情報処理学会論文誌 Vol. 50 No. 9 2193–2206 (Sep. 2009)

推薦論文

企業の情報セキュリティ対策における モチベーションの構造に関する考察

菅野泰子[†1,†2] 寺田真敏[†1,†2] 山田安秀[†2]
鎌倉稔成[†1] 土居範久[†1]

情報化が進んだ今日，情報セキュリティ対策は必須である．これまで情報セキュリティに関して多くの研究がなされてきたが，情報セキュリティ対策を実施する主体の意識や行動に関しては，その解明が進んでいない．情報セキュリティ対策のモチベーションにかかわる諸要因を把握し，その構造を明らかにすることにより，情報セキュリティ対策の推進に寄与できる．本論文では，情報セキュリティ対策を進める動機となる要因（動機要因）や対策の実施を阻害する要因（阻害要因）を把握するための調査結果から，情報セキュリティ対策のモチベーション因子を示す．次に 516 名の回答データと探索的因子分析から，要因の特徴を抽出した後，因子の構造について構造方程式モデリング（SEM）を用いた妥当性の検証について述べる．調査ならびに検証の結果，動機要因として計 6 因子を，阻害要因として計 4 因子を抽出するとともに，これらの要因から構成される情報セキュリティ対策におけるモチベーションの構造を明らかにした．

Some Thoughts Concerning Structural Model of the Motivation for Information Security in Enterprises

Yasuko Kanno,[†1,†2] Masato Terada,[†1,†2]
Yasuhide Yamada,[†2] Toshinari Kamakura[†1]
and Norihisa Doi[†1]

Various studies have been conducted on information security. However, the motivation factors and it's structure for implementing information security measures have yet to be clarified. Understanding motivation factors and clarifying the structures of those factors helps to promote information security measures. In this study, we conducted a questionnaire survey about drives and disincentives that affect the implementation of information security measures. Using the answers from the 516 respondents, we conducted exploratory factor analysis. The result showed factors of the motivation for information security, including six drives and four disincentives. We also verified the validity of the structural model of those factors using structural equation modeling (SEM) and came up with a motivation structure concerning information security measures.

1. はじめに

情報化が進んだ今日，企業は，事業目標達成において情報システムに多くを依存しており，情報セキュリティの確保が喫緊の課題となっている．しかし，情報セキュリティ対策が進んでいない組織も多い．

ISO/IEC 27002:2005 [1] の定義によれば，情報セキュリティとは「情報の機密性，完全性及び可用性を維持すること」である．だが，企業が情報セキュリティ対策を推進する動機や目的は，情報の機密性，完全性，可用性の維持だけにとどまらない．企業は社会の中に存在する以上，社会の中で，その存在価値を追求する．よって，企業の社会的存在価値と結びつけて情報セキュリティ対策の動機や目的を考える必要がある．

心理学の分野では，モチベーション理論は，「ひとに行動を惹き起こさせるエネルギー源はなんであり，それはどのように駆動していくのか」という質問に答えるものである[2]．そして，企業の情報セキュリティ対策におけるモチベーションの研究目的は，「企業が情報セキュリティ行動を起こすエネルギー源はなんであり，それはどのように駆動していくのか」という問いに答えることであり，その際，情報セキュリティ対策のモチベーションにかかわる諸要因やその構造の解明は，基本的な知見となる．

これまで情報セキュリティ技術や情報セキュリティマネジメントに関して多くの研究がなされてきた．しかし，情報セキュリティ対策を実施する主体の意識や行動に関しては，その解明が進んでいない．情報セキュリティ対策におけるモチベーションにかかわる諸要因を把握し，諸要因がどのように関係しているかという，モチベーションの構造を明らかにするこ

†1 中央大学
Chuo University
†2 独立行政法人情報処理推進機構（IPA）セキュリティセンター
IT Security Center, Information-Technology Promotion Agency, Japan
本論文の内容は 2008 年 10 月のコンピュータセキュリティシンポジウム 2008 にて報告され，同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

© 2009 Information Processing Society of Japan

とができれば，対策実施主体のニーズに合った施策を打つことも可能であろうし，対策実施側もより合理的な対策や行動をとることができる．

本論文では，企業の情報セキュリティ対策を推進する当事者を「経営層」と「情報セキュリティ責任者・担当者」に分類し，二者の意識と行動に焦点をあて，企業の情報セキュリティ対策におけるモチベーションを構成する諸要因を把握し，その構造を明らかにする．

2 章では，モチベーション理論と先行研究の調査に基づき，解決したい課題について述べる．3 章では文献調査とインタビュー調査により探索した情報セキュリティ対策におけるモチベーションを構成する諸要因を示す．4 章では，質問紙調査結果の分析により抽出したモチベーションの構成概念と，その構造についての仮説を提示する．5 章では構造方程式モデリング（SEM）により仮説の検証と考察を行い，6 章でまとめを行う．

2. モチベーションと解決したい課題

本章では，本論文で適用するモチベーション理論について示した後，情報セキュリティ対策におけるモチベーションの先行研究と解決したい課題について述べる．

2.1 モチベーション理論と本論文への適用

心理学において，モチベーション（motivation）とは動機づけのことである．新・心理学の基礎知識[3] では，「一般に，生活体を行動に駆り立てる内部的な力を動機（motive）あるいは動因（drive），要求（need），外部的な力を誘因（incentive）と呼ぶ．そして動機をもとにして，行動を起こし（行動の生起機能），一定の目標に生活体を導き，満足が得られるまで行動を持続させる一連の過程を動機づけ（motivation）と呼ぶ」としている．動機づけは，知覚，学習と並んで心理学理論の主たる研究領域であり[4]，古来多くの研究がなされてきた．動機づけ研究の対象とする範囲は広く，アプローチも多様で，認知論的アプローチ（期待理論，期待価値理論，目標理論，達成理論），情動論的アプローチ（フロー理論，リバーサル理論），欲求論的アプローチ（Maslow の欲求階層論，Deci の自己決定理論）などがある[5]．金井は，働くという人間の行動に焦点をあてたワーク・モチベーション理論の構築においては，モデルの精緻化は目的ではなく，実践家にとって，役に立てば単純なほどよい，としている[6]．

本研究では，ワーク・モチベーション理論で多用されてきた V.H. Vroom の期待理論に着目する．Vroom が定式化したモチベーションのモデルは，式 (1) によって表される．

$$F_i = f_i\left(\sum_{j=1}^{n}(E_{ij} \times V_j)\right) \qquad (i = n+1, \ldots, m) \tag{1}$$

ここで，F_i は行為 i を遂行するように作用する力（モチベーション）であり，E_{ij} は行為 i が結果 j をもたらす期待の強度（行為が望まれる結果を導くだろうという成功の主観的確率）であり，V_j は結果 j の誘意性（結果のもたらすものがどの程度魅力的か）を表す．

この理論においては，導かれる結果の価値が高く，成功の主観的確率（期待）が高いほど動機づけは高くなると予想される[7]．

本論文では，情報セキュリティ対策におけるモチベーションが期待理論に沿うと仮定し，結果の誘意性に対して，情報セキュリティ対策を行うことによってもたらされる価値の認識（以下動機要因という）をあてはめる．また，期待の強度は，対策遂行の可能性を表し，対策の実施を阻む要因（以下阻害要因という）の逆数とする．

情報セキュリティ対策の必要性とそれによりもたらされる価値を認識していたとしても，予算がとれない，経営者の理解がないなどで，対策意欲がそがれることがある．つまり，動機要因が高く阻害要因が低いほど，情報セキュリティ対策のモチベーションは高くなると考える．

2.2 先行研究と解決したい課題

情報セキュリティ対策におけるモチベーションの研究は少ない．国内においては，情報セキュリティに心理学を応用した研究が若干見られるだけである．日景らは，安心感の構造に関する研究を行い[8),9)]，内田らは，情報セキュリティに関して，心理学的側面からの研究を行うことを提案し，これまでの情報セキュリティ心理学的研究について概観している[10]．

海外においては，Higgins のモチベーション理論 regulatory focus theory にあてはめ，情報セキュリティポリシ策定者が従業者の行動をどのように想定しているかを分析した Marcinkowski らの研究[11] や，内部者セキュリティ違反行為の抑止を罰あるいは倫理教育によるべきかについて，個人のモチベーション要因を考慮すべきであるとする Workman らの研究[12] がある．しかし，これらは，情報セキュリティルールをいかに守らせるかという課題に対し，従業者のモチベーションを考慮した研究であり，情報セキュリティ対策を推進する当事者のモチベーションに関する研究ではない．国内，海外とも，筆者の調査した限りでは，組織の情報セキュリティ対策を推進する当事者に焦点をあてたモチベーションの研究はまだ行われていない．

情報セキュリティ対策のモチベーションを構成する諸要因は不明瞭であり，その構造も解明されていない．情報セキュリティ対策におけるモチベーションにかかわる動機要因や阻害要因を把握し，それらがどのように関係しているかという，モチベーションの構造を明らかにすることができれば，情報セキュリティ対策の推進を具体的に支援できる．そこで本論文

© 2009 Information Processing Society of Japan

では，これら諸要因とその構造を明らかにし，対策の推進という観点からモチベーションの構造について考察する．

3. モチベーション要因の探索

本章では，文献調査とインタビュー調査を通じてモチベーションを構成する諸要因について検討した結果について述べる．

3.1 文献調査によるモチベーション要因の探索

文献調査においては，マイクロ–マクロ関係を念頭において文献 13)–20) を調査した．マイクロ–マクロ関係とは，人の心理や行動（マイクロ）と社会（マクロ）が互いに影響しあう関係のことであり，社会心理学では重要なテーマである[21]．文献 13)–16) の報告書は，企業において情報セキュリティ対策を実施する主体の意識や行動に焦点があてられているので，マイクロ的視点からの調査対象とした．文献 17)–20) の提言や戦略については，社会的視点，つまりマクロ的視点から調査対象となる．

(1) マイクロ的視点からの動機要因と阻害要因の抽出

マイクロ的視点の文献調査からは，モチベーション構造に直接関係する動機要因と阻害要因を抽出した．文献 13)–16) に関しては，情報セキュリティに取り組む目的や方針，情報セキュリティ対策を実施したことによる効果，対策を実施する際の問題点や困難に感じていることなどを抽出し，動機要因と阻害要因に分類した．分類の結果，リスク管理，個人情報保護，社会的責任（CSR: Corporate Social Responsibility），取引先の要求，法令順守，事故防止，事業継続，競争力向上，組織・体制の整備を動機要因として抽出した．阻害要因としては，コスト，費用対効果不明，手間・効率，トップや従業員の理解のなさ，技術・知識不足，人材不足を抽出した．

(2) マクロ的視点からのモチベーションの基本的要素の抽出

マクロ的視点の文献調査からモチベーション構造全体に影響する基本的要素を抽出した．モチベーション構造全体に影響する基本的要素は大局的視野で対策の推進を考えるときに重要である．文献 17)–20) に関しては，これらの提言や戦略から，情報セキュリティ対策のモチベーションにとって重要な基本的要素を抽出する．文献 17)–20) に共通するのは「IT が経済社会システムに融合化していくなか，情報セキュリティの従来の定義（機密性，完全性，可用性）には含まれない領域，たとえば，法令順守の観点，企業経営・戦略の観点，事業継続などの観点との関連性が徐々に拡大・深化していく可能性」の認識であり，共通して重要な視点は，「情報セキュリティの取り組みにより社会的責任を果たす」こと，「情報セキュリティを経営戦略の中に位置づける」ことの 2 点である．よって，これらの文献より，「（機密性，完全性，可用性の維持を目的とする）情報セキュリティ」，「社会的責任」，「経営戦略」という情報セキュリティ推進の大きな枠組みを考えることができる．ここで「経営戦略」とは，文献 19)，20) により，具体的には，「競争力強化の視点から企業が戦略的に情報セキュリティ対策を実施」することであり，「経済性」といい換えることができる．

なお，文献 17)–20) では環境活動について言及している．たとえば，文献 17) は「環境にやさしい企業が市場で評価されるメカニズム」について，文献 18) は，「情報セキュリティが環境問題のような『社会運動』として認知されることの重要性」について言及し，文献 19) は，「情報セキュリティ問題は，環境問題同様，グローバルな展開が不可欠」としている．

文献 20) では，Porter の「『戦略的 CSR』を推し進めることで，新たな競争優位を築く」[22] という提言を紹介している．Porter は，1991 年に，“America’s Green Strategy” という論文を発表し，適切な環境規制は技術開発を促進し，競争優位をもたらすと主張した（これはポーター仮説と呼ばれる）[23]．

従来，環境への取り組みは，経済的価値を生まないと考えられ，その費用は，社会全体に押しつけられてきた．Shmidheiney は，社会全体に押しつけられていた環境対策費用を内部化（企業などの経済活動の主体が負担）するメカニズムを提案している[24]．金原らは，「環境パフォーマンスを高めようとすれば，競争力が失われるという通説に対し，ポーターの功績は，環境への取り組みが経済効率と両立する可能性を示した点にある」（趣意）[25] としている．

環境への取り組みにおいて，社会的責任もまた重要な要素である．2000 年 6 月に GRI（Global Reporting Initiative）が持続可能性報告書ガイドラインを策定し，企業に対し，環境，経済，社会的側面について報告することを求め[26]，同年 10 月には，WBCSD（持続可能な発展のための世界経済人会議）が，GRI のガイドラインで求められた環境，経済，社会についての報告は個別ではなく相互に関連すべきであると述べている[27]．環境性，経済性，社会性は，トリプルボトムラインと呼ばれ，企業のパフォーマンスを評価する 3 つの基準となっている．金原らは，「社会性は，社会の中に存在しその機能を果たすという意味では，社会的責任のある行動の意味がある」とし，広義の社会的責任を環境性，経済性の上位に位置づけている[25]．

環境対策の推進において対策費用は利益を生まないと考えられていたこと，また，社会的責任が推進要因の 1 つとなっていることから，環境対策と情報セキュリティ対策のモチベーションには，経済性と社会性において共通する点が多いと考えられる．

マクロ的視点の文献調査より，情報セキュリティ対策のモチベーションにおける基本的要

© 2009 Information Processing Society of Japan

表 1　情報セキュリティ対策実施の動機要因となる項目
Table 1　List of motivation factors – drives.

社会的要求にかかわるもの	
外部の要求	法令順守，業界標準の順守，取引先の要求，調達要件
ステークホルダーの要求	株主や顧客の期待・要求・評価・信頼感，社会的責任
競争優位	企業価値向上，競争力強化，他社に遅れない，自社の取り組みのアピール
事業継続	業務継続，事業継続，セキュリティ事故の未然防止，事故の再発防止，他
組織内の要求にかかわるもの	
組織・体制	経営層の理解，リソースの割当，担当者への評価，ポリシーや体制の整備，他
管理品質（リスク管理と効率化）	情報の管理，営業秘密や技術情報・個人情報の保護，内部犯行の防止，脅威や脆弱性への対応，セキュリティリスクへの対応，他
インセンティブ	税制面での優遇

注：事業継続は，組織内要求の側面もあるが，ここでは社会的要求の側面を重視し，社会的要求に分類する．

表 2　情報セキュリティ対策実施の阻害要因となる項目
Table 2　List of motivation factors – disincentives.

組織内における阻害要因	
経営層・体制	経営層の無理解や無関心，組織体制やルールの未整備，責任の所在の曖昧さ
コスト	対策予算獲得の困難さ，コスト的余裕のなさ，適正コストの判断の難しさ
技術・ノウハウ	対策実施の技術・ノウハウ不足，対策の優先順位づけが困難，他
人材	対策を実施できる人材の不足，人員の割当なし，他業務の兼務，相談できる専門家の不在.
評価・効果	対策実施の効果が不透明，対策に対する取引先や顧客の評価の低さ，対策実施部門への社内評価の低さ
理解・協力	教育の全員履修の困難，社内へセキュリティを浸透させる難しさ，従業員へのルール順守徹底の困難さ，監視への反発
手間・作業効率	対策実施にかかる手間ひま，時間の大きさ，作業負荷の大きさ，業務効率の低下，他

素として，情報セキュリティ，経済，社会の 3 つを抽出した．対策の推進において，この 3 つの基本的要素は重要であり，これに関し，5.2 節でマクロ的視点から考察する．

3.2　インタビュー調査

文献調査により得た知見をもとに，4.1 節の質問紙調査で使う質問紙のドラフトを作成し，このドラフトをもとに，インタビュー調査を実施した．インタビュー調査は質問紙調査を行う前の予備調査であり，その目的は質問紙尺度の精度を上げることである．

(1)　調査目的

情報セキュリティ対策のモチベーションにかかわる要因や構造を調査するための質問紙の作成．

(2)　調査方法

(a)　調査日時：2008 年 5 月 15 日～2008 年 6 月 17 日

(b)　調査手続：被験者に個別に面談を求め，実際に質問紙に答えてもらうとともに，ドラフトに記載のモチベーションの要因以外に考えられる要因，またモチベーションの構造についてフリーディスカッションを行いながら，ドラフトの改善を行った．なお，調査対象 22 名のうち 3 名には，ドラフトを改善するたびに回答をお願いし，答えやすさなど，改善の度合いを確認した．

(c)　被験者：情報セキュリティ専門家 16 名，大学教員 3 名，システム監査専門家 1 名，SE 1 名，学生 1 名．計 22 名

(3)　調査結果

情報セキュリティ対策にかかわる動機要因として 31 項目を，阻害要因として 30 項目を抽出し，これらを 4.1 節の質問紙調査で使う質問項目として質問紙を完成させた．抽出した動機要因，阻害要因を，類似のカテゴリにまとめて整理したものを**表 1** と**表 2** に示す．

4.　モチベーションの構成概念の抽出

本章では，質問紙調査結果の分析から得られたモチベーションの構成概念を示すとともに，それらの関係性について仮説を述べる．

© 2009 Information Processing Society of Japan

4.1　質問紙調査

(1)　調査目的

情報セキュリティ対策のモチベーションの構成概念（潜在因子）探索のためのデータの取得.

(2)　調査方法

(a)　調査日時：2008 年 6 月 20 日〜2008 年 7 月 31 日

(b)　調査手続：IPA の情報セキュリティセミナ[⋆1]と筆者が講師を務めるセキュリティ関連のセミナなど，計 10 セミナの受講者全員に調査用紙を配布し，セミナ終了後にその場で回収した.

(c)　調査内容：前章で検討した情報セキュリティ対策の動機要因計 31 項目について，非常に強い動機となる（7 点）〜まったく動機とならない（1 点），阻害要因計 30 項目について，克服するのが非常に難しい（7 点）〜まったく難しくない（1 点）のそれぞれ 7 段階で評定を求めた．阻害要因の状況設定としては，これらの要因によって対策の実施が阻まれている状況を想定して，自組織では，これら状況の克服が難しいかどうかをたずねた．実際の質問紙で示した説明文と質問項目を付録 A，B に示す.

(d)　被験者：IPA の情報セキュリティセミナやセキュリティ関連セミナの受講者．受講者数はセミナにより，30 名から 200 名程度までの幅があり，組織の情報セキュリティ対策の責任者や担当者が全体の 3 分の 2 程度を占める.

(3)　調査結果

セミナ受講者数 1,036 名，全回収数 898 件（回収率 86.7%）のうち，記入漏れなどの無効票を除いた有効票は 784 件であった．有効票の内訳は**表 3** のとおりである．なお，本調査の分析については，4.2 節で述べる.

4.2　探索的因子分析

本節では，質問紙調査結果をもとに探索的因子分析により行った，モチベーションの構成概念の抽出について述べる．探索的因子分析は，データを縮小する方法として用いられる．分析が成功した場合は，多くの観測変数から直接観測できない構成概念をみつけることができ，この構成概念を「潜在因子」と考える[28),29)].

(1)　分析目的

モチベーションの構成概念の抽出

⋆1 http://www.ipa.go.jp/security/event/2008/isec-semi/kaisai.html

表 3　回収状況
Table 3　Number of questionnaires collected.

職種	有効回答数
組織の情報セキュリティ責任者・担当者	474
情報セキュリティ専門家	100
経営者・部門長	42
情報や情報システムの利用者	93
その他	75
計	784

(2)　分析対象

4.1 節の調査で回収した有効票のうち，組織の情報セキュリティ対策の当事者である情報セキュリティ責任者・担当者（教育担当なども含む）474 件，および経営者・部門長（情報セキュリティ責任者兼務も含む）42 件，計 516 件.

(3)　分析方法

探索的因子分析（以下因子分析という）を実行した．分析には統計解析ソフトウェアである SPSS16.0J for Windows を使用した．因子の抽出には，最尤法を用いた.

(4)　分析結果

(a)　潜在因子の探索

因子分析は，観測変数間の相関行列に基づいて実行されるため，変数間に相関がなければ，因子分析を実行する価値がない．また，変数間に強すぎる相関（多重共線性）がある場合，これらの変数は同じ情報を表すため，係数の算出ができない．そこで KMO の測度[⋆2]と Bartlett の球面性検定[⋆3]により検定したところ，**表 4** のとおり検定結果は良好であった．分析の結果，初期の固有値が 1 以上であること，固有値の減衰状況，因子の解釈のしやすさ，約 65%の変動を吸収していることなど考慮して，動機要因に関しては 6 因子解を，阻害要因に関しては 4 因子解を採用した．また，記述統計の結果，歪度が極端な

⋆2 KMO（Kaiser-Meyer-Olkin）の測度：因子分析で取り扱う，観測変数の妥当性を示す指標．0 から 1 の範囲の値をとり，KMO が 0.5 未満の場合は，これらの変数を使って因子分析を行うことは不適切であることになる.

⋆3 Bartlett の球面性検定：帰無仮説 (H_0) = 観測変数間には相関がない，とおいて帰無仮説が棄却されれば（P 値（有意確率）< 0.05）変数間に相関があることになる．H_0 が棄却されない場合は，そのデータは，因子モデルには適していないことになる.

© 2009 Information Processing Society of Japan

表 4　KMO の測度と Bartlett の球面性検定の値
Table 4　KMO and Bartlett's test of sphericity.

	動機要因	阻害要因
KMO の標本妥当性の測度	0.951	0.961
Bartlett の球面性検定(P 値)	0.000	0.000

値を示した変数や，因子分析の結果，いずれの因子にも 0.3 以上の負荷量を示さなかった変数を除いた．動機要因は 2 変数を除き 29 項目で因子数を 6 に固定，阻害要因は 2 変数を除き 28 項目で因子数を 4 に固定し，最尤法およびプロマックス回転で因子を抽出した．プロマックス回転後の因子パターン行列を，**表 5** と**表 6** に，因子相関行列を，**表 7** と**表 8** に示す．

(b)　調査結果からの因子の解釈

因子の解釈について以下のように検討した．動機要因については，第 1 因子（AI）は，セキュリティリスクの管理に関する項目に高い負荷量を示していることから，“リスク管理因子” と命名した．第 2 因子（AII）は，他社との差別化，対外的アピール，顧客の評価に高い負荷量を示していることから，“競争優位因子” と命名した．第 3 因子（AIII）は，他社に遅れない，監査指摘の改善，事故再発防止などに高い負荷量を示していることから，“改善因子” と命名した．第 4 因子（AIV）は，内部犯行の防止や社員を被害から守るなどに高い負荷量を示していることから，“内部統制因子” と命名した．第 5 因子（AV）は，法令順守，事故による影響を避ける，事業継続に高い負荷量を示していることから，“事業継続因子” と命名した．第 6 因子（AVI）は，調達や取引先の要求に関する項目に高い負荷量を示していることから，“取引先の要求因子” と命名した．阻害要因については，第 1 因子（BI）は，技術やノウハウに関する項目に高い負荷量を示していることから，“技術・ノウハウ因子” と命名した．第 2 因子（BII）は，経営者の関心のなさや予算確保の難しさ，社内の評価などに高い負荷量を示していることから，“組織運営因子” と命名した．第 3 因子（BIII）は，業務効率低下や作業負荷の増大に高い負荷量を示していることから，“手間・効率因子” と命名した．第 4 因子（BIV）は，社員への教育やセキュリティの重要性の浸透に高い負荷量を示していることから，“理解・協力因子” と命名した．

4.3　モチベーション構造についての仮説

本節では，前節により得られたモチベーションの構成概念の構造について仮説を提示する．情報セキュリティ対策の動機要因に関しては，予備調査であるインタビュー調査において

表 5　動機要因に関する項目：最尤法，因子数 6，プロマックス回転後の因子パターン行列（$N = 516$）
Table 5　Factor pattern matrix – drive factors for information security ($N = 516$).

	AI	AII	AIII	AIV	AV	AVI
A19 IT 化の推進にあわせてセキュリティ対策を行うため	0.725	-0.017	0.200	-0.006	-0.026	-0.057
A15 情報セキュリティポリシーを整備するため	0.722	0.139	-0.010	-0.054	-0.088	0.012
A13 情報管理を確実にするため	0.715	0.193	-0.141	0.058	-0.021	-0.090
A05 ウイルスやスパイウエアなどの脅威に対応するため	0.692	-0.205	-0.150	-0.015	0.184	0.167
A20 セキュリティ事故の発生を未然に防止するため	0.690	-0.119	-0.087	0.138	0.179	-0.090
A18 ソフトウェアなどに新しく発見された脆弱性に対応するため	0.619	-0.092	0.258	-0.019	-0.063	0.116
A16 他社のセキュリティ事故に学び，対策を点検強化するため	0.568	0.095	0.130	0.084	-0.123	0.102
A22 リスクマネジメントの一環としてセキュリティリスク対応のため	0.530	0.065	-0.040	0.288	0.057	-0.034
A04 社会的責任を果たすため	0.500	0.051	-0.107	-0.032	0.390	0.003
A09 対策状況の自己診断により明確になった弱点を改善するため	0.374	0.144	0.226	-0.005	0.063	0.147
A08 他社と差別化を図り，企業の競争力を高めるため	-0.010	0.805	0.102	-0.175	0.073	0.008
A17 自社の情報セキュリティ対策を対外的にアピールするため	0.132	0.642	0.223	-0.113	-0.107	0.053
A14 対策を行うことで株主や取引先や顧客から評価されるため	-0.099	0.621	0.033	0.152	0.077	0.030
A21 対策を行うことで顧客・取引先との信頼関係を確立するため	-0.057	0.514	-0.105	0.385	0.020	0.122
A25 他社の対策の取り組みに遅れないようにするため	-0.031	0.320	0.614	0.100	-0.112	-0.076
A23 監査の結果指摘されたことを改善するため	-0.245	0.023	0.574	0.206	0.125	0.123
A10 セキュリティ事故の再発防止のため	-0.098	-0.141	0.520	0.060	0.409	0.144
A11 セキュリティに関する業界標準に従うため	0.147	0.234	0.508	-0.098	0.145	0.011
A26 事業活動と矛盾しないよう対策や体制を整備するため	0.284	0.079	0.479	0.116	0.043	-0.104
A28 自社の営業秘密や技術情報を守るため	0.017	-0.042	0.092	0.788	-0.133	0.094
A27 内部関係者によるセキュリティ上の犯行を防ぐため	0.164	-0.129	0.231	0.658	-0.111	0.020
A30 自社の社員をセキュリティ事故による被害から守るため	0.217	0.026	0.122	0.517	-0.038	-0.049
A31 情報セキュリティ対策は，事業推進上必要だと思うため	0.264	0.237	-0.032	0.413	0.010	-0.021
A24 個人情報を守るため	0.254	-0.186	0.065	0.406	0.264	-0.102
A01 法令順守のため(情報セキュリティ関連)	0.048	-0.017	0.085	-0.168	0.608	0.179
A12 事故がブランドイメージや業績に与える影響を避けるため	-0.030	0.248	0.291	-0.012	0.539	-0.183
A07 事故や災害時でも自社の中心となる事業を継続するため	0.229	0.216	-0.086	0.049	0.342	0.055
A03 取引先との契約に明記された情報の安全管理を行うため	-0.047	0.136	-0.101	0.241	0.108	0.554
A06 調達要件にセキュリティ対策実施が明記されているため	0.070	0.017	0.188	-0.071	0.049	0.695
初期の固有値	12.674	1.805	1.462	1.138	1.050	1.003
寄与率(%)	43.704	6.223	5.040	3.923	3.621	3.457
累積寄与率(%)	43.704	49.926	54.966	58.890	62.511	65.968

© 2009 Information Processing Society of Japan

表 6　阻害要因に関する項目：最尤法，因子数 4，プロマックス回転後の因子パターン行列（$N = 516$）
Table 6　Factor pattern matrix – disincentive factors for information security ($N = 516$).

	BI	BII	BIII	BIV
B21 対策を実施する技術が不足している	0.933	-0.162	-0.019	0.071
B24 情報セキュリティに関して相談できる専門家がいない	0.841	0.021	-0.070	-0.031
B05 対策を実施するノウハウが不足している	0.764	0.113	-0.098	0.024
B11 対策を実施できる人材がいない	0.739	0.081	0.027	-0.016
B10 技術の進歩が速すぎて追いつけない	0.727	0.026	-0.034	0.030
B30 最適な対策として何を行えばいいかわからない	0.670	-0.004	0.109	0.042
B07 自社の現状のセキュリティレベルがわからない	0.651	-0.010	-0.163	0.247
B14 優先すべきセキュリティ対策の順位づけがむずかしい	0.558	-0.067	0.030	0.338
B18 情報セキュリティ上のルールが整備されていない	0.483	0.155	-0.042	0.187
B28 対策に必要な人員の割り当てがない	0.397	0.183	0.394	-0.119
B03 経営層に情報セキュリティに対する関心があまりない	-0.109	0.953	-0.222	0.193
B09 対策の必要性について経営層を説得できない	-0.088	0.900	-0.177	0.204
B02 対策予算を獲得するのが難しい	0.037	0.802	0.082	-0.163
B08 必要な対策製品を購入するコスト的余裕がない	0.135	0.647	0.192	-0.207
B01 対策を推進する組織体制が整備されていない	0.266	0.507	-0.097	0.118
B04 対策を実施しても事業へのプラス効果が目に見えない	-0.044	0.487	0.345	0.003
B19 社内では対策の実施が業績向上に貢献しないと評価されている	-0.012	0.420	0.312	0.126
B26 対策の実施が株主，取引先，顧客などの評価と結びつかない	0.074	0.382	0.284	-0.019
B23 対策の実施により利便性が損なわれ業務効率が落ちる	-0.211	-0.073	0.898	0.218
B20 セキュリティルールを守るために従業員へ作業負荷がかかりすぎる	-0.112	-0.079	0.838	0.165
B15 対策を行うには手間・ひま・時間がかかりすぎる	0.233	-0.086	0.510	0.170
B22 情報セキュリティの担当者は他業務との兼務である	0.436	-0.095	0.436	-0.083
B29 対策にかける適正コストの判断がむずかしい	0.363	0.243	0.427	-0.188
B25 対策導入の際の手順やプロセスの変化に従業員が対応できない	0.306	0.017	0.315	0.270
B06 情報セキュリティ上のルールを社員に順守させるのがむずかしい	-0.002	0.068	0.145	0.658
B13 情報セキュリティ教育を全従業員に履修させるのが困難である	0.176	-0.067	0.090	0.644
B16 社内に情報セキュリティの重要性が浸透しない	0.014	0.181	0.170	0.608
B17 外部へのメール転送などを監視されることへの社員の反発がある	0.112	0.052	0.206	0.332
初期の固有値	15.390	1.598	1.303	1.198
寄与率(%)	51.299	5.328	4.345	3.992
累積寄与率(%)	51.299	56.627	60.972	64.964

表 7　因子相関行列（動機要因）
Table 7　Factor correlation matrix (drives).

	AI	AII	AIII	AIV	AV	AVI
AI	-	0.63	0.60	0.69	0.52	0.30
AII		-	0.59	0.59	0.40	0.31
AIII			-	0.44	0.29	0.38
AIV				-	0.61	0.27
AV					-	0.30
AVI						-

表 8　因子相関行列（阻害要因）
Table 8　Factor correlation matrix (disincentives).

	BI	BII	BIII	BIV
BI	-	0.71	0.73	0.63
BII		-	0.66	0.61
BIII			-	0.55
BIV				-

も，組織内部の要求と社会的要求があると指摘されていた．企業は社会的存在である以上，その活動は組織内部のみで完結するものではない．企業は事業目的達成のために，方針を定め，体制を整備し，社会に働きかける．そして，その過程で，社会からの要求にも応えなければならない．ここで動機要因として抽出された 6 つの因子について考察すると，第 1 因子（AI：リスク管理因子）は，自社に内在するセキュリティリスクの管理であり，第 3 因子（AIII：改善因子）は，監査指摘の改善，事故再発防止など，組織内部の改善要求に応えるものである．また，第 4 因子（AIV：内部統制因子）は，自社の営業秘密や技術情報を守る，内部犯罪を防ぐなど，やはり，組織内部の要求に応えるものである．そこで，これらの 3 因子は，組織内部の要求に分類することができる．

一方，第 2 因子（AII：競争優位因子），第 5 因子（AV：事業継続因子），第 6 因子（AVI：取引先の要求因子）は，社会的要求に分類することができる．企業が株主・取引先・顧客などのステークホルダの評価を得るためには，他社と差別化を図り，企業の競争力を高めなければならない．そして，それにより，競争優位のポジションを獲得できる（AII：競争優位因子）．法令順守や，事業継続の要求（AV：事業継続因子）は，組織内要求の側面もあるが，ここでは，社会的要求の側面のほうがより重要と考え，社会的要求に分類する．経済産業省の事業継続計画策定ガイドラインには，事業継続計画の必要性に関して「危機が発生したときに，企業に対して問われるのは，その企業が危機に直面した時であったとしても事業

© 2009 Information Processing Society of Japan

図 1　分類した動機要因と阻害要因のモデルの構成
Fig. 1　A motivation structure for information security with drive factors and disincentive factors.

を遂行（継続）するという社会的使命を果たせるかどうか，である．（中略）企業は，自身の被害の局限化という観点に留まらず，コンプライアンスの確保や社会的責任という観点から対策を講じなければならない」との記載がある[30]．第 6 因子（AVI：取引先の要求因子）についても社会的要求に分類される．

なお，阻害要因は組織内部にあるものなので，分類は行わない．モデルの構成を**図 1** に示す．

5.　モチベーション構造の検証

5.1　仮説の検証

本章では，4.3 節で提示したモチベーション構造の仮説について，構造方程式モデリング（SEM: Structural Equation Modeling，以下 SEM という）を用いてモデルの妥当性を検証する．

(1)　検証目的

前章で考察した仮説に基づいて動機要因・組織内要求に分類した，第 1 因子（AI），第 3 因子（AIII），第 4 因子（AIV）の 3 因子間，および，動機要因・社会的要求に分類した，第 2 因子（AII），第 5 因子（AV），第 6 因子（AVI）の 3 因子間，および，阻害要因である第 1 因子（BI），第 2 因子（BII），第 3 因子（BIII），第 4 因子（BIV）の 4 因子間にそれぞれ中程度の相関がみられたことから，それらの背後に高次因子として動機要因・組織内要求（**図 2**），動機要因・社会的要求（**図 3**），阻害要因（**図 4**）を仮定した因果モデルを構築し，その妥当性を検証する．

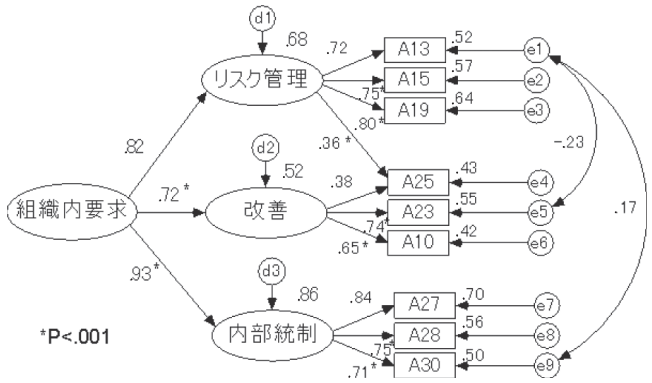

図 2　動機要因（組織内要求）の 2 次因子モデル（モデル 1）
Fig. 2　Model 1: High-order factor model about drive factors for information security based on organizational requirement.

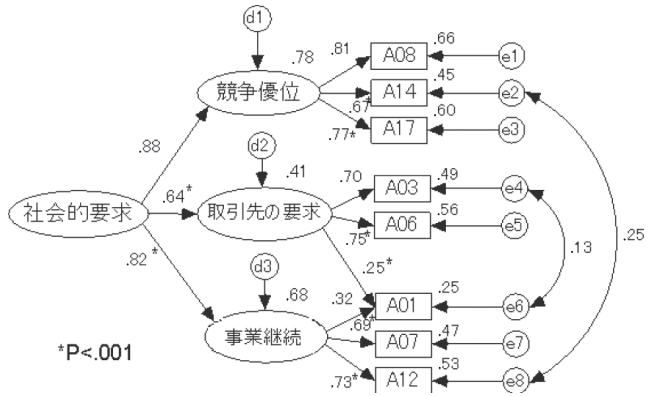

図 3　動機要因（社会的要求）の 2 次因子モデル（モデル 2）
Fig. 3　Model 2: High-order factor model about drive factors for information security based on social requirement.

© 2009 Information Processing Society of Japan

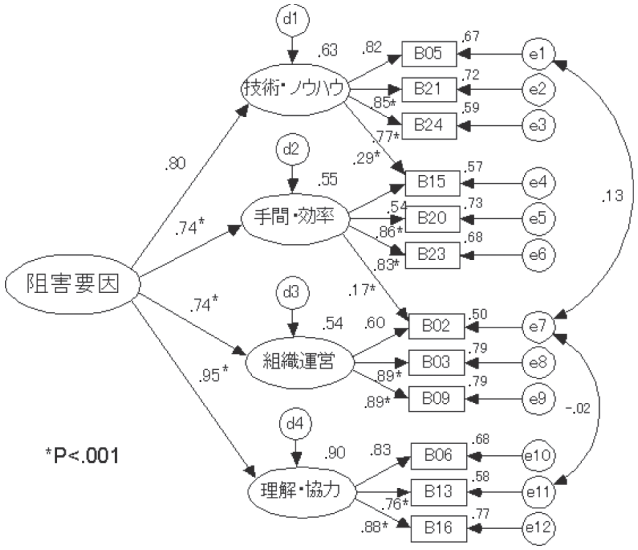

図 4　阻害要因の 2 次因子モデル（モデル 3）
Fig. 4　Model 3: High-order factor model about disincentive factors for information security.

(2)　検証方法

妥当性の検証にあたってはSEMを用いた．SEMは，共分散構造分析（Covariance Structure Analysis）ともいわれ，直接観測される変数（観測変数）から，直接観測できない潜在変数を導き出し，その潜在変数と観測変数や潜在変数間の因果関係について仮説（モデル）を設定し，その妥当性を検証して仮説の適否を判定することで，因果関係の強さを推定する統計的分析手法である[31)–34)]．なお，実際の分析には，SEM 解析ソフトウェアであるAmos16.0J を用いた．

モデルの作成にあたっては，下位の潜在変数それぞれに高い因子負荷量を示す上位 3 項目を観測変数としてモデルを構築した．

(3)　検証結果

解析結果を図 2，図 3，図 4 に示す．図 2，3，4 のパス図においては，観測変数は四角，潜在変数は楕円で描かれている．e1, . . . , e8（または e1, . . . , e12）は誤差変数であり，観測変数に独自の値である．d1, . . . , d3（または d1, . . . , d4）は撹乱変数であり，潜在変数に独自の値である．パスに隣接して出力されている数字は，パス係数であり，因子負荷量を表す．また観測変数の横に出力されている数字は信頼度である．因子負荷量と信頼度が大きいほど，潜在変数への影響が大きい．なお，パス係数は，観測変数の分散を 1 に標準化したときの推定値（標準化係数）が出力されている．また，モデルの識別性を確保するために，潜在変数から観測変数へのパスのうち，モデル内で最も上にあるパスについてはパス係数を 1 に固定し制約を加えた．制約を加えたパスについては，有意確率は表示されない．図内のパス係数の右脇のアスタリスクは，有意確率 P が 0.001 未満であることを示している．

表 9　モデル 1，2，3 の各種適合度指標
Table 9　Fit index of model 1, 2, 3.

適合度指標	RMR	GFI	CFI	RMSEA
モデル 1	0.050	0.975	0.978	0.062
モデル 2	0.063	0.972	0.963	0.081
モデル 3	0.075	0.964	0.980	0.056

最初に，作成したモデルについて分析を行った後，3 つのモデルとも，修正指数を利用して修正を加え，より適合状態の良いモデルを選択した．修正箇所は，モデル 1 では，第 1 因子（AI）から観測変数 A25「他社の対策の取り組みに遅れないようにするため」へのパス，モデル 2 では，第 6 因子（AVI）から，A01「法令順守のため」へのパス，モデル 3 においては，第 1 因子（BI）から B15「対策を行うには手間・ひま・時間がかかりすぎる」，第 2 因子（BII）から B02「対策予算を獲得するのが難しい」へのパスで，因子解釈上の問題はなく，また適合度指標の改善が期待されるため，パスを加えた．同様の理由で，修正指数に基づいて誤差変数間に共変動を加えた．この共変動は，図の中では，円弧で示されている．

分析の結果，高次因子から下位の因子へのパス係数はいずれも十分に高い値を示しており，有意確率は，いずれも 0.001 未満で有意であった．これらの結果は，モチベーションを構成する因子それぞれの背後に高次の因子を考えること，および，各因子間に因果モデルを考えることの妥当性を示している．

(4)　検証結果：適合度指標

次に，モデル全体としての妥当性を検証する．SEM においてモデルの良さを判断するポイントに，構築したモデルがデータ構造を適切に表現できているかどうかの観点があげられ，モデルの妥当性検証のために各種適合度指標が使われる．**表 9** にモデル 1，2，3 の各種適合度指標を示した．適合度指標の値はいずれも良好であり，構築したモチベーションの構造の妥当性を示している．

© 2009 Information Processing Society of Japan

5.2 考　　察

本節では，企業の情報セキュリティ対策におけるモチベーションについて 5.1 節の検証結果をふまえ，マイクロ的視点とマクロ的視点から考察する．

(1) マイクロ的視点からの考察

本論文では，Vroom の期待理論をベースに，Vroom のモデルの「結果の誘意性」と「期待の強度」を，それぞれ「動機要因」，「阻害要因」と置き換えることによって，現状の情報セキュリティ対策推進における問題点となる要因を抽出した．

ここで，本論文で得られたモデルを活用して，動機要因をどのように高め，阻害要因をいかに低減して，情報セキュリティ対策を推進すればいいのかについて考察する．考察にあたっては，被験者より寄せられたコメントも参照する．

(a) 動機要因

- 動機要因として抽出された因子について

  探索的因子分析で抽出した動機要因を構成する 6 因子は，情報セキュリティ対策を行うことによってもたらされる価値の認識を示す因子である．動機要因におけるこれら因子へのパス係数の値はいずれも高く（図 2，図 3），企業で情報セキュリティ対策を行う当事者の対策を実施する動機に与える影響が大きいことを示している．

  これまでは，組織の情報セキュリティ対策を推進するためには，情報セキュリティ上のリスクとそのマネジメントについて説くという，リスク管理因子（図 2）を中心としたアプローチであった．しかし，抽出された因子には，企業価値の向上に関わる社会的要求である，競争優位因子，取引先の要求因子，事業継続因子の 3 因子が含まれている（図 3）．このことは，動機要因を高めるには，情報セキュリティ上のリスクとそのマネジメントについて説くといったアプローチだけではなく，社会的要求も考慮し，企業の社会的存在価値と結びつけた多面的アプローチが必要であることを示唆している．

- 動機要因を高める施策

  得られたモデルを活用して動機要因を高める方法の 1 つとして，パス係数の高い動機要因（図 2，図 3）を対象に，担当者が感じている課題を抽出する方法がある．たとえば，社会的要求において，競争優位因子へのパス係数は 0.88 と高い．被験者より寄せられたコメントにも，「商売上，メリットがあると明確になれば，動機となりやすい」，「できれば他の競合との差別化を図る武器にしたい」のように，情報セキュリティ対策の推進を競争優位のポジションの獲得に結びつけたいという心理が現れている．このような課題抽出を通して，課題解決を図っていくことで，情報セキュリティ対策の推進を見込むことができると考えている．

(b) 阻害要因

- 阻害要因として抽出された因子について

  探索的因子分析で抽出した阻害要因を構成する 4 因子は，対策の実施を阻む要因である．阻害要因からこれら因子へのパス係数の値はいずれも高く（図 4），情報セキュリティ対策を推進するためには，これら因子の影響をできる限り小さくする必要がある．

  4 因子の中でパス係数が最も高いのは理解・協力因子である．このことは，対策推進の当事者が，従業員に情報セキュリティの重要性を理解させ，ポリシを守らせるという人的要素に，最も困難を感じていることを示している．

  理解・協力因子以外の因子については，人材や費用など経営資源を投下することで，低減が見込める可能性がある．しかし，理解・協力因子は，従業員の意識と行動に関わるものであるため，単に経営資源を投下しただけで解決する問題ではない．このような課題の解決には，心理学や行動科学をふまえた情報セキュリティ対策の推進が必要になると考える．

- 阻害要因を低減させる施策

  前述のとおり，阻害要因においては，理解・協力因子へのパス係数が高い（図 4）．被験者のコメントにも，「実際に対策に取り組む社員を，いかにその気にさせるかが難しい」，「“自社は大丈夫”，“自分は大丈夫” という意識が推進の壁となっている」「全社員のモチベーションアップのための教育が必要．何を（What）ではなく，どのように（How to）を教えるべき」などがある．これらは，情報セキュリティに対する意識向上と対策手順を普及するための教育について課題があることを示しており，課題解決を図っていくことが阻害要因を低減させることにつながると考える．

  ただし，従業員の意識が向上して，対策手順が分かっていても，手順が面倒だったり，自分は大丈夫と思いこんだりなどの理由で，対策意欲が現実の行動に結びつかない場合もある．本論文では，企業で情報セキュリティ対策を推進する当事者を対象としたが，このような課題を解決するためには，従業員という別の視点から情報セキュリティ対策に対する動機要因と阻害要因の解明を行っていく必要がある．これは，今後の課題としたい．

(2) マクロ的視点からの考察

3.1 節のマクロ的視点の文献調査より，情報セキュリティ対策のモチベーションにおける基本的要素として，情報セキュリティ，経済，社会の 3 つを抽出した．情報セキュリティ対策のモチベーションを理解するうえで経済性と社会性は重要である．ここでは，この 2 点について対策の推進という観点から，各因子との関連性を，環境の取り組みを参照しながら考察する．

© 2009 Information Processing Society of Japan

(a) 経済性

- 抽出された因子と経済性の関係

経済性と関連するのは，動機要因の競争優位因子と取引先の要求因子，阻害要因の組織運営因子である．組織運営因子には，B03，B09 の経営層の関心や理解のなさ，B02，B08 の予算獲得の難しさ，B01 の体制の未整備がある．被験者のコメントにも，「費用対効果を示すことが難しいため経営層の理解が得にくい，予算がとりにくい」，「情報セキュリティ対策は直接売上に結びつかないため，対策の推進が難しい」とのコメントもある．これらのコメントは，競争優位因子や取引先の要求因子と，組織運営因子の関連が深いことを示している．

- 経済性に関する問題とその解決

経済主体の活動が，市場を経由せずに他の経済主体に悪影響を与えることを外部不経済と呼ぶ[35]．情報セキュリティにおいて，対策費用は利益を生まないと考えられており，外部不経済の問題がある．情報セキュリティへの取り組みにより，競争優位のポジションや良い取引先を獲得できれば，自らが費用を負担して，外部不経済を内部化することが可能であろう．また，経営層の理解や，予算獲得の難しさという阻害要因の因子である組織運営因子の影響を克服することができる．

3.1 節の文献調査で示したように，環境対策では，多くの研究や施策を通して外部不経済の問題を解決してきた．情報セキュリティ策でも，環境対策同様に外部不経済の問題を解決するための研究や施策が必要であると考えている．

(b) 社会性

- 抽出された因子と社会性の関係

動機要因・組織内要求因子の下位因子として抽出されたリスク管理因子に，観測変数 A04「社会的責任を果たすため」が属していることについて考察する．企業全体の視野においては，社会的責任は，サステナビリティ，環境，情報セキュリティ，コンプライアンス，社会貢献，人権の尊重などを包含する上位概念である．しかし，情報セキュリティにおいて社会的責任を果たすことは，第 1 に，情報セキュリティ対策を行うことにより，社会に不利益を及ぼさないことである．よって，リスク管理因子に観測変数 A04 が属していることは，十分に首肯できる結果である．

- 社会性に関する問題とその解決

ある人や企業が被害者にも加害者にもなりうるという状況は，環境も情報セキュリティも同じである．また，文献 19) で指摘されているように，情報セキュリティは，環境問題同様，地球規模の問題である．対策をしていない企業がインターネット上に多ければ多いほど，悪意の攻撃に利用され，IT インフラそのものの存在を脅かし，ひいては社会の機能を麻痺させる可能性を孕んでいる．経済的利得の有無により，情報セキュリティ対策を行わないという選択は，本来はあってはならない．そこで，経済性の観点からの取り組みに加え，社会性の観点からの取り組み，たとえば「情報セキュリティ対策に取り組む企業が社会的に評価されるメカニズム」などの研究が，今後の大きな研究テーマとして考えられる．

6. ま と め

本論文では，組織の情報セキュリティ対策を推進する当事者の，対策を実施する動機要因や阻害要因を把握し，これら要因の構造を明らかにするために，文献調査とインタビュー調査により，情報セキュリティ対策のモチベーションにかかわる諸要因を探索した．また，探索した諸要因をもとに作成した質問紙を用いて調査を行い，情報セキュリティ対策のモチベーションについて整理した．516 名の回答データを用いて探索的因子分析を行った結果，動機要因として計 6 因子を，阻害要因として計 4 因子を抽出した．次に，これらの因子の構造について仮説を立て，その妥当性を SEM により検証し，情報セキュリティ対策におけるモチベーションの構造を示した．また，得られた構造について，マイクロ的視点とマクロ的視点から考察した．

なお，本論文では，動機要因と阻害要因を別々にモデル化したが，5.2 節で考察したように，これらの要因は，密接な関係がある．今後の課題として，情報セキュリティを推進する当事者の情報セキュリティ対策におけるモチベーションの構造に関する調査実験を継続して進めること，動機要因と阻害要因の関連性をふまえたモデル化，および，モチベーションの定式化の検討があげられる．

謝辞　本研究は，中央大学と IPA の共同研究により実施したものである．本研究を進めるにあたり，有益な助言と協力をいただいた，IPA の山岸篤弘氏および関係者各位に深く感謝する．

参 考 文 献

1) ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (2005).
2) 青池慎一，榊　博文：現代社会心理学—心理・行動・社会，慶応義塾大学出版会 (2004).

© 2009 Information Processing Society of Japan

3) 中島義明，繁桝算男，箱田裕司：新・心理学の基礎知識，有斐閣 (2005).
4) 松山義則：人間のモチベーション，培風館 (1981).
5) 上淵　寿：動機づけ研究の最前線，北大路書房 (2004).
6) 金井壽宏：働くみんなのモティベーション論，NTT 出版 (2006).
7) Vroom, V.H.: *Work and Motivation*, Wiley, New York (1964).
8) 日景奈津子，カールハウザー，村山優子：情報セキュリティ技術に対する安心感の構造に関する統計的検討，情報処理学会論文誌，Vol.48, No.9, pp.3193–3203 (2007).
9) 日景奈津子，村山優子：情報セキュリティ技術に対する安心感要因の考察，情報処理学会研究会報告，2007-DPS-130/2007-CSEC-36, Vol.2007, No.16, pp.333–338 (2007).
10) 内田勝也，矢竹清一郎，森　貴男，山口健太郎，東　華枝：情報セキュリティ心理学の提案，情報処理学会研究会報告，2007-DPS-130/2007-CSEC-36, Vol.2007, No.16, pp.327–331 (2007).
11) Marcinkowski, S.J. and Stanton, J.M.: Motivational aspects of information security policies, *Proc. IEEE International Conference on Systems, Man and Cybernetics*, Oct. 2003, pp.2527–2532 (2003).
12) Workman, M. and Gathegi, J.: Punishment and ethics deterrents: A study of insider security contravention, *Journal of the American Society for Information Science*, Vol.58, Issue 2, pp.212–222 (2006).
13) 警察庁：不正アクセス行為対策等の実態調査調査報告書（平成 15 年度–平成 19 年度）．入手先 http://www.npa.go.jp/cyber/research/index.html（参照 2008-11-23）
14) NRI セキュアテクノロジーズ：企業における情報セキュリティ実態調査（2005〜2007）．
15) NPO 情報セキュリティフォーラム：情報セキュリティに関するアンケート調査調査報告書（2006 年 3 月）．入手先 http://www.isef.or.jp/report/（参照 2008-11-23）
16) IPA：中小企業の情報セキュリティ対策確認手法に関する実態調査報告書（2008 年 4 月）．入手先 http://www.ipa.go.jp/security/fy19/reports/sme/press.html（参照 2008-11-23）
17)（社）日本経済団体連合会：企業の情報セキュリティのあり方に関する提言（2005 年 3 月）．入手先 http://www.keidanren.or.jp/japanese/policy/2005/015/index.html（参照 2008-11-23）
18) 経済産業省：情報セキュリティガバナンス研究会報告書（2007 年 3 月）．入手先 http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html（参照 2008-11-23）
19) 経済産業省：グローバル情報セキュリティ戦略（2007 年 5 月）．入手先 http://www.meti.go.jp/press/20070510001/20070510001.html（参照 2008-11-23）
20) 経済産業省：産業構造審議会情報セキュリティ基本問題委員会中間とりまとめ（2008 年 6 月）．入手先 http://www.meti.go.jp/press/20080620005/20080620005.html（参照 2008-11-23）
21) 亀田達也，村田光二：複雑さに挑む社会心理学適応エージェントとしての人間，有斐閣アルマ (2000).
22) Porter, M.E. and Kramer, R.K.: Strategy and Society: The Link Between Competitive Advantage and Corporate Social Responsibility, *Harvard Business Review* (Dec. 2006).
23) Porter, M.E.: America's Green Strategy, *Scientific American*, Vol.264, No.4 (Apr. 1991).
24) Shmidheiney, S.: *Changing Course: A Global Business Perspective on Development and the Environment*, The MIT Press. (1992). BCSD 日本ワーキンググループ（訳）：チェンジング・コース，ダイヤモンド社 (1992).
25) 金原達夫，金子慎治：環境経営の分析，白桃書房 (2005).
26) GRI: The Sustainability Reporting Guidelines (2000).
27) WBCSD: Eco-Efficiency: Creating more value with less impact (2000). 入手先 http://www.wbcsd.org/templates/TemplateWBCSD5/layout.asp?type=p&MenuId=MTUyMg&doOpen=1&ClickMenu=LeftMenu（参照 2008-11-23）
28) SPSS Japan Inc.: 多変量解析によるデータの分類 (2008).
29) 小塩真司：研究事例で学ぶ SPSS と Amos による心理・調査データ解析，東京図書 (2005).
30) 経済産業省：事業継続計画策定ガイドライン（2005 年 3 月）．入手先 http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html（参照 2008-11-23）
31) 山崎瑞紀，吉川肇子：鳥インフルエンザ（新型インフルエンザ）に関する不安要因の構造，日本社会心理学会第 47 回大会発表論文集，pp.676–677 (2006).
32) 山本嘉一郎，小野寺孝義：AMOS による共分散構造分析と解析事例［第 2 版］，ナカニシヤ出版 (2002).
33) 豊田秀樹：共分散構造分析 Amos 編，東京図書 (2007).
34) 朝野熙彦，小島隆矢，鈴木督久：入門 共分散構造分析の実際，講談社 (2005).
35) 内閣府公共料金の窓・用語解説．入手先 http://www5.cao.go.jp/seikatsu/koukyou/explain/ex_index.html（参照 2008-11-23）

付録：質問紙調査で使用した質問紙の概要

A.　動機要因に関する質問の概要

以下にあげる項目が，情報セキュリティ対策を行う動機となるかどうかについて，あなたのお考えにもっともよくあてはまる以下の 1〜7 の数字ひとつに ◯ をつけて下さい．

1. 全く動機にならない　2. あまり動機にならない　3. なんとも言えない　4. それなりの動機となる　5. 動機となる　6. 強い動機となる　7. 非常に強い動機となる

A01　法令順守のため（情報セキュリティ関連）

A02　情報漏えいを防ぐため

A03　取引先との契約に明記された情報の安全管理を行うため

© 2009 Information Processing Society of Japan

A04　社会的責任を果たすため
A05　ウイルスやスパイウエアなどの脅威に対応するため
A06　調達の要件にセキュリティ対策の実施が明記されているため
A07　事故や災害時でも自社の中心となる事業を継続するため
A08　他社と差別化を図り，企業の競争力を高めるため
A09　対策状況を自己診断した結果，明確になった弱点を改善するため
A10　セキュリティ事故の再発防止のため
A11　セキュリティに関する業界標準に従うため
A12　セキュリティ事故がブランドイメージや業績に与える影響を避けるため
A13　情報管理を確実にするため
A14　対策を行うことで株主や取引先や顧客から評価されるため
A15　情報セキュリティポリシーを整備するため
A16　他社のセキュリティ事故事例に学び，自社の対策を点検強化するため
A17　自社の情報セキュリティ対策を対外的にアピールするため
A18　ソフトウェアなどに新しく発見された脆弱性に対応するため
A19　IT 化の推進にあわせてセキュリティ対策を行うため
A20　セキュリティ事故の発生を未然に防止するため
A21　対策を行うことで顧客・取引先との間の信頼関係を確立するため
A22　リスクマネジメントの一環として，情報セキュリティリスクに対応するため
A23　監査の結果指摘されたことを改善するため
A24　個人情報を守るため
A25　他社の対策の取り組みに遅れないようにするため
A26　事業活動と矛盾しないようにセキュリティ対策や体制を整備するため
A27　内部関係者によるセキュリティ上の犯行を防ぐため
A28　自社の営業秘密や技術情報を守るため
A29　税制面での優遇（法人税，対象製品の購入時など）を受けるため
A30　自社の社員をセキュリティ事故による被害から守るため
A31　情報セキュリティ対策は，自社の事業を推進する上で必要だと思うため

B.　阻害要因に関する質問の概要

以下にあげる状況により情報セキュリティ対策の推進が阻まれているとします．あなたの組織では，このような状況の克服は難しいですか？あなたのお考えにもっともよくあてはまる 1〜7 の数字ひとつに ◯ をつけて下さい．

1. 全く難しくない　2. あまり難しくない　3. なんとも言えない　4. やや難しい　5. 難しい　6. かなり難しい　7. 非常に難しい

B01　対策を推進する組織体制が整備されていない
B02　対策予算を獲得するのが難しい
B03　経営層に情報セキュリティに対する関心があまりない
B04　対策を実施しても事業へのプラス効果が目に見えない
B05　対策を実施するノウハウが不足している
B06　情報セキュリティ上のルールを社員に順守させるのがむずかしい
B07　自社の現状のセキュリティレベルが分からない
B08　必要な対策製品を購入するコスト的余裕がない
B09　対策の必要性について経営層を説得できない
B10　技術の進歩が速すぎて追いつけない
B11　対策を実施できる人材がいない
B12　情報セキュリティを担当する部門への社内の評価が低い
B13　情報セキュリティ教育を全従業員に履修させるのが困難である
B14　優先すべきセキュリティ対策の順位づけがむずかしい
B15　対策を行うには手間・ひま・時間がかかりすぎる
B16　社内に情報セキュリティの重要性が浸透しない
B17　外部へのメール転送などを監視されることへの社員の反発がある
B18　情報セキュリティ上のルールが整備されていない
B19　社内では対策の実施が業績向上に貢献しないと評価されている
B20　情報セキュリティルールを守るために従業員へ作業負荷がかかりすぎる
B21　対策を実施する技術が不足している
B22　情報セキュリティの担当者は他業務との兼務である
B23　対策の実施により利便性が損なわれ業務効率が落ちる
B24　情報セキュリティに関して相談できる専門家がいない
B25　対策導入の際の手順やプロセスの変化に従業員が対応できない
B26　対策の実施が株主，取引先，顧客などの評価と結びつかない
B27　情報セキュリティ事故が起こった際の責任の所在があいまいである
B28　対策に必要な人員の割り当てがない

© 2009 Information Processing Society of Japan

B29　対策にかける適正コストの判断がむずかしい
B30　最適な対策として何を行えばいいかわからない

(平成 20 年 12 月 2 日受付)
(平成 21 年 6 月 4 日採録)

推　薦　文

「情報セキュリティ対策は必要」だと分かっていても，なかなか進まない理由などを，心理学的観点から調査，分析を行ったことは大変評価に値する．これは企業の大小にかかわらず共通すると考えられる（実際，大企業ですら，対策整備に約 10 年かかっている）．今後，中小企業へのセキュリティ対策を行うべきであるが，これを速やかに進めるための一考察になると考えられる．よって論文として推薦したい．

（コンピュータセキュリティシンポジウム 2008 プログラム委員長　吉浦　裕）

菅野　泰子（正会員）

中央大学大学院理工学研究科博士課程後期課程情報セキュリティ科学専攻 3 年在学．お茶の水女子大学文教育学部中国文学専攻卒業後，(株) 日本航空勤務．2003 年から（独）情報処理推進機構セキュリティセンター研究員，2006 年より同，調査役，現在にいたる．現在，IPA にて，情報セキュリティの普及啓発，海外セキュリティ組織との連携等に従事．2008 年 CSS2008 優秀論文賞受賞．日本情報経営学会，日本セキュリティ・マネジメント学会会員．

寺田　真敏（正会員）

1986 年千葉大学大学院工学研究科写真工学専攻修士課程修了．同年（株）日立製作所入社．博士（工学）．現在，システム開発研究所にてネットワークセキュリティの研究に従事．2004 年から JPCERT コーディネーションセンター専門委員，(独) 情報処理推進機構セキュリティセンター研究員，2008 年から中央大学客員講師を兼務．

山田　安秀

1988 年北海道大学大学院環境科学研究科修了，同年通商産業省（現，経済産業省）入省．1995 年カーネギーメロン大学大学院ハインズスクール修了．2002〜2004 年内閣官房にて，Japan 戦略 II，e-文書法等の策定に携わる．2007 年より（独）情報処理推進機構セキュリティセンター長．

鎌倉　稔成

1980 年 9 月東京工業大学理工学研究科博士課程中途退学，同年文部省統計数理研究所入所，1985 年中央大学専任講師，1989 年同助教授，1995 年より同教授，現在にいたる．工学博士．応用統計学会会長，日本信頼性学会，日本統計学会，日本計算機統計学会ほか各会員．

土居　範久（名誉会員）

中央大学理工学部教授，慶應義塾大学名誉教授．現在，経済産業省情報セキュリティガバナンス研究会座長，総務省電波政策懇談会座長，文部科学省次世代スーパーコンピュータ戦略委員会主査，文部科学省「次世代 IT 基盤構築のための研究開発」プログラムディレクター，科学技術振興機構社会技術研究開発センター「情報と社会」領域総括，科学技術振興機構戦略的創造研究推進事業研究総括，NPO 法人日本セキュリティ監査協会会長，ACM 日本支部長．専門は計算機科学および情報セキュリティ．情報処理学会名誉会員．

© 2009 Information Processing Society of Japan