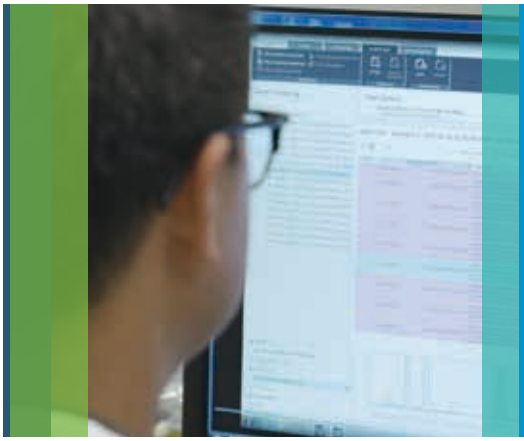

規制当局による監査: 監査を招く主な要因を回避するための戦略

Agilent OpenLab

ビジネスのグローバル化が進展するなか、規制当局はデータインテグリティと複眼的思考に対する取り組みを強めています。規制当局による監査を招く主な要因を回避し、規制環境においてデータインテグリティを保持するための戦略についてご紹介します。

規制当局による監査を招く主な要因にはどんなものがありますか？

- **トレーサビリティと透明性が不十分**
  規制当局は企業に対し、紙ベースのシステムやハイブリッドシステムから電子システムに移行して、データの完全なトレーサビリティを実現するよう求めています。
- **データ管理が不十分**
  規制当局は企業に対し、データのライフサイクル全体にわたってリスクに基づいた包括的なアプローチをとることを求めており、企業は重要なデータポイントを特定するために、すべてのデータソースにわたって適切なリスク分析を行う必要があります。
- **従前規則や 21 CFR Part 11 の要件に不適合**
  データには、ALCOA+ の要件、すなわち帰属性 (Attributable)、判読性 (Legible)、同時性 (Contemporaneous)、原本性 (Original)、正確性 (Accurate)、完全性 (Complete)、一貫性 (Consistent)、永続性 (Enduring)、利用可能性 (Available) が求められます。

Agilent
Trusted Answers

電子データの堅牢な確認プロセスには何を含めるべきですか？

多くの企業では、データのレビューが監査証跡とレポートに限定されているため、規制当局による監査の基準を満たしていません。電子データの確認プロセスには、以下のものを含める必要があります。

- ソースとなる電子データに関連するメタデータと監査証跡
- サーバーのアクティビティログ
- オペレーティングシステム固有のアクティビティログ
- アプリケーション固有のアクティビティログ
- 機器のエラーログ
- IT チケット (変更または削除されたデータについてバックエンドデータベースの変更を確認するため)
- 結果セット

データセキュリティを確保するにはどうすればいいでしょうか？

規制当局は企業に対し、防止と検出の仕組みを確立してデータの保護と管理を確実にすることを求めています。下記について確認してください。

- ソースとなる電子データは、管理された環境で保護されていますか？
- ソースとなる電子データをレビューしていますか？
- ソースとなる電子データには、意味のあるメタデータと監査証跡が含まれていますか？
- 業務の分離が適切に行われていますか？
- 目的の用途ごとに、発注元および受託製造業者によってシステムのバリデーションが行われていますか？

規制当局の監査における大きな変化と、それが分析ラボに与える影響について詳しくは、次のオンデマンドウェビナーをご覧ください。
「大きく変わった規制機関の査察への対応」
https://www.chem-agilent.com/form_webinar/?name=OpenLAB21

データの一貫性、正確性、セキュリティの確保に関する資料はこちらでご覧いただけます。
https://www.chem-agilent.com/contents.php?id=1004433

ホームページ
www.agilent.com/chem/jp

カストマコンタクトセンタ
0120-477-111
email_japan@agilent.com

アジレント・テクノロジー株式会社

Printed in Japan, October 1, 2018
5994-0295JAJP

Agilent
Trusted Answers