備考：医療機器の製造業者は、機器のインターフェースを IT ネットワークに接続することが意図する使用に含まれる場合、その接続方法に関する技術文書を提供する責任を担う。非医療用機器の製造業者に同様の義務はないが、そのような技術文書を参照するには、特別な措置を講じる必要があると考えられる。

医療用 IT 統合リスク管理者の選定に当たり、責任組織は、医療用 IT 統合リスク管理者がその責任を果たす上で必要な訓練と経験を有することを確認しなければならない。

医療用又は非医療用機器の製造業者もしくはその他の組織から提供されたリスト掲載の文書に加え、それらの製造業者又は組織の協力が必要な場合、責任協定は以下のことを行う。

a) 必要な協力の性質を明確にする。

b) 以下の内容を明示する。

— そのような協力要請の責任者

— そのような要請に対する回答の責任者

— その回答の妥当性を判断するための基準

6.3 IT ネットワークリスクマネジメントファイル

一つまたは複数の医療機器の組み入れを検討中の特定 IT ネットワークについて、責任組織は、IT ネットワークリスクマネジメントファイルを作成し、その保守を行う。

この規格の他の条項の要件に加え、IT ネットワークリスクマネジメントファイルは、特定された個々のハザードについて、以下の作業を行う際にトレーサビリティを提供する。

a) リスク分析

b) リスク評価

c) リスクコントロール手段の実施及び検証

d) 幹部の承認を受けた残留リスクの受容性の評価

備考 1：IT ネットワークリスクマネジメントファイルを構成する記録及びその他の文書は、必要な場合、その他の文書及びファイルの部分を構成することができる。IT ネットワークリスクマネジメントファイルは、全ての記録及びその他の文書を物理的に含んでいる必要はないが、最低でも、必要な全ての文書のリファレンス又はポインタを含むものでなければならない。責任組織は、IT ネットワークリスクマネジメントファイルに引用された情報をタイムリーに収集できなければならない。

備考 2：IT ネットワークリスクマネジメントファイルは、どのような形式又はタイプの媒体にも保存することができる。

附属書 A
（参考）

リスクマネジメント関係の概要

医療機器の IT ネットワーク統合に伴うリスクマネジメントの実施に関わるさまざまな役割及び関係を図 A.1 にまとめた。

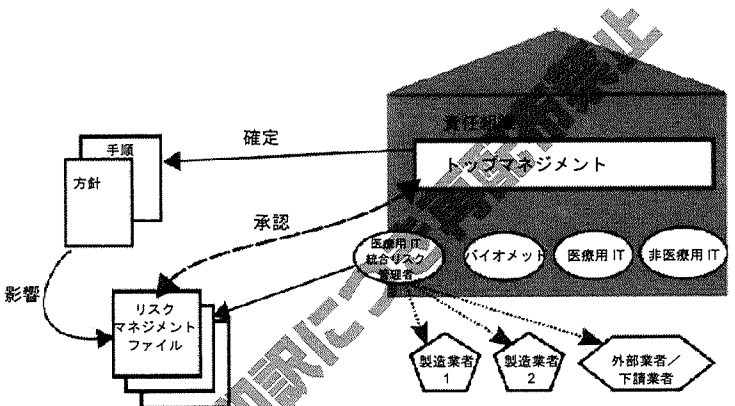

図 A.1— リスクマネジメントの実施に関わるさまざまな役割と関係の概略

附属書 B
（参考）

Recommended references

Standards

DICOM	*Digital Imaging and Communications in Medicine (DICOM)* National Electrical Manufacturers Association. http://medical.nema.org/dicom/
IEC 60300-3-9	*Dependability management – Part 3-9: Application guide – Risk analysis of technological systems*
IEC 60601-1:2005	*Medical electrical equipment – Part 1: General requirements for basic safety and essential performance*
IEC 60601-1-6:2006	*Medical electrical equipment – Part 1-6: General requirements for basic safety and essential performance – Collateral standard: Usability*
IEC 60601-1:2005	*Medical electrical equipment – Part 1-8: General requirements for basic safety and essential performance – Collateral standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems*
IEC 61907:—	*Guidance on communication network dependability engineering*
IEC 62304:2006	*Medical device software - Software life cycle processes*
IEEE 610.12:1990	*IEEE Standard Glossary of Software Engineering Terminology*
ISO/IEC Guide 51:1999	*Safety aspects – Guidelines for their inclusion in standards*
ISO 13485:2003	*Quality management systems -- Requirements for regulatory purposes*
ISO/DTS 29321:—	*Health informatics: Application of risk management to the manufacture of health software*
ISO/DTR 29322:—	*Health informatics: Guidance on risk evaluation and management in the deployment and use of health software*
ISO/TS 25238:2007	*Health informatics – Classification of safety risks from health software*
ISO/TR 27809:2007	*Health informatics – Measures for ensuring patient safety of health software*
ISO 9000:2000	*Quality management*
ISO 9000:2005	*Quality management systems – Fundamentals and vocabulary*

Organizations

NSA	USA National Security Agency NSA Security Configuration Guides http://www.nsa.gov/snac/
IETF	The Internet Engineering Task Force Papers; Network Working Group RFC 2246 January 1999: *The TLS Protocol Version 1.0.* http://www.ietf.org/rfc/rfc2246.txt
SANS	The SANS (SysAdmin, Audit, Network, Security) Institute http://www.sans.org The SANS Security Policy Project – "…everything you need for rapid development and implementation of information security policies." http://www.sans.org/resources/policies/ SANS Information *Security Reading Room* http://www.sans.org/rr/
WEDI	Workgroup for Electronic Data Interchange Security and Privacy Workgroup (SNIP) White papers: WEDI-SNIP Introduction to Security Final Rule Final Version – January 2004 *http://wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/S-411_Final-Finel_Rule.pdf* WEDI-SNIP SECURITY: Audit Trail Clarification White Paper Version 5.0 November 7, 2003 http://wedi.org/snip/public/articles/dis_viewArticle.cfm?ID=25&wpType=2
IHE	Integrated Healthcare Enterprise http://www.ihe.net/Technical_Framework/ IHE ATNA profile Audit Trail and Node Authentication IHE EUA (Enterprise User Authentication) IHE RAD TF (*Radiology Audit Trail)* draft version for public comment.

Bibliography

[1] IEC 60601-1:2005, *Medical electrical equipment – Part 1: General requirements for basic safety and essential performance*

[2] IEC 61907:—[3], *Guidance on communication network dependability engineering*

[3] IEC 62304:2006, *Medical device software, Software life-cycle processes*

[4] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[5] Global Harmonization Task Force (GHTF) – Study Group 1 (SG1), Document No. N029R11, dated 2 Feb., 2002.

3) 後日出版予定

規制プロセス用ソフトウェアの検証

作成： 米国医療計測機器振興協会
承認日： 年 月 日
承認： 米国医療計測機器振興協会

抄録： この技術情報レポート（TIR）は、機器の設計、検査、コンポーネントアクセプタンス、製造、ラベル表示、包装、流通、及び苦情処理の自動化、又は品質システム規則（21 CFR 820）に規定された品質システムに関するその他の部分の自動化に使用されるソフトウェアに適用する。また、電子記録の作成、修正、及び保守に使用するソフトウェア、及び検証に関する要件（21 CFR 11）の対象となる電子署名の管理に使用されるソフトウェアにも適用する。この TIR は、FDA の規制対象となるプロセスをソフトウェアで自動化する場合にも幅広く適用することができる。この TIR は、機器製造業者の品質システムのインプリメンテーションに使用される機器及びソフトウェアの製造に使われるソフトに適用する。医療機器又はそれ自体が医療機器であるソフトウェアのコンポーネント、部品、又はアクセサリーとして使われるソフトには適用しない。

キーワード：医療機器ソフトウェア、医療用電気機器、医療用電子機器、リスクマネジメント

SWN023

無断複製および再配布禁止

発行：
米国医療計測機器振興協会（Association for the Advancement of Medical Instrumentation）
1110 N Glebe Road, Suite 220
Arlington, VA 22201-4795

アメリカ合衆国にて印刷

ISBN x-xxxxx-xxx-x

AAMI 技術情報レポート

技術情報レポート（TIR）は、医療技術の特定分野に関する情報を提供する米国医療計測機器振興協会（AAMI）規格委員会の出版物である。

TIR に記載された内容はさらに専門家の評価を受ける必要があると考えられるが、業界及び医療従事者が至急必要とするものであることから、情報を提供することは有意義である。

規格から推奨案に至るまで、TIR の内容は様々であるが、読者はこれらの文書の違いを理解することが望ましい。

規格及び推奨案は、委員会の承認、公開レビュー、及び全コメントの決議の正式なプロセスを経る。この合意プロセスは、AAMI 規格委員会並びに、米国標準規格の場合、米国規格協会が監督する。

TIR は、規格と同じ正式な承認プロセスを経るものではない。ただし、TIR の配布には技術委員会及び AAMI 規格委員会の承認を必要とする。

もう一つの相違点として、規格及び TIR はいずれも定期的に見直しが行われるが、規格は、再確認、改訂、又は廃止の決議を経なければならず、通常は 5 年毎、少なくとも 10 年毎に決議の正式な承認が行われる。TIR に関して、AAMI は出版日から約 5 年後（及び以降は定期的）に、文書が有用か否かについて技術委員会と協議を行い、情報が関連性又は歴史的価値を有するものかどうかを確認する。情報が有用でない場合、TIR は配布から除外される。

規格又は推奨案よりも根本的な安全性又は性能の問題に対処するという理由、若しくは合意の達成が極めて困難または可能性が低いという理由で TIR が作成されることもある。規格と異なり、TIR は技術的な問題に関して相違する見解を含めることができる。

注意事項：この AAMI 技術情報レポートは、随時、改訂又は廃止することができる。急成長の分野又は技術に関する問題を取り扱うため、読者はこの文書よりも新しい情報についても考慮するように努めなければならない。

この技術情報レポートに対するコメントは AAMI まで。宛先は Standards Dept., 1110 N. Glebe Road, Suite 220, Arlington, VA 22201-4795。

SWN023

目　次

購入申請中の為閲覧不可禁止

同等規格の用語集

委員会代表者

米国医療計測機器振興協会

AAMI 医療機器ソフトウェア委員会

この技術情報レポート（TIR）は、AAMI 医療機器ソフトウェア委員会が作成した。委員会による TIR の承認は、必ずしも委員会のメンバー全員が承認投票を行ったことを意味するものではない。

この文書の発行時点における AAMI 医療機器ソフトウェア委員会のメンバーは以下の通り：

会長： Sherman Eagles
John Murray

メンバー： Randy Armstrong, Cyberonics Inc.
David R. Christie, Spacelabs Medical Inc.
Theresa Dennis, Sterigenics International
Andrew Dunham, Baxter Healthcare Corp.
Sherman Eagles, Medtronic Inc.
Christine Flahive, Belle Mead, NJ
Larry Fry, Draeger Medical
Nancy George, Towson, MD
Ron Gerner, Abbott Laboratories
Steven Gitelis, GB Lumina Inc.
Lori Haller, Steris Corp.
James Hempel, Covidien
Sam Jarrell, CerTech LLC
Jeremy Jensen, Boston Scientific Corp.
David R. Jones, Philips Medical Systems
Martin L. King, Hospira Inc.
Alan Kustnitz, Software CPR
Bernie Liebler, Advanced Medical Technology Association （AdvaMed）
Don Lin, Irvine, CA
Steve Mallory, Welch Allyn Inc.
Mark Maritch, Draeger Medical
Don McAndrews, Respironics Inc.
Mary Beth McDonald, St. Jude Medical
Dennis Mertz, Becton Dickinson
John F. Murray, Jr., U.S. Food and Drug Administration
Raj Raghavendran, Johnson & Johnson/Ethicon Endo-Surgery
Bill Riley, Hill-Rom Company
Harvey Rudolph, Underwriters Laboratories Inc.
Richard Schrenker, Massachusetts General Hospital
Xianyu Shea, Stryker Medical Division
Carla Sivak, Edwards Lifesciences
Scott Thiel, Roche Diagnostics Corp.
Ann Vu, Bausch & Lomb Inc.
James Webb, Cardinal Health

Andrew Whitman, National Electrical Manufacturers Association （NEMA）
Gregory Whitney, CR Bard

代理人： Aziz Bhai, Hill-Rom Company
Christopher P. Clark, Bausch & Lomb Inc.
Rich Eaton, National Electrical Manufacturers Association （NEMA）
Christopher Ganser, CR Bard
Jeff Gilham, Spacelabs Medical Inc.
Steve Hellstrom, Hospira Worldwide Inc.
Denise Stearns Holliman, Boston Scientific Corp.
Gene Kelly, CerTech LLC
Patricia Krantz, Medtronic Inc.
Gretel Lumley, Philips Medical Systems
David Michel, Steris Corp.
Dewey Phan, Becton Dickinson
Rodney Rasmussen, Abbott Laboratories
Miguel Rodriguez, Johnson & Johnson/Cordis
Robert Smith, St. Jude Medical
Donna-Bea Tillman, U.S. Food and Drug Administration

謝辞

AAMI 医療機器ソフトウェア委員会は、この TIR 作成を担当した規制プロセス用ソフトウェア検証作業部会の尽力に謝意を表したい。この作業部会のメンバーは以下の通り。

会長： Denise Stearns Holliman
Steve Gitelis

メンバー： Mark Allen, Bonfils
Barbara Beiersdorf, Medtronic, Inc.
Paul Brown, Medtronic, Inc.
Steve Gitelis, GB Lumina Inc.
Denise Stearns Holliman, Boston Scientific Corp.
Rich Hall, Lilly
Jeremy Jensen, Guidant/Boston Scientific Corp.
Lisa Last Hewitt,
John Murray, U.S. Food and Drug Administration
Frank Scavo, Strativa
David Vogel, Inea
Carl Wyrwa, Beckman

この文書作成に協力頂いた以下の方々に特別な謝意を表したい。Debbie Iampietro, Jennifer V. Anderson, and Kathleen O'Donnell

注記：この推奨案の作成に連邦政府関係機関の代表者が参加したことは、連邦政府又はその関連機関の承認を法的に裏付けるものではない。

緒言

これまでの検証の取り組みにおいて、“付加価値のある（value-added）”及び“ソフトウェア検証（software validation）”の表現は相互排除的になってしまう傾向があった。ソフトウェア検証が付加価値を持つ場合もあれば、持たない場合もあった。果たして、従来のアプローチは意図する使用に即したソフトウェアの性能を本当に確保できているのだろうか。“検証済み”のソフトウェアが配備されたものの、ユーザーが期待する性能を発揮できていない例はどれくらい発生しているのか。

ソフトウェア検証の活動から最大限の価値を引き出すことが重要である。結局、あなた又はあなたの会社は検証の取り組みに貴重な資源を費やしているのであり、その投資に見合った利益を享受することが特に重要である。

では、ソフトウェア検証の活動から期待通りの価値を引き出せていないと感じる人がいるのはなぜだろう。この要件を満たすのには相当な努力が必要と感じる人がいるのはなぜだろう。ソフトウェア検証の活動が仕事上の目的や利益と一致しないと感じる人がいるのはなぜだろう。クオリティの高い既製のソフトウェアを使うとき、内部でのソフトウェア検証の活動が余計だと感じる人がいるのはなぜだろう。ほとんど又はまったく何もしない人がいるのはなぜだろう。検証が必要なソフトウェアと検証が不要なソフトウェアの区別が曖昧なのはなぜだろう。

規制プロセス用ソフトウェアの検証に関するこの技術情報レポートは、上記の疑問の背景にある問題を読者に理解してもらい、より付加価値の高いソフトウェア検証のアプローチを開発するための提案を行うことを目的としている。

ソフトウェア検証を要件とする医療機器の規制は存在することに留意すべきである。規制のセクション 21 CFR 820.70（i）自動化プロセス（Automated Processes）は、あらゆる医療機器製造業者に適用できるように広義の言葉で書かれている。このセクションは、解決すべき問題又は達成すべき目標を明確にしているが、この問題をどのように解決し、この規制要件の意図にどうやって従うかについて、いかなる情報も提供していない。この話題に関して FDA が提供しているその他の具体的な情報は、ソフトウェア検証の一般原則；業界及び FDA スタッフ向け最終ガイダンス（GPSV：General Principles of Software Validation; Final Guidance for Industry and FDA Staff）に記載されている。ソフトウェア検証の一般原則（General Principals of Software Validation）のセクション 6 には、自動化プロセス機器及び品質システムソフトウェアの検証に関するガイドラインが掲載されている。

このレポートは、新たな方向性を確定するものではないが、医療機器業界の視点からこの問題を捉え、業界内で既に慣行となっている事柄について説明している。付加価値を生むやり方で規制に準拠する方法について業界がどのように考えているのか、その理解を深めるために一歩前進することが目標である。

これまで、多くの慣行がコンプライアンスの必要性に基づくチェックリスト志向のアプローチへと発展してきた。そして、これが思わぬ原因となり、意図するソフトウェアの性能を適切に具体化する付加価値の活動から逸脱してしまうこともある。このような事態が起きるのは、目的や要件がそれぞれに異なる多数の利害関係者を一つのソリューションで満足させようとするような場合である。これらの利害関係者は、品質システムのインプリメンテーション、規制上の必要性、エンジニアリングの慣行、監査及び評価の要件、ビジネス及び法的な必要性、コンサルティングサービスなど、それぞれに重視する点が異なるさまざまな見解の持ち主である。

主な課題の一つとして、すべての利害関係者、特に検証を実施する担当者と検証の妥当性を評価する監査役のニーズに即したソリューションを見つけ出すことが挙げられる。要するに、製造業者は、リスクマネジメント、クオリティ及びエンジニアリングの分野でベストプラクティスとして相当の注意を払い、この規制要件を満たすだけでなく、規制の意図に即したソリューションを創造することが期待される。

このレポートの意図は、ソフトウェア検証の任務に適用可能な概念及びツールを認識してもらうことである。まず最初に、このレポートの基本概念を理解してもらうための単純なアナロジーを紹介したい。大工のツールボックスには、ハンマーやレンチ、ドライバー、ドリルなど、多種多様なツールが入っている。大工が仕事に臨むとき、安全かつ効果的に任務を遂行するために適切なツールを選択する。例えば、板に釘を打つときは、レンチやドライバーではなく、ハンマーが最も適切なツールと考えられる。また、ユーザーの状況に応じて正しいタイプのハンマーを選ぶことも重要だ。大型のハンマーでもこの仕事をこなせるかも知れないが、板が傷つく可能性があり、釘を打つ板の数が多ければ、ユーザーは疲労困憊してしまうだろう。しかし、ツールボックスに大型のハンマーしか入っていないのなら、大工はその不適切なツールを選ばざるを得なくなる。

大型ハンマーの比喩は、すべての規制プロセス用ソフトウェアに 1 セットのツールを使用した“フリーサイズ型”の検証を示すものであり、批判的思考を採用しない場合の例である。大型ハンマーを使うのと同じように、このタイプの検証も遂行可能だが、常に付加価値を創造するとは限らないという代償を伴う。また、特定できないリスクを適切に予防できない可能性もある。つまり、フリーサイズ型チェックリストのような思考態度は、単純な低リスクのソフトウェアには仕事が過剰であり、複雑な高リスクのソフトウェアに必要な仕事は不足してしまう。

検証が必要なソフトウェアは、多種多様な意図する使用のために、多種多様なシナリオで、多種多様なリスクを伴って使われると考えられる。このように多種多様な状況で最適な検証を実現するためには、各種のツールと関連するアプローチが必要である。

このレポートは、ツールボックスの中から最適なツールを選ぶことで、批判的思考を応用してソフトウェア検証のアプローチを決定し、ビジネスの要件に準拠し、かつ矛盾しない付加価値のあるソリューションを実行する方法について提案を行う。

ソフトウェア検証の取り組みが大成功とみなされるためには、以下の条件に従うことが望ましい。

- 自動化プロセス又は関連ソフトウェアの意図する機能が、機器の安全性、クオリティ、及び品質システムの完全性を損なわない。
- 必要な活動を実行する人が、その努力は有意義でやり甲斐がある（重荷にならず、大きな価値のある活動）と信じている。
- 製造業者がコンプライアンス（法令遵守）の状態にある。
- 監査役及び検査員が、適用される活動及び結果の記録を容認できるコンプライアンスの証拠とみなしている。

はじめに

この技術情報レポート（TIR）は、批判的思考を応用したリスクベースのアプローチを使って規制プロセス用ソフトウェアの検証に適切な活動を決定する際に、読者を支援する目的で作成されている。

このレポートは、医療機器業界でこの種のソフトウェア検証の実施を担当し、監査の対象となる文書作成の任務を担う人たちの経験をまとめた努力の成果である。作成に当たり、何をすべきか、どれくらいやれば十分か、リスク分析をどのように活用するかなど、規制プロセス用ソフトウェアの検証を行う際に我々みんなが経験する疑問や問題を考慮している。この TIR の作業部会は、十分な話し合いの後、すべてのケースで活動のセット（ツールボックスの中から選ぶツール）を特定し、意図する使用に応じて処理を実行するソフトウェアの能力がどの程度信頼できるかを示すことにした。ところが、ソフトウェアの複雑さや危害のリスクが影響する程度、及び業者供給ソフトウェアの系統（例：クオリティ、安定性）などの要因によって活動のリストに違いが生じた。

完成したレポートには、次に挙げる二つの主な要素が含まれている。

- 批判的思考を応用して規制プロセス用ソフトウェアの検証で何を遂行すべきかを明確にする方法。この方法には、ソフトウェアの欠陥が危害をもたらす可能性を考慮するリスクベースのアプローチが含まれる。
- 意図する使用に即してソフトウェアが処理を実行する際に十分なレベルの信頼性を実現するために使用可能なツールを集めたツールボックス。それらのツールが、経験により何が有効で何が無効かを理解した上で採用されていることに留意すべきである。このツールボックスは、ソフトウェアエンジニアリングの優良実施に関する現行の知識を象徴するものである。さらに経験を積み、テクノロジーが進化するのに伴い、有効なツールは進化し、ツールボックスの内容も変わるだろう。

SWN023

規制プロセス用ソフトウェアの検証

1 総則

1.1 目的及び意図

この TIR の目的は、規制プロセス用ソフトウェアに応用される検証作業の適切な内容及び規模を決定する際に考慮すべき事柄について指標を提供することである。さらにこの TIR は、ソフトウェア及びその環境のさまざまな側面を分析し、評価することで、適切な深さ及び厳格さを備えた活動を実現するための方法についても指標を提供する。この TIR は、さまざまな状況への批判的思考の応用について説明、定義、及び例示を行うことで、この方法を定義することを意図している。

この TIR は、新たな FDA 承認の検証作業及び文書の最低限のセットを作成することを意図するものではない。AAMI の TIR は“ベストプラクティス”の集合であり、この文書は規制プロセス用ソフトウェア検証のベストプラクティスに対する作業部会の集合的な判断を反映するものである。

1.2 適用範囲

この TIR は、機器の設計、検査、コンポーネントアクセプタンス、製造、ラベル表示、包装、流通、及び苦情処理の自動化、又は品質システム規則（21 CFR 820）に規定された品質システムに関するその他の部分の自動化に使用されるソフトウェアに適用する。また、電子記録の作成、修正、及び保守に使用するソフトウェア、及び検証に関する要件（21 CFR 11）の対象となる電子署名の管理に使用されるソフトウェアにも適用する。この TIR は、FDA の規制対象となるプロセスをソフトウェアで自動化する場合にも幅広く適用することができる。

この TIR は以下に適用される。

- 機器の製造に使われるソフトウェア
- 機器製造業者の品質システムのインプリメンテーションに使われるソフトウェア

この TIR は以下に適用されない。

- 医療機器のコンポーネント、部品、又はアクセサリーとして使われるソフトウェア
- それ自体が医療機器であるソフトウェア

この TIR は以下の者に有用な情報及び勧告を提供する。

- 検証作業の適切な内容及び規模の決定責任者

- 内容/規模の決定を推進する分析及び評価の実施責任者
- 検証活動の計画及び実施責任者
- 検証作業の妥当性の審査及び承認責任者
- 規則遵守に関する検証の監査、検査及び評価担当者

この TIR では、品質システム規則の一般規定をどのようにして規制プロセス用ソフトウェアに適用するかを検討し、このソフトウェアを評価するためのアプローチについて説明する。ただし、法律への適合に必要な作業及び活動のリストは掲載していない。この TIR は、何らかの者に何らかの権利を創造又は付与するものではなく、ユーザーを拘束する働きをするものでもない。適用可能な法律、規則、又は両方の要件を満たすアプローチであれば、代替のアプローチを利用することができる。この TIR が特定の手法又は特定の評価テクニック若しくは方法を要求したり、提案することはない。責任者は、ソフトウェアプロジェクトごとに、具体的なアプローチ、採用するソフトウェアリスクマネジメント活動の組合せ、及び適用する努力のレベルを決定し、その根拠を示すことが望ましい。医療機器の品質管理システム及びそれらのシステムに適用される規則について具体的なトレーニング又は経験を積むことが推奨される。

1.3 文書構成

この文書は、本体と 5 つの付録で構成されている。本体は p.16 から p.41 までの 26 ページにわたり、以下の内容を記載している。

- 規制プロセス用ソフトウェアの検証のためのコンテキスト
- 批判的思考の概念及びソフトウェア検証との関係
- 一例として単純化されたウォーターフォールプロセスを採用したソフトウェアライフサイクル内における批判的思考の応用
- 批判的思考及びソフトウェアライフサイクルのサポートに必要なシステム及びプロセス

五つの付録には以下の情報が含まれる。

- 付録 A は、文書全体にわたってツールボックスとして参照され、各種ツール、又は信頼醸成活動に関する詳しい情報を掲載する
- 付録 B は、リスクモデル例を含むリスクマネジメントの簡単な考察である。
- 付録 C は、複雑さ、系統、及びリスクのレベルが異なる場合など、さまざまな状況でどのようにして規制プロセス用ソフトウェアの検証に批判的思考を応用できるかを示した例を掲載している。
- 付録 D 及び E は、定義及びリファレンスを掲載している。

2 規制のコンテクスト

このセクションの情報は、この TIR を現行の規制及び指針書のコンテクストと照合することを意図している。このセクションの意図は、TIR の情報を以下の参考資料との関連で位置づけ、この情報に関する作業部会の現在の理解又は解釈を示すことである。

規制プロセス用ソフトウェアの検証に関する完全なコンテクストを確定するいくつかの規制要素が存在する。その例を以下に示す。

- 品質システム規則（QSR）、21 CFR 820.70（i）自動化プロセスの詳細セクション
- 品質システム規則（QSR）、21 CFR 820 に定義された品質システムの一般的概念
- 21 CFR 11 の特定ガイダンス
- FDA ソフトウェア指針書、セクション 6 “Validation of Automated Process Equipment and Quality System Software（自動化プロセス機器及び品質システムソフトウェアの検証）” の詳細ガイダンスを含む一般ガイダンス “The General Principals of Software Validation（ソフトウェア検証の一般原則）”

以下のセクションでは、これらの規制要素のコンテクストについて順に説明する。

2.1 21 CFR 820.70（i）のコンテクスト

21 CFR 820.70（i）自動化プロセス

“コンピュータ又は自動データ処理システムを生産又は品質システムの一部として使用する場合、製造業者は、コンピュータソフトウェアを検証し、その意図する使用が確定されたプロトコルに準拠しているかどうかを確認しなければならない。すべてのソフトウェア変更は、承認及び発行の前に検証されなければならない。これらの検証作業及び結果は文書に記録されなければならない。”

このコンテクストについて考える際、以下の疑問を慎重に検討しなければならない。

- なぜこの規則が存在するのか
- この規則の意図は何か
- 我々が解決しようとしている問題は何か
- 我々がプロセスの自動化に使用するソフトウェアに関与する理由は何か
- 我々がこのタイプのソフトウェアを検証しなければならない理由は何か

作業部会では、ソフトウェアが製品の安全性又は品質に悪影響を与えない一定の信頼レベルを確立するために規制が存在するものと理解している。ソフトウェア障害に起因する悪影響として、欠陥製品の発売又は苦情データの不適切な傾向把握により欠陥

製品の使用現場での作業実行の必要性を特定できないことなどが挙げられる。さらに作業部会では、ソフトウェアをプロセスに導入したり、プロセスで使用中の既存ソフトウェアを変更したり、単純に既製のソフトウェアを追加使用するような場合、我々が悪影響のリスクを考慮し忘れないために規制が存在するものと考えている。プロセスの一部を自動化するためにソフトウェアを導入すれば、それはプロセスに不可欠な部分となる。人材やツール、ソフトウェア、材料など、プロセスを構成するすべての部分には、プロセスにリスクの要素をもたらす潜在的な可能性があり、危害のリスクを評価する際はそのことを十分考慮しなければならない。

関係者は、ソフトウェアを利用してプロセス又はプロセスの一部を自動化することを決定する際、自分たちがどのような状況に足を踏み入れようとしているのかを徹底的に理解する必要がある。つまり、ソフトウェア及びそれが自動化するプロセスで必要レベルの信頼を獲得するために、最も有効な方法を見つけ出すことが重要である。

作業部会では、以下を考慮することが規制の意図と理解している。

- ソフトウェアは全体的なプロセスにうまく適合するか
- ソフトウェアは何をするものか
- ソフトウェアが正常に動作しているかどうかをどのように判断するか
- ソフトウェアによって自動化されるプロセスにどのような潜在的リスクがあるか
- それらのリスクを許容可能なレベルで管理するにはどうすればいいか

2.1.1 21 CFR 820.70（i）の説明

規制要件の理解を助ける目的で、各セクションの主旨に関する作業部会の見解を検討しながら、規制の表現について以下に説明する。

“automated data processing systems（自動データ処理システム）”：従来は紙を使って手作業で実行されていたが、現在はコンピュータソフトウェアを利用して自動化されているプロセスのこと。この用語は、製造工程自動化と混同される場合もある。実際、この用語は製造工程自動化の上位集合であり、それには品質システム活動を実行するプロセスも含まれる。

“used as part of production or the quality system（製造又は品質システムの部分として使用）”：製造フロアシステム、CAPA システム、文書作成・管理システム、苦情処理システム、製品トレーサビリティシステム、及び優先業者システムなど、各種システムにソフトウェアが使用されることを意味する。

“shall validate computer software（コンピュータソフトウェアを検証しなければならない）”：ソフトウェアの信頼を確立するために必要なあらゆる仕事を意味する。規制コンテクストの要素及びこの TIR で定義されている通り、検査に限定されない。

“for its intended use（意図する使用のために）”：要件の公式声明及びプロセスの明確な定義を意味する。これには、ソフトウェアを使って何をするのかを理解していることが必要となる。

“according to an established protocol（確定されたプロトコルに準じて）”：“protocol（プロトコル）”の用語は、医療業界でもさまざまな意味で使われているが、ここでは“計画”を意味する。つまり、検証の計画は、承認された正式な文書でなければならない。

“All software changes shall be validated（すべてのソフトウェア変更は検証されなければならない）”：検証を一回限りのものとみなすのは不十分であり、ソフトウェアの使用期間を通じて継続されるライフサイクル活動の一つとみなす必要があることを意味する。

“These validation activities and results shall be documented（これらの検証作業及び結果は文書に記録されなければならない）”：検証の結果は合理的かつ容易に監査が行われなければならないことを意味する。

2.2 品質システム規則（QSR）– 21 CFR 820 のコンテクスト

ISO 13485、ISO 9000、及び 21 CFR 820 など、すべての正式な品質システムには、各品質システムのプロセスが意図する使用に適合しなければならないという基本的な仮定条件がある。例えば、顧客の苦情管理プロセスは、品質システムによって規定されたすべての要件に適合するものと考えられる。内部監査は、意図する使用に準じて、プロセスがこれらの要件を満たしていることを確認する目的で行われる。製造工程には、製品の製造に使われる前に検証されるべき明確な要件がある。しかし、QSR には、導入前に品質システムのプロセスを検証しなければならないという要件は明記されていない。従って、品質システムのプロセスをソフトウェアで自動化する場合に混乱が生じる。ソフトウェアだけを検証すべきなのか。それとも、ソフトウェアを使ったプロセスを検証すべきなのか。QSR の内容は、ソフトウェアが機能するだけでなく、品質管理プロセスそのものが機能して、規制又は会社の義務を果たすことを意味する。

2.3 21 CFR 11 のコンテクスト

<u>21 CFR 11.10 及び 21 CFR 11.10（a）には、以下の内容が記載されている。</u>

「電子記録データの作成、修正、保守、又は送信用システムを使用する者は、（中略）電子記録データの確実性、完全性、及び機密性（該当する場合）を確保するための手順及び管理を採用しなければならない。そのような手順及び管理には、（中略）正確性、信頼性、意図と一致する性能、及び無効または変造データの識別能力を確保するためのシステムが含まれなければならない。」

この規則に規定された検証要件は、医療機器述語規則 21 CFR 820.70 (i) に明記された検証要件と重複する。また、QSR には、品質記録データが正確かつ有効なものでなければならず、権限を有する者が規制された活動を行う責任を担うという要件も記載されている。このことは、規制プロセス用ソフトウェアに規則で定義された電子記録データ、電子署名、又は両方を組み込む場合、ソフトウェアにも繰り越して適用される。この TIR には、この述語規則に関する内容が含まれているため、特に指定がない限り、21 CFR 11 の検証要件を示す。正確かつ有効な電子記録データを確保するための詳細な計画及び電子署名の実行に関する内容は、この TIR に含まれていない。

2.4 “ソフトウェア検証の一般原則、FDA 及び業界向け最終ガイダンス（GPSV）”のコンテクスト

GPSV は、ソフトウェアエンジニアリング及びリスクマネジメントの観点から、ソフトウェア検証にとって良好な基礎をもたらすものと、作業部会は認識している。この TIR は、品質システムの観点から見たソフトウェア検証の実践的ガイダンスを伴う基礎に基づいており、検証活動を“デューデリジェンス（相当な注意）”の一形態とみなしている。

GPSV の数多い基本要素の一つは、（医療機器の安全性又は有効性に関する）ソフトウェアのリスクが検証努力の厳密性を高め、ソフトウェアの開発及び認定期間中に信頼醸成活動を完了すべきであるという概念である。これらの概念は、GPSV 文書でも繰り返し登場する。GPSV セクション 1 から 5 は、医療機器に含まれるソフトウェア又はそれ自体が医療機器であるソフトウェアに適用されることを意図している。GPSV セクション 6 は、自動化プロセス用のソフトウェアに関する内容である（この TIR と同じトピック）。これは、規制プロセス用ソフトウェアに何が適しているかを評価した資料の GPSV セクション 1 から 5 に定義されたものと同じレベルのライフサイクル管理及びリスクマネジメントの概念を適用する必要性を示している。この TIR の内容は、何が適切かの判断を支援する方法を定義するものである。GPSV が、製造又は品質システムの一環としてのソフトウェアの開発及びインプリメンテーションにおいて、ソフトウェア検証の基本原則（ガイダンスセクション 1-5）が重要であることを強調している点に留意すべきである。GPSV は、ソフトウェア検証を定義するものであり、この TIR の次のセクションでソフトウェア検証の定義について考察するための基礎となる。

3 ソフトウェア検証の考察

3.1 定義

FDA の規則及び関連ガイダンスにおいて、ソフトウェア検証の用語は、ソフトウェアがその意図する使用に適しているという結論に到達するまでの活動全般を網羅して広く使われている。例えば、ソフトウェア検証の一般原則には、以下のような記載がある。

“ソフトウェアが検証されたという結論は、ソフトウェア開発のライフサイクルの各段階で実施される包括的なソフトウェア試験、検査、分析、及びその他の検証作業に大きく依存する。”

“ソフトウェア検証”の用語は、単なる試験から試験を含む広範囲の活動に至るまで、広義的並びに狭義的に解釈されている。この TIR では、ソフトウェアがその意図する使用に適したものであり、信頼に値する確かなものであるという信頼度を確立するためのあらゆる活動を示すものとして、“ソフトウェア検証”の用語を使用する。選択された活動は、それがいかなるものであっても、ソフトウェアが機能することを保証しなければならない。

3.2 信頼醸成活動 － ツールボックスに含まれるツール

ソフトウェア検証のツールボックスに含まれるツールには、リスクを軽減して信頼を醸成するために、ソフトウェアのライフサイクル中に遂行される活動（ソフトウェアが検証されたという結論を裏付ける検証活動）が含まれる。それらは、基本的に、過去 30 年以上にわたるソフトウェア開発での経験的な使用を通じて、付加価値のあるリスク予防策として確立された活動の集合である。これらの活動は、ソフトウェアエンジニアリング適正基準（good software engineering practices）と呼ばれることが多い。それらの多くは、IEEE のソフトウェアエンジニアリング基準及びソフトウェアエンジニアリングインスティテュートの CMMI モデルなどの規格及び方法論で説明・定義されている。この TIR では、ソフトウェア検証されたという結論を裏付けるツールを示す。既知のツールの一覧及び解説については、付録 A を参照のこと。

3.3 批判的思考

この技術情報レポート（TIR）は、特定のソフトウェアを適切に検証するために実施すべき活動の決定に批判的思考を応用することを推奨する。批判的思考とは、ソフトウェアのさまざまな側面、及びそれを応用する環境を分析・評価し、検証中に応用すべき最も有意義な信頼醸成活動を特定するプロセスである。批判的思考は、提案されたソリューションを徹底評価して希望通りの結果がもたらされるかどうかを判断することなく、万能型の検証ソリューションを応用するだけのアプローチを回避する。批判的思考は、検証ソリューションがソフトウェアによって大きく異なることを理解し、状況やソフトウェアが同じでも、応用すべき検証ソリューションが異なることを容認する。批判的思考は、提案された検証ソリューションが規則の主旨に合致し、主な関係者全員及びそのニーズを考慮することを要求する。批判的思考は、ソフトウェアの特性又はソフトウェアの意図が変更になった場合、若しくは新しい情報が入手可能になった場合、検証ソリューションの再評価にも応用される。

批判的思考は、製造業者のコンプライアンスを確立する検証ソリューションを実現し、ソフトウェアの使用が安全であることを保証し、審査員によって適当かつ適切とみな

される証明書を完成させ、検証作業の実施担当者がその努力をあまり負担と感じずに付加価値をもたらすようなシナリオを実現する。

この技術情報リポートは、意図する使用、リスク、信頼度、及びソフトウェアが正しく機能しているかどうかを判断する能力など、ソフトウェアの主な側面を総合的に評価し、検証ソリューションに応用すべき最も有意義な信頼醸成活動を決定するための枠組みを提供する。この技術情報リポートでは、批判的思考の応用結果を踏まえて選択すべき活動のツールボックスについて説明する。

4 ソフトウェア検証及び批判的思考

4.1 概要

規制プロセス用ソフトウェアのライフサイクルを通じて、ソフトウェアが意図する機能を確実に果たせるように、適切な管理を行う必要がある。批判的思考及び選択された信頼醸成活動を応用すれば、ソフトウェアの検証された状態を確立・維持することができる。下記の図1は、プロセス自動化の決定の瞬間から規制プロセス用ソフトウェアの廃用又は使用停止に至るまでのライフサイクルに含まれる典型的な活動及び管理の概念図を示している。この図は連続的なモデルを示しているが、要素を定義し、リスクを特定し、批判的思考を応用するなど、実際のプロセスは反復的なものである点を十分に理解すること。

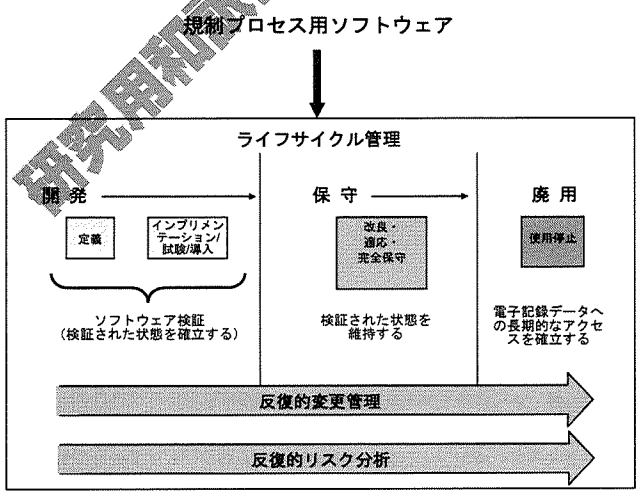

図1 ― ライフサイクル管理

ツールボックスから選択すべき基本的な信頼醸成活動とは、ソフトウェア開発のライフサイクルモデルを選ぶことである。選ばれたモデルは、さまざまなライフサイクル活動の間に他の適切なツールの選択を可能にする批判的思考及び活動を含むものでなければならない。分析及び評価の実施結果は、ソフトウェアが意図する機能を確実に果たせるようにする上で最も有意義な信頼醸成活動の選択を推進する。この TIR は、特定のソフトウェア開発モデルの使用を暗示又は指示するものではない。しかし、説明を単純化するため、この文書の残りの部分では、批判的思考の概念をウォーターフォール開発モデルの文脈内で、作業部会が各段階のために選んだ一般名を使って説明する。批判的思考及び適切なツールのアプリケーションがモデルに組み込まれる限り、他のソフトウェア開発モデル（反復的、スパイラルなど）を採用することも当然可能である。

プロセスの自動化を検討する場合、提案されたソフトウェアの意図する使用を調査し、それが規制プロセスの一部を自動化するものかどうかを確認しなければならない。もしそうであれば、ソフトウェアの意図する使用に関して検証を行う必要がある。この TIR では、規制プロセス用ソフトウェアの検証アプローチについて説明しているが、このアプローチは規制プロセス用以外のソフトウェアにも有効である。

ライフサイクルの開発段階で、リスクマネジメント及び検証プランニングの作業を実行して情報を収集し、以下の分野での決定を推進する。

- 適用される努力のレベル及び文書/成果物の精査
- 文書/成果物に記載された内容の範囲
- ツールボックスからのツール選択及びツールの応用方法
- ツール応用における努力のレベル

これら4つの分野での決定を推進する主な要因は、プロセスリスク及びソフトウェアリスクである。しかし、ソフトウェア及びプロセスの複雑さ、ソフトウェアのタイプ、ソフトウェアの系統及びソフトウェア開発の管理など、他の推進要因が決定に影響を及ぼすこともある。これらの要素の多くは、ソフトウェアが社内で開発されたものか、業者から供給されたものか、何らかの組み合わせによるものかによって影響を受ける可能性がある。このことは、ソフトウェアまたはそのコンポーネントの製造又は購入を決定する際に考慮すべきである。

この文書では、検証プランニングのプロセスを対照的な二つの要素として説明している。検証プランニングの最初の要素には、成果物の審査に応用すべき文書及び精査の厳密度の決定が含まれる。この要素の決定は、主にプロセスリスク分析の結果によって推進される。もう一つの検証プランニング要素は、ツールボックスからソフトウェアのインプリメンテーション、試験、及び導入を行うためのツール選択を推進する。これらのツール選択は、主にソフトウェアリスク分析によって推進される。これらのプランニング段階は、各種のリスク分析の成果であり、このレポートでは別々の活動

として記述されている。しかし、それらが一つの活動に統合され、それにリスク分析のさまざまな側面及び検証を進めるための結果的な選択が含まれることも多い。

ライフサイクルの開発段階で、リスクマネジメント及び検証プランニングの作業を利用して、ソフトウェアに応用すべき適切な努力のレベル、及び応用すべき信頼醸成ツールを決定する。このタイプのアプローチは、検証された状態を確立する上で基礎となる適切かつ付加価値のある活動/検証作業を遂行させる。実行後、ツールの利用及びそれに関連する成果は、ソフトウェアが検証されたという結論を裏付けるものとして検証レポートに記載される。

導入後、ソフトウェアはソフトウェアライフサイクルの保守段階に突入する。この段階では、ビジネスニーズ又は規制要件の変更に応じて、ソフトウェアのモニタリング、強化、及び更新が行われる。変更管理活動では、ライフサイクルの開発段階に応用した最初のアプローチと同じ概念を利用する。しかし、この場合は、意図する使用、故障のリスク、最初の開発段階で応用されたリスク予防策、及びソフトウェア自体の機能への影響について、変更を評価する。同様に、変更の定義、インプリメンテーション、試験、及び導入の間に、適切かつ付加価値のあるツールを選択する。このアプローチを応用することで、ソフトウェアが検証された状態で意図する使用に準じて確実に動作を継続できるようにする。

廃用の段階では、自動化されたプロセスの排除又は自動化プロセスに使われているソフトウェアの交換により、使用中のソフトウェアを取り除く作業を行う。いずれの場合も、それ以降、ソフトウェアが意図する使用に準じて動作することはなくなる。通常、廃用に関連する主な活動として、保守を必要とするデータのアーカイブ化及びソフトウェア自体の取り外しなどが挙げられる。規則に規定されたデータ保持要件に応じて、長期的なデータアクセスの方法を計画することが不可欠である。

図1は、ソフトウェアライフサイクルコントロールの主な活動を示している。その他の作業の流れとして、インプリメンテーションを行うソフトウェアに応じたプロジェクト管理、プロセス開発、業者管理（該当する場合）、などが挙げられる。これらの作業の流れには、この TIR の範囲を超えるものも多く含まれるが、それらは相互に関連し合い、ライフサイクルコントロールの活動と重複する。従って、これらの作業の流れが、ライフサイクルコントロールの活動に直接影響を及ぼしたり、相互に関連する場合は検討を行う。

図2は、別の作業の流れに含まれる活動に関連するソフトウェアライフサイクルコントロールの活動及び批判的思考を示す。批判的思考の活動は、反復的リスク分析及び検証作業の流れに登場する。組織のビジネスモデル内におけるこれらの作業の流れについて、明確かつ正式な定義を行い、ビジネスと規制の両方の観点から、プログラムを正しく管理できるようにすることが重要である。

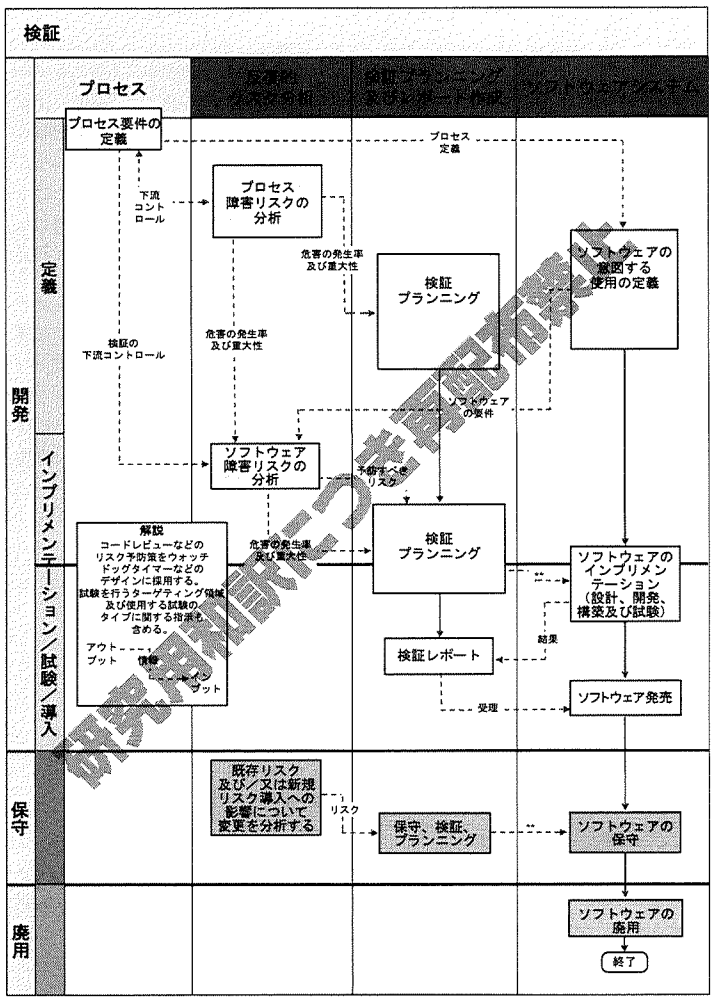

図2 － ライフサイクルコントロール作業の流れ

図2に表示された各色は、図1の全体的なアプローチのフローチャートに示したライフサイクルの各部に対応している。赤い破線は、一つの活動からアウトプットとして発信され、他の活動へのインプットを提供又は決定の推進を助ける情報を示している。この図は、インプットを必要とする活動の完了前、そのインプット情報を得る必要性によって活動の順序が決定される様子を示している。インプリメンテーションを行うソフトウェアのサイズ又は複雑さに関係なく、これらの活動をすべて遂行することが重要である。しかし、大型又は複雑なソフトウェアの場合、これらの活動は個別に行われる可能性が高く、小型又は単純なソフトウェアの場合、これらの活動が統合されたり、同時に遂行される場合が多い。

要するに、この TIR で説明する批判的思考のアプローチは、適切な信頼醸成活動又はツールを特定してさまざまな作業の流れに採り入れ、発売時にソフトウェアが検証され、それが廃用になるまで検証された状態が維持される結論を裏付けるための体系的な方法といえる。

以下のセクションでは、図1に示されたライフサイクルコントロールの各ブロックについて、さらに詳しく説明する。図2に示された反復的リスク分析、検証、及びソフトウェア活動の作業の流れを利用し、さまざまな決定ポイントと批判的思考を採り入れた決定推進要因について概要を説明する。

4.2 適用範囲

ソフトウェアを規制プロセスに使用するかどうかを決定する最初のステップは、プロセス及びソフトウェア使用の高度な定義を文書化することである。ソフトウェアが適用範囲内にあることが明白で、意図する使用の詳細な定義が既に始まっている場合、この活動を遂行しても、あまり意味はないように思えるかも知れない。しかし、それが明確にされていない状況では、この活動によりソフトウェアが適用範囲内にあるかどうかを明確に判断することができる。また、ソフトウェアが適用範囲外と特定された場合、なぜそれが適用範囲外なのかを裏付ける根拠を明確にすることができる。

自動化すべきプロセスが特定され、予想される高度なソフトウェアの意図する使用が定義されたら、規制適用評価を実行し、そのソフトウェアが規制プロセス用ソフトウェアの定義に適合するものかどうかを判断することができる。通常、ソフトウェアが適用範囲内にあるかどうかの判断は非常に簡単である。適用範囲外のソフトウェアを識別するのは、それより難しい。医療機器規則の範囲内と範囲外、両方の要素がプロセスに含まれていると、それらを自動化するソフトウェアのイメージは不明瞭なものになってしまう。この理由から、プロセス内におけるソフトウェアの使用を定義する境界線を明確に定めることが非常に重要である。これに関連して、非常に複雑なソフトウェアアプリケーションのモジュールでプロセスを自動化する場合、規制プロセスと非規制プロセスを区別する境界線を明確にすることも重要である。

<u>規制適用評価</u>

規制適用評価を利用すれば、ソフトウェアが“規制プロセス用ソフトウェア”の定義に適合し、この TIR の適用範囲内にあるかどうかを判断することができる。まず最初に、ソフトウェアで自動化するプロセス及びソフトウェアで管理されるデータ記録に適用される具体的な規則を明確にする。質問集を利用すれば、それらの規則を遵守する上でソフトウェアが果たす役割を徹底的に理解するのに役立つ。下記のような質問を考慮すべきである。

a) ソフトウェアの障害又は潜在的な欠陥は、医療機器又は医療機器の品質に影響を及ぼすか。
b) ソフトウェアは、規則（特に品質システム規則の特定要件）が求める活動を自動化又は実行するものか。
c) ソフトウェアは、当局への申請に利用するためのデータを作成又は管理するものか。
d) ソフトウェアは、規則が求める記録（機器原簿、機器履歴簿、設計履歴ファイル、臨床試験記録簿など）の作成及び/又は管理を行うもの、及び/又は将来的にアクセス可能で、規則が求める活動遂行の証拠を提供するものか。
e) ソフトウェアは、規則が求める電子署名の実行/記録に利用されるか。

最初の 2 つの質問は、規制プロセスに使用するソフトウェアを特定するのに役立つ。最後の 3 つの質問は、電子記録データ、電子署名、又は両方を保管するソフトウェアのうち、パート 11 の該当要件に適合する必要があるものを特定するのに役立つ。これら 3 つの質問に 1 つでも“イエス”があれば、検証が必要とされ、この TIR の適用範囲内にあるソフトウェアが明らかになる。質問 c、d 及び e で特定されたソフトウェアは、電子記録及び署名に関する該当の規制要件にも適合しなければならない。

プロセス及びそれに対応するソフトウェアが品質システムの一部かどうかを判断するのは難しく、実際の医療機器からの分離度はツールによってさまざまに異なると考えられている。各組織は、この境界上にあるソフトウェアをめぐる状況を慎重に検討し、このソフトウェアの障害が規制プロセスに及ぼす影響、及び製造された医療機器の安全性及び有効性に及ぼす最終的な影響について徹底的に理解する必要がある。答えが不明な場合、ソフトウェアは適用範囲内にあると考え、この TIR に定義されたアプローチを応用するのが最善策であろう。

4.2.1 医療機器規則に無関係なプロセス及びソフトウェア

プロセス又はソフトウェアに医療機器規則と無関係な要素が含まれる場合、分析を実施して、ソフトウェアのどの部分が適用範囲内で、どの部分が適用範囲外とみなされるかを判断しなければならない。そのような判断は、各種のコンポーネント、モジュール、及びソフトウェアのデータ構造の間の統合度、及び組織に求められるコンプライアンスに基づいて合理的に解釈されなければならない。大型で複雑なエンタープライズリソースプランニング（ERP）ソフトウェアなど、品質システムのサポートにソフトウェアを使用する場合、このことは特に重要である。このようなソフトウェアには、会計や財務など、医療機器規則の対象とならないプロセス用の機能を含めることができる。このような機能は、事業運営に不可欠であり、政府が規定する何らかの要件（サーベンス・オクスリー法など）に適合する必要があると考えられるが、医療機器規則が求める記録の管理に併用される場合を除き、医療機器規則及び FDA とは無関係である。

4.3 開発段階

開発段階で批判的思考を応用する場合、検証努力及び採用すべき特定ツールの選択に関して行われた決定を把握するための主な検証プランニング活動は 2 種類存在する。検証プランニング活動の第 1 部では、プロセスリスク分析（付録 B 参照）からのインプットを利用し、文書作成に応用すべき努力レベルの基礎を確立し、ツールボックスの定義セクションからのツール選択を推進する（付録 A 参照）。この時点で、努力のレベルとは、文書作成で予想される詳細の程度及び文書作成への管理職の関与／部門横断的な関与及び独立した審査の程度として定義される。検証プランニング活動の第 2 部では、ソフトウェアリスク分析からのインプットを利用し、ツールボックスからのインプリメンテーション/試験/導入ツールの選択を推進する。この段階での努力のレベルとは、リスク主導によるエンジニアリングリスク予防策の応用及び静的・動的分析による選択を意味する。活動が適切に実行されれば、ソフトウェアの検証された状態が確立され、その証拠が検証レポートに記録される。

反復型、スパイラル型、改良ウォーターフォール型など、開発段階で応用可能な開発ライフサイクルモデルは数多く存在する。この TIR は、特定のライフサイクルモデルを支持又は推奨するものではない。しかし、この TIR では、インプリメンテーション/試験/導入の前に要件定義の概念（例：意図する使用）に基づいて管理された方法を当然とみなす。これは、意図する使用に関するソフトウェアの検証を確立するための基本概念である。

4.3.1 定義

定義のブロックで遂行される活動として、プロセスの定義、そのプロセス内におけるソフトウェアの意図する使用の定義及び自動化されるプロセス内で特定された固有のリスクに基づく検証努力レベルのプランニングなどが挙げられる。図 3 は、選択されたウォーターフォールモデルの例でその部分に該当する*開発段階*の一部を示している。

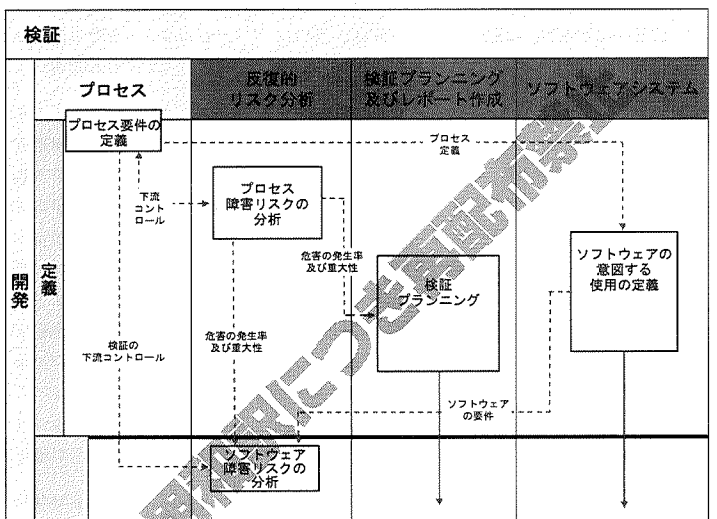

図 3 ― ライフサイクル段階 ― 定義ブロックにおける作業の流れ

4.3.1.1 プロセスに関する要件

ライフサイクルコントロールの応用における最初の基本的なステップは、自動化の対象となる部分を中心としたプロセス全体の目的及び機能を明確に定義することである。これを遂行するには、自動化するプロセスの案件に適した専門家に参加してもらうのが理想的である。この完全な定義には、ソフトウェアによって全面的又は部分的に自動化されるプロセスに関するすべての側面及び活動が含まれる。このプロセス定義がもたらす便益として以下の例が挙げられる。

- 規制の要件を明確に識別できる。
- プロセスのコンテクスト内で特定ソフトウェアの意図する使用を明確に識別できる。
- 特定ソフトウェアによって自動化されないプロセスの側面及び活動を明確に特定し、手続きなどの手段によって問題に対処できる。

- ソフトウェアの上流及び下流にあるプロセス活動を特定し、ソフトウェア障害のリスクを評価する際、及びソフトウェア障害のリスク予防策を考案する際、それらの活動について検討できる。

プロセス定義の活動は、以降のライフサイクルで行われる決定の基礎を確立するものであり、付加価値のあるリスクベースの活動に対する努力の目標設定に不可欠なため、回避又は省略することはできない。

4.3.1.2 プロセス障害リスクの分析

規制プロセス用ソフトウェアのコンテクストでリスク分析を実施し、リスクマネジメントについて検討する際、ソフトウェアは医療製品の最終的な安全性及び有効性に関係してくる（付録 B の考察参照）。検討すべきリスクにはいくつかのタイプがある。

- 人体への危害のリスク － ソフトウェアのユーザー、ソフトウェアによって制御される機器のオペレーター、そのソフトウェアによって製造又は品質が制御される機器の受動者、及び傍観者への危害のリスク。
- 規制リスク － 規制要件への不適合のリスク。ソフトウェアの障害が、規制当局に要求された記録（CAPA、苦情、DMR、DHF など）の消失又は品質システム及び製造手順からの逸脱につながる可能性がある場合、このリスクについて検討することが重要である。
- 環境リスク － ソフトウェアが機能する環境へのリスク。一般的に、有毒物質の漏れ、流出、及び火災に関連するリスクと考えられるが、それ以外のタイプの火災、洪水、爆発などもあり得る。また、ソフトウェアの障害が、他のソフトウェアで使用するデータの消失又は損傷をもたらす可能性があるかどうかなど、仮想環境についても検討しなければならない。

FDA 規則は、環境又は労働者の安全性について規定していないが（これらの問題は別の政府関係機関が統括）、この TIR では、このタイプのソフトウェアがもたらす潜在的な影響を考慮し、それらの要因を含めてリスクマネジメント活動の説明を行う。

プロジェクト完了リスク（例：プロジェクトの資金調達が予定通り実施されない）やビジネスリスク（例：事業継続性）など、他のタイプのリスクをこのモデルに取り込むことができる。しかし、この TIR の適用範囲及びリスク低減用に検討されたツールは、プロジェクト完了又はビジネスリスクのいずれにも対応していない。この文書は、プロセス障害のコンテクストにおけるソフトウェア障害に関連する人体の安全、規則及び環境のリスクを対象としている。

プロセス障害リスクの分析は、プロセス障害の結果として生じる可能性がある危害の特定を目的としている。この分析は、将来的に提案されるプロセスに重点を置きながらプロセス定義の完了直後に実施し、ソフトウェアソリューションを選択する際、特

定されたリスクについて検討できるようにしなければならない。このことは、ソフトウェアソリューションを社内で開発するか、社外から調達するかの決定にも当てはまる。例えば、プロセス障害が高リスクの危害を伴う場合、十分に理解された予測可能なテクノロジーに基づくソフトウェアソリューションを選択しなければならない。プロセス障害が高リスクの危害をもたらさない場合、よりロバストなソフトウェアソリューションに多くの時間とエネルギー、資金を費やさなければならないという懸念は少なくなる。このリスク分析の結果は、明確に文書化しなければならない。なぜなら、ツールボックスからツールを選択し、検証活動に応用すべき努力のレベルを正当化する上で重要な決定推進要因があるからである。

4.3.1.3 検証プランニング

ソフトウェアに関する要件がきちんと満たされていることを保証する上で必要な検証の範囲（確認及び客観的証拠）は、全体的なプロセスに含まれるソフトウェアの臨界値によって決まる。従って、応用する努力のレベル及び成果物の監視に関する最初の検証プランニング活動は、プロセス障害リスク分析からのインプットのみに基づいて行われる。

企業は、規制プロセスの障害に伴う危害の潜在的なリスクによって推進される努力のレベルを定義又は特定する際、チェックリストに依存する考え方を改め、エンジニアリングの観点からの適切な判断を求めるようにしなければならない。ソフトウェアの中には、意図する使用の定義、リスクの理論的根拠に関する文書作成、ソフトウェアの機能を手順ごとに記した文書作成（審査又は基本機能試験などの活動によるソフトウェアがこれらの要素に適合しているかどうかの確認を含む）、及びソフトウェア構成のコントロールなど、低レベルの努力のみが求められるものもある。さらに中レベルの努力が必要な場合、適切なレベルの検証が行われているという信頼を確立するためには、より詳細な検証プランニング、複層的な意図する使用、及び 1 回以上の検証試験レポート作成が必要となる。高リスクの危害を伴う場合、設計管理下で開発される医療機器に求められるものと同等の全面的なライフサイクルコントロール活動など、ソフトウェアに高レベルの厳密性が求められる。

この検証プランニング活動は、検証プランニングに関して反復的に行われる文書作成の初回となる。このプランニングには、“努力のレベル”の選択（決定実行）及びこれらの選択の理論的根拠（決定推進要因）が含まれる。理論的根拠は、規制プロセスの障害によってもたらされる危害のリスクに基づくものでなければならない。検証プランは、検証プランニングプロセスへの批判的思考の応用を裏付ける客観的証拠をもたらすものでなければならない。

4.3.1.4 ソフトウェアの意図する使用

ソフトウェアの意図する使用は、ソフトウェアのリスク及び複雑さによって推進される詳細の線的な進行に内包されている。つまり、プロセス内におけるソフトウェア機能及びその目的の全体像を提供するという意味である。具体的には、意図する使用とは、自動化しようとするプロセス全体にソフトウェアをどのように適合させるか、ソフトウェアが何をするか、我々がソフトウェアに何を期待するか、設計、製造及び安全な医療機器の保守を行う上で我々がどの程度ソフトウェアに依存するかを説明することといえる。ソフトウェアの使用に伴う潜在的なリスクが何かを理解するために利用する主要なツールである。

意図する使用には、以下の主な 3 つの要素がある。

- 以下に関連する目的及び意図：
  - ソフトウェアの使用（例：誰が、何を、いつ、どんな理由で、どこで、どのようにして）
  - 規則に準じたソフトウェアの使用
  - プロセス内の、又は他のソフトウェア及び/又はユーザーとのソフトウェアの境界
- ソフトウェアの使用に関する要件：複雑さと全体的なリスク増加に伴い、この要素はソフトウェアの使用に関するさらに詳しい情報をもたらす（例：使用例、ユーザーの要件など）。
- ソフトウェアに関する要件：複雑さ/リスクが増加してソフトウェアのインプリメンテーション担当者に明確な指示を与えるレベルに達したとき、この要素はソフトウェアに期待される事柄についてさらに具体的かつ詳細な情報を提供する（例：IEEE に定義されたソフトウェア要求仕様書のタイプに関する情報）。

意図する使用のために作成される文書の範囲は、ソフトウェアの複雑さ及びサイズによって異なる。単純なソフトウェアの意図する使用は、少ないセンテンス又はパラグラフで構成される。一方、さらに複雑かつ高リスクなソフトウェアの意図する使用は、数ページにわたって広範な情報が記載される。

意図する使用は正式な管理及び承認が行われなければならない。組織は、規則、品質システム及び自動化するプロセスに関する知識を備え、適切なスキル及び経験を有する人材の参加を要求しなければならない。さらに大規模なソフトウェア又は安全性が特に重要なソフトウェアの場合も、ソフトウェアエンジニアリングの優良実施、及び使用するソフトウェアに期待される技術に関する知識を備え、スキル及び経験を有する人材を参加させることが有効と考えられる。

我々は“意図する使用”の検証を行う必要はあるが、ソフトウェアの意図する使用が十分に定義されていない限り、検証を行うことはできない。

以下のセクションでは、ソフトウェアの意図する使用の要素についてさらに詳しく説明する。

4.3.1.4.1 ソフトウェアの目的及び意図

ソフトウェアの目的及び意図には、ソフトウェアの使用、規則に準じた使用、及び境界の定義という 3 つの要素に関する情報が含まれる。これらの要素（以下に説明）のさまざまな側面を調査するプロセスの完了後、読む人が品質システムのコンテクスト内におけるソフトウェアの使用について簡潔に理解できるようなソフトウェアの目的及び意図を作成できるようにしなければならない。

ソフトウェアの使用（5 つの W と 1 つの H）

ソフトウェアの使用を定義する場合、何を（what）、どんな理由で（why）、どのようにして（how）、誰が（who）、どこで（where）、いつ（when）を考慮しなければならない。これらの問いかけに対する答えは、プロセスに関する要件に準じてソフトウェアをどのように使用するかという問題の探究に役立つ。以下に示す通り、これでソフトウェアの定義に関する基本的な情報を明らかにすることができる。

表 1 ― 質問例

質問	例（要件の完全な定義ではない）
どんな問題にソフトウェアが対処しようとしているのか。	動向追跡用の製品欠陥データを効率的かつ正確に収集・保管する作業に問題がある。
なぜこのソフトウェアが役に立つのか。	ソフトウェアは世界各地から集めたデータの保管及び動向分析を可能にしてくれる。
どのようにしてソフトウェアが問題を解決するのか。	ソフトウェアはデータ収集のプロセスを推進し、動向に関する情報を自動的に保管・計算してくれる、又はプロセスを推進しないが、動向に関する情報の保管・計算に使われるデータの受動的な収集を可能にしてくれる。
誰がソフトウェアを使用するのか。	品質保証及び業務
どこでソフトウェアが使用されるのか。	ソフトウェアは、米国、ヨーロッパ及び日本の事業所所在地で使用される。
いつソフトウェアが使用されるのか。	ソフトウェアは、世界各地にある事業所の通常営業時間（月～金曜）に使用される。

これらの質問について一つひとつ検討すれば、品質、プロセスに関連するリスクのレベル、またはその両方にソフトウェアがどの程度影響を及ぼすかを判断する上で、その答えがいかに重要かが明らかになる。ソフトウェアの説明に役立つ答えを、確定した意図する使用の定義に含めなければならない。

規則に準じた使用

規則に準じた使用を評価する場合、一度答えを出した質問をさらに詳しく検討し、ソフトウェアが適用範囲内にあるかどうかを判断することができる（セクション 4.2「適用範囲」、上記「規則に準じた使用」のセクション参照）。“イエス”と答えたすべての回答を拡大し、それらの結論に達した理由を含める。ソフトウェアは適用範囲内にあることが特定されたら、（医療機器ユーザー以外の）人体又は環境への潜在的な危害を特定する必要がある。これらの質問はすべて、公衆衛生と安全性及び電子記録と署名の有効性/確実性など、規則の一部として要求される要素に対するユーザーの配慮を促すものである（セクション 2「規制のコンテクスト」参照）。

- ソフトウェアの障害又は潜在的な欠陥は、医療機器の安全性又は医療機器の品質にどのような影響を及ぼすか。
- ソフトウェアは、規則（特に品質システム規則の要件）が求める活動をどのようにして自動化又は実行するか。
- ソフトウェアは、規則遵守に利用するためのデータをどのようにして作成又は管理するか。
- ソフトウェアは、規則が求める記録、例えば機器原簿、機器履歴簿、設計履歴ファイル、臨床試験記録簿に必要な情報、又は将来的にアクセス可能で、規則が求める活動遂行の証拠を提供するための情報をどのようにして記録又は保管するか。
- ソフトウェアは、規則が求める電子署名の実行/記録にどのように利用されるか。
- このソフトウェアは、（医療機器ユーザー以外の）人体又は環境にどのような危害を及ぼすか。

ソフトウェアの境界

ソフトウェアの境界を特定することで得られるさまざまな便益がある。ソフトウェアを利用して自動化するプロセスの部分（プロセス内の境界）及びソフトウェアのインターフェースが存在する場所を特定すれば、検証作業の有効性及び効率性を高めることができる。例えば、複数のソフトウェアを個々に検証するより、一つのグループとして検証した方が効率的な場合が多い。各種のグループ分け戦略が保守段階で進行中の活動の効率にどのような影響を及ぼすかについても考慮すべきである。

プロセス内（図 4）：

自動化するプロセス内におけるソフトウェアの境界を理解すれば、意図する使用に含めるべき側面を明確に定めることができる。ソフトウェアがプロセス全体を自動化する場合もあれば、プロセス内における活動の一部を自動化する場合もある。また、ソフトウェアがプロセスに必要なデータの保管場所として機能する場合もある（図 4 参照）。プロセス内でソフトウェアが果たす役割をを理解すれば、ソフトウェアの潜在的な障害に伴うリスクを特定する際に役立つ。ソフトウェアが規制プロセス用ソフトウェアの定義に適合していることが確定している場合、プロセス内におけるソフトウェアの役割と障害リスクを理解していれば、検証に必要な努力のレベルを決定する際にも役立つ。例えば、プロセス全体を自動化し、そのプロセスを実行する唯一の手段を提供するソフトウェアには、プロセスのごく一部のみを自動化するソフトウェアに比べ、より高いレベルの検証努力が求められる。また、機器の安全性又は有効性を実現する上で不可欠なデータを保存するソフトウェアには、販売業者の成績動向分析用のデータを保管するソフトウェアに比べ、より高いレベルの努力が求められる。

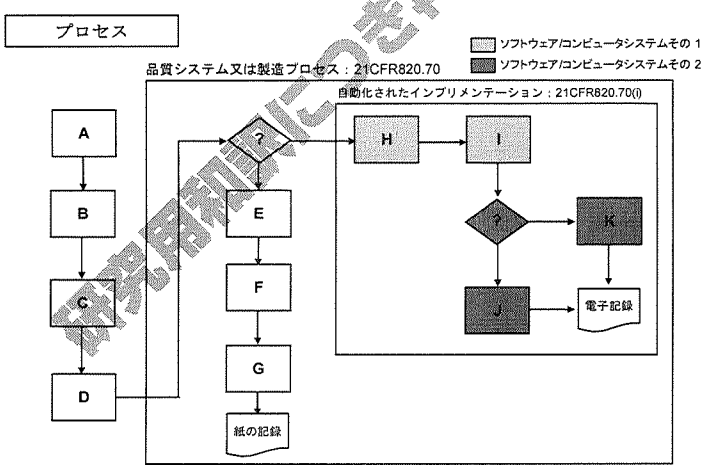

図 4 ― ソフトウェア使用及びプロセス境界の概略図

他のソフトウェアを使用する場合（図 5）：

ソフトウェアは、他の規制プロセス用ソフトウェアと外部のインターフェースで接続される。ソフトウェアと他のソフトウェアの境界を定義する場合、アプリケーションの間にあるこれらのインターフェースを特定することが重要である。検証努力の対象

には、通常、その方法の本質的な部分としての内部インターフェースが含まれる。しかし、外部のインターフェースを無視してはならない。サーバーアプリケーション又はクライアントアプリケーションの検証努力に外部インターフェースを含めるかどうかの判断は任意的なものであり、各種ソフトウェアの開発を担当するプロジェクトチームの構成に依存すると考えられる。特定のソフトウェアアプリケーションをインターフェースとして使用する場合、独自の検証活動を伴うスタンドアロンのアプリケーションとして取り扱うことができる。それ以外の場合、インターフェースで接続されたアプリケーションごとに検証活動を分割する。いずれの場合も、ソフトウェアアプリケーションの間にあるすべてのインターフェースを批判的思考のプロセスに採り入れなければならない。

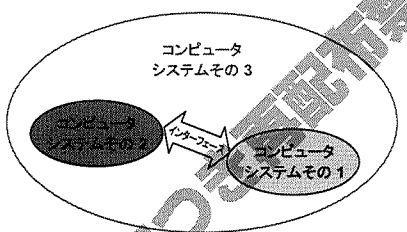

図 5 － 二つのソフトウェアの間にある境界の概略図

4.3.1.4.2 ソフトウェアの使用に関する要件

ソフトウェアの使用に関する要件は、詳細な文書に記録された追跡可能な要素で構成されており、それらの要素は、ソフトウェアの目的及び意図と比較したソフトウェアの使用に関するさらに詳細な情報をもたらしてくれる。これらの要件は、ユーザー又は製品ニーズの観点から、システム使用のシナリオに見識をもたらしてくれる。ユーザーの観点は、ユーザー要件、使用例、又は他のユーザーを中心としたニーズの定義の形式で把握することができる。医療機器ニーズの観点は、システムの影響を受けている機器のニーズを把握するものであり、具体的な機器の要件に関するリファレンス又はソフトウェアが影響を及ぼす製品ラインの概要を含む場合もある。これらのソフトウェアの使用に関する要件は、ソフトウェアに関する要件の作成に必要となる詳細な情報をもたらしてくれる。

4.3.1.4.3 ソフトウェアに関する要件

ソフトウェアに関する要件は、ソフトウェアの目的及び意図のニーズ、及びソフトウェアの使用に関する要件を満たすために何が必要かを具体的に定義するものである。これらの要件は、ソフトウェアの使用に関する要件と同様、詳細な文書に記録された追跡可能なものでなければならない。ソフトウェアに関する要件は、プロセスのリスク及びシステムの製造元に応じて、詳細のレベル及び要件定義のアプローチが異なる。これらの要件は、システムの設計、構成、またはその両方に必要な情報であり、ソフトウェアに関する要件に基づく試験活動に必要な情報でもある。

4.3.2 インプリメンテーション、試験及び導入

インプリメンテーション/試験/導入のブロック内で遂行される活動には、ソフトウェア自体に含まれるリスクに基づくソフトウェアの設計、開発/構成、構築及び試験における検証努力レベルの計画が含まれる。ソフトウェアを内部で開発せずに購入するという決定は、ツールボックスから選択するツールの種類に影響を及ぼす。しかし、ツールが違っても、結果的にソフトウェアに対する信頼を獲得できる点は同じである。この場合も、選択されたツール（決定事項）及びツール選択の理由（決定推進要因）を検証プランニング活動の際に文書に記録する。管理が適切に実行されたら、ソフトウェアをリリースする前に、検証された状態であることを検証レポートに記録する。図 6 は、選択されたウォーターフォールモデルの例でその部分に該当する開発段階の一部を示している。

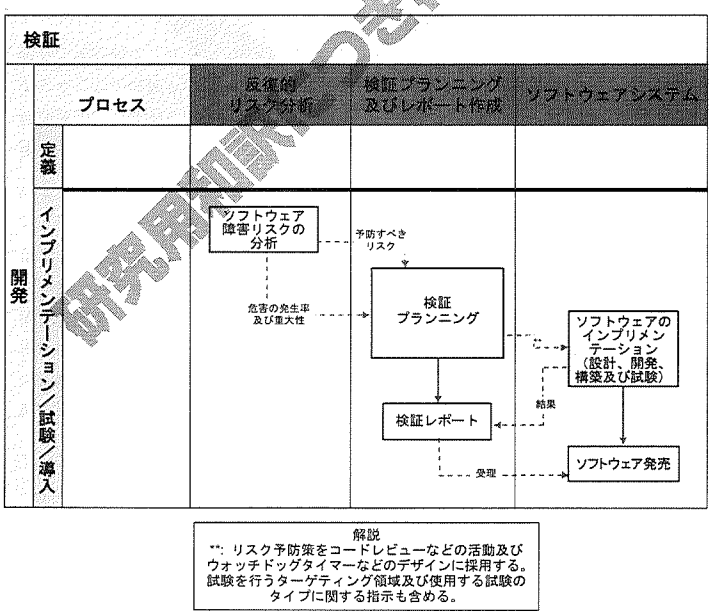

図 6 － ライフサイクル段階 －
インプリメンテーション/試験/導入ブロックにおける作業の流れ