RCSS ディスカッションペーパーシリーズ ISSN-1347-636X
第 56 号　2007 年 10 月
Discussion Paper Series
No.56 October, 2007

インターネット・サービス・プロバイダの情報セキュリティ対策の実態と課題

―第 2 回情報セキュリティ対策に関するアンケート調査の概要―

竹村　敏彦

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka, 564-8680 Japan
URL: http://www.rcss.kansai-u.ac.jp
http://www.socionetwork.jp
e-mail: keiseiken@jm.kansai-u.ac.jp
tel: 06-6368-1228
fax. 06-6330-3304

インターネット・サービス・プロバイダの情報セキュリティ対策の実態と課題

－第2回情報セキュリティ対策に関するアンケート調査の概要－

竹村敏彦*
関西大学ソシオネットワーク戦略研究センター

2007年10月

概 要

インターネットが商用利用されるようになって10年以上経った。この間、インターネットは社会生活や企業活動にとって必須のツールとなり、それを利用していくつもの新たなビジネスが展開されるようになった。そしてこれらがもたらす正の経済効果は大きく、社会としてもICT化の促進を図っている。しかしながら、コンピュータウィルス、不正アクセスなどの情報セキュリティ被害という深刻な社会問題も顕在化してきている。本稿は、これらのユーザに対してインターネットの環境を提供しているインターネット・サービス・プロバイダ（ISP）を対象にして、情報セキュリティに関する対策の現状を2007年2月に実施したアンケート調査の結果をもとに、明らかにすることを目的としている。

その結果、各ISPが施している情報セキュリティ対策の実態が把握でき、また現在直面している問題について明らかになった。

KEYWORD: Information Security, Internet Service Provider, Corporate Social Responsibility, Questionnare

*関西大学ポスト・ドクトラル・フェロー

The Topics on Information Security Countermeasure of Internet Service Providers

Toshihiko Takemura
E-mail: takemura@rcss.kansai-u.ac.jp

Research Center of Socionetwork Strategies, Kansai University,
3-3-35 Yamate, Suita, Osaka, 564-8680, JAPAN.

October, 2007

Abstract

The businesses have been improved with the Internet since more than ten years. The Internet became an indispensable tool for the social life and firms' activities, and many new businesses have been developed. The Internet brings positive economic effects for society and Japanese government has also been promoting to use ICT. On the other hand, we face a serious social trouble on information security damages such as computer virus and illegal computer access, and so on.

In February 2007, the author conducted questionnaire concerned with information security countermeasures to Internet Service Providers in Japan. The author clarifies ISP's countermeasures against information security by using a part of the results. As a result, it was clarified of the problem being able the grasp of the realities of the information security measures that each ISP gave and be facing now.

Keyword: Information Security, Internet Service Provider, Corporate Social Responsibility, Questionnare

1　はじめに

急速な情報通信技術（ICT）の進展により、インターネットは様々なビジネスにおいて一つの重要でかつ共通のインフラ（ビジネスプラットフォーム）となった。インターネットは社会生活や企業活動にとって必須のツールとなり、それを利用していくつもの新たなビジネス（B2B や B2C など）が展開されている。そしてこれらがもたらす正の経済効果は大きく、政府としても e-Japan 計画や u-Japan 計画による ICT 化の促進を図っている。このことは、企業の生産性や効率性、企業価値を高める ICT 投資の有効性が様々な実証分析から確認されている。

一方で、コンピュータウィルスや不正アクセスなどの情報セキュリティ被害という深刻な社会問題も顕在化してきている。また、これらの ICT のマイナス面についての研究は開始されて間もないために、その影響については不明なところがまだ多い[1]。今後、ユビキタス化時代が到来することを考えるとこれらの情報セキュリティの問題を経済学・経営学的に定性的かつ定量的に分析することには大きな意義があると考えられる。

本稿では、インターネット環境を個人や企業、その他の組織に提供しているインターネット・サービス・プロバイダ（ISP）を対象に、情報セキュリティに関する対策の現状を 2007 年 2 月に実施したアンケート調査の結果をもとに、明らかにする。また、同時に直面している課題についても議論していく。ISP を取り上げた理由は、ISP が情報インフラを担っており、もし情報セキュリティ事故や被害に遭遇した場合、その影響はかなり大きくなると予想できるためである。

本稿の構成は以下の通りである。次節で様々なインターネットの脅威を説明する。第 3 節においてアンケートの目的と概要を説明し、また第 4 節にてその集計結果を提示している。最後の節にて情報セキュリティ対策の現状と課題について議論し、本稿のまとめを与える。

2　インターネットの脅威と情報セキュリティ

インターネットは、単なるツールからビジネスプラットフォームへ 21 世紀の到来とともに大きく変化した。それと同時に、インターネットの脅威（例えば、コンピュータウィルス、DoS（Denial of Service）攻撃、ゼロディアタック、ボットネット、フィッシングやマルウェアなど）も劇的に様相を変えた。その内容は高度化・巧妙化したものとなっている。従来は単なる愉快犯であったものが、近年では金銭目的のネット犯罪となっている。昨今のインターネットの脅威の特徴をまとめたものが、表 1 である。情報処理推進機構（IPA）や JPCERT/CC が公開している情報インシデントに関する問い合わせ件数は年々増加傾向にある。

表 1: インターネットの脅威の特徴

	従来	現在
目的	愉快犯	犯罪・秘密暴露・金銭
経路	e-mail	Web・e-mail・IM など
侵入方法	単純かつ一度	複雑かつ連続
攻撃対象	不特定多数	特定の属性を持つ組織・個人など

また、これらの脅威をより一層拡大させている要因として、ソフトウェアやハードウェアなどの

[1]ICT の進展による負の経済効果を測定しているものとして Ukai and Takemura (2007) や Takemura and Ebara (2008) などがある。

脆弱性、利用者のモラルやインターネットの脅威に対する意識の低さなどが挙げられる。

これらのインターネットの脅威およびその他のインシデントに対して、有効なのが情報セキュリティ対策である。これは、単に情報を様々な脅威から防護するために情報システム（ファイアウォール、侵入検知システム、検疫システムなど）や技術を導入することだけではなく、組織構造の再構築や教育の必要性も含んでいる。

3　アンケートの目的・概要

榎原・中庭・竹村・横見 (2006) などで指摘されているように、地方 ISP は様々な条件によって経営状態が悪化の一途を辿っている。そのような状況において、ISP の情報セキュリティ対策を把握すること、および各 ISP が直面している情報セキュリティ対策に関する問題を明らかにすることをアンケートの目的としている。

2007 年 2 月に時点で「社団法人日本インターネットプロバイダー協会」のホームページに掲載されている 613 社の ISP を対象に郵送で記名式のアンケート調査をおこなった[2]。本アンケートの調査項目を大別すると、事業状況、情報セキュリティ対策、情報セキュリティ被害・システムトラブル、および政府に対する意見がある。それぞれの内容は多岐にわたったものとなっている。その内容については、付録を参照されたい。

4　アンケート集計結果

本稿では、アンケート調査項目のうち 5 つを取り上げることにする。なお、詳細なアンケート集計結果については竹村 (2007) を参照されたい。回収数は 63 社（回収率は約 10.3%）である。

4.1　情報セキュリティに関する規定について

図 1 には、情報セキュリティ対策として策定されていなければならないセキュリティに関する規定の状況についてまとめている。多くの ISP（88.9%）は何らかの形でセキュリティに関する規定

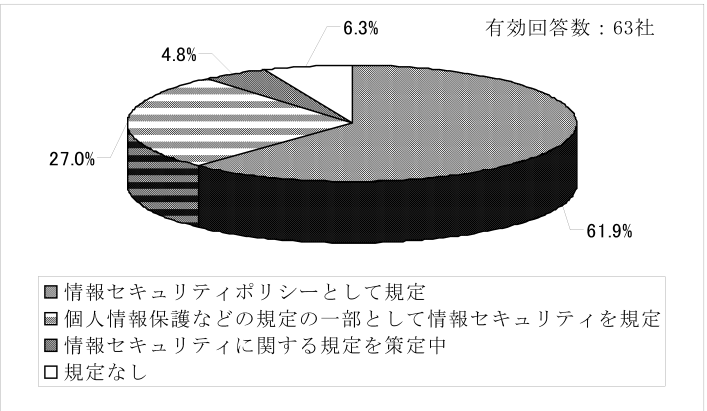

図 1: 情報セキュリティに関する規定

[2]http://www.rcss.kansai-u.ac.jp/ takemura/ を参照されたい。

をもっているものの、一部の ISP（11.3%）は現在規定をもっていないことがわかった。その規定していない理由としては、現場が必要性を認識していないことや、組織が少人数のために明確化する必要性がないこと、人材・資金不足といったことなどが挙げられている。

4.2　情報セキュリティに関する連絡体制・組織について

図 2 は情報セキュリティ事故やシステムトラブルが発生したときの連絡体制についてまとめたものである。その結果、連絡体制があると回答している ISP の割合は 93.4%になっているものの、連絡体制がないと回答している ISP の割合が 6.6%もあることがわかる。

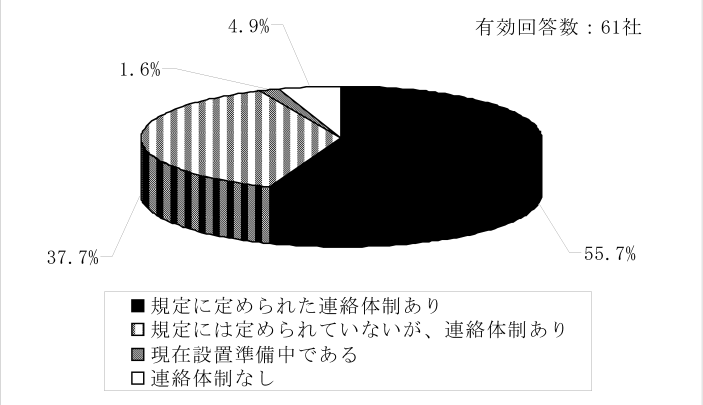

図 2: 連絡体制

また、図 3 には各 ISP の情報セキュリティ教育の実施状況を図示している。情報セキュリティ教育を実施していない ISP は資金・人材不足やその必要性がないと認識していることをその理由として挙げている。一方で、情報セキュリティ教育を実施している ISP の中で、全社的に実施している ISP の割合は 80.4%、管理者などの一部の者のみを対象に実施している ISP の割合は 19.6%となっていることもわかっている。

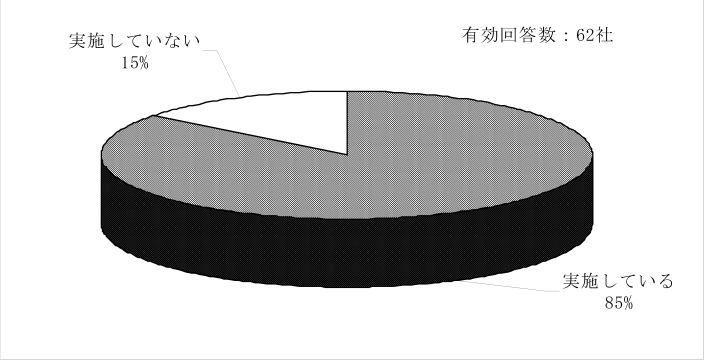

図 3: 情報セキュリティ教育の実施状況

4.3 監査体制などについて

情報セキュリティ対策を評価するためにはペネトレーションテストや様々な監査がある。図 4 と図 5 はそれぞれシステム監査と情報システム監査の実施状況をまとめたものである。図 4 と図 5 を見てわかるように、システム監査のみならず、情報セキュリティ監査を実施している ISP が多く存在することがわかる。

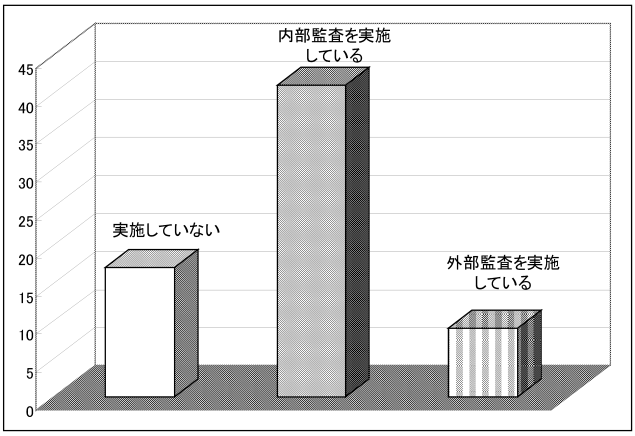

図 4: システム監査の実施状況

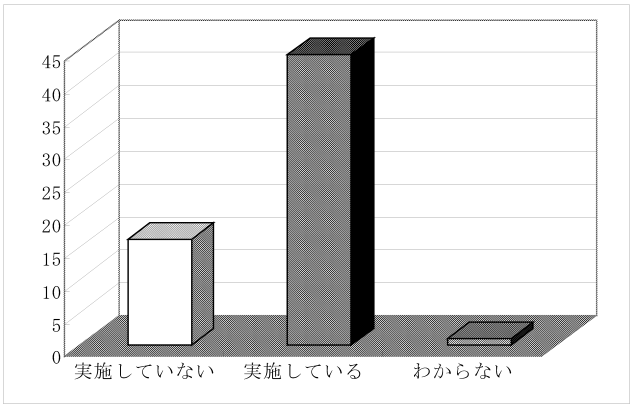

図 5: 情報セキュリティ監査の実施状況

図 6 には各種監査の必要性についてまとめたものを示している。監査やテストの必要性を認めている ISP にその理由を聞いたところ、「社会的責任（CSR）を果たすため」や「提供しているサービスの品質維持のため」などと回答している[3]。

このことは、過去に行ったアンケート調査と比較すると、ISP が社会に対して情報通信インフラを担っている企業もしくは組織・団体であることを意識していることがわかる。

[3]CSR（Corporate Social Responsibility）とは、コンプライアンス（法令遵守）、コーポレートガバナンス（企業統治）、ディスクロージャー（情報開示）などの一般に企業が社会に対して果たすべき「責任」と捉えられている。企業には、消費者、従業員、取引先、地域住民など幅広いステークホルダー（利害関係者）があり、CSR にはこうしたステークホルダーとの双方向のコミュニケーションが重要であるといわれている。つまり、企業をとりまくさまざまな立場の方々との双方向コミュニケーションがあってはじめて、ステークホルダーから信頼を得ることができるといえる。

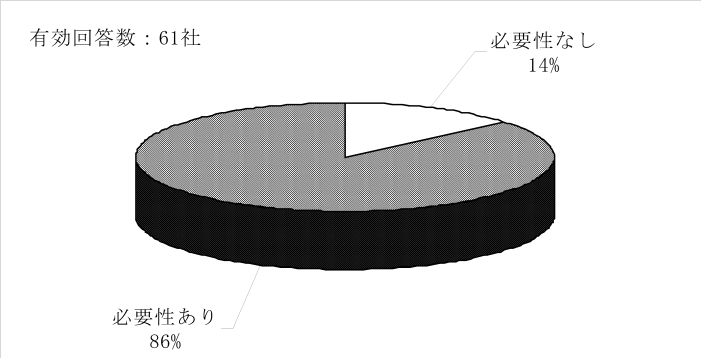

図 6: 監査やテストの必要性

4.4 対策の実施状況について

具体的な情報セキュリティインシデントに対して ISP がとっている対策について 2 つ質問した。まず図 7 は国内外問わずボットネットの拡大に寄与したとされる P2P（Peer to Peer）の利用規制の実施状況をまとめたものである。

次に、図 8 は spam メール対策に有効とされる OP25B（Outbound Port 25 Blocking）の実施状況をまとめたものである[4]。

図 7 と図 8 および自由記述から、これらの ISP の対策は有効と認められているものの、「通信の秘密」などの法律的解釈の問題が一部あり、必ずしも全ての ISP がこれらの対策を実施するに至っていない。

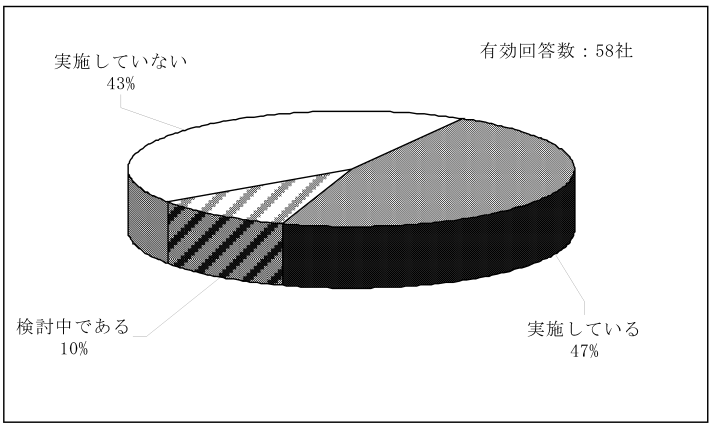

図 7: P2P の利用規制状況

また、自らの ISP を利用しているユーザに対して注意喚起をおこなっているか否かの状況についてまとめているのが図 9 である。 注意喚起をおこなっている ISP のほとんどが「ユーザのため」

[4]OP25B とは、メールの送信に使われる 25 番ポートをブロックし、特定の条件下においてメールの送信を不可能とする仕組みである。通常、一般的なユーザーがメールを送信する場合には ISP の SMTP サーバーを利用するが、迷惑メール配信事業者の場合は独自の SMTP サーバーを用意してメール配信を行なうケースが多い。そのため、OP25B を実施することにより、ISP の SMTP を利用しないメール送信のパケットをブロックし、迷惑メールの送信を防ぐことができる。

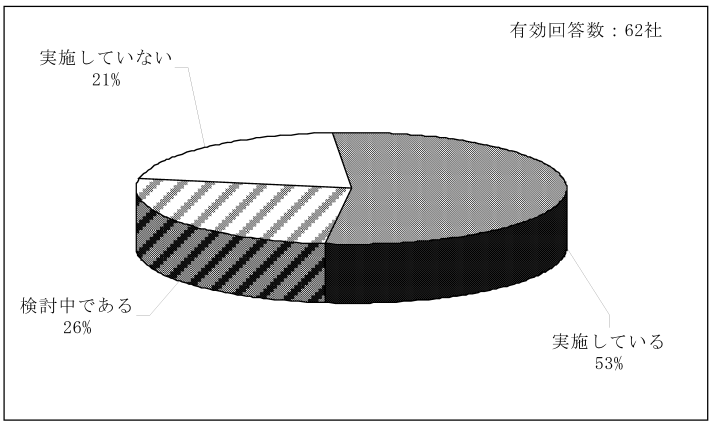

図 8: OP25B の実施状況

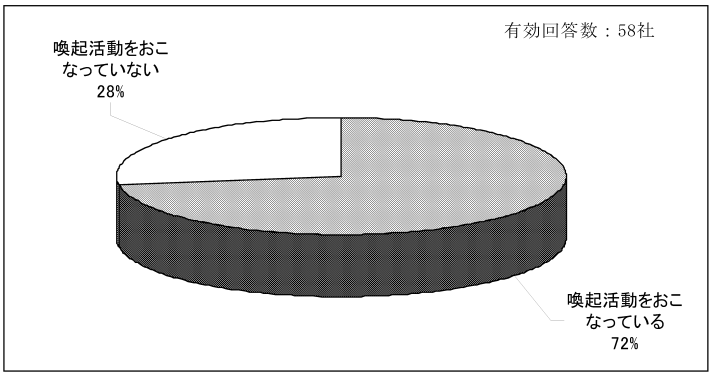

図 9: ユーザに対する注意喚起

を理由として挙げている。このユーザに対する注意喚起はある意味、ISP の直面するリスクを低減するために役立っていると思われる。

4.5 政府への希望

政府への希望として、政府に対して補助金などの制度の設立を望む ISP も存在していたものの、多くの ISP が非金銭的な制度（法律など）の整備を望んでいることがわかった。図 10 には、政府への情報セキュリティに関する要望をまとめたものを示している。

また、要望として最も多かったものはネット犯罪の罰則強化であった。続いて、無料の情報セキュリティ教育制度の充実、セキュリティ情報の共有制度の充実、省庁間で連携の取れた法制度、セキュリティ水準の策定に対して期待をよせていることがこの図からわかる。

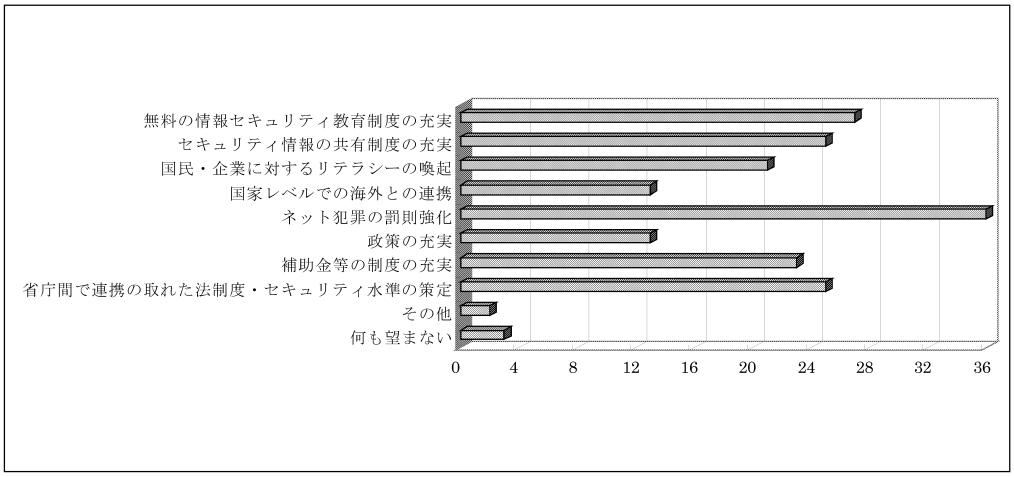

図 10: 政府への要望

5　まとめ

今回の情報セキュリティに関するアンケート調査と 2005 年 7 月に実施した榎原・中庭・竹村・横見 (2006) を比較すると、各 ISP の情報セキュリティ対策に関する態度が大きく変化していることが確認できた。特に、それは社会的責任を意識しているという特徴をもっていた。ただし、依然として資金と人材不足が問題となっていることがわかった。以前は情報セキュリティ対策の必要性を認めつつも、資金や人材不足を理由に十分な対策ができていなかった ISP が多かったものの、今回のアンケートでは認識するだけでなくそれを行動に移しているもしくは、移す努力をしている ISP が多数存在していることがわかった。

また、各 ISP のユーザに対する有効とされる情報セキュリティ対策（利用規制・注意喚起）については、ユーザの利便性や通信に関する法解釈を含む制約があるために、賛否両論であることがわかった。これは急速に進展しているインターネットに対する法整備の遅れや省庁間のコーディネートがまだうまく機能していないことが理由として考えられる。特に、管轄省庁から公表されているいくつものガイドラインが複数存在することによって ISP の対応に混乱を生じさせていることも事実である。この意味において、産業・省庁を横断する情報セキュリティ対策や政策に関するコーディネーターとしての役割を担っている内閣官房セキュリティセンター（NISC）の存在意義が今後大きくなることが予想される。もちろん、NISC がコーディネートしても、それを個人や企業が従わなければ意味がない。それゆえに、情報セキュリティ対策は、ネットワークを利用している全ユーザが施していく必要がある。

最後に、本稿ではアンケート調査一部の結果を用いて、ISP の情報セキュリティ対策の実態についてみてきた。今後、これらのデータを用いて、統計分析を行い、ISP が高い水準の情報セキュリティレベルを達成できる政策について議論していきたい。それについては、また別論文で取り扱いたい。

追記・謝辞

本稿は、文部科学省の科学研究費補助金交付課題「情報インフラにおけるセキュリティ投資の経済分析」（課題番号 18730202・若手研究 (B)・研究代表者 竹村敏彦）の研究成果である。業務多忙のなかアンケート調査およびインタビュー調査にご協力いただいた ISP 各社様に厚く御礼を申し上げたい。また、榎原博之氏（関西大学システム理工学部・准教授）と横見宗樹氏（大阪商業大学・専任講師）から有益なコメントをいただいた。

参考文献

[1] 榎原博之・中庭明子・竹村敏彦・横見宗樹 (2006)『インターネット・サービス・プロバイダの実証分析』多賀出版.

[2] 竹村敏彦 (2007)「第 2 回インターネット・サービス・プロバイダの情報セキュリティに関する実態調査報告書」関西大学

[3] Takemura, Toshihiko and Hiroyuki Ebara (2008) “Spam Mail Reduces Economic Effects,” *Proceeding of International Conference of Degital Society 2008*, forthcoming.

[4] Ukai, Yasuharu and Tohihiko Takemura (2007) “Spam Mails Impede Economic Growth” *The Review of Socionetwork Strategies*, Vol.1, pp.14-22.

第2回

インターネット・サービス・プロバイダの

情報セキュリティに関する実態調査

関西大学ソシオネットワーク戦略研究センター
竹村敏彦（ポスト・ドクトラル・フェロー）

〒564-8680　大阪府吹田市山手町 3-3-35
関西大学ソシオネットワーク戦略研究センター
TEL：06(6368)1111（内線 4533）
FAX：06(6330)3304
HP：http://www.rcss.kansai-u.ac.jp/~takemura/

本調査は ISP の情報セキュリティの管理者（責任者・担当者）を対象としております。お手数ですが該当する方に転送くださるようお願いします。また回答は本用紙に直接ご記入下さい。

※2005 年度についてご記入下さい。

※ご回答できない設問は N/A とお書き下さい。

貴社名	
サービス名	
回答者氏名	
E-mail アドレス	
部署名	
郵送先	〒
電話番号	
FAX 番号	
報告書の希望	報告書郵送希望（　）　　郵送不要（　）

※上記は調査結果を報告させていただく宛先とさせていただきますので、ご記入漏れのないようお願いします。

A 貴社の事業状況についてご回答下さい。

A-1　貴社の年間売上高・純利益についてご回答下さい。

年間売上高（万円）	
うち個人からの契約収入（万円）	
うち法人からの契約収入（万円）	
純利益（万円）	

A-2　貴社の加入者数を個人・法人別にご回答下さい。

個人（人）　　法人（社）

A-3　貴社の正規従業員数およびアルバイト・パート数についてご回答下さい。

正規従業員数（人）			
うち事務系（人）		うち技術系（人）	
アルバイト・パート数（人）			

A-4　貴社の提供しているアプリケーションサービスをご回答下さい。またそれは無料ですか。
（該当全てに○をお付け下さい）

①接続サービスのみ　　②ウェブ（有料・無料）
③メール（有料・無料）　　④ブログ（有料・無料）
⑤ＩＰ電話（有料・無料）　　⑥ストレージ（有料・無料）
⑦コンテンツ（有料・無料）　　⑧システムインテグレーション（有料・無料）
⑨ホスティング・レンタルサーバ（有料・無料）　　⑩セキュリティ（ウィルスチェックなど）（有料・無料）
⑪その他（　　）

A-5　貴社のサーバ数・クライアント数をご回答下さい。

サーバ数（台）　　クライアント数（台）

B　貴社の情報セキュリティ対策についてご回答下さい。

B-1　情報セキュリティに関する規定をお持ちですか。（該当全てに○をお付け下さい）

①ない
②情報セキュリティポリシーとして規定している
③個人情報保護規定の一部として情報セキュリティ関連の規定がある
④その他規定の一部として情報セキュリティを規定している
⑤現在情報セキュリティに関する規定を策定中である
⑥その他（　　）

B-2　B-1 で「①ない」と回答した方のみご回答下さい。

情報セキュリティに関する規定を制定していない理由をご回答下さい。（該当全てに○をお付け下さい）

①現場が必要性を認識していない　②経営者が必要性を認識していない
③人材・資金が不足している
④その他（　）

B-3　B-1 で「①ない」以外を回答した方のみご回答下さい。

情報セキュリティに関する規定の見直し状況についてご回答下さい。（該当全てに○をお付け下さい）

①見直しルールがない　②不定期ではあるが、見直しルールがある
③定期的な見直しルールがある
④その他（　）

B-4　情報セキュリティ管理担当者の人数をご回答下さい。

専任担当者（人）　兼任担当者（人）
その他（　）

B-5　情報セキュリティ事故やシステムトラブルが発生したときの連絡体制についてご回答下さい。（1 つ選択し、○をお付け下さい）

①規定に定められた連絡体制がある　②連絡体制はない
③規定には定められてはいないが、連絡体制はある
④現在設置準備中である　設置予定時期　＿＿年　＿＿月

B-6　セキュリティ関連情報の収集についてご回答下さい。（該当全てに○をお付け下さい）

①特に行っていない
②定期的に OS や基幹ソフトベンダーのホームページなどで関連情報を確認している
③セキュリティ情報を提供する組織（IPA など）のホームページを確認している
④セキュリティ情報提供のサービスを受けている
⑤セキュリティ関連のセミナーなどに積極的に参加している
⑥その他（　）

B-7　サーバのセキュリティを確保するためにどのようにして各種パッチを適用しているかご回答下さい。（1 つ選択し、○をお付け下さい）

①パッチ未適用
②問題が発生するまでパッチは適用しない
③定期的にパッチのリリース状況を確認する体制はないが、サーバ管理者などの裁量で適用している
④定期的にパッチのリリース状況を確認し常に最新状況を維持している
⑤わからない
⑥その他（　）

B-8　インターネットに接続されているクライアントのセキュリティを確保するためにどのようにして OS やウィルス定義ファイルなどのアップデートを行っているかご回答下さい。（1 つ選択し、○をお付け下さい）

①特に何もしていない　②問題が発生するまでアップデートはしない
③利用者の裁量で行っている　④常に最新状況を維持している
⑤わからない　⑥その他（　　）

B-9　ペネトレーションテスト（侵入検査）の実施状況についてご回答下さい。（1 つ選択し、○をお付け下さい）

①実施していない　②不定期ではあるが、実施している
③定期的に実施している　④わからない
⑤今後実施予定である　⑥その他（　　）

B-10　システム監査の実施状況についてご回答下さい。（該当全てに○をお付け下さい）

①実施していない　②不定期ではあるが、内部監査を実施している
③定期的に内部監査を実施している　④不定期ではあるが、外部監査を実施している
⑤定期的に外部監査を実施している　⑥わからない
⑦その他（　　）

B-11　情報セキュリティ監査の実施状況についてご回答下さい。（該当全てに○をお付け下さい）

①実施していない　②不定期ではあるが、実施している
③定期的に実施している　④わからない
⑤その他（　　）

B-12　ペネトレーションテストやシステム監査、情報セキュリティ監査の必要性はあると思いますか、またその理由も合わせてご回答下さい。（1 つ選択し、○をお付け下さい）

①必要性なし　②必要性あり

理由 （　　）

B-13　Winny などの P2P の利用規制についてご回答下さい。（1 つ選択し、○をお付け下さい）また、その理由も合わせてご回答下さい。

①必要性を感じないので、していない　②必要性は感じているが、していない
③規制を実施している　④現在検討中である
⑤その他（　　）

理由 （　　）

B-14　迷惑メール対策の OP25B（Outbound Port 25 Blocking）についてご回答下さい。（1 つ選択し、○をお付け下さい）また、その理由も合わせてご回答下さい。

①必要性を感じないので、していない　　②必要性は感じているが、していない
③実施している　　④現在検討中である
⑤その他（　　）

理由 （　　）

B-15　情報セキュリティ予算についてご回答下さい。（1 つ選択し、○をお付け下さい）

①特に予算計上していない　　②情報システム予算として計上している
③情報セキュリティ関連予算として計上している
④その他（　　）

B-16　B-15 で②もしくは③と回答した方のみご回答下さい。

情報セキュリティ関連予算の金額、また前年度からの増減額についてご回答下さい。おおよその額で結構です。

情報セキュリティ関連予算の金額（万円）	
前年度からの増減金額（万円）	

B-17　情報セキュリティを確保するために導入しているシステムをご回答下さい。（該当全てに○をお付け下さい）

①なし　　②ファイアウォール
③侵入検知システム（IDS）　　④DMZ セグメントの設置
⑤サーバ上でのウィルスチェック　　⑥検疫システム
⑦その他（　　）

B-18　情報セキュリティ対策の優先順位についてご回答下さい。（1、2、3 と番号をおふり下さい）また、その理由についてもご回答下さい。

情報セキュリティ対策　【　】　既存サービスの現状維持　【　】
新規サービスの展開・導入　【　】

理由 （　　）

B-19　貴社のユーザに対して、ホームページやメーリングリストなどで個人の情報セキュリティ対策の必要性について喚起活動を行っているかご回答下さい。（1 つ選択し、○をお付け下さい）

①はい　　②いいえ

理由 （　　）

B-20　貴社の情報セキュリティ教育の実施状況をご回答下さい。

①実施している　　②実施していない

B-21　B-20 で「②実施していない」と回答した方のみご回答下さい。

情報セキュリティ教育を実施していない理由をご回答下さい。

理由 （　　）

B-21　B-20 で「①実施している」と回答した方のみご回答下さい。

タイミングとその対象についてご回答下さい。（1 つ選択し、○をお付け下さい）

①定期的に、全社的に実施している

②不定期ではあるが、全社的に実施している

③定期的に、管理者など一部の者のみを対象に実施している

④不定期ではあるが、管理者など一部の者のみを対象に実施している

⑤その他（　　）

B-22　B-21 で①もしくは②と回答した方のみご回答下さい。

情報セキュリティ教育の内容をご回答下さい。（該当全てに○をお付け下さい）

①ウィルス・ワーム　②ネチケット　③パソコン設定

④サーバ設定運用　⑤緊急時対応　⑥ネットワーク知識

⑦通信事業に関する法律全般　⑧その他（　　）

B-23　B-21 で③もしくは④と回答した方のみご回答下さい。

情報セキュリティ教育の内容をご回答下さい。（該当全てに○をお付け下さい）

①ウィルス・ワーム　②ネチケット　③パソコン設定

④サーバ設定運用　⑤緊急時対応　⑥ネットワーク知識

⑦通信事業に関する法律全般　⑧その他（　　）

B-24　貴社で情報セキュリティ対策として今後計画しているものについてご回答下さい。（それぞれ 1 つ選択し、○をお付け下さい）

①セキュリティ関連マニュアルの作成

強く思う　思う　どちらでも　思わない　強く思わない

②情報セキュリティ教育の強化

強く思う　思う　どちらでも　思わない　強く思わない

③新しい情報セキュリティシステムの導入

強く思う　思う　どちらでも　思わない　強く思わない

④情報セキュリティ監査の強化

強く思う　思う　どちらでも　思わない　強く思わない

⑤スキルを要する人材の採用

強く思う　思う　どちらでも　思わない　強く思わない

⑥スパムメール対策の強化

強く思う　思う　どちらでも　思わない　強く思わない

⑦セキュリティ対策として他の ISP との情報共有システムの構築、またはそれへの参加

強く思う　思う　どちらでも　思わない　強く思わない

⑧セキュアなサービスを提供するためのネットワーク監視の強化

強く思う　思う　どちらでも　思わない　強く思わない

⑨ユーザ（法人・個人）に対する情報セキュリティサービスの提供

強く思う　思う　どちらでも　思わない　強く思わない

⑩その他

（　　）

C　貴社の情報セキュリティ被害・システムトラブルについてご回答下さい。

C-1　貴社が被った情報セキュリティ被害およびシステムトラブルについてご回答下さい。（それぞれ 1 つ選択し、○をお付け下さい）

項目	状況	頻度
不正アクセス（自社プロバイダのユーザによる）	なし サーバダウンせずただネットワーク障害あり サーバ数台ダウン システム全体ダウン	なし 10 回以下 50 回以下 それ以上
不正アクセス（他のプロバイダのユーザによる）	なし サーバダウンせずただネットワーク障害あり サーバ数台ダウン システム全体ダウン	なし 10 回以下 50 回以下 それ以上
ウィルス・ワーム（自社プロバイダのユーザによる）	なし サーバダウンせずただネットワーク障害あり サーバ数台ダウン システム全体ダウン	なし 10 回以下 50 回以下 それ以上
ウィルス・ワーム（他のプロバイダのユーザによる）	なし サーバダウンせずただネットワーク障害あり サーバ数台ダウン システム全体ダウン	なし 10 回以下 50 回以下 それ以上
システムトラブル（設定ミスなど）	なし サーバダウンせずただネットワーク障害あり サーバ数台ダウン システム全体ダウン	なし 10 回以下 50 回以下 それ以上

C-2　サーバ交換・修理（人件費）・損害賠償などの総被害額についてご回答下さい。おおよその額で結構です。

	万円

C-3　情報セキュリティ事故・システムトラブルに直面した方のみご回答下さい。(該当全てに○をお付け下さい)

①ホームページでお詫び広告・ユーザへの報告の実施　②サーバなどの設定変更
③新情報セキュリティシステムの導入・補強　④対策方法のマニュアル化
⑤その他（　　）

D　政府に対する意見についてご回答下さい。

D-1　国や地方自治体が定めるセキュリティ水準を遵守するという条件で、(金銭的)公的補助の必要性を感じますか。(1 つ選択し、○をお付け下さい)また、その理由も合わせてご回答下さい。

強く感じる　感じる　どちらでもない　感じない　強く感じない

理由 （　　）

D-2　同様の条件のもとで、(非金銭的)公的補助の必要性を感じますか。(1 つ選択し、○をお付け下さい)また、その理由も合わせてご回答下さい。

強く感じる　感じる　どちらでもない　感じない　強く感じない

理由 （　　）

D-3　政府に望むものがあればご回答下さい。(該当全てに○をお付け下さい)

①望むものはない　②無料の情報セキュリティ教育制度の充実
③セキュリティ情報の共有制度の充実　④国民・企業に対するリテラシーの喚起
⑤国家レベルでの海外との連携　⑥ネット犯罪の罰則強化
⑦政策の充実　⑧補助金などの制度の充実
⑨省庁間で連携の取れたセキュリティに関する法制度・セキュリティ水準の策定
⑩その他（　　）

E　自由記述

最後に、ご意見がございましたらご自由にご記入下さい。個人的な見解でももちろん結構です。

以上でございます。ご協力ありがとうございました。