

# 21 CFR Part 11 および Annex 11 コンプライアンスのサポート：Agilent Automated Compliance Engine (ACE)

本書はネットワークインストールされた ACE 3.13 以上が対象

## 概要

米国 FDA が定める連邦規則 (CFR) 第 21 条第 11 章 (21 CFR Part 11) と、それに相当する欧州連合の Eudralex 第 4 章附属書 11 (Annex 11) では、規制対象の製薬会社で電子記録および電子署名を使用する際の要件を規定しています。

21 CFR Part 11 は 1997 年に制定され、1999 年より施行されています。これらのガイドラインの目的は、該当するすべての電子記録について、ALCOA の原則 (責任の所在が明確であること、判読できること、同時であること、原本であることおよび正確であること) を確保し、その完全性を維持することにあります。

このホワイトペーパーは、これらの規制の遵守が求められる、ネットワークインストールされた Agilent ACE を使用しているお客様を対象としています。ACE ソフトウェアプラットフォームは、アジレント認定サービスエンジニアが、クロマトグラフィーシステムなどのラボ機器の機器適格性評価サービスを提供するためのツールです。ACE バージョン 3.13 で導入された機能により、お客様が適格性評価データとレポートを管理できるようになりました。ACE が提供する機能を適切に使用してコンプライアンスを遵守することは、お客様の組織の責任です。さらに、ユーザーには、関連する非技術的要件を満たすために、手順管理、すなわち標準操作手順書 (SOP) を策定することが求められます。例えば、内部監査プログラムなどの管理を確立して、システムオペレータに確実に SOP に従うよう教育する必要があります。

付録 1 では、21 CFR Part 11 の各項および EU Annex 11 の関連条項の要件を満たすうえで役に立つ ACE の機能について詳しく説明します。この説明では、機器のハードウェアおよびソフトウェアを含むシステムアクセスが、システムに保持されている電子記録に対する責任を担うスタッフによって管理されていることを前提としています。すなわち、システムが、21 CFR Part 11.3 (b) (4) で規定される「クローズドシステム」として設計されているものとします。

## 21 CFR Part 11

21 CFR Part 11 では、規制対象のラボの運営における次の3つの要素について規定しています。

- 電子記録のセキュリティ
- 作業の責任の所在の明確化
- 電子署名（使用する場合）

### セキュリティ

セキュリティは、「適切な者が適切な情報に対して適切なアクセス権を持つこと」と言い換えることができます。規制対象の組織は、システムユーザーの本人確認を行い、かつトレーニングを受けた権限のある個人にシステムアクセスを限定できなければなりません (11.10 (d)、(i)、および (g)、11.100 (b))<sup>1</sup>。ラボのスタッフは、職務に応じてさまざまな責任を担っていることから、データアクセスを分け、特定のユーザーが特定のデータセットに対して適したアクセス権を持ち、また場合によっては、他のデータセットへ別のアクセス権を持つように定義する必要があります。

### 作業の責任の所在の明確化

作業の責任の所在を明確にすること、とは、作業を「誰が、何を、いつ、どこで、どんな理由で」行ったのかを文書化することです。自動化された監査証跡では、ユーザーの操作が個別に記録され、ラボのスタッフと、そのスタッフが実行した作業が関連付けられます。監査証跡をもとに、スタッフおよび査察官は、電子記録の完全な履歴を再構成することができます。

- **誰が：**記録を作成、変更、または削除する特定の操作を行った者を明確に示します。
- **何を：**実行された操作を示します。該当する場合は、記録に保持されている古い値と新しい値を含みます。

- **いつ：**操作が実行された日時を明確に示します。
- **どこで：**影響を受けた記録を明確に示します。
- **理由：**規制対象の記録に対する変更の理由を説明します。一貫性を保つため、また監査証跡の検索および並べ替えを可能にするために、通常、理由は事前に定義されたリストから選択します。

### 電子署名

21 CFR Part 11 では、電子署名の使用を義務付けていませんが、使用する場合の実装の規定を定めています。この場合、システムでは電子署名について次の条件を満たす必要があります。

- 取り消しできない方法で該当する記録に関連付けられていること
- 署名者の氏名、および署名日時のほか、署名の意味（レビュー、承認、責任、作成者など）または理由が示されていること
- 署名された記録を表示または印刷するたびに表記されること

「セキュリティ原則としての職務の分離の主な目的は、不正行為と過失を防ぐことにあります。この目的は職務と関連する権限を複数のユーザーに分散させることにより達成できます。」

- Botha, Eloff, IBM Systems Journal<sup>1</sup>

## 付録 1: ACE による、米国 FDA 21 CFR Part 11 および関連する各国規制で規定されている要件の遵守

### 付録 1 の表に関する注記

**1 列目：**表では、21 CFR Part 11 の要件を米国 FDA の参考文献 [2] に記載されている順に記載します<sup>2</sup>。また、Part 11 の各条項の後に、それに関連する EU Annex 11<sup>3</sup> などの要件を示します。

**2 列目：**完全性を保つために、2 列目には、21 CFR Part 11 およびその他の関連する各国規制のすべての要件を示します。表中の「システム」は、データの取り込みおよび解析などの処理に使用される分析システムを指します。

多くの要件は、技術的管理（ソフトウェア機能）または手順管理（SOP）のいずれかにより満たされます。技術的管理とは、ソフトウェア、すなわちソフトウェア供給元により提供される管理機能です。また、手順管理とは、ユーザーの責任において実施する必要のある管理措置です。太字で記載されている 21 CFR Part 11 の要件は、技術的管理によって満たされる要件です。その他の各国要件は標準フォントで示しています。

**3 列目：**一部の要件には、技術的管理と手順管理の両方が関連しています。3 列目には、各要件の責任の所在を示します。「S」は分析システムの供給元を表し、「U」はユーザーを表します。

**4 列目：**4 列目には、ACE で提供される技術的管理（ソフトウェア機能）により要件を満たすことができるかどうかを「可」または「不可」で示します。

**5 列目：**5 列目では、ACE の技術的管理（ソフトウェア機能）により、規制要件をいかに満たすことができるかを説明します。また、関連する場合は、ユーザーに対するその他の推奨事項も示します。

## 1.バリデーション

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Part 11 11.10 (a)	1.1.正確性、信頼性、意図した性能の一貫性、および無効な記録や変更された記録を識別する機能を保証するために、システムのバリデーションが実施されていますか。	S、U	可	アジレント・テクノロジーでは、正確性、信頼性、および一貫した性能を評価することにより、ACE の性能を幅広く検証しています。しかし、ユーザーは、規制要件やその使用目的に従って、コンプライアンスを確保することも求められます。
Annex 11	1.2.インフラストラクチャは適格性が評価されていますか。	S	可	インフラストラクチャは、システム適格性評価の一部として適格性が評価されています。アジレントは、これを据付サービスの一部として提供します。

## 2.記録の正確なコピーと安全な保管および検索

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Part 11 11.10 (b)	2.1.システムは、FDA による調査、審査に適した、人間が判読できる形式と電子形式の両方で記録の正確かつ完全なコピーを生成できますか。	S	可	すべてのレポート記録と関連情報（サポート証明書やトレーニングデータなど）は、ロックされた .pdf 形式で表示されます。 コピーは、印刷可能な形式と電子形式の両方において、完全かつ正確で、人間が判読できる形式になっています。
Annex 11	2.2.電子的に保管された電子記録は、明確に印刷されたコピーが得られますか。	S	可	すべてのレポート記録と関連情報（サポート証明書やトレーニングデータなど）は、ロックされた .pdf 形式で表示されます。 コピーは、印刷可能な形式と電子形式の両方において、完全かつ正確で、人間が判読できる形式になっています。
Part 11 11.10 (c)	2.4.システムでは、保管期間を通して正確かつ容易に検索できるように記録が保護されていますか。	S、U	可	記録は保護されており、検索できます。
Annex 11	2.5.アーカイブ期間中にデータのアクセスが容易か、判読できるか、および完全であるかがチェックされていますか。	U	—	ACE には適用されません。これは、お客様の責任です。
Annex 11	2.6.システム（コンピュータ機器やプログラムなど）に対して該当する変更が行われた場合、そのデータを検索できることが確認され、テストされていますか。	U	可	ACE には適用されません。これは、お客様の責任です。
Annex 11	2.7.データは、物理的および電子的手段によって損傷から保護されていますか。	U	可	ACE には適用されません。これは、お客様の責任です。
Annex 11	2.8.システムでは、すべての関連データを定期的にバックアップすることが可能ですか。	U	可	システムは、定期的なバックアップに対応しています。データをバックアップするのは、ユーザーの責任です。
Annex 11	2.9.バックアップデータの完全性と正確性、およびデータを復元する機能が検証中にチェックされ、定期的にモニタリングされていますか。	U	可	ACE では、復元の際にアーカイブデータを検索できます。

## 3.システム、機能、およびデータに対する権限に基づくアクセス

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Part 11 11.10 (d)	3.1.システムへのアクセスは、権限のある者に限定されていますか。	S、U	可	ACE ソフトウェアアクセスは、トレーニングを受けて認定されたオペレータにのみ割り当てられたパスワード権限によるログインに限定されています。
Part 11 11.10 (d)	3.2.各ユーザーは、そのユーザー自身のユーザー ID とパスワードなどによって明確に識別されますか。	S、U	可	各ユーザーは、一意の ID とパスワードの組み合わせによって識別されます。システムにアクセスするには、その両方の情報を入力する必要があります。

## 4. 電子監査証跡

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Part 11 11.10 (e)	4.1.オペレータがログオンや、電子記録の作成、変更、または削除操作を実行した日時が個別に記録され、コンピュータにより生成されるタイムスタンプ付きの安全な監査証跡はありますか。	S	可	ユーザーによるすべての操作は、コンピュータにより生成されるタイムスタンプ付きの安全な監査証跡に記録されます。
FDA GLP	4.2.監査証跡には、誰がどのような変更をいつどのような理由で行ったかが記録されますか。	S	可	監査証跡には、ユーザー名、日時、トランザクションの日付、トランザクションの種類、実行された操作、および実行された理由が記録されます。
Annex 11	4.3.システムは、オリジナルの値から電子記録が変更されたかどうかを示す印字物を生成できますか。	S	可	はい。ACE は、電子記録が変更されたかどうかを示すことができます。
Annex 11	4.7.監査証跡は、定期的なレビューのために一般にわかりやすい形式で利用できますか。	S	可	監査証跡は、ACE から査察官がアクセスできるよう設定されており、容易に利用できます。
	4.8.監査証跡の内容は、情報の現実的かつ意味のあるレビューを行えるように、関連する操作のみが記録されるように設定できますか。	U	不可	監査証跡の設定はできませんが、レビューに関連する意味のある操作を記録しています。
Part 11 11.10 (e)	4.9.記録が変更された場合、以前に記録された情報はそのまま残されますか。	S	可	変更は元の記録の新しいリビジョンとして保存され、元の記録はそのまま残されます。
Part 11 11.10 (e)	4.10.監査証跡は、少なくとも電子記録に求められる期間において維持されますか。	S	可	監査証跡情報は、永久的な電子記録内に保存され、保持されます。
Part 11 11.10 (e)	4.11.監査証跡は、FDA が審査およびコピーできる状態にありますか。	S	可	監査証跡は、審査および印刷が可能です。
Annex 11	4.12.電子形式で保存されている電子記録（電子監査証跡など）は、印刷された明確なコピーが得られますか。	S	可	監査証跡は、審査および印刷が可能です。

## 5. 動作およびデバイスの確認

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Part 11 11.10 (f)	5.1.必要に応じて、認められた順序に従って手順およびイベントが実行されるようにするための運用システムチェックは設けられていますか。	S	可	作業指示書とトレーニングにより、ACE におけるイベントの順序を規定しています。
Part 11 11.10 (g)	5.2.権限のある個人のみがシステムの使用、記録への電子署名、運用システムまたはコンピュータシステムの入出力デバイスへのアクセス、記録の改変、または操作を行えるようにするための権限の確認は行われていますか。	S	可	権限のある個人のみが、ログインとパスワードを使用して ACE にアクセスすることができます。記録に署名する際にも、ログインとパスワード資格情報が必要です。
	5.3.システムは、データ入力、変更、確認、または削除を行ったオペレータを日時とともに記録するように設計されていますか。	S	可	オペレータは、日時を含め、入力および変更されたデータを記録している監査証跡に記録されます。
Part 11 11.10 (h)	5.4.システムでは、適宜、データ入力または操作の妥当性を判断するためのデバイスチェックを利用できますか。	S	可	データの妥当性を保証するために、データインテグリティがチェックされます。
Part 11 11.10 (i)	5.5.電子記録/署名システムを開発、メンテナンス、または使用する者が、その者に割り当てられた職務を遂行するための教育およびトレーニングを受け、経験を積んでいることを証明する文書がありますか。	S	可	システムユーザーのトレーニングファイルが、機器適格性評価レポートに添付されています。
Part 11 11.10 (j)	5.6.記録および署名の偽造を阻止するために、個人が各自で行った電子署名のもとで実施した操作に対して説明義務と責任を負うことを明文化したものが策定されていますか。	S	可	アジレント企業倫理・行動規範に関するトレーニングは、電子署名などの操作に対する個人の責任と説明責任を網羅しているポリシーです。
	5.7.従業員は、この手順に関するトレーニングを受けていますか。	S	可	このトレーニングは必須であり、その証拠は Agilent 学習管理システム (LMS) に文書化されています。
Part 11 11.10 (k)	5.8.システムの運用と保守に関する文書の配布、アクセス、および使用に対する適切な管理など、システム文書について適切に管理していますか。	S	可	システム文書については、管理措置を実施しています。
Part 11 11.10 (j)	5.9.システム関連の文書の作成および改訂を時系列で文書化した監査証跡を維持するための改訂および変更の管理手順は確立されていますか。	S	可	改訂と変更の手順については、管理措置を実施しています。

## 6. データインテグリティ、日時の正確性

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Annex 11	6.1.他のシステムとデータを電子的に交換するコンピュータ化システムには、正確で安全に入力され、データが処理されるように適切なチェックが組み込まれていますか。	S	可	データは、機器測定ソフトウェアと ACE 間で転送されます。これらのデータは、セキュアデータストア (SDS) により、複数の用途に使用されていないかどうかチェックされます。
Annex 11	6.2.データの正確性を確認するために追加でチェックする機能はありますか。このチェックは、他のオペレータまたは検証済みの電子的手段で行うことができます。	S	可	転送後、エンジニアがデータを確認します。

## 7. オープンシステムの管理 (オープンシステムにのみ適用)

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Part 11 11.30	7.1.電子記録の真正性および完全性、さらに該当する場合は、機密性を作成から受領まで確保するよう考案された手順および管理措置が設けられていますか。	U	—	ACE はクローズドシステムであり、このカテゴリは適用されません。
Part 11 11.30	7.2.状況に応じて必要な場合に記録の真正性、完全性、および機密性を確保するために、文書の暗号化や適切なデジタル署名規格の使用などの追加措置が講じられていますか。	U	—	ACE はクローズドシステムであり、このカテゴリは適用されません。

## 8. 電子署名 – 署名の明示および署名/記録の関連付け

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Annex 11	8.1.電子署名を使用する場合、企業の範囲内で電子署名と手書き署名では同じ影響力がありますか。 電子署名は、該当する記録に永久的に関連付けられていますか。 電子署名に署名日時が含まれていますか。	S、U	可	電子署名は、レポートに永久的に関連付けられており、日時スタンプが付けられています。
Part 11 11.50 (a)	8.2.署名した電子記録は、次に明記する署名に関する情報を含んでいますか。 – 署名者の印字氏名 – 署名が行われた日時 – 署名に関連付けられた意味 (レビュー、承認、責任、作成者など)	S、U	可	署名されたレポートには、氏名、日時、意味 (作成者) が記載されています。
Part 11 11.50 (b)	8.3.本項の (a) (1)、(a) (2)、および (a) (3) で規定されている項目は、電子記録と同じ管理の対象となりますか。これらの項目は、人間が判読できる形式の電子記録 (電子的な表示や印字物など) の一部として含まれていますか。	S	可	電子署名されたレポートは、ロックされた電子記録であり、人間が判読できる形式です。
Part 11 11.70	8.4.電子記録を改ざんする目的で署名を通常の方法で削除、コピー、または転送できないように、電子署名および手書き署名は、該当する電子記録に関連付けられていますか。	S	可	電子署名は記録に関連付けられています。
Part 11 序文	8.5.一定期間の間に入力および操作がまったく行われなかった場合、ユーザーを「ログアウト」する、自動ログアウト機能が設けられていますか。	S	可	時間ベースのロックアウト機能が設けられており、一定期間の間に入力または操作が行われない場合、ユーザーをログアウトします。

## 9. 電子署名の一般要件と署名の構成要素および管理

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Part 11 11.100 (a)	9.1. 電子署名は各担当者に一意であり、他人が再使用したり、他人に再割り当てされることはありませんか。	S、U	可	電子署名は各担当者に一意であり、他人が再使用したり、他人に再割り当てしたりすることはできません。
Part 11 11.100 (b)	9.2. 組織は、個人の電子署名または電子署名の構成要素を設定、割り当て、認証、あるいは認可する場合、事前にその個人の本人確認を行っていますか。	S	可	電子署名が設定される前に、本人確認が実施されます。
Part 11 11.100 (c)	9.3. 電子署名を使用する者は、その使用前または使用時に、1997 年 8 月 20 日以降に使用されているシステム内の電子署名が従来の手書き署名と同等の法的拘束力を持つよう意図されたものであることを FDA に対して証明していますか。 9.4. 電子署名を使用する者は、FDA の要請に応じて、特定の電子署名が署名者の手書き署名と同等の法的拘束力を持つことを示す証明書または宣誓書を追加で提出していますか。	S	可	トレーニングが完了すると、認定されます。
Part 11 11.200 (a) (1)	9.5. バイオメトリックスによらない電子署名では、識別コードとパスワードなど、少なくとも 2 つの識別構成要素が使用されていますか。	S	可	ログインとパスワードが必要です。
Part 11 11.200 (a) (1) (i)	9.6. 制御されたシステムのアクセスの連続的な期間内にユーザーが一連の署名を行わない場合、それぞれの署名の実行にはすべての電子署名コンポーネントが必要ですか。	S	—	実行されるすべての署名において、常に完全な署名が必要になります。
Part 11 11.200 (a) (1) (i)	9.7. 制御された 1 回のシステムアクセスの持続中、ある個人が一連の署名を行う場合、それ以降の署名には、当該個人しか実行できず、かつその個人のみが使用するものとして考案された電子署名構成要素が少なくとも 1 つ使用されますか。	S	—	実行されるすべての署名において、常に完全な署名が必要になります。
Part 11 11.200 (a) (1) (ii)	9.8. 制御されたシステムのアクセスの連続的な期間内にユーザーが一連の署名を行わない場合、それぞれの署名の実行にはすべての電子署名コンポーネントが必要ですか。	S	—	実行されるすべての署名において、常に完全な署名が必要になります。
Part 11 11.200 (a) (2)	9.9. バイオメトリックスによらない電子署名が、所有者本人のみによって使用されるようにするための管理措置が実施されていますか。	S	可	手順管理として、トレーニングが実施されます。
Part 11 11.200 (a) (3)	9.10. 2 名以上の協力がなく、個人の電子署名の使用を所有者本人以外の者が試みることができないように、電子署名が管理され、運用されていますか。	S	可	個人の電子署名を使用する際には、2 名以上の協力が必要になります。
Part 11 11.200 (b)	9.11. バイオメトリックスに基づく電子署名は、所有者本人以外の者が使用できないように設計されていますか。	S	—	ACE では、バイオメトリックス認証はサポートされていません。

## 10. 識別コードとパスワードの管理

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Part 11 11.300 (a)	10.1.2 名の者が同一の識別コードとパスワードの組み合わせを持つことがないように、識別コードとパスワードの各組み合わせの一意性を維持するための管理措置が実施されていますか。	S	可	ログインとパスワードの組み合わせの一意性を保証するための管理措置が実施されています。
Part 11 11.300 (b)	10.2. 識別コードおよびパスワードの発行が定期的にチェック、取り消し、または見直されるようにするための管理措置が実施されていますか。(例えば、同一パスワードの長期使用などの事象に対する対策として)	S	可	ユーザーは、定期的にパスワードを変更する必要がある、パスワードをリセットする仕組みもあります。
Part 11 11.300 (c)	10.3. 識別コードやパスワード情報を保持または生成するトークン、カード、またはその他のデバイスが紛失、盗難、所在不明の場合、あるいはこれらのデバイスへの不正アクセスがある場合に、そのデバイスを電子的に無効にするための手順は設けられていますか。適切かつ厳密な管理を用いて、一時的または永久的な代替手段を発行する手順はありますか。	S	可	ユーザーは、5 回失敗するとログアウトされ、パスワードをリセットするには、ロック解除コードの発行を依頼する必要があります。
Part 11 11.300 (d)	10.4. パスワードまたは識別コード、あるいはその両方の不正使用を防止し、システムを不正に使用しようとする行為を検出してシステムセキュリティ部門と、必要であれば組織の経営陣に直ちに緊急報告するための保護措置は設けられていますか。	S	可	ユーザーは、5 回失敗するとログアウトされ、パスワードをリセットするには、ロック解除コードの発行を依頼する必要があります。
Part 11 11.300 (e)	10.5. 識別コードまたはパスワード情報を保持または生成するトークンやカードなどのデバイスが正しく機能し、不正に改変されていないことを確認するために、これらのデバイスを導入時および導入以降定期的にテストするための管理措置は設けられていますか。	S	—	この機能は、将来のリリースに向けて開発中です。

## 11. システムの開発とサポート

Part 11 およびその他	要件	S、U	可/不可	「可」の場合、具体的に Agilent ACE により要件がいかに満たされるか。 「不可」の場合、顧客に推奨される事柄。
Annex 11	11.1. ソフトウェアまたはシステムは、適切な品質管理システムに従って開発されましたか。	S	可	アジレントのソフトウェアは、ISO 認定の品質管理システム (QMS) の一部である、製品開発ライフサイクルの中で開発されています。
Part 11 11.10 (i)	11.5. ソフトウェアを開発してサポートする担当者は、トレーニングを受けていますか。	S	可	アジレントの開発およびサポート担当者は、QMS および製品開発ライフサイクルでトレーニングを受けています。

### 参考文献

- Botha, R. A.; Eloff, J. H. P. Separation of Duties for Access Control Enforcement in Workflow Environments. IBM Systems Journal – End-to-End Security **2001**, 40(3), 666–682.

- U.S. Food and Drug Administration. Code of Federal Regulations (CFR) Title 21. Title 21—Food and Drugs, Chapter I—Food and Drug Administration Department of Health and Human Services, Subchapter A—General. Part 11 Electronic Records; Electronics Signatures [Online] <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11> (accessed November 4, 2015).

- European Commission Health and Consumers Directorate, General. Public Health and Risk Assessment. Pharmaceuticals. EudraLex. The Rules Governing Medicinal Products in the European Union.
- Good Manufacturing Practice. Medicinal Products for Human and Veterinary Use. Annex 11. Computerised Systems. [Online] [https://health.ec.europa.eu/system/files/2016-11/annex11\\_01-2011\\_en\\_0.pdf](https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf) (accessed November 4, 2015).

ホームページ

[www.agilent.com/chem/jp](http://www.agilent.com/chem/jp)

カスタムコンタクトセンター

**0120-477-111**

**email\_japan@agilent.com**

本製品は一般的な実験用途での使用を想定しており、医薬品医療機器等法に基づく登録を行っていません。本文書に記載の情報、説明、製品仕様等は予告なしに変更されることがあります。

DE-000571

アジレント・テクノロジー株式会社

© Agilent Technologies, Inc. 2024

Printed in Japan, September 11, 2024

5994-7773JAJP