CRDS-FY2007-SP-06

情報社会のディペンダビリティ

ー情報技術の目指すべき目標理念ー

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

目　　次

Executive Summary

これまでの情報技術は、ムーアの法則に象徴されるように、ひたすら高速化、大容量化、高集積化、高機能化、低電力化という「性能向上」を研究開発の目標として追求してきた。その結果、情報システムは社会の中に深くかつ複雑に浸透し、人と組織のあらゆる活動がネットワーク化された情報システムに依拠する社会、すなわち「情報社会」が出現した。情報社会では、情報システムと社会システムの間に明確な境界線を引くことはできず、システムの開発・実装において情報技術と社会技術とが一体となって機能する。

こうした状況で今後の成熟した情報社会を展望すると、我が国の科学技術政策として、今、情報技術の研究開発が目指すべき方向は、従来のような「性能向上」の追求ではなく、「ディペンダビリティ」の追求である。「ディペンダビリティ」は情報社会における安全信頼保障の要となる技術概念であり、将来を見据えた情報社会のグランドデザインに当たって最高の価値として科学技術が目指すべき普遍的な目標理念である。一方、今後の更なる「性能向上」の追求は、技術革新、経済原理、市場動向を踏まえた民間企業の経営判断と事業活力に委ねるべきである。

情報社会では、ひとたびシステム障害、重要インフラ事故、サイバーテロ、情報漏洩など、社会の期待や合意に反する事象が起きると、財産逸失、人命損傷、社会・経済機能マヒなどの深刻な事態を招く。場合によっては国家安全保障への重大な脅威になる。目指すべき社会は、人や組織が社会インフラ、情報環境から提供されるサービスの品質（信頼性、安全性）に揺るぎない確信を持ち、その良質なサービスに依拠して安寧な生活、十全な活動を展開できるディペンダブルな情報社会である

しかるに今日、我々は、ブラックボックス化、システムの複雑化・巨大化、VLSI 微細化、情報量の爆発的増加、サービス利用の多様化、システム要素の経年劣化、ネットワークにおける責任所在の不明確化など、情報社会のディペンダビリティを阻害する原因（フォールト）を生む様々なリスク要因に直面している。これらの要因は、情報社会の進化・発展に伴い、今後一層増加する。

このようなリスク要因の存在を前提として、情報社会のディペンダビリティを実現し、社会の安全信頼保障を恒久的に確立するためには、情報社会を構成する４つの階層、すなわち、

1) 基礎となるネットワーク化「情報システム」
2) 情報システムを活用して構築される社会の「重要インフラ」
3) 重要インフラを活用して提供される「サービス・情報」

4) サービス・情報を享受する人と組織が形成する「情報社会」

のすべてにおいて、ディペンダビリティの実現とその評価が必要である。

このため、この４つの階層のそれぞれにおいて、

i. ディペンダビリティを恒久的に保証するアーキテクチャ

ii. ライフサイクル・リスクを想定した設計・保全技術

iii. ディペンダビリティの定量的評価技術

の総合的な基盤研究開発を戦略的かつ永続的に推進することを提案する。

また、この研究開発を長期的な視点で戦略的かつ集中的に推進するため、情報社会の安全信頼保障に関する基盤的課題の研究開発拠点を設置することを提案する。

この研究開発へ投資する意義を要約すると、

・ 情報社会の安定化

・ 新しい経済価値と国際競争力の源泉創出

・「情報社会技術」の創出と人材育成

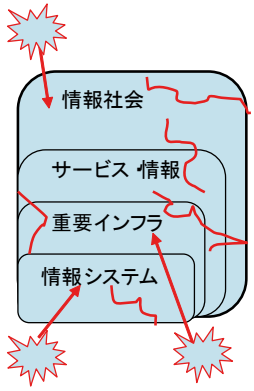
の３点にある。

この戦略イニシアティブは、2006 年 12 月に発行された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～」を具体化し、優先的に取り組むべき課題とその研究開発を戦略的かつ永続的に推進する方法を提案するものである。

情報社会のディペンダビリティ

--- 情報技術の目指すべき目標理念 ---

性能向上の追求 → ディペンダビリティの追求

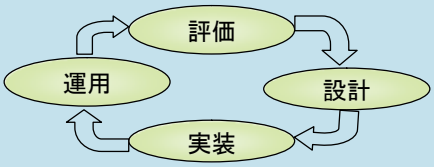


情報社会のリスク要因
- ブラックボックス化
- 複雑化・巨大化
- 情報量の爆発的増加
- サービス利用の多様化
- システム要素の経年変化
- 責任所在の不明確化

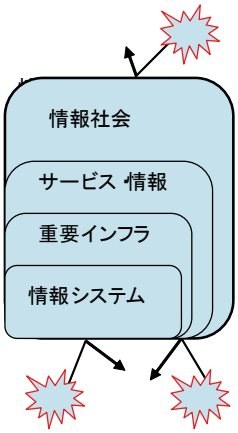
提案

◆「情報システム」、「重要インフラ」、「サービス・情報」、「情報社会」の4階層において、以下の3項目の基盤研究開発を戦略的かつ永続的に推進すべきである:

1. ディペンダビリティを恒久的に保証するアーキテクチャ
2. ライフサイクル・リスクを想定した設計・保全技術
3. ディペンダビリティの定量的評価と経済価値マッピング



◆研究開発を長期的な視点で戦略的かつ集中的に推進するため、情報社会のディペンダビリティを保証する「情報社会技術」に関する基盤的課題の研究開発拠点を設置すべきである



研究に投資する意義
- 情報社会の安定化
- 新しい経済価値と国際競争力の源泉創出
- 「情報社会技術」の創出と人材育成

人の安寧な生活、組織の十全な活動を展開できるディペンダブルな情報社会

情報社会

恒久的な安全信頼保障を確立する
情報社会技術・情報社会システム


経済


社会


生活


産業

サービス・情報

重要インフラ

4階層にわたる3項目の基盤研究開発の戦略的・永続的推進

情報システム

ディペンダビリティを恒久的に維持・保証するアーキテクチャ

ライフサイクル・リスクを想定した一貫性ある設計・保全技術

ディペンダビリティの定量的評価と経済価値へのマッピング

長期的視点で戦略的・集中的な研究推進のため、社会の安全信頼保障に関する基盤的課題の研究拠点を設置

専門用語の解説

1) ディペンダビリティ（Dependability）：「提供するサービスが良質で信頼でき、人間と社会の活動が安心してそれに依拠できる」という情報システムの属性である。自然現象、経年劣化、設計ミス、操作ミス、システム不整合など、予測不能で偶発的に生じる物理的、人為的な障害原因（フォールト）の存在を前提として、情報システムの可用性 (availability)、信頼性 (reliability)、安全性 (safety)、完全性 (integrity)、保全性 (maintainability) を総合した概念として定義される。

国際規格 IEC615081（コラム①参照）に定められている電子情報システムの機能安全 (functional safety) の概念も包含する。

本イニシアティブにおける「ディペンダビリティ」は、情報システムの属性概念から拡張し、広く社会システム、情報社会の属性を表す概念としても用いている。

2) セキュリティ (Security)：「情報をその生産者，運用者，利用者（あるいは社会）が合意した意図のとおりに利用できることを保障する」という情報システムの属性である。悪意による意図的な不正アクセス、不正侵入の存在を前提として、情報システムの可用性 (availability)、完全性 (integrity)、機密性 (confidentiality) を総合した概念として定義される。

コラム①　国際規格 IEC 61508

ＩＥＣとは国際電気標準会議のことで、電気関係の国際規格を制定する機関である。電気・電子系ならびにコンピュータ（ソフトウェア）の安全性を高めるために機能安全 (Functional Safety) に関する国際規格 IEC 61508 を 2000 年頃に制定した。機能安全とはシステムの安全を確保する機能を持つ安全系によってリスクを許容目標へ軽減する設計思想であり、その障害によって人命や社会に大きな影響を与えるものなどが対象となる。例えば、輸送機器、化学プラント、医療機器などが相当する。これらの設計製造・運用保守・改修廃却に至るライフサイクルにおける安全評価の要求や、組織の機能安全能力審査、安全評価者の独立性及び従事者の資質にも触れるなど、安全規格の全体についても記述している。設計の誤りや製造ミスなど、主に人間のエラー（失敗）によるものに対しては安全評価・対策や文書化などによって防ぐこととしている。一方、部品・材料劣化などのランダムなハードウェアフォールトに対しては、冗長化や多様化によるシステムの信頼性向上や自己診断機能設置などの対策を要求している。また、確率論的リスク解析などによって、全体システムのリスクが許容リスクを下回るようにするために、当該安全装置の安全度水準（SIL ＝ Safety Integrity Level）を決定することとしている。さらに上記の対策を確実にするために、組織の機能安全評価能力の診断や、組織を構成する個人の資質あるいは行動特性 (competency) を包含する形となっている。ソフトウェアに対して、安全ライフサイクルの導入と共に、SIL に応じて指定するソフトウェア技法の採用を要求しており、多くのソフトウェア技法を提示している。

3) ディペンダビリティとセキュリティの融合：情報社会の安全信頼保障を考えるとき、以下の理由で、ディペンダビリティとセキュリティの融合が必要になる。従来のセキュリティ研究は「秘密情報（鍵）は適切に管理されている情報システムは正しく実現されている」という仮定の上に成り立っているが、システム操作ミスによる秘密情報漏洩の可能性、仕様ミス、設計ミス、実装ミスによる脆弱性発生の可能性は情報システムに常に存在しているため、セキュリティ確保にはディペンダビリティ技術が必要である。一方、従来のディペンダビリティ研究は「フォールト（物理的、人為的）の発生は偶発的である」という基本的仮定の上に成り立っているが、実際には悪意ある人為フォールト（侵入、改竄）に偶発性はないので、ディペンダビリティ確保にはセキュリティ技術が必要である。

4) ニュー・ディペンダビリティ：2006 年 12 月に発行された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～」で、ディペンダビリティとセキュリティの技術概念を社会システムのユーザー視点で総合する新しい概念を表す用語として用いられた。本イニシアティブにおける「ディペンダビリティ」は、この新しいディペンダビリティに相当する概念を表すが、必要な場合にはセキュリティを明示的に併記することによって両者の補完関係を強調している。

5) フェイルセイフ (Fail-safe)：「システムに障害が生じる場合、それは必ず安全な（許容可能な）障害である」、あるいは「提供するサービスに障害が生じる場合、必ず安全な状態でサービスを停止する」という情報システム、社会システムの属性である。例えば、鉄道踏切の遮断機に障害が発生した場合、開いたままの状態で機能を停止すると危険であるが、必ず閉じた状態で機能停止になれば安全な障害であると言える。システム障害の発生を回避出来ない事態になった場合の「最後の手段」を提供するシステム設計思想である。

1. 情報技術は「情報社会のディペンダビリティ」を目標理念とすべきである

情報社会のディペンダビリティとは、情報社会が直面する様々なリスク要因の存在にもかかわらず、社会インフラ、情報環境から提供されるサービスの安全性と信頼性に揺るぎない確信を持ち、その良質なサービスに依拠して人々の安寧な生活と組織の十全な活動を展開できる、という情報社会の属性である。人と組織のあらゆる活動が情報システム・ネットワークに依拠する情報社会では、ディペンダビリティは最高の価値であり、情報技術の研究開発が目指すべき普遍的な目標理念である。

これまでの情報技術の研究開発は、ムーアの法則に象徴されるように、ひたすら高速化、大容量化、高集積化、高機能化、低電力化という「性能向上」をシステム開発の目標として追求してきた。その結果、情報システムは社会の中に深くかつ複雑に浸透し、人と組織のあらゆる活動がネットワーク化された情報システムに依拠する社会、すなわち情報社会が出現した。情報社会では、情報システムと社会システムの間に明確な境界線を引くことはできず、システムの開発・実装に当たっては情報技術と社会技術とが一体となって機能する。このため人間と社会と技術が複雑に絡み合う多種多様なシステムやパラダイムが次々と出現し、それらの無秩序な融合、拡張が地球規模で進行している。

こうした状況で今後の成熟した情報社会を展望すると、我が国の科学技術政策として、今、情報技術の研究開発が目指すべき方向は、従来のような「性能向上」の追求ではなく、ここで提案する「情報社会のディペンダビリティ」の追求である。今後の更なる「性能向上」の追求は、技術革新、経済原理、市場動向を踏まえた民間企業の経営判断と事業活力に委ねるべきである。今、情報技術の研究開発方向を「情報社会のディペンダビリティ」に切り替える必要性は、情報システムが技術的には無瑕疵であっても社会に実装されたときに思いがけない大きな事故、システム障害を引き起こし、重大な損害、危害を社会に与えるケースが各所で起こっている現状からも容易に思料できる。

「情報社会をよりディペンダブルにする情報技術」、あるいは「情報システムをよりディペンダブルにする情報技術」は未だ市場では広く認知されるに至っていない。しかし近い将来、情報社会の根幹を支えるべき最大の付加価値を有する技術となり、情報技術体系の新たな発

展・進化の駆動力になるとともに、国際競争力強化の源泉を創出することが先見される。このため、「ディペンダビリティの経済価値」がまだ十分に認識されない現時点では、国が先導的にその研究開発を支援する必要がある。世界的には、フランスや米国ですでにこのディペンダビリティを専門に研究する研究機関が存在し、その概念形成と技術開発において世界をリードしている現状を考えると、わが国においても情報技術、社会技術を含む広範囲の研究者集団にその重要性の認識を促すとともに、緊急にその研究開発を支援する必要がある。

「情報社会のディペンダビリティ」を実現し、社会の安全信頼保障を恒久的に確立するためには、情報社会を構成する４つの階層、すなわち、

1) 基礎となるネットワーク化「情報システム」
2) 情報システムを活用して構築される社会の「重要インフラ」
3) 重要インフラを活用して提供される「サービス・情報」
4) サービス・情報を享受する人と組織が形成する「情報社会」

のすべてにおいてディペンダビリティの実現とその評価が必要である。

このため、この４つの階層のそれぞれにおいて、

i. ディペンダビリティを恒久的に保証するアーキテクチャ
ii. ライフサイクル・リスクを想定した設計・保全技術
iii. ディペンダビリティの定量的評価技術

の総合的な基盤研究開発を戦略的かつ永続的に推進することを提案する。

また、この研究開発を長期的な視点で戦略的かつ集中的に推進する方法として、情報社会の安全信頼保障に関する基盤的課題の研究開発拠点を設置すべきである。

２．具体的な研究開発課題（４階層１２課題）

⑴ 情報システム階層

i. フォールトや不正アクセスの存在にかかわらず、実世界と相互作用するネットワーク化情報システムのディペンダビリティを恒久的に保証するシステム・アーキテクチャの研究開発
ii. 情報システムのライフサイクル・リスクを想定した一貫性のあるシステム仕様定義技術、設計技術、保全技術の研究開発
iii. ユーザー視点から情報システムのディペンダビリティを定量的に評価し、経済価値へマッピングする評価技術の研究開発

⑵ 重要インフラ階層

i. フォールトや不正アクセスの存在にかかわらず、相互に依存し合う多様な社会重要インフラのディペンダビリティを恒久的に保証するインフラ・アーキテクチャの研究開発
ii. 重要インフラのライフサイクル・リスクを想定した一貫性のあるインフラ仕様定義技術、設計技術と防衛・保全技術の研究開発
iii. ユーザー視点から重要インフラのディペンダビリティを定量的に評価し、経済価値へマッピングする評価技術の研究開発

⑶ サービス・情報階層

i. フォールトや不正アクセスの存在にかかわらず、ネットワーク化情報システム、社会重要インフラが提供するサービス･情報のディペンダビリティを恒久的に保証するサービス・アーキテクチャの研究開発
ii. サービス・情報のライフサイクル・リスクを想定した一貫性のあるサービス仕様定義技術、設計技術、保全技術の研究開発
iii. ユーザー視点からサービス・ディペンダビリティを定量的に評価し、経済価値へマッピングする評価技術の研究開発

⑷ 情報社会階層

i. システム障害、サイバー攻撃、情報漏洩、自然災害などの発生に際して、被害を最小限度に留めるフェイルセイフな社会システム･アーキテクチャの研究開発
ii. 情報社会が将来に渡って直面するリスクを想定し、ディペンダビリティの実現を促進する一貫性のあるフェイルセイフな社会システムの設計・保全技術とその運用支援ツールの研究開発
iii. 情報社会のディペンダビリティを定量的に評価し、恒久的な安全

信頼保障を科学的方法で確立する情報社会技術・システムの研究開発、政策提言、実装支援と人材育成

上記４階層、１２課題の研究開発は相互に密接に関連するため、同時に推進することが望ましい。（図１相互関連図参照）。しかし、リソースに制約がある場合、必要ならば、技術の緊急性、有効性、独自性、および相互の関連性の観点から、時間軸に沿って研究開発の優先順位を付ける。（図２優先順位図参照）
（表１「提案する内容が最小化する情報社会のリスク」参照）
（コラム②・図３「４階層のディペンダビリティ設計」参照）
（コラム③・図４「ディペンダビリティの実現方法」参照）

表1「提案する内容」が最小化する「情報社会のリスク」

	情報システムのディペンダビリティ実現と評価	社会重要インフラのディペンダビリティ実現と評価	サービス・情報のディペンダビリティ実現と評価	情報社会のディペンダビリティを実現するシステム
システムのブラックボックス化	○	○	○	○
システムの複雑化／巨大化	○	○		
VLSIの微細化	○			
情報量の爆発的増加			○	○
サービス利用の多様化			○	○
システム要素の経年劣化	○	○	○	
責任所在の不明確化		○		○

図1 「提案する内容」の相互関連図

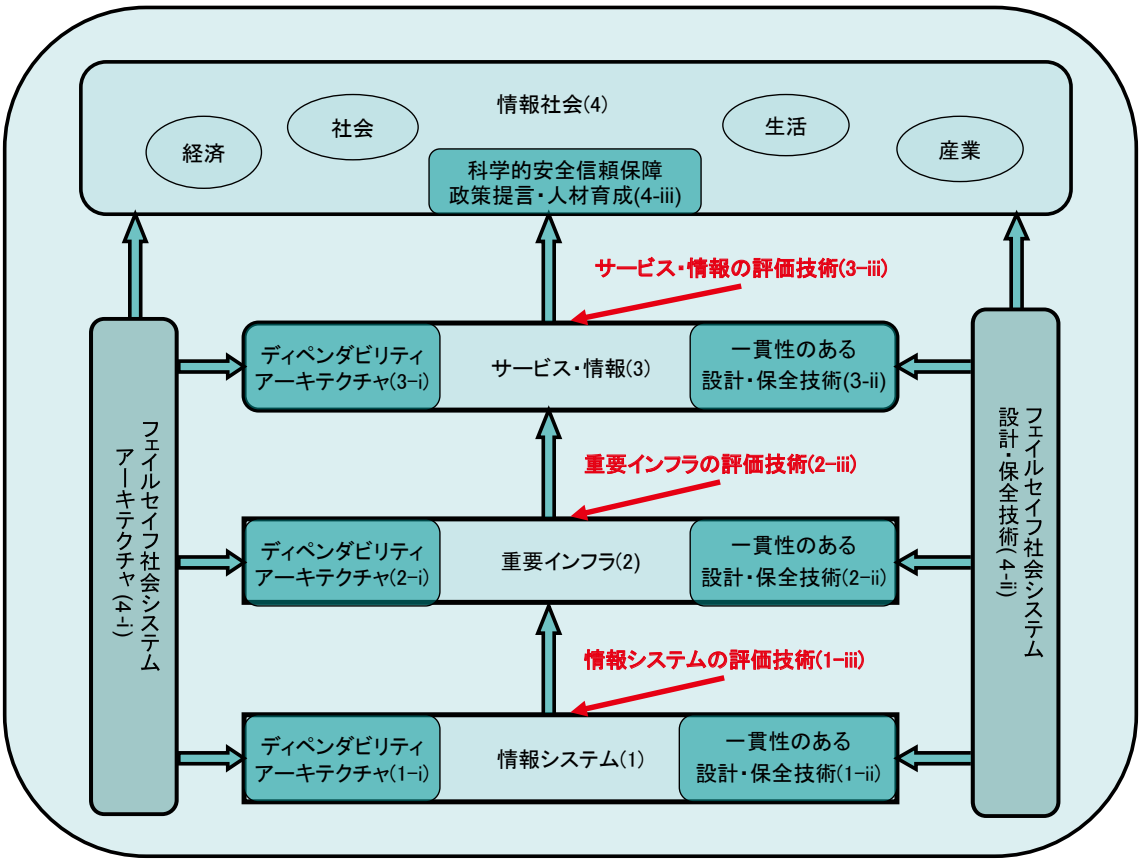
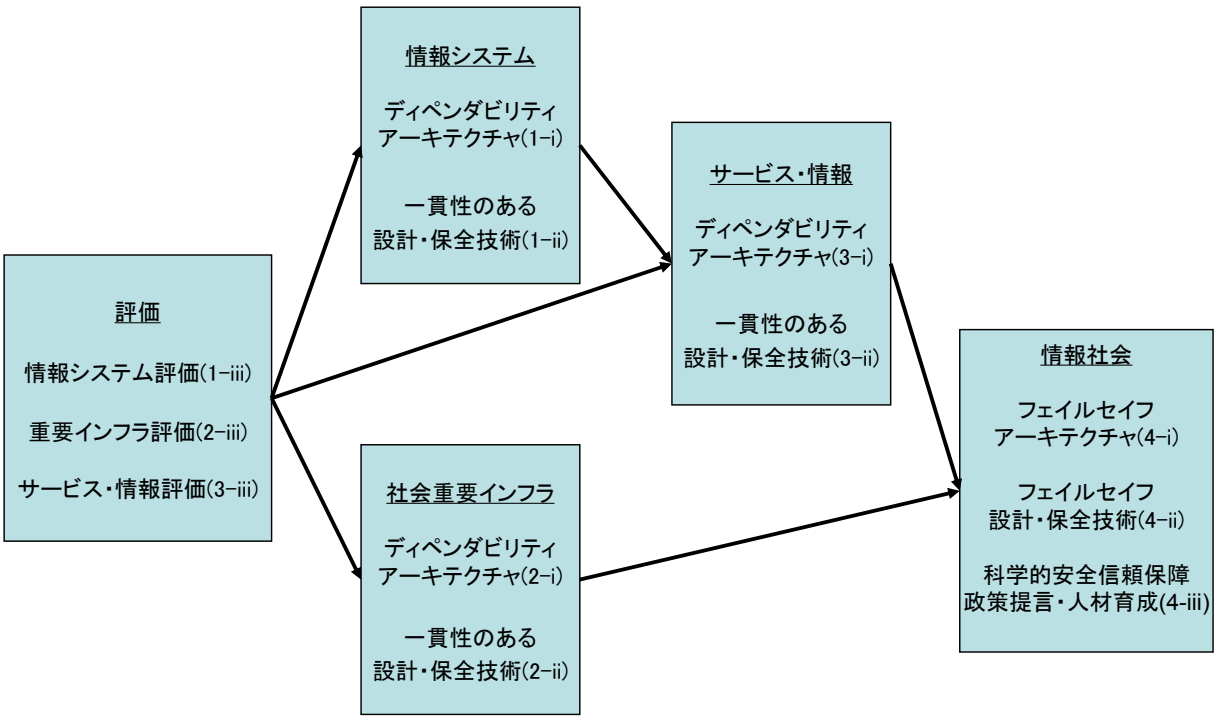


図2 「提案する内容」の優先順位図



コラム ②　4階層のディペンダビリティ設計

情報社会が、様々なフォールトや不正侵入の発生リスクの存在にもかかわらず、社会インフラ、情報環境から提供されるサービスの安全性と信頼性に確信を持つことができる「安全信頼保障」を確立するためには、以下の4階層におけるディペンダビリティ設計が必要である。

1) 社会基盤となるネットワーク化情報システム

情報システムでディペンダビリティ設計とシステム保全アーキテクチャが適切に実現されていれば、たとえフォールトや不正侵入が発生しても、それがシステム障害となって現れることを回避できる。しかし、ディペンダビリティ設計が不適切、不完全な場合には、上位階層とのインタフェースにシステム障害となって現れる。

2) ネットワーク化情報システムを活用して構築される社会の重要インフラ

下位階層の情報システムの障害は、上位階層である重要インフラにフォールトを生じさせることになる。また、重要インフラ自身もフォールト発生や不正侵入の可能性を内在させる。この場合、重要インフラのディペンダビリティ設計とインフラ保全アーキテクチャが適切に実現されていれば、これらのフォールト発生にかかわらず、重要インフラの障害を回避できる。しかし、ディペンダビリティ設計が不適切、不完全な場合には、上位階層とのインタフェースにシステム障害となって現れる

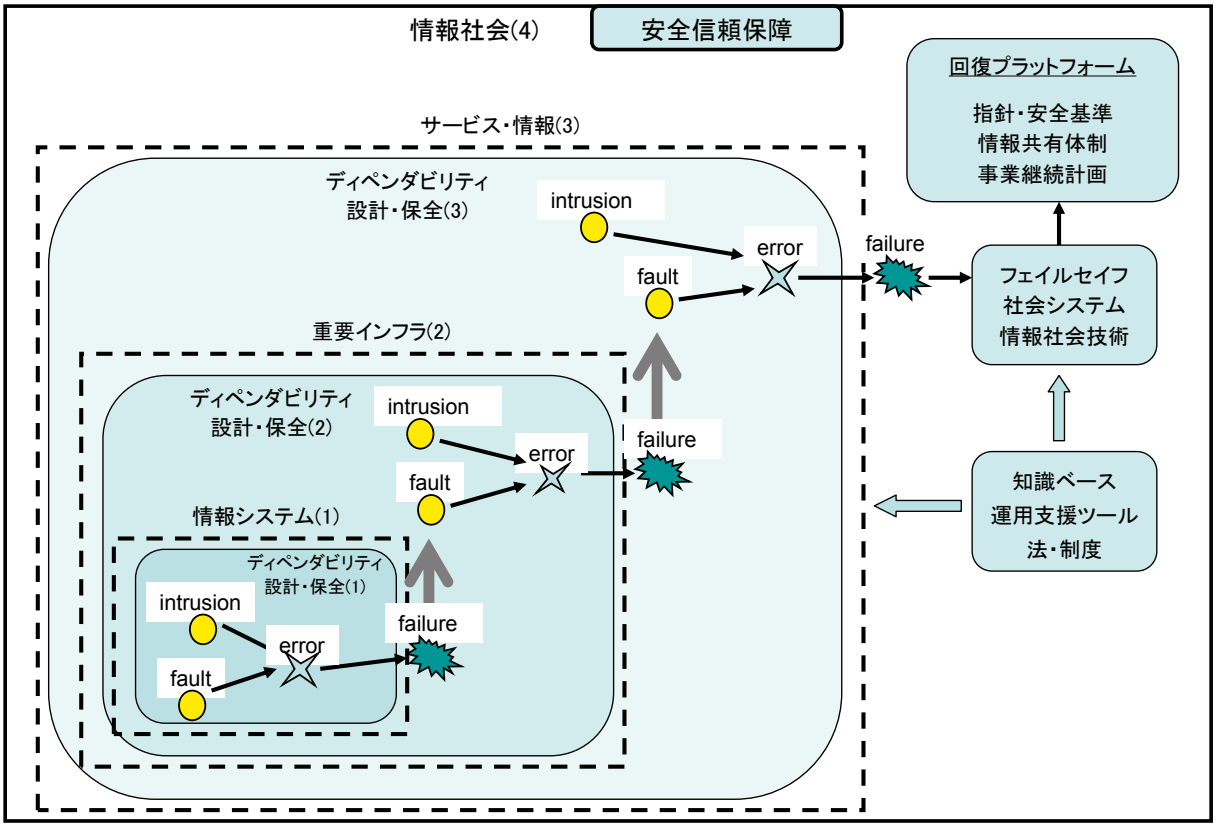
3) 重要インフラを活用して提供されるサービス・情報

重要インフラの障害は、それによって提供されるサービスあるいは情報にフォールトを生じさせる。また、サービス・情報自身にもフォールト発生や不正アクセスの可能性が内在する。この場合、サービス・情報のディペンダビリティ設計とサービス保全アーキテクチャが適切に実現されていれば、これらのフォールト発生にかかわらず、サービス・情報の障害を回避できる。しかし、ディペンダビリティ設計が不適切、不完全な場合には、上位階層とのインタフェースにシステム障害となって現れる

4) サービスを受ける人と組織が形成する情報社会

情報社会の階層で人や組織が受けるサービス・情報にひとたび障害が起きると、これを回避する手段はなく、社会は大きな被害を受ける可能性がある。この場合、障害のために期待するサービスが停止しても、必ず「安全側」でのサービス停止状態になることを保証する「フェイルセイフ」な社会システムが構築されていれば、被害を最小限度に留めることができる。また、適切な回復プラットフォームが構築されていれば、被害を最小限度に留めつつ、社会の活動や事業を要求されるレベルまで早期に回復させることができる。このようなフェイルセイフな社会システムが実現されていれば、社会の「安全信頼保障」に確信を持つことができる。
（図3「4階層のディペンダビリティ設計」参照）

図3　4階層のディペンダビリティ設計



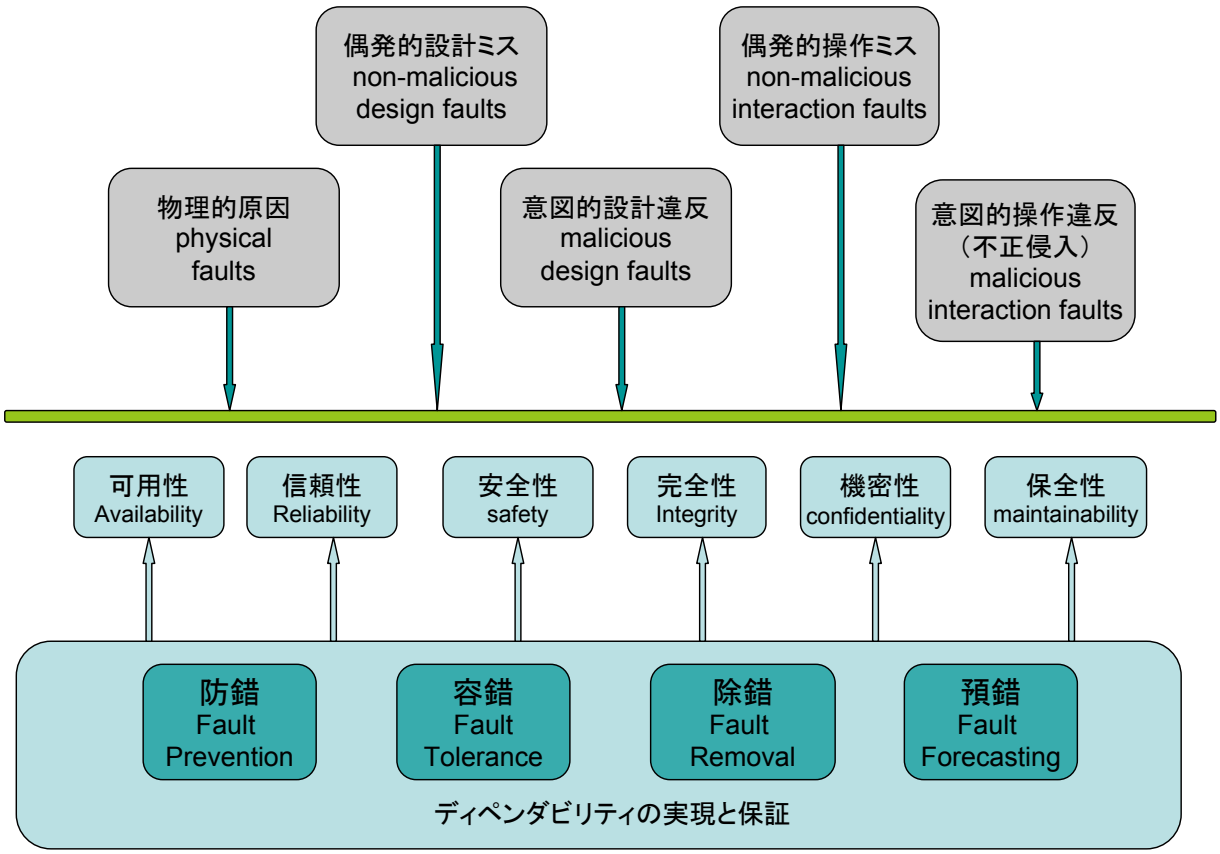
コラム③　ディペンダビリティの実現方法

これまで、ディペンダビリティとセキュリティを実現する多くの方法、手段が開発され、蓄積されているが、これらは次の4つのカテゴリーに類型化される。

- fault prevention（防錯）：フォールトの発生や混入を予防する手段
- fault tolerance（容錯）：フォールトが発生してもサービスの障害を回避する手段
- fault removal（除錯）：フォールトの数や深刻度を低減する手段
- fault forecasting（預錯）：フォールトの現存数、将来の発生と影響を推定する手段

fault prevention（防錯）と fault tolerance（容錯）は信頼できるサービスを提供する能力を実現する方法であり、fault removal（除錯）と fault forecasting（預錯）はシステムに要求される機能とディペンダビリティ／セキュリティが適切に実現されているとの確信を得る方法である。（図4「ディペンダビリティの実現方法」参照）

図4　ディペンダビリティの実現方法



3．今、何故、情報社会のディペンダビリティに研究開発投資をするのか？

世界は情報社会に向かっている。情報社会とは、人と組織のあらゆる活動がネットワーク化された情報システムの提供するサービス、あるいは“情報”に依拠する社会である。今日、個人と社会の活動の根幹を支える重要インフラ（エネルギー網、交通網、情報通信網、金融網、医療網、防災網、防犯網、企業基幹網、行政網など）は情報システムがその基盤を成している。また、これからの情報社会で重要とされるサービス（例えば「新産業創造戦略における重点サービス分野」に掲げられるコンテンツサービス、健康・福祉サービス、ビジネス支援サービス、観光･集客交流サービス、環境･エネルギーサービスなど）の品質と生産性はそれを支える情報システムに大きく依存する。

いわば子供の遊びから国家安全保障まで人と組織のあらゆる活動が情報システムに依拠する情報社会では、ひとたびシステム障害、重要インフラ事故、サイバーテロ、情報漏洩など、社会の期待や合意に反する事象が情報システムに起きると、結果として人命損傷、財産逸失、社会・経済機能マヒなど、社会全体に深刻な事態を招くことになる。場合によっては国家安全保障への重大な脅威になる可能性さえあり、その影響の大きさは計り知れない。

今日のネットワーク化情報社会には、ブラックボックス化、システムの複雑化・巨大化、VLSI の微細化、情報量の爆発的増加、サービス利用の多様化、システム要素の経年劣化、ネットワークにおける責任所在の不明確化など、社会のディペンダビリティを阻害する様々なリスク要因が存在する。（コラム④「情報システムのディペンダビリティを阻害するリスク要因」参照）

また、加速度的に成長するグローバルなネットワークがこれらのリスク要因を一層増幅させ顕在化させる新しい情報環境を生み出している。例えば、グリッドコンピューティング、組込みシステムのネットワーク化、モバイル・システム、P2P ワイヤレスなど、ディペンダビリティ／セキュリティ保証のない新しい情報システムのパラダイムが次々に出現し、それらの無秩序な融合、拡張が進行している。

さらに、情報システム自体のリスク要因に加え、人間や社会構造に起因して、

- 高齢化、知識の偏在のために生じやすくなるシステム操作ミス
- 世代交代の進行によるシステム設計技術、保守技術の空洞化

・ユビキタスコンピューティング環境におけるハードウェアの経年劣化
・技術革新、市場競争が招く製品サイクル短期化によるソフトウェアの経年劣化

なども新たなリスク要因になってきている。

コラム ④　情報社会のディペンダビリティを阻害するリスク要因

a）**ブラックボックス化**：人と社会のすべての活動が依存しているにも拘わらず、情報システムの全容を誰も把握できない。国の重要インフラの相互依存性を含めて、ネットワーク化された情報システムで今何が起きているのか、将来何が起き得るのか、誰も把握していない。

b) **システムの複雑化・巨大化**：システム仕様の不明確化、設計ミス、操作ミス、経年劣化に加えて、複雑に絡み合ったオープンシステムの相互作用、人間とシステムの予期せぬ相互作用が潜在している。このため大規模で複雑化する情報システムの「設計・実現の正しさ」、「運用・保全の確かさ」に確信が持てない状況になっている。

c)**VLSI の微細化**： ハードウェア中枢である VLSI の微細化が進み、リーク電流、発熱、プロセスパラメータ変動、性能変動、ソフトエラー、クロストーク、IR ドロップなど、これまで見られなかった物理現象が、VLSI をハードウェア基盤として構築されている巨大な情報システムの安全性、信頼性に対する深刻なリスク要因になりつつある。

d) **情報量の爆発的増加**：グローバルなネットワーク上で毎日大量に生産され、蓄積され、加工され、流通し続ける巨大な情報量は、人間の処理能力をはるかに超え、その大部分は人間に直接アクセスされることが永久にない。提供される情報の大部分は、検索され、要約され、優先順位づけられた結果である。この情報量の爆発が「情報の安全性、信頼性」に対する脅威であり、情報社会のディペンダビリティ／セキュリティに対する深刻な阻害要因である。

e) **サービス利用の多様化**：日々進化し、変貌し続けるネットワーク化システムには無邪気な初心者ユーザーも悪意の練達ユーザーも等しくアクセス可能であり、また多様なサービスが生まれている。そこに悪意か過失かに関わらず人為的フォールトの生じる可能性がユビキタスに存在し、日常的にシステムを障害、不正侵入、情報漏洩の危険に曝している。さらに世界規模でサイバーテロの脅威が常に存在する。

f) **システム要素の経年劣化**：社会の至る所に埋め込まれた膨大な数のハードウェア要素の物理的な経年劣化に加えて、その上に構築された巨大システムの動作環境変化やシステム更新によって、関連するソフトウェア要素の論理的な経年劣化が潜在的に進行し、その相互依存関係を十分に把握できない状況が生まれている。

g) **責任所在の不明確化**：自律的に発達してきたグローバルなインターネットは、互いに独立に設計された巨大な数の「システムのシステム」であり、明確に定義されないまま拡大を続けている。その結果、ネットワーク化システムで起きた事象、あるは将来起き得る事象に対する責任の所在が明らかでない。

これら様々なリスク要因の相乗効果が、ネットワーク化情報システムにおける物理的なフォールト、人為的なフォールト、システム同士や人間とシステムの間の相互作用によるフォールト、悪意による不正アクセスや不正侵入など、様々なフォールト発生の機会を増やし、結果として、情報社会の根幹を脅かすシステム障害、重要インフラ事故、サイバーテロ、重要情報の漏洩などの重大被害を招く可能性を高めている。

実際、例えば、最近のニュース報道に限っても、メガバンクのシステム障害、東証の売買システム停止、東証「1 円 61 万株」誤発注事件、東京航空交通管制部のシステム障害、防衛省の情報漏洩、全日空発券システムの障害、NTT ひかり電話回線の障害、北東アメリカの大停電、エストニア政府機関へのサイバー攻撃、アメリカ国防総省へのハッカー侵入、ロサンジェルス国際空港入国審査システムの停止、首都圏 JR・私鉄自動改札停止など、情報システムに関わる障害事例は枚挙にいとまがない。
（表２「情報社会のリスク要因が引き起こしたシステム障害事例」参照）
（コラム⑤「情報システムの障害事例」参照）

表2 「情報社会のリスク要因」が引き起こした「システム障害事例」

	メガバンクシステム	東証売買システム	東証誤発注	航空管制システム	防衛省情報漏洩	全日空発券システム	NTT電話回線	北東アメリカ大停電	エストニアDDoS攻撃	米国防総省ハッカー侵入	LA空港入国審査	首都圏JR・私鉄自動改札機
ブラックボックス化	○	○		○				○	○	○	○	○
複雑化巨大化	○	○	○	○		○		○			○	○
VLSI微細化												
情報量爆発的増加					○	○	○		○		○	
サービス利用多様化			○		○				○	○		○
システム経年劣化		○		○		○	○	○			○	
責任所在不明確化	○				○			○	○	○		

コラム ⑤　情報システムの障害事例

1) メガバンクのシステム障害

2002 年 4 月 1 日、第一勧銀・富士銀・興銀 3 行の合併で誕生したみずほ銀行のコンピュータシステムに大規模な障害が発生した。数百万件に及ぶ公共料金の引き落とし漏れ、数万件の二重引き落とし、数千件の企業向け振り込みの遅れ、百件以上の預金残高記録の誤り、旧富士銀の ATM で富士銀以外のキャッシュカード使用不能などのトラブルが相次ぎ、完全に正常化するまでに 1 ヶ月かかった。こうした事態を受けて、金融庁は、みずほグループに、経営責任の明確化や再発防止策の確実な実施を求める業務改善命令を出した。

みずほホールディングスの発表によれば、原因は，旧第一勧銀のホスト・コンピュータと旧富士銀のホスト・コンピュータを接続する部分の不具合だった。具体的には，ホスト・コンピュータ同士のデータのやり取りを中継する「リレー・コンピュータ」と、ホスト・コンピュータとの接続プログラムにバグがあったとのことである。

しかし、真の原因はコンピュータシステムに対する経営陣の認識不足と指摘されている。合併する3行の経営陣は、システム統合の難しさを理解しておらず、当初は、システム統合の責任を負うＣＩＯ（Chief Information Officer）さえ決めていなかったと言われている。現場は、相次ぐ方針転換で混乱をきわめ、2002 年初めの時点でプログラムが完成していないという状態で、テスト不足のまま統合本番を迎えることになった。

なお、2002-03 年には、みずほ銀行以外に、UFJ 銀行、三井住友銀行、りそなグループ、八千代銀行などでも同様の原因でシステム障害が発生している。

2) 東証の売買システム停止

2005 年 11 月 1 日、東京証券取引所（以下、東証と略す）の売買システムに障害が発生し、午前の取引を全面的に停止した。

東証の発表によれば、障害を引き起こした主因は、売買システムの開発・保守を担当する富士通が 10 月 13 日に作成した作業指示書における記載漏れである。いわば、メンテナンスにおける人為的なミスであった。

この作業指示書は、5 月に売買システムを更新した際に混入したバグを修正し、修正後のプログラムを売買システムに再登録するためのもので、富士通が作成し、運用担当ベンダーである東証コンピュータシステム（TCS）に送付された。売買システムのプログラムは COBOL で記述されている。COBOL では、複数のサブモジュールをつなげて、一つのプログラムを構成する。10 月 13 日の作業指示書には、サブモジュール間の呼び出し関係を指定し直す手順が抜けていたため、プログラムの中の古い呼び出し関係が、書き換えられることなく残ることになった。

これが毎月末に実施する「コンデンス」処理で顕在化した。コンデンスは、ファイルの読み書きを繰り返して使用しなくなったディスク領域を解放して再利用できるようにするための処理である。10 月 31 日のコンデンス処理では、13 日に再登録したサブモジュール間の呼び出し関係をシステムが自動検証した結果、これらを別個のモジュールと判断し呼び出し関係を切断した。翌 11 月 1 日朝、参加者データ・ファイルを読み込むプログラムが起動したものの、正しいサブモジュールを呼び出せず、読み込みに失敗したため、売買システムは起動しなかった。

3) 東証の「1 円 61 万株」誤発注事件

2005 年 12 月 8 日、証券会社の株式売買担当者が東証マザーズ市場において、「1 株 61 万円で売り」の注文を出すところを、誤って「1 円で 61 万株売り」の注文を出し、その取り消しができなかったため市場は大混乱となり、証券会社も巨額の損失を出した。

この事件の原因は、 1）売買担当者の不注意による入力ミス、 2）「売買取り消し」の処理ソフトウェアにバグがあったこと、3）東証側のシステムが「おかしな」注文であってもそれは証券会社側がチェックした結果だから受け入れるという方針で構築されていたため、「非常識な」注文内容がそのまま市場に出たこと、4）証券会社側の発注システムには一定の制限を超えると警告が出る仕組みがあったが、この警告は極めて頻繁に出るため、警告が出ても無視する ことが通常の状態であったことなど、人間をループに含む情報システムにおいて、設計ミス、操作ミス、運用ミスなどの人為的なフォールトが重なったことにある。

4) 東京航空交通管制部のシステム障害

2003 年 3 月 1 日、東京航空交通管制部で日本上空の飛行計画を一括管理する飛行計画情報処理システム（FDP）に障害が発生し、全国の空港で、欠航 215 便、大幅な遅延 1500 便以上、足止めされた客 30 万人以上とシステム障害による被害として航空史上最大規模になった。

直接の原因は、このシステムで各航空機の管制業務に必要な便名、行き先、飛行経路などの情報を全国各地の管制部門に対して出力するプログラムに存在したバグにあった。このプログラムを前年 9 月に開発したＮＥＣは 1 月にはこのバグを発見していたが、あるデータが主メモリの特定の位置に格納されたときだけに発生するもので表面化することはないと判断してそのまま放置していた、というミスが重なった。その結果、3 月に防衛庁と飛行計画データをやり取りする「防衛庁システム対応プログラム」を FDP に追加した際、誤作動が生じる条件が整って、システムダウンが発生したものである。また、FDP はこうした事態を防ぐ『フェイルセーフ機能』を実装しているが、オンライン統計処理プログラムに関する処理には、同機能を適用していなかった。さらに、割り当てられたデータ領域の範囲をチェックする機能があれば、所定の範囲を超える問題は発生しなかった。すなわち、ソフトウェアの設計ミスにシステムのメインテナンスミス、運用ミスが重なった人為的フォールトによる障害だった。

なお、2004 年 4 月 8 日にも東京航空交通管制部の航空路レーダー情報処理システム（RDP）で２重系運用しているハードが２台ともダウンする障害が発生し、少なくとも国内空港を出発する航空機 120 便に 30 分以上の遅延が生じた。原因はソフトウェアのバグとされている。

5) 防衛省の情報漏洩

2004 年頃から、政府機関、自治体、防衛省、警察、企業などの保有する機密情報、個人情報が、P2P ファイル共有ソフト Winny を利用したスパイウェア Antinny に感染して個人用 PC からネットワークへ流出する例が頻発している。

防衛省関連のごく最近の例では、

- 2006 年 2 月、海上自衛隊佐世保基地配備の護衛艦「あさゆき」の電信室所属通信員（曹長）の私物 PC から自衛艦のコールサイン一覧、隊員名簿等の個

人情報、「極秘」とされる暗号書や乱数表などの文書名一覧表などの流出が発覚。
- 2006 年５月、陸上自衛隊久里浜駐屯地の通信学校で使用されていた地対艦誘導弾（SSM-1）システムに関する教育用資料の流出が発覚。
- 2006 年８月、陸自第１４旅団（香川県善通寺市）に所属する３等陸曹の私物パソコンから陸上自衛隊の訓練などに関する内部資料の流出が発覚。
- 2006 年 11 月、航空自衛隊２等空尉の私物 PC からイラクなど中東地域担当の米中央軍が一定期間秘密指定していた輸送業務の態勢表、「指定前秘密（秘）」扱いの航空総隊司令部の実動演習の部隊用資料などの内部資料流出が発覚。

軍事機密情報が簡単に筒抜けになったことに危機感を持った防衛庁（当時）は 2006 年２月、軍事機密情報の保守施策として私物パソコンの持ち込みを厳禁したほか、DELL より 40 億円分のパソコンを緊急調達し隊員に割り当てた。しかしその後も内部資料の流出（武器庫内見取り図や部内専用の訓練資料、隊員名簿・住所録等の個人情報）は後を絶たず、防諜体制の不備が国内外から懸念されており、情報管理体制の強化が当面の課題の一つとなっている。

Winny による情報流出事件は今後も続くと考えられている。 防衛省以外でも、警察から捜査資料・被害者情報、学校から生徒個人情報、病院から患者カルテ情報、企業から顧客情報、県会議員から後援会情報、プラントエンジニアリング社員から原発内部技術情報、刑務所から受刑者情報、裁判所から競売情報、放送局から出演者情報、航空会社から空港制限区域暗証番号など、様々な重要情報・個人情報の流出発覚が続いている。

6) 全日空発券システムの障害

2007 年５月 27 日、全日空の国内線予約・搭乗手続きシステムに障害が発生した結果、130 便が欠航、306 便が遅延し、８万人弱の旅行客に影響が出た。

システム障害の発生箇所は「総合旅客システム（able-D）」と呼ばれる全日空グループの予約・発券システムのうち、国内旅客系に関するホスト端末間（全６系統中３系統）であった。障害が発生した３系統（サーバ３台）は５月上旬から 24 日まで２週間かけてアプリケーションの更新を行っており、26 日になってから原因不明の処理速度低下が起きていたとされる。

全日空は、空港にある端末とホストコンピュータを結ぶネットワーク機器のメモリ故障が原因でホストと端末との間の通信が滞ったため、ホストにデータが滞留し、長時間にわたって予約や発券、搭乗手続きができないというシステム障害につながったとする調査結果を発表した。

7)NTT ひかり電話回線の障害

NTT グループの IP 電話サービス「ひかり電話」に、ネットワーク・トラフィックの巨大化、システム複雑化に対応しきれない設計ミス、メインテナンス・ミスに起因すると思われる障害が各地で頻発している。

- 2006年９月19-21日、NTT東日本の「ひかり電話」に障害。約80万人のユーザーに影響。原因は呼制御サーバーで、主に企業で使われる代表番号に関連する機能のソフトウェアの不具合。着信した呼を同一グループに設定した電話機に順番に振り分ける機能の処理が大幅に増加したことで，ソフトウェアに不具合が発生して呼制御サーバーの輻輳を引き起こした。その影響が中継系の呼制

御サーバーにも及び，輻輳の範囲が拡大した。

- 2006 年 10 月 23-25 日、NTT 西日本で障害発生。23、24 日に発生した障害は容量設計のミスに伴う「呼処理サーバー」に発生した負荷が限界を超えたため。25 日に発生した障害は状況の推移を見守ろうとして接続可能な回線数を制限したことにより空いた回線の奪い合いが発生し、制御信号の衝突処理が中継系呼制御サーバーの処理を圧迫するという予想外の事象が発生したことが原因。
- 2007 年５月 23 日、NTT 東日本と西日本の間で約４時間不通。東西 NTT 合計で約 318 万回線のひかり電話が影響を受けた。問題を起こしたのは、両社のひかり電話網をつなぐ中継網内の呼制御サーバー。メンテナンス担当の NTT-ME は５月 21 日深夜から 22 日早朝にかけて呼制御サーバーのハードディスクを予防的な保全作業で交換したが、その際に作業員が入力したコマンドに誤りがあり、ハードディスク内の一部データが損壊した。そして 23 日午前６時 25 分、損壊したデータが呼制御サーバーのメモリに読み出されダウンしてしまった。問題となった呼制御サーバーには、待機系のサーバーとハードディスクも用意されていたが、待機系に切り替わるのはサーバーのハードウエア故障の場合で、今回のようなソフトウェアに起因するケースでは機能しなかった。手動で待機系に切り替えることも可能だが、その措置はとらなかった。
- 2007 年５月 16 日、NTT 東日本のネット接続サービス「フレッツ」と IP 電話「ひかり電話」が前日夕から約７時間にわたって一部に障害。影響を受けたのは、フレッツサービス約 239 万契約（B フレッツ約 100 万契約、フレッツ ADSL 約 126 万契約、フレッツ ISDN 約 13 万契約）と、ひかり電話約 50 万契約。NTT 東日本の発表によれば、同社ビル内に設置したルータ１台にハード故障が発生し、パッケージを交換した際、全ルータでルート情報の自動書き換えが行われた。その際に処理能力を超えるルート情報が発生し、連鎖的に多くのルータで処理能力オーバーとなり、パケット転送処理を自律停止するに至った。

8) 北東アメリカの大停電

2003 年８月 14 日午後４時過ぎ、アメリカ合衆国、カナダにまたがる北東アメリカで世界最大規模の大停電が起きた。アメリカ 4000 万人、カナダ 1000 万人の計 5000 万人が停電の被害を受け、この停電による経済損失は 60 億ドル（約 7000 億円）と見積もられた。特に、航空会社や証券取引所は、この日だけで大赤字となった。

ニューヨーク、クリーブランド、デトロイト、ボストン、トロント、オタワなどの大都市では自動車道路が歩道となって交通麻痺となったため、公園や路上で一晩を明かす仕事帰りの人や学生などが多く出た。真夏のことで翌日の日中は気温が 30℃以上になったが、エアコンや扇風機は使用できなかった。

停電が発生した８月 14 日は、MSBlast ワームが拡大を開始したわずか３日後であった。そのため、急速に増殖する同ワームが直接的あるいは間接的な原因となって連鎖的停電を引き起こし、最終的にニューヨーク、トロント、デトロイトといった主要都市の大停電に発展したのではないかとの憶測を呼んだ。

2004 年４月５日、米加合同の調査特別委員会は、停電は組織的ミス、人為的ミス、コンピュータの障害が複合的に連鎖して発生したもので、MSBlast ワームが原因

ではないとの最終報告書を発表した。同報告書によると、確かに主要電力網の状態を監視するソフトウェアを実行していたサーバーとそのバックアップなど、いくつかのコンピュータシステムが故障したが、FERC（Federal Energy Regulatory Commission）が設置した特別調査委員会 U.S.-Canada Power System Outage Task Force の作業部会 Security Working Group の調査によると、誰かが悪意をもって停電に直接的あるいは間接的に関与した証拠はなく、また停電の発生当時にインターネットに広まっていたワームやウィルスが、停電と直接関わりのあった電力会社の発電・送電システムに影響を与えた証拠も見当たらなかった。

同報告書は、Midwest ISO と FirstEnergy（米国北東部および中西部で事業展開する電力会社７社からなるグループ企業）におけるシステム障害と人為的ミスの複合的連鎖が停電の根本原因だったと、結論づけている。

9) エストニア政府機関へのサイバー攻撃

2007 年４月 27 日から約３週間にわたって、エストニアの大統領府や政府、国防省、外務省など多数の政府機関と主要な銀行や新聞社が猛烈なサイバー攻撃を受けた。遠隔操作で数百、数千台のコンピュータから一度に大量のアクセスを標的のインターネット・サイトに集中させて、そのネットワークサービスを不能にする DDoS(Distributed Denial of Service) 攻撃であり、攻撃を受けたサイトは停止などに追い込まれ、一時は携帯電話網や救急ネットワークも攻撃を受けた。

エストニア政府は４月 27 日に、第二次大戦でのソ連軍の勝利を記念した銅像を首都タリンの中心部から郊外に移転した。これに対してロシアは「戦死者に対する冒涜（ぼうとく）だ」などと猛反発し、政財界の有力者がエストニア製品のボイコットや経済制裁を呼びかけるなど両国関係は急激に悪化していた。

エストニアは、一部の発信元がクレムリンやロシア政府のコンピュータであると主張し、北大西洋条約機構（NATO）は事実関係の究明と防衛策の構築支援を目的に電子犯罪の専門家をエストニアに派遣し、調査に乗り出した。一方、クレムリンの報道官は再三にわたってロシアの関与を否定し、ハッカーがクレムリンや公的機関のコンピュータを装って攻撃を仕掛けている可能性を指摘した。真相は不明である。

10) 米国国防総省へのハッカー侵入

米国の国防総省（ペンタゴン）によれば、2007 年６月、ペンタゴンのコンピュータネットワークがハッカーに侵入されたため、ロバート・ゲイツ国防長官執務室の電子メールシステムを含む一部のコンピュータシステムを停止させ、ネットワークから切り離した。切り離されたシステムはその後３週間は復旧しなかったが、国防総省のオペレーションに重大な影響はなかった。

英経済紙フィナンシャル・タイムズはペンタゴンの信頼できる筋からの確度の高い情報として、「ハッカーは中国人民解放軍に所属しており、人民解放軍が関与している可能性が高い」と報道した。

中国政府は、一貫してサイバー犯罪を取り締まっているとして、これを否認している。

人民解放軍は定期的に米国の軍事ネットワークを監視しており、ペンタゴンも中国のネットワークの監視を続けていると言われているが、米国高官は、今回の侵入は軍事関連のコンピュータシステムを停止に追い込む技術レベルを示すもので、中

国の脅威に懸念を表明した。ペンタゴンは現在、今回の侵入でどれだけの情報がダウンロードされたか調査中であるが、ほとんどの情報は機密指定のない情報とされている。

なお、ドイツと英国のいくつかの政府機関のコンピュータシステムにも同様な中国を発信元とするハッカーからの侵入があったと報じられている。

11) ロサンジェルス国際空港入国審査システムの停止

2007 年８月 11 日、米国ロサンジェルス国際空港の税関・入国審査システムが９時間にわたって停止し、その間、入国審査ができず、到着便の１万７千人以上の旅客が飛行機の中にそのまま最大で６時間も閉じこめられた。数千人の乗り継ぎ客は空港周辺でホテルを探さねばならなかった。さらに、翌 12 日に前日とは無関係の別の障害が発生し、空港の 29 台の端末の接続が切れたため、数千人の旅客に影響が出た。

全国データベースとの接続も空港内 LAN との接続も切断されたため、入国審査ができず、数時間後にバックアップシステムに切り替えたが、処理量は通常システムの半分だった。

原因はデスクトップコンピュータに搭載されたネットワーク接続カードの不具合であったことが判明した。欠陥のあるネットワーク接続カードによるネットワークアクセス速度低下がドミノ効果によって空港の税関・入国審査ネットワーク全体に拡大し、障害の連鎖に発展した。

12) 首都圏 JR、私鉄自動改札システムの障害

2007 年 10 月 12 日早朝首都圏で、「Suica」を発行する JR 東日本 192 駅と、「PASMO」を発行する私鉄、地下鉄の 470 駅で、始発電車の業務に向けて自動改札システムを立ち上げたところ起動せず、利用者が自動改札ゲートを通過できない広域の障害が発生し、朝の通勤ラッシュ時に各駅で 260 万人の足に影響を与えた。

自動改札機を運営する関東 IC カード相互協議会、PASMO 協議会、JR 東日本によれば、原因は、不正カード情報を自動改札機に配信する際の送信データがある長さ、ある件数になるという条件が重なった場合に読み込み不能になるという潜在プログラムミスが当日顕在化したため。今後の防止策として、データ配信時のチェック箇所増強、プログラム設計審査の充実、ソフトウェア検証自動化の推進などを挙げている。

なお、JR 東日本では、2006 年 12 月１日にも「Suica」の使える首都圏 511 駅の３分の１以上の 184 駅で利用者が改札ゲートを通過できなくなる大規模な障害が発生している。原因は潜在していたプログラムミスが 11 月から 12 月に日付が変わった時点で顕在化したためとされる。

情報社会の目指すべき姿は、様々なリスク要因の存在にもかかわらず、人や組織が致命的損害を被らないことを保証され、社会インフラ、情報環境から提供されるサービスの安全性と信頼性に揺るぎない確信を持ち、安寧な生活、十全な活動を展開できるディペンダブルな社会である。

このようなディペンダブルな情報社会の建設には、

1) 社会基盤となるネットワーク化情報システム
2) ネットワーク化情報システムを活用して構築される社会の重要インフラ
3) 重要インフラを活用して提供されるサービス・情報
4) サービス・情報を享受する人と組織が形成する情報社会

の４階層のすべてにおいて、ライフサイクル・リスクを想定したディペンダビリティを実現し、評価し、恒久的に保証するアーキテクチャとシステム設計・保全技術の総合的な研究開発が必要である。

情報社会のディペンダビリティとセキュリティに関して、2001 年９月 11 日の惨事以来､欧米では「これまでは単なる想像に過ぎなかった事柄が今や現実である。これまでは思いも及ばなかった事柄が今は想像できる」という認識が浸透した。その結果、1) 国の重要インフラ防衛への関心の急速な高まり、2) ネットワーク化情報システム全般の安全信頼保障に関する研究の活発化、3) ディペンダビリティとセキュリティの融合化、4) 重要研究領域への投資に関する欧州 (EC) と米国（NSF, DHS）の政策当局の連携、などが起きている。

世界のこのような状況を背景に、事柄のグローバルな性質に鑑み、我が国においても早急に、情報社会の安全信頼保障に向けた研究開発を長期的視野で戦略的に推進する必要がある。特に、基盤となるネットワーク化情報システム、およびそれを活用して構築された社会の重要インフラの防衛・保全体制を早期に確立するための技術とシステムの開発は焦眉の急である。

一方で、「ディペンダビリティ」は情報社会における安全信頼保障の要となる技術概念であり、将来を見据えた情報社会のグランドデザインに当たって最高の価値として科学技術が目指すべき普遍的な目標理念である。技術の進歩と社会・環境の変化に対応して新たに生じ得る様々なリスク要因の絶え間ない検証と、それに基づいた情報社会システムのアーキテクチャと設計・保全技術のダイナミックな更新によって、情報社会の安全と信頼を恒久的に保証するため、ディペンダビリティの確立と維持に向けた基盤的課題の総合的研究開発を戦略的かつ永続的に推進する必要がある。

情報社会におけるディペンダビリティの恒久的保証は、我が国社会の安全信頼保障の要諦であり、国が永続的に追求すべき最優先の政策課題である。従って、提案する内容の実現・実践には国による研究開発投資が適切であり、また必要である。

特に、提案内容を特徴づける以下の２点を効果的に実施するためにも、国の研究開発投資による誘導が必要である。

1) エネルギー確保、医療・福祉、環境保全などのような公共サービス分野、あるいは電力網、交通網、金融網、防災網などのように社会の重要インフラ分野におけるディペンダビリティの公共的価値の評価から出発し、情報システムのディペンダビリティを市場の評価で定まる経済的価値へマッピングする段階に至るまでは、国による研究開発投資が適切である。市場における経済価値評価が可能になった段階で民間による研究開発投資のインセンティブが必然的に生まれる。その結果として、新しい経済価値に基づく国際競争力の源泉が創出されることが期待できる。

2) サービス品質の保証にかかわる基本的な技術概念であるディペンダビリティは、本来、我が国の産業社会において伝統的に培われてきた得意分野であり、我が国発の国際標準制定に照準を合わせた研究開発を推進すべきである。その場合、民間投資だけでは困難であり、第３者的立場である大学、国研などの活動が重要な役割を果たすため、国の研究開発投資による誘導が必要になる。

提案する研究開発の戦略的かつ永続的な推進に国が投資する積極的意義は、大きく以下の３つにまとめられる。

第一の意義は、情報社会の安定化である。国家の基盤、企業活動の基盤、生活の基盤であるネットワーク化情報システム、社会の重要インフラの安全性・信頼性を確保し、人や組織の活動が依拠するサービスと情報に対する信用を保証し、情報社会の安全と信頼を恒久的に保証するシステムを確立することによって、情報社会の安定化と将来の発展が確保される。

第二の意義は、新しい経済価値に基づく国際競争力の新たな源泉創出である。ディペンダビリティの定量的評価指標の確立、経済価値へのマッピングとその可視化によって市場における経済価値評価の対象となり、ディペンダビリティを最優先の設計目標とする技術開発促進への企業インセンティブが生まれる。その結果、産業の国際競争力強

化、国際標準化への主導的貢献など、国際社会において我が国が先導的役割を果たし続けることが期待できる。

第三の意義は、新しい学際分野「情報社会技術」の創出である。情報社会におけるディペンダビリティ／セキュリティの価値に関する社会的合意形成のプロセスを通じて、社会の安全・信頼を保障する科学的方法論としての「情報社会技術」が創出され、それが情報社会の健全な発展を促す政策立案と社会実装への支援ツールを提供するとともに、人材育成のプラットフォームになる。

（コラム⑥「サービスの社会的価値と経済的価値」参照）

コラム ⑥　サービスの社会的価値と経済的価値

社会的価値とは、安全保障、エネルギー確保、医療･福祉、環境保全などのように、公共社会の利益あるいは国家の利益になると政府が判断して、政策として提供するサービスの価値をいう。経済的価値とは市場の評価(需給関係)で定まる価値である。経済的価値の評価者が市場であるのに対して、社会的価値の評価者は政府・政権担当者であり、政府の評価者は納税者である。公共サービスが民営化され、競争市場が創られると、公共サービスに経済的価値が生まれる。

4. 情報社会のディペンダビリティに関する研究開発の推進方法

我が国では、情報セキュリティに関する研究者あるいはディペンダブルコンピューティングに関する研究者の研究実績はかなりあるが、それらを統合して学際横断的に研究している研究者の数が欧米に比較して少ない現状を考慮すると、個別の研究者に資金を支給する方式ではなく、以下のように２段階に分けた戦略的かつ永続的な研究開発の推進が適切である。

まず第１段階では、大学の研究者を中心として、ネットワーク化情報システム、重要インフラの担当省庁及び事業実施者との連携のもとで前記の４階層の研究開発計画をプロジェクト的に早急に立ち上げる。

次に第２段階で、３年以内を目途として、重要インフラやサービス・情報分野および社会技術・社会システム分野も含む情報社会の安全信頼保障に関する基盤技術の永続的な研究開発を戦略的かつ集中的に推進する研究拠点を設置し、上記の研究開発計画と成果をこの新設研究拠点に集積する。拠点は必ずしもひとつとは限らず、２、３カ所の拠点が相補的、競争的、協調的に機能するのが効果的と思われる。

この新設研究拠点は、技術の進歩と社会・環境の変化に対応したPDCA (Plan, Do, Check, Action) サイクルを通じて、恒久的に「社会の安全信頼保障」を維持・進化させる情報社会技術・情報社会システムに関する基盤的研究開発の推進、人材育成と国際ネットワーク形成、政策提言と実装支援を行うナショナルセンターとして機能させるべきである。

新研究拠点のイメージを以下に例示する。

1) ミッション：情報社会のディペンダビリティを恒久的に保証する情報社会技術・システムに関する基盤的研究開発の推進、人材育成と国際ネットワーク形成、政策提言と実装支援を通じて、情報社会の安全信頼保障の実現に貢献する。

2）研究戦略：欧州、米国におけるこの分野の研究は国家安全保障あるいは国土防衛をターゲットとしているのに対して、本研究拠点のターゲットは「情報社会の安全信頼保障」である。このターゲットへ向けた研究戦略として、今後重要な研究課題になるが、まだ欧州、米国ではそう認識されていない、あるいはまだ着手されていない課題に

研究の重点を置く。具体的には、

- ユーザー視点の環境適応メトリクスとその評価技術
- サービスレベルからシステム設計レベルまで一貫性を保つ階層的仕様定義
- サービス品質の可視化とその経済価値へのマッピング
- サービス・情報のディペンダビリティ・アーキテクチャと設計・保全
- サービス・情報のディペンダビリティの定量的評価とその保証
- フェイルセイフ社会システムのアーキテクチャと設計・保全

などはその例であり、本研究拠点における研究戦略の中心課題になり得る。国際標準化と我が国における認証機関の設置を視野に入れた研究推進を行う。

一方、重要インフラの防衛に向けたシステム解析、評価、保証技術の研究は、欧米においても国家安全保障に関わる科学技術政策の重要課題として認識され始めているが、我が国においても「情報社会の安全信頼保障」の視点から独自に推進すべき緊急課題であり、関連省庁、事業実施者との十分な連携が必要である。

３）研究領域：前記４階層の研究項目を軸とし、ディペンダビリティとセキュリティを目標理念として情報技術と社会技術を融合した「情報社会技術」を研究領域とする。研究者の専門領域は、コンピュータ科学、応用数学、情報通信工学などを主体とする情報コア分野、自動車、ロボティクス、宇宙航空、エネルギー、生産技術、医療工学、ビジネス、サービスなどの情報応用分野、法律、経済、金融、心理学、社会学、教育学などの社会技術分野を想定する。

４）規模と構成：専任のシニア研究者（プロジェクトリーダー）と併任・流動研究者を合わせて相当規模の研究者集団とする。また段階的に連携大学院制度を活用した博士課程大学院学生、政府出資金受託プロジェクトによるポスドク研究者、民間受託プロジェクトによる常駐の企業派遣研究者を想定する。また欧州、米国の関連分野研究拠点との連携プログラム（研究者交換、共通ベンチマーク／テストベッド／データセット構築など）も想定する。

フランスの LAAS-CNRS と米国の UIUC-ITI は、現時点で情報システムのディペンダビリティに関して世界をリードする研究拠点であるが、そのカバーしている研究開発分野は限定的である。（コラム⑦：「ディペンダビリティに関する欧米の研究拠点の例」参照）

本イニシアティブの「提案する内容」は、情報社会を構成する４つの階層、すなわち、「情報システム」、「重要インフラ」、「サービス・情報」、「情報社会」のそれぞれにおいて、ディペンダビリティを恒久的に保証する当該階層のアーキテクチャ、ライフサイクル・リスクを想定した当該階層の設計・保全技術、当該階層のディペンダビリティの定量的評価技術に関する研究開発、政策提言、実装支援、人材育成の戦略的かつ永続的な推進である。これに対して、LAAS-CNRS の活動は、現時点で「情報システム」及び「重要インフラ」の研究開発に限定されている。また UIUC-ITI の活動は、「情報システム」、「重要インフラ」に加えて、NSA Center for Information Assurance Education に見られるように、「サービス・情報」分野の一部の活動も見られるが、その関心の範囲は限定的である。「提案する内容」と比較して、LAAS-CNRS と UIUC-ITI がカバーする範囲を図に示す。（図５「提案する内容」の研究領域」参照）

欧州と米国のファンディング当局間の連携への動きが進んでいることから、我が国においても、情報社会先進国との間で相互に補完関係にあって共同研究が効果的な分野に関して具体的な国際連携実現へ向けた働きかけを行うことが望ましい。

コラム ⑦　ディペンダビリティに関する欧米の研究拠点の例

情報システムのディペンダビリティに関する世界の研究拠点としてフランスの LAAS-CNRS と米国の UIUC-ITI が代表的である。

i) LAAS-CNRS

フランスの国立科学研究機構 CNRS (Centre National de la Recherche Scientifique) に属する LAAS(Laboratoire d'Analyse et d'Architecture des Systemes) は Toulouse に立地するシステムアーキテクチャ・解析研究所である。2006 年度時点で、シニア研究者 182 名（内、101 名は大学教授を兼任）、技術支援スタッフ 70 名、事務支援スタッフ 44 名、学生（博士課程、ポスドク）285 名であり、年間予算規模（人件費を含む）は 2893 万ユーロ（約 48 億円）である。全部で１７ある LAAS の研究グループの一つが Dr.Jean-Claude Laprie を中心とする "Dependable Computing and Fault Tolerance" グループであり、18 名の常勤シニア研究者（その内６名は大学教授を兼任）と 17 名の Ph.D 学生が政府予算に加えて競争的研究資金（受託プロジェクト）を得て働いている。このグループはこれまでディペンダビリティ基本概念の提案などで世界をリードしている。現在、以下の研究テーマに関するプロジェクトを実施している。

- Security: Security Policies, Access Control for Privacy, Distributed Authorization Scheme, Intrusion Tolerance
- Algorithms & Architectures: Mobile Systems, Service Oriented

Architectures, On-line Adaptation & Reflexive Computing, Multi-level Integrity, Safety-critical Autonomous Systems, Dependable Nano-architectures
- Software Testing: Proof-based Testing, Robustness Testing, Testing of Mobile Systems
- Analytical: AADL-based Dependability Modeling, Evaluation of Security, Assessment of Dependencies in Critical Infrastructures
- Experimental: Measurement of Critical Execution Times, Characterization of Intrusions(Honeypots), Benchmarking wrt Accidental Faults & Intrusions

ii) UIUC-ITI

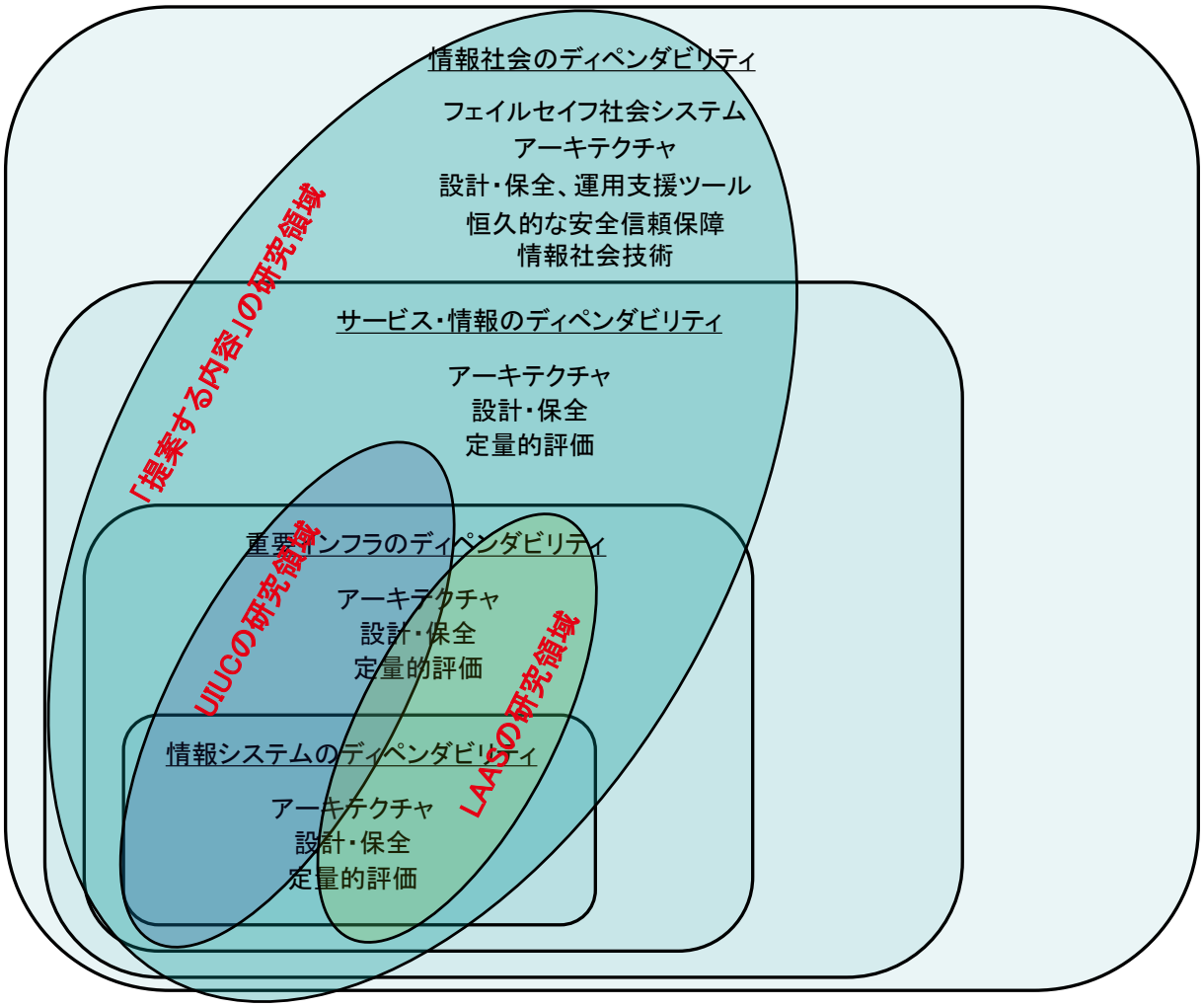
UIUC（University of Illinois at Urbana-Champaign）内に設置されているITI(Information Trust Institute) は、イリノイ大学のComputer Science, Electrical & Computer Engineering, Aerospace Engineering Industrial & Enterprise Systems Engineering からのファカルティの他にCollege of Law, College of Business, department of Mathematics, National Center for Supercomputing Applications (NCSA), and Coordinated Science Laboratory などから87名のシニア研究者（プロジェクトリーダー）が大学院併任で参加している。この他に多数の博士課程学生、企業研究者が競争的研究資金（受託プロジェクト）や産学連携研究資金のもとで、主として、電力網システム、銀行システム、防衛システム、国土安全保障などの応用分野をターゲットにした多くの研究プロジェクトを推進している。

これらの研究プロジェクトのテーマは大きく３つの分野に分かれる：
- Critical Infrastructure & Homeland Defense
- Embedded & Enterprise Computing
- Multimedia and Distributed Systems

また、政府機関や民間企業との連携研究のために７つのセンターが設置されている:
- Boeing Trusted Software Center
- Center for Autonomous Engineering Systems and Robotics
- Center for Information Forensics
- National Center for Advanced Secure Systems Research
- NSA Center for Information Assurance Education
- Trustworthy Cyber Infrastructure for Power Center
- Trusted ILLIAC

さらに、高校生、大学、大学院、社会人向けに多様な教育プログラムを実施している:
- Short course on cyber trust and cyber security
- ITI-approved certificate programs
- A planned information trust and security specialization

図5 「提案する内容」の研究領域



5. 科学技術上の効果

1) 新しい学際分野「情報社会技術」の創出

情報社会におけるディペンダビリティ／セキュリティの実現と保証には、情報技術とともに社会システム、社会技術と呼ぶべき概念、技術、プロセスが必要である。その結果、必然的に情報技術と社会技術が融合する新しい学際分野「情報社会技術」が創出され、社会の安全信頼保障にかかわるアーキテクチャとシステムデザイン、その社会実装を支援するツールの開発基盤、および人材育成のプラットフォームを確立する効果がある。

2) 新しい設計目標の導入と定量的評価による情報技術の進化

コンピュータの誕生以来、これまでの情報技術発展の駆動力は、主として、システムの高機能化、高速化、高集積化であり、情報システムの研究開発におけるシステム設計目標、評価対象も専ら「性能の向上」であった。これに対して、成熟した情報社会では、その安全と信頼を担保するディペンダビリティ／セキュリティが社会のグランドデザインに当たって掲げられるべき最高の価値であり、情報技術が目指すべき普遍的な目標理念である。この新しい設計目標の導入とその定量的評価の確立が新しい情報技術体系の創出とその進化の駆動力になり得る。

3) 科学的根拠のあるディペンダビリティ／セキュリティ保証の実現

従来は感覚的とされてきた信頼と安全という概念を情報社会におけるディペンダビリティ／セキュリティという技術概念に変換し、情報システム、重要インフラ、サービス・情報におけるディペンダビリティ／セキュリティ保証の科学的根拠を提示し、恒久的に社会の安全信頼保障を確保する科学的基盤を確立する効果がある。

6. 社会的効果

1) 情報社会の安定化

国家の基盤、企業活動の基盤、生活の基盤であるネットワーク化情報システム、およびそれが提供するサービス・情報の安全性・信頼性を科学技術の裏付けを以て実現し、評価し、恒久的に保証するアーキテクチャとシステム設計・保全技術を確立することによって、フェイルセイフな社会システムが実現され、情報社会の安定化と将来の発展が確保される。

2) 重要インフラのディペンダビリティ／セキュリティ保証

社会を支える重要インフラ（エネルギー網、交通網、情報通信網、金融網、医療網、防災網、防犯網、企業基幹網、行政網など）の相互依存性とリスク管理をネットワーク化情報システムの視点から検証し、その安全性・信頼性を恒久的に保証することによって、安寧な生活と十全な社会・経済活動を可能にする社会の安全信頼保障の実現に貢献する。

3) ディペンダビリティ／セキュリティ価値の社会的合意形成

これまでディペンダビリティ／セキュリティの価値は主観的であると考えられてきたが、定量的な評価指標の確立、テストベッドによる検証と正当化、評価基準、調達基準の策定のプロセスを通じて、定量的な価値の社会的合意が形成される。

7. 経済的効果

1) 新しい経済価値の創出

これまで、サービス・情報はもちろん、社会基盤である情報システムのディペンダビリティ・セキュリティが市場で評価される経済価値を持つことはなかったが、定量的評価指標とその計測法の確立、ベンチマーキング手法の開発で、ディペンダビリティ／セキュリティの客観的な比較評価が可能になり、市場における経済価値評価の対象になる。

2) 民間における技術開発インセンティブ

市場における経済価値評価が可能になることによって、ディペンダビリティ／セキュリティを価値とする製品計画、技術開発のインセンティブが生じ、それによって企業によるディペンダビリティ／セキュリティ指向設計の技術開発が促進される。その結果は産業の国際競争力を強化・拡大するとともに、国際標準化への主導的貢献へつながる。

3) 金融・経済インフラのディペンダビリティ／セキュリティ保証

情報システムの安全かつ安定的な稼動が決済システムに対する信用確保の大前提であり事業の根幹である金融分野において、科学的な方法でそのサービスに対するディペンダビリティ／セキュリティ保証の基盤が提供されることは金融の国際競争力強化に直結する。

8．優先順位と時間軸に関する考察

情報社会のディペンダビリティを確立するために提案する４階層（12 課題）の研究開発は相互に密接に関連するため、同時に推進することが望ましい（図１相互関連図参照）。しかし、リソースに制約がある場合、必要ならば、技術の緊急性、有効性、独自性、および相互の関連性の観点から、時間軸に沿って研究開発の優先順位を付ける（図２優先順位図参照）。

その場合、情報システム、重要インフラ、サービス・情報の各階層におけるディペンダビリティ実現に向けたシステム仕様、設計、実装の目標を適正かつ効果的に設定するために、各階層を通じたユーザー視点からの「ディペンダビリティの定量的評価」の研究開発を最優先するべきである。その結果、ユーザー視点の評価メトリクスに基づいて、各階層におけるディペンダビリティ設計・保全・保証の目標がトップダウン・アプローチで一貫性を保って設定され、研究開発が効果的に推進される。また、評価によるフィードバックが、長期的視野で技術進歩と環境変化に対応する動的なディペンダビリティ確立を可能にする。

階層に優先順位を付ける場合には、技術の緊急性と有効性の観点から、「ネットワーク化情報システム」と「重要インフラ」の研究開発を先行させ、次いで「サービス・情報」から「情報社会」へと連続的に実施する。

この優先順位を前提に、時間軸に沿って以下のように研究開発を推進する。

1) 優先順位に従って４階層（12 課題）の研究開発プロジェクトを直ちに立ち上げ、３年～５年以内に成果を出す。この場合、特に「重要インフラ」階層に関しては、既設重要インフラの担当省庁、事業実施企業と大学・研究機関との密接な連携が必要である。
2) ３年以内に「情報社会の安全信頼保障」に関する恒久的な課題に戦略的に取り組む研究拠点の設置を目指す。先行した研究開発プロジェクトとその成果を新設の研究拠点に集積する。
3) ５年以内に評価指標の国際標準化と認証機関の設置を目指す。
4) 10 年以内に社会・環境の変化と技術の進歩に対応した PDCA サイクルを通じて恒久的に「社会の安全信頼保障」を維持・進化させる情報社会システムを確立する。
5) その結果として、安全信頼保障の確立した情報社会、すなわち、人と組織が「安全と信頼」に確信を持ち、安寧な生活、十全な活動を展開できるディペンダブルな情報社会を実現する。

9. 検討の経緯

2005.9　「ディペンダビリティ」をキーワードに俯瞰ワークショップⅡ（上総アーク）を開催
2006.5　「ディペンダビリティ・ワークショップ」を開催
2006.5　「ディペンダブル VLSI ワークショップ」を開催
2006.10「情報システムのディペンダビリティ評価」に関する欧州調査を実施
2006.10「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
2006.11 ″EU-US 1st Workshop on System Dependability & Security″ 招待出席・調査
2006.12 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－」を発行
2006.12「情報システムのディペンダビリティ評価」に関する米国調査を実施
2007.4 ″EU-US 2nd Workshop on System Dependability & Security″ 招待出席・調査

表３　電子情報通信系俯瞰ワークショップⅡ（上総アーク）参加者リスト（研究者　３１名）

（所属は当時）

親委員会	田中　英彦 （情報セキュリティ大学院大）	三宅　なほみ （中京大）	古田　勝久 （東京電機大）	下記分科会 コーディネータ	
コメンテータ	土居　範久 （中央大）	久間　和生 （三菱電機）			

（所属は当時）

分科会	ＩＴの社会応用	ロボティクス／制御	ネットワーク	ｺﾝﾋﾟｭｰﾃｨﾝｸﾞ	エレクトロニクス／フォトニクス
コーディネータ	中島秀之 （公立はこだて大）	小菅一弘 （東北大）	三木哲也 （電通大）	南谷崇 （東大）	谷口研二 （阪大）
サブコーディネータ					保立和夫 （東大）
コーディネータ補佐	西田佳史 （産総研）	井村順一 （東工大）	西一樹 （電通大）	丸山宏 （ＩＢＭ）	成瀬雄二郎 （東芝）

メンバー	野島久雄 （成城大）	淺間　一 （東大）	江崎　浩 （東大）	徳田雄洋 （東工大）	安浦寛人 （九大）
	田村　大 （博報堂）	菅野重樹 （早大）	中川正雄 （慶応大）	天野英晴 （慶応大）	葛原正明 （福井大）
		矢野雅文 （東北大）	久保田文人 （ＮＩＣＴ）	関口智嗣 （産総研）	木村神一郎 （日立）
			並木淳治 （C＆C財団）		横森　清 （リコー）

表４「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者リスト（研究者24名）

1	菊野　　亨	大阪大学	教授
2	土肥　　正	広島大学	教授
3	森　　欣司	東京工業大学大学院	教授
4	佐々木良一	東京電機大学	教授
5	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
6	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	教授 情報システム検証研究センター長
7	中尾　康二	KDDI 株式会社技術統括本部	セキュリティ部長
8	本間　浩一	フリーランス	
9	丸山　　宏	日本 IBM 株式会社	基礎研究所長
10	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
11	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
12	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
13	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
14	伊関　　洋	東京女子医科大学先端生命医科学研究所	教授
15	藤井真理子	東京大学	教授
16	野島　久雄	成城大学	教授
17	高瀬　國克	電気通信大学	教授
18	松本　雅行	東日本旅客鉄道株式会社 研究開発センター	社設備部担当部長 研究開発センター　担当部長
19	谷口　研二	大阪大学	教授・ＣＲＤＳ特任フェロー
20	小菅　一弘	東北大学大学院	教授・ＣＲＤＳ特任フェロー
21	三木　哲也	電気通信大学	教授・ＣＲＤＳ特任フェロー
22	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
23	中島　啓幾	早稲田大学	教授・ＣＲＤＳ特任フェロー
24	今井　秀樹	中央大学・ＡＩＳＴ	教授・ＣＲＤＳ特任フェロー

付録Ⅰ 具体的な研究開発課題の例

情報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、長期にわたって科学技術政策が目指すべき最優先課題の一つである。その具体的な研究開発課題の例を、1) 情報システム、2) 重要インフラ、3) サービス・情報、4) 情報社会、の４階層に分けて示す。

階層１：情報システム

情報システムはそのミッションや応用分野によっていくつかのクラスに分類できる；

- 重要インフラに関わるシステム：　国民生活、社会・経済活動、科学技術、国家機能などの基盤であり、代替が困難な情報システム
- 企業基幹システム：　企業経営の根幹である事業活動、生産活動、経済活動などの基盤を支える情報システム
- 組込みシステム：　生産機械、ロボット、家電、情報機器、医療機器、自動車、航空機など、特定用途の機器、システムに埋め込まれた情報システム
- その他の情報システム：パソコン、端末機器、ゲーム機など

社会の基盤であるこれら各クラスの情報システムとそのネットワークに関して、その要求水準に応じたディペンダビリティ／セキュリティを確立するため、以下のような課題の解決に向けた研究開発を推進する必要がある。

1) フォールトや不正アクセスの存在にかかわらず、実世界と相互作用するネットワーク化情報システムのディペンダビリティを永続的に保証するシステム・アーキテクチャ

グローバルなネットワークの拡大、進化によって、例えば、グリッドコンピューティング、組込みシステムのネットワーク化、モバイル・システム、P2P ワイヤレス、分散システム／分散データベース、オープンソースソフトウェア、アドホックネットワーク、システムエリアネットワークなど、ディペンダビリティ保証のない新しい情報アーキテクチャと情報環境が次々と生まれ、これら異種パラダイムの融合、拡張が進んでいる。このため、実世界と相互作用するオープンで異種混合の大規模かつ複雑なネットワーク化情報システムのディペンダビリティ／セキュリティを実現し、進化・向上させるアルゴリズム／アー

キテクチャ／プロトコル技術、自律制御技術、知識ベース技術などの研究開発が必要である。これらの研究開発のキーワードを以下に列挙する。

- ディペンダビリティ／セキュリティのモデリング
- ディペンダビリティ／セキュリティ要求工学
- 障害分析／リスク分析
- フォールトモデル／脅威モデル
- ディペンダブル／セキュアシステム開発方法論
- ディペンダビリティ・アーキテクチャ
- セキュリティ・アーキテクチャ／プロトコル
- 暗号プロトコル
- 暗号技術（暗号、ディジタル署名、認証法、電子投票、電子決済など）
- 量子暗号技術（量子論に基づく鍵配送技術、量子計算論的安全性の理論）
- 侵入検知／欠陥検知
- フォールトトレランス／侵入トレランス
- 多階層統合
- 自律適応システム

2) 情報システムのライフサイクル・リスクを想定した一貫性のあるシステム仕様定義技術、設計技術、保全技術

巨大で複雑な情報システム（ソフトウェア、ハードウェア、VLSI、インタフェースなど）のライフサイクルに渡るリスクを想定したシステム仕様を定義し、それを正しく実現し、かつ保全することは情報システムにおけるディペンダビリティ／セキュリティ確保の基礎的要件である。ライフサイクルを通じたシステム保全のため、システム仕様定義、設計・検証・製造・テスト・運用、保全を通じた一貫性のある技術の研究開発が必要である。その際、ユーザー視点の評価メトリクスを各システム階層（応用･サービス、ミドルウェア、OS、ハードウェア）における開発目標・設計仕様へ一貫性を保って分解・帰着させることによって、設計目標達成がユーザー視点のディペンダビリティ評価へ合理的に帰結することを可能にする設計方法論、設計プラットフォームの開発が特に重要である。研究開発のキーワードを以下に列挙する。

- ディペンダブル／セキュアシステムの設計方法論／設計ツール
- ディペンダビリティ・ソフトウェアエンジニアリング
- 巨大ソフトウェアシステムの検証、診断

・形式的ディペンダビリティ方法論
・複雑制御システムの検証／正当化
・フォールト予防技術：セキュリティポリシー、アクセス制御、アクセス権／認証
・フォールト除去技術:証明ベーステスティング、ロバストテスティング

3) ユーザー視点から情報システムのディペンダビリティを定量的に評価し、経済価値へマッピングする評価技術

これまでの情報システムの設計目標と評価指標は主として高機能化、高性能化であったが、情報社会の安全信頼保障の基盤となる情報システムとそのネットワークの評価指標はディペンダビリティ／セキュリティでなければならない。その際、従来のエンジニアリングの伝統であった部分の信頼性の積み上げによって全体の信頼性向上を図るボトムアップアプローチではなく、ユーザー視点の評価メトリクスを出発点とするトップダウンのシステム的アプローチを採らなければ所期の目的は達成できない。このため、以下の３項目の研究開発が本質的である。

・情報システムのユーザー（ステークホルダ）の視点からディペンダビリティ／セキュリティを評価し、保証するための定量的指標（メトリクス）の開発とその正当性検証、およびその計測法・計算法・評価法の研究開発
・情報システムのディペンダビリティ／セキュリティの品質モデリング、合意形成、価値の可視化、経済価値へのマッピング、ディペンダビリティ・ベンチマーキング、予測技術の研究開発
・ディペンダビリティ／セキュリティ評価の正当性、有効性を確認するための十分な規模のテストベッドとデータセット構築

以下に研究開発のキーワードを列挙する。

・ユーザー視点の評価メトリクス
・ディペンダビリティ／セキュリティ計測法・定量的評価法・可視化技術・ツール
・ディペンダビリティ／セキュリティ品質のモデリング
・ディペンダビリティ／セキュリティ価値の合意形成
・経済価値マッピング技術
・ディペンダビリティ・ベンチマーキング
・ディペンダビリティ予測技術
・テストベッド／データセット構築

階層２：重要インフラ

重要インフラとは、エネルギー網、情報通信網、交通網、金融網、医療網、教育網、防災網、防犯網、行政網、防衛網、ビジネス基幹網など、国と社会のあらゆる活動が依拠する社会基盤であり、オープンで異種結合のネットワーク化された情報システムがその基盤の制御において重要な役割を果たす。情報社会の重要インフラのディペンダビリティ／セキュリティ確保のため、以下のような課題の解決が必要である。

1) フォールトや不正アクセスの存在にかかわらず、相互に依存し合う多様な社会重要インフラのディペンダビリティを永続的に保証するインフラ・アーキテクチャ

社会の諸活動を支える電力供給網、交通網、通信網、水道網、防災網などは広範囲に亘って相互に複雑な依存関係にあり、それらがネットワーク化された情報システムの制御に依存している。このため、そのディペンダビリティ／セキュリティを脅かす様々なリスク要因に直面している。情報社会の安全信頼保障のためには、多様な重要インフラの相互依存性解析に基づいたリスク分析と、障害やサイバー攻撃が社会の活動に及ぼす影響の予測が緊急かつ最重要の課題である。その上で、相互に複雑な依存関係を形成する重要インフラが将来に渡って永続的なディペンダビリティを維持するためのインフラネットワークのアーキテクチャの開発とのその社会的な実装が必要である。このための研究開発のキーワードを以下に列挙する。

- 重要インフラの相互依存性モデリングと解析
- 相互依存性のインパクト解析と評価モデリング
- 分散アーキテクチャのリスク相互干渉解析
- 障害伝播ドミノ、カスケード、障害増幅
- 異種システムの相互作用性
- 障害・攻撃のインパクト解析・推定
- ディペンダビリティ／セキュリティ評価・予測のシステム技術
- センサーネットワーク
- サイバー・セキュリティ
- インフラ・アーキテクチャ

2) 重要インフラのライフサイクル・リスクを想定した一貫性のあるインフラ仕様定義技術、設計技術と防衛・保全技術

技術の進歩と環境変化に対応して要求される水準のディペンダビリティ／セキュリティ確保の保証が可能な重要インフラのシステム設計技術と、その防衛・保全技術ならびにそれを実現するシステム技術の開発が緊急の課題である。研究開発のキーワードを列挙する。

- ディペンダビリティ／セキュリティ設計方法論
- 重要インフラを防衛・保全するシステムアーキテクチャ
- 複数組織環境のセキュリティポリシーとアクセス制御機構
- 重要インフラ制御・管理の分散アーキテクチャ
- リスク／脅威モデリング
- 異種統合システムのディペンダビリティ設計
- セイフティ・クリティカルシステム
- 過負荷、攻撃、障害の下での可用性保証技術
- サバイバビリティ

3) ユーザー視点から重要インフラのディペンダビリティを定量的に評価し、経済価値へマッピングする評価技術

社会活動への影響の視点からの重要インフラのディペンダビリティ／セキュリティを評価するメトリクスの開発、その計測法、定量的評価法、可視化技術の開発が、永続的な情報社会の安全信頼保障にとって必須である。キーワードを以下に示す。

- 重要インフラメトリクス開発
- 計測法、計算法
- テストベッド開発、評価法
- 可視化技術
- リスク分析
- ディペンダビリティ／セキュリティの定量的評価
- ベンチマーキング

階層３：サービス・情報

サービスとは、一般に「ある実体（人、組織、人工物、情報システムなど）から他の実体へ物理的、論理的あるいは情緒的に有益な作用を及ぼす行為」と考えることができるが、情報社会を前提とすれば、ネットワーク化された情報システムによって直接的あるいは間接的に提供されるサービス、すなわち“情報”そのものと考えて良い。例えば、電子政府、電子商取引、電子投票、電子決済、モバイルサービス、VOIP／ワイヤレス、ウェブサービス、RFID、P2P、グリッド、センサーネットワーク、ユーザーインタフェースなど、今後の情報社会で重要になると考えられるサービスはネットワーク化情報システムが提供する“有益な情報”である。

情報システムの提供するこれらのサービスあるいは情報のディペンダビリティ／セキュリティの確保は情報社会の安全信頼保障の根底を支える基本的課題である。このため、以下の課題の研究開発推進が必要である。

1) フォールトや不正アクセスの存在にかかわらず、ネットワーク化情報システム、社会重要インフラが提供するサービス・情報のディペンダビリティを永続的に保証するサービス・アーキテクチャ

情報システムとそのネットワークによって生産、蓄積、流通する大量情報、及び検索、要約、優先順位付けされた二次情報、あるいはユビキタスコンピューティング環境で収集される大量のセンサー情報から抽出され、加工された情報、さらにこれらの情報を活用して提供されるサービスのディペンダビリティ／セキュリティを実現し、長期に渡って保証するサービスモデル、情報モデル、サービス・アーキテクチャ、サービス認証・管理技術、情報保証技術の研究開発が重要である。

- サービスモデリング
- 情報モデル
- 最適化
- サービス・オントロジー
- サービス品質としてのディペンダビリティ／セキュリティ
- アクセス権限付与とユーザー認証
- バイオメトリクス
- データマイニングのディペンダビリティ
- データストリーミング

2) サービス・情報のライフサイクル・リスクを想定した一貫性のあるサービス仕様定義技術、設計技術、保全技術

技術の進歩による情報システム自身の進化と社会・環境変化に対応した動的なサービス･ディペンダビリティ実現を可能にするサービス･情報の設計プラットフォームと、システムのライフサイクルを通じたリスク管理、障害影響予測を可能にするサービスの設計技術、保全技術の体系化・構造化が重要である。研究開発のキーワードは以下の通り。

- ディペンダビリティ・セキュリティマネジメント（情報資産の特定、リスク分析・管理、リスク軽減策）
- サービスのディペンダビリティ／セキュリティのモデリング、計測、実現
- サービスアベイラビリティのユーザー諸問題
- サービスの発見／創出
- サービス改善／強化
- サービス創造メカニズム
- ディペンダブルサービスシステム
- 情報フロー制御
- セキュリティ要求を満たすビジネスモデル設計
- サービス指向アーキテクチャ／ミドルウェア
- サービスのディペンダビリティ／セキュリティ要求、設計・テスト
- サービスの開発、分析、テスト、モデリング、環境、ツール
- サービス実現、認証、支援のアベイラビリティ基準
- サービス管理・認証
- サービスインタフェース：ユーザビリティ、セキュリティ、アベイラビリティ

3) ユーザー視点から情報システムのディペンダビリティを定量的に評価し、経済価値へマッピングする評価技術

人間要素を含む広義の情報システムによって提供されるサービス・情報に対して、ユーザー視点からの主観も含むサービス価値の合意形成、評価メトリクスの開発、その計測法、計算法、定量的評価、可視化方法、経済価値へのマッピング技術、SLA 方式の確立とその社会システムに与えるインパクトの分析など、サービス・情報のディペンダビリティ確立への科学的･工学的アプローチの基盤整備が必要である。

- サービス水準合意 (SLA)

・ロバスト・サービスインフラの設計、モデリング、評価
・サービス評価メトリクスの計測法、計算法、可視化技術
・サービス・ディペンダビリティ評価技術・ツール
・経済価値と社会価値
・サービス市場原理
・個人情報保護技術／信用管理
・情報保証

階層４：情報社会

情報社会の基盤であるネットワーク化情報システム、それに依拠して構築される社会の重要インフラ、その上で提供される多様なサービス・情報の各階層におけるディペンダビリティ実現を促進・支援する社会システム（防犯、防災、監査、認証、保障、保険、法・制度、国際標準など）とその運用支援ツールの開発を含む情報社会技術、ならびにその知見に基づいた政策提言と、実装支援、人材育成を含む総合的な研究開発の成果として情報社会の永続的な安全信頼保障が実現される。このため、以下の課題の研究開発推進が必要である。

1) システム障害、サイバー攻撃、情報漏洩、自然災害などの発生に際して、被害を最小限度に留めるフェイルセイフな社会システム・アーキテクチャ

基盤となる情報システム、その上に構築される社会の重要インフラ、そこから提供されるサービス・情報のディペンダビリティが不完全な場合、最終的に、情報社会におけるシステム障害、サイバー攻撃、情報漏洩、自然災害となって大きな被害をもたらすことになる。このため、４階層の最上位レベルである社会システムでは、システムに障害が発生してもその結果として常に被害を最小限度に留めるフェイルセイフ・アーキテクチャとして情報社会に実装されている必要がある。そのキーワードを以下に列挙する。

・ディペンダビリティ／セキュリティを確保する社会システムのアーキテクチャ
・フェイルセイフ
・セキュアな企業基幹アーキテクチャ
・ディペンダビリティ／セキュリティ経営
・システム監査
・監視社会とプライバシ保護
・ビジネス／電子商取引／電子決済

・大量情報処理技術を活用したサーベイランス技術・システム
・標準化、ガイドライン、認証

2) 情報社会が将来に渡って直面するリスクを想定し、ディペンダビリティの実現を促進する一貫性のあるフェイルセイフな社会システムの設計・保全技術とその運用支援ツール

技術の進歩と社会・環境の変化に対応して長期に渡ってディペンダビリティ実現を支援・促進する社会システムも進化を遂げる必要がある。このため、社会・環境の変化永続的に全体として一貫性を保って機能するフェイルセイフな社会システムの設計、保全技術と、その実装・運用のための支援ツールの開発が必要である。
そのキーワードを以下に列挙する。

・社会システム運用支援ツール
・信用モデルと信用管理
・共通基準プロトコル
・法規制

3) 情報社会のディペンダビリティを定量的に評価し、永続的な安全信頼保障を科学的方法で確立する情報社会技術・システムの研究開発、政策提言、実装支援と人材育成

情報社会の永続的な安全信頼保障を確立するために、ディペンダビリティの定量的な評価に基づいた科学的方法の開発が必要である。このため、情報技術と社会技術の融合した新しい学際分野「情報社会技術」、および「情報社会システム」の研究開発、その成果に基づいた社会実装に関する政策提言と実装支援、さらにこの分野の研究開発、政策理解、実践能力を有する優れた人材の育成が必要である。
そのキーワードを以下に列挙する。

・ディペンダビリティ／セキュリティの公共的価値と市場経済価値
・モデリング、分析、マッピング技術・ツール
・教育（情報倫理、情報法学、情報経済学、情報社会学など）
・コンピュータ犯罪
・法情報学 (Information Forensics)

付録Ⅱ 国内外の状況

1) ＥＵ：ＦＰ６，ＦＰ７(2007-20013) においてセキュリティ・ディペンダビリティが重要課題

EU-ICT Security & Dependability Taskforce
"ICT Security & Dependability Research beyond 2010: Final Strategy" 2007.1
EU-ICT INCO-TRUST (International Co-operation in Secure, Dependable and Trusted ICT Infrastructures) プログラムがスタート
D&S 関連予算総額 (2007-2008)：　90M EURO

2) 米国： National Strategy to Secure Cyberspace 2004.2

NITRD プログラム：Cyber Security and Information Assurance(CSIA)
High Confidence Software and Systems(HCSS)
〃Leadership Under Challenges: Information Technology R&D in a Competitive World〃
Formal Assessment of NITRD by PCAST　発行 2007.8

3) IEEE Transactions on Dependable and Secure Computing

2004 年１月スタート、年４回発行

4) EU-US Summit Series: Workshop on System Dependability and Security

EC/NSF/DHS 共催の非公開 WS、重要研究分野の提案と EU-US 連携の模索、
第１回：Dublin, 2006.11　第２回：Urbana-Champaign, 2007.4

5) JST-CRDS：戦略イニシアティブ「ニュー・ディペンダビリティ宣言」2006.12

6) 日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会発足　2007.1

7) 内閣官房情報セキュリティセンターの状況

「第２次提言：我が国の重要インフラにおける情報セキュリティ対策の強化に向けて」2005.4.22
「第一次情報セキュリティ基本計画」2006.2.2
「セキュア・ジャパン 2006」 2006.6.15　「セキュア・ジャパン 2007」 2007.4.23
情報セキュリティ政策会議　技術戦略専門委員会報告書 2006
2007.6.29

戦略イニシアティブ

情報社会のディペンダビリティ
ー情報技術の目指すべき目標理念ー
CRDS-FY2007-SP-06

独立行政法人 科学技術振興機構 研究開発戦略センター
平成19年12月
生駒グループ

〒102-0084 東京都千代田区二番町3番地
電話 03-5214-7484
ファクス 03-5214-7385
http://crds.jst.go.jp/
平成19年12月
