


配布版



# 医薬品製造におけるセキュリティ管理 ～ベンダーの役割、ユーザーの役割～

2010年2月9日

 ITエンジニアリング株式会社

製薬ソリューション部 横井 昭彦



# 目次

---

1

医薬品製造の特徴

2

医薬品製造法規制とセキュリティ管理

3

セキュリティ管理への問いかけ



# 医薬品製造の特徴①

- ・ プロセス製造業のバッチ型生産
  - － 規模が小規模
    - ・ スケールメリットは小
    - ・ バッチ単位の厳重な管理（原料ロットの混在やフィードバックは禁止）
  - － 法規制に対応した生産
    - ・ 製造管理と品質管理の分離
    - ・ 品質管理と品質保証の分離
  - － 計測に関しても一般製造業と異なる基準
    - ・ 日本薬事局方に代表される独自の基準（例えば、バラツキの取扱い）



# 医薬品製造の特徴②

---

- 医薬品業界のビジネス環境
  - 医療用医薬品は政府が価格を決定（薬価）
    - 医療費削減のため、政府がジェネリック医薬品（特許切れ品）の普及を推進
  - 新製品の不足
    - 2010年問題
  - 大手（国内・外資）と中堅以下の格差
    - 国内大手は売上・利益の多くを海外に依存



# 医薬品製造の特徴③

---

- セキュリティ管理との関係
  - 電子記録・電子署名の法規制で注目
    - FDA（米国の厚生労働省）のPart11（1997年）
    - データのセキュリティに重点
    - 米国の医薬品業界の反対で、ペナルティを保留中（2003年以降）
      - 莫大なコストを投じても対応が困難
  - ITの進歩で再度注目
    - ネットワーク
    - 制御系と管理系との融合



# 目次

---

1

医薬品製造の特徴

2

医薬品製造法規制とセキュリティ管理

3

セキュリティ管理への問いかけ



---

2-1 厚生労働省ガイドライン

2-2 GAMP 5ガイド

2-3 GAMP 5のセキュリティ管理

2-4 GPG “ITインフラ”

# 厚生労働省のガイドライン①

- ・ 正式名称は「コンピュータ使用医薬品等製造所適正管理ガイドライン」
- ・ 医薬品製造に関係するコンピュータシステムのバリデーション(CSV)〈適格性評価〉を規定
- ・ 旧版は1993年に発行、改訂版が2010年前半に発行予定
- ・ 後述のGAMP5ガイドの考え方をいくつかの部分で採用





---

2-1 厚生労働省ガイドライン

2-2 GAMP 5ガイド

2-3 GAMP 5のセキュリティ管理

2-4 GPG “ITインフラ”

# GAMP5ガイドの概要①

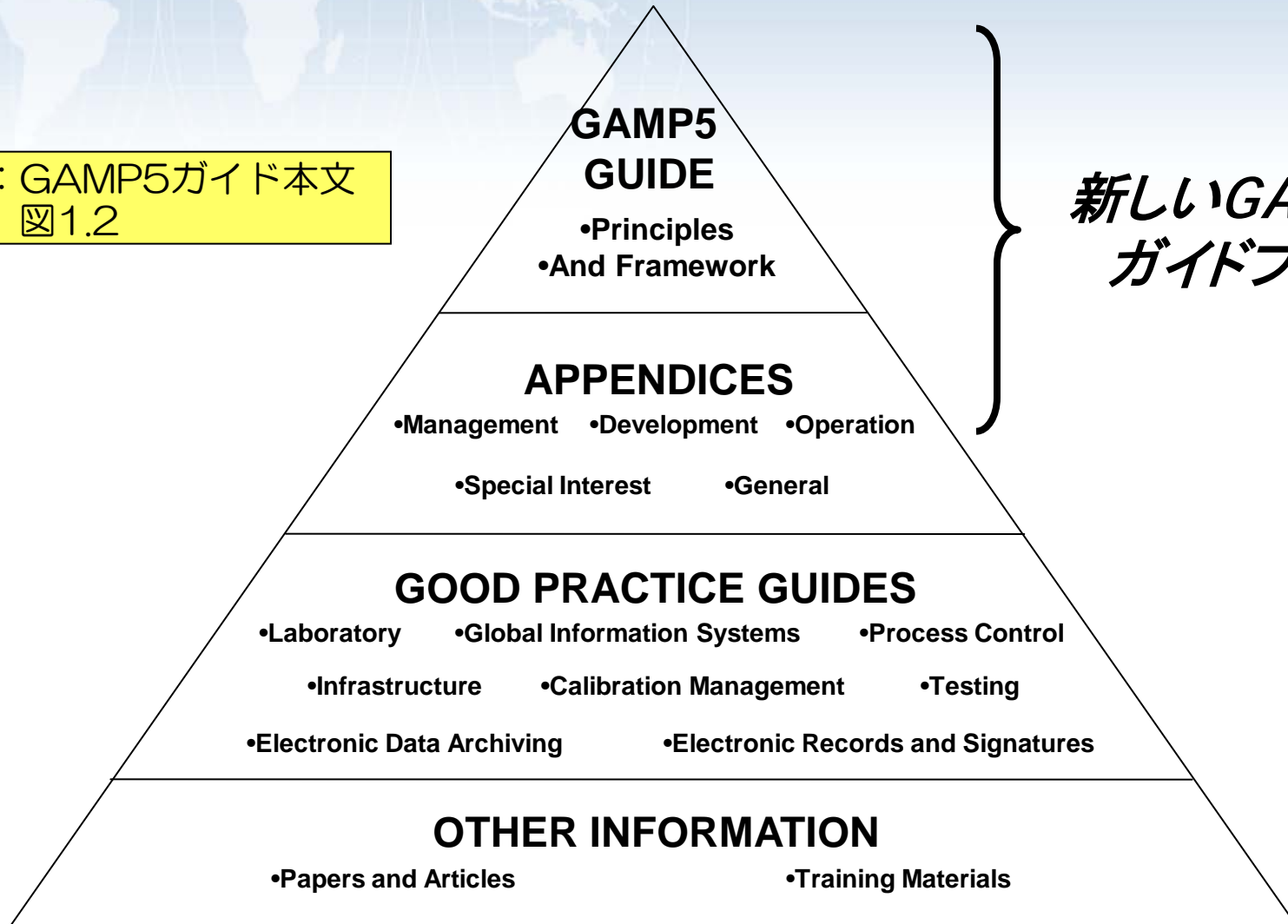
---

- ・ 医薬品製造に関係するコンピュータシステムのバリデーション(CSV)に関するガイドライン
- ・ 医薬品に関係する国際的なエンジニア団体であるISPE（本部は米国）傘下のGAMPフォーラム(GAMP COP)が発行
- ・ 最新版は2008年2月に発行
- ・ セキュリティ管理は付属資料O（運用）の11に記載



# GAMP5ガイドの概要⑥文書体系

出典：GAMP5ガイド本文  
図1.2



新しいGAMP5  
ガイドブック



---

2-1 厚生労働省ガイドライン

2-2 GAMP 5ガイド

2-3 GAMP 5のセキュリティ管理

2-4 GPG “ITインフラ”

# GAMP5付属資料011-①

- セキュリティ管理の対象は、組織が規制対象と判断するシステム、記録、およびプロセス
- セキュリティ管理は、以下を確実にするためのプロセス
  - 機密性(Confidentiality)
  - 完全性(Integrity)
  - 利用可能性(Availability)
- セキュリティ管理の効果
  - IT資産の保護
  - セキュリティ脆弱性が事業に与える影響やインシデントを最小限に抑制
- ISO17799の参照・活用も推奨



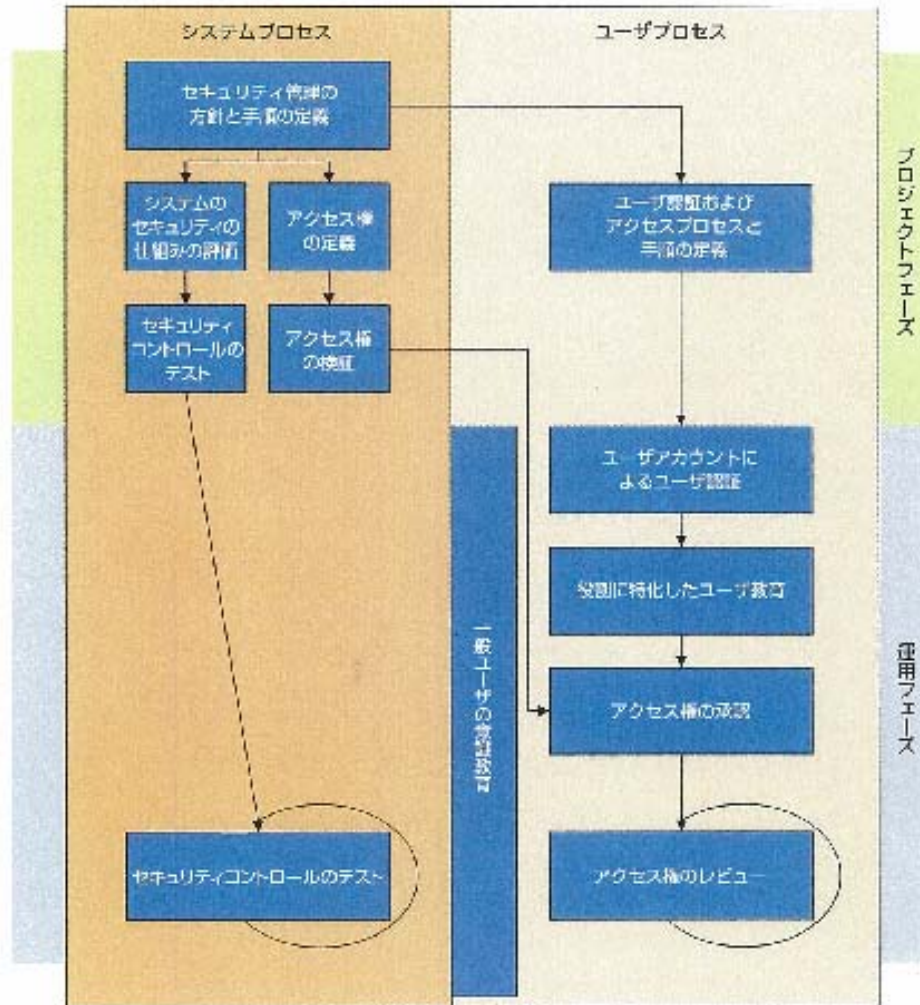
# GAMP5付属資料011-③（重要な要件）

- セキュリティ上の役割と責任、方針、基準、および手順の確立および保持
- セキュリティの監視と定期的なテストの実施
  - ・ システムのアクセスログの手作業でのチェック
  - ・ ロックアウトの自動通告
  - ・ トークンのテスト
- 特定されたセキュリティ上の弱点やインシデントに対する是正措置の実施
- システムへのアクセスを許可されている人員リストの作成・維持
- システムの物理的および技術的なセキュリティの仕組みの設計の評価
- （必要に応じた）テストの実施



# GAMP5付属資料011-④ (プロセス)

図011.1



# GAMP5付属資料011-⑥

## ・ 実施における原則

### － システムの影響度

- ・ 初期リスクアセスメントにより（患者の安全、製品の品質、データの完全性に対する）全体的な影響を決定
  - － プロセスの複雑性
  - － システムの複雑性、新規性、用途
- ・ システムの影響度に基づいて、プロセスオーナーは、運用時に支援対象となるプロセスと記録に対する適切なレベルの保護を提供する適正な管理を定義





# GAMP5付属資料011-⑦

## ・ 実施における原則

### － 従業員の意識

- ・ 企業は、効果的なコミュニケーションの実現と教育プログラムを通じて、従業員のコンピュータ化システムのセキュリティに対する意識を確立
- ・ 対象は、すべての従業員（常勤、パートタイム、および短期雇用契約者）のほか、システムへのアクセス権を持つ他の全ての人員
- ・ ライン管理者は、ユーザの活動は監視される場合があること、方針と手順に従わない従業員に対して処置の対象となることをエンドユーザに認識させる



# GAMP5付属資料011-⑩

## ● 実施における原則

### － 情報セキュリティに関する方針

#### ・ トピックスでカバーすべき項目

- － 物理的なセキュリティ
- － アクセスへの許可と取り消しを含むシステムへのアクセスのセキュリティ（ユーザIDの発行とパスワードの管理など）
- － 第3者機関のアクセス
- － 電子メッセージシステム
- － 共有のネットワーク資源
- － インタネットへのアクセスと使用
- － モバイルコンピューティング資源の使用（ラップトップコンピュータ、PDA、スマートフォン等）
- － 外部コンピュータシステムとの接続性
- － ウイルス対策方針
- － 侵入検知



---

2-1 厚生労働省ガイドライン

2-2 GAMP 5ガイド

2-3 GAMP 5のセキュリティ管理

2-4 GPG “ITインフラ”

# GPG「ITインフラ管理」③

## ～本文6. 3～

- 情報セキュリティの目的
  - 機密性：情報は権限のある要員だけがアクセス可能であることを保証
  - 完全性：情報の正確性と完全性、および処理方法の保護
  - 可用性：権限のあるユーザが、情報とその関連するリソースに必要なに応じてアクセスできることの保証
- 情報セキュリティ管理項目の例
  - セキュリティ事象管理
  - 侵入検知
  - サーバの強化（例えば、不要なアプリケーション・ツールの削除、および未使用ポートの閉鎖）
  - ウイルス定義ファイルの更新
  - ソフトウェア入手先の考慮（例えば、承認されているサプライヤから）
  - 災害復旧計画
  - ユーザアクセス管理



# GP G 「ITインフラ管理」 ー⑧

## ～付属文書6～

- 経営層の関与

- セキュリティプログラムの制定
- 管理部門や個人の配置
- セキュリティプログラムの監視

- 達成には、以下のコントロールが有効

- ・ 管理上のコントロール（方針、標準、手順、ガイドライン、セキュリティ啓発研修、事象管理等の作成を含む）
- ・ 技術的なコントロール（アクセスコントロールの仕組み、パスワードやリソースのマネジメント、特定と認証の方法、セキュリティ装置を含む）
- ・ 物理的なコントロール（施設や他の部門への個人アクセスの管理、システムのロック、ワークステーションから不要なドライブの除去、施設周辺の管理、侵入監視を含む）



# GPG「ITインフラ管理」⑪

## ～付属文書6～

- 脆弱性のマネジメント
  - 是正措置
    - ・ パッチの適用
    - ・ セキュリティ設定の変更
    - ・ ネットワークトポジーの利用
  - 現実的なアプローチ
    - ・ システム一覧表の作成
    - ・ 脅威の評価
    - ・ 優先順位の設定
    - ・ 優先順位に基づく分類
  - パッチの適用や修正の実施頻度
    - ・ 日次よりも週次・月次、または計画保全での実施が有効な場合が多い



# GPG「ITインフラ管理」①9

## ～付属文書6～

### ・ セキュリティ更新の互換性に関する問題点

- ・ セキュリティパッチは、通常限られたバージョン番号の製品のみ利用可能
- ・ 相互関連のあるソフトウェアのサプライヤが、互換性のあるバージョンを提供しないケース
- ・ バリデーションと可用性の要件がアップグレードのオプションへの制約条件となるケース
- ・ 重要なセキュリティパッチがインストールできないケースでは、望ましくない結果を生ずる可能性
  - システム管理者が、管理を運用に頼る
  - そのシステムを、他のシステムや企業のネットワークから隔離する



- ・ 企業のセキュリティ方針に、方策の概要を記述すべき



# 目次

---

1

医薬品製造の特徴

2

医薬品製造法規制とセキュリティ管理

3

セキュリティ管理への問いかけ





# ベンダーとユーザー

- ユーザーを一つの区分としてよいのでしょうか？
  - GAMP 5の提案である「プロセスオーナー」と「システムオーナー」に区分する方が現実的ではないか？
  - プロセスオーナー：アプリケーションシステムの運用・結果に責任をもつ人
  - システムオーナー：インフラストラクチャやアプリケーションシステムの維持に責任をもつ人
  - 小さなシステムでは、プロセスオーナーとシステムオーナーを同一人が担当する場合は存在⇒会社組織として全てのシステムを同一人が担当することは不適當
  - データセキュリティに関しては、だれが責任をもつか事前に決めることが重要



# ベンダーとユーザー

---

- ベンダーとユーザーの分類も今後は困難？
  - 業務のアウトソーシング（極端な場合が製造の委託・受託）
    - 中間工程の委託は？
  - ユーザ業務の外部リソースによる代行
    - SME（対象分野の専門家）
    - コンプライアンス業務のSMEの代行



# 説明責任

- セキュリティを含む各種管理業務では、「方針に従ってきちんと実行されている」と説明できることが重要ではないでしょうか？
  - 絶対的に実施・維持すべき事項が存在
    - ID・パスワードに関する従業員の教育
  - 現実的な管理の実施が必要な事項も存在
    - 完全な変更管理と試験プロセスを実施⇒ビジネス上のリスク
    - 変更管理や試験なしに直接・間接のパッチ適用を実施⇒コンプライアンス上の問題が発生



# リスクに基づく管理

- 説明責任をコストインパクト最小で実現するには、リスクに基づく管理が最も有効ではないでしょうか？
  - 方針管理へのリスクの明記
  - 客観的なリスク評価指標の策定
    - 固有技術の専門家との協調
  - 対象となるシステム一覧表の作成と維持
    - 80%や90%の一覧表は大幅に価値が低下



# 組織と体制

- セキュリティを含む各種管理業務では、「管理には一定のコストが必要」という認識をトップマネジメントが持つ、持たせることが基本ではないでしょうか？
  - 数年の運用期間全体でのコスト負担を想定
  - 方針に基づく手順の策定と、着実な実施
  - 体制がなければ、管理の維持は困難
  - 権限・組織・処遇の関係は？



# お問い合わせ先

ITエンジニアリング株式会社

〒221-0031 横浜市神奈川区新浦島町1-1-25

テクノロジー 100ビル

製薬ソリューション部

横井 昭彦 yokoi@ite.co.jp

TEL:045-441-9055, FAX:045-441-9130

URL: <http://www.ite.co.jp/>

