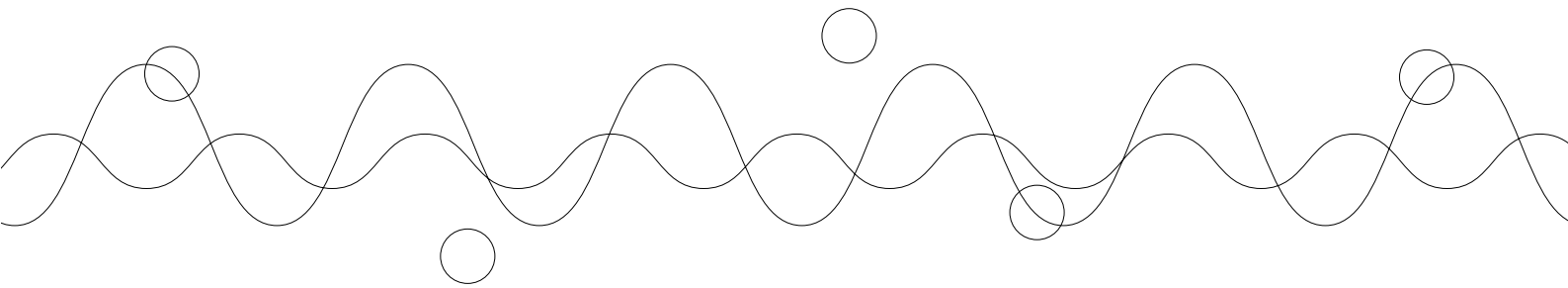
CRDS-FY2006-WR-09

「情報システムのディペンダビリティ評価」に関する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

科学技術振興機構・研究開発戦略センターでは、「情報化社会の安全と信頼を担保し、国際競争力の強化に向けて、ディペンダビリティを最高の価値とする新しい情報技術体系の研究開発戦略を推進すべき」との提言を行っている。

この提言に沿った研究開発成果の技術的、経済的、社会的効果を明示するためには「ディペンダビリティの定量的評価」が必要である。すなわち、情報システムの提供するサービスのメトリクス定義、測定法、計算法、評価法、ベンチマーキング、正当性検証、可視化、経済価値へのマッピングなどの方法論を確立する必要がある。

「定量的評価」によって「ディペンダビリティの価値」に関する社会的合意が形成され、制度・政策に反映されることによってディペンダビリティ技術の研究開発が促進され、さらにそれが産業競争力の強化、企業価値の向上、国際標準化の主導につながるなど、我が国の国際競争力の新たな源泉を創出することが期待できる。

こうした認識から、ユーザ視点のディペンダビリティ評価技術を確立するための基礎的研究分野としてどのようなテーマが重要かを明らかにすることを目的としたワークショップを2006年11月24、25日に開催した。

ワークショップには、コンピュータシステム、ソフトウェア工学、ディペンダビリティ、セキュリティ、ネットワーク、企業基幹システム、システム検証、システムインテグレーション、人間協調ロボット、自動車エレクトロニクス、鉄道列車制御、外科医療、経済学、認知科学など、多岐に亘る分野の専門家18名と関連省庁政策担当者、JST関係者が参加した。

2日間にわたる本ワークショップの結論、提言を要約すると、以下の通りである。

1）情報社会では、エネルギー網、情報通信網、交通網、金融網、行政網などの重要インフラを含むあらゆる社会活動、産業活動が情報システムに依存している。このような社会の安全と信頼を保証するために、ディペンダビリティとセキュリティを最高の価値とする「情報社会技術」の体系を構築することは、科学技術政策が目指すべき最優先課題の一つである。

2）ディペンダビリティとセキュリティの研究コミュニティは国際的にもこれまで互いに独立に活動しており交流はほとんどなかった。しかし、両者の概念および技術には共通点が多いので、多様なリスクを内包する情報社会の安全と信頼を保証するためには、ディペンダビリティとセキュリティの

概念・技術が互いの共鳴効果を保ちつつ統一化される必要がある。

3）サービスレベルにおけるユーザ（ステークホルダー）視点からのディペンダビリティ評価がシステム開発レベルにおけるデザイナの設計目標にまで一貫性を保って分解されるようなメトリクス、言い換えれば、システム設計目標の達成がサービスレベルにおけるユーザの評価に合理的に帰結するようなメトリクスの開発が必要である。

4）社会の変化と技術の進歩によって情報システム自身の目的は進化し、情報システムを取り巻く環境も変化する。そのようなシステムの進化と環境の変化に対応したディペンダビリティ評価を可能にするアーキテクチャ、システムのライフサイクルを通じた評価プラットフォーム、その評価方法の体系化・構造化が必要である。

5）人間要素を含む広義の情報システムに対して、ユーザ視点からの主観も含む評価メトリクスの定義、計測、モデリングとその可視化、リスク分析・管理、SLA（Service Level Agreement）方式の確立が必要である。

6）ディペンダビリティ／セキュリティの評価技術の正当性、有効性を確認するための相当規模のテストベッド構築が必要である。

CONTENTS

1

ワークショップの位置付けと狙い

独立行政法人科学技術振興機構(JST)研究開発戦略センター(CRDS)は、科学技術の研究分野を俯瞰的に展望し、今後重要となる研究領域、課題を系統的に抽出し、社会ニーズの充足と社会ビジョンの実現に向けた研究開発のファンディング戦略を立案・提言している。その活動の一環として、重要研究テーマについて専門家によるワークショップ(WS)を開催している。

このたび、CRDSでは、2006年11月24、25日に「情報システムのディペンダビリティ評価」に関するWSを開催した(プログラムは付録I参照)。本報告書はその結果をまとめたものである。

1．1　ワークショップの位置付け

これまで情報システムやそれを構成するデバイスの研究開発は主としてその高機能化、高速化、高集積化を目指して行われてきた。しかし社会のあらゆる活動が情報システムに依存するようになった現在、単にこのような方向を追求するだけではなく、それに加えてディペンダビリティを重視した研究開発を展開していくことが必要な時期を迎えている。CRDSではこのような観点からディペンダビリティを軸にしたWSをシリーズで開催してきた。まず2006年5月に「ディペンダビリティWS」[1]を開いて、ディペンダビリティの概念と重要研究分野を明確にした。続いて同月「ディペンダブルVLSI WS」[2]を開いて、VLSIから見たディペンダビリティの捉え方と技術課題を明らかにした。今回の「情報システムのディペンダビリティ評価」WSは、上記二つのWSに続くものである。

なお、ここで言うディペンダビリティとは、従来のディペンダビリティとセキュリティの概念を総合した「(広義の)ディペンダビリティ」あるいは「ニュー・ディペンダビリティ」[3]のことである。

1．2　ワークショップの狙い

社会の安全と信頼を保証するためには、その社会基盤を支える情報システムのディペンダビリティが確保されなければならない。CRDSでは、「情報化社会の安全と信頼を担保し、国際競争力の強化に向けて、ディペンダビリティを最高の価値とする新しい情報技術体系の研究開発戦略を推進すべき」との提言を行っている[3]。この提言に沿って情報技術体系の研究開発を促進し、その成果の技術的、経済的、社会的効果を明示するためには、「ディペンダビリティの定量的評価」が必要である。具体的には、情報システムの提供するサービス品質のメトリクス定義、測定法、計算法、評価法、ベンチマーキング、正当性検証、可視化、経済価値へのマッピ

1)ディペンダビリティワークショップ報告書，CRDS-FY 2006-WR-07(2007)．
2)「ディペンダブルVLSI」に関する科学技術未来戦略ワークショップ報告書，CRDS-FY 2006-WR-08(2007)．
3)戦略イニシアティブ 情報化社会の安全と信頼を担保する情報技術体系の構築 ――ニュー・ディペンダビリティを求めて――，CRDS-FY 2006-SP-07(2006)．

ング、などの方法論確立が必要である。その結果、「ディペンダビリティの価値」に関する社会的合意が形成され、調達基準、監査・認証制度などの政策に反映されることによって、ディペンダビリティ技術の研究開発が促進され、さらにそれが産業競争力の強化、企業価値の向上、国際標準化の主導につながるなど、我が国の国際競争力の新たな源泉を創出することが期待できる。

本ワークショップは、こうした認識から、ユーザ視点のディペンダビリティ評価技術を確立するために基礎的研究分野としてどのようなテーマが重要であるかを明らかにし、これらの重要研究テーマを推進するための挑戦課題・推進方法などを時間軸を加えて明確化することを目的として開催した。

1．3　ワークショップの構成

ワークショップ参加者は、コンピュータシステム、ソフトウェア工学、ディペンダビリティ評価、情報セキュリティ、ネットワーク、企業基幹システム、システム検証、システムインテグレーション、人間協調ロボット、自動車エレクトロニクス、鉄道列車制御、外科医療、経済学、認知科学など、多岐に亘る分野の専門家、および、関連省庁の政策担当者とJST関係者である。参加者の一覧表を付録Ⅱに示す。

付録1に示すように、2日間にわたる本ワークショップは次の5つのセッションで構成された。

セッション1（問題提起）：「ディペンダビリティ評価の意義」および「ディペンダビリティ評価研究の現状」についての紹介の後、4名の専門家による異なる立場からの「評価メトリクス」と「経済価値」に関する問題提起が行われた。

セッション2（グループ討議）：3つのグループに分かれて、それぞれの専門分野、応用分野から見たディペンダビリティ評価に関する研究の現状俯瞰と重要研究テーマの抽出作業が互いに独立に行われた。

セッション3（全体討議）：3つのグループのリーダーから各グループの討議の状況に関する中間報告が行われた。

セッション4：（グループ討議）：中間報告の結果を踏まえて、各グループの討議が続行された。

セッション5：（全体討議）：以上の討議をまとめた報告が各グループリーダーからなされた後、全体で議論を総括した。

2

ディペンダビリティ評価に関する問題提起

2．1　ディペンダビリティ評価の意義　　南谷　崇（JST/CRDS）

情報社会は人と社会のあらゆる活動が情報システムに依存している。情報システムなしでは、エネルギー網、交通網、通信網、金融網、行政網などの社会重要インフラを含めて、日常生活、企業活動、国家機能は全く成り立たない。情報社会におけるあらゆる活動の基盤を成すこの情報システムに、万一障害が発生し、期待するサービスが停止したり、想定しない事態が起きると、個人や社会の活動が混乱に陥り、尊い人命や貴重な財産が失われるかもしれない。場合によっては国際的な信用を失い、国家安全保障が脅かされる可能性がある。実際、安全制御系不調による鉄道列車事故、大都市の広域停電、メガバンク合併に伴うシステム障害、証券取引所の売買システム停止、ファイル交換ソフトによる重要情報の大量漏洩、DDoS攻撃、データ改竄など、情報システムの障害、重要インフラの事故、システムへの不正侵入など、情報社会の安全と信頼を脅かす事件の例は枚挙にいとまがない。

目指すべき情報社会の安全と信頼の根本基盤を支えるこのような情報システムは、その提供するサービスが良質で信頼でき、そのユーザが安心してそのサービスに依拠できるという性質、すなわちディペンダビリティをその第一義的属性として備えるべきである。

こうした認識から研究開発戦略センターでは、戦略イニシアティブ「情報化社会の安全と信頼を担保する情報技術体系の構築」を発行し、「情報化社会の安全と信頼を担保し、国際競争力の強化に向けて、ディペンダビリティを最高の価値とする新しい情報技術体系の研究開発戦略を推進すべき」との提言を行ってきている。

この提言に沿った情報技術体系の研究開発を促進し、その成果の技術的、経済的、社会的効果を明示するためには、実現される情報システムがそのサービスを受けるユーザーの視点から見てどの程度安全で信頼することができるのか、すなわち情報システムのディペンダビリティとセキュリティがどのレベルで達成されているのかを定量的に評価し、明示する手法の確立が必要である。さらに、その評価結果が経済的価値として表現され、ユーザに対して可視化される必要がある。

これまで、情報システムの「価値」はもっぱらその機能と性能にあると考えられてきた。設計者ももっぱらシステムの高機能化、高速化、高集積化を目指してきた。しかし、これからの成熟した情報社会では、その基盤となる重要社会インフラ、電子政府、電子商取引、インターネットサービス、ユビキタスコンピューティングなどの実現においてディペンダビリティとセキュリティを最も価値ある設計目標とすべきである。

そのためには、多様な応用分野と環境におけるユーザ視点からのディペンダビリティ／セキュリティのメトリクス、計測法、計算法、評価方法、可視化方法を確立し、さらに経済価値へのマッピング方法を確立する必要がある。

その結果、測定法に裏付けされた評価基準策定によってディペンダビリティ技術の開発が促進され、産業競争力の強化、企業価値の向上、国際標準化の

主導など、我が国の国際競争力の新たな源泉を創出することが期待できる。

情報システムのディペンダビリティ評価に関する研究はこれまでも行われている。しかし、これまでは、主として物理的なフォールトが所与の確率で発生することを前提にシステムのアベイラビリティやリライアビリティを推定するモデルベースの評価研究やソフトウェアによる疑似フォールを注入してシステムのロバスト性を確認するフォールトインジェクション研究が中心であった。

そのような状況にあって、以下の3つの新しい論点は、これまで我が国においても欧米においても十分研究されてこなかった、困難であるが重要な研究課題を提示している。

1）従来の情報システムを提供するベンダーの立場あるいは設計者の視点からではなく、サービスの提供を受けるユーザの視点からのディペンダビリティ／セキュリティのメトリクス定義と測定法の開発。

2）従来の物理的要因だけではなく人間の引き起こすリスク要因やシステム同士の相互作用から生じるリスク要因を内包する情報システムのディペンダビリティとセキュリティの評価。

3）ディペンダビリティ／セキュリティ評価の経済価値へのマッピングの確立とその社会システムに与えるインパクトの分析。

これらの論点を軸として、情報システムのディペンダビリティ評価研究の現状を俯瞰し、今後の重要分野と研究課題を抽出する作業は、戦略的プロポーザル作成に向けての重要なステップである。

2．2　ディペンダビリティ評価研究の現状　　土肥　正（広島大学大学院）

2．2．1　ディペンダビリティ評価の概要

"Dependable" とは頼りがいのあるという意味であり、信頼性や安全性を包含した一般的な概念としてコンピュータ工学分野において既に認識されている。従来から用いられてきた性能評価（Performance Evaluation）との相違点は、性能評価がある与えられたシステムワークロードに基づいて計測されるのに対し、ディペンダビリティ評価は与えられたフォールトロードに基づいてディペンダビリティを計測する点にある。すなわち、システムにおいてフォールト、エラー、脆弱性などの存在が前提にあるとき、それらの影響についてのシステム属性を示す評価尺度として定義される。性能評価における代表的な評価尺度がスループットやレスポンスタイムなどであるのに対し、ディペンダビリティ評価尺度として信頼度、アベイラビリティ、MTTF（Mean Time to Failure）などが挙げられる。

ディペンダビリティの定量的評価に向けての基本方針として、ターゲットシステムの同定を行った上で、ブラックボックスとしての情報システムに対するディペンダビリティ評価の重要性を確認する必要がある。事実、障害発生によるリスクと社会に与えるインパクトが年々増加している現在において、システムの開発サイ

クルとライフサイクルの短縮により、ディペンダビリティを価値規範としてもつ成熟した高度情報化社会への対応と基盤技術の確立が必要とされている。その際、ディペンダビリティ・メトリックとして何をどのように定義し、定量化すべきなのかについて明らかにし、さらに各評価主体（開発者・生産者、もしくは顧客・ユーザ）の立場に立脚したディペンダビリティ評価を実践することは重要である。

ディペンダビリティ評価における重要な側面は、具体的なターゲットシステムに対するディペンダビリティの測定法並びに計算法の開発である。可観測もしくは観測不能な情報に基づき、発生する可能性のある障害やフォールトの分類、要因解析、フォールト検出・回復処理のメカニズムを精査することが肝要である。一般に、計測データに基づいてディペンダビリティを評価する方法論をMeasurement based Approachと呼び、ディペンダビリティ・メトリック自体もしくはメトリックを構成する属性パラメータを直接計測することが行なわれる。実システムを用いた物理的計測実験だけでなく、テスト、プロトタイプの開発もこれに該当する。さらに、合理的にメトリックを評価するためのデータ測定技術、データマネジメント技術、評価主体と動作環境に応じたメトリック評価についても十分に検討する必要がある。特に、システム障害など、所謂、稀な事象を記述するためには数理解析もしくはシミュレーションに基づいたModeling based Approachが必要であり、計測とモデル化によるバランスのとれた評価法を確立することが最重要課題となる。

2．2．2 国際会議および研究機関調査報告

2005年秋に実施したCoimbra大学、Critical Software社、LAAS-CNRS、Airbus社への訪問や、各種国際会議（IEEE DASC 2006、EDCC 2006、ISSRE 2006）に参加して得られた知見について報告する。まずCoimbra大学とCritical Software社によって精力的に行なわれているFault Injection技術の開発と、DBenchに代表されるベンチマーキングに基づいたディペンダビリティ評価のための研究プロジェクトに強く印象を受けた。EDCC 2006で発表されていた多くの論文もこの話題に深く関連しており、この研究領域におけるヨーロッパのレベルの高さを感じ取った。コインブラ大学とCritical Software社以外にも、LAAS-CNRS、バレンシア工科大学、イリノイ大学アーバナシャンペイン校、カーネギーメロン大学は独自にFault Injectionシステムを開発しており、我が国における当該分野の技術動向が世界からは大きく遅れていることを痛感した。

しかしながら、Fault InjectionもMeasurement based Approachのひとつの技法であり、ユーザレベルのディペンダビリティ評価の観点からはまだまだ多くの問題が散見される。また、Modeling based Approachとの効果的融合例や経済価値へのロードマップなどは現状では明らかにされておらず、ターゲットシステムに関する具体的な目標達成型の研究プロジェクトの提案が必要不可欠であろう。また、単一の研究機関として最も多くの研究者を有し、ディペンダビリティ理論の創成期から世

界の研究拠点として君臨してきたLAAS-CNRSでの調査では、Fault Injectionのようなひとつの領域のみに特化することなく、研究領域を広く設定しながらもバランスのよいテーマを常に配備していることに印象を受けた。DBenchプロジェクトでもLAASはリーダ的な役割を果たしているが、ハードウェア、ソフトウェア、組込みシステム、セキュリティなど手薄な領域がほとんどないといった感想を持った。またAirbus社など産業界と密接に連携し、航空機制御システムに代表されるSafety Critical Systemsのディペンダビリティ評価プロジェクトを活発に実施している点も特徴的であったことを付記しておく。

IEEE DASC 2006やISSRE 2006に参加した経緯から、ソフトウェアシステムのディペンダビリティ評価の宇宙産業への応用も盛んに行なわれていることを知ったのは大変有意義であった。NASAが研究投資しているディペンダビリティ評価における各種（民需）要素技術開発や、IBM社が精力的に取り組んでいる自律計算（Autonomic Computing）分野は次世代ディペンダビリティ技術として大きな注目を集めている。事実、ディペンダビリティ評価技術の適用領域は依然広く、セキュリティ分野においては多くの未解決な領域が山積されているのが現状である。

2．2．3 今後の課題と展望

我国におけるディペンダビリティ評価に関する問題点として、官民学によるシステマチックな連携や、実用的なディペンダビリティ評価技術開発の必要性が挙げられる。実際、Measurement based ApproachとModeling based Approachの効果的な融合は多くなく、DBenchによる測定結果ですら有効なメトリックの算出には至っていないことが指摘されている。さらに、情報通信技術の開発サイクルとの同期調整の必要性を意識しながらも、普遍性のある基盤評価技術体系を構築するためには、高信頼化システムのディペンダビリティ評価プロジェクトを継続的に実施すべきである。また、ディペンダビリティ評価結果を通じて経済価値を創造するためのシナリオを模索することが重要課題であるにも拘わらず、ディペンダビリティ評価目的や最終到達目標まで至っている研究プロジェクトが未だに存在しないことを見聞することができた。すなわち、経済価値へのMappingという概念自体がディペンダビリティ評価分野においてまだ普及していないのが現状であり、その意味において、魅力的なターゲットシステムの選定や新しいディペンダビリティ評価技術の開発、価値創造に向けての方策について議論を尽くすことは非常に有意義であると考える。

情報システムのディペンダビリティ評価技術の開発は、我々人類が情報システムの恩恵を享受する限りにおいては避けては通れない重要な課題である。ディペンダビリティを最高の価値と位置づける基盤技術の開発は、我が国が情報システムの品質向上に向けて世界的なイニシアティブをとり、新しい情報技術に積極的に貢献してゆくためには、魅力的かつ最も効果的な研究領域であると確信している。

2．3　ネットワークサービスの評価メトリック　　中尾　康二（KDDI）

（以下は内容一覧）

ネットワークへの依存の高まりとセキュリティ被害の深刻化／日本におけるインターネット利用者／Internetを何に使っているのか／PCと携帯／家庭からのアクセス／A short history of computing & insecurity／最近のインターネットにおける攻撃／動画による脅威紹介／3-D実時間パケットフロー可視化／Botnetsの基本的な動作／IRCを介したHerder and Botの通信／IRC Protocol／SDBot.Bの場合のチャットやりとり／ボットを使ったSPAM mail business／ボットを使ったPhishing fraud／ボットを用いたDDoS attacks／Webアプリ高危険度脆弱性内訳／SQLインジェクション／フィッシングとは／フィッシング届出件数／フィッシングメール／ポップアップウィンドウ／アドレスバー偽装／紛らわしいURL／ワンクリック詐欺とは／ワンクリック詐欺の被害状況／ワンクリック詐欺の手口／不正侵入により、Web改ざん／守るべきもの、それは情報資産／情報セキュリティにおける脅威とは／セキュリティに関する脅威の分類／情報セキュリティにおける脅威の変化／脅威、脆弱性、および資産に対するリスク／インシデント事例／では、情報セキュリティの確保とは／情報セキュリティマネジメントの必要性（相関図）／情報資産のリスク分析、評価及び対応／情報資産への重要度付与（例）／脅威の識別／脅威の発生頻度の評価（例）-発生の確率-／脆弱性の識別／脆弱性の度合いの評価（例）／脆弱性の数値化について（ソフトウェアの例）／リスク値の定量的付与（例）／リスク値を低減させるための対応／情報セキュリティ対策とは（具体例）／リスク回避及び移転／企業におけるリスク分析／適切なセキュリティ対策の適用例：情報漏えい／リスク管理→セキュリティマネジメントとは／Information Security Management System（ISMS）の必要性 PDCA model／情報セキュリティマネジメントシステムの確保／ISO/IEC SC 27/WG 1における標準化によるセキュリティマネジメント確保／ISO/IECの組織構造／最新の活動：ISO 27000 ISMSファミリー国際規格／ISO 27002（17799）／情報セキュリティマネジメントガイドライン：17799／ISO/IEC 17799の改訂／ISO 27004／有効性測定の例／国内におけるISMS事業展開／ISMSとは／ISMS制度の目的／マネジメントシステム（PDCA）／マネジメント枠組みの確立／日本におけるISMSの体制／The Number of Certified Organizations／情報システムと事業リスク／企業運営における情報セキュリティマネジメントの位置付け／情報セキュリティマネジメントの問題点／従業員規模とセキュリティポリシー策定状況／情報セキュリティマネジメントの成功要因／取引先選定時の情報セキュリティ観点／ISMSの今後／日本ISMSユーザグループの役割／日本ISMSユーザグループの活動内容／ネットワーク事業者としての取り組み－Telecom-ISAC Japanの活動－／Telecom-ISAC Japanの目的／Telecom-ISAC Japanの概要／2004年DDoS攻撃対応事例（Antinnyワーム）／DDoS攻撃／ISPでフィルタ

ーをかけた場合は？／ターゲットサイトのＡレコードを削除。しかし／Antinnyワームの ISP ネットワークへの影響／ブラックホール IP による攻撃回避策／パケット破棄は各 ISP で設定した／広域モニターにかかわる活動／Telecom-ISAC Japan 全体システム概要図／ISP との連携を考慮した広域モニターの狙う範囲／ Telecom ISAC Japan のミッションフレームワーク／安全なネットワーク構築の指標（ITU-T）／ITU-T X.805 Approach／X.805 の利点／ユーザ視点からの活動／SPREAD 会員／ SPREAD の目的 SPREAD の位置づけ／SPREAD の仕組み／近畿ブロックの例／内閣官房における活動／内閣官房情報セキュリティセンター（NISC）の機能・体制／「第１次情報セキュリティ基本計画（仮称）」に向けた検討／「政府機関の情報セキュリティ対策のための統一基準（2005 年項目限定版）」（2005.9.15）／Evaluation Results of Information Security Measures regarding Terminals and Web Servers／How to See the Evaluation Results of Information Security Measures in the Government Agencies／効果的な ISMS 構築運用、これが狙い！！ 安心・安全のビジネス価値の向上に繋がる／重点研究開発項目／セキュリティ技術研究の鳥瞰図／広く相互に関連するセキュリティ確保／Interoperability is a Trust Issue

２．４　適合度評価による非数値的尺度（メトリック）

木下　佳樹（産業技術総合研究所システム検証研究センター）

２．４．１　自己紹介

私どもの研究分野は算譜意味論で、現職ではシステムの信頼性向上技法の研究をしており、情報処理システム開発の数理的技法の科学研究（算譜意味論、形式技法、定理証明の計算機支援）やフィールドワーク（技法導入実験による技術移転、研修コース研究開発）、ソフトウェア認証の技術基盤提供（計測標準研究部門（NMIJ、旧計量研）と連携して、OIML/D-SW（SC 5/WG 2）、IEC 61508などの規格に関係）などを行なっている。

情報システム開発の数理的技法とは、情報システムを数学の枠組で記述し、調べることによって、システムの信頼性を向上させる技法である。情報システムの記述のために用いられる数学は代数や論理学などの、いわゆる離散数学で、自然現象を記述するために用いられる解析学とはかなり違った数学が用いられる。パターン認識や有限要素法等でも数学が用いられるが、情報処理システムそのものを記述するのではなく、処理の対象を記述している。実際、これらには、自然現象を記述するのとおなじ解析学の系統の数学がより多く用いられている。

２．４．２　信頼性とディペンダビリティ

ディペンダビリティという言葉はいろいろに解釈されているようであるが、私ど

もは、ディペンダビリティ＝信頼性＋安全性＋セキュリティ＋可用性＋保守性＋公平性＋諸々のもの、と見なしている。セキュリティや信頼性はディペンダビリティの一部というわけである。

ところで、以下の☆に安全、セキュア、可用などなど、ディペンダビリティの他の性質のどれを入れても正しくなる。

『システムを☆に設計・実現しても、設計・実現の信頼性が低ければ☆なシステムとはいえない。』

したがって、「信頼性」はディペンダビリティの他の性質の基盤になっている、という点で特別なもののように思われる。この特別な関係があるために、信頼性実現の研究に携わる我々が、ディペンダビリティのいろいろな側面に関係することになっているのだと考えている。

2．4．3 認証＝規格＋技術文書＋認定

我々の仕事のもう一つの側面がソフトウェアの認証である。システムが基準を満たすことを、利用者は、製造者による宣言によって、あるいは第三者による認証によって知ることができる。第三者による認証のためには。次の三つが必要である。

1. 認証の基準を標準規格として提示すること
2. 認証の方針と手順の具体的かつ客観的な提示（Guidelines、技術文書）
3. 認証者がその能力をもつことの認定（認証者が多数になるときに必要）

2．4．4 適合性評価による非数値的尺度

既に述べたように、私どもは、組込システムの研究をしているわけではないが、組込システムの世界が近年、我々の研究分野に注目している、という関係にある。ソフトウェア認証に関連する活動を始めて五年になるが、その間、計量器組込ソフトウェアの認証立ち上げのお手伝いを主にやってきた。ご承知のように我国のNational Measurement Instituteは産総研の中の計測標準研究部門（旧計量研究所）で、同じ産総研の中にいるのでお手伝いしやすいという関係にあるからである。

さて、ソフトウェアに限らず、認証のためには評価が必要である。確かにソフトウェア認証でも評価はしている。ではそこでの尺度は何であろうか。ここに数値尺度は出てこない！

2．4．5 適合性評価による尺度

ようやく、今日お話したいことに到達した。

適合性評価は、指定された検証項目の集まりを満たすか否かの真偽値ベクトル（tuple）を与えるものである。真偽値ではなく、「実現の仕方」かもしれない。

そこで、このようにして得られたベクトルがシステムの（検証項目の集まりに相対的な）尺度（メトリック）であると考えてはどうかと考える。

適合性評価は、（ベクトルの形をした）尺度を『測定』する行為であるといえる。しかしこうして測定される尺度は数ではない。全順序でもないが、順序は

ついている。(False/Trueをtupleに拡張)。

2．4．6 何のための情報システム評価？

情報システムを評価するのは、同じ仕様のシステムが複数ある場合にシステム選択のためのデータ、あるいは発注したシステムを検収するためのデータ(注文どおりのものが収められているのかを判定する)を提供したいからであろうと思われる。

そのようなデータを使って、二つのシステムの評価を比べたい、あるいはシステ評価がある程度以上である、と言いたいわけである。

そのためには、評価の結果に順序(半順序)がついておれば十分だと思われる。評価結果は数である必要はなく、全順序ですらなくともかまわないはずである。

2．4．7 基準適合試験による評価？

情報処理システムが基準に適合しているかどうかは、数ではなかなか測れない。しかし、全体が基準に適合するかどうかのTrue/False、または基準がどのように満足されているかのデータを提供することはできる。そこで、評価基準の項目に「適合しているか否か」あるいは「適合のしかた」を評価の『尺度』(メトリック)としてはどうか、と考える。この尺度は数ではないが、比べられる。

2．4．8 評価基準の例：秤組込S/W(WELMEC 2.3より)

欧州の秤組込みソフトウェアの認証ガイドラインであるWELMEC 2.3から、評価基準の例をとりあげて、上記の提案の具体例とする。基準を満足しているか否かが数値で表しにくいことがよくわかっていただけると思う。

基準項目の例に、「普通の方法によってわざと行う変更から保護されていること」というのがある。これを満足する具体的な条件の例が二つある：

- 規制ソフトウェアがshellを通してのみアクセスされるものである、という条件。
- 規制ソフトウェアが、明確に規定されたインターフェイスを通してのみアクセスされる、という条件。

別の基準項目の例として、「規制対象外ソフトウェアとのインターフェイスが保護されていること」というのがある。これを満足する具体的な条件の例が以下の三つである。

- 規制部分に関するデータや機能を扱うプログラムモジュールを規定する。
- 保護されるインターフェイスによって実現する機能を規定する。
- 保護されるインターフェイスを通してやり取りするデータを規定する。

2．5　ソリューションサービスの評価メトリック　　笠原　裕（NEC）

ソリューション・サービスのディペンダビリティ評価の指標（メトリックス）を明確にする上での課題について紹介する。ソリューション・サービス分野では、システム側からではなくユーザの視点から「提供されるサービスが正確で信頼できる」ことがディペンダブルであることである。従って、評価の指標は、顧客満足度による評価やオペレータが介在する場合のディペンダビリティなど人間系を含んでいることや、重要インフラの場合などはシステムダウン時の社会的な影響も考慮することが要請される。

2．5．1　ソリューション・サービスのディペンダビリティ

ソリューションとは顧客に最適解を提供することである。ソリューションプロバイダは、顧客の要望に応じて、システム設計を行い、必要なプロダクトやサービスをコンポーネントとして組み合わせ、カスタマイズしてシステムとして構築する。複数のコンポーネントを複雑に組み合わせるので、ソリューションのディペンダビリティは、コンポーネントのディペンダビリティに左右される上に、組み合わせにより新たに発生する問題もある。また、ディペンダビリティに対する要求レベルも業種・業務や顧客毎に異なるので、評価指標もこれらを表現できることが必要になる。ソリューションが重要インフラを構成する場合などは、オペレーションに携わる人間系やシステムダウン時の社会的な影響も含めて性能や品質を確保することが要請される。

サービスとは、供給者と受給者が協同して価値を創造する行為である。サービスの特徴として、無形性、生産と消費の同時性などが挙げられ、さらにディペンダビリティ評価の概念は難しくなる。従事している人数でも売り上げにおいても、国内産業の70％近くがサービス産業であると言われており、製造業のサービス化も益々進展しており、情報システムが絡むサービスの割合も増えている。サービスの場合、受容者である顧客の満足度が重要な評価指標の代表的なものとなる。個人毎に要求水準は異なることが多く、指標化そのものと共に満足度を測る手法の開発が必要である。

2．5．2　ソリューション・サービスの事例とディペンダビリティ

①超ミッションクリティカルシステム

NTTドコモのiモード(*)センター「CiRCUS(**)」は今や数千万人のユーザの情報のライフラインとなっている。Webサイト閲覧毎秒5万アクセスとメール送受信毎秒2万5千件の処理能力があり、24時間365日無停止でサービスが提供されている。CiRCUSに代表されるような重要インフラで超ミッションクリティカルなシステムのディペンダビリティは通常のオフィスシステムとは要求水準の違いもさることながら、想定範囲も格段に広い。ディペンダビリティ評価の指標についても、ここまでで十分とは言い切れない面がある。

（*）iモードは、NTTドコモの登録商標です
（**）CiRCUSは、iモードサービスのシステムの名称です

②社会システム

図2.5.1は、総務省主管のナショナルプロジェクトとして進められている「緊急医療支援システム実証実験」の例である。無線LANと3Gの通信環境をシームレスにハンドオーバーすることで、救急車と病院間でのリアルタイムの音声・映像通信を可能にするものである。救急車と病院をリアルな映像で結ぶことで、医師の判断や病院側での準備、救急車内での初期処置などが可能になって行く。この仕組みには、情報システム、通信の安定性、医師、救急救命士などが含まれており、系としてディペンダブルであることの指標の設定は複雑である。このように、医療、教育、環境などの社会的なシステムではITシステムだけではなく人間系、社会的な影響なども含めてディペンダブルであるとは、どういうことかを指標化して行かねばならない。

③人間系が重要なファクタとなる例

昨今のシステム障害は、ヒューマンエラーに拠るものが多い。航空管制や証券会社の誤発注などのオペレータミスや、システム統合において人間組織間の連携が十分に行われていなかったために新システム稼働後に機能不全が見つかるなどの例がある。ディペンダビリティとして人間系を含んだ指標が必要であり、システム構築プロセスにおいても組織間連携などを評価する指標も必要かもしれない。

また、ソリューション・サービスの最終ユーザは人間である。ヒューマンインタフェースの観点からは、応答性能、画質、使い易さなどは個人毎に評価が異なる。さらに、顧客満足度に至っては定性的・情緒的であり指標化と測定

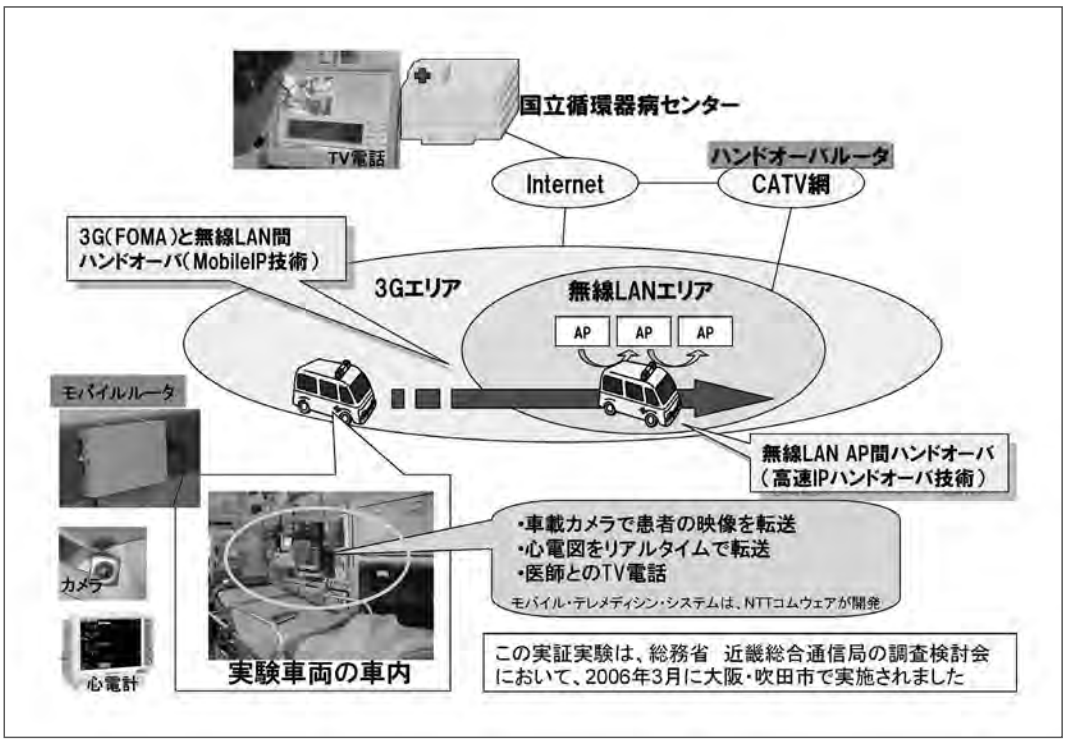


図2.5.1 緊急医療支援システム実証実験
―救急車と病院間でのリアルタイム音声＆画像通信―

方法が大きな課題である。

④市場環境に影響を受ける例

社会の急速な変化を予測できなかったためにシステム機能や性能が不足してシステムダウンを引き起こす例がある。また、チケットの申し込みの殺到や株取引の集中、オンラインゲームへの予想外の参加者数集まるなど、市場の動きの読み違いでシステムが機能不全になる例も散見されている。システム設計時のディペンダビリティでは不足することが、想定外の環境や事象のために起こっているのである。ディペンダビリティの指標の明示には前提となる条件の明確化が必要であり、これはSLAの問題とも関連する。

⑤通常の企業ソリューション例

図2.5.2は電子会議ソリューションの例である。利用者から見たソリューションとしての評価軸は、普通の対面会議と比べて同等の機能を果たせるかである。詳細には、音質、同時発話、リアルタイム性、臨場感などが評価の対象になる。さらに、投資効果という意味では、電子会議ならではのプラス機能のドキュメントやアプリケーションの共有が評価対象になる。ディペンダビリティという意味では、ダウンしない、会議の秘匿性、性能、E2Eの品質などが評価指標となる。一般のソリューションでは、サービスされる機能と投資効果を含む満足度が評価軸になると思われる。

2.5.3 課題

ソリューション・サービスのディペンダビリティ評価指標に関して、事例を挙げ

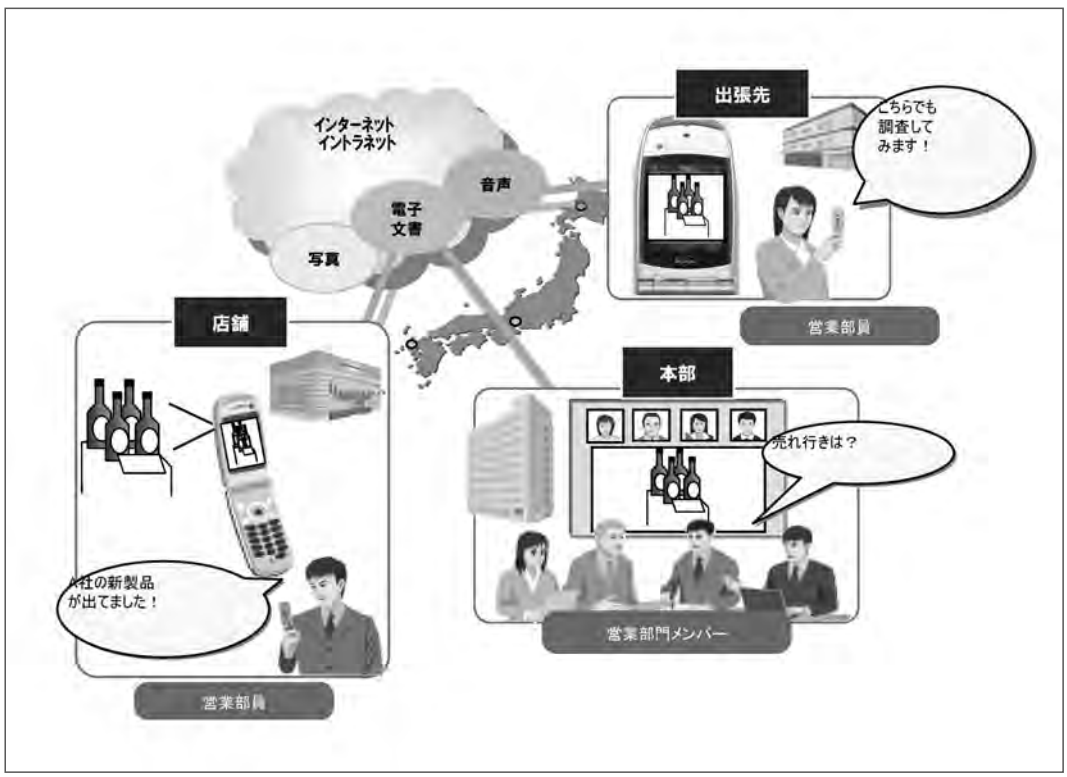


図2.5.2 電子会議ソリューションの例

ながら難しさを示してきたが、ここで改めて課題としてまとめておく。

ソリューション・サービス分野では、従来から情報システムのディペンダビリティ評価指標として使われている、可用性、信頼性、安全性、完全性、保全性などに加えて、ユーザ視点からの評価軸も必要である。また、ソリューション・サービスには人間系を含んだ評価指標が必要であり、重要インフラなどは性能要件や安全性に加えて社会的な影響までを評価指標に加えるべきである。

一方で、重要性は認識できるものの、人間系、社会的な影響まで含めたディペンダビリティをどう確保できるかは大きな課題である。評価が最終ユーザに委ねられる場合は定性的・情緒的になる場合も多く、如何に定量的な指標に分解して行くかは大きな課題である。時間軸の観点も重要で、社会的な変化を予測していなかった、思いもかけない使われ方をしたために発生するシステムダウンへの対処も技術・法律的な観点からつめて行く必要もある。さらに、コストも重要な要素であり、投資―リスクの問題を定量化して行く必要もある。

2．6　ディペンダビリティの経済価値

藤井　眞理子（東京大学）

2．6．1　高い企業の関心

米国における企業改革法（Sarbanes-Oxley Act）やその日本版といわれる金融商品取引法の成立などを背景として、企業における内部統制や財務報告の適正さ、さらにはこれらの裏づけとなる企業の情報システムのあり方などに対する関心が高まっている。これらの法律は、最高執行責任者や最高財務責任者に内部統制の有効性に関する検証や財務報告の適正性について、保証や高い水準の規律を求めるものである。

また、これらと関連したリスク管理の枠組みとして米国トレッドウェイ委員会（COSO）が提唱している「全社的リスクマネジメント（ERM：Enterprise Risk Management）」などへの関心も高い。さらには、災害等の関係から政府の防災計画においては事業継続計画（BCP）の策定が要請されており、災害などのカタストロフィックなリスクから日常の業務における多様なリスクまで、その認識と評価、対応が企業経営における大きな課題となっている。

こうしたなかで、現代の企業活動のあらゆる場面で不可欠の要素となっている情報システムについて、それが信頼に足るかどうかが重要な問題であるとの認識は、漠然とではあるかもしれないが広く共有されているものと考えられる。業務のあり方を示した当局の指針において「システムが安全かつ安定的に稼動することは決済システム及び銀行に対する信頼を確保するための大前提」とされている金融分野など、事業の根幹に情報システムのあり方が関わっている産業も少なくない。高い内部統制の規律などが必要な近年の社会経済環境を生かし、規制対応にとどまらない積極的な情報システムへの取組みを行うことこそが日本の企業にも求められている。

より質の高い情報システムが効率的

に供給されるためには、その経済価値が正しく評価されることが不可欠であるとの認識が今回のワークショップにおける問題意識と考えられるが、そもそも経済価値はどのように把握されるのか、順に考えてみたい。

2．6．2 ディペンダビリティの意義と評価

情報システムの利用者には、ベンダなど直接にシステムを用いて内部あるいは外部にサービスを提供する「直接ユーザ」と、エンドユーザにあたる「間接的な消費者」が考えられる。最終的には、サービスのエンドユーザとなる消費者から高い評価が得られるシステムでないと、ベンダなどの直接的な利用者にとっての価値も高まらないであろう。

エンドユーザがディペンダビリティに対してどのような経済価値評価を行っているかを知るには、そのサービスが日常的に把握できるものであり、市場で取引されているのであれば、価格（市場価値）がこれを知るもっとも手近な尺度である。さまざまな情報システム・サービス（あるいは商品）の中に「ディペンダブルなシステム」と「そうでないシステム」が存在し、消費者がその差を認識していれば、価値は価格差の形で把握できる。サービスが不特定多数に及び、価格が付けられていない場合に、消費者がその潜在的な価値を区別できるとしたときにはどれだけを払う意思があるかは、アンケート調査などにより知ることができるだろう。

市場における価格形成を促すために、サービスの水準を示した指標や最低水準の設定が役に立つことも多い。エンドユーザが理解しやすく、参照しやすいディペンダビリティの指標が定義できるのかどうかは一つの大きな研究テーマだろう。金融の例でいえば、「企業の信用度」という包括的な概念は格付機関が存在することにより指標化され、一般の投資家にも参照可能な情報となった。ディペンダビリティという概念が指標を構成する要素に分解できるのかどうか、また、それぞれの要素が客観的に把握され、定量化できるのかどうかについての深い議論も必要と考えられる。

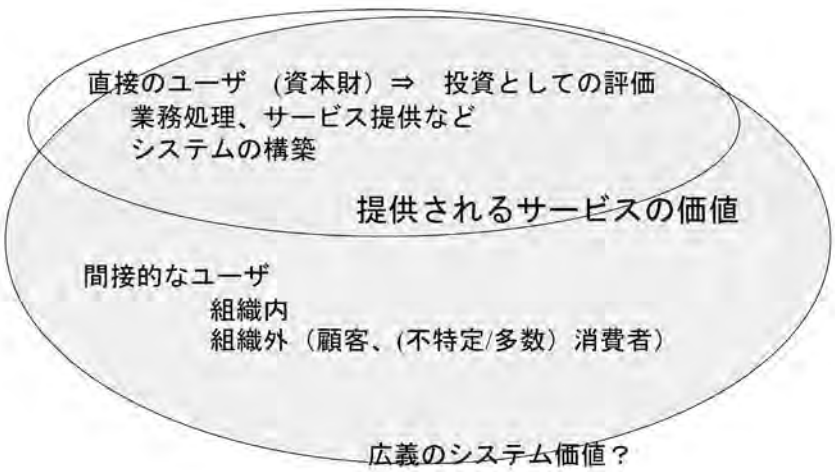


図2.6.1 情報システムが経済価値を生み出す体系

2．6．3　ディペンダブルな情報システムへの投資

直接的なユーザであるベンダなどにとっては、情報システムは重要な資本財である。すなわち、何らかの価値が付加されたサービスのフローを生み出すための投資と捉えられる。投資の経済効果は、一義的にはその投資により生み出されるフローとしてのサービスの価値による。サービスのフローとしての経済価値が資本化され、ストックとしての資産価値に反映されるわけだ。

資産の評価は、将来、その資産から生み出されるフローの価値とその時間パターンが評価できれば、現在価値として計算できる。現在価値で評価するためには、ディペンダビリティの時間変化も関係してくる。また、ディペンダビリティという価値は、従来の情報システムでは提供できない「まったく新しい価値の高いキャッシュフローを生み出すシステム」であることに基づくのか、あるいは、サービスは変わらないが保険つきのシステムであると理解すべきなのか、などディペンダブルな情報サービスをどのように規定するかも論点であろう。

ディペンダビリティが企業の生産活動に及ぼす効果は、いくつかの側面から整理できる。第1に、プロセス技術の効率性を高めるための投資という側面が考えられる。IT化は、米国では「ニューエコノミー」といわれるほどの画期的な影響を経済に及ぼしたことが知られているが、日本では産業別にみてもミクロレベルでみてもITや情報化投資が生産性の向上をもたらしたことを見出している実証研究は少ない。情報システムのディペンダビリティの効果だけを取り出して検証することは難しいとしても、基礎となる情報システム投資の経済効果、特に経済の供給サイドにおける実証研究を進め、その中で情報システムの優劣やIT投資の規模やタイミングが生産性に影響を与えるメカニズムが解明されればディペンダビリティの意義もより明確になるのではないだろうか。

第2に、リスク管理の側面からディペンダビリティを考えると、これがリスクの回避、防止、低減に資することにより「リスク軽減投資」としての意義を持つことが考えられる。耐震強化事業や治水事業、防災投資などと同様、よりディペンダブルなシステムへの投資が報われるケースが考えられる。

リスク管理とディペンダビリティの概念を効果的に結びつけるためには、まず期待損失額の定量把握や損失が生じる確率分布の特徴についての情報が必要である。システムの適切な運用が損なわれる場合に生じる直接ユーザ、間接ユーザの損失、企業活動における機会損失（BCPの側面）などを把握する手法を確立する必要があるほか、事故事例のデータベース（損失額、復旧費用、レピュテーションのマイナスなど）の構築などが役に立つ。損失額は、保険でいえば補償額に対応するため、客観的な把握手法がある程度合意される必要がある。

また、情報システムの不具合のリスクはどのようなタイプのリスクとして理解されるのか、事故確率の予想とディペンダビリティの関係を明らかにすることはとりわけ重要である。さまざまな事故は、多頻度であるが損害の程度は日常的と捉えられるもの、少頻度であり損

害も局所的に生じるもの、あるいは、少頻度ではあるが一度生じると破壊的な損害をもたらす可能性のある事故、などいくつかのタイプに分類される。リスク対処策の費用対効果を考えたり、制度設計を論じたりするには、こうしたリスクのタイプを正しく認識することが重要となる。

継続的な情報システムの運用においては、システムの質に依存したモニタリング/メインテナンス･コストも問題になるかもしれない。情報システムの質に応じた維持費用に係るプラス、マイナスの便益の程度を経済的に評価できれば、結果としてシステムの経済価値評価が容易になるだろう。

最初に述べたような企業のリスク管理のあり方を問う流れを勘案すれば、知的資産としてのリスク管理能力が企業価値を高める、あるいは、経営資源としての情報システムのディペンダビリティが安定した企業収益に貢献し、企業価値の向上につながるという側面も指摘できるだろう。伝統的なファナンス理論では企業が当該企業に固有のリスク(すなわち分散投資によって取り除くことのできるリスク)を管理しただけでは企業価値は高まらないとの考え方もあるが、適切なリスク管理により破綻の可能性が減少することが重要な場合も少なくない。「リスク管理は市場が評価する企業の価値をどのように高めるのか」という問いは、情報システムを通じたリスク軽減投資としての側面の価値を明らかにすることとも関連する問題であり、企業がディペンダブルな情報システムの導入をどのように正当化しているのか、といった実証分析を含め、これから分析が行われるテーマであろう。

2．6．4　ユーザ企業による経済価値評価

警察庁は「不正アクセス行為対策等の実態調査」を毎年行っており、その中に大手･中堅企業における情報セキュリティ投資の阻害要因についての回答がまとめられている。これをみると、「費用対効果がみえない」「どこまで行えばよいのか基準が示されていない」など、投資効果の判断の難しいことが阻害要因となっている状況がうかがえる。

情報システムの経済価値が実際的な意味を持つためには、供給者だけではなく、ユーザがこれを認識することが不可欠である。ディペンダビリティの価値も情報システムの価値と不可分であると捉えれば、情報システムの評価に必要と考えられる標準化された評価システムや必要な情報の開示、認証システムや継続的な評価システム、トラッキングレコードなどが重要であるほか、供給企業のマーケティングやブランディングなども関係するかもしれない。

供給側の企業が自ら生み出す情報システムの経済価値を明確に説明できたとして、現実に質の高い情報システムが流通するためには、ユーザサイドの企業がディペンダビリティという価値は最終的に自企業の価値向上をもたらすと判断できる見通しのあることが必要である。システム供給企業、ユーザ企業いずれの側においても業績の高まり等を通じて自らの価値向上につながると経営者が確信できる見通しがないと、実際の供給、あるいは購入のインセンティブには至らないであろう。

この点を考えると、経営陣にいかに

「情報システムのディペンダビリティの価値」を認識してもらうかが重要な鍵となる。企業を取り巻く最近のキーワードには、情報関係だけでも情報資産管理やITガバナンス、IT統制、情報システムの信頼性、情報セキュリティなどがあり、リスクマネジメントやBCP、企業の社会的責任（CSR）、法令順守に関連しては、不正競争防止法、金融商品取引法、個人情報保護法、製品・サービスの安全性など、実に多くの項目がある。これらはいずれもさまざまな形で相互に関連している概念であるが、その中で「情報システムのディペンダビリティ」がどのように位置づけられ、企業活動にどのような寄与をすると期待できるのか、他の重要項目と何が異なるのか、などについて明解なメッセージの発出が求められている。

3

現状俯瞰と重要研究課題に関する分科会検討結果

3．1　グループＡの検討結果

笠原　裕（グループＡリーダー）

ワークショップの目的は、情報システムのディペンダビリティ評価の指標（メトリックス）を明確にするための重要研究課題を抽出することである。グループＡでは、システム側からばかりではなく、サービスの視点、ユーザの視点からの評価メトリックスを検討し、それらの間の関係を考察することで課題抽出を行った。

エンドユーザの視点からすると、高可用性、高信頼性、完全性のレベルがいくつと言われてもぴんと来るものではなく、単に情報システムがダウンして大事なデータを失ったり、タスクが継続遂行できなくなったり、金銭的な被害を被ったりすることがないことを保証して欲しいというのが要請である。従来のディペンダビリティやセキュリティの分野で使われて来ている指標はシステム開発者・構築者向けの指標であって、しかも、情報システムに閉じた（人間系、社会的な受容性を含まない）指標であると言える。一方、システム側の視点からすると、情報システムを改善して行く上では、指標を定量化することが必要である。ダウンしないようにする、安全性を高める、といった表現だけでは、どの程度ディペンダブルなのか解らない。この種の議論を重ね、グループとして以下の課題を重要研究課題として提案した。

「ユーザ視点からシステム視点まで共通に、あるいは分解可能な形の指標の創出」

あくまでもユーザ視点を起点に置き、共通の言葉で語れるまでは行かないにしても、分解して行けばシステム視点に辿り付くことができる指標を創出しようというものである。指標が明確になることで、ユーザの要求、システム側が提供できる機能と対価といったものの透明性が増すという効用がある。ユーザ、ベンダそれぞれが自己責任を問われることにもなるが、一般的な社会の方向性として理に適ったものであるといえる。以下に議論の経過と議論の中で挙げられた主な討議ポイントについて紹介する。

3．1．1　検討のアプローチ

ディペンダビリティ評価の視点を、システム、サービス、ユーザの3レベルに分けて、それぞれのレベルにおける評価指標を挙げることから検討を行った。事前アンケートでワークショップ参加者から研究課題として提起されたテーマを、上記の3レベルに分け、同類の課題提案をまとめた。そして、グループの討議で重要な評価指標や研究課題と思われる項目を追加し、検討のスタートポイントとした（図3.1.1参照）。

図で、白いラベルがワークショップメンバーから事前に出された研究課題、水色、ピンクのラベルはグループＡの議論で追加した評価の指標や重要な視点項目である。図の左側がシステム視点、以下、右に進むに連れてサービス視点、ユーザ視点である。事前アンケートでも社会システム的な研究課題や経済的価値などの項目が多く挙げられている。ディペンダビリティ、セキュリティといった分野にまで、経済、社会、人間といった立場からの研究が重要であるという認識になってきているのが大き

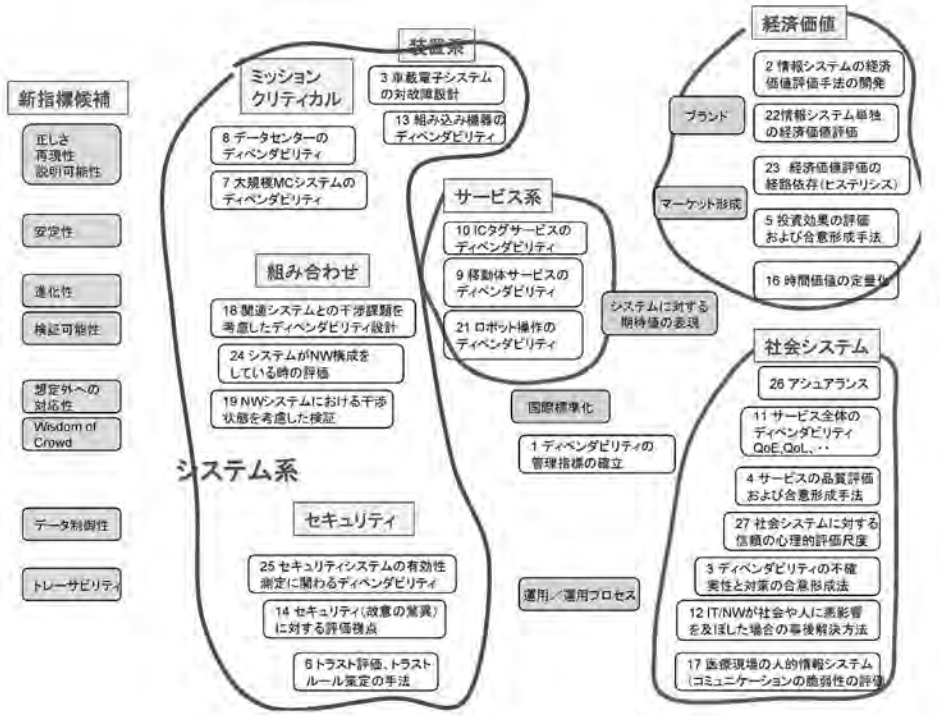


図3.1.1　事前アンケートによる研究課題のまとめと追加すべき指標の検討

な特徴である。

3．1．2　主な討議トピックス

ユーザにとって情報システムがディペンダブルであることは、ユーザの期待を裏切らないことに始まり、ユーザの期待をどう表現するのか、これを情報システムの評価指標にどうつないで行くのかが論点である。以下、取り上げた討議課題の主なものについて述べる。

■ ユーザの期待値とディペンダビリティ

ユーザにとって情報システムがディペンダブルであるということは、曖昧な表現かも知れないが、究極的にはユーザの期待を裏切らないことであると考えた。ユーザの期待の指標化は、いわばユーザが商品･サービス選択において参考にする指標を作ることであり、顧客満足度やユーザにとっての経済的価値などを如何に定量化するかなど非常に難しい課題を含んでいる。

ユーザの期待値の中に一定レベルのディペンダビリティが含まれれば、ディペンダビリティに対する投資もスムーズに行われると思われる。ディペンダビリティよりは遙かに世の中に浸透しているセキュリティでさえ、従来からセキュリティではお金が取れないとよく言われている。あって当然の機能であると思われがちだからであることと、必要以上の(期待値以上の)機能には投資は行われないからである。情報システムのディペンダビリティが、本来ユーザの期待値の中に含まれるべき機能として納得してもらうこと、このためにユーザに対する啓発活動を行っていくことも重要である。

■ ユーザ視点からシステム視点への分解：分解可能性／説明可能性

ユーザの視点からサービスの視点、システムの視点へと指標を分解して、シ

ステムレベルの定量的なディペンダビリティ評価指標につないで行くことが重要な研究課題である。人間系まで含めてシステムの規模が広がるに従って、構成要素の組み合わせ問題や、事故が起こった際に、どこで何が起こったのかトレースバックする機能が必須になる。この問題はディペンダビリティ評価の指標の分解可能性（ユーザ側からシステム側に向けて）、あるいは合成可能性（システム側からユーザ側に向けて）を明確にして行くことが課題となる。

■ 時間軸の重要性

情報システムのディペンダビリティを考える上では、時間軸の観点も重要で、社会的な変化を予測していなかった、思いもかけない使われ方をしたためにシステムが機能不全になる例も沢山ある。情報システムの設計時には必ず想定されている環境があるはずである。ディペンダビリティを評価する指標としては、想定範囲をどうパラメータに取り込むか？将来に渡ってどう保証するか、どう定義するかが課題となり、技術ばかりでなく法律的な観点も必要になるだろう。システムの進化で対応するのか、SLAといった契約条件の明確化で対応するのかなど具体的な方法を考えて行くことが必要である。

3．1．3　重要課題の抽出と研究推進方法

■ 重要課題

上記の議論を踏まえて、以下の研究課題を抽出した。

- ユーザ視点からシステム視点まで共通に、あるいは分解可能な形の指標の創出
- 結果の保証をするシステムの概念、構築方法
- システムにもPL（product liability）を課すことの国民経済的な比較検討

最初の指標の創出が重要課題である。図3.1.2に重要課題の位置づけを示す。

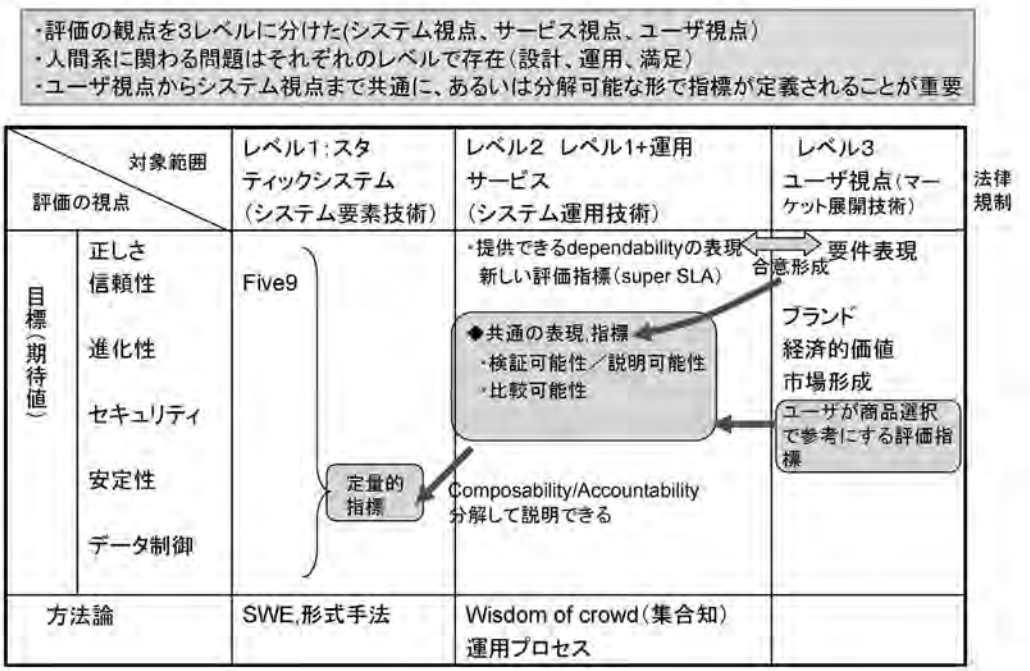


図3.1.2　ディペンダビリティ評価、重要研究課題の枠組み

この課題の解決により以下のような効果を得ることができる。

- 情報システムの機能·性能から、経済的価値までつなげることができる、これにより、ユーザ側、システム提供側が共通の言葉でコミュニケーションできる
- 情報システムの提供者と価値の受容者の間で、各種の透明性が増す機能·性能の要求水準、価格、動作の境界条件など
- 産業界にとっては、契約時の不透明性が削減され、オーバーロード／赤字プロジェクトの撲滅につながる
- ユーザにとっては、必要な価値だけを適切な対価で入手できる
- 究極的には、情報システムのディペンダビリティを記述する指標の国際標準化を推進することにより日本が技術的にも情報システムの認定においてもディペンダビリティ先進国となれる

■ 研究推進方法

ディペンダビリティ評価メトリクスを明確にするための研究推進には実証が必要で、テストベッドとしてのシミュレータ／エミュレータを開発して、これに経済モデルや人間系が関与する場合の条件も入れ込んで、指標が正しくディペンダビリティを示すことができるかを継続検証して行くというものである。また、超ディペンダブルなシステムを開発することで、必要とされるディペンダビリティの評価指標を精緻化して行くことも考えられる。具体的な場としては、防衛分野、宇宙分野、医療分野などが考えられる。NASA ではグランドチャレンジとして、市中に無人の自動車を走らせる実験を行うと宣言したようである。

3. 1. 4 今後の研究課題の俯瞰マップ

図3.1.3は、抽出した新しいディペンダビリティ評価の視点を縦軸に、とシステム視点～ユーザ視点を横軸に今後の

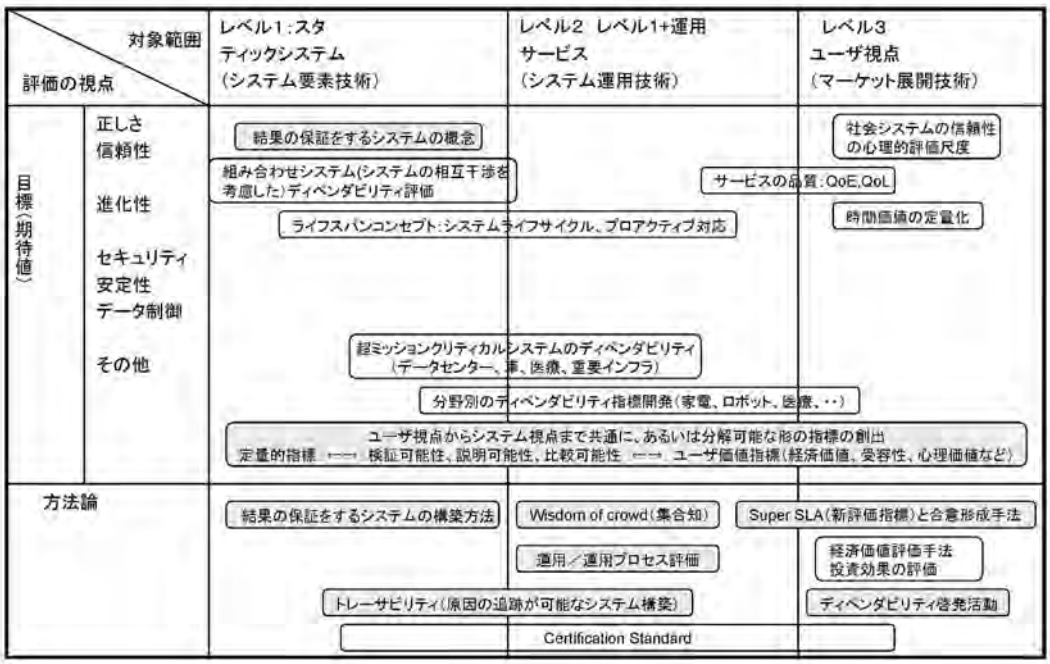


図3.1.3 今後の研究課題の俯瞰マップ

研究課題を整理したものである。

以上、ユーザ視点からのディペンダビリティ評価の指標創出の課題について検討し、重要課題として、サービス視点、システム視点の評価指標に分解して行くこと、実証を通して評価指標を繰り返し精緻化して行くことが重要であると考えた。今後、この検討結果の具体化が進んでいくことを期待する。

3．2　グループＢの検討結果

赤津　雅晴（グループＢリーダー）

グループＢの議論の出発点は、「なぜ今ディペンダブルなのか」という問いかけであった。ディペンダビリティという概念は決して新しいものではない。情報システムに対する信頼性や安全性に対する要求は、昔から絶えず存在してきた。それにもかかわらず、工業社会から知識社会への転換期といわれる今の時代にあって、ディペンダブルを再考することの背後にある新たな時代の要請は何なのか。それを議論することで、ディペンダビリティの新たな研究課題も見えてくるという目論見である。

社会生活や企業活動に関する多様な現状がメンバーから提示されたが、そこに共通していたキーワードは「変化」であった。例えば、従来では各企業が生業としている事業領域は比較的固定かつ明確であったが、業種の垣根はどんどんと取り払われて、異業種間の融合や他業種への参入は日常茶飯事に行われている。しかも、このような変化の激しさは、単に量的な側面にとどまらない。どのような変化が起こるかを事前に予測することが困難になってきている。その結果、起こりうる変化に事前に備えておいて、変化に柔軟に対応することも難しくなっている。

一方、人々の価値観や情報システムの目的も多様化している。また、情報技術の発達により、一人一人の要求に個別に対応することが比較的容易になってきた。インターネットの進展は個人へのパワーシフトを引き起こしている。この傾向は、情報システムのディペンダビリティにも影響を与えている。情報システムが故障しない、あるいは、故障してもすぐに復旧するといった基本的な要件は共通だとしても、それに加えて、情報システムを利用するユーザ各人からみて、「頼れる」情報システムの要件は多様化してきている。

このような背景から、情報システムのディペンダビリティ評価に求められることは、「変化」を前提としたものでなくてはならないということである。従来は、フォールトと呼ぶ不具合に対して、それが人為的なものであれ物理的なものであれ、情報システムの設計段階で、すべてリストアップして、それに備えるというのが、ディペンダビリティの基本的な考え方であった。しかし、これからは、設計段階で決めた基準が絶対ではなく、それは時間軸とともに変化するということを意識しなくてはならない。そして、様々な「変化」に対して情報システムを柔軟に適応させていくために、Plan-Do-Check-Action のいわゆる PDCA サイクルを回すことが重要である。

グループBでは、「変化」を前提にディペンダビリティ評価を考えていくという基本方針が固まったところで、次に、研究俯瞰マップの軸を議論した。ある情報システムがある変化に対してディペンダブルであるかどうかを評価するという文脈で考えたときに、結論として対象とする変化の特徴を以下の二つの軸で整理することとした。第一に、変化の対象である。具体的に言えば、その変化が情報システムの外部環境なのか、それとも情報システムの目的(内部仕様と言い換えても良いかもしれない)なのかという軸である。第二に、その変化の予測容易性である。

この二つの軸で構成される4つの象限で、それぞれディペンダビリティ評価の視点が変わる。以下、順に概説する。

1) 予測可能な環境変化:この象限に入る変化の典型例としては、事前に計画されたイベントに呼応したwebシステムのアクセス数の急激な変化があげられる。この象限の変化に対しては、変化の兆候をより早く、より正確に観測、予測することや、変化が起こったときに備えて多様な対策を準備しておくことが重要になる。

2) 予測不可能な環境変化:新種のコンピュータウイルスの発生が、この象限に入る変化の例である。ここでは、未知の攻撃に対して情報システムのアーキテクチャがいかに頑強であるか、技術に脆弱性がないか、アーキテクチャの技術の組み合わせが効果的に機能しているかといった点が評価のポイントになる。

3) 予測可能な目的変化:複数の情報システムを接続したり、既存の機能を継承しつつ機能拡張を図っ

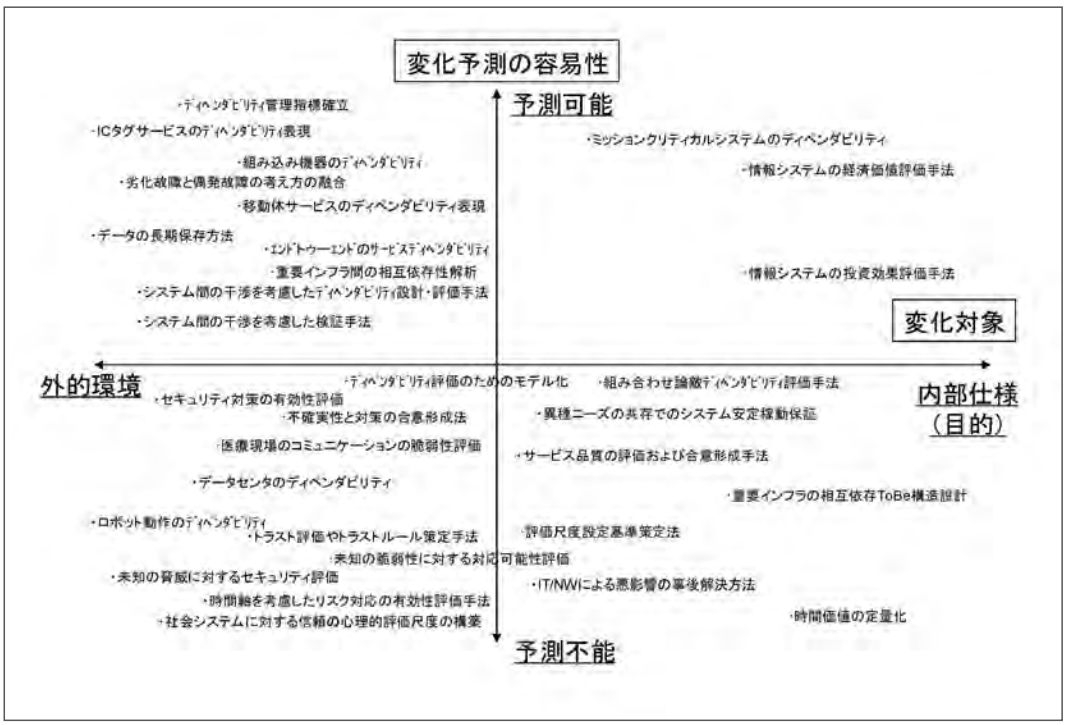


図3.2.1 「ディペンダビリティ評価」研究俯瞰マップ

たりするようなケースが該当する。このような変化に対して、情報システムには相互接続性や互換性などが要求される。

4）予測不可能な目的変化：ビジネス環境の変化や価値基準の変化によって、情報システムの目的も変わってしまうというケースである。例えば、JR東日本殿のSUICAのシステムは、駅改札の処理スピードを上げることが第一の目的であった。しかし、現在では、多様な決済機能という異なる目的も備えている。このような最初の設計段階では未知な目的の変化に対しては、情報システムのアーキテクチャの柔軟性が問われる。すなわち、ビジネス環境の変化に対して、情報システムの更改や保守がどの程度容易かが評価の項目に挙げられる。

以上の二つの軸上で、ディペンダビリティ評価に関する研究をマッピングしたものを図3.2.1に示す。

3．3　グループCの検討結果

丸山　文宏（グループCリーダー）

3．3．1　グループ討議のアプローチ

グループ討議を進めるにあたって、セキュリティと具体的なシステム（特に、医療システム）をターゲットとして検討していくこととした。特に、医療システムに関しては、脳外科手術のリアルタイムな映像をベースにした可視化システムによりスタッフの情報共有・コミュニケーションを実現する取り組みを対象とし

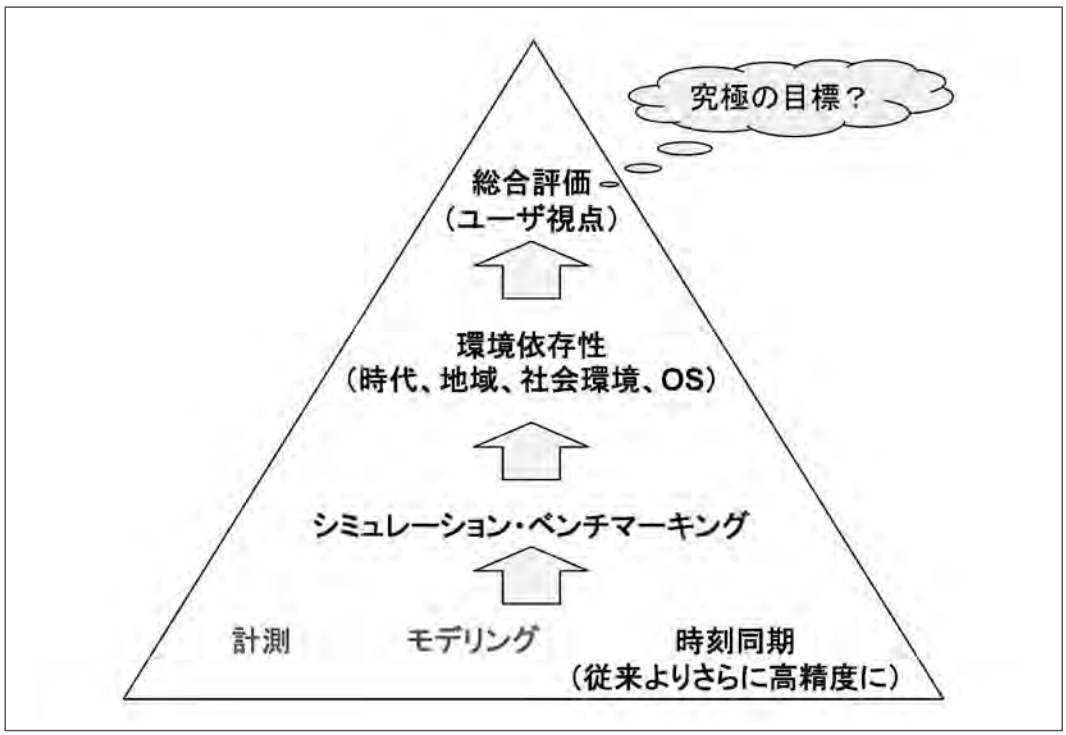


図3.3.1　「D&S評価」研究俯瞰マップの共通ベースとなる階層

て、人間系の比重が大きい情報システムのディペンダビリティについての具体的な議論を行った。

俯瞰マップの作成にあたって、その軸として何を設定するかが問題となった。例えば、情報システムの階層（情報システムに人間を含まないものから、人間系の比重が大きいもの、さらに、法律や社会制度などに深く関わるもの、といった階層が考えられる）や情報システムの分類（重要インフラ・システム、企業基幹システム、組み込みシステム、その他のシステム）を検討した。

最終的には、システムに対する人間の関与（X軸）とCriticality（Y軸）を設定したが、これに加えてもうひとつ別の切り口（言わば、X-Y平面の奥行きにあたるZ軸）もあるのではないかという議論となり、次の図に示す、共通のベースとなる階層を設定した。この図の意味するところは、D&S（ディペンダビリティおよびセキュリティ）をユーザ視点で総合評価するためには、計測、モデリングという下位のレイヤー（時刻の同期という技術的課題もある）をベースとして、シミュレーション・ベンチマーキング、環境依存性（時代、地域、社会環境、OS）というレイヤーを考慮しなければならないということである。

3．3．2　俯瞰マップ

次の図の俯瞰マップでは、システムに対する人間の関与を横軸、システムのCriticality（重大性）を縦軸に取った。

それぞれの領域に課題が存在するが、グループCでは、システムへの人間の関与が大きい領域（網掛けした領域）にフォーカスした。この領域を「ヒューマンファクタを含むD&S価値の可視化」と呼ぶ。その中には、D&Sリスク分析・管理、D&Sリスクコミュニケーション、SLA設計、ヒューマンインタラクションという課題領域が存在するが、大

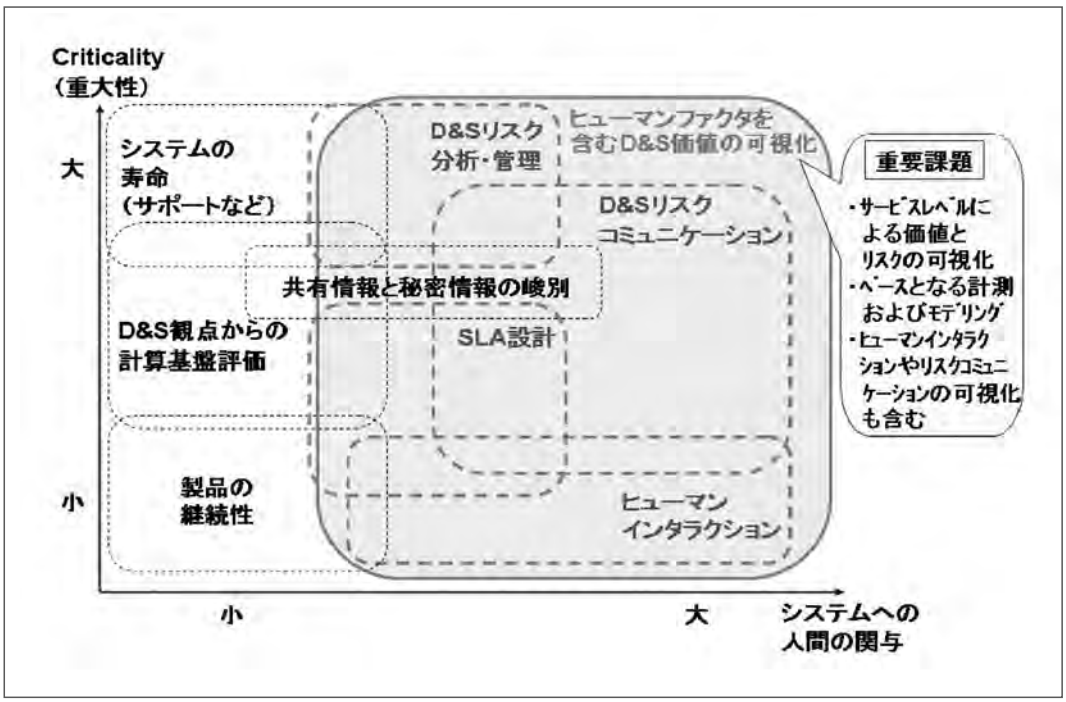


図3.3.2　俯瞰マップ

枠では、

- サービスレベルによる価値とリスクの可視化（ヒューマンインタラクションやリスクコミュニケーションの可視化も含む）
- 可視化のベースとなる計測およびモデリング

とまとめることができる。

3.3.3 重要課題

俯瞰マップに表現した課題をブレークダウンして、最も重要な課題として以下の6つを抽出した。

（1）計測

計測は、上記の俯瞰マップのどの領域にも共通に必要な課題である。通常の情報システムを対象にした計測技術は確立されているが、ヒューマンファクタや主観的な評価指標の計測・評価はまだこれからと言える。モデリングとの効果的融合も課題である。

（2）モデリング

モデリングは、計測と同様、上記の俯瞰マップのどの領域にも共通に必要な課題である。学問の基本的なベースとなるという意味でも重要な意味を持つ。様々なモデリングが可能ではあるが、もちろんどんなモデリングでも構わないわけではなく、実際のデータと整合性のあるモデリングが重要である。

（3）可視化

可視化には2通りの可視化があると捉えた。ひとつは映像データによる可視化であり、前述の脳外科手術のリアルタイムな映像をベースにした可視化はこれに当たる。もうひとつは取得データの可視化であり、「コックピット」と呼ばれるシステムやマイニング結果の可視化などがこれに当たる。研究の事例は多いが、製品レベルの事例はまだ少ないと言える。

（4）D&Sリスク分析・管理

リスク分析・管理は、もともと軍需の分野で進んでおり、日本では遅れている領域である。また、リスク分析は行われているが、必ずしも定量評価に結び付いていない。D&S（ディペンダビリティおよびセキュリティ）の観点からの定量評価も含めたリスクの分析・管理が課題である。

（5）SLA（サービスレベルアグリーメント）設計

SLA設計は、取り組みはあるが十分ではない領域である。特に、日本ではサービスレベルを曖昧にしておく傾向がある。障害かどうかの定義も明確でないケースがあり、これもサービスレベルを曖昧にしておく理由のひとつになっている。SLA設計については国際標準化も重要である。

（6）ヒューマンインタラクション

ヒューマンインタラクションは、特に人間の関与が大きい情報システムのディペンダビリティにとって重要な課題である。ユーザ視点からの定量的評価の取り組みはまだ少ない。

4

本ワークショップの提言

本ワークショップによる提言は以下の通りである。

1）情報社会はネットワーク化された情報システムをその社会基盤とする。エネルギー網、情報通信網、交通網、金融網、行政網などの重要インフラを含むあらゆる社会活動、産業活動、経済活動、政府機能は情報システムに依存している。このような情報社会の安全と信頼を保証するために、その基盤である情報システムのディペンダビリティとセキュリティを最高の価値とする情報社会技術の体系を構築することは、科学技術政策が目指すべき最優先課題の一つである。

2）ディペンダビリティは、自然現象に起因する物理的なフォールト、人間の営為に起因する人為フォールト、システムの複雑性と人間能力の限界に起因する相互作用フォールトなどの阻害要因の存在を前提にして情報システムへの信頼を獲得する技術概念である。一方、セキュリティは、悪意ある人間によるシステムへの不正アクセスや犯罪の可能性を前提にして情報システムの安全を確保する技術概念である。両者の研究コミュニティは、その歴史的経緯から、これまで互いに独立に活動しており、交流はほとんどなかった。しかしながらこの二つの概念および技術には共通点が多く、両者を切り離して議論することに無理がある。多様なリスクを内包する情報社会の安全と信頼を保証するためには、ディペンダビリティとセキュリティの概念・技術が互いに共鳴効果を持ちつつ統一化される必要がある。

3）サービスレベルにおけるユーザ（ステークホルダー）視点のディペンダビリティ評価がシステムレベルにおけるデザイナの設計目標にまで一貫性を保って分解されるメトリクス、また逆に、システム設計目標の達成がサービスレベルにおけるユーザ評価に合理的に帰結するようなメトリクスの開発が必要である。

4）社会の変化と技術の進歩によって情報システム自身の目的は進化し、情報システムを取り巻く環境も変化する。そのようなシステムの進化と環境の変化に対応したディペンダビリティ評価を可能にするアーキテクチャ、システムのライフサイクルを通じた評価プラットフォーム、その評価方法の体系化・構造化が必要である。例えば、SUICAは改札口の流れをスムーズにするという当初の目的から、電子マネーへと進化してきた。

5）人間要素を含む広義の情報システムに対して、ユーザ視点からの主観も含む評価メトリクスの定義、計測、モデリングとその可視化、リスク分析・管理、SLA（Service Level Agreement）方式の確立が必要である。

6）ディペンダビリティ／セキュリティの評価技術の正当性、有効性を確認するための相当規模のテストベッド構築が必要である。

付　　録

付録Ⅰ　ワークショッププログラム

「情報システムのディペンダビリティ評価」に関する ワークショッププログラム

◆ 開催日・場所
開催日：平成18年11月24日（金）～11月25日（土）
場　所：JST研究開発戦略センター2階大会議室
〒102-0084 東京都千代田区二番町3番地麹町スクエア2階

◆ 主　催
独立行政法人科学技術振興機構　研究開発戦略センター　生駒グループ
連絡先（TEL）03-5214-7484（担当：嶋田、伊東）
（FAX）03-5214-7385

◆ プログラム

第1日　11月24日（金）

全体会議

開催挨拶　丹羽邦彦　CRDSシニアフェロー　9：00～ 9：15
問題提起　（※以下の講演タイトルは仮題です）
ディペンダビリティ評価の重要性　9：15～ 9：40
南谷 崇　（CRDS シニアフェロー）
ディペンダビリティ評価研究の現状　9：40～10：05
土肥正（広島大学教授）
ネットワークサービスの評価メトリック　10：05～10：30
中尾康二（KDDI（株）技術統括本部セキュリティ部長）
組込みシステムサービスの評価メトリック　10：45～11：10
木下 佳樹（産業技術総合研究所　システム検証研究センター長）
ソリューションサービスの評価メトリック　11：10～11：35
笠原 裕（日本電気株式会社　ソリューション開発研究本部長）
ディペンダビリティの経済価値　11：35～12：00
藤井 眞理子（東京大学 教授）

グループ討議1　13：00～17：00

中間報告（全体）　17：00～18：00

グループ討議2　19：00～21：00

第2日　11月25日（土）

全体討議　9：00～12：00

グループリーダーから報告
討議・まとめ
閉会挨拶

以上

付録II　ワークショップ参加者一覧

「情報システムのディペンダビリティ評価」に関するワークショップ参加予定者一覧　（2006年11月24日、25日）

菊野　　亨	大阪大学 教授
土肥　　正	広島大学大学院 教授
森　　欣司	東京工業大学大学院 教授
佐々木良一	東京電機大学 教授 情報メディア学科長
木下　佳樹	産業技術総合研究所 システム検証研究センター長
篠田　陽一	北陸先端科学技術大学院大学 教授 NICT 情報通信セキュリティ研究センター長
中尾　康二	KDDI 株式会社　技術開発本部　情報セキュリティ技術部長
本間　浩一	フリーランス
丸山　　宏	日本 IBM 株式会社　基礎研究所長
赤津　雅晴	株式会社日立製作所　システム開発研究所第 5 部長
笠原　　裕	日本電気株式会社　ソリューション開発研究本部長
丸山　文宏	株式会社富士通研究所　IT コア研究所主席研究員
浅野　正春	株式会社日立製作所 オートモーティブシステム G 主管技師長
伊関　　洋	東京女子医科大学先端生命医科学研究所　教授
藤井眞理子	東京大学　教授
野島　久雄	成城大学　教授
高瀬　國克	電気通信大学 教授
松本　雅行	東日本旅客鉄道株式会社 JR 東日本 研究開発センター 担当部長
星野　利彦	文部科学省 研究振興局 情報課 情報技術推進室長
木村　裕明	文部科学省 研究振興局 情報課 課長補佐
小柳　尚夫	文部科学省 研究振興局 情報課 調査員
亀屋　俊郎	経済産業省 研究開発課 補佐
木俵　　豊	内閣府 科学技術政策担当 政策統括官付，総合科学技術会議事務局 参事官付
谷口　研二	大阪大学 教授・ CRDS 特任フェロー
小菅　一弘	東北大学大学院 教授・ CRDS 特任フェロー
三木　哲也	電気通信大学 教授・ CRDS 特任フェロー
田中　英彦	情報セキュリティ大学院大学 教授・ CRDS 特任フェロー
中島　啓幾	早稲田大学 教授・ CRDS 特任フェロー
今井　秀樹	中央大学教授・ AIST 情報セキュリティ研究センター長・ CRDS 特任フェロー
丹羽　邦彦	JST/CRDS シニアフェロー
南谷　　崇	JST/CRDS シニアフェロー
佐々木和則	JST/CRDS シニアフェロー
成瀬雄二郎	JST/CRDS シニアフェロー
波多腰玄一	JST/CRDS シニアフェロー
伊東　義曜	JST/CRDS 主任調査員
楠本　博之	JST/CRDS フェロー
石正　　茂	JST/CRDS フェロー
嶋田　一義	JST/CRDS アソシエイトフェロー
雄山　泰直	JST/CRDS フェロー
安藤　利夫	JST/CRDS 調査役
中神　雄一	JST/CRDS 主査
中田　一隆	（独）科学技術振興機構 第一係長
平川　誠也	（独）科学技術振興機構 主査
酒井　重樹	（独）科学技術振興機構 副調査役
薬師寺　崇	（独）科学技術振興機構 主査

付録Ⅲ　グループ構成

グループ討議の際のグループ分け

「情報システムのディペンダビリティ評価」に関するワークショップ（2006/11/24-25）

【グループA】

@会議室A：2F大会議室

笠原　　裕	日本電気株式会社　（リーダー）
菊野　　亨	大阪大学
篠田　陽一	北陸先端科学技術大学院大学 NICT情報通信セキュリティ研究センター
丸山　　宏	日本IBM株式会社
浅野　正春	株式会社日立製作所
藤井眞理子	東京大学
今井　秀樹	中央大学　産総研情報セキュリティ研究センター JST/CRDS
小菅　一弘	東北大学大学院　JST/CRDS
丹羽　邦彦	JST/CRDS
石正　　茂	JST/CRDS

【グループB】

@会議室B：2F中会議室

赤津　雅晴	株式会社日立製作所　（リーダー）
森　　欣司	東京工業大学大学院
木下　佳樹	産業技術総合研究所
中尾　康二	KDDI株式会社技術統括本部
高瀬　國克	電気通信大学
野島　久雄	成城大学
佐々木和則	JST/CRDS
嶋田　一義	JST/CRDS

【グループC】

@会議室C：3F大会議室

丸山　文宏	株式会社富士通研究所　（リーダー）
佐々木良一	東京電機大学
土肥　　正	広島大学
本間　浩一	フリーランス
松本　雅行	東日本旅客鉄道株式会社　研究開発センター
伊関　　洋	東京女子医科大学
三木　哲也	電気通信大学　JST/CRDS
谷口　研二	大阪大学　JST/CRDS
成瀬雄二郎	JST/CRDS
伊東　義曜	JST/CRDS
波多腰玄一	JST/CRDS

付録Ⅳ　事前アンケートまとめ

アンケート集計結果（「情報システムのディペンダビリティ評価」に関するワークショップ　@JST／CRDS　H18.11.24-25）　　配布資料4

研究課題	研究により問題が解決された場合のインパクト あるいは、解決されない場合の影響	何がその問題の解決を困難にしているのか ※可能ならば、以下の点にも言及してください。 ・その課題に対する現在のアプローチの限界 ・まだ十分ではないが、見込みのありそうなアプローチ ・まだアイデアは提案されていないが、望ましいアプローチ
ディペンダビリティ管理指標確立に関する研究	解決した場合のインパクト システムの客観的評価が可能となる指標ができれば、システムの運用のいろいろな形態（故障、改修、改良、取替、テストなど）によるシステムの能力、限度などの比較ができるので、開発へのインセンティブが生じる。 解決されない場合の影響 定量的な比較ができないため、経済価値に転化しにくい。	何が課題解決を困難にしているか 故障以外のシステム形態の評価に関する研究がまだ少ない。システムの応用分野によって形態がさまざまに変化する。 要求レベルが多様である。 可能なアプローチ 現在はフォールトトレラントなどであるが、これを改修・取替などに演繹的に適用する。 アシュアランス技術の適用などについても検討する。
情報システムの経済価値評価手法の開発	解決された場合のインパクト 情報システムの市場取引が容易になることによる取引の拡大、質の高いシステムの供給、効率的な情報システムへの投資につながることが期待される。 解決されない場合の影響 効率的な情報投資が実現されない。	現状 情報システムやそのディペンダビリティの概念が社会科学分野あるいは企業の経営者等に十分理解されておらず、情報システムのディペンダビリティを価値として評価するという認識が低いように見受けられる。 環境（システム）などについては、負の価値の認識（公害、海域汚染の問題等）の場合も含め、経済価値評価の手法が提案されている。 ユーザーが特定される場合から取り組み、不特定（多数）のユーザーの場合に拡張する、あるいは、ディペンダビリティの重要性などに応じた具体的事例を想定して研究を進めてゆくことが有効ではないか。
ディペンダビリティの不確実性と対策の合意形成法の検討	確率に関しては常に不確実性が伴い、ディシジョンが困難になる。また、意思決定にはいろいろな関与者がおり、合意形成過程だ大切となる。	多重リスクコミュニケータの開発（JST　RESTEXの「情報と社会」の中で検討中であり見当結果を参考までに添付します。）
サービス品質の評価および合意形成手法 （情報システムによって影響を受ける人、組織、社会の立場から、情報システムの品質を評価する）	利用者の事前の期待と事後の満足度とのギャップを減らすことによって、アウトソーシングサービスや保守・監視サービスなどの事業拡大、付加価値向上を図り、情報・通信産業の発展を促す。	課題解決が困難な理由 情報システム提供側と利用側の認識のギャップ（例：提供側…可用率、利用側…業務停止によるビジネス損失）が大きく、それを埋める手段がない。 可能なアプローチ JEITAや総務省などからでているSLA（Service Level Agreement）策定のためのガイドラインは、議論のベースにはなる。しかし、十分に利用者視点にはなっていない。
投資効果の評価および合意形成手法	SIビジネスにおいて、人月単価×開発工数で価格が決まってしまう現状では、コスト競争力で中国やインドには勝てない。ビジネス視点での情報システムの価値の明確化を通じて、価値ベースの価格設定、競争を実現することにより、情報・通信産業の競争力を強化する。	課題解決が困難な理由 情報システム単独では価値を生まず、その価値はそれを使う人や組織、業務プロセスに依存する。 可能なアプローチ 直接財務的な効果を算出するのではなく、情報システムの効果を評価する指標群（KPI：Key Performance Indicator）を用意して、KPIレベルでの合意形成から入る。
トラストの評価やトラストルール策定の手法	web上に存在する膨大な情報、知識、エージェントの中から、信用できるリソースを抽出する手段を各人が持つことによって、健全な情報化社会を実現する。	課題解決が困難な理由 リアルな世界においても難しいテーマであるのに加えて、「顔が見えない」ということに関連して評価のための情報が不足している。 可能なアプローチ SNS上に流れる情報に対するキーワード解析やコミュニティ参加者の社会構造分析などは利用できるか。
大規模ミッションクリティカルシステムのディペンダビリティ	解決された例：ドコモのサーカス。それまでのシステムダウン頻発に比較して、圧倒的な頑健性を示した。最近は、年間のダウン時間が数秒のオーダーになった。 解決されなかった例：東京証券取引所。市場に混乱を引き起こし、国内の景気にさえ影響を与えかねなかった。	現状のミッションクリティカルシステム構築は、個別のシステムに対する最新のチューニングによって実現されている。いわば、匠の世界。 より工学的に取り組み、きちんと設計する事が重要。 パフォーマンスエンジニアリングを提案する。上流設計段階から、性能を作り込む、デザインすることが重要。
データセンターのディペンダビリティ	ASPやSaaS、ユーティリティコンピューティングなどが一般的になると、データセンターが社会インフラとして非常に重要な地位を占める。これがダウンしたり、サービスレベルが低下したり、あるいはデータロスが起こったりすることは絶対にさけないといけない。 企業活動から、広く国民一般の生活にまで影響を与える。	データセンターがそれぞれ個別に運営されているため、局所的な災害等にも影響を受けてしまう。 複数データセンターがお互いにバックアップ可能にしておけば、壊滅的な被害は避けうるものと思われる。
移動体サービスのディペンダビリティ表現 （モバイル／無線LAN）	インパクト　サービスの透明性が得られていない 例：モバイル／WiFiは、有限の資産を割り当てているだけなので、極めて不透明になっている。 サービスを向上させるために、評価尺度が必要。	・コンピュータシステムの耐故障概念が強い MTBFとかMTTR、稼働率が支配してきた。 ・電話の呼損率のようなメジャーが必要
ICタグサービスのディペンダビリティ	現状　モバイルや物流に適用されるRFIDなど、ICタグを利用したサービスが増えている。 解決されない場合　安心してタグを利用することができない。必ず、確認する仕掛けをいれないと実用には供さない。	読み取り装置は偏波をかけているので、タグの向きにより、（原理的に）読めない場合がでてくる。
サービス全体のディペンダビリティの研究 （例として、 QoE（Quality of Experience、体験の質）/ QoL（Quality of Life）/ QoG（Quality of Governance）/ QoX・・・）	現状　主としてネットワークの分野で、帯域と遅延許容時間のトラフィック・サービスを保証するレベルでしかなく、上位サービスのエンドエンドでのディペンダビリティの研究は途上段階。 インパクト　上位サービスの価値を客観的に評価することで、サービス商品の差別化、品質向上、価格の適正化が可能になる。	・上位サービスの多様性、人の価値観の多様性への対応が困難 ・IPTVのQoEに関してはITU-T/SG13で議論中

研究課題	研究により問題が解決された場合のインパクト あるいは、解決されない場合の影響	何がその問題の解決を困難にしているのか ※可能ならば、以下の点にも言及してください。 ・その課題に対する現在のアプローチの限界 ・まだ十分ではないが、見込みのありそうなアプローチ ・まだアイデアは提案されていないが、望ましいアプローチ
IT/NWが社会や人に悪影響を及ぼした場合の事後解決方法:	現状　従来のIT/NWセキュリティはIT/NWが外側から受ける脅威に対してCIA(Confidentiality, Integrity, Availability)を保持すること。IT/NWから外側(人や社会)へ悪影響を及ぼすことを防ぐ、あるいはそうなった場合の責任分解と解決策についての研究が途上。現状は技術的手段ではなく裁判などの法的手段に委ねられている。	・十分ではないが現在行われているアプローチは以下 － METIで検討中の「情報システムの信頼性に関するガイドライン」とそれに基づく「信頼性評価指標」の作成、認証制度・保険制度・政府調達での活用 － 裁判外紛争解決手続(ADR)法による認証制度
組込み機器のディペンダビリティ	[解決されない場合の影響] バリエーションが多数ある組込み機器の評価指標がない場合、ユーザが機器を選択する際、定量的な判断を容易に行うことが困難。特に情報家電などコンシューマ向け機器の場合、利用者に対してディペンダビリティによる付加価値訴求が難しくなる可能性がある。	●機器のカテゴリ分けなどにより、利用者が機器を選択する場合の比較を行える指標が必要 ●接続性、拡張性、耐障害性など個別に評価する項目と、機器トータルでの評価などが考えられる。
セキュリティ(故意の脅威への対応)に関する評価視点での検討	解決された時のインパクト: ・システムの「安心」を実現する際に必要となる評価をすべて網羅した評価が可能になる。 解決されない時のインパクト: ・実際のシステムがさらされる脅威の解決は半分(意図しないものだけ)しか評価できていないことになる。	セキュリティとディペンダビリティが領域は重なるがアプローチが違うコミュニティで検討されていることが多いため。 ・それぞれの専門化で共通の認識を作れるフレームワークの策定と両領域の専門家による集中討議が必要。
ディペンダビリティ評価のためのモデル化	解決された場合のインパクト: エンドユーザの行動予測や需要予測などの予測、および、異常検出などがモデルをベースに可能となる。 解決されない場合の影響: ケースバイケースのアドホックな対応になり、きちんとした形で知見が蓄積されていかない。	何が課題解決を困難にしているか: ・測定されたデータの不足(モデル化に必要なデータが不足) ・システム／サービス毎の個別性
時間価値の定量化	解決された場合のインパクト: システム／サービスのメリットとして作業時間の短縮を謳っているものが多いが、それが実際にどのくらいの価値に結び付くのか明確になる。 解決されない場合の影響: 時間の価値と他の経済的な価値を一律で比較することができない。	何が課題解決を困難にしているか: ・ユーザや状況毎に時間の価値は異なる ・時間とその価値を結び付けるデータの不足
医療現場の人的情報システム(コミュニケーション)の脆弱性の評価方法の開発	解決された場合のインパクト: リスクコントロールされた医療環境 解決されない場合の影響: 医療環境の悪化に歯止めがかからなくなり、最終的には医療システムの崩壊につながる恐れがある。	何が課題解決を困難にしているか: 収集される情報に客観性が欠けている。客観的観測手段が確立されていない。情報を総合的に管理し評価するシステムが確立されていない。 現在のアプローチの限界: 現在の唯一の資料は、ヒヤリハットレポートであるが、認知された事象だけしか報告されていない。認知されていない事象が放置されるため、本質的解決につながらない。 可能なアプローチ: 客観的観測手段を構成し、客観的評価を可能にする。 評価方法の妥当性を検証する。
1. 周囲の関連システムとの干渉課題を考慮しながらのディペンダビリティ設計・評価手法の開発	協調システム(ネットワークシステム)のディペンダビリティを机上評価できるので、 @ディペンダビリティを確保しながら @開発工数の削減、期間短縮　が可能。 ネットワークシステムの複雑化に対応できず、信頼性の確保ができない。	個々のシステム毎に、最適な設計環境を構築している。 ⇒ 複数のシステムを共通的に開発・評価するツールがない。
2. ネットワークシステムにおいて、システム間の干渉状態も考慮しながら、検証条件を生成するための 「理論」「アルゴリズム」「ツール」の開発。	ディペンダビリティ評価のための検証の質が向上する。(抜けのない検証ができる)	設計者にとって、干渉状態を把握すること(＝干渉状態を可視化すること)が難しい。
3. 車載電子システムの耐故障設計のために、「劣化故障」の考え方を「偶発故障」に評価基準を変更する考え方を確立すること。	「電動化設計」を理論的裏付けをベースに実行できる。	「劣化故障」と「偶発故障」の接点を見出せるか？
ロボット動作のデペンダビリティの研究	解決された場合のインパクト:従来工場の柵に囲われて作業していたロボットが人間の生活の場に入り込みサービスをすることが可能になる。 解決されない場合の影響:今後の高齢少子社会における福祉はロボットの導入が鍵となる。人間に対する絶対的な安全性なしではロボットのこれ以上の応用は困難である。	動作環境が不定形、非定常な非整備環境である。あらゆるバリエーションに対応できる制御法が確立されていない。 ・非整備環境におけるロボット動作のデペンダビリティの評価法自体が分かっていない。 ・人間並みのロボットの実現は不可能、人間の生活環境にある程度の整備を与え、デペンダビリティ評価を可能にする動作体系の構築から始める。
情報システム単独の経済価値評価(ディペンダビリティ、セキュリティを議論する以前の問題)	システム開発の投資マネジメントの合理的指標になるでしょう。	システム単独で経済価値を生むわけではない。事業全体の経済価値評価の手法は共通の考え方があると思いますが、システム単独の評価を切り出すことができません。
経済価値評価の経路依存(ヒステリシス)	例:セキュリティ対策の投資額、時期の決定に寄与。(例えば、1万人の個人情報漏洩事故が起きた場合、2002年と2006年では経済価値評価が違うと思われます。)	企業単独、システム単独で評価することはできない。社会情勢に応じて環境要素のウェイトを時間に応じて変える必要があると思いますが、モデルも参考指標もありません。
システムがネットワーク構成している場合の評価(システム同士がネットワークを構成している場合。単独システムの評価の合計は全体の評価にはならない)	単独企業内でも、複数のシステムがある場合に。どのように評価すればいいか困っています。	

研究課題	研究により問題が解決された場合のインパクト あるいは、解決されない場合の影響	何がその問題の解決を困難にしているのか ※可能ならば、以下の点にも言及してください。 ・その課題に対する現在のアプローチの限界 ・まだ十分ではないが、見込みのありそうなアプローチ ・まだアイデアは提案されていないが、望ましいアプローチ
セキュリティシステムの有個性測定に関わるディペンダビリティ	解決された場合のインパクト： リスク評価が十分になされ、セキュリティ対策の実施に関わる有効性が明確化され、投資効果が明白となる。 解決されない場合の影響： 実施するセキュリティ対策の有効性が明確にならないため、どこまで投資してよいのか曖昧となり、セキュリティ確保の継続が困難となる。	有効性の評価指標が一元的に定義できず、評価のクライテリアが企業により異なる。 ・現状、他企業における事例に準拠したり、評価指標が漠然とした一般論になってしまう。 ・有効性評価指標を与えるための一般的な導出手法がなく、例示に留まっているといった限界がある。 ・多くの事例から、より具体的な評価指標の導出ロジックを構築していくことが考えられるが…
アシュアランス	社会のニーズを反映したシステムの構築、運用に有用な実践的評価基準が求められる。システムを取り巻く環境が変化し、ユーザニーズが多様化しており、動的なシステム・環境において異種のニーズを共存させ、システムの安定稼動を保証させることが緊急の課題である。	ユーザの視点のみならず、システムの安定稼動を保証するにはオペレータの視点をも取り込む必要がある。 異種システム、たとえば制御と情報のシステム共存があり、双方の知見を反映させなければならない。
社会システムに対する信頼の心理的評価尺度の構築	チャレンジのために受け入れるべきリスクと安全確保のために避けるべきリスクの区別がなされていにことにより、過度に安全サイドに振られ、チャレンジをする機会が失われている（たとえば、子どもの遊び環境） また原発・電磁波などに対する過度の不安の発生。	リスクの心理的評価尺度についての研究が不足していること。また、リスクの受容についての社会的合意がとれていない。

付録Ⅴ　講演資料

付録Ⅴ．1　ディペンダビリティ評価の意義

ディペンダビリティ／セキュリティ評価技術の意義

科学技術振興機構
研究開発戦略センター

2006.11.24-25　JST-CRDS（麹町スクエア）

情報社会の信頼と安全

子供の遊びから国家安全保障に至るまで人と社会のあらゆる活動が情報システムに依拠

最高の価値　ー　情報システムの提供するサービスが良質で信頼でき、
人の生活と社会の活動が安心してそれに依拠できること！

障害の原因となる様々なフォールト発生や不正侵入の脅威が増大している！

自然現象による物理フォールト
半導体・実装部品の経年劣化、自然界からの電磁波の影響など
過失による人為フォールト
ソフトウェアやLSIの設計ミス、システム操作ミス、設計仕様や保守文書の記述ミス、
悪意による人為フォールト
不正侵入、ウィルス感染、DDoS攻撃、サイバーテロなど
相互作用によるフォールト
オープン環境での仕様ミス、異種システム統合ミス、ネットワーク家電の接続不具合

万一の障害（期待するサービスの停止、想定外の事態）が発生すると、
社会の混乱、人命の損傷、財産の逸失、安全保障への脅威など
最近の例：鉄道事故、航空管制トラブル、銀行システム障害、サーバ不正侵入
東証の売買システム停止、ファイル交換ソフトによる重要情報流出、、、

戦略イニシアティブ「ディペンダビリティ宣言」(印刷中)

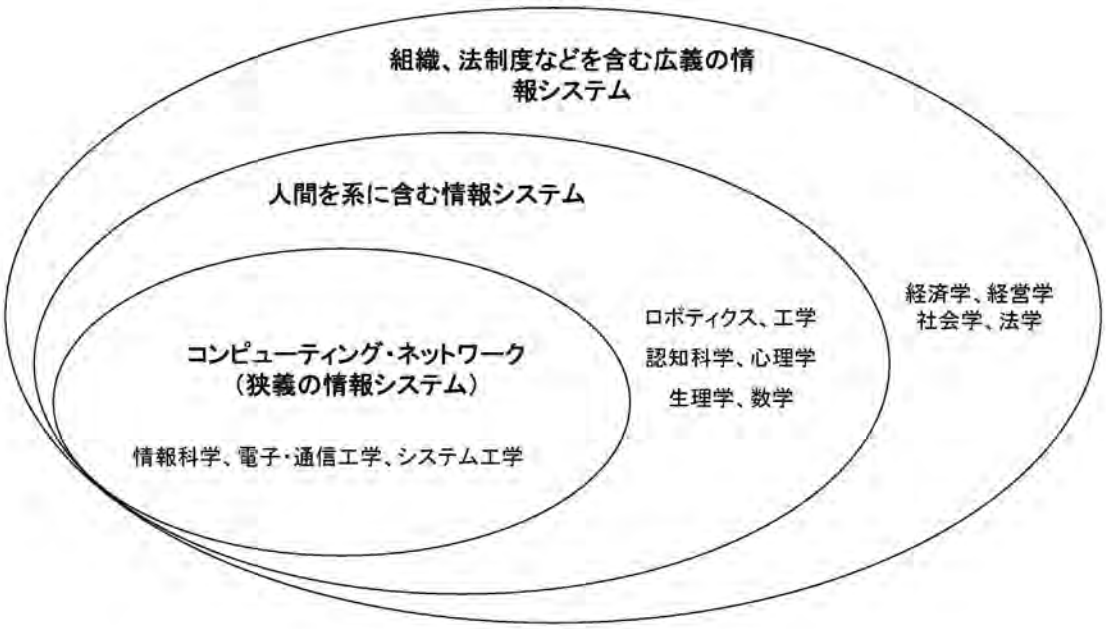
情報化社会の安全と信頼を担保する情報技術体系の構築

～ ニュー・ディペンダビリティを求めて ～

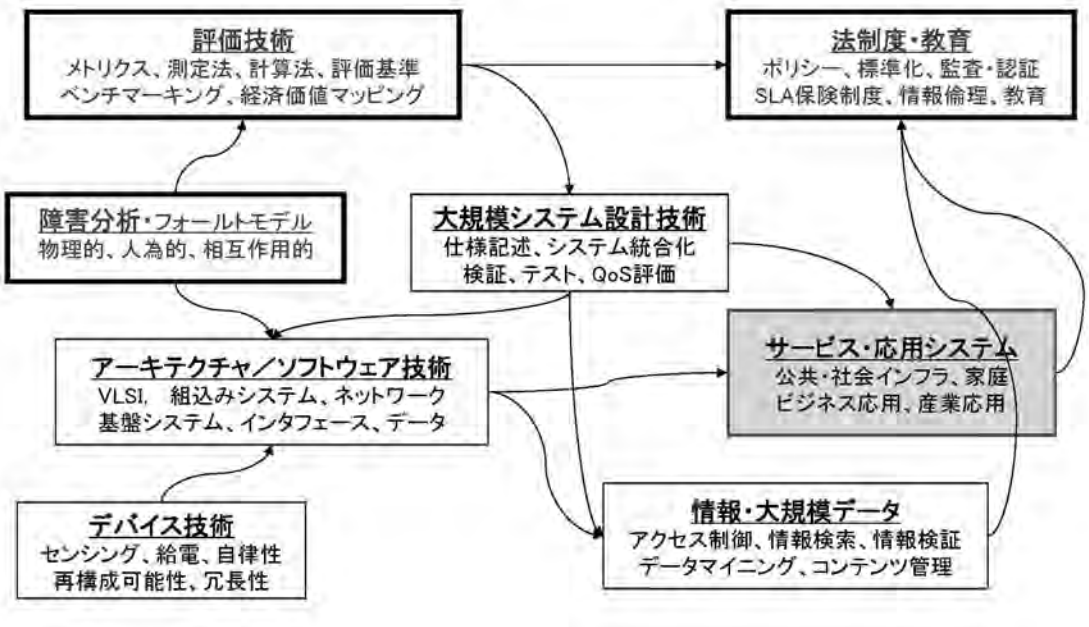
- 情報化社会の安全と信頼を担保し国際競争力の強化に向けて、「ニュー・ディペンダビリティ」を最高の価値とする新しい情報技術体系の総合研究開発戦略を推進するべきである
- ニューディペンダビリティ:
  情報システムのディペンダビリティとセキュリティを社会システムにおけるユーザー視点で融合する新概念

  - 情報社会の安全と信頼を担保する技術基盤の確立
  - 新しい経済価値創出による産業競争力の強化
  - 情報科学と人文・社会科学が融合する新学術分野の創出

情報システム階層と関連学術分野



ディペンダビリティ研究開発課題の例



「D&S評価」研究

情報システムの経済価値はこれまで高機能化、高速化、高集積化！
今後はディペンダビリティ／セキュリティが新たな経済価値に！

- ディペンダブルでセキュアな情報システム実現への最初のステップ：
  当該システムがどの程度ディペンダブルあるいはセキュアかを定量的に示す評価指標と価値の可視化が必要

- 評価指標の定義、正当性・有効性の検証
- 測定法、計算法、評価法の開発、ベンチマーキング
- サービス品質、D&S価値の可視化
- 経済価値へのマッピング、ツール開発
- 社会システムへのインパクト解析、監査・認証制度

- 技術開発へのインセンティブ
  - 産業競争力の強化
  - 国際標準化を主導
  - 企業価値の向上
- ＝＞ 国際競争力の新たな源泉創出

EU-US Summit Series on Cyber Trust
Workshop on System Dependability & Security
Dublin, 15-16 Nov. 2006

http://www.securitytaskforce.org/

- 共催：EC, NSF, DHS
- 狙い：gain a shared understanding of priority critical issues and promising dependability and security research directions, and to foster collaboration between EU and US research teams
- 参加者：欧州25名、米国25名、オーストラリア１名、日本１名

DAY1

- **Panel A:** Dependability & Security of Future Networked Systems – architecture and design issues
- **Panel B:** Dependability & Security of Future Networked Systems – scalability and context-awareness
- **Panel C:** Security & Privacy in Dynamic Wireless Networks
- Australian perspective in securing future communication networks *(Ed Dawson)*
- Japanese perspective in future networked dependable systems (*Takashi Nanya*)

DAY2

- **Panel D:** Evaluating the Dependability & Security of Networked Systems – modeling, simulation, predictive evaluation, assurance cases
- **Panel E:** Evaluating the Dependability & Security of Networked Systems – monitoring, operational assessment, auditing
- **Panel F:** Future Test Beds

ワークショップ・アジェンダ

- 情報システムにおけるD&S評価技術を確立し、経済価値を可視化するにはどのような研究開発が必要か？その研究俯瞰マップを作成し、重要研究分野と課題を抽出する
- ユーザー視点のD&S評価
- 俯瞰マップの軸
  - 情報システムの階層（レベル1，2，3）
  - 応用分野（サービスの種類とユーザー環境）
- 情報システムの分類
  - 重要インフラ・システム：代替困難。社会経済活動、人命に多大な影響
  - 企業基幹システム：企業活動に多大な影響
  - 組込みシステム：大部分（＞95%）のコンピュータ、ネットワーク化
  - その他のシステム：パソコンなど

ワークショップのアウトプット

アウトプット

1. D&S評価研究の俯瞰マップ
2. 重要課題抽出
3. 研究推進方法（時間軸を含む）

進め方

- 問題提起：
- グループ別の討議

各グループの作業

- アウトプットへのアプローチ
- 俯瞰マップ作成
- 重要課題発掘
- まとめ

1日目

- 全体会議　3時間
  - 開催趣旨説明: 9:00~9:15　丹羽
  - 問題提起:　9:15~12:00
    - D&S評価の意義:南谷　9:15 ~ 9:40
    - ディペンダビリティ評価研究の現状:土肥(広島大)9:40~10:05
    - ネットワークの評価メトリック:中尾(KDDI)　10:05 ~ 10:30
    - 組込みシステムの評価メトリック:木下(産総研)　10:45 ~ 11:10
    - ソルーションサービスの評価メトリック:笠原(NEC)　11:10 ~ 11:35
    - ディペンダビリティの経済価値:藤井(東大)　11:35 ~ 12:00
- グループ討議　13:00~17:00　4時間
  - グループA:菊野、篠田、丸山宏、笠原、藤井(今井)(小菅)
  - グループB:森、木下、中尾、赤津、高橋、野島(中島)
  - グループC:佐々木、土肥、本間、丸山文宏、松本、伊関(三木)(谷口)
- 中間報告(全体)　17:00~18:00(各グループ15分)
- グループ討議　19:00~21:00　2 時間

2日目

- 全体討議　9:00~12:00　3時間
  - まとめへ向けた方針　9:00~9:10
  - グループリーダーから報告　9:10~10:10 (各グループ20分)
  - 休憩　10:10~10:30
  - 討議　10:30~11:45
  - 総括と今後の方針　11:45~12:00
- 閉会

ワークショップのアウトプット

- 「D&S評価」研究俯瞰マップ
- 重要研究課題
- 研究推進方法（時間軸を含む）

HIROSHIMA UNIVERSITY

「情報システムのディペンダビリティ評価」に関するワークショップ
JST 研究開発戦略センター，平成18年11月24日ー25日

ディペンダビリティ評価研究の現状

土肥　正
広島大学大学院工学研究科情報工学専攻

— Outline —

- ディペンダビリティ評価の概要
- 国際会議 & 研究機関調査報告
  Coimbra 大学，Critical Software 社，LAAS-CNRS，Airbus 社
  IEEE DASC 2006, EDCC 2006, ISSRE 2006
- 課題

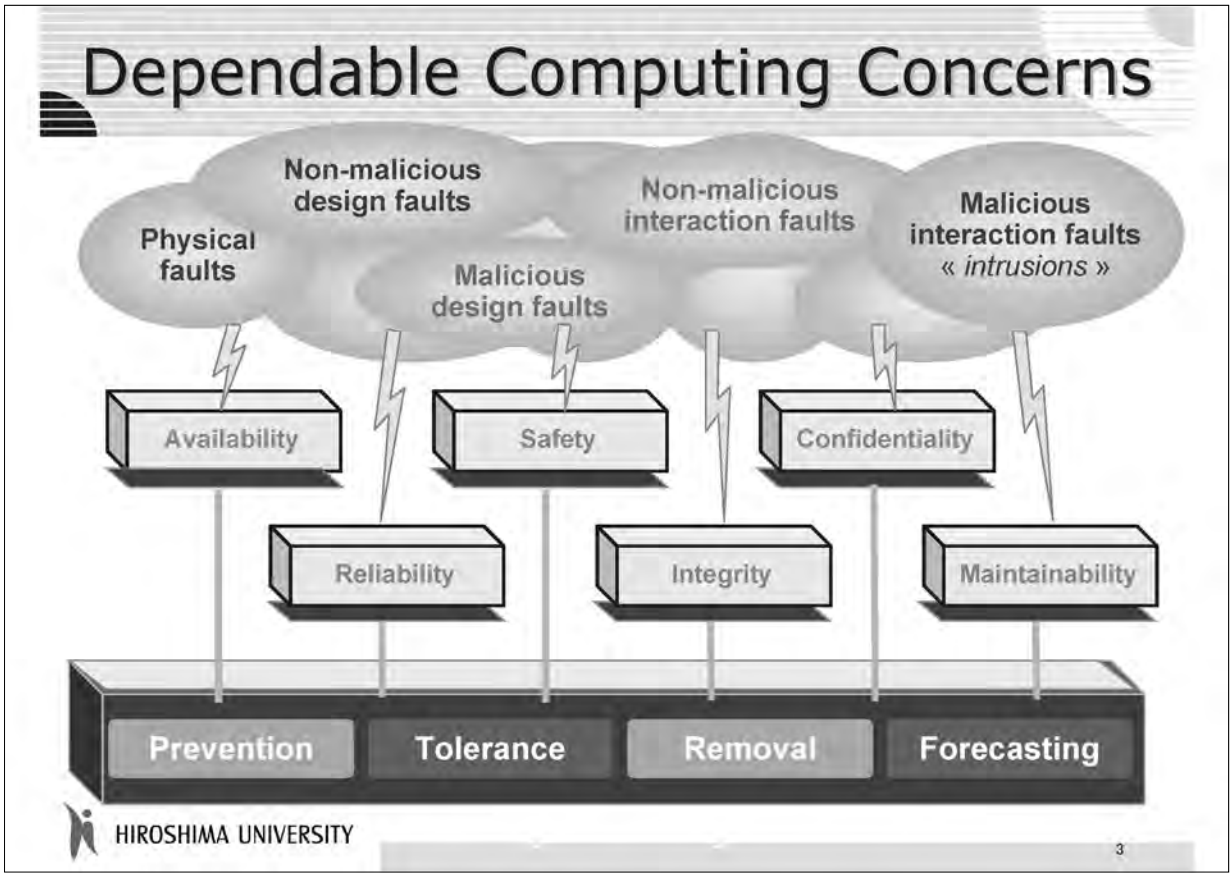
ディペンダビリティ評価の概要

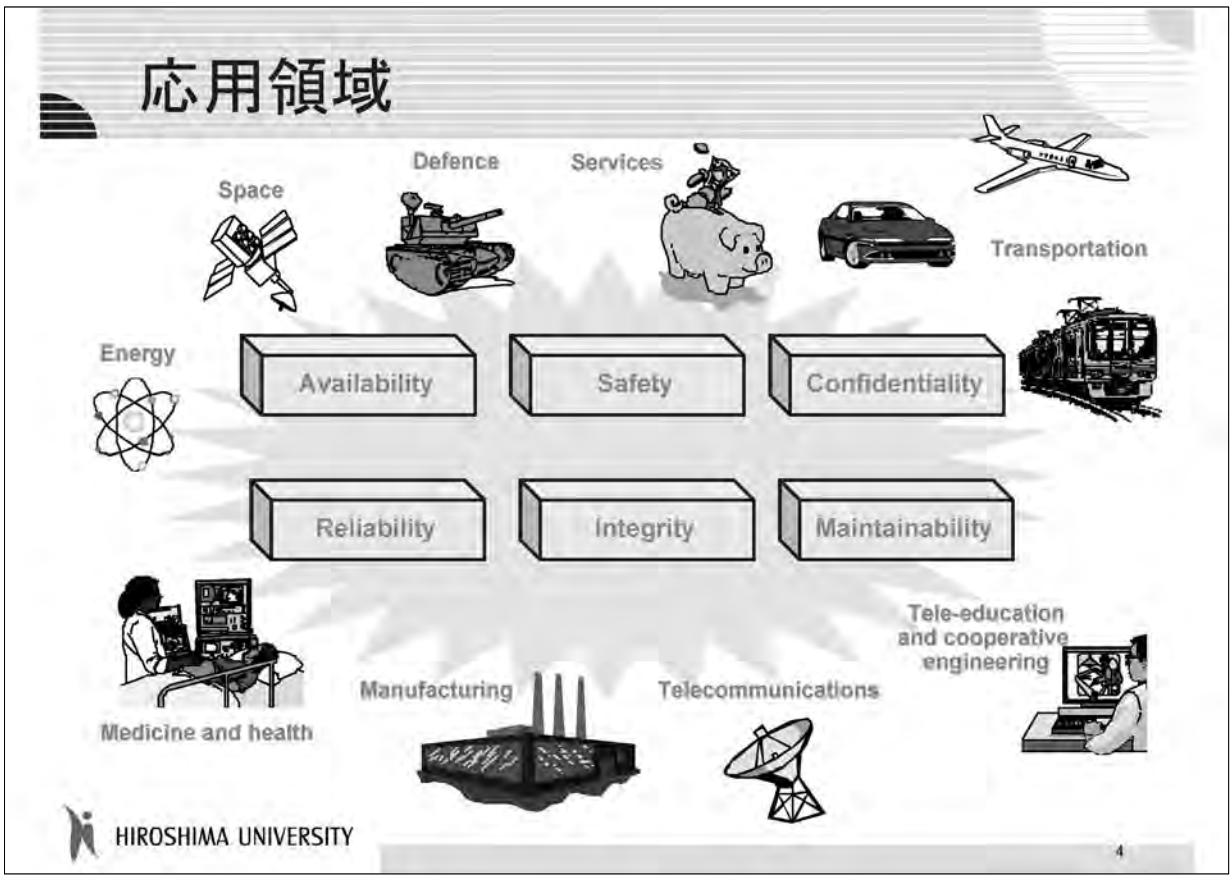
- "Dependable" →「頼りがいのある」
  「信頼性や安全性を包含した一般的な概念」
- 性能評価とディペンダビリティ評価の相違点

性能評価 (Performance Evaluation)
- 与えられたシステムワークロードに基づいて性能を計測
- 具体的な性能評価尺度：スループット，レスポンスタイムに関連した各種モーメント，ブロッキング確率，他

ディペンダビリティ評価 (Dependability Evaluation)
- 与えられたフォールトロードに基づいてディペンダビリティを計測
- フォールト，エラー，脆弱性などの存在が前提
- 具体的なディペンダビリティ評価尺度：信頼度，アベイラビリティ，MTTF，他

HIROSHIMA UNIVERSITY　2


Dependable Computing Concerns
Physical faults
Non-malicious design faults
Malicious design faults
Non-malicious interaction faults
Malicious interaction faults
« intrusions »
Availability
Safety
Confidentiality
Reliability
Integrity
Maintainability
Prevention
Tolerance
Removal
Forecasting
HIROSHIMA UNIVERSITY
3


応用領域
Space
Defence
Services
Transportation
Energy
Availability
Safety
Confidentiality
Reliability
Integrity
Maintainability
Medicine and health
Manufacturing
Telecommunications
Tele-education and cooperative engineering
HIROSHIMA UNIVERSITY
4

ディペンダビリティを如何に評価するのか？

ディペンダビリティの定量的評価に向けての基本方針

- **ターゲットシステムの同定～ブラックボックスとしての情報システム～**

  ・ ディペンダビリティ評価の重要性
  (a) 航空システム，鉄道システム，宇宙システム，軍事システム などの mission critical systems
  (b) 銀行システム，機密データベース，医療システム，災害復旧支援システムなどの社会基盤情報システム
  (c) HW, SW, MW, OS, embedded systems, database, server systems, 各種 applications などの general purpose systems

  ・ ディペンダビリティ評価の緊急性
  (i) 障害発生によるリスクと社会に与えるインパクト
  (ii) システムの開発サイクルとライフサイクルの短縮
  (iii) 成熟した高度情報化社会への対応と基盤技術の確立

Contd.

- メトリックの定義（何を定量化すべきなのか？）

  「一体誰の為の評価なのか？」
  ・ 開発者・生産者の立場に立脚したディペンダビリティ評価
  ・ 顧客・ユーザの立場に立脚したディペンダビリティ評価

- 測定法・計算法の開発

  「何が可観測で何が観測不可能か？」
  ・ 情報システム全体の処理パスを完全に制御することは困難
  ・ あらゆる詳細設計書やソースコードを入手することは困難
  ・ 複数のサブシステムから構成される全体システムの制御情報を完全に把握することは困難

  「発生する可能性のある障害やフォールトの分類」
  ・ フォールトの種類，原因の特定化，要因解析
  ・ フォールト検出・回復処理のメカニズム

Contd.

「計測を行なうためには？」 → **measurement-based approach**

- ディペンダビリティメトリック自体もしくはメトリックを構成する属性パラメータの計測
- 実システムを用いた物理的計測実験
- テスト
- プロトタイプの開発
- シミュレーション実験
- 測定技術，データマネジメント，統計的推定・検定

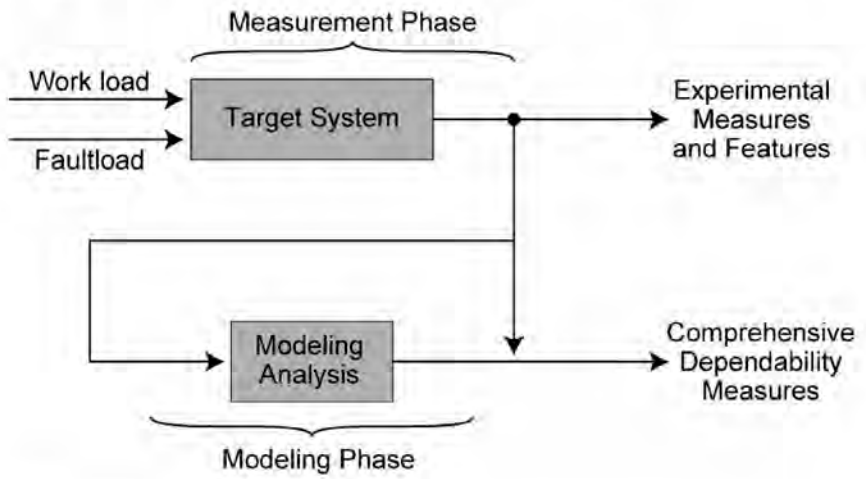
評価法の開発（如何に合理的にメトリックを評価するか？）
「評価主体と動作環境に応じたメトリック評価」

- 可観測でない情報の可視化
- 高精度ディペンダビリティ評価の要求 （*e.g.* AV = 99.999%）
- システムの運用環境やシステムの実動作環境の同定
- 「稀な事象」の記述 → **modeling-based approach**

HIROSHIMA UNIVERSITY 7

Contd.-

measurement-based approach と modeling-based approach の効果的融合



HIROSHIMA UNIVERSITY 8

Contd.

- ディペンダビリティ評価の効用

「評価目的は何か？」
- ターゲットシステムに対する有効性と限界の定量化
- ベンチマーキング（システムディペンダビリティの比較）
- フォールト情報のdisclosureへの対応
- ユーザや社会におけるディペンダビリティ情報の共有
- さらなるディペンダビリティ向上に向けての施策

「最終到達目標は何処か？」～付加価値から最高の価値へ～
- ディペンダビリティ評価のための合理的かつ普遍的な total guideline の作成
- 経済価値への mapping と企業の国際競争力への転化
- 情報産業，ユーザ・市場，研究開発，教育分野全体でのディペンダビリティ価値の共有（*e.g.* QC 効果）
- 新しいビジネスモデルの創造

国際会議 & 研究機関調査報告（1）

Coimbra 大学訪問: 10月16日・17日（於, Coimbra）
Critical Software 社訪問: 10月17日（於, Coimbra）
6th European Dependable Computing Conference (EDCC 2006) への参加：10月18日-20日（於, Coimbra）
LAAS 訪問: 10月23日・24日（於, Toulouse）

実システムに対する measurement-based approaches

- ヨーロッパにおける Dependability Benchmark (DBench) プロジェクト
- Simulating Fault Injection によるディペンダビリティ計測の実例
- Fault Injection Tool の開発
  Critical Software 社 「Exception」
- ターゲットシステム: Windows などのOS，宇宙システムにおける実時間システムカーネル，自動車のエンジン制御アプリケーション，OLTPシステム，サーバアプリケーション，他

DBench

DBench (Dependable Benchmark)

- 1998年～2002年に実施されたEU における ディペンダビリティ評価プロジェクト (Information Society Technology による財政支援)
- 参加研究機関:
  LAAS-CNRS (コーディネータ)
  Critical Software 社
  University of Coimbura
  Friedrich Alexander University, Erlangen-Nurnberg
  Polytechnic University of Valencia

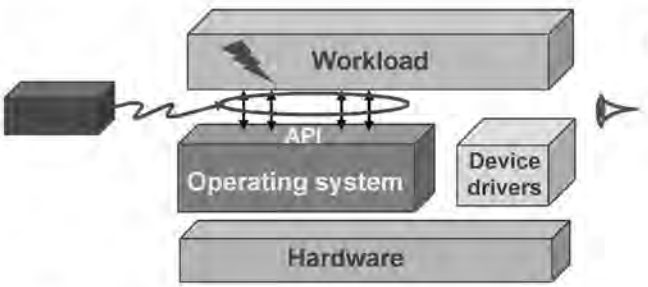
DBench の目的

- 情報システムのディペンダビリティを計測することで，実システムの定量的な比較を行なうためのベンチマークを開発

HIROSHIMA UNIVERSITY

11

Contd.



OS Outcomes

SEr	Error code
SXp	Exception
SPc	Panic
SHg	Hang
SNS	No signaling

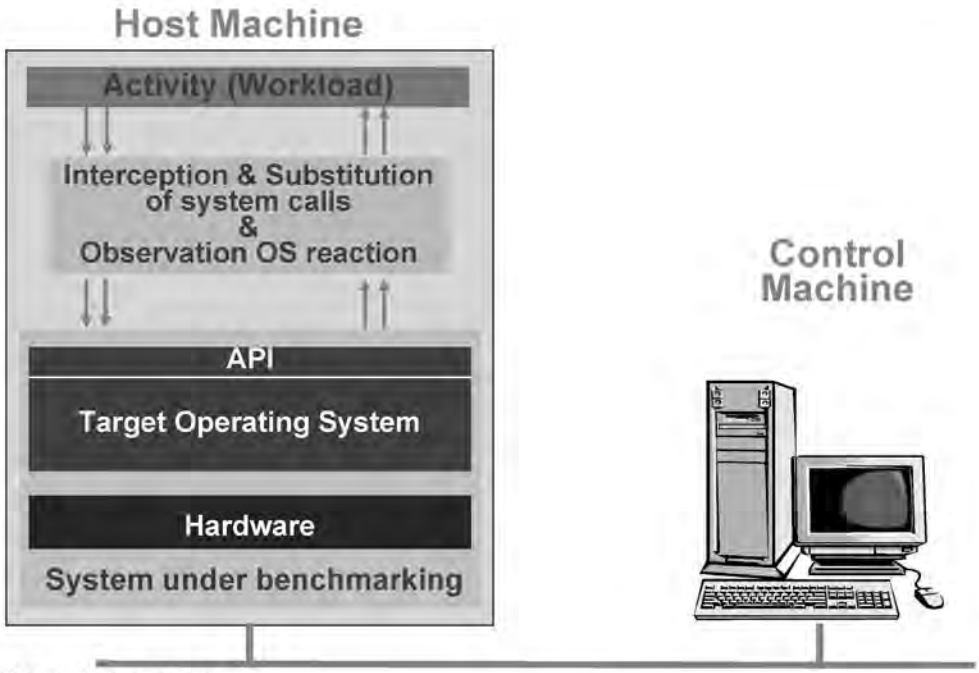
Measures

- POS: OS Robustness [%SEr %SXP %SPc %SHg %SNS]
- Texec: OS Reaction time in the presence of faults
- Tres: OS Restart time after fault insertion

HIROSHIMA UNIVERSITY

12

Contd.



Contd.

Software Fault Injection (SFI)

- Jeffrey Voas and Gary McGraw, *Software Fault Injection: Innoculating Programs Against Errors*, Wiley, 1997.
- ソフトウェアを用いて故意に障害を発生させ，異常時のシステムの挙動やバグの数を推定するための方法
- Physical Fault Injection v.s. Simulating Fault Injection
- ソースコードレベルでのSFI v.s. 低レベルSFI(ライブラリの改変，システムコールの改変，カーネルの改変)

DBench の応用例

- Operations Systems
- 宇宙システムにおける実時間カーネル
- 自動車のエンジン制御アプリケーション
- OLTPシステム(データベース)
- サーバアプリケーション

国際会議 & 研究機関調査報告(2)

Critical Software 社訪問: 10月17日 (於, Coimbra)
LAAS 訪問: 10月23日(於, Toulouse)
Aitbus 社調査: 10月24日(於, Toulouse)
IEEE 2nd International Symposium on Dependable, Autonomic and Secure Computing (DASC 2006) への参加:10月29日-11月1日(於, Indianapolis)
IEEE 17th International Symposium on Software Reliability Engineering (ISSRE 2006) への参加:11月7日-11月10日(於, Raleigh)

- Mission critical systems (航空・宇宙システム)の評価

  - Fault Injection によるディペンダビリティ計測の実例
    Critical Software 社 「Exception」の応用領域
  - LAAS-CNRS におけるプロジェクト例
  - Airbus 社による航空制御システムのディペンダビリティ評価
  - IBM, NASA による autonomic computing プロジェクト
  - NASA 研究プロジェクト

HIROSHIMA UNIVERSITY 15

CSW による事業展開

Critical
Dependability & Embedded Systems

- 1999
  - Xception – project with NASA JPL
  - Competencies based on low level programming
- 2001
  - Portugal becomes ESA member
  - Space market becomes more relevant
- 2002
  - Creation of Lisbon spin-off (Command & Control)
- 2003
  - RAMS and ISVV in Aeronautics & Space
- 2005
  - Galileo on-board software project
  - RTEMS Qualification (Open-source RTOS)
  - Xception for JAXA
  - R&D project with NASA – IV&V
- 2006
  - Qualification, Certification and Gap Analysis
  - Project Management Office

HIROSHIMA UNIVERSITY 16

Contd

CRITICAL SOFTWARE

Critical

Critical Softwareは、ミッションおよび事業に決定的な情報システム向けのソフトウェア開発会社として世界のリーダー企業で、航空業界におけるもっとも難しいプロジェクトの一つ、NASAジェット噴射研究所に積極的に携わっています。

Critical Softwareは、要求が厳しく特殊な顧客の要件に合わせたソフトウェアソリューションの立案、設計、開発を行います。この企業はIEEE 12207、ESA PSS05、およびNASA SELスタンダードなど、開発プロジェクトにおいてもっとも厳格なソフトウェアエンジニアリング基準と方法を用いて品質レベルを保証しています。

D&E Services

- Consulting
  - Dependability, RAMS, Safety & Security*
  - Business continuity*
  - Security Solutions – Audits
  - Verification & Validation services
- Independent Software Verification and Validation (ISVV)
  - Software Level
  - System Level
  - Applications/Systems Qualification
- Software
  - Experience in aeroespace, aeronautics, defense, bank and automotive
  - Simulation Models development
  - V&V (Verification & Validation), tests
  - FDIR (Fault-Detection, Isolation and Recovery)
  - Software Product Assurance/Quality Assurance (PA/QA)
  - Xception Fault Injection Tool

6

HIROSHIMA UNIVERSITY

17

LAAS における研究動向

DEPENDABLE COMPUTING AND FAULT TOLERANCE

Senior Researchers (18)

- **Jean Arlat** (DR2 CNRS) (group leader)
- **Agnan de Bonneval** (MC UPS)
- **Jacques Collet** (DR2 CNRS)
- **Alain Costes** (Prof INPT - ENSEEIHT)
- **Yves Crouzet** (CR1 CNRS, HdR)
- **Yves Deswarte** (DR2 CNRS)
- **Jean-Charles Fabre** (Prof INPT - ENSEEIHT)
- **Jérémie Guiochet** (MC IUT)
- **Mohamed Kaâniche** (CR1 CNRS, HdR)
- **Karama Kanoun** (DR2 CNRS)
- **Marc-Olivier Killijian** (CR2 CNRS)
- **Jean-Claude Laprie** (DRCE1 CNRS)
- **Vincent Nicomette** (MC INSA)
- **David Powell** (DR1 CNRS)
- **Nicolas Rivière** (MC UPS)
- **Matthieu Roy** (CR2 CNRS)
- **Pascale Thévenod** (DR2 CNRS)
- **Hélène Waeselynck** (CR1 CNRS)

Research Engineer

- **Christophe Zanon**

PhD Students (15)

- **Carlos Aguilar Melchor**
- **Éric Alata**
- **Amine Baina**
- **Étienne Baudin**
- **Ludovic Courtès**
- **Éric Lacombe**
- **Caroline Lu**
- **Benjamin Lussier**
- **Minh Nguyen**
- **Thomas Pareaud**
- **Thomas Robert**
- **Ana Elena Rugina**
- **Nicolas Salatge**
- **Géraldine Vache**
- **Piotr Zając**

CNAM Doctorate

- **Frédéric Sorbet**

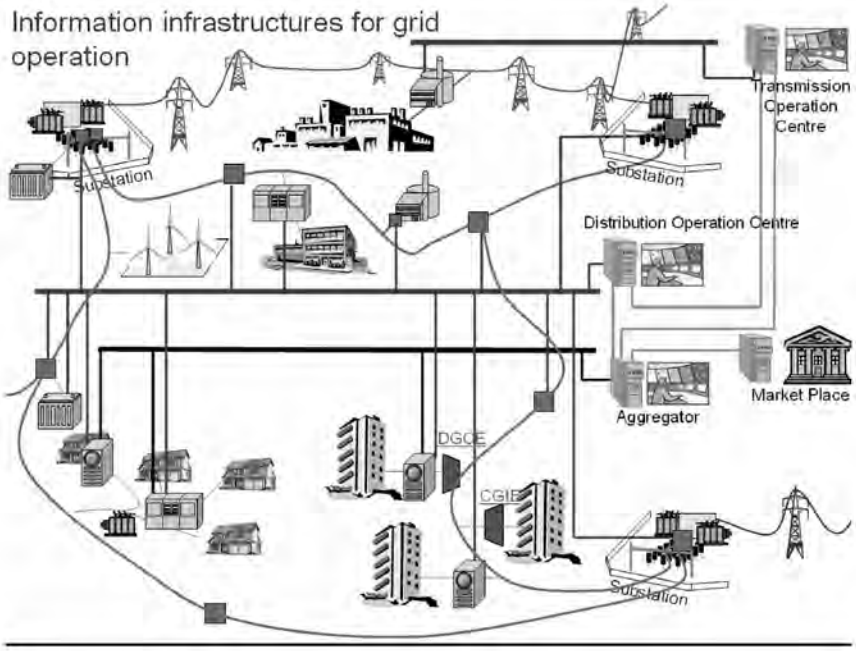
Visiting Researchers

- **Jean-Jacques Quisquater** (UCL -BE)
- **Philippe Bulens** (UCL - BE)
- **Zoltan Micskei** (BUTE - HU)

HIROSHIMA UNIVERSITY

18

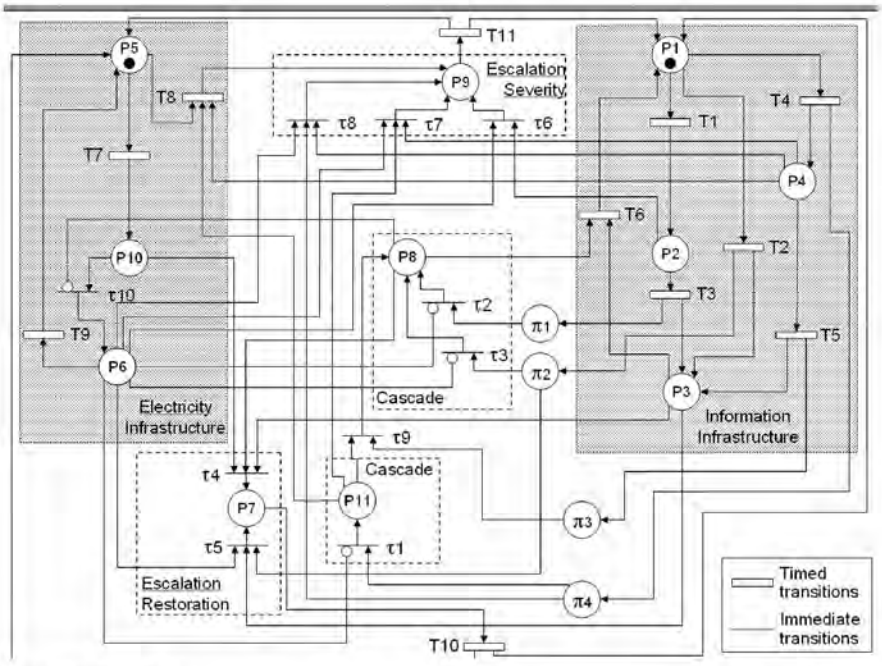
Modeling Interdependencies between the Electricity and Information Infrastructures



HIROSHIMA UNIVERSITY

19

Contd.



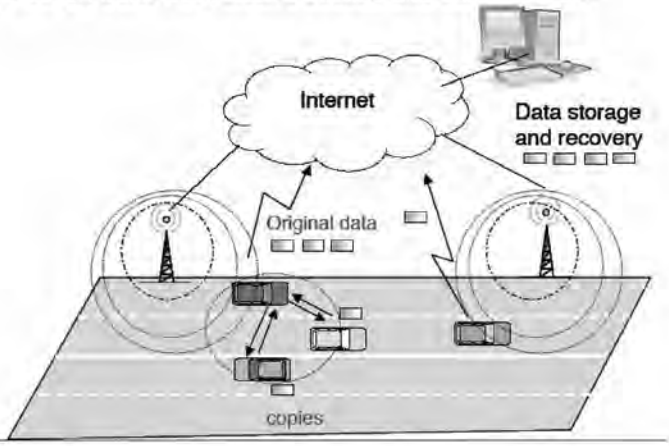
HIROSHIMA UNIVERSITY

20

HIDENTS プロジェクト

Highly Dependable IP-based NET works and Services

- Platooning
- Infotainment and work with highly mobile terminals
- Assisted transportation
- Distributed-black box: Cooperative backup and data recovery



HIROSHIMA UNIVERSITY

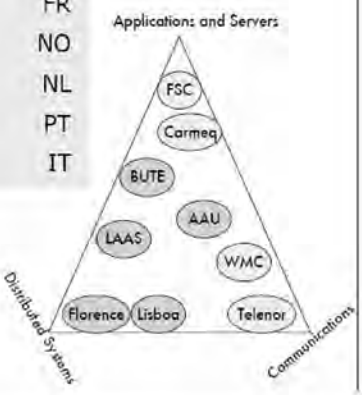
21

Contd.

Consortium: 9 partners from 8 countries

Aalborg University (coordinator)	DK
Budapest Univ. Tech. and Economics	HU
Carmeq GmbH	GER
Fujitsu Siemens Computers	GER
LAAS-CNRS	FR
Telenor	NO
Wireless and Mobile Comm.	NL
Univ. of Lisboa	PT
Univ. of Florence	IT

- Industry: Carmeq, FSC, Telenor, WMC
- Additional involvement of other companies via advisory council



5

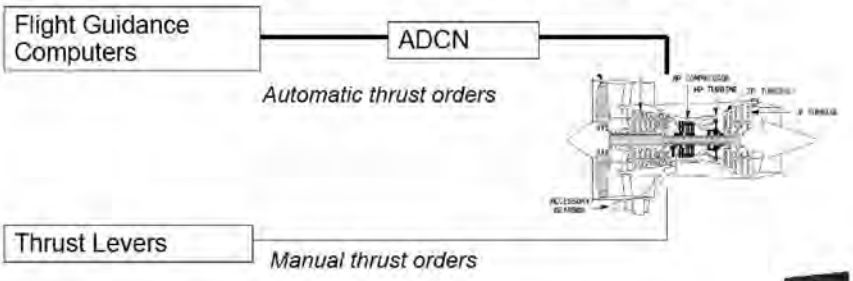
HIROSHIMA UNIVERSITY

22

Airbus における DC 研究

ADCN LOSS – EXAMPLE

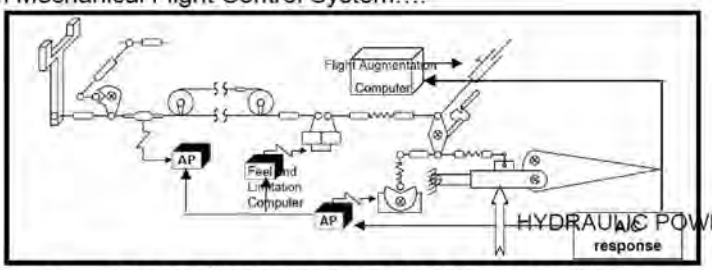
- Total Loss of Engine Control is classified as potentially Catastrophic
- Consequently, engine information necessary to control engine thrust shall not be transmitted only through ADCN
  - Automatic Thrust orders are transmitted through ADCN
  - Manual Thrust orders are transmitted via analog signals



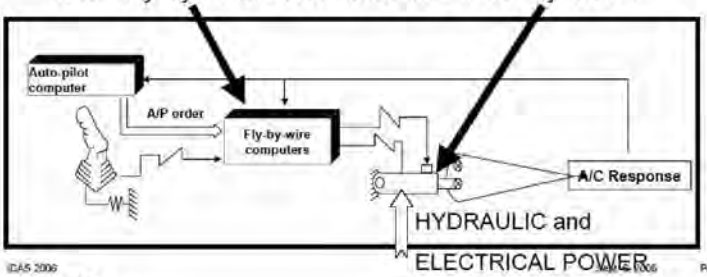
フライ・バイ・ワイヤ(Fly-by-Wire)におけるディペンダビリティ設計

What is Fly-by- Wire?

From Mechanical Flight Control System….

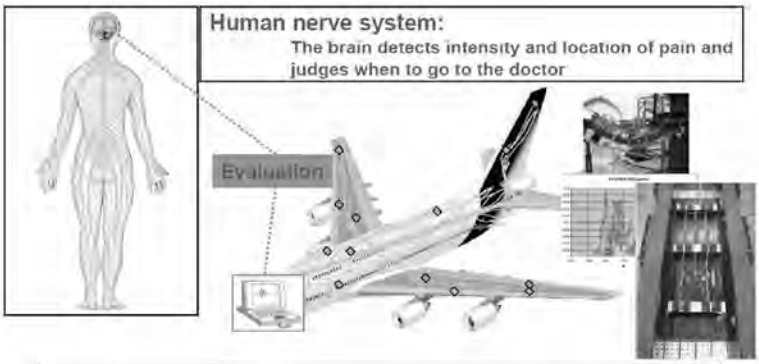


to … "Fly-by-Wire" associated to "Power-by-Wire".



JASTAC プロジェクト(2006年7月～)

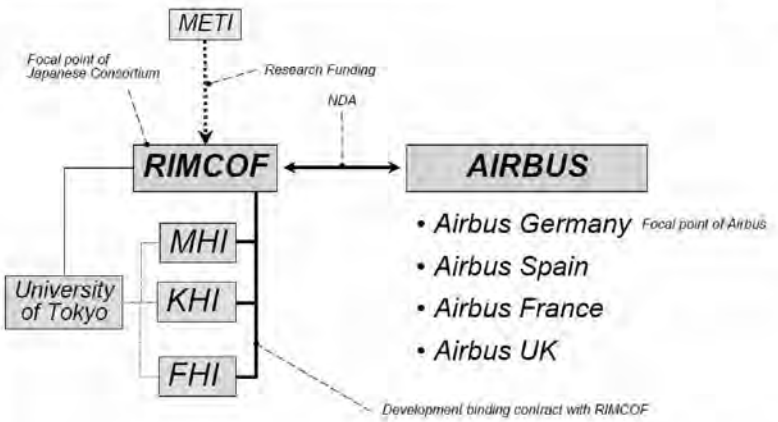
SHM system concept



SHM system:
The SHM system checks the structure (diagnosis) and evaluates the follow up actions for maintenance (prognosis)

Contd.-

JASTAC – project structure



Autonomic Computing & Dependability

DASC 2006 (Sep. 29-Oct. 1, IUPU) アジェンダ

- Autonomic Computing and Selfware
- Cryptography
- Autonomic Computing and Monitoring
- Reliability and Security Modeling
- Autonomy Supported by Grid and Pervasive Computing
- Network Security
- Self-Adaptation and Scheduling
- Autonomous Intrusion Detection
- Autonomy in Sensor Networks
- Automated Trust Management
- Access Control
- Autonomic Computing and Context Awareness

HIROSHIMA UNIVERSITY 27

European Dependable Computing

EDCC 2006 (Oct. 18-20, Coimbra U.) アジェンダ

- Robustness and Fault Tolerance
- Practical Experience Reports and Tools
- Fast Abstract
- Fault Injection
- In Search of Real Data on Faults, Errors and Failures
- Hardware Implementation Fault Tolerance
- Education in Dependable and Resilient Computing – Meeting the Needs of the Information Society
- Dependable Storage and Services

HIROSHIMA UNIVERSITY 28

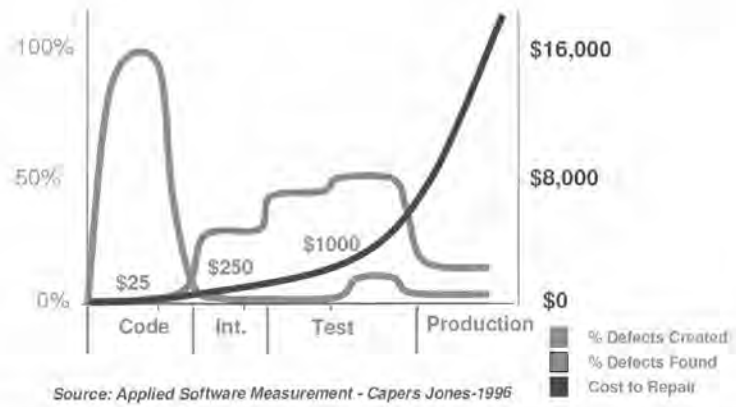
Software Reliability Engineering

ISSRE 2006 (Nov. 7-10, NC State U.) アジェンダ

- Testing I & II & III & IV
- Modeling I & II
- Metrics
- Security
- Static and Dynamic Analysis
- Tools
- Industry Practice – Software Metrics
- Industry Practice – Empirical Studies
- Industry Practice – Software Development I & II
- Industry Practice – Predictions/Risk Assessment
- Industry Practice – Testing
- Government – Budget/Schedule/Mandates
- Government – Security of Systems
- Government – Large Scale Systems
- Panel Discussion I & II
- Experience Reports I & II
- Fast Abstract I & II
- Student Papers

IBM Test Helper System

Finding Bugs Late is Expensive and Time-Consuming

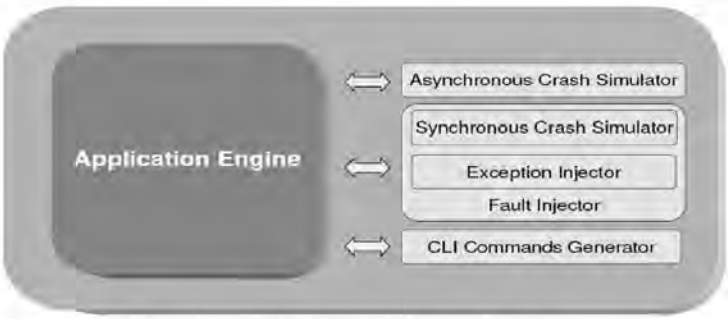


Source: Applied Software Measurement - Capers Jones-1996

Contd.-

IBM Software Group | Tivoli Software

The Test Helper System: General Architecture



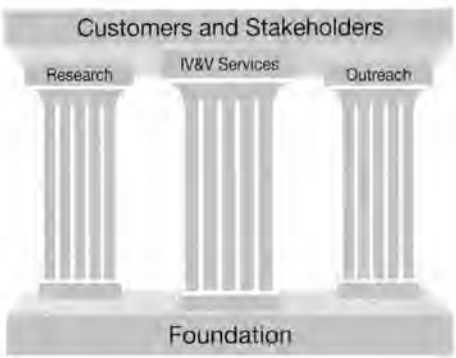
The internal structure of the application process

HIROSHIMA UNIVERSITY

31

NASA IV&V

- NASA Independent Verification and Validation Facility
  - 2005 年 大学等との共同(委託)研究プロジェクト件数 40 件
  - 2005 年 NASA の主要ミッションに対するプロジェクト件数16件
- 共同研究プロジェクトのほとんどが情報システムのディペンダビリティ関連研究



HIROSHIMA UNIVERSITY

32

Contd.-

- IV&V 研究プロジェクトの一例

Verification and validation of adaptive systems (2001-2005):
PI: Bojan Cukic (West Virginia University)
Government POC: Lisa Montogomery (IV&V)

Toward more reliable software reliability prediction (2001-2006):
PI: Katerina Goseva-Popstojanova (West Virginia University)
Government POC: Lisa Montogomery (IV&V)

Integrated software into probabilistic risk assessment (2000-2006):
PI: Carol Smidts (University of Maryland)
Government POC: Judith Connely (IV&V)

Reducing software security risk through an integrated approach (2000-2005):
PI: David Gilliam (JPL)
Government POC: Allen Nikora (JPL)

課題～プロポーザルに向けて～

- 官民学によるシステマチックな連携の必要性
- 実用的なディペンダビリティ評価技術開発の必要性
  - measurement-based approach と modeling-based approach の効果的な融合は多くはない！
  - DBench による測定結果ですら有効なメトリックの算出には至っていない！
- 高信頼化システムのディペンダビリティ評価プロジェクトの継続性
  - 情報通信技術の開発サイクルとの同期調整
  - 普遍性のある基盤技術体系の構築は可能か？
- ディペンダビリティ評価技術の適用領域の模索
  - セキュリティ分野など未解決領域が山積
- 価値創造へ向けてのシナリオ
  - ディペンダビリティ評価目的や最終到達目標まで至っている研究プロジェクトは存在しない（経済価値へのmappingという概念自体が普及していない）


Contd.-
魅力的なターゲットシステムの選定
緊急領域，未踏領域は何か？
我国が誇る情報通信固有技術への適用
新しいディペンダビリティ評価技術の開発
計測・モデリング・評価・価値創造のサイクル達成
日本版DBenchの開発
ディペンダビリティ評価のための汎用ツールの開発
価値創造
付加価値の評価と企業の国際競争力への転化
情報産業，ユーザ・市場，研究開発，教育分野全体での価値の共有
ビジネスモデル
Thank you
HIROSHIMA UNIVERSITY
35

セキュリティに関わる評価メトリック

KDDI(株式会社)
技術開発本部　セキュリティ技術部
中尾康二

ネットワークへの依存の高まりと セキュリティ被害の深刻化

インターネットへの脅威の増加

Slammer、Blaster等ウイルス、ワームの蔓延が引き起こすセキュリティ被害の深刻化

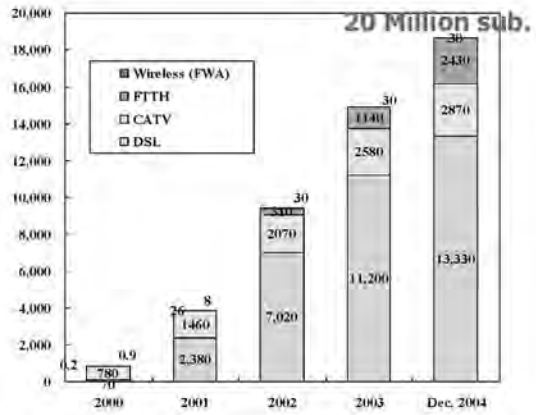


Figure 2: Transition in the number of broadband subscribers

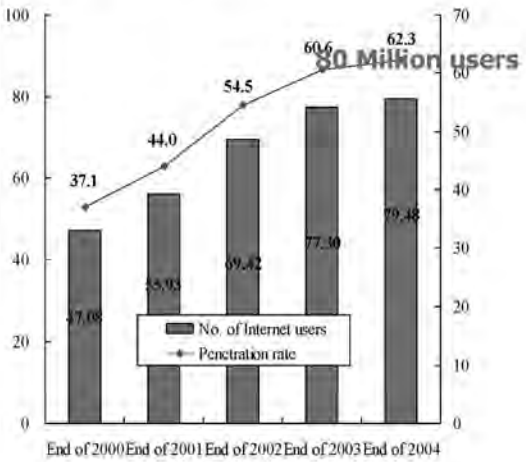
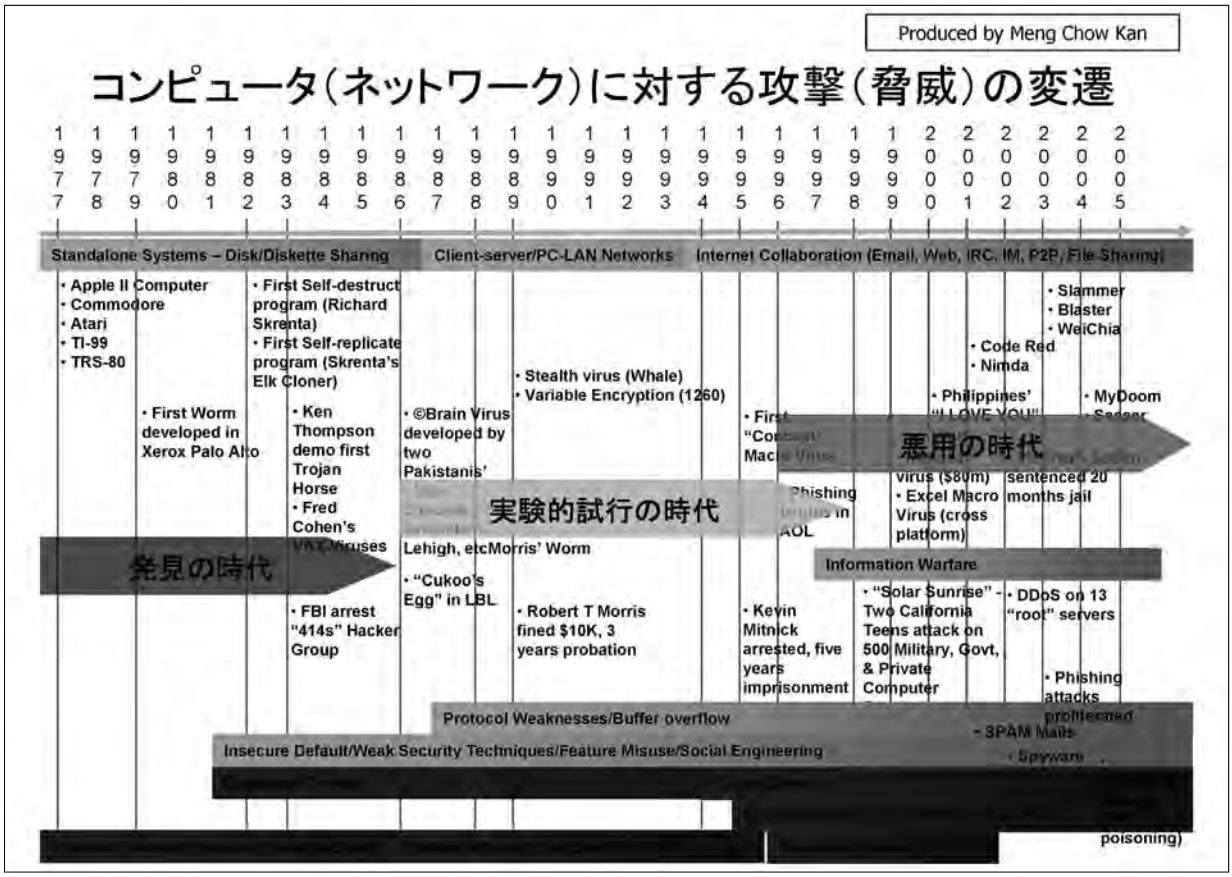
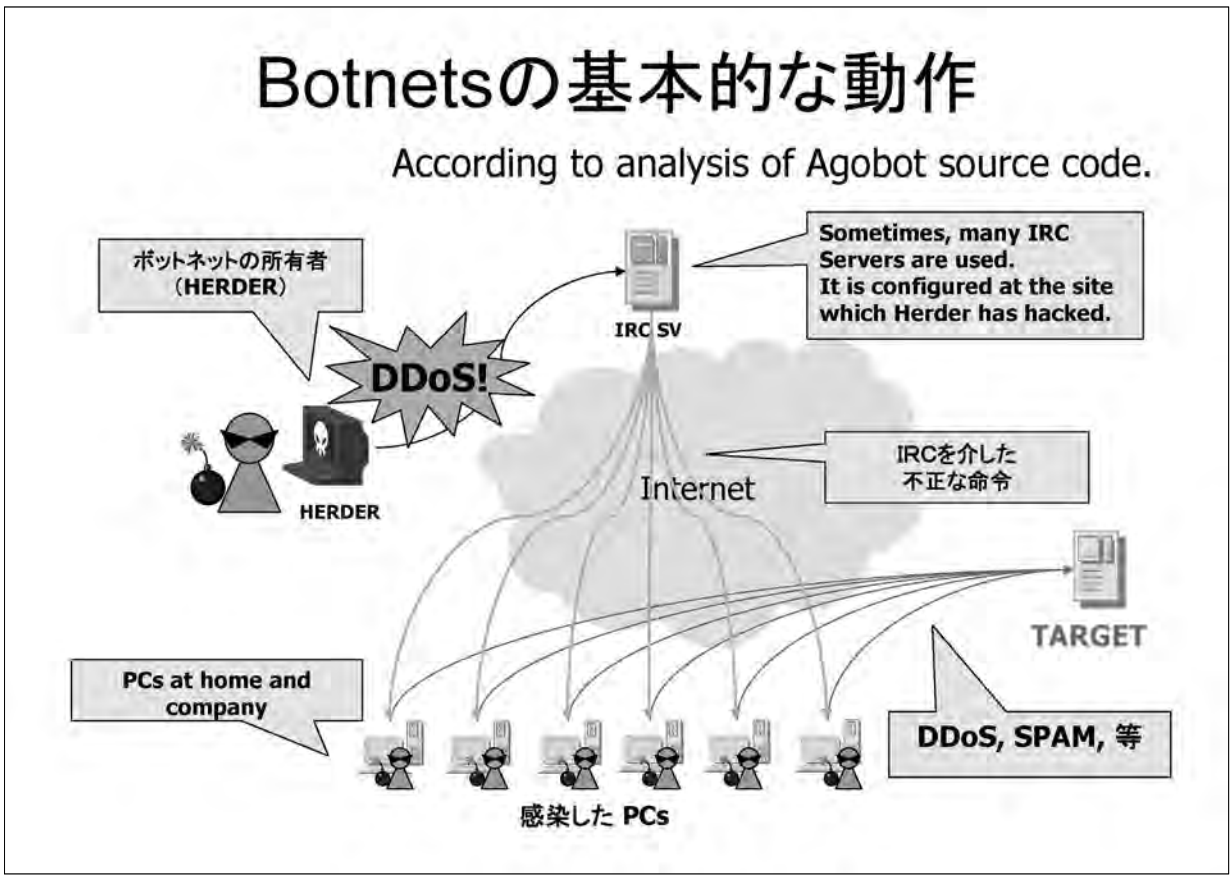


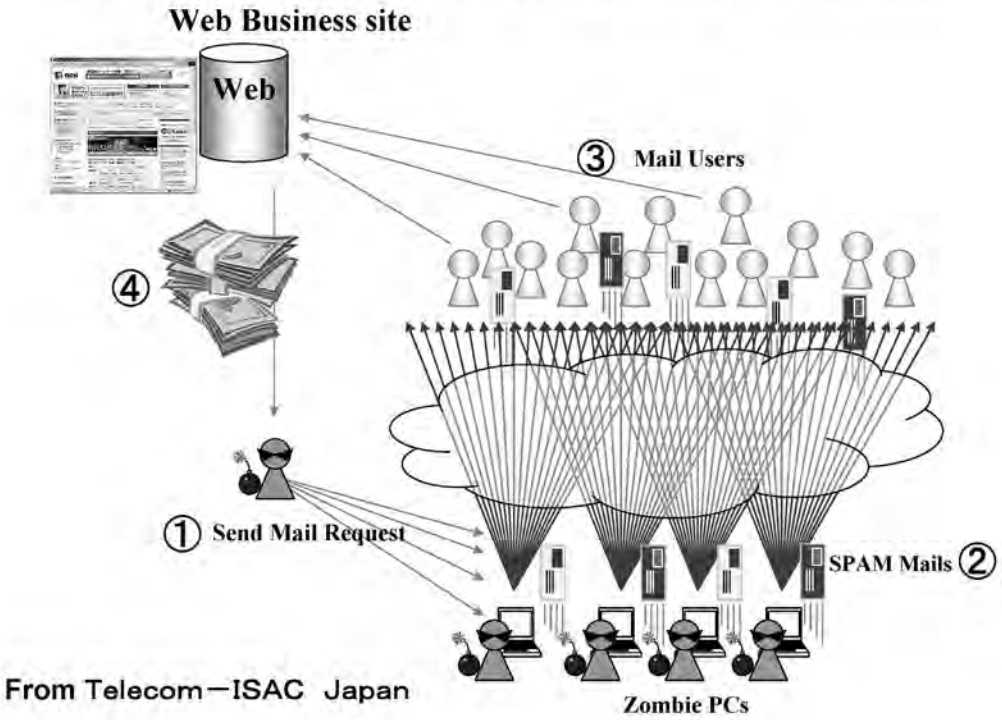
Figure 1: Number of Internet users and penetration rate

NiCT


Produced by Meng Chow Kan
コンピュータ(ネットワーク)に対する攻撃(脅威)の変遷
1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005
Standalone Systems – Disk/Diskette Sharing
Client-server/PC-LAN Networks
Internet Collaboration (Email, Web, IRC, IM, P2P, File Sharing)
• Apple II Computer
• Commodore
• Atari
• TI-99
• TRS-80
• First Worm developed in Xerox Palo Alto
• First Self-destruct program (Richard Skrenta)
• First Self-replicate program (Skrenta's Elk Cloner)
• Ken Thompson demo first Trojan Horse
• Fred Cohen's Virus
• ©Brain Virus developed by two Pakistanis'
• Stealth virus (Whale)
• Variable Encryption (1260)
• Code Red
• Nimda
• Slammer
• Blaster
• WeiChia
• Philippines' "I LOVE YOU"
• MyDoom
• Sadear
• First "Concept" Macro Virus
悪用の時代
実験的試行の時代
発見の時代
Phishing
AOL
virus ($80m)
• Excel Macro Virus (cross platform)
sentenced 20 months jail
Lehigh, etcMorris' Worm
• "Cukoo's Egg" in LBL
Information Warfare
• FBI arrest "414s" Hacker Group
• Robert T Morris fined $10K, 3 years probation
• Kevin Mitnick arrested, five years imprisonment
• "Solar Sunrise" - Two California Teens attack on 500 Military, Govt, & Private Computer
• DDoS on 13 "root" servers
• Phishing attacks proliferated
Protocol Weaknesses/Buffer overflow
- SPAM Mails
Insecure Default/Weak Security Techniques/Feature Misuse/Social Engineering
• Spyware
poisoning)

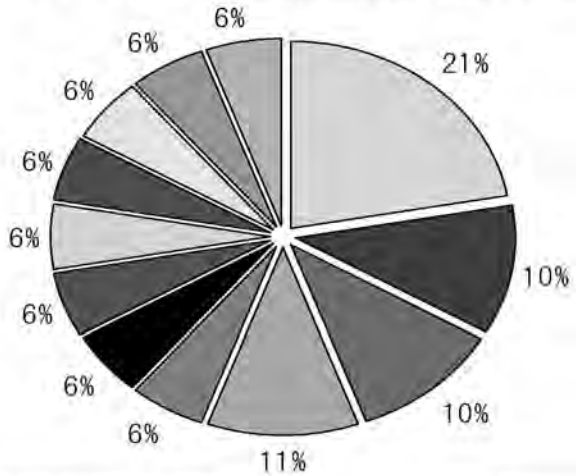

Botnetsの基本的な動作
According to analysis of Agobot source code.
ボットネットの所有者
(HERDER)
DDoS!
HERDER
IRC SV
Sometimes, many IRC Servers are used.
It is configured at the site which Herder has hacked.
IRCを介した
不正な命令
Internet
TARGET
PCs at home and company
DDoS, SPAM, 等
感染した PCs

（例）ボットを使ったSPAM mail business



From Telecom－ISAC Japan

Webアプリ高危険度脆弱性内訳



- SQLインジェクション
- パラメータマニプレーション
- HTTPレスポンス分割
- OSコマンドインジェクション
- 専用パスワード認証の回避
- 任意のファイルダウンロードが可能
- クロスサイトスクリプティング
- 閲覧、変更可能な他ユーザ情報
- Oracleアプリケーション・サーバDAD管理画面
- セッション情報の閲覧が可能
- 特定画面でのアクセス権限のチェックの欠如
- 非表示項目の露呈

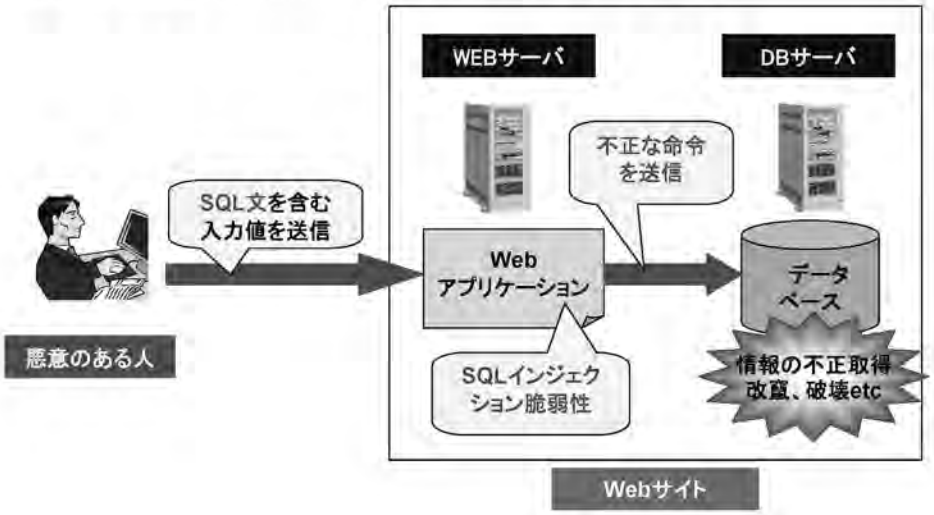
2005年10大ぜい弱性被害

第1位	SQLインジェクション
第2位	Winnyによる情報漏えい
第3位	ルートキット
第4位	フィッシング詐欺
第5位	スパイウェア
第6位	ボット
第7位	CSRF
第8位	情報家電ソフトウェア脆弱性
第9位	セキュリティ製品の持つ脆弱性
第10位	ゼロデイ攻撃

（IPAセキュリティ白書より抜粋）

SQLインジェクション

- 入力値チェックが不十分な入力フォームにSQL文を与えてSQLデータベースを不正に操作する攻撃
- Direct SQL Command Injectionとも呼ばれる



フィッシング

フィッシング(Phishing)とは

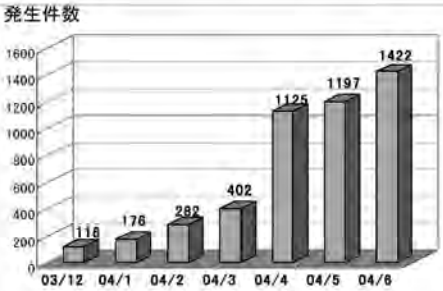
フィッシングとは、本物の金融機関などのHPをそっくりまねて作成された偽サイトを用意し、本物サイトに見せかけて信用させ、個人の口座番号やクレジットカード情報などを盗み取る手法である。
多くのフィッシングサイトは電子メール等で偽のお知らせを送り、同メールに記されているURLをクリックさせて偽サイトに誘導している。

◆これまでは、本物そっくりのHPを作成しても、URL(http://で始まるサイト名)は異なるため、このWebブラウザのURL表示部分(アドレスバー)を隠して表示させていたが、Internet Explorerのアドレスバーに偽URL情報を表示することが出来る不具合が発見されたため、今後はこれを利用してURLも本当のサイト名に偽った情報を表示させて信用させ、個人情報を入力させるような手法が広まることが懸念されている。

被害状況

米国：・発生件数　：176件(2004年1月)→1422件(6月)
　　・被害総額　：24億ドル(2004年4月まで)
　　・被害者数　：198万件(2003年中)
日本：まだ大々的な被害は報告されていないが、
　①他通信事業者や一部クレジット会社が会員向に注意案内を出している。
　(日本語のフィッシングサイトが構築されている模様)
　②ある通信会社Iユーザの HPが改竄され、フィッシングサイトとして利用された
　(2004・10～05・07　45件)

発生件数



米国でのフィッシング件数は急増、被害は莫大！

・Fish(動詞)：(それとなく)[…を]手に入れようとする
・sophisticated されたメールを悪用する

8

ワンクリック詐欺

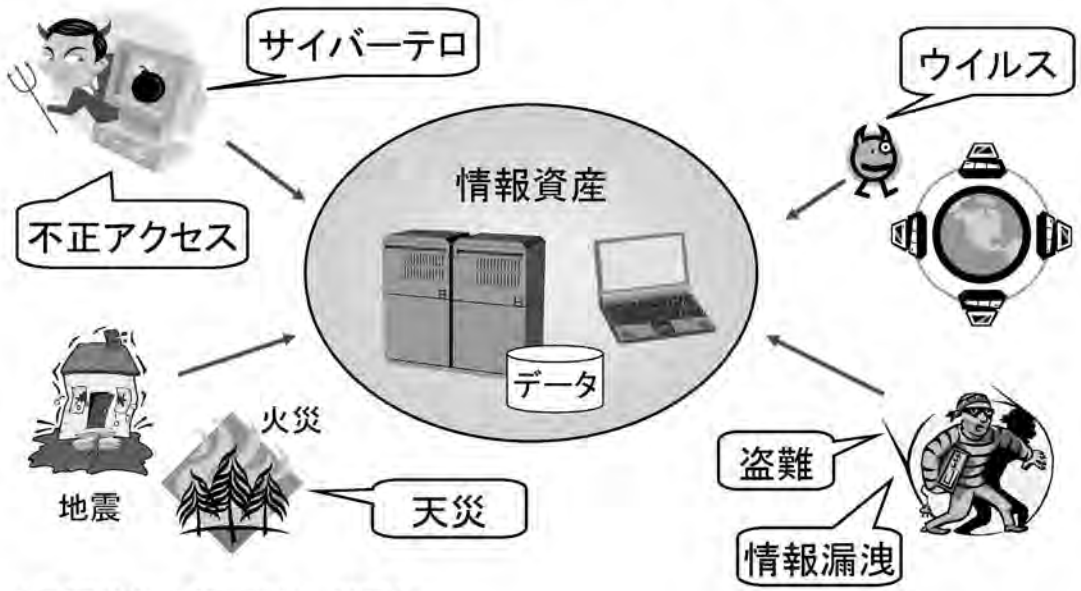
- ワンクリック詐欺とは、Webページ中の画像やリンクをクリックしただけで料金を請求される架空請求・不正請求詐欺の一種
- 「ワンクリック料金請求」や「ワンクリック不正請求」、「ワンクリック架空請求」と呼ばれることもある
- 最近では、画像をクリックすると料金を明示した確認画面を表示する手口が増えている。料金請求画面の表示までに利用者がクリックを2回することから、ツークリック詐欺と呼ばれることがある。

本詐欺が増加してきている

S
SecureBrain

KDDI

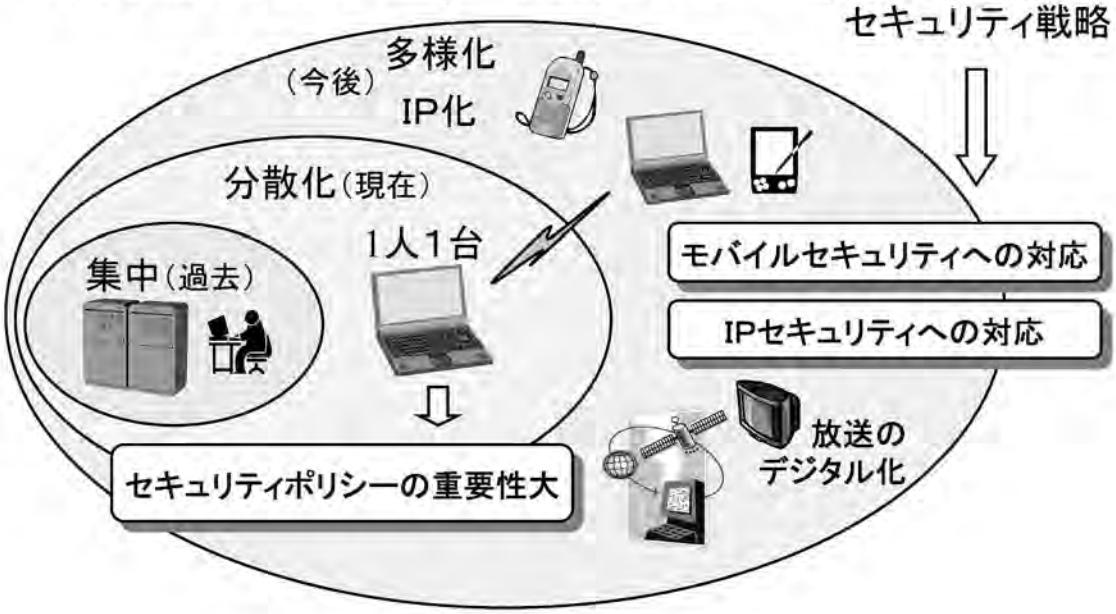
情報セキュリティにおける脅威とは



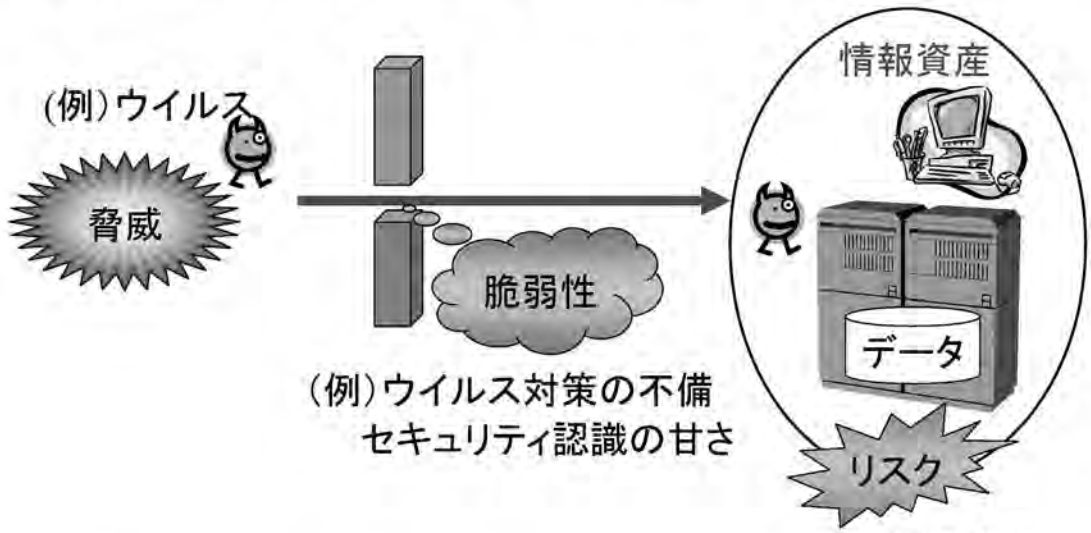
＜意図的な攻撃、事故、災害＞
・情報資産の機密性・完全性・可用性を失わせ、組織に影響を与えるもの。

情報セキュリティにおける脅威の変化

情報資産の多様化 ⇒ 脅威の多様化 ⇒ 新たな情報セキュリティ戦略



脅威、脆弱性、および資産に対するリスク



(例)ウイルス対策の不備
セキュリティ認識の甘さ

サービス停止
データ破壊

・情報資産の重要度×脅威×脆弱性
・情報セキュリティ対策の必要性

では、情報セキュリティの確保とは

「情報資産の機密性・完全性・可用性の（セキュリティ）維持」

・機密性：許可された者だけが情報にアクセスできること
・完全性：情報、処理方法が正確であり、完全であることを保護すること
・可用性：許可された者が必要なときに、情報及び関連する資産にアクセスできることを確実にすること

情報セキュリティマネジメントの必要性（相関図）

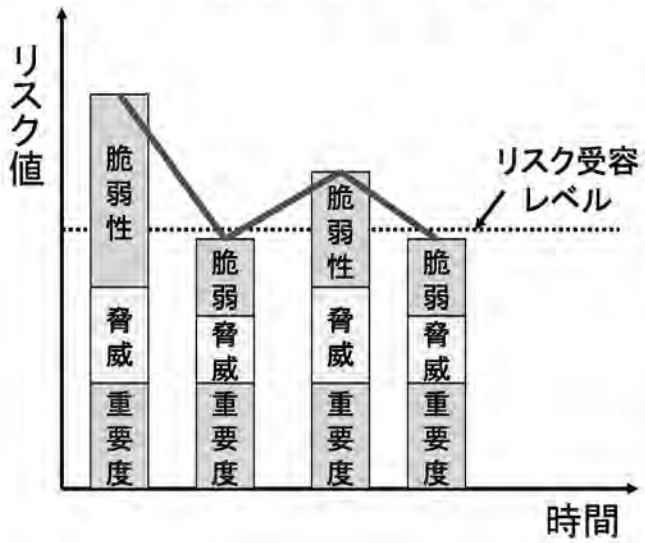
1. 脆弱性、脅威、資産価値の評価
2. リスク分析・評価
3. リスク低減・回避のための対策選択
4. インシデント対応
・・・
5. 対策技術
・IDS、Firewall
・ウィルス駆除
・インシデント分析
・暗号・認証技術
等

P-D-C-Aに則った情報セキュリティマネジメント（ISMS）の確保

ISMS基準 監査基準
脆弱性共有 ISP連携
OECD 各種法規制
最新技術 研究開発
・・・

情報資産のリスク分析、評価及び対応

情報セキュリティマネジメントを確保するため、情報資産のリスク分析、評価及び対応を、継続的に実施することが重要。



単純算定例（直和型）

「情報資産のリスク値」＝
「重要度のレベル」＋
「脅威のレベル」＋
「脆弱性の度合い」

「リスク受容レベル」＝
「リスクの保有が許容できるレベル」

情報セキュリティ対策とは（具体例）

情報セキュリティ対策の実施

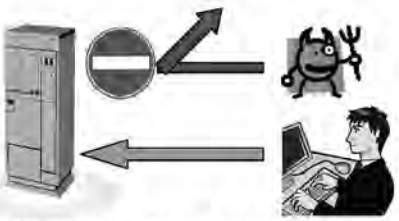
①物理的対策

不正侵入等から保護

②人的対策

情報セキュリティの重要性の周知徹底

③技術的対策



情報資産へのアクセス制御

④運用等における対策

情報セキュリティ対策の遵守状況の確認

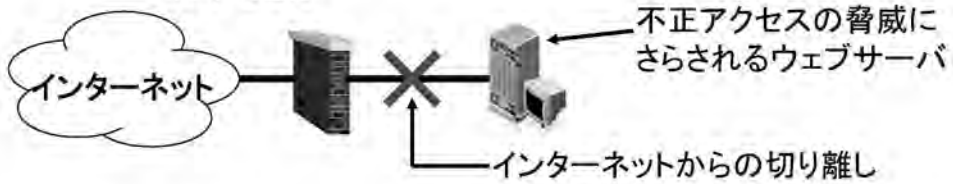
⑤緊急時における対策

危機管理面の整備

リスク回避及び移転

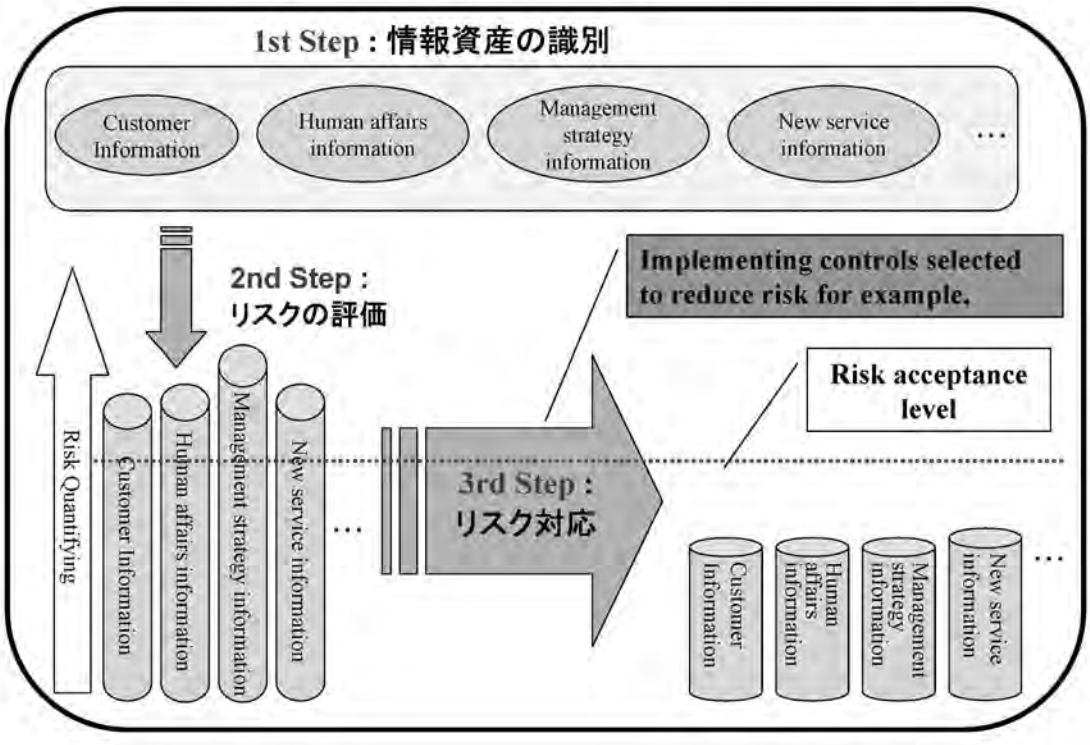
情報資産の有するリスクへの対応方法としては、前述の「受容できるレベルまで低減する」方法の他に、次の様な方法がある。

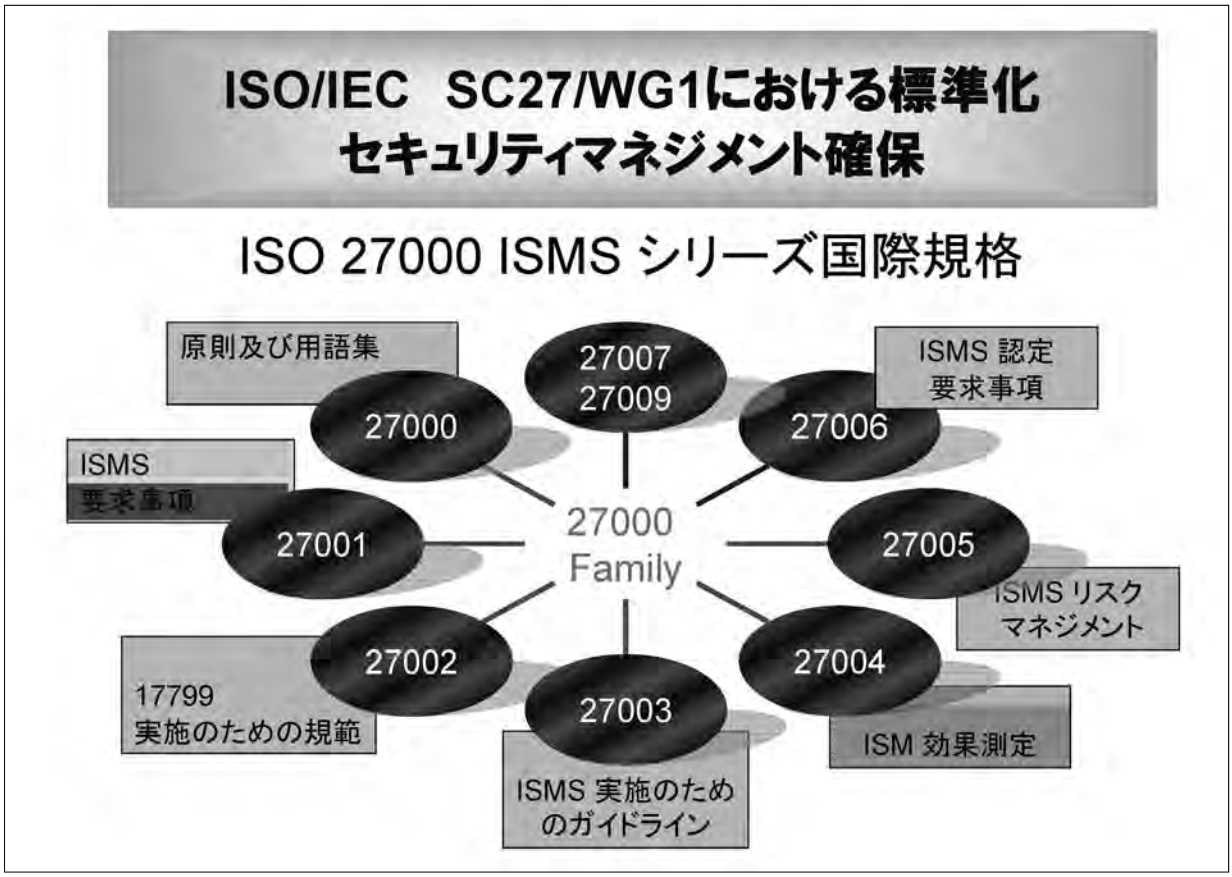
①リスクの回避：業務の廃止、情報資産の破棄により、リスクが発生しないようにすること

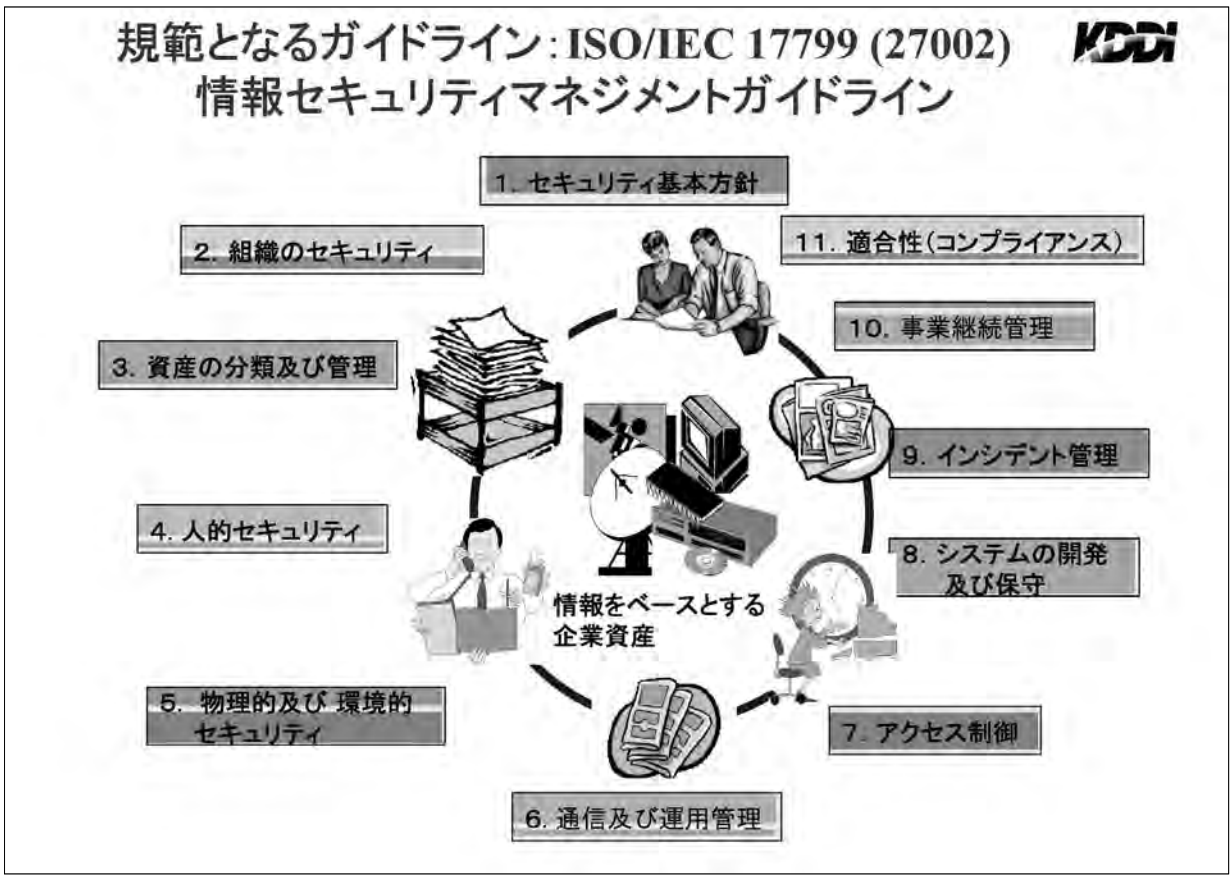


②リスクの移転：リスクを、契約等により他者に移転すること

すなわち、企業におけるリスク分析では




ISO/IEC SC27/WG1における標準化
セキュリティマネジメント確保
ISO 27000 ISMS シリーズ国際規格
原則及び用語集
27000
27007
27009
ISMS 認定
要求事項
27006
ISMS
27001
27000
Family
27005
ISMS リスク
マネジメント
27002
17799
実施のための規範
27004
27003
ISM 効果測定
ISMS 実施のため
のガイドライン


規範となるガイドライン：ISO/IEC 17799 (27002)
情報セキュリティマネジメントガイドライン
KDDI
1. セキュリティ基本方針
2. 組織のセキュリティ
11. 適合性（コンプライアンス）
10. 事業継続管理
3. 資産の分類及び管理
9. インシデント管理
4. 人的セキュリティ
8. システムの開発
及び保守
情報をベースとする
企業資産
5. 物理的及び 環境的
セキュリティ
7. アクセス制御
6. 通信及び運用管理

セキュリティの測定のガイドライン規格 ISO/IEC 27004

- 本プロジェクトは、情報セキュリティマネジメントの測定に関わる規格を作成することを目的としている。
- 本開発は、EFFECTIVENESS of ISMS Implementation（ISMS実施の有効性）について、測定することを目指している。
  - *パフォーマンスターゲットを決める*
  - *何を、どのように、どのタイミングで測定するのかを議論。*
- 現状は、第1次草案レベル

国内におけるISMS事業展開

ISMSの要求する主要なコンセプト

- 組織における個別のセキュリティ技術対策の他に、組織のマネジメントとして、自らのリスク評価により必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。
- 組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善すること。

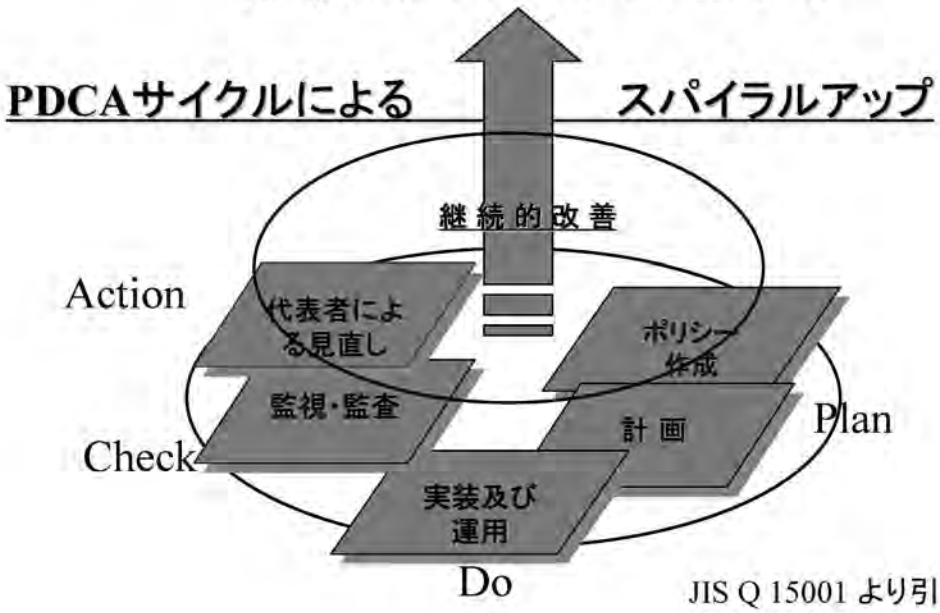
(財)日本情報処理開発協会　資料より

ISMS制度の目的

- 組織全体の情報セキュリティマネジメントの有効性についての客観的な評価基準を提示。
- ネットワークを介してビジネスを行う際の取引相手の情報セキュリティレベルを評価する手段。
- 国際標準「ISO/IEC 17799（Code of practice for information security management）」をもとに、国際的な取引の安全性・信頼性を確保。
- ISMS認証基準は国際標準ISO/IEC 17799:2000および英国規格BS7799-2:2002をもとにして作成。

(財)日本情報処理開発協会　資料より

ISMSでは、マネジメントシステム（PDCA）に基づく運用が鍵



JIS Q 15001 より引用・加筆

(財)日本情報処理開発協会　資料より

日本ISMSユーザグループ（J-ISMS UG）の活動内容（認証を受ける側の取組）

J-ISMS UGでは、次のような活動を展開予定

- ISMS構築・維持・改善のためのUG内情報共有
  - 会員向けセミナーの開催
  - 会員向け研究会、事例報告会
  - 会報発行
  - その他、会員間の交流・意見交換会 等
- ISMS普及促進のための啓発活動
  - オープンセミナーの開催
  - コンファレンスの開催
  - プロモーション活動の展開
    - WEB情報発信
    - ジャーナル発行
    - パンフレット、その他資料等の作成・提供

ISMSの今後

- ISMS国際規格化のさらなる推進
- ISMSの有効性測定に関わる検討の加速化
  （情報セキュリティマネジメントの評価に繋がる）
- リスク分析手法の検討の具体化
- ISMS構築、運用における
  課題抽出、情報共有（ユーザGの活用）
- 課題解決に向けた活動：ガイドライン化が要
- セクターベースのISMS Specificationの作成
- 国際的なクロスボーダー認証機構の構築

Telecom-ISAC Japanの目的
（ネットワーク事業者としての取組）

＊わが国の重要インフラである情報通信基盤の安全性確保

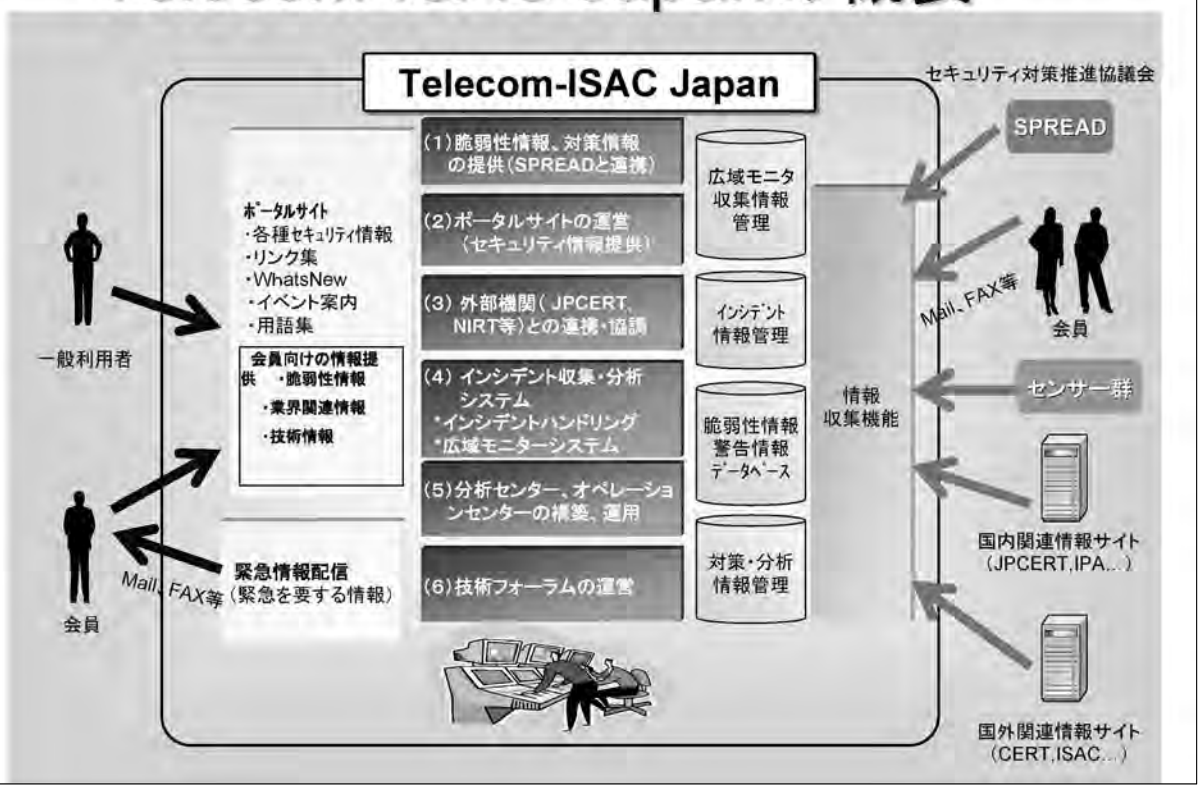
＊情報通信事業者を中心とする会員制で運営

＊参加資格要件を満たした会員間で対象とするインシデントに対する防護連携を図る

＊会員間でのインシデントに関する適切な情報共有をはかるための場の提供及び、会員間の連絡・連携をはかる中立且つ信頼された機関

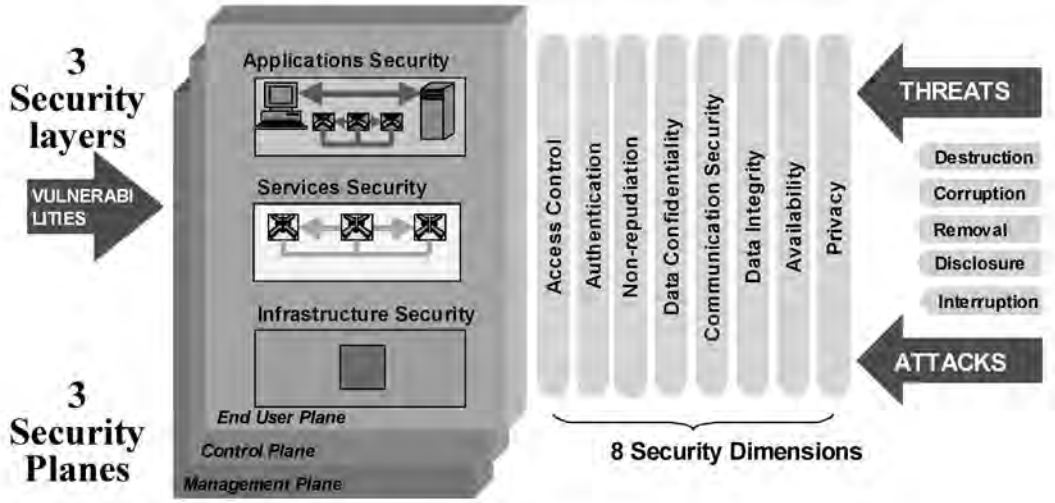
＊具体的には、通信サービスの提供を妨げる各種インシデントを収集・分析し、その分析結果を会員間で共有する

Telecom-ISAC Japanの概要



安全なネットワーク構築の指標(ITU−T)

X.805: Security Architecture for End-to-End Communications



・ぜい弱性は、各層、プレイン(面)、次元に存在する
・72 のセキュリティ観点 (3 Layers ✖ 3 Planes ✖ 8 Dimensions)

ITU-T X.805によるNWセキュリティ評価のアプローチ

	Infrastructure Layer	Services Layer	Applications Layer
Management Plane	Module One	Module Four	Module Seven
Control/Signaling Plane	Module Two	Module Five	Module Eight
User Plane	Module Three	Module Six	Module Nine

Execute
- **Top Row for Analysis of Management Network**
- **Middle Column for Analysis of Network Services**
- **Intersection of Each Layer and Plane for analysis of Security Perspective**

Access Control	Communication Security
Authentication	Data Integrity
Non-repudiation	Availability
Data Confidentiality	Privacy

The 8 Security Dimensions Are Applied to Each Security Perspective

内閣官房におけるセキュリティ評価の活動
「政府機関の情報セキュリティ対策のための統一基準（2005年項目限定版）」（2005.9.15）

●各府省庁の情報セキュリティ対策の整合化・共通化を促進し、**政府機関全体としての情報セキュリティ水準の向上を図るべく、「政府機関の情報セキュリティ対策のための統一基準」とその運用枠組みを政策会議決定**（平成17年9月15日）。

●今後、各府省庁は本基準を踏まえて対策を実施し、**内閣官房情報セキュリティセンター（NISC）が対策実施状況を検査・評価。**

ポイント

1. 政府機関統一基準の策定と省庁対策基準の見直し（水準の底上げ）
各府省庁の情報セキュリティ対策の整合化・統一化と、その水準の着実な引き上げ

2. 各府省庁の対策実施状況の検査と評価に基づくPDCAサイクルを確立
第三者の視点で内閣官房情報セキュリティセンター（NISC）が検査・評価し、当該評価結果を基に情報セキュリティ政策会議が結論→見直し

3. 政府機関統一基準の対策項目の具体化（個別ガイドライン群の策定）
各府省庁における具体的なレベルでの対策実施を支援するための個別ガイドライン群の策定
（例：webサーバ設置、モバイルPC管理等）

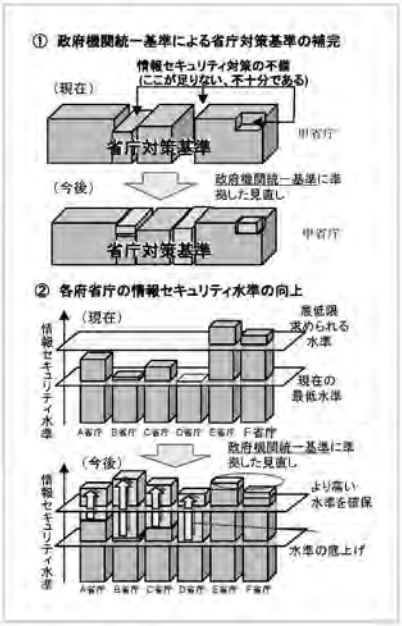
今回策定した文書

政府機関統一基準（2005年項目限定版）
「政府機関の情報セキュリティ対策のための統一基準」
各府省庁の情報セキュリティ対策内容の整合化・共通化を促進するために、各府省庁が採るべき情報セキュリティ対策を定めたもので、緊急性の高いものを中心に取りまとめ

＜盛り込まれた内容の例＞
- ●情報の格付け及び取扱制限に関する基準を明示する手順の整備
- ●情報の持ち出し等の制限事項の強化
- ●一定の情報システムに対するアクセス制御・ログ管理機能の導入
- ●サービス不能攻撃（DoS攻撃）対策の実施
- ●省庁ネットワークに対する不用意な接続の禁止
- ●外部委託先が遵守すべき事項等を含めた契約書の取り交わし

PDCAサイクルの確立
政府機関統一基準（2005年12月版(全体版初版)）の策定（年内目途）
→ 内閣官房情報セキュリティセンターによる検査・評価（本年度内目途）

対策の具体化
具体的対策基準として個別ガイドライン群を作成



端末とWebサーバの情報セキュリティの評価結果
（評点　A：良好、B：ほぼ良好、C：不十分、D：不良）（中尾の理解）

Inspection items

Inspection items for terminals	
Measures for oblique programs	• Status of applying patches to OS • Status of applying patches to main applications • Status of implementing anti-virus software
Measures for information protection	• Status of implementing cryptographic function on mobile PCs
Management of terminals	• Status of physical measures for terminals

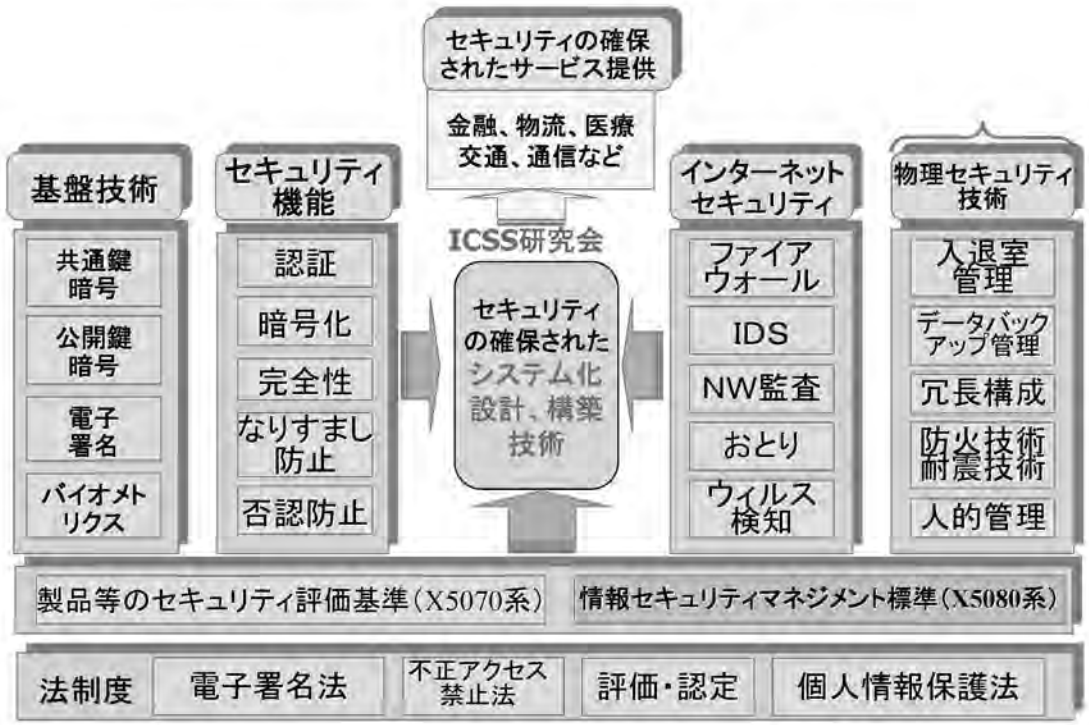
Inspection items for web servers	
Measures for oblique programs	• Status of applying patches to OS • Status of applying patches to web server applications　etc.
Measures for oblique access	• Status of measures for oblique access
Measures for Information protection	• Status of implementing access control for users
Management of servers	• Status of implementing access control for administrators • Status of measures for data recovery

➢This list shows the result based on the inspection in each government agency as of the end of March, 2006.

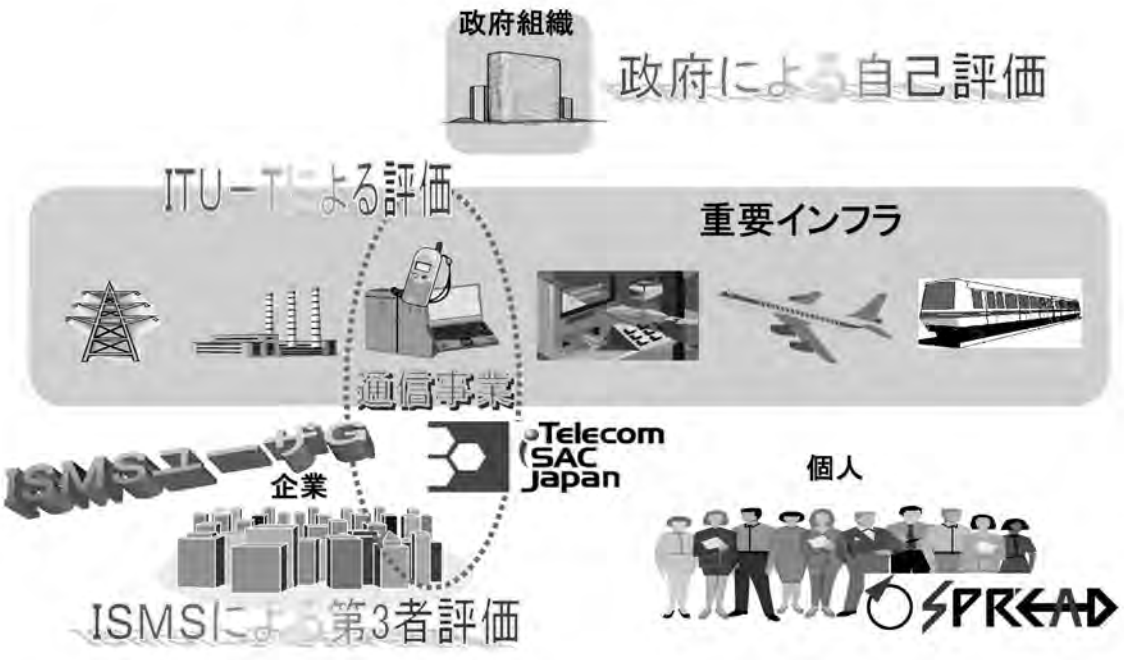
Government agencies	Evaluation results	
	Terminals	Web servers
Cabinet Secretariat	B	B
Cabinet Legislation Bureau	C	B
National Personnel Authority	C	B
Cabinet Office	C	C
Imperial Household Agency	D	C
Fair Trade Commission	C	A
National Police Agency	D	B
Japan Defense Agency	C	B
Financial Services Agency	B	B
Ministry of Internal Affairs and Communications	C	B
Ministry of Foreign Affairs	D	B
Ministry of Justice	D	C
Ministry of Finance	C	B
Ministry of Education, Culture, Sports, Science and Technology	C	B
Ministry of Health, Labour and Welfare	D	B
Ministry of Agriculture, Forestry and Fisheries	C	B
Ministry of Economy, Trade and Industry	C	B
Ministry of Land, Infrastructure and Transport	D	C
Ministry of the Environment	B	B

Level	Ratio	Level	Ratio	Level	Ratio	Level	Ratio
A	x＝100%	B	80%≦x＜100%	C	60%≦x＜80%	D	x＜60%

セキュリティ技術研究の鳥瞰図



広く相互に関連するセキュリティ確保



付録Ⅴ．4　適合度評価による非数値的尺度（メトリック）

AIST

資料5
1

適合性評価による
非数値的尺度（メトリック）

2006.11.24-5, ディペンダビリティWS

産業技術総合研究所 (AIST)
システム検証研究センター (CVS)
木下佳樹

AIST

CVS

自己紹介

- 研究分野：算譜意味論
- 職：システム検証研究センター長
  - 数理的技法の科学研究
    算譜意味論、形式技法する定理証明の計算機支援
  - 数理的技法のフィールドワーク
    技法導入実験による技術移転、研修コース研究開発
  - ソフトウェア認証
    計測標準研究部門（NMIJ, 旧計量研）と連携、
    OIML/D-SW (SC5/WG2), IEC61508などの規格に
    関係

AIST

システムの信頼性向上技法の研究をしている。

- 数理的技法：**情報システム**を**数学**の枠組で記述し、調べることによって、システムの**信頼性**を向上させる技法。

  自然現象を数学の枠組で記述するのとは違う。

  パタン認識、有限要素法等は自然現象を数学で記述。

  システムの記述に適しているのは離散数学。

AIST

信頼性とディペンダビリティ

- ディペンダビリティ

  ＝**信頼性**＋安全性＋セキュリティ＋可用性＋保守性＋公平性＋…

  ？セキュリティ、**信頼性**⊆ディペンダビリティ

- 「信頼性」は他の性質の基盤

  以下の■に安全、セキュア、可用 etc.のどれを入れても正しい

  『システムを■に設計・実現しても、設計・実現の**信頼性**が低ければ■なシステムとはいえない。』

  信頼性実現の研究に携わる我々が、ディペンダビリティに関係するのは、この意味において。

AIST CVS

認証＝規格＋技術文書＋認定

- システムが基準を満たすことを、利用者はどのように知ることができるか。
  - 製造者による**宣言**
  - 第三者による**認証**
- 第三者による認証のために必要なこと：
  - 認証の基準を**標準規格**として提示すること
  - 認証の方針と手順の具体的かつ客観的な提示
    - Guidelines, **技術文書**
  - 認証者がその能力をもつことの**認定**
    - 認証者が多数になるときに必要

AIST CVS

試験活動とその内容

AIST

組込システムのメトリック
➔適合性評価による非数値的尺度

- **組込システム**の研究はしていない。。。
  組込システムの世界が我々の仕事に注目している
- ソフトウェア**認証**の準備活動は開始以来五年
  計量器組込ソフトウェアの認証立ち上げ
  NMIJは法定計量の国家機関。
- 認証のためには**評価**が必要。
  確かに評価はやっている！
  ➔ではそこでの**尺度**は何なのか？
  数は出てこない！

AIST

今日お話したいこと：
適合性評価による尺度

- **適合性評価**は、指定された**検証項目**の集まりを満たすか否かの**真偽値ベクトル** (tuple) を与える。
  真偽値ではなく、「実現の仕方」かもしれない。
- 得られたベクトルがシステムの（検証項目の集まりに相対的な）**尺度**（メトリック）であると考えてはどうか。
- 適合性評価は、（ベクトルの形をした）尺度を『**測定**』する行為である。
- しかしこうして測定される尺度は**数ではない**！全順序でもないが、順序はついている。（False ≦ True をtupleに拡張）。

独立行政法人 産業技術総合研究所　システム検証研究センター

AIST

何のための情報システム評価？

- システム選択のためのデータ提供
  同じ仕様のシステムが複数ある場合；コンパイラ、データベース、通信ミドルウェアなど
- 発注システム検収のためのデータ提供
  注文どおりのものが収められているのか？

AIST

評価はどうあってほしいか？

- 二つのシステムの評価を**比べたい**。
- システムの評価がある程度**以上**である、といいたい。

➔

- 評価の結果に**順序**がつけられれば十分。
- 評価結果は**数**である必要はなく、**全順序**でなくともよい。

≪が（半）**順序**だとは：

反射的：x≪x

反対称的：x≪y しかも y≪x ならば x=y

推移的：x≪y しかも y≪z ならば x≪z

x≪y か y≪x が常に成り立つ⇒**全順序**

全順序でない順序例：数の対に対して (u,v)≪(x,y) ⇔(u≦xかつ v≦y)によって≪をさだめると、これは順序だが、(1,2)≪(2,1)でも(2,1)≪(1,2)でもない。

AIST

基準適合試験による評価？

- システムが基準に適合しているかどうか、
  基準＝標準、仕様 etc.
  数では測れない。
  全体が基準に適合するかどうかの True/False、または
  基準の満足され方
- 評価：基準の項目に「適合しているか否か」あるいは「適合のしかた」を評価の『尺度』（メトリック）としてはどうか？
  この尺度は数ではないが、比べられる。

AIST

例：秤組込S/W (WELMEC2.3より)

基準項目　普通の方法によってわざと行う変更から保護されていること

規制対象ソフトウェアの対応例

- 規制ソフトウェアはshellを通してのみアクセス。
- 規定されたインターフェイスを通してのみアクセス。

基準項目　規制対象外ソフトウェアとのインターフェイスの保護

規制対象ソフトウェアの対応例

- 規制部分に関するデータや機能を扱うのに用いられるプログラムモジュールを規定する。
- 保護されるインターフェイスによって実現する機能を規定する。
- 保護されるインターフェイスを通してやり取りするデータを規定する。

独立行政法人 産業技術総合研究所　システム検証研究センター

付録Ⅴ．5　ソリューションサービスの評価メトリック

情報システムのディペンダビリティ(評価)」
に関するワークショップ 資料

ソリューションサービスのディペンダビリティ評価の課題
ーメトリックス設定の困難さー

2006. 11. 24

NEC ソリューション開発研究本部

笠原 裕

1

ソリューションとは :顧客に最適解を提供すること

◆顧客の要望に応じて、システム設計を行い、必要なあらゆる要素（プロダクト、サービス）を組み合わせ、カスタマイズして提供

◆プロダクト (コンポーネント)
NW装置、サーバ、クライアント端末、OS、ミドルウェア、アプリケーション

◆サービス
コンサル、システム構築（SI)、運用管理、サポートサービス、アウトソーシング

ディペンダビリティの観点からの特徴

◆複数要素の複雑な組み合わせ
→ 要素の性質に左右される、組み合わせにより新たに発生する問題もある

◆要求レベルは、業種・業務毎に異なる、顧客の要求にも依存（顧客満足）
→ 要求レベルを定量的に表現する方法論が必要

◆人間系、社会的な影響も含めて（重要インフラの場合など)性能や品質を確保することが要求される

2

サービスとは :供給者と受容者が協同して価値を創造する行為

サービスの特徴 :無形性、生産と消費の同時性、・・・・

◆サービス産業： 国内産業の 70%近く 多種多様 次ページ参照）
ICTが絡まないサービスについては、とりあえず今回の検討の対象外。
リッツカールトンホテル、サウスウェスト航空、・・

◆情報サービス： 性能や品質についての評価尺度に加えて、サービスの内容についての評価はユーザーに委ねられる。 (例)情報検索、SNS、コンテンツ配信、・・

◆ITサービス 前ページのソリューションの一部として捉える）

ディペンダビリティの観点からの特徴

◆サービス産業毎に評価軸は異なる、共通軸も例えば顧客満足度など定量化が困難
→ 満足度を測る手法、パラメータ化の手順 (フレームワーク)が研究対象？

◆人間が絡む度合いが大きい
→ 人間系を含むディペンダビリティの評価尺度が必要

◆情報サービスの場合は、情報自体の信憑性、機密性、などが定量化対象？

ソリューションの事例とディペンダビリティの範囲

①NTTドコモのiモードセンター 「Circus」 :情報のライフライン
·1秒間に最大7万5000件(Webサイト閲覧:毎秒5万アクセス、メール送受信:毎秒2万5000件)
·1日あたり約65億件を処理、24時間365日無停止で提供
·利用者 :5000万人
·サーバー400台、ストレージ約400TB、ネットワーク機器600台
·トンネルと携帯電話 :新幹線は、約1000席 :7割の人が携帯電話の電源を入れていると、トンネルを抜けたとたんに、700台の携帯電話が、いっせいに、基地局に接続を求める。
⇒ 5秒で接続を完了できる。

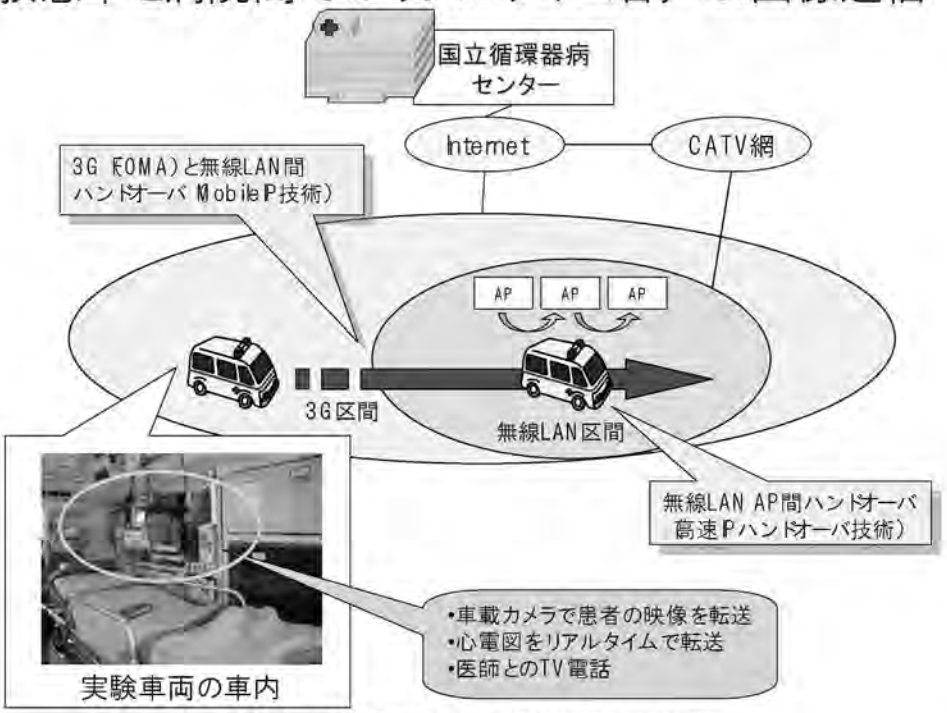
(*) iモードは、NTTドコモの登録商標です。
(*) CiRCUSは、iモードサービスのシステムの名称です

◆超ミッションクリティカルな重要インフラのディペンダビリティとは？

②救急車からの無線LAN接続によるリアルタイム情報共有 画像伝送を中心とした）
·最終的には患者が助かることがソリューション
·何か不具合が起こった時に、原因はNW,ハンドオーバー技術、オペレータミス、医者の指示ミス、・・・

◆重大な責任が発生する可能性のあるシステムでは、その所在の切り分けができる仕掛けも必要、メトリックスで十分に示せるか？ (NWはこれで十分など)

総務省との緊急医療支援システム実証実験
～ 救急車と病院間でのリアルタイム音声＆画像通信 ～」



③人間系が重要なファクタになるソリューション
・オペレータミス、人間的な連携が十分にとれないことに起因するシステムエラーが多発
航空管制、証券会社の誤発注、メガバンクの合併、スペース・シャトルの事故、原発の事故
・個人毎に評価が異なる（満足度など）場合
応答性能、画質、要求性能を絶対値で示し難い、過剰品質になることもある

◆ディペンダビリティとして人間系を含んだ指標、あるいは指標の決め方論も必要

④市場環境と深く関連するソリューション
・社会の急速な変化を予測できてなかったためシステムの能力が不足してダウン
携帯電話における加入者の急増
・市場の動きの読み間違い
集中的なアクセスでフラッシュピークが発生（チケットの申し込み、株取引の集中など）
オンラインゲームへの参加者多数で動作不良

◆ディペンダビリティの指標明示には、前提となる条件の明確化が必要
SLA(Service Level Agreement)問題に関連
利用者がこのぐらいの人数の時に、これだけの性能が出る・・・

⑤普通の企業向けソリューション
(例)電子会議ソリューション
ソリューションとしての評価軸：
·普通の対面会議と比べて同等の機能を果たせるか
音質、同時発話、リアルタイム性 音声、画像の遅延問題)、臨場感、投資効果
·十機能
ドキュメント共有、アプリケーション操作の共有、
·ディペンダビリティ関連では
落ちない、会議の秘匿性 盗聴されない)、性能 同時参加者数)、E2Eの品質

◆サービスされる機能と満足度 投資効果を含む)が評価軸になる

課題

·ソリューション ·サービス分野では、ディペンダビリティの 6指標に含まれない
評価軸も必要になりそう。 顧客満足度など

·人間系を含んだ指標が必要
オペレータが介在するシステム、組織間 人間間)連携が重要な場合

·重要インフラなどは社会的な影響まで考えた、性能要件や安全性まで配慮
されるべき。与える影響の度合いで、レベルを定義することも一つの方法

·サービス分野では、評価がサービスの需要者の委ねられる、定量化は難しい
サービス、ソリューションは業種 ·業務毎に要求レベルが千差万別

·システムコストも重要なファクタ
無制限に投資すればディペンダビリティは高くなるが、投資ーリスクの問題を
定量化して、システム構築時に意志決定者が選択をすることが重要

付録Ⅵ　グループ討議まとめ資料

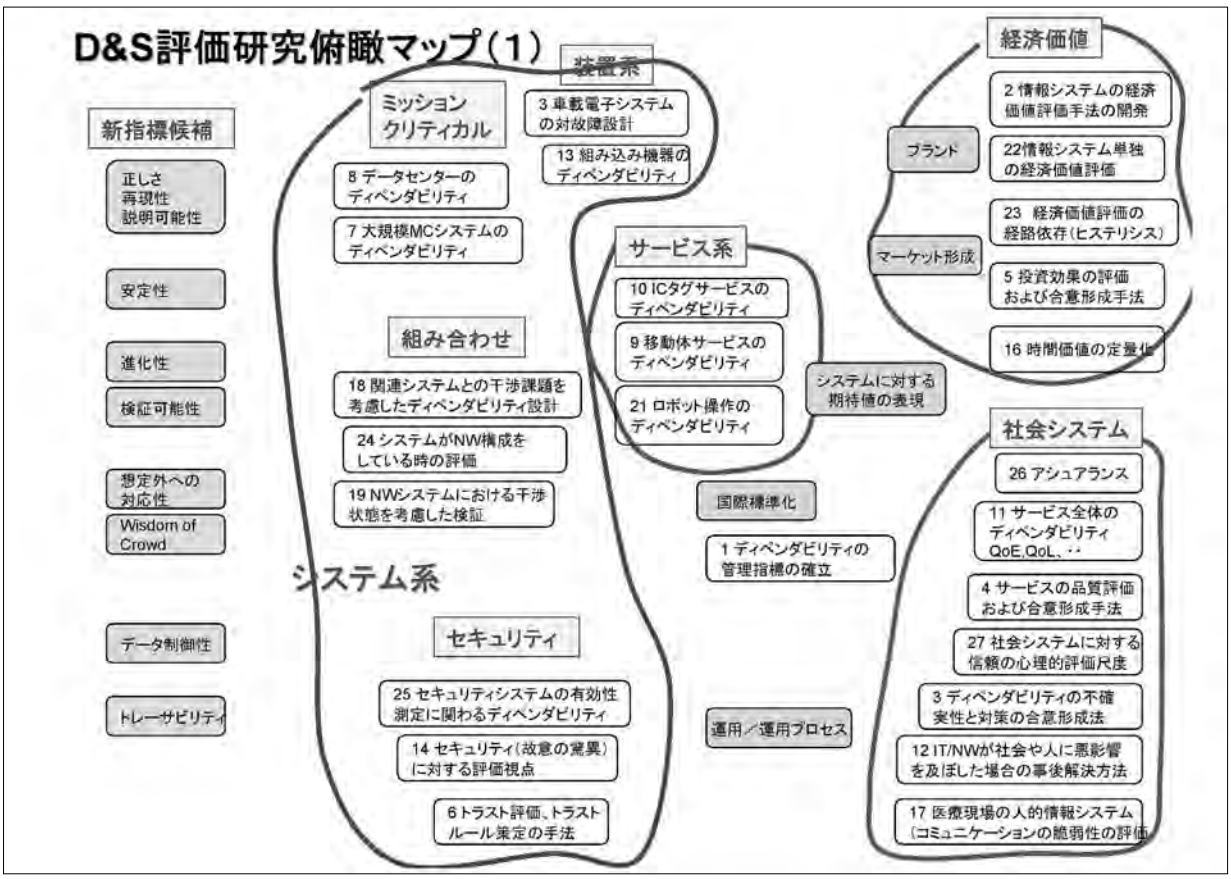
付録Ⅵ．1　グループＡ

「情報システムのディペンダビリティ評価」
に関するワークショップ資料

Aグループ検討結果報告
ーディペンダビリティ研究課題と研究推進方法の提案ー

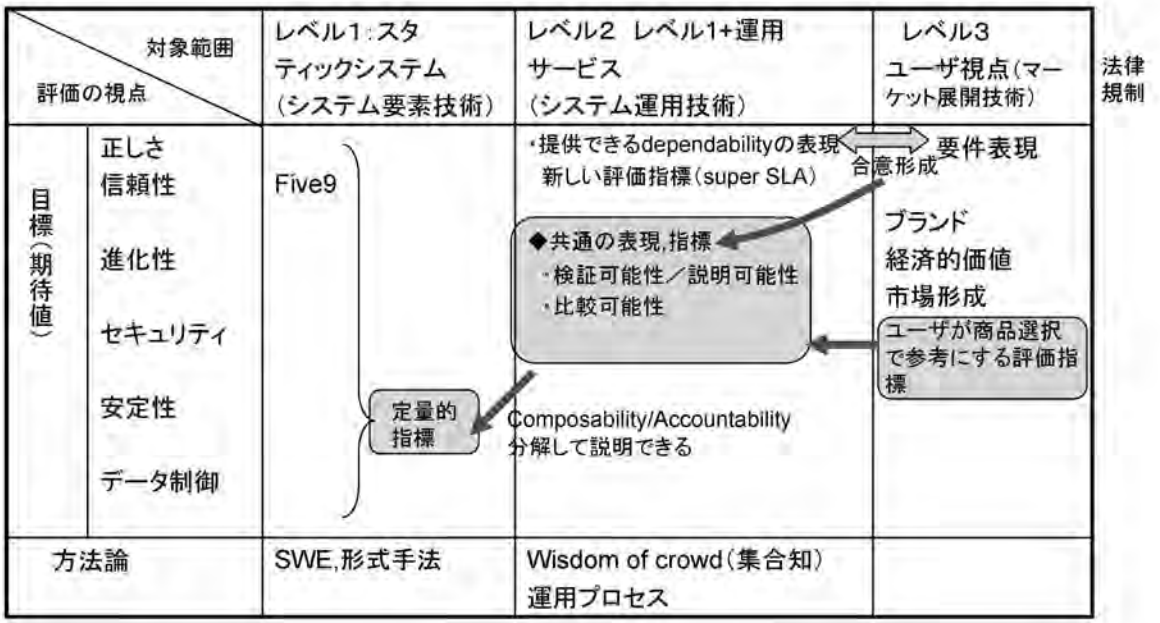
2006. 11. 25

ワークショップAグループ
菊野　亨、篠田　陽一、丸山　宏、藤井　眞理子
小菅　一弘、丹羽　邦彦、石正　茂、笠原　裕
（木俵　豊、田中　英彦、南谷　崇）



D&S評価研究俯瞰マップ(2)

・評価の観点を3レベルに分けた(システム視点、サービス視点、ユーザ視点)
・人間系に関わる問題はそれぞれのレベルで存在(設計、運用、満足)
・ユーザ視点からシステム視点まで共通に、あるいは分解可能な形で指標が定義されることが重要



研究課題

・ユーザ視点からシステム視点まで共通に、あるいは分解可能な形の指標の創出
・結果の保証をするシステムの概念、構築方法
・システムにもPL(product liability)を課すことの国民経済的な比較検討

【課題解決による効果】

◆情報システムの機能・性能から、経済的価値までつなげることができる
共通の言葉でコミュニケーションできる

◆情報システムの提供者と価値の受容者の間で、各種の透明性が増す
機能・性能の要求水準、価格、動作の境界条件、・・

◆産業界にとっては、契約時の不透明性が削減される
→オーバーロード/赤字プロジェクトの撲滅

◆ユーザにとっては、必要な価値だけを適切な対価で入手できる

◆情報システムのディペンダビリティを記述する指標の国際標準化を推進することにより日本が技術的にも情報システムの認定においてもディペンダビリティ先進国となれる

研究推進方法

実証ベースで指標の精度を上げる

①仮説として立てた指標の検証

◆仮説検証のためのテストベッドの構築：Town simulator/ emulator

Model-based/ measurement-based/ 第3のsimulation-based approach
経済価値のモデルをテストベッド上で時間加速実験、指標の有効性を評価

◆人間系のsimulationを含む・・・ゲームの形式

人間系を含む場合は時間加速は難しいが、ユーザ自体の研究も可能

②超dependableなシステムを作ってそこから指標を抽出する：Grand Challenge

(例)ディペンダブル特区での無人運転国家プロジェクト、ミサイル防衛、手術

③既に存在するデータの分析から指標をデザイン
事故のDB，自動車分野など

グループBからのアウトプット

グループBメンバー

- 高瀬先生：ロボティクス
- 野島先生：認知科学
- 森先生：情報理工学・技術経営　自立分散システム
- 赤津先生：情報システム・サービスの評価
- 木下先生：プログラム理論
- 中尾先生：情報ネットワークのプロトコル・情報セキュリティ
- 佐々木：CRDS　情報セキュリティ担当
- 嶋田：CRDS　大規模情報ハンドリング担当

1. 「D&S評価」研究俯瞰マップ

社会的背景　なぜ、今、dependableなのか？

- 社会の変化が激しくなってきている。
- 産業構造の変化も激しくなってきている。
- 変化に応じて、予測や対応が困難になってきている。
- 価値観・目的が多様化している。
- 主体によって目的も変わる。（設計者の視点からユーザーの視点へ）

- PDCAをまわすのが重要である。
- 時間軸を意識すべきで、最初に決めた基準が絶対ではない。
- 変化を前提に「ディペンダビリティ」を考えなければならない。

- 評価対象について、「環境の変化」と「目的の変化」の軸がある
- 評価対象について、「予測可能」と「予測不可能」の軸がある。

1. 「D&S評価」研究俯瞰マップ

	環境の変化	目的の変化
予測可能	①例）暗号方式の変化、事前に計画されたイベント 観測する状態や対策案の多様性	④例）複数システムの接続、機能の継承、 コンパティビリティ
予測不可	②例）新種ウイルス、突発的トランザクション増加 機能・性能としての対応の容易性	③例）ビジネス環境の変化、価値基準の変化 構造（アーキテクチャー）としての対応の容易性

対症療法的な従来型アプローチでは解決困難な領域であり、新たな研究パラダイムが必要

2. 重要研究課題

- まずは、前記の「変化が予測不可能な領域」における課題に絞る。
- 「PDCAサイクルへの適用」という目的を意識して、
  以下の各フェーズでの課題を考える。

- 構造（アーキテクチャ）上の課題と、アーキテクチャがフィックスした前提での個別の技術課題とを分けて考える。
- 標準化には、構造の議論が不可欠であり、前者が重要。

2. 重要研究課題

	構造（アーキテクチャー）	評価	個別技術	評価
変化の認知・識別	・環境変化を測定しやすい構造 ・context awarenessを容易にする構造	・測定のしやすさ	・環境変化の測定技術 ・環境の記述手法 ・context awarenessを可能にする技術	・環境変化の大きさ ・awarenessの度合い
リスクの評価・分析	・リスクの識別を容易にするアーキテクチャ（例：第三者による監査等） ・重要インフラの相互依存関係検出を容易にする構造	・リスク識別の容易さ ・重要インフラの相互依存関係の複雑さ	・リスクの認知 ・重要インフラの相互依存関係の検出技術	・リスクの評価（影響度合い、発生確率など） ・重要インフラの相互依存度
情報共有、合意形成	・コミュニティ内での共通認識を醸成する情報公開、共有の構造（例：CSR, Wisdom of community） ・合意形成を促進する関与者間の構造	・dependabilityに対する理解度・リテラシー ・関与者の納得感	・情報共有技術 ・合意形成手法	・情報共有量 ・合意に至る時間
対応実施、継続性確保	・予見のカバレッジを広げ、リスク対応を容易にする構造 ・予見だけでなく、回復までの連続的な対応ができる構造	・時間軸を考慮したリスク対応の有効性	・効果的なリスク対応手法	・ポイントでのリスク対応の有効性

未知の変化への耐性、即応性

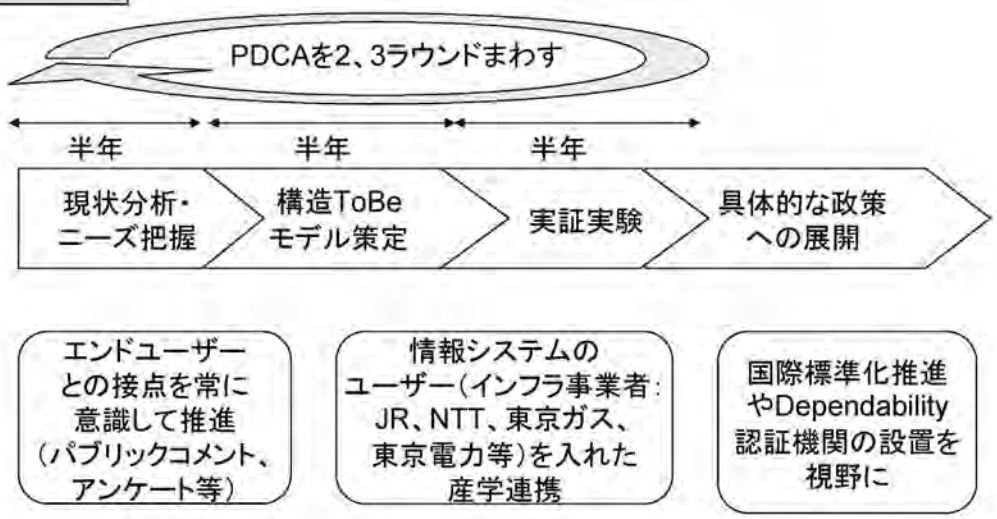
補足：こんな評価尺度がほしい

- 評価尺度は、単純で、計測容易なものでなければいけない
- 人に使われなければ、評価尺度を作る意味がない
- 人間の直感に訴え、納得ができるようなものでなければならない

3. 研究推進方法

基本方針	構造上の課題に力点をおく。

アプローチ



ディペンダビリティ評価における重要研究課題

2006年11月25日

グループC

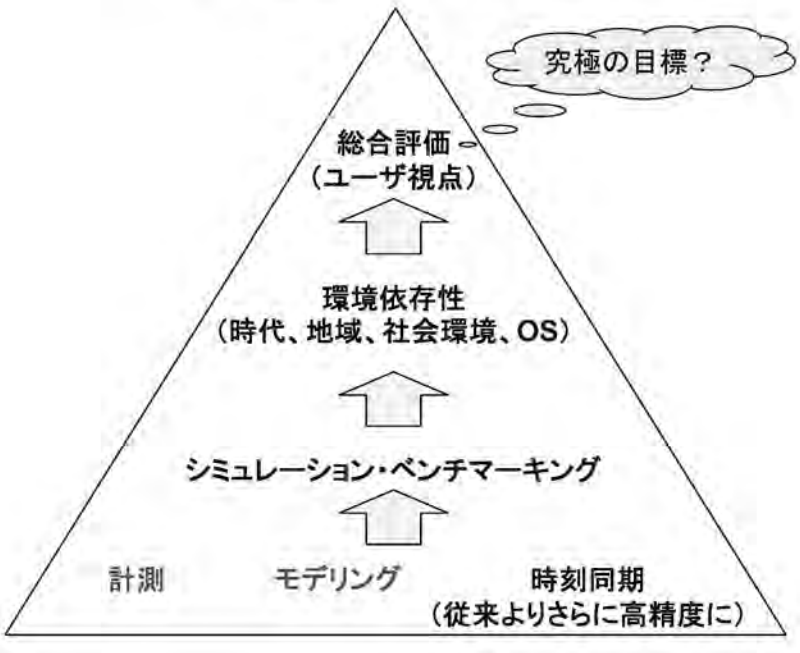
メンバー

- 丸山　文宏（富士通研究所）→企業システム・サービス
- 佐々木　良一（東京電機大学）→セキュリティ
- 土肥　正（広島大学）→ディペンダビリティ
- 本間　浩一（フリーランス）→企業システム
- 松本　雅行（東日本旅客鉄道）→列車運行システム
- 伊関　洋（東京女子医科大学）→医療システム
- 三木　哲也（電気通信大学）→ネットワーク
- 成瀬　雄二郎（JST/CRDS）→LSI・デバイス
- 伊東　義曜（JST/CRDS）→半導体
- 波多腰　玄一（JST/CRDS）→半導体

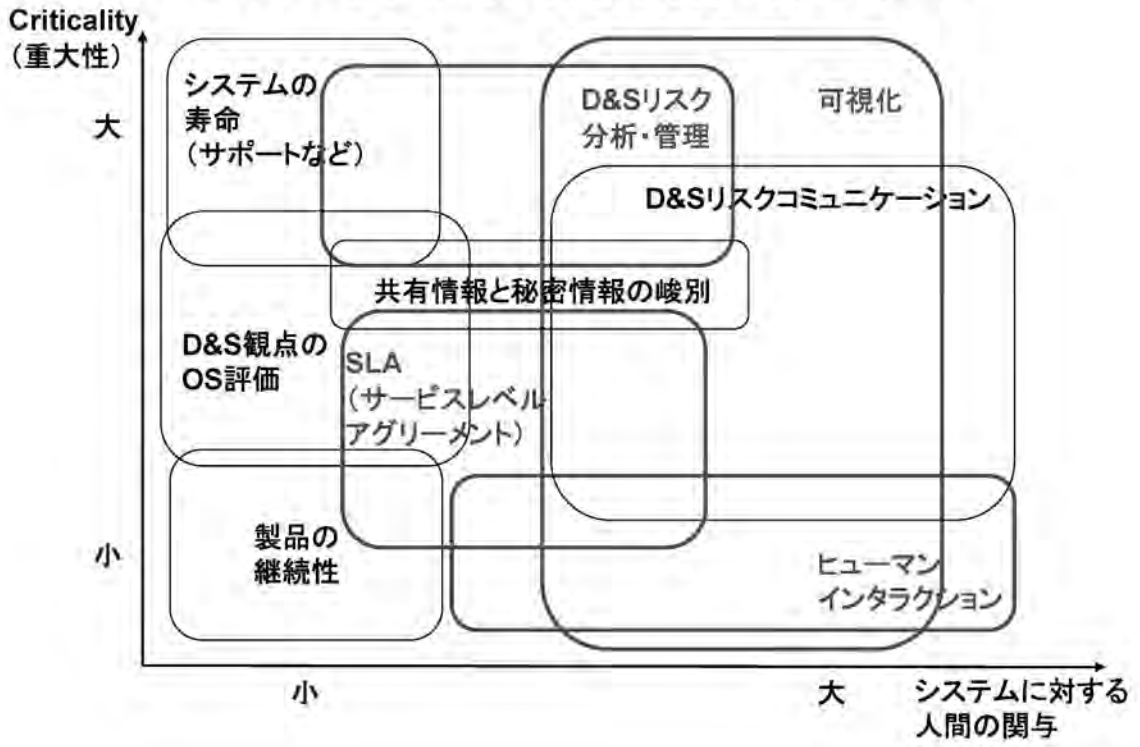
グループ討議のアプローチ

- セキュリティと具体的なシステム（特に、医療システム）をターゲットとして検討
- 研究俯瞰マップの軸として、システムに対する人間の関与（X軸）とCriticality（Y軸）に加えて、共通のベースとなる階層を設定

「D&S評価」研究俯瞰マップ ～ベースとなる階層～



「D&S評価」研究俯瞰マップ



重要研究課題（1）

- 計測
  - ヒューマンファクタや主観的な評価指標の計測・評価はまだこれから
  - モデリングとの効果的融合も課題
- モデリング
  - 学問の基本的なベース
  - 実際のデータと整合性のあるモデリングが重要
- 可視化
  - 映像データによる可視化
    - 手術の映像など
  - 取得データの可視化
    - 「コックピット」やマイニング結果の可視化など
  - 研究の事例は多いが、製品レベルの事例はまだ少ない

重要研究課題(2)

- D&Sリスク分析・管理
  - もともと軍需で進んでいる領域で、日本では遅れている
  - リスク分析は行われているが、定量評価に結び付いていない
- SLA(サービスレベルアグリーメント)
  - 取り組みはあるが十分ではない(特に、日本では曖昧にしておく傾向がある)
    - 障害かどうかの定義も明確でないケースがある
  - 国際標準化が重要
- ヒューマンインタラクション
  - ユーザ視点からの定量的評価の取り組みはまだ少ない

グループ討議のアプローチ

ユーザ視点のディペンダビリティの評価リスト

セキュリティと医療システム
が対象

将来のシステムを見越して

トレードオフの関係にある指標を組み合わせて
ニュー・ディペンダビリティの総合評価指標(特に、デペンダビリティ<狭義>とセキュリティ)

寿命

ソフトにおける
セキュリティとディペンダビリティの融合

主観的な評価指標(ヒューマンエラー、ヒューマンインタフェース)
→主観的な評価指標の評価方法

◇ 執筆者一覧（執筆者：敬称略）◇

「情報システムのディペンダビリティ評価」
に関する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