2023 年度グラデュエーションペーパー

予稿

題　　目	
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 *Consideration of cyber risk countermeasure capabilities necessary for CXO in ESG management*	
技術経営論文	ビジネス企画提案

学籍番号	8822241	氏名	安岡 祥吾

教　員	
主査	加藤 晃　教授
担当審査委員	

東京理科大学大学院　経営学研究科　技術経営専攻

「　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　」

目次

第 1 章　研究概要 ..... エラー! ブックマークが定義されていません。

1.1　はじめに ..... エラー! ブックマークが定義されていません。

1.2　研究の背景・目的 ..... エラー! ブックマークが定義されていません。

1.2.1　研究の背景：サイバーセキュリティを取り巻く環境 エラー! ブックマークが定義されていません。

1.2.2　研究の目的：安心安全で持続可能な企業運営のためのサイバーセキュリティ ... エラー! ブックマークが定義されていません。

第 2 章　リサーチクエスチョンとリサーチデザイン . エラー! ブックマークが定義されていません。

2.1　リサーチクエスチョン ..... エラー! ブックマークが定義されていません。

2.1.1　企業経営におけるサイバーセキュリティリスクの認知度、優先度の認識 . エラー! ブックマークが定義されていません。

2.1.2　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 エラー! ブックマークが定義されていません。

2.2　仮説とリサーチデザイン ..... エラー! ブックマークが定義されていません。

2.2.1　仮説 ..... エラー! ブックマークが定義されていません。

2.2.2　文献レビュー手法 ..... エラー! ブックマークが定義されていません。

第 3 章　サイバーセキュリティについての調査と考察 .. エラー! ブックマークが定義されていません。

3.1　サイバーセキュリティの動向 ..... エラー! ブックマークが定義されていません。

3.2　最新のサイバー攻撃や脅威に関する調査と考察 エラー! ブックマークが定義されていません。

3.2.1　ランサムウェア：Wannacry を発端としたサイバー攻撃ビジネスモデルの確立 . エラー! ブックマークが定義されていません。

3.2.2　サプライチェーン攻撃：大阪急性期・総合医療センターにおける国内での被害事例 ..... エラー! ブックマークが定義されていません。

3.2.3　AI を活用したサイバー攻撃：これからのサイバー攻撃と脅威 エラー! ブックマークが定義されていません。

第 4 章　サイバーセキュリティ対策 ..... エラー! ブックマークが定義されていません。

4.1　サイバーセキュリティ対策.....エラー! ブックマークが定義されていません。

4.2　技術的サイバーセキュリティ対策.....エラー! ブックマークが定義されていません。

4.2.1　ゼロトラストセキュリティアーキテクチャ.エラー! ブックマークが定義されていません。

4.2.2　AI を活用した技術的サイバーセキュリティ対策エラー! ブックマークが定義されていません。

4.3　非技術的サイバーセキュリティ対策 .....エラー! ブックマークが定義されていません。

4.3.1　SOC の構築と運用 .....エラー! ブックマークが定義されていません。

4.4　サイバーセキュリティリスクマネジメント....エラー! ブックマークが定義されていません。

4.5　新たな課題と仮説 .....エラー! ブックマークが定義されていません。

第 5 章　サイバーセキュリティの経営的責任：CISO エラー! ブックマークが定義されていません。

5.1　CISO とは .....エラー! ブックマークが定義されていません。

5.2　CISO の役割と責任.....エラー! ブックマークが定義されていません。

5.3　CISO に関する調査レポートと先行研究について. エラー! ブックマークが定義されていません。

5.4　CISO の現状.....エラー! ブックマークが定義されていません。

5.5　CISO の Capability..... 6

5.5.1　平時における Capability.....エラー! ブックマークが定義されていません。

5.5.2　有事における Capability.....エラー! ブックマークが定義されていません。

5.6　中間課題と深掘りすべき内容 7

第 6 章　ESG 経営時代におけるサイバーセキュリティ情報開示.エラー! ブックマークが定義されていません。

6.1　ESG 経営におけるサイバーセキュリティ情報開示の必要性エラー! ブックマークが定義されていません。

6.2　サイバーセキュリティ情報開示.....エラー! ブックマークが定義されていません。

6.3　サイバーセキュリティ情報開示規制とグローバルスタンダード エラー! ブックマークが定義されていません。

6.3.1　事例 1 ：米国の情報開示　米国証券取引委員会(SEC) .エラー! ブックマークが定義されていません。

6.3.2　事例 2：ヨーロッパの情報開示　EU 関連法案と規制...エラー! ブックマークが定義されていません。

6.4　情報開示が不十分であった場合のリスク エラー! ブックマークが定義されていません。

6.5　国内企業におけるサイバーセキュリティ情報開示の調査と考察 7

第 7 章　さいごに ..... エラー! ブックマークが定義されていません。

7.1　今後の研究課題 9

7.2　あとがき 9

用語集 ..... エラー! ブックマークが定義されていません。

参考文献・引用 ..... エラー! ブックマークが定義されていません。

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、サイバーセキュリティインシデント、ネットワークやクラウドといったサイバー空間での事件・事故が増加している。企業においてサイバーセキュリティインシデントの発生は「重要なリスク」の一つになっており、社会生活においてもサイバー攻撃等による実害が発生する割合が増加している。特に日本企業においては、各企業が具体的にどのような対策を講じているのか、ステークホルダーの目線で情報を手にいれるためにはハードルが高いと実感している。これは企業や組織が実際に取り組んでいるサイバーセキュリティへのアプローチを上手くアピールできていない可能性があると考えた。サイバーセキュリティにおいて強力なリーダーシップと、しっかりとした責任モデルを構築するためには、専門の人材が必要だと考えている。

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、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。

研究背景と先行研究調査

下記 2 点の状況を踏まえ、本研究の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】

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。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。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 Risk Barometer　Identifying the major business risks for 2023, Allianz」[3] から作成

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。

【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】
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。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、継続的なセキュリティ対策が必要だと考えている。

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。

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
・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

結果の考察と今後の展望

【日本企業における CISO の現状】
日本企業における CISO の現状を把握するために、実態に関する文献調査を行った。データは、「ＮＲＩセキュアテクノロジーズ株式会社」が 2022 年に発行した「NRI Secure Insight 2022」[18] の情報である。結果として、2022 年時点での日本企業における CISO の設置率は「41.9%」であった。同じ調査で、米国の結果は「97.0%」であった。また、日本企業における CISO の設置率は企業規模によっても大きく差があり、従業員数 1000 人未満の企業では設置率が「37.7%」、従業員数が 10000 以上の企業では「68.1%」であった。サイバーセキュリティ対策には「人、モノ、カネ」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。この実態をさらに詳細に表している情報として、IPA が 2020 年 3 月に発表した「企業の CISO 等やセキュリティ対策推進に関する実態調査 -調査報告書-」[19] によると、日本企業のサイバーセキュリティに対する経営層の認識については下記の通りである。

【経営層のセキュリティ認識】
・経営層のセキュリティに対する全般的なリスク認識は高まっている。
・経営層はサイバーセキュリティに漠然と課題認識を有しているものの、具体的な課題を十分に理解できている経営層は少ない。

CISO の Capability
CISO の現状、役割や課題、日本において設置率を上げるための要件等を加味した上での CISO に必要な要素は何か、それを技術的スキルだけでも、経営的素質でもなく、後天的に獲得可能な能力として定義化することが可能なものという前提のもと、“Capability”としてまとめた。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。

図 1　日本企業における CISO に必要な Capability マトリックス

	平時 Peacetime	有事 Emergency	指標 KPI
技術 Technology 	P：セキュリティポリシー策定 D：セキュリティトレーニング C：脆弱性診断 A：技術的対策	O：SOC運用 O：War Room リード D：インシデントレスポンス A：ポリシー変更	・MTTD：平均検出時間 (Mean Time To Detection) ・脆弱性対応スピード
経営 Management 	P：リスク分析/リスク計画 D：コミュニケーション C：取締役会報告/予算化 A：情報開示	O：SOC運用 O：CSIRT運用 D：経営判断 A：ステークホルダー管理	・MTTR：平均対応時間 (Mean Time To Response) ・費用対効果

出所　筆者作成

中間課題と深掘りすべき内容

CISO の Capability の調査や定義化を行っていく中で、新たな疑問が生じた。技術的/非技術的スキル共にある程度定義化がされているにも関わらず、CISO の定着率が高くないことと、組織のサイバーセキュリティの取り組み状況が見えにくい点である。サイバーセキュリティの取り組み状況の見える化、情報発信、より厳密に言えば「情報開示」については以下の理由からこれからの企業経営において重要なものとなってくる。

・ESG 投資や SDGs の進行により、企業の透明性は必須要件になり始めている

・サイバーセキュリティに関する情報開示は、海外では必須事項になっており、制裁や罰則、訴訟問題に発展するケースも出てきている

そこで、本研究ではさらに CISO の Capability における「情報開示」について深掘りを行った。

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。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。

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。

国内企業におけるサイバーセキュリティ情報開示の調査と考察

ここまで論じてきた情報開示の必要性と日本企業における今後のあり方を考察するために、下記ドキュメントにおける開示情報をまとめ、考察を行った。

・有価証券報告書
・情報セキュリティ報告書
・CSR 報告書
・サステナビリティレポート
・総合報告書(Annual Report)
・コーポレートガバナンス報告書

表 2 は平成 27 年度と平成 28 年度の上場企業における対外的情報開示状況をまとめたものである。全業種で「有価証券報告書」においてはサイバーセキュリティ関連の情報記述がされている傾向がある。これは平成 16 年 3 月期から有価証券報告書への記載が義務付けられている「事業等のリスク」において、サイバー攻撃やコンピュータウィルスによる被害、及びそれによって生じる情報漏洩や業務影響について記載している企業は多い。また、リスクに対する対策についても触れている企業は比較的多く、うち 2 社は「教育・人材育成」について記載している。「CSR 報告書、サステナビリティレポート、統合報告書」については、「基本方針等の策定状況」や「管理体制」、「教育・人材育成」、「社外との情報共有体制」、「第三者評価・認証」について記載している企業が確認された。なお、「技術・通信」業の企業では、CISO の任命と役割についても記載されており、別途調査した「情報セキュリティ報告書」の発行に関しても、「技術・通信」業は多くの企業が発行していることが確認できた。IT を生業とする企業体はサイバーセキュリティについてもサービスの提供や防衛に対するビジネスを行っている関係から、比較的意識の高い傾向が見てとれた。各企業の CISO は、こうした先行企業の取り組みを参考にし、どういった対策が必要なのかという点よりも、どういった情報発信をすることで、ステークホルダーや社会に対して安心感を与えられるのか、意識すると良い。

表 2　上場企業におけるサイバーセキュリティ関連の開示状況

大分野	中分野	記載の有無					
		有価証券報告書		CSR 報告書 サステナビリティレポート 統合報告書		コーポレートガバナンス報告書	
		平成 27 年度	平成 28 年度	平成 27 年度	平成 28 年度	平成 27 年度	平成 28 年度
技術	医薬品	○	○	×	×	○	○
	電気機器	○	○	○	○	×	×
	自動車	○	○	○	○	○	○
	通信	○	○	○	○	○	○
金融	銀行	○	○	○	○	×	×

	証券	○	○	○	○	×	×
	保険	○	○	○	○	×	×
消費	食品	×	×	○	○	×	×
	小売業	○	○	×	○	×	×
	サービス	○	○	×	×	○	○
素材	化学	○	○	×	×	×	×
	窯業	×	○	×	○	○	○
	非鉄・金属	○	○	○	○	○	○
	商社	×	×	×	○	×	×
資本財・その他	建設	○	○	○	○	×	×
	機械	○	○	○	○	×	×
	不動産	×	×	×	○	×	×
運輸・公共	鉄道・バス	○	○	○	○	×	×
	海運	○	○	○	○	×	×
	電力	○	○	－	×	○	○

出所　「企業のセキュリティ対策に係る情報開示の実態等に関する調査」[27] より筆者作成

今後の研究課題

今回の研究を通して、企業継続のための CISO の役割や Capability についての考察はできたが、分かったことは、サイバーセキュリティに関する情報の過多と、情報の速さである。膨大な情報の中から、最適かつ正確な情報を、最適なタイミングで入手し、自社の戦略やサイバーセキュリティ運用に役立てることも、CISO 及びサイバーセキュリティに関わる職種では必要だと感じた。この最適情報の収集は、詰まるところ情報開示にも直結する重要なスキルであると考えている。

また、情報開示に関しても、現在検討されている情報開示に関するガイドライン等の検討状況や、それを踏まえた日本企業での今後のあり方の予測と対応についても調査することで、ガイドラインに先行した適切な情報開示のあり方を模索できるのではないかと考えている。

あとがき

これからの企業経営には、AI の活用、効率化と開発スピードを増すための DX の推進や競合企業や外部企業とのデータ連携といった具合にサイバー空間でのデータの扱いが重要になることに比例して、サイバーセキュリティリスクの増加、それに伴う対策の新規検討や対策費用の増加といった財務課題も発生する。

そして、ESG 経営において「サイバーセキュリティ」に対する重要性が世界中で高まっていることもあり、上場企業におけるサイバーセキュリティの情報開示はより詳細を求められる方向に向かっている。今回の調査結果や事実を前向きに捉え、今改めて業界内でのサイバーセキュリティに関する情報開示レベルの水平化を意識することにより、自社でできていないこと、やるべきことの棚卸しに、また、しっかり実施していることを適切に開示するこ

とでステークホルダーやサプライチェーンにとって安心材料になると確信している。本研究が、本当の意味でサイバーセキュリティ脅威に怯えることなく、純粋に研究や開発、競争を行うことで、日本企業のイノベーションを加速的に促進する DX を実現する一助となれば幸甚である。

参考文献・引用

1. 独立行政法人 情報処理推進機構: DX 白書 2023. https://www.ipa.go.jp/publish/wp-dx/dx-2023.html,2023
2. ソニー・ホンダモビリティ株式会社: 企業情報. https://www.shm-afeela.com/ja/corporate/ , 2022
3. *Allianz: Allianz Risk Barometer Identifying the major business risks for 2023*. 2023
4. 総務省: 令和 5 年度版 情報通信白書. 2023
5. 地方独立行政法人大阪府立病院機構　大阪急性期・総合医療センター: 情報セキュリティインシデント調査委員会報告書. https://www.gh.opho.jp/pdf/report_v01.pdf, 2023
6. *Lockheed Martin: Cyber Kill Chain® framework.* https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, 2019
7. 独立行政法人 情報処理推進機構: 情報セキュリティ 10 大脅威. 2014-2023
8. *Bloomberg: Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak.* https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak, 2023
9. *Mandian*: 攻撃者による生成 AI 利用への関心が高まる。一方で、その利用は依然として限定的. https://www.mandiant.jp/resources/blog/threat-actors-generative-ai-limited, 2023
10. *PwC: NIST SP800-207* 「ゼロトラスト・アーキテクチャ」の解説と日本語訳. https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture-jp.html, 2020
11. 日本マイクロソフ: *Microsoft 365 Copilot* を発表 – 仕事の副操縦士. https://news.microsoft.com/ja-jp/2023/03/17/230317-introducing-microsoft-365-copilot-your-copilot-for-work/, 2023
12. *Google Cloud: Supercharging security with generative AI.* https://cloud.google.com/blog/products/identity-security/rsa-google-cloud-security-ai-workbench-generative-ai?hl=en, 2023
13. 山田 道洋、菊池 浩明、松山 直樹、乾 孝治: 個人情報漏洩の損害額の新しい数理モデルの提案. 情報処理学会論文誌 Vol.60 No.9 1528–1537, 2019
14. 株式会社ベネッセホールディングス: 第 61 期第 1 四半期決算報告書. https://pdf.irpocket.com/C9783/SAip/g8DO/UCks.pdf

15. 株式会社ベネッセホールディングス: 令和 5 年 2 月 27 日東京高等裁判所判例. https://www.courts.go.jp/app/files/hanrei_jp/950/091950_hanrei.pdf
16. 一般社団法人　日本サイバーセキュリティ・イノベーション委員会: 取締役会で議論するためのサイバーリスクの数値化モデル. https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf, 2018
17. 特定非営利活動法人日本ネットワークセキュリティ協会: *CISO* ハンドブック. https://www.jnsa.org/result/2018/act_ciso/, 2018
18. NRI セキュアテクノロジーズ: *NRI Secure Insight* 企業における情報セキュリティ実態調査. 2022
19. 独立行政法人 情報処理推進機構: 企業の *CISO* 等やセキュリティ対策推進に関する実態調査. https://www.ipa.go.jp/archive/security/reports/2019/ciso.html, 2020
20. *Wikipedia: OODA* ループ. https://ja.wikipedia.org/w/index.php?title=OODA%E3%83%AB%E3%83%BC%E3%83%97&oldid=68251854, 2018
21. 日本取引所グループ: *ESG* 情報開示枠組みの紹介. https://www.jpx.co.jp/corporate/sustainability/esgknowledgehub/disclosure-framework/03.html,
22. 金融庁: 企業内容等の開示に関する内閣府令. https://elaws.e-gov.go.jp/document?lawid=348M50000040005_20230401_505M60000002011, 2023
23. 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. https://www.fsa.go.jp/news/r4/sonota/20230131/20230131.html, 2023
24. 総務省: サイバーセキュリティ対策情報開示の手引き. https://www.soumu.go.jp/main_content/000630516.pdf, 2018
25. atmarkIT: SolarWinds、米国証券取引委員会に詐欺行為と内部統制の不備で告発される. https://atmarkit.itmedia.co.jp/ait/articles/2311/13/news048.html
26. *SEC : SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures.* https://www.sec.gov/news/press-release/2023-227, 2023
27. 経済産業省: 企業のセキュリティ対策に係る情報開示の実態等に関する調査. 2018