硬直化した組織によく見られる
「目的と手段を混同させたセキュリティ対策」

2022 年 1 月 20 日

名和 利男

はじめに

2021年9月28日に閣議決定された「サイバーセキュリティ戦略[1]」（以下、本戦略）は、「1.2. 本戦略の位置づけ」において、文脈中で出てくる「経営層」を含む「あらゆる主体」に向けた強いメッセージが示されている。

- 「我が国としてのサイバーセキュリティに取り組む決意を、あらゆる主体、各国政府、そして攻撃者に対して発信するものである。」

また、「4. 目的達成のための施策」で最初に掲げられている取り組みが「経営層の意識改革」としており、経営層が自分事として捉えるべきことを、次のような表現で伝えている。

- 「経営層にとって、デジタル化とサイバーセキュリティ対策は、他人事ではなく、同時達成されるべき業務と収益の中核を支える基本的事項となり、両者を理解することが経営の基本的な素養・知識となると想定され、サイバー空間に関わるリスクの存在はデジタル化に取り組まない言い訳たり得なくなると考えられる。」

このように、本戦略はデジタル化とサイバーセキュリティ対策を、企業経営における「収益の中核を支える基本事項」であることを明確に示した。ただ、筆者の活動領域で観察できる限りでは、一部の大手企業がこのような考え方に基づく行動を始めているが、他の大半の企業はこの戦略の存在すら気づいていない状況がみられている。

そして、少なからず経営層において「デジタル化とサイバーセキュリティ対策」を「なんとかしよう」という発言や姿勢は見られているものの、社会的要請と化した「サイバーセキュリティ対策」に対して、横並び意識や同調圧力を醸し出すように、「準拠することを目的」として「対策のための対策」を行っている節（ふし）が見られる。

筆者は、13 年間ほど自衛隊に従事した経験の中で、「訓練のための訓練」を絶対にしないよう厳しく戒められてきた。必ず設定された目的に沿った訓練をするために、何度も大きな声での目的復唱や、事後の行動振り返りなどを積み重ねてきた。そのため、「自組織と顧客の利益を守るという目的」に沿って、サイバーセキュリティ対策を「手段」とすべきはずなのに「準拠することを目的」としている状況に強く違和感を覚える。多くの企業セキュリティ担当者との対話の中で、彼らがもっともストレスを感じ、限られたリソースの大半を費やすのは、「予算獲得のための説明（説得）」や「部門間調整」等である。急激に進展するサイバー脅威に追随するために割り当てるリソースの比重が、少ないという状況さえ散見される。このような経験をしている企業の多くは、「組織目的に沿った取り組みをするために、新しい価値を提供したり、環境変化に対応したりする際に、組織のパフォーマンスが十分に発揮できない」でいる。硬直化した組織でよく見かける光景である。

そこで、本コラムでは、このような状況の改善につながるような認識と洞察を共有させていただく。

---

[1] サイバーセキュリティ戦略　https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf

民間企業における「立派な（なんちゃって）サイバーセキュリティ」

民間の銀行、会社、公共的団体などに対してその事業について監督の職権を有する官庁（監督官庁）が、それぞれ独自にサイバーセキュリティに関する指針、ガイドライン、手引（以下、指針等）などを策定し、準拠することを求めている。一見すると、合理的かつ妥当性のある取り組みであるが、それぞれの指針等の内容に着目すると、類似した要求事項がみられる。特に、準拠すべき指針等が複数存在している場合、それらの要求事項の一部に不整合や辻褄を合わせるために一定の労力を伴う箇所が散見される。

さらに、それぞれの指針等を作成している担当部門は、限られた予算と人的リソースで行うため、適用すべき対象の状況認識に、客観性や専門性が確保されていない。そのため、指針等の立案の根拠となるリスク見積もりが不十分になり、どうしても低レベルの要求事項になりやすい。また、想定読者からの圧力や干渉を回避するため、踏み込んだ記述が困難になることもある。

一方、その想定読者である民間企業は、明示的および暗黙的に、同じ事業領域における横並び意識や同調圧力に影響を受けて、指針等の要求に準拠する姿勢が見られる。しかし、指針等に記述されている事項をすべて適用しようと努力することはなく、自組織の都合や予算に合わせて、実施可能なところを中心に適用しようとする。全く適用できない領域は、将来課題として先送りする傾向が見られる。このような状況であるにも関わらず、外部に対して「準拠している」という表現で説明責任を果たそうとする。

このように、監督官庁等が策定したサイバーセキュリティに関する指針等に準拠する企業は一定数存在しているが、その多くで、最近のサイバー脅威に起因するリスクに適用しているとは言い難い状況になっている。見た目は「非常にすぐれているさま」や「十分に整っているさま」を演出しているが、実情は、「内容は差し置いて外面を気にかけるさま」が目立った体裁を整える努力に多くのリソースが割かれている。

丸投げ体質、責任者不在、事なかれ主義でサイバーリスク増大

サイバー脅威に適合した強固なセキュリティコントロールを実現するには、最近のサイバー脅威を理解した上で、自組織において発生する可能性のあるリスクを特定するためにアセスメントを行い、その結果に基づいて適用させるべきセキュリティコントロールを設計および実施することが必要である。この実施責任は、経営層にあるが、彼らが適切な指示や管理を行うのに必要な、能力や知識を有していることは稀である。

現実的には、企業という閉じた環境の中で必然的に、ある種の固定概念（他人の意見や周りの状況によって変化せず行動を規定するような観念）が定着し、過去の成功体験がバイアスになることで、サイバー脅威に対する状況認識（理解）に偏りや不足が発生している。

一部の企業では、旧態依然の日本型組織によく見られる「丸投げ体質、責任者不在、事なかれ主義」が根強く残っている影響で、情報セキュリティ対策部門に対して「実現可否が評価されていない事項」や「与えている権限や予算・リソースでは達成が困難な事項」まで立案や調整をさせている。

オンプレミスが主流であった昔の IT システムであれば、情報資産に対する脅威への対応は、人材配置や組織構造を部分的に変更する「組織配置」で成果を上げることができていた。現在、クラウドファーストという考え方、つまり、企業や官庁などの組織が情報システムを導入あるいは更新する際に、運用基盤にクラウドサービス利用を第一に検討することが進展していくと、「組織配置」のみでは守ることができなくなる。このことが十分に認識されていない。

また、デジタル(IT)化が推進された事業部門は、直接サイバー攻撃による事業へのインパクトが発生する可能性が高まっているため、サイバーセキュリティの取り組みに主体的かつ積極的に関与しなければならない。ところが、事業部門は、上層部からの強固なセキュリティコントロールを受けることが少なく、強制力のない情報セキュリティ部門からの要請を軽視しがちである。実際には、売り上げの未達回避の努力に最大限集中するあまり、サイバーセキュリティへの協力は非常に限られたものとなる。

日本特有の非合理的かつ低効果なサイバーセキュリティ対策

海外の民間企業における「サイバー脅威に適合したセキュリティ対策」として、組織として強固なセキュリティコンロトールを持続的に推進する最善策がいくつも存在している。その最善策に基づく活動を支援しようと、それぞれの国家サイバーセキュリティ機関(米国ではCISA[2]、英国では NCSC[3]等)が知識体系を構築および整備し、自国の企業や官庁などを支援するための国家レベルの情報流通基盤(米国では HSIN[4]、英国では CiSP[5]等)が運用されている。

日本では、責任主体が広く分散化しており、個別具体的な取り組みが目立つが、セキュリティの意識の低い企業にまで支援を行き渡らせる点では、日本のほうが優れているとみることができる。しかし、日本の企業が推進している取り組みの一部において、目的と手段が混同し、合理性や効果で疑問が残るものがみられる。以下、その典型的なものを説明する。

日本で独自に発達した「標的型メール訓練」(社員のモチベーションと生産性を低下させ、効果が持続しない)

日本における「標的型攻撃メール訓練」の多くは、「社員が不審ファイル(標的型攻撃メール)を開かないようにする」ことを目的としている。他の主要国においては「フィッシング認識トレーニング」という名称で、「CISO と社員がフィッシングメールに対する認識を獲得および向上させる」ことをめざしたものである。

そのため、日本の「標的型攻撃メール」は、開いてしまった社員とその総数などを伴う「開封率」を経営層が報告し、それに基づいて対策指示を出すことが多い。一見すると、経営層にとっては合理的な取り組みのように見えるが、社員にとっては「周囲が開かないように注意を払っている状況の中で自分だけが開いてしまった」というネガティブな状況に陥り、それに輪をかける形で「開封率」として経営層に報告されることで、モチベーションを下げることになる。さらに、上司から「今後は開くな」というような指導が入ったり、開封した人だけを集めた集合教育への参加を求められたりすることで、生産性を押し下げる要因になる。しかし、このような流れで得られる効果は、人間の記憶の忘却とともに自然消滅する。

一方、他の主要国の「フィッシング認識トレーニング」は、フィッシングメールを識別して開封せずに報告すると 1 ポイント、開封しても報告すれば 0.5 ポイントが本人に付与されると

[2] Cybersecurity & Infrastructure Security Agency(CISA) https://www.cisa.gov/
[3] The National Cyber Security Centre(NCSC) https://www.ncsc.gov.uk/
[4] Homeland Security Information Network(HSIN) https://www.dhs.gov/homeland-security-information-network-hsin
[5] The Cyber Security Information Sharing Partnership(CiSP) https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

ともに、部門ごとの「報告率」が CISO に提出される。これにより、CISO にとっては、その「報告率」をベースに、組織としてのフィッシングメールの識別（認知）能力を図ることができ、もっとも報告率の高い部門に、実施すべき最善策のヒントがあることを見出すことができる。そのため、これに貢献した部門に対してランチチケット等の報酬を与える合理的な理由ができる。社員にとっては、部門内でフィッシングメールを見つけようとするポジティブな姿勢が高まり、他の部門に報告率で勝った場合、会社負担のランチを獲得することができるため、「次もランチチケットを獲得したい」という潜在的な目標が設定される。このようなサイクルが持続的に続くことが期待できるため、社員におけるフィッシング認識能力とモチベーションの両方が向上することに加え、生産性の維持も確保される。

外部サービス事業者に要求する「チェックリストの提出依頼」（他社にまでセキュリティコントロールしているように見せかける）

一部の日本企業が実施している「外部サービス事業者」に対する「セキュリティのチェックリストの提出依頼」は、非常に奇妙な取り組みである。外部サービス事業者に対するセキュリティ姿勢やリスク評価については、当該事業者が公表している情報やデジタル・フットプリント（インターネットを利用したときに残る情報）の調査だけで、高い精度で信頼性や安全性に対する客観的評価を行うことができる。それにも関わらず、そのような努力を行わず、わざわざ（他社である）当該事業者にセキュリティのチェックリストの提出を求めるという安直な行為をしてしまう背景には、「日本企業における制度疲労した官僚体制」があると考えられる。

もし、外部サービス事業者に対して、営業秘密や個人情報を預けて処理などを行わせ、かつそのコストに見合う十分な対価を支払う場合は、サプライチェーンリスク管理の観点から、セキュリティチェックリストの提供を求める合理的な理由がある。しかし、ユーザー1人あたりの利益が極端に少ない金額や無償のサービスを提供する外部サービス事業者においては、セキュリティチェックリストに対応するだけの経済合理性がない。それを承知の上で、外部サービス事業者に対してセキュリティチェックリストの提出を求める場合は、その日本企業の倫理観に疑問を感じざるを得ない。

リーダーシップを失った「修辞的セキュリティ対策」（言葉を美しく巧みに用いて効果を水増しする記述文化）

2021 年 6 月 28 日、英国国際戦略研究所が公表した「Cyber Capabilities and National Power: A Net Assessment（サイバー能力と国力：ネットアセスメント）[6]」において、日本の総括の一部で、日本のサイバーセキュリティ戦略について、次のような評価がされている。

- Its first mature cyber-security strategy was issued in 2013, building on several earlier policies that were focused on **rhetorical principles** of classic information security of a narrow technical kind.（その最初の成熟したサイバーセキュリティ戦略は 2013 年に発表され、狭い技術的な種類の古典的な情報セキュリティの**修辞的（美辞麗句的）な原則**に焦点を当てたいくつかの初期の政策に基づ

[6] Cyber Capabilities and National Power: A Net Assessment 7.Japan https://www.iiss.org/-/media/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---japan.pdf

いている。）

例えば、「政府機関等のサイバーセキュリティ対策のための統一基準（令和３年７月７日、サイバーセキュリティ戦略本部）[7]」において、特定の文字を検索すると「適切な／適切に」は334、「必要に応じて」は16もある。これらの文脈の多くで、誰が、どの場で、どのタイミングで、どのような基準で「適切」あるいは「必要に応じて」を決めるのが不明瞭となっている。実際には、サプライチェーンの末端（再委託先等）が、極めて限られた情報に基づいて決めることがしばしばである。このような「判断の丸投げ」の連鎖は、リーダーシップを失った「修辞的セキュリティ対策」とみなすべきものである。

おわりに

今回のコラムは、日本が国内外に発信している「サイバーセキュリティ戦略」で示されていた「経営層の意識改革」に基づいて、企業の中で改革努力をされている方々を支援する目的で執筆させて頂いた。そのため、マイルドな表現ではどうしても「伝わりにくさ」が生じるため、あえてできるだけシャープな表現を使った次第である。

日本の企業が取り巻く環境が変化していることに加え、サイバー脅威が想定を超えた進展を見せている中で、企業内部の仕組みを不退転の決意をもって変革していかなければならない。しかし、依然として、企業利益を守るために「変わるべきところ」が一向に変わらない状況が見られている。

筆者が企業支援をする経験の中で得られた知見に基づいた「硬直化した組織によく見られる目的と手段を混同させたセキュリティ対策」の認識と洞察が、読者の変革努力に少しでも役立つことを期待する。

以上

[7] 政府機関等のサイバーセキュリティ対策のための統一基準
https://www.nisc.go.jp/active/general/pdf/kijyunr3.pdf