Vol.2011-GN-79 No.7
2011/3/17

集合知ゲームを用いた情報セキュリティ対策への意識調査に関する検討

吉開範章[†]　栗野俊一[†]　飯塚信夫[††]
神田大彰[†]　高橋俊雄[†††]

ウイルスに感染した状況は、緊急(パニック）状態の一種と考えられ、心理学の対象となる領域であるが、これまでに報告された例はない。また、情報セキュリティ分野において、個人が対策する意思があっても、対策行動はとらない等の現象が知られており、個人の振る舞いや意思決定などに関する研究が始まっている。今回、感染ＰＣを有するユーザーの情報セキュリティに関する意識を、集合知をベースとする集団仮想ゲームを使って実験的に調査し、ウイルス対策への協調行動を誘発させる方策についてにアンケート結果も交えて検討したので、報告する。

Survey and Experiment on Consciousness of Information Security Protection by "Wisdom of Crowd" Game

NORIAKI YOSHIKAI[†]　SHUN-ICHI KURINO[†]
NOBUO IIDUKA[††]　HIROAKI KANDA[†]
TOSHIO TAKAHASHI[†††]

The situation under virus attack can be considered to be a kind of Panic. However, there have been no report about such a circumstance in the psychology. In the field of the information security, it is well known that some people do not take action for protection even if they would have the will for carrying on the protection. For investigating the thinking mechanism, the research of individual behavior and the decision making has been started. This paper mentions the experimental research results about the consciousness of Information security protection by using the wisdom of crowd game, and the analytical results for how to incubate the cooperative action based on the experimental data and some questions.

1. はじめに

DDoS(Distributed Denial of Service) 攻撃は、全世界を通じて増加しており、政府・官庁・自治体及び企業など、集団的活動を行う組織にとっては、大きな脅威となっている。損失額で示すと、Amazon、Yahoo、eBay 等のサイトに対する DDoS 攻撃の累積損失額を１２億ドルと見積もる報告や、サイトへの数日間の攻撃で Microsoft は５億ドルの損失を受けたとの報告も出されている[1]。DDoS 攻撃の中で、最近、特に大きな問題になっているボット攻撃においては、対策事業を行っているサイバークリーンセンター（ＣＣＣ）から感染ＰＣ保有者への注意喚起に対して、3 割だけが対策を実施しているとの報告がある[2]。企業や組織におけるセキュリティ対策疲れが見え始めている今日[3]、ウイルス感染下におけるヒトへの説得が旨くいけば、新しいＩＴ投資を行うことなく、ボットネット自体を消滅させることが可能になるかもしれない。そのためには、ウイルス感染の事実を教えられた個人の心理は、どのように変化し、どのようなプロセスを経て、行動に結びつくのかを知る必要があり、説得心理学の応用を検討することに意味がある。そこで、今回、ボットウイルス対策を前提に、説得心理学を基礎にした情報セキュリティ対策を、アンケートと共に実験を交えて検討したので、その概要について報告する。

2. 情報セキュリティリスクの関連研究

情報セキュリティは総合科学であり、「ヒト」の心理・行動の研究が必須であるが、ソーシャルエンジニアリングが研究主体であり、リスク認知・パニック心理に関する研究は、ほとんどなされていない[4]。

一方、従来から、災害や地震などでのパニックに対する説得心理学の研究はなされている[5]が、情報セキュリティ環境でのパニックの研究は、全くなされていない。

個人の振る舞いや意思決定と社会との関連についての研究としては、情報セキュリティ対策の状況を、個人の合理性と社会の最適性の乖離である社会的ジレンマ状況に想定した実証研究の報告がある[6]。この報告では、実行意図はあるものの、実際の状況は、対策ツールのダウンロード率 32．4%と相違があることが指摘されている。また社会的ジレンマ状況を表す４つの認知要素である自己への危機感､社会への危機感、無効感、コスト感のうち、実行意図に最も影響を与えたのは、自己への危機感であったという分析結果を報告している。

† 日本大学理工学部
College of Science & Technology, Nihon University
†† 日本大学豊山女子高等学校
Nihon University, Buzan Girls Senior High School
††† 雇用能力開発機構
Employment and Human Resources Development Organization of Japan

3. 情報セキュリティ対策への意識調査方法

3.1 実験の必要性

一般に、心理学の調査においては、Ｗｅｂや電話、あるいは紙ベースでの質問を用いたアンケート調査が主体であるが､情報セキュリティ対策を推進することを目的に、個人の意思決定のメカニズムに注目したアンケートによる意思決定分析の試みがある[6]。これによると、8 割の回答者は実行意図をもつ状況にあり、実行しない個人の有する意思決定プロセスを分析することが必要とされていた。本アンケートでの質問では、回答者の保有するＰＣが、ウイルスに感染したと仮定した状況下での回答をお願いした。実際にはリスク下にない状況での回答であり、現実の状況における心理とは乖離している可能性が高いと考える。

3.2 調査フロー

実験での実験協力者の振る舞いを調査する前に、実行意図を分析調査する目的で、アンケートによる調査を実施した。本調査で想定するボット対策において、ＩＳＰから利用者に送られてくる注意喚起メールを“説得メッセージ”とし、駆除ツールをダウンロードする行動を“態度変容”として捉えると、社会心理学の一分野である説得心理学の枠組みで考えることができる[5]。本調査では、説得メッセージを理解して、同意するかどうかの判断をするまでのプロセスに注目した「精緻化見込みモデル」[7]と、メッセージから脅威を感じ、脅威査定による対処行動に注目した防護動機理論[8]の両方を前提に分析する。具体的には、アンケートにより、情報セキュリティに対する意識、インターネットに対する意識、デモグラフィックデータを得ることにより、実験結果との関係の分析、例えば、実行意図と属性との関係、対策実行意図と実施した行動との相関性、対策実行に影響を与える要因等を明らかにする。詳しいアンケートによる調査報告は、文献[9]を参照されたい。

4. 実験概要

4.1 環境と設備

実験協力者には、実験の真の目的は伏せて､「集合知を使ったゲーム環境下における心理実験」（以降、仮想ゲームと呼ぶ）と伝え、情報セキュリティに関連する実験とは推測できないように工夫した。

実験環境としては、実験協力者が実験に必要な情報のみを得る環境を準備することから、外部環境の影響を受けにくい消音室を実験協力者毎に用意し、その中に、実験協力者が操作する実験ソフトが動作するＰＣを準備して、部屋の中からゲームに参加できる環境をセットした。

実験は、実験協力者が仮想ゲームを行う過程において、ウイルス感染に関するインシデントを表示し、その情報に対して、どのような行動をとるのかを観測する。そのため、実験協力者の行動記録だけでなく、その行動を監視し、場合によっては、説得的にコントロールするような機能（監視用ＰＣ群）を有する環境も準備する必要がある。また、実験協力者の行動により、ＰＣが感染したことを実感させるために、インターネットにアクセスし、何らかの操作を実施させる必要があり、実験ネットワークは、インターネットとのインタフェースを持つ必要がある。図１に、実験設備構成の概要を示す。

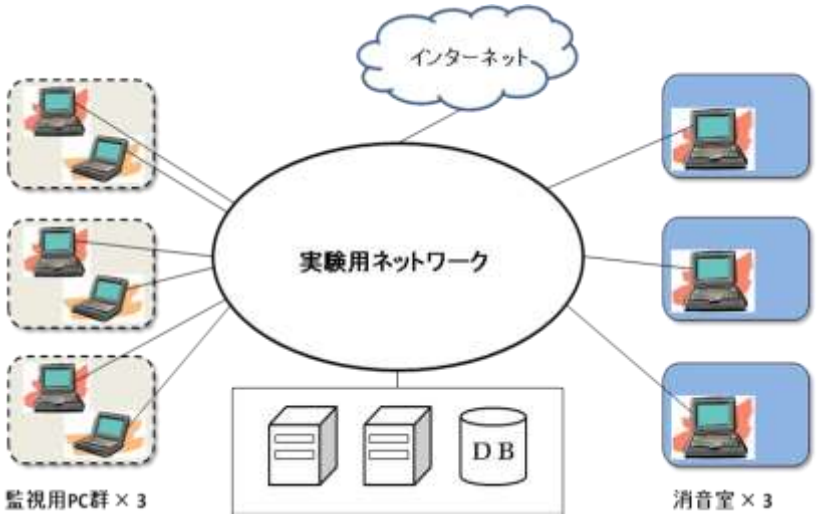

図 1　実験設備概要

4.2 実験シナリオ

実験の目的から、シナリオとしては、仮想ゲームの趣旨説明を含む「事前説明」と、仮想ゲームに参加した状況における実験状態（正常な動作をするゲーム状態と、ウイルスの感染による異常状態に区分）と、実験終了後の処理に区分される。主な実験フローを図 2 に示す。

なお、実験終了後には、（社）日本心理学会の倫理綱領[10]に基づき、真の実験目的を説明し、実験協力者が実験中に感じた疑問や不安などに対する対応を行った。

（1）事前説明：　実験協力者 3 名を同じ部屋に集め、実験の趣旨説明を行う。この時、集合知による意思決定のための実験であり、そのために個室に入る必要があると説明する。また、会場には、3 名が集まっているが、関東一円に、約１００名の参加者が同時にゲームに参加していること、及び、正解は多数決論理で決まり、自分の回

答が正解であれば、ポイントを得られ、それに比例して報酬が与えられると説明する。正解の場合は、10 ポイント獲得、不正解の場合は 10 ポイント減点となる。さらに、制限時間内に回答しない場合は、20 ポイント減点として、必ず回答させて、ゲームに集中させる環境とした。

（2）仮想ゲーム練習： 実験協力者を各自、消音室に案内し、5 分程度のゲームトレーニングを実施する。実験協力者の画面例を図 3 に示す。練習問題として、明解な回答が無く、チャットと他の参加者の回答状況を通じて、他者の動向を踏まえた対応により正解に近づけることを分からせる。さらに、2 問目の練習問題として、インターネット検索により、正解が分かる問題を準備する。検索サイトとしては、Wikipedia のみがアクセスできるようにフィルタリングした。

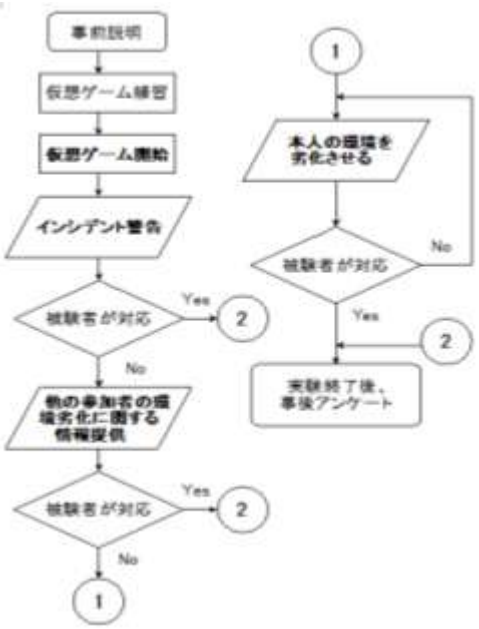

図 2 実験全体のフロー

図 3 実験協力者の画面

（3）仮想実験の開始： ゲームは 1 問あたりの回答可能時間を設定し、カウントダウン表示で時間内の回答を意識させる。1 ゲーム当たりの時間配分は、最初の回答までの考察時間が 1 分、調査及び再回答可能時間が 5 分、正解表示時間が 5 秒とした。調査時間内に、地図上のバルーンをクリックして、最大 10 名まで他者の回答状況をモニターできる。さらにチャットにより、自分が参加しているグループ（メンバー数：5 名）メンバー間での意見交換により正解を予測する環境も準備し、それを考慮して、最初の選択した回答を変更可能とできる構成とした。

（4）ウイルス感染警告： ウイルスに感染の可能性を示す警告メッセージ画面(以降インシデントと呼ぶ、)を表示する。さらに、実験協力者が指定されたボタンをクリックすると、感染状況のチェックを可能とし、その後に、ウイルス感染を明示する。（図 4 参照）さらに、ボット対策専門の駆除を行わせる駆除に必要なファイルを取得するためのボタンをクリックすると、「駆除完了」が出て、実験を終了する。インシデント発生後、30 秒経っても、何も対策を取られなかった場合、30 秒おきにインシデントが繰り返し表示され、それでも何も行動しない場合、実験に参加している他者のＰＣの環境が劣化したことを、チャットにより知らせるようにする。さらに、それでも対策しない場合は、ＰＣの処理速度が遅くなることにより、実験協力者のゲーム環境が悪化するように制御する。

ウイルス感染を知った実験協力者の行動としては、ＰＣ対策をせず、消音室を出て、システム管理者を探す行為が予想される。そこで、実験運用者は、協力者の見えない所で、待機し、もし協力者が出てきた場合は、実験は終了し、別室にて、事後アンケートに進む。

図 4 ウイルス感染を明示する画面

(5) 終了後の事後アンケート：実験協力者個々に、別室に移動後、真の実験目的と内容について打ち明け、実験への理解を求める。また、謝礼金を支払う。実際の報酬は、ポイントに関わらず、一律同額を支払った。

4.3 実験システムと運用

実験システムは、Web サービス用サーバー、ＤＢサーバー、プロキシーサーバー、ワクチンダウンロード（ＶＤ）サーバーから構成される。Web アプリケーションとしては、実験参加者用アプリと、管理者用アプリから成る。ゲーム開始時に実験協力者 PC（クライアント）と監理者用 PC（クライアント）からアクセスされ、Ｗｅｂアプリを各ＰＣ端末にロードする。その際に、ＤＢサーバーに格納されたシナリオデータをＰＣ端末にロードし、以降、実験協力者、管理者用アプリケーションは、そのシナリオに沿った形で進行する。また実験終了時には、ユーザーの回答内容やポイント等をログ情報として取得し、ＤＢに格納する。プロキシーサーバーは、実験協力者が Web 検索を行う場合のフィルタリング機能のために使用する。また、ＶＤサーバーは、ウイルス感染する
インシデントが起きた場合に、ワクチンソフトをダウンロードするためのサーバーであり、ワクチン用ソフトのバイナリーファイルを格納している。

5. 分析と考察

5.1 アンケート調査の結果

一般社会人 2254 名に対して、アンケートを実施した。その分析結果として、以下のような事が分かった。

(1) ボットへの対処行動の意思に最も影響を与えたのは、一般に犯罪心理でも言われているように、「危険認知」ではなく「効果性認知」であった。したがって、対処行動を行うことがどのようにリスク低減につながるのかをユーザーが明確に認識できるような情報を盛り込むことが有効であり、脅威を煽ることは得策でないと思われる。

(2) メディアスキルが高い群は、中心ルートである文章の中身を吟味することによって対処行動の意思決定を行う傾向が高い。

(3) メディアスキルの低い群に対しては、文章の中身を詳細に記載することの効果は低く、他の要因による促進を検討する必要がある。

(4) メディアスキルおよび関与・知識が低い群を対処行動に向かわせるためには、より直感的に、ネットの安心・信頼がわかるように情報提供やリテラシー教育を行う必要がある。

5.2 実験結果

アンケート回答者の中から、ウイルス感染の有無、対策実行意志の有無をパラメータにして、100 名の実験協力者を選定し、2010 年 4 月 17 日から 5 月 29 日までに、1 回当たり 2 名もしくは 3 名の参加者に対する実験を 35 回実施した。図 5 に、その時の実験風景を示す。

図 5 実際の実験風景

表 1 に、実験協力者が実際に行った行動を示す。対策を実施した参加者は 37 名であった。インシデント表示後、すぐに対応した者は 15 名、チャットで他者のネットワーク環境の異常を知らされて対応した者が 6 名、実験協力者自身の環境劣化後に対応した者が 16 名となった。また最後まで、対応しなかった者は 63 名であった。なお、インシデントが出て直ぐに、実験途中で、管理者を探すために消音室から退席した参加者は、対策意志があったと考え、対応者として扱った。

表 1 実験協力者の行動

レベル	被験者行動	ウイルス対策	人数	
1	インシデント情報表示後、すぐに対応。()は実験途中で退席	実行	15(2)	37
2	チャットでネット環境の異常を知らされて対応		6	
3	被験者自身の環境劣化後に対応		16	
4	最後まで対応せず	不実行	63	
合計			100	

5.3 分析結果と考察

(1)アンケート結果と実験結果の関係：

実験におけるウイルス対策対応者と非対応者の比率は、アンケート調査の結果と、ほぼ同じであった。

そこで、アンケートで実行意図があると回答した参加者と、実験での行動との関連を分析した。それぞれの回答と対応行動との比率を、表 2 に示す。アンケートで実行意志があると回答した 35 名のうち、実際に対策行動をとった者は、38.3%であり、残りの 61.7%は対策行動を取らなかった。また逆に、アンケートで実施意思がないと回答した者のうち、65.0%は、行動を取らなかったが、残りの 35.0%は、実施行動をとった。被験者タイプ別に、アンケートでの回答（4 件法）と実験時の対策実行レベルとの二群の代表値の差に関するマンホイットニーのU検定（両側検定）を行った。検定の結果、アンケートでの実行意図と、実験における対策行動とが同じであることを統計的には確認できなかった。

表 2 実行意図と対処行動の比率

	実験	
アンケート	対策行動を取る	対策行動をとらない
実行意図あり	38.30%	61.70%
実行意図なし	35.00%	65.00%

(2)30 パーセントルールの理由：アンケートと実験共に、ウイルス対策対応者と非対応者の比率は、３：７となった。この比率に関しては、災害研究において、一般に観測されるものである[11]。例えば、1980 年、愛知県大府市で起こった化学物質を貯蔵した倉庫の火災において、青酸ガスの発生する恐れが出たために、半径 1 キロ以内の住民に避難指示が出された。その時に実際に避難行動をとった住民は 3 割であった。この傾向は、津波や火山の噴火等での退避行動などにも観測され、７割の人々が、不実行とする経験則が存在すると言われていている。3 割という数値の根拠は不明であるが、自分の身に危険が及ぶような災害時において、かなりの人々が不実行を選択する理由としては、「日常化へのバイアス（Normalcy Bias）」 が働くためと社会心理学では考えられている。人々は警報を受け取ると、その内容を明確にしたり、確認したり、あるいは否定するような付加的情報を獲得しようとする。しかし、ここに非日常的な事態を平常的・日常的なものに歪め、危機到来の予兆を異常事態とは無関係な身近で日常的な事柄に引き付けて解釈する傾向が介在する。このことを、日常化へのバイアスと呼ぶ。このバイアスが働くと、危機に関する情報を幾ら繰り返し流し続けても人々は平常的な解釈を取り続け、警報を信用するまでに至らない。

今回の実験においては、ゲームに参加し、ポイントを稼ぐことに集中している状況が平常状態である。そこに、ウイルス感染というインシデントが発生したとしても、自分なりの意味を付与し、それに自分なりの意義つけをするが、この付与や意義つけの仕方によって、同じ情報でも様々な意味に受け取ることになる。つまり、ウイルス感染という情報自体は共通でも、自身の経験や知識などを基に意味付けし、日常化へ歪めて解釈する傾向があると考えられる。つまり、情報そのものよりも、情報への意味付与や意義づけの仕方が重要であり、今回の実験では、感染対策への意味や意義を感じた実験協力者は、対策をとったし、感じなかった協力者は行動しなかったと考えられる。では、次に、アンケートの結果と実験での対応者との間に統計的な相関が無かった理由について考察する。主な理由は、両者の測定環境の違いにあると考えらえれる。アンケートでは、防護動機理論に基づき、回答者に、まず、脅威文章を読ませ、ウイルス感染への恐怖感を与えた後に回答させた。一方、実験においては、何のバイアスもかけることなく、単なる集合知ゲームへの情報のみを与えて実験データを取得した。この点だけをとっても、環境が大きく違うことがわかる。ただ、一方では、ある特徴を持つ実験協力者は、ウイルス対策行動を取るケースが高かった。特に、インシデントを出すと仮定したサイバークリーンセンターを認識した協力者は、2 名と少なかったが、いずれもインシデント発生後、すぐに対策行動を取った。事後アンケートより、これらの協力者は、いずれもウイルス感染経験があり、さらにウイルス対策を実施することの意義が、何よりも大きいとの判断から、この行動になったことが分かっている。

(3)ウイルス対策実行（可能）者のプロファイル：実験で、対策行動を取った実験協力者の特徴を、各自のアンケート回答内容を基に抽出してみる。今回の場合、サンプルデータが少ないため、通常の統計処理による分析では、誤差が大きくなる可能性がある。そこで、多くの事例を比較検討して、ある程度、一般的な言明を行いたいが、統計分析ができるほど標本数が得られない場合に有効とされる分析法である、「ブール代数分析」[12]を使った。この分析法は、少ないサンプルで使える事以外に、変数間の複雑な相互作用効果を詳細に分析することができ、また多くの事例を一度に比較分析できる長所がある。その反面、分析に用いる独立変数の取り方により結果が大きく左右され、一般の検定が出来ないという、短所もある。そこで、本実験での分析においては、変数の決定プロセスとして、質問項目全体を対象に、ウイルス対策を実施した協力者と、実施しない協力者のアンケート結果の比較で、矛盾発生の有無を確認し、矛盾が出ない範囲で、ウイルス対策行動に影響を及ぼしにくいと考える質問項目を削除する作業を続け、残った質問組み合わせ対する論理式を作成する方法を実施した。詳細については、付録に記す。結果として、①ウイルス対策を実施する人は、インターネットへの信頼とプロバイダーへの信頼に関係なく、メディアスキルが高い。
②インターネットへの信頼とプロバイダーへの信頼を持つ者は、ウイルス駆除の義務を感じている。

③ウイルス駆除の義務を感じ、かつ社会的ジレンマを認知している者は、プロバイダーへの信頼がある。
等の分析結果が得られた。

6. まとめ

アンケートと実験の両方を実施して、ウイルスに感染後の対策行動を実施する方策について検討した。アンケート結果から、効果性認知が、対策を促すための説得には特に有効であることが暗示された。また実験から、実験参加者の日常化へのバイアスにより、対策行動に大きな影響が出ることが明らかになった。さらに対策行動を取る人は、ウイルス感染経験があり、またメディアスキルが高い場合が多く、そのプロファイルとしては、5 節で述べたように、インターネットとプロバイダーへの信頼、さらに社会的ジレンマに関する認知に、相互関係があることが分かった。

社会心理学の手法を用いた情報セキュリティ研究自体が､ほとんどなされておらず、まして実験とアンケートを同時に研究した例は、他に知らない。それだけに、多くの今後の課題が存在する。例えば、脅威を認知させる文章の作成法を明らかにする必要がある。さらに実験とアンケートの実施条件を整合させて、理論と実験の比較が可能となる環境を作る必要があろう。さらに、日常化へのバイアスの壁を破って、対策実行させる手段を具体化する必要がある。

謝辞 最後に、本研究を進めるに際して、社会心理学に関する貴重なアドバイス・コメント頂いた東京大学池田謙一教授、高木大資氏に感謝する。さらに実験に協力した日本大学理工学部数学科の皆さんにも感謝する。なお、本研究は、ＩＰＡの「情報セキュリティと行動科学研究会」と科研費 No.22500234 の支援を受けた。

参考文献

1) http://www.cisco.com/web/JP/product/hs/security/tad/tech/dda_wp.html
2) サイバークリーンセンター活動実績 http://www.ccc.go.jp/report/201009/1009monthly.html
3) 内閣官房・情報セキュリティセンター：セキュアジャパン 2008、2008.6
4) 内田勝也、矢竹清一郎、森貴男、山口健太郎、林華枝：情報セキュリティ心理学の提案、情報処理学会研究報告,CSEC, 2007(16), pp.327-331, 2007.
5) 深田博巳：説得心理学ハンドブック、北大路書房 2004..
6) 小松文子、高木大資、松本勉：情報セキュリティ対策における個人の利得と認知構造に関する実証研究、情報処理学会論文誌,pp.1711-1725,vol.51.9, 2010
7) Petty, R.E., Cacioppo, J.T.,: The elaboration likelihood model of persuasion, in L. Berkowitz(ED.), Advances in experimental social psychology, pp.123-205, vol.19, 1986.
8) Rogers, R.W.,: Cognitive and physiological process in fear appeals and attitudes changer: A revised theory of protection motivation. in J.T. Cacioppo & R.E. Petty (eds), Social psychophysiology , New York, Guiford Press, pp.153-176, 1983 .
9) 島、高木、吉開、沼田、上田、猪俣、小松：情報セキュリティ対策の促進を促す説得コミュニケーションによる態度変容の調査報告、電子情報通信学会 SCIS2011,2F2-1, 2011.
10) アメリカ心理学会「サイコロジストのための倫理綱領および行動規範」、明文社、1996
11) 池田謙一：緊急時の情報処理、東京大学出版会 1997.
12) Ragin, C. C.,: The Comparative Method, University of California Press 1987 ；鹿又信夫（監訳）ミネルヴァ書房。.

付録： ブール代数分析法

ブール代数分析は事例を比較する際に、ある条件が存在するか否かを、複数の二値とする変数のブール演算式の形で表現する。そしてそのブール演算式を縮約して表わす分析法である。実験協力者のうち、ウイルス対策を実施した人 と、実施しなかった人を比較する事例として用いた。実験協力者は、事前にアンケートに回答している。アンケートの質問は 35 個あり、この回答結果を二値変数で表し、分析を行った。
以下に、分析プロセスを示す。
まずウイルス対策を実施した人の回答結果と、ウイルス対策を行わなかった人の回答結果では一致する場合がないことを確認した。

次にウイルス対策の行動に影響を及ぼさない質問項目を取り除いた。その結果として、以下の 8 個の質問の組み合わせで、ウイルス対策を実施した人と実施しなかった人の区別が可能であることがわかった。

[A] Twitter の閲覧や書き込みを行うことができる。
[B] ボットウイルスに感染した場合、ウイルスの駆除手順を実行する責任がある。
[C] 今までにボットウイルスに関する報道を見たり聞いたりしたことがある。
[D] インターネット上の大多数の人がボットウイルスの駆除を行っていない。
[E] 友人集団の仲間の望むように行動する必要はないと思う。
[F] 友人集団の仲間がどう思おうと、私は自分のやり方でものごとを行う。
[G] 技術的な仕組みが整備されているので、インターネット上での情報のやり取りは安全である。
[H] 契約しているインターネットサービスプロバイダは信頼できる。

次に、ウイルス対策を実施した 15 人に対してこの 8 つの質問に関する論理式を作成し縮約を行った。論理式は質問を $A \sim H$ で表わし、条件が存在するものを“ A ”, 条件が存在しないものを“ $\overline{A}$ ”と表現した。R をウイルス対策を実施する行動を表すとして縮約を行った結果、以下の論理式となった。

$$R = \overline{A}BD\overline{E}F\overline{G}\overline{H} + AB\overline{C}D\overline{F}GH + AB\overline{C}D\overline{E}G\overline{H} + \overline{A}B\overline{C}D\overline{E}FH + BCD\overline{E}F\overline{G}H + \overline{A}B\overline{C}D\overline{E}F\overline{G}H + \overline{A}BCDE\overline{F}GH + A\overline{B}CDEFGH$$