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-

要旨

2020 年度　経営学研究科

博士学位請求論文（要旨）

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 －

経営学専攻

杉原　大輔

1 問題意識と目的

本研究は、企業組織において「セキュリティ文化」の醸成を図るべく、情報セキュリティに関する教育と訓練のあり方や、それらを支える組織の体制のあり方について考察する。具体的には、標的型メール攻撃に関する教育と訓練を起点として、組織のメンバーに情報セキュリティの重要性が真に認識され、セキュリティ・ファーストな振る舞いがメンバーの内心から表出される状態を生み出すマネジメントに求められる要件や要素を導出することを目的としている。

「セキュリティ文化」とは OECD が 2002 年に提唱した概念であるが、その要旨は、情報ネットワークとそれに接続された情報システムや情報端末の開発者とその利用者に向けた、セキュアな開発と利用の啓発にある。情報ネットワークや情報システムが一部の専門技術者のものであった時代から、一般個人の日常生活空間にもインターネットと小型の情報端末が広く普及し、利用者の数は比較にならないほど増加している現代となっていることからも、このセキュリティ文化の概念はより重要なものとなっている。しかしながら、一部の専門技術者を除けばそのセキュアな利用はあまり意識されてはおらず、OECD が意図したようなセキュリティ文化が広く醸成されることは困難であると言わざるを得ない。

現実にはこれらの情報ネットワークと情報端末を活用して、年間では 370 兆円を超える商取引が日本国内でなされている一方で、この取引に必要な情報、いわゆる個人情報の漏洩といった情報インシデントも多発している。その原因は、情報端末などの利用時における不注意や過失によるものを中心として、故意の持ち出し、システムや端末の脆弱性を利用した外部からの悪意を持った侵入やいわゆるウィルス感染などによる。ここに挙げただけでも、企業組織にとって情報セキュリティ向上の取り組みが求められる範疇は多岐にわたるのだが、なかでも、企業組織に求められる取り組みの第 1 位に挙げられる

標的型攻撃の一種として、外部の悪意と組織メンバーの過失が結び付いたことによる情報の流出として標的型メール攻撃による被害がある。この標的型メール攻撃の手法は、近年増加するフィッシングやビジネスメール詐欺などの手法と軌を同じくしていることからも、個人情報の流出による補償やレピュテーションの低下といった問題への対応としての個人情報の保護という観点だけではなく、企業の競争力の核心であるような機密情報の流出や、直接的な金銭被害を防止するという点でも、これに備えることは重要となっている。

当然、実務の現場においても情報が重要であることはメンバーに繰り返し伝えられ、ハード・ソフトの両面において情報セキュリティ向上の実践がさまざまに取り組まれている。しかし、それは外部環境の変化に対応した、採用する行動パターンの単なる変更、いわゆる Know-How の変更にとどまってしまい、現実の業務の効率とのコンフリクトの種となりやすく、結果としてそれらはなかなか定着しづらい。

そこで、先に述べたような、企業組織が外部の悪意のターゲットとされその餌食となる、または間接的な加害者となることを抑止するためには、ハード・ソフトといった対応だけではなく、これを企業組織の文化から捉え、対応していくことが重要であると考える。すなわち、現代の企業活動において必須のツールである情報ネットワークと情報端末を利用するに際しての、新しい企業文化の醸成が必要であることを訴えるものである。文化からのアプローチは、企業文化が、組織目標の達成のために多様な活動に従事する多様な人々によって構成される集団の特徴として外部からの観察されうるものであると同時に、メンバーの規範であり、社会性そのものであり、それらメンバーの内心の集合体であるがゆえに、重要である。このことから、組織文化は組織そのものとして例えられることも多く、これをいかにマネジメントするのかは喫緊の課題となる。

ここで必要なのは、外部からの情報セキュリティ向上の要求に対応して採用する行動パターンの単なる変更ではなく、組織のメンバーが情報セキュリティの重要性を真に認識し、情報セキュリティを重視することを当然の仮定として内面化し、共有し、それが日常の会話に、振る舞いに表出する状態である。このような状態を目指していかに組織をマネジメントするのかが問題なのである。

そのため、組織のメンバーの思考や行動様式が、情報セキュリティを最重要視するということを意味する「セキュリティ・ファースト」という価値観に則り、振る舞いとして表出する状態こそを「セキュリティ文化」と定義し、このセキュリティ文化を、標的型メール攻撃訓練を軸にして醸成するためのマネジメントの要件とその充足のあり方を析出することが本研究の目的となる。

2 構成及び各章の要約

第Ⅰ章では、まず本研究の提起する問題の前提となる情報漏洩による被害の現状とその原因を確認し、それに対して情報の保護とはいかなることなのかを確認した。そして、これらに対して企業組織は

どのような備えが求められているかを確認し、それらに対して企業組織がどのようなアプローチを取るべきであるか述べた。

現実には、情報端末とネットワークを活用して、年間 370 兆円を超える商取引が日本国内でなされているなかで、この取引に必要な情報、いわゆる個人情報や企業の機密情報の漏洩が多発し、なおかつその規模も拡大している。こういった現状に対して、企業組織には様々な対応が求められるが、本研究ではハード・ソフトといった従来的な捉え方だけでなく、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。具体的な個別の対応に焦点を当てれば、外部から悪意のある標的型攻撃の対応が企業に求められる対応の第 1 位に挙げられているが、その一種である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研究の目的とする。

第 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基本的な研究から確認した。続いて、本稿の目的である組織文化の醸成または変化といった、組織文化のマネジメントに関する先行研究から、求められる要件を整理した。文化人類学を中心とした古典的研究では、機能主義的な議論からメンバーの認識や理解といった個人の内面に着目した解釈主義的な議論へと変化し、それらを踏まえた経営学的視点でも、組織メンバーの行為の意味や価値に対する認識といったメンバーの内心についての議論に注目が集まっていた。本研究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としてこれを認識する。

第Ⅲ章では、目指すべきセキュリティ文化とはいかなるものかについて、中心的な概念を提示した OECD によるセキュリティ文化を踏まえ、その類する先行例のひとつである原子力安全文化と比較をしながら、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た。そこでは、なにより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が見い出されたが、この課題を克服するために求められる要件や要素を織り込みながら、セキュリティ文化が企業組織の文化となったときどのような文化として醸成することになるかを、組織的な事故を防ぐ文化として示された「安全文化」（Reason, 1997）になぞらえて提示した。

第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た。先行研究では、文化を醸成するという試みにおいては、マネジメントの効果の把握、特に成果測定の部分が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経営組織論における組織文化とはメンバーの内心の問題であ

り、その測定の難しさという点にある。しかし、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考えた。

続く第Ⅴ章では、前章における検討を踏まえ、情報セキュリティを文化として企業組織に定着を図る取り組みについて、教育と訓練のあり方を実践の面からの課題の導出を試みる。この目的のため、企業組織内で一般的に行われる「標的型メール攻撃訓練」について確認し、その効果と限界を分析しながら課題を指摘し、その解決策を検討した。そして、この解決策をどのように実現するのか、運用するのかというマネジメントの実践面についての研究課題として、具体的には、訓練や教育の効果測定の指標の設定の問題と、それらを実施する体制のマネジメントにおける課題、そして、これらを通してこれまでに検討したセキュリティ文化は本当に企業組織の中心的文化となり得るのかを、課題として設定した。

第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ることを試みた。研究方法としては、情報セキュリティについての教育と訓練、なかでも標的型メール攻撃訓練に取り組む企業に対するインタビュー調査とした。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と訓練の設計とその頻度、および実行体制のあり方を探った。調査対象は、訓練の対象者数や訓練実績の違いから生まれる差異からこれらを検討すべくＸ・Ｙ・Ｚの３社とした。

Ｘ社の事例は、おおよそ初回の訓練であり、教育内容の理解度のチェックと位置づけられた。それは今後の教育訓練の方向性を打ち出すための組織の状態把握といえる。訓練結果は被訓練者のリテラシーによる差が見出され、先行研究の拡充が果たされた。内容の改訂や階層別の実施といった拡充が今後の課題として指摘できた。

Ｙ社の事例では、年間２回程度の訓練を数年間実施していた。メンバー個人による対応に重きを置いておらず、疑わしい事由に遭遇したときは社内の専門家へ連絡することを周知するための教育と、そうした教育コンテンツへの誘導の役割を担う訓練である。訓練は、多様なメンバーに対する柔軟な教育のトリガーとしての役割を担っていた。また、職位別の訓練を実施しているが、成果指標は役職の高さに反比例しており、役職の高い者ほど訓練の参加が求められることが明らかとなった。そして、Ｘ社との比較では企業規模が大きいことから、組織を細かく分割したブロック制と、ブロック内部にピラミッド構造の情報セキュリティについての体制が構築されていた。

残るＺ社は、Ｙ社と同程度の規模であり、ブロック制とピラミッド構造の体制が採用されていることは共通していたが、長期にわたり非常に高い頻度で訓練を実施していた。月１回という訓練サイクルの高速化は、個人レベルで担当者を指定するという密なセキュリティの情報流通体制の作り込みとそれを活用した訓練実施負担の分散、ブロック単位での責任制と結果の把握によって生まれる競争性によって支えられていた。さらに、長期にわたり蓄積された１次データの分析とそこから得られた知見を基にした積極的な教育内容と訓練の改善があり、組織的な学習がなされていることが見い出せた。この事例は、他社の手本となるような組織体制の構築と運用といえた。

第Ⅶ章では、本研究のまとめとして、前章での企業事例の考察から得られた知見を整理し、まず、小規模な２社を比較考察し、訓練の目的や結果の蓄積の違いから、訓練実施時の成果測定の在り方について論じた。結論は、次のとおりである。まずＸ・Ｙの２社の事例からは、組織の状態把握や情報リテラシー向上という目的のみにおいては、開封率を KPI として実施することは適当である。しかし、対応能力向上という目的においては不適切といえる。また、訓練の KPI を報告率へと転換することは、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。

この組織的な取り組みについては、続く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と訓練の内容とその頻度、および実行体制のあり方として論じた。報告という振る舞いの定着という直接的な目的を果たすためにも、訓練は高い頻度が必要になるが、それにはまず実務的な負担の低減が肝要である。これに対しては、ミクロ的な視点として、教育資料の作成と訓練実施の上流を担う CSIRT と、下流を担う事務局という負担の分散により達成していた。これによりまず報告のボトルネックが解消され、訓練サイクルの高速化の前提が整う。次に、高い頻度による訓練への慣れや飽きが懸念されるが、これに対してはメゾ的な視点として、訓練結果についての責任単位を、組織を分割したブロック制とすることで回避されていた。ブロック制の効果としてブロック単位間の競争が生まれ、ブロック内部では教育と訓練の活性化が図られる。そしてマクロ的な視点からは、仕組みや体制の構築といった成文的な組織の実装の問題だけではなく、これらの活動全体の正統化が重要である。これについては、情報セキュリティ体制の頂点として経営者層が、訓練結果に対して関心を示し、フィードバックすることで正統化されていた。一方で、結果向上への投資となる教育についてはその責任をブロックごと委ねるといったように柔軟性が確保されていることも、教育と訓練の実施主体への権限移譲として正統化を後押しすると考えられた。このような組織の在り方が求められる。

そして最後に、経営組織論の解釈主義的な文脈からも企業の中心的文化としてセキュリティ文化が醸成されたと評価ができるのかを確認するため、少数ではあるがインタビュー調査によって組織メンバーの内心を確認することを試みた。結果として、訓練に対する印象は一様に好意的であり、それは訓練の効果を明確に認識していることによるものであった。それは、報告行動の定着という訓練の直接的な目的が達成されているというだけでなく、情報セキュリティへの認識の向上がもたらされているという効果である。組織メンバーは、高い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、メールを介した情報のやり取りの仕方から、情報そのものの扱い方へと関心の焦点が拡大し、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認識していた。このように、外部的に観察可能な指標の充実とともに、メンバーの内心においてもそれを当然のものとする内心が形成されていた。さらには、訓練が行われることそのものが当然のことであるという認識も形成されていた。これらをもってして、セキュリティ文化は企業組織の中心的文化となり得ると結論付けた。

そして第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、課題に対する結論として提示し、これらを成果とし、本研究の限界と今後の課題を述べて終える。