JBFシンポジウム　JSQA発表

OECD GLPのデータインテグリティガイダンスへの対応

－DIリスクマネジメントによる具体的事例検討－

一般社団法人日本QA研究会
GLP部会第3分科会
下川　智春

前回：JSQAからの報告（2025年3月）

第29回GLP研修会（2024年10月）

Data Integrity（DI）への更なる対応のお願い

- 2021年にOECDガイダンス文書No.22（GLP環境下におけるDI）が発出されて以降、その求められる事項に対しては、周知期間が必要だったため、これまで留意事項に留めてきた。
- 一定の周知期間を経たので、今後はより踏み込んだ対応として、当該文書で求められている事項のうち、下記4点について優先的に具体的な取り組みを進めることとしたい。
- 具体的な内容及び適用時期については、今後、業界団体やその他関係者の意見を聴きつつ検討するが、各施設においてもどのように対応すべきか検討を始めてほしい。

1. **DI対応（特に監査証跡）した機器への移行**
2. **オリジナル（特に動的）データの生データ化**
3. **秤量値等の自動記録化**
4. **ブランクワークシートの管理**

前回のJBFシンポジウム（2025年3月）

- アンケート調査による実装状況の調査
- 2回にわたって、重要項目の要求レベルについて意見交換

業界4団体の検討結果及びPMDAコメントについて報告

第30回GLP研修会（2025年10月）

第29回GLP研修会で示したDIに係る重点4項目

1. DI対応（特に監査証跡）した機器への移行
2. オリジナル（特に動的）データの生データ化
3. 秤量値等の自動記録化
4. ブランクワークシートの管理

項目1と2は双方とも「電子データの取り扱い」に関する事項であり、纏めた方が理解がしやすいと考えた

1. DI対応機器への移行（監査証跡・オリジナルデータの保存）
2. 秤量値等の自動記録化
3. ブランクワークシートの管理

以降のスライドでは、重点3項目として、各項目を説明する

DI対応に際してのリスク評価

（DIガイダンス： 5. Principle actions to ensure data integrity ）

2. TFM is expected to implement a fully documented system with supporting rationale that provides an acceptable state of control based on the data integrity risk. **An example of a suitable approach is to perform a data integrity risk assessment** where the processes that produce, process and/or store data are mapped out and each of the formats and their controls are identified and the data criticality, inherent risks and appropriate mitigations documented.

DI対応に際しては、各データプロセスに対して、例えば、以下のような点についてリスク評価を行うことが重要である：

- データライフサイクルを通じて、DIを脅かすリスクは何か、それがどの段階（プロセス）に存在するか？
- 特定されたリスクは、測定機器やコンピュータシステムに付属する機能（メタデータなど）を利用すれば、許容できるか？
- そのデータは試験の再構築性に重要か？

第30回GLP研修会ではDIに係る項目が3項目になり
業界団体の意見も踏まえた**より具体的な内容**となっている

前回：JSQAからの報告（2025年3月）

今後の対応のポイント

キーワード：リスク分析

➢リスク分析に基づいた対応方針の策定

- 各施設の業務内容、DI対応状況は様々なことは承知している
- 対応の優先順位や今後の対応方針など各施設でリスク分析を実施して定めることが必要（→リスク分析結果を用いた説明）

➢生データの電子化

- データが生成してから廃棄するまでのライフサイクル全般の管理が必要（ALCOA+）
- 電子で取得したデータ（オリジナルデータ）は静的でも保存が必要

➢生データの電子化に向けた新たな運用手順の策定

- DI対応機器の導入だけでなく、電子データの管理方法（バックアップ、アーカイブ含む）や監査証跡のレビュー手順など新たな運用方法が必要
- DI非対応機器を継続使用する場合、ハイブリッドによる代替方法は受け入れ可能だが人手を介する作業は完全でない（→リスク分析結果を用いた説明）

JSQAの取組：DIリスクマネジメント

各施設の状況をヒアリング

- PMDAの求めるDIリスク分析の手法がイメージできず困っている
- いろいろな機器があって、どこから手を付けて良いか分からない
- リスク評価の具体例を示してもらえると、参考になる

安全、品質に関するリスク分析の考え方や手順の情報はあるが
DIに関するリスク分析の方法、具体的事例に関する情報がなく困っている

⇒ JSQAでは、今回のテーマ
「OECD GLPのデータインテグリティガイダンスへの対応
－DIリスクマネジメントによる具体的事例検討－」
について活動した

本発表の目的とアプローチ

本発表の目的

PMDAが示すDIに係る重点3項目のうち、「DI対応機器への移行（監査証跡・オリジナルデータの保存）」に関して、モデルケースを通じてDIリスクマネジメントの手法を紹介する

アプローチ

- OECD GLP No.22（DIガイダンス）をベースに、システム面からアプローチ
  対象システムの仕様／運用の把握 ⇒ハザード特定
- FMEAモデルによるリスクアセスメント
  ハザードの見える化、優先度付け、低減策の具体化

本日の内容

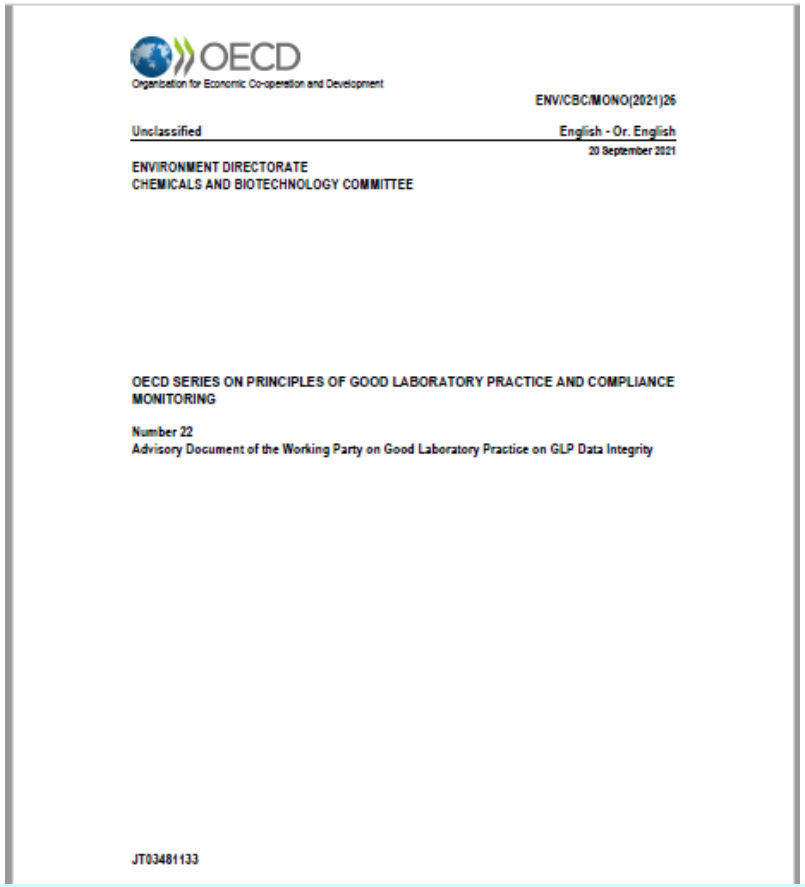
１．DI関連チェックシート

２．DIリスクマネジメントによる具体的事例検討

３．まとめ

１．DI関連チェックシート

OECD GLP データインテグリティガイダンス



OECD
Organisation for Economic Co-operation and Development

ENV/CBC/MONO(2021)26

Unclassified — English - Or. English
20 September 2021

ENVIRONMENT DIRECTORATE
CHEMICALS AND BIOTECHNOLOGY COMMITTEE

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

Number 22
Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity

JT03481133

GLP 原則及び適合性モニタリングに関する
OECD シリーズ No. 22
GLPデータインテグリティに関するGLP作業部会の
アドバイザリー文書
2021年9月20日　最終版発出

GLP試験施設で遵守すべきDIに関する基本的な考え方が示されたガイダンス

↓ 上記の要件を点検観点として反映

JSQAでは、自施設の分析機器（システム）における
DI対応状況を自己点検するための『DI関連チェック
シート』を作成し、会員向けに活用を推奨した。

【参考】JSQAウェブサイト-「研究成果」-「公開成果物」-「GLP部会」にてOECD GLP文書No.22の「英文・和訳対比表」を公開

DI関連チェックシート（抜粋）

DI関連チェックシート

対象システム：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

チェック日：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

チェック者：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

DIガイダンス（OECD GLP No.22）を踏まえた要求仕様		DIガイダンス根拠条項	適合	不適合	適用外
データ					
1	シーケンス、メソッドおよび結果が、日時付きで印刷可能であること。	3.1，3.2，6.14	□	□	□
2	データはリレーショナルデータベースで一元管理されることが望ましく、既存データが上書きされない構造であること。	3.2，6.11	□	□	□
3	結果はメタデータとともに、完全性を保持した形で保存されること。	6.3	□	□	□
監査証跡					
4	監査証跡の機能を有すること。	6.1，6.13，7.1，7.2	□	□	□
5	監査証跡の機能により、操作履歴（いつ、誰が、何を実施したか）を記録し、その記録内容の表示および検索が可能であること。	3.1，6.13，7.2	□	□	□
6	監査証跡は、削除または訂正できないこと。	3.1	□	□	□
7	監査証跡機能を無効化（OFF）できないこと。	6.13	□	□	□
電子署名					
8	署名された電子記録に署名者個人が特定できること。	6.4	□	□	□
9	署名された電子記録に、署名が行われた日時が含まれること。	6.4，6.13	□	□	□
10	署名情報を紙媒体またはPDFで出力する場合、署名者の氏名、署名の意味、署名の日時等を出力できること。	6.14	□	□	□
11	電子署名には、ユーザーIDおよびパスワードの入力を必要とすること。	6.4	□	□	□
12	署名された電子記録に、署名の理由（レビュー、承認等）が含まれること。	6.4	□	□	□

OECD GLP No.22に基づき「DI重要7領域」を定め、各々に対する要求仕様をチェックシートにまとめた

- データ
- 監査証跡
- 電子署名
- アクセスコントロール
- バックアップ
- アーカイブ
- 教育

DI関連チェックシート（データ、監査証跡）

	DIガイダンス（OECD GLP No.22）を踏まえた要求仕様	DIガイダンス根拠条項
データ		
1	シーケンス、メソッドおよび結果が、日時付きで印刷可能であること。	3.1、3.2、6.14
2	データはリレーショナルデータベースで一元管理されることが望ましく、既存データが上書きされない構造であること。	3.2、6.11
3	結果はメタデータとともに、完全性を保持した形で保存されること。	6.3
監査証跡		
4	監査証跡の機能を有すること。	6.1、6.13、7.1、7.2
5	監査証跡の機能により、操作履歴（いつ、誰が、何を実施したか）を記録し、その記録内容の表示および検索が可能であること。	3.1、6.13、7.2
6	監査証跡は、削除または訂正できないこと。	3.1
7	監査証跡機能を無効化（OFF）できないこと。	6.13

DI関連チェックシート（電子署名）

DIガイダンス（OECD GLP No.22）を踏まえた要求仕様		DIガイダンス根拠条項
電子署名		
8	署名された電子記録に署名者個人が特定できること。	6.4
9	署名された電子記録に、署名が行われた日時が含まれること。	6.4、6.13
10	署名情報を紙媒体またはPDFで出力する場合、署名者の氏名、署名の意味、署名の日時等を出力できること。	6.14
11	電子署名には、ユーザーIDおよびパスワードの入力を必要とすること。	6.4
12	署名された電子記録に、署名の理由（レビュー、承認等）が含まれること。	6.4

DI関連チェックシート（アクセスコントロール）

	DIガイダンス（OECD GLP No.22）を踏まえた要求仕様	DIガイダンス根拠条項
アクセスコントロール		
13	適切なユーザーアクセス権限を設定できること。	8.1、8.2
14	レビューを行う者には、結果の数値等を変更する権限を付与しないこと。	8.2
15	端末のアクセス管理に依存しない、ソフトウェア側のアクセス制御が行える機能を備えていること。	8.2
16	ユーザーごとに、職責に応じた権限を割り当てることができること。	8.2
17	ユーザーごとに、個別のIDおよびパスワードを設定できること。	8.2
18	パスワードは、管理者であっても参照できない構造であること。	6.4、8.2
19	データの作成者が、明確に識別できること。	8.2
20	重複するユーザーIDが登録できないこと。	8.2
21	過去に使用されていたユーザーアカウントを追跡できること。	8.2

DI関連チェックシート（バックアップ、アーカイブ、教育）

	DIガイダンス（OECD GLP No.22）を踏まえた要求仕様	DIガイダンス根拠条項
バックアップ		
22	測定データのバックアップを取得でき、電子記録として保存できること。	6.14、6.15
23	ハードウェア障害に備え、システムのバックアップを取得できること。	3.6、6.15
24	バックアップデータには、生データ、メタデータ、監査証跡を含むすべてのデータが含まれること。	3.6、6.13
25	バックアップデータを使用して、システムを正確に復旧できること。	3.6
26	指定のメディア（DVD、DAT（磁気テープ）、外付けHDD）を使用できること。	6.15
アーカイブ		
27	プロジェクト単位でアーカイブを作成できること。	6.16
28	指定のメディア（DVD、DAT（磁気テープ）、外付けHDD）を使用できること。	6.16
29	アーカイブしたデータをリトリーブ（再取得）できること。	6.16、3.2
30	アーカイブ操作が監査証跡に記録されること。	6.13
教育		
31	システム導入時に、使用者および管理者に対して教育が実施されること（必要に応じて、メーカーによる教育を受けること）。	3.4、4、5、6.1

DI関連チェックシート（実務上の補完要件）

	DIガイダンス（OECD GLP No.22）外の要求仕様*	DIガイダンス根拠条項
ウイルス対策ソフトについて		
32	ウイルス対策ソフトと競合しないこと。	–
スタンドアロンのデータ管理について		
33	データは付属PC内で管理し、USBやDVDなど外部メディアに移して移動できること。	–
時刻管理について		
34	ネットワーク上のタイムサーバーと自動同期すること。（ネットワーク接続）	–
35	管理者権限で時刻を校正することができること。（スタンドアロン）	–
障害対策要件、サービス要件（メーカーサポート）について		
36	導入後のトレーニングやトラブル発生時のサポート体制があること。	–

＊ No.22の条項には明示されないものの、DI確保に有用な実務上の補完要件

２．DIリスクマネジメントによる具体的事例検討

DIリスクマネジメントプロセス

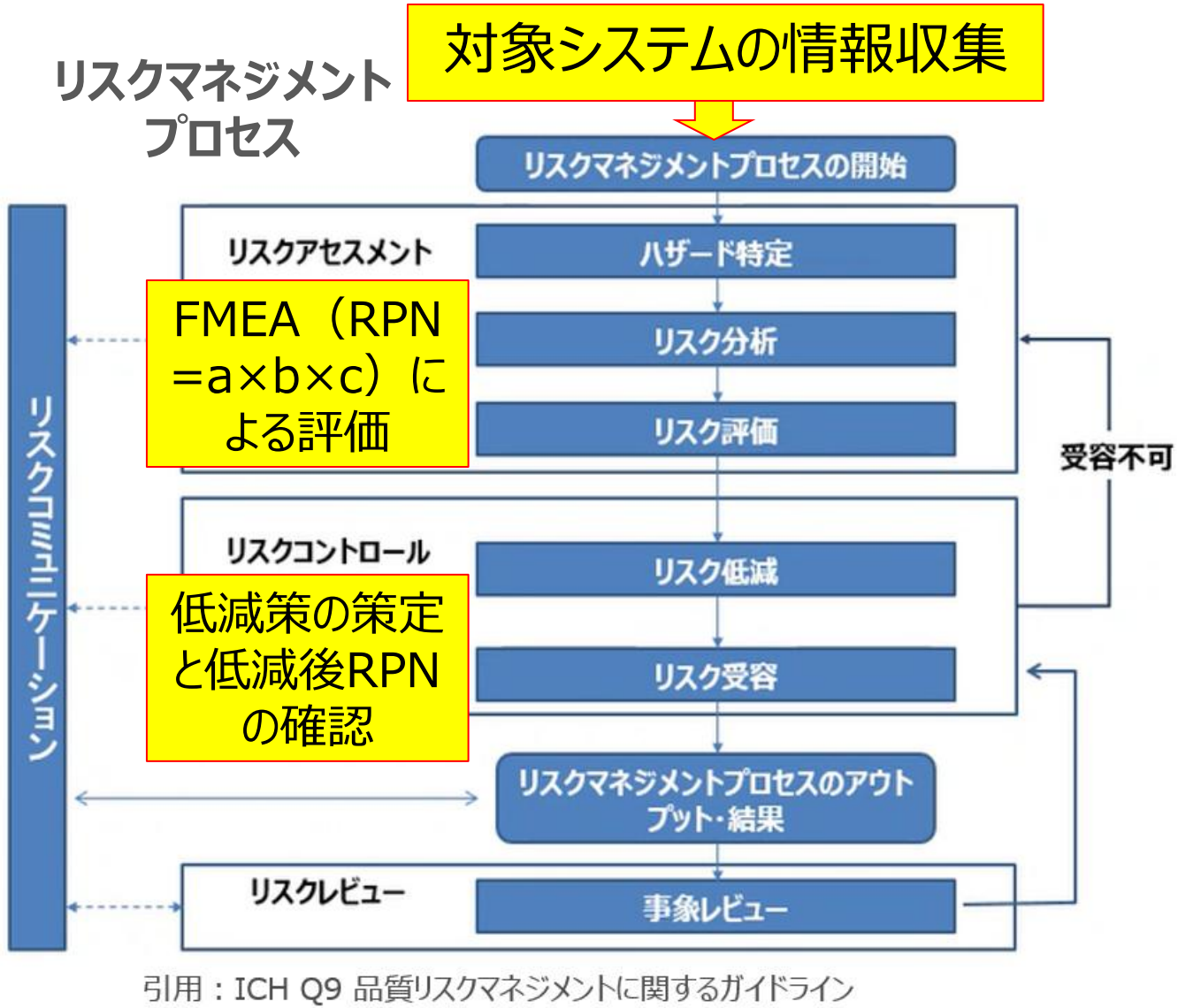
今回紹介するDIリスクマネジメント手法

- FMEAモデルを用いた
  リスクマネジメント手法をDIに適用
- 対象システムの情報収集

DIに関するハザードとリスクとは？

- ハザード：
  データが壊れたり、改ざんされたり、
  逸脱したりする起点となる事象（問題）

- リスク：
  ハザードによって起こる具体的な
  結果（悪影響）およびその度合い



引用：ICH Q9 品質リスクマネジメントに関するガイドライン

施設所有“機器”のDI対応状況（資料イメージ）

施設所有の機器リスト

機器	・・・	・・・	DIリスク分析
機器A	・・・	・・・	分析中
機器B	・・・	・・・	未着手
機器C	・・・	・・・	完了
・・・	・・・	・・・	・・・

施設所有機器の一覧とDIリスク分析の実施状況を管理するための台帳
（着手／進捗／完了の可視化）

機器Aのハザードリスト（FMEAモデル）

分類	ハザード	・・・	低減策	・・・	完了予定日
データ	・・・	・・・	・・・	・・・	・・・
監査証跡	・・・	・・・	・・・	・・・	・・・
電子署名	・・・	・・・	・・・	・・・	・・・
・・・	・・・	・・・	・・・	・・・	・・・

個別機器のハザードを列挙し、
FMEA手法によりリスク分析を実施、
低減策と優先順位を決定

対象システムの情報収集（DIリスク分析の前準備）

DIリスク分析を行うにあたり、対象システムに関する以下の情報を収集

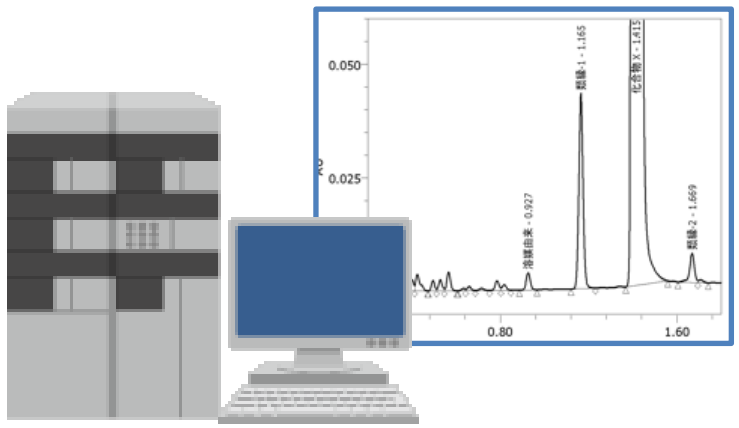
- DIガイダンスを踏まえた要求仕様 ⇒ DI関連チェックシートを活用
- 対象システムの仕様（機能）
- 対象システムの運用（使用状況）

分類	DIガイダンスを踏まえた要求仕様	対象システムの仕様	対象システムの運用	想定されるハザード	ハザード詳細	・・・
データ	・・・	・・・	・・・			
監査証跡	・・・	・・・				
電子署名	・・・	・・・				
・・・	・・・	・・・				
分類	DIガイダンス外の要求仕様	対象システムの仕様	対象システムの運用	想定されるハザード	ハザード詳細	・・・
時刻管理	・・・	・・・	・・・			
・・・	・・・	・・・	・・・			

DI関連チェックシートをベースに
仕様、運用を調査

モデルケース（既存HPLC／スタンドアロン）

以降のDIリスク分析は、下記**モデルケース**に基づいて実施



既存の**HPLC**（導入後10年使用）

- **スタンドアロン**で使用
- 電子データはローカルで保管、フラットファイル形式
- データ、シーケンス、メソッドは紙に印刷する
- DIに関する各種機能がある
  監査証跡、電子署名、個別ID、
  権限設定、バックアップ、アーカイブ、など

従来より施設の生データの定義が「紙」で、
DIに関する各種機能を有効化していない

本モデルは重点項目「DI対応機器への移行（監査証跡・オリジナルデータの保存）」に対応

対象システムの情報収集（例）

収集した情報をリスト化
⇒DIガイダンスを踏まえた要求仕様を満たさない部分を赤字で強調

分類	DIガイダンスを踏まえた要求仕様	対象システムの仕様（モデルケース）	対象システムの運用（モデルケース）
データ	• シーケンスとメソッドおよび結果が、日時付きで印刷可能であること。 （以下略）	データはフラットファイル形式 • シーケンスとメソッド及び結果が、日時付きで印刷可能である。 （以下略）	ローカルでフォルダ管理 • データはローカルのDドライブにプロジェクト単位のフォルダを作成し区分けして保存している。 （以下略）
監査証跡	• 監査証跡の機能を有すること。 （以下略）	• 監査証跡の機能を有する。 ✓ 監査証跡には以下の記録がない →ソフトウェア外の操作（上書き・削除・ファイル名変更、データコピーなど）、印刷記録 （以下略）	監査証跡のレビューは実施していない。 以下の紙データを元に、試験が正しく実施されたことを照査している。 （以下略）

※ 詳細内容はスライド22・23を参照

対象システムの情報収集（データ）

DIガイダンスを踏まえた要求仕様	• シーケンスとメソッドおよび結果が、日時付きで印刷可能であること。 • データはリレーショナルデータベースで一元管理されることが望ましく、既存データが上書きされない構造であること。 • 結果はメタデータとともに、完全性を保持した形で保存されること。
対象システムの仕様（モデルケース）	• シーケンスとメソッド及び結果が、日時付きで印刷可能である。 • 全てのデータはフラットファイルで管理され、変更（上書き・削除）可能な構造になっている。 • 結果はメタデータとともに、完全性を保持した形で保存される。
対象システムの運用（モデルケース）	• データはローカルのDドライブにプロジェクト単位のフォルダを作成し区分けして保存している。 • フォルダにはデータ、シーケンス、メソッド、レポートの各ファイルを一括して保存している。 • ファイル名は以下の運用ルールに従って命名、担当者が設定する（測定日-連番）。 • 測定者はファイル名の修正、ファイルの削除の権限を有している。 • 他の試験で使用したメソッドやレポートをコピーしてカスタマイズして使用可能である。 • 管理者権限を有する1ユーザー（ID：admin）のみ登録し、測定者は共用で使用している。 • 電子データのレビュー（電子データの保存確認、監査証跡の内容確認）は実施していない。

対象システムの情報収集（監査証跡）

DIガイダンスを踏まえた要求仕様	• 監査証跡の機能を有すること。 • 監査証跡の機能により、操作履歴（いつ、誰が、何を実施したか）を記録し、その記録内容の表示および検索が可能であること。 • 監査証跡は、削除または訂正できないこと。 • 監査証跡機能を無効化（OFF）できないこと。
対象システムの仕様（モデルケース）	• 監査証跡の機能を有する。 ✓監査証跡には以下の記録がない。 → ソフトウェア外の操作（上書き・削除・ファイル名変更、データコピーなど）、印刷記録 • 監査証跡の機能により、操作履歴（いつ、誰が、何を実施したか）を記録し、その記録内容の表示、検索が可能である。 • 監査証跡は削除、訂正ができない。 • 監査証跡機能を無効化（OFF）できない。
対象システムの運用（モデルケース）	監査証跡のレビューは実施していない 以下の紙データを元に、試験が正しく実施されたことを照査している。 • 測定操作を記載したワークシート • 測定前に印刷したシーケンス、メソッド • 測定後に自動印刷されたクロマトグラム • 各種使用記録（試料・標準物質・カラム・機器など）

対象システムの情報収集のポイント

情報収集はDIリスクマネジメントのスタート

正しい情報が必要、情報収集に時間がかかる

⇒ 多くの専門分野にわたるチームでの対応を推奨

①リーダーを指名し、リソースを確保する

- リーダーはDIリスク分析プロセス全体を把握し、責任（R）／承認（A）の経路を明確化
- 必要工数の試算、スケジュール・優先順位の設定

②専門性を持つメンバーを招集し、役割を割り当てる

- DIガイダンス：QA（No.22／社内基準に精通）
- 仕様：ベンダー、システム管理者、機器管理者など
- 運用：利用者、機器管理者など

誰が精通しているか？（管理者、利用者が全て把握しているとは限らない）

対象システムの情報収集のポイント

③作業内容や収集すべき情報をメンバーに周知する。
- 背景と到達点（優先度・低減策・受容）を共有
- 雛型の明示（入力例つき）
- ライフサイクル（生成、処理、レビュー・報告・使用、保存・アーカイブ、廃棄）に沿って、データ（紙・電子）の運用実態を調査

言葉で説明できないことも多い
⇒実際の事例を見せた方が
共通理解を得やすい

④収集情報をレビューし、根拠資料と実機確認で妥当性を検証する
- 根拠資料：
  仕様書、取扱い説明書、CSV記録（テスト記録・点検記録等）、監査証跡
- 実機：
  現設定の確認（権限・監査証跡設定・バックアップ設定・アーカイブ設定 等）

全ては正しい情報から始まる
・推測で片づけない（多分、～だろう、～と思う）
・悪い情報を含めた現状把握（過去の経緯は不問）

FMEAモデル（リスクアセスメント）

影響度（a）	小～大	1、2、3、4
発生度（b）	小～大	1、2、3、4
検出度（c）	容易～困難	1、2、3、4

前半：リスクアセスメント

リスクアセスメント

分類	ハザード	ハザード詳細	影響度詳細	影響度	発生度詳細	発生度	検出度詳細	検出度	RPN	選択●
データ	悪意を持ったデータ削除	データはローカルでフォルダ管理しており、誰でも作為的に特定のデータを削除することができる	データ改ざんに繋がる可能性がある	4	測定者はデータ削除の権限を有しており、特定のデータを容易に削除可能	4	電子データのレビュー（電子データの保存確認、監査証跡の内容確認）は実施していないため、データ削除を検出するのは難しい	4	64	●

ハザード：
想定される事象（問題）

ハザード詳細：
ハザードが起こる背景、要因

リスク：ハザードによって起こる具体的な結果（悪影響）およびその度合い

- **影響度詳細**：リスクの影響（重大性）は？
- **発生度詳細**：リスクが起きる頻度は？発生する要因から考える
- **検出度詳細**：リスクが起きた場合、検出可能か？検出方法から考える

FMEAモデル（リスクアセスメント）

評価基準

影響度（a）	小～大	1、2、3、4
発生度（b）	小～大	1、2、3、4
検出度（c）	容易～困難	1、2、3、4

前半：リスクアセスメント

リスクアセスメント

分類	ハザード	ハザード詳細	影響度詳細	影響度	発生度詳細	発生度	検出度詳細	検出度	RPN	選択●
データ	悪意を持ったデータ削除	データはローカルでフォルダ管理しており、誰でも作為的に特定のデータを削除することができる	データ改ざんに繋がる可能性がある	4	測定者はデータ削除の権限を有しており、特定のデータを容易に削除可能	4	電子データのレビュー（電子データの保存確認、監査証跡の内容確認）は実施していないため、データ削除を検出するのは難しい	4	64	●

影響度、発生度、検出度：評価基準に基づき、点数を付与（今回は４段階に設定）

RPN（Risk Priority Number リスク優先指数）：
RPN＝影響度×発生度×検出度

選択：RPN等を基準に、対策を優先すべきハザードに●を記入

ハザード特定のポイント

リスクの要因を分類して、ハザードを洗い出すこと

「DIの要求事項」と「対象システムの仕様・運用」の乖離が「リスクの要因」

リスクの要因を体系的に分類し、想定されるハザードを洗い出す

ここで拾い切れないと、以降のリスク評価から漏れる

＜リスクの要因の分類例＞

- システム的要因：　DIに関する重要機能がない
- 運用的要因：　DIに関する重要機能があるのに、運用手順が曖昧、形骸化。
- 人的要因：　DIに関する重要機能があるのに、運用手順から逸脱している
  GLPの手順から逸脱している、教育が不足している
  人手を介する作業が多い

リスク分析・リスク評価のポイント

3つの指標について、具体的に分析すること

ハザードから起こるリスクを明確にすること（1つのハザードから複数のリスクが生じることも）
リスクに紐づく要因を明確にすること

影響度：データ改ざん（履歴のない変更など）・消失など、重大な影響につながるか？
バックアップデータからの復旧は可能か？

発生度：意図して発生させることができるか？（権限設定が適切か？）
特定の条件にならないと発生しないか？（スケジュール設定が適切か？）
現在の運用上の問題か？（DI対応機能を使用しているか？）
測定者の理解の問題か？（GLP、システムの理解度は十分か？）

検出度：監査証跡から検出可能か？（ログに情報が残るか？検出方法があるか？）
人のレビューで見落とさずに検出できるか？（漏れ、人間の能力差、など）
現在の運用上の問題か？（監査証跡レビューを実施しているか？）

FMEAモデル（リスクコントロール）

影響度（a）	小～大	1、2、3、4
発生度（b）	小～大	1、2、3、4
検出度（c）	容易～困難	1、2、3、4

■ 後半：リスクコントロール

リスクコントロール

	低減策	期待効果/懸念事項	低減後 a	低減後 b	低減後 c	低減後 RPN	Δ RPN	採用○
A	電子データのレビューの実施	電子データのレビューにより、電子データが削除されていないことが検出できる。 レビュー後にデータ削除される可能性がある。						
B	FIX後のデータの保護（アクセス権変更）	FIX後のデータの変更（改ざん、削除）を防ぐことができる。いつFIXしたか確認する必要がある。 アクセス権の変更忘れがある.						
C	FIX後のデータの保護（アーカイブ実施）	FIX後のデータの変更（改ざん、削除）を防ぐことができる。アーカイブした履歴を管理する必要がある。						
D	SOP作成、教育（低減策A～C）（手順の明文化）	電子データのレビュー～FIX後のデータの保護まで一連の作業が手順化でき、データ削除の防止、検出が可能になる。 人手を介するため作業を失念する可能性がある。						

低減策：
リスクを低減する方法。
いくつかの低減策を
組み合わせてもよい。

期待効果/懸念事項：
リスク低減策に期待する効果。
低減できない残留リスク、
低減策を実施した後に
新たに発生するリスクなど、
懸念事項があれば記載する。

※本資料の「FIX」＝データの最終確定（ロック）を指す。

FMEAモデル（リスクコントロール）

評価基準

影響度（a）	小～大	1、2、3、4
発生度（b）	小～大	1、2、3、4
検出度（c）	容易～困難	1、2、3、4

■ 後半：リスクコントロール

リスクコントロール

	低減策	期待効果/懸念事項	低減後 a	低減後 b	低減後 c	低減後 RPN	Δ RPN	採用 ○
A		れて	4	4	2	32	-32	
B		とが	4	2	4	32	-32	
C		とが	4	2	4	32	-32	
D		。	4	2	2	16	-48	○

低減後の影響度/発生度/検出度：
低減策によりリスクを低減した後の点数を、
評価基準に基づき点数化。

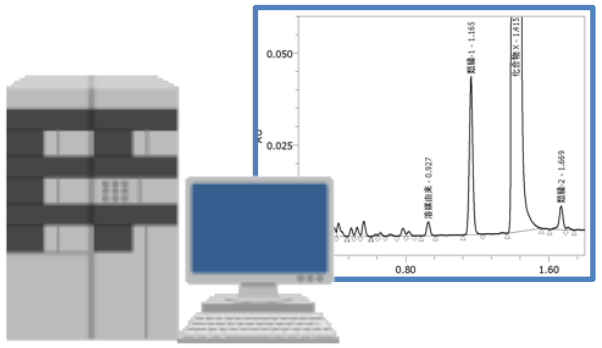
低減後のRPN：
低減後RPN＝低減後の影響度×発生度×検出度

ΔRPN：
ΔRPN＝リスク低減前 RPN - リスク低減後 RPN

採用：
採用する低減策を選択します。

リスク低減のポイント

モデルケース



DIに関する各種機能がある
監査証跡、電子署名、
個別ID、権限設定、
バックアップ、アーカイブ、など

まずはDIの各種機能を有効にすること

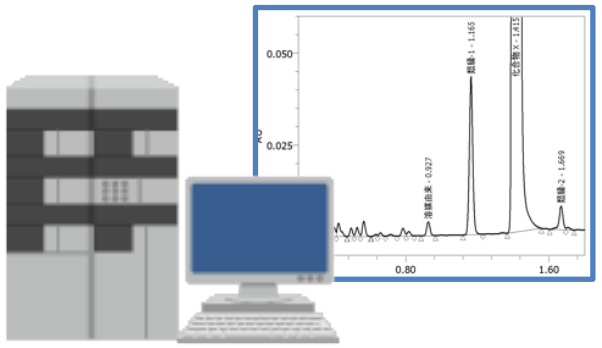
これまでの運用方法はリスクが高い状態である認識

- 紙が生データ
- 電子データレビューを実施していない
- 監査証跡のレビューは実施していない
- 電子署名機能を使用していない
- 測定者はファイル名の修正、ファイルの削除の権限を有している
- 管理者権限を有する1ユーザー（ID：admin）のみ登録し、測定者は共用で使用している
- バックアップ、アーカイブはしていない

- 測定者にファイル名の修正、ファイルの削除の権限を与えない　⇒　生成データの保護
- 各ユーザーにIDを付与　⇒　監査証跡のレビューによる検知

リスク低減のポイント

モデルケース



DIに関する各種機能がある
監査証跡、電子署名、
個別ID、権限設定、
バックアップ、アーカイブ、など

DIの各種機能はホントに有効か？

機能を有効にしてみたものの・・・

- 監査証跡
  - レビューに必要な情報が残っていない
  - 管理者権限を有するものしか閲覧できない
- 電子署名
  - 再解析した場合、レポートに再解析者が表示されない
- アクセスコントロール
  - ソフトウェア内ではデータ削除を制限できても
  - OS上ではデータ削除を制限できない
  - （OSでの削除はファイルシステムの“改変”に該当する）

ユーザーの求める機能を有しているのか確認すること

リスク低減のポイント

リスクアセスメント

分類	ハザード	ハザード詳細	影響度詳細	影響度
データ	悪意を持ったデータ削除	データはローカルでフォルダ管理しており、誰でも作為的に特定のデータを削除することができる	データ改ざんに繋がる可能性がある	4

システム設定だけでなく人への対応も必要

「データ改ざんに繋がる可能性」は確かに問題

⇒具体的に何が問題なのか？

・測定者がデータを削除できること

→ システム設定変更

・測定者がデータを削除することを問題と感じていないこと → 教育（GLP）

リスクコントロール

	低減策	期待効果/懸念事項	低減後 a	低減後 b	低減後 c	低減後 RPN	Δ RPN	採用 ○
E	測定者へのGLP教育	データ削除がなぜダメなのかGLPの要求事項から理解し、無知による削除を防ぐことができる。	4	4	4	32	-32	
F	低減策A～Eの実施	無知による削除を防止することができる。レビューとデータ保護の手順を決めることでデータ削除が検出可能になり、悪意を持った削除を抑制することができる。 人手を介するため作業を失念する可能性がある。	4	2	2	16	-48	○

リスク低減のポイント

低減策は具体的（手順、指標）にすること

①手順

- システム内に機能を有している場合
  - 測定者に有効化した機能を教育すること
  - SOPに規定（明文化）すること
- システム内に機能を有していない場合
  - 不足している情報は人手を介して記録する（紙）
    ⇒ 人手を介する作業は完全でない（作業漏れを検知する手順、教育がより重要）
    （監査証跡機能がない影響、さらに人手が・・・）

具体的な手順
教育
明文化（SOP）

②指標

低減策の効果を評価する指標を設定（定量的モニタリング）

- 効果を評価する期間
- 低減策の実施結果、ハザードの発生頻度、SOPの理解度（テスト・実技）など

リスク受容

低減策を実施した場合の残存リスクが受け入れ可能か否かを判断し、
採用する低減策を決定する

残存リスク：RPNは最小の1にならない

- DIに関する各種機能が不足しているが、継続使用する場合
- 人手を介する作業

⇒リスクが可能な限り低減され、コントロールできている前提で
特定の条件下で合理的な判断がされた場合、リスクを受け入れる

低減策の優先順位：ΔRPNだけでは判断できない場合もある

- 特定の機器：短時間で対応可能なものから実施
（大幅な手順変更、機種更新は時間がかかる）
- 複数の機器：重要度の高い機器から実施
（稼働率、売上率、新規導入機器など）

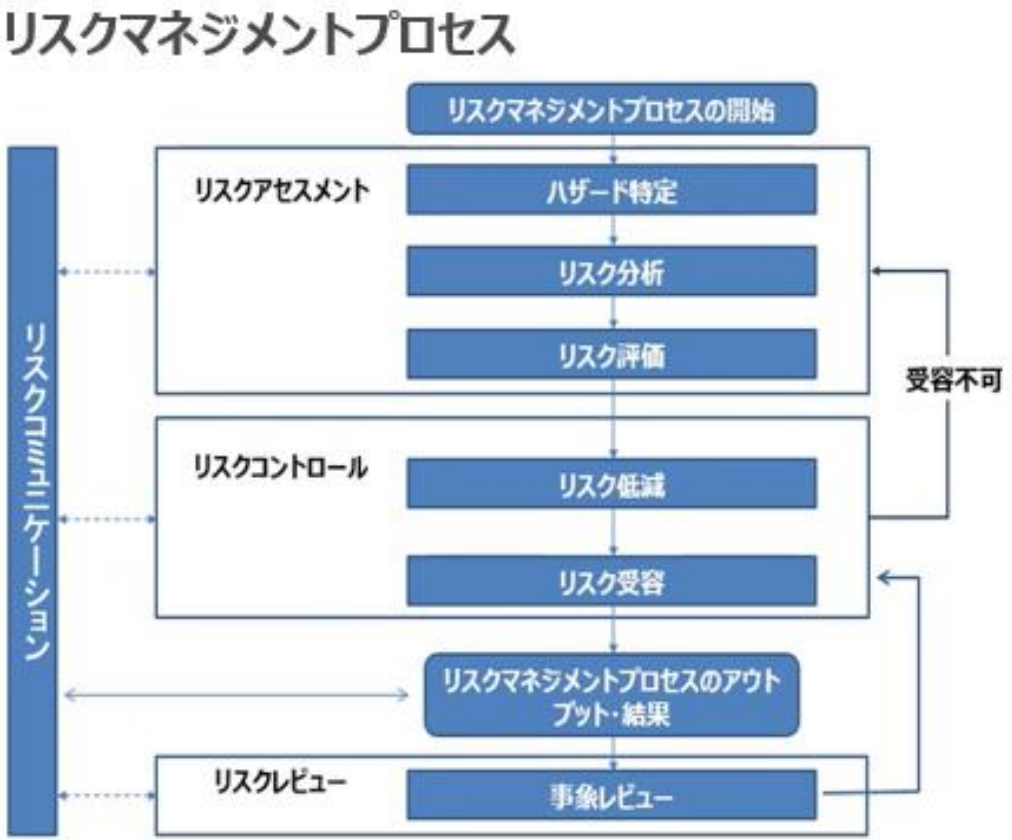
事象レビュー

低減策の効果を定量的な観点で評価する

同じハザードを再発させないこと

- システムは長期に渡って使用する
  同じハザードを再発させないことが重要

- 効果が不十分なら再度リスク低減策を策定し直し
  サイクルさせる（失敗を恐れず何度もチャレンジ）

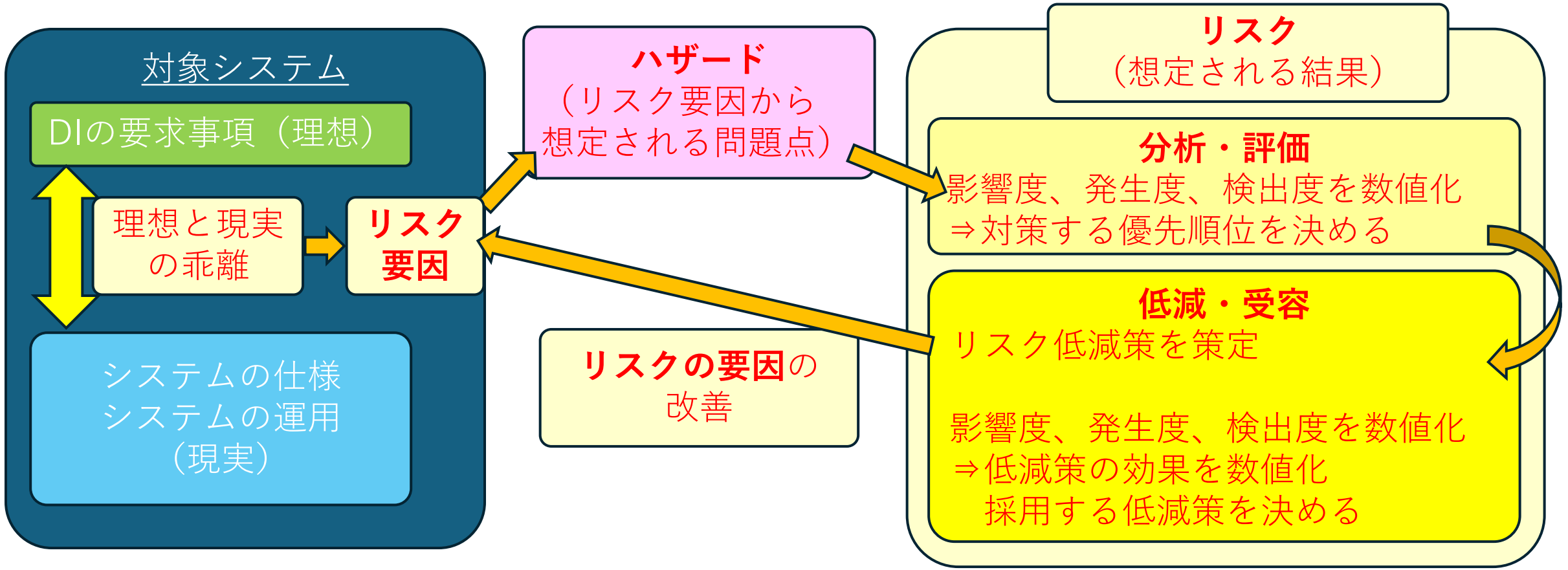


引用：ICH Q9 品質リスクマネジメントに関するガイドライン

３．まとめ

DIリスクマネジメントの体系図（まとめ）

DIのリスクマネジメントの重要ポイント：対象システムの仕様、運用を把握すること



・DIのハザード：データが壊れたり、改ざんされたり、逸脱したりする起点となる事象（問題点）
・DIのリスク：　ハザードによって起こる具体的な結果（悪影響）およびその度合い

まとめ

- DIに関するリスク分析の方法、具体的事例に関する情報がないことから、DIリスクマネジメントの手法を検討した。
- DIガイダンスを踏まえた要求仕様をまとめた「DI関連チェックシート」を作成した。
- FMEAモデルを用いたリスクマネジメント手法をDIに適用し、DIガイダンスをベースにシステム面からのアプローチを検討した。

＜本手法の重要ポイント＞

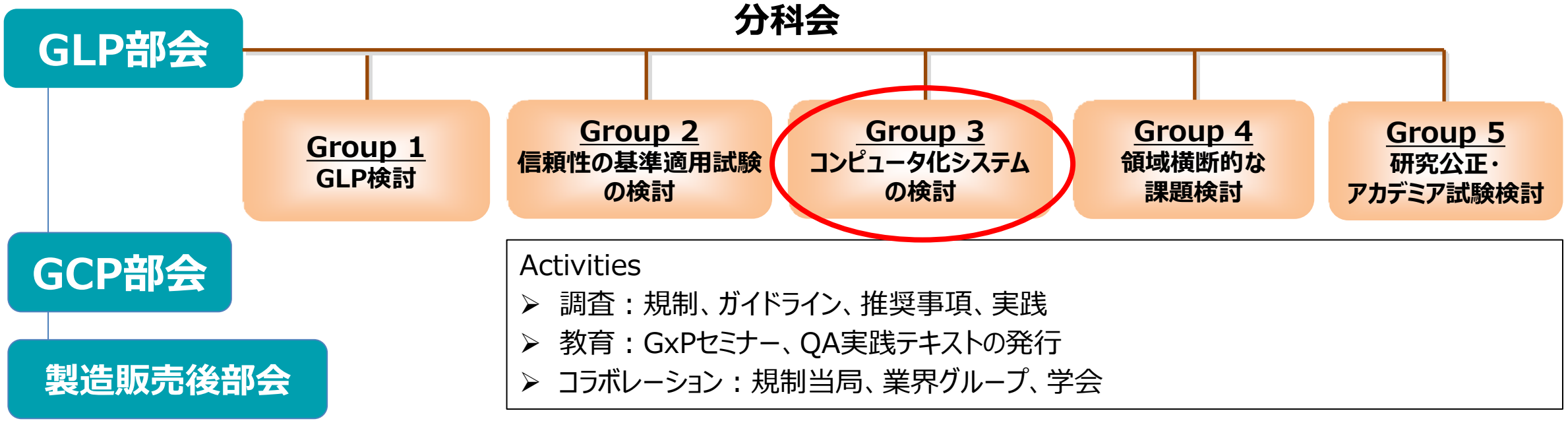
- ハザード特定時に必要な情報のパターン化
  - ✓ DIガイダンスを踏まえた要求仕様、対象システムの仕様、対象システムの運用
- FMEA手法によるリスクマネジメントプロセスの実施
- リスク低減策のパターン化（具体的な手順、教育、明文化）
- 人が介在する作業特有のリスクを見極める

日本QA研究会とは

- **日本QA研究会（Japan Society of Quality Assurance：JSQA）**
  - 日本QA研究会は、医薬品、医療機器、農薬、化学物質、食品、動物用医薬品、飼料添加物等における品質及び信頼性保証（QA＝Quality Assurance）に係る者で構成される一般社団法人です。
- **活動内容**
  1. 品質及び信頼性保証に関する研究
  2. 収集情報及び研究成果に基づく資料及び成果物の発行
  3. グループ活動、講演会、教育研修講座、合同部会総会等の開催
  4. 関係官庁、関係団体等との交流
  5. 関係行政機関からの情報収集と会員への情報提供
  6. 海外関連機関との交流及び海外情報の収集と会員への情報提供
  7. その他、本会の目的達成に必要な事項

以下のサイトから抜粋
https://jsqa.com/about/activity/index/

日本QA研究会の組織体制



GLP部会第3分科会

非臨床試験に使用するコンピュータ化システムの信頼性保証の検討に加え、
新技術（AI，クラウドサービスなど）の導入に関連する課題についても検討する。

- 第1グループ： 非臨床試験へのAI導入検討及び関連する法規制の検討
- 第2グループ： 非臨床試験におけるコンピュータ化システムの適正管理及び信頼性保証部門DI教育の検討

以上、皆さまの参考になれば幸いです

ご清聴ありがとうございました