

---

# FDAコンプライアンスとリスクのガバナンス： 医療機器ソフトウェアの検証

2011年5月

Coverity, Inc, Rutul Dave  
Hospira, Harsh Dharwad

---

## 初めに

長年の間に医療機器のソフトウェアへの依存度はどんどん大きくなりました。医療機器へのソフトウェアの採用は、初歩の心臓ペースメーカーのメトロノーム回路から、心電図分析、レーザー手術、患者のフィードバックに基づいて投薬量を調整する点滴システムなどへと発展しています。IMD（埋め込み医療機器）のソフトウェアは、心臓ペースングや除細動、薬物送達、インスリン投与といった生命維持のための機能を実現しています。他のほとんどの業界と同様、医療機器におけるソフトウェアの開発規模は2年ごとに倍増しています。最新式の輸液ポンプは10万行超、陽子線治療機器は100万行超のソースコードで構成される場合があります。

## ソフトウェアによる技術革新の現実

イノベーションの最先端を担う医療機器メーカーは、患者の生活を改善するデバイスを構築するために、ソフトウェアに大きく依存しています。ソフトウェアで機能を構築することで、より速やかにデバイスの機能を構築できます。しかし、ソフトウェアには、メリットと共に不具合も付き物です。米国の規制団体であるFDA（食品医薬品局）は2010年前半に、23件の不具合が発生したデバイスのリコールをしました。これらはすべてクラスIの「製品の使用により健康上重大な悪影響を被ったり死亡したりするのに相当な可能性があると考えられるデバイス」に分類されます。そして、これらのリコールのうち少なくとも6件は、ソフトウェアの不具合によると思われるものでした。

OEMメーカー（他社ブランドの受託製造者）にとっての課題は、デバイスを市場にリリースする前にできるだけ多くの不具合を見つけ、修正することです。なぜなら、たった1つの不具合を見逃したために大怪我や死を招く可能性があるからです。このため、技術革新過程に不可欠な工程としてソフトウェアの検証が非常に重視されることになります。

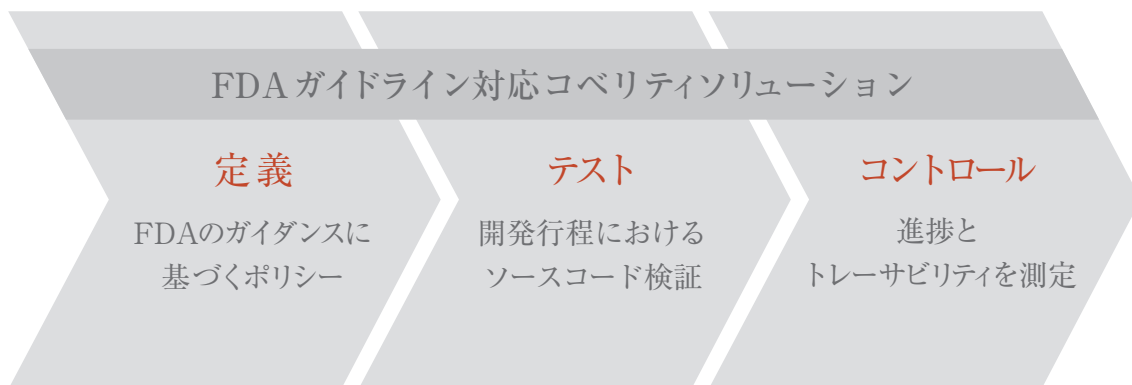
## 開発中のソフトウェアの検証

FDAはデバイスメーカーを支援するために、「ソフトウェア検証における原則（General Principles of Software Validation）」というガイドラインを発表しました。これには、ソフトウェア検証、不具合発生防止、変更後のソフトウェア検証、独立したレビューの必要性、コーディングガイドラインの順守、および開発テストなどの推奨事項が含まれています。

OEMメーカーは、これらのガイドラインやソフトウェア開発のベストプラクティスの実行をサポートする技術やプロセスに関心を持っています。どの開発ソリューションを使用すれば、規制要件にスムーズに対応できるでしょうか。そして、複雑化したソフトウェアで不具合が生じ、不具合や予期しない動作といったリスクによってソフトウェアのメリットが損なわれないようにするには、どのベストプラクティスに従ったらいでしょうか。

静的解析によってソースコードテストが成熟した結果、従来の V&V (Verification and Validation : 検証と妥当性確認) 技術が大きく向上しています。FDA は 2009 年、ソフトウェアを実行しないでソフトウェアが正しいことを検証する手法である静的解析のメリットを認め、実行時エラーを検出するための輸液ポンプ用ソフトウェア安全性テストのガイドラインにこの手法を盛り込みました。最新式の静的解析は、シンボリックパス・シミュレーションによってソースコード中の複雑な不具合を検出できます。1 シンボリックパス・シミュレーションは、プログラムで考えられるすべての実行パスを解析するプロセスです。さらに、静的解析技術は、パスカバレッジに焦点を当てることで、単なるパターンマッチングを超えて進化しています。パスカバレッジによって、実行時、実際に起こり得る不具合をより多く発見することができるようになります。新しい静的解析技術は「疑わしい構文」から「実行時の不具合」へと焦点を移行することで、ソースコードベース内の複雑なやり取り (例: ソースコード内のパスを通して操作される変数の値、関数のパラメータの処理と対応する戻り値の関係) をより多く評価します。成熟した解析ソリューションでは、このように一段と高度な技術を使ってソースコードを解析するために、パスフロー解析とプロシージャ間解析を組み合わせ、制御フローが所定ソフトウェアシステム内で 1 つの関数から他の関数に移るときに何が起るかを評価します。

静的解析は、開発チームが「ソースコードの不具合を抱えたまま製品を出荷しない」という課題に確実に対応するうえで非常に有用です。しかし、規制プロセスをサポートして、ソフトウェア開発プロセスにおける長期的なベストプラクティスを構築するには、静的解析などのツールを使った自動ソースコードテストという強みに基づいたガバナンス、リスク管理、および要件のコンプライアンス (遵守) を包括したソリューションが必要です。このようなソリューションにより、開発組織はソフトウェアのコンプライアンス要件に基づいて基準となるソフトウェアポリシーを定義・検証し、そのポリシーに対するテストを行い、開発プロセス全体を通して開発リスクを管理することができ、生産するソフトウェアとデバイスの品質と安全性についても先を見越して規範を示し、コントロールすることもできます。コベリティの最新製品である Coverity Integrity Control® の使用で、医療機器用ソフトウェアのガバナンス、リスク管理、および要件のコンプライアンス (遵守) のための 3 つのステップから成るプロセスの実行ができるようになりました。



### 定義 - FDA のガイダンスに基づくポリシー

第1のステップでは、規制要件とソフトウェアの品質を確保するための予防的プラクティスという目標に即した明確で具体的なポリシーを確立します。たとえば、FDA ガイドラインに基づくポリシーでは、開発やテストで次の段階に移行する前に、すべての実行時エラーを特定して修正することが必要です。同様に、「新しいデバイスを一番に市場に提供する」という事業目標により、静的解析が検出した不具合を解決するための所要日数を制限するようなポリシーが必要になります。Coverity Integrity Control では、内部の品質基準と FDA の具体的なガイダンスに基づき、組織にとって重要なポリシーを 1 か所で定義し、継続的にコンプライアンスを確認するためのテストのしきい値を設定できます。



図1:FDA発行のソフトウェア検証ガイドの一般原則としてアウトライン化されたポリシーを設定できます

### テスト - 頻繁かつ早期に

ポリシーを確立したら、次のステップではこれらのポリシーに対するテストを行います。コベリティのソースコードテスト・ソリューションでは、まだ開発中のソースコードについて、確立したポリシーに対するテストを実行できます。開発段階からポリシーに対するテストを行うことにより、(品質保証部門によるテストや出荷後といった後工程で問題が発見された場合と比較して) 問題を最小限のコストと時間で修正することができます。Coverity® Static Analysis では高度なアルゴリズムを使用して、実行時のソフトウェアクラッシュや予期せぬ動作を招きうるデバイスの整合性に影響を与える可能性があるハイリスクな不具合を特定し、優先度を決定します。これによってユーザーは、大規模かつ、複雑なソースコードベース上で NULL ポインター参照、メモリーリーク、バッファオーバーフローといった通常は見つけにくい実行時の不具合を検出できます。不具合が検出されると、リスクと影響によって優先順位付けされたポリシー違反が開発者に自動的に通知されるため、開発者はどの問題を一番最初に修正すべきかを認識できます。また、このソリューションはお客様の既存のワークフローに組み込むことができるため、品質とコンプライアンスを維持するための継続的なアプローチがそれぞれのビルドと統合に適用されます。

### コントロール - リスクとコンプライアンス

管理者とマネージメントにとっては、単なる不具合の一覧を手に入れるだけでは不十分で、ソフトウェアの品質とリスクを把握できる高い可視性が重要です。また、規制ガイドラインやコンプライアンス要件を犠牲にしながら開発を進めるようなことがないようにしなければなりません。この可視性は、最終的な納品製品をコントロールし、進捗状況を測り、開発プロセス全体にわたってソフトウェアを管理できるようにするために必要なものです。Coverity Integrity Control は、リスク指標とコンプライアンス違反に対するリアルタイムの可視性を提供します。「定義」段階で確立されたポリシー違反にはフラグが立てられ、開発サイクルを通して更新されていきます。



図2:Coverity Integrity Controlはリスクとコンプライアンスメトリックスに関するマネージメントレベルの可視化を実現しています

## まとめ

医療機器メーカーは、ソフトウェアの開発により、患者がより良い生活を送り、競合他社との差別化を図り、市場に一番先に投入が可能な革新的なデバイスを提供できます。しかし、ソフトウェアには不具合や複雑さというリスクが付き物で、医療機器メーカーはそのようなリスクを管理するという課題を克服しなければなりません。医療機器で使用されるソフトウェアが増加し、クラス II およびクラス III デバイスではアジャイルのような新しいソフトウェア開発手法の使用がますます普及する中で、ソフトウェアの検証プロセスをサポートするソリューションが必要とされています。

米国 FDA のような規制団体は、ソフトウェアへの依存度の高まりを踏まえ、検証ガイドラインを提供しています。そして、患者ケアの向上を目的とした最近の携帯機器アプリケーションの普及を受けて、FDA はモバイル医療アプリケーション用ガイドラインの草案作成を始めています。

ソフトウェアの不具合のリスクを管理するという課題は、ソフトウェア開発の優先順位と内部および規制ポリシーを明確に一致させ、利用可能な最善のテクノロジーを使用して開発中にポリシーに対するソースコードのテストを行って、開発全体を通してソフトウェアの品質、信頼性、安全性を改善することで対応できるのです。

コベリティのソースコードテスト・ソリューションは、1,100 以上のお客様が、個々のソフトウェアとブランドの整合性を保護するために採用しています。医療機器を始めとするさまざまな業界の 35 億以上の製品が、このソリューションの下で開発され市場に提供されてきました。御社のソフトウェアの整合性を保護し、ソフトウェアソースコードのガバナンスにご興味のある方は、弊社 (japan\_sales@coverity.com) までお問い合わせください。

コベリティ 日本支社  
〒163-0510 東京都新宿区西新宿1-26-2 新宿野村ビル10階  
TEL: 03-5909-8838 E-mail: japan\_sales@coverity.com  
Website: [http://www.coverity.com/index\\_jp.html](http://www.coverity.com/index_jp.html)

Coverity, Inc. 米国本社  
185 Berry Street, Suite 1600 San Francisco, CA 94107 USA  
E-mail: sales@coverity.com  
Website: <http://www.coverity.com> <http://scan.coverity.com>

