セキュリティ文化の醸成
-企業組織における標的型メール攻撃訓練を中心として-

2020 年 2 月 10 日

「博士学位請求論文」審査報告書

審査委員　（主査）　経営学部　専任教授

氏名　　中　西　　晶　　㊞

（副査）　経営学部　専任教授

氏名　　高　橋　　正　泰　　㊞

（副査）　経営学部　専任教授

氏名　　歌　代　　豊　　㊞

１　論文提出者　　杉原　大輔

２　論文題名　　セキュリティ文化の醸成

－ 企業組織における標的型メール攻撃訓練を中心として －

（欧文題）　Developing security culture :

Focusing on targeted email attack training in corporate organizations

３　論文の構成

序

I 本研究の目的とその背景

II 文化にまつわる基本的な概念整理

III セキュリティ文化とはどのような文化か

IV 現代的マネジメントと文化

V 研究課題の導出

VI 企業事例

VII 総合的考察

VIII 結論

補論 1 : マネジメントシステムと文化

補論 2 : 測定の対象としての「振る舞い」10traits の例から

補論 3 : CSIRT について

４　論文の概要

本論文は，セキュリティ文化の醸成について，組織文化論の視点などを参照し，企業組織における標的型メール訓練の事例研究をもとにその要件と要素を検討するとともに，セキュリティ文化が組織の中心的文化たりえるかを議論するものである。

Ⅰ章では，まず本論文の提起する問題の前提となるセキュリティ被害の現状とその原因を確認し，それらに対して企業組織が組織メンバーの集合体としての文化的アプローチの必要性を提起する。具体的には，標的型メール攻撃への備えとしての教育や訓練を中心として，情報セキュリティを重視する文化を醸成することを本論文の目的とすることを述べている。

Ⅱ章では，企業組織の中心的な文化としてセキュリティ文化を醸成していく，または，従来からの文化をセキュリティ文化へ変化させていくという前提として，文化および企業文化とは何か，文化はいかに形成されるのかについて Schein(1985 ほか)や O'Reilly(1989)，Deal & Kennedy(1982)など基本的な研究から確認している。さらに，組織文化のマネジメントに関する先行研究から，セキュリティ文化の醸成に求められる要件を整理している。本論文は現実の企業組織の問題解決を論ずることに主眼があり，まず機能的な要件整備を目指すものであるが，そのなかでもメンバーの内心に踏み込む必要性があることを指摘している。

Ⅲ章では，目指すべきセキュリティ文化について，中心的な概念を提示した OECD による定義を踏まえ，企業組織においてこの文化を醸成していくための課題を検討している。そこでは，セキュリティ文化に類似する原子力安全文化と比較して，自らが情報セキュリティに貢献すべき当事者であるという認識を持ちにくいという課題を見い出している。この課題を克服するために求められる要件・要素を織り込みながら，企業組織の文化としてのセキュリティ文化の醸成について，組織的な事故を防ぐ文化として示された「安全文化」（Reason, 1997）との対比で提示している。

Ⅳ章では，セキュリティ文化を醸成する具体的な手段について検討している。Schein や O'Reilly などの先行研究では，文化を醸成するという試みにおいて，マネジメントの効果の把握，特に成果測定の部分は否定的に捉えられている。それは，第Ⅱ章で確認したように組織文化とはメンバーの内心の問題であり，その測定が困難であるところに起因すると本論文では分析している。そのうえで，本論文では，現代的な組織運営においては否定的に捉えるよりもむしろ積極的に活用するべきであり，組織内における振る舞いを代理指標として測定することが現実的な解であると主張する。

続くⅤ章では，前章における検討を踏まえ，セキュリティ文化を企業組織に定着させる取り組みについて，教育訓練のあり方に注目し，研究課題の導出を試みている。具体的には，企業組織内で一般的に行われる「標的型メール攻撃訓練」を対象に，効果測定の指標設定の問題と，それらを実施する体制のマネジメントにおける課題について実践面から提示しつつ，これらを通して，セキュリティ文化は企業組織の中心的文化となり得るのかを研究課題として設定している。

Ⅵ章では，前章で導出された課題を明らかにすべく，現実の企業組織での実事例の収集・分析からの考察を加えている。研究方法は，教育訓練，なかでも標的型メール攻撃訓練に

取り組む企業3社（X社，Y社，Z社）に対するインタビュー調査である。この調査から，訓練の実際とその効果や実施するうえでの課題，そしてこれらの実施の周辺的な実務や組織全体の情報セキュリティを推進する体制を明らかにし，セキュリティ文化の醸成に有効な教育訓練の設計とその頻度，および実行体制のあり方を探っている。

Ⅶ章では，前章での企業事例の考察から得られた知見を整理している。まず，訓練としては小規模な 2 社を比較考察し，教育訓練における指標（KPI）を中心に検討している。この指標の問題は，訓練実施の体制と訓練実施主体のキャパシティの問題と密接に絡み，組織的な取り組みや実施主体に対する支援が必要であると考察している。この組織的な取り組みについて，Z 社の事例から，企業組織においてセキュリティ文化を醸成するための教育訓練の内容とその頻度，および実行体制のあり方を検討している。さらに，高頻度の訓練によって情報セキュリティへの認識が維持されることで，組織メンバーは自らの業務と情報セキュリティの関係性を見い出し，これにより情報セキュリティに対する当事者性が生まれ，さらにそれを踏まえた行動が表出し，組織内に定着しているということを確認している。これらをもって，セキュリティ文化は企業組織の中心的文化となり得ると結論付けている。

Ⅷ章では，これまでの議論を総括しながら，前章での考察結果を踏まえて結論として提示しするとともに，本論文の限界と今後の課題を述べている。

また，補論1では，文化の測定の問題に関連するマネジメントシステムと文化について議論している。補論2では，その測定の対象としての「振る舞い」に関して，原子力安全文化において提示されている10traitsの例を紹介している。また，補論3では，情報セキュリティにおいて組織の中核を担うCSIRT(Computer Security Incident Response Team)の現状と課題について検討している。

５　論文の特質

本論文の特質として，以下の点を上げることができる。

第一に，現在社会において重要な課題となっている情報セキュリティに対する取組みについて，OECD(2002)が提出した「セキュリティ文化」という概念から，複数社の企業事例を紹介し，分析したというところである。標的型メール攻撃訓練という限られた範囲の取組みであるが，実際の運営者を中心に組織メンバーに対してインタビューを行い，訓練結果のデータ等も含めた詳細の情報を収集することとができている。

第二に，この「セキュリティ文化」を理解するにあたり，まず，SchienやO'Reilly，Deal & Kennedyといった古典的な組織文化論を紐解くとともに，「文化」そのものの定義ついて，文化人類学などの代表的な定義についても確認しているところである。

第三に，「セキュリティ文化」も含め，現場で使用されるマネジメントシステム等における文化概念に言及し，「文化の測定」についての議論を提示したことである。

第四に，セキュリティ文化の近接概念である安全文化論や高信頼性組織論に触れるとともに，上記マネジメントシステムに関連し，参照例として原子力安全文化について紹介しているところである。安全やセキュリティ，信頼性など一般的な組織文化論においては，必ずしも十分に注目されていなかった分野にも焦点を当てているところに特質がある。

６　論文の評価

情報セキュリティに関する研究と実践において組織文化やマネジメントの重要性が認識されるようになってまだ日は浅い。一方，組織文化研究において，セキュリティという観点から論じられたものは数少ない。本論文はその間隙をうめるものとして位置づけられる。また，実際の関係者に対してインタビューを行うことによって収集した詳細なデータは，非常に貴重である。一方で，本論文には，以下のような課題があるといえる。

第一に，組織文化を議論するときの研究者としての視点である。本論文では，機能主義と解釈主義の双方について言及しているが，そのための議論の混乱も若干生じている。議論そのものは必要な部分もあるが，それぞれの内容についてより深く理解し，検討を進めていく必要があろう。

第二に，研究対象と研究方法についての課題である。本論文では「セキュリティ文化」そのものの醸成とその測定について問題提起をしている。しかし，研究対象として扱っているのは，教育訓練，その中でも標的型メール攻撃訓練という，ごく限られた対象となっている。これについては，今後，制度やリーダーシップなど，論文中でも提示されている他の側面も含めた多面的な分析が期待される。また，研究方法について，単純なインタビュー分析に留まっている。研究の妥当性を高めるには，論文でも語っているようにコード化等を含めたより精緻な分析も求められる。

第三に，概念の整理とそのための先行研究の確認についてである。本論文で使用する概念は，複数の専門領域にまたがって使用されているとともに，実践の現場でも用いられるものである。そのこと自体が本論文の問題意識といえるのだが，時に十分な定義づけが行われないまま議論を進めていると感じられる部分もある。構成上の都合などさまざまな制約もあるかもしれないが，さらに丁寧で緻密な検討が必要であろう。また，それを裏付けるためには，基本的な文献はもちろん，国内外の最先端の研究へのアクセスを試みていくことを期待する。

しかしながら，セキュリティ文化の醸成という視点から企業の実態に迫った本論文は，少なくとも日本においては現状まだ多く取り組まれていない貴重なものであり，理論的にも実践的にも，関連分野に対する一定の貢献をするものと評価できる。

７　論文の判定

本学位請求論文は，経営学研究科において必要な研究指導を受けたうえ提出されたものであり，本学学位規程の手続きに従い，審査委員全員による所定の審査及び最終試験に合格したので，博士（経営学）の学位を授与するに値するものと判定する。

以　上