資料６－２

次世代の情報セキュリティ政策に関する研究会

中間報告書（案）

2008 年 4 月

次世代の情報セキュリティ政策に関する研究会

目　　次

１．はじめに

２．情報通信環境の現状
　２－１　インターネットの普及とブロードバンド化の急速な進展
　２－２　モバイル端末によるインターネット利用等の進展
　２－３　社会経済活動の ICT 依存の増加
　２－４　我が国の ICT 産業の現状
　２－５　ICT による生産性の向上と ICT 産業の国際競争力強化
　２－６　ネットワーク利用の高度化に伴う負の側面への対応

３．情報セキュリティ対策の現状と課題
　３－１　情報セキュリティ脅威の対象となる資産と主な情報セキュリティ脅威の分類
　３－２　昨今の情報セキュリティ脅威の変遷
　３－３　情報セキュリティ脅威の現状及び今後の予測
　３－４　情報セキュリティ対策の取組み状況と課題

４．近い将来のＩＣＴ環境と情報セキュリティ脅威・課題
　４－１　近い将来におけるＩＣＴ環境の変化
　４－２　近い将来のＩＣＴ環境における情報セキュリティの脅威・課題

５．現状及び近い将来のＩＣＴ環境における情報セキュリティ対策の重要性
　５－１　今後の情報セキュリティに関する主な課題等
　５－２　今後の情報セキュリティ対策について重点的に検討・実施すべき事項等

６．終わりに

１．はじめに

近年、我が国では、ブロードバンド環境の整備が進展し、これに伴い、国民生活や様々な社会経済活動におけるＩＣＴの利用が促進されている。今後、少子高齢化が進む我が国においては、ICT 利用による生産性の向上や社会経済活動の活性化がより一層求められており、そのためには、ICT の安心・安全な利用環境を整えることが必要である。

言い換えれば、年々、社会経済活動の ICT 依存度が高まる中、コンピュータウイルスの蔓延、企業・官公庁における情報漏えいの多発等、様々な情報セキュリティに関する問題への適切な対処は、これまで以上にその必要性が認識されてきている。

政府では、これまで、2000 年の高度情報通信ネットワーク社会形成基本法（以下、「IT 基本法」という。）の制定以来、官民を挙げてＩＣＴの利活用の促進に取組むとともに、その一方で顕在化してきた様々な情報セキュリティインシデントに対処するため、2005 年 5 月に高度情報通信ネットワーク社会推進本部（以下、「ＩＴ戦略本部」という。）に情報セキュリティ政策会議を設置し、また、2006 年 2 月には「第１次情報セキュリティ基本計画」を定めるなど、情報セキュリティの強化に向けた取組を推進してきたところである。

総務省では、政府における情報セキュリティ強化の方針のもと、ICT の基盤である情報通信分野やインターネットの利用者における情報セキュリティ確保のため、様々な施策を推進してきている。

こうした中、昨今では、ネットワークを経由したウイルス感染の巧妙化・高度化、あるいは被害の深刻化等が進んでいる状況であり、このような脅威の変化に対して継続的な対処が必要となっている。また、次世代ネットワークの整備促進、ブロードバンド・ゼロ地域の解消、次世代無線通信システムの実現等、ＩＣＴの利用環境も急速に進展しており、近い将来の情報通信環境の変化及びその変遷過程において想定される情報セキュリティ上の課題を明確化し、それに備えた対策を講ずることも極めて重要である。

以上を踏まえ、本研究会では、現状のインターネット等の利用環境において継続的に対策を講じていかなければならない課題を明らかにするとともに、3 年から 5 年後の近い将来におけるＩＣＴ利用環境を想定し、その変遷過程を含めて利用環境の変化により生ずる課題や問題点等を抽出し、そのために必要となる対策を導出するとともに、今後、取り組むべき情報セキュリティ政策の在り方について検討している。

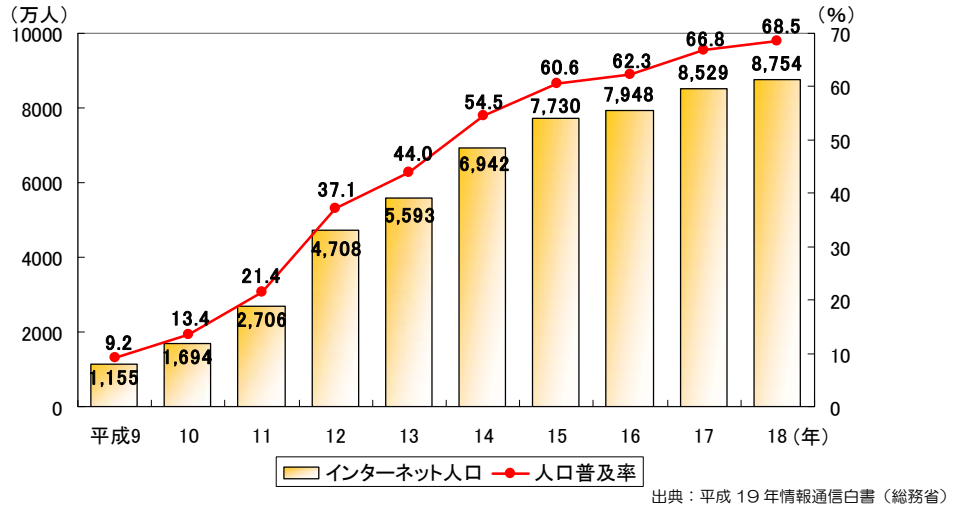
本報告書は、本研究会での検討内容を取りまとめた中間報告である。

２．情報通信環境の現状

２－１　インターネットの普及とブロードバンド化の急速な進展

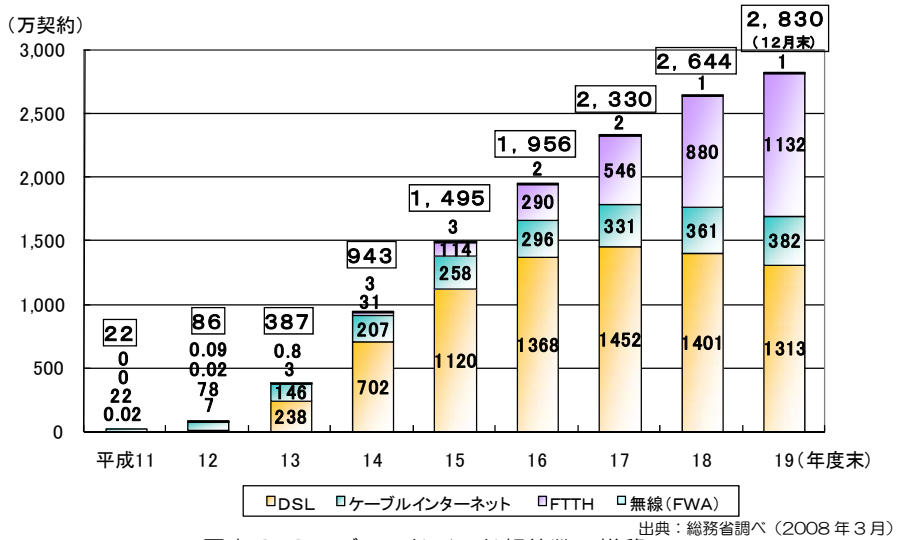
1990 年代中頃から一般での利用が進んできた我が国のインターネットは、90 年代後半まではアナログ回線や ISDN 回線によるダイアルアップ接続が主流であったが、2000 年頃以降、常時接続・ブロードバンド化が進展し、2006 年末のインターネット利用者数は 8,700 万人を越え、人口普及率にして約 70%に達している（1997 年末の利用者数は約 1,200 万人。人口普及率にして約９%であった。）【図表 2-1 参照】。

また、2007 年 12 月末現在の我が国のブロードバンド契約数は 2,830 万件で、そのうちの 40%にあたる 1,132 万件は、光ファイバ（FTTH）契約であり、年々その割合は増加している【図表 2-2 参照】。このようにインターネットは、非常に短期間で多くの国民が利用する情報通信手段として定着・普及してきていると言える。



出典：平成 19 年情報通信白書（総務省）

図表 2-1：インターネット利用者数及び人口普及率



出典：総務省調べ（2008 年３月）

図表 2-2：ブロードバンド契約数の推移

このように我が国においてブロードバンド・インターネットの普及が進展した背景としては、ブロードバンド接続環境の整備が挙げられ、2007 年９月末時点において、全世帯数の 95.7％である 4,951 万世帯において既に整備されており、さらに政府としては 2010 年度までにはブロードバンド・ゼロ地域解消を目指している。また、利用料金の推移をみても、DSL の契約料金は 2000 年度末と 2006 年度末で比較した場合、約 1/3 にまで料金が低下するなど、広く国民がインターネットを利用できる安価で高速な環境の整備が着実に進んできている。

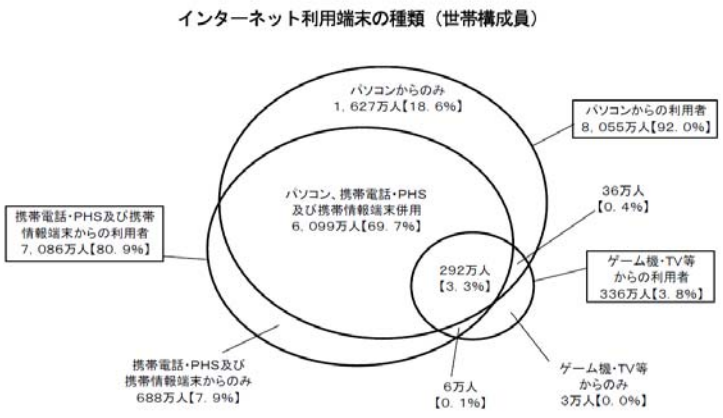
２－２　モバイル端末によるインターネット利用等の進展

ブロードバンド・インターネット接続環境の整備に加え、携帯電話・PHS は、2007 年末現在で、その契約数が 1 億件を越えており、広く国民が所有する情報通信手段となっている。このようにほぼ国民一人が 1 台を保有するまで普及した身近な情報通信手段である携帯端末・PHS、または携帯通信情報端末（PDA）といったモバイル端末を使ってインターネットに接続する利用者は、2006 年末現在で 7,086 万人（前年比 163 万人）に達しており、また携帯電話利用者の約７割が、週 1 回以上インターネットの接続手段として利用しているなど、モバイル端末によるインターネット接続が進展してきている【図表 2-3 から図表 2-5 参照】。

NTTドコモ	53,170,300
au	29,312,200
ツーカー	325,300
ソフトバンク	17,814,200
EMOBILE	238,500
ウィルコム(PHS)	4,626,400
総計	105,486,900

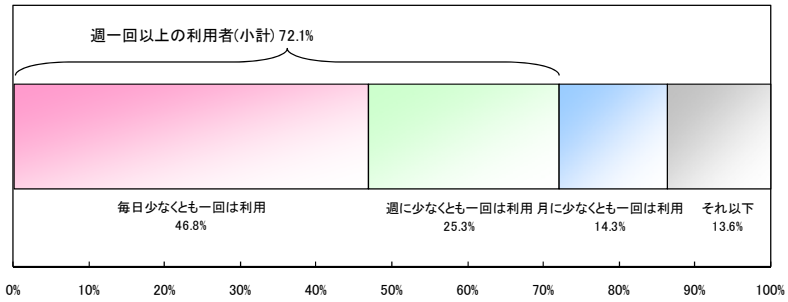
出典：電気通信事業者協会調べ(2008年1月)

図表 2-3：携帯電話・PHS の契約数



出典：平成 18 年通信利用動向調査（総務省）

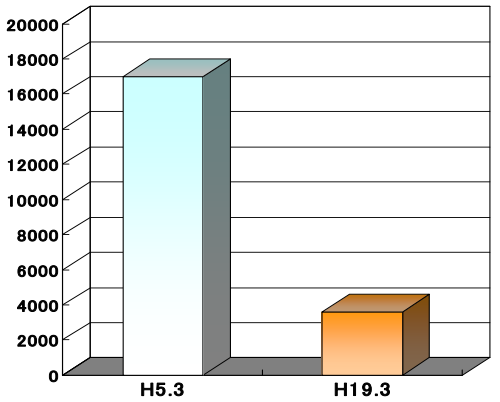
図表 2-4：インターネット利用端末の種類



出典：平成 18 年通信利用動向調査（総務省）

図表 2-5：携帯電話によるインターネット利用頻度

また最近は、携帯電話の多機能化による ICT 利用の高度化が進んでおり、音声通話機能、インターネット接続やメール機能に加え、電子マネー機能、ＧＰＳ機能、ネットワーク対戦型のゲーム機能、ワンセグ受信機能など、多くの機能を装備する端末が主流となっている。例えば、2007 年３月現在、ある携帯電話事業者における電子マネー機能を有する端末の普及率は、40%近くにまで達している。携帯電話の料金についても、2007 年度末現在の利用料金は、1992 年度末と比較した場合で約 1/5 にまで低廉化しており、料金の面からも利用し易い環境が整ってきていることが伺える。【図表 2-6 参照】。

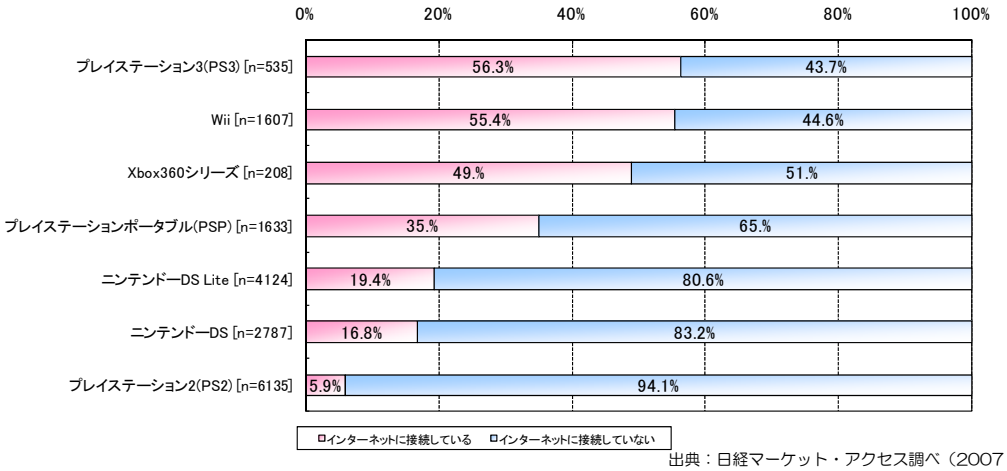


出典：総務省調べ

図表 2-6：携帯電話料金の推移

その他、インターネット接続手段の多様化という観点では、DVD/HDD レコーダー、ＴＶなどの情報家電がネットワークに接続して利用され始めており、最近の特徴としては、家庭用ゲーム機がインターネットを通じた対戦型のゲーム機能だけではなく、

専用のサイトのほか一般のサイトにも接続できるようになってきている点が挙げられ、その利用者数も増加傾向にあると考えられる。例えば、ゲーム機の販売台数は急増（主要なゲーム機の国内外累計販売台数は、Wii：2,013 万台（第３四半期販売台数（前年同期比）：118%増）、PS3：1,049 万台（第３四半期販売台数（前年同期比）：195%増）、DS：6,479 万台（第３四半期販売台数（前年同期比）：15%増）（2008 月１月、各社 HP より））しており、その多くがインターネット接続及び Web ブラウジングが可能になっている。また、国内での据置型ゲーム機からのインターネット接続は、利用者のおよそ５割を占めているとの報告もある【図表 2-7 参照】。



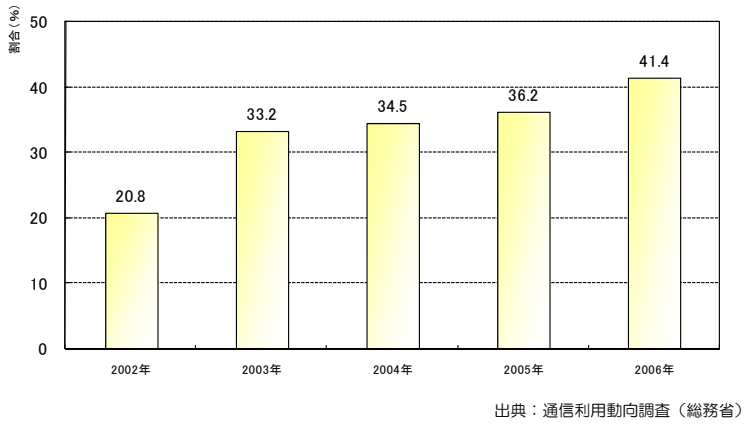
出典：日経マーケット・アクセス調べ（2007 年６月）

図表 2-7：主なゲーム機によるインターネット利用率

２－３　社会経済活動の ICT 依存の増加

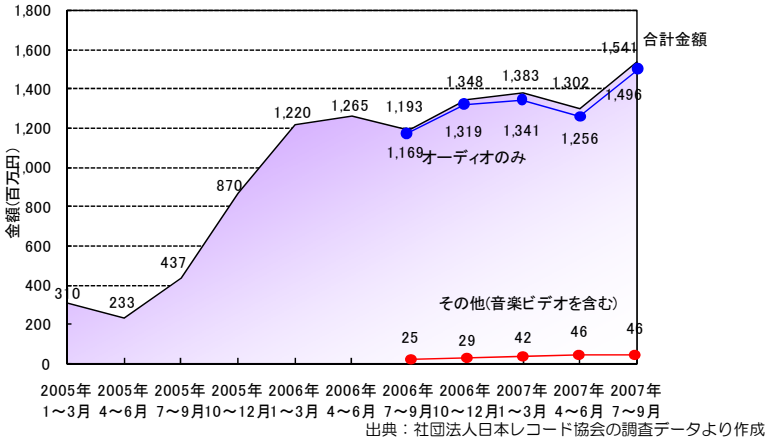
我が国では前述のとおり、低廉かつ高速な ICT 利用環境の整備が進展しており、これにより様々な社会経済活動が ICT を利用して行われるようになってきている。

個人における ICT 利用について、例えば、インターネット利用者のうち、インターネットにより商品などを購入したことのある人の割合は、2006 年度までの５年間で増加傾向にある他、音楽配信・ミュージックビデオ配信なども、急速な伸びを示しており、B2C の電子商取引が身近なものになっていると伺える【図表 2-8、図表 2-9 参照】。



出典：通信利用動向調査（総務省）

図表 2-8：インターネットによる商品・サービスの購入状況（世帯）



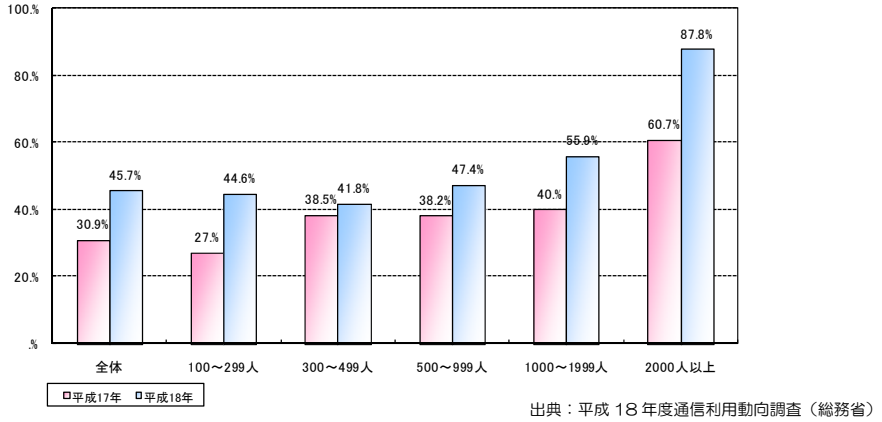
出典：社団法人日本レコード協会の調査データより作成

図表 2-9：有料音楽配信による売上実績

また、最近では、個人の利用者（消費者）が単に提供される情報やサービスを受信（消費）するだけではなく、SNS、ブログといった手段を用いて積極的に情報発信するケースが増大しており、例えば、2007 年 11 月現在のブログ開設者数は 1,300 万を越え、10 人にひとりの開設率に上ると報道されている（1 月 27 日付日本経済新聞 1 面）。さらに、個人が発信する情報が商品生産者やサービス提供者に影響する 1 つのメディア（CGM: Consumer Generated Media）として認知され、こうした個人が発信する莫大な情報が資産となって、製品の生産、販売等のビジネス展開に大きく影響するような状況となってきている。

その他、セカンドライフに代表される３次元仮想世界の登録・利用者が急増しており、日本の企業でもこのバーチャル世界においてビジネス活動を展開しているところもある。当該サービスは PC のみの利用に留まらず携帯電話からも利用可能となるなど、今後も利用環境の拡大や利用者数の増加に向けた取組みが進むことにより、より一層こうしたバーチャル世界での企業によるビジネス展開も進むものと期待される。

一方、企業の ICT 利用においては、様々な指標があるが、例えば、電子商取引を導入している企業の割合は企業の規模によらず増加傾向であり、全体として ３１％（2005 年）から４６％（2006 年）と伸びを示している【図表 2-10 参照】。また、国内の企業間の電子商取引の市場規模では、102 兆円（2004 年）、140 兆円（2005 年）、148 兆円（2006 年）と進展するなど（2007 年５月、経済産業省：電子商取引に関する市場調査）、企業における ICT 利用の進展が伺え、ICT に対する社会経済活動の依存度が大きくなってきている。



出典：平成 18 年度通信利用動向調査（総務省）

図表 2-10：電子商取引の実施状況（企業）（従業員規模別）

また、我が国の企業活動の状況を図る指標として広告費もその一つであるが、2007 年のインターネット広告費は、6,003 億円（前年比 24.4%増）となり、新聞・テレビには及ばないものの、雑誌とラジオの広告費を上回る結果となっている（2008 年 2 月、電通 NEWS RELEASE）。この要因としては、回線のブロードバンド化によるインターネットでの動画視聴が一般化してきたことや、より表現力が豊かになったことで企業のブランディングにも活用されるようになってきたこと等が挙げられている。さらにテレビ CM と連動して検索への誘導を促すクロスメディア手法が定着してきているなど、企業活動におけるインターネットの果たす役割が大きくなってきていると考えられる。

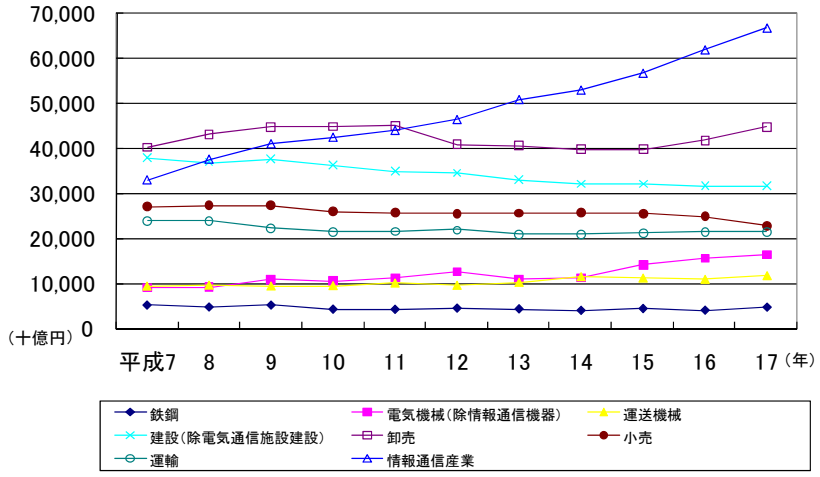
２－４　我が国の ICT 産業の現状

ICT 依存が高まる我が国の社会経済活動において、我が国の成長に対する情報通信産業の寄与度も大きなものとなっている。

国内総生産（GDP）の観点からみてみると、情報通信産業の実質 GDP は、1995 年から 2005 年までの間、過去 10 年以上にわたり一貫して増加している。その間の平均成長率は 7.3%で、主要産業の中で最も高い成長率を示している【図表 2-11 参

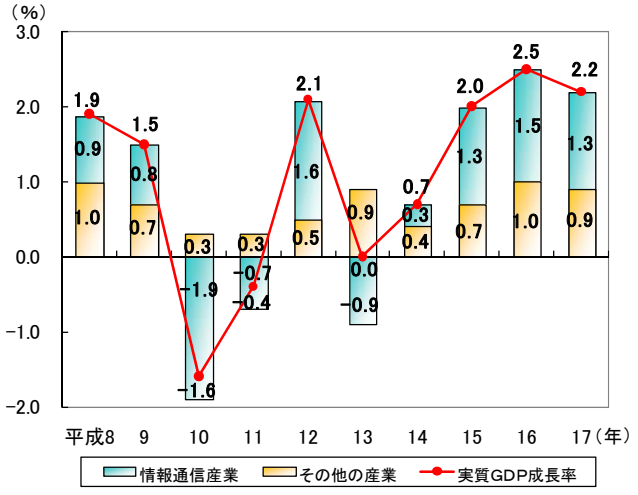
照】。また、我が国の実質 GDP 成長率に対して、情報通信産業は、1996 年以降、一貫してプラスに寄与しており、2005 年の情報通信産業の寄与率は 42.4%で、我が国の経済成長に最も大きな影響を与えている【図表 2-12 参照】。

一方、情報化投資による経済成長についての日米比較においては、我が国は米国に対して大きく水を開けられている状況である。具体的には、1990 年から 2005 年までの情報化投資の推移を比較した場合、我が国の増加率は 1.9 倍となっているのに対して、米国は 6.2 倍に達している。また、同期間の GDP の推移では、我が国が 1.2 倍となっているのに対して、米国は 1.5 倍の伸びを示しており、情報通信白書（平成 19 年度版）によると、情報化投資が GDP 成長を牽引してきたとされている【図表 2-13 参照】。



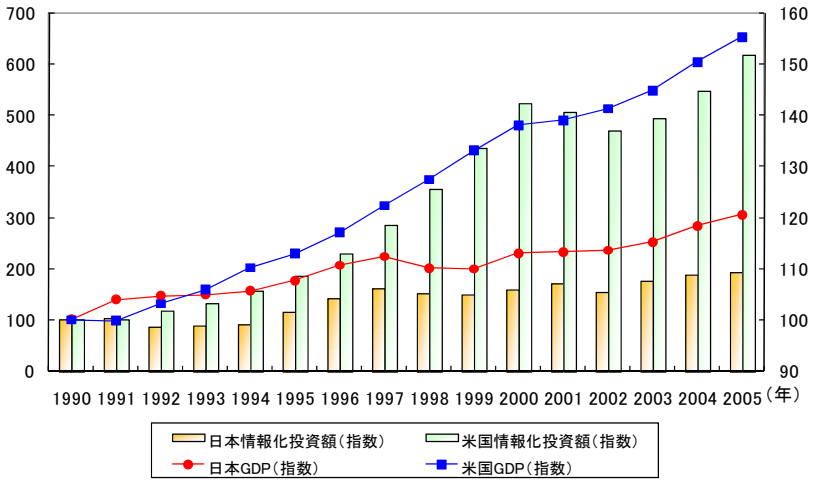
出典：ICT の経済分析に関する調査（総務省）

図表 2-11：主な産業の実質 GDP の推移



出典：ICT の経済分析に関する調査（総務省）

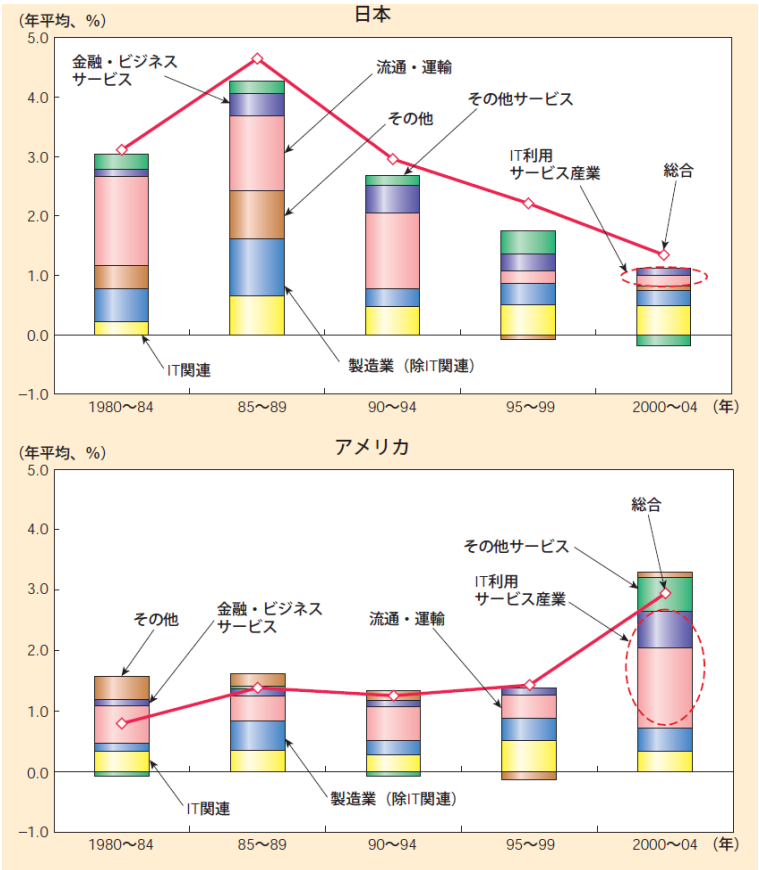
図表 2-12：平成 19 年情報通信に関する現状報告(総務省)



出典：ICT の経済分析に関する調査（総務省）

図表 2-13：日米の情報化投資額及び GDP の推移

さらに、流通・運輸や金融等の IT 利用サービス業の労働生産性への貢献に関する日米比較では、米国では 2000 年以降、IT 利用サービス業が労働生産性向上に大きく貢献している一方、我が国の寄与度は小さく、その理由として IT ネットワーク化や企業の組織改革の遅れがあると指摘されている。【図表 2-14 参照】。



出典：平成 19 年度年次経済財政報告（内閣府）

図表 2-14：日米の労働生産性上昇率の業種別寄与度

２－５　ICT による生産性の向上と ICT 産業の国際競争力強化

前述のような我が国の ICT 産業を取巻く現状を踏まえ、「経済財政改革の基本方針 2007」（2007 年 6 月 19 日 閣議決定）では、「人口減少というこれまでに経験したことのない状況の中で、経済成長を持続させ、生活の質を高くしていくことが今後の日本経済の最も重要な課題である」とし、「成長力加速プログラム」（2007 年 4 月 25 日 経済財政諮問会議）などの成長力強化に政府一丸となって取組むことで、「我が国の労働生産性の伸び率、すなわち一人が１時間働いて生み出す付加価値の伸び率を５年間で５割増にすること」を目指している。

また、「成長力加速プログラム」においては、サービス革新戦略として、IT による生産性の向上や ICT 産業の国際競争力の強化、情報セキュリティの向上などに取組み、経済効率と質を引き上げ、国際的にも見劣りのしない生産性水準にキャッチアップするとしている。

このように、今後の我が国の経済成長にとって、ICT による生産性の向上や ICT 産業の国際競争力の強化は不可欠であり、これまで以上に ICT を安心・安全に利用できる環境を整備するための情報セキュリティ対策への取組みが重要となってきている。

２－６　ネットワーク利用の高度化に伴う負の側面への対応

前述のとおり、年々、ICT 利用の急速な普及、言い換えれば、社会経済活動の ICT 依存が進んできており、今後もその傾向は続くとものと考えられる。特に、経験をしたことのない少子高齢化社会に直面する我が国において、持続的な経済成長を実現するためには、これまで以上に ICT が果たすべき役割は重要なものになると考えられる。

しかしながらその一方で、ICT 利用の負の側面である情報セキュリティに関する問題や利用者における不安感が顕在化してきている。例えば、「社会基盤等におけるサービスの停止や機能低下等」、「我が国におけるサイバー犯罪の状況」、「情報漏えい」、「インターネット利用における不安感」及び「利用者のセキュリティ対策実施状況」については、以下のとおりである。

（社会基盤等におけるサービスの停止や機能低下等）

社会生活の基盤である重要インフラ（重要インフラは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用が不可能な状況に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものであり、「重要インフラの情報セキュリティ対策に係る行動計画」（2005 年 12 月、情報セキュリティ政策会議決定）においては、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、物流の 10 分野とされている。）における ICT

利活用が進展するにつれて、重要インフラにおけるIT障害が発生している状況となってきている。

海外での例としては、インターネットを介したシステムへの不正侵入により電力装置の動作が妨害され、実際に複数の都市で停電が引き起こされたことがあると2008年1月に米国において報道されている。そのほか、1999年にはガスパイプラインシステムが「トロイの木馬」を用いた犯行により、約24時間乗っ取られた事件や、2000年にオーストラリアにおいて、下水システムを操作して100万ガロンの下水をホテルや公園等にまき散らした事件、2003年1月に米国において、コンピュータウイルスにより原子力発電所の安全監視システムが約5時間にわたって停止した事件などが発生している。

我が国においても、2007年、IPネットワークの機能障害による長時間かつ広範囲にわたるIP電話の不通など電気通信サービスで度々IT障害が発生したほか、医療機関でのウイルス感染、地方自治体等でのホームページ改ざんによる不正プログラム混入などが発生し住民サービスに影響が生じている。

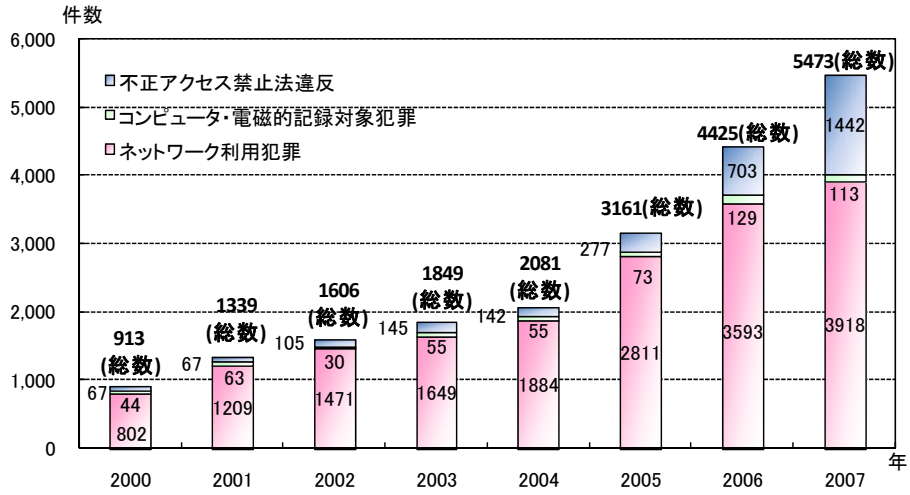
こうした継続するIT障害に関する問題に対して、政府では、「内閣官房情報セキュリティセンター」（NISC）や「情報セキュリティ政策会議」の設置、「第1次情報セキュリティ基本計画」や年度計画にあたる「セキュア・ジャパン」の策定等を行い、政府機関・地方公共団体、重要インフラ、企業、個人の主体毎に目標を定め施策に取組んでいる状況である。

（我が国におけるサイバー犯罪の状況）

我が国における2007年中のサイバー犯罪の検挙件数は5,473件となり、前年（4,425件）より23.7%の増加となっている。これは2003年から過去5年間で約3倍に達している状況である。このうち、不正アクセス禁止法違反は1,442件で前年の2.1倍に増加するとともに、児童買春及び青少年保護育成条例違反や著作権法違反などの増加によりネットワーク利用犯罪の件数（3,918件）も、前年比9.0%の増加となっている。また、2007年の主なサイバー犯罪検挙事例のひとつとして、中学生の被疑者がオンラインゲーム上のアイテムを収集する目的で、キーロガーをダウンロードさせて他人のユーザIDとパスワードを入手して同オンラインゲームを運営する会社のコンピュータに不正アクセス行為を行う事例が取り上げられており、コンピュータ犯罪の低年齢化の傾向がうかがえる。

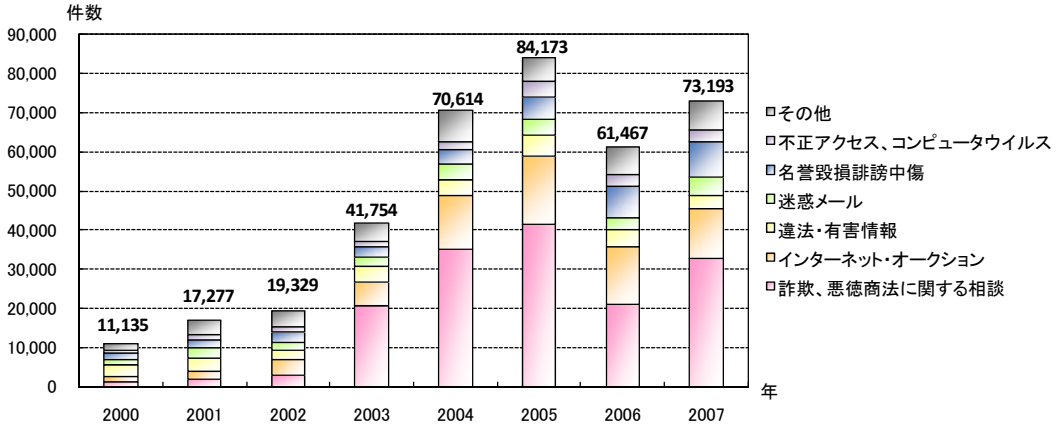
また、都道府県警察のサイバー犯罪相談窓口に寄せられたサイバー犯罪等に関する相談の受理件数は、前年（61,467件）比19.1%増の73,193件となっており、その中でも詐欺・悪質商法に関する相談及び迷惑メールに関する相談がそれぞれ前年度比で56.2%増及び58.5%増と急激な伸びを示している【図表2-15及び図表2-16参照】。なお、2005年から2006年の相談件数の減少は、Web上に開設されている「インターネット安全・安心相談システム」の活用が進んできていることによるもの

とされている。



出典：警察庁調べ（2008 年 2 月）

図表 2-15：サイバー犯罪の推移（検挙件数）



出典：警察庁調べ（2008 年 2 月）

図表 2-16：都道府県警における相談受理件数の推移

（情報漏えい）

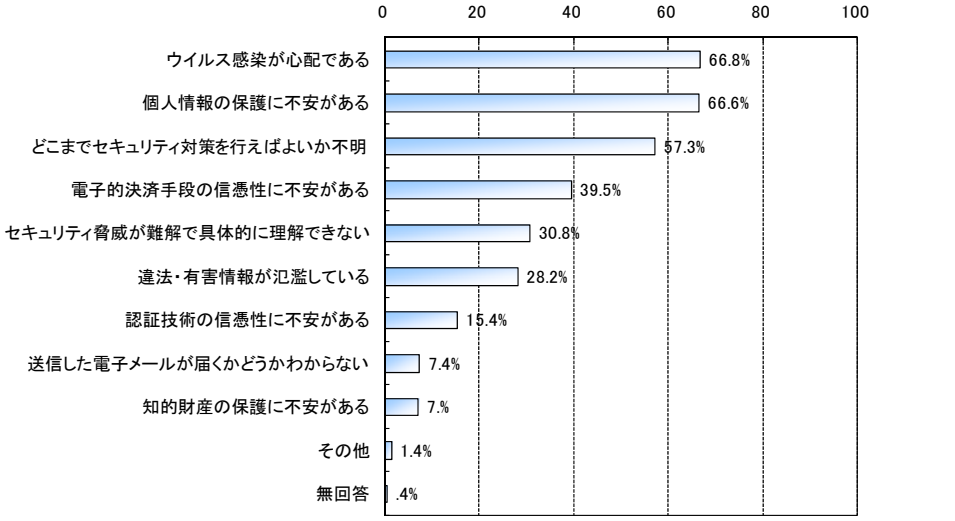
企業や官公庁における情報漏えいは、ここ数年来、継続して発生しており、2007 年 10 月に公表されている「2006 年 情報セキュリティインシデントに関する調査報告書 Ver.02.00」（NPO 日本ネットワークセキュリティ協会）によると、2006 年の個人情報漏えいの公表件数は 993 件となり、2005 年の 1,032 件と同規模の件数となっている。また、同年の情報漏えいの特徴としては、情報漏えいの対象となった人の数が、2005 年は約 880 万人であったのに対し、2006 年ではその 2.5 倍に相当する約 2,200 万人に増加し、1 件あたりの被害が大幅に増大していることを示している。

情報漏えいの原因としては、紛失・置忘れ（29.2%）、盗難（19.0%）、誤動作（14.7%）、

ワーム・ウイルス（12.2%）の順となっており、前年と同様の傾向を示しているが、特にワーム・ウイルスが原因とされる情報漏えいに関しては、前年が 1.1%であったのに対して急増している。これは、Winny や Share といった自動転送型ファイル共有ソフトを介して拡散する暴露型のウイルスによる個人情報漏えいによるものと分析されている。

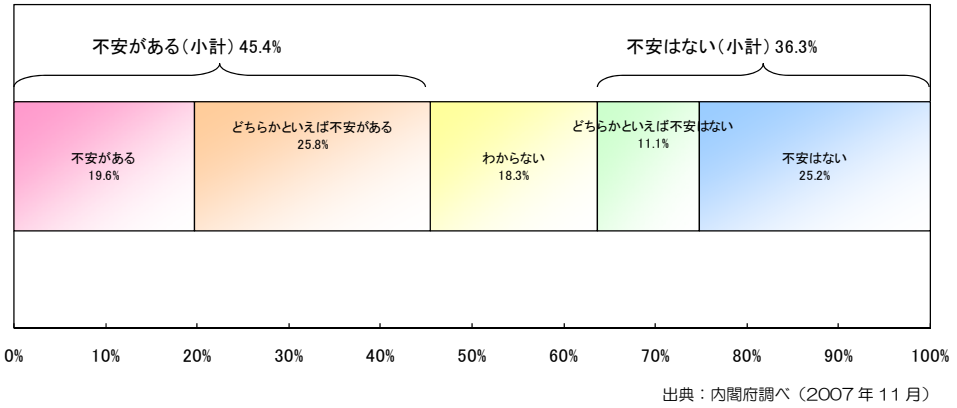
（インターネット利用における不安感）

2006 年末現在、インターネット利用世帯の４０%以上は、その利用に何らか不安を抱えている状況であり、その主たる要因としては、「ウイルスの感染が心配である」が 66.8%、「個人情報の保護に不安がある」（66.6%）、「どこまでセキュリティ対策を行えばよいか不明」（57.3%）の順となっている【図表 2-17 参照】。このインターネット利用に対する不安感については、内閣府が 2007 年 11 月に実施した調査においても 40%を超える結果となっており、依然として、不安感は解消されていない状況にあることを示しているといえる【図表 2-18 参照】。



出典：平成 18 年度通信利用動向調査（総務省）

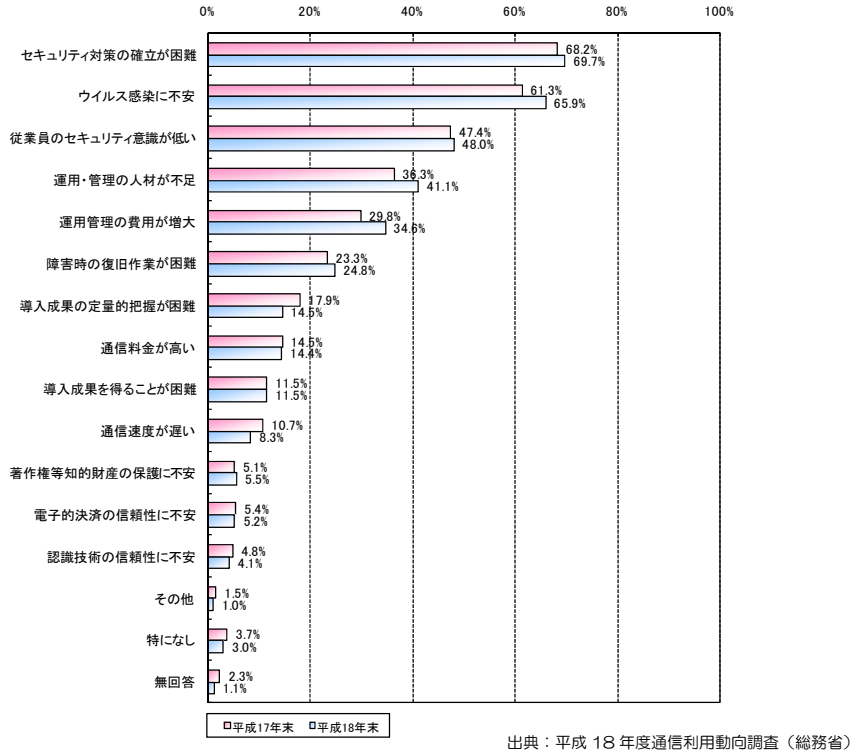
図表 2-17：インターネット利用で感じる不安の内容（世帯）（複数回答）



出典：内閣府調べ（2007 年 11 月）

図表 2-18：インターネット利用に対する不安感

また、2006 年末現在、企業における企業通信網、インターネットなどの情報通信ネットワークの利用上の問題点として、「セキュリティ対策の確立が困難」が 69.7%、次に「ウイルス感染に不安」が 65.9%と「セキュリティ関連」が上位を占め、「従業員の意識」、「運用・管理の人材が不足」など、人材面の問題を挙げる企業も多数ある状況となっている【図表 2-19 参照】。



出典：平成 18 年度通信利用動向調査（総務省）

図表 2-19：情報通信ネットワーク利用上の問題点（企業）（複数回答）

（利用者のセキュリティ対策実施状況）

最も基本的な情報セキュリティ対策のひとつであるパスワード管理の国際比較において、日本は、パスワードを頻繁に変更する利用者の割合が、わずか 13%に留まっており、調査を実施した 8 カ国中最下位となっている。日本以外の調査対象国においてパスワードを頻繁に変更すると回答した利用者の状況は、ブラジル 51%、中国 39%、オーストラリア 38%、イギリス 30%、ドイツ 25%、アメリカ 22%、フランス 21%となっている。

また、子供がインターネットで何をしているかを、親子でオープンに話す家庭の割合においても、日本は 22%と最下位となっており、他の調査対象国では、中国 71%、オーストラリア 59%、ブラジル 59%、フランス 54%、アメリカ 50%、ドイツ 45%、

イギリス 44%となっている。（出典：2008 年 2 月、シマンテック「ノートン・オンライン生活リポート」）

　こうしたデータから類推されるように、IT による生産性の向上や ICT 産業の国際競争力の強化が求められる中、利用者のインターネットをはじめとした ICT サービス利用における安心感や情報セキュリティに関連する被害が継続する状況となっており、我が国における基本的な情報セキュリティ対策は決して十分なものではなく、より一層の対策強化が必要であると考えられる。

３．情報セキュリティ対策の現状と課題

ICT が安心・安全に利用できる社会インフラとしてより一層の役割を果たすためには、現状における情報セキュリティ対策の課題を割り出すとともに、情報通信技術や利用スタイル等の変化により生じる可能性がある将来の情報セキュリティの問題について、検討することが必要である。

こうした観点から、本研究会では、今後の情報セキュリティ対策の検討にあたり、①現在の情報通信環境における脅威・課題、及びその対策状況を把握・整理することで、対策が不十分な項目や更に効果的な対策を講ずべき項目を洗い出す、②今後３年から５年における近い将来の情報通信環境及びその変遷過程における環境の変化を捉え、そこで発生する可能性が高い主な脅威・課題を抽出し整理する、という２つの時間軸に沿って、検討を進めてきている。

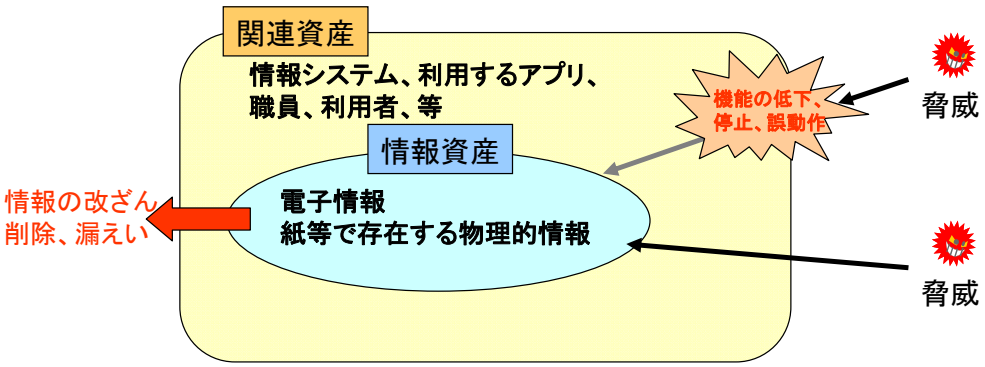
ここで、本章では、現在の情報通信環境における脅威・課題、及びその対策についての検討状況を述べることとする。

３－１　情報セキュリティ脅威の対象となる資産と主な情報セキュリティ脅威の分類

本研究会では、情報セキュティ脅威・課題及びその対策を検討するにあたり、その前提として、情報セキュリティ脅威の対象として守るべき資産と主な情報セキュリティ脅威の分類を以下のとおりとして検討を進めてきている。

（情報セキュリティ脅威の対象となる資産）

情報セキュリティ脅威の対象となる資産は、図表 3-1 に示すとおり、企業情報や個人情報といったデータそのものである「情報資産」、及びハードウェア資産、ソフトウェア資産、サービス資産、人的資産といった情報資産と関連する「関連資産」により構成される。



図表 3-1：情報セキュリティ脅威と情報資産

（主な情報セキュリティ脅威）

主な情報セキュリティ脅威は、図表 3-2 のとおり、以下の４分類としている。

ア）ボット等マルウェアによる脅威

（ワーム型感染のウイルスによる脅威）

イ）ソーシャルエンジニアリングを駆使した脅威

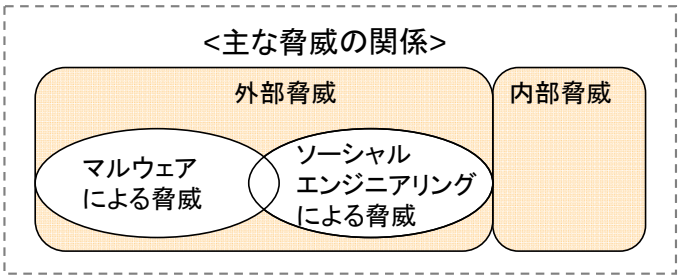
（フィッシング等、人間の行為、行動の弱点、盲点等をついてマルウェアに感染させたり、情報を盗み出す脅威）

ウ）外部脅威

（外部からの不正アクセス、自然災害等）

エ）内部脅威

（人為的ミス、意図的な犯行等）



図表 3-2：主な情報セキュリティ脅威の分類

	脅威の個別具体例（手法及び目的）	
ボット等マルウェアによる脅威	（手法） •ソフトウェアの脆弱性を攻撃（ワーム型感染） （目的） •ハードウェアクラッシュ •ソフトウェア改ざん・削除・誤動作 •サービス不能化攻撃	•情報の削除・改ざん・不正入手 •スパムメール発信 •フィッシングメール発信 •ウイルス感染メール発信　等
ソーシャルエンジニアリングを駆使した脅威	（手法） •なりすまし電話・メール、トラッシング スキミング •リバースソーシャルエンジニアリング （トロイの木馬等） •フィッシング（Web Spoofing）	•多段型Webマルウェア感染 •ターゲットアタック（高度ななりすまし） （目的） •不正に情報を入手 •マルウェアの感染
外部脅威	•地震等自然災害による機能停止等 •物理的攻撃による機能停止等 •脆弱性をついた不正侵入によるハードウェアクラッシュ、ソフトウェア改ざん・削除・誤動作等（Web改ざん等）	•ID、パスワードの不正利用による侵入（なりすまし）による情報の削除・改ざん・漏えい等 •盗聴 •盗難
内部脅威	•職員による設定・操作ミスによる機能低下・停止・誤動作 •職員による情報の削除・改ざん・漏えい（意図的・非意図的） •ハードウェア・ソフトウェアの不具合	•委託先管理不備による情報漏えい（セキュリティマネジメントの不備による） •盗聴、ショルダーサーフィン •盗難

図表 3-3：主な情報セキュリティ脅威の個別具体例

３－２　昨今の情報セキュリティ脅威の変遷

情報セキュリティ脅威としては、コンピュータをはじめとする情報システムが、社会活動に利活用され始めてからこれまでの間、ソフト・ハードの不具合、ウイルス感染や自然災害といった外部脅威、利用者側の人為的ミスや意図的な犯行等による情報の改ざん・消去・消滅といった内部脅威が、継続して存在している。その一方で、ICT利用の進展に伴い、守るべき情報資産の量、種類、質は常に変化してきており、さらに、コンピュータが相互に接続してネットワークを構成したことによってウイルスの感染経路がインターネット等ネットワークを介したものとなってきたことが大きな変化点であると捉えられる。このようにネットワークを介してもたらされる脅威は、遠隔でかつ広範囲に被害をもたらすことが可能であるため、その経済社会的影響の大きさを踏まえると、昨今の情報セキュリティ脅威の多くは、こうしたネットワークを通じてもたらされる脅威と捉えることが可能である。その脅威の変遷は以下のとおりである。

90 年代前半、コンピュータがスタンドアロンで利用されており、これらを標的にした、FD や CD-ROM といった外部記憶媒体で感染するシステム領域感染型ウイルスやファイル感染型ウイルスが横行していた。

90 年代後半から 2000 年代当初にかけては、利用環境が LAN からインターネットに発展していく過程であり、マクロ型ウイルスから Melissa や Love Letter に代表されるマスメーリング型のウイルスへ、さらには CodeRed、MS ブラスト等に代表されるソフトウェアの脆弱性をつく大規模感染型に変化してきた。これら大規模感染型ウイルスは、企業システム、一般ユーザのＰＣに広範囲に被害を及ぼすだけでなく、電気通信事業者のネットワーク設備自体の機能にも影響するものとして、その被害は報道等でも大きく取り上げられた。また、これらウイルスの感染目的は、一部で情報漏えいを引き起こすなど経済的利益を得ることを意図したものもあったが、その多くは攻撃者の興味本位や自己技術の誇示、愉快犯的な発想による無差別的な攻撃と分析されている。

これに対して、数年前からは、DoS・DDoS 攻撃（サービス停止攻撃・協調分散型 DoS 攻撃。大量のデータを送信することで、狙ったサーバ等を利用不能にする攻撃。）により特定の企業の ICT 機能を麻痺させることで当該企業に経済的損失を与えたり、多量のスパムメールを送信したり、スパイ行為により情報を盗み取ったりと、金銭的な利益の追求という明確な目的をもった脅威に変化してきている。その代表的なものがボットであり、2002 年にはじめて Agobot と呼ばれるボットが発見されて以来、現在のネットワーク上の脅威の殆どは、このボットに起因していると言われている。

また、近年のボット等により生じるネットワーク上の様々な情報セキュリティの脅威は、ウイルスを作製する者、それらを配布・感染させボットネットワークを構築す

る者、それを利用して多量のスパムメール送信／情報詐取をする者、その情報を売買する者等がそれぞれ分業・組織化されており、非合法なビジネスが成立していると言われている。こうした組織犯罪化がより問題を深刻化させていると考えられる。

さらに、最近の傾向としては、ウイルス感染の手法がより巧妙化・高度化してきており、特に、いわゆる脅威の潜行化（脅威が見えにくくなること）が進んできていると言われている。例えば、正規の Web サイトの脆弱性をついて事前に不正なコードを埋め込んでおき、利用者が通常利用するように感染した正規の Web サイトを閲覧するだけでウイルスに感染させる手法、または本当にウイルスに感染させたい相手を絞って、その相手が興味を持つような内容のメールにウイルス感染したファイルを添付して送り、そのファイルを開くことで感染させるといったソーシャルエンジニアリングを駆使した感染手法などが発生している。これらの感染手法はいずれも感染事実が見極め難く、対策が著しく遅延する状況を招いている。

	1980年代後半	90年代後半、2000年当初	最近の傾向
感染経路	FD,CD-ROM等の 外部記憶媒体を経由	ネットワーク経由 （メール、ダウンロード、ワーム型）	ネットワーク経由 Web感染、メール感染
対象	PC ミニコン	PC インターネットサーバ	PC、携帯電話、PDA、 情報家電 特定の個人・組織の情報
活動形態	PC等の不具合	PCの不具合、情報漏えい ネットワークの脅威 （DDos攻撃、スパム）	ネットワークを用いた脅威 情報漏えい 詐欺行為（フィッシング等）
目的	能力の誇示	能力の誇示、経済目的	経済目的 犯罪、スパイ行為
対策	個別での対応 CERT/CCの設立	電気通信事業者 ネットセキュリティ関連事業者	電気通信事業者 ネットセキュリティ関連事業者 各組織
備考	モーリスワーム、等	Happy99、Melissa、Loveletter CodeRed、SQLスラマー MSブラスト、Sadmind/IIS Worm、等	Botnet スピア型メール ターゲットアタック、等

図表 3-4：情報セキュリティ脅威（マルウェア）の変遷

３－３　情報セキュリティ脅威の現状及び今後の予測

前節の情報セキュリティの脅威の変遷に示すとおり、昨今の情報セキュリティ脅威としては、ボット等のマルウェアによる脅威、ソーシャルエンジニアリングを駆使した脅威が深刻な問題である。

また、これら現在発生している情報セキュリティ脅威の今後の傾向としては、これまでも脅威・攻撃の手口が次々と巧妙化してきたように、更に高度化された方法に変貌していくものと容易に考えられるうえ、次章で述べる情報通信環境の変化に伴って脅威の対象となる情報資産が質的・量的に爆発的に増加すると予想されることから、

より対策が困難な状況になるものと考えられる。

（ボット等マルウェアによる脅威の現状と今後の傾向）

ボットとは、コンピュータを悪用することを目的に作られた悪性プログラムで、ボットに感染したコンピュータはインターネットを通じて悪意を持った攻撃者に遠隔操作される。感染したコンピュータは、主として、コンピュータから情報の詐取、スパムメールの発信、フィッシング詐欺サイトの表示、DDoS 攻撃、ボットの感染拡大等の被害をもたらし、その種類は、亜種も含めて明確にボットと判明したものだけでも、23,868 件（2008 年 3 月 20 日現在、シマンテック定義による）あり、また、亜種の発生周期も短期化する傾向にあり、今日ではわずか数分で変異する場合もあると言われている。

国内でのボットの感染率は、2005 年（平成 17 年）時点で、ブロードバンドユーザーの２%から 2.5%にあたる（当時のブロードバンドユーザー数にして40 万から 50 万人）との試算もあり、こうした状況を受けて「サイバークリーンセンター」等の取組みを政府としても進めているところではあるが、今後もボットに感染したＰＣが遠隔で操られることによって発生する脅威に対する対策は、世界的にも継続的な課題になると考えられる。実際、世界で流通している全メールのうち約 80%がスパムメールであり(Symantec：2007 年 12 月調査)、そのほとんどがボットによるものとされている。しかも、そのスパムメール送信国は主にアメリカ(28.4%)、韓国(5.2%)、中国(4.9%)、ロシア(4.4%)と続いており(英ソフォス：2007 年 10 月調査)、日本国内の対処はもとより、諸外国との連携による抜本的な対策が必要となる課題である。

また、これまでのボットの感染手法は、ネットワークを利用するソフトウェアの脆弱性をつく、いわゆるワーム型の感染が主流であったが、現在では、ワープロや表計算ソフト等の脆弱性を利用したり、事前に Web サイトの脆弱性をついて正規の Web サイトに不正なコードを埋め込み、インターネット利用者がその不正コードが埋め込まれた正規の Web サイトにアクセスしただけでマルウェアに感染したり、或いはマルウェアの配布サイトに誘導させられたりする手法が確認されている。しかも、対価を得られるデータを盗み出すために最終的に感染させたいマルウェアをダウンロードするまでに、Web サイトのリダイレクトやダウンローダによる通信を複数回組み合わせ、対策者側の迅速な発見を巧妙に逃れる手段を講じている場合が発生してきている。

さらに、問題を悪化させる要因のひとつとして、複数の Web の脆弱性をついた攻撃を容易に実行できる攻撃ツールがネット上で販売されていることが挙げられ、こうしたツールを利用することで特段に詳しい知識がないものでも容易に攻撃が実施できてしまうような状況にまでなってきている。

加えて、我が国を限定的に狙ったマルウェアの開発が行われるようになってきていると言われているほか、例えば、ウイルス対策ソフトを感知して迂回を試みたり、ネットワーク上に設置した観測システムやマルウェア解析環境を感知して動作を停止した

り、本来の攻撃とは無関係または無意味な古い攻撃に置き換えて誤認させるものなど、対策側を混乱させ実態の把握を遅らせることを意図していると思われる方策を講じてきている状況である。

今後もこうした攻撃手法の巧妙化は短期間に繰り返し実行され、攻撃者側としては少ない労力で大きな効果を上げ、対策者側では多大な手間と費用を掛けなければならないような脅威へと変貌を遂げていくと予想される。

≪国内事例１≫

2006年１月に英国のカジノサイトが攻撃を受けて恐喝されていた事例が報道されたところであるが、我が国でも 2007 年 4 月、都内のある出版社に対して同様にボットによるDDoS攻撃が発生した。その概要は、攻撃対象となるWebサイトにDDos攻撃を仕掛けておき、技術料として指定の金額を払えば攻撃を回避できるという連絡をするというものであった。今回の事件では、セキュリティ対策事業者等の迅速な対応により、要求の金額を払うことなく、事件は収束した模様であるが、同社のサイトが利用できなくなったことにより経済的損失は少なくないと考えられる。

また、やり取りされたメールや電話は日本語であるほか、要求する金額も著しく高額な値ではなく、数十万程度であった模様であり、攻撃の地域化、及び被害者が一先ずの回避策として支払いを応じてしまいそうな額に抑えるなどといった攻撃の巧妙化が伺える。

≪海外事例１≫

海外におけるボット対策の取組事例として、米国において連邦捜査局（FBI）及び司法省（DOJ）が、メーカー、ISP、CERT/CC 等と共同で実施しているプロジェクトである「OPERATION BOT ROAST（ボット撲滅プロジェクト）」が挙げられる。本プロジェクトは、ボットネットワークの所有者の特定及び逮捕、ネットワークを制御するサーバ（コマンドコントロール（C&C）サーバ）の解体を通じたボットネットワークの撲滅を目指しているとされる。

本プロジェクトの成果として、2007 年 11 月までに、①100 万台を超えるボット感染 PC を特定、②ハーダーと呼ばれるボットネットを悪用する人物やボットの感染活動を行った人物等８名を起訴、③ニュージーランドにおける当局と連携して、ボットネットを構築した人物の身柄を拘束する、等の実績が報告されている。

≪海外事例２≫

カナダ･ケベック州警察が、2008 年２月 20 日、最大で 100 カ国以上に及ぶ 100 万台の PC で構成されるボットネットを運用していた未成年者３名を含む 17 人を逮捕したと報道されている。また、その被害額は最大で 4,500 万カナダドルに及ぶものとされている。

≪海外事例３≫

2007 年 4 月後半から 3 週間にわたり、エストニアの大統領府、政府機関、著名な銀行や新聞社が DDoS 攻撃を受けてサイトが停止したほか、一時は携帯電話網や救急ネットワークも被害を受けたと報じられている。なお、この DDoS 攻撃は、複数のボットネットを用いたものとの分析もある。また、この攻撃で見られた複雑さや連携はこれまでに無いもので、様々な技法を用いて念入りにタイミングを選び、特定の標的を狙った攻撃であったと言われている。その他、エストニアは世界でも最もデジタル化、ネットワーク化が進んでいる国の 1 つと言われているが、現地を視察した NATO の専門家は、これがもし他の国だったら「もっとひどいことになっただろう」とコメントしている模様である。

≪海外事例４≫

ボット感染の被害が大きく拡大している事例として、世界最大級のメール送信ボットネットを構築している「Storm Worm」が挙げられる。Storm Worm は、最新の時事ニュースに関連した情報に誘導すると見せかけたり、家族からのポストカードに見せかけるなど、巧妙なソーシャルエンジニアリングの手口により、2007 年 1 月から短期間でその感染が世界中に拡散し、その後もユーザの興味を引く様々な手法を用いて、感染活動を継続しているとされている。

Storm Worm に感染した端末は、1 分間に平均 3,500 通ものスパムメールの大量送信を行い（2007 年 1 月 22 日付シマンテック報道）、また、2008 年の 1 月に「Storm Worm」によって送信されたスパムメールは、ピーク時において全世界のメールトラフィック全体の 16%にも及んだと報告されている。（2008 年 1 月 30 日付 Sophos 報道）

加えて、Storm Worm によるスパムメールの送信は、株価を操作することによって不正に金銭的な利益を得る目的にも利用されているとの指摘がされている。（2007 年 1 月 22 日付シマンテック報道）

こうした Storm Worm の特徴のひとつとして、構築されたボットネットの管理方法に P2P を利用している点が挙げられ、ボットネットを集中管理するサーバが存在しないことから、その活動を停止されることが難しいとされている。そのほか、ピア間のやり取りを暗号化しているばかりか、暗号鍵も絶えず変更されるとともに、30 分毎にバイナリを変更して変形していくため、ウイルス対策ソフトのウイルス定義情報では検知しづらい状況になっているとされている。

≪海外事例５≫

正規の Web サイトに不正なコードを埋め込み、マルウェアの配布サイトに誘導させる手法の実例としては、「MPack」、「IcePack」が挙げられる。これらは、Web サイトの複数の脆弱性を悪用する機能を格納した攻撃ツールとして数百ドルにてネット上で販売されており、こうしたツールを利用することで特段に詳しい知識がないもの

でも容易に攻撃が実施できる状況となってきたと言われている。
2007 年、イタリアでは 3000 以上のサイト、トルコでは 4 万以上のサイトに不正なスクリプトが埋め込まれたと報告されており、我が国でも複数の企業が同様の攻撃を受け、その中には数日間サービスを停止したケースもあるとの被害報告もされている。また、海外では、在外公館の公式サイトなどの政府系サイトや、国連など国際機関のサイトにも被害が及んだ模様である。

（ソーシャルエンジニアリングを駆使した脅威）
ソーシャルエンジニアリングの手法としては、金融機関などを装って電子メールを送り、住所、氏名、口座番号、クレジットカード番号などを詐取するフィッシングが世界的に大きな被害をもたらしている。
従来型のこうしたフィッシングに加え、昨今では、ソーシャルエンジニアリングを駆使した巧妙な手口として、スピア型メール（標的型メール）が挙げられる。これは、一見すると不審なメールに見えないように標的となった企業や組織毎に、実際に取引等がある関係者等からの情報に見せかけるように送信者情報が偽装されていたり、企業や組織が興味を引くような文面にカスタマイズされており、こうしたメールに添付されたファイルを誤って開封してしまうと、ウイルスに感染したりするものである。こうしたメールは不特定多数に大量に配信されることがなくネットワーク設備への影響もないことから気付かれ難く、さらに標的用にカスタマイズされたウイルスやスパイウエアが利用されることもあることから、通常のウイルス対策ソフトでは対処できないなど、発見が遅れ対策が後手に回るケースが多くなっていると言われている。
今後も企業情報・個人情報等を不正に取得するための手段として、特定の者に対してカスタム化したソーシャルエンジニアリングを駆使した脅威は、より巧妙化していくと考えられる。

≪国内事例１≫
フィッシング対策協議会４半期レポート（2007 年 10-12 月期）によると、2007 年 12 月に、同協議会に報告されているフィッシング情報は 26 件あり、4 ヶ月間上昇している。事案としては、これまでの銀行に関連するものの他、国内の大手オークションサイトを対象としたフィッシングメールが短期間で大量に配布されたケースや、銀行系以外の有名企業の関連企業を装うケースが登場してきていると報告されている。また、日本の大学や地方公共団体のサイトに英語のフィッシングサイトが作成された事例があることも報告されるなど、依然としてフィッシングの脅威は継続して発生している状況である。

≪国内事例２≫
ソーシャルエンジニアリングを駆使したスピア型メールの事例として、2007 年９

月の就任直後に総理大臣を騙ったメールが確認されたとの報道がなされたほか、これまでも、著名な政治家を騙った不審なメールが出回り、受信者が添付されたファイルを開くことでウイルスに感染してしまうというケースがいくつか報告されている。また、政府機関を騙り、関係企業において限定的に不審なメールが出回ったケースもあり、この場合は報道発表に関連する追加情報を添付しているとみせかけて、ウイルスに感染したファイルを添付したメールが送付されたものであったことが報告されている。

≪海外事例１≫

2007 年上半期において、世界に流通したフィッシングメールの総数は、前期に比べて約 18%の増加となっている（2007 年９月、「シマンテック インターネットセキュリティ脅威レポート」）。また、フィッシングサイトのうち最多の 59%が米国にホスティングしており、次いで、ドイツ（6%）、イギリス（3%）、日本は第８位（２%）となっている。この原因として、米国は Web ホスティングプロバイダが多く存在しているため、このような結果となっていると考えられている【図表 3-5 参照】。また、フィッシングサイトの内訳としては、金融機関を装ったものが 72%と最大で、金銭的な利益を獲得できるデータが直接的な標的となっていることが読み取れる。

さらにこういったフィッシング攻撃を助長する背景として、正規の Web サイトになりすまして自動的にフィッシング Web サイトを作成する複数のツールキットの存在がある。これらのツールキットは闇市場で取引され、フィッシングメールを自動的に作成・送付する機能も備えていると言われている。また、これらツールキットのうち、最も広く使用されている上位３位のツールキットにより作成されたフィッシング Web サイトは、全体の 42%に及ぶとの調査結果も報告されている（2007 年９月、「シマンテック インターネットセキュリティ脅威レポート」）。

ランク	前期ランク	国名	今期の割合	前期の割合
1	1	米国	59%	46%
2	2	ドイツ	6%	11%
3	3	英国	3%	3%
4	10	オランダ	2%	2%
5	11	ロシア	2%	2%
6	4	フランス	2%	3%
7	7	カナダ	2%	2%
8	5	日本	2%	3%
9	8	中国	1%	2%
10	6	台湾	1%	3%

出典：シマンテック社調べ（2007 年９月）

図表 3-5：フィッシング Web サイト設置数の上位国

≪海外事例２≫

2008 年 1 月、米国において、スパイウエア駆除ツールに見せかけてウイルスをインストールさせようとする悪質サイトが報告された。報告されたサイトには、スパイウエア駆除ツールなどに関するブログやニュース、製品情報などが掲載されており、ツールのレビュー記事なども満載されている模様である。また、ページは定期的に更新されていて、一見、正当な Web サイトに見えるなど、ウイルス感染の手口の巧妙化が進んでいることを示している。

そのほか、現状生じている問題として、Winny 等の自動転送型ファイル共有ソフトを利用したウイルスの拡散等が挙げられる。

2007 年 1 月、Winny で流通するファイルについて無作為に調査した結果、調査時に流通していたファイル全体のうち約 4.5%にマルウェアが含まれているとの結果が出ている。検出されたマルウェアの多くは、.lzh や.zip などの圧縮フォルダの中に複数のファイルと一緒に同梱され、さらに取得したマルウェアの約 95.5%は音楽ファイル等のファイルアイコンに偽装されていた。このように目視での安全性確認が困難であるため、.lzh などの圧縮フォルダの大半にはマルウェアが含まれているという前提で情報セキュリティ対策が必要である。今後も P2P 等の管理者不在のオーバーレイ・ネットワークがウイルス配布・感染の手段としても利用されることが強く懸念される。

３－４　情報セキュリティ対策の取組み状況と課題

前節までに示すように、様々な情報セキュリティ脅威が発生しており、特にネットワークを通じて発生する脅威の巧妙化・高度化が大きな問題となっている現状において、どういった主体がどのような対策を講じて、情報セキュリティの確保に努めているか、先に提示した４つの情報セキュリティ脅威に沿って、対策実施主体毎に、その対策及び実施における課題等を取りまとめた。
なお、対策実施主体は、次に示す７つに分類している。

（主な情報セキュリティ対策実施主体の分類）

ａ.利用者（個人）
ｂ.利用者（企業等）
ｃ.情報セキュリティ関連事業者（ＡＶＶ、情報セキュリティソリューション提供事業者等）
ｄ.電気通信事業者（ＩＳＰ、アクセス系、携帯電話系、無線通信系）
ｅ.ＯＳ/アプリケーション/サービス提供事業者
ｆ.機器開発事業者
ｇ.政府機関

ア．ボット等マルウェア感染による脅威への取組み状況

ボット等マルウェアによる脅威に対する取組							
その他	・ニュースなど一般情報源からの情報収集 ・ITリテラシーの取得	・運用ポリシーの設定 ・監査の実施 ・ニュースなどからの情報収集 ・社内教育 ・各種認証制度の取得	・教育の提供 ・アラートレポート ・アラートサービス	・運用の高度化 ・啓発活動 ・アラートレポート ・アラートサービス ・abuse対応 ・サポート	・啓発活動 ・アラートレポート ・アラートサービス		・啓発活動 ・関連法整備（企業） ・ガイドラインの制定等、運用の高度化支援（企業） ・情報セキュリティ対策の普及啓発
アプリケーション/ サービス	・パーソナルFWの導入 ・ウイルス対策ソフトの適用 ・ウイルス対策サービスの利用	・パーソナルFWの導入 ・ウイルス対策ソフトの適用 ・ウイルス対策サービスの利用 ・ネットワーク監視サービスの利用	・ウイルス対策ソフトの提供 ・企業ネットワーク監視サービスの提供 ・脆弱性対応	・ウイルス対策サービスの提供 ・ネットワーク監視サービス提供（企業） ・安全なWebサーバなどの提供	・脆弱性対応（パッチ作成・提供等）		・情報セキュリティ対策の普及啓発 ・各種調査実施
ＯＳ/ ミドルウェア	・バージョンアップ、パッチの適用	・バージョンアップ、パッチの適用	・ウイルス対策製品の提供		・脆弱性対応（パッチ作成・提供等）	・脆弱性対応（パッチ作成・提供等）	・情報セキュリティ対策の普及啓発 ・税制優遇（企業） ・各種調査実施
端末（ｴｯｼﾞｼｽﾃﾑ含む）／ ホーム（企業） ネットワーク	・BBルータの導入 ・認証の適用 ・バックアップ、冗長化	・認証の適用 ・バックアップ、冗長化 ・ネットワークFW、IDS、IPS等対策機器の導入 ・運用 ・FW、IDS運用サービスの利用 ・サーバセキュリティ製品の導入 ・パッチの適用	・ウイルス対策製品の提供 ・FW、IDS等対策装置の提供 ・FW、IDS運用サービス提供（企業） ・企業ネットワーク監視サービスの提供	・FW、IDS運用サービス提供（企業） ・BBルータのファームウェア管理サービスの提供（個人） ・企業ネットワーク監視サービスの提供		・組み込みシステムの脆弱性対応 ・脆弱性対応（パッチ作成・提供等）	・税制優遇（企業） ・各種調査実施
ネットワーク（ インターネット ／公衆網）				・ネットワーク設備の運用・維持管理、緊急対応、事業者連携 ・ネットワーク監視 ・ＶＰＮ、専用線の提供 ・(不必要な通信の除去)			・ガイドラインの制定等、運用の高度化支援（企業）
要素技術			・収集技術 ・解析技術 ・検知技術 ・駆除技術	・ネットワーク設備 ・通信上の異常検出 ・フィルタ ・帯域制御	・設計段階からのセキュリティ対策 ・脆弱性の検出	・設計段階からのセキュリティ対策 ・脆弱性への対応	・研究開発の推進 ・関連団体による収集、解析、検知、駆除技術
	利用者（個人）	利用者（企業等）	情報セキュリティ関連事業者（ＡＶＶ、情報セキュリティソリューション提供事業者等）	電気通信事業者（ＩＳＰ、アクセス系、携帯電話系、無線通信系）	ＯＳ/アプリケーション/サービス提供事業者（ウエブサイト運営者、ASP・SaaS等を含む）	機器開発事業者	政府機関

図表 3-6：主な対策実施主体の取組み（ボット等マルウェア感染による脅威）

ボット等マルウェア感染による脅威に関する対策は、利用者（個人）によるウイルス対策ソフトの適用やブロードバンドルータの導入、利用者（企業）による IDS 等の情報セキュリティ対策装置の導入など、利用者（個人）及び利用者（企業）による対策が主として行われている。電気通信事業者においては電気通信設備への対策等も行われている他、ウイルス対策サービスの提供やＶＰＮや専用線の提供等も行われている。引き続き、脅威の変化や高度化を踏まえ、各対策実施主体において適切な対策を講じていくことが重要であると考えられる。

特に、ウイルス対策ソフトの適用、OS・アプリケーションソフトウェア等を最新の状態にアップデートすること、ブロードバンドルータの導入、無線 LAN 等を利用する際のセキュリティ対策等、インターネット利用者が行う際の基本的な情報セキュリティ対策の徹底を図るための普及・啓発が必要であるとの指摘がある。

ボット対策については、総務省と経済産業省は、2006 年 12 月から両省の連携プロジェクトとして「サイバークリーンセンター（www.ccc.go.jp）」を立ち上げ、Telecom ISAC Japan、複数の ISP、JPCERT コーディネーションセンター、IPA（独立行政法人 情報処理推進機構）と協力しながら、ボットウイルスに感染したインターネット利用者への注意喚起や駆除ツールの提供を行っているほか、ウイルスの感染防止策等について周知・啓発活動を実施している。本プロジェクトはボットに感染

したインターネットの利用者に対して直接駆除を促すもので、攻撃者や制御サーバである C&C サーバを特定することを目的とした他国の取組みとは異なるものであり、世界的にも独自な官民連携プロジェクトによる具体的な対策事例として一定の評価を受けているが、我が国におけるボット感染者を減らすため、また前述に示した利用者が行う情報セキュリティ対策の徹底を図るため、更に活動を充実すべきであると指摘されている。

また、インターネット利用者が誤ってウイルス等に感染してしまった場合などには、独自に説明書を用いて解決しようにも技術用語等が難しすぎて理解できないことがあるほか、いったいどこに問い合わせて良いかも分からないことが多くあるとされている。こうした場合に対応するため、身近にかつ簡単に相談等ができ、迅速な復旧が可能となるような取組みが、今後より一層重要になると指摘がある。

一方、現状の対策は、脆弱箇所の修正やウイルス対策ソフトの定義情報のアップデートなどによる受動的な対策に頼らざるを得ない状況となっており、マルウェア等による不正な通信（やスパムメール等による不要な通信）を減少させる或いは停止する、又は不正な Web サイトへのアクセスを制限する或いは禁止するといった能動的な対策が実施できるような環境とはなっていないことが課題であり、こうした不要な通信の流通量の増大が電気通信事業者の設備の維持・運用にも大きく影響を及ぼしているとの指摘もある。

さらに、マルウェアの作成そのものについて、ネットワーク上を流通するウイルス等が蔓延している状況や、これにより多くの被害等が生じている状況を改善するため、サイバー犯罪条約に基づく、いわゆるウイルス作成罪の制定が強く望まれている。さらに、ボット等マルウェア感染による脅威に関する対策等について、海外との連携対応が十分ではないとの意見もある。

イ．ソーシャルエンジニアリングを駆使した脅威への取組み状況

ソーシャルエンジニアリングを駆使した脅威　に対する取組							
その他	・知人等の啓発	・従業員等の啓発	・利用者の啓発	・利用者の啓発	・利用者啓発	・利用者啓発	・法執行機関による摘発強化 ・法律面、制度面からの、対策の促進 ・海外との連携の支援 ・利用者啓発
アプリケーション/サービス	・ウイルス/フィッシング/スパム対策ソフト・サービスの利用 ・パーソナルＦＷの導入 ・URLフィルタリングサービスの利用 ・バージョンアップ、パッチの適用	・ウイルス/フィッシング/スパム対策ソフト・サービスの利用 ・パーソナルＦＷの導入 ・URLフィルタリングサービスの利用 ・バージョンアップ、パッチの適用、サービスの導入	・脆弱性対応 ・ウイルス/フィッシング/スパム対策ソフトの提供 ・パーソナルＦＷソフトの提供 ・MSSの提供 ・バージョンアップ、パッチサービスの提供	・ウイルス/フィッシング/スパム対策サービスの提供 ・パーソナルＦＷサービスの提供 ・バージョンアップ、パッチサービスの提供 ・SPF/Sender ID（送信元アドレス偽装防止技術）の提供・利用	・対ソーシャルエンジニアリング的な機能の提供 ・安全な利用者認証の仕組みを提供(SSOなど) ・個人証明書の提供 ・SPF/Sender ID（送信元アドレス偽装防止技術）/証明書等の扱いに適したアプリケーションの提供 ・利用者に危険をもたらすサイトの警告・非表示		・アプリケーションの普及啓発 ・情報セキュリティ対策の普及啓発・促進（法律面、制度面）
ＯＳ/ミドルウェア	・バージョンアップ、パッチの適用 ・セキュリティの強いシステムの利用	・バージョンアップ、パッチの適用	・バージョンアップ、パッチサービスの提供		・脆弱性対応 ・安全な利用・設定等の情報提供 ・保護/防止機能の提供		
端末（ｴｯｼﾞｼｽﾃﾑ含む）／ホーム（企業）ネットワーク	・端末認証・個人認証の適用 ・ルータ(FW)等の利用	・端末認証・個人認証の適用			・サーバー証明書(EVSSL)の利用	・脆弱性対応 ・安全な利用・設定等の情報提供 ・保護/防止機能の提供	
ネットワーク（インターネット／公衆網）	・ネットワーク上で違法有害情報フィルタリングを提供するISPの選択	・Proxyによる違法有害情報フィルタリング	・スパムフィルタの提供 ・利用者に危険をもたらすサイト等の情報共有	・DNSを利用したフィッシングサイト等の警告システム提供 ・利用者に危険をもたらすサイトの警告・非表示 ・送信元詐称や攻撃通信の排除	・ネットワーク上でのセキュリティサービス提供 ・利用者に危険をもたらすサイト等の情報共有		・ネットワーク上での対策の支援 ・海外との対策・法的措置の支援
要素技術			**・ウイルス/フィッシング/スパム対策技術 ・パーソナルＦＷ ・URLフィルタリング ・バージョンアップ/パッチ適用技術**	**・ウイルス/フィッシング/スパム対策技術 ・パーソナルＦＷ ・URLフィルタリング ・通信の遮断・排除 ・個人認証・端末認証 ・Sender ID/SPF（送信元アドレス偽装防止技術）**	**・サーバー証明書(EVSSL) ・利用者認証（SSO） ・脆弱性対策 ・情報共有 ・Sender ID/SPF（送信元アドレス偽装防止技術）**	**脆弱性**	
	利用者（個人）	利用者（企業等）	情報セキュリティ関連事業者（ＡＶＶ、情報セキュリティソリューション提供事業者等）	電気通信事業者（ＩＳＰ、アクセス系、携帯電話系、無線通信系）	ＯＳ/アプリケーション/サービス提供事業者（ウエブサイト運営者、ASP・SaaS等を含む）	機器開発事業者	政府機関

図表 3-7：主な対策実施主体の取組み（ソーシャルエンジニアリングを駆使した脅威）

ネットワークを利用するソーシャルエンジニアリングを駆使した脅威については、マルウェア感染による脅威と同様、利用者（個人）及び利用者（企業）による対策が主となっている。特に、ソーシャルエンジニアリングを駆使した脅威は、利用者が安易にクリックしたり、個人情報を書き込んだりしないようにするといった情報セキュリティに関する個人の基本的なリテラシーに依存するところが大きいことから、利用者への啓発が重要な対策となっている。

しかしながら、特定の企業や組織を標的にしたスピア型メールのように、脅威は非常に小規模化、潜行化、巧妙化してきており、これらに対抗するための抜本的な対策を講じることが出来ていないとの指摘がある。

また、これらの脅威は局所化し、企業や業界を越えた大規模な障害が発生しないことから、組織間の情報共有や対策の連携が進まず、日々高度化する脅威に対して迅速な対策が取れなくなるのではないかと危惧する指摘もある。

ウ．外部脅威への取組み状況

エ．内部脅威への取組み状況

外部脅威（A：全般　B：不正アクセス　C：自然災害）に対する取組							
その他		・BCPの策定（A） ・運用ポリシーの策定 ・監査の実施 ・データセンターの利用 ・組織内CSIRT設置 ・ISMS（取得） ・セキュリティ啓発(受ける側)	・注意喚起/AlertCon ・ISMS(取得支援) ・セキュリティコンサルティング ・ハニーポットによる脅威分析 ・ネットワークの脆弱性診断	・(通信サービスに関する)CSIRT設置 ・事業者連携 協調の枠組 ・サイバー攻撃対応演習	・データセンター設備提供	・(製品に関する)CSIRT設置	・ガイドラインの作成等、対策の普及啓発（A） ・CEPTOAR-Council(設置検討の支援) ・情報セキュリティ啓発 ・国際協調の枠組み作り ・情報セキュリティに関する法律
アプリケーション/サービス	・Personal Firewallアプリケーションの導入（B） ・バージョンアップ、パッチの適用（B） ・データバックアップソフト/サービスの適用（A）	・バージョンアップ、パッチの適用（B） ・企業ネットワーク監視サービスの適用（B） ・認証サービスの適用 ・データバックアップソフト/サービスの適用 ・ウィルス・スパム対策等ソフト・サービスの利用	・企業ネットワーク監視サービスの提供（B） ・脆弱性対応（B） ・脆弱性情報の提供 ・認証サービスの提供 ・コードレビュー ・Web脆弱性診断 ・PKIサービスの提供 ・ウイルス対策ソフトの提供	・データバックアップソフト/サービスの適用（A） ・ウィルス・スパム対策等サービスの提供	・データバックアップソフト/サービスの提供（A） ・FW/IDS/IPS等セキュリティソリューション(開発・提供) ・脆弱性対応（B） ・認証サービスの提供（B） ・ペネトレーションテスト	・FW/IDS/IPS等セキュリティソリューション(開発・提供) ・脆弱性対応	・情報セキュリティ対策の普及啓発（B） ・対策導入支援(税制)（C）
ＯＳ/ミドルウェア	・Personal Firewall機能付きOSの導入（B） ・バージョンアップ、パッチの適用（B） ・データのバックアップ（A）	・バージョンアップ、パッチの適用（B） ・データのバックアップ（A） ・ハードディスク暗号化			・Personal Firewall機能付きOSの提供（B） ・脆弱性対応	・脆弱性対応	・情報セキュリティ対策の普及啓発（B） ・対策導入支援(税制)（C）
端末（ｴｯｼﾞｼｽﾃﾑ含む）／ホーム（企業）ネットワーク		・ネットワークFW、IDS、IPS等対策機器の導入 ・VPN装置の導入（B） ・認証の実施（B） ・UPSの適用（C） ・システムの二重化	・ネットワークFW、IDS、IPS等対策機器の提供 ・FW、IDS運用サービス提供			・認証サーバの提供（B） ・脆弱性対応（B） ・UPSの提供（C） ・生体認証端末(指紋認証携帯電話機等)	・情報セキュリティ対策の普及啓発（B） ・対策導入支援(税制)（C）
ネットワーク（インターネット／公衆網）		・VPN・専用線サービスの導入（B）		・ネットワーク設備の運用・維持管理、緊急対応、事業者連携(A) ・ネットワーク監視サービスの提供（B） ・VPN・専用線サービスの提供（B）			・運用の高度化支援（B）
要素技術			**・解析・対策技術の高度化（B） ・CVE（脆弱性識別番号）**	**・ネットワーク設備（A）**	**・設計段階からのセキュリティ・故障対策（A） ・CVE（脆弱性識別番号） ・脆弱性自動パッチサービス**	**・設計段階からのセキュリティ・故障対策（A） ・CVE（脆弱性識別番号） ・DPI ・ハードウエアベース暗号方式(量子暗号等)**	**・研究開発の推進（A）**
	利用者（個人）	利用者（企業等）	情報セキュリティ関連事業者（ＡＶＶ、情報セキュリティソリューション提供事業者等）	電気通信事業者（ＩＳＰ、アクセス系、携帯電話系、無線通信系）	ＯＳ/アプリケーション/サービス提供事業者（ウエブサイト運営者、ASP・SaaS等を含む）	機器開発事業者	政府機関

図表 3-8：主な対策実施主体の取組み（外部脅威）

内部脅威（人為的ミス、意図的な犯行等）に対する取組							
その他	・Ｐ２Ｐアプリケーション等の利用の自粛 ・個人向け情報セキュリティに関する啓発	・運用ポリシーの設定 ・監査、教育、運用の実施 ・データ保護（バックアップ）、現物保管、散逸防止 ・入退出管理、映像監視 ・セキュリティポリシーの策定 ・セキュリティマネジメントの確立 ・各種認証制度の取得 ・委託業者との適切な契約		・運用の高度化 ・インシデント・故障対応演習 ・機械操作・保守訓練 ・ヒューマンエラー抑止に関する技術導入（組織マネジメント、MMI）	・サーバ証明書の取得	・暗号モジュールの提供 ・放出電磁波による情報漏洩に対する対策	・法令の整備 ・情報システム運用等に関するガイドラインの作成等、運用の高度化支援 ・情報セキュリティ対策の普及啓発 （セキュアなシステム開発運用フレームワーク）
アプリケーション/サービス	・ウイルス対策ソフトの適用、サービスの導入 ・バージョンアップ、パッチの適用 ・パーソナルFWの適用	・ウイルス対策ソフトの適用、サービスの導入 ・バージョンアップ、パッチの適用 ・目的外利用対策 ・企業内情報管理ソリューションの採用 ・Ｐ２Ｐアプリケーション利用対策	・脆弱性対応 ・ウイルス対策ソフトの提供 ・企業ネットワーク監視サービスの提供 ・ログ管理ソリューションの提供 ・Ｐ２Ｐアプリケーション検知ソフトウェアの提供 ・ソリューションの提供	・ウイルス対策サービスの提供 ・ログ管理サービスの提供 ・誤操作防止インターフェースの導入	・脆弱性対応 ・アプリケーションによる不正検知 ・企業内情報管理ソリューションの提供 ・Ｐ２Ｐアプリケーション利用監視サービスの提供	・ハード化装置の提供 ・企業内情報管理ソリューションの提供	・情報セキュリティ対策の普及啓発
ＯＳ/ミドルウェア	・バージョンアップ、パッチの適用	・バージョンアップ、パッチの適用 ・安全なOS/ミドルウェアの選択			・脆弱性対応 ・ロバスト化（要塞化・ハード化）	・ハード化装置の提供	・情報セキュリティ対策の普及啓発
端末（ｴｯｼﾞｼｽﾃﾑ含む）／ホーム（企業）ネットワーク	・認証の適用 ・バックアップ・冗長化 ・セキュアクライアント（モバイル含む）	・認証の適用 ・FW、IDS等対策機器の導入 ・企業ネットワーク監視サービスの適用 ・バックアップ・冗長化 ・アクセス制御（認証・識別の適用　等） ・暗号化による管理 ・シンクライアント化 ・セキュアクライアント（モバイル含む） ・ネットワークの物理的隔離	・FW、IDS等対策装置の提供 ・VPN装置の提供 ・企業ネットワーク監視サービスの提供	・電波漏洩対策 ・企業ネットワーク監視サービスの提供	・利用者認証 Webアクセス認証 ・利用者情報ディレクトリ ・操作監視・持出制御	・組み込みシステムの脆弱性対応 ・情報漏えい防止アプライアンスの提供 ・シンクライアントシステムの提供 ・暗号化機器の提供 ・画面遮蔽フィルター	・情報セキュリティ対策の普及啓発
ネットワーク（インターネット／公衆網）	・認証の適用 ・バックアップ・冗長化	・認証の適用 ・バックアップ・冗長化		・ネットワーク設備の運用・維持管理、緊急対応、事業者連携 ・ネットワーク監視 ・ＶＰＮ、専用線の提供 ・Ｐ２Ｐ暴露ウイルス感染者への対策注意喚起 ・検疫ネットワークサービスの提供	・ネットワークの分離（セキュリティドメイン）		・ガイドラインの作成・支援 ・運用の高度化支援
要素技術			**・解析・対策技術の高度化 ・暗号、認証 ・電子透かし**	**・ネットワーク設備 ・データ秘匿（暗号化） ・無線ＬＡＮセキュリティ ・携帯電話セキュリティ**	**・設計段階からのセキュリティ対策 ・不正利用防止**	**・設計段階からのセキュリティ対策 ・耐タンパ、暗号アルゴリズム、高速実装 ・TEMPEST技術研究開発 ・利用者認証、機器アクセス制御 ・本人認証、電子証明書、電子署名**	**・情報漏えい対策の研究開発**
	利用者（個人）	利用者（企業等）	情報セキュリティ関連事業者（ＡＶＶ、情報セキュリティソリューション提供事業者等）	電気通信事業者（ＩＳＰ、アクセス系、携帯電話系、無線通信系）	ＯＳ/アプリケーション/サービス提供事業者（ウエブサイト運営者、ASP・SaaS等を含む）	機器開発事業者	政府機関

図表 3-9：主な対策実施主体の取組み（内部脅威）

ボット等マルウェア感染による脅威やソーシャルエンジニアリングを駆使した脅威以外の外部脅威と内部脅威については、主として利用者（企業）において対策が求められてきたところであるが、今後も内部統制の強化が必要であり、不断の対策の実施・改善が望まれている。

特に、紛失・置き忘れや従業員が誤ってウイルスに感染した自宅の PC を利用すること等による情報漏えいが継続して発生しており、完全に人為的ミス等による脅威を取り除くことは不可能であるが、事前の抑止対策に加え、事後の被害拡大を防止・軽減するための対策実施がより一層求められる状況である。

現状の対策や課題に関する共通的な事項として、特に、対策実施主体である利用者（個人）について、情報セキュリティ対策に対する意識やスキルが必ずしも高くないと考えられる、いわゆる「永遠のビギナー」に、自らの責任だけで情報セキュリティ対策を全面的に託すことは難しいと考えられるとの指摘が多数なされている。永遠のビギナーは、年少者や高齢者など、これまでインターネットを利用する機会が少なかった者も幅広くインターネットを利用する環境となっていくことにより増加すると予想されるうえ、現状では何ら問題を感じることなく利用している場合であっても、情報通信機器の高機能化やサービスの多様化により、期せずして、こうした層になってしまう利用者もあると考えられる。

また、社会経済活動の ICT への依存が高まる状況において、特に、政府機関、重要インフラに対するサイバー攻撃等による被害の甚大さを考慮し、ネットワークを通じたこうした社会基盤への意図的な攻撃への対処について、十分に検討を深めるべきとの指摘がある。

４．近い将来のＩＣＴ環境と情報セキュリティ脅威・課題

４－１　近い将来におけるＩＣＴ環境の変化

近年、情報通信環境は、情報通信技術の進展や企業・個人による ICT 利用の急速な普及等を背景に、目覚しく変化している。特にネットワークの IP 化、全国でのデジタル放送の放送開始、通信・放送サービスの融合、デジタル家電の普及、携帯端末の高機能化等、今後数年間における情報通信環境も、ICT の利用領域の拡大や利用者の増加とともに大きく変化していくものと考えられる。また、こうした情報通信環境の変化に応じて、情報セキュリティの脅威・課題もその状況が変化していくものと考えられる。

こうしたことから、本研究会では、安心・安全を確保した情報通信環境を基盤とした我が国の社会経済活動の健全な発展に資するため、現状における情報セキュリティの課題等を整理するとともに、近い将来（3 年から 5 年後）における情報通信環境の変化を予測し、その環境変化とそこに至るまでの変遷過程において発生、継続、又は拡大するであろう将来の情報セキュリティの主な脅威や課題を可能な限り洗い出し、来るべき将来に備え、現時点から取組みを強化しなければならない対策の方向性等について、検討を行ってきている。

こうした検討にあたり、先ずは、情報通信を取り巻く環境がどのように変化していくのか、我が国の社会的な大きな変化とともに、その情報通信環境の変化をいくつかに分類し、以下のように取りまとめた。

（社会変化の状況）

今後我が国が直面する大きな社会変化の一つとして少子高齢化が挙げられる。日本の少子化、高齢化は益々進展し、日本の将来推計人口(平成 18 年 12 月　国立社会保障・人口問題研究所)によると、2005 年に 20.2%だった 65 歳以上の人口は、2030 年には 11.6 ポイント増の 31.8%になると予測されている。

また、団塊の世代が 2007 年から 2010 年を境に定年退職を迎え、社会保障給付費の増加率が経済成長率を大きく上回って急増すると予測されている。その一方で、人口減少、世帯減少が進み国内消費の冷え込みが予測される中、新たな消費活動の主体に成長することも期待されている。

さらに、政府として、仕事と生活の調和が実現した社会として、具体的には、①就労による経済的自立が可能な社会、②健康で豊かな生活のための時間が確保できる社会、③多様な働き方・生き方が選択できる社会、になっていくことを推進しており、ライフスタイルの多様化、人口構成の変化、環境問題への対応等から、在宅勤務をはじめとした様々な勤務形態が増加していくものと考えられる。

その他、日本の企業活動では、国内需要の大幅な拡大は見込めず、中国をはじめとする国外市場での市場開拓を進めるために海外事業を強化する傾向が一段と強まって

いくとの予測がある。

（情報通信環境の変化の状況）

近い将来（3 年から 5 年後）の情報通信環境は、情報通信技術の高度化、ICT の利用領域の拡大や利用者の増加等が進展し、一言で言えば、ユビキタスネット社会（いつでも、どこでも、何でも、誰でもネットワークに簡単につながり、利用できる社会）の実現が進んでいる。具体的な変化の状況は、以下のとおりである。

① 情報通信ネットワーク技術の高度化が一層進展

ア）2010 年、我が国におけるブロードバンド・ゼロ地域が解消

イ）電気通信網の IP 化（NGN）の普及とインターネットとの並存

ウ）IPv6 の利用促進（IPv4 との共存）

エ）2009 年サービスインを目標とした広帯域移動無線アクセスシステム等無線アクセスの多様化

オ）2011 年以降、高速移動時に 100Mbps を確保する第 4 世代移動通信システムが実現

カ）家電のネットワーク化（情報家電）・高機能なロボットの普及

キ）FMC、FMBC（固定通信、移動通信、放送の融合）サービスの台頭

ク）P2P 等、オーバーレイ・ネットワークの利用拡大

② スマートフォン等、携帯電話の高機能化によるモバイル利用環境の進展

ア）OS、アプリケーションのオープン化、ＡＰＩの公開

イ）携帯端末等を利用して、ホームネットワークに繋がった情報家電を制御

ウ）携帯端末による認証・電子決済

エ）GPS の標準搭載により、位置情報利用の拡大

③ ネットワークを流通するデータ量、ネットワークと接続するデバイス数の爆発的増加

ア）新たな消費主体の台頭やライフスタイルの多様化を背景としたインターネット利用者数の増加

イ）携帯電話端末、ＰＤＡ、ゲーム端末等、non-PC によるインターネット利用の増加

ウ）ブログ、SNS などの CGM（インターネットを通じて消費者が情報を生成し発信していくメディア）の増加

エ）大容量マルチメディアコンテンツの流通拡大

オ）情報家電のほか、運輸、卸売・小売、医療・福祉、製造等での RFID の利用拡大

④ 消費活動等の変化

ア）2010 年にはテレワーカーを就業人口の２割にする政府目標

イ）非接触ＩＣカードの普及による電子マネーの利用拡大

ウ）口コミ情報や価格比較の利用が進むなど、こだわり型の消費活動の増大

エ）RFID によるリアルタイムの商品管理

オ）商品情報・顧客情報の増大と営業戦略の変化

カ）仮想世界の普及

⑤ ICT 利用領域等の拡大、ＩＣＴ利用による生産性向上等

ア）社会インフラとしての ICT の重要性が一層増すとともに、様々な分野における ICT 利用の拡大による業務効率の改善や新しい事業の開発が促進

イ）ASP・SaaS の利用促進（2010 年の ASP・SaaS の市場規模予測：1.5 兆円（2005 年８月、ASP 白書（ASPIC、㈶マルチメディア振興センター））

４－２　近い将来のＩＣＴ環境における情報セキュリティの脅威・課題

前節に記述した近い将来の情報通信環境の変化及びそこに至るまでの変遷過程において発生、継続、又は拡大すると想定される将来の情報セキュリティの主な脅威や課題は、以下のとおりである。

① 情報通信ネットワーク技術の高度化

ア）2010 年、我が国におけるブロードバンド・ゼロ地域が解消

イ）電気通信網の IP 化（NGN）の普及とインターネットとの並存

ａ）サーバ等の攻撃ではなく、ネットワークに接続した携帯電話や情報家電等の機器が直接的な攻撃の対象となる。

ｂ）利用者関連の情報が集約するサービス･ストラタムが攻撃の対象となる。

ｃ）NGN の伝送プロトコルに関連する脅威が発生する可能性がある。（回線の乗っ取り、不正転送、盗聴、タダ掛けなど。実装レベルでの不具合。）

ｄ）NNI・UNI・SNI 等を通じて複数の電気通信事業者やアプリケーションサービス、利用者端末（利用者自身）が連携する際に、成りすまし等が発生する可能性がある。

ｅ）ＮＧＮになっても、現状発生しているインターネット上のセキュリティ問題（スピア攻撃やウイルス感染等）が減少・消滅せず、脅威は継続・巧妙化していく。

ｆ）NGN におけるサービスのオープン化・水平連携型の促進による関係事業者の増加により、インシデント対応が複雑化する。

ウ）IPv6 の利用促進（IPv4 との共存）

ａ）IPv6 化により NAT／プロキシがなくなることで、内部ネットワークや端末・アプリケーションが直接攻撃にさらされる可能性がある。

ｂ）グローバル IP アドレスが固定化されるため、行動分析が容易になると共に、特定アドレスへの継続的な攻撃が可能になる。

ｃ）IPv4 上で IPv6 のトンネルリングの利用や、不正に IPsec が利用されることで、FW、IDS 等が機能せず、適切な管理が出来ない状況の下で、ウイルス感染や侵入行為等が進む可能性がある。

ｄ）IPv6 対応ルータの自動アドレッシング、ルータ発見機能により、任意のルータを新設することにより、既設ルータのアドレス設定やルーティングが強制的に変更させられる恐れがある。

ｅ）マルチキャスト通信を介した無差別攻撃の可能性がある。

ｆ）現在でも生じている TCP/IP の脆弱性に関連する攻撃事象が、IPv6 でも継続して生じる場合がある。（SYN Flood 攻撃、ICMP Echo リクエスト等）

ｇ）IDS 等のセキュリティ機器の IPv6 対応への遅れが懸念される。

ｈ）IPv4 と IPv6 の混在するネットワークが利用されることにより、運用管理上の負担が増加し、セキュリティ事故につながる可能性がある。

エ）次世代無線システム等無線アクセスの多様化

オ）第 4 世代移動通信システムの実現

ａ）利用者数・端末数の増加により、利用者への攻撃が増加する可能性がある。

ｂ）OS やアプリケーション等の共通化により、脆弱性等の影響が及ぶ範囲の拡大が懸念される。

ｃ）携帯電話等を利用した個人情報、機密情報の流通量が増えると想定され、当該情報を標的にした盗聴、不正アクセス、改ざんなどの攻撃が増加する可能性がある。

ｄ）無線通信技術の脆弱性をつく攻撃、端末の盗難・紛失等による被害が拡大する可能性がある。

ｅ）無線局数の増加等により、無線基地局やアンテナへの物理的な盗聴や不正アクセス、破壊などの脅威が増加する可能性がある。

ｆ）携帯端末等に対して、ＰＣ端末と同等のセキュリティ対策が実装できるか、課題となる。

カ）家電のネットワーク化（情報家電）・高機能なロボットの普及

ａ）様々な情報家電機器やサービスが普及することで、IT の知識やセキュリティ意識が必ずしも高くない利用者が増加し、設定ミスやこうした利用者を標的にしたソーシャルエンジニアリング攻撃が増加する可能性がある。

ｂ）OS やアプリケーション等の共通化により、脆弱性等の影響が及ぶ範囲が

拡大する。また、多様な実装が行われることによって、脆弱性の増加や対応の遅れが懸念される。

c）情報家電等を通じて流通する個人情報や機密情報の量が増えると想定され、当該情報を標的にした盗聴、不正アクセス、改ざんなどの攻撃が増加する可能性がある。

d）サイバー攻撃の踏み台化や、家電製品を誤動作させることにより人命に影響を及ぼすような攻撃に発展する可能性がある。

e）家電製品のライフサイクルに対応した情報セキュリティ対策が確立されていない。（売切り、長期間利用、転売・破棄）。

f）通常のインターネットでは好ましくないとされる利用方法により、ネットワークやサーバの過負荷等が生じる可能性がある。（監視ビデオを１秒ごとにメールサーバに送信し、それを１秒ごとに pop で取得するといった使い方等）

キ）FMC、FMBC（固定通信、移動通信、放送の融合）サービスの台頭

a）携帯電話・固定電話の複数端末を跨って、個人情報や機密情報が流通するケースが増大し、当該情報の盗聴、不正アクセス、改ざんなどの攻撃が増加する可能性がある。

b）ウイルスが埋め込まれた不正なコンテンツがブロードキャストされる可能性や、放送局への成りすましによる偽造コンテンツの送信等が発生する可能性が生じる。

ク）P2P 等、オーバーレイ・ネットワークの利用拡大

a）一定の利用者やサービスなどで閉じた仮想ネットワークを構成することで、ビジネス上の利点がある一方、嗜好が近く、ソーシャルエンジニアリングによる攻撃がし易くなる可能性や、管理者不在の有害ネットワークとして、構成される可能性がある。

② スマートフォン等、携帯電話の高機能化によるモバイル利用環境の進展

ア）OS、アプリケーションのオープン化、ＡＰＩの公開

イ）携帯端末等を利用して、ホームネットワークに繋がった情報家電を制御

ウ）携帯端末による認証・電子決済

エ）GPS の標準搭載により、位置情報利用の拡大

a）利用者数・端末数の増加により、利用者への攻撃の増加が懸念される。

b）OS やアプリケーション等の共通化により、脆弱性等の影響が及ぶ範囲が拡大する可能性がある。また、多様な実装が行われることによって、脆弱性の増加や対応の遅れが懸念される。

ｃ）携帯電話等を利用した個人情報、機密情報の流通量が増えると想定され、当該情報を標的にした盗聴、不正アクセス、改ざんなどの攻撃の増加する可能性がある。

ｄ）サイバー攻撃の踏み台化や、家電製品を誤動作させることにより人命に影響を及ぼすような攻撃に発展する可能性がある。

ｅ）様々な情報家電機器やサービスが普及することで、IT の知識やセキュリティ意識が必ずしも高くない利用者が増加し、設定ミスやこうした利用者を標的にしたソーシャルエンジニアリング攻撃の増加が懸念される。

ｆ）携帯端末に対して、ＰＣ端末と同等のセキュリティ対策が実装できるか、課題となる。

③ ネットワークを流通するデータ量、ネットワークと接続するデバイス数の爆発的増加

ア）新たな消費主体の台頭やライフスタイルの多様化を背景としたインターネット利用者数の増加

ａ）様々な情報家電機器やサービスが普及することで、IT の知識やセキュリティ意識が必ずしも高くない利用者が増加し、設定ミスやこうした利用者を標的にしたソーシャルエンジニアリング攻撃が増加する。

ｂ）利用者の増加に伴い、各種サービスの入り口となる Web ブラウザの脆弱性をつく攻撃の影響範囲が拡大する可能性がある。

イ）携帯電話端末、ＰＤＡ、ゲーム端末等、non-PC によるインターネット利用の増加

ａ）利用者数・端末数の増加により、利用者への攻撃が増加する。

ｂ）OS やアプリケーション等の共通化により、脆弱性等の影響が及ぶ範囲が拡大する。また、多様な実装が行われることによって、脆弱性の増加や対応の遅れが懸念される。

ｃ）携帯電話等を利用した個人情報、機密情報の流通量が増えると想定され、当該情報を標的にした盗聴、不正アクセス、改ざんなどの攻撃の増加する可能性がある。

ｄ）携帯端末等に対して、ＰＣ端末と同等のセキュリティ対策が実装できるか、課題となる。

ウ）ブログ、SNS などの CGM（インターネットを通じて消費者が情報を生成し発信していくメディア）の増加

ａ）インターネットの利用形態や消費活動への影響が大きい反面、情報セキュリティ意識が必ずしも高くない情報発信者の増加による意図しない個人情

報の漏えいや事実に反する情報が意図的または非意図的に流通する可能性が増加する。

b）事故を装った意図的な個人情報の漏えい・プライバシーの侵害が発生する可能性がある。

c）CGM による風評被害や、特定個人へのバッシング等といった問題が拡大する可能性が高い。

エ）大容量マルチメディアコンテンツの流通拡大

a）情報セキュリティ意識が必ずしも高くない情報発信者の増加による意図しない個人情報の漏えいが増加する。

b）（一部の利用者により）大量のメディアコンテンツが流通することにより、ネットワーク設備への影響が懸念される。

オ）情報家電のほか、運輸、卸売・小売、医療・福祉、製造等での RFID の利用拡大

a）情報家電、RFID 等で利用される個人情報、機密情報の流通量が増えると想定され、当該情報を標的にした情報漏えい、改ざんなどの攻撃の増加する可能性が高い。

b）ＩＣカード、読み取り装置との間での通信データの盗聴・改ざんなどが発生する可能性がある。

④ 消費活動等の変化

ア）2010 年にはテレワーカーを就業人口の２割にする政府目標

イ）非接触ＩＣカードの普及による電子マネーの利用拡大

ウ）口コミ情報や価格比較の利用が進むなど、こだわり型の消費活動の増大

エ）RFID によるリアルタイムの商品管理

オ）商品情報・顧客情報の増大と営業戦略の変化

a）流通する個人情報や機密情報の量が増えると想定され、当該情報を標的にした情報漏えい、改ざんなどの攻撃の増加する可能性が高い。

b）様々なネットワーク機器やサービスが普及することで、IT の知識やセキュリティ意識が必ずしも高くない利用者が増加し、設定ミスやこうした利用者を標的にしたソーシャルエンジニアリング攻撃が増加する。

カ）仮想世界の普及

a）仮想世界の通貨等を標的にした情報漏えい、改ざんなどの攻撃が増加する可能性が高い。

⑤ ICT 利用領域等の拡大、ＩＣＴ利用による生産性向上等

ア）社会インフラとしての ICT の重要性が一層増すとともに、様々な分野における ICT 利用の拡大による業務効率の改善や新しい事業の開発が促進

イ）ASP・SaaS の利用促進

ａ）ネットワークを介して提供される設備やサービスを利用する場合などでは、当該サービスの提供者の設備に障害が発生した場合に被害の範囲が広範になることから、こうした設備等を意図的に攻撃する可能性が高くなる。

ｂ）外部に集約される企業情報等を標的にした情報漏えいや改ざん等の攻撃が増加する可能性がある。

ｃ）暗号の危殆化に伴い、機密保護や認証を目的として暗号を利用している各種のシステムやサービスにおいて、盗聴、不正アクセス、改ざんなどの攻撃が生じる可能性がある（SHA―1、1024bitRSA など）。

ｄ）ICT を活用した業務システムの増加に伴い、公開鍵暗号基盤(PKI)の利用拡大が想定され、証明書の発行・失効等管理の複雑化・処理量の増大が懸念される。

ｅ）社会インフラとして広く利用されているシステムやサービスにおいて、その依存度が高いものほど、移行期における可用性、継続利用性の確保が懸念される。

以上を踏まえ、近い将来における「ユビキタスネット社会」での情報セキュリティについて、それぞれの環境変化等による主な脅威と課題を集約すると、次のようにまとめられると考えられる。

① 脅威の対象となる範囲の拡大（物、人）

ア）ネットワークに接続される機器・デバイスが爆発的に増大し、脅威の対象範囲が拡大する。

イ）OS、アプリケーションの共通化・寡占による単一仕様化により、１つの脆弱性が及ぼす対象範囲が拡大する。また、多様な実装が行われることによって、脆弱性の増加や対応の遅れが懸念される。

ウ）インターネット利用の進展により、情報セキュリティに関する意識や知識が必ずしも高くない利用者が増加する。

エ）情報の保持、管理する場所・主体の変化が生じる。

② 脅威の対象となる情報の増加・多様化

ア）ビジネスモデルや利用形態の変化に伴い、決済情報、認証情報、位置情報等の個人情報や企業情報が、ネットワークを流通する機会が増大する。

イ）仮想世界の通貨等、新しい価値ある情報の流通が増加する。

③ 対策の困難性の拡大

ア）情報通信技術の進展や、利用形態・ビジネスモデルの恒常的な変化により、将来の脅威予測が困難である。

イ）ネットワークに接続される端末・デバイスや情報量の爆発的な増大、利用する個人の増加、及び業界を越えて機器製造業者、電気通信事業者、サービス提供事業者等の多くの関係者が複雑に関連し合うと想定される環境において、情報セキュリティを検討するに当たっての参照モデルが確立されていない。

ウ）ソーシャルエンジニアリングを駆使した対象範囲を絞った攻撃が進行するなど、ウイルス感染や意図的に情報漏えいを引き起こす手法が高度化・潜行化していく。

エ）社会インフラとしてのＩＣＴ利用拡大により、システム・サービスの可用性、継続利用性に対する要求が高まることにより、迅速な対策実施が必要とされるにもかかわらず、システムのライフサイクル等に依存した長期的な対応しかできないケースが増える。

オ）情報セキュリティ対策の主体、責任範囲が不明確となりやすい。

カ）情報セキュリティに関するインシデントが発生した場合に、国内外の情報共有し、迅速かつ効果的な対策を実施する体制が確立されていない。

５．現状及び近い将来のＩＣＴ環境における情報セキュリティ対策の重要性

５－１　今後の情報セキュリティに関する主な課題等

第３章で取りまとめた現状の情報通信環境で生じている情報セキュリティに関する脅威、現状の対策実施における課題等、及び第４章で取りまとめた近い将来での情報通信環境における情報セキュリティ脅威等を踏まえ、今後の情報セキュリティに関する主な課題等は、以下のとおりに集約することが可能である。

① ボットに感染したＰＣを踏み台にしたスパムメールの送信や DDoS 攻撃、情報漏えいといった様々なインシデントが今後も継続して発生する。また、Web 感染型やソーシャルエンジニアリングを駆使したマルウェア感染手法等、今後も悪意をもった攻撃者によるマルウェアの感染手法等が巧妙化、高度化し、国内外を通じて引き続き ICT 利用環境における最大の情報セキュリティ脅威となる。

② 情報通信技術の高度化、サービス内容の多様化、ICT 利活用領域の拡大等により、ネットワークに接続される情報通信機器数・端末数、利用者数が爆発的に増大することとなる。このように、これまで以上に多くの関係者が複雑に絡み合って形成される情報通信社会においては、各情報セキュリティ対策実施主体の責任範囲の不明確化によって情報セキュリティ対策に遅れが生じ、脅威が増大する。加えて、重要インフラをはじめとした社会基盤における ICT 依存が進展し、設定ミス等による非意図的な要因によって引き起こされる障害においてもその影響の範囲が広域化する可能性がある。また、システム・サービスの可用性、継続利用性に対する要求から、迅速に対策を実施することが困難なケースが増えることも予想される。

③ 上記②と関連して、ネットワークを流通する企業及び個人に関する情報の種類及び量が著しく増加するととともに、情報通信機器・端末の高機能化により、例えば、これまで以上に携帯端末側に個人情報等が保存される可能性があるなど、情報資産を保持・管理する方法や場所の多様性が増すこととなり、情報セキュリティ対策が困難になる。

④ サービスの多様化、ICT 利活用領域の拡大等によって利用者層も広がることとなり、今後は、これまで以上に必ずしも情報セキュリティ対策についての意識が高いとは言えない、いわゆる「永遠のビギナー」による ICT サービスの利用が増加していくこととなる。この場合、永遠のビギナーが悪意の第３者からの最大の標的とされる可能性が高いほか、適切な情報セキュリティ対策を行わない永遠のビギナーがボット等のマルウェアに感染することにより、自らが被害者となるだけではなく、他人に被害を及ぼす加害者となることから、一部の者が高度な情報セキュリティ対策を講じても、我が国の全体としての情報セキュリティ向上には繋

がらないという状況に陥ることとなる。

⑤ さらに、ネットワークに繋がる情報通信機器・端末の OS、アプリケーションの共通化・寡占による単一仕様化によって１つの脆弱性が及ぼす影響範囲が拡大する可能性や、スマートフォンに代表されるように複数の通信経路を持つ場合のマルウェア拡散が複雑化・広域化する可能性があるほか、新しい技術を導入することによってこれまで想定し得なかった脅威が発生する可能性等が増大することとなる。

５－２　今後の情報セキュリティ対策について重点的に検討・実施すべき項目等

上記のような今後の情報セキュリティに関する主な課題に対応し、我が国がより一層 ICT を利用した社会経済活動の活性化・効率化、国際競争力の強化を実現するため、重点的に検討・実施すべき項目等は以下のとおりである。

なお、ここで挙げる以外の対策についても、継続的な取組みが重要であることは言うまでもない。

（利用者を取り巻く環境における情報セキュリティ対策の徹底）

利用者（個人）（本節では、企業としての ICT 利用ではなく、自宅や企業において個人がインターネット等を利用することを念頭にしている。以下、特に断りがない場合を除き「利用者」とする。）における情報セキュリティ対策の徹底は、今後も一貫して基本的な対策であると考えられる。

サービス提供事業者や機器製造事業者、電気通信事業者等の ICT サービス提供者側が事前に想定し得る対策を講じた上で製品・サービス等を提供しなければならない責任を有していることはそもそもの前提であるが、これまでも繰り返し述べてきているとおり、適切な情報セキュリティ対策を行わない利用者がボット等のマルウェアに感染すること等によって、自らが被害者となるだけではなく、他人に被害を及ぼす加害者となってしまうことに鑑み、「利用者は、インターネットをはじめとした ICT 利用にする際の社会的責任として、必ず一定程度の基本的な情報セキュリティ対策を講じなければならない」と考えることが妥当であると思われる。

しかしながら、永遠のビギナーに代表されるように、必ずしも情報セキュリティ対策をはじめとする情報リテラシーが高くない利用者もインターネット等を利用することを考慮し、ICT サービス提供側で、利用者の情報セキュリティ対策の負担を軽減する対策を行うこと等が必要である。

なお、以下に挙げる具体的な項目の検討・実施のほか、利用者間や利用者と ICT サービス提供者側との間で生じた問題（紛争等）を迅速に解決する体制、電気通信事業者や ICT サービスを利用する企業等における情報セキュリティ対策コスト負担のあ

り方、サイバー犯罪等に関連する法制度の検討・執行状況、電気通信事業者やICTサービスを利用する企業等における事業継続性等を勘案した実効性のある対策のあり方等については、継続的に検討を進めることが必要である。

① 利用者における情報セキュリティ対策の徹底に向けた普及啓発

利用者がボット等に感染することにより、自らが被害を受けるだけではなく、他人へ迷惑をかける加害者になってしまう場合があることを重く認識し、これまで以上に、インターネット等を利用する際の情報セキュリティ対策の徹底を図るため、政府は電気通信事業者をはじめとする関係機関等との連携のもと、サイバークリーンセンター等を通じて、普及啓発活動のより一層の充実に努めるべきである。

現状、サイバークリーンセンターの活動実績として、ISPからの注意喚起によって感染ユーザがボット等の駆除等を行った場合には、再感染率が著しく低下する(注)との結果が出てきている。こうした状況からも推測されるように、利用者に自分の問題として認識してもらえるか否かが普及啓発の成果に大きく影響するものと考えられることから、情報セキュリティ対策の実施の必要性を利用者に直接的に伝えられるような創意工夫が必要である。

(注) サイバークリーンセンターに参加するISP（１社）において、2007年９月から12月までの間、４週間後に再感染をした利用者数を調査した結果、当該ISPからの注意喚起によりCCCのWebサイトを訪問しない場合と訪問した場合を比較したところ、それぞれの再感染率が約１４％と約２％になり、７分の１に低下した実績が報告されている。

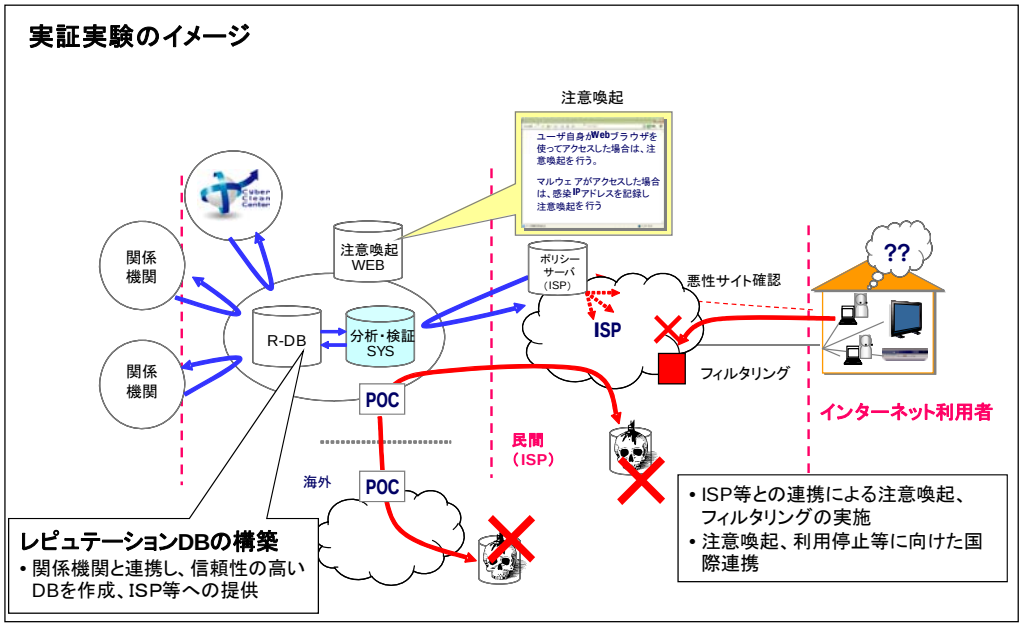
② 電気通信事業者による情報セキュリティ対策の推進

一部の利用者が高度な情報セキュリティ対策を講じても、我が国の全体としての情報セキュリティ向上には繋がらないという現実を踏まえ、より社会全体として情報セキュリティ向上を実現するための効率的かつ効果的な取組みとして、電気通信事業者による以下の対策について、早急に検討を行うことが必要である。

ア）電気通信事業者が、マルウェアの感染活動等に利用されている通信ポートを閉じてマルウェアが活動できない状態にするなど、情報セキュリティを確保するために電気通信事業者が取り得る正当業務行為の範囲についてのガイドラインを検討することが必要である。なお、検討にあたっては、インターネット利用者が現在利用しているサービスが利用できなくなる場合があることや、ウイルス感染の手法等が激変し、より解析や対処が困難になる可能性があることを十分に考慮する必要がある。

イ）上記ア）の検討に資するため、正規のWebサイトを閲覧しただけでマルウェ

アに感染してしまう状況を踏まえ、利用者が誤ってフィッシングサイトやマルウェア配布サイト等の危険な Web サイトと通信することを防止するため、信頼性の高いレピュテーション・データベース（危険な Web サイト等に関するリスト）の構築とその運営方法等についての実証を促進し、その効果を検証することが必要である。



図表 5-1：実証実験のイメージ

なお、上記 2 項目については、利用者の情報セキュリティ対策の充実に加え、ネットワークを流通する不要なトラフィックの低減や、紛争解決の手間を未然に防ぐことにつながることから、電気通信事業者にとっても効果があるものと期待される。

③ ユーザーサポート体制の充実

情報セキュリティ対策は、事前の対策の充実を図っても万全ではなく、インシデントが発生した際にいかに迅速に事態を掌握し、復旧を図るかも、重要な対策である。こうしたことを踏まえ、利用者が実際にマルウェアに感染して被害を受けた場合等にどのような対処を行えば良いか、身近にかつ気軽に相談できるユーザーサポート体制を地域に根差した NPO の活動等として充実することが必要である。こうしたサポート体制の実施により、以下のような複数の具体的なメリットがもたらされるものと期待される。

・利用者個人にとっては、時間や費用を浪費せず、迅速に不具合等の原因究明が可能となる。
・対応事例等を集積・分析することにより、同様の障害に迅速に対応できるノウ

ハウを共有したり、再発防止の手段の検討が可能となる。

・今後普及が予想される情報家電を含む情報通信機器・端末や ICT サービスを提供する事業者のカスタマーサービスセンター等にとっては、原因や症状が不明確な問合せが減ると共に、当該ユーザーサポート体制に所属する技術的知識を有する人材が仲介することにより、的確な情報を簡潔に相手方に伝えられるようになることで、同カスタマーサービスセンターに要する経費等の削減効果が期待される。

・ユーザーサポート体制に所属する人材としては、電気通信事業者や情報通信機器関連のベンダー等の技術者等を活用することが有効であり、高齢者の雇用機会確保にも貢献するものと期待される。

なお、このユーザーサポート体制の実現に当たっては、対処のポイントを分かり易く、迅速にかつ的確に伝えることが必要であるとともに、活動する個人や組織、地域等によってその能力に差が生じてしまうと、上記メリットを効果的に享受することが出来なくなると考えられるため、一定程度のスキルを身につけている者が当該業務にあたるよう、その知識やスキルを認定する仕組みを検討すべきである。また、この認定制度については、情報通信機器やサービスの進歩に対する迅速な対応を考慮すると、民間を主体にした取組として検討することが妥当であると考えられる。

（産学官連携による先進的な研究開発の実施）

① ボット等マルウェア感染手法の巧妙化等への対策

ボットに感染したＰＣを踏み台にしたスパムメールの送信や DDoS 攻撃、情報漏えいといった様々なインシデントが今後も継続して発生するほか、Web 型の感染手法（しかも、きっかけとなった Web サイトから直接マルウェアがダウンロードされるのではなく、Web のリダイレクトやダウンローダを複数回利用して感染する仕組みになってきている）による場合や、ソーシャルエンジニアリングを駆使したスピア型メールを利用する場合など、攻撃の手口が巧妙化・高度化してきており、今後も新しい感染手法が開発され、実行されるものと容易に想像される。

こうした状況を踏まえ、感染手法の悪質化・被害の局所化への対策を強化することが必要であり、こうした事象を高度に観測・把握・分析し、障害を低減・除去する先進的な一連の対策技術について、継続的な研究開発に取組むことが重要である。

その際、迅速かつ効果的な対策を実施するための情報収集機能として、感染活動が近隣の IP アドレスに限定されることが多いことや日本国内で流通しているソフトウェアの脆弱性をついたマルウェアが増加していること、標的や被害が局所化していること等を考慮し、日本国内の状況を的確に把握することを目的に、従

来型の受動的な観測システムに加え、利用者のプライバシーに配慮しつつ利用者側の状況を積極的に把握するための観測網の強化が必要である。

また、我が国において情報セキュリティ対策等に係る人材の育成についても積極的に取り組むことが必要である。特に、高等教育機関においては、我が国の研究開発・技術開発分野の拠点として、優れた人材を養成することが必要であり、「人材育成・資格制度体系化専門委員会報告書」（2007 年 1 月、情報セキュリティ政策会議）等において指摘されているところである。さらに、総務省では、抜本的な高度人材育成政策について検討するため、2007 年９月から「高度 ICT 人材育成に関する研究会」を開催しており、2008 年５月頃を目途に最終的な報告書をとりまとめる予定としている。

なお、平成 18 年度から実施されている「先導的 IT スペシャリスト育成推進プログラム」に関して、平成 19 年度に採択されたプロジェクト「社会的リスク軽減のための情報セキュリティ技術者・実務者育成」（通称：IT Keys 奈良先端科学技術大学院大学、大阪大学、京都大学、北陸先端科学技術大学院大学）については、情報セキュリティ対策の立案遂行を主体的に実施しうる実務者の育成を目標としており、この中でサイバークリーンセンターにおける実習を取り込み、実践的知識の習得を念頭にしたカリキュラムを計画中である。

上記に加え、サイバークリーンセンターでは、情報処理学会と連携し、業務において取得したマルウェア検体や攻撃が含まれた通信データを活用して、ネットワークインシデント解析、可視化技術等に関するコンテストを行うワークショップの年内開催を計画している。

今後、こうした産学官が連携した人材育成の取組みが、より活性化することが極めて重要である。

さらに、総務省では、我が国の成長力・競争力の強化を図るため、情報通信分野の専門的人材を育成する研修事業に対し、当該事業に必要な経費の一部を助成すること目的に「情報通信人材研修事業支援制度」を実施している。また、企業等における戦略的情報化を担う人材を育成するため、実践的育成手法である PLB（Project Based Learning）教材（情報セキュリティマネージメント分野を含む。）を開発している。加えて、横須賀テレコムリサーチパークにおいて、情報セキュリティ技術も対象にした「ＹＲＰ情報通信技術研修」に取組むなど、情報通信分野の人材育成に取り組んできているところであるが、より一層の取組の強化が期待される。

② IPv6 等の新しい技術が実装されていく過程で生じ得る技術的な課題への対策

現在の IPv4 ネットワークにおけるアドレス在庫の枯渇に対応するため、IPv6 化の対応が必要であるという基本的認識のもと、Routing Header 0 (RH0) 問題、

IPv6 パケットが任意個のオプションヘッダを許容する問題といった、現状でも様々な脆弱性が発見され、その対策を進めている状況を踏まえ、IPv6 技術がより安心して利用できる基盤技術となるよう、継続的な研究開発の実施が必要である。

③ Ｐ２Ｐネットワークや CGM 等において信頼できる情報を共有するためのレピュテーションＤＢ高度化技術の検討

情報通信技術の高度化や利用形態の多様化が進展する状況において、管理者不在となる P2P ネットワーク、消費者が様々な情報を生成し発信するＣＧＭ等のオーバーレイ・ネットワークでは、趣味・嗜好の近い利用者が集まったコミュニティを形成した情報交換等が進展し、それによるビジネス展開の期待が高まるとともに、P2P ネットワークにおいては、障害等に対するロバスト性も高くなることが期待される。その一方で、利用者の判断を誤らせるような事実に反する情報が意図的・非意図的に流通する場合やフィッシング等ソーシャルエンジニアリングを駆使した詐欺等に関連する情報が流通する場合があるほか、マルウェアの感染・流通手段となること等により、利用者が不利益を被る可能性も高くなると想定され、これらの P2P ネットワーク等の利用にあたっては、利用者自身によって流通している情報や情報発信元の信憑性の判断をしなければならない場面が多く発生することになる。

しかしながら、利用者が個別に流通する情報の信頼性を判断することは極めて困難であることから、その判断を補完するものとして、利用者自身が情報発信元や情報そのものの信頼性を評価し共有できるレピュテーション機能や情報の質や信頼性を検証する技術等の実現方法について検討することが必要である。なお、当該技術開発の意図とは反対に詐欺情報やマルウェアの共有や拡散を助長することがないように留意が必要であるとともに、管理者が不在となる場合のオーバーレイ・ネットワークの在り方についても、継続的な議論が必要であると考えられる。

（関係機関における連携強化）

① 実効性のある情報共有体制の充実

脅威が巧妙化、潜行化し、また被害が局所化していることから、感染事実が把握しづらい状況なっていることを考慮し、日本国内において、政府機関、電気通信事業者、情報セキュリティ関連事業者、情報セキュリティに関連する産学官の研究機関等が、前述の観測網等で収集・分析できたインシデント情報等を迅速に情報共有できるよう、その連携体制の充実を図ることが望まれる。

なお、情報共有等の実効性を高めるため、ネットワークインシデントの状況等の調査を行い、再発防止策等を提示する専門的な機関の設置についても、引き続

き検討すべきである。

② 国際連携の促進

現在発生している情報セキュリティ脅威の多くは、必ずしも全世界的に大きな影響を生ずるような大規模な事象ではなく、むしろ地域や嗜好等を絞ることで特定の範囲に脅威が限定される傾向にあると言えるが、その発信源は、ボットによるスパムメールや DDoS の発信元アドレスを例に取れるように、非常に広範囲に渡り、また、各国法制度、組織体系、情報セキュリティそのものに対する考え方等が異なることから、迅速な対応が不十分な状況にある。こうした状況に対処していくためには、これまでも繰り返し指摘されてきているところではあるが、日本国内における連携のみならず、事案解決に向けた諸外国との情報共有等の連携が必要であり、脅威の潜行化が進行する状況やエストニアの事例を教訓に政府機関・重要インフラにおけるサイバー攻撃への耐性強化の必要性が高まっている状況を踏まえ、その対応を検討する必要がある。

このため、例えば、APEC、OECD 等の国際的な枠組みを利活用しつつ、各国政府及び関係機関との間で、情報セキュリティに関連するインシデント及びベストプラクティス等に関する情報の共有・分析等における協調・連携体制を構築及び強化していくことが挙げられる。その際、我が国のボット対策プロジェクト（サイバークリーンセンター）等、国際的にも先進的な取組については、世界に向けた情報発信及び海外展開・協力体制構築に向けた検討等を実施していくことが望ましい。

（ユビキタスネットワーク社会における情報セキュリティ対策に関する業界横断的な検討体制の整備等）

ユビキタスネットワーク社会において、利用者が安心・安全に様々な情報通信機器・端末を駆使し、多様なサービスを利用できるようになるには、電気通信事業者、ＯＳ/アプリケーション/サービス提供事業者、今後普及が予想される情報家電を含む情報通信機器・端末の製造・販売事業者、情報セキュリティ関連事業者等が、それぞれ独自に情報セキュリティ対策を実施するだけではなく、お互いに協調・連携することが重要である。

このため、上記のような全ての関係者が参加し、継続的に、情報セキュリティに関連する課題やその対策等について検討する業界横断的な検討体制を整備することが必要である。この体制において、障害・対策事例等の共有のほか、各主体が個別に担うべき対策領域や、協調・連携して行うべき効果的な対策手法、そのコスト分担の在り方等について検討を進めることが期待される。

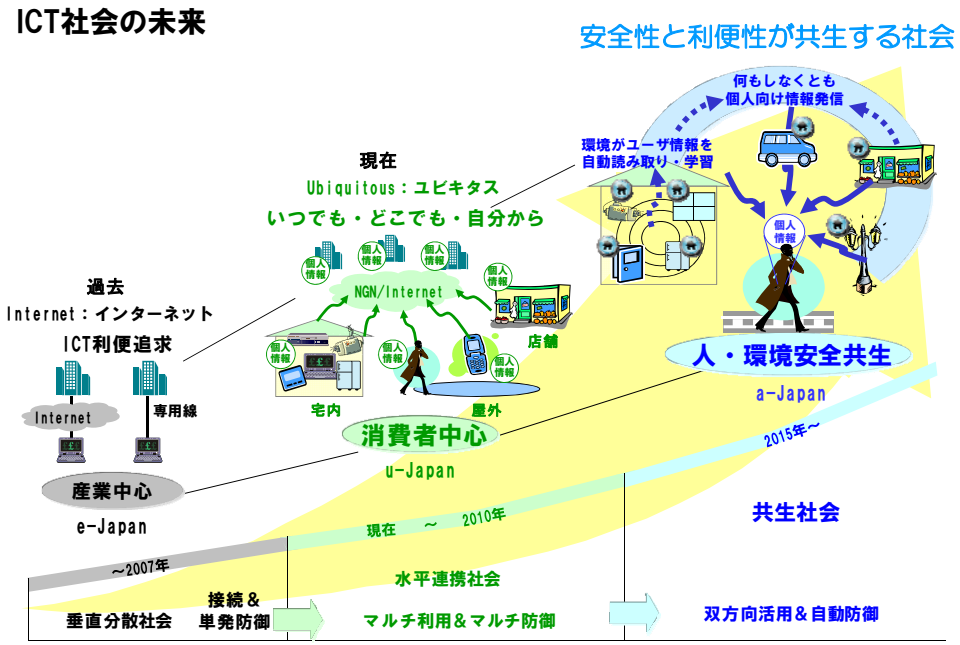
（利用者、情報通信環境、情報セキュリティが共生する ICT 社会モデルの検討）

将来の情報通信環境では、複数の関係者が関連してサービスが提供され、またネットワークに接続される端末や利用者数、情報量が爆発的に増加すると予測されており、こうした極めて複雑化が進む状況において、情報セキュリティを検討するに当たっての参照モデルが確立されていないと指摘されている。

このため、ICT サービスの多様性・利便性を確保しつつ、併せて情報セキュリティ対策が施されている環境を、「利用者（利便性）、情報通信環境（多様なサービス）、情報セキュリティが共生する ICT 社会モデル」として実現することについて、具体的な実証モデルを構築して、その有効性や課題の検証を進めることが重要である。

その実証モデルの例として、端末認証技術・シングルサインオン技術、本人情報や属性情報が漏えいし不正に利用されないための個人情報等の保護・管理技術等を組合せるなどして、利用者が複雑な設定をすることなくワンストップで安全にサービスが利用できるようなモデルなどが考えられる。

なお、本件の検討に当たっては、認証や個人情報の保護を実現する上での基礎となる暗号技術が、常に技術進展に伴う危殆化の危険性を孕んでいることを踏まえるべきである。



図表 5-2：情報セキュリティが共生する ICT 社会モデルのイメージ

６．終わりに

本研究会では、これまで、現状のインターネット等の利用環境において継続的に対策を講じていかなければならない課題、及び３から５年後の将来におけるＩＣＴ利用環境を想定し、その変遷過程を含めた情報通信環境の変化により生ずる課題等を抽出し、そのなかで重点的に取り組むべき主な項目を抽出・整理してきたところである。

今後は、ユビキタスネットワーク社会における情報セキュリティ対策が充実し、より安心・安全な ICT 利用環境において、我が国の生産性向上や国際競争力の強化が実現されるよう、最終報告に向けて、その主な項目等について、広く意見を募り、より具体化に向けて検討を深めることとしている。

参考資料１

「次世代の情報セキュリティ政策に関する研究会」開催要綱

１　背景・目的

ブロードバンド化の進展により、国民生活や社会経済活動におけるＩＣＴへの依存度が高まる一方で、ＩＣＴの安心・安全な利用に対する要求が高まり、情報セキュリティに対する取組はその重要性を増している。

総務省では、これまでも様々な情報セキュリティ政策に取り組み、我が国の安心・安全な情報通信環境の整備を行ってきたところであるが、昨今では、ネットワークを経由したウィルス感染の巧妙化・高度化、あるいは被害の深刻化等が進展している状況と言われている。

本研究会では、現状のインターネット等における具体的な脅威を洗い出し、その脅威に起因する情報セキュリティ事案の状況・傾向を明らかにするとともに、将来におけるＩＣＴ利用環境を想定し、ＮＧＮなどの多種多様なネットワーク上の脅威に対して必要となる取組など、課題や対策等を抽出し、国際的な連携の在り方等も視野に入れつつ、今後、総務省として取り組むべき情報セキュリティ政策の在り方を検討する。

２　名称

本会合は、「次世代の情報セキュリティ政策に関する研究会」（以下「研究会」という。）と称する。

３　主な検討事項

（１）現状のインターネット等における具体的な脅威の洗い出し
（２）脅威に起因するインシデントの最近の動向と傾向
（３）将来のネットワーク環境・利用環境（ＮＧＮ、ＩＰｖ６、移動体端末等）における脅威分析と課題抽出
（４）今後、取組が求められる情報セキュリティ政策の方向性

４　構成員

別紙のとおり

５　運営

（１） 本研究会は、政策統括官（情報通信担当）の研究会とする。
（２） 本研究会には、座長及び座長代理を置く。
（３） 座長は、構成員の互選により定め、座長代理は座長が指名する。
（４） 座長は、本研究会を招集し、主宰する。

（５） 座長代理は、座長を補佐し、座長不在のときには、座長に代わって、本研究会を招集し、主宰する。
（６） 座長は、必要に応じ、関係者等の出席を求め、意見を聞くことができる。
（７） 座長は、上記の他、本会の運営に必要な事項を定める。

６　庶務

本研究会の庶務は、情報通信政策局情報セキュリティ対策室が行う。

７　開催期間

平成１９年１０月から平成２０年６月頃を目処に計９回程度の開催を予定。

別紙

「次世代の情報セキュリティ政策に関する研究会」構成員名簿

（敬称略、五十音順）

新井　悠	㈱ラック 研究開発本部 先端技術開発部 部長
有村　浩一	テレコム・アイザック・ジャパン 企画調整部 部長
綾塚　保夫	㈱ＮＴＴドコモ 情報セキュリティ部 情報セキュリティ担当部長
飯塚　久夫	ＮＥＣビッグローブ㈱ 代表取締役執行役員社長
小倉　博行	三菱電機㈱ インフォメーションシステム事業推進本部 システム統括部 システム第一部 主席技師長（第 6 回～）
加藤　朗	東京大学 情報基盤センター 准教授（第 1 回～第 5 回） 慶応義塾大学大学院 メディアデザイン研究科 教授(第 6 回～）
菅　　隆志	三菱電機㈱ 情報技術総合研究所情報技術部門 部門長（第 1 回～第 5 回）
木村　孝	ニフティ㈱ 経営補佐室 担当部長
小屋　晋吾	トレンドマイクロ㈱ 戦略企画室 室長
小山　覚	㈱ＮＴＴＰＣコミュニケーションズ 執行役員 ネットワーク事業部 バリューサービス部長・事業企画部長
齋藤　衛	㈱インターネットイニシアティブ 技術開発本部 プロダクトマネージャ
佐田　昌博	㈱ウィルコム 技術企画部長
篠田　陽一	北陸先端科学技術大学院大学 情報科学センター 教授（独立行政法人情報通信研究機構 情報通信セキュリティ研究センター センター長）
下村　正洋	ＮＰＯ日本ネットワークセキュリティ協会 理事・事務局長
高倉　弘喜	京都大学 学術情報メディアセンター 准教授
高橋　正和	マイクロソフト㈱ チーフセキュリティアドバイザー
手塚　悟	㈱日立製作所 システム開発研究所 情報サービス研究セ

		ンタ センタ員
	徳田　敏文	日本アイ･ビー･エム㈱ ＩＴＳ事業ＩＳＳ事業部ＩＳＳ技術 部長
【座長代理】	中尾　康二	ＫＤＤＩ㈱ 運用統括本部 情報セキュリティフェロー（独立行政法人情報通信研究機構 情報通信セキュリティ研究センターインシデント対策グループ リーダ）
	則房　雅也	日本電気㈱ 第一システムソフトウェア事業部セキュリティグループ エグゼクティブエキスパート
	福智　道一	ソフトバンクＢＢ㈱ 技術統括 商用ネットワークセキュリティ推進室 室長
	藤井　俊郎	松下電器産業㈱ 情報セキュリティ本部 参事
	藤本　正代	富士ゼロックス㈱ マネジメントイノベーションオフィス シニアマネジャー
	水越　一郎	東日本電信電話㈱ コンシューマ事業推進本部ブロードバンドサービス部 サービス企画担当部長
【座長】	安田　浩	東京電機大学 未来科学部 教授
	山口　英	奈良先端科学技術大学院大学 情報科学研究科 教授
	山内　正	㈱シマンテック総合研究所 取締役 コンサルティング研究本部 本部長
	横田　孝弘	ＫＤＤＩ㈱ モバイルネットワーク開発本部 au技術企画部 坦当部長

参考資料２

「次世代の情報セキュリティ政策に関する研究会」開催経緯

日　程	議　題
第 1 回 （10 月 23 日）	○ 研究会の目的及び検討スケジュール ○ 情報セキュリティに関する脅威の現状　等 プレゼンテーション： ・小屋構成員（次世代ネットワークにおける脅威） ・中尾構成員（最近の見えない脅威と情報セキュリティ対策）
第 2 回 （12 月 5 日）	○ 検討の方向性及びとりまとめ方法 ○ 情報セキュリティに関する脅威及び課題　等 プレゼンテーション： ・山内構成員（最近のセキュリティ動向について） ・新井構成員（マルウェアの現況） ・小山構成員（次世代情報セキュリティ対策について）
第 3 回 （12 月 20 日）	○ 現在の情報通信環境における主な脅威・課題への対応 ○ 情報通信環境の変化と情報セキュリティ対策 ○ 情報セキュリティに関する脅威及び課題　等 プレゼンテーション： ・藤井構成員（デジタル情報家電の現状と課題） ・手塚構成員（「主要な環境変化」による影響と新たな課題について） ・中尾構成員（ITU-T における ID 管理の状況）
第 4 回 （1 月 31 日）	○ 情報通信環境の変化と情報セキュリティの脅威・課題 ○ 今後の情報セキュリティに関する脅威及び課題　等 プレゼンテーション： ・則房構成員（5 年後の情報セキュリティ） ・水越構成員（NGN とセキュリティ） ・独立行政法人情報通信研究機構（IPv6化に伴うセキュリティ環境変化とその影響について） ・横田構成員（モバイルセキュリティの動向と課題）
第 5 回 （3 月 6 日）	○ 中間報告書の骨子 ○ 今後の情報セキュリティに関する課題　等 プレゼンテーション： ・綾塚構成員（近い将来の情報セキュリティ～第 4 世代移動通信とユビキタスの視点から～） ・高倉構成員（巧妙化する malware の現状）

	・福地構成員（今後の情報通信環境の変化に対して必要となる情報セキュリティに関する取組）
第 6 回 （4 月 3 日）	○ 中間報告書のとりまとめ