２Ｅ２５

ESG 経営における CXO に必要なサイバーリスク対策 Capability の考察

○安岡 祥吾（東京理科大学大学院，パロアルトネットワークス株式会社）

1. はじめに

昨今の DX の加速や、働き方改革によってデジタル活用が進む中で、セキュリティインシデント、つまりサイバー空間での事件・事故が増加している。企業においてはセキュリティインシデントの発生はビジネスの存続に重大な影響を与える「重要なリスク」の一つになっている。特に日本企業においてはサイバーリスクに対する財務的な影響(リスクファイナンス)や継続的なサイバーセキュリティ運用の重要性が増していると実感している。

そこで、本研究では日本企業におけるサイバーセキュリティリスク対策(以下、セキュリティ対策)のリーダーである CISO（Chief Information Security Officer：最高情報セキュリティ責任者)に焦点をあて、セキュリティ対策の陣頭指揮を執るために必要な Capability を再考し、特に経営的観点において必要とされる能力とは何か、考察することを目的としている。

なお、セキュリティ対策を適切に行うことは「費用対効果が得られない」「どれだけやってもイタチごっこだ」といったネガティブな思考ではなく、「企業の社会的価値向上」「DX やグローバル化といった推進事業の安心した促進」といったポジティブな思考へ変換すべきであり、全ての企業におけるイノベーション促進のために重要な要素であると認識し、本テーマを選定した。

2. 研究背景と先行研究調査

本研究を実施する必要性を下記 2 点定義し、リサーチクエスチョンとした。

【セキュリティインシデントの増加と経済影響の拡大】

まず、社会的にみたセキュリティ対策の重要性はどう考えられているのか、先行調査行った。

調査は国内外の代表的なリスクレポートを選定し、文献レビューにて実施した。表 1 はドイツのアリアンツ保険会社による「2023 年　最も重要なグローバルビジネスリスク指標」である。コロナウイルスのパンデミックや世界的な半導体不足、気候変動といった様々なリスク環境がある中で、サイバーインシデントが前年に引き続き第 1 位（34%）にランクされている。サイバーインシデントとは、サイバー犯罪、システムダウンを引き起こすマルウェア/ランサムウェア、データ侵害、罰金および罰則などのことであり、サイバー攻撃はサイバーインシデントそのもの、または事件・事故を引き起こす主要な原因となっている。アリアンツによれば、サイバー犯罪事件による世界経済の損失は年間 1 兆ドルを超え、世界の GDP の約 1%を占めると推定されている。

表 1　2023 年、最も重要なグローバルビジネスリスク指標

順位	投票	動向	ビジネスリスク	例・備考
1	34%*	→	サイバーインシデント	サイバー犯罪、システムダウンを引き起こすマルウェア/ランサムウェア、データ侵害、罰金および罰則
2	34%*	→	ビジネス中断	サプライチェーン分断を含む
3	25%	↑	マクロ経済の発展	インフィレ・デフレ、通貨政策、緊縮政策
4	22%	↑	エネルギー危機	供給不足/停電、価格変動
5	19%*	→	法と規制の変更	貿易戦争と関税、経済制裁、保護主義、ユーロ圏崩壊
6	19%*	↓	自然災害	暴風雨、洪水、地震、山火事、極端な気象現象
7	17%	↓	気候変動	地球温暖化による物理的、運用的、財務的リスク
8	14%*	→	熟練労働者の不足	
9	14%*	↓	火災、爆発	
9	13%	→	政治リスクと暴力	政治的不安定、戦争、内乱、ストライキ、暴動、略奪

*：同じ%であっても、順位が上の事象の方が回答実数が多い。

出所：Allianz (2023)『Allianz Risk Barometer　Identifying the major business risks for 2023』から作成

表 2 は日本におけるリスク要因トップ 10 であり、ここでもサイバーインシデントは前年に引き続き第 1 位（51%）にランクされている。すなわち、サイバーセキュリティリスクは、グローバル、日本とも最大のビジネスリスク要因となっているのである。実際、業界や事業規模を問わず標的になる可能性があり、経済のみならず、社会的にも緊急かつ高度な対策が求められていると言える。

表 2　日本におけるトップリスク 10

順位	投票	動向	ビジネスリスク		順位	投票	動向	ビジネスリスク
1	51%	→	サイバーインシデント		6	12%	↑	政治リスクと暴力
2	35%	→	自然災害		7	9%	↑	法と規制の変更
3	33%	→	ビジネス中断		7	9%	↑	エネルギー危機
4	30%	↑	気候変動		9	7%	↑	火災、爆発
5	16%	↑	新技術		9	7%	↑	マクロ経済の発展

出所：Allianz Global Corporate & Specialty

このような状況であるにもかかわらず、2023 年に入っても日本企業でのセキュリティインシデントは連日のようにニュースに登場し、大企業を中心に数万を超える情報漏洩や操業停止といった結果を招いている。しかし、ニュースで報道され、詳細な報告書を発行している企業はまだ健全あると思っている。なぜならば、セキュリティインシデントは自社が被害を受けていることを発見すること自体が出来ていない企業も多く存在する可能性があり、また、自社が攻撃を受けることによって、取引先企業(サプライチェーン)が被害を受けるといった可能性もある。各企業がこの状況を正しく理解し、抜本的な対策を講じるためにはどうすればいいか、これがリサーチクエスチョンの 1 点目である。

【ワンショットではない継続的なセキュリティ対策の重要性】
2 点目のリサーチクエスチョンは、セキュリティ対策は継続することが重要であるにも関わらず、これが実施できる体制を構築できている企業が少ないと実感したことである。サイバーセキュリティリスクはこれまでも、これからも常に変化し続けるため、継続的な対策が求められる。セキュリティ専門部署を作ったら終わり、セキュリティ対策製品を導入したら終わり、ではない。自社のサイバーセキュリティリスク分析、それに応じたセキュリティ対策戦略の確立はファーストステップにしかすぎず、下記のように継続的なセキュリティ対策が必要だと考えている。
・自社のビジネス変化に応じた継続的なサイバーセキュリティ戦略の見直し
・投資対効果(ROI)の定点観測とセキュリティ対策における KPI の定義と達成管理
・セキュリティ対策の平時運用と有事運用の定義化

では、上記 2 点を把握した上で、企業がとるべき施策は何か、これが本研究のリサーチクエスチョンである。

3. 仮説と研究方法

前述のリサーチクエスチョンを解決するために、継続的なセキュリティ対策のリーダーシップを発揮する役割が重要であり、CISO の設置が必要だと仮説を立てた。では、CISO に求められる Capability とは何か。CISO の Capability に関する研究は海外を中心に行われており、本研究での技術的 Capability のスキルセットについてはそれらを参考にしている。一方で経営的観点での Capability について詳細に触れられているケースはほとんど確認できず、サイバーセキュリティと経営の相関関係を論じた研究はほとんど発見できなかった。先行研究調査と日本企業における CISO の役割といった観点で文献レビューを行ったところ、下記のような結果を得られた。
・日本における CISO というポジション自体の設置率の低さ
・CISO に求められる Capability の技術的スキルへの偏り
・技術と経営の両利きで戦略を考えられる人材の少なさ(両方求めることへのハードルの高さ)

これらを踏まえ「現実的な CISO の Capability」を考察するために国内外の文献レビューを実施した。上記内容については研究論文だけでなく、外部シンクタンクや各国、民間企業が発行しているレポート等から包括的にデータ収集を行い、必要情報の抽出と精査をデータマイニングと精読により分析した。

なお、学術論文へ民間レポートを引用するにあたり、以下の点を考慮し分析を行なった。
・情報ソースとしての発行元企業、団体の信頼性評価
・バイアス認識と複数ソースの確認
・適切な出典元と発行対象、年式等の確認

4. 結果の考察と今後の展望

【日本企業における CISO の定着度】
2022 年時点での日本企業における CISO の設置率は「39.4%」であった(企業における情報セキュリティ実態調査 2022 より抜粋)。同じ調査で米国の結果は「96.2%」であった。セキュリティ対策には「人、モノ、金」というリソースが必要である。このリソースを確保し、最適化し、マネジメントしていくことが CISO の役割であることを考えると、この結果はそのまま日本企業のセキュリティ対策レベルを示していると言っても過言ではないかもしれない。特に、「継続的なセキュリティ対策」の意識が高くないが故に、CISO という役割の重要性を理解しきれていない企業が多いとも考えられる。

【日本企業における CISO の Capability のまとめ】
様々な文献を参考にし、日本企業における CISO に必要な Capability を「技術/経営」「平時/有事」でプロットし、それぞれの KPI を定義した。その中で、本研究で特に重要だと結論づけたのは「情報開示」である。

図 1　日本企業における CISO に必要な Capability マトリックス(筆者作成)

	平時 Peacetime	有事 Emergency	指標 KPI
技術 Technology	・セキュリティポリシー策定 ・セキュリティガバナンス策定 ・セキュリティトレーニング	・CSIRT運用 ・インシデントレスポンスリード (被害の拡大防止と) ・外部連携 (ISACやJPCERT/CC、セキュリティベンダーとの連携指揮)	・MTTD：平均検出時間 (Mean Time To Detection) ・脆弱性対応スピード
経営 Management	・予算化 ・リスク計画 (リスク分析/リスク対応計画の策定) ・コミュニケーション **・情報開示**	・ステークホルダーマネジメント **・クライシスマネジメント** **(マスコミ対応、プレス発表等)** ・事後対応/対策力	・MTTR：平均対応時間 (Mean Time To Response) ・費用対効果

【ESG 経営におけるセキュリティ対策情報開示の重要性】
現在のところ、日本ではセキュリティ対策について法的に定められている「開示義務」はない。しかし、昨今では ESG 情報(企業が長期的に成長するために経営に必要な観点)の開示が広がっており、投資判断情報や企業の格付けとしても用いられている。表 3 のように、サイバーセキュリティは ESG 情報開示の要素の一つとしてスタンダードとして定義されている。

表 3　IFRS サステナビリティ開示基準

領域	環境	社会資本	人的資本	ビジネスモデルとイノベーション	リーダーシップとガバナンス
一般問題カテゴリ	・GHG 排出 ・大気質 ・エネルギー管理 ・水及び下水管理 ・廃棄物及び危険物管理 ・生態系への影響	・人権と地域社会へのつながり **・顧客のプライバシー** **・データセキュリティ** ・アクセスとアフォーダビリティ ・製品の品質と安全性 ・顧客の福祉 ・販売慣行と製品のラベリング	・労働慣行 ・従業員の健康と安全 ・従業員のエンゲージメント、多様性とインクルージョン	・製品設計とライフサイクル ・ビジネスモデル回復力 ・サプライチェーン管理 ・材料の調達と効率 ・気候変動の物理的影響	・経営倫理 ・競争行動 ・法規制環境の管理 ・クリティカルインシデントリスク管理 ・システミックリスク管理

ESG 情報開示については、今後開示の必要性が増加する、もしくは詳細な情報開示の義務化も十分に考えられる。金融庁が公表した「企業内容等の開示に関する内閣府令」においても下記の通り言及されている。
・有価証券報告書等に、「サステナビリティに関する考え方及び取組」の記載欄を新設する
・「ガバナンス」及び「リスク管理」については、必須記載事項とする
・「戦略」及び「指標及び目標」については、重要性に応じて記載を求めることとする

上記は「令和５年３月 31 日以後に終了する事業年度に係る有価証券報告書等から適用」とあるが、更に注目すべきは以下のコメントである。
「サステナビリティ情報については、現在、国内外において、開示の基準策定やその活用の動きが急速に進んでいる状況であるため、サステナビリティ情報の開示における「重要性（マテリアリティ）」の考え方を含めて、今後、国内外の動向も踏まえつつ、本原則の改訂を行うことを予定しています。※金融庁 「企業内容等の開示に関する内閣府令」等の改正案に対するパブリックコメントの結果等について(一部抜粋)」
これはつまり、今後セキュリティリスクに対する情報開示がより厳密に義務化され、より詳細な情報開示が求められる可能性があることを示唆している。具体的には下記のような情報の開示が義務化されてもおかしくはない。
・最新の脅威を考えた対策を講じているか(脅威/リスクを定義し、その具体的な対策)
・対策内容を適切に開示しているか(総務省作成の「サイバーセキュリティ対策情報開示の手引き」にあるように攻撃者にとって有益になる情報を伏せる前提で)
・具体的な脅威および対策を講じるためのリーダーシップがあるか(CXO や Board メンバーがサイバーセキュリティに通じている/経歴がある)
・リスクの完全排除ではなく、転嫁や分散をしているか(サイバー保険への加入)
・サイバーセキュリティインシデントが発生した際の対応力を明確に示しているか(財務的、非財務的)

これらを踏まえて、適切な情報開示は企業防衛、事業継続と社会的信頼性向上のためにも重要であり、IT や財務、リスク、社内外の組織特性を考慮した情報発信を行うためには、CISO による情報収集、分析、レポーティング力が必要だと結論づけ、CISO の経営的 Capability として「情報開示」と定義した。

また、本研究は継続中であり、今後は一度特定業界に絞って、より深い Capability の考察と、実際の CISO や同等の役割の方へのヒアリングを行い、CISO Capability の精度やリアリティについて考察を深めていきたいと考えている。

参考文献

[1] 情報セキュリティ 10 大脅威，IPA 情報処理推進機構（2014-2023）
[2] Allianz Risk Barometer　Identifying the major business risks for 2023，Allianz (2023)
[3] ESG 情報開示枠組みの紹介，JPX 日本取引所グループ
[4] 企業内容等の開示に関する内閣府令（2023）
[5] 情報セキュリティ白書，IPA 情報処理推進機構（2008-2023）
[6] データ侵害のコストに関する調査，IBM セキュリティ（2022）
[7] PDCA サイクルと OODA ループ，厚生労働省（2022）
[8] Exploring the Role of Chief Information Security Officer Capabilities in Cybersecurity Risk Management (2021)
[9] Assessing the Competencies of Chief Information Security Officers (2018)
[10] NRI Secure Insight 企業における情報セキュリティ実態調査, NRI セキュアテクノロジーズ(2022)
[11] サイバーセ キュリティ対策情報開示の手引き，総務省(2019)