

SESSAME / EEBOF CONTENTS 2005 JaSS7'05

## 組み込みソフトウェア品質向上のための Activity Mapping

- 組み込みソフトウェア製品群における効率的な品質向上施策の分析 -

SESSAME 組み込みソフトウェア管理者・技術者育成研究会  
EEBOF (Embedded Engineer's Birds Of a Feather)

酒井 由夫

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EEBOF CONTENTS 2005

## プレゼンテーションのシナリオ

- 主人公は組み込みメーカーの **品質保証部門の実務担当者** と **製品開発部門のプロジェクリーダー** です
- 2人は、社長から **「ソフトウェアの不具合で製品のリコールが頻発し回収費用が利益を圧迫している。2年で回収をとまらぬリコールが起こらないようなソフトウェア開発の資格を作り、ロードマップを提出しろ！」** という特命を受けました
- この命題について2人は次のようなディスカッションをしています
  - QA 「CMMやRUPのようなプロセスを導入しよう！」
  - 開発 「それで、具体的に不具合を減らせるのか？」
  - QA 「QA部門の人員を増やし、もっと効率的かつ短期間に不具合を見つけてくれ」
  - 開発 「冗談じゃない！不具合を作り込まないようにするのが先だろ！」

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EEBOF CONTENTS 2005 日経コンピュータ 2004.12.27号「組み込みソフトの巨大化に立ち向かう」p119より

## 組み込みソフトが原因になった不具合の例

- 携帯電話やAV機器などの故障を引き起こした事例
 

公表日	社名 / 製品名	不具合の内容
2004.03.09	NTTドコモFOMA「N900i」	メモリーカードの画像を縮小加工後、電話着信や特定の操作で再起動する
2004.05.13	松下電器産業「DIGA DMR-E95H」	250Gバイト・ハードディスクの112Gバイト以降に録画 / 再生できない
2004.10.21	KDDI「W21K」	電話を発信するとほぼ同時に着信があった場合、電話番号の内容が消滅する
- 自動車のリコールにつながった事例
 

公表日	社名 / 製品名	不具合の内容
2004.03.18	英ジャガー「XJ8」など12車種	6速自動変速機で、勝手にギヤが3速に固定されたり後退に入る
2004.08.31	仏プジョー「206」など10車種	電源制御装置の不具合により、リモコン・キーでドアロック時にホーンが鳴り続ける
2004.09.14	独BMW「525i」など7車種	着座センサーの情報が感知できず、事故時に助手席エアバッグが作動しない

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EEBOF CONTENTS 2005

## 理想論でなく、実効効果の高いActivityベースで考えよう！

- その後、**品質保証部門の実務担当者** と **製品開発部門のプロジェクリーダー** は「**リコールが起こらないようなソフトウェア開発のフレームワーク作り**」という命題について冷静に考え、実効効果の高い組み込みソフトウェア品質向上のための **具体的な Activity** を洗い出し、それを開発プロセスにマッピングし、段階的に目標を達成できるようにロードマップを作りました

ソフトウェア品質向上の Activity Map

ソフトウェア品質向上の Load Map

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EEBOF CONTENTS 2005

## Agenda

- 高信頼性ソフトウェアのイメージをつかむ
- 信頼性向上のActivityをマッピングする
- 組織成熟度と注力すべきActivityの関係を知る

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EEBOF CONTENTS 2005

## 高信頼性ソフトウェアの実現イメージ

- まず、最初に**「どのようにしたら組み込みシステムを高信頼性へと導くことができるのか？」**というイメージを示します
- 最終的な**「理想モデル」**と**「そこに至るまでの過程」**を掴んでおくことは重要です

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCP CONTENTS 2005

## 高信頼性ソフトウェア・システムへの道筋

バグが多く潜在する未熟な組込みシステム

軽微なバグ

重大なバグ

システムが分割されていない

Validation Verification

QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCP CONTENTS 2005

## コア資産を切り出し、結合度を弱めます

コア資産

高凝集 (high cohesion) 疎結合 (low coupling) を目指す

Validation Verification

QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCP CONTENTS 2005

## コア資産を高凝集・疎結合にします

結合度小

コア資産

Validation Verification

QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCP CONTENTS 2005

## まず、コア資産のバグを抽出します

重大なバグ

軽微なバグ

テスト環境

コア資産

いくつかのバグは残るかもしれません

Validation Verification

QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCP CONTENTS 2005

## 残りのシステムをドメインに分割します

ユーザー インターフェース

コア資産

ドメイン

Validation Verification

QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCP CONTENTS 2005

## ドメインごとにバグを抽出し、不具合を抑制します

- ドメインによって効率的な不具合の抽出手段が異なります
- 例えばユーザーインターフェースには機能テストが有効です

ユーザー インターフェース

コア資産

不具合の抑制

重大なバグ リスク分析

バリデーションの実施

不具合を完全に抽出できなくても、バリデーションによりシステムの重大なリスクを抑制することができます

Validation Verification


QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## 電子ポットのリスク分析・妥当性確認 例示

- R & Dセンターの省電力研究室から、電子ポットの温度テーブルを最適化することで、ポットの消費電力を10%削減できるという調査報告が回ってきました
- この調査報告を受けて、ポットの消費電力を削減すべく設計変更を行いました

		EO: ( )				
		<-3	-3	=0	3	>3
TO ( )	<-3	0	100	100	100	100
	-3	0	70	70	70	100
	=0	0	30	30	50	100
	3	0	0	0	30	100
	>3	0	0	0	0	100



EO: 目標の水温 - 現在の水温  
TO: 前回の制御周期時の水温 - 今回の制御周期時の水温

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## ポットから煙がでた！ 例示

- ユーザー先で使用中の電子ポットで煙がでたという報告がありました
- ポットを分解したところヒータの異常加熱により、周りの部品が焼けこげていました
- 品質保証部門の解析チームがプログラムを解析したところ、**省電力のために変更した温度テーブルの組み込みでミスがあり、テーブルのヒータ制御量の中に誤って負の値が定義された部分がありました**
- 負の値がヒータ制御のソフトウェアに渡るとヒータを最大出力で熱してしまうプログラムになっていたことが判明しました
  - エラー監視のプログラムでヒータ連続オンの時間の上限を監視していませんでした

		EO: ( )				
		<-3	-3	=0	3	>3
TO ( )	<-3	-1	100	100	100	100
	-3	0	70	70	70	100

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## リスク分析表を使った信頼性の向上 例示

- フィールドで起こった不具合の対策をコア資産に追加し、より強固なものにします

番号	障害	原因	重要度	発生の可能性/故障率	対策	実施確認の方法	チェック
No.	Hazard	Cause	Level of Concern	Likelihood/Failure Rate	Method of Control	Trace	Check
A-1	ヒータの異常加熱により火災が起こる	サーモスタットの故障 ヒータの故障	High	1/10000 (故障率)	・ <b>ハードウェアによる対策</b> 温度ヒューズによるヒータへの回路切断 ・ <b>ソフトウェアによる対策</b> プグーによる温度検知とエラー検出(30秒)を行う。	設計書番号 #001 テスト計画 #001	
	水の量が少ないうちに加熱した		High	たまにあり (Moderate)	・ <b>ソフトウェアによる対策</b> 残り水の検出センサーの状態ならば、ヒータや沸騰ボタンは動作しない。	設計書番号 #002 テスト計画 #002	
	ヒータ制御ソフトウェアの完全対策不備		High	まれ (Low)	・ <b>ソフトウェアによる対策</b> ヒータ制御期間のマイクス値は受け付けられない連続ヒータONの時間上限を設ける。	設計書番号 #003 テスト計画 #003	

出典: Guidance for FDA Reviewers - Premarket Notification Submissions for Automated Testing Instruments Used in Blood Establishments

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## システムの信頼性を高めることができました

- 不具合がゼロになることはまれです
- しかし、**重大な欠陥は検出または抑制され、コア資産の信頼性はアップしています**



Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## 高信頼性ソフトウェア実現の心得

- 限られた予算、限られた期間内で不具合をゼロにすることは不可能に近いと考えましょう
- リコールに至るような重大な不具合を取り除くまたは抑制することが先決です
- 製品のソフトウェアをドメイン分割し、コア資産を分離した後、コア資産の信頼性を高めることが効果的です
- 作成したソフトウェアがユーザーニーズを満たしているかどうかを確認すること (Validation: 妥当性確認) とリスク分析の結果と対策を蓄積し、対策をもれなく実施することが重要です

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## Agenda

- 高信頼性ソフトウェアのイメージをつかむ
- 信頼性向上のActivityをマッピングする
- 組織成熟度と注力すべきActivityの関係を知る

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## ソフトウェアの信頼性を高めるには？

- ソフトウェアの不具合を作り込む原因は後にも先にも人間です
- 高信頼性ソフトウェアを目指すには過ちを犯しやすい人間の活動をコントロールする必要があります
- ソフトウェアの品質向上を目的としたActivityを“過ちを犯しやすい人間の活動をコントロールするという視点”で分類すると右のようになります

人間の過ちを軽減する Activity (取り組み)	人間の介在を少なくする Activity (取り組み)
プロセスの定義	MDD(モデル駆動開発)
リスク分析	ソフトウェア資産の再利用
コーディングルールの定数	覆れたアーキテクチャフレームワークの採用
静的コードテスト	
メトリクス分析による指導	
テスト・レビュー・インスペクション	
ソフトウェア資産の再利用	
不具合・仕様変更データベースの整備	
UMLによるシステム構造の視覚化	
不具合発生・対策履歴の分析	

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005 参照: 保田隆浩著「ソフトウェア品質保証の考え方と実践」, P.86 図1.10 「不信頼性のための方針」

## 信頼性向上の Activity Map

不具合を作り込まない努力

プロセスで抑える

不具合を抽出する努力

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## Software Subsystem の結合

- システムはサブシステムの集合体です
- 個々のサブシステムの信頼性が高ければ、システムに信頼を込め込むのと同じです
- システム全体の信頼性を高めるには、個々のサブシステムのVerification(検証)とユーザー要求に基づいたValidation(妥当性確認)を行うことが重要です
- サブシステムが高信頼・疎結合の関係になっている必要があります

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## COTSに爆弾が含まれていたら？

COTS: Commercial Off-The-Shelf (商用で即利用可能なソフトウェア部品)

- 製品に使うために購入した“商用で即利用可能なソフトウェア部品”=COTSには、爆弾が含まれていないとは限りません
- ブラックボックスのCOTSに含まれる爆弾は、Software Validation や Design Validation によって取り除きます
- 具体的にはCOTSに対してブラックボックスで機能テストをしたり、サブシステム同士の結合テストや製品の機能テストによって爆弾を見つけます
- 見つけた爆弾はCOTSの供給者に取り除いてもらうしかありません
- 社内で過去に作成した中身の分からないサブシステムでも同じです
- 検証が十分に行われ市場で長い時間使用されたサブシステムは再利用できます

Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## Software Product Line と Engineer

- 製品群におけるコア資産は製品群の価値が凝縮された重要なサブシステムです
- コア資産の信頼性を高めることが製品群全体の信頼性を向上させることにつながります
- 不具合を作り込むのは人間です
- エンジニアの教育は不具合の元を断つことに直結しています

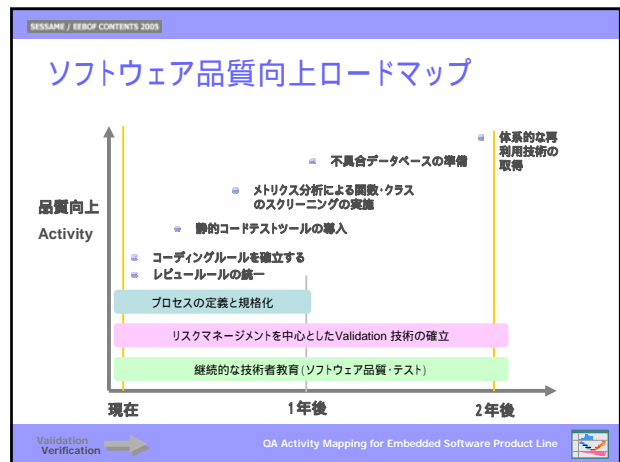
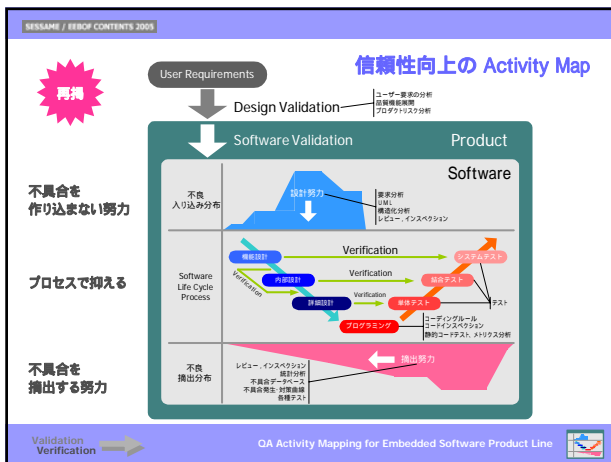
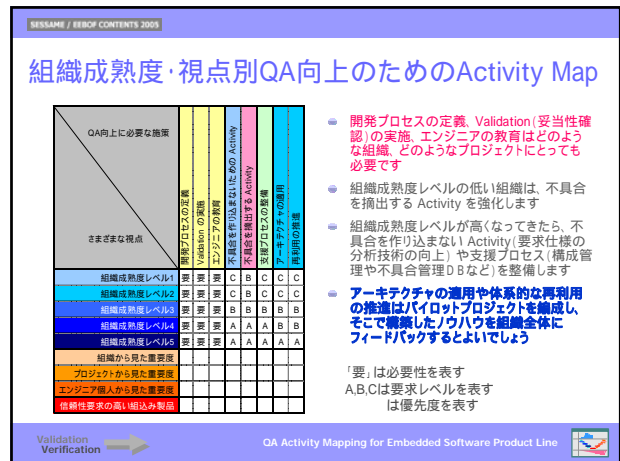
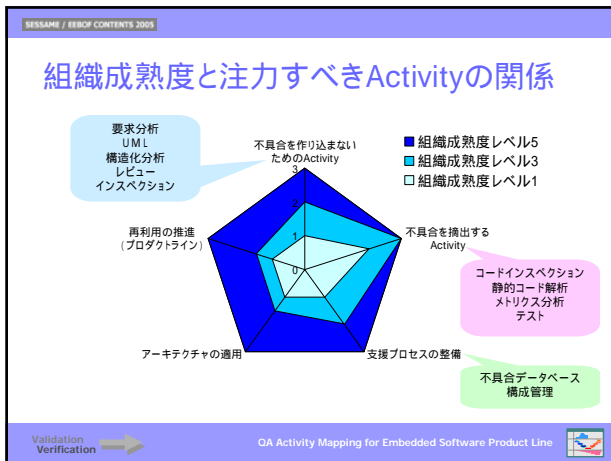
Validation Verification → QA Activity Mapping for Embedded Software Product Line

SESSAME / EBCF CONTENTS 2005

## Agenda

- 高信頼性ソフトウェアのイメージをつかむ
- 信頼性向上のActivityをマッピングする
- 組織成熟度と注力すべきActivityの関係を知る

Validation Verification → QA Activity Mapping for Embedded Software Product Line



### まとめ

- 高信頼性ソフトウェアの実現は、不具合を作り込む人間の活動をコントロールすることに尽きます
- 高信頼性ソフトウェア製品のイメージを掴むことが重要です
- 製品開発の工程を意識し、設計時に不具合の入り込みを少なくする Activity と作成した成果物に入り込んだ不具合を抽出する Activity について理解します
- 組込み製品群において、市場で長い間利用されたソフトウェアサブシステムの再利用が高信頼性ソフトウェアの実現に最も効果があります
- 製品に使うために購入した「商用で即利用可能なソフトウェア部品」=COTS は使用者が検証(Verification), 妥当性確認(Validation) を実施し信頼性を確認します
- 信頼性を検証したコア資産を再利用することで、潜在的価値を向上させることができます
- 組織成熟度や、組織、プロジェクト、技術者個人といったスコープの違いを考え、取り組むべき組込みソフトウェア品質向上のためのActivity が何かを分析し、そこに注力を注ぐことが高信頼性ソフトウェアを実現するために最も効果的です

Validation Verification → QA Activity Mapping for Embedded Software Product Line

### 参考文献

- General Principles of Software Validation; Final Guidance for Industry and FDA Staff 3.1.2 Verification and Validation, <http://www.fda.gov/cdrh/comp/guidance/938.html>
- 保田勝通, ソフトウェア品質保証の考え方と実際, 日科技連, 1995年
- 松本吉弘, ソフトウェアエンジニアリング基礎知識体系-SWEBOOK-, オーム社, 2003年
- 酒井由夫, 「組込み商品群におけるソフトウェアの妥当性確認」, JaSST 04: Japan Symposium on Software Testing 2004, Tokyo, Japan, Jan, 2004
- 安富大輔, 川井奈央, 今剛, 渡辺晴美, 佐藤啓太, 「組込みソフトウェア開発技術体系化に基づく技術導入」, 組込みソフトウェアカンファレンス2003, Tokyo, Japan, Nov, 2003

Validation Verification → QA Activity Mapping for Embedded Software Product Line

## 本ドキュメントのご利用に際して

- 本著作物の著作権は作成者または作成者の所属する組織が所有し、著作権法によって保護されています
- SESSAMEは本著作物に関して著作権者から著作物の利用を許諾されています
- 本著作物はSESSAMEが使用許諾を与えた利用者個人に対して使用を認めたものです
- SESSAMEから使用許諾を与えられた利用者個人以外の方で本著作物を使用したい場合は [query@sessame.jp](mailto:query@sessame.jp) までお問い合わせください

SESSAMEが著作権者から許諾されている権利

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・上映及び頒布・貸与・翻訳・翻案・二次的著作物の利用

- ドキュメント中には、Microsoft社、Adobe社等が著作権を所有しているクリップアートが含まれています

