

Tips: アクセス記録の収集

Ver. 1.0
2019 年 10 月

概要：

- FileMaker Server あるいは FileMaker Cloud for AWS を利用することにより、基本的なアクセス記録を収集することができます。
- FileMaker Pro Advanced を単独で利用する場合、あるいは、さらに詳細なアクセス記録を取得するために、FileMaker 関数、スクリプト、スクリプトトリガ等を利用することができます。
- 各医療機関等で要求される標準的なセキュリティ・レベルや、対象となる医療情報システムに求められる機能に応じて対応する必要があります。システムで要求事項に対応できない場合は、人手による操作記録を義務付ける必要があります。

内容

| | |
|---|----|
| Tips: アクセス記録の収集 | i |
| 1. ガイドライン要求事項の内容 | 1 |
| 1.1. ガイドライン要求事項の概要 | 1 |
| 1.2. アクセス記録を取得する対象操作 | 1 |
| 1.3. アクセス記録の記録項目 | 2 |
| 1.4. アクセス記録の提示方法 | 2 |
| 1.5. アクセス記録の管理方法 | 3 |
| 2. アクセス記録収集に関する FileMaker プラットフォームの基本機能 | 4 |
| 2.1. FileMaker Server 18 | 4 |
| 2.1.1. イベントログ | 4 |
| 2.1.2. アクセスログ | 5 |
| 2.1.3. ログファイルのサイズ変更 | 5 |
| 2.1.4. ログファイルのダウンロード | 6 |
| 2.1.5. 外部サーバーアカウントを利用する場合の認証記録（Windows） | 7 |
| 2.2. FileMaker Cloud for AWS 1.18 | 7 |
| 2.2.1. ログファイルのダウンロード | 7 |
| 2.2.2. Access.log | 8 |
| 2.3. FileMaker Pro 18 Advanced | 9 |
| 3. より詳細なアクセスの記録の取得方法の例 | 10 |
| 3.1. 機能を自作する | 10 |
| 3.1.1. ユーザのログイン時刻、利用時間等を記録する | 10 |
| 3.1.2. データ（レコード）の追加・削除を記録する | 11 |
| 3.1.3. データ（レコード）の編集を記録する | 11 |
| 3.1.4. データ（レコード）の表示を記録する | 12 |

| | |
|--|----|
| 3.1.5. FileMaker Server のログファイルを世代管理する | 12 |
| 3.2. サードパーティ製のツールを利用する | 12 |
| 4. アクセスの記録の保護 | 14 |
| 4.1. FileMaker Server におけるログファイルの保護 | 14 |
| 4.2. FileMaker Cloud for AWS におけるログファイルの保護 | 14 |
| 4.3. ログファイルに対する改ざん・削除の検出 | 14 |
| 5. 補足 | 15 |

用語

| 本ドキュメントでの略称 | ガイドライン |
|--------------|---|
| 厚生省ガイドライン | 厚生労働省 「医療情報システムの安全管理に関するガイドライン 第 5 版」(平成 29 年 5 月) |
| 経産省ガイドライン | 経済産業省 「医療情報を受託管理する情報処理事業者向けガイドライン (第 2 版)」 (平成 24 年 10 月) |
| 総務省ガイドライン | 総務省 「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン (第 1 版)」(平成 30 年 7 月) |
| 3 省 3 ガイドライン | (上記 3 ガイドラインをまとめている) |

本ドキュメントでは、以下の製品を対象としています。

- FileMaker Pro 18 Advanced
- FileMaker Server 18
- FileMaker Cloud for AWS 1.18
- FileMaker Go 18

1. ガイドライン要求事項の内容

1.1. ガイドライン要求事項の概要

医療情報システムにおいてアクセスの記録（アクセスログ）を収集することは、医療情報の質を担保し、個人情報を含む資源を厳重に管理して不正利用がないことを確認するために極めて重要です。

このため、3省3ガイドラインのいずれにおいても、医療情報システムでのアクセス記録の取得を「必須」機能と位置付けております。なお、厚労省ガイドラインでは、次のように、医療情報システムがアクセス記録機能を持つことを前提としながらも、当該機能を持たない場合は人手による操作記録を最低限の対応として挙げています。

情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。（6.5 技術的安全対策 C. 7）

3省3ガイドラインには、アクセスの記録に関し、(1) アクセス記録を取得する対象操作、(2) 記録項目、(3) 記録内容の提示方法、(4) 管理方法について、それぞれ要求事項を挙げています。以下、それぞれについてまとめます。

1.2. アクセス記録を取得する対象操作

3省3ガイドラインにおけるアクセス記録の対象操作を表1にまとめます。

表1に示すように、3省3ガイドラインにおいて対象としているアクセス記録を取得する操作は、医療情報システムに対する利用からの通常のアクセスだけでなく、保守（リモートメンテナンス含む）のためのアクセス等も含まれています。

また、医療情報システムに対する直接アクセスに加えて、ネットワーク接続や関連情報へのアクセスも記録対象とされています。

表1 3省3ガイドライン中の「アクセス記録」に関する要求事項の掲載状況

| No. | アクセス記録を要求する対象操作 | 厚労 | 経産 | 総務 |
|-----|------------------------------------|----|----|----|
| 1 | 医療情報システムの利用（通常アクセス） | ○ | ○ | ○ |
| 2 | 保守 | △ | ○ | ○ |
| 3 | リモートメンテナンス | ○ | - | ○ |
| 4 | ネットワーク接続（認証ログ及び接続ログ） | - | ○ | - |
| 5 | システム運用情報（システム及びサービス設定ファイル等）の複製及び利用 | - | ○ | - |
| 6 | IoT 機器を含むシステム操作 | △ | - | - |

（○：「最低限」or「必須」、△：「推奨」、-：記載なし；
但し、総務省ガイドラインは要求度合いについての分類がされていないためすべて「○」とした）

1.3. アクセス記録の記録項目

3 省 3 ガイドラインで取り上げられているアクセス記録の記録項目を表 2 に示します。これらのうち、「アクセス（操作）された医療情報」は、3 省 3 ガイドラインに共通して明記されており、医療情報ごとのきめ細やかなアクセス管理が強く求められていることがわかります。

なお、記録項目の具体的な内容については、3 省 3 ガイドラインの中では、経産省ガイドラインの中で詳しく「推奨」しています（「7.6.12 ログの取得及び監査」(2)）。

表 2 ガイドラインにおけるアクセス記録を取得する対象操作

| No. | アクセス記録の主な記録項目 | 厚労 | 経産 | 総務 |
|-----|---------------------------------|----|----|----|
| 1 | 利用者のログイン時刻 | ○ | △ | - |
| 2 | アクセス時間 | ○ | △ | - |
| 3 | アクセス（操作）された医療情報 | ○ | △ | ○ |
| 4 | 作業内容 | - | △ | - |
| 5 | ログオン可否、ファイル／データベースへのアクセス可否 | - | △ | - |
| 6 | アクセス元 IP アドレス（ネットワークからのアクセスの場合） | ○ | △ | - |
| 7 | システム起動／停止イベント | - | △ | - |
| 8 | 修正パッチの適用作業において変更されたファイル | - | △ | - |

（○：「最低限」or「必須」、△：「推奨」、-：記載なし；
但し、総務省ガイドラインは要求度合いについての分類がされていないためすべて「○」とした）

1.4. アクセス記録の提示方法

取得したアクセスの記録を分析、利用するために、厚労省ガイドラインと経産省ガイドラインには、アクセス記録の提示方法について、それぞれ以下のような要求事項が含まれています。不正アクセスが起こったときにその状況解明を効率よく行うことに留まらず、常日頃から不正アクセスの兆しがないかを監視することも推奨されています。

- アクセスした診療録等の識別情報を時系列順に並べて表示（厚労省ガイドライン 6.8 5; 推奨）
- 指定時間内でどの患者に何回のアクセスが行われたかを確認（厚労省ガイドライン 6.8 5; 推奨）
- 作業者 ID と、情報の識別子（資産台帳記載の番号等）、生成時系列、アクセス時系列等、多様な指標での並び替え（経産省ガイドライン 7.6.12 (1); 推奨）
- 情報の種別、アクセス時間等での絞り込み等（経産省ガイドライン 7.6.12 (1); 推奨）
- 専用のログサーバにログデータを集約して分析管理する（経産省ガイドライン 7.6.12; 推奨）

1.5. アクセス記録の管理方法

3 省 3 ガイドラインでは、アクセス記録を保護するだけでなく、アクセス記録に対する不正な改ざん等の検出・防止策や、ログファイルの容量超過等について対策を施すことが要求事項として挙げられています。これらはいずれも、「最低限」あるいは「必須」の要求事項です。

- アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止（厚労省ガイドライン 6.5 8、経産省ガイドライン 7.6.12 (5)）
- 容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。（経産省ガイドライン 7.6.12 (5)）
- ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。（経産省ガイドライン 7.6.12 (5)）
- サイバー攻撃等によりサービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全（総務省ガイドライン 3.2.8（イ）3.④、同 3.6.2 (8)（イ）3.④）

2. アクセス記録収集に関する FileMaker プラットフォームの基本機能

FileMaker Server および FileMaker Cloud for AWS は、稼働するとサーバーアクティビティをログに記録します。ログファイルを使用して、クライアントアクセス情報と、規制および監査目的に必要なその他の情報を収集できます。

2.1. FileMaker Server 18

FileMaker Server は、処理を行う過程で、以下のログファイルにアクティビティやクライアントアクセスなどの情報を記録します。

- イベントログ
- アクセスログ
- 使用状況ログ
- Web 公開ログ
- FileMaker Data API

各ログファイルの内容は、プレーンテキストファイルを開くことができるアプリケーションであれば、どのアプリケーションでも表示、印刷することができます。macOS の場合は、コンソールアプリケーションを使用することもできます。

macOS のコンソールアプリケーションでは、FileMaker Server が実行状態になっていてもログファイルを開くことができます。コンソールアプリケーション上では、イベントは連続的に記録され、最新のログイベントがウインドウの末尾に表示されます。

FileMaker Server のすべてのログファイルは、次の Logs フォルダに保存されます。

- Windows : [ドライブ]:¥Program Files¥FileMaker¥FileMaker Server¥Logs
- macOS : /ライブラリ/FileMaker Server/Logs

FileMaker Server のログファイルは、予め設定されたサイズに到達すると、ファイル名に「-old」が付加されて名称変更され、新しいログファイルが作成されます。さらに、新たなログファイルが設定されたサイズに達すると、既存の「*-old」ファイルは上書きされるので注意が必要です。ログファイルを長期間保存するには、ログファイルの最大サイズを適切に設定する（2.1.3）か、あるいは「*-old」ファイルを退避させる作業（3.1.5）が必要です。

2.1.1. イベントログ

FileMaker Server は、サーバーイベントをタイムスタンプと共に、「Event.log」という名前の専用のファイルにタブ区切り付きで記録します。このファイルには、ユーザがログイン（認証）に失敗した場合などのような警告レベル及びエラーレベルのアクセスに関するメッセージの他、主に次のようなイベントが記録されます。詳細は、FileMaker Server 18 ヘルプ「イベントログ」を参照してください。

- データベースサーバーの起動または停止
- データベースサーバーによって開かれたデータベースファイルと閉じられたデータベースファイル
- 適切に閉じられなかったファイルに対して実行される一貫性チェック

なお、「Event.log」ファイルのサイズがログファイルのサイズの制限に達すると、このファイルの名前が「Event-old.log」に変更され、新しい「Event.log」ファイルが作成されます。さらに、新たな「Event.log」ファイルが指定されたログサイズに達すると、既存の「Event-old.log」は上書きされるので、すべてのログを保全するためには別フォルダへの定期的なコピーを行う等、対応が必要です（3.1.5）。

2.1.2. アクセスログ

FileMaker Server は、データベースへのアクセスをタイムスタンプと共に、「Access.log」という名前の専用のファイルにタブ区切り付きで記録します（図 1）。このファイルには、次のようなイベントが記録されます。

- データベースサーバーに接続した、または切断したクライアント
- 独自のアカウントまたはゲストアカウントを使ってクライアントがアクセスしたデータベース

「Access.log」ファイルに記録されているのは、情報レベルのメッセージのみです。警告レベルおよびエラーレベルのメッセージはすべて「Event.log」ファイルに記録されています。

| | | | | |
|-------------------------------|----|-----|-----------|---|
| 2018-07-17 20:54:52.560 +0900 | 情報 | 638 | FMS001001 | クライアント「Tanaka」が「N01001」[192.168.101.31]から「ProAdvanced 18.0.1 [fmapp]」を使用して接続を開始しています。 |
| 2018-07-17 20:54:52.560 +0900 | 情報 | 94 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として開いています。 |
| 2018-07-17 20:56:35.138 +0900 | 情報 | 98 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として閉じています。 |
| 2018-07-17 20:56:35.138 +0900 | 情報 | 22 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]が接続を解除しています。 |
| 2018-07-17 20:56:59.012 +0900 | 情報 | 638 | FMS001001 | クライアント「Tanaka」が「N01001」[192.168.101.31]から「ProAdvanced 18.0.1 [fmapp]」を使用して接続を開始しています。 |
| 2018-07-17 20:56:59.012 +0900 | 情報 | 94 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として開いています。 |
| 2018-07-17 20:56:59.012 +0900 | 情報 | 98 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として閉じています。 |
| 2018-07-17 20:56:59.012 +0900 | 情報 | 22 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]が接続を解除しています。 |
| 2018-07-17 21:00:26.868 +0900 | 情報 | 638 | FMS001001 | クライアント「Tanaka」が「N01001」[192.168.101.31]から「ProAdvanced 18.0.1 [fmapp]」を使用して接続を開始しています。 |
| 2018-07-17 21:00:26.868 +0900 | 情報 | 94 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として開いています。 |
| 2018-07-17 21:03:18.457 +0900 | 情報 | 98 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として閉じています。 |
| 2018-07-17 21:03:18.457 +0900 | 情報 | 22 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]が接続を解除しています。 |
| 2018-07-17 21:04:02.003 +0900 | 情報 | 638 | FMS001001 | クライアント「Tanaka」が「N01001」[192.168.101.31]から「ProAdvanced 18.0.1 [fmapp]」を使用して接続を開始しています。 |
| 2018-07-17 21:04:02.003 +0900 | 情報 | 94 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として開いています。 |
| 2018-07-17 21:06:18.297 +0900 | 情報 | 98 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として閉じています。 |
| 2018-07-17 21:06:18.297 +0900 | 情報 | 22 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]が接続を解除しています。 |
| 2018-07-17 21:06:50.733 +0900 | 情報 | 638 | FMS001001 | クライアント「Tanaka」が「N01001」[192.168.101.31]から「ProAdvanced 18.0.1 [fmapp]」を使用して接続を開始しています。 |
| 2018-07-17 21:06:50.733 +0900 | 情報 | 94 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として開いています。 |
| 2018-07-17 21:06:50.733 +0900 | 情報 | 98 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として閉じています。 |
| 2018-07-17 21:06:50.733 +0900 | 情報 | 22 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]が接続を解除しています。 |
| 2018-07-17 21:09:34.136 +0900 | 情報 | 638 | FMS001001 | クライアント「Tanaka」が「N01001」[192.168.101.31]から「ProAdvanced 18.0.1 [fmapp]」を使用して接続を開始しています。 |
| 2018-07-17 21:10:06.778 +0900 | 情報 | 94 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として開いています。 |
| 2018-07-17 21:10:06.778 +0900 | 情報 | 98 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「手術予定」を「Tanaka01」として閉じています。 |
| 2018-07-17 21:12:30.406 +0900 | 情報 | 22 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]が接続を解除しています。 |
| 2019-02-26 15:24:32.499 +0900 | 情報 | 638 | FMS001001 | クライアント「Tanaka」が「N01001」[192.168.101.31]から「ProAdvanced 18.0.3 [fmapp]」を使用して接続を開始しています。 |
| 2019-02-26 15:24:32.499 +0900 | 情報 | 94 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「予約管理」を「user」[192.168.101.31]として開いています。 |
| 2019-02-26 15:51:13.493 +0900 | 情報 | 98 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]がデータベース「予約管理」を「user」[192.168.101.31]として閉じています。 |
| 2019-02-26 15:51:13.493 +0900 | 情報 | 22 | FMS001001 | クライアント「Tanaka (N01001)」[192.168.101.31]が接続を解除しています。 |

図 1 FileMaker Server の Access.log ファイル（サンプル）

「Access.log」ファイルのサイズが予め指定されたログサイズに達すると、「Event.log」と同様に、「Access-old.log」にリネームされ、新たな「Access.log」ファイルが作成されます。さらに、新たな「Access.log」ファイルが指定されたログサイズに達すると、「Access-old.log」にファイル名にリネームされて、既存の「Access-old.log」は上書きされるので、すべてのログを保全するためには別フォルダへの定期的なコピーを行う等、対応が必要です（3.1.5）。

2.1.3. ログファイルのサイズ変更

FileMaker Server では、保存するログファイルのサイズを最大 1,000MB まで設定することができます。ログファイルのサイズを変更するには、次の操作を行います。

1. Windows のスタートメニューから「コマンドプロンプト」を起動します。
2. ログファイルのサイズを変更するために、次のコマンドを実行します（サイズを 50MB に変更する場合）。

```
fmsadmin SET SERVERCONFIG LOGSIZE=50
```

3. コマンドを実行すると、FileMaker Admin Console の username と password の入力を求められますので、それぞれを入力します。
4. 結果として「LogSize = 50 [default: 40, range: 1-1000] 」と表示されれば、ログファイルのサイズ変更は完了です。

2.1.4. ログファイルのダウンロード

FileMaker Admin Console の【構成】の【ログ】で、FileMaker Server の稼動中にデータベースサーバーがイベント、クライアントアクセス、使用状況情報を収集し記録するためのログファイルをダウンロードすることができます。（図 2）。

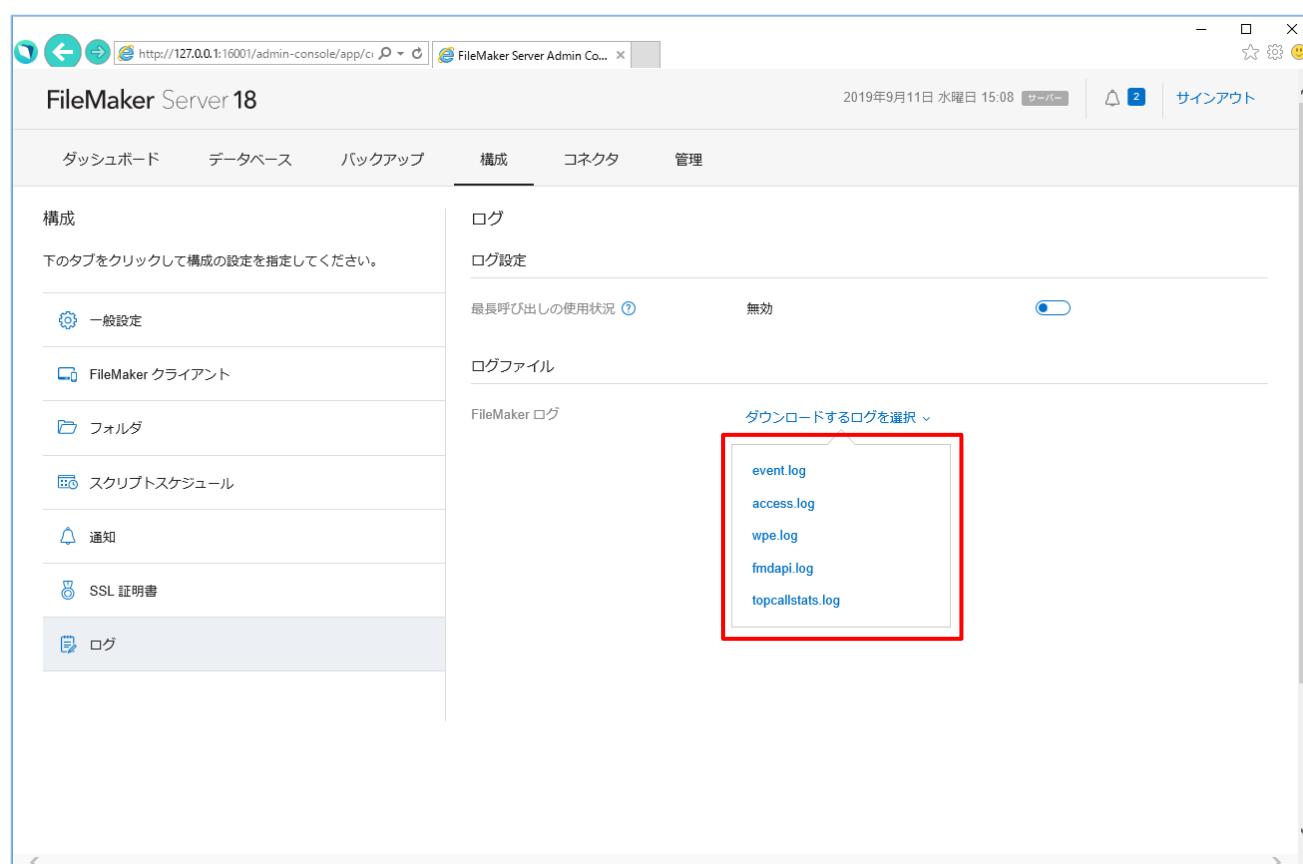


図 2 FileMaker Server でのログファイルのダウンロード (Admin Console)

ログファイルをダウンロードするには、次の操作を行います。

1. FileMaker Admin Console の【構成】の【ログ】を選択します。
2. 「ダウンロードするログを選択」をクリックします。
3. ダウンロード可能なログファイル名を選択し、FileMaker Admin Console の指示に従って、ダウンロードします。

2.1.5. 外部サーバーアカウントを利用する場合の認証記録 (Windows)

FileMaker Server で 外部認証を利用して FileMaker Pro Advanced のファイルを共有している場合で、マスタマシンが Windows のとき、すべてのログイン試行の記録は Windows セキュリティログに記録されます。Windows セキュリティログの詳細については、Windows のマニュアルを参照してください。

2.2. FileMaker Cloud for AWS 1.18

FileMaker Cloud for AWS は、アクティビティ、クライアントアクセス、およびその他の情報を追跡してその情報を表 3 に示すログファイルに保存します。

FileMaker Cloud for AWS の各ログファイルは、所定のサイズの制限に達すると、このファイルの名前が「Event-old.log」に変更され、新しい「Event.log」ファイルが作成されます。さらに、新たな「Event.log」ファイルが指定されたログサイズに達すると、「Event-old 2.log」等、順次数字を付加したファイル名にリネームされて保存されていきます。

表 3 FileMaker Cloud for AWS のログファイル

| ログファイル | 内容 |
|-----------------------|--|
| event.log | FileMaker Cloud for AWS データベースサーバーの実行時に発生したイベント。データベースサーバーが開始または停止した時や、データベースファイルが開かれたり閉じられたりした時、認証に失敗した時など。 |
| gateway.log | 仮想 DBA ボットのアクティビティ。これは、AWS および FileMaker ハブと通信します。 |
| journal.log | 通知およびユーザの操作。メモリまたはデータボリュームの使用状況に関する通知や、バックアップの開始などの操作など。 |
| wpe.log | Web 公開エンジンのイベント (Web 公開エンジンのエラー、FileMaker WebDirect のエラー、FileMaker スクリプトに関連したエラーなど)。 |
| fmshelper.log | 他のすべてのプロセスを実行、開始、および停止するユーティリティプロセス。 |
| awsmanager.log | AWS 関連のすべてのアクティビティ (インスタンスのアップグレード、更新やスナップショットのアクティビティなど)。 |
| fmdapi.log | 発生したすべての FileMaker Data API のエラーと、共有データベースにアクセスした FileMaker Data API 呼び出しに関する情報。 |
| stats.log | FileMaker Server のパフォーマンス、およびログインしたクライアント数 |

2.2.1. ログファイルのダウンロード

FileMaker Cloud for AWS において記録されたログファイル (表 3) をローカル・コンピュータにダウンロードするには、次の操作を行います (図 3) :

1. Admin Console で、[Configuration] > [Logging] をクリックします。
2. [Select the log to download] をクリックします。
3. ログファイル名をクリックします。

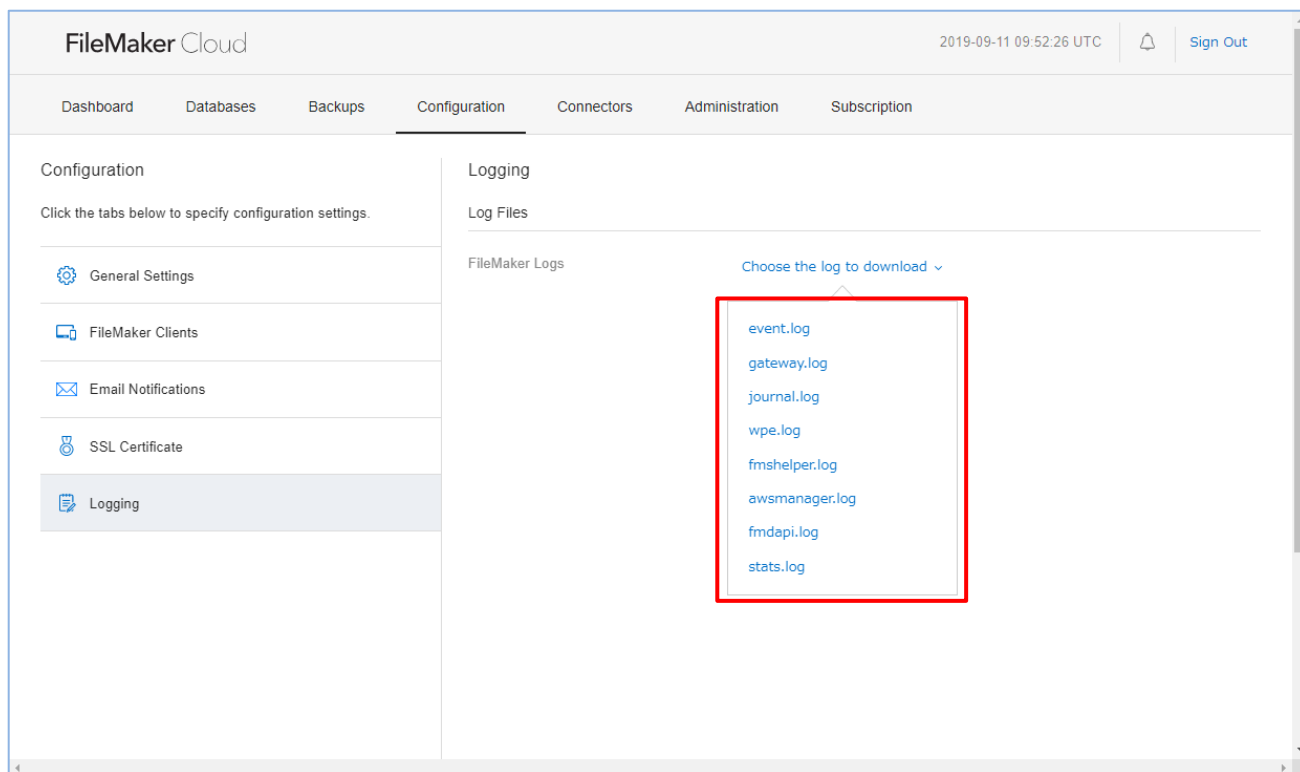


図 3 FileMaker Cloud for AWS のログファイルのダウンロード画面 (Admin Console)

2.2.2. Access.log

FileMaker Cloud for AWS では、表 3 の各ログファイルに記録される情報の他に、コネクションやデータベースのオープン／クローズ、アクセスしたアカウントとアクセス元 IP アドレス等のユーザ認証に関する情報が、「Access.log」というファイルに記録されます (図 4) ¹。

| | | | |
|-------------------------------|-------------|-----|--|
| 2019-10-15 03:51:47.564 +0000 | Information | 94 | host18 Client "user-1 (user-1 の MacBook Air) [221.xxx.xxx.xxx]" opening database "サマリーDB" as "doctor_kishi". |
| 2019-10-15 03:57:03.311 +0000 | Information | 98 | host18 Client "user-2 (user-2 の MacBook Pro) [17.xxx.xxx.xxx]" closing database "サマリーDB" as "doctor_miyazaki". |
| 2019-10-15 03:57:03.312 +0000 | Information | 22 | host18 Client "user-2 (user-2 の MacBook Pro) [17.xxx.xxx.xxx]" closing a connection. |
| 2019-10-15 05:36:03.425 +0000 | Information | 638 | host18 Client "user-2" opening a connection from "user-2 の MacBook Pro (17.xxx.xxx.xxx)" using "ProAdvanced 18.0.3 [fmapp]". |
| 2019-10-15 05:36:03.426 +0000 | Information | 94 | host18 Client "user-2 (user-2 の MacBook Pro) [17.xxx.xxx.xxx]" opening database "サマリーDB" as "doctor_miyazaki". |

図 4 FileMaker Cloud for AWS の Access.log (サンプル)

このファイルは FileMaker Cloud for AWS が AWS 上に保有するファイルですが、現状、Admin Console から取得できないため、SSH アクセス ² 経由で取得します。

¹ クラリス・ジャパン株式会社に仕様確認済み。(2019 年 10 月)

² <https://fmhelp.filemaker.com/cloud/18/ja/fmcgsg-aws/#aws-security-features>

2.3. FileMaker Pro 18 Advanced

FileMaker Pro Advanced を単体で利用する場合は、FileMaker 関数、スクリプト、スクリプトトリガ等を利用して、アクセスの記録を取得することができます。

詳しくは、3 章を参照してください。

3. より詳細なアクセスの記録の取得方法の例

3.1. 機能を自作する

FileMaker Pro Advanced を単体で利用する場合、あるいは、FileMaker Server におけるイベントログ及びアクセスログに記録される情報よりも詳細な記録を残したい場合は、FileMaker 関数、スクリプト、スクリプトトリガ等を利用して、必要な情報を取得することができます。

なお、以下の実装例は、より詳細なアクセスの記録を取得するために利用可能な方法の一つであって、それを実現するための唯一の方法ではありません。各 FileMaker カスタム App に求められる機能や利用されるシーンに合わせて、適切な方法を検討してご利用ください。

3.1.1. ユーザのログイン時刻、利用時間等を記録する

✓ 実装方針：

- ・ データベースにログ用のテーブル（「サインインログ」）を用意して、アクセスの記録をレコードとして保存する
- ・ FileMaker プラットフォーム標準のログイン・ダイアログの代わりに、カスタムダイアログを作成し、必要なデータ（ログイン／ログアウト時刻、パスワード変更イベント等）を取得する
- ・ イベントの時刻は、「サインインログ」の新規レコード追加時刻を利用する

✓ スクリプト例：

```
変数を設定 [ $Account ; 値: Get(アカウント名) ]
変数を設定 [ $Operation ; 値: Get(スクリプト引数) ]
#
レイアウト切り替え [ 「サインインログ」 ; アニメーション: なし ]
If [ $Operation="サインイン" ]
    カスタムダイアログを表示 [ "サインイン" ; "ユーザ名とパスワード指定し、サインインをクリックして下さい。" ; $Account ; $Password ]
    If [ Get(最終メッセージ選択)=1 ]
        再ログイン [ アカウント名: $Account ; パスワード: ..... ; ダイアログあり: オフ ]
        変数を設定 [ $Error ; 値: Get(最終エラー) ]
        #
        If [ $Error = 212 ]
            カスタムダイアログを表示 [ "エラー" ; "指定されたアカウント名とパスワードはこのファイルへのアクセスに使用できません。" ]
        Else If [ $Error = 0 ]
            新規レコード/検索条件
            フィールド設定 [ サインインログ::操作内容 ; "サインイン" ]
            フィールド設定 [ サインインログ::ログインアカウント ; $Account ]
            レコード/検索条件確定 [ ダイアログあり: オフ ]
        End If
    End If
End If
Else If [ $Operation="パスワード変更" ]
    カスタムダイアログを表示 [ "パスワード変更" ; "新しいパスワードを指定して下さい" ; $Password1 ; $Password2 ]
    If [ Get(最終メッセージ選択)=1 ]
        If [ Exact($Password1;$Password2) ]
            パスワード変更 [ 旧パスワード: ..... ; パスワード: ..... ; ダイアログあり: オン ]
            変数を設定 [ $Error ; 値: Get(最終エラー) ]
            If [ $Error = 1 ]
                カスタムダイアログを表示 [ "メッセージ" ; "パスワードの変更をキャンセルしました。" ]
            Else If [ $Error = 208 ]
                カスタムダイアログを表示 [ "エラー" ; "パスワードに十分な文字が含まれていません。" ]
            Else If [ $Error = 209 ]
                カスタムダイアログを表示 [ "エラー" ; "現在のパスワードと新規パスワードを同一にすることはできません" ]
            Else If [ $Error = 0 ]
```

```

        カスタムダイアログを表示 [ "メッセージ"; "パスワードは変更されました。" ]
        新規レコード/検索条件
        フィールド設定 [ サインインログ::操作内容 ; "パスワード変更" ]
        フィールド設定 [ サインインログ::ログインアカウント ; $Account ]
        レコード/検索条件確定 [ ダイアログあり: オフ]

    Else
        カスタムダイアログを表示 [ "エラー"; "処理中に何らかのエラーが発生しました。システム管理者にエラー番号を伝えてく
        ださい (エラー番号 : " & $error & ") " ]
    End If

    Else
        カスタムダイアログを表示 [ "エラー"; "指定されたパスワードと確認用パスワードの内容が一致しません。" ]
    End If
End If
End If
レイアウト切り替え [ 「初期画面」 ; アニメーション: なし ]

```

3.1.2. データ（レコード）の追加・削除を記録する

✓ 実装方針：

- ・ データベースにログ用のテーブル（「操作ログ」）を用意して、レコードの追加・削除のイベントを記録する
- ・ レコードが削除されたときは、テーブルに用意しておいた「削除フラグ」フィールドにフラグ値を設定し、以降の処理では削除されたレコードとして扱う

✓ スクリプト例（削除操作の記録）：

```

# スクリプト引数： 操作内容、テーブルオカレンス名、レコードのプライマリキーが改行区切り
変数を設定 [ $Operation ; 値: GetValue (Get(スクリプト引数);1) ]
変数を設定 [ $Table ; 値: GetValue (Get(スクリプト引数);2) ]
変数を設定 [ $PKey ; 値: GetValue (Get(スクリプト引数);3) ]
変数を設定 [ $Account ; 値: Get(アカウント名) ]
#
If [ $Operation="削除" ]
    # 現在のレコードの削除フラグに「1」をセットすることで、論理削除とします。
    # 論理削除が行われた後のレコード操作はアクセス権セットおよび、レイアウト対応とします。
    フィールドを名前を設定 [ $Table & "::削除フラグ" ; 1 ]
End If
#
# 操作ログ記録用のレイアウトに切り換え
レイアウト切り替え [ 「操作ログ」 (操作ログ) ; アニメーション: なし ]
新規レコード/検索条件
フィールド設定 [ 操作ログ::操作内容 ; $Operation ]
フィールド設定 [ 操作ログ::ログインアカウント ; $Account ]
フィールド設定 [ 操作ログ::対象テーブル ; $Table ]
フィールド設定 [ 操作ログ::操作対象レコード主キー ; $PKey ]
フィールド設定 [ 操作ログ::タイムスタンプ; Get(ホストのタイムスタンプ) ]
レコード/検索条件確定 [ ダイアログあり: オフ ]
#
# 操作ログ記録用のレイアウトに切り換え前のレイアウトに戻る
レイアウト切り替え [ 元のレイアウト ; アニメーション: なし ]

```

3.1.3. データ（レコード）の編集を記録する

レコードの編集操作を記録するには、FileMaker 関数・スクリプト・スクリプトトリガなどを利用して実装することも可能ですが、商用ツールを利用することにより簡便に効率良く機能を実装することが可能です。

編集記録を取得可能なツールについては、3.2 節を参照してください。

3.1.4. データ（レコード）の表示を記録する

✓ 実装方針：

- ・ スクリプトトリガ OnRecordLoad により、表示されたレコードの主キーを操作ログ用テーブルに記録する

✓ スクリプト例：

```
# このスクリプトは、レイアウトのスクリプトトリガ（OnRecordLoad）で起動する様に設定
# ウィンドウの固定
変数を設定 [ $Operation ; 値: "レコード表示" ]
変数を設定 [ $Table ; 値: Get ( レイアウトテーブル名 ) ]
変数を設定 [ $PKey ; 値: 操作ログ::主キー ]
変数を設定 [ $Account ; 値: Get(アカウント名) ]
#
# ターゲットのテーブルに余計なOnRecordLoadを発生させないために、
# 新規ウィンドウを開き操作ログレイアウトを表示。レコードを追加して、ウィンドウを閉じる。
新規ウィンドウ [ スタイル: ドキュメント ; 使用するレイアウト: 「操作ログ」 (操作ログ) ; 高さ: 0 ; 横幅: 0 ; 上: 0 ; 左: 0 ]
新規レコード/検索条件
フィールド設定 [ 操作ログ::操作内容 ; $Operation ]
フィールド設定 [ 操作ログ::ログインアカウント ; $Account ]
フィールド設定 [ 操作ログ::対象テーブル ; $Table ]
フィールド設定 [ 操作ログ::操作対象レコード主キー ; $PKey ]
フィールド設定 [ 操作ログ::タイムスタンプ; Get(ホストのタイムスタンプ) ]
レコード/検索条件確定 [ ダイアログあり: オフ ]
ウィンドウを閉じる [ 現在のウィンドウ ]
```

3.1.5. FileMaker Server のログファイルを世代管理する

FileMaker Server が生成するログファイルのサイズが予め指定されたログサイズに達すると、これまでログを記録していたファイルのファイル名に「-old」の文字列が付加され、さらに新たなログファイルが生成されます。さらに、新たに作成されたファイルが指定されたログサイズに達すると、既存の「*-old.log」は上書きされてしまいます。

このため、すべてのログファイルを保全するためには、ログファイルが保存されるディレクトリを定期的に監視し、「*-old.log」のファイルが生成されたことを検知した時点で、別のディレクトリに「*-old.log」ファイルの転送し、日付を含めたファイル名ヘリネームする等、ユーザによる対応が必要となります。

3.2. サードパーティ製のツールを利用する

FileMaker プラットフォームに、サードパーティ製のツールを導入することによって、アクセスの記録を取得することができます。このようなプラグイン・ツールを各クライアントに導入することにより、クライアントで行われたアクセスの記録を容易に取得することができます。また、サーバーサイド・ツールを導入することにより、ログデータ自体を別のデータベース（Oracle 等）に記録することもできます。

ただし、サードパーティ製のツールは、OS のバージョンアップや開発ベンダの都合等により、意図しないタイミングで利用ができなくなることがあるので注意が必要です。また、サードパーティ製ツールによって取得されるログがガイドライン要求事項のどの部分を満たすのか、利用者自身が十分検証する必要があります。

【サードパーティ製ツールの例】

- fmDataGuard (Linear Blue)³
- MBS FileMaker Plugin (Monkeybread Software)⁴
- SyncServer Pro (Linear Blue; server-side)⁵

³ <https://www.linearblue.com/products/fmdataguard/>

⁴ <https://www.monkeybreadsoftware.de/filemaker/>

⁵ <https://www.linearblue.com/products/syncserver-pro-database-synchronization/>

4. アクセスの記録の保護

ログファイルの保全について、厚労省ガイドラインは次のように記載しています。

アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であることから、その保護は必須である。従って、アクセスログへのアクセス制限を行い、アクセスログへの不当な削除／改ざん／追加等を防止する対策を講じなければならない。(6.5 技術的安全対策 B.(3))

これに対して FileMaker Server あるいは FileMaker Cloud for AWS において生成されたログファイルは、管理者しかクライアントマシンへのダウンロードができないものの、OS のファイルシステム上で通常のファイルと同様にアクセスが可能であるため、ログファイルに対して適切なアクセス制限を行って、ログファイルを保全する必要があります。

以下、FileMaker Server および FileMaker Cloud for AWS のそれぞれのログファイルを保全するための実施例をご紹介します。

4.1. FileMaker Server におけるログファイルの保護

FileMaker Server が記録するログファイルに関しては、Windows Server または macOS へのログインを管理者以外に行えないように、管理者のログイン情報を適切な方法で保全する必要があります。また、一般的な保全方法としては、FileMaker Server を運用するサーバーにおいて、一般ユーザのアカウントは作成せず、管理者アカウントのみがログインできる環境を作ることが挙げられます。また、ネットワークを介したアクセスに対しては、不用意なポート開放は避けることで、予期せぬ不正アクセスを防止することができます。

4.2. FileMaker Cloud for AWS におけるログファイルの保護

FileMaker Cloud for AWS が記録するログファイルは、CentOS 内の所定のディレクトリに保存されます。このディレクトリに外部からアクセスするためには、SSH (Secure Shell) を使用した通信が前提となります。

SSH による通信では、公開鍵暗号を利用し、共通鍵を暗号化して鍵交換を行っているため、秘密鍵、公開鍵の情報が漏洩しなければ、外部からのアクセスはできません。すなわち、FileMaker Cloud のログファイルが保存されているディレクトリ自体へは、正当な権限を持つユーザ以外はアクセスできません。

また、SSH が使用するポート番号「22」に対して外部からアクセスできないようにポートへのアクセスを制限することも、ログファイル保護の有効な措置となります。

4.3. ログファイルに対する改ざん・削除の検出

ログファイルに対する意図的な改ざん・削除を自動的に検出することは、一般に困難です。したがって、まずはログファイルに対する不正なアクセスを封じることが重要です。

5. 補足

アクセス記録を取得する対象操作（1.2）には、医療情報システムに対する直接アクセスに加えて、ネットワーク接続や関連情報へのアクセスも記録対象とされています。これらについては、FileMaker カスタム App だけではなく OS やネットワーク機器において得られるアクセス証跡を収集する等、別途対応を検討してください。