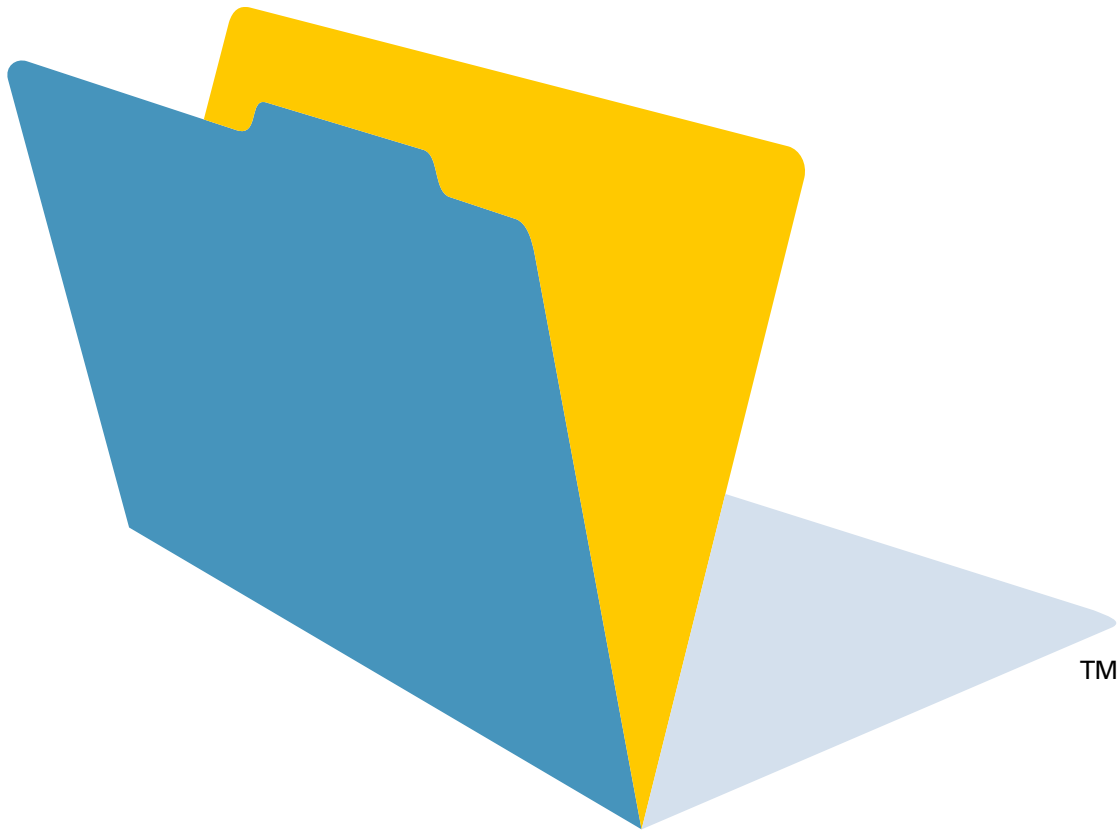


FileMaker 7

セキュリティガイド



© 2004 FileMaker, Inc. All Rights Reserved. FileMaker 及びファイルメーカーは、FileMaker, Inc. の登録商標です。ScriptMaker 及びファイルフォルダロゴは FileMaker, Inc. の商標です。

FileMaker のドキュメンテーションは著作権により保護されています。FileMaker, Inc. からの書面による許可無しに、このドキュメンテーションを複製したり、頒布することはできません。このドキュメンテーションは、正当にライセンスされた FileMaker ソフトウェアのコピーがある場合そのコピーと共にのみ使用できます。

また、製品及びサンプルファイル等に登場する会社名、氏名、住所などのデータは全て架空のもので、実在する企業、人物とは一切関係ありません。

スタッフはこのソフトウェアに付属する「Acknowledgements」ドキュメントに記載されます。

詳細情報については www.filemaker.co.jp をご覧ください。

第01版

目次

第1章

データベースのセキュリティについて

このガイドについて	5
セキュリティの目標	5
データに対する潜在的な脅威	6
セキュリティの計画	7

第2章

セキュリティの「上位 10 項目」のリスト

1. 物理的なセキュリティの確認	9
2. オペレーティングシステムのセキュリティの確認	9
3. ネットワークセキュリティの確立	10
4. データベースを保護するための計画の策定	10
5. アカウントとアクセス権セットによるデータアクセスの制限	11
6. データベースと他の重要なファイルのバックアップ	12
FileMaker Pro ファイルの修復について	13
7. ウィルス対策ソフトウェアのインストール、実行、およびアップグレード	13
8. セキュリティ対策のテスト	13
9. セキュリティ対策の評価、反復、および改善	14
10. FileMaker Pro 7 および FileMaker Server 7 へのアップグレードによるセキュリティの強化	14
FileMaker Pro 7 でのセキュリティの強化点	14
FileMaker Server 7 でのセキュリティの強化点	15

第3章

ソリューションへのセキュリティの組み込み

アカウントとアクセス権セットによるアクセスの制限	17
ファイルアクセスの制限のヒント	17
効果的なパスワードの作成のヒント	18
FileMaker Server を使用してファイルをホストする場合の考慮事項	19
Web 公開のセキュリティに関する考慮事項	19
Web 公開用にデータベースを設計する場合のヒントと注意事項	19
Web ベースの攻撃からのデータベースの保護	22
Web サーバーのセキュリティ	22
暗号化または VPN を使用したデータの保護	22
Web 公開での SSL (Secure Sockets Layer) セキュリティの使用	23
ワイヤレスネットワークについて	23
XML に関する考慮事項	23
Apple Events と ActiveX に関する考慮事項	24

第1章

データベースのセキュリティについて

FileMaker® Pro ソフトウェアでは、単独での使用、ピアトゥピアベースの共有、FileMaker Server を使用した共有、ODBC または JDBC によるアクセス、あるいはイントラネット内での共有またはインターネットユーザとの共有が可能なデータベースを作成することができます。共有するデータ、存在する脆弱性の種類、およびデータベースとデータベースファイルの保護方法を検討することが不可欠です。

場合によっては、データがそれほど重要ではなかったり、ビジネスに不可欠でなかったり、機密ではないことがあります。また、ソフトウェア自体が1人のユーザによって安全な場所で使用される場合や、セキュリティに関する考慮事項が問題にならない、オープンで信頼できる環境で使用される場合もあります。ただし、ほとんどの場合は、データはビジネスに不可欠か、重要であり、データを保護する手段を講じる必要があります。設計、テスト、および使用のすべての段階で、セキュリティ対策を計画および実装することをお勧めします。

このガイドについて

- このドキュメントでは、FileMaker Pro 7、FileMaker Developer 7、および FileMaker Server 7 のセキュリティ上の問題のみを説明します。旧バージョンのファイルメーカー Pro のセキュリティについては、www.filemaker.co.jp からドキュメントをダウンロードしてください。
- アカウントとアクセス権を定義してデータベースファイルを保護する手順を含む、FileMaker Pro の機能についての手順ごとの説明については、FileMaker Pro ヘルプを参照してください。
- FileMaker Pro のドキュメントでは、インターネットまたはイントラネット上で Web ブラウザを使用してアクセスできるデータベースのことを指す場合に、「Web 公開」という用語を使用します。
- このガイドでは、FileMaker Developer の特定の機能を説明する場合以外は、「FileMaker Pro」を、FileMaker Pro と FileMaker Developer の両方を指すものとして使用しています。

重要 FileMaker に関するドキュメントの PDF は、www.filemaker.co.jp/downloads からダウンロードすることができます。このドキュメントの最新版も、この Web サイトから入手できます。

セキュリティの目標

FileMaker データベースを保護する場合に考慮すべき一般的な問題には、次の3つがあります。

- プライバシー
- 整合性
- アクセス

データのプライバシー

データベースを設計および導入する場合、権限のないユーザ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。

データの整合性

権限のあるユーザがデータを作成および更新できる十分にオープンなシステムを設計すると同時に、意図的でない変更を防止します。さらに、ファイルを不正に操作する可能性がある権限のないユーザに対しては、アクセスを制限する必要があります。残念ながら、情報システムにアクセスして企業の資産を盗もうと試みる可能性があるユーザが存在します。

データのアクセス

データベースは、必要時にのみユーザが利用できるようにする必要があります。これは基本的である反面、見過ごされがちな考慮事項です。データベースの設計者およびネットワーク管理者は、ハッカーばかりでなく、必要以上のアクセスを持つ従業員についても考慮する必要があります。データと特定の機能の両方へのアクセスを、実際にそのアクセスが必要なユーザにのみ提供することを設計目標にします。必要な場合以外は、Web 公開などの共有オプションを有効にしないでください。

データに対する潜在的な脅威

意図的でない変更と意図的な変更の両方から、データおよびデータベースのデザインを保護する必要があります。いずれかのユーザが、デザインの外観のコピー、ユーザが入力したデータの参照、システムの損傷（多くの場合は、別のユーザのユーザ ID を使用して）、不正なデータの入力、レポートやレイアウトの破壊、計算式の破壊、スクリプトの破壊などの操作を試みる可能性があります。

データに対する最も一般的な脅威には、次のようなものが含まれます。

- 正当なユーザや事故による意図的でない脅威。権限のあるユーザが不注意から、誤操作、参照すべきでないデータの参照、アクセスできないはずのレコードの削除または変更、およびファイルの削除または損傷を行って、システムが利用できなくなる可能性があります。
- 既知のユーザによる意図的な脅威。参照すべきでないデータにアクセスすることで利点があるハッカー、データを変造する可能性があるハッカー、または意図的にデータを損傷しようとするハッカーについて考慮します。
- 不正な侵入者または匿名ユーザによる脅威。ほとんどの場合、これらは、情報の盗難、損傷、または Web システムを利用できなくすることを試みる、匿名アクセスを持つ侵入者によるインターネットベースの脅威です。

特にインターネットでは、小規模のビジネスとより大規模なワークグループが同じ脅威に直面する可能性がある点に注意してください。小規模なビジネスおよび自宅オフィスの従業員は、自分たちは目立たないため安全だと考えていることがありますが、これは現在では当てはまらなくなっています。ハッカーは、自動化されたツールを使用して脆弱なシステムを検出および侵入します。通常、システムをクラックするためにハッカーが費やす時間とリソースは、データの価値によって決まります。多くの場合は、単に、別の目標の攻撃に伴う痕跡をわかりにくくするために使用できるシステムを見つけることが攻撃の目的です。

一般的に、小規模なビジネスにアクセスするのは、より大規模な組織にアクセスするよりも簡単です。これは、多くの場合、小規模なビジネスには、効果的な防御方法（経験豊富なネットワーク管理スタッフが管理するファイアウォールなど）がなく、コンピュータシステムに関する基本的なセキュリティ標準もない（たとえば、一部のコンピュータで最も安全なバージョンのオペレーティングシステムが使用されていない場合など）ためです。

多くの場合、外部の侵入者は、ワークグループまたは小規模なビジネスのデータへのアクセスを必要とします。システムを無効にすることが侵入者の目的の場合もありますが、重要な情報（クレジットカード番号や、パスワード、生年月日のような個人識別情報など）へのアクセスの取得を試みる方がより一般的です。侵入者はワークグループから離れた場所にいると想定され、システムに関して直接の知識をほとんど持っていない可能性があります。侵入者は、自動化されたスクリプトを使用して、よく知られた弱点を持つシステムを見つけます。侵入者に別の目標を選ばせるには、適度なセキュリティがあれば十分です。

セキュリティの計画

最初に、FileMaker Pro ビルトインのセキュリティ機能であるアカウントとアクセス権セットをマスタします。セキュリティに対して、柔軟性がある多層的で反復的な方法を取ることを計画してください。

- セキュリティ計画は、個人の固有のデータアクセス必要条件を考慮できるよう十分に柔軟である必要があります。
- アクセスのすべての領域でセキュリティを階層化します。これには、コンピュータのロック、データベースへのアカウントとアクセス権の設定、ディレクトリへのアクセスの制限、およびデータを保護する他の手段の実施が含まれます。
- セキュリティを継続的に評価して、引き続きデータが保護されていることを確認します。これには、ユーザが最も安全な最新のソフトウェアバージョンを使用していることの確認、継続的なパスワードの変更、ログファイルの評価による突然の攻撃の回避、およびバックアップ計画の遵守が含まれます。時間の経過とともにファイルに構造やデータを追加していくのに従って、セキュリティオプションを設定およびテストします。

次の表は、開発者またはネットワーク管理者が職場の変動要素および関連するリスクをどのように評価できるかを示します。

職場の変動要素	リスクレベルへの影響
経験不足のデータ入力スタッフ、高い異動率、新しいコンピュータユーザ	意図的でない脅威が発生する高いリスク。これらの脅威は、主にデータ誤入力と効果的でないバックアップ方法によって引き起こされます。
経験不足のデータベース設計者	<ul style="list-style-type: none"> ■ 意図的でない脅威の高いリスク。これらの脅威は、不適切なファイルアクセスやデータベース機能アクセスを持つ従業員によって引き起こされます。 ■ 従業員は、適切なセキュリティ対策を使用せずにファイルを共有して、意図的でない脅威を招く場合があります。 ■ FileMaker Pro アカウントとアクセス権を正しく設定してファイルを適切に保護していない場合、データが公開されます。
経験不足のネットワーク管理者	<ul style="list-style-type: none"> ■ 意図的でない脅威が発生する高いリスク。これらの脅威は、不適切なオペレーティングシステムセキュリティと効果的でないバックアップ方法によって引き起こされます。 ■ 特に Web またはワイヤレスネットワーク上でファイルが共有されている場合は、ネットワークセキュリティが低いと、意図的な脅威のリスクが増加します。 ■ また、FileMaker Pro および FileMaker Server ビルトインのネットワーク共有を使用せずに、ファイルサーバーから共有ファイルにアクセスする場合にもリスクが発生します。不適切な方法でファイルが共有されると、従業員がファイルを不適切にコピーする可能性、およびレコードのロックや潜在的な破損の問題を招く可能性があります。
低い物理的なセキュリティ	意図的な脅威が発生する高いリスク。これは、コンピュータの盗難の可能性があるためです。
重要または貴重なデータのデータベースへの保存	データの盗難という意図的な脅威が発生するリスクの増加。特に、Web 上でデータが共有されている場合や、データへのアクセスが適切にモニタおよび保護されていない場合、リスクが増加します。

第 2 章

セキュリティの「上位 10 項目」のリスト

データベースファイル、ホストコンピュータ、ワークステーション、およびそれらがアクセスするネットワークが盗難や損傷に対して安全であることを確認します。この章では、データと設備を保護するために実装できる 10 のセキュリティ対策について説明します。この「上位 10 項目」リストには、以下が含まれます。

- 物理的なセキュリティの確認
- オペレーティングシステムのセキュリティの確認
- ネットワークセキュリティの確立
- データベースを保護するための計画の策定
- アカウントとアクセス権セットによるデータアクセスの制限
- データベースと他の重要なファイルのバックアップ
- ウィルス対策ソフトウェアのインストール、実行、およびアップグレード
- セキュリティ対策のテスト
- セキュリティ対策の評価、反復、および改善
- FileMaker Pro 7 および FileMaker Server 7 へのアップグレードによるセキュリティの強化

この章の以降で、これらの各対策を詳細に説明していきます。

1. 物理的なセキュリティの確認

コンピュータを評価して、物理的に安全であることを確認します。

- ホストコンピュータは、机や動かせない物にカギで固定された専用のコンピュータにする必要があります。ハードドライブを取り外すことができないようにコンピュータを保護します。カギのかかる部屋にコンピュータを保管することで、コンピュータへのアクセスを制限します。
- データベースにアクセスするクライアントワークステーションを保護します。パスワードが必要なスクリーンセーバを使用することで、コンピュータをロックしてアクセスを制限します。
- テープや CD などの持ち運び可能なメディアに保存されているファイルのバックアップコピーの物理的なセキュリティを確保します。

2. オペレーティングシステムのセキュリティの確認

オペレーティングシステムのセキュリティ機能を使用して、重要なデータへのアクセスを制限します。ネットワーク管理者は、FileMaker データベースのシステムを管理および維持する権限のある個人に対してのみ、アクセスを提供する必要があります。さらに、次の作業も実行することをお勧めします。

- システムのユーザ ID とパスワードを追跡する
- FileMaker Pro アプリケーションとファイルのディレクトリ、サーバー、および Web ページへのアクセスを制限する
- ファイル共有および FTP のリモートアクセス設定を確認する
- ファイルのアップロードまたはダウンロードアクセスを制限する
- すべてのユーザが最も安全な最新バージョンのオペレーティングシステムを使用していることを確認する

- 手順を効率化するために、外部認証を有効にすることができます。外部認証では、Windows ドメイン認証または Apple OpenDirectory に設定されているアカウントを使用します。詳細については、15 ページの「FileMaker Server 7でのセキュリティの強化点」を参照してください。
- FileMaker Pro ファイルをファイルサーバーに配置して共有せずに、FileMaker Pro および FileMaker Server ビルトインのネットワーク機能を使用してください。これによって、不適切な方法でファイルが共有されている場合に発生するファイルの不適切なコピーや、レコードロックまたは潜在的な破損の問題を防止します。

3. ネットワークセキュリティの確立

イントラネットまたはインターネット上で共有されるデータベースでは、TCP/IP プロトコルが使用されます。ピアトゥピアまたは FileMaker Server でデータベースを共有する場合も、TCP/IP プロトコルを使用できます。TCP/IP は、データを移動したり、クライアントがデータに接続できるようにする点では優れていますが、セキュリティを主要な目的として設計されていません。予防措置を講じていない場合、TCP/IP によって、ホストコンピュータ、サーバーソフトウェア、データベース、および内部ネットワーク上の他のクライアントコンピュータへの不正なアクセスが提供される可能性があります。TCP/IP は高度なデータ保護機能を備えていないため、不正なユーザの侵入経路に、ファイアウォールや SSL データ暗号化などの障壁を設けることが重要です。暗号化プログラムなどの他社製品の詳細については、22 ページの「暗号化または VPN を使用したデータの保護」を参照してください。

- 最も一般的に使用されるバリエーション方法は、ファイアウォールです。ファイアウォールは、「ファイアウォールの外部」にある公開環境と、「ファイアウォールの後方」にあるプライベートな環境という2つの独立した環境にネットワークを分割します。ファイアウォールの外部のユーザは、公開する TCP/IP またはハードウェアアドレスにのみアクセスできます。公開されるサーバーコンピュータにセキュリティを集中できると同時に、ファイアウォールの後方のコンピュータはより少ない保護手段で運用することができます。
- Apple AirMac と他の 802.11b ネットワークカードおよびベースステーションなどのワイヤレスネットワークデバイスを使用すると、セキュリティ上の問題となる可能性があります。これらのデバイスは、建物の壁の外にまでネットワークトラフィックをブロードキャストする可能性があるため、ワイヤレスネットワーク信号を暗号化することが非常に重要です。必ず、利用可能な最大レベルの信号暗号化を使用してください。詳細については、23 ページの「ワイヤレスネットワークについて」を参照してください。

4. データベースを保護するための計画の策定

データベースの設計を計画する際は、FileMaker データベースファイルの保護方法も計画する必要があります。設計時にデータベースにセキュリティを組み込む方が、後で組み込むよりも大幅に簡単です。

- 特定のテーブル、フィールド、レコード、レイアウト、値一覧、およびスクリプトなど、保護するファイルの範囲のリストを作成します。必要なさまざまなレベルのアクセスを確保するために必要なアクセス権セットの数を計画します。
- 各ユーザに対して個別のアカウントが必要か（推奨）、それとも複数のユーザが共有できるアカウント（「Marketing」または「Sales」アカウントなど）が必要かを判断します。
- ゲストアカウントを有効にするかどうかを判断します。ゲストアカウントを使用すると、ユーザは、ログインしてアカウント情報を入力せずにファイルを開くことができます。ゲストアカウントを使用する場合は、可能な限り最も制限されたアクセス権セットを割り当てます。使用しない場合は、ゲストアカウントを無効にすることを検討してください。
- 特定のアクセス権セットに対して、拡張アクセス権（FileMaker ネットワーク共有やインスタント Web 公開など）を有効にする必要があるかどうかを判断します。
- 必要なアカウントをファイル内に作成して、各アカウントに適切なアクセス権セットを割り当てます。

ユーザの種類の一覧とそれらのアクセス権の概要を記入した次のような表の作成を検討してください。

ユーザの種類	レコードの表示	レコードの作成	レコードの編集	レコードの削除	スクリプトの変更	スクリプトの実行	値一覧の変更	メニュー
マネージャ	可	可	可	可	可	可	可	すべて
マーケティング	可	可	可	制限付き *	制限付き *	可	不可	編集のみ
営業	可	可	可	制限付き *	不可	可	不可	編集のみ
人事	可	可	可	可	可	可	不可	すべて
法務	可	不可	不可	不可	不可	可	不可	最小
ゲスト	可	不可	不可	不可	不可	不可	不可	最小

* レコードごとのアクセス権を使用して、レコードの削除などの一部の機能に対して制限付きアクセスを提供することができます。レコードごとのアクセス権の詳細については、FileMaker Pro ヘルプを参照してください。

5. アカウントとアクセス権セットによるデータアクセスの制限

FileMaker Pro ファイル内で最も基本的なセキュリティ方法を提供するには、アカウントとアクセス権セットを使用します。アカウントとアクセス権セットを使用すると、ユーザが表示および操作することができるデータベースファイル内の項目を制限できます。次の操作を制限することができます。

- ファイルアクセス: ファイルを開くには、ユーザはアカウント名とパスワードを入力する必要があります。
- データアクセス: 個々のテーブルの特定のレコードまたはフィールドを表示専用にするか、完全に隠します。
- レイアウトアクセス: レイアウトモードでユーザがレイアウトを表示または変更できないようにします。
- 値一覧およびスクリプトへのアクセス: ユーザが値一覧およびスクリプトにアクセスして変更したり、スクリプトを実行できないようにします。
- データの出力: ユーザがデータを印刷またはエクスポートできないようにします。
- メニューアクセス: 限られたセットのメニューコマンドのみを利用可能にします。

アカウントによってファイルが制限されている場合、ユーザは、データベースを開く前、またはデータベースに接続する前に、アカウント名とパスワードを知っておく必要があります。ユーザが入力するアカウント名とパスワードによってどのアクセス権セットが使用されるかが決まり、使用されるアクセス権セットによって、ファイル内で操作可能な項目が制限されます。アカウントとアクセス権セットの詳細については、17 ページの「アカウントとアクセス権セットによるアクセスの制限」を参照してください。

ヒント

- セキュリティは、定義するユーザアカウントとパスワードに応じて決まります。詳細については、18 ページの「効果的なパスワードの作成のヒント」を参照してください。
- 管理者レベルのユーザアカウント名とパスワードを他のユーザと共有しないでください。これによって、物理的なセキュリティ、オペレーティングシステム、またはネットワークセキュリティが回避された場合に、ファイルを保護します。
- データベースに保存されているアカウント/パスワードの代わりに、データベースでグループ名に基づいて外部サーバー認証を実行できるように FileMaker Server を設定することができます。詳細については、15 ページの「FileMaker Server 7でのセキュリティの強化点」を参照してください。

重要 新しい FileMaker Pro ファイルは、初期状態では保護されていません。ファイルを開くと、ユーザは、自動的に、完全アクセス権セットが割り当てられている Admin アカウントでログインします。他のユーザが完全アクセスでデータベースを開くことができないようにするには、Admin アカウントの名前を変更して、パスワードを割り当てます。他のユーザとファイルを共有する前に、ファイルのセキュリティを計画して、各ユーザに必要なアクセスレベルを割り当ててください。

6. データベースと他の重要なファイルのバックアップ

ビジネスに不可欠な情報サービスを実行する代替サイトおよびシステムを含む、データの復元計画を策定します。最新のバックアップがあれば、あるユーザがファイルの管理者アカウントの情報を紛失した状況や、ユーザエラー（場合によってはデータベースの設計の不備）によってデータが不適切に削除または変更された状況からの回復に役立てることができます。

次の点に注意してください。

- データベースは FileMaker Server でホストし、定期的にスケジュールされた自動バックアップを作成します。

たとえば、平日の午前 6:00、午前 9:00、正午 12:00、午後 3:00、午後 6:00、および午後 11:30 に、ファイルのローカルバックアップを作成します。深夜には、企業のバックアップシステムにシステム全体の増分バックアップを作成します。最後に、金曜日の深夜に完全システムバックアップを実行します。バックアップテープは、コピーして離れた場所に保管します。この方法によって、複数のドライブの重大な障害以外の何らかの理由でサーバーが停止した場合、データファイルのより最近のバックアップ（つまり、失われたデータの最大 3 時間分）を使用することができます。重大なドライブ障害が発生した場合は、前日の夜のテープを使用して、損失を 1 日分のデータにまで最小化することができます。当然、これらの手順は、ユーザの状況とデータの価値に合わせて調整できます。
- バックアップコピーが損傷していたり、アクセス不能でないことを確認します。必要になる前に、バックアップコピーが正しく機能することを確認してください。ハードドライブに対して診断ツールを実行して、ファイルを定期的にバックアップします。
- バックアップコピーからファイルのセット全体を復元できることを確認します。
- データを定期的にエクスポートして、ファイルの損傷に対して保護します。
- バックアップメディア自体を保護します。バックアップは、耐火性のある別の場所に保管します。
- ネットワーク管理者が不在の場合にファイルを元に戻ることができるバックアップ管理者を割り当てます。
- 冗長性を計画します。停電が発生した場合は、無停電電源装置（UPS）によって少なくとも 15 分間電源を維持して、すべてのファイルを安全に閉じることができる必要があります。所定の時間内に電源を復旧できない場合は、発電機を使用してサーバーに電源を供給することを検討します。さらに、ルータとファイアウォールの電源についても検討します。インターネットアクセスが 48 時間以上中断された場合、コミュニケーションに問題があるかどうかを判断します。
- 侵入者がデータベースサーバーを停止させ、そのサーバーを以前の状態に復元できない場合に、サービスの提供を継続する方法を検討します。
- 発生の可能性がある追加の状況を評価して、各状況に対応するための計画を作成します。

また、ネットワーク管理者は、データシステムおよびビジネスに不可欠な機能に対するリスクを評価する必要があります。たとえば、次の点を考慮します。

- データまたは独自の知的財産の盗難。
- サーバー、ネットワーク、データストレージ、データバックアップストレージなどのネットワークインフラストラクチャの中断、盗難、または損傷。パスワードクラッカーや、その他の種類の悪意を持った妨害および破壊行為によって損傷が発生する可能性があります。ほとんどの問題は、組織の内部に起因します。
- 建物の火災、環境または生物学的危害、洪水などによる企業インフラストラクチャの中断または破損。

- 公共インフラストラクチャの中断または破損。環境条件、または竜巻や洪水などの悪天候によって引き起こされる電気、通信（音声およびデータ）、交通網（鉄道、バス、電車）を含みます。

重要 予想外の停電、ハードドライブの障害、ソフトウェアの障害などのサーバー障害が発生した場合は、バックアップファイルを使用します。システム障害によって FileMaker Server が不適切にシャットダウンした場合、キャッシュデータがディスクに書き込まれておらず、ファイルが適切に閉じられていないと、ファイルの破損につながる可能性があります。ファイルを再度開いて整合性チェックまたは修復を実行しても、ファイルは内部で破損したままになっている可能性があります。ファイルの修復では、問題が解決されたことを保証できません。

FileMaker Pro ファイルの修復について

データベースファイルが不適切に閉じられ、前回のバックアップ以降のデータを修復する必要がある場合は、修復機能を使用します。修復は元のファイルを置き換えるためのものではないため、修復を実行すると、元のファイルと異なる名前の新しいファイルが作成されます。修復は強力な処理で、可能なかぎり多くのデータを元に戻すために、レイアウトやスクリプトなどが削除される場合があります。修復されたファイルからデータをエクスポートして、元のデータベースファイルのクリーンなバックアップにインポートすることをお勧めします。

修復には長い時間がかかることがあるため、失われる可能性があるデータの量に応じた間隔でローカルバックアップを作成します。

7. ウィルス対策ソフトウェアのインストール、実行、およびアップグレード

ほとんどのコンピュータはインターネットに接続できるため、電子メールの添付ファイルを通じて送信されるウィルスの攻撃に対して脆弱です。すべての従業員がウィルス対策チェックソフトウェアを定期的に行っていること、およびウィルス警告の典型的な兆候を理解していることを確認してください。従業員は、コンピュータにファイルをコピーまたはダウンロードする前にすべてのファイルをスキャンする必要があります。また、知っているユーザからであっても、要求していない添付ファイルは開かないようにする必要があります。

8. セキュリティ対策のテスト

すべての状況をテストして、すべての共有技術でユーザアカウントが正しく動作していることを確認することが重要です。

次に例を示します。

- さまざまなユーザアカウントを使用してファイルを開き、作成した各アクセス権セットをテストします。制限が意図したとおりに動作することを確認し、アクセス権セットに必要な修正を加えます。
- すべてのユーザアカウントで操作方法とスクリプトをテストします。アカウントにはさまざまなアクセス権が設定されている場合があるため、一部のユーザに対しては、レイアウトやテーブル、スクリプトステップなどの特定の機能へのアクセスが有効でない可能性があることを考慮してください。
- ユーザが、Web 上でのインスタント Web 公開、XML、JDBC などのさまざまな方法でデータベースにアクセスする場合は、該当する技術のアカウントもテストします。
- Web 上でファイルを公開する場合は、スクリプトを開いて [Web の互換を区別して表示] を有効にし、すべてのステップがサポートされるようにします。Web 互換ではないステップがスクリプトに含まれる場合は、[ユーザによる強制終了を許可] スクリプトステップを使用して、以降のステップの処理方法を決定します。詳細については、「日本語エキストラ」フォルダ内の「マニュアル (PDF)」フォルダにある『FileMaker インスタント Web 公開ガイド』を参照してください。

- 予期せぬ結果が発生しないかどうかをテストします。たとえば、さまざまなユーザアカウントでファイルを開いて、ユーザに実行が許可されていないアクションを実行してみます。可能な場合は、アクセス権セットへのアクセスを削除することを検討してください。
- 他の開発者を採用して、データに不適切にアクセスしてみます。
- 開発時だけでなく、導入後も定期的にテストを実行します。

9. セキュリティ対策の評価、反復、および改善

セキュリティに対しては、反復的な方法を取ることが重要です。たとえば、新しいユーザがデータベースにアクセスする場合は、新しいユーザの会社での職務または役割に応じて、データ自体とデータベース構造に対するアクセスの適切なレベルを再評価することをお勧めします。

FileMaker Pro データベースを開発する前に、次の質問に自問自答します。また、ファイルは時間の経過に従って変更されるため、継続的にも自問自答します。

- 重要なものは何か
- それが重要な理由は何か
- どの程度重要か
- その損失または公開による被害はどの程度か
- 損失または公開を防止するためのセキュリティの最低レベルはどの程度か
- そのセキュリティの実装に使用できるツールは何か

セキュリティを評価するために、FileMaker Pro および FileMaker Server でログファイルを有効にして、ユーザの操作を確認します。また、ユーザのアカウント名、パスワード、および IP アドレスを記録するスクリプトと計算式を含めると、操作を追跡することもできます。

10. FileMaker Pro 7 および FileMaker Server 7 へのアップグレードによるセキュリティの強化

FileMaker Pro および FileMaker Server では、セキュリティが再設計されています。他の多くの新機能に加えて、アカウントとアクセス権セットを割り当てた場合のより強力で効率的なユーザ体験を実現するためにも、FileMaker Pro 7 を使用してください。

FileMaker Pro 7 でのセキュリティの強化点

- 新しいセキュリティモデルはより直感的で、他のツールと同様に機能します。ユーザアカウントとパスワードを作成したり、複数のユーザおよびテーブルでアクセス権セットを共有できます。
- FileMaker Pro では 1 つのファイル内で複数のテーブルがサポートされているため、1 組のアカウントとアクセス権セットで、単一のファイルに複数のテーブルが含まれるデータベースを保護できます。
- Get(アカウント名) 関数を使用して、関数およびスクリプトで現在のユーザを判断できます。これによって、特定のアカウント名のみで実行できるスクリプトを作成するなど、さまざまな可能性が広がります。
- 次回データベースを開いたときに新しいパスワードを指定するようユーザに要求したり、指定した日数の経過後にパスワードを変更するようユーザに要求する設定を有効にすることができます。
- パスワードの最小文字長を設定できます。

- FileMaker ネットワークでは、アカウント名とパスワードに一方の暗号化アルゴリズムを使用して、パスワードクラックツールによる暗号解読を防止しています。ユーザアカウント名とパスワードはホストコンピュータ上で確認され、クライアントコンピュータ上でのハッキング、あるいは実行可能ファイルまたは一時ファイルを使用したパスワードのクラックを防止します。アカウント名とパスワードは、安全な場所に保管してください。アカウント名とパスワードを紛失した場合は、ファイルを再作成しなければなりません。

FileMaker Server 7 でのセキュリティの強化点

FileMaker Server でデータベースをホストする場合は、FileMaker Pro および Web ベースのクライアントに対してデータの安全性を高める多くの機能を利用することができます。特定の機能の詳細については、『FileMaker Server Web 公開インストールガイド』、または FileMaker Server に付属の『FileMaker Server 管理者ガイド』を参照してください。

- FileMaker ネットワークを使用してユーザアカウント情報およびデータを暗号化するには、[FileMaker Server への接続を保護する]を有効にします。
- Web ベースのクライアントとファイルを共有する場合は、Web サーバーアプリケーションで SSL 暗号化を有効にして、Web 上でホストからゲストコンピュータに渡されるデータを暗号化します。詳細については、23 ページの「Web 公開での SSL (Secure Sockets Layer) セキュリティの使用」を参照してください。
- インスタント Web 公開、XML、および Web 公開エンジンの XSLT など、特定の拡張アクセス権を有効または無効にすることができます。たとえば、あるサーバー上のすべてのファイルがインスタント Web 公開で共有されることがわかっている場合は、他の種類の Web 公開をすべて無効にすることができます。XML データへのアクセスを許可する拡張アクセス権がファイルに含まれていても、そのサーバー上の Web 公開エンジンでファイルがホストされているときは、XML データへのアクセスを利用できません。詳細については、『FileMaker Server Web 公開インストールガイド』を参照してください。
- Apple OpenDirectory や Windows ドメインなど、組織でユーザおよびグループに対して一元管理された認証を使用する場合は、認証サーバーに基づいてユーザを認証するアカウントを設定できます。これにより、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することなく、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。外部サーバーを使用したアカウントの認証の詳細については、FileMaker Server ヘルプを参照してください。

重要 データベースファイルに1つまたは複数の外部サーバーアカウントが含まれる場合は、オペレーティングシステムのセキュリティ設定を使用して、ファイルへの直接アクセスを制限してください。制限しない場合、権限のないユーザが、認証サーバーの環境を複製した別のシステムにファイルを移動して、ファイルへのアクセスを取得できることがあります。外部サーバー機能を使用して認証されるアカウントのグループ名は、テキスト文字列として保存されています。グループ名を別のシステムに複製すると、コピーされたファイルに、グループのメンバーに割り当てられたアクセス権セットを使用してアクセスすることができ、データが不適切に公開される可能性があります。

- データベースを効果的かつ簡単にメンテナンスするには、ログファイルおよびファイルバックアップの機能を有効にします。

第3章

ソリューションへのセキュリティの組み込み

開発者およびネットワーク管理者には、データベースファイルの設計と導入におけるセキュリティの管理と、定期的なセキュリティの管理に対する責任があります。

アカウントとアクセス権セットによるアクセスの制限

ファイルを保護する主要な方法は、FileMaker Pro でアカウントとアクセス権を定義することです。管理者本人にしかわからない管理者パスワードを使用して、すべてのファイルへのアクセスを制限することをお勧めします。これによって、他のセキュリティ対策が回避された場合に、ファイルが保護されます。

重要 古いデータベースのセキュリティ設定がどのような方法で最新バージョンの FileMaker Pro に変換されるかについては、『旧バージョンのファイルメーカーデータベースの変換』を参照してください。アカウント名、パスワード、およびアクセス権セットに関するあらゆる情報を網羅した詳細および手順ごとの操作については、FileMaker ヘルプを参照してください。

アカウントを使用して、保護されたファイルを開こうとしているユーザを認証します。

- 各アカウントには、アカウント名およびパスワード（オプション）を指定します。
- 各データベースファイルには、Admin およびゲストという2つのアカウントがあらかじめ定義されています。Admin アカウントには完全アクセス権セットが割り当てられています。セキュリティを強化するために、Admin アカウントの名前は変更することをお勧めします。ゲストアカウントでは、ユーザは、アカウント名とパスワードを入力せずにファイルを開くことができます。ゲストアカウントの名前は変更できません。デフォルトでは、ゲストアカウントには閲覧のみのアクセス権セットが割り当てられています。[アカウントとアクセス権]で異なるアクセス権セットを割り当てることができます。
- セキュリティを最大限に高めるには、各ユーザに対して固有のアカウントを作成します。

アクセス権セットを使用して、データベースファイルへのアクセスのレベルを指定します。各データベースファイルには、完全アクセス、データ入力のみ、および閲覧のみアクセスの3つのアクセス権があらかじめ定義されています。

- 各アカウントには1つのアクセス権セットが割り当てられ、これによって、ユーザがそのアカウントを使用してファイルを開いたときのアクセスのレベルが決まります。
- 表示可能なレイアウトや利用可能なメニュー、印刷を許可するかどうかなど、データベースアクセスを制限するアクセス権セットを作成することができます。また、アクセス権セットを使用して、ファイル内の特定のテーブルのレコードまたはフィールドへのアクセスを制限することもできます。

拡張アクセス権は、アクセス権セットによって許可されるデータ共有オプションを決定します。アクセス権を有効にして、FileMaker ネットワーク、インスタント Web 公開、および XML または XSLT を使用したカスタム Web 公開で共有されているファイルと、ODBC または JDBC クライアント、および FileMaker Mobile から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、拡張アクセス権はすべて無効になっています。

重要 セキュリティを最大限に高めるには、すべてのファイルに対してユーザ名とパスワードを要求するアカウントを作成します。新しいセキュリティ機能を活用するには、指定した期間後にパスワードを変更するようユーザに要求し、パスワードの最小文字長を指定します。

ファイルアクセスの制限のヒント

- [ファイルオプション] ダイアログボックスで指定されているアカウント名とパスワードを使用して自動的にログインすることは避けます。

- 多くの場合、ユーザが1つのセッションで複数のソリューションを操作しなければならないときは、各ファイルで同じパスワードを使用すると便利です。ユーザが自分のパスワードを変更した場合は、すべてのファイルでパスワードを変更しないかぎり、これは効果的ではありません。アカウントを作成するときは、すべてのソリューションファイルにアカウントを作成する必要があります。利便性を考えて、1つのファイルに複数のテーブルを定義することができます。FileMaker Server によるファイルのホスト、および Windows ドメインや Apple OpenDirectory などの外部認証サーバーの使用を検討してください。詳細については、15 ページの「FileMaker Server 7でのセキュリティの強化点」を参照してください。
- アカウントが複数のユーザによって使用される場合は、定期的にパスワードを変更します。さらに、ユーザがグループを離れたときは、アカウント名とパスワードも変更します。
- スクリプトを使用して、重要なファイルのみを処理する起動ファイルを作成します。データは起動ファイルには保存されておらず、代わりに、スクリプトによって重要なファイルに移動されます。ユーザは、重要なデータや危険な機能（レコードの削除など）へのアクセスを制限するデフォルトのアカウント名とパスワードでファイルを開きます。[スクリプトを完全アクセス権で実行]を有効にすると、ユーザにアクセスを提供していないアクション（レコードの削除など）をスクリプトによって実行できます。
- 各テーブル内の特定のレコードを表示、編集、および削除するレコードアクセス権を設定することができます。ユーザの部署、役職、担当職務などの多くの条件に基づいて、ユーザのアクセスを特定のレコードに制限します。レコードアクセス権の詳細については、FileMaker Pro ヘルプを参照してください。
重要 特定のレコードへのアクセスを制限すると、データアクセスモデルがより複雑化します。さまざまなユーザアカウントでログインしてレイアウト、レポート、およびスクリプトをすべて評価することで、ソリューションを十分にテストしてください。予想される動作がユーザにわかるように、具体的な条件を文書に記録してください。
- セキュリティの目的でレイアウトを使用しないでください。CGI リクエストや他のソースなどからファイルを保護する唯一の方法は、フィールドごとまたはテーブルでアカウントアクセスを制限することです。
- FileMaker Developer を使用すると、完全アクセス権セット、および完全アクセス権セットを使用するアカウント（Admin アカウントを含む）を完全に削除することができます。この操作は回復不可能です。今後どのユーザにもファイルへの完全アクセスが必要ないことが確実な場合にのみ実行してください。詳細については、FileMaker Developer の『デベロッパーズガイド』を参照してください。

効果的なパスワードの作成のヒント

- 安全なパスワードは、8文字を超える長さで、大文字と小文字を混在させた文字と少なくとも1つの数字で構成されます。無関係な2つの単語を組み合わせ、文字を数字に置き換えることを検討してください。たとえば、b0att!me というパスワードでは、「o」をゼロに、「i」を感嘆符にそれぞれ置き換えています。
- ファイルが Web 上で公開される場合、アカウント名とパスワードには、表示可能な ASCII 文字のみ（a から z、A から Z、および 0 から 9 など）を使用することをお勧めします。アカウント名とパスワードのセキュリティを高めるには、「!」や「%」などの記号を含めます。ただし、コロンは含めないでください。FileMaker Server でデータベースをホストする場合は、SSL 暗号化を有効にします。
- 容易に推測できる文字列がパスワードに含まれていると、パスワードのセキュリティが低下します。容易に推測できる文字列とは、名前（特に家族やペットの名前）、生年月日、記念日、および password、default、master、admin、user、guest、client などの標準的な用語です。
- パスワードは頻繁に（可能であれば 30 から 90 日ごとに）変更します。
- パスワードは一度だけ使用します。
- 可能な場合は、常に各ユーザに固有のパスワードを割り当てます。ユーザアカウントを共有する必要がある場合は、パスワードを定期的に変更してください。
- マスタファイルやリストのセキュリティが十分に確保されている場合以外は、パスワードをマスタファイルやリストに記録しないでください。
- ユーザアカウントを他のユーザと共有しないでください。ユーザがファイル管理者からのみアカウント名とパスワードを受け取るようにしてください。

FileMaker Server を使用してファイルをホストする場合の考慮事項

FileMaker Server を使用してデータベースをホストする場合は、次の点に注意してください。

- リモートアクセスを有効にしている場合は、パスワードを要求するようにしてください。詳細については、FileMaker Server オンラインヘルプを参照してください。
- FileMaker Pro ファイルは、ネットワークディレクトリ上ではなく、ローカルサーバーに保存します。パフォーマンス上最も重要な要因の1つは、ディスクに対するデータの高速な読み取りと書き込みです。
- ファイル共有を無効にするか、または FileMaker Server でホストされたファイルにユーザが直接アクセスできないことを確認します。ファイルサーバーから FileMaker Pro ファイルをコピーすることができる場合、ファイルは「オフライン」での攻撃に対して脆弱です。たとえば、外部サーバー機能で認証されるアカウントのグループ名は、テキスト文字列として保存されています。グループ名を別のシステムに複製すると、コピーされたファイルに、グループのメンバーに割り当てられたアクセス権セットを使用してアクセスすることができ、データが不適切に公開される可能性があります。詳細については、15 ページの「FileMaker Server 7でのセキュリティの強化点」を参照してください。
- [共有ファイルを開く] ダイアログボックスまたはインスタント Web 公開データベースホームページにファイル名を表示しないようにしても、アカウントとアクセス権を使用してファイルを保護することの代わりにはなりません。
- FileMaker Server のコマンドラインインターフェース (CLI) のコマンドには、アカウント名とパスワードを含めることができます。権限のないユーザが、画面に入力された CLI コマンドに含まれるパスワードを参照できないようにしてください。パスワードが記述された CLI コマンドに含まれるスクリプトファイルやバッチファイルへのアクセスを制限するには、オペレーティングシステムのファイル所有権とアクセス権の機能を使用してください。

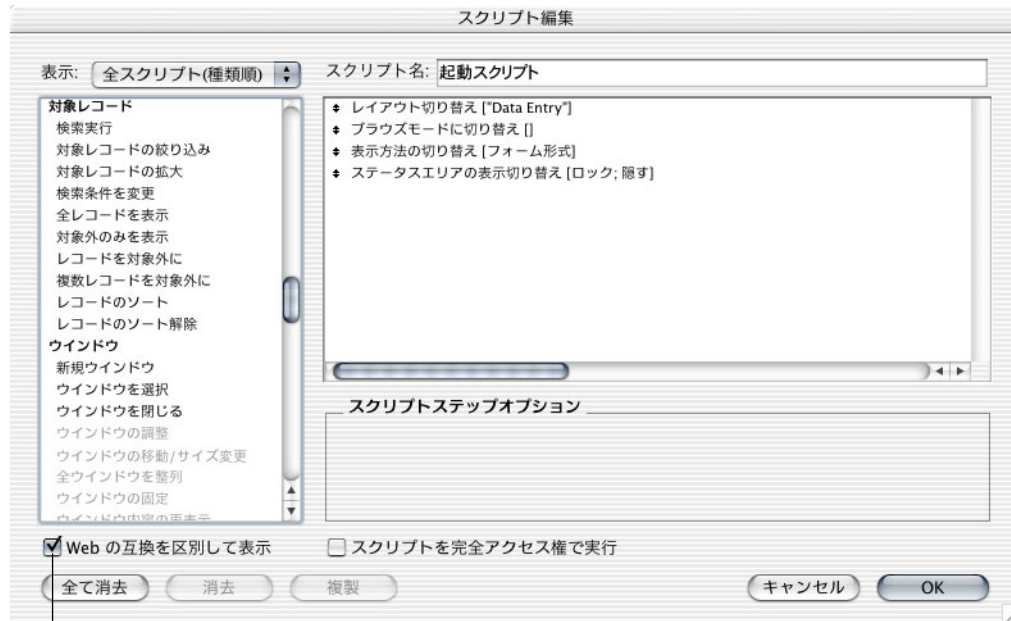
Web 公開のセキュリティに関する考慮事項

FileMaker Pro ソフトウェアでは、イントラネットまたはインターネットにデータベースを公開して、ユーザが Web ブラウザソフトウェアを使用してデータベースをブラウズ、検索、および更新できます。この方法では、他の FileMaker Pro クライアントとファイルを共有するよりもリスクが増加します。

Web 公開用にデータベースを設計する場合のヒントと注意事項

1. アカウントとアクセス権セットを定義します。
 - すべてのファイルをユーザ名とパスワードで保護します。クライアントに対して固有のアカウントを使用することが現実的でない場合は、デフォルトのユーザ名とパスワードでログインするゲストアカウントを使用することができます。ただし、この場合、データベースをホストするコンピュータの IP アドレスまたはドメイン名を知っている任意のユーザがファイルを利用できることとなります。
 - データおよびデータベース構造を変更するアクセス権は、必要な場合にのみ割り当てます。
 - 必要な Web 公開の拡張アクセス権のみを有効にします。たとえば、XSLT を使用したカスタム Web 公開のみを使用する場合は、その拡張アクセス権を適切なアクセス権セットで有効にし、他の Web 公開の拡張アクセス権は無効のままにします。
2. 以前のリリースからソリューションを変換する場合は、Web セキュリティデータベースがサポートされなくなった点に注意してください。FileMaker Pro で、アカウント、パスワード、および関連するアクセス権を変換後のデータベースファイルに移動する必要があります。詳細については、『旧バージョンのファイルメーカーデータベースの変換』を参照してください。
3. セキュリティを高めるため、リモートでアクセスされるデータベースを FileMaker Pro クライアントで Web 上に公開することができなくなりました。ホストコンピュータからのみ Web 上にファイルを公開できます。

4. インスタント Web 公開で、データの表示用にあらかじめ定義されたレイアウトに制限されることがなくなり、Web ユーザは、アカウントに基づいてすべてのレイアウトを利用することができます。アクセス権セットを使用してアカウントに対してレイアウトを制限することは可能ですが、セキュリティを確保するためにレイアウトに依存しないでください。最適なセキュリティを確保するには、テーブル、レコード、フィールド、スクリプト、および値一覧を使用してデータへのアクセスを管理します。
5. インスタント Web 公開のクライアントがインスタント Web 公開の [ログアウト] ボタンをクリックしなかった場合や、[アプリケーションを終了] ステップが含まれるスクリプトを実行しなかった場合、データベースへの接続はアクティブなままです。他の Web ユーザがデータにアクセスすることができたり、ユーザがファイルにアクセスできなくなる場合があります。また、Web ユーザは、ブラウザを終了して、Web ブラウザのキャッシュファイルからアカウント情報を消去する必要もあります。詳細については、「日本語エキストラ」フォルダ内の「マニュアル (PDF)」フォルダにある『FileMaker インスタント Web 公開ガイド』を参照してください。
6. ビルトインのインスタント Web 公開データベースホームページにファイル名を表示しないようにするには、共有設定ダイアログボックスの [インスタント Web 公開のホームページに表示しない] を選択します。これは、ソリューションに複数のファイルが含まれていて、一部のファイル名を表示しない場合に便利です。この機能は、ファイルにアカウントとアクセス権を定義する代わりには使用しないでください。
7. スクリプトの結果を検査します。
 - レコードを削除するステップがスクリプトに含まれていて、Web ユーザがレコードの削除を許可しないアカウントでファイルを開いた場合、レコードを削除するステップは実行されません。ただし、スクリプトは引き続き実行される場合があり、予期しない結果になる可能性があります。[スクリプトを完全アクセス権で実行] を有効にして、レコードを削除するスクリプトを許可するか、またはアカウントとアクセス権を使用して、ユーザが通常はアクセスできない他の制限付きアクションを実行できるようにすることを検討してください。また、特定のユーザのアクセス権セットを変更し、それらのユーザに対して [アクセスなし] のスクリプトを指定することによって、ユーザによる特定のスクリプトの実行を制限することもできます。
 - Web 上で公開されるデータベースには、どの Web ユーザが実行しても問題の発生しないスクリプトを含める必要があります。サポートされていないスクリプトステップを参照するには、スクリプトを開き、[スクリプト編集] ダイアログボックスの [Web の互換を区別して表示] チェックボックスを選択します。グレー表示されるスクリプトステップは、Web 上ではサポートされていません。
 - サポートされていないステップ（たとえば、[メールを送信] などの Web 互換ではないステップ）や、ユーザが実行するためのアクセス権を持たないステップがスクリプトに含まれる場合は、[ユーザによる強制終了を許可] スクリプトステップを使用して、以降のステップの処理方法を決定します。詳細については、「日本語エキストラ」フォルダ内の「マニュアル (PDF)」フォルダにある『FileMaker インスタント Web 公開ガイド』を参照してください。



Web 互換でないスクリプトステップをグレー表示するには、[Web の互換を区別して表示] を選択します。

8. データベースファイルや重要なデータを FileMaker Pro の「Web」フォルダ（またはそのサブフォルダ）に保存しないでください。
9. Web 上で公開されているファイルにアクセスしているユーザの IP アドレス（およびリクエストの日付と時刻などのオプション）を追跡するには、ログファイルを有効にします。
10. FileMaker Pro では、あらかじめ指定した IP アドレスを使用するユーザにアクセスを制限することができます。FileMaker Server でファイルをホストする場合は、Web サーバーアプリケーションでクライアント IP アドレスに対して制限を設定できます。
11. Web 上で公開されるデータベースを FileMaker Server でホストする場合は、Web サーバーアプリケーションで利用可能な SSL 暗号化などの追加のセキュリティ対策を使用することができます。詳細については、23 ページの「Web 公開での SSL (Secure Sockets Layer) セキュリティの使用」を参照してください。また、使用していない Web 公開技術を無効にすることもできます。詳細については、『FileMaker Server Web 公開インストールガイド』を参照してください。
12. Web 上で公開されるデータベースを FileMaker Server でホストしている場合、Web 公開エンジンは、特定のポートとプロトコルを使用して FileMaker Server および Web サーバーと通信します。ホストコンピュータおよびファイアウォール上で、ポートを開いたり、プロトコルを許可しなければならない場合があります。詳細については、『FileMaker Server Web 公開インストールガイド』を参照してください。
13. FileMaker Server でデータベースをホストして、XML を使用したカスタム Web 公開を使用する場合は、Web ブラウザからセキュリティをテストして、公開される可能性のある要素を確認することができます。
 - XML を使用して Web 上で公開されているデータベースの名前を参照するには、ブラウザに次のアドレスを入力します。
`http://<ip: ポート >/fmi/xml/fmresultset.xml?-dbnames`
 - XSLT を使用して Web 上に公開されているデータベースを参照するには、次のアドレスを入力します。
`http://<ip: ポート >/fmi/xsl/stylesheets_name.xsl?-grammar=fmresultset&-dbnames`
 - データベース内のレコードのフィールドを参照するには、ブラウザに次のアドレスを入力します。
`http://<ip: ポート >/fmi/xml/fmresultset.xml?-db=dbname&-lay=layoutname&-findany`

- データベース内のスクリプト名を参照するには、ブラウザに次のアドレスを入力します。

`http://<ip: ポート >/fmi/xml/fmresultset.xml?-db=dbname&-scriptnames`

- データベース内のレイアウト名を参照するには、ブラウザに次のアドレスを入力します。

`http://<ip: ポート >/fmi/xml/fmresultset.xml?-db=dbname&-layoutnames`

クエリーコマンドとパラメータの詳細については、『FileMaker Server カスタム Web 公開ガイド』を参照してください。

Web ベースの攻撃からのデータベースの保護

最初に、このドキュメントで説明されているセキュリティ手順を確認します。ホストコンピュータは、外部の世界への接続であると同時に、保護されていない場合は、外部の世界から内部ネットワークへの接続にもなります。次の点を確認します。

- Web 上 (特にインターネット上) で共有されるソリューションに対しては、Web 公開コンポーネント、ファイアウォール、SSL などの標準的なインターネット技術からデータベースを分離する 2 つ (またはそれ以上) のコンピュータを使った設定を検討してください。これによって、ファイルへのアクセス、および Web ユーザの Web ブラウザとサーバーの間の通信が保護されます。
- ファイル共有や FTP などのリモートアクセスの設定を確認して、ホストコンピュータとの間でファイルをアップロードまたはダウンロードするための直接アクセスが、ファイルへの不適切なアクセスが防止される方法で制限されていることを確認します。
- TCP/IP を使用して FileMaker Pro データベースをホストする場合は、ホストコンピュータおよび内部ネットワークへのアクセスが不正なユーザに許可される可能性があります。ファイアウォールは、ネットワークを分離して、「ファイアウォールの後方」にあるファイルを保護するために不可欠です。これにより、ファイアウォールの外部のユーザが公開されていない TCP/IP アドレスにアクセスするのを防止します。

Web サーバーのセキュリティ

Web 上にデータベースやイメージなどのコンテンツを公開する場合、Web サーバーアプリケーションは、データに対するリクエストの処理および実行という重要なタスクを実行します。ユーザがブラウザに Web アドレスを入力すると、入力したアドレスにある Web サーバーソフトウェアに対し、データやイメージを検索してユーザのコンピュータにダウンロードするよう要求していることとなります。ダウンロードされたら、ブラウザに表示できます。この処理の整合性を保護するために、Web サーバーは独自のセキュリティのしくみを備えています。

FileMaker Server でデータベースをホストする場合は、Microsoft IIS (Internet Information Server) や Apache HTTP Server などの他社の Web サーバーアプリケーションを使用して、Web 上にファイルを公開します。SSL 暗号化などの追加のセキュリティ機能を活用して、ホストから Web クライアントにより安全にデータを転送することができます。

暗号化または VPN を使用したデータの保護

暗号化および VPN (仮想プライベートネットワーク) を使用して、TCP/IP ネットワーク上のデータベースを保護することを検討します。暗号化とは、特定のアプリケーションによってのみ結果 (暗号文) を理解できるようにデータ (平文) を操作する処理です。

次の方法によって、データを保護することができます。

- 安全な VPN を設定して、ネットワークトラフィックが WAN (Wide Area Network) を移動するときの一部 (またはすべて) のネットワークトラフィックを暗号化する
- FileMaker Server を使用してデータベースをホストして、Web サーバーアプリケーションで SSL 暗号化を設定する
- これらの方法を組み合わせる

Web 公開での SSL (Secure Sockets Layer) セキュリティの使用

SSL プロトコルは、Web サーバーとクライアント (Web ブラウザ) 間で暗号化および認証された通信を可能にする標準化された方法です。SSL 暗号化は、FileMaker Server でホストされたデータベースでのみ利用でき、Microsoft IIS (Internet Information Server) や、Apache Group の Apache HTTP Server などの Web サーバーアプリケーションで有効です。

SSL 暗号化では、「暗号」と呼ばれる数式を使用して、サーバーとクライアントの間で交換される情報を判読不可能な情報に変換します。その後、これらの暗号を使用して、「暗号鍵」によって情報を判読可能なデータに再変換します。

SSL の有効化と設定の詳細については、Web サーバーに付属のマニュアルを参照してください。

ワイヤレスネットワークについて

注意すべきもう 1 つのセキュリティ脆弱性は、「Wi-Fi」接続とも呼ばれる 802.11x ワイヤレスネットワークデバイスです。802.11x ワイヤレスネットワークデバイスには、以下が含まれます。

- ラップトップなどのステーション (802.11x ワイヤレスアクセスを持つデバイス)
- ネットワークへのアクセスのポイントであるアクセスポイント (ワイヤレスハブまたはブリッジ)
- LAN (Local Area Network) 自体
- 認証サーバー (クライアントがネットワーク接続を試みたときにクライアントを認証する独立したデバイス)

ネットワークへの無線周波数アクセスでは、トランスミッタの範囲内の無線によってパケットが盗聴されやすくなります。このため、侵入者がワイヤレスプロトコルを使用して企業ネットワークにアクセスすることが可能になります。高感度アンテナを使用すると、通常の「動作」範囲からかなり離れた場所からでもこのような侵入を実行できます。

たとえば、FileMaker Server でファイルをホストしている場合、ファイルに十分なユーザアカウントセキュリティが設定されていないと、侵入者がデータにアクセスすることができます。WAN でのアクセス制御方法を理解している侵入者は、ネットワークにアクセスして有効なコンピュータアドレスを盗み出し、そのコンピュータに割り当てられている IP アドレスを使用できる場合があります。一般的な方法は、有効なコンピュータがネットワークの使用を停止するまで待ってから、ネットワークにおけるそのコンピュータの場所を乗っ取り、ネットワークのすべてのデバイスまたはより広いインターネットにアクセスする方法です。

重要 ネットワークの物理的なセキュリティを評価するときは、ワイヤレスネットワーク信号をパスワード保護および暗号化してください。必ず、利用可能な最大レベルの信号暗号化を使用してください。

XML に関する考慮事項

XML および XSLT スタイルシートは、データのアクセス、配布、および表示のための業界標準になりつつあります。FileMaker Server のカスタム Web 公開機能では、XSLT スタイルシートを使用して、XML データをフィルタおよび変換することができます。この機能を使用して、Web ユーザに送信される XML ファイル内のメタデータを削除または変更したり (フィールド名を隠す場合など)、クエリー文字列パラメータ (データベース名やレイアウト名の値など) を静的に定義して、クエリー文字列パラメータが Web ユーザに公開されたり、Web ユーザによって変更されるのを防止できます。詳細については、『FileMaker Server カスタム Web 公開ガイド』を参照してください。

注意 XML 形式のデータは基本的にテキストです。つまり、適切な方法を使用して暗号化されていないと、盗聴されて読み取られる可能性があります。TCP/IP でデータをブロードキャストして、FileMaker Server でデータベースをホストする場合は、Web サーバーアプリケーションで SSL 暗号化を使用することをお勧めします。これによって、ネットワークトラフィックを監視して FileMaker Pro データを抽出できる「パケットスニッファ」アプリケーションをブロックします。

重要 必要な場合以外は、拡張アクセス権を有効にしないでください。

Apple Events と ActiveX に関する考慮事項

FileMaker Pro は、Apple Events (Mac OS) または ActiveX (Windows) のコマンドを処理することができます。たとえば、外部スクリプトがタイムアウトになって次のコマンドが処理されない場合、これによって予期しない結果が発生する可能性があります。

他社の技術を導入する場合は、すべてのスクリプトとユーザの状況を十分にテストしてください。