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-

明治大学大学院経営学研究科

2020 年度

博士学位請求論文

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 －

Developing security culture：

Focusing on targeted email attack training in corporate organizations

学位請求者　経営学専攻

杉原　大輔

目次

図表目次

附言

本博士学位請求論文における以下の構成部分の初出は次の通りであり、これらに加筆修正を加えたものである。

第III章第 5 節
杉原大輔・中西晶（2014）「高信頼性組織（High Reliability Organization）入門　第 2 回：高信頼性組織のプラクティス」経営情報学会誌 Vol.23,No.3,経営情報フォーラム

第VI章第 1 節・第 2 節
杉原大輔（2018）「標的型メール攻撃対応訓練と実行体制の事例紹介 －心理的安全に着目して－」セキュリティ心理学研究 2018, 日本心理学会第 82 回大会, 日本心理学会

補論 3
杉原大輔（2018）「日本における企業内 CSIRT の現状と課題 －NCA 早期加盟チームの実態から－」開智国際大学紀要, 第 17 号, pp.5-21, 開智国際大学

序

情報セキュリティに関する問題は、業種や業態を問わずして、正常な組織プロセスを阻害するリスクに直結する。もっとも直接的なケースでは、中核となるサービスの提供が全くできなくなることがあり得る。間接的なケースであっても、核心的な営業秘密に関するものであれば競争力と利益の源泉を棄損し、サービス提供に付帯して必要となる個人情報に関するものであれば顧客の信用を失墜し、それらの回復には多大なコスト、多大な時間が必要になることは火を見るよりも明らかである。

つまり、現代的な組織において情報の扱いは要であり、安定した事業の継続や発展のみならず、事業やサービスの廃止、さらには組織の継続そのものに影響を及ぼすなど、情報セキュリティ向上の重要性は論を待たない。情報端末と情報ネットワークを活用してなされる商取引は日本国内だけでも 370 兆円を超えている現状[1]では、ゼロリスクを求めて情報端末と情報ネットワークの利用を止めるという選択はもはやあり得ず、堅牢なシステムとセキュアな活用の徹底を追求することが現実的かつ当然の答えとなろう。

情報セキュリティや、情報システム、そして情報セキュリティインシデントという単語からは、表面的にはハッカーとクラッカー[2]の技術のぶつかり合いであり、悪意ある攻撃者が繰りだす新たな手法にシステム管理者や利用者が翻弄され、種々の情報が悔しくも窃取されているかのような印象を受ける。しかし、現実の情報セキュリティインシデントの多くは、情報端末と情報ネットワークの利用者によって引き起こされており、特に単なる不注意が主たる原因であることは各種調査でも指摘されている[3]。

---

[1] 経済産業省（2020）令和元年内外一体の経済成長戦略構築にかかる国際経済調査事業（電子商取引に関する市場調査）。内訳等の仔細については後述する。

[2] ソフトやハードをエンジニアリングするにあたり、高度な技術を持つ人々の総称として「ハッカー」が使われていた。一方で、違法にセキュリティやソフトウェアのコピーガードなどを破ることについてクラックする（割る）という表現を用い、これらを行う者を悪意のある技術者として「クラッカー」と区別するようになった。しかし、報道レベルでは混同してどちらも「ハッカー」として扱われることが多いため（例えば https://www.afpbb.com/articles/-/3203517 など）、これを嫌ってホワイトハッカーと表現することもある。

[3] 仔細については第 I 章で確認する。

これに対し、早くからOECD（1992）はセキュリティ・ガイドライン(Organization for Economic Co-operation and Development Security Guideline)によって、情報保護の重要性を訴えていた。そして、利用者の急速な増加に伴ってこのガイドラインに改定を加え、情報システムの開発者に対してはセキュアなシステム開発を、そして利用者に対しては情報ネットワークへの参加者として情報セキュリティへの貢献を呼びかけ、来たる情報社会が備えるべき「セキュリティ文化」として、基本的な対応について原則として提示した（OECD, 2002）。このOECDによるセキュリティ文化の概念が一般市井にも広く認知されているかは別として、現代の企業組織において情報が重要であることは、組織のメンバーへも繰り返し伝えられている事項であろう。しかし実際の組織内部では、現場オペレーションを考慮しないポリシーが制定され、それゆえポリシーは業務効率の名の下に反故にされ、ポリシーの遵守状況を確認する監査も書類だけでパスするという表面的なセキュアが出来上がり、結果として情報そのものやその媒体の扱いにおいて注意が欠ける、すなわち情報セキュリティへの意識が低いという現実が生じている。

組織が持つべき情報セキュリティへの意識という点においては、組織の目的的にも最大限の注意が向けられていることが期待されていたにもかかわらず、その期待が見事に裏切られた事例として、2015年に発生した日本年金機構からの個人情報の漏洩が挙げられる。電子メールや携帯電話のショートメッセージサービス（SMS）といった媒体を利用したメッセージの伝達は、日常生活の一部となっているが、外部からの悪意ある電子メールを受信したことが起点となり、大量の個人情報の流出を招いた事例である。これは、外部からの悪意、簡単に言えば標的型メール攻撃[4]を受け、マルウェア[5]に感染し、個人情報が流出したのだが、内実としては大量に保有する個人情報の保護を目的として設計されていた業務システムと運用ルールが整備されていたにもかかわらず、業務効率を優先したい現場の要望によって、これから逸脱した問題含みの業務プロセスが内部的に公式化されていたことによる。このプロセスに対しては、そもそも問題があることを上層部は認識してか、個人情報の含まれるファイルに対して利用権限の制限やパスワードの設定といったある程度の予防

[4] 無差別にメールを送信するのではなく、特定の組織や個人を狙ってメール送信し、添付ファイルなどからマルウェア感染を狙うもの。開封を促すためにメッセージを、その組織や個人に合わせ個別化するなどの特徴がある。第Ⅴ章にてもう少し詳しく説明する。

[5] ウィルス・ワーム・トロイの木馬といったプログラムコード群の総称。ハードウェア／ソフトウェアの脆弱性を利用して侵入・感染を試みるもので、その多くは、PC内部のデータやキーボードからの入力を外部に送信することを企図して制作されている。

的なルールを設けたにもかかわらず、現場レベルにおいてはその最低限のルールさえ遵守されていなかった。このような組織内のオペレーションの状況に加え、こういった標的型メール攻撃についての教育はなされてはいなかった。また、メールの文面も業務を騙るものであり、当該個人に添付ファイルの開封を避けることを期待することは難しかったと言える。さらには、当該組織にはCISO[6]とその補佐官が任命されており、現場レベルでも情報セキュリティインシデントへの対応のアドバイザーが指名されてはいたものの、いずれの役割も肩書のみの運用であり、実務的には対応がなされなかった。斯かる状況の重なりから、事態の認識から取るべき対応までが遅くなり、被害が拡大し、結果として 125 万件という大量の個人情報が流出した[7]。

この事例では、個人情報を扱っているという認識の希薄さによる問題は、現場の個人レベルで顕在化したわけだが、現場の業務効率優先を認める組織的な姿勢があり、情報セキュリティについての教育も手薄であり、組織的な体制は有名無実だったように、組織全体に根深く広がっていた問題である。このように、情報セキュリティに対する社会的な要請に対して、表面的には情報セキュリティへの認識と備えを持っているように見えるが、本来的に求められる認識と運用には程遠い「名ばかり CSIRT」（近藤ら, 2018, p.45）のような実際が、この他の一般的な組織においても危惧されてる[8]。

この日本年金機構の例では、情報セキュリティが破られることで、流出した個人情報から実損害に結び付いたという報告はないが、対象となる個人への通知や新規の基礎年金番号の振り出しが行われるとともに、年金の手続きに関連したサービスや Web サイトによる情報提供が長期間停止した。これが営利企業であれば、商品やサービスの提供といった企業活動そのものが停止してしまうだけでなく、長期を掛けて育てたブランドやレピュテーションを著しく毀損することになる。電力やガス、通信などといったインフラ的なサービスを提供する組織であれば、影響の範囲はより広く、多様な 2 次的損害が発生することが危惧される。

---

[6] Chief Information Security Officer：最高情報セキュリティ責任者。業務内容の仔細については、情報処理推進機構（2020）「企業の CISO 等やセキュリティ対策推進者に関する実態調査」などを参照されたい。
https://www.ipa.go.jp/security/fy2019/reports/2019DL_index.html#L1

[7] 仔細については、日本年金機構における不正アクセスによる情報流出事案検証委員会（2015）「検証報告書」を参照されたい。
https://www.mhlw.go.jp/file/05-Shingikai-10201000-Daijinkanbousoumuka-Soumuka/0000095309.pdf

[8] Computer Security Incident Response Team：シーサート。情報セキュリティに関するインシデント対応に特化したチーム。仔細については第Ⅴ章第 1 節第 3 項および補論 3 にて詳説する。

こういった特定の組織などを狙う標的型の対となる無差別型のものとして、大手通販サイトや宅配事業者や金融機関を騙り、日常生活においてこれら事業者のサービスを利用している消費者個人を誤認させ、個人情報の窃取を狙う「フィッシング（Phishing）」も増加を続ける一方であり、2020 年 6 月単月で 1 万 6 千を超える報告が寄せられている。これは前年対比で 3 倍となっている[9]。この手法の土台として、企業組織の Web サイトなどが不正に書き換えられ、踏み台にされるケースもあるが、これも標的型メールによるマルウェア感染がその起点となっていることがあり、企業組織側の備えも必要となる。

無差別型の類例としては、電子メールや SMS を利用し、実在するサービスを騙り、利用者の注意を引く文章を送り付け、真正なものと誤認させるような精巧な偽の Web サイトへ誘導し、個人情報の入力を促すのが主な手口となる「スミッシング（SMising）」があり、これにより個人情報の窃取にとどまらず、直接の金銭的被害も増加している[10]。これは標的型メール攻撃と軌を同じくしていることから、個人にも情報セキュリティに対する認識の向上によって被害を防ぐことが期待できる。しかし、無差別型とは言え、送信者がメールアドレスや電話番号といった個人情報を大量に保有していることが前提となり、その個人情報は標的型メールによってマルウェアに感染した情報システムから窃取されたものであると考えることもできる。この反対に、個人に対して無差別的に行なわれるフィッシングやスミッシングによって窃取されたメールアドレスなどの個人情報が標的型メール攻撃に利用されていることも考えられることから、やはり組織そして個人ともに情報セキュリティに対する認識の向上が求められている。

事業やサービスの停止は企業組織にとって一大事であるが、民間営利企業のサービス提供においても情報セキュリティを重視しなかったことが原因で大きなインシデントが発生している。例えば、大手コンビニエンスストアチェーンが新たに提供した決済サービスでは、個人認証の設計の甘さに気づいた悪意ある不正アクセス者の餌食となり、総額で 3000 万円を超える不正利用が発生し、結果としてサービス提供から 3 か月でサービスの廃止に追い込まれた[11]。これは、資金決済のオンラ

---

[9] フィッシング対策協議会（2020）「2020/06 フィッシング報告状況」
https://www.antiphishing.jp/report/monthly/202006.html

[10] 「スミッシング」と呼ばれるもの。たとえば、読売新聞オンライン「ネット不正送金急増　4 か月被害１４４件 過去の年間最多上回る」2020 年 5 月 23 日版
https://www.yomiuri.co.jp/local/aichi/news/20200522-OYTNT50103/

[11] 株式会社セブン&アイ・ホールディングス 2019 年 8 月 1 日付けプレスリリース
https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf

イン化、キャッシュレス化という現代的な要求への対応のなかで、協業他社とのシェア競争を重視し、スピード感にこだわったことが、情報セキュリティを顧みない拙速なサービス提供につながったといえる。情報セキュリティに対する優先順位の低さが露呈した一例であり、著名で大規模な企業組織であっても組織が持つべき情報セキュリティへの意識が薄いと言わざるを得ない。

営利組織のビジネスの環境については、日本国内での企業間取引（B to B）においてインターネットをベースとした電子商取引（E-コマース：EC）の市場規模は、2017 年に 300 兆円を超え、2019 年には 352 兆円に達している。B to C においては、日本国内で物販約 10 兆円、サービスおよそ 7.2 兆円、デジタル（コンテンツ）約 2.1 兆円と合計で 19.3 兆円を超え 20 兆円に迫る額の取引がなされており、B to B と合わせると 370 兆円を超える[12]。それぞれの市場における EC を率で見ると、B to B では 31.7%、B to C では 6.76%となっている。B to C のなかでも物販についてはスマートフォン経由による取引が 42.4%と 4 割を超えた[13]。さらにはこのスマートフォンの普及から活発になっているネットオークションやフリーマーケットアプリケーションを活用した C to C は 1.7 兆円を超えており、インターネットを介した商取引は合計で 373 兆円を超えることになる。

個人情報という保護客体だけで考えれば、企業が個人と直接やり取りする B to C と、C to C を媒介するサービスやシステム・アプリケーションを提供する企業は、膨大な量の個人情報扱う。これをビジネスにおいて積極的に扱いたい企業組織側と、保守的に扱いたい、もしくはこれについて関心の無い個人側という対立構造であるが、企業がビジネスチャンスとして積極的に活用したいのであれば、例えば個人情報保護法といった法的要請とその適合のみならず、デューディリジェンスの観点からも情報セキュリティに対してはより積極的な企業文化となることが求められている。しかし、企業の実務の文脈において語られる文化とは、これを経営課題の解決における機能的なものとして捉え、ルールとマニュアルを前提とした Know-How の整備や行動の標準化といった、特定の行動パターンの追求に止まってしまう。これに対して、本稿では、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、当然のものとして共有され、それが、日常の会話に、振る舞いに表出する状態としての「セキュリティ文化」を企業組織において醸成することを目的とする。そこで、この達成に求められる要件や要素を確認しながら、現実の組織の活動からさらなる要素や要件を導

[12] 経済産業省（2020）「令和元年内外一体の経済成長戦略構築にかかる国際経済調査事業（電子商取引に関する市場調査）」

[13] 経済産業省による推計値（同上書, p.37）。

き出したいと考えている。それらを踏まえ、現実の企業組織の実務においてどのように活用すべきかといった知見の提供につながることも期待する。

本稿の構成と見通しは次のとおりである。

まず第Ⅰ章において、情報セキュリティにまつわるインシデントの発生状況やその被害の様態、そして情報の保護についての基礎的な定義を確認しながら、それらが棄損される原因などについて整理する。そして、こういった情報セキュリティインシデントを防ぐためにも企業組織において、組織の文化としてこれに取り組んでいく必要性と、取り組みの具体的手段として標的型メール攻撃についての教育と訓練を主題として選択する理由を説明する。

第Ⅱ章では、企業組織の文化としてセキュリティ文化を醸成する。または、セキュリティ文化へと転換していくという試みの前提として、文化および組織文化とはどのようなものであり、文化はいかに形成されるのかということについて基本的な研究から確認する。続いて、本稿の目的である組織文化の醸成、ないし変化または変革といった、文化を何らかの方法でマネジメントする試みについての先行研究を確認し、要件を整理する。ここまでの文化の醸成、そして変革の要件を踏まえ実務での留意点として再度検討整理する。

第Ⅲ章では、目指すべき組織文化としての「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（2002）による「セキュリティ文化」を踏まえ、先行例としての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ことにおける課題を検討する。そして、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表出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）を下敷きにしながらその定義を試みる。

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する。それは、文化はマネジメントの対象としてなじまないという指摘、具体的には、マネジメントである以上の取り組みの成果を評価する必要があるが、成果の測定についての問題が指摘されていることによる。このため組織文化の醸成や変革の手段として教育や訓練を選択し、その成果の測定の対象として振る舞いを用いることの妥当性についてを、これらに言及するマネジメントについての先行研究から確認しながら、これが可能であるならばどのような課題があり、企業組織においてはどのように取り組むことで課題を乗り越えることができるのかを検討する。

続く第Ⅴ章では、前章における検討を踏まえ、標的型メール攻撃訓練を手段としてセキュリティ文化を醸成していく取り組みにおいて、明らかにすべき課題を設定する。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とその効果について確認し、限界と課題を指摘し、その解決策を検討する。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実践面についての課題として整理する。

第VI章では、前章で導出された課題を明らかにすべく、現実の企業組織で取り組まれている実事例を確認し、考察していく。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してインタビュー調査を行い、訓練の実態とその効果の実際や、訓練を行う中で認識する課題とその解決について、そしてこれらの実施の実務や企業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内容とその頻度、および実行体制のあり方について、考察を加えながら探っていく。

第VII章では、本研究のまとめとして、前章で行った事例ごとの考察を、事例の比較を通した再整理によって掘り下げていくことで、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について検討する。そしてこれらの事例においては、先行研究で示されていた文化の醸成や変革に求められていた要件はどのように充足されていたか確認する。最後に、これらの実務的・機能的な面だけではなく、文化の解釈主義的なアプローチとして、メンバーの組織内の活動の実態や、標的型攻撃メール攻撃に関する教育と訓練の効果、訓練の実行体制、そしてこれらを踏まえた組織の内部の状況に対する組織メンバーの認識を、メンバー個人に対する個別のインタビューによって調査し、標的型メール攻撃訓練を通じてセキュリティ文化は組織の中心的な文化として醸成されうるのかの確認を試みる。

第VIII章では、本研究の結びとして、これまでの取り組みを要約しながら振り返り、事例の分析を通した考察から得られた知見を、企業組織においてセキュリティ文化を醸成するための要件として整理しながら結論として提示する。併せて本研究の限界と今後の課題を述べる。

I　本研究の目的とその背景

1 情報セキュリティインシデントの現状とその原因

(1)　情報セキュリティインシデントの損害の現状

情報セキュリティインシデントがニュースで取り上げられることは日常的である。この情報セキュリティインシデントの例として、被害が広範にわたるため世間の耳目を集めるという意味においても、まず挙げられるのが、組織からの個人情報の漏洩である。これはパブリック／プライベートとセクターを問わず発生しており、日本においては、JNSA による（Japan Network Security Association:　NPO 法人日本ネットワークセキュリティ協会）「2018 年情報セキュリティインシデントに関する調査報告」によれば、2018 年中に発生した個人情報の漏洩は 443 件発生しており、対象となる個人情報は 560 万人強、推定される損害賠償額は 2,684 億円にのぼっている[14]。前年対比でも依然として増加傾向にある（表 1）。

情報セキュリティインシデントの検知から内部的な処理、被害者への通知、その後の対応といった組織側の損害額に関しては、Ponemon（2018）が行った、世界の主要 13 か国、2 地域（アセアン・中東）と広範な調査によって、その平均額が次のように示されている（表 2）。増加率は 6.4%と、こちらも増加している。コストとしては非常に高額である。

表 1：日本国内における情報漏洩の実態とその規模

	2018 年データ	2017 年データ
漏洩人数	5,613,797 人	5,198,142 人
漏洩件数	443 件	386 件
想定損害賠償額	26,845,743 万円	19,142,742 万円
1 件当たりの漏洩人数	13,334 人	14,894 人

出典：JNSA（2019）「2018 年情報セキュリティインシデントに関する調査報告」より筆者作成

[14] 2018 年 1 月 1 日から 12 月 31 日までに、当該組織からプレスリリースなどによって公表されたものを集計したもの。

表2：世界各国における情報漏洩による平均損害額

	2018年データ	2017年データ
n数	477	419
損害額	386万ドル	362万ドル

出典：Ponemon (2018)より筆者作成

(2) 情報の保護とは

このように非常に高いコストとなることが予想される情報セキュリティインシデントであるが、情報を保護するということはいかなることかについて、その用語や定義を確認したい。OECD（1992）による情報セキュリティ・ガイドライン（Guidelines for the Security of Information Systems）[15]によれば、

・利用可能性(availability)：データ、情報、情報システムのアクセスと利用とが決められた手順で適時にできること。
[認可されたエンティティが要求した時に、アクセスおよび使用が可能である特性][16]

・機密性(confidentiality)：データと情報が正当と認められた人間、メッセージ、プログラムのみによって、正当と認められた時刻と手順で開示できること。
[認可されていない個人、エンティティまたはプロセスに対して、情報を使用させず、また、開示しない特性]

・完全性(integrity)：情報及び処理方法が完全かつ確実であることを保護すること。
[正確さ及び完全さの特性]

という3点が「個人データ等の保護」であるという。

ここで、情報セキュリティについても、その定義を確認しておきたい。

先のOECDによるセキュリティ・ガイドラインと、ISO/IEC[17]では以下のように示されている。

---

[15] 2002年に改訂されている。新たに盛り込まれた内容については次章にて確認する。

[16] [カッコ]内はJIS Q 27000: 2014（ISO/IEC27000: 2014）情報セキュリティマネジメントシステムによる定義。このなかの「エンティティ」は「"実体""主体"などともいう。情報セキュリティの文脈においては、情報を使用する組織及び人、情報を扱う設備、ソフトウェア及び物理的媒体などを意味する」と注記される。（p.187）

[17] International Organization for Standardization：国際標準化機構／International Electrotechnical Commission：国際電気標準会議

・情報システムがその利用可能性、機密性、完全性に障害が発生し、その障害が危害を引き起こした場合、その情報システムに依存する人々の利益をこの危害から保護すること（OECD, 1992）

・通常、適切な行動をとることにより、事故または悪意に基づく行為からデータおよび資源を保護すること（ISO/IEC, 1998）

この基礎的な定義について名和（2005）は、前者を情報システムの不具合と利用者の関係について、後者をシステム障害への情報システム保有者の姿勢として説明している（名和,2005,p.23）。

こういった基礎的な定義を踏まえ、2000 年代に入り情報システムと情報ネットワークの活用が進むと同時に、企業経営に ISO9001 を中心としたマネジメントシステムの導入も進むことで、2002 年に ISMS（Information Security Management System）が登場する。当初は情報技術に関連した事業主が認証の対象であったが、翌年に全業種に対象が拡大されたことで次のような定義が提示される。

・外部からの侵入・内部での不正取得を防ぐ IT 技術と、リスクを洗い出し最小化を図っていく情報リスクマネジメントとしての内部統制の 2 面から構成される、物理的・技術的・手続的・人的といった 4 面からの継続的な情報に関する危機管理の総体（藤谷, 2003）

・組織内の各種情報を多方面のリスクから防衛し、安定的な事業継続を確保しながら、経営リスクを最小化し、企業価値向上を実現する継続的なマネジメントシステム（吉田, 2004）

・情報処理システムと、これらに関連する人的資源、技術的資源、知的資源などの組織上の資源からなり、情報を提供し頒布するものである情報システムを誤ることなく運転すること[18]（名和, 2005）

これらの定義は、情報システムと情報ネットワークを活用した企業活動が増えたことで情報資産の重要性の認識が高まり、これを保護するために情報セキュリティの問題を企業組織の経営におけるリスクマネジメントの対象として捉え、マネジメントシステムによって統制するとしている。サイバーセキュリティはあくまでそのうちの 1 つであると同時にツールでもあるという位置付けとなる。

[18] 本文中では、ISO/IEC2382-1 による情報システムの定義を踏まえ、情報セキュリティの「目的」として表されている。

このように、情報システムと情報ネットワークを活動の基盤とする企業が増加し、情報資産の価値が高まったことにより、その管理と運用についてISMSのような認証規格が登場することとなった。しかし、ISMSもサイバーセキュリティのみを対象としているわけではない。サイバーセキュリティは、マネジメントシステムによる統制の一手段・一部と位置づけられている。先の藤谷などによる定義が導かれた2000年代前半においては、情報システムと情報ネットワークの利用は当然に企業活動の一部であるが、インターネットが商用開放されたのはその直前である 1998 年であり、これをベースとして商業活動を行う企業はまだ多くなかったことからも、ネットワークやインターネットに対する比重はまだ小さいように読み取れる。しかし、次節で詳しく確認するが、情報漏洩は紙媒体での流出や音声での情報の盗取、そしてUSBなどの記憶媒体やラップトップPCの紛失によって発生することが多く、目に見えない電子データへのセキュリティ認識だけではやはり不十分であるという点で、現在においても十分通用するものであるといえる。

ただし、先に確認したようにBtoB・BtoCともにインターネット上のみで完結する取引が増加の一途にある現在においては、サイバーセキュリティの比重は高くなっていることは間違いなく、こうした変化に伴って2005年に国際規格としてISO/IEC27001:2005に発展し、現在の情報セキュリティマネジメントシステムの原型となった。ここでの情報セキュリティの定義は、先のOECD（1992）によるセキュリティ・ガイドラインを踏まえ

・情報の機密性、完全性及び可用性を維持すること

という辞書的定義がなされる。こののち数度の改定を受けISO/IEC27001:2013が最新の規格となり、このなかで「真正性、責任追跡性、否認防止、信頼性などの特性を維持することを含めることもある」という注記がなされた。

これらの用語の定義は以下のとおりである。

・真正性：エンティティは、それが主張する通りのものであるという特性[真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する][19]
・責任追跡性：あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できることを確実にする特性（JIS X 5004）

[19] [カッコ内]は、JIS Q 13335-1: 2006 用語及び定義　による

・否認防止：主張された事象又は処置の発生、およびそれを引き起こしたエンティティを証明する能力[ある活動又は事象が起きたことを、後になって否認されないように証明する能力]

・信頼性：意図する行動と結果とが一致しているという特性

これらは、組織内部での情報システムの利用者の拡大に伴って、利用者の本人認証を確実にすること（真正性）、データなどへのアクセスログの確保と解析能力を担保すること（責任追跡性）、文書作成者の特定ができること（否認防止）、情報システムが安定して稼働し、求める水準を達成すること（信頼性）を情報システムとその保有者に求めるものである。

このような変化は、次のように捉えることができよう。旧来までのサイバーセキュリティは情報セキュリティの一部であった。表現を変えれば、マネジメントシステムを土台とする情報セキュリティのサブセットとして位置していた。それは、メインフレームと呼ばれた大型のコンピューターがいわゆる電算室などに据え置かれ、一部の関係者が専門技能を持って運用するものであったからである。ある意味で閉じた狭い世界であったものが、情報ネットワーク化に伴ってホスト／クライアントというシステムの構成になり、組織内での利用者が増え始めた。これにより多くの業務のペーパーレス化が進み、電子データの比重が高まった。さらには、技術の進展と端末のモジュール化によって情報端末が低価格化し、従業員１人に対して１台の貸与も一般的なこととなり、組織内の情報ネットワーク構成は膨大なものとなったことで、情報ネットワーク内で分散してデータを保持し処理されることが多くなった。そして、端末の小型化により組織の外部からサイバー空間を経由してシステムに接続し、処理が完結するに至っている。

このように、電子データで処理される業務が増え、関与する人の数も増え、それによって求められる要件が増えた、すなわちサイバーセキュリティの比重が大きくなっているのだ。ここで扱われる電子データは、情報の処理という観点においては、多量に移動させることができ加工も容易であるというメリットをもたらしたのではあるが、この反面として一瞬にして多量が漏洩し、改ざんが容易であるというデメリットももたらされたのである。加えて、リアルタイムでその漏洩を検知することが難しく、ハード／ソフトウェアだけでなくこれらを扱う人間のヒューマンエラーといったように必ずセキュリティホールがあること、そして目に見えないという点がデメリットとしてこれに加わるため、リスクも大きく対策が急務である。また、情報の流出だけがリスクではない。情報ネットワークとこれに接続した情報通信機器で構成される情報システムが企業活動の基盤となっており、名和（2005）の定義にあるように、これが外部からの悪意によってシステムダウンしたり、

ランサムウェアなどによって情報システムの正常なオペレーションが妨げられることを防ぐことも情報セキュリティの範疇であり、これらの点でサイバーセキュリティの重要性が高まっていることがわかる。これを前提とするならば、情報セキュリティの向上には、まずサイバーセキュリティへの認識を高めることで、紙媒体や物理的セキュリティを含めた情報セキュリティ全体に対する認識をもたらすことができると捉える方が自然であり、まず身近な PC や情報ネットワークの利用における情報セキュリティの認識を高めることが現代的なアプローチであると考える。

(3) 情報セキュリティインシデントの原因

前項で確認した情報保護の基本的な 3 つの要件である、利用可能性、機密性、完全性が破られる原因は、吉田（2004）によれば①過失行為型、②故意行為型、③不正アクセス型、④ウィルス型[20] の 4 つに整理されている。①と②は組織内部の人的要因として理解でき、③と④は組織外部からの悪意と内部の機器的要因の複合として捉えることができる。「①過失行為型」は、データの入った USB メモリやラップトップ PC ごとの紛失、メールの誤送信、アップロード時の設定ミスなど、なんらかの人間の行為を起点として発生するものである。「②故意行為型」は、情報にアクセスできる権限を与えられた従業員やそのデータ処理の委託先企業の従業員などが、意図的に情報を改竄したり、持ち出すことである。この意図的な行為を防止することは容易ではない。予防の手段や仕組みについて関係者を性悪説に基づいて構築せねばならないからである。さらに、意図的な漏洩である場合は情報の売買に結び付くことが予想され、これを買い受け悪用しようとする者によって、ア）迷惑メール・迷惑電話・迷惑ダイレクトメール増加、イ）Web サービスのアカウント乗っ取り、ウ）クレジットカードの不正使用、エ）振込め詐欺、特殊詐欺の被害などが、個人データ等が漏洩された当該個人に起こる可能性が生じる。実際に、この「②故意行為型」に含まれる意図的漏洩のケースとして、2016 年に実際に発生した企業事故では、個人情報が名簿業者に売却され、当該顧客宛てのダイレクトメールおよび勧誘電話から発覚した経緯がある[21]。

---

[20] 現在では、悪意あるツールとしてマルウェア（malware）と呼ばれることが一般的。プログラムやデータファイルを媒介とするウィルスと、単体で機能するワーム（worm）やボット（Bot）は厳密には別のものとされるが、ここでは一括してウィルスとする。

[21] 2014 年 7 月 9 日付ベネッセ HD ニュースリリース https://www.benesse-hd.co.jp/ja/about/release_20140709.pdf 事件の経緯や複合的な原因については、樋口晴彦（2018）ベネッセ顧客情報漏えい事件の事例研究, 千葉商大論叢, Vol. 53, No.1, pp.155-171 を参照のこと

「③不正アクセス型」、「④ウィルス型」については、組織の利用する情報機器のハード・ソフトの脆弱性を突いて情報を引き出すことを企図した外部の悪意によるものである。このパターンには、ア）企業がなかなか情報の漏洩に気づかない、イ）短時間に大量のデジタルデータが流出する、ウ）インターネット上に漏洩されたデジタルデータの回収は事実上不可能である、エ）社会の関心が高く注目を浴びる、オ）犯人の特定は非常に困難である、というような特徴がある（吉田, 2004）。業務において顧客の情報を取得活用する企業にとっては、漏洩件数の多少によっても影響度が大きく左右されることから、「③不正アクセス型」、「④ウィルス型」においては、大量の漏洩を容易に引き起こすインターネット上の漏洩防止、いわゆるサイバーセキュリティ対策が非常に重要となる。

いずれにせよ、個人情報漏洩を起こした企業の側では、ア)漏洩原因の調査・対応によって生じる時間の損失・調査費・マスコミ会見・謝罪広告・クレーム処理、イ)民事・刑事上の責任によって生じる損害賠償責任・お詫び金・安全管理義務違反・第三者提供違反などの刑事罰、ウ)社会的信用の失墜・企業イメージダウン、エ)風評悪化による従業員の士気や社内のモチベーション低下などが起こる可能性が生じる。

この問題の特徴的なことは、たとえ企業側に過失がなく、運悪く不正アクセスや標的型攻撃等の被害者となった結果の漏洩であったとしても、個人情報等の管理責任、漏洩の結果責任を問われる点である。また漏洩に至らなくとも、個人情報等の利用の過程でコンプライアンス違反が認められた場合の課徴金は、EU 発の GDPR などによって巨額化している[22]。こういった法的・経済的制裁のみならずその後生じる風評悪化などの社会的制裁を受けるリスクによって、経営上の判断において個人情報等の積極的活用が委縮しかねないという問題もはらんでいる（白石, 2018）。

ここまで述べてきた情報セキュリティインシデントの原因については、Ponemon（2018）によれば、情報セキュリティインシデントの発生源としては、いまだに現役の従業員が中心的なものとして推定されており、彼らの不注意やヒューマンエラーに関連することが多いとしている。各種の調査では具体的な原因の内訳については表 3 のようになっている。

[22] 制裁金の上限基準が、企業の全世界年間売上高の 2%、または、1000 万ユーロのいずれか高い方と定められている（第 83 条第 4 号）。実際のケースとして 2019 年 1 月の米国 Google 社に対する 5000 万ユーロ（個人情報の利用の明示の不明確さに対して）、英国 British Airways 社に対する約 1 億 8000 万ポンド（2018 年に発生した個人情報漏洩のインシデントに対して）などが有名。

表3：データ漏洩のパターン

データ漏洩のパターン	（件）
人的ミス	11,347
特権保持者による不正使用	10,490
物理的窃盗及び紛失	9,701
DoS 攻撃（Denial of service attack：サービス妨害）	9,630
その他すべて	8,886
クライムウェア[23]	7,951
Web アプリケーション攻撃	5,334
POS への侵入	534
サイバースパイ活動	247
ペイメントカードスキミング	102

出典：ベライゾン（2016）データ漏洩／侵害調査報告書より筆者作成

それらの要因を整理したものが表4である。まず「内部犯行」に分類されるものが、前述の「②故意行為型」に該当する。このような悪意のある内部者による持ち出しなどの積極意思に基づくものは、合わせても5%未満と僅かである。これらは、先のOECDによる「個人データ等の保護」の定義による「機密性」という観点からは、退職者や異動などによるデータ等へのアクセス権の与奪管理の漏れといったような不作為が起因となるため、管理者側の認識の向上が必要である。また、ここでいう内部者については、下請け・外注といった関連組織も含めた問題でもあり、単一組織外にも内部統制の理論を拡張し、いかに機能させるのかという問題（藤谷, 2003）でもある。

次に「通信傍受・窃盗」については、入館者や設備利用者の把握・管理といったような物理的なセキュリティの問題がベースとなるが、サイバーセキュリティと密接に関連することがわかる。商用の高度・大規模なレベルにおいては、RooterやHub、無線設備といった情報ネットワーク接続の起点となる通信機器の一部の製品について、ハードウェアレベルでのバックドアの存在も指摘されており、機器の購買行動に影響が出ている。

ここまでにおいて外部の悪意と表現してきた「サイバー攻撃」に分類されるものについては、最多がマルウェア感染であり、これに続くものが標的型メール攻撃となっている。

[23] Crimeware：ウィルスやワーム、マルウェアなど何らかの犯罪目的に作成されたプログラムの総称であり、これらを別個に識別しない場合に用いる。

表4：企業内の情報セキュリティインシデントの発生状況とその内訳（複数回答／n=665）

流出の要因	流出の経路（仔細）	割合（%）
内部犯行	退職者による不正持ち出し	2.1
	従業員による権限外アクセス・持ち出し	2.0
	システム管理者による権限外アクセス・持ち出し	0.3
通信傍受・窃盗	PC・ストレージメディア・文書等の窃盗被害	5.9
	データ通信・音声通信の傍受	0.3
サイバー攻撃	マルウェア感染	26.0
	標的型メール攻撃	17.3
	DoS・DDoS（Distributed Denial of Service）攻撃	8.6
	Web アプリケーションの脆弱性攻撃	5.6
	なりすまし	4.8
	ミドルウェア・OS 等の脆弱性攻撃	2.7
	アカウントのハッキング	1.2
ヒューマンエラー	メール・FAX の誤送信	37.1
	外部ストレージメディアの紛失・誤留置	33.7
	社員 ID・ビジネス文書等の紛失・誤留置	19.5
	システムの設定ミス・操作ミス	15.9
	機密情報の誤アップロード	4.1
その他	特になし	29.2
	その他	1.1
	無回答	0.5

出典：NRI セキュアテクノロジー「過去 1 年間で発生した事件・事故」企業における情報セキュリティ実態調査 2017 より筆者作成

最多であるマルウェアは、ウィルス・ワーム・トロイの木馬といったプログラムコード群の総称であるが、その多くは、ハードウェア／ソフトウェアの脆弱性を利用して侵入・感染を試みる。篤志家などによって発見された脆弱性は、対策が見出された上で公表されることが通常であるが、当然にタイムラグがあり対策とともに公表されるまでの間にも感染の危険は存在し続けることとなる。さらに、マルウェア感染・アプリケーションやソフトの脆弱性を足掛かりとした攻撃は、ハードやソフトの脆弱性に対してメーカーやベンダーによって配布されるアップデートや対策パッチの施工

漏れ、設定のミスなどによることが多い[24]。これも管理側の問題といえるが、数多くの端末を完全に管理することはなかなか難しく、これに加えてシステム管理者が把握していない IT 機器などを事業部門が独自の判断で利用しているといったいわゆる「シャドウ IT」もこの問題を大きくしているという現実がある[25]。同時に、このシャドウ IT へのアクセスにおいて次で説明する「なりすまし」の被害も懸念されており、情報システム部門やセキュリティ担当部門が関与することなく利用されるシャドウ IT については、組織全体のセキュリティ認識の向上がその活用において重要になるであろう。

なりすましやアカウントのハッキングは ID とパスワードの組み合わせを推測し、または何らかの方法で取得して本人に成り代わることである。企業組織の内部では、ある一定の法則に従って社員番号や氏名とそのイニシャルなどの組み合わせなどで合成された ID が付与されることが一般的であり、ビジネスの遂行において不特定多数と交換される名刺に記載される個人アドレスと共通する運用であることも多く、その取得や推測は手間ではあるが不可能であるとは言い難い。そして利便性や管理の問題からこれを複雑化することは実務的な観点からは難しいであろう。組み合わせのもう一方であるパスワードについては、設定するパスワードの強度は利用者のモラルに依存することになると同時に個人の管理の問題でもあり、利用者の情報セキュリティに対する認識のレベルに依存することになる[26]。また、パスワードの強度と利便性は相反する関係にあり、堅牢性の高いパスワードの強制は利便性を損ね、ログインの手間を省くためにログオフしないという運用につながりかねない。さらに、必ずしも桁の多さが堅牢性を高めることにはつながらないという指摘もあり（高橋, 2018）、多要素を活用した認証といった現代的な対策が求められている。一般の利用レベルでは、情報ネットワークに接続され利用されている Web カメラや無線 LAN などのアクセスポ

---

[24] Government technology (2002) “Security First”では、米国国防総省の調査結果に基づき、外部からの攻撃によるインシデントの 97～98%は技術的問題ではなく、パッチの適用漏れ・設定ミスに起因していると指摘。
https://www.govtech.com/security/Security-First.html（最終アクセス 6/30/2020）

[25] 例えば、US DataVault (2017) Building Trust in a Cloudy Sky では、事業部門の独自の判断によるクラウドシステム利用の実態とその問題について議論している。
http://usdatavault.com/library/Building-Trust-in-a-Cloudy-Sky.pdf?fbclid=IwAR2SrwZWcuHNpxPlGNp4WC9EQ61IkTgANeg1umYJ1rqlcHNrKiMIfoC1kyw

[26] パスワードをこまめに変更することも推奨されていたが、現在ではその手間などを前提として否定的な論調が増えている。例えば以下など https://blogs.technet.microsoft.com/secguide/2019/04/24/security-baseline-draft-for-windows-10-v1903-and-windows-server-v1903/ (2019/5/19 最終アクセス)

イントの設定が出荷状態のまま利用されていることによって管理者権限を悪用されてしまう危険が指摘されており、一般家庭での利用を含め、IoT の活用が飛躍的に増加するであろう今後において注意喚起がなされている[27]。

一方で、ログインしたまま PC を放置・離席するというような個人のセキュリティ認識レベルの問題だけではなく、職場やグループ単位で共通の ID やパスワードが使われるというように、業務遂行上の簡便さを優先させがちな集団レベルでの情報セキュリティ認識の問題もまたここに含まれよう。また、ID やパスワードをソーシャルエンジニアリング[28]などによって窃取されることもあり得るため、必ずしもサイバーセキュリティへの認識だけでは防ぐことが難しいものであると言える。

そして、現実に組織が最も対応しなくてはならないものはメール・FAX の誤送信、PC・USB の紛失、ID の紛失、アップロード時のファイル選択ミスなど、その多くがメンバーのなんらかの過失、いわゆる「ヒューマンエラー」によるものであり、前述の「①過失的行為型」に該当するものである。

近年の情報セキュリティは、セキュリティ技術者の不足が各種メディアを通じて語られ、ビッグデータ解析による経営戦略策定がもてはやされているように、IT をベースとするサイバーセキュリティのものであるという認識がもたらされているが、その多くは原始的かつ物理的なレベルにおいて発生していることがわかる。

この点で、情報セキュリティとは IT 関連に特化したサイバーセキュリティだけでなく、さきの藤谷（2003）・吉田（2004）・名和（2005）らによる定義にあるように、組織全体での取り組みが必要なのである。

(4) 本稿の目的

ここまで、情報セキュリティインシデントの発生原因を整理し、その容態を確認してきたが、これらの情報セキュリティインシデントのうち、分類では「①過失的行為型」と「④ウィルス型」の

---

[27] 2017 年から 2018 年にかけて、総務省が民間事業者で利用されている IoT 機器の調査を行った。結果として民間事業者等に対して 36 件の注意喚起がなされた。なお、調査の手法そのものについて問題提起がなされ、公的な調査に関する法整備が進められており、NICT（情報通信研究機構）が公的な業務としてこれを担うこととなった。

[28] Social Engineering：広義には、集団の振る舞いへの働きかけを対象とする研究領域であるが、ここではその一分野として、情報システムを攻撃するにあたり、IT をベースとしたアプローチではなく、関与する人間に接触を図り何らかの方法でアクセス権限や情報そのものをだまし取るアプローチのこと。

複合型である、外部者の悪意と内部者の過失が絡むことでもたらされる情報セキュリティインシデントがある。その代表例が、標的型メール攻撃によってマルウェアなどに感染することに起因する漏洩・ネットワーク侵入である。この標的型メール攻撃は、組織体の情報セキュリティにおける脅威の最たるものとして挙げられている標的型攻撃の一種となり（表5）、セキュリティレベルの高いシステムの導入といったハード的対策と、教育や訓練といった組織メンバーに対して行うソフト的対策の両輪があらゆる組織において喫緊に求められている。

表5：「情報セキュリティ10大脅威2019」より上位3つの抜粋

順位	個人	昨年順位	組織	昨年順位
1位	クレジットカード情報の不正利用[29]	1位	標的型攻撃による被害	1位
2位	フィッシングによる個人情報等の搾取	6位	ビジネスメール詐欺による被害	3位
3位	不正アプリによるスマートフォン利用者への被害	4位	ランサムウェアによる被害	2位

出典：「情報セキュリティ10大脅威2019」（2019）IPA（情報処理推進機構）より筆者作成

現代のビジネス環境における標的型メール攻撃による懸念は、マルウェアなどに感染し、これを起点として起きる被害は情報漏洩だけではない。ランサムウェア[30]による営業妨害と金銭的被害にもつながることがある。そして同時に、インターネット上における組織の対外的窓口となるホームページの内容改竄や損壊による閲覧不能といった直接の被害を受けるだけでなく、内容改竄によりフィッシングの土台とされ閲覧者を詐欺被害に導くといったように間接的に加害側の立場となりかねないという問題もある。また、標的型メールの手口は、巨額の損失[31]に結び付きかねないビジネス詐欺メールにも応用されており、2018年の調査では日本国内では調査対象者の40%が詐欺メー

[29] 2018年版までは「インターネットバンキングの不正利用」との合計項目であったが、「インターネットバンキング被害の減少、クレジットカード被害の増加」を理由として、2019年より個別の項目となっている。

[30] Ransom ware：いわゆる身代金ウィルス。「Wanna cry」と命名されたマルウェアによって、PC内のデータがアクセス不能になり、データの復旧に対して金銭を要求される。2017年5月に世界で流行した。

[31] 日本航空（株）は取引先に成りすましたメール発信者に、2017年8月から9月にかけて3回計約4億円を振り込んだ。うち2回の小規模な被害は米国にある支店に送られたメールによるもの。日経新聞「アドレス1字違い見逃す」2017年12月21日朝刊；朝日新聞「『振り込め詐欺』日航3.8億円被害」2017年12月21日朝刊

ルを受信した経験を持つことも報告されている[32]。この割合は、この前年 2017 年との比較では 3 倍となっており、ビジネスメール詐欺への対策としても急務である。

しかし、認識された脅威に対してハード的対策を充実させると、それに依拠して低下したリスクを埋め戻すような行動が増加するという「リスク補償行動」（芳賀, 2012a, p.52）という人間の特性も指摘されている。そしてこの特性は、ハード的対策の向上によってのみ見受けられるのではなく、訓練によって技能を獲得したという自信によってももたらされることが事例と共に報告されている（同上書, pp.38-45）。ここまでを踏まえれば、企業組織はハード的対策を取るとともに、ソフト的アプローチとして教育や訓練を充実させることが必要であることは言うまでもない。しかし、インシデントを防止するにはそれだけでは不足しており、組織という人間の協働体の内部に生じる社会性に着目する必要があるだろう。なかでも、これらの取り組みが何を目的とし、何を意味するものであるのかを共有した、社会性の象徴である文化的アプローチを見出すことがより重要であると考える。

後に詳しく確認するが、OECD はこういった状況に先んじて、1990 年代より情報セキュリティの重要性を訴え、2000 年代に入り「セキュリティ文化」という概念を提示し、情報端末の利用者すべてを「参加者」として情報セキュリティへの貢献を広く求めている。しかし、抽象的な規範を示すにとどまり、企業組織がビジネスを進めていくうえで、いかにこの概念を取り込んでいくのかを詳述するものではない。これに対して産業界では、企業組織の情報セキュリティをマネジメントシステムによって統制し、維持向上しようとする行動の大きな流れがある。しかしながら、マネジメントシステムにおいて設定されるセキュリティポリシーは、業務効率の問題から運用の現場において反故にされることが、各所で指摘されており、その効果には疑問がある。

実務的に運用されるマネジメントシステムもまた組織文化に言及し、組織的な方針に沿った文化の醸成をマネジメント項目に据えているものがある。にもかかわらず、セキュリティに関するポリシーが遵守されない現実があることは、マネジメントシステムによる文化のマネジメントはうまくいっていないことを意味している、もしくはマネジメントシステムが定義し意図する「文化」は、文化と呼ばれる別の何か、たとえば Thompson（1967）は、組織文化を組織能力の 1 変数としてとらえ、これを組織メンバーの行動の統一性として表現したが、こういった表面的な組織行動を意味

[32] TRENDMICRO（2018）「ビジネスメール詐欺に関する実態調査 2018」
https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180814-01.html

しているのであって、機能主義的な文化の理解にとどまっており、解釈主義的側面から説明される組織文化または企業文化ではないのではないかという疑問も生まれる。

企業組織が情報をより活用し成果を上げるために、そして前項で確認したように、企業組織が悪意のターゲットとなる、または間接的な加害者となることを抑止するため、現代の企業活動において必須のツールである情報システムと情報ネットワークの利用に際しての新しい文化の醸成が必要である。そのため、組織のメンバーの思考や行動様式が「セキュリティ・ファースト」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、企業組織においてこのセキュリティ文化を醸成するための要件を検討し、さらにセキュリティ文化が企業組織の中心的な文化となりうるかを確認することが本研究の目的である。

2 研究の意義と新規性

情報セキュリティは、世界レベルで見れば米中の経済・軍事両面での覇権争いの中核的なテーマであり、日本も産官学全体おいてこれに無関係ではない。政府調達においても特定メーカーの排除が打ち出されるなど、企業活動にも大きな影響を与えており、扱うべきトピックとして喫緊のものだといえる。このようななかで、情報セキュリティを向上させるべく、設備・機器を導入し、搭載される基盤やチップの安全性や、インストールされるアプリケーションの堅牢性や安定性の向上を追求するといったハード的対策や、それらを専門に開発し、取り扱う技術者の育成や、利用者としての一般従業員の教育や訓練といったソフト的対策は、多くの組織で取り組まれている。しかし、これらは組織のマネジメントの機能的な問題とその解決として情報セキュリティを認識し、ISMSのようなマネジメントシステムによって把握管理しようとする現実的な対処に過ぎない。

本研究は、企業組織における情報セキュリティの問題とその解決としてのハード的対策・ソフト的対策を、機能的なマネジメントの問題として捉えることを不足とし、これらの効果が真に発揮され、組織の情報セキュリティの最大化をもたらすためには、別のアプローチが必要であることを主張するものである。それは、個人が集合した協働の体制としての組織に対するアプローチとして、企業組織の文化からこれを把握し、情報セキュリティの向上を経営組織論から、なかでも文化的アプローチによってこれを達成しようとする点、さらに、組織文化論であることから機能的な問題解決の視点を持つと同時に組織メンバーの認識の問題として具体的にこれを確認しようとする点に意義があると考える。特に、組織外部者の悪意と組織内部者の過失が強く結び付いたものであるという点でも、実務的な点から企業組織に求められる対応の第 1 位に挙げられる標的型攻撃の一種で

ある「標的型メール攻撃」への対応を議論の中心に据え、標的型メール攻撃に対する備えとしての教育と訓練について、民間営利企業での施策の実際を確認し、具体的な取り組みとその要点を明らかにすることに新規性があり、これらを軸としてセキュリティ・ファーストを旨とするセキュリティ文化の要件とその醸成のプロセスを提示することは、組織の目的や形態を問わずして情報セキュリティインシデントが発生する今日において、多方面へ貢献すると考える。

現代のビジネスーインターネット環境においては、標的型メール攻撃によってマルウェアなどに感染し、これを起点として起きる被害は情報漏洩だけではない。先に述べたように、ランサムウェアやホームページの改竄などによる営業妨害と金銭的被害にもつながることがある。さらには、標的型メール攻撃と手法が軌を一にするビジネスメール詐欺への対策としても有意である。これらへの対応に係るコストといった短期的な経済的損失を防ぐというだけでなく、知的財産という経済的権益と競争優位性の保護とともに、長期的な取り組みが必要とされるレピュテーションや信頼の獲得といった無形の資産の形成についても貢献が可能であると考える。

教育や訓練の実践という点だけをみても、標的型メール攻撃訓練をこれからの課題や取り組みとする組織も少なくないことから、そういった企業の将来の実践において役立つ実務的・理論的示唆を提供できることは意義があると考える。

また、企業組織における情報セキュリティの運用の体制という点においては、大規模な情報セキュリティインシデントの発生や政府機関の広報の強化を受けて、情報セキュリティインシデント対策の専門チームとして CSIRT（Computer Security Incident Response Team[33]）を実装し、これら CSIRT が連携するための組織である NCA（Nippon CSIRT Association: 日本シーサート協議会[34]）への加盟も急増したが、この流れは続いている。しかしその実際は、NCA 設立から参加していた先駆的なチームとそれから数年間逓増状態において加盟したアーリーアダプターといった、もとよりセキュリティに関心が高かった古参のチームと、2015 年を境に急増した新規加盟のチームには持てる知識と経験の量に分断がある。こういった専門組織の新規の実装や運用、その実際の活動内容の実際を確認するという点では、今後も増加をたどると考えられる新規加盟のチームへの知識の提供と経験の圧縮にも貢献すると考える。

[33] CSIRT については、第Ⅴ章および補論 3 にて詳述。

[34] 正式名称は、一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会

II　文化にまつわる基本的な概念整理

セキュリティ文化を企業組織の文化の中心的なものにするという本稿の目的においては、従来からの企業文化とは並行的にセキュリティ文化を発達させ、上位の文化として醸成していく、または従来からの企業文化をセキュリティ文化へと変化させるといったアプローチが考えられる。そこで、本章ではまず、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する。これを踏まえ、本稿の目的である文化の醸成ないし変化または変革についての先行研究を確認し、実務的な留意点として活かすべく、その要点を整理する。

1 文化と企業文化

(1)　文化の定義

人間集団の特定環境への適応を対象とする文化研究は、民俗学や文化人類学を中心として行われており、これらの研究の知見から導き出された文化の定義は、

- それぞれの社会成員によって獲得される知識や信念、芸術、道徳、慣例、およびその他一切の能力や習慣を含む１つの複合体（Tylor, 1871, p.1）
- 行為や加工品に顕在する、社会を特徴づける慣習的了解（Redfield,1941,p.132）
- 習得された行動と行動の諸結果との総合体であり、その構成要素がある一つの社会メンバーによって分有され伝達されているもの（Linton, 1945, p.32; 邦訳書, pp.49-50）
- ある人間集団の成員の行動に影響を及ぼす期待、了解、信仰、あるいは同意の全てを含む。これらの観念は、意識的なものであるとは限らないが、常に社会的学習によって伝達されるものであり、それらはあらゆる人間社会が当面する適応上の諸問題に対して、一組の解決となっているもの（Bock,1974, p.14; 邦訳書, p.48）

というように、人々が日常の生活を営む上で発生する緒課題に対して、集団内部で発明され維持された解決策の束という機能主義的な捉え方がベースにあった。これに対して、Geert（1973）は、こういった機能主義的な研究は、文化を説明しようと彼らの生活様式を細かく要素分解し、比喩を用いながらそれを精緻化する一方で、これらの複合体であると説明することで、文化を理解するにあたっての混乱のもとになっている（邦訳書, p.148）と批判し、「人間は自分自身がはりめぐらした意味の網の中にかかっている動物であると私は考え、文化をこの網として捉える。したがって、

文化の研究はどうしても法則を探求する科学実験の一つにはならないのであって、それは意味を探求する解釈学的な学問に入ると考える」（邦訳書, p.6）と述べ、求められるのは、表面的には不可解な社会的表現を解釈することであり、これに必要なのは、意味、象徴、概念を掘り下げることであると主張した（邦訳書, p.148）。

本研究での研究の対象である企業組織をその範疇とする経営組織論における文化研究でも、組織の目的達成のための機能的側面、合理性を対象とする、いわゆる機能主義的な研究が中心であったといえる。しかし、こういった批判により、人間が構成する組織の不合理な側面に注目し、組織メンバーの行為の束を対象とする、上述の広義の文化研究に加えて、組織の持つ現実（Reality）をその対象とし、その特殊性を生み出す要因を研究する分野となっていったのである。その特徴は差異に注目し、その差異を生み出すメカニズムを解明することであり、組織を一つのシステムとみなし、文化のもつ、外部へは異質性を、内部には同質性をもたらすという性質から文化を研究するとされる（高橋ら,1998, p.185）。

高橋ら（1998）のいう「現実をその対象」にするとは、外部から観察可能な行為は、その行為者にとってどのような意味を持った振る舞いであるかという組織のメンバーの主観、すなわち個人の認識といった人の内面に着目するということを意味する。

こういった観点による文化研究によれば、文化の定義とは次のようなものとなる。

- 「文化は、象徴に表現される意味のパターンで、歴史的に伝承されるものであり、人間が生活に関する知識と態度を伝承し、永続させ、発展させるために用いる、象徴的な形式に表現され伝承される概念の体系を表している」（Geertz, 1973, 邦訳書, p.148）
- 文化とは、主としてシンボルを通じて習得され伝達される思考・感情・反応の形式である。文化は人間集団が作り出した優れた業績から構成されており、人間の手によって具体的な形を与えられた様々なものを含む。文化の中核は、伝統的、すなわち歴史的に継承され選択された観念と、とりわけこの伝統的観念に付随する価値からなっている（Kluckhohn,1951,p.86 脚注 5）（Hofstede,1980,p.25；邦訳書 p.12）
- 文化　－社会的現実の別語－　は、産物であり、過程であり、人間の相互作用の形成者であり、その結果である。また、文化は人々の進行中の相互作用から常に創造され、再創造される（Jelinek,et.al,1983,p.331）
- 文化は、明確な生活様式として認識される無数の行動や実践を伴った意味のシステムである（Gregory,1983,p.364）

・　文化とは、一定の範囲で共有された神話やシンボルに隠れた中心的価値の集合として定義される（Broms & Gahmberg,1983,p.482）

というように文化とは集団における「観念」や「価値」とった個人の内面の集積であり、集団内での行為の目的や意味そして価値の共有化は、それらを「記号」（Bock,1974,p.14; 邦訳書,vol.1,p.48）やモノ、人に付与した「シンボル」を通じて行われることが特徴である。そしてこのシンボルを引き継いでいくことで、集団内で伝達していくことができるという。

このように、経営組織論における文化研究においても、機能主義的な把握と解釈主義的な把握という二つの立場があるが、前者は、解決策の束がどのように出来上がり、用いられているかの理由を明らかにするものである。後者はメンバーの行為について、それを行う組織メンバー自身らがどう認識し、理解しているか、その認識と理解は何を通して行われて、組織全体としてどう形成されているかを明らかにしようとするものとなる。この違いについて寺本（2013）は、「組織の変数としての文化」と「組織のメタファーとしての文化」という Smircich（1983）の整理を踏まえつつ、前者は組織内部の諸要素を分解し文化的なものとして捉え、メンバーの振る舞いの理由を説明しようとする静的なものであり、後者は、組織を共有された意味やシンボルの体系など組織文化そのものとして見るもので、共有の過程やシンボルが形成されるプロセスが組織そのものであるという動的な組織観によると説明し、組織文化についての現代的研究の意義は後者にあると述べている。

本研究は、現実に運営される企業組織の現実的な課題の解決にあたり、文化的にアプローチすることの重要性を指摘し、これを試みるものである。文化からこれを捉えることが重要であるのは、組織文化が組織そのものであるならば、メンバー個人が特定の集団のメンバーシップを獲得すること、言い換えれば自身も文化を構成する一部となっていくことを意味する「社会化」によって組織と個人の調和もたらすと考えるからである。

この社会化について Child(1954)は「極めて広い範囲での行動可能性を持って生まれた個体が、より狭い範囲に制限された現実的行動を発達させる方向へと導かれるプロセス全体をいう。何が習慣的なものであり、許されているかということの範囲は、この個人の属する集団の基準によって決まることである」（p.655）と述べるが、この「属する集団」とは本研究では企業組織となる。こういった特定の組織における社会化については、組織心理学やキャリア論の文脈においては、「組織の一員として認められるために、個人が価値体系、規範、必要な振る舞いを身に付けていく過程」(Schein,1988, p.54)とされ、文化の定義で取り上げた文化人類学の文脈では、「個人が社会の一員となることを学習する過程。公式の教育と、社会的役割への非公式な誘導を含む。米国の人類学では

『社会』より『文化』の概念に重きを置くため、用語として『文化化(enculturation)』を用いることが望ましいとされるが、ほぼ同義」[35]とされる。

したがって社会化とは、文化の定義のなか示されていた、集団を特徴づける種々様々なものを、その集団内部の個人の側から捉え、その社会との関わりにおいて相応しい性質と適切な振る舞いを獲得するプロセス全体を意味するものである。重要な点は「個人が他の人々との相互影響(transaction)を通じて、社会的に重要な行動や経験について、その個人特有の型を発達させていくプロセス全体」（Child, 1969）というように、組織の他のメンバーとの相互作用の中で組織のメンバーとして求められる役割を認識し、振る舞いとして表出させていくという点であり、単なるマニュアルの習熟により特定の行動の獲得し、効率よく業務を進め、組織に貢献するということではないのである。

組織全体における調和を問題とする点で、組織と個人の両者にとって極めて重要なものと言え、個人の特定の振る舞いを組織の文化から捉え、導くことが、組織の永続の視点からも求められているからである。

そして、問題解決について文化的なアプローチを試みるという点では、一義的には、問題解決の機能としてこれを捉え、組織の構成要素の一部としての文化、すなわち内部変数として検討していく必要があると考える。しかしながら、文化の本質はメンバーの内心にあり、集団として意味を見出したもの、メンバーに共有された観念や価値を中心としてこれを追求しなければ、根本的問題解決には不足であることもまた間違いない。

そこで、組織目標の達成のために文化をマネジメントするという機能主義的な観点に立ちつつも、メンバーに共有された価値を中心として、個人の内面に着目した企業における文化のモデルを提示した Schein の議論について確認する。

(2)　企業文化のモデル

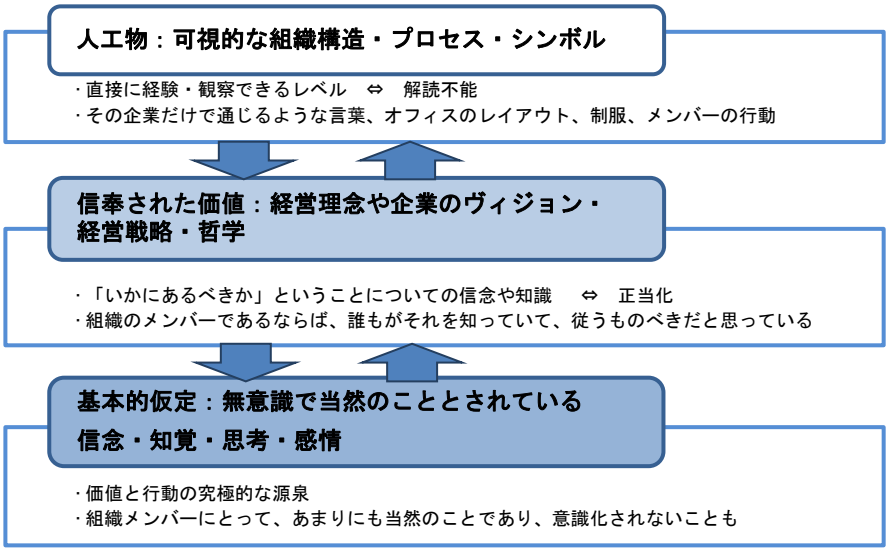
企業組織の文化について Schein（1985; 1999; 2010）は、従来からの文化研究の成果を踏まえ、文化は外的社会、内的社会における様々な問題に対処した経験によって獲得されるもの、すなわち成功体験によって形成される社会的学習の産物であるとする（Shein,1985, 邦訳書, p.10）。特に、企業組織の文化は、企業の創業当時の組織の創設者の考え方ややり方が共有され、上手くいくことにより文化的要素になっていくといい、その成功が続くことで、物事の本質やあるべき姿に関する暗

[35] *Macmillan dictionary of anthropology*, 1876, P. 261 “socialization”

黙の仮定となると述べている（Shein,1999, 邦訳書, p.38）。文化的諸要素とは、Hofstede（1980）による文化の定義にある「文化は人間集団が作り出した優れた業績から構成」され「継承され選択された観念」と「観念に付随する価値」を体現したものである。社屋やオフィスレイアウトといった目に見えるモノや、人事や会計システムといった直接には目にすることはできないようなモノであるが、それらは、創業当時の環境への対処行動の成功によって生まれ、その成功の持続によってより強固になった信念が組織内に浸透することで、組織独自のパターンをもって表出したものであり、要約すれば、「創業者の成功体験の拡大再生産のための諸要素」となろう。

そして、それが具現化するのは「目に見える行動、儀式、風土といった文物、および、標ぼうされている価値観」（Schein, 2010, 邦訳書 p.211）であるとする一方で、「その本質は、共有された暗黙の仮定である。この共有された仮定を意識することもできるが、普段は気づかないところで作用している」(同上書. p.211)といい、組織文化とは組織メンバーがより深いレベルで共有し、無意識のうちに機能するものとしている。また、組織そのものや環境についての考え方を「当然のこと」とするような「基本的仮定のパターン」とも述べ、これらを整理した文化の三層モデルを提示する。

図 1：文化の三層モデル（Schein,1985; 1999）



出典：Schein(1985, 邦訳書, p.19; 1999, 邦訳書, p.18)を基に筆者作成

この 3 層のボトムとなる基本的仮定には、まず「組織が持つ自然に対する人間の関係」（Schein,1985, 邦訳書, p.108）すなわち、環境は支配するもの、調和するもの、従属すべきもの、という組織と外的環境との関係性の認識があるという。そしてこれは同時に、環境の技術・政治・経済・社会文化などのどの局面に注目するかを仮定し、それによって組織戦略をも方向づけられる

という。この認識の違いによって基本的な仮定も変化するが、そのポイントには6つのタイプがあるとして、次のように整理している。

① 現実と真理の本質（the nature of reality and truth）

何が現実で、何が現実でないかを規定する仮定。何をもってして現実とするのかのコンセンサス。

② 時間の本質（the nature of time）

時間の定義の仕方、文化における時間の重要性を規定する仮定。時間の使い方、計画の立て方、期限などに関するコンセンサス。

③ 空間の本質（the nature of space）

空間の配置の方法や空間の象徴的な意味を規定する仮定。メンバー間の物理的・社会的な距離感を規定するもので、これによりコミュニケーションの在り方も決まる。

④ 人間性の本質（the nature of human nature）

人間の属性を規定する仮定。セオリーX・Y（McGregor, 1960）を引き合いにしながら、善か悪か、完全か否かというような人間観であると説明する。これによりメンバーの動機付けや報奨・管理のシステムの在り方が決まる。

⑤ 人間的活動の本質（the nature of human activity）

その環境において、何をすることが正しいのかを規定する仮定。能動的－受動的と両端に据える行動志向性であるとともに、自らのキャリア研究を引き合いに、仕事・家庭・個人の関係性の相対的重要性についての志向（Schein, 1978）をこれに加えている。これらが組織の意思決定のスタイルに影響を与えるという。

⑥ 人間関係の本質（the nature of human relationship）

人々の関係は個人主義なのか、集団主義なのか、コンフリクトは、いかに解消されるのか、いかに意思決定を行うのかを規定する仮定。組織内の権力勾配や個人の参加の程度を規定するという。

これら6つの仮定が組織内に存在し、相互に関連することで、ある一連の仮定、ともすれば「会社の常識は世間の非常識」と表現されるような自動的な思考様式となり、いわば無意識に近い形での意思決定とそれにつらなる振る舞いを誘導することとなる。

企業文化としてこの3層が生成されるプロセスについては、先にも確認した通り、企業の創業当時の組織の創設者の考え方ややり方が共有され、上手くいくことにより文化的要素になるとされる。すなわち人工物が先に作られ組織内で運用されることが先に立ち、その運用がうまくいくことで、物事の本質やあるべき姿に関する暗黙の仮定として内面化されていくという順であると理解できる。したがって、組織メンバーの深い内面にまで意図した影響を与えるには、価値観が反映された組織構造や業務プロセス、そしてそれらを表現したシンボルといった人工物を作り運用することが前提となり、さらにはそれが成功し続ける、すなわち適切なものとして認識されるまで運用され続けることが必要になる。

企業文化の起点についてScheinが「創業者」という人称を用いるのは、それを引き継ぐ「継承者」がいるということを当然の前提としているからと考えられるが、文化は企業組織の発展と永続の根源でもある。組織の古典的定義に従えば、複数人、共通目的、コミュニケーションと永続性が組織の要件であり、メンバーに変動があっても、組織体は維持されていく（Barnard, 1938）。すなわち、組織という外殻と共に、文化という無形のものも継承されていくのだが、メンバーの変更があるにもかかわらず、そういった有形無形のもの、ここでは表象・価値観・仮定が集団内部でどのように受け継がれていくかという問題がある。その答えが、価値観が物質化された人工物であり、それは成文的な組織構造やそれにつらなるオフィスのレイアウトであったり、なにより先の文化の定義にも挙げられていたシンボルとなろう。

しかし、こういった文化の表象物が受け継がれるなかで、メンバーと環境の変化によって新たな解決策が求められたり、従来からの解決策が変化し、また淘汰されることがある。むしろ環境の変化を当然とするのならば、文化の変化は避けられず、変化が必須であることを前提として組織の経営者とメンバーは積極的に関与すべきといえる。であるならば、共有された仮定から自動的な思考様式としてもたらされる無意識に近い形での意思決定とそれにつらなった振る舞いを、意識的に組織メンバーから引き出す、すなわちマネジメントすることはできるのか、その要点はなにかについて確認する。

2 文化のマネジメント

(1) 「強い文化」

Deal & Kennedy（1982）は、企業文化を「人は平常いかに行動すべきかを明確に示す、非公式な決まりの体系」（邦訳書, p.29）と定義し、組織のメンバーが何を期待されるかを知り、いかに行

動すべきかの判断基準となるものと説明する。そして、これがメンバーに浸透し、意図せずとも表出している状態を「強い文化」と表現した。同じく Schein（1985）も、文化はその影響力が強いほど、組織メンバーたちの判断を支え、方向付け、あるいは行動を抑制／促進する影響力を持ち、この働きが大きいほど「強い文化」であると述べている。

この「強い文化」について O'Reilly（1989）は、①文化と戦略のフィット、②被雇用者の企業へのコミットメントの向上、という 2 点において企業組織にとって価値があるという。

「①文化と戦略のフィット」については、シリコンバレーにある半導体製造業 3 社の競争戦略の選択を比較しながら、いずれも特徴的な文化を持つことを示し、それぞれに違った戦略を選択しながらも成功している理由について、組織戦略の遂行においてはそれを支えるシステムとそれにフィットした価値観の共有がなされていることによると結論付けている。

また、競争優位の源泉の 1 つとしてメンバーの高い献身を挙げ、それは「②被用者の企業へのコミットメントの向上」によってもたらされるという。この高い献身の前提となるコミットメント、すなわち組織と個人を結び付けるものが信頼であるとする。そして、ここで言う信頼とは、組織内部において何が称賛の対象であり何が受け入れられないものなのかが明確に示された状態のことであり、それこそが文化なのだという。この線引きこそが組織が標榜する価値観そのものであり、理解と内面化によってもたらされるコミットメントこそがメンバーの熱意や献身の根源となり、これらを拡大再生産することに決定的な役割を持つとする（O'Reilly, 1989, pp.16-18）。

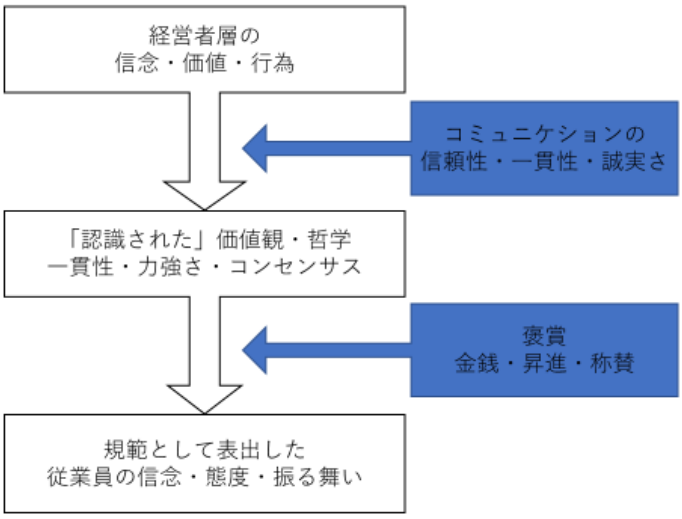
(2)　文化の発達：Schein の企業文化と O'Reilly のモデル

組織内部において何が称賛の対象であり何が受け入れられないものなのかが明確になっており、その線引きがメンバーに内面化された状態こそが「強い文化」であるが、そういった「強い文化」はどのように創られていくのだろうか。営利組織としての企業に着目すれば、前節で確認したように、創業者の成功体験とそこから生まれた価値観がその企業における正しいやり方、正しい考え方としてメンバーに共有されることから始まる。これに沿った形で付随する組織的な要素、すなわちマニュアルや教育が確立し、人事や会計などの管理のシステムが作られることで正しいやり方、正しい考え方が強化されていく。そして、それに従って行動することで「共有された仮定」として内面化されることで創られていくという（Schein, 1985）。この仮定の内面化を補完する機能を持つものが「褒賞」である。創業者の成功体験から導き出されたものをなぞることで、組織の中で「成功」することが褒賞である。そして、成功という結果に対する金銭的な報酬だけでなく、文化に沿

った求められる振る舞いについて創業者の持つ価値の表現者として支援を受け、組織内で重用されることもまた報酬であるという（Schein,1985; 1990; 2010）。

このようなプロセスを O'Reilly（1989）はモデルとして提示している（図 2）。

図 2：文化発達のモデルとマネジメントに求められる要素



出典：O'Reilly（1989）p. 23 をもとに筆者作成

まず、経営者層が持つ信念や価値観をメンバーに伝達することが起点となるが、信念や価値観を正しく伝達するためには、コミュニケーションの相手としてメンバー相互の「信頼性」と、その「信頼性」を獲得するための「誠実さ」が求められる。この信頼性と誠実さの源泉は、信念や価値観といった経営者層の内面的なものと、彼らの発言や行動という表面的なものの「一貫性」であるという（O'Reilly, 1989, pp.23-24）。この一貫性によって組織メンバーが、トップマネジメント層の持つ信念や価値観を認識し、さらにメンバー間で共有されることで、組織内で期待されるもの、求められる振る舞いについてのコンセンサスを獲得する。そして、コンセンサスに基づいて実際の振る舞いとして表出してくることを支持するのが「褒賞」であり、Schein（1985）と同じく金銭や昇進、称賛を例示する。なかでも称賛については、表彰や記念品を与えることによっても可能だが、それらよりもメンバーの前で褒めることの方が価値は大きいことがあり、かつ頻繁に用いることができる点で有用であると述べる（O'Reilly, 1989, p.22）。

彼が提示するこのプロセスの特徴は、起点となる信念の表明は必ずしも明確なものでなくても、その後の行動に「一貫性」があればメンバーはその信念を推論し、コンセンサスとなり共有することができるという点である。そして「このコンセンサスもまた褒賞されるとき、明確な規範が生まれてくるだろう」（O'Reilly, 1989, p.23）というように、褒賞を活用することによって、推論から正

統化された認識として内面化され、振る舞いとして表出していくという。そのため信念から褒賞までの一貫性が強調されている。

そして、このモデルにおいて求められる要素を①選択と参加、②シンボリックなアクション、③他者からの情報、④包括的な褒賞システムという４つの「メカニズム」として表現し、整理している。組織文化研究の差異に注目するという観点で言えば、文化の強さ・弱さとは、何が行われている・行われていない、ではなく４つのメカニズムが用いられる程度の違いであるという（O'Reilly, 1989, p.19）。

まず「①参加と選択」とは、彼は「巻き込まれ（involved）」と表現するが、組織における自らの必要性を認識させるために、組織内の公式なものであれ非公式なものであれ、仕組みや集団への参加を組織側が促すという。そして、参加対象へのコミットメントを増幅させるためには、「自らが選択した」という心理的状況を作り出すことが重要であり、積極性には程度の差はあることを前提としても「強い文化」を持つ組織は、「参加」することを自ら「選択」したという状況を作り出すという。そのため、人々の選択する機会を増やすことで、自分たちの行為への責任感を育てることを支援することが肝要であるという。

次いで「②シンボリックなアクション」とは、経営者層だけでなく管理職層も含めたマネジメント層の振る舞いを指す。マネジメントの重要なことのひとつは、組織内での昇進や組織の再編成といった変化に、複数の意味と解釈を持たせいないよう出来事の解釈・意味を共有することであり、自らの振る舞いによってこれを導くことであるという。組織メンバーは、「組織内では何が重要であるか」についての関心が一番高く、なによりも上司を通じてこれらを理解する。この理解は、直接尋ねるというだけでなく、観察し、耳を傾けることによって成されるため、部下を持つ管理者層は自らの振る舞いがどう見えるかに敏感でなければならず「日常のシンボル」として行為することに取り組む必要があるとする。

第３のものとして、「③他者からの情報」を挙げる。経営者層や管理職層がシンボルとしてメッセージを伝達すると同時に、個人の行動を規定するのが他人の目、ここでは同僚からのメッセージだという。彼は、職務設計による組織コミットメントの引き出し、特に組織目標と個人の成長欲求のすり合わせに疑問を投げかける。そして、「実際にも事実にも、直接の経験から生じるすべての学習現象は、他の人々の行動を観察することによって代行的に起こり、それが彼らに影響を及ぼす」（O'Reilly, 1989, p.19）というように Milgram, S. や Bandura, A.といった心理学者によってもた

らされた知見[36]を踏まえながら、組織内における具体的な振る舞いは「状況と他者の期待」によって社会的に規定されており、自らの振る舞いに注意が払われていることが最大の要因であるとする。そして、集団内で「何を期待されているか」と同時に「何をすべきか」についても他者からの合図を利用しているとする。その期待に応えるべく、身近な他者の振る舞いとその結果を観察することによって期待される振る舞いを習得するのだ。特に、組織内で新しい状況にあるときの人は、何をするのか、出来事にどのように対処するのかの説明を他人に求めるが、強い文化の下では、状況の理解の一貫性を確保し、組織の部分間で我彼的な態度を最小化しようとするという。そういった状況下での組織の目標は、「解釈の矛盾を最小化することでリアリティを強く社会的構成として創り出すこと」（O'Reilly, 1989, p.22）であり、そのために同僚とのコミュニケーションによってメンバーを社会化していくことが組織にとって重要になる。

最後に「④包括的な褒賞システム」を挙げている。直接的には、給与やボーナスといった金銭的な報酬と、昇進昇格・認知や承認といった非金銭的な報酬を意味する。これらによって「何が経営者層の注意を集めているかの単純な分析となり、文化が何を支持しているかへの感覚を我々にもたらす」（O'Reilly, 1989, p.23）という。これらの褒賞のうちでは、認知や承認は頻繁に用いることができ、さらには所属の欲求（社会的欲求）を満たすものとして適切であるという。特に強調するのは、正しい振る舞いに対してはその場で褒賞することが、動機づけをより強くするということである。注意すべきは経営者層の要求事項（発言）と褒賞（行動）の対応関係のズレである。ここで重要なのは、先述のモデルにおいても挙げられていた「一貫性」、すなわち経営者層の言動の一致であり、これこそが何が注目を集めているかの分析の中心となるという。

ここまで確認してきたことを再度整理するが、意図した文化を形成する、すなわち文化のマネジメントを企図する際には留意すべき 4 つの要素がある。まず、①組織的な活動への参加を自ら選択したという認識を個人に作りだすことである。これは、活動内容へのコミットメントの向上をも

---

[36]Milgram(1965)は、ヒエラルキーを持った組織構造の内部では、参加者たちは、自分の目的に従って行動しているのではなく、高い権威を持っていると認識した他人の考えを実行する代理人として自分を捉えるようになり、上位者の考えを読み取ろうとすることを実験により見出している。「服従行動」と呼ばれる。Bandura(1963)は、幼児期の行動は、直接的な体験からの学習だけでなく、周囲の観察を通した模倣によって引き出されていると考え、これを実験によって明らかにし、「観察学習」「モデリング」と名付けた。そして観察対象の行動の結果（報酬）を観察することでも引き出されることを確認し、これを「代理強化」と呼んだ。これらを踏まえて「社会的学習理論」（Social Learning Theory）を提示した。模倣した行動を実践したことから得られた満足感などがその行動を再現する動機付けとなるとも述べている。

たらす。そして、②経営者層や管理職層といったいわゆるマネジメント層は、活動の方向性を示すもの、すなわちシンボルとしてメンバーから常に観察されているという認識を持つことである。これによって組織全体の活動の方向性が示され、また理解されることになる。これに対して個々人の活動の具体性を示すものとして、③活動の内部における個人の役割とその役割に根差した振る舞いは、身近な他者によって導かれているとすれば、その関係性をいかに作り出すかである。コミュニケーションの相手として、また、観察することでなされる代理学習の対象となる模範をいかに配置するかが論点となろう。そして最後に、④目指す方向性に適合した活動に対しての褒賞を用意することである。シンボルによって示された方向性の理解や解釈のズレを修正し、また、褒章を受けるものを観察することも活動の方向性を理解するヒントなのである。そして、組織内部の社会性の観点から認知や承認という褒賞がもっとも簡便であり有効である。

これらの効果を認識し、いかに恣意的に活用するかが強い文化の醸成、すなわち強い文化のマネジメントの要点である。

3 文化を変化させる

前節では、文化とはどのようなものか、企業組織の文化はどのように形成されるのか、そして意図する方向に形成することはできるのかについて確認した。そこで本節では、すでに形成されている企業文化を変化させることはできるのか、できるとするならばどのような要件が求められるのかを確認していく。

本稿において「新しい振る舞い」が求められているのは個人情報や企業機密の保護についての社会的な要請であり、セキュリティ文化が求められるのは、外的環境の変化とそれによる対処すべき新たな課題の発生に他ならない。社会的要請としてセキュリティへの対処が求められることも外的環境の変化の一つであり、これが従来からの振る舞いを許容しない場合は、文化を変えていく必要があるということになる。

しかし Ansoff（1977）は、組織がこういった戦略的な革新の試みにおいては、戦略の実践には①誰が推進するのか（strategic thrust）、②やる気を呼び起こすような風土はあるか（strategic culture）、③問題解決のリーダーシップは誰がとるのか（managerial capability）、④資源の調達と配分はどのように行われているのか（logistic capability）といったものが組織の慣性として影響し、これらの要因によって組織的な抵抗が生まれ、その強弱によって革新に必要となる時間は変化すると述べる（邦訳書 p.231-235）。現代的な組織経営においては対応のスピード感を度外視すること

はできないため、これらの組織的な慣性や抵抗をいかに抑えていくのかを含めて、文化を変化させることの要点を確認していく。

(1) 文化変革論

企業文化の変化についての研究は、おおよそ2つの流れがある。まずは1960年代以降、活発化していたM&Aにより企業文化同士が接触することによっておこる意図しない結果としての変化を「文化変容」と表現し、整理したもの[37]。そして1970年代後半からの、不確実性への対処やイノベーションといった組織の生存をかけて意図的に変化させることを企図した「文化変革」に関するもの（Schein, 1985; 1990; 2010; Kotter,1996; Tushman & O'Reilly, 1997; Nadler,1998; Taffinder, 1998など）である。

Scheinによる組織文化研究で確認したように、企業組織の文化とは、創業当時の環境への認識、ここでは価値観と表現されるものとそれに基づく対処行動の成功によって生まれ、その対処行動が組織メンバーに共有され、メンバー個々に成功を収めることでその価値観や行動が正統なものと認識され、その成功の持続によってより強固になる。そして、それを補助するのが、成功の持続を目的に、価値観に沿った形で用意された人工物、先の例であればマニュアルや教育、人事や会計といった組織運営の日常のツールであり、これらを「文化的要素」（Schein, 1985; 1990; 2010）と呼ぶ。

そして、文化が正しいかどうかの基準は常に、組織がその主要な業務で成功をおさめられているか、組織内の人間関係をうまく管理できるかといった実利的なものである。目標が達成できなかったり、組織がうまくいかなくなったりし始めれば、この文化的要素のいくつかが機能しなくなっているということであり、変革しなければ組織の存続にかかわるとする（Schein , 1990 ;2010）。

しかしながら、組織の成果に低下がみられても組織構造や組織プロセスがなかなか変革されない／しない場合がある。その理由については、組織構造と組織プロセスの間に適合的な関係がいったん出来上がってしまった時に組織の慣性力が最も大きくなることが原因（Child, 1977）と指摘される。この慣性力とは何であるか、そして慣性力が大きいと変化できない理由が、ここで議論している「文化」とこの「文化的要素」となる。すなわちScheinが「共通の仮定」と表現した、成文化されることがなく目には見えないソフト面と、それによって形成され、さらには仮定を強固にする作用を持つ「文化的要素」が組織の構造とプロセスそのものとなっているのである。したがって、

---

[37] Berry（1976; 1984）による文化人類学における文化変容研究をベースに、M&Aによって接点を持った2つの企業文化がそれぞれどのように収斂していくのかを検討したNahavandi & Malekzadeh（1988）が最も著名。

新しい目標にむけた実践には、それにフィットする新しい文化とその文化的要素が必要となるが、これはO'Reilly（1989）がシリコンバレーの企業群の比較において文化のマネジメントの必要性としても述べていた通りである。

この実践という観点では、加護野は、組織文化は人々の観念の中に体系化された実践的知識として存在しているものという指摘のもと、文化が「日常の理論」（加護野, 1988, p.8）であるから組織的抵抗が生まれると指摘している。文化とは、「信念と実践的知識の組み合わせ」（同上書, pp.27-28）という機能的な体系であると述べ、文化と文化的要素は機能そのものであり、基本的には人々が通常担当している業務において最適化されたルーチンそのものとして組み込まれているものだからであるという。すなわち文化の変革には、日常レベルでのコストと効率のコンフリクトがまず立ち現れることを意味している。

企業組織における文化の重要性を認識し、これを変化させる試みにおいて発生するコンフリクトの解消について、現場の自主性の重要性を指摘するのが、Deal & Kennedy（1982）である。彼らによれば、文化をどのように変化させるべきなのかについて①目標の明確化、②多くの社員とともに取り組むこと、③過度に管理しない、という3点をプロセスの要点として求め、さらにプロセスに必要な要素として、ア）合意、イ）信頼関係、ウ）技術の養成、エ）忍耐、オ）柔軟性の5つを挙げる。

「ア）合意」とは、同僚間での意見の一致を意味する。そして「イ）信頼関係」とは、目的達成の意思を伝達するための経路構築の前提として求められるものである。「ウ）技術の養成」とは、改革を新たな文化を支える新たなシステムに対する技術訓練とみなし、また、この訓練を改革の一過程とみなすこと、「エ）忍耐」は、変化になじむために求められるもので、何かに置き換えることのできないもの、「オ）柔軟性」とは組織内部の人々の日常経験に応じた修正を許容すること、とその要件を説明している。

「ア）合意」と「イ）信頼関係」そして「ウ）技術の養成」は、「①目標の明確化」「②多くの社員とともに取り組むこと」を満たすために必要なものとして理解できる。そして、「エ）忍耐」と「オ）柔軟性」は「③過度に管理しない」という変革の要点を満たすものであり、加護野の指摘するコンフリクトの解消には時間を要すること、そして、組織内部の現実に沿った形での新たなやり方の模索もまた組織においては重要であるという示唆として理解できる。

一方で、このコンフリクトを意図的に起こし、なおかつその程度を積極的に管理することが文化の変革のマネジメントの要点であるとSchein（1999; 2009）は述べ、その管理に際しては「心理的

安全」が必要であると主張する。この心理的安全をどのように生み出すかについては、文化の変革のステージモデルの中で説明されている。

このモデルは、解凍－移行－再凍結という3段階のステージモデルである。まず、「解凍」では、現在の態度・行動を肯定する均衡状態を流動的にし、心理的緊張状態を生み出す。次いで「移行」では、心理的緊張を解くために情報の探索、処理、利用が行われる。そして、「再凍結」では、このプロセスによって生じた新しい状態を組織内に定着させるというモデルであり、Lewin（1951）による個人の態度変容の研究を援用し、組織変革プロセスをグループダイナミクスの視点より捉えたものである。

Schein（1985）は、この3段階のプロセスに沿って企業における文化の変革を以下のように説明する。

①解凍－変化の動機付け
・否定的確認
・生き残れるかの不安・罪悪感の創り出し
・学習不安を克服するための心理的安全の確保
②移行－新しい概念と新しい意味の学習
・役割モデルの模倣
・解決法の探索および試行錯誤による学習
③再凍結－新しい概念と意味、基準の内面化
・自己概念およびアイデンティティに取り込む
・継続している関係に取り込む

企業文化の変革は、結果として組織全体が変容する、言い換えればメンバーの日常の会話や振る舞いそのものが変容する必要がある。そのためにまず、均衡している状態を壊すことである「①解凍」は、「変化の動機づけ」とされる。そのメンバーが行動を変容させることを「動機づけ」る起点となるのが「否定的確認」である。これは、現状を維持することでは将来的に組織そのものの生存が危ぶまれるというように自組織の立場に対する否定的な情報である。

情報の種類には、ア）経済的、イ）政治的、ウ）技術的、エ）法的、オ）倫理的、カ）内面的の6種があり、中でも「カ）内面的な苦痛」は自己実現の欲求に関連し、自発的な学習の動機となる

と指摘する。しかし同時に、この自発的な学習の動機となる内面的な苦痛も何らかの情報がもたらされることで触発されると説明している。

そして、これらの情報がどこからもたらされるかという情報源は、ア）大損害とスキャンダルといった組織的な事故や不祥事、イ）新技術の導入、ウ）M&A、エ）従業員の懸念を払しょくするようなカリスマ的リーダーシップ、オ）教育と訓練、と整理している。この中で「イ）新技術」について、本稿が対象とするITは極めて変革に対して強い力があると述べる。それは新しい操作方法の学習だけではなく、リモートワークや在宅勤務など働き方そのものをも揺るがすものであるからだという。そして「オ）教育と訓練」による介入が最も重要であるという。それは、「従業員は、環境上の事象にかかわる危険について、教育を受けない限り、責任感ある新しい行動パターンが必要であることを受け入れない」（Schein, 1985, 邦訳書, p.108）からであり、さらに、既存の価値観を直接否定するのではなく、疑念を持たせることができるという点で、否定的確認の土台として適していると主張している。

これらの情報源からもたらされた情報をきっかけに自組織の立場を「否定的確認」することで変化への動機づけが生まれるが、この動機とは、否定的な情報を脅威として認識することで生ずる、その後にどう生き残っていくのかという不安と、現状を維持することの罪悪感だという。

この「生き残りへの不安」と「現状を維持することの罪悪感」によって新しい取り組みをモチベートするのであるが、一方で変革によって導入される新技術などの習得における個人的な遅延や、導入プロセスにおける一時的な効率の低下といった「学習不安」も同時に発生する。この関係性については、「生き残りへの不安」が、「学習不安」を上回る図式が必要となる。しかしながら、「生き残りへの不安」が「学習不安」を大きく上回ってしまうほど「生き残りへの不安」を過度に煽ると、確証バイアスや正常性バイアス[38]が働き、現状に対する否定的確認そのものが棄却されてしまい、新たな学習にまで至らなくなってしまう（Schein, 1985, 邦訳書, p.215）。したがって、こういった情報によって不安を高めつつ、一方ではその解決として求められる新しい学習プロセスに対する別の不安の緩和を用意する必要があり、この緩和の源が「心理的安全」であるという。

---

[38]「確証バイアス」は、Snyder, M. & Swann, W. B.（1978）によって報告されたもので、自身の持っている考えや仮説を裏付けるような情報のみを選択的に収集しようとする傾向のこと。
「正常性バイアス」は、Weinstein, W.（1980）によって報告されたもので、ネガティブなインパクトを持つライフイベントの発生確率について、他人に比べて自分自身については低く見積もる傾向のこと。楽観バイアスや恒常性バイアスとも呼ばれる。

心理的安全とは、学習棄却と新規学習のプロセスにおける一時的な生産性の低下や個人レベルでの学習遅滞に対する不安といったコストの認識を除去するためのもので、新たな学習に際して、①明確で信頼できる将来像、②新しい行動レベルの目標、③学習者に機会があること、④適切なトレーニングと時間と費用、⑤新しい行動に合致した報酬／管理／規律のシステムなどの構造的サポート、が提供されることにより生まれるという（Schein, 1985, 邦訳書第 2 版, pp.113-114）。

このなかで、「⑤新しい行動に合致した報酬／管理／規律のシステム」は、Schein（1990; 2010）のいう「文化的要素」に該当し、組織の環境の変化に合わせて進化するものであり、この進化を管理するのがリーダーシップの主要な役割であると主張する（邦訳書第 2 版, p.213）。すなわちリーダーシップの発露の対象は、構造的サポートのコントロールを通じて抵抗を克服できる程度にすること、すなわち、心理的安全と生き残りへの不安のバランスをとることであり、これこそが変革を管理するカギであろう。

(2) 組織変革論

このリーダーシップに着目しながら文化変革の 3 段階モデルの精緻化を試みているのが、1990 年代に入り「不確実性」として表現された組織の外的環境への対処としての Kotter（1996）, Tushman & O'Reilly（1997）, Nadler（1998）, Taffinder（1998）などの組織変革の議論である[39]。

組織変革論の多くも前節の文化変革論同様、ステージモデルとして定義されている。たとえば Nadler（1998）は、①必要性の認識、②共有する方向の決定、③変革の実行、④総まとめ、⑤持続、という 5 段階のモデルとして提示している。同じく 5 段階のモデルとして Taffinder（1998）は、①変革への目覚め、②変革のビジョン提示、③変革のシナリオ作成、④実践、⑤変革バリューの追及、として 説明する。どちらも、外部環境に対して組織変革の必要性を見出し、新たな組織像を提示する行動が「解凍」段階の前に付加されている。さらにステージモデルの精緻化を試みるものとして、Tushman & O'Reilly（1997）では、まず①変革を導く、②組織変革の実行、③変革の査定、という Lewin（1951）の 3 段階モデルと同様の大区分を提示する。そして、最初の「解凍」に該当する「①変革を導く」においては、ア）ビジョンにあふれたリーダー、イ）上級チームの設定を、続く「移行」に該当する「②組織変革の実行」では、ウ）変革の政治的な力を管理する、エ）個人

[39] 組織変革論は、1990 年代の米国流経営学の議論の中心であった。それは、経済成長率で日米の逆転現象が起き、「ジャパンアズナンバーワン」として経済制度・社会制度から考察した Vogel（1979）研究に対し、躍進の続く日本企業に対抗するために米国企業に求められるイノベーションの議論と重ね合わせて議論されることが多く、経営組織論の視点からその要件の整理を試みている。

の抵抗の管理、オ）転換期の統制の維持を、最終段階である「再凍結」に該当する「③変革の査定」では直截的にカ）変革の査定というように、それぞれの段階において必要となる具体的行動として示している。同様に、具体的行動としてステージモデルを示すものとして、Kotter（1996）は①危機意識の醸成、②変革のため連帯チームを築く、③ビジョンと戦略の創造、④ビジョンの周知徹底、⑤従業員の自発を促す、⑥短期的成果の実現、⑦成果を活かした更なる変革の推進、⑧新しい方法の企業文化への定着、の８段階モデルとしている（表６）。

表６：組織変革論のステージの整理

Lewin（1951）	Nadler（1998）	Taffinder（1998）	Tushman & O'Reilly（1997）		Kotter（1996）
	①必要性の認識	①変革への目覚め			
解凍	②共有する方向の決定	②変革のビジョン提示 ③変革のシナリオ作成	①変革を導く	ア）ビジョンにあふれたリーダー イ）上級チームの設定	①危機意識の醸成 ②変革のため連帯チームを築く ③ビジョンと戦略の創造
移行	③変革の実行 ④総まとめ	④実践	②組織変革の実行	ウ）変革の政治的な力を管理する エ）個人の抵抗の管理 オ）転換期の統制の維持	④ビジョンの周知徹底 ⑤従業員の自発を促す ⑥短期的成果の実現 ⑦成果を活かした更なる変革の推進
再凍結	⑤持続	⑤変革バリューの追及	③変革の査定	カ）変革の査定	⑧新しい方法の企業文化への定着

出典：筆者作成

これらの研究者による組織変革の議論は、不確実な環境下において求められる包括的・抜本的・意識的な変革であり、変革プロセスをステージ区分により捉え、危機の認識の醸成とそれに対応するビジョンの提示とその共有のためのコミュニケーションを重視し、その役割を経営者層のマネジメントに求めるものであるとまとめることができる。

4 文化のマネジメントについての整理と考察

本章では、組織の外部環境の変化に合わせ、適切な振る舞いが表出する文化を醸成する、または適切な振る舞いが表出する文化へと変化させることを目的として、文化の概念と組織文化の醸成や

変革のモデルを中心にその要点を確認してきた。本節では、これまでの要点を整理しながら、若干の考察を加えたい。特に、現代的な企業の実務の面に落とし込むためにこれらの理論的な要点との接合における留意点はどのようなものであるか、実践においてどのような点がポイントとなるかを検討、整理して本章を終えたい。

(1)　文化の醸成局面

まず文化とは、機能主義的な見地に立てば、「集団で生活するなかで生まれる諸問題に対する解決策の束であり」、組織の内部的な問題解決と外的な環境への適応のプロセスにおいて生まれたものであることから、「特定の行動や道具の特徴といったように外部からの観察可能性が高く、習慣として維持されてきたもの」である。そして解釈主義的な見地に立てば、「集団で生活するなかで生まれた道具や行為に見い出した意味や価値の体系であり、思考や感情と共に表現されることで社会的に学習され伝達されるもの」といえよう。

一方で、組織が共通目標を持った集団であるという基本的前提に立てば、その目標達成に向けて集団を統制する何らかのシステムが必要であり、これを積極的にコントロールする必要があることが繰り返し主張されている。コントロールの対象は、目に見えるような物理的なもの、目にすることのできない心理的なものと広範に及んでおり、この幅広いコントロールの対象全般を「企業文化」と捉える方が理解しやすい。

特に企業組織の内部という観点では、創業者という明確な起点があり、創業者の成功体験とそこから生まれた価値観が、組織メンバーに共有され、目に見える人工物や目には見えない制度などを意味する「文化的諸要素」として表面化すると同時に、それらを通じて「基本的仮定」として内面化されたことにより深層で機能するもの（Schein,1985; 1999; 2010）であり、無意識的な意思決定とそれにつらなる振る舞いを誘導することになる。

この振る舞いを強く規定する企業文化こそが「強い文化」（Deal & Kennedy, 1982 ; Schein, 1985）であり、O'Reilly（1989）はこういった強い文化を醸成する利点のひとつに「文化と戦略のフィット」を挙げていた。それは、選択された戦略を有効に機能させるためには、戦略の実践を支持する文化が求められるという機序であり、組織目標達成のための一要素として組織文化を捉えるものである。そして、こういった「強い文化」をどのように醸成するかについてモデルとして提示した。そこでは「コミュニケーションの一貫性」と「褒賞」を要件としていた。これらは、経営者層の持つ信念や価値観が、組織メンバーとのコミュニケーションにおいて伝達される中で、その言動に一貫性が見出されることによってメンバーにも組織の価値観として認識され、その認識に沿った行動

が褒賞の対象となることで内面化が促され、組織における規範となり振る舞いとして表出するというものであった。そしてこのプロセスでは、組織体は意識的に「選択と参加」、「シンボリックなアクション」、「他者からの情報」、「包括的な褒賞システム」という 4 つのメカニズムを用いていると説明していた。

(2) 文化変革の局面

ここまでは、O'Reilly（1980）を軸として、文化醸成の局面について確認してきた。しかし、メンバーと環境の変化によって新たな解決策が生まれたり、従来からの解決策が変化し淘汰されることがある。すなわち、組織メンバーの入れ替わりや、外的環境の変化に適応するための新しい目標が設定され、戦略もまた再構築されるのは自然なことであり、さらに、その実践においては戦略にフィットする文化が必要であることは事例による説明を確認したとおりである。

このように能動的に捉え、環境の変化を当然とするならば、文化の変化は避けられないものであり、むしろ変化が必然であるならば、これにも積極的に関与すべきといえる。第 I 章で確認したように「新しいやり方」が求められるのは、組織の活動における個人情報や企業機密の保護についての側面であり、これにフィットするセキュリティ文化が求められるのは、外的環境の変化とそれによる対処すべき新たな課題の発生に他ならない。社会的要請としてセキュリティへの対応が求められており、これが従来からのやり方を許容しない場合は、文化とそれに根差した文化的要素の変革が必要となる。

そこで、文化変革の議論において基本となる解凍－移行－再凍結という 3 段階モデルについて、Schein（1985; 1990; 2010）の議論から確認した。そこでは、まず旧来の組織の慣性を止めるキッカケとなる変化の動機付けとして、現状に対する否定的確認による「生き残りへの不安」と、変化への対応として求められるこれまでの学習棄却と新しいやり方を習得する際の学習遅滞の不安を払拭するための「心理的安全」が求められていた。

否定的確認は 6 種類の情報源からもたらされると整理されていたが、その一つが「スキャンダル」である。しかし、危機感の発生源が、実際に情報セキュリティインシデントを起点として情報漏洩が起こり、メディアなどに「スキャンダル」として取り上げられ、ステークホルダーからの信頼と評判が低下したあとでは遅いのである。この代替となり、本研究に深く関連するものとして、「新技術の導入」と「教育と訓練」の 2 つが挙げられている。彼も IT がその中心と述べていたが、PC やスマートフォンといった情報端末、それらをインターフェースとした情報処理システムや社内イントラ、そしてその両者を組織の外部から接続し処理を可能にするインターネットは、現代で

はすでに「新」技術と呼ぶことが難しいほどに日常業務に浸透している。だからこそここで問題となるのは、これらを利用するに際しての新しい「思考や感情」そしてそれに基づいた「振る舞い」を身に着けることが求められていることなのだ。

そしてこの要求に対して、企業組織において現状についての認識を更新し、メンバー間で共有するためには、統一的かつ末端までの確実な情報提供が必要である。その手段としては「従業員は、環境上の事象にかかわる危険について、教育を受けない限り、責任感ある新しい行動パターンが必要であることを受け入れない」（Schein, 1985, 邦訳書, p.108）という指摘の通り「教育と訓練」が最適であろう。

しかし、危機感を煽りすぎると、現状に対する否定的な認識を棄却させてしまうことにつながる。一方で、新たな学習に対しての不安が高いこともまた、危機への対処に必要な訓練の拒絶につながってしまう。そのため、これらのバランスを取るとともに、これらを受け入れるための要素として「心理的安全」を用意する必要がある。この心理的安全は、①明確で信頼できる将来像、②新しい行動レベルの目標、③学習者に機会があること、④適切なトレーニングと時間と費用、⑤新しい行動に合致した報酬・管理・規律のシステムなどの構造的サポート、の提供が求められていた。この③学習の機会と④適切なトレーニングとは、まさに文化的要素のひとつである企業内での「教育」や「訓練」であると言え、教育と訓練のなかで「①将来像」と「②目標」を明確化し、「目標」と一貫性のある「⑤報酬・管理」、すなわち目標に誘導する報酬システムによって補完される。

同様の指摘は Deal & Kennedy（1982）が挙げていたモデルにおいても見受けられる。彼らのモデルでは、メンバー内での「①合意」と「②信頼関係」醸成のためのコミュニケーション経路を確保することによってメンバー内で目標を明確化し、新しい「③技術養成」のための訓練によって多くのメンバーの参加を促す一方で、新技術の獲得には時間がかかることへの理解を示す「④忍耐」と、現場の実情に合わせてカスタマイズすることや、最終的な結果に一定の幅を許容する「⑤柔軟性」を持つことが求められていた。

これらの点で、文化の醸成と文化の変革の局面の大きな違いは、目的的で体系的な教育と訓練を用意することにあろう。文化は、「常に社会的学習によって伝達される」（Bock,1974, p.14; 邦訳書, p.48）と定義され、醸成の局面では「他者からの情報」が一つの要素であったように、社会的に伝達されるものであることが示されていた。しかし、文化の変革の局面においては、それらを含めてリセットの必要があり、新たな「将来像」や「行動レベルの目標」として特定の方向性とその必要性を「教育」で示し、それに対して一貫性を担保した「トレーニング」や「技術の養成」といった

訓練を意図的に組み込む必要性が強調されている。そしてこれらの教育や訓練のアウトプットを報酬によって促進するという構造になるが、これについては、文化の醸成の局面においても要素として挙げられており、共通したものとなっている。文化の発達・変革に求められるこういった要件や要素については、以下のように整理することができる（表7）。

表7：文化の醸成と変革に求められる要件と要素の整理

O'Reilly（1989）		Schein（1999; 2010）		Deal & Kennedy（1982）	
局面：文化の醸成		局面：文化の変革		局面：文化の変革	
要件	要素	要件	要素	要件	要素
・コミュニケーションの一貫性 ・褒賞	①選択と参加 ②シンボリックなアクション ③他者からの情報 ④包括的な褒賞システム	・否定的確認による生き残りへの不安の醸成 ・心理的安全の醸成 ・2つのバランスをとる	①将来像 ②行動レベルの目標 ③学習機会 ④トレーニングと時間と費用 ⑤構造的サポート	・目標の明確化 ・多くの社員と取り組む ・過度に管理しない	①メンバー間の合意 ②信頼関係(経路) ③技術の養成 ④忍耐 ⑤柔軟性

出典：筆者作成

違いについては次のような点である。組織への個人の新規参入が続くことを前提に、新参者を対象として彼らをいかに組織にコミットさせるのかという観点での議論が醸成の局面である。一方の変革の局面はすでに参入を果たし、一定のコミットメントがあると推定できるメンバーを対象とした議論である。したがって変革の局面における組織内で成そうとする動きは、解凍－移行－再凍結というモデルで示されていたように、従来からの組織的行動からの脱却と、新たな組織的行動の提示、獲得である。ここでは新旧の文化が一時的に並行することを前提として、従来までの組織的なモーメントをゆるめながら新たなモーメントを作り出すという段階がある。新たなモーメントの発生が確認できたのちは、そのモーメントの安定を図りつつ、従来のモーメントから完全に離脱を目指す段階が次段階となる。そして新たなモーメントを加速させ、企業活動の推進力として活用する段階が最終段階となる。しかし、環境が動態であることを前提とすれば組織的な対応も常に行われているのである。この流れを前提とするならば、組織の長期的な発展を目指すなかでは、醸成の次段階は変革であり、変革の次段階は醸成というサイクルが長期的に繰り返されるのであって、醸成と変革を区分して検討する意味は薄い。むしろ、従来からのメンバーも新たな文化においては新規

参入者として捉えなおせば、どちらの要件・要素も区別なく扱う方が、長期的な発展を目指すなかでは合理的である。

これを踏まえれば、O'Reilly が示した文化醸成において組織が用いる 4 つのメカニズム、すなわち 4 つの要素は、文化の変革の文脈であれば次のようになると考える。

「①選択と参加」は、「新技術の導入」と「教育」を通じた「否定的確認」によって動機づけることができ、充足できよう。このなかで生まれる「メンバー間の合意」と「信頼関係」によって「目標の明確化」が図られることも期待できる。

「②シンボリックなアクション」は、組織の新たな方向性を反映した経営層や管理職層の振る舞いであった。これについては、経営層や管理職層も「技術の養成」や「学習の機会」、「トレーニング」に参加することによって組織全体の優先的課題であることを示すことができ、また彼らの成果も共有されることがあるならば、メンバーによる観察と理解を容易にすると考えられる。

他者からの情報の再配置と報酬の再定義がより重要である。「③他者からの情報」は、集団内における振る舞いの質やそのタイミングについても社会的に構成されているという観点から、求められる振る舞いの参照点となるものの必要性が示されていた。そして、その観察の対象は身近な同僚を指していた。こういった集団内の人的ネットワークと文化の関係は、近代組織論における知見である組織内の人間関係の重要性と同様に、企業文化の形成にも公式の組織図とは別に形成される非公式な情報網が重要な役割を果たしているという（高橋, 2006）。Deal & Kennedy（1982）はこれを「文化のネットワーク」（邦訳書 p.20）と呼び、経営者層はこの存在を認め、活用することで、変化を促進する新しい風潮をもたらしたり、緊密な支配機構として利用したりすることが可能になるという。

文化が変わるとは振る舞いが変わることと同義であると考えるが、文化を変えるのであればそういった振る舞いを参照すべき「他者」から得られる情報も、従来とは違った情報が提供される必要があろう。なにより、参照の基準となる「他者」も従来の他者とは違う者が必要になると考えられる。であるならば、新たな文化に沿った新たな「他者」を意図的に創り出し、ネットワークとして管理していく必要があると考えられる。ただし、高橋（2006）が指摘するように、必ずしも公的組織ではないと考えられるため、目にすることは出来ないかもしれないが、これを文化の人工物として捉え、ネットワークとして改組改編を主導することができれば、文化の変化を強力に後押しすることができると考える。さらに、公式組織的にこれを構築することができたならば文化変革のシンボルとして機能することも期待できる。

「④包括的な褒賞システム」とは、文化の変革の局面では賞罰の再設計であり、線の引き直しである。この「褒賞」は、これまで見てきたすべての論者に共通する要素であった。褒賞は、金銭的な報酬だけでなく認知や称賛といった非金銭的なものが有用であるとされるが、議論の中心は何が給付されるかではなく、何に対して給付するか、いかに給付するかというものであった。

文化とは集団内における振る舞いの基準であり、集団内で「受け入れられる／受け入れられない」の線引きとしての賞罰が明確であることがメンバー間の信頼の源泉であるとO'Reillyは主張していた。そのため、新しい文化に沿った新しい振る舞いの獲得の成功に対する褒賞が制度設計に現れる必要がある。これは、狭義の褒賞のみを意味してはいない。同時に罰科もこれに含まれる。ただしここでは、罰科が「ない」ことの表示である。訓練による新技術の獲得の過程における学習遅滞や一時的なアウトプットの低下を許容する「忍耐」、すなわち罰の無いことが前述のネットワークの内部において示されることこそが「心理的安全」の確保につながるのであり、これこそが「包括的」な褒賞のシステムとして機能するのである。この点で先の新設されたネットワークと褒賞制度が「構造的サポート」となるであろう。

(3)　リーダーシップとの関係

前節の表7で整理した要件とは、文化の成熟・変化に必要なこれらの要素をいかにコントロールするかというリーダーシップの発露の対象そのものでもあるが、これに続く組織変革の議論においても経営者層の役割として

・ビジョンを繰り返し伝える、ビジョン達成のための決定に人々を参画させる、努力に対して適切な支援を行う、成功に対して評価し褒賞を与える（Kotter, 1996）

というように、組織の外的環境の変化を察知し、変化の必要性を認識し、それを危機感として組織で共有する（組織内で増幅する）ために不安をメンバーに伝達し、対案となる新しいビジョンを提示し、その実現に向けてメンバーを鼓舞する強い牽引力が強調される（Tushman & O'Reilly, 1997; Nadler, 1998; Taffinder, 1998）。しかし、各論者によって多少の違いはあるが、環境内の危機の発見、組織内での危機感の醸成とそれをテコとして利用する経営者層のリーダーシップの発露に依る点は共通しており、経営者層のリーダーシップに期待が集中しすぎているきらいがある。

この点で、経営者層によるリーダーシップだけではなく、管理者層や現場のフォロワー層によるリーダーシップもまた重要であると考える。それは、Deal & Kennedy（1982）が、Scheinが表現するところの「文化的要素」として求められる5要素を管理することがリーダーシップの役割であ

るとする一方で、プロセスにおいてはそれらを「過度に管理しないこと」を求めていた点にある。文化の変革の局面を論じる Schein と Deal & Kennedy とのモデルとの比較においては、どちらも組織の経営者層の主導で新たな組織目標を掲げ、教育を通して変化を促し、時間をかけて訓練を重ねることで新たなスタイルを獲得するという点は共通しているが、褒賞によるコントロールを強調する Schein と、一定の成果があれば自主性に委ねるという Deal & Kennedy という違いになる。後者は、変化のプロセスの起点となる「目標の明確化」も、信頼性あるコミュニケーション経路を通したメンバー間の合意に委ねるというものであり、フォロワー側の働きも大きい。

このメンバーの自主性は、O'Reilly（1989）のプロセスモデルにおいても見受けられ、将来像や信念についてリーダーによる明確な提示を必ずしも求めてはいなかった。それは、リーダー自身の振る舞いよってそれを示すことができ、その振る舞いからフォロワーは推論が可能であるからだ。そして、推論を確信へと昇華させるのが他者からの情報と褒賞システムというモデルであり、どちらも組織内部の社会的な関係性、すなわちフォロワー同士の関係性に依存するともいえる。

本研究で取り上げる日本国内の企業組織に目を向ければ、管理者層や現場のフォロワーの持つこういった能力や機能について、古川（1990）や金井（1991）は、環境変化に一番近い現場を牽引しながら、一方で収集された情報を分析し、経営者層に伝達するだけでなく、ときには説得することでより良い経営判断を導く働きを中間管理職に見出し、当時好業績が続いていた日本企業の推進力と環境変化への対応のカギは、中間管理職層のリーダーシップにあると主張している。この点で、日本の企業組織における文化の変革は、経営者層のリーダーシップはもとより、環境変化への感度を持ち、組織の上下に影響力を行使することができる中間管理職層が存在するという組織的な強みによって方向付けられ、また推進されることが期待されるため、このような人材をエンパワーメントすることも文化変革の実務においては肝要だと考える。これが自主性のコアとなり「過度に管理をしない」、すなわち「現場に即した適度な管理」が生まれることが期待できる。ただし、これは単にメンバーの自主性に委ねるということを意味しない、メンバー間の合意、すなわち相互作用によって生まれるものを尊重するのであり、この相互作用を導くことこそがリーダーシップの根幹となろう。

(4)　実務における課題

本章の最後に、実務において組織文化を取り扱うことの課題を述べて終えたい。

本章では企業文化の醸成や変革をマネジメントの問題としてこれを捉える先行研究を確認してきたが、実務において、企業文化をマネジメントしようとする際の端的なまとめは次のようなものとなる。

まず、文化の変革といった大掛かりなものはもとより、何か新しい取り組みを企図する経営者層は、強いリーダーシップによるけん引というだけではなく、メンバー間での合意形成を主導することで目標達成を果たしていく必要がある。これは、組織的な慣性、すなわち従来までに最適化されていた日常を断ち切るためには相当な力が必要となるからである。その力は、O'Reilly が文化醸成のメカニズムとして指摘していたように、新たな方向へ進むことの意思決定への「参加」であり、コミットメント向上によってもたらされることが期待できるからである。この前提として、新たな方向へと転換の必要性を認識させ、新たな活動へと動機づけるためのキッカケとしての「教育」と、メンバーの働き方そのものに密接に関連する「IT」の掛け合わせは、もっとも有力なものとして注力する必要があろう。

さらに「目標の明確化」も、信頼関係醸成のためのコミュニケーション経路を確保することによって組織内で自主的に図られるとされることから、教育と対になる訓練をコミュニケーション経路の１つと位置づけ、新たな目標達成に求められる新しい技術養成のための訓練の機会を可能な限り多く提供し、訓練を通じたコミュニケーションに多くのメンバーの参加を促すことが求められよう。

そして、このコミュニケーションを通じて醸成される「信頼関係」は、新技術の獲得には時間がかかることを理解した「忍耐」が、獲得のプロセスにおける失敗の許容として表現されていることによって生まれる「心理的安全」をベースに醸成されることを認識することに加え、現場の現実に合わせたカスタマイズを許容する「柔軟性」を維持することが求められることを認識する必要がある。

特定の目的達成に向けた企業文化を持つにはこのような要件があり、目標に沿ったシステムとして実装する際にはこのような要素を取り込む必要があるのだが、これをどのようにクリアしていくのかというのが実務的な課題となる。それは、本研究が実在する企業組織における実務を研究の対象とし、そこから文化醸成について何らかの知見を得ようとするものであり、組織目標達成に対する機能主義的な議論は避けることができないことによる。

実務的なプロセスとしては、環境の変化に対応した特定の将来像を新たな企業文化、すなわち価値観を共有した集団の像と共に示し、その状態への到達に向けて教育や訓練が企画され、実施に移

される。その実施後において何らかの指標を測定し、その指標の変化をもってして文化の醸成や変化の進展の度合いとして認識し把握することで、その教育や訓練の展開もまた強化や修正が図られることになるだろう。マネジメントである以上、こういった取り組みの成果が最大の関心事であり、結果の把握が最終的な課題となるはずである。具体的には、文化的諸要素の変化とそれに沿った活動のアウトカムの測定と把握の問題である。しかし、文化はマネジメントの対象であるとする一方で、それはメンバーの内面の問題であるとされる。この点で、何を、どのように測定することによって何を把握すべきなのであろうか。そして測定され、把握されたものは果たして本当に文化なのだろうか。

何らかのシステムの整備を通して、メンバーが新しい組織目標の達成に向けて新しい価値観を共有し、統一されることが最も望ましいが、本質的に統一されているかどうかは、あくまでも個人の内面レベルの問題であり、これを正しく測定することは不可能であることもまた従来から指摘される通りである（Shein,1985; Deal & Kennedt,1982）。

これは矛盾ではなく、メンバーの内心の問題であるがゆえに外部からそれを正確に測定することが困難であることを指摘している。しかし、その困難さを前提として、ここに踏み込まなければ、それは企業文化として醸成されたといえるのか、変革されたといえるのかという本研究の根本的課題の解決とは言えない。であるならば、内面に影響をもたらすマネジメントが求められるとともに、測定されるアウトカムが内面に支えられたものであることを確かめる必要があり、何らかの方法で試みることが求められていることは間違いない。

文化のマネジメントの第 1 の成果として直接的にアウトカムを把握することができるものへのアプローチが必要であるのは言うまでもないが、それだけではなく、困難を指摘されるメンバー個々人の内面の把握が必要であり、これにいかにアプローチするかを留意点として残しながら、本論をすすめることとする。

Ⅲ セキュリティ文化とはどのような文化か

本稿では、まず序章において、現代の企業組織の経営においては情報そのものと情報を活用するための情報システムの重要性が高まっており、同時に、活用だけではなく保護に対する取り組みが強く求められていることを述べてきた。そして第Ⅰ章では、いわゆる情報インシデントの原因を確認しながら、対応となる情報保護への取り組みについて、ITを充実させるといったハード的なアプローチと、これを用いる人に対するソフト的アプローチとしての教育や研修というだけでなく、これらを包括した組織内のメンバーによる社会性からのアプローチの必要性を提起した。これに応じるため、第Ⅱ章では組織文化なかでも企業文化がいかに醸成されるのか、さらには、常に変化する外的環境への対応として、それまでに醸成されてきた文化を新たな文化へと変革するために求められるものを先行研究より整理し、確認した。

この第Ⅲ章では、こういった経営環境下にある企業組織に求められている文化とはどのようなものであるかについて、そして情報と情報システムを利用する際に求められる組織メンバーの振る舞いはどのようなものであるかについて検討したい。まず、本研究の関心の中央にある「セキュリティ」を冠してOECDによって提示された「セキュリティ文化」について確認する。次いでこのセキュリティ文化の類例として提示される「原子力安全文化」について概観しながら、2つの文化についての比較をとおしてセキュリティ文化の醸成が困難である要因を探る。そして、最後に企業組織に求められるセキュリティ文化とはどのようなものであるかについて、組織的な事故とその防止についての研究の第一人者であるReason（1997）による「安全文化」をベースとして検討する。

1 OECDセキュリティ文化

情報ネットワークと情報端末の利用が一般市井へと急速に広がっていくなかで、OECDが提唱した概念が「セキュリティ文化」である。2002年に策定された「情報システムおよびネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて（OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security）」のなかでセキュリティ文化は、

> *“culture of security – that is, a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks”.*

「情報システム及びネットワークを開発する際にセキュリティに注目し、また、情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れること」[40]

と説明される。

これ以前にも、情報システムの開発や運用といった専門的な業界内では1992年に策定された、Guidelines for the Security of Information Systems（情報システムのセキュリティに関するガイドライン）が存在していたが、①インターネット利用者の増加による相互連結性が増大していること、②エネルギー、輸送、金融といった重要インフラはもとより、一般ビジネスだけでなく行政サービスの提供にも不可欠となっていること、③ICTの発達により通信そのものが変化し多様化していることの3点が背景にあるなかで、2001年に発生した米国での同時多発テロの発生を受け、テロなどの外部からの悪意を意識した形で改訂が加えられたと説明されている（OECD, 2002, p.7）[41]。

この新しいガイドラインでは、①認識、②責任、③対応、④倫理、⑤民主主義、⑥リスクアセスメント、⑦セキュリティの設計及び実装、⑧セキュリティマネジメント、⑨再評価という9つの原則が示されている。

以下の表8は、規範として示された各原則の一覧である。

「①認識」では、自らの利用する情報システムに障害を発生させることは、これにつながる情報ネットワークの性質上、他者にも損害を与えうることを理解し、参加者としてセキュアな利用法についてまず認識することを求めている。

「②責任」では、参加者それぞれのITリテラシーに合わせて応分の責任を持つことを求めている。エンドユーザには利用する製品やサービスのセキュリティ手段を定期的に検討することを、開発者においては製品やサービスのセキュリティ向上に取り組むとともにエンドユーザが責任を果たせるような情報提供の努力を求めている。

「③対応」では、ネットワークの特徴として被害の拡大が速い点を挙げ、インシデント発生時には参加者のタイムリーな協力を求めている。また、開発者レベルに対しては、情報共有だけでなくインシデントの予防や検出、対応においての協力関係の構築を要請している。

---

[40] 経済産業省／情報処理振興事業協会セキュリティセンター（2002）「新OECD情報セキュリティ・ガイドラインの概要」の訳による

[41] 日本国内においても、同時期に重要インフラに対するサイバーテロを前提とした対策案をまとめている。「重要インフラのサイバーテロ対策に係る特別行動計画」（2000年12月12月 情報セキュリティ対策推進会議決定）

表8：OECD セキュリティ文化の原則

	原則	命題
1	認識の原則	参加者は、情報システムおよびセットワークのセキュリティの必要性ならびにセキュリティを強化するために自分たちにできることについて認識すべきである。
2	責任の原則	全ての参加者は、情報システムおよびネットワークのセキュリティに責任を負う。
3	対応の原則	参加者は、セキュリティの事件に対する予防、検出及び対応のために時宜を得たかつ強力的な方法で行動すべきである。
4	倫理の原則	参加者は、他者の正当な利益を尊重すべきである。
5	民主主義の原則	情報システム及びネットワークのセキュリティは、民主主義社会の本質的な価値に適合すべきである。
6	リスクアセスメントの原則	参加者は、リスクアセスメントを行うべきである。
7	セキュリティの設計及び実装の原則	参加者は、情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである。
8	セキュリティマネジメントの原則	参加者は、セキュリティマネジメントへの包括的アプローチを採用するべきである。
9	再評価の原則	参加者は、情報システム及びネットワークのセキュリティのレビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。

出典：OECD（2002）Guidelines for the Security of Information Systems and Networks Towards a Culture of Security, pp.9-12 より筆者作成
訳は、経済産業省／情報処理振興事業協会セキュリティセンター（2002）による「新 OECD 情報セキュリティ・ガイドラインの概要」による

「④倫理」では、第 1 の原則である「①認識」で求められていた、ネットワークのアンセキュアな利用は他の参加者の利益を害する行為であるという認識に基づいて、ベストプラクティスを採用することで他者の利益を尊重することを求めている。

「⑤民主主義」とは、セキュリティの在り方とその実践について述べるものであり、ネットワークを通じて行われる情報交換の自由や秘密の保護といった、民主主義社会において認められる個人の自由とその保護を尊重することを求めている。これは、組織のシステム管理者や開発者だけではなく、サービスプロバイダといったインターネットレベルの管理者をも意図していると捉えることができる。

「⑥リスクアセスメント」とは、リスク判断、すなわちどの程度セキュリティに注力するかの前提として、自らに対する脅威、および自らの脆弱性を検討し、他者から受ける、または他者に与えうる潜在的な損害について考慮することである。これは主に組織的な情報システムの管理者に対する要求であるが、エンドユーザ個々人にも求められているといえる。

「⑦セキュリティの設計及び実装」は、守るべき情報価値に対して適切に設計されたシステム、ネットワーク、ポリシーを採用し、製品やサービスの選択をすることを求めている。そのため、主に情報システムの開発者や管理者に向けられたものとして捉えることができるが、エンドユーザに対しても、自らの利用する情報端末について製品やサービスの適切な選択を求めている。端的には情報端末の利用や選択に際して広く情報収集を求めるものといえる。また、情報資産の価値との比例を前提としていることから、組織・個人が持つ情報資産の価値の評価が行われることを前提としており、「⑥リスクアセスメント」と表裏のものとして理解できる。

「⑧セキュリティマネジメント」では、先の「⑥リスクアセスメント」に基づいて、あらゆる階層のあらゆる運用について、将来的なインシデントの予見とその予防から発生時の対応、発生後の復旧、平時の保守や監査といった包括的なマネジメントを行うことを要請する。これは、組織的な情報システムの利用者、なかでも開発者や管理者に向けられたものと理解できる。そして、セキュリティ体系の一貫性を確保するために、セキュリティポリシーと現場における手続きや手順との調和（co-ordinate）を求める。ゼロリスクを追求する強権で硬直的なマネジメントの追求ではなく、情報資産の管理と活用のバランス問題として、現場のオペレーションにおける負担や現実的なコストと効果いった視点から検討すること求めていると理解することができる。

そして、最後に「⑨再評価」である。これは、進化する脅威を認識し、これに対応するためにシステムやネットワークのセキュリティを再評価し、更新しつづけることを求めている。

いずれの原則においても、情報機器とそれが接続する情報ネットワークを利用する者すべてを「参加者（participants）」と呼び、「すべきである（should）」と結んで（書き出して）いる。民主主義の原則にあるように、自由と権利を重視した世界ではあるが、自由に利用する権利に対する参加者の義務として、セキュアな利用についての諸ルールが課された世界へ「参加」するための心得である。個々の能力には当然に差があることを前提としつつも、ネットワーク利用におけるリスクに対処すべく、有効なポリシーを作成し、それを実践し、全員がそのセキュアな利用について当事者意識を持つこと、すなわち情報ネットワークのセキュリティ維持を自らも担っているという「当事者性」を求めていると考えられる。

学術的にはセキュリティ文化は次のような定義がされている。

- *the assumption about those perceptions and attitudes that are accepted and encouraged in order to incorporate information security characteristics like the way in which things are done in an organisation.*
  組織内での物事の進め方といった、情報セキュリティの特性を組み込むために受け入れられ、

奨励されているも認識や態度についての仮定(Da Veiga & Eloff, 2007, p.362)

- *The collection of perceptions, attitudes, values, assumptions and knowledge that guides how things are done in organization in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behavior in a way that preserving the information security becomes a second nature.*
  情報資産を保護し、情報セキュリティを守ることが第二の性質になるように従業員のセキュリティ行動に影響を与えることを目的とした、情報セキュリティの要求事項に整合するために組織内でどのように物事を行うかの指針となる認識、態度、価値観、仮定、知識の集合体
  （Alhogail & Mirza, 2014, p.2）

これらの定義も、ここまでに確認したOECDの「セキュリティ文化」（2002）の定義や、そこで併せて示された原則などを踏まえ、情報の保護という課題に対する集団の活動の持つ特徴や解決策の束という機能主義的な見立てである。これら先行研究のレビューを行った Mahfuth ら（2017）は、情報セキュリティ文化の標準的な定義はなく、情報セキュリティ文化の学術的定義の多くは主にSchein の文化の三層モデルの議論から整理を試みたものであると述べている（p.5）。そして、主にZakaria(2006)の研究を踏まえ、次のような定義を行っている。

- *classified as a subculture of an organization and it includes the daily tasks, activities, guidelines and practices of the employees in an organization which should help them to protect the organization's information assets and reduce the risks to those assets.*
  組織のサブカルチャーとして分類される、組織の情報資産を保護し、それらの資産へのリスクを軽減するのに役立つ、組織内の従業員の日常業務、活動、ガイドライン、および慣行
  (Mahfuth ら, 2017, p.2）[42]

これらの定義がなされた年代を経て、技術の進歩と利用者の増大によって、あらゆる業界の活動において情報機器や情報端末の利用が深く浸透し、情報セキュリティインシデントが大規模化していることを受け、2015年にOECDは、これを媒介するインターネット利用からの利益の享受を維持するためには、組織の意思決定のプロセスにリスクマネジメントとしてデジタルの視点を取り込む必要があるとし、これを訴える“*Digital Security Risk Management*”を公表している。電子データを扱う環境をデジタル環境と呼び、この空間に参加する人々による、セキュリティの向上の自主的な活動を求めている。企業組織であれば、インターネットを利用したE-コマースの発達を前提とし

[42] 訳はいずれも筆者による。

て、そこで扱われる個人情報の保護を重視する必要がある点で、このデジタル環境でのセキュリティを意味するサイバーセキュリティとしてリスクマネジメントに取り込み、検討していく必要がある。このサイバーセキュリティについてVon Solms & Van Niekerkk（2013）は、人々がサイバーセキュリティを認識する方法と、デジタル情報、システム、および人々の保護に影響を与えるサイバースペースにおける結果的な行動に関係しているものであるとし、Von Solms & Von Solms （2018）は、情報セキュリティのサブセットとしている。

本研究では、情報を扱う際の認識と振る舞いについて検討を試みており、ネットワーク利用とデジタルデータの扱いに限定したサイバーセキュリティだけではなく、これらを含みより包括的な情報セキュリティの向上を企図している。しかし、企業組織の活動においてこれらを利用することは日常的なことであるため、サブセットとされているが、ネットワーク利用とデジタルデータの扱いからアプローチすることは意味あることだと考える。

2 原子力安全文化

前節において述べた「当事者性」という点では、このセキュリティ文化に先んじて提案された概念として、IAEA[43]による「原子力安全文化」（INSAG-4[44], 1991）がある。

その定義は次のようなものである。

> "*Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.*"
>
> 「*安全文化とは、組織体および個人における性格と姿勢とが一体となって、原子力プラントの安全問題が、最高の優先度をもって、その重要性にふさわしい注目を受けるようにするものである。*」[45]

この原子力安全文化は、1986年に起きたチェルノブイリ原発事故における施設管理者たちのCan Do文化[46]に対する批判として提唱されたものである。この原子力安全文化の概念モデルも、

---

[43] International Atomic Energy Agency：国際原子力機関

[44] International Nuclear Safety Group：国際原子力安全諮問グループ。上記のIAEA事務局に対する助言・勧告を行う専門チーム。

[45] 訳は筆者による。

「安全問題の最優先」という組織的に「標榜する価値」を中心として、表層となる「人工物と振る舞い」、深層となる「基本的な仮定」という Schein（1985）による企業文化の三層構造として表現される（倉田, 2014）。そして、方針レベル[47]・管理者レベル・現場レベルといった組織の階層にかかわらず、すべての個人が安全についての当事者意識を持ちながら業務を遂行するというものであり、すべてにおいて安全確保が優先するという態度と素養の集合的マインド[48]が維持された状態を意味する。

原子力安全文化の持つ特徴としてまず 1 つめに挙げられるのが、原子力安全を、プラントを管理運営する「運転体」にのみ委ねるのではなく、「政府及び規制行政体（以下「規制体」）」と、設備メーカーや研究機関などといった「その他の支援組織体（以下「協力体」）」を安全の担い手として当事者に含めることである。運転体とは、主に商用原子炉を用いて発電を行う電力事業者を指す。規制体とは、電力事業者等に対して法などによる規制をかける行政などの監督機関である。2019 年現在の日本では原子力規制委員会などがこれにあたる。協力体とは、原子力発電プラントの建設や原子炉そのものの設計製造を担うメーカーなどを指し、原子力利用に関する研究機関などの学術分野もここに含まれる。そして 2 つめとして、これらの 3 者は「オープンで協働的」な関係性であるとしたことである。「規制体」という表現からは規制者と被規制者という「運転体」との上下・従属関係のものとして認識されてしまいそうであるが、それぞれ「異なる説明責任」があるとしてこれを否定し、運転体・規制体・協力体のそれぞれ 3 者がフラットな立場で先の集合的マインドによってもたらされる現状認識を共有することによって安全状態が達成・維持されるという（INSAG-4, 1991）。

---

[46] 過去の成功体験に依拠した自身の能力を過信した状態であり、個人の態度としては「なせばなる症候群（can do syndrome）」と表現されることもある。

[47] 一般的には経営者層を意味する。一般に見受けられるマネジメントシステムなどで、経営者層によって決定され、示される全社的な大目標やポリシーを「方針」と呼ぶことが多いことによる。

[48] この「集合的マインド」とは、原子力発電所や送配電網といった複雑な技術システムを扱う組織を参与観察した高信頼性組織研究による知見の 1 つである。代表的な研究者である Weick によれば、まず「マインド」について、定められたルーチンワークにおいても「いつも通り」という思い込みを懐疑的な態度で排除し、現在の状況における僅かな違いに注意を払い、新奇な状況にも意味付ける能力と説明する（Weick, 2001）。端的には「現状認識における注意力の質」として表現でき、こういったメンバーの注意深さが組織的に表れた状態といえる。

原子力安全文化において、運転・規制・協力の 3 つの立場、そしてそれぞれの組織内の 3 つの階層について対等な関係を強調することは、いかなる理由であろうか。原子力安全文化においては、すべての者が「安全」を志向の中心に据え、組織内の階層レベルの違いについても、例えば上位層からの指示があいまいであったり、現実にそぐわないものであったりした場合にも、盲従することなく立ち止まり、保守的な判断を自らの責任で行うことを推奨している。これについて倉田（2014）は、メンバーが訓練を積むことだけでなく「自分が現在の業務に対してプロフェッショナルであると自覚しているかが仕事の質の向上に大きな影響を与える」（倉田, 2004, p.119）と述べ、自らの担う業務に対する責任と自信と誇りという「プロ意識」によってさらなる安全に向けた研鑽が導かれるという。そして、安全を確保することを通して社会に貢献し、また安全の欠損によって社会にマイナスの影響を与えうる立場にあるという「使命感」もまた安全に対する組織と個人の姿勢の向上に重要な要素であるとする。すなわち安全に対して自らが積極的に寄与するという「主体性」と、自らも社会に影響を与えうる関与者であるという自覚である「当事者性」を持つことが概念の中心にあると考えることができる。

3 セキュリティ文化を醸成することの課題

原子力安全文化とセキュリティ文化の類似点と相違点について名和（2005）は、双方がマニュアル化を目指すものであることを類似点として挙げる一方、管理方式に違いがあると述べる。類似点として挙げるマニュアル化とは、OECD が原則に掲げた順番からこれを、認識、信頼醸成、枠組みの作成、ポリシー策定、行動様式、手段、手順の開発、標準の整備というように整理し、「目的が結局は文化のマニュアル化になっている」（名和, 2005, p.252）と批判する。すなわち標準化、いわゆる Know-How の定着を求めるものであって、第 II 章で確認したように文化の本質である標榜する価値の内面化とは別のものであるという指摘として理解できる。

相違点となる管理方式については、原子力はその特殊性から技術と装置が関係者に独占されていることで完全な管理が可能であるのに対し、IT と情報ネットワークは万人に開放され、さらにユーザーレベルのバラツキが大きいことからそれが難しいという。この点で、原子力安全文化は専門家と専門組織向けのものであり、セキュリティ文化は万人向けのものであると述べている（名和, 2005 , p.255）。

万人に向けられたものだからこそ OECD のセキュリティ文化の概念においては利用者を「参加者」としてことさらに「当事者性」を強調することにつながっていると推察することができる。原

子力安全文化で求められていた「プロ意識」すなわち、安全確保に対する積極的な姿勢として表現される「主体性」をも同時にエンドユーザに伴わせることは難しいであろう。セキュリティ文化が普遍的なものとなる、すなわち OECD が提示した種々の原則が当然のこととして人々に取り込まれ、行われるようになることが困難である理由はここにあると考える。

企業レベルでは、知的財産を含む営業秘密は競争優位において重大であり、核心的なものであるほど、その取扱いも慎重さを増し、パスワードや暗号化による保護、アクセス権のコントロール、最終的には物理的な切断などの手段が採られる。しかし、これが日常的な業務プロセスでの活用のレベルまで降りてくると、携帯した PC や USB メモリを紛失する、機密性の高い情報の印刷文書が適切にファイルされず机上に留め置かれる、パスワードが共有され使いまわされる、サーバ内での利用が義務付けられたデジタルデータをローカル PC にダウンロードする、そして利用後に削除もせず保存してしまう、というようにポリシーとかけ離れた運用が散見される[49]。このように、エンドユーザが自ら扱う情報と利用するネットワークに対してセキュリティを意識できない理由はどのようなものであろうか。

まず 1 つ目として考えられるのが、環境認識の限界である。自らが利用している情報端末とそれが接続されているネットワークといった情報環境に対する認識である。意識できるのは職場として目に見える範疇がせいぜいの限界であり、全社的なもの、場合によっては世界規模に悪影響を与えうるものとしてこれを認識しづらいこと、いわゆる「システム思考」[50]には至らないことにある。

そのベースには、情報セキュリティが技術の問題であるという認識が一般にはあり、自分には無関係であるという態度になりやすいことであろう。寺田ら（2014; 2016）は、「ウィルス感染」「詐欺被害」「情報漏洩」の被害を経験した 2000 名に対する調査から、リスクよりもメリットを優先することを意味するベネフィット認知が強い人物はマルウェア感染や詐欺にあいやすく、PC 操作やインターネット利用について自信のある人、惰性で行動する傾向の強い人については情報漏

---

[49] より一般的なポリシー違反の例については、次を参照されたい。Oracle「よくあるセキュリティー違反」https://docs.oracle.com/cd/E19253-01/820-4576/appol-5/index.html

[50] 問題解決に際して、問題発生の機序を事象の背景にある複数の要因の全体的な構造から検討し、問題の個別最適ではなく全体最適としての解決を志向するアプローチ。マサチューセッツ工科大学でシミュレーション技術として開発された（Sterman, J. D., 2000）。経営学への導入においては、Senge, P.（1990）による『学習する組織』などが著名。思考の特徴として、大局観・動的・循環（因果）などが挙げられるが、組織がこれを採れ入れるときの問題（学習障害）の克服として、メンバー個人の信念と集団としてのメンタルモデルの改善、そしてビジョンの共有を図ったうえでのチーム学習を訴える。

洩の被害が多い、そしてセキュリティ対策は手間であるというコスト認知の高い人はウィルス感染しやすいことを見出している。これらは、「自分だけは大丈夫」という正常性バイアスとともに、場合によっては、ウィルス等の感染によって端末の不具合が生じても「困るのは自分だけであって他人には迷惑をかけていない」というように、被害の範囲についての認知を矮小化し、自らもネットワークの一部を構成している「当事者」であるという認識になりにくいことを表わしているのではないだろうか。どちらも個人の情報リテラシーレベルの問題といえるが、これらは、私生活であれば携帯回線やインターネット、企業組織の内部であれば情報システムといった情報の媒介物がおおよそインフラとして提供されているため、利用できて当然のものであり、そこから利便を得ているにもかかわらず、利便に対する反対給付としてセキュリティに対する貢献は考えにくい、という一方向性のものとなってしまう。職業生活において情報端末や情報ネットワークをまったく活用していないことは考えにくいが、利用していても組織内の情報システムの範囲の認識は持ちづらいのであり、これがプライベートで使用する情報端末であればなおさらのことであろう。

2つ目として、保護の対象となる客体のタイプの問題で「自分事」にしづらい、先の原子力安全文化において求められていた「当事者性」を持ちにくいことである。

先の原子力安全文化との比較では、先に確認した文化の定義となった「INSAG-4」に続く「GSR Part3」(IAEA, 2006)において、

> *"The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards."*
>
> *「適切な運転状態を確保すること、事故の発生を防止すること、あるいは事故の影響を緩和することにより、業務に従事する者、公衆および環境を、放射線による過度の危険性から守ること」*[51]

というように、何から誰を（何を）守るのかということが明確に示されており、物理的にイメージがしやすい。だからこそ倉田（2014）が、安全文化を醸成するためのポイントの1つとしてプロ意識と使命感を挙げたように、原子力安全文化は原子力プラントに関連してベネフィット（ここでは単に生活の糧、給与と考えてよいだろう）を得ている人々に対して、彼らが持つべきプロフェッショナリズムを強調し、自らの業務に対してプロ意識を持つことを求めている。

---

[51] 訳は筆者による

一方のセキュリティ文化は、

> *「情報システム及びネットワークを開発する際にセキュリティに注目し、また、情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れること」*[52]

と述べるのみであり、これにつづく原則でも、参加者であることを当事者性として強調するものの、何を守るのかを明確には謳ってはいない。

いずれの文化もツールとして対象物を利用するエンドユーザに対して当事者意識を持つことを求めているのではあるが、原子力安全文化では注意の対象である原子力がそのままベネフィットの直接的源泉であるのに対して、情報システムは自己の業務を遂行する上での単なるツールの一つでありベネフィットに直接結びつくものではないことから、その利用についてプロ意識を持つことを求めるのは難しく、また過剰ともいえよう。たとえば、現代的な生活に欠くことのできないスマートフォンは情報端末そのものであるが、私的所有者をエンドユーザと見立てたならば、「管理方式の違い」として名和が説明していたように、膨大な数のユーザが利用する開かれた世界であり、その利用法も多様なことから抽象的な表限にとどまらざるを得ないのだ。

そして、3つ目として、セキュリティ文化の議論の対象となる保護の対象物として、直接目視することが難しい電子情報を保護することが含まれているが、セキュリティが破られることによる被害についてはイメージしにくいことである。放射線も電子情報もどちらも目には見えないが、放射線が漏れ出ることにより起きる被害が物理的にも身体的にも目に見える形で発生する原子力と比べ、電子情報の漏洩は悪用され被害が具体化するまでにタイムラグがあることが多く認識しにくい。また、自分自身の生命・身体・財産に具体的な損害が発生し、被害の対象となることもイメージしにくいのだ。たとえば顧客情報であれば、本来は企業が「預かっている」という位置づけのものであり個人や組織の所有物ではない。そして、保護の対象として認識されるのは個人情報そのものにとどまってしまい、そこから派生する権利という非常に抽象度が高く、概念的であり、これもまた目には見えないものまでは認識されていないからだと考える。たとえば個人情報保護法は、その目的を定めた第1条の末尾において、「個人の権利利益を保護することを目的とする」とある。これは、保護の対象は個人の権利であり、個人情報の保護はあくまで手段であることを意味する。具体

[52] 訳は筆者による

的には、個人情報は、生命・身体・財産と同列であるプライバシー権に直接かかわってくるという点で、基本的人権に含まれるものであると考える。

しかし、プライバシー権は概念的でもあり、直接に自分が侵害するというイメージがしにくいため、逆からの説明をするならば、流出した情報が悪用され被害として具現化するまで、情報の流出それだけでは被害とは認識しにくい点で、情報保護に注力することを自分事にしにくいのであろう。しかし、いかに些細な情報であっても、それを悪用しようとする者にとっては十分であり、生命・身体・財産の侵害が発生するかもしれないのだ[53]。さらに、こういった情報を保護する立場のとして活動する個人も、組織を離れれば消費者や生活者としての側面を同時に持っているはずであり、そこでは個人情報を「預けている」個人・顧客となるが、サービスの受益や利便性との関係において提供した自らの個人情報の価値には無頓着な行動をとりがちである。

このように、自らもネットワークの一部を構成する者であるがその認識は持ちづらい。そして、誰から何を守るのは個人レベルでは具体的に意識しづらい。さらに、誰もが加害者にも被害者にもなり得るにもかかわらず、その実害をイメージしづらい。この 3 点が相まって、当事者性を持つことを繰り返し求められているが、当事者意識を持つことはかなりの困難となっていると考えられる。

ここまで見てきたように、セキュリティ文化の醸成には、その前提として、

・自らの振る舞いがすべての情報環境に影響を与えうるという認識になりにくい
・電子情報であれば、情報そのものは目で見ることはできない
・情報インシデントによって自分の身体財産が直接的に侵害されることの想像が働きにくい

という特徴を持つ。

またインシデントとして現実化した時、組織レベルでは多大な金銭的なコストがかかることはもとより、組織に対しての罰則と社会的制裁は大きくなることは、これまでの実事例や第 I 章でふれたように GDPR の例[54]を鑑みれば想像に難くないが、従業員個人レベルでは故意の情報の持ち出

---

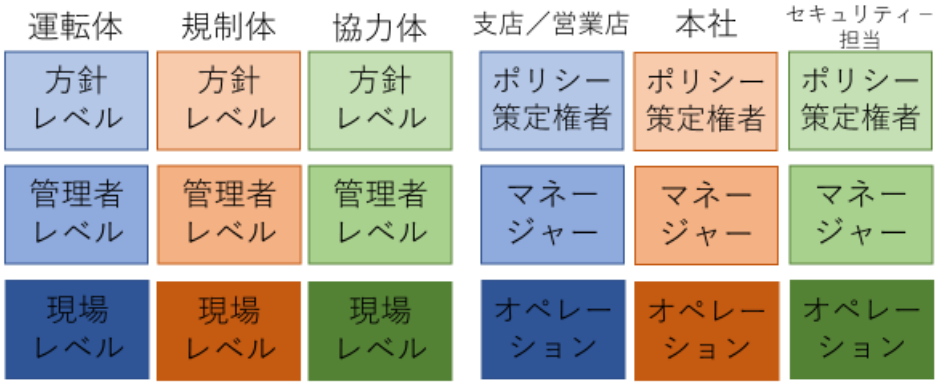
[53] 情報ネットワークを介したデジタルデータの漏洩事例ではないが、地方自治体からの個人情報の漏洩により身体・生命の重大な侵害に直結した事例がある。詳しくは内田（2015）「情報セキュリティからみたストーカー殺人事件の考察」などを参照されたい。

[54] 制裁金の上限基準が、企業の全世界年間売上高の 2%、または、1000 万ユーロのいずれか「高い方」と定められている（第 83 条第 4 号）。具体例については脚注 21 を参照されたい。

しなどの内部不正を除けば直接的な罰則は考えにくい[55]。このように、ポリシー策定者としての経営者層とポリシー運用者としての管理者層、そしてポリシーの遵守を課された現場の人々のリスク評価の相違が実務的に問題となって現れているのだ。

媒体にかかわらず情報セキュリティとその備えは企業になくてはならないものであるが、こういった特徴から、OECD の定義するセキュリティ文化とその原則は、組織のメンバーにおいて内面化しにくいといえる。だからこそ、開発者や管理者と組織内の一般的な利用者を結び付けるという点で、特に組織運営においては原則「⑧セキュリティマネジメント」が重要であり、中心的課題となると考える。しかしそれは、およそ利用者の実態を無視したポリシーが一方的に設定され、利用者には「面倒」という理由で無視されやすい。巨額の費用をかけ開発されたセキュリティ向上のためのシステムは、オペレーションの実際を無視した設計がゆえに利用されないまま廃棄されるという事例まであるように[56]、実際の組織においてセキュリティと現場の実務の調和を目指すマネジメントは難しく、それゆえセキュリティ文化を醸成することも難しいといえる。だからこそ、参加者としての「当事者性」を向上させるためにも、原子力安全文化を参考としてこれを一般的な企業になぞらえれば、ポリシーの策定者としての経営者層、ポリシー運用者としてのマネージャー、そしてオペレーションの現場という 3 つのレベルが情報セキュリティについて集合的マインドを維持し、支店や工場といった営業拠点・本社・情報システムなどを含めたセキュリティ担当部門の 3 者で現状認識をアップデートし続けることであると考えられる。

図 3：原子力安全文化とセキュリティ文化の 3 層



出典：筆者作成

[55] 少なくとも、本稿の中心的テーマとなる標的型メール攻撃によって情報漏洩の踏み台にされたことそのものによって個人が民事・刑事の被告として訴訟が進行した例はない（2019 年 8 月現在）

[56] 日本経済新聞「政府のサイバー攻撃対策システム、全く使用せず廃止、開発に 1 8 億円、検査院調査」2019 年 10 月 29 日朝刊

4 安全文化

セキュリティ文化の基本的な概念について原子力安全文化と比較しながら確認し、セキュリティ文化を醸成することが難しい理由について検討してきたが、こういった文化が求められている産業界には、普遍的に追求され、標榜される「安全第一」という言葉があり、この「安全」を関心の中心に据えた文化として「安全文化：Safety Culture」（Reason, 1997; 2003）の概念がある。組織における安全の考え方について最も多く引用されているのがこの概念である（刈間・井上, 2007）とされることからも、本節では原子力安全文化の基底となっており、セキュリティ文化の基底となることも期待できる「安全文化」を確認したい。

組織事故の研究者である Reason（1997）によれば、「安全文化」とは「情報に立脚した文化：informed culture」（邦訳書, p276）とされる。これは、組織内の情報の流れが活発な状態を指し、その情報は①報告する文化（reporting culture）、②公正な文化（just culture）[57]、③柔軟な文化（flexible culture）、④学習する文化（learning culture）、という 4 つの構成要素により引き出されるものであるという（邦訳書, p.278）。

「情報に立脚した文化」とは、経営者層が正しい判断をするためには、組織内で起きていることについて正確な情報を取集する必要があり、そのための効果的なシステムである「安全情報システム」が備わった状態を意味する。ただしこれは、現場から経営者層という上方の流通のみを意味しない。現場の人々が問題に直面した時に正しい判断を自律的に下すためにも、等しく正確な情報を持っている必要があるとする。そのため情報がいきわたった文化としても理解できる。

「報告する文化」とは、この安全情報システムが機能するための土台といえるものであり、実際に発生したアクシデントや潜在的な危険と隣り合っている現場の人々の積極的な参加を前提としている。このため、自ら犯したエラーやミス、そしてニアミスをも積極的に報告しようとする雰囲気が求められている（Reason, 1997）。そのため、報告を促進するために求められるものとして、自分の犯したエラーやミスは隠したいという感情を取り除くこと、報告することが罰則につながらないこと、報告することが組織の改善に役立っている実感が持てること、報告の簡便さを備えることが求められる（Reason, 2003）。

---

[57] 訳は筆者による。芳賀（2012b）などでは「正義」の訳が当てられ「公正」はカッコ書きで併記の形をとっている。

「公正な文化」とは、第II章で確認した文化の定義にも見られた「許容できる行動と許容できない行動の境界がどこにあるのか」（Reason, 1997, 邦訳書, p.278）が明確であり、メンバーがそれにコミットした状態であるとする。これはエラーやミスの真なる原因と責任がどこに帰属するのかが慎重に判断され、賞罰の行使の基準もまた明確な状態である。これが報告する文化を促進するとし、Reason は航空業界における安全性向上の取り組みの一つであるニアミス情報を共有する活動を参考例としている。航空業界では、事故を未然に防ごうというプロアクティブな活動の一つとして、航空安全報告システムを整備し、効果を上げている。これは、事故につながりかねない小さなミスの情報を収集し共有することを目的としているが、実際の事故発生においても捜査や刑事罰によって真相究明の妨げとなることを排除するためという面もある（Reason, 1997, 邦訳書, pp.279-281）。Reason（1997）は、このシステムが成功した要素として①懲戒処分からの保護、②極秘性・匿名化、③報告の収集・分析者と懲戒権者の分離、④報告者の所属組織へのフィードバック、⑤報告の容易さ、の５つを挙げ、①から③までの要素についてを、自らのエラーを報告してもらうため報告システムに対する報告者の信頼感の醸成のためのものであると述べている（同上書, p.280）。

「柔軟な文化」とは、「変化する要求に効率的に対応できる文化」（同上書, p.303）として、複雑な技術システムを一定以下の事故率で運転し続ける組織である「高信頼性組織（HROs：High Reliability Organizations）」と呼ばれる組織群における研究を引き合いにしてこれを説明している。

高信頼性組織群は、繁忙時には階層的組織を緩め意思決定権限を積極的に現場レベルに移譲し、非常時においては専門知識を持つ者たちに委ねる。一方の上層部は組織を俯瞰することに徹し、最適な資源配分による支援を行う。これは、インシデントは起きうること、インシデントの原因は局所的ではないことを上層部が理解していることを前提として、素早いフィードバックを可能にする情報エスカレーションルール設定と意思決定権限の移譲であり、経営層と現場の相互の敬意に裏付けられるものである（Weick & Sutcliffe, 2001, 2007, 2015）。

「学習する文化」とは、これまでに述べた３つの文化によって駆動する「安全情報システムから正しい結論を導き出す意思と能力、そして大きな改革を実施する意志」（Reason, 1997, 邦訳書, p.278）をもつ状態である。適切な行動（準備し、実行し、テストすること）を導くために、観察すること（注意し、気を配り、心に留め、追跡すること）、考えること（分析し、解釈し、診断すること）、創造すること（想像し、設計し、計画すること）を求めている（Reason, 1997）。そして、経験から学ぶだけではなく、プロアクティブな態度により他者の経験からも教訓を引き出し、ベストプラクティスを組織内で共有しようとする積極的な状態を指す（Reason, 2008）。

情報共有の起点となる報告行動の促進という観点では、「(報告者にとって)役立つフィードバックが得られないと感じるほど、事象報告があがってこなくなる。」（Reason,1997,邦訳書 p.285）という航空業界における安全情報システムについての研究からの指摘もまた重要であろう。報告がどのように処理され、組織の役に立ったのかという情報によってもたらされる「自己効力感」によってさらなる貢献が組織にもたらされると期待できるからである。

5 高信頼性組織と 5 つの原則

柔軟な文化において、組織形態の柔軟さとして触れられていた「高信頼性組織」であるが、この高信頼性組織研究の代表例としては、1980 年代より、航空管制・送配電システム・原子力発電所・原子力空母・原子力潜水艦（La Port, 1988; La Port, 1996; La Port and Thomas, 1995; Bourrier, 1996; Rochlin et al., 1987; Bierly and Spender, 1995）などの巨大で複雑な技術システムを対象に、複雑な技術システムを運用しながらも重大事故の発生を一定の水準以下に抑えている組織として、長期にわたる参与観察を手段として行われたものが挙げられる。

日本に高信頼性組織の概念がもたらされるきっかけとなった Weick & Sutcliffe（2001）の研究では、組織文化を研究の柱の一つに据え、前節で確認した「安全文化」（Reason, 1997）を企業組織が持つべき文化のモデルの一つとして取り上げている。そして、高信頼性組織研究の知見から、組織の信頼性を高める、彼らの表現に倣って端的に表せば「不測の事態を未然に防ぐ」、「発生時には被害を最小限に食い止める」ための組織メンバーの振る舞いについて、次の 5 つの原則（Discipline）として帰納的に導出している。

①失敗にこだわる（Preoccupation with Failure）
②単純化に抵抗する（Reluctance to Simplify）
③オペレーションに鋭敏になる（Sensitivity to Operations）
④レジリエンスを重視する（Commitment to Resilience）
⑤専門知を重んじる（Deference to Expertise）

これらの原則について、以下のように説明できる（杉原・中西, 2014）。

最初の原則となる「①失敗にこだわる」は、自らの成功体験よりも失敗体験を重視することであり、中核的な趣旨は 2 つある。ひとつは「失敗は学習のチャンス」であると捉え、いかに教訓を引き出すかというものであり、自己の失敗事例だけでなく代理学習をいかに充実させるかというも

のである。ふたつ目は、トップレベルでは組織戦略の遂行において犯したくない間違いを明確化すること、現場レベルでは失敗やエラーから起こる計画からの逸脱が小さく可逆的なうちに発見できるように、僅かな差異に気を配ることである。ここで具体的に求められる振る舞いは、エラーを発見したら（過ちを犯したのが自分であっても）率直に報告することである。それは、失敗の影響が拡大する前の問題が御しやすいうちに対処するのが最少のコストで済むと組織メンバーが共通の認識を持っていることを前提としている。そしてこの原則を具現化するために組織は、報告する仕組みを実践に組み込むことが求められる。

続く「②単純化に抵抗する」とは、先の原則①のベースともいえるもので、小さな失敗を発見するためには僅かな差異に気づく必要があり、眼前に広がる状況に対する認識を大括りで単純なものにしてはいけないという戒めである。この原則は、状況の認識を豊かにするためにメンバーの相互作用を重視し、メンバー個々人に対しては、現状に対して常に疑いを持つこと、疑問を提起すること、常に対話を繰り返すことで疑問を解決していくことを振る舞いとして求めている。一方、組織に対しては、対話を通じたより適切な「センスメイキング（Sensemaking）」[58]をもたらすためにメンバーの多様性を確保し、教育・配置・再教育といった実践に組み込むことが求められる。

「③オペレーションに鋭敏になる」とは、「多くのシステムの内側に存在する、面倒な現実に敏感に反応すること」と Weick & Sutcliffe（2001）は表現している。この行動原則も中核的な趣旨は2つあり、組織活動の基礎となる現場の活動に重きを置き、注目を向け続けること、そしてその活動の実際が当初の意図やデザイン、計画などから逸脱した状態で惰性によって行われてはいないかをチェックすることである。端的には組織活動の継続性を確保するためのものであるが、組織には、現場から集まる多くの情報に基づいて組織活動の全体を俯瞰すること、また現場の活動の限界を見極め、適時の支援を怠らないことを求めている。そして個人レベルには、組織運営の全体像を正しく認識するために、現場から情報を組織の上方向に報告し共有するというだけでなく、現場レベルもまた経営者層の持つ認識や意図を積極的に収集し、理解することが求められている。

高信頼性組織は、組織の直面する状況について平常時・繁忙時・非常時という三つの局面に分けてそれぞれに備えるという特徴があるという（Rochlin et al., 1987）。これまでの3つの原則は、失敗を防ぐ／小さく留めるためのものであり、「平常時」そして「繁忙時」の活動におけるものであ

[58] Weick の代表的研究のひとつでもあり、意思決定（Decision Making）の前提となる、状況や環境に対する認識や理解を、組織メンバーの相互作用によって統一していくプロセスを意味する（Weick, 1995）。

った。これから確認する２つの規範は「非常時」のものであるが、非常時のための平時からの備えでもある。

「④レジリエンスを重視する」とは、組織の内憂外患に対する対抗力／復元力に注目することであり、これまでの原則と同様に組織活動の継続性を確保するためのものであるが、エラーは発生しうるという認識の下、その防止と同じように回復についても考えておくという思想である。

Weick＆Sutcliffe（2001; 2007; 2015）によれば、これらの規範が導出された高信頼性組織の特徴とは、失敗がないということではなく、失敗によって無能力な状態にはならないというものであり、オペレーションを縮退させることはあっても断絶させないことである。これについては、民間の営利組織でのコストの制約の問題から批判する向きもあったが[59]、彼らはコミュニケーションの冗長性としてこれを捉え、「概念的余剰（Conceptual Slack）」と呼ぶコミュニケーション経路の充実を表現している。

彼らは、危機的状況からのいち早い回復にはフィードバックの速さが肝要であるとし、複数の経路を使い、事態の進行についての情報をやりとりすることで、単に共有するというだけでなく状況認識の統一を図ることを振る舞いとして求めている。そのため、組織に対しては、出来事に対するメンバーの分析視点の多様性の維持を、個人に対しては多様な意見を相互作用により発展させるための、理解したフリではなく何が起きているのか質問する意欲、そして情報交換を豊かにし加速させるために相互に敬意を持つことを求めている。第１や第３の原則における報告の経路とも通ずるところであり、組織メンバーの相互作用を重視し、相互作用を通じて状況認識の精度を高めるという彼らの主張のポイントでもある。

「⑤専門知を重視する」原則は、専門知識の量と組織階層上の地位の高さは比例関係にあるという思い込みや誤解を戒めるものである。先に触れたように、平常時・ピーク時・非常時という組織内の状況に対する認識に基づいて、組織に対しては状況の変化に伴って行為および意思決定権を、その直面する問題について適切な知識を備える者に委譲するというように、階層型組織における指示命令／権限義務関係の硬直性を緩め、問題解決に対するリーダーシップの発露の柔軟性を求めている。これと同時に、問題解決に必要となる知識の源泉は、組織内に存在するタイムリーでアドホックな非公式ネットワークであり、これを尊重するという姿勢でもある。ここで注意すべきは、尊重するのは「専門知識」あり、特定の「専門家」ではない。したがって個人に対してはまた、例え

[59] 初期の研究では、組織的冗長性として表現され、バックアップ体制の充実として機能の２重化などを意味していた（Rochlin, 1988）。

専門家と称する人物の持つ知識であったとしても、専門家と呼ばれる人物とその者の持つ知識を切り分け、鵜呑みにすることなく相互作用を通じて目の前の局面におけるさらなる適応性を高めることを求めている。

そして、これらの振る舞いは、Weick＆Sutcliffe（2001; 2007）の表現によれば「マインドフルネス（Mindfulness）」と呼ぶ組織メンバーの注意深さによって裏付けられているという。彼らの定義では、「現状の予想に対する反復チェック、最新経験に基づく予想の絶え間ない精緻化と差異化、前例のない出来事を意味付けるような新たな予想を生み出す意思と能力、状況の示す意味合いとそれへの対処法に対する繊細な評価、洞察力や従来の機能の改善につながるような新たな意味合いの発見、といった要素が組み合わさったもの」（Weick & Sutcliffe, 2001,邦訳書, p.58）であり、悲劇的な不測の事態につながりかねない出来事を、できる限り小さな芽のうちに見つけ出し摘み取るために、5つの原則にあるプロセスを組織全体で継続することで、この注意深さが育まれるという。

したがって、高信頼性組織における注意深さとは、事故を起こさないこと、そして事故を起こさないということに付随して産まれてくる当該組織への信頼を維持しつづけるためにも、組織メンバーに備えることが求められるものである。事故を未然に防ぐ、被害を拡大させないことで組織的成果を維持し続けるという組織が標榜する価値は、注意深さとしてメンバーに内面化されているということになる。そして、5つの原則はその注意力が表出した具体的な例として理解することできる。

6 セキュリティ文化の再定義

OECD（2002）によるセキュリティ文化については、基礎的な概念が原則として提示されているのみであるため、ここまでの検討を踏まえ、企業組織におけるセキュリティ文化について具体的に再定義を試みたい。

（1） 標榜する価値についての検討

まず、OECD（2002）によるセキュリティ文化については、「情報システム及びネットワークを開発する際にセキュリティに注目し」という冒頭は、企業が情報システムを開発または導入する際の仕様の問題として捉えることができる。これについては、一義的には情報システム部門やセキュリティ専門部門が担う部分であり、インシデントのトレンドや技術についての最新の知見と情報に基づいて要求水準を決定することが求められている。二義的には自社が外部に提供する製品やサービスの開発においても情報セキュリティを意識し、開発プロセスの初期段階からこれを取り入れて

いくこと、いわゆる「セキュリティ・バイ・デザイン」と同じ志向性が、多種多様な企業活動に従事する多くのメンバーにも求められている。

しかし、どんなにシステムに注意を払いコストをかけても完璧なものはあり得えず、当然に限界がある。したがって、「情報システム及びネットワークを利用し、情報をやりとりするに当たり、新しい思考及び行動の様式を取り入れること」というように後半部分において、これらの機器やシステムを利用する人々がその限界を補完するという構造になっていると理解できる。

では、情報を中心とした現代的な企業活動に際して、堅牢性や安定性を志向した機器やソフトの導入といった、ハード的な対策を補完するため組織のメンバーに求められる新しい思考と新しい行動の様式とはどのようなものであろうか。前章で見てきたように、文化とは人間の活動そのものを規定するものとして定義されており、それは「信奉される価値観」を中心として、表層としての「人工物」と深層としての「基本的仮定のパターン」として組織に埋め込まれており、この共有された仮定によって特定の思考が導かれ、一定の振る舞いとして表出するとされる。したがって、まず中心となる価値について検討したい。

原子力安全文化との比較において検討したように、セキュリティ文化において組織が守るべき対象は、預かる個人情報や保有する機密情報といった情報とそれに含まれる価値であるが、目に見えにくいという特徴がある。それは、電子データとして保持されていることが多いからということと、情報が価値そのものであるからだ。情報の価値とは、営業秘密であればこれを保護することは企業の付加価値を守ることそのものであり、個人情報であればこれを保護することは基本的人権を擁護することそのものである。前者であればその組織のメンバーにとって、後者であればすべての人々にとって、究極的には個人の主観により価値の高低は生じないはずである。

したがって、セキュリティ文化とは、企業組織における付加価値と普遍的な基本的人権を護るという価値が共有された状態である。そして、セキュリティ文化を持つ組織とは、この2点について組織メンバーが価値を理解し共有することで、インシデント発生時だけでなく平時においても組織全体に求められるものとして「常に、情報資産を守ることにプライオリティを置き、情報資産の価値にふさわしい態度を持つ個人とその集合としての組織」となろう。より具体的には、「いかなる状況においても情報セキュリティにプライオリティを置くこと」が共有された暗黙の仮定として置かれ、それにより「情報システムによる対応の限界を認識し、最優先で情報漏洩のリスクを最小化する行動」が、技術者や開発者の立場にあれば「情報システムの稼働の安定を最大化する行動」

が、予想される振る舞いとして表出する状態、言うなれば「セキュリティ・ファースト」が定着した状態こそがセキュリティ文化が醸成された姿となる。

特に学術的定義では、情報セキュリティの文化を「サブカルチャー」や「第二の性質」というように、組織の中心的な文化としては捉えていないものがあった(Alhogail & Mirza, 2014; Mahfuth ら, 2017）。現実の企業組織では、組織の存続や発展を目指すにあたり日常の業務において情報をいかに活用するかの比重が大きくなっていることは既に述べてきたとおりであり、サブカルチャーとしてではなく組織の中心的な文化としてこれを醸成することが求められると考える。そして、現実の企業組織の内部では、多様な人間が多様なレベルにおいてそれぞれに多様なタスクを抱えており、多様な認識を持つ小集団を形成していることにも注意が必要である。マネジメント層には、文化のマネジメントの問題として、これらの多様な小集団間のコンフリクトにおいてもセキュリティ文化から逸脱した独自の下位文化の発達を許さず、あくまでもセキュリティ・ファーストを組織に共通した最上位の価値と位置づけ、これに則った振る舞いが表出するようリードすることが求められよう。

そのためにも組織メンバーの価値観の共有がなにより求められるが、それこそが標榜された価値としての「セキュリティ・ファースト」となる。「セキュリティ・ファースト」は、標榜された価値として名詞であるが、同時に、文化が表出した具体的な振る舞いを表わす動詞でもある。

（2） 下位文化への展開

このセキュリティ・ファーストが内面化され、振る舞いとして表出するために、組織はどのような文化となることが期待されるかについて、多くの企業組織の関心事となる組織的な事故を防ぐための文化として Reason（1997）によって提示された「安全文化」とその下位文化を下敷きに表現することを試みたい。具体的には次のような組織の状態となるであろう。

①報告する文化：組織のセキュリティは、組織のメンバー全員が、個々人で最適な判断ができるほどに十全な情報と知識を持っていることによってもたらされる。そのために、些細な兆候であってもそれを組織のメンバーで共有すべく報告することが推奨される。それは、組織の安全が脅かされることにつながるかもしれないという疑念を個人が持ったとき、躊躇なくそれを報告することを求めるが、それは「その内容が業務の中断をもたらすような情報であっても歓迎され、非難の対象にはならない」（Weick & Sutcliff, 2010, p.96）という職場環境であること、すなわち前章で確認した「心理的安全」（Schein, 1990;2001）がメンバー内に確保されている状態でもある。

そして実務的には、業務を妨げない報告の収集の体制が備わっており、さらに、組織の情報セキュリティの状況が改善していることについて実感できる状態である。この状態は、次に述べる公正な文化によって支持されていることが前提となる。

②公正な文化：「許容できる行動と許容できない行動の境界がどこにあるのか」（Reason, 1997, 邦訳書, p.278）をメンバーが明確に理解しコミットしている状況であるという。第Ⅰ章で確認したように、組織外部からの悪意と組織内部のメンバーのエラーが結び付いた情報漏洩のパターンとして標的型メール攻撃がある。標的型メール攻撃は、外部の悪意者が、情報システムに対してマルウェア等を侵入させる踏み台として、内部のメンバーのエラーを利用する。そのため、電子メールの受け手にとって開封が必要なメールであると誤認させ、添付ファイルの開封を促し本文中のリンク先へと誘導するために文面を工夫するというように、攻撃側が常に上手である。したがって、ここでの誤認、開封、クリックは人間のエラーではあるが、あくまで結果であり原因ではない。よってセキュリティポリシーに対して相当程度の懈怠であると認められるものを除いては免責を原則とすべきである。

組織行動においてメンバーが自らの過失を隠匿しようとするのは自然なことである。特に懲罰につながるとなればなおさらである。たとえば、繁忙感を抱えながら業務を行うなかで、日常的に利用している電子メールによる外部からの攻撃に対して回避行動がとれなかったことが懈怠とみなされ、強く叱責・指導を受けるようなことがあれば、それを隠そうとする行動が起きても何ら不思議ではない。結果として報告行動は委縮することとなり、組織のセキュリティ確保のために本質的に有用であるはずの情報収集の妨げとなってしまうのである。そして、情報システムを危険にさらすこととなり、最終的にはセキュリティ確保を担うセキュリティ担当部門への信頼構築の妨げにもつながると考える。さらには、エラーが発生しうる機会そのものに関わろうとしないという消極的な対象行動が導かれることも指摘されており（三沢ら, 2014）、エラーの発生を減少させようとする学習につながらないだけでなく通常の業務の滞りまでもが懸念される。

この公正な文化を醸成し、心理的安全の土壌を整備するためにも、実務的には経営者層や管理職層のヒューマンエラーに対する認識をまず改善する必要があると考える。そのため、訓練に先行する集合的な教育とは別建てで、文化的視点から組織的なセキュリティについて講習を行い、認識を共有することが求められよう。

③柔軟な文化：組織の内部／外部の状況に応じて、適切な組織形態を採ることができることを意味していた。特定の組織形態を意味しているわけではないが、官僚制をベースとした階層型組織と

権限移譲が行われたフラットな組織とを行き来できることを意味している。状況に応じた変化というだけでなく両の側面を同時に持つこととしても考えられ、さすればそれは、経営者層から組織のセキュリティを担う専門家たちへのエンパワーメントと規律の両立として理解することができる。この実現のためには、上層部は専門家たちが必要とするものを、専門家たちもまた上層部が必要とするものを、経営者層向け研修等を実施する中で相互に理解する必要がある。

④学習する文化：適切な行動のために、観察し、考え、創造することを大事にすることであり、公正な文化に支えられた報告する文化によって収集された観察の結果を分析し、蓄積し、共有し、活かしていくことで、より良い組織を常に目指す姿勢を組織のメンバーが保持する状態である。そしてそれだけではない、情報と情報ネットワークを利用する自己も、そのネットワークの一部であり、自己の行為が及ぼし得る影響は個人の想像をはるかに超えること、そしてその影響は自分自身に還ってくるということを理解し、組織のメンバーが「当事者」としてこれに積極的にかかわろうとする姿勢を持つ状態である。

これらの下位文化が醸成されることで、最終的な文化の状態として、組織のあらゆる場面、種々の行為の場においても、情報セキュリティの面で最適な意思決定をおこない、それを実践していくことで組織の情報セキュリティに貢献し、組織の発展につなげようとする振る舞いにあふれた組織となっていることが期待される。

7 小括

本章では、保有する情報資産の価値の高まりとともにその保護が重要となる環境下において、情報システムを通して情報資産を活用する企業組織に求められる文化とはどのようなものであるかについて、検討してきた。まず、本研究の関心の中央にある「セキュリティ」を冠して OECD によって提示された「セキュリティ文化」とは、情報端末と情報ネットワークの利用者を「参加者」と呼び、参加者自らも文化の一部、すなわち文化の「当事者」という認識を持ちセキュリティへ応分の貢献を求めていた。しかし、このセキュリティ文化の類例となる原子力安全文化との比較においては、何を目的としてどんな文化が求められるのかという点で明確さに欠けるものであった。具体的には、これに関与する者においては一定以上の知識を持っていることが期待でき、安全を確保することがベネフィットの源泉そのものである原子力安全文化に比べて、両者の知識レベルにバラツキが大きく、利用の程度とその利用から得られるベネフィットも様々である参加者に「プロ意識」を求めることは難しく過剰であるといえる。それゆえ何を守るべきなのか、そして、それにより何

がもたらされるのかという点で抽象度が高いといえる。それは、情報システムは組織または個人の目的達成のための道具の一部であり、利用する情報端末が接続するネットワーク全体への影響を想像しにくい、すなわちセキュリティを意識しない利用法によって引き起こされる可能性がある他者への影響を想像しにくいからである。これと同時に、安全な利用が侵されることによる直接の被害が想定しにくいという２つの点で情報セキュリティの問題を自分事にしにくい、すなわち参加者という当事者の意識が持ちにくいということが課題として整理できた。

次に、多くの企業組織にとって関心事として順位が高いと考えられる、組織的な事故を防ぐために組織が醸成すべき文化として挙げられる「安全文化」（Reason, 1997）について確認した。この安全文化とは、組織的な事故を起こさないために、組織のメンバーそれぞれが組織にとってより良い行動が選択できるよう、等しく十分な情報を持っている状態としての「情報に立脚した文化」を意味していた。そしてこの文化となるためには、その下位文化として、報告する文化、公正な文化、柔軟な文化が求められるが、さらには、これらの下位文化が備わることによって生まれる学習する文化を通じて醸成されていく文化であった。これらの下位文化はいずれも組織内の情報流通を促進するための文化であり、その起点としてなによりもまず組織メンバーの「報告」を重視し、報告しやすい仕組みや心理状態を育てる土壌となり、報告という振る舞いを引き出すためのものであった。

安全文化は、組織的な成果の持続に重きを置き、組織的な事故を起こさない組織として研究された「高信頼性組織」研究のなかでも、そういった組織が持つ文化の一例として取り上げられるものであった。そしてこの高信頼性組織では、組織的な成果を持続させるため、事故を起こさない（被害を最小限にとどめる）ための組織メンバーの「振る舞い」について５つの原則として議論されていた。これは、組織的な成果を持続させること、事故を起こさないことの結果として生まれてくる信頼を維持することに価値を置き、そのために組織のメンバーが持つべき注意深さとして内面化され、振る舞いとして表出したものであると考えられた。このメンバーの振る舞いと企業文化については、組織メンバーの振る舞いを強く規定する「強い文化」のメリットは、①文化と戦略のフィット、②被雇用者の企業へのコミットメントの向上という２点において価値があるとされる（O'Reilly,1989）。しかしこれは、競争環境下における他社との競争優位性として論じられていた。セキュリティ文化の追求は、情報漏洩などによってレピュテーションを含めた広義の意味での損失を防ぐという点ではこれにマッチするが、競争に打ち勝つことを直接の目的とはしていない。原子力産業分野における例も、原子力の安全な利用が関与者たちのベネフィットに直接結びつくという点で、これを推進するインセンティブは高いといえ、情報セキュリティとは異なる。この点で、セ

キュリティ文化の醸成は、経営者層にとってはコストの認識が強くなり、優先順位が高くならないことは理解に難くない。しかし、競争戦略をトップマネジメント層が構築する際、それを現場層が実行する際、当然の前提としてセキュリティ・ファーストで実践されるという点で、文化と戦略のフィットと被雇用者の企業コミットメントの向上は重要であると考える。

最後に、ここまでの議論を踏まえ、情報システムを通じた情報資産の活用によって活動する現代の企業組織に求められるセキュリティ文化とはどのようなものであるべきかについて再定義を試みた。本研究におけるセキュリティ文化を持つ組織とは、営業秘密であれば企業の付加価値そのもの、個人情報であれば基本的人権を守り擁護することそのもの、という保有する情報資産の価値を組織メンバーが理解・共有し、「常に、情報資産を守ることにプライオリティを置き、情報資産の価値にふさわしい態度を持つ個人とその集合としての組織」となる。Schein による文化の 3 層になぞらえれば、「いかなる状況においても情報セキュリティにプライオリティを置くこと」が共有された暗黙の仮定として置かれ、それにより「情報システムによる対応の限界を認識し、最優先で情報漏洩のリスクを最小化する行動」が予想される振る舞いとして表出する状態、言うなれば「セキュリティ・ファースト」が定着した文化である。

次章では、このセキュリティ文化を醸成するために、実務的なマネジメントと文化の関係について検討していく。

Ⅳ 現代的マネジメントと文化

本章では、前章において導き出した、現代の企業組織に求められるセキュリティ文化を醸成するための具体的な手段について検討したい。

第Ⅱ章においては、企業組織の文化の醸成や変革のプロセスに求められる要件や要素を確認する中で、組織メンバーに対して新たな文化の必要性を認識させ、そして旧来からのビジネスプロセスを新たなものへと転換していくための取り組みとして「教育」と「訓練」を中心に検討することが求められると確認した。しかし一方で、それらを行った成果が、本質的に文化と呼べるものなのか、特に解釈主義的な見方からは、文化とはメンバーの内心の問題であることからも、内心の変化が留意点として残ることを述べた。

そこで、「教育」と「訓練」を中心とすることの妥当性についてを、実務的なマネジメントの議論から再度確認し、これらの取り組みとその成果の測定に着目しながらどのように実践すべきかを検討していく。最後に、企業組織においてそれら充足するためには何が求められているのかについて、より実践的な側面の課題について確認する。

1 文化の醸成と測定

(1) 手段としての訓練

今日において企業組織が何らかの取り組みを進める際に、PDCA サイクルを踏まえた各種のマネジメントシステムを無視することは難しいであろう。この現代的なマネジメントのツールとして普及している ISO マネジメントシステムなどでもたびたび「文化」に言及するが、そもそも文化は何らかのマネジメント対象となるのか、そしてマネジメントの成果として測定できるのであろうかという根本的な疑問につながる[60]。Deal & Kennedy（1982）は、文化とは理念・神話・英雄・象徴の組み合わさった精神的なものの総体であり、メンバーにとって重要な意味を持つ、広く浸透した哲学であることから、企業文化を数字で測定することはできないと指摘している。同様の指摘として、Schein（1985）は組織文化を、目に見える表層としての人工物、標榜される価値、深層としての共有された仮定の 3 層で表し、文化の本質はメンバーに共有された仮定であり、目に見えず、それゆえ測定することは困難であると述べている。さらに、測定が可能なものとしてコントロール

[60] マネジメントシステムによる文化への言及については、補論 1 を参照されたい。

しようとする組織変革の議論については「文化の表面的事象と底流にある類型、あるいは、文化の本質なり、核と考えられるものの混同」（Schein,1985, 邦訳書, p.58）であるといい、それらが提示する組織変革のプログラムは、測定方法についてのコンセンサス、すなわち測定方法の新たな視点についての議論でしかないと批判している（同上書, p.80）。

この測定方法についてのコンセンサスとは、Schein が組織文化の外的環境への適応サイクルとして整理した 5 つのステップのうちの一つである。これは、文化とは、外部環境からもたらされる制約と内部の問題解決の束として結果として出来上がったものであると同時に、外部環境への適合とそのための内部プロセスの統合の「機能そのもの」であるという考え方による。この適応サイクルは、①使命と戦略、②目的、③手段、④測定、⑤修正であり、それぞれについては、下表のようなものである(表 9)。

表 9：Schein が示す外部環境への適応サイクル

①	使命と戦略	中核をなす使命、第一義的責務、顕在および潜在している機能の共有された理解を得ること
②	目的	中核をなす使命から導き出される目標についてのコンセンサスの構築
③	手段	組織構造、作業の分担、褒賞制度、権限の仕組みなどの、目標を達成するために使われる手段についてのコンセンサスの構築
④	測定	情報や管理システムのような、グループがどのくらいその目標を達成しているかを測定するために使われる基準についてのコンセンサスの構築
⑤	修正	目標が達成されないとき、戦略の適切な補正あるいは修復についてのコンセンサスの構築

出典：Schein（1985）邦訳書 p.69 より筆者作成

これら 5 つのステップについては必ずしも順を追うものではなく「存続企業となれば、多分同時にほとんどのステップとかかわることになる」（邦訳書, p.68）というように全体を同時に進めていく必要があるという。

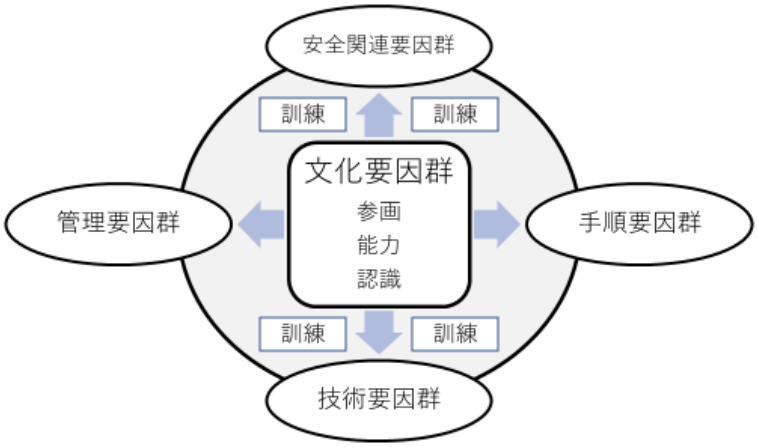
先の批判を鑑み、セキュリティ文化の醸成をマネジメントの対象と位置づけ、成果として正しく捉えるためにも、本稿の目的としているセキュリティ文化の醸成をこれらのサイクルにあてはめて考えてみたい。

「①使命と戦略」は、「究極の生存の問題についての共有の概念を構築」（Schein, 1985, 邦訳書 p.68）することとされるが、企業組織の情報セキュリティの向上は社会的要請でありこれに応える必要があること、さらには情報セキュリティに重きを置かなければ事業の存続も脅かされることを共通の理解とすること。これを受けて「②目的」は、「セキュリティ・ファースト」が共有された

価値として内面化され、これが当然の仮定となることである。ではその「③手段」についてはいかにすべきだろうか。

これについては、文化とマネジメントを繋ぐ媒介が「訓練」であると Reason（1997）が主張していることに着目する。彼は、組織全体の安全に関して「組織全体にあまねく存在する」（邦訳書,p.172）ものとして、組織の中核的な文化を囲むように①安全関連要因群、②管理要因群、③技術要因群、④手順要因群、⑤訓練、という文化の周辺的要素によって構成されるサブシステム群を示している（図 4）。

図 4：組織安全の背景となる重要なプロセスにおけるサブシステム群



出典：Reason（1997）邦訳書 p.173 を基に筆者作成

「①安全関連要因群」については、事故報告・安全施策・緊急時資源と手順書・業務外の安全性を、「②管理要因群」については、変更管理・指導力と運営・コミュニケーション・雇用と配置・購買管理・生産と防護の不均衡を、「③技術要因群」は、保守管理・自動化レベル・ヒューマンインタフェース・工学的制御装置・設計・ハードウェアを、「④手順要因群」として、標準・規則・監理・運営手順といったものを例示する。これらの要因群は、前章で確認した Schein が「文化的要素」と呼んだものであると理解できる。そして、これらの周辺的な文化的要素と中心となる文化を繋ぐものが「⑤訓練」であるとして、正式／非公式の訓練法・訓練部門の存在・技能と業務遂行能力を例示する（邦訳書, p.172）。彼は、この図における訓練ついて、「関連事項を局所的に個々に取りまとめたものではなく、訓練が全般に通じる共通的なものとして表現」として図説する。

この図を情報セキュリティの実務に置き換えれば、組織によって定められたセキュリティポリシーや、情報システムを支える IT、ポリシーに沿って作成される手順やルールが諸要素であり、そ

れら文化に繋ぐものが組織内で実施される「訓練」であると捉えることができる。Schein（1985; 1990; 2010）は、組織の文化を変えるためにはこういった「文化的要素」を変えることの必要性を示していたが、これを踏まえれば、Reason の示す「訓練」も文化的要素の一つでしかないが、周辺的な複数の「文化的要素」と組織メンバーの認識や能力といった本質としての「文化」を繋ぐ重要な要素であり、新たな「②目標」の達成の手段としてこの「訓練」を選択し、訓練をどのように行っていくか、変えていくか、が重要なものとなると考える。

これについては、Reason（1997）は「平時において正しいデータを集めることが、知的で望ましい警戒状態を継続していく一番良い方法であり、おそらく唯一の方法であろう」（邦訳書, p.277）と述べている。すなわち、こういった手順やルールの遵守の様態といった、情報セキュリティに関する組織の状態を把握する手段としても、平時における訓練とその効果測定こそが最適解であると考える。

訓練が手段として選択されるのならば、次に検討の対象となるのが「④測定」である。特に、企業組織がなんらかの目的に対する投資として訓練を行うのであれば、時間と予算が必要となる。現実的には、それらを確保するためにはコストと効果としてこれを認識し、組織的な目的の達成に貢献するものであるということを示す必要があろう。実務の面では訓練の効果測定の指標の設定とその測定が表立ってくるが、訓練の成果を組織文化そのものに置くと、効果の測定という点では、文化を測定することは本質的に不可能であり、測定しようとしてもそれは測定指標に関する表面的な議論だという批判（Deal & Kennedy, 1982；Schein,1985）に再度立ち戻ることになる。Schein（1985）に従えば、組織文化とは標榜する価値を内面化したメンバーによる当然の仮定を共有した状態である。であれば訓練の成果は、組織が新たに標榜する価値の内面化の程度、そして内面化から生まれる当然の仮定が共有されている程度が測定の対象となるが、この可能性について次節で検討する。

（2） KPI の設定

先の Schein による文化の変革における目標設定についての批判は、組織文化の変革においては、目標設定で議論がとまってしまいがちであり、それでは単なる文化の 1 要素の変更でしかないというものである。そしてそれは、現実的な問題として、目標の達成度合いとしての外部環境への適合度合いを測定するにあたり、内部統合との兼ね合いの問題として複雑に分化した機能単位ごとの重要な指標、いわゆる KPI（Key Performance Indicator）との整合性やコンフリクトの懸念といった、統一的な指標を用いることの難しさに由来することを指摘するものである。しかし同時に、文化の

変革の入り口では、やはり目標設定とその達成度の測定の指標、すなわち KPI の設定が重要であることを示唆していると理解できる。

であるならば実務では、文化変革の必要性を新たな KPI の設定を通じて「使命」として伝え、「目的」を説明し、「手段」を整え、実行していく方が自然であり重要なのではないだろうか。本研究は、企業の文化としてセキュリティ文化を醸成していく、もしくは従来からの企業の文化をセキュリティ文化へと変化させることを目的としている。そして、手段として「教育」と「訓練」が最適解であるとした。このため、サイクルの次段階である「④測定」については、文化の醸成や変化の度合いを教育や訓練の成果として置き換え示す必要がある。それゆえ、訓練の KPI を変化させ、KPI に対する仮定を変化させるためにそれに即した訓練を設定し、訓練の実践を通して使命と伝え目的を説明していくことの方が自然であると考える。すなわち新たな KPI の設定こそが文化変革に求められるシンボルの掲示であり、場合によっては設定の行為そのものがシンボリックな行為となりうる。そして、このシンボルに対して一貫性のあるものとして、Schein（1985）の言う組織文化の外的環境への適応の 5 つのステップを構築することが、まさに彼の言う 5 つのステップ全体を同時に進めていく正しい方策となる考える。

手段として選択した教育や訓練などの効果の測定については、古くから Kirkpatrick(1959; 2005)[61] による 4 段階の評価モデルが知られている[62]。このなかで 3 段階目として示されるのが「振る舞い（Behavior）」である。これは受講者に対するインタビューや他者による多面的評価による測定であり、教育を受けた結果としての受講者の行動の変化の程度が尺度となり、振る舞いや姿勢がその対象となる。この組織メンバーの「振る舞い」に着目し、評価の対象として用いている組織文化の醸成活動の事例として、原子力の分野において実践されている例がある。

2011 年 3 月に発生した東京電力福島第一原子力発電所での過酷事故を受けて、東京電力が取り組む「原子力安全改革[63]」の一環として、「10 traits」に基づく自己評価が取り入れられている[64]。

---

[61] Kirkpatrick (2005)については、初版からの修正や e-Learning の普及などを反映した第 3 版となる。

[62] 現代的視点として、この 4 段階モデルを踏まえ、教育や訓練の成果を投資による収益として認識し、ROI（Return on Investment）のような指標から評価を行うことを 5 段階目に加えたモデルも Phillips, J. J.（1996）によって提示されている。ビジネスの発想として欠くことはできないが、この考え方は 1980 年代のアメリカ企業の低迷期におけるコストカットの流れを受けたものであることも念頭に置くことの必要性も指摘されている（例えば檜垣（2006）など）。

[63] 正確には「福島原子力事故の総括及び原子力安全改革プラン」2013 年 3 月に東京電力が公表

[64] 仔細については、補論 2 を参照のこと

10 traits とは、WANO[65]が、「健全な原子力に係る安全文化の特性」（WANO, 2013, p.9）として、すなわち原子力安全文化の表出として、原子力関連組織のメンバーの望ましい振る舞いを 10 の要素として整理・提示したものである[66]。これは、①組織のメンバー全員に求められるもの、②経営者層に特に求められるもの、③具備すべき要件として組織そのものに求められるもの、という 3 重の構造になっている。「①組織のメンバー全員に求められるもの」として「安全への個人の決意」が挙げられ、3 つの要素で説明されている。「②経営者層に求められるもの」では、「安全へのマネジメント層の決意」が挙げられており、いずれもリーダーシップ発揮の方向性について示すもので 3 つの要素で説明されている。「③具備すべき要件として組織そのものに求められるもの」では、マネジメントシステムの運用について、すなわち PDCA サイクルによって業務を推進する際の要件を書き出し、4 つの要素として説明される。そしてこれらが、原子力発電所で働く職員の安全優先の意識醸成のベースとなるよう、要素ごとに対して 3 つ程度を標準として最多では 8 つの具体的な振る舞いとして定義されている（WANO, 2013, pp.9-30）[67]。

実践の観点では、個人レベルで 1 日の「行動の振り返り」のための参照点として用いられており、具体的には、これを基準として自己の 1 日の振る舞いを自己評価したものを蓄積し、さらにより深い内省につなげることを意図してグループ内でその結果について話し合うという取り組みを実施している。KPI の観点では、表 10 のように用いられている。

表 10：東京電力の原子力安全改革における振る舞いに関連した PI と目標値

PI（Performance Indicator）	Target
Traits を活用した振り返り活動の実施率	100%
振り返り活動において「わからない」と回答した率	10%以下
各指標の移動平均	増加傾向
振り返り結果を討議するグループ・部内会議の実施数	月あたり 2 回以上
振り返り結果に関する経営者層によるレビュー回数	四半期あたり 1 回以上

東京電力（2015）p.53 より安全意識に関する部分を抜粋し加筆　筆者作成

[65] World Association of Nuclear Operators：世界原子力発電事業者協会。1989 年に創立された原子力発電に関連する民間事業者の団体

[66] 10 Traits の発祥は、INPO：Institute of Nuclear Power Operations：原子力発電運転協会（米国内の原子力事業者による自主規制団体）にある。これを世界標準として WANO が採用した。

[67] それぞれの要素については補論 2 を、個別の項目ごとの振る舞いの仔細については付録を参照されたい。

そして、このグループ単位での振り返りの実施率などは組織の内外に公表されている[68]。ベースとなる振り返り活動そのものは、あくまで本人の主観による評価ではあるが、対外的にもこれを公表することで結果について内部のみならず外部からの注目があることを意識することができ、その意味付けをより大きくすることができるのであろう。この取り組みは、2014 年から実施されており、継続・繰り返しもまた重要だということがわかる。

以上のように、企業組織での取り組みはその成果の把握として「測定」が求められ、KPI の設定は重要であることは先に述べたが、そのためにも測定可能なものとすること、可視化が必要である。その対象が文化である場合には、KPI の変更によって起きる表面的事象と、測定された結果に対して用意される評価報酬とに一貫性を持たせるべき事象を正しく峻別し、内部統合の問題としての価値観の内面化、すなわち共有された仮定が表出したと考えられる「振る舞い」を測定することが合理的かつ限界であり、現実的な解となろう。であるならば、「文化の表面的事象と底流にある類型、あるいは、文化の本質なり、核と考えられるものの混同」（Schein, 2001, 邦訳書, p.58）という批判は、外部環境への適合の程度を測定する KPI と内部統合の程度を測定する KPI の混同をしてはならないという戒めであり、測定する KPI の選定が重要であるという指摘にほかならず、文化の表現としての人工物がいかに機能しているのか、測定されている振る舞いはいかなるものなのかを見極めることを求めていると理解したうえで、「振る舞い」を文化の醸成や変革の測定の代理的な指標として選択することは妥当であると考える。

そして、現場における活動だけではなく、こういった活動の結果に対するフィードバックもまたマネジメントにおいて重要であった。それは、「どんなに注意深くデザインされていようとも、統制としてのシステムが機能するのは、結果に気を配り、細心の注意を払っている人が居ると、モニタリングされている人たちが信じることができるときだけ」(O'Rilly,1989, p.11)と指摘されるように、何らかの目標に向けたマネジメントの一部として教育や訓練を実施するのであれば、これらを主管する部門だけがその結果を把握するのではなく、経営者層もこれを認知し、また教育や訓練に参加するすべてのメンバーが経営者層の反応を参照できるようにする必要がある。参加する組織メンバーが結果に対して興味を持たなければ演習の目的を果たすことはできないのは当然だが、メンバーが自らの振る舞いを内省的に認識するだけでなく、それについて他者が関心を持っていることがわかる仕組みを備えることもまたマネジメントにおいて重要であると考える。

---

[68] たとえば、原子力安全改革プラン 2018 年度第 3 四半期進捗報告など
http://www.tepco.co.jp/press/release/2019/pdf1/190220j0102.pdf

2 「振る舞い」とマネジメント

(1) 中西（2007）によるマネジメントのモデル

前項では原子力産業での事例を確認したが、こういった原子力産業も研究の対象の一つである高信頼性組織研究では、組織の標榜する価値をメンバーが内面化した結果と考えられる、外部から観察可能な「振る舞い」が5つの原則としてまとめられていた（Weick & Sutcliffe, 2001; 2007; 2015）。

そういった振る舞いにあふれる組織のマネジメントについて、その要件を確認したい。高信頼性組織に求められる要件について整理した中西（2007）は、「第 1 層：組織プロセス（組織行動）」「第2層：組織マネジメント」「第3層：組織文化」の3層構造のモデルとして整理している。

表11：高信頼性組織の三層構造

組織プロセス	正直さ／慎重さ／鋭敏さ／機敏さ／柔軟さ
組織マネジメント	評価報酬／情報共有／内部統制／教育訓練／意思決定
組織文化	信頼の文化／正義の文化／学習の文化／勇気の文化

出典：中西（2007）p.47 より筆者作成

第1層では、5つの組織プロセス[69]を個人と個人の集合体である組織全体に求められる特徴としてまとめている。5つの原則について第Ⅱ章で確認したとおりであるが、それぞれを端的に表現したものであり「鋭敏さ」「正直さ」「慎重さ」「機敏さ」「柔軟さ」としている。「鋭敏さ」とはオペレーションにおける小さな異変に対する自律的な姿勢、「正直さ」とは自らの失敗であっても進んで報告する姿勢、「慎重さ」とは状況判断における単純な解釈を戒め、相互作用による認知の精緻化を求める姿勢である。そして「機敏さ」とは状況の変化に対する即応であり、最悪の想定を踏まえそれに準備する姿勢である。「柔軟さ」とは問題発生における解決への知識の在りどころへ組織的な権限移譲であり、同時に自らも専門性をもってそれに参加し貢献するという姿勢である。

第 2 層は、これらの姿勢を引き出すための組織マネジメントの要件について整理し「評価報酬」「情報共有」「教育訓練」「内部統制」「意思決定」の5つを提示している。

「評価報酬」は、「鋭敏さ」と「正直さ」を引き出す源泉となる。高信頼性組織では失敗の「報告」を評価し、称賛をもってこれに応える。組織内で求められるものが賞罰の線引きによって理解

[69] Weick & Sutcliffe（2001）では、5つの原則（Discipline）には ”process “ の語があてられており、中西（2007）もこれに準じて「プロセス」として表記している

される。「慎重さ」を活かした状況判断には「情報共有」が求められる。組織メンバーの現状認識をアップデートしていくためにはメンバー間の相互作用が必要であり、そのためにはコミュニケーションチャネルの在り方が重要である。またチャネルの整備だけでなく情報交換の際の権威勾配を適切なものにする必要がある。

「教育訓練」は、適切なオペレーションの実践の前提となる必要なスキルと知識を獲得し、さらに高信頼性組織の文脈においてはマインドの深耕にも必須の要件である。特に、問題発見型の教育に重きを置くこと、教育内容と平時のマネジメントの一貫性を維持することが重要となる。この一貫性こそが組織の価値観を学習するために必要なものであり、一貫性の欠如は「隠れたカリキュラム」として機能し、標榜する価値とは別のものを学習することにつながるという。

「内部統制」とは、現代的な経営のガバナンス一般に通ずるが、5 つの特徴を引き出すための諸制度が、適切に運用されているか常に確認することである。信頼性の棄損につながりかねない芽を管理者層が、時には経営者層も自ら率先して探し、制度の健全性を担保する必要がある。

「意思決定」とは、「機敏さ」と「柔軟さ」を発露するために組織的な意思決定をどのように行うかであり、問題により近いレベルへの意思決定権限の移譲が中心的な概念であるが、それは、組織の下位方向というだけではなく組織上方へのエスカレーションもこれに含まれる。問題解決に当たるメンバーへの支援として、意思決定の責任の明確化を図るとともに情報やリソースの配分をコントロールすることも伴う。

これらのマネジメントが実践されることによって、「鋭敏さ」「正直さ」「慎重さ」「機敏さ」「柔軟さ」を備えたメンバーの振る舞いが誘導される。しかし、これらのマネジメントを裏打ちするものこそが文化であり、特に組織としての信頼性の確保には「組織メンバーどうしの相互の信頼はもちろん、社会との信頼関係を重視する文化」（中西, 2007, p. 127）が必要であるといい、深層である第 3 層として「信頼」「正義」「学習」「勇気」がメンバーの内心、すなわち基本的な仮定となっているという。

まず「信頼」については、「信頼性」とは他者からの信託を受ける側の特性であり、依頼者から見て信頼性の高い主体であろうという志向性を持つことと説明する。続く「正義」については、Reason（1997）の「安全文化」を引き合いに公正さ、正義の重要性を指摘する[70]。特に、パブリックセクターを主な研究対象として見出された高信頼性組織の概念がプライベートセクターへと広ま

[70] Reason は”Just”の語を用いており、中西は「正義」をあてている。筆者は第Ⅲ章 4 項で「公正」を当てている（脚注 55 を参照）。

る中で、企業経営におけるコンプライアンスや倫理の実装は必須であり、これこそが相互の信頼の源泉であり、先の「信頼の文化」の土台であるという。３つめの「勇気」については、振る舞いの「正直さ」の背景として、自分の犯したミスを正直に申告する勇気、些細な事象を報告する勇気がまず必要となる。これに加えて、想定外への対応として常識外の行動をあえて行う勇気を持つことである。最後の「学習」は、これまでの３つの文化が揃った状態で機能するものであり、それには「単に現場の改善活動や失敗からの学習というよりもより広い視点から検討」（中西, 2007, p.131）が必要であると述べる。目指すべき方向性として Senge（1990）による「学習する組織」の５要件を挙げ、なかでも組織メンバーがシステム思考を基に大局観を描くことができる文化だという。

マネジメントの部分に着目すれば、中西（2007）のモデルもこれまでの論者と同様に、「教育訓練」において期待される行動を示し、「評価報酬」を通じて期待される行動を統制する。そして、「内部統制」を通じて全体の一貫性の確保を図るというモデルとなる。そしてこの「内部統制」を担うマネジメント層の振る舞いや、「情報共有」と「意思決定」の実践もまた組織の標榜する「注意深さ」の深耕を表すシンボルとして機能し、個人における内面化を促進すると理解できる。

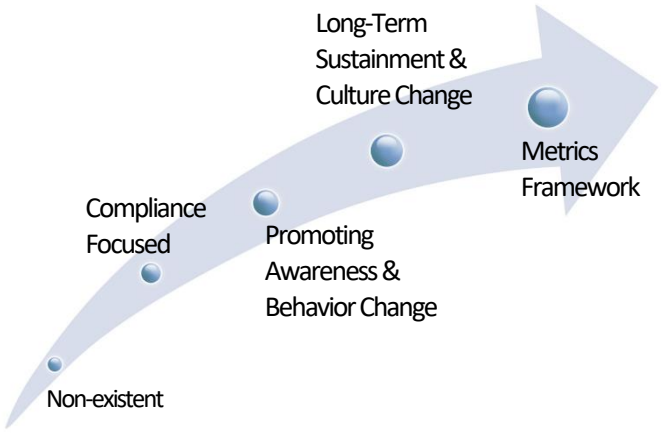
これらを通じ、ヒューマンエラーを前提として織り込んだ文化を醸成すること。それは、問題の早期解決につながる申告を引き出すために、心理的安全が確保された報告する文化と公正な文化を醸成することに加え、ベストプラクティスを積極的に取り込むというだけではなく、システム思考の獲得を視野に入れた学習する文化を醸成することは、情報セキュリティへの備えとしてのセキュリティ文化にまさに求められるものだと言えよう。

(2)　情報セキュリティの成熟モデル

企業組織におけるセキュリティ文化の醸成について、組織メンバーの情報セキュリティに対する認識の発達の程度としてこれを捉え、発達のステージモデルと実務的な視点からのマネジメントについて Spitzner(2014)が提示している（図５）。これは、情報セキュリティに対する認識を専門家のそれと同一の高さまで引き上げ、組織内でどう統一するかについてのプロセスモデルである。

情報セキュリティに関するポリシーを策定、啓発し、情報セキュリティに対する組織メンバーの認識を向上させ、振る舞いの変化を起こし、これを長期間持続させることで文化として醸成する。そして最終的に、測定により管理するというステージが最終的な到達点となる。それゆえ、測定指標の設定は重要なことになる。

図5：セキュリティ認識の成熟モデル



4 測定フレームワークでの管理

3 認識の長期的な維持と文化の変革

2 認知と行動変容を促進

1 コンプライアンスを注視

0 存在しない

出典：Spitzner (2014)

Making Awareness Stick, p.3 より筆者作成

ここでは、最終段階に至るまでの段階である、認識を向上させ、振る舞いに変化を起こす段階でのマネジメントに着目して、これを確認したい。このプロセスにおいて彼はコミュニケーションの重要性を強調しており、コミュニケーションをつかさどる役員の設置までも主張している。そして、e-Learning・社内報・情報ポータルといった組織内の様々な技術とチャネルの活用法について例示しながら、セキュリティが高まることによって組織と個人がメリットを感じるという「感情のレベル」でのコミュニケーションから始めることで、セキュリティリテラシーを向上し、情報セキュリティに対する認識を高いレベルで共有することを狙いとしている。

このなかで特徴的な点は、アンバサダー制度と彼が呼ぶ仕組みである。これは社内に実装されているセキュリティチームの補助者となる者をボランティアとして組織内の各所に配置し、この補助者を支援し集中的にレベルアップさせることで、セキュリティのネットワークハブとすることを企図している。彼はこのアンバサダーをコミュニケーションチャネルの、特に教育ツールの 1 つとしても位置づけており、トップダウン式（一方向）の教育から「同僚による教育」（Spitzner, 2014, p.21）への転換であるとしている。

これと同時に彼は、リーダーシップにも注目する。特に、セキュリティ認識を組織に浸透させるためには、セキュリティ業務に対するコミットメントが必要であり、このコミットメントをどのように表現させるかについてトップを教育すべきだと主張する。そのために、セキュリティチームからトップへの働きかけと、そのための直接のコミュニケーションチャネルを開発すべきであると述べている。彼の主張のポイントは、①多チャネルを活用したコミュニケーションを通じて、情報セキュリティの向上による個人レベルのメリットを認識してもらう必要がある。②その中心となるの

が教育であり、その教育の手段として従来的なトップダウン式の縦方向の教育だけではなく、同僚からもたらされる情報による横方向からの教育が必要である。③そしてセキュリティの専門チームの補助者となる者を育成し、これに充てる。④セキュリティの向上活動に対して経営者層にコミットメントを表現させることでセキュリティに対する組織メンバーの認識を方向付ける、ということである。端的には、①認識を持たせる、②教育訓練による認識の維持と向上、③組織作り、④一貫性の維持、となる。これらのプロセスは、リーダーによる危機の発見から、教育による周知によって組織全体で危機感を共有し、訓練を通して危機への対処としての新たな目標を提示し、褒賞を通じて支持するという、第II章において文化の醸成や文化の変革論として確認したプロセスに、教育のための体制づくりが強調されるものとなっている。そしてこの体制は情報セキュリティの重要さを周知し、認識を向上させるのためのコミュニケーションを充実させるものとしても位置付けられる。

「①認識を持たせる」は、情報セキュリティは自分事にしにくいという課題についての指摘であり、個人のメリットと結びつけることでセキュリティに興味をまず持たせ、その重要性を認識させるために多くのチャネルを通して訴え続けることが必要であるということである。

そして、その中心となるのが「②教育」である。まず従来的なトップダウン式の縦方向の教育や訓練であるが、それらはどのように実施すべきだろうか。恐怖心の喚起、すなわち Schein（1999）のいう「生き残りへの不安」として組織文化を変革する必要性を組織メンバーに認識させるには教育が最たる手段であると Schein（1985）は指摘していた。そして、横方向からの教育という点については、O'Reilly（1988）が「他者からの情報」すなわち、振る舞いの参照点となるものが常に身近に存在していることを文化醸成の要件に挙げていた。

さらに、「③組織作り」によってセキュリティ教育を相互に補完するような縦と横の構造、企業組織内部であれば従来的な縦の教育の基盤となる体系的なネットワーク構造を構築することである。これと同時に、振る舞いの参照点となる「同僚」をこのネットワーク構造に埋め込んでいくことが一案となろう。これがセキュリティ文化の骨格となり、メンバーにとって目に見ることのできる、体感することができる「組織文化の人工物」（Schein,1985）になると期待できると同時に、Reason（1997）のいう安全文化の土台となる情報安全システムのための情報ネットワークとして機能することが見込まれる。

そして「④一貫性の維持」とは、経営者層のコミットメントの表現である。これはいくつかの方法が考えられるが、まず一つ目としては、経営者層にも訓練に参加してもらうことを通して、この

取り組みに対してのコミットメントを表わすことが第一歩となろう。経営者が参加することはセキュリティ向上の取り組みとしての教育と訓練の正統性となる。二つ目として、この取り組みを推進する者、ここではセキュリティの専門部署への支援行動である。経営者層がそういった専門的な人々を重視することは、組織的な投資でもあり、経営者層の関心とその優先順位の現れとしてメンバーに認知されることで、組織が標榜する価値を推測する事を可能とする。さらに三つ目としては、教育や訓練の結果のモニタリングとフィードバックである。これが情報セキュリティへの姿勢の一貫性となり、共有された仮定につながっていくと考えられる。

ここまでを文化の3層構造になぞらえて示すならば、セキュリティに関連した教育と訓練は人工物であり、その実施に際してバックボーンとなる教育の組織的な体系もまた人工物である。そして、その訓練を繰り返すこと、その実施主体と組織的な体系を経営者層が支援することはセキュリティの価値の表現である。また、訓練を繰り返すことを通じて、組織が追求する価値の内面化を促し、組織におけるセキュリティに対する仮定が共有され、求められる振る舞いとしてセキュリティ・ファーストな振る舞いが表出するというように理解できる。

これを補強するのが経営者の振る舞いである。自らも訓練に参加すること、訓練の実施体制を経営者層が支援すること、そして、経営者層が訓練の結果をモニタリングし、フィードバックすることが、コミットメントの表れであり、セキュリティに対する一貫した振る舞いとなり、組織メンバーがその価値を推論し内面化に寄与することになると期待できる。

このように、教育と訓練は、充実すべきコミュニケーションのひとつとして、組織作りの鍵として、経営者層のコミットメントの表現の対象であると同時に表現の方法そのものとなることが可能であると考えられる。

3 小括

本章では、まず、本研究の目的である企業組織において文化を醸成することや文化を変化させる試みにおいて、その必要性をメンバー認識させ、新たな方向へと導くことに必要なものとして教育と訓練が挙げられていたことを踏まえ、それらを手段とすることの妥当性と、特に企業組織のマネジメントである以上、これらの取り組みの成果が当然の関心事となるが、成果の把握は何を対象としてどのように行うべきかを中心に検討した。

前提として、組織的な取り組みの成果の対象を文化そのものに置くと、マネジメントの効果の測定という点では、文化の本質はメンバーの内心に関するものでありこれを正確に測定することは本

質的に不可能であり、測定しようとしてもそれは単なるKPIに関する表面的な議論だという批判（Deal & Kennedy, 1982；Schein,1985）があることを踏まえたことによる。

これらの批判は、文化を醸成する、文化を変化させることは、組織メンバーの内心が変化することで結果として組織全体が変わることであるが、現代的企業は専門性によって複雑に分業しており、活動の目標も細分化しているなかで、統一的な指標を設定することは、全体を反映したものにならないという注意である。これは、単一的なKPIの設定の難しさの指摘であるが、同時にKPIの設定の重要さを示すものといえた。

そこで、企業組織においてセキュリティ文化を醸成することは、外部環境からの要請でもあることから、この批判の土台であるSchein（1985）によって示された組織の外部環境への適応サイクルをもとに、この要請に応えることを「使命」として据え、セキュリティ・ファーストがメンバーの共有された仮定となることを「目標」とした場合、具体的な「手段」としては教育や訓練が妥当であるかを検討した。ここでは、Reason（1997）が、組織メンバーの認識や能力といった文化の中核的なものと周辺的な文化的要素とを結び付けるものこそが訓練であると述べており、さらにこれを組織の平時において実施し、測定することが、組織の状態の確認として最善かつ唯一のものだという主張に従い、平時における訓練を手段として文化を醸成していくことが最適解であるとした。

次に、訓練を手段とした上での、その効果の把握である「測定」については、企業組織などで行われる教育や研修の評価軸として一般的に知られるKirkpatrick（1959）による、4段階モデルの3段階目として示される「振る舞い（Behavior）」を測定の対象とすることが現実的な選択であると考えた。そこで、振る舞いを測定の指標として用いることの妥当性を検討するにあたって、振る舞いによって組織文化の状態を把握し、維持する取り組みの実例として、東京電力で行われている取り組みの概要を確認し、そこで行われているマネジメントについて確認した。原子力安全に寄与するものとして個別具体的に例示された振る舞いと実際の振る舞いについてのメンバー個人による比較と内省が出発点となるが、その結果についてグループによっても討議を行うことや、またこれを長期にわたり行なっていることで他者評価によっても醸成、定着が認められていた。そして、これらの成果を外部にも公表しているが、結果に対する注目があることをメンバーが認識することによって取り組みに緊張感をもたらし、メンバーの関心を維持し、取り組みそのものを持続していくことにおいてプラスに効果することが考えられた。これにより、「振る舞い」を測定の対象として文化の醸成の程度の代理指標として用いることは妥当であるとした。

続いて、この原子力産業も研究の対象としている高信頼性組織研究のマネジメントのモデル（中西, 2007）から、組織の標榜する価値をメンバーが内面化し、共有していくためのマネジメントの要件を確認した。それは、高信頼性組織研究では組織の特徴となる組織メンバーの 5 つの振る舞いが Weick & Sutcliffe（2001; 2007; 2015）によって見出されているが、それらは組織の標榜する価値の実現に求められるものが「注意深さ」としてメンバーに内面化され、それが表出したものであると考えられることによる。要件としては、マネジメント全体の一貫性を重視するもので、「教育訓練」とその結果に対する「評価報酬」とこれらを監督する「内部統制」によって一貫性を保つことが中心となる。しかしそれだけではなく、「内部統制」を担うマネジメント層の「情報共有」と「意思決定」における振る舞いもまた「注意深さ」を表すシンボルとなり、メンバーに対して価値の内面化に寄与するというものであった。このマネジメントモデルでも教育訓練は価値の内面化の起点となるものであり、組織が標榜する価値をメンバーが共有するという成果は目標となりえること十分に示している。特に、組織メンバーがシステム思考を持つことが教育の重点として指摘されている点が、セキュリティ文化の醸成においては有用なものであると考えられることから、実務的な課題を検討する際の参考としたい。

最後に、実務的な視点からの組織メンバーの情報セキュリティへの認識の成熟、本研究でいうセキュリティ文化醸成についてのモデルとそのマネジメントの要件を確認した。そこでは、情報セキュリティが向上することのメリットを理解させ、情報セキュリティに対する「①認識を持たせる」、そして「②教育」によって認識の維持と向上につとめる、そしてこれらのための「③組織作り」、そしてマネジメント全体の「④一貫性の維持」が要件として挙げられており、ここでも文化醸成の核となると考えられるものは教育であった。特に認識向上のためのコミュニケーションの充実の一つとして、従来的なトップダウン式の教育を強化するとともに、横方向の教育として、日常の行動の参照点としての同僚の影響を重視し、これを育てるという取り組みが求められ、それを経営者層は支援することが求められていた。実践の面で具体的かつ有用な提案として捉え、これについては検討すべき課題としていきたい。

本章では、セキュリティ文化を醸成することについて、Schein（1985）の提示する外部環境との適応サイクルをベースに検討したが、セキュリティ文化を醸成することを「使命」とし、セキュリティ・ファーストを当然の仮定としてメンバーに共有されることを「目的」とした場合、その「手段」として教育や訓練を行うことは実務的に最適解と考えられた。そしてその効果の「測定」は、

教育や訓練の受講者の振る舞いを対象とすることが限界ではあるが、実例からは妥当かつ有用であると判断できた。

本研究の目的であるセキュリティ文化の醸成は、企業組織をその対象とするが、企業組織の情報セキュリティに対する脅威と求められる対応として、標的型攻撃への対応が最たるものとして挙げられていた。教育と訓練を手段として価値の内面化と共有が可能であるとするならば、標的型攻撃の一種である「標的型メール攻撃」に関する教育と訓練を手段として、「セキュリティ・ファースト」を内面化することを目標としたマネジメントによって、セキュリティ文化として醸成することも可能であると考えられる。そこで次章では、マネジメントの中心となる訓練と教育をどのような体制で運用するのかについて検討するため、実際に行われている標的型メール攻撃訓練から、その効果と課題、その解決として目指すべき体制と訓練について検討する。

Ⅴ 研究課題の導出

ここまでにおいて、教育や訓練の最終的な目標を「組織が標榜する価値の共有」として明確に打ち出し、そのプロセスにおける効果の把握については振る舞いを代理指標として用いること、そしてその成果について経営者層の関心を表現することで、経営学的な意味での文化の醸成は可能であると結論付けた。これは、マネジメントを通じた価値の内面化によって組織成員を方向付けることができるという意味である。本章では、前章のこの結論に立ち、教育と訓練を起点として文化を醸成していくことが十分に可能であるならばどのような組織を構築し、どのように運用すべきかについて検討する。

たとえば情報セキュリティに関するマネジメントシステムである ISMS では、セキュリティ教育をマネジメントシステムの基本的な目的を示す方針のうちの 1 つに含め重要視している（中尾ら, 2015）。ISO/IEC27002: 2013 では「情報セキュリティの意識向上、教育及び訓練」を 7.2.2 で定め、「情報セキュリティに関する各自の責任及びその責任を果たす方法について、認識させることを狙いとすることが望ましい」とし、長期かつ定期での計画が期待されている。特に、情報セキュリティの目的や自らの行動が組織に及ぼす影響について理解するために、過去の情報セキュリティインシデントの経験を反映させ、Know-How にとどまらず Know-Why を重視することを求めている。

この教育のなかでは、a)経営者層の情報セキュリティに対するコミットメント、b)組織内で定められたポリシーとその遵守について、c)情報保護に対する個人の一般的な責任、d)パスワードや個人のデスクに情報及び情報媒体などを放置しないことや、パスワードの管理、紛失を含めた情報セキュリティインシデントに遭遇した際の連絡先、といった職場での基本的な手順、e)情報セキュリティについての情報の入手先、といったような側面が含まれることが望ましいとされる。すなわち、情報セキュリティに対する組織の姿勢を理解させるとともに、組織内で従事する業務に関連した情報とその活用におけるリテラシーの向上を目的とした教育を求めている。業務において顧客の個人情報を利用する企業にとっては、「Ｐマーク」[71] の取得・維持において、情報セキュリティに関す

[71] 「プライバシーマーク®制度」。JIPDEC(一般財団法人日本情報経済社会推進協会)が設定する個人情報保護の取り組み・要件を満たした事業所に付与される。1998 年より JIPDEC が運営するは、事業者の個人情報を取り扱う仕組みとその運用が適切であるかを評価し、その証として、事業活動においてプライバシーマークの使用を認める制度。審査基準は、JIS Q 15001「個人情報保護マネジメントシステム－要求事項」をベース

る教育をすべての従業員が受講することが求められていることから、教育の実施と確実な受講が必須の取り組みとなる。

そこでまず、分析の視点として、実践の面から検討すべく、教育と訓練について、なかでも本研究の対象である標的型メール攻撃訓練が一般ではどのように行われているのかその実態について確認する。第 I 章において確認したように情報漏洩が事件・事故として取り上げられる日々が続いているが、企業もこれを他山の石とせず自らの戒めとして捉え、教育や研修に取り込み、訓練を実施している。なかでも標的型メール攻撃は、組織体の情報セキュリティにおける脅威の最たるものとして挙げられている標的型攻撃の一種であり、セキュリティレベルの高いシステムの導入といったハード的対策と、教育や訓練といった組織メンバーに対して行うソフト的対策の両輪が、あらゆる組織において喫緊の対応が迫られていることはこれまでに述べたとおりである。

企業組織の情報セキュリティの問題の解決として、これまでの組織文化に関する先行研究の知見から、セキュリティ文化の醸成という目的において、教育と訓練を行っていくのであるが、企業組織が実施する教育と訓練である以上、成果の測定として KPI の設定は避けられないため、いかなる KPI がふさわしいのかという、前章で確認したようなセキュリティ文化醸成のモデルの実践という論点に移ることになる。マネジメントの体制をどのように造り、訓練の効果測定としての KPI をどのように設定するべきかという論点であるが、これらについて検討するため、次項では実際に行われているセキュリティに関連した教育訓練の実際を確認し、その効果と課題を把握する。

1 標的型メール攻撃訓練の実態

(1) 標的型メール攻撃とは

標的型メール攻撃とは、情報セキュリティ上の組織外部からの悪意ある攻撃のうち、無差別に攻撃が行われるものではなく、特定の組織あるいはグループを標的とした標的型攻撃の一種であり、特定の受信者に対してマルウェアのダウンロードを期待した電子メールを送ることである。メール本文に、URL が記載されており、アクセスするとマルウェア等がダウンロードされてしまうものと、添付ファイルを利用したものがある。添付ファイルについては、PDF ファイルや表計算シートなど一般的に用いられるビジネスアプリケーションの脆弱性を利用している。この添付ファイル

にしており、個人情報保護法等のコンプライアンスを前提とする。2018 年 12 月 1 日現在で 16,000 超の事業所が認定を受けている。

を開くことをキッカケとして、ファイルに埋め込まれたマルウェアが活動し、PC 上で動作するソフトウェアの脆弱性を利用して、PC 上で取得した情報を外部のサーバなどに送信しようとするという流れになる。そのため送信者側は、メールそのものや添付ファイルの開封を促すために、メールの件名や文面、添付ファイルの名前が各組織を狙ったものにカスタマイズしている。例えば、2015 年に発生した日本年金機構から情報漏洩の件では、波状に攻撃メールが送られてきていたが、第 1 波には厚生労働省の Web サイトに掲載されている文書名が記載されており、第 2 波には年金に関係するセミナーや研修の告知が記載されているといったように、受信者の業務に関連があることを匂わせ、開封を促していた。このように、対象のユーザや組織について個別化されているため、ユーザ自身が個々の攻撃に対して正しく対応できるようになることが呼び掛けられている（JPCIRT/CC, 2008）。NCA に加盟している企業に対するアンケート調査では、およそ 85.7%の企業で標的型メール攻撃訓練が実施されている[72]。組織内外との通信手段として電子メールや SMS を用いることは極めて一般的であるがゆえに、標的型メール攻撃についての教育や訓練は必須のものとなっている。

(2) 訓練の流れ

訓練のフレームは、まず前項に示したような標的型メール攻撃についての注意喚起を目的とする集合的な教育が行われ、一定の時間の経過後に訓練対象者に向けたメール配信が行われることが通常の組み合わせとなる。

一般的には、集合的な教育または e-Learning をチャネルとして活用した教育である。ただし、この教育は、PC やアプリケーション、インターネットのセキュアな利用についてといったような一般的側面を含む包括的なものである。この中にセキュリティインシデントの事例に関するものがあり、標的型メール攻撃はあくまでそのうちの一つとなる。

ISMS においては、標的型メール攻撃に対する教育は、12.2.1 に定められる「マルウェアに対する管理策」のなかで、検知についてハード的な対策の充実を求めるとともに、「それらを受け取った時の対応について、すべての利用者に認識させる」としており、これに対応するものとなる。

---

[72] NCA 標的型攻撃メール訓練ワーキンググループによる調査とその結果に関する内部資料より
アンケート期間 2018 年 6 月 27 日から 7 月 19 日　メール訓練に関する 11 項目で構成
配布 73 チームに対して 41 チームが回答（回答率 56%）うち 36 チーム（85.7%）がメール訓練を実施している。

標的型メール攻撃に関連する教育の具体的な内容としては、まずこういったメールによるインシデントが実在し、被害が発生していることを他社などの事例から知ることである。組織は技術システムレベルで対処を試みているが、当然システムに完全なものはないのでこれをすり抜ける形で届くメールがある現実を知ることから始まる。次に、こういったメールについての対応として惰性で行動しないことを求める。まずは送信元のアドレスや送信者表示のチェックである。そして、心当たりのない発信元や件名である場合は、①メールそのものを開封しない、②開封したとしても心当たりのない内容であれば本文記載の URL を閲覧しない、③添付された各種ファイルを開けない、ということが標的型メール攻撃による被害を回避するための基本的な行動として共有される。その後、研修内容の理解程度について何らかの試験方式による確認が付加的に行われることもある。

その後、いくばくかの期間を経たのち、知識の定着の確認を含め、実践として標的型メール攻撃訓練が行われることになる。業務に関連がありそうな件名や文面によって、本文中に埋め込まれた URL に誘導する URL 埋め込み型や、添付ファイルの開封を促す添付ファイル型として受講者に送信される。

(3) 主な実施主体としての CSIRT

こういった訓練を民間の営利企業で実施する場合、多くの企業では CSIRT が中心となってその実務を主導することが多い。CSIRT とは、組織内で発生したコンピュータセキュリティに関連するインシデントハンドリングサービスを行うチームである。

CSIRT が提供するサービスは、イニシアチブが求められるフェーズからの分類としては、（a）アラート・警告やインシデントハンドリングといった「事後対応型（Reactive）」、（b）告知や侵入検知といった「事前対応型（Proactive）」、（c）平時におけるリスク分析や教育といった「セキュリティ品質管理（Security Quality Management）」の 3 点が挙げられている（West-Brown et al., 2003）。

日本国内の企業 CSIRT は、しばしば消防署に例えられることがある。これは、インシデントの発生時には事故対応に当たり、事故の発生していない平時には、予防体制の構築や組織内に対するセキュリティ教育や啓蒙活動に従事することが多いことによる（中西ら, 2012）。この啓蒙活動という点で、利用者の認識の向上や情報ネットワーク環境をセキュアに保つという面からこれを公衆衛生の維持向上活動と捉え、さらには情報端末の利用者の気軽な相談先や具体的な治療を担うという面から「病院」として例えられることもある。

この標的型メール攻撃訓練やその前置きとなる教育といった活動は、平時のサービスとなる「セキュリティ品質管理（Security Quality Management）」に含まれる[73]。

2 従来型訓練の問題点

(1) 従来型訓練の成果と限界

訓練である以上、目的があり、その目的に対する効果について何らかの KPI が設定され測定されることになる。先にも述べたように、標的型メール攻撃による被害の回避は、まず心当たりのない発信元や件名のメールそのものを開封しないこと、開封したとしても心当たりのない内容であれば本文記載の URL を閲覧しないこと、添付された各種ファイルを開けないこと、という 3 つの回避行動が基本となる。当然、各組織体はメンバーがこういった対応行動が適切に選択できるよう教育研修に注力している。これに続く標的型メールへの対応訓練は、こういった回避行動が集合的な教育などにより情報共有されたうえで、開封率が KPI として設定され、その成果を検討されることが多い。

こういった訓練とその結果に関する報告をレビューした内田（2015）によれば、日本国内の自治体における訓練で、メール本文中の URL のクリックを訓練の KPI に据えたものの例として、初回の訓練として、実施の予告をせず訓練を行った結果は 40%のクリックがあったが、これから 2 年後において訓練を実施したところ、その成果として予告なしの訓練では 12.5%／予告ありの訓練では 6.3%までの低減が確認されている[74]。また、海外のコンサルタントの事例では、毎月訓練を繰り返すことで４％まで低減することも報告されているという[75]。

このように、従来型の訓練によっても回避行動の増加・危険行動の減少が認められ、その有効性は当然に是認されるものである。しかし、訓練を重ねても４％のメンバーは、なおもこれらの回避行動がとれず、それにより悪意のある外部者を呼び込む起点となってしまっているということでもある。

まず、この開封率という KPI の設定そのものに問題があると考える。訓練担当者や訓練対象者の属するセクション管理者としての上司にとっては、設定された KPI とその値は非常に強いメッ

---

[73] CSIRT や CSIRT のコミュニティである NCA については、補論 3 を参照されたい。

[74] 藤沢市・豊島区・横浜市などでの調査

[75] Spitzner (2014) Measuring Chang in Human Behavior, RSA Conference

セージ性を持っており、メール本文に埋め込まれたURLのクリックに関する数値がKPIである場合、クリックした者を過失者とみなし叱責するという構図になりやすい。しかし、現場のオペレーションから見れば、多様なステークホルダーと多様なやり取りが交わされている。多忙なメンバーがポリシーの順守に拘泥することによって真に重要な業務関連メールを見過してしまう可能性も含んでおり、現業と訓練のトレードオフが発生することになる。また、抜き打ち指名型で訓練を実施し、回避行動がとれない結果となった場合には、その個人宛てに強い指導・叱責が即座に入るという訓練手法をとる企業もある[76]。この訓練の実施フレームは、一見すると非常に効率が良く、効果も高そうである。しかしこの手法も、繁忙感を抱えながら業務を推進する者にとって、CSIRTを筆頭とするセキュリティ担当者／部署へのイメージがネガティブなものとなってしまうことが懸念される。さらに、情報セキュリティ関連サービスのベンダーによる調査[77]では、調査対象者の約30%においてこの訓練の結果が自身の査定や考課に直接影響があると回答している結果を示している。さらにこれによってメールの閲覧にかかる時間が大幅に伸びているとの回答を受け、現実の業務において効率の著しい低下がもたらされていることを危惧している（デジタルアーツ, 2019）。訓練の結果が自身の業務査定や考課に直接紐づけされた訓練を続けていくことは、訓練そのものにも忌避感情をもたらしかねないと考える。

このように、従来型の訓練では、平時においてはこれら担当者が主導する教育・訓練に対する望ましい姿勢が得られないことでその効果を最大化することが難しく、また、重大なインシデントが現実化した時には全社的な協力が得られないことも危惧される。

ここに従来型訓練の限界がある。これは、従来型訓練の目的が個々人の情報リテラシーの向上にとどまってしまい、個々人の認識や心情をはじめとする個人の特性、その個人が担う業務の特性や、それらから生まれる反応といった受講者側の視点が欠けていることによると考える。開封の必要性を感じさせるような発信元の偽装・なりすまし、開封を促すような文面・内容の個別化、精巧化という攻撃者が常に防御側を上回るという前提の下では、開封率をゼロにすることは困難を極めるであろう。訓練を実施するからには開封率は「ゼロ」を建前として標榜せざるを得ないことは理解できるが、こういったマイナスの影響について考慮されることなく、開封率がKPIに設定され、必罰型で展開されることは望ましくない。

---

[76] 2018年3月3日に行われたNCAのワーキンググループでの聞き取りなど。

[77] デジタルアーツ（2019）「勤務先における標的型攻撃対策に対する意識・実態調査」
https://www.daj.jp/company/release/common/data/2019/042401.pdf

根本的には、失敗を恥ずかしさゆえに隠そうとするのは人間の本質であり、さらにそれを叱責されるならばなおさら隠そうとするのが人間本来の学習である。これは、損失回避と呼ばれるが、まだ顕在化していない可能性のレベルにおいても、利得よりも損失を過大視する心理傾向をもっていることによる[78]。さらに、失敗に対して忌避感情を持つだけでなく、そもそも成功／失敗の機会に関わろうとしない消極的な対処行動となり学習につながらないことも三沢ら（2014）によって指摘されている。実務に置き換えればメールアプリケーションそのものを立ち上げることを避けるという極端な対処行動もあり得るということだ。

仕事で利用する単なるツールのひとつであることから、タイムプレッシャーや繁忙感を持っている場合、メールの真贋を検討する余裕がない場合などは、単なる送り手側の間違い、メールの不具合として自らのエラーを認知することなくやり過ごされてしまうことは往々にしてあるだろう。また、開封したのちに文面や内容から標的型メール攻撃であることに気が付いた場合、冷静さを失ってしまうことも考えられるが、プレッシャーが高い状況下に置いては、訓練によって最初に身に着けた反応に立ち返る傾向がある（Weick,1987）とされることから、最初の訓練が重要である。にもかかわらず最初の訓練が叱責・必罰型の訓練であると、訓練の効果を減殺し、逆効果となることは想像に難くない。

標的型メール攻撃によるマルウェア感染などは、即座に認識することは難しく、影響は事後的であることが多い。そして攻撃は、テストとしての第 1 波、本番としての第 2 波というように波状になされることが多い。具体的には、先述の日本年金機構からの個人情報漏洩の例では、5 月 8 日から 5 月 18 日というように、およそ 10 日の間隔があったとされている[79]。そのため、訓練といった仮想環境はもとより、現実の業務を行う本番環境において積極的な放置、すなわち問題あるサイトへのリンクをクリックしたことや添付ファイルの開封を隠すという行動は、インシデントそのものと言える。そのため、このクリックや開封を積極的に表面化させること、すなわち報告という振る舞いによって表面させることが重要となる。

(2) 問題の改善としての心理的安全とその効果

前項で検討したように、必罰型の訓練によって生まれる懸念を除去し、インシデント発生を表面化させる、すなわち情報セキュリティインシデントの起点となってしまった可能性があることにつ

---

[78] Kahneman, D. & Tversky, A.（1979）による「プロスペクト理論」の土台としても知られている。

[79] 日本年金機構における不正アクセスによる情報流出事案検証委員会（2015）「検証報告書」を参照されたい。

いての報告を促すには、何が求められるのだろうか。これが訓練の成果を把握するKPIの設定の問題の中心的課題となると考えているが、これを解決に導くのが、第Ⅲ章で検討した「公平な文化」によって「心理的安全」が確保されることで、「報告という振る舞い」が引き出される「セキュリティ文化」であろう。

訓練の成果を測定する指標として、開封率というKPIではなく新たな別のKPIが設定されるということは、新たなKPIとその目標値の達成に向けて新たな学習を始めることに他ならない。新たな学習に際しては、①明確で信頼できる将来像、②新しい行動レベルの目標、③学習者に機会があること、④適切なトレーニングと時間と費用、⑤新しい行動に合致した報酬／管理／規律のシステムなどの構造的サポート、が提供されることによって新たな学習に対する「心理的安全」が生まれるとされていた（Schein, 1985, 邦訳書第2版, pp.113-114）。これは、新たな取り組みに伴って個人レベルで発生する学習遅滞や一時的な生産性の低下が許容されること、すなわち批判や懲罰の対象にならないことが示され、そしてそれが規律と報酬システムによっても支持されていると実感でき、一貫性が保たれていることが理解できることで安心して新しい学習に取り組むことができるというものであった。

であるならばこの心理的安全は、訓練を通じた新たな学習において、訓練の目的である組織の新たな目標、すなわち標榜する価値を正しく認識させ、さらに内面化を促進することでメンバーに共有される仮定のレベルにまで組織に埋め込むことを補助するといえる。訓練を真に文化醸成の取り組みとするためには、心理的安全が常態となることこそが文化の変革の中心的問題であるといえ、KPIの設定と結果の取り扱い方がこれに直結している。

第Ⅲ章において「安全文化」（Reason, 1997）を下敷きとして検討した「セキュリティ文化」においても重要な要素である。要素として求められる下位文化としての「報告する文化」において「報告のしやすさ」もその要件の1つとして挙げたが、これは物理的にも精神的にも報告しやすいことを意味している。報告を促進するためには報告の物理的な側面での簡便さが必要であるとともに精神的な面でも報告を妨げる心理的要因を排除する、すなわち心理的安全を確保する必要がある。だからこそ、訓練であるとしても結果をもってして叱責につながることを避けなくてはならない。

またKPIの設定は、何が称賛され支持される行為であり、何が非難される行為であるかが明確にされている「公正な文化」に根差したものでなくてはならない。すなわち、開封してしまうことは完全に避けることができないことを前提とするならば、開封したことそのものが叱責や懲罰の対象であることはあり得ない。むしろ、開封したことの表面化が必要であり、これを積極的に報告し

て共有することが求められるのであり、開封してしまったとしてもこれを報告する行為こそが称賛され、支持される振る舞いとして明示され、達成すべき訓練の成果として選定される必要がある。

「セキュリティ文化」の４つの下位文化の残り２つに言及するならば、平時においてはこういった訓練を実施し情報セキュリティ向上を推進する者、そしてインシデントが現実化した非常時においてはこれに最前線で対応する者に対して、組織的な対応として積極的に権限を委譲し、エンパワーメントする「柔軟な文化」もまた、組織全体として情報セキュリティに価値を置いているという推測をメンバーにもたらすだろう。そして、これらの下位文化が揃うことで、個人レベルには積極的な情報提供を促し、訓練の KPI とその結果について関心を持ち、さらにこれらを活性化させようとする「学習する文化」へとつながっていくと考えられる。

このような組織の状態が「セキュリティ文化」が醸成された組織であるとしたが、「報告すること」を KPI の軸とした標的型メール攻撃訓練を通じて、自らが組織の情報セキュリティに関する情報共有に積極的に参加し、それが組織内で評価され、メンバー間の相互の敬意に基づいて適切な者が推進し、ベストプラクティスを組織内で積極的に共有する文化が醸成されると、導出される組織メンバーの振る舞いと、それによる組織的な成果は次のようなものとなることが期待できる。

①標的型メール攻撃は波状に実行されることが多いため、攻撃の初期段階において一部のメンバーにおいて回避行動が正しく取れなかったとしても、攻撃が疑われる事象が早期に認識され、報告されればメンバー間で攻撃の発生の情報が共有され、第２波以降の被害の発生は抑止できる。

②標的型メール攻撃を認識し、正しく回避行動がとれたメンバーによる報告があれば、一部において回避行動がとれず、かつ攻撃であると認識できていないメンバーが存在したとしても、組織的に事態に対処することが可能となる。

③情報セキュリティに関する教育や訓練の中でこういった報告や周囲に知らせる行動を KPI の一つに据えて情報収集の対象とすることで、組織全体の情報セキュリティに対する備えを測定し改善を重ねることができる。

④現場レベルでは、平時はもとよりインシデント発生時に取るべき行動とそれによる業務への影響の最小化、そして影響下からの復旧についてのベストプラクティスが共有され、インシデント発生を織り込んだレジリエントな事業活動が確保される。それは、情報システムを利用する際の他者に与えうる影響を、当事者として正しく認識し、これに貢献しようとする主体性とともに保持されていることに基づく。

(3)　研究課題の導出

本研究では、文化の変革に求められる「心理的安全」を生み出すために必要とされる諸要素について、Schein（1985）の示した「①将来像の提示」、「②行動レベルの目標設定」はリーダーシップの問題として捉える。つづく「③学習の機会」、「④適切なトレーニング」については教育研修・訓練の問題として捉える。残る「⑤報酬・管理・規律のシステム」を、これら中でもっともミクロサイドで作用する「文化的要素」の問題として捉える。そして、この3つの問題の中核として、リーダーシップと文化的要素を繋ぐ媒体として機能するものが教育と訓練であると考え、標的型メール攻撃訓練をその主要な題材とし、これらの要素をどのように用い、そしていかに文化を醸成するかということに関心の中心がある。

そして、情報セキュリティに対する価値、すなわちセキュリティ・ファーストを信奉する価値の中核として、この価値に沿って人工物として設計された諸要素と、この価値を内面化した組織メンバーの共有された基本的仮定による3層構造によって成る文化を、教育訓練を通じて醸成するために、訓練の成果を測定する手段、測定の対象となるもの、そしてそれらをどのように用いることが組織的な成果につなげることができるかを検討してきた。結論として標的型メール攻撃訓練の実施に際して、「報告」という振る舞いを訓練の成果測定のKPIに据え、訓練を行うことが適切であると考えた。

そこで、セキュリティ文化を醸成するという目的に適うよう、訓練の成果の測定指標であるKPIをどのように設定し、運用していくのかという実践面での問題を新たな課題として本稿における基本的な研究課題とする。

セキュリティ文化の醸成という自分事にしにくい価値観を内面化するという本研究の目的においては、報告という振る舞いを文化醸成の代理指標として、どの程度の頻度においてサイクルを回していく必要があるのか、すなわち実施の頻度はどの程度が適切であるのかも課題とする。

ここまでの課題にあるように、「実装」や「サイクルを回す」といった実践に付随する問題として組織的な面についての課題がある。具体的には、訓練の実施を担う者はどういった者が適切であるのか、見出された頻度を実践するにはどのような体制でこれを支えていくのかについては現実的で組織的な課題である。そして、これらの実践を包括的に推進する者、すなわちリーダーシップに関する課題でもある。文化の醸成という中心的な目的おいてこれらを行うのであるが、企業文化の議論では、経営者層の価値や信念、または組織に対する脅威やそれへの対処としてのビジョンをいかに組織内に伝播させるかというように、経営者が起点となるモデルが多く提示されていた。一方

で日本企業の例として、プレイングマネージャーとして現場をリードしながらも、そこでの情報をもとに経営者層の意思決定に好影響を及ぼす中間管理職の存在が見出されていた。従って、セキュリティ文化の醸成を主導する主体は、本稿の関心で言えばまず訓練の企画実行の主体はどのような者であり、組織においてどのような位置づけの者が適切であるか、そしてそれらの者を中心としてどのような組織体制を構築するかが課題となる。

そして、これは旧来からのトップダウン式、すなわち縦方向からの教育にのみ関連した課題ではない。第IV章で確認したSpitzner（2014）の指摘では、情報セキュリティに関するコミュニケーションの充実は、同僚によってもたらされる横方向からの教育がその一部をなしていた。この横方向から教育が可能となる同僚をどのようにつくり、組織として機能させるのかについては論点として残ることになる。横方向の教育とは、振る舞いの参照点を身近に配置するといういわゆる「お手本モデル」であるが、この前提なるネットワークをどのように作るのかという実務的な議論である。これは、縦方向の訓練の実施にも影響を与えることになると考えられ、先に挙げた訓練実施の組織体制と並行した議論になると考えられる。

そしてこれらの実務的な課題を明らかにしたのちに、これらの訓練実施のプロセスや実行体制は、文化の醸成や変革といった局面における理論的な側面をどのように充足しているのかを整理する。具体的には、①O'Reillyが文化の醸成において求められる要件と要素をどのように充足しているのか、②Deal & Kennedy（1982）が示した文化変革の要件と備えるべき諸要素をどのように充足しているのかである。後者については、文化の変革に求められる「心理的安全」（Schein, 1985）を生み出すための要件と備えるべき諸要素とともに、情報セキュリティに対する「当事者性の向上」の視点として整理していく。そして、これらの他にも文化の醸成や変革に要件や要素を見出すことを試みる。

最後に、先行研究に従えば、企業文化とは組織メンバーに共有された仮定というように、メンバーの内心の問題であるが、これらの課題が明らかにされることを通じて、本研究で示したところの「セキュリティ・ファースト」を中心的な価値としてメンバーが共有したセキュリティ文化は企業組織において醸成されうるのか、そして、標的型メール攻撃訓練はこれに真に貢献しているのかを確かめることが最大の課題である。

以上を明らかにすべく、次章では企業において行われている標的型メール攻撃訓練の実際を確認する。

Ⅵ 企業事例

本章では、前章において導出された課題を解明すべく、事例研究を行う。事例研究では、実存する企業組織において実施されている情報セキュリティ向上の取り組みの一つである「標的型メール攻撃訓練」の実際を確認し、その目的や実施の内容、特に KPI の設定や実施の体制、そして訓練の効果について把握する。次いで、それらの実態を踏まえ、企業組織の訓練に付随する課題や問題点を抽出し、その改善について実践的な面から検討する。これらの情報・資料の収集の手段としてインタビューによる調査を選択した。なぜなら、標的型メール攻撃訓練は現代的な企業組織に必須の取り組みではあるが、新たな取り組みであるためその運用や組織に踏み込むような仔細な 2 次資料がない。それは、本稿が課題として明らかにしようとするものの中心は教育や訓練についてであり、これらは基本として企業独自のノウハウである。また本研究は情報セキュリティに関連するものであり、企業秘密個人情報といった情報の管理に密接に関連するものであることから、これを喧伝するインセンティブは見当たらないことによると考えられる[80]。そこで、これに取り組む企業組織にアプローチし、その実際を調査することが求められると考えたことから、企業を分析単位としてインタビュー調査をその手段として実施する。

研究対象の事例の選定とその方法については、少数のケーススタディが前提となる。もちろん、多くの事例について行うのが望ましいが、先にも述べたが教育や訓練は、それぞれの企業組織の独自のノウハウを含んだ独自の取り組みである。また、情報セキュリティに関する側面は、備えを強調するとかえって標的になりやすいという独特の問題を持っており、広範な対象を選定したり、機微に至る深い調査は困難があることによる。

本研究では、事例として 3 社を対象とした。これは、企業規模といった外的な基準や訓練の経験といった内的な差異についても踏まえることが必要であると考え、これを可能にするためである。

調査対象企業の概要は次の通りである（表 12）。

[80] IR 資料等でサイバーセキュリティの向上の取り組みについて説明を行っている企業も多いが、その一方でサイバーセキュリティに関する情報公開を行うことで、かえって攻撃者の興味を惹き、そのターゲットとなることでインシデントの危険が高まるという認識、もしくはこれへの懸念はまだまだ強いのが実際である。

表 12：インタビュー対象企業の概要一覧

	業種（1	規模（2	目的	頻度
X社	生活関連サービス業・娯楽業	2,000	教育内容の実践	年1回
Y社	情報通信業	8,000	リテラシー向上	年2回
Z社	サービス業	8,000	教育内容の実践	年12回程度

1）総務省の定める日本標準産業分類（平成25年10月改定）（平成26年4月1日施行）の大分類に基づく

2）訓練対象アカウント数

出典：筆者作成

X社は初回の訓練として取り組んだ企業であり、その訓練結果から教育の効果や訓練実施における基本的な課題を把握することにおいて適切だと考える。Y社は、X社との比較において企業規模が大きいこと、そして訓練の経験の蓄積があることで、蓄積された結果から訓練実施における発展的な課題を把握できると考えことによる。Z社は、企業規模はY社と同規模であるが、一般的に確認できる訓練の回数との比較では訓練の頻度が特異的に高いことが特徴である。この高い頻度で行われる訓練について、これを仔細に確認することで前2社において把握された課題の解決や、継続的に訓練を実施していく上での要件整備などについて検討できると考えたことによる。

問題における基準として野村（2017）は、Yin（2014）による5つの分類とGomm et al.(2000)による3つの分類を統合、再整理し、「極端／珍しい／決定的」、「一般的／典型的」、「後継的／新事実考察型」と挙げている。この3社の事例においてはX社およびY社の2つの事例が「一般／典型的」となろう。しかし、それだけでなく訓練の結果については先行研究との比較が可能である点で「後継的」として位置付けることもできると考える。これらに対して残るZ社は、取り組みが長期間にわたっている例となり、「極端／珍しい／決定的」という点と、時系列として変化を確認できる点で「後継的／新事実考察型」を備えた例といえる。

この点で、Z社を調査対象として選択したこと、訓練の実績が長期かつ豊富であり、そのサイクルが非常に速いという特異的な事例を対象とすることは「レアケース」といえ、この事例について深耕することは、Yin（2014）がいう「単一ケーススタディ」として認められる場合に準じるものとなり、この点ではおよそ単一のケーススタディに近いものになるとも考える。しかしこれにより、「単一の研究対象の内部に生じるダイナミクスの理解に焦点を当てる研究戦略」（Eisenhardt,1989,p.534）といった点においても十分に貢献できるものとなると考える。

このように、これら3つの企業事例を用いることで企業規模、訓練目的、取り組みの期間の違いから比較、考察が可能となる。そして、この共時的な分析を踏まえたうえで、取り組み期間の長

い企業を事例として取り上げることで、その結果の長期的蓄積についてを通時的に分析することが可能となる。なにより、取り組みを長期間にわたって維持できているという事実もまた本研究の分析の対象であり、中核的な課題である。

これらを踏まえ本章は次のように展開する。まず、小規模・一般的という点でＸ社の事例を確認し、先行研究との比較を通じてその効果や問題点の整理を行う。次いで、大規模・一般的な例としてＹ社を取り上げる。Ｙ社の事例についても同様に、先行研究との比較を通じてその効果や問題点の整理を行う。そしてこれらを踏まえ、大規模・決定的、そして後継的な例としてＺ社を取り上げる。Ｚ社で行われる訓練の内容とその結果、そして実施の体制について確認し、その結果について時系列の視点を加えて分析する。そして、Ｘ社およびＹ社の２つの事例と比較しながら、Ｚ社の事例から得られた知見を、特に運用についての特異点を整理する。

本論に進む前に、以下が前提となることを確認し、付しておく。まず、本稿が課題として明らかにしようとするものの中心は教育訓練や研修についてである。これらは企業独自のノウハウであり、また本研究は情報セキュリティに関連するものであり、企業機密や情報の管理に密接に関連するものであることは先に述べたが、これにより研究目的としての論文の内容として公表できる範囲には限界がある。これらを当然のこととして、さらに研究倫理として、企業名およびインタビューイに

表13：インタビューの概要と対象者一覧

手法	対象	コンディション	
インタビュー	Ｘ社	日時および期間	2018年5月22日午後1時からおよそ2時間
		場所	Ｘ社本社会議室
		インタビューイ	Ｘ社情報セキュリティ担当役員Ａ氏 Ｘ社情報セキュリティ担当Ｂ氏（CSIRTメンバー） Ｘ社情報セキュリティ担当Ｃ氏（CSIRTメンバー） 情報子会社X²情報システム担当者Ｄ氏（CSIRTメンバー）
	Ｙ社	日時および期間	2018年9月4日午後4時より約1時間半
		場所	明治大学駿河台キャンパス内演習室
		インタビューイ	Ｙ社情報セキュリティ担当Ｅ氏（CSIRTメンバー）
	Ｚ社	日時および期間	①：2018年11月15日午後3時からおよそ2時間 ②：2019年2月5日午前10時よりおよそ1時間半
		場所	明治大学駿河台キャンパス内演習室
		インタビューイ	Ｚ社情報セキュリティ担当Ｆ氏（CSIRTメンバー）

出典：筆者作成

ついては記号でマスクし、インタビュー調査によって得られた情報の記述内容については各企業の承諾を得て行なった。調査の概要と対象者は表 13 の通りである。

なお、本章第 1 項の X 社の事例および、第 2 項の Y 社の事例については、2018 年 9 月に行われた日本心理学会第 82 回大会、セキュリティ心理学研究 2018 セッションでの「標的型メール攻撃対応訓練と実行体制の事例紹介　－心理的安全に着目して－」に基づいている。

1 X 社の事例

本節では、X 社を例として、その直近の取り組みと結果を取り上げる。調査は、2018 年 5 月に X 社の本社においてインタビュー調査を行い、資料の提供を受けた。

(1)　調査の概要

日時：2018 年 5 月 22 日午後 1 時からおよそ 2 時間

場所：X 社本社会議室

インタビューイ：X 社情報セキュリティ担当役員 A 氏・X 社情報セキュリティ担当 B 氏（CSIRT メンバー）・X 社情報セキュリティ担当 C 氏（CSIRT メンバー）・情報子会社 X^2 情報システム担当者 D 氏（CSIRT メンバー）

X 社は、関西地方に拠点を置き、生活関連サービス業・娯楽業を主たる業務としている[81]。西日本に約 50 の営業拠点を抱えており、情報システム系子会社として X^2 がある。この 2 社を合わせ、管理の対象となるアカウントは、およそ 2,000 アカウントである。

主業務では、法人・個人を顧客としてサービスを提供しており、従来からの対面型の販売に加え、インターネットサイトを利用した販売がある。このサービス提供の過程において大量の個人情報がやり取りされ、X 社内に蓄積されることになる。これらの事情から、①守るべき情報資産の価値が高いことで悪意のある外部者のターゲットとなりやすいこと、②営業地域が広く、比較的小規模の拠点が多いというジオグラフィック的特徴がまずある。そして、③従業員数が多い、パートタイマー・期間雇用者・派遣労働者といった多様な労働力を活用していることに加え、近年の労働環境を受けてその流動性も高いというデモグラフィック的特徴などがあることから、統制の面で多様な課題を抱えており、これを克服するうえでも、外部の悪意者による古典的な攻撃手法である標的型メ

[81] 総務省の定める日本標準産業分類（平成 25 年 10 月改定）（平成 26 年 4 月 1 日施行）に基づく

ール攻撃への対応としての教育研修と訓練は、セキュリティの向上にとって重要なファクターとなっている。

(2) 教育研修と訓練の概要

まず、訓練については次の通りであった。

訓練実施の主体は、X社およびX[2]社の技術系の従業員から構成されているCSIRTであり、彼らが訓練を企画している。実施の頻度は年に1回であり、外部コンサルタントを活用し、社内に実存するアカウントと類似するアカウントより送信される。訓練の対象となるアカウントは、一般職層の従業員に付与されているおよそ2,000アカウントである。これには、正規従業員だけではなく、派遣労働者、短期の契約社員といったいわゆる非正規従業員も含まれている。

訓練のフレームは、次のとおりである。まず、前段として社内報おいて訓練実施の予告を行う。次に、本文中にダミーとなるURLを埋め込んだメールを送信する。これを開封し本文のURLをクリックしリンク先にアクセスしたアカウント数を計測する。このリンク先は、いわゆる文字化けしていて意味のない文字・記号が羅列されているページとなっており、これにより標的型メール攻撃であると認識できた者は、利用しているPCからLANケーブルを抜いたうえでCSIRTへの通報を求めるというものである。したがって訓練のKPIは、クリック率と報告数となる。

X社では、この訓練の前提となる教育研修として、教育教材を社内報に盛り込み、同時にミニテストを付録することで、知識のインプットとアウトプットを同時に図る構造となっている。これを毎月1回程度であるがおよそ2年間継続してきた実績があった。これは、情報リテラシー全般の獲得と向上を目的としているものであり、標的型メール攻撃のみを対象としたものではない。ミニテストの中には、PC本体に関するものもあり、例えばデスクトップ型であれば背面に接続されているケーブルのタイプや構造の理解と把握を求めている。標的型メール攻撃に関するものについては、他社事例とその影響、標的型攻撃のメールであると認知するための要点、そして実際にURLをクリックしてしまった時の具体的な行動として、デスクトップ型であればLANケーブルを抜き、上長に報告することなどである。

こういった情報リテラシーのボトムレベルからの強化を目指すX社が、標的型メール攻撃がインシデントとして顕在化した場合に個人に求める行動は、報告と報告の前段として自らがLANケーブルを抜くことである。そして報告を受けた上長は、「LANケーブルを抜いてある旨」をCSIRTへ通報し、その後の処置について指示を受けるという流れになっている。外部からの悪意

によってマルウェア等への感染し、これがネットワークを介して接続されるその他のアカウント・機器への感染拡大を防ぐためである。

(3) 訓練の結果

ここで、X社の実際の訓練の結果を確認する。まず、第1のKPIである本文中に埋め込まれたURLの「クリック率」であるが、事業系のX社では約20%であった。そしてシステム系のX[2]社では約5%であった。そして、第2のKPIである「報告」については、44件の通報がCSIRTに寄せられた。このうちURLをクリックしてからの通報は23件とおよそ半数であった。一番望ましい状態である、メールが届き開封し、件名や本文を確認したところその内容に疑念を抱き、標的型メール攻撃の疑いとしてCSIRTへ通報した者は11件であった。

この結果に、時間軸を加えて分析してみると、訓練メールの送信から1時間以内にクリックしたのは45件で、この訓練における開封者の半数超であった。そして、この45件の開封のうち通報は10件であった。「クリックしてからCSIRTへ通報」した者のうち、最も早かったものは7分後であった。最も望ましいクリックしていない状態での通報は12分が最速であった。手順外であり望ましいとは言えないが、メールによってCSIRTへ通報したものが3件あり、それぞれ14分後・15分後・48分後であった。

X社では訓練後において、クリックした者に対してクリックの理由について事後アンケートを実施しており、その結果についても確認したい。X社の意向により、具体的な回答数は伏せるが、クリックした理由については降順で以下の通りであった。

①送信者・件名・本文を確認したが、不審であるとは思わず、内容を確認する必要があったと思ったため
②クリックするつもりはなかったが、操作を誤ったため
③件名や本文が自身の職務や事務に関係するものであり、内容を確認する必要があると思ったため
④件名や本文に個人的な興味があったため
④訓練メールだと気が付いたため（上記と同数）
⑥送信者・件名・本文を確認しなかったため

(4) X社の事例についての考察

ここまでのX社の事例について、若干考察を加えたい。

X社では、URL本文埋め込み型による標的型メール攻撃訓練を実施しているが、その目的は以前より行われている教育による知識が実践できるかの確認にあると言える。それは、標的型メール攻撃が実存することを再認識し、それに遭遇した場合、特に当事者となった場合はLANケーブルを抜き報告することである。よって組織の情報セキュリティの備えをチェックするという試験的な意味合いがある。

その結果を測定する指標として用いられた第1のKPIである「クリック率」では、事業系の一般従業員では20%、事業系との比較においてはITリテラシーが高いと考えられる技術系の従業員が多いX[2]社においても5%程度のクリック率であった。これは、訓練を繰り返し、知識が身に着いていると考えられる人々でも4%程度は開封してしまうという先行研究と整合する結果であった。やはりこの程度のクリック率が訓練の最初の壁となると考えられる。第2のKPIである「報告数」に関連して、時間軸を加えた分析ではクリックした者の半数が、メールが届いてから1時間以内に開封・クリックしており、それらの者で最速の通報は7分後、クリックしないで疑念を持ち通報した者の最速は12分後であった。

また表14に示す、クリックした理由の「②クリックするつもりはなかったが、操作を誤ったため」、「⑥送信者・件名・本文を確認しなかったため」の2つについては主要な要因はヒューマンエラーである。特に②は攻撃であると認識できていたにもかかわらず、極めて単純な操作ミスによってインシデントにつながっている。そして、「①送信者・件名・本文を確認したが、不審であるとは思わず、内容を確認する必要があったと思ったため」、「③件名や本文が自身の職務や事務に関係するものであり、内容を確認する必要があると思ったため」、「④件名や本文に個人的な興味があったため」の3つは、攻撃側の詐術によりクリック行動を誘発されている。最多の回答である①の「送信者・件名・本文を確認した」が、「不審であるとは思わず」、「内容を確認する必要がある」と思わせるというように常に攻撃者側が防御者側を上回っており外的要因が大きいといえるのだが、それだけでなく②の「操作を誤った」というように攻撃を認識し、回避できる可能性があったなかでも誤ってクリックしてしまうことが加わるように、人が被害の起点となる可能性を大きくしている。

第I章で触れたように、標的型メール攻撃による被害は、外部者の悪意と内部者のエラーの複合により発生するものであり、本事例で確認したように人間のミスの余地も僅かだが確実に残っていると想定すれば、やはりクリックや添付ファイルの開封をゼロにすることはほぼ不可能であろう。であるならば、時間軸での分析が示すのは、適切な通報がCSIRTに寄せられれば、15分程度で全

表14：クリックの理由とその要因

	クリックの理由（降順・件数は秘匿）	主要要因
1	送信者・件名・本文を確認したが、不審であるとは思わず、内容を確認する必要があったと思ったため	詐術
2	クリックするつもりはなかったが、操作を誤ったため	ヒューマンエラー
3	件名や本文が自身の職務や事務に関係するものであり、内容を確認する必要があると思ったため	詐術
4	件名や本文に個人的な興味があったため	詐術
4	訓練メールだと気が付いたため（上記と同数）	
6	送信者・件名・本文を確認しなかったため	ヒューマンエラー

出典：筆者作成

社的な注意喚起を含めた初動が可能であるということだ。今後の訓練においては、この反応の速さを組織全体の健全性と考えるべきであろう。特に、クリックしない・添付ファイル未開封の状態での通報の速さが最たる目標となろう。

組織的な事故をいかに防ぐかという高信頼性組織の議論でも、素早いネガティブフィードバックこそエラーを乗り越えるカギであるという（Weick & Sutcliffe, 2007）。速やかなフィードバックそのものと、そのための正確なコミュニケーションの確立こそが、小さなエラーを不確実性の高い事象にまで発展させないための組織のレジリエンスの中核であるという。これに従えば、従業員の気づき・知らせる速さとともに、そのための通報手段をきちんと設計することも重要になる。

(5) X社の訓練の今後の課題と方向性

最後に、X社の訓練の今後の課題と方向性について付言したい。X社は、今後、他のグループ企業との経営統合を視野に入れた大規模な組織改編が予定されており、X社内に集積される顧客情報がより増えることで、ターゲットとしても魅力を増す。これに付随して、情報セキュリティの主管やインシデントハンドリングがどのような運用形態になるのかは不明ではあるが、営業拠点の数や管理するアカウントも数倍に膨れることが見込まれている。

こういった中で、X社はどのように訓練を展開していくべきであろうか。まず、①グループ全社の各社単位でのセキュリティ体制・セキュリティへの認識・IT リテラシーレベルなど把握していない他の地域の現状を知る必要がある。そしてなにより、演習は繰り返していくものとして②X社および X^2 社の状態の再確認として訓練を実施し、本節で取り扱った訓練との比較が必要であろう。そして、これをベースとして、③X社で実施してきた教育・訓練の適正さを確認し今後の活動の正

統性を得ること、そして④これを担ってきた CSIRT へのエンパワーメント獲得、の 4 点であろう。特に③と④について、今回の標的型メール攻撃訓練は、予算とシステムの問題から外部のコンサルタントに委託して、URL　埋め込み型で展開したという。そのため分析もコンサルタントが行っており、KPI そのものや事後のアンケート調査の報告書はコンサルタントが作成している。この点で、この報告書の質的な分析、事後の分析の余地がまだまだあるといえる。クリックした者の属性や、担当する業務の状況や前後に受診しているメールの内容といったクリック時の条件などもファクターとして捉え、事前の教育研修とミニテストに活かすことができると考える。このミニテストは、なにより 2 年間継続してきた事実があり、X 社にとって強い文化的要素として理解することができる。なぜなら X 社は、本社機能を除けば、営業拠点が比較的小規模であり広範に多数散在するという地理的条件があるが、それぞれの拠点にセキュリティの担当者・技術者を配置することは困難であるし、集合的な教育を分散して実施することもコストがかかるうえに、拠点側も人員が少数であることから送り出しにも難しさがある。この点で、ミニテストは有効な手段であり、継続すべき価値があると考える。実際の標的型メールを受信した際に『*これは訓練か？*』と CSIRT に問い合わせが複数寄せられるようになっているほどであり、リテラシー向上の効果が見受けられる。しかし、こういった事由も正確に記録として残しているわけではないため、ミニテストをベースとした教育研修の効果を数値化することは残念ながらできない。このような教育研修と訓練を継続的に実施、拡大しての実施に向けてはやはり予算獲得が必要であり、そのためには経営層の支援が必要である。そのためには「目標とする状態」の提示とそれに対するこれまでの「成果の見える化」が必要であり、こういったことも成果としてアピールすべき対象であるはずだ。これは、セキュリティ文化の醸成を、訓練を繰り返していくことを通じて、実務的にはマネジメントシステムのなかでこれを行っていくという現実の課題からも求められるはずである。

そしてもう 1 点、X 社での標的型メール攻撃訓練は、一般職層のみを対象としており経営層や管理職向けには訓練を実施していない。その理由について CSIRT の管理者は、表向きは『*繁忙であるため*』であるが、セキュリティポリシーに関連して、標的型メール攻撃訓練の目標は「開封率ゼロ」を標榜していることから、『*クリックすることは確実であり、部下の前でクリックしてしまうことがないように忖度していた*』と述べている。この点で、経営者層や管理職自らが体験していないため、ヒューマンエラーに対する理解と訓練に対する温度差があることが懸念される。この懸念をまず払拭するために経営者層や管理職層も訓練の対象として実施することが期待される。経営者層も訓練に「参加」していることは、セキュリティが上位の価値であることを示す一貫した振る舞

いであり、経営者層や管理職層が自らクリックし、CSIRT に報告しているという事実、そしてその姿もまた一つの象徴的なシーンであろう。それは、経営者層が訓練とそれを主導する CSIRT に対する一定のコミットメントを示すものとして、また、訓練そのものがセキュリティ文化のシンボルとして認識されることを可能にすると考えられるからだ。

最後に、全社的なセキュリティポリシーに関連するものであるが、前述のとおり、標的型メール攻撃訓練に関しては「開封率ゼロ」を掲げている。経営者層の決定事項である全社的なポリシーを撤回・転換することは ISO の実務として実組織ではなかなか困難な道程であると思われる。しかし、X 社の CSIRT の管理者は、『*これは私のマターである*』としてこの転換に意欲を示しており、経営者層の支援の下でクリック率・開封率から報告率への転換がなされることを期待したい。

2 Y 社の事例

本節では、前節で確認した X 社と対比的な例として Y 社の事例を取り上げる。調査は、2018 年 9 月に明治大学駿河台キャンパス内の演習室においてインタビュー調査を行い、資料の提供を受けた。

(1) 調査の概要

日時：2018 年 9 月 4 日午後 4 時より約 1 時間半

場所：明治大学駿河台キャンパス内演習室

インタビューイ：Y 社情報セキュリティ担当 E 氏（CSIRT メンバー）

Y 社は関東地方に本店所在地を定める、情報通信産業に属する企業である[82]。日本全国に 10 を超える拠点を置き、管理するアカウントは約 8,000 アカウントと企業規模は大規模である。情報通信産業であることからも情報セキュリティへの備えも早く、従来から SOC[83]が実装されていたが、これを対外的窓口の一元化と情報セキュリティにおける取り扱い範囲をサイバー事象についても明確化することを目的として 2015 年に CSIRT を設置した。標的型メール攻撃対応訓練は、この CSIRT が企画・実行している。標的型メール攻撃訓練はチームの実装当時から行われており、2015 年からである。訓練そのものは年 2 回を、半期ごとに 1 回のペースで行なっており、対象と

[82] 総務省の定める日本標準産業分類（平成 25 年 10 月改定）（平成 26 年 4 月 1 日施行）の大分類に基づく。

[83] Security Operation Center の略称。 情報システムを監視し、サイバーインシデントの検知や対策を主導する役割を担う組織体として企業組織に実装される。近年は機能のみをコンサルタントに外注することも多い。

なるアカウントは、正規職員だけではなく、派遣従業員・契約社員等のいわゆる非正規従業員を含めた約 8,000 アカウントの全数である。これまでの訓練の目的は開封率の低減であり、目標値は「開封率ゼロ」であった。

(2) 教育研修と訓練の概要

Y 社では訓練の実施に先立って、従業員であればだれでもアクセスできる社内イントラのポータルページに訓練実施期間を掲示し、注意喚起したうえで実施する。自社内に専用のサーバ 2 台を設置し、この 1 台より訓練用のワードファイルを添付したメールを送信する。訓練の実施から分析までトータルで 2 週間弱である。8,000 アカウントに対しての送信は 1 日かけて小分けにして送信する。これは、社内のセキュリティのシステムに、大量のデータの一斉送信ができない仕組みを実装していることによる。

添付されるワードファイルにはビーコン[84]が埋め込まれており、開封されるともう 1 台のサーバで開封した際に発信される信号を受信、記録する方法によって実施している。この受信側のサーバについては、4 日程度の運用となっている。これは、訓練対象者が休暇を取っていたり、休日を挟んだ翌営業日の出勤時のメールが溜まった状態からの開封を意図的に狙うこともあることによる。したがって Y 社での訓練は、この後にその理由は詳述するが「開封率」を KPI として実施している。

訓練メールに添付されているファイルを開封すると、その内容としてまず訓練である旨が表示され、標的型メール攻撃についての注意を促し、開封してしまった際にとるべき行動を示した上で、標的型メール攻撃に関する e-Learning サイトへ誘導する。添付ファイルを開封すると示される、Y 社における標的型メール攻撃に遭遇した際に求められる行動は、①上長への報告、②上長から自分の所属するセクションにおいて指名されているセキュリティマネージャー（仮称・後述）への報告である。この点で、Y 社における標的型メール攻撃訓練は、URL をクリック・添付ファイルを開封してしまった後の報告行動の実践を目的としてはいない。標的型メール攻撃がありえるということを認識し、さらなるセキュリティリテラシーの獲得を促すキッカケとして位置づけられるものである。

事前の教育について確認すると、全社教育として年に 1 回、受講期間を指定して e-Learning を活用した一般研修をおこなっている。一般研修であるため、あくまで PC 利用に関する全般的なリテ

[84] 利用者識別のためにデータ内に埋め込む識別情報。

ラシー向上を目的とした教育であり、セキュリティについてもそのうちの 1 項目として取り上げられてはいるが、標的型メール攻撃に特化したものではない。多くの e-Learning と同様に講座の末尾はテスト形式となっている。

Y 社において定められている、セキュリティインシデント全般に遭遇した際の情報エスカレーションは、①インシデントに遭遇した当人が上長に報告する。②上長は同時にみずからのセクションにおいて指名されているセキュリティマネージャー（仮称・後述）に報告する。③セキュリティマネージャーがその対応を規程や細則にのっとり実施する、というものである。インシデントの内容がサイバーなものであれば、セキュリティマネージャーにより CSIRT へと情報を繋ぐことになる。したがって、標的型メール攻撃であれば、①当該の URL をクリック・添付ファイルを開封してしまった者は、まず上長に報告する。②上長は、自分の所属するセクションにおいて指名されているセキュリティマネージャーに報告し、LAN ケーブルを抜く指示を受ける、②セキュリティマネージャーは、所定の処置（LAN ケーブルを抜く）を済ませた旨を CSIRT に報告をする、というものである。したがって、マルウェア等への感染が疑われる PC をネットワークから切り離す責任・主体は、セキュリティマネージャーである。

(3) セキュリティの体制

この、セキュリティマネージャー（仮称）とはどのような存在であるかについては、Y 社のセキュリティ体制について確認するなかで明らかにしたい。Y 社のセキュリティポリシーには「事業部の長は、事業部のセキュリティマターの責を負う」と明記されている。そのセキュリティマターがサイバーインシデントであるならば、Y 社には管理すべきアカウントがおよそ 8,000 アカウントあるが、Y 社にはおよそ 20 事業部があるため、このおよそ 20 名の事業部長がそれぞれおよそ 400 アカウントに対してセキュリティマターの責任を持つことになる。しかし、400 のアカウントを直接に管理することは困難であるため、規定において「事業部長は、実務を担う者としてセキュリティマネージャー（仮称）を指名する」と再委任されており、運用的には事業部長がセキュリティマネージャーを 3 名から 5 名程度指名している。このセキュリティマネージャーは、必ずしも技術的知識の高い人物が選任されているわけではない。個人の役職や担当としては、事業レベルのリスクマネジメントをその職掌とする人物が多いのが実際である。現実的には、各事業部内の企画部門の管理職レベルが指名されている。その理由は、事業部内の業務の仔細を把握しており、発生したセキュリティマターの事業に対するリスクを判断することが可能だからである。

そして、さらにこのセキュリティマネージャーが、自らのサポートとして実働する補助者としてセキュリティリーダー（仮称）[85]を5名程度指名している。よって、20×3×5=300名がY社のセキュリティのキーマンとなっており、なかでもこのセキュリティリーダーがインシデント発生時の第1の防波堤として活動することになる。

X社において発生するセキュリティインシデントは、第I章で確認したセキュリティインシデントの現状を支持するものである。最も多いのが社員証やPCの紛失というのが実際で、サイバーインシデントは一部である。この一部のサイバーインシデントの技術的なケアとサポートを担うのがCSIRTであり、現場の管理としてリスクマネジメントを任されているのが、事業部長をトップにセキュリティマネージャーを中核とした前述の300名のピラミッド構造となる。この組織構造をもって当該事業部において発生した情報セキュリティインシデントの早期解決を目指すこととなる。

CSIRTメンバーであるE氏からみたX社の従業員のリテラシーレベルの評価は、『*そもそもサイバーセキュリティは技術要素が広範多岐にわたるため、能力の高い技術者ですら、セキュリティの技術面においては、これを完璧に身に着けているというのは難しい*』というものである。一般従業員についても、企業規模が大きく多様な従業員がいるため、『*組織の中にはいろいろな人が居るため、マニュアルを配ってもそれすら興味関心・理解を示さないことがある*』また、『*現場で対応すると、（開封の罪悪感から：筆者加筆）パートナー社員に泣かれてしまったことがある。現場の現実としてはこんなのがザラなので、こういった人に機微の判断を頼むことは負担が大きく現実的でない。だから、「何かあったら言ってね」と言える人を配置する*』という意図により、セキュリティリーダーが分散配置されたこの体制となっているという。

そのため、このセキュリティマネージャーとセキュリティリーダーの約300名に対しては、全従業員を対象に実施している一般的なセキュリティリテラシーに関する研修と別に、現在のセキュリティ／サイバーインシデントのトレンドとその対応といった、セキュリティのコアとしてより高度なセキュリティに関する研修を実施している。

(4) 訓練の結果

Y社の直近の訓練の結果について確認する。Y社では訓練のKPIは添付ファイルの開封率に設定されているが、本稿では、この開封率を職層ごとに細分化して取り上げる。前節で確認したX社

[85] 本稿では、この実務的な補助者を「セキュリティリーダー」と呼称し、用いていく。

では、経営層・管理職層に対しては訓練を実施してなかったため、この対比として価値の高いデータであると考えるからである。

表 15 ：Y社の職層別にみる開封率

職位	開封率 A	開封率 B
上級管理職	8%	13%
中間管理職	7%	9%
一般職	6%	7%

（各職位の n 数については、Y 社の要望により秘匿）

出典：筆者作成

直近 2 回の訓練 A・B のうち、訓練 A では、上級管理職（役員を含む）は 8%、中間管理職では 7%、一般職では 6%であり、開封率は上位層に向けて僅かな上昇傾向がみられた。しかし訓練 B では上級管理職では 13%、中間管理職では 9%、一般職では 7%というように、上位層に向けて開封率の明確な上昇の傾斜があった（表 15）。この結果は、前節で確認した X 社のセキュリティの管理者が懸念していたように、上位の職層ほど標的型メール攻撃のターゲットにはうってつけであり、マルウェア等に感染したことによる被害の踏み台になる可能性が高いことを示している。

Y 社では、2015 年に実施した初回の訓練から調査日現在までで延べ 7 回の訓練を実施しているが、開封率については訓練を重ねたことによる学習として開封率が一貫して低下の傾向にあるというわけではない。これについては次で触れる。

(5)　Y社の事例についての考察

Y 社では、訓練の KPI は開封率においてあるもの、開封率そのものは訓練の直接の目的にはなっていない。過去 7 回の訓練について、開封率が低下傾向にあるわけではないことを述べたが、これも訓練に効果がないことを意味しているわけではない。その理由は、訓練ごとに件名・本文ともに趣を大きく変えていることにある。第 I 章で述べた通り、攻撃側の悪意と技術が上回る状況であり、件名や本文も進化している。Y 社 CSIRT はこれを意識して、件名や本文に工夫を凝らしている。むしろ、教育訓練への誘導として開封率を高めることについてインセンティブすらあるためであり、具体的には訓練であることの見極めの手掛かりを残しつつも、社内システムの更改といったような実際に社内で進行している具体的なイベントにタイトルや文章を絡ませるなど開封へと積極的に誘導している。

この開封率について、管理職の、とりわけ役職が上がるにつれて開封率が高いという結果が示されていたが、管理職であれば、例えば部下からの伺いや報告、経営者層から発信される管理職向けの情報共有というようにそもそも集まってくるメールの数が多いこと、その内容についても管理職の文字通り、組織内での職責に基づいたマネジメントの範疇として確認すべきものであるという認識になりやすく、そして多忙であることの複合した結果であろう。経営者層については、管理者層と同様の理由とともに、セキュリティへの認識の程度の問題があるのではないかと考えられる。ハード的対策への投資は、営む事業の内容から許容しやすいが、ソフト的対策についてはやはり経営者としての費用対効果の意識は強いものとなろう。またオペレーションの現場からは遠く、自らが情報端末とネットワークの参加者、すなわち当事者であるという意識はより持ちにくいのではないだろうか。こういった点で、上位の職層であればあるほど多忙であり、また組織の対外的な交流活動が多く、外部からの儀礼的な挨拶メールなどへの対応も職責として求められることから、教育研修と訓練の強化を含めた対策が求められるのはまさに上位職層だと言える。

Y社の教育と訓練における目的に関して、個々人の情報セキュリティに対する認識を高めるという目的は叶いつつも、最終的に求める報告の行為については不安がある。ビーコンの受信サーバにて添付ファイルの開封の有無はとれている。しかし、開封理由などの追跡調査はしていない。したがって、開封と報告の差分なども CSIRT として把握はしていない。そして、この訓練は教育へのキッカケとしての位置づけであり、開封時に訓練であることが表示されるため、「抜線の指示を受ける」という行為の有無についても確認はとれていない点だ。ただ、時々、訓練であることを認識しない開封者がセキュリティマネージャーに開封の報告し、訓練と実践の区別がつかないまま情報システム部門の担当者に「処置済み」の報告を入れることで、CSIRT による調査の対象となることがある。むしろこれは、正しいエスカレーションルールに則り、求められている行動ができており、体制が機能していることの左証であろう。

また、セキュリティリーダーらに対しても、訓練の前提として彼らに行っている集合的な教育によって身に着けた知識の発露を期待している。これと同時に、訓練に際しては普段通りに振舞うことを求めている。よって、予告によって訓練が行われていることを認識しているリーダーが「訓練が行われているので注意するように」というようにそれぞれの職場において注意喚起することを禁じているわけでもない。この点では、訓練の KPI である開封率が有効数として機能するかには疑問が残るが、メール攻撃があり得るという認識を持たせるこという訓練の主目的は達成できていると評価できよう。

セキュリティ体制については、管理するアカウントが先のX社との比較では4倍であるが、組織がより大きくなり管理するアカウントが増えるといった表面的な問題への対処というだけでなく、これは責任単位の明確化とともにメンバーの多様性の増加への対応という視点があると考えられる。組織体が大きくなれば人の異動も増加する。これに並行して多様化するメンバーに対して、徹底して統一的な教育を行うことはもちろん不可能ではないが、組織にとっても個人にとっても、時間、費用ともに多大なコストとなるのは明白である。Y社の訓練は、教育への誘導という位置づけられるが、訓練をきっかけとした情報セキュリティとセキュリティ体制への認識を持つ良い機会として機能している。責任単位の明確化は、責任者からはスパンオブコントロールの明確化であり、責任単位内に実働者としてセキュリティリーダーを分散配置することでセキュリティ活動の把握が容易になる。一方の責任単位のメンバーにとっても自らが所属するセキュリティ体制の全容が小さくなることで、セキュリティ体制との距離感が近く、メンバーの情報セキュリティに対する当事者性を向上させることが期待できると考える。また、報告ルートの明確化でもあり、これらが相まってより早い対応につながることも期待できる。

(6) Y社の訓練の今後の課題と方向性

調査日現在のY社では、「開封率の最小化と報告の全数化」が訓練実施の目的として標榜されることとなっており、訓練のKPIを「報告率」へと転換を企図している。さらに本事例の翌年度については、4半期ごとに1回の年4回を、翌々年度からは月1回程度の実施を計画している。その目的は、『訓練の常態化による緊張感の維持』にあるという。今後は、現在行っている訓練期間の予告を行わずに訓練を実施し、「報告行動の徹底」の目的の下に添付ファイルを開封した時に訓練である旨の表示もせず、開封率と報告率の2つがKPIとなるということである。

これについては、以下のような点が課題となると考えられる。

これまで通りの「開封率」の低減は、引き続き標的型メール攻撃の認知を高めるという取り組みになるだろう。そして新たに加わる「報告率」の向上のためにまず、報告行動の前提となる知識と認識の獲得のために、教育研修において報告方法と報告先の周知の徹底を図るというように、標的型メール攻撃に関するコンテンツの割合の増加が必要になる。この点についてはe-Learningに動画コンテンツの実装で対応を検討しているという。ただし、開封数と報告数の差分が訓練のターゲットとなる以上、そのフォローとして未報告者に対するアンケートや聞き取りといった調査が必要であり、マンパワーが必要となる。また、この差分の集計にも課題がある。すなわち連絡網と受付の体制の整備が課題となる。現在は、訓練であれ、本番であれ、最終的にはCSIRTへの報告がなされ

る。Y 社ではこの担当者は数名であるという。仮に開封率を 15%とした場合、1000 件超の報告が寄せられることになる。報告数を KPI に置き、報告を求める以上はすべて受け付ける必要があり、平時の業務を通常通り行いながらの負担度は高く、本質的にはプライオリティの高い本番の報告とその対処が滞る可能性も含む。さりとて、報告の実感が伴わないものは、報告行動の満足感につながらず、今後の報告行動の意欲の妨げとなりかねないことから、報告方法を含めて検討が必要であろう。

3 Z社の事例

本節では、非常に高い頻度で標的型メール攻撃訓練を実施しており、データが蓄積されているZ社を取り上げる。調査は、2018年11月および2019年2月に明治大学駿河台キャンパス内の演習室においてインタビュー調査を行い、資料の提供を受けた。

(1) 概要

インタビューの概要は以下の通りである。

日時①：2018年11月15日午後3時からおよそ2時間

日時②：2019年2月5日午前10時よりおよそ1時間半

場所：明治大学構内演習室にて実施

インタビューイ：Z社情報セキュリティ担当F氏（CSIRTメンバー）

Z社は、関東地方に本店所在地を定める、サービス業に分類される企業である[86]。営む事業はほぼ単一であるが、地理的には日本国内各地に分散しており、海外の拠点もいくつか保有している。中核となる事業では、大量の個人情報・クライアント企業の営業秘密・個人の生年月日などに連動するような期限に厳密な成果物を扱っており、保有・利用する情報資産の価値とこれに対するセキュリティへの意識は非常に高いといえる。

(2) 現在の教育研修と訓練の概要

Z社での訓練は、2013年を初回として毎月1回のペースで訓練を実施しており、2018年11月現在で延べ30回を数えている。訓練対象のアカウントは、正規従業員のみならず、契約社員・アルバイト、派遣従業員、事業所内請負作業者などを含めたおよそ7,000の国内アカウントと海外の拠点に付与するおよそ1,000アカウントの合計およそ8,000アカウントである。対象となるアカウント数そのものは前節で確認したY社とほぼ同数である。

訓練の主管部署は、全社的な情報セキュリティに関連する委員会（以下「セキュリティ委員会」）の下部に、仮想組織として実装されているCSIRTである。メンバー13名（うち3名が専任）であるが、情報システム系だけでなく、CSR（Corporate Social Responsibility）やリスクマネジメントの担当者なども参加している。Z社のCSIRTは、インシデントハンドリングを中心とするが、それ

[86] 総務省の定める日本標準産業分類（平成25年10月改定）（平成26年4月1日施行）に基づく。

にとどまらず全社的なセキュリティ戦略を立案する役割を担う。そして、CSIRT の立案する戦略の実践・実行・兵站を情報システム部門が担うという分担になっている。

訓練そのものは、この CSIRT が企画・立案・実行までを担っている。実在するドメインと酷似したドメインを訓練用に取得し、外部のレンタルサーバを借り、開封時にビーコンが飛ぶようにプログラムしたワードファイルを添付したメールを送信する形式で行われている。海外にも事業所があり、現地採用の従業員も多数在籍するため、中国語・英語での訓練メールも作成して実施している。そして発信されたビーコンを受信し集計する。Z 社にはクライアントの代理としてメールを大量に送信するサービスがあることから、流通するメールの数量制限は設けられておらず、全アカウントに向けて一斉に送信することができる。しかしながら、この訓練を全アカウントに対して一斉に送信する方法で実施すると、受信から開封までもおよそ同時期になり、受信側（被訓練者）である現場でちょっとした騒ぎになり、訓練を実施していることが広範に伝わってしまい、訓練の意味がなくなってしまうという失敗を経験した。よって現在では、アカウントをランダムに抽出し、間欠的に送信するシステムを Z 社内にて開発して利用している。

添付されているドキュメントファイルを開封すると、まず冒頭に訓練メールである旨と、サッカーのレフェリーが用いるレッドカードを意識したイラストが表示される。そして、標的型メール攻撃を受けた場合に報告を行うためのフォーマットがその下部に続く。開封してしまったものは、このフォーマットを埋めた上で、あらかじめ定められた報告先に提出を行うことが求められている。Z 社ではこれを報告としてカウントしている。したがって、Z 社での標的型メール攻撃訓練において設定される KPI は、開封率と開封したことの報告率の 2 つである。

(3) 訓練の概要

Z 社では毎月 1 回を標準として実施しており、その流れは次のようになっている。

①CSIRT が訓練の予告・教育資料を配布

②ブロック内での展開・教育の実施

③CSIRT が訓練メール送信

④CSIRT が URL のクリック・添付ファイルの開封の集計

⑤ブロック内事務局での開封通報受付・CSIRT へ回送

⑥CSIRT が集計値の速報を公表

⑦CSIRT から、開封した者と開封したにもかかわらず未通報であった者をブロック事務局に通知

⑧ブロック内での共有・未通報者の再教育・事後アンケート

⑨CSIRT がアンケート回収・未通報者の分析

これらの作業を 1 か月でこなしており、多様なタスクを非常に高速なサイクルで回しているといえる。まず、教育については、CSIRT が教育資料として e-Learning コンテンツと手元資料としてのプレゼンテーションスライドを作成している。内容は、他社事例から始まり、攻撃のタイプやその対策、そして攻撃メールに遭遇した場合の対処、クリック・開封してしまった場合の振る舞いについて説明しており、プレゼンテーションスライドにして 30 枚近いものである。当初は IPA の公開資料を基に作成されていたが、月に 1 回の実施にもかかわらず毎回資料の改定を行ない、訓練の回を重ねる中でここまでのボリュームとして至ったという。

しかしながら、ここまで入念な資料の作り込みの一方で CSIRT は教育を主導しない。作成された教育資料をどのように利用するかは、ブロック責任者と事務局に一任されている。そのため CSIRT は、資料の改訂された個所とそのポイントを案内し、最低限の教育範囲として示すことで、各ブロックが教育の省力化を希望する場合にはそれに応えることができるように努めている。そして、訓練の KPI は開封率と報告率に設定されていることから、中心となる教育内容は報告の行動についてであるが、教育資料によって示される振る舞いは、①LAN ケーブルを抜く、②PC の使用を中止する、③自分の所属するブロックのセキュリティ責任者もしくは所属長に通報する、という 3 段階のものである。まずは、X 社・Y 社でもあったように PC に接続されている LAN ケーブルの物理的対処である。Z 社では X 社と同様に PC 利用者個人が LAN ケーブルを抜くこととされている。そして、PC の使用中止については、マルウェア等への感染が疑われる動作の時点でのメモリの状態を保存し、分析と対処に活用する目的から、他の操作を行うことや電源そのものを切ることを禁止している[87]。そして、通報・報告の行動であるが、報告先となるセキュリティ責任者とブロックについては、次節において確認する。

(4) セキュリティ体制

Z 社では、全社的なセキュリティ体制についてブロック体制を敷いている。規定として、全社単位のセキュリティ委員会の事務局長が各ブロックに対して体制整備の指示を発し、これに従ってブ

[87] 最新の研究では、自らが感染した PC が外部との通信経路を遮断されたことを感知すると、自らの存在を検出できないように振舞うマルウェアも発見されているため、抜線の行為については賛否があるが、ここでは議論しない。

ロック単位の体制が構築されている。実務的には日本国内を約 25 ブロックに分割（本社内も数ブロックに分割）し、それぞれのブロックにセキュリティ責任者を置く。Z 社内の事業部とほぼ同じイメージであり、事業部長がセキュリティ責任者を兼任することも少なくない。そして、全社的なセキュリティ委員会の下部組織として、このセキュリティ責任者を長とするブロック単位のセキュリティ委員会が置かれており、この責任者の下に 3～5 名程度のセキュリティ担当者が任命され委員となっている。ブロック内の IT 関連機器の把握・管理などを担っており、この委員会の中には別途に事務局が設置され、訓練に関する実務も担っている。ここまでの責任者および事務局として実務を担うこれらの人は、個人の本来業務とは離れた無報酬のメンバーである。この担当者として任命される者の属性は、必ずしも情報システムに関連する業務を担当する者（いわゆる理系の人物）ではなく、総務や経理といった文系畑も含めて多様ではあるが、IT リテラシーが高いと評価される人物が指名されているという。前節で確認した、開封した者に求められる振る舞いの 3 つ目における報告先は、このセキュリティ担当者と事務局になる。

(5)　訓練の結果

Z 社は訓練をこれまでにおよそ 30 回繰り返している。これまでの訓練の初回の訓練は英文による URL 埋め込み型で行っており、クリックするとリンク先のページに訓練である旨が表示される。このページへのアクセス数をカウントしており、結果としてクリック率はおよそ 30%というものであった。これから数回のうちはこの形式で実施され結果が集計されているが、メールの件名や文面によってクリック率が上下した。訓練を重ねることでクリック率が一貫して低下するという期待が外れ、上下に変動する結果を鑑みて、訓練を企図している CSIRT 内で『*クリック率はゼロにはならないのではという議論が起きた*』という。さらに、訓練を全社一斉にではなく、数ブロックずつ日をずらして実施したところ、後半に実施したブロックの開封率が一貫して低下するという結果も確認されていた。訓練内容が漏れ伝わってしまい訓練の目的に適っていないこと、そして訓練の KPI をクリック率としていることについて議論を深め、クリックしたことの「報告率」を KPI に加えることとなった。そして報告の計測方法について検討し、添付ファイルをドキュメント形式にするのであればそのまま印刷できる点に着目し、添付ファイル内で訓練であることの表示と、報告のためのフォームとして実装することが議論された。これにより、訓練前の教育から訓練後の報告までの一貫した、現在の形式の原型ともいえる形が生まれ、初回の訓練からおよそ半年後の訓練においてメール本文を日本語としたドキュメントファイル添付型へと転換した。転換後の初回の訓練

における報告率は 50%であった。この頃から開封率が低下し 5%前後で推移を始め、一方の報告率も漸増していった。

開封率の低下と報告率の上昇はという結果は、一見すると非常に望ましいように見える。しかし、訓練の狙いは報告行動の定着にあり、開封率の低下は報告行動には結び付かないということを意味する。ここで CSIRT は、訓練における大目標である報告行動を経験してもらうことを意図し、その前段となる開封率を高めるため、メールの件名と本文に工夫を凝らした。結果として開封率は 10%を超えた。そして同時に報告率も約 85%に到達した。それ以後、開封率は低減、報告率は同水準をキープしていた。

しかし、ドキュメントファイル添付型に転換してから 1 年を経過した頃、開封率は低水準を維持する一方で、報告率が訓練初回の 50%に近付くほどの下落傾向を見せる。ここで CSIRT は、この理由を確認すべく訓練後のアンケートに踏み切った。事前の教育無し、訓練予告なしという、現状把握のための実験的事例としての X 社の例でもあったように、報告しなかった理由について「どこに（誰に）報告したらよいか分からなかった」という回答が散見された。この結果を受け、報告先の周知の徹底に取り組みを行う。結果、ここから半年かけて報告率は上昇、開封率 10%超に対して、報告率がおよそ 98%という過去最高を記録するに至っている。

これ以降については、開封率は、訓練内容によって 1%から 5%程度であり、直近半年間だけをみれば移管した低減傾向を示しており、そして報告率は 90%前後で定位している。しかし、逆の見方をすれば、10%前後は未報告である。開封率が低減しているため絶対数としては僅かな件数ではあるが、報告率は 100%の達成に至ったことがないのだ。

また、開封者ごとの開封回数については、1 回にとどまる者が開封経験者の約 75%と大半であるが、複数回開封した者では 2 回がおよそ 20%、4 回以上が 1%という集計となっている。

(6)　訓練結果の追跡調査と改善

訓練の概要で確認したように、Z 社の CSIRT は、未通報者のリストアップとブロックへの通知によって再教育を促している。これに加えて、前項でも確認したように未報告者へのアンケート調査を実施している。そこで収集された理由の詳細については、「①報告先がわからなかったから」、「②添付ファイルの開封途中でキャンセルしたから」、「③通報することを忘れたから」、「④開封していない（本人の主観）」というように大別できるものであった。

前項で触れたように、まず「①報告先がわからなかったから」への対策として、通報先の認知の徹底を図るべく社員 ID カードを保持するためのカードケースに同封できるようなカードを配布し

た。このカードの特徴は、報告先については本人に記載させるために白抜きの状態の白紙で配布したことである。所属ブロックの責任者名と個人単位で通報先を定められているブロック事務局の担当者名について、これをあらかじめ記載されたものを配布するのではなく、自らが報告先を調べ、記入するという行為を通じて認識し、定着することを意図したのだ。これにより報告率が大幅に高まったのは先述のとおりである。

「②添付ファイルの開封途中でキャンセルしたから」は、被訓練者の思い込みに基づくものである。マイクロソフト®社のワード®というワードプロセッサアプリの固有の特徴として、アプリケーション立ち上げの画面の隅に、キャンセルボタンが配置されている。添付ファイルの開封途中に標的型メールであることに気づいた者が、このキャンセルボタンを押したことで、ワードファイルが展開された画面の表示にまで至らず、本番であれば感染には至らなかったという思い込みによるものであった。実際には、画面上に表示されなかったというだけで、ファイルとプロクラムの読み込みは進んでおり、仕込まれたマルウェア等への感染も完了している。そのため報告が必要な事例なのだ。これは、このアプリケーション固有の特徴によるものであるが、CSIRT の分析によって判明したもたらされたものである。CSIRT は、このキャンセルの事例については、教育研修資料に反映された。

さらに、Z 社 CSIRT は、前節で確認した、開封経験者のうちおよそ 1%とごく僅かではあるが多数回開封者の特徴を捉えるためにその行動をユニークな方法によって追跡調査している。電子メールは文字情報であることから、CSIRT はその視線に着目し、多数回開封者のメーラー（メール送受信のアプリケーション）の立ち上げから、受信ボックスの展開、メールの選別、メールの開封までの行動について調査したのである。

その結果として、開封しない者との対比では、まずメールの受信ボックスの展開時から視線はほぼ移動せず、機械的に開封作業に移ることが判明している。また、展開された後のメールの一覧に対しても、開封しない者は、件名、発信元、そして発信された時刻を逐次確認したうえでメールを開封していくのに対し、連続回開封者の視線はほぼ移動せず、個々のメールへの開封作業へと移っていく。そして、開かれたメールに対する操作における視線も、未開封者は宛名、発信元、書き出し、文末の署名まで確認するのに対し、複数回開封者は、宛名、あいさつ文、本題の書き出しまで来た時点で添付ファイルの開封に移ることが確認できた。この調査の成果については、実際の視線の動きを例示しながらメール本文の全体にわたって確認が必要であることが現在の教育研修の資料に盛り込まれている。

(7)　Z社の事例についての考察

ここまで見てきたように、Z社の標的型メール攻撃訓練は、Z社での教育研修と訓練は、標的型メール攻撃であることを「見抜く」能力の育成よりも「通報する」という振る舞いを重視している。仕掛けとして、開封した添付ファイルはそのまま報告のフォームとなり、それを用いて報告することそのものを体験するところまでが一貫している。なによりも「報告のしやすさ」によって報告行動を後押しする重要な点でもある。

開封率については、訓練そのものが添付ファイル内の報告書によって報告することを経験してもらうことも目的に含まれるため、訓練を企画するCSIRTメンバーは時節柄にあわせたテーマを練り、件名と本文とに工夫を凝らすことで開封を促していることもあり、一貫した低減傾向にはない。一瞥では訓練の成果に疑問符が付くかもしれないが、報告行動を経験させ促すためには合理的な結果と言えよう。

Z社の標的型メール攻撃訓練においては、開封してしまったときに具体的には、抜線、使用中止、報告という3つの振る舞いが求められている。これらを訓練ではなく実際の攻撃メールが届き、開封してしまった時に自然の振る舞いとして表出することを期待し、1か月に1回という驚異的なサイクルで演習を繰り返しているのだ。その直接的な結果として、実際の標的型メール攻撃、いわゆる「実弾」についても日当たりで5件程度がシステムをくぐり抜け着弾するが、開封せずに疑わしいものとして報告が上がっているという。月に1度というペースで実施されることで、情報セキュリティ分野において組織に必須の対応の第1位として挙げられていた標的型メール攻撃への備えが、知識レベルと行動レベルにおいて確実に獲得され、定着しているといえよう。

この驚異的サイクルを支えている仕組みの特徴的な点は、Z社のブロックごとに設置されている事務局である。報告の受付はCSIRTが行う企業もあるが、訓練対象のアカウントが多数であると、ランダムに間欠的に送信していたとしても、報告率が高い状態で推移している望ましい状況においては報告が集中し受付側がパンクしたり、正しい集計とならない可能性がある。これを補完するためZ社では、報告の受付と集計はブロックごとの事務局が行っている。ブロックごとに責任者を置き、その実働となる担当者を配置するところまでは、Y社の体制と同様である。Z社はこれに事務局を実装している点が異なる点である。訓練が高速サイクルで機能しているのはこの事務局が担うところが大きいといえる。

また、訓練の概要で確認したように、教育研修の資料を作成するのはCSIRTであるが、実際の教育研修に責任を持つのはセキュリティ責任者と事務局である。ブロックごとの業務の繁忙や折々

の実務上の制約などを勘案して、教育をどのように行うか、訓練ごとに改定される資料をどう用いるかは任されている。裏を返せばブロック独自に展開ができるということであるが、これは、「過度に管理しない」という Deal & Kennedy（1982）による文化変革の要件の 1 つをまさに満たすものであり、この自由度が Z 社の文化的要素の強みになっていると考えられる。

教育訓練を独自に展開することができることが利点となる理由は、ブロックごとに訓練の結果を競っているかのような状態が自然と生まれていることによる。報告率については、ブロックごとの集計を CSIRT が集約し、一覧として全社のセキュリティ委員会に報告されている。公式に競争として銘を打ったことはないが、訓練結果に対して役員の注目も集まることで、結果としてブロック間で競争意識が生まれ、責任者と事務局の訓練に対するモチベーションが上がり、さらには高頻度による事務の繁忙からの嫌気や飽きを低減させるという効果につながっていると考えられるのだ。

現時点において、事務局内の事務作業は、現業では実務を抱えているボランティアによって行われている。これについてインタビューイである F 氏は、業務をお願いする立場から*『無報酬であることは一つの懸念事項』*と述べてはいる。しかし、結果に対する役員の注目そのものも含め、当人たちが一種のゲームとして捉え、自ブロックの結果に一喜一憂することで、教育をより良くする強い動機が生まれ、さらにその効果が表れる訓練を自分事として認識し、楽しんでいることが内的報酬となっていると考えられ、これも Z 社の訓練が高速のサイクルを維持できている理由の主たるもののひとつであると考える。

Ⅶ　総合的考察

本章では、前章において確認した3社の事例とそれに基づく考察を、第Ⅴ章で導出された課題に沿って再度整理し、結論を提示したい。そのため、まず各社の訓練の結果を整理しながら、KPIの設定とその用いられ方について訓練の目的が類似するＸ社とＹ社の比較を中心に再確認する。次に、訓練実施の体制に着目し、訓練対象アカウントがともに約8,000である点で規模的に類似しているＹ社とＺ社について比較を行いながら、特に訓練頻度が突出するＺ社の特徴を再整理する。

そして、Ｚ社の事例をもとに、文化の醸成や文化の変革において求められていた要件や要素はどのように充足されていたか、そしてそれらの他にも備えるべき要件や要素を「当事者性」の視点から確認する。

最後に、文化とはメンバーの認識や内心の問題であるという文化の経営学的定義において、セキュリティ・ファーストを旨とするセキュリティ文化は企業文化たりえるのかを、小規模ではあるがＺ社のメンバーに対して行った構造化したインタビューによるデータを元に確認する。そして、セキュリティ・ファーストな振る舞いを導出する企業文化を醸成するためにはどのようなマネジメントの努力が必要であるかを結論としてまとめる。

1 KPIについての考察１：Ｘ社とＹ社の比較を通した考察の整理から

3社の通した事例の比較と考察の整理の前提として、各社の標的型メール攻撃訓練の概要は次の通りである。

表16：各社の訓練概要比較

	訓練対象	KPI	訓練頻度	目標／目的	抜線の主体	基本的な教育	教育の頻度
Ｘ社	2,000	クリック率・報告率	(初回)	定められた行動の実践／試験的	本人	ミニテスト	－
Ｙ社	8,000	開封率	年2回	リテラシー向上／試験的（教育的）	SM(1	e-Learning	－
Ｚ社	8,000	報告率	月1回	定められた行動の実践／定着	本人	集合研修	月1回

(1：セキュリティマネージャー

出典：筆者作成

まず、訓練の目的について、標的型メール攻撃訓練によって組織メンバーの情報セキュリティへの認識や状態を確認するといった面があるＸ社とＹ社、訓練の繰り返しによって振る舞いの定着を図ることが明確な目的となっているＺ社という大別ができる。そしてこれは、訓練頻度にも違いが表れているといえる。そこでまず、訓練の目的が類似であるＸ社とＹ社について比較整理をおこないながら要点を整理していく。

Ｘ社とＹ社を比べると、単純に企業規模に見立てても約４倍の開きがある。そして、大量の個人情報を業として扱うＸ社と、情報通信産業を担うＹ社での情報セキュリティの位置づけも異なっているため、これを同列に扱うことはもちろんできないが、訓練実施の目的が組織の情報セキュリティの備えの状況をチェックする意味を持つことは共通していることから、この２社の標的型メール攻撃訓練とその前提となる教育研修、そしてセキュリティの体制についての要件を確認する。

まず訓練の目的について、Ｘ社では、ミニテストを２年間繰り返すことによって知識の定着を図り、その発露の程度を確認するというものであった。Ｙ社では、年に１回の e-Learning の受講機会の提供と半期に１度のペースでの訓練の実施し、教育・訓練のいずれも標的型メール攻撃と遭遇した際の行動の理解を深めてもらうというものであった。これによって訓練の目標については、Ｘ社では①標的型メール攻撃があり得ることを実体験し、セキュリティへの意識を持たせる、②早期に適切な対処をするために速やかな報告行動を実践する、という２段構造になっている。このため訓練の KPI は、その実施が外注化されているということもありメール本文に埋め込まれた URL の「クリック率」と「報告率」の２本立てとなる。Ｙ社では、①標的型メール攻撃があり得ることを認識させる、②e-Learning へと誘導し、具体的対処を再確認させる、という目標を持っている。このため訓練実施の KPI は「開封率」となっている。

クリック率・開封率という KPI については、今回の事例となった訓練では、Ｘ社の事業系に属する従業員で 20%、情報技術系で 5%であり、Ｙ社では一般職レベルでは直近２回の訓練において 6%・7%というものであった。Ｘ社の情報技術系従業員と、情報通信企業であるＹ社の従業員が同程度の開封率であったことは、もとよりセキュリティへの意識があり、セキュリティへの親和性が高そうな技術系であっても標的型メール攻撃があった場合には開封は避けられないことを端的に示しているだろう。Ｘ社の例でも３件あったように標的型メール攻撃であると認知した時点での通報が最善手として望まれるが、教育によって送信元や件名のみから本物の標的型メール攻撃であることを見抜く力を強化しようとしても限界がある。だとすれば、クリックしてしまったら／開封してしまったら「報告する」という、次善の振る舞いを求めることが現実的である。

この「報告する」という振る舞いに付随する振る舞いとして、X社では個人がLANケーブルを抜くことが求められているが、Y社では求められていない（報告によってセキュリティマネージャーに指示を仰ぐ）という違いが目立った差異となる。これについて、Y社E氏の言を借りるならば*『「自らが消火訓練に参加しているという実感」なのか「まずは報告して専門家の指示を仰げ」なのかであれば、後者の位置づけ』*と述べていたが、これに沿えばX社の訓練の位置づけは前者となろう。

この違いは、訓練対象者の規模と事業運営の地理的な問題を含めたセキュリティ体制の違いにある。X社は事業が一元的でありアカウント数が2,000と比較として少数だが、各事業所が分散し小規模であることから、これを組織化するよりは個々人がまず当事者としてセキュリティに対する責任を果たしてもらうことが結果として選択されている（最終的な処置と安全の判断は専門家であるCSIRTが行うが）。これに対してY社は、多数の事業部から成り、アカウント数は8,000と比較として大規模であるが、地理的に集約されている。組織内のセキュリティを事業部単位で枠組みし、事業部長を頂点としてセキュリティマネージャーを任命し、さらに現場での実務者としてセキュリティリーダーを任命するという平時のセキュリティ体制を構築し、そして彼らに対して特別の教育を行うことは、Spitzner（2014）が意図したアンバサダー制度の具体的な実装例であり、さらなる拡大版といえるだろう。日常において相談し、何かあれば指示を仰ぐことができる同僚が身近に存在することは、メンバーにとって非常に心強く、またセキュリティリーダーに行う付加的な教育を通してセキュリティリーダーがセキュリティ情報の発信者となり、また振る舞いの手本となることは、O'Reilly（1989）が示した文化醸成の要素である「他者からの情報」の強化にほかならない。

「クリック率」「開封率」というKPIを標的型メール攻撃訓練に用いることについての結論として、この両社のように訓練の目的が事前の教育内容の理解・定着度合いの確認や、追加的教育へ誘導にある場合、もしくは訓練の頻度を上げることができない場合で、Reason（1997）が平時における情報収集というような、組織の状態を確認する目的においてはKPIを「開封率」とすることはなんら問題ないだろう。しかし、メールを送信元や件名から見極め、開封を避けることを組織メンバーの目標とし、その程度の測定として開封率をKPIに設定すること、そして目標値をゼロとすることは、これまで確認してきた事例に基づけば不可能であり意味は薄いと考えるべきである。訓練の実施者やこれを指示する管理職、そして経営者層はヒューマンエラーに対する認識を改めるとともに訓練の目標を再検討する必要があるだろう。

この、訓練の目標と KPI の設定との関係においては、Y 社 CSIRT メンバーである E 氏による『*「自らが消火訓練に参加しているという実感」なのか「まずは報告して専門家の指示を仰げ」なのかであれば、後者の位置づけ*』という説明は、ある示唆であると捉える。この発言は、メンバーの背景の多様さから、全員に高いレベルの当事者意識を持ってもらうことは難しいという判断から導かれていたわけであるが、これがカギとなっていくと考えられる。これは、当事者性をあえて求めないという選択であるが、これを逆から読めば訓練によって積極的な当事者性を高めるためには、前者を重視していくことが近道であり、組織の情報セキュリティへの当事者性の向上に寄与する、すべてのメンバーに内心として共有されるためには、報告を KPI として、報告という振る舞いの意味を一段上げる必要があるということだと理解できるからである。

では、次段階の KPI として「報告」を採用することについて、訓練の実行体制からこれを検討すると、先述のセキュリティ体制のピラミッド構造が整備されていたとしても、報告を受け付ける機能に量的・質的な制限があれば、そして訓練の対象であるアカウント数が増えれば増えるほど報告経路の問題が出てくる。これは、Y 社での将来的な訓練の展開においても懸念される事項であった。この報告受付の機能の実装という実務的な課題は、報告を振る舞いとして定着させるためには訓練を繰り返す必要があると考えるが、そのために訓練の頻度を上げることを企図するのであればなおさら大きな課題となる。

次節では、この課題を整理するために、訓練対象アカウント数が 8,000 と Y 社と同規模でありながら、訓練を毎月 1 回のペースで続けている Z 社の訓練内容とその体制について再整理する。

2 KPI についての考察２：Z 社の事例の考察の整理から

「報告」という振る舞いの定着を目標として標的型メール攻撃訓練を繰り返している Z 社であるが、調査日現在においてほぼ毎月 1 回のペースで訓練を実施している。当然に「報告率」が訓練の KPI となる。開封率はデータ収集されているが、開封者・未報告者の追跡のための参考資料であり、この低減を目指すよりもむしろ開封・報告を経験することが重要であると考えていることからも KPI となっていない。

「報告させる訓練」という前提のため、訓練メールに添付されたファイルが開封されるとそのまま報告フォームとなる。添付ファイルを開封してしまった者は、そのまま表示されたフォームを用いて報告を行うのだが、これも報告を促進するための「報告のしやすさ」を補完する仕掛けとして重要な機能だといえる。

この機能の効果を阻害する問題が、報告集中による報告先のボトルネックの問題と、これとは真逆の性質である「誰に」報告したらよいかわからないという問題である。前者のボトルネックについては、報告の経路とそれを受ける側のキャパシティの問題であり先の２つの企業事例での懸念事項であった。後者である報告したくても「誰に」、「どのように」報告したらよいのかわからないというのは訓練の価値を棄損する最大の問題であり、これが解決されないと本質的に「報告率」を訓練の KPI にすることはできないということを意味している。

このように、誰に報告するのかをいかに浸透させるのかも実務的な課題である。訓練の前提となる教育の問題でもあるが、企業が行わなければならない教育は、情報セキュリティに関連したものだけではないのはもとより、情報セキュリティに関したものも情報リテラシー教育全般の一部であるというのが現実である。開封したにもかかわらず報告しなかった者に対しての追跡調査によってこの問題が存在することを明らかにし、その解決として報告を「誰に」するのか明確化を図るべくメンバー全員に配布したのが Z 社のカードであり、個人レベルで報告の担当者が決定されている。これにより「報告率」を訓練の KPI に据え訓練を実施する諸条件が整ったと言える。訓練の KPI を「報告率」とするためにはここまでを諸条件として整える必要があるということだ。

この担当者とはもちろん訓練の報告受付のみを担っているわけではない。次節で詳述するが、日常業務における情報セキュリティに関する相談を受けるアドバイザーとなっている。これが、振る舞いの身近な参照点として、そして情報セキュリティのキーパーソンとして機能しているのだ。そして、この担当者をブロック単位で束にしたものが事務局である。事業部をおおよその単位としてその長をセキュリティの責任者に任じ、これが数名の実務担当者に再委任され、さらにこの実務的な担当者が数名の補助者を擁することでピラミッド構造を取るという情報セキュリティの体制は、Y 社と Z 社に共通しており、Z 社の担当者とはこの補助者である。これを束ね事務局という名称を付し、インシデント発生時の拠点として機能するだけでなく、訓練実施の実務と事前の教育についても担っているのが Z 社である。この担当者が身近に存在すること、そして彼らが組織化されていることが、訓練を繰り返すことにおいて非常に重要なポイントとなる。

次節では Z 社のこの体制について、セキュリティ体制の運用について訓練を軸に再度確認し要点を結論として整理する。

3 訓練体制とリーダーシップについての考察：Z社の事例の考察の整理から

前章で見てきたように、Z社では1か月に1回という高頻度で、標的型メール攻撃訓練を長期にわたり繰り返してきていた。本研究で取り扱う事例の中では、アカウント数だけで見れば規模も大きく、この訓練の経験とそれを支える体制は特筆すべきものである。

まずは、社内をブロックに分割し、ブロックごとの責任者とその委任を受けた実務上の責任者数名、そしてその補助者たる担当者、そしてこの担当者が組織化され事務局を形成しているという構造がその特徴である。なにより訓練の活性化は、このブロック単位での活動によって生まれた競争的な要素によってもたらされていた。

そして、訓練を企画し、それに沿うべく教育資料を改訂し続けるCSIRTと、自ブロックの業務都合を勘案しながら改訂された教育資料を適宜に活用し教育を主導する一方で、訓練の報告の受付とその集計の実務を事務局が行うという役割の分担である。月に1度の展開なのでサイクルは非常に速い。それでもほぼ月1度という頻度で回すことができているのは、煩雑な事務作業をブロックの事務局が担ってくれている点が大きい。

報告を直接CSIRTに対して行わず個別に定められた担当者に対して行うことで、報告の集中による連絡回線や実務的なパンク状態を回避するという現実的な面もある。しかし、本来の狙いは、訓練の報告受付の分散化ではなくセキュリティマターに関する相談者が身近に存在することを周知することにある。この仕組みは、Spitzner（2014）が提案しているアンバサダー制度に非常に近しいものとなっている。むしろその改訂版といえるだろう。Reason（1997）の安全文化に従えば、振る舞いとしての報告を促進するためには、その下位文化である報告する文化に必要な要件として「報告のしやすさ」が挙げられていたが、報告フォームの活用という報告の簡便さとともに、報告を実行するにあたりその物理的な近さもまた重要な要素となるはずだ。Z社では、個々人レベルで担当者が指定されており、担当者名をカードに自ら記入してもらうことで認知の徹底を図っていた。

このような体制によって訓練の高速サイクルが支持されているのだが、訓練の結果の取り扱いもまた要点である。ブロックごとに事務局で集計された結果は、ブロックごとの責任者、そしてCSIRTで構成される全社的な情報セキュリティの会議体である委員会へと申達され、取りまとめられたうえで公表される。訓練の結果は、経営者層には4半期単位で共有されている。前期の結果を受けた経営者層が、自らが所管する事業部のブロックに対して次期に向けて発破をかけることがあり、これによってブロック単位の活動が報告率100%の達成に向けてより活発になることもあ

るという。文化の醸成や変革において重要視され、さらにはマネジメントシステムの問題点として挙げられていたように、やはり経営者層のコミットメントが、運用されるシステムのアウトプットへの関心という形で表現され、そしてそのシステムの一部を担う自らが注目を受けているという認識は組織内においてなにより重要だということが理解できる。

そして、ブロックごとに集計し公表されること、その結果について経営者層の関心が示されていることで自然と生まれたブロック間の「競争性」や「ゲーム感覚」が、訓練の実施を担う者にとっても訓練参加者にとっても非常に良い効果となっていると考える。この 2 点が、訓練そのものを持続的なものとしていくための強いポイントとなっている。

前章の Z 社の事例のセキュリティ体制の項で確認したように、役割の分担の違いから CSIRT そのものに予算配分をしていないため、そのコミットメントが予算の金額に現れることはないが、このように活動に対する経営者層のコミットメントは高い。それは、Z 社は主たる事業において機密性の高い情報を大量に扱っているため、情報の取り扱いに対する意識はもとより相応に持っていたと考えられ、そのため情報セキュリティへの理解と親和性も高かったからではないかと推察できる。

組織変革論などで議論されていたリーダーシップの発揮という点では、全社的な情報セキュリティの委員会の設置という経営者層のリーダーシップと共に活動の結果への関心という形で信託を受けた CSIRT がより強いリーダーシップを発揮することによってセキュリティ文化の醸成がなされている。この経営者層のリーダーシップについては、セキュリティ体制と CSIRT の活動に対する支持と支援によって、その権限の委譲として明確に理解することができる。一方の CSIRT が発揮するリーダーシップについては、訓練の量的な面だけでなく、質的な面で現れることになる。Z 社は高速な訓練サイクルによる経験の蓄積がある一方で、念入りな事後的分析が行われている点が、他社との大きな違いである。訓練を繰り返すことで開封率が低い水準で定位していることについては、失敗を経験することで失敗しない方法を学習し、それにより失敗そのものは低減していくが、それと同時に失敗を経験しないことによって学習の機会が失われていくという「学習のジレンマ」（谷口, 2008）も指摘できる。そして、訓練履歴のなかでは、短くはあるが報告率が連続して低下する期間もあった。しかし、この一時期の報告率の低下という異常事態に CSIRT が早急に気づき、危機感をもち素早く具体的な対処を施したことは、「報告しない」という別の失敗に目を凝らした結果であろう。

未報告の事例の分析については、その成果として、報告先の周知の徹底を図るために配布した白抜きのカードが生まれたことについては既に述べたとおりだが、その他のものとして、添付ファイ

ルの開封キャンセルの事例もあった。これについてはアプリケーションの特徴と結びついて生まれたものであり、CSIRT としては想定していないものであった。しかし、未報告者の追跡調査からこの事例とその理由を析出したＺ社では、キャンセルの事例も回避することの難しい攻撃者の詐術として位置づけている。そのため、キャンセルの前提となる開封させないためのソフト・ハード両面の対策を打った。これも、豊富な経験と地道な分析との接合によるものである。

多数回開封者の視線調査によってもたらされた知見は、多数回開封者の特徴ではあるが、これを特定個人の特性として位置づけることなくヒューマンエラーの一種として捉え、システムによる低減を図るべく、メールの送信元ドメインによって色分け表示するシステムを導入した。これに合わせて、開封時の確認作業によって平時の業務効率が低下することを防ぐ目的に、社内でのメールのやり取りについては、送信者名のブック化、件名の表示方法の統一といったようにメールの送信時の新たなルールを設けた。これにより、送信時にもセキュリティ・ファーストな振る舞いの定着も期待できる。繁忙な実務を抱える繁忙な現場の人々にとっては、遵守しなくてはならない手順の増加のように見えるかもしれないが、開封時の確認作業を軽減することができることで相殺できる。さらには、社外へのメール送信においても誤送信を防ぐことができ、不意の情報漏洩の防止には有用である。このようにＺ社では多様な角度からのセキュリティ文化構築へのアプローチがなされている。

最後に、Ｚ社の訓練の今後の課題と方向性について付言したい。これまでの結果からは、Ｚ社にはセキュリティ・ファーストが定着した、熟成したセキュリティ文化が根付いているように見える。それでもまだ「根付いているように見える」と筆者が表現する理由は、Ｚ社における１つの事例として*『通報のなかった従業員に対する聞き取りにおいて、「この仕事が済んだら通報するつもりだったが、そのまま忘れてしまった」と述べた従業員がいる』*と述べられていたことにある。この例のように、セキュリティの重要性は十分理解しているが、行動のプライオリティが従来と変わっておらず、セキュリティ・ファーストにはなりきれていないと指摘できる例があることによる。確かに訓練であることが判明しているゆえに従来のプライオリティが維持されているということであろうが、中断の手間と時間を惜しまず報告が優先されることが訓練の最終的な目的であり、この点から見ればまだ真の行動変容には至っていないと評価できる。しかしこれについては、IT 機器の進化を含めた労働環境の変化が要因のひとつとなっていると CSIRT では分析している。モバイル機器を活用しどこでも仕事ができるようになったことで、セキュリティ体制において地理的な孤立が生まれていることの表れであると考えている。このように企業の内的・外的な環境は常に変化して

おり、この変化への対応として、企業文化も企業文化としてのセキュリティ文化もまた常にブラッシュアップが必要であることの一つの例である。

これとは別に、派遣従業員や請負の作業者に対して付与しているアカウントも訓練の対象となっており、開封や報告の検証対象となっている。こういった人々は、企業対企業の契約によって社外よりやってきてZ社内でその業に就くのであるが、Z社ではこういった者も訓練だけではなく事前の教育の対象としている点は評価できる。さらに契約レベルでは、派遣元企業・発注先企業側に情報セキュリティに関連した研修実施の義務を課しており、相手方企業においてこういった教育研修が実装されているかどうかは、契約企業の選定作業としてZ社が確認する規程になっているという。しかしながら、Z社内で作業する者に対して相手方企業内でこれらが確実に履行されているかのチェックは、実務的な困難さから行われていないようである。ビジネスの世界における実務的な困難さという現実は想像に難くないが、セキュリティ・ファーストとしてはその徹底に期待したい。

また、報告率については、個々のブロック単位では報告率100%が数多く見受けられる。連続記録としても最長で16回を数えるブロックもあるほどだ[88]。しかし、全社単位、約25ブロック全てが同時に100%を達成したことは残念ながら未だないそうである。本稿の執筆時点においても訓練は繰り返されおり、この間にも報告率100%が達成されている可能性も高い。しかし、これも1度達成されれば目的達成というものではなく、むしろ達成した暁には、報告率100%の維持により高い努力が必要になろうことから、これについても期待したい。

一般的に言われる学習曲線を鑑みると、毎月1回という頻度が適切であるか、訓練のプロセスにボランティアベースで進むステージがあることには議論の余地はあろうが、訓練の目的を「報告」行動の定着に置き、情報セキュリティの運用体制を整備し、これに支えられる訓練の高速の改善プロセスは、他社が手本とするに最適な仕組みであると考える。

[88] 第Ⅶ章第4節で扱うZ社のメンバー個人に対するインタビュー日現在（2020年7月末現在では、28か月連続（継続中）が最長となる）。

4 文化の醸成や変革に求められる要件と要素についての考察：Z社の事例の考察の整理から

では、実務的な観点からは秀でた事例として考えることのできるZ社の事例からは、セキュリティ文化を企業の中心的文化として醸成していく試みにおいて、文化の醸成や文化の変革に求められる要件や要素はどのように充足されていたのか、次のように整理することができる。

まず、文化の醸成に求められる「コミュニケーションの一貫性」と「褒賞」という要件（O'Reilly,1989）を満たすために考慮すべき要素は4つであった。

①選択と参加

ここでは、個々人レベルで訓練への参加を選択するというオプションは存在しえない。これは、O'Reilly が例として用いたカルト集団ではないが、営利企業に従業員として「参加する」ことそのものとして捉えることが現実的であろう。自らが参加している組織の訓練に経営者層も含めて「全員が参加している」という事実に意味が見い出されさると考える。

②シンボリックなアクション

経営者層が訓練に参加することそのものもシンボル的行為であるし、その訓練を実施している主体を支援し、なにより訓練の結果に興味を示し、フィードバックを行なっていることが、組織のメンバーから見えていることが情報セキュリティを重視するという価値を表現したシンボリックな振る舞いである。そして、それだけではなく、次の「他者からの情報」にもつながっていく。

③他者からの情報

訓練実施時の事務局を包括したセキュリティ体制が身近にあることを実感することができる担当者の存在である。不在時の代理者も個人レベルで設定されているという綿密なネットワーク構造であった。現実には訓練の報告先として設定されているだけでなく、日常業務をセキュリティ・ファーストに進めるための無数の参照点が身近にあるということなのだ。このセキュリティ・ファーストに則った業務の進め方をするための知識の体系とも表現できるセキュリティ体制に名実ともに経営者層が参加し、機能していることが、参照点としての他者である担当者の意味と価値をさらに大きくしていると考えられる。

④包括的な褒賞

訓練の結果によって個人が個別に、そしてブロックという集団単位でも褒賞が与えられることはなかった。しかし、経営者層が結果に関心を示し、フィードバックすることは、その活動に対する褒賞であり、これによってコミュニケーションの一貫性が担保されていると言えよう。さらにフィードバックによって競争がうまれ、より良い結果とそれに対するさらなるフィードバックを求めて競争心が満たされることも一つの褒賞なのかもしれない。これとは別に、Schein は、創業者のやり方を踏襲して成果を出すことも褒賞であることを指摘していたが（Schein,1985; 1990; 2010）、先の「③他者からの情報」で触れた、セキュリティ・ファーストに則った業務の進め方をするための知識の体系から具体的な知識を引き出し、活用し、セキュリティ・ファーストに則った業務の進め方をすることで成果を出すことそのものが褒賞となっていることも考えられる。

これらが、文化を醸成していく、情報セキュリティを重視するという価値観を、メンバーが内心として取り込み、基本的な仮定として共有するために求められていた基本要素をどのように充足していたかである。

そして、旧来からの文化を変化させる、いわゆる文化の変革において求められる要件からこれを捉えなおすと、「目標の明確化」、「多くの社員と取り組む」、「過度に管理しない」という 3 つの要件(Deal & Kennedy, 1982）であり、これを満たすための 5 つの要素からは次のようなものとなる。カッコ書きについては、Schein（1985）による心理的安全を軸とした文化変革に求められる要素であり、これら 5 つにそれぞれ対応する要素と考えたものである。

①メンバー間の合意と②信頼関係（将来像／行動レベルの目標）

情報セキュリティが重要であると比較的早くからに認識され、訓練のターゲットを開封率ゼロとして「行動レベルの目標」が提示され、取り組まれていたが、初期段階でその困難さと非現実的な目標であることに気づき、KPI の転換が図られ、新たな行動レベルの目標として「報告」が KPI となったことがこれに該当しよう。訓練の経験を積みながら、目標の変更のプロセスを含め、メンバー間の合意によって緩やかに目標が明確化されていったといえるのではないだろうか。

そしてこれにより、開封という過失の問題ではなく、報告しないという不作為が問題であるという転換となり、過失そのものは処罰の対象から外れることで信頼関係を築く基礎となった。これが直接的な心理的安全の源泉でもあり、これが公正な文化につながっていく。さらに、添付ファイルの開封や本文に埋め込まれた URL のクリックが機械的に検知され、それが訓練結果となるという受動的なものであったものが、URL のクリックや添付ファイルの開封を前提として、それについ

て報告するという振る舞いが求められ、自分が動かなくてはならないという能動的なものとなることで、「当事者性」を付加するきっかけとなったとも考えられる。

③技術の養成と④忍耐（学習機会／トレーニングと時間と費用）

なによりまず、心理的安全の確保がなされた全員参加の訓練が、長期間・高頻度でおこなわれ、報告率 100%の追求が続けられているという実績に表れていると考える。Z 社のメンバー個人に対するインタビュー調査日現在（2019 年 2 月）においても、およそ月 1 回というペースで、延べ 40 回を超える訓練を実施している[89]。あくまで長期的な成果として報告率 100%を追求し、この目標達成に資するように、訓練結果の仔細な分析が行われ、分析に基づいて訓練内容と教育資料の絶え間ない改善が CSIRT によって続けられているが、それだけではない。教育と訓練の集計はブロックごとの事務局と分散した現場レベルの担当者が担うというように多くのメンバーが常に参与している。これにより、組織の情報セキュリティはセキュリティの専門的なチームだけが担当するものではないというように「当事者性」を向上させていると考えられる。そして、報告という振る舞いによって情報セキュリティの向上に参加することになり、結果として「多くの社員と取り組む」は自然と満たされることになる。

⑤柔軟性（構造的サポート）

柔軟な文化として現れていた。経営者層は教育と訓練の実施主体に任せる一方で、自らも訓練に参加し、訓練結果に関心を持ち、そしてフィードバックを行うことが、活動に正統性を与えるシグナルとなっている。フィードバックは訓練に参加するメンバーへに対する褒賞であり、シグナルもまた実施主体への褒賞であり、支援となっている。そして実施主体もこれに応え、工夫を凝らした訓練の企画と、訓練の前提となる教育の資料の改訂を高い頻度で行っていた。この教育の実践については、これもブロック単位という体制の特徴をうまく活かし、一律で強制的な教育の実践とはならず、訓練の結果やブロック内の業務の状況に合わせて展開できるという非常に柔軟性に優れる運用がなされていた。現場に近いレベルで展開の意思決定ができるという点も当事者としての自主性を促進すると考えられる。

これこそが Schein のいう「構造『的』サポート」であると考えるが、この柔軟な運用の前提となるのが構造であり、なにより訓練の実行体制であろう。これは訓練の実施だけでなく情報セキュリティの体制そのものでもあるが、ポイントとなるのが、組織を分割したブロック制が敷かれ責任

[89] 2020 年 8 月の執筆時現在では、延べ 48 回とのこと。

単位が小さくなっている事である。そして責任単位であるブロックごとに、事務局を中心として情報セキュリティの担当者で構成されるネットワークが構築されていることで、メンバーと担当者との距離感が非常に近いものとなり、彼らの活動を観察することも含めて、情報セキュリティそのものが身近なものであること、自分も無関係ではないという、当事者性の源泉となっていると考える。

文化の醸成において理論的に検討された要件や要素をこのように充足していると考えられるZ社の事例の特徴は、なにより長期間・高頻度で実施され続けている訓練である。その背景には全社的なセキュリティ体制が名実ともに存在し機能していることと、それらをより個人にとって身近なものとするブロック制という組織構造のサポートがある。この特徴を文化の定着に必要な教育や訓練の持続性という観点から捉えると、本質的に求められているのは、この構造によってよって生まれた、競争心という集団生活における極めて原始的で基本的な要素ではないだろうか。これがZ社の訓練に備わったことは、必然なのか偶然なのかは判断できないが、内部者にとっても、自らのブロックの結果というだけでなく他のブロックとの比較が、訓練の結果と全社的な成果を確認するにあたって極めて単純な仕掛けとして役立っており、また、教育と訓練の単純な動機付けとして機能していることから、文化の変化の要件とされる訓練を継続していくための要素として「ゲーム性」や「競争心」を意図的に持ち込むことをマネジメントの要件に加える必要があると考える。

「④忍耐」は、心理的安全を生むためにも一時的な能力の低下や成果の遅滞を我慢するという意味であり、文化の変革には長時間かかることへの覚悟でもあることから必須の要素である。しかし、忍耐という表現は、文字通り耐え忍ぶという、マネジメント側もマネジメントされる側にとっても暗くつらい道のりがイメージされる。これでは持続性においてプラスのイメージを期待することは難しい。これを置き換えることを主張するものではないが、教育や訓練に持続性を加味するという意図において、イメージとして「忍耐」と対になる「ゲーム性」もしくは「競争心」を要素として加えることを主張しておきたい。マネジメントとして、取り組みの結果と成果を外部に公表することを、内部的な関心を維持し続けることの動機づけとする例も示したが、内部的な効果として、経営者層だけでなく組織全体が結果に興味を持つ、持ち続けるという点で有効であると考える。そして、確保した心理的安全の効果を最大化するという点でも有意に機能すると考える。

では、理論的な要件をこのように充足し、実務的にも最適な仕組みによって展開されていると評価した教育と訓練は、セキュリティ文化の醸成に本当に寄与しているのであろうか。報告することを求める訓練を繰り返すことを通じて、報告という「振る舞い」は確実に実行されていることは間違いない。しかし、組織文化とは、組織メンバーによる組織の標榜する価値観の内面化と振る舞い

としての表出の問題であった。すなわちこの報告という振る舞いは、セキュリティ・ファーストが内面化され、具体的な振る舞いとして表出したものなのかどうかである。これについて確認するため、次節において少数ではあるが Z 社のメンバーに対して行ったインタビュー調査を基に検討し、結論を導出したい。

5 「セキュリティ文化」醸成についての考察：Z社に対する追加的調査から

最後の課題としていた「セキュリティ文化は企業組織の文化となるか」について検証したい。すなわち標的型メール攻撃訓練を繰り返すことでセキュリティ・ファーストが内面化され、振る舞いとして表出しているのか、より現実的には、「表出している振る舞いは、内面からもたらされているのか」である。本来であれば、アンケート調査票などの大規模な量的調査によってこれを検証すべきであるが、調査対象企業は民間の営利企業であることもあり、これを実施することは困難であった。この代替として、ごく少数を対象にしたものであるがZ社の従業員に対して追加的なインタビュー調査を実施した。

それは、寺本（2013）が、経営組織論での文化研究における「組織のメタファーとしての文化」（Smircich, 1983）研究の現代的意義を強調したように、本研究において、文化を人間集団の組織運営上の特定課題を解決するものという機能的な組織文化論の立場から、訓練を文化変革のツールと位置づけ、その効果を KPI から捉え、その是非を論じるというだけでは不十分であると考えたことによる。

本研究の対象は、民間の営利企業組織であり、組織内の特定の課題解決にコストをかけ、具体的な解決や改善というリターンを追求するのは当然である。その具体的なツールとしてマネジメントシステムなどが存在しているが、そのマネジメントの対象の１つとして文化に言及しているのは従来的な機能主義視点の文化論としてのものであり、文化を組織内の一変数として捉えるものである。文化の醸成についてを、こういった問題解決の手法から検討し、その効果とともに分析の対象とすることは経営学において意味あることだと考える。しかし、それだけでなく、それによって現れるメンバーの行為についてを、それを行うメンバー自身らがどう認識し、理解しているか、その認識と理解は何を通して行われて、組織全体としてどう形成されているかを併せて明らかにすることが現代的な組織文化研究における要点であると考える。

そこで、解釈主義的な立場から、単に組織メンバーの認識の確認を試みるというだけでなく、個々人の業務と情報端末の活用の状況や、それに関連する文化的要素として定常的に現れる標的型

メール攻撃訓練とその実行体制との関係性において生じる認識を、個別具体的に確認することを関心の中心においてインタビュー調査を行った。

(1) 調査の概要

今回実施したインタビュー調査の概要は以下の通りである。

表 17：インタビュー対象者の概要と調査実施日時

	社歴	担当職務	調査日時
G 氏	39 年	業務推進	2019 年 7 月 3 日午後 4 時 30 分より 30 分
H 氏	26 年	監査	2019 年 7 月 3 日午後 5 時 00 分より 30 分
I 氏	21 年	販売	2019 年 7 月 4 日午後 4 時 00 分より 30 分
J 氏	26 年	経理	2019 年 7 月 4 日午後 4 時 30 分より 30 分
K 氏	30 年	営業	2019 年 7 月 4 日午後 5 時 00 分より 30 分

出典：筆者作成

調査は、半構造化面接を採用し、以下の項目について質問し、回答を得た。

・入社年次と現在担当する業務歴・内容について
・業務で使用する情報端末の種類と業務時間内での利用時間の割合について
・業務におけるメールの使用状況について（メールの確認頻度とメール処理数およびそれに要する時間）
・直近および初回の標的型メール攻撃訓練に対する認識について（自身の訓練結果や職場の同僚間の反応や認識について）
・訓練の効果について
・実務とのコンフリクトについて
・訓練の頻度について
・訓練の意味について
・Z 社のセキュリティ向上におけるリーダーシップについて

(2) 調査の結果

分析は、調査母数が極めて少数であるため、頻度分析やコード化による要素抽出といった詳細なものは行わず、各回答を列挙し、共通点を見い出すといった粗分析に留め、考察を行なっていく。

まず、業務に利用している情報端末の種類と業務時間中における情報端末の利用の程度についての質問に対する回答は表 18 の通りであった。

当然に全員がPCを活用し業務を行っているが、外出の多い営業職であるK氏を除けば、業務時間のおおよそをPCのモニターに向かっているというように業務における依存度が高いことがわかる。個人に1台ずつ貸与されているPCによって構成される情報ネットワークを中心とした情報端末が企業活動の中心となっていることが改めて確認できる。

表18：利用する情報端末の種類と利用の程度

	利用端末	情報端末の画面に向かう程度
G氏	デスクトップ型PC	常に
H氏	デスクトップ型PC	出社してから常に
I氏	ラップトップ型PCとスマートフォン	常に
J氏	ラップトップ型PCとフューチャーフォン	業務時間の8割くらい
K氏	デスクトップ型PCとスマートフォン	業務時間の半分くらい

出典：筆者作成

このように依存度の高い情報端末であるが、このなかで本稿の関心の中心である標的型メール攻撃訓練に関するものである連絡手段として電子メールのアプリケーションの利用の頻度と、日中における平均的な処理数について尋ね、あわせてその中で実際の標的型メール攻撃に遭遇したことがあるか、訓練メールの添付ファイルを開封したことがあるかを尋ねた。回答は表 19 の通りである。

各人ともにアプリケーションそのものは常に立ち上げており、メールの確認頻度としては受信の通知があるごとに目は向けるが内容に緊急度がないと判断した時は、1時間に1度程度にまとめて対応するというのが基本的な対応であった。営業職であるK氏については、顧客への対応の速さを重視するために頻繁にチェックし、都度の対応をしていることがわかる。実際の処理数については、従事する職務が対外的／対内的な業務のどちらに比重があるか、そして職位の高さによって違いがあるようだ。具体的には、対外的な業務の比率が高いと、顧客などの組織の外部との連絡手段としてのメールが増える。職位が高い場合は、自身が関係するプロジェクトや部下の数が増え、部下や関係者からの直接の報告や連絡というだけでなく、部下とその担当顧客や関係者間のやりとりについても、内容の周知や確認を目的としてC.C.で同送されてくることで、受信するメールの数が増えるようである。

表19：メールの利用状況に関する回答

	メールチェック頻度と使用状況	メール処理数と対応時間	実弾の経験／訓練での開封経験
G氏	1時間おきくらい／他の作業をしながら眺める感じ	20通くらい。CCを入れると30通。／業務時間の1割くらいのイメージ	あり／ない
H氏	1時間に1回くらい／常にメーラーを開いているので届けばその都度	20～30通くらい。／合計して1時間くらい	なし／あり
I氏	ほぼ常に	200通くらい。CCの整理を除いて返信するのは30～50通。／1時間～1時間半	なし／なし
J氏	感覚的には1時間に1回。画面上の受信の通知に気づけば確認はする。	30～40通くらい。CC含めて50通。返信するものはそのうち2割から3割で10～20通／1日で言ったら30分くらい	なし／あり
K氏	頻繁に。お客さんの仕事柄、時間に追われるケースが多いので、やっぱり早目に答えないと。	100通くらい。返信するのは7割くらい。メールでのやり取りが、電話よりも全然多いですね。	なし／あり

出典：筆者作成

このように実務において用いられている電子メールであるが、この電子メールに悪意を添付して送信してくる外部者への備えとして行なわれる標的型メール攻撃訓練の効果に関する認識が本節における最初の論点である。まず、第1の訓練の効果としての、標的型メール攻撃への反応について尋ねたときの回答は表20の通りであった。

訓練のまず最初の目標である「報告行動」の定着という観点では、

『*標的型攻撃というか、訓練っぽい、あれっ？ていうメールが来た時は、●●さんに、「今、訓練メール流しました？」と聞いて、「流してないよ」と言われて。このメールは怪しいかな？となる*（J氏）』

『*「これ、いいんですか？答えちゃって。」「クリックしていいですか？」と問い合わせがある*（G氏）』

というように、報告行動の前段階となる「標的型メール攻撃があり得ること」そして、「疑わしいメールは開かない」という知識ベースの定着がみられると同時に、疑わしいメールが届いたときには身近な同僚に対して、当該メールが訓練によるものなのか実際の攻撃なのかを判断するために、訓練メールが全体に流れているかを尋ねるという行動が起きているようである。特にJ氏の挙げた個人名は、近隣に配置されている担当者のことと推察され、身近な同僚がセキュリティのキーマン

表20：訓練の効果としての訓練メールへの反応

G氏	「これ、いいんですか？答えちゃって。」「クリックしていいですか？」と問い合わせがあるということは、意識している人が確実にいるということです。
H氏	やったことによって、意識が高くなったと思います。ブロックで数字を出される。開いちゃった人数で、年間の成績表みたいなものをつけていたんです。集計を事務局が真剣に取り組んでいました。なので、そうすると、気を付けます。もう３年、やっていますよね。すごい浸透してきたと思います。そうですね。認知、認知度と重要度が増したのはこの２年、３年ていう感じですかね。本当は、うちの会社の一番大切な資源、資源というか、個人情報、お客様が預ける情報資産を扱う。そこが崩れちゃえば会社としてダメになってしまうところを守るのが、情報セキュリティであったんですが、それまではかけ離れている、情報セキュリティは守るものという認識があまりなかった、つながっていなかったんですよね。それが密接なものだという認識になった。 社内に浸透したのは訓練のおかげでしょうか。絶対、全員が、パソコンを持っている人全員が参加なので、そういう意味で言えば、認知度を上げたのはこの訓練のおかげですね。
I氏	意味があります。緊張感あると思いますよ。あれがなかったら、ずるずるだと思います。一発何か起こしたらアウトでしょう。研修より訓練。研修やっても、正直あまり意味がないと思います。一回踏んでみて、あっとならないとダメだと・・・。認知していると思いますよ。線を抜く、パソコンは触らない、すぐ報告する。 絶対、やらなきゃいけないでしょ。うちは。ありますよ。（相手が）会社さんの場合、個人情報のリストをメールで送ってくるんですけど、いやいや、送らないでください。ダメです、担当ベースでやりません。と。 根幹です。うちの会社の根幹ですから、個人情報で何かあったら終わりです。売上マイナスです、それだけで。このデータのもらいかた、いいの？と、どうするの？といったとき、まずはＣＳＲ(※1)に確認しようというのが、ちゃんと浸透していると思います。うちの会社のなかに。やったことないケースだけど大丈夫かどうか確認しよう、というのは浸透していると思います。
J氏	引っかからない自信はないですが、怪しいかなっていう、あれは、気にして、気になった時に、確認はしています。標的型攻撃というか、訓練っぽい、あれっ？ていうメールが来た時は、●●さんに、「今、訓練メール流しました？」と聞いて、「流してないよ」と言われて。このメールは怪しいかな？となる。でも、フィルタでほとんどひっかかっているので、そんなにないと思う。やっぱり流れるとアラートになるので、私、今まで１回だけひっかかったことがあって、それが悔しくて。自分の中で。自分のパソコンの、この、画面の下のところに、真っピンクの付箋を貼っているんです。それが普通の状態、見慣れてしまう。それが、他の地区でも、デカデカとテプラで、パソコンのディスプレイの上に、「メールを開く前に・・・」と貼っているところもあって。素晴らしい取り組みとは思うんですけど、結局それがもう普通の状態になるんです。常態化しています。
K氏	やっぱり認識をするので、それは意味があることだと思います。いわゆる、忘れないというか。いつくるかわからないよ、という心構えは持つことになるので、それはそれで意味があると思いますけど。 うちは個人情報を武器にしている会社なので、そこで何か感染させられて情報流出になってしまうと、完全にうちにとっては命取り。非常に重要な問題だと捉えています。

※1）情報セキュリティ委員会

出典：筆者作成

として機能していることもここから伺うことができる。

そして、訓練の直接の目的となる報告行動そのものに関連するものとして、

『*認知していると思いますよ。線を抜く、パソコンは触らない、すぐ報告する*（I 氏）』

というように、定められている手順を実行することについては確実に定着しているようである。これは、前章の Z 社の事例の中で確認したように、報告率がほぼ 100%で推移していることからも効果の認められるところであろう。

そして、次段階の目的となる訓練を繰り返すことによる「情報セキュリティの認識の向上」という目的的な面について触れる回答としては、まず標的型メール攻撃について述べるものとして、

『*やっぱり流れるとアラートになるので*（J 氏）』

『*やっぱり認識をするので、それは意味があることだと思います。いわゆる、忘れないというか。いつくるかわからないよ、という心構えは持つことになるので、それはそれで意味があると思いますけど*（K 氏）』

『*意味があります。緊張感あると思いますよ。あれがなかったら、ずるずるだと思います。一発何か起こしたらアウトでしょう。研修より訓練。研修やっても、正直あまり意味がないと思います。一回踏んでみて、あっとならないとダメだと・・・。*（I 氏）』

というように「緊張感の維持」という効果があるという認識が共通してみられる。特に、机上の研修だけでなく、実践ベースの訓練との組み合わせが重要であることを強調する回答でもあるが、この緊張感の維持ということに関しては、

『*私、今まで 1 回だけひっかかったことがあって、それが悔しくて。自分の中で。自分のパソコンの、この、画面の下のところに、真っピンクの付箋を貼っているんです。それが普通の状態、見慣れてしまう。*（J 氏）』

というように、緊張感の維持や定常的なリマインドを目的とした個人レベルでの対応として、日常業務において視界に常に入るような位置にリマインダーを配置するという実践として現れているという。しかも、これは J 氏特有の取り組みではなく、

『*それが、他の地区でも、デカデカとテプラで、パソコンのディスプレイの上に、「メールを開く前に・・・」と貼っているところもあって。素晴らしい取り組みとは思うんですけど、結局それがもう普通の状態になるんです。常態化しています。*（J氏）』

というように、組織に共通してみられるという。

ここまでで確認できたように、標的型メール攻撃訓練を繰り返すことによって獲得された標的型メール攻撃への認識や備えをベースとして、情報セキュリティ全体への認識の向上も確認することができたが、この認識が高まった結果としてどのような影響が最終的に表れるのだろうか。これについては、

『*絶対、やらなきゃいけないでしょ。うちは。ありますよ。（相手が）会社さんの場合、個人情報のリストをメールで送ってくるんですけど、いやいや、送らないでください。ダメです、担当ベースでやりません。と*（I氏）』

『*このデータのもらいかた、いいの？と、どうするの？といったとき、まずはＣＳＲに確認しようというのが、ちゃんと浸透していると思います。うちの会社のなかに。やったことないケースだけど大丈夫かどうか確認しよう、というのは浸透していると思います*（I氏）』

というように、メールを利用するにあたってしてはならないこと、するべきことが明確になり、業務における顧客との実際のやり取りについてもセキュアな方法によってこれを実現しようとする行動が起きていることが認識されているようだ。標的型メール攻撃への緊張感が持続することは、情報セキュリティへの認識を持続し、その結果として情報漏洩といったインシデントを防止するための別の振る舞いとして表出していることがわかる。

そして、これらの新しい振る舞いがなぜ生まれてきたのかである。それは、『*本当は、うちの会社の一番大切な資源、資源というか、個人情報、お客様が預ける情報資産を扱う。そこが崩れちゃえば会社としてダメになってしまうところを守るのが、情報セキュリティであったんですが、それまではかけ離れている、情報セキュリティは守るものという認識があまりなかった、つながっていなかったんですよね。それが密接なものだという認識になった。*』というように、情報こそが自組織の業務の根幹であり、それをセキュアに扱うことこそが信頼の源泉であるということが訓練を通して理解され、繰り返されることで内面化され、結果として「情報セキュリティの自分事化」が起きていることが理由として見い出せる。セキュリティ文化の達成を難しくする理由の一つに、情報セ

キュリティに対する当事者性を持つことの難しさを挙げたが、Z社ではそれに成功している。ただし、Spitzner（2014）が挙げていたような個人のメリットと直接結び付けることによって認識されたのではなく、

『*一発何か起こしたらアウトでしょう（H氏）*』

『*個人情報を武器にしている会社なので、そこで何か感染させられて情報流出になってしまうと、完全にうちにとっては命取り。非常に重要な問題だと捉えています（K氏）*』

という回答があるように、どちらかといえば自らの所属する組織の信頼の維持として、もしくは自組織の評判を棄損することの延長線にある個人のデメリットを防ぐことと結び付けて捉えられており、組織へのコミットメントが高いとされる日本的な企業組織での自分事化の特徴であるかもしれない。

では、こういった効果として組織メンバーに認識されている標的型メール攻撃訓練であるが、こういった認識がもたらされるに至る訓練の頻度は Z 社においては月に 1 度というペースであるが、この訓練の頻度に関する感想を求めたところ回答は次の通りであった。

表21：訓練の頻度に対する認識

G氏	（月に）2回はちょっと多い。2か月に1回と言われると・・・1か月に1回かな。だから、もっと、あるいはランダムにやるのもいいのか。あるいは、通知しないとか。
H氏	ちょうどいいんじゃないでしょうか。集計する側の苦労も知っているので、あの、まぁ。頻度については別に。
I氏	まぁ、多くもなく、少なくもなく。月1本も来ているのかな？2か月に1本くらいのイメージなんですけど、毎月出しているんですか？うちって。緊張感を持つなら、月1回ならいいんですけど。
J氏	そうですね。あんまり、ちょくちょく来ても、なんか、疑って、そろそろ来るだろうとなっちゃうんで、忘れたころに今来ているので、まあまあ、頻度的にはいいのかな、と思います。
K氏	今ぐらいでいいんじゃないかな。あんまり頻度多くても困っちゃうんで。1か月いっぺんなのか、2か月、1か月半にいっぺんなのか、今、1か月にいっぺんだと思うんですけど、まあ、それくらいであれば。特にいいのかな、という気がしています。

出典：筆者作成

現状の訓練の頻度については、

『*忘れたころに今来ているので、まあまあ、頻度的にはいいのかな、と思います*（J氏）』

端的に「忘れたころ」というように、日常業務の繁忙のなかではセキュリティへの意識が薄くなることがやはりあることが伺える。しかし同時に、効果についての回答でも確認したように、標的型メール攻撃があり得ることを『*認識する*』『*アラートとして*』『*いつ来るか分からないという心構えは持つことになる*』というように、1か月に1度という現状の頻度はセキュリティ認識をリマインドする機能として肯定的に捉えられていることがわかる[90]。

さらに、

『*2か月に1本くらいのイメージなんですけど、毎月出しているんですか？うち*（I氏）』

という回答もあるように、訓練の頻度を正しく認知していないコメントもある。表面的には訓練そのものが認識されていない、ともすれば訓練の効果そのものについても否定的に受け取ることもできよう。しかしこれは、ハード的対策により自動的に破棄されていることに加え、メールの件名や内容から自らの業務に関連しないと判断して、破棄することが無意識と言っていいレベルで行われていることによると考えられる。特にK氏は営業職であり、メール利用の頻度が高く、処理数が多い中でこれが自然に行われているのは、訓練とその事前の教育が繰り返され、このなかで標的型メール攻撃の類例を学ぶことで培われたものと推測でき、「繰り返すこと」がいかに重要であるかの一例として捉えることができる。

一方で、月 1 回のペースで繰り返される訓練や、その効果として現れている振る舞いによって、かえって業務に支障をきたすことはないのか、いわゆる訓練と実務とのコンフリクトはないのかという問いについては表 22 のような回答であった。

『*訓練のせいで、というのはないですね。*』

『*そうですね。それはないかな。*』

---

[90] 学習効果（学習と記憶に関するエビングハウス（1885）の研究より示された「忘却曲線」と「学習曲線」）、すなわち短期記憶と長期記憶の関係性については、長期記憶への変換もしくは棄却の分岐点がおよそ 30 日であることが指摘されていることに整合的である。また、知識ベースで取り込んだ短期記憶（手続き記憶・情報）を、行動として出力することが短期記憶から長期記憶（意味記憶・知識）へと変換が図られることの鍵であることも指摘されている。

Ebbinghaus, H. (1885) "Memory: A Contribution to Experimental Psychology." New York: Dover (宇津木保(訳) 望月衛(閲) (1978)『記憶について:実験心理学への貢献』, 誠信書房)

というように、まずは「ない」と明確に否定する回答が多く、業務の円滑な推進の大きな妨げとなるような事例は発生していないようである。同時に、自らの業務に直接関係がなさそうであると判断したメールは、開封せずにいったん留め置いて、時間に余裕があるときに再度確認するというパターンが見いだせる。これに関連して、訓練の実施に関する具体的な改善の指摘として、あるメールが訓練であったことの周知（タネ明かし）については、訓練実施後に比較的速やかに行うことが求められているが、訓練を円滑に繰り返していくための留意点であろう。

表 22：訓練による実務とのコンフリクトについて

G氏	私ですか？訓練のせいで、というのはないですね。 体験は必要だと思うんです。結局、現場がリスクが大きいので。
H氏	それはないですね。ないですが、つい昨日、いらないメールはどんどん捨てたいのでメルマガ等。２～３日していなかったので、いや、もっとかな？昨日ちょっと過去のメールをばーっと見たら、一個どうしても覚えがない「あなたのパスワードを更新した」というメールがあって、それはどうしても、あれ？これなんだったけな？と思い出せなくて。で、アドレスを見て、うちの会社のっぽいと思って調べました。「電子稟議システム」のパスワードがわからなくなって自分でパスワード変更したんですが、それのリプライだった。でも、アドレスにちょっと覚えがなかったということがありました。
I氏	なんかその、どうなんだろう。ま、訓練やった後に、訓練でした、というメールが来てもいいのかな、と思います。うち（Z社）のやつはいいんですけど、グループ企業全体でやってるやつで、メールが来て、いかにも怪しくて、開けなかったんですけど、これ、業務的に開けなきゃいけなかったのか、どうなのかっていうのが悶々として。一応、ごみ箱には置いておきながら、あれって大丈夫だったのかな？答え合わせが来ない。だったら、そういうのだったら、１週間なりなんなり経過したら訓練でしたというのが来ればいいんですけど。結構、１か月後だかに来て、ねぇ。訓練だったら答えあわせしてくれてもいいような気がしますよね。
J氏	そこまではないんですが、まぁ、ちょっと、タイトルが文字化けしているのがたまに来ていたりして、そういうのはやっぱり、しばらく放っておいたりして、ちょっと時間があるときに過去のメールを見たら、ここからだったのか、これは、見ても大丈夫だったのか、というのはあります。
K氏	そうですね。それはないかな。

出典：筆者作成

最後に、組織のセキュリティ向上の取り組みを牽引する者、すなわちリーダーシップを発露する者はどのように認識されているのだろうか。これについての回答は表 23 の通りである。

Z社内の情報セキュリティを牽引する者についての質問では、まず「CSR：情報セキュリティ委員会」の名前が出てくると同時に必ず「事務局」という言葉が出てくる。セキュリティ体制の中心である CSR とともにその下部組織であるブロック単位の事務局というピラミッド構造がセキュリティを牽引するものと認識されていると言えよう。

表23：情報セキュリティの向上においてリーダーシップを発揮している者について回答

G氏	社長と言いたいところですが、社長ともいえますし、そもそもＩＳＯがトップマネジメントという意味で、社長方針が入っていますし、社長が最後バシっと絞めるところがあるので。 メインとしては、情報セキュリティ管理委員会（以下「CSR」）、ですかね。委員会メンバー。そのトップの委員長。会社としては、セキュリティ委員会ですね。そこが、事務局がちゃんとやっているか、チェック機能もあります。
H氏	肩書的にはCSR委員長。実務としてはやっぱり、事務局。 あとは、最近、会社の中で、情報セキュリティの重要性が増したといえば、やはり、セキュリティ・バイ・デザインという観点がうまれ、営業の人もセキュリティ系のことに関わりそうだとなると、電話をしてくる、相談してくる流れができているといえば、牽引されている。
I氏	ＣＳＲがまずあって。やっぱり、やっていいかどうかを、きちっと判断する。最近はいろんな技術も出てきていて、あんまりがちがちしすぎてもダメなんですが、緩くてもダメで、ＣＳＲが機能しているのは、一つあると思います。なかったら、全然違うと思います。情報セキュリティも含めて、事務局です。
J氏	情報セキュリティ担当。あと、職場に、担当者みたいのがいるので、その人が普段どれぐらい頑張っているかちょっとあれとして、そういう人がちょっと意識を近場にやっていると思います。 （その人たちに聞くことはありますか？） はい、私のグループの人が一回やっちゃった時に、聞いたことはありますね。これでよかったんだっけ？と。
K氏	そういう部署があるので、ＣＳＲとか、管理（筆者注：事務局のこと。K氏の職場・職域でのローカルな呼称）とか、それぞれの部署がありますから、その部署が牽引しているというものありますし、と、思っています。それなりのことはやっていると思います。あと、それぞれの管理部（注：事務局のこと）がありますので、そこがやっぱり営業が例えば個人情報を扱ってないよね、定期的にチェックしているので。 ・営業であれば、営業統括。管理部という部署があるものですから、そこが主導で、営業の中は、やっていますね。でも、会社としては、ＣＳＲとかがあります。そこが基本的に動いていると認識しています。

出典：筆者作成

では、この認識がどのように生まれたのかについては、セキュリティ・ファーストが内面化され、そこから表出したセキュアな「振る舞い」の具体例についての回答から紐解くことができる。

例えば、訓練の効果についての回答として見られた、

『このデータのもらいかた、いいの？と、どうするの？といったとき、まずはＣＳＲに確認しようというのが、ちゃんと浸透していると思います。うちの会社のなかに。やったことないケースだけど大丈夫かどうか確認しよう、というのは浸透していると思います（I氏）』

という回答や、ここでのリーダーシップに関する質問に対しての

『*営業の人もセキュリティ系のことに関わりそうだとなると、電話をしてくる、相談してくる流れができている*（H氏）』

というような回答である。

このように、実務的には手順が増え面倒なものであっても、セキュリティの確保のためにそれを省くことはしないという目に見える振る舞いが「浸透」「定着」していると認識されているのだが、それは、「相談」「確認」のカウンターとしての事務局とその背後にあるCSRを頂点としたセキュリティ体制が現実にしっかりと機能していることを同時に意味していよう。ここでの「相談」とは、業務の進め方についてセキュリティの面で疑義を持った時は、身近にある事務局に問い合わせを行うことであるが、

『*そこで集計をしている、というんですかね。その人たちが、ああだの、こうだの、というのではなくって、そこで集計して、セキュリティ委員会というのがうちの会社にあるので、そこでこうなっています、これはまずいんじゃないの？というのが書面で返ってくるので、なんとかしなさいとか、次回までには交渉するように、それは書面で返ってきます*（K氏）』

『*ＣＳＲがまずあって。やっぱり、やっていいかどうかを、きちっと判断する*（I氏）』

というように、事務局が直接に指示や回答するものだけではなく、内容によっては事務局がCSRに上程し、CSR内での議論を経て、判断が示されるというプロセスがごく一般的に認識されており、これが情報セキュリティに関わる仕事の組織的な進め方として共有されていることによると考える。むしろそれは、仕事を進める中で事務局に問い合わせるかどうか、すなわちセキュリティに関わるかどうかを判断するプロセスが常在していのるのであり、常に情報セキュリティが意識されている状態こそがＺ社の常態であり、また仕事の進め方そのものといえ、このセキュリティ体制の運用こそがＺ社そのものという見方ができるだろう。

一方で、

『*そこが、事務局がちゃんとやっているか、チェック機能もあります*（G氏）』

というように、各ブロックに設置される事務局に対してCSRが持つ統制機能の重要さを指摘する発言もあり、情報セキュリティのガバナンスの体系として認識し、理解されていることも伺える。

このように、情報セキュリティが自分事化され、セキュリティ・ファーストな業務の進め方をメンバー自ら求めるようになっているのだが、そのプロセスの中心にＺ社の情報セキュリティの体

制があり、その活動が日常業務においても実感できることが、目には見ることのできないセキュリティ体制に実体を与え、組織の標榜する情報セキュリティに対する価値観の内面化の促進を果たしている。そしてそれは、

『*職場に、担当者みたいのがいるので、その人が普段どれぐらい頑張っているかちょっとあれとして、そういう人がちょっと意識を近場にやっていると思います*（J 氏）』

というように、CSR を頂点として、ブロック単位に責任者が置かれ、その実働部隊としてセキュリティ担当者がブロック内に分散配置されていることが大きい。さらに、彼らが事務局を形成し、高い頻度で繰り返される標的型メール攻撃訓練と事前の教育の現場レベルの起点となっていること。そしてこの教育と訓練だけでなく、日常においてもセキュリティに関連する事項についての情報のハブとなっていることで、実務においても情報セキュリティの中心的な機能を果たすと同時に、現場で従業するメンバーの身近に存在し、その活動が目に見えるというこの仕組みこそが Z 社のセキュリティの象徴となっているのだ。教育と訓練とそれらの実施体制は、そのまま日常業務におけるセキュリティの体制であり、どちらも経営者層の参加が組織メンバーから見えることで、組織そのものの活動として認知されている。これらの総合的な結果として、

『*もう３年、やっていますよね。すごい浸透してきたと思います。そうですね。認知、認知度と重要度が増したのはこの２年、３年ていう感じですかね。本当は、うちの会社の一番大切な資源、資源というか、個人情報、お客様が預ける情報資産を扱う。そこが崩れちゃえば、会社としてダメになってしまうところを守るのが、情報セキュリティであったんですが、それまではかけ離れている、情報セキュリティは守るものという認識があまりなかった、つながっていなかったんですよね。それが密接なものだという認識になった*（H 氏）』

という評価が導かれているのだが、それは

『*社内に浸透したのは訓練のおかげでしょうか。絶対、全員が、パソコンを持っている人全員が参加なので、そういう意味で言えば、認知度を上げたのはこの訓練のおかげですね。*（H 氏）』

というように、経営者層を含めた組織メンバーの全員で訓練を繰り返し続けたことの成果であると認識されている。

(3)　考察の整理と結論

本節では、最後の課題としていた「セキュリティ文化は企業の中心的な文化となりえるのか」について検証すべく、前項において、ごく少数を対象にしたものであるがZ社の従業員に対して追加的なインタビュー調査を実施し、その回答を整理しながら多少の考察を加えた。本項ではその考察を整理して課題に対する結論としたい。

まず、業務の遂行においては、業務の種類を問わずしてPCを利用し、社内の情報システムを活用している。その業務時間内においては、おおよその時間、業務に利用されておりその依存度は非常に高いものであった。そして、社内外とのコミュニケーションツールとしての電子メールは、常にアプリケーションが利用されている状態であり、これもなくてはならないものであった。実際の利用状況は、受信数は1日当たり20通から200通と従事する業務によって大きな開きがあるが、業務として返信するものも最少の20通程度から70通程度、それに要する時間も合計で1時間程度というように、業務においても少なくない割合を占めている。これらを鑑みるに、情報端末と情報ネットワーク、そして電子メールを利用するにあたっての、情報セキュリティに対する認識と姿勢は非常に重要であり、組織として対応が必要である第1位の事象として挙げられていた標的型メールへの備えとしての教育と訓練は何より重要であることが改めて確認できた。

そして、その標的型攻撃メール訓練に対する認識こそが、本研究の関心のである情報セキュリティに対する認識向上、すなわちセキュリティ文化の醸成の起点となることが期待されているが、これについては、一様に「必要なもの」であるという認識であった。それは、2つの点からその必要性を認識していると考えられる。まず、日常でのメール利用における緊張感の維持という点である。そして、報告行動の定着という目的に対して、教育を通した手続き的知識の獲得だけでは不足であり、知識の構造化という点からも訓練を通した報告行動の体験が必要であるという一段深い認識も生まれていることによる。

これらは、メールを活用するにあたっての最低限のリテラシーとして、疑わしいメールの添付は開封しないというだけでなく、組織の情報セキュリティへの貢献には開封してしまった時の次善としての報告行動が重要であるということが正しく理解されていることの表れであろう。

報告行動の定着を目的とした訓練を繰り返すことは、このような認識を形成することが可能なのだ。

このような認識を導くに至った標的型攻撃メール訓練であるが、月1回という頻度についても一様に適当であるという認識であった。それは、情報セキュリティへの認識を維持するという点で

リマインドとしても有用であるという評価を伴っていた。この点で、教育と訓練という単一のチャネルによって情報セキュリティの認識の維持を図るためには、この程度の頻度によって喚起し続けることが必要であるのだ。ただし、高い頻度の訓練によって定期的に引き上げられるということだけではなく、メール利用についての注意喚起に自ら取り組む実践も生まれ、さらにそれが組織内に共有されるに至っていた。

ここまでは、訓練そのものに対する認識と、訓練の直接的な目的である報告行動の定着についてであるが、最終的な目標である情報セキュリティ認識の向上については、相当な位置に引き上げられたといえる。それは、訓練を重ねる中でメールを利用するにあたってしてはならないこと、するべきことを正確に認識し、それを着実に遵守することだけでなく、これらの認識を起点として情報そのものの取り扱い方についての認識に変化が現れていたことによる。

彼らは、教育と訓練を重ねるなかで、メールの利用方法のいかんによっては情報保護の弱点となり得ることを理解したと同時に、万が一に情報セキュリティインシデントが自組織において発生した場合のインパクトの大きさを認識し、それによって情報セキュリティの重要性を認識することで、情報そのものの扱い方の認識が変化していったと考えられる。

訓練を高い頻度で繰り返すことの効果として、メールの利用方法を意識し続けることになり、情報のやり取りの仕方そのもの、個人情報や機密情報の取り扱いを業の中核とするZ社においては仕事の進め方そのものに注意の焦点が移り、仕事と情報セキュリティが一体のものであるという認識になり、情報セキュリティの自分事化が図られたのだ。これは、セキュリティ文化の課題として挙げた、情報ネットワークの参加者として情報セキュリティに対する当事者性を持つことの難しさ、そして組織内でのリスク認識の統一の難しさがクリアされたといえる。

ここまでが、標的型攻撃メール訓練がどのように認識され、そしてどのような効果を生んでいるのか、そしてその効果をどのように認識しているのかについての整理と考察であった。ここからは、Z社において情報セキュリティを牽引する者に対する認識についてである。

回答者たちは一様に、「CSR：情報セキュリティ委員会」と「事務局」をセットで挙げていた。事務局は、職場に分散して配置される情報セキュリティ担当者の束であり、CSRはこの事務局を統合するものである。この頻度の訓練を支えている体制であり、またZ社の情報セキュリティ体制そのものといえる。それは、情報セキュリティに対する認識の維持に貢献する訓練の土台として、そして日常の業務において情報のより適切な取り扱いを参照する身近な存在として認識される事務局と、その事務局に影響力を適切に行使するCSRという構造として認識していた。Z社では、訓

練においては個人単位で報告先となる担当者が定められており、CSR を頂点として職場の隅々まで張り巡らされたネットワークであるが、担当者が非常に身近に存在するという点でもこのネットワークを認識しやすいということがこれを後押ししていた。さらに、名目だけではなく実質としてこのネットワークの頂点で責任を果たす経営者層を認知できていたことは何より意義があった。これこそが情報セキュリティに対する経営者層のコミットメントとして、メンバーに情報セキュリティを重視する姿勢が推認され、組織が重視するものの内面化を促進していたと考えられる。そして、メンバーはこの構造を十分に活かし、日常業務における情報資産の取り扱いをより適切にすることに結び付けていた。この構造の内部では、資産としての情報の取り扱いについての双方向の情報流通が果たされており、むしろ、社内における速やかな情報流通の状態こそをセキュリティ体制として理解していることが伺えた。

ここまでみてきたように、訓練が月 1 回という高い頻度で繰り返されることによって、標的型メールへの備えの認識が高い水準で維持され、訓練の成果として報告という振る舞いが定着しているというだけではなく、情報セキュリティ全体の向上の必要性の認識へと広がり、自らの仕事と情報セキュリティの関係性の理解が深まり情報セキュリティが自分事化されたこと、そしてその表出として仕事の進め方そのものが「セキュリティ・ファースト」なものへと変化していた。それは、訓練を通して自組織の情報セキュリティのあるべき姿の理解が深まり内面化が進んだことの表出だが、訓練の頻度が高いことで情報セキュリティに対する認識が維持されたことだけがその理由ではない。自らの業務の進め方がセキュアなものであるかを確認するという振る舞いや、事務局を経由して伝達される CSR からの指示を遵守するという姿勢は、事務局となる同僚が身近に存在していること、そしてその事務局を統括する情報セキュリティ体制が組織図上のものだけでなく実際に機能していることを認知できることの 2 点が内面化を支えたのだ。

このように、インタビュー調査における回答を整理し、考察を行った結果として、Z 社における標的型攻撃メール訓練を通じたセキュリティ文化の醸成活動の結果は次のようになる。

まず、Schein が提示する文化の三層モデルになぞらえるならば、Z 社の情報セキュリティを重視する経営者層の持つ価値観は、報告を重視する訓練と、現場の担当者－ブロック単位の事務局－全社的な CSR という、メンバーがその活動を目にし、実感できる活きたセキュリティ体制という人工物として表れていることが確認できる。経営者層の価値観は、この人工物である訓練に経営者層自らも参加し、その結果に注意を払い、体制と運用を支援するという振る舞いを通して組織メンバ

ーに認知され、体感されることによって、価値観が最上位であることがシンボリックに表現され、組織の中心となっている。

そして、これらの活動を通して、経営者層の持つ価値観に対する認知を深め、メンバーは情報セキュリティの自分事化、ここではセキュリティ重視の価値観が十分に内面化されている。それは情報セキュリティを優先する姿勢である「セキュリティ・ファースト」が、組織の内部における日常の会話に、そして業務中の振る舞いにおいて表出するに至っていることからもそう評価できる。これらにより、Z社の文化は情報セキュリティを中心的価値とした三層の文化として説明できるものになっている。

表24：Z社の情報セキュリティ文化の3層

文化の三層（Schein,1985）	見い出されたもの	確認された事例
人工物	訓練／組織体制	・ 報告をKPIとする高い頻度の訓練 ・ 報告先カード／事務局 ・ 担当者－事務局－CSRというセキュリティ体制
標榜する価値	経営者層の振る舞い	・ 訓練への参加 ・ 訓練結果への関心 ・ CSRの牽引
基本的仮定	セキュリティ・ファースト （メンバーの振る舞いとして	・ セキュリティ・バイ・デザイン／セキュリティ優先の営業活動 ・ 業務における事務局の活用／事務局への相談 ・ メール利用に際する注意喚起の共有 ・ 標的型メールに遭遇した際の初動の振る舞い

出典：筆者作成

そして、もう一つの文化的な視点として、Reason（1997; 2003; 2008）が提示する「安全文化」を下敷きに第III章で検討してきたセキュリティ文化の4つの下位文化の視点からは、Z社の文化は次のようなものである。

まず、訓練において求められる報告行動はもとより、業務において情報を処理するプロセスに関する情報が、現場から事務局を通じてCSRへ、そしてCSRから事務局を通じて現場へとスムーズに流通する体制を名実ともに備え、正しいデータ集積がなされていることは報告する文化が醸成されていることの現れとして。

正しいデータ集積のためにも、ヒューマンエラーの認識を改善し訓練の指標として開封率ではなく報告率を実装すること。そして、報告行動に重きがあることを訓練結果のモニタリングを通じて表現し続けることは公正な文化の現れとして。

現場に配置される担当者とその集合体である事務局に教育の運用を委任し、自らも訓練に参加し、訓練実務を担う CSIRT へのコミットメントを示す一方で、訓練結果へのフィードバックは怠ることなく、日常業務に対しても CSR を通じて事務局や各ブロックの活動のモニタリングを怠らず、管理監督の最終的な責任を持ち、方針決定に対しても適切に執行しているという経営者層の姿勢は柔軟な文化の表れとして。

そして、これら 3 の文化が醸成された結果としての CSR に集積されたデータを、より適切なプロセスへの改善に活用し、全社的に共有するというだけでなく、個人レベルにおいても認識を維持するためのベストプラクティスが組織の各所で生まれ積極的に共有する姿勢は、学習する文化の醸成として評価することができよう。

なによりも、情報セキュリティに対して当事者性を持つ、情報セキュリティが自分事化されているということは、自らの振る舞いが情報システム全体に影響を与えうることを理解している状態であると理解でき、これは中西（2007）が学習する文化の本来あるべき姿と指摘していた、システム思考を身に着けるという意味における「学習する文化」までもが醸成されていると評価できる。

繰り返される訓練とそれを実施する体制によって、情報セキュリティのあり方についての認識を共有し、それが内面化され、職種を問わずして同様の振る舞いが確認できるというだけでなく、訓練が高い頻度で繰り返されていることそのものがメンバーにとっては普通のこと、当然のこと、必要なものと仮定されていることは、訓練を通じて新しい文化を醸成するというだけでなく、訓練そのものが既に文化であるともいえよう。これらを踏まえ、Z 社の企業文化はこれまで本研究で検討してきた「セキュリティ・ファースト」がメンバーの内心として共有される「セキュリティ文化」であると考える。

VIII　結論

1 本論文の結論と成果

本研究のこれまでの議論と設定された課題、課題に対する企業事例を通した分析の結果を結論としてまとめたい。

本研究では、企業組織の情報セキュリティを向上させることについて、組織が標榜する価値が組織メンバーの内心において当然の仮定として共有されている状態として表現される組織文化からこれを捉え、組織のあらゆるメンバーが情報セキュリティに重きを置いた文化を醸成することの重要性を指摘し、情報セキュリティと企業組織の文化に関する議論を発展させるなかで、これを達成するための要件や要素を明らかにすることを目的とした。

それは、近年の情報端末とそれらを繋ぐ情報ネットワークの利用の急速な拡大がまずあり、それを組織の持続や発展に活用しようとする組織や、生活の利便の追求において漫然と利用する個人の間において、やり取りされる情報の漏洩や窃取を中心とした問題が発生し、その影響と規模は年々大きくなっていることによる。

そこで、情報を、そして情報端末と情報ネットワークを活用する際に持つべき注意深さを、企業組織に求められる情報セキュリティに対する当事者性として組織のメンバーに持たせることはできるのか、そしてこれを、マニュアルの書き換えによる行動パターンの変化としてではなく、組織が標榜する価値を組織のメンバーが内面化したことによる振る舞いの表出を追求するという視点で、その達成に向けてどのようにアプローチすべきかについてを、企業組織内で行われる教育と訓練を中心として検討することを主意として、論を進めることとした。具体的には、活動のあらゆる側面において情報セキュリティにプライオリティを置いた状態として定義した「セキュリティ・ファースト」が組織メンバーの内心において共有された仮定となり、この内心から情報セキュリティに重きを置いた振る舞いが表出するセキュリティ文化の醸成を目指して、まずは企業文化の醸成についての理論的な要件や要素を把握し、それらを教育と訓練やその周辺的な実務を担う組織的な諸要素に結び付け、置き換えながら要点を明らかにすることを試みた。

まず、企業組織の文化の醸成においては、マネジメントの質が大きく問われる。企業組織の文化とは、組織のメンバーが何を期待されるかを知り、いかに行動すべきかの判断基準（Deal & Kennedy,1982）とされ、それは、組織が標榜する価値を中心として、それらが具現化した表象物

（人工物）と、価値がメンバーに当然の仮定として内面化され、共有され、行動の基準となって振る舞いに表出された状態として説明される（Schein, 1985）。これを踏まえれば新たな文化の醸成とは、標榜する価値の変化に基づいた、組織メンバーが内心として持つ判断基準や当然の仮定の修正である。そしてこれは、採用する行動パターンの単なる変更ではなく、多くのメンバーにとっては従来までの仮定との接合であり、企業組織であればそれまでの業務の在り方との接合が目標となり、非常に大掛かりなものとなる。そして、こういった変化のキッカケとして、そして変化を推進するものとして有力であるのが教育と訓練とされていたことから、この教育と訓練のマネジメントに注目することとした。それは、教育や訓練の実施の内容や方法といった直接的な面だけでなく、実施主体や訓練対象者をも含めた組織全体のあり方といった教育と訓練のプロセス全体の一貫性が、変化に対する抵抗を抑制するためにまず求められる心理的安全の確保だけでなく、新しい文化の醸成そのものにおいて、間接的なものとして組織メンバーの内心に大きな影響を及ぼすからだ。

そして次に、どのような組織文化を醸成するべきなのかを検討した。現代的な企業組織が備えるべき文化として考えられるセキュリティ文化の、中核的な概念を提示したOECD（2002）によるセキュリティ文化は、情報端末と情報ネットワークを利用することで多様な利便を得る人々を参加者と呼び、利便の反対給付として情報セキュリティに貢献すべき「当事者」として、なにより情報セキュリティに対する認識の向上を訴えるものであった。

しかし、対象となる人々の範囲の広さ、リテラシーの格差などから、あくまで一般的で抽象的なものにとどまらざるを得ず、これを達成することにおける具体的な要件を提示するものではないこと、そして、情報と情報ネットワークの利用については、自らの振る舞いがすべての情報環境に影響を与えうるという認識になりにくい。そして、特に電子データそのものは、目で見ることはできない。さらに、情報インシデントによって自分の身体財産が直接的に侵害されることの想像が働きにくいことが特徴として挙げられ、これらが情報セキュリティに対する当事者性を個人に持たせることを難しくしていると考えられた。

このように、組織メンバーにとって当事者としてこれを認識しにくいという特徴をもつ情報セキュリティであるが、現代的な組織にとって、組織全体での情報セキュリティに対する認識の向上は喫緊に求められている。そこで、組織メンバーに情報セキュリティに対する当事者性が備わっている組織の状態とは具体的にどのような状態であるか、組織的な事故に関する研究者であるReason（1997）が提示した「安全文化」を下敷きにして、検討した。それは、①メンバーのより良い判断を行うための情報の流通を促進するために報告という振る舞いを重視する文化、②これを支える

ものとして、情報インシデントは外部の悪意が起点となってることを正しく理解し、これへの対処における失敗を叱責し、懲罰を課すことなく、失敗そのものの報告を促進する雰囲気が醸成されている文化、③情報セキュリティの向上にむけて、組織のヒエラルキーにこだわることなく適切な者がこれを担い、こういった者を組織全体が積極的に支援する文化、④より良い判断に向けてベストプラクティスを積極的に共有しようとする姿勢を持ち、組織全体に影響を与えうる当事者としてこれに関わろうとする文化である。そしてこれらの文化を土台として、組織内での種々の意思決定とその実践において、情報セキュリティの面で最適なものであることを志向し、組織の情報セキュリティに貢献するという振る舞いにあふれた状態であるとした。

そうした文化を、企業組織においてマネジメントの対象としてどのように醸成していくかが本研究の中心テーマであるが、企業組織のマネジメントである以上、マネジメントの成果の把握が関心事となる。特に教育や訓練は、従業員に対する中長期的な投資であるが、ここで問題になるのが成果をいかに測定し、把握するかである。これについては、文化そのものを成果の対象として測定することは、文化の本質はメンバーの内面であることから困難であり（Deal & Kennedy,1982）、さらには変化の度合いの把握を目的に新たな測定指標を設定することは、多様な活動を包含した組織では表面的なものにとどまってしまうという指摘（Schein, 1985）に留意しながらも、組織が標榜する価値が内面化された結果として表出したと考えられる振る舞いに注目して、これを代理指標として測定することが、事例などからも現実的な解であると考えた。

そして、セキュリティ文化を新たな企業文化として醸成していく具体的手段として、企業組織の文化の変革において特に有効とされていた教育と訓練に着目し、現代的な組織に求められる情報セキュリティの向上において課題の最上位となっている標的型攻撃のうち、その一例である標的型メール攻撃についての訓練を研究の焦点とした。そこで、標的型メール攻撃訓練の実際についての先行研究などから訓練の成果指標、いわゆる KPI の用い方や、組織の体制などの実務的な問題を整理した。

標的型メール攻撃とは、情報の窃取などを目的として、いわゆるウイルスなどを情報システムに侵入させる試みとして、対象となる個人や企業に電子メールを送信するものである。送信の対象となる個人や企業ごとにメールの件名や文面がカスタマイズされていることから、受信者は自身に関係あるものと誤認してしまい、電子メールの本文に記載された悪意あるサイトへ誘導する URL をクリックしたり、添付したファイルを開封してしまうことが起点となる。これに対する一般的な教育と訓練は、前提としてまず情報リテラシー全体の向上が目的であり、外部からの悪意としての標

的型メール攻撃については、数ある情報活用や情報セキュリティの一般的知識のあくまで一部でしかないことが多い。その中では、この標的型メールの特徴などを紹介し、それらの特徴から標的型メールであることを見極め、悪意を回避することが求められる。そして、これらの知識が獲得されたことを前提として、URL のクリックや添付ファイルの開封を問題的な行為として捉え、これを測定する訓練がおこなわれる。先行研究ではこういった訓練にもちろん一定の効果は認められた。しかし、一定の水準以上となることを期待することは難しいこと、そして、誤認に基づくこれらの行為を個人の過失とみなし、過失をゼロとすることに固執することがあれば懲罰に結び付きやすく、訓練そのものの忌避や、訓練実施者などの専門家への憎悪感情につながり、本来の目的とは逆の効果をもたらすことが懸念された。

これらを踏まえ、標的型メール攻撃訓練をセキュリティ文化の醸成を目的として効果的に実施し、運用していくためには、問題の解決として①KPI のあり方、②訓練頻度のあり方、③組織の体制のあり方、とくにこれはリーダーシップの発露のあり方として、これらはどのようなものが望ましく、実務的にどのように実装され、マネジメントされることが望ましいのかを、そしてこれらは、④文化の醸成や変革について理論的に求められていた要件や要素はどのような対応関係となるかを、最後に⑤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うるのかを、明らかにすべき課題として設定した。

これらの課題に対して、実際に標的型メール攻撃訓練を行っている企業組織に対してインタビュー調査を実施し、3 つの企業事例を組織サイズや訓練の発展段階を切り口として分析、考察し、比較を通して結論をだすことを試みた。

そして、これらの課題に対する企業事例の分析の結果と結論は次の通りとなる。

(1) KPI のあり方について

まず、訓練の KPI については、訓練の目的に応じた使い分けが必要である。訓練が初めての取り組みである場合や、訓練の経験が浅い場合、そして訓練の前段となる教育の浸透の程度、例えば標的型メール攻撃が実在することに対する認識の程度といった情報リテラシーの状態把握、すなわち組織内の状態の把握に用いるのであれば、クリックや開封といった行為を訓練の KPI に用いることは、ソフト的な仕掛けによって把握可能であり、訓練の実施主体にとっても負担が低く、妥当である。そして、一般的な情報リテラシー教育のなかでは十分にケアしきれない分野、たとえばこういった標的型メール攻撃に特化した教育コンテンツへの誘導という目的においても適当である。

しかし、訓練の最終的な到達点として、クリックや開封がゼロの状態を作ることを目標に、このKPIを用いた訓練を繰り返すことは、3社の事例においてもこれらをKPIに用いた訓練の結果は先行研究に整合的であり、一定の効果は当然に認められるがクリックや開封をゼロにすることはかなり困難であった。この点で、クリックや開封をKPIに用いることは、経営者層などのポリシー策定者がわかりやすい目標として「ゼロリスク」への固執をもたらし、結果に対する懲罰につながることが懸念されること、そしてこれにより訓練に対する忌避感情を引き起こしかねないことから望ましくないといえた。

訓練が、組織全体での情報セキュリティに対する認識の向上、ここでのセキュリティ文化の醸成のためにあるのならば、開封率の低減の追求とともに別のアプローチが必要であり、「報告」という振る舞いに焦点を当てたKPIが設定すべきである。これを訓練のKPIとして用いているZ社の事例からは、良好な訓練結果が持続しているとともに、報告という行為の必要性もメンバー自身に認識されていた。これは、訓練に報告という能動的な行為が伴うことで、自らの振る舞いが組織の情報セキュリティの向上に寄与しているという感覚がもたらされ、これが、自らも組織の情報セキュリティの当事者であることの認識となっていくということが考えられる。

(2)　訓練頻度のあり方について

適切な訓練の頻度については、訓練の目的とKPIの設定に依存することになるが、訓練の目的が、組織の状態把握やリテラシー向上の一環であるならば、教育コンテンツの改訂やその他の教育研修などとの兼ね合いから随時に実施することが望ましいだろう。企業組織であればメンバーの変化もあることから、新しいメンバーがこれらから漏れないように留意することも求められる。

訓練の目的が、セキュリティ文化の醸成、実務的には組織全体での情報セキュリティに対する認識の維持・向上のためにあるのならば、「報告」をKPIとした訓練をひと月に1度程度という頻度が望ましい。これは、訓練対象者へのインタビューにおける発言からも彼らの実感として認識の維持に「必要」として表現されていたことによる。

しかし、これだけの頻度で行われる必要があると、訓練内容の品質の維持や、訓練のKPIである報告の「受け付け」の問題につながるため、訓練を実施するための組織的な体制が問題となる。

(3) 体制のあり方（リーダーシップのあり方）について

セキュリティ文化を醸成する目的において、高い頻度で訓練を実施していくために求められる体制は次のようなものであった。

まず、訓練においては、報告エスカレーションルールの基本となるセキュリティの体制が求められる。Z 社では、第Ⅶ章での個人に対する調査日現在で、3 年半という期間にほぼ毎月 1 回のペースで標的型メール攻撃訓練が繰り返されているが、この驚異的な頻度を可能にしたのがセキュリティ体制であった。組織を任意の単位で分割し、分割された単位の総責任者と共にこれを補佐する数名の実務上の責任者、そして現場レベルでの実働部隊となる補助者というという体制は Y 社と同様であるが、この組織の隅々に埋め込まれている補助者が事務機能を担えるよう事務局と銘打って組織している点が特筆であった。組織全体では、川上を経営者層や総責任者が参加する全社的な委員会が、川中を CSIRT が、川下を事務局が担うという全体像となり、訓練実施のプロセスにおいても役割分担を可能にし、事務局が報告の受付を担うことで、X 社・Y 社で懸念されていた報告の受付という実務的問題が解消され、高い訓練頻度が確保されていた。

そして、組織の隅々に埋め込まれた補助者とその集合である事務局が、訓練だけでなく日常業務のなかでも情報セキュリティに関する情報の収集、発信、共有において効果的に機能することにより情報セキュリティに対する認識が向上し、日常の業務と接合を果たし、組織メンバーの当事者性が向上していたのだ。

このように組織を分割し、責任単位を小規模化したなかでのセキュリティ体制の構築は、組織がより大きくなり管理するアカウントが増えることへの現実的な対応でもあるが、それだけではなく、メンバーにとっては組織的な取り組みの中での自らの位置が明確になり、取り組みとの距離感も近くなることで、名ばかりではなく活きたもの体制として認識され、自らもこれに関与しているという実感を生み、当事者性の向上にも寄与していると考えられる。

標的型メール攻撃訓練が、この体制の下で高い頻度で繰り返されることによるメンバー個人に対する効果としては、メンバー個人へのインタビューで確認したように、3 つ認められた。1 つ目としては、訓練そのものの直接的な目標である標的型メール攻撃への対処が浸透することである。まずは、LAN ケーブルを抜くこと、操作の中止、報告という 3 段階の初動が正しく理解されており、これは報告率がほぼ 100%に近いという結果からも効果として明確である。情報セキュリティ分野において組織に必須の対応の第 1 位として挙げられていた標的型攻撃の一種である標的型メール攻撃への備えが、知識レベルと行動レベルにおいて確実に獲得され、定着できることが確認できた。そしてこれは、文化の単なるマニュアル化ではなく、メンバーの発話に「これは我々に必要なことである」とあったように、当然の仮定として内心から表出していると考えられる。

２つ目に、組織全体としての情報セキュリティ体制が具体的に認知されることである。繰り返される訓練の目的である報告行為の徹底を通じて、その受付窓口としての担当者が身近に存在することが認知されるというだけでなく、担当者の集合的存在としての事務局、そして事務局を統括する情報セキュリティ委員会が最上位に存在しており、これに経営者層が参加していることも訓練の結果に対するフィードバックがあることから認識できている。さらに、身近な同僚が参加する事務局の活動を通じて、情報セキュリティ委員会に参与する経営層が訓練の結果について興味関心を持っていること、結果の改善について具体的な働きかけがあることを認知できることが、次の３つ目の効果である内面化を後押ししている。

そして３つ目として、情報セキュリティに対する当事者性の向上である。それはもともと関連のあるものとして認識されていなかった情報セキュリティと日常業務の接合として現れており、訓練の受付窓口というだけでなく、日常の業務遂行においても身近な担当者と事務局を活用することで「情報セキュリティがどう在るべきか」が共有され内面化されるに至ったのである。そして、それが情報セキュリティを優先する姿勢である「セキュリティ・ファースト」として現れている。

これは、訓練によって意識づけられ、日常の業務においても積極的に活用されている職場のセキュリティ担当者として機能する「身近な同僚」の働きが大きい。この身近な同僚を通じて、自らの業務の情報セキュリティに関連する側面を認識し、さらに彼らを通じて情報セキュリティ委員会との具体的なやり取りがあることで全社的なセキュリティ体制とのつながりが実感できることである。

これらは、先の訓練における報告受付の担当者が、日常の業務における情報の取り扱い方に関する身近な問い合わせの窓口として、そしてセキュリティ委員会が責任ある情報発信元として機能することで、具体的な形で情報セキュリティが日常業務の遂行の中心軸となっていることを体感することによって生まれたものである。

本研究は、教育と訓練を中心に文化の醸成を検討してきたが、この結果からは、教育や訓練によって注意が喚起されるだけでは、ここまで到達することはないだろう。散発的な訓練の独立的な実施ではなく、継続的に実施する機構とそれを支える組織の体制が存在すること、そしてその活きた体制との距離感の近さによって生まれた認識であるからだ。

このような体制が運用されるなかで、確認されたリーダーシップは次のようなものであった。

まず、訓練実施の起点となる CSIRT の、情報セキュリティの専門家によるリーダーシップとして、標的型攻撃のトレンドをキャッチし工夫を凝らした訓練と、訓練結果を仔細に分析し、そこか

ら得られた知見を反映して素早く丁寧にコンテンツが改訂される教育とを牽引する専門家の情熱と強いリーダーシップであった。

これに対する、経営者層のリーダーシップは、訓練においては、専門家への委任、訓練結果に対するフィードバックという形で表現されていた。日常においては、全社的なセキュリティ体制の頂点において、肩書だけでなく実態として積極的に関与していることがメンバーからも認識されていた。これらは、表立ち、外部環境変化への対応を力強く鼓舞する強いリーダーシップではなかった。情報セキュリティを重視しているという姿勢が、経営者層の日常の振る舞いに垣間見えるというシンボリックな表現である。これら２つのリーダーシップが相乗して組織の文化がセキュリティ文化となるよう導いていた。

一例ではあるが、訓練を中心としてセキュリティ文化を醸成していくことにおいて求められるリーダーシップは、このようなあり方が求められる。

(4) 文化の醸成や変革に求められる要件と要素

本研究で扱ったＺ社の事例からは、文化の醸成に求められる「コミュニケーションの一貫性」「褒賞」という２つの要件は、①訓練への経営者層も含めた全員参加（選択と参加）、②訓練結果へのコミットメントによって示される訓練の正統性と、組織全体に張り巡らされたネットワーク状のセキュリティ体制が運用されるなかで、経営者層が名実ともに活動しているというシンボル性（シンボリックなアクション）、③日常の業務において情報セキュリティとの接点となる担当者が身近に存在する組織体制が作られていること（他者からの情報）、④経営者層の訓練結果へのフィードバックとこれによって生まれるより良い結果への競争心、そしてこのセキュリティ体制を活用してセキュリティ・ファーストな業務推進を行うことそのもの（包括的な褒賞）、が要素として見いだされ、満たされていた。

また、文化の変革としてこれを捉えると、「目標の明確化」、「多くの社員と取り組む」、「過度に管理しない」という３つの要件は、①訓練の KPI を開封率から報告率に転換し現実的な目標として設定しなおしたこと、これが、訓練を経験する中で問題を認識し、その解決として自らで進めたこと（メンバー間の合意）、②これによって問題の焦点が、開封という過失から報告しないという不作為に移ることで心理的安全が確保され信頼関係の基礎となったこと、これと同時に、報告という振る舞いが求められることになり、訓練に対する当事者性が生まれたこと（信頼関係）、③心理的安全が確保された訓練が組織の全員参加において長期間・高頻度で行われ続けていること（技術の養成）、④報告率 100%の達成を目指して訓練を工夫し、結果を仔細に分析し、教育を細

やかに改訂し続けていること、そして訓練の実施、日常のセキュリティ体制の運用は、メンバーの身近な人物が多く参加することで専門家だけのものでないことが認識されていること（忍耐）、⑤教育と訓練を推進する専門家への委任と、組織を分割したブロック単位に教育の実践を委ねること（柔軟性）、などが要素として見い出され、満たされていた。

これだけではなく、Z社の事例では、組織体制にブロック制を採用し、「過度に管理しない」ことによる柔軟性と自主性によって、訓練結果に対するゲーム性や競争心が生まれ、これらが訓練そのものを継続する、言い換えれば文化の醸成活動に持続性を与える効果的な要素となっていることが考えられた。このため、文化の醸成において求められる要素にゲーム性や競争心を加えることを提案した。

(5) 「セキュリティ文化」は企業組織の中心的文化となるか

これまでに述べた4つの研究課題に対する結論、事例を通して確認され、考察された状態は、組織メンバー自身からはどのように認識されているのか、すなわち「セキュリティ・ファースト」が内面化され、振る舞いとして表出しているのか、それらは第Ⅲ章で検討したセキュリティ文化であると言えるのかを、少数ではあるがメンバーに対するインタビュー調査を通してこれを明らかにすることを試みた。

この調査でのメンバーの発話からは、頻度の高い訓練そのものも日常に取り込まれ、自分たちに当然に必要なものであるという認識に至っていること、そしてこれによって、日常の業務においても情報セキュリティにプライオリティを置くことを当然のこととし、これに従った振る舞いにあふれていることが確認できた。それは、訓練を通じて獲得された「標的型メール攻撃への備えが重要である」という認識が、月に1度という頻度の訓練によって維持されることによって、情報セキュリティ全体への認識として拡がり、日常の業務と接合を果たしているというものであった。これらから、結論として、標的型メール攻撃訓練は、企業組織におけるセキュリティ文化の醸成に正の効果を多分にもたらしており、セキュリティ文化は、訓練という文化的要素を変化させ、継続して運用するというマネジメントを通じて企業組織の中心的な文化として醸成しうるとした。

ただし、訓練だけではなく、この訓練頻度を支える組織的なネットワーク、ここではセキュリティ体制を構築するというマネジメントが併せて求められる。このセキュリティ体制に対する認識が同時に影響を与えていたからである。メンバーの日常に距離感近く担当者が存在し、事務局として情報セキュリティに貢献していると認知されていることがまずある。そしてこの事務局に対する全社的な委員会からのフィードバックがガバナンスの一部として認識されていたように、セキュリテ

ィ体制の責任者である経営者層の責任が、規定上の形式的なものではなく実質的に果たされていると認知されていたことが大きい。これによってセキュリティ体制そのものが生きた組織体制として認識され、組織の目指す方向を示すもの、ここでは「セキュリティ・ファースト」を標榜するシンボルとなっていた。

これらは、情報セキュリティへの経営者層の関心の表れであり、セキュリティ担当者をエンパワーメントし、継続的な教育と訓練の実施を支援し、その結果に関心を払い、時には現場を叱咤激励することを通じて、情報セキュリティを重視する一貫した姿勢を示すマネジメント層のコミットメントを示すものである。そして、エンパワーメントを受けたセキュリティの実務担当者が、継続的な教育と訓練を牽引する一方で、教育の実践については現場の裁量に委ねるという柔軟性を備えたプロセスが展開された結果である。

このように、企業組織内の教育と訓練という文化的要素の在り方を変革し、それを継続し、改善し続けることを通じて、情報セキュリティが当然に優先されるという仮定を共有することに成功したのである。この継続的な訓練の実施については、組織体制が大きく貢献しており、これこそがメンバーにとって身近な情報セキュリティのシンボルであると同時に、日常的な実務の遂行にも深く根差していることで、情報セキュリティに対する当事者性を持つことを可能にしたといえる。この組織の情報セキュリティに対して当事者性を持つことの難しさは、情報セキュリティの特徴の一つとして指摘したが、Z社の事例ではこれを克服していた。それは、情報セキュリティを重視するという経営者層が標榜する価値を中心に、情報セキュリティの体制が人工物として位置し、有事の際には報告するという振る舞いが徹底して取られるというだけでなく、平時においても情報セキュリティを軸とした業務の進め方を追求することが自然の振る舞いとして表出する企業文化となっていた。

以上の事から、セキュリティ文化は企業組織の中心的な文化となりえるかという課題について、セキュリティ文化は企業組織の中心的な文化となりえると結論付けた。

これらを明らかにしたことが、本論文の成果である。

2 本研究の限界と課題

これまで繰り返し述べてきた通り、企業組織においては情報の活用が持続的な成長の鍵であり、そのため情報セキュリティの重要性は増すばかりである。そして、情報セキュリティにおいて完全なものはあり得ず、不断の努力が求められている。もし、仮に、完全だと自認するようなものがあ

るとするならば、文学のものであるが「完全すぎるものは、崩壊の過程に現れる現象の一つにしかすぎないのだ」（安部, 1982, p.227）という哲学的な文を借りて警句としたい。情報セキュリティに対する脅威として、悪意ある攻撃者側の知恵や技術が防御側を常に上回っており、事後的な対処となることはやむを得ない状況にある。そしてこれは、情報システムやネットワークといったいわゆるサイバー空間の対処だけでなく、物理的な媒体であってもソーシャルエンジニアリングなど、利用者の過失を誘発し、注意喚起するだけでは防ぐことは難しいものがあるからだ。そのため、事後的であっても気づくことができ、早急に報告し、被害を低減するための努力は、不断の、そして当然のものとして組織メンバーに備わるべき要件として、組織はこれを維持し続ける必要がある。本研究では、教育や訓練をその中心的手段としたが、教育や訓練は、一般的には企業独自のノウハウであり、またその結果が個別に公表されることは考えにくい。これら教育と訓練の実態を、その発展段階に沿って仔細に確認し、分析できたこと、そして一つの例ではあるが理想に近い組織の状態がマネジメントによって到達可能であると示せたことは、実務においても理論においても貢献だと考える。

ただし本研究において扱った事例は 3 社と少ないこと、企業規模からみればいずれも大規模な企業組織であり、日本国内に存在する企業全体のなかで多くを占め、近年では情報セキュリティに対する対処の遅れが指摘されている中小企業への汎用化、一般化という点では難があるとも考えられる。しかし、多様な人々による多様な仕事が集積しているという点は同じであり、むしろ組織サイズが小さいことは、何らかの組織的な課題に対する当事者性の認識を持つことや、経営者層との距離の近さによって価値の共有を図ること、そして全社的な制度の一貫性を担保することにおいては有利であると考えられ、本稿で取り上げた情報セキュリティの側面だけでなく、メンバーの社会性によって組織的な課題を解決しようとする際の助けとなることを期待する。

一方、本研究の今後の課題として以下が挙げられる。まず、文化の醸成の程度を検討するにあたり、組織メンバーの認識について確認するため、メンバーに対する質的調査によってこれを試みたが、その数も少数であり、発話のコード化やそれに基づく分類といったような精緻な分析手法に基づいた結論の導出ではない。文化を測定することについては、その手法を含め種々の問題があることが指摘されているが、質的研究手法の充実とともに量的なアプローチの検討が課題となる。

そして、扱った企業事例からは、これらの教育と訓練は、情報セキュリティに対する認識を向上させ、セキュリティ文化の醸成に十分資すると結論付けたが、教育や訓練の実施主体やこれらを取り巻く組織的な体制といったその他の文化的要素に大きく依っていることも見出された。これを踏

まえれば、メンバーの認識に影響を与えるものは、当然これらにも限られないのであり、より広範な要素を探り、要素間の相互的な影響に焦点を当てた研究を重ねていくことが必要だと考える。

そのため、より多くの企業実践を確認し、まず教育と訓練の内容の高度化についての、教育や訓練そのものの評価として触れた Kirkpatrick の 4 段階モデルからの整理や、通時的な分析が課題となる。そして、これらの活動を直接的に担う CSIRT のような専門組織の成熟と、これらの結果としての組織全体での情報セキュリティの成熟といった複数の視点を同時に持ちながらの、文化の醸成の段階をより精緻化することを今後の課題としたい。

引用・参考文献

調査資料・報告書

経済産業省 商務情報政策局 情報経済課（2019）「平成 30 年度我が国におけるデータ駆動型社会に係る基盤整備（電子商取引に関する市場調査）」
https://www.meti.go.jp/press/2019/05/20190516002/20190516002-1.pdf

経済産業省 商務情報政策局 情報経済課（2020）「令和元年内外一体の経済成長戦略構築にかかる国際経済調査事業（電子商取引に関する市場調査）」
https://www.meti.go.jp/press/2020/07/20200722003/20200722003-1.pdf

経済産業省 商務情報政策局 情報セキュリティ政策室・情報処理振興事業協会 セキュリティセンター（IPA/ISEC）（2002）「情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて－新 OECD 情報セキュリティ・ガイドラインの概要－」
http://www.mofa.go.jp/mofaj/gaiko/oecd/security_gl_a.html

デジタルアーツ（2019）「勤務先における標的型攻撃対策に対する意識・実態調査」
https://www.daj.jp/company/release/common/data/2019/042401.pdf

東京電力ホールディングス（2015）「原子力安全改革プラン進捗報告（2014 年度第 3 四半期）」
https://www.tepco.co.jp/cc/press/betu15_j/images/150203j0102.pdf（2019 年 11 月 1 日アクセス）

ベライゾン（2016）「データ漏洩／侵害調査報告書」

IAEA Safety Series No. GSR Part 3. “The Management System for Facilities and Activities” (2006)
http://www-pub.iaea.org/MTCD/publications/PDF/Pub1252_web.pdf.

JIPDEC(一般財団法人日本情報経済社会推進協会
https://privacymark.jp/news/other/2018/1101.html（2018 年 12 月 1 日アクセス）

JNSA（2019）「2018 年情報セキュリティインシデントに関する調査報告」
https://www.jnsa.org/result/incident/data/2018incident_survey_sokuhou.pdf

JPCIRT/CC（2008）「標的型攻撃対策手法に関する調査報告書」
https://www.jpcert.or.jp/research/2008/inoculation_200808.pdf

NRI セキュアテクノロジー（2017）『過去 1 年間で発生した事件・事故』企業における情報セキュリティ実態調査 2017

World Association of Nuclear Operators（2013）*Traits of a Healthy Safety Culture*, PRINCIPLES.

海外文献

Alhogail, A. and Mirza, A.（2014） Information Security Culture: A Definition and a Literature review, *Comput,* Appl. Inf. Syst., pp.1-7

Ansoff, H. I.（1979）"*STRATEGIC MANAGEMENT,*" Palgrave Macmillan.（中村元一 監訳 田中英之・青木幸一・崔大龍 訳：2007『アンゾフ　経営戦略論　新訳』中央経済社）

Bandura, A.（1974）"*SOCIAL LEARNIMG THEORY*," Prentice-Hall, Englewood Cliffs（野原広太郎　訳（1979）『社会的学習理論　―人間理解と教育の基礎―』金子書房）

Barnard, C.（1938）"*The functions of the executive*," Cambridge, Harvard（山本安次郎・田杉競・飯野春樹 訳（1968）『経営者の役割』ダイヤモンド社）

Bierly, P. E. & Spender,C.（1995)Culture and high reliability organizations: The case of the nuclear submarine, *Journal of Management*,Vol.21, No.4, pp.639-656

Bock, P. K.（1974）*Modern cultural anthropology: An introduction*, Alfred A. Knopf（江渕一公　訳『現代文化人類学入門（１）』講談社学術文庫）

Bourrier, M.（1996）Organizing Maintenance Work At Two American Nuclear Power Plants, *Journal of Contingencies and Crisis Management*, Vol.4, No.2, pp.104-112

Broms, H. & Gahmberg, H.（1983）Communication to Self in Organizations and Cultures, *Administrative Science Quarterly*, Vol.28, No.3, pp.482-495

Caldini, R.（1984）"*Influence: The New Psychology of Modern Persuasion*," Quill, New York

Child, I. L.（1954）Socialization, *Handbook of social psychology II*, Addison-Wesley Publishing.

Child, I. L.（1969）Socialization, The individual in a social context, *The handbook of social psychology III*, Addison-Wesley Publishing

Child, J.（1977）"*Organization: A choice for Men*," Harper & Row

Da Veiga, A. and Eloff,J. H. P.（2010）A framework and assessment instrument for information security culture, *Comput. Secur.*, vol. 29, no. 2, pp.196-207

Deal, T. E., Kennedy, A. A.（1982）"*Corporate cultures: The rites and rituals of organizational life*," Addison-Wesley（城山 三郎 訳（1983）『シンボリック・マネジャー』新潮社）

Eisenhardt, K.M.（1989） Building theories from case study research, *Acad Manage Rev*, Vol.14, No.4, pp.532-550

Geertz, C.（1973）"*The Interpretation of Culture*," Basic Books.（吉田禎吾・中牧弘允・柳川 啓一・板橋 作

美　訳(1987)『文化の解釈学１』岩波現代選書）

Gregory, K. L. （1983） Native-View Paradigms: Multiple Cultures and Culture Conflicts in Organizations, *Administrative Science Quarterly*, Vol.28, No.3, pp.359-376

Hofstede, G. (1980) *Culture's consequences*, Beverly Hills, Sage（萬成博・ 安藤文四郎 訳（1984）『経営文化の国際比較―多国籍企業の中の国民性』産能大出版部）

Hofstede, G. (1980) *Cultures and Organizations*, M. E. Sharpe, Inc.（岩井 紀子, 岩井 八郎 訳『多文化世界―違いを学び共存への道を探る』有斐閣）

Jelinek, M., Smircich, L. and Hirsch, P. (1983) A Code of Many Colors, *Administrative Science Quarterly*, Vol.28, No.3, pp.331-338

Kirkpatrick, D. L. (1959) Techniques for evaluating training programs, *Journal of the American Society of Training Directors*, Vol.11,pp.1–13

Kirkpatrick, D. L. & Kirkpatrick, J. D. (2005) *EVALUATING TRAINING PROGRAMS: The Four Levels Third ed.* Berrett-Koehler Publishers Inc., San Francisco

Kotter, J. P.（1996） *Leading Change,* Harvard Business School Press（梅津祐良 訳（2002）『企業変革力』日経BP 社）

Kotter, J. P.（2008） *A SENSE OF URGENCY,* Harvard Business School Press（村井章子 訳（2009）『企業変革の核心』日経BP 社）

La Porte, T. R. (1988) The United States air traffic control system: increasing reliability in the midst of rapid growth, *Institute of Governmental studies*, University of California Berkeley.

La Porte, T. R. (1996) High Reliability Organizations: Unlikely, Demanding and At Risk, *Journal of Contingencies and Crisis Management*, Vol.4, No.2, pp.60-71

La Porte, T. R. & Thomas, C. W. (1995) Regulatory Compliance and the Ethos of Quality Enhancement: Surprises in Nuclear Power Plant Operations, *Journal of Public Administration Research and Theory*, Vol.5, No.1, pp.109-138

Linton, R. (1945) *The cultural background of personality*, Appleton-Century（清水幾太郎, 犬養康彦 訳（1952）『文化人類学入門』東京創元社）

Macmillan dictionary of anthropology (1876) Macmillan

Mahfuth, A., Yussof, S., Baker, A. A., Ali, N.（2017） A Systematic Literature Review Information Security, IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8002442（最終アクセス 2020/7/31）

Mayer, R.C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review*, 20, 709-734

McGregor, D.M. (1960) *The Human Side of Enterprise,* McGraw-Hill（高橋達男 訳（1970）「企業の人間的側面」産能大学出版部）

Milgram, S. (1969) *Obedience to Authority,* Harper & Row, New York

Nadler, D. A.（1998）"*Champions of Change*," Jossey-Bass,（斉藤彰悟 監訳 平野和子 訳（1998）『組織変革のチャンピオン：変革を成功に導く実践ステップ』ダイヤモンド社）

O'Reilly, C. (1989) Corporations, Culture, and Commitment: Motivation and Social Control in Organizations., *California Management Review,* vol.31, No. 4, pp.9-25

Peters, R. G., Covello, V. T., McCallum, D. B.（1997）The determinants of trust and credibility in environmental risk communication: An empirical study, *Risk analysis*, vol.17, No.1, pp.43-57.

Ponemon (2018) Cost of data breach study: Impact of business continuity management. https://www.ibm.com/downloads/cas/AEJYBPWA

Reason, J. (1997) *Managing the risk of organizational accidents*, Ashgate Publishing Limited.（塩見弘 監訳 高野研一・佐伯邦英 訳（1999）『組織事故 －起こるべくして起こる事故からの脱出－』 日科技連出版社）

Reason, J.（2003）*Managing Maintenance Error,* Ashgate Publishing.（高野研一・弘津祐子・佐相邦英・上野彰 訳（2005）『保守事故』 日科技連出版社）

Reason, J.（2008）*The Human Contribution: Unsafe Acts, Accidents and Heroic Recoveries,*" Ashgate Publishing.（佐相邦英 監訳・電力中央研究所ヒューマンファクター研究センター 訳（2010）『組織事故とレジリエンス 人間は事故を起こすのか, 危機を救うのか』 日科技連出版社）

Redfield, R. (1941) *The folk culture of Yucatan*, Chicago Press.

Rochlin, G. I., La Porte, T. R., Roberts, K. H.(1987) The self-designing high-reliability organization aircraft carrier flight operations at sea, *Naval War College Review,* Vol.40, No.4, pp.76-92

Schein, E. H.（1978）*Career Dynamics: Matching Individual and Organizational Needs*, Assison-Wesley.（二村敏子・三善勝代 訳（1991）『キャリア・ダイナミクス』白桃書房）

Schein, E. H.（1985）*Organizational Culture and Leadership*, Jossey－Bess（清水紀彦・濱田幸雄 訳（1989）『組織文化とリーダーシップ』ダイヤモンド社）

Schein, E. H.（1988） Organizational socialization and the profession of management, *MIT Sloan Management Review,* Vol.30, No.1, pp.53-65

Schein, E. H.（1996） Three Cultures of Management: The Key to Organizational Learning, *Sloan Management Review,* Vol.38, No.1, pp.9-20

Schein, E. H.（1999） *The Corporate Culture Survival Guide,* Jossey－bass（金井壽宏 監訳 尾川丈一・松本美央 訳（2004）『企業文化 －生き残りの指針－』白桃書房）

Schein, E. H.（2009） *The Corporate Culture Survival Guide,* John Wiley & Sons（尾川丈一 監訳 松本美央 訳（2016）『企業文化[改訂版]ダイバーシティと文化の仕組み』白桃書房）

Senge, P. M. (1990) *The Fifth Discipline: The Art & Practice of The Learning Organization,* Random House Business Books （守部 信之 訳（1995）『最強組織の法則-新時代のチームワークとは何か-』徳間書店）

Sharp, J.（2007） *The Route Map to Business Continuity Management: Meeting the Requirements of BS 25999*, BSI Standards

Smircich, L.（1983）Concepts of Culture and Organizational Analysis, *Administrative Science Quarterly*, Vol.28, No.3, pp.339-358

Spitzner, L.（2014）*Making Awareness Stick* https://www.sans.org/sites/default/files/2017-12/STH-Presentation-MakingAwarenessStickv2.pdf（最終アクセス：2020年8月23日）

Snyder, M. & Swann, W. B.（1978）Hypothesis-testing processes in social interaction, *Journal of Personality and Social Psychology*, Vol.36, pp.1202-1212

Sterman, J. D.（2000）*"Business Dynamics: Systems Thinking and Modeling for a Complex World,"* McGraw-Hill Professional,（小田 理一郎・枝廣 淳子 訳（2009）『システム思考』東洋経済新報社）

Taffinder, P.（1998）*"Big Change,"* John Wiley & Sons, 1998.（チェンジ・マネジメント・グループ 訳（1999）『ビッグ・チェンジ』東洋経済新報社）

Thompson, J. D.（1967）*"Organizations in Action: Social science bases of administrative theory,"* McGraw-Hill（鎌田伸一・二宮豊志・新田義則・高宮晋 訳（1987）『オーガニゼーション イン アクション』同文館出版）

Tushman, M. L. & O'Reilly, C. A.（1997）*"Winning Through Innovation,"* Harvard Business School Press（斎藤彰悟　監訳, 平野和子 訳（1997）『競争優位のイノベーション』ダイヤモンド社）

Vogel, E. F. (1979) *"Japan as Number One: Lessons for America,"* Harvard University Press.（邦訳書：広中和歌子・木本彰子 訳（1979）『ジャパン アズ ナンバーワン: アメリカへの教訓』TBS ブリタニカ）

Von Solms, R. & Van Niekerk, J. (2013) From information security to cyber security, *Computers & Security,* Vol.38, pp.97-102

Von Solms, B. & Von Solms, R.（2018）Cybersecurity and information security - what goes where?, *Information & Computer Security,* Vol.26, No.1, pp. 2-9

Weick, K. E.（1995）*Sensemaking in Organizations,* SAGE Publications, Inc.(遠田雄志 ・西本直人 訳（2001）『センスメイキング イン オーガニゼーション』文眞堂)

Weick, K. E. and Sutcliffe, K. M. (2001) *Managing the Unexpected: Assuring High Performance in Age of Complexity 1st Edition*, Jossey-Bass.（西村行功訳 (2002)『不確実性のマネジメント：危機を事前に防ぐマインドとシステムを構築する』ダイヤモンド社)

Weick, K.E. and K.M. Sutcliffe (2007) *Managing the Unexpected: Resilient Performance in an Age of Uncertainty 2nd Edition*, Jossey-Bass.

Weick, K.E. and K.M. Sutcliffe (2015) *Managing the Unexpected: Sustained Performance in a Complex World 3rd Edition*, Jossey-Bass.（中西晶 監訳, 杉原大輔・高信頼性組織研究会 訳（2017）『想定外のマネジメント：高信頼性組織とは何か』文眞堂)

Weick, K.E.（1987）Organizational Culture as a Source of High Reliability, *California Management Review,* Vol.29, No.2, pp.112-127

Weinstein, N.（1980）Unrealistic Optimism about Future Life Event, *Journal of Personality and Social Psychology,* Vol.39, No.5, pp.806-820

West-Brown, M. J., Stikvoort, D., Kossakowski, Klaus-Peter, Killcrece, G., Ruefle, R., and Zajicek, M. (2003)『*Handbook for Computer Security Incident Response Teams (CSIRTs) 2nd ed*』., Carnegie Mellon University. (http://www.sei.cmu.edu/reports/03hb002.pdf : 2003 年 4 月),（有限責任中間法人 JPCERT コーディネーションセンター 訳, http://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf, 2013 年 3 月 21 日).

Yin, R. K.（1994）"Case Study Research: Design and Method".（近藤公彦 訳（2011）新装版『ケーススタディの方法　第 2 版』,千倉書房)

Zakaria, O.（2006）Internalisation of information security culture amongst employees through basic security knowledge, *IFIP Int. Fed. Inf. Process.*, Vol. 201, pp. 437-441

国内文献

安部公房（1982）『箱男』新潮文庫

池田浩・三沢良（2012）失敗に対する価値観の構造－失敗感尺度の開発－,教育心理学研究, Vol.60, pp367-379

内田勝也（2015）情報セキュリティからみたストーカー殺人事件の考察, 2015 年春季全国研究発表大会要旨集, 経営情報学会, pp.197-200

内田勝也（2015）標的型メール攻撃に対するセキュリティ心理学マネジメントからの考察, 2015 年秋季全国研究発表大会要旨集,経営情報学会, pp.65-68

加護野忠男（1988）『組織認識論　－企業における創造と革新の研究－』千倉書房

刈間理介・井上隆孝（2007）組織安全文化の概念と学校での安全教育が寄与すべき方向性に関する考察, 安全教育学研究, Vol.7, No.1, pp.17-34

倉田 聡（2014）『安全文化―その本質と実践』日本規格協会

見目悠平・谷本茂明・菊池 修・杉浦 芳樹・佐藤周行・金井 敦(2013)「CSIRT における人的資源管理方式に関する研究」プロジェクトマネジメント学会 2013 年度秋季研究発表大会予稿集 pp.105-110

近藤光・寺島健一・寺本直城・杉原大輔・高木俊雄・中西晶（2013）「日本企業における CSIRT 構築の事例―カーネギーメロンモデルとの比較―」『第 66 回全国大会　日本情報経営学会予稿集【春号】』, pp.111-114.

近藤光・寺本直城・寺島健一・杉原大輔（2013）「日本企業における CSIRT 構築の事例　―CSIRT 構築における制度的企業家」,『日本情報経営学会第 67 回全国大会予稿集【秋号】』, pp85-88

近藤光・寺本直城・杉原大輔・中西晶(2018)「CSIRT におけるレジリエンスの罠：日本における現状と課題」日本情報経営学会誌, Vol. 37, No. 3, pp.27-48.

白石斉（2018）「グローバル企業における個人データ等に対する活用と保護のあり方―EU一般データ保護規則の施行を契機として―」明治大学大学院経営学研究科修士論文

杉原大輔（2018）「日本における企業内CSIRTの現状と課題 －NCA早期加盟チームの実態から－」開智国際大学紀要, 第17号, pp.5-21, 開智国際大学

杉原大輔（2018）「標的型メール攻撃対応訓練と実行体制の事例紹介 －心理的安全に着目して－」, セキュリティ心理学研究 2018, 日本心理学会第 82 回大会, 東北大学, 2018 年 9 月 27 日

杉原大輔・中西晶（2014）「高信頼性組織（High Reliability Organization）入門　第 2 回：高信頼性組織のプラクティス」 経営情報学会誌 Vol.23,No.3,経営情報フォーラム

高橋 正泰・磯山優・山口善昭・文智彦(1988)『経営組織論の基礎』中央経済社

高橋優（2018）「ネットワークサービスの重要性評価と管理行動」, セキュリティ心理学研究 2018, 日本心理学会第 82 回大会, 東北大学, 2018 年 9 月 27 日

谷口勇仁（2008）「高信頼性組織（HRO）研究に内在するジレンマ」, 経済学研究, Vol.58, No.2, pp.61-69, 北海道大学

寺田剛陽・津田宏・片山佳則・鳥居悟（2014）「IT 被害に遭いやすい心理的・行動的特性に関する調査, マルチメディア、分散、協調とモバイル」 DICOMO2014 シンポジウム論文集, 情報処理学会, pp. 1498-1505

寺田剛陽・片山佳則・津田宏・鳥居悟（2016）「人の行動特性に基づくセキュリティ対策」 FUJITSU, Vol.67, No.1,pp.76-82

寺本直城（2013）「解釈主義的組織文化論における人間観-「遊戯人」（Homo Ludens）の可能性-」 経営学研究論集, 明治大学, Vol.38, pp.77-93

寺本直城・中西晶（2014）「CSIRT 組織化の契機」第 69 回全国大会日本情報経営学会予稿集（秋）, pp. 203-206.

中尾康二・北原幸彦・竹田栄作・中野初美・原田要之助・山下真（2015）『ISO/IEC 27002:2013(JIS Q 27002:2014)情報セキュリティ管理策の実践のための規範 解説と活用ガイド (Management System ISO SERIES)』日本規格協会

中西晶（2007）『高信頼性組織の条件』生産性出版

名和小太郎（2005）『情報セキュリティ-理念と歴史-』みすず書房

芳賀繁（2012a）『事故がなくならない理由　安全対策の落とし穴』PHP 新書

芳賀繁（2012b）「ヒューマンエラーは捌けるか-「裁く文化」は安全文化を阻害する-」 日臨麻会誌, Vol.32, No.7, pp.954-960

羽原敬二（2006）「空の安全－技術、政策、そして法－」 ノモス, Vol.19, 関西大学

藤谷護人（2003）『e-Japan 時代の情報セキュリティと個人情報の保護』IMS 出版

丸山満彦・尾嶋博之・前中敬一郎・本木賢太郎・中瀬 真一・田島義之（2011）『「想定外」に強い事業継続計画のすすめ―BS25999 で高める危機対応力』 中央経済社

吉田良夫（2004）『個人情報管理の急所』中央経済社

補論 1：マネジメントシステムと文化

ここで、現代的な組織運営において必須のものとなっているマネジメントシステムについて、PDCA サイクルによって推進される認証型のマネジメントシステムを中心に企業組織の文化との関係について確認しておきたい。

1 マネジメントシステム

産業界ではもはや当然のものとなっている ISO9000 シリーズのようなマネジメントシステムには、そのベースに良く知られる Plan・Do・Check・Action から成る PDCA サイクルが存在し、食品衛生であれば HACCP[91]、情報処理であれば ISO/IEC27001（ISMS）といったような外部機関による認証制度を備えたシステムも同様である。このサイクルを回す目的は、例えば ISO9000 であれば「品質」の保証である。このサイクルを適切に循環させることで、業務の品質が確保され、結果として商品・サービスの品質も確保され、顧客と自組織に貢献できるとする。先の ISMS であれば、情報資産を取り扱う組織として信頼に値することを、外部認証を通して表示することが可能となる。このマネジメントシステムのルーツは TQM（Total Quality Management）であり、いわゆる理系的である。コンセプトの基本は、生産システムにおける異常値の検出とその是正のための統計的手法であり、これを文系的業務も含めた組織全体に応用を図ったものといえる。

マネジメントシステムの多くは「方針」と呼ばれる組織的な目標に対して、「リスク及び機会への対応」というリスクマネジメントの観点から組織内部の各部門・各機能が担う貢献について、必要なタスクとして方針をブレイクダウンした形で定める。そしてタスクレベルでは、計画期間内にマイルストーンを置き、その進捗をチェックする。

現場レベルでは、業務の品質を担保するために求められる要件を「要求事項」として明記し、定型的業務や組織全体に対する影響度が低い非定型的な意思決定業務については、マニュアルを作成し、手順をフローとして規定し文書化することで、欠員や異動などによる人員の変化にもスピーディに対応できることも意図している。

---

[91] “Hazard”、“Analysis”、“Critical”、“Control”、“Point”による頭字語で、食品を製造する際に安全を確保するための管理手法。抜き取り検査によるチェックではなくプロセス全体でこれらを認識し、全件を対象とすることが特徴。

これらが適切に実施・運用されているかを確認するのが監査（内部監査）である。アウトプットは適切に記録されているか、マニュアルやフローは順守されているかといったように、要求事項が満たされているかを確認する。この結果を適合／不適合として判断し、不適合であれば是正を求める。もちろん、定められた文書の内容が現実と乖離する場合は文書そのものの改訂を要求する。外部機関によるマネジメントシステムの認証そのものは、この監査から是正までが適切に運用されているかを確認し、その適正さを保証するものである。

(1) リスクマネジメントと文化

本項では、ISO の各種のマネジメントシステムにおける「リスクマネジメント」に関する規格である ISO31000 について確認する。

まず、リスクマネジメントについては、その実装と運用に関する標準化規格として 2009 年に ISO31000 規格が発行されている。この ISO31000 では、リスクマネジメントを「①組織内での価値を創造し、保護するもの。②好ましくない影響を管理するプロセスにとどまらず、組織のあらゆるプロセスにおいて不可欠な部分であり、意思決定の一部である。③組織に合わせて作られ、人的及び文化的要素を考慮に入れることが重要である。④組織の継続的改善を促進するものとして位置づけており、透明性があり、かつ、包含的であり、周辺状況によって変化するリスクに対応することが重要である。」と説明している。

ISO31000 は、先行する ISO9000・ISO14000・ISO27000 シリーズとは違い、これら認証を目的とした規格との整合性を重視するためにガイドラインとして提示されている点が特徴となる。

そして、価値を創造し、その価値が組織のあらゆる部分で意思決定に現れ、文化との接合を果たし、継続的な改善の基礎であるという上述の説明に沿った有用なリスクマネジメントとするために、まず組織の状況を把握することがリスクマネジメントの枠組みを設計する上で大きな要件であることを指摘する。すなわち、リスクマネジメントのプロセスを開始する前に、組織の状況を把握し、理解したうえで、リスクマネジメントの枠組みを構築することを求めている。

情報セキュリティを企業のリスクマネジメントの一部として捉えれば、情報セキュリティに関するリスクを評価し、セキュリティポリシーを策定し、一般従業員にはこれに沿って実務を運用してもらうという構図となる。このため ISMS には、ISO/IEC27001 で要求される事項に適合するためリスクマネジメントが適切になされていることを証する指針として情報セキュリティのリスクマネジメントに特化した ISO/IEC27005 も規格されている。そこでは①状況の見極め、②情報セキュリティリスクアセスメント、③情報セキュリティリスク対応、④情報セキュリティリスクの許容、⑤

情報セキュリティリスクの協議及びコミュニケーション、⑥情報セキュリティリスクのモニタリング及びレビュー、という 6 段階のプロセスが提示されている。先の ISO31000 と同じく、組織の状況把握が起点とされている。

(2) マネジメントシステムと訓練：ISO22301 事業継続マネジメント

こういったマネジメントシステムと教育や訓練の関係性について述べるものとしては、2012 年 5 月に ISO 22301 として発行された事業継続マネジメントシステム（BCMS）規格が存在する。これは、BCP（Business Continuity Plan: 事業継続計画）の作成を中核として、計画をどのように策定・運用していくかに、リスクマネジメントの視点を導入するためのガイドラインである。他のマネジメントシステムのベースとなることを意図し、他のマネジメントシステムと同様に「リスク及び機会への対応」が盛り込まれている。

ISO 22301 におけるリスクとは、「事業の中断・阻害を引き起こすインシデント」である。これは、大規模災害だけではなく、第 1 章で確認したような情報漏洩や情報システム障害、さらにそれらによって引き起こされる風評による企業イメージへの悪影響や、それによる商品・サービスの売上低下をもその範疇としている。

この規格のベースには英国の事業継続マネジメントシステム規格 BS 25999 があり、事業継続マネジメントを、PDCA サイクルを基本として①組織の理解、②BCM 戦略の決定、③BCM 対応の開発と導入、④演習、維持およびレビュー、のサイクルモデルによって提示している。なかでも「④演習、維持およびレビュー」が重要視されており、演習を繰り返すことで組織文化に BCM を定着させることを目指していた（丸山ら, 2011）。

この ISO 22301 のなかでは、演習とは次のように定義されている。

> 3.18 演習（exercise）
>
> 組織内で、パフォーマンスに関する教育訓練を実施し、評価し、練習し、改善するプロセス[92]

この演習とは、「事業継続の手順がその目的を達成しているかどうかを確認するために実施されている教育訓練、評価のプロセス」（中島, 2013）であり、この教育訓練と評価を繰り返す上で何を目的としているかが重要になるといえる。

---

[92] 原典は ISO22300 による。

その目的については、

－方針、計画、手順、教育訓練、装置又は組織間合意の妥当性確認
－役割及び責任を担う要因の明確化並びにそれらの教育訓練
－組織間の連携及びコミュニケーションの改善
－資源の不足の特定
－個人のパフォーマンスの改善のおよび改善の機会の特定
－臨機応変な対応を練習するために統制された機会

というように、目的の例として前掲の定義に注記されている。これらの目的は単独で設定されるわけではなく複合的に用いるのが一般的とされ、中島ら（2013）は次のように例示している。

・参加するスタッフがその与えられた役割を期待通りに遂行できるか（又は、遂行するためのノウハウを習得するためも含む）
・実施された演習訓練で、求められる一定レベルを達成することができたか

これらの複合的な目的は、組織がリスクと捉える事象が発生した時に個々人に与えられる役割の整理と、役割を果たすにあたってそれぞれに定められる手順を遂行する能力をチェックすると同時に、役割の配分や遂行手順そのもの妥当性をチェックすることにあると理解できる。一方で、ここで挙げられるように「レベルを達成」したかの判断については、定義に付記される注記２において、

試験は、演習の独特かつ特有の形態であり、計画中の演習の到達点又は目的の枠内で、合否の要素を予想することが含まれている

とあるように、演習の目的に対する組織全体での達成度については合否判定を行うことも想定されているが、個々人がペーパーテストに定められた基準点をクリアすることは意味しないという（中島ら, 2013）。

このように、ISO22301 も他のマネジメントシステムと同様に「サイクルを繰り返す」ことが中核となる。これは、演習を繰り返すことによってビジネスパフォーマンスの持続性の向上を目指すものであると同時に、ISO22301 が外部認証のモデルではないことによると考えられる。ベースとなった BS25999 においても、演習を繰り返すことで BCP を組織文化に埋め込むことを意図していたように、1 度基準をクリアすればそれで目的達成というものではない。また、仮に認証のモデル

であったとしても、更新のためには一定水準が維持される必要がある。そのためにも演習を繰り返すことが必要であるし、メンバーが一定不変であることはあり得ない企業組織においては、教育研修と訓練の継続がより必要である。

また、個人のレベルにおいても繰り返すことは重要である。例えば、柔道であれば「受け身」を、茶道であれば作法を「型」として繰り返し行う。これらに求められているのは、自身がアウトオブコントロールの条件下でも、無意識レベルで取れる行為の確立なのだ。そのためにも、教育・研修を通じて基本となる行動を示し、特定の状況下において表出するように訓練を繰り返すことが求められる。

2 文化の測定とは

(1) 文化の測定とは

ここまでマネジメントシステムのいくつかを概観し、「文化的要素を考慮に入れる」というようにマネジメントシステムはたびたび文化に言及することを確認した。マネジメントシステムの企画者も組織の持つ人的な側面である文化の存在を意識し、これに影響を与えることを意図していることがわかる。特にリスクマネジメントをその主眼とするISO22301の由来であるBS25999でも、演習を繰り返すことでBCMが組織文化の一部となることを企図していた。しかし、これらが意図している文化とは非常に表面的なものであるという印象は否めない。

演習はあくまで仮想環境ではあるが、演習の繰り返しこそが、本番環境において求められる振る舞いを導出させることが期待できる手段であることは理解できる。しかし、ここでの振る舞いとの関係は、特定の場面における特定の振る舞いの誘導であり、内面化された価値観により自然に表出した振る舞いと同等のものであるかということには疑問が残る。手続き的知識にとどまってしまうことが懸念され、本番環境において出現するか、すなわち構造化できているかも未知である。この点でマネジメントシステムが意図する「文化」とは非常に表面的なものではないかという疑問である。

補論 2：測定の対象としての「振る舞い」10traits の例から

2011 年 3 月に発生した東京電力福島第一原子力発電所での過酷事故を受けて、東京電力が取り組む「原子力安全改革[93]」の一環として、「10 traits」に基づく自己評価が取り入れられている。10 traits とは、WANO[94]が、「健全な原子力に係る安全文化の特性」（WANO, 2013, p.9）として、すなわち原子力安全文化の表出として、原子力関連組織のメンバーの望ましい振る舞いを 10 の要素として整理・提示したものである[95]。これは、①組織のメンバー全員に求められるもの、②経営者層に特に求められるもの、③具備すべき要件として組織そのものに求められるもの、という 3 重の構造になっている。

まず、「①組織のメンバー全員に求められるもの」として「安全への個人の決意」が挙げられ、これには次の 3 つの要素があり、それぞれ 3 ないし 4 つの振る舞いとして定義される（WANO, 2013, pp.9-30）[96]。

1.個人の説明責任（PA）

すべての個人が、安全への個人的な責任を負う。原子力安全に関する責任と権限は、明確に定義され、明確に理解されている。報告の関係性、職位の権限、そしてチームの責任は、原子力安全が最重要であることを強調する。

2.疑問を持つ姿勢（QA）

個人は、満足することなく、エラーや不適切な行動の結果であるかもしれない違いを特定するために、既存の条件や想定や異常そして活動に疑問を持ち続ける。全ての従業員は、プラントの安全に望ましくない影響を与えうる想定や価値観、条件に注意深くある。

3.安全コミュニケーション（CO）

コミュニケーションは原子力安全に焦点を当てている。安全コミュニケーションの幅は広く、プラントレベルでのコミュニケーション、仕事に関連したコミュニケーション、作業者レベルのコミュニケーション、設備へ貼りだすラベル、運転経験、文書作

---

[93] 正確には「福島原子力事故の総括及び原子力安全改革プラン」2013 年 3 月に東京電力が公表

[94] World Association of Nuclear Operators：世界原子力発電事業者協会。1989 年に創立された原子力発電に関連する民間事業者の団体

[95] 10 Traits の発祥は、INPO：Institute of Nuclear Power Operations：原子力発電運転協会（米国内の原子力事業者による自主規制団体）にある。これを世界標準として WANO が採用した。

[96] 個別の項目ごとの仔細については、付録に掲載

成が含まれる。リーダーは、原子力安全の重要性を伝えるために、公式・非公式のコミュニケーションを用いる。組織の上方への情報フロー（報告・収集）は、組織の下方への情報フロー（指示・命令）と同じくらい重要であるとみなされる。

ここでは個々人の当事者性と、そして当事者として持つべき基本姿勢となる疑念を規定している。経営層だけでなく、現場レベルの個々人に対しても自己の振る舞いの一つひとつを漫然と行わず、考え、理由を把握すること。その行為がつねに安全に貢献できているかという疑念を持ち、時には自らの行為を規定するマニュアルそのものを疑うこと。この規定は、「安全文化」の基本である情報流通のためのコミュニケーションの質についての確認であると言える。

次いで、「②経営者層に求められるもの」として、「安全へのマネジメント層の決意」が挙げられており、これも 3 つの要素がある。いずれも、リーダーシップ発揮の方向性について示しているのだが、具体的には、ア）リーダーシップを発揮する際して、イ）組織的な意思決定を行うに際して、ウ）問題解決に際して、求められる要素、言い換えれば何に注意を払うべきか、何が求められているかを列挙していると言える。なかでも「リーダーシップアカウンタビリティ」では最多の 8 項目が明記されている。

1.リーダーシップアカウンタビリティ（LA）

リーダーは、意思決定と行動において原子力安全への決意を表現する。

エグゼクティブと上級管理職は、原子力安全の主導者であり、言葉と行動の両方で決意を表現する。原子力安全のメッセージは、頻繁に、一貫して、機会のあるごとに独立したテーマとして伝えられる。原子力関連組織全体の指導者は、安全のための例を示す。企業のポリシーは、原子力安全が組織の最優先事項であることを強調している。

2.意思決定（DM）

原子力の安全を支える、もしくは影響を与える決定は、系統的、厳密かつ完全である。

予期せぬ、不確実な状況に直面した場合には、発電設備を安全な状態にするために、現場のオペレーターに権限が与えられ、想定に理解が与えられる。上級管理者は、そういった保守的な判断を支持し強化する。

3.信頼できる職場環境（WE）

信頼と尊重が組織に浸透すると、尊重される職場環境が作られる。ある意味それは、タイムリーで正確なコミュニケーションを通じて獲得される。異なる専門家の意見が奨励され、

議論され、タイムリーな方法により解決される。従業員には、その懸念に応じて実行されるステップの情報が与えられる。

第3の要素群として、「③具備すべき要件として組織そのものに求められるもの」では、マネジメントシステムの運用について、すなわちPDCAサイクルによって業務を推進する際の要件を書き出している。ここで注目したいのは、継続的な学習、そして懸念の提起のための環境である。全体的な組織能力の向上のために、継続性に重きを置くことで長期的なP（計画）を可能とする点で、経験を積むための長期的な教育プランの作成が求められていると言える。また、C（確認）においても、自己と他者（社）の両面の視点を求めることで自己満足に陥ることを牽制している。どちらも、短期的なPに固執しがちなマネジメントサイクルを戒め、長期的視点を促していると理解できる。そして、個人が関わる局所的な活動だけでなく、それらを統合して全体最適なマネジメントのために実装すべき要素とその基本となる運用方法を示している。

1. 継続的な学習（CL）

継続的に学習する機会に重きを置き、追求され、実行する。運転経験は高く評価され、経験から学ぶ能力は十分に発達していること。自己評価、トレーニング、ベンチマークは学習を刺激し、パフォーマンスを改善させるために用いられる。原子力安全は、多様なモニタリング技術によって絶え間なく精査されており、その中には独立した「新鮮な視点」を提供する。

2. 問題の識別と解決（PI）

潜在的に安全に影響を及ぼす問題は、迅速に特定され、十分に評価され、直ちに対処、修正され、その重要性に応じたものである。組織の問題を含む広範な問題の特定と解決は、原子力の安全を強化し、パフォーマンスを向上のためにある。

3. 懸念の提起のための環境（RC）

安全認識の職場環境（SCWE）とは、個人が報復、脅迫、嫌がらせ、差別の恐れなしに原子力安全上の懸念を提起できる環境が維持されていることをいう。発電所の管理者は、そのような懸念を個人が自由に伝えることを許す定期査定基準、手続きを創り、維持しなければならない。

4. ワークプロセス（WP）

原子力安全を維持するために、作業活動の計画と統制の活動が実施されていること。

作業管理は、仕事が特定され、選択され、計画され、スケジュールされ、実行され、完了され、評価される慎重なプロセスである。作業管理プロセスに組織全体で関与し、完全にサポートするものである。

これらが、原子力発電所で働く職員の安全優先の意識醸成のベースとなるよう、振る舞いの指針として示されている。東京電力では、これに基づいて個々人の振る舞いを計測し、それを採点するというものではなく、個人レベルで1日の「行動の振り返り」のための参照点として用いられている。具体的には、これを基準として自己の1日の振る舞いを評価したものを蓄積し、より深い内省につなげることを意図してグループ内でその結果について話し合うという取り組みを実施している。

KPIの観点からは、次のように用いられている。

表25：東京電力の原子力安全改革における振る舞いに関連したPIと目標値（再掲）

PI（Performance Indicator）	Target
Traitsを活用した振り返り活動の実施率	100%
振り返り活動において「わからない」と回答した率	10%以下
各指標の移動平均	増加傾向
振り返り結果を討議するグループ・部内会議の実施数	月あたり2回以上
振り返り結果に関する経営者層によるレビュー回数	四半期あたり1回以上

東京電力（2015）p.53より安全意識に関する部分を抜粋し加筆　筆者作成

このグループ単位での振り返りの実施率などは組織の内外に公表されている[97]。ベースとなる振り返り活動そのものは、あくまで本人の主観による評価ではあるが、対外的にもこれを公表することで結果について内部のみならず外部からの注目があることを意識することができ、その意味付けをより大きくすることができるのであろう。平時の社内のやり取りにおいても、『*当たり前にできているというようなこと。あるいは上司と部下が仕事の話をしてるときに、こういう課題があって、こういうことをやりたいんだって言ってるときに、じゃあ、君はこのTraitsのどこに問題があるから、そういうことだと思うんだっていうふうな形で、業務の中にTraitsを意識しているようにしていることとか、そういうところもよく見られるというところが、そこまでやると根付いてる。意識*

[97] たとえば、原子力安全改革プラン2018年度第3四半期進捗報告など
http://www.tepco.co.jp/press/release/2019/pdf1/190220j0102.pdf

してやってきたから。』[98]と表現されるほど全体に浸透しており、10traits がその冒頭で強調するように、立場の異なっていてもすべての者が等しく認識を持つことできているといえよう。この取り組みは、2014 年から実施されており、継続・繰り返しが重要なのである。

なお、10traits の各項目の仔細については、付録を参照されたい。

[98] 2017 年 5 月 29 日に東京電力ホールディングス株式会社本社にて実施した安全文化を調査の主題としたインタビュー調査に基づく。

補論 3：CSIRT について

CSIRT の機能の中心は、インシデント分析とその他のサービスに大別され、後者は、インシデントの対応解決、対応支援、対応の連絡調整のうち 1 つ以上を行うものとされている(West-Brown et al., 2003)。後者のうち、「インシデントの対応解決、対応支援」とは、より具体的には、インシデント発生時の対応、インシデント関連情報、脆弱性情報、攻撃予兆情報といった各種情報の収集分析や、発生することが予見されるインシデントへの対応方針や手順の策定などがあり、彼らはこれらを「サービス」として定義して活動しているが、実際の活動内容は組織内の状況によって様々である（近藤ら, 2018）。例えば、残る「対応の連絡調整」として、情報セキュリティの向上には、インシデントの影響が潜在的に広範であることや、第 3 者からの通報によりインシデントが発覚する事例も多いこと、さらに近年では、日本国内の企業事情を巧みに利用した攻撃手法や、対応ノウハウの蓄積が難しい標的型攻撃など、常に新手の攻撃手法が開発され、単独の CSIRT では迅速に対応することが困難な状況になっていることから、重視されているのが組織間連携である（近藤ら,2018）。そのため、日本国内では、インシデント対応能力を持った最初の組織体として JPCIRT/CC[99]があり、組織間連携のコアとして情報セキュリティやインシデントについて広く情報の収集／発信をしている。政府レベルでは、ナショナル CSIRT に位置づけられる NISC[100]があり各行政機関内の CSIRT の統括を行なっている。

企業内 CSIRT については日立製作所がその先駆的な例とされ、2004 年に発足している（見目ら, 2013）。こういった企業内 CSIRT の連携のための組織として NCA（Nippon CSIRT Association: 日本シーサート協議会[101]）がある。2007 年に前述の日立製作所を含めた企業内 CSIRT の 6 チームにより発足し、加盟チームは 2020 年 7 月現在で 400 を超える[102]。加盟チーム数の推移は表 26 の通り 2013 年を境に急増しており、近年における情報セキュリティへの認識の高まりを直接反映していると言えよう。

---

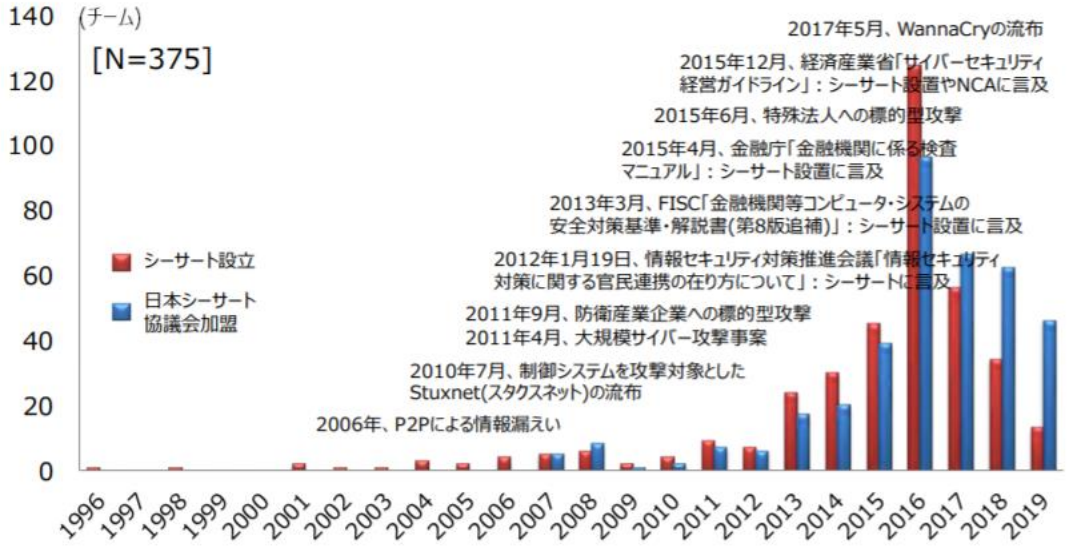
[99] 一般社団法人 JPCERT コーディネーションセンター：Japan Computer Emergency Response Team Coordination Center

[100] 内閣サイバーセキュリティセンター：National center of Incident readiness and Strategy for Cybersecurity

[101] 正式名称は、一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会

[102] 2020 年 7 月 1 日現在　https://www.nca.gr.jp/member/index.html

表 26：加盟組織の設立年と加盟数の推移



出典：日本シーサート協議会（2019）「加盟組織一覧 2019 年版」p. 16
（http://www.https://www.nca.gr.jp/imgs/nca_teams_2019.pdf, 最終アクセス 2020 年 8 月 1 日）

この他にも、産業分野ごとの特徴的な問題の解決のために監督官庁主導で連携をとることがあり、金融庁主導の金融 ISAC や総務省主導の ICT-ISAC などが存在している。

この CSIRT の企業組織における実装としては、欧米では CISO や CIO（Chief Information [Security] Officer）の直下に置かれ、インシデント発生時はもとより平時においても、組織内への指示命令の権限を持つことが一般的モデルとされる(West-Brown et al., 2003)。これに対する日本企業では、情報セキュリティに対する認識や、リスクマネジメントとしての優先順位の付け方に差があること、日本企業の一般的な特徴として管理系・事務系・現業を主管する部門が強く、情報システム部門などの情報処理部門が中心とはなるものの、こういったいわゆる管理部門の数多くの部署を横断する仮想組織となり、意思決定の権限を持たない（持てない）チームとして実装される。結果としてアドバイザリーに特化することとなり、強い権限をもって何かを主導することは難しいものとなることがチーム運営上の課題として指摘されている。

具体的には、①担当する者が兼任という形でチームの業務を担うことになる。②いずれも境界線があいまいであり、組織の理論として担当業務の押し付け合いや権限の引っ張り合いが起きる。③機能はあるが実態（明確な部署ではない）がないため、予算の付与に工夫が必要になる。④最終的な意思決定権者までにいくつかの階層を経ることになり対応へのスピード不足にもつながる（近藤ら, 2013a・2013b；寺本・中西, 2014 など）ということである。これらの課題の根源には、日本国

内の企業内 CSIRT の草創期は、情報端末と情報ネットワークが急速に普及し始めた直後であり、市井一般の情報セキュリティへの認識はまだまだ低く、危機感を持った組織内の少数の篤志家によってボランティア的に運営されることが多かったことや、企業組織内での何らかのトラブルを契機に設立されたのであっても、トラブル解決のプロセスとその後の組織学習によって、当該企業にその必要性が感じられなくなるといったプロセス的な問題がある。さらには組織内の公式組織として成立しても平時の活動は表立つことはなく、平時におけるトラブルの予防的活動はその効果を測定することが困難であるため、企業の上層部の理解が得にくい点も挙げられる（杉原, 2018）。

2015 年 10 月に実施された、NCA 設立初期の少数の加盟チームを対象として行われた小規模な調査においても、組織横断的(情報系子会社などとの企業横断の例も含め)に実装されるチームが 75%に及び、情報システム部門を中心に総務、法務、広報といったいわゆる文系部門を周辺として、最多では 8 部門にも渡って構成されているチームも存在していた。また、個人のレベルでもその 7 割は主たる業務は別の業務に就いている兼任のチームメンバーであり、さらにこれとは別に、インシデント発生時においてのみチームに加わるサポートメンバーも多いというのが日本企業の CSIRT の特徴といえる（杉原, 2018）。この傾向は、加盟チーム数が 400 を超える現在では、情報セキュリティの重要性の認識が高まったこともあり、監査や法務といったリスクマネジメントに関連した部門がこれに加わる傾向が強く、より広範な組織横断的な色彩が濃くなっていくと考えられる。この変化は、先に挙げた運営上の課題である上層部の理解や、組織全体での情報セキュリティに対する認識の向上といった点では、良い方向に作用することが期待できる。

付録

表 27：10 traits のうち組織メンバー全員に求められるもの

安全への個人の決意

Ⅰ　1.　個人の説明責任（PA）

すべての個人が、安全への個人的な責任を負う。原子力安全に関する責任と権限は、明確に定義され、明確に理解されている。報告の関係性、職位の権限、そしてチームの責任は、原子力安全が最重要であることを強調している。

PA.1	基準	個人は、原子力基準を遵守することの重要性を理解している。組織内のすべてのレベルにおいて、これらの基準を満たしていない場合の説明責任を果たす。
PA.2	仕事の主体者	個人は、原子力安全を支える振る舞いや作業実践に対して、個人的な責任を理解し発揮する。
PA.3	チームワーク	個人と作業グループは、原子力安全が維持されていることを確実にするために、組織内のみならず、組織の境界を越えてコミュニケーションを持ち活動を連携させる。

2.　疑問を持つ姿勢（QA）

個人は、満足することなく、エラーや不適切な行動の結果であるかもしれない違いを特定するために、既存の条件や想定や異常そして活動に疑問を持ち続ける。全ての従業員は、プラントの安全に望ましくない影響を与えうる想定や価値観、条件に注意深くある。

QA.1	核は特別で独特であると認識されている	個人は、複雑な技術が予期せぬ経路で失敗しうることを理解する。
QA.2	未知なるものを疑う	個人は、不確実な状況に直面したときには立ち止まる。作業を進行させる前に、リスクを評価し管理する。
QA.3	想定を疑う	個人は、何かが正しくないと思ったときには、想定を疑い、反対する意見を述べる。
QA.4	満足しない	個人は、成功といえる結果が期待できるときでも、間違いの可能性や潜在的な問題、内在するリスクを認識し、備える。

3.　安全コミュニケーション（CO）

コミュニケーションは原子力安全に焦点を当てています。安全コミュニケーションの幅は広く、プラントレベルでのコミュニケーション、仕事に関連したコミュニケーション、作業者レベルのコミュニケーション、設備へ貼りだすラベル、運転経験、文書作成も含まれます。リーダーは、原子力安全の重要性を伝えるために、公式・非公式のコミュニケーションを用いる。組織の上方への情報フロー（報告・収集）は、組織の下方への情報フロー（指示・命令）と同じくらい重要であるとみなされます。

CO.1	作業プロセスコミュニケーション	個人は、安全コミュニケーションを作業活動に組み込む。
CO.2	意志決定のための基盤	リーダーは、オペレーション上の、そして組織的な意思決定は、タイムリーなコミュニケーションによってなされることを確実にする。
CO.3	自由な情報の流れ	個人は、監督や監査、規制組織体を含めて、組織の上下、組織全体で開かれた誠実なコミュニケーションを持つ。
CO.4	期待	リーダーは頻繁にコミュニケーションを持ち、原子力安全が組織の最優先であるという期待を強化する。

出典：WANO（2013）Traits of a Healthy Nuclear Safety Culture, PRINCIPLES, PL 2013-1 より筆者作成

付録

表 28：10 traits のうち経営者層に特に求められるもの

安全へのマネジメント層の決意

II　1.　リーダーシップアカウンタビリティ（LA）

リーダーは、意思決定と行動において原子力安全への決意を表現する。

エグゼクティブと上級管理職は、原子力安全の主導者であり、言葉と行動の両方で決意を表現する。原子力安全のメッセージは、頻繁に、一貫して、機会のあるごとに独立したテーマとして伝えられる。原子力関連組織全体の指導者は、安全のための例を示す。企業のポリシーは、原子力安全が組織の最優先事項であることを強調している。

LA.1	資源	リーダーは、人員、設備、手続き、その他の資源が原子力安全を支えるために利用可能であり、適切であることを確保する。
LA.2	現場での存在感	リーダーは、プラントの監視、指導、基準と期待の強化のために、現場に現れる。基準や期待からの逸脱は速やかに是正されます。
LA.3	インセンティブ、制裁および褒賞	リーダーは、インセンティブ、制裁および褒賞が原子力安全政策に沿っていることを確実にし、原子力安全が最優先であることを反映した行動と結果を強化する。
LA.4	安全への戦略的コミットメント	リーダーは、原子力安全が最優先であることに合致するようにプラントの優先順位を確保する。
LA.5	チェンジマネジメント	リーダーは、原子力安全が最優先であることを維持するよう、変化を評価し実施するための体系的なプロセスを用いる。
LA.6	役割、責任と権限	リーダーは、原子力安全の確保に資するよう役割、責任、権限を明確に定義する。
LA7	定期的な試験	リーダーは、多様なモニタリング技術を通じて、原子力安全文化の評価を含む原子力安全が継続的に精査されていることを保証する。
LA.8	リーダーのふるまい	指導者は、安全の基準を定めるようなふるまいを示す。

2.　意思決定（DM）

原子力の安全を支える、もしくは影響を与える決定は、系統的、厳密かつ完全である。予期せぬ、不確実な状況に直面した場合には、発電設備を安全な状態にするために、現場のオペレーターに権限が与えられ、想定に理解が与えられる。上級管理者は、そういった保守的な判断を支持し強化する。

DM.1	一貫したプロセス	個人は、一貫した体系的なアプローチで意思決定を行う。リスクの見積りは、必要に応じて内包されている。
DM.2	保守的なバイアス	個人は、単に許可されているというものを超えて、慎重な選択を強調するような意思決定を実践する。たとえば、提案された行動は、完了する前で不安全であると判断するのではなく、実行する前に安全であると判断される。
DM.3	説明責任	原子力安全の意思決定のために、個人または一元的な説明責任が維持される

3.　信頼できる職場環境（WE）

信頼と尊重が組織に浸透すると、尊重される職場環境が作られる。ある意味それは、タイムリーで正確なコミュニケーションを通じて獲得される。異なる専門家の意見が奨励され、議論され、タイムリーな方法により解決されます。従業員には、その懸念に応じて実行されるステップの情報が与えられる。

WE.1	尊重が明示的であること	誰もが尊厳と尊敬をもって扱われる。
WE.2	意見が評価される	個人は、懸念を表明し、提案し、疑問を呈することが奨励される。異なる意見も奨励され尊重される。
WE.3	高レベルの信頼	信頼は、組織全体の個人やワーキンググループの間で醸成される
WE.4	コンフリクトの解消	コンフリクトの解消には公正で客観的な方法が用いられる。

出典：WANO（2013）Traits of a Healthy Nuclear Safety Culture, PRINCIPLES, PL 2013-1 より筆者作成

付録

表 29：10 traits のうち具備すべき要件として組織そのものに求められるもの

マネジメントシステム

Ⅲ　1. 継続的な学習（CL）

継続的に学習する機会に重きを置き、追求され、実行されます。運転経験は高く評価され、経験から学ぶ能力は十分に発達していること。自己評価、トレーニング、ベンチマークは、学習を刺激し、パフォーマンスを改善させるために用いられる。原子力安全は、多様なモニタリング技術によって絶え間なく精査されており、その中には独立した「新鮮な視点」を提供する。

CL.1	運用経験	組織内外での関連した経験は、体系的かつ効果的に収集され、評価され、教訓は組織全体にタイムリーに共有される。
CL.2	自己評価	組織は、自らのプログラム、実践、およびパフォーマンスについて自己批判的で客観的な評価を日常的に実施する。
CL.3	ベンチマーキング	組織は、知識、技能、安全なパフォーマンスを継続的に向上させるために、他社の事例から学習する。
CL.4	トレーニング	質の高い訓練は知識のある労働力を維持し、原子力安全を維持するための高い基準を強化する。リーダーは、人員、設備、手続き、その他の資源が原子力安全を支えるために利用可能であり、適切であることを確保する。

2. 問題の識別と解決（PI）

潜在的に安全に影響を及ぼす問題は、迅速に特定され、十分に評価され、直ちに対処、修正され、その重要性に応じたものである。組織の問題を含む広範な問題の特定と解決は、原子力の安全を強化し、パフォーマンスを向上のためにある。

PI.1	特定	組織は、是正処置プログラムを、問題を特定するために低い閾値で実装する。個人は、プログラムの期待に沿ってタイムリーに問題を特定する。
PI.2	評価	組織は、原子力の安全性の重要性に見合う条件の範囲と原因に対する問題解決と解決策を後押しすべく問題を徹底的に評価する。
PI.3	決意	原子力の安全性の重要性に見合った、タイムリーに問題に対処する効果的な是正措置をとる。
PI.4	傾向	組織は、定期的に、是正措置プログラムやその他の調査からの情報を総体として分析し、問題のある傾向または条件を特定する。

3. 懸念の提起のための環境（RC）

安全認識の職場環境（SCWE）とは、個人が報復、脅迫、嫌がらせ、差別の恐れなしに原子力安全上の懸念を提起できる環境が維持されていることをいう。発電所の管理者は、そのような懸念を個人が自由に伝えることを許す定期査定基準、手続きを創り、維持しなければならない。

RC.1	SCWE ポリシー	原子力安全上の懸念を提起するために個人の権利と責任をサポートする政策を実施し、嫌がらせや嫌がらせを容認しない政策を実施する。
RC.2	懸念を提起するための別のプロセス	組織は、ライン管理の影響から独立した、懸念を提起し、解決するためのプロセスを実施する。原子力安全に関する問題は、自信と適時かつ効果的な方法で解決される期待を持って提起される。

4. ワークプロセス（WP）

原子力安全を維持するために、作業活動の計画と統制の活動が実施されていること。作業管理は、仕事が特定され、選択され、計画され、スケジュールされ、実行され、完了され、評価される慎重なプロセスである。作業管理プロセスに組織全体で関与し、完全にサポートするものである。

WP.1	作業管理：	組織は、原子力の安全が最優先事項であるように作業活動の計画、統制、実

		行プロセスを実行する。このプロセスには、実行される作業に見合った原子力安全リスクの特定と管理が含まれる。
WP.2	設計マージン	組織は、設計マージン内で機器を運用し、維持する。マージンは、注意深く維持され、体系的かつ厳格なプロセスによってのみ変更される。核分裂生成物の防御壁の維持、安全関連の設備の防護の深さ、操作性と機能に特に注意が払われている。
WP.3	文書	組織は、完全、正確、最新の文書を作成し、維持する。
WP.4	手順の順守	個人は、プロセス、手順、および作業指示に従う。

出典：WANO（2013）Traits of a Healthy Nuclear Safety Culture, PRINCIPLES, PL 2013-1 より筆者作成

付録

頭字語インデックス

BCM：Business Continuity Management：事業継続マネジメント

BCMS：Business Continuity Management System：事業継続マネジメントシステム

BCP：Business Continuity Plan：事業継続計画

CIO：Chief Information Officer

CISO：Chief Information Security Officer：最高情報セキュリティ責任者

CSIRT：Computer Security Incident Response Team

EC：electronic commerce：電子商取引（E-コマース）

GDPR：General Data Protection Regulation：一般データ保護規則

HACCP：Hazard Analysis Critical Control Point：危害分析重要管理点

IAEA：International Atomic Energy Agency：国際原子力機関

ICT-ISAC：ICT Information Sharing And Analysis Center Japan：一般社団法人 ICT-ISAC

IEC：International Electrotechnical Commission：国際電気標準会議

INPO：Institute of Nuclear Power Operations：原子力発電運転協会

INSAG：International Nuclear Safety Group：国際原子力安全諮問グループ

IPA：Information-technology Promotion Agency：独立行政法人情報処理推進機構

ISMS：Information Security Management System：情報セキュリティマネジメントシステム

ISO：International Organization for Standardization：国際標準化機構

JIPDEC：Japan Information Processing and Development Center：一般財団法人日本情報経済社会推進協会

JIS：Japanese Industrial Standards：日本産業規格

JNSA：Japan Network Security Association：NPO 法人日本ネットワークセキュリティ協会

JPCIRT/CC：Japan Computer Emergency Response Team Coordination Center：一般社団法人 JPCERT コーディネーションセンター

KPI：Key Performance Indicator：重要業績評価指標

NCA：Nippon CSIRT Association：日本シーサート協議会（一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会）

NICT：National Institute of Information and Communications Technology：情報通信研究機構

NISC：National center of Incident readiness and Strategy for Cybersecurity：内閣サイバーセキュリティセンター

OECD：Organization for Economic Co-operation and Development

付録

SMS：Short Message Service：ショートメッセージサービス

SOC：Security Operation Center

TQM：Total Quality Management

WANO：World Association of Nuclear Operators：世界原子力発電事業者協会