21 CFR Part 11
第7部　既存システムの適合化

テクニカルノート

Wolfgang Winter, Ludwig Huber, Agilent Technologies

かなり古くなったラボの装置で取得したデータを、Part 11の要求事項に適合させるために保証することが難しい場合がある。
皆さんが新しい適合済の装置に切り換えることを決めたとしても、移行の間はデータの安全を保ち、かつこのことを立証する必要がある。周到なアクションプランを用意することで、皆さんが必要となる対策は一層容易になる。

アクションプランを作成するために、レガシーデータシステム（既存データシステム）の21 CFR Part 11への適合に向けた段階的なアプローチを使用する。我々のアドバイスは、Part 11への対応で必要となるステップに主眼を置いた特定の分析ラボ装置についてのプランを皆さんが作成する手助けになる。このアプローチは3つの主要管理事項（ギャップ分析、要求事項の定義、および実行）を用いる正式のプロセスに準拠している。FDAのレガシーシステムの現状に対する解釈は非常に明快である。「レガシーシステムはPart 11への適合から免除されない」(1)。

レガシーシステムの分類

FDAの規制を受ける製薬会社が、主に技術的な理由から、現在のレガシーシステムの状態に大きな関心を持っていることは確かである。たった1つの解決策が、バイオ製薬産業が使用するすべてのレガシーシステムには当てはまる訳ではない。多くのレガシーシステムには、Part 11が義務付ける技術制御手段に違反する技術的な制限がある。技術的な管理に関する議論については、本シリーズの第一部を参照すること（2)。他にも、製薬会社はレガシーシステムの適合化に対する不十分な業者サポートに直面することがある（例えば、業者の収益が製薬産業にほとんど依存していない場合)。

レガシーシステムを適合化しようとする会社が直面する作業範囲が膨大になることがあり、空調モニターや自動化生産コントローラなどの装置、プロセス文書と標準操作手順書（SOPs）を管理するために用いるいくつかのワードプロッセシングアプリケーションソフトウェアさえも含まれることがある。レガシーシステムはその類似点から、主に以下の3つのカテゴリに分類される。

カテゴリ1。製薬産業が設立した強力なビジネスパートナである業者からのレガシーシステム。クロマトグラフシステムはこのカテゴリに当てはまる。

カテゴリ2。事業の繁盛が製薬産業に依存していないものの、基準的な技術を使用する業者からのレガシーシステム。ワードプロッセシング文書管理システムはこのカテゴリに含まれる。

カテゴリ3。中心顧客層に製薬産業が含まれない非基準的な技術の業者、およびPart 11適合性にアップグレードするだけの余裕を持てない小さな業者からのレガシーシステム。空調システムの業者がこのカテゴリに含まれる。

アプローチの相違

最初のカテゴリに含まれる業者からのレガシーシステムは、間違いなく適合化が最も容易である。カテゴリ1のシステムは、皆さんの会社とシステムメーカーの協力によって対処することができる。数人のコンサルタントが、適合化の解決策を提示するようにメーカーをプッシュすることを会社に勧めることもある。

カテゴリ2のシステムは対処するのがいくらか難しくなる。というのも、通常は、システムを適合化に向けてアップグレードするための既存の解決策をメーカーが所有していないからである。

お分かりのように、カテゴリ3のシステムからは最も大きな問題が発生する。簡単な技術的な解決策は存在していない。その上、メーカーが対象となるシステムの適合化に関心を持っていないこともある。該当するシステムをより新しいバージョンに置き換えたり、すべてを別の供給者からのシステムに交

換したりすることが、時には、唯一の解決策になる。近い将来いくつかのシステムが適合しなくなるが、だからと言って、すべてのレガシーシステムが24カ月以内に適合しなくなるわけではない。しかし、すべてのシステムについてPart 11の要求に対処するための対策を取る必要はある。どんな解決策も利用できない場合は、当局はおそらく、検討中のレガシーシステムに対する最低限のアクションプランを開発するように求めるだろう。

段階的な実行

カテゴリ1のレガシーシステムでのPart 11不適合に対処するために、段階的なアプローチが使用される。このアプローチは、アプリケーション、データセキュリティ、およびコンピュータが生成した監査証跡の実施に焦点を合わせる。本シリーズの第二部と第三部で述べられたように、監査証跡はPart 11を実行する場合の最も難しい要求事項である(3、4)。オペレーティングシステムの機能やリレーショナルデータベース管理システムなどのいくつかの既存技術を評価することが、実行上の手助けになることがある。

3つの主要管理事項（ギャップ分析、要求事項の定義、および実行）による段階的アプローチは公式のプロセスに則っている。このアプローチはクロマトグラフデータシステム以外にも作用し、カテゴリ2のシステムだけでなく一部のカテゴリ3のシステムにおいても、Part 11の要求事項に対処するために使用できる。

ここでは、Part 11のサポートに用いるプロセスとツールの両方を例証するために、レガシーシステムのケーススタディとしてケミステーション（Agilent、パロアルト、CA）を使用する。データセキュリティとデータインテグリティを達成するために、適合性の解決策には標準的なツール（Windows NTのセキュリティ機能）と標準的な機能（コピーとペースト、改訂管理） を使用する。また、それらの能力と限界についてツールを評価して、なぜ、どのようにそれぞれを評価したのかを議論する。

ステップ1、ギャップ分析

実行プランにおける最初のステップは現状調査にすべきである。システムのどの部分がPart 11に不都合かあるいは適切であるかを割り出して、現在のデータ構造を特定する。さらに、Part 11に完全に適合するために付け加える必要のあることを決定する。

現在のデータシステムのほとんどは、事前に定義された場所とサブディレクトリを持ったファイルベース構造を使用している。我々の例では、生データとメタデータは別々のサブディレクトリに格納され、すべての生データは生データファイルに独自のサブディレクトリを持っている。メタデータ（メソッド、シーケンス、およびログブックなど）は別のディレクトリに格納される。データ構造は、メタデータの完全なリンクや安全な保管なしに、メソッドを生データと同じサブディレクトリに格納する。

以上の状況はファイルベースシステムではごく一般的である。そのようなシステムは、通常1つのソースからデータを収集して、様々な場所にそれを格納する。それらの場所は決してリンクされず、かなり頻繁に上書きされる一時データと格納される結果データとにデータは分けられる。一時データと永久データの分割、特に一時データの上書きはPart 11に明白に違反しており、対処する必要がある。

ギャップ分析。我々のケーススタディでのギャップ分析から、典型的なファイルベースシステムにとしての結果を得た。

- システムのデータ処理の設計はデータセキュリティを保証しない。例えば、電子記録はコンピュータのハードディスクに格納され、突発的なあるいは意図的な上書きからは保護されない。
- アプリケーションソフトウェアは、起動時に固有のユーザIDやパスワードの入力指示ができない。
- 関連する記録の間のリンクは、脆弱だったり実在しなかったりする。例えば、関連する記録は1つの中央場所に格納されるのではなく、さまざまな分散したファイルに格納される。
- 監査証跡は不完全か、もしくはユーザ依存のどちらかであったり、両方のことだったりする。

ステップ2、定義済みの要求事項

次のステップは、最初のステップで発見されたギャップに適切に対処するための実行プランである。このプランでは変更の領域を定義し、解決策を提案する必要がある。プランでは使用されるツールを必ずしも定義する必要はないが、どのタスクにどのツールを使用するかを示す必要がある。我々の場合は、データを一時的なディレクトリに保護する必要があり、そのデータを固定記憶装置の場所にコピーするために標準的なファイルシステムの機能を使用する必要がある。

Part 11プラン実行のためのステップは、以下のプロセスアプローチに記載されている。

定義フェーズ。ギャップ分析の結果を基にした新しいソフトウェアのために、要求事項を定義して文書化すること。

プロダクトデザインフェーズ。可能なところでは、現在の実行の評価を最終的なデザインに組み入れて、現在利用できるツールからてこ入れすること。ぜひとも、現在のシステムで既に良いことを再利用すること！

実行。プロダクトデザインを、以前のステップで文書化されている要求事項を立証的に実行するコードに変えること。テストケースとテスト結果を書き留めることを忘れないこと。

我々のケーススタディでは、定義フェーズでセキュリティ要求事項と要求事項の

データインテグリティに対する具体的な影響を文書化する。ここには、システムが管理している電子記録のすべての変更と修正とともに、コンピュータ生成の信頼できる監査証跡を含める必要がある。

既存のツール

プロダクトデザインフェーズには、NTファイルセキュリティを含むWindows NTや中央のデータ集積所となるためのリレーショナルデータベース管理システム（RDBMS）など、何らかの商業的に利用できるソフトウェア技術の評価が含まれる。

Windows NTファイルシステム（NTFS）では、あるファイルとディレクトリへのアクセスを制限するためにファイルのアクセス許可を使用する。あいにくこの技術は、ファイルベースのデータ管理システムのデータセキュリティの要求すべてを満たさないことがある。NTFSアクセス許可構造の1つの制限は、アプリケーションがアクセスするデータとユーザがアクセスするデータとをオペレーティングシステムがほとんど区別できないことである。通常、電子記録を修正するアプリケーションは、その時にログオンしているユーザを認識する。このことで、データセキュリティとしてのNTファイルアクセス許可の使用が、データディレクトリの読み取り/書き込みの常時アクセスを必要としないアプリケーションだけに制限される。

アクセス拒否。以下の例はNTFSアクセス許可を使用する場合の可能性と限界を示す。ソフトウェアアプリケーションはデータ取り込みの間、ログブックエントリを作成する。このアプリケーションはログブックが格納されるフォルダに読み込み/削除のアクセスができなければならない。というのも、いくつかのログブックデータは他のディレクトリにコピーされ、データ取り込みの終了時にログブックのデータ量を最小化するために削除されるからである。このフォルダにアクセスするとき、NTはこのアプリケーションを現在ログオンしているユーザとして認識する。このユーザがそのフォルダにアクセスできる場合にのみ、アプリケーションはログブックに書き込むことができる。その他の場合、このユーザはアクセスを拒否される。しかし、そのフォルダにアクセスできる別のユーザは、ディレクトリで直接データを操作するためにデータにアクセスすることができる。データ作成が一時的なイベントのときはいつも、またアプリケーションの削除特権が所定のディレクトリに要求されないときは、NTファイルのアクセス制限がデータセキュリティのニーズに対処する。

上記の例はまた、Part 11の実行に際してのレガシーシステムに対する新しいシステムの優位性を完全に浮き彫りにしている。新しいシステムは設計によって問題を防止することができる。これに対し、レガシーシステムはその機能の一部としてデータを削除するように設計されていて、アドオンフックの問題に対処する必要がある。従来のデータ管理設計に対する現代のデータ管理設計についての詳細な議論については、本シリーズの第三部を参照すること（4）。

Windows NTのアクセスセキュリティの対象は、「1台のパーソナルコンピュータ（PC）で作業する1人のユーザ」という前提に限られる。NTは、複数のユーザ間で共有しているデスクトップに関するデスクトップセキュリティについては、共通のNTアカウントを使用したユーザの一意の識別をやめない限り、どんなサポートも提供しない。しかし、クロマトグラフのデータ取り込み環境は、複数のユーザが1台のコンピュータを共有し、同じPCから数台の機器を操作することをたびたび必要とする。共有ログオンの議論については、第二部を参照すること（3）。

リビジョン管理。ファイルベースのNTシステムにおけるもう1つ別の問題は、電子記録の改訂管理または改訂制御（コントロール）である。Part 11は、すべての改訂結果に生データとメタデータの両データを付して格納することを要求する（以前のエントリを上書きしてはいけない）。クロマトグラフのデータファイルは、特にダイオードアレイや質量分析などの3-D技法によるものは、ファイルサイズが数メガバイト（MB）に及ぶ。このデータをマルチ再処理する場合は、1つの結果に対する完全なデータインテグリティは最終的に10－20MBのデータになってしまい、不都合なだけでなく性能に影響を与えかねない。

我々は、次のような評価基準によって、NTがシステムのデータセキュリティ実行に適していることを見つけた。

- すべてのユーザはユーザ自身のPCを持ち、通常はPCを共有しない。
- アプリケーションソフトウェアは通常、適切な取り込みファイルにデータを収集しながら取り込み専用モードで実行される。
- データの再処理は要求されない。あるいは、そのような要求事項は極めて限定されている。
- アプリケーションソフトウェアがデータを修正する場合、NTログブックとファイル監査オプションとを用いて監査証跡が作成されるように、このソフトウェアがファイルに修正データを書き込む。

それらの要求事項は多くの標準的なシステムを除外するので、より高度なデータ保管と結果管理オプションを考察することは役に立つ。

データ保管。Part 11の要求事項は、ボリュームの大きな互いに依存しているデータ用に1つの中央データロケーションを用いたデータの管理と保管の解決策と、権限を有する人にデータアクセスを限定するための組み込みのユーザ管理を提供する解決策も義務付けている。解決策もまた、変更履歴（自動監査証跡）などの簡単な改訂管理ツールを提供する必要がある。このことはデータベース管理システムのための理想的なタスクのように思われるが、どうだろうか？

定義上、リレーショナルデータベースは中央のデータ集積所である。デー

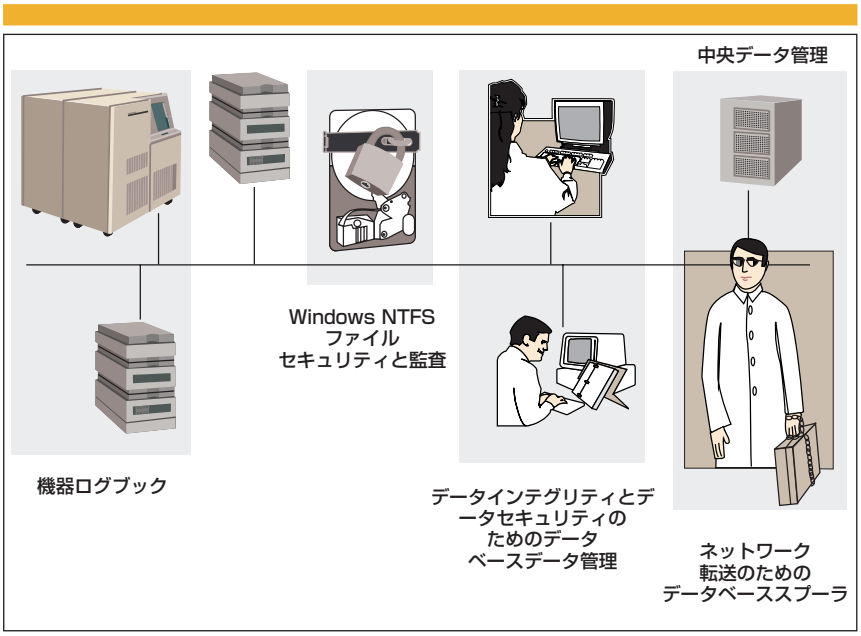

図1. Agilentのケミステーションセキュリティパックで使用されるセキュリティツール

タベースシステムにおける改訂の管理は、フラットファイルシステムよりも洗練されていて達成が容易である。リレーショナルデータベースは、すべてのデータ（生データとメタデータの両方）に新しい結果を付して格納する代わりに、データ項目をテーブルとこのテーブルに対するリンクに格納する。さらに、RDBMSは、監査証跡での容易な変更文書化を考慮するために、以前のデータバージョンと結果を比較するデルタ値として、新しい結果を格納する。データベースの知的なバックアップとアーカイブは付加的なセキュリティを提供するが、このことは、ハードディスクに欠陥がある場合に生じるような物理的な損失の場合においてさえもデータが再現できることを意味する。

ケーススタディでは、RDBMSが仕事のための理想的なツールになるとの結論を下した。この特別の場合では、クロマトグラフの結果データの既存のスタディデータベースシステムの適用性が現状調査の一環として調査された。我々の初期評価はまったく間違っておらず、改めて一からやり直す必要のないことを示した。

しかし、既存のデータベースシステムを安全な中央データ集積所として選択することは1つの重要な質問に答えていない。どんな方法で既存のデータファイルをレガシーデータシステムからPart 11に適合したデータベースに移動するのか？直接保管にはソフトウェアコードの大幅な変更が必要なので、データベースでの直接保管はレガシーシステムとめったに互換性がない。したがって、データをファイルシステムからデータベースにコピーする必要がある。このコピープロセス自体が信頼できる監査証跡を有する必要があり、ユーザの干渉や操作から保護される必要もある。

ステップ3、実行

完全なデータセキュリティのための成功の秘訣は、取り込みデータの保管を最終データの保管と管理から切り離すことである。実行へのアプローチの1つでは、取り込み中の中間的なデータバッファとしてハードディスク上にある所定のファイルベースのデータ構造を使用し、すべての取り込みと最初の合格結果データを作成直後にハードディスクからコピーする。基本的にデータのコピーは、保護されていない不確かな場所から、データを信頼できるファイル場所に転送するか、データベースに直接転送するかのいずれかになる。

データ転送を管理するためのツールの1つは、標準的なWindowsの機能からスプール済み転送（プリンタスプーラの動作方に類似）を入手できる。もちろん、コピープロセスはPart 11のセキュリティ要求事項に従う必要がある。コピープロセス中の重要なセキュリティ要求事項には次のようなものがある。

- コピーコマンドを保護された場所に格納して（NTFSアクセス権を通常使用する）、権限のないアクセスを拒否すること。
- 転送エラーの場合に、転送の問題を管理および文書化するオペレーティングシステムを使用して、データ管理を保証すること。
- データの正確さを確認するために、例えばチェックサム計算を使用して、データ転送の正確さと完全性を確保すること。チェックサム保護は、すべてのデータファイルがハッシュ値を持っていることを意味する。それぞれの時間データがネットワークを通して転送されると、チェックサムが再計算されて初期値と比較される。逸脱があると、それぞれエラー警告として表示され、対応するデータ転送は取り消される。

最終的な設計案。我々のケーススタディにおける最終的な設計案は、結果の保管にはリレーショナルデータベースを定義することに帰する。ここでは、ローカルハードディスク上に一時的なデータファイルを確保するためにNTFSアクセス許可権を用い、さらに、ネットワークを通して正確にかつ完全にデータを転送するためにデータ転送ツールを用いる。それらの主要要素の組み合わせによって、システムソフトウェアの要求事項すべての実行が、レガシーシステムを21CFR Part 11に完全適合することを可能とする。図1に、クロマトグラフデータシステムでデータセキュリティ、データインテグリティ、およびシステム生成の監査証跡を確保している、我々

の実行プランの主要な特色を示す。

実行中の問題。実行プロセス中に、概してユーザは更なる問題に必ず直面する。主な難問は、アプリケーションのセキュリティ機能の完全性と有効性を確実にするために繰り返して再確認する反復プロセスの必要性である。このことは、ソフトウェアをテストして評価する内部と外部の両方のユーザを巻き込む。もう1つの難問は、実行時の問題について決定することである。時々、1つの機能に1つ以上の実行選択肢があり、これが全体の機能になると質問されるかもしれない（「我々はなぜ、この愚かなチェックを同じように必要とするのか？」）。そのような状況では、最終決定をするときに助かるとの評判が良い中立のレフリーやタイブレイカが役に立つ。中心的なQA担当からのバリデーション専門家が、それらの状況において実際に有用であることを証明している。

成功。特定のデータ構造に対する重要な変更を実行する場合、データ取り込みと保管の分離は、データ取り込みと再解析のサイクルの間のデータを保証することの問題に対する一般的な回答と考えられるかもしれない。クリーンな実行プロセスの主な要求事項は、データ転送の適切な管理と、データベース管理システムのOracle（Redwood Shores、CA）やWindows NTオペレーティングシステムに見られるような標準的な製品のセキュリティツールである。監査証跡と改訂管理は、リレーショナルデータベースの結果管理を用いると容易に実施される。

参考文献

(1) P. Motise,“Update on 21 CFR Part 11［21 CFR Part 11の更新］,” presentation at the Institute of Validation and Technology Electronic Records and Signatures conference［バリデーションとテクノロジー学会 電子記録と電子署名会議でのプレゼンテーション］,Washington DC, August 1999.

(2) L. Huber,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 1, Overview and Requirements,”BioPharm 12 (11), 28−34 (1999).（日本語版は，Ludwig Huber，近藤　直人，21 CFR Part 11 試験室における電子署名と電子記録；第一部　規制の概要ならびに要求事項，横河アナリティカルシステムズ，2000年6月，資料番号TI 16C0A3-004）

(3) W. Winter and L. Huber,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 2, Security Aspects for Systems and Applications,”Bi4oPharm 13 (1), 44−50 (2000).（日本語版は，W. Winter, L. Huber，近藤　直人，21 CFR Part 11 試験室における電子署名と電子記録；第二部　システムとソフトウエアのセキュリティー，横河アナリティカルシステムズ，2000年11月，資料番号TI 16C0A3-005）

(4) W. Winter and L. Huber,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 3, Ensuring Data Integrity in Electronic Records,”BioPharm 13 (3), 45−49 (2000).（日本語版は，W. Winter, L. Huber，近藤　直人，21 CFR Part 11試験室における電子署名と電子記録；第三部　電子記録の完全性保証，横河アナリティカルシステムズ，2001年4月，資料番号TI 16C0A3-006）

Printed in Japan, October 01, 2002
5988-0948JAJP

http://www.agilent.co.jp/chem/yan
横河アナリティカル システムズ株式会社