15-B-3

国際スタンダード認証に求められる「要件から検証結果までのトレーサビリティ管理」の効率化の取組み [1]

1. 概要

安全性が求められるシステムのソフトウェアに対する規格である、ISO 26262（自動車安全規格）、DO-178B/C（航空システムや装置の安全規格）、IEC 61508（電気／電子／ソフトウェアの機能安全に関わる国際規格）等の国際スタンダードの認証では、開発ライフサイクル全体にわたる計画的な作業と、それを証明する文書等の成果物（被認証物）が証拠として要求される。

特にその中でも DO-178B/C では、検証結果までを含めた要件トレーサビリティの管理が求められているが、この作業を人手にのみ頼って行うと、以下の問題への対応が必要になってくる。これは、他の国際スタンダードの認証でも同様と考えられる。

- 要求仕様、設計、ソースコード等、様々な成果物と検証結果とのトレーサビリティを管理する作業は複雑で作業の正確性が問われる
- 各開発段階の担当者と検証担当者間の情報伝達や意思疎通を欠く恐れがある
- 開発工数全体の 50～80%を占めるといわれる検証作業の工数が増大する

上記の課題に対応したツールとして LDRA 社の TBmanager がある。このツールは、要件から検証結果までのトレーサビリティ管理の作業を包括的に支援することができるツールとして開発された。また、国際スタンダードで要求されるオブジェクティブ（達成すべき課題）と被認証物を関連付け 、認証プロセスを支援し、開発ライフサイクル全体にわたる計画的な作業を管理する標準的な環境を提供する。この結果、大幅なコスト削減が図れるとともに、品質の向上を図ることができる。

ここでは、国内の航空システムの国際スタンダード認証取得を目的に、要件から検証結果までのトレーサビリティ管理の自動化を支援するツールとして、TBmanager を用いた事例を紹介する。

[1] 事例提供: 富士設備工業株式会社　浅野 義雄 氏

2. トレーサビリティ管理の自動化に踏み切った理由や経緯

(1)　国際スタンダード認証に関する課題

ISO 26262、DO-178B/C、IEC 61508 などの国際スタンダードでは、開発工程全般にわたって要件が満たされていること（システムの正しい要件が、正しい方法で、正しく開発されていること）を証明する証拠として、詳細な追跡（要件トレーサビリティ）が求められる。

国際スタンダードに準拠し、かつ納期を順守するという、市場要件を満たすためには、検証成果物まで含めたトレーサビリティ管理の効率化を図る必要があり、そのためには認証プロセスの計画・実施・実証が高度に一体化された環境を整備して、要件定義から検証までの一連のワークフローにおける作業を支援することが急務である。

表 15-B-3-1 に国際スタンダードで要求されるトレーサビリティツールのカバー対象を示す。表 15-B-3-1 に示すように DO-178B/C については、要件仕様から検証結果までのすべての被認証物が要求されており、TBmanager はすべてをカバーできている。

表 15-B-3-1　国際スタンダード要求認証対象とトレーサビリティツールのカバー対象

被認証物（注 1）	国際スタンダード		トレーサビリティツール	
	DO-178B/C	ISO 26262、IEC 61508 など	TBmanager（注 2）	他のトレーサビリティツール
要件仕様	○	○	●	●
設計	○	○	●	●（注 3）
ソースコード	○	○	●	●（注 3）
検証結果	○	－	●	×

○：要求認証対象、－：要求認証対象外、●：ツールカバー対象、×：ツールカバー非対象

注 1：被認証物は例として 4 点列記している

注 2：TBmanager は、要件管理ツールやテストツールと連携

注 3：ツールによってはカバー非対象もある

(2)　要件トレーサビリティの課題

要件トレーサビリティを管理することは困難な課題である。新しいアプリケーションを開発する場合であれば、要件定義とレビューの段階でのトレーサビリティを確立すればよいが､人手に頼っていては正確性を欠き､工数が増大するという問題がある。一方、レガシーシステムでは、要件が設計、あるいは実装の詳細に埋め込まれていることや、ソースコードが不規則に展開されていて、要件に対するトレーサビリティとしてそのままでは役に立たないため、熟練したエンジニアの投入やさらなる工数の増大、スケジュールの遅延などの問題が生じる。

このような事態を改善するため、要件からソースコードまでのトレーサビリティ管理の支援ツールが多く提供されるようになった。しかし、現状において手に入るツー

ルではコーディングスタンダードチェック等の解析や、単体テスト、カバレッジ解析などの検証作業はサポートされていない（表 15-B-3-1「他のトレーサビリティツール」の「検証結果」欄参照）。このため、開発工程において最も複雑で手間のかかる検証作業と、成果物まで含めた要件トレーサビリティは、相変わらず人手に頼らざるを得ない状況であり、それに伴う認証費用、開発工数等の増加が現状の大きな課題となっている。

3. 適用のための事前準備や工夫

ここでは支援ツールとして TBmanager を使用する上での工夫点を記す。

（1） 要件のインポート

要件トレーサビリティを実現するために、まず、要件を本ツールにインプットする必要がある。要件は Word・Excel・PDF などのファイルに定義されていることが多いため、これらのファイルを XML 形式でインポートする仕組みを構築した。

（2） 各種成果物のインポート

要件管理ツール、テストツールなど他のツールとの連携を図るため、インポートやエクスポートのインターフェース仕様を XML 形式で記述することとした。したがって、他のツールからの設計情報などを XML 形式で出力させ、本ツールと連携させた。

なお、レガシーシステムで開発された設計情報でも XML 形式に変換できる場合は、本ツールとの連携ができ、トレーサビリティを確立することができる。

（3） 既存システムでの国際スタンダード認証取得

国際スタンダードの認証を取得するには、開発工程全般にわたって要件が満たされていることや、厳密な開発計画書とそれに従った成果物が要求される。既存システムで作成される各種成果物は開発計画書に準拠している必要がある。このため、国際スタンダードが要求している開発計画書を作成し、認証取得上、必要な成果物を明確にした。また、各ワークフローにおけるトレーサビリティの要件を整理するなどの準備作業を行った結果、本ツールが活用できるようになった。

4. 適用技術の概要と効果

4.1. TBmanager の概要

（1） 国際スタンダード認証への対応

本ツールでは、国際スタンダードで要求される各種のオブジェクティブ（達成すべき課題）が一覧表示できる。各種国際スタンダードのオブジェクティブを図 15-B-3-1（ISO 26262 の表示例）に示す。図 15-B-3-1 では左側の Standard の画面で国際スタンダードを選択し、右側の Details の画面にその詳細情報（各種オブジェクティブ）が表示されている。

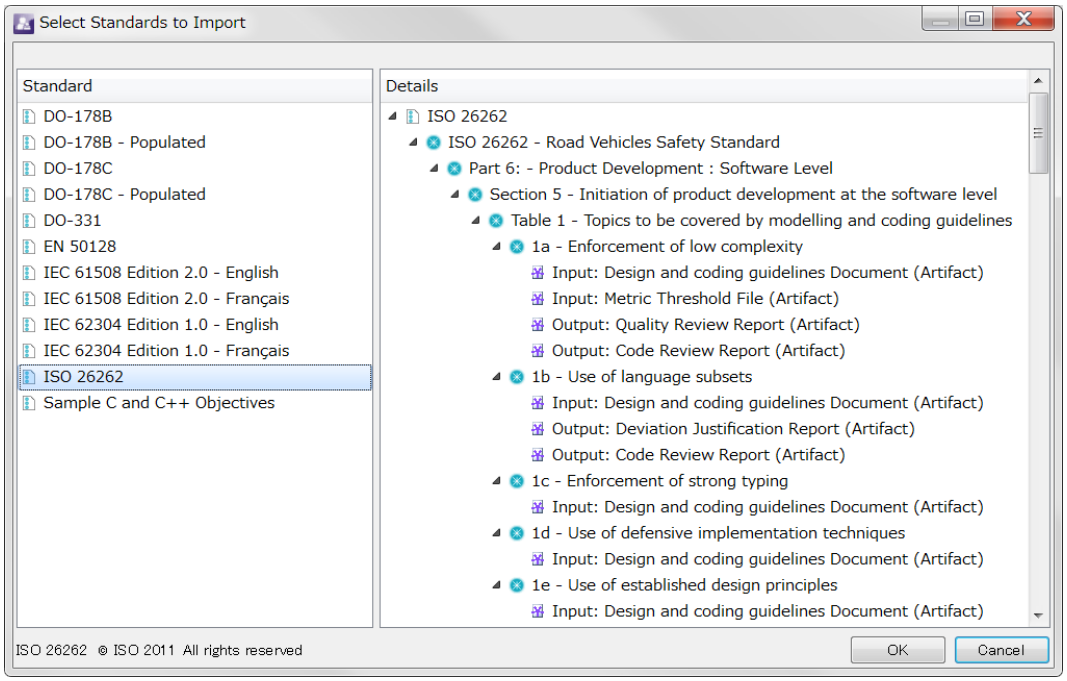

図 15-B-3-1　各種国際スタンダードのオブジェクティブ（ISO 26262 の表示例）

また、国際スタンダードのオブジェクティブに検証成果物を登録し、これらの関連を表示できるようにした。成果物が登録された例を図 15-B-3-2 に示す。図 15-B-3-2 では図 15-B-3-1 の右側の Details から展開され、オブジェクティブにコードレビュー報告書（Generated Code Review Report）、コーディングガイドライン（Coding Guidelines Document）、品質レビュー報告書（Generated Quality Review Report）などの検証成果物との関連が表示できるようになっている。

これらの登録された計画文書、開発成果物、検証結果等は、その進捗を追跡（オブジェクティブの達成度）することができる。

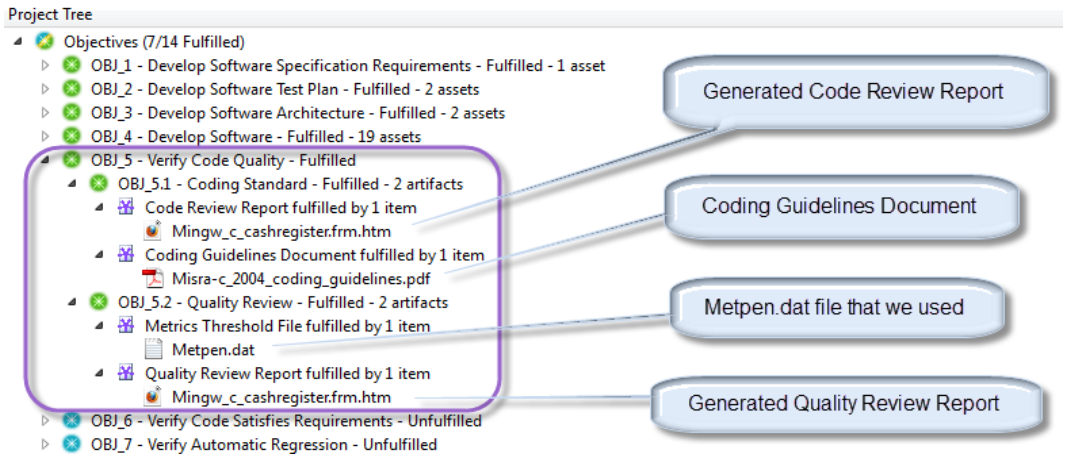

図 15-B-3-2　スタンダードのオブジェクティブに検証成果物が登録された例

(2)　要件から検証結果までの一貫したトレーサビリティ

IBM® Rational® DOORS®などの要件管理ツールや Word・Excel・PDF などのファイルに定義される要件を本ツールにインポートするとともに、各要件に、それを実装するソースコードを割当てて、静的解析や動的作業（単体テスト、カバレッジ解析など）の検証作業を設定し、これらを連携させることで要件から検証結果までのトレーサビリティの管理を可能とした。要件から検証結果までのトレーサビリティの表示例を図 15-B-3-3 に示す。

図 15-B-3-3 では、左側の Project Tree にインポートされた要件である High-Level Requirement（“REQ_xxxx”、上位要件）や Low-Level Requirement（“LLR_xxxx”、下位要件）（あるいはデザインモデル）を表示し、右側の Procedure で、その要件に対して実装するソースコードを紐付けして、コーディングスタンダードチェック等の解析や単体テスト、カバレッジ解析などの検証項目（Verification Tasks）を設定し、これらを連携することができる。

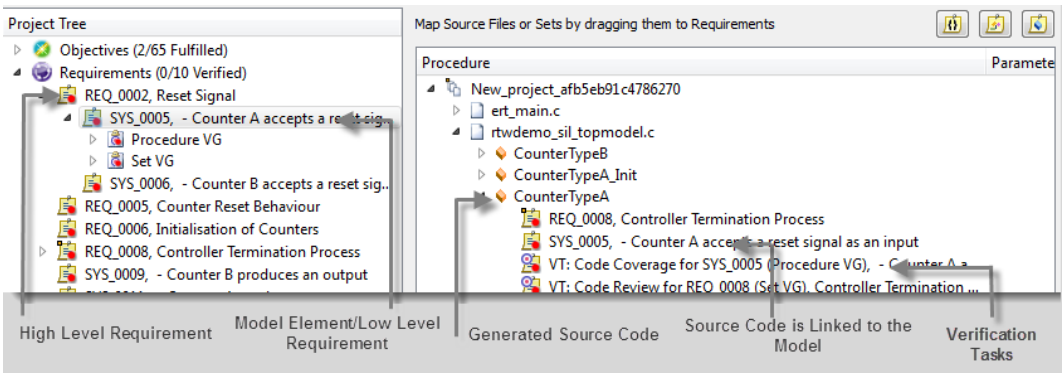

図 15-B-3-3　要件から検証結果までのトレーサビリティの表示例

次に、要件に設定された検証項目から連携されたテストツール（TBrun や Testbed など）を起動して、要件に紐づけられたソースコードを直接テストすることを可能とした。これにより、様々なテスト結果を要件に関連付ける作業を効率化し、これらのトレーサビリティを管理して、エビデンスとして残すことができる。要件に設定された検証項目から検証ツールの直接起動の表示例を図 15-B-3-4 に示す。図 15-B-3-4 は、図 15-B-3-3 の Procedure から展開されるもので、要件（REQ や LLR）に設定された検証項目（VT）から検証ツール（Verify with LDRA tool suite など）を直接起動できることを示している。

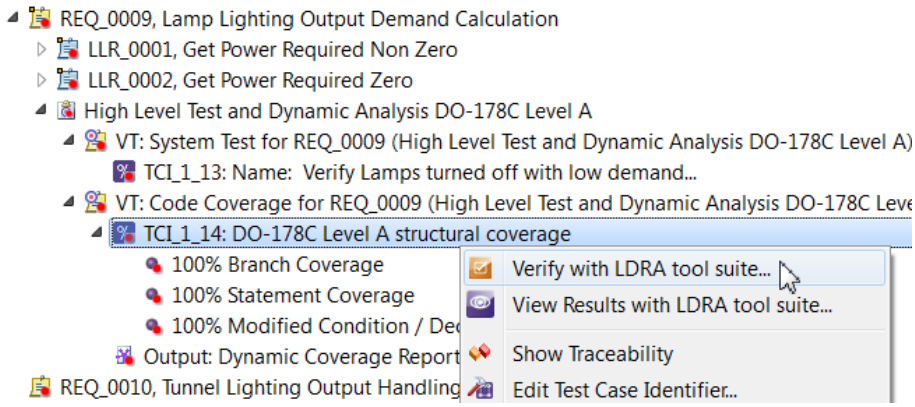

図 15-B-3-4　要件に設定された検証項目から検証ツールの直接起動の表示例

(3)　トレーサビリティの可視化

仕様（Specifications）、テスト仕様（Test Specification）、テスト（Tests）について、トレーサビリティの状況を可視化するようにした。トレーサビリティの可視化の例を図 15-B-3-5 に示す。図 15-B-3-5 では、それぞれがどの項目に紐付いているかが示されている。要件、テスト仕様、テスト結果の関係を視覚的に表示し、包括的なレポートを出力することができる。また、設計ドキュメントについても同様に要件やテストなどとのトレーサビリティを可視化することができるようにした。要件～テスト結果（検証結果）までの状況を可視化することは、検証作業を効率化し信頼性を高める上で重要である。

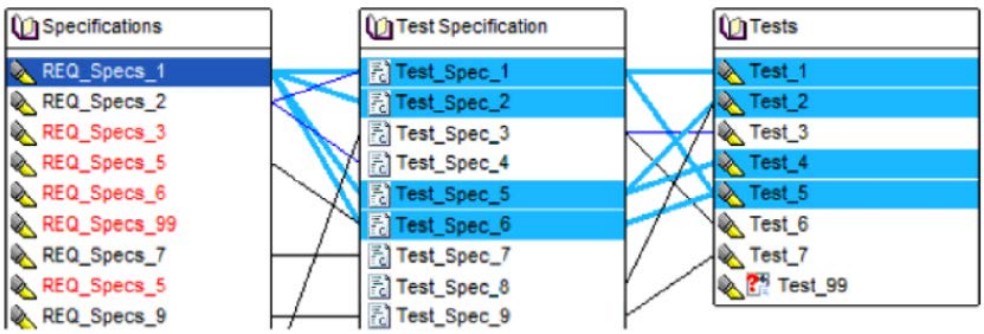

図 15-B-3-5　トレーサビリティの可視化の例

4.2. Tbmanager の使用結果

DO-178B/C が適用される航空システムの開発に本ツールを使用した。国際スタンダードの認証では、開発ライフサイクル全体にわたる計画的な作業と、それを証明する文書等の成果物（被認証物）を証拠として提出できた。また、国際スタンダードで要求されるオブジェクティブ（達成すべき課題）と被認証物の関連付けとこれらの関係を一覧表示させることができた。

要件管理ツールやテストツールを連携させることで、要求仕様、設計、ソースコード等の

様々な成果物と検証結果とのトレーサビリティ作業を効率よく実施することができた。また、トレーサビリティ作業自体もが正確になり、品質の向上を図ることができた。また、開発ライフサイクルの早期段階から計画的に作業を管理することで、コンプライアンスリスクの軽減を図ることも可能となった。さらに、要件から検証結果までのトレーサビリティの作業が自動化され工数を減少させることに伴い大幅なコスト削減が図れた。

開発ライフサイクルでは様々な成果物が作成されるが、異なるリポジトリに保存されている場合が多く、トレーサビリティの管理・保守作業は手間がかかり不正確なものになる。これらの一連の作業プロセスは、テストツールと連携した本ツールを使用することで自動的に管理できる。各種開発成果物間のトレーサビリティの表示例を図 15-B-3-6 に示す。図 15-B-3-6 では、デザインモデル上の下位要件（Requirements from Design Model）が本ツールにインポートされ、各要件にモデルから自動生成されたソースコード（Code Generated from Design Model）が紐付けされて、検証項目（Verification Activities）が設定され、検証結果（Test Data Reports）にリンクしている。

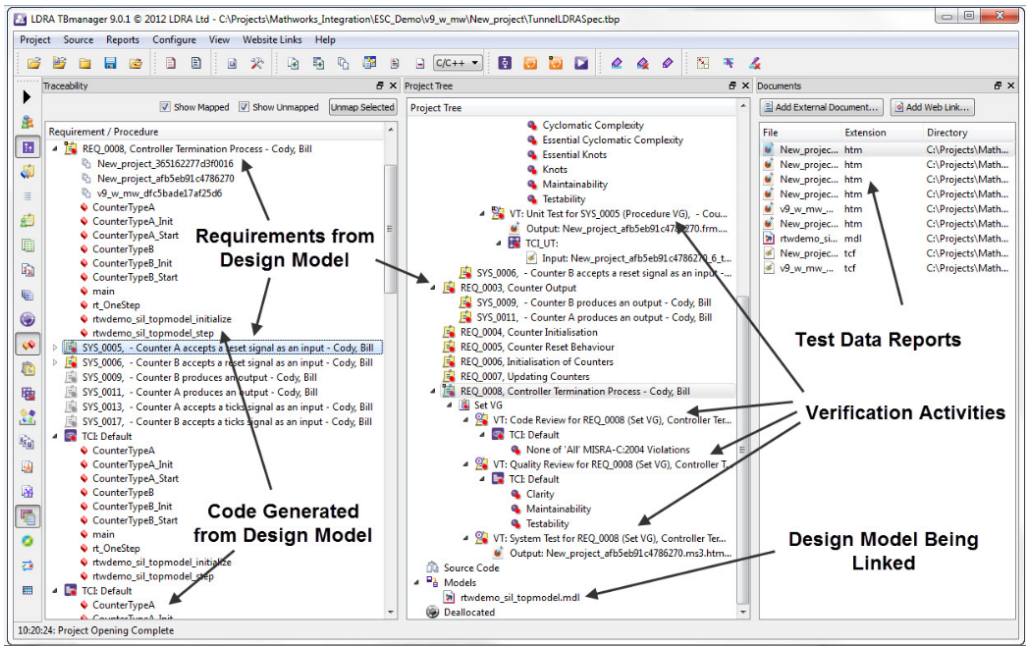

図 15-B-3-6　各種開発成果物間のトレーサビリティの表示例

このように、成果物まで含めたトレーサビリティ管理の自動化を図り、検証計画・実施・実証などを高度に一体化したワークフローを支援できることで、生産性が向上し、国際スタンダードへの準拠と、開発工数と納期の順守などの、市場要件を満たすことができる。

また、要件から検証結果までのトレーサビリティ管理の自動化を図り、検証計画・実施・実証など高度に連携したワークフローが支援されることで、間違いの元になる人手に頼った作業の多くを排除できるとともに、限られたリソースと工数で、国際スタンダードなどの監査要件を満たすエビデンスを残すことができる。

5. 適用後の課題と今後の活動

トレーサビリティをより正確に管理するためには、要件、設計、検証結果といった様々な成果物を正しくインポート／エクスポートできる機能と検証作業の結果を連携させることが必要であり、適用後の課題は、これを継続的に強化していくことに力を注ぐことである。

開発ライフサイクルにおける要件トレーサビリティとテスト手法は、組込みのアプリケーションを含む種々のアプリケーションにもマッチし、その効用は、セキュア、ミッションクリティカルなアプリケーションを実現できることである。

ISO 26262、DO-178B/C、IEC 61508 などスタンダードへの準拠が必要な場合、本手法を採用することで、監査の要求に対応できる開発体制を容易に構築することができる。

米国 Mectron 社では、民間航空機システムや防衛システムの国際スタンダード DO-178B/C のソフトウェア認証取得に必要な監査証跡を目的に TBmanager を採用した。スタンダード認証には、IBM® Rational® DOORS®の要件エンジニアリングデータベースから、ソースコード、ソフトウェアテストに至る、要件から全システムへのリンクを示す必要があったが、本ツールにより、認証／検証作業は効率的に管理され、開発予算内で納期通りに出荷できたことが Mectron 社から報告されている。

今後は、航空機をはじめ、国内外の機能安全を求められる他の案件に取り組む予定である。

6. まとめ

近年、安全性や高いセキュリティ性能を求められるアプリケーションの開発が急速に増えている。また、コンプライアンスを満たすといった市場要求から、開発手法やテスト自動化の改善が迫られている。

TBmanager は、国際スタンダードに準拠し、要件から検証結果までトレーサビリティ管理の効率化を図った。また、国際スタンダードの認証プロセスの計画・実施・実証が高度に一体化された環境を整備して、要件定義から検証までの一連のワークフローにおける作業を支援することができた。この結果、間違いの元になる人手に頼った作業の多くを排除し、限られたリソースと工数で、監査要件を満たすエビデンスを残すことができた。そして国際スタンダードへの準拠と、開発工数と納期の順守といった市場要件を両立することが可能となった。

参考文献

[1] M. A. Hennell, J. C. P. Woodcock and M. R. Woodward
THE SAFETY INTEGRITY LEVELS OF IEC 61508 AND A REVISED PROPOSAL、
http://www.cems.uwe.ac.uk/~ngunton/worksheets/sil_proposals.pdf
[2] TBmanager　Team-wide Workflow Management Software、
http://www.ldra.com/en/tbmanager
[3] MEDTEC Japan Onlin、医療機器の開発者に求められる IEC 62304 の知識、
http://www.jmdmt.com/ja/news/2011/04/14/497
[4] モデル駆動型開発における要件トレーサビリティの課題、
http://www.fuji-setsu.co.jp/products/LDRA/Traceability_MDD.html