIGN：	プロトコルの作成に関する書き込み権限
SUBJ-ADMIN：	被験者パネルの個人情報の書き込み権限
SYSTEM-MANAG：	システム設定に関する書き込み権限
VALIDATE-SUB：	被験者の組み入れに関する管理者権限

上記のユーザーグループ「RANDOM-TABLE」のみ特殊で、**MENU** タブでの設定に加え、**REPORTS** タブで盲検下における被験者の割り付けに関するレポートが出力できるように設定されています。なお、**PROTOCOLS** 及び **STUDY CENTRES** タブでもアクセス権限の設定は行えますが、インストール直後はプロトコル及び実施施設が定義されていないため、既定のユーザーグループにも含まれていません。

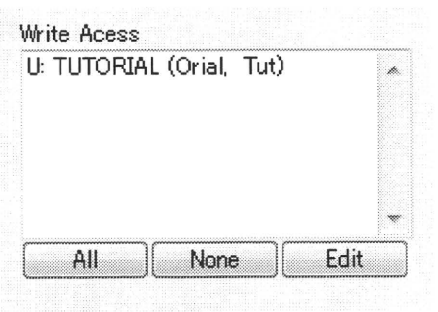
尚、既定のユーザーグループには、読み取り権限を与えるユーザーグループが一つしかないことが分かります。既定の設定では、多くのモジュール・タブへの読み取り権限は全ユーザーに与えられています。

5　アクセス権限の付与

本章では、作成したユーザーアカウントやユーザーグループに各種権限を付与する方法について説明します。ユーザーアカウント（**USERS** タブ）、ユーザーグループ（**GROUPS** タブ）でのみで設定できる諸権限については、第 3 章及び第 4 章で説明しています。本章で取り扱うアクセス権限は、ユーザーアカウントとユーザーグループの両方に割り当てることが可能です。一般的には、**PROTOCOLS** 及び **STUDY CENTRES** へのアクセス権限はユーザーアカウント単位で、**MENU** 及び **REPORTS** へのアクセス権限はユーザーグループ単位で割り当てますが、システム上の制限はありません。

5.1　基本的な操作

設定が行えるタブが 4 つありますが、基本的なアクセス権限の設定方法は同一で、下図のフィールドから行われます。**REPORTS** タブを除く全てのタブでは、下図のフィールドが読み取り、書き込み、及び管理者権限の設定用に 1 つずつ設けられています。

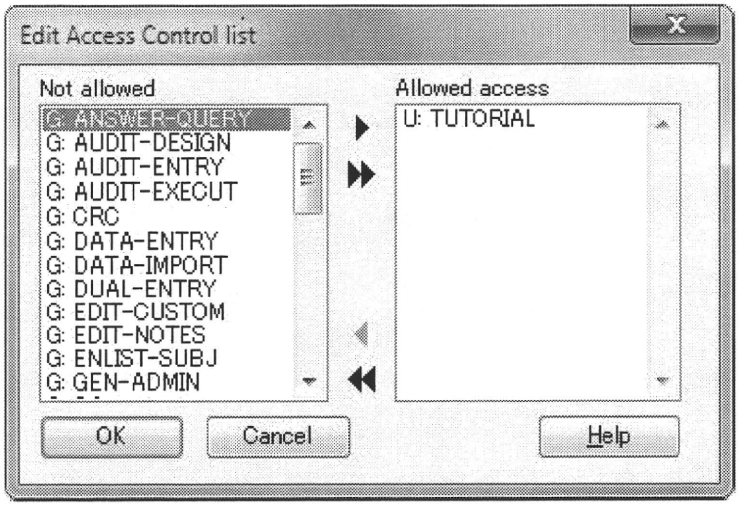


① アクセス権限の設定を行うには、フィールドの下に表示される All、None、Edit ボタンをクリックします。

All：登録されている全てのユーザーアカウント・グループにアクセス権限が付与されます。

None：アクセス権限は如何なるユーザーアカウント・グループにも付与されません。この設定を行うと、実質的には、All rights が有効になっているユーザーアカウント・グループのみがアクセスを許可されている状態になります。

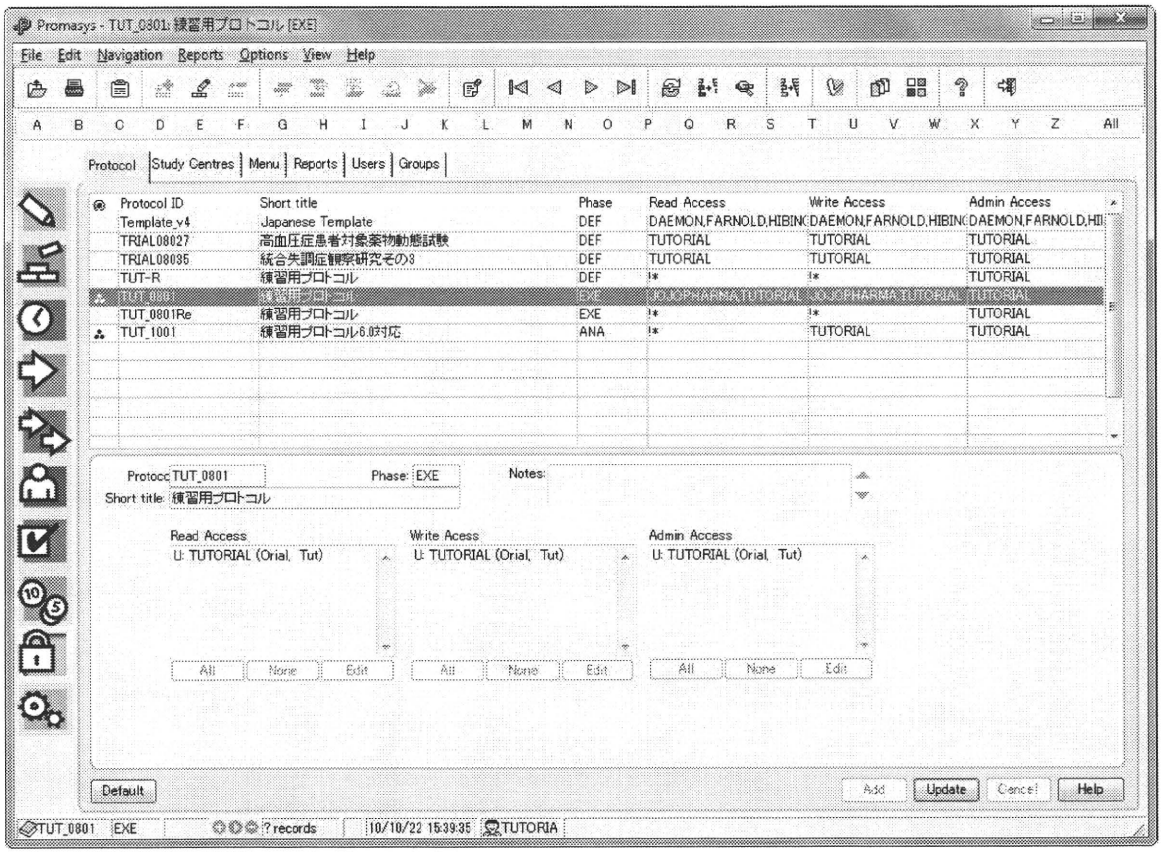
Edit：「Edit Access Control list」子ウィンドウが展開し、アクセス権限をユーザーアカウント・グループ単位で付与できます。



② Edit をクリックして展開する「Edit Access Control list」には、Not allowed と Allowed access の二つの一覧が表示され、この中でユーザーアカウントの先頭には「G」と、ユーザーアカウントの先頭には「U」と表示されます。アクセスを許可するユーザーアカウント・グループを Not Allowed の一覧でクリックしてハイライトします。複数のユーザーアカウント・グループを同時に割り当てる場合は、キーボードの CTRL キーを押しながら他のユーザーアカウント・グループをクリックします。▶ボタンをクリックすると、ハイライトされたユーザーアカウント・グループが Allowed access へ移動します。アクセスの許可を取り消すには、Allowed access から取り消すユーザーアカウント・グループを選択し、◀ボタンをクリックします。確定するには、OK をクリックします。

アクセス権限の設定は基本的に以上の 2 ステップからなります。本章の残りでは、各タブにおける設定について解説しますが、重複を避けるため実際の付与の手順については上記の説明を参照下さい。

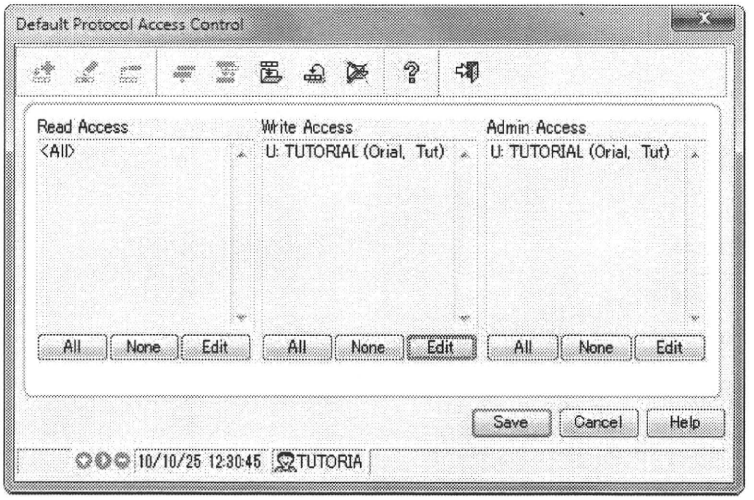
5.2 プロトコル



各プロトコルへのアクセス権限は、**ACCESS CONTROL** の **PROTOCOLS** タブで設定します。
ウィンドウの上部分にプロトコルの一覧が表示されます。一覧からアクセス権限の設定を行うプロトコルを選択し、ウィンドウ右下 Update をクリックします。Update クリック後は、Read Access、Write Access、Admin Access の各フィールドが編集可能になります。以後は、上記 5.1 の手順でアクセス権限を設定し、その後 Save をクリックし、変更を確定します。

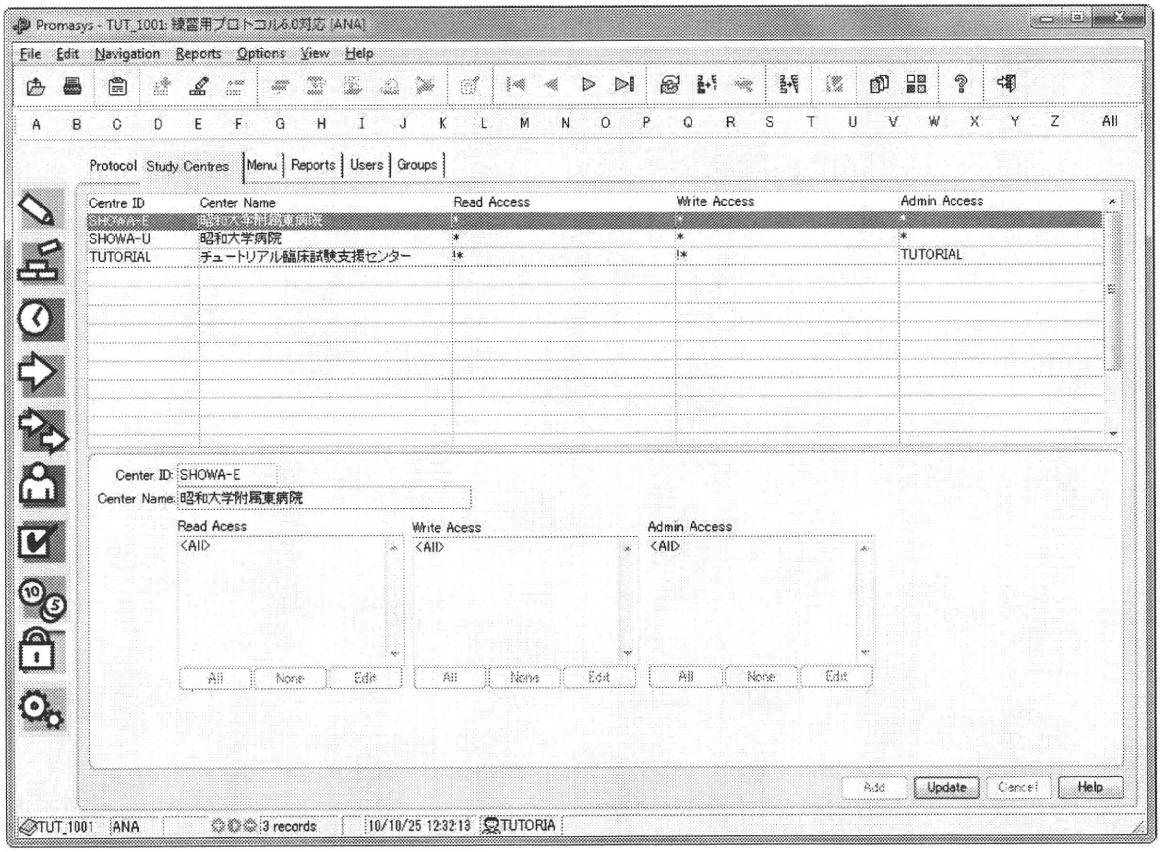
5.2.1 既定のアクセス権限を変更する

プロトコルの（**GENERAL ADMINISTRATION > PROTOCOLS** での）新規作成時、プロトコルへのアクセス権限はシステムの既定の設定に準じます。この設定を変更する場合、**ACCESS CONTROL** モジュールの **PROTOCOL** タブでウィンドウ左下 Default をクリックします。「Default Protocol Access Control」子ウィンドウが展開します。



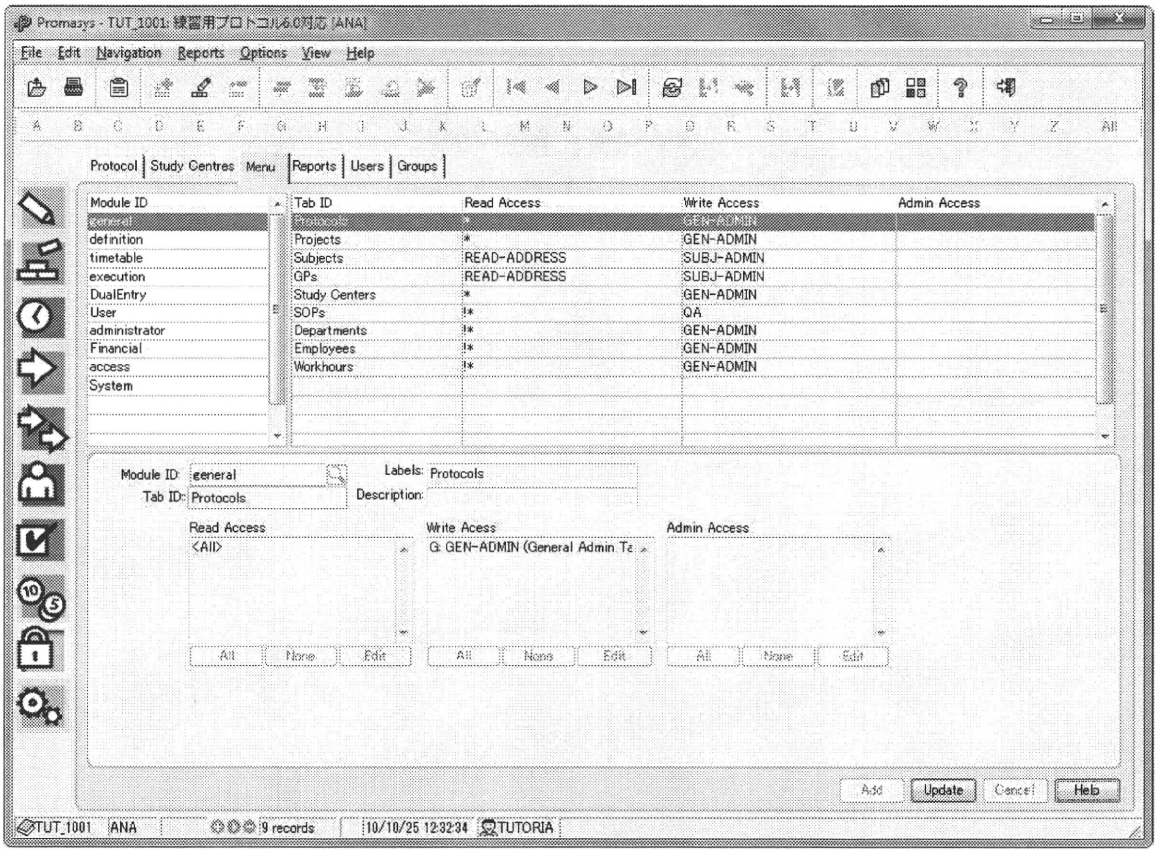
設定方法は、通常のアクセス権限の設定と同様です。ウィンドウ右下の Update をクリックし、上記 5.1 の手順でアクセス権限を設定した後、Save をクリックして既定の設定を保存します。Admin 欄に管理者レベルのユーザーアカウントを最低一つは設定していないと、**GENERAL ADMINISTRATION > PROTOCOLS** でプロトコルを新規作成した場合、アクセス権限を設定するのに All rights 属性が有効になっているアカウントが必要になってしまいます。

5.3 実施施設



GENERAL ADMINISTRATION モジュールの **STUDY CENTRES** タブで定義される各実施施設へのアクセス権限の設定は、**ACCESS CONTROL** の **PROTOCOLS** タブで設定します。ウィンドウの上部分に実施施設一覧が表示されます。一覧からアクセス権限の設定を行う実施施設を選択し、ウィンドウ右下 Update をクリックします。Update クリック後は、Read Access、Write Access、Admin Access の各フィールドが編集可能になります。以後は、上記 5.1 の手順でアクセス権限を設定し、その後 Save をクリックし、変更を確定します。

5.4 モジュール・タブ



プロマシスの各機能へのアクセス権限は、**ACCESS CONTROL** の **MENU** タブで設定します。プロマシスでは、機能の大半がモジュール・タブ単位で管理されているため、プロマシスの各機能へのアクセス権限は、ユーザーアカウント・グループに付与されている各モジュール・タブへのアクセス権限に準じます。プロマシスのデータ入力用の eCRF や WebCRF インターフェースにおいても、各モジュール・タブへのアクセス権限がそのまま反映されます。例えば、WebCRF で被験者をプロトコルに登録するには、**EXECUTION** モジュールの **ENLISTMENTS** タブへの書き込みアクセスが許可されている必要があります。

ACCESS CONTROL の **MENU** タブではウィンドウの左上部分にモジュールが表示され、右上部分に現在選択中のモジュールの各タブ及び各タブのアクセス権限の設定が表示されます。一覧からアクセス権限の設定を行うタブを選択し、ウィンドウ右下 Update をクリックします。Update クリック後は、Read Access、Write Access、Admin Access の各フィールドが編集可能になります。以後は、上記 5.1 の手順でアクセス権限を設定し、その後 Save をクリックし、変更を確定します。