「スマート革命」が促す 第2章 ICT産業・社会の変革

第1章で分析したとおり、ICT は依然として、幅広い産業・社会分野への実装を通じて、また ICT 産業の拡大 を通じて、我が国及び世界での成長のエンジンとして機能しており、先進国、新興国はもとより、識字率の低い開 発途上国においても、電力、水道など他の社会インフラに先立って、例えば太陽光発電により作動する単純な機能 の携帯電話システムの導入が社会の発展のきっかけとなる一方で、中国、韓国のメーカー等が開発途上国に積極 的にシステムの売り込みを図る姿がみられるなど、ICT による成長とそれに伴い急拡大する ICT 市場を巡って、 ICT の活用側、ICT 産業の側双方で競争が起きている。

他方、特に先進国を中心に、ブロードバンド、特にワイヤレス・ブロードバンドの普及、クラウド環境への移行、 ソーシャル利用の拡大を契機に、ICT のパラダイム転換が生じつつある。昨年から本年にかけて急速に普及しつ つあるスマートフォンにより、そのようなネットワーク・サービスにいつでも、どこでもアクセスできるようにな りつつある。その一方で、このような変化は、昨年度の日本の一部電機メーカーの厳しい決算状況にみられるよう に、ICT 産業の各セクターの浮沈をもたらし、また一部のスマートフォンによる「垂直統合型」サービスの提供 は、水平分離型(パソコン)または通信キャリア主導型の垂直統合モデル(携帯電話)に占められてきた我が国の ICT 産業の構造に根本的な変化をもたらしつつあるようにもみえる。

本章では、まず第1節で、ユビキタスネットワーク環境の完成とビッグデータに代表されるスマート化の始動に より進行しつつある「スマート革命」を概観するとともに、特にインターネットがグローバルな社会基盤となるこ とにより生じつつある課題、とりわけ制度的課題やその国際議論、深刻化するサイバー攻撃など情報セキュリティ を巡る動向を紹介しつつ、「スマート革命」の原動力として広範な産業・社会分野の期待を集めているインターネッ トの知識創造基盤としての役割に関し、ビッグデータの動向を紹介する。次に第2節で、様々な財・サービスの流 通基盤として国境を越えて機能しつつある点について、特に成長性の高いモバイル産業に焦点をあて、スマートフォ ン・タブレット端末の普及がマーケットや利用者にもたらしている急速な変化やそれにより見込まれる経済波及効 果について分析し、その構造変化について展望する。最後に、第3節で、モバイル産業と並ぶ無線系ネットワーク・ サービスの柱である放送メディアの新展開について展望する。

「スマート革命」 —ICT のパラダイム転換・ 第一節

1 「ユビキタスネットワーク」環境の完成と「スマート革命」

(1) インターネット・携帯電話の社会基盤化

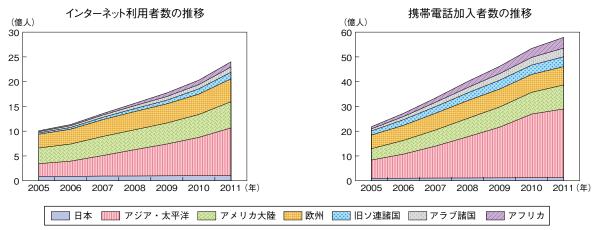
第1章で検証したように、ICT は世界の成長の原動力としてその機能は実証され、常識となりつつある。その 中核に位置するのが、インターネットである。インターネットは先進国、新興国、開発途上国を問わず全世界に急 速に普及が進んだ。平成23年5月のドーヴィルG8サミットに先立ちパリで開催されたe-G8フォーラムに提出 されたレポート「Internet Matters」「では、インターネットはグーテンベルグの印刷技術ではなく電気の発展と 商用化と比肩すべきとの議論を紹介し、「電気は、高層階まで上ることができるエレベーターを可能にし、巨大な 超高層ビルの夜明けの到来を告げることにより、世界中の街の風景を変えた。電気と同様に、インターネットは世 界の風景を変えつつある。インターネットははるかな距離の橋渡しをし、直ちに利用できる情報のほとんど絶える ことのない奔流にすぐにアクセスすることを可能にすることにより、世界をよりフラットにしつつある。」と述べ

^{1 &}quot;Internet matters: The Net's sweeping impact on growth, jobs, and prosperity" Mckinsey Global Institute 本文 p.1 参照。

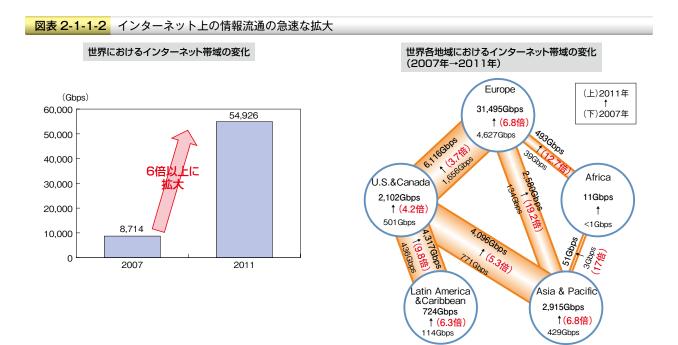
ている。また、平成24年4月のストックホルムインターネットフォーラムでは、スウェーデンのビルト外務大臣が、 「インターネットは 21 世紀の『水』であり、水のあるところに『命』が生まれる。インターネットへのアクセス が確保されたところに『希望』が生まれる。インターネットの自由の欠如は今日における貧困の一形態となる。」と、 インターネットを水に例えてその役割の重要性を強調した。昨今、サイバー攻撃による政府・企業への被害がたび たび報じられているが、これはグローバルに、オープンに広がるインターネットがあらゆる国の社会・経済活動に 不可欠の基盤になったことの副作用とも見て取れる。インターネットはあらゆる社会活動の基盤となり、人々の生 活の利便性の向上や経済活性化の原動力としての役割を果たしている。

また、第1章第2節で紹介したように、電力インフラなど他のインフラが整備されていない、識字率の低いハ ンディのある地域でも先行して整備が進み、貧困から発展への起爆力となっている携帯電話も、特に開発途上国に おいて、固定電話と異なりインフラ整備が比較的容易であるという特性と、音声通話や SMS という誰でも容易に 扱える情報伝達の特性を生かして貧困から発展への「壁」を打破する技術として、成長の「第一歩」としての重要 性を増している。例えば、ケニア・Safaricom の前 CEO の Michael Joseph は、2000 年(平成 12 年)の CEO 就任時には「この国の市場規模はせいぜい5万人」と発言していたが、現実に、2010年(平成22年)の退任時 には、契約者数は約1,200万人に達していた。このように、携帯電話の普及は、その整備の最前線にいる人々の 予測すら超えて、爆発的に普及しつつある。

図表 2-1-1-1 インターネット・携帯電話の世界普及の動向(地域別)



ITU 資料により作成



(出典) 総務省「海外主要国における情報通信産業等に関する調査」(平成24年)(TeleGeography's Global Internet Geography により作成)

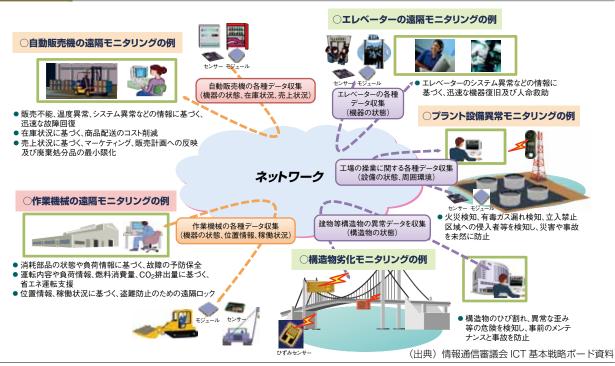
(2) ユビキタスネットワーク環境の完成

以上の ICT の社会経済発展への役割の増大、とりわけインターネットの社会基盤化は、無線技術、ストレージ技術など ICT 技術の革新を背景としたネットワーク・サービス環境の飛躍的進化により、その適用範囲を大きく拡大している。平成 23 年版情報通信白書において、「ユビキタスネットワーク社会の現実化」(第3章第1節)として述べたとおり、総務省において推進してきた u-Japan 政策の目標であるユビキタスネットワーク社会の構築、すなわち「『いつでも』(昼でも夜でも24時間)、『どこでも』(職場でも家でも、都会でも地方でも、移動中でも)、『何でも』(家電も身の回りの品も、車も食品も)、『誰でも』(大人も子供も、高齢者も障害者も)、ネットワークに簡単につながる社会の実現」²が、少なくとも技術・サービス・各種機器など環境面の整備は整ったものと考えられる。

具体的には、まずネットワークインフラの分野では、LTEに代表されるワイヤレス・ブロードバンドの発展・普及、Wi-Fiの広範な端末機器への導入・家庭内外におけるアクセスポイントの整備による有線網・無線網の統合利用、放送のデジタル化による通信との融合・連携型サービスの拡大など、特に無線通信技術の革新を背景に、これまでバラバラに運用されていた個々のネットワークを統合的に利用することが可能となりつつある。その上で、これまで個々の企業等に分散して設置されてきたサーバーなどコンピュータ資源についても、クラウドを通じて利用者向けサービスとして提供されるようになり、統合の方向に進みつつある。さらに、平成23年版情報通信白書で詳しく分析したように、メディア・サービスのレベルでは、インターネット上で個々の利用者が情報を受発信しコミュニティ空間を形成する「ソーシャル」化が特に若年層を中心に進展しており、人と人との絆の強化を通じて国民の幅広い層の社会的包摂に貢献する可能性が示されている。

昨年より本格化したスマートフォンやタブレット端末の世界的な普及は、このように進化したネットワーク・サービス環境に、パソコンに匹敵する機能を有する携帯端末を通じて、誰もが、どこでも接続し、インターネット上に展開する多種多様なサービスの利用を可能にしつつある。それは、インターネットショッピングやオンラインゲームなど従来からあるネット上のサービス利用を促進するとともに、よりパーソナルかつ文書閲覧に適したユーザーインターフェース機能を生かして、電子新聞や電子書籍の利用を飛躍的に拡大する潜在的効果も秘めている。我が国では、現在はスマートフォンの普及が先行しているが、米国では、電子書籍の内容充実を背景に、タブレット端末の普及も大きく伸びている状況にある。スマートフォン、タブレット端末の登場により、利用者は、複数のスクリーンを用途により使い分け、あるいは連携させるマルチスクリーン型のサービス利用がいつでも、どこでも可能となった。

図表 2-1-1-3 M2M 通信サービス事例



2 よくわかる u-Japan 政策(総務省/ユビキタスネット社会の実現に向けた政策懇談会) p.41

また、インターネットは、人と人との結びつきにとどまらず、モノとモノとの間でも、人間を介在せずに相互 に情報交換し、様々な機器に埋め込まれたセンサーネットワークにより自動的に最適な制御が行われるシステム (M2M) を通じてつながりを強めており、次に述べるビッグデータの活用とあいまって、社会インフラの効率的制 御や業務改善に役立てる動きが顕在化している(図表 2-1-1-3)。

このように、インターネット・携帯電話の社会基盤化、ワイヤレス・クラウド・ソーシャルを背景とするネットワー ク・サービス環境の進化に加えて、いつでも、どこでもネットワークへの入口であり出口として機能するスマート フォン等の登場により、ユビキタスネットワーク環境が具体的な全体像を顕したということができるだろう。ICT ネットワークは、単なるコミュニケーションツールを超えて、民主主義の基礎となる表現・言論の自由を確保し人 と人との絆を強化する基盤としての役割、様々な財・サービスがデジタル情報となって国境を越えて流通する基盤 としての役割を担うに至ったのである。

(3) ユビキタスネットワーク環境の完成に伴う新たな潮流 ースマート化ー 「スマート革命し

上記のインターネットの社会基盤化は、ネットワーク上に流通・蓄積されるデジタル情報の爆発的な増大をもた らしつつある。また、ユビキタスネットワーク環境の完成、とりわけクラウド、ソーシャル、高機能化した端末(ス マートフォン・タブレット端末)により、ネットワークを構成する各レイヤーが情報の分析・活用能力を備え、そ れを拡大しつつある。その結果、ネットワーク・サービスの運用主体を含めた利用企業等は、多種多量のデータ(ビッ グデータ)の生成・収集・蓄積が可能・容易になり、その分析・活用による異変の察知や近未来の予測等を通じ、 利用者個々のニーズに即したサービスの提供、業務運営の効率化等が可能になるとともに、ビッグデータの活用に よる新産業の創出も期待されている。

例えば、事業活動においては、ビッグデータの分析・活用により以下のような効用を通じて事業の効率的な実施 が期待されている。

- ・製品開発:どのような製品を開発することが消費者に対して訴求するかがわかる。
- ・販売促進:誰に、何を、いつ売ればよいのかがわかる。
- ・保守・メンテナンス・サポート:いつ、どのようなメンテナンスを行えばよいかがわかる。
- ・コンプライアンス:不正の予兆や、特に注視するべき事象が何であるかがわかる。
- ・業務基盤・社会インフラの運用:全般的な性能向上・コスト削減が実現される。

ビッグデータ活用は、既に各種オンラインショッピングサイトにおける利用者の購買履歴に応じたレコメンド表 示など具体化しつつある。現在、エネルギーの効率的利用等の観点から注目を集めているスマートグリッドも、社 会インフラ運用におけるビッグデータ活用の一類型であるといえよう。

このように、ユビキタスネットワーク環境において、多種多量の情報の流通・蓄積とその分析・活用が進展す ることにより、ICT ネットワーク・サービスは新たな付加価値が創造される知識創造基盤となり、第1章で詳細

図表 2-1-1-4 デジタルデータの成長と「ビッグデータ」の定量的価値

いわゆる「ビッグデータ」の定量的価値(例)

50億台の携帯電話が使用(2010年)

300億のコンテンツが毎月Facebook上で共有

IT費用の5%増加で、年間40%増のデータ創出

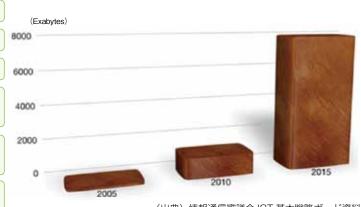
米国のヘルスケアでは年間3000億ドルの価値 創出が期待(スペインの年間ヘルスケアコストの2倍)

EUの公共セクターでは年間2500億ユーロの価 値創出が期待(ギリシアのGDPを超える)

個人の位置情報データを活用することで**年間** 6000億ドルの消費者価値創出が期待

小売の営業利益に60%改善の見込み

10年間のデジタルデータの成長



(出典) 情報通信審議会 ICT 基本戦略ボード資料 ([2011 Digital Universe Study:Extracting Value from Chaos] (IDC/2011.6),[Big data:The next frontier for innovation.competition.and productivity」(McKinsey Global Institute/2011.5) により作成)

に分析した ICT がもたらす 成長への2つの道筋、すな わち企業・家計・政府が生 産性向上その他様々な課題 解決の原動力としての役割 と、アプリケーションサー ビス、通信サービス、機器 製造など ICT 産業の裾野の 広い生産・雇用創造の役割 双方が飛躍的に強化される ことが見込まれる。いわば、 ユビキタスネットワーク環 境と「スマート化」の融合 が、「スマート革命」ともい える ICT の新たな革新をも たらし、成長のエンジンと しての ICT、万能ツールと しての ICT の機能を強化し

図表 2-1-1-5 「スマート革命」のイメージ

●最近のスマートフォン等の普及、M2M通信の可能性、ビッグデータの活用への新潮流が、 「ユビキタス」と「スマート」の融合を加速し、「スマート革命」へ



つつ、我が国の社会経済活動全体の風景を変える可能性を秘めているといえよう。

2 サイバー空間の在り方に関する国際議論の動向

(1)サイバー空間とその役割

インターネットは、その上で多様なサービスのサプライチェーンやコミュニティなどが形成され、いわば一つの 新たな社会領域(「サイバー空間」)となっている。このようなサイバー空間の持つ重要性や価値の認識が高まって いく中、近年、サイバー空間の在り方に関して様々な国際機関や国際会合で議論が繰り広げられている。

(2) 新興・途上国における規制・管理強化の動き

2010年(平成22年)12月から2011年(平成23年)1月にかけて、チュニジアにおいて「ジャスミン革命」 と呼ばれる民主化運動が起こり、長期政権に終止符が打たれた。この革命に端を発し、中東・北アフリカ地域の多 くの国において、いわゆる「アラブの春」と呼ばれる民主化運動が発現し、エジプト・リビアなどにおいても長期 政権が崩壊した。

平成23年版情報通信白書(第2節)において、先進国以外でも、インターネット利用率は低いものの、チュニ ジア等ソーシャルメディアの利活用が進展している国が存在していることを指摘したが、これらの一連の動きにお いては、市民同士のリアルタイムな連絡や国内外への情報の発信などにおいて、インターネットやソーシャルメディ アが大きな役割を果たしたといわれている(トピック「『アラブの春』とソーシャルメディア」参照)。

アラブの春においてインターネットやソーシャルメディアが民主化運動に大きな役割を果たしたことを受けて、 新興・途上国においては、ネットへの規制や政府の管理を強化する動きが強まっている。

例えば、イランでは2011年(平成23年)6月に通信大臣が、国外のインターネットから切断された「ナショナル・ インターネット」構築のためのテストを開始する旨を発表した。

また、中国においては、同年11月に中国国家インターネット情報弁公室がインターネット接続事業者に対し健 全なインターネット文化発展のための管理強化を要請したほか、同年 12 月には北京市政府が中国版 Twitter「微 博 (ウェイボー)」の実名登録を義務付ける新たな規定を施行している。

ベラルーシにおいては 2012 年(平成 24 年)1 月に自国民・自国在住民による国外のウェブサイトへのアクセ スを禁止し、違反した場合に罰金を科す法律が導入された。

(3) サイバー空間の在り方に関する諸外国の取組状況

このような新興・途上国のネット規制や政府管理強化の動きに対して、2011年(平成23年)に入って、欧米諸国は、 首脳や閣僚が主導して情報の自由な流通やインターネットのオープン性等の基本理念を表明している。

米国のクリントン国務長官は 2010 年(平成 22 年)1 月を皮切りに、インターネット上における人権保護やイ ンターネットへのアクセスの自由を守る必要性に関するスピーチを行っているが、2011 年(平成 23 年)2 月からは、 インターネットがアラブの春において果たした役割を強調しつつ、その主張を強めている。

2011年(平成23年)5月には米大統領府が「サイバー空間の国際戦略」を公表した。この戦略は、①開放的な、 ②相互運用可能で、③安全な、④信頼性の高いサイバー空間を将来にわたり維持発展させることを目的として、幅 広い課題を認識した上で包括的に国際連携に向けた方針を示した米国初の戦略である。①基本的自由、②プライバ シー、③情報の自由な流通の3つを中核的な原則とし、経済やネットワークの保護、インターネットの自由等の領 域について優先すべき政策課題として取組を実施することとした。

英国では2011年(平成23年)2月、ヘーグ外相がミュンヘン安全保障会議において、「全ての人がサイバー空 間にアクセスする能力を持つ必要性」や「サイバー空間のイノベーションのオープン性と思想、情報、表現の自由 な流通の保障」などを含むサイバー空間における「7 つの原則」を提唱した。さらに英国政府は、同年 11 月に「英 国サイバーセキュリティ戦略」を公表した。この戦略においては、2015 年(平成 27 年)をターゲットとした英 国におけるサイバーセキュリティのビジョンを掲げるとともに、当該ビジョンを達成するための目標、官民等のパー トナーシップでの取組並びにセキュリティと自由及びプライバシーの両立等の基本原則、個人・民間セクター・政 府それぞれの役割及び責任が言及されている。

(4) サイバー空間の在り方に関する国際的な議論の状況

2011年(平成23年)はインターネットに関わる様々な国際会合が開催され、サイバー空間の国際ルールの在 り方に関する議論が活発に行われた。

同年5月にドーヴィル(フランス)で行われた G8 ドーヴィル・サミットでは、3 つの優先課題の一つとしてイ ンターネットが取り上げられた。首脳宣言においてインターネットがグローバル経済成長の牽引力であることが確 認されるとともに、①クラウドコンピューティング等の新たなサービスによるイノベーション・成長機会の認識、 ②知的財産侵害への対応、個人情報保護、セキュリティ等における国際協力の推進、③児童のための安全なインター ネット利用環境整備等について盛り込まれ、採択された。

また、同年11月にロンドン(英国)で開催されたロンドン国際サイバー会議においては、サイバー空間の経済的・ 社会的便益、サイバーセキュリティの確保、サイバー空間における国際安全保障等が議題となった。特にサイバー 空間の①経済成長・発展、②社会的便益、③サイバー犯罪、④安心・安全なアクセス、⑤国際安全保障について分 科会が設けられ議論が行われた。

同会議の議長声明においては、①世界規模での自由な情報流通、思想・表現の自由を推進・保護し、投資を促進 するとともに、国境を越えたサービスの発展を支える政策が求められる旨が確認されたこと、②人権保障を阻害し ない範囲でのサイバーセキュリティの確保、言語・文化・思想の多様性の尊重、プライバシー・個人データの保護、 デジタル・ディバイドの解消等についての必要性が確認されたこと、などの内容が盛り込まれた。

また、このフォローアップとして、2012 年(平成 24 年)10 月にハンガリーでブダペスト国際サイバー会議が 開催される予定である。

このほかにも、2011 年(平成 23 年)には、6 月にパリ(フランス)で開催された OECD インターネット経済 に関するハイレベル会合や同年 10 月にパリで開催された New World2.0(インターネット大臣級セミナー)、同 年 11 月にアヴィニヨン(フランス)で開催されたアヴィニヨン文化サミット 2011(G8 文化大臣会合)、12 月に ハーグ(オランダ)で開催されたフリーダムオンライン閣僚級会合等において、インターネットやサイバー空間の 在り方に関する議論が行われた。これらのうち、ハーグで開催されたフリーダムオンライン閣僚級会合においては、 インターネット上の表現の自由の保護を目的として形成された有志による共同宣言(Joint Action)が発表された。 また、12 月の OECD 理事会においては、前述の OECD ハイレベル会合で策定されたインターネット政策立案の ための原則が勧告化された。

国連総会第一委員会(国際安全保障・軍縮担当)は、2010年(平成22年)12月、「国際安全保障の文脈にお ける情報及び電気通信分野の進歩」に関する政府専門家グループを設置して国家の ICT 利用に関する規範につい て 2012 年 (平成 24 年) から 2013 年 (平成 25 年) にかけて議論することを決定した。これを受け、2011 年 (平 成23年)9月、ロシア・中国・ウズベキスタン・タジキスタンの4か国が、国連総会に「情報セキュリティのた めの国際行動規範(案)」の共同提案を行った。この行動規範(code of conduct)案においては、①テロリズム、 分離主義、過激主義を扇動する情報や、他国の政治、経済、社会的安定性や精神的・文化的環境を弱体化させる情 報を阻止するために協力すること、②他国の政治経済社会の安全保障に脅威を与えるためにそのリソース、重要イ ンフラ、中核技術やその他の優位性を使用することを防ぐため、ICT 製品や ICT サービスの安全を確保するよう 努力すること、③情報スペースにおける権利及び自由については、関連する国内法令に従うという前提で十分に尊 重すること、といった事項が盛り込まれており、情報セキュリティの確保に関し、各国の主権の尊重を強調する内 容となっている。

国連総会第二委員会(経済・金融担当)においては、委員会はもとよりその委託を受けた経済社会理事会下部の 科学技術委員会においても、世界情報社会サミット(WSIS)のフォローアップの一環としてインターネットガバ ナンスの在り方に関する議論が行われている (第5章第7節参照)。

また、ITU 憲章や条約を補完する業務規則であり、国際電気通信業務の提供、料金決済等について取り決めて いる国際電気通信規則(ITR)が、2012年(平成24年)12月にドバイ(アラブ首長国連邦)にて開催される世 界国際電気通信会議(WCIT-12)において、1988年(昭和63年)に制定されてから初めて見直されることとなっ ている。インターネットに関連する新たな課題を盛り込むかどうかが焦点のひとつであり、2011 年(平成 23 年) 9月には、中国が、「国が通信セキュリティ確保の責任を負い、権利を有する」との趣旨の条文案を提案した。こ れに対し、我が国からは、「国が電気通信事業者に対してセキュリティ確保措置を奨励する」旨の対案を提案し、 2012年(平成24年)3月のアジア地域内の調整では、我が国の対案が多数の支持を集めた。なお、同年4月に はロシアが、「国による加入者の特定、主権・国家安全保障等の侵害を目的とする国際通信サービスの利用制限、 競合するインターネット資源管理メカニズムの構築」といった趣旨の条文案を提案しており、今後 ITU 会合にお いて調整が図られることとなる。

(5) 我が国の対応と今後の課題

我が国は、米国、英国、欧州委員会等との二国間会合において議論を行っており、また、多国間会合においても 積極的に議論に参画している。

米国との間では、2012年(平成24年)1月に「日米情報通信技術(ICT)サービス通商原則」を策定し、そ の原則の一つとして、国境を越える情報流通を妨げるべきではないことを掲げた。同年3月にはインターネットエ コノミーに関する日米政策協力対話においてインターネットのオープンな特性と相互運用性の維持の原則を再確認 し、さらに同年4月の日米首脳会談で公表されたファクトシートにはサイバー空間に関する問題についての連携深 化が盛り込まれた。

英国との間で、同年4月に公表された日英両国首相による共同声明においてサイバー空間に関する二国間の協 議の強化等が盛り込まれたことを受け、同年5月に川端総務大臣とハント文化・オリンピック・メディア・スポー ツ大臣との会談において、インターネット政策課題における日英間での連携を確認する共同声明を発表した。この 声明では、①インターネットガバナンスについて、マルチステークホルダーアプローチが最善の方法である、②イ ンターネット政策が、国際レベルで首尾一貫性があり、整合的であることを確保する、③現在の情報の自由な流通 を享受し続けることができるよう国際的なコンセンサスを実現するために相互に協力する、といったことが確認さ れた。

さらに、欧州委員会との間においても、同年5月に川端総務大臣と欧州委員会クルース副委員長との間でインター ネットに係る政策課題における日 EU 間での連携等を内容とする共同声明を発表した。この声明では、①インター ネット政策が、国際レベルで首尾一貫性があり、整合的であることを確保する、②情報の自由な流通が不当に制約 されることのない国際的なコンセンサスを実現するために相互に協力することについて確認されたほか、サイバー 空間におけるセキュリティ確保に向けて連携するために日EUインターネット・セキュリティフォーラムの開催に 合意したこと等が盛り込まれた。

サイバー空間の在り方の国際的な議論は、今後、インターネットが果たしている国民生活や経済活動の土台とし ての役割、社会経済システムにイノベーションをもたらす重要な社会基盤としての役割、民主主義の発展や基本的 人権の保障のための支えとしての役割、プライバシー・個人情報の保護、情報セキュリティの確保、知的財産権の 保護など、多角的に行われる可能性がある。我が国としても、今後の我が国の目指すべきビジョンに資する国際ルー ルづくりがなされるよう積極的に議論に参加している。

トピック

「アラブの春」とソーシャルメディア

アラブの春(Arab Spring)とは、2010年(平成22年)から2011年(平成23年)にかけてアラ ブ世界において発生した民主化運動の総称であり、2010年(平成22年)12月のチュニジアでの「ジャ スミン革命」から、アラブ世界に波及し、現在も続いている。アラブの春をめぐる主な事件を挙げると、 以下のとおりである。

図表 1 「アラブの春」を巡る主な事件

国	期間	概要
チュニジア	2010年12月 ~ 2011年3月	●2010年12月にチュニジア南部の町Sidi Bousid(シディ・ブジット)で起きた事件(※)をきっかけに、職の権利、発言の自由化、大統領周辺の腐敗の罰則などを求め、全国各地で連日ストライキやデモが行われた。こうした抗議のデモは、政府の長期体制そのものに対するデモへと急速に展開することとなり、僅か1ヶ月後の2011年1月に、22年に及ぶベン・アリ政権が崩壊した(ジャスミン革命と呼ばれる)。 ●抗議デモが広がるにつれ、その様子を携帯電話、ビデオカメラで録画した画像や動画が、事件当日からFacebook、YouTubeに次々とアップロードされた。Facebookには政府に抗議する複数のグループに1週間で1万人以上が参加し、YouTubeでは"Sidibousid"とタグ付けされた動画が3万件にも及んだ。また同様のハッシュタグを通じて、Twitterでは関連のコメントが大量に投稿され、反政府運動に関連するツイートを象徴するものとして情報が拡散した。 ● さらに、政府に危害を加えられる心配のない海外在住のチュニジア人がハブとなり、情報が近隣諸国を中心に海外にも急速に広まった。2011年1月14日から16日の間に18%のジャスミン革命関連のツイートはチュニジア国内から発信され、8%は近隣諸国、32%は海外から発信されたものだった。 ● ベン・アリ前大統領が亡命した当日も、ハッシュタグ"Sidibousid"のツイート数は総計13,262件に及んだ。また、当日のチュニジア国内のプログの約25%は、旧アリ政権に関する評価について記されたものであり(前月は5%)、"革命"が主要トピックとして続いた。** ※26才の青年が警察官によるたび重なる嫌がらせに耐えかね、自らのから体に火を付けて警察、行政に抗議(半年後に死去)。
エジプト	2011年1月~ 2011年2月	●ジャスミン革命をきっかけに2011年1月より大規模な反政府デモが発生し、デモ開始から僅か1ヶ月後の2月に、旧ムバラク政権はエジプト軍最高評議会に国家権力を譲渡し、29年に及ぶ政権に終止符が打たれた。 ●チュニジアと同様に、Facebook、YouTube、Twitpic等のサイトを通じてインターネット上で画像・動画等多くの情報が拡散した。反政府に係る情報共有のために2010年頃より急速に登録者が拡大したFacebookページ。We Are All Khaled Said"を中心に、デモ参加者間の情報共有などが活発化した。同サイトは大規模デモ(2011年1月25日)の計画を宣言し、9万以上の参加者が登録したとされる。。 ●エジプト政府は、こうした反政府デモの混乱を鎮圧するために、Twitterの接続をブロックした後、広い地域において1月28日から5日間にわたりインターネット接続の遮断を行った。しかし、ネット回復後、その反動でエジプト内のFacebookユーザー数が爆発的に拡大、政権崩壊の直前の2週間でFacebook内に32,000のグループ、14,000のページが新たに作成された。。さらに、政権文代に係るエジプト内のTwitterのツイートは10倍にも拡大したとされている。エジプトの政治に関するツイートは1日2300件だったものが、革命中には23万件に増加し、550万人の人々がネットに投稿された動画を見ている。またツイートやプログ投稿の多くは周辺国を中心とする海外からのものだった。ハッシュタグ半egypt /#jan25が、2011年第1四半期にアラブ地域で最も多いツイートを記録している(同期間中、#egyptのメンションは約140万、#jan25は約120万)10。 ●革命後、2月18日にエジプト軍最高評議会がFacebookのページを開設し、国民との対話を始めている11。
リビア	2011年2月~ 2011年8月	●2011年2月15日に発生した人権活動家の弁護士の釈放要求デモをきっかけにカダフィ大佐の退陣を求めるデモが国内で拡大し、2011年8月に42年に及ぶカダフィ政権が崩壊するに至った。 ●インターネットインフラを厳重に制御していた旧政府は、デモの拡大を受け2月18日には同国内のインターネットの接続を遮断し、とりわけFacebookやTwitter等のソーシャルメディア、アルジャジーラの報道サイトの遮断からはじめたとされる ¹² 。こうした動きや、また他アラブ国と比べネット利用率が低いこと等から、革命は成功したものの、チュニジアやエジプトと比べるとソーシャルメディアの活躍は限定的であったと言われている。
イエメン	2011年1月~ 2012年2月	●サーレハ大統領(当時)の退陣を求める反政府抗議活動が発生し、2011年2月3日のデモでは2万人以上が集る大規模なものとなった。サーレハ大統領はその前日の2月2日、2013年に行われる次期大統領選に出馬しないこと、世襲もしないと表明するとともに、11月になって副大統領に大統領権限を移譲することに同意。12月10日に暫定政権が発足。 ●教育水準やネット普及率が低い状況でありながらも、若年層の比率が高いことから、一部においてソーシャルメディアが活用されている。いわゆる活動家が始めたFacebookやTwitterなどのソーシャルメディア上のキャンペーン等が展開し、多くのイエメン人が、TwitterやFacebookでキャンペーンに参加し、宣伝に加わったとされる。中にはノーベル平和賞受賞者でイエメンの中心的活動家であるTawakkol Karmanも含まれ、Facebook上でキャンペーンロゴを同士のプロフィール写真として使っている。反体制デモの中心地チェンジ広場(Change Square)では、Media Committeeと自称するグループが革命における民衆の声として、プログ、YouTube、Facebook等を通じて情報を発信している13。

(出典) 総務省「情報通信産業・サービスの動向・国際比較に関する調査研究」(平成 24 年)

このようなアラブの春の動きに、ソーシャルメディアはどのような役割を果たしたのだろうか。ドバイ の政府系シンクタンクであるドバイ政府校(Dubai School of Government)が、FacebookとTwitter の市民運動への影響について調査分析を行っており 14、その内容を紹介しつつ、「アラブの春」へのソーシャ ルメディアの影響を概観する。

チュニジアで発生した「ジャスミン革命」以降のデモ活動について、図表2に示すとおり、2月4日の シリアでの抗議活動を除き、ソーシャルメディアにおいて参加の呼びかけが行われている。アラブ地域で

- 3 http://www.tgdaily.com/software-features/58426-arab-spring-really-was-social-media-revolution http://www.onlinesocialmedia.net/20110118/tunisia-twitter-revolution-social-media-aspects/
- http://gigaom.com/2011/01/14/was-what-happened-in-tunisia-a-twitter-revolution/
- 5 Project on Information Technology and Political Islam: (アメリカのワシントン大学のプロジェクトで、300 万件のツイート、YouTube に投稿された動画、ブログなどの分析を通して、ソーシャルメディアを介してチュニジアやエジプトの情報が世界中に広がっていた姿 を数値的に分析)
- 6 http://www.nytimes.com/2011/01/26/world/middleeast/26egypt.html?_r=1&hp http://www.thedailybeast.com/newsweek/2011/01/22/the-revolution-comes-to-egypt.html
- http://www.csmonitor.com/Innovation/Horizons/2011/0202/Egypt-reopens-Internet-Facebook-access
- 8 http://www.huffingtonpost.com/2011/02/02/egypt-facebook-use-internet_n_817710.html
- 9 http://dl.dropbox.com/u/12947477/publications/2011_Howard-Duffy-FreeIon-Hussain-Mari-Mazaid_pITPI.pdf
- 10 http://www.dsg.ae/en/ASMR2/Images/report.pdf
- 11 http://bikyamasr.com/27802/supreme-military-council-promotes-itself-on-facebook/
- 12 http://www.huffingtonpost.com/2011/02/18/libya-internet-shut-down-_n_825473.html
- 13 http://english.al-akhbar.com/content/social-media-yemen-expecting-unexpected
- 14 "Civil Movements: The Impact of Facebook and Twitter" Dubai School of Government 2011 年(平成23年)5月

の抗議の呼びかけの多くは、主として Facebook によりなされており、同校では、「Facebook が、人々 が抗議行動を組織した唯一の要因ではないが、それらの呼びかけの主たるプラットフォームとして、運動 を動員した要因であることは否定できない。」とし、「Facebook の浸透度が低い国においても、活動の中 核にいる人々が他のプラットフォームや伝統的な現実世界の強固なネットワークを通じてより広いネット ワークを動員する有益なツールであった。」としている。また、その一方で、抗議活動自体が、アラブ世界 における Facebook 利用者の増加につながっているとみられるとしている(図表3)。

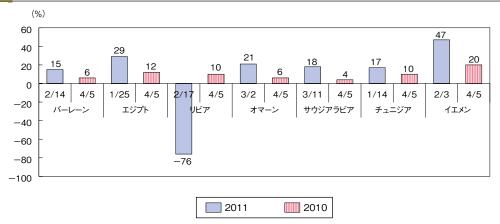
図表 2 デモ活動に係る Facebook による抗議の呼びかけ

Facebook普及率*	18.8%	5.5%	0.93%	1.19%	32%	4.3%	7.8%	12.9%	1.67%	12.8%
	Yes**	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
デモの有無										
国名	チュニジア	エジプト	イエメン	シリア	バーレーン	リビア	オマーン・	サウジアラビア	シリア	パレスチナ
Facebookでデモの呼び かけがあった日付	1月14日	1月25日	2月3日、10日	2月4日	2月14日	2月17日	3月3日 3	3月11日、20日	3月15日 以降	5月15日
出典	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)

- 抗議活動開始時点での、各国におけるFacebook普及率
- 最初の抗議活動はFacebook上での呼びかけでははなかったが、その後の活動では行われていた。
- (1) http://www.thedailybeast.com/blogs-and-stories/2011-01-15/tunisa-protests-the-facebook-revolution/
- (1) http://www.newanyon.com/2011/01/22/the-revolution-comes-to-egypt.html
 (3) http://articles.cnn.com/2011-02-10/world/yemen.student.protest_1_student-protest-demonstration-facebook?_s=PM:WORLD
- (4) http://www.google.com/hostednews/afp/article/ALeqM5gmg4rvAfz5HpVrBLnRRPpOxQUwvQ?docld=CNG.48f3fb2a5d4e5791795d 8c3f3b8c5311.8e1
- (5) http://www.google.com/hostednews/afp/article/ALeqM5i2YM2LCYTyiuV6jLNIhaLdIPiOAA?docId=CNG.174090b19aab9f0dd09252 4489bf4699.331
- (6) http://globalyoicesonline.org/2011/02/16/libya-protests-begin-in-benghazi-ahead-of-february-17-day-of-wrath/
- (7) http://www.nytimes.com/2011/03/01/world/middleeast/01oman.html
- (8) http://www.reuters.com/article/2011/02/23/us-saudi-facebook-idUSLDE71M08Q20110223
- (9) http://www.bbc.co.uk/news/world-middle-east-12749674

(出典) Civil Movement: The Impact of Facebook and Twitter / Dubai School of Government

2011年 (平成 23年) における Facebook 利用者の増加率 (2010年 (平成 22年) 同時期との比較)

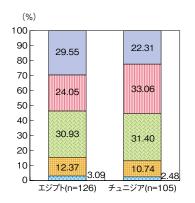


(出典) Civil Movement: The Impact of Facebook and Twitter / Dubai School of Government

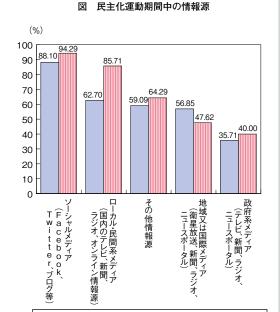
同校がエジプト・チュニジア両国の Facebook 利用者に対して行った市民運動期間中の Facebook 利 用調査によると、「アラブの春」の期間中に Facebook を使用した主な理由は「運動の背景に関する認知 度を高めること」が両国で最も高く、運動や関連情報に関する情報発信や、運動に係る計画や活動家間の 管理を含めると、8割を超える利用者が市民運動関係の情報行動を Facebook において行っていたことに なる (図表 4)。 また、「市民運動期間中に、どこから事件に関する情報を得ていたか。」 との質問に対しては、 ソーシャルメディアとの回答が両国とも最も高い(図表 4)。

図表4 民主化運動期間中のソーシャルメディアの利用(エジプト・チュニジア)

図 2011年初頭の民主化運動期間中のFacebookの主な利用用途



- 運動に係る計画や活動家(集団や個人)間の管理のため
- 運動や関連情報に関する情報発信のため
- 運動の背景に関する国内の認知度を高めるため
- エンタテインメント/ソーシャル利用(友人との交流、ゲーム等)のため
- **※※** その他



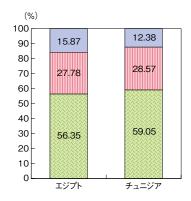
■ チュニジア(n=105)

(出典) Civil Movement: The Impact of Facebook and Twitter / Dubai School of Government

なお、両国での調査では、政府機関によ るインターネットの遮断の効果についても 質問しているが、両国で半数以上が、より 人々の活動を活発化させるなど社会運動側 にとって肯定的影響があったと回答してい ることが興味深い(図表5)。このように、 「アラブの春」の動きは、ソーシャルメディ アと密接な関係にあり、ソーシャルメディ ア利用者は、表現の自由に対する価値観を 強めているといえるだろう。

図表 5 政府によるインターネット遮断の抗議活動への影響

■ エジプト(n=126)



- 影響なし:インターネットの遮断、Facebookのブロッキングは活動に まったく影響を与えなかった。
- 否定的影響があった:コミュニケーションや活動準備に人々が利用 している主たるチャネルが遮断された。
- 肯定的影響があった:団結を高め、決意を固めていなかった人々を 活動へと後押した。コミュニケーションや団結のための創造的方法 の開拓を促した。

(出典) Civil Movement: The Impact of Facebook and Twitter / Dubai School of Government

深刻化するサイバー攻撃への対処と情報セキュリティ確保に向けた課題

(1) 近年の情報セキュリティに関する脅威の動向

インターネットがグローバル社会における社会経済活動に不可欠の基盤となる中で、世界規模でのコンピュータ ウイルスのまん延、サイバー犯罪の増加、国民生活・社会経済活動の基盤となる重要インフラにおけるシステム障 害など、情報セキュリティに対する脅威が世界的に拡大し、その対処が国際課題となり、前述のとおりサイバー空

図表 2-1-3-1 ウイルス種類の増加状況

データベースに登録されたマルウェアサンプルの合計 70,000,000 60,000,000 50,000,000 40 000 000 30,000,000 20,000,000 10,000,000 010年 2011年 1月 2月 3月 4月 5月 6月 7月 8月 9月 10月11月12月1月 2月 3月 4月 5月 6月

(出典) 総務省「情報通信産業・サービスの動向・国際比較に関する 調査研究」(平成 24 年)(マカフィー社資料により作成)

間の国際ルールづくりの主要テーマとして議論が進め られている。我が国においても、平成23年9月に判 明した三菱重工業等に対するサイバー攻撃事案をはじ め、国家の中枢である衆議院・参議院両院が攻撃を受 けるなど、従来の「愉快犯」的な攻撃から、我が国の 重要な情報の窃取を意図したものと想定される標的型 攻撃の脅威が顕在化したところである。また、1に示 したクラウド、ソーシャル、スマートフォンの普及等 のユビキタスネットワーク化の進展や、ICT への依 存度の更なる高まりに従い、スマートフォン等を狙っ たマルウェアの増加など、新たなリスクも表面化しつ つある。このような情報セキュリティを取り巻く環境 変化に対し、早期の情報共有、官民連携の強化など関 係者が一体となった対策の強化の必要性に直面してい る。

2011年(平成23年)に我が国において脅威が顕在化した標的型攻撃は、一般に情報窃取等を目的に少数の攻 撃対象に密かに潜入して行われるものであり、これまでに多数発生していた DDoS 攻撃(分散サービス不能攻撃) のように攻撃を顕示するものとは性格が異なっている。

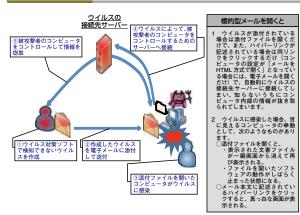
標的型攻撃メールでは、攻撃対象に合わせて時事情報等を利用し、メールの文面を巧妙化して開封させやすくす るなど、高度なソーシャルエンジニアリングの手法が用いられている(図表 2-1-3-2)。また、メールを介して感 染したマルウェアが情報システム内に潜伏し、更にネットワーク利用者を管理するサーバーへ侵入を試みるなど技 術的に洗練されたものもあるが、更に進化すると見込まれている。

2011 年(平成23年)には複数の府省庁に標的型攻撃メールが届いたと報告されているが、そのうち、一部の 省庁では職員が標的型攻撃メールに添付されたファイルを開封し、マルウェアに感染する結果となった。また、衆

議院及び参議院にも標的型攻撃メールが送信され、開 封した国会議員の端末がマルウェアに感染したほか、 国の重要な情報を扱う一部の企業においても、標的 型攻撃メールを介してマルウェアに感染し、情報が 窃取された可能性が生じるなど、その被害は広がり をみせている。

なお、セキュリティベンダーのシマンテック社が 2012年 (平成24年) 4月に公表したレポートによ れば、2011年(平成23年)12月には一日平均154 件の標的型攻撃が発生しており、その対象は、政府や 大企業のみならず幅広い業種や中小企業に及び、職 種も広範な範囲に及んでいるとしている(図表 2-1-3-3)。

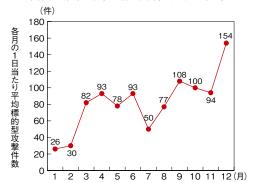
図表 2-1-3-2 標的型メール攻撃(イメージ図)



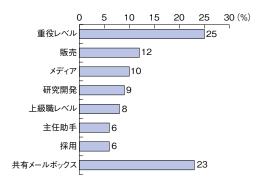
内閣官房情報セキュリティセンター資料により総務省作成

図表 2-1-3-3 世界における標的型攻撃の増加

- ●標的型攻撃の増加 1日当たり平均 77件(2010)→82件(2011)
- ●2011年各月の標的型攻撃の増加傾向(一日当たり平均)



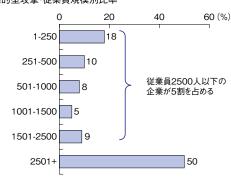
●標的とされた受領者の役職等の分析



●標的型メール攻撃・上位10位の部門別比率



●標的型攻擊·従業員規模別比率



(出典)総務省「情報通信産業・サービスの動向・国際比較に関する調査研究」(平成 24 年) (INTERNET SECURITY THREAT REPORT 2011Trends(Symantec 社)より作成)

なお、「サイバー攻撃」については厳密な定義は存在しないが、いわゆる「サイバー攻撃」に該当する行為につ いては、図表 2-1-3-4 のように整理することができる。

図表 2-1-3-4 いわゆる「サイバー攻撃」と政府の対応

サイバーな転の手法	=±\// > = XD 999	政府の主な対応					
サイバー攻撃の手法	該当しうる犯罪	被害防止、把握	発生時対処				
・不正侵入 ・不正コマンド実行	不正アクセス行為 (不正アクセス禁止法) 等	「政府機関の情報セキュリティ対策のための統	「政府機関の情報セキュリティ対策のための統 ・犯罪捜査(必要に応じ、ICPO等を通じ、捜 協力を外国治安機関等に依頼)	が生じ、若しくは生じる			
・ウイルス攻撃	不正指令電磁的記録 作成・供用罪 (刑法) 等		(政府機関) ・情報集約・共有による被害拡大防止 (重要インフラ)	恐れのあるサイバー攻撃 事態又はその可能性のあ る事態である場合			
・データ改ざん・破壊 ・DoS 攻撃	電子計算機損壞等業務妨害 (刑法) 等	る第2次行動計画」に基づく「安全基準」等の整備・浸透 (企業等・個人)	・セプター等を通じた情報共有による被害拡 大防止 (企業等・個人)	官邸危機管理センターに官邸 対策室等を設置し、初動対処 を実施			
・情報漏えい ・重要情報の窃取	(準備行為として不正侵入 やウイルス攻撃が行われる ことがほとんど)	・官民の情報共有による被害防止 ・情報セキュリティ月間等による普及啓発	・相談窓口での相談受付				

内閣官房情報セキュリティセンター資料により総務省作成

最近の我が国及び各国におけるサイバー攻撃事例については、図表 2-1-3-5 に示すとおり、特にその内容におい て深刻度を増してきており、国の安全や国民生活に関わる政府機関や重要インフラ等に対する攻撃に対し、上記2 に示したとおり、ドーヴィル G8 サミット首脳宣言をはじめ各種国際会議において重大な懸念が示されており、サ イバー空間の国際ルールづくりに併せて、サイバー空間の情報セキュリティ確保についても国際連携により対処す ることの重要性が繰り返し示されている 15。

¹⁵ 例えば、2011 年 5 月 G8 ドーヴィル・サミット首脳宣言において、サイバー攻撃に対する以下のような懸念が示されている。 「17. インターネッ 耐えば、2011年5月 GO ドーウィル・リミッド自動宣言において、サイカー収撃に対するは下のような感恩が小されている。「T. インダーネットトークスがサービスの安全は、様々な利害関係者に関わる問題である。・・・インターネットを通じた有害ソフトの拡散及びボットネットの活動による攻撃を含め、インフラ、ネットワーク及びサービスの公正性に対するすべての形態の攻撃には、特別な注意を払わなければならない。・・・インターネットが、平和及び安全という目標と整合的でない目的で、かつ、重要なシステムの公正性に悪影響を与え得る目的で使用される可能性があるという事実は、依然として懸念事項である。」

図表 2-1-3-5 最近のサイバー攻撃事例

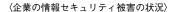
時期	業種(国)	攻撃概要			
2007年4月	政府 (エストニア)	エストニア政府機関等がDDoS攻撃を受けた。政府機関、報道機関、銀行等のWEBサイトが利用不能になり、電子商取引、オンライン決済等にも障害が発生した。			
2008年8月	政府 (グルジア)	グルジア政府WebサイトがDDoS攻撃を受けた。ロシア軍がグルジア攻撃中の出来事であり、政府機関、報道機関、銀行等のウェブサイトが利用不能に なった。			
2009年7月	政府 (米国)	米国のホワイトハウスや国務省等の政府関係機関14サイトが大規模なDDoS攻撃を受けた。			
2009年7月	政府 (韓国)	韓国の青瓦台や国会等の政府関係機関21サイトが大規模なDDoS攻撃を受けた。			
2009年12月	企業 (米国)	可用性が高いと言われたDNSプロバイダー NeuStar社のUltraDNSサービスbotnetによりDDoS攻撃を受けた。また、そのサービスを利用する企業が提供 しているWEBサービスが引きずられて利用不能になった。			
2010年1月	金融 (米国)	ニューヨーク州ロングアイランドのSuffolk County National Bank(SCNB)において、ハッカーがオンラインバンキングシステムをハッキングした。ID・パスワードファイルがSQLインジェクションで抜き取られ、不正侵入された。			
2010年2月	政府機関 (ラトビア)	ラトビア国税庁において、電子納税システムがハッキングされた。ID・パスワードがSQLインジェクションで抜き取られ、不正侵入された。			
2010年4月	企業 (米国)	テキサス州の大手電力会社Lower Colorado River Authorityのコンピュータシステムに海外のある単一のIPアドレスから4800回の総当たり攻撃を受けた。実際にはログインされなかった。			
2010年7月	金融 (米国)	インディアナ州において、クレジットカードの中央処理システムがハッキングされた。ID・パスワードが、SQLインジェクションで抜き取られ、不正侵入された。			
2010年8月	電力 (イラン)	イランの原子力発電所へのスタックスネットによる攻撃が判明した。その後、ナタンズにある核燃料施設のウラン濃縮用遠心分離機を標的としたサイバー攻撃も判明し、遠心分離機が全て停止した。			
2010年9月	政府 (日本)	日本の政府機関等がDDoS攻撃を受けた。			
2010年秋	政府 (カナダ)	ハッカーが、カナダ政府のIT職員をだまして政府のコンピュータにアクセスできるよう画策し、国家財政委員会及び財務省で深刻なインターネット障害が発生した。			
2010年12月	企業 (米国)	Google社、金融機関、政府機関、IT、金融、メディア、化学等、米国の30社以上が、Internet Explorerの脆弱性を狙った情報搾取用のプログラムを仕組まれるゼロディ攻撃をうけ、不正アクセスされた。			
2011年1月	政府 (エジプト)	ハッカー集団「アノニマス」がデモ鎮圧のため、インターネット回線を遮断したエジプト政府にDDoS攻撃を行い、機密情報の暴露を突きつけて回線の再開をさせた。			
2011年1月	政府 (アイルランド)	ハッカー集団「アノニマス」または「ラルズ・セキュリティー」のメンバーが、アイルランドの政党「統一アイルランド党」のWEBサイトを運用していた米アリゾナ州のサーバーに不正アクセスし、改ざんを行った。			
2011年3月	政府 (韓国)	韓国の大統領府や在韓米軍、銀行など国内主要約40機関がDDoS攻撃を受け、ホームページの閲覧が一時的に困難になった。			
2011年4月	企業 (日本)	2011年4月16日〜17日に、Sony Online Entertainmentのシステムが不正アクセスを受け、約2,460万人分のアカウントの個人情報が流出した。さらに、4月 17日〜19日に、Sony Computer Entertainment Americaのゲーム機向けオンラインサービス「PlayStation@Network」及び映画・音楽配信サービス 「Qriocity」が不正アクセスを受け、約7,700万人分のアカウントの個人情報が流出した。合計約1億人分のアカウントの個人情報が漏洩した。			
2011年4月	金融 (韓国)	農協のサーバーを管理する会社の社員のノートパソコンがウイルスに感染し、ハッカーの遠隔管理下に置かれ、サーバーに対する攻撃が行われた。 これにより農協のATMサービスを含む金融取引が一時停止するなどの被害が発生した。			
2011年6月	金融 (国連)	国際通貨基金(IMF)のコンピューターシステムがサイバー攻撃を受けていたことが判明した。			
2011年7月	政府 (イタリア)	ハッカー集団「アノニマス」がイタリアのサイバー犯罪対策機関CNAPICから盗み出された情報を入手し、一部を公開した。			
2011年夏	政府 (英国)	英外務省を含む複数の政府機関に対して相当規模のサイバー攻撃が行われたが、未遂に終わった。			
2011年9月	企業 (日本)	三菱重工が標的型攻撃を受けていたことが判明した。			
2011年10月	政府 (日本)	衆議院・参議院が標的型攻撃を受けていたことが判明した。衆議院ではPCとサーバー計32台、参議院ではPCとサーバー計31台の感染が認められた。また、外務省や在外公館、国土地理院等へもサイバー攻撃が行われていたことが判明した。			
2011年11月	企業 (日本)	富士通が運用している電子申請システムのサーバーがサイバー攻撃を受けた。10県、約200自治体が利用しており、9県でサービスが一時利用できなくなる被害が確認された。			

(出典)総務省「情報通信産業・サービスの動向・国際比較に関する調査研究」(平成24年)

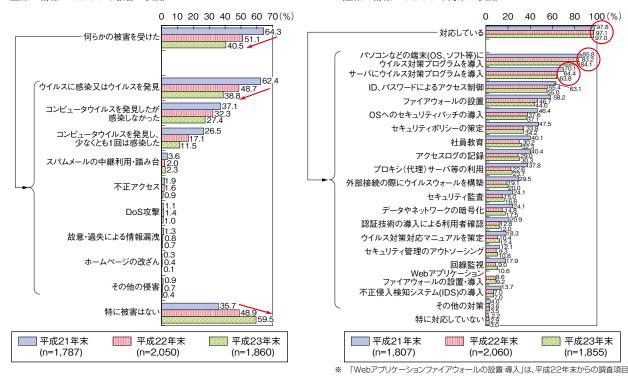
一方、我が国の企業におけるウイルス被害やその対策を含む情報セキュリティを巡る状況を最近3年間について 通信利用動向調査の結果からみると、「ウイルスに感染又はウイルスを発見」と回答した企業の比率は平成21年 調査の 62.4%から平成 23 年調査では 38.8%と大きく低下しており、逆に特に被害はないという回答は、平成 21 年調査の35.7%から平成23年調査では59.5%と大きく上昇している。対策の状況については、何らかの対策を 講じているとの回答が、平成21年調査から平成23年調査にかけていずれも97%台と高い水準で推移しており、 ウイルス対策プログラムをパソコンなどの端末やサーバーに導入する対策を中心に取組が進んでいる。企業の情報 セキュリティ全般でみれば、継続的な対策の浸透により情報セキュリティ被害の減少に一定の効果をあげているこ とがわかる。また、資本金規模別に被害及び対応状況について通信利用動向調査の結果からみると、おおむね企業 の規模と被害・対応状況には関連性が見て取れる。被害については、おおむね資本金規模の大きい企業に被害が生 じる傾向が高く、データセキュリティへの対応についても、10億円以上の資本金規模の企業は100%対応してい る一方、1,000万円以下の企業については約5%が未対応としている。

97.8 97.1 97.0

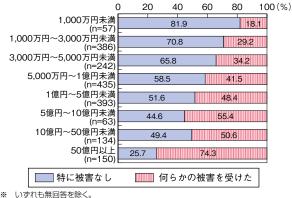
図表 2-1-3-6 企業の情報セキュリティ被害及び対策の状況



〈企業の情報セキュリティ対策の状況〉



過去1年間に情報通信ネットワークで受けた被害(資本金規模別・平成23年末)



※ いずれも無回答を除く。

データセキュリティへの対応状況(資本金規模別・平成23年末)



(出典) 平成 23 年通信利用動向調査

(2) 諸外国におけるサイバー空間への戦略的取組

ア 米国における取組

米国では、サイバー空間のセキュリティ確保に関連する組織として、国土安全保障省、国防総省・国家安全保障 局がある。国土安全保障省では、国防関係を除く連邦政府ネットワークや民間重要インフラの保護を主に、関連省 庁や FBI 等と連携してサイバーセキュリティ全般を所管している。他方、国防総省・国家安全保障局では、国防、 安全保障に関する分野を所管しており、2009年(平成21年)6月にはサイバー司令部を設立している。

米国での具体的な取組としては、2011年 (平成 23年)5月に上記 2(3)に示した「米国サイバー空間の国際戦略」 を発表したが、同月にホワイトハウスから、重要インフラのサイバーセキュリティ対策強化のための連邦省庁の権 限の明確化等を含むサイバーセキュリティ立法提案を公表している。

本提案では、①アメリカ国民の防護(情報漏洩の検知、コンピュータ犯罪への罰則)、②連邦政府のコンピュー タとネットワークの防護 (管理、人事、侵入防止システム、データセンター)、③国家重要インフラの防護 (産業界・ 州政府・地方政府への政府支援・任意の情報共有、重要インフラのサイバーセキュリティ計画)、④個人のプライ バシーと自由を守るためのフレームワークの構築について、各機関の権限の明確化や各種規律の策定等が示されて いる。

また、同年7月には、国防総省より、「米国サイバー空間上の作戦のための国防総省戦略」が公表された。これは、 2010年(平成22年)の「国家安全保障戦略」等を受けて、同省が初めてサイバー空間戦略を取りまとめたもので、 当該戦略では、同省がサイバー空間で効果的に作戦展開し、国家利益を保護し、安全保障上の目標を達成するため の指針として、①サイバー空間の作戦領域化、②ネットワーク・システムの防護、③米国政府機関や民間との連携 強化、④同盟国や国際的パートナーとの堅牢な関係構築、⑤人材開発・技術革新への投資の5つの戦略的イニシア ティブを提示している。

イ 欧州における取組

欧州連合では、欧州ネットワーク情報セキュリティ庁が、ネットワークセキュリティ及び情報セキュリティに関 する予防・対応能力を強化することを任務として、分析のための情報収集等を行っているが、近年のサイバーセキュ リティを巡る状況を踏まえ、2010 年(平成 22 年)9 月に EU 諸機関及び加盟国等のサイバーセキュリティ能力 向上支援など、同庁の役割強化が欧州委員会から提案されており、欧州議会及び加盟国政府により構成される理事 会において審議中である。

また、安全保障分野では、2007年(平成19年)4月のエストニアへのサイバー攻撃事案を機に、2008年(平 成20年)3月に、NATO加盟国のサイバー防衛能力向上のためのサイバー防衛センターが設立されている。同 センターは、エストニア、ドイツ、イタリア、スペインなど7か国が中心に活動し、サイバー防衛能力向上に関す る戦略・戦術の研究・訓練等を行っている。

個別国では、上記 2(3) に示した 2011 年 (平成 23年) 11 月の英国政府による 「英国サイバーセキュリティ戦略」 の公表のほか、ドイツ連邦政府においても「ドイツのためのサイバーセキュリティ戦略」が 2011 年(平成 23 年) 2月に閣議決定されている。同戦略では、安全なサイバー空間を確保し、ドイツの経済的・社会的繁栄を維持・促 進することを目的として、①基幹的な情報インフラの保護、②ドイツ国内での安全な IT システム、③行政機関に おける情報セキュリティの強化、④サイバー防御センターの設立、⑤サイバーセキュリティ評議会の設立、⑥サイ バー空間における犯罪の抑制、⑦サイバーセキュリティを強化するための EU 及び世界規模の効果的な連携、⑧信 頼性の高い情報技術の活用、⑨連邦政府における人材開発、⑩サイバー攻撃に対処するためのツールの 10 分野を 戦略分野として設定している。

(3) 我が国におけるサイバー攻撃に対する取組の強化

ア 三菱重工業等へのサイバー攻撃事案の発生とその対応

我が国では、平成 17 年に IT 戦略本部の下に情報セキュリティ政策会議、内閣官房に「情報セキュリティセン ター」が設置され、情報セキュリティ対策の強化に政府が一体となった取組を進めてきた。2011 年度(平成 23 年度)の年度計画である「情報セキュリティ 2011」(2011年(平成 23年)7月情報セキュリティ政策会議決定) では、冒頭に述べた近年の ICT の利用形態の急速な変化やサイバー攻撃等の脅威の複雑化・高度化など情報セキュ リティを取り巻く著しい環境の変化を踏まえ、それらに的確に対応するため、大規模サイバー攻撃事態への対処態 勢の整備や平素からの情報収集・共有体制の構築強化、スマートフォンの情報セキュリティ確保推進やソーシャル メディアの利用に係る情報セキュリティ確保など新たな環境変化に対応した情報セキュリティ政策の強化に係る施 策が盛り込まれている。

その後、三菱重工業等に対するサイバー攻撃事案が発生した。まず、防衛装備品や原子力プラントを製造して いる三菱重工業のコンピュータがウイルスに感染し、情報が抜き取られた痕跡ありとの新聞報道(平成23年9月 19日)があり、それに対し、同社によれば、標的型攻撃によるウイルス感染により、情報が流出した可能性があ るとされた事案である(ただし、製品や技術に関する情報の流出は確認されていない。)。その後、IHI、川崎重工業、 三菱電機に対しても同様の攻撃があったとの報道がなされたが、各社からは関係省庁からのヒアリング調査に対し て、調査時点で重要な情報の漏えいは確認されていない旨回答があった。

政府においては、直ちに内閣官房において全府省庁の担当課長等を集め、「政府内の迅速な情報共有」の徹底を 指示するなどの対応を進めるとともに、平成23年10月7日に情報セキュリティ政策会議を開催し、標的型サイバー 攻撃対策等について意見交換を行った。その上で、情報セキュリティ政策会議議長(内閣官房長官)名で、国民に 対するメッセージとして、「情報セキュリティ対策の強化について」を公表した。同メッセージは、官民連携の強 化に向けた取組方針を示すとともに、不正プログラムをめぐる現在の状況にどのように対応すべきかについて全て

の国民に対し提示されたものである。国民の重要な情報を扱い国の安全に深く関わる企業に対して、企業の情報セ キュリティの一層の強化や、政府・民間双方向の情報共有等の官民連携への協力を要請するとともに、一般企業等 に対して、職員の情報セキュリティ意識の向上、感染時に被害を最小限にとどめる対策の実施を呼びかけた。また、 国民全般にパソコンやスマートフォン等のセキュリティ関連ソフトを常に最新の状態に維持するなどの対策の実施 を呼びかけた。

同会議では、官民連携の強化のための分科会について設置方針が決定され、平成23年10月の設置以降鋭意検 討が行われ、平成24年1月の情報セキュリティ政策会議に対して、国の安全に関する重要な情報を扱う契約にセ キュリティ条項を定めることなどを内容とする報告が行われた。

イ 「情報セキュリティ 2012」の決定

このように、我が国においても、防衛産業を狙った国家安全保障にも直接かかわる深刻な標的型攻撃が発生じた 事態も踏まえつつ、①国や国の安全に関する重要な情報を扱う企業等に対する高度な脅威への対応強化、②スマー トフォン等の本格的な普及に伴うリスクの表面化に対応する安全・安心な利用環境の整備、③国際連携の強化を基 本方針とする 2012 年度(平成 24 年度)の年度計画「情報セキュリティ 2012」が平成 24 年 7 月に決定された ところである。

図表 2-1-3-7 「情報セキュリティ 2012」の骨子について

1. 最近の環境変化

- ○本格的なサイバー攻撃の発生と深刻化
 - 我が国の政府機関における標的型攻撃の顕在化
 - 更なる進化が見込まれる標的型攻撃
- ○社会経済活動の情報通信技術への依存度の更なる高まり とリスクの表面化
 - スマートフォン等の本格的な普及とマルウェア等による脅威 の拡大
 - 制御システム等に対するリスクの高まり

○新たな技術革新に伴う新たなリスクの出現

- M2M(Machine To Machine)環境の出現
- ○重大な情報通信システム障害のリスク回避に向けた取組 の必要性の高まり
 - 東日本大震災における電力の喪失や建物の損壊等
 - 携帯電話事業者等におけるシステム障害の発生

- ○諸外国における取組の強化
- 諸外国における情報セキュリティに対する戦略的な取組の強化
- サイバー空間における国際的規範作りに関する議論の進展

2. 基本方針

「国民を守る情報セキュリティ戦略」(2010年度〜2013年度の4か年計画)で示された基本的考え方、及び、最近の環境 変化と関連施策の実施状況を踏まえた以下の視点の下、施策を重点化して取りまとめる。

簭

- ○国や国の安全に関する重要な情報を扱う企業等に対する高度な脅威への対応強化
- ○スマートフォンの本格的な普及等新たな情報通信技術の広まりに伴うリスクの表面化に対応した安全・安心な利用環境の整備
- ○国際連携の強化

3. 主な施策

- (1) 標的型攻撃に対する官民連携の強化等
- (2) 大規模サイバー攻撃事態に対する対処態勢の整備等 (7) 情報セキュリティ人材の育成
- (3) 政府機関等の基盤強化
- (4) 重要インフラの基盤強化
- (5) 情報通信技術の高度化・多様化への対応
- (6) 研究開発、産業振興の推進
- (8)情報セキュリティリテラシーの向上等
- (9) 制度整備
- (10) 国際連携の強化

情報セキュリティ政策会議資料により作成

(4) 総務省における取組

総務省では、情報セキュリティ対策について、内閣官房情報セキュリティセンターをはじめとした関係府省及び 民間事業者等との連携の下、以下の取組を実施している。

ア テレコムアイザック官民協議会の設置

サイバー攻撃への対処には、官民が協調して取り組むことが重要であることから、総務省、独立行政法人情報通 信研究機構(NICT)及び財団法人日本データ通信協会テレコムアイザック推進会議は、情報共有や技術的な課題 解決等を目的に「テレコムアイザック官民協議会」を設置したところである。

本協議会において、サイバー攻撃に関する情報共有や対応策の強化に向けた議論をするとともに、所管の電気通 信及び放送分野の事業者や地方公共団体等との連携の充実に努めている。具体的には、平成23年10月に開催し

た「サイバー攻撃対処に向けた官民会合」において、総務大臣から、官民の実務担当者による「テレコムアイザック官民協議会」の立ち上げ等を要請し、設置された同協議会において、サイバー攻撃に関する情報共有や対応策の 強化に向けた議論が行われているところである。

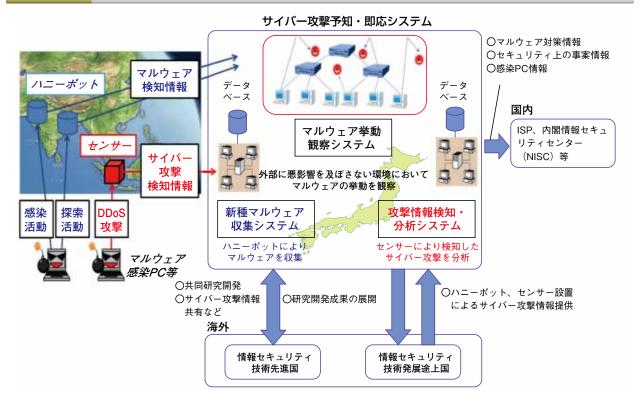
イ サイバー攻撃への対応を強化するための研究開発の推進

我が国におけるサイバー攻撃(DDoS 攻撃等、マルウェアの感染活動)に対処し、そのリスクを軽減するため、総務省では、国内外のインターネットサービスプロバイダ、大学等との協力によりサイバー攻撃に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術の研究開発及び実証実験を実施しているところである。

米国とは、2011 年度(平成23年度)のインターネットエコノミーに関する日米政策協力対話において、サイバー攻撃に関するデータの共有及び研究開発の分野での協力関係を加速化していくことで一致したことを踏まえ、具体的な議論を開始したところである。その他、EU、ASEAN 諸国等とも連携を強化すべく、交渉を進めている。

また、標的型サイバー攻撃に対する技術的な対応として、NICT において、マルウェアに感染したコンピュータからの情報流出に対処する技術の研究開発を実施している。

図表 2-1-3-8 サイバー攻撃への対応を強化するための研究開発・イメージ図



総務省におけるウイルス感染事案の発生

総務省においても、平成 23 年 11 月にウイルス感染事案が発生した。11 月 4 日に、職員用パソコン 23 台が、「トロイの木馬」の新種ウイルスに感染していることが判明した。感染経路は、メールに添付されて いたファイルを開封したことによるものであり、「平成 23 年(2011 年)東北地方太平洋沖地震(東日本 大震災)について(平成23年7月26日17:00):緊急災害対策本部発表資料」という、震災に関連する 内容を騙ったものであった。

また、これら23台のパソコンから、当該感染により、何らかの情報が外部に送信されたことが確認され ている。外部に送信された情報は特定できていないが、業務で関わった方の名刺情報などの個人情報、職 員やその家族の個人情報、業務上の情報が含まれている可能性がある。ただし、このような情報が含まれ ていたとしても、外部に送信された可能性があるのは、その一部であると考えられる。

総務省では、本件事案も受けて、①ウイルス感染防止対策の強化、②ウイルスに感染した場合であっても、 早期に感染を発見できる仕組の整備、③ウイルス感染の拡大を防止する仕組の整備、④外部への情報の流 出を極力食い止める仕組の整備、⑤情報が流出した場合であっても、流出した情報を可能な限り特定でき る仕組の整備といったように、想定される局面ごとに、情報セキュリティの一層の強化に努めている。

4 知識情報基盤として新たな付加価値を創造する ICT とビッグデータの活用

ユビキタスネットワーク環境の完成、とりわけ無線通信技術の進展、クラウドサービスやソーシャルサービスの 定着というネットワーク・サービスレベルでの進化と、スマートフォン等の普及・M2M 通信の進展というデバイ スレベルでの進化があいまって、多様で膨大なデジタルデータがネットワーク上で生成、流通、蓄積されている。 民間調査機関の推計によれば、国際的なデジタルデータの量は、2011年(平成23年)の約2ゼタバイト(2兆 ギガバイト= 2,000 エクサバイト)から、2016 年(平成 28 年)には約 4 倍の約 8 ゼタバイトに拡大すると見込 まれている。また、各国の企業・組織において、革新的なサービスやビジネスモデルを生み出し、的確な経営判断 を行い、あるいは業務の効率化を図るなどの狙いから、このようなビッグデータを活用しようという動きが始まっ ており、例えば、米国ヘルスケアで年間 3,000 億ドル、EU 公共セクターで年間 25,000 億ユーロ、位置情報デー タの活用により年間 6,000 億ドルの消費者価値創出等が推計されている(前出<mark>図表 2-1-1-4</mark>参照。)。このようなビッ グデータによる付加価値創造を成長にどう生かすかに向けて、米国をはじめとする諸外国も注目し、戦略的取組を 開始している。

(1) ビッグデータとは何か

ビッグデータとは何か。これについては、ビッグデータを「事業に役立つ知見を導出するためのデータ」とし、ビッ グデータビジネスについて、「ビッグデータを用いて社会・経済の問題解決や、業務の付加価値向上を行う、ある いは支援する事業」と目的的に定義している例 16 がある。ビッグデータは、どの程度のデータ規模かという量的 側面だけでなく、どのようなデータから構成されるか、あるいはそのデータがどのように利用されるかという質的 側面において、従来のシステムとは違いがあると考えられる。

まず、その量的側面については(何を「ビッグ」とするか)、「ビッグデータは、典型的なデータベースソフトウェ アが把握し、蓄積し、運用し、分析できる能力を超えたサイズのデータを指す。この定義は、意図的に主観的な定 義であり、ビッグデータとされるためにどの程度大きいデータベースである必要があるかについて流動的な定義に 立脚している。…中略…ビッグデータは、多くの部門において、数十テラバイトから数ペタバイト(a few dozen terabytes to multiple petabytes) の範囲に及ぶだろう。」との見方 「がある。ただし、ビッグデータについては、 後に述べるように、目的面から量的側面を考えるべき点について、留意する必要がある。

次に、その質的側面についてみると、第一に、ビッグデータを構成するデータの出所が多様である点を特徴とし て挙げることができる。現在既に活用が進んでいるウェブサービス分野では、オンラインショッピングサイトやブ

¹⁶ 鈴木良介著「ビッグデータビジネスの時代」(平成 23 年 11 月)p.14 参照。

¹⁷ McKinsey Global Institute "Big data: The next frontier for innovation, competition, and productivity" (平成 23 年 5 月) p.1 参照。

ログサイトにおいて蓄積される購入履歴やエントリー履歴、ウェブ上の配信サイトで提供される音楽や動画等のマ ルチメディアデータ、ソーシャルメディアにおいて参加者が書き込むプロフィールやコメント等のソーシャルメ ディアデータがあるが、今後活用が期待される分野の例では、GPS、IC カードや RFID において検知される、位置、 乗車履歴、温度等のセンサーデータ、CRM(Customer Relationship Management)システムにおいて管理さ れるダイレクトメールのデータや会員カードデータ等カスタマーデータといった様々な分野のデータが想定されて おり、さらに個々のデータのみならず、各データを連携させることでさらなる付加価値の創出も期待されるところ である。

図表 2-1-4-1 ビッグデータを構成する各種データ(例) ソーシャルメディアデータ マルチメディアデータ ウェブサイトデータ ウェブ上の配信サイト等 において提供等される音 ☞ ソーシャルメディアにお いて参加者が書き込むプロ フィール、コメント等 ECサイトやブログ等に おいて蓄積等される購入履 声、動画等 歴、ブログエントリー等 m / # / e ビッグデータ カスタマーデータ センサーデータ ICT(情報通信技術)の進展により生成・ CRMシステムにおいて管 GPS、ICカードやRFID等 収集・蓄積等が可能・容易になる多種多量 において検知等される位置、 理等されるDM等販促デー タ、会員カードデータ等 のデータ(ビッグデータ)を活用すること 乗車履歴、温度、加速度等 により、異変の察知や近未来の予測等を通 じ、利用者個々のニーズに即したサービス 187 の提供、業務運営の効率化や新産業の創出 等が可能。 オフィスデータ ログデータ オペレーションデータ オフィスのパソコン等に ウェブサーバー等におい 販売管理等の業務システム において生成等されるPOS データ、取引明細データ等 おいて作成等されるオフィ て自動的に生成等されるア クセスログ、エラーログ等 ス文書、Eメール等

(出典) 情報通信審議会 ICT 基本戦略ボード「ビッグデータの活用に関するアドホックグループ」資料

質的側面の2点目としては、ビッグデータは、その利用目的からその対象が画定できるものであり、その意味では、 冒頭に掲げた定義例が有用である。ただし、その利用目的から特徴に着目する場合においても、データの利用者(ユー ザー企業等)とそれを支援する者(ベンダー等)両者の観点からは異なっている。

データを利用する者の観点からビッグデータを捉える場合には、「事業に役立つ有用な知見」とは、「個別に、即 時に、多面的な検討を踏まえた付加価値提供を行いたいというユーザー企業等のニーズを満たす知見」ということ ができ、それを導出する観点から求められる特徴としては、「高解像(事象を構成する個々の要素に分解し、把握・ 対応することを可能とするデータ)」、「高頻度(リアルタイムデータ等、取得・生成頻度の時間的な解像度が高いデー タ)」、「多様性(各種センサーからのデータ等、非構造なものも含む多種多様なデータ)」 の 3 点を挙げることがで きる。これらの特徴を満たすために、結果的に「多量」のデータが必要となる。

他方、このようなデータ利用者を支援するサービスの提供者の観点からは、以上の「多量性」に加えて、同サー ビスが対応可能なデータの特徴として、「多源性(複数のデータソースにも対応可能)」、「高速度(ストリーミング 処理が低いレイテンシーで対応可能)」、「多種別(構造化データに加え、非構造化データにも対応可能)」が求めら れることとなる。

このように、ビッグデータの特徴としては、データの利用者やそれを支援する者それぞれにおける観点から異なっ ているが、共通する特徴としては、多量性、多種性、リアルタイム性等が挙げられる。ICT の進展により、この ような特徴を伴った形でデータが生成・収集・蓄積等されることが可能・容易になってきており、異変の察知や近 未来の予測等を通じ、利用者個々のニーズに即したサービスの提供、業務運営の効率化や新産業の創出等が可能と なる点に、ビッグデータの活用の意義があるものと考えられる。

(2) ビッグデータの活用イメージ

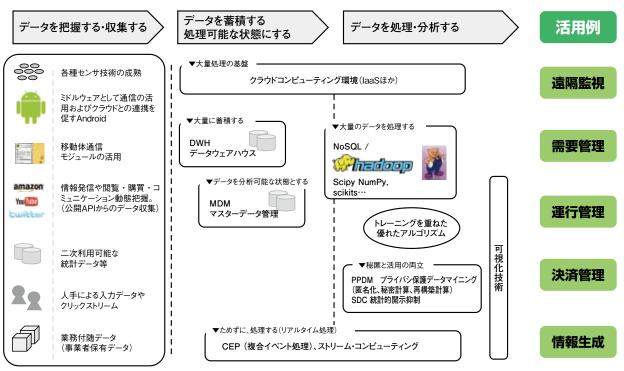
ビッグデータの活用については、現在、検索、電子商取引、ソーシャルメディア等のウェブサービス分野におい て多量に生成・収集等されるデータを各種サービスの提供のために活用することを中心に進展してきている。その 代表例が、グローバルに展開する Amazon、Apple、Facebook、Google など米国のネット系プラットフォーム 事業者である。各社は、利用者の商品・デジタルコンテンツ等の購買履歴や決済情報、コミュニケーションの発信 履歴など膨大なデータを蓄積しており、それらのデータを活用しつつサービス革新等を進めることが、各社の競争 力につながっている側面があると考えられる。

しかし、ビッグデータ活用はそれにとどまるものではなく、データの収集・蓄積・分析に至る技術の高度化 や商用サービス・機器の登場(図表 2-1-4-2 参照)により、多様な付加価値が創造されると考えられる。海 外の民間調査会社が発表したレポート 18 では、ビッグデータによる付加価値創造について、①透明性の創造 (Creating transparency)、②需要の発掘、柔軟性の顕在化、パフォーマンスの増大の実験の可能化(Enabling experimentation to discover needs, expose variability, and improve performance)、③人々のセグメン ト化による動作のカスタマイズ (Segmenting populations to customize actions)、④自動化されたアルゴ リズムによる人間の決断の代替・支援 (Replacing/supporting human decision making with automated algorithms)、⑤新たなビジネスモデル、製品、サービス革新 (Innovating new business models, products, and services) の5類型を提示している。

ビッグデータとして活用されるデータについては、今後は、ウェブサービス分野のデータ・技術のみならず、 M2M 等のセンサーネットワーク等から収集されるデータも含め、多様なデータが想定されている。このような多 種多量のデータを実社会分野において分野横断的に、かつリアルタイムに活用し、交通渋滞、医療の充実や犯罪抑 止といった社会的課題の解決や、電力網など業務基盤・社会インフラの効率的運用といった効果をもたらすことが 期待されている。第1章第5節に示した ICT を活用した街づくりに係る地方公共団体アンケート結果でも示され ているように、地方公共団体においても、地域経営戦略におけるデータ・ICTの活用やいわゆる「スマートシティ」「ス マートタウン」構想に対しては、具体的な取組はこれからの状況にあるもののおおむね必要性は感じており、財政 面の対応や実証実験による具体的効果の提示により飛躍的に進む可能性がある。今や、ビッグデータは、公的部門 を含むあらゆる事業分野において重要性を増大させつつあり、個々の企業レベルにおいても競争力向上や成長の鍵

図表 2-1-4-2 ビッグデータ活用のイメージ

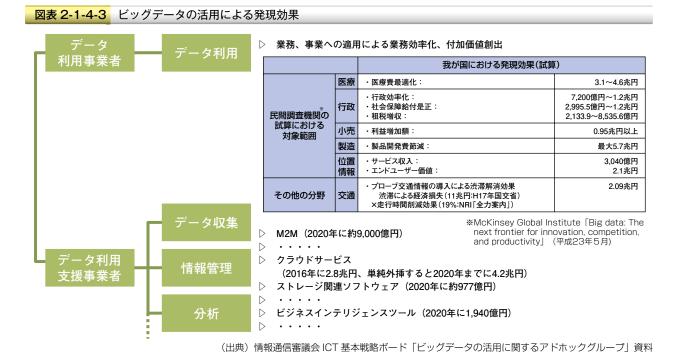
●データの収集・把握技術、大量のデータを分析可能な状態で蓄積する技術、大量のデータを高速で分析する技術などビッグデータ 活用を支える技術や各種サービスが登場し、様々な活用例を生み出している。



(出典) 情報通信審議会 ICT 基本戦略ボード「ビッグデータの活用に関するアドホックグループ」資料

となると同時に、各部門の生産性向上やサービス革新、消費者価値の増大等を通じて、国全体の成長を担う存在となりつつあると考えられる。

また、ビッグデータは、新たな ICT サービスの創造を通じて ICT 産業の成長にもつながることが見込まれる。情報通信審議会 ICT 基本戦略ボード・ビッグデータの活用に関するアドホックグループでは、ビッグデータの社会経済効果について、「ビッグデータの活用に関する市場規模等の計測手法については、国際的に確立されていない状況であるが、諸外国に関する民間調査機関による試算等を前提とした場合の日本における効果として、データの利用事業者及びその支援事業者からなるビッグデータの活用に関する市場においては、今後、少なくとも $10\,$ 兆円規模の付加価値創出及び $12\sim15\,$ 兆円規模の社会的コスト削減の効果があると考えられる。」としている。



(3) ビッグデータの活用事例

ビッグデータの活用は、既に我が国においても一部企業において始まっており、具体的な成果をあげつつある。 ここでは、情報通信審議会基本戦略ボード・ビッグデータの活用に関するアドホックグループのヒアリングで紹介 された具体的事例として、本田技研工業の例等を紹介する。

ア 本田技研工業の例

同社では、ドライバーの快適なカーライフを実現するため、より安全で環境にも配慮したドライブ情報ネットワークとして、安全・安心、防災、天気、省燃費ルート等の情報を提供する「internavi」を 2002 年(平成 14 年) からサービス提供開始し、2012 年(平成 24 年) 5 月現在、会員数は 145 万人に達している。

同サービスでは、2003年(平成 15 年)に、会員から 5 分毎の間隔で収集した装着車の走行データ(Floating Car Data: FCD)の共有により、渋滞を回避し、目的地へより早いルート案内を行う「フローティングカーシステム」を導入している。これにより、主要幹線を対象とする VICS(Vehicle Information & Communication System)を補完し、現在、毎月 1 億 km のデータがアップロードされている。2012年(平成 24 年)5 月末現在、蓄積した走行データは 25 億 km に達している。

本システムによる効果としては、例えば以下の効果が挙げられる(いずれも同社からの提供情報)。

- ① VICS と FCD を融合した渋滞予測による効果検証結果(東名阪 100 サンプルのシミュレーション)では、約 20%早いルートが案内され、CO2 換算では約 16%の削減効果があった。
- ②埼玉県の道路行政の取組において、FCD より急ブレーキポイントの多発地点を抽出し、街路樹の剪定や路面表示により、急ブレーキ回数が約7割減少した。
- ③ 2006年(平成18年)のNPO法人防衛推進機構の研究への協力により、2007年(平成19年)の新潟県中

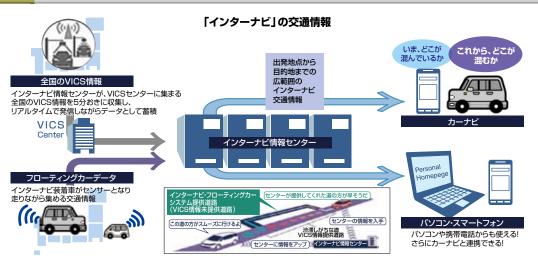
越沖地震、2008年(平成20年)の岩手・宮城内陸地震において、FCDを活用した通行実績マップが生成・ 公開された。また、平成 23 年 3 月の東日本大震災においては、同マップを翌朝公開するとともに、Google や NPO 法人 ITS-Japan をはじめ、各種行政機関や研究機関にも提供し、活用された。

東日本大震災での取組としては、このほか、①津波警報と地震情報や首都圏の通行止め状況のカーナビ画面への 配信、②地震時の位置情報付の家族へのメールによる安否連絡、③国土交通省河川局が設置した 11 か所の浸水セ ンサー観測値のカーナビやスマートフォンへの配信等が実施された。

また、目的地への走行ルート等と財団法人日本気象協会から提供される凍結予測等の気象情報との連携により、 路面凍結発生の予測時刻や予測時点等のカーナビ画面への表示・音声警告等の気象・減災情報を提供している。

加えて、車両内のセンサーから収集している燃料噴射量のデータ活用により、例えば、燃費のよいルートの 探索・予測や車両の制御等が可能となっている。また、アメリカの車種では、車載の CAN (Controller Area Network)による故障データ等の活用により、故障部位のディーラーや顧客への連絡等を実施するまでに至って いる。

図表 2-1-4-4 「インターナビ」の交通情報



情報通信審議会 ICT 基本戦略ボード「ビッグデータの活用に関するアドホックグループ」資料により作成

イ その他の取組事例

情報通信審議会基本戦略ボードで紹介された他の取組事例は図表 2-1-4-5 のとおりである。

図表 2-1-4-5 その他の取組事例

【国内における取組事例】

楽®天

Infoseek 楽@天





- ターゲティング広告について、リアルタイム性を加味した データベースシステムにより、会員の多種多量に及ぶデータ を集約・分析
- ☞ 数千万人の会員の属性、数千万点の商品購入履歴、各種 サービスの利用履歴、会員ランキング、ポイント活用等の データを日次等で分析し、顧客特性等に応じた広告等を配信
- ☞ 会員が2つ以上の他サービスを利用する割合が2007年の 31.4%から2009年6月に38.2%に向上し、また、クリック率 や購買率が数倍に上昇。

カブドットコム証券

- 投資情報について、分散処理ソフト「Hadoop」(ハドゥー プ)を組み込んだシステム等により、ツイッター等のソー シャルメディア上のデータを分析
- ☞ 46者の対象銘柄について、1日当たり約900万行のソー シャルメディア上のデータを収集し約4万3千のキーワード で絞り込み、登場頻度と株価動向の相関関係等を分析
- 今後、対象銘柄の増加や分析精度の向上等の開発により、 新たな投資情報サービスの提供が期待

❷ 国土交通省 関東地方整備局 ◆ 車京都



- ☞ 平成24年2月に開通した「東京港臨海道路 | の東京ゲート ブリッジについて、多数のセンサーにより、橋のひずみや振 動を常時検知し、橋の破損状況をデータとして把握可能
- 橋を通過する車両の重さを算出することにより、過積載を 遠隔監視し、橋への負担や事故につながる車両の走行を防止 することも可能

徳島大学病院 Tokushima University Hospital





- ISF EHR(電子健康記録)について、分散処理ソフト「Hadoop」 やデータ管理ソフト「Cassandra」等を組み込んだシステム により、医療機関等の診療等データを集積し、疾病を管理・
- ☞ 徳島大学病院や保健センター等のデータを同病院内の サーバーに蓄積し、診療所20カ所の検査結果等を集約・分
- 慢性疾患対策の観点から、継続的な健康情報の管理によ り、包括的な疾病予防管理サービスの提供が期待

図表 2-1-4-5 その他の取組事例(つづき)

【海外における取組事例】

SANTA CRUZ



- 窃盗事件について、余震予測システムをベースとした犯罪 予測システムにより、過去8年分及び日々更新される犯罪 データを分析
- □ 同市内を500フィート(約152メートル)四方のエリアに区 切り、最も犯罪が起きる可能性の高い地域トップ10が警察
- ☞ 市民からの呼出が増加する一方で、警察官数が減少する現 状におけるより効果的な人員配置や、窃盗事件に対する抑止 効果が期待

TIOU



- 新生児集中治療について、予測分析システムにより、新生 児に装着されたセンサーから送られてくるバイタル・デー タ(体温、心拍数、血圧値など16種類)をリアルタイムで収 集・分析
- 予め登録された新生児の平均データから成る基準モデル と比較し、心肺停止や院内感染などの罹患リスクの存在を伝
- 看護師による直接診断より6~24時間早く新生児の容 態異常が検知可能となり、また、複数患者の同時観察により 院内感染予測等に寄与

T · · Mobile ·



- ☞ 解約者について、1ペタバイトを超える大規模なデータ分 析システムにより、3,400万人の契約者データを分析
- ☞ 2週間分の分析により、一定の契約者グループの中の1人 が解約し事業者を乗り換えた場合、同じグループの契約者が 一般的な契約者と比較して7倍高い確率で乗り換えている ことが判明
- ☞ 分析結果を踏まえ、解約する前に、契約者に対し、 ピンポ イントで優遇キャンペーン等を打つことが可能となり、経営 が改善

🕵 shopperception



- マイクロソフト社のモーションセンサであるKinectを活 用し、スーパー等の小売分野において、買い物客の行動を分 析
- 陳列棚におけるどの商品に客が手を伸ばす回数が多いの か等について、リアルタイムでセンシングし、ヒートマップ による見える化や最適に商品配置
- ☞ 商品を一旦手に取った後に陳列棚に戻す顧客に対し、デジ タルサイネージ等の活用により、当該商品に関する広告をリ アルタイムに提供

(出典) 情報诵信審議会 ICT 基本戦略ボード資料

(4) ビッグデータの戦略的活用に向けた諸外国の取組

ア 米国

米国では、上記のネット系プラットフォーム事業者や各 ICT ベンダーが既にビッグデータ活用に向けて積極的 な取組を進めており、米国政府においても、科学技術政策局(OSTP)が平成 24 年 3 月 29 日、ビッグデータ研究・ 発展イニシアティブ (Big Data Research and Development Initiative) を発表して、政府として戦略的に取り 組む姿勢を明確にしている。

同イニシアティブは、急速に増大するデジタルデータを活用することを目的として、大量・複雑なデジタルデー 夕から知識と洞察を抽出する能力の強化を図るものであり、同局幹部は「情報技術の研究開発に対する政府のこれ までの投資によって、スーパーコンピューティングとインターネットの創造の飛躍的な進歩につながった。それと 同様に、われわれが今日から始めるこの取組によって、科学的発見、環境・生物医学研究、教育、国家安全保障に 対するビッグデータの活用能力が変化していくことになる。」と声明で述べている。同局は、本イニシアティブが、 米国が直面している最も差し迫った課題の解決に役立つとの見解を示している。

同イニシアティブでは、①巨大な量のデータの収集、保存、運用、分析、共有に必要な中核技術の進歩、②科学 技術分野での発見速度の加速や、国家安全保障の強化、教育・学習の変化への当該技術の活用、③ビッグデータ技 術の発展・活用に必要な労働人口の拡大を目指すとしている。

同イニシアティブでは、国立科学財団 (NSF)、国立衛生研究所 (NIH)、国防総省、エネルギー省、国防高等 研究計画局(DARPA)、地質調査所の6機関が参加する。このうち、DARPA はデータ解析ツール開発プログラ ム (XDATA プログラム) に年間約 2,500 万ドルを 4 年間に渡り投じる。エネルギー省は 2,500 万ドルをかけて 新たな研究機関(SDAV)を設立する。米国政府では、同イニシアティブに対する民間機関の参加を呼びかけている。

イ EU

EU では、2010年(平成22年)5月に策定された「欧州のためのデジタルアジェンダ」において、欧州におけ るデジタル単一市場、ひいては包摂的な知識社会 (inclusive knowledge society) を実現するための必要な施策 としての位置付けの下で、第7次研究枠組計画 (FP7) における ICT プロジェクトとして、3億ユーロ(約330億円) の予算をかけ、2011年(平成23年)から5年計画のFI-PPP(次世代インターネット官民連携)プログラムが 実施されている。

図表 2-1-4-6 アメリカにおけるビッグデータの活用に関する研究開発の動向

アメリカ政府により、ビッグデータ活用に向けて、2億ドル以上の研究開発投資

~"Big Data Research and Development Initiative"を2012年3月29日に公表~

科学技術政策局(OSTP)が本イニシアチブを作成、下記をはじめとする多くの機関がこの取組をサポート。

- 大容量のデジタルデータの収集、保存、蓄積、管理、分析及び共有のためのツールと技術の向上を図る。
- ビッグデータを利用して、理工学の研究の加速、安全保障の強化、教育及び学習の改革の実現を目指す。

国立科学財団(NSF)



- ぼ データサイエンティスト育成のための大学でのプログラム。
- カリフォルニア大学での1,000万ドルのプロジェクト。
- ☞ 「Earth Cube」*プロジェクト支援のための助成金。

(※)地球科学者が地球に関する情報を利用、分析、共有できるシステム

国立衛生研究所(NIH)



☞ 200テラバイトにものぼる1,000のゲノムプロジェクトの データがクラウド上で自由に手に入る。



国防総省 U.S. Dovetnest or D

☞ ビッグデータ新規研究プロジェクトに6,000万ドル投資。

☞ ビッグデータに関するコンペティションを開催。

エネルギー省



☞ 2,500万ドルかけて、「SDAV」(Scalable Data Management, Analysis and Visualization)という新たな研究機関を設立。

国防高等研究計画局(DARPA)



program」を実施し、非構造データを含めたデータ解析 プログラムツールを開発。

地質調査所



☞ 「John Wesley Powell Center」を提供することで、 地球システム科学に関するビッグデータを分析等できる 場を科学者に提供。

政府機関に加え、企業や大学、非営利組織にも、参加を呼びかけ

(出典) 情報通信審議会 ICT 基本戦略ボード資料

FI-PPP プログラムは、インターネット技術との強い統合を通じ、交通、医療又はエネルギー等の公共サービス のインフラと業務プロセスを"smarter" (more intelligent, more efficient, more sustainable) にする大きな 必要性の下、次世代インターネット技術・システムにおける欧州の競争力強化と、公共的・社会的分野において次 世代インターネットで強化されたアプリケーションの出現の支援を目的としている。また、ネットワーク・通信イ ンフラ、端末、ソフトウェア、サービス及びメディア技術に関する研究開発を含む産業主導で全体的な(holistic) アプローチによるとともに、需給を引き寄せ、研究のライフサイクルにおいて早期の段階から利用者を関与させな がら、実利用における実験と検証を促進することとしている。

このプログラムのうち、次世代インターネットの中核となるプラットフォームとしての "FI-WARE" の設計・ 開発・実装に関するプロジェクトが、4.100 万ユーロ(約 45 億円)の予算をかけ、2011 年(平成 23 年)5 月よ り3カ年計画で実施されている。そして、このプラットフォームにおける具体的な機能として、各種サービスを提供・ 管理するためのコンピューティング・蓄積・ネットワーク資源を提供するクラウドホスティングや、膨大なデータ ストリームを効果的に処理・分析等し、価値ある知識に整理する機能などが想定されている。

(5) ビッグデータの積極活用による成長の実現に向けて

上記のように、ビッグデータは、日本再生への GPT (General Purpose Technology) としての ICT の潜 在力を飛躍的に高める可能性を秘めている。震災復興・日本再生にICTがそのけん引力となって貢献していく上で、 ビッグデータの活用により、ユビキタスネットワークをスマート化し、ICT が社会の課題解決力やサービス革新・ 生産性向上など経済成長力をさらに高めることが重要である。

一方、ビッグデータの活用においては、様々な分野で生成される多種多量のデータを横断的に活用し社会全体で 知識や情報の共有が可能となるように、その公開や流通を促進し、かつ分野横断的な連携を図ることや、個人に関 するデータの取扱いをめぐる問題など実社会への適用において生じる制度的課題、技術開発の進展状況等に関する 国際的な動向を踏まえつつ技術的課題の解決に取り組むことが求められている(例えば、米国のネット系プラット フォーム事業者による利用者の行動履歴等各種情報の活用は、主要国においてプライバシー保護との関係で諸問題 を発生させている。)。この他にも、ビッグデータの活用に必要な統計等の知識を備えた人材の不足や、その経済効 果や社会的課題の解決効果の見える化を図り各産業部門や地域、国民利用者にその意義を目に見える形にすること

による理解促進など、ビッグデータを幅広い分野で活用する環境を整備するための課題が存在し、このような課題 に対し国際連携も図りつつ対応することが求められている。

このような観点を踏まえ、ビッグデータを戦略的に推進する必要性としては次のような点が挙げられる。

まず、競争の激化等が進展する国際経済・社会において、我が国は、これまで ICT をはじめとする科学技術力 とともに車の両輪として成長を支えてきた人的資源が世界に先駆けて今後急激に減少・少子高齢化していく状況と なっている。さらに、労働力人口の減少とあいまって、経済成長が低下していく恐れに見舞われており、今後の我 が国の成長のためには、既存資源の高度な活用や新たな資源の活用が早急に必要な状況となっている。

他方、我が国においては、東日本震災を契機として情報及びそれを支える ICT が命を守るライフラインである ことが再認識され、また、ICT の進展により多様なデータ資源が爆発的に生成・蓄積等されてきている。

したがって、以上のような状況において、ものづくりをはじめとする我が国の強みを生かしつつ国際競争力を強 化し、更なる成長を実現するためには、ビッグデータを戦略的な資源と位置付け、国として実社会分野におけるビッ グデータの利活用を積極的に推進することが重要である。

具体的には、既に第1章のトピックで「オープンデータの活用に向けた期待」を紹介したが、多様な分野におい て閉じた形で保有されているデータについて、オープンガバメントの推進等、官民におけるオープンデータ化、横 断的活用のための環境整備の在り方について検討を進めることが求められよう。また、ものづくりに世界的な強み を有している我が国において、個人情報等にも配慮しつつ、M2M 等のセンサーネットワーク等を通じて生成・収 集等される多種多量のデータについて、社会全体で共有可能な知識や情報の創発が促進されるよう蓄積・公開・流 通・連携等させることを通じ、分野横断的かつリアルタイムに解析等利活用して、社会的課題の解決や経済の活性 化を実現することも重要である。さらに、認証、秘匿化や制御等に関する技術のさらなる発展等により、安心・安 全なビッグデータの利活用が進展していくことが期待される。

以上を踏まえると、「課題先進国」である我が国において、ビッグデータを利活用することで付加価値を生み出し、 ICT の成長けん引力、ツールとしての機能を強化し、様々な課題解決につなげ、新たな価値創造が可能な環境を 実現することが求められているといえよう 19。

図表 2-1-4-7 ビッグデータの活用を推進するための基本的な方向性(ICT 政策として取り組むべき課題)

- 多様な分野において閉じた形で保有されているデータについて、オープンガバメントの推進等官民におけるオープンデ ータ化、街づくりや防災等への活用等横断的活用のための環境整備の在り方
- ② リアルタイムで活用するビッグデータについて、センサ等から生成されるデータを安心・安全に収集・解析・流通等す るための基盤技術の研究開発・標準化の在り方
- ❸ 技術やビジネス等の様々な分野における知識や能力等を備えたビッグデータの活用に関する人材について、産学官のプロ ジェクトを通じた育成等による確保の在り方
- ビッグデータビジネスの創出に寄与するM2M(人が介在せず、ネットワークに繋がれた機器同士が相互に情報交換等 を行う機器間通信) の普及促進の在り方
- 正確性の確保等のために多様な用途への転用が制限されているデータや既存制度の保護対象とならないため整備が進ま ないデータ等について、その活用を阻む規制・制度の在り方
- 様々な業種の民間事業者、研究機関、学識経験者、行政機関等から広く構成され、データ資源の蓄積等を通じて、ビッ グデータの活用について国内の普及・展開を図るための推進体制の在り方
- 動際的な取組事例等の共有等を図るための外国政府等との意見交換の在り方や、ビッグデータの活用による経済価値の 見える化等のための計測手法の在り方

(出典) 情報通信審議会 ICT 基本戦略ボード資料

¹⁹ 情報通信審議会において検討されている「Active ICT JAPAN の実現に向けた ICT 総合戦略(案)」においては、ビッグデータ利活用による社会・ 経済成長が重点領域の一つとして位置づけられ、その実現のための戦略としてアクティブデータ戦略が盛り込まれている(第5章第1節2参照)。