インターネットセキュリティ行動を促進、抑制する要因
－なぜ人はセキュリティをしないのか？－

越智啓太
（法政大学文学部）

１，問題

インターネットを安心して使用するためには、適切なセキュリティを実施することが不可欠である。ネット経由での攻撃や情報流出、詐欺などの被害は、年々増加しており、かつ巧妙化しているにもかかわらず、十分なセキュリティ対策を行っていないものも少なくからである。セキュリティの問題は、個々人の問題というだけではない。例えば、標的型攻撃においては、組織内におけるもっともセキュリティ的に脆弱なメンバーが、組織全体の脆弱性を規定してしまう。そのため、最弱メンバーのセキュリティ不全が、、企業の情報漏洩やシステムダウンなどの被害をもたらしてしまう場合がある。さらに、自分のパソコンが気づかぬうちにに DDos 攻撃に踏み台になっていた場合には、迷惑メール配信や不正アクセス、場合によってはテロ攻撃に荷担していることになってしまう。企業だけでなく、特に学校においてはもともとセキュリティ意識が十分でなかったり、インターネット知識やスキルが未熟な多数のユーザーがいるため、状況はより深刻である。

このため、システム管理においては、ユーザーひとりひとりが適切なセキュリティ対策をすることを促進することが重要になってくる。人間という最弱なシステム要素をより強化するという必要性である。しかし、現在のところ、このような人的な要因に関する研究はそれほど多く行われているわけではない。本研究は、個人のセキュリティ行動についてそれを促進、あるいは抑制する行動に影響する要因について明らかにし、今後のセキュリティ教育、セキュリティ対策に対して方向性を示してみたいと思う。

本研究では、次のような方向で研究を進めることにする。

１）インターネットセキュリティに対する行動尺度の作成

インターネットセキュリティに関するユーザーの行動といってもそこには異なったさまざまな種類のものが存在する。そのため、「ユーザーのセキュリティ行動」というひとことでまとめてしまって議論をするのはあまりにもラフなものになってしまう。そこで本研究では、まず、インターネットセキュリティ行動を統計的な手法で分類し、いくつかの下位因子を抽出し、尺度化することにする。この尺度は、個人のセキュリティの脆弱性を測定する診断尺度としての役割も担うものになるであろう。

２）インターネットセキュリティに関する態度・認知・知識尺度の構成

インターネットセキュリティ行動に影響する要因として、コスト意識などのさまざまなネットに対する態度や認知、知識の要因があると思われる。そこで、つぎにこれらについてそれぞれ測定するための尺度を構成することにする。

３）インターネットセキュリティ行動に影響する諸要因

最後に１）で構成したインターネットセキュリティに関するユーザーの行動を規定する要因について２）の態度や認知の尺度との相関を分析し、インターネットセキュリティを促進あるいは抑制する要因について明らかにして行ってみたいと思う。

２，方法

調査参加者：18 歳以上の男女 1500 名、男性 750 名、女性 750 名、年齢層 10 代、20 代、30 代、40 代、50 代以上の 5 つのカテゴリーでそれぞれ 300 名ずつ。平均年齢 36.83 歳（標準偏差 15.14)、男性 36.94 歳(標準偏差 15.30)、女性 36.71 歳(標準偏差 14.98)。

調査方法：調査はウェブ調査で行った。実施は、2016 年 12 月である。調査協力者は、調査内容、所要時間の目安等についての解説文書を読んで、調査に協力すると同意したもののみに実施した。回答に要した時間は 15 分程度であった。なお、調査対象者には商品などと交換することができる一定のポイントが謝礼として与えられた。回答は PC やスマートフォン上で行われ、設問の呈示順序は尺度内でランダム化されていた。

調査項目：調査参加者の年齢、性別、居住県、家族構成（婚姻、子どもの有無)、職業に関する質問、一般向けのセキュリティ入門書などから収集したインターネットセキュリティに関する行動に関する項目 43 項目、インターネットセキュリティに関する態度や認知に関する項目 82 項目、コンピューターとネットワークに関する知識を測定する項目 16 項目、パーソナリティに関する項目（短縮版 5 因子性格検査）10 項目、犯罪不安に関する項目 9 項目を実施した。今回の報告では、セキュリティ行動 43 項目と、セキュリティに対する態度・認知に関する行動 82 項目の分析データについて報告する。

３，インターネットセキュリティリスクの特徴

インターネットセキュリティに関する行動に関する項目は、インターネットセキュリティに関する一般向けの入門書籍の中から、「このような行動は危険、あるいはすべきではない」とされている行動を網羅的に４３種類ピックアップしてリスト化した。「パスワードをメモにして貼っておく」、「公共の場所でパスワードでログインする」などの項目であり、それぞれの行動をどのくらい行っているのかについて、「まったくあてはまらない（1)」～「どちらでもない（4)」～「よくあてはまる（7)」まで 7 件法で評定させた。評定の平均値の高い項目と低い項目を以下の Table.1、2 にあげる(この Table にあげてある項目は実際の質問項目を簡略化したものである)。

一般にセキュリティを増加させるような行動は比較的良く行われており、リスクを増加させるような行動はあまり行われていない傾向がある。とくにリスク度が大きな行動は行われない傾向があり、この点ではそれなりのセキュリティ行動が行われていることを意味している。しかしながら、あまり行われていない行動でもその評定値は 2 以上であり、一定数のインターネットリスク行動が行われている現状も垣間見える(一般にこの種の調査では自らのリスク促進的な行動は過小報告されることが知られており、そのような意味でも、実際にはそれなりのリスキーな行動が行われていることが考えられる)。

Table 1. よく行われているリスク行動・セキュリティ行動

よく行われている行動（R はリスク行動、S はセキュリティ行動）	平均値（SD）
１，個人情報を Web などに載せない（S）	4.84（2.07）
２，ネット上でクレジットカードの決済を行っている（R）	4.38（2.26）
３，大文字と小文字を混在させたパスワードを使用している（S）	4.31（1.92）
４，パスワードを使い回している（R）	4.10（1.93）
５，SNS で公開範囲を限定している（S）	4.06（2.13）
６，アプリのバージョンアップをまめに行う（S）	4.05（1.89）
７，セキュリティソフトで定期チェックしている（S）	4.04（2.00）
８，まめにセキュリティアップデートを行う（S）	3.97（1.94）
９，写真を SNS にあげるときに写っている人の了解を取る（S）	3.95（1.98）
１０，複数のアカウントを同一パスワードにしている（R）	3.85（2.01）

Table 2. よく行われていないリスク行動・セキュリティ行動

よく行われていない行動（R はリスク行動、S はセキュリティ行動）	平均値（SD）
１，自宅の住所電話番号を SNS に載せる(R)	1.98（1.48）
２，パスワードを人に教えたことがある(R)	2.20（1.55）
３，怪しい URL にアクセスしたことがある(R)	2.33（1.51）
４，怪しい添付ファイルを開く(R)	2.37（1.56）
５，共有の PC でパスワード入力を行う(R)	2.37（1.64）
６，怪しいアプリをダウンロードする(R)	2.38（1.53）
７，個人写真を SNS にアップロードする(R)	2.39（1.78）
８，怪しい動画や画像をダウンロードする(R)	2.40（1.58）
９，他人の USB を自分のパソコンにさす(R)	2.46（1.62）
１０，知らない人からのメールを開く(R)	2.58（1.60）

４，インターネットセキュリティに関する行動尺度の構成

上記の分析では、セキュリティリスク項目をただ単に集計しただけであったが、次にそれぞれの行動の共起頻度をもとにして、セキュリティリスク行動をいくつかの下位因子に分解することにする。４３項目を全項目を因子分析し、同じ因子になったものや概念的に類似した項目をまとめてさらに因子分析（重みづけのない最小二乗法、プロマックス回転）をくり返し、最終的に４項目ずつからなる全２０項目のリスク行動尺度５つと７項目からなるセキュリティ行動尺度ひとつを構成した。以下にそれぞれの尺度を示す。

1）サイト閲覧・ダウンロード系リスク尺度

第 1 尺度は、怪しいサイトの閲覧や怪しいアプリ、動画などのダウンロードに関連した 4 つの項目から構成された。構成された尺度は、ひとつの因子で分散の 59.86%を説明することができた、α係数は 0.851 となった。尺度の平均値は 10.13、標準偏差は 5.40、歪度は 0.552、尖度は-0.404 となり、得点 0 にやや偏った分布となった。

Table 3. サイト閲覧・ダウンロード系リスク尺度

項目	因子負荷量	共通性
1，怪しいサイトを閲覧したことがある	.715	.512
2，怪しいアプリ(プログラム）をダウンロードしたことがある	.814	.662
3，怪しい動画や画像をダウンロードしたことがある	.847	.717
4，怪しい添付ファイルを開いてしまったことがある	.709	.503

2）パスワード公共リスク尺度

第 2 尺度は、パスワードに関するリスク尺度であるが、この因子は、その中でもパスワードを公共の場所で入力したり（ショルダーハッキングなどの恐れがある)、他人にパスワードを教えたりするというリスク項目 4 つから構成される因子となっている。構成された尺度は、ひとつの因子で分散の 46.91%を説明することができた。α係数は 0.775 となった。尺度の平均値は 10.06、標準偏差は 5.13、歪度は 0.432、尖度は-0.677 となった。

Table 4. パスワード公共リスク尺度

項目	因子負荷量	共通性
1，電車内やカフェなど公共の場所でパスワード入力を行っている	.674	.454
2，他人と共有のパソコンでパスワードを入力している	.623	.389
3，他人の目の前でパスワードを入力することがある	.793	.629
4，パスワードを人に教えたことがある	.636	.405

3）パスワードの管理リスク尺度

第 3 尺度は、パスワードに関するリスク因子で、とくにパスワードを PC に記録したり、パスワードを使い回しすることに関するリスク尺度である。構成された尺度は、ひとつの因子で分散の 41.83%を説明することができた。2 番目の項目が若干異質なものと

なったが概念的には類似度が大きいと思われるので、あえてこの尺度にいれることにした。そのため、α係数は 0.682 となり低めである。尺度の平均値は 15.28、標準偏差は 5.70、歪度は-0.238、尖度は-0.351 となった。

Table 5. パスワード管理リスク尺度

項目	因子負荷量	共通性
1，ＩＤやパスワードをパソコンに記憶させている	.535	.287
2，パスワードをノートやメモに書いている	.261	.068
3，パスワードを使い回している	.820	.672
4，複数のアカウントで同一のパスワードを使用している	.804	.646

4）フリーワイファイリスク尺度

第４尺度は、ネットカフェや街中などのフリーワイファイでのリスキーなネットの仕様の個人差を測定したものとなった。いうまでもなく、フリーワイファイは情報がそこから抜き取られることが多く、十分に注意しないと危険な通信手法である。この尺度は、フリーワイファイ使用時の暗号化確認や送受信情報への注意に関するものとなっている。この尺度は、ひとつの因子で分散の 67.79%を説明することができた。α係数は 0.890、平均値は 14.50、標準偏差は 6.66、歪度は 0.32、尖度は-0.662 となった。

Table 6. フリーワイファイリスク尺度（逆転尺度）

項目	因子負荷量	共通性
1，フリー Wi-Fi を使用するときは暗号化を確認する	.781	.610
2，フリー Wi-Fi の使用はできるだけ避ける	.725	.526
3，フリー Wi-Fi で重要な情報の送信は避ける	.881	.776
4，フリー Wi-Fi を使用するときは送受信する情報の内容に注意する	.894	.798

5）個人情報リスク尺度(逆転尺度)

第５尺度は、自分自身の個人情報や他人の個人情報をウェブ上で流出させてしまうことに関する関するリスク尺度である。個人情報をできるだけウェブに載せないようにしている、ネットに写真などを投稿する場合、位置情報が含まれていないかをチェックする、などの 4 つの項目から構成され、ひとつの因子で分散の 51.84%を説明することができた。α係数は 0.806 となった。尺度の平均値は 16.70、標準偏差は 6.48、歪度は-.295、尖度は-0.492 となった。

Table 7. 個人情報リスク尺度

項目	因子負荷量	共通性
1，個人情報はできるだけウェブに載せないようにしている	.606	.368
2，SNS などでは公開範囲を限定している	.691	.478
3，自分の写真をネットにアップする場合、一緒に写っている人に了解を取るか他人の顔を隠す	.787	.619
4，ネットに写真などを投稿する場合、位置情報が含まれていないかをチェックする	.780	.609

6）セキュリティ強化行動尺度

ここまであげてきた尺度はリスク行動を行う、あるいはリスク行動を行わないという尺度であったが、より積極的にセキュリティを強化する方向の行動についての尺度を構成した。この尺度のみは全部で 7 項目から構成されている。ひとつの因子で分散の 42.49%を説明することができた。α係数は 0.835、尺度の平均値は 24.65、標準偏差は 9.10、歪度は-0.65、尖度は-0.19 となった。

Table 8. セキュリティ対策行動尺度

項目	因子負荷量	共通性
1，パスワードは頻繁に変更している	.505	.255
2，プログラムやアプリのバージョンアップはまめに行う	.628	.394
3，添付ファイルを開くときはセキュリティソフトでチェックをする	.673	.453
4，自分のパソコンはセキュリティソフトで定期的なチェックをしている	.760	.577
5，セキュリティソフトをまめにアップデートする	.777	.603
6，添付ファイルを送るときはパスワードでロックする	.566	.321
7，パスワードを入力するときは後ろに人がいないかを確認する	.609	.371

7）インターネットセキュリティ尺度間の相関

上記の 6 つの尺度の間の相関係数について以下に示す。全体的に見て、リスクを増加させるような項目（サイト閲覧、パスワード公共、パスワード管理）と、セキュリティを促進させるような項目（フリーワイファイ（逆転項目）、個人情報（逆転項目）、セキ

ュリティ行動）がそれぞれ相互に相関が高いことがわかった。それぞれの項目は比較的独立性が高かった。

Table 9. インターネットセキュリティ尺度相互の相関係数

	パス公共	パス管理	フリー	個人情報	セキュリティ
サイト閲覧	.546	.350	.146	.143	.291
パスワード公共		.425	.083	.121	.175
パスワード管理			.095	.259	.155
フリーワイファイ				.485	.615
個人情報					.494

次に、尺度間の相関関係を明確にするためにクラスター分析を行った。クラスター分析は、Ward 法で行い、それぞれの変数ごとに個人データを Z 得点に変換し、変数ごとのユークリッド平方距離を用いて分析を行った。デンドログラムを以下に示す。

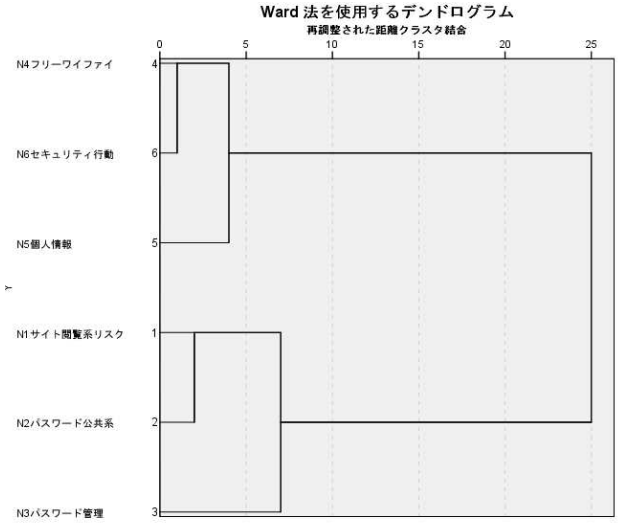

Fig 1. インターネットセキュリティ尺度クラスター分析結果

８）リスク増加尺度とインターネットセキュリティ促進尺度の構成

以上の結果を基にして、サイト閲覧、パスワード公共、パスワード管理尺度についてそれぞれの尺度について、個人ごとに標準化した得点の合計をリスク増加尺度の得点とし、フリーワイファイ（逆転項目）、個人情報（逆転項目）、セキュリティ行動尺度について、個人ごとに標準化した得点の合計をセキュリティ促進行動尺度の得点とした。これらの尺度の相関係数は、$r=0.248$（無相関検定 $p<.01$）となった。これは、リスクとセキュリティを同時に増加させている、つまり、リスキーな行動もとるが、セキュリティも強化するというものが一定程度いることを意味している。

５、インターネットセキュリティに関する態度・認知尺度の構成

次に、インターネットセキュリティをめぐる個人のさまざまな態度や認知を測定するための尺度を構成した。

１）セキュリティのコスト感尺度

セキュリティのコスト感尺度は、コンピューターに対して各種のセキュリティ対策を施したり、そのための知識を習得したり、時間をとったりすることに対するコスト感を測定する尺度である。「パスワードをこまめにかえるのは面倒だ」、「セキュリティソフトの購入や設定が面倒くさい」など９つの項目からなる。因子分析したところ、ひとつの因子にまとまり、全体の分散の 60.12%を説明することができた。

２）セキュリティリスクに対する軽視尺度

この尺度は、セキュリティリスクをたいしたことがない、実害はない、何とかなるだろうと考える態度を測定するものである。「自分のパソコンがウィルスに感染してもたいしたことはないだろう」、「自分のパソコンの情報が漏れたとしてもたいした実害はないだろう」など４つの項目からなる。因子分析したところひとつの因子にまとまり、全体の分散の 67.18%を説明することができた。

３）セキュリティリスクに関する社会認識尺度

この尺度は現在の社会において、セキュリティリスクがどの程度深刻な問題であると考えているのかを測定する尺度である。「インターネットセキュリティの問題は社会的に深刻な問題である」、「世の中ではたくさんのインターネット犯罪が発生している」など５つの項目からなる。因子分析したところ、ひとつの因子にまとまり、全体の分散の 77.39%を説明することができた。

４）セキュリティの実行者割合についての認知尺度

この尺度は自分の周囲の友人や同僚がインターネットセキュリティの実行に対してどの程度積極的であるのかを測定するものである。関連する 8 項目を因子分析したところ、2 つの因子が抽出され、第 2 因子までで、全体の分散の 60.47%が説明できた。プロマックス回転をしたところ、第 1 因子は、「自分のまわりでは真剣にセキュリティ対策している人はそれほど多くない」など、自分のまわりがセキュリティをないがしろにしているという程度を測定するものとなり、第 2 因子は「自分のまわりの人はコンピューターセキュリティに熱心である」など、第 1 因子と反対に自分のまわりがセキュリティに熱心だという尺度となった。尺度間の相関は、r=.187 であった。そこで、この第 1 因子と第 2 因子をそれぞれ別の尺度とすることとした。

５）セキュリティ被害確率の認知尺度

この尺度は自らがウィルス感染や情報漏洩、アカウント乗っ取り等のインターネットのセキュリティリスクの被害に遭うかどうかについての主観的な確率を測定する尺度である。「自分のパソコンから情報漏洩する可能性が少ないだろう」などの当初用意した 11 項目を因子分析したところ 2 つの因子が抽出されたので 2 項目を削って、1 因子からなる尺度を構成した。この 9 項目で全体の分散の 63.43 %が説明された。

６）セキュリティリスク対処能力の自己認知尺度

この尺度はさまざまなセキュリティ上のリスクに対して自分が対処可能だと考えているのかを測定する尺度である。当初準備した 11 項目を因子分析したところ、２つの因子が抽出された。プロマックス回転の結果、1 つの項目が両方の因子に寄与していたため、この項目を削除して再度、因子分析を行なったところ、5 項目ずつ 2 つの因子が抽出された。この 10 項目で全体の分散の 61.58 %が説明された。第 1 因子は、「自分のパソコンに何か異常事態が起きた場合、ある程度は対処できる」などの項目からなり、各種のセキュリティリスクに対して対処ができるという認知を、第 2 因子は、「パソコンやネットで警告メッセージが出ても意味がわからないことが多い」などの項目からなり、各種のセキュリティリスクに対して自分は何をしたら良いのかがわからないという因子であった。因子間相関は、r=-.218 であった。

７）コンピューターに関する自己効力感尺度

この尺度は、PC やインターネットの使用に関して自分の力で難しい問題でも解決しようとする、試みようとする動機づけを測定する尺度である。「パソコンやインターネットで難しいように見えることであってもやってみれば理解することができると思う」など当初準備した 6 項目を因子分析したところ、ひとつの因子にまとまったが、因子負荷量が低かった 1 項目（「ネットで新しいサービスがあると積極的に使用してみるほうである」）、概念的にこの尺度に適切でない項目（「ネットの危険性や攻撃への対処法については十分に理解している」）１項目を削除して４項目の尺度を作成した。この 4 項目によって分散の 63.5%を説明することができた。

８）セキュリティ対策の効果性認知尺度

この尺度は、セキュリティソフトの導入などさまざまなセキュリティ対策が実際に効果をもつものなのかについての認知を測定するものである。当初用意した 7 項目を因子分析したところ、2 つの因子が抽出され、全体の分散の 53.87%が説明された。第 1 因子は、「セキュリティソフトはあまりあてにならないと思う」などセキュリティ対策に対して効果がないと考える因子で、3 項目から構成された。第 2 因子は、「自分が行ったセキュリティ対策によってネット上の脅威から身を守れていると思う」など、第１因子と反対にセキュリティ対策には効果があると考える因子で残り 4 項目から構成された。因子間の相関は r=.456 となった。セキュリティ対策が効果がないと考える尺度と効果があると考える尺度に比較的高い正の相関があるのは若干、矛盾していると思われるが、「セキュリティソフトは過信してはならないので、当てにならないが、ある程度の脅威を防いでくれているのは確かなので、そのような意味では効果がある」といった考えを多くの

人がしていると思われるので、実際上、矛盾するのではないのであろう。

９）セキュリティ不安に関する尺度

この尺度は、パスワード破り、ウィルス、個人情報乗っ取りなど各種のインターネットセキュリティリスクに対してどの程度不安を感じているのかを測定する尺度である。「自分のパスワードが破られるのではないかと不安である」など当初用意した 9 項目を因子分析したところ、ひとつの因子にまとまり、すべての分散の 61.60 %を説明することができた。

１０）セキュリティ教育に関する尺度

この尺度は以前、そして現在、どの程度セキュリティ教育を受けてきたか、受けているかについての自己評定質問である。「コンピューターセキュリティについての授業を中学、高校、大学等で受けたことがある」など当初準備した 5 項目を因子分析したところ、ひとつの因子のみでまとまり、すべての分散の 47.18%を説明することができた。

１１）セキュリティ被害経験についての尺度

この尺度は、いままでネットなどでなんらかの被害を受けたことがあるのかを測定するものである。不正ログイン、SNS 乗っ取り、クレジットカード不正使用、チャージ金窃取、ウィルス感染、不正請求、ネットショッピングトラブルについて質問した。この尺度に関しては、回答カテゴリーが、全くない（１）、おそらくない（２）、一度程度ある（３）、２～３度程度ある（４）、４～５回程度ある（５）、ときどきある（６）、よくある（７）とした。7 項目の被害経験評定値を因子分析したところ、ひとつの因子が抽出された。ただし、この中の一項目（「不正請求のメールが届いたことがある」）は、因子負荷量が比較的少なかったため、削除し、再び因子分析を行った。その結果、一つの因子で全体の 71.75 %の分散を説明することができた。

６，インターネットセキュリティ行動を規定する要因

１）リスク行動を促進する要因

インターネットリスク行動を促進する要因を明らかにするために、インターネットリスク尺度得点を従属変数、インターネットセキュリティに対する態度・認知尺度１１個を独立変数とする重回帰分析を行った。変数の選択は、ステップワイズ法で行い、F 値が $p<.05$ で変数投入、$P>.1$ で変数除去を行った。その結果、６ステップで６変数を選択して終了した。調整済み R 二乗=0.176、推定値の標準誤差は 2.16 となった。

以下に選択された変数と標準化 β の値を示す。このうち被害経験は、それがリスク要因となっているという因果関係であるよりもむしろ、リスク行動を行うことが被害経験を引き起こしているという逆の因果関係があると思われる。また、被害不安も同様で、リスク行動を行うことによってある程度の不安が生じているという因果関係だと思われる。それ以外の変数を見てみると、コスト感と社会認識、周囲の人々がセキュリティ行動をないがしろにしていることがリスク行動を引き起こす重要な要因であることがわか

る。つまり、「セキュリティの問題は社会的にもたいした問題ではないし、対処も面倒だし、まわりも熱心でない」と感じている人ほどリスク行動が促進されることがわかった。

Table 10. インターネットリスク行動を促進する要因

要因	標準化 β	有意確率
被害経験	.294	p<.01
コスト	.202	p<.01
社会認識	-.156	p<.01
周囲ないがしろ	.107	p<.01
自己効力感	.090	p<.01
被害不安	.061	p<.05

２）セキュリティ行動を規定する要因

インターネットセキュリティ行動を促進する要因を明らかにするために、インターネットセキュリティ尺度得点を従属変数、インターネットセキュリティに対する態度・認知尺度１１個を独立変数とする重回帰分析を行った。変数の選択は、ステップワイズ法で行い、F 値が p<.05 で変数投入、P>.1 で変数除去を行った。その結果、１０ステップで１０変数を選択して終了した。調整済み R 二乗=0.243、推定値の標準誤差は 2.16 となった。

Table 11. インターネットセキュリティ行動を促進する要因

要因	標準化 β	有意確率
社会認識	.267	p<.01
コスト	-.162	p<.01
自己効力感	.150	p<.01
セキュリティ軽視	-.140	p<.01
周囲熱心	.122	p<.01
対処能力	.095	p<.01
セキュリティ教育	.082	p<.01
効果なし認知	-.080	p<.01
被害不安	.068	p<.05
周囲ないがしろ	.062	p<.05

興味深いことに社会認識がもっとも β が大きくなった。つまり、現在の社会にセキュ

リティ上の脅威があると感じるほどセキュリティ対策を行うということである。また、セキュリティ対策にコスト感を感じていないほど、セキュリティを軽視していないこと、周囲がセキュリティに熱心であること、セキュリティ教育を受けてきたことがあるほど、セキュリティ行動が促進されることがわかった。また、対処能力や自己効力に見られるようにコンピューターやセキュリティの各種の問題について、自分の力で対処できる、やってみればなんとかなると感じているほどセキュリティ行動が促進されていることがわかった。

7，考察

本研究では、人々のインターネットセキュリティ行動の促進、抑制要因をあきらかにするために研究を行った。まず、セキュリティの個人差を測定する尺度を作成し、次にセキュリティに関する態度、認知に関する尺度を作成した。つぎにこれらの尺度を用いて、セキュリティ促進、抑制要因を明らかにした。

本研究で示された第 1 の結論は、インターネットセキュリティ促進行動とリスキー行動促進はそれぞれ異なったメカニズムによって生じているものであり、それを促進、抑制する要因も異なっているということである。そのため、セキュリティを高めるためには、セキュリティ行動の促進とリスキー行動の抑制は分けて考える必要性があるだろう。

第 2 に、リスキー行動を規定する要因として、「セキュリティの問題は社会的にもたいした問題ではないし、対処も面倒だし、まわりも熱心でない」という態度が明らかになった。したがって、リスキー行動を減少させるためには、セキュリティが社会的に大きな脅威であるという教育、セキュリティソフトの簡易化などのセキュリティコストの低減、周囲の人々のセキュリティ意識をまとめてあげるという対策が必要だということがわかった。

第 3 に、セキュリティ行動を規定する要因として、「セキュリティの問題は社会的に大きな問題であり、そのためには対処コストはわりにあうものであり、まわりも熱心である」というリスキー行動と逆の態度、認知が重要になることがわかったが、それに加え、コンピューターやネットに関しての効力感、つまり、自分のセキュリティ行動が役に立っているという認知が重要であることが示された。また、対処能力がそれなりにセキュリティ行動と関連していたということは、一部の「難しいことはわからないので、セキュリティもわからない、それゆえ、対策もわからない」という層が存在することを示している。ここでは、やはりコンピューターユーザーに対する広範囲のセキュリティ教育が必要であることを示しているのであろう。

本研究で開発された、セキュリティ尺度はいままで漠然と語られることの多かった、セキュリティを個人差をもとに測定し診断することができるものであり、今後のセキュリティ研究に重要な役割を果たしていく可能性を持っている。また、企業や学校におけるセキュリティ診断においても有効に使用できると思われる。ただ、このセキュリティ尺度はあくまで、主観的なセキュリティ行動を測定しているものであり、実際の行動をどの程度反映できているのかには問題がある。今後はこれらの点についてより詳細な研究を行っていくことが不可欠であろう。