ET2016
JASA技術本部セミナー

安全誘導型設計の特徴と試行
--意図を記述すれば、安全性が高まる--

2016年11月16日

中村　洋
株式会社レンタコーチ
JASA　安全仕様化WG

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

はじめに

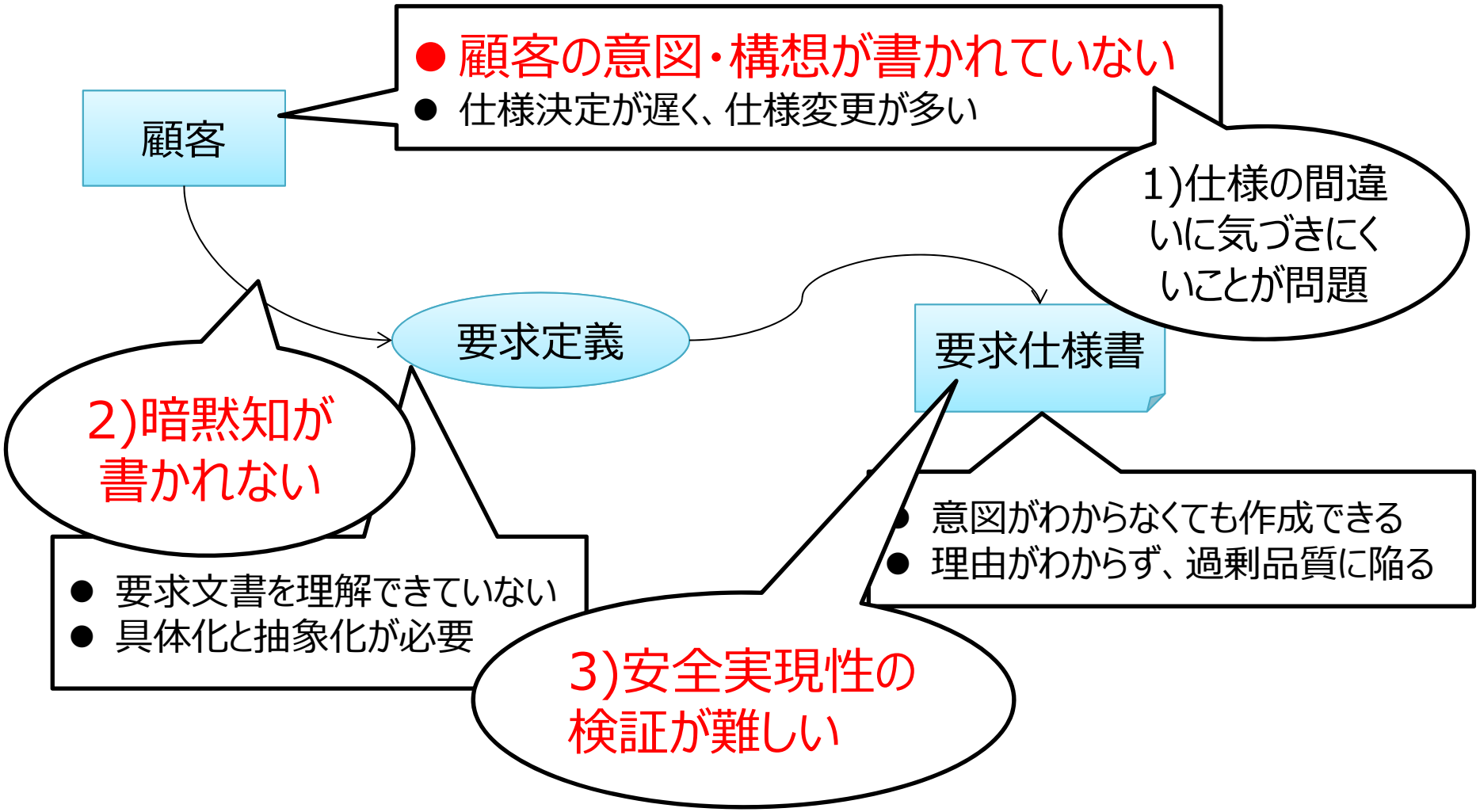
◆背景

- 2012年度から3年間：意図したものが実現できる要求定義
- 2015年度から：安全が関わる要求を仕様化するプロセス
- 2016年度には、「安全誘導型設計」と名付けたプロセスモデル

◆概要

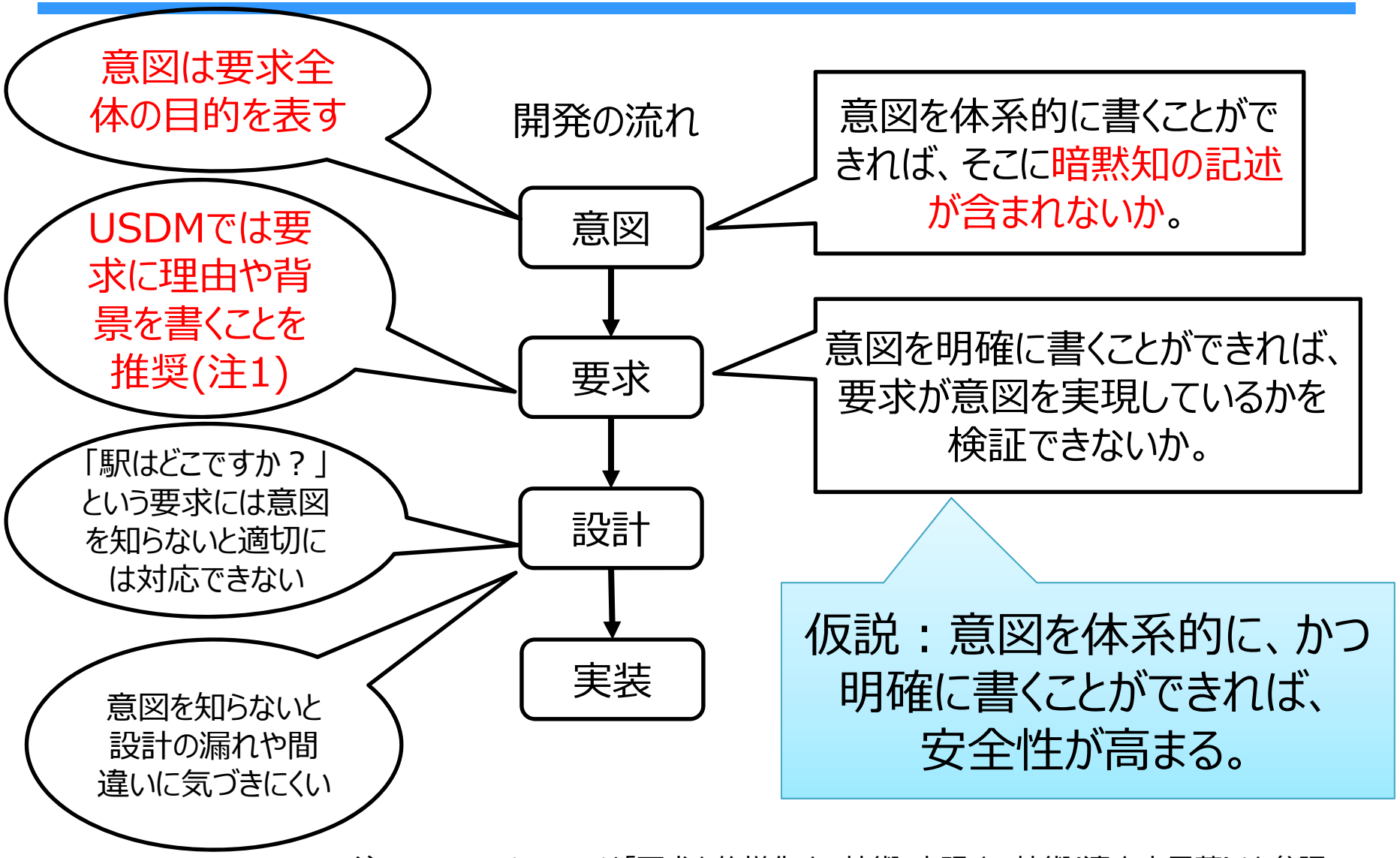
- 安全が関わる要求の仕様化の現状と課題を考慮すると、要求定義に先立つ意図の記述が、要求段階における安全実現性の検証が、ともに求められている。
- 安全誘導型設計は、「意図を記述すれば、安全性が高まる」仮説に基づくプロセスモデルであり、意図記述とハザード分析を柱とする。特に、意図記述は、標準的な意図体系フレームワーク、適用分野固有のテンプレートを使用することを特徴とする。
- 仮想的な電動アシスト自転車を題材として、安全誘導型設計を試行し、意図を記述すれば、システム記述だけでなくハザード分析も容易にし、「安全性の検証と安全の作り込み」を助けることを確認した。

要求の仕様化に関する現状と課題



備考：「要求の仕様化に関する、課題、プロセス及び手法、2015年3月、JASA」に加筆。

意図の役割と期待効果



注1：USDMについては「要求を仕様化する技術・表現する技術(清水吉男著)」を参照。

安全誘導型設計の狙い

◆適用分野

- ■ 組込み製品を対象とするシステム開発
- ■ 一般的に、安全が関わるシステム開発

◆適用プロセス

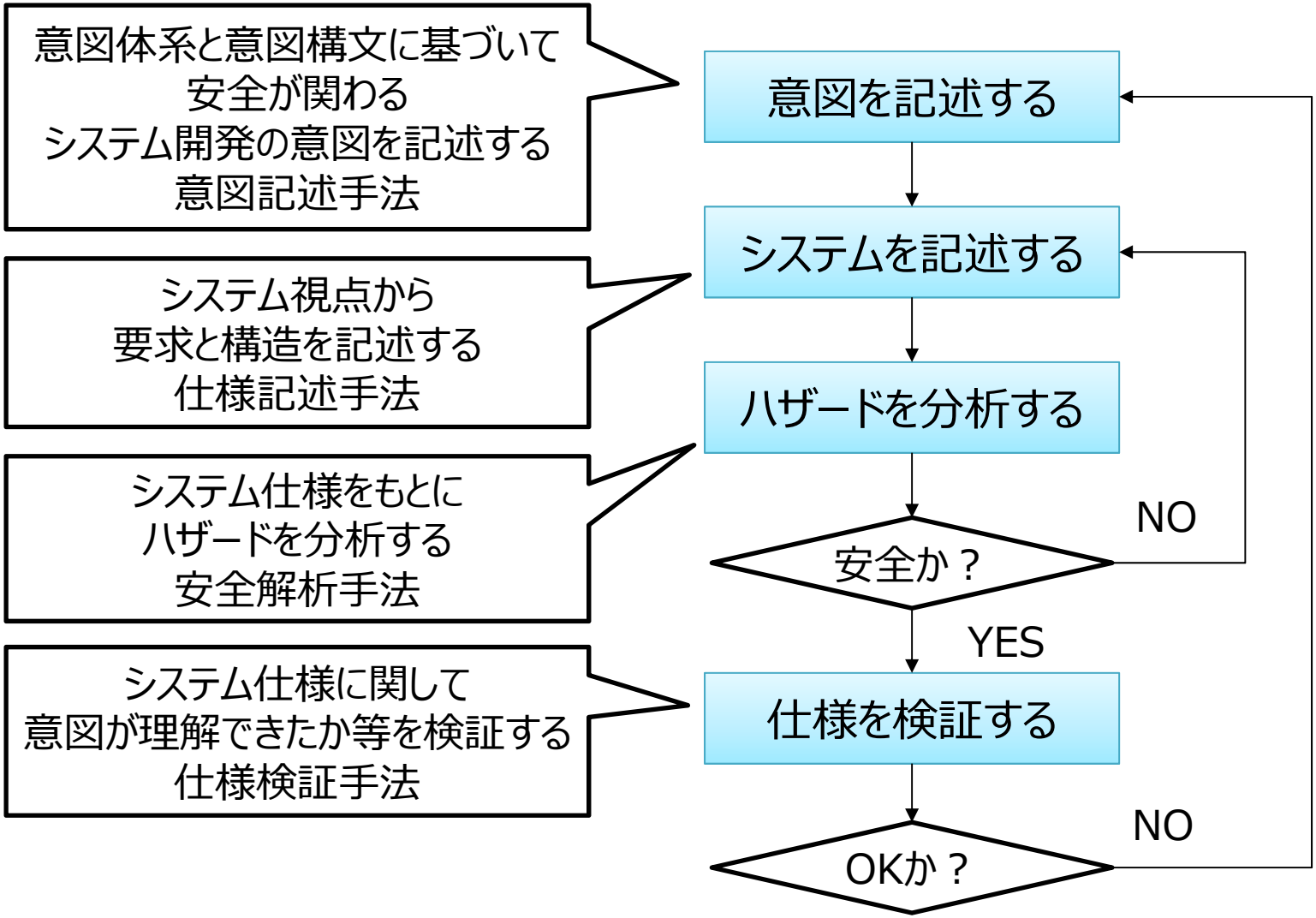
- ■ システム開発においてコンポーネント設計に先立ち、システム全体の要求を分析し、構造を設計するプロセス

◆利点

- ■ 要求分析段階において、安全性の検証と安全の作り込みを支援する。
- ■ 要求仕様が意図したことを実現しているかという、意図実現性の検証を支援する。

命名時の思い：
- ➢ 意図に照らして、安全か非安全かを判断し、
- ➢ 安全が実現する方向に進めば、適切に要求と構造を設計できる

安全誘導型設計のプロセスモデル



意図体系フレームワーク

第1階層	第2階層	視点
開発計画		開発をマネジメントするための視点
	納期	
	コスト	
	品質を検査する手段	
	安全を検査する手段	
開発目的		開発者と顧客が合意するための視点
	達成目的	
	システムに対する要求と制約	
	使用者に対する要求と制約	
	使用環境に関する仮定事項	
	事故に関する情報	
	ハザードに関する情報	
	システムの限界	

第1階層が記述すべき視点、
第2階層が記述事項を示す。

記述事項をさらに
細目に分けて、個
別の意図を記述。

第1階層	第2階層	視点
システム機能		システム開発者の視点
	製品に関する物理原則	
	システムレベルの設計原則	
システム構造		コンポーネント開発者へ伝達するための視点
	安全関連系	
	新規と流用の区分	
システム運用		運用へ伝達するための視点
	推奨する使用法	
	誤使用	

試行の概要

◆対象システム開発
- ■ 仮想的な電動アシスト自転車

◆対象機能
- ■ 電動アシスト機能に限定

◆安全誘導型設計の適用範囲
- ■ 意図記述
  - ●意図体系テンプレートを作成
  - ●意図項目ごとに意図を記述
- ■ システム記述
  - ●与えられた要求を記述
- ■ ハザード分析
  - ●STAMP/STPA手法を適用

◆参照資料
- ■ ヤマハ製電動アシスト自転車　PASナチュラL取扱説明書

意図体系テンプレートを用いて意図記述(一部)

第1階層	第2階層	項目	視点	要求する、規定する、又は選択する意図
開発目的			開発者と顧客が合意するための視点	
	達成目標			
		競争優位		トップブランドの地位を維持する。
	システムに対する要求・制約			
		機能の利点		自然で滑らかな乗り心地を実現する。
				坂道でもパワフルで滑らかな乗り心地を実現する。
	使用者に対する要求・制約			
		使用目的		目的外[illegible]に関わる安全にコストをかけない。
	使用環境に関する仮定事項			
		法的制約		利用[illegible]に法的制約を避ける。
	事故に関する情報			
		多発事故		
	ハザードに関する情報			
		急加速		
		重量		

意図は、実現可能性などの要求特性を
満たす必要がない。
それでいて、つい、要求を書いてしまう。
しかし、意図は、要求を縛る。

意図に対応する要求の記述(一部)

第1階層	第2階層	項目	要求・規定事項
開発目的		トップブランドの地位を維持	
	達成目標		
		競争優位	連続アシスト距離を40kmとする。
	システムに対する要求・制約		
		機能の利点	ペダルを踏む力や走行速度、変速位置に応じて、基準の範囲内でアシストできる。
		自然で滑らかな乗り心地	ペダルを踏む力、走行速度、ペダルを回す力を検出できる。
		坂道でもパワフル	変速位置を検出できる。

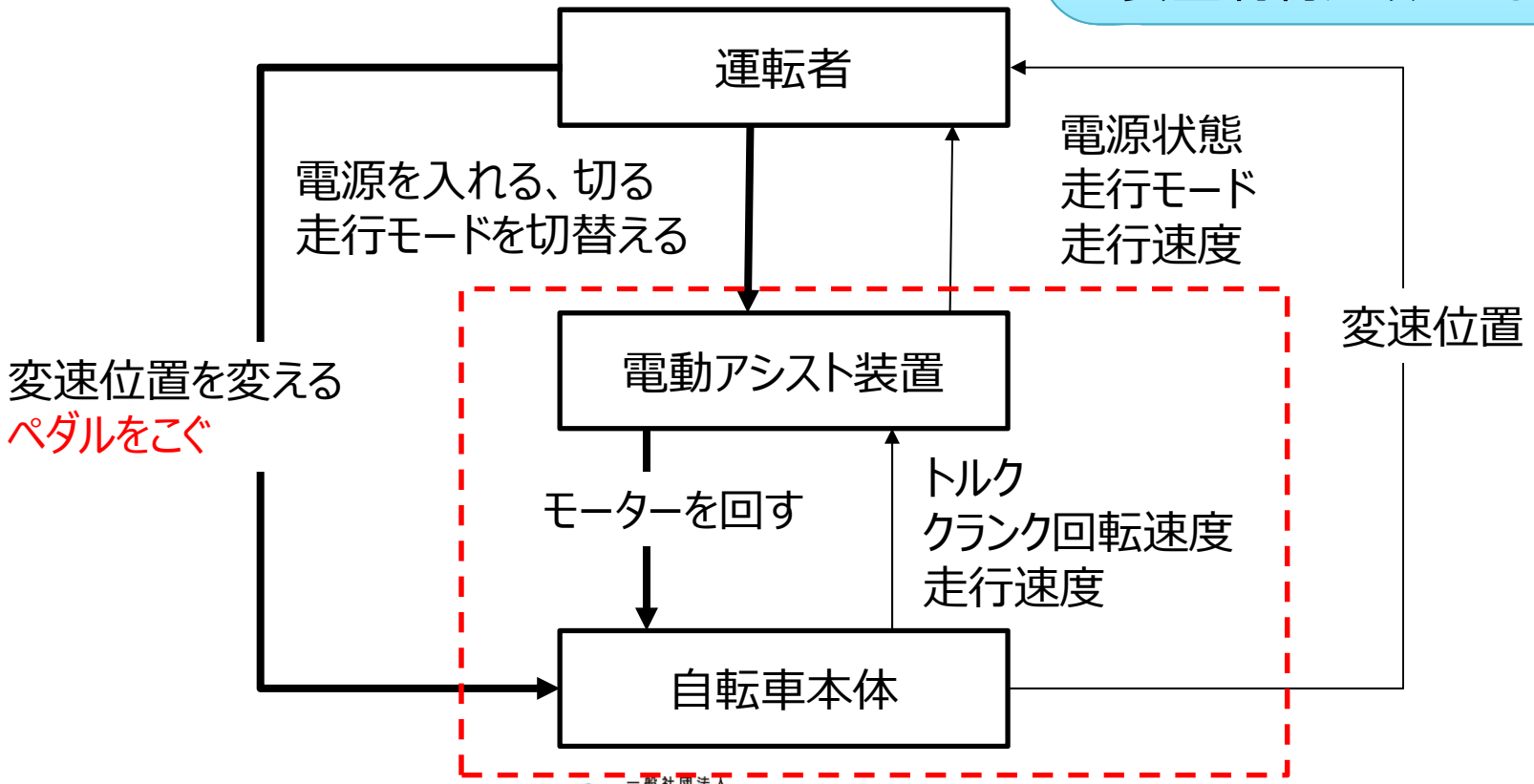
要求は、実現可能性、検証可能性などの要求特性を満たさなければならない。

意図を実現できるという論証も必要になる。
(例：業界最高水準を達成すれば、ブランド地位を維持)

意図しない急加速を防ぐための制御構造

事故：運転中の転倒又は衝突
ハザード：意図しない急加速
安全制約：意図しない急加速を防止する
対象外：バッテリ関係、本来の自転車機能

運転者はハザードを引き起こさないようにペダルを踏むが、電動アシスト装置がそれとは違う動きをすると、安全制約が破られる。



ハザードシナリオと対策

UCA	ハザードシナリオ	対策
UCA-1: 走行速度0km/h モーター無回転で ペダルを強くこぐ	1. 乗り出しのときに、運転者がペダルを強く踏んでしまう。 2. トルクが急に大きくなる。 3. それを検知して、アシスト装置がモーターを急に強く回す。 4. 自転車が急に加速され、ハザードを引き起こす。	対策1： モーターが無回転のときには、トルクが急に大きくなっても、モーターを強く回さない。 対策2： 運転者がモーター回転速度を認識できるようにし、無回転時には強くペダルを踏まないように注意喚起する。
UCA-2: 走行速度10km/h未満 モーター無回転で ペダルを強くこぐ	1. ゆっくりと走っているときに、運転者がアシストが働いていないことを知らずに、ペダルを強く踏んでしまう。 2. これ以降はUCA-1に同じ	

モーターが回転せず、
アシストが働いていない状態

「自然で滑らかな乗り心地を実現する」という意図に照らすと、対策2が適切。

考察

- 要求段階で安全性を検証し、安全を作り込むためには、意図の体系的な記述が役に立ちそうだ。
- 意図を体系的に記述するときには、意図体系テンプレートに沿った記述が便利であり、その元になる標準的なフレームワークの整備が望まれる。
- 意図は、要求とは異なり、要求特性に制約されないが、要求の目的や根拠などの役割を担い、その記述には訓練、演習が必要だ。
- 意図記述とそれを反映するシステム記述を用意し、STAMP/STPA手法を用いてハザード分析を試行してみると、適切な安全制約を導き出すことができた。
- 「意図を記述すれば、安全性が高まる」と主張できるのではないか。

日経テクノロジーオンライン　連載コラム：IoT時代の安全性検証技術
関連解説記事が掲載中

2016年度活動概要

◆目的
- ■ 安全が関わる要求を仕様化するプロセスの研究
- ■ その仕様化を支援する方法論(プロセスモデル又は手法)の提案

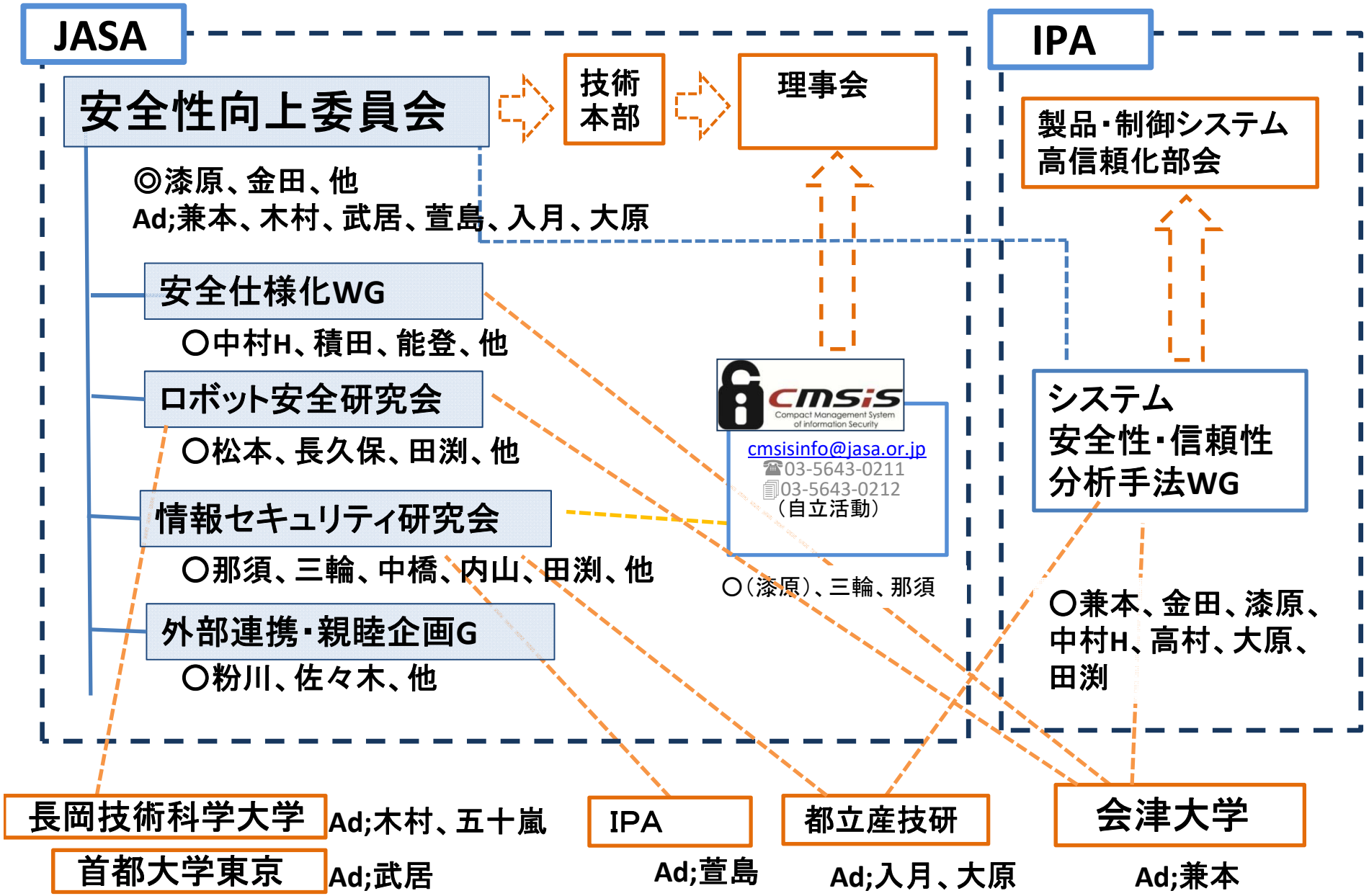
◆方針
- ■ 重点課題に方向を合わせて、自主的に活動する。
- ■ 活動結果を共有し、相互啓発を図る。

◆重点課題
- ■ 安全誘導型設計を支援するプロセスモデル及び手法

◆題材
- ■ 電動アシスト自転車(メーカの取説を参照)

◆活動方法
- ■ 月1回の会合で活動結果を報告・討議する。
- ■ メールを利用して情報・意見交換を進める。
- ■ 適宜、勉強会を計画する。

H28年度安全性向上委員会　活動体制



ご清聴ありがとうございました

2016/11/16 発行

安全誘導型設計の特徴と試行
ーー意図を記述すれば、安全性が高まるーー

発行者　一般社団法人 組込みシステム技術協会
東京都中央区日本橋大伝馬町6-7
TEL: 03(5643)0211
FAX: 03(5643)0212
URL: http://www.jasa.or.jp/TOP/