資料１０－２

次世代の情報セキュリティ政策に関する研究会

報告書（案）

2008 年 7 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、社会経済活動の ICT 依存度が高まる一方で、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が生じており、こうした問題に適切に対処し、情報セキュリティの確保を図ることが、これまで以上に重要となってきている。

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み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、情報通信ネットワーク基盤やインターネット等の様々な ICT サービス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サイバー攻撃の巧妙化・高度化、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、その環境も急速に進展していることから、このような近い将来の ICT 環境及びその変遷過程において生じるであろう情報セキュリティ上の課題を抽出し、それに備えた対策を講ずることが極めて重要である。

以上を踏まえ、本研究会では、現状の ICT 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年後といった近い将来における ICT 環境を想定し、その変遷過程を含めた ICT 環境の変化により生ずる課題や問題点等を抽出し、これらを解決するために必要となる対策の導出等、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きたところである。

本報告書は、本研究会での検討内容を取りまとめたものであり、今後、総務省をはじめとした政府機関、電気通信事業者、ICT サービス提供事業者、情報通信機器

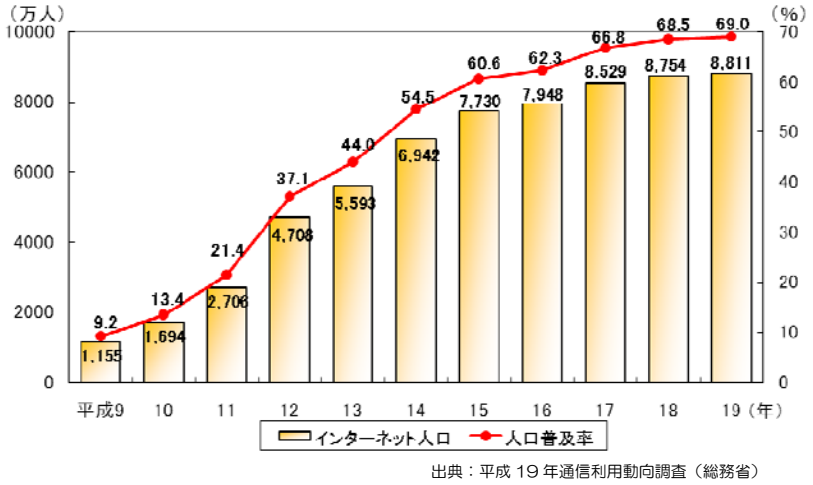
関連のベンダ、インターネット利用者等によって、ここに掲げる情報セキュリティを確保するための各種対策等の着実な実施、また施策の具体化に向けた継続的な検討が行われることによって~~り、近い将来における~~安心・安全な ICT 環境整備の一助となり、我が国の ICT 利用による生産性の向上や社会経済活動の活性化に寄与することを期待するものである。

2．ICT 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

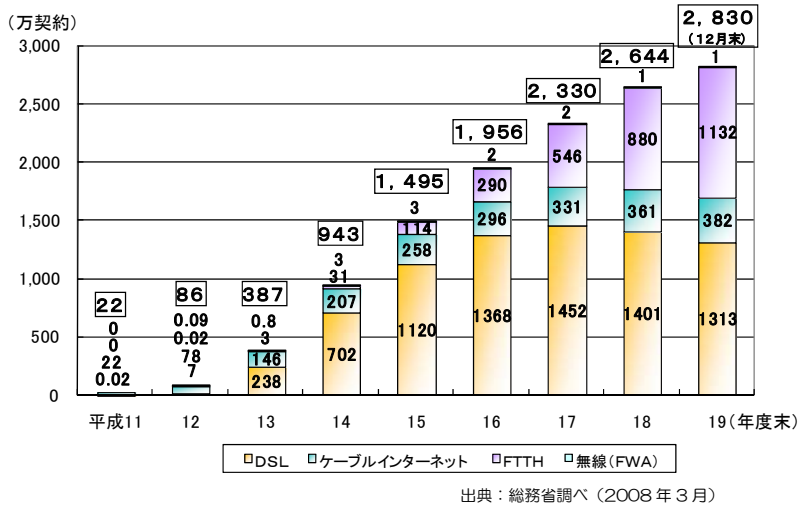
1990 年代中頃から徐々に一般へも普及した我が国のインターネットは、90 年代後半まではアナログ回線や ISDN 回線によるダイアルアップ接続が主流であったが、2000 年頃以降、ADSL や光ファイバ回線による常時接続・ブロードバンド化が浸透するとともに利用者数も増大し、2007 年末のインターネット利用者数は 8,800 万人を越え、人口普及率にして約 70%に達している[1]【図表 2-1 参照】。

特に、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 万件に達し、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 年通信利用動向調査（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

[1] 1997 年末のインターネット利用者数は約 1,200 万人であり、人口普及率にして約 9%であった。

また、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挙げられるブロードバンド接続環境[2]の整備については、2007 年 12 月末時点において、既に全世帯数の 95.8%である 4,953 万世帯に達しており、さらに政府として 2010 年度までにブロードバンド・ゼロ地域を解消することを目指している。加えて、我が国のブロードバンド料金として DSL の利用料金の推移をみてみると、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低廉かつ高速に利用できる環境の整備が着実に進んできていることが窺える。

２－２　モバイル端末によるインターネット利用等の進展

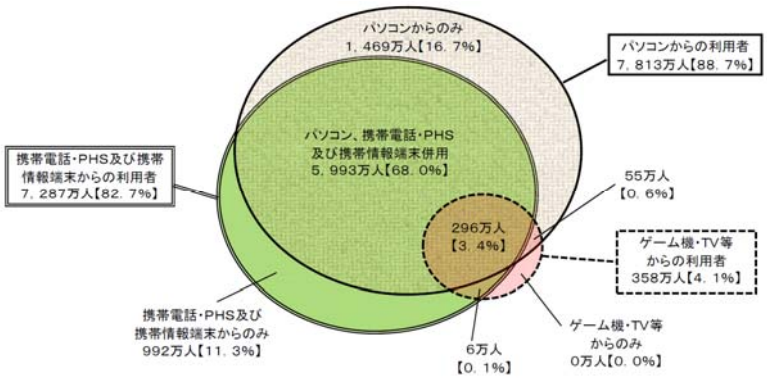
ブロードバンド・インターネット接続環境の整備に加え、携帯電話・PHS は、2007 年末現在でその契約数が 1 億件を越え、2008 年 3 月末時点で 1 億 800 万契約に達しており、広く国民が所有する情報通信手段となっている。このようにほぼ国民一人が 1 台を保有していると言えるまで普及した身近な情報通信手段である携帯端末・PHS、または携帯通信情報端末（PDA）といったモバイル端末を使ってインターネットに接続する利用者は、2007 年末現在で 7,287 万人（前年比 201 万人増）に達しており、また携帯電話利用者の７割強が、週 1 回以上インターネットの接続手段として利用しているなど、モバイル端末によるインターネット接続が浸透してきている【図表 2-3 から図表 2-5 参照】。

NTTドコモ	53,544,500
au	30,292,900
ソフトバンク	18,952,800
EMOBILE	555,400
ウィルコム(PHS)	4,613,900
総計	107,959,500

出典：電気通信事業者協会調べ（2008 年 5 月末）

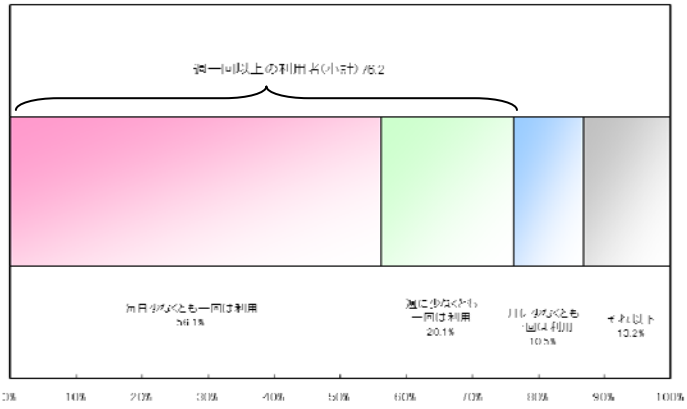
図表 2-3：携帯電話・PHS の契約数

[2] ここで、ブロードバンドとは、一般世帯で固定的に利用される FTTH、ADSL、ケーブルインターネット、無線(FWA)を指す。



出典：平成 19 年通信利用動向調査（総務省）

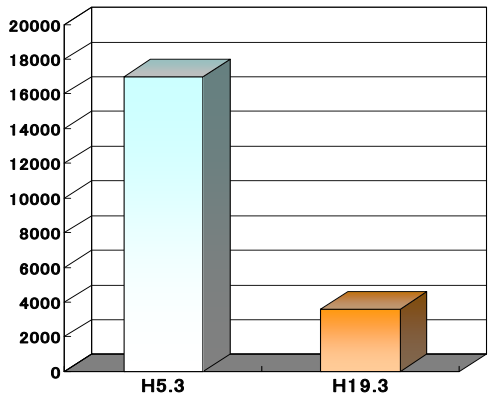
図表 2-4：インターネット利用端末の種類



出典：平成 19 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。さらに、携帯電話の料金についても、2007 年度末時点と 1992 年度末時点とを比較した場合で約 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窺える。【図表 2-6 参照】。

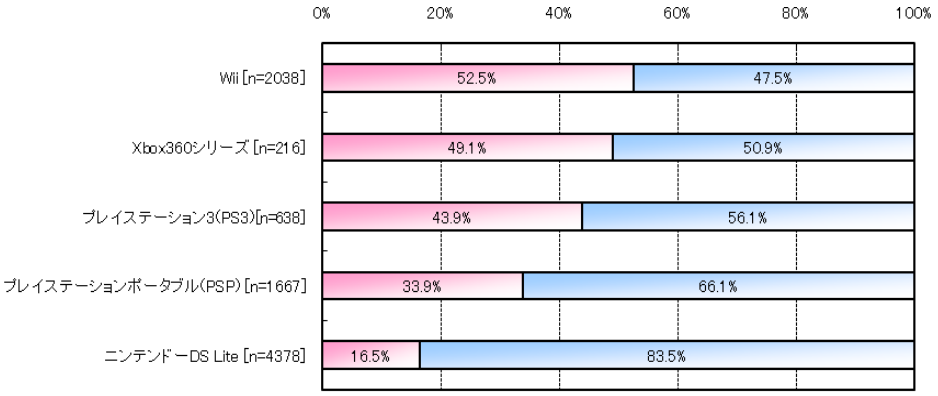


※ H5.3.25から「800MHzﾃﾞｼﾞﾀﾙ方式」開始
※ H5.3の料金は、無料通話分を含まないプランAの料金
※ H19.3の料金は、無料通話分1,000円分を含むタイプSSの料金

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いる。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をもつだけではなく、専用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[3]しており、その多くでインターネット接続及び Web ブラウジングが可能となっている。また、国内での据置型ゲーム機の利用者のおよそ５割が、当該ゲーム機からインターネット接続をし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 12 月）

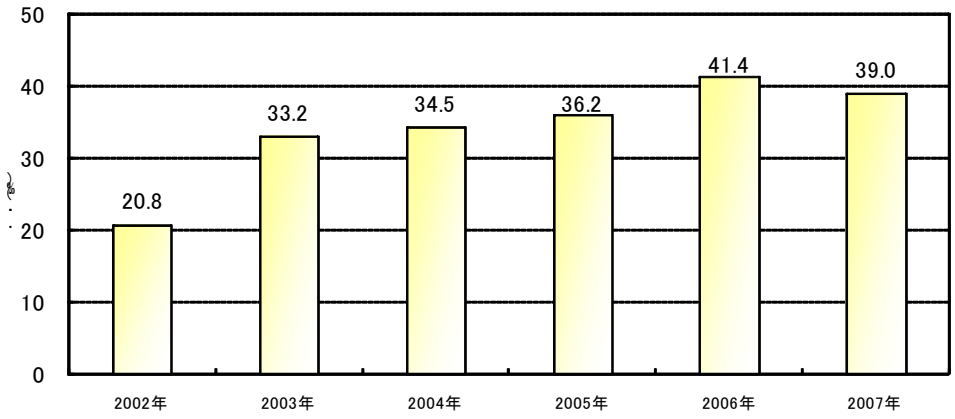
図表 2-7：主なゲーム機によるインターネット利用率

[3] 主要なゲーム機の国内外累計販売台数(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)

２－３　社会経済活動の ICT 依存の増加

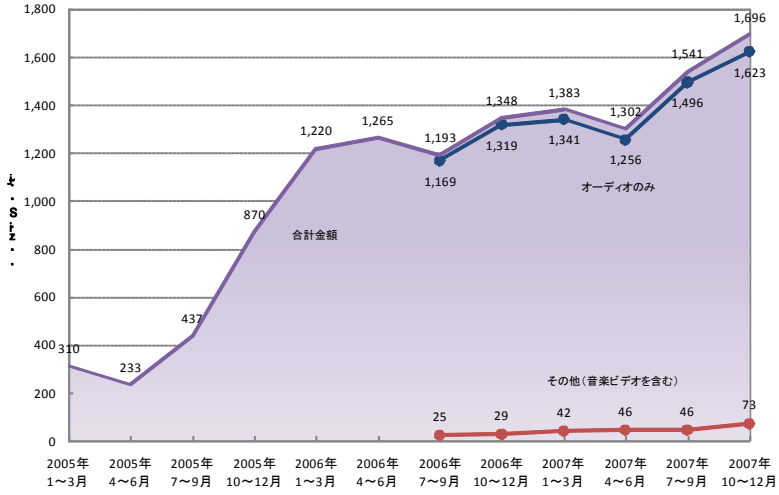
我が国では前述のとおり、低廉かつ高速なインターネット利用が可能となっていることに代表されるように、ICT 環境の整備が進んでおり、これにより様々な社会経済活動が ICT を利用して行われるようになってきている。

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、インターネットを通じて商品などを購入したことのある人の割合は、ほぼ４割にまで達している他、音楽配信・ミュージックビデオ配信の利用が急速な伸びを示す等、B2C の電子商取引が身近なものになっていると言える【図表 2-8、図表 2-9 参照】。



出典：平成 19 年通信利用動向調査（総務省）を基に作成

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

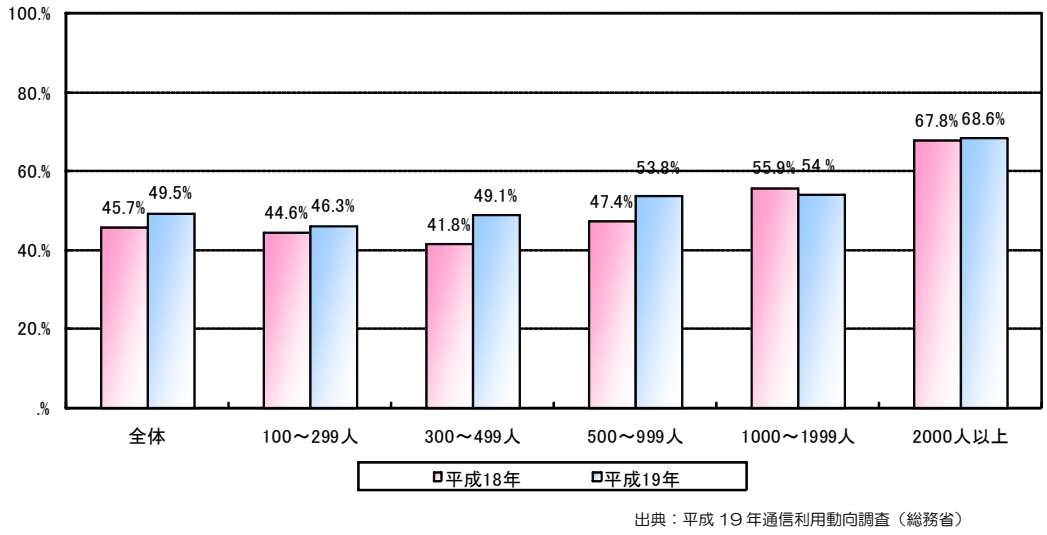
図表 2-9：有料音楽配信による売上実績

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きている。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[4]。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といわれている。

その他、セカンドライフに代表される３次元仮想世界（バーチャル世界）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 のみから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等により、こうしたバーチャル世界での企業によるビジネス展開がより一層進むものと期待される。

一方、企業の ICT 利用につ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をみてみると、45.7%（2006 年）から 49.5%（2007 年）と増加傾向を示している。【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[5]、企業における ICT 利用が進展しており、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 19 年通信利用動向調査（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のーつに広告費がもそのーつであるが、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、

[4] 2008 年 1 月 27 日付日本経済新聞（1 面）による。
[5] 2007 年 5 月、「電子商取引に関する市場調査」（経済産業省）による。

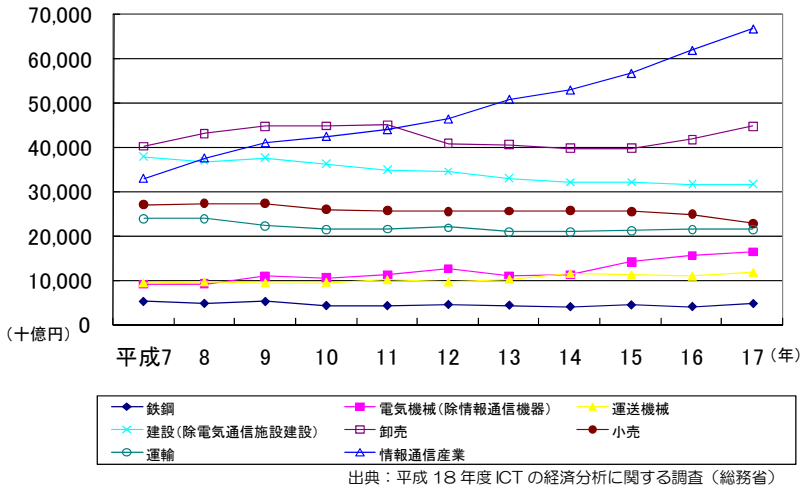
新聞・テレビには及ばないものの、雑誌とラジオの広告費を上回る結果となっている[6]。この要因としては、通信回線のブロードバンド化によるインターネットでの動画視聴が一般化してきたことや、インターネット広告がより表現力が豊かになったことで企業のブランディングにも活用されるようになってきたこと等が挙げられている。さらにテレビ CM と連動してインターネット検索への誘導を促すクロスメディア手法が定着してきているなど、企業活動におけるインターネットの果たす役割が大きくなってきていると考えられる。

２－４　我が国の ICT 産業の現状

我が国の社会経済活動の ICT 依存が高まる状況において、我が国の経済成長に対する ICT 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、ICT 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、ICT 産業は、1996 年以降、一貫してプラスに寄与しており、2005 年の ICT 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】。

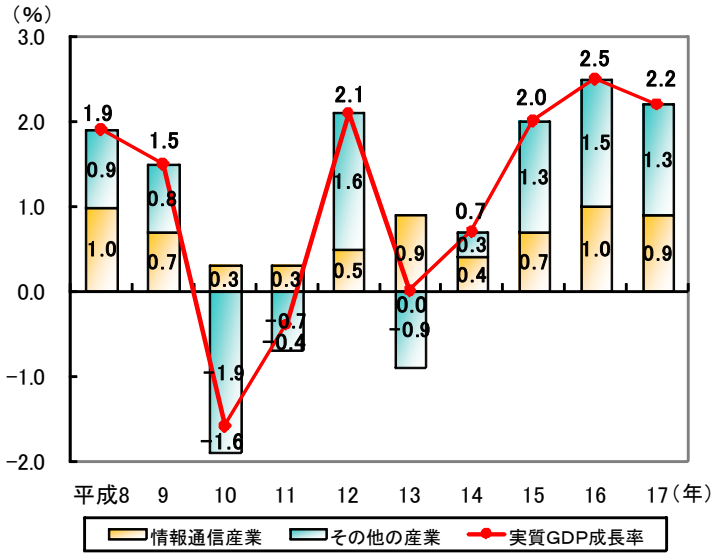
一方、情報化投資による経済成長についての日米比較においては、我が国は米国に対して大きく水を開けられている状況である。具体的には、1990 年から 2005 年までの情報化投資の推移を比較した場合、我が国の増加率は 1.9 倍であるのに対して、米国は 6.2 倍に達している。また、同期間の GDP の推移では、我が国が 1.2 倍となっているのに対して、米国は 1.5 倍の伸びを示しており、情報通信白書（「情報通信に関する現状報告」（平成 19 年度版））によると、情報化投資が GDP 成長を牽引してきたとされている【図表 2-13 参照】。



出典：平成 18 年度 ICT の経済分析に関する調査（総務省）

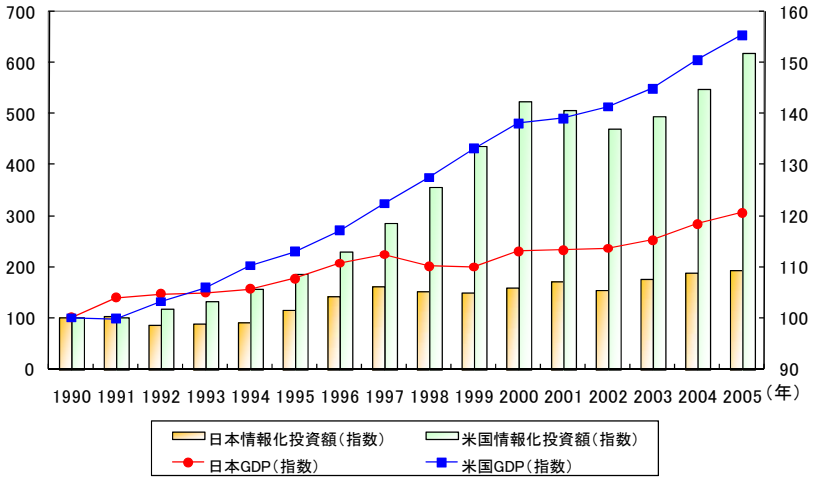
図表 2-11：主な産業の実質 GDP の推移

[6] 2008 年 2 月、「電通 NEWS RELEASE」（電通）による。



出典：平成 18 年度 ICT の経済分析に関する調査（総務省）

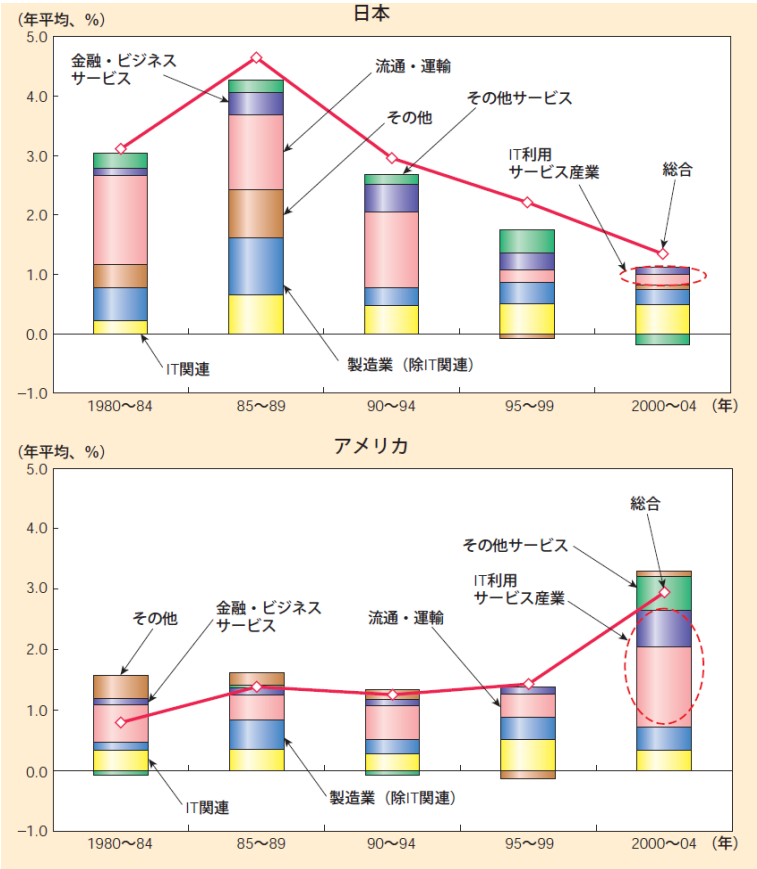
図表 2-12：実質 GDP 成長率に対する成長率の寄与



出典：平成 18 年度 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

我が国では、これまで述べてきたとおり、様々な社会経済活動における ICT の利用が進展してきており、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状況において、我が国が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[7]における ICT の利活用が進むにつれ、重要インフラにおける IT 障害の発生が社会問題化している。

海外の例としては、2008 年 1 月、米国において、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、下水システムを不正に操作して 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。また、2008 年５月には、大手銀行において、システム統合初日、提携金融機関の ATM での当該銀行の一部入金取引が出来なくなるなどといったシステム障害を発生したケースがあった。

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

---

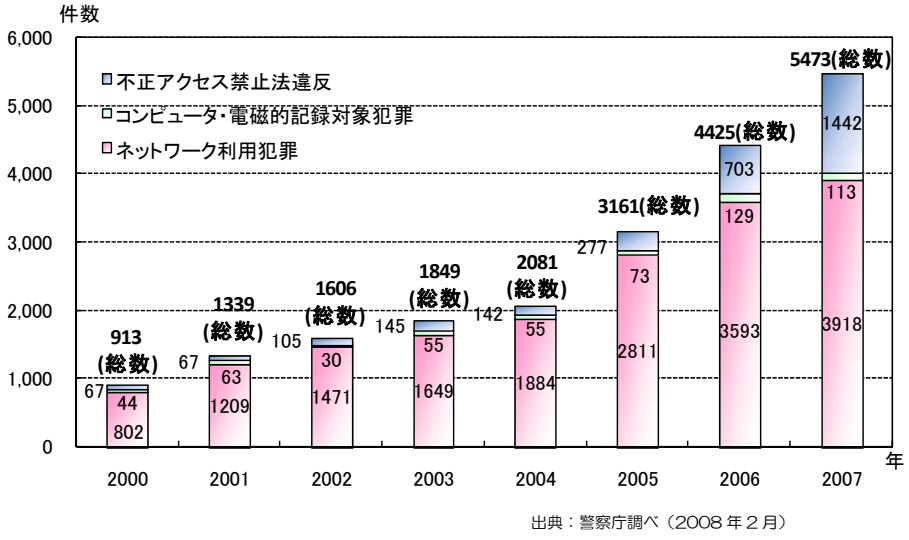
[7] 重要インフラは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用が不可能な状況に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものであり、「重要インフラの情報セキュリティ対策に係る行動計画」（2005 年 12 月、情報セキュリティ政策会議決定）においては、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流の 10 分野とされている。

組んでいる状況である。

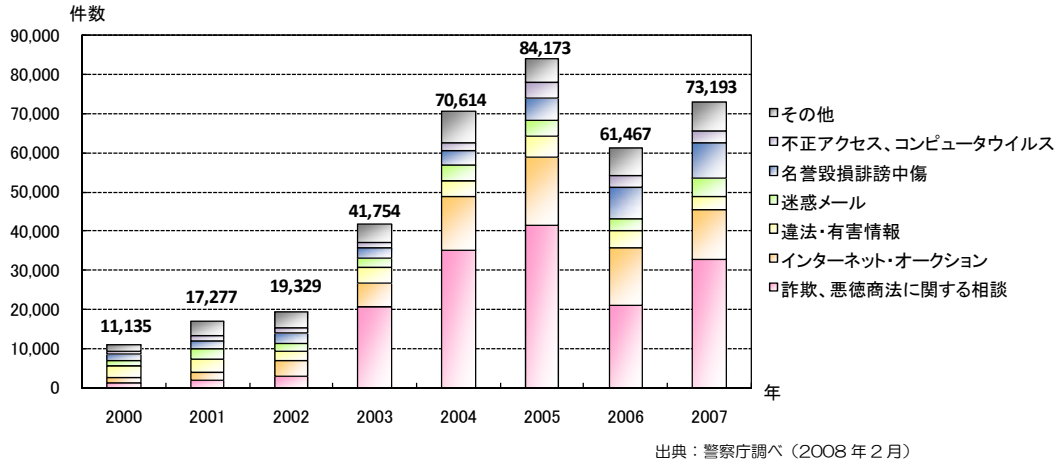
（我が国におけるサイバー犯罪の状況）

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 倍に達した状況である。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窺える。

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。



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）

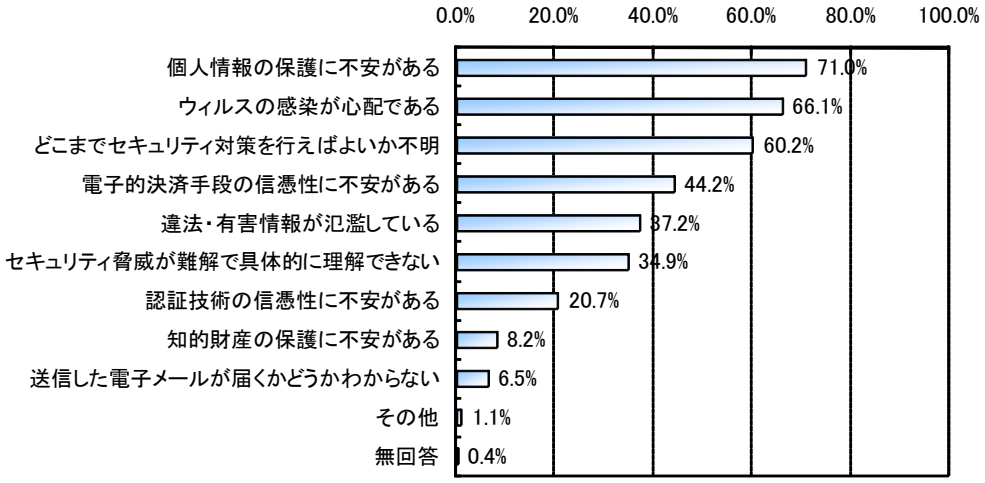
企業や官公庁における情報漏えいは、ここ数年来継続して発生しており、2008 年に入ってからも病院の患者情報や発電所の情報等といった重要インフラ関連の情報漏えいが、ファイル共有ソフトに関連する漏えい事案として発生している。

2008 年５月に公表されている「2007 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. 1.0」（NPO 日本ネットワークセキュリティ協会）によると、2007 年に新聞やインターネットニュースなどで報道された個人情報漏えいインシデントの件数は、前年と比較して 129 件減少し、864 件であった。一方、漏えい人数（情報漏えいの対象となった人の数）については、前年と比較して大幅に増加し、約 3,053 万人（＋約 800 万人）となっている。これに伴い、想定損害賠償総額も大幅に増加し、２兆円の大台を突破したとされている。

また、情報漏えいの原因としては、「紛失・置き忘れ」(20.5%)が最も多く、続いて「管理ミス」(20.4%)、「誤操作」(18.2%)、「盗難」(16.6%)、「ワーム・ウイルス」(8.3%)という順番になっている。特に「管理ミス」が昨年度(8.3%)より大幅に増加しているが、その原因として、組織の建物内での誤廃棄や紛失を公表するようになったことが影響していると分析している。

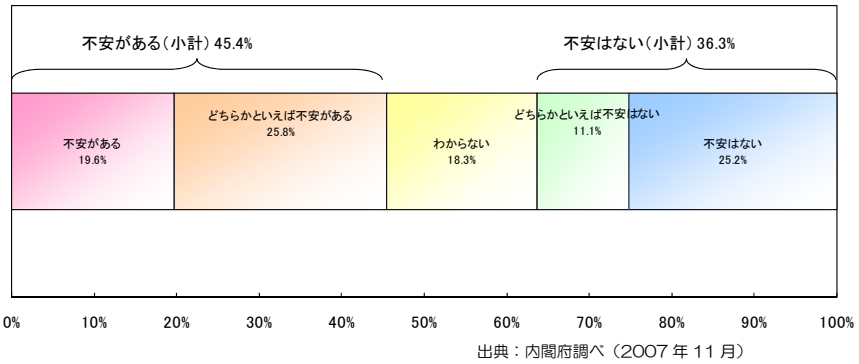
（インターネット利用における不安感）

2007 年末現在、インターネット利用世帯の約５０%は、その利用に何らかの不安を抱えている状況であり、その主たる要因としては、「個人情報の保護に不安がある」（71.0%）、「ウイルスの感染が心配である」（66.1%）、「どこまでセキュリティ対策を行えばよいか不明」（60.2%）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 19 年通信利用動向調査（総務省）

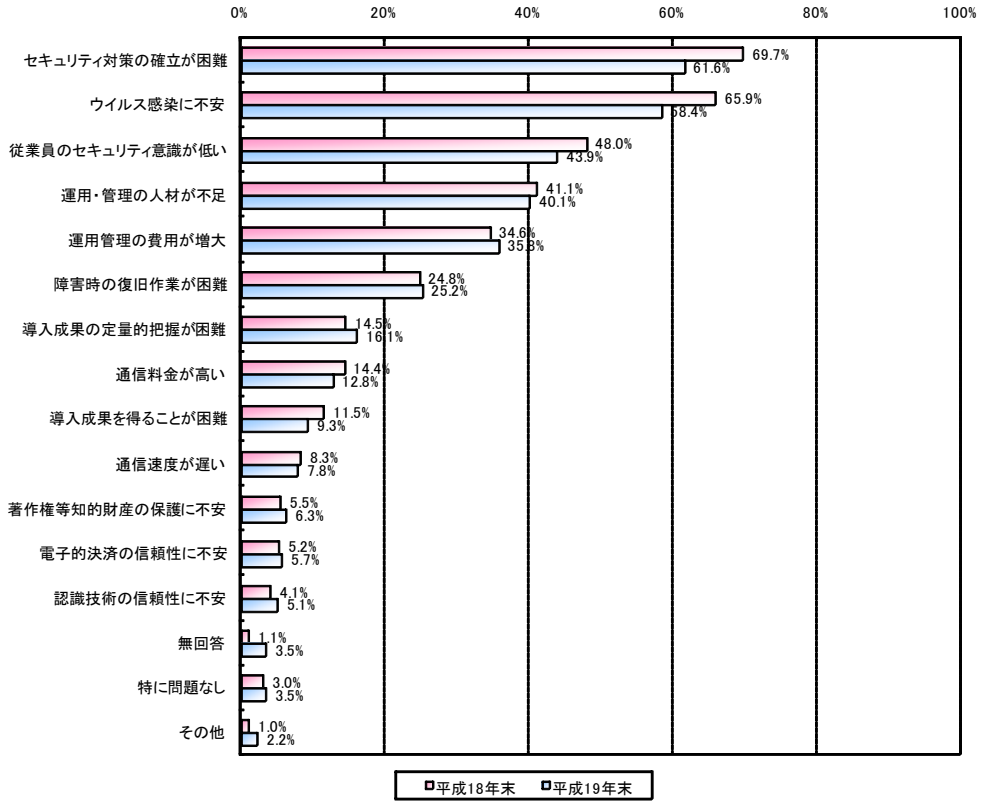
図表 2-17：インターネット利用で感じる不安の内容（世帯）（複数回答）



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、2007 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 61.6%、続いて「ウイルス感染に不安」が 58.4%となり、昨年と比較して減少しているものの、依然として高い割合で「セキュリティ関連」の不安が上位を占めている他、「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】。



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[8]。

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[9]。

こうした様々なデータから類推されるように、現在の ICT 環境において、情報セキュリティに関連する被害が継続して発生するとともに、インターネット等の利用者も何らかの不安感を抱いたまま ICT サービスを利用している状況である。こうした事態を改善し、安心・安全な ICT 環境を構築するためには、我が国における情報セキュリ

[8] 2008 年 2 月、「ノートン・オンライン生活リポート」（シマンテック社）による。
[9] 2008 年 2 月、「ノートン・オンライン生活リポート」（シマンテック社）による。

ティ対策をより一層強化することが必要である。

３．情報セキュリティ対策の現状と課題

安心・安全な ICT 環境を構築するためには、現状における情報セキュリティ対策の課題や対策を整理するとともに、~~情報通信技術~~ ICT 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及びその解決策等について、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、安心・安全な ICT 環境を整備していく上で、①現在の ICT 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こと、②今後 3 年から 5 年後といった近い将来の ICT 環境及びその変遷過程といった環境の変化を捉え、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こと、の２つの観点から検討を進めてきたところである。

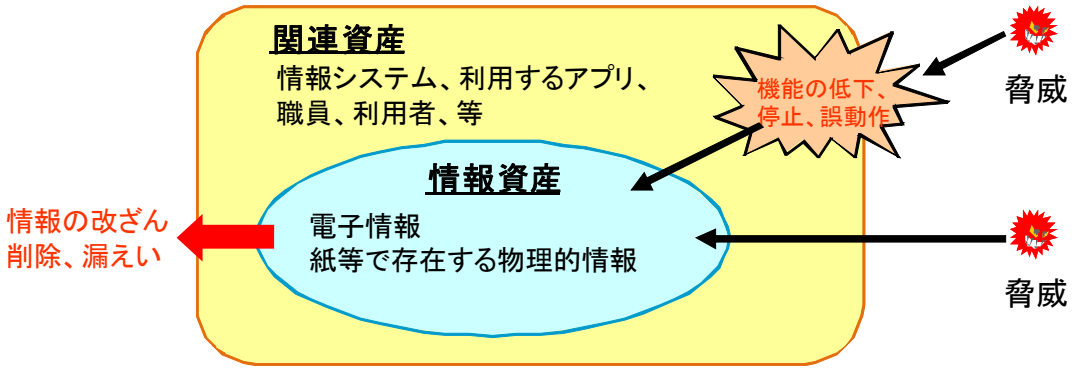
そこで、本章では、現在の ICT 環境における脅威・課題、及びその対策についての検討状況を述べることとする。

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、情報セキュリティ脅威・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

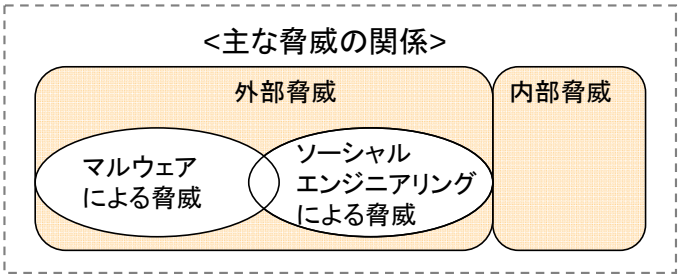
（フィッシング等、人間の行為、行動の弱点、盲点等をついてマルウェアに感染させたり、情報を盗み出す脅威）

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経済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。これら内部脅威・外部脅威に加え、ICT 利活用の進展に伴い、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、情報セキュリティ脅威に関する大きな変化点であると捉えることができる。

このようにネットワークを介してもたらされる脅威は、遠隔からかつ広範囲に被害をもたらす可能性があるため、その社会的・経済的な影響の大きさを踏まえ、本研究会では、主にこうしたネットワークを介してもたらされる脅威に着目して検討を行っている。その脅威の変遷は以下のとおりである。

90 年代前半、コンピュータの多くは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 などの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てフィッシングサイトに誘導したり、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する者・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。とりわけ、こうした犯罪の組織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。例えば、利用者が通常利用する正規の Web サイトにそのサイトが有する脆弱性をついて事前に不正なコードを埋め込んでおき、関連する脆弱性を有する PC を用いて利用者が当該サイトを閲覧した場合に、利用者に気付かせることなくウイルスに感染させる手法が挙げられる。本件については、2008 年 3 月頃から我が国でも多数の Web サイトに不正なコードが埋め込まれたとの報道やセキュリティ対策事業者等による注意喚起が行われている。また、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、対策の著しい遅延を招いている。

	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
脅威の対象	PC ミニコン	PC、~~インターネット~~サーバ 特定の個人・組織の情報	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
備考	Elk Cloner、 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	ボットネット、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、主として、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等が深刻な問題である。

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、今後も、より一層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、次章で述べるように ICT 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、これらを標的にした攻撃が多く発生することにより、これまで以上に対策が困難になっていくものと考えられる。

（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。ボットに感染したコンピュータでは、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攻撃や被害が生じ、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、2 万種類以上あると報告 ~~23,868 種類~~[10]~~ある~~されている。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、仮にこれらボットに感染したコンピュータが一斉に攻撃活動を行った場合には世界中のインターネットの機能を停止させるだけの能力があることが報告されたことも受けて「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、インターネットの世界的な普及、コンピュータの性能の向上、ブロードバンド環境の進展等とあいまって、継続的な国際的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[11]、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[12]、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、これまでのボット等の感染手法は、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、事前に不正なコードを埋め込まれた Web サイトを閲覧しただけで、ボットを含むマルウェアに感染したり、マルウェアを配布する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、この Web サイトの閲覧による感染手法の場合、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ある。

さらに、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

[10] 2008 年 3 月 20 日現在における、シマンテック社の定義によると 23,868 種類存在すると報告されている。
[11] シマンテック社における 2007 年 12 月の調査による。
[12] 英ソフォス社における 2007 年 10 月の調査による。

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が講じられてきている状況である。

加えて、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者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。しかも、マルウェア作成ツールと数百万件のメールアドレスをセットにしたもので、数万円程度で販売されているという報道もある。

そもそも、こうした DDoS 攻撃、スパムメールの発信等は、IP ネットワークの性質を悪用して発信元を詐称したり、踏み台となった PC を利用したりして行われており、詐称された真の発信元の探査や、ボットに感染した PC を遠隔に操作する者の特定の難しさが、悪意をもった攻撃者側の特定に大きな障害となっている。

このように、今後も、攻撃手法の巧妙化は短期間に繰り返され、攻撃者側としては少ない労力で大きな効果を上げる一方、対策者側では益々多大な手間と費用を掛けなければ対処できないような状況になるものと予想される。

≪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ように明確に特定の地域に絞った攻撃であるほか、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、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窺える。なお、こうした事件は、2008 年に入ってからも発生している状況であり、鋭意セキュリティ対策事業者等による対処が行われているところであると思われるが、被害を受けた企業においてはこうした恐喝へ絶対に屈しない姿勢で対処することが大切である。

≪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。

具体例としては、Storm Worm に感染した端末から 1 分間に平均 3,500 通ものスパムメールの大量送信を行うこと[13]、2008 年の 1 月に「Storm Worm」によって送信されたスパムメールがピーク時には全世界のメールトラフィック全体の 16%に

[13] 2007 年 1 月 22 日付シマンテック社報道による。

も及んだこと[14]、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Storm Worm によるスパムメールの送信が行われていること[15]などが伝えられている。

なお、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 分毎にバイナリコード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。

さらに、昨今では Storm Worm を凌駕するスパムボットの台頭も指摘され始めている。

≪海外事例５≫

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。

こうした正規の 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でネット上において販売されており、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。

（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、実際に取引がある関係者等からのメールに見せかけるように送信者情報が偽装されていたり、標的となった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ウェア

[14] 2008 年 1 月 30 日付英ソフォス社報道による。
[15] 2007 年 1 月 22 日付シマンテック社報道による。

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が、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、過去４ヶ月間上昇傾向を示している。事案としては、これまでと同様、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、受信者がそのメールに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[16]。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されており、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】。なお、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たフィッシング Web サイトを自動的に作成する複数のツールキットの

[16] 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」（シマンテック社）による。

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[17]。

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、スパイウエアウェ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、スパイウエアウェ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、一見すると正当な Web サイトに見えるようにページが定期的に更新されるなど、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、モバイル環境における脅威等が挙げられる。

（自動転送型ファイル共有ソフトを利用したウイルス拡散）

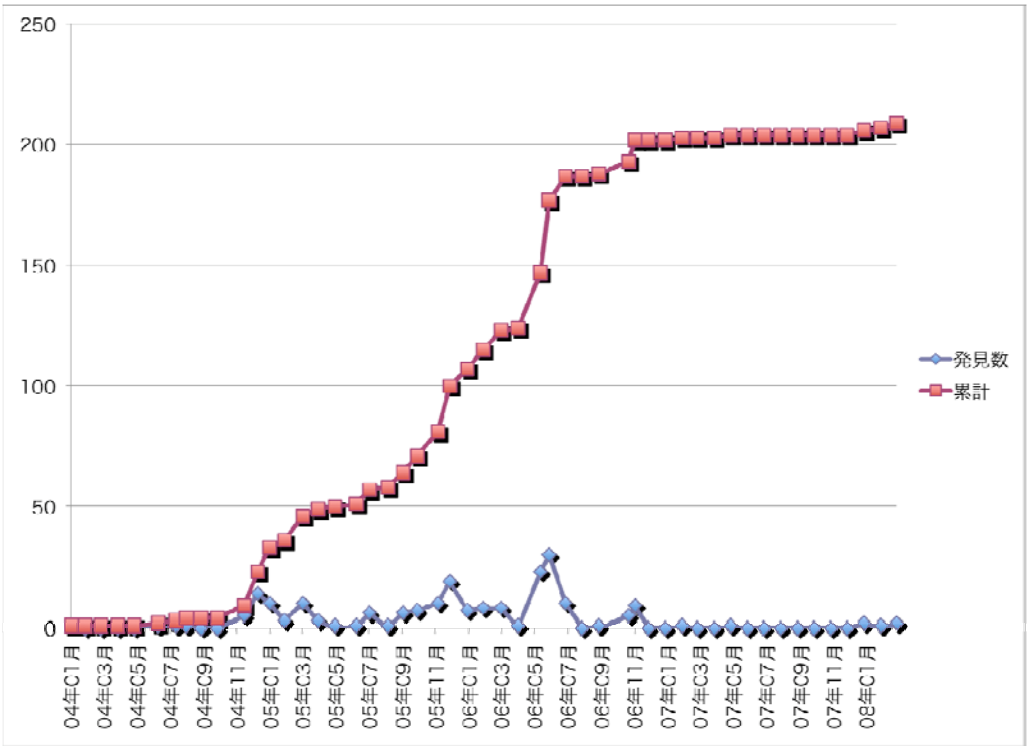
2007 年 1 月、Winny で流通するファイルについて無作為に調査した結果、調査時に流通していたファイル全体のうち約 4.5%にマルウェアが含まれているとの結果が出ている。検出されたマルウェアの多くは、.lzh や.zip などの圧縮フォルダの中に複数のファイルと一緒に同梱され、さらに取得したマルウェアの約 95.5%は音楽ファイル等のファイルアイコンに偽装されていた。このように目視での安全性確認が困難であるため、.lzh などの圧縮フォルダの大半にはマルウェアが含まれているという前提で情報セキュリティ対策が必要である。今後も P2P 等の管理者不在のオーバーレ

[17] 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」（シマンテック社）による。

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。

（モバイル環境における脅威）

近年、携帯電話は高度化・多機能化が進み、最近では、携帯通信情報端末（PDA）機能を持つ「スマートフォン」と呼ばれる携帯電話端末が市場に拡大している。スマートフォンは、OS を土台に様々なアプリケーションソフトを実装することができることから、PC に近い情報機器といえる。こうした機能の柔軟性（自由度）を高くすることを実現している一方で、OS やアプリケーションの脆弱性を狙った悪意のあるプログラムによる攻撃によって、利用者の利益が阻害されるなどの脅威となることが想定される。実際、公開されている情報では、2004 年 1 月に初めて携帯電話向けのマルウェアが発見されて以降、この 4 年間で月平均約 4 種類の新種マルウェアが発見されており（現在累計で約 200 種類のマルウェアが発見されている。）、そのほとんどがスマートフォン向けのものであると言われている。なお、2007 年以降、発見数の減少が確認されるが、これはある海外の携帯電話端末メーカーがセキュリティを強化したヴァージョンの OS を採用したことにより、マルウェアの作成が困難になったためと考えられている【図表 3-6 参照】。



米シマンテック社報告による

図表 3-6：モバイルマルウェア ~~Malware~~ 発見数の月次推移

日本では、これまで国内の携帯電話事業者が独自の仕様を採用してきたこと等から、日本の携帯電話のソフトウェアの脆弱性を狙うマルウェアが皆無に等しかったと思われるが、日本国内でのスマートフォンの普及が進むにつれ、マルウェア感染の危険性が高まってきており、具体的には、以下のような危険性が考えられる。

① OS やミドルウェア、基本アプリの脆弱性が攻撃され、ネイティブ機能を悪用される危険性がある。携帯用のネイティブ機能には、不正利用されにくいように利用者に警告を発する場合があるが、警告画面が出る前に、ユーザに警告画面を無視させるようなメッセージを表示し、操作を促すことが考えられる。

② ~~web~~Web サービスと連携した攻撃も懸念される。携帯電話向けブラウザは高機能化が進んでいることから、iframe を利用した攻撃のように、PC への攻撃と同等の攻撃が発生することが懸念される。

③ 携帯電話特有の事情がセキュリティの低下を引き起こす可能性が考えられる。例えば、携帯電話のブラウザにはアドレスが表示されないものが多いため、フィッシングが確認しづらい仕様になっているのではないか危惧される。

（Linux 環境における脅威）

Linux は、UNIX 互換のオープンソース・ソフトウェアの OS で、当初は学術機関を中心に利用が進み、その後、主に中小規模のサーバ用 OS として一般企業等にも普及してきたものであり、ネットワークやシステムの安定性、必要な機能を選択して実装できることでスリム化や多機能化が可能であるといった柔軟性等に優れていると言われている。また、その自由度の高さから、組み込み機器からメインフレームまで幅広く応用されており、近年では、一般ユーザが PC 用 OS として採用する例がよく見られるようになってきている。例えば~~特に~~、低価格 PC（ULCPC: Ultra Low Cost Personal Computer）向けの OS として、2007 年 10 月頃から一般に出回り始め、これまで PC に余りなじみのなかったユーザ層向けの新しい市場として注目されており、新興国や教育の現場における Linux を採用した PC の大量導入が話題となっ~~たりし~~ている。

このように、~~、~~一般利用者向けとして Linux を採用した PC や製品が今後ますます普及した場合には、攻撃ターゲットとなる可能性~~しての旨み~~が増大~~するため、Linux 向けの攻撃が増加~~するものと~~ことが~~予想される。

今回、総務省において実施した調査研究[18]においても、Linux におけるセキュリティのぜい弱性を狙った攻撃や、パスワードクラッキングといったセキュリティ対策のあまさをついた攻撃が行われ、不正に侵入された後のフィッシングコンテンツの設置やフィッシングメールの送信などといったボット化（踏み台化）が確認されている。なお、Linux は、比較的導入は容易でも、セキュリティに関する設定や修正は一定レベル以上のスキルが必要となる場合が多いと言われており、セキュリティ対策が進ま

[18] 2008 年 3 月「モバイル環境や Linux システムにおける Malware の脅威に関する調査研究」（総務省）

ずに放置されてしまう危険性があると懸念される。

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、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、現在の状況を整理するため、先に提示した４つの情報セキュリティ脅威毎に、以下に示す７つの対策実施主体による対策及び実施における課題等を取りまとめた。

（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（ウイルス対策ソフトウェアベンダ ~~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（~~I S P~~ISP、アクセス系、携帯電話系、無線通信系）
ｅ.~~O S~~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みの例							
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（ウェブサイト運営者、ASP・SaaS 等を含む）	機器開発事業者	政府機関

図表 3-~~67~~7：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 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。

その際、技術の進歩や別々の機能を実現するソフトウェアを同時に利用することにより、対策の安全性が低下する可能性や新たな脅威が発生する可能性があることから、情報セキュリティ対策は常に最新の対策を適切に実施することが重要であることを正確に利用者に理解してもらうよう、不断の努力が必要である。

ボット対策については、総務省と経済産業省が、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 PC を利用する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。

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問題を解決しようにも、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。

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。なお、こうした課題に係る制度について、３－６節において諸外国も含めた現状を整理している。

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いてウイルス作成を罰する規定が制定されることが強く望まれている。加えて、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みの例							
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（ウェブサイト運営者、ASP・SaaS 等を含む）	機器開発事業者	政府機関

図表 3-~~7~~8：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との指摘もある。

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）に対する取組みの例							
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（ウェブサイト運営者、ASP・SaaS 等を含む）	機器開発事業者	政府機関

図表 3-89：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）に対する取組みの例							
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（エッジシステム含む）／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	・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（ウェブサイト運営者、ASP・SaaS 等を含む）	機器開発事業者	政府機関

図表 3-~~9~~10：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困難であるが、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。

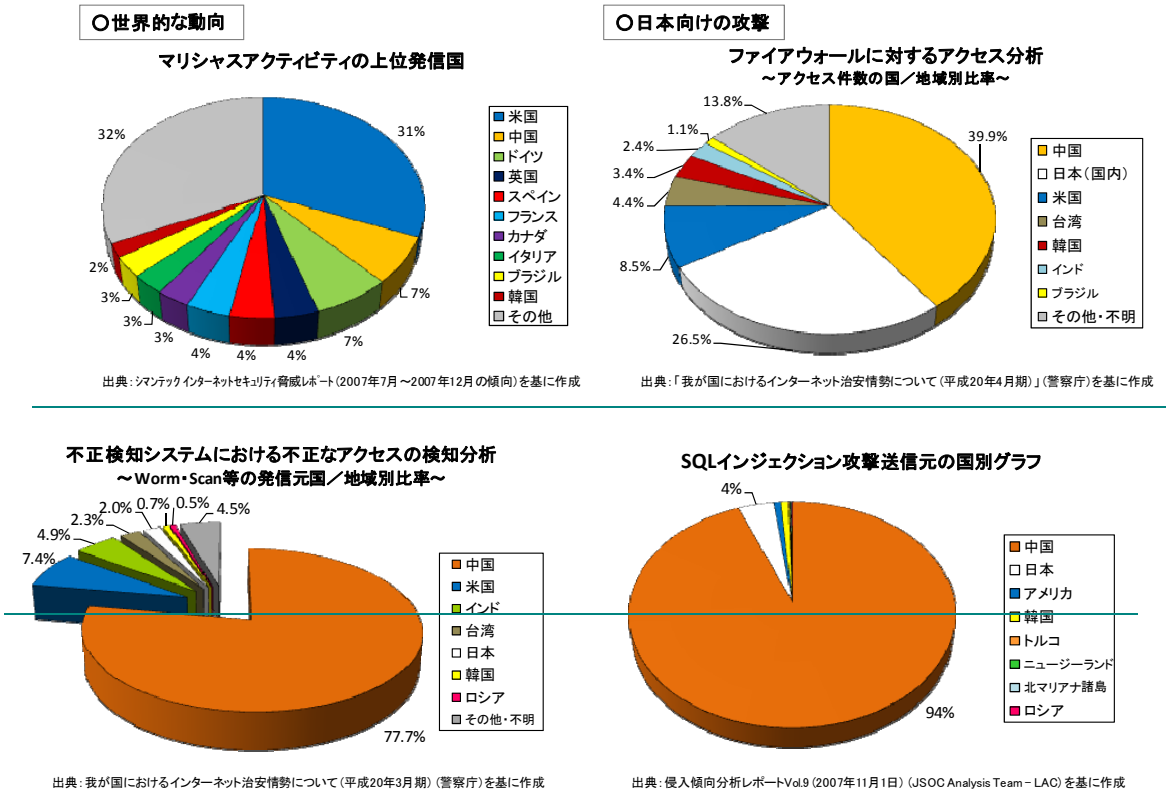
現状の対策や課題に関する共通的な事項として、特に、対策実施主体である利用者

（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。

３－５　情報セキュリティに関する国際的な対応状況と課題

３－３節で挙げられている事例からも分かるとおり、情報セキュリティ脅威はインターネットを通じ世界中に影響を及ぼす可能性があり、過去には、MS ブラストや SQL スラマーといったマルウェアが世界的に大流行するという事態も発生している。現在発生している脅威の多くは、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、その発生元は、ボットによるスパムメールや DDoS の発信アドレスを例に取れるように、非常に広範囲に渡っている。また、我が国に向けた脅威の発信元について見てみると、国内発と比較して海外発のものが多い傾向にあり、我が国の ICT 環境を安心・安全なものとするためには、国内における対策の実施のみならず、国際連携の推進等、国際的な視点が必要である【図表 3-1~~0~~1 参照】。



図表 3-~~1 0~~11：セキュリティ脅威の国際動向~~（日本に向けた脅威）~~

（ISP における国際的な情報セキュリティ脅威への対応状況と課題）

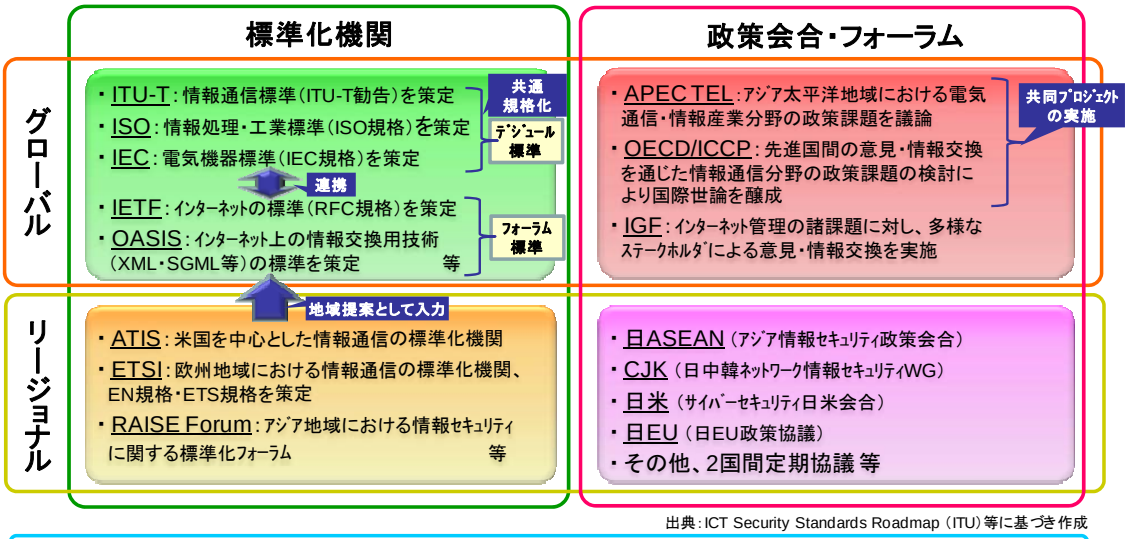
こうした状況の中、ISP においては、例えば、海外から自ネットワーク内に向けた DDoS 攻撃に対するフィルタリング等の自ら実施する対処に加えて、Peering 対向 ISP との契約に基づくインシデントハンドリングや、*nog（Network Operators' Group: nanog, janog 等）、NIC 系活動(ARIN, RIPE, APNIC 等)、nsp-security 等のコミュニティにおける情報共有、あるいは MAAWG（Messaging Anti-Abuse

Working Group)や APWG (Anti-Phishing Working Group)といった特定目的の活動団体への参加等を通じて、情報セキュリティ脅威に対する国際協調を図っている。

また、様々な業種に渡る CSIRT (Computer Security Incident Response Team)間の国際協調の場である FIRST ~~(Forum of Incident Response and Security Teams)~~等において、事案情報・脆弱性情報の共有や DDoS、フィッシング等の事案に対する国際協調対応が図られており、依頼に基づく連携対処ではあるが、一定の効果を上げている状況である。

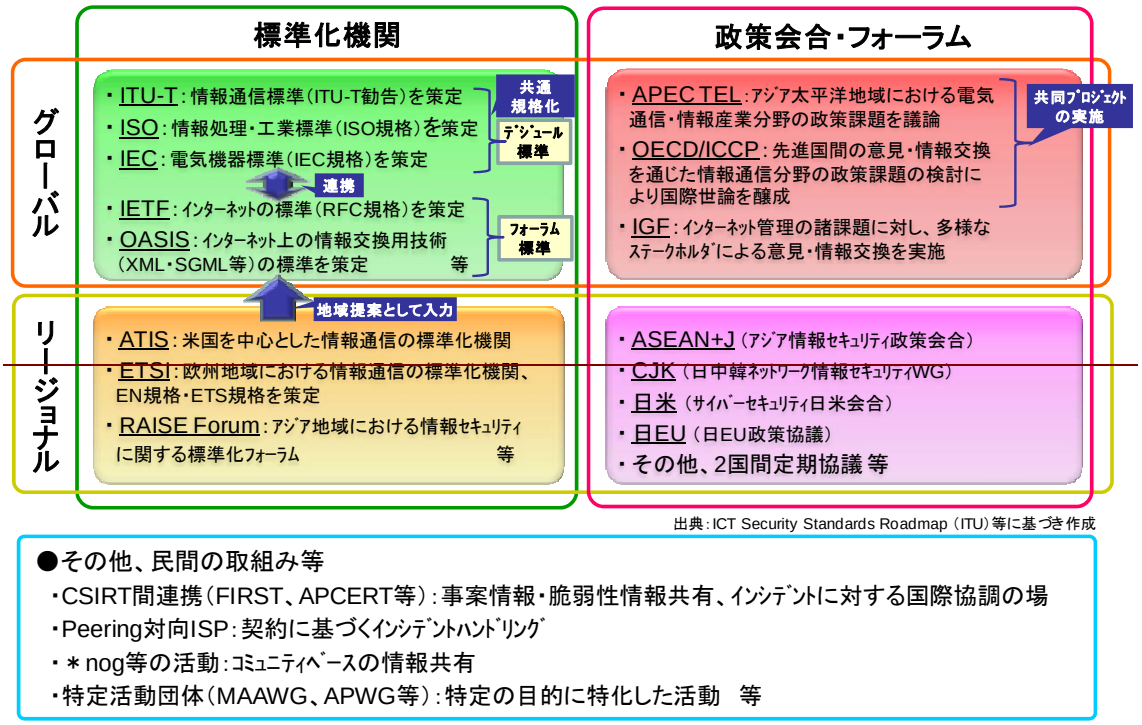
しかしながら、通信事業に関連する法制度的な環境、文化、技能やネットワーク環境、時差、言語といった国際間における様々な違いが迅速かつ適切な対応へのハードルとなっていることに加え、さらに昨今の国際事案においては、例えば、ボットネットにおけるハーダーのような行為者、ボット感染 PC のような物理的に攻撃を行う資源（とその管理者）、物理的に攻撃を受ける Web サイト等の資源（とその管理者）、当該 Web サイトへの攻撃により自らの提供サービスに問題の生じるサービス提供者、当該サービスの問題によって被害を受ける利用者等、多くの利害関係者が存在し、かつそれらが異なる国や地域に分散するといったように複雑化してきており、状況の把握や適切な対処が難しくなってきているとの指摘がある。

また、国際連携を推進するにあたり、まず国内の状況整理（事案対応における通信事業者の役割の明確化、国内被害者と対策組織がコンタクトできる仕組み、対策組織間の連携・協調の促進）をすべきとの指摘もある。



出典：ICT Security Standards Roadmap（ITU）等に基づき作成

●その他、民間の取組み等
- CSIRT間連携（FIRST、APCERT等）：事案情報・脆弱性情報共有、ｲﾝｼﾃﾞﾝﾄに対する国際協調の場
- Peering対向ISP：契約に基づくｲﾝｼﾃﾞﾝﾄﾊﾝﾄﾞﾘﾝｸﾞ
- ＊nog等の活動：ｺﾐｭﾆﾃｨﾍﾞｰｽの情報共有
- 特定活動団体（MAAWG、APWG等）：特定の目的に特化した活動　等



図表 3-~~1 1~~12：情報セキュリティに関する国際会合の動向

（標準化活動および政策会合等の動向）

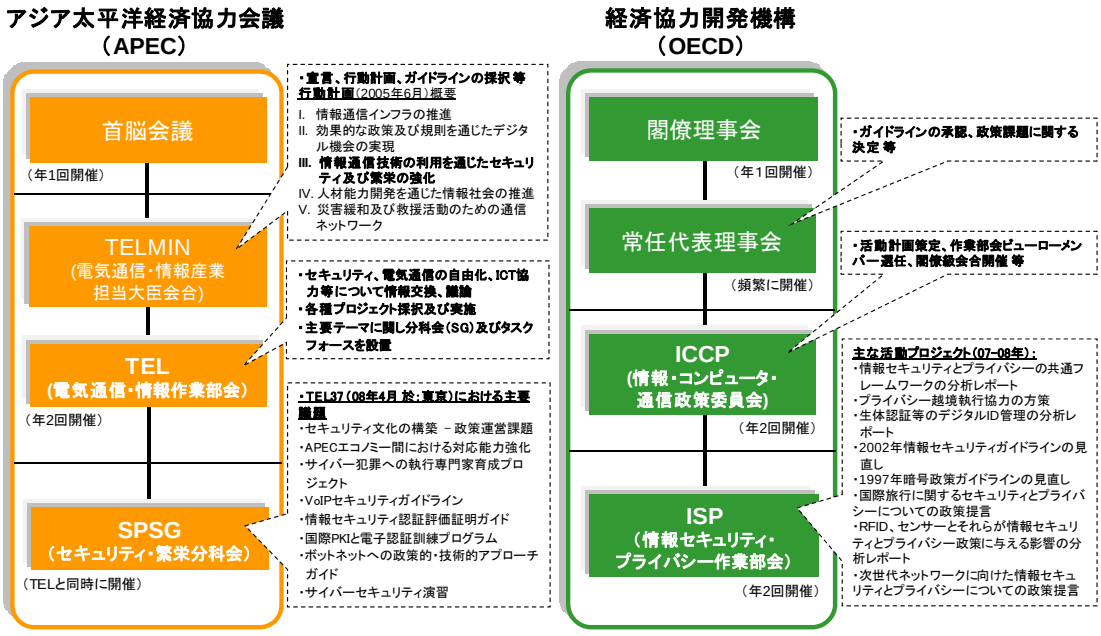
情報セキュリティに関する国際標準化に関しては、グローバルな場として ITU-T や ISO/IEC 等のデジュール標準化機関や IETF のようなフォーラム標準化機関があり、暗号/認証技術、セキュアな通信サービスのためのアーキテクチャ、情報交換のためのデータモデルやフォーマット、情報セキュリティマネジメント等の幅広い範囲を扱っている。また、リージョナルな場としては RAISE Forum（アジア地域）、SWIS（日中韓中心）等の活動があり、地域における標準化施策を共有し、グローバルな標準化に向けた地域提案等について協調を図っている【図表 3-12 参照】。最近では、基軸となる技術の標準化に加え、連携の仕方や意識向上のための施策検討についてもが標準化の必要性が認識されてミッションに追加され始めてきており、例えば連携の枠組みやセキュリティ文化促進に焦点を置いた国際標準等~~ガイドラインや、セキュリティ文化促進のためのガイドライン等~~について検討がなされ始めているところである~~【図表 3-11 参照】~~。

我が国においては、情報セキュリティに関する先進的な技術開発が多数行われており、これらの技術を国際的に展開していくにあたり、標準化の場は非常に重要である。標準化された規格が実際に利用されるためには、標準化作業の当初から規格のユーザとの連携を図り、ユーザの意思を反映したものとすることが重要との指摘がある。

情報セキュリティに関する議論を行っている国際的な政策会合に関しては、グローバルな場として APEC~~/~~ TEL や OECD/ICCP 等があり、基本政策（中長期戦略、組

織・体制整備、能力開発等）及び主要なセキュリティ課題（重要インフラ保護、スパム・ボット対策等）に関する情報共有や意見交換が行われている他、各国の政策規範となるガイドラインの策定やセキュリティ対策技術に関する調査研究プロジェクト等も実施されている【図表 3-1~~2~~3 参照】。また、IGF 等のフォーラムにおいては、産学官の多様なステークホルダによる自由闊達な意見交換が行われている。一方、リージョナルな場としては、日 ASEAN 会合や APT（アジア・太平洋電気通信共同体）、日中韓（CJK）ネットワーク情報セキュリティワーキンググループ等があり、政策面・技術面での情報交換、地域特有の課題に対する検討及び連携体制の強化等が行われているほか、グローバルな会合に向けた地域内の意見集約を行う場としての役割を果たしている。また、日米、日 EU をはじめ諸外国との政策協議等の場を通じた情報交換を行っているところである。

なお、政策レベルでの議論においても、各国の法制度、組織体制及び対処能力等が不均衡であるなか、より実効的な国際連携の実現に向けて今後どう取り組むべきかを検討することが課題となっている。同様の課題は、法制度や文化的背景が比較的似ていると考えられる欧州地域においても指摘されており、欧州連合（EU）加盟国間の不均衡な対応を是正することで各国のセキュリティレベルを均一化し、国境を越えた協調的取組みに着手すべきとされている[19]。



図表 3-~~12~~13：APEC 及び OECD の体制と情報セキュリティに関する取組みの概要

[19] 2008 年 5 月、ENISA のオンラインセキュリティに関する年次報告書による。

３－６　情報セキュリティに関連する各国の法制度等の状況

情報セキュリティ対策を実施するにあたり、特に電気通信事業者が新しい情報セキュリティ対策等を実施するに当たっては、電気通信事業者が取り得る正当業務行為等の範囲等について、電気通信事業法第４条にある「通信の秘密」等の我が国の法制度との関係を整理しながら、具体化を図っていく必要がある。また、海外から発信される情報セキュリティの脅威について、国際的な連携を図って対処してくためには、諸外国の制度の現状を把握することが必要である。こうしたことから、以下に、我が国及び主な諸外国の情報セキュリティに関連する制度について、文献等による基礎的な調査により把握できた内容について、整理している。

また、現状では、諸外国の制度の内容が不明確なところがあり、また今後の我が国の情報セキュリティ対策の充実を図るための参考とするためにも、電気通信事業者による情報セキュリティ対策の実態等もあわせ、その詳細を把握するための継続的な調査・検討が必要である。

なお、以下の取りまとめについては、我が国の法制度を基に、主な諸外国の制度を比較する形で整理している。

	「通信の秘密」に関連する規定	「通信の秘密」の対象となる範囲	「通信の秘密」の侵害について
日本	**〇日本国憲法** ・**第21条第2項**:検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。 **〇電気通信事業法** ・**第 4 条第 1 項**:電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。 ・**同条第2項**:電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。	・個別の通信に係る通信内容のほか、個別の通信に係る通信当事者の氏名、発信場所、通信日時、通信量やヘッダ情報等の構成要素、通信の存在の事実の有無を含む。	・通信の秘密を発信者又は受信者の意思に反して自己又は他人の利益のために利用することは、通信の秘密の侵害(窃用)に当たる。 ・通信の秘密侵害行為に該当する場合であっても、違法性阻却事由があれば(正当防衛、緊急避難又は正当業務行為に該当すれば)、当事者の同意の有無に関わりなく、許される。 ・正当業務行為に該当する場合には、(1)目的の正当性、行為の必要性、(2)手段の相当性を満たすことが必要。 ・具体的には、電気通信事業者が電気通信役務を提供するために必要な行為については正当業務行為として違法性が阻却。 ・迷惑メール対策の OP25B は正当業務行為とされうる。 ・「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」において、DoS 攻撃等の大量通信等への遮断等を始めとする対処について、通信の秘密の侵害の該当の有無、通信の秘密を侵害したとしても違法性が阻却されうるのか否かについて、基本的な考え方を整理し、該当する事例を挙げている。
	日本における「通信の秘密」に該当、類似または関連する規定	通信*及び通信データ**等の定義、範囲等	通信*及び通信データ**の取扱い等
米国	**〇合衆国憲法** ・**修正第 1 条**:連邦議会は、国教を樹立し、または宗教上の行為を自由に行うことを禁止する法律、言論または出版の自由を制限する法律、並びに人民が平穏に集会する権利、及び苦情	**〇合衆国法典 第 18 編 犯罪及び刑事手続** ・**第 2510 条**(定義)**第 1 項**:**「有線通信(wire communication)」とは**、音声の伝送であって、その全部又は一部が、州際の若しくは外国との通信又は州際の若しくは外国との通商に影響を与	**〇合衆国法典 第 18 編 犯罪及び刑事手続** ・**第 2511 条**(有線通信、口頭の会話又は電子的通信の傍受及び開示の禁止)**第 2 項**:(a)(i)交換台のオペレータ又はその設備が有線通信若しくは電子的通信の送信に利用される有線

	の処理を求めて政府に対し請願する権利を侵害する法律を制定してはならない。 ・**修正第 4 条**:不合理な捜索及び逮捕または押収に対し、身体、家屋、書類及び所有物の安全を保障されるという人民の権利は、これを侵してはならない。令状は、宣誓または確約によって裏付けられた相当な理由に基づいてのみ発行され、かつ捜索すべき場所、及び逮捕すべき人、または押収すべき物件を特定して示したものでなければならない。 **○合衆国法典 第 18 編 犯罪及び刑事手続** ・**第 2511 条**(有線通信、口頭の会話又は電子的通信の傍受及び開示の禁止)**第 1 項**:この章に別段の定めがある場合を除き、次の者は第 4 項の定めに従い処罰され、又は第 5 項の定めに従い訴訟を提起される。 (a)有線通信、口頭の会話又は電子的通信を、意図的に傍受し、傍受を試み、又は他の者を説得して傍受させ、若しくは傍受を試みさせる者 (b)次の場合に、口頭の会話を傍受するための電子的、機械的その他の装置を意図的に利用し、利用を試み、又は他の者を説得して利用させ、若しくは利用を試みさせる者 (i)その装置が、有線通信に利用される電話線、ケーブルその他類似の接続線に設置され、又はそれを通して信号を送信する場合 (ii)その装置が無線による通信を送信し、又はそうした通信の送信を妨害する場合 (iii)その者が、その装置又はその構成要素が、郵送され、又は	える通信の送信のために設備を提供し、又はこれを運営する者により、設置され、又は運営される、発信点と受信点の間に電話線、ケーブルその他類似の接続線(切替地点における接続線の利用を含む。)を使った通信の送信のための設備を利用して行われるものをいう。 ・**同条第 2 項:「口頭の会話(oral communication)」とは**、通信が傍受を受けないという期待を正当化する状況の下で、傍受を受けないという期待を表明する者により発される口頭の会話をいう。ただし、電子的通信は含まれない。 ・**同条第 4 項:「傍受(intercept)」とは**、電子的、機械的その他の装置の利用を通じて、有線通信、電子的通信又は口頭の会話の内容を音声その他の形態で捕捉することをいう。 ・**同条第 8 項:「内容(contents)」とは**、有線通信、口頭の会話又は電子的通信に関して使用されるときは、通信の主旨、意図又は目的に関する情報を含む。 ・**同条第 12 項:「電子的通信(electronic communication)」とは**、符号、信号、文字、画像、音、データ又はある種の情報の伝送であって、その全部又は一部が、州際の又は外国との通商に影響を与える有線、無線、電磁気、光電子変換又は光変換を用いたシステムを利用して送信されるものをいう。ただし、次のものは除く。 (A)有線通信又は口頭の会話 (B)信号音のみのページング装置により行われる通信 (C)追跡装置からの通信(この編の第3117条の定めるところに従う。) (D)電子的蓄積及び資金移転に利用される通信システムにお	通信サービス若しくは電子的通信サービスのプロバイダの職員、被用者若しくは代理人は、サービスの提供又はサービスのプロバイダの権利若しくは財産の保護に必然的に付随する活動に従事する場合には、通常の職務の過程で通信を傍受し、開示し、又は利用することは、この章の下では違法とされない。ただし、公衆向けの有線通信サービスのプロバイダは、機械又はサービスの質をコントロールするためのチェックを除き、サービス監視又はランダム監視をしてはならない。 ・**第 2702 条**(顧客の通信又は記録の自発的開示)**第 a 項**:禁止 b 項に定める場合を除き、次のことを禁止する。 (1)公衆に電子的通信サービスを提供する人又は団体が、サービスが電子的に蓄積されている期間に、通信の内容を、人又は団体に対し、意図的に漏示すること。 (2)公衆に遠隔コンピュータ処理サービスを提供する人又は団体が、そのサービスにおいて次のように保持され、又は維持される通信内容を、人又は団体に対して意図的に漏示すること。 (A)サービスの受信契約者又は顧客を代理し、その者から電子的送信により受理すること(又は、その者から電子的送信により受理した通信をコンピュータ処理して作成すること)。 (B)プロバイダが蓄積以外又はコンピュータ処理以外のサービスを提供する目的で通信内容へアクセスする権限を与えられていないときに、受信契約者又は顧客に蓄積サービス又はコンピュータ処理サービスを提供する目的だ

	州際の若しくは外国との通商により輸送されたことを知っている、又は知っている理由がある場合 (iv)その利用又は利用の試みが、(A)その営業が州際の若しくは外国との通商に影響を及ぼす営業所若しくは事業所の土地で行われる場合、又は(B)その営業が州際の若しくは外国との通商に影響を及ぼす営業所若しくは事業所の営業に関係する情報を得、若しくは得ることを目的とする場合 (v)その者がコロンビア特別区、プエルトリコ準州又は他の合衆国の領域若しくは領地において行動する場合 (c)情報が、この項に違反して、有線通信、口頭の会話又は電子的通信の傍受により取得されたことを知り、又は知っている理由がありながら、有線通信、口頭の会話又は電子的通信の内容を、故意に他の者に開示した者又は開示を試みた者 (d)情報が、この項に違反して、有線通信、口頭の会話又は電子的通信の傍受により取得されたことを知り、又は知っている理由がありながら、有線通信、口頭の会話又は電子的通信の内容を、故意に利用し、又はその利用を試みた者 (e)(i)この章の第 2511 条第 2 項(a)(ii)、第 2511 条第 2 項(b)-(c)、第 2511 条第 2 項(e)、第 2516 条及び第 2518 条により授権される方法により傍受された有線通信、口頭の会話又は電子的通信の内容を他の者に対し、故意に開示し、又は開示を試みた者 (ii)情報が犯罪捜査と関連して通信の傍受により取得されたことを知り、又は知っている理由がある者 (iii)犯罪捜査との関連で情報を取得し、又は受領した者	いて、金融機関により蓄積された電子資金取引情報 **・第 2703 条**(顧客の通信又は記録の要求された開示)**第 c 項**:電子的通信サービス又は遠隔コンピュータ処理サービスに関する記録 (1)政府機関は、電子的通信サービス又は遠隔コンピュータ処理サービスのプロバイダに対し、そのサービスの受信契約者又は顧客に関する記録その他の情報(ただし、通信の内容は含まない。)の開示を、次のいずれかの場合にのみ要求することができる。 (A)捜査の対象とされている犯罪の管轄権を有する裁判所が連邦刑事訴訟規則に定められた手続を利用して発付する令状又は州の同等の令状を取得した場合 (B)この条の d 項に基づく開示のための裁判所命令を取得した場合 (C)開示について受信契約者又は顧客の同意を得ている場合 (D)その受信契約者又は顧客が電話勧誘販売(この用語の意味は、この編の第 2325 条に定めるところに従う。)に従事しているときに、電話勧誘販売詐欺に関わる法執行捜査に関連して、プロバイダの受信契約者又は顧客の氏名、住所及び営業所について、公式の要求書面を提出する場合 (E)(2)の規定に基づく情報を求める場合 (2)政府機関が、連邦法若しくは州法により授権される行政上の罰則付召喚令状若しくは連邦若しくは州の大陪審若しくは公判の罰則付召喚令状を利用する場合又は(1)の規定に基づき入手できるその他の手段を利用する場合には、電子的通信サー	けのためにすること。 (3)公衆に対する遠隔コンピュータ処理サービス又は電子的通信サービスのプロバイダが、そのサービスの受信契約者又は顧客に関する記録又は他の情報(ただし、(1)又は(2)の対象となる情報を含まない。)を政府の機関に対して意図的に漏示すること。 **・同条第 b 項**:通信の開示の除外 a 項に記述されたプロバイダは、次のいずれかのときに通信の内容を漏示することができる。 (1)通信の宛名人又は所定の受信者若しくはその宛名人又は所定の受信者の代理人に対するとき (2)この編の第 2517 条、第 2511 条第 2 項(a)又は第 2703 条において別に授権されるとき (3)通信の発信者、宛名人又は所定の受信者の、若しくは遠隔コンピュータ処理サービスの場合には受信契約者の、法律に基づいた同意を得ているとき (4)通信を宛先に送信するために雇われた者、権限を与えられた者又はその設備を利用する者に対するとき (5)サービスの提供若しくはサービスにおけるプロバイダの権利又は財産の保護に必然的に付随するとき (6)次に該当する場合に、法執行機関に対するとき (A)内容が次のものである場合 (i)サービス・プロバイダにより意図せずに取得され、かつ (ii)犯罪の遂行に関係することが明らかに認められる場合 (B)1990 年犯罪規制法(Crime Control Act of 1990)第 227 条により要求される場合

	(iv)正式な権限に基づく犯罪捜査を故意に妨害する意図を持つ者 **・第 2701 条**(蓄積された通信への違法なアクセス)**第 a 項**:犯罪 この条の c 項に定められる場合を除き、次の者はこの条の b 項の定めに従い処罰される。 (1)電子的通信サービスを提供する設備に権限なく意図的にアクセスする者 (2)その設備にアクセスする権限を意図的に越し、有線通信又は電子的通信がシステムに電子的に蓄積されている間のその通信に対する権限に基づくアクセスを取得し、改変し、又は妨害する者 **・同条第 c 項**:除外 この条の a 項は、次のものにより授権された行為には適用されない。 (1)有線通信サービス又は電子的通信サービスを提供する人又は団体 (2)サービスの利用者自身の通信又はその利用者宛ての通信について、その利用者 (3)この編の第 2703 条、第 2704 条又は第 2518 条	ビス又は遠隔コンピュータ処理サービスのプロバイダは、政府機関に対し、そのサービスの受信契約者又は顧客について次の情報を開示する。 (A)氏名 (B)住所 (C)近距離及び長距離電話接続記録、又は通話の時間及び期間の記録 (D)(開始日を含む)サービスの期間及び利用されるサービスの種類 (E)電話番号、機器番号又は暫定的に割り当てられたネットワーク・アドレスを含む受信契約者の他の番号若しくはその識別子 (F)(クレジットカード番号又は銀行口座番号を含む)サービスの支払いのための方法及び財源 **・第 3127 条**(章の定義)**第 3 項**:**「ペンレジスター(pen register)」とは**、有線通信又は電子的通信の送信元となる機器又は設備により送信される局番、経路、宛先又は信号の情報(ただし、この情報には通信の内容は含まれない。)を記録し、又は解読する装置又はプロセスをいう。ただし、この用語は、請求書若しくは請求書に付随する記録のために、若しくはプロバイダにより提供される通信サービスのために、有線通信サービス若しくは電子的通信サービスのプロバイダ若しくは顧客が利用する装置若しくはプロセスを含まず、又は通常の営業の過程で費用計算その他類似の目的のために有線通信サービスのプロバイダ若しくは顧客が利用する装置若しくはプロセスを含まない。	(C)人の死又は重大な身体的傷害の急迫の危険に関わる緊急事態のために、遅滞なく情報を開示することが要求されているとプロバイダが合理的に信ずる場合 **・同条第 c 項**:顧客の記録の開示の除外 a 項に定められるプロバイダは、サービスの受信契約者又は顧客に関係する記録その他の情報(ただし、a 項(1)又は a 項(2)に定める通信の内容を除く。)を次のいずれかに従って漏示することができる (1)第 2703 条により別に権限を与えられるところに従うこと。 (2)顧客又は受信契約者の法律に基づいた同意によること。 (3)サービスの提供又はサービスにおけるプロバイダの権利若しくは財産の保護に必然的に付随するところに従うこと。 (4)人の死又は重大な身体的傷害の急迫の危険に関わる緊急事態のために、情報の開示が正当化されるとプロバイダが合理的に信ずる場合に、政府機関に対してすること。 (5)政府機関以外の者に対してすること。 **・第 3121 条**(ペンレジスター及びトラップ・アンド・トレース装置の利用の一般的禁止;除外)**第 a 項**:一般規定 この条に定められる場合を除き、何人も、この編の第 3123 条又は 1978 年外国諜報監視法に基づき裁判所命令を取得するまでは、ペンレジスター又はトラップ・アンド・トレース装置を設置し、又は利用することはできない。 **・同条第 b 項**: 除外

		・同条第 4 項:「トラップ・アンド・トレース装置(trap and trace device)」とは、有線通信又は電子的通信の源を合理的に特定するような発信者番号又は他の局番、経路、宛先若しくは信号の情報を特定する、入来する電子的その他の信号を捕らえる装置又はプロセスをいう。ただし、この情報には通信の内容は含まれない。	a 項の禁止は、電子的通信サービス又は有線通信サービスのプロバイダによる次のようなペンレジスター又はトラップ・アンド・トレース装置の利用には適用されない。 (1)有線通信サービス若しくは電子的通信サービスの運転、整備及び検査、プロバイダの権利若しくは財産の保護又はサービスの乱用若しくはサービスの違法な利用からのサービス利用者の保護に関するもの (2)プロバイダ自身、有線通信の完遂のためにサービスを提供する別のプロバイダ又はそのサービスの利用者を、不正、違法又は乱用的なサービスの利用から保護するために、有線通信又は電子的通信が開始され、又は終了した事実を記録するもの (3)サービスの利用者の同意を得ているもの
EU	**〇個人情報の処理と電子通信部門におけるプライバシーの保護に関する欧州議会及び理事会(2002 年 7 月 12 日)の指令(2002/58/EC)** **・第５条**(通信の機密性)**第１項**:加盟国は通信及びそれに関連するトラフィックデータの機密性を、公的通信ネットワーク若しくは一般に利用可能な電子通信サービスによって保証できるよう、国家的な立法措置を講じなければならない。特に、利用者以外の者による、通信あるいはそれに関連するトラフィックデータの聞き取り、録音、保存及びその他の傍受又は監視を、第 15 条 1 項により法的に権限を付与された場合を除いては、利用者の同意なく行うことを禁じる。ただし、本項は通信の伝達に不可欠であり機密性の本義を損なわないデータの技術的保存	**〇個人情報の処理と電子通信部門におけるプライバシーの保護に関する欧州議会及び理事会(2002 年 7 月 12 日)の指令(2002/58/EC)(一般大衆がアクセスできる、あるいは公共通信ネットワークでの電子通信サービス提供の枠内で発生する、あるいは処理されるデータの保存、並びに指令 2002/58/EC を修正する欧州議会・理事会指令(2006/24/EC)により修正)** **・第 2 条**(定義): **(b)「トラフィックデータ」とは**電子通信ネットワーク上における情報の移動や、それにかかる通信費用の請求書の作成のために処理されるデータを意味する。 **(c)「ロケーションデータ」とは**電子通信ネットワークで処理され、一般に利用可能な電子通信サービスの利用者の端末機器の	**〇個人情報の処理と電子通信部門におけるプライバシーの保護に関する欧州議会及び理事会(2002 年 7 月 12 日)の指令(2002/58/EC)** **・第６条**(トラフィックデータ)**第１項**:公的通信ネットワークあるいは一般に利用可能な電子通信サービスの提供者によって処理若しくは保存されたトラフィックデータは、通信の目的として不必要になった場合に、消去あるいは利用者を識別できないような状態にしなければならない。ただし本規定は、本条 2 項、3 項、4 項及び第 15 条 1 項の効果を毀損するものではない。 **・同条第２項**:トラフィックデータは、加入者への支払請求書の作成及び接続費用の支払いの目的においてのみ処理する

	を妨げるものではない。 ・**同条第 2 項:**本条 1 項は、司法実務行為の一環として、商取引あるいはその他の業務上の通信の証拠を提供する目的の場合、法的に権限を与えられた、通信及びそれに関連するトラフィックデータの記録を妨げるものではない。 ・**同条第 3 項:**加盟国は、情報を保存する目的及び、加入者又は利用者の端末に保存された情報にアクセスする目的で、電子通信ネットワークを利用することが基本的に認められないこと、また利用が認められる場合は、EU指令 95/46/EC で規定されているように、関係する加入者あるいは利用者に、明確かつ包括的な情報が提供され(特に処理の目的に関する情報は重要である)、データ制御装置によるこのような処理を拒否する権利が与えられることを保証しなければならない。本規定は電子通信ネットワークにおける通信の伝達の実行及び円滑化という唯一の目的として、加入者あるいは利用者によって明確に要求された、情報化社会向けサービスの提供に厳密に必要な目的のために行われる技術的保存あるいはアクセスを妨げるものではない。	地理的位置を示すデータを意味する。 **(d)「通信」とは**有限の参加者の間で、一般に利用可能な電子通信サービスによって情報を交換又は伝達することを意味する。ただし電子通信ネットワーク上の放送サービスの一部として一般に情報が伝達される場合は含まない。しかしこの場合も、受信者が識別可能な一般の加入者あるいは利用者となる可能性がある場合は「通信」に該当する。 **(e)「通話」とは**リアルタイムに双方向通信ができる、一般に利用可能な電話サービスによって構築される接続を意味する。	ことができる。また処理が許されるのは、請求書の内容の合法的な調査がなされている期間、あるいは支払いが請求されている期間のみである。 ・**同条第 3 項:**一般に利用可能な電子通信サービスの提供者は、電子通信サービスのマーケティング及び付加価値サービスの提供の目的で、本条 1 項で言及されたデータを、関連する加入者及び利用者の同意を得た上で、そのようなサービスあるいはマーケティングに必要な期間と程度の範囲において処理することができる。またその際は、加入者及び利用者がいつでも同意を撤回できるようにしなければならない。 ・**同条第 4 項:**サービス提供者は本条 2 項及び 3 項に記載された目的で処理されるトラフィックデータの種類と処理される期間を加入者あるいは利用者に通知しなければならない。ただし 3 項に記載された目的による処理に関しては、同意に先立って通知が行われなければならない。 ・**同条第 5 項:**本条 1 項、2 項、3 項、4 項の規定に従ってトラフィックデータを処理する者は、公的通信ネットワーク及び一般に利用可能な電子通信サービスの提供者による権限付与の下、請求書の作成、通信管理、顧客の質問への対応、不正行為の調査、電子通信サービスのマーケティング、付加価値サービスの提供を行う者に限定されなければならない。またトラフィックデータの処理は、上記の目的として必要な場合にのみ可能である。 ・**同条第 6 項:**本条 1 項、2 項、3 項、5 項の適用は、紛争(特に相互接続と料金請求に関する紛争)の解決を目的として、適用法規に従い管轄権を有する団体にトラフィックデータを通知する権利を侵害するものではない。

			・**第 15 条**(EU指令 95/46/EC の適用)**第 1 項**:EU指令95/46/EC第13条に規定されたように、本指令第5条、6条、8 条 1 項、2 項、3 項、4 項、9 条で規定された権利と義務の範囲を制限することにより、民主主義社会において、国家の安全、防衛、公安を確保し、犯罪となる攻撃及び電子通信システムの不正使用の予防、調査、探知、告訴を行う、必要、適当かつバランスのとれた施策が可能となる場合、加盟国は、このような制限を目的とした法的措置を採用することができる。加盟国は、この目的を達成するために、特に、限られた期間データを保存するための法的措置を採用することができる(この措置は本項によって正当化される)。本項に記載された全ての措置は、共同体法の一般原理(欧州連合に関する条約第6条1項2項も含む)に従わなければならない。
英国	・憲法上の規定は明らかではない。 **〇調査権限規制法**(Regulation of Investigatory Powers Act 2000) ・**第 1 条**(不法傍受)**第 1 項**:何人も、連合王国の場所において、次の各号のいずれかにより、ある者が通信の伝送の過程で、故意に、かつ合法的な許可を得ないで通信を傍受することをもって、罪とするものとする。 (a)公的な郵便業務 (b)公的な遠隔通信システム ・**同条第 2 項**:何人も、連合王国の場所において、私的な遠隔通信システムによる通信の伝送の過程で、次の各号の両者により、通信を傍受することをもって、罪とする。	**〇調査権限規制法**(Regulation of Investigatory Powers Act 2000) ・**第2条**(「傍受」の意味と位置付け等)**第 2 項**:何人も、次の各号のいずれかに該当するとき、及びその場合に限り、その者は、本法の適用上、ただし本条に掲げる規定に従うことを条件にして、電気通信システムによる通信の伝送の過程で、通信を傍受するものとする。 通信が伝送されている間に、通信の送信者又は想定される受信者以外の者に通信の内容の一部又は全部を利用させるために、 (a)当該システム又はその管理を変更し、又は妨害すること (b)当該システムによって行われた伝送を監視すること	**〇調査権限規制法**(Regulation of Investigatory Powers Act 2000) ・**第3条**(傍受令状のない合法的傍受)**第3項**:次の各号の両者に該当するときは、通信の傍受を含む行為は、本条によって許可される。 (a)当該行為が、郵便業務又は電気通信業務を提供する者による行為又はこの者に代わる者による行為であったとき (b)当該行為が、郵便業務又は電気通信業務の提供又は活動に関連する目的のために、若しくはこれらの業務に関して、これらの業務の利用に関する制定法・制定法規の執行に関連する目的のために行われたとき

	(a)故意に、かつ合法的な許可を得ないで (b)第 6 項により、本人の行為が本条に基づく刑事責任を免れる状況にある場合を除いて **○プライバシーと電子通信に関する規則(EC 指令)**(The Privacy and Electronic Communications (EC Directive) Regulations 2003) ・**第 6 条**(通信の機密性)**第 1 項**:第 4 項に従い、第 2 項の要件を満たさずに、何人も加入者や利用者の端末設備に、情報を保存するために、また保存された情報にアクセスするために電子通信ネットワークを利用してはならない。 ・**同条第 2 項**:要件はその端末設備の加入者や利用者が、 (a)その情報の保存又はアクセスの目的について明確で包括的な情報を提供されていること;かつ (b)その情報の保存又はアクセスについて拒否する機会を与えられていること ・**同条第 3 項**:加入者や利用者の端末設備の情報を保存又はアクセスするために同一人物により複数回電子通信ネットワークが利用される場合、第 2 項の要件を初回の利用に満たしていればこの規則には十分である。 ・**同条第 4 項**:第 1 項は以下の場合における情報の技術的な保存やアクセスには適用されない。 (a)電子通信ネットワークを利用した通信の伝送を実行又は助長する唯一の方法であるとき (b)そうした保存やアクセスが加入者や利用者から要求された情報社会サービスの提供に厳格に必要であるとき	(c)当該システム中を構成する装置へ、又は装置から無線電信によって行われる伝送を監視すること ・**同条第 8 項**:本条の適用上、第 2 項 a 号中の、通信が伝送されている間に通信の内容を人に利用させるとみなす事案には、通信が伝送されている間に、通信の内容がその後に人に利用されるように転換され、又は記録される事案が含まれるものとする。 ・**同条第 9 項**:通信に関して、本法律中の**「トラフィックデータ(traffic date)」とは**、次の各号のすべてに該当するデータをいうが、この文言には、コンピュータファイル又はコンピュータプログラムがそれを蓄積している装置によって特定される範囲のみの通信によってアクセスされる、又は接続される当該ファイル又は当該プログラムを特定するデータが含まれる。 (a)通信を伝送し、又は伝送することができる人、装置又は場所を特定し、又は特定しようとするデータ (b)通信を伝送し、又は伝送することができる装置を特定し、選択し、又は特定若しくは選択しようとするデータ (c)通信の伝送(の全部又は一部)を有効とするための電気通信システムのために用いられる装置を作動させるための信号を含むデータ (d)当該データ又はその他のデータを特定の通信に含まれるデータ又はこれに随伴するデータとして特定するデータ ・**第 21 条**(通信データの合法的獲得及び開示)**第 4 項**:本節中の「通信データ」(communication date)とは、次の各号に掲げるト	・**第 22 条**(通信データの取得及び開示)**第 1 項**:第 2 項に該当する理由により通信データを取得することが必要である、と本節の適用上指名された者が信じたときは、本条の規定を適用する。 ・**同条第 2 項**:次の各号のいずれかにより通信データを取得することが必要であるときは、前項中の、第 2 項に該当する理由により通信データを取得することが必要であるものとする。 (a)国家の安全のため (b)罪を予防若しくは探知するため、又は秩序違反を阻止するため (c)連合王国の経済的繁栄のため (d)公共の安全のため (e)公衆衛生を保護するため (f)政府部局へ支払うべき租税、関税、割当金その他の課税、分担金又は負担金を査定又は徴収するため (g)非常の際に、死亡、傷害若しくは人の身体的若しくは精神的健康への危害を阻止するため、又は障害若しくは人の身体的若しくは精神的健康への危害を軽減するため (h)国務大臣が下した命令をもって、本条の適用上定めた(a 号から前号までの規定に該当しない)目的のため

		ラフィックデータ又は情報をいう。 (a)郵便業務又は遠隔通信システムによって通信を伝送するか、又は伝送することができる場合における当該業務又はシステムのために(送信者によると、その他によるとを問わず)通信に含まれるトラフィックデータ又は通信に付随するトラフィックデータ (b)(前号に該当する情報とは別に)通信の内容を含まず、かつ次の各号に掲げる業務又はシステムの人による利用に関係する情報 (i)郵便業務又は遠隔通信業務 (ii)遠隔通信業務の人への提供又は当該業務の人による利用に関連する、遠隔通信システム (c)郵便業務又は遠隔通信業務が提供される者に関して、当該業務を提供する者が保有又は取得する、a 号又は前号に該当しない情報 **○プライバシーと電子通信に関する規則(EC 指令)**(The Privacy and Electronic Communications (EC Directive) Regulations 2003) ・**第 2 条**(解釈)**第 1 項**:本規則において、 **「通信(communication)」とは**、限られた者の間を、公衆電子通信サービスを利用して、任意の情報の交換や伝送を行うことを意味する。ただし、その情報を受信する特定の加入者または利用者に関連づけることができる情報を除き、プログラムサービス(放送)の一部として伝えられた情報は含まない。 **「トラフィックデータ(traffic data)」とは、**電子通信ネットワーク上の通信の伝送の目的で、又はその通信に関する請求書作成	**○プライバシーと電子通信に関する規則(EC 指令)**(The Privacy and Electronic Communications (EC Directive) Regulations 2003) ・**第 7 条**(トラフィックデータの処理の制限)**第 1 項**:第 2 項及び第 3 項を除き、公衆通信提供者によって処理され、又は保存される加入者又は利用者に関するトラフィックデータは、通信の伝送の目的に必要なくなった際には、 (a)削除されなければならない;又は (b)個人の場合には、その加入者又は利用者の個人データを構成しないように修正しなければならない; (c)企業加入者の場合には、もし加入者が個人ならば、個人

		の目的で処理されるデータを意味し、通信のルーティング、持続又は時間に関するデータを含む。 **「位置データ(location data)」とは**、電子通信ネットワークで処理された、公衆電気通信サービスの利用者の端末装置の地理的位置を示し、以下を含むデータを意味する。 (f)端末設備の緯度、経度又は高度;又は (g)利用者が異動する方向; (h)位置情報が記録された時間	データとならないよう修正しなければならない。 ・**同条第 2 項**:加入者又は相互接続の料金の支払いの目的のために、公衆通信提供者によって保存されたトラフィックデータは、第 5 項の中で指定される間その提供者によって処理し、かつ保存してもよい。 ・**同条第 3 項**:加入者又は利用者に関するトラフィックデータは、以下の場合に、公衆電子通信サービスの提供者によって、処理し、かつ保存してもよい。 (a)そのような処理及び保存が、加入者や利用者に対する電子通信サービスの営業のため、又は付加価値サービスの提供のために行われる場合;かつ (b)トラフィックデータに関係のある加入者又は利用者が、そのような処理又は保存に同意している場合;かつ (c)そのような処理及び保存が、第 a 号の中で指定された目的に必要な間のみ行われる場合。 ・**同条第 4 項**:利用者又は加入者が第 3 項に従い同意していても、いつでもそれを取り消すことができなければならない。 ・**同条第 5 項**:第 2 項でいう間とは、支払いに関して訴訟が行われている、又は申し立てられている場合には、その期間の終わり、若しくはそうした訴訟手続きが行われている場合には、その訴訟手続きが最終決定した時である。 ・**同条第 6 項**:以下の期間まで、訴訟手続きは最終決定されたとして取り扱ってはいけない。 (a)上訴がその期間内にもたらされない場合、どちらか一方によって上訴を行うことができる通常の期間の終了まで(裁判所の命令か、それ以外の命令かによらず、その期間の延長の可能性は除く);又は

			(b)上訴が行われる場合には、その上訴の終了まで。 ・**同条第 7 項:**第 6 項中の上訴は、上訴の許可への適用を含んでいる。 ・**第 8 条**(第 7 条の下でのトラフィックデータの処理に関する追加要件)**第 1 項:**トラフィックデータの形式及び処理の期間に関する情報を、そのデータに関係する加入者または利用者に対して提供していない場合には、公衆通信提供者は、第 7 条第 2 項または第 3 項の下で行われるトラフィックデータの処理を行ってはならない。そして、第 7 条第 3 項の下で行われる処理の場合には、同意を得る前にその情報を提供しなければならない。 ・**同上第 2 項:**第 7 条に従うトラフィックデータの処理は、パラグラフ(3)にリストされた活動の 1 つ以上に必要なものに制限されるものとし、公衆通信提供者、あるいは彼の権限の下で行動する人によってのみ実行されるものとします。 ・**同上第 3 項:**第 2 項で参照される活動は以下に関係のある活動である。 (a)料金請求またはトラフィックの管理; (b)顧客問い合わせ; (c)不正行為の防止または検知; (d)電子通信サービスのマーケティング;あるいは (e)付加価値サービスの提供。 ・**同上第 4 項:**任意の規定に含まれている、またはその規定によって起きている紛争(訴訟手続きまたはそれ以外)の解決に関連したどんな提供のためにも、これらの規則の何も、十分な権威を持つ人へのトラフィックデータの提供を妨げてはならない。

ドイツ	**〇ドイツ連邦共和国基本法** ・**第 10 条第 1 項:**信書の秘密並びに郵便及び電気通信の秘密は、不可侵である。 ・**同条第 2 項:**制限は、法律に基づいてのみ行うことができる。その制限が、自由で民主的な基本秩序の擁護、又は連邦及びラントの存立若しくは安全の擁護のためのものであるときは、法律により、その制限が当事者に通知されないこと、及び裁判上の方法に代えて、議会の選任した機関及び補助機関によって事後審査を行うことを定めることができる。 **〇電気通信法**(Telekommunikationsgesetz) ・**第 88 条**(通信の秘密)**第 1 項:**電気通信の内容及びその詳細な状況、特に、電気通信の伝送に誰が関与しあるいは関与したかどうかという事実は、通信の秘密により守られる。 ・**同条第 2 項:**全てのサービス提供者は通信の秘密を守らなければならない。秘密確保の責務は、基づくべき事実が終了した後も存在するものとする。 ・**同条第 3 項:**第 2 項による責務は、その技術システムの保護に必要な措置を含む電気通信サービスの商業的な提供のために必要な措置により、自らあるいは他者から、電気通信の内容あるいは詳細な状況についての知識を得ることを禁じるものである。その責務は、通信の秘密に守られる事実についての知識を第 1 文にのべる目的の場合に限り、利用することは許される。他の目的のためにその知識を利用すること、特に他者への提供は、本法あるいは他の規定がそれを定めまたその際電気	**〇電気通信法**(Telekommunikationsgesetz) ・**第 3 条**(概念規定): 3.**「属性データ」(Bestandsdaten)とは、**電気通信サービスに関する契約関係の実現、内容の設定、変更あるいは終了についてのデータである。 19.**「ロケーションデータ」(Standortdaten)とは、**電気通信ネットワークにおいて作成され、利用され、また公衆向けアクセスの電気通信サービスのエンドユーザーの端末機器の地点を示すデータである。 30.**「トラフィックデータ」(Verkehrdaten)とは、**電気通信サービスの提供において作成され、加工され、あるいは利用されるデータである。	**〇電気通信法**(Telekommunikationsgesetz) ・**第 96 条**(トラフィックデータ)**第 1 項:**サービス提供者は、それが本章にのべる目的に必要な限り、以下のトラフィックデータを作成し利用することができるものとする。 1.顧客カードあるいは顧客番号の利用において関係する接続、端末装置、個人に関する権利者認識についての番号あるいは特徴、移動体接続の場合には、固定地点データも含む 2.伝送されるデータ量により料金が左右される場合に限り、データ及び時刻についての開始と終了 3.利用者により要求される電気通信サービス 4.固定交換接続の端点、伝送されるデータ量によって料金が左右される場合に限り、データと時刻に関する開始と終了 5.料金精算に加え、電気通信の設置・保守のために必要なその他のトラフィックデータ ・**同条第 3 項:**サービス提供者は、公共的にアクセスできる電気通信サービスの提供者によって利用される加入者関連のトラフィックデータを、関係する者の同意がある場合、その電気通信サービスのマーケティングのため、電気通信サービスの需要に見合った供給のため、そのために必要な時間空間において付加的な利用を持つサービス提供のために利用することができる。発信者データは遅滞なく匿名化されるものとする。第 1 文にのべる目的のためのサービス提供者によるトラフィックデータの利用は、発信者の同意によってのみ認められるものとする。その場合、発信データは遅滞なく匿名化

	通信の提供への関与について明白に規定する場合に限り、許されるものとする。刑法典(Strafgesetzbuch)第 138 条による届け出の義務は優先されるものとする。 ・**同条第 4 項**:船舶内あるいは航空機内に電気通信設備が存在する場合、その運航を行う者あるいはその代表者に対して、秘密の確保の責務が生じるものとする。		されるものとする。 ・**同条第 4 項**:同意を求める場合、第 3 項第 1 文に述べる目的においてどのようなデータ形式で加工されるのか、またどの程度の期間それが蓄積されるのかを、加入者に知らせるものとする。さらに、加入者には常時その同意を撤回できることを知らせるものとする。 ・**第 97 条**(料金通知と料金精算)**第 1 項**:サービス提供者は、第 96 条第 1 項に従い作成されるトラフィックデータを、そのデータが加入者の料金通知と精算に必要な場合に、利用することができる。サービス提供者が外国の事業者の公共的な電話ネットワークでサービス提供する場合、その公共的な電話ネットワークの事業者はそのサービスの提供のために生じるトラフィックデータをサービス提供者に渡すことができる。それが料金徴集及び詳細な計算の準備のために必要な場合、第 2 項に述べるデータを第三者に渡すことができる。その第三者は契約により、第 88 条による通信の秘密の遵守及び第 93 条、第 95 条から第 97 条、第 100 条によるデータ保護を義務づけられるものとする。連邦データ保護法第 11 条はこれに影響されない。 ・**第 98 条**(ロケーションデータ)**第 1 項**:公共的な電気通信ネットワークあるいは公共的にアクセスできる電気通信サービスの利用者に関して利用されるロケーションデータは、それが匿名化されあるいは加入者が同意し、必要な期間内に追加的利用のサービスに必要な措置を準備する場合、それに限り加工することができる。加入者は共同する合意について共

			同利用者に知らせなければならない。加入者は立地データの加工に関する同意を常時撤回することができるものとする。 ・**同条第 2 項**:加入者が立地データの加工に同意する場合、加入者はネットワークへの接続に関するデータあるいは情報の伝送のためのデータの加工を簡明な方法でまた無料により適宜差し止める可能性を持つようにしなければならない。 **第 100 条**(電気通信設備による障害と電気通信サービスの濫用)**第 1 項**:サービス提供者は電気通信設備の障害あるいは故障の確認あるいは修復のため、必要な場合、加入者及び利用者の属性データ及びトラフィックデータを収集し利用することができるものとする。
韓国	**○大韓民国憲法** ・**第 18 条**:すべての国民は、通信の秘密を侵害されない。 **○通信秘密保護法**(통신비밀보호법) ・**第 1 条**(目的):本法は、通信及び対話の秘密と自由に対する制限は、その対象を限定して厳格な法的手続きをふむようにすることによって、通信の秘密を保護して通信の自由を伸張することを目的とする。 ・**同法第 3 条**(通信及び対話秘密の保護):何人も本法と刑事訴訟法又は軍事法院法の規定によらなくては、郵便物の検閲又は電気通信の間諜をしたり、公開されない他人間の対話を録音又は聴取できない。	**○通信秘密保護法**(통신비밀보호법) ・**第 2 条**(定義): 1 **"通信"とは、**郵便物及び電気通信をいう。 2 **"郵便物"とは、**郵便法による通常郵便物と小包郵便物をいう。 3 **"電気通信"とは、**電話・電子メール・会員制定補サービス・模写電送・コードレス呼び出しなどのように有線・無線・光線及びその他の電磁的方式によってすべての種類の音響・文言・符号又は影像を送信するとか受信することをいう。 11 **"通信事実確認資料"とは**次の角材のいずれかにあたる電気通信事実に関する資料を言う。 가 加入者の電気通信日時	**○通信秘密保護法**(통신비밀보호법) ・**第 3 条**(通信及び対話秘密の保護)**第 1 項**:誰でもこの法と刑事訴訟法または軍事裁判所法の規定によらなくては郵便物の検閲・電気通信の盗聴または通信事実確認資料の提供をしたり公開にならない他人の間の対話を録音または聴取することができない。ただし、次の各号の場合には当該法律が決めるところによる。 1 還付郵便物などの処理:郵便法第 28 条・第 32 条・第 35 条・第 36 条などの規定によって爆発物など郵便禁制品が入っていると疑われる小包郵便物(これと類似の郵便物を含む)を開破する場合、受取人に配達できないとか受取人が受領を拒否した郵便物を発送人に還付する場合、発送人の住所・

	○電気通信事業法(전기통신사업법) ・**第 54 条**(通信秘密の保護)**第 1 項**:何人も電気通信事業者が取り扱い中にある通信の秘密を害したり漏洩したりしてはならない。 ・**同条第 2 項**:電気通信業務に従事する者又は従事した者はその在職中に通信に関して知ることになった他人の秘密を漏洩してはならない。	나 電気通信開始・終了時間 다 発・着信通信番号など相手の加入者番号 라 使用度数 마 コンピュータ通信またはインターネットの使用者が電気通信役務を利用した事実に関するコンピュータ通信またはインターネットのログ記録資料 바 情報通信網に接続された情報通信機器の位置を確認することができる発信基地局の位置追跡資料 사 コンピュータ通信またはインターネットの使用者が情報通信網に接続するために使う情報通信機器の位置を確認することができる接続の追跡資料 **○情報通信網利用促進及び情報保護等に関する法律** (정보통신망 이용촉진 및 정보보호 등에 관한 법률) ・**第 2 条**(定義)**第 1 項**:この法で使う用語の定義は次のとおりとする。 3.**"情報通信サービス提供者"とは**「電気通信事業法」第 2 条第 1 項第 1 号の規定による電気通信事業者と営利を目的に電気通信事業者の電気通信役務を利用して情報を提供したり情報の提供を媒介したりする者をいう。	姓名が漏落になった郵便物として受取人が受取を拒否して還付する時にその住所・姓名が分かるために開破する場合または有価物が下がった還付不能郵便物を処理する場合 2 輸出入郵便物に対する検査:関税法第 256 条・第 257 条などの規定による信書以外の郵便物に対する通関検査手順 3 拘束または服役中の人に対する通信:刑事訴訟法第 91 条、軍事裁判所法第 131 条、「刑の執行及び収容者の処遇に関する法律」第 41 条・第 43 条・第 44 条及び軍行刑法第 15 条・第 16 条などの規定による拘束または服役中の人に対する通信の管理 4 破産宣告を受けた者に対する通信:「債務者回復及び破産に関する法律」第 484 条の規定によって破産宣告を受けた者に送った通信を破産管財人が受領する場合 5 混信除去などのための電波監視:電波法第 49 条ないし第 51 条の規定による混信除去など電波秩序維持のための電波監視の場合 ・**同条第 2 項**:郵便物の検閲または電気通信の盗聴(以下"通信制限措置"という)は犯罪捜査または国家安全保障のために補充的な手段に利用されなければならず、国民の通信秘密に対する侵害が最小限に止めるように努力しなければならない。 ・**同条第 3 項**:何人も端末機器固有番号を提供したり提供を受けてはならない。ただし、移動電話端末機製造業社または移動通信事業者が端末機の開通処理及び修理など正当な業務の移行のために提供したり提供を受ける場合にはその限りではない。

			○情報通信網利用促進及び情報保護等に関する法律 (정보통신망 이용촉진 및 정보보호 등에 관한 법률) **・第 45 条**(情報通信網の安全性確保など)**第 1 項:**情報通信サービス提供者は情報通信サービスの提供に使われる情報通信網の安全性及び情報の信頼性を確保するための保護措置を用意しなければならない。 **・同条第 2 項:**放送通信員会は第 1 項の規定による保護措置の具体的内容を決めた情報保護措置及び安全診断方法・手続き・手数料に関する指針(以下"情報保護指針"という)を定めて告示し情報通信サービス提供者にその遵守を勧告することができる。 **・同条第 3 項:**情報保護指針には次各号の事項が含まれなければならない。 1.正当な権限のない者の情報通信網へのアクセスと侵入を防止するとか対応するための情報保護システムの設置・運営など技術的・物理的保護措置 2.情報の不法流出・変造・削除などを防止するための技術的保護措置 3.情報通信網の持続的な利用が可能な状態を確保するための技術的・物理的保護措置 4.情報通信網の安定及び情報保護のための人材・組職・警備の確保及び関連計画の樹立など管理的保護措置 **○情報保護措置及び安全診断方法・手続き・手数料に関する指針** (정보보호조치및안전진단방법・절차・수수료에관한지침)

			・**第 2 条**(情報保護措置の内容):法第 45 条第 2 項によって情報通信サービス提供者が情報通信網義安全性及び情報の信頼性を確保するために用意しなければならない管理的技術的物理的保護措置の具体的な内容は別表 1 に示す。 [別表 1]保護措置の具体的な内容(第 2 条関連) 2.技術的保護措置 2.1.ネットワーク保安 2.1.1.トラフィックモニタリング ・ネットワークモニタリング装置を利用してバックボーン網、主要ノード及び外部網と接続される主要回線のトラフィック疎通量を 24 時間モニタリング

*)通信:ここでは、通信内容、contents を示す用語として使用している。

**)通信データ:ここでは、トラフィックデータ等、通信を成立させるために必要となる通信(内容)以外のデータを示す用語として使用している。

邦訳については以下の資料を参考にしている。

合衆国法典 第 18 編 犯罪及び刑事手続: 国立国会図書館「外国の立法 215(2003.2)」

調査権限規制法: 国立国会図書館「外国の立法 214(2002.11)」

個人情報の処理と電子通信部門におけるプライバシーの保護に関する欧州議会及び理事会の指令(2002/58/EC):
http://www.asahi-net.or.jp/~LG9H-TKG/news030601.htm

一般大衆がアクセスできる、あるいは公共通信ネットワークでの電子通信サービス提供の枠内で発生する、あるいは処理されるデータの保存、並びに指令 2002/58/EC を修正する欧州議会及び理事会の指令(2006/24/EC):「平成 19 年度 内閣官房セキュリティセンター サイバー空間における権利利益の保護・救済のための基盤にかかる調査研究 報告書【概要版】」

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、ICT 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 ICT 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。また、こうした ICT 環境の変化に応じて、情報セキュリティの脅威・課題そのものも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 ICT 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 ICT 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課題への対策の方向性等について、検討を行ってきたところである。

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 ICT 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は 2030 年に 1 億 1522 万人に減少し、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[20]。

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を推進しており、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目指している。国・地方公共団体、企業、働く者といった関係者がそれぞれの役割を果たすことにより、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

[20] 平成 18 年 12 月、「日本の将来推計人口（平成 18 年 12 月推計）」（国立社会保障・人口問題研究所）による。

いくとの予測がある。

（ICT 環境の変化の状況）

近い将来（3 年から 5 年後）の ICT 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、いわば、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状況であると考えられるその具体的な変化の状況は、以下のとおりであると予測される。

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・ゼロ地域の解消

イ）電気通信網の IP 化（NGN:Next Generation Network(次世代ネットワーク)）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、自動車をはじめとした工業製品の ICT 化の進展

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及びそれに伴う API の公開

イ）携帯端末等を利用したホームネットワークに繋がった情報家電の制御

ウ）携帯端末による認証・電子決済

エ）GPS の標準搭載による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、製造等様々な分野での 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[21]）

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 ICT 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）サーバ等への攻撃ではなく、ネットワークに接続した携帯電話や情報家電等のクライアント用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~~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）は減少・消滅せず、脅威は継続・巧妙化していく。

[21] 2005 年 8 月、「ASP 白書」（ASPIC、(財)マルチメディア振興センター）による。

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、ファイアウォール 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）移動通信システムの高度化

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）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）フェムトセル方式の設備が導入される見込みがあるなど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、成りすまし、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、ブロードバンドルータと PC 端末のパーソナルファイアーウォールによるセキュリティレベルと同じレベルの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、自動車をはじめとした工業製品の ICT 化の進展

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、家電製品やロボット・自動車等の工業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 POP3~~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）利用者やサービスなどである程度限定的に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及びそれに伴う 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、ブロードバンドルータと PC 端末のパーソナルファイアヤーウォールによるセキュリティレベルと同じレベルの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、ブロードバンドルータと PC 端末のパーソナルファイアヤーウォールによるセキュリティレベルと同じレベルの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。

近い将来の ICT 環境の変化及びそこに至るまでの変遷過程として挙げられる各項目について、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、前述のとおりである。これらを踏まえ、近い将来における「ユビキタスネット社会」における情報セキュリティに関する主な脅威と課題は、次のようにまとめることができると考えられる。

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~~ ICT 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 ICT 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の ICT 環境における情報セキュリティ脅威等については、今後の情報セキュリティに関する主な課題として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 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~~ ICT 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三~~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、本人が気付かないうちに他人に被害を及ぼす加害者となることから、一部の者のみ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には、以下に掲げる項目について、重点的に検討・実施すべきである。

なお、ここで取り上げた項目以外についても、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必要不可欠かつ現実的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、本人が気付かないうちに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 を利用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。

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等

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、本人が気付かないうちに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の活動等を通じて、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、利用者が自分の問題として認識でき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直接かつ正確に利用者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サイバークリーンセンターの 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％になるという実績が報告されている。

また、現状、小中学生の時代からインターネットや携帯電話といった情報通信機器や ICT サービスを利用する状況にあり、今後も低年齢時から多様な ICT サービスが利用されるものと考えられることから、単に高度な ICT 機器やサービスを扱えるのではなく、交通安全ルールの徹底のように、子供達が安全に安心して ICT サービスを利用できるよう、ICT メディアリテラシーを育成する取組みを、これまで以上に積極的に実施していくことが必要である。さらに、「永遠のビギナー」の一角を占める高齢者等についても、多様な ICT サービスの利用拡大が見込まれることを踏まえ、高齢者や ICT に不慣れな利用者の被害が増大しないよう、積極的な対策が必要である。

加えて、ICT サービスの利用にあたっては、適切な情報セキュリティ対策を講じることは必要不可欠であるが、情報セキュリティに関しては完全な予防策を講じることは困難であり、場合によっては何らかの障害が起り得る可能性があるということを、利用者側に正しく理解してもらう取組みを併せて実施すべきである。

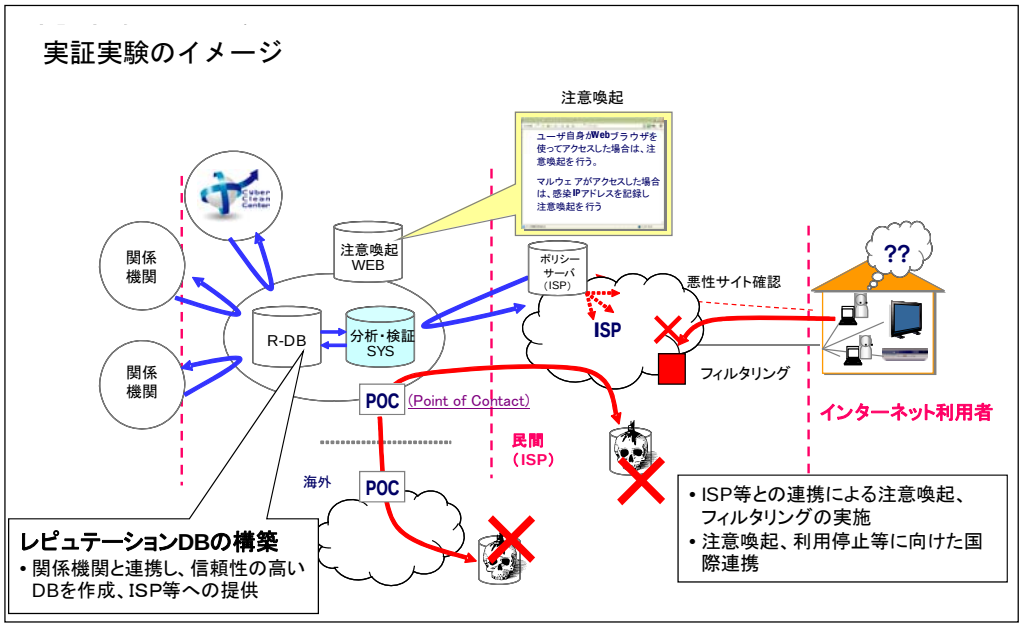
② 電気通信事業者による情報セキュリティ対策の推進

一部の利用者のみ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、こうした対策については、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。

ウ）電気通信事業者による情報セキュリティ対策の実施に関連して、電気通信事業法第 4 条にある通信の秘密との関係を整理することが必要であり、このため、諸外国における法制度及び電気通信事業者が実施する情報セキュリティ対策の実態等を把握することを目的とした詳細な実態調査及び比較検討が必要である。

こうした結果を踏まえ、電気通信事業者が取り得る情報セキュリティ対策等の行動規範の明確化についての検討を継続して実施していくべきである。なお、諸外国から発信されている脅威については、当該国や関係諸国と連携した対処が重要であり、こうした国際連携を円滑に実施する観点からも、諸外国の実態

を把握することは極めて有効である。

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て、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、利用者とサービス提供事業者間等の相互で的確にかつ簡潔に情報交換できるようになることから、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経験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みとして検討することが妥当であると考えられる。

④ 利用者、ICT 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 ICT 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）、ICT 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

（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、攻撃元を詐称した通信の発信源を特定する技術であるIPトレースバック技術については、既に研究開発に取組んでいるところであり、今後ISP間をまたがるシステムの構築や運用方法の確立といったISPでの実装に向けた検討、及び国際的なトレースバックシステムの実現に向けたITU等での国際標準化の取組み等による国際展開を強化すべきである。これにより、仮に発信元が詐称されていても発信源を探知することが容易になり、迅速な事案対応が可能になるものと期待される。

さらに、2007年度に実施した調査[22]等において報告されているように、Web型のマルウェア感染手法が出現している他、ボットの通信プロトコルの変化や暗号化、ウイルス対策ソフトの停止を試みるもの等の手口の巧妙化が確認されており、こうした実態に常に対処するための対策技術の高度化が必要である。また、マルウェアの分類について、現状、一貫したルールがないことから、注意喚起が正しく伝わらず迅速に対応ができない可能性や、セキュリティ対策ソフトの動作が非効率になる可能性、技術者間での情報共有が円滑に行えない可能性などが指摘されており、こうしたマルウェア検出・解析等の効率化に向けた統一的なマルウェアの分類方法や可視化手法等の開発も急ぐべきである。

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、Type 0 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。

[22] 2008年3月「スパムメールやフィッシング等サイバー攻撃の停止に向けた試行に係る請負」報告書(総務省)

③ 暗号・認証技術等の基盤的な研究開発の充実

今後、ICT を利用した様々な社会経済活動が進展すると期待されており、こうしたサービスを安心・安全に利用できるようにするための基盤技術として、成りすましの防止、流通するデータ等の真正性の確保、安全な通信の確保等を実現する暗号・認証技術等の開発が重要である。特に、暗号・認証技術等については、コンピュータの処理能力の向上や解読技術の進展によって、その安全性は時間の経過とともに低下していくことから、常に当該技術の安全性を客観的に評価する必要がある。

実際、これまで広範なシステムで利用されていた鍵長 1024 ビットの RSA 暗号や SHA-1 などの安全性低下が問題視されており、より強固な暗号への移行が必要とされている。なお、暗号の移行にあたっては既存サービス・システムへの影響を考慮し、円滑かつ効率的な移行方式の検討が必要である。

また、モバイルサービスの高度化、~~NGN~~NGN・センサーネット等の新たなネットワークサービスの出現、情報家電・RFID 等の多種多様な機器のネットワーク接続など年々ネットワーク環境は変化しているため、サービス、ネットワーク、機器、ユーザ等の様々な認証対象を柔軟かつ安全に認証する認証連携技術や省電力かつ小型化されたデバイスを実現する認証の実装化技術等の開発が必要と考えられる。

以上のように暗号・認証技術は求められる要件は日々変化しているが、国民の社会生活に密着する重要インフラの安定的な運用、さらにはナショナルセキュリティといった観点から、我が国として国産技術の開発に継続的に取り組むべきであると考えられる。併せて、こうした分野の技術の国際標準化や世界的な利用の普及についても、注力することが重要である。

④ ~~P2P~~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~~DB 高度化技術の検討

~~情報通信技術~~ ICT 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、または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、利用者自身が情報そのものや情報発信元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 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、~~O S~~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。

② 今後の電気通信事業者（ISP）間の情報共有体制のあり方について

これまで、ネットワーク全体に大きな影響を及ぼす形態のセキュリティインシデント等に関して、Telecom-ISAC Japan による電気通信事業者の情報共有・連携対処が有効に機能してきたところである。一方、昨今の脅威は巧妙化、潜行化し、また局所的に深刻な被害を及ぼす形態に変化してきていることから、これまでのような大規模な脅威に備え続けることは言うまでもないが、変化し続ける脅威に常に的確に対応できるよう、不断の検討が必要である。その際に、従前どおりの電気通信事業者間の情報共有・連携対処のあり方に関する機能検証・連携強化に加え、電気通信事業者とセキュリティ対策事業者といった他の業界との間の効果的な情報共有・連携対処のあり方も課題であることから、上記①において行う業界横断的な検討体制の整備や検討状況を参考にしつつ進めることも必要である。

なお、電気通信事業者間の IT 障害に関する情報共有については、2007 年に立ち上げられた T-CEPTOAR における、固定系のネットワークインフラを設置する電気通信事業者、アクセス系の電気通信事業者、ISP 事業者、携帯電話事業者の 4 業態間の連携が促進されるよう、より一層の活動の充実が期待される。

③ 脅威分析等に関する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の専門家が、最先端の脅威やインシデント情報を迅速に情報共有し、かつ有効な対策を提示できるよう、その連携体制の充実を図ることが望まれる。

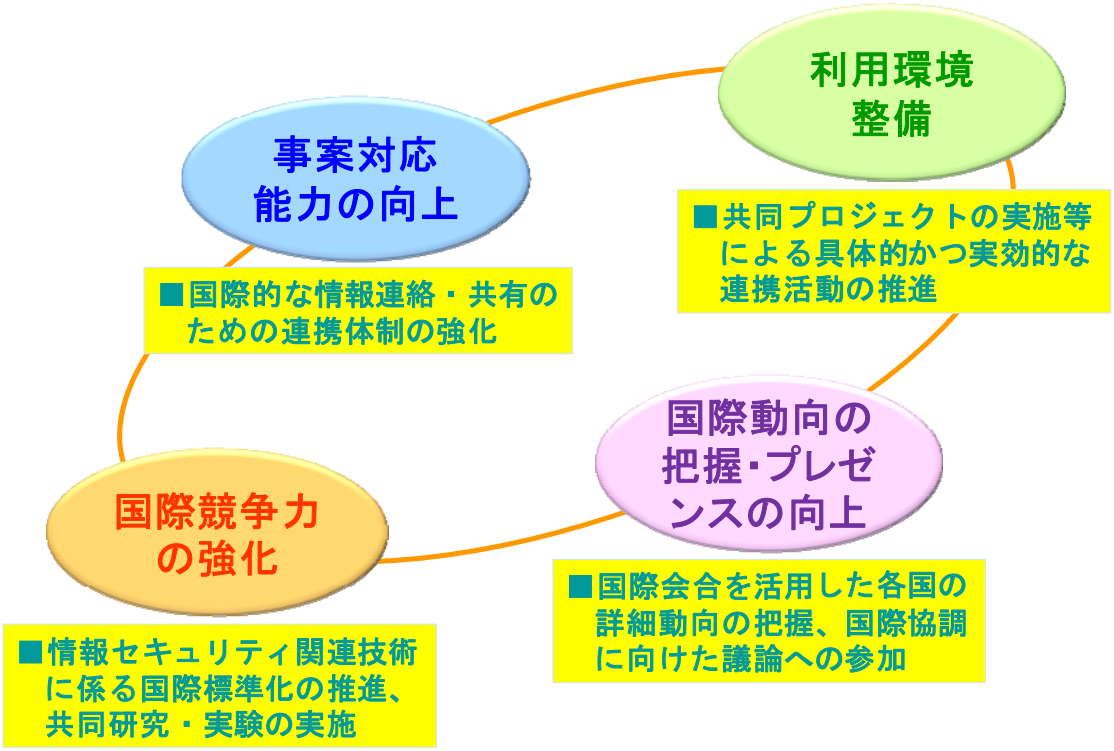
なお、情報共有等の実効性を高めるため、ネットワークインシデントの状況等の調査を行い、再発防止策等を提示する専門的な機関の設置についても、引き続き検討すべきである。

（安心・安全なグローバル ICT 環境の実現に向けた国際連携の推進）

インターネットには国境がなく、海外からの脅威が我が国の ICT 環境に深刻な影響を及ぼす可能性があることは、これまでも繰り返し指摘されてきたところであり、我が国において、利用者が安心して ICT サービスを利用でき、電気通信事業者が安定的に役務を提供できる環境を実現するためには、グローバルな情報セキュリティ確保に向けた積極的な国際連携の推進が不可欠である。

各国・地域間において、法制度、組織体系、文化等の様々な違いが存在する中、実効的な国際連携を実現するためには、リージョナル（地域）／バイ（２国間）の枠組みを活用し、まずは制度・体制等の連携障壁が少なく、同じ方向性を持ったパートナーと連携を開始することで、グローバルな枠組みへのインプットに向けた協力関係を醸成することも必要と考えられる。また、国際連携の成功のためには、自国のみでなく参加する全ての国にメリットのある取組みであることが重要であり、我が国の先進的な取組みを国際的に展開し、各国に積極的にノウハウを提供していくことは、海外における情報セキュリティ対策を促進し、海外からの脅威を未然に防止することに繋がると共に、我が国の情報セキュリティ対策のさらなるブラッシュアップにも役立つ等、結果として我が国における安心・安全な ICT 環境の整備に大きく寄与するものと考えられる。

国際連携の検討にあたっては、事案への対応や情報共有のみならず、脅威を未然に防止するための利用環境整備や情報セキュリティ分野における国際競争力の強化も見据えつつ、以下の 4 つの観点から施策を検討していくことが必要である【図表 5-3 参照】。



図表５-３：国際連携の推進に向けた取組みの方向性

① 利用環境整備

我が国の先進的な取組みを国際的な共同プロジェクトとして展開することで、グローバルな ICT 環境の整備に向けた、実効的な国際連携を推進することが必要である。例えば、サイバークリーンセンターや経路ハイジャック対策について、海外事業者等と連携して推進することで、海外からの脅威を未然に防止し、我が国の安心・安全な ICT 環境の整備を促進することが可能であると考えられる。

② 事案対応能力の向上

２国間・多国間の政策協議や、FIRST 等の既存の情報共有スキームを活用しつつ、電気通信事業者間や所管官庁間をはじめとした、政府から民間までの各レイヤーにおける国際的な情報共有スキームの整備・強化に向けた取組みが必要である。

③ 国際競争力の強化

我が国では、情報セキュリティに関する先進的な技術開発が多数行われており、これらの技術について、国際標準化や共同実験等を通じて国際的に広く展開していくことは、グローバルな ICT 環境の整備に資するのみならず、情報セキュリティ分野における我が国の技術や製品の国際競争力強化の観点からも非常に重要である。例えば、トレースバック技術のような最先端の情報セキュリティ技術を利

用した国際的なフィールド実験プロジェクトを実施し、当該技術の検証・改良に役立てると共に、共同で国際標準化へ向けた活動を展開するといった取組みが考えられる。

④ 国際動向の把握・プレゼンスの向上

以上の施策を円滑かつ着実に検討・推進していくためには、２国間・多国間の政策協議等の国際会合の場を活用し、最新の情報セキュリティ脅威・事案の動向、各国の取組み状況、国際的な議論の趨勢等について継続的な情報収集・調査に努めると共に、我が国の先進的な取組みを世界に発信することで、プレゼンスの向上を図ることが重要である。さらに、各国の情報セキュリティに係る法制度、組織体系や、専門家団体や業界団体の活動状況、既存の国際連携スキーム、標準化の動向等についても調査を実施し、より効果的な国際連携、標準化活動等の検討に資することも必要である。

（情報セキュリティ対策に係る人材育成の推進）

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、~~ICT 領域全般的に、その人材の予備軍であるはずの情報工学系学部学科の学生数の減少、企業が求める人材と高等教育機関が排出する人材の量と質のミスマッチが生じていること等がかねてから指摘されており、特に高度な知識や経験を必要とする情報セキュリティ分野については、その傾向がより顕著であると考えられる。

こうした状況を踏まえ、「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）では、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ることり、~~「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~~が~~~~において~~指摘されている~~ところである~~。

また、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、2008 年 5 月に最終的な報告書をとりまとめている。同報告書では、高度 ICT 人材育成に向けた取組みの基本方針として、必要な高度 ICT 人材が自律的に輩出されるようなメカニズムが構築されることが必要とされており、そのため産学官が連携して総合的・複合的に実施する必要がある取組みとして、1)ICT 産業構造の改革、2)高度 ICT 人材予備軍（新卒採用段階）の実践的な能力の育成、3)高度 ICT 人材候補者（社会人）の継続的育成、4)グローバル化への対応、5)高度 ICT 人材育成の取組みの横展開の推進（高度 ICT 人材の量的拡大、地方人材の育成）、6)高度 ICT 人材育成を一体的、継続的に進めるための推進体制の強化・整備が挙げられている。さらに、喫緊に取り組む必

要がある高度 ICT 人材育成策として、1)実践的な高度 ICT 人材育成に特化した新たな「育成の場」の整備、2)ICT 人材の育成の場を社会・経済・産業の環境・ニーズの変化に的確に対応できるよう支援するための仕組み（ナショナルセンター的機能）の整備が必要との提言がなされている。

さらになお、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としている。

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通信データ等を活用して、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予定している。

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。

その他さらに、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 PBL（Project Based Learning）教材（情報セキュリティマネ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、より一層の取組みの強化が期待される。

（その他、継続的な検討課題）

上記のほか、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について、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について、サイバー犯罪等に関連する法制度について、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について、等が継続的な検討課題として挙げられる。

６．終わりに

本研究会では、現状の ICT 環境において顕在化している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年から５年後の将来における ICT 環境の姿を想定し、その変遷過程を含めた ICT 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整理・峻別してきたところである。

特に、今回の取りまとめにおいては、近視眼的な対策の導出のみにとらわれず、現時点では直ぐに具体的な対策として導入できるものでなくとも、将来の安心・安全な ICT 環境の確保に向けて情報セキュリティ政策を実施していく際に重要な視点となる様々な検討の方向性についても言及している。

今後も ICT 技術の高度化や提供される ICT サービスの多様化が進み、現時点では想定されていない新たな脅威や課題が発生することが容易に想像されることから、ますます複雑化する状況に適時かつ適切に対応するために、関連する各主体が連携した対策を実施していくことが、これまで以上に必要になるものと考えられる。

以上を踏まえ、情報セキュリティ対策が適切に施された安心・安全な ICT 環境が構築されるよう、本報告書にある個別施策を着実に実施するとともに、引き続き検討すべき課題及び今後発生する新たな課題について、その具体的な対策の実施に向け、継続的かつ精力的に検討していくことが重要である。

こうして実現される安心・安全な ICT 環境を基盤として、より一層、我が国の生産性向上や国際競争力の強化が実現されることを期待するものである。

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 サービス事業統括本部 セキュリティ情報統括部 部長
佐田　昌博	㈱ウィルコム 技術本部 副本部長
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　郁夫	弁護士（第 7 回～）

	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 シニアマネージャ
	徳田　敏文	日本アイ･ビー･エム㈱ 経営イノベーション
		情報セキュリティ推進室 情報セキュリティ担当部長
【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
		シニアマネージャー
	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 総合メディアセンター長
	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 担当部長

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）

	・福智構成員（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み）
第 6 回 （4 月 3 日）	○ 中間報告書のとりまとめ ○ 重点的に検討・実施すべき事項の具体化　等 プレゼンテーション： ・有村構成員（T-ISAC-J モデル（事業者間連携スキーム）2.0　官民連携スキーム 2.0 に関する考察） ・NTT コミュニケーションズ（新たな安全・簡単アイデンティティ管理体系　セキュア・アイデンティティ流通基盤）
第 7 回 （5 月 1 日）	○ 情報セキュリティに関する国際連携について　等 プレゼンテーション： ・中尾構成員（国際連携・協調について） ・齋藤構成員（ISP から見た国際事案とその協調対処について）
第 8 回 （5 月 23 日）	○ 中間報告書の意見募集結果について ○ モバイル環境及び Linux システムにおける Malware の脅威について ○ ISP の活動と通信の秘密について　等 プレゼンテーション： ・セキュアブレイン（モバイル環境における Malware 等の調査） ・日本電気（Linux システムにおける Malware の脅威に関する調査研究） ・高橋郁夫構成員（ISP の活動と「通信の秘密」）
第 9 回 （6 月 18 日）	○ 情報セキュリティに関する調査研究・研究開発の動向について プレゼンテーション ・NTT 情報流通プラットフォーム研究所（ボットネット実態調査） ・奈良先端科学技術大学院大学（トレースバック技術への取組み） ○ 報告書（案）について　等
第 10 回 （7 月 2 日）	○ 報告書のとりまとめについて

用語集

abuse／abuse 対応

スパムメール発信や、掲示板への悪意ある書き込みなどの迷惑行為。また、このような迷惑行為を受けた人から来る苦情に対応することを abuse 対応という。

APEC TEL：Asia-Pacific Economic Cooperation Telecommunications and Information Working Group（アジア・太平洋経済協力　電気通信・情報作業部会）

APEC とは、アジア太平洋地域の持続可能な発展を目的とし、域内の主要国・地域が参加するフォーラムで、域内の貿易投資の自由化・円滑化、経済技術協力を主要な活動とする。APEC には 13 の分野担当大臣会合が設けられており、情報通信分野については、電気通信・情報産業担当大臣会合（TELMIN）によって示された指針の下、電気通信情報作業部会（TEL WG）において具体的な議論、検討が行われている。

API：Application Program Interface

アプリケーションを開発する際に使用できる命令や関数の集合。

APT：Asia-Pacific Telecommunity（アジア・太平洋電気通信共同体）

アジア・太平洋地域における電気通信に関する専門機関。アジア太平洋地域における電気通信の均衡した発展を目的として、研修やセミナーを通じた人材育成、標準化や無線通信などの地域的な政策調整及び電気通信問題の解決等を行う。

APWG：Anti-Phishing Working Group

金融機関、オンラインショッピング事業者、ISP、メーカー、法執行機関、消費者団体等、世界中の関係者から構成されるフィッシング対策を実施している団体。

ASEAN：Association of Southeast Asian Nations（東南アジア諸国連合）

１）域内における経済成長、２）地域における政治・経済的安定の確保、３）域内諸問題の解決を目的として東南アジア 10 カ国が加盟する地域連合。

ASP・SaaS：Application Service Provider / Software as a Service

ネットワークを通じて、アプリケーション・ソフトウェア及びそれに付随するサービスを利用させること、あるいはそうしたサービスを提供するビジネスモデル。

BCP：Business Continuity Plan（事業継続計画）

何らかの障害が発生した場合に重要な業務が中断しないこと、または業務が中断した場合でも目標とした復旧時間内に事業が再開できるようにするための対応策などを定めた包括的な行動計画。

C&C サーバ：Command and Control サーバ

ボットネットの管理者等からの指令を感染したコンピュータに中継する機構。

CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response

IT 障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止のため、政府庁から提供される情報について、適切に重要インフラ事業者等に提供し、関係重要インフラ事業者等間で共有することにより、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資するため、国内の 10 重要インフラ分野内に整備している「情報共有・分析機能」。

CEPTOAR-Council

それぞれの分野に整備された CEPTOAR の代表で構成される協議会とし、各重要インフラ分野ごとのサービスの維持・普及に係る情報のうち、複数の重要インフラ分野に共通するもの、及び分野を越えたベストプラクティス等の共有を行うもの。

CERT/CC：CERT コーディネーションセンター

インターネットを介した不正アクセス、不正プログラム、システムの脆弱性に関する情報を収集・公開する団体。

CSIRT：Computer Security Incident Response Group

情報システムの運用におけるセキュリティ上の弱点・問題に関する報告を受け、その調査、対応活動などを行う組織の一般名称。

CVE：Common Vulnerabilities and Exposures

オープンソースを含めたソフトウェア製品の脆弱性について、ID を付与することで、脆弱性情報の一意性を確保するためのプロジェクト。

DoS 攻撃：Denial of Service Attack（サービス妨害攻撃）

大量のデータを特定宛先に送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃をいう。また、多数の PC から一斉に行われる DoS 攻撃を **DDoS 攻撃**（Distributed Denial of Service Attack（分散型サービス妨害攻撃））という。

EVSSL：Extended Validation SSL

米 CA/Browser Forum によって標準化された SSL サーバ証明書。従来の SSL 証明書より、証明書発行時発行時の認証プロセスの審査がより厳格である。

FIRST

民間企業、政府機関、学術機関等、世界中の CSIRT 等のインシデント対応組織が参加し、インシデント情報の交換や協力等を行う国際フォーラム。

FMC：Fixed Mobile Convergence（固定通信と移動通信の融合）

携帯電話を家の中では固定電話の子機として使えるといったような移動体通信と有線通信を融合した通信サービス。FMBC（Fixed Mobile Broadcast Convergence（固定通信と移動通信と放送の融合））とは、FMC に放送を融合した通信サービス。

ICMP Echo リクエスト

インターネット制御通知プロトコルである Internet Control Message Protocol のうち、ネットワーク接続状況をテストするための信号。通常 ping と呼ばれ、実装されている。

IDS：Intrusion Detection System（侵入検知システム）

ネットワークを監視し、侵入や異常を検知して管理者に通報等するシステム。

IETF：Internet Engineering Task Force

インターネット上で利用される各種プロトコル等を標準化する任意組織。

iframe

インラインフレーム。Web ページ上にフレームとして他所の Web ページを埋め込む要素のこと。

IGF：Internet Governance Forum（インターネット・ガバナンス・フォーラム）

2003 年及び 2005 年に開催された世界情報サミット（WSIS：World Summit on the Information Society）の結果を受け、国連事務総長主導の下、インターネット管理に関する課題をオープンかつ包括的に議論するために設置されたフォーラム。

IPS：Intrusion Prevention System（侵入防止システム）

不正なパケットを自動的に遮断する機能など、インターネットに接続されたネットワークやサーバを不正侵入から防御するためのシステム。

IPsec：Security Architecture for Internet Protocol

暗号技術を用いて、データの改ざん防止や秘匿機能を提供する通信プロトコル。

IPv4：Internet Protocol Version4

現在のインターネットで利用されているインターネットプロトコル。IP アドレスによって通信経路の制御を行っているが、インターネットの急速な普及により、アドレス資源の枯渇が生じると予測されている。

IPv6：Internet Protocol Version6

IPv4 をベースに、管理できるアドレス空間の増大、セキュリティ機能の追加、優先度に応じたデータの送信等の改良を施した次世代インターネットプロトコル。

ISMS：Information Security Management System

個別の問題の技術対策の他に、事業リスクに対する取組み方に基づき、自らのリスクアセスメントにより必要なセキュリティレベルを決め、適切な情報セキュリティを確立し、運用、監視、維持及び改善を行う仕組みのこと。

ISO/IEC ： International Organization for Standardization/International Electrotechnical Commission（国際標準化機構/国際電気標準会議）

各国の代表的標準化機関から成る国際標準化機関で、ISO は電気及び電子技術分野を除く全産業分野の、IEC は電気及び電子技術分野の国際規格の作成を行っている。情報通信分野については、JTC1（Joint Technical Committee 1）において、合同で審議が行われている。

ITU-T ： International Telecommunication Union – Telecommunication Standardization Sector（国際電気通信連合　電気通信標準化部門）

電気通信分野における技術、運用及び料金を世界的規模で標準化するための研究を実施している国連の専門機関。

Linux

UNIX 互換のオープンソース・ソフトウェアの OS。ソースコードの公開、再配布、改変の自由を認めるといったライセンス体系に基づいている。

MAAWG：Messaging Anti-Abuse Working Group

米国を中心に通信事業者やベンダ等により構成される迷惑メール対策団体。

MMI：Man Machine Interface

人間が機械を操作したり、機械が人間にデータを伝えるための、人間と機械の接点における仕組みやルールなどの総称。

NAT：Network Address Translation

インターネットに接続された企業等で、一つのグローバルな IP アドレスを複数のコンピュータで共有する技術。

NNI：Network-Network Interface

NGN において、ネットワーク間を接続するためのインタフェース。

OECD/ICCP：Organisation for Economic Co-operation and Development/ Committee for Information, Computer and Communications Policy（経済協力開発機構　情報・コンピュータ通信政策委員会）

OECD は、先進国間の自由な意見交換・情報交換を通じて、１）経済成長、２）貿易自由化、３）途上国支援に貢献することを目的とした国際機関である。ICCP は OECD に 29 設置されている委員会の１つで、情報・コンピュータ・通信に関するシステム・サービスの分野における技術の発展とその応用から生じる政策課題と、これらが経済・社会に与える影響ついて検討を行っている。

P2P：Peer to Peer

不特定多数のコンピュータを直接接続して情報をやり取りするネットワーク形態。

POP3：Post Office Protocol Version 3

メールサーバに保存されている電子メールを電子メールソフトが取りに行く際に利用されるプロトコル。

RAISE Forum：Regional Asia Information Security Exchange Forum

セキュリティ標準の開発、選定、展開に関する経験や知見を共有するための場を提供するとともに、国際標準の開発や普及のためのアジア地域における協力を促進することを目的としたフォーラム。

RFID：Radio Frequency Identification

IC チップを利用した非接触認証技術。

RSA：Rivest Shamir Adleman（開発者３名の名前）

桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つ。

SHA-1：Secure Hash Algorithm 1

認証やデジタル署名等に使われるハッシュ関数の一つ。160 ビットのハッシュ値を生成する点が特徴で、データの改ざん検出に利用される。

SNI：Application Server-Network Interface

NGN において、各種アプリケーションサーバとネットワークを接続するためのインタフェース。

SNS：Social Networking Service

人と人とのコミュニケーションを促進・サポートするコミュニティ型の Web サービス。具体的には、参加者はオンライン上で自分のプロフィールや日記を公開し、共通の趣味や友人の友人といったつながりを通じて新たな人間関係を構築する。

SSO：Single Sign-On

一回の認証処理で複数のサービスを利用可能とする認証機能。

SWIS：Standardization Workshop on Information Security

日本、中国、韓国を中心として、情報セキュリティ関連技術等の国際標準化を目指すワークショップ。

SYN Flood 攻撃

サーバを機能停止に追い込む DoS 攻撃の手法の一つで、確立しない TCP 接続を大量に試みる攻撃のこと。

TCP：Transmission Control Protocol

インターネットで標準的に使用されている通信プロトコル。インターネットにおける主要なサービスに使用される通信プロトコルの基盤となっている。

TEMPEST

コンピュータや周辺機器などが発する微弱な電磁波から様々な情報を盗み出す技術。

Type 0 Routing Header （RH0）問題

IPv6 Protocol Type 0 Route Header の仕様によるぜい弱性で、Type 0 ルーティングヘッダをに関し、経由地指定を大量に行うことにより、ぜい弱性の影響を受けるホスト間でのネットワークトラフィックを増大させる DoS 攻撃が可能となる問題。

UNI：User-Network Interface

NGN において、ユーザ（端末機器）とネットワークを接続するためのインタフェース。

UPS：Uninterruptible Power Supply（無停電電源装置）

大容量のバッテリーを内蔵し、商用電源の停電時に内蔵バッテリーから電源を供給する装置。

VPN：Virtual Private Network

公衆回線をあたかも専用回線のように仮想的に利用できる技術。

Web ホスティングプロバイダ

インターネットに情報を発信するコンピュータ（サーバ）の容量の一部を間貸し、Web の運営サービスを提供する事業者。

Winny

日本で開発されたファイル共有ソフトの一つで、利用者同士で自動的にネットワークを形成し、所持しているファイルのリストが共有できる。高い匿名性が主な特徴。

アラートサービス、アラートレポート

セキュリティインシデントなどの発生等を知らせるサービス。

インシデントハンドリング

インシデントの未然防止、拡大防止・早期復旧、再発防止のための対応。

ウイルス（コンピュータウイルス）

他人のコンピュータシステムを破壊すること等を目的に作られた特殊なプログラム。感染活動のために、自分自身を複製する仕組みを持ち、ウイルスが埋め込まれた電子メールやホームページの閲覧等を通して次々と増殖するものもある。

オーバーレイ・ネットワーク

既存ネットワークの上位層において目的に応じた仮想的なリンクを形成／構成する別ネットワーク。

キーロガー

キーボードの入力等の操作状況を記録するプログラム。

組み込み機器

特定の機能を実現する目的でコンピュータを組み込んだ電子機器の総称。

経路ハイジャック

各インターネットサービスプロバイダのルータは通信経路を確立するために経路情報を保持・交換しているが、誤った経路情報をネットワーク上に広報することにより、正しいネットワークに情報を到達させなくしたり、情報を横取りしたりすること。

公開鍵暗号基盤（PKI）：Public Key Infrastructure

公開鍵暗号を用いて、盗聴・なりすまし・改ざん・事後否認といった危険性に対して、安全な電子通信を確保するための仕組み。

自動転送型ファイル共有ソフト

インターネットで不特定多数のユーザとファイルをやり取りすることができるファイル共有ソフトの中で、情報を管理するサーバがなく、すべての情報がバケツリレー方式で利用者間を転送される仕組みを持ったソフトウェア。Winny などが該当する。

情報セキュリティインシデント

情報管理やシステム運用に関して脅威となる現象や事案のこと。ウイルス感染や不正アクセス、情報漏えい、迷惑メール送信、DoS 攻撃等が含まれる。

情報セキュリティマネジメント

組織における情報セキュリティ目標を設定し、リスクアセスメントに基づいた適切な管理策を選択、実施するとともに、見直し、改善を行うことで、継続的に情報セキュリティ確保に努めること。

スキミング

他人のクレジットカードやキャッシュカードの磁気記録情報を、「スキマー」と呼ばれるカード情報読取り装置を用いて不正に読み出し、複製する行為。

スパイウェア

利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム。

スパムメール

受信者の都合を無視し、無差別にメールを大量配信すること、又はこのようにして配信されるメール。

スピア型メール

ある特定の地域、国、企業、団体、一般利用者などを標的とし、当該標的のみを攻撃することを目的として送られるメール。

ソーシャルエンジニアリング

ネットワークシステム等への不正侵入を達成するために必要な ID やパスワードなどを、人間の心理的な隙などを突いて入手する方法。

ターゲットアタック

不特定多数への攻撃ではなく，ある特定の地域、国、企業、団体、一般利用者などを標的とした攻撃。

ダウンローダ

特定の Web サーバなどからマルウェア等をダウンロードするプログラム。

ツールキット

フィッシングサイトやマルウェア等を容易に作成するために、頻繁に使用されるパーツなどがまとめられているソフトウェア。

デジュール標準

標準化機関により制定された標準で、明確に定められた手続に基づき広範な関係者の参加を得て策定されるもの。

トラッシング

ソーシャルエンジニアリングの手法のひとつ。ごみ箱やごみ集積所などから，機密情報や個人情報等を収集する行為。

トロイの木馬

コンピュータの内部に潜伏して、システムを破壊したり、外部からの不正侵入を助けたり、そのコンピュータの情報を外部に発信したりするプログラム。

トンネリング

インターネット等の公衆回線網上に、ある２点間を結ぶ閉じられた仮想的な直結通信回線を確立すること。

ネイティブ機能

その機器にある固有の機能。

バイナリコード

実行ファイルなど、コンピュータが直接解釈して実行できる形式で表現されたプログラム。

パスワードクラッキング

様々なパターンのパスワードでログインを試み、他人のパスワードを探り当てること。辞書攻撃や総当たり攻撃（ブルートフォースアタック）などの手法がある。

ファームウェア

ハードウェアの基本的な制御を行うために、あらかじめ機器に組み込まれたソフトウェア。

ファイアウォール

外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことを目的としたシステム。またはシステムが導入された機器。

ファイルアイコン

アプリケーションやファイルを識別しやすいよう画像によって記号化したもの。

フィッシング（phishing）

金融機関等からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人の金融情報（クレジットカード番号、ID、パスワード等）を入力させるなどして、個人情報を不正に入手する詐欺的な行為。

フェムトセル方式

超小型で出力が非常に小さな携帯電話基地局が、半径数十メートル程度の通話エリア（セル）をカバーする方式。

フォーラム標準

関係するメーカー、団体、個人などの関係者により構成される任意の組織をフォーラムと言い、国際的に広く開放されたフォーラムにおいて作成される民間の標準。

プロキシ

インターネットとの接続を代行するシステム。

ブログ

インターネット上で公開されている日記形式のホームページのこと。

ペネトレーションテスト

セキュリティ上の脆弱性を発見するために、実際にシステムなどを攻撃して侵入を試みるテスト手法。

ボット／ボットウイルス

コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク（インターネット）を通じて外部から操ることを目的として作成されたプログラム。

マクロ型ウイルス

マイクロソフト社の Office 製品等のアプリケーションソフトに搭載されているマクロ機能を使って作成されたコンピュータウイルスのこと。Melissa（メリッサ）等が有名。

マスメーリング型ウイルス

電子メールに自身のコピーを添付して拡散するコンピュータウイルス。

マルウェア

malicious software を組み合わせた造語。コンピュータウイルス、ワーム、スパイウェアなどの「悪意のあるソフトウェア」の総称。

マルチキャスト通信

複数の通信相手先に対してデータを同時配信する通信方式。

メインフレーム

企業等の基幹業務システムなどに用いられる大規模コンピュータ。

リダイレクト

ある Web サイトから別の Web サイトに自動的に転送させること。

リバースソーシャルエンジニアリング

ターゲット側から不正侵入するために必要な ID やパスワードなどの情報を、攻撃者に提供してしまうこと。

ワーム

他のファイルに寄生して増殖するのではなく、自分自身がファイルやメモリを使って自己増殖を行うタイプのウイルス。