CRDS-FY2006-WR-07

ディペンダビリティワークショップ報告書

独立行政法人科学技術振興機構 研究開発戦略センター
Center for Research and Development Strategy Japan Science and Technology Agency

Executive Summary

独立行政法人科学技術振興機構（JST）研究開発センター（CRDS）では、科学技術に求められる社会的・経済的ニーズを踏まえて国として重点的に推進すべき研究領域や課題を選び、そのファンディング戦略を明確にするための活動を行っている。このような活動の一環として、重要研究テーマについて専門家による科学技術未来戦略ワークショップを開催している。

2005年に開催した「電子情報通信系俯瞰ワークショップII」において、「ディペンダビリティ」がキーワードのひとつとして議論され、これを軸に据えた幾つかの具体的なプロポーザルを検討している。今回のディペンダビリティワークショップは、まずディペンダビリティの基本概念についての合意形成を目的としており、今後開催予定の「ディペンダブルVLSI」、「ディペンダビリティ評価技術」、「ディペンダブルネットワーク」のディペンダビリティシリーズの源流と位置付けている。

本ワークショップの問題提起として、以下の6件の講演が行われた。

1. ディペンダビリティについて
2. ディペンダビリティの概念と課題
3. 情報通信ネットワークのディペンダビリティ
4. 社会サービスのディペンダビリティ
5. 自動車におけるディペンダビリティについて
6. 米国に於ける研究戦略動向（CITRISにおけるディペンダビリティ研究事例の紹介）

さらに、これを受けてグループ討議では、ディペンダビリティの概念整理、およびディペンダビリティに関する重要研究分野の提言という2つの課題について討論を行った。

本ワークショップで議論された結果として、ディペンダビリティとは、ユーザ視点の概念であり、予測不可能性（想定外事象）を秘めた系において広義のサービスレベルが保証されること、また、その度合いであるという定義が挙げられた。また、具体的な研究開発課題として以下が挙げられた。

■ IT技術課題

- 人間も含めた社会全体の安全性、安定性を漸近的に保証するための技術体系
- Metricsの確立
- Virtually Dependable Systemの概念の確立
- Virtual Isolationの概念の確立
- SLAのコンフリクトマネジメント

- サービス、セキュリティ、プライバシーの三律背反への対応
- 長期的な問題列挙と解決策の議論
- 定義からの逸脱の評価・検出
- Dependability の実現モデル
- 暗黙知を形式知にする技術の確立
- 仕様を作る技術
- システム全体（HW/SW）を把握する技術の研究
- CPU アーキテクチャ、FTIC 技術、最適化
- 多様性の必要性に関する提案

■ 社会技術課題

- 社会システムの再構築に関する議論
- Dependability の社会的・経済的価値
- インフラに対する課金の仕組み
- Liability の保証のしくみ
- 参照システムの特定と比較する方法
- Human Error を前提とするシステム設計技術
- ユーザ教育、普及活動

さらに具体的な推進方法として以下が挙げられた。

- Grand Challenge の提示
- Real な実験場（Dependable City/Campus の構築）
- ソサイアティの構築
- 失敗例の蓄積
- 大規模国家プロジェクト

本ワークショップでの議論を踏まえ、ディペンダビリティを軸にした具体的な戦略プロポーザルに反映させていく予定である。

CONTENTS

1

本ワークショップの位置づけ

独立行政法人科学技術振興機構（JST）研究開発センター（CRDS）では、科学技術に求められる社会的・経済的ニーズを踏まえて国として重点的に推進すべき研究領域や課題を選び、そのファンディング戦略を明確にするための活動を行っている。このような活動の一環として、重要研究テーマについて専門家による科学技術未来戦略ワークショップを開催している。

2005年9月29-30日にかずさアークで開催された「電子情報通信系俯瞰ワークショップII」※において、「ディペンダビリティ」がキーワードのひとつとして議論され、これを軸に据えた幾つかの具体的なプロポーザルを検討している。今回のディペンダビリティワークショップは、図1.1に示すように、まずディペンダビリティの基本概念についての合意形成を目的としており、今後開催予定の「ディペンダブルVLSI」、「ディペンダビリティ評価技術」、「ディペンダブルネットワーク」のディペンダビリティシリーズの源流と位置付けている。

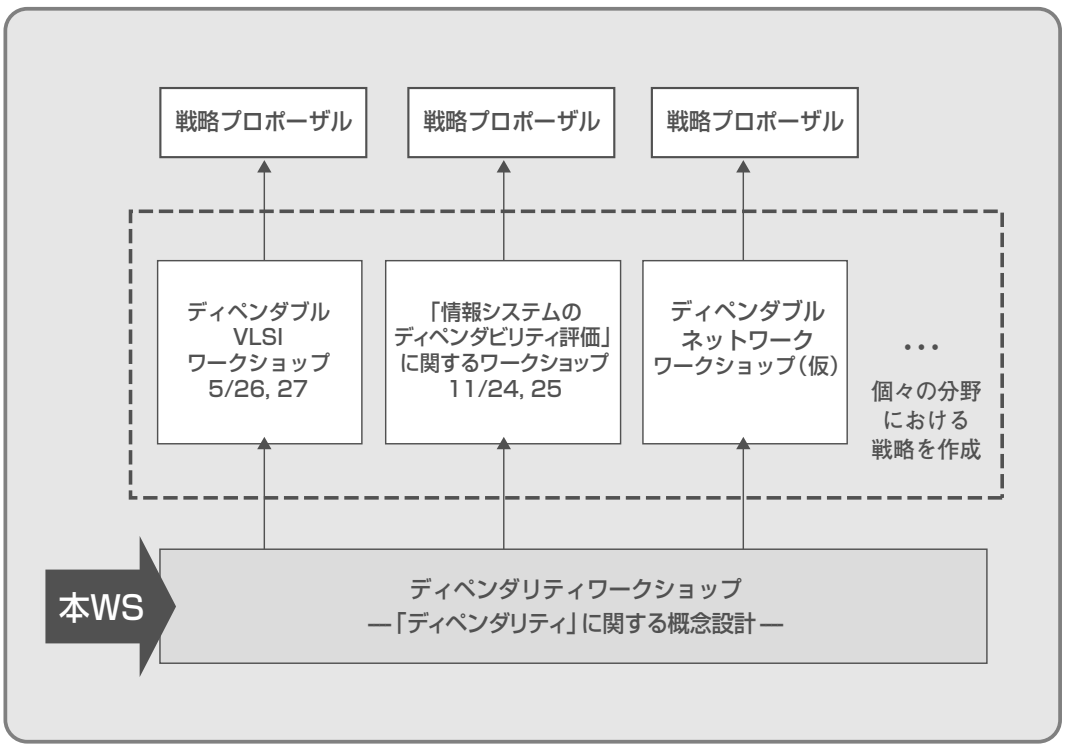


図1.1 ワークショップの位置づけ

※ 科学技術未来戦略ワークショップ（電子情報通信系俯瞰WS II）
報告書 CRDS-FY 2005-WR-16（2006）

（ワークショップの構成）

本ワークショップは以下に示すように3つのセッションで構成した（プログラムは付録参照）。
第1部：ディペンダビリティについて6件の講演による問題提起
第2部：2つの課題を設定して3グループに分かれて討議
　　課題1：ディペンダビリティの概念整理
　　課題2：ディペンダビリティに関する重要研究分野の提言
第3部：グループ討議結果の発表と全体討議

なお、このワークショップに先立ってディペンダビリティに関する事前アンケートを実施した。アンケート結果のまとめについては、付録参照。

2

ディペンダビリティへの問題提起

本ワークショップのテーマである「ディペンダビリティ」への問題提起として、以下の6件の講演が行われた。

- ディペンダビリティについて‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥安浦 寛人（九州大学）
  ディペンダビリティというテーマを、幅広い視点で眺め、どんな問題があるかを提起。
- ディペンダビリティの概念と課題‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥南谷 崇（東京大学, CRDS）
  ディペンダビリティの研究コミュニティでこれまでどういうことがなされており、これから何をしなければいけないか。
- 情報通信ネットワークのディペンダビリティ‥‥‥‥‥‥‥‥‥‥‥‥‥‥市川 晴久（NTT）
  情報通信分野におけるディペンダビリティの話題。
- 社会サービスのディペンダビリティ‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥岩野和生（日本IBM）
  サービスという観点から今どういう取り組みをやっているのか、その観点から考えたときのディペンダビリティの新しい側面。
- 自動車におけるディペンダビリティについて‥‥‥‥‥‥‥‥服部雅之（トヨタ自動車）
  社会に与える影響が大きいシステムとしての自動車における電子技術を中心とした設計の課題。
- 米国に於ける研究戦略動向（CITRISにおけるディペンダビリティ研究事例の紹介）‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥井上隆秀（UCB CITRIS）
  ベンチマークの題材として、米国カリフォルニア大学の中にある研究機構CITRIS（Center for IT Research on Interest of the Society）の紹介。

Dependabilityについて

安浦寛人
九州大学システムLSI研究センター

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とは

- 偶然、過失、悪意の攻撃によって生じる不具合に対して、システムの安心・安全を確保できる性質
- IFIP WG10.4などで議論
- 人々がその生命、財産、プライバシーなどを安心して委ねられるシステムへの要求

ー＞より広く深い議論

（南谷先生資料、アンケートまとめ参照）

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な情報通信システム

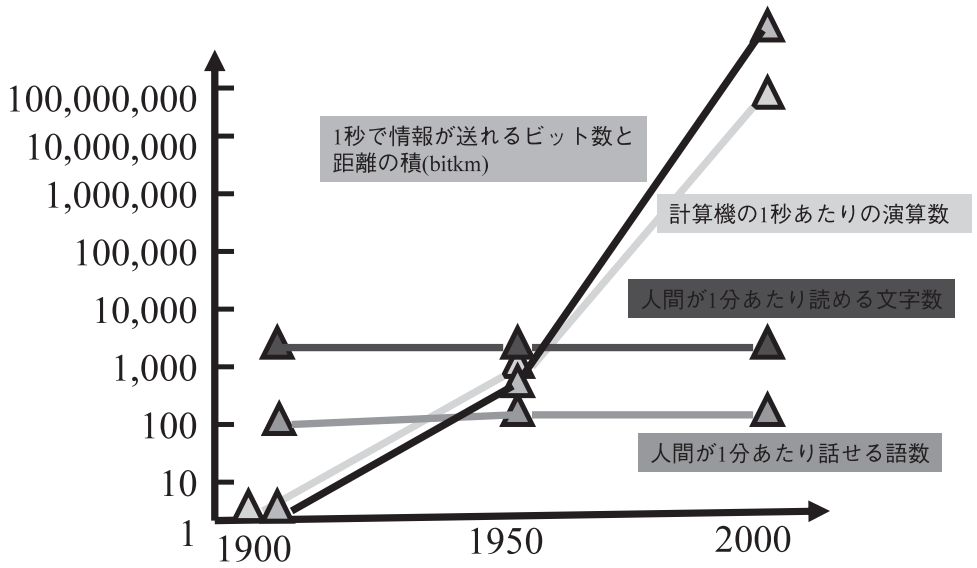
- 情報通信システムは社会の神経系である。
- 誰が何にDependするのか？
  - Systemが部品やDeviceにDependする。
  - 人や社会がSystemにdependする。
    - 何を守るのか？＝＞Life（人命）、Property（財産）、Privacy
  - Dependability Chainの明確化
- SystemがDependableでなくなる原因は？
  - 自然現象による脅威
  - 人間活動（設計、製造、運用）における誤りやミス
  - 悪意ある攻撃による脅威
  - システム同士、システム一人、人同士のインタラクションに起因する不具合
  - 規定できない「仕様」
- SystemのLife Cycleの中での脅威の位置づけ
- 設計者、製造者、販売者、運用者の責任の明確化

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

社会の神経系としての情報通信システム

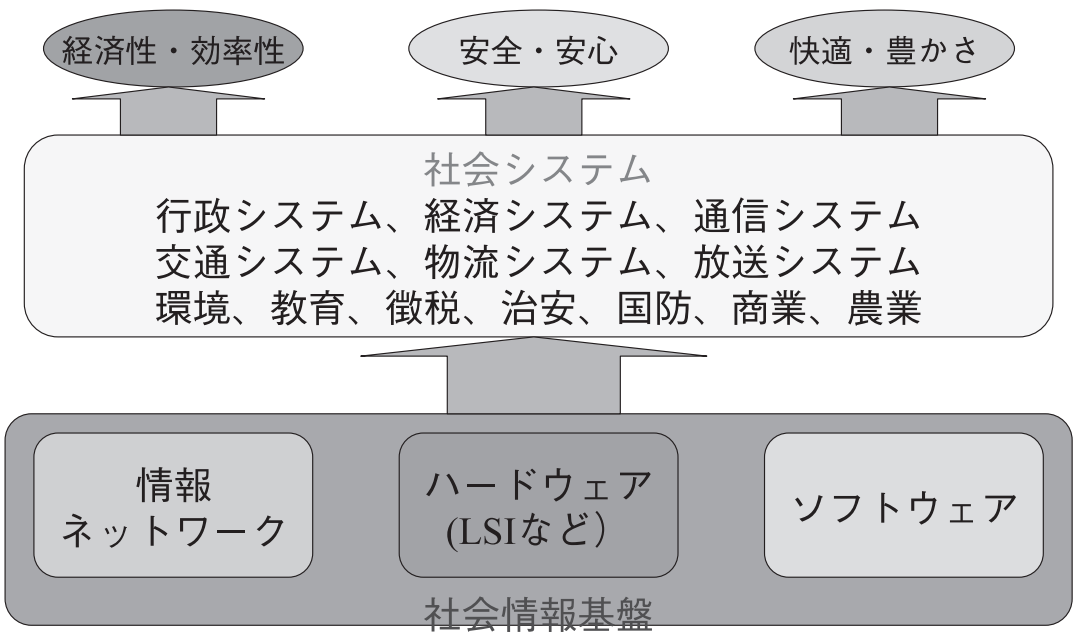
- 20世紀後半は既存の社会システムの中に情報通信技術を部分的に導入し、サービスの高度化、高速化を進める時代であった。
- 通信速度、情報処理速度の向上は、システムの設計時に想定しなかった事態を生み出すようになった。
- 21世紀は情報通信技術を前提として社会システム自身を再設計する時代。
  - 社会情報基盤(Social Information Infrastructure)
  - ユビキタス社会、e-Japan、u-Japan

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

社会情報基盤の構築

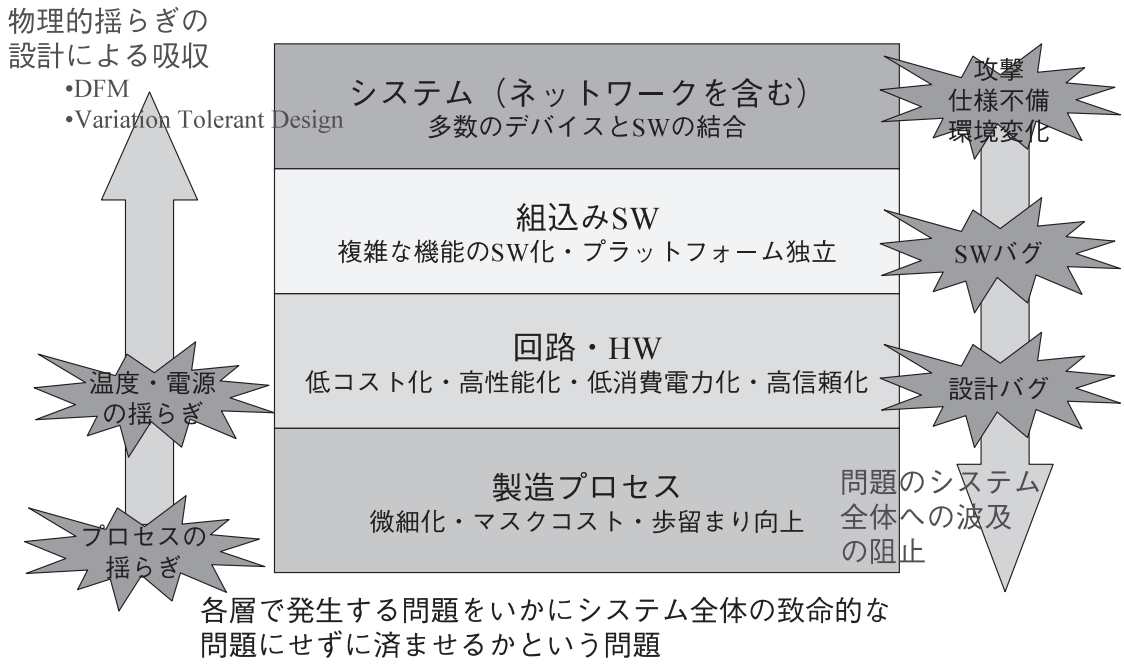


何が問題か？

- 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
- 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



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

仕様が作れないシステム

- これまでのシステム設計は、「仕様」によって規定されていた（社会とシステム・設計・製造のインタフェース）
- 仕様が作れなくなった原因
  - システム境界の不明確化
    - ネットワークによる接続
    - 出荷後のソフトウェアのダウンロード
    - 時々刻々変化する外部環境
  - 技術の変化と拡大の速さ
    - 検証されない技術の更新
    - 大局が見えにくい局所的技術競争
  - 技術や規格のブラックボックス化
- 仕様からポリシーへ
  - 環境の変化への柔軟かつ即時的対応
  - 想定範囲の拡大
  - 責任の明確化（誰の責任か？運用者、設計者、許認可権限者）
  - 保険システムの変革（動的なリスク管理）

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

社会システムの開発への要求

- 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な移行

何ができるかより
どうあるべきかを考えることが重要

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

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、システム一人、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

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

- 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 (Abandonment)

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

携帯電話用チップの例

	自然現象	人的ミス	人的攻撃
企画	製品寿命	仕様不備	企画の盗難
設計	耐故障設計 自己修復機能	設計ミス、バグ	設計の盗難 特殊回路挿入
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	見逃し率	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		情報の未消去	情報抜取

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

電子マネーの例

価値の量（大きさ）と保存則の保証

2,000 年

1,000年

金属貨幣
価値の量：物質（金属）
価値の保存則：物質保存則

紙幣
価値の量：情報（印刷）
価値の保存則：物質（紙）

電子マネー ？
価値の量：情報
価値の保存則：情報

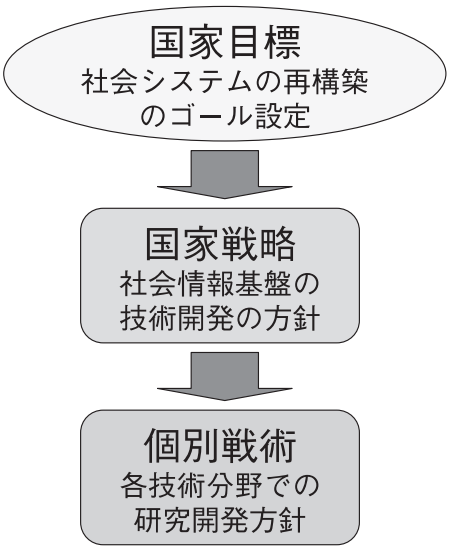
完全なコピーが可能な
情報で価値が保存できるか？

ICカードは財布か貨幣か？

- 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
  - 偽物は許されない
  - 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？
  - 技術的、制度的な問題が山積
- 電子マネーは現金貨幣の電子的実現といえるか？
  - 別の制度として社会が受容したほうがdependableではないか？

何が求められているのか？

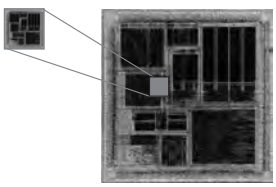
- 新しい情報通信技術と方法論
  - 社会や個人がDependableな社会システムの構築手法とその要素技術としての情報通信技術
  - 社会制度や規則と連携した社会システムの再構築への技術側からの参画
- 社会システムの再構築を担う人材の育成



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

「価値」と「信用」を委ねられる Dependable社会システムの構築

Security Core Chip



社会システムレベル
社会システム（決済・徴税・認証システム）
制度、法体系、経済システム、通信ネットワーク

デバイスレベル
携帯電話・ICカードなど個人用デバイス
バックエンドの発行・運用情報システム
セキュリティ技術（暗号）、プライバシー保護
仕様作成、組込みSW開発、危機管理技術

チップレベル
高信頼性、長寿命、低消費電力、自己修復
設計、製造、テスト段階での偽造防止技術
Secure Coreの分離、真贋性保証技術
「価値」や「信用」を載せられる集積回路の技術

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

ディペンダビリイティ・ワークショップ 2006.5.12-13

ディペンダビリティの概念と課題

南谷　崇

科学技術振興機構

研究開発戦略センター

ディペンダビリティ＝安心・安全

「提供されるサービスが正確で信頼がおける」
というコンピューティングシステムの性質
＝＞　安心・安全な社会と生活を支える情報基盤
子供の遊びから国家安全保障まで！

概念と定義

- IFIP WG10.4 “Dependable Computing and Fault Tolerance” (1980 ~　)
- A.Avizienis, J.-C. Laprie, B.Randel, C.Landwehr: ”Basic concepts and taxonomy of dependable and secure computing”, IEEE Trans. on dependable and secure computing. Vol.1. No.1 (Jan. - March 2004)

VLSI技術微細化によるリスク

- *半導体集積回路技術の微細化が、信頼性、安全性にとって深刻な問題！*

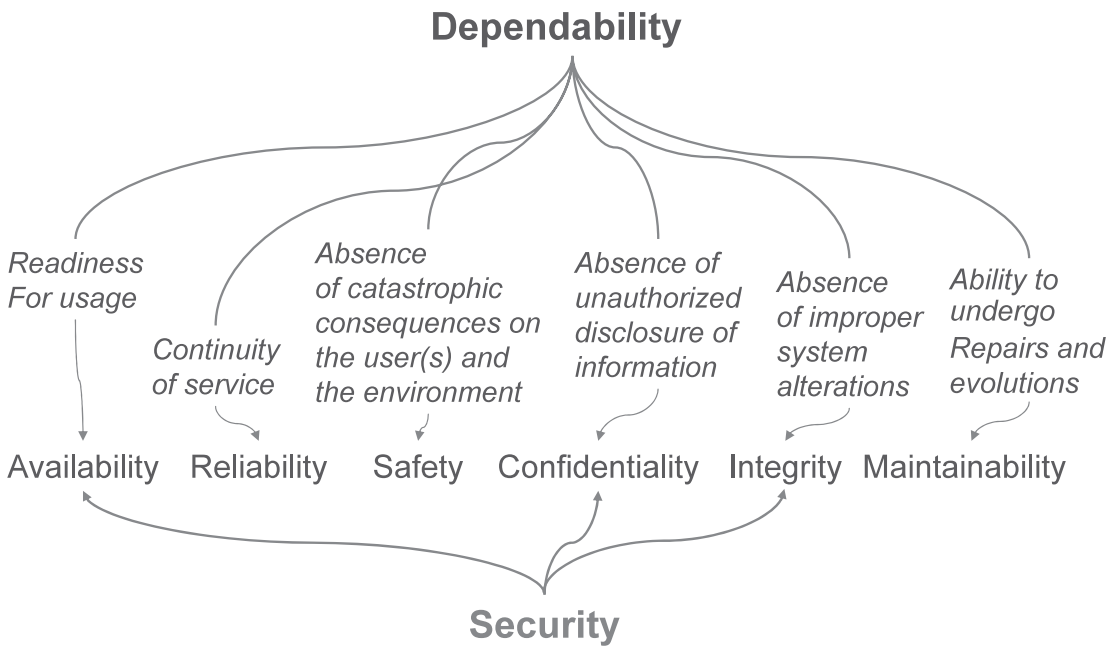
- リーク電流：トランジスタのしきい値電圧を下げることによるサブスレッショールドリーク電流に加えて、ゲート絶縁膜が薄くなることによるゲートリーク電流の急激な増加。
- PVT変動：プロセスパラメータ(P)の変動、電源電圧(V)の変動、温度(T)の変動。
- ソフトエラー：宇宙線が大気と反応して生成される中性子線などによって引き起こされるメモリビット反転や論理誤動作
- クロストーク：配線幅が縮小して配線間カップリング容量が増加することに よ る信号変形、遅延変動
- IRドロップ：電源線の抵抗成分による電圧降下が信号の安定性を毀損

- *10年後に1チップ1000億オントランジスタが搭載されるとすると、そのうち20%はPVT変動などで動作せず、10%は動作中に故障し、残りの70%は常にソフトエラーの脅威に晒される状況を想定する必要があるとの指摘がある！*

ネットワーク社会が直面するリスク

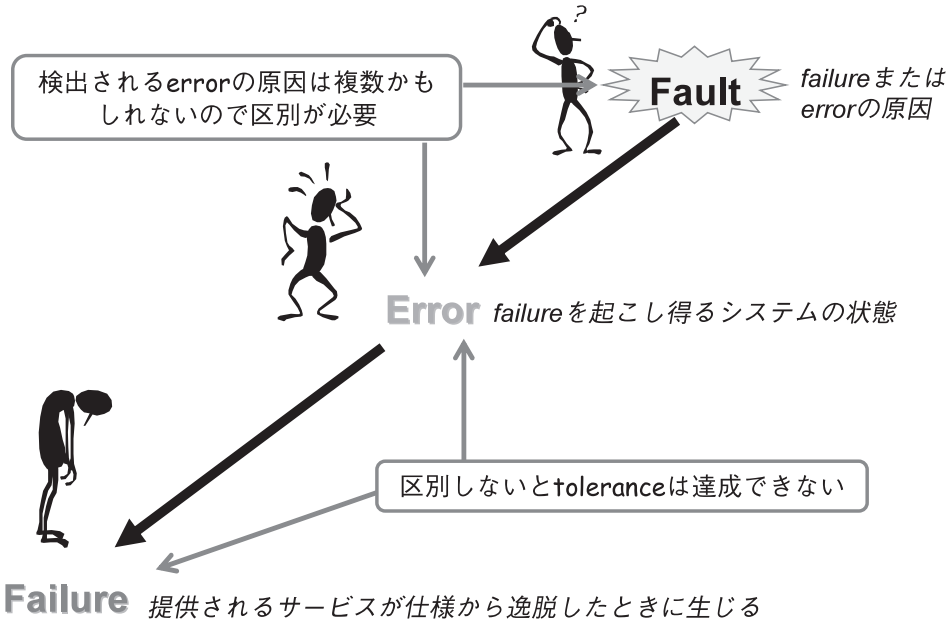
- ブラックボックス化:　個人、社会のすべてが依存しているのに誰もシステムの全容を把握できず、その事実すら外から見えない
- システムの複雑化：　仕様の不明確化、システム経年劣化などで、複雑に絡み合ったシステム同士、人間とシステムの予期せぬ相互作用が人知れず発生
- 情報量の大規模化：　世界中で毎日大量に生産され続ける巨大な情報量が国境を越えて蓄積、流通、処理
- 利用の多様化：　経験のない無邪気なユーザーも悪意を持った練達のユーザーもアクセス可能。人為フォールトの可能性がユビキタスに存在
- 責任所在の不明確化：　ネットワークは、互いに独立に設計された巨大な数のシステムのシステムであり、明確に定義されていない

•Dependability: ability to deliver service that can justifiably be trusted
•Service delivered by a system: its behavior as is perceived by its user(s)
•User:another system that interacts with the former
•Function of a system:what the system is intended to do
•(Functional) Specification: description of the system function
•Correct service: when the delivered service implements the system function
•System failure: event that occurs when the delivered service deviates from correct service, either because the system does not comply with the specification, or because the specification did not adequately describe its function
•Failure modes: the ways in which a system can fail, ranked according to failure severity
•Dependability: ability to avoid failures that are more frequent or more severe than is acceptable to the user(s)
•When failures are more frequent or more severe than acceptable:
meta-failure, I.e. a dependability failure

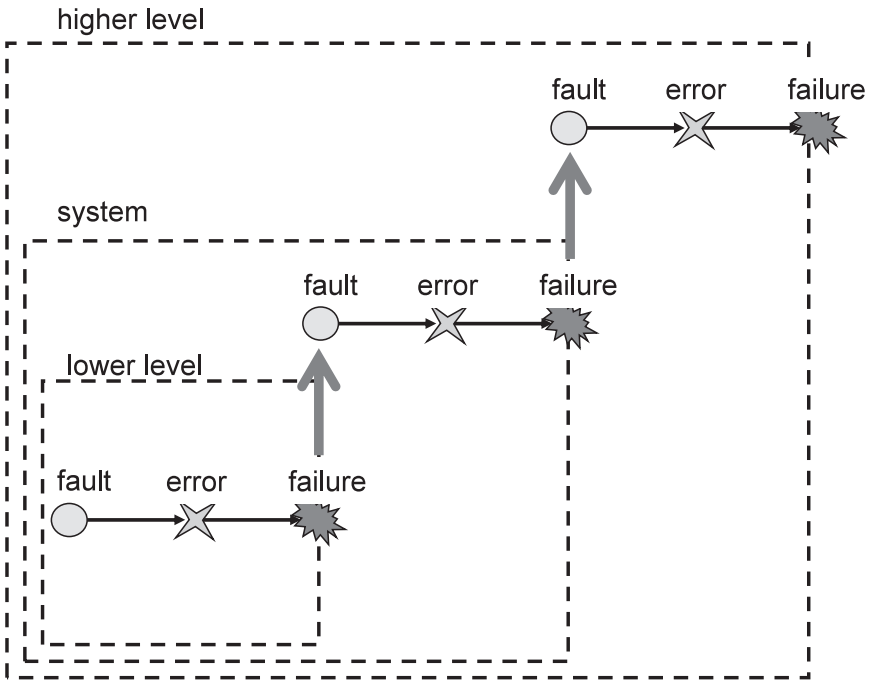


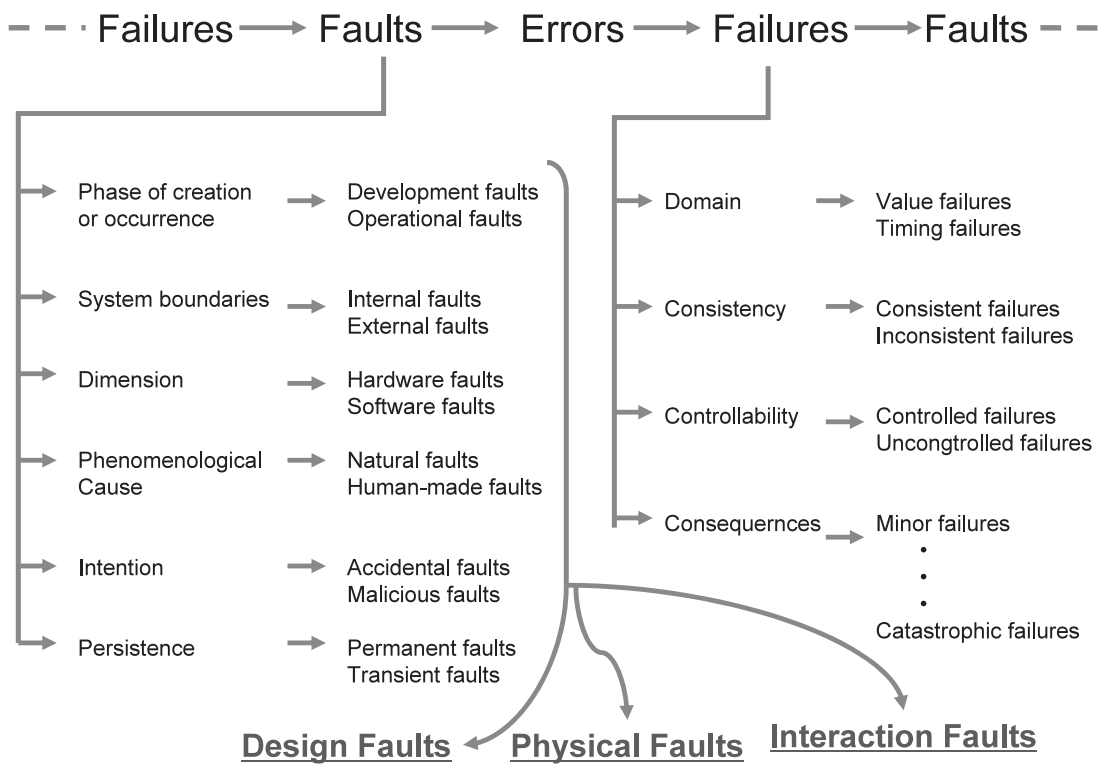
Absence of unauthorized access to, or handling of , system state

Dependability 阻害要因の因果関係

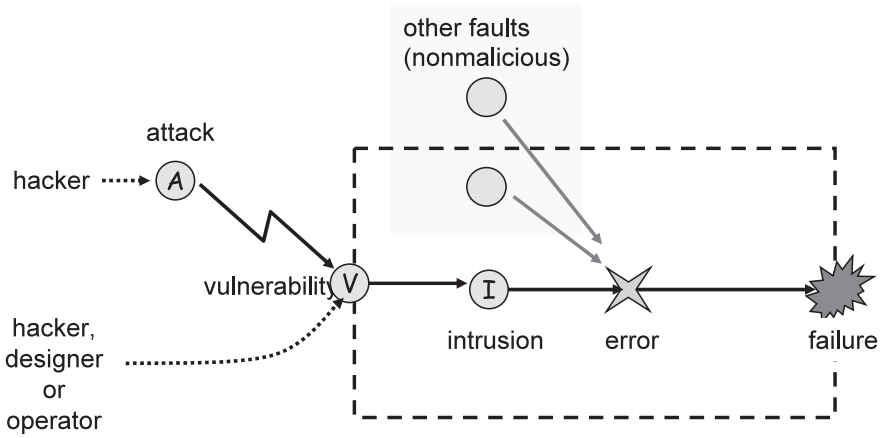


Fault Model: Recursion





Fault & Intrusion



- **attack** - malicious external activity aiming to intentionally violate one or more security properties; an *intrusion* attempt
- **vulnerability** - a malicious or non-malicious fault, in the requirements, the specification, the design or the configuration of the system, or in the way it is used, that could be exploited to create an *intrusion*
- **intrusion** - a malicious interaction fault resulting from an *attack* that has been successful in exploiting a *vulnerability*

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水準

- サービス品質：ディペンダビリティとパフォーマンス
- 要求仕様：Service Level Agreement
  - 望ましい（正常な）品質レベル
  - 許容できる品質レベル
  - 許容不可
- フォールトトレランスの段階
  - 1) 狭義のフォールトトレランス：要素にフォールトが発生してもシステムとしては所望の品質レベルのサービスを維持
  - 2) 漸次縮退(graceful degradation)：1)を維持できなくなったら、許容レベルまでサービス品質を漸次縮退する
  - 3) フェイルセイフ（フェイルストップ）：2)を維持できなくなリサービス品質が許容レベル以下になったらシステムを安全側の状態へ固定する＝＞最後の手段

フォールトトレランスの実現原理

- 「冗長性」と「分散性」
  - 冗長性がなければ誤り検出もフォールトマスクもできない
  - その冗長性がフォールトの影響範囲に集中したのでは効果がない
- 冗長性の形態
  - 空間：多重化、反復配列など
  - 時間：再試行、交番論理、マルチスレディングなど
  - 情報：誤り検出訂正符号、システム不変量、シグネチャーなど
  - 仕様の解釈：アナログ値、ファジー値、許容精度など
  - 問題の表現：ニューラルネットによる最適化問題、多重符号状態割り当てなど

どのような形態の冗長性をどのように実現するか？

フォールトトレランス要素技術

- *対象とするフォールトモデルの明確化が必要！*

- フォールトの局限化：波及範囲の限定＝＞上位システムへの影響防止
- 誤り検出：２重化、語の符号化、系列の符号化、時間監視、 ”I’m alive”、Heart Beat、一貫性／合理性チェック、評価尺度はCoverageとLatency
- フォールトマスク：多重化、誤り訂正符号、フォールトマスク論理、時間冗長
- 再試行：過渡的フォールトに効果
- 診断：マイクロプログラム診断、システムレベル診断、ビザンチン合意など、永久的フォールトの同定に必要
- システム再構成：動的２重化、動的冗長系、超並列など、予備要素へ切り替え、システムから切り離し
- システム回復：チェックポイント設定、ファイルバックアップ、情報分散
- 再起動：最後の手段

現状(1)

- 第３期科学技術基本計画スタート
  ＝＞「安心・安全」は科学技術が目指すべき普遍的理念、国家目標

- 高度情報化社会、ネットワーク社会において
  - 情報通信技術そのものにおける安全・安心の確保
  - 情報通信技術を活用した安全・安心の確保

- 安心・安全な情報化社会の実現を脅かす要因：
  - VLSI技術の微細化（リーク電流、ソフトエラー、PVT変動）
  - システムの複雑化（仕様の不明確、設計ミス、経年劣化、
  - ネットワーク利用の多様化（大量情報、サイバーテロ、相互作用）

- フォールト（障害の原因）
  - 物理的なフォールト(physical faults)
  - 人為的なフォールト（悪意および無意識）(human-made faults)
  - 相互作用によるフォールト(interaction faults)

現状(2)

- 物理的フォールト
- 長年の研究で積み上げられた膨大な知的資産
  - 概念、理論、実現手法、評価手法、ツールなど

- 人為的フォールト（悪意、過失）、設計フォールト、相互作用フォールトなどは今後の課題

- IFIP WGでディペンダビリティ・ベンチマーキングの活動開始

- VLSI微細化に起因する物理的フォールトのリスク

- システムの複雑化に起因する（無意識的）人為フォールトのリスク
  - メガバンクのシステム障害、東証のシステム停止

- 悪意ある人為フォールトに起因するサービス停止、情報漏洩
  - 不正アクセス、コンピュータ・ウイルス、DoS攻撃など

ディペンダビリティの技術課題

- 間欠的なハードウェアフォールト（ソフトエラー）
- 大規模システムの設計・運用
- 大量情報の処理
- 人間とコンピュータの相互作用
  - ウィルス、サイバーテロ、予期せぬ相互依存

- 仕様技術／Service Level Agreement
- 厳密な設計技術（仕様記述を含む）
- 検証技術
- フォールトトレランス技術（人為的、相互作用）
- ディペンダビリティ評価技術（ベンチマーク）
- ディペンダビリティ基準とSLA保証

今後： サービスのディペンダビリティ

- 地球規模ですべての「もの」と「こと」がネットワークを介して接続。その多くは過渡的、予測不能、また望ましくない接続である可能性
- ディペンダビリティを脅かす多くの事象は、そのようなネットワークにおける制御不能かつ予測不能な、人と人、人とシステム、システムとシステムの間の相互作用から生じる

従って、

- ディペンダビリティ研究の対象は、単なる情報システムではなく、人間を含み、情報技術を基盤とした社会システム
- ディペンダビリティの評価は、そのような社会システムで提供される「サービス」に対してなされなければならない。
- そのときの重要課題は、サービス・ディペンダビリティの評価尺度と測定法の開発

ディペンダビリティ研究のレベル

- 第１レベル：個人、企業、国家の活動が依存する情報システムのディペンダビリティ。コンピュータ科学、情報通信工学、システム工学の研究対象。
- 第２レベル：人間とシステムの相互作用を含む広義の（人間系を含む）情報システムのディペンダビリティ。上記の分野に加えて、認知科学、心理学、生物学、数学などが必要。サービスサイエンスはこのレベル。
- 第３レベル：情報システムを前提に構築される組織、制度、施設などのディペンダビリティ。上記に加えて、さらに社会学、法律学、経済学、政治学などが必要。
- 第４レベル：提供されるサービスの評価に際してその価値観に文化、習俗、宗教などが関わる場合があるが、これらは対象外？

分野共通の課題

- ディペンダビリティ評価尺度の定義と測定方法の確立
- ディペンダビリティ基準の標準化と経済価値化
- 基準達成へ向けた技術開発の促進
- 要求仕様／SLA保証の技術、制度
- サービス・ディペンダビリティ
- 人為的フォールト、相互作用フォールトのモデル化

各分野の研究課題例(1)

- 1）エレクトロニクス・フォトニクス分野
- 五感／体内情報センサー
- 環境情報センサー
- 給電デバイス
- 再構成可能デバイス
- 非可逆的デバイス
- セルフチェッキングデバイス

- 2）コンピューティング分野
- ディペンダビリティ評価／ベンチマーキング
- 人為的フォールトに対するトレランス技術
- 情報システムのセキュリティ
- 大規模ソフトウェア／システムの設計・検証
- 分散・並列処理のディペンダビリティ
- 実時間／組込みシステムのディペンダビリティ
- データ管理／データ工学

各分野の研究課題例(2)

- 3）ネットワーク分野
- 情報通信セキュリティ
- ネットワーク自己診断、修復
- ネットワーク の相互作用モデリング
- ネットワークの責任所在

- 4）ロボティクス分野
- 制御のディペンダビリティ
- 計測のディペンダビリティ
- 機構・作用のディペンダビリティ
- ディペンダビリティの対人モデリング

- 5）社会サービス分野
- 社会インフラ応用／ビジネス応用／産業応用のディペンダビリティ
- 安全工学／人間工学／心理学
- ディペンダビリティ教育／情報倫理
- 標準化／ガイドライン／認証
- 損害保険

ディペンダビリティーワークショップ

情報通信ネットワークのディペンダビリティ

2006年5月12日

NTT先端技術総合研究所

市川　晴久

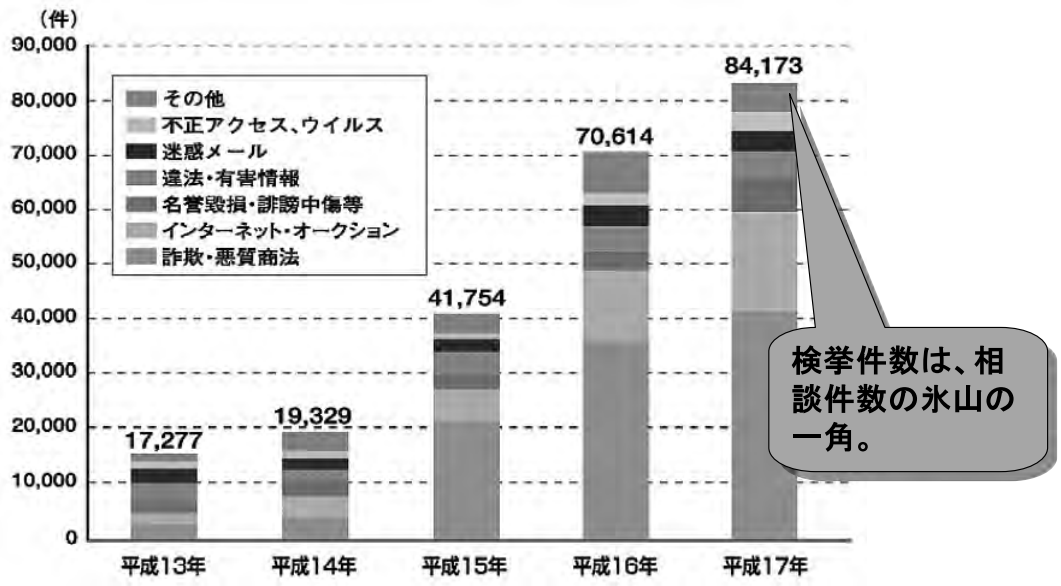
概要

- ディペンダブルインターネットへの取り組みの現状
- ネットワークの一色化の流れとディペンダビリティに対するリスクの増大
- 電話網の安心・安全設計に学ぶ
- 多色なネットワーク／アプライアンス・デファインド・ユビキタス・ネットワークの提案

インターネット利用で話題にのぼる被害例

- 情報漏えい
  - プライバシ（個人情報）問題　⇒組織（企業など）の責務
  - 企業機密漏洩による経済的損失
- サービス停止
  - ウィルス、DDoS攻撃などの企業ITシステムの被害による経済損失、社会活動の障害
- 情報改竄・詐欺
  - 不正請求
- 迷惑行為
  - SPAMメールなど

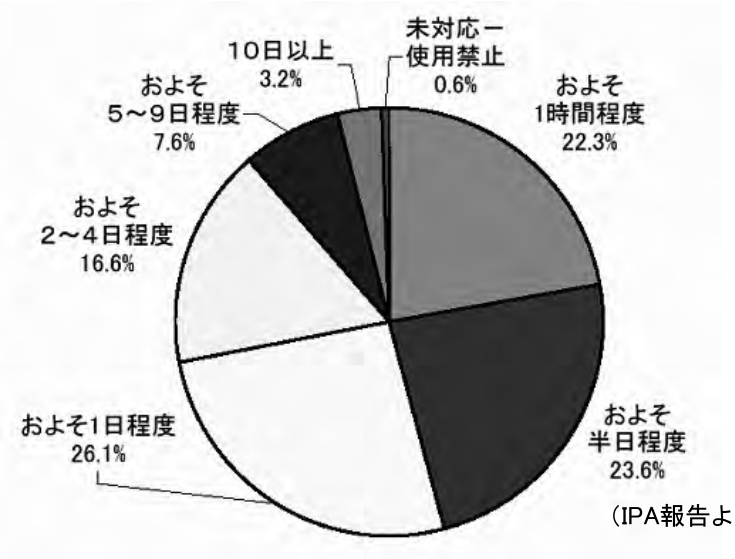
ハイテク犯罪に関する相談件数



出展：http://www.npa.go.jp/cyber/statics/index.html

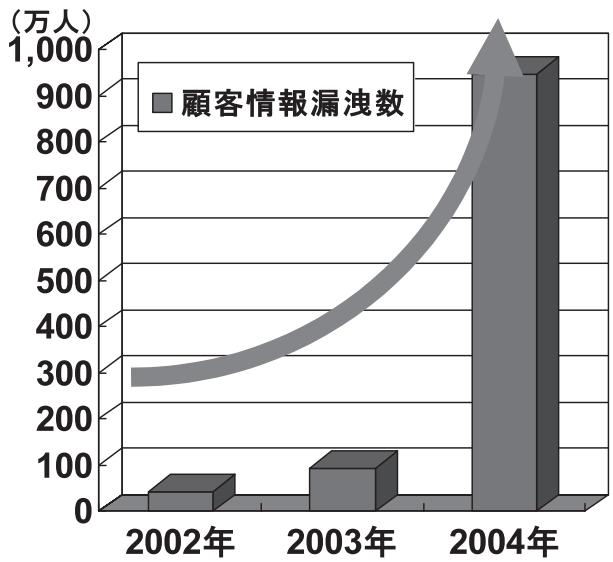
2003年に猛威をふるったMSブラストにおけるケーススタディ

回復に要する時間は、1日以上が半数を超える



（IPA報告より）

個人情報漏洩事件(人数)の増加と傾向



傾向

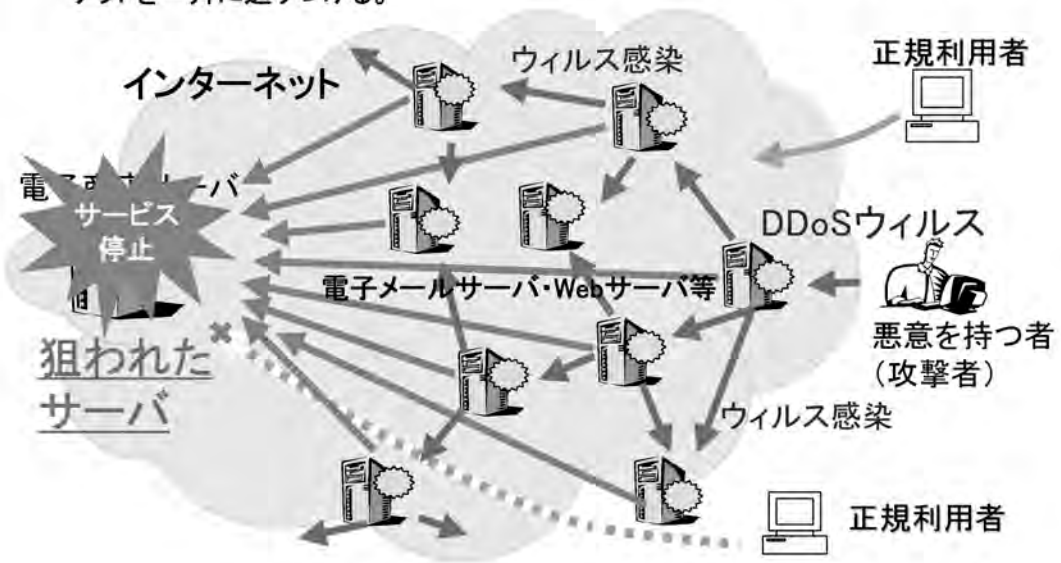
- NW,媒体利用による情報漏洩数の増加
- 機密情報（※）の漏洩増加
- ウィルス、P2Pソフト等の悪用

※基本4情報（氏名・生年月日・性別・住所）以外の口座番号、信用情報、クレジット番号等

参考：以下サイトに掲載の、1万人以上の情報漏洩を抜粋。
http://www.monthlyiso.net/SITE1PUB/sun/7/news/list1.html

分散サービス停止攻撃(DDoS攻撃)の脅威

ステップ1：世界中にある多数のサーバに(時限装置付の)DDoSウィルスを仕掛ける。
ステップ2：ウィルスを仕掛けられたサーバが、狙われたサーバに対して悪意の通信パケットを一斉に送りつける。



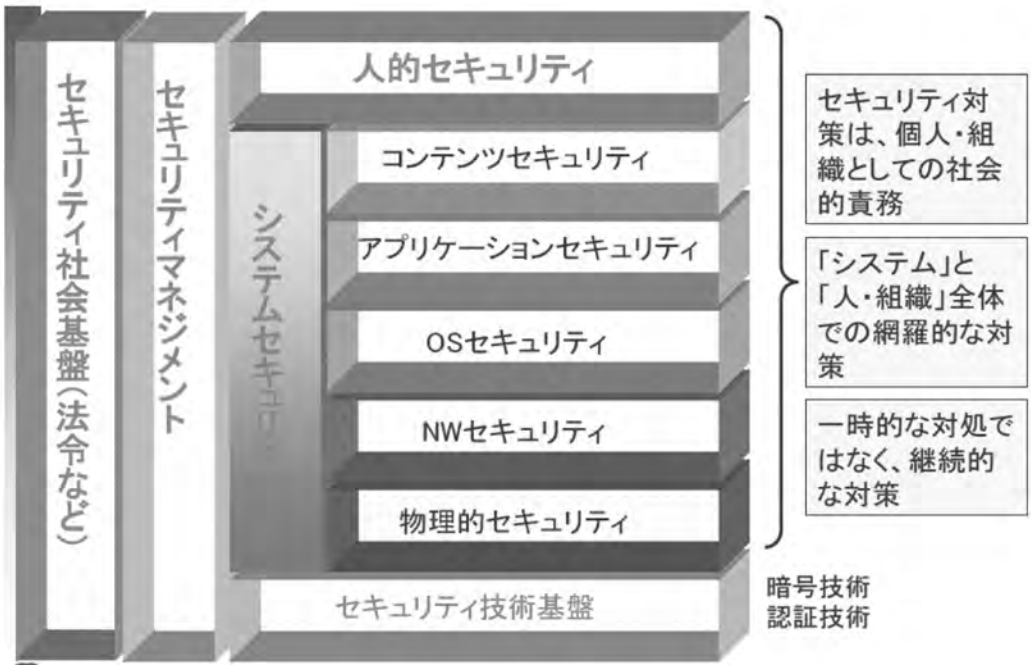
DDoS攻撃被害の現状

年	DDoS攻撃被害概要
2004	■Antinny によるコンピュータソフトウェア著作権協会 (accsjp)攻撃(現在) ■NetSkyによるDDoS対策に追われる企業 (4月) ■米国レコード工業会(RIAA) サーバダウン(3月) ■SCO、MSのサイトがMydoomにより麻痺(2月)
2003	■韓国のインターネットがSQL Slammerにより麻痺(1月)
2002	■社団法人コンピュータソフトウェア著作権協会のサイトに攻撃 (4月) ■DoS攻撃の実行とC:¥をフォーマットしてしまうSupovaワームが流布(7月) ■インターネットの基幹サーバをなす13台のルートサーバに攻撃(10月)
2001	■CIAに攻撃(5月) ■DoS攻撃ウイルス(CodeRed)が広域に蔓延(7月) ■文部科学省のWebサイトに攻撃(8月) ■The New York Timesのサイトに向けて大量のデータが送られる攻撃が発生(10月) ■カーネギーメロン大学のCERT(Computer Emergency Response Team) Coordination Centerに攻撃(12月)
2000	■米国YAHOO! (2月), 米国大手オークションサイトのeBay (2月) ■米国CNN(2月), 米国Amazon(2月)

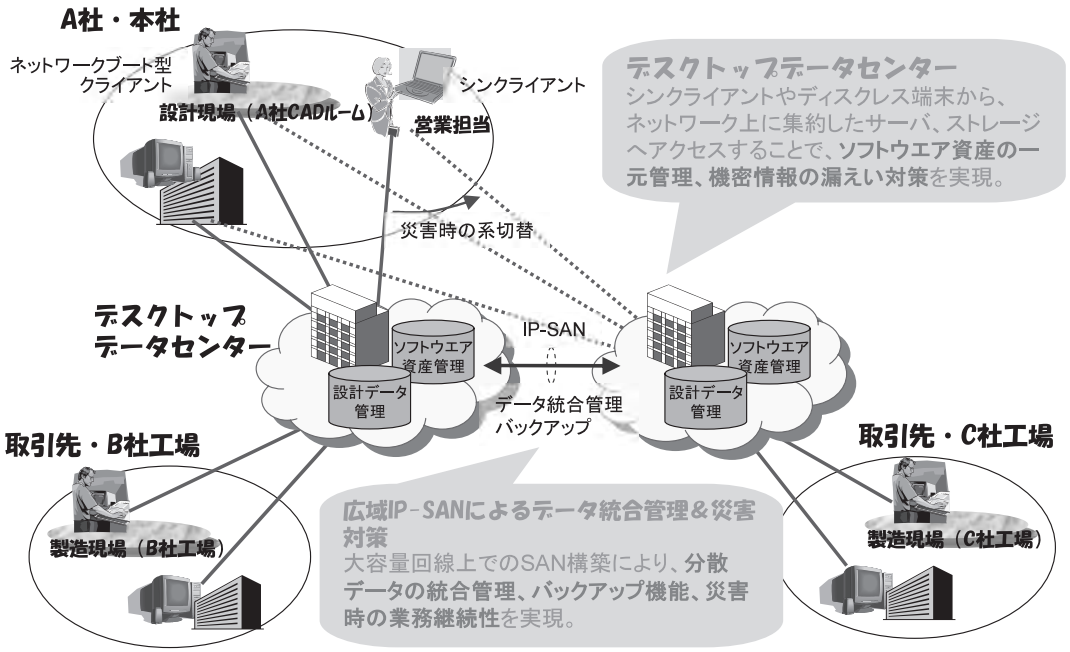
・約10時間麻痺状態
・ある通信販売サイトの売り上げ1／3

約12億ドルの経済的損失

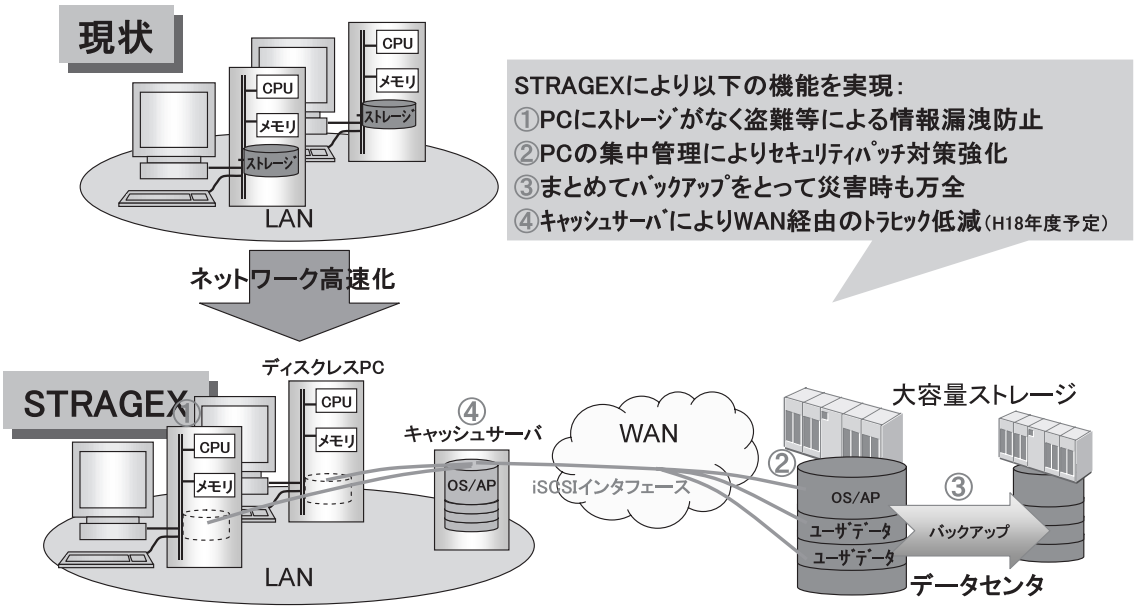
セキュリティ対策は総合ソリューション



ストレージ・セントレック構想

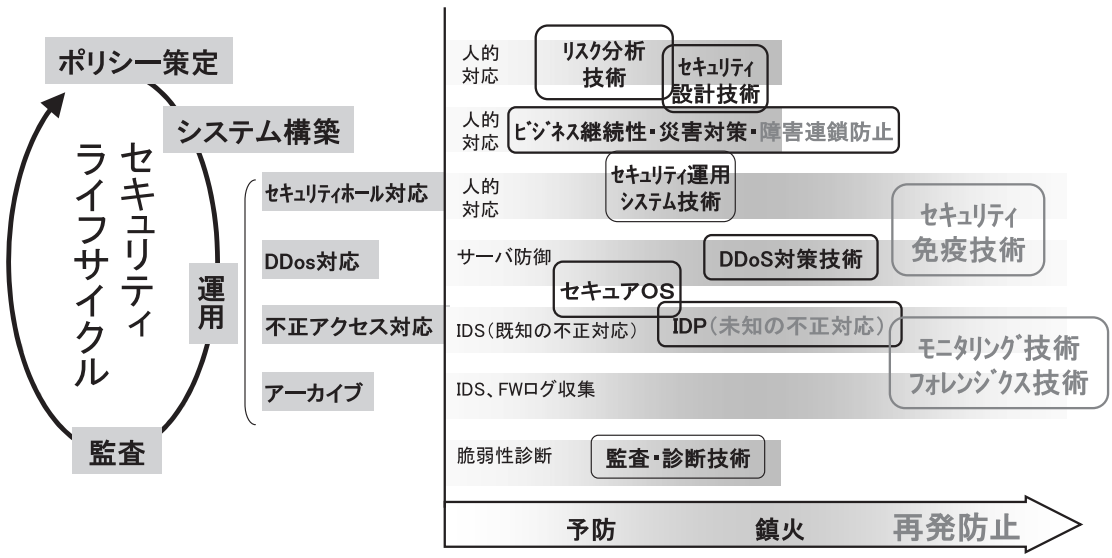


STRAGEXのご紹介



今後の方向性:再発防止技術

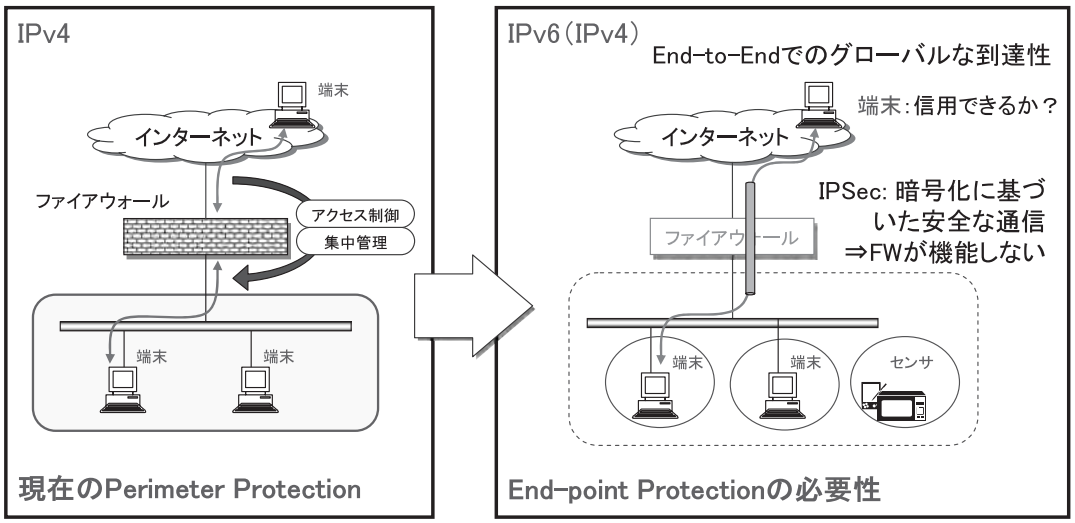
予防、鎮火から再発防止技術へ



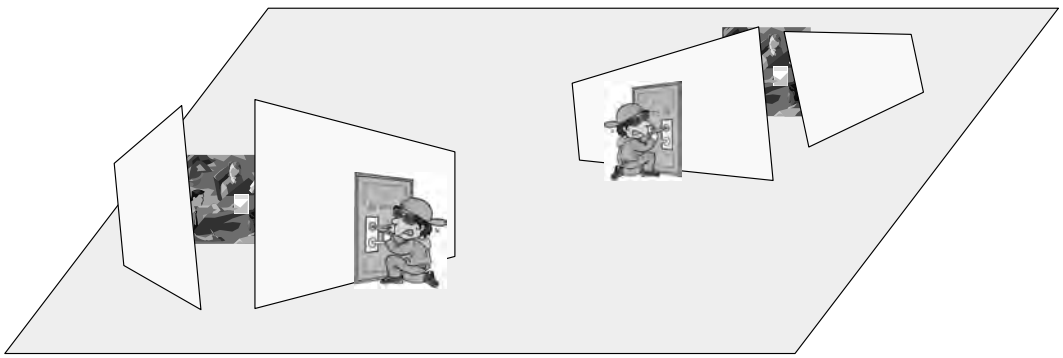
今後の方向性：End-point Protection

“Perimeter（境界線）Protection”の限界

- □ Mobile端末普及、port80への収斂 ⇒ ｱﾌﾟﾘｹｰｼｮﾝの脆弱性の課題
- □ VPNを介して端末が直接外界と通信

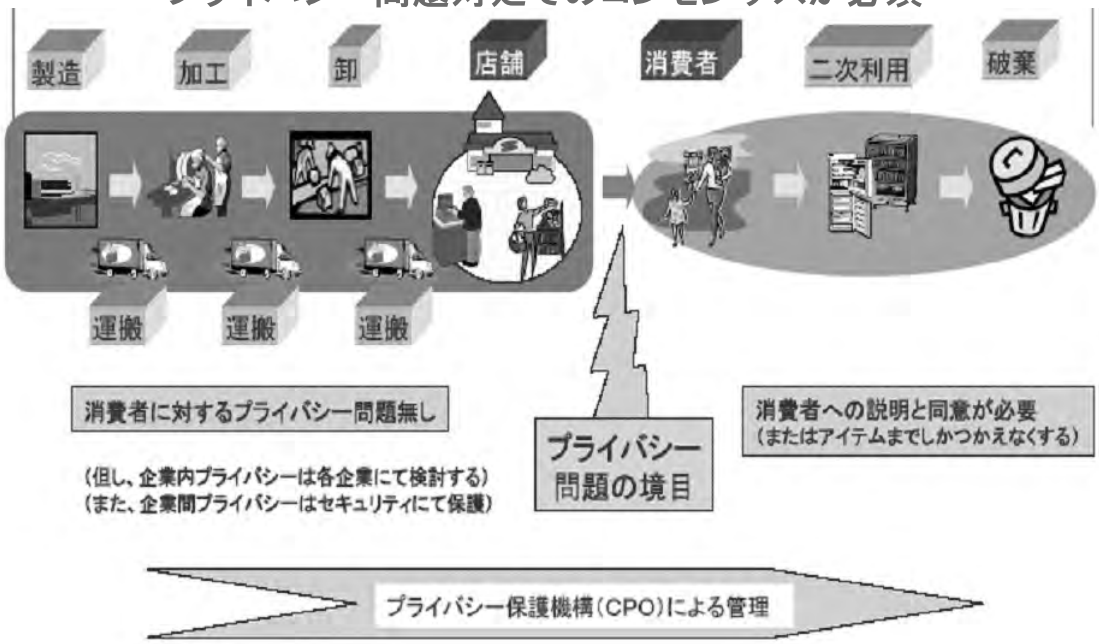


インターネット上でセキュアな「個室」を作るのは容易でない



電子タグのSCM適用:

プライバシー問題対処でのコンセンサスが必須



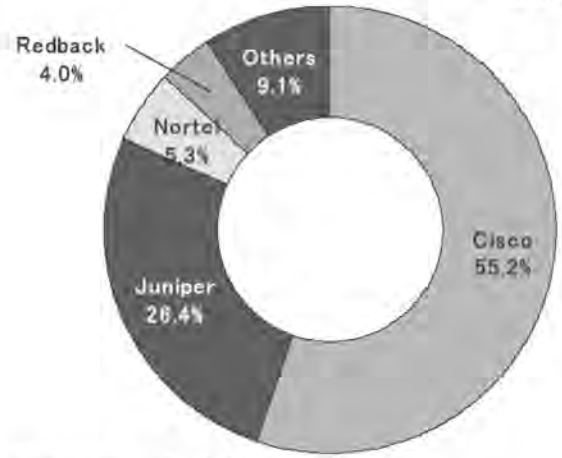
ユビキタスネットワーキングフォーラム　電子タグ高度利活用部会報告より

- ディペンダブルインターネットへの取り組みの現状
- **ネットワークの一色化の流れとディペンダビリティに対するリスクの増大**
- 電話網の安心・安全設計に学ぶ
- 多色なネットワーク／アプライアンス・デファインド・ユビキタス・ネットワークの提案

寡占状態にあるルータ市場

2003年　世界のルーター市場シェア（金額）

総務省の調査研究データより



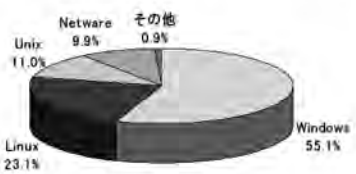
資料：ガートナー　データクエスト

URL：http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2004/2004-1-01-3.pdf

寡占化するサーバ・クライアントOS市場

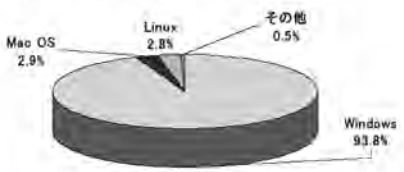
MSソフトの「単一栽培」とウィルス耐力について、賛否両論があるが、、
**　米国国土安全保障省は予防措置として、リナックスやUNIXの導入を拡大する方針**

2002年世界のサーバーOS市場シェア（本数）

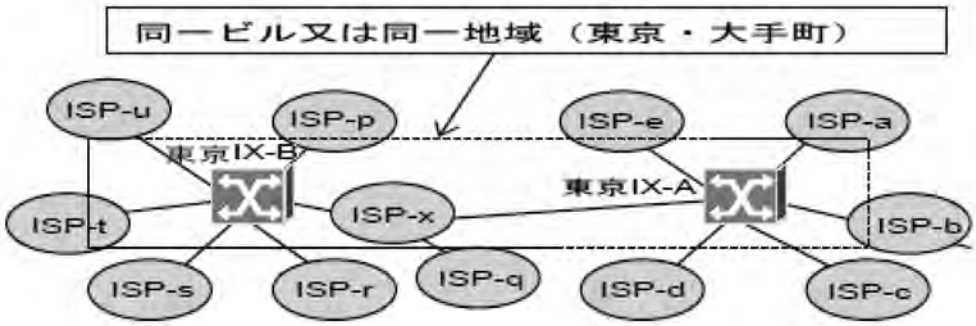


資料：米IDC

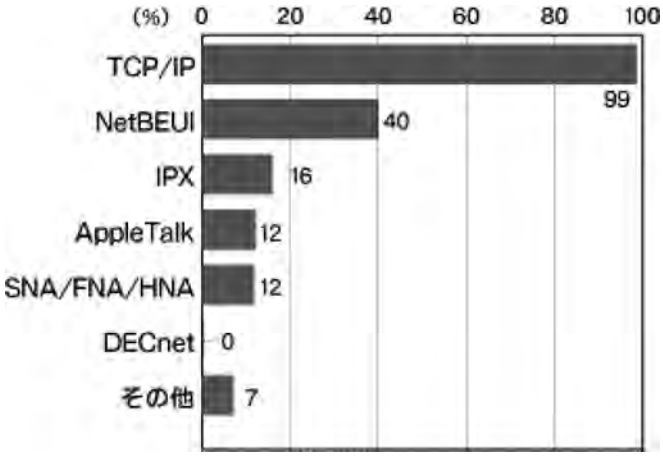
2002年世界のクライアントOS市場シェア（本数）



IXポイントが東京に集中



「すべてをIPへ」～高まるプロトコルのIP統一化意向

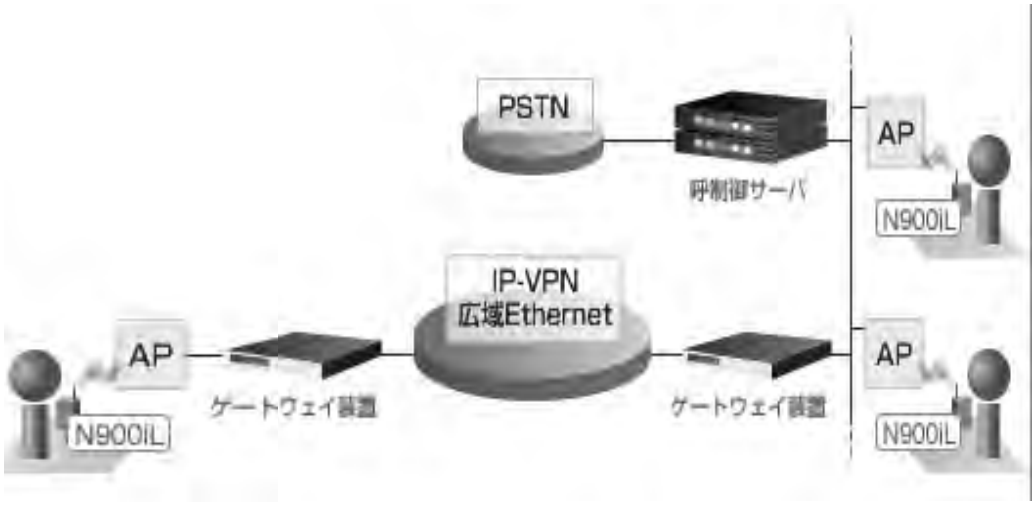


ネットワークプロトコル利用状況（複数回答　N=238）

アンケート調査結果　2002年2月～3月

http://www.atmarkit.co.jp/fnetwork/survey/survey06/network1.html

携帯電話とインターネットの融合



ドコモのモバイルセントレックスシステム　PASSAGE DUPLEの構成

IX運用技術者の必須装備

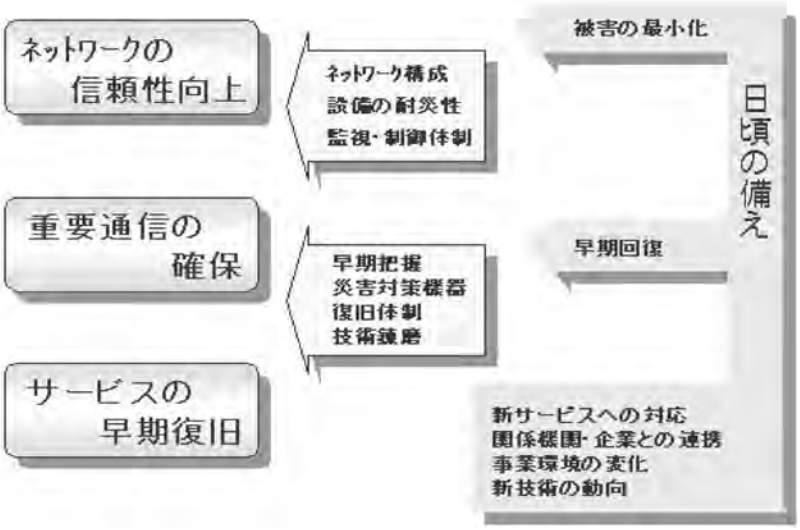
携帯やPHSがすべてIP化されたら．．．
インターネットを保守できなくなる？

- ディペンダブルインターネットへの取り組みの現状
- ネットワークの一色化の流れとディペンダビリティに対するリスクの増大
- **電話網の安心・安全設計に学ぶ**
- 多色なネットワーク／アプライアンス・デファインド・ユビキタス・ネットワークの提案

http://www.ntt-east.co.jp/saigai/housin/housin.html

災害対策方針

災害に強い通信設備の構築を図るとともに、万一、被災時は重要な通信の確保や、早期復旧を図る。



電話サービスの安心・安全基準

- **サービス品質**
  - □ 接続性
  - □ 通話品質
    - ■ 了解性
    - ■ 接続遅延
- **安心**
  - □ 通信の秘密保持
  - □ ユニバーサルサービス
- **不測事態への耐力**
  - □ 不測事態の要因
    - ■ 故障
    - ■ 天災：地震、火災、水害、雷
    - ■ 輻輳
    - ■ 不正使用、テロ、、
  - □ 確保すべき能力
    - ■ 重要通信の確保
      - □ 110、119番通報
      - □ 安否確認サービス

出典： 渡邉 均、間瀬 憲一： ″通信網の信頼性技術〟，システム制御情報学会論文誌，Vol.41，No.10，pp.422－428，199

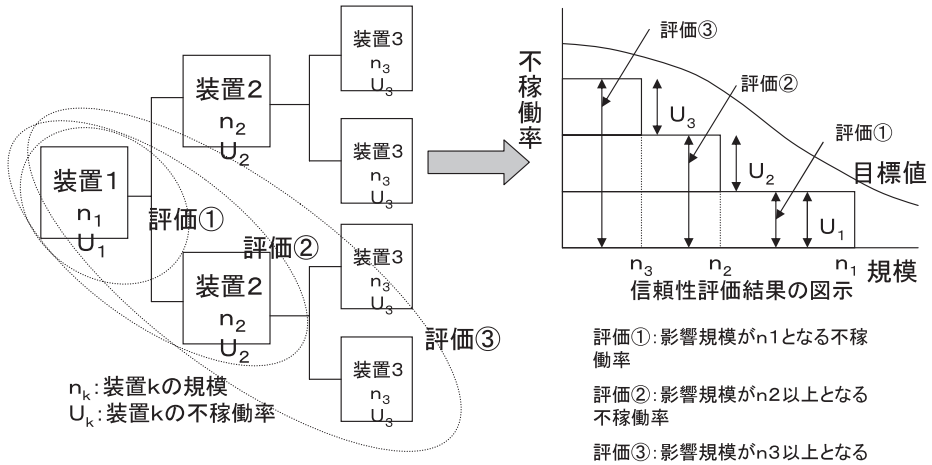
高信頼化策の体系

分類	具体的施策（例）
故障発生の低減	・高信頼性部品の使用 ・システム構成の冗長化：完全2重化、共通冗長化 ・共通装置への負荷分散
故障時間の短縮	・自動回復技術（交換機） 系の自動構成技術、ｲﾆｼｬﾙﾌﾟﾛｸﾞﾗﾑﾛｰﾄﾞ ・各種の保守性向上施策 保守エリアの広さの適正化、予備ﾊﾟｯｹｰｼﾞの配置
故障の影響の軽減	・設備の多重化 送路の多ルート化、中継交換機の分散設置 ・トラヒック制御 規制的制御、拡大的制御（ﾀﾞｲﾅﾐｯｸﾙｰﾁﾝｸﾞ）
その他災害対策	・移動交換機、無線局、電源等の配置 ・衛星を利用した臨時回線の設置

出典： 渡邉 均、間瀬 憲一：〝通信網の信頼性技術〟，システム制御情報学会論文誌，Vol.41，No.10，pp.422－428，199

信頼性設計

交換機等の内部装置は、重要な箇所は2重化されるなど、高度な信頼性設計がなされている。
重要度は、故障時の影響ユーザ数で判断している。



評価①：影響規模がn1となる不稼働率

評価②：影響規模がn2以上となる不稼働率

評価③：影響規模がn3以上となる不稼働率

出典： http://www.ntt-east.co.jp/saigai/kyokun/kyokun.html

災害と高信頼化策の歴史

年	災害名	被害等の状況	教訓と実施した対策
1968年	十勝沖地震	青森県を中心に4500加入 本土～北海道の通信が途絶	・市外伝送路の2ルート化多ルート化 ・TV中継伝送路のループ化 ・孤立防止用無線
1975年	旭川東光局火災	東光局収容の18900加入（13日間） 機械室から出火	・ハロン消火設備の導入 ・大容量可搬型電話局装置 ・大容量可搬型電源装置
1978年	宮城沖地震	仙台市を中心に400加入（7日間）	・機械室の架、フリーアクセス床の補強 ・橋梁添架管路等の所外設備の強化
1982年	長崎豪雨	長崎市を中心に20000加入（8日間）	・長時間停電対策・バッテリーの増容量 ・発電機の増配備
1983年	島根豪雨	島根県を中心に12000加入 河川氾濫で1局が機能停止（20日間）	・衛星利用の拡大 ・可搬型ディジタル交換機（KS-1） ・広域災害用光ケーブルの開発
1984年	世田谷とう道火災	世田谷局収容の89000加入のほか 専用線多数（9日間）	・出火防止（難燃ケーブルの採用） ・延焼防止（防火壁） ・とう道内作業管理の強化
1990年	7.2九州北部豪雨	佐賀県、熊本県等で18300加入 河川氾濫で2局が機能停止（5日間）	・可搬型加入者無線方式の開発 ・災害対策機器のディジタル化
1993年	北海道南西沖地震	奥尻島を中心に1450加入(12日間)	・災害対策機器の機動性向上 ・災害対策用ポータブル衛星の開発
1995年	阪神・淡路大地震	神戸市を中心に30万を越える加入 （14日間）	・全国利用型伝言ダイヤル ・衛星利用の拡大 ・被災地情報ネットワーク開発

十勝沖地震

昭和43年5月16日発生
マグニチュード7.8

通信関連の被害
八戸市の無線中継所が大被害
本州ー北海道の通信が災害の最中に２時間途絶

教訓等
電話網安定品質基準制定（昭和45年）の契機となる。
また、その後中継交換機の分散化（例：前橋、立川等）を行なった。

写真：ポータブル衛星　人が持ち運べるタイプで、しかも衛星を使えますから災害時に機動性を発揮します。交通遮断や山中での災害などにおける臨時回線の作成、特設公衆電話の設置などに威力を発揮します。

出典：　三石庄一郎、長崎勝：“47.7豪雨を契機とする災害対策について”，　施設、25-3

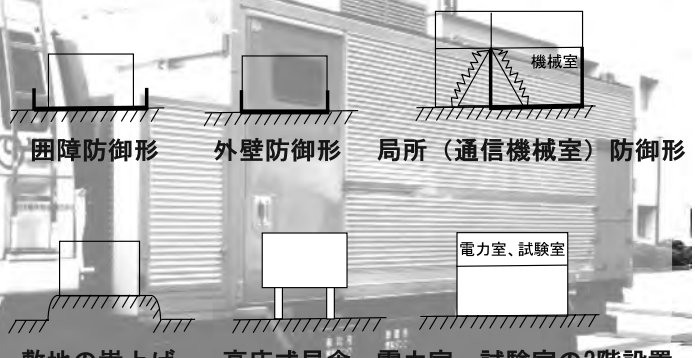
水害対策

昭和47年7月豪雨

被害状況

罹障回線数 / 通信局	回線種別	
	市内電話回線	市外電話回線
四　国	970	465
九　州	17,870	3,550
東　北	1,260	40
信　越	50	0
中　国	21,080	5,860
近　畿	34,360	280
関　東	6,310	2,995
東　京	1,400	0
東　海	10,640	4,440
合計	93,940	17,630

局舎の水防対策進展



囲障防御形　外壁防御形　局所（通信機械室）防御形

敷地の嵩上げ　高床式局舎　電力室・試験室の2階設置

写真：移動電源車　長時間停電が発生し、予備電源も停止した場合、最大1，000kVAの発電能力を備えた移動電源車により通信電源を確保します。

出典： 保全局災害対策室:“世田谷電話局とう道火災被害の応急復旧 ”， 施設、37-1

世田谷とう道火災

昭和59年11月7日発生
原因は工事中の失火

通信関連の被害

収容加入者（8万9千）全数不通
復旧に約１週間

教訓等

ケーブルの難燃化等
応急措置は移動無線車や衛星回線を幅広く展開

写真:可搬型ディジタル交換機　電話をつなぐ交換機が被災した場合、非常用交換機をヘリコプター等で輸送し、10日間程度で臨時電話局を構築することができます。

出典： 米重太平、五十嵐克彦:“阪神・淡路大震災を教訓とした激甚災害対策 ”, NTT技術ジャーナル　1995.10

阪神大震災

平成７年１月17日発生
直下型地震（震度７）

通信関連の被害状況

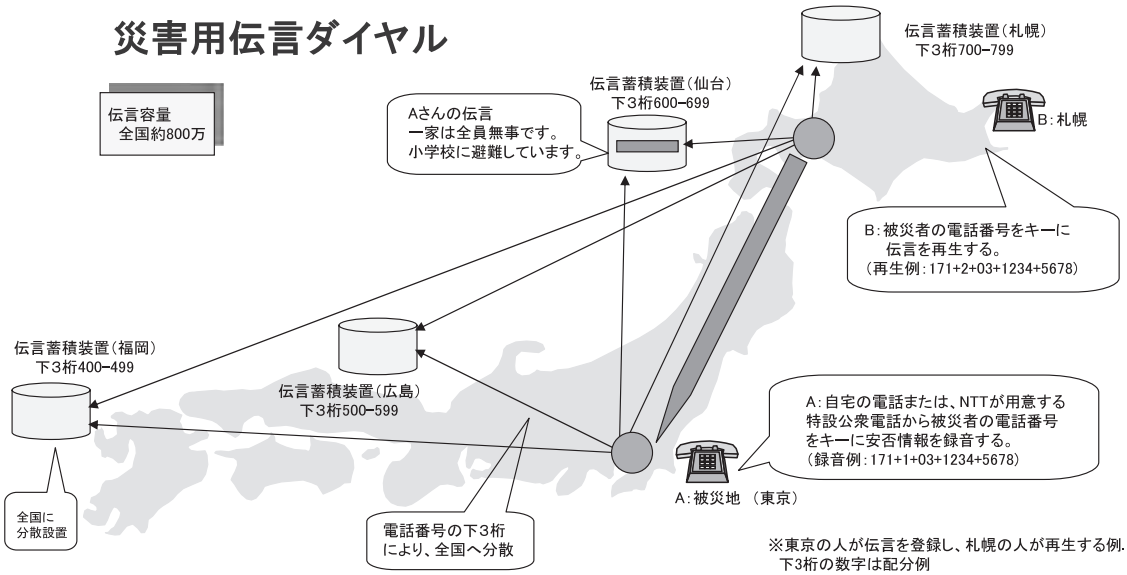
○設備の状況			○サービスの状況	
ネットワーク系設備の被災	長距離系設備	・主要交換機は影響回避 ・主要伝送路は予備伝送路へ切り替え	電話サービス	・30万を超える電話が普通 ・通常ピーク時の50倍のトラヒックで長期輻輳
	地域系設備	・バックアップ電源破損（28.5万回線罹障） ・ノンヒューズブレーカ断による現地駆けつけリカバリ	専用サービス	・3500回線が故障（全体の14%） ・110,119番への無効発呼が発生
アクセス系設備の被災		・架空ケーブルと引込線が大きな被災（19.9万回線罹障）	公衆電話サービス	・商用電源停止のためカード不可 ・金庫充満による使用不能
建物・鉄塔等設備の被災		・建物は3ビルが被災の他はおおむね問題なし ・鉄塔2基が被災	PNWサービス	・大口法人ユーザへ、移転を含め優先対応

教訓等

加入者輻輳により、緊急時の通話に支障。安否確認の手段の必要性認識。一方で、中継系伝送路は設備の強度も向上し分散も進んだので殆ど被害は無かった。強度的には過去の対策が奏効。

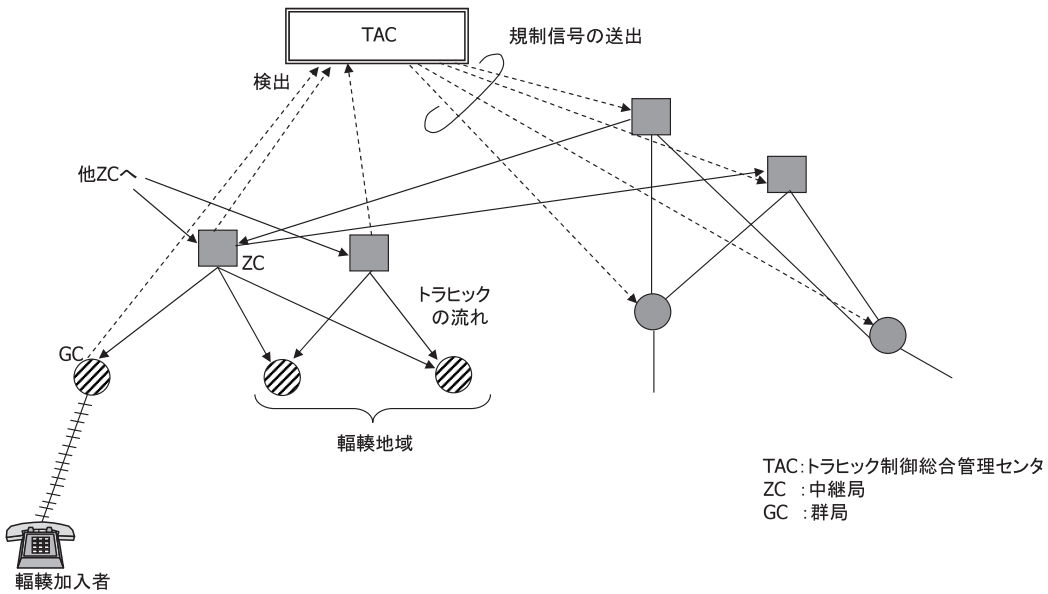
出典: 橋本博明、小林充佳、竹田直樹:“災害用伝言ダイヤルの運用開始 ”, NTT技術ジャーナル 1998.3

阪神大震災



インターネットのセキュリティ −電話網からのレッスン−、京都大学 高橋達郎教授の講演資料より

輻輳制御



電話ネットワークの安心・安全

- 長期間を経なければ得られない災害経験をもとに高信頼化
- 高信頼化の中身はハードから運用、サービスまで広範囲、多様
  - 装置の二重化、建物、輻輳制御、伝言ダイヤルなど
- その多くはキャリアの社内努力で実現
  - 「標準」はほとんど存在しない
  - 大きなコストが必要
    - 不測事態発生時にしか、ユーザはメリットを実感できない？

- ディペンダブルインターネットへの取り組みの現状
- ネットワークの一色化の流れとディペンダビリティに対するリスクの増大
- 電話網の安心・安全設計に学ぶ
- **多色なネットワーク／アプライアンス・デファインド・ユビキタス・ネットワークの提案**

ICTによる情報交流・共創社会の到来

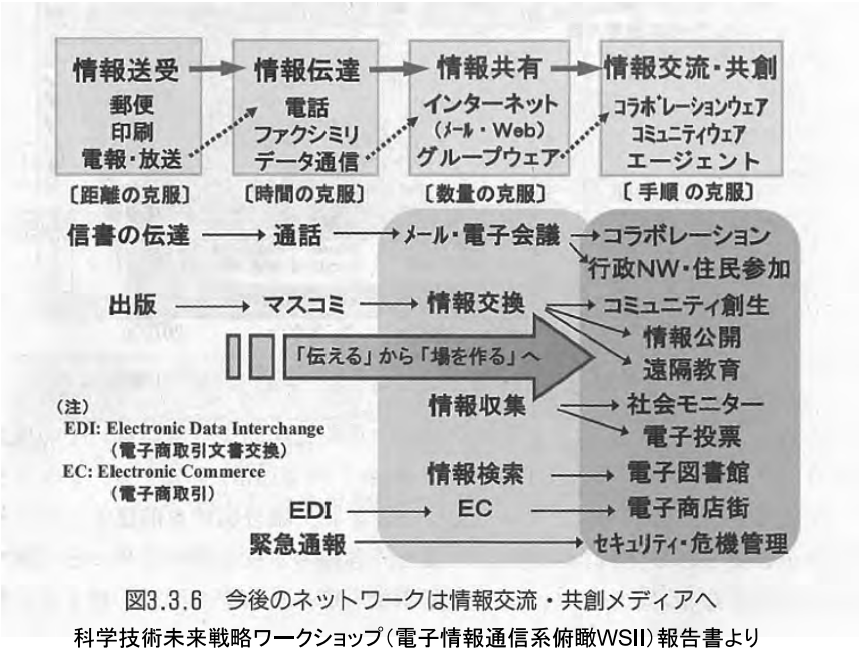


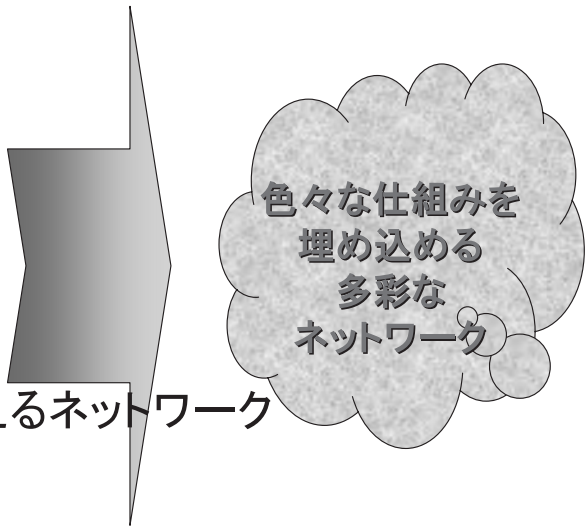
図3.3.6　今後のネットワークは情報交流・共創メディアへ

科学技術未来戦略ワークショップ(電子情報通信系俯瞰WSII)報告書より

交流・共創時代のディペンダビリティ

・・頼みに、当てに、信頼できる。・・少し広く考えて。。。

- 優しいネットワーク
  - □ 人と社会に優しい
  - □ 環境に優しい
- 賢いネットワーク
  - □ 高性能
  - □ 低コスト
  - □ 何でもつなぐ
- 何時でも何処でも使えるネットワーク
  - □ 場所を選ばない
  - □ 時間を選ばない



多彩ネットワーク

- 安心・安全実績のある、仕組み(「色」)の異なるネットワークを
  - できるだけリソース独立に維持・運用し、
  - 「使いこなし」あるいは「自動化」によりインターネットワーキングさせたい
- 独立化の対象となるネットワークリソース
  - 端末(ハード、ソフト)
  - L0: 管路、電柱など
  - L1: 線路、波長
  - L2: 方式、プロトコル
  - L3、L4、、、

多色ネットワークの目的と条件

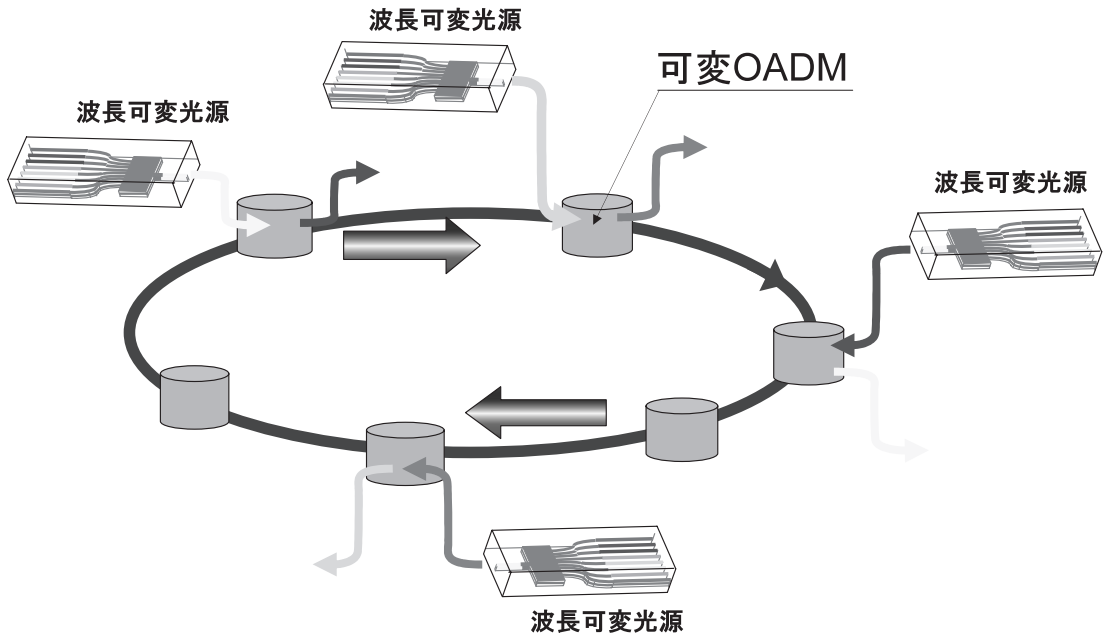
- 目的
  - 既存ネットワークの安心・安全実績の継承と蓄積
    - ネットワークのトータルな安心・安全度向上
- 条件
  - 要素ネットワークが日々、使われること
    - ユーザ、保守者のスキルを維持するのに必要
  - 維持コストを出せること
    - 「安心・安全基準」の存在(競争ルールへの組み込み)
    - 低コスト(技術の役割)
    - コスト増を受容させるユーザメリット

ネットワークリソースのバーチャルな分離に貢献する技術

- L1: 波長レベルの分離
  - ROADM
- L2: 無線プロトコル
  - ソフトウェア無線
-
-
-

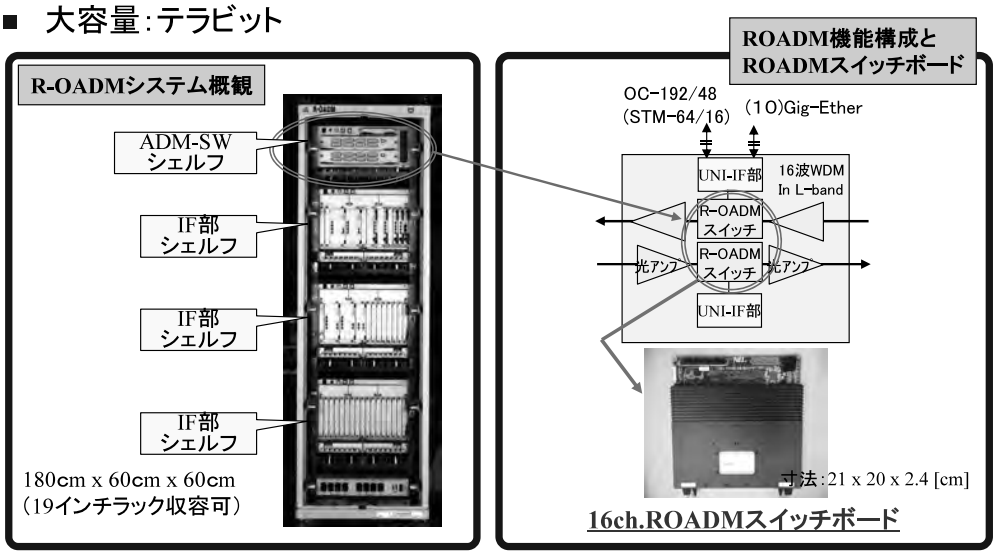
システムにおける適用例

（可変OADMリングシステム）

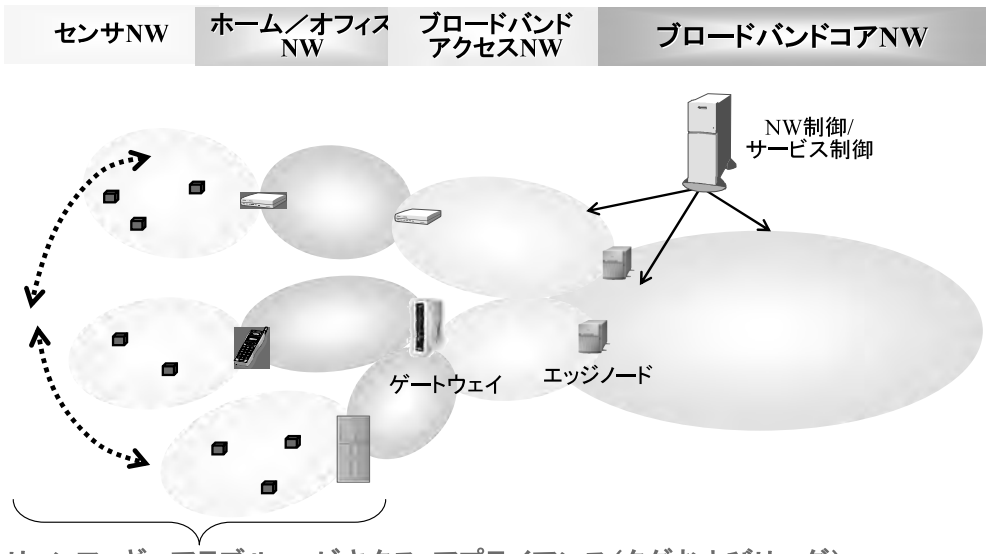


ROADM:ﾘｺﾝﾌｨｷﾞｭｱﾗﾌﾞﾙ・ﾄﾗﾝｽﾍﾟｱﾚﾝﾄ化OADM

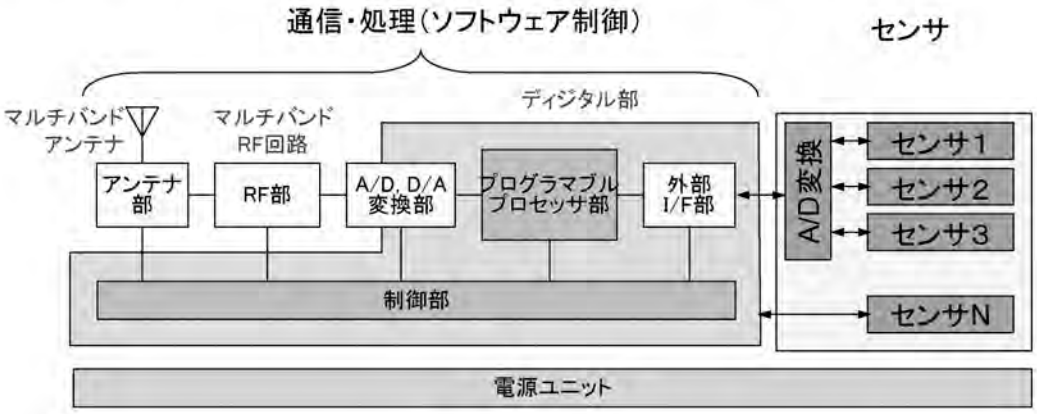
- トランスペアレント：1R光伝送・広域（200Km)・低遅延・伝送フレーム再生チップ
- リコンフィギュアラブル：波長編集
- 大容量：テラビット



ユビキタスネットワークとリコンフィギュアラブル・ユビキタスアプライアンス



リコンフィギュアラブル・ユビキタスアプライアンス



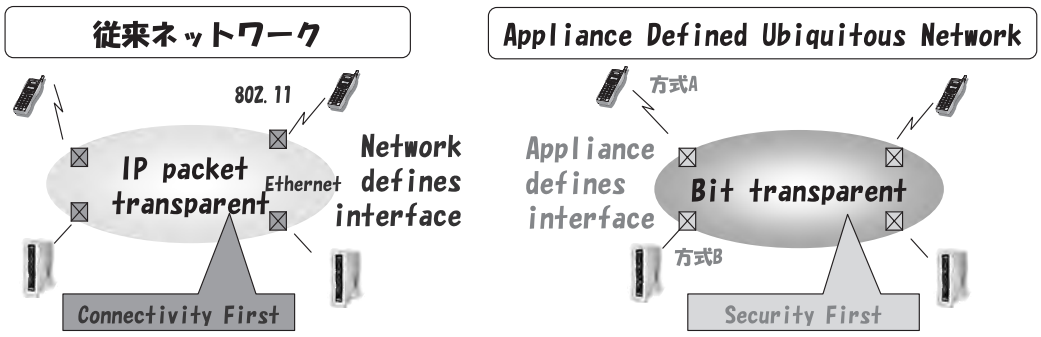
ソフトウェア無線を内蔵するアーキテクチャ例

- ソフトウェア無線：ソフトウェアの書き換えにより、機能変更・追加が可能な無線装置
  ①周波数　②通信方式（伝送速度等）　③サービス（音声、画像、メール、Web等）

ADUNの提案

ADUN（アドゥン）：アプライアンス・デファインド　ユビキタス　ネットワーク

- **アプライアンスが持ち込んだインターフェースをネットワークが自動的にサポートするユビキタスネットワーク**
  - **従来はNW側が規定したIFのアプライアンスを接続**
    →　アプライアンスのIFをNWが自動サポートして個別プライベート網構築
  - **接続性重視　→　セキュリティ（ユーザ・アプライアンス毎のclosed網）を優先**
  - **小さなユビキタスアプリを蓄積し、連携した広範なユビキタスアプリを提供**
- **小規模な応用市場毎の多様なワイヤレス方式を受容し、セキュリティ・プライバシーにクリティカルなデータをユーザコントロールの範囲で収集、処理可能**



研究開発のアウトプット
プラットフォームを形成していくフレームワーク

- 「技術の種」+「成長する仕組み」
  - 市場成立時には、技術ベンダー、サービスプロバイダ、アプリケーション産業、技術者コミュニティ、標準化などを牽引する仕組みなどが日本中心に出来上がる
- フレームワークの必須要素
  - Goal/Concepts、Platform Architectural Principles
    - 成長を通じて維持されるべき目標、設計原則
    - 日本の強みや特徴を織り込むシナリオを含むべき
      - マクロ動向を先取り、大規模市場を目指すビジョン、目標とするビジネスモデル
      - プラットフォームシフトを引起す可能性を内在するアーキテクチャ
        - 非主流、斬新
      - 日本が強い持続的技術の成長成果を投入
  - Technology seeds、課題
  - R&Dをドライブするアプリケーションとそれを使い込む『場』
    - 構想を体現・実証する原始システム
    - 開発者自身が未熟な技術をユーザとして使い込み磨く
  - 技術者集団

ADUNの設計原則

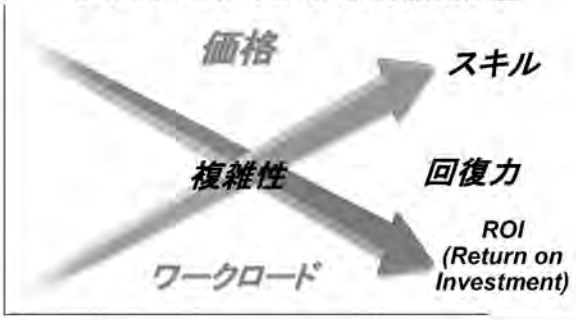
- アプライアンスがインタフェースを決める
  - PC主導(IPパケット)からアプライアンス主導(ストリーム)へ
    - 大容量トラヒックを生む映像系アプライアンスはストリームを入出力
    - 無数に散らばるアプライアンスの主流は無線インタフェース
      - インタフェースの種類やプロトコルが多様化する
      - 電波(ストリーム)をディジタル化すれば、無線インタフェースのトランスペアレント収容が可能になる
- アプライアンスはクローズドなネットワークに接続する
  - 独自のインタフェース／プロトコルによる高いセキュリティ
  - 他網との相互接続性は信頼あるキャリアのみが提供


IBM
IBM
ディペンダビリティワークショップ
社会サービスの Dependability
- Dependability Workshop I -
2006年5月12日
日本アイビーエム株式会社
岩野和生


ディペンダビリティワークショップ
IBM
Dependability とは？
• 伝統的 Dependable System の定義
– A. S. Tanenbaum: “Distributed Systems”
1. 可用性 / 2. 信頼性 / 3. 安全性 / 4. 保守性
– 古典的 Fault Tolerance の考え方
• MTBF, MTTR
• 冗長化、モジュール化（Fail First）
• システムの拡大化、複雑化に伴う概念の拡張
– プロセッサーレベルから社会全体まで
– Autonomic Computing
1

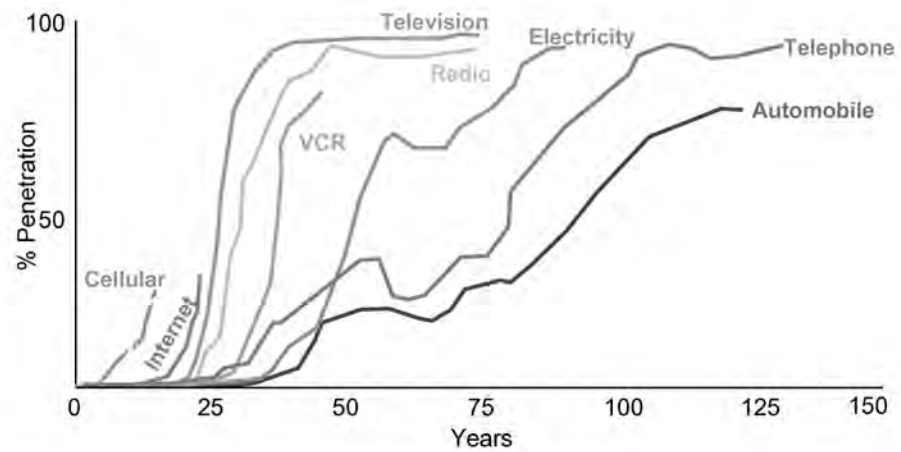
企業が直面している問題

- TCO
- ROI
- TTM
- 安全、安心
- SLA保障
- 法律
  - プライバシー
  - アクセシビリティー
  - コンプライアンス
  - リスク管理
- 人件費の増大
- スキルの不足
- 複雑度 （Complexity）
- 予測不可能性
- システム、インフラの脆弱性

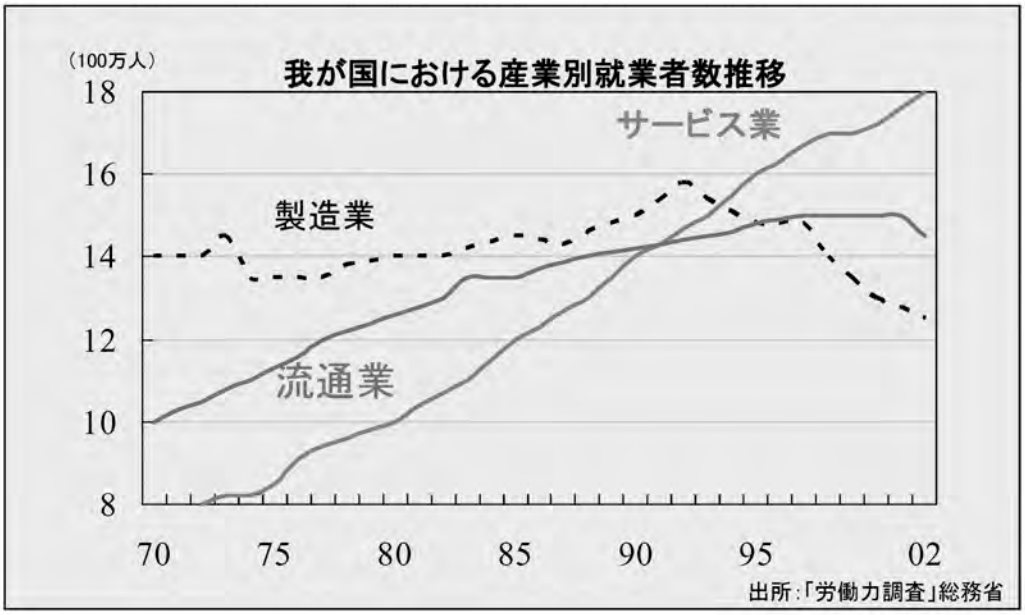


イノベーションの加速するペース

- 新しいイノベーションほど、普及するスピードは加速



経済のサービス化



今日のIT環境とお客様の抱えている課題

様々な既存システム保守のため新規アプリケーションの実装は遅れています

今日の障害の80%は人間（40%はオペレーター）のエラーに起因します

複雑な異機種環境の管理

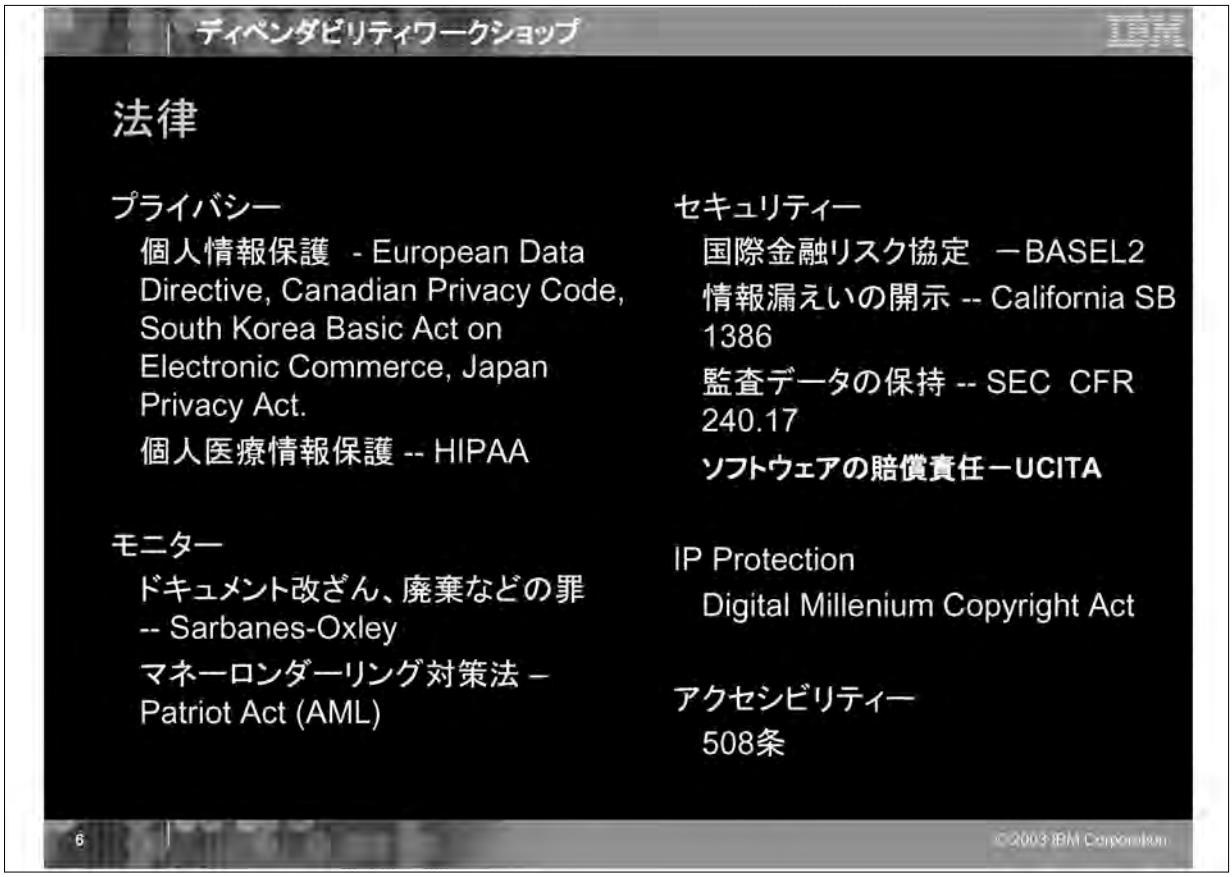
レガシー・アプリケーションの情報が十分にドキュメント化されていないため、複雑な製品をまたがった問題の分析と解決を難しくしています

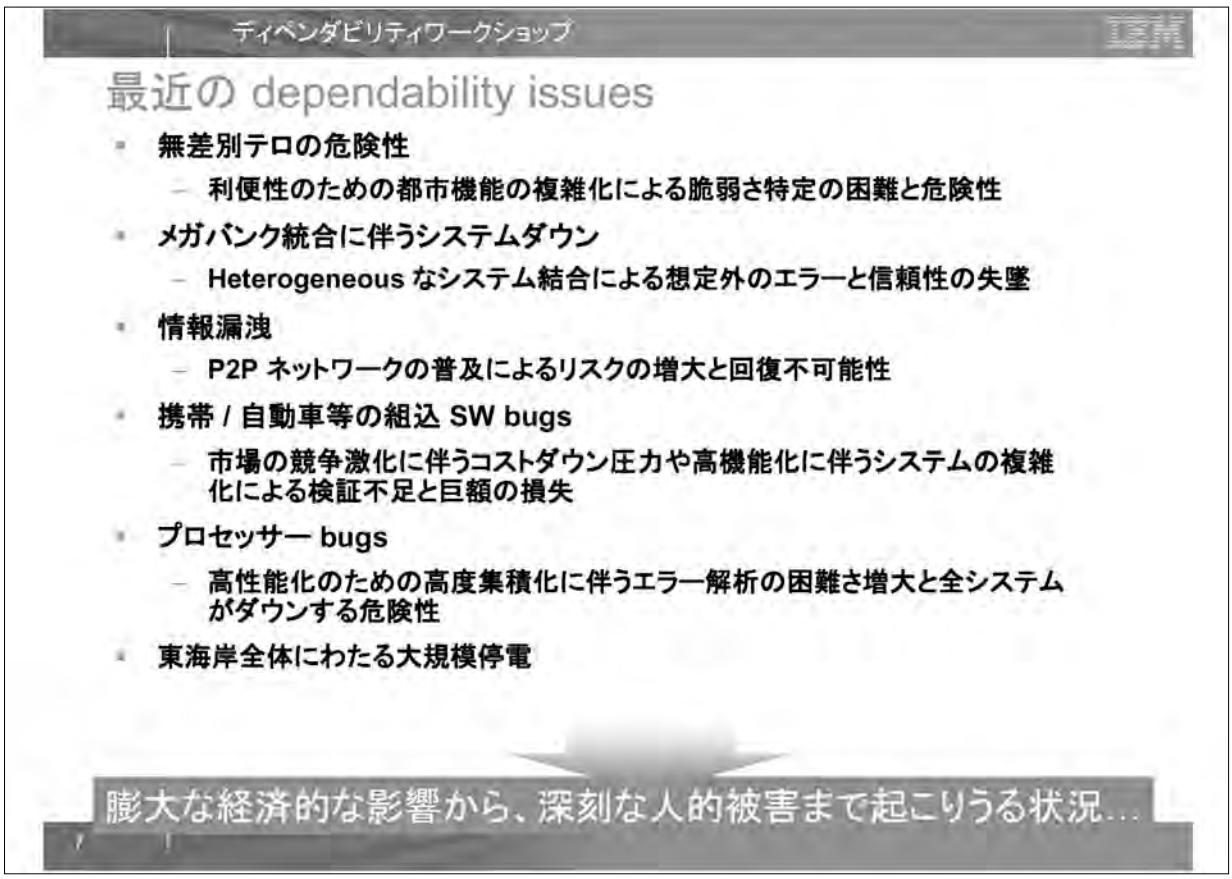
全体の25-50%の時間が問題分析に費やされています

複数製品にまたがる問題分析ができるエキスパートは、貴重で人件費も高い
障害時80%は問題判別に要する

ミッション・クリティカルなシステム障害のコストは年間$2.8Mにものぼります

IT投資の80%は運用、維持、小規模な機能拡張に費やされています


ディペンダビリティワークショップ
IBM
法律
プライバシー
個人情報保護 - European Data Directive, Canadian Privacy Code, South Korea Basic Act on Electronic Commerce, Japan Privacy Act.
個人医療情報保護 -- HIPAA
モニター
ドキュメント改ざん、廃棄などの罪 -- Sarbanes-Oxley
マネーロンダーリング対策法 – Patriot Act (AML)
セキュリティー
国際金融リスク協定 －BASEL2
情報漏えいの開示 -- California SB 1386
監査データの保持 -- SEC CFR 240.17
ソフトウェアの賠償責任－UCITA
IP Protection
Digital Millenium Copyright Act
アクセシビリティー
508条
6
© 2003 IBM Corporation


ディペンダビリティワークショップ
IBM
最近の dependability issues
無差別テロの危険性
利便性のための都市機能の複雑化による脆弱さ特定の困難と危険性
メガバンク統合に伴うシステムダウン
Heterogeneous なシステム結合による想定外のエラーと信頼性の失墜
情報漏洩
P2P ネットワークの普及によるリスクの増大と回復不可能性
携帯 / 自動車等の組込 SW bugs
市場の競争激化に伴うコストダウン圧力や高機能化に伴うシステムの複雑化による検証不足と巨額の損失
プロセッサー bugs
高性能化のための高度集積化に伴うエラー解析の困難さ増大と全システムがダウンする危険性
東海岸全体にわたる大規模停電
膨大な経済的な影響から、深刻な人的被害まで起こりうる状況…
7

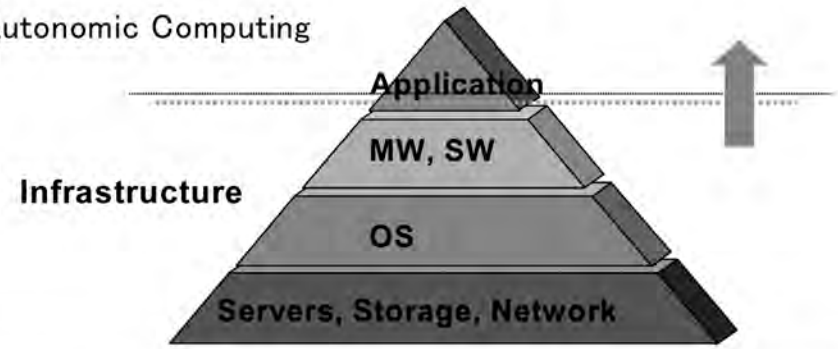
オートノミックコンピューティング？

IBM

What? *Initial Definition in 2001*

- **Autonomic Computing is self-management technology for providing reliable, always available, and robust e-business infrastructure to assure service level objectives.**

The scope of Autonomic Computing



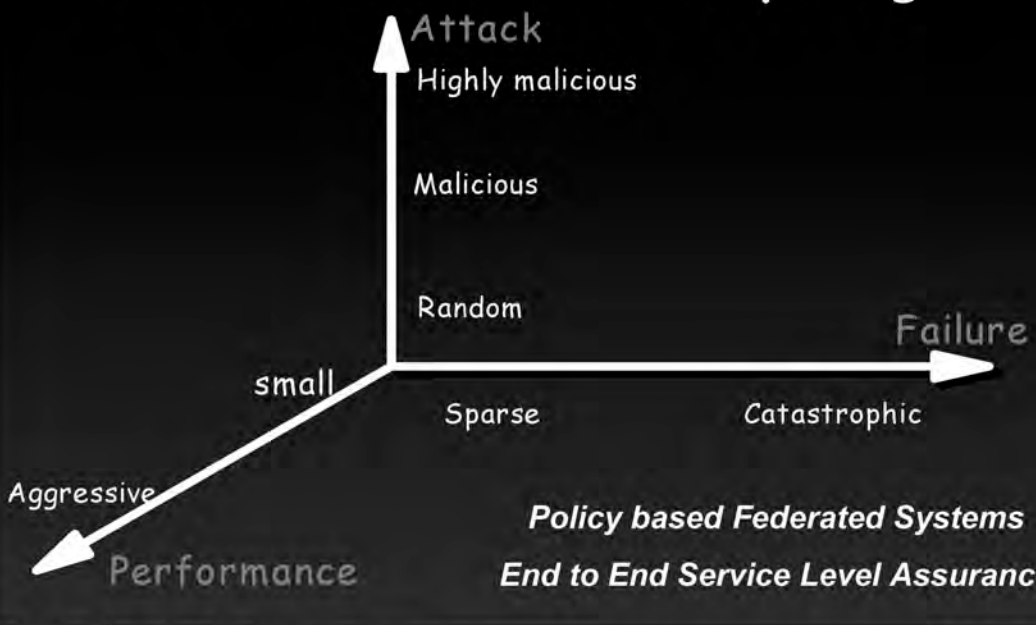
IBM: Setting the Industry Agenda

8

ディペンダビリティワークショップ

IBM

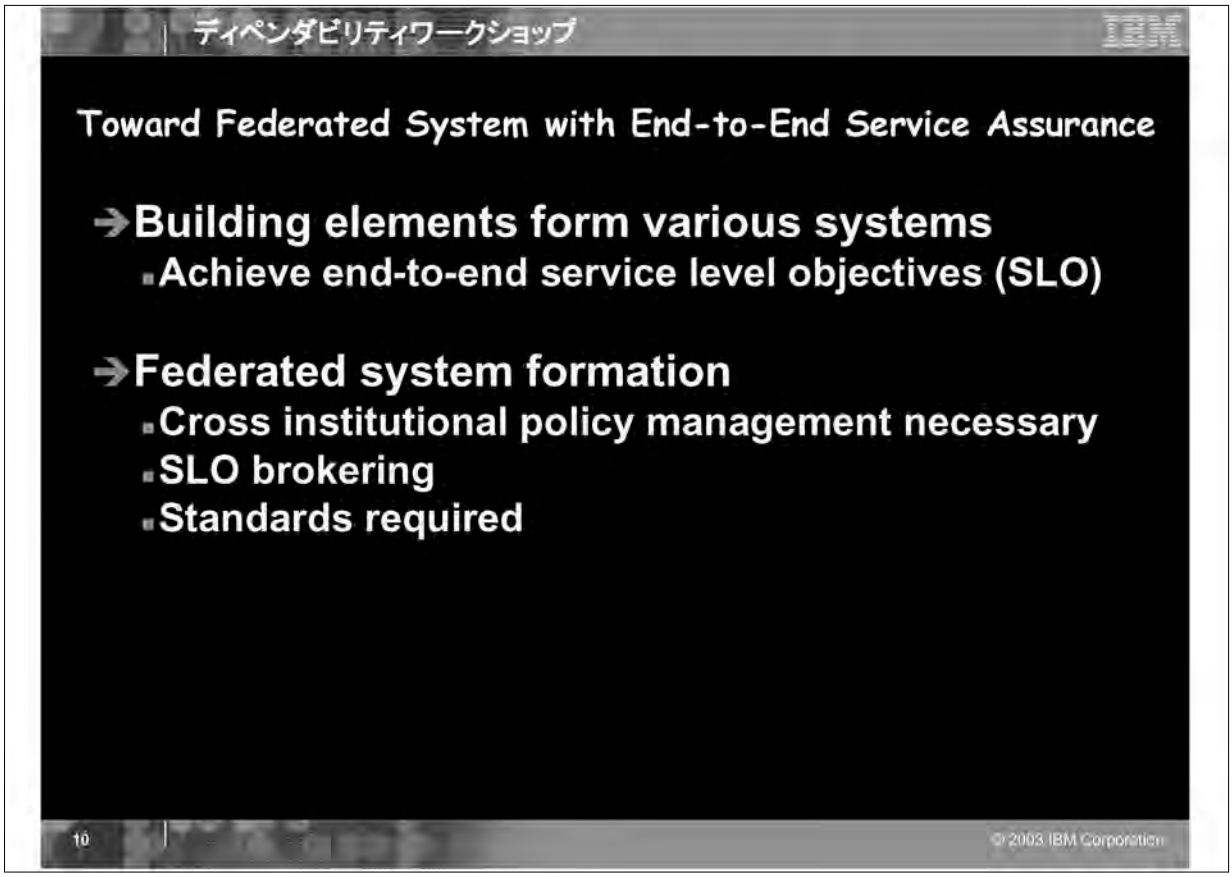
Scales of Autonomic Computing

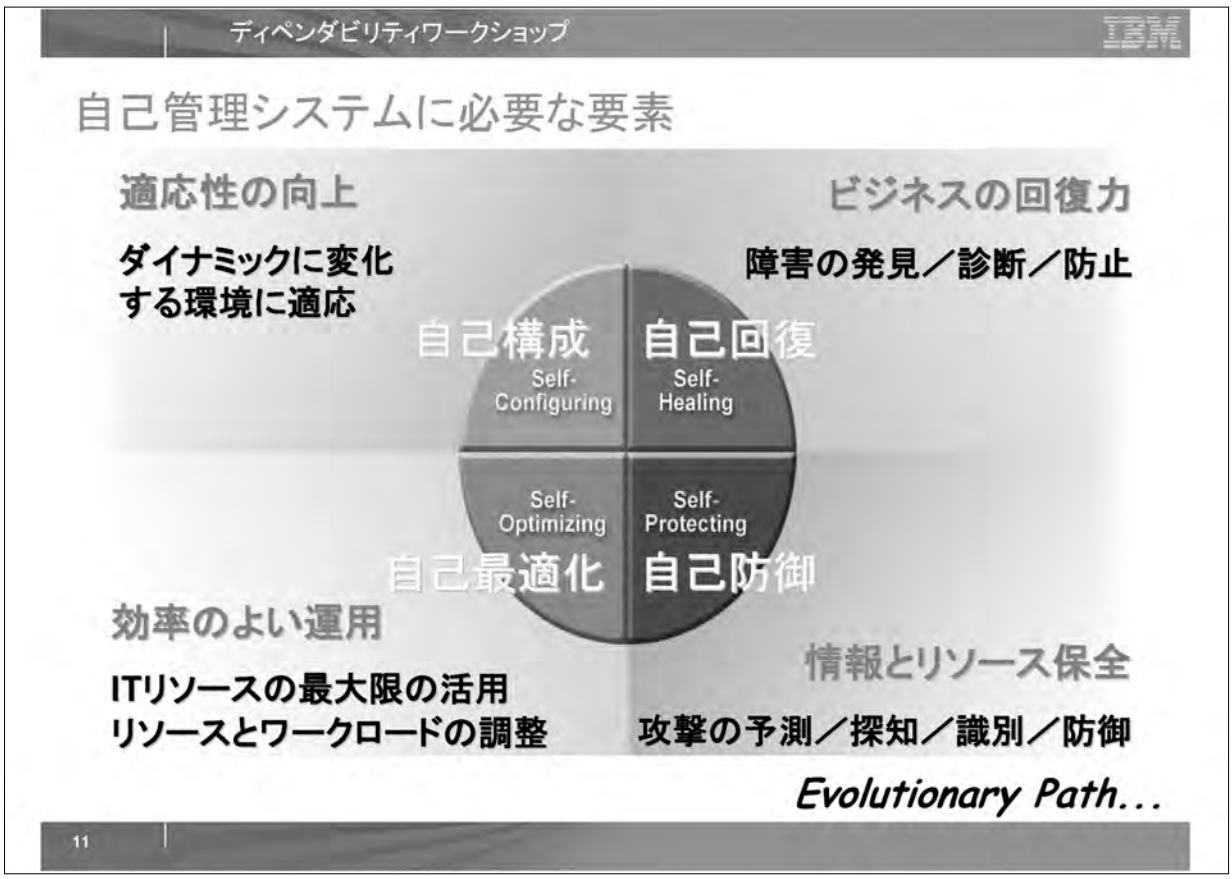


Policy based Federated Systems

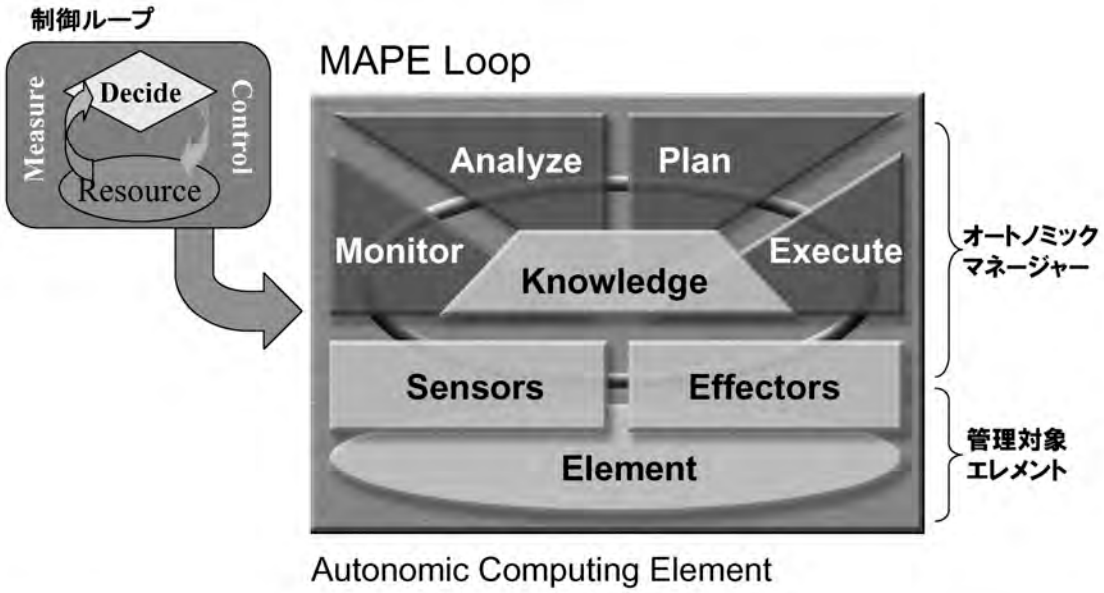
End to End Service Level Assurance

9


ディペンダビリティワークショップ
IBM
Toward Federated System with End-to-End Service Assurance
➔Building elements form various systems
▪Achieve end-to-end service level objectives (SLO)
➔Federated system formation
▪Cross institutional policy management necessary
▪SLO brokering
▪Standards required
10
© 2003 IBM Corporation

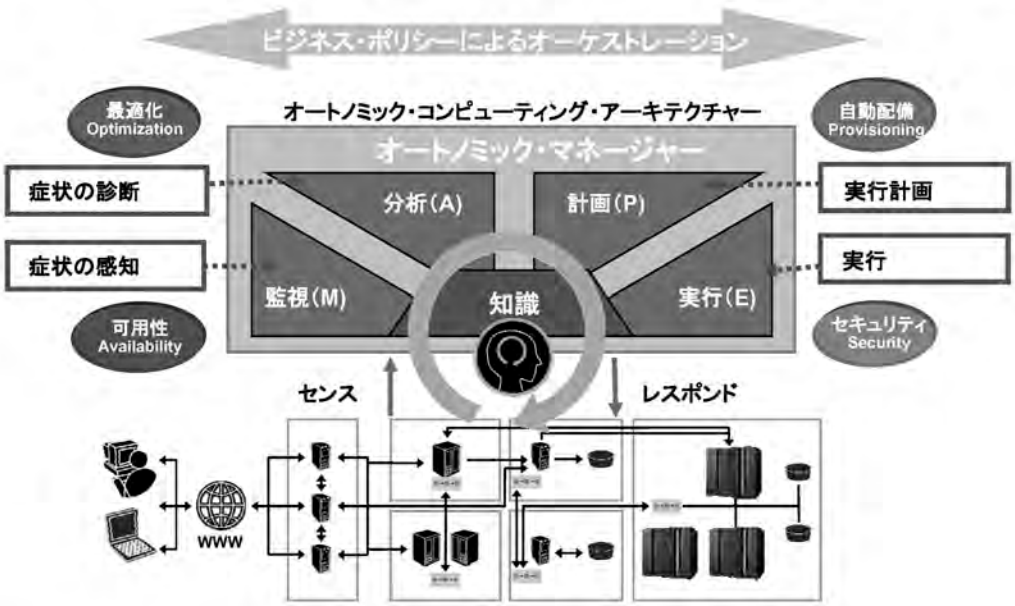

ディペンダビリティワークショップ
IBM
自己管理システムに必要な要素
適応性の向上
ダイナミックに変化
する環境に適応
ビジネスの回復力
障害の発見／診断／防止
自己構成
Self-
Configuring
自己回復
Self-
Healing
Self-
Optimizing
Self-
Protecting
自己最適化
自己防御
効率のよい運用
ITリソースの最大限の活用
リソースとワークロードの調整
情報とリソース保全
攻撃の予測／探知／識別／防御
Evolutionary Path...
11

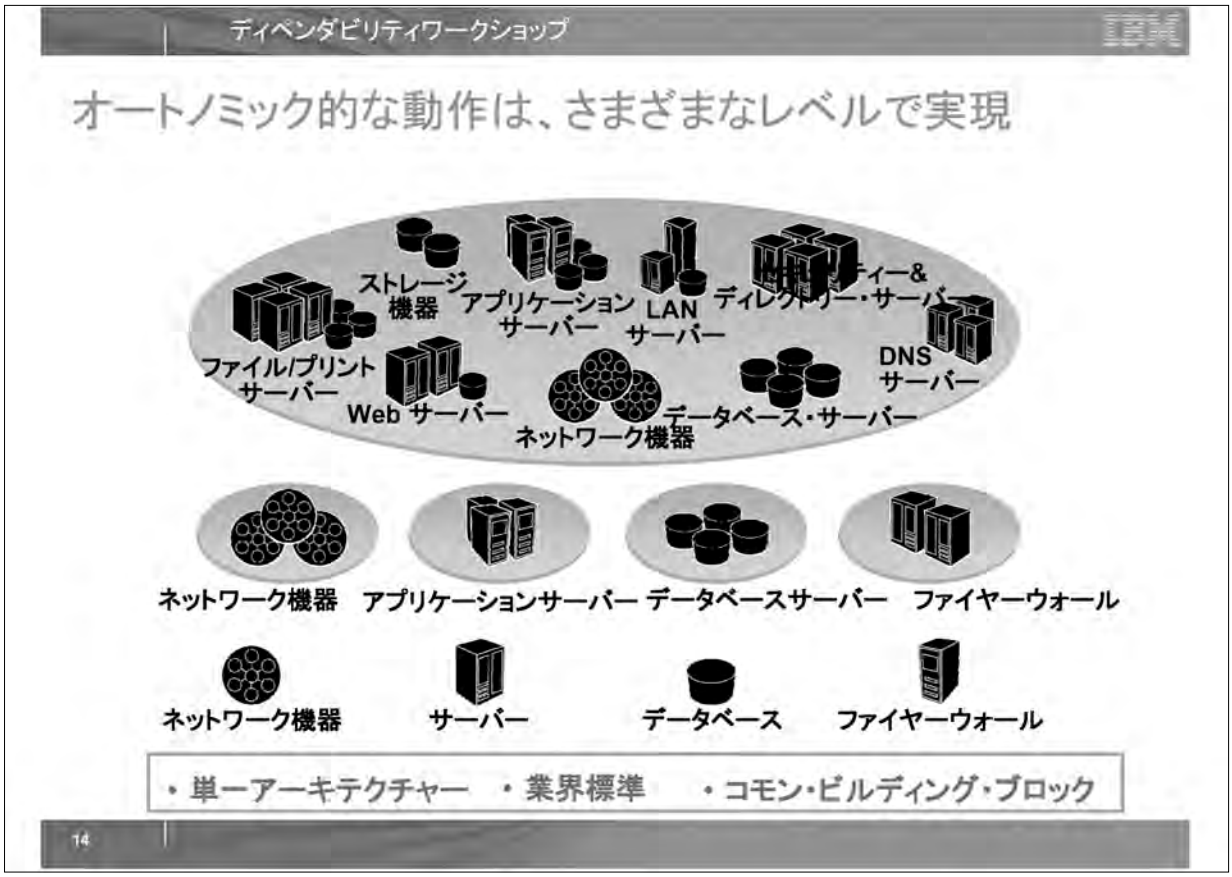
オートノミック・コンピューティング・アーキテクチャー

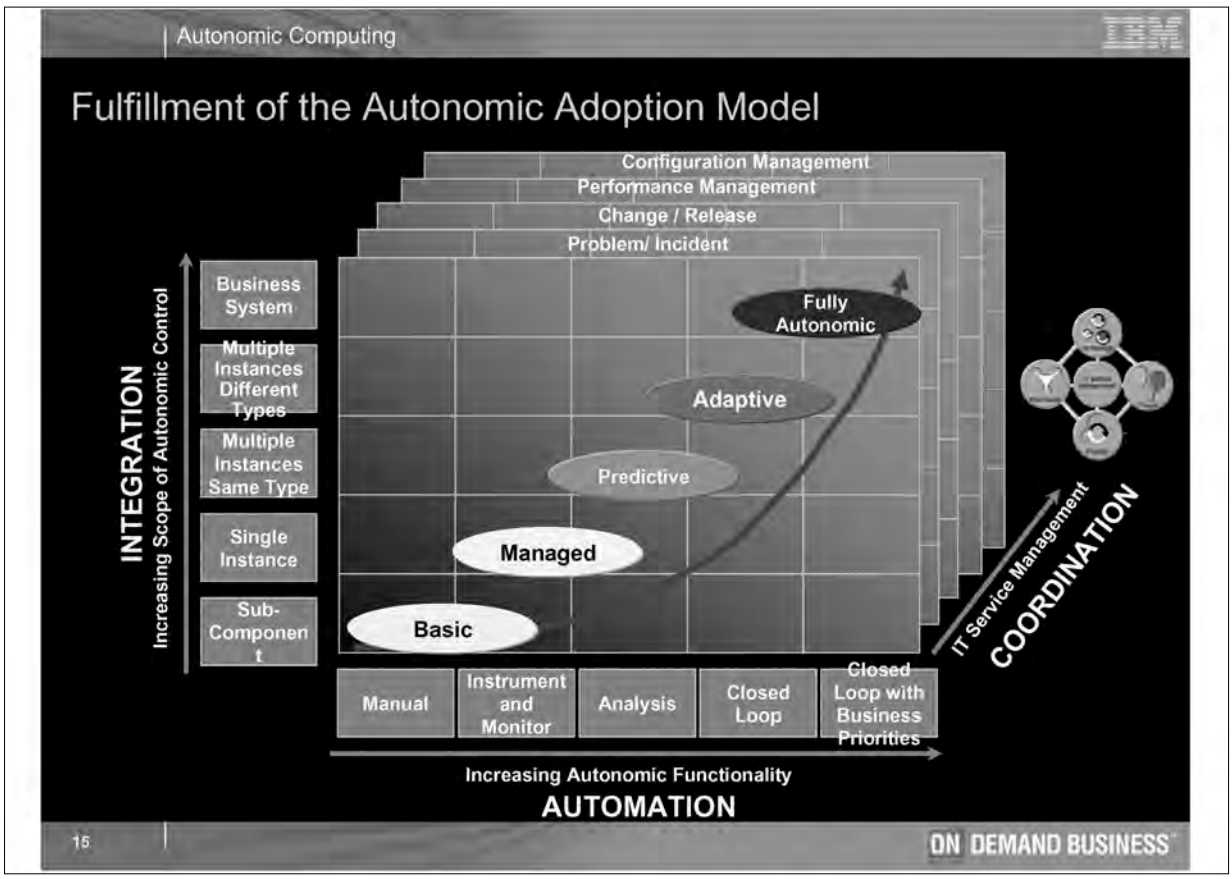


Autonomic Computing Element

オートノミック機能の統合によりシステムに自己管理を実現



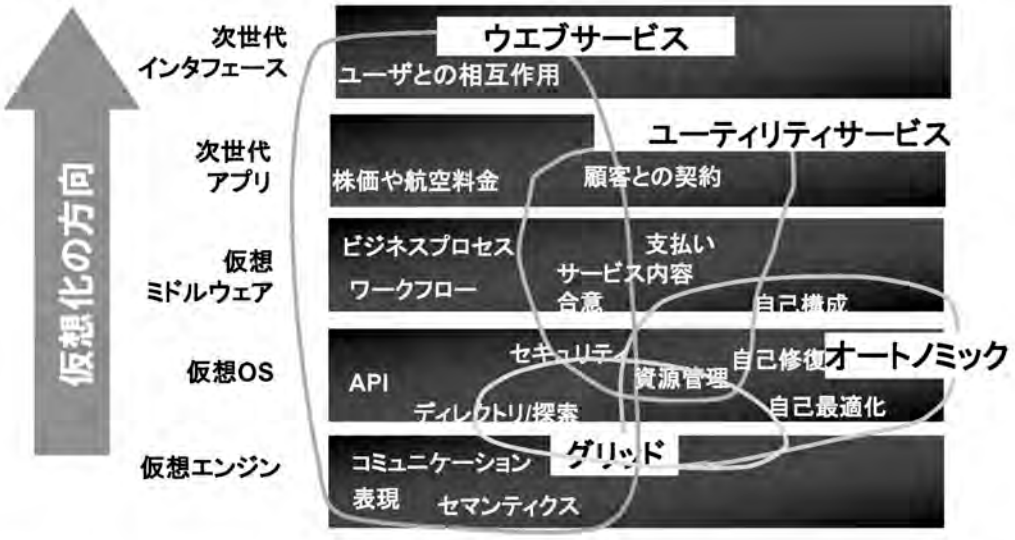

ディペンダビリティワークショップ
IBM
オートノミック的な動作は、さまざまなレベルで実現
ストレージ機器
アプリケーションサーバー
LAN サーバー
ディレクトリー・サーバー
ファイル/プリントサーバー
Web サーバー
ネットワーク機器
データベース・サーバー
DNS サーバー
ネットワーク機器
アプリケーションサーバー
データベースサーバー
ファイヤーウォール
ネットワーク機器
サーバー
データベース
ファイヤーウォール
・単一アーキテクチャー ・業界標準 ・コモン・ビルディング・ブロック
14


Autonomic Computing
IBM
Fulfillment of the Autonomic Adoption Model
Configuration Management
Performance Management
Change / Release
Problem/ Incident
INTEGRATION
Increasing Scope of Autonomic Control
Business System
Multiple Instances Different Types
Multiple Instances Same Type
Single Instance
Sub-Component
Fully Autonomic
Adaptive
Predictive
Managed
Basic
IT Service Management
COORDINATION
Manual
Instrument and Monitor
Analysis
Closed Loop
Closed Loop with Business Priorities
Increasing Autonomic Functionality
AUTOMATION
15
ON DEMAND BUSINESS

4年の歩み

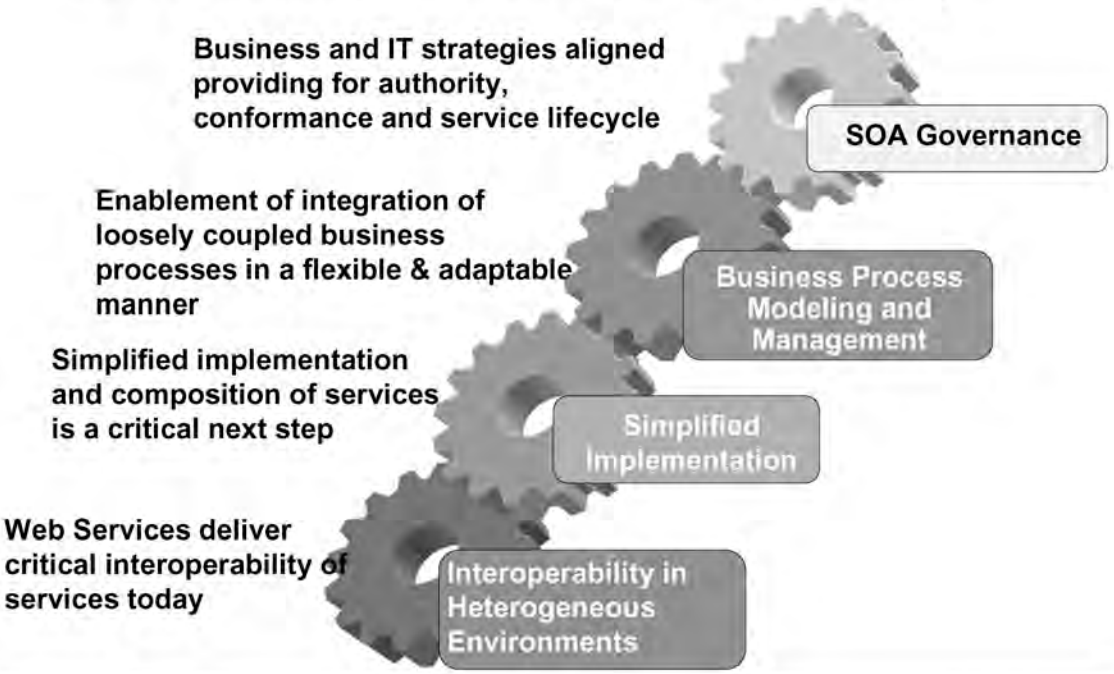
IBM	・アーキテクチャの青写真を発行 ・115以上のお客様事例 ・60以上のパートナー ・450の自己管理オートノミック・フィーチャー ・特許550件 DB2 Information Management Software / Lotus software / IBM ThinkVantage / Tivoli software / eserver / WebSphere software / TotalStorage™ / Rational software
業界における協業	・60以上のパートナーとの製品提供 ・ACツールキット ・自己管理オートノミック・フィーチャー SINGLESTEP / Cisco Systems / HitachiSoft / macrovision
標準化における協業	・問題判別の標準 ・CBEに基づくWSDM 1.0 ・Solution Deployment Descriptor 標準 ・OASISのテクニカル・コミッティに共同議長 ・管理の標準 hp invent / ca / FUJITSU / Sun / OASIS
学術における協業	・33以上の国際会議 ・オートノミック・コンピューティングの第一回、第二回IEEE国際会議 ・10以上のジャーナル IEEE / AUTONOMIC COMPUTING

サービスオリエンテッドアーキテクチャ (SOA)

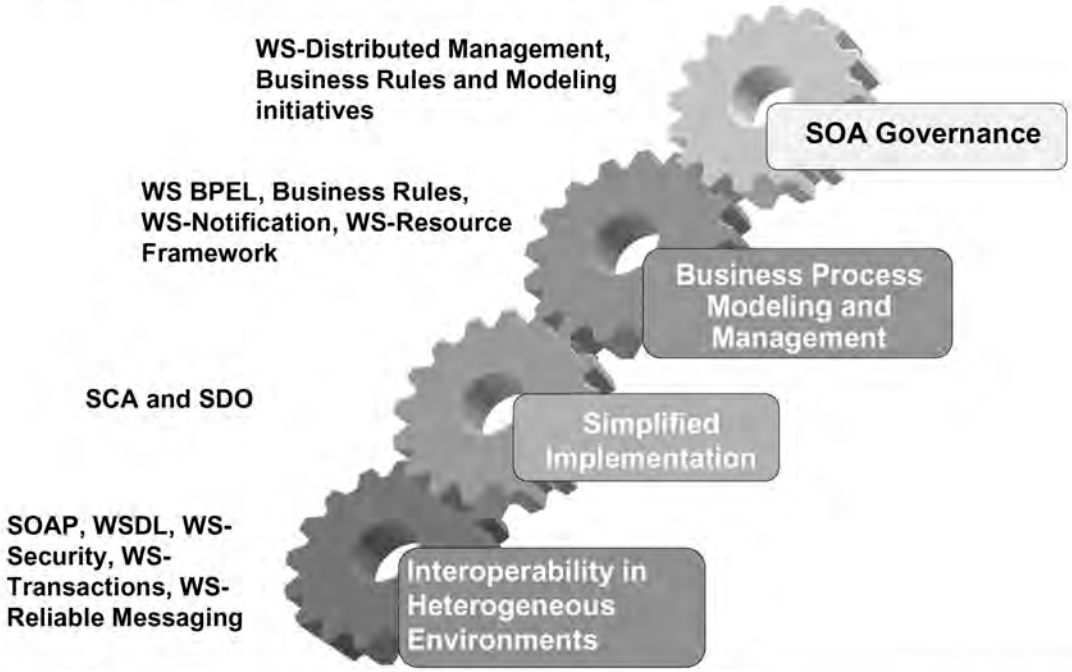


- 企業トランスフォーメーション
- オートノミックなIT管理技術を土台にして
- オートノミックビジネスマネジメント

SOA Infrastructure Standards Roadmap



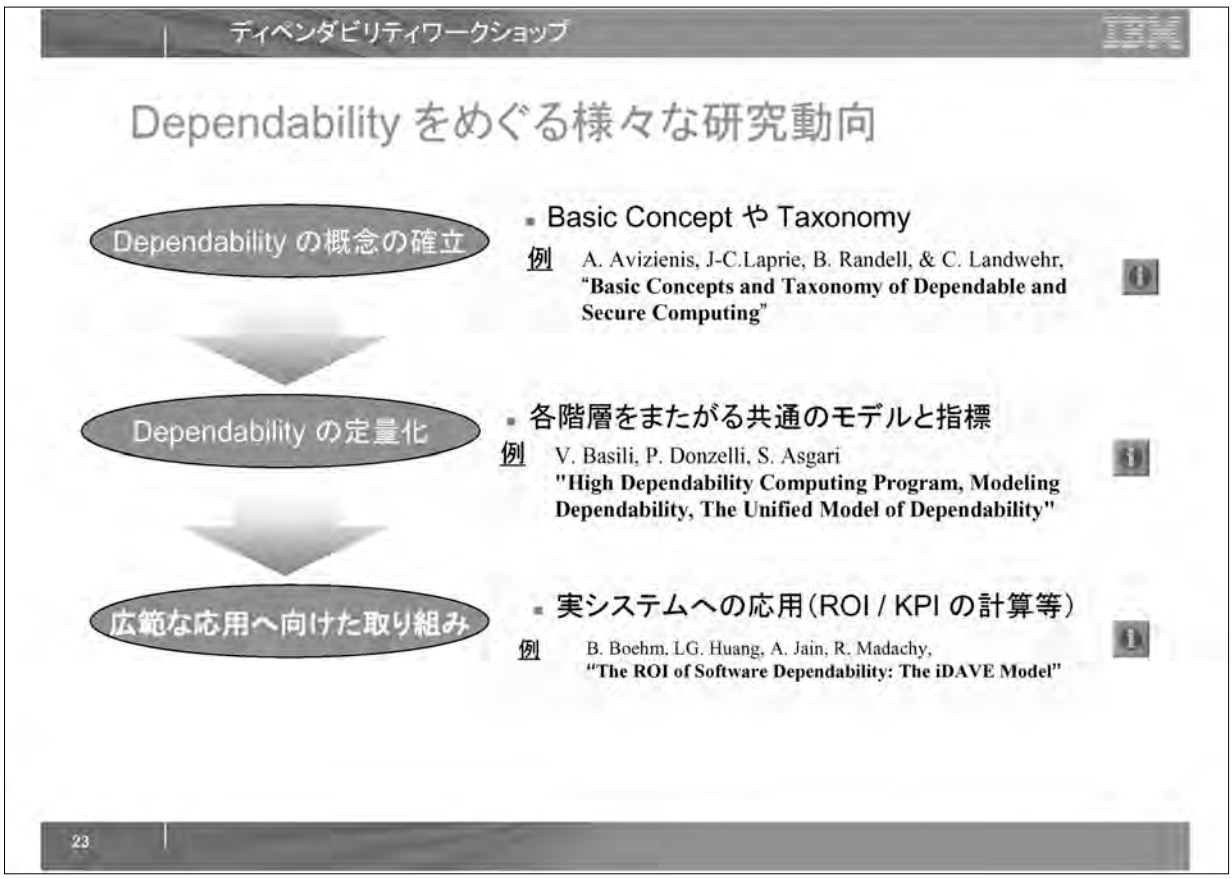
SOA Infrastructure Standards Roadmap



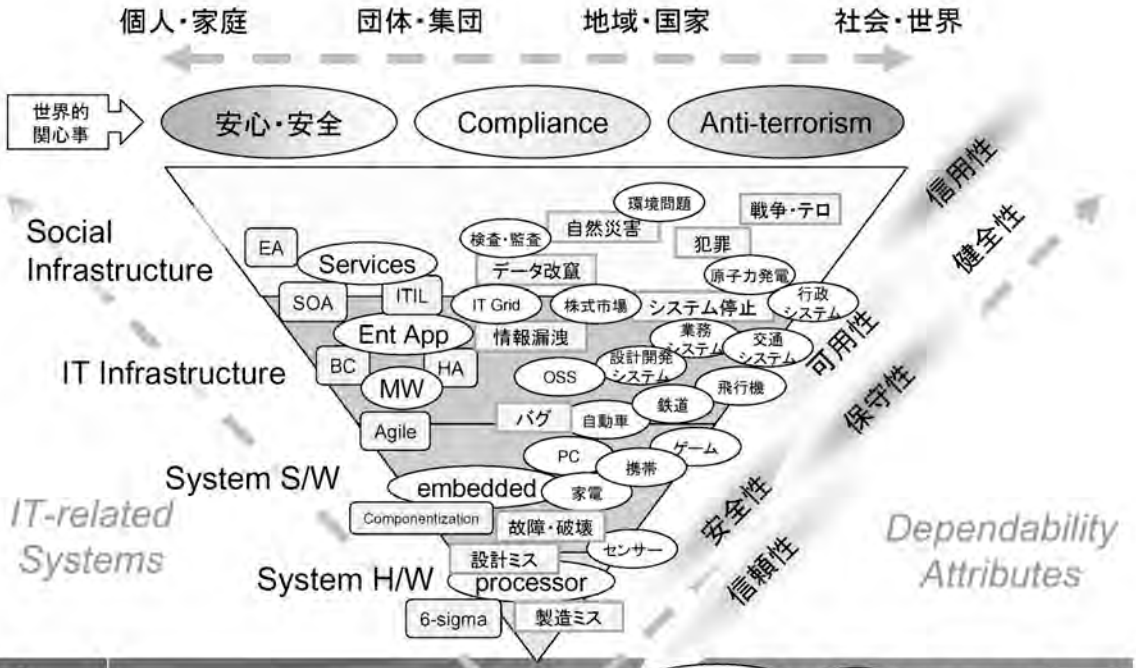
Web Services – a Simple View

Business Processes	Business Process Execution Language For Web Services (BPEL4WS)			
Quality of Service	Reliability	Transactions	Management	Security
Description	Web Services Description Language (WSDL)			
Messaging	Simple Object Access Protocol (SOAP)		Other Protocols Other Services	
	Extensible Markup Language (XML)			


ディペンダビリティワークショップ
Challenges Ahead
Architecture
Metering, monitoring & control
Metrics, Time units
Human system interface
Life cycle of autonomic elements
Multi-agent learning & negotiation/conflict resolution
Optimization & prediction
Continuous operations
Software Engineering
Testing, verification, robustness
Software tools
Problem determination
Standard, Open Source
Federated System
Availability, fault tolerance & recovery
Policies, SLA, and SLO, Impact Prediction/Analysis
End to end security
Theory
Distributed resource management & scaling
Peer system interaction
Protocol, Information
Context awareness
Global state, Prediction
Societal Issues
Cultural change & trust
Insurance, Liability
Law, Compliance, Social
22


ディペンダビリティワークショップ
Dependability をめぐる様々な研究動向
Dependability の概念の確立
Basic Concept や Taxonomy
例 A. Avizienis, J-C.Laprie, B. Randell, & C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing"
Dependability の定量化
各階層をまたがる共通のモデルと指標
例 V. Basili, P. Donzelli, S. Asgari "High Dependability Computing Program, Modeling Dependability, The Unified Model of Dependability"
広範な応用へ向けた取り組み
実システムへの応用(ROI / KPI の計算等)
例 B. Boehm, LG. Huang, A. Jain, R. Madachy, "The ROI of Software Dependability: The iDAVE Model"
23

Dependability の広がり



Service Dependabilityに向けて

- **Definition**
- **Scope**
- **Metric, Monitor, Policy**
- **Architecture, Sense and Respond**
- **Societal System**

2. 5 自動車におけるディペンダビリティについて

自動車におけるDependabilityについて

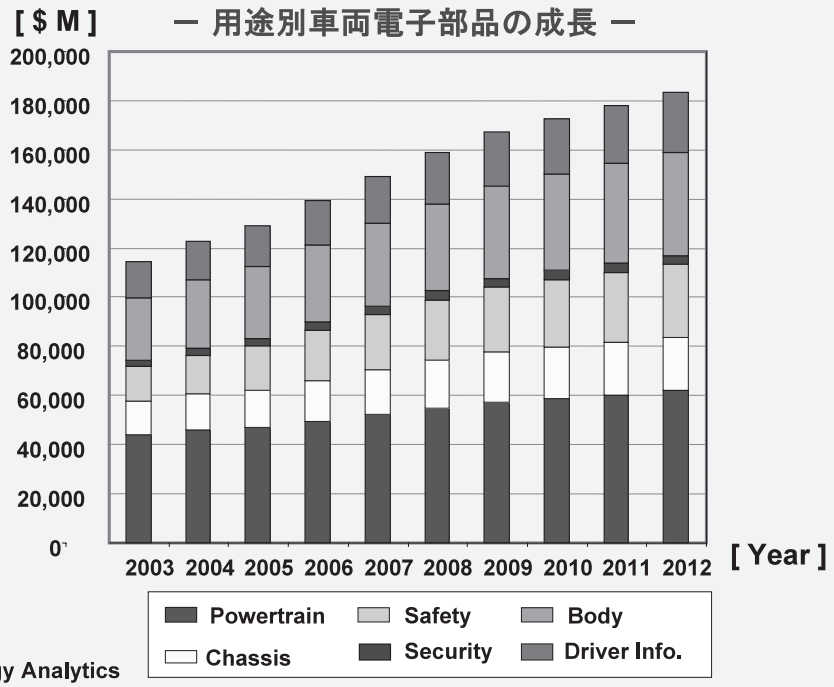
トヨタ自動車株式会社
第3電子技術部 第31電子室
服部雅之

TOYOTA

Toward Realization of Sustainable Mobility Society

TOYOTA

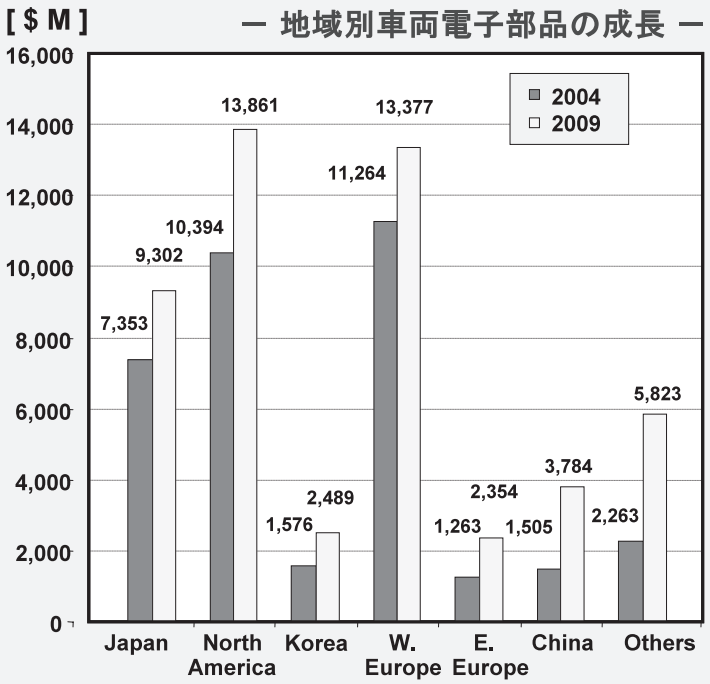
車両電子部品の成長（1）



Source:Strategy Analytics

TOYOTA

車両電子部品の成長（2）



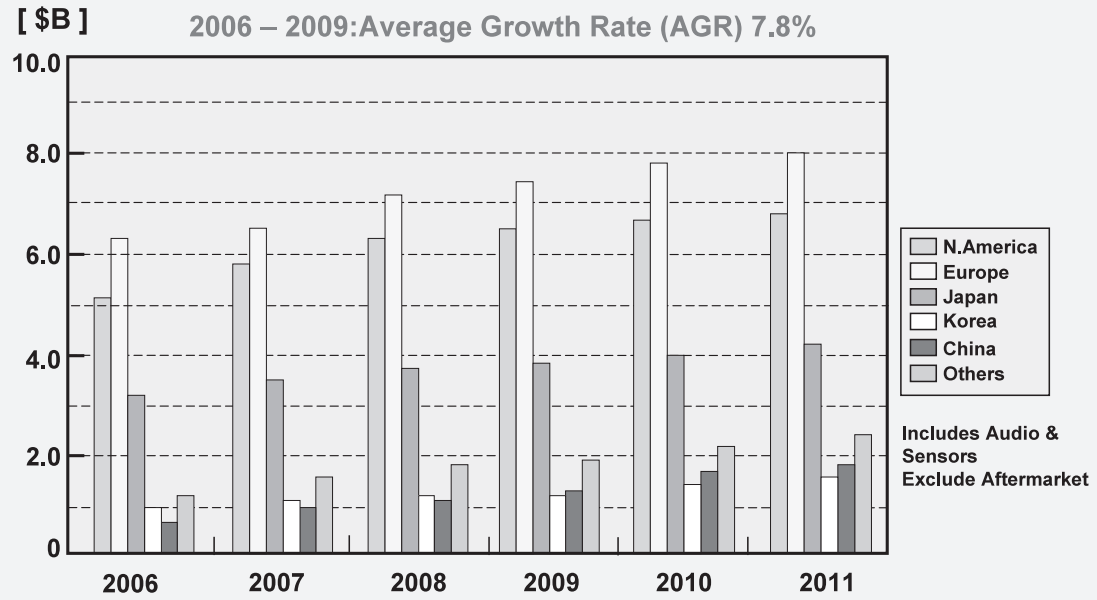
AGR 2004 – 09

- Japan : 4.8%
- NAFTA: 5.9%
- South Korea: 9.6%
- W. Europe: 3.5%
- E. Europe: 13.3%
- China: 20.2%
- Others: 20.8%
- Overall: 7.4%

Source:Strategy Analytics

TOYOTA

車載半導体の市場（1）

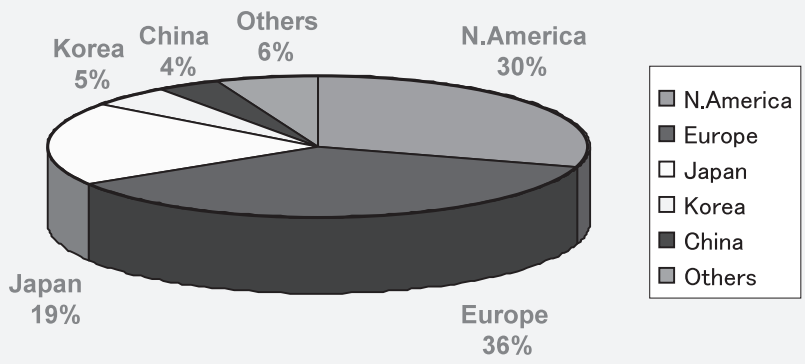


Source: Strategy Analytics

TOYOTA

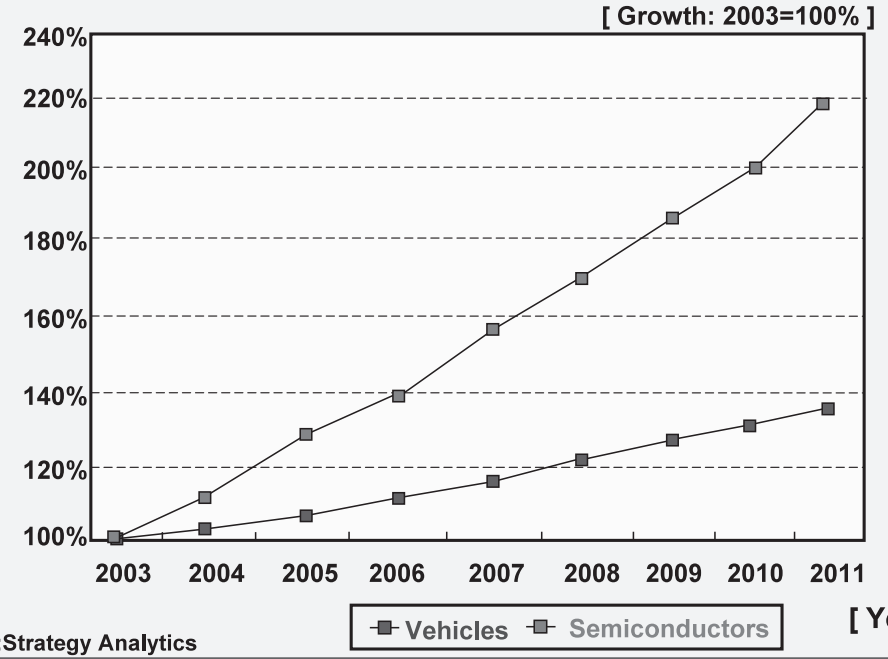
車載半導体の市場（2）

ー 地域別車載半導体のニーズ ー
(2005)



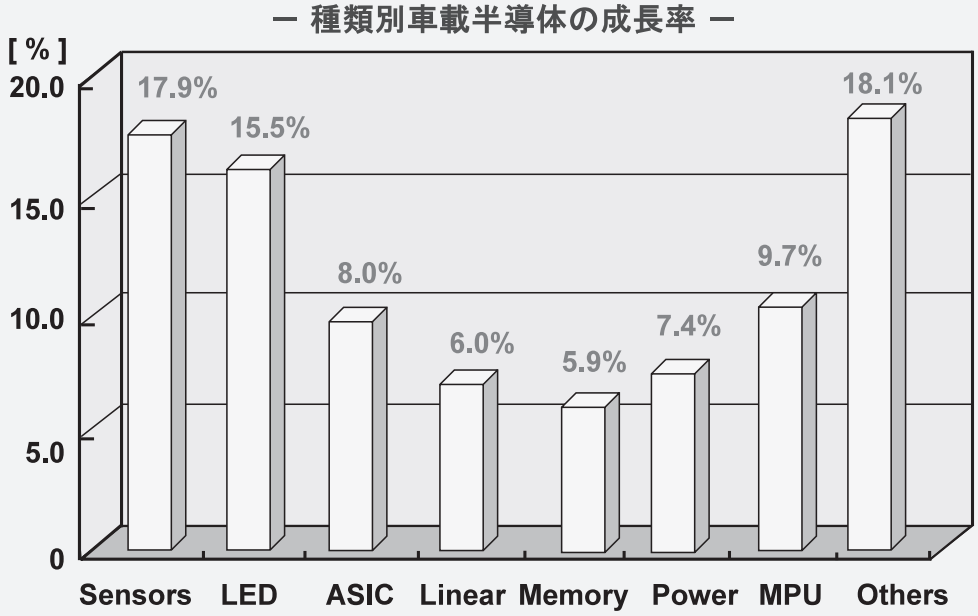
TOYOTA

車載半導体の成長（1）



Source:Strategy Analytics

車載半導体の成長（2）

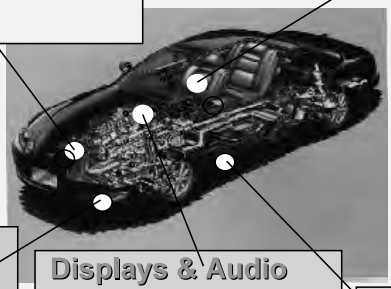


Source: Strategy Analytics

カーエレクトロニクス

Engine & Power Train
EFI (Electronic Fuel Injection)
KCS (Knock Control System)
ECT (Electronic Controlled Transmission)
ACC(Active Cruise Control)
HV(Hybrid Vehicle Control)
CVT,Engine Mount
Cooling Fans

Comfort & Convenience
Climate Control
Power Seat
Preset Steering Wheel Position
Power Windows
Liquid Crystal Glare proof Mirror
Back Guide Monitor
Door Lock Control
Night View
Keyless,Remote Engine Starter
Immobilizer



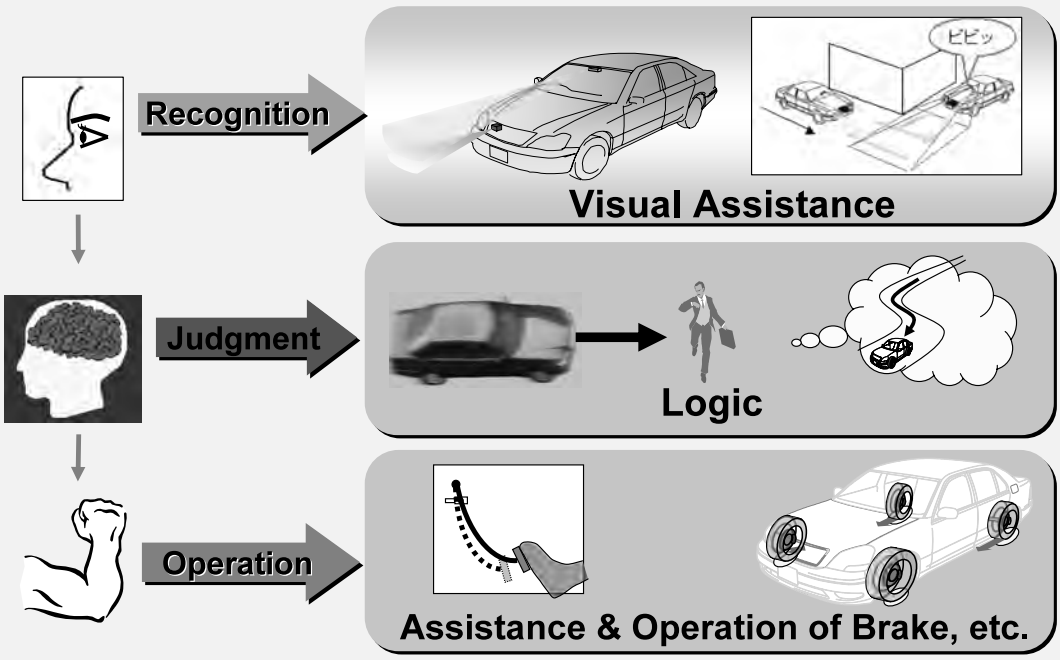
Chassis & Safety
Active Control Suspension
Active 4WS (4-wheel Steering)
ABS (Anti-lock Brake System)
TRC (Traction Control)
VSC (Vehicle Stability Control)
VDM(Vehicle Dynamic Control)
PCS(Pre-Crash System)
Ultra-Sonic Sensing

Displays & Audio
Electron Multi-Vision
Navigation System
Television
Super Live Sound System
Cellular Mobile Telephone
Digital TV,FMAM
HUD

Signal Communications & Wiring Harness
Multiplex Communication System
Diagnosis
Starter,Alternator,Battery
VICS,ETC

TOYOTA

Themes of Engineering Development

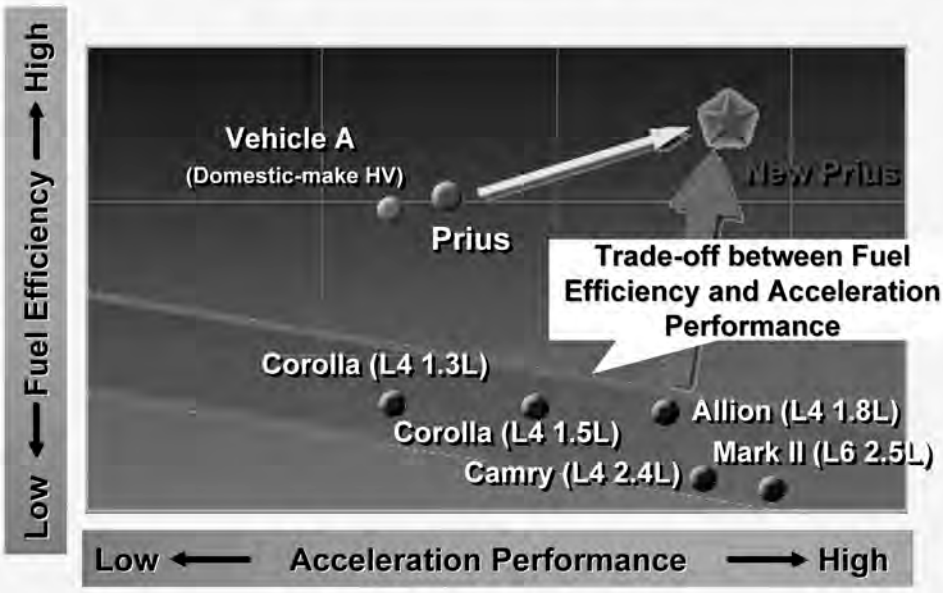


TOYOTA

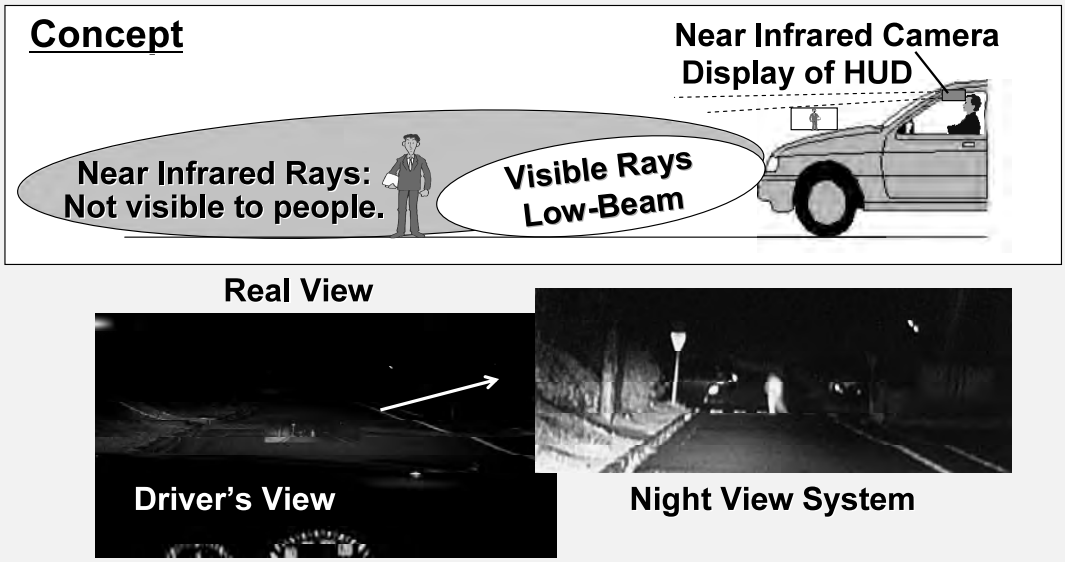
Hybrid System（THSⅡ）

Power control unit

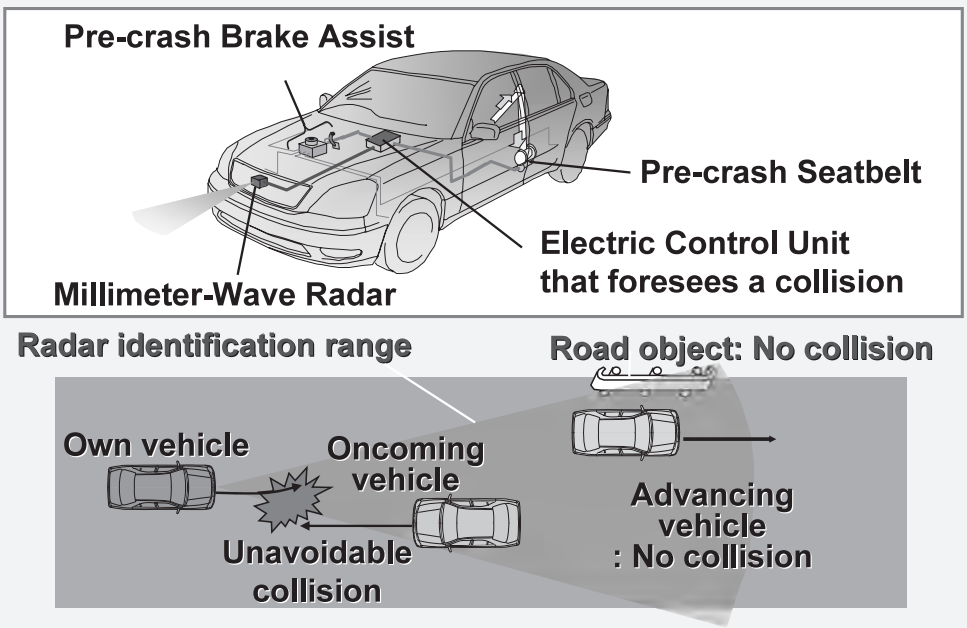
燃料効率と加速性能



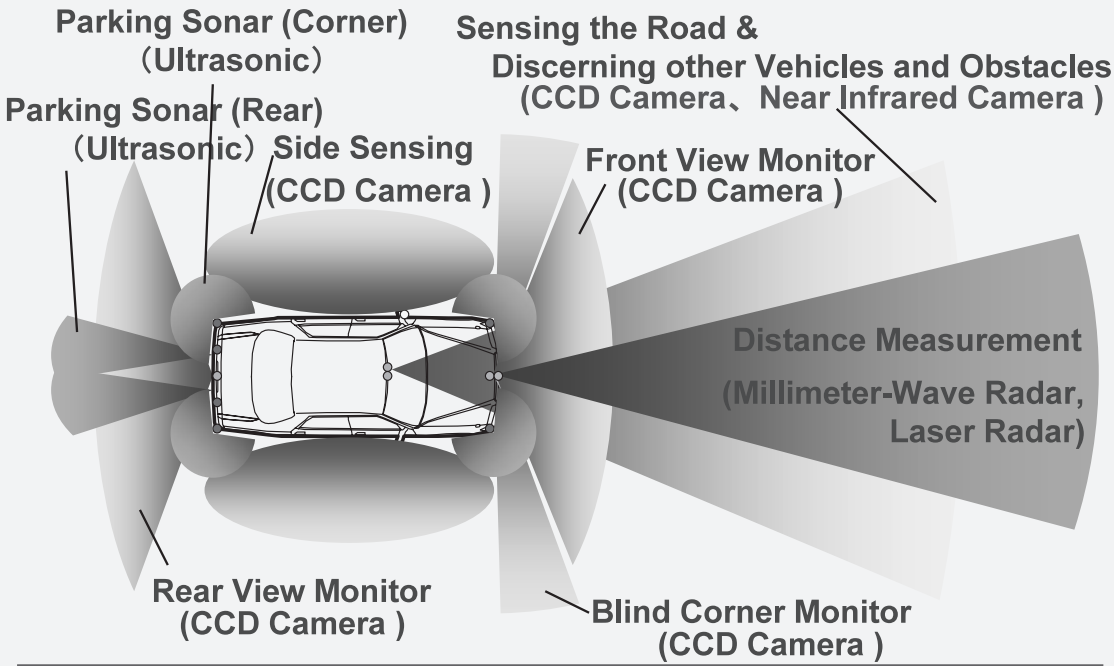
Night View System



Pre-crash Safety System

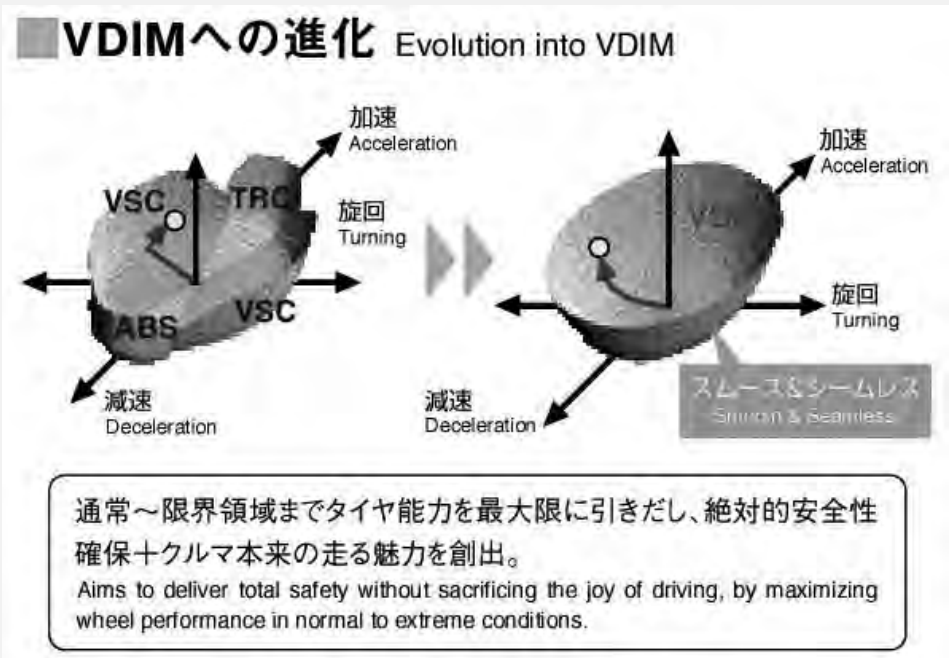


Surrounding Monitor Systems

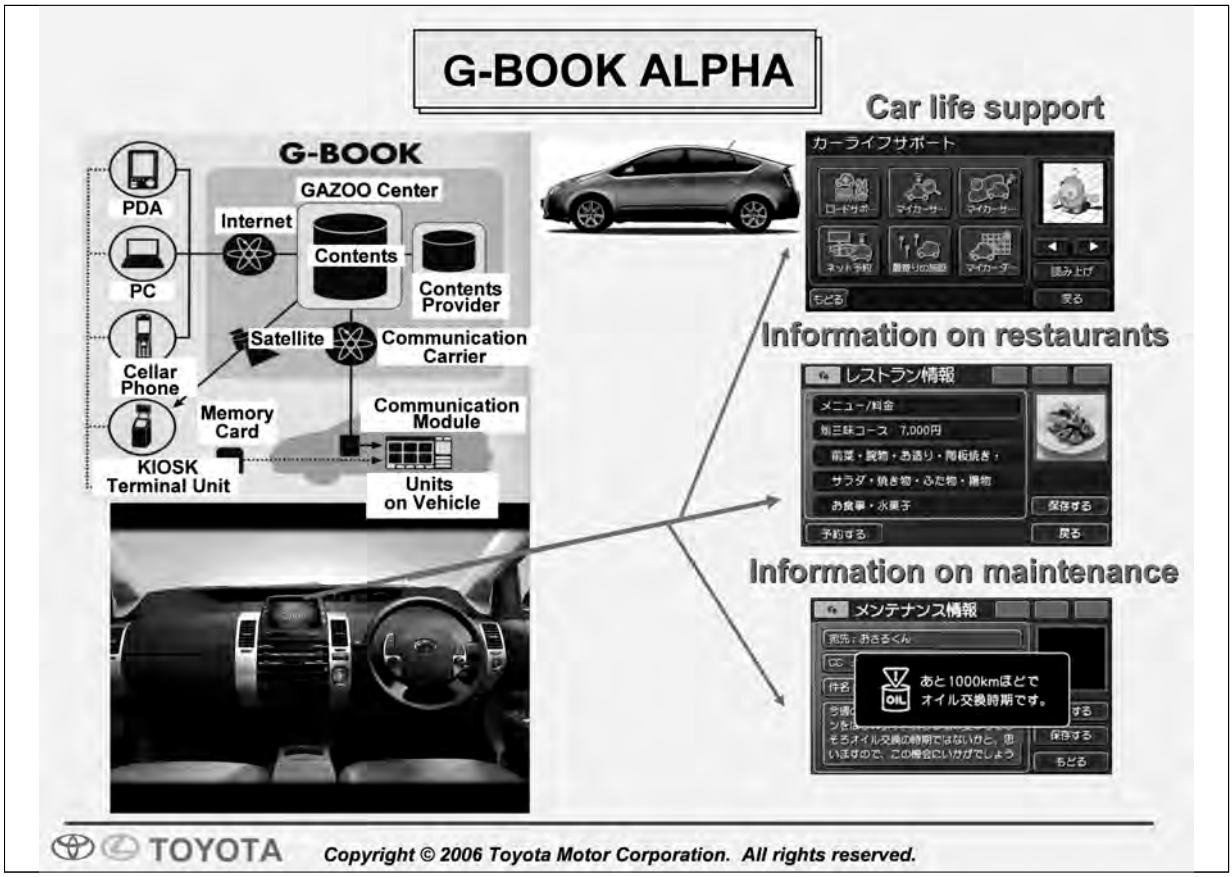


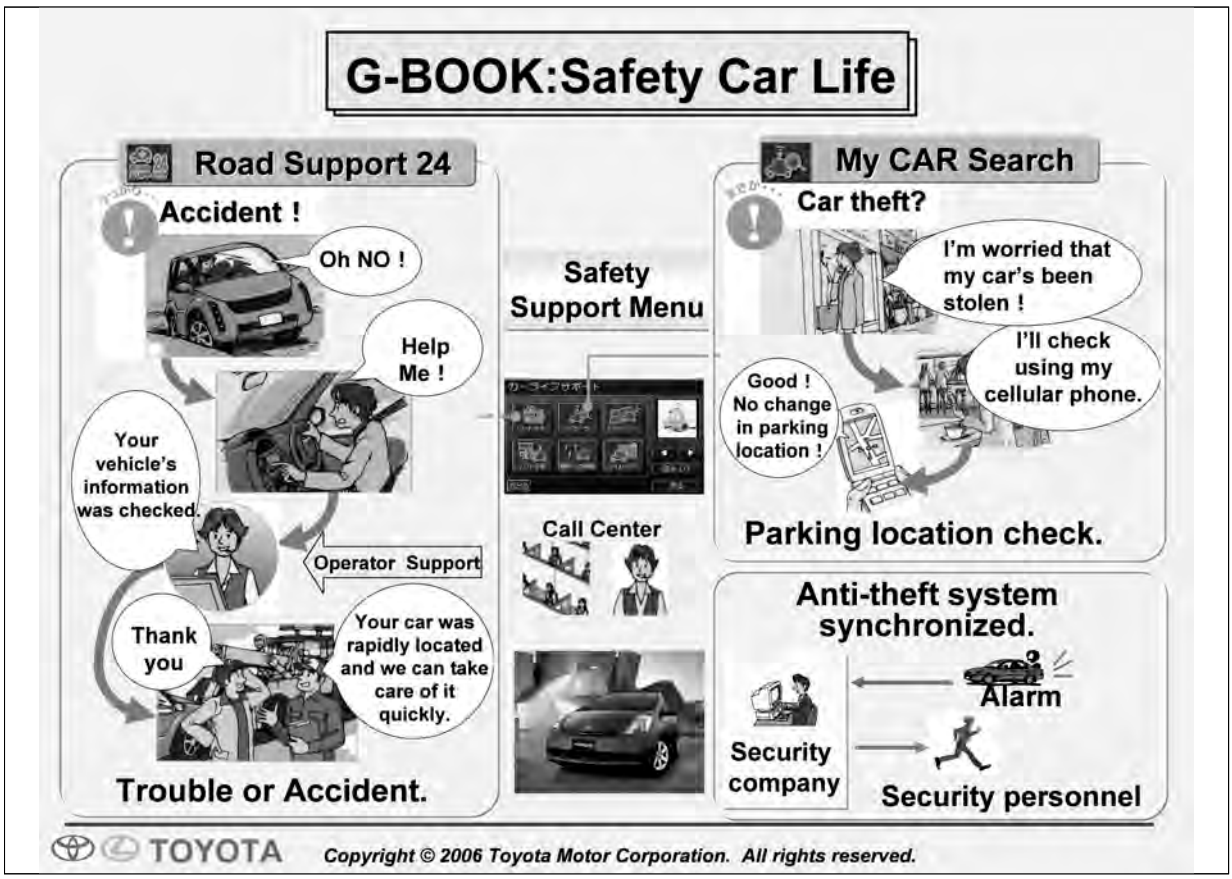
TOYOTA

VDIM System



TOYOTA


G-BOOK ALPHA
G-BOOK
PDA
PC
Cellar Phone
KIOSK Terminal Unit
GAZOO Center
Internet
Contents
Contents Provider
Satellite
Communication Carrier
Memory Card
Communication Module
Units on Vehicle
Car life support
カーライフサポート
Information on restaurants
レストラン情報
Information on maintenance
メンテナンス情報
あと1000kmほどで
オイル交換時期です。
TOYOTA
Copyright © 2006 Toyota Motor Corporation. All rights reserved.


G-BOOK:Safety Car Life
Road Support 24
Accident !
Oh NO !
Help Me !
Your vehicle's information was checked.
Operator Support
Thank you
Your car was rapidly located and we can take care of it quickly.
Trouble or Accident.
Safety Support Menu
Call Center
My CAR Search
Car theft?
I'm worried that my car's been stolen !
I'll check using my cellular phone.
Good ! No change in parking location !
Parking location check.
Anti-theft system synchronized.
Alarm
Security company
Security personnel
TOYOTA
Copyright © 2006 Toyota Motor Corporation. All rights reserved.

ITS and the Ubiquitous Network

TOYOTA

Safety | Environment | Convenience

Automotive Telematics Network

TOYOTA

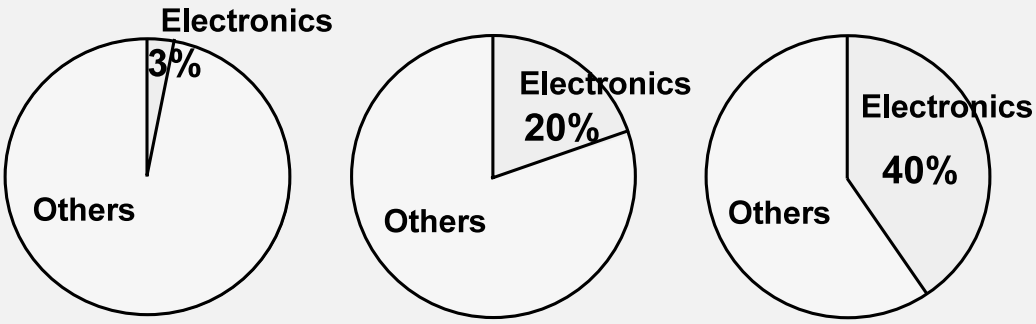
車両電子部品の比率の推移

～1980年 → 2005年 → 2015年～

ステレオ、エアコン、ワイパー
ランプ、バッテリー、ヒータファン

ABS、TRC、EPS、VDIM
パワトレ制御、ナビ、エアバッグ

自動走行、衝突検知、
テレマ、乗員検知、X-By-Wire



補助的機能　周辺的機能　本質的機能

TOYOTA

必要な演算性能

パワトレ制御
ﾃﾞｼﾞﾀﾙ処理　ﾓﾃﾞﾙﾍﾞｰｽ　燃焼圧制御
高度排ｶﾞｽ処理　HV制御　FC制御
ﾊﾟﾜﾄﾚ統合制御　車両統合制御

予防・衝突安全
ACC制御　白線検知　ｽﾃﾚｵ画像処理
乗員検知　衝突回避
ﾌﾟﾘｸﾗｯｼｭ　ﾅﾋﾞ協調運転　自動走行　人工知能

安心・快適
ITS/ｲﾝﾌﾗ協調　渋滞回避走行　ｲﾝﾌﾗ誘導走行
G－BOOK　3Dｸﾞﾗﾌｨｯｸｽ　ﾌﾞﾛｰﾄﾞﾊﾞﾝﾄﾞ接続

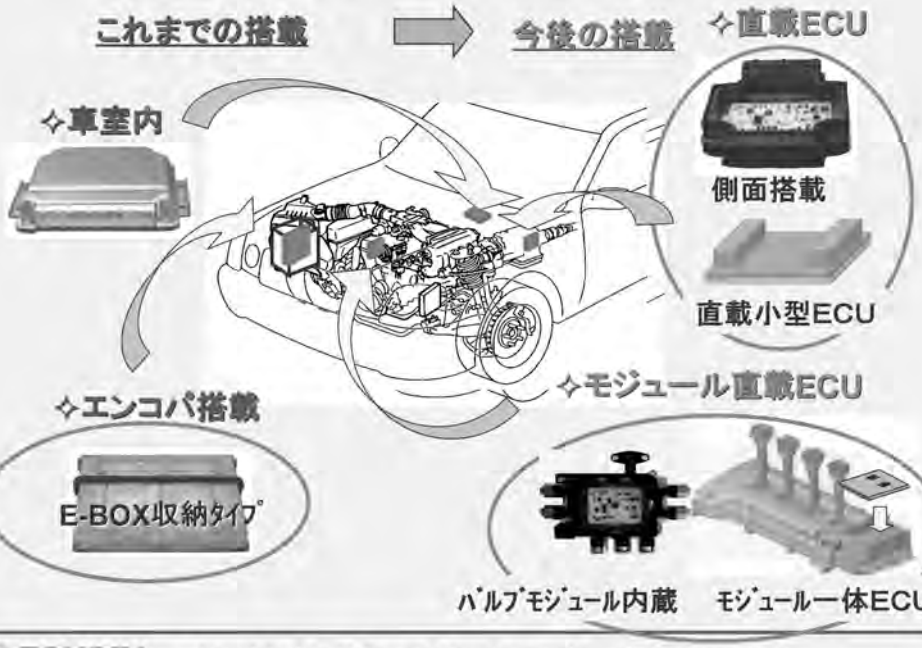
必要処理性能　100DMIPS　1DGIPS　10DGIPS

TOYOTA

車両電子部品の技術動向(1)

高温対応・小型化技術開発が必須

これまでの搭載 ➡ 今後の搭載



TOYOTA

車両電子部品の技術動向(2)

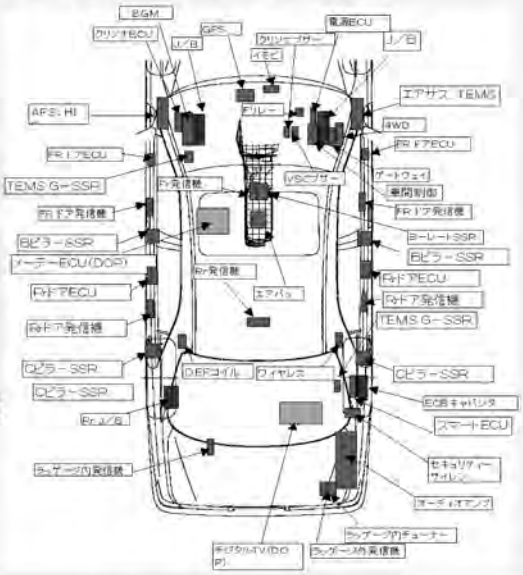
車両電子システムの増大に伴い、ECU搭載スペースが厳しくなっており、
次世代車両成立に向け、ECUの小型化・標準化が必須な状況

クラウン クラス

ECU計60個以上

('06年車種では、70～80個)

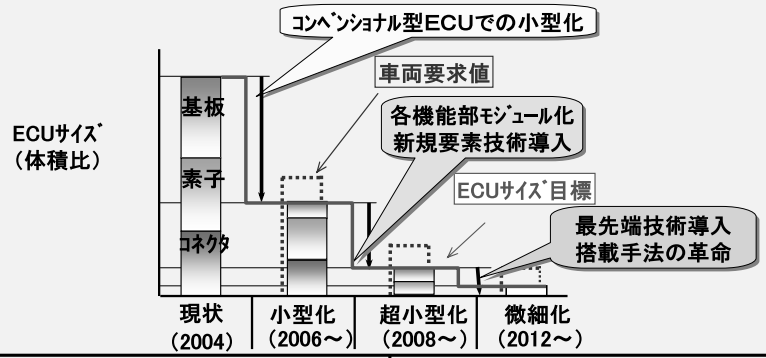
・単独配置検討は限界
・統一した設計思想による効率化
　⇒設計・素子の標準化
・ECUサイズの小型・標準化が必要
　⇒小型ICパッケージ・実装技術開発
・民生を超えた先端技術が必要

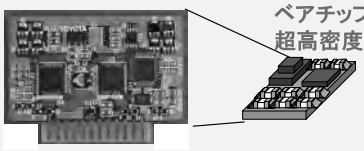
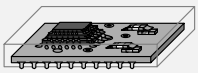


TOYOTA

車両電子部品の技術動向(3)

ECU小型化が待ったなしの状況:高集積化/高密度実装

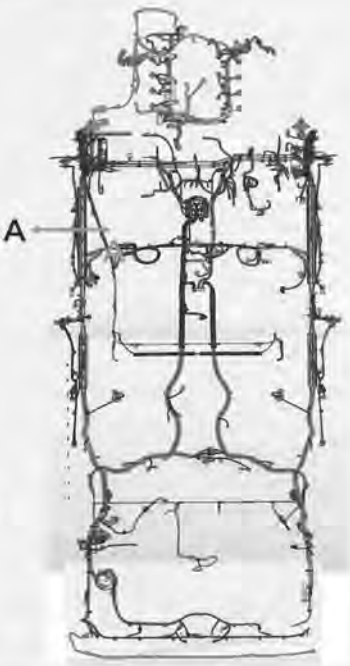


2008 超小型化	2010 ～微細化
 ベアチップ実装 超高密度実装 体積1/N (面積1/L×高さ1/H) 耐熱125℃	 SiP化 体積1/M (面積1/K×高さ1/H) 耐熱125℃
モジュール化	ワンチップECU

車両電子部品の技術動向(4)

WHの増加が車両設計を圧迫

- WHが肥大化し配策困難
- 変更を見越した余裕が必要



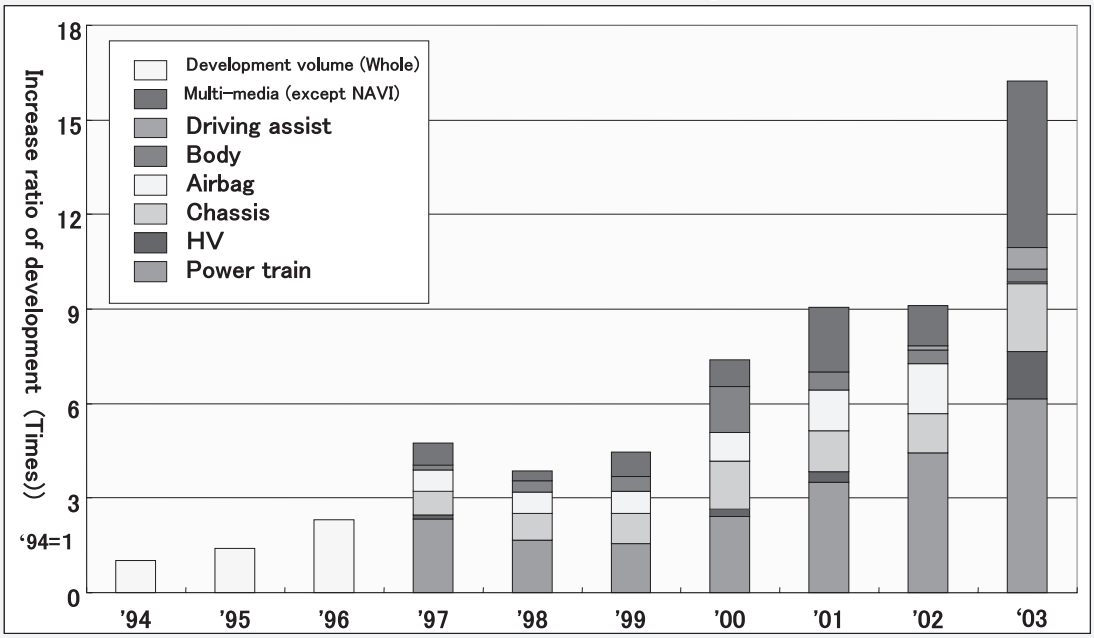
- 多重通信採用と全体回路見直しでWH削減要
- ECUの複合化

断面積比100%

変更を考慮し20%の余裕必要

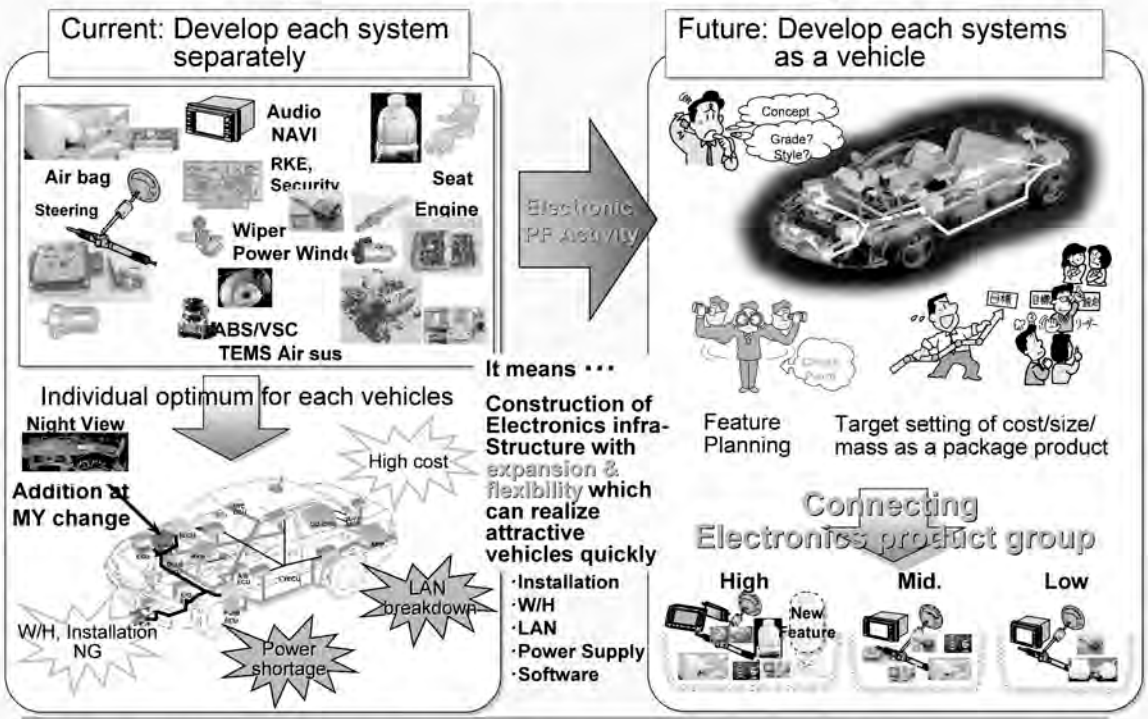
車両電子部品の技術動向(5)

Increase of Software Development Volume



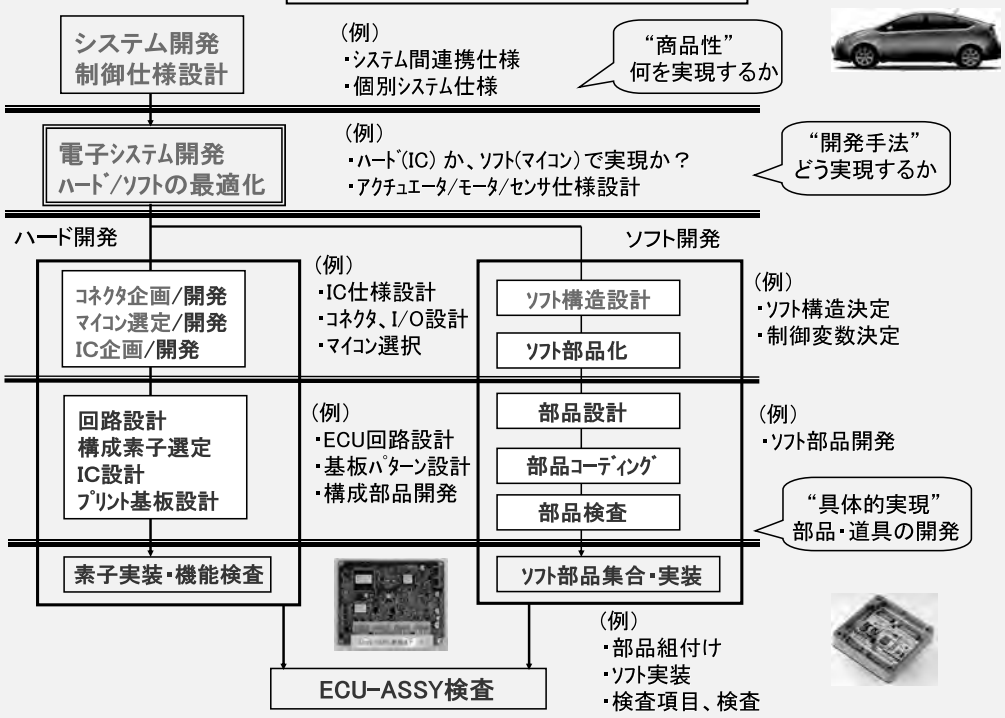
TOYOTA

Electronic Platform



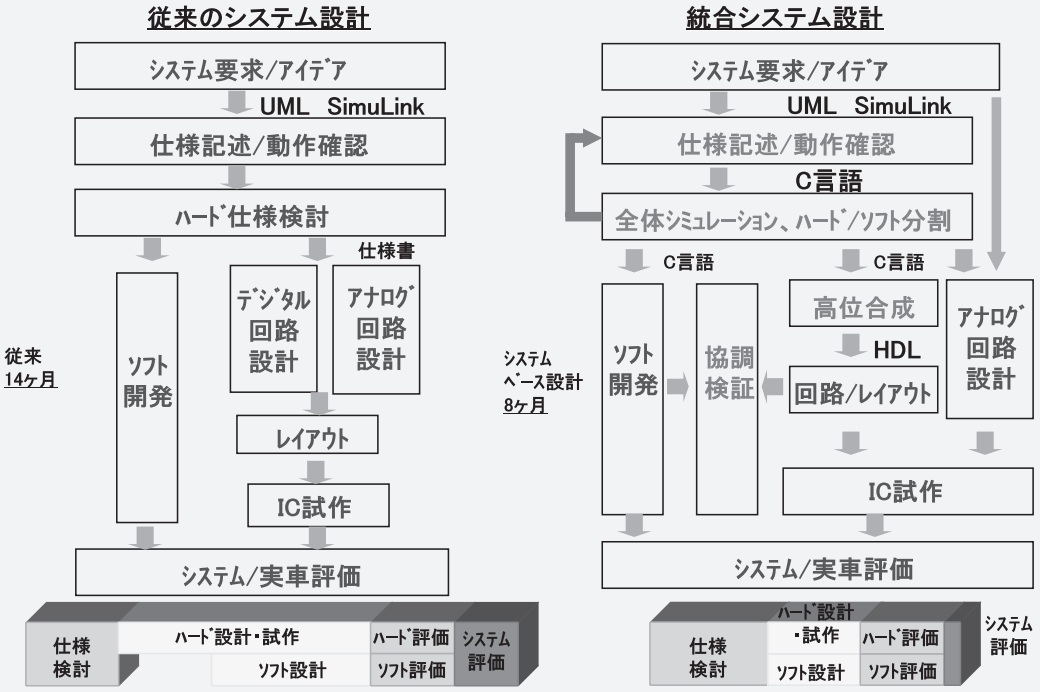
TOYOTA

電子システム開発工程



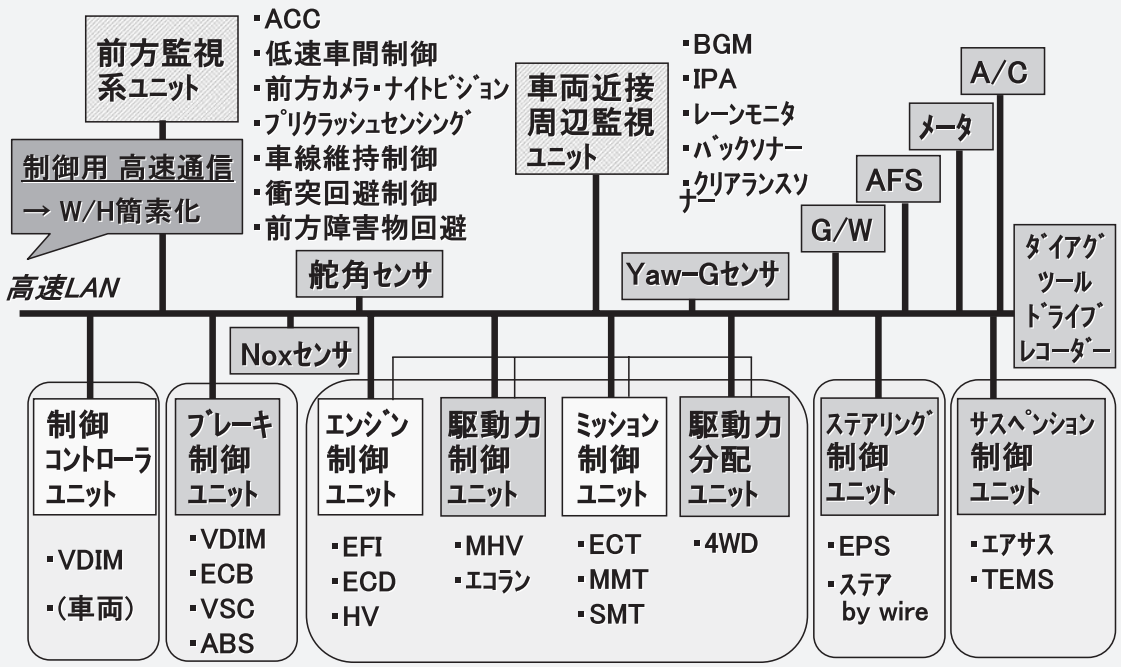
TOYOTA

車両制御用ICの新規開発フロー



TOYOTA

制御ECU全体の将来図



車両制御用半導体の役割

1）ECUの小型化、統合化

- 最先端半導体技術を用いた小型・高品質・高信頼ICの実現
- システム設計からIC設計までスルーで開発出来る設計手法の確立
- デジタル/アナログ/パワー素子のシステム最適な複合化
- 小型/高信頼性パッケージと、それを実装できるプリント基板の実現

2）ECUのユニット/モジュール一体化

- 小型化、高信頼性化
- デジタル/アナログ/パワー素子のシステム最適な複合化
- モジュール実装に最適なICパッケージ

3）インテリジェントアクチュエータ化

- 低損失素子、高温対応化、高信頼性化
- デジタル/アナログ/パワー素子のシステム最適な複合化
- モジュール実装に最適なICパッケージ

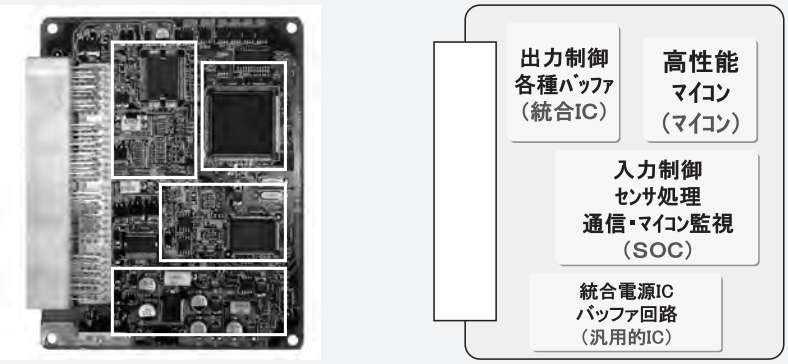
車両ECU用半導体開発

車両制御ECU用半導体の内訳

マイコン、統合IC（出力制御IC、入力制御IC、ﾏｲｺﾝ監視）、
センサ信号処理、統合電源IC、各種汎用IC（ﾛｼﾞｯｸ、ﾊﾟﾜｰMOS）

⇒1）マイコン、2）統合IC、3）SOC*（ASIC）、4）汎用的ICに分類

*SOC：System On Chip



エンジン制御ECUの事例

車両半導体開発の動向

1）マイコンは高性能化・コアの標準化が進展
- ⇒標準化か独自高性能化か判断が必要
- ⇒車両制御ｿﾌﾄ構造に最適なCPUｺｱの開発（ARM）が進展

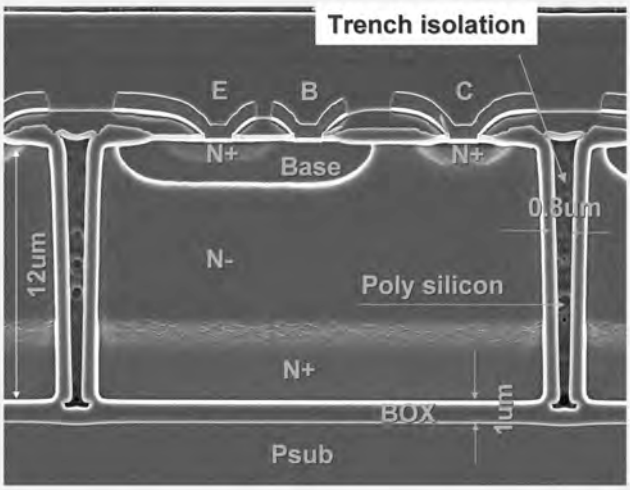
2）統合ICはｱﾅﾛｸﾞ、ﾃﾞｼﾞﾀﾙ、ﾊﾟﾜｰの複合高集積化が進展
- ⇒ECUのｺｽﾄ、性能、小型化を決める重要技術
- ⇒設計/製造技術を蓄積する事で性能差別化が可能

3）先端システムを実現するSOCは短期開発が必須
- ⇒開発のｽﾋﾟｰﾄﾞがｼｽﾃﾑの勝敗を決定
- ⇒ﾊｰﾄﾞ/ｿﾌﾄとの最適分担による機能最適化が必要
- ⇒ｼｽﾃﾑ開発からIC開発までｽﾙｰに設計する環境が必要

4）汎用的ICは枯れた技術で安く長く作り続ける事が必要
- ⇒数世代前のﾌﾟﾛｾｽ技術でも製品設計可能なｲﾝﾌﾗ整備
- ⇒枯れた技術とは言え車載IC品質の確保が必須
- ⇒開発IPの流用と低ｺｽﾄ生産の実現

統合ICプロセス技術

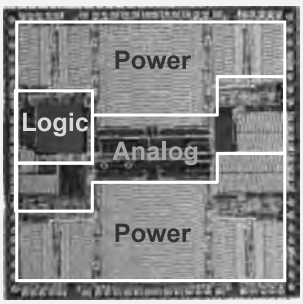
ー 小型/高温対応のためSOI構造が有利 ー

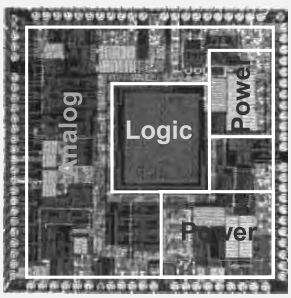


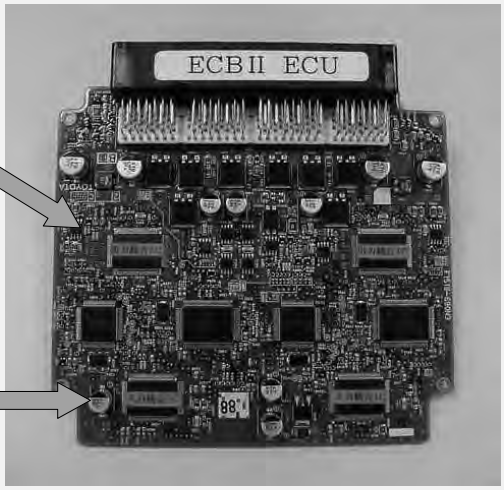
TOYOTA

統合IC開発事例

High Integration SOI ICs for Brake Systems





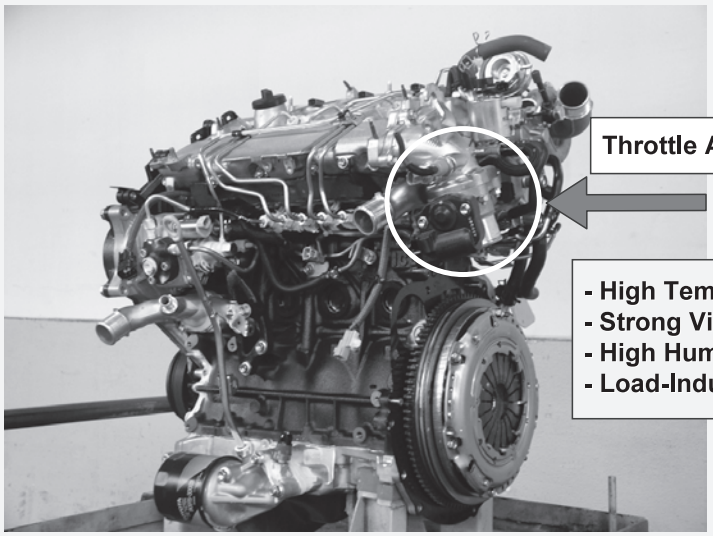


TOYOTA

インテリジェントアクチュエータ技術

TOYOTA

Photomicrograph of TOYOTA Diesel (1CD-FTV:2.0L) Engine



TOYOTA

Toyota Luxury Class Automobile Engine Room

TOYOTA

信頼性技術（1）

Location	Max Temp.	Vibration Level	Fluid Exposure
On Engine On Transmission	>140℃	30G	Harsh
At the Engine (Intake Manifold)	125℃	20 - 30G	Harsh
Under hood Near Engine	120℃	10G	Harsh
Under hood Remote Location	110℃	10G	Harsh
E-Box	105℃	3 - 5G	Benign
Passenger Compartment	85℃	3 - 5G	Benign

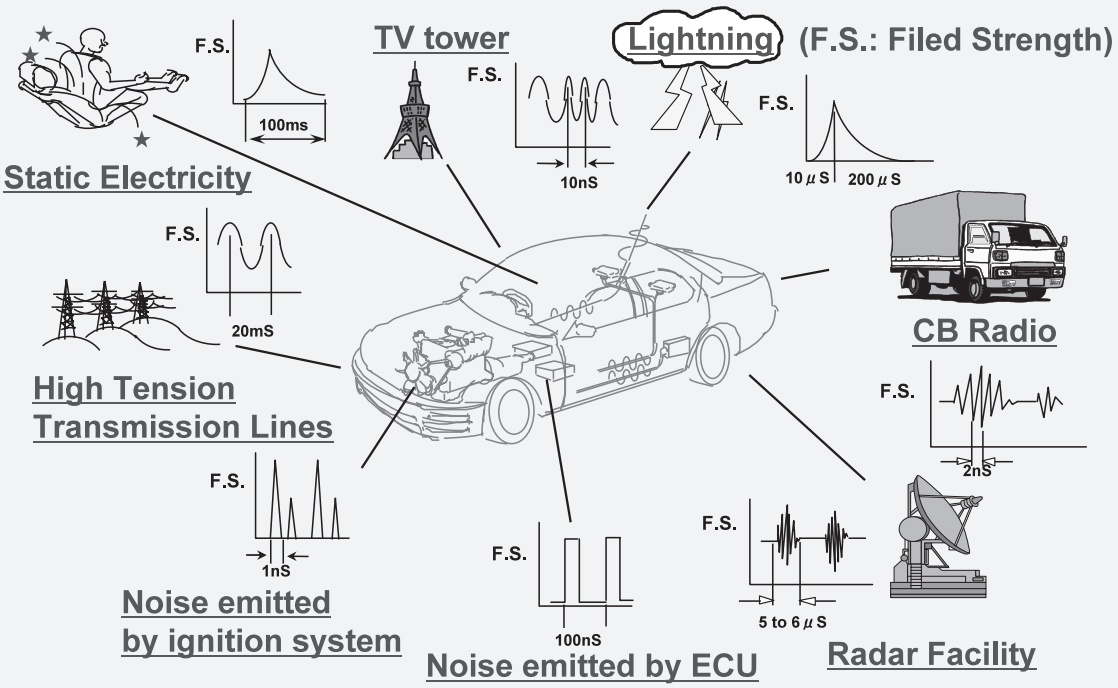
TOYOTA

信頼性技術（2）

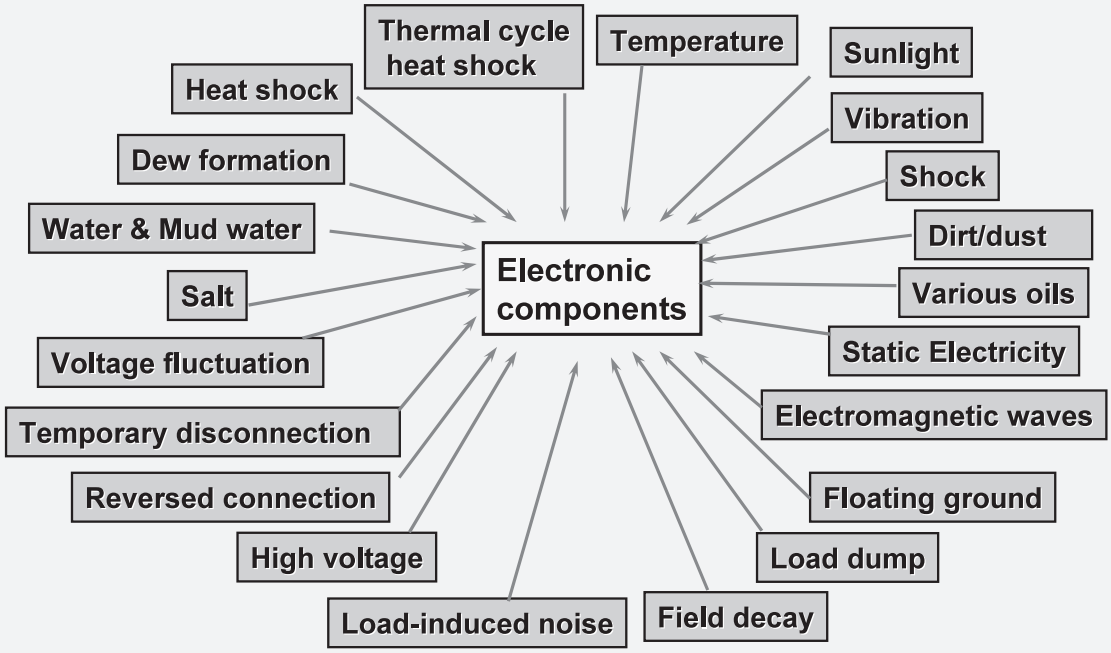
		Home Electronics	Aircraft	Automobile
Environment items	Accuracy	Several %	0.1 to 1%	0.1 to 1%
	Temperature range of operation	0 to70℃	-65 to 350℃ *	-40 to +140℃
	Vibration	5G	20G *	25G
	Fluctuation of power supply	±10%	±10%	±50%
	Electromagnetic environment	Good	Good	Bad
	Other	Water	Salt water	Salt water, Exhaust gas

＊MIL STD 446 the 7th group

Electromagnetic Environment



Environment of Electronic Components



TOYOTA

車載部品への要求

1). High Reliability under Severe Conditions
- High Ambient Temperature
- Severe Thermal Cycle
- High Vibration Level

2). High Quality
- Zero Defect Concept
- Continuous "KAIZEN" Approach

3). High Cost Efficiency
- Low Cost by High Technologies
- Small Size and High Integration

4). Short Device Design Cycle

5). Long Term Relationship

TOYOTA

車載部品のDependability

（1）自動車用電子システムは加速度的に複雑化が進展
⇒Dependabilityを考慮(設計指針)したシステム設計が重要
⇒外部インフラからの完全なセキュリティ確保が必須

（2）将来の自動車の性能はエレクトロニクスで決まる
⇒日本には幅広い基盤技術があり、有利な位置付け
⇒エレクトロニクス化が進むとシステムの脆弱性も高まる

（3）自動車の進化のためにはシステムの複合化が必須
⇒ Dependabilityを担保した実装技術、部品技術、
半導体技術が重要

（4）システムから半導体開発までスルーで開発出来る（ホールが無い）開発環境がDependability確保に大切
⇒最適なハード/ソフトの切り分け、設計ツールのチェーン化
⇒高精度/高速動作モデル：メカとエレキの境界

TOYOTA

CITRIS
Center for Information Technology Research in the Interest of Society

米国に於ける研究戦略動向
< CITRISにおける dependability 研究事例の紹介 >

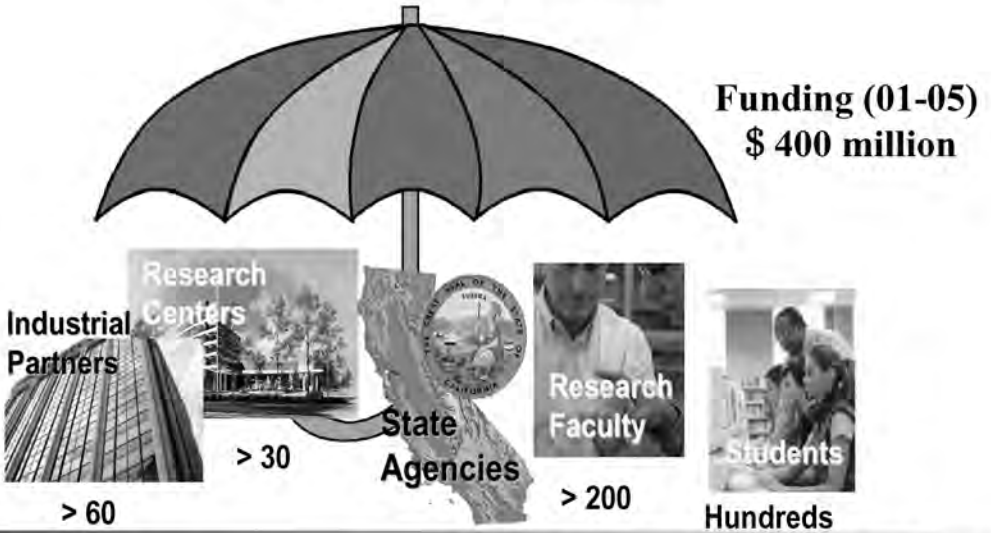
An Introduction to CITRIS,TRUST

JST Dependability Workshop
May 12,13 2006 Tokyo Japan

Takahide Inoue: < tinoue@citirs-uc.org >
CITRIS: < www.citris-uc.org >
Center for Information Technology on Interest of the Society

What is CITRIS?

Center for IT Research on Interest of the Society
It's NOT a School (学部ではありません)
It's a Institute (研究機構です)
It's a Center of Centers



CITRIS

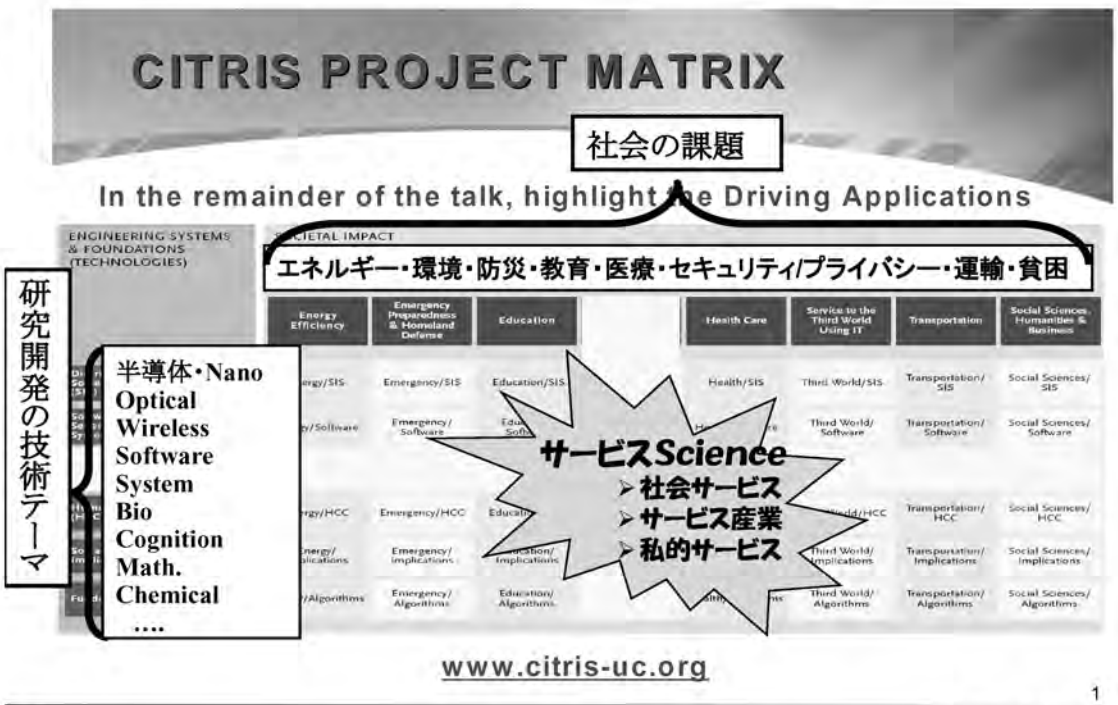
What is CITRIS (Center for IT Research in the Interest of Society)?

- CITRISは2001年にカリフォルニア大学4校（UC Berkeley, UC Davis, UC Merced, UC Santa Cruz）によって設立された研究機構 *1) です。
- その理念は“社会の課題に挑戦し、個人と社会の質を向上する為に、新しい情報技術の協同研究体を創り・育て・成果を社会に還元する場”となる事です。
- CITRISはCenter of Centersとして機能する。
- CITRISは、理念の具体化の為、次の3つの基本方針を組み合わせた新しい研究手法によって運営されています。
  - Quality of Lifeの実現に大きなインパクトを与え、その解決に情報技術が重要な役割を果たす社会的課題を見出し定義する。
  - 基礎材料・デバイス・ソフトウエアから複雑なシステム化技術（これらを総称してITと云っています）全てのレベルで広義の情報技術の英知を集積して用いる。
  - 使命達成に必要な信頼感、充足感、安全感、プライバシー、バランス感、サービス、経済性などの社会的要因をモデル化・計測し、その向上に必要となる、新しい理論の基盤原理を見出す。
- またCITRISは、カリフォルニア州政府が”次世代経済”の基盤を築く為に創った カリフォルニア大学と多くの州の主導的企業が協力する枠組み California Institute of Science and Innovation：(CISI)四機構の一つです。
  - QB3 (Quantum Biology, Biomedicine)
  - Cal IT² (Information and Communications)
  - CNSI (Nano -Technology)
- 実際にはCalifornia州/連邦政府の他、多くの企業・個人をスポンサーに持つ。

＊1）最近LBNLとLLNLが追加。

CITRIS

How CITRIS works ? ：社会の課題とIT技術のMatrix



www.citris-uc.org

1

CITRIS

How CITRIS works?:

"社会の課題に挑戦し、個人と社会の質を向上する為の新しい情報技術（IT）の協同研究体を創り・育て・その成果を社会に還元する場" である事です。

CITRIS Centers to Date

- **Berkeley Sensor and Actuator Center**
- **Berkeley Wireless Research Center**
- **Berkeley Institute for Soft Computing**
- **Gigascale System Research Center(GSRC)**
- **Davis Optical Networking Center**
- **UCSC Environmental Monitoring Center**
- **UCSC Storage Center**
- Center for Hybrid and Embedded Systems and Software (CHESS)
- Wireless Research Foundations
- Wireless EmBedded Systems (WEBS)
- Berkeley Institute of Design (BID)
- Berkeley Quantum Information and Computation Center
- Davis Center for Genomics
- UCSC led ARO_MURI Dynamic Ad-Hoc Wireless Networks (DAWN)
- UCSC led ONR-MURI Therminnic Energy Conversion Center
- UC Davis led Optical Networking center
- Process Informatics Model (PRIME)
- Davis Bio-photonics Center
- Davis Computational Science Center
- Merced Energy/Water Initiative
- Davis + Berkeley Cybersecurity (DETER + EMIST)
- Center for Intelligent Systems (CIS)
- Information and Communication Technologies for the Third World (ICT4B)
- CONSRT (Opto-Nano Electronics Center)
- COINS (Nano MEMS Center)
- Process Informatics Infrastructure (PRIME)
- Team for Research in Ubiquitous Secure Technologies (TRUST)
- Western Nanotechnology Institute (WIN)

***Those listed in Red added since CITRIS inception**

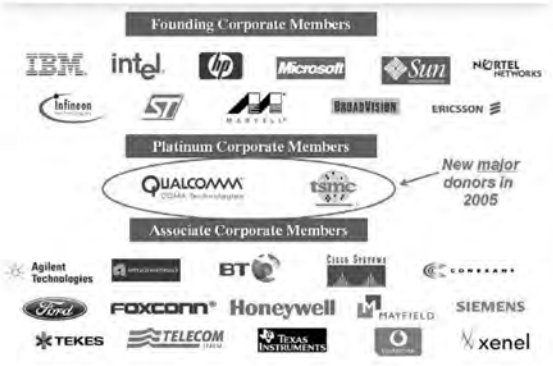
CITRIS

How CITRIS works? Partnership

Very diversified member profile

A partial list of Collaborative and Affiliate-center industrial members.

See www.citris-uc.org for complete list.



Accenture	CUREe	Lockheed Martin	Samsung
Bluesoft	Cygnal	Mesh Networks	SensiCast
BMW	Digital Sense	Millennial Net	Sensoria
Bosch	Dust Inc.	Mitre	Time Domain
Cal OES	Ember	Mobile Aria	Ubicom
Canyon Construction	FEMA	Motorola	Webraska
CENIC	France Telecom	Pangea Foundation	Wheels of Zeus
Chipcon	Honeywell	Phillips	Xerox
CommerceNet	I-Logix	Pirelli	Xsilogy
ConnecTerra	Kestrel	Port & Air Research Institute	Zeevo
Crossbow	Kiyon	Rutherford and Chekene	And More!

What is Trust (Team for Research in Ubiquitous Secure Technologies) ?

CITRIS Centers to Date

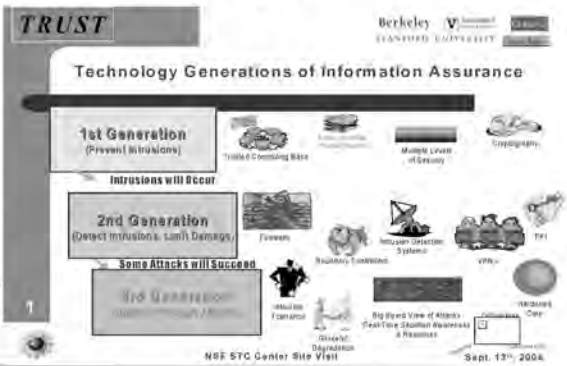
- Berkeley Sensor and Actuator Center
- Berkeley Wireless Research Center
- Berkeley Institute for Soft Computing
- Gigascale System Research Center(GSRC)
- Center for Hybrid and Embedded Systems and Software (CHESS)
- Wireless Research Foundations
- Wireless EmBedded Systems (WEBS)
- Berkeley Institute of Design (BID)
- Berkeley Quantum Information and Computation Center
- Davis Center for Genomics
- UCSC led ARO MURI Dynamic Ad-Hoc Wireless Networks (DAWN)
- UCSC led ONR-MURI Thermionic Energy Conversion Center
- UC Davis led Optical Networking center
- Process Informatics Model (PRIME)
- Davis Optical Networking Center
- Davis Biosphotonics Center
- UCSC Environmental Monitoring Center
- Davis Computational Science Center
- Merced Energy/Water Initiative
- Davis + Berkeley Cyber Physical Systems (DECYBER + EMIST)
- UCSC Storage Center
- Center for Intelligent Systems (CIS)
- Information and Communication Technologies for the Third World (ICT4D)
- CONSRT (Nano Electronics Center)
- COINS (Bio MEMS Center)
- Process Informatics Infrastructure (PRIME)
- Team for Research in Ubiquitous Secure Technologies (TRUST)
- Western Nanotechnology Institute (WIN)

*Those listed in Red added since CITRIS inception

Trust はNSFのFundを受けて2005年に発足したNSF Science & Technology Center の一つで、10年間に渡り総額 $ 40 millionの研究資金を受けて運営されている*1)。

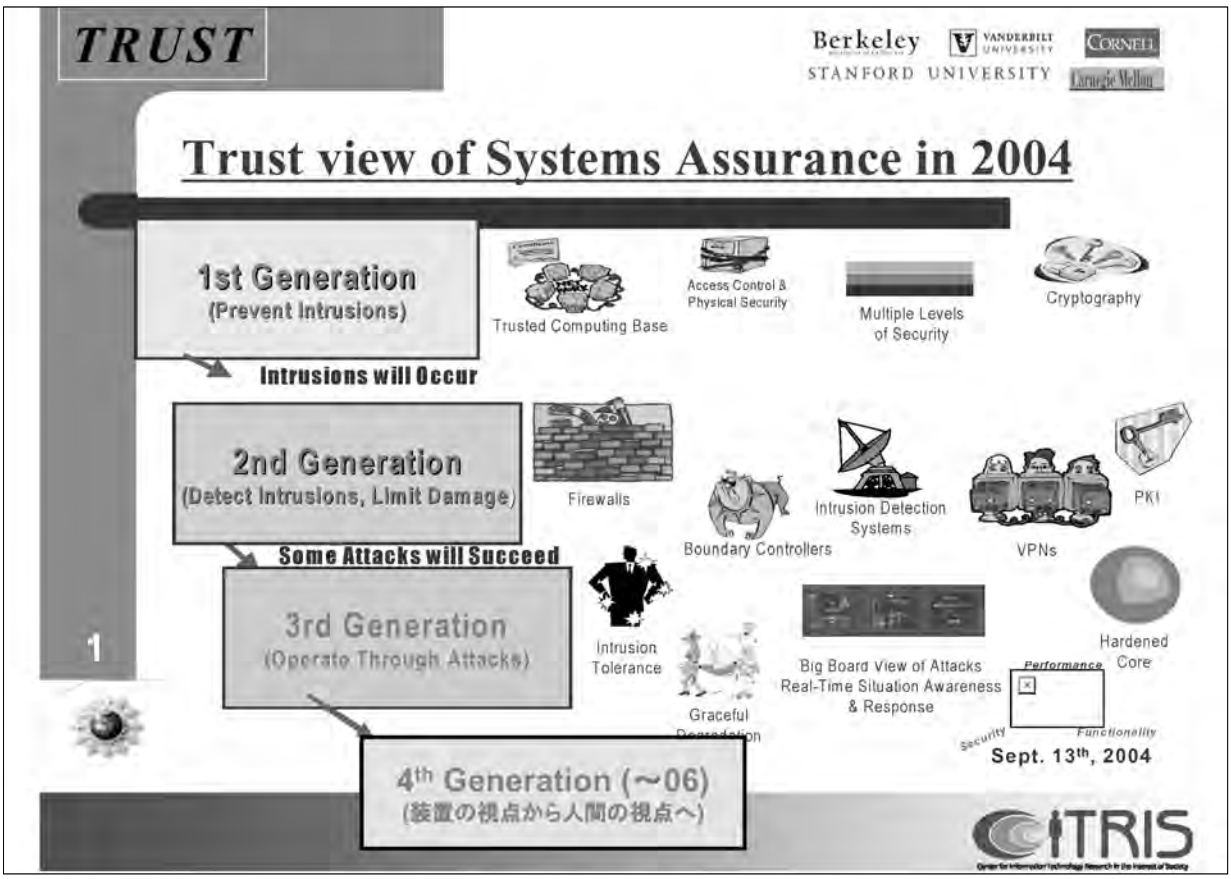
CITRISのDirector である Shankar Sastry が PI を務める事でも判る様に、その研究テーマと活動は、CITRISの影響を色濃く受けていて実際TRUSTはCITIRSの申し子の感がある。

PI: Principal Investigator



*1) TRUSTを構成する大学群

Carnegie Mellon, Cornell University, MILLS, San José State University, Smith College, Stanford University, Berkeley, Vanderbilt University



TRUST

Berkeley VANDERBILT UNIVERSITY CORNELL
STANFORD UNIVERSITY Carnegie Mellon

TRUST Worthy (Dependable) System & Society

- 通常云われる “情報システム” の概念を超えた次元にある
- 複雑多様に重なり合った概念の総合体
  - 要素技術 ＋ システム工学・安全工学・心理学・社会学・法学・経済学・政治学の視点
  - コンピュータ 情報ネットワークの安全性
  - 重要な建造物の保護・安全管理
  - 社会の安全性・利便性・住み良さ・居心地よさ・効率・競争力
  - 経済政策、プライバシーとの兼ね合い
  - “Humanity ” を中核に置いた考え方 ：個人と社会環境の関係、主観的満足度・安心感
- *従って TRUST は*、安全性、ソフトウエア技術、複雑に相互依存するシステムの解析、経済性、法律、環境、社会通念等などの複合体を “全方位的に” 研究、設計・実証実験する。
- 目標:
  - 要素技術としての部品・ソフトウエア・通信とコンピュータシステムetc,. のTrustworthiness技術
  - モデルとなる社会環境への組み込み、実証実験
  - 実社会の受益者に、この課題の意義と得られる効果を提言する

1

CITRIS

TRUST

Berkeley VANDERBILT UNIVERSITY CORNELL
STANFORD UNIVERSITY Carnegie Mellon

TRUST 研究テーマの選定とチーム

- 安全工学
  - Softwareの安全性
  - 信頼の置けるプラットフォーム
  - Cryptography の応用
  - 情報ネットワークの安全性
- システム工学
  - 複雑系の相互依存関係のモデル化とそれを使ったシステム解析
  - 安全性の高いネットワークを基盤としたシステムの設計研究
  - 信頼できる部品(H/S)を基本としたモデルベースのシステム設計
  - 安全性の高い情報マネジメントTool の研究
- 社会・経済・法律・政治的考慮
  - 経済性・社会環境・大衆の側からの挑戦
  - デジタル化社会とプライバシー
  - マンマシンインターフェースと安全性・信頼安心
- 人間系の研究
  - 信頼感(不信感)・安心感・満足感・サービスの研究
  - 信頼感・満足感・安心感・満足感・サービスのROI (経済性)

1

CITRIS

TRUST

Berkeley VANDERBILT UNIVERSITY CORNELL
STANFORD UNIVERSITY Carnegie Mellon

Trustの研究テーマ （2006年4月）

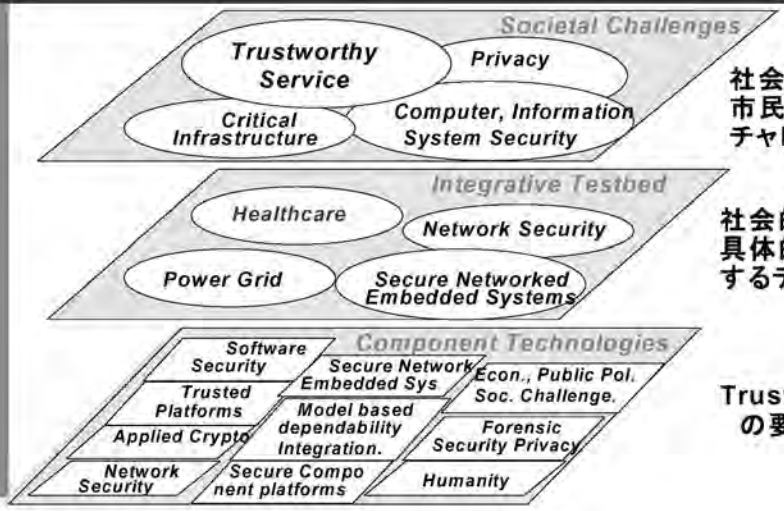
- サイバーセキュリティ（Critical Net・e-Commerce・e-Government)
- 防災モニタリング (地震・火事・水害）
- 人災（事故・人命 / 傷害・Critical Infrastructure）
- エネルギー・デマンドレスポンス
- 医療データベース （個人情報データ）
- 老人の社会的自立支援
- 社会浸透・還元: 教育・知識/技術移植
  - Test Bed

CITRIS

TRUST

Berkeley VANDERBILT UNIVERSITY CORNELL
STANFORD UNIVERSITY Carnegie Mellon

Trustworthinessの要素技術と社会展開手法



社会各層に対して社会的・市民的・経済的・法律的チャレンジを提言する。

社会的チャレンジを具体的に実証実験するテーマと場

Trustworthiness の要素技術

CITRIS

TRUST

Berkeley VANDERBILT UNIVERSITY CORNELL
STANFORD UNIVERSITY Carnegie Mellon

社会への浸透：教育・知識I技術移植・リーダシップ

- Trustworthy Society の実現には、社会各層への問題提起・提言と浸透活動が必須である
  - それがないと、絵に描いた餅になる
- Trustworthiness の全ての要素技術を再点検する必要があり、またそれらの教育が必要である
- 要素技術群はバラバラでは無く、整合性が必要である
- 教育のターゲット：大学学部、大学院、K-12
  - "liberal" technologically literate education

CITRIS

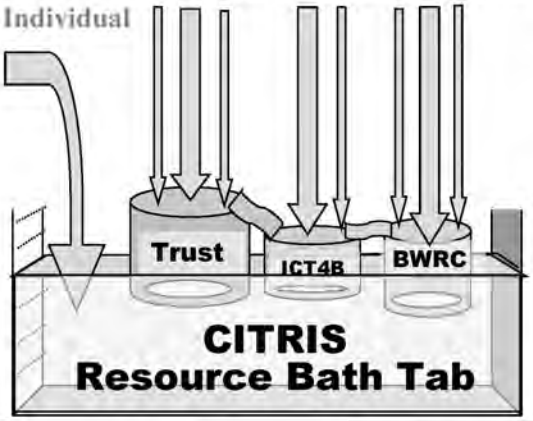
CITRIS

CITRISのストラクチャ・モデル・ファンデング・ROI

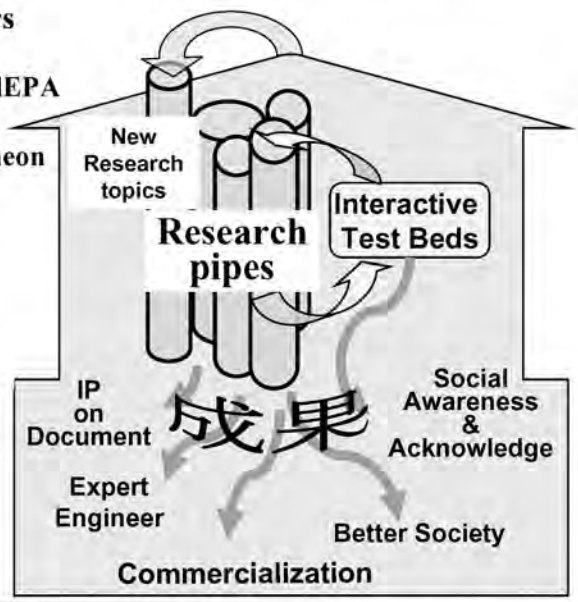
CITRIS Bath Tub Model

Funding through CITRIS
- Gov
- Industrial
- Individual

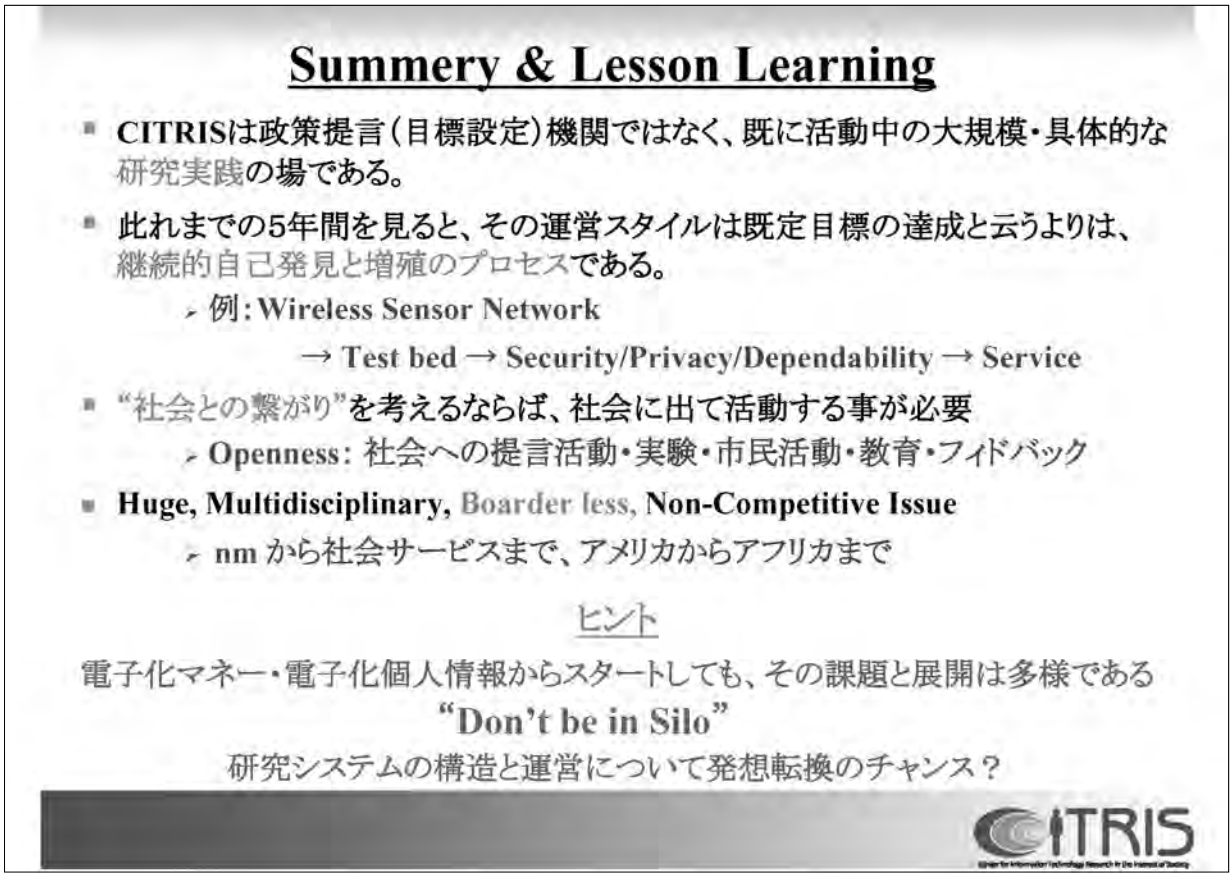
Funding for Individual Centers
- Governmental
  - ✓ NSF, NIH, DoD, DoE, CalEPA
- Industrial
  - ✓ MS, IBM, Intel, HP, Infineon



CITRIS ROI Food-chain Model



CITRIS


Summery & Lesson Learning
CITRISは政策提言（目標設定）機関ではなく、既に活動中の大規模・具体的な研究実践の場である。
此れまでの5年間を見ると、その運営スタイルは既定目標の達成と云うよりは、継続的自己発見と増殖のプロセスである。
例：Wireless Sensor Network
→ Test bed → Security/Privacy/Dependability → Service
“社会との繋がり”を考えるならば、社会に出て活動する事が必要
Openness：社会への提言活動・実験・市民活動・教育・フィドバック
Huge, Multidisciplinary, Boarder less, Non-Competitive Issue
nm から社会サービスまで、アメリカからアフリカまで
ヒント
電子化マネー・電子化個人情報からスタートしても、その課題と展開は多様である
“Don’t be in Silo”
研究システムの構造と運営について発想転換のチャンス？
CITRIS

3

ディペンダビリティの概念整理および重要研究分野に関する討議結果

グループ討議では、１．で述べたように、ディペンダビリティの概念整理、およびディペンダビリティに関する重要研究分野の提言という２つの課題について討論が行われた。各グループの討議結果を以下に示す。

３．１　G1グループの討議結果

■ ディペンダビリティ大陸

ディペンダブルなシステムの作成方法がある程度確立していて、仕様もわかっている領域と、予測できない事態、仕様もわからない領域があり、その境にあるディペンダビリティフロンティアに今遭遇している。このフロンティアが、経験を積むにつれて成長していくことが必要と考え、図3.1に示すようなディペンダビリティ大陸というものを考えた。

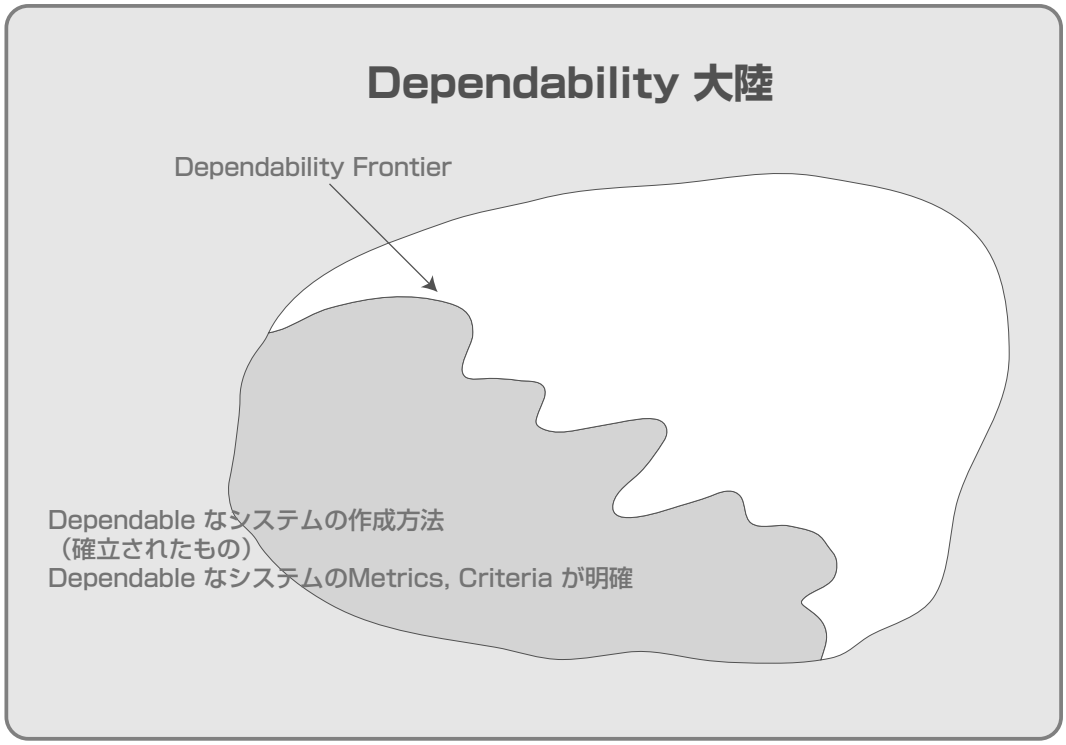


図３.１　ディペンダビリティ大陸

課 題1　ディペンダビリティとは

予測不可能性を秘めた系（今のネットワークなど）における、広義のサービスレベルを保証すること

現状および課題

1．系が閉じていないから不確実性が生まれる。
2．不特定な人を相手にしている。
3．パッケージ型の製品から、ネットワーク型の製品になってきた。
- ネットワークでは端末が認証できていない。
- 携帯電話のように作り手が予想していないものが生まれてくる。
- どこまでメーカーが保証しなければならないのか、何が起こるのか、本当にわからない。だけど、何かが起こると、メーカーは保障責任を問われる。
- サービスレベルという議論では、そうしたドメインすら定義されておらず、知恵をどのようにためていけばよいかもわからない。
- Fault modelを作ることが難しい。

実現方法例

▌システムには階層があり、下のレイヤーから独立したシステムとする。
▌メトリックを決める。（メトリックを決めるとポリシーが決まる。ポリシーが決まると、モニタが決まる。モニタが決まると、フィードバックループが決まる。）
▌周りの環境が変わるから、フィードバックループを入れて、サービスの連続性を持たせることで、付加価値をつける。
- 兆候の早期検知とそれへの対処が行えるシステムとする。
- 情報システムのセキュリティを保証する機能として、考えられる攻撃の辞書をまず作る。リバイズをする。それに対して機能を選ぶ。それを満たすことができているかをテストする。

▌システムがAutonomousであることがコアである。自律分散は必要な基盤技術の一つだが、一方でインフラをどうしていくかが別の課題としてある。（インターネットのアーキテクチャーをどうしていけばよいのかなど）
▌最終仕様書は書けなくてよい。指標も最初はなくてよい。まわしながらやっていく。
▌コンポーネントごとにMaturity Levelというものも作る。リスクマネジメントができる設計にする。

課 題2　具体的な研究開発課題

予測不可能性を秘めた系（今のネットワークなど）における、広義のサービスレベルを保証する技術体系を目指す

■ＩＴ技術課題
■社会技術課題
■推進方法

【技術的課題】

▌Dependability Metrics
▌Virtually Dependable System
▌Virtual Isolation
▌SLA（Service Level Agreement）のコンフリクトマネジメント技術
▌サービスとセキュリティとプライバシーの三律背反を避けるための理論（Game Theory？）
▌インターネットのアーキテクチャー
▌トレーサビリティとそれを隠す技術
▌トレーサビリティを悪用してディペンダビリティを損なう技術への対応
▌トラフィックをモニタするシステム
▌システムの内部ステータス（異常兆候）を顕在化する技術

【社会技術】

▌社会の静脈系を作る（一円以下のお金を集める）というお金が集められる世界が安全に作る仕組み
▌Liability（製造物の責任が明確になっていること）を保証できるシステムやシステムデザイン

【推進方法】

▌Dependable City、Dependable Campus
▌ディペンダブルシステムの問題を、徹底的に洗い出し、次のディペンダブルシステムのあり方について、グランドチャレンジを明確化するグループを作る

3．2　G 2 グループの討議結果

■ なぜディペンダビリティか？

▌人間のパフォーマンスを飛躍的に急速に改良する現象が起きている

- 加速要因：　VLSIの大規模化、検索エンジンの高性能化、ネットワークの高速大容量化、ユビキタスネットワークの浸透など
- そのような現象への参入コストが低い
  - ・大規模に急速に普及

▌ネットワーキングにより潜在バグが顕在化してくる

- 既存システムを組み合わせ、改造、発展させていくしかシステムを作れない
  - ・システムが大規模化、企業再編＝システム統合、、、
- 要素システムのフォールトは不可避、不明確

▌ICTによる社会イノベーションが想定外の大損失をもたらすことがある

- ネットワーク上への社会システム移行は始まったばかり。コンピュータとネットワークの真の意味が出現してきている

▌フィロソフィーとサイエンス・技術を同時に考える必要がある

課 題1　ディペンダビリティとは

参照システムのディペンダビリティとの比較においてディペンダブルと判断されること

- 現時点の判断が将来、変わっても大きな被害が出ない
- 相対的、漸進的

絶対基準でフェイタルなことが起きないこと

- 一回の被害の規模が巨大でないこと
  - ・年間1万人が死亡する交通事故よりも500人が一度に死亡する航空機事故の方が問題になる

課 題2　研究開発課題

▌ディペンダビリティ定義のための参照システムを特定する手法
▌ディペンダビリティ定義からの逸脱を評価・検出する技術
- 大規模社会シミュレーション
- モニタリング、データマイニング
- 仕様と前提知識からのシステム統合インパクトの評価

▌ディペンダビリティを実現するシステムモデル
- ヘテロなサブシステムからディペンダビリティポリシーを守るシステムを構成するモデル：　例）MAPEモデル
- フォールトの範囲限定が容易なコンポーネントアーキテクチャ

▌ユーザをシステム内要素に含めたシステム設計法
- 非技術的な社会システムとの結合

▌「常識」の確立、ユーザ教育
- 責任の所在はユーザの「常識」に依存する

▌イノベーションとディペンダビリティの両立
- 期待されるディペンダビリティの範囲での最大限のイノベーションを促進

▌経済性とディペンダビリティの両立

3．3　G 3グループの討議結果

■ たたき台となったいくつかの議論

▌米で軍関係のお金がつかなくなる（特注の時代）→ **民生用部品を使った開発　信頼性をユーザ側からみる必要性が出てきた　社会システムの保証の必要性**

▌**間違いのあることを前提にせざるをえない複雑なシステム**

▌**ディペンダビリティはコストとのバランス**　どれだけのコストを払っていいかどれかでのリスクを引き受けるか

▌**自己責任にするには原理を教えておかないといけない**　クルマは免許制あり、「だれもしない始業点検」がある ⇔ コンピュータウイルス

▌**いままでの工業製品は小さい事故に手を打てた　IT では最初の事故が甚大な影響を持つ　フィードバックがかかるまえにえらいことが起こってしまう**

▌ディペンダビリティを言い出すと、開発者の意図とかかわらず攻撃が起こるので、

性善説から性悪説に立って考えざるを得なくなってきた　ユーザに分かる説明責任　保障できるレベルを定量的に示すことが必要になってきた

- eBay　架空商取引が起こりうる　何が起こっているかを利用者に知らせることが必要、取引だから死活問題で利用者側にも知るモチベーションがある　**社会への普及研究**
- コストと所要性能が最大になるように、最適な組み合わせを研究することが必要　障害？要因のひろがりが大きくなっている　構成技術それぞれについては研究があっても全体の最適化についての研究はなされていない
- チェックする機能、仕様を作る機能（コンパイラのようなもの）→あいまいな仕様を仕様にする機能（暗黙知を形式知にする研究はありうる）米国なら企業と大学が一緒にやっているが、日本では・・・論文にならない（ものすごく大事だけど一番大事なところはオープンにできない、企業の中に入って研究している人は皆無に等しい）　最適な研究の推進方法と研究領域を選べれば
- ハード・ソフト協調設計・操作　オンラインモニタリング
- テストとはいわずにCPUのアーキテクチャの研究は大学でありうるのではないか、「ディペンダブルCPU」
- ネットワークのエラー訂正みたいに　計算の途中でミスがあっても訂正するような技術　ネットワーク・オン・チップ　CDMA　このような研究には数学が必要
- フォールトトレラントIC　冗長性と分散性以外には？　知能化（学習、適応・・・）チューニング
- ディペンダビリティのモデル（ケース）づくり　イメージが伝わるように　モデルのパラメターを明らかにする（メトリクス）　ディペンダビリティの計量　→ディペンダビリティのエンジニアリングへ
- ヒューマンエラーを考慮したシステム設計　（例：医療システム・・・）

課 題1　ディペンダビリティとは

・ユーザの視点から評価するものとして、提供されるサービスの保証の度合い（従来は開発者の視点から評価するものとして、提供される機能の保証の度合い）
・ディペンダビリティはコストとのバランス
・ITをIRTにaufhebenするために必要なもの

（状況の認識）

- 間違いのあることを前提にせざるをえない複雑なシステム
- いままでの工業製品は小さい事故に手を打てた　ITでは最初の事故が甚大な影響を持つ　フィードバックがかかるまえにえらいことが起こってしまう
- 性善説から性悪説に立って考えざるを得なくなってきた
- 民生用部品を使った開発　信頼性をユーザ側からみる必要性　社会システムの保証の必要性
- 自己責任にするにはユーザに原理を教えておく必要がある

課 題2　具体的な研究開発課題

- 暗黙知を形式知にする研究
- 仕様を作る機能 を実現する研究
- ハード・ソフト協調設計・操作　オンラインモニタリング
- 「ディペンダブルCPU」
- フォールトトレラントIC　（数学が必要）
- コストと所要性能が最大になるように、最適な組み合わせを研究
- ディペンダビリティのモデル（ケース）づくり
- ヒューマンエラーを考慮したシステム設計
- 社会への普及研究

4

まとめ

■ 議論の基本方針

- 人々が安全で安心して生活でき、快適で公正でかつ適度な競争を行える社会（人類・国が目標とする社会）を支える情報システム構築の指導原理を与える。
- 社会のあり方とその基盤となる思想・哲学・制度を考えながら情報技術を考え、わが国の国際競争力を高める。
- 技術の基本方針としてのDependabilityの概念を明確化し、その研究戦略を与える。
- 国・納税者、利用者（一般市民）、学会・研究者、企業・産業界へのそれぞれへの説明の論理

■ 何故Dependabilityか?

- 人間の能力の急速で飛躍的な拡大
- オープンなシステムが世界規模で実用され、新しいシステム構築の基本方針が必要

- システムの接続により潜在バグの顕在化がおこる
- Faultは不可避なのでその存在を前提としての技術開発が必要
  - 予防、回避、事故時の対策、回復
  - 最初の事故が膨大な損害を与える
  - 性悪説を前提にせざるを得ない
- 民生用部品による社会システムの保証
- ユーザ責任と製造者・設計者責任の明確化の必要性

■ Dependabilityとは

- ユーザ視点の概念
- 予測不可能性（想定外事象）を秘めた系において広義のサービスレベルが保証されること。また、その保証の度合。
  - 有限責任を宣言できるシステム　→　ユーザ視点へ
  - 人類全体の為に無限責任を負うべきシステム
  - 参照システムとの比較
  - 絶対基準における定義
- IRTとの接続

■ 研究課題

▌IT技術課題

- 人間も含めた社会全体の安全性、安定性を漸近的に保証するための技術体系
- Metricsの確立
- Virtually Dependable Systemの概念の確立
- Virtual Isolationの概念の確立
    - ・各レイアへの要求と役割の明確化
- SLAのコンフリクトマネジメント
- サービス、セキュリティ、プライバシーの三律背反への対応
    - ・ポリシーと具体的な方法論
    - ・トレーサビリティとセキュリティ
    - ・モニタとプライバシー
    - ・可視化とセキュリティ
- 長期的な問題列挙と解決策の議論
- 定義からの逸脱の評価・検出
- Dependabilityの実現モデル
    - ・方法論
    - ・テストケース
- 暗黙知を形式知にする技術の確立
- 仕様を作る技術
- システム全体（HW/SW）を把握する技術の研究
- CPUアーキテクチャ、FTIC技術、最適化
- 多様性の必要性に関する提案

▌社会技術課題

- 社会システムの再構築に関する議論
- Dependabilityの社会的・経済的価値
    - ・人類、国、企業、個人それぞれの立場での定義
    - ・リスクの評価技術
    - ・経済性、イノベーションとDependabilityの両立
- インフラに対する課金の仕組み
    - ・社会の静脈系の構築
- Liabilityの保証のしくみ
    - ・技術、制度、保険、法律
- 参照システムの特定と比較する方法

- Human Error を前提とするシステム設計技術
- ユーザ教育、普及活動

■ 推進方法

- Grand Challengeの提示
- Realな実験場
  - ・Dependable City/Campusの構築
- ソサイアティの構築
- 失敗例の蓄積
- 大規模国家プロジェクト
  - ・方針決定の為のSteering
  - ・要素技術開発の研究
  - ・総合的なReal Worldでの実験
  - ・実用システムの継続的なモニタと新しい問題の発掘と解決

付　　録

付録 I

ワークショップ　プログラム
（ディペンダビリティ WS）

場　　所：JST 社会技術研究開発センター　（りそな・マルハビル　18 F）
日　　時：平成 18 年 5 月 12 日（金）14：00～22：00
　　平成 18 年 5 月 13 日（土）9：00～11：30
総合司会：丹羽邦彦　シニアフェロー

第 1 部

5 月 12 日（金）

13：30～14：00　受付
14：00～14：10　CRDS の活動と戦略プロポーザルについて
　　生駒俊明　センター長（CRDS）　（10 分）
14：10～14：25　ワークショップの進め方について
　　成瀬雄二郎　シニアフェロー（CRDS）　（15 分）
14：25～14：45　『ディペンダビリティについて』
　　安浦 寛人　九州大学 教授　（20 分）
14：45～15：05　『ディペンダビリティの概念と課題』
　　南谷 崇　東京大学 教授　（20 分）
15：05～15：30　『情報通信ネットワークのディペンダビリティ』
　　市川 晴久　NTT 先端技術総合研究所 所長　（25 分）
15：30～15：55　『社会サービスのディペンダビリティ』（仮）
　　岩野 和生　日本 IBM 執行役員　（25 分）
15：55～16：05　休憩　（会議室 2 にコーヒーをご用意します）
16：05～16：30　『自動車のディペンダビリティ』（仮）
　　服部 雅之 トヨタ自動車　車両技術本部 室長　（25 分）
16：30～16：50　『米国における研究戦略動向（CITRIS TRUST）』（仮）
　　井上 隆秀 UCB CITRIS アドバイザー　（20 分）
16：50～17：05　質疑応答
17：05～17：30　グループ討議の課題説明　成瀬雄二郎　シニアフェロー

第 2 部

課題 1．ディペンダビリティの概念整理
課題 2．ディペンダビリティに関する重要研究分野の提言
　　含む　VLSI へのメッセージ（期待・要求：自由記述／箇条書）
17：30～18：30　夕食（会議室 1）・休憩
18：30～22：00　3 グループ討議（第 1～第 3 会議室）

第 3 部

5 月 13 日（土）

9：00 ～ 9：05　事務連絡
9：05 ～ 9：50　3 グループの発表　（各 15 分）
9：50 ～ 11：30　総合討論とまとめ

以上

付録Ⅱ

ディペンダビリティワークショップ参加者一覧　（2006年5月12日、13日@JST）

No.	氏名	所属
1	有村　博紀	北海道大学 大学院情報科学研究科 教授
2	市川　晴久	NTT先端技術総合研究所 所長
3	井上　隆秀	University of California, Center for IT research on Interest of Society, Internal Technology Business Advisory
4	岩野　和生	日本アイ・ビー・エム株式会社 ソフトウェアー開発研究所所長 執行役員
5	岡本　和也	株式会社ニコン，大阪大学 客員教授
6	菊野　亨	大阪大学 大学院情報科学研究科 教授
7	木村　晋二	早稲田大学 大学院情報生産システム研究科 教授
8	黒田　忠広	慶應義塾大学 理工学部 電子工学科 教授
9	佐藤　了平	大阪大学 先端科学イノベーションセンター 教授
10	柴田 随道	NTTマイクロシステムインテグレーション研究所 研究企画担当部長
11	田中　英彦	情報セキュリティ大学院大学 情報セキュリティ研究科 教授
12	谷口　研二	大阪大学 大学院工学研究科 教授
13	所　眞理雄	株式会社ソニーコンピューターサイエンス研究所 代表取締役社長
14	中島　秀之	公立はこだて未来大学 学長
15	中島　啓幾	早稲田大学 理工学部 教授
16	服部　雅之	トヨタ自動車株式会社 車両技術本部 第3電子技術部 第31電子室 室長
17	福田　晃	九州大学 大学院システム情報科学研究院 教授
18	福田　剛志	日本アイ・ビー・エム株式会社 大和ソフトウェア研究所 部長
19	福田　敏男	名古屋大学 大学院 工学研究科マイクロ・ナノシステム工学専攻 教授
20	前口　賢二	SIRIJ 半導体産業研究所 所長
21	松澤　昭	東京工業大学 大学院理工学研究科 教授
22	松本　勉	横浜国立大学 大学院環境情報研究院 教授
23	三木　哲也	電気通信大学 情報通信工学科 教授
24	森川　博之	東京大学 大学院新領域創成科学研究科 助教授
25	安浦　寛人	九州大学 システム情報科学研究院 教授

27	中里　学	文部科学省 研究振興局情報課 課長補佐
28	酒井　重樹	JST戦略的創造事業本部 副調査役
29	薬師寺　崇	JST戦略的創造事業本部 主査
30	福島　恵子	JST戦略的創造事業本部 主査
31	生駒　俊明	JST研究開発戦略センター センター長
32	丹羽　邦彦	JST研究開発戦略センター シニアフェロー
33	佐々木　和則	JST研究開発戦略センター シニアフェロー
34	成瀬　雄二郎	JST研究開発戦略センター シニアフェロー
35	南谷　崇	JST研究開発戦略センター シニアフェロー
36	伊東　義曜	JST研究開発戦略センター 主任調査員
37	石正　茂	JST研究開発戦略センター フェロー
38	嶋田　一義	JST研究開発戦略センター アソシエイトフェロー
39	雄山　泰直	JST研究開発戦略センター フェロー
40	竹間　清文	JST研究開発戦略センター フェロー
41	石井　哲也	JST研究開発戦略センター アソシエイトフェロー
42	安藤利夫	JST研究開発戦略センター 調査役
43	中神　雄一	JST研究開発戦略センター 係員
44	黒澤　景	独立行政法人 物質・材料研究機構 企画調査室

付録Ⅲ

ディペンダビリティワークショップ
第二部　グループ構成（敬称略）

G 1（会議室 1）　リーダー：岩野和生（日本 IBM）
書　　記：佐々木和則、嶋田一義（JST ／ CRDS）

メンバー：

中島秀之	公立はこだて未来大学
松本勉	横浜国立大学
森川博之	東京大学
南谷崇	JST/CRDS（東京大学）
福田晃	九州大学
松澤昭	東京工業大学
前口賢二	半導体産業研究所

G 2（会議室 2）　リーダー：市川晴久（NTT 先端技術総合研究所）
書　　記：成瀬雄二郎、伊東義曜（JST ／ CRDS）

メンバー：

所眞理雄	ソニー コンピュータサイエンス研究所
福田剛志	日本 IBM
田中英彦	情報セキュリティー大学院大学
有村博紀	北海道大学
佐藤了平	大阪大学
岡本和也	大阪大学
木村晋二	早稲田大学（北九州）

G 3（会議室 3）　リーダー：福田敏男（名古屋大学）
書　　記：丹羽邦彦、石正茂（JST ／ CRDS）

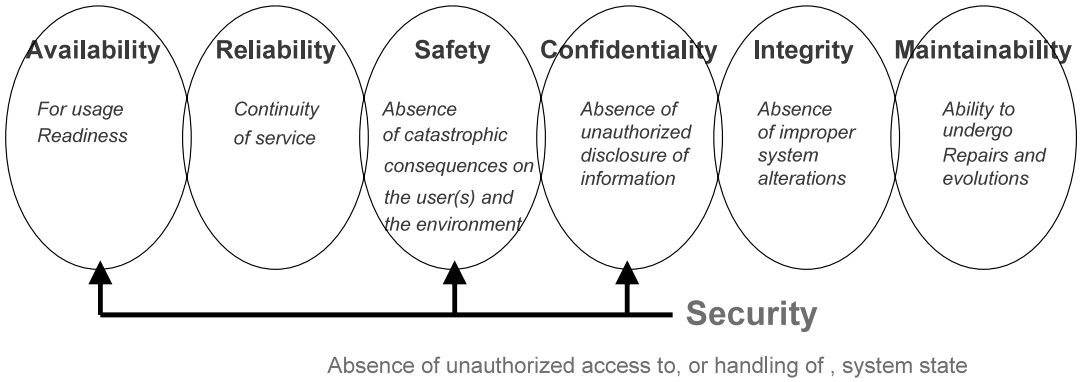
メンバー：

井上隆秀	UCB　Center for IT research CITRIS
柴田随道	NTT　マイクロシステムインテグレーション研究所
菊野亨	大阪大学
服部雅之	トヨタ自動車
谷口研二	大阪大学
中島啓幾	早稲田大学
（安浦寛人）	九州大学

以上

付録Ⅳ　事前アンケートまとめ

Q1　ディペンダビリティとは？



抜粋

- **サービスにDepend,ハード・ソフト両面から人の心まで考慮した安全・安心を提供する方法・技術**
- **開発者・使用者全体の信頼性**
- **システム監視・制御・発展・交代する能力**
- **Human　Erorrに対して人とシステムからなる社会の系がTolerant**
- **簡単・快適・便利、安全・安心の包含概念**
- **人類が全面的に頼れる社会システム**

- **Dependabilityにレベル差：生命を預けられる～ゲーム**

Q2　ディペンダビリティを実現するために必要なことは？

エレクトロニクス・フォトニクス

- センシング技術
- 性能（処理速度、容量、等）向上
- ロバスト・メンテナンス用意・インテリジェント部品、システム
- 不要電磁波輻射防止技

コンピューティング

- 危険の明確化
- 危険予測技術
- 危険回避技術
- システムの単純化
- フェールセーフ/フォールト トレラントなシステム構築
- 想定外危機対応技術
- ウィルス対策ワクチン
- 誤りに対しての責任明確化
- 性能（処理速度、容量、等）向上
- サービスサイエンス
- システム工学
- フォールトモデル明確化
- 重要情報鍵分散技術
- 不要電磁波輻射防止技術
- システムのメンテナンス永続化
- 人とシステムの役割分担明確化
- 統合システムの正常動作確認技術
- フォールトモデルの確立
- ソフトディペンダビリティ 創出

ネットワーク

- モニタリング技術
- センシング技術
- 災害時対処法
- データの総暗号化
- 不要電磁波輻射防止技術
- ウィルスのネットワーク上対策

ロボティクス

- モニタリング技術
- センシング技術
- 危険予測技術
- 危険回避技術
- システムの単純化
- Dynamic self Test
- システムロボティクス
- ロボット工学
- テスト仕様の明確化
- 不要電磁波輻射防止技術
- 価値の最大化をもたらす評価・判断方法の確立
- 診断技術・解析技術向上
- ディペンダビリティ 評価法
- センサー情報からの現場再現技術
- 統合システムの正常動作確認技術
- システム追加による不具合検出法
- フォールトモデルの確立

社会

- ディペンダブルシステム証明認証機構　・ディペンダブルのスムースな社会への普及活動　・情報利用の不正対策法整備　・低消費エネルギー　・悪用者対策　・社会システム学

Q3　直面しているディペンダビリティに関わる問題は？（その1）

自然・物理系のFault

・量子揺らぎ等の製造不良
・熱雑音，量子雑音，宇宙線，などによる集積回路誤動作
・VLSI製造ばらつき、電源や信号線のノイズ、ソフトエラー
・携帯PCのHD不起動で、過去のメールにアクセス不能
・想定外の環境での最適動作
・ノイズ・デバイス劣化・動作環境変化で発生する回路系の
・動作不良や誤動作が不明確
・物性限界、微細化・高集積化による不良確率増大
・ソフトエラー、ノイズによる誤動作
・ワイヤレス通信での環境、構造物によるフェージング現象、
・スループットの低下や通信信頼性の不安定化.
・携帯電話の電池寿命、故障
・複雑系のシステムを実現する上での適性解を与える方法論
・物を落として壊した。情報処理の途中で情報が消滅した(停電)
・酸化膜故障、配線故障、しきい値変動、素子バラつき、
・宇宙線ソフトエラー、熱暴走、静電破壊、電磁障害
・宇宙線の影響による故障のないLSIの一時的な誤動作.
・ハードディスクの新製品で頻発する初期不良
・長期稼動によるソフトウェアの経年劣化
・温度、プロセス、電圧ばらつき、およびデータ依存のクロストークによる遅延ばらつき(VLSI内部)

人為的Fault 【ミス・エラー】

・思い込み（電子メイル送付事実だけで、連絡済みと錯覚）
・設計ミス，製造ミス。設計者が想定外環境での誤動作
・多量パスワードの忘れ
・ハードウェアの設計誤りの解析、誤りの定義困難
・正しさの仕様の記述と仕様の完全性の判定が困難
・製造プロセスミス・ばらつき、システマテイック不良、
・静電破壊などの取扱いミス、設計ミス・検証ミス、テストカバー率
・外観重視デザインによる人為的操作ミスなど
・システムの使いにくさ.（例：銀行のATMで送金などの複雑な操作の一部を取り消す場合に最初から再入力）
・JR西日本の事故、高速船(鹿児島)の事故など(システムの設計段階で予測外?)
・設計・検証ミス（設計者と検証者が同一）
・ファイルのバージョン管理ミス
・ストレージシステム・データベースシステム管理操作ミス
・誤って大事なファイルを消去してしまう。

Q3　直面しているディペンダビリティに関わる問題は？（その2）

人為的Fault 【悪意・攻撃】

・リバースエンジニアリングによる粗悪模造品製造
・保証しえない（事前に考えていない）環境下での使用
・迷惑メール
・ウィルス（含む大学NWでの発生）
・ワーム
・他人に成りすまして預金引き出し(商品購入)
・Creditカードの複製、パスワード盗難
・パチンコ台裏ROMなどチップ置換
・設計情報の漏洩流出
・強い電波による誤動作誘発
・チップ漏電磁波で情報を傍受
・回路応答の解析による。ハードウエア情報の不正抽出
・イモビソフト書き換え、イモビ自体の交換による車盗難
・個人情報・企業秘密の不正取得・窃盗、成りすまし
・SPAMメール（誤ってまぎれている大事なメールを消去

システム・システム、システム・人、人・人の相互作用によって生じるFault

・チーム設計時、細部仕様の各人の認識違いの潜在的エラー
・米国仕様PCでサポートされている筈の日本語で不具合
・保険医療機関間の不整合
・アナログ回路とデジタル回路の混載
・TV会議システムで遠隔地の音声遅延による激論時不具合
・Web でホテル予約をし、確認のE-mail も来たが、不予約
・システムの複雑化で開発環境は分散するが、統一プラットフォーム不整備によるデバイス開発時のヒューマンエラー
・古い世代の記録媒体読み取り不可能
・デバイスと設計のインタフェース（システムとシステム）
・検証での擬似エラーと真性エラーの区別（システムと人）
・モジュール間や担当者間のインタフェースミス（人と人）
・オーバーテストの結果，正常なものまで故障と判定
・システム接続（システムホール）による検証不足のエラー
・ECU間の通信エラーによる誤動作
・情報システムの統合時の多大な作業に伴う誤り
・想定外入力（例：ライブドア事件の際の東証システム）
・複数システム同時動作による設定条件不一致による不具合
（例：水のあふれ検知システムと消火スプリンクラー
IT機器接続の相性の存在）
・環境変化でネットワーク機器が不良動作の責任が不特定
（全く同一環境を作り出し困難のため不良動作再現不可）

Q4　ディペンダビリティの評価尺度・手法

	エレクトロニクス・フォトニクス	コンピューティング	ネットワーク	ロボティクス	社会
尺度	Mean Time To Failure (MTTF) Mean Time Between Failure (MTBF) 歩留まり 故障率 Statistical Delay Quality Model Weibull plot	ビットエラーレート ソフトエラーレート ロジックエラーレート テスト・カバレッジ	利用実績 普及率 検証のカバレージ 暗号強度		テニスの技術認定
手法	加速度テスト システム機能検証 フィールドテスト デザインレビュー 設計検証CAD システム検証エミュレータ テスター バーンイン スクリーニング 受入検査 工程内検査 統計的行程管理 不良解析 品質管理教育 品質管理組織 トレーサビリティ	出荷前テスト ソフト分野のベンチマーク		統計的品質管理	ノウハウの積み上げ

Q5　VLSIに求められるディペンダビリティとは？

Availability
継続的に供給されること
セカンドソースが確保できること

Safety
低消費電力
リサイクルの可能性

Confidentiality
内部処理の秘匿性
情報が自動的に消滅する機能
チップ内にそのチップを認証する仕組みを持つ
情報漏洩の防止能力
安易に変更出来ない暗号化設計手法
搭載された情報へのアクセス防止
ユーザ・コンピュータ認証能力

Integrity
チップに乗せるソフトウェアを認証して、処理内容を保証する仕組み
高信頼アーキテクチャー

Reliability
自己維持本能
厳格にタイミング仕様が満たされなくても動作するVLSI設計技術
一部の不良があっても動作する機能
一部の不良があると自動的に不良品と分別できる機能
回路が確実な結果を出す仕組み
どのような状況にあっても、所定の機能を発揮できること
動的に処理内容を認証する仕組み
給電が止まっても直前の情報処理を再現できるもの
機能的バグの少なさ
実装の機械的強度
処理能力に余裕があること
ソフトエラー耐性
動的な変動（温度の変化等）への対応
対環境耐性、長期信頼性の高さ
耐攻撃性
耐衝撃性
コンピュータウィルス検出能力とその実行防止能力
書き込み要求が妥当なものか否かの判断機能

Maintainability
自己テストと自己修復
誤動作の検知と対処
Dynamicなセルフテスト＆リペア機能
自己認識性
自己監視能力
自己終端能力
機能不正の症状・理由を対応可能な様にレポートする機能
統一インターフェース
スペックの公開
スペックが細部まで保証されていること
システム毎の設計指針の確立
問題発生時にデバック容易な故障診断ツール
回路系の動作不良・誤動作の明確化
動作不良・誤動作のテスト技術、補償技術（特にアナログ回路）
高信頼性設計
システム設計とリンクしたLSI設計ツールチェーン

Others
コストを意識した冗長性

本報告書の各章の資料について

本報告書の各章の内容は、それぞれ以下の方々に作成して頂いた資料に基づき、独立行政法人科学技術振興機構（JST）研究開発センター（CRDS）が編集したものである。

ディペンダビリティワークショップ
報告書

独立行政法人 科学技術振興機構 研究開発戦略センター

制作担当　生駒グループ

〒102−0084　東京都千代田区二番町3番地
電話　03−5214−7481
ファクス　03−5214−7385
http://crds.jst.go.jp/
2007年3月