サイバーセキュリティとISP：法と経済学の視点からのサーベイ*

Cybersecurity and ISP: A Survey from the Perspective of Law and Economics

絹 川 真 哉

インターネットが情報通信の社会インフラへと成長し、公共性を強めていく中、サイバーセキュリティの重要性は以前にも増して大きくなっている。一方、ボット等のマルウェアによるサイバーセキュリティ上の脅威も増大を続けている。クラウドコンピューティングサービス等のインターネットに依存したビジネスを今後さらに発展させていくには、サイバーセキュリティの確保は重要な政策課題である。

ボットネット駆除等、サイバーセキュリティの確保に関する法規制については、これまで様々な議論・提言がなされており、ISP（Internet Service Provider）の役割の重要性がとくに指摘されている。一方で、実際に、政府とISPの協力によるマルウェア除去の取り組みが先進各国においてすでに実施されている。我が国においても、総務省・経済産業省連携プロジェクト「サイバークリーンセンター（CCC）」が2006年度から2010年度の期間、ISPとの協力のもと、ボット駆除を進めてきた。

日本は国際的にみてもボット感染率が低く、CCCの活動に一定の効果があったと推測される。サイバーセキュリティを向上させ、インターネット関連ビジネスの発展を支えていく上で、CCCの活動の継続等、ISPからの協力は欠かせない。

Keyword: サイバーセキュリティ、ボットネット、ISP、間接責任:

* 本論文は、情報セキュリティ大学院大学が富士通株式会社からの委託業務として実施した研究プロジェクト「クラウドコンピューティングのセキュリティに関する法的諸問題の検討」（平成22年度実施）の報告書の一部として筆者が執筆したレポートを、大幅に加筆・修正したものである。研究の機会を提供していただいた情報セキュリティ大学院大学の林紘一郎教授、株式会社富士通総研の浜屋敏主任研究員に感謝します。

1. はじめに

全世界のインターネットユーザーは2005年から2010年の間に倍増し、2010年には約20億人となった。ブロードバンド契約者数については、特に先進国での普及スピードが速く、2010年に全世界で5億人以上に達した[1]。インターネットが情報通信の社会インフラへと成長し、公共性を強めていく中、サイバーセキュリティの重要性が以前にも増して大きくなっている。

一方、マルウェア（悪性プログラム）によるサイバーセキュリティ上の脅威も増大を続けている。例としては、ボットネットを介したDDoS攻撃が挙げられる。「ボット」はコンピュータを外部から遠隔操作することを目的として作成されたマルウェアで、「ボット」に感染したコンピュータのネットワークが「ボットネット」である[2]。DDoS（Distributed Denial of Service）攻撃は、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にすることでサービスを妨害する攻撃で、専用の攻撃ツールやボットネットを利用して行われる。その主な動機は、攻撃対象に対する抗議や自己主張であるが、近年では、金銭目的の恐喝手段としても行われており、さらには攻撃を代行する者も現れている[3]。

インターネットに大きく依存したビジネスサービスは、マルウェアによるセキュリティリスクによって大きな被害を受ける可能性がある。インターネット、とりわけブロードバンドの普及による後押しで近年大きく成長しているビジネスの例としては、同じ物理サーバを仮想化技術によって複数ユーザーが共有し、インターネットを通じてサービスの提供を受けるクラウドコンピューティングサービス（以下、クラウド）がある[4]。サイバーセキュリティの問題がクラウド普及へ負の影響を与えうることは、例えば、情報セキュリティ大学院大学原田研究室によるクラウドユーザーの意識動向調査が示唆している[5]。同研究室は、企業・行政機関・大学等の情報セキュリティ担当者を対象としたアンケート調査を2010年8月に実施した。クラウドのリスク要因としては、事業者内部のセキュリティ違反とともに、事業者と自組織を結ぶネットワークのダウンや障害が挙げられている。情報セキュリティ担当者が「重大なリスク」としたリスクのうち、「事業者と自組織を結ぶネットワークがダウンするリスク」を挙げた情報セキュリティ担当者は約4割、「中程度のリスク」として挙げた情報セキュリティ担当者と合わせると約7割となった。また、「事業者へのDDoS攻撃でサービスが中断したり品質低下するリスク」についても、「重大」と回答した情報セキュリティ担当者が2割以上、「中程度」と合わせると6割近い結果となった[6]。

[1] 以上、インターネットとブロードバンドの普及に関するデータは、International Telecommunication Union Website, Statistics, “The World in 2010: ICT Facts and Figures”（http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf、最終アクセス：2011/5/18）

[2] ボットの詳細については、例えば、サイバークリーンセンターのウェブサイト（https://www.ccc.go.jp/index.html、最終アクセス：2011/5/18）等を参照。

[3] 国内大手インターネット接続事業者の一つ株式会社インターネットイニシアティブの定期発行技術レポート「Internet Infrastructure Review Vol. 9 November 2010（http://www.iij.ad.jp/development/iir/index.html、最終アクセス：2011/5/18）」による。

[4] クラウドコンピューティングサービスの一般的な説明については、例えば、日経ビジネス2010.2.15「クラウド大旋風」などを参照。

[5] 調査結果については、http://lab.iisec.ac.jp/~harada_lab/enq/2010_questionnaire_result.pdf（最終アクセス：2011/5/18）

[6] DDoS攻撃によってクラウドサービスに一時的な障害が発生したケースとして、2009年12月のAmazonおよびSalseforce.comの事例がある（ITmedia News 2009/12/25「AmazonやSalesforceに一時障害、DNSプロバイダーにDDoS攻撃」http://www.itmedia.co.jp/news/articles/0912/25/news021.html、最終アクセス：2011/5/18）。いずれも、利用しているDNSサービスプロバイダが大規模なDDoS攻撃を受けたため障害が発生したが、プロバイダ側の対応で間もなく復旧している。

クラウドが今後のインターネットビジネスにおいて極めて重要である点は、多くの関係者が指摘している。例えば、総務省は「スマート・クラウド研究会報告書」（平成22年5月17日公表）の「はじめに」で、「クラウドサービスは今後のICTの柱の一つとなるものである」とし、「我が国におけるクラウドサービスの創出・普及が遅れると、我が国ICT産業全体の「空洞化」を招き、国際競争力が著しく低下することが懸念され、早急に取り組むことが必要」と述べている[7]。今後、クラウドの普及を進める上で、ボットネットを通じたDDoS攻撃等のサイバーセキュリティリスクを極力小さくすることが重要な課題の一つとなろう。

では、ボットなどマルウェアを排除し、インターネット環境をより安全にするために何をすべきなのか。その実現のため、インターネットサービスプロバイダ（Internet Service Provider、以下ISP）がより積極的に係るべきだ、という議論が研究者や専門家の間で支持されており、先進各国のサイバーセキュリティ対策においても、ISPとの協力、あるいはISPに対する規制が課題の一つとなっている。本論文は、法と経済学の観点から、それら議論および研究成果を整理しつつ紹介する。

以下、第2節では、セキュリティ専門家や法学者・経済学者によるISPの役割・責任に関する議論を紹介する。第3節では、サイバーセキュリティとISPに関するOECDによる実証研究の結果を紹介する。第4節では、ボットネット駆除に関する費用問題、および、いくつかの国々に関するサイバーセキュリティ対策について紹介する。最後に論点をまとめる。

2. ISPに対する法規制の可能性

2.1 ISPの役割増大を求める声

ISPの法的責任については、著作権侵害など、利用者がサーバにアップロードした違法コンテンツに対する責任を制限する法制度が構築されている[8]。しかし、クラウド化の進展等、インターネットの公的インフラとしての性質がより強まる中、サイバーセキュリティの確保にもISPは責任を持つべきいう考え方が多くの研究者や専門家の間で広まっている[9]。

例えば、オンライン・ジャーナル「CIO.com」2005年11月1日の記事「Seeing No Evil: Is It Time To Regulate the ISP Industry」[10]は、エンドユーザーがDDoS攻撃や個人情報盗難等の被害を受ける前にリスクを取り除くよう企業や消費者がISPに求める圧力が日増しに高まっているとして、様々な専門家の意見を紹介しつつ、ISPに対してセキュリティ対策を義務化する法規制の是非を検討している。ユーザー側の意見として、Federal Trade Commission（FTC）CIOのStephen Warrenは、「州政府や地方自治体が水道会社に対して安全な水の供給を義務付けているように、インターネットへの入り口を提供するISPに対して安全なデータの配送を義務付けるのは理にかなう」と述べている。また、Notre Dame University副CIOのDewitt Latimerは、「ISPが加入者のコンピュータのウィルス・スキャンを行うとともに、ネットワーク・トラフィックを監視してハッキング攻撃の発生をチェック、不審なネットワーク・ユーザーを遮断すれば、他のすべてのユーザーの通信の安全を守ることができる」とし、「そうした役割を担える

[7] http://www.soumu.go.jp/menu_news/s-news/02ryutsu02_000034.html（最終アクセス：2011/5/18）

[8] 著作権分野におけるISPの責任制限法制については、例えば、生貝（2011）を参照。

[9] それら研究者・専門家の意見のサーベイとして、例えば、Rowe et.al.（2009）を参照。

[10] http://www.cio.com/article/13526/Seeing_No_Evil_Is_It_Time_To_Regulate_the_ISP_Industry（最終アクセス：2011/5/18）

のは、ネットワークに出入りするすべてのトラフィックを中継するISPだけ」と指摘している。

法学者からは、例えば、Zittran（2006）が、様々なアイデア・新技術の土壌としての役割をインターネットから失わせないという観点から、ISPによるサイバーセキュリティ確保の優位性を説く。技術に疎い多くのアマチュアがネットワークに参加し、新しいコンテンツ等の創造に貢献するには、ネットワークのセキュリティが重要である。しかし、技術知識の疎いアマチュアが自らセキュリティを確保することには限界がある。このため、セキュリティの脅威が高まるほど、多くのアマチュアユーザーがPCから離れ、PCより創造する力が弱い（限られたアプリケーションしか使えない）がより安全な端末を使うようになる可能性が高い。結果として、ユーザーによるイノベーションは低下してしまう。このような事態を回避する手段の一つとして、Zittran（2006）は、ユーザーにセキュリティ確保の責任をすべて負わせるよりもISPを通してマルウェアの除去を実現した方が望ましいかもしれないとし、ネットワーク中立性の原則の修正を提案している。

2.2 マルウェア被害に対するISPの間接債務

法と経済学の専門家からはLichtman and Posner（2006）がサイバーセキュリティに対するISPへの法的責任について論じている。以下、彼らの主張を詳しく紹介したい。

サイバーセキュリティの確保を法規制によって実現する手段として、まずは、マルウェアを作成・配布する当事者をどう罰すかが問題となる。その軸となるのが、私的規律（private legal systems, PLSs）の醸成によってネットワーク参加者を律するのか、公的規律によって当事者への罰則等を強化していくのか、という互いに反する2つの議論である（Grady and Parisi, 2006）。これに対し、Lichtman and Posner（2006）は、ネットワークのいわば「関所」の役割を担うISPに、マルウェアによって生じた損失に対して間接債務（Indirect Liability）を課すという提案を行っている。そうすることで、ISPがネットワークに出入りするマルウェアの監視を行い、マルウェアに感染したエンドポイントの特定、そしてマルウェアの除去により積極的になると考えられるからである。

一般的に、過失等の不法行為を行った者に対して責任を負わせることができないのは、（1）行為者の特定が困難か、特定できたとしても賠償能力がない、あるいは、（2）費用等の問題から、契約による関係者間での責任の割当が困難、という場合である。さらに、（3）間接債務者が行為者の特定を行うことは可能、（4）間接債務者は不法行為がもたらす負の経済を内部化できる、という2つの条件が満たされる場合、間接債務が社会的に望ましい。

例えば、トラック配送サービス事業におけるドライバーと事業者について考える。ドライバーが起こした事故に対し、まず事故の目撃者がいない等、どのドライバーが事故を起こしたのか被害者には分からない場合（条件1）、あるいは、ドライバーと事業者が保険契約を結んで賠償に備える等ができない場合（条件2）、ドライバーに対する賠償請求は実現できない。一方、事業者は、いつどこで誰がトラックを運転していたかを把握しており（条件3）、さらに、ドライバー教育や健康管理などによって事故のリスクを小さくすることができる（条件4）。したがって、ドライバーの過失責任を事業者に負わせることは、社会的に望ましい。

Lichtman and Posner（2006）は、マルウェア被害とそれ対するISPの間接債務は、上記4つの条件を満たすと論じる。まず、マルウェアを作成しネットワークに広める行為者の特定は困難なことがほとんどである（条件1）。発信元アドレスの詐称やボットネットを利用した攻撃が多

いためである。また、仮に行為者が特定できたとして、被害損失の大きさと比べて、行為者の支払い能力は非常に小さい可能性が高い。つぎに、契約による責任の割当も困難である（条件2）。ここで、契約の当事者として想定されているのは、相互に接続された異なるISP同士である。ある一つのISPにおける加入者がセキュリティ上の脅威を引き起こした場合、その脅威は他のISPへと伝播する。しかし、最初のISPとその他多くのISPとの間で、あらゆるサイバーセキュリティリスクを事前に考慮して相互の責任を明確にした契約を結ぶことは事実上不可能である。費用の面から難しいだけでなく、新しいセキュリティリスクが常に発生しているからである。一方、ISPは、自身のネットワークに接続されている機器のうちどれが問題の発生源になっているのかを特定できる立場にあり（条件3）、そして、それらに対処することで（各ISPの）ネットワーク内のセキュリティリスクを低下させることも、技術的には可能である（条件4）。したがって、サイバーセキュリティリスクのもたらす損失の間接責任をISPに負わせることは社会的に望ましい、という議論が可能となる。

2.3　間接債務の問題点

しかし、ISPに間接債務を導入することで、様々な問題も生じうる。まずは、ISPによる過剰反応、つまり、マルウェア対策が十分でないが感染はしていないユーザー等を含めて排除対象になってしまう可能性である。例えば、間接債務によってセキュリティ投資が増加し、その費用が接続料金に反映されれば、インターネット接続への需要がさほど大きくなく、セキュリティ意識があまり高くないユーザーはサービスの購入をやめる、あるいは利用を減少させるかもしれない。この場合、より多くの消費者がネットワークに接続されることで生じる外部経済（友人同士の連絡のとりやすさ、広告効果の増加など）が減少する。

もうひとつの問題は、ユーザー自身によるセキュリティ確保の努力（ファイヤーウォールやウィルス対策ソフトのインストール等）を減少させる可能性である。多くのユーザーが自らマルウェア対策を行わない場合、マルウェア対策ソフトの需要も低下し、それらを開発する企業の開発投資インセンティブにも影響を与えうる。

Lichtman and Posner（2006）は、以上の問題点を認めながらも、ISPに対する間接債務の優位性は変わらないと主張する。まず、ISPの過剰反応によるセキュリティ意識の低いユーザーの排除に対し、排除された場合に外部経済が減少する一方、排除されなかった場合には負の外部経済が大きいままであると指摘する。そして、負の外部経済がネットワークの利便性を下げ、インターネットから大きな効用を得ているユーザーを含むすべてのユーザーの利用を妨げるのに対し、ISPの間接責任が排除するユーザーは、ネットワーク利用の効用が低くかつセキュリティ対策が不十分なユーザー、そして意図的にマルウェアをネットワークに送り込もうとするユーザーであり、すべてのユーザーの利用を妨げるよりも選択的、効率的である。

また、ユーザーのセキュリティ対策へのインセンティブについても対処可能である。各ユーザーがセキュリティ対策行うことがサイバーセキュリティにとって重要である以上、例えば、ISPがユーザーと契約を結ぶ際、セキュリティ対策を必要事項の一つとすることが考えられる。そして、ウィルス定義ファイルの更新が長期間行われない等、セキュリティに関する契約内容が守られない場合はISPが接続を拒否できるなどの条項を加えることもできる。

その他に起こりうる問題として、Lichtman and Posner（2006）は以下を挙げている：

（1）マルウェア被害は広範囲に拡散しているた

め、多くのユーザーにとって被害は小さく、個々のユーザーがISPに対して賠償請求するインセンティブは非常に弱い可能性がある。

(2) 被害を受けたユーザーとマルウェア発信元の間に複数ISPが存在する場合、誰を訴えれば良いのか？

(3) マルウェア発信元の特定に必要な情報を記録しないことで、ISPは間接責任を回避しようとするかもしれない。

(4) ある国のISPに間接債務を課しても、他国のISPに間接債務が課されなければ効果がない。

Lichtman and Posner（2006）は、まず、最初の3つについては、通常の不法行為に対する間接債務と同様に対処できると説明する。(1) については、集団訴訟を起こす、国が訴訟を起こす等が考えられる。(2) については、連帯債務を適用できる。そして、(3) については、立証責任をISPに課せば良い。また、(4) については、その重要性を認めながらも、例えば、米国、日本、EU諸国等の主要国がISPに対してマルウェア被害の間接責任を課せば、他の国の政策にも影響を与えうるとしている。

では、ISP側は、サイバーセキュリティに関する法規制の必要性についてどうみているのだろうか。前出の2005年11月CIO.comオンライン記事は、まず、セキュリティ対策を行っていないISPが存在する一方で、大手ISPに関しては様々なセキュリティ対策を実施している点を指摘している。例えば、EarthLinkなど一部のISPは「25番ポートブロック」によってマルウェアの拡散防止を図っており、さらに高度なセキュリティサービスを追加料金で企業に提供しているISPも多い[11]。そして、「ほとんどのISPはサイバーセキュリティの法規制化には断固として反対している」と指摘し、「サイバーセキュリティは業界の自主規制で実現できる」、「標準化されたセキュリティアプローチは費用がかかり過ぎる上、すべての顧客がそのようなアプローチを望んでいるわけではない」というISP側の主張を紹介している。

3. ISPの役割に関する実証研究

3.1 サイバーセキュリティに対するISPの重要性

前節では、「ボット等マルウェアの除去にISPがより積極的に係るべき」という議論を紹介してきた。では、マルウェア除去の責任をISPに課すことは、サイバーセキュリティを確保するために現実的かつ効率的な手段なのだろうか？このような観点から、van Eaten et.al.（2010）は、ボットネットを除去してサイバーセキュリティを確保する上で、ISPがどれだけ重要な位置を占めているかについて実証研究を行った。以下、詳しく紹介したい。

van Eaten et.al.（2010）は、ISPによるボットネット除去が有効となるためには、以下3つの仮説を検証する必要があると論じる。

仮説1： ISPがボットに感染した機器をコントロールする上で重要な位置を占める。

仮説2： ボットに感染した機器をコントロールする上で重要な位置を占めるISPの多くは大手ISPである。

仮説3： ISPは、その業務の範囲内で、ボット

[11] 日本の大手ISPについては、例えば、株式会社インターネットイニシアティブやエヌ・ティ・ティ・コミュニケーションズ株式会社が、法人向けにDDoS対策サービスを販売している。各社ウェブページ（http://www.iij.ad.jp/service/system/IIJ-SD.html、http://www.ocn.ne.jp/business/security/ddos/）を参照（最終アクセス：2011/5/18）。

ネット除去のインセンティブを持ち得る。

仮説1は、Lichtman and Posner（2006）によるISPの間接債務が有効となるための基礎的な仮定でもある。仮に、ボットに感染した機器の多くがISPを通さずにインターネットに接続しているならば、ISPではなく、大学等、他の異なるネットワーク媒介者がボットネット除去に係るべきとなる。仮説2は、仮説1と関連している。もし、ボット感染機器の多くが小規模ISPに接続されている場合、それらISPはボットネット除去の負担を負えず、大規模ISPの負担がさらに大きくなる可能性がある。そして、仮説3は、サイバーセキュリティ確保の政策的インプリケーションを得る上で重要となる。もし、ボットネット除去を行うことがISPの競争条件を著しく制限するようであれば、ISPはそのようなインセンティブを持ちえず、ISPの自主的取り組みによるボットネット除去は期待できない。この場合は、例えば、Lichtman and Posner（2006）が主張するように、マルウェア被害に対する間接債務をISPに課すなどの法制度が必要となろう。

van Eaten et.al.（2010）は、2005－2009年の間にスパムトラップが収集したスパム1090億件の送信元である約1億7千万のIPアドレスデータより、上記3つの仮説を検証した。それまでの実証分析より、スパムのほとんどがボットネットから発信されていることが分かっている。例えば、シマンテック社「MessageLabs」のレポートによれば、2009年のスパムの83.4%がボットネットより発信されていた。したがって、スパム発信元データは、ボット感染したコンピュータを示す指標として使うことができる。そして、van Eaten et.al.（2010）はスパム発信元IPアドレスの国を調べ、接続されているISPを特定している。その結果、OECD加盟34カ国および他の6カ国を加えた40カ国の200以上のISPが特定されている。

まず、仮説1について、全世界のマルウェアに感染した機器の60－74%が、上述の200以上のISPに接続されていた。仮説1の通り、ボットネットを駆逐する上で重要な位置を占めるのは、大学等ではなく、ISPだと言えよう。しかも、それら200以上のISPには、中小ISPのみではなく、大手ISPも多く含まれると推測される。OECD諸国のインターネット接続サービス市場の90%近くが、それら200以上のISPで占められているからである。

次に、仮説2については、ボット感染機器数でISPの分布を調べている。分布は大きく偏っており、感染機器数の多い上位10のISPで全感染機器数の30%を、上位50のISPでほぼ半数を占めていた。契約者数が多ければそれだけボットに感染する機器も多くなるので、ボットネットを構築している機器の多くが、中小ISPでなく、大規模な一部ISPに集中していると推測できる。したがって、何らかの政策的手段によってそれら少数のISPに働きかけることで、ボットネットを駆除することができる可能性がある。

最後に、仮説3を検証するために、van Eaten et.al.（2010）は、いくつかの条件のもとで各ISPの感染機器数の比較を行っている。それら各条件の下で各ISPの感染機器数に大きな違いがあれば、ISPはボットネット対策に対して裁量を持つ、ということになる。言い換えれば、ISPは、接続機器のボットへの感染防止またはボットネット除去の取り組みを行おうとすればできる、ということになる。van Eaten et.al.（2010）は、まず、ISPの規模（契約者数）でボット感染機器数の比較を行い、契約者数の増加とともにボット感染機器数も増加するものの、同規模ISPの間でもボット感染機器数には大きな幅があることを見出している。さらに、

アメリカとドイツを例にとり、同じ国のISPの比較も行っている。法制度などの違いがISPのインセンティブに影響する可能性があるためである。その結果、同規模かつ同じ国のISPでも、ボット感染機器数に比較的大きな違いがあることが示された。以上の結果は、仮説3を支持する。同じ制度のもとでの同規模ISPでもボット感染機器数に大きな違いが生じうるということは、ボットネット駆除の取り組みがISPによって異なりうることを示唆するからである。つまり、ISPによってはボットネット駆除へのインセンティブを持ちうる、ということになる。

3.2 ISPによる違いの説明

では、いくつかの条件が同じISP同士でボット感染数に違いが生じるのはなぜなのか。van Eaten et.al.（2010）は、ISPごとのボットネットの活動を様々な要因で説明する回帰分析を行っている。被説明変数の「ISPごとボットネット活動」としてはいくつかの候補が使用されている（ISP発のスパム数、ISP発のスパム数／契約者数、ISP内のスパム送信元IP数、ISP内の感染数／契約者）。これら被説明変数と複数の説明変数を用い、単相関、通常の回帰分析（Ordinary Least Square、OLS）、そしてパネルデータ回帰分析が行われている。主な説明変数、および、それら説明変数と「ISPごとボットネット活動」との関係は以下の通りである。

（1）制度要因

説明変数：London Action Planメンバー国のISP、欧州評議会（Council of Europe）「Convention on Cybercrime」メンバー国のISP

London Action Planは、2004年11月、27カ国の政府・政府機関がスパム対策の国際協力を議論し、策定した行動計画[12]。Convention on Cybercrimeは、2004年7月に発行された、メンバー各国が共通のサイバー犯罪防止政策を行うことを目的とした条約（CETS No.: 185）[13]。ともにサイバーセキュリティ向上を目指す国際協力体制であるが、London Action Planはサイバーセキュリティに関する規制当局の活動、Convention on Cybercrimeは法執行機関の活動に影響する要因である。頑健性は低いものの、これらに加盟している国のISPのボット感染は低くなる傾向がある。

なお、日本はLondon Action Planのメンバーである。もう一方のConvention on Cybercrimeについては、日本は協定策定の会議に欧州評議会非メンバー国の一つとして米国やカナダなどとともに参加しているものの、批准はしていない。欧州評議会非メンバー国からは米国のみが批准している（2010年3月時点）。

（2）組織要因

説明変数：ISPの規模（契約者数）、ケーブル事業者ISP

規模の大きいISPほどボット感染は低いという結果が得られている。これは、それまで言われてきた「大規模ISPは競争圧力が低いため、セキュリティ対策も十分でない」という言説を覆す。また、ケーブル事業者の方が他の事業者よりもボット感染が低いという結果も得ている。van Eaten et.al.（2010）は、ケーブル事業者がネットワークアドレス変換（Network Address Translation）や25番ポートブロックをDSL事業者よりも多用しているからではないかと推測している。

[12] 詳細については、http://www.londonactionplan.com/（最終アクセス：2011/5/18）を参照。

[13] 概要についてはhttp://conventions.coe.int/Treaty/en/Summaries/Html/185.htm、条文についてはhttp://conventions.coe.int/Treaty/en/Treaties/Html/185.htm、加盟状況についてはhttp://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENGを、それぞれ参照（最終アクセス：2011/5/18）。

（3）国要因

説明変数：違法コピーの多さ、教育水準

違法コピーの多さとの関係がモデルによって異なる結果となった一方、教育水準については一貫してボット感染に対して負の効果を持った。すなわち、より教育水準の高い国のISPの方が、より低いボット感染を示した。

4. ボットネット除去の政策対応

4.1 ボットネット除去の費用

前節で紹介したvan Eaten et.al.（2010）による実証研究は、ISPがボットネット除去に関してキープレーヤーである点、また、国や規模等の異なるISP間で、ボットネット除去へ向けた取り組みへのインセンティブが異なる可能性を示唆する。そのような違いが生じる大きな理由の一つに、ISPがボットネット除去に取り組む際に発生する費用の大きさがある。ボットネット除去の政策対応を検討する上で、まずはそれら費用の内訳を把握する必要がある。

Rowe et.al.（2009）は、ISPがセキュリティを確保するために必要な費用として、技術費用と法的問題の2つを挙げる。前者については、ボットに感染した機器の特定および除去には、設備等の導入や運用等、様々な費用が必要になる点を指摘する。また、ハッカーがそれらを回避する技術を常に見出している以上、その都度新しい技術を開発する必要があるとする。後者については、ユーザーとの契約がしばしばISPによるフィルタリングを難しくする点､そして、セキュリティ対策を提供すればするほど、マルウェアによる損失が生じた場合に間接責任を問われる可能性が高まる点を指摘する。

Clayton（2010）は、マルウェア除去においてはその費用が最も重要な課題であるとし、政府とISPが協力してマルウェア除去を行うためのスキームを提案している。感染機器とユーザーの特定、ユーザーに対する除去ソフトの配布に加え、ユーザーが自身で除去できない場合の技術者派遣までがそのスキームに含まれ、各段階で少なくない費用が生じる。例えば、技術者派遣のコストについては、米国Comcastの例があり、マルウェア除去に技術者派遣が必要な場合は約90米ドルをユーザーに請求している。これらの費用のため、ISP単体でセキュリティ対策を行うのは現実的ではない。競合ISPとの価格競争があるため、ISPが自身でセキュリティ対策のためにそれら多くの費用を投じるインセンティブは小さいからである。一方、個々のユーザーにとっても、費用と労力を割いてボット等マルウェアを除去するインセンティブは大きくない。これらの理由から､Clayton（2010）は、ボットネット駆除に必要な費用に対する政府補助金などの政策対応が必要と論じる。

4.2 各国の政策対応

ISPがボットネット対策などサイバーセキュリティ確保において重要である点は、いくつかの国の政府においても認識されている｡そして、ISPがサーバーセキュリティ確保の対策を自ら行うには、上で説明したように大きな費用が発生する。ボット除去などサイバーセキュリティの確保が社会的に有益である一方、それを実現できる立場にあるISPのインセンティブはさほど大きくない。したがって、サイバーセキュリティ確保に対しては国の役割が重要となり、実際、多くの国の政府がISPと協力してボットネット駆除に乗り出している。以下、いくつかの例について紹介する。

（1）米国

Office of Management and Budgetは2007年11月に「Trusted Internet Connection initiative（TIC, OMB Memorandum M-08-05）」を発行した。米国政府機関が安全にインターネットに接続できるよう、利用するISPを絞り込み、ISPレベルで

のフィルタリングを要求している（Rowe et.al., 2009）。TICはGeneral Services Administration（GSA）の「Networx」プログラムにおけるISPとの契約によって運用されており、AT&Tなど5社が請け負っている[14]。前出のCIO.comオンライン記事は、このような政府の取組がISPのセキュリティ対策を促し、同等のサービスが民間にフィードバックされる可能性があるというセキュリティ専門家の主張を紹介している。

また、Federal Communications Commission（FCC） は、「Cyber Security Certification Program」を開始するための意見調査を2010年4月21に開始した[15]。このプログラムは、通信事業者に対してセキュリティ対策を促し、かつ、エンドユーザーに対して通信事業者のセキュリティ対策への取組に関してより完全な情報を与えようとするものである。他にも、これまでに行われた米国連邦政府による取り組みとしては、Federal Bureau of Investigation（FBI）による2007年「Operation Bot Roast」（ボットに感染したPCのオーナー 100万人以上と接触）、Federal Trade Commission（FTC）による2005年「Operation Spam Zombies」（ISP・消費者との協力のもとボットネットを特定・排除）がある（Rowe et.al.,2009）。

なお、米国ではこれまで、いくつかの大手ISPがボットネットの温床となっている下位ISPを遮断している。例えば、スパム等の大量配信で知られる企業をホスティングしていたISPとして、2008年9月にIntercageが、同年11月にMcColoが、それぞれ上位ISPに接続を強制遮断されている。いずれも、サービス遮断措置は警察または裁判所の命令にもとづいて行われたものではなく、上位ISPの自主的判断によるものであった[16]。一方、2009年6月には、スパイウェア・フィッシング・児童ポルノ等サイバー犯罪の温床となっていたISPとしてPricewertが上位ISPから遮断されているが、こちらは、Federal Trade Commissionからの申し立てにより連邦地裁が下した業務停止命令に対応したもの[17]。

（2）欧州

van Eaten et.al.（2010）によれば、ドイツではマルウェア除去をサポートする政府出資のコールセンターが設立され、ISPを通じて顧客がそのコールセンターを利用できるようにされた。また、オランダでは、主要ISP各社が、各ネットワーク内のボットネット除去への義務に同意している。さらに、Clayton（2010）によれば、イギリスの超党派議員グループがイギリス国内のISPが政府と協力してボットネット駆除することを提案し、ルクセンブルグにおいても政府（Luxembourg Ministry of Economics）がISPによるボットネット駆除の支援策を評価中（2010年5月時点）である。

（3）オーストラリア

Australian Communications and Media Authority（ACMA） は、Australian Internet Security Initiative（AISI）のもと、ボットに感染していると思われるコンピュータに関する情報を収集、AISIに協力しているISPに日々報告している。協力ISPは、この情報にもとづき、ボット感染機器のユーザーを特定、連絡を取っ

[14] 詳細については、GSAウェブサイトの「Networx Overview（http://www.gsa.gov/portal/category/25318、最終アクセス：2011/5/18）」を参照。

[15] FCC Headlines 2010（http://www.fcc.gov/headlines2010.html、最終アクセス：2011/3/18）, 4/21/10, “FCC Launches Inquiry on Proposed Cyber Security Certification Program for Communications Service Providers.”

[16] COMPUTERWORLD.jp, 2008年11月26日「“ボットネットISP”のサービス強制遮断を巡り賛否両論」（http://www.computerworld.jp/news/sec/128189.html、最終アクセス：2011/5/18）

[17] COMPUTERWORLD.jp, 2009年6月9日「FTCが悪名高いボットネットISPを遮断、スパムが一時的に減少」（http://www.computerworld.jp/topics/vs_2/149750.html、最終アクセス：2011/5/18）

てボット除去手段のアドバイスを行う。2005年に6つのISPとの協力の下で試験運用が行われ、現在（2011年5月6日現在）は103のISPが協力している[18]。

（4）日本

2006年からに総務省と経済産業省が共同で「サイバークリーンセンター（Cyber Clean Center, CCC）」を設立し、ISPとの協力でボット駆除を行っている。そのスキームはClayton（2010）と同様、CCCがボット感染している機器のIPアドレスを特定、そのIPアドレスを割り当てたISPに連絡、そしてISPがユーザーに連絡し、ユーザーはCCCのサイトから駆除ソフトをダウロードする、というもの。CCCは2006年度から2010年度までの5カ年で計画され、2010年4月時点で、ISP76社、セキュリティベンダ7社が協力している。CCCの取組のもと、国内ブロードバンドユーザにおけるボット感染率は、2005年の2 ～ 2.5%に対し、2008年には1%にまで減少したと報告されている[19]。

以上のように、いくつかに国においては、政府がISPに要請、またはISPと協力する形で、サイバーセキュリティ対策を行っている。このような国の取り組みがどれだけ効果を持つのかについて、3.2節で説明したvan Eaten et.al.（2010）の回帰分析の結果は、弱いながらも、国の対策の効果を支持するものとなった。London Action Plan、そしてConvention on Cybercrimeの加盟国において、ボット感染率が低下する傾向が観測されるからである。この点をより明確にするため、van Eaten et.al.（2010）は、国ごとのISPのボット感染率を、各国のISP契約者一人当たりボット感染機器数を用いて比較している。OECD諸国の中でも、日本は特に低い感染率となっており、2009年時点において、低感染率1位のフィンランド、2位のカナダに次ぐ3位となっている。これらボット低感染率の国々は、サイバーセキュリティに関する国とISPの協力が密なことで知られており、2009年だけではなく、観測期間2005－2009を通し、一貫して低感染率上位であった。

5. まとめ

クラウドの普及等によってインターネットが電気や水道のようなユーティリティに近づく一方、サイバーセキュリティリスクの脅威は増大している。本論文は、インターネットをより安全にする上でのISPの役割について、法と経済学の視点からこれまでの議論や研究成果について整理・紹介した。

ボットネット駆除等サイバーセキュリティの確保に関する法規制についてはいまだ議論の段階である一方、現実には、政府とISPの協力によるマルウェア除去の取り組みが各国で進んでいる。日本はOECD諸国の中でもボット感染率が低く、サイバークリーンセンター（CCC）の取組が一定の成果を上げていたと推測できる。より安全なインターネット環境の実現に向け、日本は先導的役割を果たしてきたと言えよう。

CCCは期限付きの事業であるため、その活動は2010年3月でいったん終了したが、2011年4月以降は新しい枠組みで運営されている[20]。安全なインターネット環境をユーザーに提供し、インターネットを用いたサービスをより発展させるには、CCCの活動継続は必須である。今後は、より多くのISPと協力していく、海外の関

[18] AISIの詳細については、ACMAウェブサイト（http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317、最終アクセス：2011/5/18）を参照。

[19]「平成21年度サイバークリーンセンター活動レポート」（https://www.ccc.go.jp/report/h21ccc_report.pdf、最終アクセス：2011/5/18）

[20] サイバークリーンセンター・ウェブサイト「サイバークリーンセンターについて」より（https://www.ccc.go.jp/ccc/index.html、最終アクセス：2011/518）

連機関との連携を深める等、その活動を拡大していく必要があろう。

参 考 文 献

生貝直人（2010）「プロバイダ責任制限法制と自主規制の重層性－欧米の制度枠組と現代的課題を中心に－」『情報通信政策レビュー』第2号、総務省情報通信政策研究所（http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/02/ikegai2011.pdf、最終アクセス：2011/5/18）

Clayton, R.（2010）“Might Government Clean-up Malware?”10th Annual Workshop on Economics and Information Security（WEIS10）, available at http://weis2010.econinfosec.org/papers/session4/weis2010_clayton.pdf（最終アクセス：2011/5/18）

Grady, M., and F. Parisi（2006）“The Law and Economics of Cybersecurity: An Introduction,”in The Law and Economics of Cybersecurity, edited by M. F. Grady and F. Parisi, Cambridge University Press.

Lichtman,R., and E. P. Posner（2006）“Holding Internet Service Provider Accountable,”in The Law and Economics of Cybersecurity, edited by M. F. Grady and F. Parisi, Cambridge University Press.

Rowe, B., D. Reeves, and M. Gallaher（2009）“The Role of Internet Service Providers in Cyber Security,”Research Brief, Institute for Homeland Security Solutions, available at https://www.ihssnc.org/portals/0/PubDocuments/ISP-Provided_Security_Rowe.pdf（最終アクセス：2011/5/18）

van Eaten, M., J. M. Bauer, H. Asghari, S. Tabatabaie（2010）“The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data.”OECE Science, Technology and Industry Working Papers, OECD Publishing, available at http://www.oecd-ilibrary.org/science-and-technology/the-role-of-internet-service-providers-in-botnet-mitigation_5km4k7m9n3vj-en（最終アクセス：2011/5/18）

Zittran,J.L.（2006）“The Generative Internet,”Harvard Law Review, Vol. 119, pp1975-2040.