社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
SITE2011-30(2011-12)

# コンピュータウィルス感染下における ヒトの意識と行動に関する実験と考察

栗野 俊一† 伊藤 和美† 池田 由季† 吉開 範章†

†日本大学理工学部数学科 〒101-8308 東京都千代田区神田駿河台 1-8-14

E-mail: †kurino@math.cst.nihon-u.ac.jp , csku08020@g.nihon-u.ac.jp ,

csui08011@g.nihon-u.ac.jp , yoshikai.noriaki@nihon-u.ac.jp

**あらまし** DDoS 攻撃に対する新しい情報セキュリティ対策を具体化するために，コンピュータウィルス感染時のヒトの意識に関する研究を行っている. ウィルス感染時における心理状況は, 一種のパニック状態と見なせるが, 現在までに報告された例はない．今回，その対策を検討するための基礎データを収集する目的で，ウィルスに擬似感染させる実験を行い，ヒトの心理と行動の特徴を分析したので報告する.

**キーワード** コンピュータウィルス，DDoS 攻撃，説得心理学，正確確率検定

# Study on Consciousness and Behavior under Computer Virus Infection

Shun-ichi KURINO† Kazumi ITO† Yuki IKEDA† Noriaki YOSHIKAI†

† Nihon University, College of Science & Technology, Department of Mathematics

1-8-14 Surugadai, Chiyoda-ku, Tokyo, 101-8308 Japan

E-mail: †kurino@math.cst.nihon-u.ac.jp,csku08020@g.nihon-u.ac.jp,
csui08011@g.nihon-u.ac.jp,yoshikai.noriaki@nihon-u.ac.jp

**Abstract** We have been researching individual behavior and consciousness under computer virus infection. The situation under virus infection can be considered to be a kind of panic, however, there has been no report. So, we had the experiments to collect the basic data for our research and analyzed. This paper mentions the experimental method and experimental results for individual consciousness and behavior.

**Keyword** Computer Virus, DDoS Attack, Persuasion Psychology, Exact Test

## 1. まえがき

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，集団活動を行う組織にとっては，大きな脅威となっている[1]. 日本国内でいえば, 2011 年 9 月に人事院や内閣府などが管理するホームページが DDoS 攻撃を受け, 最長で 2 時間 20 分の間閲覧不可能となった[2]. DDoS 攻撃に限らず，本田技研工業(2011 年 3 月)，ソニーマーケティング(6 月)，三菱重工業(8 月)などの大企業を狙ったサイバー犯罪も相次いで起きている[3]. 今やサイバー犯罪による収益は 1 兆ドル以上となり麻薬密売による収益を超え，最も収益の上がる違法ビジネスとなっているとの報告もある[4]. それにも関わらず，DDoS 攻撃の中でも，特に大きな問題となっているボット攻撃において，対策事業を行っているサイバークリーンセンター(CCC)が, 感染 PC 保有者にその感染事実を通知しても，その中の 3 割だけしか対策を実施しなかったとの報告がある[5]. このような状況が続く中，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きている[6]. もし，ウィ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となりうる. そこで，説得心理学を基礎にした DDoS 攻撃に対する情報セキュリティ対策について研究を行っている[7]. しかし，コンピュータウィルス感染時のヒトの意識と行動に関する研究の報告は，工学の分野はもとより，心理学においても全く無く，その対策を検討するためにも，基礎データを収集する必要がある事がわかった. そこで，学生を実験協力者とするウィルスに擬似感染させる実験を行い，ヒトの意識と行動に関する基礎データを収集し, 分析を行ったので報告する.

## 2. 従来研究

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，工学的な研究としては，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[8].

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[6]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を想定した質問紙による実証研究の報告がある[9]. この報告では，かなりのヒトが実行意図はあるものの，実際の状況は，CCC の通知に対する対応率に見られるように低く，両者にギャップが存在す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.

## 3. 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. しかし，アンケートのように，回答に恣意性の高い調査方法は，倫理的な内容に関わる質問を行った場合，正直な回答を行うインセンティブを低くする可能性があり，対策意欲を示してもその対策意志と実施実行にはギャップが存在する. その結果，文献[9]に示されるように，アンケート結果と実証データの違いが発生すると考える. 従って，ウィルス感染のような環境において，ヒトの行動自体をアンケートのみで調査することだけでは，正確なデータが得られないと考える[7]. そのため，実際の行動を伴う環境での行動観察実験を行い，対策意志と実施実行に何が影響しているのかを明らかにする必要がある.

## 4. 実験システムと方法

実験全体のフローを図 1 に示す. 実験関係者としては，次の 3 種類が必要となる. なお，実験協力者は，全て学生にお願いした.

(1)実験協力者:実験の対象者.

(2)実験実施者:実験協力者に扮して，協力者の行動の監視や誘導を行う.

(3)説明員:全体の進行役. 実験の説明や実験終了後の対応を行う.

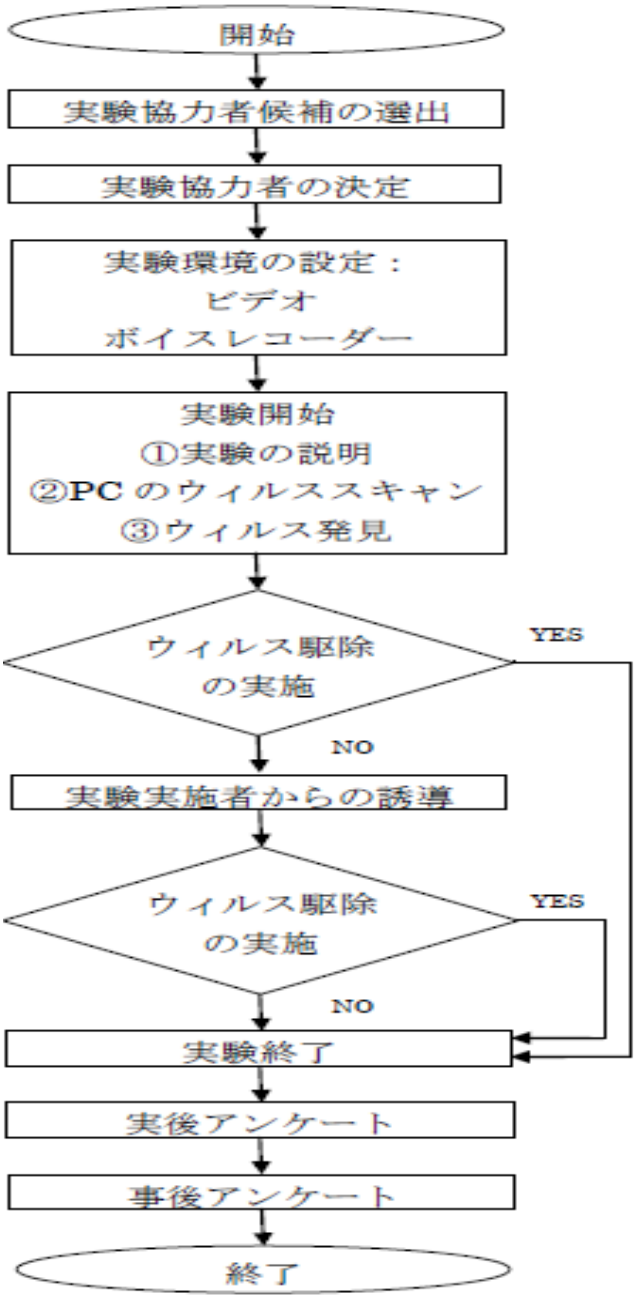


図 1. 実験フロー


図 2. 実験風景

実際の実験風景を図 2 に示す．1 名の実験協力者に 2 名の実験実施者が両サイドに座り，どちらかが，協力者の行動を観察し，もう一方が，極力，協力者との親密な関係を維持しながら，対話により，協力者の心理状況を把握するように行動する．

### 4.1 実験準備

実験協力者を顔見知りの学生の中から，ランダムに選出し，実験参加を交渉する．交渉では，作業内容説明・参加日時（約 2 時間）・謝礼金（２千円相当のカード）の説明を行う．ここで実験協力者には，ウィルスの実験ということはふせ，教材用コンテンツ作りと偽っておく．内容を偽る理由は，ウィルスの実験であることを伝えてしまうと，それを念頭に置いて行動してしまい，実験結果に大きな影響が出てしまうためである．これらの 3 つが了承されれば実験協力者が確定する．実験当日は，実験協力者の行動を観察するために，ビデオやボイスレコーダーの設置を行う．

実験は実験協力者以外にも，同一の実験協力者に扮して一緒に実験を行う実験実施者が必要となる．実験実施者は主に実験協力者の監視や誘導役となっているので，これは，実験を担当した我々が直接担当することにした．

注：ビデオ＆ボイスレコーダーの使用は，事前には断ることなく実施したが，実験後の説明にて，目的を含め全てを説明し，ビデオ等の使用について協力者の同意を得ないものは削除している．

### 4.2 実験実施

実験協力者と実験実施者がそろった時点で説明員が登場し，説明を始める．ここでも真の内容はふせ，教材用コンテンツ作りというアルバイト内容の説明をする．作業内容の説明時には，作業マニュアルを実験協力者および実験実施者に配布し，マニュアル通りに作業を進めるよう指示をする．続いて，実験協力者，実験実施者に，作業のために PC の設定が必要であることを告げ，ウィルス対策ソフトをインストールしているようであれば常駐監視機能をオフにさせる．この際，協力者に疑念を抱かせないために，「作業に必要なソフトがウィルス対策ソフトと相性が悪く，常駐監視機能をオフにしておけなければソフトが使用できない」というアルバイトの特殊条件の説明を行う．作業の説明，および PC の環境設定を終えると，説明員は退出する．ここから協力者に扮した実施者は，協力者と同様に説明員の指示に従いマニュアル通りに作業を開始する．マニュアル通りに作業を進めていくと，CD を用いたウィルススキャンを行う項目にたどり着く．これを指示どおりに進めると実験協力者にはウィルスが検知されてしまい，実験実施者にはウィルスが検知されないという状況になる．ここからの実験協力者の行動を観察する．なお，ウィルス検知時の画面イメージと非検知時の画面イメージは図 3 に示すとおりである．

・ウィルス検知時のポップアップ


・ウィルス非検知時のポップアップ


図３．ウィルス検知時のポップアップ

### 4.3 擬似的なインシデント発生の方法

今回の実験ではテストウィルス[10]を用いてウィルスの擬似感染を行った．このテストウィルスは，本来，使用しているセキュリティソフト・ウィルス対策ソフト・アンチウィルスソフトが，ウィルスを検出した際にどのような警告を表示し対処を促すのか，対策ソフトとして問題なく動くかどうかを確認するためのものである．テストウィルスという名前ではあるが，正確にはウィルスではなく，対策ソフトの開発元が意図的にウィルスと判定するようにウィルスデータベースに登録してあるだけの，何もしない実行ファイルであり，ウィルス的な挙動は一切しない．

インシデント発生手順を以下に述べる．まずウィルススキャンソフト[11]とテストウィルスが入っている CD を，実験協力者が持参した PC に挿入する．持参した PC に常駐監視機能がある対策ソフトをインストールしている場合，そのソフトがテストウィルスに反応

してしまうため，CD の挿入前に常駐監視機能をオフにしておく．CD 内の指定されたファイルを実行すると，ウィルス対策ソフトを起動するだけではなく，同時にテストウィルスが入ったフォルダを PC にコピーする．ただし，実験実施者の PC には前もって同じフォルダ名の空のフォルダを作成しておき，コピーさせないようにしているため，ウィルスが検知されない．

### 4.4 実験終了条件と実後アンケート

実験は実験協力者のウィルス駆除行動の有無で終了する．実験協力者が，実験実施者からの指示や助言を得ずに駆除してしまった場合は，その場で実験終了となる．ウイルス検知のポップアップが出て，時間をおいてもなかなか駆除しなかったり，あるいは，ポップアップを無視して，本来の作業の目的で伝えられている作業用コンテンツ作りを始めようとした場合は，実験実施者からの助言や誘導を行い，駆除の有無を観察した．助言や誘導を受けてもウィルス駆除行動を行わない，あるいは，作業用コンテンツ作りを始めた時点で，その協力者は「対象行動なし」と判定し，実験を終了とする．実験終了後，実験後のアンケート（実後アンケート）を取った後，実験全体が終了となる．実後アンケートでは，以下の項目をインタビュー形式で質問した．

- スキャンによってウィルスが発見された際にどのように感じたか
- ウィルス駆除行動を行った（行わなかった）理由
- ウィルス感染経験の有無
- ウィルスについてどのようなイメージを持っているか
- ウィルスに対する危機感の有無
- ウィルス対策の状況
- 今後本物のウィルスに感染した場合，どのような行動をとるか

## 5. 事後アンケート

実後アンケートとは別に，一定の時間をおいて，改めて，実験協力者に対し，事後アンケートを行った．事後アンケートの内容は，表 1 に示す．アンケートは計 7 問で，ウィルス感染をしたときに対処行動をした協力者は，ウィルスに関する知識や意識，危機感などを持ち合せているという仮説[7]の下，作成されたものである．また，各質問項目の回答が 2 値に分割できるように回答を設定した．

## 6. 分析方法

### 6.1 実験データ

今回の実験データは，実後アンケートのデータおよび事後アンケートのデータの 2 種類がある．実後アンケートはテキスト形式，事後アンケートは数値でのデータとなっている．今回は数値によってウィルス対処行動と関連のあるパラメータを見出すために，事後アンケートのデータを用いて分析を行った．実験協力者および事後アンケート有効回答者の分布を表 2 に示す．実験協力者は総勢 38 人（対象者：大学生，男：23 人，女：15 人）で，ウィルス駆除行動をとったのが 22 人（誘導あり：3 人，誘導なし：19 人），行動なしが 16 人であった．全ての実験協力者に対し，Web アンケー

表1.事後アンケートの設問内容

| 設問No. | 設問の内容 | 回答 |
|---|---|---|
| Q1 | 今回の実験以外で、今までにコンピュータウイル感染したことがありますか？ | 経験あり |
| | | 経験なし |
| Q2 | コンピュータウイルスに対してどのようなイメージちですか？ | 危機感あり |
| | | 危機感なし |
| Q3 | あなたの実験前のコンピュータウィルス対策につ当てはまるものを以下の項目から1つ選択してくい。<br>・実験前に自分の意思で対策していた。<br>・実験前に他人の勧めで対策していた。<br>・実験前はウィルス対策をしていなかった。(未更新・期限切れを含む) | 対策あり |
| | | 対策なし |
| Q4 | 実験をしたことでコンピュータウイルスに対する意変化しましたか？ | 変化あり |
| | | 変化なし |
| Q5 | あなたはコンピュータウィルスがどのように感染かを知っていますか？知っているものを以下の項ら選択してください。(複数選択可)<br>インターネット・サイトの閲覧/Eメール/USB/CD-ファイル共有ソフト/ファイルのダウンロード/マクログラムの実行/何も知らない/その他 | 4種類以上 |
| | | 4種類未満 |
| Q6 | あなたはコンピュータウィルスが感染すると、コンタにどのような影響を及ぼすかを知っていますか下の項目の中から当てはまるものを選択してくだ(複数選択可)<br>画面に異常が発生する/システムが立ち上がらなまたは、起動時に異常な時間を生ずる/ソフトが頻フリーズする/データの破壊・盗用・流出を行う/意ないアクセスを始める/意図しないメールの送信れる/何も知らない/その他 | 4種類以上 |
| | | 4種類未満 |
| Q7 | あなたはコンピュータウィルスを何種類知ってい か？ | 4種類以上 |
| | | 4種類未満 |

表2. 実験協力者と事後アンケート有効回答者の分

(1)実験協力者

| | 対処行動あり | | 対処行動なし | 合計 |
|---|---|---|---|---|
| | 誘導あり | 誘導なし | | |
| 男 | 2 | 10 | 11 | 23 |
| 女 | 1 | 9 | 5 | 15 |
| 合計 | 3 | 19 | 16 | 38 |
| | 22 | | | |

(2)事後アンケート有効回答者

| | 対処行動あり | | 対処行動なし | 合計 |
|---|---|---|---|---|
| | 誘導あり | 誘導なし | | |
| 男 | 0 | 8 | 10 | 18 |
| 女 | 0 | 5 | 4 | 9 |
| 合計 | 0 | 13 | 14 | 27 |
| | 13 | | | |

トを用いた事後アンケートを行った．有効回答が得られたのは 27 人（対処行動あり：13 人，対処行動なし：14 人）であった．

### 6.2 分析手法

対処行動の有無と，事後アンケート各項目間の関連を調べる目的で相関係数を求めた．アンケート各項目の回答を表 1 のように 2 値に分割し，対策の有無との 2×2 分割表を作成した．相関係数の中でも最も単純な係数としてφ係数があげられる．φ係数を求める際にはχ二乗値を必要とするが，今回のデータからカイ二乗値を求めると，一部の期待度数が 5 未満となり，カイ二乗値が歪んでしまう．そこで，ピアソンの積率相関係数を 2×2 の分割表に適用した四分点相関係数を用いた．また有意性の検定には，今回のデータの一部の期待度数が 5 未満であるため，カイ二乗分布を用いた検定は適切ではない[12]．したがって，四分点相関係数での分析の際によく用いられ，2×2 分割表での検定に適しているフィッシャーの Exact 検定（フィッシャーの正確確率検定）を用いた．なお，分析ツールとしては R を用いた[13]．

## 7. 実験結果と分析

事後アンケートの各項目と対処行動の有無との四分点相関係数及び p 値を表 3 に示す．

(1)ウィルス感染経験の有無との相関；協力者のウィルス感染経験の有無について四分点相関係数を求めたところ，弱い相関が表れた($r = 0.34$)．フィッシャーの Exact 検定を行ったところ，有意性はなかった($p > 0.05$)．

(2)ウィルスに対する危機感の有無との相関；協力者がウィルスに対して危機感を持っていたかどうかについて同様に相関係数を求めたところ，強い相関が表れた($r = 0.63$)．有意性の検定を行ったところ，有意的な値を示した($p < 0.01$)．

(3)実験参加時のウィルス対策の有無との相関；協力者が実験参加時にウィルス対策を行っていたかどうかについて同様に相関係数を求めたところ，弱い相関が表れた($r = -0.35$)．有意性の検定では，有意的な値は表れなかった($p > 0.05$)．

(4)実験後のウィルスに対する意識の変化との相関；実験参加後にウィルスに対する意識が変化したかどうかについて相関係数を求めたところ，強い相関が表れた($r = -0.48$)．また検定でも有意的な値が表れた($p < 0.01$)．

(5)ウィルスの感染経路についての知識との相関；ウィルス感染経路と対処行動の有無の間には弱い相関が表れた($r = 0.23$)．しかし，検定では有意性は示せなかった($p > 0.05$)．

(6)ウィルスによる被害についての知識との相関；ウィルスが及ぼす影響についての知識と対処行動との間には，有意性はなかったものの($p > 0.05$)，弱い相関が表れた($r = 0.35$)．

(7)ウィルスの種類についての知識との相関；ウィルスの種類についての知識と対処行動の有無については相関はなかった($r = -0.19$)．検定においても有意性はなかった($p > 0.05$)．

以上をまとめると，相関係数が有意な値を示したのは，「ウィルスに対する危機感の有無（$r = 0.63$, $p < 0.01$）」と，「ウィルスに対する意識の変化($r = -0.48$, $p < 0.01$)」の 2 つの項目であった．つまり，「対処行動を取る協力者は，ウィルスに対する危機感を持ち合せており，実験終了後にウィルスに対する意識の変化が起きていない傾向にある．」，また「対処行動を取らなかった協力者は，ウィルスに対する危機感をあまり持ち合せておらず，実験終了後にウィルスに対する意識に何かしらの変化が出る傾向にある．」という事がわかった．その他の項目においては，検定において有意的な値を示せなかったが「ウィルス感染経験の有無($r = 0.34$)」，「実験前のウィルス対策の有無($r = -0.35$)」，「ウィルスに対する知識（ウィルスが及ぼす影響）($r = 0.35$)」など弱い相関が表れている項目も存在するため，実験の改良やサンプル数の追加などの検討を行う必要がある．対処行動を取らない協力者に対して意識の変化を与えることができるであろうという結果が表れたことから，ウィルスに感染するという経験を擬似体験することの重要性が示唆された．

表3.分析の結果

| 項目 | 相関係数 | p値 |
|---|---|---|
| Q1 ウィルス感染の有無 | 0.34 | 0.12 |
| Q2 ウィルスに対する危機感の有無 | 0.63 | 0.002 (**) |
| Q3 ウィルス対策の有無 | −0.35 | 0.103 |
| Q4 実験後のウィルスに対する意識の変化の有無 | −0.48 | 0.021 (*) |
| Q5 ウィルスに関する知識（感染経路） | 0.23 | 0.385 |
| Q6 ウィルスに関する知識（ウィルスが及ぼす影響） | 0.35 | 0.12 |
| Q7 ウィルスに関する知識（ウィルスの種類） | −0.19 | 0.596 |

(* = p < 0.05, ** = p < 0.01)

## 8. まとめと今後の課題

ウィルス感染状況におけるヒトの心理と行動を実験により調査する方法を提案し,実験データに基づき,ウィルス感染による意識の変化と対処行動の相関関係について分析した．その結果として，ウィルス感染の擬似体験により,ウィルスに対する意識の変化があり,自発的な対策行動を向上させる可能性があることを,実験的に示すことができた．このことを利用して，新しいウィルス対策案を検討する予定である．


### 謝辞

最後に，本研究を進める際して，貴重な意見を頂いた東京大学大学院人文社会系研究科社会心理学研究室・池田謙一教授，高木大資氏に感謝いたします．また，実験の推進及びデータ分析に携わった日本大学大学院理工学研究科数学専攻･飯塚信夫氏,神田大彰氏,及び数学科吉開・栗野ゼミの皆様に感謝いたします．なお，本研究は，科研費 No.22500234 及び日本大学学術研究助成金（総 11-010）の支援を受けて実施した．


## 文　献


[1] 独立行政法人情報処理推進機構セキュリティセンターサービス妨害攻撃の対策等調査―報告書―,
http://www.ipa.go.jp/security/fy22/reports/isec-dos/2010_isec_dos.pdf，2010.

[2] 文芸春秋編 日本の論点 PLUS
http://www.bitway.ne.jp/bunshun/ronten/sample/keyword/110922.html

[3] 日経コミュニケーション，“日本も“サイバー犯罪先進国”に”，2011.10.31
http://itpro.nikkeibp.co.jp/article/COLUMN/20111024/371283/?ST=security

[4] 日経コミュニケーション，“麻薬密売を超えるマーケット”，2011.11.01
http://itpro.nikkeibp.co.jp/article/COLUMN/20111024/371284/?ST=security

[5] サイバークリーンセンター活動実績，https://www.ccc.go.jp/report/201101/1101monthly.html

[6] 内閣官房・情報セキュリティセンター：セキュアジャパン 2008，2006

[7] 吉開範章，栗野俊一，飯塚信夫，神田大彰，高橋俊雄，“集合知ゲームを用いた情報セキュリティ対策への検討”，情報処理学会研究会報告 GN-79，no.7，2011.

[8] 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.

[9] 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

[10] EICAR Test Virus,
http://www.rexswain.com/eicar.html

[11] Clam Win Portable,
http://portableapps.com/apps/utilities/clamwin_portable

[12] 杉山高一，藤越康祝，“統計データ解析入門”，みみずく舎，2009

[13] 大門貴志，吉川俊博，手良向聡，“R による統計解析ハンドブック”，メディカルパブリケーションズ，2010