CRDS-FY2006-GR-04

ATTAATC A AAGA C CTAACT CTCAGACC
AAT A TCTATAAGA CTCTAACT
CTC G CC AATTAATA
TTAATC A AAGA C CTAACT CTCAGACC
AAT A TCTATAAGA CTCTAAC
TGA C CTAACT CTCAGACC

G-TeC報告書

「情報システムのディペンダビリティ評価」国際技術力比較（欧州、米国）

0101 000111 0101 00001
001101 0001 0000110
0101 11
0101 000111 0101 00001
001101 0001 0000110
0101 11
00110 11111100 00010101 011

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

複雑にネットワーク化された情報システムを基盤とする情報社会は、偶発的に生じる人間の設計ミスや操作ミス、ハードウェアの物理的な不具合、悪意を持つ人間によるシステム侵入やデータ破壊、社会や環境の変化に対するシステムの劣化など、その信頼と安全を脅かす様々なリスクに直面している。目指すべき社会の基盤を成す情報システムは、このような多様なリスクの存在にもかかわらず、その提供するサービスが良質で信頼でき、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」との提言を行った。

この提言に沿って新しい情報技術体系の研究開発を促進し、その成果の経済・社会的効果を明示するためには、社会システムレベルから構成要素レベルまでユーザ視点で情報システムのディペンダビリティを定量的に示す指標とその評価手法の確立、およびそれらに基づいた経済価値の可視化が必要である。また、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、国際標準化など、我が国の国際競争力の新たな源泉の創出が期待できる。

このような観点から「情報システムのディペンダビリティ評価」についての世界における研究開発動向の調査を実施した。

調査は次の3つの方法で実施した。

1）ディペンダビリティ評価に関する世界的拠点となっている欧州と米国の研究機関の訪問
2）ディペンダビリティ研究の最新成果が発表される2つの国際会議への出席
3）欧州と米国のファンディングエージェンシによる非公開ワークショップへの参加

調査の結果得られた主な所見は以下の通りである。

1）システムのモデリング解析、フォールトインジェクションによるシミュレーションなど、ディペンダビリティ評価の基礎的研究は欧米で進んでいるが、実システムの評価に結びついていない。原因はシステムの複雑さと規模の大きさにあるが、この状況は今後さらに深刻になるため、その克服にはブレークスルーが必要である。また、別の原因として、ディペンダビリティの経済価値が十分認識されない状況で、メーカーもユーザも評価技術の基礎となる実システムのフォールトや障害に関するデータを公表してこなかったことが挙げられる。
2）一方で、フォールトインジェクション・ツールを提供して組み込みソフトウェアの評価を行うポルトガルのベンチャー企業（Critical Software社）が世界の宇宙開発関連の政府機関・企業との取引で急成長している。各国の顧客に加えて、米国のNASAや我が国のJAXAもその顧客である。ソフトウェアの信頼性・頑健性を評価する商用ツールが他に見あたらないことが同社の急成長を支えていると思われる。
3）ディペンダビリティ・ベンチマークのプロジェクトが2002年から2004年まで、フランス、ポルトガル、イタリア、スウェーデンを中心とするEUプロジェクト（FP 6）として3年間実施され

たが、対象がOSなどの一部のシステムに限られ、また人為フォールトに対する考慮が十分ではないなど、国際コミュニティでも成果があったとは見なされていない。ベンチマーキングは今後の課題である。

4）情報システムのディペンダビリティだけではなく、情報システムを活用した重要インフラ（電力・エネルギー網、情報通信網、輸送網、金融網、政府中枢など）のディペンダビリティ・セキュリティ確立が社会の安全保障に欠かせないとの認識から、広域電力制御の依存性解析のプロジェクトがEC（欧州）とNSF（米国）のファンディングで実施されている。欧州はLAAS/CNRSが拠点、米国ではUniv. Illinoisが中心になり電力会社とコンソーシアムを形成している。

5）米国ではI 3 P（Institute for Information Infrastructure Protection）が、ディペンダビリティとセキュリティの評価指標を定めること（Metrics）が、経済活動にとっても社会の安全にとっても必須であるとして、次の4つのグランドチャレンジを提言している。

チャレンジ1：適切なセキュリティ・メトリクスを定義する
チャレンジ2：メトリクスを評価する方法を定める
チャレンジ3：異なる階層（組織、システム、構成要素）のメトリクスを総合する
チャレンジ4：設計、更新、運用段階でのメトリクス測定ツールを開発する

6）欧・米ともに経済価値へのマッピングの視点はまだ十分認識されていない。ユーザ視点の評価指標、評価手法も未開発である。しかし、多くの面談者が評価メトリクスから経済価値へマッピングの重要性に賛同している。

7）欧州（EC）と米国（NSF, DHS）のファンディング組織が連携した共同研究へ向けての動きが始まっているが、そこでも、ディペンダビリティ／セキュリティの評価技術が将来EUとUSで優先的に投資すべき重要分野に一つとして挙げられている。

以上の所見から、戦略プロポーザル創案にあたっては、以下のような視点からの提言を行うことが望ましい。

1）欧米に比較してディペンダビリティ／セキュリティ分野の研究者が少ない我が国では、個別の研究者に資金をばらまくのではなく、ディペンダビリティ/セキュリティ研究拠点を設置してアプリケーション（社会インフラも含む）研究者を巻き込んだ戦略的な研究推進が必要である。

2）国の安全保障の観点から、国の重要インフラ（電力・エネルギー、情報通信、輸送、金融、政府機関）を含めた我が国のネットワーク全体の依存性解析調査を早急に実施し、ディペンダビリティ／セキュリティの国家的長期戦略を構築する必要がある。

3）ディペンダビリティ／セキュリティを主たる目標とする技術開発を促進するためには、そのためのインセンティブの存在が重要であり、ユーザ視点からのディペンダビリティ／セキュリティ評価指標の開発、およびそれに基づいた経済価値へのマッピングとその可視化が必要である。

4）欧州と米国の連携、共同研究、テストベッド構築、国際標準化への動きに積極的に関与し、グローバルな価値指標構築へ向けた我が国からの働きかけが必要である。そのために、欧州、米国のファンディング当局と連携する我が国の窓口を早急に整備する必要がある。

CONTENTS

1

はじめに

はじめに

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・セキュ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。

この提言に沿った情報技術体系の研究開発を促進し、その成果の経済・社会的効果を明示するためには、情報システムのユーザ視点からのディペンダビリティを定量的に示す評価指標とその評価手法の確立、およびそれに基づいた経済価値の可視化が必要である。

しかしながら、物理的要因だけではなく人間的な要因や複雑なシステム相互作用要因を含む情報システムのディペンダビリティ評価技術に関する現状は、我が国も含めて国際的にも、確立された評価尺度や測定法が存在せず、また経済価値へのマッピングも未開発の状況にある。

こうした認識から、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」に関するワークショップを開催し、評価技術の研究俯瞰マップの作成、重要技術課題の抽出などの作業を行った。このワークショップ開催に前後して、その議論の合理性と正当性を補強するため、これまでディペンダビリティ評価に関する研究で世界をリードしている欧州と米国の研究拠点を訪問し、その研究動向と今後の展望を調査するG-TeCを実施することとした。

まず、2006年10月18日～20日にポルトガルのコインブラで、欧州でこの分野のトップ研究者が集まる国際会議 EDCC（ European Dependable Computing Conference）が開催されたので、この会議への参加を含めて、この前後に欧州における拠点であるフランスのLAASとポルトガルのコインブラ大学を訪問調査した。また、ディペンダビリティ技術のユーザ企業であるAirbus社（フランス）とフォールトプロジェクションの商用ツールを開発するコインブラ大学発のスタートアップ企業であるCritical Software社（ポルトガル）を訪問調査した。

次に、2006年11月15、16日にIrelandのDublinで、欧州のEC（European Commission）と、米国のNSF（National Science Foundation）及びDHS（Department of Homeland Security）が共催するワークショップ"EU-US Summit Series：Workshop on System Dependability & Security"が開催された。この会議は、欧州と米国からそれぞれ25名程度のトップ研究者を招き、ディペンダビリティとセキュリティの研究において将来重要となる優先分野に関して欧州と米国で認識を共有し、両者が連携した共同研究の可能性を醸成することを目的としているが、日本もオーストラリアと共に特別に招待されて参加し、意見交換を行った。この会議は、我が国が将来、ディペンダビリティ評価技術の国際標準化活動に主導的に関与していく場合に大きな意味をもってくる可能性がある。

最後に、12月18，19日に環太平洋地

域を中心とする国際会議PRDC（Pacific Rim International Symposium on Dependable Computing）に参加するとともに、ディペンダビリティ研究の米国における拠点であるイリノイ大学を訪問調査した。

最終的には、これらの調査で得られた知見と、上記「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における議論を基にした提言内容を戦略プロポーザルとしてまとめ、広く科学技術政策関係機関、研究者コミュニティへ向けて発信し、ファンディング戦略の実現に活用することを目指している。

2

調査の必要性と重要性

調査の必要性と重要性

今日、我々の社会では、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。この依存度は今後ますます高まり、もはや情報システムなしでは日常生活や企業活動、国家機能さえも成り立たなくなるだろう。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、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など、情報システムの障害やその関連事故は枚挙にいとまがない。目指すべき社会の基盤を成す情報システムは、多様なリスクの存在にもかかわらず、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、その成果の経済・社会的効果を明示するためには、情報システムのユーザ視点からのディペンダビリティを定量的に示す評価指標とその評価手法の確立、およびそれに基づいた経済価値の可視化が必要である。

これまでの情報システムは、もっぱら高機能化、高速化、高集積化を目指してきたが、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重要なシステム目標とすべきであり、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／セキュリティの評価尺度、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。また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、国際標準化など、我が国の国際競争力の新たな源泉の創出が期待できる。

しかしながら、物理的要因だけではなく人間的な要因や複雑なシステム相互作用の要因を含む情報システムのディペンダビリティ評価技術に関する現状は、我が国も含めて国際的にも、確立された評価尺度や測定法が存在せず、また経済価値へのマッピング手法も未開発の状況にある。このような認識から、研究開発戦略センターでは「情報システムのディペンダビリティ評価」に関するワ

ークショップを開催し、ディペンダビリティ評価研究の現状を俯瞰し、重要分野と研究課題を抽出する作業を行った。

一方、情報システムのディペンダビリティ評価に関して、システムを提供する側の視点からではあるが、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算出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観測するフォールトインジェクション研究では、欧米のいくつかの研究拠点が先行している。これらの研究拠点におけるこれまでの研究成果と現状、今後の研究方向に関して調査し、国際的な技術動向の比較を行うことは、人間要素まで含めてユーザ視点のディペンダビリティ評価と経済価値の可視化を狙った研究開発推進計画の立案に欠かせない。特に、フランス・ツールーズの国立研究所 LAAS/CNRS と米国の University of Illinois, Urbana-Champaign は、それぞれこれまでディペンダビリティ評価技術の分野で世界をリードしてきた欧州及び米国の拠点である。この二つの研究拠点の訪問調査は、世界の研究動向を把握する上で必須であり、またこの 2 カ所が世界の評価研究の動向を代表していると考えることができる。

今回、研究開発戦略センターが開催した「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における議論では、

1）人為的要因および相互作用的要因によるシステム・ディペンダビリティへの脅威

2）ユーザ視点のディペンダビリティ評価指標と測定法開発

3）経済価値へのマッピングの確立

というこれまでにはない 3 つの新しい視点を導入している。これらはこれまで欧米においても十分研究されてこなかった視点である。少なくとも、これまでの科学技術雑誌や国際会議での発表論文など、既存の出版物からはこのような視点での議論は見えていない。従って、特にこの 3 つの視点の新規性、有効性を確認するためにも、欧州及び米国における上記拠点の研究者を直接訪問して現状及び今後の方向を調査することが極めて重要であり、また戦略プロポーザルの作成にとって必要なことであった。

3

調査方法

調査方法

調査は3期に分かれる。

1期(2006.10.16-24):
国際会議EDCC参加及び欧州の拠点研究機関の訪問

2期(2006.11.15-16):
EU-US Workshop on System Dependability & Security参加

3期(2006.12.15-20):
国際会議PRDC参加及び米国の拠点研究機関の訪問

毎年ヨーロッパで開催されるディペンダブルコンピューティングに関する国際会議EDCCでは、ヨーロッパの大学、研究機関、企業における最新の研究成果が発表され、研究者が集まるので、この会議への参加はヨーロッパの研究動向を調査するための極めて効率的な機会を提供する。今年はEDCCがディペンダビリティ評価のためのフォールトインジェクション技術の研究で実績があるポルトガルのコインブラ大学で開催されたため、この会議への参加を調査日程の中心に据えた。訪問調査する研究機関としては、フォールトインジェクション技術の研究で実績があるコインブラ大学と、ディペンダビリティ研究に関するヨーロッパにおける中心的研究機関であるフランス・ツールーズのLAAS/CNRSを選んだ。また、ディペンダビリティ評価に関連する企業として、ディペンダビリティ評価のビジネスで急成長を遂げているコインブラ大学発のスタートアップであるCritical Software社と、ディペンダブル組込みシステムの大きなユーザであるAirbus社を選んで訪問調査を行った。但し、Airbus社に関しては、A380の納期遅延に伴う経営陣の交代と事業のリストラ問題が発生したため、訪問直前の9月末になって「会社の事情によりすべての外部からの訪問を断る」と通告され、LAAS内の場所を借りてAirbus社の技術担当者との面談を行った。

同じく毎年環太平洋地域の諸国(アジア、オセアニア、米国西海岸など)の研究者が集まる国際会議PRDCがカリフォルニア大学リバーサイド校で開催されたため、この会議への出席に合わせて、米国におけるディペンダビリティ研究の中心機関の一つであるイリノイ大学のCoordinate Science LaboratoryおよびInformation Trust Instituteを訪問調査した。

さらに、欧州のEC(European Commission)と、米国のNSF(National Science Foundation)及びDHS(Department of Homeland Security)が共催するワークショップ"EU-US Summit Series:Workshop on System Dependability & Security"に日本もオーストラリアと共に特別に招待されて参加し、意見交換を行った。

これら一連の調査に参加したメンバは以下の通りである。

生駒俊明(センター長):1期のEDCC、LAAS、Airbus社調査に参加
南谷　崇(シニアフェロー/東京大学教授):すべての調査に参加
成瀬雄二郎(シニアフェロー):1期の調査に参加
石正　茂(フェロー):1期のEDCC、

LAAS、Airbus 社調査のみ参加

土肥　正（広島大学教授）：1 期の調査に参加

土屋達弘（大阪大学助教授）：1 期の LAAS、Airbus 社調査のみ参加

4

欧州拠点の調査結果

欧州拠点の調査結果

4.1 コインブラ大学

日時：10月16日15：00-18：00、17日 15：00-18：30
場所：Departamento de Engenharia Informatica, Universidade de Coimbra, Polo II-3030-290, Coimbra, PORTUGAL
面談研究者：Prof. Enrique Madeira, Prof. Joao Gabriel Silva（Dean）, Prof. Marco Vieira

【詳細説明】

10月16日に宿泊ホテルでMadeira教授と待合わせ、コインブラ大学情報工学科を訪問する。情報工学科はコインブラ市の旧市街にあるメインキャンパスではなく、少し街中から離れた別キャンパスに位置している。ディペンダブルシステム研究グループの所有するスペースや設備を見学した後、Madeira教授の居室で、今回のJST-CRDS の調査目的について説明し、ディペンダビリティの計測と評価に関する研究動向について情報交換を行なった。コインブラ大学ディペンダブルシステム研究グループはフォールトインジェクションに基づいたディペンダビリティ評価研究の拠点であり、グループでこれまでに達成した研究成果と現在進行中のプロジェクトについて意見交換を行なった。夕食時などの時間を利用し、Joao Gabriel Silva教授、Marco Vieira 教授と研究上の討論を行なった。

10月17日の午後は、再度、コインブラ大学を訪問し、ディペンダブルベンチマーク（Dependability Benchmark：DBench）に関する研究について説明を受けた。まず最初に、Vieira教授によるオンライントランザクション処理（OLTP）システムのDBenchに関する研究成果について報告を受けた。続い

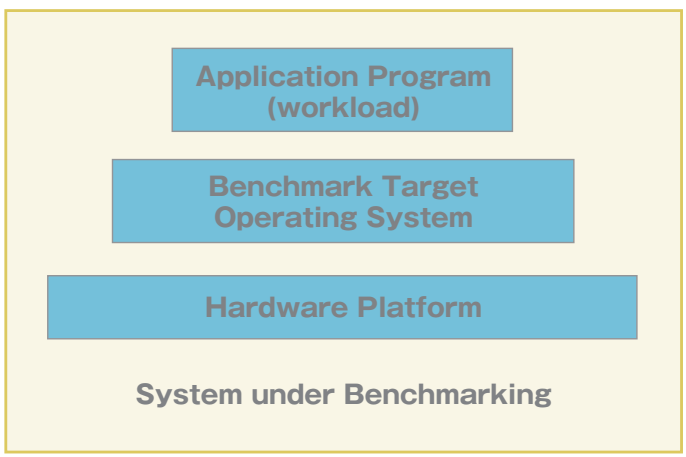

図1　ベンチマーキングの概念図

て、コインブラ大学の大学院生によるWebサーバーシステムのDBenchについて研究発表があった。

DBenchは、1998年～2002年にEUにおける Information Society Technology（ist）によって財政支援を受け、ヨーロッパの各研究機関によって実施されたディペンダビリティ評価プロジェクトであり、プロジェクト終了後も継続して研究が行なわれている。フランスのLAAS-CNRS がコーディネータを務め、Critical Software社、コインブラ大学、Friedrich Alexander University、Erlangen-Nurnberg、Polytechnic University of Valenciaが参画していた。DBenchの目的は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することである。DBenchで解析の対象となったシステムはWindowsなどのOS、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システムなどであり、現在では、さらにいろいろな情報システムへの適用やセキュリティ評価への応用が検討されている。

ベンチマーキングの基本的な原理を理解するために、ターゲットシステムとしてOSを考えよう。オープンソースのOSとは異なり、WindowsなどのOSでは障害が発生してもユーザが直接ソースコードにアクセスすることが出来ない。さらに、OS上で発生した障害に関連したバグレポートはユーザに公開されることはないので、ユーザがOSのディペンダビリティを評価するためには生産者側からの広告情報だけに基づくしか方法はなく、ディペンダビリティを計測・評価することは永久に不可能である。そこで、あるworkloadを負荷したApplication Programを規定のハード

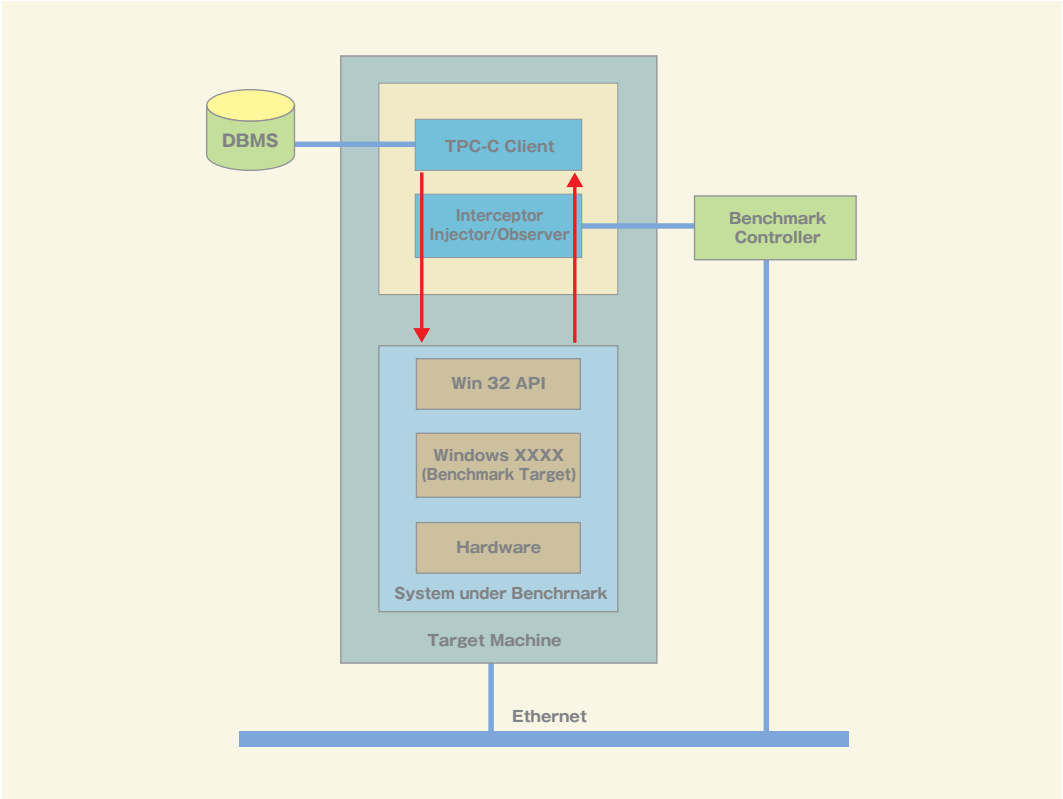

図2　OSベンチマーキングのシステム構成

ウェアプラットフォーム上で稼動させ（図1を参照）、フォールトを挿入することでシステムのディペンダビリティを計測する。より具体的には、図2に示すような実験設備を構築し、ある種のFault Loadに沿った形でFault Injection Toolを使用してコード上でフォールを挿入し、出力としてシステムのロバストネス、リスタート時間、リアクション時間などの属性パラメータを計測する。このような実験を模擬的に繰返す方法をSimulating Fault Injectionと呼び、通常のPhysical fault Injectionとは区別される場合が多い。

属性パラメータの実現値の統計的な性質（平均、分散）を調べることで、ベンチマーキングの指標を得ることが出来るが、さらに信頼度、定常アベイラビリティ、MTTF (Mean Time to Failure)、MTTR (Mean Time to Recovery) などの定量的ディペンダビリティ評価尺度を算出することも可能である。但し、図3に示す通り、上述のようなディペンダビリティ評価尺度を計測するためには様々な形でモデル化を行なう必要があり、Measurement-based approach とModeling-based approachの両方が必要とされる。

このように、ターゲットシステムが何であるかによって、ベンチマーキングのシステム構成や計測単位の属性パラメータが異なるので、標準的な方法論が確立されることが急務となっている。セキュリティシステムのベンチマーキングの問題はさらに深刻で、Security loadを如何に設定しどのようなベンチマーキングのシステム構成を行なうべきかについても明らかになってはいない。また、図3で述べたMeasurement-based approachとModeling-based approachの融合は未だに効果的な形で実現されておらず、ディペンダビリティ計測に向けた研究成果の進展が期待される領域である。

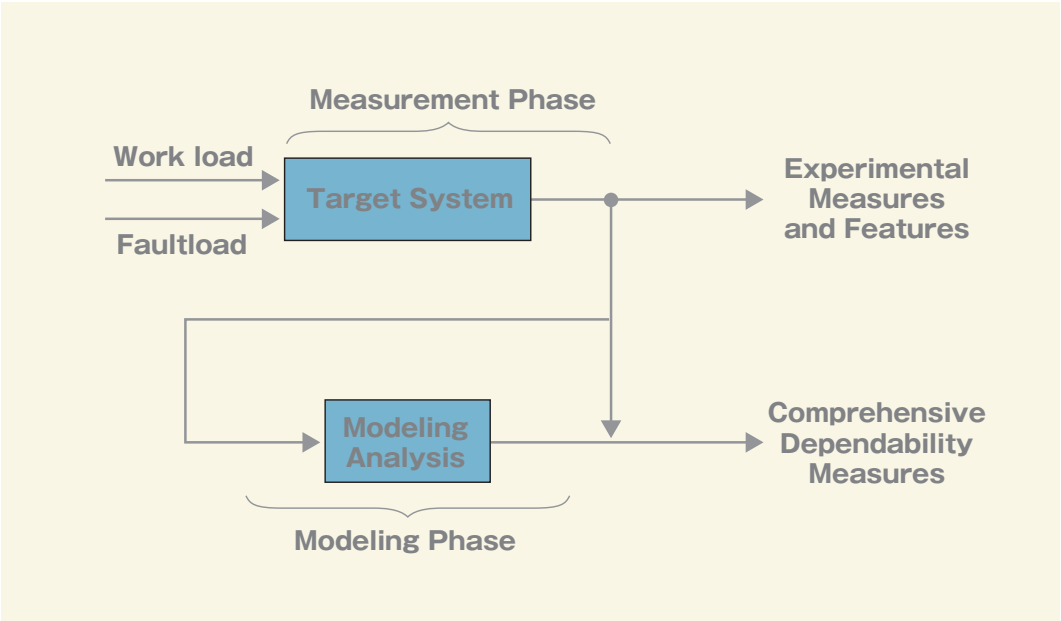

図3　ディペンダビリティ評価手続きの一例

4.2 Critical Software 社訪問

日時：10月17日 9：30-11：30
場所：Critical Software（CSW）、Coimbra、PORTUGAL

【スケジュール】
JST Visit to Critical Software

9：30-9：35	*Welcome Address* Henrique Santos Madeira（University of Coimbra） Nuno Silva（CSW）
9：35-10：00	*JST-CRDS Presentation：Introduction about the Mission* Takashi Nanya（JST-CRDS）
10：00-10：30	*CSW Company Presentation* Nuno Silva（CSW）
10：30-10：40	*Coffee Break*
10：40-11：00	*Exception Fault Injection Tool Demo*
11：00-11：15	*Dependability & Embedded*
11：15-11：30	*Open Discussion*

【詳細説明】

（a）CSW Company Presentation

Project managerのRicardo Maia氏が不在であったため、Engineering Manager のNuno Silva氏からCSWの概要紹介があった。CSWはコインブラ大学の卒業生が4名で起業したベンチャー企業であり、1998年に設立された。会社設立当初は、コインブラ大学ディペンダブルシステム研究グループの出身であったということで、フォールトインジェクション技術を中心にしたソフトウェアシステムの高信頼化技術が業務の中心であった。しかしながら現在では、一般的なソフトウェアの開発業務の割合も増加してきているが、Mission Critical System や Business Critical System を対象としたソリューション部門も会社の重要な収益源となっている。 CSWの過去5年間の平均成長率は50％を超え、従業員数140～220名、平均年齢20代後半という若き優良ベンチャー企業である。

ディペンダビリティ評価業務の中でも、Fault Injection Tool「Exception」はディペンダビリティ研究コミュニティだけでなく世界各国の企業や研究機関から注目を集めている。対象とするシステムの領域はIndustry、Aerospace、Defense、Telecommunication、Public Sectorと多岐に渡り、NASAや日本の宇宙開発事業団や、NATOや各国の政府機関などとのプロジェクトにも数多く携わっている。具体的な事例として、宇宙システムに使用されるオープンソース実時間処理カーネルの評価、日本のJAXAの開発したシステムの検証を行なうためのExceptionの活用、EUのグローバルナビゲーション衛星システムであるGALILEOシステムの評価、ポルトガルにおけるFire Hazardシステムの開発などが紹介された。

(b) Exception Fault Injection Tool Demo

Fault Injection Tool「Exception」の説明とデモが用意された。Fault Injectionの原理的な説明と動作規則については、Madeira教授から補足的に説明がなされた。担当者によって、実際にfault Loadに従ってフォールトを自動生成し、システムの実行ごとに挿入したフォールトの影響をシミュレートしている様子を解説してもらった。デモを通じて、CSWもExceptionのいくつかの問題点を把握しており、さらなる進化形を開発するためにもコインブラ大学を始めとする大学との共同研究を将来的にも行なってゆきたいとのことであった。

4.3 EDCC-6参加報告

4.3.1 会議概要

2006年10月18日～20日の3日間、ポルトガルのコインブラ市において第6回ヨーロッパディペンダブルコンピューティング会議(6 th European Dependable Computing Conference: EDCC-6)が開催された。コインブラ市は丘の上にあるコインブラ大学を中心に発展してきた歴史のある街で、商業都市のポルトに次いでポルトガル3番目の文化都市である。人口は10万人弱の小さな都市ではあるが、コインブラ大学はディニス王によって1290年に設立されたヨーロッパ最古の大学のひとつであり、1911年にリスボン大学が設立されるまでは国内唯一の大学であった。ポルトガルの大学数が非常に少ないにもかかわらず、コインブラ大学のディペンダビリティ研究グループのプレゼンスは非常に高く、リスボン大学の研究グループとともに、ディペンダビリティ研究のヨーロッパにおける研究拠点として既に認識されている。

EDCC-6はコインブラ大学の中でも古いCollege of Jesusで開催された。EDCC-6の実行委員長はコインブラ大学のJoao Gabriel Silva教授であり、プログラム委員長はChalmers University のJohan Karlsson教授が務めた。EDCC-6は小規模ながらも質の高い論文が発表される会議として知られており、今年はRegular Paper 11本、Practical Experience Report 2本、Tool Paper 1本が採択された。本年度は、当初55本(Regular Paper 47本、Practical Experience Report 4本、Tool Paper 4本)の論文投稿があり、33本がヨーロッパから、13本が北米及び南米から、6本がアジアからの投稿であった。Regular Paperは3名のプログラム委員と最大4名までの外部査読委員によって査読が行われた。Practical Experience ReportとTool Paperも同様に、3名のプログラム委員が査読を行い、1名もしくは2名の外部査読委員が割当てられた。最終的に、55本の投稿に対して延べ296名による査読が行われ、各論文に対する平均査読者数は5.4名であった。本年度のRegular Paperの採択率は23.4%、Practical Experience Reportの採択率は50%、Tool Paperの採択率は25%であった。EDCCに投稿されるほとんどの論文が極めて質が高いので、感覚的には、実質採択率はさらに低いものと予想される。査読結果は、2006年6月15日～16日にスウェーデンのGöteborgで開催されたプログラム委員会で慎重に議論され、2日間の議論を通じて採択論文が選定された。

EDCC-6への参加者は60名弱であり、ヨーロッパにおいてディペンダビリティ研究に携わるほとんどすべての研究者が参加していた。EDCCは単に高品質の論文を発表する場だけではなく、西ヨーロッパにおけるディペンダビリティ研究者コミュニティの情報交換の場としても機能しているようである。共同研究の促進やファンディング情報の交換など、研究者間のネットワークを形成するためにEDCCが一役買っていることは間違いない。ちなみに、今回、日本からのEDCCへの参加者はG-TeC関係者5名を含めた7名であり、国別参加リストの中ではかなり上位に位置していた。10月17日の夕刻のレセプションには、世界各国から参加者が集結し、新旧の親交を温めた。学会場はヨーロッパの大学特有の伝統的な階段教室となっており、時空を超えて伝統と歴史の重みを感じながら会議に臨むという心地よさを感じた。10月18日のWelcome Address and Introductionでは、実行委員長のSilva教授の挨拶に続き、プログラム委員長のKarlsson教授から論文選択過程の詳細な説明があった。会議は10月20日の午前中まで続き、ほとんど全ての参加者が最後のセッションまで残っていた。EDCCは2年に1回、南米で開催されるLADCと交互に開催されるようで、次回の学会は2008年に開催されることになる。

Tuesday, October 17

19:00-21:00 Welcome Reception（Conference Venue）

Wednesday, October 18

08:30-09:00 Conference Registration
09:00-09:30 Welcome Address and Introduction
09:30-10:30 Keynote Address：*A business case for dependability*
Joao Carreira
10:30-11:00 Coffee Break
11:00-12:30 Session 1：Robustness and Fault Tolerance
Design of a highly dependable operating system
Jorrit N. Herder, Herbert Bos, Ben Gras, Philip Homburg and Andrew S. Tanenbaum
Automatically finding and patching bad error handling
Martin Suesskraut and Christof Fetzer
Communication integrity in networks for critical control systems
Anis Youssef, Yves Crouzet, Agnan de Bonneval, Jean Arlat, Jean-Jacques
Aubert and Patrice Brot

12:30-13:30 Lunch
13:30-15:00 Session 2 A：Practical Experience Reports and Tools

A fault tolerant VoIP PBX on standards based COTS platform
Anand Gorti
Lessons learned from the deployment of a high-interaction honeypot
Eric Alata, Vincent Nicomette, Mohamed Kaaniche and Marc Dacier
Session 2 B：Fast Abstracts I

15：00-15：15 Coffee Break

15：15-16：15 Session 3：Fault Injection
Temporal characterization of embedded systems using Nexus
Juan Pardo, Jose-Carlos Campelo, Juan-Carlos Ruiz and Pedro Gil
Injection of faults at component interfaces and inside the component code：are they equivalent?
Regina Moraes, Ricardo Barbosa, Joao Duraes, Naaliel Mendes, Eliane Martins and Henrique Madeira

16：15-16：30 Coffee Break

16：30-18：00 Panel 1：*In search of real data on faults, errors and failures*
Chair：Miroslaw Malek

18：00-19：00 Visit to the Physics Museum of the University of Coimbra

Thursday, October 19

09：00-10：30 Session 4 A：Hardware Implemented Fault Tolerance
SEU mitigation techniques for microprocessor control logic
Ganesh T S, Viswanathan Subramanian and Arun Somani
Fault-tolerant distributed clock generation in VLSI systems-on-chip
Matthias Fugger, Ulrich Schmid, Gottfried Fuchs and Gerald Kempf
Dynamic derivation of application-specific error detectors and their implementation in hardware
Karthik Pattabiraman, Giacinto Paulo Saggese, Daniel Chen, Zbigniew Kalbarczyk and Ravishankar Iyer
Session 4 B：Fast Abstracts II

10：30-11：00 Coffee Break

11：00-13：00 Session 5：Student Forum
N/2 + 1 alive nodes progress condition
Ruben De Juan Marin

Robustness testing for reactive systems
Saad Khorchef Fares
COTS-based safety critical systems : challenges and approaches
Gabriella Carrozza
Fast & early validation of VLSI systems
Luis J. Saiz
Proactive resilience
Paulo Sousa

13 : 00 - 14 : 30 Lunch
14 : 30 - 15 : 30 Special Session : Research on Trust and Security in FP 7
15 : 30 - 16 : 00 Coffee Break
16 : 00 - 16 : 30 EDCC Business Meeting
16 : 30 - 19 : 00 Local Tour
20 : 00 - Conference Banquet

Friday, October 20

08 : 30 - 10 : 00 Panel : *Education in dependable and resilient computing ? Meeting the needs of the information society*
10 : 00 - 10 : 30 Coffee Break
10 : 30 - 12 : 30 Session 6 A : Dependable Storage and Services
Impact of WAN channel behavior on end-to-end latency of replication protocols
Roberto Baldoni, Carlo Marchetti and Antonino Virgillito
Customizable service state durability for service oriented architectures
Xianan Zhang, Matti Hiltunen, Keith Marzullo and Richard Schlichting
Storage tradeoffs in a collaborative backup service for mobile devices
Ludovic Courtes, Marc-Olivier Killijian and David Powell
Rephrasing rules for off-the-shelf SQL database servers
Ilir Gashi and Peter Popov
10 : 30 - 12 : 30 Session 6 B : Fast Abstracts III
12 : 30 - 14 : 00 Lunch

4.3.2 詳細説明

（1）Keynote Address：A Business Case for Dependability

学会のスタートを飾る基調講演は、（株）Critical Software 社（CSW）ディペンダビリティ評価部門の J. Carreira 博士によって行なわれ、ディペンダビリティ評価ビジネスの現状についての概要説明があった。G-TeC 関係者は前日に CSW を訪問し、より詳細な説明を受けていたので、特に新しい情報が得られたというわけではなかったが、Fault Injection Tool の Exception を武器にディペンダビリティ評価ビジネスで活躍していることは世界的にも徐々に認知され始めているようである。コインブラ大学との共同研究やコインブラ大学から優秀な人材を確保するルートを常に保持しているという意味で、CSW は世界中のディペンダビリティ研究者コミュニティから熱い注目を集めている。

（2）Robustness and Fault Tolerance

ロバストネス評価と耐故障評価のセッションでは 3 つの Regular Paper の発表があった。Construction of a highly dependable operating system では、OS の障害の多くがデバイスドライバに含まれるバグに起因することに着目し、kernel tables の数を削減し、各々のドライバを独立した権限を与えない use-mode process として稼動させることで、この問題が緩和されることを実証している。

Automatically finding and patching bad error handling では、サーバシステムで発生するエラーを自動的に検知しパッチをあてるために、フォールトインジェクションを用いた方法を提案し、具体的にどのタイプのパッチが機能的であるかを決定するために 2 値コード上の静的な解析を行っている。Communication integrity in networks for critical control systems では、LAAS-CNRS と Airbus France が共同で communication integrity protection scheme を開発し、error detecting code として cyclic redundancy code が適していることを示した。

（3）Practical Experience Reports and Tools

10 月 18 日午後の最初のセッションは Practical Experience Report 1 本と Tool Paper 1 本から構成された。A fault tolerant VoIP PBX on standards based COTS platform では、Voice over IP Softswitches のディペンダビリティを向上させるためのデザインと実行に焦点を当て、サービスアベイラビリティフォーラム（SAF）仕様のミドルウェアを用いてオープンソースである asterisk private branch exchange application に耐故障性を付加することに成功している。Lessons learned from the deployment of a high-interaction honeypot では、ハニーポットと呼ばれる脆弱性を予め埋め込んだサーバを意図的に配置しておくことで、悪意のある攻撃者の攻撃パターンを探知する方法に着目し、高い interaction を有するハニーポットを6ヶ月間観測した結果について報告された。

（4）Fault Injection

このセッションではフォールトインジェクションに関する Regular Paper 2 本が発表された。Temporal charac-

terization of embedded systems using Nexus は、ヨーロッパにおいてコインブラ大学、LAAS と並んで Fault Injection 研究が盛んな Technical University of Valencia からの発表で、実時間組込みシステムに対してフォールトインジェクションを実行する場合においてフォールトの効果を計測し分析するための方法論について述べている。Injection of faults at component interfaces and inside the component code：are they equivalent? はコインブラ大学と CSW の共同研究であり、API（Application Program Interface）のパラメータを操作することで interface faults を挿入し、Java や C 言語で記述されたコンポーネントアプリケーションのディペンダビリティを実験的に評価する方法を提案している。

（5）Panel 1：In Search of Real Data on Faults、 Errors and Failures

Miroslaw Malek 教授（Humboltdt-Universitat zu Berlin）がコーディネートするパネルでは、コンピュータシステムのフォールト、エラー、障害データの重要性と、それらの企業における活用についてパネリストからの報告を受けた。パネリストは D. Controneo（Universita di Napoli）、D. Penkler（Hewlett-Packard）、H. Madeira（University of Coimbra）、M. Reitenspiess（Fujitsu Siemens Computers）であり、企業や大学におけるアカデミック研究の観点からフォールトや障害に関する実データのマネジメントについて議論があった。余談ではあるが、G-TeC 参加者は Malek 教授、Penkler 博士、Reitenspiess 博士と夕食を共にし、ヨーロッパの中でも特にドイツにおけるディペンダビリティ研究の現状、サービスアベイラビリティフォーラム（SAF）における活動と企業コンソーシアムなどの話題で議論を行った。

（6）Hardware Implemented Fault Tolerance

10 月 19 日の最初のセッションはハードウェアフォールとトレランスに関する 3 本の Regular Paper が発表された。SEU mitigation techniques for microprocessor control logic はアイオワ州立大学からの発表で、マイクロプロセッサの制御ロジックを保護するために 3 種類のアーキテクチャ構成を提案したものである。シミュレーション実験を通じて、フォールト検知能力も向上が見られた。Fault-tolerant distributed clock generation in VLSI systems-on-chip では、VLSI 上に実装される broadcast primitive に基づいた fault-tolerant tick generation algorithm を提案している。提案された VLSI チップに対するクロック生成法を検証するために、FPGA プロトタイプに基づいた実験の内容についても紹介した。Dynamic derivation of application-specific error detectors and their implementation in hardware はイリノイ大学アーバナシャンペイン校からの発表で、アプリケーションの実行 corruption が発生したときに広範囲に渡るデータエラーを予防するために、アプリケーションに特化した自動化されたエラー検知機能を導入している。提案アルゴリズムはエラー検知カバレッジを最大にするよう設計されており、フォールトインジェクションに基づいた実験を通じてその有効性が検証されている。

（7）Education in Dependable and Resilient Computing-Meeting the Needs of the Information Society

学会バンケットの翌日にも拘らず、最終日の10月20日も早朝から多くの参加者が会場に集まった。最終日の最初の時間帯にはパネル討論会が企画され、Johan Karlsson教授がコーディネータとなり、ディペンダビィリティ計算とレジリエント（弾性）計算の教育現場における課題について話し合われた。パネリストは、W. Arendt（Chalmers University of Technology）、R. Jimenez-Peris（Universidad Politecnica de Madrid）、L. Simoncini（Universita di Pisa）、P. Verissimo（Universidade de Lisboa）であり、各国・各大学における当該教育現場におけるニーズとシーズについて紹介があった。

（8）Dependable Storage and Services

最後のセッションでは、主にディペンダブルストレージとWANチャンネルのサービス効果に関する研究発表があった。Impact of WAN channel behavior on end-to-end latency of replication protocolsでは、2つもしくは3つのtier architectureを用いて実行される複製プロトコルの性能解析を行なっている。ソフトウェア複製に対して3つのプロトコルのend-to-end latencyを比較することで、ネットワークチャンネルに対するプロトコルの感度を調べている。Customizable service state durability for service oriented architecturesでは、アーキテクチャレベルでサービスディペンダビリティの向上を実現するために、サービス状態の耐久性と呼ばれる属性に着目することを提案しており、Webサービスのアベイラビリティを向上させるための定性的な方法について検討を行っている。Storage tradeoffs in a collaborative backup service for mobile devicesは、モバイル環境において共同バックアップサービスを実現する際に必要とされるであろう耐故障技術を提案し、ストレージレイヤのプロトタイプを開発することで、いくつかのストレージレイヤアルゴリズムを比較・評価している。Rephrasing rules for off-the-shelf SQL database serversでは、SQLサーバから得られたバグレポートの解析と耐故障サーバの構築が障害検知能力を向上させることに成功した経験から、データ分散など他の耐故障性の側面を調査するためにSQL rephrasing ruleを定義することを提案している。

4.4 LAAS/CNRS訪問

4.4.1 調査結果概要

ディペンダブルコンピューティングの世界的な拠点であるLAAS（Laboratory for Analysis and Architecture of Systems）研究所を訪問し、LAASで実施されているディペンダブルコンピューティングに関する研究調査と情報交換を行った。まず最初に、Directorである Malik Ghallab博士から、LAAS研究所が携わっている研究分野や、人員の規模といった組織に関する基本的な情報について説明を受けた。その後、南谷教授から、JST-CRDSの基本情報や訪問の意図について説明を行った。引き続い

て、ディペンダブルコンピューティング分野における世界的な研究者であるJean Arlat博士、Karama Kanoun博士、Jean-Claude Laprie博士、Mohamed Kaaniche博士との議論を行った。

【スケジュール】
Visit of the JST-CRDS Delegation

9：00-9：30	Welcome Address Malik Ghallab（LAAS-CNRS）
9：30-10：00	JST-CRDS Delegation：Introduction about the Mission Takashi Nanya（JST-CRDS）
10：00-10：30	The Dependable Computing and Fault Tolerant Research Group Jean Arlat（LAAS-CNRS）
10：30-11：00	State of Knowledge in Dependability Evaluation Karama Kanoun（LAAS-CNRS）
11：00-11：15	Break
11：15-11：45	Dependability Evaluation of Critical Infrastructures：Modeling Interdependencies Jean-Claude Laprie（LAAS-CNRS）
11：45-12：15	Evaluation of Security：Characterization of Attacks Mohamed Kaaniche（LAAS-CNRS）
12：15-12：45	Dependability Benchmarking Karama Kanoun（LAAS-CNRS）
12：45-14：15	Lunch
14：15-15：00	Brief Presentations of Selected IST Projects： -Network of Exellence：ReSIST Jean-Claude Laprie（LAAS-CNRS） -Specific Targeted Research Projects： CRUTIAL and HIDENETS Mohamed Kaaniche（LAAS-CNRS）
15：00-16：00	Discussion：Additional Questions, Future Plans, etc.
16：00	End of Meeting

【詳細説明】

（a）The Dependable Computing and Fault Tolerant Research Group

まず、Jean Arlat博士から、LAASにおけるディペンダブルコンピューティング研究に関する概要説明があった。フォールトを以下の5つに分類するものとする。

- 物理フォールト
- 設計フォールト

- 悪意ある設計フォールト
- インタラクションフォールトイントルージョン（悪意あるインタラクションフォールト）

このうち、LAASの研究が網羅しているのは、物理フォールト、設計フォールト、イントルージョンの3種類である。これらのフォールトに対して、4つの方法論であるフォールト予防、フォールトトレランス、フォールト除去、フォールト予測を組み合わせ、ディペンダブルコンピューティングを実現している。

より具体的には、例えば、ポリシーやアクセス制御など、セキュリティの実現技術は、主にフォールト予防に属する。フォールトトレランス技術としては、ディペンダブルなシステムアーキテクチャの設計が挙げられる。また、フォールト除去に関しては、テスト技術が代表的な例である。ディペンダビリティに関するベンチマーク技術は、フォールト予測の代表例である。

ディペンダブルコンピューティングの実際の応用としては、ナノシステム、ロボティックス、自動車・列車、航空・宇宙、通信といった、非常に広範な分野を対象をしている。開発技術の実用例として、2重系におけるプライマリ、セカンダリコンピュータの情報の整合性を保持するためのプロトコルが、2005年よりニューヨーク地下鉄の一部路線で実際に運用されている。

他機関との共同プロジェクトも盛んであり、EU、および、フランス国内を中心に、10程度のプロジェクトを実施している。また、LAASと競合関係にある他の代表的な研究拠点として、アメリカ合衆国におけるイリノイ大学アーバナシャンペイン校、およびカーネギーメロン大学があげられた。

(b) State of Knowledge in Dependability Evaluation

次に、Karama Kanoun博士から、ディペンダビリティ評価に関する研究動向と成果について報告を受け、議論を行った。フォールトは、偶発的なものか悪意あるものかという、2種類に大別することができ、Kanoun博士との議論では偶発的な（accidental）フォールトに関する話題を中心として、その定量的評価について意見交換を行った。具体的には、ソフトウェアの信頼度成長のモデリング、確率モデルによるシステムアーキテクチャのディペンダビリティ評価、そして、フォールトインジェクションの3技術分野を対象に議論を進めた。

ソフトウェアは、設計フォールトの検出と修正を繰り返すことで、その信頼度が時間の経過とともに変化していく。ソフトウェア信頼度成長モデルとは、そのような信頼度の変化をモデル化することで、ソフトウェアシステムの信頼を推定するフォールト予測技術である。この技術分野に関しては、新しいモデルの提案、ソフトウェアアーキテクチャの構造を考慮したモデル化、また、システムの進化を観測することによる推定手法の開発等が、LAAS研究所の成果として挙げられる。そして、これらの手法の妥当性は、電話通信システム等の実際のソフトウェアの観測によって得られたデータによって裏付けられている。

確率モデルによるシステムアーキテクチャのディペンダビリティ評価では、マルコフモデルや、一般化確率ペトリネット等、確率事象を解析するための基本的なツールを基盤に、システムの複雑化に伴う記述の困難化や、考慮すべき状態数の爆発的増加を解決する手法を提案している。このような評価によって、システムのディペンダビリティが定量的に

評価できるばかりでなく、例えば、ディペンダビリティを最適化するような、障害と修復に対するシステムの運用ポリシーを決定することが可能となる。

確率モデルを構築する上で、フォールトの振る舞いが定量的に裏付けられていれば、正確なシステムディペンダビリティの評価が可能となる。フォールトインジェクションで得られるデータは、このような、上位のシステムレベルにおけるディペンダビリティ評価にとって、不可欠なものとなる。LAAS研究所では、論理レベルにおけるソフトウェアを用いたものと、ピンレベルのハードウェアレベルの両者について、フォールトインジェクションの研究を行っている。

これまでにディペンダビリティ評価を行った実システムは、原子炉の制御システムから、旅行代理業務用のウェブベースのアプリケーションに及ぶ。このようなモデリング・予測手法に対し、産業界から抵抗があるのではないかとの懸念に関しては、最初はそうであるが、実際にデータをフィードバックすることで、徐々に理解が得られるとのことであった。特に、航空産業を中心に、信頼性の分析用途に関して、ADL（architecture description language）から、上記の数学的なモデルへの転換が進んでいるとの回答があった。

（c）Dependability Evaluation of Critical Infrastructures：Modeling Interdependencies

Laprie博士からは、狭義のコンピュータシステムを離れて、電力網を例として、生活基盤における障害のモデル化、ディペンダビリティの評価について、研究説明があった。この研究では、特に、別々の事象の有機的な相互作用（inter-dependency）に注目している。具体的には、2003年米国での電力障害事故のように、別々のフォールトが相互作用しあうことで、システム全体が障害状態に陥るような場合である。このような現象に対しては未だに研究が不十分であり、その可能性を定量的に予測することは、社会的に重要であるといえる。

具体的な手法としては、インフラストラクチャの構成要素、電力網であれば、電力網自体と制御のための情報基盤、といった要素を抽出し、それぞれの動作をモデル化するとともに、異なる2要素間での、原因・結果の関係についてもモデル化する。これらのモデルを最終的に組み合わせることで、システム全体の動作を記述したモデルを得ることができる。

ディペンダビリティの定量的な評価は、各事象の生起率を推定し、モデルを一般化確率ペトリネットとして表現することで、可能となる。そのような生起率に関する値が得られるのかという疑問には、実際にデータが存在するということである。

（d）Evaluation of Security：Characterization of Attacks

Mohamed Kaaniche博士からは、悪意あるフォールト、特に、イントルージョンを対象に、システムのセキュリティを定量的に評価する技術に関して説明があった。具体的には、以下の二つの研究について議論した。まず一つは、システムのコンフィギュレーションが与えられた場合に、セキュリティの度合いを評価する研究である。ここで、セキュリティの度合いは、侵入者が目的を成し遂げるのに必要な平均的な困難度として定義される。この尺度を、METF（Mean-Effort to Security Failure）と名付けている。METFの値は、目的達成に至るシナリオをモデル化し、侵入

の各段階に必要な労力を重み付けすることで得られる。

次に、ハニーポットを用いて実際の攻撃のデータを収集し、分析した結果について説明があった。ハニーポットとは、そのようなデータを収集するためにネットワークに接続される、おとりのサーバである。この分析の結果、侵入が試みられるまでの平均間隔、攻撃者の地域、他のサーバへの攻撃の伝搬過程などに関する、貴重なデータが得られている。このような実証データは、イントルージョン対策への洞察を与えるだけでなく、上記のセキュリティの評価モデルに組み入れることで、評価の精緻化が可能となる。

(e) Dependability Benchmarking

次に、Karama Kanoun 博士から、DBench プロジェクトの研究成果について報告があった。これは、LAAS 研究所を中心とした、ディペンダビリティベンチマークに関するプロジェクトであり、ディペンダビリティベンチマークの枠組みの提案と、その枠組みに従ったディペンダビリティベンチマークのプロトタイプの開発が、その主な成果である。これらのプロトタイプは、以下のようなシステムを対象にしている。

- 汎用 OS
- 宇宙用のオンボードシステムにおける実時間カーネル
- エンジン制御
- オンライントランザクショ処理

報告では特に汎用 OS、具体的には、Windows および Linux ファミリーについて、データを交えて説明があった。ベンチマークの具体的な手法は、アプリケーションからの API の呼び出しを操作して、フォールトを注入し、不正な値を用いて API を呼び出す。これに対するシステムの反応を観測することで実現される。評価尺度としては、フォールト以後の OS の状態、フォールト発生から異常状態に至るまでの反応時間、リスタート時間等が用いられる。このように、ディペンダビリティには多くの様相が存在するので、様々な尺度を提供する必要がある点は、性能ベンチマークとの著しい違いである。

ディペンダビリティベンチマークは、性能に関する通常のベンチマークと違い、まだ企業には広く受け入れられているとはいえないが、ここ数年で状況は変化しつつあるという。また、自身でベンチマークを作りつつある企業もあるとのことである。普及を妨げている要因として、自社製品が低く評価されることや、情報を開示することで競争上不利になることへの恐れが考えられる。したがって、ベンチマークに対するインセンティブをどう生み出すかが、実用上の課題であるという認識に至った。

(f) Brief Presentations of Selected IST Projects

最後に、Laprie 博士、Kaaniche 博士から、現在進行中の幾つかのプロジェクトについて説明があった。Laprie 博士からは、ReSIST (Resilience for Survivability in IST) プロジェクトについて説明があった。このプロジェクトはユビキタスコンピューティングシステムにおけるディペンダビリティの実現を目指して、従来のディペンダブルコンピューティングの考えを、より広い対象に拡大することを基本的な枠組みとしたプロジェクトである。

また、Kaaniche 博士からは、CRUTIAL (Critical Utility Infrastructural resilience) プロジェクトと HIDENETS (Highly-

Dependable IP-based Networks and Services）プロジェクトについて説明を受けた。電力網とそれを制御する分散システムを対象に、モデル化手法と、アーキテクチャについて研究を行うものである。前述の、電力網を具体例とした生活基盤における障害のモデル化に関する研究は、このプロジェクトの一部である。また、後者のプロジェクトは、車々間通信を主アプリケーションとして、無線通信のディペンダビリティを達成することを目的としたプロジェクトである。

4.5 Airbus社との調査・討論

当初ツールーズ市にあるAirbus本社を訪問し、研究開発中の最新技術を見学する予定であったが、Airbus 社自体の都合により、LAASにAirbusの管理責任者、技術者を招いて研究・調査・討論会を開催することになった。Airbus社は航空機製造会社の大手であり、輸送機器制御におけるディペンダビリティ技術の応用について長年研究開発を行なっている。コーディネータのMichel Diaz博士（LAAS-CNRS）から今回の経緯について説明があり、南谷教授からJST-CRDSの基本情報や訪問の意図について説明を行った。引き続いて、Jean-Pierre Daniel 氏（ Airbus）、Patrick Ringeard氏（Airbus）、Luis Nobre氏（Airbus）によって、Airbus社において用いられているディペンダビリティ技術や他企業との協力研究プロジェクトについて紹介を受けた。

日時：10月24日 9：00-14：00
場所：LAAS-CNRS、7 av.du Colonel Roche, 31077 Toulouse Cedex, FRANCE

【スケジュール】
Meeting between the JST-CRDS Delegation and Airbus Representatives

9：00-9：15	Welcome Address Michel Diaz（LAAS-CNRS）
9：15-9：45	JST-CRDS Delegation：Introduction about the Mission Takashi Nanya（JST-CRDS）
9：45-10：30	A Process Towards Total Dependability-Airbus Fly-by-Wire Paradigm Jean-Pierre Daniel（Airbus）
10：30-10：45	Break
10：45-11：30	Introduction of IMA Impact on A/C System Safety Patrick Ringeard（Airbus）
11：30-11：50	JASTAC, SHM Research with Japan Luis Nobre（Airbus）
12：10-12：30	Further Discussion and Wrap-Up
12：30-14：00	Lunch
14：00	End of Meeting

【詳細説明】

(a) A Process Towards Total Dependability-Airbus Fly-by-Wire Paradigm

まず、Jean-Pierre Daniel 氏からフライ・バイ・ワイヤ(Fly-by-Wire)において、ディペンダビリティを達成するための、設計法について説明があった。フライ・バイ・ワイヤとは、操縦桿の動きを油圧作動機構等によって直接アクチュエータに伝えるのではなく、電気信号に変化して、コンピュータ等で必要な処理を行った上で、電気的に伝送する方式を指す。

説明では、まず、COMMON(command(control) + monitoring)と呼ばれる、基本的な制御装置の概念について説明があった。COMMON では、モニター側はセンサの値をモニターし、異常を検出すると COM 側の制御をカットすることで物理的なフォールトに対応し、安全性を保障する。システム及びコンピュータの設計では、航空産業分野で定められた DO 178 B 等の高い設計基準を満たすことで、事前に設計エラーの混入を最大限防いでいる。

フォールトトレランスを実現するためには、多重系を用いるが、同じ原因によって同時に複数の系が影響を受けるのを防ぐため、多重化された各モジュールは、物理的に異なる位置に配置するとともに、異なる種類の設計とすることを、基本的な方針としている。このような系を、dissimilar な冗長性と呼んでいる。これは、パイロットの振る舞い、すなわち、人的なフォールトにも当てはまり、複数段階のプロテクションを用意して対応している。上記の技術を用いて、危機的な状況が生じる確率が、1 時間の飛行で 10 の-9 乗以下になるように、設計が行われているとのことである。

(b) Introduction of IMA Impact on A/C System Safety

次に、Patrick Ringeard 氏から、IMA と ADCN について説明があった。これらはそれぞれ、Integrated Modular Avionics と、Avionics Data Communication Network の略である。ADCN は機内でデータ通信を提供するネットワークである。これは、インターネットの技術をベースに、障害検出等の機能も含め、航空機制御に必要な機能を実現したものとのことである。一方、IMA は、OS とハードウェアからなる計算ノードで、アプリケーションとは独立した汎用のモジュールである。機体には、100 程度のノードが存在し、ADCN に接続される。

このネットワークは、単一のフォールトで壊滅的な状況が引き起こされないように、その設計自体によって(by design)保障される。例えば、ネットワーク自体は、2 系統からなり、スイッチもそれぞれ別個のもの用いる。また、ADCN の障害でエンジンの制御ができなくなった場合は、ADCN でない経路でエンジンが制御できるように設計している。IMA の障害についても、同様に対処されており、例えば、降着装置のブレーキが IMA によって制御できない場合のために、IMA とは無関係の、非常ブレーキ装置が用意されている。これらの冗長化技術により、1 時間の飛行で 10 の-9 乗以下の障害確率が達成される。この信頼性の計算は、通常のフォールトツリー分析(FTA)を用いて行っているとのことである。

(c) JASTAC、SHM Research with Japan

Luis Nobre 氏からは、日本との共同プロジェクトである JASTAC(2006

年7月～)について説明を受けた。このプロジェクトは、複合材料(composite material)、特にカーボンファイバーを用いた材料を対象とした、モニタリング技術に関するものであり、このような技術を、SHM(Structural Health Monitoring)と称している。複合材料とは、複数の材料から構成され、元の材料より優れた特性を持つ材料を指し、金属からの転換が進んでいる。プロジェクトでは、生物が神経系によって痛みを感知するように、複合材料をモニターし、例え飛行中であっても、損傷・疲労の検出を可能にすることを目指している。既に、各種の損傷について、センサによる検出技術の開発が進行中とのことである。

(d) Further Discussion and Wrap-Up

最後に、Jean-Pierre Daniel氏からは、産学共同プロジェクトの例として、AIRSYSについて簡単な説明があった。これは、AIRBUSと、フランスの研究・教育機関であるONERA、LAAS、IRITとによる枠組みで、傘下で20プロジェクトが現在行われているとのことである。

4.6 全体の印象

今回の欧州調査では、まずコインブラ大学とCritical Software社によって精力的に行なわれているフォールトインジェクション技術の開発と、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い印象を受けた。EDCC-6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CSW以外にも、LAAS-CNRS、Technical University of Valencia、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、フォールトインジェクションも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との融合や経済価値へのマッピング手法などは、現状では明らかに存在していない。ディペンダビリティ評価に関する各要素技術を各々の研究者ならびに研究グループで独立に行なうことも自由な発想を養う上で必要ではあるが、我が国におけるディペンダビリティ評価研究の底上げを図り、広く評価適用対象領域を模索するためには、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、EDCCにおける活動とヒューマンネットワークからは、ディペンダビリティ研究の最高峰であるアメリカに匹敵するような高品質の研究成果を生み出すための努力が見受けられる。

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、フォールトインジェクション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との印象を受けた。

DBench プロジェクトでも LAAS はリーダー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、ツールーズが Airbus やコンコルドをはじめとする航空産業の中心地であることから、産業界との繋がりも深く、常に実システムへの適用可能性と評価を念頭に研究プロジェクトを実施しているものと考えられる。ディペンダビリティ技術という情報産業のほとんど全てに関連する基盤技術を国家レベルで育成し、継続的にその成果を期待するためには LAAS-CNRS における Dependable Computing and Fault Tolerance 研究グループ（約 30 名の研究スタッフ）規模の拠点を我が国にも形成する必要がある。また、LAAS では他の研究グループ（Power Integration and Devices Group、Microwave Integrated Devices and Systems for Telecommunications Group、Photonics Group、Nanoaddressing and Nanobiotechnologies Group、Technology、Micro and Nanostructures Group、Microsystems and Systems Integration Group、System Engineering and Integration Group、 Qualitative Diagnosis and Supervisory Control Group、Methods and Algorithms in Control Group、Modeling、 Optimization and Integrated Management of Activity Systems Group、Telecommunication Networks and Systems Group、 Robotics and Artificial Intelligence Group、Software and Tools for Communicating Systems Group の計 14 グループ）と共同で研究を行なっていることからも、組織内における研究成果のパフォーマンスが極めて高いことが特徴にもなっている。

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り、また、ディペンダビリティ計測と価値創成のための模索は未踏の問題である。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、今回の欧州調査を通しても依然として魅力的であり、我が国が当該分野で世界的なイニシアチブをとり、新しい情報技術に積極的に貢献してゆくためには最も適したテーマであるものと確信している。

5

EU-US Summit Series : Workshop on System Dependability & Security 参加報告

EU-US Summit Series : Workshop on System Dependability & Security 参加報告

5.1 経緯

ポルトガル・コインブラで開催されたEDCC（European Dependable Computing Conference）に参加した際、その場に出席していたEC（European Commission）の「ICT for Trust and Security」部門の副責任者であるDr. Thomas Skordasと生駒センター長、南谷シニアフェローが面談し、ファンディング・エージェンシーとしてのEC及びJSTの活動に関して情報交換を行い、今後もディペンダビリティの研究推進活動に関する情報交換を続け場合によっては両者の連携の可能性を探ることで合意した。

その際、標記の会議への出席を打診され、その招待を受諾した。

会議は、2006年11月15、16日にIrelandのDublinで開催され、南谷シニアフェローが出席した。

5.2 会議の性格

この会議はその名前のとおり、欧州のEC（European commission）と、米国のNSF（National Science Foundation）及びDHS（Department of Homeland Security）の共催で、欧州と米国からそれぞれ25名程度のトップ研究者を招き、ディペンダビリティとセキュリティの研究において将来重要となる優先分野に関して欧州と米国で認識を共有し、両者が連携した共同研究の可能性を育成することを目的としている。

標題の"Summit Series"とは、今回（2006年11月15、16日）のIreland、Dublinにおける第一回ワークショップの結果を受けて、引き続き第二回を2007年4月または5月に米国、イリノイ州Urbana-Champaignで開催する、ということを表している。

欧州と米国の間では、情報科学・情報技術の分野で、両者の連携を模索したこの種の会議が1998年頃から、毎年開催されており、今回は"Dependability & Security"の分野に絞った初めてのワークショップである。

5.3 会議の概要

会議出席者（招待）は、米国から25名、欧州から31名、カナダから1名、オーストラリアから1名、日本から1名である。その他に、ECから「ICT for Trust and Security」部門の責任者と副責任者を含む4名、NSFから1名、DHSから1名が参加した。

会議は2日間に渡って6つのパネル討論で構成され、各パネルは6人ずつがポジショントークを行った後でフロアを交えた討論を行った。6人のパネリストは、地域的に欧州から3名、米国から3名が選ばれ、分野的にも、Dependability分野から3名、Security分野から3名が選ばれる、というようにバランスに気を遣っているのが印象的であった。

今後、dependabilityとsecurityの特

に必要なアプリケーション分野としては、重要インフラ、電子商取引、電子政府、電子投票、将来のインターネット、スケーラブルシステム、ユビキタス／パーベイシブコンピューティングなどが挙げられていた。

プログラムの構成は以下のとおり：

Day One

Welcome、Workshop objectives and format
(EU representative - Willie Donnelly
US representative - Bill Sanders)

Keynote speakers：Setting the scene for the Workshop
Representative from the European Commission（Thomas Skordas）
Representative from NSF（Karl Levitt）
Representative from DHS（Doug Maughan）

Panel A：Dependability & Security of Future Networked Systems
- architecture and design issues
Co-Chairs：David Du（NSF、US）& Paulo Verissimo（Univ. Lisboa、Portugal）
Rapporteur：Jim Clarke
Speakers：
Ravishankar Iyer（Univ. Of Illinois, US）
Michel Riguidel（ENST, France）
Felix Wu（UC Davis, US）
Bart Preneel（Katholieke Univertsiteit Leuven, Belgium）
Yair Amir（JHU, US）
Neeraj Suri（TU Darmstadt, Germany）

Panel B：Dependability & Security of Future Networked Systems
- scalability and context-awareness
Co-Chairs：John Knight（Univ. Virginia, US）& Brian Randell（Univ. Newcastle upon Tyne, UK）
Rapporteur：Jim Clarke and John Knight
Speakers：
Jean-Claude Laprie（LAAS, France）
Nick Weaver（Berkeley, US）
Christof Fetzer（TU Dresden, Germany）
George Kesidis（Penn. State, US）
Gerard LeLann（INRIA, France）
Ming-Yuh Huang（Boeing, US）

Panel C：- Security & Privacy in Dynamic Wireless Networks
Co-Chairs：Gene Tsudik pdf（UC Irvine, US）& Roberto Baldoni,（U. Roma, Italy）
Rapporteur：Michael Bailey
Speakers：
David Kotz（Dartmouth, US）
Reijo Savola（VTT, Finland）
Joe Evans（KU,US）
Stephan Engberg（Priway, Denmark）
Wenke Lee（Georgia Inst. Of Technology, Atlanta, US）
Paddy Nixon（UCD, Ireland）

Australian perspective in securing future communication networks（Ed Dawson）

Japanese perspective in future networked dependable systems（Takashi Nanya）

Day Two

Panel D：Evaluating the Dependability & Security of Networked Systems – modeling, simulation, predictive evaluation, assurance cases
Co-Chairs：William H. Sanders（Univ. of Illinois, US）& Dieter Gollmann（TU Hamburh-Harburg, Germany）
Rapporteur：Stephan Engberg
Speakers：
John Rushby（SRI International, California, US）
Bev Littlewood（City University, UK）
John McHugh（DAL, Canada）
Aad van Moorsel（Newcastle, UK）
O. Sami Saydjari（Cyber Defense Agency, LLC, US）
Robin Bloomfield（City Univ. + Adelard, UK）

Panel E：Evaluating the Dependability & Security of Networked Systems – monitoring, operational assessment, auditing
Co-Chairs：David M. Nicol（Univ. of Illinois, US）& Marcelo Masera（JRC, Italy）
Rapporteur：Jim Just
Speakers：
Roy Maxion（CMU. US）
Evangelos Markatos,（FORTH-Creta, Greece）

Alfonso Valdes (SRI, US)
Fabio Martinelli (IIT-CNR, Italy)
Todd Heberlein (NetSQ, US)
Andras Pataricza (Univ. of Budapest, Hungary)

Panel F：Future Test beds
Co-Chairs：Doug Maughan (DHS, US) & Jim Clarke (Waterford Institute of Technology, Ireland)
Rapporteur：Zeta Dooly
Speakers：
Mike Bailey (Univ. of Michigan, US)
Pekka Nikander (Ericsson NomadicLab, Finland), Mikko Sarela (Helsinki Univ. of Tech)
Anthony Joseph (Berkeley, US)
Jim Just (Global Info Tek, US)
Henrique Madeira (Univ. of Coimbra, Portugal)

5.4 所見

DependabilityとSecurityに関する重要課題を抽出してEUとUSの間で優先分野に関する共通認識を持つ、ということが会議の目的だとされたが、6つのパネルでは、それぞれ6名のパネリストが自分の研究分野に関するそれぞれの持論を述べただけで、パネルとしても、また会議全体としても特別な結論はなかった。唯一の結論らしきものは6番目のパネルのタイトルともなっていたテストベッドで、EUとUSの間の共同プロジェクトの可能性の一つとして大規模テストベッドを構築する提案があった。しかし、具体的な姿はまだ明らかではない。共同で重要分野を抽出することに関して、主催者(EC, NSF, DHS)と参加者との間にかなりの意識のギャップがあり、EUとUSが共同でできることは何もない、という意見もあった。

最近、日本を無視してEUとUSで話を進めていく、いわゆる"Japan passing"とも思える場面があちこち生じていると言われるが、今回のこの会議もそのようになる可能性があった。しかし、今回、日本とオーストラリアも参加して一定の存在感を示し得たため、今後、EU-USからさらにInternationalに広げていくべきだ、との機運が出てきた。このことは、今後の評価技術の国際標準化への動きを考えると、大きな収穫であると考えられる。

6

米国拠点の調査結果

米国拠点の調査結果

6.1 イリノイ大学

イリノイ大学アーバナ：シャンペーン校（University of Illinois, Urbana-Champaign）は計算機科学、電子情報工学の分野で全米のトップ10に入る有力校であり、とりわけディペンダブルコンピューティングの分野では世界をリードしている。この分野でCenter of Excellenceを形成しているのが同大学の二つの研究所、すなわち、Coordinate Science Laboratory（CSL）とInformation Trust Institute（ITI）であり、専任の研究者に加えてDepartment of Computer Science（CS）、Department of Electrical and Computer Engineering（ECE）の多くの教授がこの二つのどちらかあるいは両方を兼務している。今回の調査は、このCSLとITIを訪問し、朝8時30分から夕方6：00まで、working breakfast, working lunchを含めて、15名の中心研究者との個別面談によって実施した。

訪問日時：2006年12月15日
8：30 - 18：00

面談者：Prof. Ravishankar Iyer
（Director of CSL）
Prof. William H. Sanders
（Director of IHI）
Prof. Dick Blahut
（Head of ECE）
Prof. Marc Snir
（Head of CS）
Prof. Molly Tracy
（Vice Director of ITI）
Prof. Nikita Borisov
Prof. Klara Nahrstedt
Prof. Naresh Shanbhag
Prof. Elyse Rosenbaum
Prof. Himanshu Khurana
Prof. Roy Campbell
Prof. David Nicol
Prof. Grigore Rosu
Prof. Zbigniew Kalbarczyk
Prof. Steve Lumetta

Information Trust Institute（ITI）は情報システムのディペンダビリティとセキュリティに関する基礎研究、応用研究、教育を行う米国の拠点の地位を築きつつある。所長のProf. William H. Sandersは5で述べたEU-US Summit Series： Workshop on System Dependability & Securityにおける米国側の代表を務めている。80名以上の教授とシニア研究者、および多数の大学院生、企業研究員がこのITIに集結し、主として3つのテーマ領域に分かれて研究を行っている：

1）Critical Infrastructure & Homeland Security

現代社会は、エネルギー網、交通網、通信網、金融網などのように相互に依存した多数の重要インフラが継続してなく機能することに依存している。これらの重要インフラはそれを支える情報システムが正常に機能することに依存している。これらのインフラに偶然あるいは意図的に障害が引き起こされるとその社会的影響は計り知れない。従って、この

ような重要インフラに対する脅威を軽減あるいは除去する研究を進めている。

2）Embedded & Enterprise Computing

豊かで快適な日常生活は、安全で信頼できる電力網、交通網、通信網、医療装置に依存するが、これらはいずれも組み込みシステムを土台にして構築されている。また、政府機能、ビジネスなどは、企業システムの上に実現される情報検索、トランザクション処理、データマイニングなどに依存している。このように社会と人間が依存する組み込みシステムと企業システムのディペンダビリティ、セキュリティを総合的かつ統一的に研究を進めている。

3）Multimedia and Distributed Systems

自動車から健康管理まで、マルチメディア分散システムは日常生活に浸透しているが、その信頼性、安全性の確保が要求される。これまでは軍用の重要インフラなどのように閉じたシステムに限られていた技術は家庭、学校、病院、消防署、警察などの情報環境に拡大されてきており、そこではマルチメディア分散システムが重要な役割を果たす。

これらの研究領域が、現在、以下の7つの研究センター（プロジェクト）において、それぞれの目的に従って展開されている。

1）Boeing Trusted Software Center

ボーイング社とイリノイ大学との共同研究センターであり、長期的な視野で、ネットワーク、組み込みシステム、ワイヤレスセンサーシステム、分散システムのソフトウェアディペンダビリティに関する広範囲の総合的な研究を進めている。

2）CAESAR：the Center for Autonomous Engineering Systems and Robotics

自律システム、マルチエージェントシステム、ロボティクスのディペンダビリティ、セキュリティを基礎から応用まで研究している。特に人間とロボットの相互作用、遠隔操作、ロボットによる建設作業などの信頼性、安全性に重点を置いている。

3）Center for information Forensics

大量情報の分析、パターン解析、システム侵入、化学・生物学汚染、情報の不正改竄など、情報システムに関わる犯罪の分析、対策技術、法制度などを広範囲に研究している。研究者の専門分野は、パターン認識、機械学習、データマイニング、統計学、ゲーム理論、暗号、情報理論、ネットワーク、信号解析、言語解析、ソフトウェア工学、化学、生物学、心理学など多様で広範囲である。

4）NCASSR：National Center for Advanced Secure Systems Research

イリノイ大学のDept. of Computer Science、海軍のPacific Northwest National Laboratory, Naval Postgraduate School, Naval Research Laboratoryの研究グループが連携して、サイバーインフラのディペンダビリティとセキュリティに関する諸問題を扱う。海軍研究所（Office of Naval Research ）の出資で、イリノイ大学のスーパーコンピュータ応用センター（NCSA）が運営している。

5）NSA Center for Information Assurance Education

1998年5月に出された重要インフラ防衛に関する国家政策（Presidential Decision Directive 63）に基づいて、国家安全保障局（National Security Agency）が国全体で開始した情報安全教育（Information Assurance Education）プログラムの実施拠点のひとつとしてイリノイ大学に設置された。修士、博士課程、社会人教育などを提供している。

6）TCIP：Trustworthy Cyber Infrastructure for Power Center

イリノイ大学、コーネル大学、ダートマス大学、ワシントン州立大学の連携による電力網のサーバーインフラのディペンダビリティとセキュリティの確保を目的とする研究プロジェクトである。我々の生活と社会が全面的に依存する全国的な電力供給網のディペンダビリティとセキュリティを確保するために、2005年8月に発足した。NSF（National Science Foundation）が5年間に渡って$7.5 Millionの資金を提供している。また,Department of Energyと Department of Homeland Securityが、NSFに連携して資金を提供する約束をしている。

7）Trusted ILLIAC

いわゆる"On-demand/utility computing"あるいは"Adaptive enterprise computing"の実現を支援するためのディペンダブルでセキュアな計算機クラスタ・プラットフォームを構築することを目的として、偶発的なフォールトと悪意の攻撃に対処するシステムアーキテクチャとデザインの研究を行っている。IBMやSunmicrosystemsなどとディペンダビリティ評価で連携研究を行っている。

イリノイ大学ITIが中核メンバとして参加するI3P（Institute of information Infrastructure Protection）は、全米の情報インフラに対する脅威を同定し緩和する専門家の集まるコンソーシアムであり、大学、国立研究所、NPOなどが参加して、情報インフラの脆弱性を克服する研究と関連する政策提言を行う全米にバーチャルラボラトリとして機能している。事務局はダートマス大学が担当している。

このI3Pが昨年、ディペンダビリティとセキュリティの評価指標を定めること（Metrics）は困難であるが、経済活動にとっても社会の安全にとっても必須であるとして、次の4つのグランドチャレンジを提言している。

チャレンジ1：適切なセキュリティ・メトリクスを定義する
チャレンジ2：メトリクスを評価する方法を定める
チャレンジ3：異なる階層（組織、システム、構成要素）のメトリクスを総合する
チャレンジ4：設計、更新、運用段階でのメトリクス測定ツールを開発する

全体を総括すると、イリノイ大学のITIはディペンダビリティ・セキュリティ技術の基礎から応用まで社会のニーズと密接に連携した研究を多面的な角度から行う米国の中核研究拠点である。情報社会における国の重要インフラから基幹システム、組み込みシステムまで、産官学が密接に連携して研究を進めるのみならず、長

期的視野を持って人材育成に力を注いでいる点は特に注目に値する。

6.2 PRDC 2006参加報告

会議概要

2006年12月18-20日に、米国カリフォルニア大学リバーサイド校(University of California at Riverside)で環太平洋ディペンダブルコンピューティング国際会議(The 12 th IEEE Pacific Rim International Symposium on Dependable Computing)が開催された。IEEE Computer Society, Technical Committee on Dependable Computing and Fault Tolerance とIFIP WG 10.4"Dependable Computing and Fault Tolerance"の共催である。1991年に日本の川崎市で第1回が開催されてから16年目に当たる今回の開催がまだ12回目である理由は、当初は隔年開催としてスタートしたものが、途中から技術の進歩に合わせて毎年開催に切り替えられたことによる。「環太平洋」の名前に拘わらず、ヨーロッパからの参加者も多い。

この会議の実行委員長はProf. Daniel Jeske(Univ. California, Riverside, USA)、プログラム共同委員長は、Prof. Gianfranco Ciardo(Univ. California, Riverside, USA)、Prof. Yuanshun Dai(Purdue University, USA)であり、名誉委員長としてディペンダビリティ評価の研究で著名なProf. Kisor S. Trivedi(Duke University, USA)を迎えて開催された。

会議プログラムは、117件の投稿論文の中から、厳しい査読を経て採択された41件のレギュラー論文と16件のショート論文、および3件の基調講演で構成され、3日間毎日、最初に1時間の基調講演でその日のセッションの幕を開けた会議の参加者は70名であった。

発表論文は、信頼性モデリングと評価、ソフトウェアの誤り検出とテスト、分散システム、セキュリティ、アベイラビリティ評価、侵入検出、ネットワークプロトコル、ディペンダブルシステムのアーキテクチャと最適化、システムリカバリとメンテナンスなど、多岐に渡る。一方、残念ながら、今回の主たる調査対象とした人間要素を含む情報システムのディペンダビリティや評価メトリクスに関連する話題に見るべきものはなかった。

次回は2007年12月にオーストラリア・メルボルンで開催される。

Detailed Program

Dec. 18 (Mon.) Opening session 8 : 30 - 9 : 00

Keynote Speech Prof. Way Kuo EGN II 138 9 : 00 - 10 : 00

Title : Quality Wave in Light of The Nano Development
Abstract : Nano technologies are a driving force for strong economic growth in the world, and some analysts predict that its impact will bring to us the next industrial revolution. In the 2005 National Academy's publication of Keck Futures Initiative, reliability is cited as the key element of the success of nano fabrication and manufacturing. In this keynote speech, we will address both the historical review of the nano technologies ever since the industrial revolution and recent development, particularly those events which have great impacts on quality and computing. Some new challenges will be discussed as well.

Coffee Break 10 : 00 - 10 : 30

Session 1 : Reliability Modeling	ENG II 138 Dec.	18(Monday)10:30-12:30
PRDC-109	Two-Dimensional Software Reliability Models and Their Application	Tadashi Dohi
PRDC-133	A Strategy for Verification of Decomposable SCR Models	Dejan Desovski Bojan Cukic
PRDC-155	Detection and Correction Process Modeling Considering the Time Dependency	Yanping Wu
PRDC-159	DETECTING AND EXPLOITING SYMMETRY IN DISCRETE-STATE MARKOV MODELS	Michael McQuinn William Sanders Doug Obal

Session 2 : Fault Detection	ENG II 143 Dec. 18 (Monday) 10 : 30 - 12 : 30	
PRDC-124	An Evaluation of Similarity Coefficients for Software Fault Localization	Rui Abreu Peter Zoeteweij Arjan J.C. van Gemund
PRDC-125	SEVA : a Soft-Error- and Variation-Aware Cache Architecture	Luong Dinh Hung Masahiro Goshima Shuichi Sakai
PRDC-216	An Operating-System-Level Framework for Providing Application-Aware Reliability	Zbigniew Kalbarcyzk Long Wang Weining Gu Ravishankar Iyer
PRDC-149	Minimal System Conditions to Implement Unreliable Failure Detectors	Antonio Fernández Ernesto Jiménez

Sergio Arévalo

Luncheon 12：30-1：30

Session 3： Software Test	ENG II 138	Dec. 18 (Monday) 1：30 - 3：30	
PRDC-106	A New Approach to Improving the Test Effectiveness		Shiyi Xu
PRDC-120	A Framework for Inheritance Testing from VDM++ Specifications		Aamer Nadeem Michael Lyu
PRDC-156	Assessment on Undetectable Burst Errors in Tandem CRCs		Meng-Lai Yin Bruce Orenstein
PRDC-163	Efficient Built-In Self-Test Schemes for Video Coding Cores： a Case Study on DCT/IDCT Circuits		Shyue-Kung Lu

Session 4： Security	ENG II 143	Dec. 18 (Monday) 1：30 - 3：30	
PRDC-134	Flexible, Cost-Effective Membership Agreement in Synchronous Systems Raul Barbosa Johan Karlsson		Raul Barbosa Johan Karlsson
PRDC-177	Towards Adaptive Secure Group Communication：Bridging the Gap between Formal Specification and Network Simulation		Sebastian Gutierrez-Nolasco
PRDC-187	Quantum oblivious transfer and Fair Digital Transactions		Yao-Hsin Chou Sy-Yen Kuo I-Ming Tsai Chien-Ming Ko
PRDC-207	Storing RSA Private Keys In Your Head James Diamond		Jeff Hooper Taisya Krivoruchko

Coffee Break 3：30 - 4：00

Session 5： Availability	ENG II 138	Dec. 18 (Monday) 4：00-5： 30	
PRDC-108	Database Transaction Management for High-Availability Cluster System		Ken-ichiro Fujiyama Nobutatsu akamura Ryuichi Hiraike
PRDC-139	Restoration Strategies in Mesh Optical Networks： Cost vs. Service Availability		Ashwin Sampath Daniel Jeske
PRDC-161	Modeling High Availability Systems		Ranjith Vasireddy David Trindade Rick Castro Kishor Trivedi swami Nathan

Session 6： Intrusion Detection	ENG II 143	Dec. 18 (Monday) 4：00-5：30	
PRDC-121	Base Address Recognition with Data Flow Tracking for Injection Attack Detection		Satoshi Katsunuma Hiroyuki Kurita Ryota Shioya Kazuto Shimizu

		Hidetsugu Irie Masahiro Goshima Shuichi Sakai
PRDC-186	STARS：Stateful Threat-Aware Removal System for Self-healing Spyware	Ming-Wei Wu Yennun Huang Yi-Min Wang Sy-Yen Kuo

Dec. 19 (Tue.) Breakfast / Coffee 8：30 - 9：00

Keynote Speech Professor Takashi Nanya EGN II 138 9：00 - 10：00

Title："Challenges in Dependability of Future Networked Systems"
Abstract：As networked systems pervade every aspect of the modern information society, we are faced with serious threats to dependability due to problems caused by accidental events such as human mistakes and physical malfunctions or by intentional behavior being either malicious or non-malicious. In this talk, we discuss major challenges and give views of future directions in research on the dependability of evolving networked systems toward an advanced information society.

Session 7：Reliability Prediction & Optimization ENGII 138 Dec. 19 (Tue.) 10：00 - 12：00

PRDC-130	A Best Practice Guide to Resource Forecasting for the Apache Webserver Guenther Hoffmann	Miroslaw Malek Kishor Trivedi
PRDC-141	Software Reliability Prediction and Assessment Using both Finite and Infinite Server Queuing Approaches	Chin-Yu Huang Wei-Chih Huang
PRDC-146	On Statistically Estimated Optimistic Delivery in Wide-Area Total Order Protocols	Jose Mocito Ana Respicio Luis Rodrigues
PRDC-158	Early Software Reliability Prediction with Extended ANN Model	Qingpei Hu Min Xie Szu Hui Ng

Session 8：Dependability Applications ENG II 143 Dec. 19 (Tue.) 10：00 - 12：00

PRDC-148	A Dependable Outbound Bandwidth Based Approach for Peer to Peer Media Streaming	Sheng-De Wang Zheng-Yi Huang
PRDC-151	A Pragmatic Protocol for Database Replication in Interconnected Clusters	Jon Grov Fernando Pedone Luis Soares Alfranio Correia Junior José Orlando Pereira Rui Carlos Oliveira
PRDC-157	An efficient commit protocol exploiting primary-backup placement in a distributed storage system	Xiangyong Ouyang Tomohiro Yoshihara Haruo Yokota

PRDC-164	Reliable Video Transmission Techniques for Wireless MPEG-4 Streaming Systems	Sheng-Tzong Cheng

Luncheon 12：00-1：00

Session 9：Survivability	ENG II 138	Dec. 19(Tue.)1：00-2：30
PRDC-122	On the fly estimation of the processes that are alive/crashed in an asynchronous message-passing system	Michel Raynal Achour Mostefaoui Gilles Tredan
PRDC-129	Synchronous Set Agreement：a Concise Guided Tour (including a new algorithm and a list of open problems)	Michel Raynal Corentin Travers
PRDC-171	Dependable Multithreaded Processing Using Runtime Validation	Kaiyu Chen Sharad Malik
PRDC-173	Improving Fast Paxos：being optimistic with no overhead	Andre Schiper Bernadette Charron-Bost
PRDC-191	Fault-Tolerant Partitioning Scheduling Algorithms in Real-Time Multiprocessor Systems	Hakem Beitollahi Geert Deconinck
PRDC-126	Resource Availability Optimization for Priority Classes in a Website	Vasilis Koutras Agapios Platis

Coffee Break 2：30 - 3：00

Short Paper Track 1	ENG II 138	Dec. 19(tue.)3：00-5：00
PRDC-110	Evaluating the Impact of Fault Recovery on Superscalar Processor Performance	Toshinori Sato Akihiro Chiyonobu
PRDC-115	A Scenario of Tolerating Interaction Faults Between Otherwise Correct Systems	Bogdan Nassu Takashi Nanya
PRDC-119	Detection and Recovery for Disconnection Failures in a Web-based Medical Teleconsultation System	Chih-Hsun Chou Kuo-Feng Ssu Wei-Te Shih Pau-Choo Chung
PRDC-123	Leader Election in the Timed Finite Average Response Time Model	Martin Suessikraut Christof Fetzer
PRDC-127	A Replication Model for Trading Data Integrity against Availability	Johannes Osrael Lorenz Froihofer Karl M. Goeschka
PRDC-128	Improving Data Transmission with Helping Nodes for Geographical Ad Hoc Routing	Shin-Hung Chung Kuo-Feng Ssu
PRDC-153	Towards Timely ACID Transactions in DBMS	Marco Vieira António Costa Henrique Madeira
PRDC-154	Monitoring Database Application Behavior for Intrusion	José Fonseca

	Detection	Henrique Madeira Marco Vieira

Short Paper Track 2	ENG II 143	Dec. 19 (Tue.) 3 : 00 - 5 : 00
PRDC-160	Implementation Results of a Configurable Membership Service for Active Safety Systems	Carl Bergenhem Johan Karlsson
PRDC-175	Ontology based IT-security planning	Stefan Fenz Edgar Weippl
PRDC-180	The Hierarchy of BGP Convergence on the Self-Organized Internet	Jinjing Zhao Peidong Zhu Xicheng Lu Feng Zhao
PRDC-190	Dynamic Policy Decision for Reconfigurable Coded-WDM PONs	chuan-ching sue
PRDC-192	Fault-Tolerant Rate-Monotonic Scheduling Algorithm in Uniprocessor	Hakem Beitollahi Geert Deconinck
PRDC-198	The Survivability of the Augmented Logical Ring Topology in WDM Networks	Yung-chiao Chen chuan-ching sue Sy-Yen Kuo
PRDC-203	A Hybrid Multipath Routing in Mobile ad hoc Networks	chuan-ching sue
PRDC-211	A Generic Trust Overlay Simulator for P 2 P Networks	wang wei

Dec. 20 (Wed.) Breakfast / Coffee 8 : 30 - 9 : 00

Keynote Speech Professor Michael R. Lyu EGN II 138 9 : 00 - 10 : 00

TITLE - Code Coverage : The Missing Link Between Software Testing and Software Reliability?

ABSTRACT - While hardware testing and reliability techniques are closely related, software testing and reliability approaches were developed independently, sometimes with conflicting principles. Software testers spend their most testing efforts in exceptional test cases, while software reliability engineers require software to be tested under a normal operational profile. Software testers are interested in knowing how software testing covers the development requirements. Software reliability engineers are interested in how software reliability is perceived from customer views. Software testers do not trust numbers. Software reliability engineers insist software quality cannot be an objective attribute without creditable reliability measures.

The main issues in software testing are the design and evaluation of effective test cases, and relating software testing with the resulting reliability. Code coverage was proposed as an estimator for testing effectiveness, But it remains a controversial metric in linking testing with reliability. In this talk, we focus our research questions regarding the measure of code coverage on testing effectiveness under various testing strategies, and evaluate the influence of code coverage to software reliability measurement. We conduct experiments to investigate the relationship between code coverage and fault detection capability under different testing profiles. From our experimental data, code coverage is merely a moderate indicator for fault detection regarding the overall testing strategies examined

on the whole test set. However, it is clearly a good fault detection estimator with exceptional test cases. Moreover, we analyze the effects of different coverage metrics and how coverage can be used to in reliability measurement, and establish a new reliability model incorporating both testing time and code coverage. New research directions in software testing and reliability will also be given.

Session 11：Maintenance and Recovery ENG II 138		Dec. 20 (Wed.) 10：00 - 11：30
PRDC-143	Design Tradeoff and Deadlock Prevention in Transient Fault-Tolerant SMT Processors	Xiaobin Li Jean-Luc Gaudiot
PRDC-144	Incorporating Network Connectivity Analysis in Maintenance Planning	Meng-Lai Yin Rafael Arellano
PRDC-212	Low-Overhead Run-Time Memory Leak Detection and Recovery	Timothy Tsai Kalyan Vaidyanathan Kenny Gross
PRDC-193	End-to-end consensus using end-to-end channels	Matthias Wiesmann
PRDC-213	Performance and Reliability Analysis of Web Server Software Architectures	Swapna Gokhale Paul Vandal Jijun Lu
PRDC-140	A Single-Chip Fail-Safe Microprocessor with Memory Data Comparison Feature	Kotaro Shimamura Takeshi Takehara Yosuke Shima Kunihiko Tsunedomi

7

まとめ

まとめ

今回の調査の結果得られた主な所見は以下の通りである。

1）システムのモデリング解析、フォールトインジェクションによるシミュレーションなど、ディペンダビリティ評価の基礎的研究は欧米で進んでいるが、実システムの評価に結びついていない。原因はシステムの複雑さと規模の大きさにあるが、この状況は今後さらに深刻になるため、その克服にはブレークスルーが必要である。また、別の原因として、ディペンダビリティの経済価値が十分認識されない状況で、メーカーもユーザも評価技術の基礎となる実システムのフォールトや障害に関するデータを公表してこなかったことが挙げられる。

2）一方で、フォールトインジェクション・ツールを提供して組み込みソフトウェアの評価を行うポルトガルのベンチャー企業（Critical Software社）が世界の宇宙開発関連の政府機関・企業との取引で急成長している。各国の顧客に加えて、米国のNASAや我が国のJAXAもその顧客である。ソフトウェアの信頼性・頑健性を評価する商用ツールが他に見あたらないことが同社の急成長を支えていると思われる。

3）ディペンダビリティ・ベンチマークのプロジェクトが2002年から2004年まで、フランス、ポルトガル、イタリア、スウェーデンを中心とするEUプロジェクト（FP 6）として3年間実施されたが、対象がOSなどの一部のシステムに限られ、また人為フォールトに対する考慮が十分ではないなど、国際コミュニティでも成果があったとは見なされていない。ベンチマーキングは今後の課題である。

4）情報システムのディペンダビリティだけではなく、情報システムを活用した重要インフラ（電力・エネルギー網、情報通信網、輸送網、金融網、政府中枢など）のディペンダビリティ・セキュリティ確立が社会の安全保障に欠かせないとの認識から、広域電力制御の依存性解析のプロジェクトがEC（欧州）とNSF（米国）のファンディングで実施されている。欧州はLAAS/CNRSが拠点、米国ではUniv. Illinoisが中心になり電力会社とコンソーシアムを形成している。

5）米国ではI3P（Institute for Information Infrastructure Protection）が、ディペンダビリティとセキュリティの評価指標を定めること（Metrics）が、経済活動にとっても社会の安全にとっても必須であるとして、次の4つのグランドチャレンジを提言している。

チャレンジ1：適切なセキュリティ・メトリクスを定義する

チャレンジ2：メトリクスを評価する方法を定める

チャレンジ3：異なる階層（組織、システム、構成要素）のメトリクスを総合する

チャレンジ4：設計、更新、運用

段階でのメトリクス測定ツールを開発する

6）欧・米ともに経済価値へのマッピングの視点はまだ十分認識されていない。ユーザ視点の評価指標、評価手法も未開発である。しかし、多くの面談者が評価メトリクスから経済価値へマッピングの重要性に賛同している。

7）欧州（EC）と米国（NSF，DHS）のファンディング組織が連携した共同研究へ向けての動きが始まっているが、そこでも、ディペンダビリティ／セキュリティの評価技術が将来 EU と US で優先的に投資すべき重要分野に一つとして挙げられている。

以上の所見から、戦略プロポーザル創案にあたっては、以下のような視点からの提言を行うことが望ましい。

1）欧米に比較してディペンダビリティ／セキュリティ分野の研究者が少ない我が国では、個別の研究者に資金をばらまくのではなく、ディペンダビリティ/セキュリティ研究拠点を設置してアプリケーション（社会インフラも含む）研究者を巻き込んだ戦略的な研究推進が必要である。

2）国の安全保障の観点から、国の重要インフラ（電力・エネルギー、情報通信、輸送、金融、政府機関）を含めた我が国のネットワーク全体の依存性解析調査を早急に実施し、ディペンダビリティ／セキュリティの国家的長期戦略を構築する必要がある。

3）ディペンダビリティ／セキュリティを主たる目標とする技術開発を促進するためには、そのためのインセンティブの存在が重要であり、ユーザ視点からのディペンダビリティ／セキュリティ評価指標の開発、およびそれに基づいた経済価値へのマッピングとその可視化が必要である。

4）欧州と米国の連携、共同研究、テストベッド構築、国際標準化への動きに積極的に関与し、グローバルな価値指標構築へ向けた我が国からの働きかけが必要である。そのために、欧州、米国のファンディング当局と連携する我が国の窓口を早急に整備する必要がある。

G-TeC 報告書
「情報システムのディペンダビリティ評価」
国際技術力比較（欧州、米国）

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