国際連携による安全・安心なインターネット社会の構築に向けて

第１回インターネット・ガバナンス・フォーラム（IGF）への提言

2006 年 10 月 17 日

(社)日本経済団体連合会

Ⅰ．はじめに

１．情報革命がもたらす経済・社会構造の変化と新たな課題

インターネットに代表される情報通信技術の発展は、国民生活の利便性の向上や新ビジネスの創造等の大きな成果をもたらすとともに、現在の社会・経済構造に変革をもたらしつつある。たとえば、電子メールによる地球規模での瞬時の情報交換、在宅勤務や遠隔医療の実現、IP マルチキャスト[1]等による通信・放送の融合など、インターネットを中核としたイノベーションが進行中である。さらに、インターネットにより、世界中の誰もが多様な形態の情報、コンテンツを作成し、それを世界中に発信できる環境が整ったことで、情報やコンテンツが広く世界で利活用されるという知の創造と交流の新たなサイクルも登場している。

このような情報社会の基盤であるインターネットは、まさに企業にとってのインフラでもあり、その自由かつ安全な利活用を支えるガバナンス、セキュリティの問題は、産業界にとっての重要な課題である。特に、日本は世界最高レベルのブロードバンド環境を有し、最もインターネットの恩恵を享受している国家の一つとして、世界の情報インフラであるインターネットの安定運用と発展に貢献すべき立場にある。

一方、インターネットの発展は、サイバー犯罪やスパム[2]の増加、デジタル・デバイド[3]拡大等の負の課題を生み出している。これらの課題について、国際社会としての対応が強く求められているが、インターネットがなかった時代の国際ルールをそのまま適用することはできず、また、各国ごとの個別対応では十分な成果を得ることが難しい。従って、国際協調による新しい制度や解決策について、早急に検討しなければならず、この成否が情報社会の健全な発展の鍵を握っている。

２．サミットからフォーラムへ

情報通信技術の発展に伴う、先進国と途上国の間のデジタル・デバイド拡大、および、インターネットが抱える諸課題に応えるため、国連は、世界中のステークホルダーが議論を行なう場として世界情報社会サミット（World Summit on the Information Society：以下 WSIS）を開催した。

第１回 WSIS（2003 年 12 月 於ジュネーブ）では、インターネットに関する幅広い分野についての議論を行ない、国際協力の重要性およびデジタル・デバイド解消の必要性などに

---

1 インターネット等を利用して、コンテンツを特定多数に同時送信するサービス形態。

2 営利目的等で無差別大量に送信される迷惑メールの通称。2005 年現在、世界で流通している電子メールの約７割がスパム(スパムメール)と言われている（総務省：迷惑メールへの対応のあり方に関する研究会最終報告書 http://www.soumu.go.jp/s-news/2005/050722_2.html）

3 情報技術を十分に利活用できるものと、そうでないものとの間に生じる格差。

関する基本的な認識を盛り込んだ「基本宣言」および「行動計画」を採択した。

第２回 WSIS(2005 年 11 月 於チュニス)では、第１回 WSIS で議論が収斂しなかった「誰がどのようにインターネットを管理・運営するか」という資源管理[4]に関する問題が焦点となった。このテーマは政治問題化され、米国を中心とする、現行のインターネット管理体制の継続を主張するグループと、米国中心の管理体制に反対するグループとの間で議論が紛糾し、インターネットが分断される最悪の事態も想定された。また、本来 WSIS の場で議論されるべき、セキュリティ対策、デジタルデバイドの解消等の諸課題の検討が不十分となることも懸念された。

日本経団連では、第２回 WSIS の開催に先立ち、提言「インターネットガバナンスのあり方について[5]」を公表し、日本の産業界としての意見を表明するとともに、ミッションを派遣し、本会議等で民間主導によるインターネット管理体制の継続や、マルチステークホルダーによる対話の継続を主張し、国際商業会議所（ICC）等の関係団体や日本政府と共同で働きかけを行なった。その結果、第２回 WSIS では、「インターネット資源の管理については、課題もあるものの、既存の枠組みは効果的に機能している」こと、「インターネット・ガバナンス・フォーラム（IGF）を設置し、マルチステークホルダーの参加による議論を継続する」ことが宣言に盛り込まれた。結果的に経団連の提言内容がほぼ反映されているが、セキュリティ問題をはじめとする諸課題への対応は、IGF に持ち越された。

IGF は、マルチステークホルダーによる対話のための会合（multi-stakeholder policy dialogue）と位置づけられ、国連事務総長の主催により、本年 10 月末にその第１回会合がギリシア(アテネ)で開催される。われわれは、世界中のマルチステークホルダーが集まる IGF に向けて、ブロードバンド先進国である日本の知見を紹介するとともに、安全・安心なインターネット社会の構築に向けた具体的な提案を行い、IGF に日本の産業界として貢献する。

---

4 インターネットは協調・分散管理をその基本的な枠組みとしているが、ネットワーク上での一意性を確保する必要があるため、基幹である IP アドレスおよびドメイン・ネーム・システム部分では、集中管理となっている。WSIS では ICANN （Internet Corporation for Assigned Names and Numbers）を中心とした米国主導型の管理システムであることが議論の対象となった。

5 http://www.keidanren.or.jp/english/policy/2005/065.html 参照。同提言における主な内容は以下のとおりである。
①ICT の利活用による経済発展や福利厚生の増進を、利用者の立場で考えることを基本スタンスとして、デジタルデバイドの解消、セキュリティ対策、流通するコンテンツの知的財産権確保など、信頼できる利活用環境の整備のための諸課題について、国際機関、政府、民間企業、市民社会が一緒に議論することが重要である。
②懸案事項となっているインターネット資源の管理について、環境変化への柔軟な対応や迅速な意思決定ができる、民間部門による管理を継続することが妥当であり、政治問題化すべきではない。
③WSIS 閉幕後も、インターネットに関する諸課題について、マルチステークホルダーの参加による議論を継続すべき。

Ⅱ．IGF へ向けた提言

１．基本的な考え方

（1）IGF の役割

自由で開かれたインターネットは、民間主導で発展してきたが、それをより安全かつ安心して利用できる環境を構築することこそ、国際社会の最重要課題である。このような課題については、すでに G8、OECD、EU をはじめ、多国間の枠組みでの検討がなされているが、世界各国のマルチステークホルダーによる会合であるという点で、IGF はより広範な国際社会のコンセンサス形成の場として最適と考える。このことを最大限に生かし、IGF では国際社会の協調、パートナーシップによる対応が必要である「安全・安心なインターネット社会の実現に関する課題（セキュリティ対策やスパム対策等）」および「インターネットの利活用を支える社会的・文化的基盤の整備に関する課題（セキュリティ教育、表現の自由とコンテンツ規律のバランス問題等）」について、国際機関、各国政府、企業、市民社会の知見を集め、必要となる対策に関するコンセンサスの形成、あるいはベストプラクティスの共有等を促進すべきである。そして、国際機関、既存団体等の意義ある活動成果を共有し、また、IGF での議論を参考にして、さらに個別組織における取り組みの課題解決力を向上させる、という好循環を作り上げる機能が、IGF には求められる。

（2）第一回 IGF への期待

日本経団連は、第１回 IGF においては「検討の緊急度が高いもの」「インターネット社会発展の根本に関するもの」を優先的に検討すべきであり、WSIS で十分検討されなかった信頼できるインターネット環境の構築等について議論を行なうことが重要であると考える。今回設定されたテーマ[6]は日本経団連の提案とほぼ一致しており、課題の設定については評価できる。

われわれは、民間主導による自由で開放的なインターネットの存在が、今日の情報社会の発展の基礎であり、現行のガバナンス体制は、今後とも維持されるべきと考える。しかし、ウイルス、フィッシング、スパム等によって、インターネットの安全・安心な利活用が阻害されている現状を放置し、インターネットの世界が無法地帯と化してしまうことは防がなければならない。そこで、自由・開放性と安全・安心のバランスをうまくとりつつ、誰もが自由に不安なく利用できるインターネット社会を実現させるための方策について、日本の産業界として、今回の IGF に向けて具体的な提案を行ないたい。

安全・安心なインターネット環境は、国ごとの個別対応では十分な効果は期待できず、各国の知見を踏まえ、IGF の場で意見と情報の交換が行なわれることが重要である。たとえばセキュリティ対策では、国境を越えた犯罪が一般的であるため、どこか一箇所でも対策レベルの低い国があると、そこが犯罪の温床となりかねない。また、BOT[7]等により、利用者が意図せずに犯罪に加担してしまう可能性もあるため、利用者も含めた全ての関係者が関与しなければ、十分な成果が得られない。

---

6 第１回 IGF における検討テーマは、多くの関係者が数ヶ月にわたり検討を重ねた結果、「開発のためのインターネット・ガバナンス」を全体テーマとした上で、「開放性」「セキュリティ」「多様性」「アクセス」の４つとなった。

7 利用者の知らないうちに PC にインストールされ、製作者の指令で動作するプログラム。迷惑メールや DDoS 攻撃等のほとんどは、BOT により引き起こされていると考えられている。

インターネット社会が持続的に発展するためには、「安全・安心」に利用できる環境整備に向け、国際機関、世界各国の政府、企業、市民社会が連携することが何よりも重要であり、また、これらの課題解決には、国際社会の共同アクションが不可欠である。そのための枠組みについて、以下、具体的な提案を提示する。

また、ブロードバンド先進国である日本は、スパム対策やP2P[8]技術を利用したファイル共有ソフトの悪意ある不正目的利用等について、先行して様々な事象を経験している。後段において、これらの事象への対応をケースとして整理しているので、今後、各国でブロードバンド化が進む中、ベスト・プラクティス、あるいは反面教師として、是非活用してもらいたい。

２．安全・安心なインターネット社会の実現に向けた提案

（１）セキュリティ確保のための新たな国際連携

①国際的な情報共有体制の構築

対策レベルが劣っている国・地域があると、犯罪者は、サイバー攻撃を仕掛けるためのインフラとして、その地域のシステムやマシンを利用し、BOT 等により攻撃をしかけてくるため、一国での個別対応のみでは、セキュリティ確保のための十分な対策を行なうことはできない。従って、国際社会が一致団結し、インシデント情報や対策ノウハウに関する情報等を共有するとともに、協調してセキュリティ対策にあたるための仕組み作り[9]を目指すべきである。

FIRST(Forum of Incident Response and Security Teams.[10])は、各国のCSIRT[11]間でのセキュリティ情報の交換を行なっており、セキュリティ・インシデントの早期検知、対応と再発防止を目的とした、国際的な情報共有のための枠組みとして有効と考える。CSIRT が存在しない国・地域は、まずはNational CSIRT の設置を積極的に検討すべきであり、国際機関や先進国等は、人材やノウハウの提供による支援[12]を推進すべきである。

②トレーサビリティの確保

サイバー犯罪においては、インターネットの匿名性が悪用され、行為者の追跡が困難であるのが一般的である。このため、利用者のトレーサビリティを確保することが重要である[13]。

一般に、利用者の確認のためには、レジストリあるいはレジストラにより運営されてい

---

8 当事者同士がサーバを経由せずに直接情報のやり取りを行なうインターネットの利用形態、またはその技術を用いたアプリケーション。

9 法整備が遅れている地域は、サイバー攻撃を行なうリスクが小さく、犯罪者に狙われやすいため、国際的にサイバー犯罪に関する法整備を進めることも重要である。

10 http://www.first.org/

11 Computer Security Incident Response Team の略。コンピュータ・セキュリティ・インシデントに関する報告を受け取り、調査・対応を行う組織体の名称。

12資金的な援助よりも、先進国が有する、セキュリティ対策の枠組み、ノウハウ、モデルそのものを途上国に提供することの方が重要である。また、このような支援を行なうことで全体のレベルアップをはかることは、インターネットにつながる全ての利用者にとって利益となることである。なお、JPCERT/CC では、アジア各国における CSIRT 設立支援活動を積極的に行なっている。

13 意図的に犯罪行為を行う者の場合、本提言にある対策を実施してもトレーサビリティが確保できない可能性もあるが、BOT による、利用者が意図しない攻撃の解消につながることが期待できる。

るwhois[14]が利用されているが、実際には必ずしも正確な情報が登録されておらず、インシデント発生時に、当事者への連絡がうまくつかないことも多い。従って、whois への適正な情報登録、並びに登録情報の定期的（例：毎年）な更新の義務化を含む、当事者への確実な連絡が可能となるしくみを、インターネットガバナンスの主体が、その活動の一環として構築[15]することは、インシデントへの早期対応を実現する上で、非常に有意義である。ただし、これらはあくまでトレーサビリティ確保のための一手段であり、プライバシーの保護の観点から登録項目を限定し、かつ、プライバシーに関する登録情報の参照には厳しい要件を課すことが望ましい。

また、悪意を持ったメール送信者を特定するために、DNS サーバにおける IP アドレスの逆引き[16]情報の登録を国際的に推進することも有効である。

③スパム対策

今日、我々が受信するメールの過半数はスパムとなっている。スパムはネットワークに大きな負荷を与えるとともに、利用者の利便性を著しく損っている。また、フィッシングサイトへの誘導に、スパムが利用されていることもあり、その撲滅は喫緊の課題である。

スパムに対応するためには、一般的なセキュリティ対策と同様に、「法制度」「技術」「教育・啓発」による多面的な対策を、適切な役割分担に基づき関係者が連携して実施することが必要である。例えば、政府には、法制度面から「送信者情報を偽った送信の禁止」等の実効性のある迷惑メール規制を実施する役割があり、民間事業者には、「送信ドメイン認証技術[17]」や「２５番ポートブロック[18]」等の最新の技術的対応を実施するとともに、悪質事業者の情報を共有して、被害の拡大を防止する役割がある。これら両者が密接な協力関係のもと、スパム撲滅の姿勢を明確に示すことが、迷惑メール対策の基本となると考える。そして、このような対策を世界規模で行うことなくしては、われわれの利用しているインターネット環境におけるスパム撲滅は期待できない。今後、様々な場を通じて、必要な対策についての情報交換およびその対応を行なうべきである。

なお、日本における携帯電話発のスパム撲滅の成功例については、Ⅲ章に記述した。

（２）インターネットの利活用を支える社会的・文化的基盤の整備

①キャパシティ・ビルディングによるデジタル・デバイドの解消

先進国と途上国のデジタル・デバイド解消のためには、途上国におけるインフラ整備とともに、リテラシー向上のための教育プログラムが必要である。これらの実施にあたっては、既存の国際機関を中心として、各国政府、企業、市民社会がパートナーシップを構築・強化し、世界中の誰もがＩＣＴを利活用できる環境を整備していかなければならない。

②セキュリティ文化の普及

---

14 IP アドレスやドメイン名の登録者などに関する情報を、インターネットユーザが参照できるサービス。レジストリやレジストラが提供している。

15 今日では登録代行業者による登録が一般的だが、この場合も、代行業者で正確な情報登録を行なうことで、トレーサビリティは確保できる。

16 IP アドレスに対応するドメイン名を調べること。このような「逆引き」用のデータが設定されていないことも多い。

17 メールの発信元サーバ情報（ドメイン）を、受信サーバ側で認証する技術。これにより、送信元が特定できたメールだけ受信する、といった対策が可能となる。ただし現在は一部認証を正しく行なえない場合がある等の課題があり、さらなる検討が必要と考えられている。

18 25 番ポートへのアクセスを制限することで、ISP が自社の提供するメールサーバを経由しないメールをブロックする対策。BOT に感染した「ゾンビ PC」によるスパム送信対策として有効と考えられている。

先進国においても、セキュリティ文化[19]が十分に普及しているとは言いがたい。日本でも、リテラシー教育に比べ、インターネット社会におけるリスクに関するセキュリティ教育はまだまだ不十分であり、今後、在宅勤務や遠隔医療が普及する時代を迎えるにあたり、その重要性が増すと考えられる。例えば、ウイルスの感染を防ぐためには、ワクチンソフトを利用し、かつ、適切にパッチファイルをあてることに加えて、出所が明らかではないファイルを実行しないことが重要であることは広く知られている。しかし、それでも感染者が後を絶たないことは、セキュリティ問題の重要性に比べて、利用者の情報セキュリティに対する認識レベルが低いことが背景にある。特に最近では、BOT に感染した被害者が、知らないうちに加害者になっていることが増えている。このように、セキュリティの教育・啓発が不十分なまま、利用者が増えると、インターネットの利用そのものが危険を拡大することになる。生涯教育も必要な分野であるので、WEB ページでの啓蒙にアニメーションを利用する等、効果的な情報提供方法についての経験を蓄積し、活用していくべきである。

一方、途上国については、支援のための教育プログラムとして、単に利用方法（リテラシー）を教えるだけでは、セキュリティ上の問題が世界規模で深刻化することに繋がりかねない。従って、技法だけでなく作法も含む教育・訓練となるように、セキュリティ面の教育も一つの柱とするべきであり、各国政府や民間団体等の支援についても、この視点を追加することが重要である。また、セキュリティ教育・啓蒙を行なう主体として、前述の National CSIRT を利用することも考えられ、先進国等はそのための人材、ノウハウの提供および教育のための教材等の共同開発を推進すべきである。

③高度情報セキュリティ人材育成

全体的なレベルの底上げとあわせて、高度化する攻撃への対応能力を高めるため、高度な情報セキュリティ人材を育成することも必要である。高度 IT 人材の育成を国家戦略の柱にしている国も多いが、そこに、これからのインターネット社会の発展を支える「高度情報セキュリティ人材の育成」も加え、さらには国際的にそのような人材育成に向けて協力の枠組みを構築すべきである。

④自由と規制のバランス

インターネットへのオープンアクセス、そしてそこにおける表現の自由は、インターネット社会の発展に必要不可欠なものであり、公序良俗を保つための規制に反しない限り、最大限尊重されるべきである。

従って、例えば有害サイトに対するフィルタリングを実施するにあたっても、そのブラックリスト登録基準は明確に説明されなければならないし、その基準設定に際し、各フィルタリング事業者またはその団体同士で定期的に意見交換することが重要である。

一方で、セキュリティ対策等のために、やむを得ず自由が制限されることもある。自由と規制（安全）のバランスに関しては、現時点では明確な答えはなく、IGF における議論を通じ、コンセンサスの形成に向けた活動を進めていくべきである。

19 OECD(Organization for Economic Co-operation and Development)では、「セキュリティ文化」の普及のための活動を継続している。

Ⅲ．日本の事例紹介

日本においては、ユビキタスネットワーク化（モバイルおよびブロードバンド環境の進展、電子タグ等の普及）の進展に伴い、従来見られなかった種類のインシデントが生じている。IGF に向けてこれらを紹介し、今後、ブロードバンドが普及し、またモバイル端末によるインターネット接続の利用者が増加する世界各国の参考に供したい。

１．携帯スパム削減

（１）現状および対策の概要

日本においては、携帯電話端末を用いてインターネットメールを送受信するという利用形態が普及しているが、この場合も通常の PC と同様、大量のスパムによる影響が発生していた。そこで、官民連携により、明確な役割分担に基づいて複合的な対策を実施した結果、迷惑メール数を激減させることに成功した。特に携帯電話（ＰＨＳを含む）から発信される迷惑メールはほぼゼロとなっている。

それぞれが実施した対策の概要[20]は以下の通りである。

①政府部門

ⅰ）実効性のある「迷惑メール」規制の実施

・「特定電子メールの送信の適正化等に関する法律（迷惑メール法）」を制定(H17.11 改正)し、送信者に対して「受信者の同意を得ずに送信される広告宣伝メールであること等の表示の義務付け」「送信者情報を偽った送信（迷惑メールのほぼ１００％がこれに該当）」および「架空電子メールアドレス宛の送信の禁止」等を強制[21]した。

・電気通信事業者に対して、一時に多数の電子メールが送信された場合等の「迷惑メール対応」を目的として、役務の提供を拒否することを認めた。

・これらの法規制により、民間での対策が容易になった。

ⅱ）情報共有体制構築のバックアップ

・迷惑メール送信者に関する情報の共有を認める（プライバシー／個人情報保護に関する法律との関係で、ガイドラインを整備）。

・民間部門での情報共有をバックアップするために、多国間・二国間での MOU を積極的に締結している。

②民間部門

ⅰ）情報共有の実施

・「渡り[22]」対策として、契約を解約した悪質事業者に関する情報の共有を行っている。

ⅱ）最新技術の導入

・技術的な解決策として、多くの ISP で「送信ドメイン認証技術」の実装、および「２５番ポートブロック」の実施を検討し、大手 ISP では既に対応を完了している。これらは、送信アドレスを詐称している迷惑メール対策として効果を発揮している。

---

20 詳細は総務省「迷惑メールへの対応の在り方に関する研究会最終報告書(http://www.soumu.go.jp/s-news/2005/pdf/050722_2_02_00.pdf)」等参照。

21 2006 年上期に 2 件の摘発を行なっている。

22 契約を解約された ISP とは異なる ISP を利用することで、スパムの送信を継続すること。

iii)携帯電話固有の対策

・携帯電話では、利用者の限定が可能であるため「送信通数の制限[23]」を行っている。

iv)フィルタリング

アドレス指定受信設定などの強力なフィルタリング機能を提供している。

③民間部門・政府部門の協力

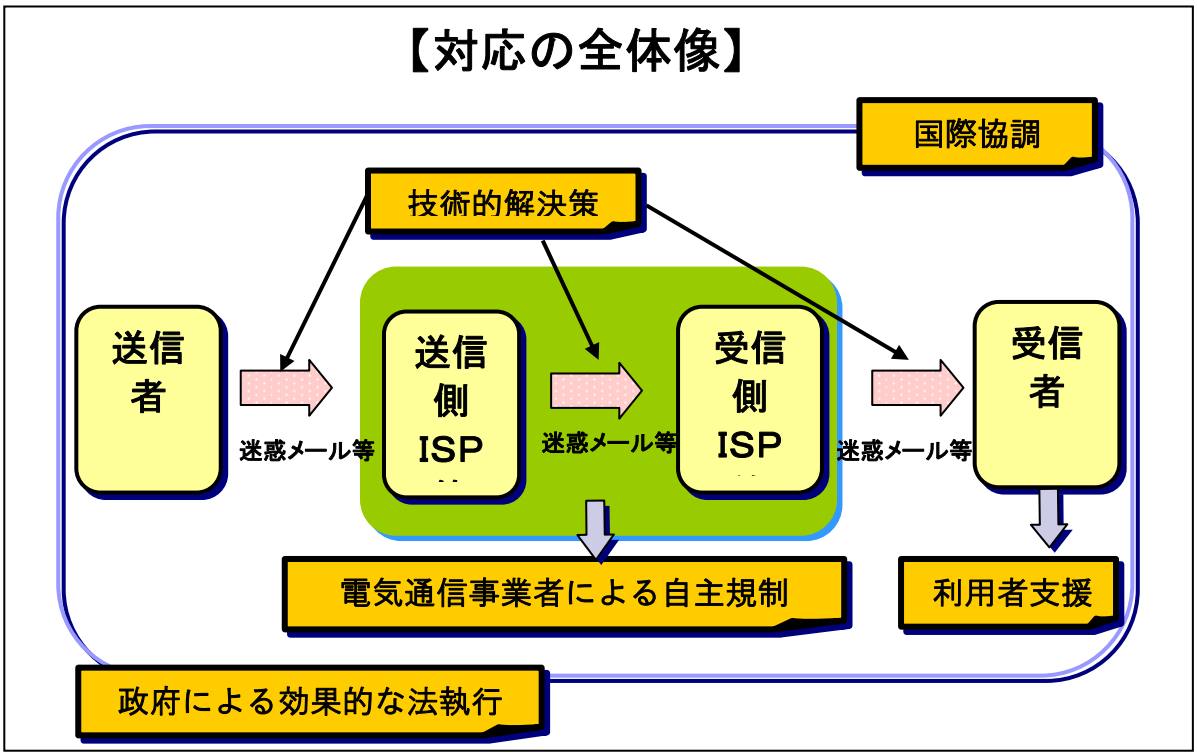
ⅰ)「迷惑メール追放支援プロジェクト[24]」を推進し、官民協力してスパムに対応する姿勢を明確に打ち出す（2005 年 2 月～）

ⅱ)啓蒙活動

・複雑なメールアドレスの利用を推奨。

（2）今後の課題

PC から発信されるスパムの対策は未だ不十分であり、今後、国際協調により実効のある対策を講じなければならない。特にブラックリストを国際的に共有する枠組みの構築、あるいは各種技術的な対策の実施を全世界協調して推進することが重要である。OECD、MAAWG[25]（Messaging Anti-Abuse Working Group）、JEAG[26](Japan E-mail Anti Abuse Group)をはじめとする既存団体のスパム対策提案も参照のうえ、技術的な対策と制度的な対策を組み合わせた、実効性のある対策について、今後、議論を深めるべきである。



※総務省迷惑メールへの対応の在り方に関する研究会　最終報告書より

23 日本の主要な携帯電話事業者は、一日一回線あたりの発信数を数百～千通程度に制限している。

24 次の枠組みとなっている。①モニター機で受信した迷惑メールを、日本データ通信協会が分析し、送信 ISP を特定した上で総務省に報告②総務省でメールの違法性を認定、ISP に通知③ISP で利用停止措置等を実施

25 http://www.maawg.org/home

26 http://jeag.jp/

２．P2P ファイル共有ソフトの脅威

（１）現状および対策の概要

日本では、IT 政策および産業界における戦略的な先行投資により、無制限定額制の高速ブロードバンド・サービスが一般化した結果、ブロードバンド環境と相性の良い「Winny」や「Share」等の P2P によるファイル共有ソフトが広く普及[27]した。しかし、これらのファイル共有を目的としているソフトには、特殊なウイルスに感染してしまうと、予期しない深刻な情報漏えいに直結する危険[28]があるが、利用者はそれを十分認識できていないことが多い。このため、日本ではファイル共有ソフトを原因とする各種情報の流出が続き、社会問題化しているが、今日においても問題は解決していない。

①主な情報漏えい事件の例（2006 年分）※

発覚時期	分野	情報の内容
2006 年 8 月	重要インフラ	原子力発電所配管関係資料
2006 年 3 月	地方自治体	住基ネット情報（642 名分の個人情報）
2006 年 3 月	警察	個人情報(犯罪被害者の実名含む)
2006 年 2 月	海上自衛隊	自衛隊関係資料（機密情報含む）
2006 年 1 月	病院	患者情報

※上記以外にも、多数の個人情報漏えいが発生している。

②複合的な要因への対策

ファイル共有ソフトによる情報漏えいは、PC が Antinny に代表される暴露ウイルスに感染することが直接の原因だが、その背景には複数の要因が密接に絡み合っている。以下に、その主な要因について、実施した対策を軸として整理する。

ｉ）技術による対応

まず、技術面からファイル共有ソフトの機能を悪用するウイルスに対処するため、開発者等がソフトの脆弱性に対応するためのパッチファイルを提供するとともに、ソフトベンダー等がウイルス駆除のためのツールを提供している。しかし、新たな脆弱性が発見された場合の“ゼロデイ・アタック[29]”の問題は残っており、また、日々亜種が発生するウイルスの全てをパターンファイルに登録するのは不可能である。このため、緊急措置的に、ISP 側で P2P によるファイル共有ソフトの利用を制限する機能を提供している事例もある。

一方、P2P ネットワーク上に漏えいした場合の事後対策の研究も進められているが、まだ有意な成果を挙げるには至っていない。

なお、Winny については、製作者がその修正あるいは改良を行えない状況になってしまった[30]ため、新しく脆弱性が発見されても、適切な修正が行なわれない状態になっている。

ⅱ）法・制度による対応

ｉ）ではカバーできない分野について、法や制度により、対応力を高めている。

---

27 2006 年 7 月 2 日時点で、代表的なソフトである「Winny」は約 50 万台のコンピューターで利用されている（ネットエージェント社の調査による）。

28 ファイル共有ソフトでは、一定の場所に存在するファイルのみ交換対象としているが、暴露ウイルスに感染した場合、その場所以外に存在しているファイルも交換対象とされてしまうため、予期せぬ情報漏洩につながる。

29 ソフトウェアにセキュリティ上の脆弱性が発見されたときに、公表前にその脆弱性を悪用して行なわれる攻撃。

30 「著作権法違反幇助」の疑いで逮捕された開発者は、今後、Winny の改良を行なわないことを誓約している。

企業や行政機関等では、重要な情報資産の制度的・人的なアクセス制限を行なうとともに、それらを外部に持ち出さない、あるいは団体と同等以上のセキュリティ対策を行っていない個人用 PC では、それらを利用しない、といったセキュリティポリシーを定め、その所属員に遵守を求めている。特に個人情報については、2005 年 4 月の個人情報保護法全面施行を受け、法的義務としての漏えい対策が行なわれている。しかし、セキュリティの重要性に関する理解が不十分、ポリシーが実態にそぐわない、等の理由により、十分機能していない団体もあり、そこから P2P ファイル共有ソフトを通じた漏えいが発生している。

個人については、P2P ファイル共有ソフトの利用の規制、あるいはウイルス対策を強制するような法は存在しておらず、このカテゴリーでの対策はほとんど採られていない。

ⅲ）教育による対応

ⅰ）ⅱ）を機能させるため、利用者がセキュリティについて十分な知識とスキルを身につける必要があり、そのための教育は重要なセキュリティ対策である。

多くの企業や行政機関等では、所属員のセキュリティ教育を行なっているが、それが不十分なところも多い。

個人ユーザーについては、内閣官房長官より Winny 利用のリスクについてコメントを発表(2006 年 3 月)し、また、マスコミ等による啓発活動も行っている。しかし、定額ブロードバンドの普及による常時接続者の増加、マスコミによる知名度向上等を背景に、不特定多数のユーザーが存在しているため、全員を対象とした教育・啓発の実施が、極めて困難なものとなっている。また、流出した極秘情報に関する情報が掲示板に収録されることで、さらに拡散が進んでいる。

さらに、肝心の教育内容も、情報漏えいがクロースアップされすぎた結果、単純に P2P によるファイル共有ソフトが悪いという誤った認識が広まってしまったため、「P2P によるファイル共用ソフトを用いる PC では、重要な情報資産を利用しない」「利用 PC のセキュリティ対策を可能な限り行なう」という基本認識の普及は、未だ不十分なままである。

（2）今後の課題

P2P によるファイル共有ソフトの中でも、特に Winny が社会問題化したのは、従前 Napstar や Gnutella 等で問題になっていた著作権侵害のみならず、プライバシー情報、さらには国家機密に属する情報までが漏えい対象となったからであるが、このような深刻な事態を招いたのは、上記の様々な要因が複雑に絡み合い、有効な対策を迅速に実施できなかったことが大きい。IGF の場などにおける関係者との意見交換を踏まえ、今後も対策のあり方について、検討を深めていきたい。

また、このような複合要因によるセキュリティ危機は、今後、ICT の浸透、あるいは新しい技術の開発等により、形をかえながら世界中のあらゆる場所で発生する可能性があると考える。本事例も参考に、このような新しい種類のリスク発生に備え、マルチステークホルダーの連携による議論を本格化させなければならない。

以　上