2014 年度卒業論文

山田正雄ゼミナール

デジタルデバイドの現状と問題点

～これからもデジタルデバイドは存在していくか～

日本大学法学部　公共政策学科　4 年

学籍番号　1150170

吉田　駿介

2014 年度　山田正雄ゼミナール　卒業論文
デジタルデバイドの過去と現状
13 期　1150170　吉田　駿介

はじめに

私たちの生活には、様々な情報であふれている。しかし、洪水のような大量の情報の全てが有益なものとはいえない。有利的なものもあれば、信用できないものもある。高度情報化社会に生きている私たちは、情報を主体的に正しく見分け、適切に判断し、利用する能力を身につけることを必要とする。また、進展する高度情報化社会のなかで社会や技術などの急激な変化に積極的に対応しながら生きていく必要がある。そのためには、情報技術革命の動向や生活との関わりについて深く考えてみることも大切である。

社会的に大量の情報が生み出され、それを加工、処理、操作するための機構が巨大化し、人々の意思決定や行動に大きな影響を与えるに至った社会は、情報化社会と言う。情報社会は、現代人に様々な利益をもたらした。情報社会のおかげで、個人的に一人ひとりが便利で多機能の通信手段を持つようになった。そしていつでも、どこでも、送信と受信ができる。携帯電話、そしてインターネットを通じて、私たちは様々な情報を手に入れることができる。家に居ながらにしても、インターネット上で買い物をすることができる。最近、在宅ワークをしている人も増えてきたようだ。要するに、社会の情報化によって、私たちの生活は以前よりもはるかに便利で、快適になったのである。

現代社会において情報化は確かに不可欠なものだが、日本やアメリカのような高度情報社会において幾つかの問題点がある。その問題点の一つは、デジタルデバイドである情報格差による社会的、経済的弱者の増加ということだ。情報格差は、情報通信機器の利用技術において使い慣れている者と使えない者の格差の問題ということを指している。情報格差は、所得や地域、人種、学歴、性別、年齢などにならぶ新たな差別の原因にもなっている。その問題を解決するには、まずみんなに情報通信手段を身につけさせることが必要であると思う。そのため、情報機器に慣れていない上の世代、あるいは下層階級にある者に新機器の使い道を教えるべきだと思う。私はそのデジタルデバイドの問題を整理・分類し、その対策を考えてみたい。

目次

第1章　デジタルデバイド

1-1 デジタルデバイドとは

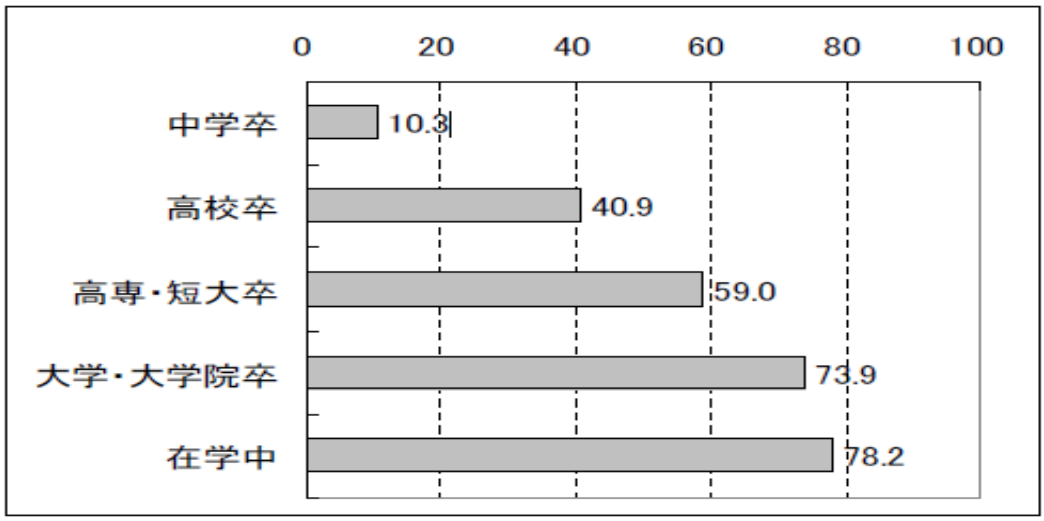
パソコンやインターネットなどの情報技術(IT)を使いこなせる者と使いこなせない者の間に生じる、待遇や貧富、機会の格差。個人間の格差の他に、国家間、地域間の格差を指す。若者や高学歴者、高所得者などが情報技術を活用してますます高収入や雇用を手にする一方、コンピュータを使いこなせない高齢者や貧困のため情報機器を入手できない人々は、より一層困難な状況に追い込まれる。いわば、情報技術が社会的な格差を拡大、固定化する現象がデジタルデバイドである。「デバイド」の直訳に「格差」という意味はなく、「分ける」「一線を画す」とかの意味である。[1]

[1] 米国では 1990 年代中盤から論議されはじめ、1999 年 7 月の商務省報告書「Falling Through the Net: Defining the Digital Divide」では年収 7 万 5000 ドル以上の世帯は、最低所得層の世帯に比べインターネットにアクセスできる比率が 20 倍以上、パソコン所有率も 9 割以上、また最高度の教育を受けた層と最低度の教育を受けた層のアクセス格差は 1 年間で 25%上昇として指摘された。また、クリントン政権は 2000 年 1 月の一般教書演説で、社会的弱者の就業機会が狭まっている問題を解決するため、学校、図書館、新設の全米 1000 ヶ所のテクノロジーセンター等でインターネットの利用機会を提供することと、教員の再訓練実施を提唱した。2000 年 10 月の報告書「Falling Through the Net: Toward Digital Inclusion」においては、インターネット世帯普及率が 58%を超えた普及の現状、格差社会、そして、家庭からアクセスできない人に公共施設のアクセスポイントが貢献していることを指摘しているが、体が不自由な人や人種などにおいて依然として格差が存在とすると同時に、ブロードバンドアクセスが新たな格差を生んでいることを示している。

1-2　デジタルデバイドの規定要因

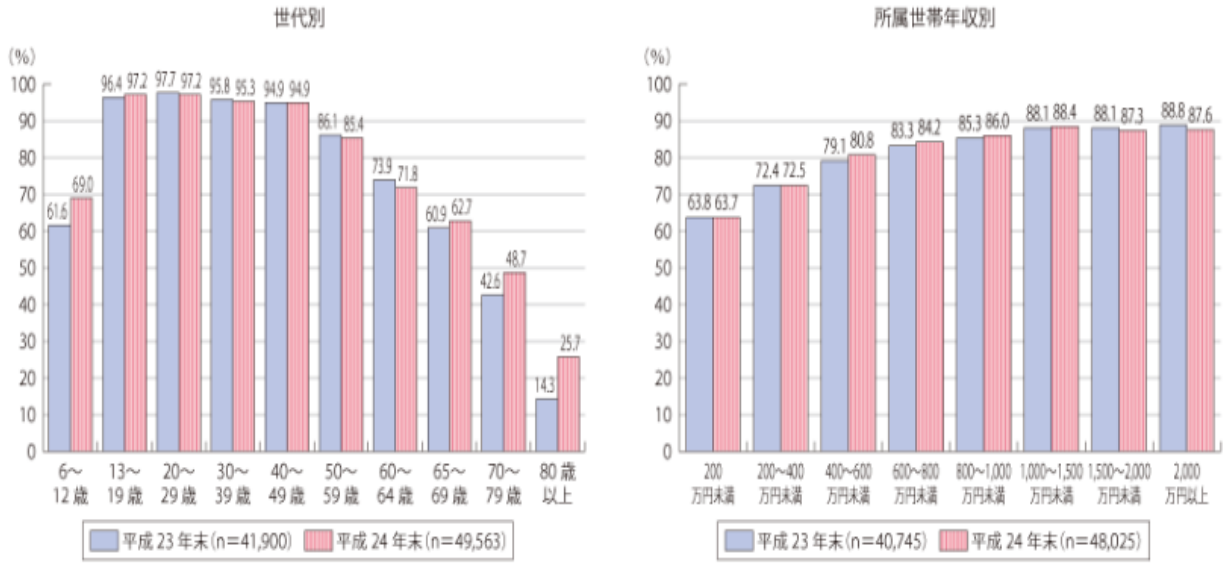
インターネットの間で格差が生じる要因として年齢・学歴・スキル・収入などが関係している。

図表 1：学歴別にみたインターネット利用率



学歴別にみたインターネット利用率がもっとも高いのは、中学校から大学院までのいずれかに在学している人で、利用率は 78%にも達している。既卒者を学歴別に比較してみると、大学・大学院卒業者の利用率がもっとも高く、学歴が低くなるにしたがって、インターネット利用率も低下する傾向がはっきりとみられる。とくに、中学卒ではわずか 10%となっており、学歴間の利用格差が著しくみられる。

図表 2：世代別にみたインターネット利用率



世代別にみたインターネット利用率では 13 歳～49 歳までは 9 割を超えているのに対し、

60 歳以上は大きく下落している。また、所属世帯年収別の利用率は、400 万円以上で 8 割を超えており、所属世帯年収の低い区分との利用格差が存在している。
平成 22 年末においては、インターネットの利用／未利用に最も大きな影響を及ぼしている要因は、年齢である。特に「60 歳以上」の属性であり、高齢になるほど、インターネットを利用していない傾向にある。また、次に大きな影響を及ぼしているのは年収である。特に、「世帯年収が 200 万円未満」となっており、所得が低いほどインターネットを利用していない傾向にある。

1-3　ネットワークインフラの「量」と「質」

ネットワークインフラの「量」とは、その時期のネットワークの技術体系が実現している料金問題も含んだネットワークの性能である。現在、日本でのインターネットはダイヤルアップでの接続が中心であり、そこで主として使用されているサービス・アプリケーションは、文字中心の電子メールと静止画中心の Web である。これらの登場は、人と人とのコミュニケーションのあり方を変え、ビジネスのやり方も変えた。

ネットワークの「質」とはコンテンツの内容やその形態の事を指す。最近では一部 Web が動画化したり、音楽配信が行われるようになったりと色々なサービスが登場している。

一方、途上国においては、いまだ多くの国民に固定電話さえ普及していないところは多く、帰って今後は、固定電話より安価にまた広範囲にネットワークのカバーができる、携帯電話や、他のネットワークが急速に普及していくかもしれない。

第 2 章　デジタルデバイドがもたらす問題

2-1　個人の「場」でのデジタルデバイド

ネットワークの質と量が高く、個人のインターネット活用能力が高ければ、経済・便益的成果を得る機会は拡大する。

インターネット上には、オークションや株、コミュニティの参加による情報交換などの様々なサービスが存在するがこれらのサービスを上手く活用することで消費の節約や、雇用機会など様々な経済的メリットを得ることができる。インターネット上で買い物をする際に、店舗で買うよりも安い値段で商品を提供する企業が増えてきている。そのために、インターネットを使える人と使えない人との間では経済的デメリットが生じるケースがある。就職活動においても最近では、インターネット上で企業の説明会の予約やエントリーシートの提出を求める企業があり、インターネットを利用していない人はその企業を受けられない場合もある。

個人の教育格差でいえば、海外の小中学校でパソコンやインターネットがなければ宿題ができない場合がある。家にパソコンやインターネットが使える子供は、よりよいレポー

トを作成するのに情報検索を行い、調べものを簡単に行うことができる。しかし、そうでない子供は調べる方法がないので、受けられる教育の水準に格差が生まれ、それが学力格差になる。パソコンを持ちインターネットが利用できるか出来ないかが子供の教育や成績に大きく影響する。

個人のセキュリティ格差では、セキュリティ対策をしていない人は不正アクセスやウイルス被害に合う場合が多い。インターネットを利用するだけではなく、ウイルス被害に合わないための知識も身につけ安全にインターネットを利用していかなければならない。

図表 3：デジタルデバイドがもたらす問題（個人）

問題の分類 発生の場	経済･便益格差	文化･教育格差	軍事セキュリティ格差
個人	所得格差 雇用機会格差 サービス授受格差	学歴格差 就学率格差 教育水準格差	ネットワーク犯罪被害 プライバシー問題

2-2　コミュニティの「場」でのデジタルデバイド

社会には、国や地域によって人種・民族・世代・性別・障碍者・などのコミュニティが存在している。インターネットの浸透はこのコミュニティに新たな格差を生じさせるとともに、既存の格差を拡大、強化している。

たとえば、アメリカでは人種ごとに地域的なコミュニティを形成している場合が多く、そこでの既存の経済格差がネットワークの量と質やその集団の情報活用能力をも規定し、さらにその違いが、個人の「場」でみられたような経済格差や教育格差をさらに拡大する傾向がある。

また、障碍者のコミュニティを考える場合、キーボードが使いにくかったり、画面の文字が見えにくかったり障碍に応じた適切なソフトがなかったりして、IT 革命に取り残されていく場合がある。障碍者の情報活用能力は端末の形状、その使用方法、機能等が使いやすくないため障碍者の力が発揮できず格差が生まれる。こうした問題を解決できれば、障碍者や高齢者などの方にも情報の入手手段、職域の開拓など今よりできる事が増えていくと思う。

図表 4：デジタルデバイドがもたらす問題（コミュニティ）

問題の分類 発生の場	経済･便益格差	文化･教育格差	軍事セキュリティ格差
社会的集団	所得格差 雇用機会格差 サービス授受格差	教育水準格差 就学率格差 固有文化の喪失	ネットワーク犯罪被害

2-3　企業・組織の「場」でのデジタルデバイド

現代の企業間競争においてインターネットを中心とした技術体系を活用する程度の違いは、競争力を規定する決定的要素ともいえる。IT 革命は、これまでになかった電子商取引を生み出し、インターネットの世界的結合がもたらした市場のグローバル化は、市場のあり方を大きく変え、インターネットにまつわるさまざまな新しい産業やサービスを生み出す一方、これまでの仕事の進め方や経営管理の方法に至るまで大きく変えている。経営管理面では、CRM（カスタマー・リレーションシップ・マネージメント)、SCM（サプライ・チェーン・マネージメント)、ナレッジマネージメントといった情報化と一体となった手法が登場し、その導入が企業間格差をもたらすことになる。ここでの格差は、経済格差が中心ではあるが、企業間における教育や開発においても、情報化の進展度合いで格差が生じ、またセキュリティの面でも大企業と中小企業との間には大きな格差が存在する。大企業は資金力によって情報化投資を積極的に行えるが、中小企業はその力がなく情報化が進まない面がある。

しかし、大企業は大きさや伝統が足枷となり、情報化時代の急速な変化に対応できない面を持つが、中小企業ではいち早く情報ネットワークを導入し、目覚ましい実績をあげている企業が数多く見られる。

図表 5：デジタルデバイドがもたらす問題（企業・組織）

問題の分類 発生の場	経済･便益格差	文化･教育格差	軍事セキュリティ格差
企業･組織	収益率の差 作業効率の差	社会貢献格差 広報力格差	ネットワーク犯罪被害

2-4　地域の「場」でのデジタルデバイド

日本では､インターネットが普及しはじめた1990年頃からインターネットを利用すれば､いつでも誰でも情報を入手することができ、地方の情報格差は解消され地域間格差がなくなると思っていたが、実際は地域間格差がなくなるどころか、東京への情報の一極集中がさらに進んで格差が拡大しているように思える。

情報化の長所は場所にとらわれず、都市でも地方でも過疎地でも同様に情報サービスを受けられるといったものだが、実際には民間の採算性等に委ねられ、回線の整備状況。人口密度等によって、通信サービスの利用環境や料金などに関して地域格差が伴ってしまう。

一方、インターネットの普及は、自治体と地域住民の関係に大きな変化をもたらし、行政サービス分野では時間と距離の制約を超え新しいサービスが模索されている。また、新しい価値観や多様化する住民ニーズへの対応が求められ、日本では少子・高齢化、地域の活性分野で地域情報化に大きな期待が寄せられている。

また、地方と都市のデジタルデバイドは、先進国でも発展途上国でも存在する。韓国やイタリアでもデジタルデバイドの中心的な課題の 1 つは都市と農村であった。

図表 6：都道府県別のインターネット利用率

都道府県 (n)		利用率 (%)	端末別利用率			
			自宅のパソコン	自宅以外のパソコン	携帯電話（PHS、携帯情報端末（PDA）なども含む）	スマートフォン
北海道	(1,434)	77.5	55.3	33.2	44.9	25.0
青森県	(855)	70.6	43.4	26.6	41.8	22.0
岩手県	(1,128)	68.9	38.4	24.2	38.4	22.0
宮城県	(1,080)	75.9	52.4	34.4	41.6	27.7
秋田県	(1,438)	70.4	47.0	32.1	35.9	21.8
山形県	(1,392)	71.9	50.7	32.0	39.1	24.0
福島県	(875)	70.2	46.2	26.7	37.7	25.8
茨城県	(1,140)	73.4	53.5	29.9	40.1	30.0
栃木県	(1,023)	76.1	54.5	31.3	42.9	27.3
群馬県	(954)	78.5	58.5	31.3	44.3	31.2
埼玉県	(1,184)	80.0	63.2	32.7	45.4	34.8
千葉県	(951)	81.0	63.0	31.0	45.7	31.9
東京都	(804)	87.3	67.6	44.5	50.7	37.8
神奈川県	(877)	87.0	70.7	38.8	47.8	38.5
新潟県	(1,125)	74.4	51.6	29.7	39.6	23.4
富山県	(1,321)	76.8	58.4	32.6	42.4	24.8
石川県	(1,248)	79.0	61.8	38.2	42.8	29.1
福井県	(1,280)	77.5	59.7	34.8	41.5	30.0
山梨県	(991)	77.4	56.9	32.5	42.4	29.6
長野県	(1,428)	75.3	56.2	33.0	43.3	25.4
岐阜県	(1,364)	75.4	56.8	32.6	37.8	30.7
静岡県	(1,301)	74.5	55.7	30.4	38.2	31.5
愛知県	(1,067)	80.5	60.0	34.1	39.3	30.3
三重県	(1,201)	78.4	56.8	32.2	40.4	28.3
滋賀県	(1,242)	81.7	63.0	33.0	43.2	34.3
京都府	(961)	78.6	61.3	32.6	43.2	32.2
大阪府	(884)	82.1	64.5	32.2	40.7	36.7
兵庫県	(1,052)	79.9	63.3	37.9	43.5	32.4
奈良県	(1,009)	80.2	62.2	32.2	41.3	34.4
和歌山県	(974)	74.6	58.2	29.6	34.1	23.9
鳥取県	(1,106)	73.9	51.3	34.6	37.5	25.5
島根県	(995)	68.8	46.2	31.6	39.0	25.0
岡山県	(1,063)	80.0	57.8	33.4	44.7	29.7
広島県	(1,239)	81.1	62.0	37.4	43.4	30.0
山口県	(969)	75.4	55.1	31.5	35.9	28.4
徳島県	(894)	74.0	51.9	32.0	43.9	25.7
香川県	(981)	78.5	57.6	35.8	39.0	29.5
愛媛県	(928)	76.1	52.0	31.7	39.8	24.6
高知県	(831)	76.8	53.5	35.4	37.9	22.0
福岡県	(813)	80.7	58.5	32.5	41.0	34.3
佐賀県	(946)	77.0	52.8	30.1	38.7	28.5
長崎県	(875)	72.6	48.1	29.2	36.9	25.5
熊本県	(977)	75.9	51.2	30.9	37.3	27.8
大分県	(920)	77.6	51.7	29.4	39.5	29.5
宮崎県	(888)	74.5	52.7	29.4	36.7	27.8
鹿児島県	(875)	74.2	43.7	26.0	35.4	25.8
沖縄県	(680)	76.7	52.2	35.0	40.8	26.0
全体	(49,563)	79.5	59.5	34.1	42.8	31.4

2-5　国家の「場」でのデジタルデバイド

国家の「場」でのデジタルデバイドの特徴は、冷戦崩壊後の世界構造を反映し、米国をその頂点として新しい序列が形成された。冷戦構造の崩壊は、それまでの米ソ両大国による世界体制、すなわち経済的には資本主義経済体制と社会主義経済体制の世界二極体制を、基本的に資本主義世界経済体制へと移行させ、市場主義と自由貿易を原則とする経済的なグローバリゼーションをもたらし、資本と商品の国境を超える移動を世界中で可能とした。これと同じくして、インターネットの世界普及は文化面でも英語と米国文化を主流とするグローバリゼーションを進めていった。政治経済体制・言語（英語以外の言語圏）からくるデジタル機器・インターネットの利用率の違いもある。

第 3 章　アジアの諸国間のデジタルデバイド

3-1　アジアにおける情報化の現状

1998 年にわずか 8 ヶ国だったインターネット接続数は 2000 年には 214 ヶ国にまでになり年々増えていっている。政策的にインターネットを拒否している国以外は、インターネットが可能になった。ただし、ワールド・ワイド・ウェブ（WWW）を含めたフル・アクセスというわけではなく、電子メールのみのアクセスという場合もある。インターネット利用者数は 1995 年には世界で 3400 万人だったが 2000 年には 3 億 1500 万人となり、途上国でも確実に利用者数が増えている。

アジア諸国の中で「ネットタイガー」と呼ばれているのは、シンガポール・台湾・香港・韓国である。この 4 ヶ国はいち早く情報化への取り組みを進め、インターネットや携帯電話の普及率でも高い数字を示している。シンガポールの取り組みは 1993 年のクリントン政権成立以前から行われており、領域の狭さもあって先進的なネットワーク構築を進めている。

3-2　バングラディッシュの現状

バングラディッシュでは携帯電話事業者、NGO、政府機関がバングラデシュの地方在住者に ICT の普及に向けた取り組みを進めており、今や地方在住者も世界と簡単につながり、情報や通信を共有できる時代になっている。

先進国は最新の ICT から大きな恩恵を受けているが、先進国と途上国の間にはデジタルデバイドが存在している。国際電気通信連合（ITU）が発表したデータによれば、バングラデシュの 2010 年の ICT 開発指数（IDI）は世界 137 位、2010 年の IDI 指数は 1.42 であった。このように、バングラディッシュの ICT 普及度は非常に低い。バングラデシュは、総人口の約 70%近くが農村に居住し、主として農業に依存しているため、ほとんどがその日暮らしに近い。

バングラディッシュでデジタルデバイドが起きる要因として以下があげられる。

・英語を読める人が少ない
・生活が貧しくサービスを受ける経済的余裕がない。
・道路や電気などの設備が十分に整っていない。

政府は、ICT の潜在的可能性を認識し、国内における普及の加速と貧困の削減に取り組んでいる。政府は、2009 年に人材開発、ガバナンス、E コマース、バンキング、医療、災害管理、公益サービス、各種オンラインサービスに利用される ICT インフラ構築に重点を置く国家 ICT 政策を承認し、ICT 政策の策定・実施を担当する科学情報通信技術省（MOSICT）の下に Bangladesh Computer Council（BCC）を置いた。

図表 7：バングラディッシュの ICT 普及状況

情報通信技術の普及状況	
年	順位
2012年	113位
2011年	115位
2010年	118位

指標	順位
インターネットを使用する個人の比率	130位
携帯電話契約者数	127位
パソコンを備えている世帯の比率	127位
家庭でインターネットにアクセスできる世帯の比率	119位
教育制度の質	85位
数学・科学教育の質	106位
デジタルコンテンツへのアクセス	112位
インターネットユーザー1人当たりの国際インターネット回線速度（kb/s）	110位

3-3　電話の普及

バングラディッシュの情報化の成功例として挙げられるのが携帯電話である。バングラディッシュではすでに6社の携帯電話会社がサービスを展開している。2012年6月末現在、契約者数は約 9,379 万人に達し、会社別では、グラミン・フォンが最も多い。

図表 8：バングラディッシュの携帯電話契約者数

携帯電話の契約者数（単位：100万人）		
事業者名	契約者数（2012年）	契約者数（2011年）
Grameen Phone Ltd. (GP)	39.293	36.493
Orascom Telecom Bangladesh Limited (Banglalink)	25.490	23.753
Robi Axiata Limited (Robi)	19.211	16.139
Airtel Bangladesh Limited (Airtel)	6.734	6.026
Pacific Bangladesh Telecom Limited (Citycell)	1.699	1.824
Teletalk Bangladesh Ltd. (Teletalk)	1.358	1.218
合計	**93.788**	**84.455**

バングラディッシュの携帯電話利用者数 9379 万人を人口の 1 億 5000 万人で割ると 60.2%になる。人口の半分以上が携帯を利用している。ただし、携帯電話を 1 台で複数で共有している場合もあるので、実際の利用者数はもう少し多い。

下の表を見てみると、ICT 機器の導入が地方部で広まり、2005 年に携帯電話を利用していた世帯全国で 11.29%だったが、現在は 63.74%まで増加していることがわかる。しかし、地方部における ICT 機器の利用は都市部に比べて遅れている。

図表 9：バングラディッシュで使われている ICT 機器の普及率

設備の種類	全国(単位:%)		地方部(単位:%)		都市部(単位:%)	
	2010年	2005年	2010年	2005年	2010年	2005年
電話	2.07	2.87	0.70	0.33	5.79	10.36
携帯電話	63.74	11.29	56.77	6.05	82.74	26.73
コンピュータ	3.01	1.36	0.97	0.17	8.58	4.88
電子メール	1.39	0.20	0.39	-	4.10	0.81

・貧困層の人々は、役に立つアプリケーションが組み込まれた携帯電話機を購入する余裕がない。
・携帯電話にはユーザーにとって役に立つアプリケーションがあるが、人々はそれらのアプリケーションの存在を知らない。
・貧困層の人々は、様々なアプリケーションのサービスをどのように利用すればよいのか分からない。
このような理由から地方部と都市部でのデジタルデバイドが生じる。

3-4　グラミン・フォン

バングラディッシュのグラミン・フォンの事例について取り上げる。バングラディッシュは、現在でも世界最貧国の一つで、一人当たり GDP は約 400 ドルという経済規模である。人口は 1.4 億人だが、その 70%以上が農村部に居住しており、さらには国土の 80%に電気が開通していないというインフラ環境である。このような最貧国において、1997 年にイクバル・カディーアにより創業されたのが、「グラミン・フォン」である。[2]同国の当時の電話普及率は、人口ベースで 1%以下であり、様々な面でビジネスの発展が著しく阻害されていた。こうした情勢の中、グラミン・フォンは「つながること＝生産性 」というカディーア氏の信念の下で立ち上げられ、町や村の一角や店頭で携帯電話を分単位で貸し出すサービスの提供を始めた。

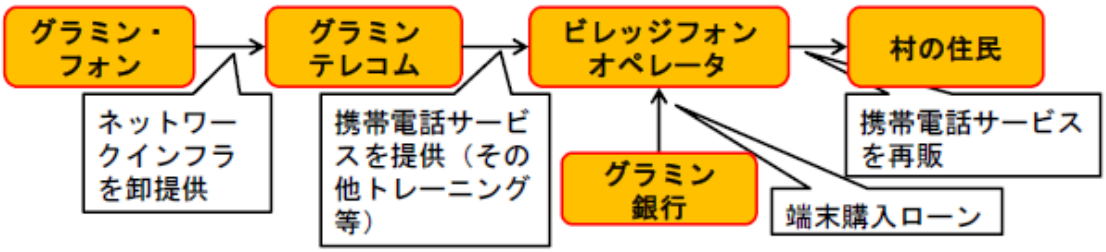
グラミン・フォンの事業は、グラミン銀行とグラミンテレコムとの関係性が重要な役割を果たしている。グラミン銀行はムハマド・ユヌス氏が 1983 年に創設したマイクロファイ

[2] ノルウェーの通信電話会社テレノール社と、米国投資家、日本の丸紅が投資した。現在の主要株主はテレノール及びグラミンテレコムである。

ナンス機関であり、マイクロクレジットと呼ばれる貧困層を対象にした低金利の無担保融資を行うことで、主に農村部の人々の自立と生活の質の向上を支援している。さらには、銀行を主体として、インフラ・通信・エネルギーなど、多分野で「グラミン・ファミリー」と呼ばれる事業を展開している。一方、グラミンテレコムは、貧困層への通信サービスを提供するために 1995 年に設立され、グラミン・フォンへ出資している非営利企業である。グラミンテレコムは、グラミン・フォンから通話時間を大口で購入し、グラミン銀行のマイクロファイナンスで電話機を購入した農村部女性（「ヴィレッジフォンレディ」などと呼ばれる）に再販し、彼女たちがさらにエンドユーザである村の住民に小売りした。女性たちは、グラミン・フォンに加入するために 12,000 タカ（約 200 米ドル）のローンをグラミン銀行から受け、加えてサービスの再販のためのトレーニングを受ける。ヴィレッジフォンレディは村の住民に携帯電話を使ってもらいその使用料金による収入でローンを返済する。これが、ヴィレッジフォン・プログラムと呼ばれる、農村部住民に携帯電話利用サービスを再販する仕組みである。

このように農村部のマーケティングはグラミンテレコムが担当し、グラミン銀行の融資担当者のネットワークを介して販売したため、グラミン・フォン自身は、農村部の顧客から料金を回収する方法や営業する方法について熟知しておく必要がなかった。こうして、携帯電話を他の人に貸すことをビジネスにする村のヴィレッジフォンレディは、爆発的なビジネスになり、携帯電話の急速な普及につながった。当時、グラミン銀行は、女性に対してお金を貸し付け、牛を買い、そのミルクを売ってお金を返済するというサイクルのビジネス・モデルで既に成功を収めていた。グラミン・フォンを設立する前に、カディーア氏はこの牛の部分を携帯電話に置き換えて、ユヌス総裁を説得した経緯がある。つまり、携帯電話を買うためのお金を女性に貸し付け、その携帯電話を村人たちに貸し出す。牛を携帯電話に置き換えることで、村人たちはコミュニケーションの基盤を手にいれることが出来き、それを使う村人たちが経済的自立を行うための大きな機会になる、といった構想を描いた。

図表 10：グラミン・フォンのモデル概要



グラミン・フォンの効果として、ヴィレッジフォン・プログラムを通じて、25 万台以上のヴィレッジフォンが 8 万以上の村に携帯電話が普及し、約 2 千万人の貧困層をカバーした。その販売を担う企業家（ヴィレッジフォンレディなど）はそれぞれの村全体の需要を合計し､村全体にサービスを提供する事によって､所有する携帯電話 1 台当たり毎月 100 米

ドルを超える収入を創出している。

同プログラムは、各主体が経済的便益を享受するとともに、貧困層の社会参加の促進など、あらゆる社会的格差の解消につながったと評価されている。グラミン・フォンは、国内の都市部及びルーラル地域をカバーし、現在 2,800 万人以上が加入しており、同国内最大の市場シェアを有する。同様のモデルが、アフリカのウガンダやルワンダにも展開されているなど、国際的な影響も大きい。その他、グラミン・フォンは、携帯電話を活用した少額決済などのモバイル・コマースの市場も爆発的な拡がりを見せている。具体的には、公共料金を携帯電話で支払う BillPay サービスや、携帯電話インターネットを通じて商品の売買を実現する CellBazaar サービスが提供されている。今まで都市部から切り離された生活をしてきた主に農村の住民が、携帯電話というインフラを利用することで、貨幣経済に参画することが容易になり、収入獲得の機会がもたらされた。この動きが、国の経済活性化に与えるインパクトは極めて大きいと考えられる。

第 4 章　軍事におけるデジタルデバイド

4-1　IT 革命の軍事的影響

戦争で優位に立つ国は、情報を収集し分析・統合して戦闘の場により早く活用できる国であるといわれている。現在、軍事においても IT 革命は進行しており、勝敗を左右するともいわれている。

先進国での、戦争や、国際間の紛争への介入といった軍事力の行使に関しては、もはや政府によってではなく、国民の総意や国際世論に大きく依存せざるをえず、CNN や、インターネットに代表される情報化の進展によって、国境を越え、複数の国の国民が、同時に同じ情報を共有することが可能になることで、国家による情報操作にも関わらず、軍事力行使への国民の合意形成がより困難なものとなる。

同時に、軍事面での情報化が進んだ国においては、軍事力の直接行使の力は保持しつつも、軍事力行使にかかわる意思決定を支援する情報システム機能や、軍事力の適切な運用を支援するネットワーク機能等を重視する傾向が強くなってきた。すなわち、直接的軍事力の存在は依然として確たる脅威であることは紛れもない事実ではあるが、IT 革命の進展は、直接的軍事力の行使の可能性を低める一方で、IT の軍事面での活用能力、すなわち軍事面でのネットワーク力やシステムの力を直接的軍事力と同様の脅威の 1 つとして認識するようになっている。

また、IT が急速に進歩している状況において、核・生物・科学兵器や弾道ミサイルといった大量破壊兵器からコンピュータ・ウイルスといった形のない情報自身までが攻撃の手段となり、攻撃の対象も国家から個人まで至っており、脅威の多様化は飛躍的に拡大している。さらにメディアを通して流れる情報そのものも、場合によっては脅威となることがある。

4-2　情報 RMA

情報 RMA[3]は大きく分けて 3 つの面がある。第一が、軍事インフラ面の革命であり、主に情報システムの整備、情報共有、戦場認識能力の向上があげられる。そしてこのなかでも情報システム上の戦いが独立したものをサイバー戦争と呼ぶ。第二が、兵器性能の飛躍的向上である。精密誘導兵器の登場と、兵器の効率的利用、精密攻撃である。第三が、運用上の革命である。これは、主に効率的な兵站管理であり IT の活用は組織内の情報の流れを効率化し、組織が行う活動のリードタイム（活動の実現に要する時間）を短縮する。

この第一と第二の複合により、システム化による戦力の発揮、広域分散化した小規模部隊からの連携した攻撃、作戦の拡大と作戦スピードの加速等が可能になる。

情報 RMA は、情報化、ネットワーク化を進め、組織面でもナレッジマネージメントを進めることで、情報の流れと意思決定を迅速にし、効率的な組織づくりを行い、軍隊の省略化を進めている。また、すべてのプロセスを電子化することで業務の効率化・高速化が実現でき、意思決定に至る一連のプロセスのスピードを高めることができる。

一方、1997 年に米国国防総省統合参謀本部議長が発表した情報 RMA が達成する軍隊の特徴として以下の 9 点があげられる。

① 戦場認識能力の向上であり、各種センター等からの情報を情報ネットワークを通じて共有化して、効率的な攻撃と防御を行う。
② システム化による戦力の発揮で、戦車や戦闘機をネットワーク化することでシステム全体としての戦闘能力を拡大する。
③ 精密誘導兵器の活用による精密攻撃であり、より効率的な攻撃を実現する。
④ 広域分散化して小規模部隊による情報ネットワークを利用した連携攻撃である。
⑤ 作戦域の拡大と作戦スピードの加速化である。
⑥ 電子空間の利用であり、いわゆるサイバー攻撃とその防御である。
⑦ 無人化と省略可であり、味方の死傷者の極少化と組織の効率化である。
⑧ 長期消耗戦から短期打撃戦への転換である。
⑨ 効率的な兵站である。

以上のような情報 RMA は戦闘のあり方を大きく変えている。特に情報インフラ面、支援体系では、正確かつ迅速に情報収集を行い、その情報を分析評価した後、指揮官の意思決定、命令の伝達、軍隊の運用に有効に活用することがいっそう重要性を帯びてきている。

軍事組織における情報の流れは、前線で戦う部隊の兵士や兵器そのもの以上に戦闘の勝敗を決する不可欠な要素である。いち早く敵を発見し、迅速に部隊を移動させ、敵を撃破し戦線を維持・拡大するためには、軍隊という組織を効率的に稼働させるための情報のマネージメントが決定的な意味を持つ。

[3] RMA とは軍事における革命のことをいう。

4-3　情報戦争

情報戦争とは、情報収集や情報解析、暗号解析やデマの流布といった情報分野での戦いの事をいう。米国国防大学戦略研究所によると、情報戦争を以下の 7 つの形態に分類している。

① 指揮統制戦争（Command-and-Control-Warfare. C2W）
実際の戦場において、物理的に相手方の指揮系統を麻痺させるか、または寸断することにより、作戦遂行を阻止する軍事戦略。具体的には砲爆撃によるハードキルと同様に、電磁波干渉、コンピューター・ウイルス、ジャミングや線切断による通信系破壊によるソフトキルが有効となる。

② 情報基盤戦争(Intelligence-Based Warfare. IBW)
情報基盤戦争は、攻撃的 IBW と防御的 IBW に分かれる。攻撃的 IBW とは、スタンドオフ兵器や火力兵器などのターゲッティング（探知、目標確認、伝達、射撃、効果までの一連のプロセス）に必要なセンサーの制度を支える情報システム。現代のピンポイント攻撃を支えているのはこの攻撃的 IBW である。防御的 IBW とは、ステルス性による防御などである。

③ 電子線（Electronic Warfare. EW）
電子線には、ジャミング信号（電波妨害）による対レーダー妨害、周波数ホッピングやスペクトル拡散による対通信妨害、暗号使用等が含まれる。

④ 心理戦（Psychological Warfare. PW）
心理戦には様々なレベルがあり、外交的なレベルから戦場における戦術的レベルまで幅広い。情報の操作と利用による心理的効果は重要で、メディアを利用した宣伝もまた心理作戦の一側面であり、これが外交上戦争を誘発する方向にも作用するが抑止する方向にも作用する。

⑤ ハッカー戦争（Hacker Warfare. ）
相手方のコンピューターネットワークに侵入し、システムを破壊したり、麻痺させたり、断続的な故障やデータの誤り発生など、多様な形態を持つ攻撃。

⑥ 経済情報戦争（Economic Information Warfare）
現在の資本主義社会においては、経済戦争と情報戦争が結合した形態をとる。国際貿易、国際経済に関する情報の統制の側面と、情報自体が持つ経済的側面の 2 つがあるが、相手国へのその流れをコントロールすることが重要である。

⑦ サイバー戦（Cyber-warfare）
様々なシステム上のセンサーを無力化し、あらゆるセーフガードが機能しないようにする Semantic 戦争や情報テロがサイバー戦争に含まれる。

また、この情報戦争の特徴として以下があげられる。

① 実施コストが安価である。情報の知識とシステムだけで可能であり、他の兵器よりコストが格段に安い。

② 境界線が曖昧化する。情報システムの世界的相互関係が複雑化し、国家間の国境が曖昧になっている。
③ システム管理機能の役割が増大する。情報システムが高度化し、その管理・統制に非常に大きな労力が必要となる。
④ 攻撃能力が増大する反面、脆弱性も拡大する。攻撃能力の増大の反面、そのシステム自体が内的に持つ脆弱性、攻撃に対する脆弱性も同時に増大する。
⑤ 地域特性が無意味化する。バーチャルなネットワーク上の戦略において、これまでの地政学的な位置、距離感覚などは無意味化する。

4-4　サイバー戦争

IT 革命は、レーダー、センサーやコンピューターネットワーク等の情報通信といった支援体系を飛躍的に発達させた。そして、支援体系であった情報通信ネットワーク自体が戦場となるに至った。これがサイバー戦争である。

情報 RMA 化が進んだ軍隊は、精密攻撃が可能となり的に先んじた行動をとることができる。また、さらにサイバー戦争を有効に活用することができ、めまぐるしく変化する戦況に迅速に対応でき、その結果、これに対応できない軍隊との戦闘の優劣は明白である。また情報 RMA への対応が遅ければ、サイバー戦争により気づかないうちに被害を受け戦わずして敗戦を招くことさえ起こりうる。

こうしたサイバー攻撃を行う主体は単独のハッカー、ハッカー集団、犯罪・テロ組織、敵国等が考えられるが、すでに、こうした攻撃は現実のものとなっている。

1997 年に米国で行われた演習では、電力供給施設に侵入し配電を止め、911 番（日本の 110 番と 119 番と一緒）の回線を遮断できることが確かめられたといわれている。また、コソボ戦争では、米国はユーゴスラビア軍のコンピューターを破壊するサイバー戦争を練り上げており、ユーゴスラビア軍の防空システムに侵入し、虚偽の標的を画面上に映し出そうとした。また 2001 年、米国のスパイ偵察機が中国国内に緊急着陸した事件後、米中間に一種のサイバー戦争が起こった。

米国では、サイバー攻撃から守るために、1996 年に米国大統領の行政命令に基づき、大統領直属機関の政策決定委員会に属する運営委員会は、国家重要インフラへの攻撃の対応として、関連機関を調整するための重要インフラ保護専門担当班と、国家重要インフラを保護し、持続に運営するための政策を開発する重要インフラ保護大統領特別委員会の 2 つの組織を設置した。その後 1998 年にはコンピューター網統合任務部隊を創設し、また、情報戦争に対応し米国の重要インフラをサイバー攻撃から守るために FBI 内に国家重要インフラ保護センターを設立した。このように様々な措置をとっている。

4-5　サイバー攻撃の事例

国内外で企業や組織を狙ったサイバー攻撃が発生している。

図表 11：国内外に発生したサイバー攻撃事例

2010年7月	イランの核関連施設が「Stuxnet」によるサイバー攻撃を受ける
2011年2月	エジプト政府への非難を続けていたハクティビスト集団のAnonymousがエジプト情報省とムバーラク大統領のWebサイトにDDoS攻撃
2011年2月	中国から欧米エネルギー会社5社が攻撃を受ける
2011年3月	韓国の大統領府や銀行など40機関が大規模ハッカー攻撃を受ける
2011年4月	ソニーオンラインエンタテインメントの「PlayStation Network」などが既知の脆弱性を突かれ1億件以上に及ぶ個人情報が流出
2011年5月	米航ロッキード・マーチン、情報システムが大規模なサイバー攻撃を受けたと発表
2011年6月	米グーグルが中国からサイバー攻撃　米韓政府関係者らが被害
2011年7月	韓国のISP、SKコミュニケーションズが不正アクセスを受け、同社のユーザー約3500万人分の個人情報が漏洩
2011年6月	米シティバンク　サイバー攻撃により36万以上の口座が影響を受ける
2011年9月	三菱重工、標的型攻撃を受けて11事業拠点、83台のPC／サーバに被害。IHIにも同様の攻撃
2012年2月	台湾フォックスコン関連のWebサイトがハクティビスト集団からサイバー攻撃を受けて情報漏洩
2012年5月	大規模なサイバー攻撃により米連邦政府職員12万3000人の情報が漏洩
2012年6月	クレジットカード決済処理会社の米グローバル・ペイメンツ、不正アクセスにより150万件以上のカード情報が流出
2012年6月	財務省、自民党、日本音楽著作権協会（JASRAC）などのWebサイトがDDoS攻撃を受ける。日本での違法ダウンロード刑事罰化への抗議の一環でAnonymousが攻撃
2012年12月	米ニューヨークタイムズ、標的型攻撃により社内ネットワークに不正侵入され、全従業員のネットワークログインパスワードが窃取されるという深刻な事態に
2013年3月	人気メガネブランドJINSのECサイトで大規模な情報漏洩
2013年3月	韓国のテレビ局や金融機関が大規模サイバー攻撃を受け、ATM1万6000台が停止など社会に大きな混乱
2013年4月	Anonymous、北朝鮮の大陸間弾道ミサイル実験などを非難し、同国関係の複数のWebサイトをサイバー攻撃
2013年4月	宇宙航空研究開発機構（JAXA）、国際宇宙ステーション関連のデータに不正アクセスがあったと発表
2013年5月	ヤフー日本法人のサーバがハッキング被害。最大で2200万件のIDが流出

① イランの核関連施設を狙った「Stuxnet」

2010 年 7 月に判明したイランのウラン濃縮施設核施設が狙われた攻撃は、“サイバーテロ”のとてつもない脅威を国際社会に知らしめた。このとき侵入したコンピューターウイルス「Stuxnet」により、同施設内に設置される遠心分離機の一部が破損したとされている。Stuxnet は、USB メモリー経由で侵入し、Windows の脆弱性を悪用して PC を感染させた後、独シーメンス製ソフトウェアを攻撃対象とする特徴を持つ。このことから、従来安全だと考えられていたスタンドアロンの産業制御システムであっても、サイバー攻撃を受ける危険が十分にあることがわかり、世界中に大きな衝撃を与えた。また、この攻撃については、疑惑がもたれるイランの核兵器開発を標的にした米国とイスラエルの共同オペレーションであるとする報道も数多くなされた。さらに、一部の軍事専門家は、サイバー攻撃が人的被害を伴わずに核開発の進捗を遅らせる効果を示したことから、核不拡散政策に有効な新しいツールとしての可能性を主張している。

② ソニー子会社を襲った過去最大規模の個人情報漏洩

ソニーの子会社ソニーオンラインエンタテインメントが運営する「PlayStation Network」および「Qriocity」が 2011 年 4 月 17 日から 19 日にかけて不正アクセスを受け、PlayStation Network の会員約 7700 万件、Qriocity の会員含め 1 億件以上に及ぶ大量の個人情報が流

出した。流出したとされる個人情報は、氏名、国と住所、電子メールアドレス、生年月日、性別、ログインパスワード/ID。さらに、1000 万件以上のクレジットカード情報も漏洩した疑いがあり、痛烈な批判を浴びた。この攻撃は、アプリケーションサーバーの既知の脆弱性を突いたものだった。Web サーバーを通じてアプリケーションサーバー上に不正ツールを仕込み侵入経路を確立。そこからさらに DB サーバーへのアクセス権を取得し個人情報にたどり着いたと見られている。
ソニー側は、国際的なハクティビスト集団である「Anonymous（アノニマス）」の関与を示唆。一方の Anonymous 側も、PLAYSTATION 3 への Linux インストールに関する情報公開に対しソニーが法的手段に出たことに抗議して同社に DDoS 攻撃を仕掛ける「Operation Sony」への参加を呼びかけていた。ただし Anonymous は情報漏洩事件への関与を否定している。
この事件を受けてソニーは、情報セキュリティ会社と協力して、より高度なセキュリティ技術の導入やシステムへの侵入および脆弱性をモニタリングするソフトウェアの追加、暗号化方式の強化、ファイアウォールの増設などの安全管理措置を講じた。そして事件から 3 カ月後の 7 月 6 日、ようやく PlayStation Network と Qriocity のサービスの全面再開にこぎ着けている。

③ 三菱重工と IHI

三菱重工業は 2011 年 9 月 19 日、同社内で利用する複数台のコンピュータがウイルスに感染し、情報漏洩の危険性も判明した事実を警察当局に報告したことを発表した。
この攻撃は標的型攻撃によるもので、次のような手順で行われたと推測されている。最初に、ある外部からの電子メールに添付されたウイルスファイルを職員が開封、ウイルスに感染したことで攻撃者は外部から感染した端末を制御できる状態になる。その後この端末から攻撃者の操る C&C サーバーを介して、新しいウイルスのダウンロード、攻撃の証跡の隠蔽、内部拡散、情報探査が実施された、という手順である。
被害を受けた PC やサーバーは三菱重工の 11 の事業拠点で合計 83 台に及んだ。ただし同社では、コンピュータのシステム情報（ネットワークアドレスなど）の一部が流出した可能性があるとしながらも、製品や技術に関する情報の流出は確認していないとしている。
翌 9 月 20 日には IHI も、2009 年 7 月頃から情報漏洩を引き起こす恐れのある大量のウイルスメールが送付されるサイバー攻撃を受けていたことを明らかにした。ただし三菱重工とは違い、IHI では実際にウイルスには感染しておらず、情報流出もなかったとしている。
日本を代表する重工業メーカーである両社に対して相次いで行われたサイバー攻撃は、日本の防衛体制にも脅威をもたらしかねない極めて重大な事件であるとして注目を集めた。

④ 日本の官公庁が Web サイト改竄被害

2012 年 6 月 26 日から 27 日にかけて財務省や最高裁判所など複数の官公庁の Web サイトの一部が書き換えられたり、閲覧できなくなったりした。同じ時期に自民党や民主党、日本音楽著作権協会（JASRAC）、国土交通省河川局なども DDoS 攻撃を受けている。財務省は同省の Web サイト内にある「国有財産情報公開システム」が改竄されていたことを確認し、26 日に同システムを閉鎖。最高裁判所の Web サイトでは、全国の裁判所のサイトにリンクするページが一時表示できなくなった。

この事件の直前の 6 月 20 日に参議院本会議での賛成多数により、違法ダウンロードの罰則化を含む改正著作権法が成立している。日本でのこの決定に対して Anonymous は抗議の意を表明し「Operation Japan」と名づけた日本政府に対するサイバー攻撃を予告していた。なお、このサイバー攻撃では、「HOIC（High Orbit Ion Canon）」と呼ばれる DDoS 攻撃用ツールが使われたと見られている。

⑤ メガネブランド JINS の EC サイトで大規模な情報漏洩

2013 年 3 月 15 日、同社が運営するメガネ通販サイト「JINS ONLINE SHOP」への不正アクセスによって情報漏洩事故が発生したと発表した。同社はその前日に Web サーバーへの不正アクセスの痕跡を発見し、クレジットカード情報漏洩の可能性を認識。急遽、情報漏洩事故対策本部を設置するとともに、カード情報漏洩事案の専門調査機関への不正アクセスの発生原因の調査や情報漏洩範囲の特定を委託した。

その後 4 月 9 日に同社は、情報漏洩した可能性のあるクレジットカード情報の範囲は、今年 3 月 6 日から 3 月 14 日の間に EC サイトにおいてクレジットカードによる購入手続きをした顧客の情報 2059 件であるとしている。そのうち顧客から不正利用があった旨の申告を受けている件数は 20 件だった。

調査の結果、今回の不正アクセスの原因は、ハッカーが JINS ONLINE SHOP のシステムに使用されていたミドルウェア「Apache Struts2」の脆弱性を利用してシステムに不正に侵入したことによるものだと判明。ハッカーはファイルの変更権限を不正に取得し情報を摂取したと見られている。また、Struts は脆弱性が指摘されていた古いバージョンを使用していたという。ジェイアイエヌでは再発防止策の実施と並行して、JINS ONLINE SHOP の再開に向けた作業に着手。新システムの完成、PCI DSS 準拠の監査、クレジットカード会社の審査などの段階を経て、2013 年 6 月中のサービス再開を見込んでいる。

⑥ 韓国のテレビ局や金融機関が攻撃され ATM1 万 6000 台が停止

2013 年 3 月 20 日に韓国で発生した複数企業への大規模サイバー攻撃は、発生日から通称「320 サイバーテロ」とも呼ばれている。この同時多発攻撃により、同国の 3 つの主要テレビ局（KBS、MBC、YTN）放送局と 2 つの大手銀行を含む複数企業のコンピュータおよびネットワークが一斉にウイルスによる被害を受けた。その結果、銀行の ATM 1 万 6000

台とインターネットバンキングが停止するなど、社会に大きな混乱を招いた。障害を受けたサーバーや PC の台数は約 4 万 8700 台に及ぶと言われる。
セキュリティ製品ベンダーのマカフィーが公表している調査結果によると、この攻撃で用いられたウイルスはコンピュータのマスターブートレコード(MBR)を書き換えるもので、感染した端末を起動不能にしてしまうという。事件を受け、韓国政府では、サイバー攻撃を行ったのは北朝鮮の工作機関であるとの見解を表明している。

⑦ IT 企業ヤフー　防御を突破され最大 2200 万件の ID が流出

ヤフージャパンは 2013 年 5 月 17 日、前日 16 日の 21 時頃に、同社の会員用 ID「Yahoo! JAPAN ID」を管理しているサーバーに外部からの不正アクセスがあったことが判明したと発表した。同社では 4 月 2 日に発生した不正アクセスを受けて監視体制を強化していたところで、新たに不審なログインを検知したという。調査の結果、最大 2200 万件に及ぶ ID が抽出されたファイルが作成されていることが判明した。

同社では、このファイルが外部に流出したかどうかは確認できていないとしながらも、サーバーと外部との通信量から判断して流出した可能性が否定できないと表明。さらにその後の調査により、流出した ID のうち 148 万 6000 件については、不可逆暗号化されたパスワード、パスワードを忘れてしまった場合の再設定に必要な情報の一部が流出した可能性が高いことを発表した。同社は 5 月 23 日 19 時より、秘密の質問を利用してパスワードを再設定するための機能を一時的に停止。また、対象の ID の利用者に対して強制的にパスワードと秘密の質問のリセットを行った。その後、ID を持つユーザーに向けて不正アクセスされた ID かどうかを確認するページを設け、該当するユーザーに対しログイン時に再設定画面を表示するようになった。ヤフーでは、今回の不正アクセスは、前回の不正アクセス後に実施した対策において関連するアカウントの認証の再設定を社内で徹底できていなかったことに起因するとしている。

4-6　日本軍事における情報 RMA

情報 RMA を推進すれば、従来型軍隊に対してきわめて優位に立てるのみならず、死傷者や損害を最小限にすることができる。非核三原則を堅持する日本にとって情報 RMA は有効なものと思われる。

日本の防衛庁は情報ＲＭＡ化された軍隊による将来戦の特徴について以下を上げている。

① 戦場認識能力の向上

将来戦では、無人偵察機や偵察衛星を含めた多様なセンサーからの情報を総合することにより、戦場に関する情報が正確に得られるようになる。さらに、得られた情報が情報ネットワークを通じて各級指揮官を始め末端の兵員にもリアルタイムで提供され情報共有が進む結果、「戦争の霧」は軽減され、効率的な攻撃の実施や防御における被害局限などが可能になる。

② システム化による戦力発揮

無人偵察機のような多様なセンサー・プラットフォームを情報ネットワークによって結びつけることによって、攻撃プラットフォーム自らのセンサーでは確認できない目標に対しても精密誘導兵器による攻撃がなされる。すなわち、攻撃プラットフォームは、自ら搭載するセンサーに加え、統合的な情報ネットワークを通じて得た多様なセンサーからの情報に基づいて、より遠距離にある目標に対して、より正確に火力を指向することとなる。

③ 精密誘導兵器の活用による精密攻撃

戦場認識能力の向上によって正確に把握されている敵目標を、確実かつ必要最小限の破壊力によって効率的に撃破するために、精密誘導兵器が必要不可欠となる。さらに、長射程の精密誘導兵器は、味方戦闘員の危険が少ない相手の射程外から軍事目標のみを正確に攻撃することができるため、攻撃側の兵員の安全を確保するとともに、民間人および施設に対する付随的損害を最小限にすることが可能である。

④ 広域分散化した小規模部隊からの連携した攻撃

戦場認識能力の向上および統合的な情報ネットワークの構築により、各部隊は情報を同時に共有でき、また、このようなネットワークにより指揮・統制を受けることができることから、分散している部隊であっても統一的な運用、戦闘が可能となる。

⑤ 作戦域の拡大と作戦スピードの加速

情報ＲＭＡ型軍隊では、戦場認識能力の向上、精密誘導兵器の長射程化や部隊の高機動性により、単位部隊あたりの作戦域が拡大する。それに伴い、陸・海・空といった異なる軍種の作戦域をオーバーラップさせることが可能になることから、必要に応じ、互いの能力を補完させ、戦力を効率的に運用するために統合的な部隊運用が行われる。

⑥ 電子的空間の利用

敵国が高度に情報化している場合には、社会インフラや指揮統制機能等をつかさどるコンピュータシステムをサイバー攻撃によって混乱ないし無力化させることが、従来の火力を用いた物理的攻撃を補完する有効な攻撃手段となる。したがって、情報化が進んだ国家では、このような攻撃から民間の情報システムを含む自らの情報システムを防護する必要性が高まる。

⑦ 無人化・省人化

味方兵員の死傷を局限するために、戦場偵察、攻撃プラットフォーム、あるいは地雷除去等、敵の攻撃を受ける危険性の高いエリアなどで行動する兵器には、極力無人兵器が使用される。また、将来戦における作戦スピードの加速化に対応するため、従来人間が行って

きた情報処理および装備品操作等において大幅な自動化・省人化が進み、戦闘効率の向上が図られる。

⑧ 長期消耗戦から短期集中的な打撃戦への変化
情報ＲＭＡ型軍隊による将来戦では、過去往々にして長期消耗戦になりがちであった、敵軍隊の殲滅や敵国土全体に対する物理的攻撃よりも、軍事部門の中枢や情報ネットワークに対し、サイバー攻撃を並用しつつ精密誘導攻撃などにより致命的な打撃を与え、短期間で敵国の国家意志を左右することがまず追求される。

⑨ 効率的な兵站管理
情報ネットワークの構築により、各部隊の位置、兵員の損耗状況、弾薬、燃料、糧食等の保有状況が正確に把握できることから、人員の補充や弾薬等の補給などの効率的な兵站管理が可能となる。
　以上の事を実現できるように防衛庁は取り組んでいる。

4-7 情報 RMA の 7 原則

① 情報化
戦場認識能力および対処能力を向上させるためには、情報ネットワークを通じて高精度かつ大量の情報を陸海空各自衛隊の部隊が共有し、いわゆるＣ４ＩＳＲ すなわち指揮、統制、通信、情報等の各機能を効率的かつ効果的に機能させる必要がある。とりわけ我が国の場合、専守防衛という受動的な防衛政策をとり、国土における防衛戦闘が想定されることから、早期に敵の侵攻を探知するとともに、上陸した敵の動静等を正確に把握するための多種多様なセンサーを開発、装備する必要がある。この際、上陸した敵部隊と我が方の部隊が極めて接近したり混在する可能性があることから敵味方の識別能力の向上に留意する必要がある。

② 統合化
人的、物的、経費的な資源の制約の中で、防衛力の役割の多様化、将来戦における作戦域の拡大に応じて、防衛力の目標達成効率を高め、また事態への柔軟な対応を可能にするために、陸海空自衛隊の統合運用を念頭に置いた戦術、組織編成および装備等が必要である。

③ 迅速化
作戦スピードの加速化を可能にするため、急激に変化する戦況に即応できる迅速な意思決定サイクルを構築する必要がある。このため、例えば人工知能を活用して、センサーからの情報を総合、分析、処理し、指揮官の判断を支援する意思決定支援システムの開発が必

要である。さらに、対処行動の時間を短縮するため、部隊の高い機動性の確保が必要である。

④ 効率化

防衛力の目標達成効率を向上させるため、目標を正確に破壊し得る精密誘導兵器等の装備システムを構築することにより対処能力を向上させるとともに、情報システムによる戦闘管理能力の向上等あらゆる手段を活用して、単位部隊あたりの戦闘効率を高めることが必要である。また、国土における防衛戦闘という観点から、有事の際に国土および民間資産が被る付随的被害を最小限にするために、精密誘導兵器を有効に活用し得る組織、戦術等を整備する必要がある。

⑤ 柔軟化

防衛力の役割の多様化、情報ＲＭＡ化された戦場における急激な状況の変化に的確に対応するため、可能な限り部隊を標準化（人員、装備等の共通化）　し、任務の内容に応じて必要な規模および機能を持った部隊を素早く柔軟に編成する能力が必要である。

⑥ 防護化

巡航ミサイルや弾道ミサイルに対する対処能力を整備する必要がある。また、ネットワーク・セキュリティを強化し、情報通信システムの無能力化や損傷を極力回避することが必要である。万一被害を受けた際にも任務を継続し得るよう、情報ネットワークの多重性や抗堪性を確保することが必要である。特に、専守防衛に基づいた体制をとる我が国では、センサーの防護を強化することによる残存性の確保が重要である。

⑦ 相互運用性

情報ＲＭＡ後の日米共同作戦において、日米が迅速な作戦の調整を行うためには、情報ネットワークを連接させ、リアルタイムで情報を共有していることが不可欠である。今後の防衛力整備においては、情報ＲＭＡという観点からも、日米の適切な相互運用性の確保が必要である。また、国連の平和維持活動などへの参加の際に、米軍以外の軍とも情報を共有し得るよう配意する必要がある。

以上の事をまとめると、多様なセンサーを含む多重化、抗堪化された情報ネットワークを基礎として、陸海空自衛隊各部隊が情報をリアルタイムで共有するとともに米軍との相互運用性を確保し、事態の変化に柔軟に対応し、かつ最短の時間で最も効率的に戦力を発揮（統合化、効率化）し得る態勢を構築するとされる。

おわりに

日本でのデジタルデバイドはパソコン・スマートフォンやインターネットが普及した頃から比べると、今現在では格段に無くなり、誰もが使える物になっている。しかし、そんな便利な世の中になっている現在でも、お年寄りや地方ではパソコン・スマートフォンやインターネットの使い方が分らない人も少なくない。第 2 章で説明した様に海外では小中学校でパソコン・スマートフォンやインターネットを使った宿題を出されるケースが増えてきている。日本でもあと数年経てば海外の様にパソコン・スマートフォンやインターネットを使って宿題を出される事が主流になってくるかもしれない。そうした時代の移り変わりに私たちも遅れをとらず柔軟に対応していくべきだと思う。

デジタル機器を発売する会社も若者からお年寄りまで誰でも使えるように、その年代に応じて使いやすいデジタル機器を提供する必要があると思う。最近では、お年寄りでも簡単に使える携帯電話（らくらくホン）が発売されている。特徴としては、携帯画面の文字が大きく見やすくなっており、電話の音も普通より大きくなっており聞きやすい作りになっている。パソコンなども、らくらくホンの様に画面の文字を大きくし、音声案内などをつけるべきだと思う。

高度情報社会においては、プライバシー侵害の危険性が従来にも増して拡大しており、そのことが新たなセキュリティ格差を生み出す要因になっているので、このような新たなデバイドを生じさせないためにも、個人が自分に関する個人情報をどのような場面で利用し、どのようなサービスを望むのかを確認し、自分自身の情報を情報社会において適切にコントロールすることが必要だと思う。

参考文献

書籍

・藤　和彦　『よみがえれ!中小企業―デジタルディバイドなんかこわくない』 平凡社新書 2001 年
・木村　忠正　『デジタルデバイドとは何か―コンセンサス・コミュニティをめざして』 岩波書店　2001 年
・C&C 振興財団　『デジタルデバイド-構造と課題-』　NTT 出版　2002 年

URL

・デジタルデバイドの現状
http://www.medialabo.info/wip/report2002j/chapter6-j.pdf
・インターネットの利用状況
http://www.medialabo.info/wip/report2002j/chapter2-j.pdf
・総務省　情報通信白書　インターネットの利用状況
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc243120.html
・新しいデジタルデバイドについての構想
http://www.mediacom.keio.ac.jp/publication/pdf2009/hirai.pdf
・デジタルデバイドの解消
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h23/pdf/n2020000.pdf
・三河山間地域情報格差対策促進事業の概要について
http://www.pref.aichi.jp/0000001534.html
・国際的なデジタル・ディバイドの解消に関する調査研究報告書
http://www.soumu.go.jp/johotsusintokei/linkdata/h23_02_houkoku.pdf
・IT の発達と軍事組織の研究－情報 RMA にともなって想定される問題を中心に－
http://www.nids.go.jp/publication/kiyo/pdf/bulletin_j6-3_2.pdf
・「サイバー戦争」は戦争か
http://www.kasumigasekikai.or.jp/R201198b.pdf
・途上国における持続的な医療機器運営に関する一考察
http://jica-ri.jica.go.jp/IFIC_and_JBICI-Studies/jica-ri/publication/archives/jica/kenkyu/07_45/pdf/01.pdf