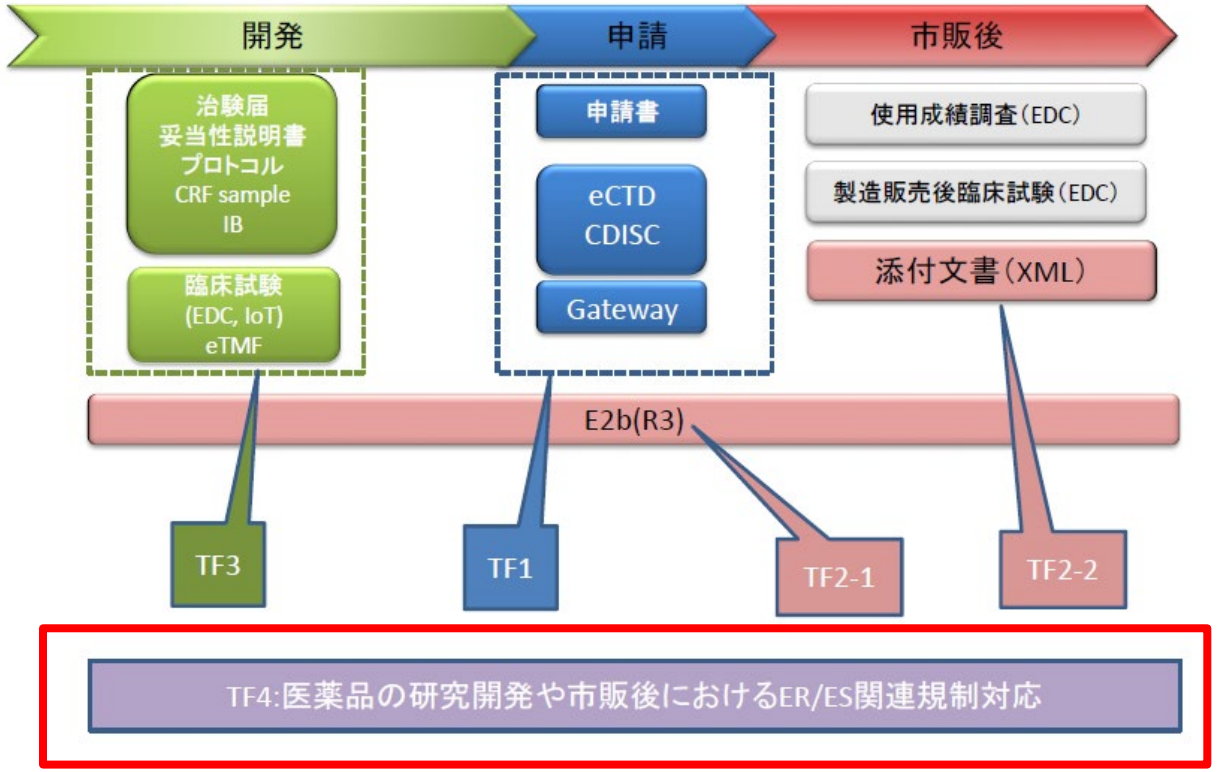
製薬協

# ベンダー契約の際のリスク評価

電磁化対応ミニセミナー
2022/12/21
医薬品評価委員会　電子化情報部会
TF4幹事　飯嶋　真弘

# はじめに




EI部会 TF4：
『医薬品の研究開発や市販後におけるER/ES関連規制対応』

（1）規制要件検討
（2）バリデーション実施手法の検討
（3）CSV教育
（4）ベンダー対応検討
（5）CSV関連のミニシンポジウムの実施検討

本日は、ベンダー契約の際のリスク評価について発表いたします。

本発表は、EI部会 TF4の歴代の検討結果と考察内容に加え、演者のこれまでの経験に基づいた情報や解釈を基に作成しています。内容については、TF内のレビューにて現時点での正確性を確認しておりますが、その他の内容については演者の意見も含まれることについてご承知おきください。

# 本日の内容

- 構築フェーズのリスク
- 運用フェーズのリスク
- 廃棄フェーズのリスク
- ベンダー契約の際のリスク評価

# ベンダー契約時のスコープ

コンピューターシステムのライフサイクル


データのライフサイクル


- ベンダーのスコープ（赤枠）の「構築」「運用」「廃棄」
- 利用者のスコープ（青枠）は「前システムの廃棄」「構築」「運用」「廃棄」「次のシステムの構築」

上記の認識の違いを踏まえてリスク評価を行う必要があります。

# ICH-Q9 品質リスクマネジメント

リスクアセスメントは下記を行います。

- リスク特定
- リスク分析
- リスク評価

またリスクに対する対応は、下記があります。

- リスク低減
- リスク受容
- リスク回避
- リスク転移

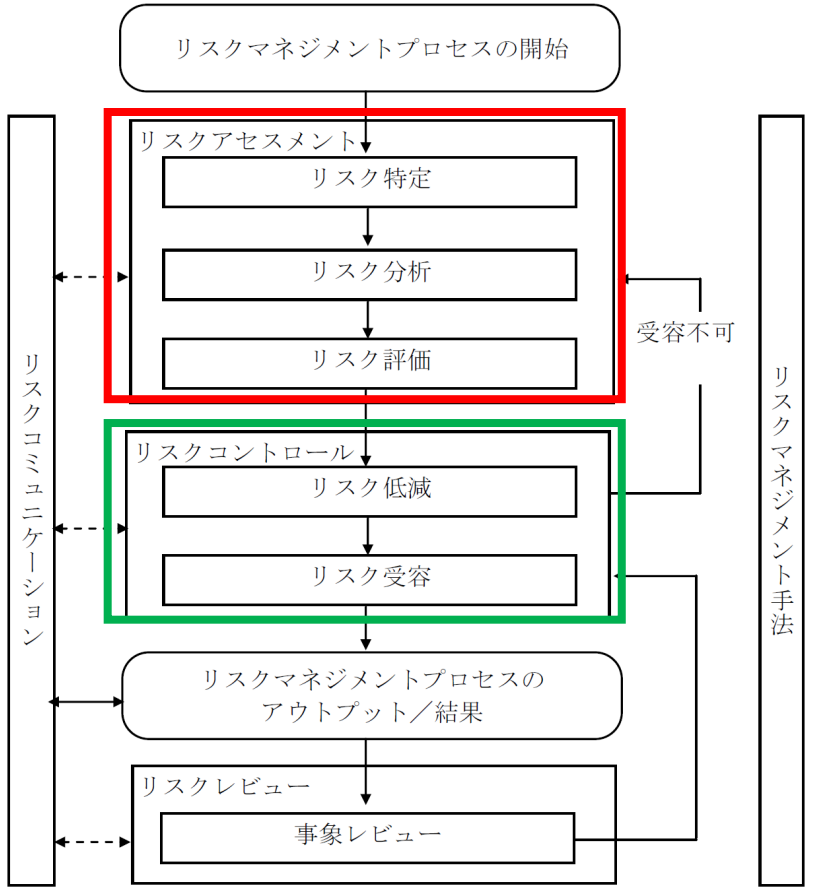



図1　典型的な品質リスクマネジメントプロセスの概要

# システムの利用にあたり検討すべきこと

- 電子規制対応　ER/ES指針
  - 真正性（セキュリティ・監査証跡・バックアップ）
  - 見読性
  - 保存性
  - CSVによる信頼性、組織・設備、教育訓練
    - 利用者がCSV(Computerized System Validation)を実施し、その結果を文書に残す必要がある
      - ユーザーの要求（URS）に対する、機能（Functional Specification）や設定（Configuration）やプログラミングが適切になされ、テストされていることを文書化すること
      - 組織体制（責任者、管理者、利用者等）の文書化（運用手順書等）、教育訓練とその記録
    - システムのセキュリティ

      特にクラウドシステムの場合、最新のセキュリティ対策に対応
- リスクベースドアプローチ
  - システムライフサイクルを通じたリスク評価

※上記の検討が難しい場合は、（IT知識のある）コンサルタントに依頼することを考慮する必要があります。

※購買や契約の担当者と早めに情報共有することでリスク評価の助けになる場合があります。

製薬協

# 構築フェーズのリスク

# ユーザー要求仕様書（URS）

CSVの目的の一つが、ユーザーの要求を満たしたシステムであることを明文化することであり、重要な文書です。

原則論は、「ユーザーの要求に従ったシステムを構築する」ですが、

多くは、用途に適合したシステムを候補にあげ、

　ユーザー要求により適合したシステムを選定

　システムで実現できないユーザー要求を修正

というプロセスでユーザー要求仕様書は作成されます。

※ベンダーのユーザー要求仕様書をそのまま受け入れる場合もありますが、そうであってもユーザー要求仕様書の責任はユーザーにあります。

# リスク評価例：ユーザー要求仕様書

## リスク特定：ユーザー要求に対応できないシステムのため、カスタマイズを行う

## リスク分析：

- ソフトウェアカテゴリ分類が4（設定）から5（プログラミング）になりCSV対応の工数が上がる
- 自社のみのカスタマイズはシステムの構築時およびバージョンアップ時に追加の工数が発生し、長期的な費用が上がる

## リスク回避

- 現在のユーザー要求に対応できないが、ユーザー要求を変更することによりカスタマイズが不要になる。

  例：部門で承認後に最終承認者が承認するワークフローが実施できないが、運用を変更することで対応

※無理に前システムやプロセスにこだわらない

# ユーザー要求に見合うシステムかの見極め

選定時のユーザー要求に対するリスク特定の方法

- なるべく具体的な要求にする
- デモンストレーションを、ユーザー要求に沿った形で実施
- 情報収集（他の同目的のシステム・企業間・ユーザー会）

# リスク評価例：スケジュール遅延

## リスク特定：スケジュール遅延

## リスク分析

- 機能要求のすり合わせに時間を割く
- スケジュール要求がベンダーと依頼者でイメージが異なる
- ベンダーの体制・人員確保・退職等

## リスク低減

- 選定時のオーディット
- Quality Management System（体制、SOP等）の確認
- 対応者の業務負荷確認

製薬協

# 運用フェーズのリスク

# 前システムからのデータの対応

前システムからのデータの対応方法

- 監査証跡付きで変更できない媒体で保存し、必要なデータのみシステムに登録
- システムに監査証跡を含めて移行
  - システムの監査証跡に前システム監査証跡を移行
  - 前システムの監査証跡をシステムの監査証跡とは別の手立てで表示

リスク特定

前システムの監査証跡をシステムの監査証跡とは別の手立てで表示

理由は廃棄フェーズで説明します。

# リスク評価例：変更管理

## リスク特定：変更管理が発生

## リスク分析

- 規制やガイドラインの変更
- ブラウザ・システムのバージョンアップによる不具合
- セキュリティ向上のための対応

## リスク低減

- 選定時のオーディット
- Quality Management System（体制、SOP等）の確認
- 対応者の業務負荷確認

製薬協

# 廃棄フェーズのリスク

# 廃棄フェーズ

- 運用時（運用終了時）にデータを出力するシステム

  例：EDC（被検者PDF　データセット　ユーザー一覧表等）

  上記の場合は、廃棄フェーズにてシステムからデータが適切に消去されることを確認すればよいため、比較的単純である。

- データ保存を目的とするシステム

  システムを廃棄する際にデータを出力する必要がある

  また、その際に、真正性、見読性、保存性を担保する必要がある

今回はデータ保存を目的とするシステムについて説明します。

# データ出力方法

## データ出力方法

- 1.ユーザーが1ファイルづつ出力（監査証跡も含む）
- 2.ユーザーが一定単位で出力できる機能により出力（監査証跡含む）※機能が必要
- 3.ベンダーがプログラムを組みデータベースから出力

## 重要事項：

- 出力時間
- 真正性・見読性・保存性の担保

## スケジュール：

システム利用終了（ユーザーに更新させない状態にする）

データ出力＋検証

システム廃棄（データ消去＋物理廃棄）

# リスク評価例：ユーザーが1ファイルづつ出力する

リスク特定：ユーザーが1ファイルづつ出力する

リスク分析

データ移行時間が非常に多くかかる

人の操作によるケアレスミスを防ぐ手立てが必要

リスク保有

データ移行の人員と時間を確保する

ダウンロードデータを別の人が確認して記録を残す

# リスク評価例：ユーザーが一定単位で機能により出力

リスク特定：ユーザーが一定単位で機能により出力

リスク分析

人の操作によるケアレスミスを防ぐ手立てが必要

リスク保有

データ移行の人員と時間を確保する

ダウンロードを別の人が確認して記録を残す

# リスク評価例：ベンダーが出力

リスク特定：ベンダーが出力

リスク分析

選定時にどのようにデータが出力されるかが不明確

出力時間が不明確

リスク保有

ベンダーの出力時のCSV対応

# データ保管および利用・移行

## データ保管

変更できない媒体もしくはバリデーションされたシステムにて保管
※重要

## データ利用・移行

- データ保存したファイルからコピーして新規登録して利用
  - データ移行前まで：前システムの監査証跡で真正性を担保
  - データ新規登録後：現システムの監査証跡で真正性を担保
- 監査証跡も含めてデータ移行して利用
  - ベンダーの力量が必要

# リスク評価例：前システムの監査証跡を別の手立てで表示

## リスク特定：前システムの監査証跡をシステムの監査証跡とは別の手立てで表示

## リスク分析：

前システムの監査証跡と現システムの監査証跡を同じ形式で出力することが難しい

## リスク保有：

例示：2028年にシステム変更する際に下記の監査証跡の対応を検討

- 2023年までに利用していた前システムのデータの監査証跡
- 現システム利用開始日から前システムのデータ移行終了日までのデータの監査証跡
  前システムか現システムか日付で識別できない
- データ移行終了後の現システムのデータの監査証跡

製薬協

# ベンダー契約の際のリスク評価

# ベンダーの対応とシステムの長期的な動向

- システム廃棄の対応については、ベンダーは消極的であることが多い。

  そのためユーザー側から強く確認する必要がある。
- 基盤システム（OSやDB等）はサポート期間が5～10年程度であり、同じタイミングでシステムのバージョンアップが必要になることが多い
- 上記タイミングで、費用増加やシステム終了することもある
- 会社の買収で対応がかわることがある

→システムを変更できる準備が重要である

# ベンダー契約の際のリスク評価

コンピューターシステムのライフサイクル


データのライフサイクル


ベンダーとユーザーのスコープの違いを認識して、リスク評価を行うことが重要になります。

対応がユーザーのみで難しい場合は、(IT知識のある)コンサルタントを間に入れることを考慮したほうがよいかもしれません。

# ベンダー契約の際のリスク評価

契約条項でリスクとなる可能性のある記載

- サポート体制（時間、期間、対象バージョン）
- サービス提供（サービス終了通知や解約などの手続き）
- データ保存（データに対する補償、バックアップ、制限事項）
- 機密情報や個人情報データの取り扱い

# ベンダー契約の際のリスク評価

**構築時**

- 電子規制対応
  - ユーザー要求
  - ソフトウェアカテゴリ分類
- スケジュール

**運用時**

- データ移行
- 変更管理
- 障害管理
- エラー管理

**廃棄時**

- 利用停止
- データ移行
- データ廃棄
- システム廃棄

**セキュリティ・QMS**

上記のすべてをベンダー契約の際に確認することはできないかもしれませんが、契約前に情報を入手し、適切にリスク評価を行い契約をすることが重要になります。

特に廃棄時はベンダーの考慮が及んでいない場合が多く注意が必要となります。

製薬協

# ご清聴ありがとうございました。