サイバーセキュリティ、AI倫理

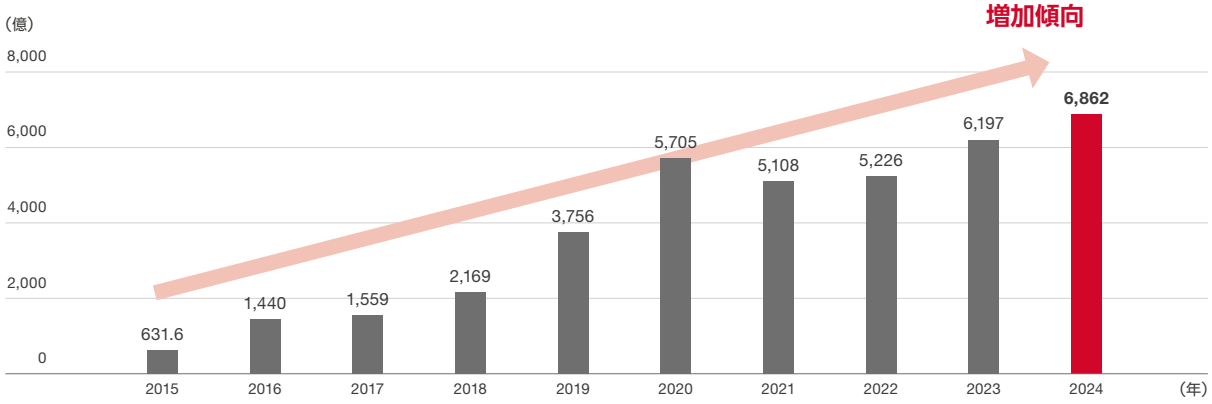
情報セキュリティを中心としたデジタル関連のリスク管理の重要性は増しています。例えば過去に発生した事例として、大手出版社、大手飲料メーカーのサーバーへの攻撃では被害が情報漏洩にとどまらず、顧客向け販売システムの停止から長期の出荷停止や制限を余儀なくされるなど、財務への影響が大きくなるケースも出ています。

世界経済フォーラムの「グローバルリスク報告書2025」においてもグローバルリスクの重要度ランキングには短期（今後2年以内）、長期（今後10年以内）のリスクとしてサイバーセキュリティに関連したリスクが上位に入ってきております。

経営層においてもリスク認識は浸透していると考えられますが、脅威はさらに高まっています。情報処理推進機構がまとめた組織に対する情報セキュリティの脅威上位10位（2025年版）にはこれまで継続的にランクインしている1位のランサムウェアによる攻撃、2位にはサプライチェーンや委託先を狙った攻撃に加えて、地政学的リスクに起因するサイバー攻撃が新たにランクインするなど脅威は多様化しています。

近年、マルウェアなどのサイバー攻撃は増加傾向にあり、国立研究開発法人情報通信研究機構（NICT）の調査によると2024年のサイバー攻撃関連として観測された年間総観測パケット数は6,862億パケットと過去10年で約10倍に増加しています。

年間総観測パケット数※の推移



（出所）国立研究開発法人情報通信研究機構「NICTER観測レポート2024」より作成
※NICTERプロジェクト（https://www.nicter.jp/project）で観測されたサイバー攻撃に関連する総パケット数

実際の被害は直接的な被害、復旧コストに加えて、業務への影響も無視できない規模になりつつあります。復旧に時間を要する場合には、競合他社による製品・サービスの代替が行われ、市場シェアの低下が起こり、業績への影響は長引くことも想定されます。

投資家にとっても業績の悪化は株価の下落、信用力の低下として影響を受けます。セクターによる重要度も考慮する必要があります。サイバー攻撃により社会的な影響が大きい航空、陸運やロジスティクスなどの業界、電力、通信などの社会インフラを支える業界、銀行などの金融機関は特にサイバーセキュリティの重要性が高いと考えらます。また、直接消費者とインターネット上でやり取りするイー・コマースについても相対的に重要性が高いと言えるでしょう。また、サイバー攻撃者にとって、金銭的に価値があるまたは地政学的に重要である場合ターゲットとなる可能性があります。

投資家として、サイバーセキュリティに関する専門知識を持ち、分析することは困難です。アプローチとしては、外部からの情報に加えて、特に重要なセクターについては、業界内の比較によりその企業にとって不足していることを発見していくことが可能です。例えば、以下に述べるような情報セキュリティに対する方針や体制整備の状況などのガバナンス、そして、セキュリティ監視の運用状況などです。その結果、改善が必要と判断される場合には、会社とエンゲージメントを行います。多くの企業では対策を行っていますが、開示が不十分な場合もあります。投資家にとって必要な開示を促していくことも重要です。

World Benchmarking Alliance が行っている Digital Inclusion Benchmark では、包摂的なデジタル経済・社会に向けた企業等の取り組みをデジタル技術へのアクセス、デジタルスキル、デジタル技術の使用、およびイノベーションの4つの観点で評価しています。その中でも企業の情報セキュリティガバナンスに関する要素として、方針や体制の整備、インシデント対応、ISO27001の取得等が挙げられています。

当社としても、経営トップのコミットメントを示す方針の策定と開示、平時の体制、すなわち責任者の特定と体制整備のためのCISO（Chief Information Security Officer：最高情報セキュリティ責任者）や専門委員会の設置、そして有事の体制であるCSIRT（Computer Security Incident Response Team）の設置、の大きく3つの要素を特に重要視しています。

当社の調べ（2025年9月時点）によると、TOPIX100構成企業における方針、平時体制、有事体制の整備状況は下記の表に示すように1年前比では進んでいると言えますが、比較的大きな課題となっているのは責任者の特定や委員会の設置といった平時の体制整備と考えています。特にCISOを設置していない企業はまだ多く、人材不足も要因の一つと考えられます。そのような中で責任者のみならず担当者の人材育成も課題と言えるでしょう。加えて、グローバルに広がるサプライチェーンに対する取り組みも課題となるでしょう。特に海外拠点における取引先などはサイバーセキュリティの脆弱性が懸念されます。サプライチェーンについてもサイバーセキュリティリスクを評価し、リスクをモニタリングしていくことが期待されます。

TOPIX100構成企業の情報セキュリティの対応状況

		方　針	CISO	委員会	CSIRT	全てを整備
TOPIX100全体（前回2024年12月）	整備済社数	70	64	49	80	41
TOPIX100全体（今回2025年9月）	整備済社数	77	70	59	85	63
差異（前回→今回）		**7**	**6**	**10**	**5**	**22**

（出所）会社公表資料、ホームページなどから野村アセットマネジメント作成

次にAIの利用についてのリスクについて見ると、技術的なリスク、社会的リスク（既存のリスクが高まる）、情報セキュリティに関することから誤情報、倫理的なものまで、幅広く存在します。

企業における利活用の状況を見ると言語系生成AIの利用が社内の生産性向上に向けて進んでいます。企業の大きな懸念としては、情報の外部流出が挙げられますが、責任あるAIガバナンスの利活用のためのAIガバナンスの構築が求められています。総務省、経産省が示す「AI事業者向けガイドライン」では、法令順守に加えて、人権、多様性、持続可能な公平公正な社会を尊重し、PDCAを回していくことが求められています。

海外での規制動向としては、欧州における法制化の動きもありますが、規制に反対する動きもあり、状況は流動的です。

一方、前出のWorld Benchmarking Allianceでは外部から確認する方法として、独自の倫理的AI原則が公開されているか、およびその運用について評価項目として提案しています。

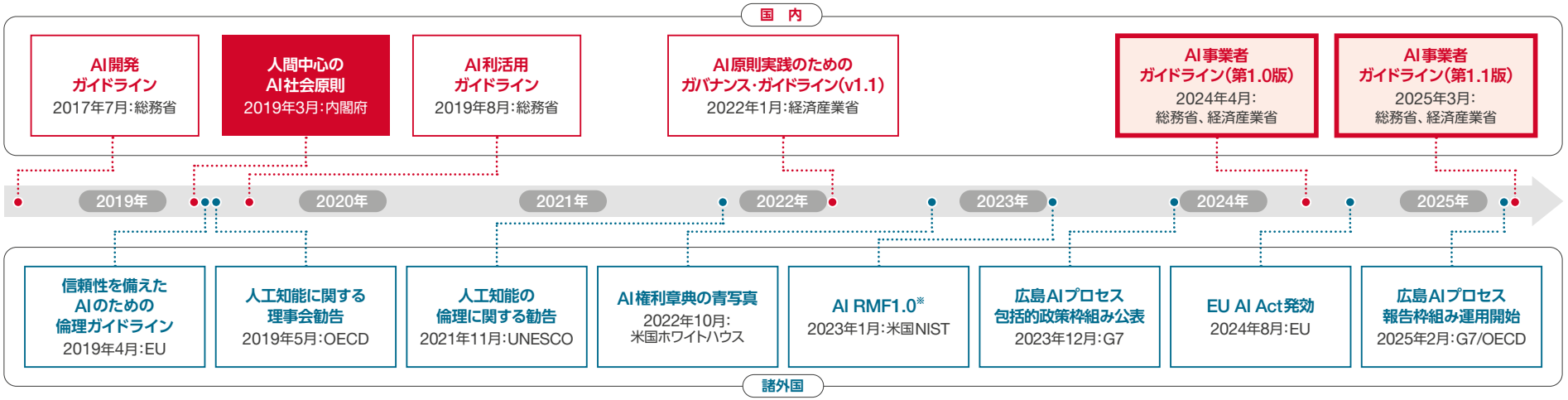
具体的には、外部から検証可能な倫理委員会、AIガイドラインの制定が挙げられます。

当社としては、課題のある会社については、対話によって対応を促していく考えです。対話にあたって、情報セキュリティに関しては前述の3つの要素点、それに加えて取り組みの範囲が海外やグループ企業、加えてサプライチェーンにまで及んでいるのかが論点と考えています。また、取引の要件として取引先にも情報セキュリティ対策を求めるというケースもあり、ビジネス面でも影響も出てくる可能性があると考えられます。

会社による開示について、取り組みが遅れている会社もある一方で、専用ページで網羅的な説明を行う、情報セキュリティに特化した年次報告書の発行をしているなどの好事例も見られます。

AI倫理やガバナンスについては、各社の取り組みはまだ始まったばかりですが、情報通信業を中心に専用ページで詳細な説明を行っている企業もあり、注目されます。今後の取り組みを後押ししてまいります。

AIの利用に関するガイドライン、規制の動向



※AI Risk Management Framework 1.0

（出所）総務省・経済産業省AI事業者ガイドライン（1.1版）概要より　https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_2.pdf

エンゲージメントの事例 日本株式

テーマ **デジタル社会のリスク管理**

野村アセットマネジメント

日本の電気機器企業

背景 近年、サイバー攻撃による企業価値への影響が懸念されています。当該企業は、顧客個人情報を含めた膨大なデータを保有・活用してビジネスを拡大しており、サイバーセキュリティ対策とその開示が重要であると考え、エンゲージメント活動を開始しました。

エンゲージメント

当該企業にサイバーセキュリティ対策の状況を確認したところ、最高デジタル責任者(CDO)や最高情報セキュリティ責任者(CISO)などの責任者を配置し、各事業部門に責任者(EISO)を任命していることなどが報告されました。ただし、これらの先進的な取り組みの説明は、現時点ではサステナビリティ・レポートに限られているため、今後の統合レポートや各種会議での開示の充実を要請しました。

会社の反応

指摘の重要性は理解。頂いた意見は統合報告書を含め、今後の情報発信の方法について参考にしたいと考えている。

結果 **従来サステナビリティレポートのみに記載されていた「サイバーセキュリティに関する取り組み・ガバナンス」が2025年より統合報告書にも記載されるようになりました。**

エンゲージメントの事例 日本株式

テーマ **デジタル社会のリスク管理**

野村アセットマネジメント

日本のサービス企業

背景 当該企業にとってデータセキュリティの重要性は高く、M&Aも広く行っているため、グループ全体での情報セキュリティの取組み強化や情報開示が必要と考え、エンゲージメント活動を開始しました。

エンゲージメント

当該企業にとって、データセキュリティの重要性は高く、M&Aも広く行っているため、グループ全体での情報セキュリティの取組み強化、具体的には責任者の設置と開示の充実を要請しました。また、当該企業はM&Aに積極的でグループ子会社も多く、情報セキュリティ体制はグループ全体を包括したものであるべきと伝達しました。

会社の反応

現在の対象は単体に留まる。ビジネスモデル上、重要な課題と認識しているので、早急に対応したい。

結果 **2025年1月に7つの基本方針を挙げ、その1つとして、情報セキュリティ基本方針を設定しました。また、2025年10月に投資家向けレポートが作成され、情報セキュリティについて記載されました。**