CRDS-FY2006-SP-07

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

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―

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

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の推進を提案する。

Executive Summary

この戦略イニシアティブは、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、「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の推進を提言するものである。ここでいう「ニュー・ディペンダビリティ」とは、これまで研究されてきたディペンダビリティとセキュリティの技術分野を融合し、かつ社会システムとの関わりまでを考慮の対象に含めた概念である。「ニュー・ディペンダビリティ」は情報技術が常に目指すべき普遍的な目標理念である。

現在の社会は高度に発達した情報システムに依存しており、その依存度が今後さらに一層高まることに疑問の余地はない。したがって、その情報システムが提供するサービスは良質で信頼でき、人の生活と社会の活動が安心してそれに依拠できるものでなければならない。また、そこで扱われる情報は正確で一貫性があり、その機密性が規定通りに守られる必要がある。従来これらの研究には、ディペンダブルコンピューティングの研究と情報セキュリティの研究の二つの流れがあったが、両者には共通する技術分野も多く、真に安心・安全な社会を実現するためには両者を融合した技術体系を確立する必要がある。またこの分野は社会との関わりが極めて強いので、単に技術的側面のみを追求するのではなく社会システムまでを含めた広い視野で考えるべきである。

情報システムの満たすべき要件は、「ニュー・ディペンダビリティ」、Figure of Merit（単位消費エネルギーあたりの性能)、コストの３つに集約される。これまでの情報システムは主として Figure of Merit／コストを追求してきた。しかし半導体は物理的微細化の限界に近づき、ソフトウェアは人間の能力を超えるまでに複雑・大規模化し、さらに情報の正確性、一貫性、機密性を保証することはこれまでになく困難になっている。このような状況を考えると、今後も Figure of Merit／コストの追求を継続する必要性は変わらないものの、「ニュー・ディペンダビリティ」／コストをより重視する方向にシフトすることが必要な時期に差し掛かっていると言えよう。またこのことは新しい付加価値と市場を生み、産業競争力の強化にもつながるものである。このような見地から、本戦略イニシアティブは新しい概念として「ニュー・ディペンダビリティ」を定義し、その分野融合的な推進を提唱するものである。

本戦略イニシアティブにおいては、「ニュー・ディペンダビリティ」のモデリングおよび評価手法、実現するための技術、および制度設計について、具体的な研究課題と推進方法を提案する。

なお「ニュー・ディペンダビリティ」については極めて広範囲な検討が必要であるので、本戦略イニシアティブを起点として、今後技術分野ごとにより具体的な提言をするためのいくつかの戦略プロポーザルの発行を予定している。

Contents

1

情報化社会の安全と信頼を担保する情報技術体系とは

1.1 ニュー・ディペンダビリティの定義

情報化社会は人間と社会に有益なサービスを提供する情報システムをその存立基盤として発展する。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ならば、この情報システムはディペンダブル (dependable) である、という。ディペンダビリティの概念は1980年頃からフォールトトレラントコンピューティングの研究コミュニティが主体となって研究され、より広い概念として発展してきた。最近、情報セキュリティ分野とも融合した広い視野でこれを捉えようという動きが見られ、両分野の専門家による概念の拡張と深化が期待されている（P.11のコラム1参照)。さらに近年情報技術と社会システムが密接不可分になりつつあることを考慮すれば、経済・法律・政治なども視野に入れたより一層広い視野で考えることが今後とるべき方向である。

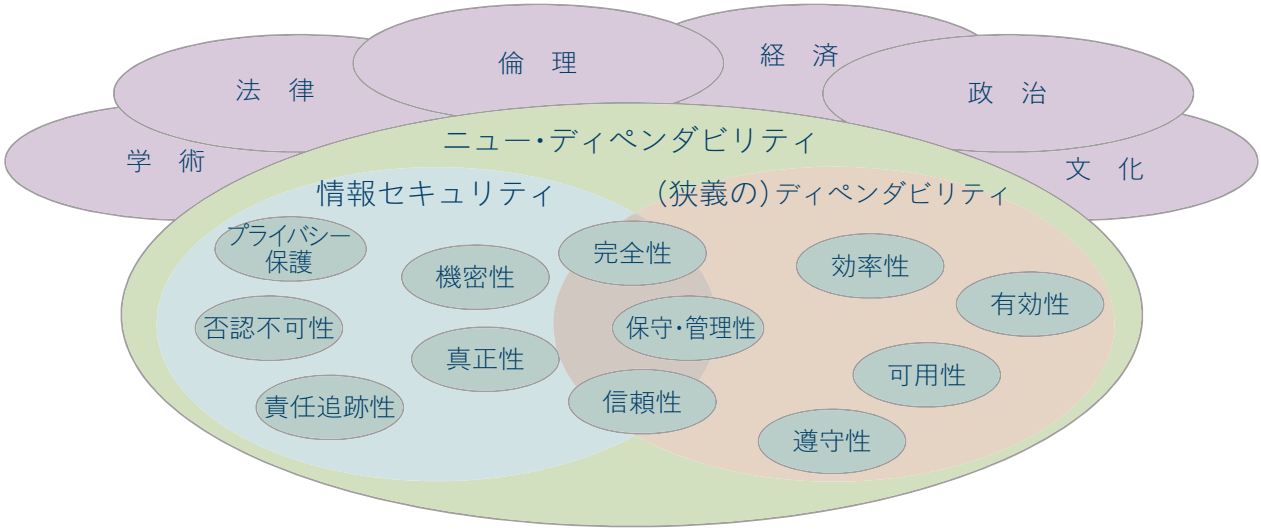


図1．ニュー・ディペンダビリティの概念
（出典：今井秀樹・渡辺創「情報セキュリティとディペンダビリティ」(2006.7.1日本学術会議拡大情報学委員会資料）を基に修正）

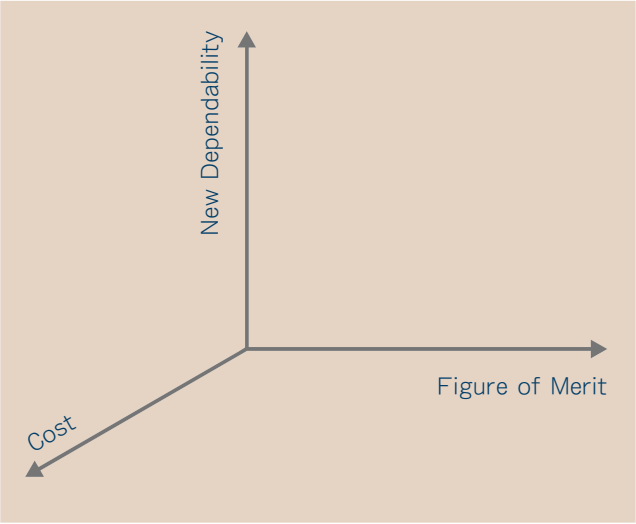


図２．情報システムの３要件

このような見地から本戦略イニシアティブにおいては、これまで研究されてきたディペンダビリティとセキュリティの技術分野を総合し、かつ社会システムとの関わりまでを考慮の対象に含めることを強調する意味で、この概念を「(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」と定義することとする。この考え方を図１に示す。現在のところ、「ニュー･ディペンダビリティ」に相当する適当な日本語がない状況であるが、これも今後の大きな検討課題の一つである。

情報システムは不完全な人間によって作られ、その最終ユーザーも不完全な人間である。また扱われる情報に対しても同様の不完全さが常に存在し、場合によっては悪意の攻撃も加えられる。したがってニュー・ディペンダビリティはある時点で完成するわけではなく永遠に追い求めるべき理念であり、情報化社会の安全と信頼を担保するとともに国際競争力の新たな源泉を創出する技術概念である。情報化社会のグランドデザインに当たって最高の価値として情報技術が目指すべき普遍的な目標理念である。

情報システムの満たすべき要件は、図２に示すようにニュー・ディペンダビリティ、Figure of Merit(単位消費エネルギーあたりの性能)、コストの３つに集約される[注1)]。この３つの要件は相容れないことが多い。例えば、ニュー・ディペンダビリティを追求すると Figure of Merit やコストをある程度犠牲にせざるを得ないといった状況が通常は生起する。したがって、いかに３つのバランスを考慮して対象とする情報システムの最適点を見いだすかが重要である。図３にこれまで情報システムが追求してきた要件および今後追求すべき要件を示す。

注１： Figure of Merit およびコストは定量的に把握しやすいのに対し、ニュー・ディペンダビリティは定量化が困難でまだ評価尺度のない状況であり、説得力のある評価尺度を作ることは大きな課題の一つである。本戦略イニシアティブにおいては３章3.1においてこれを研究課題の一つとして提言している。

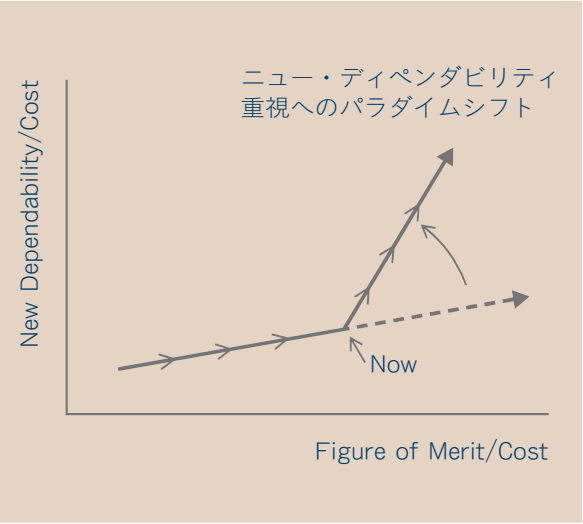


図３．情報システムの追求すべき要件

図３では単位コストあたりのニュー・ディペンダビリティおよび Figure of Merit をそれぞれ縦軸、横軸として描いている。これまでの情報システムは主として Figure of Merit／コストを追求してきた。しかし半導体は微細化の限界に近づき、ソフトウェアは人間の能力を超えるまでに複雑・大規模化する一方、社会の情報システムに対する依存度はますます高まりつつある。このような状況を考えると、Figure of Merit／コストの追求を継続する必要性は変わらないものの、ニュー・ディペンダビリティ／コストをより重視する姿勢を強めることが必要な時期に差し掛かっていると言えよう。

COLUMN 1

研究コミュニティの状況

ディペンダビリティに関する主要な国際的研究コミュニティはIFIP（国際情報処理連合）のWorking Group10.4（年2回の定期ミーティングといくつかの不定期ワークショップを開催）とIEEE Technical Committee on Fault Tolerant Computingである。両者はメインの国際会議として毎年6月末にInternational Conference on Dependable Systems and Networks（DSN）を共催し、他にもいくつかの関連ワークショップを開催している。

1980年にIFIP WG 10.4 on "Dependable Computing and Fault Tolerance"とIEEE TC on Fault Tolerant Computingと合同で「ディペンダビリティの基本概念と用語法」に関する検討が開始された。その検討の経緯と結果をまとめた論文が2004年に出版された（J.-C A.Avizienis et al 2004）*。

ディペンダビリティに関する最新技術は主として毎年のDSNで発表されている。DSNの前身は1971年にスタートしたFTCS（International Symposium on Fault Tolerant Computing）であり、2000年に新しくDSNとしてスタートした。日本では、1980年に京都、1988年に東京、1996年に仙台、2005年に横浜で開催されている。

我が国では、電子情報通信学会にディペンダブルコンピューティング研究会が設置され活動しているが、これまで主としてハードウェア、LSI分野のディペンダビリティに重点が置かれている。また、ソフトウェア科学会にディペンダブルソフトウェア研究会が設置され、活動しているが、これまで主として、ソフトウェアの形式的検証に力点が置かれている。

情報セキュリティ関連の研究コミュニティは、国際的にはIACR（International Association for Cryptologic Research）、IEEE Computer Society、ACM（Association for Computer Machinery）などが代表的で活発な活動を行っている。国内では電子情報通信学会情報セキュリティ研究専門委員会、同学会情報通信システムセキュリティ時限研究専門委員会、情報処理学会コンピュータセキュリティ研究グループなどが代表的である。

国の支援による研究プロジェクトとしては、文科省リーディングプロジェクトの一環としてH15年度からH19年度まで「e-Society基盤ソフトウェアの総合開発」プロジェクトが走っている。これは主としてソフトウェアの生産性向上とプログラム作成支援技術に重点を置いた研究開発プロジェクトである。

また、JST戦略的創造研究推進事業CRESTの領域「実用化を目指した組み込みシステム用ディペンダブル・オペレーティングシステム」がH18年度からスタートしているが、これは組み込みOSに特化している。

これらの活動は総合的な研究開発戦略を推進する際の個別課題における核となり得る。

下の図はAvizienisらにより整理された図である（A.Avizienis et al., 2004）。

＊参考文献

A.Avizienis, J.-C. Laprie, B.Randel, C.Landwehr : "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE Trans. on Dependable and Secure Computing. Vol. 1. No. 1 (Jan.-Mar. 2004)

1.2 ニュー・ディペンダビリティの必要性

今日、我々の社会では、日常の生活、エネルギー供給、健康・医療システム、交通輸送手段、生産工場、流通市場、金融・保険業務、ビジネス・企業経営、政府機能など、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存している。高度情報化社会へ向かってこの依存度はますます強まり、もはや情報システムなしでは日常生活や企業活動も、国家機能さえも成り立たない。

すべての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得られなかったり、想定しなかった事態が起きると、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。情報システムへの社会の依存度が大きくなればなるほど、平時にはその事実が一層見えにくくなり、ひとたび障害が起きた場合には人と社会が被る損失の大きさは一層深刻になる。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もある。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。

また情報の持つ価値が高まり、かつ多くの機器がオープンなネットワークに接続されることに伴って、悪意による情報の盗聴、改ざん、なりすましなどが発生して情報のセキュリティが損なわれ、生命、財産、人権に対する深刻な脅威となっている。企業や政府機関のホームページへの侵入や改ざん、コンピュータウィルスによるファイルの破壊やシステムの故障、ID やパスワードを不法に入手して銀行口座から預金を引き出す犯罪、などが大きなニュースとして取り上げられることもしばしばである。

情報システムに障害を引き起こす原因をフォールト（fault）という（P.14 のコラム 2 参照）。情報化社会の基盤を成す情報システムには、物理的、自然現象的なフォールト、人間の過失によって生じるフォールト、悪意ある人間が犯すフォールト、異なるシステム同士の複雑な相互作用によっ

て生じるフォールトなど、そのディペンダビリティを阻害する様々な脅威が潜在する。このようなフォールト発生を予防する努力はもちろん必要であり、実際これまでもデバイスからシステム、ソフトウェアに至るまであらゆるレベルでそうした信頼性向上の努力はなされている。例えば、生産現場での徹底した部品検査や「ゼロ･デフェクト運動」、あるいはバグ混入の少ないプログラミングスタイル導入で生産性向上を目指すソフトウェアエンジニアリングなどは一定の効果を挙げてきた。

しかし、情報システムのハードウェアは必ず経年劣化を引き起こす物理的材料で構成される。また、情報システムを構成する巨大なソフトウェア群は間違いを犯し易い人間によって設計され、改版され、操作される。さらに悪意を持つ人間による情報システムへの関与や攻撃はいつでも起き得る。いかなる手段を講じたとしても、このような様々なフォールト発生の可能性をゼロにすることはできない。情報システムにフォールトが存在することは常態と考えるべきである。

従って、従来のようにフォールトを予防する努力だけでは不十分であり、フォールトの存在を前提とする情報化社会のデザインあるいは情報システムの設計方法論が必要である。たとえ一部の要素にフォールトが発生したとしてもシステム全体としては期待どおりの良質で確かなサービスを提供し続けるディペンダブルな情報システムを実現する新しい情報技術の体系が求められる。

安心・安全で質の高い生活のできる豊かな国を目指すならば、その社会基盤である情報システムは、我々の生命、財産、プライバシーを安心して委ねられるディペンダブルなシステムでなければならない。ニュー・ディペンダビリティのための情報技術体系が必要な所以である。

COLUMN 2

ディペンダビリティの阻害要因：フォールト

情報システムに障害（failure）を引き起こす原因をフォールト（fault）という。情報システムの大規模化と複雑化は、必然的に以下のような新しいタイプのフォールト発生のリスクを増大させ、その結果として一層多くの深刻な障害が引き起こされる可能性を高める。

1）使用される半導体・実装部品のパラメータ変動や経年劣化による不具合あるいは自然界からの電磁波の影響など、**物理的、自然現象的なフォールト**。特に近年の LSI 技術微細化の進展で物理的フォールト発生の危険は増大している。

2）ソフトウェアや VLSI の設計ミス、システムの操作ミス、設計仕様や保守文書の記述ミスなど、**過失によって生じる人為的フォールト**。VLSI の高集積化、システムの複雑化、ソフトウェアの大規模化、オープン化などによって発生の可能性は急増している。

3）不正侵入、ウィルス感染、サイバーテロなどの**悪意による人為的フォールト**。ネットワーク利用の拡大と多様化によって常にどこにでも存在し、その危険は急増している。

4）単体では正常に動作する複数のシステムの接続、検証済みの既存部品を再利用する VLSI システム設計、人間とシステムの間の双方向コミュニケーションなど、**異なるシステム同士の相互作用によって生じる複合的フォールト**。情報システムが複雑化してブラックボックス化した結果、制御不能な相互作用フォールト発生の危険が増加している。

2 研究投資する意義

■社会の安全と信頼を担保する技術基盤の確立

■新しい経済価値の創出と産業競争力の強化

■情報科学・自然科学と人文・社会科学が融合する新しい学術分野の創出

ニュー・ディペンダビリティを最高の価値とし目標理念とする情報技術体系確立へ向けた戦略的研究開発に投資する意義は少なくとも三つある。

第一の意義は、社会の安全と信頼を担保する技術基盤の確立である。ニュー・ディペンダビリティは、人と社会に対して良質で信頼できるサービスを提供できる情報システム実現への道筋を明示する技術概念であり、これを指導原理とする情報技術の総合的な研究開発戦略の推進は、「安心・安全」を目指す我が国の社会ビジョンの実現に向けた真正面からのアプローチである。加えて、このニュー・ディペンダビリティを指導原理として情報化社会のグランドデザインを進めることは「世界一安全な国日本」の存在感を示し、将来に渡って世界におけるリーダーシップを確保する基礎を築く。

第二の意義は、新しい経済価値の創出と産業競争力の強化である。これまで情報システムの経済的価値は主としてその高速化、高集積化にあったが、ニュー・ディペンダビリティは、そのメトリクス確立によって、情報システムおよびそれによって提供されるサービスに新たな経済価値を生み出す。その価値指標に基づいた評価基準策定によって民間におけるニュー・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、保険システムの改革、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。新たに生み出される経済価値の規模は世界の損害保険の市場規模（2004年度上位５カ国で106兆円、日本は３位で11.4兆円）[注1)]と我が国の情報通信産業の市場規模（2004年度94.4兆円）[注2)]が一つの目安になる。

第三の意義は、情報科学・自然科学と人文・社会科学が融合する新しい学術分野の創出である。ニュー・ディペンダビリティはユーザー視点からのシステム属性に関わる包括的かつ融合的な概念

注１： Sigma No.2/2005、Swiss Re 社発行
注２：2006年度情報通信白書

であり、ディペンダブルなサービス価値を評価する視点は、直接のインタフェースとなる情報システムのレベルにとどまらず、社会の変化と技術の進展に伴って必然的に人間と社会のレベルへと展開せざるを得ない。このため情報科学・自然科学と人文科学・社会科学の融合による新しい学術分野が創出され、その応用として、ニュー・ディペンダビリティに価値をおく新しい社会システムとサービス産業の創出が期待される。

3 具体的な研究開発課題

3.1 モデリングおよび評価手法

1）障害解析とフォールトモデリング

情報システムに関連する障害事例の収集と解析、その原因となるフォールトの類型化、フォールトがシステム各階層におけるサービスに与える影響の解析と形式化、それを表現するフォールトモデルの開発。

2）ニュー・ディペンダビリティの評価

情報システムのニュー・ディペンダビリティを定量的に評価する尺度（メトリクス）の定義、その測定方法、計算方法の開発。客観的な比較評価を可能にするベンチマーキング手法の開発。十分な規模のテストベッドを用いたニュー・ディペンダビリティ・メトリクスの正当性と有効性の検証、社会と産業の合意形成。

3）ニュー・ディペンダビリティの経済

システムが提供するサービスを受けるユーザー（人、組織、人工物、他のシステムなど）がそのインタフェースで認識するサービス品質、許容できる障害の程度、障害による損失コスト、要求するニュー・ディペンダビリティ水準などのメトリクス確立とその相互関係の形式化。情報システムのライフサイクル・コストとニュー・ディペンダビリティ投資効果の評価技術の開発。

3.2 ニュー・ディペンダビリティを実現するための技術

1）ニュー・ディペンダブルシステムの要素技術

VLSI、組み込みシステム、社会基盤システム、ネットワーク、グリッド、ヒューマンインタフェース、センサーネットワーク、ロボティクス、モバイル携帯端末、データセンター、スーパーコンピュータなど、多様な応用分野におけるニュー・ディペンダビリティ実現のソフトウェアとアーキテクチャの研究、特に、自律性、分散性、冗長性、適応性、柔軟性などを有するニュー・ディペンダブルアーキテクチャの研究、誤り検出／訂正、異常検出、自己診断、自律再構成、自己修復、自律最適化、自己進化、仮想化技術などを含むニュー・ディペンダビリティ要素技術の研究開発。

2）データのニュー・ディペンダビリティ

ネットワーク上で大量に生成され、蓄積され、流通し、消費される情報の処理と管理におけるニュー・ディペンダビリティ、および情報内容のニュー・ディペンダビリティ確立の視点からのデータモデル、メタデータ、コンテンツ管理、データマイニング、セマンティックウェブ、知識抽出、知識統合化技術、データ検証、インタフェース技術などの研究開発。

3）情報セキュリティ技術

情報システム／ネットワークにおける暗号通信、ウィルス・侵入検知、サイバーテロ防止技術、システム回復技術、監視技術、署名・認証技術、個人情報保護技術など、情報システムの可用性、情報の完全性、秘匿性を確保する情報セキュリティ技術の開発。

4）大規模システム・ソフトウェア設計技術

大規模ソフトウェアシステム、ネットワークに接続されたオープンシステム、VLSI システムなどにおける仕様作成･記述の方法論開発、厳密な設計技術と統合化技術、検証技術、テスト技術、QoS 評価技術など、不確定要素の多い大規模で複雑なオープンシステムを正しく設計する厳密な設計方法論の確立。

5）ニュー・ディペンダビリティをサポートするデバイス技術

五感情報センサー、環境情報センサー、給電デバイス、再構成可能デバイス、セルフチェッキングデバイス、セキュリティチップなど、情報システムのニュー・ディペンダビリティ実現をサポートする新しいデバイス技術の開発。

6）応用・サービスのニュー・ディペンダビリティ

電子政府、高度情報交通システム、エネルギー供給システム、個人デジタル資源、社会経済シミュレーション、情報フロー管理などの社会インフラ応用分野、ビジネスモデリング、ガバナンス・経営戦略などのビジネス応用分野、組み込みシステム技術、仮想化環境、高速シミュレーション技術、CAD／CAM／CAE技術などの産業応用分野など、様々な応用分野における情報技術、サービスのニュー・ディペンダビリティ実現に向けた研究開発。

3.3 ニュー・ディペンダビリティの制度

ニュー・ディペンダビリティ基準の策定と標準化戦略の推進、ニュー・ディペンダビリティの監査と認証制度、SLA（Service Level Agreement）保証システムの開発、ニュー・ディペンダビリティ評価に基づくライアビリティ・システム、保険システムの改革、ニュー・ディペンダビリティ教育、情報倫理の確立、情報犯罪の法制度など、ニュー・ディペンダビリティに関連する制度・システムのあり方の検討と政策提言。

COLUMN 3

関連する学術分野

提供されるサービスを受けるユーザーの視点をどこに設定するかによって、対象となる情報システムの範囲にいくつかのレベルがあり、それに応じて関連する学術分野の範囲が広がる。

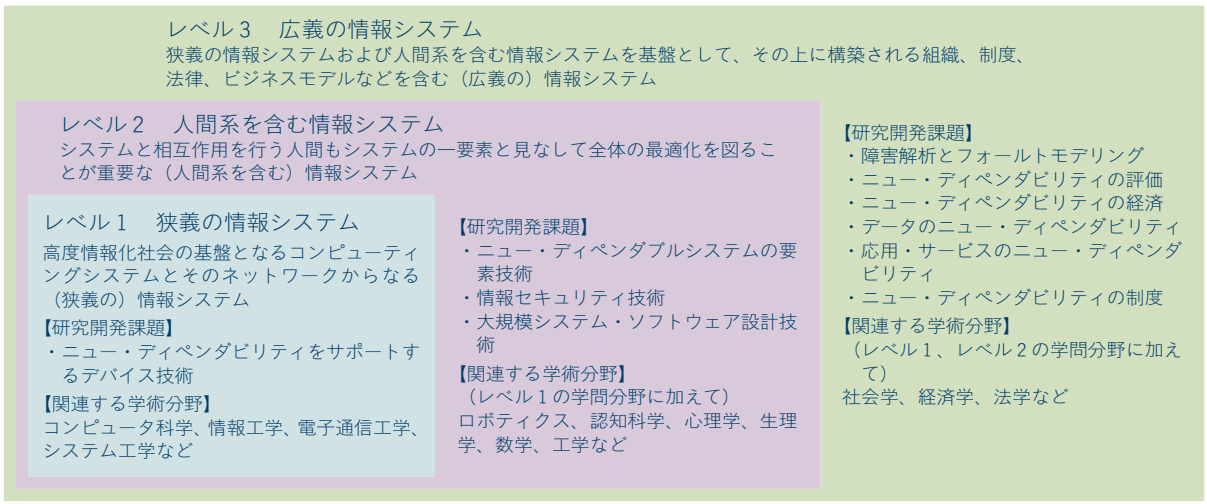
まず、レベル１は、高度情報化社会の基盤となるコンピューティングシステムとそのネットワークからなる（狭義の）情報システムである。例えば、個人用パソコンや携帯端末、企業、銀行などの巨大コンピュータシステム、自動車や産業用の組み込みシステム、サーバー、ルータなどのネットワーキング要素などをイメージすればよい。このレベルの研究投資によって、ディペンダビリティを価値指標とするコンピュータ科学、情報工学、電子通信工学、システム工学などの研究が促進され、情報通信関連産業の技術開発が促進される。

レベル２は、システムと相互作用を行う人間もシステムの一要素と見なして全体の最適化を図ることが重要な（人間系を含む）情報システムである。例えば、介護ロボットと人間の相互作用による活動が営まれる建造物空間全体から成る情報システム、医師と患者とシステムの間の相互作用を含む遠隔診療システム、ドライバーと車両と道路との相互作用が生まれる道路交通情報システムなどがこの段階に相当する。これはレベル１の学問分野に加えて、ロボティクス、認知科学、心理学、生理学、数学、工学などとの連携が必要になる。

レベル３は、狭義の情報システムおよび人間系を含む情報システムを基盤として、その上に構築される組織、制度、法律、ビジネスモデルなどを含む（広義の）情報システムである。例えば、電子政府、電子マネー、企業統治・経営などがこの段階に相当する。これらは、前記に加えて、さらに社会学、経済学、法学などが必要になる。

なお、サービスを提供する「情報システムのディペンダビリティ」と、情報システムによって提供される「サービスのディペンダビリティ」とは、その意義が全く異なることに注意を要する。前者の場合は、「良質で信頼できるサービス」に関するユーザーの合意があり、そのようなサービスを提供することが情報システムの仕様として明確に定められていることが前提である。提供されるサービスがその仕様から逸脱するかどうかが問題なのであって、サービスの内容が「本当にそのユーザーにとって良質か？」は問わない。従って、「情報システムのディペンダビリティ」は情報科学の研究対象になる。一方、後者の「サービスのディペンダビリティ」を考える場合には、「何が良質で信頼できるサービスか？」が問題になる。例えば、大量の情報の中から「有益な知識」を抽出して提供するサービスは、ある人々や組織には有益であっても他の人々や組織には有害かもしれない。すなわち、ユーザーの間でディペンダビリティの基準に関してコンフリクトが存在し、これらは政治、文化、宗教、あるいは国家体制などに依存する場合がある。従って、別のレベルの議論が必要になる。

具体的な研究開発課題と関連学術分野



4 研究開発の推進方法

ニュー・ディペンダビリティは情報化社会における安全と信頼を担保する基本概念であり、その研究は高度に包括的かつ融合的であると同時に、個別課題には学際的な未開拓分野が多いので、効果的、効率的に推進するために以下の諸点に留意する必要がある。

1) 情報化社会のニュー・ディペンダビリティを指導原理とするグランドデザインの策定、ならびにディペンダビリティ・メトリクスの国際標準化推進に向けて、関連省庁を包含する国レベルの戦略イニシアティブとする。

2) コンピュータ科学、情報工学、電子通信工学、システム工学に加えてロボティクス、認知科学、心理学、社会学、経済学、法律学など広範囲にわたる研究者が連携する場が必要である。

3) 大学の研究者に加えて、サービスの生産側と消費側の企業研究者の参加が必須である。

4) 評価メトリクスの研究と各領域のニュー・ディペンダビリティ実現技術の研究を並行させ、メトリクスの合理性と実現技術の有効性を検証するための相互フィードバックループを形成する。

5) 社会におけるユーザー視点でニュー・ディペンダビリティのメトリクスと実現技術の有効性を検証するために各研究領域共通のテストベッドを設定し、そこで実証実験を実施する。その結果に基づいてメトリクス及び実現技術の課題を洗い出して新たな段階へステップアップする研究開発のスパイラル・ループ形成を可能にする推進体制が必要である。

5 科学技術上の効果

■新しいシステム設計技術体系の確立

■新しい情報システム評価指標の確立

■新しい学術分野の開拓

科学技術上の効果は大きく分けると３つある。

第一の効果は「新しいシステム設計技術体系の確立」である。

情報システムはその動作の全容を誰も把握できなくなるほど大規模化し、複雑化している。またネットワークを介して第三者の開発した未知のシステムと接続されるオープンシステムになりつつある。その結果、システム設計の出発点であるはずの「システムの仕様」を正確に記述できない、あるいは「システムへの入力」を予知できないという状況になりつつあり、従来の「閉じたシステム」とは異なる「オープンシステム」に対する新しいシステム設計論の開発が必要になっている。さらに、経験のない無邪気なユーザーも悪意を持った練達のユーザーもアクセス可能なネットワーク環境では、故意の不正侵入によるセキュリティ上の問題に加えて、過失による誤操作やミスの可能性がユビキタスに存在する。このような人為的フォールトに対してディペンダブルなシステム設計の方法論は未確立である。このニュー・ディペンダビリティ研究への投資によって、これまでとは異なるオープンシステムに対する新しい情報システム設計論が開発され、この技術分野で日本が世界をリードするチャンスが生まれる。

第二の効果は「新しい情報システム評価指標の確立」である。

これまで情報システムの研究開発の主要な目標はシステムの高速化、高集積化、高機能化であった。これらの目標はニュー・ディペンダビリティが達成されてはじめて意味を持つ。ディペンダビリティのメトリクスと評価手法の開発によって、情報システム設計の新しい評価指標が確立され、国家基幹プロジェクトの評価視点とアカウンタビリティの提供、民間におけるニュー・ディペンダビリティ技術の開発競争の促進、国際的産業競争力の強化などにつながることが期待される。

第三の効果は「新しい学術分野の開拓」である。

前述のように、ニュー・ディペンダビリティを価値とする研究は、ユーザー視点の置き方で対象となる情報システムの範囲にレベルがあり、それに応じて関連する学術分野の範囲が広がる。コン

ピューティグシステムとネットワークから成る狭義の情報システム（レベル 1）のディペンダビリティ研究では欧米が先行しているが、これまで主に物理的フォールトが対象であった。人為的フォールトや相互作用フォールトに対する実現技術はほとんど手つかずの状況にある。人間系を含む情報システム（レベル 2）に関しては、国際的にも研究がスタートしたばかりである。最近のサービスサイエンスの提唱はこのレベルに相当する。情報システムを基盤としてその上に構築される社会的組織、制度、法律などを含む広義の情報システム（レベル 3）のディペンダビリティ研究は未開拓分野であり、今後、新しい概念形成を経て、情報科学、自然科学と社会科学・人文科学が融合した新しい学問分野の開拓が期待される。

6 社会・経済的効果

■社会ビジョンの実現

■新しい経済価値の創出

■世界一安全な国日本の国際的存在感

社会・経済的効果は大きく分けて３つある。

第一の効果は「社会ビジョンの実現」である。

ニュー・ディペンダビリティを備えた情報システム／ネットワークの実現、およびそれを基盤とするディペンダブルな情報化社会の建設に向けた戦略的な研究開発の推進は、第３期科学技術基本計画に掲げられた「安心・安全で質の高い生活の実現に向けて、国土と社会の安全を確保し、暮らしの安全を確保する」という社会ビジョンに対する真正面からの取り組みである。さらに、後で第二の効果として特に指摘するニュー・ディペンダビリティの経済価値創出によって、あらたな技術開発が促進される結果、「国際競争力があり持続的発展ができる国を目指して、革新を続ける強靱な経済・産業を実現し、科学技術により世界を勝ち抜く産業競争力を強化する」という社会ビジョン達成への貢献が期待できる。

第二の効果は「新しい経済価値の創出」である。

ニュー・ディペンダビリティのメトリクス定義、評価基準の策定とその測定手法、計算手法の開発、さらに国際標準化によって、ニュー・ディペンダビリティが情報システムの新たな経済価値になる。その結果は、SLA 保証システムの確立、損害保険システムの改革、国家基幹プロジェクトの評価視点の提供とアカウンタビリティの充足、民間におけるニュー・ディペンダビリティ技術の開発競争の促進、産業の国際競争力強化などにつながることが期待される。また、ニュー・ディペンダビリティを価値とする産業技術分野、サービス産業分野の創出が期待される。

第三の効果は「世界一安全な国日本の国際的存在感」である。

ニュー・ディペンダビリティ研究が目指す社会ビジョンの実現に向けた貢献には２つの側面がある。すなわち「情報化社会の基盤である情報システム／ネットワークにおけるニュー・ディペンダビリティの保証」と「ディペンダブルな情報システム／ネットワークの活用による社会のニュー・ディペンダビリティの確保」である。後者の側面は、前述のレベル３の情報システム、すなわち情

報システムを基盤とする社会システムのニュー・ディペンダビリティ確保に対応する。この目標達成へ向けてのイニシアティブは、「世界一安全な国・日本」を標榜し国際社会へ貢献する我が国の存在感を確固たるものにする効果をもたらす。

7 時間軸に関する考察

ニュー・ディペンダビリティ評価指標、評価手法の研究はただちに着手し、3 年以内に評価指標、ガイドラインを策定することが望ましい。その結果、ニュー・ディペンダビリティ評価指標の達成を目指した民間の技術開発の促進と高度化を図る環境を醸成し、6 年以内に基準となる指標を達成するニュー・ディペンダビリティ技術を確立し、国際標準化を狙うことが望ましい。10年以内に安心・安全な高度情報化社会を実現し、安心・安全の先進国日本の国際的存在感と世界をリードする産業競争力を確立する。

付録

欧米における関連技術への政府レベルの取り組み

1. 欧州の取り組み

欧州では、欧州委員会において、「第6次研究・技術開発フレームワークプログラム（FP6：2002年～2006年）」が策定され、研究開発投資が行われている。FP6にて設定された7つの優先分野の一つに、“Information Society Technologies (IST)”がある。FP6の4年間の予算額は、IST関係で3,964百万ユーロで、FP6全体予算の約3割を占める。（FP6全体予算額は、14,682百万ユーロ）

ISTでは、「いつでもどこでも誰もがISTサービスにアクセスできる」というビジョンを掲げ、4つの「Strategic Objectives」を設定している[1]。このうち、「Applied IST research addressing major societal and economic challenges」において掲げられている13の優先投資対象の1つに、「Towards a global dependability and security framework」がある。これは、ディペンダビリティに関連した科学技術上の発展と、欧州の産業力強化を目指すものである。例えば、2001年より、ISTのプロジェクトとして、民生品のディペンダビリティのベンチマーキングに関するプロジェクト（Dependability Benchmarking Project）[2]が実施されている。ここでは、ディペンダビリティベンチマーキングの概念、仕様、ガイドラインとベンチマーキング用プロトタイプツールの提供を目標としている。

また、FP6のもとで、情報通信技術のセキュリティとディペンダビリティに関する研究開発を、「第7次研究・技術開発フレームワークプログラム（FP7：2007年～2013年）」に向けて戦略的につなげていくために“SecureIST”というプロジェクトが推進されている[3]。このSecureISTプロジェクトでは、European Security and Dependability Task Force（STF）が、セキュリティとディペンダビリティ関連研究における重点領域、優先課題を示すことを目的として活動している。この活動を受けて、専門有識者から成るThe Secure IST Advisory Boardが、FP7へ向けて欧州のセキュリティとディペンダビリティに関する研究の将来の枠組みについての提案をしている[4]。

現在、FP7の概要が固まりつつあるが[5]、このFP7で設定されつつある9つの優先分野の1つに“Information Communication Technology（ICT）”がある。ここで、ICTについては「技術の柱」が6つ示されており、“Software, Grids, security and dependability”はそのうちの1つに位置付けられている。具体的には、動的で、適応可能で、ディペンダブルかつ信頼のおけるソフトウェアやサービス、それらのプラットフォーム、複雑システム、及び新しい処理アーキテクチャに関する技術であり、それらのユーティリティとしての提供も含まれる。

社会的な面では、例えば電子投票[6]や著作権保護[7]など特定の応用に関して法制度も含めた議論もなされるようになって来ている。

1）http://cordis.europa.eu/ist/activities/activities.htm
2）http://www.laas.fr/dbench/
3）http://www.securitytaskforce.org/
4）Secure IST Advisory Board Recommendations for a Security and Dependability Research Framework, Issue 2.0 19 June, 2006. -Project no. 004547, Project title : Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D-
5）http://cordis.europa.eu/fp7/home.html
6）http://www.iavoss.org/
7）http://www.titr.uow.edu.au/DRMTICS2005/

2. 米国の取り組み

ネットワーキング・情報技術研究開発（NITRD：Networking and Information Technology Research and Development）計画[8]は、コンピューティング、ネットワーキング、あるいはソフトウェアについて先端情報技術のブレイクスルーを目指した米国の優先投資計画である。1991年のHigh-Performance Computing Actに端を発し、1998年にNext Generation Internet Research Actで改正された米国Public Lawにより承認された。

NITRDの推進のために、省庁の壁を越えた調整を行う情報技術研究開発国家調整局（NCO：National Coordination Office）が設置されている。この局の調整により、NITRDの投資は、8つの分野（PCAs：Program Component Area）に対して行われている。この8つの分野のうちで、“Cyber Security and Information Assurance (CSIA)”、“High Confidence Software and Systems (HCSS)”が、ディペンダビリティに関連する。2007年の予算要求額は、NITRD全体で3,074百万ドル、うちCSIAが175.5百万ドル（6％）、HCSSが145.2百万ドル（5％）になっている[9]。

CSIA[10]分野の投資は、コンピュータシステムのアベイラビリティ、完全性、機密性を確保するための研究や開発を対象とする。具体的には、ネットワークセキュリティ、ディペンダブルシステム、状況認識と対応、セキュアな分散システム等に関する基礎研究及び応用研究のほか、インフラ整備、産業界への技術移転等である。

HCSS[11]分野の投資は、米国の国家セキュリティに不可欠な基礎科学と情報技術を対象とする。具体的には、航空宇宙、大規模インフラ、国防、医療に関する次世代技術、信頼性確保に関する新技術、複雑な集積化システムの保障等に関する研究開発である。なお、CSIAとHCSSは、投資課題を一部共有している。

従来の「ディペンダビリティ」と「情報セキュリティ」の一体化の動きは、数年前から米国で多く見られる。例えば、NSFでは、CISE（Computer & Information Science & Engineering）の重点分野としてCyber Trustが挙げられている[12]。これには「ディペンダビリティ」と「情報セキュリティ」の一体化の思想が入っている。ただし、「ディペンダビリティ」と「情報セキュリティ」は融合せずに並立している感があり、有機的な一体化はまだなされていないようである。

技術的な面で「ディペンダビリティ」と「情報セキュリティ」の融合の方向としては、IBMなどが提唱しているAutonomic Computing[13]やSelf Healing Computingなどもある。これらの動きは、NITRDのHCSSにも取り込まれている。

8）http://www.nitrd.gov/
9）http://www.nitrd.gov/pubs/2007supplement/
10）http://www.nitrd.gov/subcommittee/csia.html
11）http://www.nitrd.gov/subcommittee/hcss.html
12）http://www.nsf.gov/funding/pgm_summ.jsp?pims_id＝13451&org＝CCF
13）http://www-03.ibm.com/autonomic

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―

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
ファックス　03−5214−7385
http : //crds.jst.go.jp/

平成18年12月

ATTAATC A AAGA C CTAACT CTCAGACC

CT CTC G CC AATTAATA

T AA TAATC

TTGCAATTGGA CCCC

AATTCC AAAA GGCCTTAA CCTAC

ATAAGA CTCTAACT CTC G CC

AA TAATC

AAT A TCTATAAGA CTCTAACT CTAAT A TCTAT

CTC G CC AATTAATA

ATTAATC A AAGA C CTAACT CTCAGACC

AAT A TCTATAAGA CTCTAACT

CTC G CC AATTAATA

TTAATC A AAGA C CTAACT CTCAGACC

AAT A TCTATAAGA CTCTAACT

ATTAATC A AAGA C CT

GA C CTAACT CTCAGACC

0011 1110 000

00 11 001010 1

0011 1110 000

0100 11100 11100 101010000111

001100 110010

0001 0011 11110 000101