Dependable VLSI ： 新しい付加価値を求めて

安浦, 寛人
九州大学大学院システム情報科学研究院 | 九州大学システムLSI研究センター

出版情報：SLRC プレゼンテーション, 2006-11-13. 九州大学システムLSI研究センター
バージョン：
権利関係：

Dependable VLSI
ー新しい付加価値を求めてー

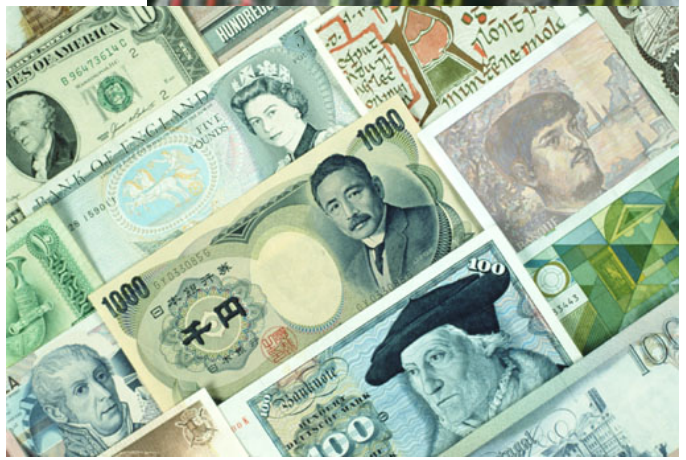
安浦寛人
九州大学システムLSI研究センター
2006.11.13

Dependable VLSI

- 社会情報基盤としてのVLSI
- 技術的課題
- Dependabilityの概念
- Dependabilityを保証する技術
- 今後の展開

情報通信システムは社会のインフラ

- 20世紀後半は既存の社会システム（19世紀後半から20世紀前半に基本設計された）の中に情報通信技術を部分的に導入し、サービスの高度化、高速化を進める時代であった。
- 通信速度、情報処理速度の向上は、システムの設計時に想定しなかった事態を生み出すようになった。
- 21世紀は情報通信技術を前提として社会システム自身を再設計する時代。
  - 社会情報基盤(Social Information Infrastructure)
  - ユビキタス社会、e-Japan、u-Japan



過去50年で何が変わったのか？

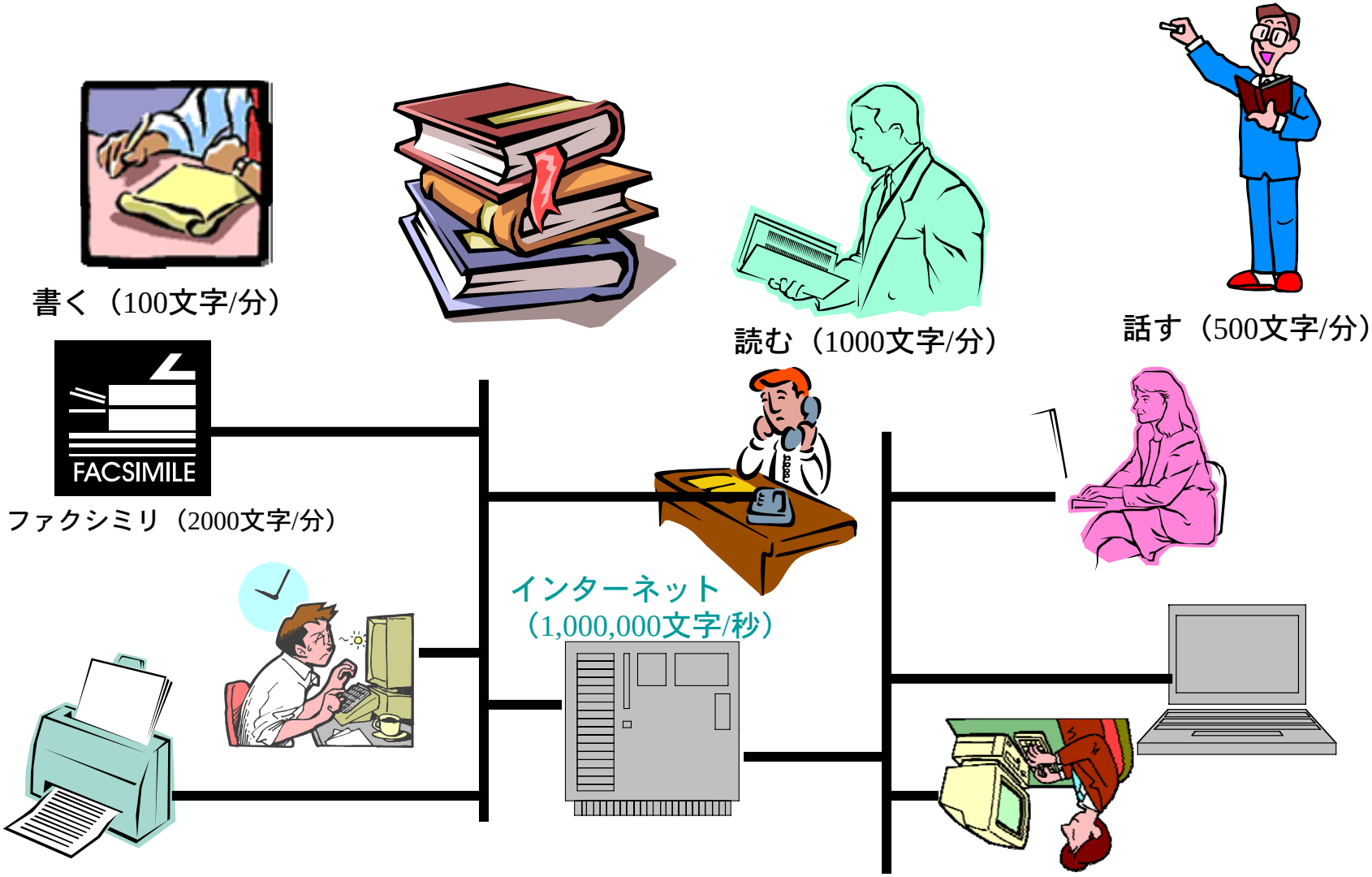
- 社会活動における物理的制約の削減
  - 100万人分の個人データの移動（トラックー＞DVDまたはファイル転送）
  - 情報の移動に対する大きさ，重さ，時間の制約
- 社会システムにおける情報の影響が伝わる時間（時定数）
  - 9.11の世界同時中継
- 物に基盤を置く経済から情報の経済へ
  - 世界的な為替や株の取引
  - Yahoo、Google、Amazon.com、楽天
  - 世界的分業体制（インドの台頭）
- 価値や信用の媒体とその裏付けの仕組み
  - 物質の保存則をベースにした過去の仕組みからの脱却
- 情報通信技術に依存したフラットな世界

The World Is Flat [Updated and Expanded]:
A Brief History of the Twenty-first Century
by Thomas L. Friedman
ISBN: 0374292795

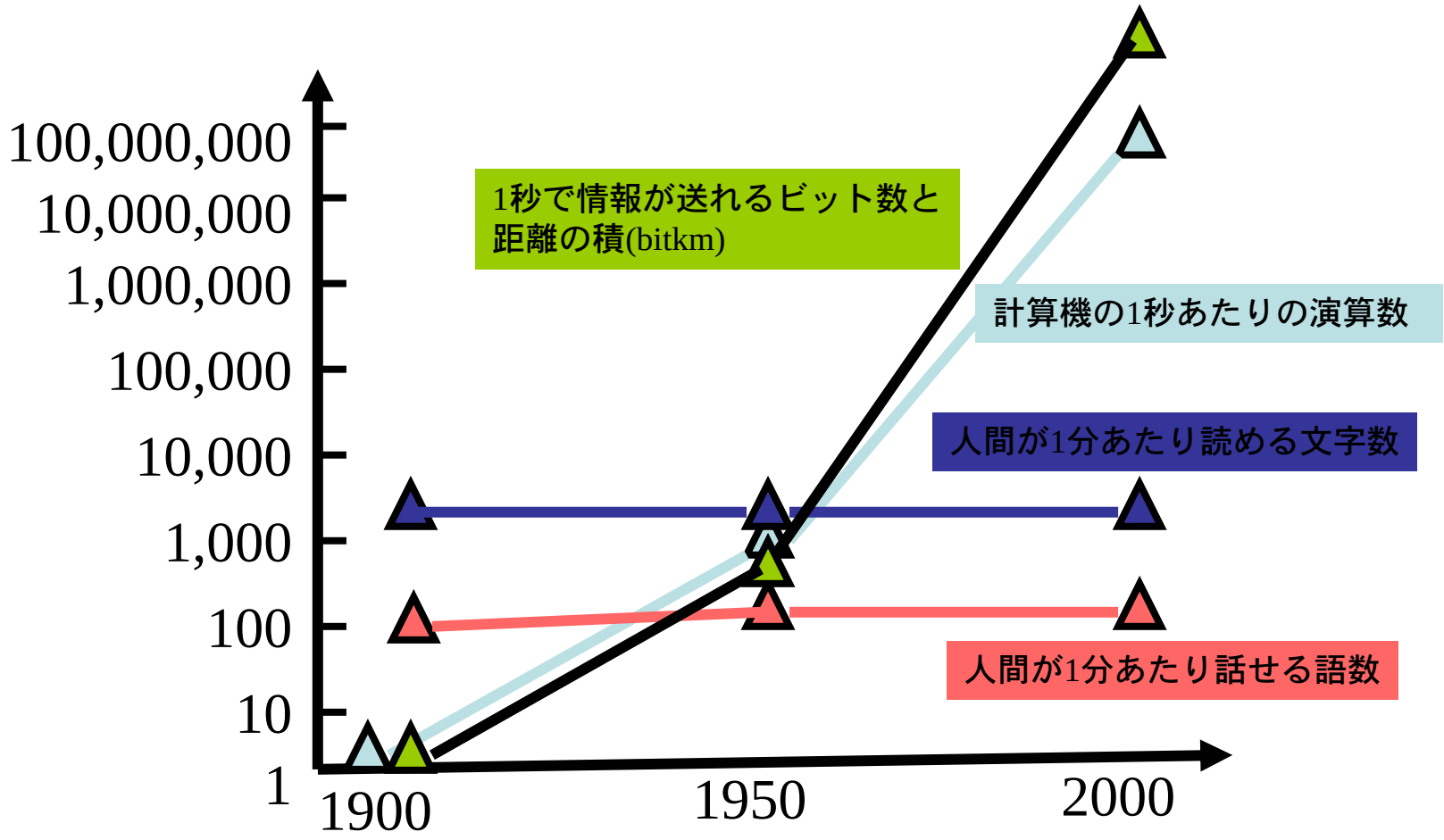
April 2006

QuickTimeý Ç²
TIFFÂià[èkÇ»ÇµÂj êLí£ÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÂÉsÉNÉ`ÉÉÇ¾å©ÇÈÇžÇ½Ç…ÇÔïKóvÇ-Ç[ÅB

人間と情報技術の能力


書く（100文字/分）
読む（1000文字/分）
話す（500文字/分）
FACSIMILE
ファクシミリ（2000文字/分）
インターネット
（1,000,000文字/秒）

情報の通信・処理の変化



ー＞社会システムの本質的な不安定化

人類文明の基盤も変わる
―貨幣システムの例―

価値の量（大きさ）と保存則の保証

2,000 年

1,000年

金属貨幣 （紀元前10C）
価値の量：物質（金属）
価値の保存則：物質保存則

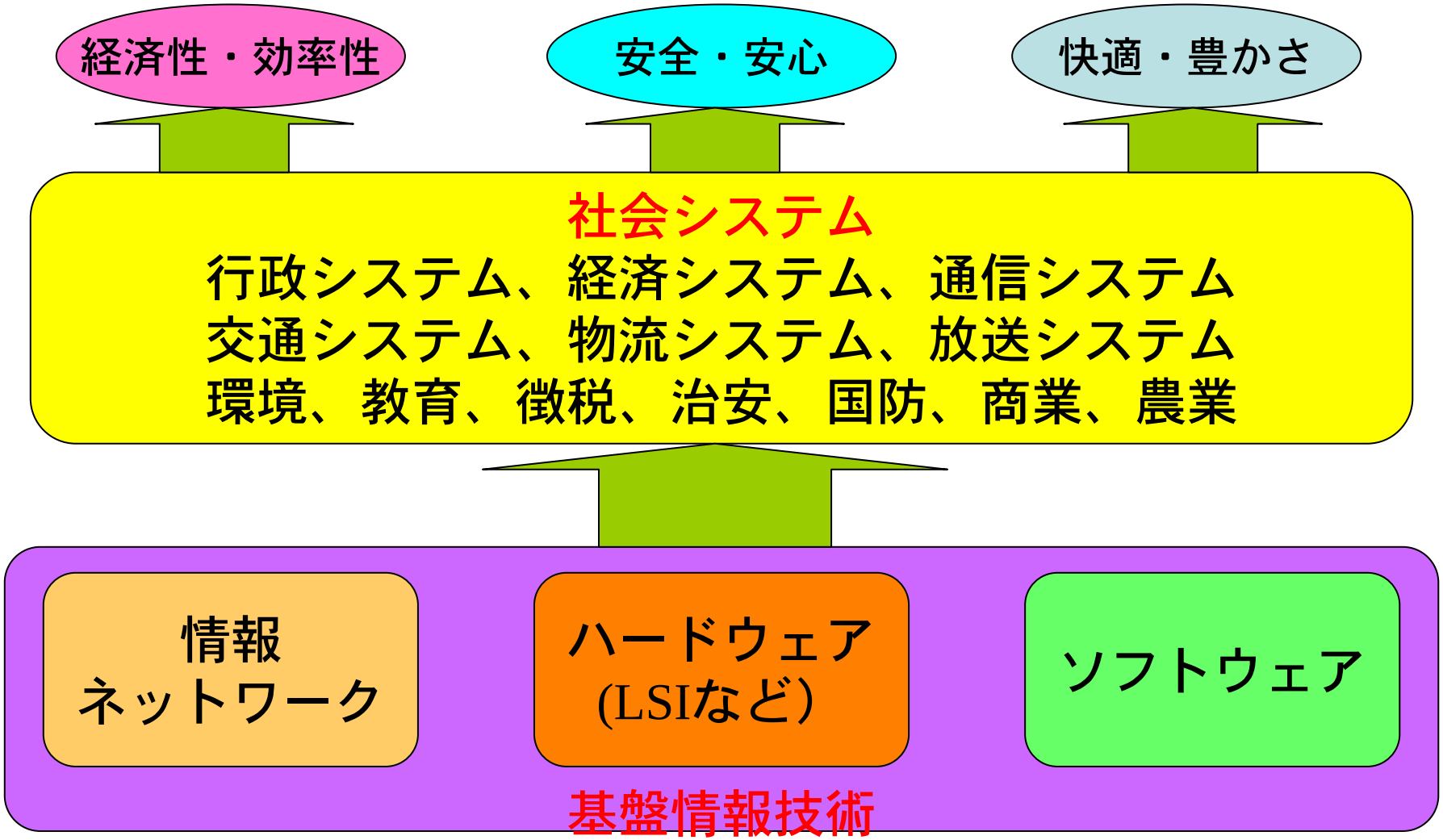
紙幣（紀元10C）
価値の量：情報（印刷）
価値の保存則：物質（紙）

電子マネー （21C）
価値の量：情報
価値の保存則：情報

完全なコピーが可能な
情報で価値が保存できるか？

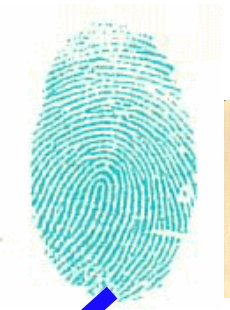
社会情報基盤の構築

Dependableな社会システムの再構築とそのために必要となる
基盤情報技術のDependability



価値や信用を搭載するLSI

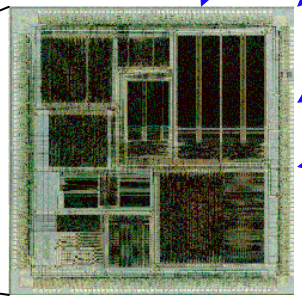
Hiroto Yasuura
Department of Computer Science and Communication EngineeringGraduate School of Information Science and Electrical EngineeringKyushu University6-1 Kasuga Koen, Kasuga, 816-8580, Fukuoka, Japan
Tel. +81-92-583-7620,
FAX +81-92-5831338
yasuura@c.csce.kyushu-u.ac.jp,
yasuura@slrc.kyushu-u.ac.jp
http://www.c.csce.kyushu-u.ac.jp/SOC/index.html,
http://www.slrc.kyushu-u.ac.jp



電子マネー

￥50,000

個人情報



¥3,000/Chip

Signature

Credit Cards

¥18,000

LSIは財布か貨幣か？

- 財布であるなら
  - 偽物でも入っている「価値」が本物なら許せる
  - ブランド品と安物の差はあっても、中身の「価値」とは無関係
- 貨幣であるなら
  - 政府の通貨発行権や徴税権と密接に関係する
  - 財務省印刷局LSI部門が必要？

Dependable VLSI

- 社会情報基盤としてのVLSI
- 技術的課題
- Dependabilityの概念
- Dependabilityを保証する技術
- 今後の展開

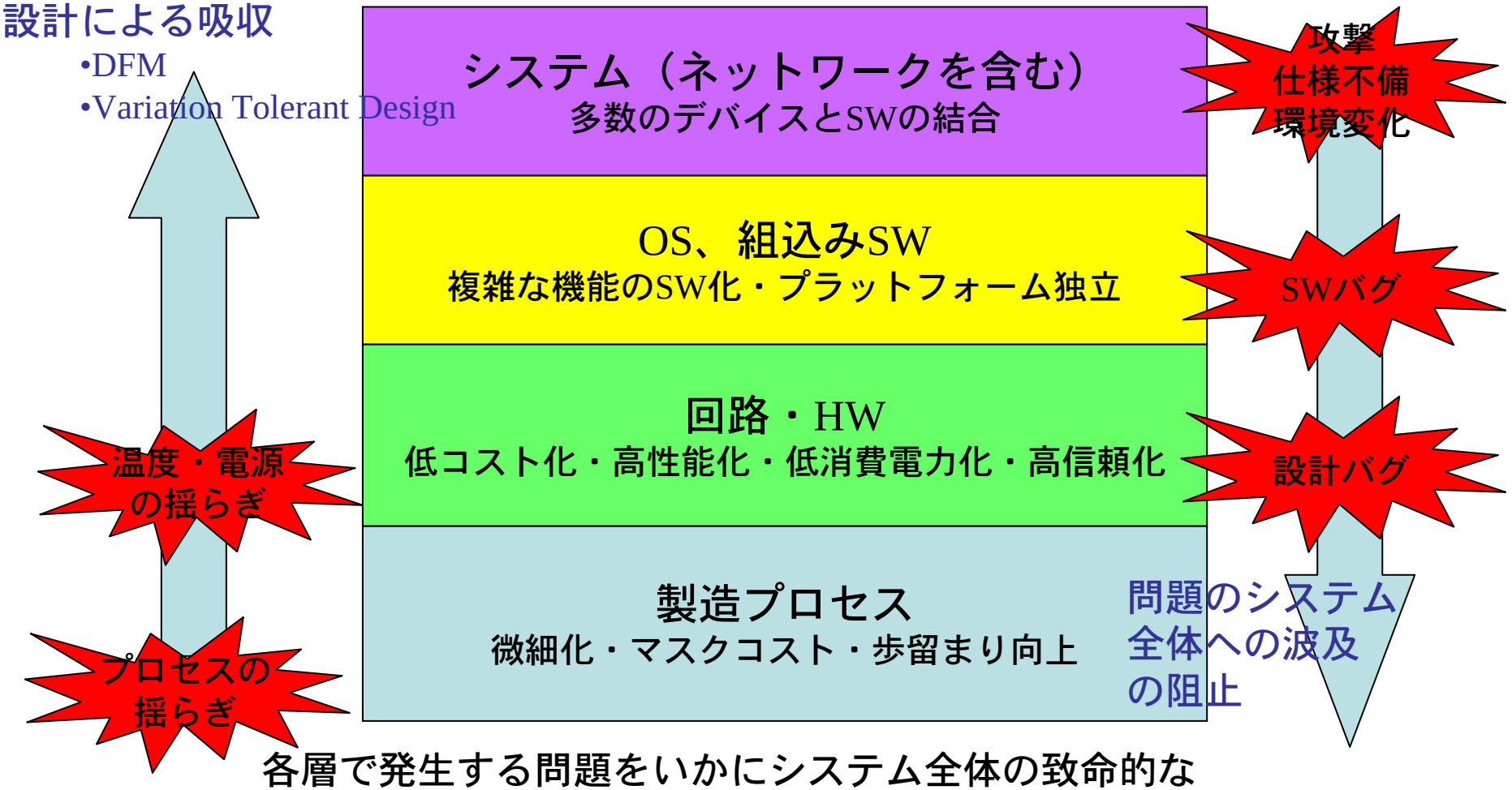
何が問題か？

- 産業・社会構造の変化
  - サービス中心の産業構造への転換
  - 価値や信用の移動速度の劇的変化
  - 社会システムの情報通信技術への依存度の増大
  - 電子情報系と機械系などの他分野技術の融合
- システムの複雑化
  - 世界的なネットワーク接続（地理的拡大）
  - 異なる分野のシステムとの接続（異分野との統合）
  - 新旧の各種システムとの接続（時間軸での統合）
  - 微細化・大規模化による揺らぎや不確実性の増大
  - 設計者、製造者、利用者の理解不足（技術と人間のギャップ）
- 想定外の事象の発生とそれへの対応
  - Specification-basedの技術からPolicy-basedの技術への転換
  - 即時的な応急回復機能への要求（Instant Recovery)
  - 保険や責任体系の変化
  - 制度、法律、規則の整備や改変との連携

JST研究開発戦略センター
ディペンダビリティワークショップ資料

揺らぎと不確実性への増大

物理的揺らぎの
設計による吸収
- DFM
- Variation Tolerant Design



各層で発生する問題をいかにシステム全体の致命的な
問題にせずに済ませるかという問題

微細化によるLSIの信頼性の問題

- リーク電流
  - 発熱、誤動作、製品寿命短縮の原因
- プロセス(P)変動
  - プロセスパラメータ(P)の変動やCVD工程などによる薄膜の破壊によるのVtの変動
- 電源(V)変動
  - 電流の偏りや電源線の抵抗成分による電源電圧の変動
- 温度(T)の変動
  - 温度の変化による回路遅延変動
- ソフトエラー
  - 宇宙線が大気と反応して生成される中性子線などによるメモリビット反転や論理誤動作
- クロストーク
  - 配線間カップリング容量による信号変形、遅延変動

人間に起因する問題

- システムの複雑化・巨大化による問題
  - 回路設計やソフトウェアのバグ
  - システム仕様の不完全化・変化
  - 想定外の事象
  - 他システムの影響
- 外部からの攻撃
  - 不法な利用者
  - テロや軍事的攻撃

Dependable VLSI

- 社会情報基盤としてのVLSI
- 技術的課題
- Dependabilityの概念
- Dependabilityを保証する技術
- 今後の展開

Dependabilityとは

- ユーザ視点の概念
  - ユーザ（利用者）が、その生命、財産、プライバシーなどを安心して委ねられるシステムが持つべき性質

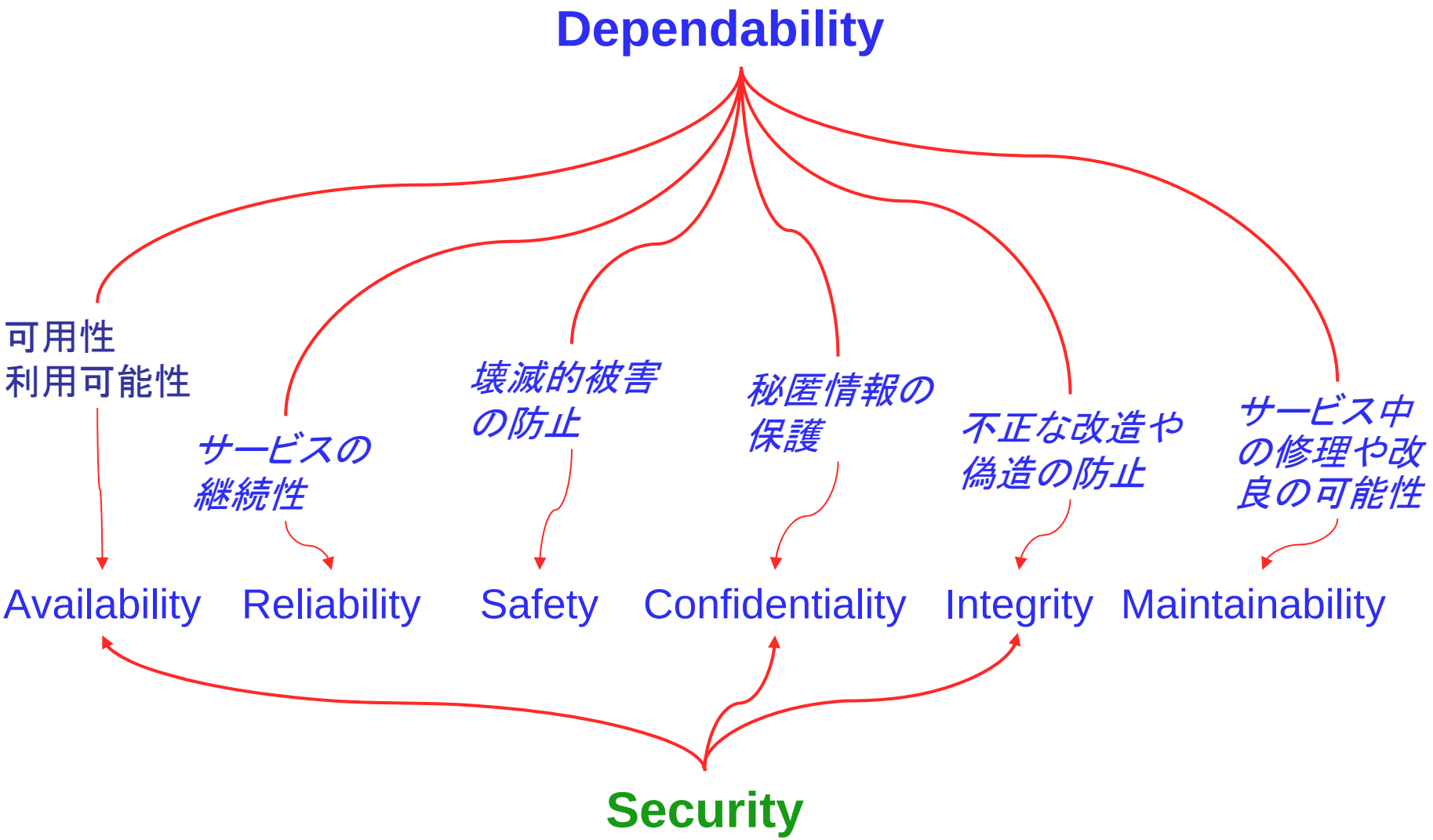
- 予測不可能性（想定外事象）を秘めた系において、システムに期待されるサービスが許容範囲内で提供されることが保証されること。あるいは、その保証の度合。
  - 合理的な有限責任をユーザに宣言するための基礎となる性質
  - 無限責任を負うべきシステム（航空機や原子力など）については、極めて厳しいレベルで要求される

安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

何故Dependabilityか？

- 社会システムが急速に発達した情報技術に大きく依存するようになり、社会システム自身の再構築が必要となっている。
- Openなシステムが世界規模で実用化され、Closed Loopを前提としたシステム開発手法が適用できず、新たな工学手法が必要である。
- 技術の微細化・高速化・高集積化による種々の物理的限界、システム複雑化や相互接続による設計ミスや運用時のエラー、悪意ある攻撃者による各種の攻撃などによってシステムの安全性・信頼性・安定性などが脅かされている。
- さらに、システムのオープン化により従来の意味での「仕様（製品と社会の契約）」が定義できなくなった。
- 上記の各種のFault（人間のエラーや攻撃を含む）は不可避なので、その存在を前提として安全で安心な社会システム構築のための技術開発が必要である。
- Commodity部品により構築される社会システムの信頼性や安全性が危惧されている。
- ユーザ・製造者・設計者・運用者・許認可権者の責任の明確化も重要である 。
- このような状況で、安全・安心を保証するための新しい指導原理と技術が必要となっている。

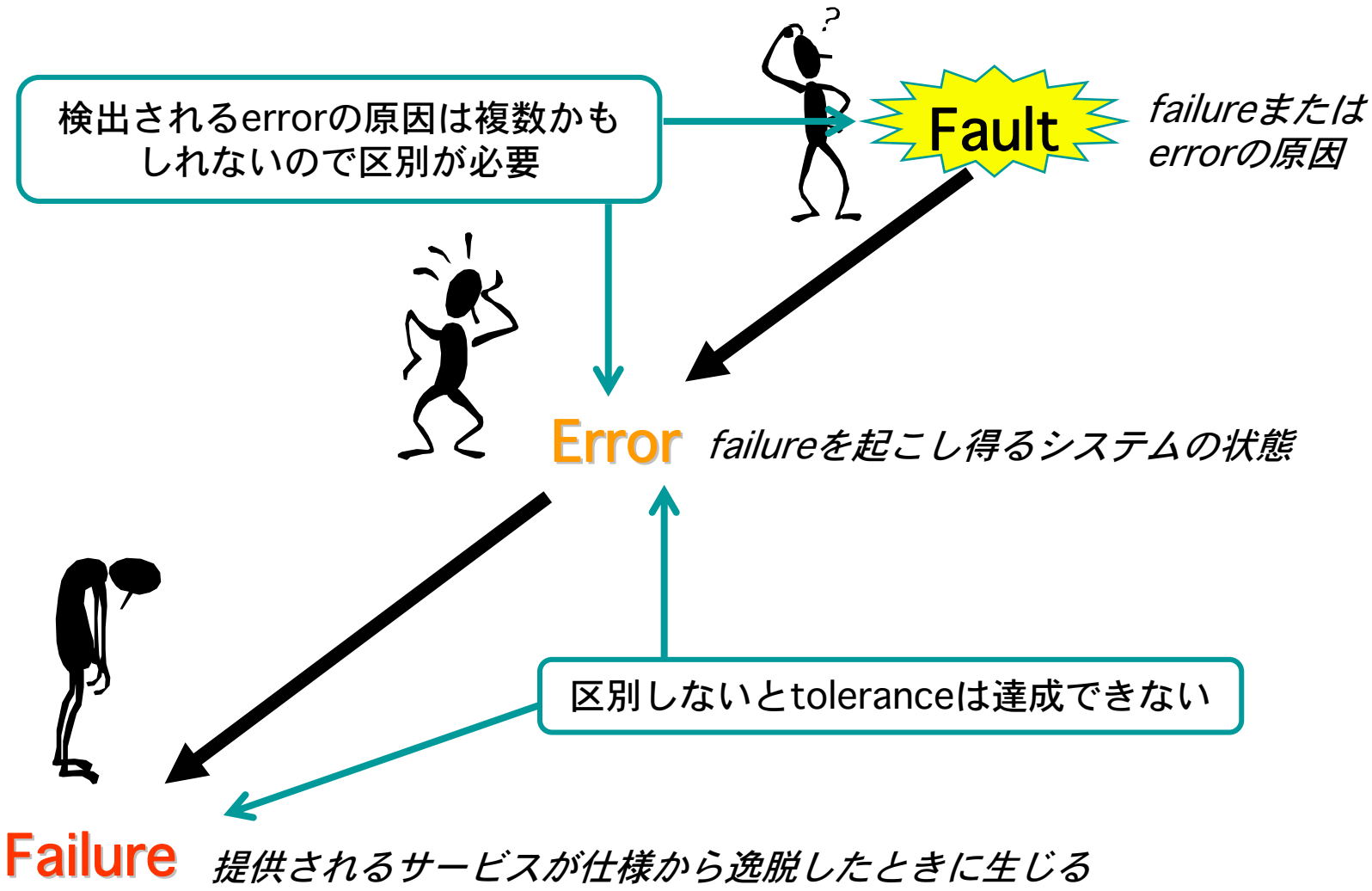
安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料



Absence of unauthorized access to, or handling of , system state

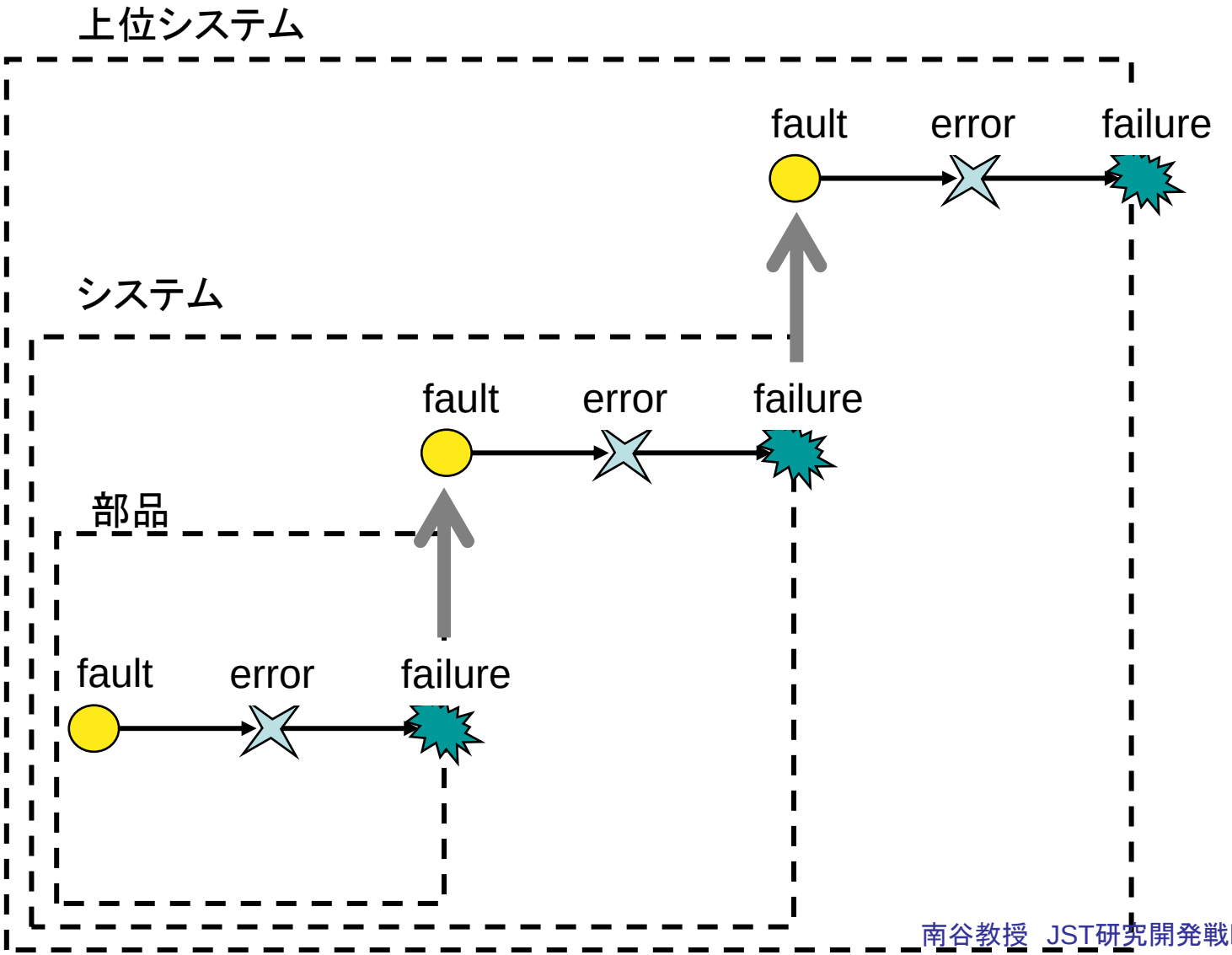
南谷教授　JST研究開発戦略センター
ディペンダビリティワークショップ資料

Dependability 阻害要因の因果関係



南谷教授　JST研究開発戦略センター
ディペンダビリティワークショップ資料

従来の故障と障害の因果関係モデル



南谷教授　JST研究開発戦略センター
ディペンダビリティワークショップ資料

Dependability Chain

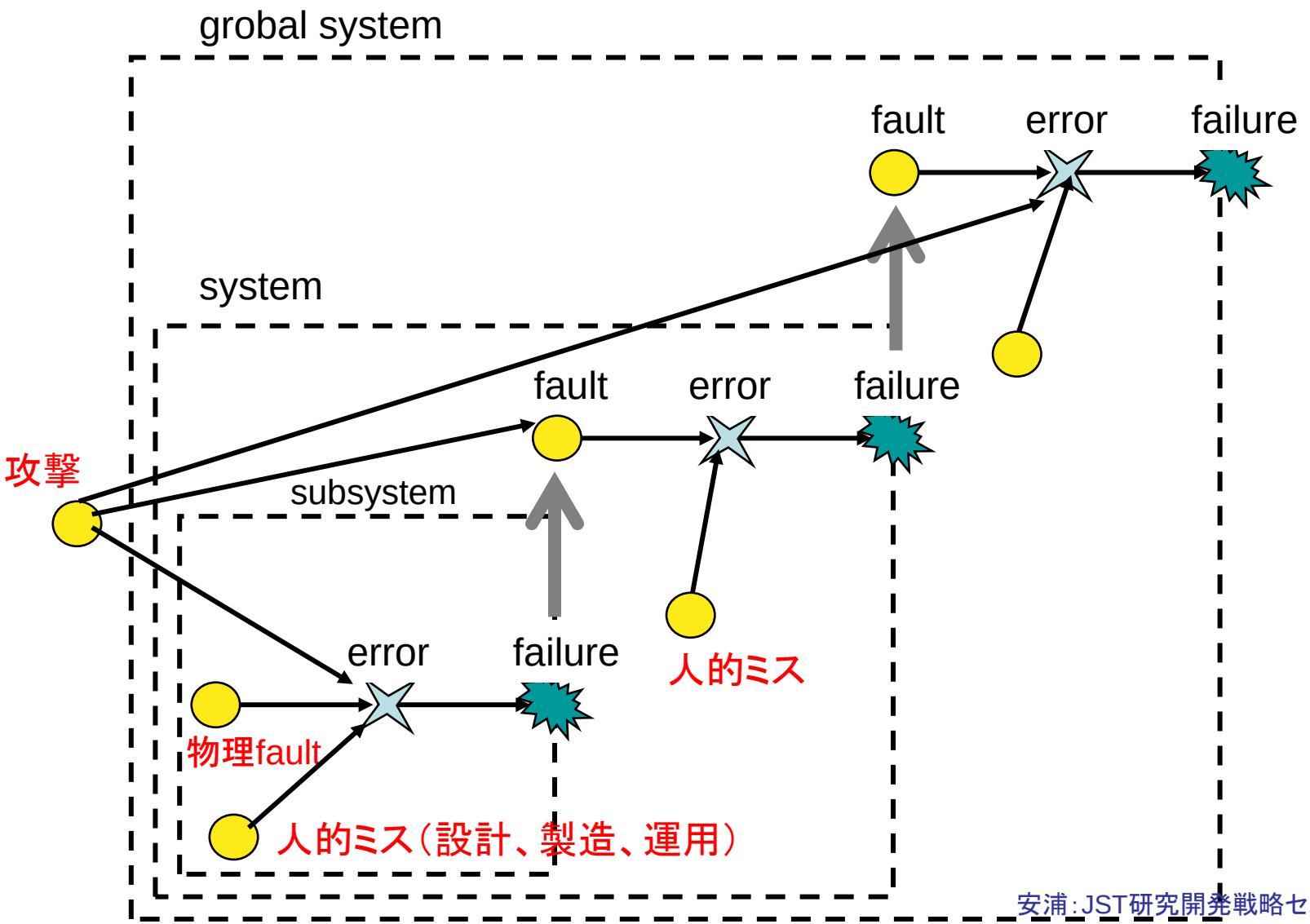
- 社会→システム
  →サブシステム
  →デバイス
- 自動車の例
  - 社会：交通システム
  - システム：自動車、道路、信号系、交通規則
  - サブシステム：エンジン、制動系、ステアリング
  - デバイス：機械系、電子系、材料系

QuickTimeý Ç²
TIFFÅiàlèkÇ»ÇµÅj êLí£ÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾å©ÇÈÇžÇ½Ç…ÇÕïKóvÇ-ÇlÅB

現代的な問題

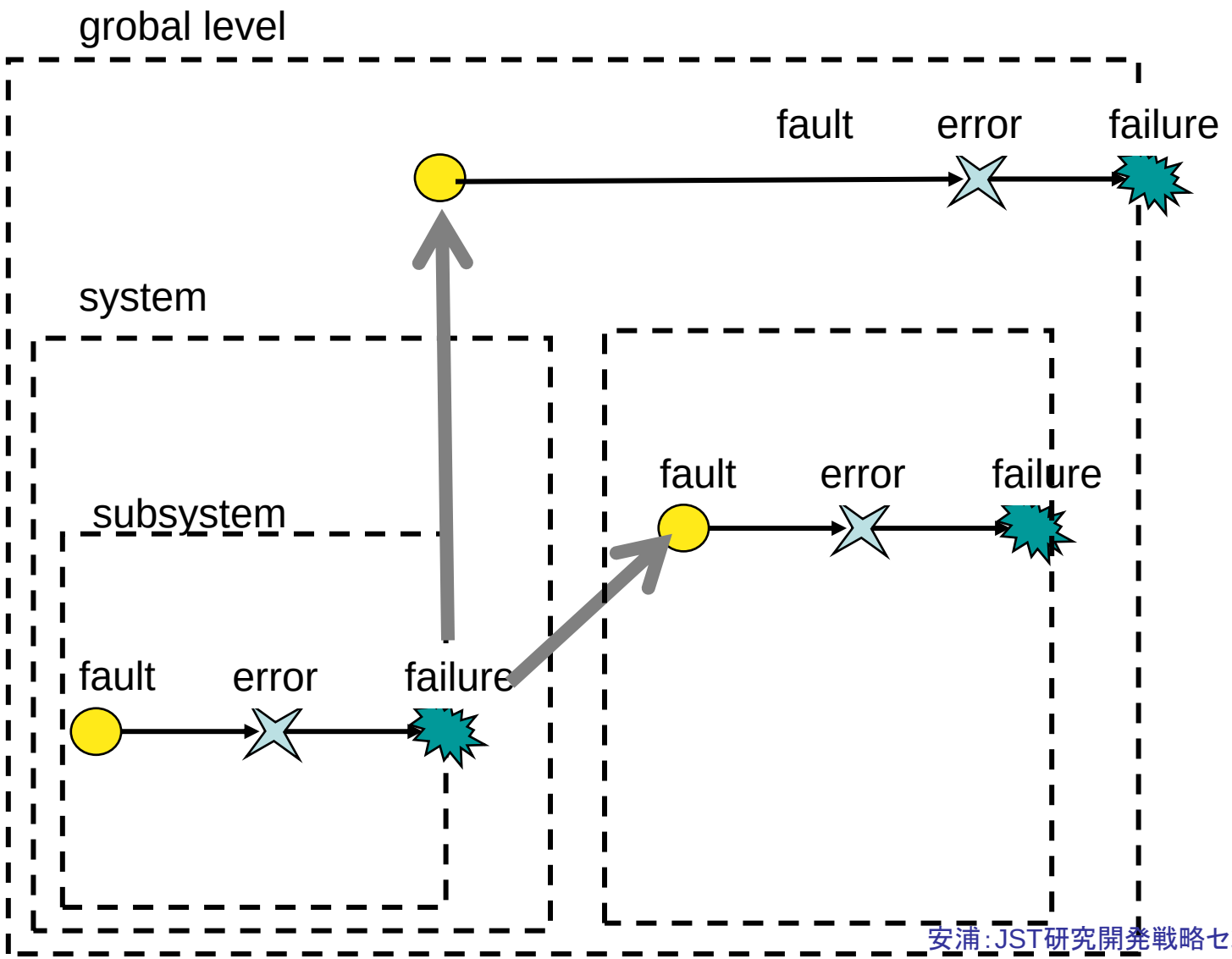
- Faultの多様化
  - 自然現象中心から人間の誤りや攻撃によるものへ
- FaultとFailureの関係の多様化
  - 階層を飛び越えた影響
  - 複数のFaultの組み合わせ効果
- Failureの定義の変化
  - システム仕様の動的な変化

Modern Fault Model: Faultの多様化



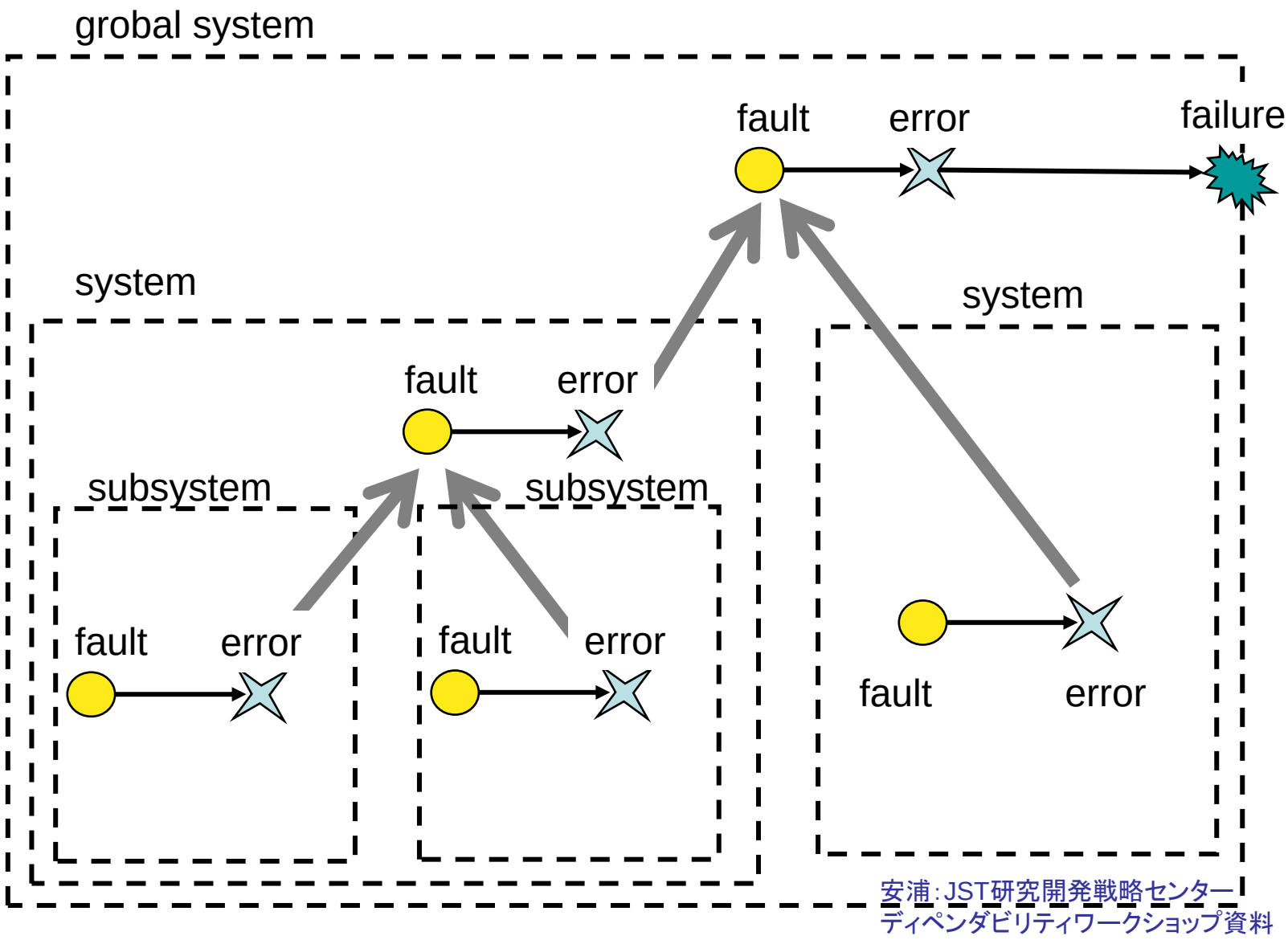
安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

Modern Fault Model:階層の透過



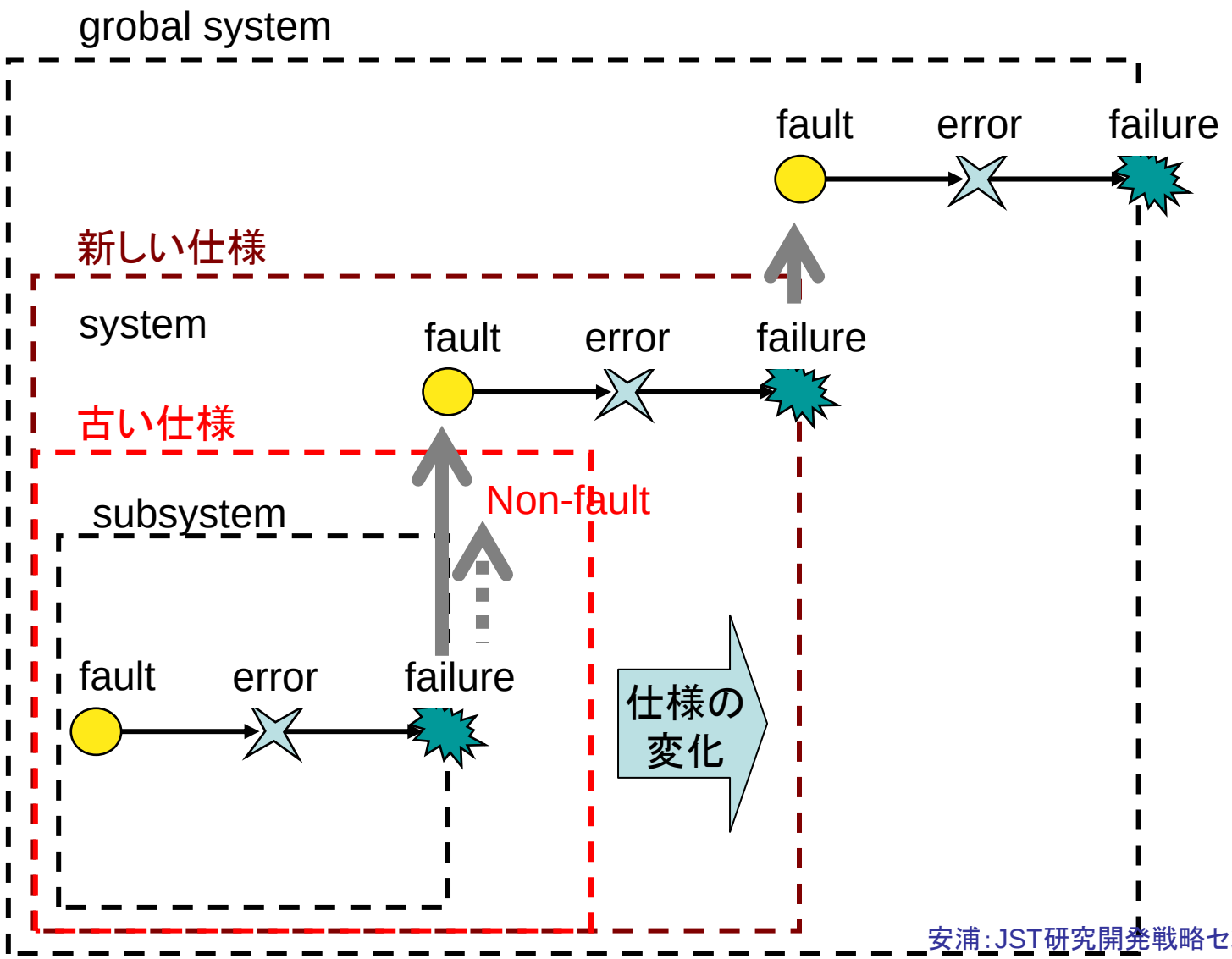
安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

Modern Fault Model:相互作用



安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

Modern Fault Model:仕様の変更



安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

Dependable VLSI

- 社会情報基盤としてのVLSI
- 技術的課題
- Dependabilityの概念
- Dependabilityを保証する技術
- 今後の展開

ディペンダビリティの実現手段

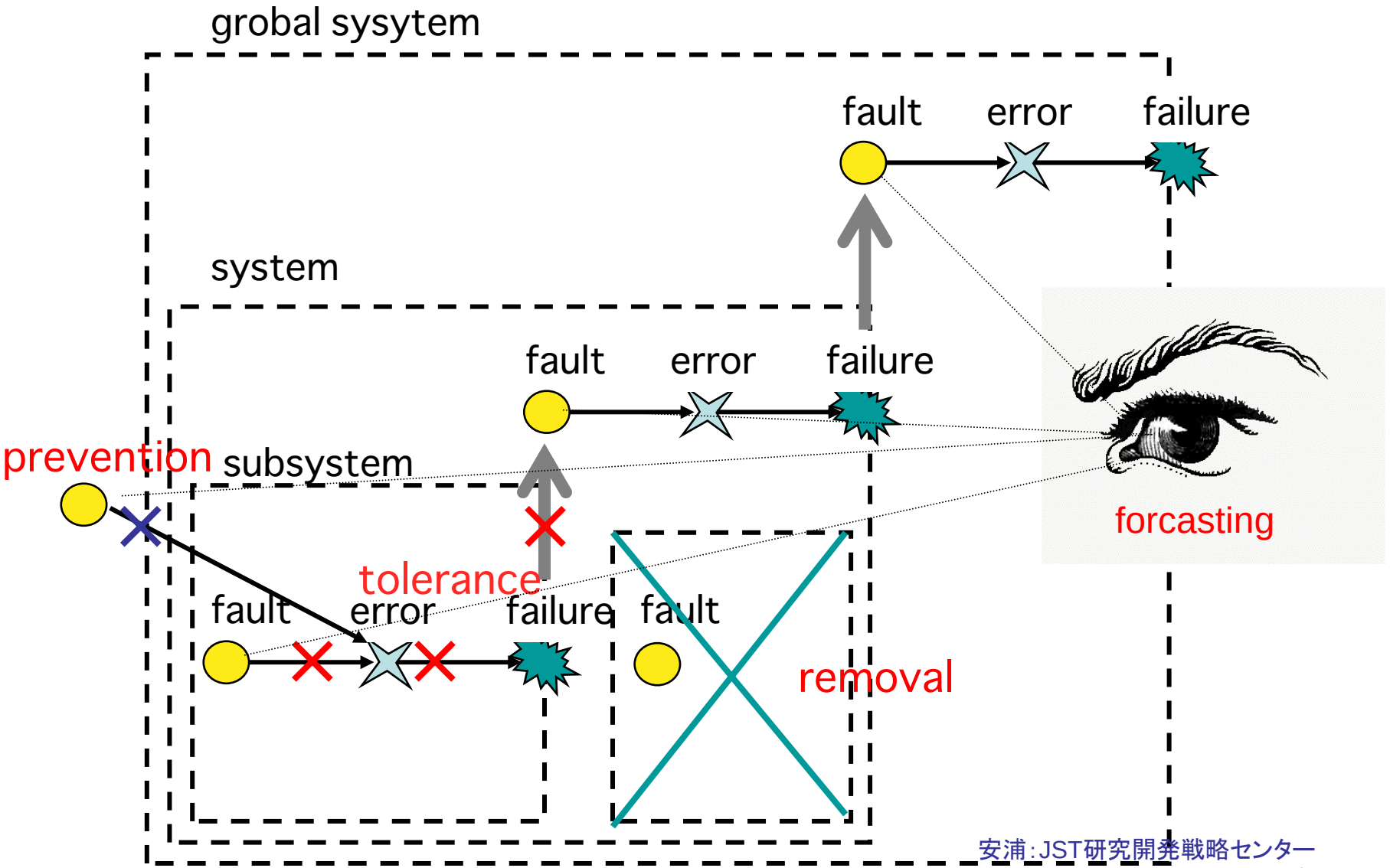
Fault prevention:
フォールトの発生や導入を予防する

Fault tolerance :
フォールトが生じても正しいサービスを提供する

Fault removal :
フォールトの数や程度を減少させる

Fault forecasting :
フォールトの現存数、影響を推定する

ディペンダビリティの実現手段



安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

阻害要因による分類

- 自然現象による脅威 (Natural Threat)
  - 自然界からの雑音
  - デバイスの故障・経年変化
  - 製造時の揺らぎ
- 人間活動（設計、製造、運用）におけるミス(Human Errors)
  - 設計や仕様上の誤り
  - 製造時の誤り
  - 運用上の誤り
- 悪意ある攻撃による脅威 (Human Attack)
  - 攻撃への耐性（設計時、製造時、運用時など）
  - 事故時の対応（波及の局所化、迅速な復旧）
  - 利用者の了解性、社会の受容環境
- 複数の要因の複合的効果
  - システム同士、システム対人、人同士のインタラクションに起因する不具合
  - 「仕様が規定できない」という本質的問題

安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

Life Cycle Stagesの視点

- Dependabilityに影響するLife Cycle Stages
  - 企画 (Planning)
  - 設計 (Design)
  - 製造 (Fabrication)
  - 検査 (Test)
  - 流通 (Distribution)
  - 運用 (Operation)
  - 廃棄・更新 (Abandonment/Replace)

人命にかかわる例（自動車用チップ）

	自然現象	人的ミス	人的攻撃
企画		仕様不備 寿命設定ミス	企画の盗難
設計		設計ミス、バグ 利用環境の想定ミス	設計の盗難
製造	製造ばらつき	製造ミス	
検査	間欠故障の見逃し	見逃し	不良品混入
流通	実装中の環境変化	不良・偽造品混入	偽造品混入
運用	経年変化、温度環境	利用事故 保守のミス	無線による攻撃
廃棄・更新		更新不整合	情報抜取

赤字：原因

安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

財産にかかわる例（電子マネー用チップ）

	自然現象	人的ミス	人的攻撃
企画		仕様不備 交換時への配慮不足	企画の盗難
設計		設計ミス、バグ 利用環境の想定ミス	設計の盗難 不正回路挿入
製造	製造ばらつき	製造ミス	違法な生産による 横流し
検査	間欠故障	見逃し	良品横流し
流通	運搬・保存中の 環境変化	運搬等の事故	盗難、横流し
運用	経年変化 宇宙線・環境	利用事故	Phishing、virus 盗聴、不正利用
廃棄・更新		更新時不整合	情報抜取・解析

赤字：原因

安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

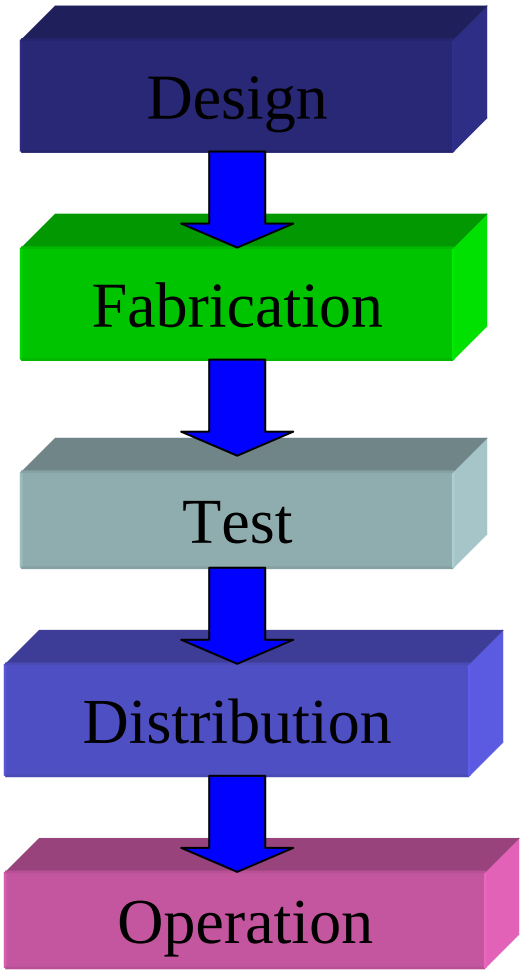
Dependability向上の対策

	自然現象	人的ミス	人的攻撃
企画	製品寿命の見積もり 環境変化の予測	仕様の完備 ライフサイクルの予測	機密保持 攻撃の予測
設計	耐故障設計、雑音対策 DFM、DFT モニタ機能の組込み 単純なアーキテクチャ	設計検証 設計品質管理 テスト容易化 製品の操作性向上	設計データ管理 耐タンパ設計 Security-on-Chip 製品管理の仕組
製造	製造ばらつきの制御	工程管理の徹底	製品管理の徹底
検査	テスト精度向上 悪環境下のテスト	工程管理、自己テスト テスト精度向上	製品管理の徹底 モニタリング
流通	環境の保全・管理	物流の管理	物流の管理 トレース技術
運用	環境モニタリング Online Self Test	利用履歴モニタリング 利用者教育	利用者教育 監視、攻撃対策
廃棄・更新	自殺、異常通知機能	自動消去機能	無効化

安浦：JST研究開発戦略センター
ディペンダビリティワークショップ資料

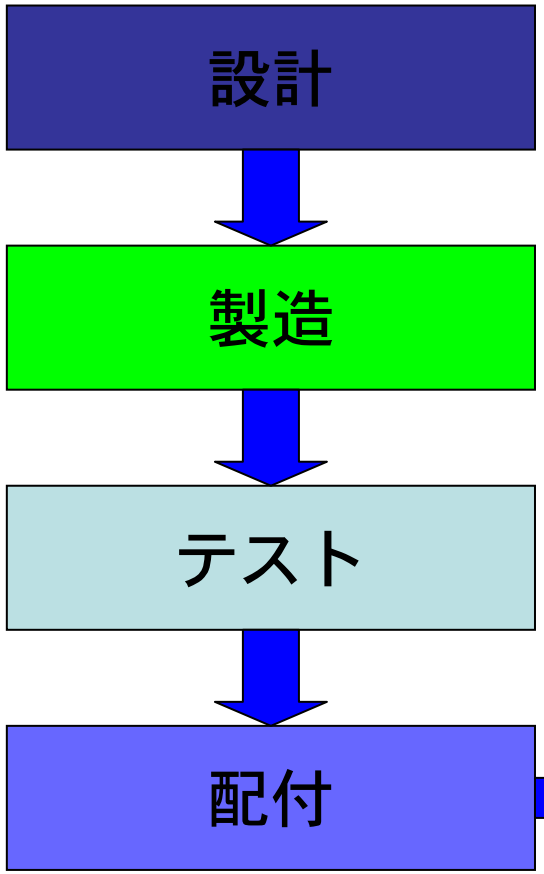
攻撃の可能性

- 設計データの漏洩・盗用
- EDAツールによる攻撃
  - スキャンパス自動挿入
  - 設計データの漏えい
  - 回路・レイアウトの変更
- チップの不正な増産
- テスト時の不正
  - 良品チップの横流し
  - テストデータや条件の漏洩
- パッケージなど後工程での盗難
- 搭載するソフトウェアからの攻撃
- 運用時の攻撃



技術的課題

特殊性の実現
材料
加工方法
機能・性能



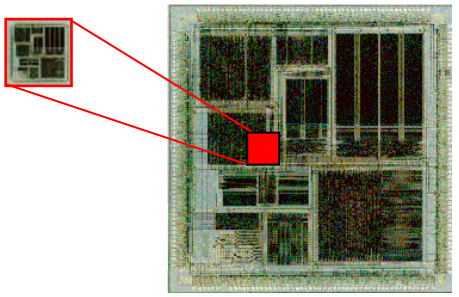
■特殊な設計・製造過程
- ●設計時の機密保持
- ●製造時の不正防止
- ●テスト時の不法行為防止
- ●配布時の盗難防止

■運用時の真贋性判定
- ●電子的・非電子的
- ●不正の検出機能

運用

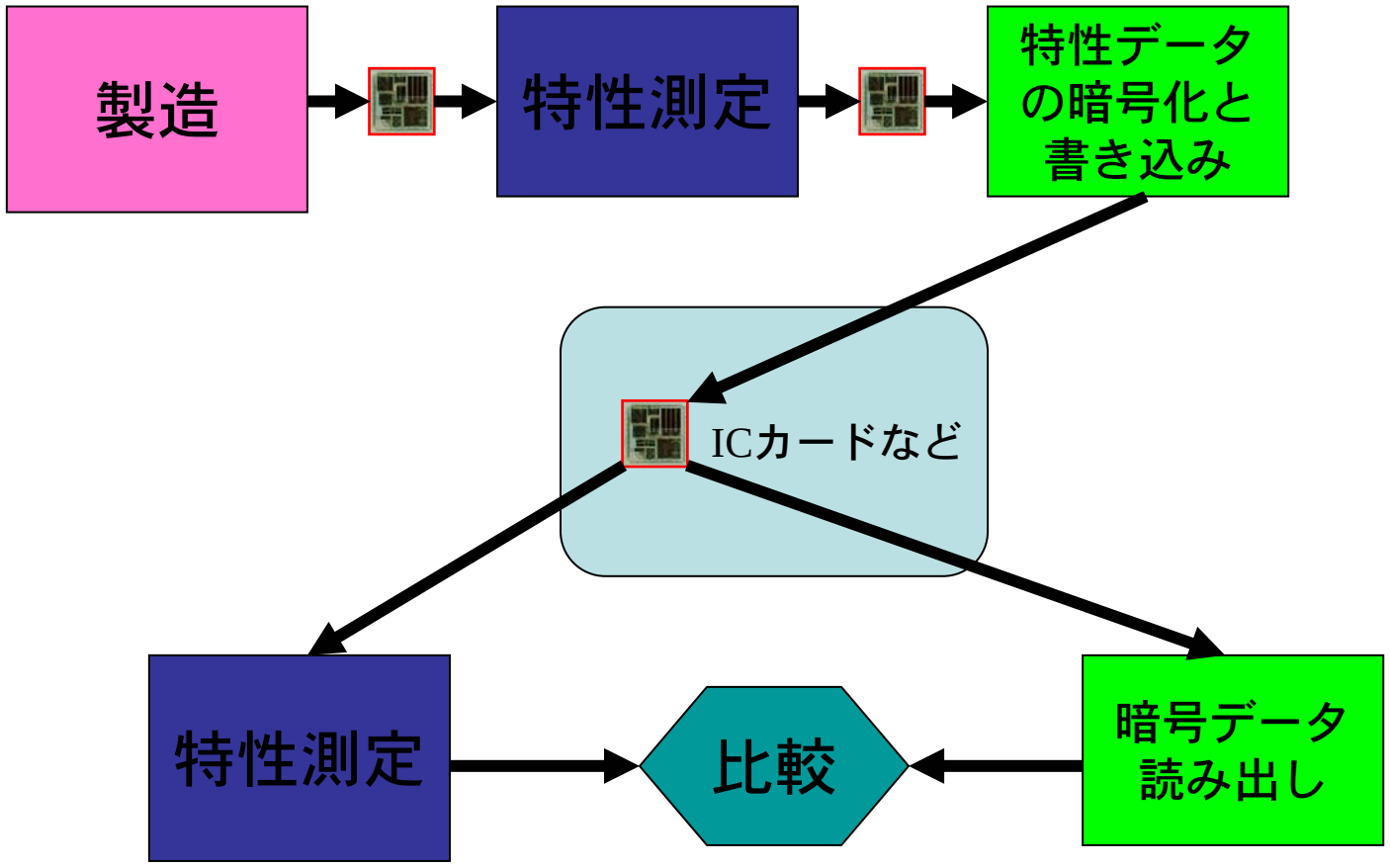
価値と信用を搭載するLSI

- 大半の機能は通常の半導体技術を使う(経済性)
- セキュリティに関する機能の部分だけを「特殊な方法」で設計・製造・テストする
- 付加価値の高いCoreとしてのSecurity Core
  - SWとして
  - IPとして
  - Chipとして(SiP技術の利用)
- 真贋性の判定方法
  - コストと有効性



Security Core

真贋性保証の例



新しいビジネスチャンス

- 半導体製造メーカー
  - 機密性の高い製造手法による製品への付加価値
  - 新しい応用分野（知財保護や信用取引）向け製品の開発
- 半導体製造機器メーカー
  - 特殊な製造装置と製造技術の開発
  - 一般端末における真贋判定機器への技術応用
- 半導体材料メーカー
  - 特殊な材料による安全性の確保
- マスクメーカー
  - 特殊なマスク技術の開発と安全管理技術の確立
- テスト機器メーカー
  - 耐タンパー性とテスト容易性を両立する技術
  - 一般端末における真贋判定機器への技術応用
- 設計ツールベンダー
  - 安全性の高い設計技術とそのためのツール
- 設計会社
  - 安全性を付加価値とするチップの製造技術
- システムメーカー
  - 価値や信用を搭載する機器の開発

Dependable VLSI

- 社会情報基盤としてのVLSI
- 技術的課題
- Dependabilityの概念
- Dependabilityを保証する技術
- 今後の展開

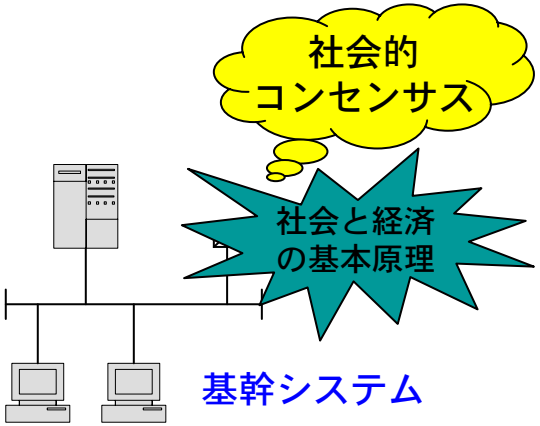
Dependable XXXが流れに

- VLSI / ハードウェアデバイス
- オペレーティングシステム
- 組込みソフトウェア
- 通信システム
- 社会情報基盤
- サービス

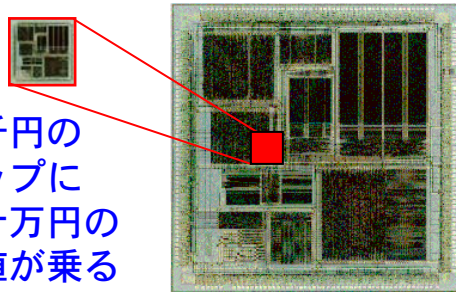
- 品質、信頼性、安全性

社会情報基盤の確立と社会システムの構築

—「価値」と「信用」を取り扱う情報技術と社会基盤—



Security Core Chip



社会システムレベル

社会システム（決済・徴税・証明システム）
法体系、経済システム、経営技術、利用技術
危機管理技術、ビジネスモデル

情報通信システムレベル

情報通信ネットワーク、情報システム
情報端末、信頼性技術
セキュリティ技術、プライバシー保護
基幹ソフトウェア技術、組込みSW開発技術

デバイス・集積回路レベル

システムLSI設計技術、高信頼化技術
設計、製造、テスト段階での偽造防止技術
高ディペンダビリティ技術、真贋性保証技術

最終目標：電子経済時代の通貨・徴税の仕組みの構築
経済システムの国家的安全保障

ディペンダブルな
社会情報基盤の開発への要求

- 数十年有効なグランドデザイン
- 社会の安定と安全を確保する仕組み
- 一般の人に分かりやすい原理
- 個人を守るためのシステム
- 地球環境に負担をかけないシステム
- 開発、運用、保守のコストと効率
- 技術の変化に対応した新しいシステムへのスムーズ

何ができるかより
どうあるべきかを考えることが重要