3 .総合分析

（１）世界最高水準のハイパフォーマンスコンピューティング技術

①　技術別の指標に対する貢献度評価

- 技術指標「ピーク時性能」から見ると、「革新的ハイパフォーマンス・コンピューティング・インフラ（HPCI）の構築（文部科学省）」によって開発された「京」が2011年に世界最高速を達成した。
- また、社会指標「HPC利用課題選定件数」「HPC産業利用企業数」においても、京の利用が進んでおり、後者は増加している。
- しかしながら、社会課題「科学技術分野におけるHPCの利活用状況」の目標に対しては、定量的に見れば、社会課題「HPCI利用課題選定件数（産業利用を除く）」は37、「HPCI産業利用企業数」は2年間累計で83にとどまっており、幅広い分野で使われているとは言いがたい。
- 「京」で開発された技術をもとにした商用機「スーパーコンピュータ　PRIMEHPC FX10（富士通）」が上市され、2013年現在で国内外11機関に設置されている。このことから、社会への実装にも貢献している。
- また「京」を活用した研究成果がハイ・パフォーマンス・コンピューティング（高性能計算技術）に関する国際会議SC12において、ゴードン・ベル賞を受賞している。宇宙の初期における大量の量子を用いた重力進化のシミュレーションを「大規模計算を非常に高い実効性能で実現した」ことが受賞理由であった。本研究は基礎物理領域での利用推進に貢献したほか、シミュレーション技術開発にも貢献したと考えられる。

3 .総合分析

（１）世界最高水準のハイパフォーマンスコンピューティング技術

②　今後取り組むべき項目

- HPC技術は、基礎科学における観測ビッグデータ解析、創薬やものづくりにおけるシミュレーション等の分野において、従来とは全く違う次元での研究開発を進めることを可能とするものである。すなわち、技術的先進性を維持しつつ、社会課題「科学技術分野におけるHPCの利活用状況」の目標を達成することにより、現状で把握できている社会的課題の解決に向けた技術開発がより促進されるとともに、新たなデータの組み合わせ分析やシミュレーションにより、従来は発見されなかった新たな機能を持った物質や新たな理論の発見、さらには今後対応すべき新たなニーズの発掘につながると考えられるため、利用する企業の技術力の向上ならびに当該科学技術分野の先進性の強化につながり、本課題領域のねらいである「国際的な優位性の確保」につながると考えられる。

- 社会課題「科学技術分野におけるHPCの利活用状況」の目標は、学術6領域において幅広くHPCを活用していくことである。現状の分野の広がりは把握することが困難だが、定量的に見れば、社会課題「HPCI利用課題選定件数（産業利用を除く）」は37、「HPCI産業利用企業数」は2年間累計で83にとどまっており、幅広い分野で使われているとは言いがたい。
  現状稼働しているHPCI「京」については、利活用が促進されるよう、適用分野に応じたアプリケーションの整備が望まれる。また、産業利用においては中小企業やベンチャー企業でも利用が可能となる技術・制度面の環境を整備することが求められる。また、「京」をベースとしたスーパーコンピュータは、既に内外11機関に設置されており、これらを活用して大学、企業などでの利活用が進んでいくことが期待される。
  したがって、数多くの領域で利活用が進むよう社会指標「HPCの利活用状況」の実現、そのための技術指標「数値計算ライブラリ」の充実を図っていく必要がある。
  また、各領域においてHPCの利活用を企画立案できる人材の育成が必要となる。
  産業利用においては、研究開発型スタートアップ企業や中小企業でも利用できるよう、専門的なアドバイスができる人材の育成、あるいは研究担当者の教育、さらには利用コストの低減に向けた財政面での支援などを行うことが望まれる。
- 技術的先進性については、今後も引き続き維持していく必要がある。HPCの技術進化がめざましく、2012年からは中国、米国のHPCにトップを譲るなど、国際間競争が激化する中、技術指標「ピーク時性能」を世界最先端に維持していくためには、2020年頃にエクサFLOPS級のHPCの実現が望まれる。しかし、それには多大な期間と費用を要することから、第116回科学技術総合会議での議論を踏まえ、対象とするアプリケーションや開発目標の設定、全体事業費の精査と工程表の具体化などを行う必要がある。科学技術総合会議では、2014年秋ごろをめどに再度評価を行い、技術開発の可否を検討することになっており、HPCについても、利活用を意識した技術開発が望まれている。

3.総合分析

（２）能動的で信頼性の高い（ディペンダブルな）情報セキュリティに関する技術

①　技術別の指標に対する貢献度評価

- 技術指標「情報通信システム全体のセキュリティの向上」の開発状況に対しては、総務省「サイバー攻撃の解析・検知に関する研究開発」でマルウェアの諜報活動を検知するセンサや分析技術の施策を行っており、同指標の技術確立に貢献している。

②　今後取り組むべき項目

- 近年、社会を支える重要な基盤的サービスである、「情報通信」「金融」「航空」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む。）」「医療」「水道」及び「物流」分野においても、ICTの利活用、並びにインターネットへの接続、クラウドの利用などが進んできている。さらに、これまでネットワークにつながっていなかった様々なものがつながれるようになってきている。そのため、外部からの攻撃によるセキュリティインシデントや、事故・トラブルが発生した場合、社会に重大な影響と混乱を引き起こす恐れがある。社会指標「重要インフラにおけるセキュリティインシデント件数」の減少を実現するに当たっては、これらの重要インフラを攻撃から守るための研究開発が重要となるが、さらに成果を重要インフラに実装し、戦略的に防御していくことが必要である（第3回ICT-WG　構成員助言より）。

3.総合分析

（２）能動的で信頼性の高い（ディペンダブルな）情報セキュリティに関する技術

②　今後取り組むべき項目

- 社会指標である「サイバー攻撃による被害総額」の減少を実現するに当たっては、既存のICT利活用範囲での研究開発に加え、医療健康、ビッグデータ、次世代インフラ等の技術指標「発展が期待される応用分野におけるセキュリティ研究開発」を推進する必要がある。
  その一分野であるクラウド利用においては、総務省事業「災害に備えたクラウド移行促進セキュリティ技術の研究開発」から、企業が実用化に向けて独自に研究開発を継続しており、製品化と社会への実装に向けた技術の実用化のための研究開発を継続する必要がある。
  その他の国の事業は、2015年を目途に確立する技術を開発しているところであり、着実に目標を達成できるよう、研究開発の着実な進捗管理が求められる。
  さらに、NISCがロードマップの改訂を計画しているとおり、多様化するセキュリティ攻撃に対応した柔軟な研究開発課題の設定とともに、諸外国とも連携し、攻撃のパターン収集等を推進することが求められる。
- 社会指標「サイバー攻撃による被害総額」ならびに「重要インフラにおけるセキュリティインシデント件数」両方の低減が求められるが、代理指標は減少してきているとは言え、新たな攻撃手法が常に出現している状況である。そのため、常に変化する攻撃手法への対応を図るため、絶えず技術開発を続けてゆく必要がある。また、開発された技術を元に、高性能だが個人や中小企業でも使いやすい情報セキュリティソフトやサービスの開発・普及を進める必要があるため、一層の実用化開発を進めていくことが望まれる。これはまた、国内で使われているセキュリティソフトがほぼ外国製である現状を打破し、国家の安全保障を強化するという観点からも重要と考えられる。
- また、今回のレビューにおいて設定した2つの指標とも公的な統計では集約されておらず、代理指標をおいて評価した。被害の実態を明らかにするとともに、施策の成果と社会実装の効果を計測する上でも、指標値の継続的な計測が求められる。

【参考】わが国の主な取組とこれまでの成果

個別課題：世界最高水準のハイパフォーマンスコンピューティング技術

取組	これまでの成果
革新的ハイパフォーマンス・コンピューティング・インフラ（HPCI）の構築（文部科学省）	• 「京」は平成23年11月にLINPACK性能10ペタフロップスを達成し、同年6月と11月の二期連続で世界スパコン性能ランキング(TOP500)において1位を獲得するとともに、その利用研究が平成23年,24年と2年連続でゴードン・ベル賞（コンピュータシミュレーション分野での最高の賞）を受賞した。 • 「京」及びHPCIについては、平成24年9月末に共用を開始した。 • 「京」の利用については、産業界を含む幅広い利用者から公募で選定した一般利用枠102課題、国が戦略的な見地から選定した戦略プログラム利用枠29課題を実施している。産業界83社を含む1,000人以上が利用し、社会的・科学的課題の解決に資する画期的な研究成果の創出が図られている。また、共用開始以降、論文82本が発表、特許2件が出願されている。（H25.10月時点）
スーパーコンピュータ PRIMEHPC FX10（富士通）	• 2011年11月に発表された市販製品。京開発のノウハウを適用した。性能は以下の通り。 • ラック：96ノード • CPU：SPARC64 Ixfx 16コア 1.650GHzまたは1.848GHz 211.2GFLOPSまたは236.544GFLOPS • メモリ：1CPUあたり32GBまたは64GB • メモリ帯域 85GB/s • 最大構成時性能：23.2PFLOPS、6PBメモリ

【参考】わが国の主な取組とこれまでの成果

個別課題：能動的で信頼性の高い（ディペンダブルな）情報セキュリティに関する技術

取組	これまでの成果
能動的で信頼性の高い情報セキュリティ技術の研究開発（総務省＋経済産業省）	• 国際連携によるサイバー攻撃予知・即応技術の研究開発 　• サイバー攻撃を予知し、即応を可能とするシステムのプロトタイプを構築。2015年までに10ヵ国にセンサー設置の目標に向け、これまで4ヵ国（H23に2ヵ国、H24に2ヵ国）に設置。 • マルウェア感染の早期検知技術の研究開発 　• マルウェア感染の早期検知技術について、ネットワーク観測によりネットワークトラヒックをリアルタイムに可視化することで、サイバー攻撃を検知するシステムを構築。 • 東北復興再生に資する重要インフラＩＴ安全性検証・普及啓発拠点整備・促進事業 　• 制御システムの接続性・脆弱性に関する検証結果の視覚化技術、高セキュア化技術、インシデント分析技術の開発を進めているところ。 　• その他の施策についても、2015年度までの技術の確立及び民間転用に向けて必要となる技術の開発を当初の計画どおり進めているところ
災害に備えたクラウド移行促進セキュリティ技術の研究開発（総務省）	本施策の結果、以下のとおりの成果が得られ、現在製品化に向けた取組が行われているところ。 （１） プライバシー保護型処理技術 ○ 暗号化してクラウド上に保存しているデータから、暗号化したまま統計値演算や頻度分布計算を行う技術、及びデータに乱数成分を付加することにより秘匿したまま統計値演算を効果的に行う技術を開発。 ○ 暗号化された評価値データから、暗号化したままデータ間の類似度に基づき推薦処理をする技術を確立。商用のクラウドサービス上で実装。 ○ 属性情報を選択的に開示可能なグループ署名の基本方式を確立。 （２） セキュリティレベル可視化技術 ○ クラウド全体のセキュリティレベルを算出する方式の設計を完了。 ○ 生体認証を含む認証について、利用者のセキュリティレベルを定量的に分析する技術を確立。 ○ データの重要度を、高精度で判定する技術を開発。 ○ クラウドのセキュリティレベル及びデータの重要度に適したデータ保護ポリシーの動的生成技術及びポリシー適合度の可視化技術を確立。
サイバー攻撃の解析・検知に関する研究開発（総務省）	○利用者の行動特性に基づくサイバー攻撃検知技術の研究開発 利用者の行動ログ抽出及び対策評価環境の基盤整備を行い、マルウェアの諜報活動を検知する小型ネットワークセンサやゲートウェイの試作、リアルタイムでのアノマリ分析技術の試作等を実施中。 ○ 既存のログに依存しない利用者環境の特性を活用したサイバー攻撃の侵入経路及び進行状況を解析する技術の研究開発 ネットワーク構成把握方式の検討や端末・サーバ上で取得する情報の整理を行い、攻撃手法やマルウェア挙動に関するログに依存しない分析手法の検討を実施中。 ○ サイバー攻撃の封込めと業務継続を可能とする組織内ネットワーク制御技術の研究開発 動的な管理ポリシーの生成技術や管理ポリシーに基づく自動的なネットワーク構成技術等について、要素技術の開発と一定規模の仮想ネットワークにおける試行を実施中。
生体情報を用いた電子署名技術（日立製作所）	• 電子署名の作成に指の静脈パターンなどの生体情報を用いることのできる、安全性を証明可能な電子署名技術を開発。本技術により、標準的な電子認証の仕組みである公開鍵基盤(PKI)と同様の機能を持つ情報セキュリティ基盤を、ICカードやパスワードを使わずに個人の生体情報で実現できる。 • 総務省委託研究の「災害に備えたクラウド移行促進セキュリティ技術の研究開発」における研究成果を一部に含む。（2013年2月18日報道発表）
自治体の被災者支援業務をクラウドサービスを用いて迅速かつ安全に行うことを可能とする情報セキュリティ技術（早稲田大学、東海大学、(株)日立製作所、日本電気(株)、(株)KDDI研究所）	(1)平常時の認証方式に依存しない、クラウド向けの柔軟で安全な認証を実現する認証基盤技術 • 災害時などにICカード認証を使用しないで業務を行う際に、平常時と同等の情報セキュリティレベルを確保し、適切な認証によって住民情報へのアクセス制御を実現する情報セキュリティ技術。 (2) クラウドを活用した災害関連情報の自動振り分け技術 • 自動振り分け技術は、災害時にソーシャルサイトなどに投稿される大量の情報を効率的に収集するため、スマートフォンなどの端末側で投稿内容から自動的にラベル付け(例：災害情報、救急情報)を行い、クラウド上のサーバが、ラベルや位置情報、システムの状態などを勘案して最適なシステムに情報の振り分けを行う技術。 (3) クラウド上でのプライバシー保護型災害対応支援技術 • プライバシー保護型災害対応支援技術は、データを暗号化したまま処理する技術。 • 総務省事業で研究開発。

【参考】指標値の検討（HPC）

◆ 社会指標（社会課題解決）

- HPCによる「国際的優位性の保持」は、科学技術における諸課題への取組において、国産のHPC技術が利活用され、課題解決に貢献することであると定義した。
- そのロードマップは、理化学研究所「計算科学ロードマップ　中間報告書　2013年9月将来のHPCIシステムの在り方に関する調査研究「アプリケーション分野」」で提示されている。
- 提示されている分野は以下の通り。
  - 生命科学
  - 物質科学
  - 地球科学（気象・気候科学、固体地球科学）
  - ものづくり（熱流体、構造解析、機械材料、プラズマ・核融合、電磁界解析、可視化・データ処理）
  - 基礎物理（宇宙研究、素粒子、原子核物理）
  - 社会科学
- これらの利活用に現在の技術開発や実用化の状況がどのように貢献しているかについて、評価を行う。
- 次ページ以降で、これらのロードマップを記載する。