有価証券報告書にみるサイバーセキュリティリスクに対する認知の抽出と分析

今村 光良[1,a)]　面 和成[1]

概要：サイバーセキュリティは企業経営の根幹を揺るがす重大なリスクである．企業のセキュリティリスクへの対応状況を知る一つの方法としては，展開されるサービスやシステムを介して技術的な脆弱性やリスクを洗い出すアプローチがある．一方で，こうしたリスクに対処する企業の姿勢や認知にはばらつきが見られ，それは人的リソース，経済的コスト，他のリスクとの相対的優先度などの要因によって左右される．このような背景を踏まえると，企業が持つ潜在的なセキュリティリスクの認知を把握することは，技術的課題とは異なる視点からリスク対応能力の実態を浮き彫りにすることにつながる．本研究ではこの観点から，企業のセキュリティリスクに対する認知を捉えるアプローチとして，公表資料に対する LLM を用いた抽出・分類のパイプラインによる分析に着目した. 具体的には，企業が対外的に報告する文書のうち、有価証券報告書に含まれるサイバーセキュリティに関する記述を対象とし，そこに現れる記載傾向を分析することで，企業の潜在的なリスク認知やその傾向を分析する．日本の上場企業 3,580 社に，上場市場や産業別など記載内容を分析した結果について報告する．

キーワード：サイバーセキュリティリスク，リスク認知，LLM，金融情報

Empirical Analysis of Corporate Cybersecurity Risk Awareness Based on Annual Reports

Mitsuyoshi Imamura[1,a)]　Kazumasa Omote[1]

Abstract: Cybersecurity poses a serious risk that could undermine the very foundations of corporate management. One way to assess a company's response to security risks is to identify technical vulnerabilities and risks through the services and systems it deploys. However, there are variations in how companies address such risks, and these variations are influenced by factors such as human resources, economic costs, and the relative priority of other risks.Given this background, understanding companies' awareness of their potential security risks can help reveal the actual state of their risk response capabilities from a perspective different from that of technical issues. In this study, we focus on an approach to capturing companies' awareness of security risks by analyzing publicly available documents using an LLM-based extraction and classification pipeline.Specifically, we target descriptions related to cybersecurity contained in securities reports, which are documents reported externally by companies, and analyze the trends in these descriptions to analyze companies' potential risk awareness and trends. We report the results of analyzing the content of 3,580 listed companies in Japan by listing market and industry.

Keywords: Cyber Security Risk, Risk Awareness, LLM, Financial Information

1. はじめに

ソーシャルエンジニアリングやボットネットなどの従来確認されていた攻撃パターン [7] に加え，AI 由来のフェイ

[1] 筑波大学 システム情報系
University of Tsukuba Faculty of Engineering
[a)] imamura.mitsuyosh.kn@u.tsukuba.ac.jp

ク [6] や LLM を用いたフィッシングやコードインジェクション [15] など，企業の事業に対する不確実性の高いサイバーセキュリティリスクの要因は益々増えている．サイバーセキュリティリスクと企業の持続性について調査した実証研究 [13] においても，組織の活動や経済的発展への悪影響が指摘されていることから，サイバーセキュリティリスクは企業にとって，優先度の高い事業リスクと言える．そのため，サイバーセキュリティリスクに対して，企業が持続的に事業を運営できる特徴を持つことや運営できない傾向にあるかどうかを評価できることは，信頼性の保証や課題解決や対策などの改善を図る上でも重要である．

ネットワークに公開される技術的な側面から企業のサイバーセキュリティリスクを評価することに焦点を当てれば，評価方法の 1 つに，インターネットの大規模スキャンデータを用いることで，設定不備や脆弱なプロトコルの利用を把握することでリスクを分析する方法がある [3]．この方法では，リスク要因とボットネット感染の間の定量的な関係を確立するための統計モデルが開発できると報告している．

確かに，技術的な側面からサイバーセキュリティリスクを評価することは，直接的な要因を明らかにするため，客観的な事実の可視化につながり，具体的な解決策を明らかにする有効なアプローチであることに違いない．一方で，その可視化された事実が認知されるか，講じられた対策がうまく機能するかという点において，主体が人であることを考慮すると，必ずしもそうとは言えない．必要性が明らかな場合であっても，当事者の意識や内部リソースの配分状況，組織文化，コスト構造などの観点から，リスクが過小評価されることで認知されなかったり，対策が機能しないことが考えられる．企業におけるサイバーセキュリティリスクの要因と影響について体系的にレビューした研究 [11] では，経営者の特性，企業運営，IT の実践，制度的環境の 4 つのカテゴリーを要因として指摘しており，技術的な側面の背後にある組織的・人的要因の重要性を浮き彫りにしている．つまり，技術的な側面の評価に併せて，人視点の評価が必要だと言える．

この点について，アンケートやヒアリングを通じて企業へ直接調査することで，実態を明らかにする試みもある [2, 16]．しかしながら，広範な調査に物理的な限界があることから，結果に対する分析の偏りや結論の一般化に課題があると言える．

そこで，この課題を解決する 1 つの方法として，本研究では，企業より公開されている文書を対象に，テキスト内容を解析することで，企業がサイバーセキュリティリスクをどのように認知しているか評価することを目指す．具体的には，日本の上場企業が提出する有価証券報告書に焦点を当て，「事業等のリスク」の項目にサイバーセキュリティに関連するリスクが掲載されているか調査する．

大規模言語モデル（LLM）を中心とした抽出・分類のパイプラインを構築することで，サイバーセキュリティリスクに関連する内容を「脅威」と「脆弱性」の 2 つの主要なカテゴリーとして抽出・分類し，掲載の有無について明らかにする．そして，掲載の有無を左右する要因を探るため，上場市場や企業規模，業種，財務などセキュリティリスクを掲載するリテラシーに関連しそうな分類により詳細な分析をする．

これにより，企業におけるサイバーセキュリティリスクの認知をテキストにより評価する方法の実現性と，サイバーセキュリティリスクの認知における傾向や特徴を明らかにする．以降，2 章では関連する技術を紹介し，3 章にて分析方法および結果について示す．4 章では考察を述べ，5 章にて本研究を総括する．

2. 関連研究

まず，本研究の分析手法であるテキストマイニングにおいて，主要な研究アプローチである LLM のバックグラウンドについて抑えておく．Attention 機構を搭載した Transformer [14] の登場によって，自然言語処理分野におけるタスク性能は飛躍的に改善し，性能向上に対する経験則の調査 [8] によって，モデル規模と性能の間にスケール則が発見されたことで，予見される性能向上を求めるように大規模化の一途をたどりながら開発が進められてきた．[18]．取り分け，テキストベースのインタラクションにより出力をコントロールする GPT(Generative Pre-trained Transformer）スタイルの LLM については，タスクに依存しない汎用的な性能の獲得示しており，実行内容を指示したプロンプトにより，翻訳や質疑応答などの特定の自然言語処理タスクに調整したモデル以上に対応できることも示している [1]．人のフィードバックをモデルに反映させた学習 [12] の導入により，更なる性能向上を獲得しており，分析における主流なアプローチとして定着している．また，入力されるテキストの上限に対応するトークン数も増加しており [5]，タスクに対する性能向上への寄与 [9] だけでなく，LLM の課題であった事前学習された知識に依存したタスク処理に，入力に外部から与えた知識を活用することで知識にない回答を導出する RAG(Retrieval-Augmented Generation) [10] と呼ばれるテクニックの適用を実現し，より抽象的かつ汎用的なタスクへの適応を実現している．

つまり，テキスト指示により GPT スタイルの LLM を利用して任意のタスクを処理することは，標準的な手段となっていることがわかる．

それではここで，LLM を用いたテキストマイニングによるセキュリティ分野における活用状況を確認しておく．LLM を対象に，サイバーセキュリティ分野における活用事例を調査した研究 [17] では，適用されているサイバーセキュリティタスクとして，セキュアなコード開発を支援す

る脆弱性やエラーを引き起こすバグの検出，マルウェアの分析を支援するバイナリやログの解析，フィッシングや有害なコンテンツの検知の支援など，幅広いタスクへの適用を指摘している．整理すると，これまでの研究においては，技術的な要因に視点があると言える．

一方で，本研究においては，文章表現から潜在的な認知や前提となる知識に基づく判断の傾向など人を要因とする課題に焦点を当てている点で，異なる課題に焦点を当てていることに留意する必要がある．これは，コンテキストの解釈を，プログラムやログに埋め込まれた内容に応用するのではなく，プログラムやログと対策に間に当てはまる人の認知というコンテキストで読み解くように応用するという点で新しい試みである．

3. 分析

本章では，分析対象となるデータのスペックや条件について紹介し，分析方法について説明する．そして，サイバーセキュリティリスクの掲載有無と掲載に関連する企業分類の分析結果について報告する．

3.1 データ

本研究で使用する有価証券報告書については，金融庁にて運営される，金融商品取引法に基づく有価証券報告書などの開示書類を電子的に開示・閲覧できるシステム (EDINET[*1]) より収集した．2025 年 6 月末時点で東京証券取引所に上場している ETF および REIT を除いた東証プライム市場 (1,623 社)、東証スタンダード市場 (1,570 社)、東証グロース市場 (610 社) の 3803 社の内，直近の傾向を明らかにするため，2024 年度の上場および分析時点において 2023 年度と 2024 年度の 2 期分の有価証券報告書の取得ができた 3,580 社 (内，東証プライム市場：1,572 社，東証スタンダード市場：1,482 社，東証グロース市場：526 社) を分析対象とした．なお，有価証券報告書については，2025 年 7 月 1 日時点で収集できる書類を対象としている．また，提出後に訂正された書類については，訂正された後の書類を分析対象としている．なお，持株会社への株式移転や名称変更などの，おおよそ実体が同一と理解できるコーポレートアクションがあった企業については，同一企業として扱う．

3.2 分析方法

本研究の分析に利用されるサイバーセキュリティリスクに関する文章データは，組成方法を図 1 に示す通り，対象の文章から指定した内容を抽出するスパン抽出問題に対応する Extraction プロセスと，抽出した文章に適切な分類を割り当てる Annotation プロセスの 2 つの工程から構成

[*1] https://disclosure2.edinet-fsa.go.jp

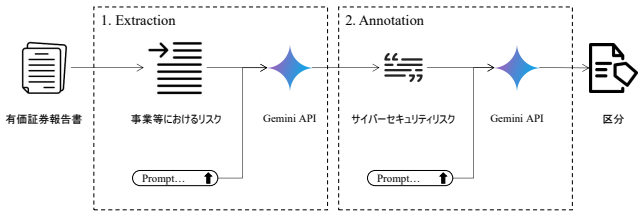

図 1 大規模言語モデル（LLM）を用いたリスク記述の抽出・分類パイプライン

表 1 「該当なし」となる場合

(応答例) 本文中に「情報セキュリティ」という言葉は一度言及されていますが、それは会社がリスク管理の対象としている広範なリスクの一つとして挙げられているだけであり、サイバーセキュリティ攻撃や情報漏洩、システム障害といった具体的なリスクの「要因」と、それによって企業に与える「影響」(「内容」) が詳細に記述されている箇所はありません。
(原文例) 上記の他、金融市況・為替変動・原材料価格高騰によるリスク、コンプライアンスを含むコーポレート・ガバナンス関連リスク、システムトラブルによるリスク、情報漏洩によるリスクなど、様々なリスクが存在しており、ここに記載されたものが当社グループの全てのリスクではありません。

することで実現している．次に各工程の詳細について説明する．

3.2.1 Extraction

有価証券報告書においては，サイバーセキュリティリスクが記載される明示的な表題やタグ付け等がないため，記載内容から関連する文章を抽出する必要がある．この課題をスパン抽出問題として定め，サイバーセキュリティに関連する文章を有価証券報告書に抜き出すプロセスについて設計した．

具体的には，サイバーセキュリティリスクに関する記載部分を抽出するプロンプトに，有価証券報告書の「事業等のリスク」項目に記載されている内容を外部参照用データとして含め，Google 社の提供する大規模言語モデルの API である Gemini API (model:gemini-2.5-flash-preview-05-20) により指定文章の抽出を試みた．なお，記載がないパターンについては，次工程の対象から除外する必要があるため，プロンプトへ該当する文章がない場合は「該当なし」と回答する指示を含めることで対応している．文章中にキーワードのみ登場する場合や，表 1 に示すような応答および対応する原文は，「該当なし」として対象から除外されている．

同一文章に対する抽出の試行回数を 3 回とし，1 度でも外部参照用データを含む文章の出力に成功した場合，その内容を採用する．もし，3 回の内，複数回の抽出に成功した場合は，最も抽出された文章量が多いものを次の工程に利用する文章として採用する．

表 2　サイバーセキュリティリスクの区分

区分番号	要因	種類	内容
1	脅威	意図的脅威	悪意を持った攻撃者による不正アクセス、マルウェア感染、データ改ざんなど
2	脅威	偶発的脅威	従業員のヒューマンエラーによる情報漏洩、誤操作など
3	脅威	環境的脅威	自然災害や、停電、通信障害など
4	脆弱性	技術面の脆弱性	システムやアプリケーションの不備など
5	脆弱性	管理・制度面の脆弱性	運用体制やポリシーの未整備など
6	脆弱性	設備面の脆弱性	災害に弱い立地、セキュリティ設備の不備など

3.2.2　Annotation

意図したサイバーセキュリティリスクに関する文章の抽出の成否を詳細に判断する 1 つの方法として，具体的なリスクを記した辞書を用意し，類似性を測るアプローチがある．そこで，当該プロセスにおいては，ISO27002 や NIST CSF[*2]のフレームワークに倣い，サイバーセキュリティリスクを記した辞書として，表 2 に示した区分に類似する文章が含まれるか分析することで，抽出の成功を判定した．

具体的には，抽出したサイバーセキュリティリスクに関する文章および表 2 を外部参照データとしてプロンプトに含め，サイバーセキュリティリスクの区分が与えた文章に含まれるか抽出した．区分の抽出には，Extraction と同様に Gemini API を利用している．なお，当該プロセスにおいても，該当するパターンがない場合は，「該当なし」と回答する指示を含めている．そのため，一度前工程において，サイバーセキュリティリスクに関する記載があると判断された文章であっても，指示した区分が含まれていないと判定される場合がある．

当該操作についても 3 回の試行があり，1 回でも区分の抽出に成功していれば，その結果を最終的な判断として採用する．複数回の抽出に成功した場合は，最も多く区分を抽出した結果を採用している．

3.3　サイバーセキュリティリスクの記載内容集計

まず，有価証券報告書より抽出したサイバーセキュリティリスクに関する文章の記載有無について報告する．図 2 は，経年変化による影響を確認するため，2023 年度から 2024 年度にかけて，有価証券報告書の「事業等のリスク」におけるサイバーセキュリティリスクの記載有無の構成割合をまとめている．それぞれ，各年度別に脅威および脆弱性に関する記述があった企業と片方に関する記載のみの企業，そして該当する記載のなかった企業の構成割合となる．

結果として，2023 年度および 2024 年度における各セキュリティリスクの記載有無の構成割合の傾向についてみれば，それぞれ，最も多いのが「該当なし」の場合であり，次いで「脅威・脆弱性」の複数記載が多く，脆弱性の記載のみが最も少ない構成割合となっており，同じ傾向が想定される．

[*2] https://www.nist.gov/cyberframework

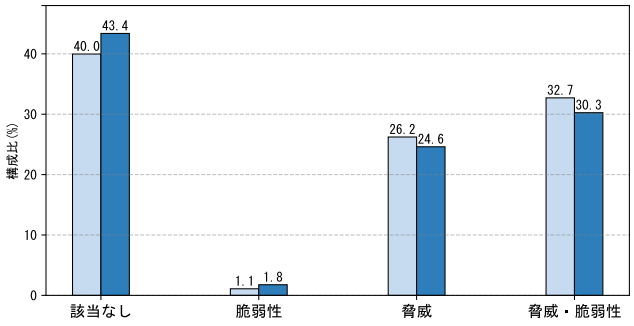

図 2　2023 年度から 2024 年度における有価証券報告書の事業等のリスクにおけるサイバーセキュリティリスクの記載状況

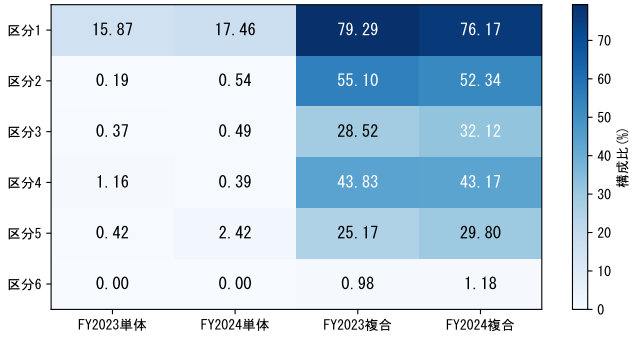

図 3　2023 年度から 2024 年度におけるサイバーセキュリティリスクの記載区分の構成割合

さらに，セキュリティリスクの記載がある場合における区分の内訳について示したのが図 3 である．ここで，セキュリティリスクの文章は，複数の区分を持つ場合があるため，各年度に対して「単体」と「複合」に分けて集計する．「単体」は単一の区分のみ抽出された場合を意味し，「複合」は文章から 2 つ以上の区分が抽出されたことを意味する．そのため，ここでの構成割合は，記載があった全体数に対する 1 区分単一年度の分類の抽出数の割合となる．

各年度の「単体」における構成割合は全体として水準が低い区分の傾向は異なるが，区分 1 の構成割合が最も高いという傾向は一致している．次に「複合」における構成割合の傾向だが，区分 1 から区分 6 までの傾向が同一であり，全体として，区分 1 および 2 の脅威に関する割合が高く，脆弱性においては区分 4 に関する内容が記載される傾向が高い．そして，全体を通して区分 6 については，あまり記載されない傾向にある．

よって，年度別の区分における内訳を確認しても，同一の傾向を持っていることからも，2023 年度と 2024 年度間における経変変化の影響は低いと言える．その上で，直近のサイバーセキュリティリスクの記載内容については，「該当なし」の企業が半数に迫る水準にあり，全体として，セキュリティリスクを記載のある企業と記載のない企業に二分していると言える．ただ，記載がある企業においても，留意が必要な点があると言える．脅威の記載がある場合，比較的脆弱性も記載する傾向だが，脅威のみを記載する企

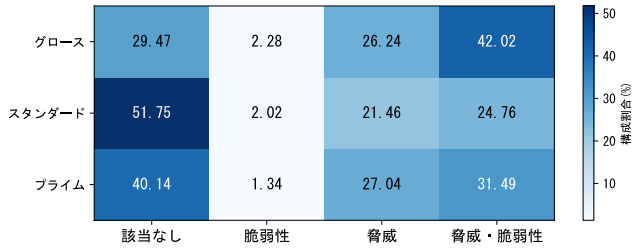

図 4 2024 年度における市場区分別のセキュリティリスクの記載状況

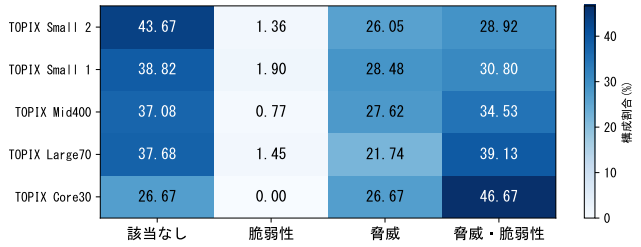

図 5 2024 年度における企業規模別のセキュリティリスクの記載状況

業も比較的多く存在する．セキュリティリスクの評価が脅威と脆弱性，資産によって決まることを考慮すると，脅威が特定できているにも関わらず，対応する脆弱性への言及がないことは，構成の不完全性が残る．確かに，脆弱性への言及を意図的に避けている場合も考えられるが，単なる担当者の理解や認知に課題がある可能性がある．

この節における調査では，セキュリティリスクの掲載有無に焦点を当て分析したが，掲載ありと掲載なしを分ける企業の意思決定の背後には，各企業が有する特徴が影響していると推察される．そこで次節では，分析の焦点を企業が持つ特徴に移し，セキュリティリスクの掲載に影響を与える共通の要因を探ることで，セキュリティリスクを掲載する企業の傾向を明らかにする．

3.4 記載内容の傾向分析

本節では，セキュリティリスクを掲載する企業の特徴を調査するため，次の 4 つの観点から傾向を分析した．以降の分析については，断りがない限り，2024 年度のデータを対象に分析した結果である．

3.4.1 市場区分および企業規模における記載傾向

東京証券取引所においては，利益基準やガバナンスの水準の違いによる，プライム，スタンダード，グロースといった市場区分や時価総額および売買代金を基にした流動性などを考慮した企業規模など，上場企業に応じた分類がある．市場区分における審査基準の違いや企業規模の大小を考慮すれば，より厳しい審査基準を持つ市場区分や規模の大きい企業については，セキュリティリスクを掲載するリテラシーと相関があると考えられる．そこで，各市場区分と企業規模について，サイバーセキュリティリスクの記載状況について調査した．

まず，市場区分別に記載方法集計した結果を表 4 に示す．この結果から，2 つの傾向が明らかとなった．まず，「該当なし」の企業が最も多かったのはスタンダード市場であり，市場全体の過半数を超えている．次に脅威および脆弱性の両方の記載がある企業が最も多かったのはグロース市場である．より審査基準の厳しい順に記載内容の傾向が現れることを踏まえれば，「該当なし」の企業が最も少なく，脅威および脆弱性の両方の記載が最も多いのがプライム市場となり，より審査基準が緩いグロース市場は逆の掲載傾向となるのが直感に合う．このギャップが示唆するのは，上場区分の形式的な基準の厳格さ以上に，各市場に属する企業の事業モデルの特性や成長ステージなど異なる特徴が，掲載の具体性や深度を左右する要因となっている可能性である．

次に，企業規模別に記載方法を集計した結果を図 5 に示す．結果は市場区分とことなり，企業規模が大きくなるにつれて，掲載なしの企業が減り，脅威および脆弱性の両方を記載する企業が多くなる傾向となった．これは，市場区分よりステークホルダーからの監視や説明責任など外部の評価に焦点があたったことがセキュリティリスクに対するリテラシーと関連した可能性がある．

3.4.2 業種における記載傾向

各企業のビジネスモデルや情報資産への依存度を考慮すれば，サイバーセキュリティリスクへの理解や認知に差異が生まれると考えることができる．そのため，事業等のリスクにサイバーセキュリティリスクが記載されるリテラシーと，業態には関係性があると考えられる．そこで，業態を反映した一つの指標として，東京証券取引所における業種分類の内，17 業種を対象に，サイバーセキュリティリスクの記載状況について調査した．

図 6 は，17 業種を対象としたサイバーセキュリティリスクの記載有無について，構成割合を示している．結果として，金融や電気・ガスなどの公共インフラといった業種については，脅威および脆弱性の両方を記載する企業が最も多い．これは，提供するサービスが国民生活に不可欠な社会基盤と密接であり，問題が発生した場合，経済や日常生活に甚大な影響を与えることが一つの要因として考えられる．また，規制が強い産業でもあることから，官公庁および業界団体の活動が活発であることも特徴としてある．一方で，医薬品や建設・資材，運輸・物流など，物理的なモノの製造や移動が事業の中核をなす業種においては，記載のない企業が比較的多い．これは，事業継続における主要なリスクが，伝統的に，サイバー空間よりも物資の不足や製造物責任，労働災害など製造過程を対象としたフィジカル空間での事象に重きを置いてきたためだと考えられる．

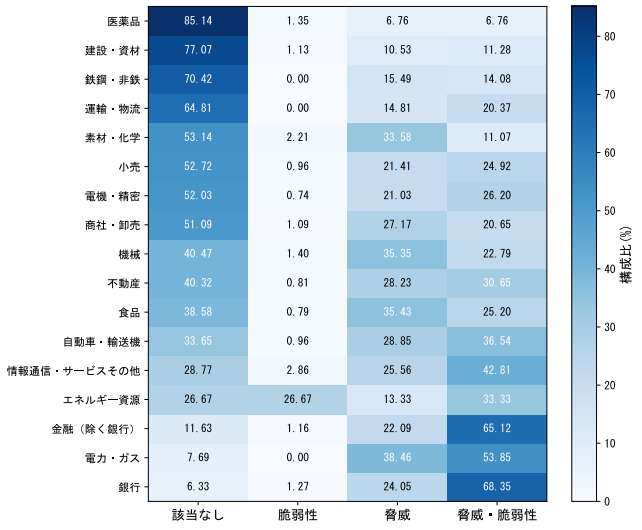

図 6　掲載状況に対する東証 17 業種の分布

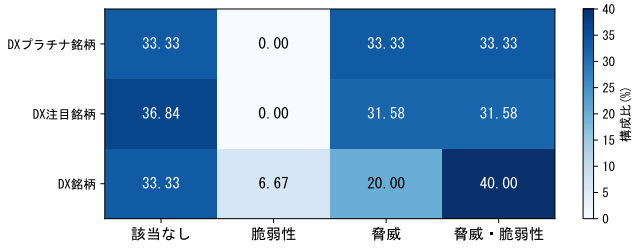

図 7　DX 銘柄 2025 のセキュリティリスクの記載状況

3.4.3　経済的連動要因における記載傾向

金融機関における運用方法の 1 つに，経済的に連動性のある要因を主体とした企業群を構成することで収益機会を獲得するアプローチがある．この内，DX や ESG などの要因については，IT 運用やリスク対策のリテラシーが高いことが想定されるため，サイバーセキュリティリスクに対する感度と関連性が高いと考えられる．そこで，DX に関連する企業群として，経済産業省が公表している DX 銘柄 2025[*3]，ESG に関連する銘柄群として，モルガン・スタンレー・キャピタル・インターナショナル (MSCI) の公表している MSCI ジャパン ESG セレクト・リーダーズ指数の構成企業[*4]を対象に，サイバーセキュリティリスクの記載状況について調査した．

まず，DX 銘柄 2025 のセキュリティリスクの記載状況を示したのが図 7 である．DX 銘柄 2025 はそれぞれ，DX 銘柄 30 企業，DX 注目銘柄 19 企業，DX プラチナ銘柄 6 企業により構成されている．結果として，DX 銘柄について，脅威および脆弱性の両方を記載する企業が比較的多い傾向にある．しかしながら，記載がない企業の構成割合と比較すると大きく水準は変わらない．選出されている企業

[*3] https://www.meti.go.jp/press/2025/04/20250411002/20250411002.html

[*4] https://www.msci.com/documents/1296102/22569066/JAPAN-ESG-SELECT-LEADERS.pdf (2025 年 6 月時点)

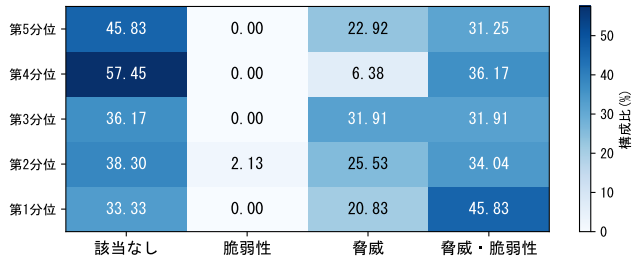

図 8　ESG 銘柄のセキュリティリスクの記載状況

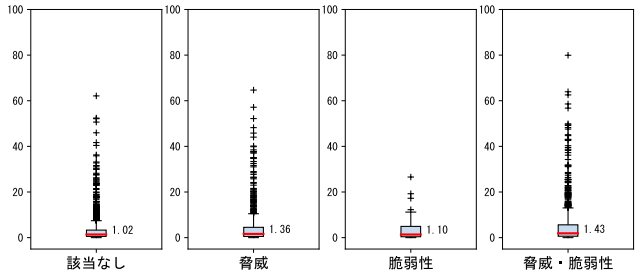

図 9　掲載状況に対する無形資産比割合別の分布

において顕著な傾向が確認できなかった．これは，デジタル技術によるビジネスモデルの変革といった成長や競争力強化など事業リスクを積極的にとる姿勢とセキュリティリスクに慎重になる姿勢が必ずしも両立するものではなく，トレードオフの関係になったことが考えらえる．

次に，ESG 構成銘柄の内，237 企業を対象に，セキュリティリスクの記載状況を示したのが図 8 である．指数算出に用いられる構成企業の重み付けをより重要度として，5 分位により分類した．1 に近づけば重みが大きく，5 が最も重みの少ない銘柄群となる．結果として，重みの順位が低ければ，記載のない企業が多くなり，順位が高い場合，脅威および脆弱性の両方を記載する企業が多い傾向が確認できた．ただし，留意が必要なのは重みが大きい企業は，一般的に時価総額も大きい大企業であり，企業規模の結果を反映している可能性もある．そのため，この傾向が ESG 評価の高さを反映したものなのか，単に企業規模の大きさによるものなのかを切り分けるための分析が必要となる．

3.4.4　財務における記載傾向

企業に対する財務に焦点を当てれば，無形資産として計上される事業に関連する情報資産の割合が高ければ，無形資産とセキュリティリスクとの関係性について調査した報告 [4] があることからも，事業リスクとして，サイバーセキュリティリスクを記載する傾向があると考えられる．そこで，資産に対する無形資産の割合を対象に，サイバーセキュリティリスクの記載状況について調査した．

図 9 は，記載有無に対する無形資産の割合の分布状況を示している．Box は四分位における第一分位から第三分位までの示しており，Box 内の赤線が中央値を示している．結果から言えるのは，掲載の有無によって，無形資産の割

合を四部位に分けた際に分布が集中する位置に違いはなく，同じ傾向にあるとわかる．これは，税制的な側面により，無形資産という会計上の分類に，サイバーセキュリティリスクの直接的な対象となる資産が計上されてない場合や，無形資産が事業におけるサイバー空間やデジタルへの依存度を必ずしも反映していないことが考えられる．

4. 考察

本章では，分析によって得られた結果が示す意味と，分析したテキストの性質に焦点を当て考える．

4.1 認知における潜在的なメカニズム

本研究では、セキュリティリスクの記載有無が生じるメカニズムを探るため，市場区分および企業規模，業種，経済的連動要因，財務の 4 つの視点から特徴を分析した．市場区分と企業規模の分析において，新興企業が集中するグロース市場ではセキュリティリスクの記載が充実している一方，中間的なスタンダード市場の企業では記載が減少し，さらに企業規模が大きくなると再び記載が充実するという，一見すれば企業の成熟度に併せ記載が充実するという直観に反した傾向が確認された．

この結果は，企業の成長プロセスにおける「リスク認知能力の限界」という観点から解釈することで，整合的な説明が可能である．具体的には，グロース市場の企業は，事業を支える人材は少ないものの，管理対象となる情報資産も限定的であるため，両者のバランスが取れており，リスクを網羅的に認知・評価できる状態にある．しかしながら，事業規模が拡大し成長の中間段階へ移行する段階において，情報資産の量と複雑性が増大し，企業としてのリスク認知能力の限界を超える．そのため，管理体制の整備が後手に回り，把握できないリスクが増加すれば，記載内容が手薄となり，結果として谷間が生じる．より企業規模が大きくなり，成熟期を迎えた企業においては，専門部署の設置やリスク管理プロセスの高度化といった組織的な成長を通じて，この谷間を克服していると考えられる．これにより，増大・複雑化した情報資産に対してもリスク認知能力が追いつき，再び質の高い情報開示が可能になったものと推察される．

さらに，この「リスク認知能力の限界」に影響を及ぼすのが業種である．業種別の分析により，金融や公共インフラなど規制が強く監視の目が強い業種においては記載が充実しており，モノの製造や移転が中心となる医薬品や建設・資材，運輸・物流などの業種においては記載がないことが確認できた．これは，業種特有の規制環境と事業モデルが，企業のリスク認知能力の限界を克服しようとするインセンティブの強弱を決定しているためだと考えられる．金融や公共インフラといった業種では，監督官庁による厳しい規制や社会からの高い要求水準といった外部からの強い圧力が存在する．これらの圧力は，企業に対してリスク管理体制の高度化を強制する強力な動機付けとなる．また，事業そのものが情報資産に大きく依存することで，セキュリティリスクは事業継続を揺るがす本質的な脅威として認知されやすくなり，経営陣が認知能力の限界を押し上げるための投資を積極的に行うことで，結果として記載が充実する傾向にある．一方で，事業の中心がモノの管理にあり，セキュリティリスクは IT 部門が管轄する副次的な問題と捉えられがちな業種においては，当該業種に特化したサイバーセキュリティ開示に関する強い規制が少ない場合，リスク認知の谷間を克服するための切迫感が生まれにくいと考える．その結果，リスク管理体制の構築が後回しにされ，開示が手薄な状態が継続すると推察される．つまり、業種という変数は，企業がリスク認知における谷間を乗り越えるスピードやその谷の深さを左右する決定的な要因として機能していることが示唆される．

このメカニズムをより調査するには，企業における社外取締役などの専門人材の配置状況や CISO（最高情報セキュリティ責任者）の設置有無といった具体的なガバナンス体制を分析することが考えられる．

留意点としては，「認知しているが開示できない」段階と「認知そのものが不足している」段階を区別する必要はある．これは，セキュリティリスクを記載することが自社の脆弱性を内外に示すことにも繋がりかねず，トレードオフとなりうるため，ジレンマを内包している．有効な対策を講じている企業であっても，防衛上の観点からあえて詳細な記述を避ける可能性がある．本研究の分析では，このような「戦略的非開示」と、単なる「認知の不足による非開示」とを区別できていない点が今後の課題となる．

4.2 形骸化の検知

本研究においては，直近の傾向を確認するため，2023 年度から 2024 年度の連続した期間における経年変化について調査した．分析結果として，掲載有無の構成割合における順位に違いがなかったことから，2024 年度が特異な年ではないという前提とした．ここで，経年変化の影響がない点について，対象としたテキストの性質に焦点を考える．

図 10 は，2023 年度と 2024 年度における事業等のリスクの原文について，文字列により正規化したレーベンシュタイン距離に基づく類似度と 2024 年度の原文における文字数の関係を示している．類似度が 0.9 以上はほぼ原文に近いことを意味し，該当する企業は全体の 9 割におよぶことがわかる．ここで，各年同月の情勢を測るため，日本銀行の公表している経済や物価見通しに関する展望レポート[*5]を確認したが，マクロ環境については異なる言及が見られることから，事業において考慮すべきリスクは異なっ

[*5] https://www.boj.or.jp/mopo/outlook/index.htm

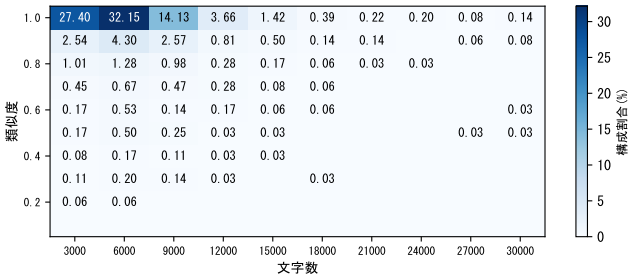

図 10 2023 年度と 2024 年度における有価証券報告書原文の類似度

ていたと言える．確かに，事業等のリスクに対する戦略が頻繁に変わっては長期的な対応を実施できないともいえるが，重要な懸念として，記載内容の形骸化が考えられる．つまり，記載があるだけで認知していると判断するだけでなく，記載内容が形骸化していないか評価する仕組みを導入する必要があると言える．

5. まとめ

本研究では，企業の持続性を危うくするサイバーセキュリティリスクについて，企業がどのように認知しているか有価証券報告書を通じ，LLM による抽出と分類のパイプラインを設計し，分析した．特に，サイバーセキュリティリスクの記述を「脅威」と「脆弱性」の二つの主要なカテゴリーに分類し，LLM を用いてその記載傾向を調査した．最終的な結論として，サイバーセキュリティリスクの記載については，半数近くの企業において，「該当なし」と，リスク認知が十分でない現状が明らかとなった．また，記載のある企業におても，「脅威」についてのみ言及があり，「脆弱性」への言及が不足している場合が多く，これはリスク認知や理解に課題がある可能性を示唆している．更に，記載の有無における企業の特性を調査した結果では，企業規模が大きいほど記載が包括的であり，特に金融や公共インフラなど社会基盤に関わる業種においては，リスク認知が高い一方で，物理的な事業が中心の業種では低い傾向が確認できた．一方で，DX 銘柄や ESG 銘柄などの経済的な連動要因記との関係については，企業規模の影響を検討する必要があり，無形資産の割合については，直接的な関連性を確認することができず，財務特性などには異なるアプローチが必要だとわかった．そして，これらの結果から，企業の成長プロセスにおける「リスク認知能力の限界」と形骸化による評価の必要性について言及した．本研究の結果は，公開資料から企業のサイバーセキュリティリスク対する認知を評価するアプローチの実現可能性を示し，サイバーセキュリティリスクに関係するステークホルダーや専門家が企業の持続性を評価する上で貢献する．

参考文献

[1] Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A. et al.: Language models are few-shot learners, *Advances in neural information processing systems*, Vol. 33, pp. 1877–1901 (2020).

[2] De Smidt, G. and Botzen, W.: Perceptions of corporate cyber risks and insurance decision-making, *The Geneva Papers on Risk and Insurance-Issues and Practice*, Vol. 43, No. 2, pp. 239–274 (2018).

[3] Edwards, B., Jacobs, J. and Forrest, S.: Risky business: Assessing security with external measurements, *arXiv preprint arXiv:1904.11052* (2019).

[4] FRUMENTO, E. and DAMBRA, C.: The role of intangible assets in the modern cyber threat landscape: the HERMENEUT Project, *The role of intangible assets in the modern cyber threat landscape: the hermeneut project*, Vol. 5, No. 2019, p. 02 (2019).

[5] Grattafiori, A., Dubey, A., Jauhri, A., Pandey, A., Kadian, A., Al-Dahle, A., Letman, A., Mathur, A., Schelten, A., Vaughan, A. et al.: The llama 3 herd of models, *arXiv preprint arXiv:2407.21783* (2024).

[6] Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L. and Pospelova, V.: The emerging threat of ai-driven cyber attacks: A review, *Applied Artificial Intelligence*, Vol. 36, No. 1, p. 2037254 (2022).

[7] Jang-Jaccard, J. and Nepal, S.: A survey of emerging threats in cybersecurity, *Journal of computer and system sciences*, Vol. 80, No. 5, pp. 973–993 (2014).

[8] Kaplan, J., McCandlish, S., Henighan, T., Brown, T. B., Chess, B., Child, R., Gray, S., Radford, A., Wu, J. and Amodei, D.: Scaling laws for neural language models, *arXiv preprint arXiv:2001.08361* (2020).

[9] Levy, M., Jacoby, A. and Goldberg, Y.: Same task, more tokens: the impact of input length on the reasoning performance of large language models, *arXiv preprint arXiv:2402.14848* (2024).

[10] Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., Küttler, H., Lewis, M., Yih, W.-t., Rocktäschel, T. et al.: Retrieval-augmented generation for knowledge-intensive nlp tasks, *Advances in neural information processing systems*, Vol. 33, pp. 9459–9474 (2020).

[11] Liu, C. and Babar, M. A.: Corporate cybersecurity risk and data breaches: A systematic review of empirical research, *Australian Journal of Management*, p. 03128962241293658 (2024).

[12] Ouyang, L., Wu, J., Jiang, X., Almeida, D., Wainwright, C., Mishkin, P., Zhang, C., Agarwal, S., Slama, K., Ray, A. et al.: Training language models to follow instructions with human feedback, *Advances in neural information processing systems*, Vol. 35, pp. 27730–27744 (2022).

[13] Vasiu, I. and Vasiu, L.: Cybersecurity as an essential sustainable economic development factor, *European Journal of Sustainable Development*, Vol. 7, No. 4, pp. 171–171 (2018).

[14] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł. and Polosukhin, I.: Attention is all you need, *Advances in neural information processing systems*, Vol. 30 (2017).

[15] Von der Assen, J., Huertas, A., Sharif, J., Feng, C., Bovet, G. and Stiller, B.: ThreatFinderAI: Automated Threat Modeling Applied to LLM System Integration, *2024 20th International Conference on Network and Service Management (CNSM)*, IEEE, pp. 1–3 (2024).

[16] Wilson, M., McDonald, S., Button, D. and McGarry, K.: It won't happen to me: surveying SME attitudes to cyber-security, *Journal of Computer Information Systems*, Vol. 63, No. 2, pp. 397–409 (2023).

[17] Xu, H., Wang, S., Li, N., Wang, K., Zhao, Y., Chen, K., Yu, T., Liu, Y. and Wang, H.: Large language models for cyber security: A systematic literature review, *arXiv preprint arXiv:2405.04760* (2024).

[18] Zhao, W. X., Zhou, K., Li, J., Tang, T., Wang, X., Hou, Y., Min, Y., Zhang, B., Zhang, J., Dong, Z. et al.: A survey of large language models, *arXiv preprint arXiv:2303.18223*, Vol. 1, No. 2 (2023).