FileMaker
セキュリティガイド

アプリの安全を守る鍵

目次

FileMaker How To Guide – アプリの安全を守る鍵

FileMaker Pro および FileMaker Server でセキュリティのオプションを構成するベストプラクティス

この情報ガイドでは、FileMaker Platform を使用してアプリを作成、管理、展開する際に、それぞれの組織のセキュリティ上のニーズを満たすためのベストプラクティスについて概説します。考慮に入れなければならない原則が 3 つあります。

- 機密性 — 許可されていない人がデータにアクセスできないようにする責任があります。
- 整合性 — 意図しない変更を防ぎながら、許可されたユーザーがデータを作成および更新できるようにする責任があります。また、ファイルを改ざんする可能性のある許可されていないユーザーのアクセスを制限しなければなりません。
- 可用性 — ユーザーが必要とする時にデータを使用できるようにする責任があります。

このガイドでは、FileMaker プラットフォームに組み込まれたセキュリティを用いてアプリを保護する方法を、ステップごとに説明していきます。それぞれのセキュリティに関するコンプライアンスと認証の要件に応じて、追加のステップが必要な場合もあります。そのような要件の詳細は、各自で確認してください。

注: このガイドでは、保護したいファイルがすでに作成されているものとして説明を進めます。

概要

FileMaker プラットフォームは、FileMaker ファイル内のデータアクセス、操作、開発の制御に役立つとともに、 たとえ共有環境であっても監査と規制コンプライアンスの要件を満たす役割を果たす完全なツールセットを提供しています。主な機能には次のものがあります。

- 強力な認証。 FileMaker Pro ファイル内に保管されるクリデンシャルはいったん暗号化されると、その後は復号されることはありません。
- 外部認証。 ユーザーを Active Directory または Open Directory を用いて認証することができます。
- きめ細かい制御。 誰が見て何をできるかを、テーブル、レイアウト、レコード、さらに個々のフィールドレベルまで、細かく決めることができます。
- データ転送の暗号化。FileMaker Server と FileMaker Pro または FileMaker Go との間でデータを暗号化するために、SSL を要求することができます。さらに、第三の認証機関（Certificate Authority: CA）からの署名付き証明書を使用することができます。.

FileMaker プラットフォームは統一されたセキュリティモデルを採用しており、ファイルに確立するセキュリティは、すべてのクライアント—iPad、iPhone、Windows、Mac、Web—で有効です（図 1）。ファイルが FileMaker Server でホストされる場合、FileMaker Server を使用して FileMaker Server とディレクトリサーバー、他のデータベース、および Web サーバーとの間で確立するセキュリティは、FileMaker Server でホストされるすべてのファイルに適用されます。

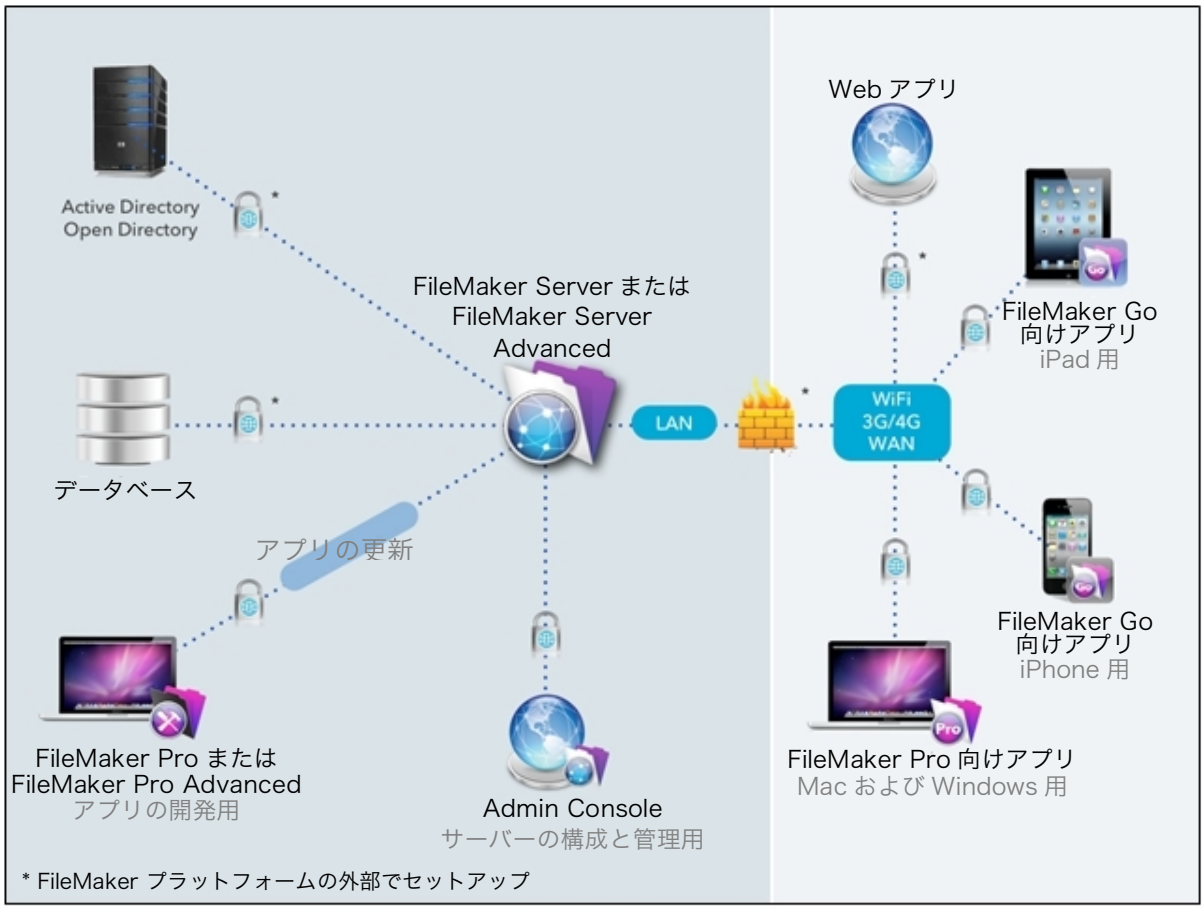

図 1. 単一マシンの FileMaker Server で展開する高水準セキュリティダイアグラム

FileMaker のセキュリティモデルは、次の 3 つの主要コンポーネントに基づいています。

1. アカウント名 – 個々のユーザーを識別
2. パスワード – ユーザーが本人であることを証明
3. アクセス権セット - ユーザー（1 人または複数）のアクセス制限を定義

アカウント名と パスワードは、各個人のファイルへのアクセスを制御します。情報セキュリティのコンプライアンスガイドラインでは、アカウント名とパスワードをまとめて ID（アイデンティティ）と呼んでいます。

アクセス権セットは、ユーザーが何を見られるか、また何をできるかを制御します。アクセス権セットを使用することによって、情報セキュリティのコンプライアンスガイドラインで役割ベースのセキュリティと呼ばれているものを定義することができます。

FileMaker Pro を使用してファイル内で定義されたセキュリティの設定は、ほとんどの場合、ファイル固有のものです。1 つのファイル内で確立されたアカウントとアクセス権セットは、そのファイルに保管されている情報とスキーマへのアクセスを制御します。

FileMaker Server 内で構成されたセキュリティの設定は、サーバー固有のもので、そのサーバーによってホストされるすべてのファイルに適用されます。

FileMaker Pro または FileMaker Pro Advanced でセキュリティを構成する

以下のセクションでは、FileMaker Pro または FileMaker Pro Advanced でファイルのセキュリティをセットアップする手順の概要を説明します。

パスワードの入力を求めるプロンプトを出す

FileMaker Pro で新規ファイルを作成すると、そのファイルを開く際にユーザーのアカウントとパスワードの入力を求めるプロンプトは自動的に出されません。何よりも先に、以下の手順に従ってこれを変更してください。

1. [ファイル] メニュー > [ファイルオプション] を選択します。
2. [次のアカウントを使用してログイン] のチェックをはずします。
3. [OK] をクリックします。

ファイルオプションの設定について詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/create_db.8.6.html - 172022

Admin アカウントにパスワードを指定する

FileMaker Pro で新規ファイルを作成すると、完全アクセス Admin アカウントが自動的に作成されます。

この完全アクセス Admin アカウントにはパスワードが設定されていません。そのため、他の作業をする前にこのアカウントにパスワードを割り当て、データおよびデータベース構造への無許可のアクセスを防ぐことが大切です。

Admin アカウントの名前を変更するには、以下の手順に従ってください。

1. [ファイル] メニュー > [管理] > [セキュリティ] を選択します。
2. [アカウント] タブから Admin アカウントを選択し、[編集] をクリックします。
3. Admin のアカウント名を変更し、パスワードを追加します。必ず、大文字と小文字および数字を含んだ複雑なパスワード規則に従ってください。

既存アカウントの編集について詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/passwords.14.11.html - 521206

アクセス権セットを作成する

アクセス権セットは、ユーザーが見られるものおよびできることへのアクセス権を設定します。アクセス権セットを使用すると、データおよびスキーマ（レイアウト、フィールド、テーブル、スクリプティング）へのアクセスを制御することができます。

新しいすべての FileMaker ファイルには、あらかじめ定義された次の 3 つのアクセス権セットが用意されています。

1. 完全アクセス - すべての開発機能を含めて、ファイルへの完全アクセスが許可されます。
2. データ入力のみ - レコードの作成、編集、削除、およびデータのインポートとエクスポートが許可されます。開発機能へのアクセスは許可されません。
3. 閲覧のみアクセス - レコードデータの表示とエクスポートが許可されます。ファイルの変更は許可されません。

拡張アクセス権を有効または無効にする以外、あらかじめ定義されているアクセス権セットを変更したり削除したりすることはできません。

あらかじめ定義されているアクセス権セットが各自のニーズに合っているかどうかを確認するために、これらのアクセス権セットをよく理解してください。現段階ではこれらの 3 つのオプションが自分のニーズに合っていると思う場合は、 認証のためにアカウントまたは外部サーバーグループをセットアップするに直接進んでもかまいません。

各自の特定の要件に合わせて、新しいアクセス権セットを作成することもできます。通常、組織内のそれぞれの役割に合った、以下のアクセスオプションで構成されるアクセス権セットを作成します。

- データアクセスとデザインのアクセス権 - レコード、レイアウト、値一覧、スクリプトを含む、幅広いセキュリティ制御へのアクセスが提供されます。
- 拡張アクセス権 - ファイル内のアクセス権セットで許可されるデータ共有オプションが決定されます。
- その他のアクセス権 - 印刷、エクスポート、および他の一部の機能が許可されます。

新しいアクセス権セットを作成するには、以下の手順に従ってください。

1. [ファイル] メニュー > [管理] > [セキュリティ] を選択します。
2. [アクセス権セット] タブから [新規] ボタンをクリックします。

また、既存のアクセス権セットを複製し、それを各自のニーズに合わせて変更することによって、時間を節約することもできます。その場合は 1 つのアクセス権セットを選択し、 [複製] ボタンをクリックしてから、[編集...] ボタンをクリックします（図 2）。どちらの場合も [アクセス権セットの編集] ダイアログが表示され、アクセス権セットを定義または変更することができます（図 3）。

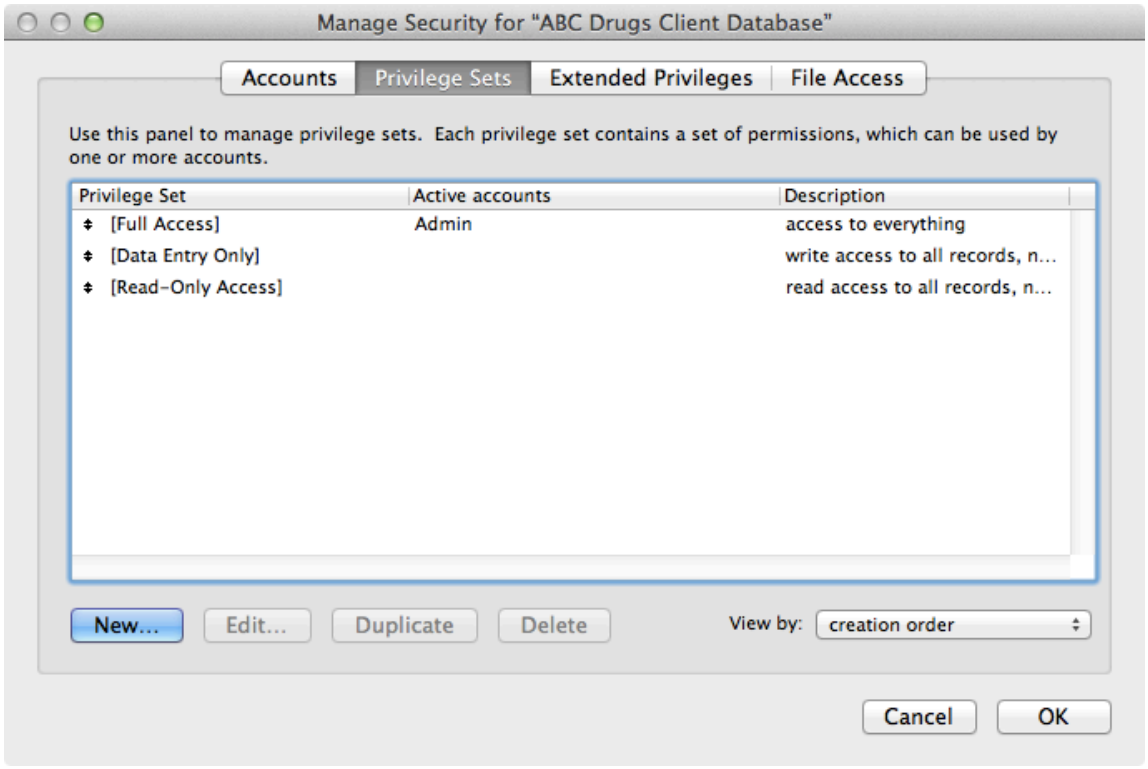

図 2. [アクセス権セット] タブで、アクセス権を作成、編集、複製することができます。

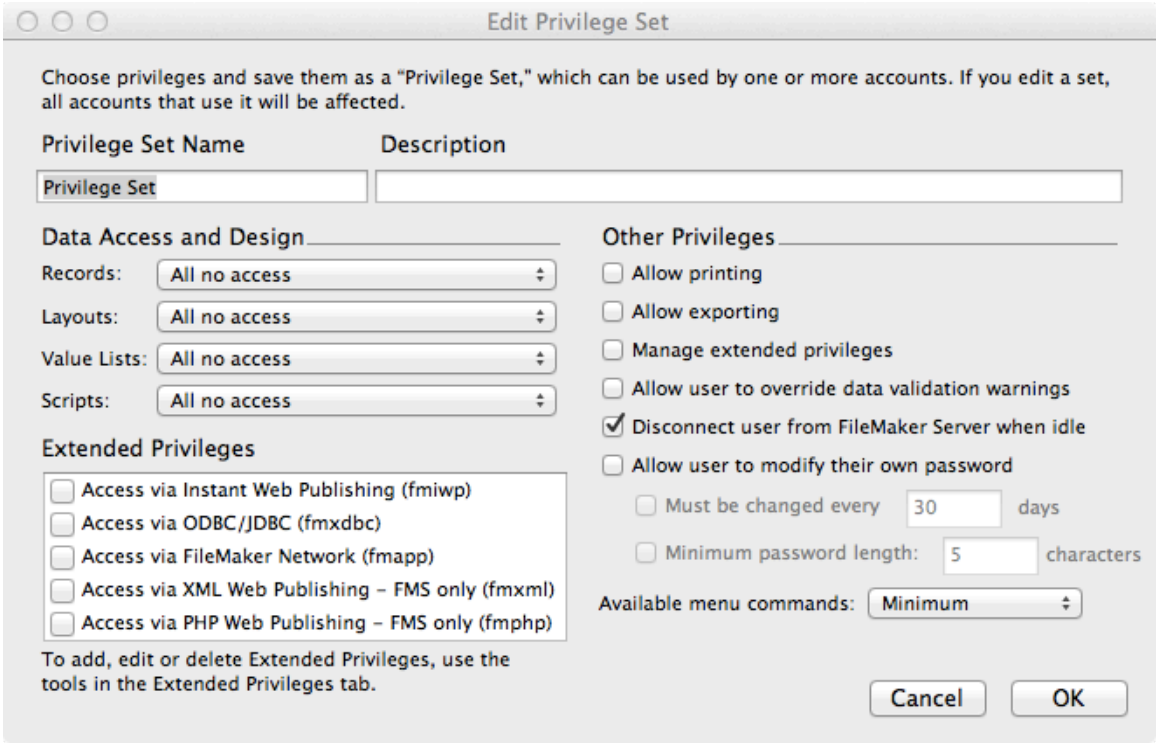

図 3. [アクセス権セットの編集] ダイアログで、そのセットに許可したいアクセス権を選択してから、[OK] をクリックします。

アクセス権セットを作成または編集すると、現在接続されているユーザーに影響を与える場合と与えない場合があります。他のユーザーが共有ファイルを使用中には、そのファイルのアクセス権セットを変更しないことが推奨されます。

アクセス権セットの作成と管理について詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/passwords.14.15.html - 521463

データアクセスとデザインのアクセス権を定義する

[データアクセスとデザイン] のセクションでは、それぞれのドロップダウンを使用して、すべてのテーブル、レイアウト、値一覧、スクリプトへのアクセスを機能ベースで許可することができます。

デフォルトでは、ほとんどすべてのアクセス権が無効になっています。これによって「最小特権の原則」を適用することができます。最小特権の原則とは、ユーザーには各自の役割を果たすために必要なすべての特権を与えるが、それ以上は与えるべきではないというものです。

各ドロップダウンには、[カスタムアクセス権] のオプションもあります。[カスタムアクセス権] では、アクセス権をさらにきめ細かく制御することができます。

[カスタムレコードアクセス権] は、テーブルごと、またはレコードごとにユーザーアクセスを制御する必要がある場合に便利です。たとえば CRM システムで、販売のマネジメントはすべてのレコードを閲覧でき、各販売担当員は自分が担当する顧客または見込み客のレコードのみを閲覧できるようにすることができます。

[カスタムレイアウトアクセス権] では、ユーザーがレイアウトを表示または変更する権利を制御するとともに、ユーザーがそのレイアウト上でレコードを表示または変更できるかどうかも制御することができます。FileMaker プラットフォームは常に、最も安全なアクセス規則の組み合わせを使用します。一般的にレコードを編集できるユーザーは、それらのアクセス権を許可していないレイアウト上では編集することができません。

[カスタムアクセス権] を使用すると、それぞれの値一覧またはスクリプトについて、ユーザーがそれを表示または実行できるか、変更または削除できるか、または新規に作成できるかを決定することもできます。

拡張アクセス権を定義する

拡張アクセス権によって、共有ファイルにアクセス可能かどうかと、共有ファイルへのアクセス方法が決まります。ファイルに対して、次のどのアクセス権セットを許可するかを設定することができます。

ダイアログボックス内のキーワード	説明
fmiwp	WebブラウザからインスタントWeb公開を利用してデータベースファイルにアクセス
fmxdbc	データベースファイルにODBCまたはJDBCデータソースとしてアクセス
fmapp	FileMaker ProまたはFileMaker Goで共有ファイルにアクセス
fmreauthenticate[X]	ユーザーが使用を中断してから再認証を求められるまでの時間を設定 —FileMaker Goクライアントのみ
fmxml	XML Web 公開によるアクセス – FileMaker Serverのみ
fmphp	PHP Web公開によるアクセス – FileMaker Serverのみ

アクセス権セットを編集する場合、そのアクセス権セットの拡張アクセス権を有効または無効に設定することができます（図 3 の左下隅を参照）。

[拡張アクセス権] タブをクリックすることで、拡張アクセス権を一度に複数のアクセス権セットに割り当てることもできます。拡張アクセス権を選択して、[編集...] をクリックします（図 4）。次に、その拡張特権を割り当てたいアクセス権セットのボックスをチェックします（図 5）。

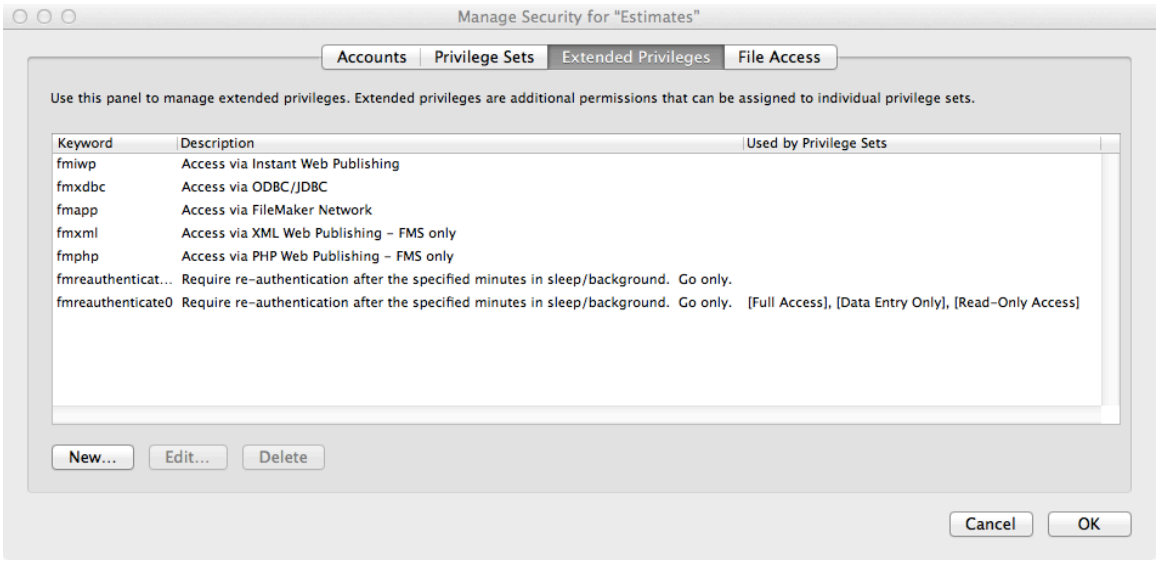

図 4. [拡張アクセス権] タブをクリックして、拡張アクセス権を管理します。

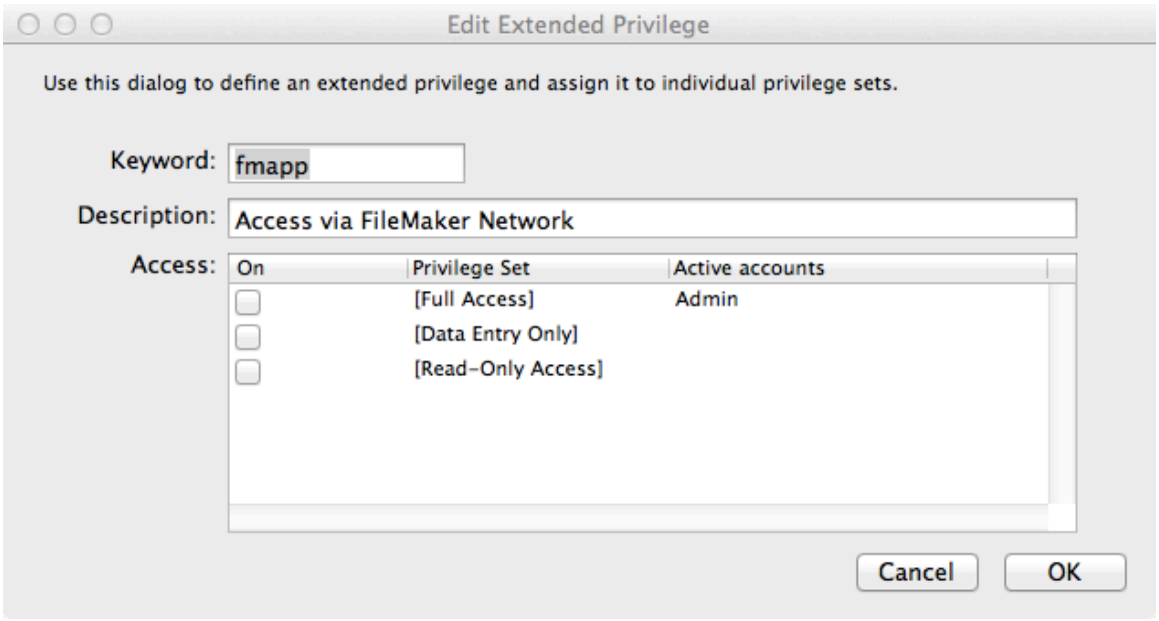

図 5. 拡張アクセス権を編集し、それを各アクセス権セットに割り当てます。

アクセス権セットに拡張アクセス権を有効にすると、そのアクセス権セットに接続されているすべてのアカウントが、拡張アクセス権によって指定された方法でファイルにアクセスできるようになります。

iPad および iPhone に関する重要事項:

ユーザーが iOS デバイスを使用することが考えられる場合には、fmreauthenticate[X] 拡張アクセス権を指定すると便利です。

FileMaker Go for iPad ／iPhone ではマルチタスクが可能です。iOS デバイスを使用している場合、ユーザーはいつでも電話に出たり、別のアプリに移動したりできます。この場合、FileMaker Go はバックグラウンドに移動し、ファイルの状態を保存します。fmreauthenticate[X] 拡張アクセス権が有効な場合、FileMaker Go がフォアグラウンドに切り替わる時点で、指定された制限時間の [X] 分が経過していれば、ユーザーはアカウント名とパスワードをもう一度入力しなければなりません。たとえば拡張アクセス権の fmreauthenticate10 では、ユーザーは最大 10 分まで FileMaker Go の使用を中断しても、再認証を求められません。このような拡張アクセス権は、必要に応じて異なる時間で任意の数だけ作成でき、異なるアクセス権セットに割り当てることができます。ユーザーはアカウント名とパスワードの入力を 5 回まで試みることができ、それを超えると FileMaker Go はファイルを閉じます。

カスタム拡張アクセス権を作成して、スクリプトを単純化することもできます。これらのカスタム拡張アクセス権を使用して、適用したいビジネスルールの管理に役立てることができます。たとえばレポート作成機能などがあります。独自の拡張アクセス権を作成するには、[拡張アクセス権] タブから [新規] をクリックし、名前と説明を入力します。

拡張アクセス権の管理について詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/passwords.14.26.html - 522737

その他のアクセス権を定義する

その他のアクセス権には、アクセス権セットがユーザーに以下を許可するかどうかが含まれます。

- 印刷
- エクスポート
- 拡張アクセス権の管理
- データ検証の警告の無視
- アイドル状態のユーザーの FileMaker Server からの接続解除
- ユーザーによるパスワードの変更
- メニューコマンドの利用（すべて、編集のみ、最小）

「印刷」には、印刷と、レコードの PDF ファイルとしての保存の両方が含まれます。

「エクスポート」には、レコードのエクスポート、レコードの Excel ファイルとしての保存、対象レコード内のすべてのレコードのクリップボードへのコピー、 FileMaker ファイルからのレコードのインポート、レコードのコピーの保存、Apple Events でのデータの使用（GetCellValue、Field Contents、Record Value、Table Contents、Layout Contents）が含まれます。

「アイドル状態のユーザーの FileMaker Server からの接続解除」には、FileMaker Server でのセットアップも必要になることに注意してください。

その他のアクセス権について詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/passwords.14.25.html#522588

認証のためにアカウントまたは外部サーバーグループをセットアップする

アクセス権セットを定義した後、アカウントの作成を開始することができます。アカウントは、保護されたファイルを開こうとしているユーザーを認証します。認証はユーザーの ID を判別して検証します。

各データベースファイルには、最初に Admin とゲストの 2 つのアカウントが含まれています。

Adminアカウントには、FileMaker内のすべての情報にアクセスできる [完全アクセス] アクセス権セットが割り当てられています。 このアカウントは完全に編集可能です。名前を変更したり、パスワードを割り当てたり、アカウントを非アクティブにしたり、Adminアカウントそのものを削除したりすることができます（ただし、ファイルには少なくとも1つの完全アクセスアカウントが必要です）。デフォルトでは、Adminアカウントにはパスワードがないため、最初にそれを変更する必要があることを忘れないでください。

ゲストアカウントでは、ユーザーがアカウント情報を入力せずにファイルにアクセスすることができます。デフォルトでは、ゲストアカウントには [閲覧のみアクセス] アクセス権セットが割り当てられていますが、ゲストアカウントには必要な任意のアクセス権セットを割り当てることができます。

ゲストアカウントは最初、非アクティブになっています。ゲストアカウントに対応する [アクティブ] の欄にあるチェックボックスにチェックを入れることで、そのゲストアカウントを有効にすることができます（ 図5）。このアカウントは完全には編集できません。ゲストアカウントを削除したり、ゲストアカウント名を変更したり、パスワードを割り当てたりすることはできません。

新しいアカウントを作成するには [新規...] ボタンをクリックします（図 6）。既存のアカウントを編集するには、そのアカウントを選択してから [編集...] ボタンをクリックします。

アカウントを作成する場合、アカウント名とパスワードを指定し、そのアカウントにアクセス権セットを割り当てます。アカウント名では大文字と小文字は区別されませんが、パスワードでは大文字と小文字が区別されます。ユーザーのパスワードの機密性を維持する必要があるため、必ず [ユーザーは次回ログイン時にパスワードの変更が必要] のボックスにチェックを入れてください（図 7）。これを使用すると、ユーザーがパスワードを忘れた場合にパスワードをリセットすることもできます。ただし、ユーザーがパスワードを変更できるのは FileMaker Pro または FileMaker Go からファイルにアクセスしている場合のみで、Web ブラウザからパスワードを変更できるようにするスクリプトを作成しない限り、Web ブラウザからは変更できないことに注意してください。

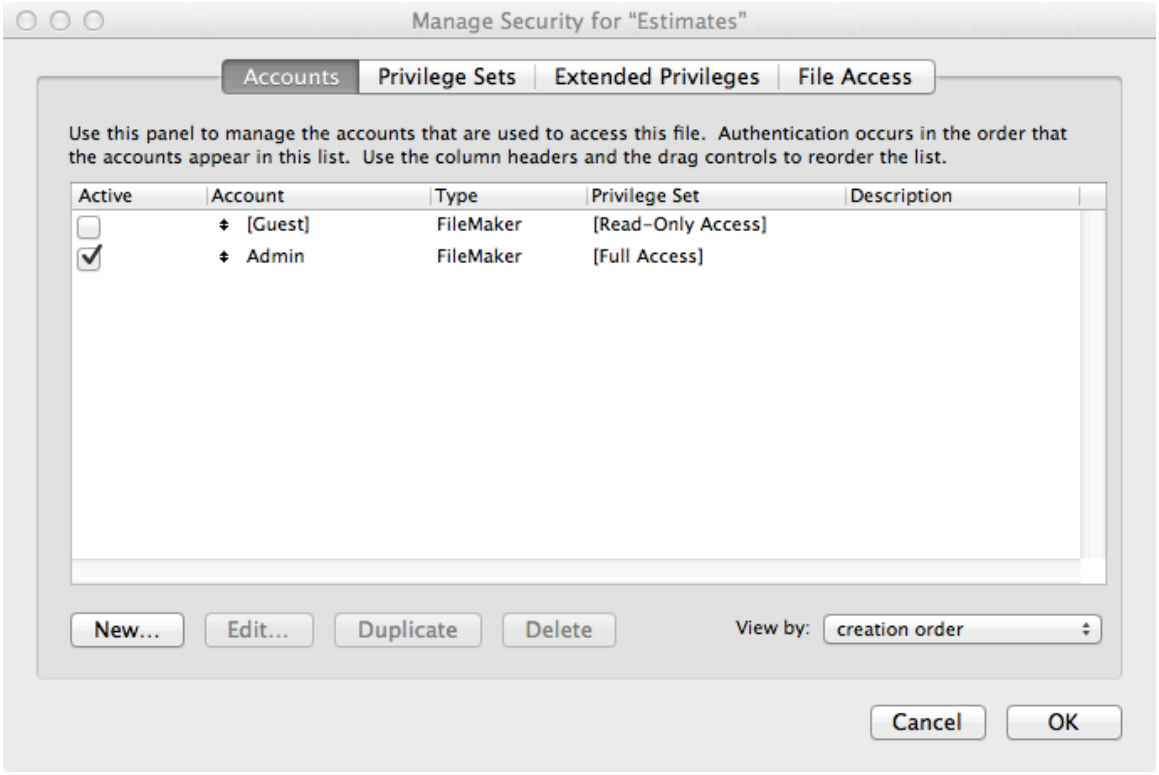

図 6. アカウントを作成、編集、および削除します。

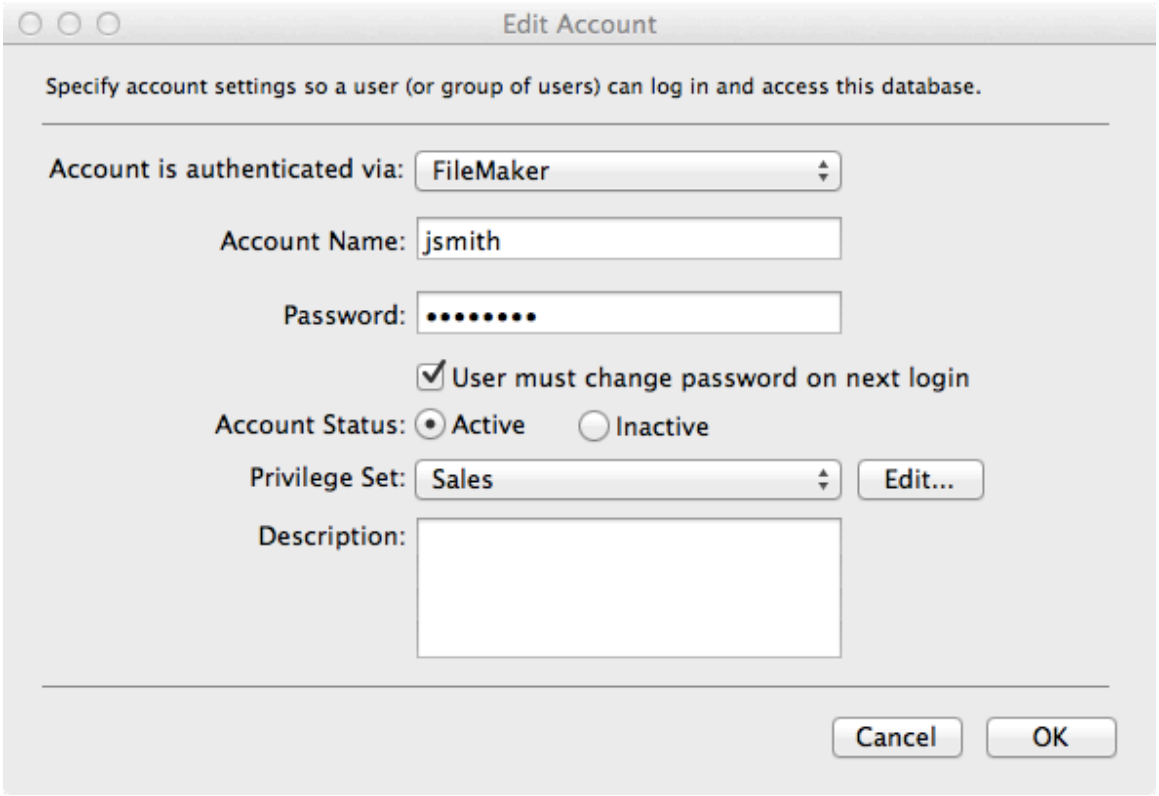

図 7. アカウント名、一時パスワード、アクセス権セットを指定します。

アカウントの作成について詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/passwords.14.10.html - 521108

FileMaker ServerまたはFileMaker Server Advancedを使用してファイルをホストする場合、Active DirectoryまたはOpen Directoryによって認証する外部サーバーアカウントを作成することができます。これによって、各FileMaker Proデータベースファイルで独立したアカウントの一覧を管理しなくても、既存の認証サーバーを使用してデータベースへのアクセスを制御することができます。

あるいは、FileMaker Serverをホストしているサーバーマシン上でローカルのセキュリティグループおよびアカウントを使用することもできます。詳細については、使用しているOSのヘルプファイルを参照してください。

外部認証は、以下の場合に特に適しています。

- 組織ですでにActive DirectoryまたはOpen Directoryを使用している。
- FileMakerファイルが複数ファイルソリューションの別のファイルによってアクセスされる。
- 組織がパスワードの最低基準を定めている。FileMaker Proでは、パスワードの長さと変更の頻度など、基本的な基準を強制することができます。外部認証ではさらに強力なパスワードの制御が提供されます。

さらに、Windows Server OS 上にインストールされた FileMaker Server を使用してファイルをホストし、外部認証に Active Directory を使用すると、Windows のユーザーはシングルサインオンを利用できます。

外部認証を使用する場合、誰かが外部認証環境をシミュレートするかグループを不適切に管理することによって、ファイルにアクセスできるリスクがあります。各自の責任において外部認証サーバーのセキュリティを保守し、これを防ぐ必要があります。

外部認証を使用するためには、FileMaker Pro を使用してファイル内に外部認証アカウントをセットアップする必要があると ともに 外部認証用に構成された FileMaker Server を使用してファイルをホストする必要があります。FileMaker Server の構成手順については、このガイドの 外部認証を有効にするのセクションを参照してください。

外部認証を実施するには、以下の手順に従ってください（図 8）。

1. [アカウント] タブで [新規] ボタンをクリックします。
2. [アカウントの編集] ダイアログボックスで、[アカウントの認証方法:] から [外部サーバー] を選択します。
3. [グループ名:] に、外部認証サーバーで定義されているグループ名を入力します。グループ名では大文字と小文字が区別されることに注意してください。Open Directory を使用している場合は、グループ名には必ずショートネームの形式を使用してください。
4. 追加する外部認証グループのそれぞれについて、これらの手順を繰り返します。

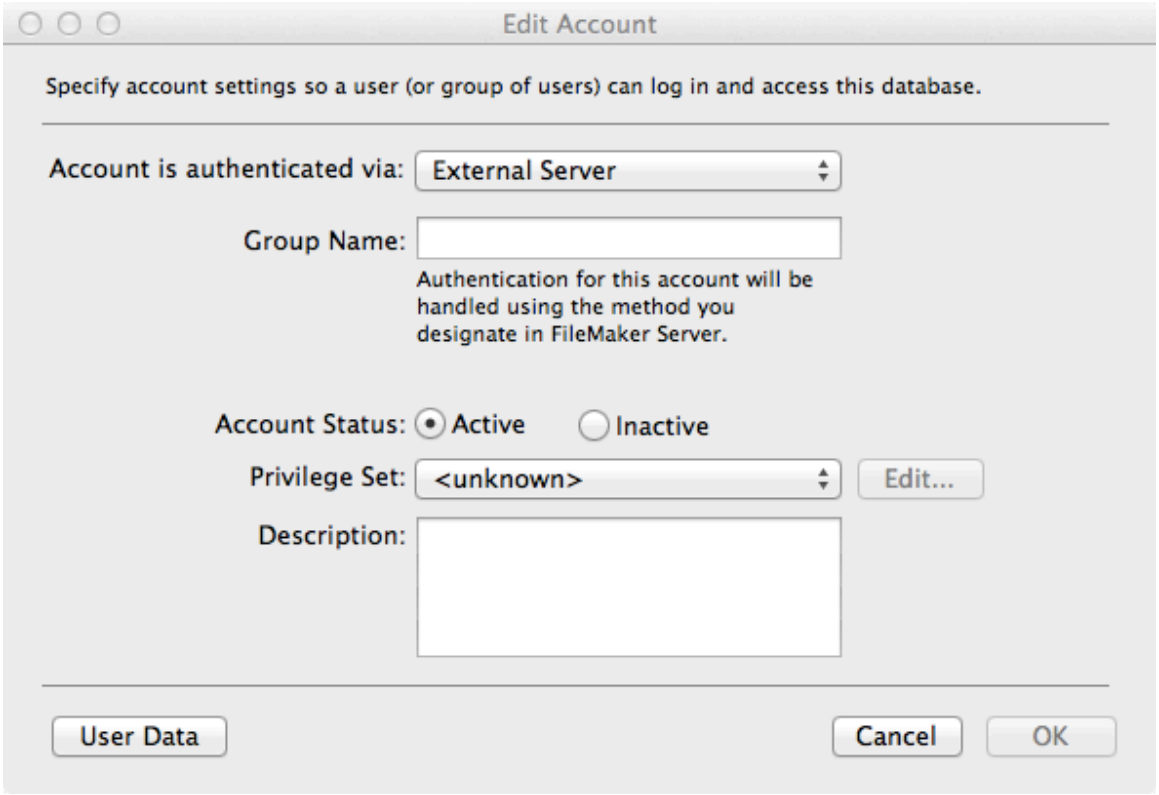

図 8. アカウントを Open Directory または Active Directory で認証することができます。

ユーザーが自分のパスワードを忘れた場合、外部認証サーバーを使用してそのパスワードをリセットする必要があります。

外部サーバーで認証するアカウントの作成について詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/passwords.14.13.html#521341

外部認証を使用する場合に重要な事項:

外部認証を有効にしている場合、アカウント名とパスワードがローカルFileMakerアカウントおよび外部アカウント、また複数のグループに属する外部アカウントのものと同じになる可能性があります。この場合、FileMaker Proは認証順序で最初に一致するアカウントを使用してファイルを開きます。最初のもの以降に一致するアカウントがあっても、それらは無視されます。そのため、上記の一方または両方の状況が存在する場合には、アカウントの認証順序を設定することが重要になります。認証順序を正しく設定しておかないと、ファイルへのアクセスに間違ったアカウントが使用される可能性があります。認証順序は、[アカウント] タブの [表示順:] メニューを使用して表示および変更することができます（図6）。ベストプラクティスとして、認証順序を心配しなくてすむよう、外部アカウントとローカルFileMakerアカウントの重複した使用を避けるようにしてください。さらに、認証順序は複数の外部認証グループに所属する人にも使用されます。

外部認証される完全アクセスアカウントを作成せず、その代わりに、何らかの理由でFileMaker Serverからファイルを除去する必要が生じた場合のために管理の目的で使用できるローカルFileMakerアカウントを維持しておくのが適切な方法です。ローカルFileMakerアカウントがないと、ファイルがホストされない場合に開くことができなくなります。

[ファイルアクセス] を使用してファイルへのアクセスを許可する

FileMaker ファイルには、複数ファイルソリューション内で相互にアクセスすることができます。これはたとえば、中核となるアクセス可能な社員連絡先情報ファイルがあって、人事、販売、業務などの各種の社内アプリでそれを使用するような場合に便利です。

複数ファイルソリューションでは、各ファイルについてアクセス権を注意深く検討することが大切です。綿密さに欠けると、たとえばユーザーが ある 1 つのファイルでは設定されたアクセス権セットによりそのファイル内のリストを印刷できないのに、複数ファイルソリューションの別のファイルからは同じリストを印刷できるような場合が生じます。

セキュリティが確立されたソリューションでは、ファイル内のスキーマ（テーブル、レイアウト、スクリプト、値一覧を含む）に対する別のFileMaker Proファイルからのアクセスを許可するかどうかを制御することができます。保護が有効になっていると、ファイルのメタデータを含み、FileMakerのデータソースを通して保護されたファイルを使用するにはまず完全アクセスの認証が必要になります。

許可対象の各ファイルには固有のIDが割り当てられて、保護対象のファイルはそれを追跡し、保護対象のファイルが名前変更または複製されてもなお確実に保護されるようにします。認証されたファイルを別のファイルで置き換えるなどして認証を迂回しようとしても、成功しません。

ファイルアクセスを制限するには、[ファイルアクセス] タブをクリックし、[このファイルへの参照の使用に完全アクセス権を要求する] にチェックを入れます。次に、[認証...] をクリックしてからファイルを選択し、 ソリューションの一部である他のファイルを認証します（図 9）。

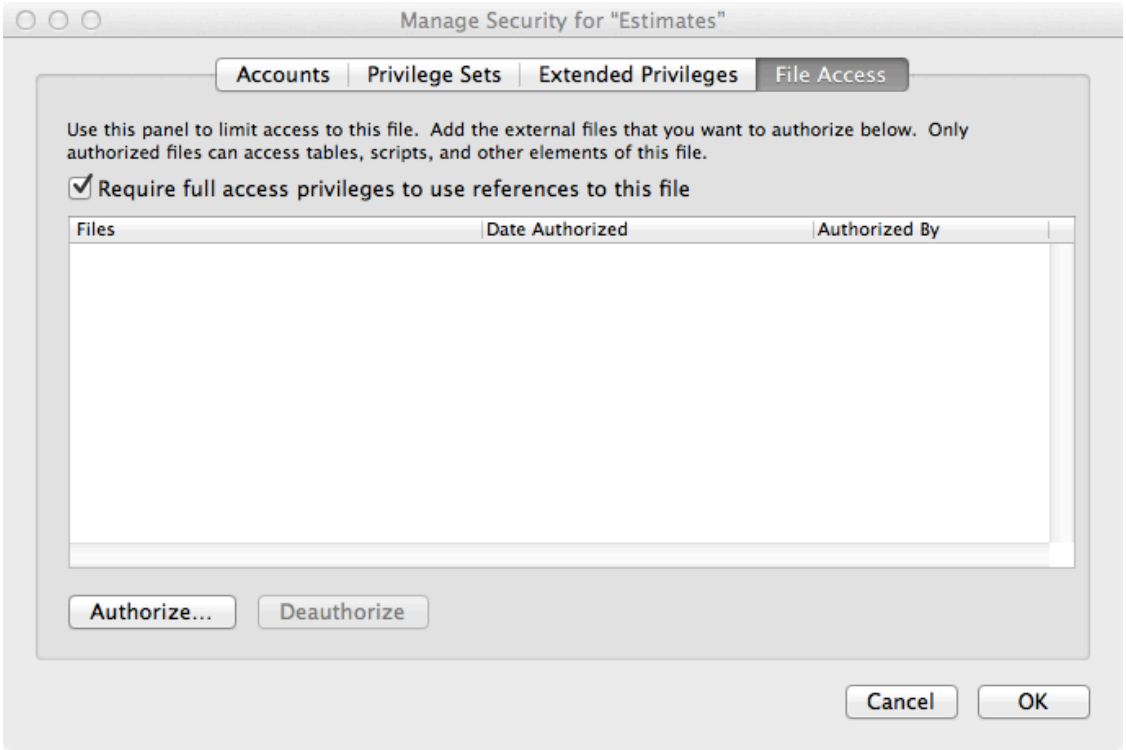

図 9. [ファイルアクセス] を使用してファイルにテーブルやスクリプトなどへのアクセスを許可します。

ファイルへのアクセス許可について詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/passwords.14.33.html#523057

スクリプトや関数などを使用してセキュリティを拡張する

レコードの削除、監査、保守は、スクリプトや関数などを用いてセキュリティを拡張できる一般的なタスクです。たとえばスクリプトを使用して以下のことを行えます。

- アカウントを追加または削除する、アカウントのパスワードをリセットする、パスワードを変更する、アカウントを有効または無効にして再びログインする。
- ユーザーが実際にレコードを削除しては困る場合にレコードをアーカイブする。
- 規制コンプライアンスおよび監査の目的で、ユーザーの現行のセッションおよび状況に関する情報を収集する。

スクリプトは、セキュリティスキーマの一部ではなく、特にデータレベルのアクセス権に適用される場合は含まれません。すべてのスクリプトを徹底的にテストし、データの整合性を保護するために [セキュリティの管理] の機能を使用してください。

実装にあたっては、FileMaker のスクリプティングおよびリレーショナルモデルをよく理解してください。

ユーザーアカウントを作成および管理するスクリプトについて詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/scripts_ref2.37.27.html#376354

Get 関数について詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/func_ref2.32.1.html#256637

さらに、何らかの規制を受ける業界で仕事をしている場合は、FileMaker Pro Advanced のデータベースデザインレポート機能を使用してデータベースのスキーマを文書化し、それを HTML ファイルや XML ファイルに公開する方法も有用と思われます。

データベースデザインレポートについて詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/fmpa_tools.24.5.html#568974

プラグインを有効または無効にする

FileMaker Pro では、プラグインを使用して追加の機能を提供することができます。セキュリティを向上させ、無許可のプラグインがインストールされるのを防ぐために、プラグインファイルのインストールを有効または無効にすることができます。

プラグインを有効にして構成するには、[環境設定] ダイアログを使用します（図 10）。これはファイル固有の環境設定ではなく、FileMaker Pro の環境設定で、プラグインをユーザーのコンピューターにインストールできるかどうか決定するものです。

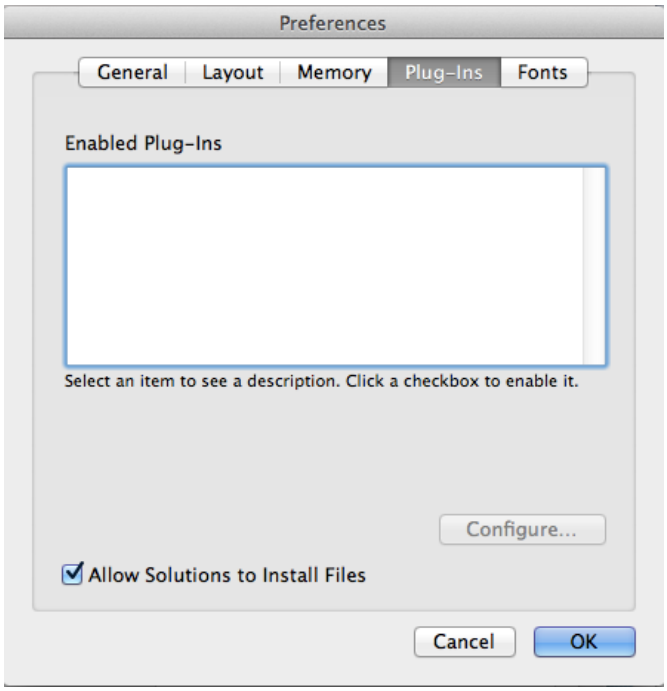

図 10. プラグインを使用すると FileMaker Pro ファイルに機能を追加することができます。

プラグインについて詳細は、以下を参照してください。
http://www.filemaker.com/12help/jp/html/preferences.26.5.html#357062

FileMaker Server または FileMaker Server Advanced のセキュリティ構成

FileMaker Server のいくつかの機能は、FileMaker Pro および FileMaker Go クライアントの両方にとってデータをさらに安全なものにします。 以下のセクションでは、Admin Console から FileMaker Server または FileMaker Server Advanced 上でセキュリティをセットアップする手順の概要を説明します。

ファイアウォールの背後に全部または一部のコンポーネントを置いて FileMaker Server または FileMaker Server Advanced をインストールする

FileMaker Server には、最大で次の 3 つのコンポーネントを含むことができます。

- データサーバー
- Web 公開エンジン
- Web サーバー

これらすべてを 1 台のマシンに展開することも、2 台または 3 台のマシンに分けて展開することもできます。複数のマシンに展開されている場合には、各コンポーネントが各自のファイアウォールに関連している部分を制御することができます。

たとえば、Database Server に入っている機密データはファイアウォールの背後に置き、顧客は Web を利用して機密ではない公開データにアクセスできるようにすることができます。 サーバーの物理的な置き場所の安全を守るのもよい方法です（たとえば鍵のかかった部屋に置くなど）。

インストールの手順に従って作業を完了すると、FileMaker Server の Admin Console にアクセスできるようになります（図 11）。

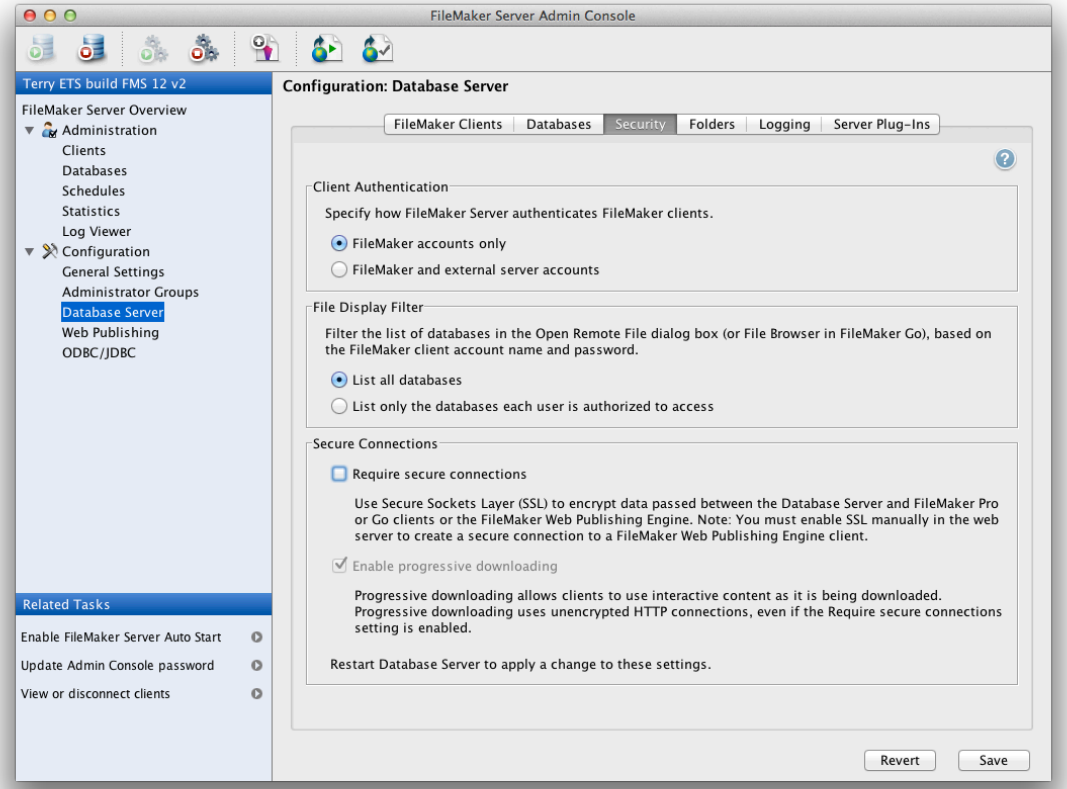

図 11. FileMaker Server の Admin Console の [セキュリティ] タブ

インストールの手順については、以下の「FileMaker Server 12 入門ガイド」の第 1 章を参照してください。
http://www.filemaker.co.jp/support/product/docs/12/fms/fms12_getting_started_ja.pdf

外部認証を有効にする

既存の認証サーバーを利用して、各ファイル内の独立したアカウント一覧を管理しなくてもファイルへのアクセスを制御することができます。

外部認証を使用するためには、FileMaker Pro を使用してファイル内に外部認証アカウントをセットアップする必要があると ともに 外部認証用に構成された FileMaker Server を使用してファイルをホストする必要があります。FileMaker Pro の構成手順については、このガイドの 認証のためにアカウントまたは外部サーバーグループをセットアップするというセクションを参照してください。

FileMaker Server で外部認証を有効にするには、以下の手順に従ってください。

1. [データベースサーバー] > [セキュリティ] タブを選択します。
2. [FileMaker と外部サーバーアカウント] を選択します。

Active Directory または Open Directory の使用を計画している場合は、FileMaker Server がインストールされているサーバーが、外部認証に使用を計画しているドメインのメンバーになっていなければなりません。

FileMaker Server マシン上でローカルセキュリティグループを使用する 計画がある場合は、このマシンがドメインのメンバーであってはなりません。

いずれの場合も、必ず徹底的にテストするようにします。このガイドのセキュリティの設定をテストするのセクションを参照してください。

ファイルの表示を制限する

デフォルトでは、ユーザーはサーバー上で使用可能なすべてのファイルを見ることができます。ただし、ユーザーがアクセスできるファイルのみを表示するよう選択することができます。以下の手順に従ってください。

1. [データベースサーバー] > [セキュリティ] タブを選択します。
2. [各ユーザーがアクセスを許可されているデータベースのみをリスト表示] を選択します。

SSL 暗号化を有効にする

FileMaker Server は、Database Server と FileMaker Pro または FileMaker Go クライアントとの間のすべてのトラフィックを暗号化することができます。また、Database Server と Web 公開エンジンとの間のすべてのトラフィックも暗号化します。

SSL を有効にするには、以下の手順に従ってください。

1. [データベースサーバー] > [セキュリティ] タブを選択します。
2. [データベースサーバーへの接続を保護] を選択します。
3. [サーバー] メニュー > [データベースサーバーの停止] を選択します（または [データベースサーバーの停止] ツールバーアイコンをクリックします）。
4. [サーバー] メニュー > [データベースサーバーの起動] を選択します（または [データベースサーバーの起動] ツールバーアイコンをクリックします）。

Web 公開に関する重要事項:

> Web サーバーと Web ブラウザの間でデータを暗号化するには、Web サーバー上でも SSL を有効にする必要があります。さらに、Web サーバーとは異なるマシン上に Web 公開エンジンを展開することを選択した場合には、これらの 2 つのコンポーネントの間でも SSL を有効にする必要があります。Web サーバーの資料（Apache または IIS）を参照してください。

FileMaker Server 12.0v1 では、SSL 暗号化が有効にされると、ストリーミングを許可するよう構成されているオブジェクトフィールド内のデータはストリーミング再生されません。その代わりに、オブジェクトフィールドのコンテンツ全体がユーザーに送信され、その後ユーザーはそのコンテンツを扱えるようになります。

FileMaker Server 12.0v2 では、[セキュリティ] タブにチェックボックスが追加され、SSL 暗号化が有効になっている場合でも暗号化されない HTTP 接続を介してオブジェクトデータのストリーミング（プログレッシブダウンロード）を有効にすることができます。

デフォルトでは、FileMaker Server はサーバー名を検証せずに暗号化された SSL 接続を提供する SSL 証明書を提供します。 セキュリティを向上させるために、特定のサーバー名または DNS 名に一致する署名付き証明書を第三の認証機関（Certificate Authority: CA）から要求して、中間者攻撃の防止に役立てることができます。

第三の認証機関からの署名付き証明書を使用するには、fmsadmin コマンドラインインターフェースを使用しなければなりません。CERTIFICATE コマンドは、FileMaker Server との SSL 接続を完全に保護するために、サーバー名またはドメインネームシステム（DNS）名に一致する署名付き証明書をインポートすることができます。

SSL 暗号化のセットアップのヘルプについては、「FileMaker Server 12 FileMaker Server ヘルプ」の 61-83 ページを参照してください。
http://www.filemaker.co.jp/support/product/docs/12/fms/fms12_help_ja.pdf

カスタム証明書の使用のヘルプについては、「FileMaker Server 12 FileMaker Server ヘルプ」の 200 ページを参照してください。
http://www.filemaker.co.jp/support/product/docs/12/fms/fms12_help_ja.pdf

Database Server と FileMaker Pro または FileMaker Go クライアントとの間の暗号化をテストするには、 Get(接続状態) 関数を使用します。この関数は以下の値を戻します。

- 0 現在のファイルに対し、ネットワーク接続なし
- 1 セキュア接続なし
- 2 FileMaker Server のデフォルトの SSL 暗号化を使用したセキュア接続
- 3 証明書でサーバー名が完全に検証されたセキュア接続

たとえば、ファイルが開かれた場合に実行される Get (接続状態) 関数を使用するスクリプトを書き、セキュア接続でなければユーザーに警告を出すことができます。

その他の SSL オプション

FileMaker Server は、エラーまたは警告を検出した場合、またはスケジュールされたタスクが完了した場合に、通知を送信することができます。FileMaker Server が SMTP 電子メールサーバーに接続した時点で SSL データ暗号化を使用するには、以下の手順に従ってください。

1. [一般設定] > [電子メール通知] タブを選択します。
2. SMTP 情報を入力する場合に、[SMTP 認証:] を選択し、次に[SSL (Secure Sockets Layer) の使用] を選択します。

SSL 暗号化を使用した電子メール通知のセットアップのヘルプについては、「FileMaker Server 12 FileMaker Server ヘルプ」の 41 ページを参照してください。
http://www.filemaker.co.jp/support/product/docs/12/fms/fms12_help_ja.pdf

さらに、Microsoft® SQL Server、MySQL、Oracle のような外部 SQL データソースに接続している場合、SSL 暗号化は FileMaker Server と外部 SQL データソースとの間のリンクには拡張されません。FileMaker Server と外部 SQL データソースとの間に SSL トンネルを作成するには、ODBC ドライバーからの SSL サポート、または他の手段による 2 地点間 SSL トンネルの作成のいずれかが必要になります。

最後に、FileMaker Server を組織の LDAP ディレクトリサービスに登録したい場合には、ディレクトリサービスアシスタントで SSL を有効にして、このプロセスを暗号化することができます。この登録は情報収集と検索のみを目的としています。外部認証の構成には、何の役割も果たしま

せん。詳細については、「FileMaker Server 12 FileMaker Server ヘルプ」の 65 ページを参照してください。
http://www.filemaker.co.jp/support/product/docs/12/fms/fms12_help_ja.pdf

サーバーがアイドル状態の場合にタイムアウトを使用する

FileMaker クライアントが FileMaker Server でホストされるファイルに接続されている場合、そのクライアントがアイドル状態でいられる最大時間を設定することができます。これは、無人のコンピューター、iPad、または iPhone を利用してファイルがアクセスされるリスクを緩和するのに役立ちます。 ただし、アイドル時間は頻繁に接続が解除されるのを避けられる十分な長さに設定してください。

これが機能するためには、FileMaker Pro 内で、アイドル状態の時に接続を解除したい各アクセス権セットについて、[その他のアクセス権] の [アイドル状態の時 FileMaker Server から接続を解除] オプション を有効にしておく必要があります。このオプションはアクセス権セットごとに設定できるので、一定のユーザーの接続を解除し、他のユーザー（[完全アクセス] アクセス権を持つユーザーなど）は常に接続を維持しておくことができます。

アイドル時間を指定するには、以下の手順に従ってください。

1. [データベースサーバー] > [FileMaker クライアント] タブを選択します。
2. [FileMaker クライアントの最大アイドル時間を設定] を選択して、時間（分単位）を入力します。

管理者グループを定義する

サーバー管理者は、管理者グループを使用して、データベース管理タスクを別のユーザーに委任することができます。また FileMaker Server の排他的で完全な制御を保持します。グループ管理者には、FileMaker Server の構成は許可されず、サーバー管理者がグループ管理者に許可したいデータベース管理タスクを指定します。コマンドラインインターフェースの使用、特に fmsadmin.exe サービスは、制約を受けることに注意してください。これらの管理者グループはその機能を採用することができません。

また外部認証を使用して、管理者グループのユーザーのクリデンシャルを検証する、および Admin Console ログインをサポートすることができます。

管理者グループのヘルプについては、「FileMaker Server 12 FileMaker Server ヘルプ」の 50-60 ページを参照してください。
http://www.filemaker.co.jp/support/product/docs/12/fms/fms12_help_ja.pdf

Admin Console でログファイルのエントリを表示する

FileMaker Server は実行時にサーバーのアクティビティを記録し、オプションで規制や監査の目的で必要になる場合があるクライアントアクセスやその他の情報を収集します。

ログファイルのエントリを表示、ソート、フィルター処理、およびエクスポートするには、Admin Console の [ログビューア] ペインを選択し、[モジュール...] で 1 つまたは複数のログフ

ァイルモジュールを選択してから、[開始:] および [終了:] の横にあるカレンダーで日付の範囲を選択します。

ログファイルのヘルプについては、「FileMaker Server 12 FileMaker Server ヘルプ」の 123-133 ページを参照してください。
http://www.filemaker.co.jp/support/product/docs/12/fms/fms12_help_ja.pdf

安全なファイル位置へのスケジュールバックアップまたはプログレッシブバックアップのセットアップ

FileMaker Server では、スケジュールバックアップとプログレッシブバックアップの 2 種類のバックアップが提供されています。ファイル内のデータを誤ってまたは故意に破壊したユーザーがいた場合、バックアップに戻ることができます。バックアップの保存には、必ず物理的に安全な場所を指定してください。

スケジュールバックアップでは、FileMaker Server は最終のバックアップ以降にデータが変更されているかどうかを確認し、変更されたデータベースとオブジェクトデータの完全コピーを作成します。

プログレッシブバックアップでは、FileMaker Server はプログレッシブバックアップフォルダ内にホストされているすべてのデータベースの完全バックアップを作成してから、指定された時間間隔ごとに、このバックアップコピーへの変更を適用していきます。

バックアップはローカルディスクにのみ保存できるため、災害復旧用にオフサイトバックアップを提供するには、連携して機能する他のツールが必要になります。

FileMaker Server はこれらのバックアップにディレクトリ構造を作成します。これらのファイルをその場で開いたり変更したりすることは避けてください。 バックアップを開く場合は、その前に必ず別の場所にコピーする必要があります。

バックアップ手順のヘルプについては、「FileMaker Server 12 FileMaker Server ヘルプ」の 143-156 ページを参照してください。
http://www.filemaker.co.jp/support/product/docs/12/fms/fms12_help_ja.pdf

セキュリティの設定をテストする

ファイルおよび FileMaker Server のセキュリティのセットアップが完全に終了したと思ったら、アプリの他の機能をテストするのと同様に、セキュリティもテストすることが推奨されます。

- 各アクセス権セットにテストアカウントをセットアップします。それらのアカウントをテスト用にアクティブにし、実動システムでは非アクティブにします。
- テストする機能および関数のチェックリストを定義します。各テストアカウントについて、チェックリストを順に実行します。
- 結果を文書化します。
- 新しい機能が追加された場合は、テストを繰り返します。

セキュリティが常にデータを保護していることを確認するために、セキュリティの評価を継続的に行ってください。これには、ユーザーがオペレーティングシステムおよびファイルソフトウェアともに、最新の最も安全なソフトウェアバージョンを使用しているかどうかの検証も含まれます。

以上のガイドラインに従うことによって、アプリを本質的に安全に保っているという自信を持つとともに、その主張を確認する文書を用意することができます。

付録 A – その他の考慮事項

本書に概要を説明したガイドラインに加え、それぞれの内部または規制の要件（COBIT、HIPAA、ISO、PCI、NIST、FIPS、など）に応じて、追加手順の実行が必要になる場合があります。

- ネットワークトラフィックすべての暗号化が必要な場合があります。FileMaker Server で SSL を有効にしてから、以下の間（FileMaker プラットフォームの外部）でも SSL を構成してください。
    - FileMaker Server データベースサーバーと外部データベース（1 つまたは複数）
    - FileMaker Server の Web 公開エンジンと Web サーバー（Apache または IIS）
    - FileMaker Server の Web 公開エンジンとデータベースサーバー（これらが 2 つの異なるマシンにインストールされている場合）
- 守るべきパスワードの最低基準が定められている場合があります。この場合には、外部認証サーバーの使用が最も適しています。
- 静止時の暗号化が必要な場合があります。市販の暗号化プラグインの使用を考慮してください。本書の発行時点では、プラグインプロバイダーはまだ FileMaker 12 用プラグインの更新を準備中です。
- 監査証跡が必要な場合があります。単純なものが必要であれば、テーブルとスクリプトを使用して FileMaker Pro で作成することができます。ニーズがより複雑な場合は、市販の監査プラグインの使用を考慮してください。

それぞれの責任において、独自のセキュリティのコンプライアンス要件を完全に理解し、適切な手順を実行する必要があります。

付録 B – 毎日の操作のためのクイックリファレンスガイド

目的は…	使用するのは…
アカウント、アクセス権、拡張アクセス権、またはファイルアクセスを管理する	FileMaker Pro または FileMaker Pro Advanced: [ファイル] メニュー > [管理] > [セキュリティ]
誰かによるデータへのアクセスを即時にやめさせる	FileMaker Server または FileMaker Server Advanced: [クライアント] を選択し、[接続されているクライアント] 一覧からクライアントを選択します。 [アクション] で、[接続を解除] を選択します。 [アクションを実行] をクリックします。 [メッセージ] で、送信する場合はメッセージを入力します。 [遅延時間] に、即時に接続を解除するために 0 を入力します。 [メッセージを送信] をクリックします。 FileMaker Pro または FileMaker Pro Advanced: [ファイル] メニュー > [管理] > [セキュリティ] [アカウント] に進みます。 [アクティブ] のチェックを外します。 そのユーザーが外部認証グループを介してアクセスしている場合には、グループ全体のアクセスを非アクティブにするのではなく、外部認証グループからユーザーを削除します。 緊急時には、ファイルを閉じて全員のアクセスをやめさせることができます。
ユーザーにパスワードを変更させる	FileMaker Pro または FileMaker Pro Advanced: [ファイル] メニュー > [管理] > [セキュリティ] [アカウント] に進みます。 アカウントを選択して [編集] をクリックします。 [ユーザーは次回ログイン時にパスワードの変更が必要] をチェックします。 注: 複数のユーザーにこのアクションを実行させるために、スクリプトを書くこともできます。 ユーザーが外部認証を介してアクセスしている場合は、Active Directory または Open Directory サーバーを使用してこれを管理します。
FileMaker Server のログファイルを表示する	FileMaker Server または FileMaker Server Advanced: [ログビューア] ペイン