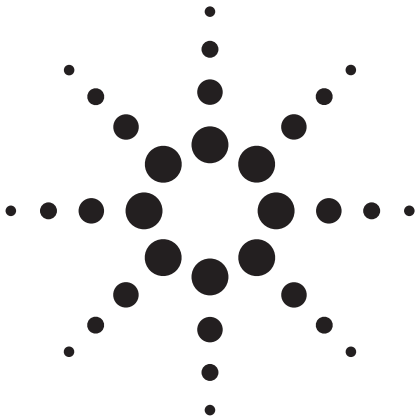

21 CFR　Part 11への対応

Agilent Technologies

21 CFR　Part 11への対応

試験室における電子署名と電子記録

第1部　規則の概要ならびに要求事項

第2部　システムとソフトウェアのセキュリティ

第3部　電子記録の完全性保証

第4部　データ変換および長期保管

第5部　装置制御とデータ取り込みの重要性

第6部　バイオメトリック認証：その限界と可能性

第7部　既存システムの適合化

BioPharm投稿文「Part 11は消えていない」

21 CFR Part 11
試験室における電子署名と電子記録
第1部　規則の概要ならびに要求事項

テクニカルノート

Ludwing Huber, Agilent Technologies
近藤　直人，横河アナリティカルシステムズ株式会社

はじめに

1997年, 米国食品医薬品局（United States Food and Drug Administration, FDA）は, 医薬品業界からの要望に答え, 電子記録(electronic records), 電子署名(electronic signature)および手書き署名(handwritten signature)に関するFDA規則を公布した(1)。連邦規則第21条第11章（21 CFR Part 11）と称する本規則で, 電子記録, 電子署名を紙の記録(paper records)および手書き署名と同等と見なすことが可能となった。本規則はFDAの医薬品関係の規制すべてに適用される。すなわち, 医薬品の安全性に関する非臨床試験の実施の基準(Good Laboratory Practice, GLP), 医薬品の臨床試験の実施に関する基準(Good Clinical Practice, GCP), および医薬品の製造ならびに品質管理に関する規則(current Good Manufacturing Practice, cGMP)も適用範囲である。

業界担当者およびFDAは, 電子署名, 電子記録の使用によるコスト削減, 医薬品審査期間の短縮, 申請書調査の迅速化, 生産性の向上を期待している。現在, 電子署名の採用ならびに申請資料への利用は, 強制されていない。それにもかかわらず, 製薬会社は本規則対応を可能な限り早急に進めようとしている。これには, 主に次の三つの理由による。

1) 現在, 試験にコンピュータを使用しないことは不可能であるから。たとえば, 試験室では, 機器からのデータの取込, 定量計算にコンピュータは不可欠となっている。この様な場合, 試験室のPart 11対応は「必須事項」となる。
2) 将来FDAが紙の記録を受け付けない時代が来るかもしれない。
3) 紙の記録に比べて電子記録にはいくつかの優れた点がある。たとえば, 保存に場所をとらないこと, 検索が容易なことなど。

本規則の試験室に対する基本的な要求事項は

* 既存, 新規に関わらず, バリデーションを済ませてからコンピュータシステムを使用する。
* 分析を再現できるよう電子記録を安全に保管する。
* ユーザとは無関係に, 自動的にコンピュータが監査証跡(Audit Trail)を作成する機器を使用する。
* システムアクセス制限により, システムおよびデータの安全保障(security), データの完全性(integrity)を確保する。
* クローズド(closed system)およびオープンシステム(open system)双方において信頼性の高い電子署名を使用する。
* オープンシステムではデジタル署名(digital signature)を使用する。

製薬会社の分析試験室では, 新規則に対応するために, 装置, 作業手順, 分析担当者に大きな影響がおよぶ。

* 現行の署名の再評価。(誰が, いつ, 何に署名しているか)
* システムとデータへのアクセスを制限するために, 社内および試験室での新規作業手順の作成(誰が何をできるか)。
* 規制に確実に対応するため, 該当コンピュータシステムのアップグレードや交換。
* 法的拘束力のある署名の基礎となるユーザID(identification code)とパスワード(password)の使用方法や取扱方法を変更。
* 電子保管(electronic archive)に対応できる専門的能力を持つ新規人材を採用。

本規則には, 1994年に公開した原案に対する業界からの130に上る意見へのFDAのコメントが納められている。それにもかかわらず, 企業内情報技術担

Agilent Technologies
Innovating the HP Way

TI 16C0A3-004
2001. 1 改訂（第 2 版）

当者や分析担当者にとっては,実際に規制に対応するには,未だに多くの不明確部分が残されている。最大の問題点は,過不足のない対応がどのあたりであるかである。

よくある問題点は,
* 最終的に承認されるまでに何回も再計算の必要があるデータでは,どの程度の記録が必要なのか?
* 自動監査証跡を実現する方法はあるのか?監査証跡として何をどこまで記録すればいいのか?
* 電子記録と電子署名とをいかにして関連づけるのか?
* Part 11に対応できない装置をどのように取り扱えばいいのか?
* 10年後にデータを再現できることをどのように保証するのか

本シリーズでは,分析試験室が効率よくこの規制に対応するための一般的な指針といくつかの例を紹介する。本規則は複雑で,一つの論文で全ての疑問に答えることは不可能なため,シリーズ化することとした。本論文は一連の論文の第1報目である。また,規制に対応していくには現在も依然として複雑で不確実な部分がある。詳細についての議論はいまだに進行中である。たとえば,監査証跡に記録される時刻は,グリニッジ標準時か現地時間のどちらにするか,データを取り込んだ時点または再計算時のどの時点でデータを保管するのかなどである。

第一回は,本規則の概要,用語,重要な点,分析試験室への影響について論じる。2報目以降では,より具体的な以下の内容について解説する。

1. システムへのアクセス制限と作業の承認
2. 生データ(raw data)および最終データ(final data)の定義および長期保管。
3. クロマトグラフィー用データシステムにおける監査証跡。
4. クローズドシステムおよびオープンシステムにおける電子署名。

本文記載事項は,本文の原稿作成時1999年8月の状況をもとにしている。本規制に関しては,様々な議論が現在も行われている。既に発表されている規制対応指針以外にもガイドラインが発表される可能性もある(2)。最新情報は,www. labcompliance. comのe-signature(21CFR11)に掲載されている。

規制作成過程と現在の状況

本規制作成は,米国製薬工業協会(Pharmaceutical Manufacturing Association, PMA, 現在はPharmaceutical Research and Manufactures of America, PhRMA)から1990年頃FDAに対して提案された。間もなく,PMAと米国Parenteral Drug Association(PDA)が本提案のためのテクニカルグループを共同で設置した。ポール・J・モティーゼ(Paul J. Motise)率いるFDA担当チームと業界代表者達は幾度も会議をもち,ペーパーレスシステムをいかにしてGMPへ適合できるか議論を重ねた。1992年,本件に対する意見を広く聞くために,FDAは規制案の事前通告(Advanced Notice of Proposed Rule Making, ANPRM)を発行した。

ANPRMが発行されると,FDAの要求に応えて規制案に対する多くの意見がFDAに寄せられた。1994年,FDAはANPRMに対する意見を反映した規則草案(proposed rule)を公表した。個人,製薬会社,輸入業者などから,再度,その草案に対する意見がFDAに寄せられた。寄せられた意見のいくつかに対して,Paul J. Motiseが回答を寄せている(3)。最終的に,21 CFR Part 11は,1997年3月に公布され,同年8月21日施行された。本規則は,FDAホームページ(http://www. fda. gov/cder/esig/index. htm)で,見ることができる。
1997年当時,本規制はその考え方や内容に対して業界から高い評価と支持を得た。しかし,時間とともに,Part 11の解釈にともなう様々な問題点が明らかとなってきた。これらの問題点は,学会や論文で発表された。

PMAのコンピュータシステムバリデーション委員会(Computer System Validation Committee; CSVC)会長を長年務め,現在は著名な業界コンサルタントであるケン・チャップマン(Ken Chapman)は,「熱い」論争の的となっているいくつかの問題点に関する論文を2つ発表して,解決法を提案している(4,5)。1998年8月号のゴールドシート(Gold Sheet)も,本件を取り上げている(6)。Ken Chapmanは,Institute of Validation Technology主催の会議でも同様の発表をしている(7)。FDAも会議に積極的に参加して,製薬会社の本規則対応を支援している。例えば,米国QA研究会(Society of Quality Assuranance, SQA)のコンピュータバリデーション部会(Computer Validation Initiative Committee; CVIC)開催の2つの会合にPaul MotiseとCharles Snipesが参加して,質疑応答を行った。

最も多くの人が参加したのは,1999年1月12日に実施された業界担当者を対象としたビデオトレーニングである(8)。全米20会場でテレビ放送が行われた。FDAから,3つのテーマで発表があった。Paul J. Motiseによる「よくある質問に対しての回答」,Halvorsonによる「バリデーション」および「Part 11とFDA査察」。FDAからは他にも数名の担当者が出席して,FDAの見解の説明,規則の推進のために積極的に発表や議論に加わった。企業によっては,2から3年の施行猶予期間を期待していたが,このビデオトレーニング(8)で規制施行までにはまだ,十分な時間があることが明らかとなった。

新規制に対する認識は高く,米国だけでなく,多くの国々で議論が行われて

いる。 以下がその理由である。

1. 米国外に拠点を置く製薬会社の多くは米国に医薬品を輸出しており, そのような企業は, 米国の規制に対応する必要がある。FDAはこれらの会社に米国の規制に準拠した査察を実施する権限を持っている。対応していない企業は, 医薬品を米国へ輸出できなくなる。その結果, ビジネスに多大な影響が生ずるから。
2. 米国以外の国々でも電子記録, 電子署名による資料提出に関して同様の問題がある。それぞれの地域での指針として米国の規制を利用する可能性が高いから。

例えば, ヨーロッパでは, EUGMP規則付属文書11 (EU GMP Annex 11 Interpretation Guide)でよく知られるInternational Association for Pharmaceutical TechnologyがPart11に関するヨーロッパにおける問題点を発表したり, 1999年9月には, ベルリンで電子記録, 電子署名に関する国際会議が開催された。これらは, ヨーロッパにある製薬会社がPart 11に積極的に対応しようとしている現れであろう。

コンピュータソフトウェアやコンピュータ化された機器のメーカは, ユーザに対してPart 11に対応したハードウェアやソフトウェアを開発, 提供することを彼ら自身の責任としてとらえている。例えば, アジレントテクノロジー社は,「Implementing Electronic Records and Signatures with Agilent Technologies's ChemStation(英語, ケミステーションにおける電子記録と電子署名)」と題するテクニカルノートを発行して, Part 11対応を手伝っている(9)。

本件関連の新規出版物, 会議, 指針についての情報は, 次の２つのホームページで精力的に取り扱われている。http://home. netcom. com/_jlboet/esiglinks. htmおよびhttp://www. labcompliance. com/e-signatures。例えば, この論文で挙げている参考文献のほとんどは, 上記のホームページやそこからのリンクで入手できる。

用語

規制の理解およびそれに対応するために, 用語を理解することは極めて重要である。ここでは, 試験室関連の具体例をつかって, 用語のいくつかを解説する。斜体文字部分は21 CFR Part 11(1)からの抜粋である(日本語は著者訳)。

電子記録:*「(電子記録とは)コンピュータシステムによって作成, 変更, 保管, 検索あるいは配布されるデジタル形式の文書, 画像, 音声, 映像, その他の情報のあらゆる組み合わせを意味する。」*

試験室における電子記録の例は,

* 機器設定条件およびデータ処理パラメータ
* 検量線
* コンピュータが取り込んだ生データ
* 解析結果
* ベースライン付きのクロマトグラム
* 装置の使用記録
* 監査証跡

これらの情報が記憶装置にデジタル形式で保存された瞬間, それは電子記録と見なされる。自動的に計算され, 中間的に使用されるRAMに書き込まれ, 記憶装置に書き込まれないデータは, 電子記録とはみなされない。HPLC紫外可視ダイオードアレイ検出器のスペクトルデータがこれに相当する。

クローズドシステム:システムへのアクセスが, システムならびに電子記録の管理責任者により管理されている環境をいう。

オープンシステム:システムへのアクセスが, システムならびに電子記録の管理責任者に管理されていない環境をいう。

多くの場合, 分析試験室のコンピュータシステムはクローズドシステムである。適切な安全管理手順を遵守することで, 試験室のシステムアクセス管理は完全なものとなる。試験室がオープンシステムとなっている可能性としては, システムの管理を外部の会社に委託している場合が考えられる。すべての人がアクセスできるホームページも, オープンシステムである。

電子署名:*「個人が作成, 承認または照査したことを証明する記号または一連の記号群としてのコンピュータデータの集合体で, 法的拘束力を有する手書き署名の同等物としてみなされる」*

電子署名は, 紙の上になされた手書き署名の電子的同等物である。指紋, 人相や声紋の識別といった生物測定(Biometrics)での特定方法を利用した電子署名も可能であるが, ユーザIDとパスワードの組み合わせで十分である。ある人のユーザIDはその会社内でその人特有のものでなければならない。クローズドシステムには, 電子署名で十分である。

デジタル署名:*「電子署名の確認ならびに電子記録の完全性を保証するために作成される, 一定の法則で暗号化された電子署名。」*

高い安全性レベルが必要となるオープンシステムには, デジタル署名が必要とされる。電子署名に加えて電子署名ならびに電子記録の暗号化が求められる。

生物測定:*「個人の身体的特徴や反復的動作の測定に基づき, 個人に特有かつ測定可能な特徴や動作により個人の同一性を検証する方法である。」*

人相や声紋認識や指紋認識がこの例である。ほとんどの場合, 特別なハードウェアやソフトウェアが必要とされ

る。この様な機器を使用する場合の最大の問題点は, バリデーション作業である。本当に特定のユーザのみを認識しているのかどうかを検証することの困難さにある。

ハイブリッドシステム(Hybrid systems):電子記録と紙の記録, 手書き署名とが共存しているシステムをいう。今日, 多くの製薬会社で採用されている。分析を再現するために生データを電子的に記録するが, 最終結果は紙に印刷して手書き署名する。FDAは禁止していないが, そのPart 11への適合性についてFDAは懸念を表明している。

メタデータ(Meta data):生データから最終報告書を再現するために必要なデータ。クロマトグラフィーでは, 積分パラメータと検量線等がこれに相当する。

要点と問題点

36ページからなる21 CFR Part 11だが, 規則本体はわずか3ページにすぎない。残りの33ページは, 業界関係者からの意見に対するFDAの見解にあてられている。

システムバリデーション

「電子記録の作成, 保管, 管理に使用するコンピュータシステムのデータの正確さ, 信頼性, 独立性および無効なデータや変更された記録を発見する機能はすべてバリデーションされていなければならない。」

これは, 既存および新規の両システムにあてはまる。規制環境下でコンピュータを使用している試験室にとっては, 基本的に新しい要求ではない。コンピュータシステムのバリデーションについては, かなり詳細な説明があり(9), 多くの製薬会社で, 実施されつつある。バリデーションに関する問題は, 新規システムよりも, 既存システムにある。既存のコンピュータシステムには, バリデーションに関する正式な試験ならびに, どのようなバリデーションがなされているのかに関する文書が必要となる。バリデーションが不可能であれば, そのシステムは21 CFR Part 11対応として使用できない。

直ちに試験を再現できるような電子記録の保管

「正確かつ完全な記録の複製を, 目に見える形式ならびに電子的に作成するための手順を作成しなければならない。当局の査察, 再調査および当局による記録の複製は, この手順に従って複製された資料を基に実施される。必要とされる記録の保管期間の間, 試験を正確かつ, すみやかに再現できるよう, 記録を保管する。」

この条文に関する第1の問題点は, 記録保管期間と現実的なコンピュータハードウエア, ソフトウエアの寿命とが大きく異なっていることである。最終結果の元となる生データならびにデータを処理した方法(メタデータ)とを一緒に保存することをFDAは求めている。データ作成時に, ユーザが使用した手法と同じものを使って, 最終結果から生データまでさかのぼることを可能にすることをFDAは希望している。最も実現困難な要求事項であろう。記録の保管は10年以上必要であるが, コンピュータハードウェアやソフトウェアの寿命はこれよりはるかに短い。これが問題である。生データとメタデータの保管, バリデーションされたファイル変換方式などの対応策に関しては, 別途議論する。

第2の問題点は, どこまでを記録として残し, 保管するかである。クロマトグラフを使った定量分析における状況は極めて複雑である。通常, データの取込, 計算, 印刷は事前に設定したパラメータに従って自動的に実行される。しかし, クロマトグラムとピークベースラインを印刷してみると, 事前に設定した積分パラメータが適切でなく, 正しいピーク面積が計算されていないことが, 時々ある。この場合, 分析担当者は生データを確認し, ピーク積分が正しく行われるように積分パラメータを変更しなければならない。この作業はトライアンドエラーで行われ, ユーザの経験に左右される部分が大きい。問題は, 最終結果と一緒に保管するのは, 最終的に採用した積分パラメータおよびクロマトグラムのプリントアウトか, あるいは, 最終的な積分条件にいたるまでの全ての積分条件かという点である。このシリーズの一つでこの点について別に述べる。

アクセス制限

「権限を有する者のみがシステムを使用できるような手順を作成する。」

物理的または論理的な方法により, 本項目は実現可能である。すでに, 多くの会社で同様の原理に基づいたアクセス制限が実施されている。ログイン時にユーザIDとパスワードを使う方法が一般的に用いられている。規制対応上の問題点として, 終夜運転で分析する際のアクセス制限がある。この間に作動しているコンピュータシステムへ権限を持たない者がアクセスするのをいかにして防止するか。例えば, スクリーンセーバーにパスワードを設定して, 不正アクセスを防止することができる。しかし, この方法も, あまりにも頻繁にパスワードやユーザIDの入力が必要になると現実的な対応ではなくなる。このシリーズで, 他の方法について論ずる。

ユーザと無関係にコンピュータが自動的に作成する時間記録を伴った監査証跡

「電子記録および電子署名に使用するコンピュータシステムは, 分析担当者が行ったコンピュータへの入力および電子記録の作成, 修正, 削除等の作業を, 自動的に記録する監査証跡の機能を有していなければならない。監査証跡は, コンピュータ自身が自動的に作成し, 作業内容を時間とともに記録する。また, 監査証跡記録を改変する事ができないような安全保障機能を有していること。監査証跡自身は, 対応する電子記録の保管期間と同じ期間保管し, 当局による閲覧やコピーに利用できるようにする。」

この節については, 多くの疑問点や論議がある。主に問題になるのは, どのように実施するのか, どこまで詳細な記録が必要なのかという点である。例えば, 検量線作成時にはどの記録が必要かといった点である。たとえば, 化合物名入力時のタイプミスを全て記録する必要があるのか。リターンキーを押した時点で記録するべきか, 検量線作成終了時に記録するべきか? 入力確認作業の回数が過剰になれば, 分析担当者の生産性に影響がでる。Ken Chapmanは, ある多国籍企業の所有する品質保証検査用の新LIMSシステムの査察状況を報告している。そのLIMSシステムは「完全監査証跡」機能を備えており, 3日後には5,000件の, 記録第5日目の監査最終日には15,000件の入力が見つかった。

次に問題となるのが, 試験担当者の過剰反応である。もし, 試験を再現するために, 試験担当者が実施した全てを記録しなければならないと考えたとすると, 担当者の生産性は著しく損なわれる。

クローズドおよびオープンシステムにおける電子署名の運用

「記録と署名の偽造を防ぐため, 電子署名の結果生じた行為, 行動に対する責任は, その署名を行った個人に帰することを明確にした電子署名の責任に関する規則を作成しその厳守につとめなければならない。」

電子署名に関する手順を作成すること以上に, ユーザIDとパスワードの管理に対する従来の考え方自身を変化させることが要求される。手書き署名を偽造する方法を同僚に教えることに比べて, 同僚間でパスワードを共有する事に対する抵抗ははるかに小さい。しかし, これはPart 11においては, 同じこととなる。

第二の問題点は, いったん署名された記録の完全性をいかに保証するかである。この問題に関する技術的な対応方法を, 本シリーズで別に論じる予定である。

オープンシステムでのデジタル署名の使用

「電子記録の作成, 修正, 保存, 転送にオープンシステムが使用される場合には, 電子記録が作成された時点から受領時点までの信頼性, 完全性及び, 必要に応じては機密性を確保できるような手順ならびに管理方法を用いる。この様な手順ならびに管理方法には, 11. 10で定めたクローズドシステムでの手順と管理に加えて, オープンシステムにおける記録の信頼性, 完全性, 機密性を保証するための追加手順としての文書暗号化や適切なデジタル署名が含まれる。」

文書暗号化ソフトウェアが必要になる。場合によっては, デジタル署名を作り出すハードウェアとソフトウェアが必要となるかもしれない。本シリーズで本件を取り上げる。

まとめ

電子署名と電子記録のもたらす影響は大きい。その大きさは, 80年代初頭のGood Laboratory Practiceや90年代前半のバリデーション導入時に匹敵する。完全な実施までは一定の時間が必要となる。以下に, Part 11に適合するためのステップをまとめた。

1. 施設や試験室内の作業で, 21 CFR Part 11の影響をうける作業を特定する。
2. 品質保証部門, 試験担当者, 情報管理(IT)部門がある場合にはその部門の人々からなるプロジェクトチームを設置する。
3. 施設内, 試験室での実施計画を作成する。
4. 円滑に実施できるようなインフラストラクチャーを準備する。
5. 電子記録, 電子署名に完全に対応するのか, ハイブリッドシステム(電子記録と紙の記録, 手書き署名の併用)を採用するのかを決定する。
6. 全社員に規則, 特に電子署名に対する理解とその責任についての認識を高める。
7. 施設, 試験室その他の関係部署職員を教育訓練する。
8. 現在行われている署名が, 規制の点からも本当に必要かどうか見直す。
9. ラボ内の全設備を確認し, 設備面でのPart 11対応をどうするかの計画を策定する。
10. コンピュータシステムについての機能仕様を作成する。
11. 新しいコンピュータシステムのバリデーションを実施する。 機器の適格性確認の各ステップ, 設計の適格性確認(DQ), 据付時の適格性確認(IQ), 稼働性能適格性確認(OQ)および稼働時適格性確認(PQ)を実施する。

12. 10で特定した仕様を用い,既存システムを評価する。仕様に適さない場合は,システムのアップグレードを検討する。アップグレードが不可能ならば,システムを交換する。
13. システムへのアクセスが権限所有者に限定されるような手順を作成する。
14. データ完全性を確実にするための監査証跡実施手順およびに全保存期間にわたるデータ再生が可能な長期保存作業手順書を作成する。

引用文献

1. Code of Federal Regulations, Title 21, Food and Drugs, Part 11 "Electronic Records; Electronic Signatures; Final Rule; Federal Register 62 (54), 13429-13466.
2. Paul Motise (FDA), responses to questions posed by the PhRMA Computer System Validation Committee about Electronic Records and signatures regulation (responses received April 21, 1997).
3. Paul Motise (FDA), responses to questions posed by the PhRMA Computer System Validation Committee about Electronic Records and signatures regulation (responses received June 12, 1997).
4. K. Chapman and P. Winter, A Way Forward, Pharmaceutical Technology, Sept. 1998。
5. K. Chapman and P. Winter, Addressing Validation Rules, Validation Technology, Vol 5 (1), Nov. 1998, 46/52.
6. Gold Sheet, August 1998, published by F-D-C Reports, Chevy Chase, MD, USA.
7. Ken Chapman, Interpretations of part 11 that require more discussion, paper to be presented at the IVT Conference on Electronic Signatures and Electronic Records, April 19/20, 1999, Washington D. C., US.
8. Paul Motise: Part 11; Electronic Records, Electonic Signatures; Answers to Frequently asked questions, Jan Halvorsen: Computer Validation: Electronic Records; Electronic Signatures and Chris Nelson: Part 11 and FDA Inspections, presented at FDA's industry training on 21 CFR Part 11, Broadcasted to 20 sites in the U. S. on Jan. 12, 1999.
9. Implementing Electronic Records and Signatures with Hewlett-Packard's ChemStation, Hewlett-Packard publication number 12-5966-2315E, Waldbronn Germany, 1998。

5980-1308JA
January 22, 2001.

Agilent Technologies(アジレント・テクノロジー社)は、ヒューレット・パッカードの電子計測、化学分析、電子部品と医用電子の４つの事業が独立した新会社です。

http:/www.agilent.co.jp/chem/yan

21 CFR Part 11
試験室における電子署名と電子記録
第 2 部　システムとソフトウェアのセキュリティ

テクニカルノート

Wolfgang Winter, Agilent Technologies
Ludwing Huber, Agilent Technologies
近藤　直人，横河アナリティカルシステムズ株式会社

いかにして, ユーザ権限を持った者のみがコンピュータシステム中のデータにアクセスできるようにするのか？あなたの電子署名は本当にあなたしか使用していないのか？あなたは, 他の人があなたのデータを消去したりしていないことをどうやって確認するか？あなたの会社はFDAの電子署名, 電子記録に対応しているか？
21 CFR Part 11対応シリーズ第二回は, これらの質問にお答えする。

はじめに

権限を持たないユーザがシステムにアクセスをしてデータを変更または消去することを防ぐのがアクセス管理である。システムへのアクセスは, 一般に企業内の情報管理規則に従って管理されている。
Part 11シリーズ第1部では, 21 CFR Part 11の概略と分析試験室におけるペーパーレスシステム導入について述べた[1]。第2部では, 分析試験室におけるデータシステムへのアクセス制限, ユーザ毎の権限設定, 監査証跡対応の実際と技術的側面について説明する。分析試験室で使用されるコンピュータシステムへのアクセスに関するセキュリティの設定, 権限やパスワード管理の妥当性について検討する。また, 現在市販されているクロマトグラフィ用コンピュータシステムがどのようにアクセス管理をしているのか, していないのかについても解説する。クロマトグラフィ用データシステムのアクセス管理機能がOSのセキュリティ機能を利用していない場合, データシステムへのアクセスを別途管理しなければならない。分析試験室における機器使用の現状を考察した結果, 我々は, 作業内容毎にアクセス権を設定することが重要であると結論した。これは, 単にデータの機密性を確実にするのみでなく, 人的ミスや事故を防ぐという点からも重要な設定である。

アクセス制限

“Procedures should be in place to limit the access to authorized users.”（権限を有する者のみがシステムを使用できるような手順を作成する）[2]。コンピュータシステムへのアクセスを制限するには大きく分けると2つの方法;物理的方法と論理的方法とがある[3]。
物理的アクセス管理とは, 試験室への立ち入りを制限することでコンピュータシステムへのアクセスを制限する方法をいう。すでに多くの製薬会社では, このような物理的管理は実施されており, 部外者が分析試験室に立ち入ることは制限されている。しかし, 現実的に, この方法のみでシステムへのアクセスを制限することはできない。ソフトウェア自身にセキュリティ機能を持たせる論理的方法でのみ, システムへのアクセスを管理することができる。FDAはすでにこの点に関して医療器具の設計に影響を及ぼすことがあるとして, 規制の中で明確に述べている。

“Failure to establish and maintain procedures to control all documents that are required by 21 CFR 820.40, and failure to use authority checks to ensure that only authorized individuals can use the system and alter records, as required by 21 CFR 11.10(g). For example, engineering drawings for manufacuring equipment and devices are stored in AutoCAD form on a desktop computer. The storage device was not protected from unauthorized access and modification of the drawings.”（21 CFR 840.40で要求されている文書管理規定への逸脱および21 CFR Part11.10(g)項で要求されている権限を持った個人のみにシステムの使用ならびに記録の変更を許可する権限承認機能の逸脱。例えば, 製造装置や器具設計図がデスクトップPCにCADファイルとして保管されている場合, そのファイルは, 権限のない人からのアクセスに対して保護

Agilent Technologies
Innovating the HP Way

TI 16C0A3-005
2000. 11 発行

されておらず, 変更も可能であるとみなされる。) [4]

誰がアクセスするのか？

コンピュータシステムへのアクセス管理は, 情報管理部門の最も重要な仕事の一つである。最近のOSは, セキュリティに関する機能が組み込まれ, 情報管理部門の仕事が楽になっていると思われるかもしれない。しかし, これを正しく運用するには, 専門家の知識, 注意深い管理, 設定が必要となる。例えば, Windows NTの様にセキュリティ機能を有したOSを使用したとしても, 適切なセキュリティとパスワードに関する規定のもとにセキュリティが管理運用されていなければ, そのシステムは全くアクセス制限がなされていないといえる。

コンピュータシステムにアクセスするには, ユーザアカウントが必要となる。権限を持ったユーザは, ユーザ名またはユーザIDとパスワードを使ってシステムへログインする。一般にログインの権限を与える場合, ある規則に則り, そのネットワーク環境下で全てのユーザがユニークとなるようなユーザIDをシステム管理者がユーザに与える。ユーザIDは名前の数文字と姓を組み合わせることが多い。仮に著者の一人の社内UnixシステムへログインするためのユーザIDがwwinterとする。このユーザIDと私しか知らないパスワードと組み合わせると, その組み合わせは, 私特有のものとなる。その結果, このユーザIDとパスワードを使って署名をした場合には, それは, その個人にしか書くことのできない手書き署名と同等と見なすことができる。

この様なユーザIDとパスワードによるアクセス管理は, OSに組み込まれており, すでにほとんどの社内ネットワーク環境下で実施されている。会社自身はすでに組織毎, 複数の事業所間, 海外事業所等からのこの様な複雑なアクセス管理を行っている。これと同様のアクセス管理を分析試験室で使用するコンピュータ化されたデータシステム上に構築することで, システムへのアクセスを管理することができるようになる。これを確実に実施するためには, 情報管理専門家の助けが必要となる。

誰が何にアクセスするのか？

この質問の答えはアクセス管理より, もう少し複雑である。「安全な」OSには“ 権限 ”とよばれる機能が備わっており, ユーザ毎にファイルへのアクセスを許可したり拒否したりする権限（ファイルアクセス権, アクセス権）を設定できる。
自分自身の作成した記録は変更できるが, 他の人の作成した記録は読み取り可能で変更できないようにするにはどうしたらいいのか？ファイルやディレクトリのアクセス権を注意深く設定すれば, この問題は解決できる。事実, 現在使用されているクロマトグラフ用データ処理システムのアクセス制限は, このレベルで行われている。システム管理者（通常, アドミニストレータ権限を持つ者をさす）が, PCに内蔵されたハードディスクやサーバのディレクトリやファイルにアクセスする権限を設定, 管理する。OSの機能である「ユーザプロファイル」を適切に設定することでユーザ毎のアクセス権を設定することができる。

ユーザプロファイルの役割

マイクロソフトWindows NT等のOSはユーザプロファイル機能を持つ。この機能は, 業務内容, 責任範囲, トレーニングレベル等の異なる多くのユーザのネットワークへのアクセス管理に使用されている。ユーザプロファイルを正しく設定することにより, ユーザのアクセス範囲を業務で必要とするファイル, プログラムやサーバへ限定できる。また, ファイルの機密性, 完全性を損なうことなく, 業務に使用する「個人的な」ファイルを共有することもできる。システム管理者がユーザプロファイルを作成, 実行させる権限を持っている。管理者は, スクリプトを書くことで迅速にこのユーザプロファイルを作成する。それでは, この機能を使って, クロマトグラフィデータへのアクセスを管理することは可能か？答えは, 残念ながらノーと言わざるを得ない。
いかに上手くユーザプロファイルを設定したとしても, それはデータシステムの外側に作られた仕組みに過ぎない。データシステムに保管された電子記録（生データ, 定量結果, メタデータ）は相互に関連しており, これらを外部から管理することは本質的に不可能または極めて困難である。従って, データシステム自身がアクセスを管理する機能を持たなければならない。データシステム自身がユーザプロファイル機能を持つことにより, クロマトグラフィデータの完全性, 機密性を保証することが可能となる。仮に, データシステム自身がこの様な機能を持たない場合, 生データの完全性等は, システム管理者のデータシステムに関する経験と知識にのみに依存する。
データ管理機能を持たないデータシステムを使って21 CFR Part 11に対応させようとする場合, データシステムがどの様にデータを保管, 管理, 組織化, バージョン化しているかに関する詳細な情報をメーカはユーザに提供しなければならない。この場合, 対策は標準的なファイル管理システムにのみ依存するので, データ管理は手作業または半自動の作業となり, 間違いの原因となるであろう。

パスワード管理

システムへのアクセス管理にもっともよく使用されているのが，ユーザIDとパスワードである。もしユーザIDとパスワードが複数の人々の間で共有されていたら，誰がシステムにアクセスしていたかわからなくなる。Part 11違反に関して以下のような警告書がFDAから発行された。ユーザIDとパスワードが複数の職員で共有された場合，データの信憑性，機密性は失われる。

“An employee user name and computer password were publicly posted for other employees to use the access the Data Management System. During the injection another employee who did not have the established user name or password was observed obtaining access to the Data Management System utilizing the posted user name and password. Three previous employees, who had terminated employment in 1997 and 1998, still had access to critical and limited Data Management System functions on March 18, 1999” (ある職員のユーザIDとパスワードが公開され，それを使って他の複数の職員がデータ管理システムにアクセスしていた。その職員が分析中に，他の職員が公開されたユーザIDとパスワードを使用してデータシステムにアクセスしていることが発見された。また，1997年から1998年の間に退職した3人の従業員が，1999年3月18日にデータ管理システムの重要かつアクセスが限定されている機能にアクセスした記録が残っている。) [5]。

どうやってパスワードの安全性を確保するか？

21 CFR Part 11の11.200(電子署名構成要素とその管理)と11.300(ユーザIDとパスワード管理)には，電子署名に使用するユーザIDとパスワードに関する要求事項が明記されている；電子署名は，*“used only by their genuine owners” (本来の署名者のみが使用すること)*ならびに*“administered and executed to ensure that attempted user of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals” (本来の署名者に代わり誰かが電子署名を使用する場合は，二人あるいはそれ以上の人間の協力が必要となるような仕組みをつくり，そのように実施しなければならない)*。

FDAの要求に対する技術的な対応策は，パスワードの機密性，完全性，信頼性，秘密性に関する原則を「確実に」実行する事である。問題は，覚えるのが難しいパスワードを忘れないようにすることである。覚えやすいパスワードは他人にとっても簡単に想像ができ，パスワード解読プログラム(password cracker)で解読することもできる[6]。かつての「安全な」OSでは，システム管理者がパスワードを発行していた。時には，パスワード作成規則に従って発行されたパスワードが複雑で安全ではあるものの，複雑すぎてユーザは何かに書き留めておかなければならないこともあった。現実的には，不正なアクセスを防ぐためにパスワードを保護しなければならないが，とは言っても，パスワード自身は，ユーザにとって覚えやすいものでなければならない。詳細は，パスワード規則を参照(文末の囲み記事)。

パスワード管理機能はOS自身も持っている。マイクロソフトのWindows NTなどのOSの「アカウントポリシー」がそれにあたる(図1)。そのシステムを使用する全ユーザのパスワードの決め方，使い方をアカウントポリシーが規定している。特に，その中には，不正なアクセスがあったアカウントに対しロックをかけて使用できなくする機能もある。

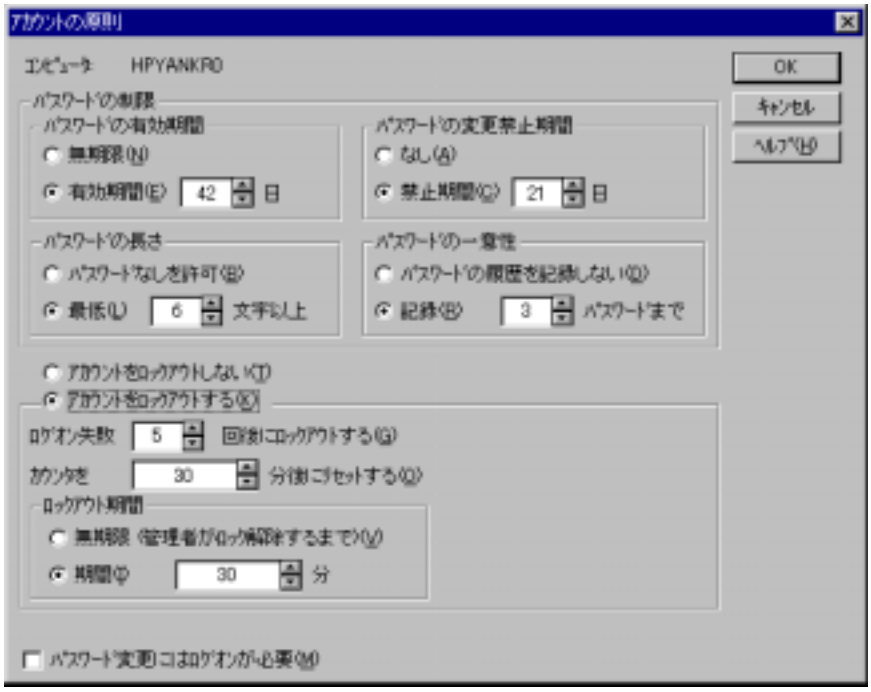

図1　Windows NTでのアカウントの設定

アカウントポリシー機能の重要な点は,必要とされる設定を一つの方法で管理できることにある。例えば,一カ所でアカウントポリシーを設定すれば,全クライアントPCの設定をこれと同じにすることができる。

これらの設定ならびに管理は,一般的には,社内情報管理部門により行われる。データシステムのセキュリティ機能がOSのこれらの機能と結びついていない場合,データシステム自身にも同様の設定,管理が必要となる。この様な場合,1ユーザに対して二つのアカウント管理と二つのパスワード;OSとデータシステム,が必要とされる。多くの試験室向けのデータシステムはOSと比べると限定されたアカウントポリシーしか有していないかまたは全く持っていない。後者の場合,21 CFR Part 11へ適合させることは極めて困難である。従って,Part 11に適合することを考えている試験室は,いろいろなメーカが提供しているデータシステムのアカウントポリシーを詳しく比較する必要がある。OSのセキュリティシステムに直接結びついた方法が最も現実的で将来性のある方法といえる。本シリーズの次の論文でこの点に関してより詳細に説明する。将来,新しい個人認識のシステム,例えば新しい暗号化や生体測定技術が登場してきたときに,この様にオープンで包括的な方法がいかに有効かを説明する。

別人になりすましてシステムにアクセスすることをいかにして防ぐか?

システムへのログインを厳しく管理しても,誰かが他のユーザになりすまして電子記録や電子署名に変更を加えたりすることを防ぐことはできない。例えば,ユーザがログオン中にシステムにアクセスしたまま席を離れた場合,実際にこの様なことが起きる可能性がある。Part 11に対するコメント63は,Part 11の重要な要求事項について述べている。「*その電子署名は,私がしたのではない*」とか「*私が署名した後で誰かが記録を変更した*」と容易に言えないようにしなければならない。コメント124では,このようなことへの対策が詳細に述べられている:

"The agency believes that, in such situations, it is vital to have stringent controls in place to prevent the impersonation. Such control include: (1) Requiring an individual to remain in close proximity to the workstation throughout the signing session; (2) use of automatic inactivity disconnect measures that would "de-log" the first individual if no entries or actions were taken within a fixed short timeframe; and (3) requiring that the single component needed for subsequent signings be known to, and usable only by, the authorized individual."[7]「*そのような状況下においても偽造を防ぐことのできる厳重な管理が必要であると当局は信じている。厳重な管理には以下の内容が含まれる;(1)一連の署名を行う間,署名者はワークステーションから離れない。(2)自動ログアウト機能を有するシステムを使用する。ある定められた短時間内に入力が無かった場合に自動的にそのユーザをログアウトする。(3)ログイン後,続けて行う署名に使用する入力(例えばパスワード,著者追加)は,ログインを許可されているユーザのみが知っていて,そのユーザのみが使用できるものであること。*」

21 CFR Part 11に対応したデータシステムを選定するにあたって,ユーザアカウントの不正使用を防ぐ対策がそのシステムに組み込まれているかをユーザは考慮しなければならない。いくつかの分析機器メーカが,このセキュリティの問題点に関してテクニカルノートを発表している[8,9]。

ユーザアクセス権

次に,電子署名に適合したデータシステムに必須となるユーザ毎のアクセス権限について考えてみたい。ここで「電子署名に適合した」とは,規則11.10に述べられている条件を全て満たしていることを意味する。

個人の責任,知識,権限に関係なく,システムにアクセスする人間全員に同一のアクセス権を与えることは,アクセス管理をしていることにならない。誰かが,データの完全性やセキュリティに影響を与えるようなシステム設定を間違って変更してしまうかもしれない。この様な場合,システムの完全性が損なわれてしまう。特にシステム管理機能を変更された場合には,極めて大きな問題となる。システム管理機能の変更は,文書化された規則に従い,任命された数名のみによってなされなければならない。この点に関して,コメント83に対する回答の中でFDAは次のように述べている;

"System access control is a basic security function because system integrity may be impeached even if the electronic records themselves are not directly accessed. For example, someone could access a system and change password requirements or otherwise override important security measures, enabling individuals to alter electronic records or read information that they were not authorized to see."[7](*システムアクセス管理は基本的なセキュリティ機能である。なぜならシステムにアクセスはするが電子記録にアクセスしない場合でもシステムの完全性が疑われるからである。たとえば,だれかがシステムにアクセスしてパスワードの設定や重要なセキュリティ機能を無効にすれば,権限のなかった個人が電子記録を変更したり,情報を見ることができるようになるからである。*)

規制で用いられている用語「権限確認(authority check)」について考えてみたい。システム管理者は各ユーザ毎にアクセス権を個別に設定しなければならないのか？コメント83によると“*do not have to embed a list of authorized signers in every record to perform authority checks. For example, a record may be linked to an authority code that identifies the title or organizational unit of people who may sign the record. Thus, employees who have that corresponding code, or belong to that unit, would be able to sign the record.*”[7]*(署名者の権限を確認する目的で全ての記録に署名権限を持つ者の一覧表を添付する必要はない。例えば, 記録に署名する事のできる人々の肩書きまたは組織を特定のコードに関連づけておく。{このコードを持つ者のみに, 特定の記録に電子署名する事のできる権限を与える, 著者追加}。このようにすることで, 対応するコードを持つか, その組織に所属する人々が記録に署名することができるようになる。)*

そのためには, データシステム自身が, 職務に応じたアクセス制限を管理, 設定できる機能を持たなければならないと, アジレントテクノロジー等の分析システムメーカは結論した。どの機能には, どの職位にあるユーザがアクセスできるようにするのかを会社が定める。この規則に従って職位毎にアクセス権を設定する。ただし, どの記録に電子署名が必要とされるかについては, 従来通り試験室の規則による。分析機器メーカの関知するところではない。

次に実際のラボで発生する複雑な事例について考察する。

PCを共有する

現実に起こりそうな例として, 1台のコンピュータを複数の人が使用する場合を例にしてこの問題を検討してみよう。このような使われ方は, 品質管理や製造現場で実際に起きることが多いと思われる。一台のコンピュータを使って複数の分析機器を制御し, なおかつそれぞれの装置の使用者が異なる場合である。このような使用環境下では, NTのログイン管理ではシステムへのアクセスを管理できない。NTへのログインで管理しようとすると, ユーザが変わる毎にセッションをシャットダウンしなければならない。データシステムにもよるが, シャットダウンをすると, データ取込が出来なくなることが多い。従って, このような手順は非現実的である。このような場合には, データシステム側での管理が必要となる。現実的な対応方法は, NTにはデスクトップ共有(シェアードデスクトップ)でログオンして, クロマトグラフィーデータシステムには各ユーザ毎にそのユーザIDとパスワードを使ってログオンする方法である。NTと違って, クロマトグラフィーデータシステムに共有アカウントを設定することは許されない。なぜなら, そのシステムを使用した個人を特定できなくなるからである。同様の理由で, 共有アカウント用のユーザIDとパスワードを電子署名に使用することは出来ない。

リモートアクセス

ある種の分析を行っている試験室では, 外部からシステムにアクセスすることが必要となる場合がある。この場合でも注意深くシステムを設定すれば, 21 CFR Part 11のクローズドシステムでのシステムアクセスが可能となる。このような場合でもユーザIDとパスワードが必要であることはいうまでもない。また,「スマートカード」と呼ばれるシステムを利用することで, セキュリティ管理をより厳重にすることができる。ユーザはスマートカードと呼ばれるパスワード発生器を持つ。外部からシステムにアクセスする際に, このカードが作成したパスワードを入力してサーバにアクセスする。カードは毎回異なるパスワードを発生するため, パスワードを悪用することはできない。また, コールバックもセキュリティを守るために有効な方法である。

保守や修理のためのログイン

二番目は, システムの保守や修理を行うためにシステムにアクセスする場合の問題である。多くのクロマトグラフィー用データシステムは, サービス用の特別なアカウントを設定している。これを使ってシステムのインストール, 設定, 保守を行う。Windows NT用のデータシステムの場合, ソフトウエアのインストール, NTの設定や必要なドライバ類のインストールのために, メーカのサービスエンジニアはアドミニストレータの権限を必要とする。

メーカは, いちいちユーザ側のアドミニストレータの手を煩わせることなく(ユーザのアドミニストレータと一緒に作業するまたは共有ログインする)データシステムの修理等を行えるようにしてサポート性をよくしたいと考えている。(21 CFR Part 11の条文によると, アドミニストレータ権限で共有ログインすることは, 好ましくないと考えられる。その共有アドミニストレータ権限でシステムに何かをした場合, その個人を特定できなるなるからである。)また, サービス用のアカウントを設けることは, データシステムのセキュリティに違反すると考える人々もいる。

どうしたらこの様な現実的な問題を解決できるのか？著者らは, 以下の方法を提案する。

データシステムにアクセスするメーカサービスエンジニアが守らなければならない手順を作成, 実施する。

サービス用アカウントを設けることがシステムセキュリティ上問題かどうかを考察する。アドミニストレータ権限をもったサービス用アカウントが必要となった場合は, システム毎にアカウント作成する。修理完了後, 直ちに

サービス用アカウントを無効にする(図2)。サービスエンジニアがシステムアクセスする必要が生じた際にのみ,システム管理者がサービス用アカウントを使用可能とする。

サービス用アカウントのユーザ権限を適切に設定して,サーバ上の機密データにアクセスできないようにする。

データシステム自体がユーザのアクセス権を設定できる機能を持っている場合,データの完全性,セキュリティに影響を与える様な権限をサービス用アカウントから削除する。例えば,データの削除,再解析,結果の承認または拒否,分析法の変更等の権限。

サービスまたは保守作業のために,データの完全性に影響すると考えられる作業が必要となった場合,これらの作業は,ユーザのシステム管理者の管理下で実施されなければならない。また,これらの作業を実施するにあたっては,その内容を事前にシステム管理者と打ち合わせ,承認を得た後に実施する。事前に承認を受けた場合には,作業時にシステム管理者の承認は必要ない。

言うまでもなく,21 CFR Part 11に適応したデータシステムはアクセス権毎にユーザ権限を設定しなければならない。従ってサービス用アカウントの権限を,データの完全性やセキュリティに関わる操作ができないように設定する。このような重要な作業を行った場合にその作業を完了するために,電子署名が必要とされる。仮にサービスエンジニアが間違ってそのような「重要な作業」をしてしまったとしても,電子署名の段階でこの作業を無効にすることができる。

21 CFR Part 11に適応するため

21 CFR Part 11に適応するために必要となるシステムアクセスのセキュリティに関して考慮しなければならないこと,評価しなければならないことを以下にまとめた。

1. アクセスを管理するためにアクセス管理機能をもったデータシステムを使用する。データシステムのユーザアカウントはOS自身のユーザアカウントと結びついていることが望ましい。
2. 個々のユーザパスワードの秘密性と信憑性を保証するために,パスワードに関する規則を作成し,実施する。データシステムに関するパスワード規則を設定するか,OSのパスワード規則に準ずるかどちらかにする。
3. バリデーション作業を軽減するために,生体測定システムが一般的になるまでそのようなシステムを導入しない。OSがそのような機能を取り込むか,もっと一般的に普及するまで導入を控える。
4. 他人になりすましてアクセスすることを防ぐ手段を講じる。データシステムが,一定時間後に自動的に使用中のウインドウをロックする機能(オートロック)を有していることが望ましい。
5. 業務内容や職位に応じたアクセス権を設定する。多数のユーザのアクセス権を管理するには,個人毎にアクセス権を設定するのではなく職位毎にレベルを設定することを推奨する。データシステムもアクセス権を設定できる機能を持つことが望ましい。
6. 一台のPCを共有しなければならい環境で分析を行う場合,データシステム自身がユーザIDとパスワードによるユーザ認証機能を持たなければならない。データシステムに共有ログインする事は,署名された電子記録を否認できないという原則に違反する。共有ログインをしていた場合に,署名を否認することができる。
7. メーカのサービスエンジニアのユーザアカウントに関するセキュリティ規則を作成する。この目的のためだけに使用する専門のユーザアカウントを一つ作成する。可能であれば,システムに保管してあるデータの機密性やセキュリティに影響のある作業ができないように設定する。サービス用ユーザアカウントは,作業終了後直ちに使用不能

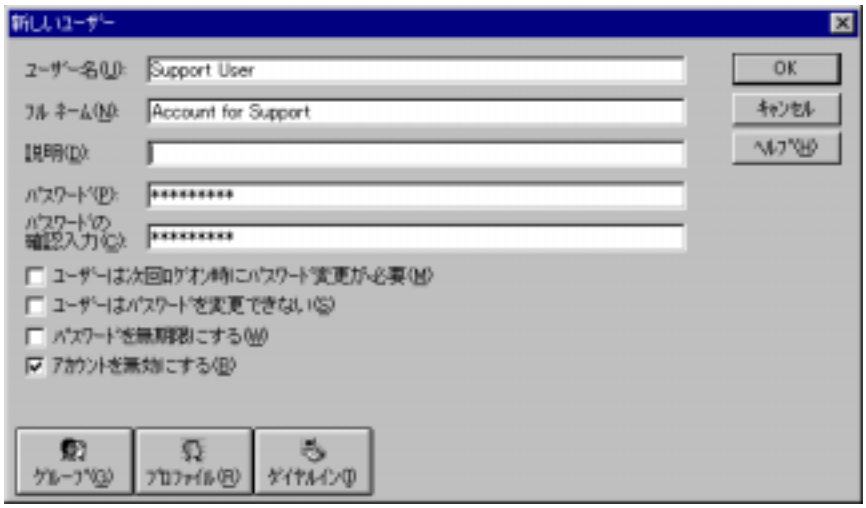

図2　Microsoft Windows NTのユーザマネージャをつかって ユーザアカウントを一時的に使用不可能にする。

Printed in Japan : 1.0.JUL.12.2000 (YG)

とする。サービス用アカウントにどのような管理が必要か考察する。

最近, 21 CFR Part 11に対する警告書や483が多数発行された。それらの多くは, 医薬品の電子製造記録の保管実務についてであるが, FDAは, 製薬会社がPart 11対応に向けて前進することもしくはPart 11対応計画を作成することを期待している[5]。古いシステムは, *"time is running out and you have to play a game of catch up"* [5](もう, 時間は無い。急いで何かしないと間に合わないぞ)である。まさにその通りである。

次の論文では, Part 11の最も重要な点, クロマトグラフィーデータシステムの核心;データの完全性について議論する。

引用文献

(1) 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)

パスワードポリシー

パスワードポリシーを作成し，ユーザを教育して，これを確実に実行することでパスワードの安全性，機密性を確保する。現実的で，有用なパスワードポリシー作成に関する指針を以下にまとめた。

1. システム管理者を含めいかなる他人も，パスワードを知ることができない。初めに情報管理部門から発行されたパスワードは，最初にログインした時に変更することをパスワードポリシーに定める。
2. パスワードは6文字以上とする。文字数が多ければ多いほどいいとは限らない。文字数を多くすると覚えておくことが難しくなり，また，入力時の間違いも多くなる。
3. パスワードは，複数の文字種から構成されなければならない。アルファベットのみでなく数字，記号を含まなければならない。
4. パスワードに，氏名，電話番号，自動車のナンバーなどの個人情報を使ってはならない。これらは容易に推定することができる。
5. パスワードに辞書にある単語を含んではならない。
6. 大文字と小文字を混在させるとパスワードが盗まれる危険性を少なくすることができる。
7. 3回続けて不正なログインがあった場合には，そのアカウントをロックして使用不能とする。
8. パスワードを定期的に変更する；6 - 8 週で変更することが好ましい。変更期間があまり短すぎてもユーザが面倒だと思うようになり，パスワードを覚えておくためにどこかに書いておくようになる。パスワードの履歴管理を行う。同じパスワードを続けてもしくは数回後でないと使えないようにする。
9. パスワードの使い回しができないようにする。不正ログイン防止の回数(7を参照)以上のパスワードを記憶しておいて使えないようにする。好ましくは5 回分のパスワードを記憶する。
10. パスワードポリシーは，ユーザがその有用性を認めたときに初めて機能する。電子署名が法的に手書き署名と同じであること，(電子，手書きに関わらず)署名の意味，署名の結果生じる次の行動，その行動の結果が及ぼす影響，これらについてユーザが正しく理解したときに初めてパスワードポリシーの重要性が認知される。

(2) *Code of Federal Regulations, Food and Drugs,* Title 21, Part 11, "Electronic Records; Electronic Signatures" (U.S. Government Printing Office, Washington, DC). Also Federal Register 62 (54), 13429-13466.
(3) L. Huber, *Validation of Computerized Analytical Instruments* (Interpharm Press, Inc., Buffalo Grove, IL, 1995).
(4) *Compliance Policy Guide: 21 CFR Part 11; Electronic Records, Electronic Signatures* (CPG 7153.17)(FDA, Washington, DC) www.fda.gov/ora/compliance_ref/cpg/cpggenl/cpg160-850.htm.
(5) *Gold Sheet* 33(7) (F-D-C Reports Inc., Chevy Chase, MD, 1999).
(6) M.J. Edwards, "The Handy Security Toolkit Revisited," *Windows NT Magazine* (October 1999) www.winntmag.com.
(7) "Rules and Regulations" comment 124, *Federal Register* 62(54) (20 March 1997), pp.13429, from the *Federal Register* Online, GPO Access, DOCID: fr20mr97-25.
(8) *Implementing Electronic Records and Signatures with Hewlett-Packard's ChemStation,* (Hewlett-Packard, Little Falls, DE, 1998) publication number 12-5966-2315E.
(9) *Using ChemStation Plus to Comply with FDA 21 CFR Part 11,* (Agilent Technologies, Little Falls, DE, 1999) publication number 5968-7930E.

21 CFR Part 11
試験室における電子署名と電子記録
第 3 部　電子記録の完全性保証

テクニカルノート

Wolfgang Winter, Ludwig Huber, Agilent Technologies
近藤直人，横河アナリティカルシステムズ株式会社

21 CFR Part 11に対応した分析試験室においては, データの完全性をいかにして守っていくかが大きな問題となってくる。別の言い方をすると電子記録の真正性と信頼性を保証すると言える。

本シリーズ第一部では, 分析試験室における電子署名, 電子記録の概要とPart 11に対応していくための提案を行った(1)。第二部では, 安全性について考察した。権限を持たない者がデータシステムを使用したり, データを変更したり, 消去したりすることをいかにして防ぐかを論じた(2)。シリーズ第3部では, 21 CFR Part 11で要求されるデータの完全性に対応するためにデータシステムに必要とされる機能について考察する。

21 CFR Part 11導入に伴って, GMPにおける要件の一つ, データの完全性を保証することの重要性が再確認された。データの完全性, すなわち, 偶発的または故意になされた変更, 改ざんや削除から生データを保護することは, データの真正性と信頼性を保証するうえで最も重要なことである。この点に関して最近, 英国のコンサルタントRobert McDwall氏は「コンピュータの(不)安全性」と題する優れた論文を発表した。その中で「安全なコンピュータはこの世に存在しない。我々が議論していることすべては, 危険性の許容される程度についてである。」"There are no secure computers. All we are talking about are the degrees of acceptable insecurity" (3). 本シリーズの第2部で, 21 CFR Part 11対応主計画書やデータの安全性について考察することが, システムの安全性とユーザ権限に関して考察することと同じであることについて述べた。しかし, データの完全性については議論しなかった(2)。今日の分析試験室のデータシステムにおける最も大きな問題は, システムへのアクセス管理とアクセスの安全保証ではなくデータの完全性を保証することである。信頼できる記録とは, データが必要とされる条件を満たして記録されていることを意味している。クロマトグラフィー用データシステム(chromatography data systems, CDS)の場合, データの完全性を保証するために生データ以外に二つの記録が必要とされる。一つは分析条件のようなメタデータ, もう一つは, 再解析等を行った場合に生じるデータの変更履歴である。

監査証跡。 電子子守り

データの安全性は別として, 以前からある規制が記録の真正性に関して要求していたのはトレーサビリティーである。昔から使われてきた実験ノートのように, データシステムの監査証跡は, 誰がいつ何をしたのかを自動的に記録する。Ron Tezlaffがいみじくも言っているように「記録されていなければ, それは噂に過ぎない」"If it's not written, it's a rumor"(4)。Paul Motiseは監査証跡を「電子子守り」"electronic nanny"と呼んでいる (5)。McDowallによれば,「監査証跡はデータに加えられる変更を監視するソフトウエアユーティリティーの一つである」"audit trail is a software utility that monitors changes to selected data sets within the main application"(6)。監査証跡は,「電子記録の作成, 変更, 削除を行う」"actions that create, modify, or delete [an] electronic record"際には必ず必要とされ, また,「保護されていて, コンピュータにより時間記録とともに自動作成」"secure, computer-generated, [and] time-stamped"されなければならないと, Part 11 Section 11.10 (e)に明記されている(7)。監査証跡に残された記録は上書きされてはならない。これらは新しい要求ではない。GMP環境下で紙の記録保管に求められていることと基本的には同じである。

FDAの査察官は, 査察中に, 製造記録や分析記録を調査する。監査証跡は,

Agilent Technologies

TI 16C0A3-006
2001. 4 発行

例えば, クロマトグラムの積分条件の変更に関する情報を記録, 管理することにより, これらの査察に必要な情報を提供する。直接製造記録等に関係しない変更にも監査証跡は必要とされる。例えば, ユーザ権限やコンピュータシステムの設定を変更した場合は, 時間(と理由)を伴った監査証跡が必要とされる。
どのように監査証跡を記録すればいいのだろうか。アジレント社のケミステーションプラスでは次のような方法で監査証跡を記録している。記録のどの部分に監査証跡が必要かを決める。この部分に変更が加えられた場合に, その変更をデータベースに登録する。もちろんデータベース自身が安全でなければならいが。このようにして, 例えば, 不正アクセス記録やユーザ権限の変更が記録される。通常の方法では, この記録(監査証跡)を変更または削除することはできない。

問題は, どの程度の変更を監査証跡として記録するかにある(監査証跡記録の詳細さの程度とも言える)。本シリーズの第一部で述べたように, あまりにも詳細に監査証跡を残すと数が多すぎてあっという間に管理できなくなる。これでは, Part 11の要件を満たすことはできない(1)。クロマトグラフィー用データシステムの監査証跡とその検索機能は注意深く設計されなければならない。ドイツのようないくつかの国では, 従業員の成果を測定することを目的にする情報システムを使用する場合には, 労働組合の承認が必要となる。試験室で使用されるデータシステムの目的は, 従業員の労務管理にあるのではなく, 電子記録の完全性を保証することにあることを十分に理解する必要がある。監査証跡に対する適切な見出語を設定することで次のような質問に答えることができるようになる:分析結果に影響を与えるような装置または手順のトラブルが分析中に発生しなかったか？一連の分析中で, 特定の試料にのみ積分条件を変更していないか？誰かがその分析結果を検討したか？どうしてその分析結果は不採用になりそれ以降の計算に使用されなかったのか？監査証跡の重要な機能にコメント入力がある。データを作成した人もしくはその結果を確認する人が変更を加えた際にコメントを入力して, なぜこのような変更を加えたかがわかるようにすることを目的としている。Part 11自体は変更理由の記録を求めていないが, いくつかの以前からある規制, たとえばGLPはその理由を明記することを必要としている。いくつかのデータシステムはコメント入力機能を有している。いくつかの選択肢から選ぶことも選択肢をユーザが定義することもできるようになっている。これらの機能により, データシステムは変更とその理由を記録することができる。たとえば, 「積分条件のある変数をXからYに変更した, これはSOPの改訂による」のように。FDAはこのようなコメントを認めているが, ただし, それが監査証跡記録の完全性を損なわない場合にのみに限られる。コメントの追加のために監査証跡記録を操作することは許されない(8)。規制に対応するためには, 監査証跡は容易に変更, 削除できてはならない。例えば, Windwos NTのイベントビュワーのような物では監査証跡とは到底認められない(図1)。OSの持つ記録作成機能によりデータシステムも監査証跡を作成している。しかし, 規制に対応するために特別な注意が必要とされる。監査証跡には, 書類の偽造を防ぐ

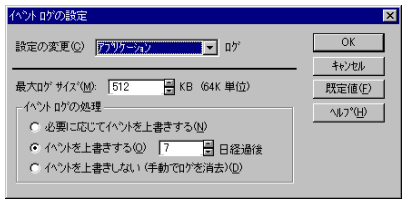

図1.Windows NTのイベントログ設定. Windows NTのイベントビュワーに残された記録は，変更や削除が可能なので，Part 11で必要とされる監査証跡に採用することはできない.

役目もある:「データは仕事を始める前もしくはその日の最後に記入された。」"The entry of data before an action occurs or at the end of the day, as an afterthought" (5)。

トレーサビリティーと時間記録

巨大なクライアントサーバーシステムを持つ多国籍製薬企業が, Part11と時間記録に関して懸念を表明した。特に電子的なバッチ記録システムについて, まず, FDAとの間で時間記録と時間帯に関する議論から始まった。異なる時間帯をまたがって作業が行われたとしても,「署名者の現地時間を記録する」"The signer's local time is the one to be recorded" と規則には明記されている(9)。これに対して会社側は,「ネットワークシステムがいくつかの時間帯にまたがっているとき, 電子署名に必要な時間記録は署名者の現地時間か, ネットワークシステム(サーバー)の現地時間のどちらなのか？」"Does an electronic signature time stamp need to be local to the signer or to a central network when an electronic batch record system spans different time zones?" この質問に対する回答の中でFDAは監査証跡における時間記録に関して次の二つの点を強調した:監査証跡における時間記録は, 作業の順番が明確にかつ分り易く記録されていなければならない "clearly document the sequence of events in human terms", そして電子署名が信頼できることを保証し, 署名者が拒絶することができないような仕組みを備えていなければならない"authenticate an electronic signature and minimize chances of signer repudiation"(10)。
監査証跡の有効性について考えてみたい。例えば, 署名者と関連づけられた現地時間で記録された監査証跡は, 署名の信頼性を高めることができる;署名したとされた人がその時間, 会議に出席中だったり, その時間はとても署名をすることができないかったとする。

するとその署名が, 偽の署名者によって行われたことが, 監査証跡からわかる。会社側は適切な調査を開始しなければならない(10)。

時間記録に関する厄介な問題を解決するには, 最先端技術と現実的な対応との両者が必要になる。なぜならクライアント/サーバータイプのデータシステムは分散型で広範囲に広がっているからである。多国籍企業で使用されているクライアント/サーバータイプのデータシステムを使うと, 異なる大陸にある分析試験室間でデータを交換できる。ユーザは, 出張時等に他の試験室からシステムにアクセスして, 監査証跡に記録が残る作業をすることができる。もし, 監査証跡に記録される時間記録が, 現地時間のみだったとすると, 監査証跡に残っている記録と実際の作業の間に矛盾が生じる(例えば実際に分析した時刻と承認の時刻)。つまり, 午前9時に承認した分析が午前11時に実施されていたということも起こりうる。分析はヨーロッパ中部時間でおこなわれ, 承認は米国東部時間で行われたことを示す何らかの証拠がないと監査証跡自体を信用することができなくなる。この点に関して, Motiseは次のように述べている。「しかしながら, Part 11は, 時間記録にサーバー設置場所の時間を同時に記録することを禁止してはいない。それは承認者の時間帯とは異なることもある。二つの時刻を記録する場合, どちらが承認者の時間帯であるかを明確にしなければならない。("Part 11 does not, however, prohibit a firm from supplementing the local time stamp with the time stamp of a remote central server that may be in a different time zone from the signer。 Where dual stamps are recorded, though, it is important that the electronic record clearly indicate which one is local to the signer")」(8)。最新のそして正確な時間記録方法として, 承認者の現地時間ではなく, 標準となる時間帯(たとえばグリニッジ標準時)で時間記録を作成する方法が採用されている。この方法をとることで, 作業者の現地時間とは関係なく, 実際の作業の流れを正しく反映した記録を作成することができようになった。

"Typewriter Excuse"タイプライターエクスキュース

GLPやGMPの旧来の解釈では, 会社が生データを定義することができた。そして, 紙に印刷され, 署名された記録が, 生データとして保管されてきた。Barbara ImmelはBioPharmに次のように書いている;「規制の目的はタイプライターエクスキュースを取り除くことにある。タイプライターエクスキュース;『真の記録は紙の記録である。我々はコンピュータを単に記録を作成するために使っているに過ぎない(図2)。』という誰かのコメントを取り消すことである。」(the rule's intent was to get rid of "typewrite excuse", the statement made by some that "The real record is the hard copy。 We just use computers to generate the record")。LCGCにMcDowallは以下のように述べている;「電子記録に移行するには, その記録を再現するために必要なデータの定義, 生データ(最初に

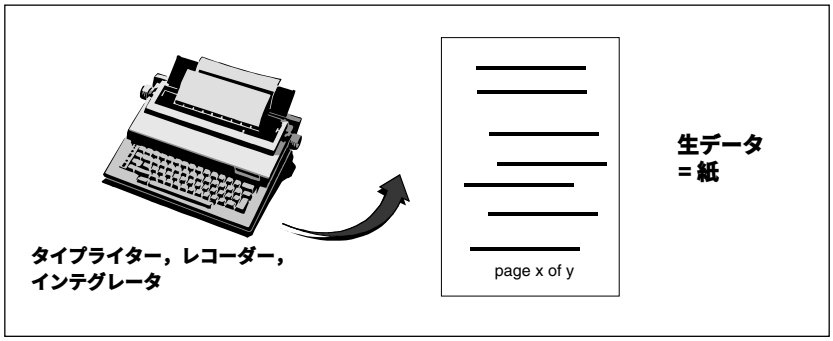

図2. いくつかの装置では生データが紙の記録となる.

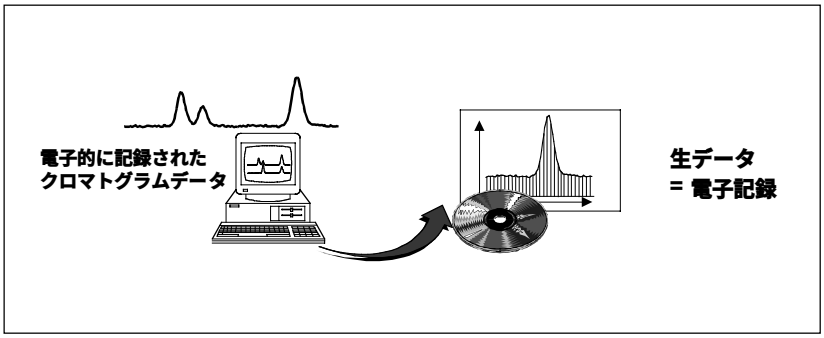

図3. クロマトグラフィー用データシステムでは，生データは電子記録であり，21 CFR Part 11への対応が必要とされる.

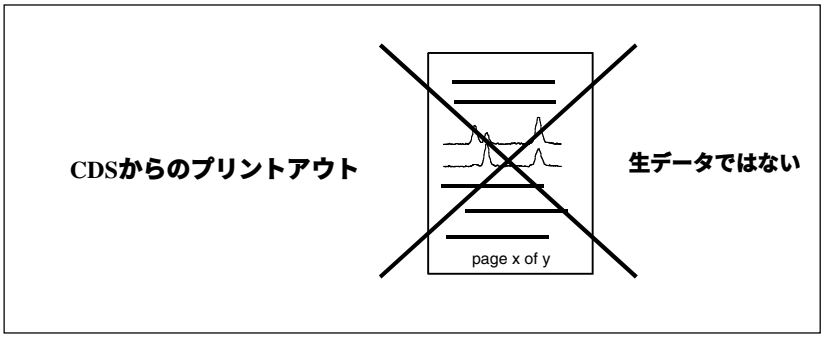

図4.電子記録を印刷したものはもはや生データとは見なされない.「タイプライターエクスキュース」は受け入れられない.

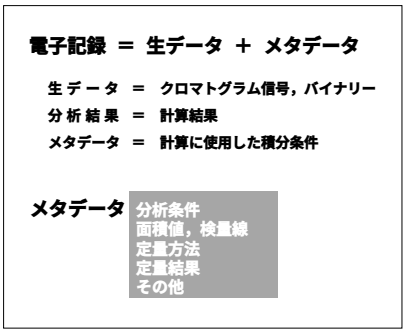

図5.電子記録の信頼性を保証するためには，生データとそれに関連するメタデータが必要とされる.

観察された結果が生データファイルとなる)やそれに付随するファイル, たとえば積分条件やシーケンスファイルが必要になる。」("A move to electronic records will require a definition of raw data (original observations taken to be the raw data files) together with other files such as the associated, integration file and injection sequence to enable the work to be reassembled") (12)。本シリーズの第一部で述べたように, FDAは将来的に紙の記録を受け付けなくなるかもしれない(3)。Part 11によれば, 記録を電子的に残しているのであれば, それらを電子的に長期間保管し続けなければならない。特に, 記録が生データの場合, それがたとえばコンピュータのハードディスクなどの「記録媒体に書き込まれたれたら直ちに("as soon as it hits a durable storage device")」保守, 保管しなければならない(図3)。従って, CDSから印刷され署名された紙の記録は, もはや生データとは見なされない!!　なぜか？電子記録の印刷物は一般的に電子記録の完全で正確なコピーと見なすことができない(印刷物には積分条件や監査証跡のような重要な情報が欠けている)からである(図4)。積分条件や監査証跡のようなデータをメタデータと呼ぶ(図5)。もはや「タイプライターエクスキュース」を言訳にできない。Immelが言っているように「たとえば電子記録が作成されない場合のように, コンピュータが本当にタイプライターのように使用されている時のみ, Part 11は適用されない。」("Only if a computer is truly being used as a typewriter - when no electronic record is created - does the rule not apply"), またMotiseも次のように書いている。「プリントアウトを本質的に信頼することはできない, なぜならプリントアウトにはデータの再構築または生データから再現するために必要なメタデータ情報を含んでいないからである。」("There is nothing inherently trustworthy that comes out of your printer," because the paper printout does not contain the metadata that is necessary to reliably reconstruct or even replay the original data) (11,13)。

メタデータは, それ故, 記録の信頼性を証明し, FDAの新しい規制(Part 11)に対応するために極めて重要になってきている。なぜなら, メタデータなしでは, 生データから測定結果を再構築することもできないし, 最終結果のトレーサビリティーも限定される。生データ, メタデータ, 監査証跡そして測定結果が完全にそろって初めて, 信憑性のある電子記録といえる。このデータセットは, 製造工程, 品質管理が管理された状態にあること示すために必要とされる(図5)。しばしば分析試験室では, メタデータ保管の重要性が忘れられている。また, 不十分な記録保管の方法を用いた場合, 生データとメタデータから試験結果を完全に再構築することができず, 査察時に問題となるであろう。

関連づけの完全性

データの完全性を保証するためには, 電子記録間の関連づけがとぎれることがあってはならない。これは, 関連づけの完全性と呼ばれる。クロマトグラフィーデータにおける電子記録の完全性とは次のことを意味する。あるクロマトグラフィーの分析結果が作成された後, それが変更されておらず, 改ざんも加えられず, または不正な処理をされていないことを証明するために, この記録に関連する他の記録, 生クロマトグラム, 積分条件, 検量線そして監査証跡との関連づけがきちんと保存されていなければならない。ある記録に関連する一連の記録が保管されていて初めて, その記録自身のトレーサビリティー, 信頼性, 信憑性が確保される。それぞれが独立して変更可能な記録間の関連性を管理することは決して易しい作業ではない。次の場合を例に考えてみたい；試料XYZを分析法Aのバージョン4で分析した。最初の分析は移動相が足りなくてうまくいかなかったが, 試料XYZのクロマトグラム1が作成された。サンプルを再分析した。最初のクロマトグラムを削除や上書きすることなく二番目のクロマトグラムを記録した(あなたが現在使用しているデータシステムで本当にこうなるのか確かめることをおすすめします)。クロマトグラム2を使って主成分と不純物を定量して, 分析結果XYZ.2-A4-1を得た。データを照査していた分析担当者が標準試料の作成ミスに気付き, 検量線の一点を不採用とした。新しい検量線を使って, クロマトグラム2を再計算して定量結果XYZ.2-A4-2を得た。再計算の結果は再照査の後, 承認され保管された。数ヶ月後, 不純物の仕様が変更になったため分析法Aは変更された。分析法Aの新しいバージョンは5となった。その年のFDA査察中に, サンプルXYZの分析結果が調査されることになった。関連づけの完全性がうまく機能しているシステムでは, 査察で必要な生データ(XYZ.2)と分析法(Aバージョン4)のバージョンを関連づけて検索する事ができる。しかし, 現行システムの多くは, 生データと分析結果を見つけることはできても, 分析法の正しいバージョンを見つけることができず, 分析法Aのバージョン5を表示する。いくつかのシステムでは, 分析法Aのバージョン4は存在しないが, 詳細な監査証跡が残されている。

まとめ

21 CFR Part 11で要求されているデータの完全性要件を満たすために必要な条件を以下にまとめた。
紙のシステムからPart 11対応の電子記録のシステムに移行するための準備をする。Part 11対応に使用するクロマトグラフィー用データシステムを, データの安全性, 完全性, 監査証跡の観点から注意深く評価する。データベースシステムは必須であるが, それ自身にも問題がないかを検討する。特にデータの安全性と完全性について調べる。現行のシステムの問題点を評価したり, 新規のシステムを導入する場合, 生データと分析結果以外のデータについても考慮する; メタデータの重要性を十分に認識する必要がある。分析結果のトレーサビリティーを確保するために, コンピュータが自動作成する時間記録付きの監査証跡機能がなくてはならない。この監査証跡は, システムの使用者と完全に独立して作成され, 記録に対して誰がいつ何をしたのか, 作成, 変更, 廃棄したのかを完全に追跡できなければならない。監査証跡は削除されたり変更されたりしてはならない。Windows NTのイベントビュワーを使った監査証跡は, 完全性と安全性に問題があり, それを使う場合には十分に安全であること, 変更や削除ができないこと, を確かめなければならない。データベースを使用したCDSを評価する場合, 生データ, メタデータ, 分析結果等の関連づけに破綻が来ないかどうかを確認する。各データの改訂記録を厳密に作成することが, Part 11対応では必須とされている。

次の論文では, 電子記録を新しいシステムに移行する場合について説明する。Part 11で発生した新たな問題は, 古いシステムで測定した記録, データをこれらが必要とされる期間を通して再現できなければならない点である。古いコンピュータシステムを保管しておくのではなく新しいシステムにデータを変換する場合について考察する。

引用文献

(1) 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)

(2) W. Winter and L. Huber, "Implementing 21 CFR Part 11 in Analytical Laboratories: Part 2, Security Aspects for Systems and Applications," *BioPharm* 13(1), 44-50 (2000).(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)

(3) R.D. McDowall, "Computer (In)security," *Sci. Data Manage*. 3(6), 8-15 (1999).

(4) C. Burgess and R. McDowall, "Practical Computer Validation" short course at Pittcon 98, p. 6.

(5) P. Motise, *Human Drug CGMP Notes* 5(4) (1997).

(6) R. D. McDowall: "Operational Measures to Ensure the Continued Validation of Computerised Systems in Regulated or Accredited Laboratories," *Lab. Autom. Inf. Manage*. 31, 25-34 (1995).

(7) *Code of Federal Regulations, Food and Drugs*, Title 21, Part 11, Sections 11.10(b) and 11.30, "Electronic Records; Electronic Signatures; Controls for Closed Systems; and Controls for Open Systems" (U.S. Government Printing office, Washington, DC). Also *Federal Register* 62(54), 13429-13466.

(8) Personal email communication between Hewlett-Packard Company (Wilmington, DE) and Paul Motise (Office of Compliance, CDER, FDA, Rockville, MD) (1999).

(9) *Code of Federal Regulations, Food and Drugs*, "Final Rule Preamble to Part 11," at Comment Paragraph 101, 21 CFR 11.50(a)(2) (U.S. Government Printing Office, Washington, DC). Also Federal Register 62(54), 13453 (1997).

(10) P. Motise, *Human Drug CGMP Notes* 6(2) (1998).

(11) B.K. Immel, "GMP Issues: An Electronic Eye Opener," *BioPharm* 12(6) , 60-63 (1999).

(12) R.D. McDowall, "Chromatography Data Systems II: Specifying, Evaluating, and Selecting a System," *LCGC Int*. 12(7), 422-431 (1999).

(13) P. Motise, "FDA Requirements for Computers in Analytical Laboratories," paper presented at the ECA Conference, Berlin, September 1999 (available at www. labcompliance. com/conferences/ august99.htm).

(14) T.P. Loomis, "The Best of LIMS Object and Relational DBMS Can be Combined," *Sci. Comput. Autom*. 15 (3), 73-76 (1998).

(15) L. Guzenda, "Seven Signs That You Need an Object Database," *Sci. Data Manage*. 3(5), 30-33 (1999).

5980-1305JA
April 27, 2001.

Agilent Technologies(アジレント・テクノロジー社)は、ヒューレット・パッカードの電子計測、化学分析、電子部品と医用電子の４つの事業が独立した新会社です。

http:/www.agilent.co.jp/chem/yan

Printed in Japan : 1.0.APR.27.2001 (YG)

21 CFR Part 11
試験室における電子署名と電子記録
第4部 データ変換および長期保管

テクニカルノート

Wolfgang Winter, Ludwig Huber, Agilent Technologies
近藤直人，横河アナリティカルシステムズ株式会社

シリーズ第4部では，電子記録の長記保管方法ならびに記録を再現するために保管しなければならないデータについて説明する。そして，長期保管のみならず，FDAが求めているデータ再生の観点も考慮したうえで，記録媒体やソフトウエアに関して何が必要なのかを説明する。

本シリーズの1-3部では，FDAの電子記録，電子署名に関する要件について説明した。データの安全性と完全性，システムへのアクセスやシステムの主要な機能へのアクセスは承認された者のみに許可されていなければならないこと，データを解析したり審査したりするときにデータの完全性が保証されていなければならないことを説明した(1-3)。データを作成，変更および削除した記録が，どの様にしてコンピュータが自動作成する監査証跡に記録されるべきか議論をした。Barbara Immelによると，記録とバリデーションが，1998年度の承認前査察で最も大きな問題だったと言う(4)。

しかし，21 CFR Part 11には，我々がまだ議論していないことも含まれている。その一つが，記録の長期保管すなわち，GLP, GCP, cGMPが必要とする期間，電子記録の完全性を保ち保管することである。Part 11は電子記録と電子署名の使用のみを対象とし，どの記録を保管するべきであるとか，何年間保管するべきかについては触れていない。これらの要件は，既存の規制に述べられている（既存の規制とは，Part 11が策定される以前から存在していた規制のこと。具体的にはGLP, GCP, cGMPを指す。これらの規制に何を保管しなければならないのか，何に署名が必要なのか，記録は何年間保管しなければならないのかが規定されている）。長期間に渡り記録を保管し，かつそれを再生可能にしておくことは，おそらくPart 11に対応するうえで，最も困難な要求かもしれない。

保管と再生

長期間に渡り記録を保管しそれを再生可能にしておくことは，規制の11.10(b)と(c)に述べられている。

「....以下の条件を満たす手順と管理；(b)正確で完全な記録の複製を，目に見える形式ならびに電子的に作成する手順を作成しなければならない。当局の査察，再調査および当局による記録の複製はこの手順に従って複製された資料を基に実施される。(c)必要とされる記録の保管期間の間，試験を正確かつすみやかに再現できるように，記録を保管する(5)。」

対応上の問題点　この要件に対応することを困難にしているのは次の3つの理由による。

- 記録をすべて電子的に保管しなければならない。データを紙に印刷することは可能だが，これを電子記録の代わりにすることはできない。「タイプライターイクスキュース」はもはや認められない(3,6)。
- 記録は，「完全かつ正確な」コピーとして保管されなければならない。完全なコピーには，各種条件や監査証跡等のメタデータも含まれる(3)。クロマトグラフィーでは，メタデータには検量線や定量方法も含まれる(2)。メタデータがあることで，試験結果を再調査する人が，生データから測定結果，定量結果を再現できる。
- 記録は，その必要とされる保管期間中を通じて，直ちに利用できるようになっていなければならない。

最初にデータ処理をしたシステムと同じものを使ってデータを再現することを，査察官は希望している。これは，分析が行われた後のある一定期間は可能である。しかし，それは時間とともに困難になる。記録の保管期間は，通常10年以上と定められている。10年後に，それを10年前にデータ処理したシステムが現役として残っている可能性はほとんどない。これが問題である。

Agilent Technologies

TI 16C0A3-007
2001. 6 発行

FDAの考え方　規制作成の過程で, 医薬品業界から電子記録コピーの選択肢の一つとして, FDAには紙に印刷した物を提出する旨の意見が提出された(5)。反対意見を持つ人々は,「FDAが必要としている電子記録は, 現在使用されている様々なコンピュータシステムを考えると, 不必要だし, 正当な理由も無いうえ, 現実的でない」と述べている。規制の前文や様々な会議でFDAやその代表者は, 上に述べた理由から規制の妥当性を主張した。

なぜ紙に出力した物が電子記録と同等でないか。

- 電子的に記録されている物すべてを紙に印刷することができない。
- 分析担当者が, データ作成に使用した物と同一の道具を使って, データを調査することをFDAは希望している。例えば, FDAは, 一番最初に使われた積分条件を使ってクロマトグラムデータを再計算し, その結果がつじつまがあっているかどうかを調査することを望んでいる。
- FDAは近代的な電子的な検索手段を利用することを望んでいる。これを使うことで査察をより効率的に行うことができるからである。このような道具を使わない場合, 査察に時間がかかり, ひいては有用な新医薬品の承認が遅れる。効率的に作業するためには, 規制する側も規制される側と同じ技術レベルで仕事をすることが必要となる。

データを取り込んだシステム, ハードウエア, OS, アプリケーションソフトウエアが現役でいる限り, そのデータを保管したり, 再解析することには, 何の問題もない。積分条件は生データと同じフォルダーに保管されていて, この両方を取り込むだけで, 再解析を簡単に行うことができる。問題は, アプリケーションソフトウエアやOSやコンピュータハードウエア自身が新しくなり, 元々のシステムが使用されなくなったときである。

FDA のガイドライン

FDAは, その業界向けガイドや会議等で,「(データ採取, 解析等に)使用したコンピュータシステムの運用を止めた後もPart 11は適用される」と明確に述べている。例えば, FDAは臨床試験に使用するコンピュータシステムについて次のように述べている。

「コンピュータは廃棄されたり, 新しいシステム(多くの場合, 互換性がない)に置き換えられることを十分に配慮したうえでなお, 申請者は古いシステムで記録したデータを検索したり, 再現したりできるようにしておかなければならない。旧システムを稼働可能な状態に保ったり, 新しいシステムへデータを変換することにより, これは可能である。

....FDAは, いつでも試験を再構築できることを期待している。これは, データのみならずデータを取得したり, 管理することにも適用される。それ故, データ保管期間中, 必要とされるすべてのソフトウエアのバージョンやデータ解析用のソフトウエアや記録を保存しなければならない。申請者自身がこれらを保管したり, メーカと契約してソフトウエアを使用できるようにしてもよい。FDAは申請者またはメーカが古いシステムを稼働できるように維持しておくことを期待しているが, 多くの場合これが極めて困難であることも認識している(7)。」

問題は, 如何にして過去の記録を再現する能力を維持するかにある。多くの企業が, 古いコンピュータを保管しておかなければならないのかと心配している。Part 11前文のコメント71には次のように書かれている。「新しいシステムに切り替える際に, データを変換することができれば, かならずしも古いコンピュータとソフトウエアを保管しておく必要はないとFDAは信じている(The agency notes that . . . persons would not necessarily have to retain supplanted hardware and software systems provided they implemented conversion capabilities when switching to replacement technologies)(8).」。

同様に Paul Motise(senior staffer and consumer safety officer in CDER 's Office of Compliance)はベルリンの会議で次のように述べている。「当局は, 旧式のコンピュータやソフトウエアをただ単にデータを再生する目的のために保管することを製薬会社に期待していない。我々は, 正確で完全な電子記録のコピーが作成可能であることを期待している。(The agency did not expect companies to save computer hardware and software for the sole purpose of recreating events. We anticipated that it would be possible to make an accurate and complete copy of those electronic records.)」。

分析試験室に求められること　これらのコメントから, 我々は次のような結論に達した。記録は電子的に保管されなければならない。そして, もともとその記録を作成したコンピュータシステムであるか否かに関わらず, ユーザーの責任で, その記録を再生できるようにしておかなければならない。

これは, 旧システム(コンピュータとソフトウエア)を使用可能に維持するまたは, 新しいシステムに合わせてデータを変換することで実現できる。このように結論すると, 以下の2点が問題となる。電子記録を何に保存するか(なぜなら電子記録は10年以上保管する必要があるから), 記録を作成するのに使用したソフトウエアが使用できなくなったときに保管された記録をどうやって読み, 再生し, 印刷するか。

ここでは, クロマトグラフィーデータを例に「直ちに再生可能"ready retrieval"」の要件に対応するための方法について考察する。そのため問題を長期保存とデータを再生する方法との二つに分けて考える。この議論に立ち入る前に, 保管と再生のためにどの様なデータを保管しなければならないのかを考えたい。HPLCのダイオードアレイ検出器の

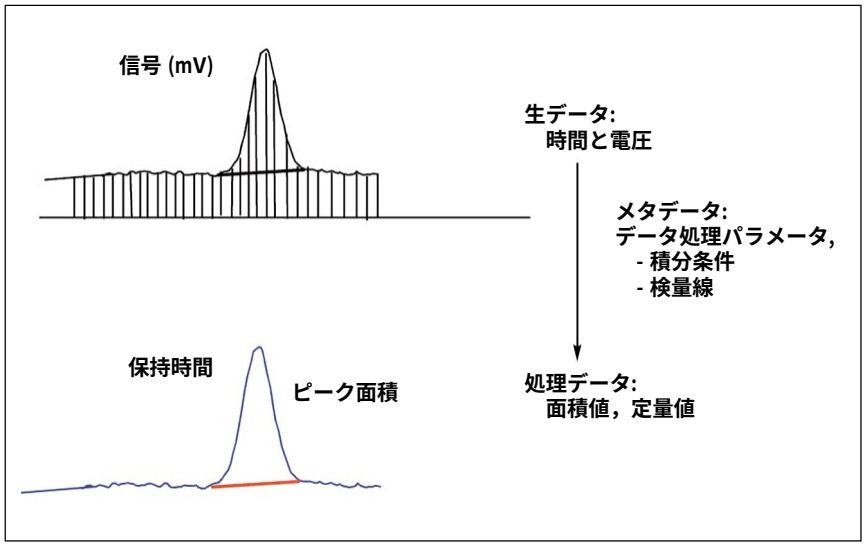

図1．クロマトグラフィーにおける生データ，メタデータ，結果

データを例に, 何を保管しなければならないかを考える。

保管すべき記録の種類

ＦＤＡの「臨床試験に使用するコンピュータに関する指針"guidance for using computers in clinical trials"(7)」は, どのような情報を保管し, 新規システムへデータ変換しなければならないかについて説明している。保管すべきデータは, 試験成績(生データや計算結果)ならびにそれに付随する「データの完全性」にかかわる記録であり, これら諸記録の正確かつ完全な複製を作成することが求められている。例えば, 付随するデータには監査証跡やデータ処理に使用した様々な計算式も含まれる。報告書の作成に使用したすべての解析用ソフトウエア, 検索式等を報告書が必要とされる期間保管しなければならない。データ変換プロトコルもバリデーションが必要である(7)。

データの種類　分析では, 通常, 生データ, 解析条件, メタデータの3種類のデータが発生する。コンピュータシステムにおける生データの定義に関して数年前に議論されたときには, 生データを, コンピュータが取り込んだデータか, コンピュータシステムからの最初のプリントアウトかをユーザが定義できた。当時, 生データはユーザが定義可能で, 紙の記録として保管できた。しかし状況は, Part 11の登場で全く変わってしまった。Part 11により, 生データは最初に長期保存媒体に記録されたもの(通常はコンピュータのハードディスク)であると定義された。クロマトグラフィーにおける生データとは, クロマトグラム波形(単位時間当りの電圧)を指す(図1)。ソフトウエアは生データからピーク面積値や濃度を計算する。測定結果は処理されたデータと呼ばれる(わり算で, 1000/5は生データで, 答えの200が処理されたデータとなる)。

生データから処理されたデータを導くために使用される係数をメタデータと呼ぶ。クロマトグラフィーで, メタデータは主に積分条件や検量線を意味する。

Part 11は, 生データの保存方法について述べているが, 何を生データとして残すべきかには触れていない。これは既存の規制で定義されているからである。

スペクトルデータ　ダイオードアレイ検出器や質量分析計はスペクトル型検出器で, データは保持時間に加えて波長または質量と強度の三次元となる。分析中に取り込まれたスペクトル情報は, 化合物同定や純度確認に使用される。スペクトル型検出器を用いた分析では膨大なデータが発生する。データ保管容量はもはやそれほど大きな問題はないとはいえ, これらのデータを扱うには少し工夫が必要である。

長時間のクロマトグラム(例えば, 1時間でピークは数本しかない)で, クロマトグラム全般のスペクトルデータを保管することはかなりの無駄を生じる。なぜなら本当にスペクトルデータが必要なのはピーク部分だけだからである。適切な機能をもったダイオードアレイ検出器ならこれが可能となる。ピーク部分のみのスペクトルを保管することの長所は明白である; クロマトグラム全部のスペクトルを取った場合データサイズは14MBとなるのに対して, ピーク部分のみのスペクトルの場合にはデータサイズは約1/30の400KBに過ぎない(図2)。

保管が必要とされるデータの種類は, 既存の規制に定められている。データが電子的に保管される場合に必要とされる要件に関してPart 11は扱っている。データには生データ, メタデータ, 測定結果が含まれる。Motiseはクロマトグラフィー生データの保管に関して次の様に明確に述べている;「バッチ記録を保管する期間と同じ期間, 分析試験室のすべてのデータを保管することをＧＭＰは求めている。クロマトグラフィー生データもこれに含まれる("GMPs require you to keep all laboratory data for as long as the batch record must be kept and that includes the chromatographic raw data itself.")。」(9)

記録媒体

電子記録は, コンピュータハードディスク, CD-ROM, DVD, 磁気テープなど様々な媒体に記録することができる。記録媒体を選択する基準は, 社内ネットワーク環境, 経験, 容量, 寿命, そして

最も重要なのはその媒体がいつまで使用可能かなどである。保管期間を設定するにあたって, 記録媒体自身の寿命よりもその媒体をいつまで利用できるかどうかの方が重要となる。例えば, 約10年前, 1990年頃には5インチのフロッピーがまだよく使われていたことを思い出してほしい。現在, 5インチのフロッピー用ドライブを持ったコンピュータを見ることはない。あったとしてもそれが現役で使用されていることはない。歴史的に見ると, 記録媒体は5年サイクルで更新されている。ほとんどの記録媒体に, 長期間記録を保管することは可能である。しかし5年後にその記録を再生できるかどうかは保証の限りではない。市場原理により, 優れた記録媒体が登場するとそれまで使われていた記録媒体は使われなくなる。8インチや5インチのフロッピーディスクが使われていた期間が短かったことを思い出してほしい。記録媒体が市場から無くなるだけでなく, それを利用できる装置も同様にして市場から姿を消す。

障害を受けたデータ　デジタル記録の別の問題として, いつデータが損傷を受けたのかがはっきりとしないことが挙げられる。デジタルデータを長期間保管した経験の無いことや, 記録媒体やそれ用のドライブが製造中止になる可能性などの理由で, 記録を新しい媒体に移すことが必要となる。この様な作業を行うにあたっては, その記録が損傷を受けない様にしなければならない。

さらに困難な問題は, その保管した記録を再生できるソフトウエアが使用可能かどうかである。

記録を取り扱うことのできるソフトウエア

電子記録は二進法, 0と1で記録されている。したがってそれを処理できるソフトウエアがあって初めてその情報は意味のある物となる。この点に関して,

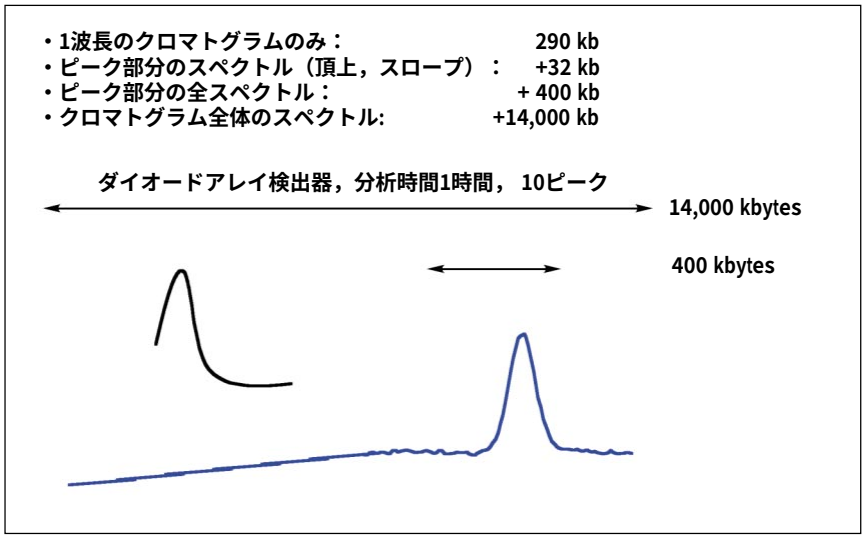

図2．データサイズの比較；クロマトグラムのみ，様々な条件でスペクトルを取り込んだ場合

我々はワープロやプレゼンテーションソフトウエアでたびたび経験している。これらのファイルを開くには, 適切なソフトウエアと正しいバージョンが必要とされる。新しいバージョンで作成したファイルを, 古いバージョンのソフトウエアでは開けないこと, 古いバージョンで作成したファイルを新しいバージョンのソフトウエアで開いて保存するときに, 新しいバージョンの形式で保存するかを聞かれたりすることを経験している。クロマトグラフィーや分光光度計の様な分析機器のデータでも同じことが起きる。クロマトグラフィー用データ処理ソフトウエアはピークの面積を計算したり, 検量線をつかって未知試料中の成分を定量したりする。もし, 分析が行われてから数年後に, 再計算をして同じ結果を得たいのであれば, 使用したソフトウエアが必要になるだろう。Part 11が導入される以前は, より一般的なデータフォーマットたとえばANDI(analytical data interchange format)(10, 11)形式で保管することでこの様な問題を回避できた。このデータフォーマットで保存していれば, 異なるデータ処理ソフトウエアを使用していても, データを再生したり表示したりクロマトグラムや定量結果を印刷することができる。しかも分析者名, 分析条件, 検量線などのデータも印刷することができる。この方法の問題点は, 最初に使用したシステムと異なるシステムを使用してデータを再処理することが許されないことである。この問題点のため, 一般的なフォーマットでデータを保管することが認められていない。査察官は, 最初の結果を得たのと同じ方法でデータの再解析する事を望んでいるからである。生データ, データ処理方法やその他のデータ処理に関する情報, たとえば検量線や再計算の履歴等を保管しなければならない。同じデータ処理ソフトウエアを使用する限り, 問題は大きくない。機器メーカはソフトウエアのバージョンが異なっても同じデータが出るようにしているからである。すくなくとも同じハードウエアとソフトウエアを使用する限りは。理想的には生データや分析結果とともにデータ処理パラメータも同じホルダーに保存することが望ましい。分析機器メーカがソフトウエアを大きく変更したり, 様々な理由からユーザー自身が他の会社のソフトウエアに切り替えたりした場合が問題となる。解析に使用したシステムが使用できなくなると, それを再解析することが全くできなくなる。

他の解決方法　論理的には古いデータを再解析するにはいろいろの方法が考えられる。しかし実際にそれを実行するとなるといろいろと困難なことが生じる。Part 11が導入されるまでは, 4つの方法があった。一つ目は, すべてのデータを紙に印刷して保管する方法である。しかしPart 11でこれは不可能となった。Part 11が導入されてもまだ3つの方法が残っている;標準ソフトウエアと標準データフォーマットを使用する方法;古いコンピュータ, ソフトウエアおよびOSを保管しておく方法;バリデーションされた方法で, 新しいシステムへとデータを変換する方法。

標準ソフトウエアと標準データフォーマット

メーカ間で合意されたフォーマットに基づき生データとデータ処理条件を保管する。現在までいくつかの方法が試みられてきた。たとえばAIA(Analytical Instrument Associatein, 米国分析機器工業会)はANDIフォーマットを開発した。しかしこれらの努力も, 今のところPart 11に適応するには十分でない。たとえばスペクトル情報に関するフォーマットがないなどの問題点がある。ASTMは標準的なフォーマットを作成すると宣言しているが, 今のところ成果は出ていない。

標準的な機能　データファイル形式の標準化よりも, データ処理機能の標準化の方がはるかに困難である。すべてのソフトウエアが, まったく同一の機能を持った時にのみ機能の標準化は可能となる。この場合, データ処理アルゴリズム(計算式など)もまったく同一であることを求められる可能性が大きい。

しかし, これは市場原理に反している。すべてのメーカのデータ解析ソフトウエアが完全に同一の機能を有してなければ, 真に標準化したことにはならない。一方, メーカはマーケットシェアを大きくするために, 常にユーザーがより使い易くなる様にメーカ独自の機能を含んだソフトウエアを開発し続けている。もし, すべてのソフトウエア間でまったく同じ結果を再現できる様にする場合, すべてのメーカのソフトウエアはまったく同じ機能を持たなければならない。このように現実と標準ソフトウエアの理想との間には大きな溝がある。古くからある確立された機能, たとえばピーク面積の計算や単純な定量などに関しては標準化は可能であろう。しかし, 新たに導入された機能については標準化は困難である。当面, このような標準化されたソフトウエアが導入されるとは考えられない。

同一メーカの新しいソフトウエアへデータ変換をするか, 古いコンピュータシステムを保管しておくかの選択が残された。

古い装置を「博物館」に保管しておく

データ保管とデータをいつでも再現できるようにしておく2つ目の方法は, そのデータを作成したコンピュータシステム(ハードウエア, ソフトウエア, オペレーティングシステム)を正しく保管しておく方法である。こうすれば, いつでも古いコンピュータを使って生データを再現したり, 再解析したりする事が出来る。この方法の唯一の利点は, ソフトウエアメーカに依存しなくてすむことのみにすぎない。ソフトウエアメーカが無くなってしまった場合にのみ有効な方法といえる。

この方法の問題点はよく知られている。OSやソフトウエアには寿命はないが, コンピュータハードウエア自身に寿命がある。OSやソフトウエアはハードウエアに依存している部分が大きく, いったんハードウエアが故障したら, 使い物にならなくなる。コンピュータの世界では技術革新がすさまじい速度で進んでいる。5年前のコンピュータでさえ修理することは困難な状況になってきている。このように, 製造中止になったコンピュータを使える状態に維持することは, 現実的には, 極めて困難である。データ保管とデータ再現のために, 古いコンピュータを博物館に保管する事は, 決して推奨できる方法ではない。

新しいシステムにデータを移動する

データ移動とは, 古いシステムで取得したデータを新しいシステムがそのままで処理できるもしくは, 新しいシステムで処理できるように古いシステムのデータを変換することを意味する。同一のメーカで, 短期間でかつ同一のコンピュータシステム上で作動している場合は, ほとんどこの方法で上手くいく。通常メーカは, データの上位互換性を保証しているので, 旧システムのデータを問題なく新しいシステムの上で処理することが出来る。これは, 事務系のソフトウエアでもよく経験している。ワードプロセッサは古いバージョンで作成されたファイルを読むことが出来る。

互換性　この点に関しては, メーカが鍵を握っている。新しいバージョンのソフトウエア(現行バージョンの更新や新規に設計されたものも含めて)は旧システムのデータに関して, 完全な互換性を保証することが理想である。データを直接読む方法でもデータを変換する方法でもそれはかまわない。完全な互換性とは, 旧システムが持っていたすべての機能を保持していることを意味する。新しい機能が付け加えられたとしても(ソフトウエアのバージョンアップではほとんどの場合新しい機能が付加されるのだが), 旧システムの機能を削除することは許されない。

妥当性検査　新しいシステムで, アプリケーションソフトウエアまたはOSを変更した場合には, 古いデータの妥当性を検査しなければならない。いく

つかの典型的な古いデータ(生データ)を再処理してその結果を,元々のシステムで得られた結果と比較することで,妥当性を確認することが出来る。ここでもソフトウエアメーカの協力が必要となる。理想的には,ソフトウエアのバージョン毎にメーカが妥当性検査用ソフトウエアを提供する。これを使って,自動的に旧システムでの計算結果と新システムでの計算結果を比較し,その結果を判定する。この妥当性検査用ソフトウエア自身もバリデーションされていなければならない。

妥当性検査においては,計算結果を以前の計算結果と比較して,その差が許容範囲内であることを調べる。このような許容範囲を定めることは大切で,後になって問題が起きることを未然に防ぐことが出来る。たとえば,クロマトグラフィーにおけるピーク面積や定量値の許容範囲は,0.05〜0.1%以内でなければならない。これは,現実的なクロマトグラフィーの再現性の範囲である。これよりも厳しい許容範囲を設定することは,不必要であるし,現実的でない。数値丸め(切り下げや切り上げなど)のアルゴリズムが変更された場合に問題となる。

データ変換の手順　必ずしも理想的とはいえないが,データの長期保管と利用には,データ変換が現在,唯一の現実的な方法である。メーカは,データ変換のための変換ツールやユーザが指定したデータを使って変換の妥当性を証明するためのバリデーションツールを提供することで,ユーザのデータ変換を手伝うことが出来る。これらの機能は,後から別途開発するよりも,製品の一部として開発されるべきである。また,ソフトウエアを購入する側は,これらの機能をそのソフトウエアの要求仕様や機能仕様に盛り込んでおく。同時に,データ変換をバリデーションするための典型的なデータをいくつか選ぶ必要がある。これらのデータを使って,古いシステムのデータを新しいシステムでもうまく処理することが出来るかを検証する。このような検証作業は変更管理手順に含まれるべきである。

データ移動の方法

LCGC Europeにデータ移動とシステム廃棄を行うための7つのステップが掲載された(12)。使用されているシステムを正確に把握し(資産管理),廃棄に関わるリスク解析をして,実施者の役割と責任を明確にしたシステム廃棄計画書を作成する。現在使用しているシステムのハードウエア,ソフトウエアの情報を収集して,システム使用終了とデータ移動に関する計画書を作成し,計画を実行して,報告書を作成する。
どのデータを移動してどのデータを移動しないかを明確に定義しなければならない。システム廃棄とデータ移動計画書の作成と実行が最も重要な仕事である。

以下に,データ変換計画に関する我々の提案をまとめた。

- データ変換に関する基本方針を作成する
- 日程とチェックポイントを定めた現実的な実施計画書を作成する
- すべてのシステムおけるデータとメタデータを定義する
- 保管の必要なデータ量を出来るだけ少なくする。たとえば,スペクトルデータはピーク部分のみを保存する,分析結果にはシステム標準書式を使う。
- 保管するデータの種類を定義する。たとえば,生データを保管しなければならないかどうか。
- 分析時に,データ処理パラメータをメタデータとして保管する(生データと同じディレクトリに分析結果を保管する)。
- データを再生,再処理して,上記の生データとメタデータ保管が正しく行われているかを確認する。
- 旧システムで採取したデータへの互換性をソフトウエアの要求仕様に盛り込む
- 適切なデータ保管媒体を選定する。指示された保管条件を厳守する。たとえば,磁気テープの場合は,定期的にテープを巻き直すことが必要とされている。
- 定期的にデータの完全性を試験する手順を作成して,実施する。データ処理パラメータは生データと同じディレクトリに保管することを再度推奨する。
- 旧システムを廃棄する前に,新システムで正しくデータを処理できることを確認する。新システムで処理した結果と旧システムで得られた結果の差が定められた許容範囲内であることを確認する。

古いデータの規制対応

Part 11に対する制度的, 技術的な対応が完了するまでに取得した生データやメタデータの扱いをどのようにしたらいいのか。Part 11は1997年8月に施行された。これ以前に取得したデータは, Part 11に対応する必要はなく, コンピュータを使って得たデータでも紙に印刷して保管すればよい。Part 11は過去にさかのぼって適用されない。

一方1997年8月以降にコンピュータシステムを使用して取得し, かつ電子的な記録媒体に保管されたデータは, すべて電子的に保管されなければならない。当時(今でもそうかもしれないが), 多くの試験室が, Part 11に対応できるシステムを有していなかった。あるシステムでは, メタデータを生データや処理データとともに保管することが出来なかった。コンプライアンスポリシーガイドの中で, どのレベルの対応を必要としているのかをFDAは明確に述べている(14)。FDAの代表者たちも制度的な対応(具体的な手順や方針を含めた)を直ちに実施するよう明言している。技術的な対応には時間がかかることを, FDA自身も認めている。しかし, 対応自身は,「最善の努力」で行わなければならない。また, 期限とチェックポイントを含む, Part 11への現実的な対応計画を作成, 実施することをFDAは期待している。

データ変換にはかなりの時間を要する。時間の経過とともにデジタルデータの量は指数関数的に増加するからである。

次回の内容

試験室における電子署名と電子記録“ Implementing 21 CFR Part 11 in Analytical Laboratories ”の最後は, Part 11に対応するための分析機器のコンピュータ制御について議論する。

引用文献

(1) 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)

(2) W. Winter and L. Huber, "Implementing 21 CFR Part 11 in Analytical Laboratories: Part 2, Security Aspects for Systems and Applications," BioPharm 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)

(3) 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)

(4) B. Immel,“ GMP Issues: Step Up to the Responsibility of QA and QC, ” BioPharm 13(2), 58-59,70 (2000).

(5) Code of Federal Regulations, Food and Drugs, Title 21, Part 11, Sections 11.10(a) and 11.10(b),“ Electronic Records; Electronic Signatures; Controls for Closed Systems ” (U.S. Government Printing Office, Washington, DC, 1999). Also Federal Register 62(54), 13429-13466. Available at www.access.gpo.gov/nara/cfr/waisidx_99/21cfr11_99.html.

(6) B. Immel,“ GMP Issues: An Electronic Eye Opener, ”BioPharm 12(6), 60-63 (1999).

(7) Center for Biologics Evaluation and Research, Guidance for industry: Computerized Systems Used in Clinical Trials (FDA, Washington, DC, April 1999). Also Federal Register 64(89). Available at www.fda.gov/ora/compliance_ref/bimo/ffinalcct.htm

(8) Code of Federal Regulations, Food and Drugs, Title 21, Part 11, Summary,“ Electronic Records; Electronic Signatures; Controls for Closed Systems ”(U.S. Government Printing Office, Washington, DC, 1999). Also Federal Register 62(54), 13446. Available at www.fda.gov/ora/compliance_ref/part11/.

(9) P. Motise,“ FDA Requirements for Computers in Analytical Laboratories, ” paper presented at the ECA Conference, Berlin, September 1999. Available at www. labcompliance. com/conferences/august99.htm

(10) E1947-98 Standard Specification for Analytical Data Interchange Protocol for Chromatographic Data (American Society for Testing Materials, West Conshohocken, PA, 1999). Available at www.astm.org.

(11) E1948-98 Standard Guide for Analytical Data Interchange Protocol for Chromatographic Data (American Society for Testing Materials, West Conshohocken, PA, 1999). Available at www.astm.org.

(12) R.D. McDowall,“ Chromatography Data System V: Data Migration and System Retirement, ”LCGC Europe 13(1), 30-35 (2000).
(13) R.D. McDowall,“ Just e-sign on the Bottom Line? ”LCGC Europe 13(2) 79-86 (2000).
(14) Compliance Policy Guide: 21 CFR Part 11; Electronic Records, Electronic Signatures (CPG 7153.17) (FDA, Washington, DC, 13 May 1999). Available at www.fda.gov/ora/compliance_ref/cpg/cpggenl/cpg160-850.htm.

5980-2324JAJP
June 30, 2001.

TI 16C0A3-007 Printed in Japan : 1.0.JULY 19.2001 (YG)

21 CFR Part 11
試験室における電子署名と電子記録
第5部　装置制御とデータ取り込みの重要性

テクニカルノート

Wolfgang Winter, Ludwig Huber, Agilent Technologies
近藤直人，横河アナリティカルシステムズ株式会社

今すぐにでも,21 CFR Part 11に対応しなければならない。現在使用中の多種多様な装置を対応させるのに最も大切なものは「計画」である。
シリーズ第5部では,装置制御の重要性と問題点について議論する。

シリーズ1-4部では,電子記録と電子署名について21 CFR Part 11 (1)が何を要求しているのかを議論した。データの安全性,完全性,長期間データ保管と保管中のデータ再生について論じた(2-5)。権限を有した限られた者のみが,システムや重要な機能にアクセスできることの重要性に関して述べた。また,データの完全性を証明するには,分析時,解析時,記録の作成,変更,削除の際に記録されるコンピュータが自動作成する監査証跡がいかに重要であるかを説明した。長期間データを保管し,保管中にデータを正しく再生する最もよい方法を紹介した。

このように第1部-4部ではシステムから発生するデータに焦点を当てていたが,第5部では装置制御について考える。分析機器の制御にのみコンピュータを使用して,データ取り込みを行わない場合,Part 11に対応する必要があるのかどうか？　答えは簡単である。「もし,紙に打ち出した測定条件を,今までの査察でFDAが要求したまたは見ていたなら,対応は必要である。」 測定条件を適切に記録しなかったら,その測定結果が,正しい手順や条件の下に測定されたことを証明することはできない。もし,測定にコンピュータを使用し,その測定に使用する機器の測定条件が電子的記録媒体(コンピュータのハードディスクや機器のデータ保存用カード)に保存されているなら,Part 11は適用される。

機器制御の規制対応

機器制御ソフトウエアに必要とされる規制対応はバリデーションと21 CFR Part 11との2つである。

21 CFR Part 11　コンピュータ制御された分析機器で,21 CFR Part 11に対応するために保管する必要のあるメタデータは,測定条件(装置設定),装置の運転記録(ログブック),分析した試料名,シーケンスファイル,監査証跡等である。これらの記録は,その試料の分析が実際に実施されたこと,どのような条件で測定されたか,測定が問題なく終了したのか,それとも何か問題があったのかを証明するための重要なデータである。これらメタデータを電子的に記録しなければならない。これらメタデータを電子的に記録できなければ,その分析が実際に実施されたことを証明することは極めて困難と言わざるを得ない。

バリデーション　その装置制御ソフトウエアが開発時にバリデーションされていること,使用時のバリデーションが可能なこと。これは21 CFR Part 11対応以前の問題である。

機器制御の段階

分析試験室は,たくさんの種類の分析機器を使用している。歴史的または戦略的な理由から,同一機器でも複数の機種が使用されている。装置制御には,その精密さと複雑さによっていくつかの段階がある(表1)。

レベル1. システムをコンピュータから制御できない場合:分析機器付属のパネルとキーボードを使って手作業で条件を設定する。データはアナログ/デジタルコンバータ(A/Dコンバータ)を使ってコンピュータに記録される(レコーダに記録する場合は,Part 11の対象外なのでここでは取り上げない)。異なるメーカの装置を組み合わせて使用した場合にしばしば見られる。このような場合,装置設定条件を印刷することは不可能なことが多い。設定条件を手書きで記録する必要がある。A/Dコンバータはオートサンプラから送られるバイナリーコード(BCD)やバー

Agilent Technologies

TI 16C0A3-008
2001. 9 発行

表1．装置制御の段階。各段階の装置制御レベルとPart 11適応の関係を示した。

レベル	制御範囲	Part 11対応上の留意点
レベル1．設定は装置毎に行い,外部出力等で分析開始,終了を同期する。データはアナログ出力される。	**アナログ信号による分析開始，終了**	**メタデータ；装置設定（分析条件）を手書きで記録 分析結果；分析結果とサンプル番号を関連付けることができない。**
レベル2．初歩的なデジタル制御（たとえば,RS232C）	**基本的な装置制御．HPLCの場合，ポンプ流速や検出器波長**	**監査証跡；装置誤作動の記録が残らない；測定が問題なく行われたことを別の方法で証明することが必要。 バリデーション；装置制御をバリデーションすることが困難。**
レベル3．完全デジタル制御（たとえば，TCP/IP）	**すべての機能を制御.オートサンプラのインジェクションプログラム,連続分析,自動波長校正,誤作動の記録**	**監査証跡とメタデータ；装置設定等に関する記録が必要なレベルであることを確認する。**
レベル4．より高度な機能	**コントロールする側とコントロールされる装置間で，ハンドシェイクプロトコルを使用：自己診断とアーリーメンテナンスフィードバック(EMF)；製造番号と型式の自動記録，電子的ログブック（装置運転記録）；装置以外の使用記録，たとえばカラムIDタグを使ったカラム使用記録；同時データ取り込み**	**一歩進んだ誤作動を防ぎ，検出する機能；バリデーション：容易になった装置の適格性確認や保守；Part 11で必要とされる装置のチェックに対応**

コード信号に対応していない。これらの信号には,注入されたサンプルビン番号,試料名が入っており,この情報を使って分析結果と試料とを関連づけることができる。試料と分析結果の対応を確実にするために,オートサンプラとA/Dコンバータの信号授受は極めて重要である考えられている(6)。

レベル2. システム全体をコンピュータから制御できるが,複数メーカの装置からシステムが構成される場合:異なるメーカの装置を組み合わせて使用しているが,中心的な装置メーカが,他社から制御コードの使用許可を受ける,または,リバースエンジニアリングと呼ばれる手法で,他社製品を解読して他社装置の制御コードを自社のシステムに組み込むことでシステムの一元制御を可能にする。この方法を使えば基本的な装置制御は可能となる,たとえば流量,溶媒組成,オーブン温度,検出器の波長など。制御コードが公開されていない場合には,元々の装置メーカからのサポートを受けられない問題がある。しかしもっと大きな問題は,バリデーションや適格性確認である。元々の装置メーカは他社が作成した装置制御プログラムに責任を負わないので,装置制御ソフトウエアを作成した会社のバリデーションサポートが重要になる。また,ファームウエアがバージョンアップされた場合,システムがうまく動かなくなる危険性もある。このようなシステムの場合,誤動作への対応や運転記録が完全で無い問題もある。バリデーション対応のためには,他社装置制御コードが正式に提供された物であり,リバースエンジニアリングで手に入れた物でないことを確認する必要がある。

レベル3. 同一メーカの装置で構成されたシステムでコンピュータからのシステム全体の制御が可能な場合:生データ,メタデータとバリデーションも含めて,完全な対応が最も容易にできる。誤動作の記録やその対策も良くできており,分析が問題なく終了したかどうか,問題が発生した時にも自己診断機能で原因を推定することができる。

高度な機能。同一メーカの利点を活かし,より高度な機能を付加することもできる。たとえば,アジレント社1100シリーズHPLCに登載されているアーリーメンテナンスフィードバック(Early Maintenance Feedback, EMF)と呼ばれる機能がある。これは装置が故障する前に,予防的保守作業を行うことを目的とした機能で,使用時間から判断して消耗部品の交換時期をコンピュータが自動的にユーザに教えてくれる。これは航空機で最初に採用された技術で,分析機器としては初めてアジレント社が採用した。

このレベルになると,装置の製造番号やファームウエア(ROM)のバージョン管理機能も持つ。どの装置を使って試料を分析したのかを確実に記録することができる。

レベル4. 通信(制御やデータ転送)がすべてハンドシェイクで行われる場合:ハンドシェイクとは,装置間の通信が一方通行ではなく,双方向で行われるような通信方法を言う。検出器のデータを受け取った側が,信号を送った検出器にデータを受け取ったことを送り返すのがハンドシェイクである。コンピュータから「分析開始」の信号が分析機器に送られると,装置はその命令を実行して,「分析を開始した」とコンピュータに信号を送り返す。もし,分析を開始できなかったときは,「分析を開始できません」と信号を送り返す。ハンドシェイクでない場合,制御信号は一方的にコンピュータから送られ,実際に分析が行われたどうかをコンピュータは知らない。それに対して,ハ

表2．装置間通信にGPIBを使った場合の長所と短所およびPart 11対応のための助言

長　所	短　所	対　策
高速データ通信に十分な速度を有している（たとえば，ダイオードアレイやLC/MSのようなスペクトル型検出器）	接続可能な装置数が限定される（最大15台）	なし
双方向かつ相手を特定した通信が可能（Part　11の要件，装置のチェックに対応する）	接続されているが使用していない装置の電源オンオフに対応していない。すべての装置は電気的にハンドシェイクしている。途中で1台の電源を切るとシステム全体の通信が止まり,データ取り込みができなくなる。	使用していない装置といえども，決して分析中に電源を切ってはならない
なし	離れた場所からPC経由で装置が正しく機能しているかどうかをか確認するためには，装置のすぐ隣にもう中継用PCが必要。	別途装置制御に関する適格性確認を実施する

表3．装置間通信にTCP/IPを使った場合の長所と短所およびPart 11対応のための助言

長　所	短　所	対　策
高速データ通信が可能	なし	積極的にネットワーク設備の充実をはかる。特にたくさんの装置を使用する大規模試験室では重要。
通信エラーの検出と修正にインターネットの技術を使用（Part　11の要件;データの完全性と装置のチェックに必要な機能）	なし	適格性確認で装置制御の信頼性を確認する。とくにシステムにつながっているが使用していない装置の電源を切った場合。
離れた場所から直接装置をコントロールできる。いかなる中継用装置も必要としない	なし	システム全体の適格性確認の中で試験する。

ンドシェイクの場合は, 分析が行われたのか(上手くいったかどうかは別), 行われなかったのかをコンピュータ自身が知っていてそれを記録する。

Part 11とバリデーションに最も対応しやすいのはレベル3以降, Part 11対応できないのがレベル1, レベル2はその中間段階と言える。

データ完全性のためのプロトコル

21 CFR Part 11で要求されているデータの完全性とトレーサビリティーと多少関係するので, やや専門的になるが, 装置間の通信に使用されているプロトコルの長所と短所について簡単に説明する。比較する通信プロトコルの一つは, 少し前の技術で, GPIB(general purpose interface bus)でIEEE 488とも呼ばれる, もう一つはTCP/IPである。

GPIBと, 最新のネットワーク技術, インターネットやイントラネットで使用される汎用的なTCP/IPプロトコルを比較した(表2, 3に2つの通信プロトコルの長所と短所および短所をカバーする方法をまとめた)。ここでは技術的な詳細については言及しない。技術に関して知りたい場合は他の文献を参照されたい(7-9)。

GPIB を使った装置との通信

GPIBはパラレル方式と呼ばれる通信方式で, 最大15台までの装置をつなぐことができる。命令やデータを含むGPIBを使った通信すべては, バイト毎にハードウエアハンドシェイクが使われている。GPIBケーブルでつながれたすべての機器は, ハンドシェイクしている。従って, GPIBにつながってはいても通信を行っていない機器が, 通信に影響を与えることがある。たとえばどれかの装置が故障するとそれが原因でGPIB全体が止まる。たとえば, 使っていない装置の電源を切っても同様の問題が発生する。

これは, 本来のGPIBの電気的な仕様ではないが, チップセット, ファームウエア, アプリケーションソフトウエアの組み合わせでこのような問題が発生する。

TCP/IPを使ったLAN接続。TCP/IPを使ったローカルエリアネットワーク(local area network, LAN)はしばしば, “インターネット接続”とも呼ばれネットワークを経由して様々な情報をやりとりすることができる。TCP/IPの基本的な考え方は, 情報をパケットと呼ばれる大きさに分割することにある。パケット自身にはチェックサムなどを使った通信エラーを検出して修正する機能が組み込まれている。進歩したシステムとGPIBとの大きな違いは冗長性にある。バケットに含まれるバイト数を計算したチェックサムは, 送ったパケットと受け取ったパケットの内容が同じであるかどうかを確認するのに使われる。同じでなかった場合, 再度送信することを要求する。この方法は, 通

信エラーの無いことを保証する優れたシステムであり, かつ21 CFR Part 11で要求されている装置のチェック(device check)とシステムとしてのチェック(system check)を可能としている。

TCP/IPを使った通信は柔軟性があり, 通信中に他の機器をシステムに付け加えたり, システムから外してもシステム全体は影響を受けない。GPIBに比べて, TCP/IPを使ったLAN環境下では, 分析に使用しない装置の電源を切ることができる。

GPIBとTCP/IP接続

GPIBがTCP/IPに比べて必ずしも劣っているわけではないが, データの完全性, システムの柔軟性, 通信速度等多くの点でTCP/IPが優れており, 今後分析機器間の通信にはますますTCP/IPが採用されてくるものと思われる。

Part 11に対応したシステム

装置の制御やデータ取り込みに用いるシステムを選択する際の注意点を以下にまとめた。

1. 現在使用中の装置がどのような装置制御をしているのかを明確にする(レベル1～4のどれか)
2. これらの装置に対して, メーカ毎にどのレベルの装置制御が可能かを調べる。
3. コンピュータから制御できない機器の機能を制御する方法を文書化する。
4. もし, 他社製の装置をコンピュータから制御している(する)場合, 公開されたプロトコルを使用しているのか, もしくは他社からライセンスを受けているかを確認する。
5. もし, それがリバースエンジニアリングにより行われた場合, 装置制御と通信の適格性確認の方法を確立する。
6. 現有システムのpart 11対応に関するギャップアナリシス(何処が対応できていて, どれが対応できていない)を行う。分析条件, 運転記録, 監査証跡, バリデーションに注意する。
7. 作成したギャップアナリシスをもとに, 対応しない場合のリスクアナリシスを行う。
8. リスクアナリシスの結果とギャップアナリシスの結果を元に, Part 11対応計画を作成する。実施責任者, 期限, 予算等を含める。
9. 計画書に従ってpart 11対応を進める。必要に応じて計画を見直し, 改訂する。

引用文献

(1) Office of Regulatory Compliance, Code of Federal Regulations, Food and Drugs: Electronic Records; Electronic Signatures, Title 21, Part 11 (U.S. Government Printing Office, Washington, DC), issued March 2000. Available at www.fda.gov/ora/compliance_ref/ part11.

(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, ”BioPharm 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)

(5) L. Huber and W. Winter,
" Implementing 21 CFR Part 11 in Analytical Laboratories: Part 4, Data Migration and Long-Term Archiving for Ready Retrieval, "BioPharm 13(6), 58-64(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;第四部　データ変換および長期保管, 横河アナリティカルシステムズ, 2001年7月, 資料番号 TI 16C0A3-007)
(6) R. D. McDowall," Chromatography Data Systems: Part 1, The Fundamentals, " LCGC North America 18(1), 56-67 (2000).
(7) W. Winter," Dynamic Interprocess Communication between a Spectrophotometer and a Spreadsheet, "diploma thesis and presentation for faculty for physical electronics, University of Karlsruhe (31 July 1989).
(8) M. F. Arnett et al.," Understanding Basic Network Concepts, "Inside TCP/IP (New Riders Publishing, Indianapolis, 1994) pp. 51-54.
(9) ANSI/IEEE Std. 488.1-1987: Standard Digital Interface for Programmable Instrumentation (The Institute for Electrical and Electronics Engineers, New York, 1987).

5988-0946JAJP
September 7, 2001.

21 CFR Part 11
第6部　バイオメトリック認証：その限界と可能性

テクニカルノート

Wolfgang Winter, Ludwig Huber, Agilent Technologies

あなたの実験室の装置はあなた自身を認識するだろうか？ ラボのバイオメトリックセキュリティシステムは、あなたの指紋や網膜を読んだり、あなたの手相や掌紋をチェックしたり、またはあなたの声や署名を認識することができる。これらのツールを用いて、あなたの業務をより効率的に、かつあなたのデータをより安全にするかどうかを決定することができるのは、あなた自身とあなたのラボだけである。あるいは、あなたが使用する化学物質やあなたがラボで着けている手袋とマスクがこのようなツールを無効にするのだろうか？

本シリーズの1-5部では，データセキュリティ、データインテグリティ、長期保管および迅速なデータ復元に焦点を合わせて、電子署名と電子記録に関するFDA規則（21CFR Part 11）の要求事項を要約した（1−5)。我々は、システムと重要な機能に対するどのようなアクセスが、権限を与えられた者に制限され得るかを示した。データの解析と評価の時点でどんなデータインテグリティが保証されるか、また、記録の作成、変更および削除がコンピュータの生成する監査証跡にどのように記入されるかも示した。我々はデータをアーカイブして、数年後にそれを正確に取り出すための最良の方法を示した。さらに、我々は機器コントロールの技術的側面を見た。そのすべてが、アクセスとデータセキュリティを保証するため、自然とバイオメトリック認証メカニズムの議論に結び付く。

「従来の」認証スキーム

21CFR Part 11の要求事項は、電子記録の信頼性を保証するために技術制御手段に権限を与える。この制御手段にはアクセスセキュリティのためのメカニズムと権限チェックが含まれる。我々は以前、Windows NT（Microsoft, Redmond, WA）などの近代的なオペレーティングシステムで利用可能な認証スキームを実行するために、ユーザアカウントとパスワードポリシーを管理する重要性について議論した（2)。Trust in Cyberspace［サイバースペースを信用する］で、Schneiderは「認証は、指定された（あるいは暗黙の）信頼レベルで断言される身元（アイデンティティ）を確認する工程である」と書いている（6)。そのようなシステムにおける従来の（かつ最も多用されている）認証スキームは、通常、パスワードや暗証番号（PIN）などのユーザが知っていること、あるいはトークン、IDカード、ICカードなどのユーザが所持しているもののいずれかを基にしている（7)。

Part 11の要求事項によると、このような認証スキームは、手続き上もしくは行動に関する手順によって補足する必要があり、この手順でパスワードやトークンのプライバシーと機密保持を保証して他人に成り済ますことを防止する。例えば、成り済ましには少なくとも2個人の協力を必要とするように、制御手段は設計されなければならない（8)。

身元確認するバイオメトリクス（生物測定学）

従来の認証メカニズムと異なり、バイオメトリクス（生物測定学）では、ユーザが実在すること（9)、あるいは指紋などの個々人に固有のもの（6）を基にする。Woodwardが説明したように、バイオメトリクスは「非常に古くて簡単なコンセプト：人間の認識」に基づくものなので、バイオメトリクスの考えは新しいものでもハイテクでもない（9)。バイオメトリクスはある個人の物理的あるいは行動上の特徴を自動的に測定し、あらかじめ測定しておいた記録との比較によって、その個人のアイデンティティ（同一性）を確認するものである。バイオメトリクスの例には、指紋分析、スピーチパターン認識、手や顔の幾何学的な形および虹

彩や網膜のスキャンがある（表1）。

要求事項ではない Part 11が開発された時点においては、バイオメトリック認証メカニズムは一般に利用できなかっただけでなく、コンピュータのハードウェアとソフトウェアのシステムも確実にサポートしていなかった。規則の意図は、規制が実施された後で開発される新しい技術の使用を見越して可能にすることにある。以前に議論したように、FDAによる規制を受ける産業におけるほとんどの環境ではクローズドシステムが考慮されている ― また、クローズドシステムは暗号化技術やバイオメトリクスを必要としない（1）。

オープンシステム（会社は電子記録の内容に責任を持つものの、このシステム自体へのアクセスを管理しないシステムなど）は、アクセスセキュリティのためのデジタル署名やデータインテグリティと機密保持のための暗号化などの高度な技術なくして、Part 11を遵守することができない。

従来の認証におけるリスクへの対応 従来の認証スキームを使用する場合のリスクは、現金自動預払機（ATM）取引における銀行カードの例が広く知られている。「従来の認証のリスク」ボックスには、このようなタイプの危険性が記載されている。

一般的に、異なったシステムのために別個のパスワードを選び、さらに適切なパスワードポリシーを実施することによって、これらのリスクが管理される。たとえ従来のスキームに問題が生じたとしても、システムへの今後のアクセスにおいて問題の原因を修正することができる。このことは金属製の鍵によるセキュリティに類似している。鍵は更新（変更）することができ、また破壊することもできる。鍵に問題が生じれば、あなたは錠前を交換（鍵を更新）することができ、あなたの所有物は再び安全になる。

バイオメトリックアプリケーション 我々の多くは既に我々の日課の中でバイオメトリクスに触れている。合衆国に頻繁に出入りする旅行者は、ニューアークやサンフランシスコなどの空港

表1. バイオメトリクスの主な種類。R. D. McDowall, "Biometrics: The Password You'll Never Forget（バイオメトリクス：あなたが決して忘れないパスワード）," LCGC Eur. 13（10）, p.736 （2000） から引用

バイオメトリック媒体	主な特徴
顔の形の認証 (Face recognition)	原理：顔の特徴の独特の形、パターン、および配置の分析。非常に複雑な技術で、主としてソフトウェアベース。 本質的に2つの読み取り方法：ビデオあるいは赤外線画像を利用。後者は赤外線カメラが高コストなので、より高価。 主な利点は、バイオメトリックシステムは「ハンズフリー」で操作できること、単にスクリーンを見つめるだけでユーザのアイデンティティが確認されること。 ユーザの連続モニタリング。 ユーザがカメラの視野から外れた場合に、機密情報へのアクセスを無効にできる。 その後、ユーザが作業するためにデスクトップに戻ると、照合が実行される。
指のスキャン (Finger scanning)	原理： 詳細部分の分析（指の画像隆線［検証］終端点、分岐点または隆線の分岐）。 最も商業的に成功しているバイオメトリック技術の1つ。 立ち入る人のアイデンティティを検証するために必要となるアプリケーションにおいて重要。
手の幾何学的な形 (Hand geometry)	原理：ハンドリーダーに載せた手の立体画像をカメラで撮影。 非常に弾力性があり、エンドユーザのスループットを高くできる。
指の幾何学的な形 (Finger geometry)	原理：手の幾何学的な形と同様の原則を用いて、指の立体画像をカメラで撮影。 物理的なアクセス管理領域で立証済み。 非常に耐久性があり、外部的条件をうまく処理。
虹彩認証（Iris recognition）	原理：虹彩（目の瞳孔を取り囲む組織の有色の輪）の分析。 多くのアプリケーション領域で折り紙付の業績を有する、非常に成熟した技術。
手のひら（Palm）	原則：指のスキャンで採用されている技術に類似。手のひらに見られる紋様を利用。
網膜（Retina）	原理：網膜は眼底に位置する血管の層。網膜からデータを得るためのスキャン技法は、エンドユーザの多くが最も迷惑に感じるものと考えられる。エンドユーザは緑色のドットに焦点を合わせる必要があり、この実行時に、システムは無害な光線を使用して固有の網膜の特徴を取得する。 すべてのバイオメトリクスの中で最も正確であると考えられる。
署名（Signature）	原理：署名の静的なイメージよりむしろ署名している間のペンの動き。 署名している間のペン圧、ペンが紙に触れる音、あるいはペンの角度など行動に関するバイオメトリクスとなる多くの場面が研究対象となり得る。 我々は、我々の名前を署名することを学び、この学習プロセスのおかげで我々の署名は独特になる。署名の速さ、速度、および圧力は、ほぼ一定している。 署名システムには専用のタブレットや専用のペンが必要。
音声認識（Voice recognition）	原理：物理的な特性と行動的な特性を融合した声に特有な特性（喉頭の物理的な大きさと身に付いた話し方を採り入れた音響）の分析。 ハードウェアはほとんど不必要（特有の特性を解析するためのソフトウェアを搭載した標準的なPCのマイクロホン）。 理想的には電話ベースのアプリケーションに適す。

従来の認証におけるリスク

パスワードはスパイされたり見られたりして「盗まれる」。

貧弱なパスワードは推測されたり、辞書ベースのセキュリティ攻撃ツールによる攻撃を受けて「解読」されたりする可能性がある。

同じパスワードがもう1つの別のシステムで使用されている場合、パスワードが危うくなるリスクは2倍に増加する。

パスワードは失くしたり忘れたりすることがある。多くのパスワードは、便利だという理由から、コンピュータ周辺のどこかに書き留められていたために危険に曝されてきた。

で、米国入国審査簡易プログラム（INSPASS）による必要なアイデンティティをバリデーションするための手の幾何学的な形スキャナを使用したかもしれない（10）。この仕組みは入国審査を抜本的にスピードアップしている。

健康管理においては、指紋スキャンとICカードによって対象者の探索とカルテの入手を加速している。また、この方法は連絡することができない患者を特定し、医療サービスの誤用を探知する助けにもなる。このようなスキャナの供給者によると、指紋認証システムは「バイオメトリック認証の有力な形式になり、99.9％の正確さであるものの、100万人を超えるデータベースから一個人を確認することも特定することもできない」（11）。もちろん、典型的なラボ環境においては、実際に識別を必要とする人の数は限られており、識別過程がランタイム性能を妨害すべきでもない。

McDowallは、最近、最新のバイオメトリックアプリケーションの概要を発表し（表1）、ラボにおけるアプリケーションにとっての長所と短所それぞれについて議論した（12）。バイオメトリックシステムを選ぶ前に、ラボ環境で通常身につけている防護用具が識別過程をどれほど厄介にするものかを事前評価する必要がある。アプリケーションはフェイスマスクを通して網膜パターンを読むことができるのだろうか？手袋は指紋スキャンのために外す必要があるのだろうか？あなたはどんな化学物質を使用するのだろうか、またその化学物質はスキャナにどんな影響を与えるのだろうか？

バイオメトリック認証におけるリスク

バイオメトリクスでは、ユーザの身体がパスワードになる。このことは、パスワード自体を盗んだり改ざんしたりすることが極めて難しいことを意味する。ユーザは貧弱なパスワードを作成できるが、ユーザは貧弱なバイオメトリックを選ぶことはできない（13）。とはいえ、バイオメトリックシステムのセキュリティに対する攻撃は、次のようなセキュリティチェーンの脆弱部に集中しそうである。入力メカニズムのセキュリティ、バイオメトリック指標のデジタル表示、およびバイオメトリック指標の単一項目性（unarity）（7）など。

永遠に失われる 言い換えると、おそらくセキュリティ攻撃は入力デバイスからではなく、それによって生成されるデータから始まるだろう。Millerは次のように書いている。

パーソナルコンピュータが提供するバイオメトリック認証データは、推定されるスキャニングデバイスが生成したかも知れないし、攻撃者が供給したビット列かも知れない。したがって、正当なバイオメトリックデータであるように見えるビット列を発生させることが可能であるという点では、そのようなシステムは無防備である。その上、バイオメトリックスキャンをバリデーションするために必要なテンプレートの所持、さらにそのテンプレートを作成するために用いるアルゴリズムの知識が、そのようなビット列を発生させるために十分な情報を供給する可能性がある（テンプレートが危ういユーザに対して）。すなわち、任意のバイオメトリック認証サーバに格納されたテンプレートデータを公開は、影響を受けたユーザにとってバイオメトリック技法の使用が永遠に不可能となるおそれがある（7）。

上記のことは、バイオメトリクスの持つ最も大きな危険は、個人のバイオメトリックデータやパラメータがいったん盗まれると、一生を通じて影響を受けてしまうことを意味する。このことは盗まれた鍵の例とは大きく異なる。バイオメトリックは更新したり破壊したりすることができない。もし攻撃者があなたの左手の親指の指紋を示すビット列を所有しているとすると、あなたは左手の親指で決して安全にシステムにアクセスできなくなるだけでなく、攻撃者によるそのビットストリームの使用はあなたに帰することになってしまう。多くのコンピュータ科学者が到達した今日の結論は、「バイオメトリクスは、リーダーから検証者までの接続が安全である状況下では有用である」（12）。

バラツキの許容 2番目の脆弱性は、大部分のバイオメトリックスキームの技術的な実施によってもたらされる。バイオメトリック測定では、測定を通して、またはテストされた特性自体によってもたらされる何らかの可変性を示す複雑なパターンを処理する。例えば、手書きの署名は書くたびにわずかに異なっている。あなたの声が異なって聞こえることもある。または、あなたの指紋のデジタル表示はカットされて改変されるかもしれない。このことは、バイオメトリックアプリケーションにおける一致の決定には組み込まれた許容範囲が必要であることを意味する。しかし、バイオメトリック認証スキームは厳格すぎる許容範囲によって無効にされることもある。この脆弱性は慎重なリスクアセスメントとシステムバリデーションによって管理する必要がある。

プライバシー バイオメトリクスに固有の付加的なリスクは人のプライバシーに関係する。「バイオメトリックは、単一要素からなるアイデンティティで

ある。我々はみんな、左手の親指の指紋は1つしか持っていない。あなたは自分の個人的なアイデンティティから自分の仕事のアイデンティティをどのように分離するだろうか？ヨーロッパのプライバシー要求事項（the OECD Cryptographic Guidelines of 1997, Principle 5［1997年のOECD 暗号ガイドライン、原則5］）に適合させるための米国の不十分な活動と相まって、みなさんの個人的な活動（購入習慣、娯楽の好み、政治活動）が仕事の活動に否応なく結び付けられるという深刻なリスクがある」(14, 15)。

バイオメトリクスの代替手段

コンピュータシステムのセキュリティも、ハードウェアトークンや公開鍵証明書などのように、ユーザが持っていたり知っていたりすることを利用することに由来する。公開鍵証明書は2つの暗号化キーを使用する。最初のキーは情報を暗号化するために、次のキーはこれを解読するために使用される。作成者のみが変更できる文書でもすべての人が読めることを保証するために、暗号解読キー［復号化キー］を利用可能とする（発行する）必要があり、これが公開鍵になる。暗号化キー（秘密鍵）は秘密にしておかれる。対象とするアプリケーションによっては他のバリエーションが可能になる（例えば、秘密性を保証するために、文書を受取人の秘密鍵で解読する必要があるかも知れない)。どちらのキーも暗号化したものを解読できないのでバリエーションが可能である。暗号化キーによる管理の弱点は、キーを支給する必要があること、信頼できる権威者（証明当局）によって人々のアイデンティティを確立し、記録する必要があることである。

ラボへの推奨

必要とされる保証を決めること あなたの分析ラボの認証スキームを定義するときには、従来の認証技術は高度のセキュリティ保証を提供しないということを忘れないことである。しかし、ほとんどのクローズドシステム環境では、しっかりしたセキュリティを含む適切な認証手順とパスワードポリシーの使用によって、最も一般的な手段による記録の劣化を効果的に防いでいる。

目的のための適合性を事前評価すること バイオメトリック認証スキームを決定する前に、それが本当に所期のセキュリティ目的に必要であるかどうかを決めることである。バイオメトリック認証には標準外の追加ハードウェアを必要とすることがあり、システムの残り部分と一緒にバリデーションすることが難しくなる可能性がある。バイオメトリックキーの更新や破壊ができないということを忘れないことである。バイオメトリックキーを傷つけたり失くしたりすると、死ぬまで利用できない。

暗号法を考慮すること あなたが開放環境で働いている場合（例えば、あなたのITインフラがサービスプロバイダに外部委託されている場合)、暗号化認証を考慮する必要がある。多くのIT環境では、ユーザ特有のパスワードを生成させるためにICカードが使用されており、制限された時間内（1分間）は有効で検証サーバと同期している。パスワードは、本人のみが知っているはずの個人的な暗合もしくはPIN（暗証番号）を用いて生成される。ハードウェアのトークンと暗証番号は、盗まれたり改ざんされたりするという本質的なリスクを伴っている。しかし、固定ユーザのログオンとパスワードの組み合わせが改ざんされ易いことと比べれば、そのリスクは小さくなるはずである。

潜在的セキュリティリスクを実践的に事前評価すること John Woodwardは Information Security誌で次のように記している。「大きなソフトウェアシステムは…欠陥なしに開発することはできないものの、脆弱性を予期して事前に対処することによって、そのようなシステムの信頼性を向上させることが可能である」(9)。例えば、あなたはバイオメトリックリーダーからバイオメトリックを検証する処理過程までの接続を保証するために特別な注意を払う必要がある。この接続が潜在的なセキュリティ攻撃に対して無防備な部分だと思われるので、あなたはこの部分が会社や部門の外からアクセスできないように手段を講じる必要がある。

専用のセキュリティ監査ガイドラインを開発すること。政府当局が展開しているセキュリティ監査でこれまでに行われた作業を有効に活用することである。例えば、オーストラリアのニューサウスウェールズのIT局は、セキュリティと監査ログの使用を中心とするグッドリスクアセスメントと監査ガイドラインを発行している（16)。

21CFR Part 11の目的と分析ラボのデータを保証することの目的に関する広大で長期的な観点から、我々の適合性タスクをより容易にするように導いてくれる。我々は以下のようなMoskowitzの発言に賛同する。「我々は、強みを活用して弱点を減らすような方法でセキュリティシステムの作成に専念する必要がある。こうすることで、我々は我々が活動を保証する人達のプライバシーを強化することができる。また我々は、このデジタル時代に必要とされるセキュリティにもかかわらず実行するために、彼らの仕事をより容易にすることができる」(15)。

ギャップを縮めること

本シリーズの最後の論文では、規則が発効するよりずっと以前に設計され、インストールされていたレガシーデータシステムについて、21CFR Part 11が要求する技術制御手段を実行することに焦点を当てる。適切なギャップ分析（適合作業に困難が存在する）と適切な修正アクションプランの所見に基づいて、Part 11の要求事項がどのように満たされるかを議論する。

参考文献

(1) 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）

(2) W. Winter and L. Huber,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 2, Security Aspects for Systems and Applications,”BioPharm 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）

(3) 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）

(4) L. Huber and W. Winter,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 4, Data Migration and Long-Term Archiving for Ready Retrieval,”BioPharm 13 (6), 58-64 (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；第四部　データ変換および長期保管，横河アナリティカルシステムズ，2001年6月，資料番号TI 16C0A3-007）

(5) W. Winter and L. Huber,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 5, The Importance of Instrument Control and Data Acquisition,”BioPharm 13 (9), 52-56 (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；第五部　装置制御とデータ取り込みの重要性，横河アナリティカルシステムズ，2001年9月，資料番号TI 16C0A3-008）

(6) Committee on Information Systems Trustworthiness, Trust in Cyberspace［情報システムの信頼性に関する委員会、サイバースペースを信用する］, F.B. Schneider, Ed. (National Academy Press, Washington, DC), 22 December 1998. Available at http://cryptome.org/tic.htm.

(7) A. Miller, Risks in Biometric-Based Authentication Schemes［バイオメトリックベースの認証スキームにおけるリスク］, Information Security Reading Room (SANS Institute, Bethesda, MD), 2000. Available at www.sans.org/infosecFAQ/biometric.htm.

(8) Office of Regulatory Compliance, Code of Federal Regulations, Title 21, Food and Drugs: Electronic Records; Electronic Signatures［規制適合性局、連邦規制のコード、タイトル21、食品と医薬品：電子記録；電子署名］, Title 21, Part 11 (U.S. Government Printing Office, Washington, DC), issued March 2000. Also Federal Register 62 (54), 13429−13466. Available at www.fda.gov/ora/compliance_ref/part11.

(9) J.D. Woodward,“Believing in Biometrics［バイオメトリクスを信じること］,”Information Security (February 1998). Available at www.infosecuritymag.com/biometrics.htm.

(10) Immigration and Naturalization Service, How Do I Apply for INSPASS? ［INSPASSの申込方法］ (U.S. Department of Justice, Washington, DC), last modified 11 August 1999. Available at www.ins.usdoj.gov/graphics/howdoi/inspass.htm.

(11) Positive Identification in Health Care Systems［健康管理システムにおける実際的な認証］, NEC Technologies, Inc. (Itasca, IL, 1998).

(12) R.D. McDowall,“Biometrics: The Password You'll Never Forget［バイオメトリクス：絶対に忘れてはいけないパスワード］,”LCGC Eur. 13 (10), 734-742 (2000).

(13) B. Schneier,“Biometrics: Uses and Abuses,”Inside Risks 100［「バイオメトリクス：使用と乱用」、100のリスクの内側］, Communications of the ACM, 42 (8), Counterpane Internet Security, Inc. (San Jose, CA), August 1999. Available at www.counterpane.com/insiderisks1.html.

(14) Organisation for Economic Co-Operation and Development, Cryptography Policy: The Guidelines and the Issues［OECD、暗号化ポリシー：ガイドラインと発刊］, March 1997. Available at www.oecd.org/dsti/sti/it/secur/index.htm.

(15) R. Moskowitz,“Are Biometrics Too Good?”［バイオメトリクスはそんなに良いか？］Network

Computing, Issue 1002 (25 January 1999). Available at www.techweb.com/se/directlink.cgi?NWC19990125S0017.

(16) Security of Electronic Information Audit Guideline［電子情報監査ガイドラインのセキュリティ］, Issue 1.0 (Office of Information Technology, Sidney, Australia), 21 January 1998. Available at www.oit.nsw.gov.au.

Printed in Japan, September 09, 2002
5988-0947JAJP

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

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

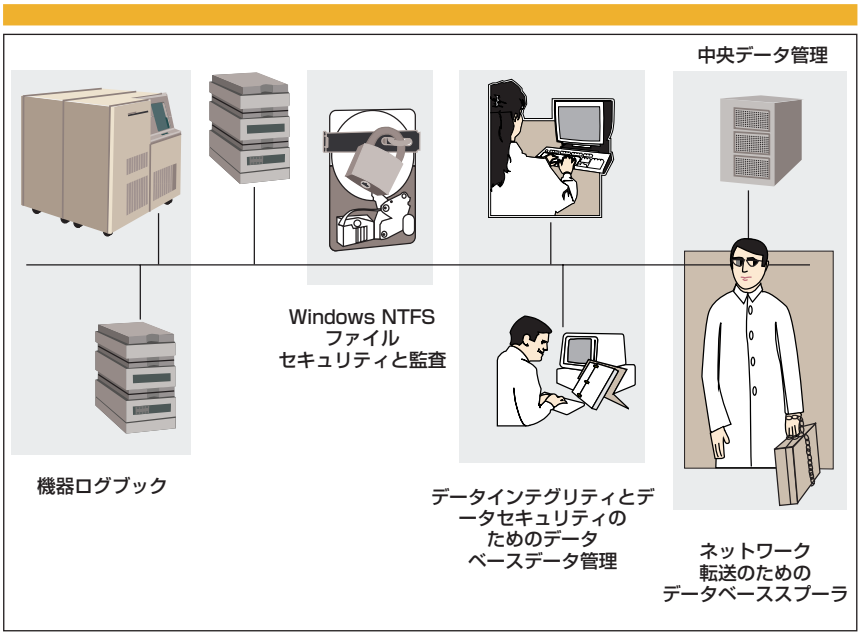

図1. Agilentのケミステーションセキュリティパックで使用されるセキュリティツール

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

21 CFR Part 11
Part 11は消えていない
電子記録の新しいドラフトガイダンス

Wolfgang Winter, Ludwig Huber
BioPharm International MAY 2003　投稿文を翻訳

電子記録と電子署名の規則はまだ引き続き有効である。今回の変更は，製薬企業が特定の電子管理を実行するかどうかの決定を，文書化されたリスクアセスメント，および対応するプレディケートルール（GLP，GMP等の既存規則）に詳述されている記録要件を考慮することによって，正当化しなければならないことを意味する。

2月20日に，FDAは新しい21 CFR Part 11ドラフトガイダンスを発行した。「新しいガイダンスは，Part 11がもう執行されないことを意味する」という噂は間違っている。新しいガイダンスは，主に，製品品質に影響するリスクの低いコンピュータシステムに向けられる。一方，製品品質の決定に使用されるクロマトグラフ用データシステム（CDS）やラボラトリ情報管理システム（LIMS）など，製品品質に影響するリスクの高いシステムについては変更はない。

白紙に戻ったガイダンス

電子記録と電子署名に関するFDAの21 CFR Part 11規則は1997年に導入された[1]。規制当局―医薬品評価・研究センター（CDER）と生物製剤評価・研究センター（CBER），医療機器・放射線保健センター（CDRH），食品安全・応用栄養センター（CFSAN），動物薬センター（CVM），および薬政部（ORA）―によるその後の施行は，製薬業界に次のような協力を産み出した。

- 規則の解釈
- カレントシステムのPart 11コンプライアンスアセスメントの実行
- ギャップ分析の実行
- 新しいシステムのバリデーション計画と実行計画の開発および実行（古いシステムの移行と廃棄計画と一緒に）
- Part 11が強制する手続き上および技術上の管理を実行するための新しいシステムの開発。

そのため，FDAがPart 11を再検討し，以前のドラフトガイダンス文書とコンプライアンスポリシーガイド（CPG）7153.17を取り下げるという意向を発表したとき，多くの人々が衝撃を受けた[2]。このことは，2月4日付けの連邦広報[3]で発表され，続いて2月20日に新しいドラフトガイダンス「Part 11，電子記録；電子署名―範囲と適用」が発行された[4]。我々が以前の論文[5]で議論したように，FDAは2002年8月に発表したCurrent Good Manufacturing Practices（CGMP）イニシアチブ[6]の見地からPart 11を再検討している。

バランスを見つけること

最初のPart 11規則の施行後に，FDAは，用語解説[7]をはじめ電子記録のバリデーション[8]，タイムスタンプ[9]，維持[10]，およびコピー[11]に関連する多くのドラフトガイダンス文書だけでなくその執行ポリシー[2]に関するCPG 7153.17も発行した。これらのガイダンス文書は業界によって研究され，コンプライアンスコストに関する関心を高めた。2つのドラフトガイダンス―電子記録の維持[10]および電子記録の電子コピー[11]は，両方とも，プレディケートルールによって要求される保有期間全体にわたって電子記録を処理すべきであると提案していたために，かなり批判された。それは10年以上になる可能性があった。また，業界の関心はそのタスクが非常に高価になる可能性があり，技術が必ずしも利用可能であるとは限らないということであった。

Part 11は枠組みを定義しているが，製薬業界とそのサプライヤがコンプライアンスに向けた実行計画に取り

組み始めたとき，実用的なシステムとプロセスに関する問題が多く発見された。

例えば，Parenteral Drug Association（PDA）はGood Electronic Records Management（GERM）のためのガイドラインを開発するためにPart 11作業部会を結成し，Good Automated Manufacturing Practice（GAMP）フォーラムはPart 11の最良の実行方法に関する文書を開発するために分科会（SIG）を結成した。両方の論文はInternational Society for Pharmaceutical Engineering（ISPE）から発行された[12, 13]。

多くの刊行物で述べられているように，適切に行うことと行い過ぎることとの間の正しいバランスを見つけることは困難である。「特定のバリデーションの努力が行われるべきであるかどうかに関して何らかの疑問がある場合，バリデーションの努力が何らかの科学的な価値を加えるかどうかを尋ねることによってのみ，最終的な答えを得ることができる」[14]。

新しい要件

Part 11が消えたわけではない。新しいドラフトガイダンスでは，新しい電子記録と電子署名の要件は何も定義していない。ここでは製品品質と公衆衛生に絶対不可欠の状況に焦点を当て直しているだけで，ほとんどプレディケートルールによって支配される。（4月の議論期間終了後に予想される）最終的なガイダンスは，技術的に複雑でバリデーション集約的な監査証跡(audit trail)，タイムスタンプ，記録の保管，および記録のコピーといった領域にはあまり重点を置かないことになりそうである。これは，特にレガシーシステム（Part 11が実効された1997年8月20日以前にインストールされたシステム）に対してプレディケートルールに従うということである。

新しいドラフトガイダンスでFDAは，プレディケートルールで強制される記録がまだ必要であると再強調しているが，より少ない記録がPart 11の対象として考えられると述べている。我々は，全体の保有期間を通じたデータ処理のための最も厳しい要件が，企業の文書化されたリスクアセスメントや作業規範に基づく時間枠に置き換えられることを期待する。

2003年2月までは，Part 11は漠然と解釈されていて，製品品質と安全性に高いリスクを与える可能性のあるシステム（最終医薬製品の品質管理分析に使用されるCDSなど）と低リスクシステム（標準操作手順書を作成するために使用されるワードプロセッサなど）とを区別しなかった。企業は，物議をかもし、かつ紛らわしい強制力である「Good Practice」(GxP)環境下で作成されるすべての電子記録について，Part 11に適合するための信頼できる活動計画を開発し，文書化し，そして実行することを要求された。

表1. 新しいPart 11の下でも施行されるプレディケートルールが要求する記録の種類の例

記録の種類	カテゴリ[a]	参照プレディケートルール
製剤が設定された仕様を遵守していることを保証するための製造，管理，およびラボラトリの記録；部品，製剤容器，およびラベリング用の記録	GMP	21 CFR 211.180
装置の洗浄・使用記録	GMP	21 CFR 211.182
マスター製造・管理記録	GMP	21 CFR 211.186
バッチ製造・管理記録	GMP	21 CFR 211.188
製造記録レビュー	GMP	21 CFR 211.192
ラボラトリ記録	GMP	21 CFR 211.194
非臨床ラボ試験用のプロトコル	GLP	21 CFR 58.120
非臨床ラボ試験の報告	GLP	21 CFR 58.185
生データ，文書化，プロトコル，最終報告書，QA検査記録とサンプル，職務記述書，トレーニング記録，機器のメンテナンス，キャリブレーションおよび検査の記録	GLP	21 CFR 58.195
INDAs[b]用の記録およびICH[c] GCPガイドラインに記載されている記録のサポート	GCP	21 CFR 312.57
	GCP	21 CFR 312.62
データ変更を文書化などの方法で可能とするようにシステムが設計されていること，および入力データの削除が防止されていることを保証する記録	GCP	ICH GCP 5.5.3 (c)
	GMP	EU GMP Guide Annex 11 §10[d]
データ変更できる権限を与えられた人のリスト	GCP	ICH GCP 5.5.3 (e)

a GMPはGood Manufacturing Practiceの略称；GLPはGood Laboratory Practiceの略称；GCPはGood Clinical Practiceの略称。
b INDAsはinvestigational new drug applications（新薬臨床試験申請）の略称。
c ICHはInternational Conference on Harmonisation（国際ハーモナイゼーション会議）の略称。
d 参考文献18を参照。

リスクベースのアプローチ

2002年8月に，FDAはサイエンスベースのリスク管理を統合品質システムアプローチに融合するイニシアチブを発表した。「最も効果的な公衆衛生の保護を提供するために，FDAはその努力レベルをリスクの重大さに調和させなければならない。政府機関はリスクベースのプログラムを実行してきているが，より系統的で厳しいリスクベースのアプローチが開発されるだろう」[6]。

GAMPガイド

規制当局からのアセスメントの実施方法に関する明確なガイダンスがないので，2月20日より前に業界評議会はガイドラインを発行した。「リスクアセスメントのためのガイドライン」というGAMP4ガイドの付録M3は，バリデーションプロセスとリスク管理との間のミッシングリンクを確立している[13]。ここでは以下のような定形化，文書化されたリスクアセスメントプロセスを提案している。

- リスクシナリオを通した作業リスクとGxPリスクの特定および評価
- 起こりうる失敗や逸脱の可能性と重大性の評価
- 失敗を検出するための確率の判断
- 適切なリスク低減戦略の定義の要求

付録M3の主要部分は「一連のGxP評価基準に対して評価される場合のシステムの機能やサブ機能がリスクを示すかどうかの判定」である。このリスクベースのアプローチは，業界，サプライヤ，および規制当局が公衆衛生と消費者保護のための重大な問題の資源に焦点を合わせることを支援するであろう。

表2. 新しい21 CFR Part 11の下でも執行される（および，執行されない）記録の種類の例

記録の種類	Part 11の対象	例
プレディケートルールで維持することが要求され，紙の記録の代わりにラボラトリ電子形式で維持される記録	はい	・オリジナルの観察 ・機器の生データワークシート ・機器校正記録 ・指定のサンプリング，テストおよび点検が実際に行われたことを立証するメタデータ ・原料とバルクのテスト結果および完成品
電子形式で維持されていても，プレディケートルールが必要とするレポート以外の記録	いいえ	機器診断ファイル，プレゼンテーションまたは作業
プレディケートルールで維持することが要求され，優れた電子形式と紙形式で維持されており，一連の規制活動がそれに頼っている記録	はい	クロマトグラフシーケンスから製品リリースまでの定量結果
プレディケートルールの下でFDAに提出する電子記録	はい	・臨床実験プロトコル ・ NDAs[a]
提出されず，プレディケートルールで維持することも要求されていないものの，提出文書の作成に使用される電子記録	いいえ	個々のソース文書からNDAs[b]向けの提出文書パッケージを照合するためのバッチファイル（スクリプト）
プレディケートルールで要求される手書きの署名，イニシャル，およびその他の一般的な署名と同等であると意図される電子署名	はい	クロマトグラフデータシステムにおけるサンプル，シーケンス情報，メソッド，および計算のデータエントリ変更を承認するために使用される電子署名

a INDAsはinvestigational new drug applications（新薬臨床試験申請）の略称。
b NDAsはnew drug applications（新薬承認申請）の略称。

継続的な実施

新しいドラフトガイダンスの第一のメッセージは，「Part 11の一部の要件に関しては施行裁量(enforcement discretion)を行使する」ために，FDAは従来より狭い範囲でPart 11を解釈するつもりであるということである[4]。施行裁量は「バリデーション，監査証跡，記録の保管，および記録のコピー」のような領域で行使される[4]。これらは業界が技術的な複雑さを管理しようとして膨大な努力を費やしていた領域である（非常にわずかな利益のために）。しかし，「施行裁量」は，監査証跡，電子プロセスおよび記録保管手順のための技術的な管理がもはや必要ではないことを意味している訳ではない。21 CFR Part 11は依然有効なのである。文書化されたリスクアセスメントによって，また対応するプレディケートルールにおける記録要件を考慮して，会社は特別の管理を実行するかどうかの決定を正当化しなければならないとだけ，FDAは言っている。

プレディケート記録ルール

新しいドラフトガイダンスでは，プレディケートルールに概説されている記録要件の重要性を強調している。製品品質に関連するプレディケートルールによって要求される記録は，継続してPart 11規制の対象となり，執行が続けられるであろう。特に，アクセスセキュリティ，稼動中のシステムとデバイスのチェック，オープンシステムコントロールおよび電子署名のための主要なテクニカルコントロールは，適切な職員研修，文書化および変更管理と共に依然として必要である。Good Clinical Practice（GCP）とGood Laboratory Practice（GLP）などのいくつかのプレディケートルールでは，特にユーザが予想される場合，規制された記録を作成するか，変更するか，または削除するための通常の操作の間の変更を追跡することに関する監査証跡は確かに必要である。

表1には，プレディケートルールによって要求される記録の例をリストしている。このリストは，Part 11の新しいガイダンスがGxP規制の対象となる分析ラボラトリで使用されるCDSにはほとんど適応していないという我々の声を補強する。GMPとCGMP規制はこの業界の作業プロセスと手法に強く影響する。記録の別のカテゴリを表2に要約した。元のGxP規制によって定義されているような記録が依然として21 CFR Part 11とその後の施行の対象であるかどうかをリストしている。

表3. 新しいドラフトガイダンスでも施行されるPart 11規制，およびFDAが新しいドラフトガイダンスで概説した「施行裁量」を行使する可能性のある記録要件

新しいガイダンスで引き続き要求され施行される記録の種類（Part 11の対象となる記録について）	新しいガイダンスに影響され，かつFDAが「施行裁量」を行使する可能性のある記録
・システムのバリデーション ・システムアクセスを承認された個人に制限すること ・稼動中のシステムチェックの使用 ・権限チェックの使用 ・デバイスチェックの使用 ・電子記録や電子署名システムを開発，維持管理，または使用する者は割り当てられた業務を実行するための教育，トレーニング，および経験を有することの決定 ・署名の説明責任 ・電子署名に関連する要件	・文書化されたリスクアセスメントでは製品品質への効果がないか低い場合は，電子監査証跡，バリデーション，記録維持，電子コピーなどのPart 11の特定要件 ・レガシーシステム（1997年8月20日以前にインストールされたもの）に対するPart 11の施行

確立した作業プロセス

規制活動を実行するために頼る，確立した作業プロセスの一部でもある記録は，依然としてPart 11要件の対象となる。ネットワークデータシステム（NDS），CDS，LIMS，および統合（基幹）業務システム（ERP）は重要な意志決定支援データを管理し，GxP施行の焦点であり続ける。これらのシステムによって管理されるデータの信頼性と確実性はセキュリティ，データインテグリティおよびトレーサビリティを保証する効率的なテクニカルコントロールに大きく依存する。

新たなドラフトガイダンスでは，電子記録が紙の記録の代わりに使用されるかどうかを決定するために，FDAは作業規範を使用することができると強調している。したがって，規制活動を記録するために電子記録または紙の記録を使用するかを決定して文書化することを，我々は推奨する。

施行裁量

FDAは，21 CFR Part 11によって強制される多くのテクニカルコントロールに「施行裁量」を行使すると発表した。この決定は，GxPとPart 11コンプライアンスへのアプローチが元に戻る必要があるかもしれない間，影響を受ける業界とサプライヤが現在過渡期にあることを認識している。従来のガイダンス文書の撤回によって，PDAのGERMガイドラインなどに含まれている業界の「Common Good Practice」の役割は，会社が正しいものに焦点を合わせることを支援する際に関与する[12]。このタイプの業界ガイドラインによって取られるアプローチと同様に，新しいガイダンスの目的は，ものごとを正しく行うのではなく，正しいことを行うことである。

Part 11は今までどおり適用される

表3には，新しいドラフトガイダンスに「最も影響を受ける」GxP要件と「影響を受けない」要件を例示する。表3は，記録に関する従来のPart 11テクニカルコントロールの大部分は施行され続けることを示している。Part 11の主要な要件は，結果としてのユーザ要件と相互に関連する（表4）。明らかに，いくつかの要件は全く変化していない。

システムアクセスは権限を有する者に**限定されなければならず**，システムは適切な場所で権限チェックを実行する必要がある。テクニカルコントロールは「なりすまし」の防止を保証する必要がある。現代のシステムでは，これらの制御は会社のセキュリティポリシーと一致したセキュリティメカニズムを通して根本的なオペレーティングシステムによって実施され，一般的なIT業務でCDSへのアクセス管理を容易に一本化することができる。

デバイスチェックは，重要な記録の信頼性と確実性を保証するための**主要なメカニズム**であり続ける。レベル4 メカニズム[5, 15, 16]は効果的かつ効率的にこの要件を実行する（「レベル4 コントロールの重要性」に関するサイドバーを参照）。

結果のレビューと承認のためのステップなどの許可された一連のステップを実行するために，**今でも稼動中のチェックが要求される。**

電子署名の要件は変化しなかった。会社が電子署名と一緒に電子記録を使用している場合，クローズドまたはオープンシステムにおけるそのような署名については，Part 11によって強制されるテクニカルコントロールが2003年2月20日以前と同様に適用される。

これらの話題をカバーする有益な議論が，これらの要件を実行するためのPDAとISPEの21 CFR Part 11適用ガイドの「Appendix 4: Key Areas for Guidance, Part 2（付録4：ガイダンスの主要領域，第2部）」に記載されている[17]。

表4. 適合システムでの使用が必要とされるテクニカルコントロールおよび結果としてのユーザ要件の例

必要なテクニカルコントロール	結果としてのユーザ要件
・システムアクセスを承認された個人に制限すること	・ログインの実施 ・セキュリティポリシー ・パスワードポリシー ・タイムアウト
・権限チェックの使用	・構成可能なユーザ機能
・デバイスチェックの使用	・レベル4 機器コントロール[a] ・機器ログブック ・ネットワーク監視 ・アーリーメンテナンスフィードバック
・稼動中システムチェックの使用	・データシステムメソッドの一部としての計算やカスタム計算の実行（別のプログラムに手動で結果を転写しない） ・結果レビュープロセスの施行（アナリストレビュー，ピアレビュー，およびQA承認）
・電子署名に関連する要件	・重要業務に対する電子署名 ・電子レビューと結果の棄却または承認

a 参考文献6を参照。

信頼できる確実な記録

DAが公表したPart 11の再検討があっても，施行の焦点はPart 11の対象となる記録に関するプレディケートルール要件である。このカテゴリに分類される記録には，信頼性と確実性が必要になる。したがって，主要なテクニカルコントロールが適切な職員研修，文書化，および変更管理と共に，アクセスセキュリティ，稼動中のシステムとデバイスのチェック，オープンシステムコントロール，および電子署名に必要である。NDS，CDS，LIMS，またはERPシステムで管理される記録は，特に製品品質に与えるリスクポテンシャルが高い場合，Part 11とプレディケートルールの対象となる。

したがって，21 CFR Part 11が消えることはない。言い換えるならば，我々が以前にBioPharmの論文で述べたように「電子記録は定着している」[16]。Part 11の対象範囲は狭められた。そして，Part 11の強制が必要であるかどうかに関する決定は，現在では，記録が製品品質と会社の文書化された作業規範に作用するかもしれないリスクに基づくであろう。

レベル4コントロールの重要性

規制当局は，例えば，生データの取得に使用される分析装置の機器パラメータに関する文書化された証拠について，完成した製剤をテストする製薬品質管理ラボに質問するであろうか？

我々の観点では，製品出荷の前に仕様に対する完成した製剤をテストするQA/QCなどのような「規制された活動」を実行するためにラボは電子生データに頼っているので，答えは「はい」である！任意の結果が，分析で使用される機器コントロールパラメータの適切な文書化のないまま，定義された手順やモノグラフによって生成されたことを立証することは非常に難しい。

21 CFR Part 11のオリジナルの精神における信頼できる確実な結果を保証するために，電子的にメタデータ（機器のコントロールパラメータを含む）を管理することは重要である。このことはまた，製品品質に悪影響を及ぼす人工的なリスクも低減する。

レベル4機器コントロールは機器の識別や構成情報を自動追跡するために高度のメカニズムを使用しており，これらのコントロールはアーリーメンテナンスフィードバック（EMF）などの警告メカニズム実現のための前提条件である。我々は以前に，機器コントロールとEMFのレベルの詳細について議論した[2, 15]。機器とシステムコントローラとの間の通信が確実で信頼できる場合に限って，分析機器が生成する電子記録は確実で信頼できる。信頼できかつ追跡可能なレベル4機器コントロールが，新しいCGMPイニシアチブと新しいPart 11ドラフトガイダンスにおいても対象となっている電子生データ，メタデータ，および結果の正確さに対する適切で重要な手段であり続けると，我々は確信している。

参考文献

(1) FDA, "Code of Federal Regulations, Title 21 Food and Drugs, Part 11 Electronic Records; Electronic Signatures: Final Rule," Federal Register 62(54), 13429-13466 (20 March 1997).
(2) Office of Regulatory Affairs, "Enforcement Policy: 21 CFR Part 11; Electronic Records; Electronic Signatures (CPG 7153.17), Section 160.850, Compliance Policy Guide (FDA, Rockville, MD, 13 May 1999).
(3) FDA, "Withdrawal of Draft Guidance for Industry on Electronic Records; Electronic Signatures, Electronic Copies of Electronic Records," Federal Register 68(23), 5645 (4 February 2003).
(4) FDA, "Draft Guidance for Industry on 'Part 11, Electronic Records, Electronic Signatures - Scope and Application;' Availability of Draft Guidance and Withdrawal of Draft Part 11 Guidance Documents and a Compliance Policy Guide," Federal Register 68(37), 8775-8776 (25 February 2003). Available at www.fda.gov/cber/gdlns/prt11elect.htm.
(5) Winter, W. and Huber, L., "Instrument Control in Pharmaceutical Laboratories - Compliance with 21 CFR Part 11, Part I," Pharm. Technol. Eur. 15(3) suppl., 40-45 (2003).
(6) Office of the Commissioner, "Pharmaceutical CGMPs for the 21st Century: A Risk-Based Approach (FDA, Rockville, MD, August 2002). Available at www. fda.gov/oc/guidance/gmp.html.
(7) FDA, "Draft Guidance for Industry; Electronic Records; Electronic Signatures, Glossary of Terms; Availability," Federal Register 66(185), 48886-48887 (24 September 2001). Available at www.fda.gov/ cber/gdlns/essigglos.htm.
(8) FDA, "Draft Guidance for Industry; Electronic Records; Electronic Signatures, Validation; Availability," Federal Register 66(185), 48886 (24 September 2001). Available at www.fda.gov/cber/gdlns/ esigvalid.htm.
(9) FDA, "Draft Guidance for Industry; Electronic Records; Electronic Signatures, Time Stamps; Availability," Federal Register 67(54), 12999 (20 March 2002). Available at www.fda.gov/cber/gdlns/esigtime.htm.
(10) FDA, "Draft Guidance for Industry; Electronic Records; Electronic Signatures, Maintenance of Electronic Records; Availability," Federal Register 67(172), 56848-56849 (5 September 2002). Available at www.fda.gov/cber/gdlns/esigmaint.htm.
(11) FDA, "Draft Guidance for Industry; Electronic Records; Electronic Signatures, Electronic Copies of Electronic Records; Availability," Federal Register 67(218), 68674-68675 (12 November 2002). Available at www.fda.gov/cber/gdlns/esigcopies.htm.
(12) PDA, "Good Electronic Records Management (GERM)," Good Practice and Compliance for Electronic Records and Signatures, Part 1 (ISPE,Tampa, FL, September 2002).
(13) GAMP Forum, "Management Appendices, M3: Guideline for Risk Assessment," The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture (ISPE, Tampa, FL, October 2001).
(14) Huber, L., Validation of Computerized Analytical and Networked Systems (Interpharm Press, Inc., Buffalo Grove, IL, 2002).
(15) Huber, L. and Winter, W., "Implementing 21 CFR Part 11 in Analytical Laboratories, Part 5: The Importance of Instrument Control and Data Acquisition," BioPharm 13(9), 52-56 (2000). Agilent publication number 5988-0946EN.
(16) Winter, W., "Electronic Records Are Here to Stay," BioPharm Eur. Special issue of Pharm. Technol. Eur., 29-31, (September 2002).
(17) PDA, "Complying with 21 CFR Part 11: Electronic Records and Electronic Signatures," Good Practice and Compliance for Electronic Records and Signatures, Part 2 (ISPE, Tampa, FL, October 2001).
(18) European Commission, "Annex 13: Manufacture of Investigational Medicinal Products," Good Manufacturing Practices, Vol. 4 (Enterprise Directorate-General, Brussels, Belgium, November 2001).

著者

Wolfgang Winterはネットワークデータシステムのシニアプロダクトマネージャです。Ludwig Huberは Agilent TechnologiesのHPLCと製薬ビジネスの世界的なプロダクトマーケティングマネージャです。
Agilent Technologies GmbH, PO Box 1280
D-76337, Waldbronn, Germany,
+49.7243.602.454
fax +49.7243.602.501
wolfgang_winter@agilent.com
www.agilent.com

June 15, 2003
5988-9718JAJP

Agilent Technologies

June 30, 2003
5988-9754JAJP

横河アナリティカル システムズ株式会社

●カストマコンタクトセンター ☎ 0120-477-111
1）システム、製品および部品に関するご相談窓口
2）製品の操作、アプリケーションの問合せおよび故障時の連絡窓口
3）ユーザートレーニングの申し込み窓口

ホームページ　http://www.agilent.co.jp/chem/yan