資料５－５

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 骨子（案）

2008 年 3 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

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の利用が促進している。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重要性が増してきている。

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の利用・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事案に対処するため、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をもとに、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、これら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展開、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発生することが予想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対策等を抽出し、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

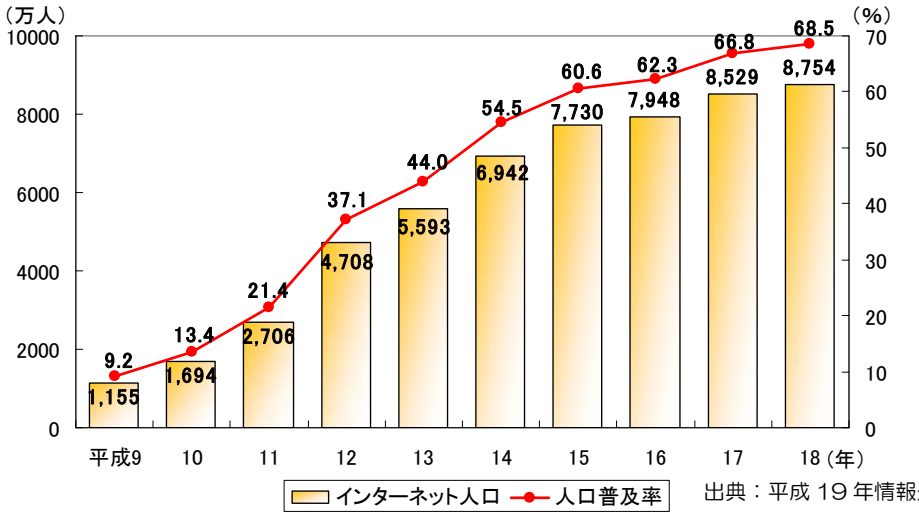
2．情報通信環境の現状

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

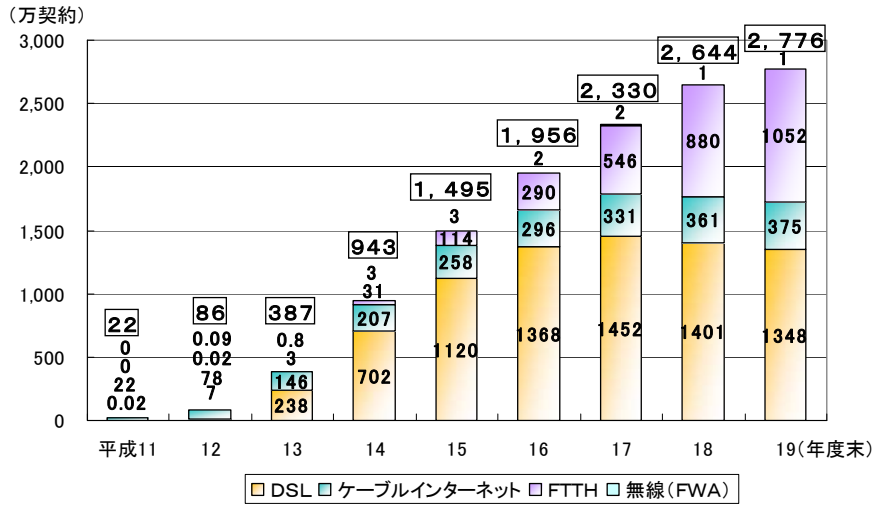
・ 2000 年頃以降、常時接続・ブロードバンド化が進展し、2006 年末のインターネット利用者数は 8,700 万人を超え、人口普及率にして約 70%に達している。

・ 2007 年９月末現在の我が国のブロードバンド契約数は 2,776 万件。うち、1,052 万件（38%）は、光ファイバ契約であり、年々その割合は増加。
インターネットは、多くの国民が利用する情報通信手段として定着・普及。

・ また、ブロードバンド接続環境は、2007 年９月末時点において、全世帯数の 95.7％である 4,951 万世帯で整備。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。



出典：平成 19 年情報通信白書



出典：平成 19 年情報通信白書

・ 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環境の整備が着実に進展。

2－2　モバイル端末によるインターネット利用等の進展

・ 携帯電話・PHS は、2007 年末現在での契約数が 1 億件を超え、また、モバイル端末（携帯端末・PHS、または携帯通信情報端末（PDA））によるインターネット接続利用者は、2006 年末現在で 7,086 万人に達している。

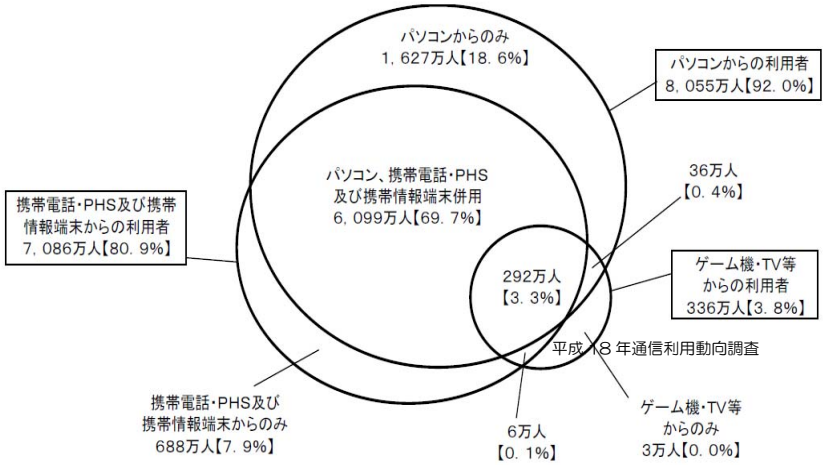
・ また、携帯電話利用者の約７割が、週 1 回以上インターネットの接続手段として利用している。

携帯電話・PHS の契約数

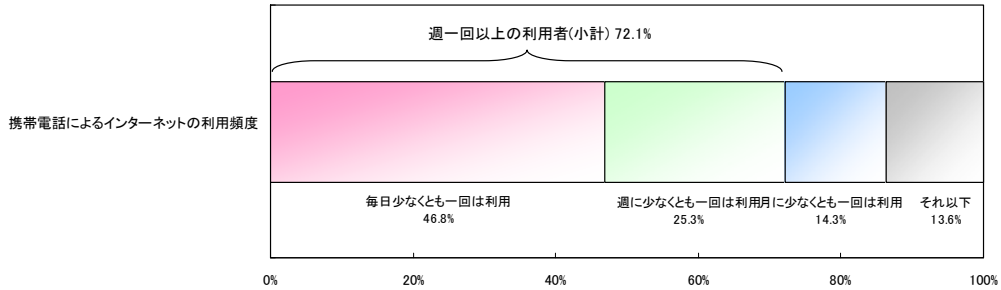
NTTドコモ	53,170,300
au	29,312,200
ソーカー	325,300
ソフトバンク	17,814,200
EMOBILE	238,500
ウィルコム(PHS)	4,626,400
総計	105,486,900

電気通信事業者協会(2008/1時点)

インターネット利用端末の種類（世帯構成員）



1



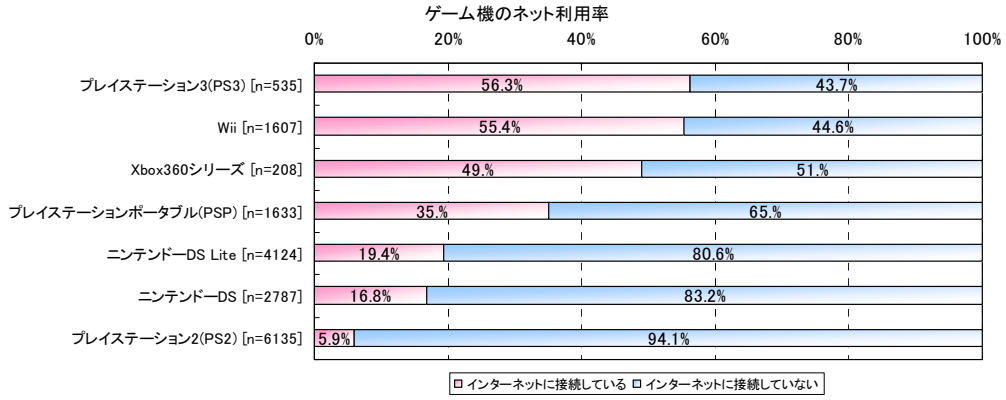
平成18年通信利用動向調査

2

3 ・ さらに、最近の携帯電話は、音声通話機能、インターネット接続やメール機能に
4 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
5 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おり、例えば、ある
6 携帯電話事業者の電子マネー機能を有する端末の普及率（2007 年３月時点）
7 は 40%近くにまで達している。

8 ・ その他、DVD 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
9 され始めており、特に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
10 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
11 てきている点が最近の特長として挙げられる。例えば、インターネット接続可能

なゲーム機の販売台数は急増しており、特に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割を占めるとの報告もある。

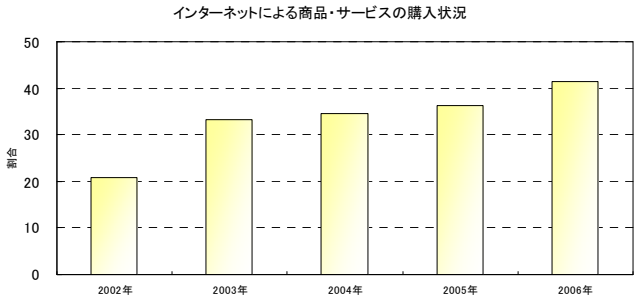


「日経マーケット・アクセスINDEX」2007年6月調査

２－３　社会経済活動の ICT 依存の増加

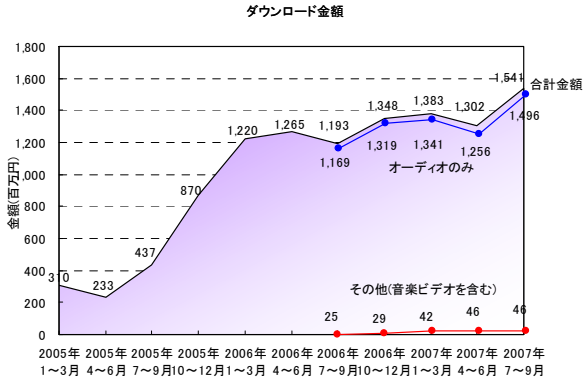
・ 我が国では低廉かつ高速な ICT 利用環境の整備が進むにつれ、様々な社会経済活動が ICT を利用して行われるようになってきている。

・ 個人における ICT 利用では、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 年までの過去５年間において増加傾向を示している他、音楽配信・ミュージックビデオ配信の利用なども進んできている。



通信利用動向調査（世帯編）

・



社団法人日本レコード協会の調査データより作成

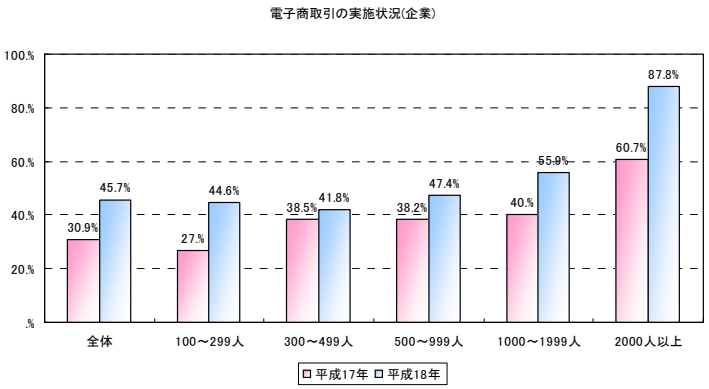
・ また、最近では、ブログ開設者数は 1,300 万を超え（2007 年 11 月現在）、10 人にひとりの開設率に上ると報道されるなど、SNS、ブログといった手段を用いて積極的に情報発信するケースが増大。

・ さらに、個人の情報発信は、それら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。個人が発信する莫大な情報が資産となって、製品の生産、販売等に影響。

・ 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。また、携帯電話でも本サービスが利用可能。今後もビジネス展開が進むものと期待。

・ 企業の ICT 利用では、例えば、電子商取引を導入している企業の割合は増加傾向であり、約３１％（2005 年）から約４６％（2006 年）と伸びを示している。

・ 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）と拡大するなど（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。



平成18年通信利用動向調査

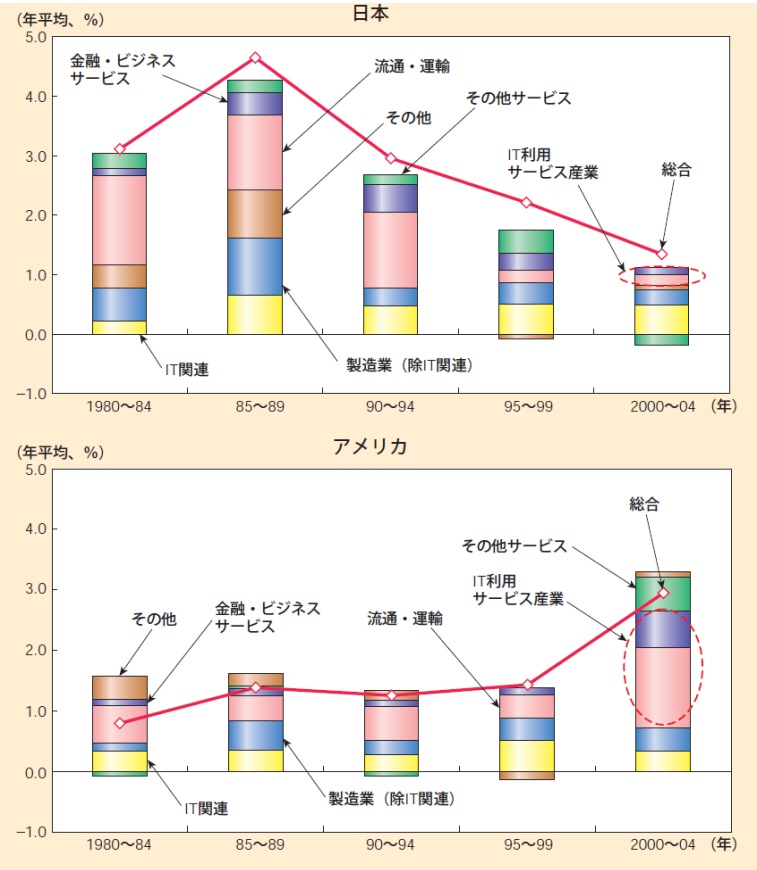
２－４　我が国の ICT 産業の現状

・ 我が国の成長に対する情報通信産業の寄与度は、大きなものとなっている。

・ 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おり、その間の平均成長率は 7.3%。主要産業の中で最も高い成長率を示している。また、情報通信産業は、我が国の実質 GDP 成長率に対して、1996 年以降一貫してプラスに寄与。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。

・ 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。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 倍であるのに対して、米国は 6.2 倍。また、同期間の GDP の推移では、我が国の 1.2 倍に対して、米国は 1.5 倍の伸びを示しており、情報化投資が GDP 成長を牽引。

・ さらに、流通・運輸、金融等の ICT 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、ICT 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い。その理由として ICT ネットワーク化や企業の組織改革の遅れと指摘されている。



図：平成 19 年度年次経済財政報告(内閣府)

2－5　ICT による生産性の向上と ICT 産業の国際競争力強化

・ 我が国の ICT 産業の現状を踏まえ、「経済財政改革の基本方針 2007」（平成 19 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」（平成 19 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み、「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」では、サービス革新戦略として、ICT 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。

・ 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。

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

・ 年々、社会経済活動の ICT 依存が進んできており、今後もその傾向は継続。また、これまで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、ICT が果たすべき役割はさらに拡大。

・ その一方で、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。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」の状況は、次のとおり。

・ **（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における ICT 利活用に伴うリスクが顕在化してきている状況。

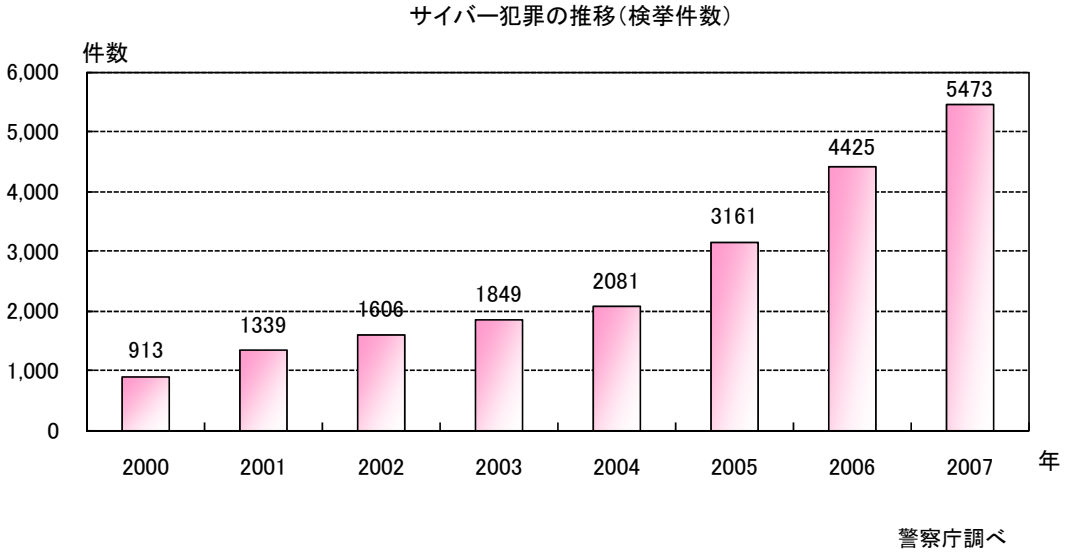
・ 例えば、海外においては、ネットワークを介して潜入したワーム、または内部犯行により、ガス、水道、電気（原子力発電所）のシステムが停止したり機能が低下したりする事件が報告されるなど、重要インフラ分野での IT 障害が発生。

・ 我が国においても、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、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。

・ 継続する情報セキュリティ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。

・ **（我が国におけるサイバー犯罪の状況）**

2007 年中のサイバー犯罪の検挙件数は 5,473 件で前年（4,425 件）より 23.7%の増加を示し、2003 年から過去５年間で約３倍に達している（「平成 19 年中のサイバー犯罪の検挙状況等について」2008 年２月、警察庁）。このうち、不正アクセス禁止法違反が 1,442 件で前年の 2.1 倍、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。



警察庁調べ

・ **（情報漏えい）**

ここ数年、企業や官公庁における情報漏えいは継続して発生。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（「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」（2007 年 10 月、NPO 日本ネットワークセキュリティ協会））。

・ また、2006 年に情報漏えいの対象となった人の数は、前年比の 2.5 倍に相当する約 2,200 万人に増加。情報漏えいの原因は、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%）の順で前年と同様の傾向。

・ なお、ワーム・ウイルスに関しては、前年（1.1%）よりも急増。これは、Winny や Share といった自動転送型ファイル共有ソフトに感染する暴露型のウイルスによる個人情報漏えいの増加によるものと分析。

・ **（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。その主たる要因は、

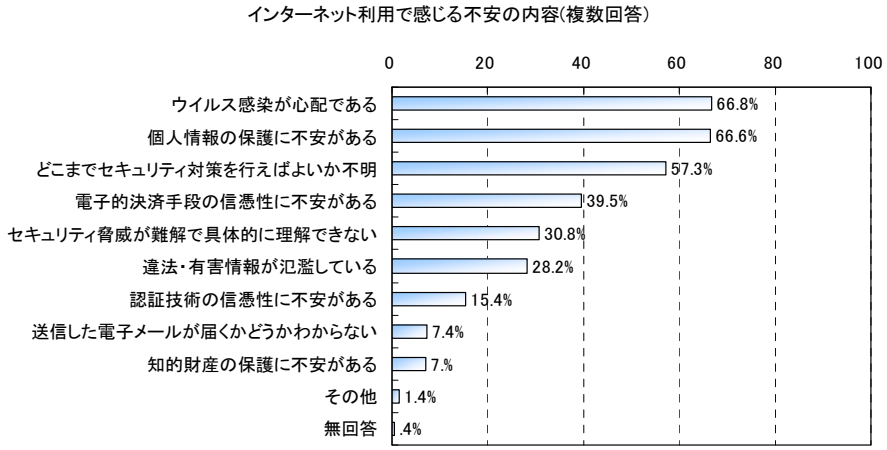
「ウイルスの感染が心配である」：66.8%

「個人情報の保護に不安がある」：66.6%

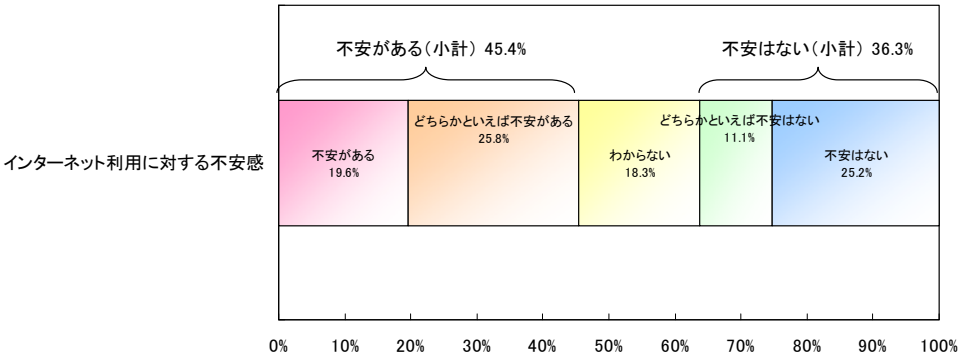
「どこまでセキュリティ対策を行えばよいか不明」：57.3%　の順。

・ 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%を超える結果であり、依然として不安感は解消され

ていない状況にある。



通信利用動向調査(総務省) 2006年末調査



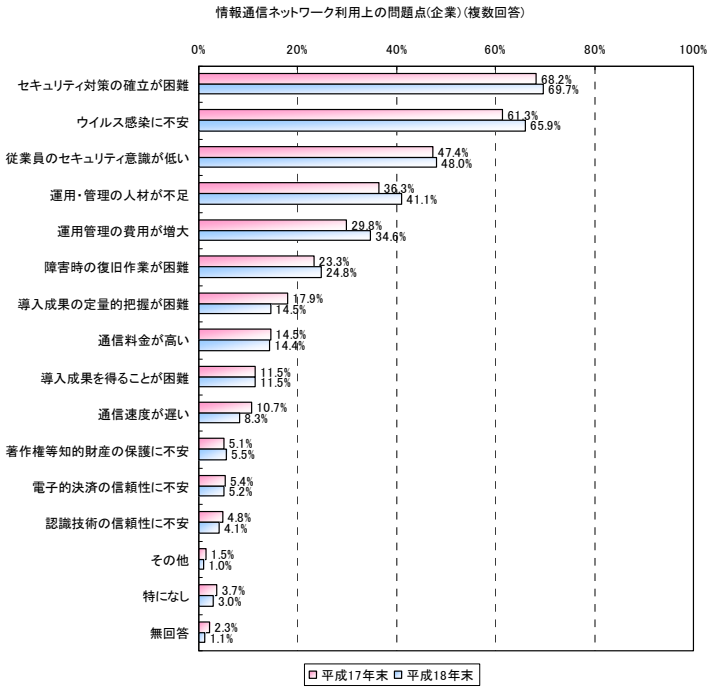
世論調査報告書(内閣府)　2007年11月

・ また、2006 年末現在、企業における情報通信ネットワークの利用上の問題点は、

「セキュリティ対策の確立が困難」: 69.7%

「ウイルス感染に不安」: 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。



平成18年　利用動向調査(総務省)

・ **（利用者のセキュリティ対策実施状況）**

最も基本的な対策であるパスワード管理について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。

また、子供がインターネットで何をしているか、親子でオープンに話す家庭の割合も、日本は 22%と最下位となっている。（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」）

3．情報セキュリティ対策の現状と課題

・ ICT が安心・安全に利用できるようにするためには、現状の情報セキュリティ対策における課題、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。

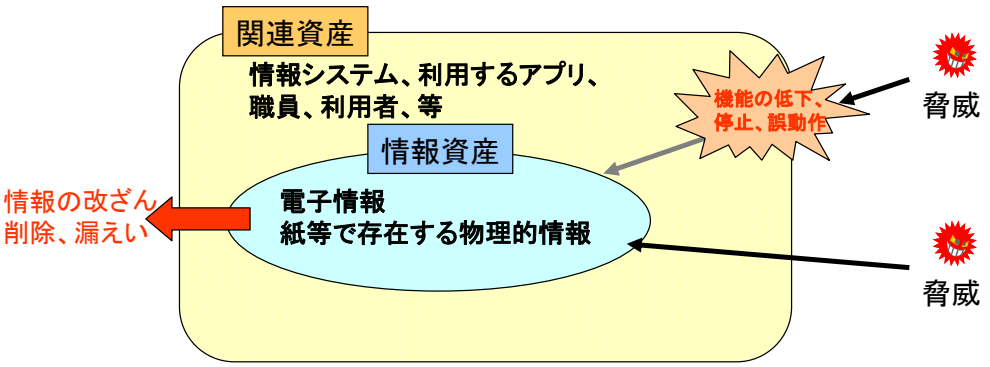
・ こうした観点から、本研究会では、①現在の情報通信環境における脅威・課題、及びその対策状況を整理し、対策が不十分な項目や更に効果的な対策を講ずべき項目を洗い出す、②今後３年から５年における近い将来における情報通信環境及びその変遷過程における環境の変化を捉え、そこで発生する可能性が高い主な脅威・課題を抽出し整理する、という２分類で、検討を進めてきている。

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

・ 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、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を以下のとおりに整理。

・ **（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、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、人的資産といった関連資産である。



・ **（主な情報セキュリティ脅威）**

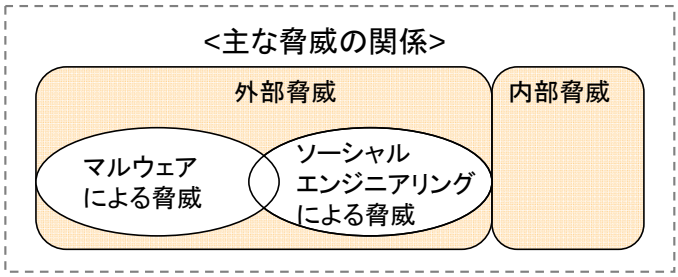
主な情報セキュリティ脅威は、以下の４分類とする。

ア）ボットウイルス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）



	脅威の個別具体例（手法及び目的）	
ボットウィルス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 •ウィ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（高度な成りすまし） （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、PWD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

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は、コンピュータ等の情報システムが利用され始めて以来、ソフト・ハードの不具合やウイルス感染、自然災害といった外部脅威、利用者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。

・ 一方、ICT 利用の進展に伴い、コンピュータが相互に接続しネットワークを構成したことにより、ウイルスの感染経路が変化し、またそれらがもたらす経済的・社会的影響が増大。昨今の情報セキュリティ脅威の多くは、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できる。

・ 90 年代前半、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。

・ 90 年代後半から 2000 年代当初にかけて、マクロ型ウイルス、Melissa や Love Letter 等のマスメーリング型のウイルス、MSBlaster、CodeRed 等のソフトウェアの脆弱性をつく大規模感染型に変化。また、これらウイルス感染の目的の多くは、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。

・ 数年前からは、DoS・DDoS 攻撃、多量のスパムメール送信、情報詐取など、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。その代表的なものが Bot（ボット）ウイルスであり、現在のネットワーク上の脅威の殆どは、ボットが原因になっていると言われている。

・ なお、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を送信したり、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・組織化しており、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。

・ 最近は、さらにウイルス感染の手法がより高度化・巧妙化し、脅威の潜行化が進んできている傾向。例えば、正規の Web サイトに不正なコードを埋め込み、その感染した正規の Web サイトを閲覧しただけでウイルスに感染させたり（ここでは「Web 感染型」という。）、ウイルスを感染させたい少数の相手にカスタマイズしたメール送付して感染させる、ターゲット型／スピア型と言われる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報告されている。

	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）	ネットワークの脅威 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

３－３　情報セキュリティ脅威の現状及び今後の予測

・ 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。

・ これら現在発生している情報セキュリティ脅威は、今後も更に高度化することが容易に想像される。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にも量的にも爆発的に増加すると予想されることから、より対策が困難になると考えられる。

・ （ボット等マルウェアによる脅威の現状と今後の傾向）

　ボットは、主として、コンピュータから情報の詐取、迷惑メールの発信、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す。

・ 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の２から 2.5%。当時のブロードバンドユーザ数にして４０万から 50 万人との試算もあり、「サイバークリーンセンター」等の取組みを政府としても推進中。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は、世界的にも継続的な課題。

・ 実際、流通している全メールのうち約 80%がスパムメール(Symantec：2007 年 12 月調査)で、そのほとんどがボットによるものとされている。

・ また、これまでのボットの感染手法は、ワーム型の感染が主流であったが、ワープロや表計算ソフト等の脆弱性を利用したり、Web 感染型、ターゲット型/スピア型に変化。さらに、ネット上で販売されている複数の Web の脆弱性を格納した攻撃ツールを利用することで、容易に攻撃を実施できる状況にあることが悪化の一要因。

・ 国内事例１：
　2007 年 4 月に都内のある出版社がボットによる DDoS 攻撃を受けた事例
海外事例１：
　米国連邦捜査局（FBI）等による「OPERATION BOT ROAST の事例
海外事例２：
　カナダ・ケベック州警察が 2008 年 2 月、ボットを操る犯罪集団を逮捕
海外事例３：
　エストニア共和国への大規模 DDoS 攻撃の事例
海外事例４：
　「Storm Worm」の事例
海外事例５：
　「MPack」、「IcePack」の事例

・ **（ソーシャルエンジニアリングを駆使した脅威）**
　フィッシングに加え、スピア型メール（ターゲット型メール）による攻撃が発生。通常のウイルス対策ソフトでは発見し辛いなど、対策が後手に回るケースが多いと言われている。今後もソーシャルエンジニアリングを駆使した脅威は、巧妙化していく傾向。

・ 国内事例１：
　国内のフィッシングの状況
国内事例２：
　スピア型メールの事例
海外事例１：
　海外のフィッシングの状況
海外事例２：
　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サイトの事例

・ その他の事例

P2P ファイル共有ソフトにおけるマルウェアの流通状況

３－４　情報セキュリティ対策の取組み状況と課題

・ 対策実施主体を次に示す７つに分類し、対策の状況と課題を整理。

（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

・ **（ボット等マルウェア感染による脅威への取組み状況）**

ボットウイルス等マルウェアによる脅威に対する取組

	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
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

・ 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）及び利用者（企業）による対策が主となっている。

・ ボット対策については、2006 年 12 月から総務省と経済産業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」を立ち上げ、ISP 等と協力しながら、

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、感染防止策等について周知・啓発活動を実施しており、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されている。

・ また、誤ってウイルスに感染してしまった場合などに、身近で簡単に相談等ができる取組みがより一層重要との指摘がある。

・ 一方、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或いは停止、又は不正な Web サイトへのアクセスを制限或いは禁止するような積極的な取組みの必要性も指摘された。

・ 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。また、海外との連携対応の必要性等についての指摘もある。

・ **（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

・ 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も、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、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、情報セキュ

リティに関する基本的なリテラシーの向上が重要との指摘がある。

・ 特定の組織等をターゲット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、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されるとの指摘もある。

・ **（外部脅威及び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)（B）
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)（B）
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)（B）
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

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

・ 外部脅威と内部脅威については、主として利用者（企業）における対策として、企業における内部統制の強化を考慮し、継続的な対策の実施・改善が望まれる。

・ 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、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必要。

・ 現状の対策や課題に関する共通的な事項として、対策実施主体である利用者（個人）については、特に、今後は、年少者や高齢者などこれまでインターネットを利用してい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。こうした必ずしも情報セキュリティ対策に対する意識が高くないと考えられる利用者である、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いう指摘が多数なされている。

・ 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、こうしたネットワークを通じた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。

3―5　現状の情報セキュリティ対策における主な課題とその対応策

・ 現在発生している脅威の状況等を踏まえると、以下に示す課題について、重点的に取組むことが必要。なお、引き続き多様化する ICT サービスの安心・安全な利用のためには、利用者（個人・企業）による情報セキュリティ対策が基本的かつ重要な対策となっていることから、政府機関等における ICT 利用にあたっての基本的なリテラシーの向上のための普及啓発等の取組みを始め、ここで挙げるもの以外の対策についても、継続的な取組みが必須。

・ **（ボット等マルウェア感染手法の巧妙化等への対策）**

Web 感染型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型など、次々と巧妙化・高度化する新しい感染手法への対応を強化すべく、こうした事象を高度に観測・把握・分析し、障害を低減・除去する一連の対策技術の継続的な研究開発に取組むことが重要。

・ 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、従来型の受動的な観測システムに加え、利用者サイドの状況を積極的に把握するためのネットワークインシデントの観測網の強化が必要。

・ また、益々感染事実が把握しづらい状況となっていることを考慮し、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、分野を超えた迅速な情報共有等の連携の充実が望まれる。なお、情報共有等の実効性を高めるため、事故状況等の報告の義務化の是非についても検討すべきである。

・ **（事案解決のための国際連携の促進）**

ボットにより発生する脅威の多くは、複数の国を跨り、広範囲に渡る状況である。こうした事案に対処していくためには、諸外国との情報共有等の連携が必要。

・ このため、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・連携体制の構築及び強化が挙げられ、その具体化を検討すべき。

・ **（基本的な情報セキュリティ対策が徹底できる社会の構築に向けた取組の検討）**

今後の ICT の利用者層の広がりを考慮し、いわゆる「永遠のビギナー」における情報セキュリティ対策が必要不可欠な課題。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について検討を進めるべき。

・ 具体的には、以下のような取組が挙げられる。

① 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検証を進めることが必要。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可能性や、ウイルス感染の手法等が、より解析や対処が困難になる可能性について十分に考慮すべきである。

② 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、フィッシングサイトやマルウェア配布サイトなど悪性な Web サイトへのアクセスを防止等するため、信頼性の高いレピュテーション DB（危険な Web サイトに関するリスト）の構築とその運営方法について実証を促進することが必要である。

③ 事前の情報セキュリティ対策の充実に加え、実際にマルウェアに感染して被害を受けた場合等のために、身近にかつ気軽に相談できるようなユーザサポート体制を充実することが必要である。

なお、このユーザサポート体制における個人や組織、地域等によるレベル（能力）に差が生じないよう、一定程度のスキルを保証（認定）する仕組みを併せて検討すべきである。

４．近い将来のＩＣＴ環境と情報セキュリティ政策のあり方

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。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は、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。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るべきである。

・ こうしたことから、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について可能な限り洗い出しを実施。

・ 情報通信環境の変化の状況について、以下のとおり分類・整理。

・ **（社会変化の状況）**

〇日本の少子化、高齢化は益々進展し、65 歳以上の推計人口は、2030 年には 31.8%になると予測。

〇団塊の世代が 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。一方、新たな消費活動の主体に成長することが期待。

〇仕事と日常生活のバランスをとった、多様性を尊重した活力ある社会へ変化。また、ライフスタイルの多様性、人口構成の変化、環境問題への対応等から、在宅勤務などの多様な勤務形態が増加。

〇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）

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次世代無線システム等無線アクセスの多様化

オ）2010 年頃、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が就業人口の 2 割に達する。

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中小企業等でのＩＣＴ利用による生産性向上

ア）ＡＳＰ・SaaS の市場規模が 2010 年には 1.6 兆円に達するとの予測があるなど、ＡＳＰ・SaaS をはじめとした ICT 利用による生産性や効率性の向上

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

・ 情報通信環境の変化等において発生、継続、又は拡大すると考えられる情報セキュリティの主な脅威や課題は、以下のとおり。

①情報通信ネットワーク技術の高度化が一層進展。
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
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
④消費活動等の変化
⑤中小企業等でのＩＣＴ利用による生産性向上
に関連する脅威等について、第４回研究会の資料４－６に基づいて記載。

・ 近い将来での「ユビキタスネット社会」における主な脅威と課題は、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
イ）OS、アプリケーションの共通化により、１つの脆弱性が及ぼす対象範囲が拡大。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
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
エ）情報の保持、管理する場所・主体の変化

②脅威の対象となる情報の増加
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
イ）仮想世界の通貨等、新しい価値ある情報の流通が増加

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
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

エ）情報セキュリティ対策の主体、責任範囲が不明確

オ）情報セキュリティに関する事案が発生した場合に、迅速かつ効果的な対策を実施するための（国内外の情報共有・連携を含む）体制が確立されていない

5．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

・ 第４章において述べたとおり、近い将来のＩＣＴ環境においては、情報通信技術の高度化、サービス提供や消費活動の多様化等を背景に、利用者数、ネットワークに接続される機器・端末数、ネットワークを流通する情報資産が爆発的に増加することにより脅威が増大。

・ また、脅威が高度化・潜行化する中で、いわゆる「永遠のビギナー」が増加することも情報セキュリティ対策の困難性を増す要因。

・ さらに、これまでの垂直型のビジネスモデルに加え、ソフトウェア・ハードウェアの製造・販売事業者、電気通信事業者、サービス提供事業者等が協調・連携して実現される水平展開型のビジネスモデルへの転換が進むとの予測にも留意が必要。

・ こうした中、少子高齢化等の問題を払拭し、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には、ひとつには、多数の関係者が絡み合う複雑系において、利用者の利便性を可能な限り損なうことなく情報セキュリティを確保できる環境として、「利用者（利便性）、情報通信環境、情報セキュリティが共生（共存）する新しい ICT の社会モデル」を構築することが必要。

・ その他、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、Ｐ２Ｐネットワーク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の高度化技術等への対応が必要である。

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

利用者が携帯電話端末・スマートフォン、情報家電機器等の様々な端末・情報通信機器等を駆使し、多様なサービスを利用できるよう、利便性を確保すると共に、併せて情報セキュリティ対策が実施できるよう、サービス提供側が業界を越えて連携し、サービス提供側の機能として情報セキュリティ対策を実装（提供）することについて、検討を進めるべきである。

〇本モデルの具体的な実装を検討するため、ソフトウェア・ハードウェアの製造・販売事業者、電気通信事業者、様々な業種のサービス提供事業者等が参加する検討スキームを構築すべきである。

〇OS やソフトウェアの共通化による脅威の広域化への対応策、プラットフォーム機能のオープン化を含む複数のレイヤー間が協調する情報セキュリティ対策の実施方法（責任領域の明確化）等について、継続的に検討することが必

要。

○具体例として、個人認証・端末認証やシングルサインオン技術、ネットワークを流通する情報の保護・管理技術、接続された端末等の適切なセキュリティを自動的に確保する技術等を複合的に組合せ、利用者が難しい設定をすることなくワンストップでセキュアなサービスが利用できるようなモデル環境の実証・検証が考えられる。

○なお、検討に当たっては、利用者の端末がマルウェアに感染し、他人に迷惑を掛ける恐れがあることを考慮し、利用者の社会的責任として、インターネット等を利用する際には必ず一定レベルの情報セキュリティ対策を講じておくことを基本とする社会モデルとして実現することについて、コスト負担のあり方も併せ、検討を進めるべきであると考えられる。

・ **（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）**

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、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 技術がより安定した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。

・ **（Ｐ２Ｐネットワーク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）**

管理者不在となるＰ2P ネットワーク、消費者が様々な情報発信をするＣＧＭ等において、事実に反する情報が意図的・非意図的に流通す場合やフィッシング等ソーシャルエンジニアリングによる攻撃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ることから、これらの利用にあたっては、利用者自身が提供される情報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。

・ こうした状況において、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の実現方法について検討することが必要である。

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、その移行過程を含めて利用環境の変化により生ずる課題等を抽出し、そのうち、優先的に取り組むべき主な項目を抽出・整理してきたところ。

今後は、その主な項目について、実施していく上で考慮すべき等に関して、具体的な検討を加えていくことが必要であると考えられる。その際、国際連携のあり方等については重要な視点であることから、こうした観点を含み、本研究会として更に検討を進めることが必要であると考えている。

（今後の予定）

４月上旬　第６回研究会　中間報告書案とりまとめ
７月中　　最終報告書案とりまとめ