



【信】品質説明力のある、 高信頼性ソフトウェア開発への チケット駆動開発適用

2017年4月13日

イーソルトリニティ株式会社

本資料使用上の注意

- 本資料はイーソル株式会社およびイーソルトリニティ株式会社（以降弊社）の著作物であり、本資料の著作権は作成者である弊社が有します。
- 本資料の利用は個人の範囲に限ります。
- 本資料の商用利用（著作物の複製・上演・演奏・公衆送信及び送信可能化・口述・展示・上演及び頒布・貸与・反訳・翻案・二次著作物の利用）はこれを禁じます。
- 本資料は講演資料を抜粋したものです。
- 講演資料はイーソル株式会社のWebにて公開いたします。

はじめに

- 近年「安心・安全」が重要な関心事となり、コンピュータやコンピュータが搭載される機器（システム）にも「安心・安全」が求められている。
- 安全な製品開発は、製品に高い信頼性を持たせるために開発であり、これは、事前に合意した開発プロセスにそって、安全への要求を定義し、それを確実に設計・実装・テストするとともに、プロジェクトが確実に実施されていることを確認することで実現される。
- これらは、開発プロセスの定義と遵守、開発要求の確実な追跡とプロジェクト監査によって実現するが、大変に手間がかかる。
- この課題に対してチケット駆動を応用することで業務改善を実現したので、その内容を紹介する。

コンピュータ搭載システム (組込みシステム) を取り巻く状況 ～安心・安全への要求～

組込みシステムに機能安全が求められる状況

• 組込みシステムの適用範囲の拡大

- 安全装置へのコンピュータ適用
- 機械的／電氣的に実現していた（安全）機能をソフトウェアが実現
⇒ソフトウェアが“安全”の責務を負う
※物理的対策（機械的、電氣的）がソフトウェアに置き換わる
→センサーで検出しCPU（ソフトウェア）が判断し対応する

• 安全に対する社会意識の変化＝証明／説明責任の発生

- 先端技術の潜在リスクに対する不安
- メーカーの説明／証明責任の要求の高まり

• 組込みシステムが“繋がる”ことによる複雑化

- 繋がる組み合わせは無限大
 - 繋がった先の品質は保証されとは限らない
- 複雑化により信頼性・安全性の確保が困難に

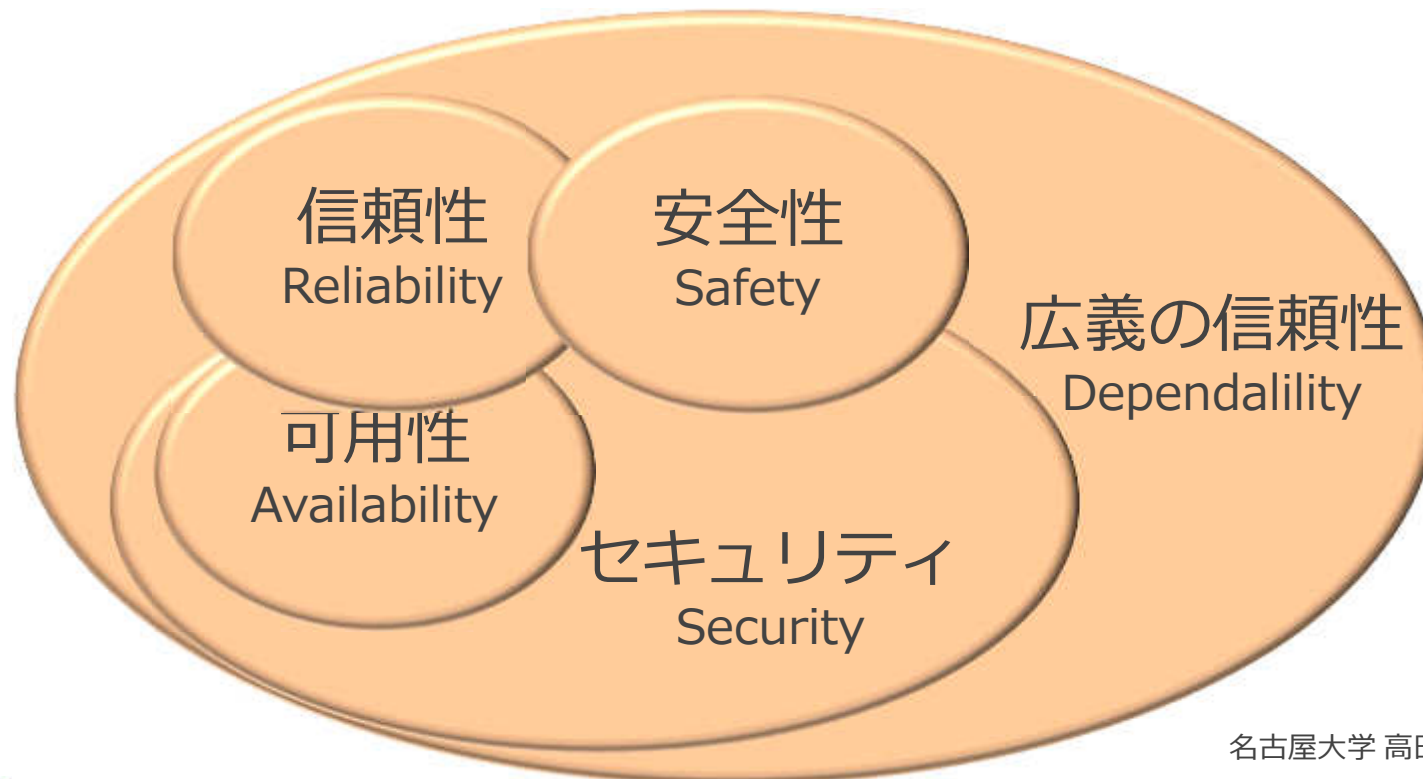
留意すること

- **安全対策は“新しい概念・活動”では無い**
 - “安全の確保・実現”は当たり前の要求
 - “生命維持”は本質的要求
 - 交通（車・鉄道・船舶・航空）
 - ⇒ 無事故を実現（危険を回避）するための各種方策や仕組み
 - 家電
 - ⇒ 発火・発煙の防止策（主に電気回路）
 - ⇒ 誤動作・誤使用の回避策（主に機構、使い方）
- **安全に対する社会意識の変化＝証明／説明責任の発生**
 - これまで：メーカーのノウハウを無条件に信頼
 - これから：エビデンスによる社会への説明／証明
- **安全規格（ISO/IEC/IEEE/JIS）は安全を説明するための枠組み**
 - エキスパートのノウハウ・ベストプラクティス集
- **安全規格はPL法（製造者責任）対策**
 - 開発・製造過程に瑕疵が無いことを証明方策を提示

安全開発・高信頼性開発の要点

用語：信頼性と安全性

- 広義の信頼性（Dependability）
 - 狭義の信頼性（Reliability）、可用性（Availability）、安全性（Safety）、セキュリティ（Security）を包含する概念

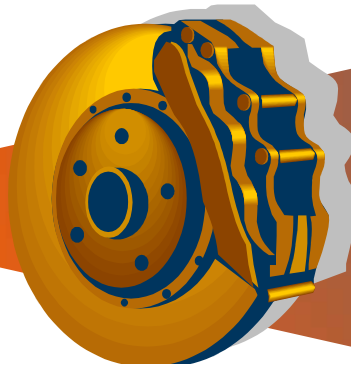


名古屋大学 高田教授の資料より抜粋

用語：信頼性と安全性

• 安全性は信頼性の上に成立する

- システム＝機能の集合体として1つ1つの機能の信頼性が確保されることにより安全を実現する
- 信頼性の向上／確保を実現する装置・部品や開発・製作の過程が重要視される



車の安全

安全性：ブレーキ

信頼性：ブレーキを構成する部品の信頼性

ブレーキ設計の信頼性

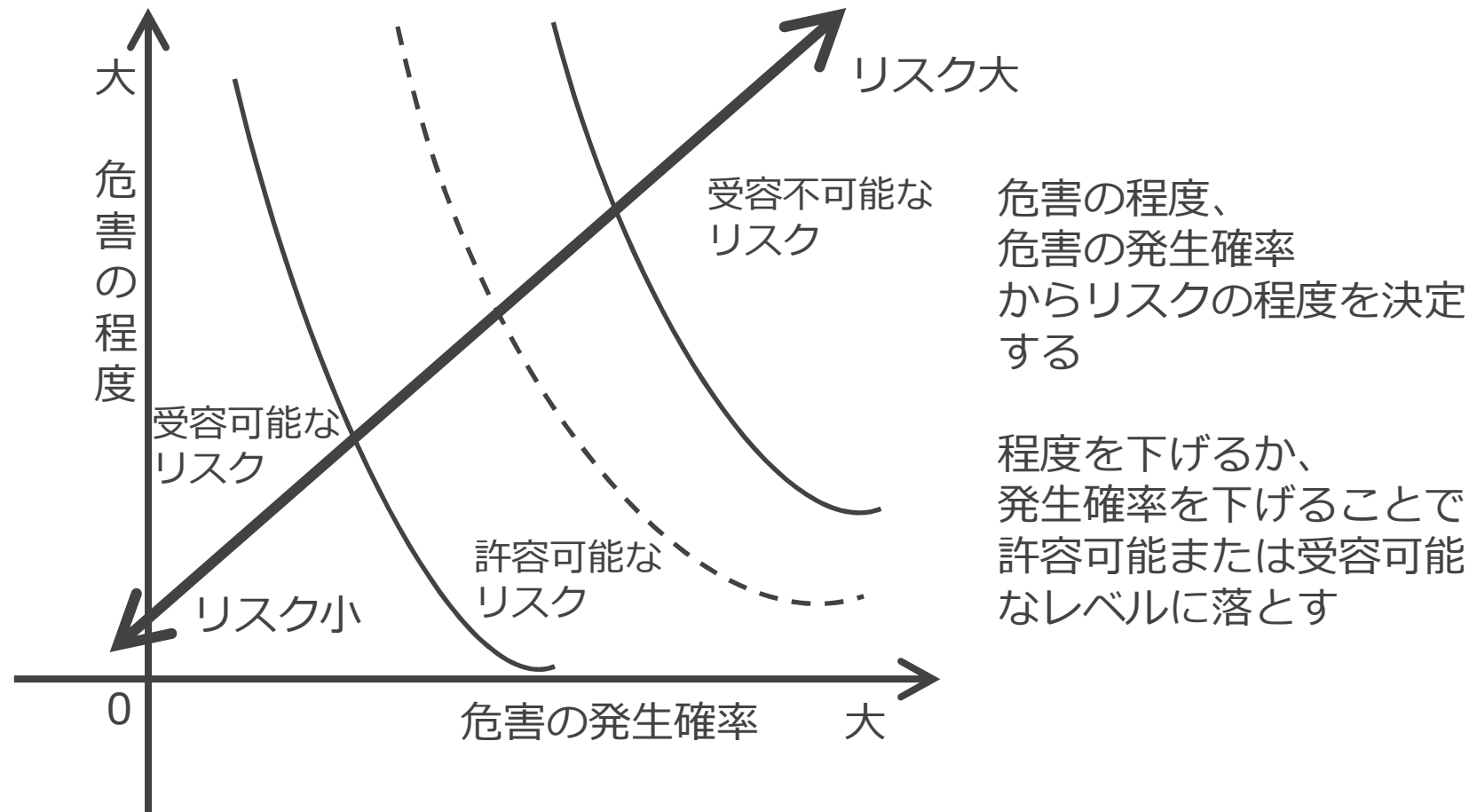
ブレーキ製作の信頼性

規格による安全の定義

- ISO/IEC Guide51 (JIS Z 8051)
 - 受容できないリスクからのがれていること
原文：“Freedom from unacceptable risk”
- ISO 26262
 - 不合理なリスクが存在しないこと
原文：“Absence of unreasonable risk”
要は
 - 「危険でない状態（リスクが無い状態）」
 - 但し
 - 「リスクゼロの状態」の意味ではない
「リスクを受容できる状態が安全である」という意味
⇒ **「リスクが受容可能な状態まで抑えられている状態」**
を安全と定義

安全の確保（リスクの低減）イメージ

- ISO/IEC Guide51の定義（概念図）

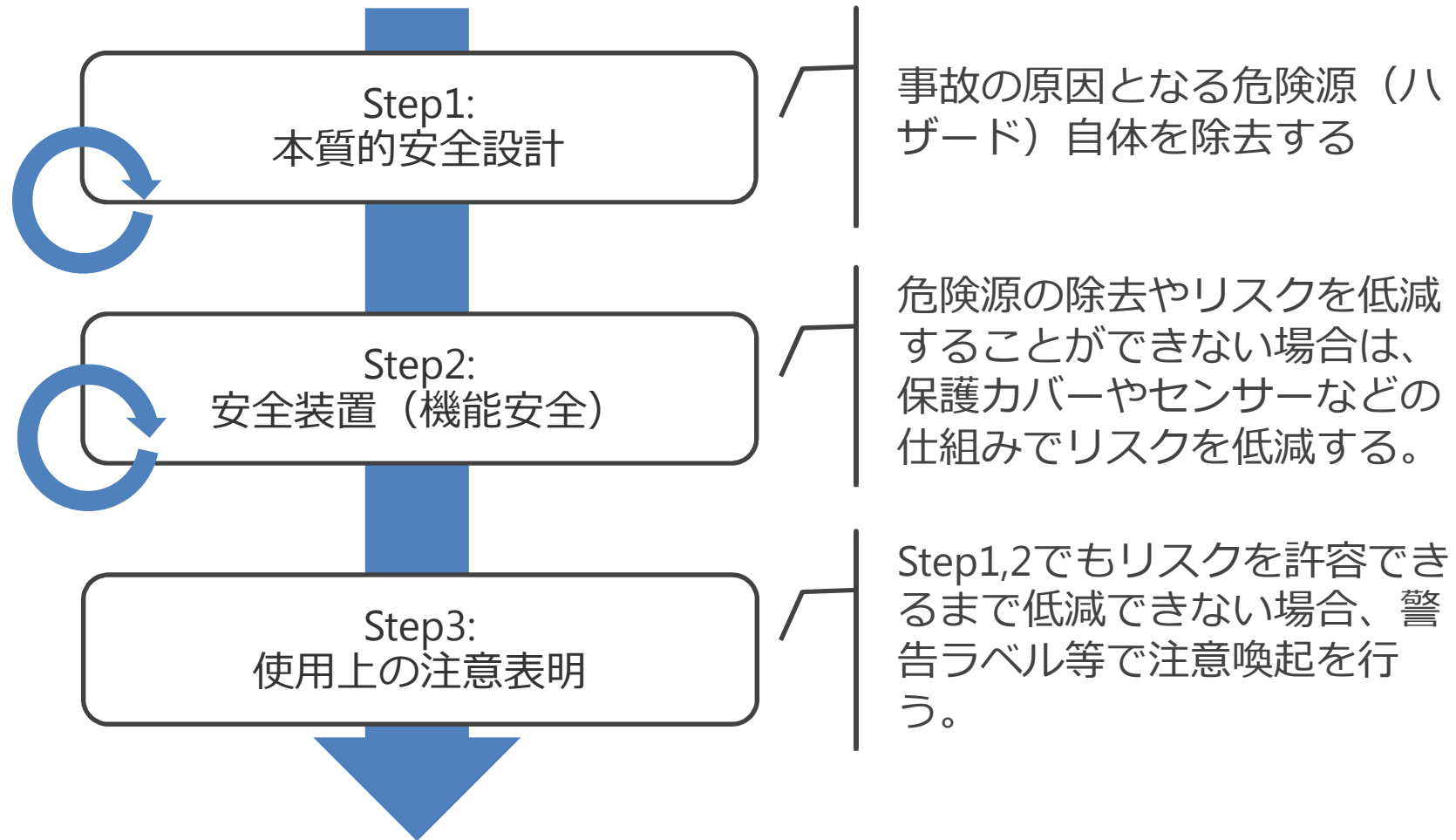


システム／ソフトウェア製品品質と利用時の品質

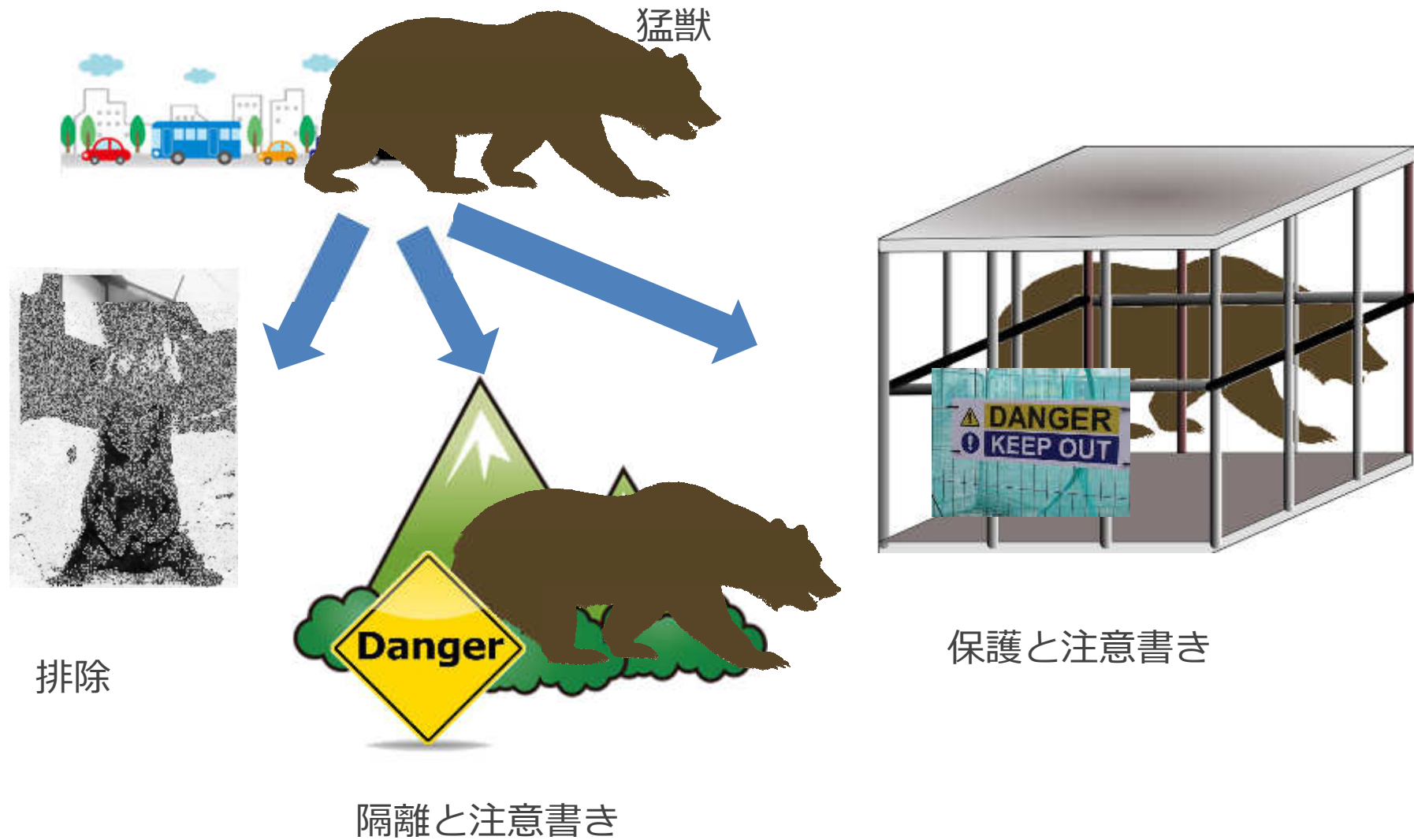
- ISO/IEC9126 Software engineering -- Product quality –
 - ソフトウェア品質特性のひとつとして定義
 - 利用時品質の“安全性（Safety）”
詳細は規定されていなかった
 - ISO/IEC9126 は ISO/IEC25000シリーズに置換えられた
- ISO/IEC 25000： Software Engineering
-- Software product Quality Requirements and Evaluation (SQuaRE) –
 - 利用時の品質のひとつ“リスク回避性”として定義され副特性も定義
 - “リスク回避性(freedom from risk)”
 - ・ 経済リスク緩和性
 - ・ 健康・安全リスク緩和性
 - ・ 環境リスク緩和性

リスク低減の方策

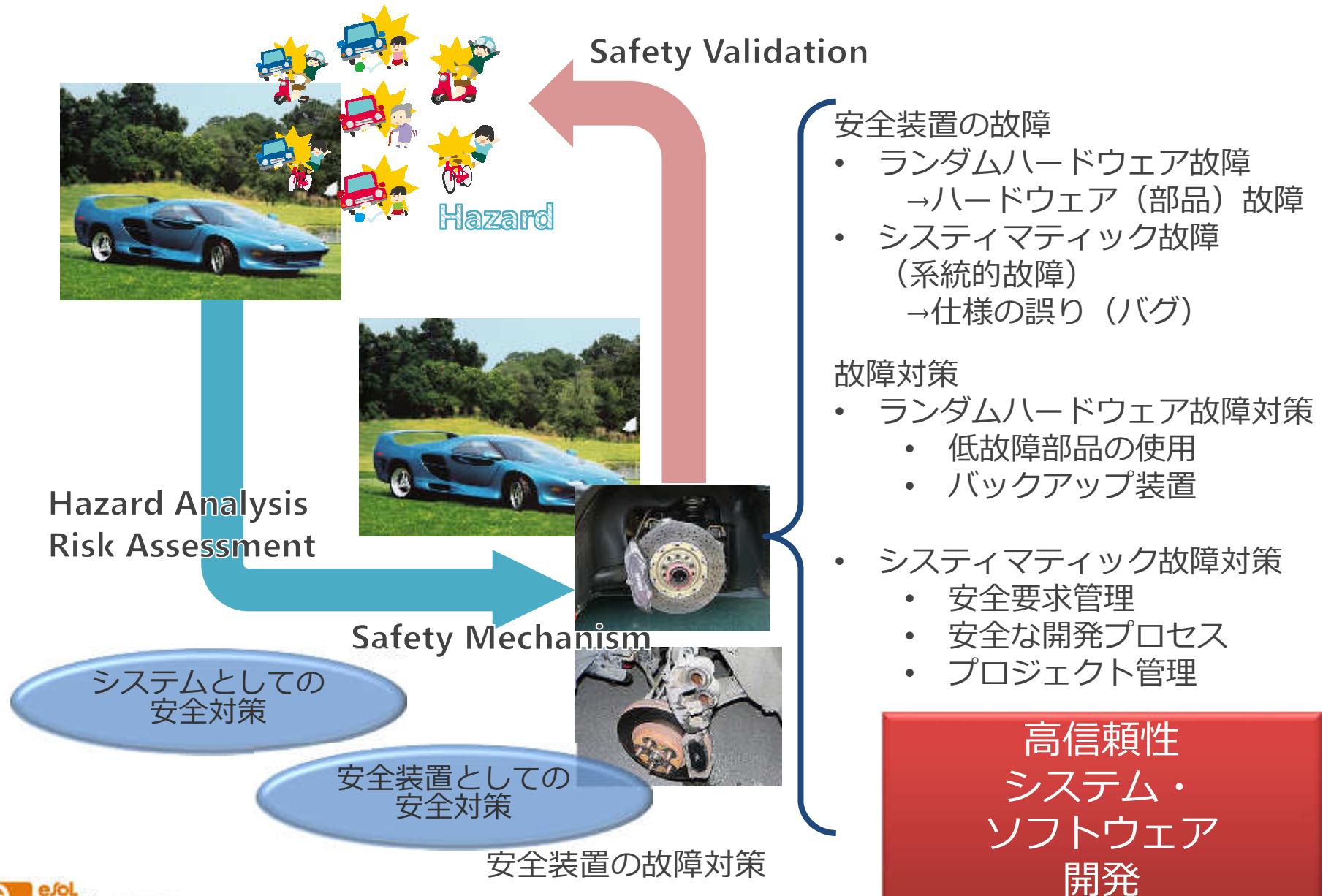
- 3-Step-Method



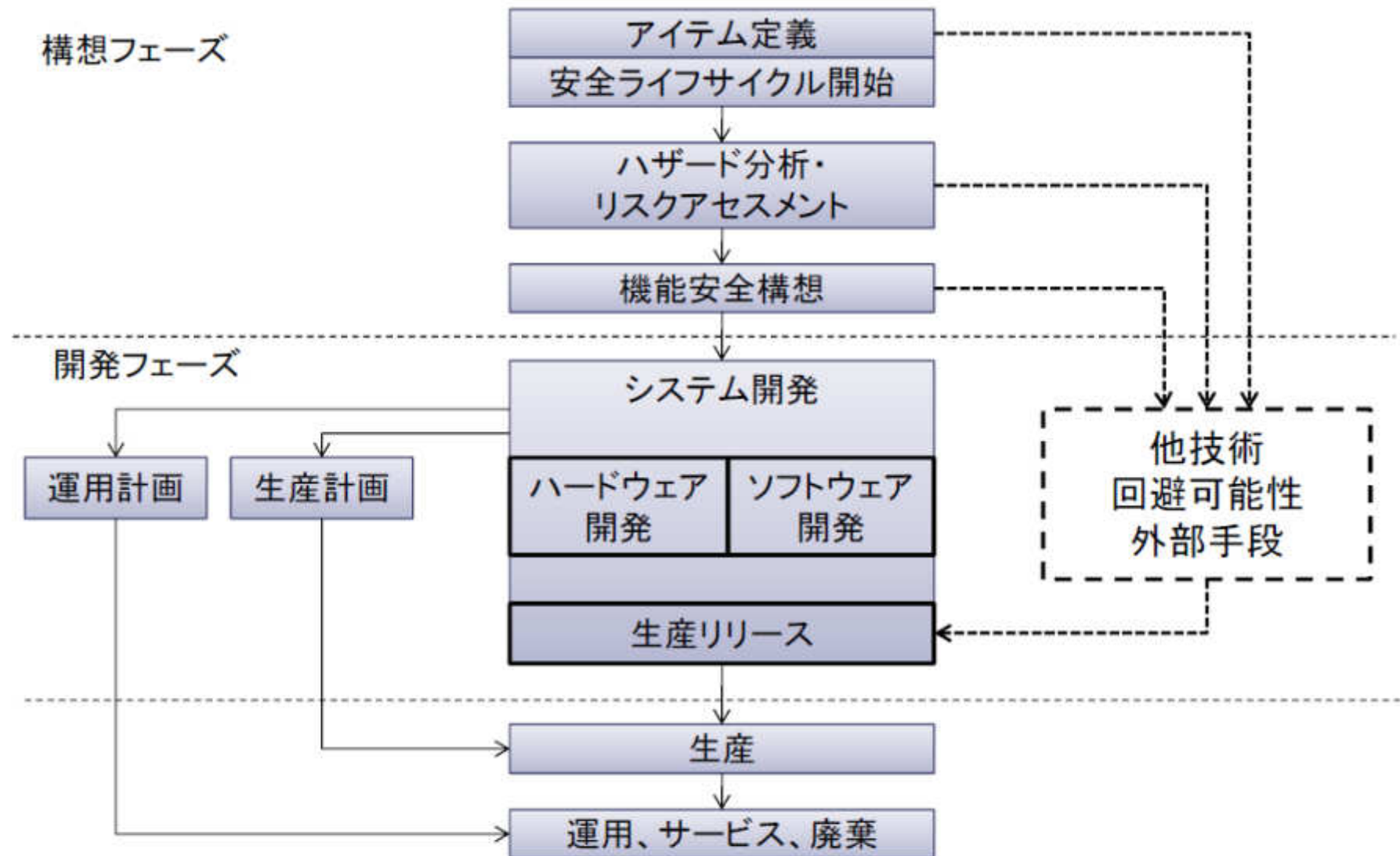
安全達成イメージ



Safety Systemの構築

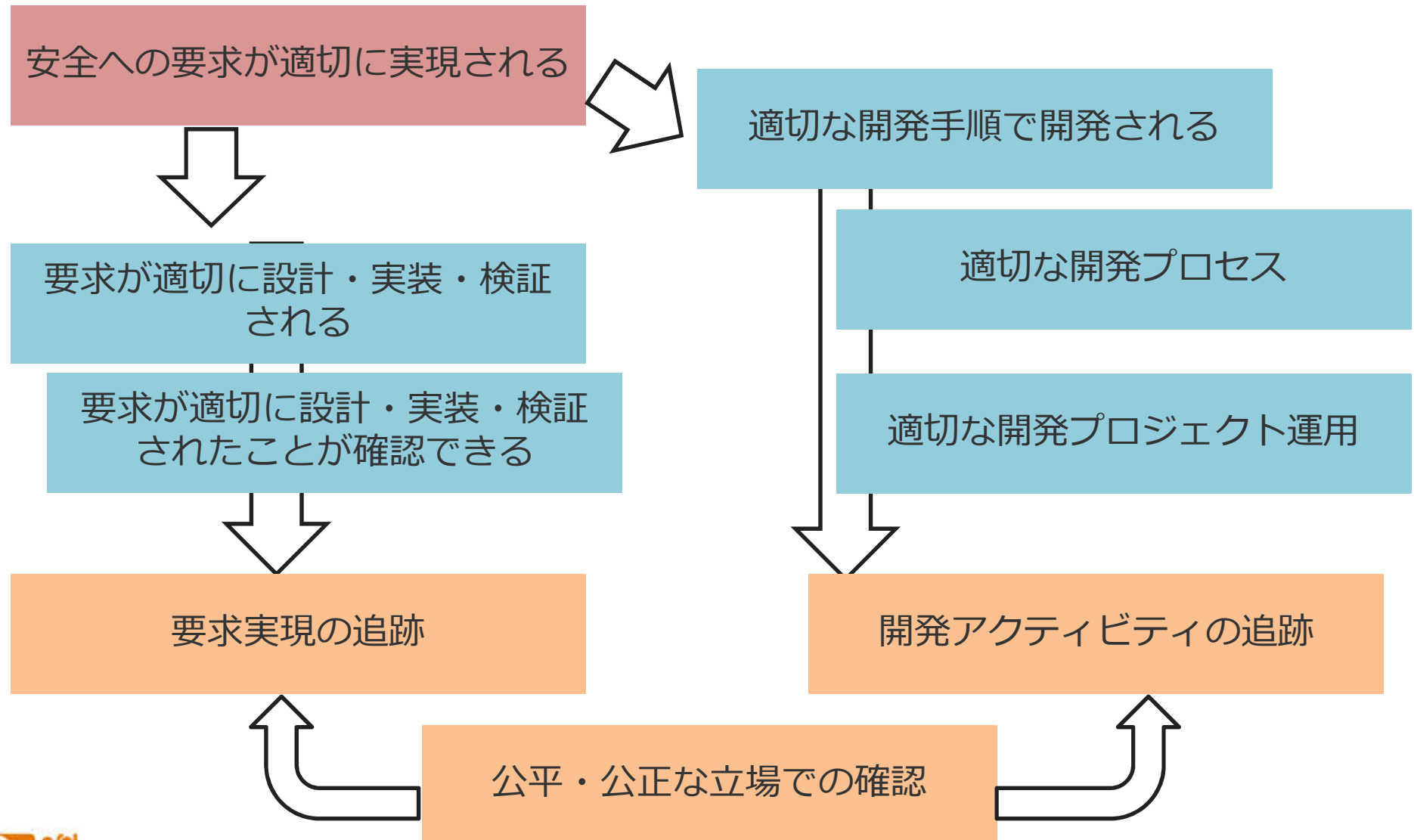


高信頼性開発≡安全ライフサイクル



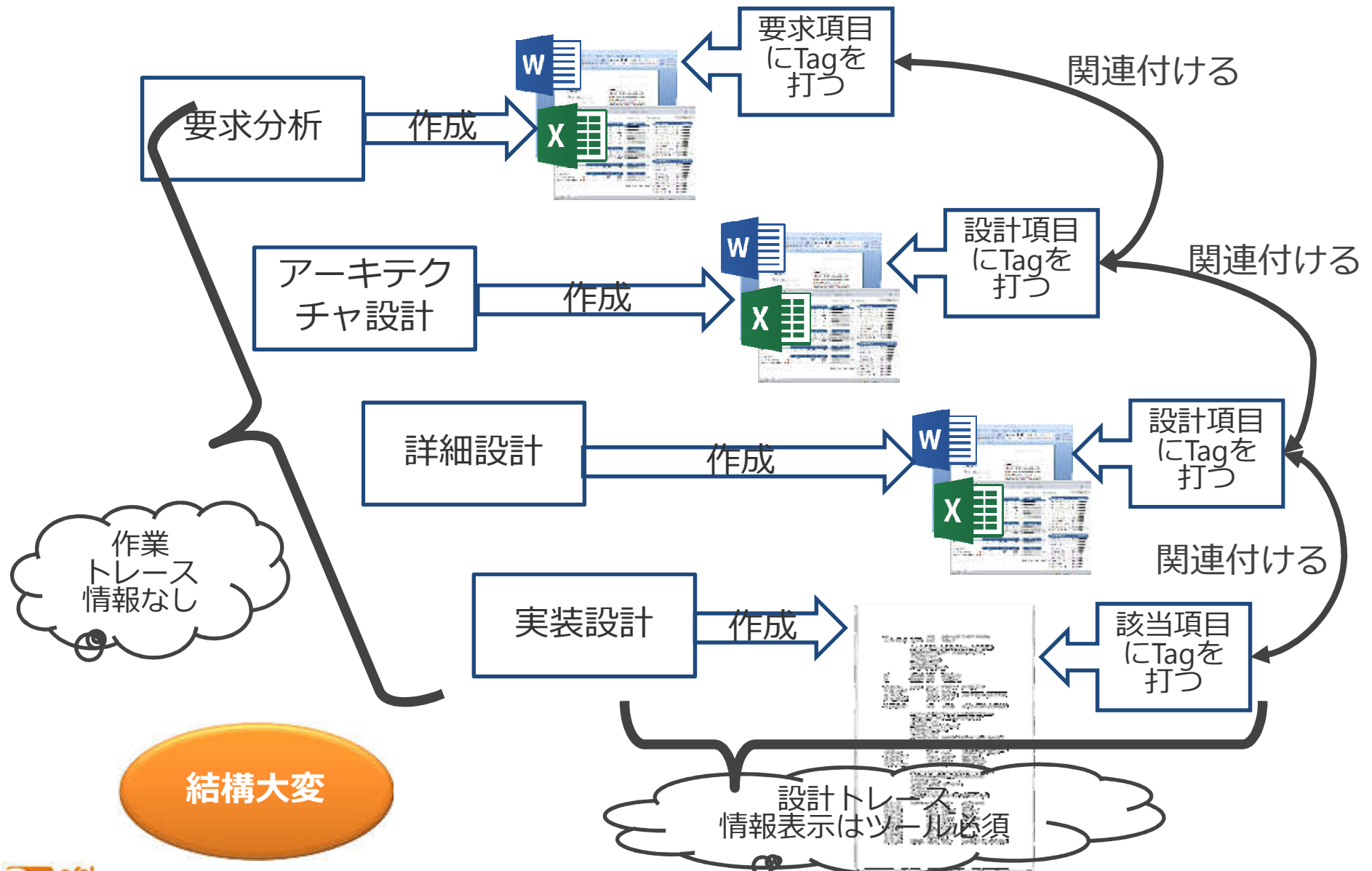
出典:ISO 26262第2部から引用

高信頼性開発の肝



高信頼性開発へのチケット駆動適用

要求トレーサビリティ確保：従来手法

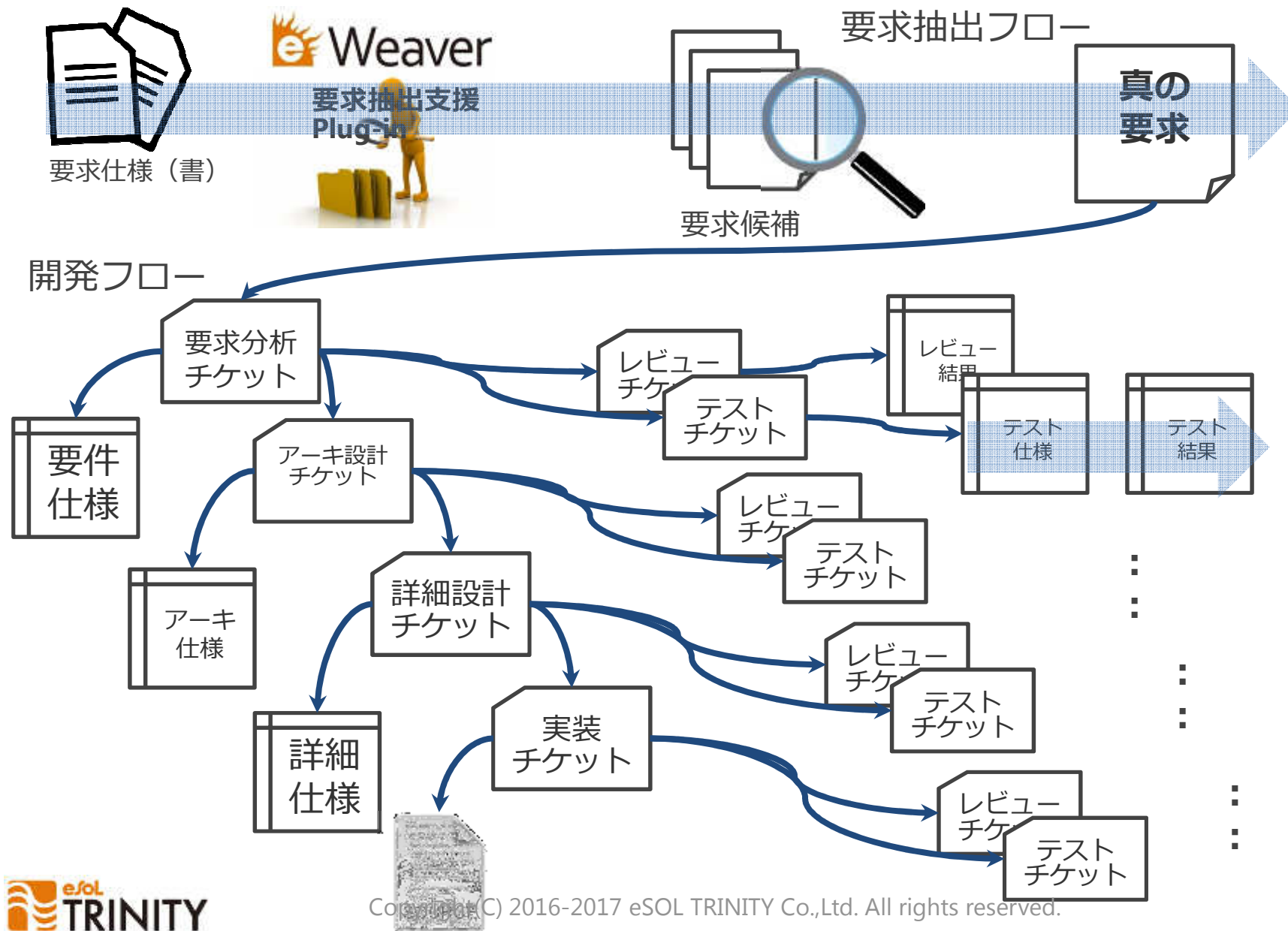


要求実現の追跡

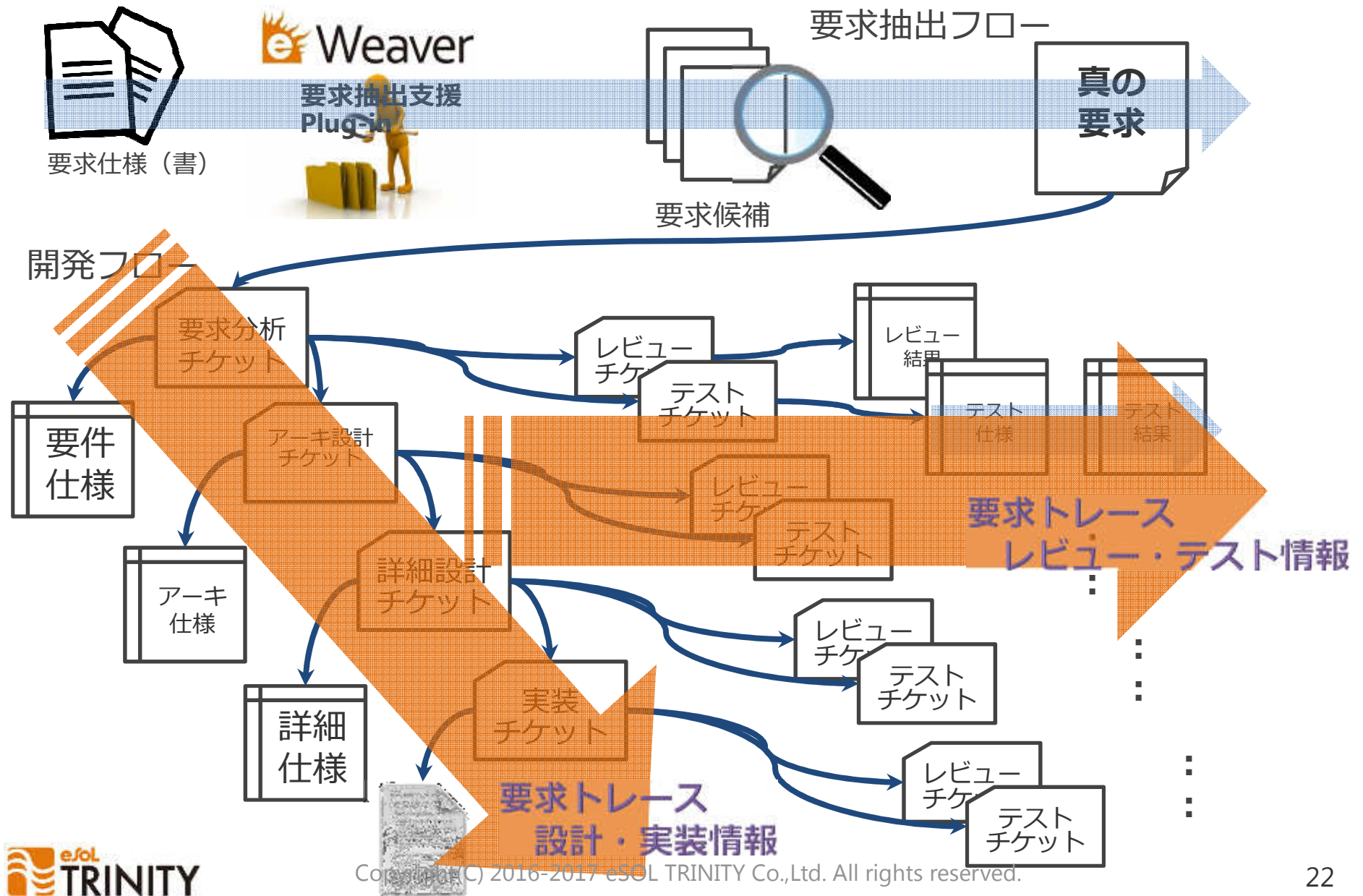
適切な開発プロセス

適切なプロジェクト運営

eWeaver上での開発フロー



要求トレーサビリティ



要求とアーキ設計のトレース

任意のトラッカーを
キー列として選択

キー列のアイテムにリン
ケージされた各トラッカー
のアイテムの表示

トラッカー	項目名
Requirement	2.2 保護機能
Requirement	2.2.1 【REQ004】 保護機能における機能レベルの設定
Requirement	【REQ004】 保護機能における機能レベルの設定
Requirement	2.2.2 【REQ005】 メモリ保護機能における実装依存性の削減
Requirement	【REQ005】 メモリ保護機能における実装依存性の削減
Requirement	2.2.3 【REQ006】 メモリ保護機能のコンフィギュレーションの標準化
Requirement	【REQ006】 メモリ保護機能のコンフィギュレーションの標準化
Requirement	2.2.4 【REQ007】 非信頼OSアプリケーションに対する
Requirement	【REQ007】 非信頼OSアプリケーションに対する
Requirement	2.3 マルチコア対応
Requirement	2.3.1 【REQ009】 マルチコア対応OSのリアルタイム性
Requirement	【REQ009】 マルチコア対応OSのリアルタイム性

ArchitectureDesign

リンケージの抜けもれチェック

アイテム 一覧リンケージ 紐付リンケージ トレーサビリティ表示 リポート リンク

[第1・第2トラッカー]を選択して[適用]ボタンを押下し、トレーサビリティマトリクスを表示します。[検索キーワード]によって、さらに絞り込み検索します。

第1トラッカー Requirement ▼ 検索キーワード
第2トラッカー ArchitectureDesign ▼ 検索キーワード 適用

リンケージを確認したい二つのトラッカーを選択

Detailed relation table

Requirement	ArchitectureDesign	リンケージ数
32	2056	136

リンケージされていないアイテムの一覧表示

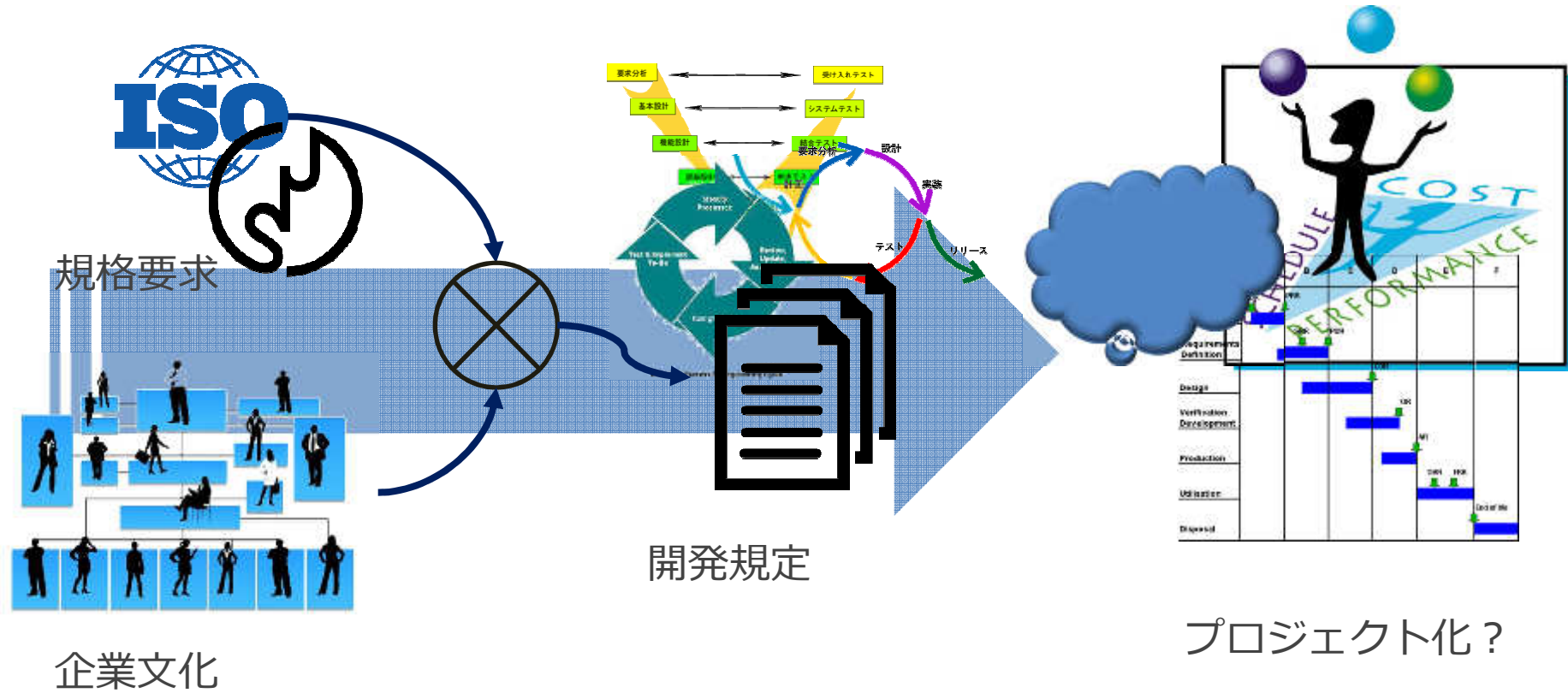
● リンケージなしアイテム リンケージ済みアイテム 表示切替

※ 青文字は、親子関係のリンケージがあるアイテムを示します。

Requirement	ArchitectureDesign
#10000069: 2.3.9	#10011493: 2.25.2.10Cの識別
#10000068: 2.4 その他	#10011492: 2.20.3システムリービストの不正な処理への保護
#10000067: 2.3.3 マルチコア拡張	#10011491: 2.14.1 フックルーチンの識別
#10000066: 2.2.5.2.2.2	#10011490: 2.13.6 スケジュールテーブルの操作
#10000065: 2.1 AUTOSAR OS仕様との関連	#10011489: 2.30 ファイル構成
#10000064: 2.4.2 [REQ020] 安全性の向上	#10011488: 2.28.2 ミューテックスの操作
#10000063: 2.4.1 [REQ019] OSによるメモリ活用	#10011487: 2.26.2 スピンロックの操作
#10000062: 2.3.4 [REQ018] マルチコア対応OSにおけるアプリケーション単位	#10011486: 2.22.4 強制終了処理
#10000061: 2.3.3 [REQ016] マルチコア対応OSにおけるコア間通信	#10011485: 2.20.1 処理単位の不正な処理に対する保護
#10000060: 2.3.2 [REQ013] マルチコア対応OSにおけるプログラミングによる非同期動作	#10011484: 2.18.6 OSAPの操作
#10000059: 2.3.1 [REQ012] マルチコア対応OSにおけるマルチタスク処理	#10011483: 2.13.5 スケジュールテーブルの非同期操作

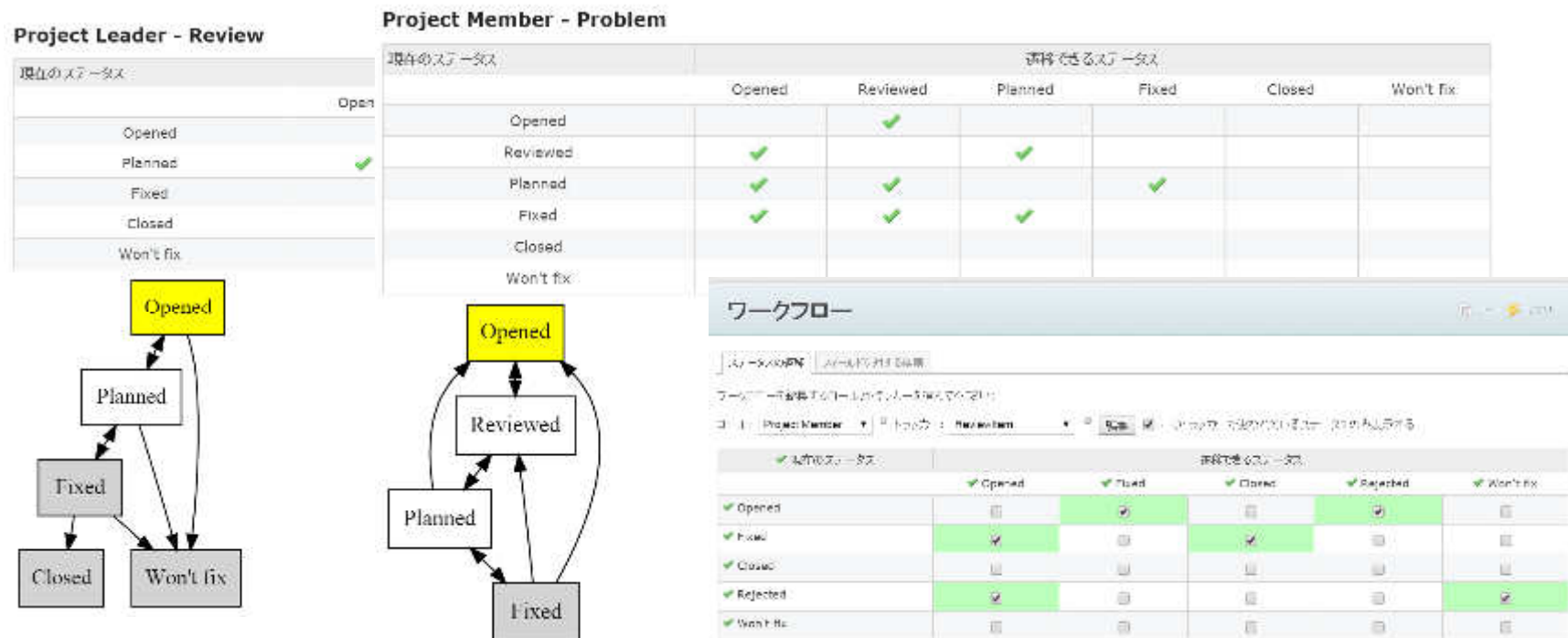
要求実現の追跡
適切な開発プロセス
適切なプロジェクト運営

プロセス作成からプロジェクト運営

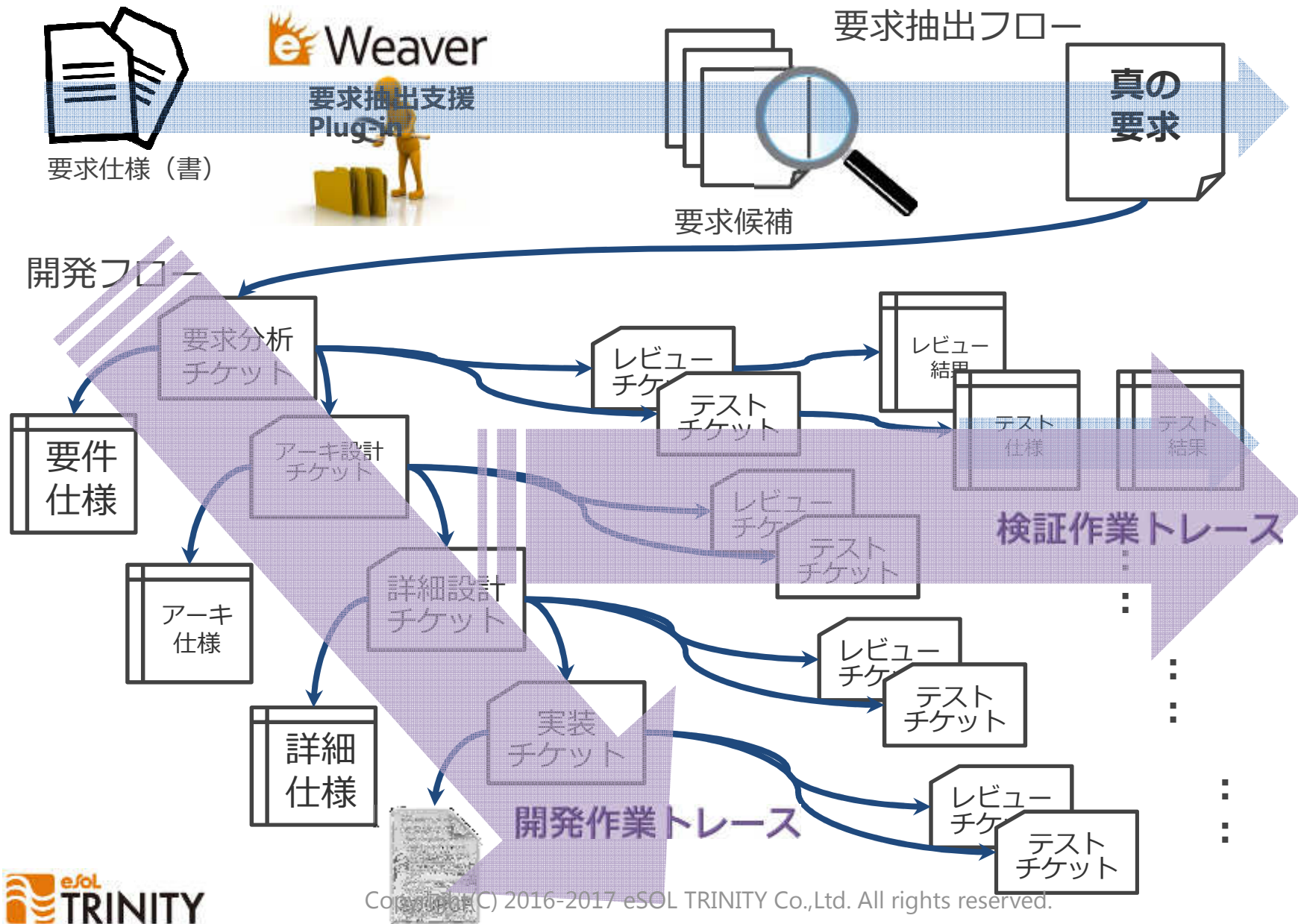


Redmineによるワークフロー定義

- プロジェクト関係者のワークフローを定義できる
- トラッカーと呼ぶチケットの種別定義を用いて、チケットが持つ情報を設定でき、この**トラッカー毎**にワークフローが設定できる



作業トレーサビリティ



海外事例とその応用

SafeScrum

独立系研究機関SINTEF（ノルウェー産業科学技術研究所）で開発・改良が進められている手法

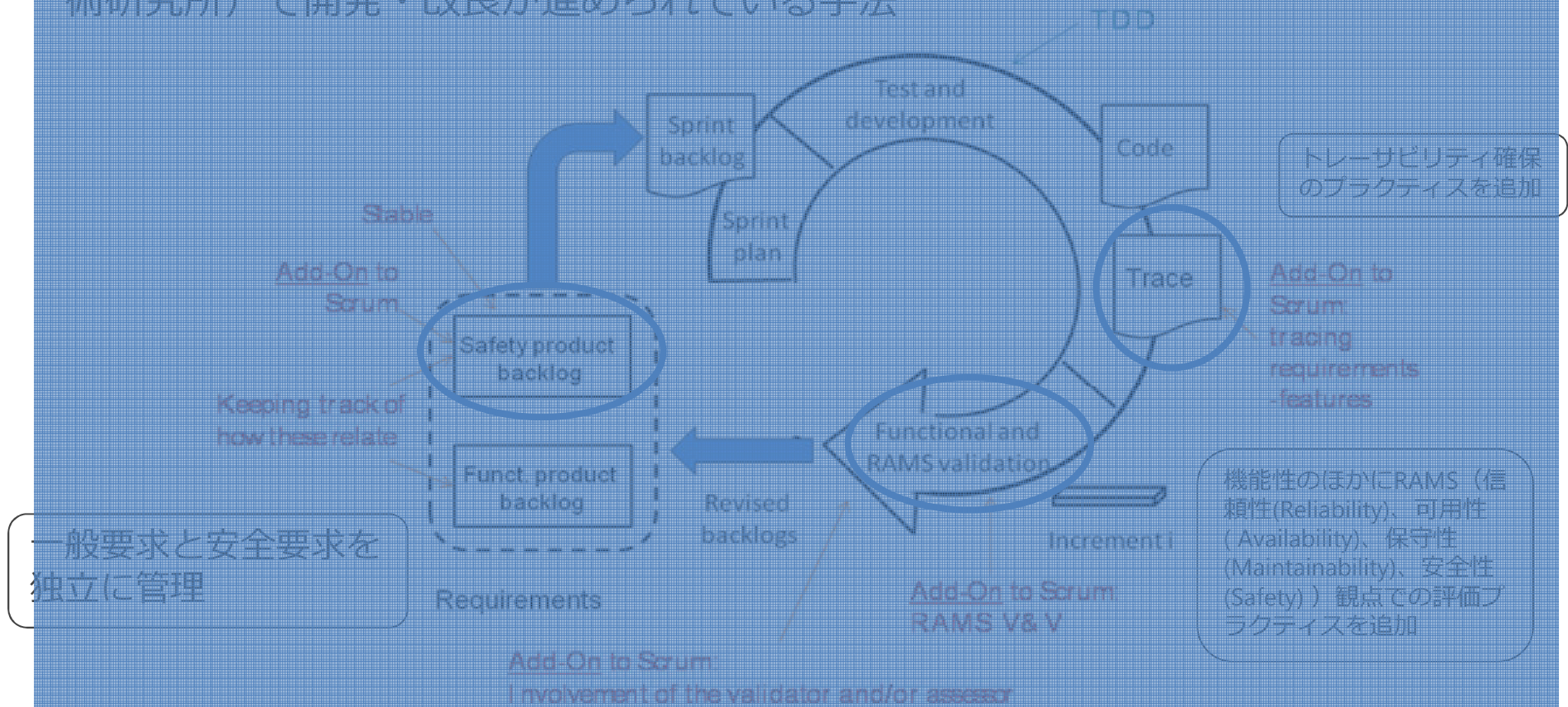


Figure 2: The SafeScrum model. TDD: Test Driven Development

Agile in Automotive (Cycle Model)

Kugler Maag CIE社（独）で開発・改良が進められているSCRUMの拡張手法

Agile in Automotive:
a Process using Repeated Cycles (Scrum Sprint)



Ro
安
M

Agile on Automotive (Roles)

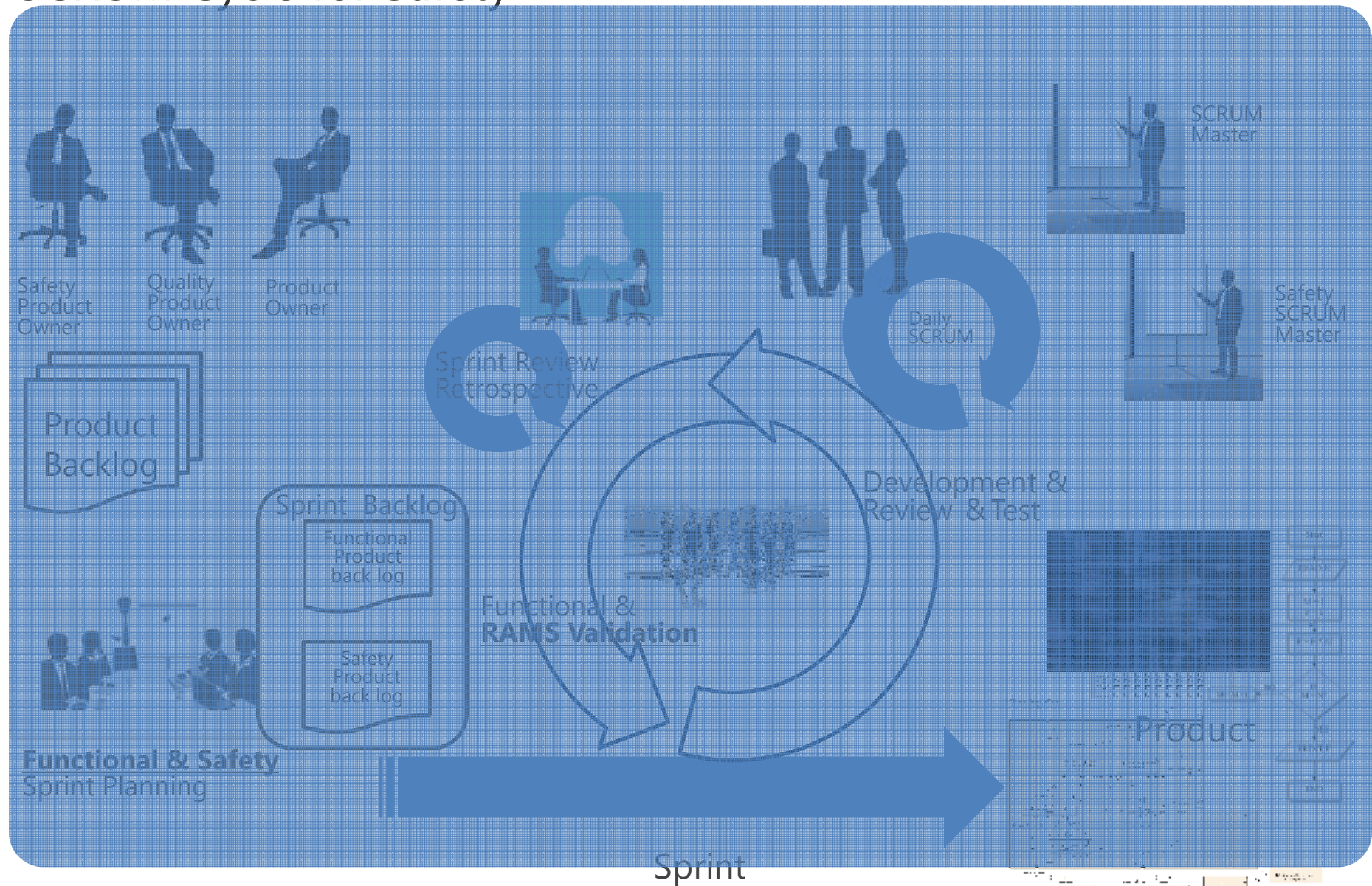


出典：AGILE IN AUTOMOTIVE SCRUM POKET GUIDE（ENGLISH VERSION） KUGLERMAAG CIE

SCRUMサイクル

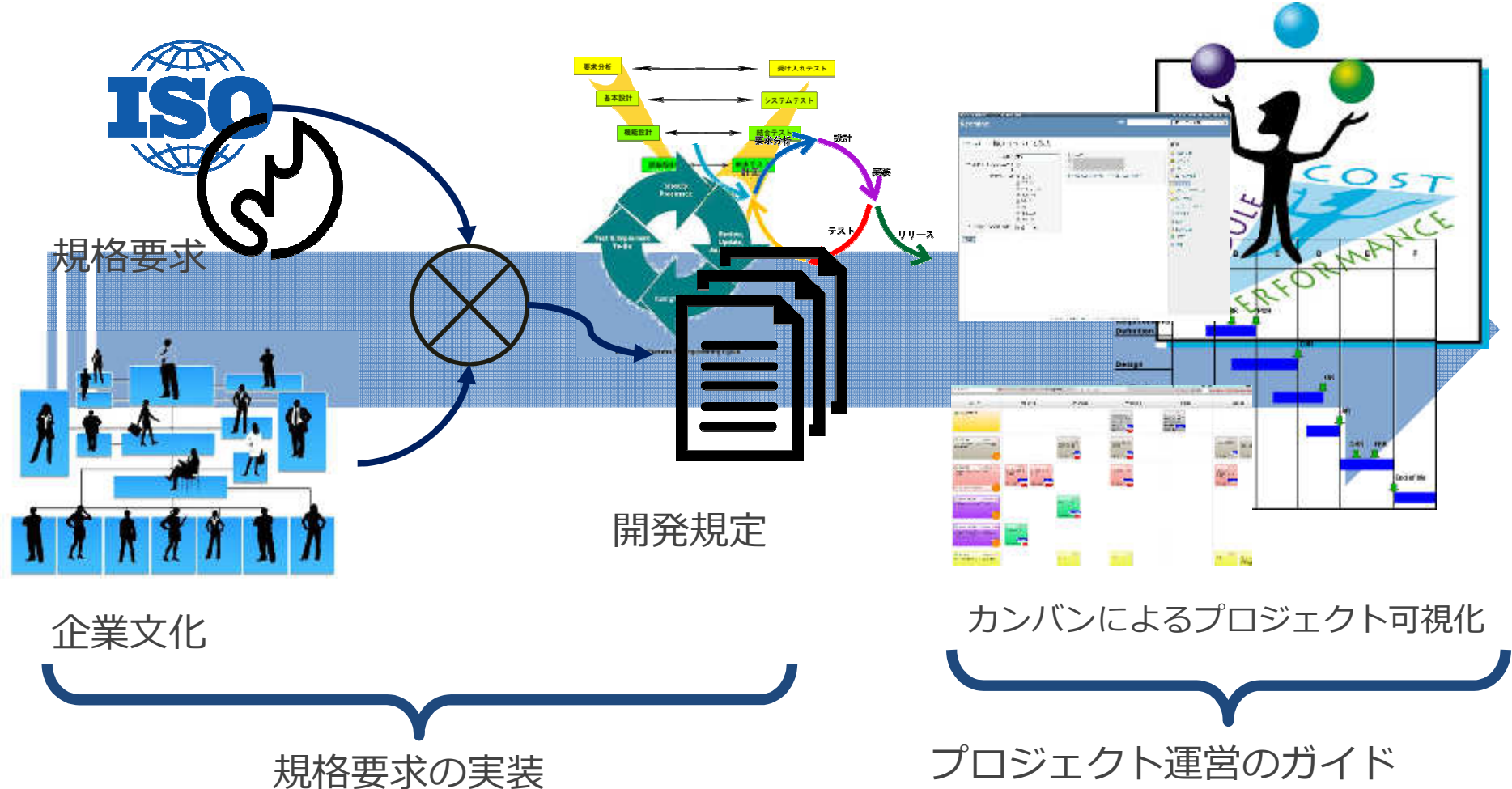


SCRUM Cycle for Safety



プロセス作成からプロジェクト運営

ワークフローをトラッカーで実現



カンバン/Task

WBS※とWorkの状態を同時に表す

task status

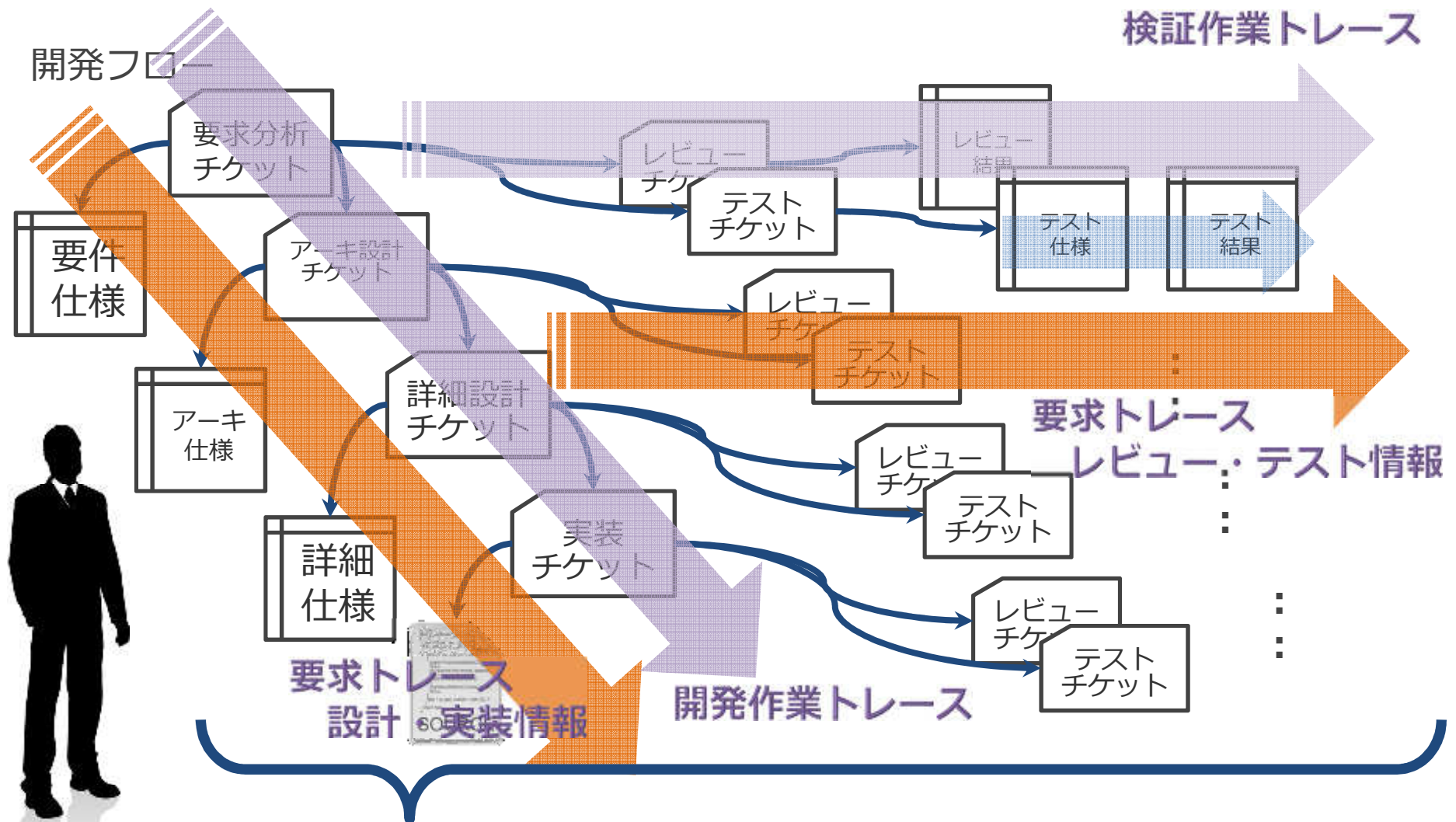
Opened Planned Working Fixed Closed

WorkingのTaskは必ず一つ
(並行で複数着手しない。
Storyも同じ)

OpenからClosedへ

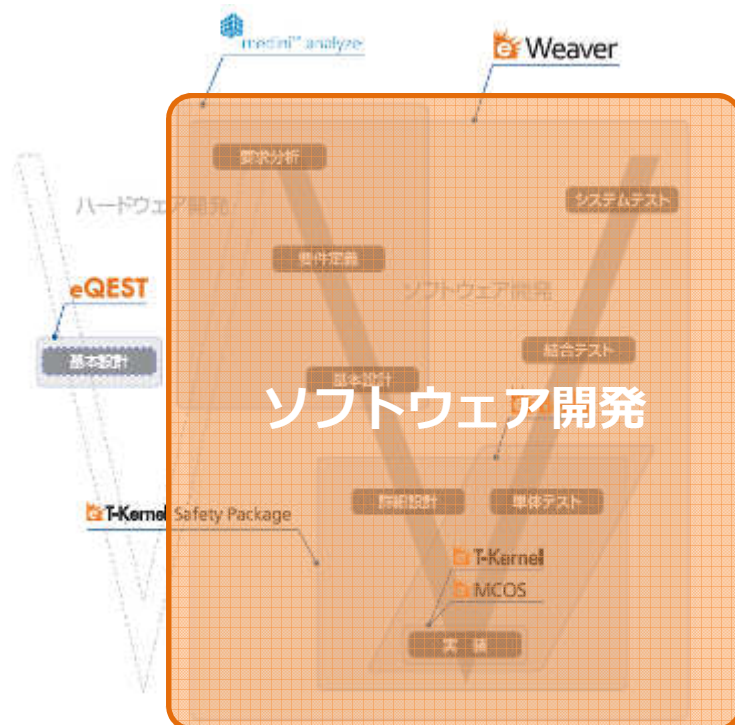
※WBS (Work-Breakdown-Structure)

適切性監査（2つのトレース情報）



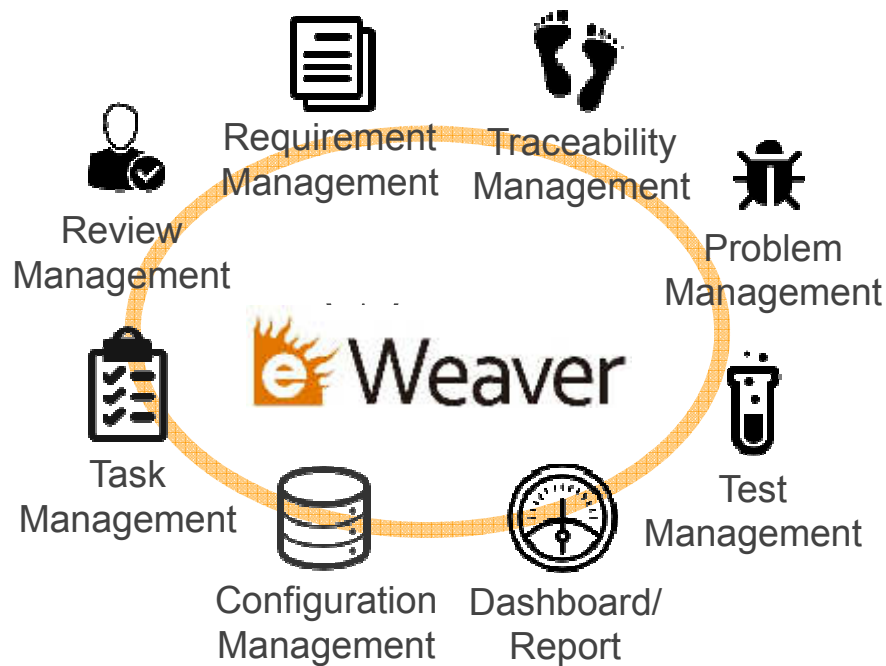
eWeaver

開発プロセス支援ツール



製品概要

ソフトウェアライフサイクル全般のプロセスの管理機能

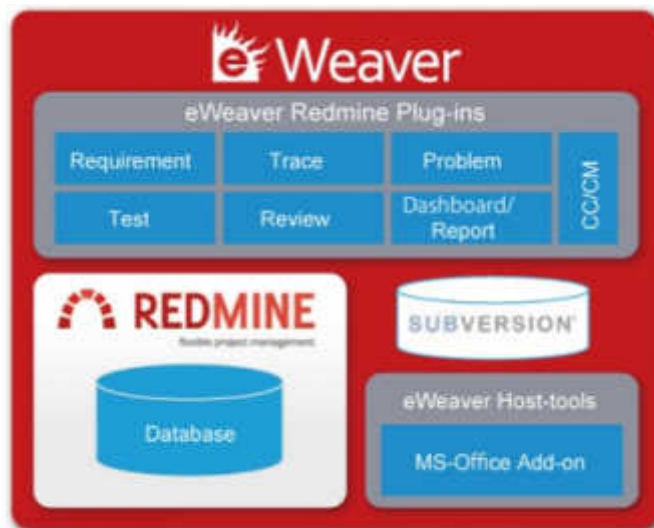


- 開発プロセス支援ツール
- 要求、仕様、コードなど、開発成果物の各種要素を「アイテム」として統一管理、これらのトレーサビリティや開発工程のアクティビティとの連携を管理
- 要求管理、テスト管理、変更/構成管理、問題点管理、障害管理、レビュー活動管理、そしてこれらのトレーサビリティ管理（ライフサイクルトレース）

高度化するソフト開発の**アジャイル化**（素早く変化に対応）と効率的な**トレーサビリティ**管理機能を付加しております

システム構成

開発に必要な機能群を**オール・イン・パッケージ**にて提供



「Redmine」や「Subversion」などのオープンソースを基盤に、マイクロソフト社の「Microsoft Word」や「Microsoft Excel」で作成した文書との連携機能を含む独自のRedmineプラグインなどを実装

期待効果

管理情報の見える化・
省力化
(追跡性の向上)



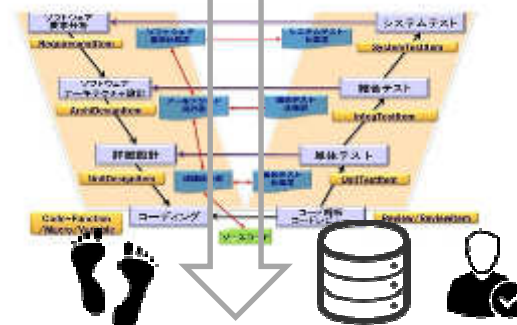
開発管理コストの削減

Scrumのサポート



頻発する変更要求に対応する
柔軟な開発管理の実現

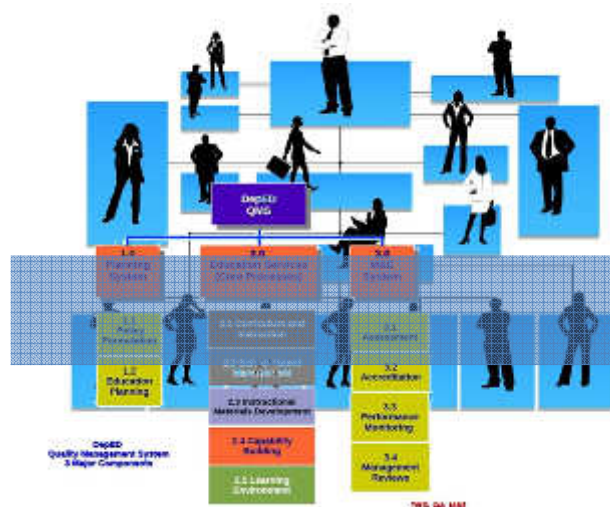
トレーサビリティ
管理機能



機能安全規格が求める
追跡性の確保

変化に強く、生産性と開発効率の高い
開発組織の醸成をサポート

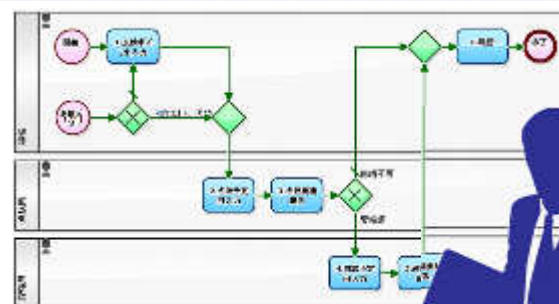
コンサルティングサービス



企業文化を活かす



最適なソリューション



業務分析
カスタマイズ

 **Weaver**

Thank you for your time
and attention.

eSOL Spirit

Core Spirit

「楽しいチャレンジ」
を生きる

Mission

私たちは、
革新的なコンピュータテクノロジーによって
市場を創造し、社会を豊かにすることを
使命とします

Vision

私たちは、
世界中で活躍する世界トップクラスの
テクノロジーカンパニーを目指します

Value

e xcellence	卓越性の追求
S peed	スピード重視
O wnership	当事者意識
L ink	絆