様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年　5 月　20 日現在

機関番号：34416
研究種目：若手研究(B)
研究期間：2010～2012
課題番号：22730241
研究課題名（和文）
企業と個人の情報セキュリティ対策に関する実証分析
研究課題名（英文）
Empirical Studies on Information Security Measures in Japan
研究代表者
竹村　敏彦（　TAKEMURA TOSHIHIKO　）
関西大学・ソシオネットワーク戦略研究機構・助教
研究者番号：00411504

研究成果の概要（和文）：本研究では、アンケート調査等から得られたデータを分析し、高度情報化時代における安心・安全社会を実現するために必要とされる企業および個人の情報セキュリティ対策はどのようなものかを明らかにした。その結果、リスクへの態度といった心理的要因とともに、情報セキュリティ意識などが情報セキュリティ行動等に影響を与えていることを明らかにし、労働者が情報セキュリティに関わるルール違反をしなくなるような職場環境の整備が必要であることを示唆している。

研究成果の概要（英文）：In this research, we clarified the effective information security measures and policies through the analyses using on micro data collected from our Web-based survey. As a result, we found that the information security behaviors were affected by not only psychological factors such as attitude toward the risk, but also the degree of information security awareness. Finally, we suggested to need the arrangement of workplace environment.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	900,000	270,000	1,170,000
2011 年度	1,000,000	300,000	1,300,000
2012 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	2,900,000	870,000	3,770,000

研究分野：社会科学
科研費の分科・細目：経済学・経済政策
キーワード：情報セキュリティ経済学、Web アンケート（インターネット）調査、リスクマネジメント、情報セキュリティ意識、情報セキュリティ行動、セキュリティインシデント、組織

１．研究開始当初の背景

情報科学の分野において、暗号化技術・自己防衛ネットワークをはじめとする情報セキュリティ技術に関する研究は従来から行われ、その研究蓄積は膨大な量となり、それらの技術を実用化することで一定の成果をあげている。しかしながら、情報セキュリティを経済学の視点からアプローチしている

研究（セキュリティエコノミックス；Economics of Information Security）は2000年頃に本格的に始まったばかりで、国内外ともにその研究蓄積はまだ数少ない。その中でも実証研究は、定性的な研究もしくは小規模なインタビュー調査結果に基づく限定的な定量研究といった状況にとどまっている。このように定量的な研究が行われてこなかった理由として、分析に用いることができる企業等の情報セキュリティ対策に関するデータが存在していなかったこと、また、研究者が情報通信技術のもつ生産性、効率性や企業価値の向上等の正の経済効果にしか注目してこなかったこと、研究対象が情報セキュリティであるために文理融合の研究体制が必要とされること等が挙げられる。特に、データに関しては、先行研究でも指摘されているように、情報セキュリティ対策に関するアンケート調査を実施したとしてもその回収はかなり低いものとなり、分析ができないことが多い。加えて、情報セキュリティ対策の費用対効果の測定が容易ではないことが研究を難しくさせている。そのために、セキュリティエコノミックスにおける実証研究は今なお萌芽状態にあるといえる。

２．研究の目的

本研究の目的は、アンケート調査等から得られたデータを定性的かつ定量的に分析し、高度情報化時代における安心・安全社会を実現するために必要とされる企業および個人の情報セキュリティ対策はどのようなものかを明らかにすることにある。それと同時に、十分な情報セキュリティ対策を実施しなかったことによって生じる経済損失（労働生産性の低下等）額についての試算もあわせて行う。そして、これらの実証研究の結果を踏まえて、有効かつ実現可能な情報セキュリティ対策および政策のグランドデザインを具体的に提示する。

本研究で行う実証分析は、学術的な意義だけでなく、（情報セキュリティに関する政策の一材料となりうることを考えると）実務的にも大きな意義を持っている。

３．研究の方法

本研究では、公表されているデータを用いた分析も行っているが、主要な部分は、本研究を通じて独自に調査を実施し、収集・蓄積した個票データを用いた分析している。

（１）個票データの収集・蓄積－Webアンケート調査の実施－

本研究では、近年注目を浴びている調査手法である Web アンケート（インターネット）形式の調査を2010年度（平成22年度）、2011年度（平成23年度）および2012年度（平成24年度）に計3回実施し、個票データの収集・蓄積を行った。この調査は、2 年以上、同一組織（企業）で働き、調査会社にモニターとして参加している個人（労働者）を対象とし、彼らの情報セキュリティへの意識や情報セキュリティに関する行動を把握するために行ったものである。情報セキュリティ意識、学歴、リスクへの態度や賃金体系、組織属性、企業内で実施されている情報セキュリティ対策に関する状況、情報セキュリティ被害遭遇状況等に関する 60 問以上にもわたる質問で構成された調査票を設計した。

調査に際しては、モニターを利用する Web アンケート調査では、調査対象者への調査票公開時期（曜日・時間）によって、サンプルに偏りが生じるために、雇用形態（正規・非正規）と所属する組織の上場の有無による事前割付を行った（表 1 参照）。なお、調査のサンプルサイズはいずれの年度も 1200（人）と設定した。ただし、実際の調査では不良回答者の除去等を行うために、オーバーサンプルをとっている。不良回答者の除去には、これまで得られた Web アンケート調査の経験・知見等から、回答者の回答時間の長さをはじめとするいくつかの指標を作成・利用した。

表 1: 調査対象者割付　（人）

	上場	非上場
正規雇用	500	500
非正規雇用	100	100

質問項目に関して、2010年度のアンケート調査では、情報セキュリティおよびその対策に対する意識（awareness）と情報セキュリティに関する行動を中心とした質問票を設計し、2011年度の調査では、加えて、情報セキュリティに対する意図（intention）や態度（attitude）、情報セキュリティに関する知識等に関する質問項目を追加した。さらに、2012年度の調査では、職場環境に関する社会心理学で用いられる「属人風土」や組織コミットメント等に関する新たな質問項目を採用した。なお、新たに調査項目を採用したことで、調査項目から外したものもいくつかある。しかしながら、全体的な情報セキュリティ対策等に関する動向を把握できる調査内容となっている。

（２）統計分析

本研究では、主として、収集・蓄積した個票データを用いた統計分析を行った。その際、心理学的要因をモデルに組み込みやすいミクロ経済学や行動科学の理論的フレームワークを採用し、また、統計手法としては、ロジット回帰分析やパネルデータ分析、構造方程式モデリング、Man-Whitney の順位和検定などを用いた。

（３）研究体制・研究協力者からの支援

本研究は、経済学のみならず、情報工学や経営学、法学、社会心理学や政策実務といった様々な観点から遂行される必要がある。そのために、研究協力者からの支援をうけながら小規模研究会の開催や研究成果の外部発信を積極的に行った。

①　小規模研究会の開催

2005 年度（平成 17 年度）から竹村敏彦（研究代表者）が主催している研究会のメンバーや研究協力者、政策実務家等と、アンケート調査の企画・設計に関する綿密な議論をはじめとする研究全般に関する研究会を、大阪および東京にて、研究期間を通じて、20 回程度開催した。

②　研究成果の外部発信

研究成果は、上述したように、学術的な意義だけでなく、実務的にも大きな意義を持っているため、国内外の学会・研究会などで報告し、それを査読付学術雑誌に投稿するだけでなく、竹村敏彦（研究代表者）のホームページを通じて積極的に研究成果に関する情報の外部発信を行った。

また、本研究で収集・蓄積した個票データは、学術的にも実務的にも価値があるものであることを鑑みて、個人や組織を特定化できる情報を除き、学術目的にのみ利用できる体制をとっている。この活動はこの分野の学術発展に寄与するものである。詳しくは竹村敏彦に問い合わせをされたい。

４．研究成果

（１）調査結果から見た情報セキュリティ対策および意識の動向

2010～2012 年度の Web アンケート調査の結果から見た情報セキュリティ対策や個人の意識の変化などについて一部を紹介する。

①　トラブル遭遇被害状況の推移

過去 2 年間で遭遇したコンピュータウイルス・ワーム感染などの情報セキュリティ被害について質問しており、その被害状況の推移は図 1 の通りである（一部抜粋）。

ウイルス・ワーム感染の被害に遭遇している個人の割合は、若干低下傾向にあるものの、他の被害に較べるとまだ高く、不正アクセスやパスワードの盗難・盗聴の被害に遭遇している個人の割合も 1～2%となっている。

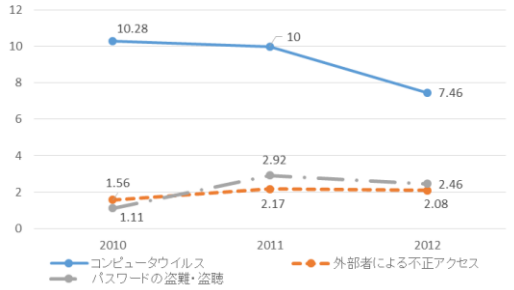

図 1：情報セキュリティ被害の推移

②職場における満足度の推移

職場において仕事、職場、IT 化、情報セキュリティに対する満足度を 10 点満点で評価した結果（平均値）が図 2 の通りである。

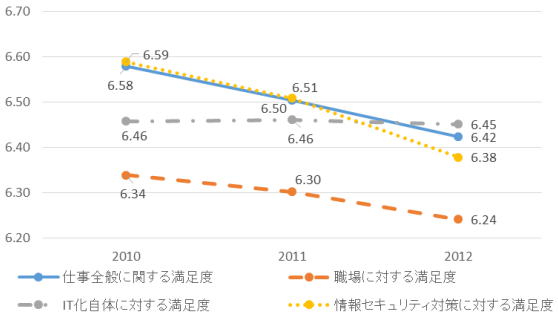

図 2：職場における満足度の推移

IT 化自体に対する満足度は 3 年でほぼ横ばいであるのに対して、それ以外の満足度については低下傾向にあることがわかる。職場に対する満足度は他のものと比較しても、若干低い水準にあり、また情報セキュリティに対する満足度はこの 3 年でもっとも低下が激しいことがわかる。

③対策についての考え・意見の推移

対策についての考え・意見を 1：強くそう思わない～7：強くそう思う、の 7 段階で回答者に評価してもらったものの平均をとったものが図 3 である（一部抜粋）。

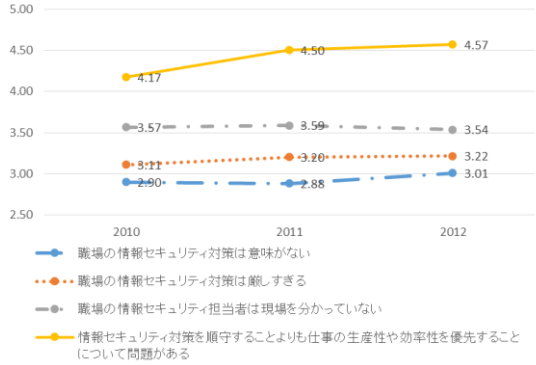

図 3：対策についての考え・意見の推移

図 3 を見てわかるように、企業の情報セキュリティ対策およびその担当者に対して一定の評価を下し、その評価は経年変化を見てもそれほど変化していないことがわかる。また、日常業務の生産性よりも情報セキュリティ対策の遵守が優先されるべきであると認識している個人が若干ながら増加傾向にあることがうかがえる。

（２）企業と労働者の間の情報セキュリティへの意識の違いについての分析

Albrechtsen, E.：A Qualitative Study of Users' Views on Information Security (Computer & Security, 26, 276-289, 2007年) 等において、対策を実施する企業の情報セキュリティ担当者と一般従業員の間には、情報セキュリティ対策に対する意識の違いがあり、この差異により対策の有効性が失われていることが指摘されている。

Takemura, T., et al.: Analysis of Awareness Gap between Security Managers and Workers in an Organization with Regard to the Effectiveness of the Information Security Measures (JIP, 19, 253-262, 2011年)では、2種類のアンケート調査によって収集された個票データを用いて、企業の情報セキュリティ担当者と一般従業員の間に情報セキュリティ対策に対する意識の違いがあるかを検証している。この検証により、情報セキュリティ担当者に対して、より有効となる情報セキュリティ対策に関する情報を提供することができる。

分析では、表2に示した対策を実施したことで実感できる効果（対策に対する肯定度）でもって、対策に対する意識を測っている。

表2: 対策を実施したことで実感できる効果

#	内容
E1	社員の情報セキュリティに対する意識向上
E2	リスク管理の重要性に対する理解・認識の向上
E3	情報資産の見直し
E4	業務プロセスの見直し・修正
E5	社内における情報の共有・活用
E6	企業の社会的責任（CSR）としての自覚
E7	ビジネスパートナーや顧客からの評価
E8	提供する製品やサービスの質の向上
E9	競争力の強化

これらの効果は、1: 全く効果がないと思う～4: とても効果があると思う、の4段階で評価されている。これらの効果は大別すると組織内で実感できるものとそれ以外（市場等）で実感できるものになる。表2のE1～E5は組織内で実感できる効果、E6～E9はそれ以外で実感できる効果をそれぞれ表している。これらの効果の実感の程度について、表3のカテゴリー別に対策を実施している情報セキュリティ担当者（管理者）と従業員の間で違いがあるか否かを、研究代表者（竹村）が2008年11月と2009年3月にそれぞれ実施した2種類のWebアンケート調査の個票データに対して、Bonferroni修正を施したMann-Whitneyの順位和検定を行った。

分析の結果、上場企業と従業員数が1000人以上の企業においては、いずれの効果も管理者と従業員の間で統計的な違いはなかった。また、公共性が高い企業においても一部の効果を除いて両者に統計的な際は確認されなかった。一方で、非上場企業、公共性が高くない企業、従業員数が1000人未満の企業においては、多くの効果について統計的な際が確認された。つまり、これらの企業では、管理者と従業員において効果の実感に違いがあることがわかった。

表3: カテゴリー （人）

カテゴリー	内容	管理者	従業員
上場オプション	上場企業	89	793
	非上場企業	411	707
公共性	高くない	326	915
	高い	174	585
従業員規模	1000人未満	372	817
	1000人以上	128	683

分析結果から、企業規模等によって、管理者と従業員の間に情報セキュリティ対策に対する意識のギャップが生まれやすいことが示唆され、対策は従業員の意見も取り入れる必要性があることを主張している。

（3）情報漏洩につながる行動に影響を与える要因の探索

多くの企業では、情報漏洩に関するセキュリティ事故や被害を防止するために様々な対策が講じられている。例えば、USBなどの媒体によるデータの持ち出しを、情報セキュリティ技術を導入することにより禁止している企業は少なくない。一方で、技術を導入せずに、情報セキュリティポリシーや社内ルールを策定することにより、対策を講じている企業も存在している。前者の場合はある種強制的に採択を実施することが可能であるが、後者の場合は例えルールが確立していたとしても、それを守らない従業員も少なからず存在しており、対策の効果が低下するだけでなく、組織全体の情報セキュリティ水準の低下にも繋がることが指摘されている。時として、日常の業務を遂行するために、ルールに従わないことが深刻な問題ではないという誤った判断が最悪の場合、情報漏洩を引き起こしてしまうことがある.

竹村・小松「情報漏洩に関わる行動に影響を与える要因の探索」(Proc. of SCIS2012, 2012年）では、情報漏洩につながる行動を取り上げ、ルール策定の有効性、リスク認知や情報セキュリティ意識の向上、管理者への評価などとの関係について検証を行っている。これらの関係を明らかにすることで、情報漏洩に関わる行動を組織のメンバーにとらせない施策について議論ができる。

個人の情報漏洩につながる行動メカニズムを解明するために、構造方程式モデリング（SEM; Structural Equation Modeling）のフレームワークを用いた。図4はキーとなる要因のいくつかを組み込んだモデルを示している。この背景にある理論として、計画的行動理論（TPB; Theory of Planned Behavior）や不正のトライアングル（fraud triangle）などがある。

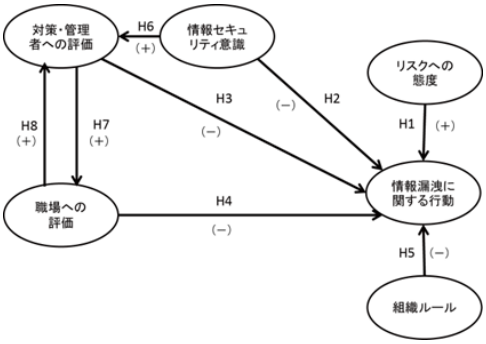

図 4: 基本モデル

なお、情報漏洩につながる行動（1: ポータブルディバイスによる顧客情報の持ち出し、2: 顧客情報の電子メールへの添付、3: 仕事と関係の無いウェブサイトへのアクセス、4: 職場の電子メールの私的電子メールへの転送、5: 自宅で利用しているソフトウェアのインストール、6: 会社のノートパソコンの社外持ち出し、7: 職場の LAN への持ち込みパソコンの接続）を取り上げた。

分析の結果、モデルの当てはまりのよさを表す指標の 1 つである GFI はいずれの行動においても 0.9 を下回ることはないが、必ずしも高い値となっているとは言いがたい。しかしながら、総じていずれの行動についても当てはまりのよいモデルであると判断できる。

仮説 H5 と仮説 H7 はいずれの行動において支持されたものの、仮説 H4 と仮説 H8 はいずれの行動においても支持されなかった。つまり、これらの結果から、共通して，情報漏洩に関わる行動を防止・抑止するためには組織内でその行動を禁止するルール化を進めることが最も有効かつ効果的であることと同時に、職場満足度は直接，情報漏洩に関わる行動に影響を与えていないことがわかった。それ以外の仮説については、行動によって支持されたり、そうでなかったりという結果となった。仮説 H2 は多くの行動で支持され、直接的だけでなく、(他の要因を介して）間接的にも情報セキュリティ意識の向上が情報漏洩に関わる行動を防止・抑止するためには有効となる一方で、仮説 H3 に関して、多くの行動で支持されるものでなく、管理者への不満が即座に情報漏洩に関わる行動につながらないことがわかった。

（4）違反行為に関する分析

基本的には、多くの企業で情報漏洩につながる表 4 に示した行動（1: ポータブルディバイスによる顧客情報の持ち出し、2: 顧客情報の電子メールへの添付、3: 仕事と関係の無いウェブサイトへのアクセス、4: 職場の電子メールの私的電子メールへの転送、5: 自宅で利用しているソフトウェアのインストール、6: 会社のノートパソコンの社外持ち出し）はルール等によって、禁止されていることが多い。表 4 を見てわかるように、企業のルールとして存在しているにもかかわらず、そのルールを違反している従業員が少なからずいる。この事実は、情報セキュリティ対策においては由々しき問題である。

表 4: 情報漏洩につながる行動の経験とルールの有無 （人）

		経験あり	経験なし
行動 1	全面禁止	102	685
	禁止でない	103	160
行動 2	全面禁止	55	662
	禁止でない	93	202
行動 3	全面禁止	56	918
	禁止でない	165	181
行動 4	全面禁止	80	578
	禁止でない	278	237
行動 5	全面禁止	54	854
	禁止でない	120	180
行動 6	全面禁止	38	501
	禁止でない	126	162

Takemura, T., Komatsu, A.：Who Sometimes Violates the Rule of the Organizations?: Empirical Study on Information Security Behaviors and Awareness (WEIS2012, 2012 年)では、これらのルール違反のメカニズムをロジットモデルを用いて分析している。非説明変数としては、各講堂の経験の有無、説明変数としては、態度（リスク回避度や未来結果熟慮）、行動への動機付け、情報セキュリティ意識、職場環境（職場満足度や企業規模など）を用いている。なお、組織のルールにより、行動が全面禁止されている企業に属している回答者が分析の対象である。

分析の結果、近視眼的認知と遠視眼的認知が多くの違反行為に影響を与えていること、情報セキュリティ意識が高い人ほど、ルール違反をしない傾向にあることなどが確認された。また、企業規模や職場満足度などは違反行為と関係ないことも確認された。

（5）セキュリティインシデント等による被害額の試算

電子メールは日常業務の円滑化を図る上で便利であるが、一方で迷惑メールを処理するために時間浪費を余儀なくされる。フィルタリングソフトを用いたとしても、この技術は必ずしも完璧ではなく、取引相手からのメールを誤って迷惑メールとして認識してしまうこともあり、少なからず手動で迷惑メールを処理する必要がある。この認識の下、迷惑メールを処理（削除）するために用いられている労働時間がどの程度の国内総生産（GDP）水準を低下させるのかといった経済的損失額を経済学的フレームワークによって試算した。2001 年から 2010 年における各産業の GDP、資本ストックと労働力で構成されるデータによるパネルデータ分析を行い、セミマクロの生産関数の各係数パラメータ

を推計した。なお、データの加工方法については、内閣府経済社会総合研究所「最新の固定資本マトリクスを用いた IT 関連データの構築およびそれにもとづく IT 投資の日本経済に及ぼす影響の分析」（研究会報告書等 No.55、2011 年の第 3 章）を参考にした。竹村敏彦が 2009 年度に実施した調査データから迷惑メール処理時間等を計算し、推計された係数パラメータを用いた生産関数とリンクさせることで、産業別の経済損失額を試算したところ、産業により被害の大きさに差異があることを確認した。

十分な迷惑メール対策が施されなければ、この労働損失および GDP 損失は増加することになり、技術的対応や法整備に加えて、これらを低減させるための対策について早急に考える必要があることが示唆された。また、この一連の迷惑メールによる経済損失の試算方法は、情報処理推進機構の「情報セキュリティ被害と対策に関する委員会」（委員長：田中秀幸（東京大学））の中で検討されたコンピュータウイルス被害推計モデルの基礎となり、更なる分析が進められている。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 10 件）

① Komatsu, A., Takagi, D., Takemura, T.: Human Aspects of Information Security: An Empirical Study of Intentional versus Actual Behavior. Information Management and Computer Security, 査読有, Vol.21(1), 2013, 5-15
DOI: 10.1108/09685221311314383

② Takemura, T., Tanaka, H., Matsuura, K.: Analysis of Awareness Gap between Security Managers and Workers in an Organization with Regard to the Effectiveness of the Information Security Measures. Journal of Information Processing, 査読有, Vol.19, 2011, 253-262
DOI: http://dx.doi.org/10.2197/ipsjjip.19.253

③ 竹村敏彦・高田義久・小林徹: 日本の ISP の情報セキュリティ対策に関する実証分析, 経済政策ジャーナル, 査読有, 第 8 巻第 2 号, 2011 年, 55-58

④ Takemura, T.: Statistical Analysis on Relation between Workers' Information Security Awareness and the Behaviors in Japan. Journal of Management Policy and Practice, 査読有, Vol.12(3), 2011, 27-36
http://www.na-businesspress.com/JMPP/takemura_abstract.html

⑤ 竹村敏彦: Web アンケート調査データを用いた情報セキュリティ教育に対する意識と行動に関する分析, 情報通信政策レビュー, 査読有, 創刊号, 2010 年, 35-46
http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/01/takemura2010.pdf

〔学会発表〕（計 12 件）

① Takemura, T., Komatsu, A.: Who Sometimes Violates the Rule of the Organizations?: Empirical Study on Information Security Behaviors and Awareness. WEIS 2012, Germany, 26th June, 2012

② Komatsu, A., Takagi, D., Takemura, T.: Human Aspects of Information Security: An Empirical Study of Intentional versus Actual Behavior. HAISA 2012, Greece, 7th June, 2012

③ 竹村敏彦・小松文子「情報漏洩に関わる行動に影響を与える要因の探索」2012 年暗号と情報セキュリティシンポジウム（SCIS2012）, 金沢エクセルホテル東急, 2012 年 1 月 31 日

④ Takemura, T., Empirical Analysis of Behavior on Information Security. The 4th IEEE International Conference on Cyber, Physical and Social Computing, China, 21th October, 2011

⑤ Takemura, T., Tanaka, H., Matsuura, K.: Awareness Gaps on Effects of Information Security Countermeasure between Managers and Employees: An Empirical Study Using Micro Data Collected from Web-Based Survey. 4th IFIP WG 11.11 International Conference on Trust Management, Japan, 17th June, 2010

〔図書〕（計 1 件）

① Takemura, T., Komatsu, A.: An Empirical Analysis on Information Security Behaviors and Awareness. In: Bohme, R. (edt), Economics of Information Security and Privacy. Springer, Chapter 5, 近刊, 2013

６．研究組織

(1)研究代表者

竹村　敏彦（TAKEMURA TOSHIHIKO）
関西大学・ソシオネットワーク戦略研究機構・助教
研究者番号：00411504