IPA Software Reliability Enhancement Center
Information-technology Promotion Agency, Japan

安心・安全な社会を支えるソフトウェアシステムの構築へ

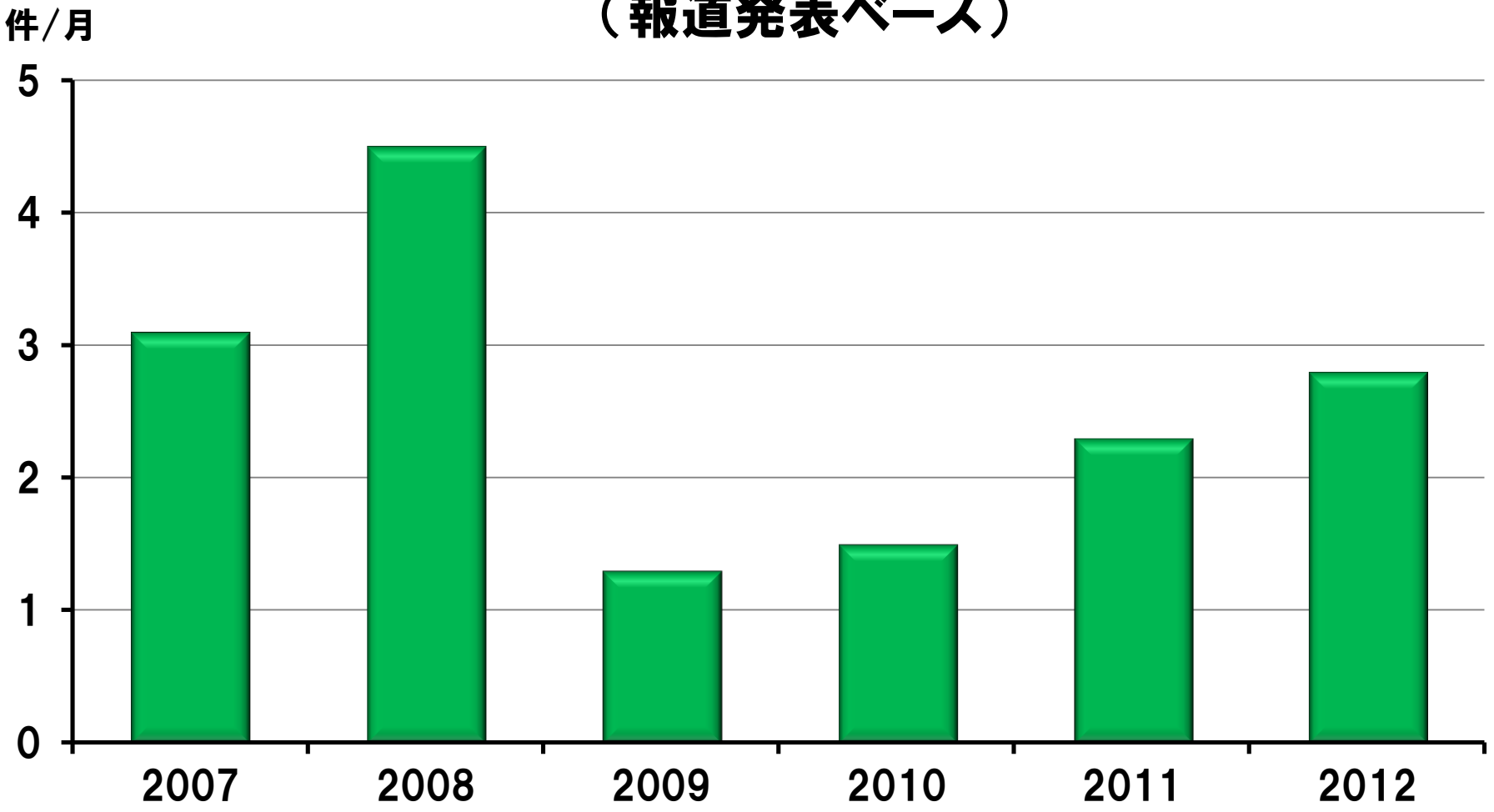
2014年2月21日

独立行政法人 情報処理推進機構(IPA)
技術本部 ソフトウェア高信頼化センター(SEC)
所長　松本隆明

なかなか減らないシステム障害

SEC
Software Reliability
Enhancement Center

社会経済活動に多大な影響を及ぼした情報システムの障害
（報道発表ベース）



IPA/SECの調査による

最近の障害の特徴

- 製品・装置の故障も、内蔵されているソフトウェアが原因であるケースが多い
- システム系の障害では、類似の原因に起因するケースが多い

自動改札機の不具合による大規模障害

2007.10.12

- JR東日本、地下鉄、私鉄の662駅で自動改札機が使えなくなる
- 原因は、ネガデータを中央のコンピュータから受け取る際、改札機のソフトウェアに不具合があり正しく読み込めず

2007.10.18

- 地下鉄等の65駅で窓口処理機が使えなくなる
- 原因は10/12のトラブルと同一。改札機と窓口機で不具合の発生条件が異なった

約260万人の利用者に影響

日本製自動車はソフトウェアが疑われた

SEC
Software Reliability Enhancement Center

NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Enter Email Address SUBSCRIBE SEARCH Home
Sign up for Email Updates

DRIVING SAFETY | VEHICLE SAFETY | RESEARCH | DATA | LAWS & REGULATIONS | ABOUT NHTSA

- About the Administrator
- Calendar
- Congressional Testimony
- Jobs at NHTSA

Print | Share | RSS Feed | Email

U.S. Department of Transportation Releases Results from NHTSA-NASA Study of Unintended Acceleration in Toyota Vehicles

DOT 16-11
Tuesday, February 8, 2011
Contact: Olivia Alair

...grity to conduct new research into whether ...d role in incidents of unintended acceleration.

...ehicles capable of producing the large throttle openings required to create dangerous ...o mechanical safety defects identified by NHTSA more than a year ago - "sticking" ...elerator pedals to become trapped by floor mats - remain the only known causes for ...nts. Toyota has recalled nearly 8 million vehicles in the United States for these two

- 2009年～2010年日本製自動車の「意図しない急加速(UA)」に関するクレームが急増
- 米国議会や米運輸省道路交通安全局(NHTSA)から品質報告を求められるもメーカ側は説明に苦慮
- NHTSAは第三者機関であるNASAに不具合の有無の調査を要請　→結果はシロ

電子スロットル制御システムのソフトウェアが疑われた

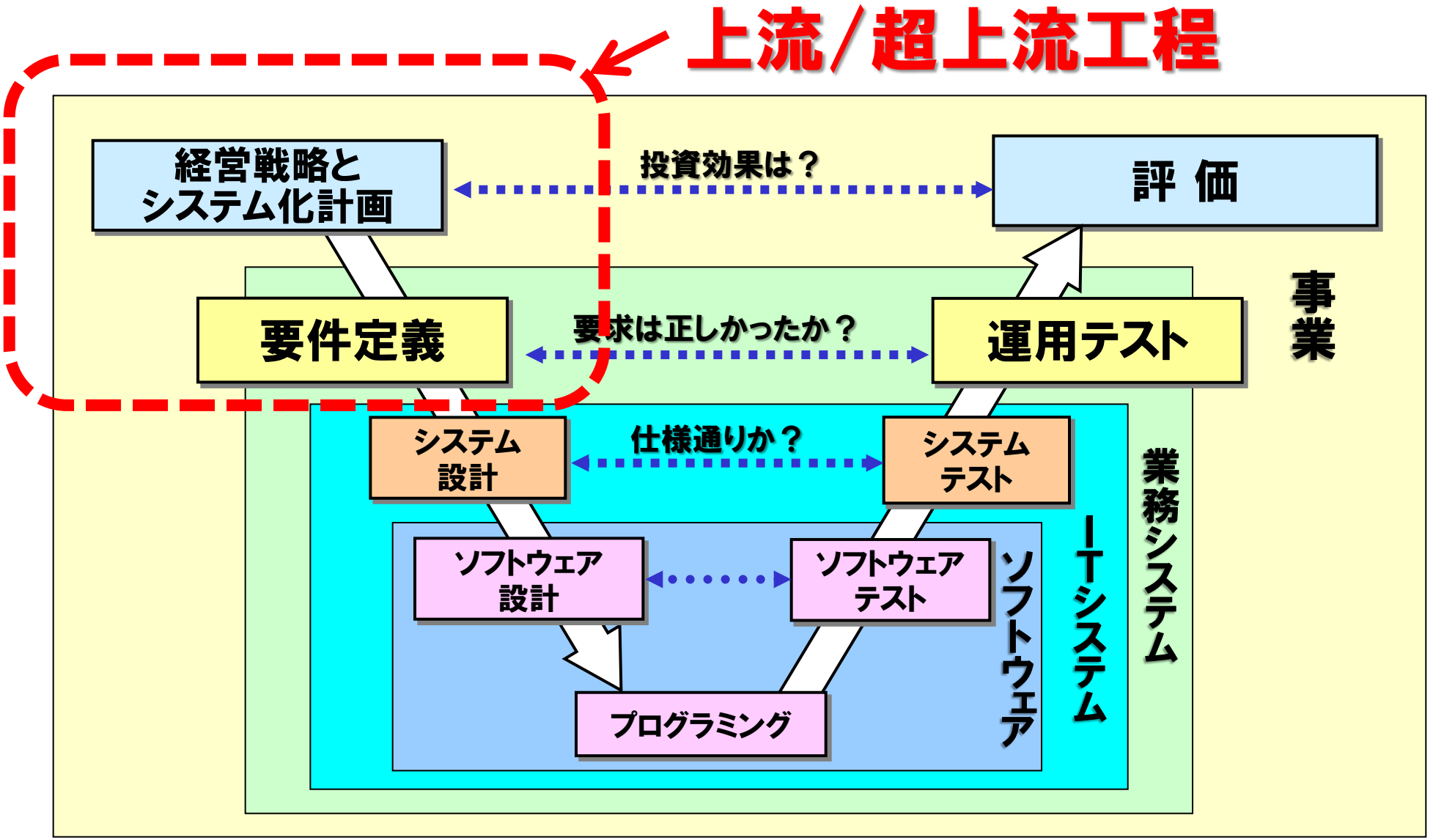
出典:http://www.nhtsa.gov/PR/DOT-16-11

ハードウェア開発とソフトウェア開発

SEC
Software Reliability Enhancement Center

	要件定義	設計	製造
ハードウェア開発			
ソフトウェア開発			

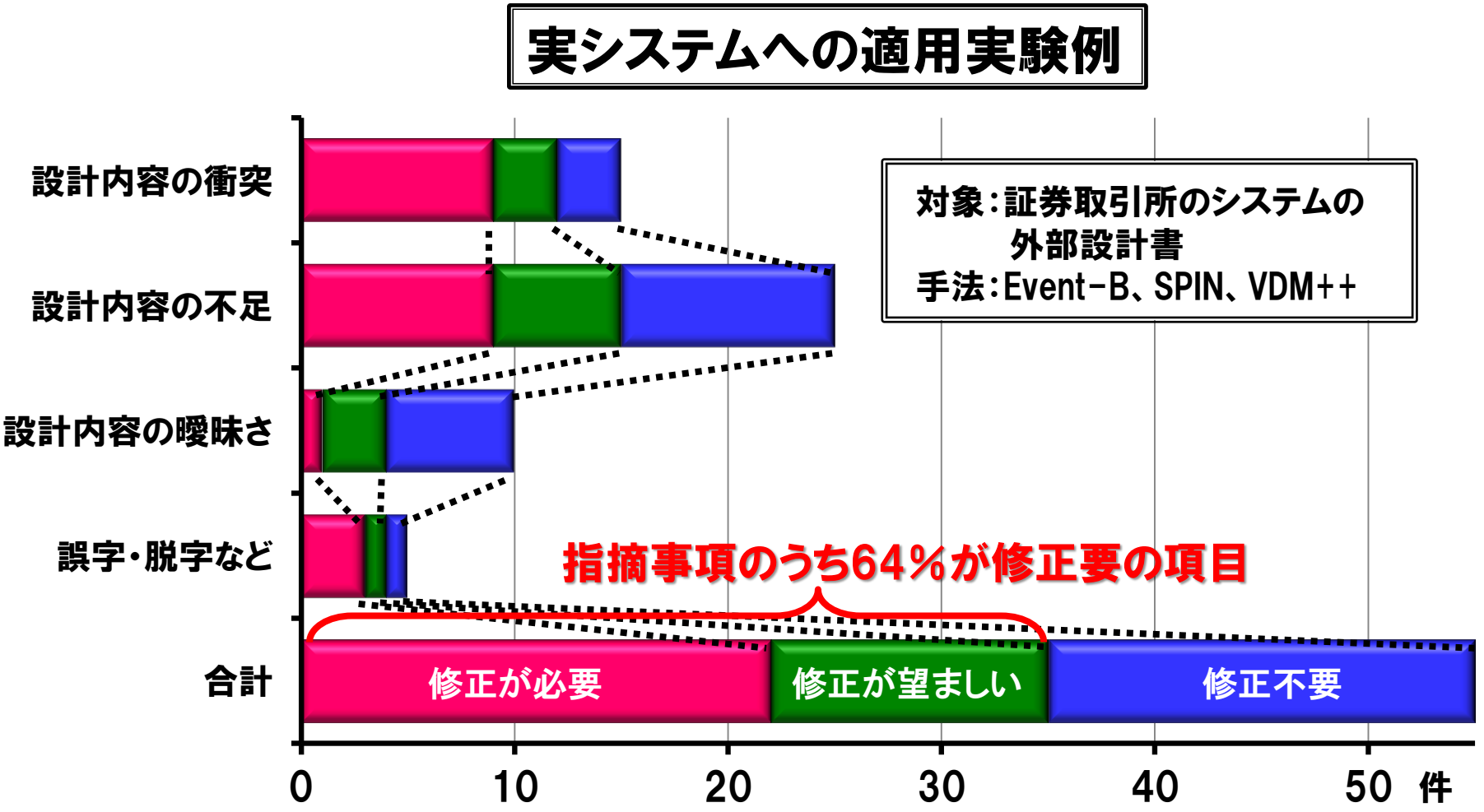
ソフトウェア開発は上流工程がカギ



形式手法の適用

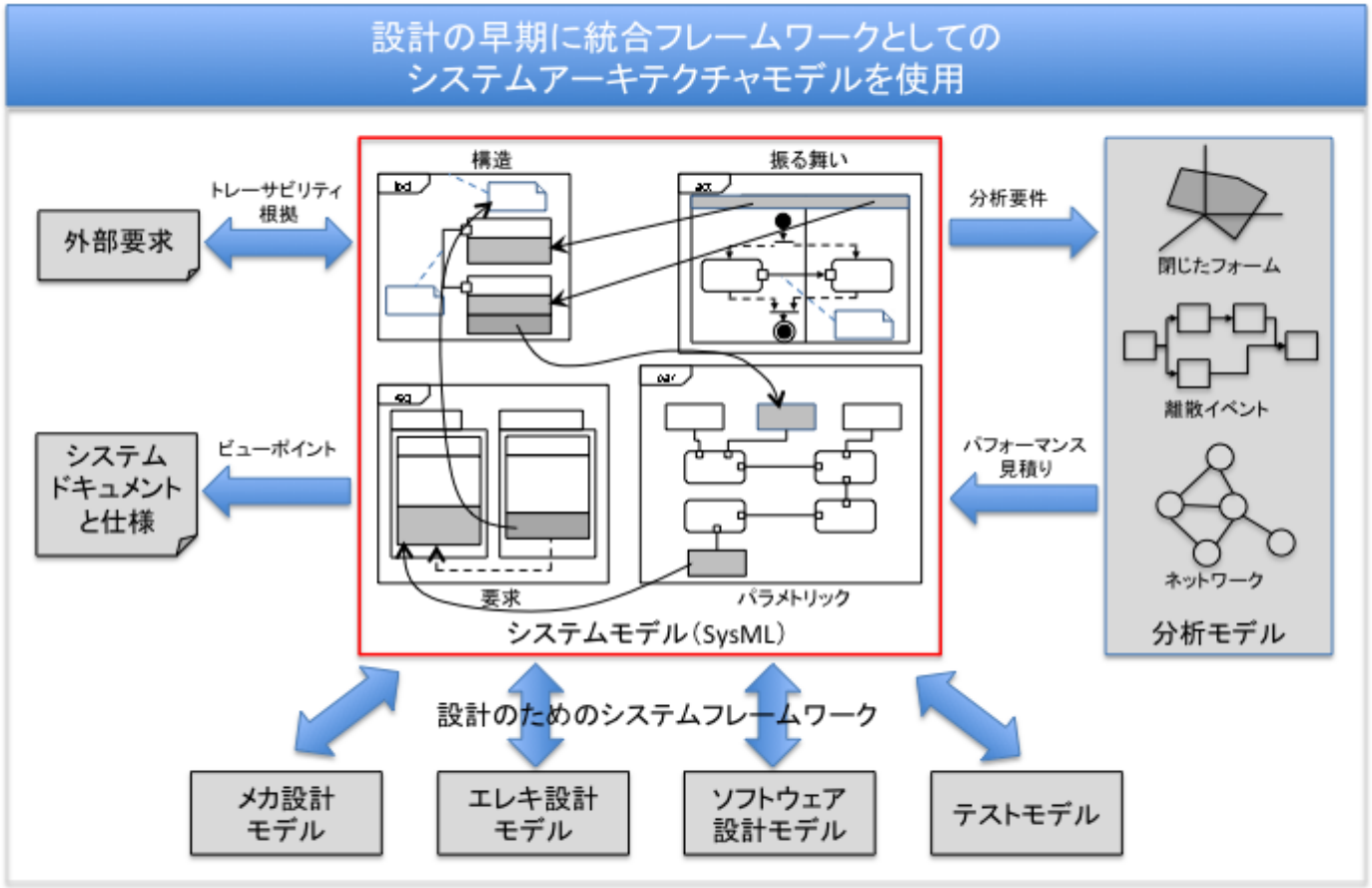
SEC
Software Reliability Enhancement Center

- 形式手法とは、数学的な規範を用いることで、設計の曖昧性や不正確さを排除する手法の総称



モデル指向開発(MBSE)の適用

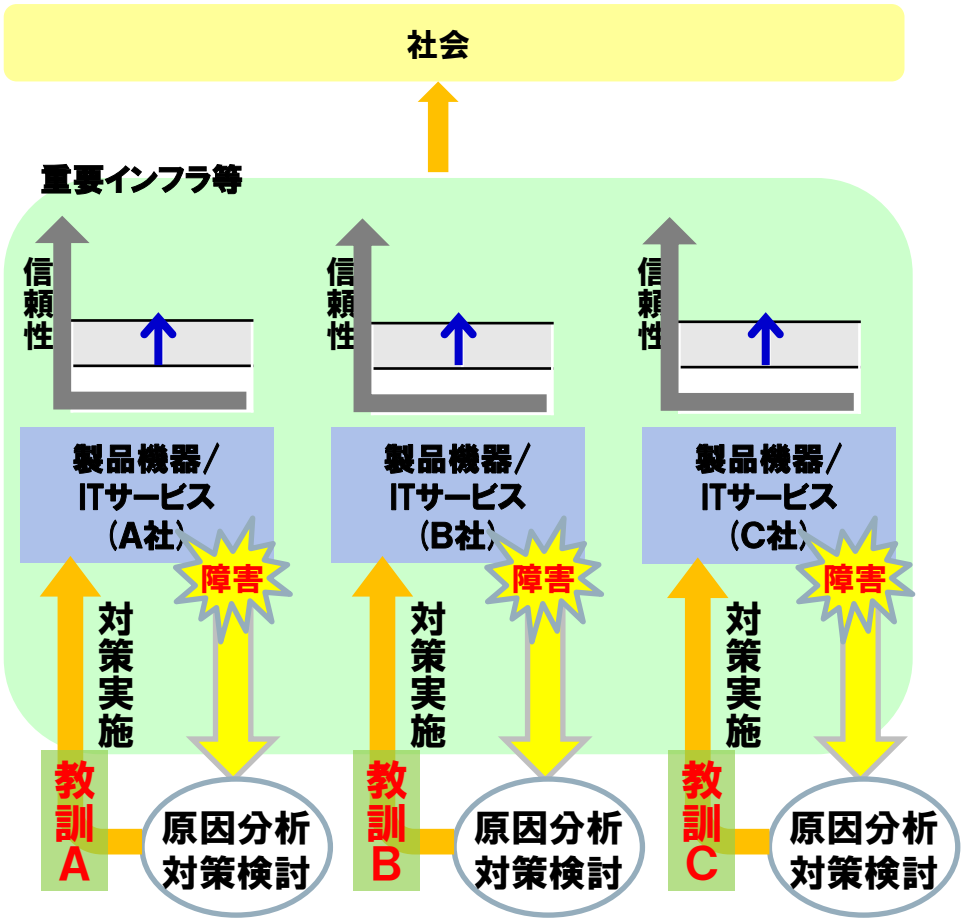
- 対象のモデルを適切に構成要素に分割(decompose)できるため、QCDSE(品質、コスト、納期、安全性、環境)などのバランスをとることができる



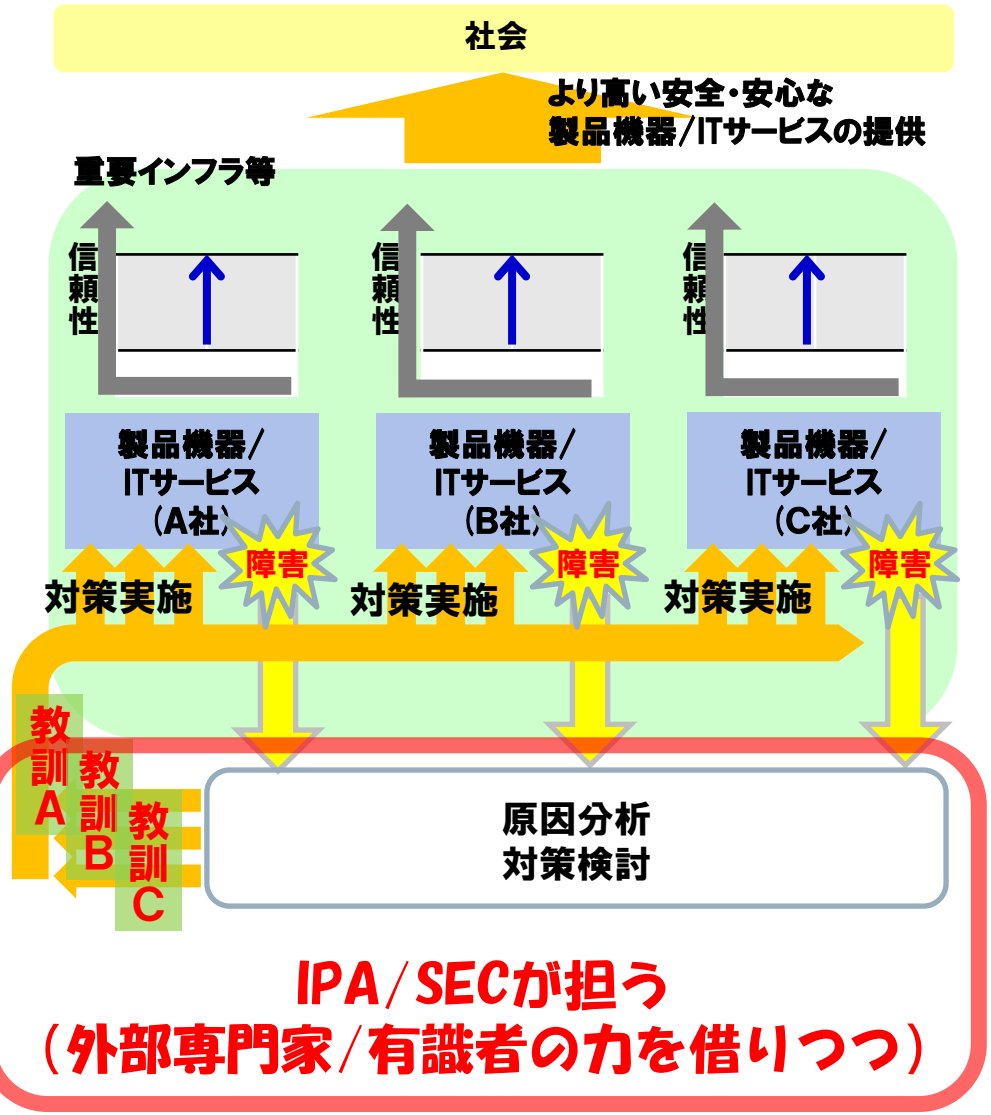
類似障害の再発防止の仕組み作り

SEC Software Reliability Enhancement Center

現状（教訓の共有なし）



障害に基づく教訓の共有による信頼性向上のしくみ



日本製自動車の不具合懸念の事例からの教訓

SEC
Software Reliability Enhancement Center

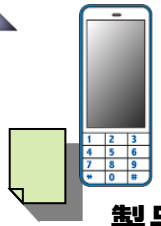
- これまでの日本企業は、利用者の要望に個々に答えることで高品質というブランド力を築いてきた
- 実際、日本製のソフトウェアの品質は海外に比べて1桁以上高いとの調査結果
- しかしながら、企業の主張だけでは、第三者による客観的な評価
  - 会計処理における監査と同等
- 一旦ブランドが傷つくと、その損失は極めて大きい
  - 今回のケースでは直接的な不具合は検出されなかったためUAに対する損害賠償請求にはメーカ側が勝訴したが、ブランドイメージの低下により車両の価値が下がったとして顧客から訴えられ、11億ドル（当時のレートで約940億円）支払うことで和解

Trust Meでは通用しない!!

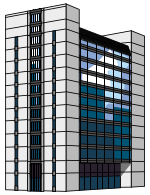
第三者が品質を確認する仕組みの導入

利用者

提供



製品
品質説明

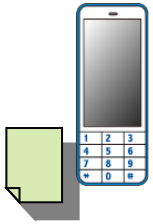


供給者

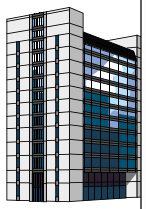
第三者が品質確認する制度の導入

供給者のメリット

顧客からの信頼向上
ブランド力向上
製品事故等による事業リスクの低減
国際市場における競争力の強化



製品、
品質説明

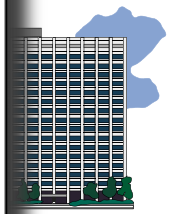


供給者

利用者のメリット

製品の適切な選択
製品の安全な利用
確認による安心感

判定結果

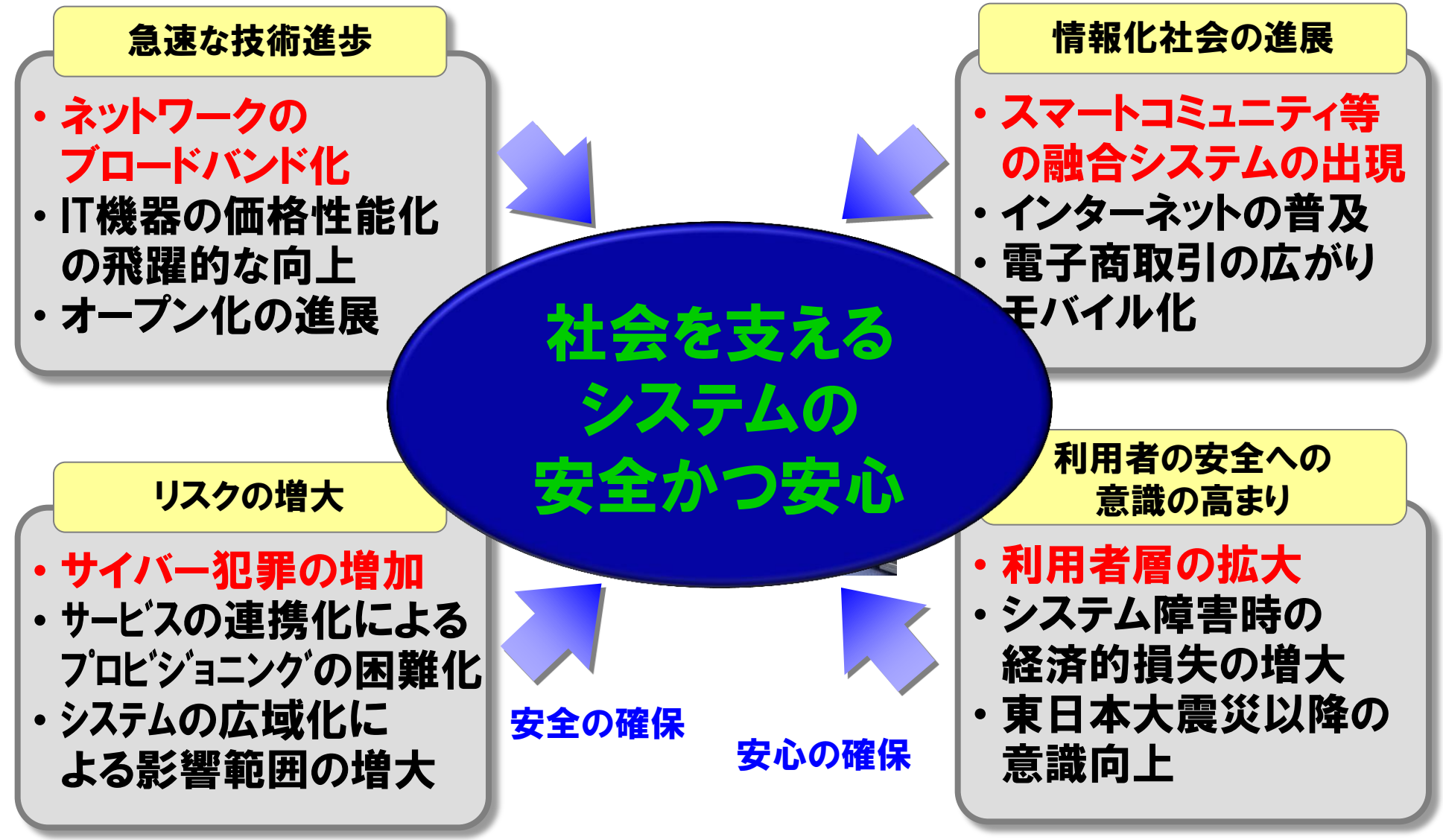


三者

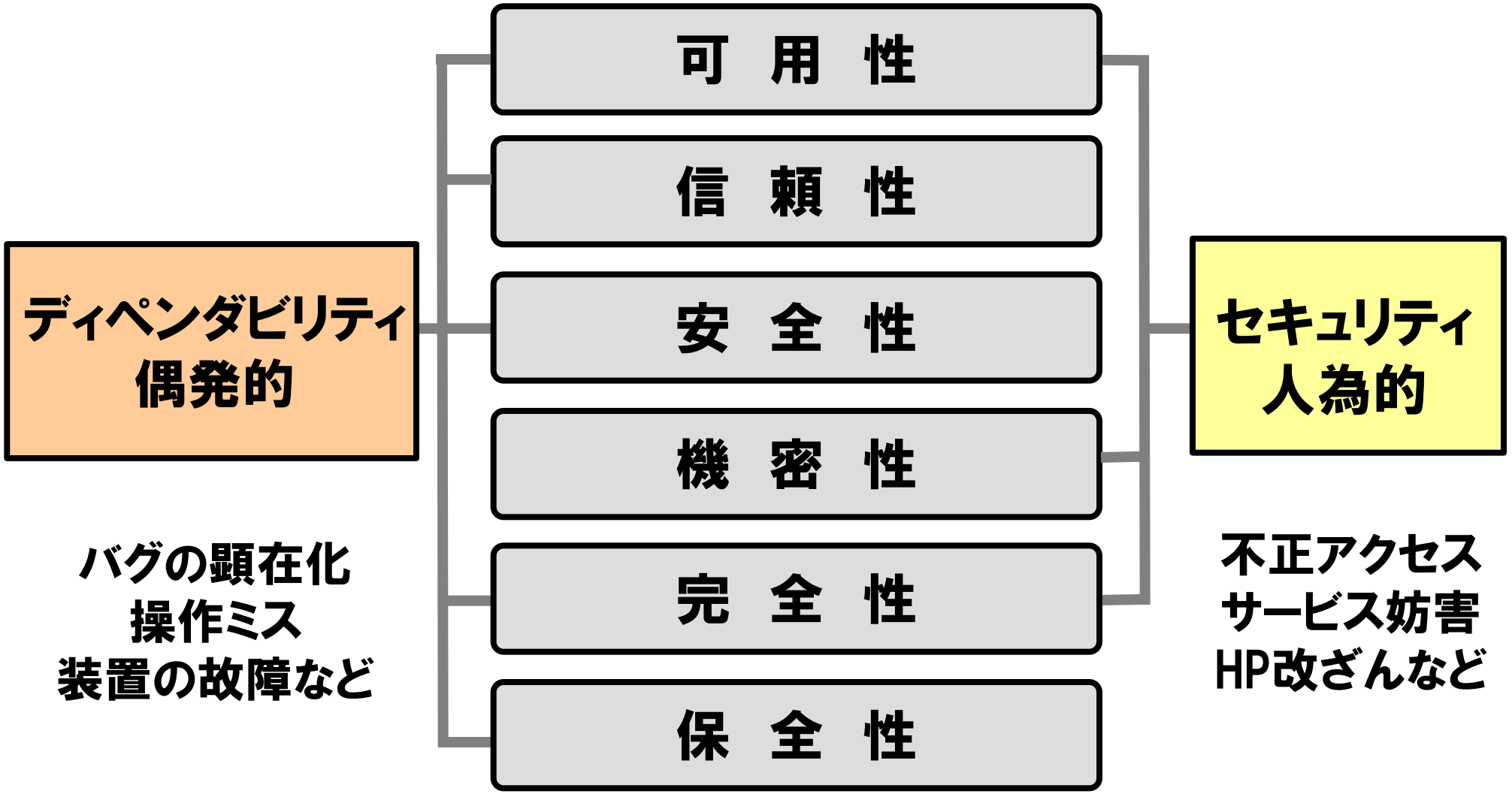
審査基準

ソフトウェアシステムを取り巻く環境の変化

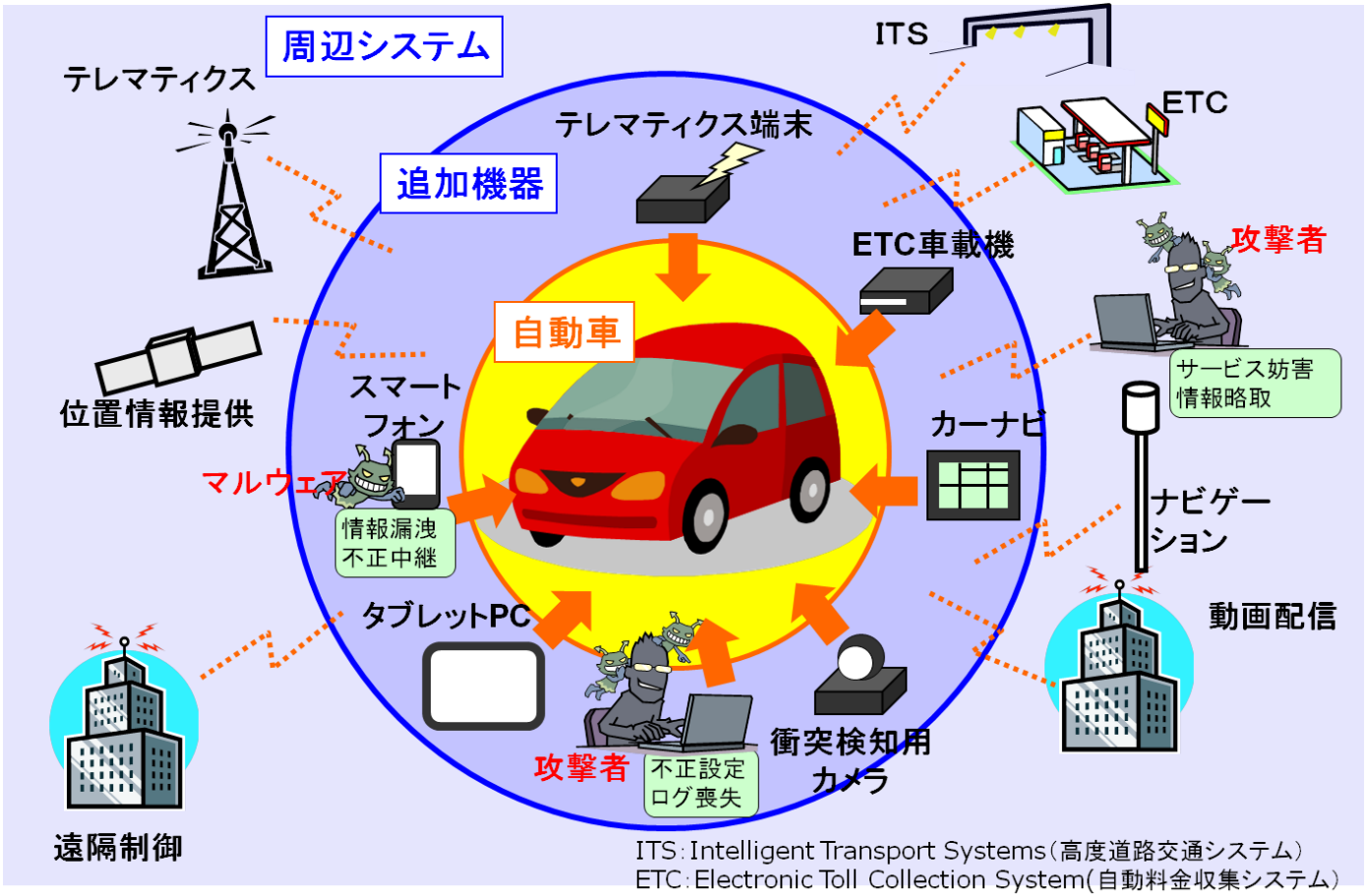
SEC Software Reliability Enhancement Center



ディペンダビリティとセキュリティの確保



自動車も外部と繋がる



自動車が様々な機器やサービスに繋がることで、様々な場所に攻撃者が現れる可能性がある。

「セキュリティ」への対策が必要

ディペンダビリティの重要性

SEC
Software Reliability Enhancement Center

- **自動車は、特に安全性と可用性を同時に満たす必要がある。**
  - 安全でなければならないが、高速道路や砂漠での走行等を考えると、何かあった時に安全のため停止してしまうだけではなく、必要とされる時には可能な限り継続して走り続けられる可用性等も必要。

自動車のようなコンシューマデバイスは
「ディペンダビリティ」を保証することが必要

ディペンダビリティを保証する体系的な枠組み

SEC
Software Reliability Enhancement Center

IPAが中心となって、産官学連携により枠組みを策定