12

日本のCISO

私のキャリアにおいて、日本での6年間の生活は本当に幸運なものでした。日本が大好きで、メットライフ・ジャパンのCIOとして神戸と東京で生活する機会を得られたことは、私にとって大きな 恩恵でした。

日本は複雑な社会で、多くの突拍子もないことや予期せぬ特徴があります。訪れたり旅行したりする場所としては魅力的で日本の生活の質に魅了されるでしょう。日本社会は極めて尊重の念が深く、上司への物理的なお辞儀といった習慣は、多くの西洋人にとって不快に感じるかもしれません。しかし、仕事は過酷で、日本のサラリーマンの持久力とキャリアへの絶対的な献身には感服しています。

この国は成功への高い期待があります—野球の試合を見ればすぐにわかります！

伝統的にキャリアでは長期の在籍が期待されており、従業員は極端に高い忠誠心を持ち、長年同じ企業に勤め続けます。日本全体としても高齢化が進んでおり、サイバーセキュリティ分野で新たなキャリアをスタートさせる新卒の学生の数が少ない状況です。

日本のCISOは課題に直面しています。日本は中国、北朝鮮、ロシアに地理的に近いだけでなく、東アジアの緊急事態（台湾を含む）に備えて米軍基地が国内に配置されているためです。日本の技術は多くのテクノロジー製品の中核を成しており、米国を含む他国軍の装備にも組み込まれています。 彼らは、敵対的な国家から自社の企業を防衛する必要があります。一方でISC2の2023年調査1によると、サイバーセキュリティ専門家の不足が深刻化しており、約11万人の人材不足が指摘されています。

言語スキルを有する外国人労働者を簡単に採用できないことが、この状況をさらに悪化させています。既存の従業員は、多言語スキルを有しているというだけで、サイバーセキュリティの

1 「How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023」https://cybergovernancealliance.org/wp-content/uploads/2024/01/ISC2_Cybersecurity_Workforce_Study_2023-1.pdf

担当となった内部異動者であることが多く、これらの従業員はバイリンガルである可能性はありますが、サイバーセキュリティの経験や資格を有していない場合があります。

ここでは、みずほフィナンシャルグループのグループCISOである寺井理氏を紹介します。寺井氏は、テクノロジーとクラウド分野で豊富な国際経験を持つIT幹部です。野村グループと日本興業銀行で成功を収めたキャリアを有しています。

金融IT分野で30年以上の経験を有する寺井氏は、日本の伝統的な金融機関のCISOとしての課題、およびその背景にある構造的・歴史的な課題について共有します。

日本のCISO

寺井 修

最初に、この本への寄稿の機会を与えてくれたデイビッドに感謝したいと思います。私はCISOとしてのキャリアはまだ短いですが、サイバーセキュリティを担当して約4年間、知識を吸収し、良いプラクティスを積極的に取り入れるよう努めてきました。

私がデイビッドと出会ったのはFS-ISAC APACサミットでした。このサミットは、他の企業のCISOと交流ができる、最も興味深くインタラクティブな機会の一つです。FS-ISACのイベントで他のCISOと交流できることは、私にとって非常に有益で重要なことです。これは、最先端のイニシアチブやアイデアに触れる機会を得られるだけでなく、デイビッドのような人々と個人的なつながりを築ける機会だからです。

同時に、他の企業と私の銀行、そして他のCISOと私との間には、文化的な違いだけでなく、知識や経験の面でもギャップを感じることがよくあります。

この本への寄稿を依頼された際、私は躊躇しました。現在サイバーセキュリティに携わっている読者に対して、価値ある洞察を提供できるかどうか疑問だったからです。しかし、デイビッドと話し合った結果、多様な経験や背景を持つ人々を包含することが重要だと理解しました。したがって、私の記述は短いものの、CISOとしてこれまで取り組んできた課題や重点を置いた点、および日本の企業文化とIT環境の特徴について、読者に紹介したいと思います。

日本におけるCISOへの道のり

なぜ私のCISOとしてのキャリアは短いのか？これは、特に伝統的な金融機関における日本の企業の人事アプローチを象徴していると考えます。

日本の伝統的な金融機関の人事制度にはいくつかの特徴がありますが、最もよく知られているのは「年功序列制度」です。これは、昇進が本質的に年齢に基づいて決定されるシステムです。このシステムでは、CISOのような上級職に昇進するためには、一定の年齢に達する必要があります。最近では、年齢に関係なく能力のある人材がより早く昇進できるよう、人事制度が進化しつつありますが、年齢は依然として昇進の主要な要因の一つです。

当然、大手金融機関のCISOとなるには、知識だけでなく、インシデント対応などの緊急事態における経験や、上級幹部に積極的にアプローチする勇気も必要です。したがって、どれだけ知識が豊富であっても、20代の従業員がCISOを務めることは現実的ではありません。しかし、日本において一般的なのは、CISOの任命が経験だけでなく、自身と他のリーダー層との年齢バランスにも基づいている点です。30代のCISO候補者が優れた知識と経験を持っていても、その候補者と他のC-suiteメンバーやCISOの下で働く他の部門長との年齢差について、社内で懸念が生じることは容易に想像できます。

伝統的な日本企業は、長年にわたり組織内の人的関係の調和を乱さないよう実践を積み重ねてきました。私はそのような企業で非常に若いCISOが任命される事例を見たことがなく、おそらく私のキャリアにおいても目にすることはないでしょう。そのため、日本国外のCISOで10年以上その職位に就いている人に出会うと、彼らを羨ましく思います。鍵となる点は、日本という国は他と異なり、ここでCISOとして活動することはその違いを反映しているということです。

伝統的な日本の金融機関の人事システムの特徴の一つは、「ジェネラリスト」の育成に重点を置いている点です。私の場合、欧米では典型的なキャリアパスではない道を経てCISOになりました。大学卒業後、銀行のIT子会社で働き、その後ITサービスプロバイダー、ITコンサルティング会社を経て、証券会社のITインフラ責任者に就任しました。

サイバー人材の育成

私がCISOとして勤務する銀行のサイバーチームメンバーのキャリアをみると、新卒で銀行に入社した社員はさまざまな業務を経験していますが、概ねIT経験は4年未満です。サイバーセキュリティ経験はさらに少ないです。サイバー部門に配属される前、一部のメンバーは個人や法人営業、市場系業務、海外事業計画、経営関連会議体の調整、コンプライアンスなど、幅広い業務に従事していました。

これらのメンバーが上司から、銀行のトップリスクの一つであるサイバーセキュリティを担当する部署への異動を告げられた際、高く動機づけられたメンバーもいました。サイバーセキュリティというダイナミックで 成長する分野に真の興味を持ってチームに加わったメンバーもいました。しかし、他の一部のメンバーは「技術者集団」に放り込まれることに不安を感じていました。

CISOとして、このような新規メンバーが離脱せず、サイバーセキュリティ分野に残り続けるためにすべきことは3つあると考えます。

第一に、彼らを教育しスキルを向上させるためのトレーニングを提供することです。これは、ITシステムの構築や運用方法、脆弱性の種類、アタックサーフェスの意味、サイバー攻撃の防御方法、サイバー攻撃の検出方法、サイバー攻撃が検出された場合の対応方法などを単に説明するトレーニングプログラムを提供するだけではありません。これらのスキルは新しく配属されたメンバーが習得すべきものではありますが、彼らは最近まで異なる役割を担っていたことを忘れてはなりません。例えば、顧客に資産管理の提案を行うような業務に従事していた人々が、このような大きなマインドセットの変更を遂げることは、非常に困難な課題です。

これは、キャンプファイアに点火器を使うことに例えることができます。点火器なしでも火を焚くことはできますが、点火器があると簡単です。しかし、点火器を使っても、火が強く燃えるまで扇ぎ続け、少しずつ薪を追加する作業は欠かせません。これは、各個人による継続的な努力が必要です。サイバーセキュリティの仕事を始めた直後、会議でよく使われるサイバーセキュリティやITの専門用語を理解できないために仕事の内容が理解できず、辞めたくなるというのは、キャンプファイアで火が起こせずあきらめたくなることと同じです。こういったことを防ぐために、火が消えない状態に素早く到達するために点火器（トレーニング）が必要です。

二つ目に、サイバーセキュリティの役割を担うことが、自身の幅広いビジネススキルを向上させる有効な手段であるというメッセージを伝えることです。これは、銀行などの金融機関で働く人々にとって特に重要です。銀行業務は驚くほど部門間が分断されているのが現実です。担当する顧客や業務内容によって、連絡を取る部門が異なります。一部の部門は自然と幅広い範囲をカバーしています——例えば人事、内部コミュニケーション、コンプライアンスなどです。サイバーセキュリティにおいては、日常的により広範なステークホルダーとコミュニケーションを取らなければなりません。

例えば、大規模なサイバー演習を行う際、サイバーセキュリティチームは、危機管理チーム、IT、事務、ビジネスフロント、コンプライアンス、法務、リスク管理といった多くの部署と、演習の日程やシナリオ、ロジスティックスについて調整を行う必要があります。こういう業務をうまく推進できている人をみると、機能や部門を越えて効果的にコミュニケーションを取る能力が、サイバーセキュリティチームで働く上で重要であることがわかります。

三つ目は、サイバーセキュリティの重要性と目的、およびそれが業務に与える影響がいかに大きいかをサイバーセキュリティ担当者に伝え、そのような重要な業務を担っているという自覚とやりがいを持たせることです。

すべての銀行員は、銀行業務や決済プロセスがいかに重要で不可欠かを理解しています。しかし、サイバーセキュリティがこのような銀行システムの安定した機能の基盤となっている点については、理解が不足しています。

銀行員は、例えば日本での金利上昇が信用リスクや市場リスクにどう影響するかを考慮するといったことを自然におこなっています。しかし、例えば活発で強力なランサムウェア集団に関する情報をもって、ビジネスにどのようなリスクをもたらすか、理解している人や、少なくとも理解しようとしている人は非常に少ないと思います。サイバーセキュリティ担当者の役割は、金融機関で働く人全員に対してサイバーリスクが天災ではなく、信用リスクや市場リスクと同様に、事業遂行において考慮すべきリスクの一つであることを理解させ、1線による自律的な管理を促進することです。

さらに、サイバーセキュリティコミュニティにおける情報交換と共有という、極めて重要でユニークな活動もサイバーセキュリティの業務の魅力の一つであるということも付け加えたいと思います。自社の銀行や組織内での閉鎖的な活動のみを行うだけでは不十分です。日本では、金融機関のサイバーセキュリティ担当者が実践的な情報を共有する「金融ISAC」というサイバーセキュリティコミュニティがありますし、グローバルではFS-ISACがあります。よく、サイバーセキュリティは「非競争領域」と言われますが、他の非競争領域において、これだけオーガナイズされた形でプラクティスの共有や共同作業が行われている業務領域はほかにはないと思います。コーポレート領域の仕事は社内の人とのコミュニケーションが多いですが、金融ISACやFS-ISACに参加して同業他社の人たちとつながり、悩みやプラクティスを共有し切磋琢磨できるということは非常に刺激的で楽しいことであるということも、サイバーセキュリティを担当する人にとって魅力的なポイントです。

私は、お互いに協力し合うことで、コミュニティ全体のサイバーセキュリティ強化、さらには社会全体の強化に貢献できると心から信じています。営利銀行として、社会貢献の一般的なアプローチは、顧客へのサービス提供を通じて社会の発展に貢献することですが、サイバーセキュリティは、金融業界と顧客をサイバー攻撃から保護することで、より直接的に貢献できます。

この点で、サイバーセキュリティの役割は非常に意味深く、名誉ある仕事です。私たちは、私たちが取り組んでいる仕事がこの重要な影響を与えることを人々に認識してもらうことが重要だと考えています。

リスク受容の問題

CISOとして、リスク受容に関する問題に対処することは常に困難でした。銀行を運営するには、考慮すべき多様なリスクが存在します。リスクを管理できない銀行は、市場で成功できず、規制当局から免許を剥奪されるか、信頼できるサービスを提供できないため顧客の信頼を失うことになります。

市場リスクと信用リスクの概念は長い歴史を持ち、現在では金融当局を含む世界中で認識されています。これらのリスクの定義において、リスクの量と管理が定量化されている点は、グローバルな理解において有利な特徴です。これらの分野では、歴史的なデータが豊富で、その正確性にも信頼が置けます。（ただし、時折激しい市場暴落が発生し、機関に影響を与えることもあります。）

サイバーリスクの場合、リスクを定量化する一般的な実践方法は私がしる限りまだ存在しません。むしろ、一部のCISOが試みたものの、最終的に定量化を断念した例なら知っています。これが、CISOがビジネス部門とのリスクコミュニケーションを困難にする主要因の一つです。経営陣やビジネス部門はサイバー対策の必要性は理解していますが、サイバー対策が削減するリスクの量を定量化するのが難しいため、他のリスクへの対応やサイバー対策投資の優先順位付けに苦労しています。

事業中断リスク、コンプライアンスリスク、法的リスクに加え、サイバー攻撃リスクにはレピュテーションリスクが含まれます。企業がサイバー攻撃を受けたというニュースは、一般に過剰に報道され、事実よりも誇張される傾向があります。そして、企業は被害者であっても謝罪が求められます。これは特に日本において顕著です。さらに、ソーシャルメディアでは、ニュースが誇張され、真偽不明の情報と共に拡散されます。これにより、企業のイメージが長期にわたって損なわれる可能性があります。経営陣が最も避けたいのは、自社がサイバー攻撃を受けたというニュースです。

サイバーセキュリティの責任者になって気づいたことは、サイバーリスクに対してゼロトレランスのアプローチを主張し、サイバー攻撃に対して極度に敏感になっている人が役員のなかにいるということです。一方、恐怖に駆られて決断するのではなく、合理的にサイバーリスクを管理し、企業の枠組みに基づいたリスクベースのアプローチを採用する主要なステークホルダーも存在します。当然ながら、後者があるべきアプローチですし、私の推奨するのもこちらです。

CISOが直面する問題は、許容可能なリスクの判断です。個人的には、日本人はリスクベースのアプローチが得意ではないと感じています。日本社会における損失や失敗に対する許容度は極めて低いです。例えば、大多数の個人は、損失の可能性がある投資よりも貯蓄を好む傾向があります。彼らはデメリットをメリットよりも重視する傾向があります。

同時に、日本では顧客の高い要求に応えるために、製品やサービスの品質を重視する文

化があります。歴史的に、顧客の需要に応えて高品質な製品を生産する製造業が繁栄してきました。また、日本では電車が数分遅れただけで駅員に苦情を言う顧客がいることもよく知られています。

その結果、経営者は（顧客がどのような理由でもサービス停止を許さないだろうという懸念から）リスクに対してゼロトレランスの姿勢を採用することが多くなります。私はこのような状況を、サイバーセキュリティだけでなく、ITシステム障害の分野でも何度も目にしてきました。これは、日本人にはリスクに基づく判断が得意ではないためです。私は、日本の金融機関でCISOを務める上で、これが最も難しい部分だと感じています。

例を挙げましょう - 日本では、管理ポリシーのルールが遵守されていないことは一般的に受け入れられません。しかし、脆弱性評価で発見されたギャップに対して、会社ポリシーで定められた期限を超えて対応することが許されるかどうかが、典型的な質問です。

ルールを満たせない場合、決定は脆弱性への攻撃の発生可能性と発生時の影響に基づくリスク受容基準に基づいて行われます。これは論理的に思えますが、最終的にリスクを受容するか否かの決定の妥当性をどのように検証すべきでしょうか？

残念ながら、この質問に対する簡単な答えはありません。最終的には管理者の判断に委ねられるとよく言われますが、その管理者の判断はどのような根拠に基づいているのでしょうか？

私の感覚では、多くの場合、先述したように個人の恐怖に基づいて判断が行われているようです。特に、サイバーインシデントが発生した場合に責任を問われるため、上級管理者の判断は（理由は明らかではないですが）保守的なものになりがちです。

伝統的な日本企業や、重要なインフラの管理を担う金融機関では、この感覚は理解できますが、経営陣の個人的な感性や気まぐれに左右されるべきかどうかは疑問です。

CISOとして、私は経営陣が個人的な恐怖（私はそれらを「ゴースト」と呼んでいます）に左右されずに合理的な判断を下せるよう、可能な限りの助言を提供するように努めています。しかし、これは口で言うほど簡単ではなく、取締役会への報告内容に関するプレゼンテーションや記事の数を考えると、世界中のCISOが同じ課題に直面していると思います。私は一人ではありません。

ガバナンス会議

私が勤務する金融機関では、サイバーセキュリティリスク管理プロセスの運用状況をレビューするため、経営陣と取締役会メンバーが参加する複数のガバナンス会議を設置しています。

このような会議で真に有意義な議論を行うためには、CISOは2つの点を明確にすべきだと考えます。

まず、経営陣や取締役会メンバーが理解できる形で、会社のサイバーリスクを提示することです。経営陣は、事業運営にどの程度のサイバー攻撃リスクが関連しているか、そのうちのどの程度が適切に管理されているか、そして残存するリスクの内容と規模を知りたいと考えています。すべての情報は、この視点に集約されるべきです。

サイバーセキュリティチームの日常業務には、絶え間ない外部攻撃からの防御と内部システムにおける脆弱性の診断が含まれます。サイバー脅威には、国家支援を受けた攻撃者、ランサムウェア、インターネットバンキングサービスにおける詐欺などが含まれます。CISOの課題は、現場での活動を経営陣が知りたいビジネスリスクに適切に翻訳できるかどうかです。

CISOがこのようなガバナンス会議での議論の質を向上させるためにすべきもう一つのことは、経営陣と取締役会のメンバーのサイバーセキュリティに関する知識レベルを向上させることです。サイバー攻撃のリスクを議論するためには、経営陣と取締役会のメンバーがサイバー攻撃の基本知識とサイバー脅威の動向を理解している必要があります。

当社のサイバーセキュリティチームは、経営陣と取締役会メンバー向けに年1回のオンライントレーニングを提供してきましたが、これでは不十分だと考えました。そのため、ほとんどの役員が出席する週次の会議でサイバーセキュリティについて話すことにしました。取り上げたテーマには、例えば、他社でのサイバーインシデント、日本と外国の政府のサイバーセキュリティ政策と規制の動向、サイバー脅威アクターの説明などが含まれます。約5分間説明し、CEOを含む経営陣が質問やコメントを述べます。

これは体系的な教育方法ではないことは承知していますが、最新のサイバーセキュリティ動向を経営陣に伝えることで、サイバーセキュリティが経営陣の意識に定着したと考えています。これが、ガバナンス会議における意味のある議論の基盤となりつつあります。

日本企業におけるIT/サイバーセキュリティチームの課題

日本の銀行で働いた経験のないCISOやサイバーセキュリティ専門家と話す際、最も伝えにくい点の一つは、なぜ日本の銀行ではサイバーセキュリティのソリューションの導入にそんなに時間がかかるのかということです。確かに時間はかかりますし、正直なところ私自身もイライラするほどです。なぜでしょうか?私は3つの理由があると考えています。

第一に、日本の組織には十分なサイバーセキュリティ人材が不足しています。2022年に日本のサイバーセキュリティコンサルティング兼ソリューションプロバイダーであるNRI Secure Technologiesが実施した調査結果はこちらです2：

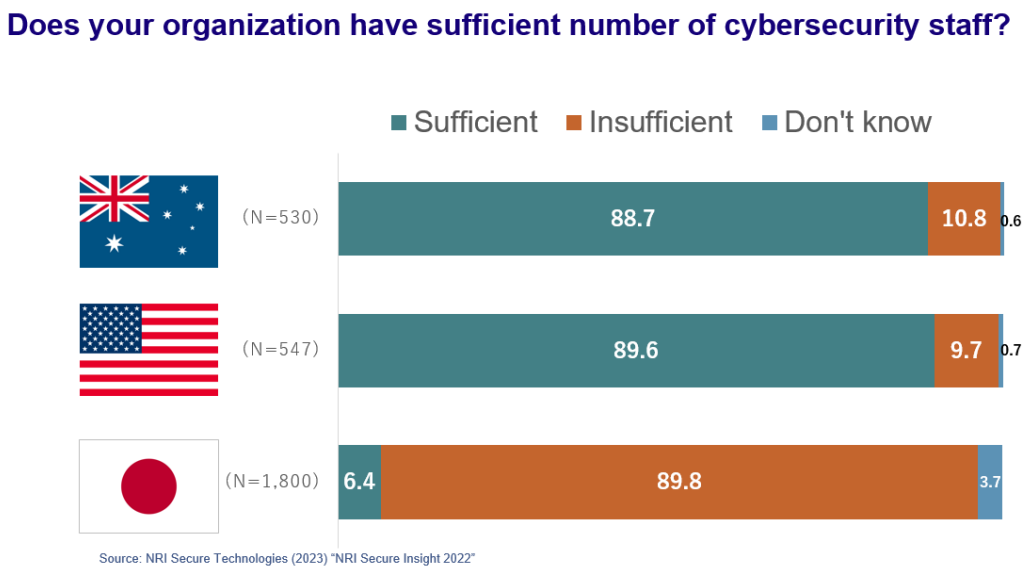

図14.1：NRI Secure Technologiesのサイバーセキュリティ人材に関する調査結果

オーストラリアと米国の組織のほぼ90%が「十分なサイバーセキュリティ人材を保有している」と回答しています。一方、日本の組織のほぼ90%は「十分な人材を保有していない」と回答しています。大きな違いですね!

ちなみに、同じ調査では、組織内にCISOのポジションがあるかどうかを尋ねる別の質問もあります。結果によると、オーストラリアと米国の組織のほぼ97%が「CISOを設置している」と回答しています。しかし、日本では組織内にCISOがいるのはわずか42%です。

2 NRIセキュアテクノロジーズ(2023)『NRI Secure Insight 2022』https://www.nri-secure.co.jp/news/2023/0201-2

日本のサイバーセキュリティチームの人員不足が深刻なため、サイバーセキュリティ担当者は、直面する脅威への対応、インシデントの対応、規制関連業務などに追われており、将来の改善に時間を割くことができない場合があります。

第二に、日本の企業には内部のITエンジニアが非常に少ない状況です。以下は、日本の総務省が実施した調査の結果です。3

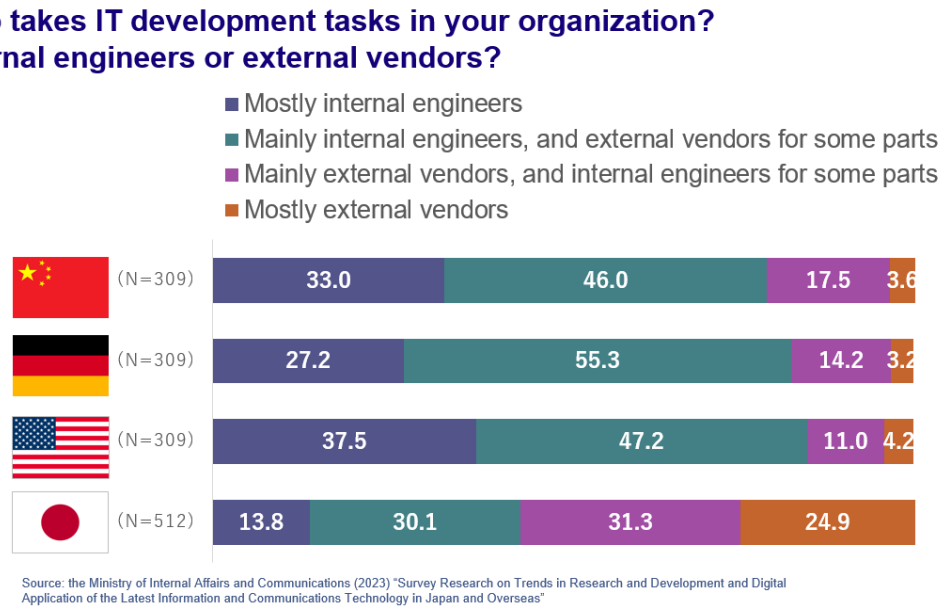

図14.2：総務省のIT開発タスク配分に関する調査結果

この調査の質問は、「貴社のIT開発タスクは内部のエンジニアか外部ベンダーか、いずれが担当しているか？」というものです。4つの選択肢が提示されています。最初の2つの選択肢は、組織が内部でIT開発の能力を有していることを意味します。最後の2つの選択肢は、組織がIT開発において外部ベンダーに依存していることを意味します。

中国、ドイツ、米国の3カ国では、これらの国における組織の約80～85%が内部でIT開発の能力を有しています。

3 総務省（2023）『日本国内外における最新情報通信技術の研究開発動向及びデジタル活用に関する調査研究』https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/excel/f00350.xlsx

一方、日本においては、その割合は44%に留まっています。日本の組織の過半数が外部ベンダーに依存していると回答しており、四分の一はIT開発を完全に外部ベンダーに依存していると回答しています。

これはサイバーセキュリティソリューションの導入において何を意味するのでしょうか?

サイバーセキュリティツールの導入やその概念検証(POC)には、多くの実践的な作業が伴います。しかし、日本の組織ではこれらの作業を外部のベンダーに依頼する必要があります。当然、コストがかかります。

一部の日本の金融機関は、上記のような状況下で生き残れないと感じ、社内エンジニアリング能力の確保を試みています。これは良い動向であり、この方向性を支援し推進していきたいと考えています。

日本の金融機関が直面する最後の課題は、ITチーム構造に関するものです。非日系企業の場合、ITシステムを構成する各技術スタックや機能は、その分野のスキルと経験を持つメンバーで構成されるチームが担当しています。

この構造の利点は、各領域が専門知識を持つ人材によって横断的に管理されるため、標準化が自然に促進される点です。また、多くのセキュリティ製品は各領域をカバーしているため、この構造は組織全体にツールを適用する際に比較的容易です。例えば、異なるアプリケーション領域に異なる証明書管理ツールを配備するのではなく、すべてのITシステムをカバーする単一のツールを実装するだけです。

一方、日本の銀行、特に伝統的な大手銀行では、ITチームは業務アプリケーション領域ごとに組織化されていることが多くあります。各チームには、ITインフラストラクチャ、セキュリティ、ITサービス管理の機能が含まれています。これは業務アプリケーションごとに一元化されたチーム構造です。

以下に、これらの2つのITチーム構造のイメージを示します:

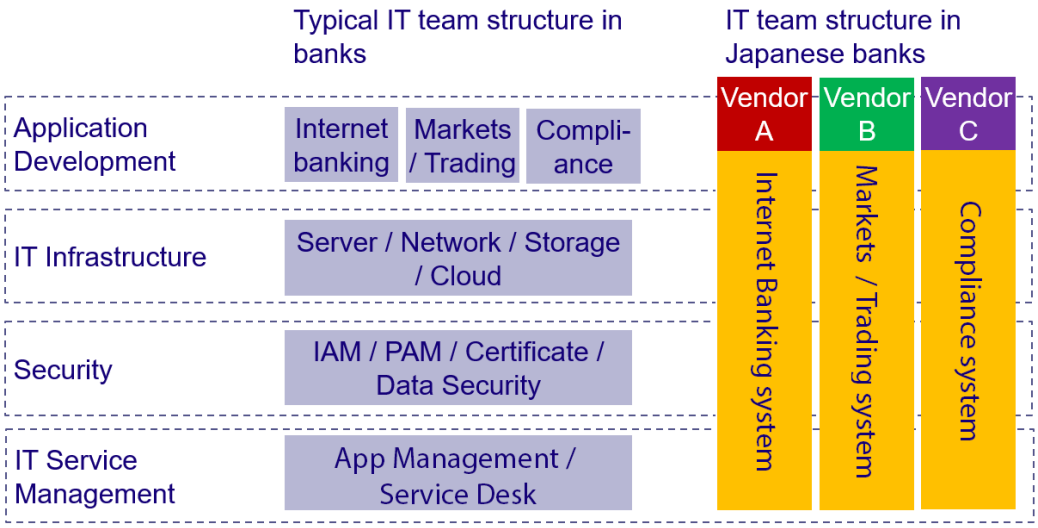

図14.3: 2種類のITチーム構造

日本のITチーム構造では、特定の事業領域において最適化された迅速な意思決定とリソース配分が実現されると考えられています。しかし、組織全体の見地からは、これは限定された領域での最適化であり、組織内に「サイロ」を生むことになります。

この構造は、特定の機能を実現するための単一のツールを導入し、専門家が組織全体をカバーして活用する際に適していません。例えば、組織全体にクリプトインベントリーを作成する管理ツールを導入する場合、このチーム構造では、誰が責任を持って導入をリードするかが明確ではありません。

これは従業員だけの問題ではありません。図14.3に示すように、異なるベンダーが異なる事業領域をサポートするケースも少なくありません。こうした構造は、耐量子計算機暗号（PQC）への移行のような全社的なプロジェクトを調整することを困難にします。これらのプロジェクトは、全体的な可視性とクロスファンクショナルなチームワークを必要とします。

これらが、日本の金融機関が直面している課題です。CISOの役割は、従来の組織構造に慣れたCIOや他の経営幹部と協力し、これらの課題を克服することです。

CIOは、IT組織の効率化を常に模索しています。私たちはCIOと、水平型組織の必要性と有用性について議論し、変革のアプローチを共に検討しています。例えば、私の場合、現在システムごとに管理されている電子証明書を銀行全体で統一した方法で管理する仕組みの導入と、これに沿った横断的な組織の設立をCIOに提案しました。

行動の呼びかけ：日本からの情報を世界と共有する

日本の企業のCISOは、日本がグローバルなサイバーセキュリティ分野における立場を理解し、よりグローバルな視点で他者と協力する努力をすべきだと提案します。

中国、北朝鮮、ロシアに囲まれ、台湾からわずか111kmの地理的条件から、日本は世界でも類を見ない関係性を各国と築いてきました。政治、ビジネスから家庭レベルまで、あらゆる面で親密さと警戒心が交錯する複雑な関係にあります。

サイバーセキュリティの観点から、ハイブリッド戦争が実践的な戦術として用いられていることを知る私たちは、地域で危機が発生した場合、日本は間違いなくサイバー攻撃の標的となることを理解しています。また、機密情報の盗難リスクについても深刻な懸念を抱えています。

一方、日本国内で発生するサイバーインシデント、攻撃手法、脅威アクターの活動について、世界の他の地域のCISOと共有できているとは言い難い状況です。もちろん、IPA（情報処理推進機構）やJPCERT/CC（JPCERTコーディネーションセンター）のような公的機関が英語で情報を提供していることは承知していますが、私の知る限り、日本の金融機関やコミュニティから海外への情報共有は十分ではありません。

現在、機械翻訳が発展したことで、海外の人が日本から送信される日本語の情報を取得し理解することは技術的に可能です。しかし、日本語を母国語として使用する私たちと、海外の人の情報収集能力には違いがあるでしょう。さらに、日本の独自の地政学的立場を考慮すると、日本の企業のCISOは、世界他の地域との情報共有においてより積極的であるべきです。

私の結論

これまでの執筆内容を見返してみると、私は日本の金融機関がサイバーセキュリティ対策を進める上での障壁に焦点を当ててきたことに気づきました。否定的な意図はありませんが、このような障壁が日本の金融機関のCISO（最高情報セキュリティ責任者）に、独特な挑戦とやりがいをもたらす経験を提供してきたと感じています。

日本の企業の人事制度は、長年培われた雇用慣行や文化と深く結びついており、他の地域と同等の柔軟性を実現するには相当な時間がかかります。

このような制約下で、CISOとしてできる限りの努力を尽くすことが私の責務です。例えば、サイロ化されたシステム環境とオペレーティングシステムの標準化に取り組んでいます。当行には多くのインターネットゲートウェイが存在し、そのうちの一部はIT部門で管理されていません。これらのゲートウェイを標準化されたゲートウェイに統合する取り組みを進めており、このイニシアチブは経営陣の支援を受けており、サイバーセキュリティの強化に効果的だと考えています。

この取り組みは、サイバーセキュリティの強化だけでなく、みずほ銀行のITインフラを安全かつ業務の俊敏性を高めるものとして構築する努力を促進する点でも、私のキャリアにとって非常にやりがいのある挑戦です。

私は、これが私の優先事項のトップに位置付けられていることに非常に前向きです。また、日本の企業におけるCISOには、このような前向きで挑戦的な精神が求められると信じています。先ほど述べた人事制度のため、日本のCISO全員が自らCISOになることを動機付けられていないかもしれませんが、日本のCISOには、CISOが単に企業や顧客をサイバー攻撃から守るだけでなく、社会の安全にも貢献する重要な役割を果たしていることをより認識してほしいと思います。

私は金融ITシステム分野でほぼ30年間働いており、蓄積した知識には自信を持っています。この視点が、特に日本のCISOを目指す方々にとって、サイバーセキュリティへのアプローチを検討する際の参考になれば幸いです。

デビッドの主要なポイント – 日本のCISO

日本を管轄対象に含むグローバルまたは地域レベルのCISOにとって、この役割を真に果たすためには、年1回の日本訪問を超える深い理解が不可欠です。日本は私が住んだ他の地域よりも社会的な複雑さが格段に高く、サイバーセキュリティもその現実を反映しています。

日本を効果的に保護するために、CISOが対処しなければならない独自の教訓が存在します。多くのグローバル企業にとって、日本は売上と成長の機会においてトップ3の貢献国です。

この章の教訓は、日本をグローバルな業務範囲に含むCISOや、この国に拠点を置くチームと協力するCISOにとって、洞察を提供します。リーダーとしてこれらの微妙な違いを理解することは、あなたの役割での成功に役立ちます。

この章からの私の主な学びは以下の通りです：

- 役職年数要件 - 日本には役職年数に基づくキャリアシステムが存在し、CISOは技術的専門知識に関わらず、一定の年齢に達するまで任命されない場合があります。この文化的なアプローチにより、日本のCISOの在任期間は国際的な同業者と比べて短い傾向にあります。
- ジェネラリストではなく専門家 - 日本企業のサイバーセキュリティ人材プールは、営業やコンプライアンスなどのビジネス部門から内部異動してきた「ジェネラリスト」が中心で、技術的な背景が薄い傾向があります。CISOはこれらの専門家にトレーニングを提供し、マインドセットの変革と必要な技術スキルを育成する必要があります。
- リスク回避文化 - 日本の組織は極めてリスク回避的で、リスク受け入れはCISOにとって課題となっています。CISOは、個人的な恐怖ではなくビジネスロジックに基づく意思決定を促進するため、合理的でデータ駆動型のリスク評価を提供する必要があります。
- リソース制約が深刻 – （サイバーセキュリティ業務の）空きポジションは11万件を超えています。これらの制約により、サイバーセキュリティチームは戦略的な改善ではなく、直近の脅威への対応に重点を置かざるを得ず、ロードマップのソリューション実装が大幅に遅れています。この状況は、日本チームと協力する際の参考となり、CISOとしてこの地域を担当する場合にも役立ちます。

- サイロの打破 - 日本の銀行におけるサイロ化は深刻で、ITチームは通常、技術スタックではなくビジネスアプリケーション領域ごとに組織化されており、企業全体でのツール展開に抵抗するモノリシックなチームが形成されています。この構造は、企業全体での標準化されたセキュリティソリューションの展開を困難にし、広範な調整 努力を必要とします 。
- 脅威インテリジェンス – 日本のCISOは、国際的なサイバーセキュリティコミュニティと脅威インテリジェンスやサイバーインシデント情報を積極的に共有し、グローバルなサイバーセキュリティの取組みから恩恵を受けるべきです。この広範なネットワークは、日本のCISOがグローバルコミュニティから学ぶ上で役立ちます。