オープンシステム
ディペンダビリティ国際規格

2011年11月18日

DEOS プロジェクト / 標準化サブコアチーム

産業技術総合研究所
高井利憲

内容

1. 様々な分野の規格に見る
   Open Systems Dependability
   – Safety
   – Security
   – IT Service
2. それら規格の課題と
   Dependability 関連規格の現状
3. DEOSプロジェクトが目指す
   Open Systems Dependability 規格
4. スケジュール

Functional safety（機能安全）

- Safety critical system においても、ソフトウェアの役割が大きくなってきた
- しかし、ソフトウェアを含むシステムは、従来通りの絶対安全は求められなくなっていた

- 1998年：IEC61508 Functional safety of electrical/electronic/programmable electronic safety-related systems 発行

Safety

Safety Integrity level (SIL)

- discrete level, corresponding to a range of safety integrity values

ソフトウェアを含むシステムでは、従来型の絶対安全を求めることができなくなり、コストに相応の安全性を合意し、達成するために導入された概念

Safety

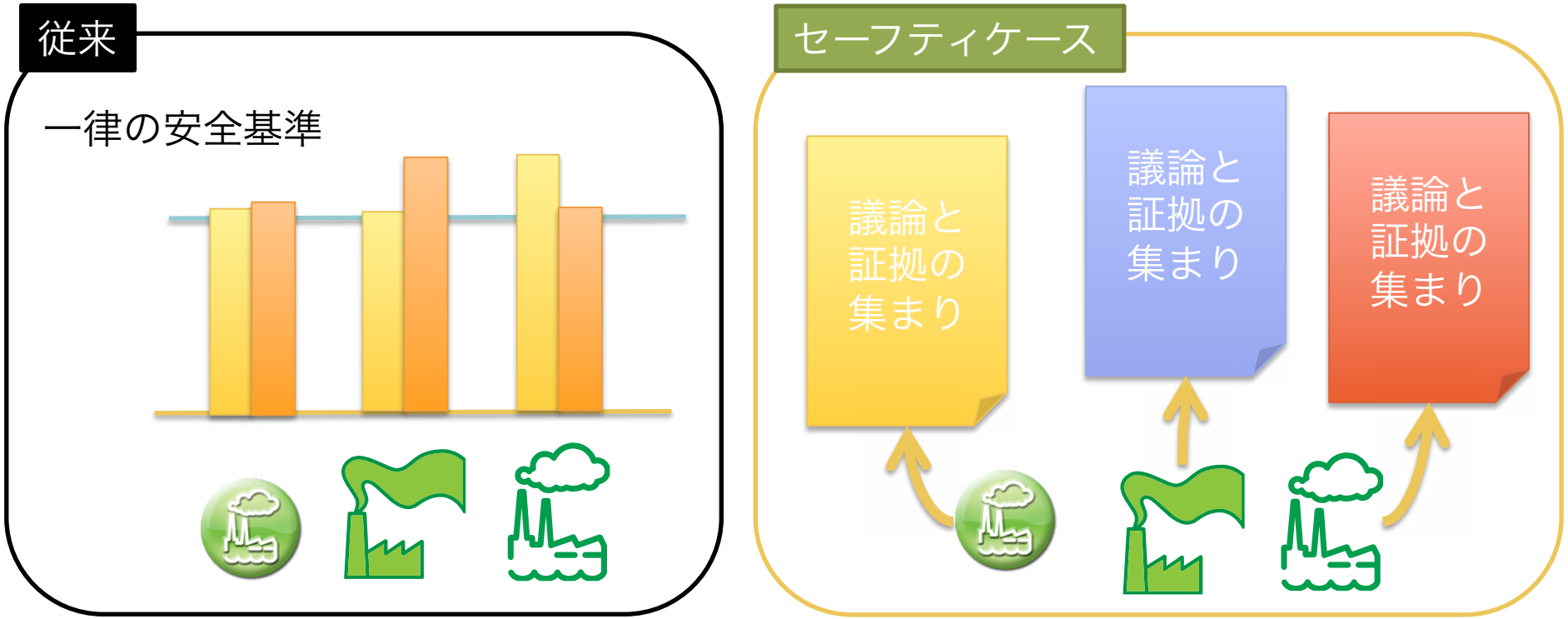
Safety case: background

安全性が求められる分野では、厳しい
定量的な基準が決められていた

しかし重大事故が絶えなかった

	軍事	鉄道	石油化学プラント	原子力
きっかけとなった事故	• 英国にて1980年～1989年にかけて、27機のHawk 損失、23機のTornado 損失、24機のSea King ヘリコプター損失	• 1987年ロンドン地下鉄Kings Cross 駅火災事故	• Piper Alpha 石油生産プラットフォーム爆発火災	• 1957年ウィンズケール火災事故 • 1986年チェルノブイリ事故 （2011年福島事故）
その対応	英国国防規格: Requirements for safety related software in defense equipment (00-55) や Safety management requirements for defense systems(00-56) にて safety case を要求	The Railways (Safety Case) Regulations 1994	The Offshore Installations (Safety Case) Regulations 1992	1998年第一回原子力の安全に関する条約国別レビューにて、ほとんどの国でsafety case を運用しているとの報告

Safety case



- 一律の安全基準をどんなに厳しくしても絶対的な基準は得られなかった
  - e.g. 福島原発を念頭に置いた場合の津波の基準は？
- 個別にリスクアセスメントを行い、個別の事情について証拠に基づきながら議論し、記述しておくことが各分野で求められた
  - e.g. ISO26262 Road vehicles - Functional safety

Safety

Safety culture / Safety lifecycle

- 1986年４月に、旧ソ連チェルノブイリ原子力発電所事故が発生
  - IAEAはこの事故の原因と対応について、「いわゆる人的要因にあり、Safety cultureの欠如にあった」と報告

安全にはゴールはなく、全ての階層の
従業員が、安全について常に問いかける
姿勢を持たなければならない

  - 具体的には、Safety management system など
    プロセスによる対応
  - e.g. Safety lifecycle in IEC61508, ISO26262

Safety

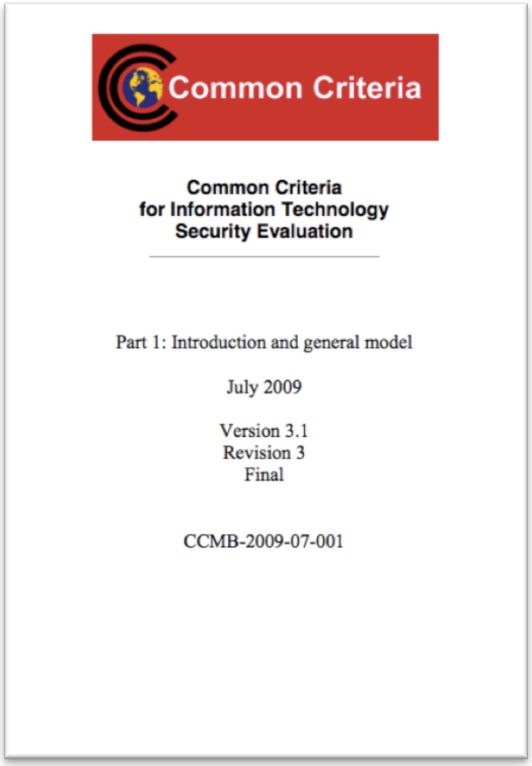
Safety 分野まとめ

- 背景
  - ソフトウェアにって実現された安全機能に対しては、従来型の安全性が適応できない
  - 定量的な基準によっては致命的な事故は防ぐことはできない
- 対応
  - Safety integrity level → コストに応じた対応
  - Safety case → 定性的な安全性評価
  - Safety culture / lifecycle → プロセスによる対応

Safety

Common Criteria

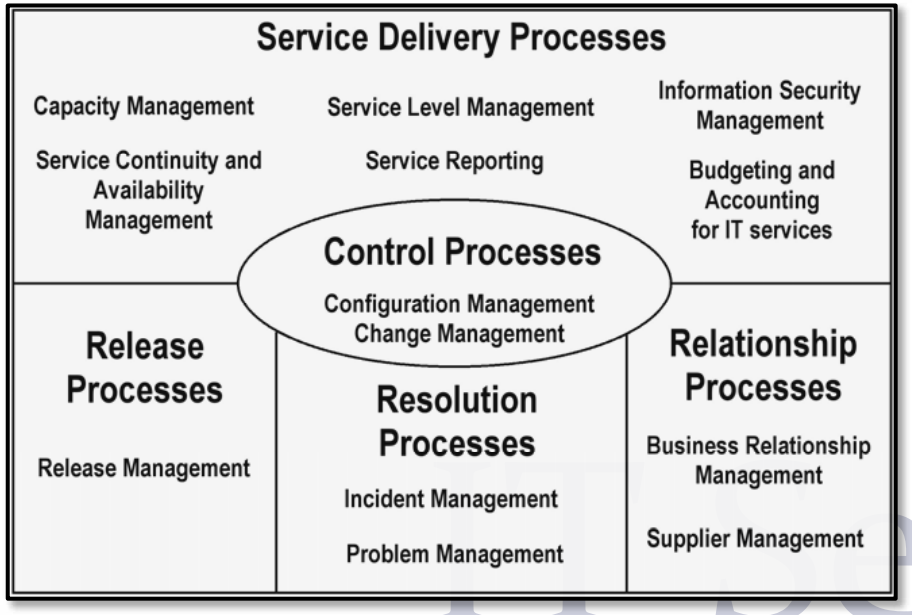
- ISO/IEC15408 Evaluation criteria for IT security
  - 具体的なセキュリティ要件を定義するのではなく製品ごとにセキュリティ要件を定義しその達成を示すための枠組みを提供
  - Evaluation Assurance Levels (EAL)
  - Security Target



Security

Service level agreement (SLA)

Web サービスなどの受発注時、サービスの
機能に関する仕様だけでなく、
障害発生の頻度や障害発生時の対応など、
障害発生を前提とした合意形成を！



OSD視点からの既存規格のまとめ

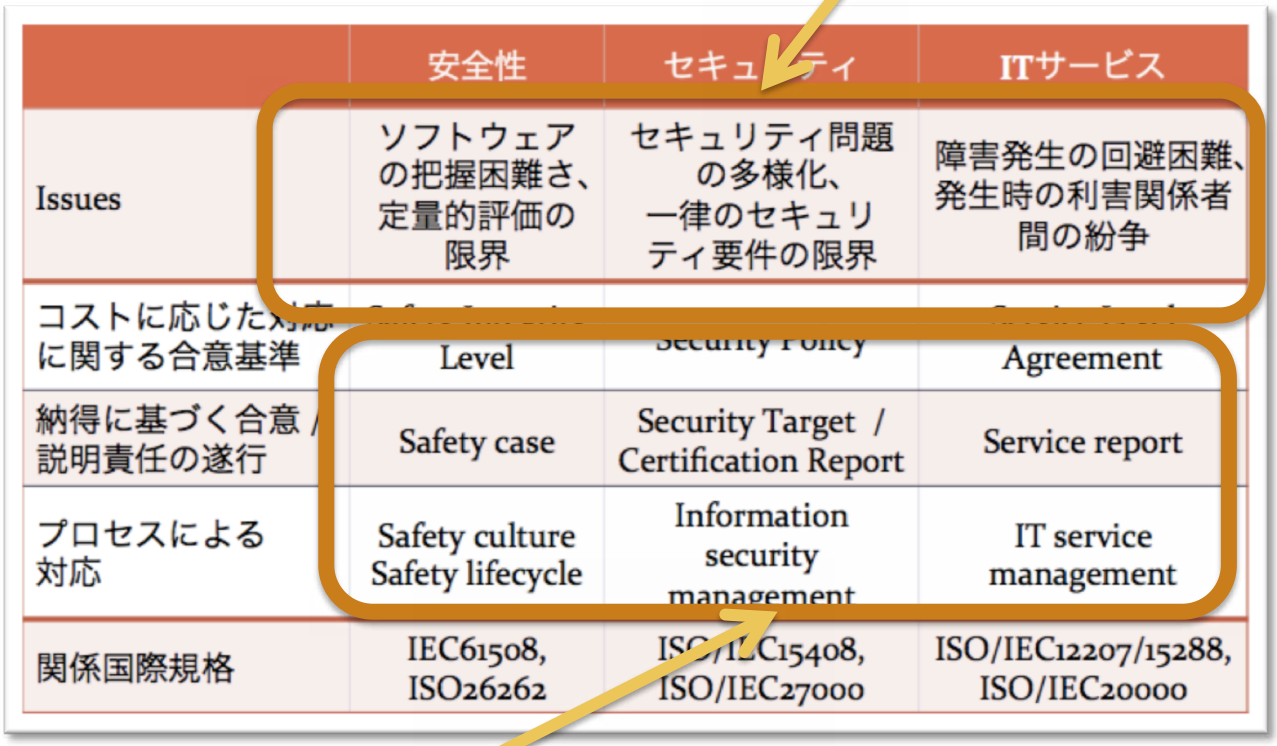
- Issues
  - 変化の予測不可能性
  - 全体像の把握困難性
    - 利害関係者間の認識の齟齬
- 対処手段
  - コストに応じた品質特性やリスク抑制のレベル
  - 納得に基づく合意形成
  - 説明責任の遂行による責任履行
  - プロセスによる対処

既存規格のOSD的観点まとめ表

	安全性	セキュリティ	ITサービス
Issues	ソフトウェアの把握困難さ、定量的評価の限界	セキュリティ問題の多様化、一律のセキュリティ要件の限界	障害発生の回避困難、発生時の利害関係者間の紛争
コストに応じた対応に関する合意基準	Safety Integrity Level (SIL)	Evaluation Assurance Level (EAL)	Service Level Agreement(SLA)
納得に基づく合意 / 説明責任の遂行	Safety case	Security Case/ Security Target / Certification Report	Service report
プロセスによる対応	Safety culture Safety lifecycle	Information security management	IT service management
関係国際規格	IEC61508, ISO26262	ISO/IEC15408, ISO/IEC27000	ISO/IEC12207/15288, ISO/IEC20000

既存国際規格の課題

(1) Issue への分野にまたがる共通認識がない

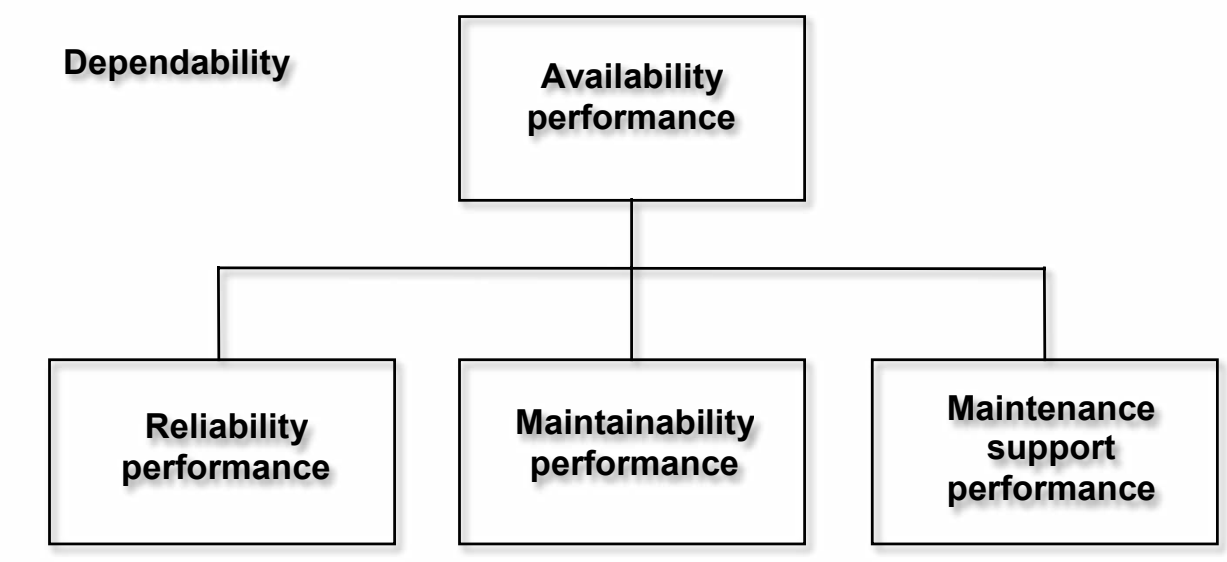


	安全性	セキュリティ	ITサービス
Issues	ソフトウェアの把握困難さ、定量的評価の限界	セキュリティ問題の多様化、一律のセキュリティ要件の限界	障害発生の回避困難、発生時の利害関係者間の紛争
コストに応じた対応に関する合意基準	Level	Security Policy	Agreement
納得に基づく合意 / 説明責任の遂行	Safety case	Security Target / Certification Report	Service report
プロセスによる対応	Safety culture Safety lifecycle	Information security management	IT service management
関係国際規格	IEC61508, ISO26262	ISO/IEC15408, ISO/IEC27000	ISO/IEC12207/15288, ISO/IEC20000

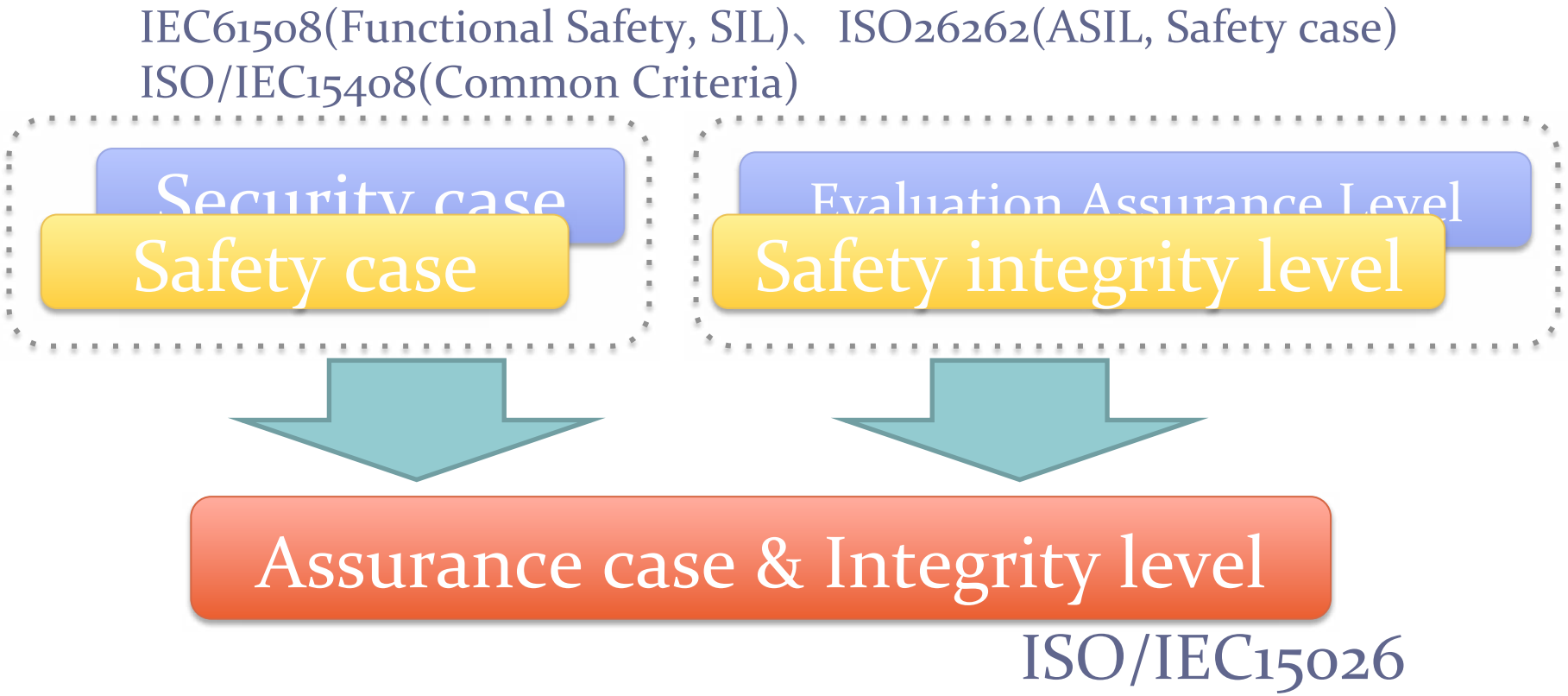
(2) 類似の対策がとられているにもかかわらず共通認識がなく、対応関係も不明

(1) Issue の共通認識

- ディペンダビリティ規格の現状
  - IEC 60300: Dependability management
    - 前述 Issues に対する統一的な視点を dependability から与えてほしい
    - しかし、そうはなっていない！

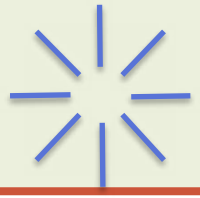


(2) 対策の共通認識



- ISO/IEC15026
  - 1998年版は、Safety integrity level の一般化である Integrity level に関する規格
  - 現在、Part 1 ～ Part 4 に拡張し改訂中
    - DEOS プロジェクトから2名が Editor として参加

DEOSプロジェクトが目指すOSD規格

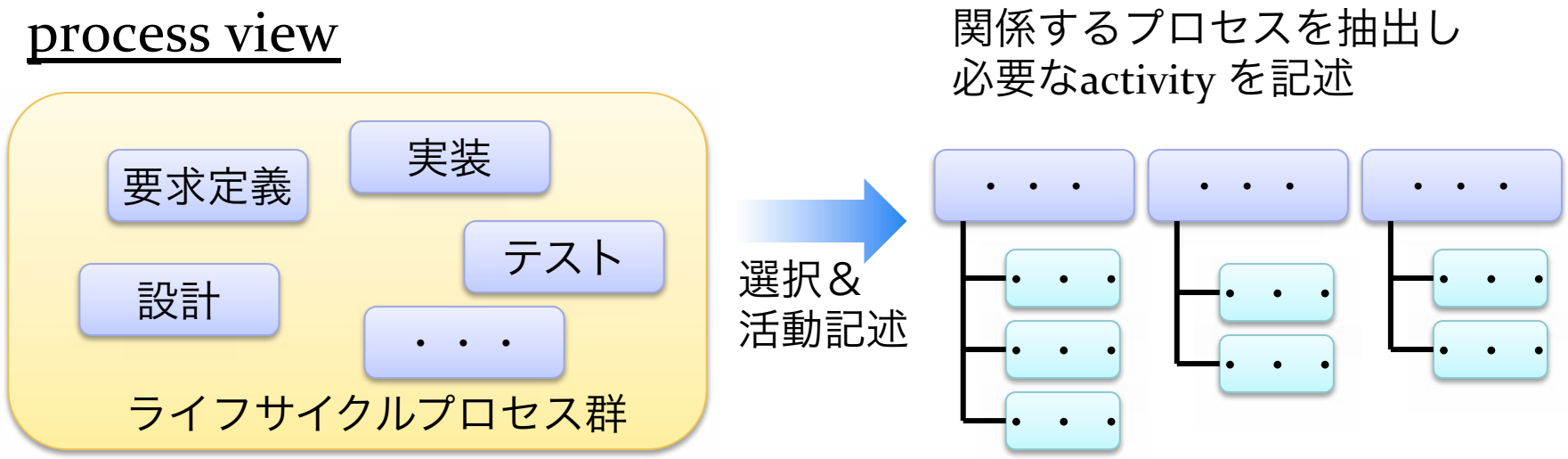
	安全性	セキュリティ	ITサービス	Towards OSD
Issues	ソフトウェアの把握困難さ、定量的評価の限界	セキュリティ問題の多様化、一律のセキュリティ要件の限界	障害発生の回避困難、発生時の利害関係者間の紛争	
コストに応じた対応に関する合意基準	Safety Integrity Level	Evaluation Assurance Level (EAL)	Service Level Agreement	Integrity level
納得に基づく合意 / 説明責任の遂行	Safety case	Security Case/ Security Target / Certification Report	Service report	Assurance case
プロセスによる対応	Safety culture Safety lifecycle	Information security management	IT service management	
関係国際規格	IEC61508, ISO26262	ISO/IEC15408, ISO/IEC27000	ISO/IEC12207/15288, ISO/IEC20000	ISO/IEC15026-1～4, IEC TC56 NWIP, DEOS Process の国際規格版

Processについて:
ISO/IEC15026Part 4

改訂中 ISO/IEC15026-4において Assurance case を含む System/Software lifecycle process のガイドラインを策定中

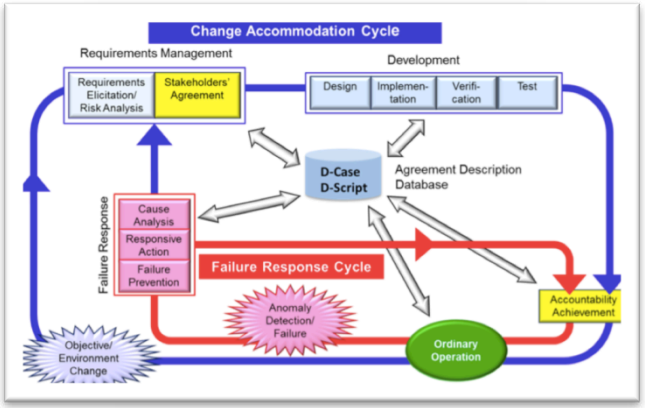
– ただし、具体的なプロセスモデルは含まず

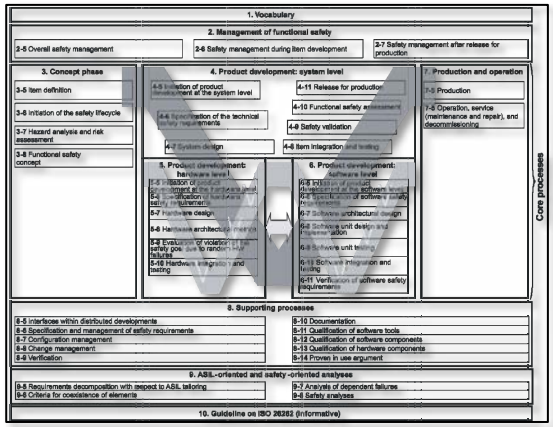
process view



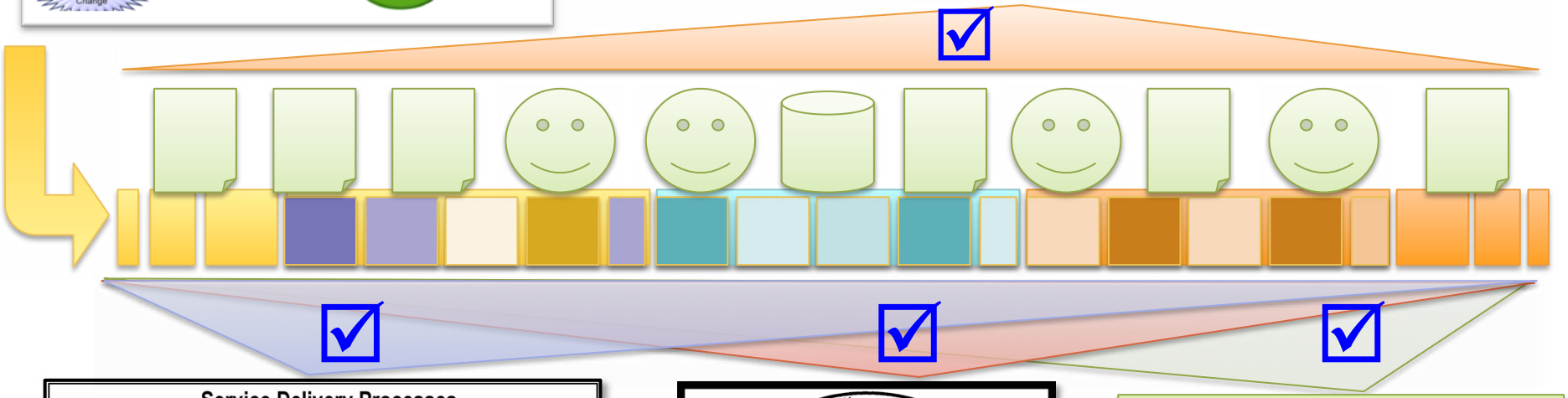
プロセスについての概念を共有できれば・・・

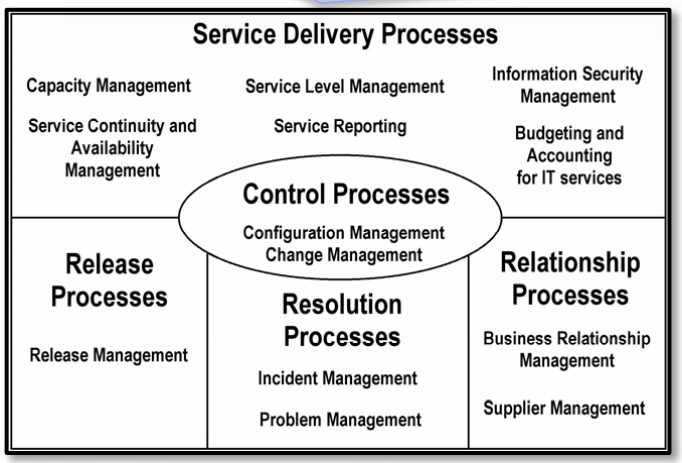
DEOS Process



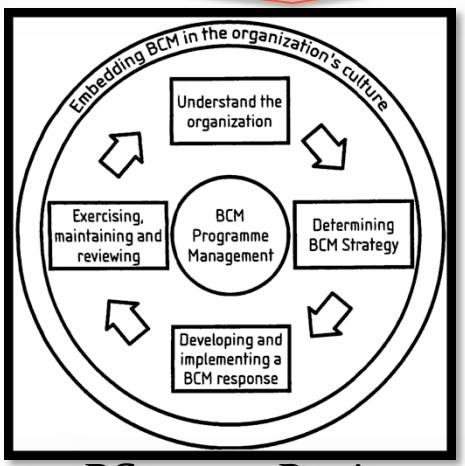


ISO26262
Road vehicles
— Functional safety





ISO/IEC20000 *IT Service management*



BS25999 *Business Continuity management*

Others
- Security management
- Quality management
- System assurance
- TOGAF

- etc...

オープンシステムディペンダビリティ国際規格に向けて

- Assurance case および Integrity level への一般化は、従来型枠組みの範囲内

- 運用時の新たなリスクの判明、事故発生時の緊急対応、利害関係者の変化などに対応した dynamic な
  - Assurance case & Integrity leve → D-Case
  - lifecycle process → DEOS Process

に対応した新しい国際標準規格の提案へ

Open Systems Dependability認証規格

IEC 60300を策定している IEC TC56にて
New work-item proposal を提案準備中

Assessment of dependable open system life cycle

- Target: dependable open system life cycles
  - Stakeholders' agreement formation
  - Accountability achievement process
  - Service continuity
- Validation: development of assurance cases
  - Document of validation of open system requirements (assurance case)
- Assessment: evaluation of 1. using the result of 2.
  - The quality of validation process (2.) should also be assessed by evaluating the assurance case

NWIP: Assessment of dependable open system life cycleのねらい

Open system 概念の明確化

- Indeterminacy in elements and purpose
- Specification changes over time and stakeholder

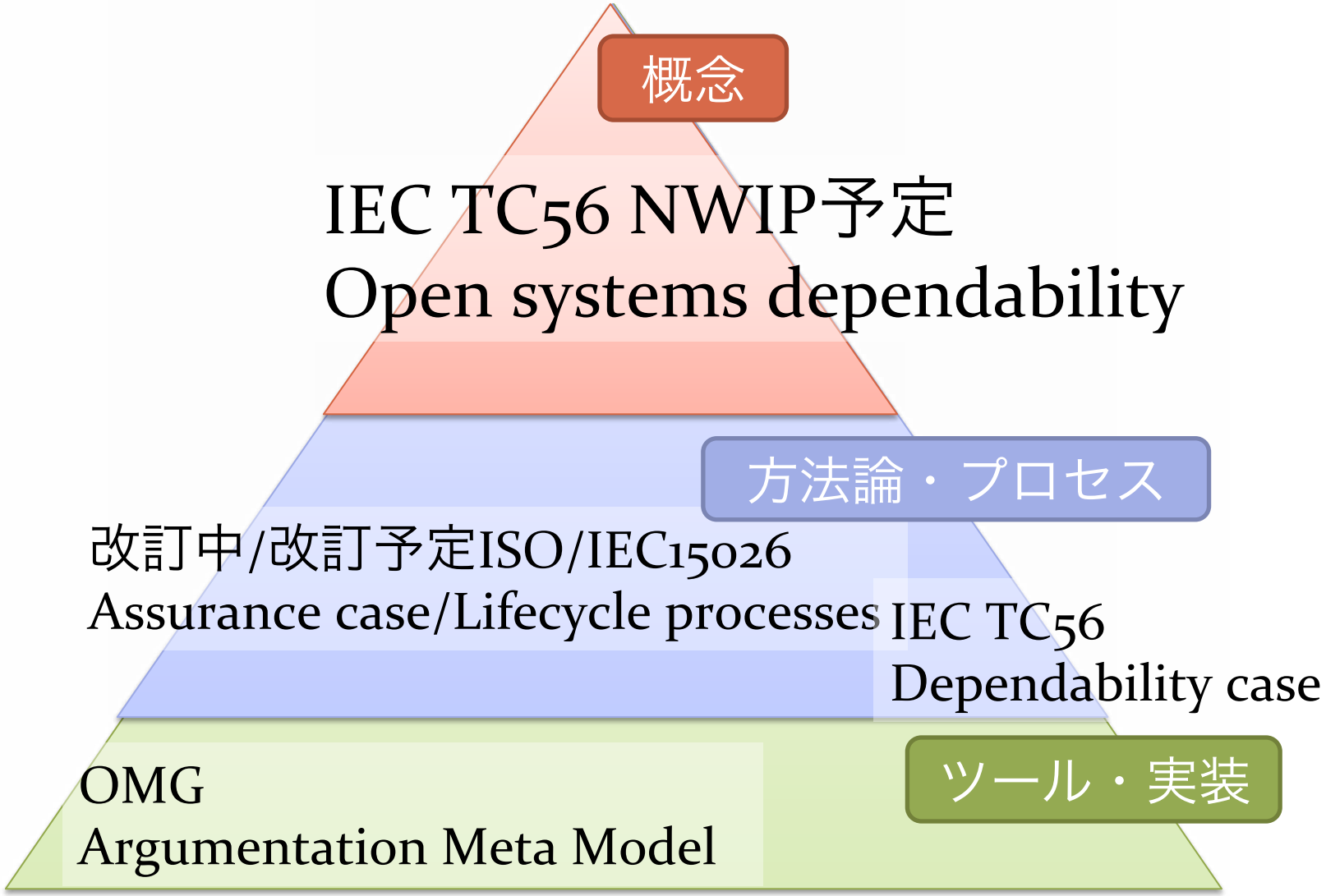
Dependable open system lifecycle 実現手段の明確化

- Stakeholders' agreement formation
- Achievement of accountability
- Process for service continuity
  - Change accommodation cycle
  - Failure response cycle

スケジュール

- TC56 NWIP提案準備中
  - 今月国際会議にて提案内容案紹介
- ISO/IEC 15026 System and software assurance
  - Part 1: Concepts (TR) 発行済
  - Part 2: Assurance case 発行済
  - Part 3: System Integrity levels FCD通過
    → FDIS投票へ（今月）
  - Part 4: Assurance in life cycle WD4通過
    → CD投票（今月）
- OMG
  - Assurance case の標準化へD-Caseの技術要素の反映を目指している

標準化戦略


概念
IEC TC56 NWIP予定
Open systems dependability
方法論・プロセス
改訂中/改訂予定ISO/IEC15026
Assurance case/Lifecycle processes
IEC TC56
Dependability case
ツール・実装
OMG
Argumentation Meta Model

OSD的視点による標準化のメリット

- 複数の分野の国際標準規格が対処しようとしている問題群に対する共通の視点の提供
- （将来）様々な分野の規格に対応すべき製品の戦略的な認証手段の可能性
- （将来）Assurance case（具体的にはD-Case）のネットワークによる Open Systems Dependability 向上へ貢献