日本特有のサイバーレジリエンスのあり方

2021 年 10 月 7 日

名和 利男

近年、日本企業がサイバー攻撃を受けて、周囲に対して深刻な被害を与えている事案が目立っている。しかし、被害の発生数は増加の一途をたどっているにも関わらず、これを抑止するための有効策が見当たらない。現在多くの企業において、現場のセキュリティ担当者が苦しんでいる。

そこで、諸外国がサイバー脅威に適合した対策として大きく舵を切り、現在注目されているサイバーレジリエンスについて、実務に則した知見と解釈を提供させていただく。そして、それを踏まえた形で、筆者の日本企業への対処支援活動をベースに、日本特有のサイバーレジリエンスのあり方について考察する。

サイバーレジリエンスとは

サイバー空間におけるレジリエンス（以下、サイバーレジリエンス）に関する定義について、日本国内では諸外国の文献をベースにしたものが多く見られるが、行政機関が民間企業向けに示した明確な定義は見当たらない。ただし、行政機関の施策の中で、次のような説明がされている。

- 防衛省・自衛隊の「サイバー攻撃等への対処能力を強化するサイバーレジリエンス技術の研究（平成 29 年度）」[1]：「サイバー攻撃等によって指揮統制システムや情報通信ネットワークの一部が損なわれた場合においても、柔軟に対応して運用可能な状態に回復する能力」
- 独立行政法人情報処理推進機構（IPA）の「責任者向けプログラム 業界別サイバーレジリエンス強化演習（CyberREX）」[2]：「部署・部門のサイバーセキュリティに関する対応力・回復力を強化し、企業組織全体の強靭化を図ることを意図」

一方、物理空間におけるレジリエンスについては、その概念に基づく施策を推進している米国において、次のような定義が見られる。

- 米国科学アカデミーの「Disaster Resilience A National Imperative(2012)」[3]：「不利な

[1] 政府のサイバーセキュリティに関する予算（7 ページ目後段）
https://www.nisc.go.jp/conference/cs/dai10/pdf/10shiryou10.pdf
[2] 責任者向けプログラム 業界別サイバーレジリエンス強化演習（CyberREX）
https://www.ipa.go.jp/icscoe/program/short/specific_industries/index.html
[3] Disaster Resilience A National Imperative(2012)
https://www.nap.edu/catalog/13457/disaster-resilience-a-national-imperative

事象（adverse events）に備え、計画、緩和、回復、そして首尾よく適応する能力」

- 米国大統領令第21号「Critical. Infrastructure Security and Resilience」[4]：「変化する状況に備えて適応し、混乱に耐えて迅速に回復する能力」

この物理空間のレジリエンスにおける重要アクションをサイバー空間に適用した定義が、米国の官民連携施策「Public-Private Analytic Exchange Program」[5]において、次のように示されている。

- サイバー空間におけるレジリエンス：「変化する状況に**適応**し、混乱に**備え**、**抵抗**性を持ち、迅速に**回復**する能力」

サイバー空間に適用された重要アクション（適応、備え、抵抗、回復）について、「誰が・何を・どのように」という観点で眺めると、日本企業におけるサイバーレジリエンスのあり方を幾つか示唆することができる。

- ***適応（Adapt）：*** *過去の混乱からの学習により、破壊的な出来事や将来の脅威に対して、管理手法の変更や対応戦略の調整を事前に行うこと。*
  - 【日本企業に対する示唆】「管理手法の変更」や「対応戦略の調整」の実施主体は、経営層である。したがって、経営層自らが、「過去の混乱」を「学習」しなければならない。また、年に数回程度の「学習」では、「管理手法の変更」や「対応戦略の調整」をするために必要な内容を本質的に理解することは不可能であるため、持続的に「学習」する必要がある。さらに、これらを「事前に行う」ということは、インシデントが発生する前に実施することを意味している。
- ***備え（Prepare）：*** *潜在的な脅威やストレス要因を予測、予想、対策を計画し、リスクのあるシステムの重要な機能を特定、監視すること。*
  - 【日本企業に対する示唆】 受動的な姿勢では、「潜在的な脅威やストレス要因を予測、予想、計画」することはできない。「サイバー脅威」については、セキュリティ対策部門が説明できるが、「社内や関連会社のストレス」については、それぞれの部門や関連会社の管理者が把握して説明できる。したがって、準備においては、組織内のさまざまな部門が緊密に連携する必要がある。
- ***抵抗（Withstand）：*** *危険に晒されている状況下でも、パフォーマンスの低下や機能の喪失を招くことなく、事業活動を維持する。*
  - 【日本企業に対する示唆】組織の司令塔（経営層）が、「危険に晒されている状況」でも、「パフォーマンス」や「機能」をコントロールできるシステムや実務

[4] Presidential Policy Directive -- Critical Infrastructure Security and Resilience
https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[5] Cyber Resilience and Response
https://www.dhs.gov/sites/default/files/publications/2018_AEP_Cyber_Resilience_and_Response.pdf

能力を保持していることを意味している。予算や人的リソースは有限であるため、経営層は「危険に晒されている状況」を事前に把握し、「パフォーマンス」や「機能」に与える仕組みや影響を正確に見積もり、自分自身の実務能力を発揮可能な状態にしておくことが前提となる。

- ***回復（Recover）：****不利な事象から事業の運営、パフォーマンス、機能を完全に取り戻す、あるいは回復する。*
  - 【日本企業に対する示唆】 組織内の事業に係る重要な要素を「取り戻す、あるいは回復」するまでのプロセスを、各事業部門に対して明示し、必要な指南を与える主体が必要である。危機管理において、この責任主体は経営層となる。そのため、経営層自らが、「事業の運営、パフォーマンス、機能」の状態を迅速に把握できる仕組みを整えておかなければならない。

日本企業に残る「日本型組織の特徴」

近年、日本企業に対するサイバー攻撃による被害が増加しており、それによる機会損失や利益低下も拡大している[6]。また、諸外国では、社会インフラが一時的に機能喪失するという事象さえ発生している[7]。

これを受けて、企業におけるサイバーレジリエンスへの関心が高まり、投資も拡大している[8]。しかし、日本企業は、サイバーレジリエンスの重要性に対する理解が乏しく、新型コロナウィルス感染拡大以降の個人デバイスに対するサイバーセキュリティ対策費増加率は、比較 7 カ国中で日本が最も低い状況にある[9]。

日本企業は、諸外国から遅れているというよりは、実際に発生しているサイバー脅威に適応した取り組みができていない状況が見られる。これは、欧州の GDPR（一般データ保護規則）が施行されて 3 年以上経過しているのにも関わらず、日本企業のデータ保護体制に遅れがみられる[10] ことにも現れており、日本企業全体として、セキュリティ姿勢が依然として低いということができる。

日本企業がこのような状況に陥っている理由や背景として、管理強化の観点で強く指摘さ

---

[6] セキュリティ事案による影響 – 総務省 情報通信白書令和 2 年版
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd134120.html
[7] コラム：米パイプライン攻撃、インフラ脆弱性への最大の警告
https://jp.reuters.com/article/breakingviews-us-pipelines-idJPKBN2CS08J
[8] 先進企業から学ぶサイバーセキュリティの要諦
https://www.accenture.com/jp-ja/insights/security/invest-cyber-resilience
[9] ウェブルート、世界と日本を比較したサイバーレジリエンスに関する意識調査を発表
https://www.fnn.jp/articles/-/135868
[10] 日本企業、データ保護体制に遅れ – 日経新聞 2021 年 10 月 7 日
https://www.nikkei.com/article/DGKKZO76381640W1A001C2KE8000/

れているのが「日本型組織の特徴」である[11]。

- 非公式組織と公式組織の二重構造： 社員同士ならびに組織と個人が契約やルールを超えた非公式な人間関係の紐帯で結びついている「非公式組織」と、権限の階層・命令と服従・ルールによる統制といった「公式組織」の側面を有する。
- 不明確な職務： 個人の職務が明確に定義されておらず、分担は決められていても、実際には課や係のような集団単位で行われる仕事が多い。また、組織の末端まで権限が委譲されていない。
- スタッフのライン化： 社員のモラル（士気）対策として、管理職に就けない人に対して管理職に準ずる待遇と肩書きを与える。

このような特徴により、日本型組織は、組織の意思決定が事実上、根回しなどの非公式なコミュニケーションで行なわれることが多く、場の空気に左右され、暗黙の合意形成によって意思決定がされる。また、下の側には上司が喜ぶ情報や、人事評価にプラスになるような情報のみを伝えようとする動機が働き、上司から直接命令されなくても上司の立場や意向を忖度して行動するようになる。これにより、上司は背後にある権限や影響力をちらつかせながら、無言の圧力で部下を動かすことができ、直接命令を下したわけではないため、いざという時は言い逃れができる。さらに、組織としての必要性よりも、処遇の論理を優先して役職が与えられているために、組織の意思決定に影響が出てしまう。これらから生じる圧倒的に組織優位な「組織と個人の力関係」が、「集団無責任体制」の性質を強めている。

昭和 29 年から 48 年にかけて発生した「神武景気」、「岩戸景気」、「オリンピック景気」、「いざなぎ景気」、「列島改造ブーム」により、日本経済が飛躍的に成長を遂げた時期において、会社全体が一つの目的に向かって有機的に連携する必要があった。これにより、会社に対する高い忠誠心、チームワークの尊重、仲間との信頼を重んじる行動様式が強く求められたため、上述の日本型組織の特徴が必然的に構築されていった。

現在、SNS により、顧客の価値観の多様化が一層進展し、一律の経済成長が発生しにくい社会環境となった。これに影響を受ける形で、日本企業は、組織全体に共有する目的の浸透が難しくなり、業務が複雑化していった。また、社会的要請による会社ルールの厳格化などにより、下部組織の自主性が薄れていった。

ところが、堅牢なまでの日本型組織の特徴は、さまざまな場に依然として存在しており、内輪の論理が優先する場の空気、変化に対する無自覚な抵抗、社内の複雑な利害関係に起因する問題処理の遅延など、日本型組織の弱点が顕在化している。最近、相次いで報道されている日本企業の不祥事がそれをよく表している。

[11] 日本型組織と不祥事 - 同志社大学 太田 肇
https://www.jstage.jst.go.jp/article/abjaba/87/0/87_82/_pdf/-char/ja

サイバー攻撃により会社利益を失うセキュリティ姿勢

日本型組織の弱点は、サイバー攻撃に対する事前対策の定着、発生直後のインシデント対処活動、再発防止策の策定において、負の影響を与えている。この例示は、枚挙に暇がないが、筆者の対処支援活動において強く危惧するものとして、「サイバーレジリエンスを自ら阻害させていることに気付いていないセキュリティ姿勢」の存在がある。

セキュリティ姿勢（security posture）とは、情報セキュリティリソース（人、ハードウェア、ソフトウェア、ポリシーなど）に基づく企業のネットワーク、情報、およびシステムのセキュリティステータスと、企業の防御を管理し、状況の変化に対応するための機能のことである[12]。

次の状況は、その象徴的なものである。

- サイバー攻撃により発生するリスク評価において、組織の下の側に対して強い期待や前提を敷いていることに気づかない。
    - 推定される要因：上司は背後にある権限や影響力を（無意識に）ちらつかせながら、無言の圧力で部下を動かすことに慣れている。
- 経営層や上司に了承を得るための「サイバー攻撃対策」を包括的であるかのように見せつける。
    - 推定される要因：上司が喜ぶ（上司が受け入れる）情報や、自部門と自身にプラスになるような情報を伝えようとする（無自覚な）動機が働いている。
- 実際のサイバー脅威に適合していない設計や内容のコンテンツによる教育訓練を、僅かな頻度で実施して、目標達成とみなしている。
    - 推定される要因：業務に影響を与えることを極力避けるという場の空気が強い。

また、本コラム執筆時点（2021 年 10 月上旬）において、日本企業におけるセキュリティインシデントとして公開された情報[13] は、次のとおりである。

- 10 月 01 日：地方自治体の学童保育で児童 2 名の事例を委託先が誤送信 ★
- 10 月 01 日：脆弱性原因で 9,515 名のカード情報など流出か、通販会社
- 10 月 04 日：料金未払い騙るフィッシング、携帯電話会社ユーザーに 1 億円の被害発生
- 10 月 04 日：銀行で 8,000 名のデータ誤提供、暗証番号なども流出か　★
- 10 月 05 日：食品メーカーが不正アクセスを受け、情報流出の可能性

---

[12] security posture
https://csrc.nist.gov/glossary/term/security_posture

[13] サイバーセキュリティ.com　最新個人情報漏洩事件・関連ニュース(2021 年 10 月 7 日付)
https://cybersecurity-jp.com/leakage-of-personal-information

- 10 月 05 日：通販会社のサイトに脆弱性、206 名のカード情報流出か
- 10 月 06 日：麻雀大会関連メール誤送信でアドレス 98 件流出、大会企画企業★
- 10 月 06 日：自治体が 270 の医療機関向けた一斉メールを誤送信 ★
- 10 月 07 日：自治体が DV による情報保護対象者の情報を外部に流出 ★
- 10 月 07 日：仮想通貨取引所のアカウントがサイバー被害、6,000 名の仮想通貨が不正出金

（「サイバーセキュリティ.com」記事を参考に一部加工）

このわずか 7 日間だけの統計であるが、★で示した事例に注目すると、半数が人為的要因によるインシデントであることに気づく。他の時期においても、同様な傾向が見られる。

あくまで筆者の企業支援の活動の中で得られた感覚レベルの捉え方であるが、日本型組織の特徴を持つ日本企業において、人為的要因によるインシデントの発生は、ある意味、約束されたものであると見ている。

日本型組織の特徴は、長く同じ組織で仕事をしている経営層や社員にとっては、自ら気付くことが難しく、外部からの指摘を受け入れることは拒否する傾向がみられる。そのため、サイバーレジリエンスの本質を理解し、自らの組織を客観視して変革努力をしている日本企業は、ほんの僅かであり、未だその広がりは見られない。

日本特有のサイバーレジリエンス

以上を踏まえて、今後、日本企業は、どのようにしてサイバーレジリンスを獲得すればよいのか？

2011 年の東日本大震災を経験した際、日本型組織の日本企業およびその社員は、素晴らしい行動をしていた。最近では、2021 年 10 月 7 日 22 時 41 分に関東地方で震度 5 の地震が発生した直後、筆者の手元のスマホで緊急地震速報が鳴ると同時に、ほとんどのテレビ局が速報番組に移行した。そして、国は迅速に関係省庁の局長などを緊急参集させ、官邸対策室を設置した[14]。重要インフラ事業者は、夜通し安全確認と復旧作業に努力し、順次正常に戻していった。

これは、日本の国家と国民が、過去の厳しい経験を積み重ねたことにより、必然的に培ったレジリエンス能力であると言える。

そうであれば、今後、私たちが、サイバー攻撃による深刻な被害の発生を許すという厳しい経験を積み重ねていくことで、いつしかサイバーレジリエンス能力を獲得することができ

[14] 我が国の危機管理について - 官邸
https://www.kantei.go.jp/jp/singi/ka_yusiki/dai2/siryou2.pdf

るかもしれない。

ところが、今の日本企業は、DX（デジタルトランスフォーメーション）に象徴されるようなデジタル化を推進し、事業構造や業務プロセスに大幅な改革を実現していかなければ、企業存続すら危うくなっている[15]。また、地震等の災害と異なり、サイバー攻撃は企業の努力で、ある程度コントロールできるものである。ただし、大規模サイバー攻撃（サイバーテロ）については、国家機関と連携して対処することが期待される。

したがって、私たちは、深刻なサイバー攻撃を経験していなくとも、経営層や社員の全てが、サイバー空間の状況認識の獲得努力を持続的に行い、自発的かつ積極的に想像力[16]を高めていかなければならない。いまだに日本型企業の特徴を持つ日本企業に所属する方々は、これを理想に近いものとして捉えるかもしれないが、サイバー攻撃によって深刻な被害を受けた日本企業は否応なしに、状況認識と想像力とを発揮せざるを得ない状況に陥っていることに目を向けていただきたい。

これまで、日本企業の多くの現場のセキュリティ担当は、並々ならぬ努力を積み重ねてきた。しかし、その努力の大半が、社内調整と経営層からの理解獲得になっている事実がある。本来は、会社に影響を与えるサイバー脅威対処に全ての努力を向けるべきである。

率直な表現で申し上げると、（組織全体を動かすことのできる権限とパワーを有している）経営層自らが、企業のサイバーレジリエンス能力獲得の阻害要因になっているケースさえある。この矛盾は現場の担当者が、辛抱強くかつ静観しているが、そう遠くない将来に、崩壊することは間違いない。

つまり、日本特有のサイバーレジリエンスの取組みは、経営層自らの意識変革と企業全体に対する献身的な努力の積み重ねにかかっていると言える。

（了）

[15] 企業活動におけるデジタル・トランスフォーメーションの現状と課題 – 総務省 情報通信白書令和 3 年版
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/n1200000.pdf

[16] 心的な像、感覚や概念を、それらが視力、聴力または他の感覚を通して認められないときに作り出す能力のこと。
https://ja.wikipedia.org/wiki/%E6%83%B3%E5%83%8F%E5%8A%9B