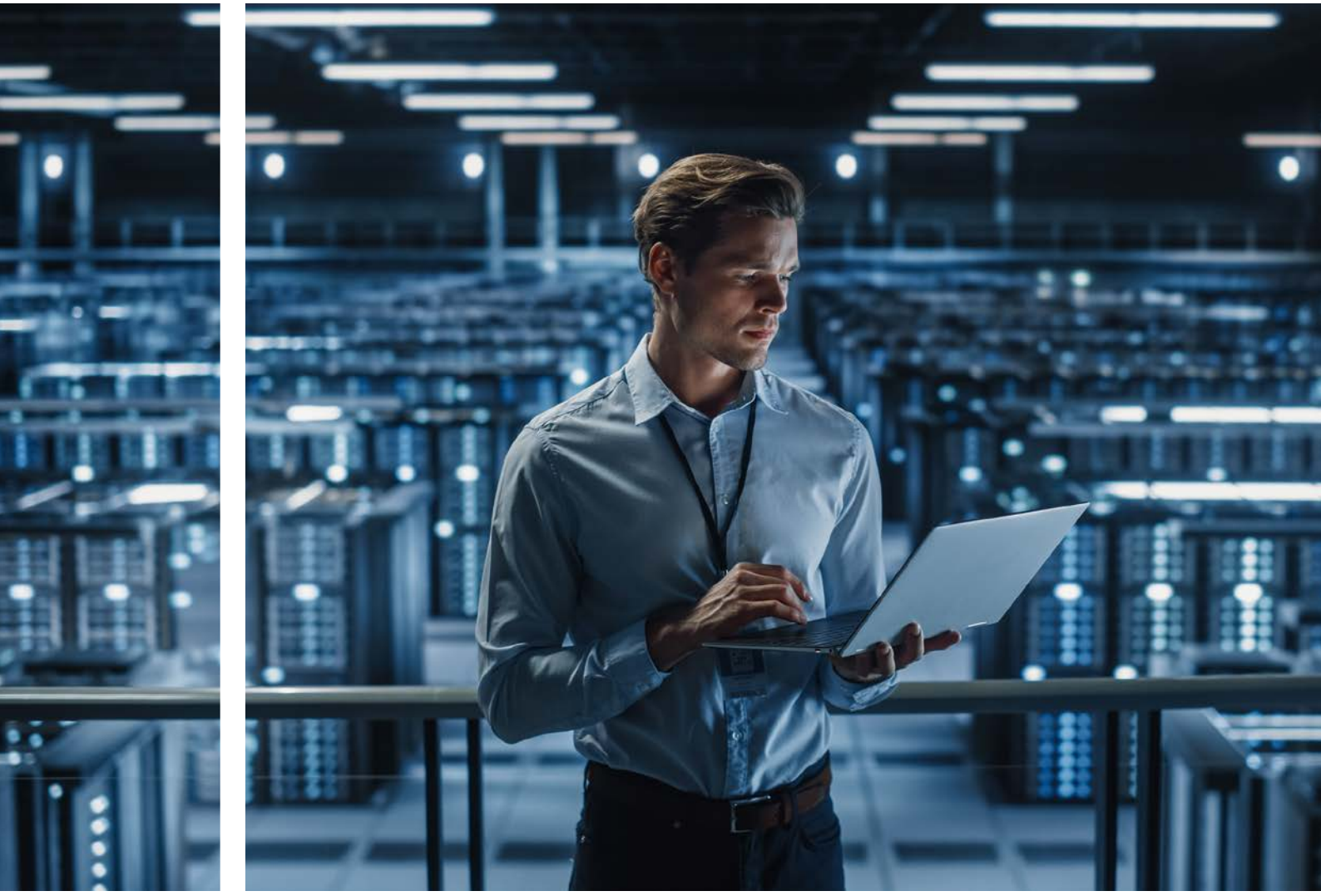
「サイバーセキュリティおよびプライバシー情報開示」に関する日米投資家の意識調査2024

――米国投資家の9割が「サイバーセキュリティ情報開示」を投資判断の1つとして捉え、「取締役会の関与状況」を最も注視



pwc

www.pwc.com/jp

目次

はじめに

現代のビジネスにおいて「サイバーセキュリティ」は重要課題です。とりわけサイバーインシデントは、企業の業績、信用、評判にマイナスの影響を及ぼすだけでなく、投資家にも損失をもたらします。このため、世界の投資家や格付け機関において、企業のセキュリティリスク評価への関心[1]が急速に高まっており、近年、各国政府機関においても投資家との対話機会創出のため、サイバーセキュリティやプライバシーに関する情報開示の規制やガイドラインを強化する傾向にあります。

米国においても、米国証券取引委員会（SEC）が2023年7月に公開した新たなサイバーセキュリティ開示規則[2]が同年12月より順次適用[3]されています。本規則では、投資家にとって「重要」と判断されるサイバーインシデントなどを適時開示することを、SEC登録企業に義務付けています。このような背景からPwC Japanグループにおいても、サイバーセキュリティに関して、国内外投資家に対しどのような情報開示を行うべきか、ご相談いただくことが多くなりました。そこでPwCコンサルティング合同会社では、社会課題への先駆的な取り組みとして「サイバーセキュリティおよびプライバシー情報開示に関する日米投資家の意識・着目点」を明らかにすることを目的に、2023年10月に日米投資家を対象としたアンケート調査を実施し、米国投資家203名および日本投資家141名、計344名[4]から回答[5]を得ました。本レポートでは、「サイバーセキュリティ情報開示における日米投資家の『12の傾向』」を紹介します。

本レポートが皆様にとって「サイバーセキュリティに関する情報開示の在り方」を見直す際の参考となることに加え、企業のセキュリティの取り組みが日米投資家に「正しく、ポジティブに評価される」ことを心より願っております。

---

1 PwC「グローバル投資家意識調査2023」 https://www.pwc.com/jp/ja/knowledge/thoughtleadership/global-investor-survey.html
PwC「グローバル投資家意識調査2022」 https://www.pwc.com/jp/ja/knowledge/thoughtleadership/investor-survey.html
PwC「グローバル投資家意識調査2018」 https://www.pwc.com/jp/ja/press-room/investor-survey180327.html

2 Securities and exchange commission,“Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure”（2023/6/26）

3 重要性のあるインシデントの開示要件は、2023年12月18日より発効され（小規模報告企業にはさらに180日間の猶予）、リスク管理、戦略およびガバナンスに関する開示については、2023年12月15日以後に終了する事業年度より全ての登録企業に適用されています。

4 本調査では、米国および日本において「①機関投資家として、仕事で株式を運用する者」「②機関投資家でアナリストとして企業のセキュリティ関連情報を分析・評価する者」を調査対象としています。本レポートでは、それぞれの国において①②のグループでは有意な差が見られなかったため、1つのグループ「機関投資家」として分析結果をまとめています。

5 一部、有識者6名へのインタビュー調査も含みます。

1 米国証券取引委員会（SEC）における サイバーセキュリティ情報開示の動向

SECは、2011年よりサイバーセキュリティ情報開示に関するガイダンスを強化しており、2017年のジェイ・クレイトン委員長の「サイバーセキュリティ声明[6]」を皮切りに2018年、2022年、2023年と投資家に対するSEC登録企業へのサイバーセキュリティ情報開示における規則を改訂してきました（図表1）。2023年7月に公開された新規則では、投資家にとって「重要」と判断されたサイバーインシデントに関する情報の適時開示をSEC登録企業に義務付けており、指定フォーマットであるForm 10-Kなどで報告できるよう改訂されています（図表2・3）。さらに、SECの過去プレスリリースを見ると、サイバーインシデントにおける情報開示が不適切と判断した企業名を公開し、最も高い事例で3,500万米ドル（約52億円）の罰金を請求していることからも、SEC登録企業にとって適切なサイバーセキュリティ情報開示が重要だと言えます（図表4）。

図表1：SECにおけるサイバーセキュリティリスクの情報開示に関するガイダンス・規則

公表時期	文書名	概要
2011年 10月13日	CF Disclosure Guidance: Topic No. 2 Cybersecurity	サイバーセキュリティリスクおよびサイバーインシデントに関する開示義務に対して、企業の財務部門の見解を示したガイダンス
2018年 2月26日	Commission Statement and Guidance on Public Company Cybersecurity Disclosures	2011年のガイダンスを基本とした、上場企業のサイバーセキュリティリスクやインシデントに関する情報開示策定におけるガイダンス
2022年 7月26日	Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure	2022年3月9日の提案に対するコメントを基に修正を加え、重大なサイバーセキュリティインシデントを開示すること、およびサイバーセキュリティのリスク管理、戦略、ガバナンスに関する重要な情報を毎年開示することを義務付ける規則
2023年 7月26日	Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure	登録会社に対し、経験した重大なサイバーセキュリティインシデントを開示すること、およびサイバーセキュリティのリスク管理、戦略、ガバナンスに関する重要な情報を毎年開示することを義務付ける規則

6 SEC,“Statement on Cybersecurity”（2017/9/20）https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20

図表2：2023年7月に公表された「Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure」の概要

	内容	対象者	報告フォーム	適用期限
主な要件	① サイバーセキュリティリスク評価と管理	米国証券登録企業（Registrants）	10-K（年次報告）	年次報告書（2023年12月15日から、あるいはこれ以降終了会計年度から適用）
		外国民間発行者（Foreign Private Issuers）	20-F（年次報告）	
	② 重要インシデント報告	米国証券登録企業（Registrants）	8-K（重要事項報告）	インシデントを確定してから4営業日以内（2023年12月18日以降適用）
		外国民間発行者（Foreign Private Issuers）	6-K（重要事項報告）	

図表3：インシデントの報告内容

	カテゴリ	報告内容
① サイバーセキュリティリスク評価と管理	サイバーセキュリティリスク管理と戦略	重大なサイバーセキュリティリスクの評価、識別、管理フロー体制の構築を投資家に分かりやすく記載 • サイバーセキュリティリスク管理をいかに企業全体のリスク管理に組み入れているか • 第三者専門家の評価を経ているか • サードパーティリスクを管理するフロー体制を構築しているか • 重大なインシデントリスクの重大な影響あるいはその可能性についてなど
	サイバーセキュリティガバナンス	• 取締役会のサイバーセキュリティリスク管理への参加状況 - サイバーセキュリティリスク管理チーム - 取締役会が報告を受けるフロー • 管理職のサイバーセキュリティリスク管理への参加状況 • サイバーセキュリティリスク管理に参与する管理職の専門知識、取締役会への報告など
② 重要インシデント報告	報告内容の詳細	被害企業への影響についての報告であり、事件そのものの詳細を報告することではない • インシデントの性質、範囲、時期、財務・業績に与える重大なまたは合理的影響 【攻撃者への情報提供となる点について】 • インシデント対応完了の有無、データ漏えいの有無、脆弱性情報などについて詳細を求めない
	報告期限	• 4営業日はインシデントの発見日ではなく、重大なインシデントであると被害企業が確認した日から計算 しかし、確認のための作業などを故意に遅延させることは違反行為となる • ベンダーなどによるインシデントの場合、特別調査は必要なく、通常のコミュニケーションで良い 【重大なインシデントの定義】 投資家目線から見た「重大なインシデント」であること
	インシデント定義	被害企業が自社に「重大な影響がある」と判断したインシデント
	適用除外	国家安全に関わるインシデントで、DOJ（米国司法省）から書面通知がある場合
	未報告の結果	米国証券法などにより訴訟提起される可能性あり

図表4：SECにおけるサイバーセキュリティリスクの情報開示規則違反に対する罰金（参考：2018年以降）

	罰金	概要
A社	約3,500万米ドル （約52億円※）	事象：個人情報漏えい 経緯：企業は、当該データ侵害の開示を怠り、投資家を誤解させたとして告発された
B社	約100万米ドル （約1.5億円※）	事象：個人情報漏えい 経緯：企業は、情報開示していたサイバーセキュリティポリシーおよび手順の不履行により本事象が発生したとして告訴された
C社	約49万米ドル （約7,200万円※）	事象：個人情報漏えい 経緯：企業は、脆弱性関連の開示管理・手順違反で、業務停止命令および違約金の支払いを命じられた
D社	個社異なる 約20万～30万米ドル （約3,000万～4,400万円※）	事象：個人情報漏えい 経緯：当該事象に関連した複数企業は、サイバーセキュリティポリシーと手順の不履行により制裁を受けた

※1米ドル＝148.117円で計算

2 サイバーセキュリティ情報開示における日米投資家の「12の傾向」

私たちは、サイバーセキュリティおよびプライバシー情報開示に関する日米投資家の意識・着目点を明らかにすることを目的に、日米機関投資家を対象としたアンケート調査を2023年10月に実施し、米国投資家およびアナリスト203名、日本投資家およびアナリスト141名、計344名から回答を得ました。

今回の調査結果より、投資先企業の「サイバーセキュリティ情報開示における日米投資家の『12の傾向』」が明らかになりました（図表5）。

図表5：サイバーセキュリティ情報開示における日米投資家の「12の傾向」

サイバーセキュリティに関する評価の重要性	1. 投資先企業の「サイバーセキュリティ情報開示」を重要視する米国投資家は8割と、日本投資家より多い 2. 米国投資家の9割が「サイバーセキュリティ情報開示」を投資判断の1つとして捉える 3. サイバーセキュリティ情報開示投資判断への採用理由は、米国投資家では「SEC情報開示義務化」がトップ
投資先企業との対話 ① 開示情報における評価の傾向	4. 米国投資家の7割がサイバーセキュリティ情報開示評価の「独自指標」を持ち、日本投資家と比較して「サイバーリスク管理体制」よりも「取締役会の関与状況」を評価する傾向にある 5. 平時よりForm 8-Kなどを情報源とする米国投資家は半数を占める 6. 「投資先のサイバーセキュリティ情報開示は十分と言えない」日本投資家は5割と多い 7. リスクの高い業界・保有期間・投資規模に応じて、投資先企業のサイバーセキュリティ情報開示の「評価の重みづけ」を変える米国投資家は9割超と多い 8. 投資規模が大きい場合「1社ずつ個別評価する」米国投資家は7割と、日本投資家（3割）より多い
投資先企業との対話 ② 質問の傾向	9. 投資先企業へサイバーセキュリティについて質問する米国投資家は9割超、うち過半数が平時・有事におけるサイバーセキュリティに特化した質問項目を準備 10. 米国投資家は「チームにセキュリティ担当者がいる」が半数を超え、日本投資家は採用中・採用検討中が4割と、評価強化が進む
投資先企業のインシデントを起因とする「損失・売却・訴訟」	11. 投資先が「サイバーインシデントやリスクを適切に開示しなかったこと」を起因とする損失経験は、日米投資家ともに7割超と多い 12. 米国投資家の「インシデント起因の売却・訴訟」経験の割合は、日本投資家より高い

サイバーセキュリティに関する評価の重要性

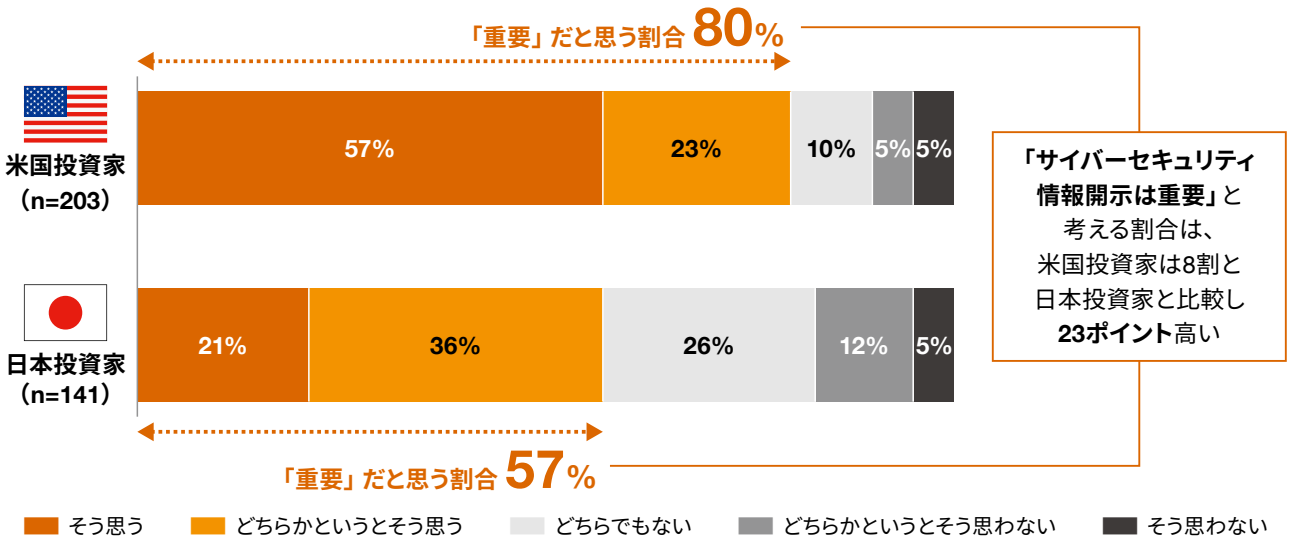
Finding 1 **投資先企業の「サイバーセキュリティ情報開示」を重要視する米国投資家は8割と、日本投資家より多い**

日米投資家344名（米国投資家203名、日本投資家141名）に「投資先企業が、サイバーセキュリティやプライバシーに関する取り組みやセキュリティ事故情報を開示することは重要だと思うか」と質問したところ、「重要だと思う」と回答した米国投資家は80%と、日本投資家の57%と比較し23ポイント高い結果となりました（図表6）。

このことから、米国投資家は日本投資家よりも投資先企業のサイバーセキュリティ関連の情報開示の重要性を認識する傾向にあることが、データとして裏付けられました。

日米有識者インタビューにおいても、サイバーセキュリティ情報開示における重要性の高まりが示されるとともに、投資家として開示情報の評価の難しさがあげられています（図表7）。

図表6：投資先企業がサイバーセキュリティ情報開示を行うことを重要と考える日米投資家の割合



Q. あなたは、投資先企業が、サイバーセキュリティやプライバシーに関する取り組みやセキュリティ事故情報を開示することが重要だと思いますか。

図表7：日米有識者インタビュー「投資先企業のサイバーセキュリティ情報開示を重要視するか」

米国機関投資家	重視する傾向があると感じる。 欧米の投資家はサイバー攻撃を数多く目撃しており、投資先企業のシステムハッキングにより在庫管理問題、財務上の損失、競合他社への影響まで引き起こしていることを懸念している。さらに生成AIの採用企業が増える中、生成AIへのリスクおよびAIを悪用した攻撃も高まると認識している。 • **規制リスク** 米国において、連邦政府レベルでは、SEC（米国証券取引委員会）が情報セキュリティと運用・回復力を規則に取り入れた。州レベルでは、最も厳格なCCPA、EUではGDPRにおいてプライバシーに関する規制が厳しくなっている。 • **格付け機関のIndex** 投資家目線では、規則への準拠は最低限であり、さらに異なる要素も求める。特にESG 投資家やサステナビリティ投資家にとって、特定の要因に基づき株を購入する際に、例えばMSCI ESG Leaders Indexes[7]への選出や、MSCI ESG Ratingsに基づき購入することもあるため、サイバーセキュリティもランクを構成する要素として重要視する。 • **海外を含む関連会社全体との適切な協力** また、関連会社のサイバーセキュリティが脆弱であれば、常に弱者をターゲットとする攻撃者の標的になる。LockBit 3.0ランサムウェアや、AIを使用した攻撃により複雑化した攻撃に対抗するため、本社だけでなく、製品ディーラー、販売店、コンサルタント、そして国と連携し対策を行うべきである。 • **日本企業の情報開示は遅れている** 日本企業は米国など海外企業と比較し、サイバーセキュリティ関連情報開示への対応、またサイバーセキュリティへの投資について後れを取っていると認識している。
日本機関投資家	SaaSやリモートワークの普及に伴い、企業においてますますリスクが高まっており、投資家の中でもサイバーセキュリティ情報開示の重要性は高まっている。企業が取らなくてはならない施策として、システム的な対策だけでなく、人材育成など幅広く対策が増えているように感じる。 • **投資機関の顧客のコンセプトに「情報セキュリティ」が採用されれば、投資機関での重要度は上がる** 投資機関は、顧客企業のコンセプトに合わせて評価する。投資機関の顧客企業のコンセプトとして「ESG」が採用されやすいが、「情報セキュリティ」をコンセプトとして希望する顧客が増えれば、投資家としても四半期ごとに説明責任が発生するから、情報セキュリティについて評価する機会が増えるだろう。
外資系格付け機関	投資家として「開示情報はあればあるほど良い」「開示は重要」というのは一般論としてあるが、以下3点の理由から、情報開示は前向きとして捉えるものの、開示情報や方法といった実現の面では非常に難しいと考えている。 • **技術的な専門知識がなければ理解できない** 例えばアニュアルレポートなどへ開示する場合、読者は機関投資家やファンドマネージャーなど証券アナリスト、一般投資家などである。すると、テクノロジーの詳細を連ねられても、専門知識がなければ理解できない内容となる恐れがある。 • **一方、分かりやすい情報は横比較できない** 逆に、分かりやすく説明しようとすると簡略化されすぎてしまい、各社似たような開示となり、横比較が難しくなる。その結果、開示情報に価値がなくなってしまう恐れがある。 • **詳細な開示情報は、攻撃者のターゲットとなり得る** また、どの製品・サービス・アプローチを採用するかなど、開示しすぎることでハッカーへヒントを提供することとなり、脆弱な箇所を推察できやすくなることが懸念点となる。

7 “MSCI ESG Leaders Indexes”, https://www.msci.com/msci-esg-leaders-indexes

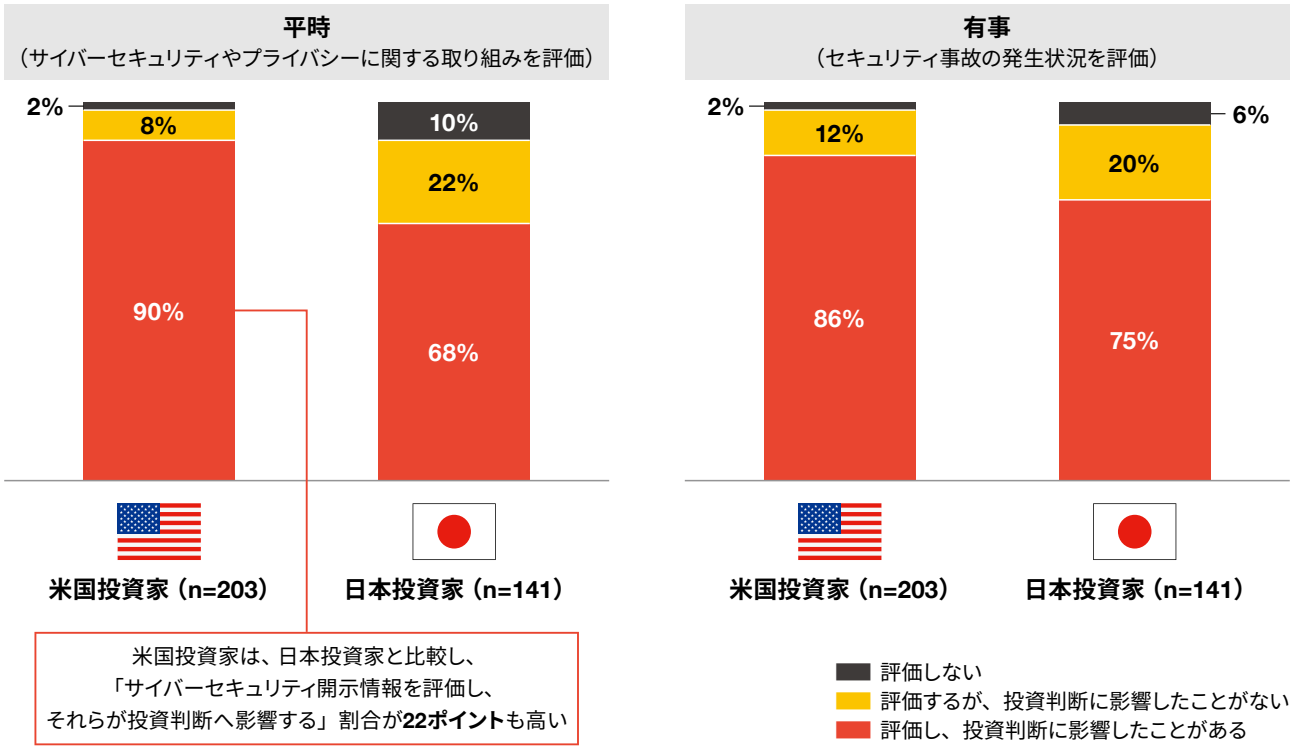
Finding 2　米国投資家の9割が「サイバーセキュリティ情報開示」を投資判断の1つとして捉える

次に「投資をする際に、投資先企業のサイバーセキュリティやプライバシーに関する取り組み（平時）やセキュリティ事故の発生状況（有事）を評価しているか、またそれらが投資判断に影響を与えたか」と質問したところ、「評価し、投資判断に影響したことがある」と回答した割合は、米国投資家では9割、日本投資家においても約7割存在することが明らかになりました（図表8）。

具体的には、米国投資家のうち「投資先企業のサイバーセキュリティやプライバシーに関する取り組み（平時）を評価する」と回答した割合は90%、「投資先企業のセキュリティ事故の発生状況（有事）を評価する」と回答した割合は86%でした。

一方、日本投資家のうち「投資先企業のサイバーセキュリティやプライバシーに関する取り組み（平時）を評価する」と回答した割合は68%、「投資先企業のセキュリティ事故の発生状況（有事）を評価する」と回答した割合は75%で、平時より有事を評価する割合がやや高くなりました。

図表8：サイバーセキュリティ関連情報開示（平時・有事）を評価し、それらが投資判断へ影響を与えた割合

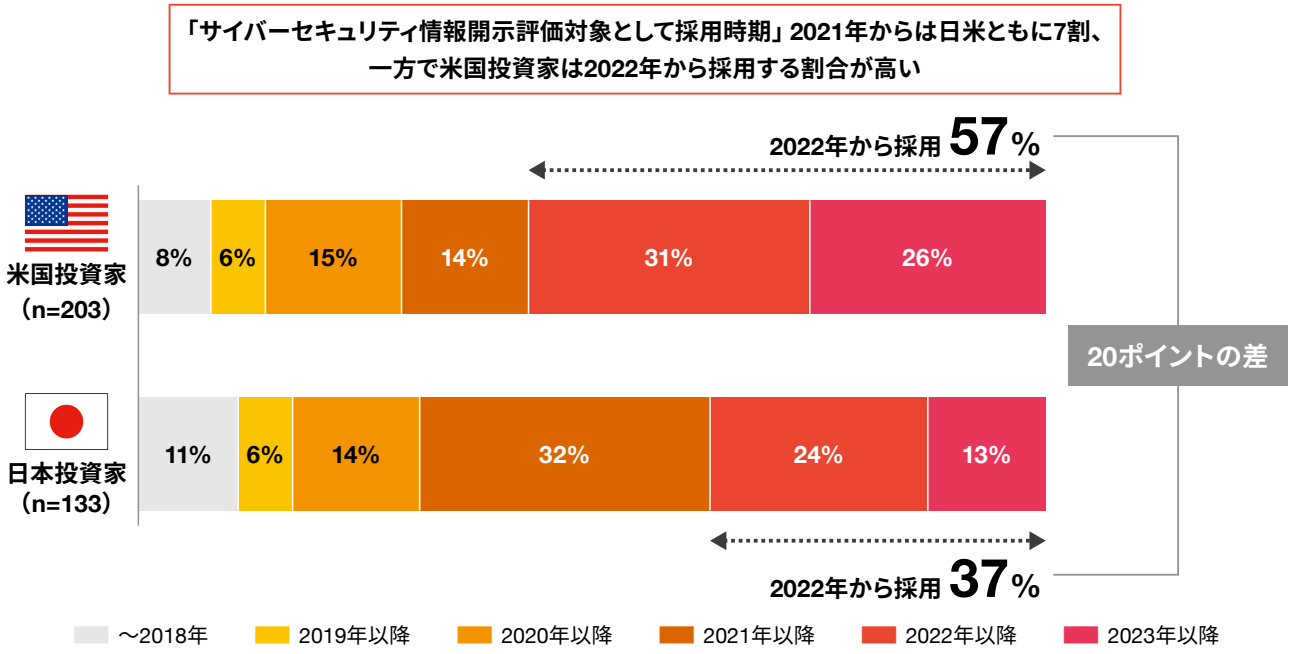


Q. あなた、またはあなたが所属する組織は、投資をする際に、投資先企業の「サイバーセキュリティやプライバシーに関する取り組みやセキュリティ事故の発生状況」を評価しますか。

2022年からサイバーセキュリティ情報開示を評価対象とした米国投資家は6割と、日本投資家より多い

また、サイバーセキュリティ情報開示（平時または有事）を投資判断として評価するとした日米投資家（336名）が、投資判断に「サイバーセキュリティ情報開示」を評価対象として採用した時期は、日米投資家ともに「2021年から採用」が7割と差は見られませんでした（図表9）。一方で、米国投資家（203名）は「2022年から採用」した割合が57%と、日本投資家（133名）の37%より20ポイント高く、比較的最近になって注目が特に高まっていると言えます。

図表9：サイバーセキュリティ情報開示（平時または有事）を投資判断として評価するとした日米投資家（n=336）が、投資判断にサイバーセキュリティ情報開示を採用した時期



Q. 前問で「評価する」と回答した方へ質問です。あなた、またはあなたが所属する組織が、投資先企業の「サイバーセキュリティまたはプライバシー」を投資判断に採用したのはいつからですか。最もあてはまるものを1つお知らせください。

Finding 3　サイバーセキュリティ情報開示投資判断への採用理由は、米国では「SEC情報開示義務化」がトップ

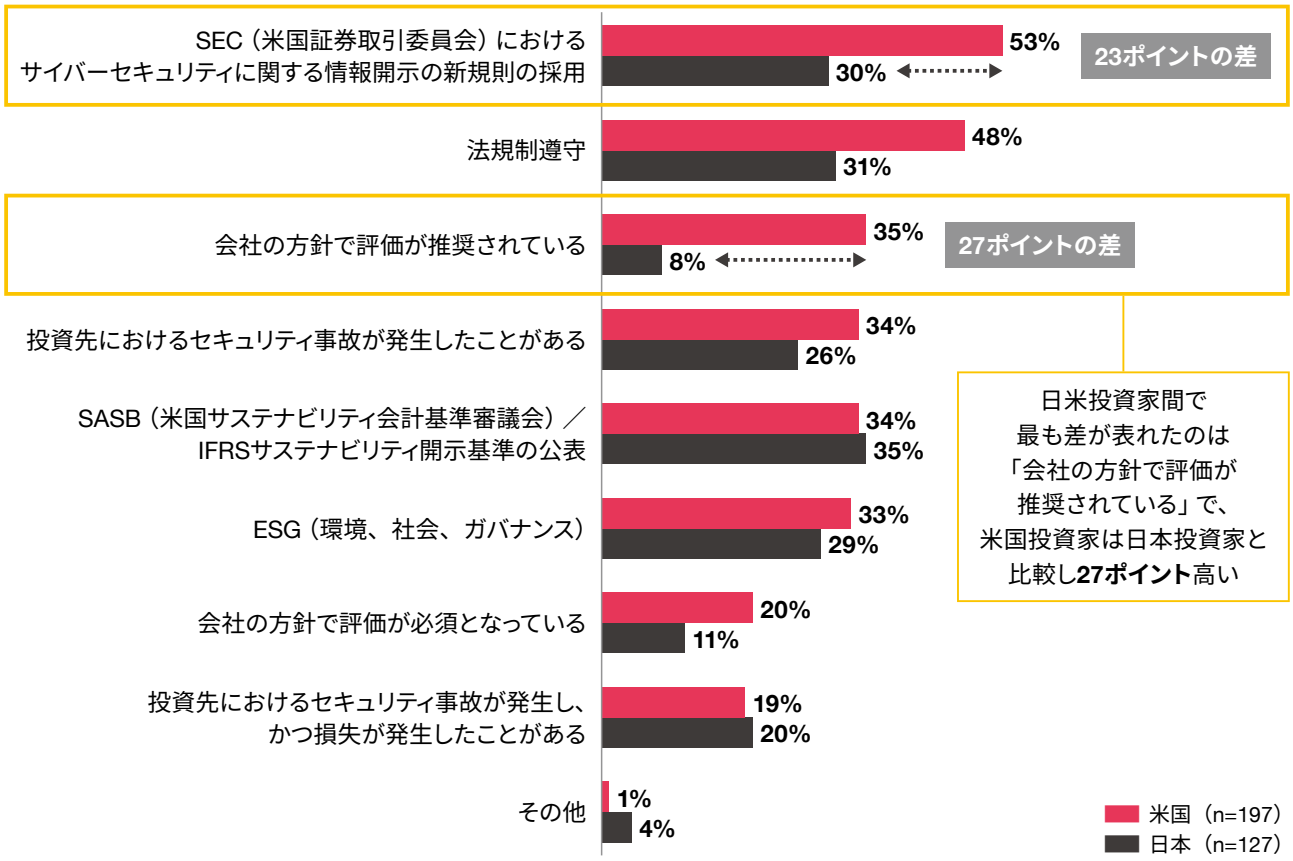
投資先企業のサイバーセキュリティ情報開示（平時）を投資判断として評価すると回答した日米投資家（324名）に「投資先企業のサイバーセキュリティおよびプライバシー関連開示情報を投資判断の1つに採用した理由」を確認したところ、米国投資家（197名）では「SEC（米国証券取引委員会）におけるサイバーセキュリティに関する情報開示の新規則の採用」が5割超と最も高く、日本投資家（127名）では「SASB（米国サステナビリティ会計基準審議会）／IFRSサステナビリティ開示基準の公表」が35%で最も高くなりました（図表10）。

具体的には、米国投資家（197名）においては、「SEC（米国証券取引委員会）におけるサイバーセキュリティに関する情報開示の新規則の採用」が最も高く53%、「法規制遵守」が48%、「会社の方針で評価が推奨されている」が35%、「投資先におけるセキュリティ事故が発生したことがある」「SASB（米国サステナビリティ会計基準審議会）／IFRSサステナビリティ開示基準の公表」がともに34%、の順に高くなりました。

次に、日本投資家（127名）においては、「SASB（米国サステナビリティ会計基準審議会）／IFRSサステナビリティ開示基準の公表」が最も高く35%、次いで「法規制遵守」が31%、「SEC（米国証券取引委員会）におけるサイバーセキュリティに関する情報開示の新規則の採用」が30%、「ESG（環境、社会、ガバナンス）」が29%、「投資先におけるセキュリティ事故が発生したことがある」が26%の順に高くなりました。

日米投資家を比較すると、特に2つの項目で差が確認できました。1つ目の項目として、「会社の方針で評価が推奨されている」を選択した割合は、米国投資家では35%と、日本投資家8%と比較して27ポイント高く、国内投資機関では企業で推奨される割合が極端に低いことが分かります。2つ目は「SEC（米国証券取引委員会）におけるサイバーセキュリティに関する情報開示の新規則の採用」の項目で、米国投資家は53%と、日本投資家30%と比較して23ポイント高くなりました。

図表10：サイバーセキュリティ情報開示（平時）投資判断への採用理由：日米投資家比較



Q. あなた、またはあなたが所属する組織が、投資先企業の「サイバーセキュリティおよびプライバシー」を投資判断の1つに採用した理由を教えてください。あてはまるものを全てお知らせください。

投資先企業との対話 ① 開示情報における評価の傾向

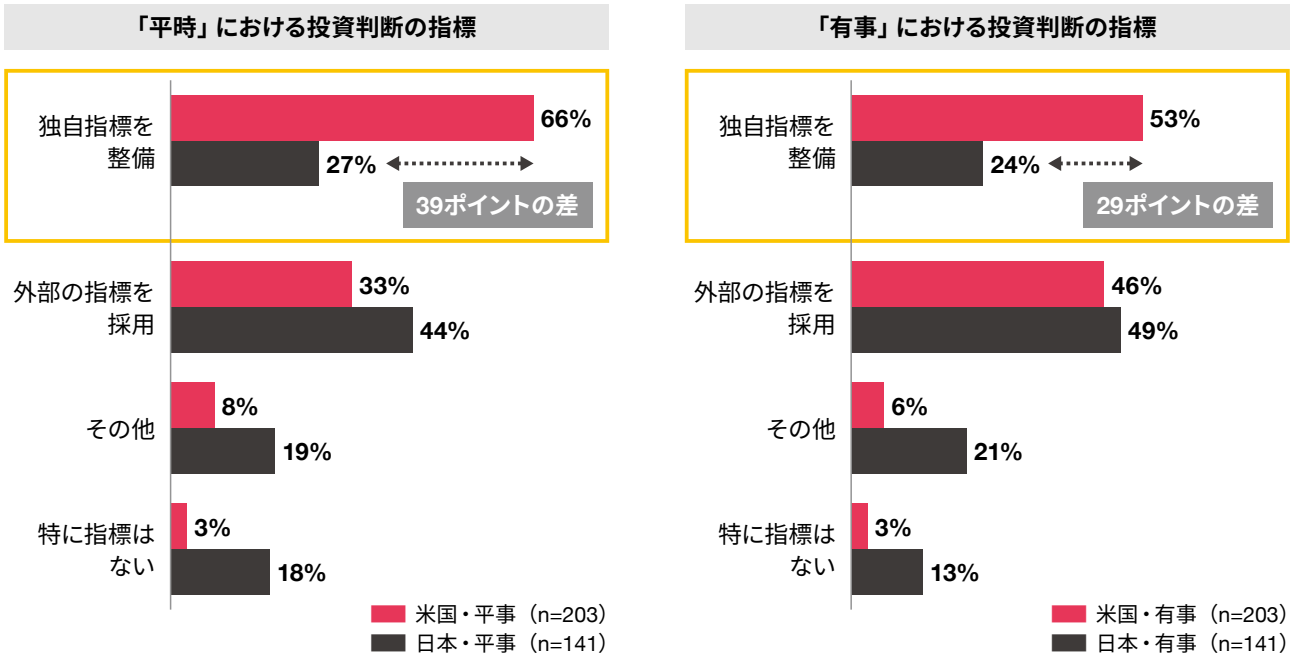
Finding 4 **米国投資家の7割がサイバーセキュリティ情報開示評価の「独自指標」を持ち、日本投資家と比較して「サイバーリスク管理体制」よりも「取締役会の関与状況」を評価する傾向にある**

サイバーセキュリティ情報開示評価の「独自指標」の有無

日米投資家に「投資先企業の『サイバーセキュリティおよびプライバシーの取り組み（平時）』評価時の指標はあるか」と確認したところ、「独自の指標がある」と回答した米国投資家の割合は66%と、日本投資家と比較し約40ポイントも高いことが明らかになりました（図表11）。

具体的に見ると、平時（図表10：左）においては、米国投資家（203名）では「独自指標を整備」が最も高く（66%）、「外部の指標を採用」が33%、「その他」8%、「特に指標はない」3%の順に高くなりました。有事（図表10：右）においても「独自指標を整備」が最も高く（53%）、「外部の指標を採用」が46%、「その他」が6%、「特に指標はない」が3%の順に高くなりました。米国投資家においては、「外部の指標を採用」するとした割合が有事は約半数（46%）と高く、平時の3割（33%）と比較し13ポイント高いことから、投資先企業でのインシデント発生時には、セキュリティ技術など専門知識を有する外部専門家の評価を採用する傾向があるのではないかと推察します。

図表11：サイバーセキュリティ情報開示（平時・有事）の評価、独自指標の有無：日米国投資家比較



独自指標における評価項目

次に、「独自指標を整備」と回答した日米投資家172名が評価するとした評価項目を見ると、平時・有事において、米国投資家は「取締役会の関与状況」を評価する割合が最も高く、日本投資家は「サイバーリスク管理体制」や「CISO設置の有無」を評価する傾向にあることが分かりました（図表12・13）。

具体的に見ると、平時における評価項目について、米国投資家（134名）では「取締役会の関与状況」が最も割合が高く（56%）、次いで「サイバーリスク管理体制」が40%、「CISO設置の有無」が39%、「セキュリティ方針・戦略の有無」が30%、「ISMSなどセキュリティ認証[8]の取得状況」が27%の順に高くなりました（図表12）。

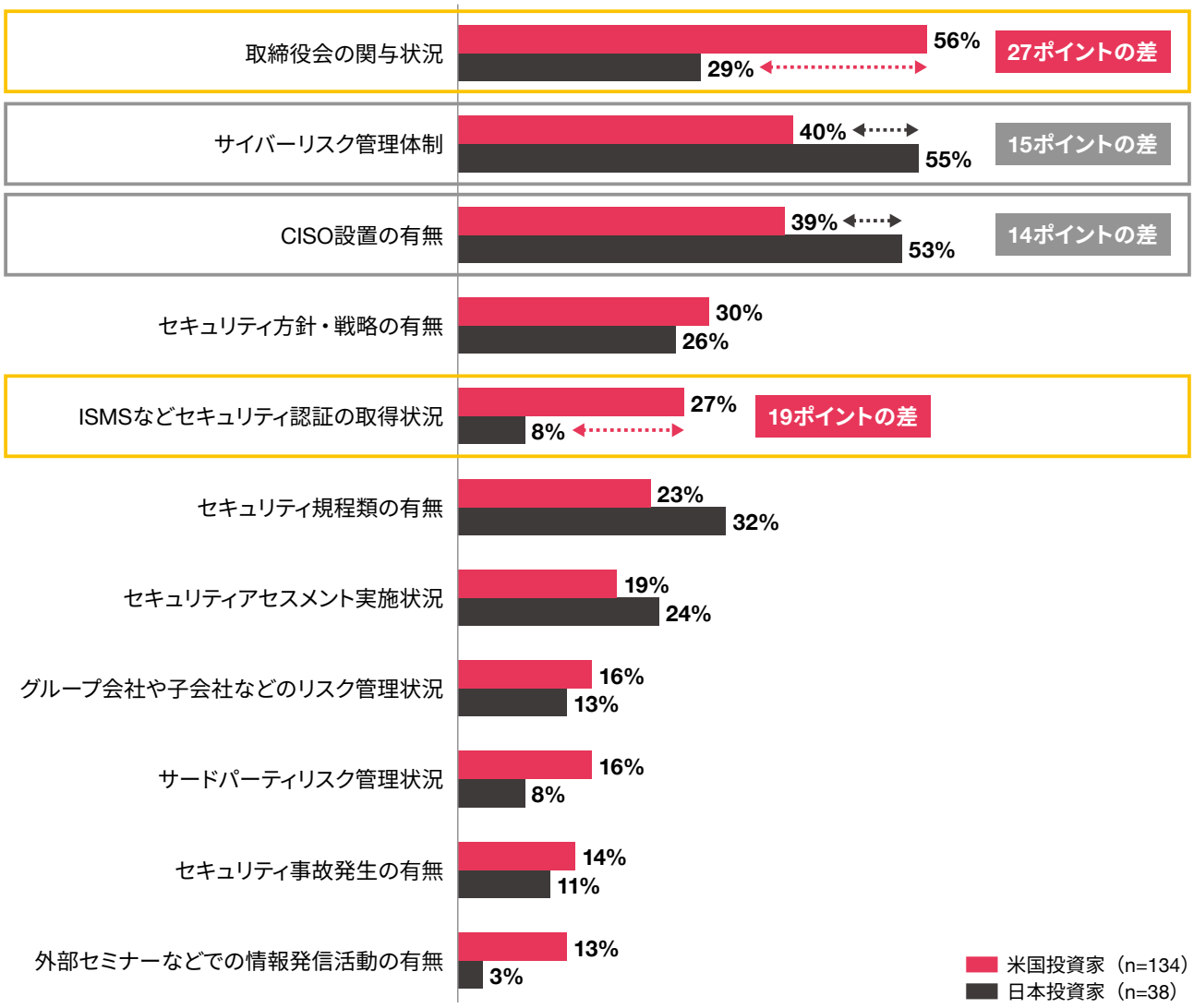
日本投資家（38名）を見ると、「サイバーリスク管理体制」が最も高く（55%）、次いで「CISO設置の有無」が53%、「セキュリティ規程類の有無」が32%、「取締役会の関与状況」が29%、「セキュリティ方針・戦略の有無」が26%の順に高くなりました（図表13）。

独自指標を整備しているとする日米投資家を比較すると最も差が現れたのは「取締役会の関与状況」で、米国投資家（56%）は日本投資家（29%）と比較し27ポイントも高く注視していることが分かります。また、「ISMSなどセキュリティ認証の取得状況」においても米国投資家（27%）と比較して日本投資家は8%と低く、19ポイントの乖離が見られます。

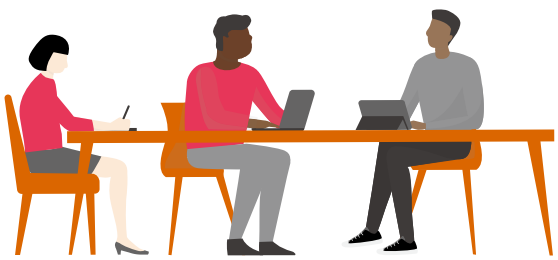
また、機関投資家インタビューにおいては、「多くの上場企業におけるサイバーセキュリティ開示情報は見栄えが良いものの、公開情報などからは実態が伴っているかまでは評価できないと考えている。このため、ISMS認証などの第三者機関の認証を評価対象としている」「インシデントが起きてから初めてサイバーセキュリティの取り組みが伴っていないことが明らかになることがある」といった意見がありました。これらの意見から、投資家とのコミュニケーション手段の1つとして「第三者認証を取得し開示すること」は、企業のセキュリティ管理体制の有効性を投資家へ分かりやすく示すことに繋がると言えます（図表14）。

8 ここでいう「セキュリティ認証」とは、ISMS（ISO/IEC 27001）、Pマーク、PCI DSSなど第三者認証を指します。

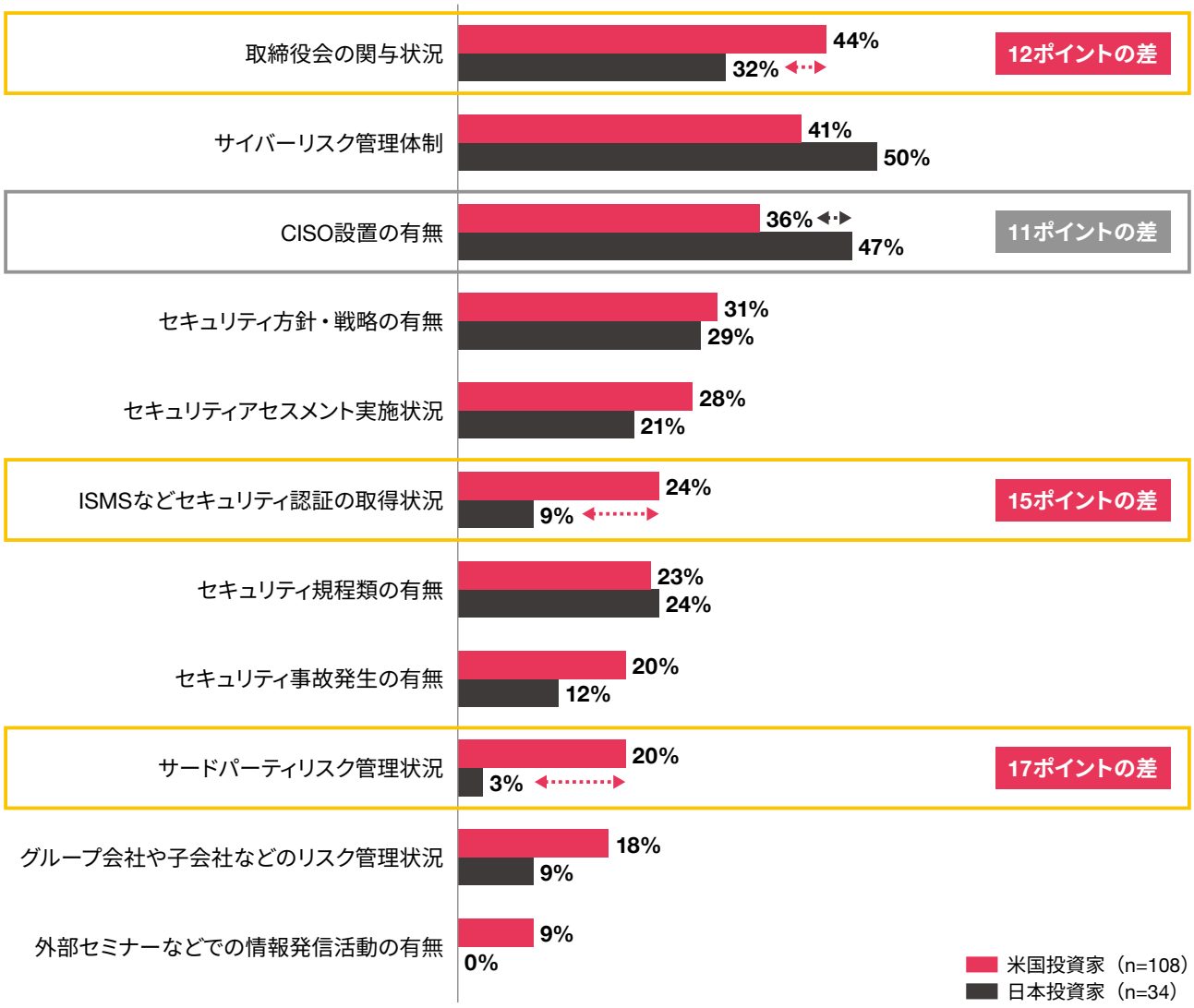
図表12：日米投資家のサイバーセキュリティ情報開示の評価項目（平時）



Q. 前問で「独自指標を整備」していると回答した方へ質問です。あなた、またはあなたが所属する組織は、投資先企業の「セキュリティ・プライバシーへの取り組み」を評価する際に特に着目する内容を教えてください。あてはまるものを全てお知らせください。



図表13：日米投資家のサイバーセキュリティ情報開示の評価項目（有事）



Q. 前問で「独自指標を整備」と回答した方へ質問です。あなた、またはあなたが所属する組織は、投資先企業の「セキュリティ・プライバシーへの取り組み」を評価する際に特に着目する内容を教えてください。あてはまるものを全てお知らせください。

図表14：日米有識者インタビュー「何を評価するのか」

米国機関投資家	私は企業のクオリティ評価を行っている。日本企業も評価しており、毎年来日して取材も行っている。 私の分析プロセスでは、まず、1つ目の要素として「国」について見る。日本が対象であれば中国などからの脅威がある。2つ目は「会社」について、過去のインシデント、企業情報、ヘッドニュースを確認している。3つ目は「ビジネス全体」について見る。 **＜一般＞** • **国レベルの脅威への対策** まずセキュリティは「機会」よりも「リスク」と捉えている。 投資リスクの3つのレベル（1：会社、2：製品サプライチェーン、コンサルタント、外部ベンダーを含む社内ビジネス全体、3：国）のうち、国レベルでのリスクが大幅に高まっていることに注目している。ロシアや北朝鮮などからの攻撃は主に欧米に向けられるが、日本では自動車会社や工業会社に対し知的財産や技術を盗もうとする脅威が増大している。 **＜企業の開示情報＞** • **ESGへの投資** サイバーセキュリティおよびプライバシーはESGおよび持続可能な社会の非常に重要な要素である。 • **セキュリティガバナンス構造の開示** 以下のようなガバナンス構造のポリシーがあることを確認する。 - 最高セキュリティ責任者、CEO、委員会は「誰」か - 当該3人が「取締役会に報告する体制」があるか - 取締役会に「サイバーセキュリティ業務経験のある取締役」が含まれているか※ ※米国では多くの取締役会でサイバーセキュリティ専門家を配置しているが、欧州や日本でさえ多くの企業はこれに取り組んでおらず、ビジネス自体に特化している。 • **委託先に対するセキュリティポリシー** ある企業のインシデント事例では、ハッカーが委託先のメールの一部にアクセスが可能であったが、核関連のビジネスのため非常に危険だった。投資先企業だけでなく、最も弱い部分からの攻撃を想定することが非常に重要である。 • **製品・サービス自体の脆弱性管理・アセスメント状況** 製品・サービスには多くの脆弱性が見つかるため、正しくアセスメントされているか確認する。私が投資する企業は、製品の脆弱性によるインシデント発生後、米国国防省のサイバーセキュリティ成熟度レベル（CMMI[9]）の採用を決定した。しかし、これは会社の施策の一部にすぎず、実際は未だに脆弱性が残っているのではないかという不安がある。 • **模擬攻撃などによるセキュリティ訓練の実施状況** 米国では、例えば、四半期に1度、標的型攻撃メール訓練を行い、従業員をテストする例がある。このようなシミュレーターの利用が、社内意識の向上や、より実態に近い評価に繋がると考える。 • **第三者認証は評価対象** 米国企業も日本企業も同じだが、サイバーセキュリティ情報開示は「見栄えが良い」ものの、公開情報などからは実態が伴っているかまでは評価できないと考えている。このため、第三者機関が評価した情報、例えばISO/IEC 27001（ISMS認証）などの第三者機関の認証取得状況を評価対象としている。ヘルスケア分野においてはHIPAAへの準拠や過去の問題・罰則について確認する。

9 U.S. Department of Defense, “Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program”（2021/11/4）
https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/

日本機関投資家	まず、投資家としては、セキュリティは「機会」というよりも「リスク」として評価する。「機会」としての評価はつけづらいが、例えばエンジニア派遣ビジネス（正社員でエンジニアを雇い企業に派遣する）においては、顧客企業の重要な情報を扱うため、この部分で契約の在り方や人材育成などは、唯一の「機会」評価として認識できる。サイバーセキュリティ評価は、ESGの「S（Social）」の一貫として評価している。 **＜評価対象＞** • **開示情報では、セキュリティに対する「ガバナンス」を見る** 企業がどのような体制で情報セキュリティ対策を取り、その評価を経営にフィードバックしているか、という点を評価する。 - 開示情報の記載量 企業によって記載量はかなり異なる。半ページ記載する企業もあれば1～2ページにわたる企業もある。特に評価するわけではないが、これを基に企業とミーティングで確認する形を取る。例えば投資先企業のサービスが攻撃を受けた際に、その年の報告書における「情報セキュリティ」の項目が分厚くなっており、企業として手厚く対処している印象を受けた記憶はある。ただ、それが投資判断に直結するかというと、そうではない。 • **取材では「過去インシデントへどのように対処し改善がなされたか」をヒアリング** サイバーセキュリティの開示情報を評価するには、セキュリティ専門知識が必要となり、投資家として正しく評価できない恐れがある。このため、そこに重きを置くよりは、実際に過去に起きた重要なインシデントの第三者委員会の報告書を見て、どのような対策を取り、「今」どのように改善されているのか、そのようなところを見る。ただ、これらの質問に対し、企業は平たく回答する印象を持つ。 **＜確認方法＞** • **開示情報は「有価証券報告書」や「統合報告書」** 情報セキュリティだけではなく、他に対するリスクも同様だが、まず見るところは「有価証券報告書」のリスクの部分。最近では「統合報告書」を出す企業が多く、情報セキュリティ記載があるので確認している。 • **チェックリストベースの取材** チェックリスト（情報セキュリティ項目を含む）に基づき企業を個別取材する。企業はセキュリティ施策の回答案を準備しているが、当該セキュリティ対策が実際に当該企業のリスクをどの程度抑えられているかまでは、残念なことに、リスクが顕在化した時に初めて分かるような状況である。 情報セキュリティの項目はあくまで一項目に過ぎず、それをもって他社と横比較をするというわけではなく、リスクとして一応調査する、という位置づけである。 - 取材では、セキュリティ専門家は同席していない印象 取材ではIR部門が窓口となるが（ここ数年では大手企業ではサステナビリティ委員会などと兼務）、3～6人参加して1人しか発言しないこともある。情報セキュリティ専門家が同席する印象はない。ESGも同様にかなり表面的な対話となる。 上場企業のサイバーセキュリティ情報開示は評価するが、実態は取材をしても分からない。特にインシデントが起きて初めて当該企業のサイバーセキュリティの取り組み実態を知ることも多い。
外資系格付け機関	企業の開示情報、実際に遵守されているかまでは見えない。企業によってはウェブページなどに、サイバーセキュリティの取り組みや、CIOやCISOにどのような責任と権限があり、社内ではこういう研修制度がありさまざまな取り組みを実施している、と開示しているが、それらの内容そのものは、実際に遵守されているのかは分からない。このため例えば以下のような仕組みのガバナンスが見えると良い。 • **セキュリティ責任者の権限・経験** セキュリティ責任者の氏名を公開した上で、当該責任者は取締役会の中でどのような権限・発言力があるのか。例えば営業部門の役員などから邪魔が入らず、本当にサイバーセキュリティだけに専念できているか。また、これらの責任者は、誰でもできるものではないと理解しているため、実務経験のバックグラウンドがあるなら、その経歴を記述すべきだと考える。ここまでやっていると「この会社は本気だ」と捉えられる。

Finding 5　平時よりForm 8-Kなどを情報源とする米国投資家は半数を占める

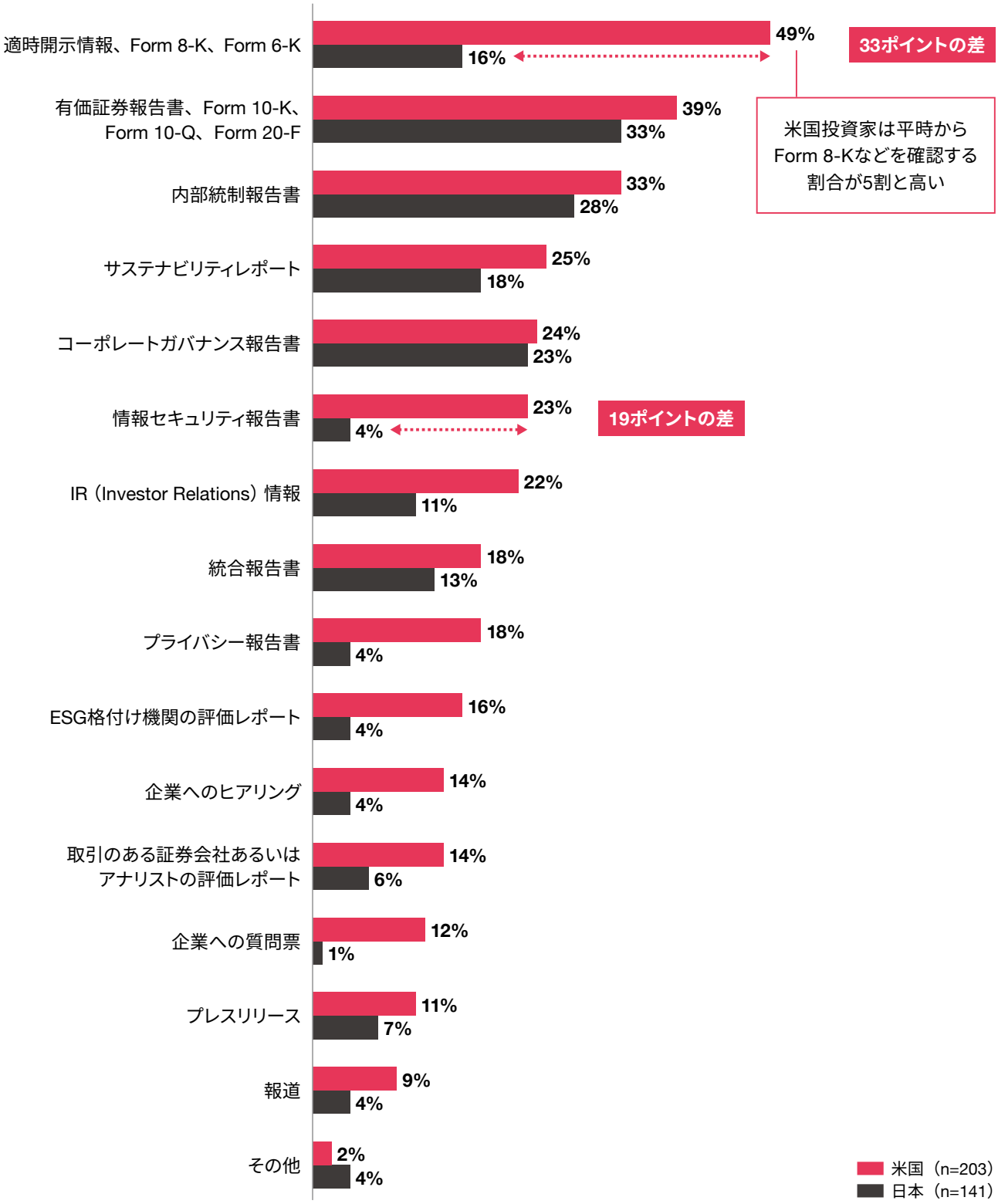
日米投資家に「投資先企業のサイバーセキュリティおよびプライバシー関連情報をどこで確認するか」と確認したところ、平時でも米国投資家の約半数は「適時開示情報、Form 8-K、Form 6-K」と回答しました。これは日本投資家よりも33ポイントも高く、特徴的です（図表15）。

具体的に見ると、平時のサイバーセキュリティ情報開示として確認する情報源は、米国投資家では、「適時開示情報、Form 8-K、Form 6-K」が最も高く（49%）、次いで「有価証券報告書、Form 10-K、Form 10-Q、Form 20-F」が39%、「内部統制報告書」が33%、「サステナビリティレポート」が25%、「コーポレートガバナンス報告書」が24%の順に高くなりました。次に、日本投資家を見ると「有価証券報告書、Form 10-K、Form 10-Q、Form 20-F」が最も高く（33%）、次いで「内部統制報告書」が28%、「コーポレートガバナンス報告書」が23%、「サステナビリティレポート」が18%、「適時開示情報、Form 8-K、Form 6-K」が16%の順に高くなりました。

また、有事のサイバーセキュリティ情報開示として確認する情報源は、米国投資家では、「有価証券報告書、Form 10-K、Form 10-Q、Form 20-F」を参照する割合が最も高く（45%）、次いで「適時開示情報、Form 8-K、Form 6-K」が38%、「内部統制報告書」が31%、「情報セキュリティ報告書」が26%、「統合報告書」「コーポレートガバナンス報告書」がともに23%の順に高くなりました（図表16）。次に、日本投資家を見ると「内部統制報告書」が最も高く（32%）、次いで「有価証券報告書、Form 10-K、Form 10-Q、Form 20-F」が29%、「コーポレートガバナンス報告書」が23%、「適時開示情報、Form 8-K、Form 6-K」「サステナビリティレポート」がともに16%の順に高くなりました。日米投資家間で最も差が現れたのは、「情報セキュリティ報告書」（米国26%、日本4%）および「適時開示情報、Form 8-K、Form 6-K」（米国38%、日本16%）で22ポイントの差となりました。

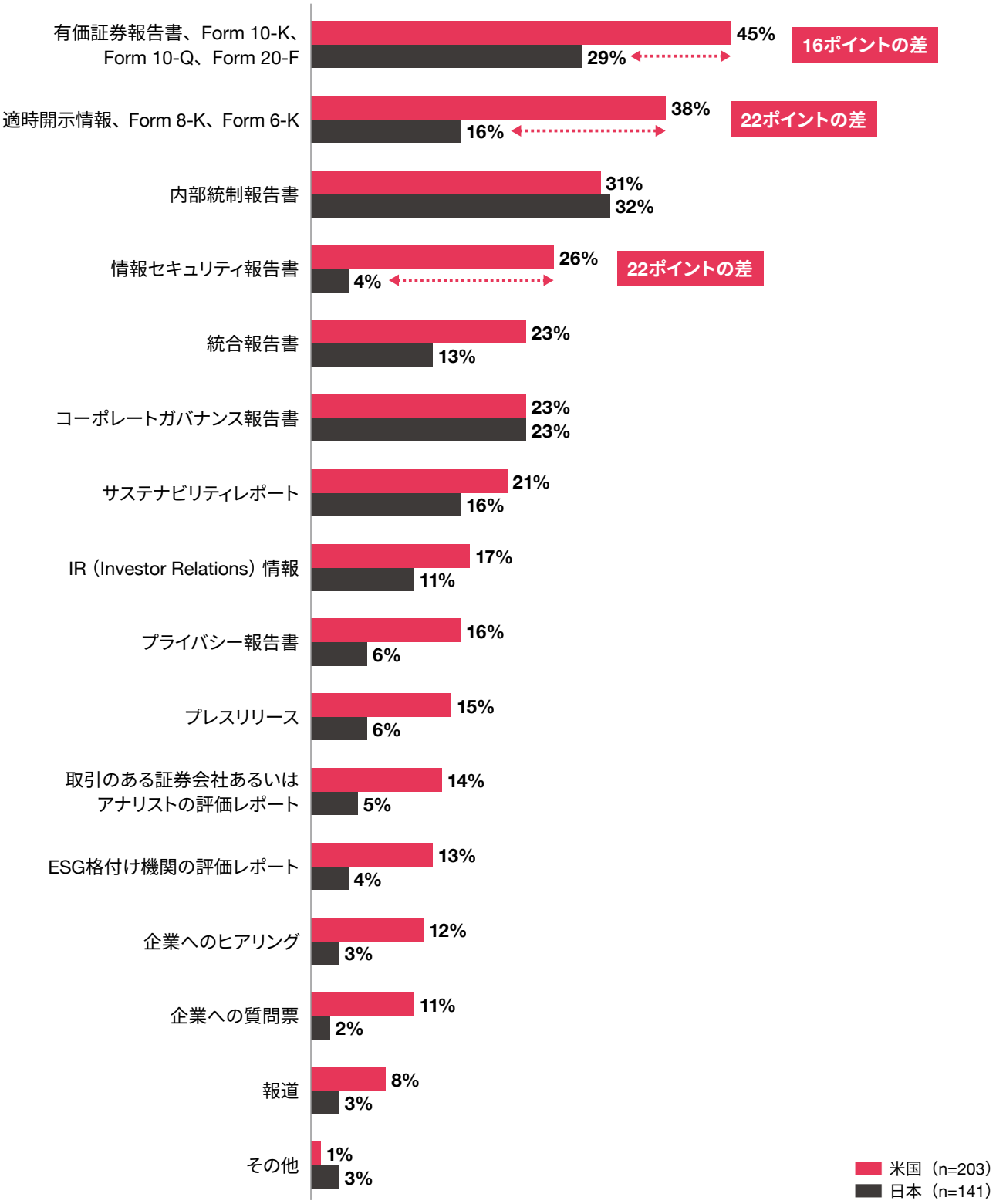
この他、日米有識者インタビューの回答にあるように、有事の情報源として「早く情報入手ができる」という理由で報道や業界記事などを見ていること（図表17）を踏まえると、メディアに適切な情報開示を行うことも重要と言えます。

図表15：サイバーセキュリティ開示情報（平時）の情報源



Q. あなた、またはあなたが所属する組織は、投資先企業の「サイバーセキュリティおよびプライバシー」に関する情報について、どこで情報を確認しますか。あてはまるものを全てお知らせください。

図表16：サイバーセキュリティ開示情報（有事）の情報源



Q. あなた、またはあなたが所属する組織は、投資先企業の「サイバーセキュリティおよびプライバシー」に関する情報について、どこで情報を確認しますか。あてはまるものを全てお知らせください。

図表17：日米有識者インタビュー「投資先企業のサイバーセキュリティ情報開示の情報源」

米国機関投資家	情報源としてForm 8-Kなどは見ているが、投資家にとっては最新の情報を入手することは難しいため、同業界情報誌・報道、セキュリティブログ／レポートなどを複数参照することも多い。なぜなら、そちらの方がよりテクニカルで、情報が早いためだ。
日本機関投資家	（一部再掲） 情報セキュリティだけではなく、他に対するリスクも同様だが、まず見るところは「有価証券報告書」のリスクの部分。最近では「統合報告書」を出す企業が多く、情報セキュリティ記載があるので確認している。 この他、投資先でインシデントが発生した際の情報源は、報道で第一報を知った。

Finding 6 「投資先のサイバーセキュリティ情報開示は十分と言えない」日本投資家は5割と多い

日米国投資家に「投資先企業のサイバーセキュリティおよびプライバシー情報開示は十分と言えるか」と確認したところ、米国投資家よりも日本投資家が「情報開示は十分でない」と答える割合が高く、約半数を占めました（図表18）。

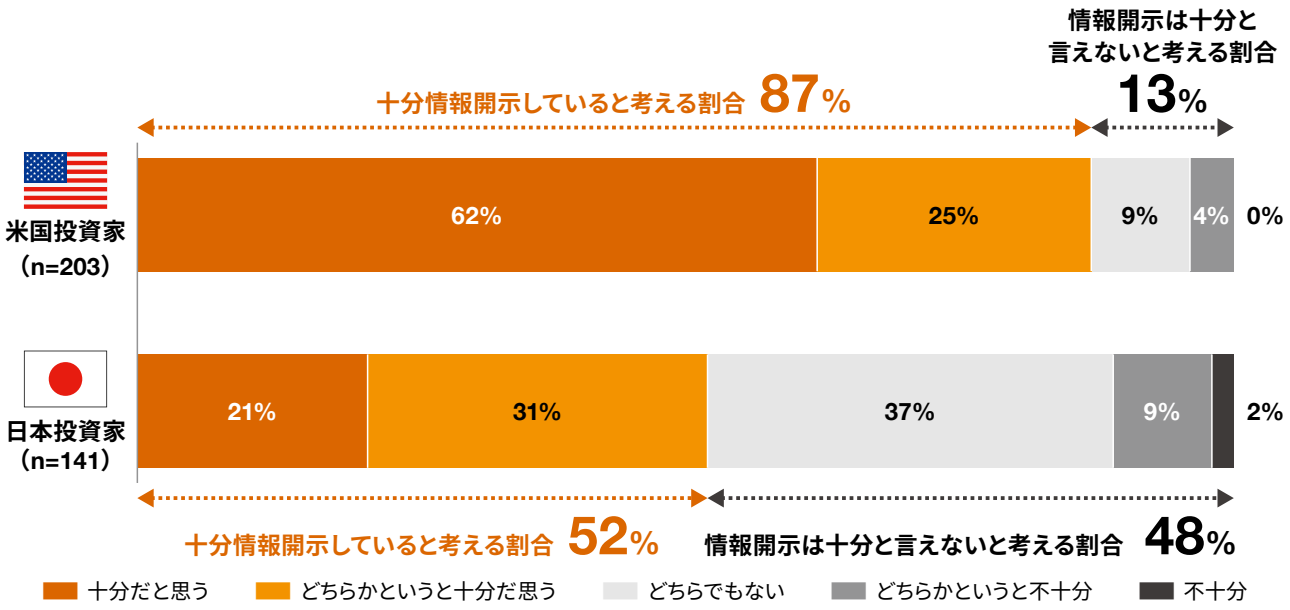
具体的に見ると、米国投資家では、「十分だと思う」とする割合が全体の62%、「どちらかというと十分だと思う」が25%、「どちらでもない」が9%、「どちらかというと不十分」が4%となりました。このため、米国投資家は「十分だと思う・どちらかというと十分だと思う」の合計が全体の87%と、高く評価している傾向にあります。

一方で、日本投資家を見ると、「十分だと思う」とする割合が全体の21%、「どちらかというと十分だと思う」が31%、「どちらでもない」が37%、「どちらかというと不十分」が9%、「不十分」が2%となりました。日本投資家は「情報開示は十分と言えない」とする割合が全体の48%と半数を占めることから、投資家・企業間のサイバーセキュリティに関する対話において課題があり、改善の余地があることが分かります。

考察 なぜ日本投資家は「情報開示は十分と言えない」割合が高いのか

このような背景としていくつか仮説が立てられます。
1つ目は、米国のForm 10-Kなどではリスクについて分量面で多く記載される傾向があるため、十分な情報セキュリティ開示がなされていると考えられる一方で、日本ではそれらの記載が不十分であること。
2つ目は、今回の調査の回答者である日本投資家の属性として、サイバーセキュリティにリテラシーの高いグループが出現してしまった可能性があること。
3つ目は、インタビュー（図表7・図表14）でもあるように、投資家の評価する側が、専門性が高すぎるため十分な評価ができない、つまり「評価者の力量」に課題があり、十分だと回答する割合が高く出すぎている恐れがあること。
私たちは、後述するセキュリティ専門家の採用率も踏まえると、1つ目の仮説が最も有力なのではないかと推察します。
この仮説が正しいとすると、日本企業は開示情報の内容だけでなく「量」についても再考の余地があると言えます。

図表18：投資先企業のサイバーセキュリティおよびプライバシー情報開示は十分だと考える割合



Q. 投資先企業の「サイバーセキュリティおよびプライバシー」の開示情報は、あなた、またはあなたが所属する組織が投資判断を下すのに十分な情報が開示されていると思いますか。最もあてはまるものを1つお知らせください。

Finding 7 リスクの高い業界・保有期間・投資規模に応じて、投資先企業のサイバーセキュリティ情報開示の「評価の重みづけ」を変える米国投資家は9割超と多い

日米投資家に「セキュリティリスクの高い業界・保有期間・投資規模に応じて評価の重みづけを変えるか」と確認したところ、「変える」と回答した米国投資家は9割超と日本投資家（約8割）より高くなりました（図表19）。

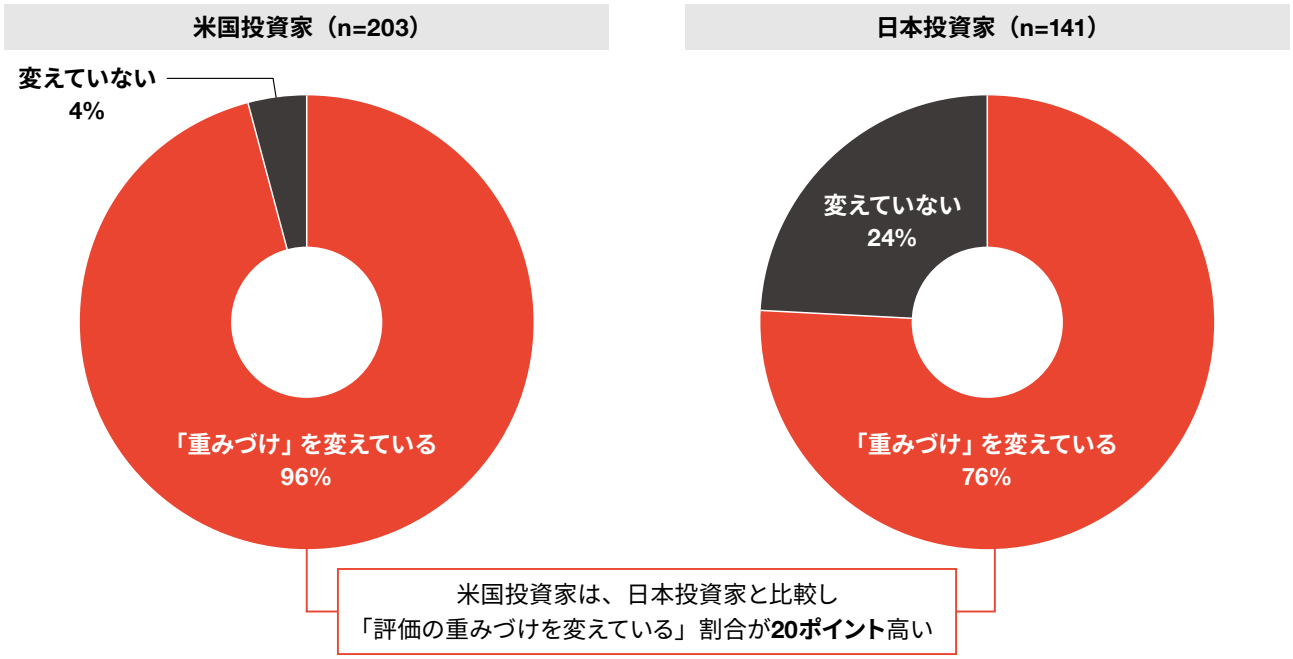
さらに、「セキュリティリスクの高い業界」「株式保有期間」「投資規模」の3つの観点から評価の重みづけを変えるかを確認したところ、「変える」と回答した割合は、日米投資家ともに「セキュリティリスクの高い業界」が最も高くなりました（図表20）。

また「セキュリティリスクの高い業界」を具体的に見ると、米国投資家（154名[10]）においては、「卸売業、小売業」「製造業」が最も高く（ともに21%）、次いで「金融業、保険業」「情報通信業」がともに19%、「建設業」が15%の順にセキュリティリスクが高い業界だと認識されていることが分かりました（図表21）。次に日本投資家（84名[11]）においては、「金融業、保険業」が最も高く（27%）、次いで「情報通信業」が18%、「建設業」が17%、「サービス業（他に分類されないもの）」が12%、「電気・ガス・熱供給・水道業」が11%の順にリスクが高い業界だと認識されていることが分かりました。

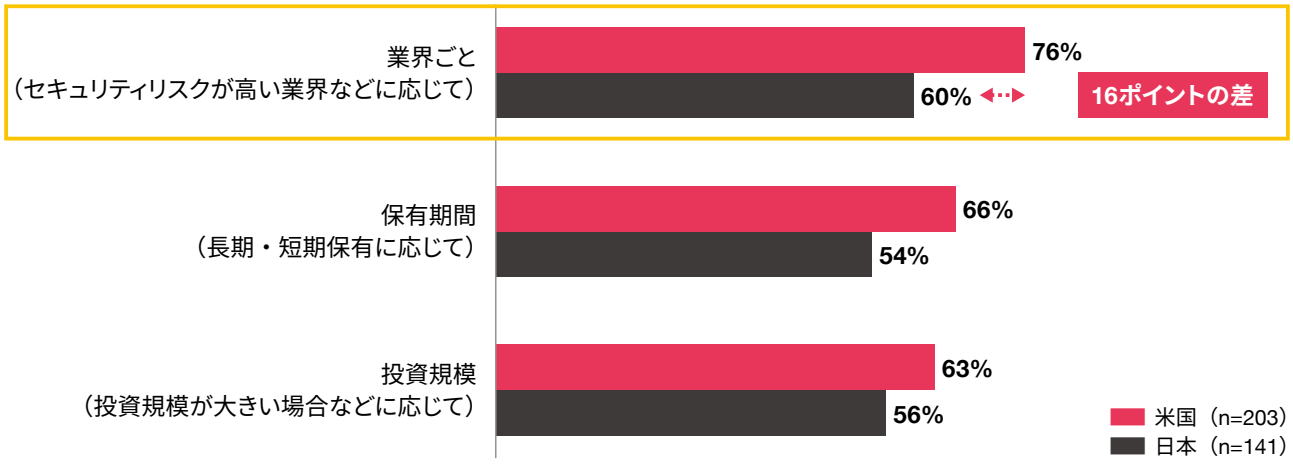
この他、「株式保有期間」においては、米国投資家は、1年以上株式保有する場合に評価の重みづけをすると回答した割合が7割と、日本投資家よりやや高い傾向があり（図表22）、同様に「投資規模」においては、「1億円以上」「100万米ドル以上」とする割合が日米投資家ともに半数程度存在します（図表23）。

10 セキュリティリスクの高い業界ごとに評価の重みづけを変えるとした米国投資家154名
11 セキュリティリスクの高い業界ごとに評価の重みづけを変えるとした日本投資家84名

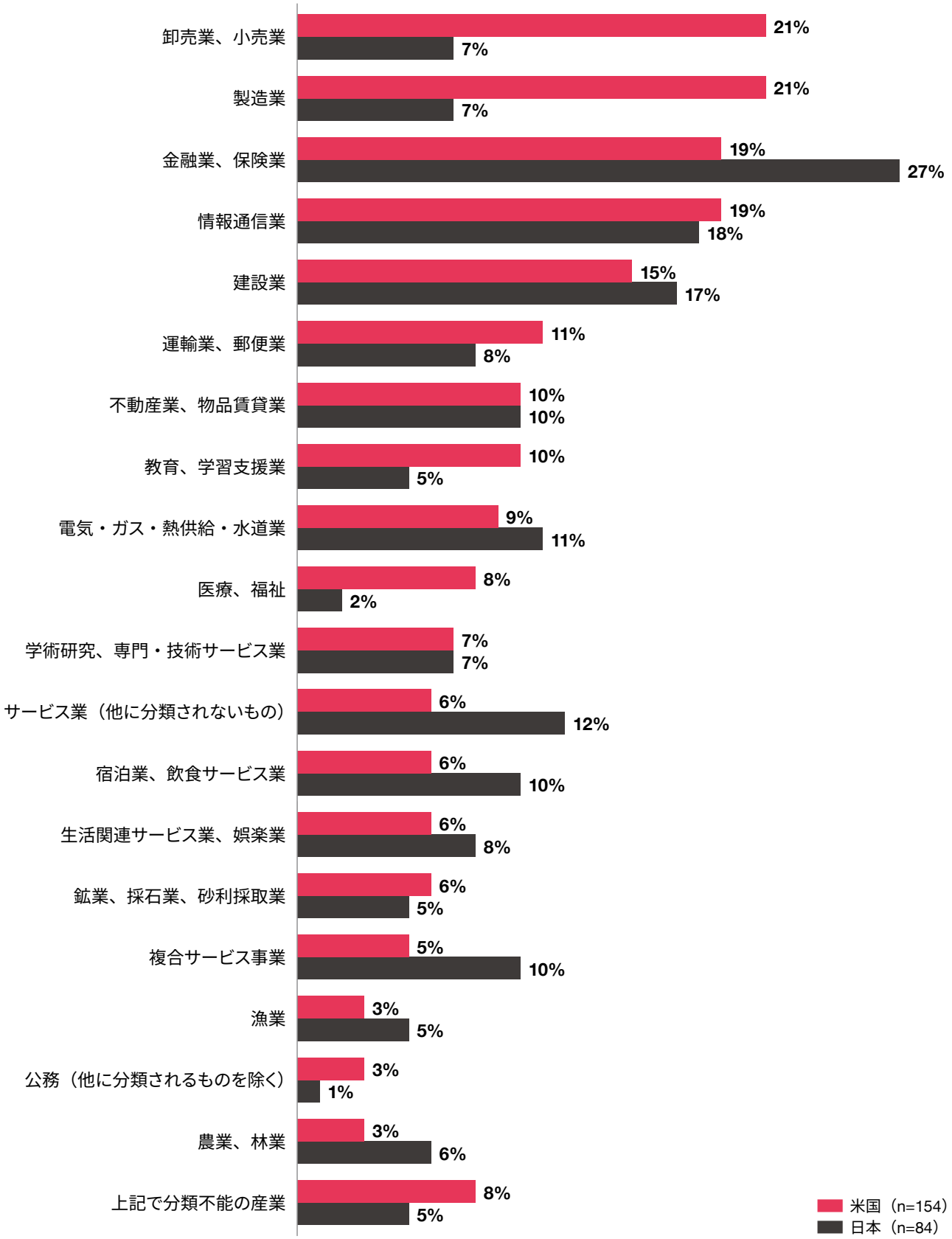
図表19：セキュリティリスクの高い業界・保有期間・投資規模に応じて評価の重みづけを変えると回答した割合



図表20：セキュリティリスクの高い業界・保有期間・投資規模に応じて評価の重みづけを変えると回答した割合

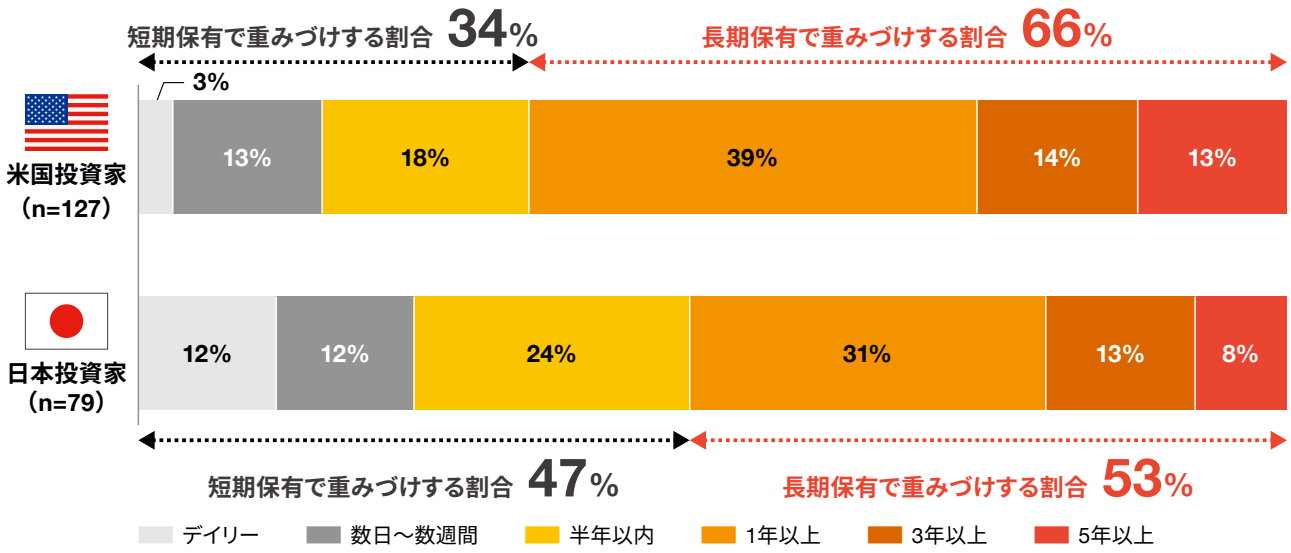


図表21：投資家が「セキュリティリスクが高い」と認識する業界



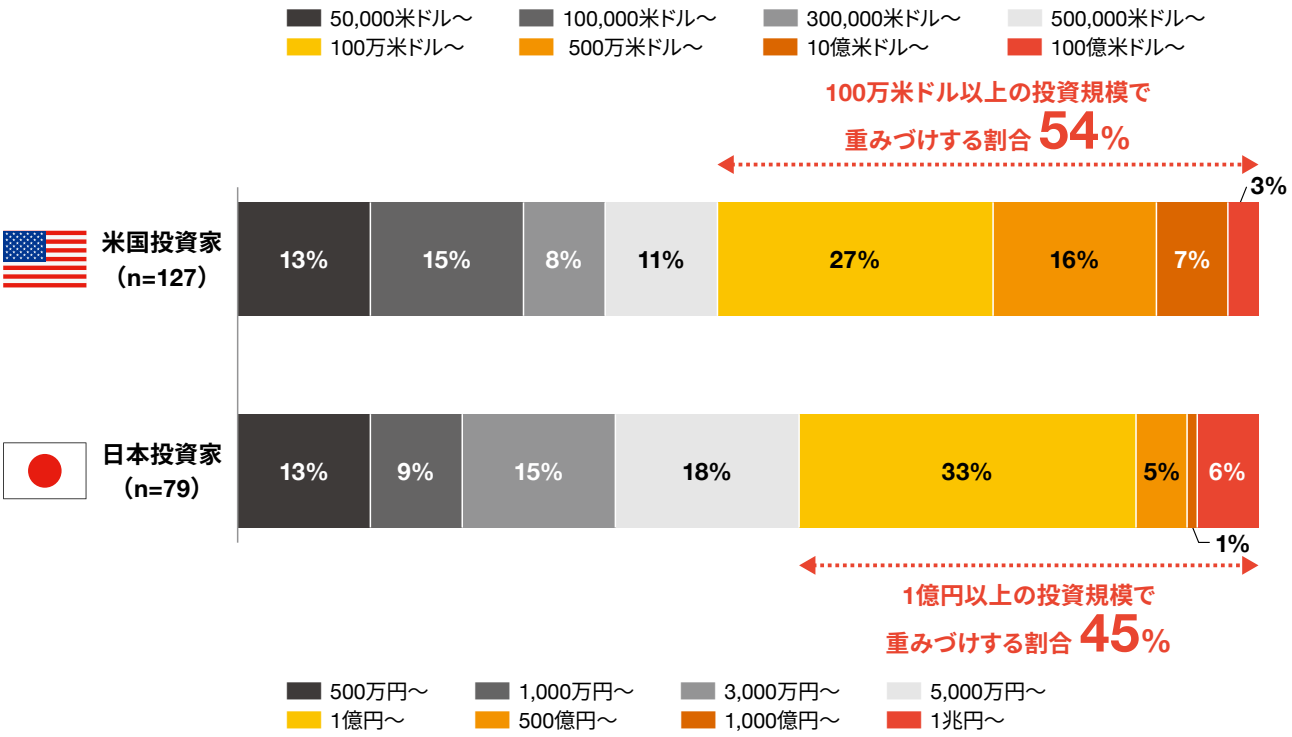
Q. 前問で業界ごとに重みづけを変えていると回答した方へ質問です。あなた、またはあなたが所属する組織は、もしくはあなたの会社が、投資先企業の「サイバーセキュリティおよびプライバシー」について特に評価する業界（セキュリティリスクが高いとする）を教えて下さい。あてはまるものを全てお知らせください。

図表22：評価の重みづけを変えるとする保有期間



Q. 前問で保有期間に応じて重みづけを変えていると回答した方へ質問です。あなた、またはあなたが所属する組織が、投資先企業の「サイバーセキュリティおよびプライバシー」について評価対象とする保有期間を教えてください。最もあてはまるものを1つお知らせください。

図表23：評価の重みづけを変えるとする投資規模



Q. 前問で投資規模に応じて重みづけを変えていると回答した方へ質問です。あなた、またはあなたが所属する組織は、投資金額がいくら以上であれば、投資先企業の「サイバーセキュリティおよびプライバシー」について、評価対象としますか。最もあてはまるものを1つお知らせください。

Finding 8　投資規模が大きい場合「1社ずつ個別評価する」米国投資家は7割と、日本投資家（3割）より多い

日米投資家に「リスクの高い業界・保有期間・投資規模に応じて評価は、1社ずつ個別評価するか」と確認したところ、「1社ずつ個別評価している」とした割合は、「投資規模が大きい場合」で最も差が顕著に現れ、米国投資家は67%と日本投資家（34%）より33ポイント高くなりました（図表24）。

各カテゴリの具体的な傾向は以下のとおりです。

① 投資規模が大きい場合

米国投資家においては、「1社ずつ個別評価している」が67%、「1社ずつ個別評価せず、ESG格付け機関などの情報を参照」が30%、「評価していない」が3%となりました。次に日本投資家においては、「1社ずつ個別評価している」が34%、「1社ずつ個別評価せず、ESG格付け機関などの情報を参照」が49%、「評価していない」が17%となりました。

② セキュリティリスクの高い業界の場合

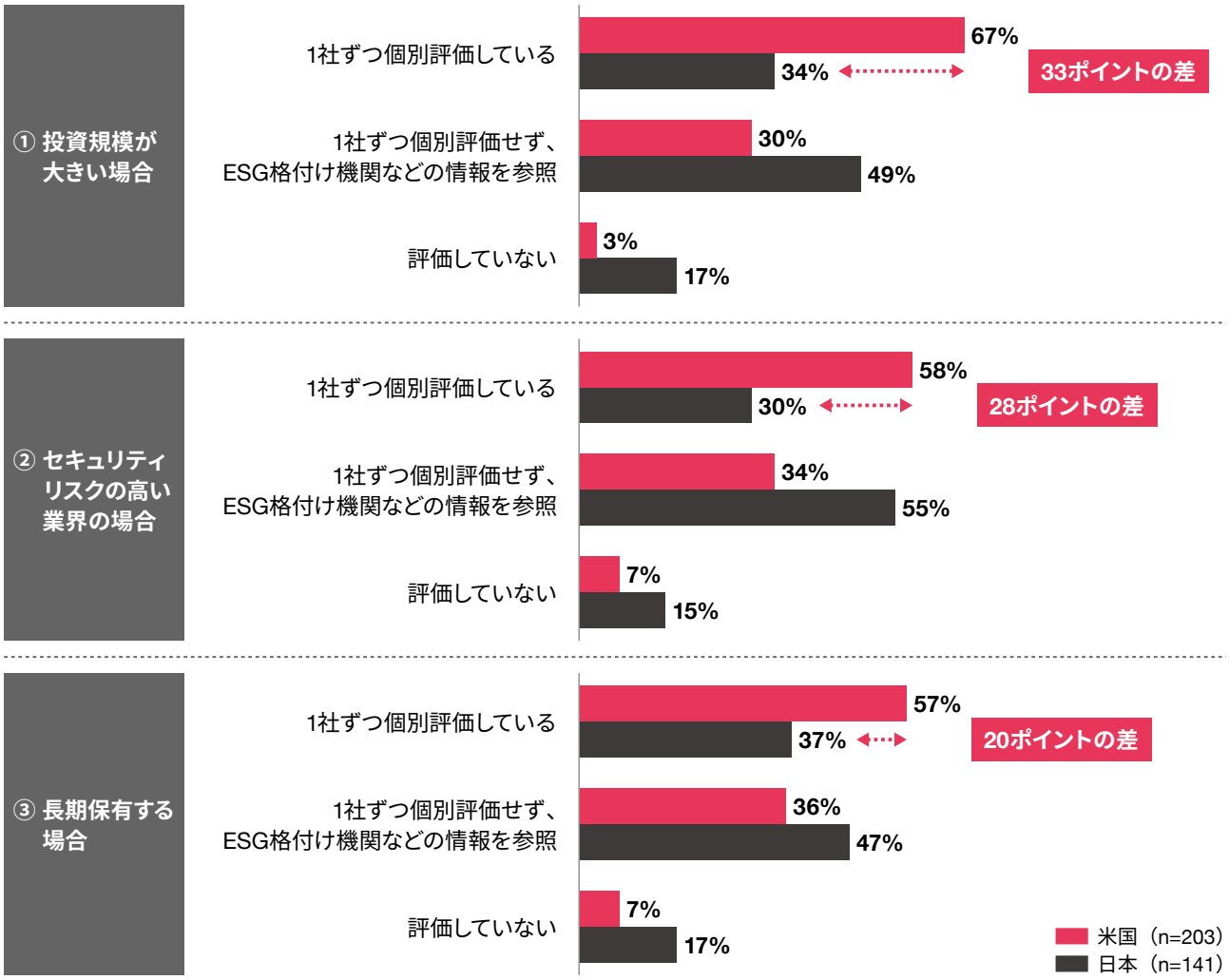
米国投資家においては、「1社ずつ個別評価している」が58%、「1社ずつ個別評価せず、ESG格付け機関などの情報を参照」が34%、「評価していない」が7%となりました。次に日本投資家においては、「1社ずつ個別評価している」が30%、「1社ずつ個別評価せず、ESG格付け機関などの情報を参照」が55%、「評価していない」が15%となりました。

③ 長期保有する場合

米国投資家においては、「1社ずつ個別評価している」が57%、「1社ずつ個別評価せず、ESG格付け機関などの情報を参照」が36%、「評価していない」が7%となりました。次に日本投資家においては、「1社ずつ個別評価している」が37%、「1社ずつ個別評価せず、ESG格付け機関などの情報を参照」が47%、「評価していない」が17%となりました。

これらから、米国投資家ではリスクの高い業界・保有期間・投資規模に応じて「1社ずつ評価」する傾向があると言えます。また、日本投資家では、個別評価よりも「格付け機関などの評価」を参照する傾向があり、「評価しない」割合も2割弱と一定数存在することが明らかになりました。

図表24：セキュリティリスクの高い業界・保有期間・投資規模に応じて、投資先企業を1社ずつ個別評価するか



投資先企業との対話 ② 質問の傾向

Finding 9 **投資先企業へサイバーセキュリティについて質問する米国投資家は9割超、うち過半数が平時・有事におけるサイバーセキュリティに特化した質問項目を準備**

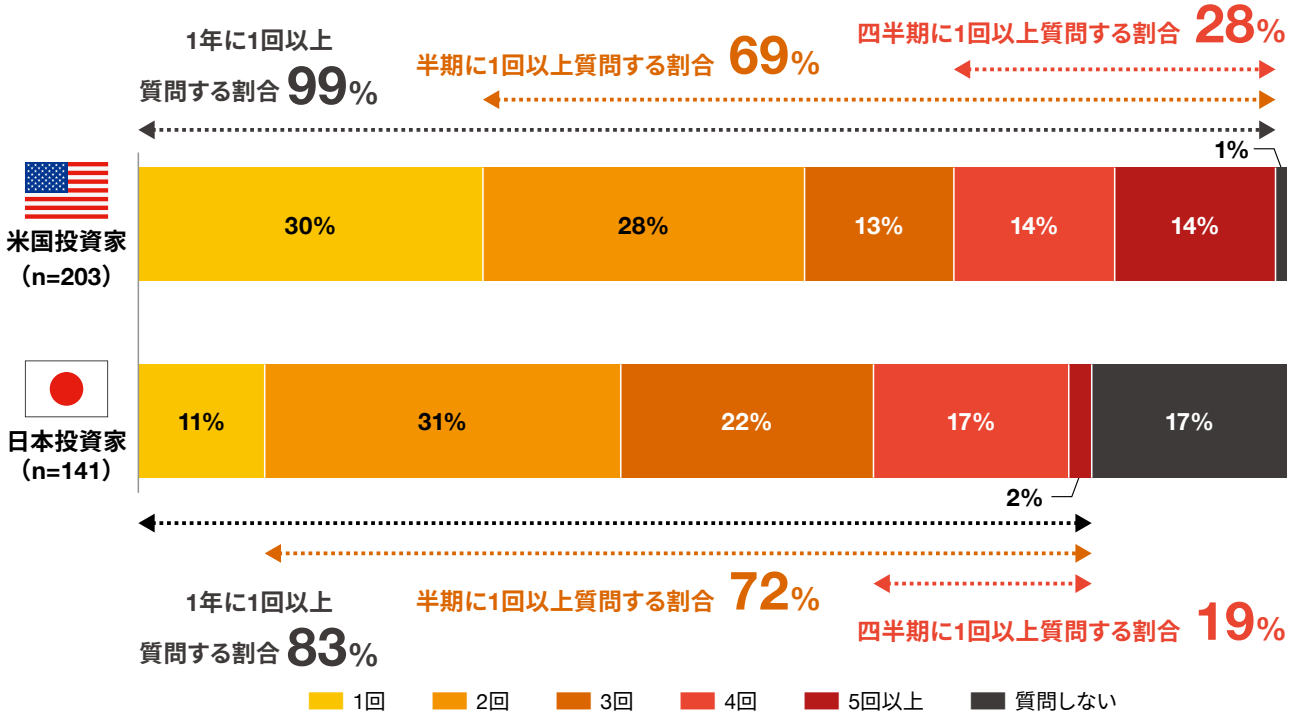
投資先へサイバーセキュリティについて質問する米国投資家は9割超

日米投資家に「『サイバーセキュリティ』について投資先企業へ質問する回数は、1年に何回程度か」確認したところ、「年に1回以上質問する」と回答した米国投資家の割合は9割超、日本投資家は約8割と、日米投資家ともに高くなりました（図表25）。

具体的に見ると、米国投資家では、「年に1回以上質問する」割合が全体の99%、「年に2回以上質問する（半期ごと）」が69%、「年に3回以上質問する（4カ月ごと）」が41%、「年に4回以上質問する（四半期ごと）」が28%となりました。

次に、日本投資家を見ると、「年に1回以上質問する」割合が全体の83%、「年に2回以上質問する（半期ごと）」が72%、「年に3回以上質問する（4カ月ごと）」が41%、「年に4回以上質問する（四半期ごと）」19%となり、日米投資家において、有意な差は確認できませんでした。

図表25：投資先企業との対話：サイバーセキュリティについて質問する割合



Q. あなた、またはあなたが所属する組織が、投資先企業へ質問する回数は、1年に何回程度ですか。

米国投資家の過半数が、平時・有事における質問項目を準備

日米投資家において「1年あたりのサイバーセキュリティ関連質問回数の割合」では差が確認できなかった一方、「投資先に対してサイバーセキュリティ関連質問項目を準備する割合（平時）」は、米国投資家では過半数を占め、日本投資家（27%）より27ポイントも高く、またこれは有事においても同様の傾向であることが明らかになりました（図表26）。

1. 平時における投資先へのサイバーセキュリティ関連質問項目の準備状況

具体的に見ると、米国投資家では、平時における投資先へのサイバーセキュリティ関連質問項目を「用意している」とする割合は全体の54%、「現在準備中である」が35%、「現在検討中」が9%、「用意しておらず、用意する予定もない」は3%となりました。

次に、日本投資家を見ると、「用意している」とする割合は全体の27%、「現在準備中である」が47%、「現在検討中」が24%、「用意しておらず、用意する予定もない」は2%となりました。

2. 有事における投資先へのサイバーセキュリティ関連質問項目の準備状況

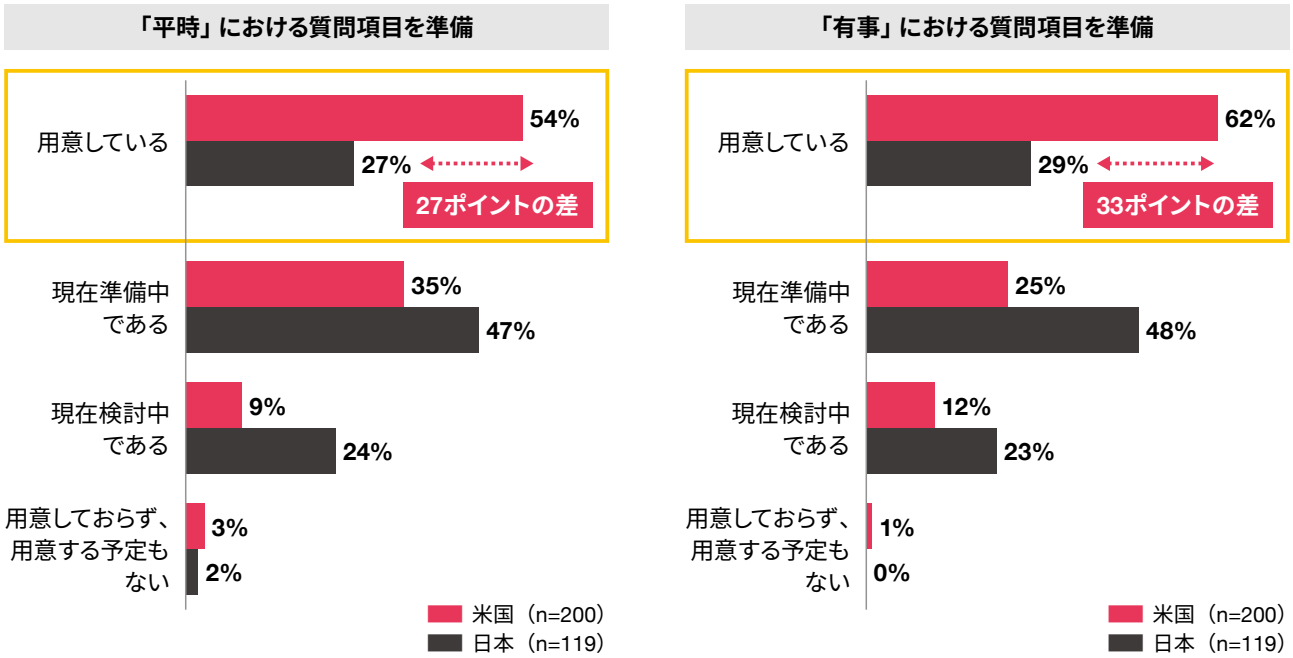
米国投資家では、有事における投資先へのサイバーセキュリティ関連質問項目を「用意している」とする割合は全体の62%、「現在準備中である」が25%、「現在検討中」が12%、「用意しておらず、用意する予定もない」は1%となりました。

次に、日本投資家を見ると、「用意している」とする割合は全体の29%、「現在準備中である」が48%、「現在検討中」が23%、「用意しておらず、用意する予定もない」は0%となりました。

米国投資家はサイバーセキュリティ関連の質問項目を準備しており、特に有事において準備状況の割合が高い傾向にあることが明らかになりました。日本投資家においては、準備済みの割合は約3割と低いものの「現在準備中」である割合が約半数を占めているため、近年中に日本投資家においても7割を超える見込みです。これらのことから、今後、投資家との対話の中でより一層、サイバーセキュリティ関連の質問を受ける機会が高まると言えます。

また日米有識者インタビューの中で、日本企業はインシデント発生時に原稿読み上げで回答する傾向にあるが、このいわゆる日本方式の対話は海外投資家には通用しない、とのコメントがあることから、海外投資家に対し自身の言葉で説明することがグローバル企業には求められることでしょう（図表27）。

図表26：投資先へのセキュリティに関する質問項目の準備状況



Q. 前問で投資先企業へ質問すると回答した方へ質問です。あなた、またはあなたが所属する組織は、投資先企業へ「サイバーセキュリティおよびプライバシーの取り組みやリスク、セキュリティ事故」について質問項目を用意していますか。最もあてはまるものを1つお知らせください。

図表27：日米有識者インタビュー「海外投資家に対し日本企業はどのようなことができると良いか」

外資系格付け機関	• **原稿なしで対応できることが求められる** サイバーインシデントが発生した際に「原稿なしで英語で対応できる」ことが求められる。日本企業は、典型的な日本方式で、誰かが準備した原稿を読み上げながら深くお辞儀して謝罪する形式を取るが、これは海外投資家には通用しない。 • **セキュリティ責任者は、専門家が着任すべき** インシデントを説明する担当者の職階が高い場合、その担当者が「どこまで知って」いて、本当にそれらを「仕切る技術力」があるのかを疑われる恐れがある。本当に仕切っていれば、どのような質問が来ても回答できるはずだからだ。年功序列が残る日本企業において、業務経験のない者がCIOやCISOに任命されることがしばしばあるが、責任者がテクノロジー専門家であることが重要である。 また、同業他社がインシデントを起こした際に、普通であれば自社も大丈夫だろうか、と考えるはずである。そのような時に投資家から「同業他社でのインシデントを踏まえ、貴社ではどのような対応を予定しているか」などの質問があっても何も回答がない場合、「これまでの期間に何をしていたのだろうか」と考えてしまう。ただしこれは、組織の中で権限が何番目にあるかにも依存する。一方で、権限があっても、それを仕切る能力がなければ効果的なセキュリティ対策を遂行できるとは言えない。 • **海外投資家への対応は「英語」が望ましい** 海外投資家の共通言語は英語であるため、できれば英語が望ましいが日本語でも良い。しっかり頭の中でシステム図面を描き、何がどうなったか説明ができればそれで良い。

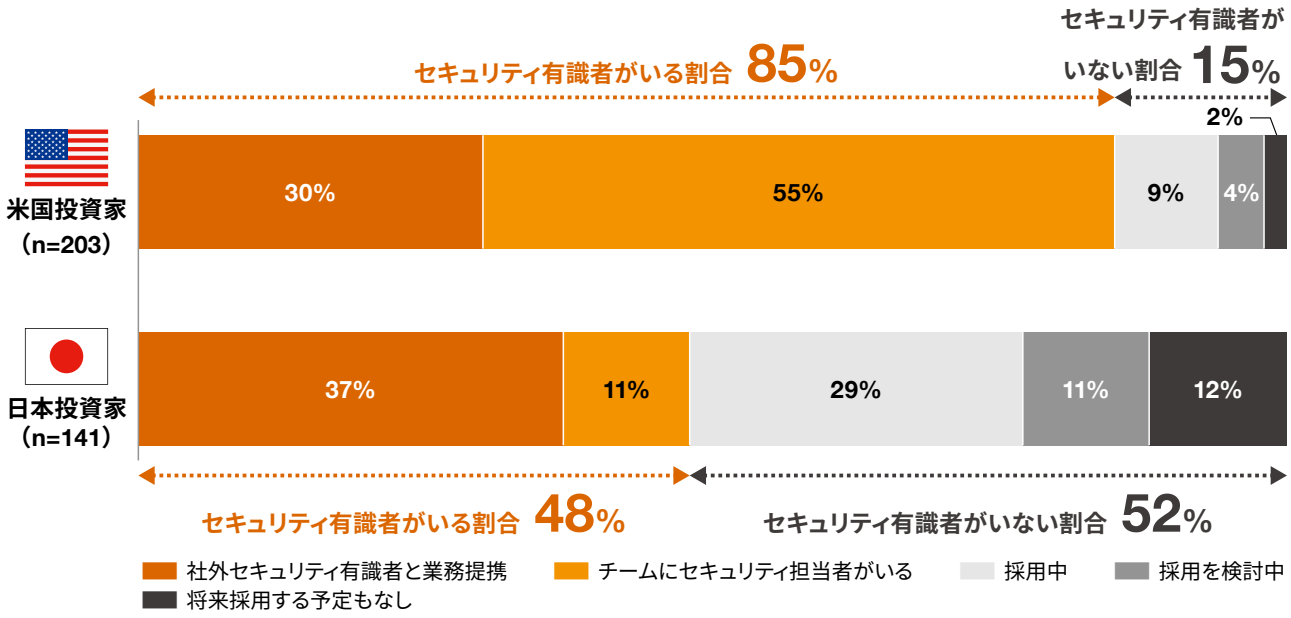
Finding 10　米国投資家は「チームにセキュリティ担当者がいる」が半数を超え、日本投資家は採用中・採用検討中が4割と、評価強化が進む

日米投資家に「投資先企業へのヒアリング実施にあたり、チームにセキュリティ担当者がいるか」と確認したところ、米国投資家の過半数が「チームにセキュリティ担当者がいる」としており、日本投資家（11%）と比較して44ポイントも高いことが明らかになりました（図表28）。

具体的に見ると、米国投資家では、「チームにサイバーセキュリティ担当者がいる」とする割合は全体の55%、「社外セキュリティ有識者と業務提携している」は30%であり、サイバーセキュリティの有識者がいるとする割合が85%と高いことが分かります。さらにチームにサイバーセキュリティ担当者が不在とする米国投資家（15%）においても、「現在採用中である」が9%、「採用を検討中である」が4%と、改善されることが見込まれています。

次に、日本投資家を見ると、「チームにサイバーセキュリティ担当者がいる」とする割合は全体の11%、「社外セキュリティ有識者と業務提携している」は37%であり、サイバーセキュリティの有識者がいるとする割合が48%と半数存在することが分かります。またチームにサイバーセキュリティ担当者が不在とする日本投資家（52%）においては「現在採用中である」とする割合が29%、「採用を検討中である」が11%となっており、今後、米国投資家だけでなく日本投資家においても、投資先企業へのサイバーセキュリティに関する専門的な質問がされる可能性があるため、企業は特に有事の際の対話についてCISOなどと方針を十分に議論することが求められます。

図表28：ヒアリング実施にあたり「チームにセキュリティ担当者がいるか」

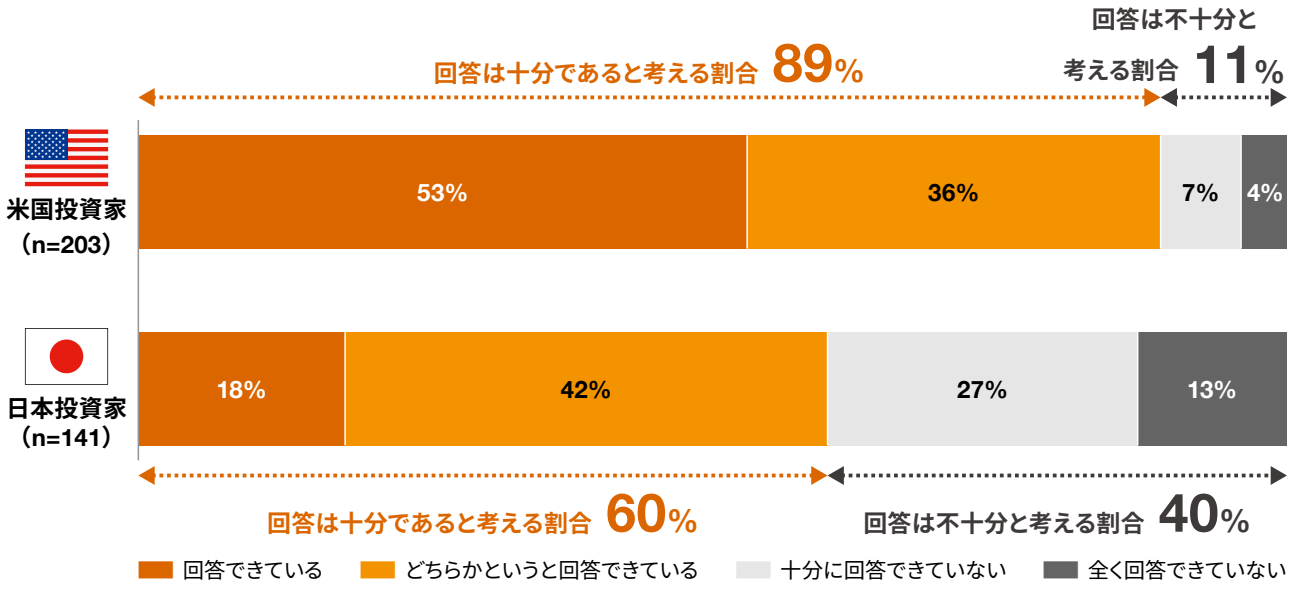


Q. あなた、またはあなたが所属する組織は、投資先企業へ「サイバーセキュリティおよびプライバシーの取り組みやリスク、セキュリティ事故」の質問をするため、サイバーセキュリティおよび／またはプライバシーの有識者をチームに採用していますか。最もあてはまるものを1つお知らせください。

参考　投資先へサイバーセキュリティについて質問する米国投資家は9割超

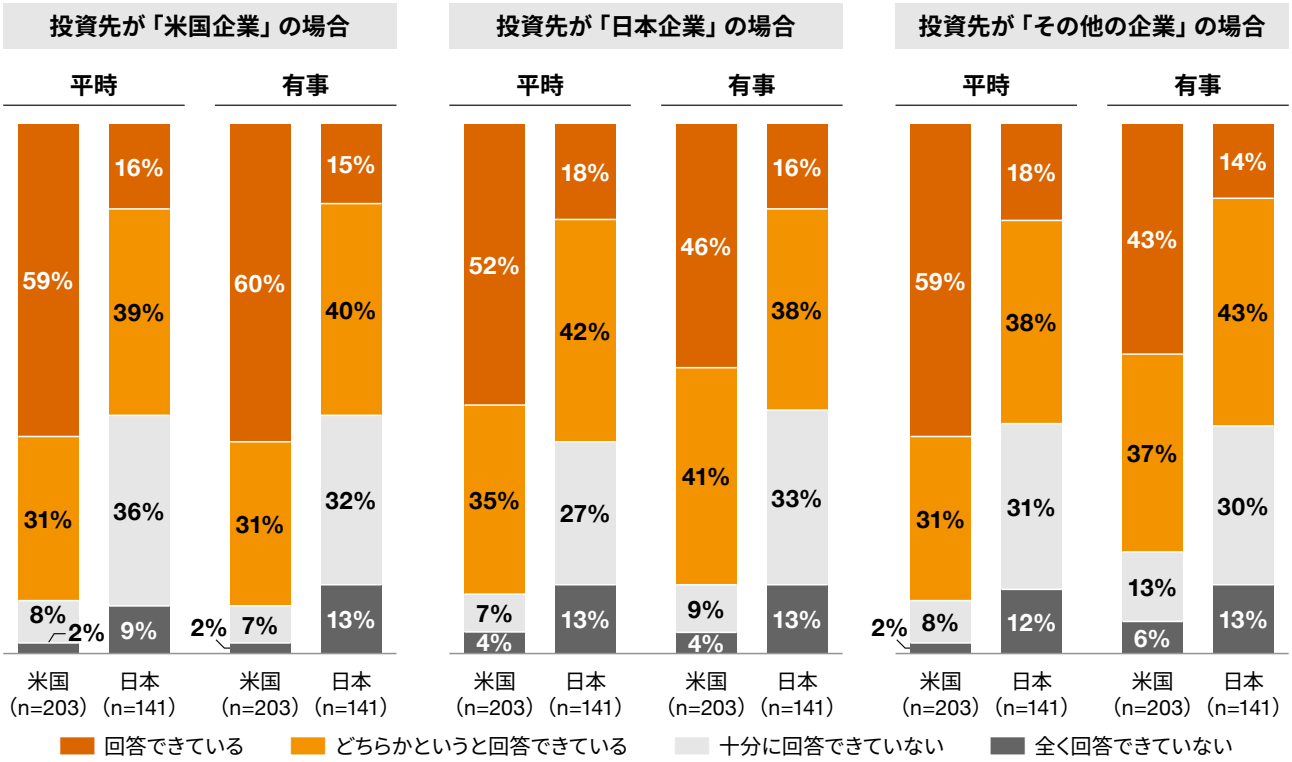
日本企業がセキュリティ関連の質問へ十分に回答できていると考える米国投資家は約9割と高い一方、同じ質問に対する日本投資家の回答では6割に留まり、不十分と考える割合が4割も存在することが分かりました（図表29・30）。この傾向は平時・有事ともに、また日本企業以外の投資先企業においても現れていることから、日本投資家の求める期待値が高い、または評価者の力量が不十分である可能性が推察されます。

図表29：投資先企業（日本企業）が「サイバーセキュリティに関する質問」へ十分に回答できていると考える割合（参考）



Q. 以下それぞれの国の投資先企業は「サイバーセキュリティおよびプライバシーの取り組みやリスク、セキュリティ事故」について、あなた、またはあなたが所属する組織からの質問に十分に回答できていると思いますか。最もあてはまるものを1つお知らせください。

図表30：投資先企業が「サイバーセキュリティに関する質問」へ十分に回答できていると考える割合（参考）



Q. 以下それぞれの国の投資先企業は「サイバーセキュリティおよびプライバシーの取り組みやリスク、セキュリティ事故」について、あなた、またはあなたが所属する組織からの質問に十分に回答できていると思いますか。最もあてはまるものを1つお知らせください。

投資先企業のサイバーインシデントを起因とする「損失・売却・訴訟」

Finding 11 **投資先が「サイバーインシデントやリスクを適切に開示しなかったこと」を起因とする損失経験は、日米投資家ともに7割超と多い**

日米投資家に「投資先企業の『サイバーインシデントリスクやセキュリティ事故発生』を企業が適切に開示しなかったことにより損失を受けた回数」を確認したところ、「損失経験がある」と回答した米国投資家の割合は86%、日本投資家は75%と、日米投資家ともに高くなりました（図表31）。

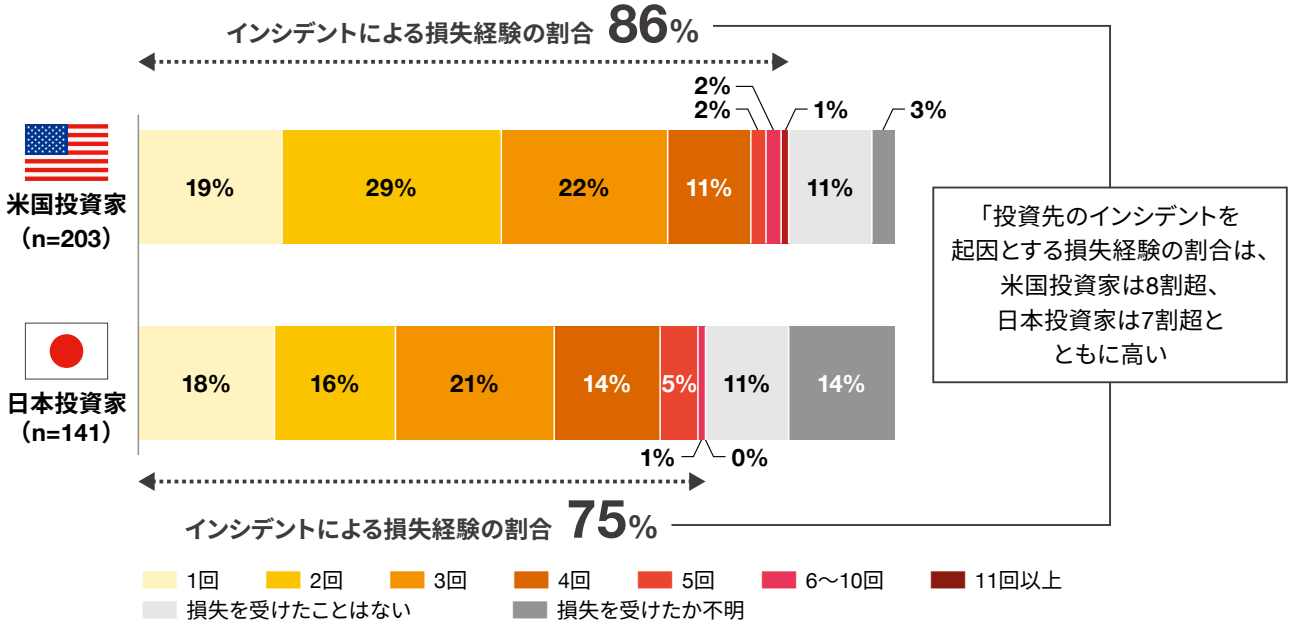
米国投資家の回答を見ると、「損失を受けた」とする割合は86%、「損失を受けたことがない」が11%、「損失を受けたか分からない」が3%となりました。

さらに損失を受けた回数を確認すると「1回だけ経験がある」米国投資家は全体の19%、「2回」は29%、「3回」は22%、「4回」は11%、「5回以上」は5%となり、複数回経験する割合が過半数を超えることが分かります。

日本投資家の回答を見ると、「損失を受けた」とする割合は75%、「損失を受けたことがない」が11%、「損失を受けたか分からない」が14%となり、日本投資家の方が米国投資家と比較して損失への影響を把握できていない割合がやや高くなっています。

さらに損失を受けた回数は「1回だけ経験がある」日本投資家は全体の18%、「2回」は16%、「3回」は21%、「4回」は14%、「5回以上」は6%となり、複数回経験する割合は、日本投資家においても過半数を超えることが分かります。

図表31：投資先企業におけるサイバーインシデントやリスクを起因とする損失経験の有無

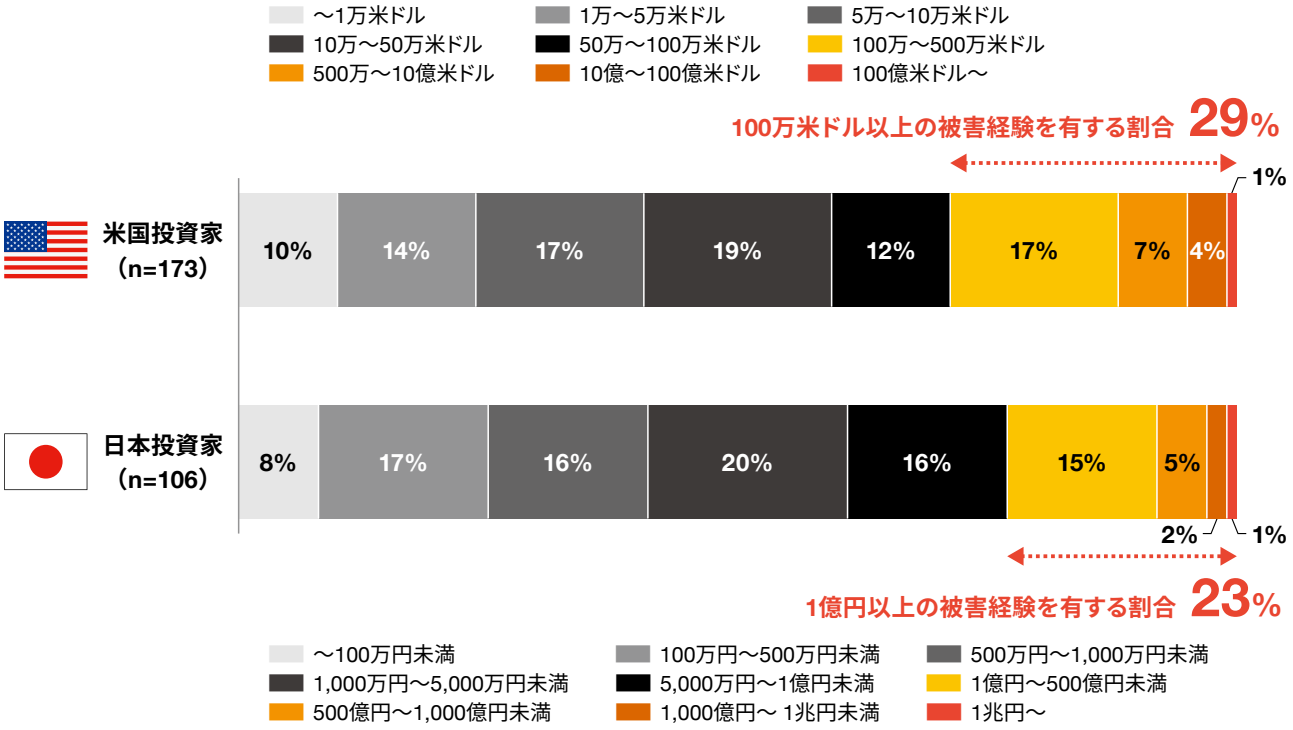


Q. 前問で損失を受けたと回答した方へ質問です。あなた、またはあなたが所属する組織が、投資先企業の「サイバーインシデントリスクやセキュリティ事故発生」を企業が適切に開示しなかったことにより損失を受けた回数を教えてください。最もあてはまるものを1つお知らせください。

投資先におけるインシデント起因の損失額

さらに損失経験があるとした米国投資家173名、日本投資家106名に「投資先におけるサイバーインシデントを起因とする損失額（複数経験した場合は最も被害が大きい1件）」について確認したところ、「100万米ドル以上の被害経験を有する」米国投資家は約3割、「1億円以上の被害経験を有する」とした日本投資家は2割超となりました（図表32）。

図表32：投資先におけるインシデント起因の損失額（最も被害が大きい1件）



Q. あなた、またはあなたが所属する組織は、投資先企業の「サイバーインシデントリスクやセキュリティ事故発生」を企業が適切に開示しなかったことにより、損失を受けた経験はありますか。受けたことがある場合は、発生から半年以内の損失額（含み損含む）として、最もあてはまるものを1つお知らせください。

Finding 12　米国投資家の「インシデント起因の売却・訴訟」経験の割合は、日本投資家より高い

日米投資家に「投資先企業の『サイバーリスクやインシデント発生』を理由とした、売却や訴訟の経験有無」を確認したところ、「経験がある」と回答した米国投資家の割合は売却・訴訟それぞれ約4割、日本投資家においてもそれぞれ約2割と、一定数存在することが明らかになりました（図表33）。

インシデントを起因とする「売却」経験

「投資先企業の『サイバーリスクやインシデント発生』を理由とした『売却』経験の有無」については、米国投資家では、「売却したことがある」が44%、「実際には売却していないが、売却を検討したことがある」が43%、「売却を検討したことはない」が13%となり、インシデントを起因とする「売却」経験・検討した経験を持つ米国投資家は合計で87%と高くなりました（図表33：左）。

続いて、日本投資家においては、「売却したことがある」が18%、「実際には売却していないが、売却を検討したことがある」が50%、「売却を検討したことはない」が32%と、米国投資家と比較して実際の売却経験は少ないものの、インシデントを起因とする売却の検討経験を持つ割合は米国投資家より高くなりました。

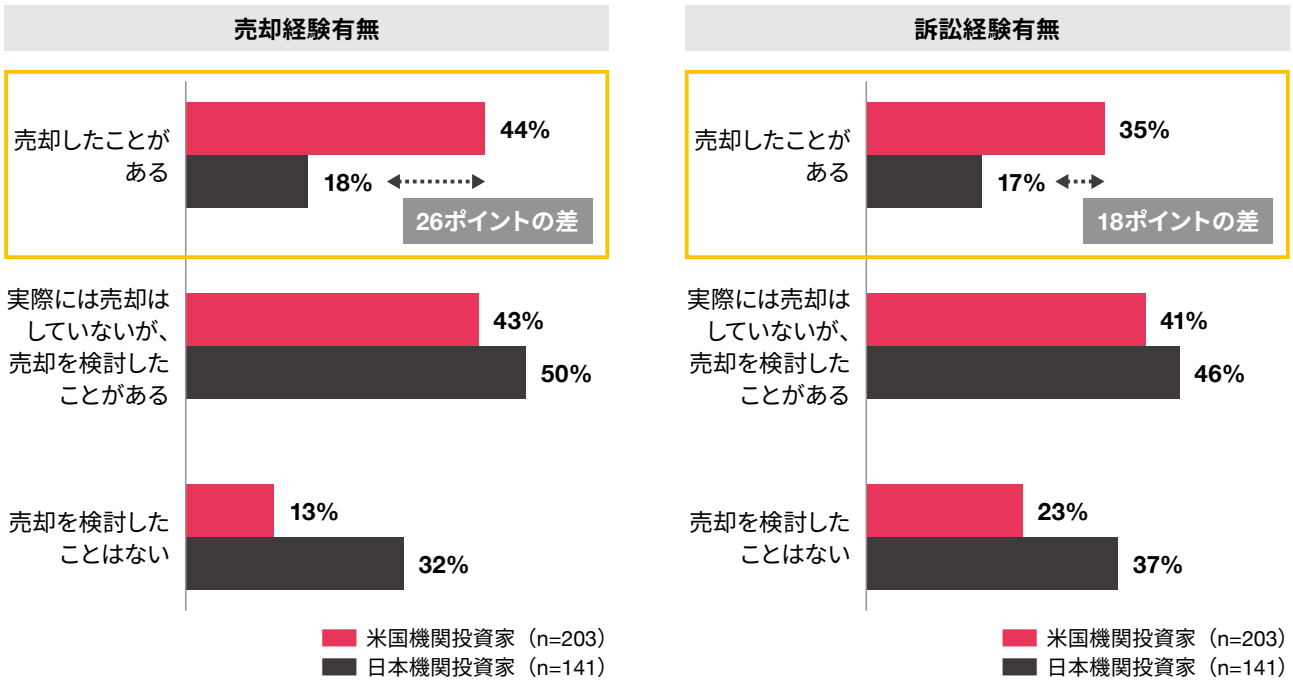
インシデントを起因とする「訴訟」経験

米国投資家では、「投資先企業の『サイバーリスクやインシデント発生』を理由とした『訴訟』経験の有無」について、「訴訟したことがある」が35%、「実際には訴訟していないが、訴訟を検討したことがある」が41%、「訴訟を検討したことはない」が23%と、インシデントを起因とする「訴訟」経験・検討した経験を持つ米国投資家は合計で76%と高くなりました（図表33：右）。

次に、日本投資家を見ると、「訴訟したことがある」が17%、「実際には訴訟していないが、訴訟を検討したことがある」が46%、「訴訟を検討したことはない」が37%と、インシデントを起因とする「訴訟」経験・検討した経験を持つ日本投資家は合計で63%と過半数を超えました。日本投資家においては、訴訟経験は少ないながら約2割と一定数存在しており、また、インシデントを起因とする訴訟を検討した経験を持つ割合は、米国投資家より高くなりました。

これらから、サイバーインシデント発生時には、米国投資家は日本投資家と比較して売却・訴訟する割合が高く、また日本投資家においても一定数の売却・訴訟経験者が存在することが分かりました。したがって、平時からサイバーインシデント発生を想定した、投資家との適切なコミュニケーションの在り方（情報開示・質問対応）について対応方針を検討しておく必要があると言えます。

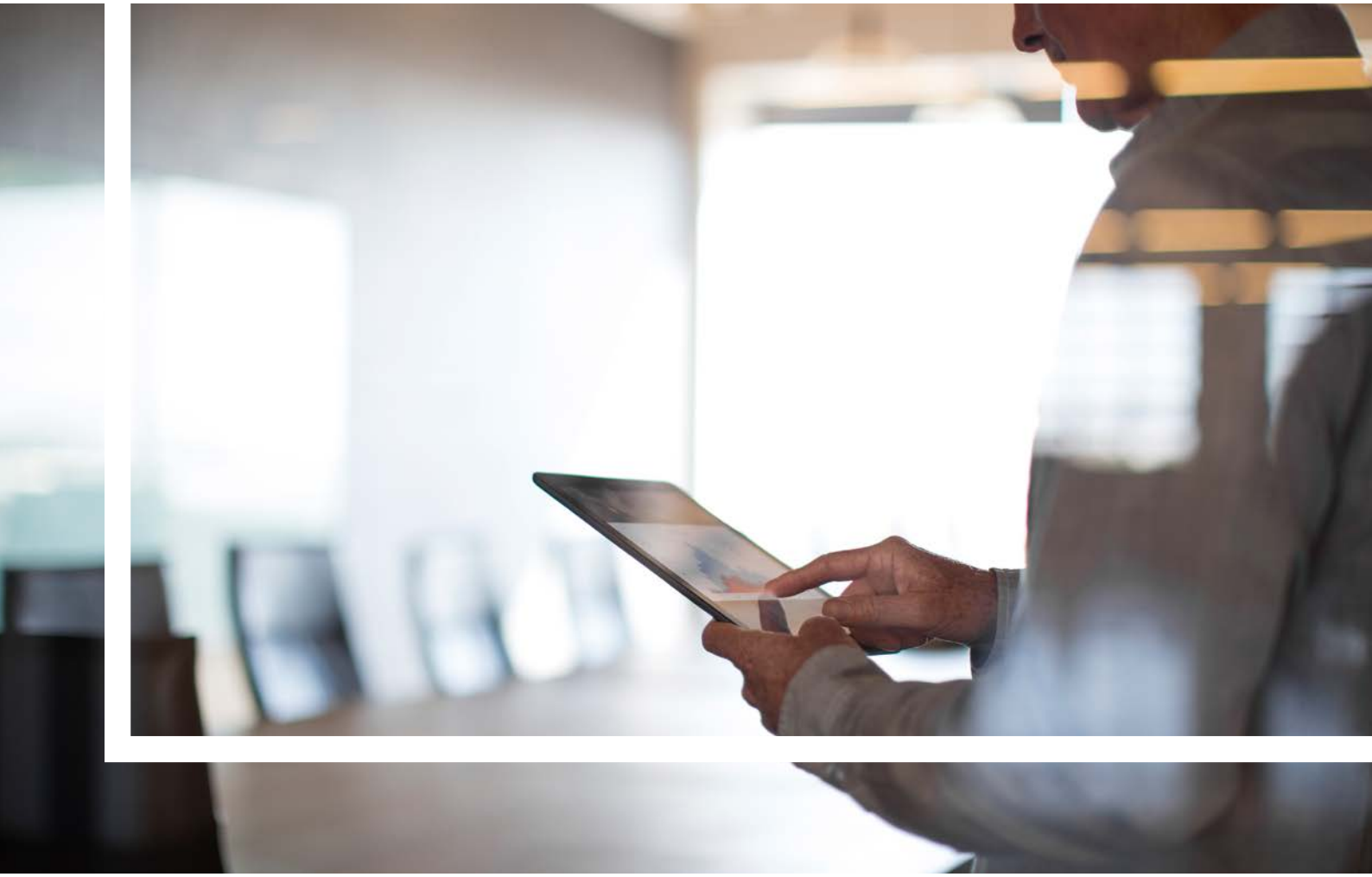
図表33：投資先企業のサイバーインシデントを起因とする、売却・訴訟の経験



Q. 以下それぞれの国の投資先企業は「サイバーセキュリティおよびプライバシーの取り組みやリスク、セキュリティ事故」について、あなた、またはあなたが所属する組織からの質問に十分に回答できていると思いますか。最もあてはまるものを1つお知らせください。

図表34：日米有識者インタビュー「サイバーインシデント発生による格付けへの影響」（参考）

外資系格付け機関	格下げについては、結局信用力を反映するものであるため「債務支払いの能力に影響するか」という点に集約される。例えば、売上の問題か、訴訟や和解金の費用負担か、または修復費用か。見通しの範囲でキャッシュフローと債務のバランスが崩れると判断した場合は、格下げになり得る。一方で、金銭的な損失が軽微、もしくはその他の収益源があって問題なければ格下げにはならない。 • **格下げされた事例** 事例として、情報漏えいによる訴訟・和解金、およびシステム・データ復旧により10億米ドル規模の損失が出て、格下げとなった米国企業があった。



3 日本企業への3つの推奨事項

本調査から、日米投資家におけるサイバーセキュリティに関する意識の実態として12の傾向を示しました。これらの傾向を受けて、米国株式市場に上場する日本企業や米国投資家と対話機会のある日本企業は、以下3点について見直されることを推奨いたします。

(1) 取締役会のサイバーセキュリティへの取り組み関与の在り方

投資先企業のサイバーセキュリティへの取り組みについて、最も多くの米国投資家が選択した評価対象は「取締役会の関与状況」であり、これが6割を占めました。このため私たちは、企業のサイバーセキュリティ責任者は以下の各ポイントを押さえる必要があると考えます。

1. 自社・子会社などにおける取締役会の「サイバーセキュリティへの取り組み関与状況」を把握する
2. 取締役会の関与が十分であると確認された場合は、投資家に対し適切に情報開示されているかを確認する
3. 定期的に、上記1.2.が適切に遂行されているかを確認する

Tips

インタビューでは、格付け機関・投資機関は以下への対応ができるとポジティブな評価を行う、としています。

- CISOは、サイバーセキュリティに関する業務経験・専門性があることが望ましく、当該経験がある場合はその旨を経歴に明記すること
- 取締役会でのCISOなどセキュリティ責任者に発言力および権限があり、当該責任者がセキュリティ施策に専念・遂行できるガバナンス体制を示すこと
- 投資家への取材に対し、原稿なしで回答ができること

(2) 投資家との対話：米国では「Form 8-K、Form 10-K」、日本では「有価証券報告書」で手厚く開示

投資先企業を評価する際に参照する情報源は、日米投資家で異なる傾向が明らかになりました。このため、「投資家との対話」としてサイバーセキュリティ情報開示を検討する際には、有事／平時によって、どこに情報を記載すべきかを併せて検討することが必要だと考えます（図表35）。さらに、日米有識者インタビューで共通して見られたように、企業の取り組みが実際に遵守・運用されているかを第三者評価などで示すことはポジティブな評価を得る上で重要な要素と言えます。

Tips

特に、日本投資家では「サイバーセキュリティ情報開示が十分でない」と評価する割合が半数と高く出ています。これは、既存の報告書において、海外と比較してリスクに関する情報量が少ないことが1つの要因となっている可能性があるため、量の点でも見直しが必要だと考えます。

図表35：「対話」の対象に合わせた情報開示場所の選択

「対話」の対象	用途	主な情報開示場所
米国投資家	平時	Form 8-K、Form 6-K
	有事	Form 10-K、Form 10-Q、Form 20-F
日本投資家	平時	有価証券報告書、統合報告書など
	有事	内部統制報告書

(3) 訴訟リスクを考慮した対応

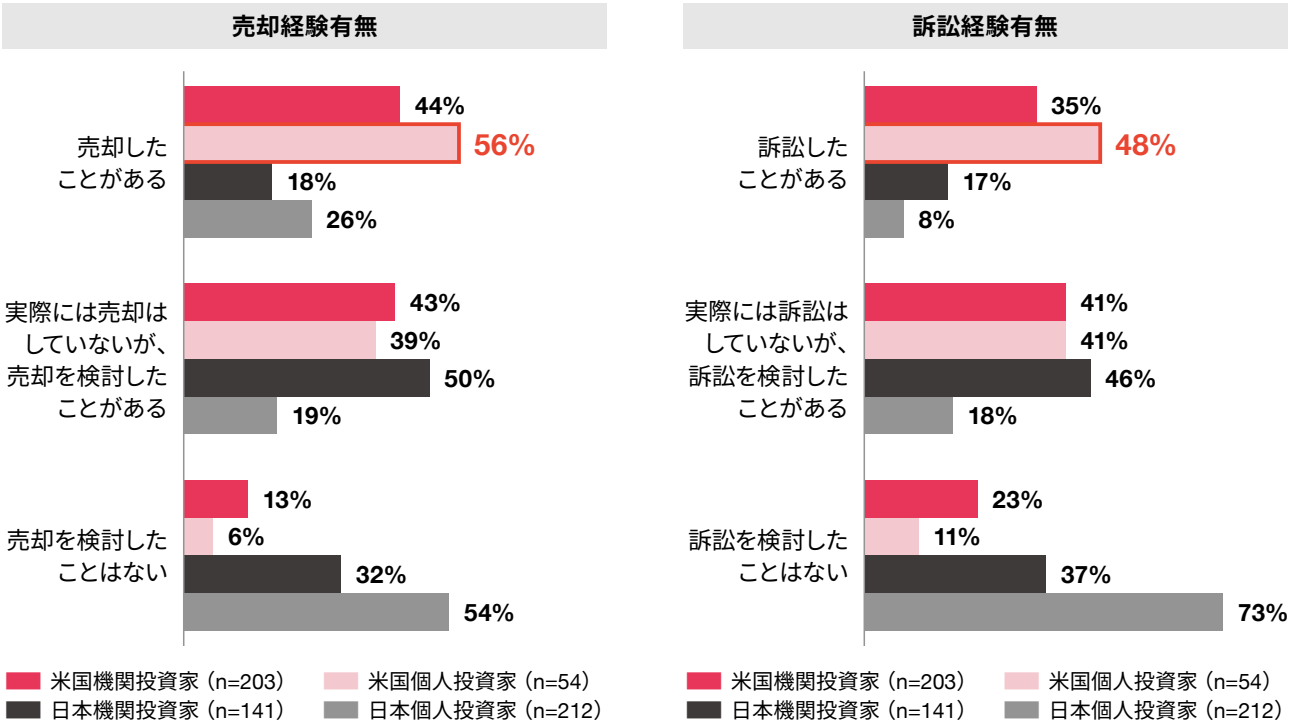
また、米国投資家は、日本投資家よりも、インシデントを起因とする売却・訴訟の可能性が高いことが、改めてデータで示されました。

さらに、インシデントの情報開示が不適切だった場合はSECが告訴するケースもあることから、インシデント発生時には真摯に情報開示・報告を実施しなければなりません。

Tips

図表36に記載するとおり、米国個人投資家グループは米国機関投資家よりも訴訟経験の割合が高く約5割を占めるというデータも確認できていることから、米国市場の上場企業は、平時より適切な情報開示を行うとともに、訴訟された際にどのように対応すべきかも併せて検討しておくと良いと考えます。

図表36：投資先企業のサイバーインシデントを起因とする、売却・訴訟の経験（日米機関投資家および日米個人投資家比較）



以上、3つの観点から自社の対応を見直すことで、企業のサイバーセキュリティ情報開示は、日米投資家からポジティブな評価を受けることができると私たちは考えます。

調査概要

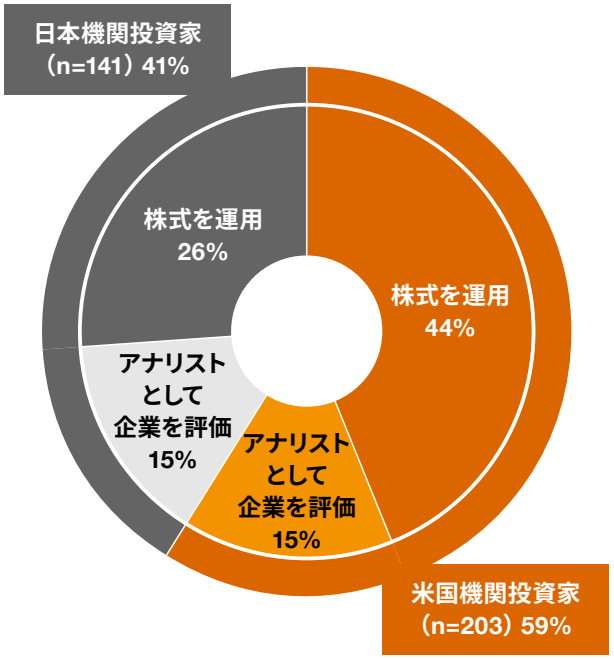
調査名	「サイバーセキュリティおよびプライバシー情報開示」に関する日米投資家の意識調査2024
調査対象	米国および日本における以下業務従事者 • 機関投資家として、仕事で株式を運用する者 • 機関投資家でアナリストとして企業のセキュリティ関連情報を分析・評価する者
調査方法	インターネットによるアンケート調査および有識者へのインタビュー調査
調査期間	アンケート調査　：2023年10月12日～ 10月25日 インタビュー調査：2023年11月～ 2024年3月
回答者数	アンケート調査　：344名（米国投資家203名、日本投資家141名） インタビュー調査：6名（日本投資家、米国投資家、外資系格付け機関など）
分析	PwCコンサルティング合同会社
データ提供	一般社団法人日本IT団体連盟

回答者の属性

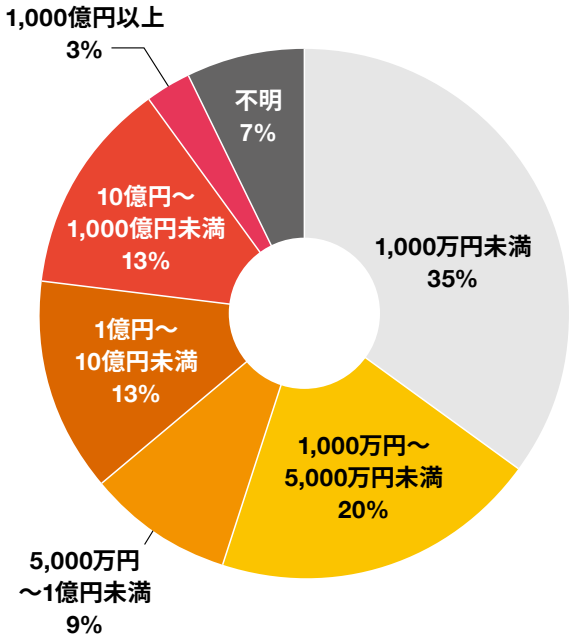
今回のアンケート調査では、日本投資家141名および米国投資家203名、計344名から回答が得られています。ここでいう投資家とは「機関投資家として、仕事で株式を運用する者」「機関投資家でアナリストとして企業のセキュリティ関連情報※を分析・評価する者」が対象となっています（図表37）。また、回答者について、投資規模（図表38）、最も多く投資する業界（図表39）、日本株式保有有無および日本株式への投資割合（図表40）、主な勤務地（図表41・42）は以下のとおりです。

図表37：回答者の属性（日米投資家）

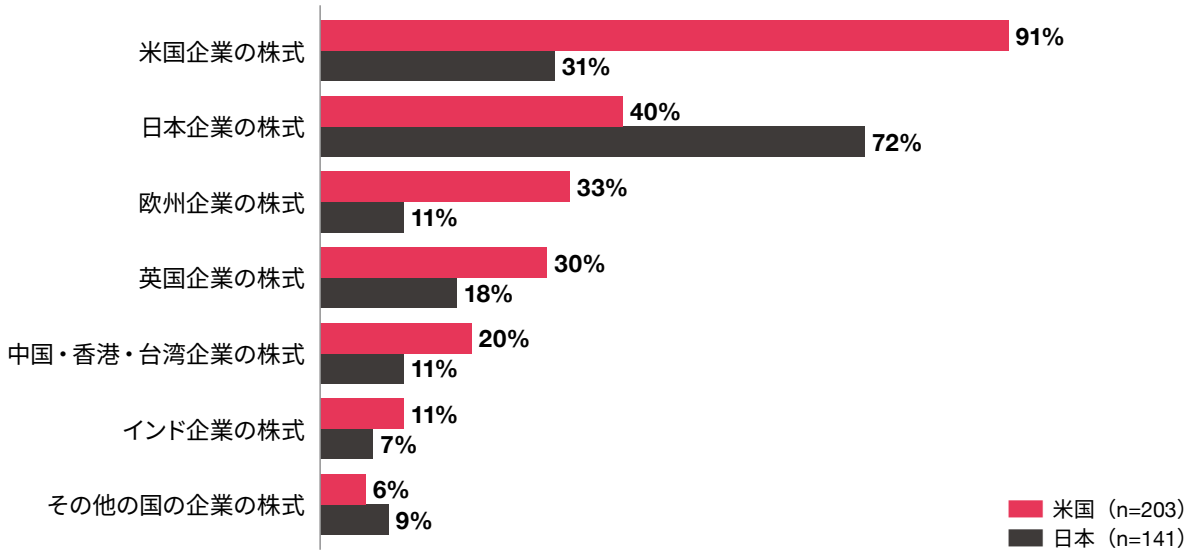
日米投資家の属性（n=344） 単一回答



投資規模（n=344） 単一回答

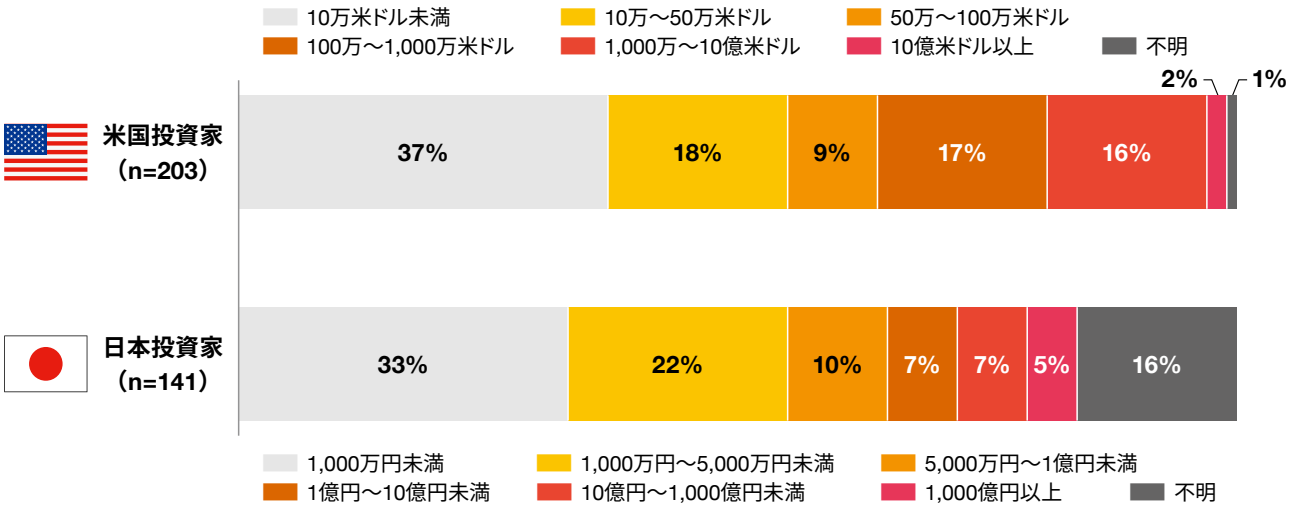


保有株の属性（n=344） 複数回答

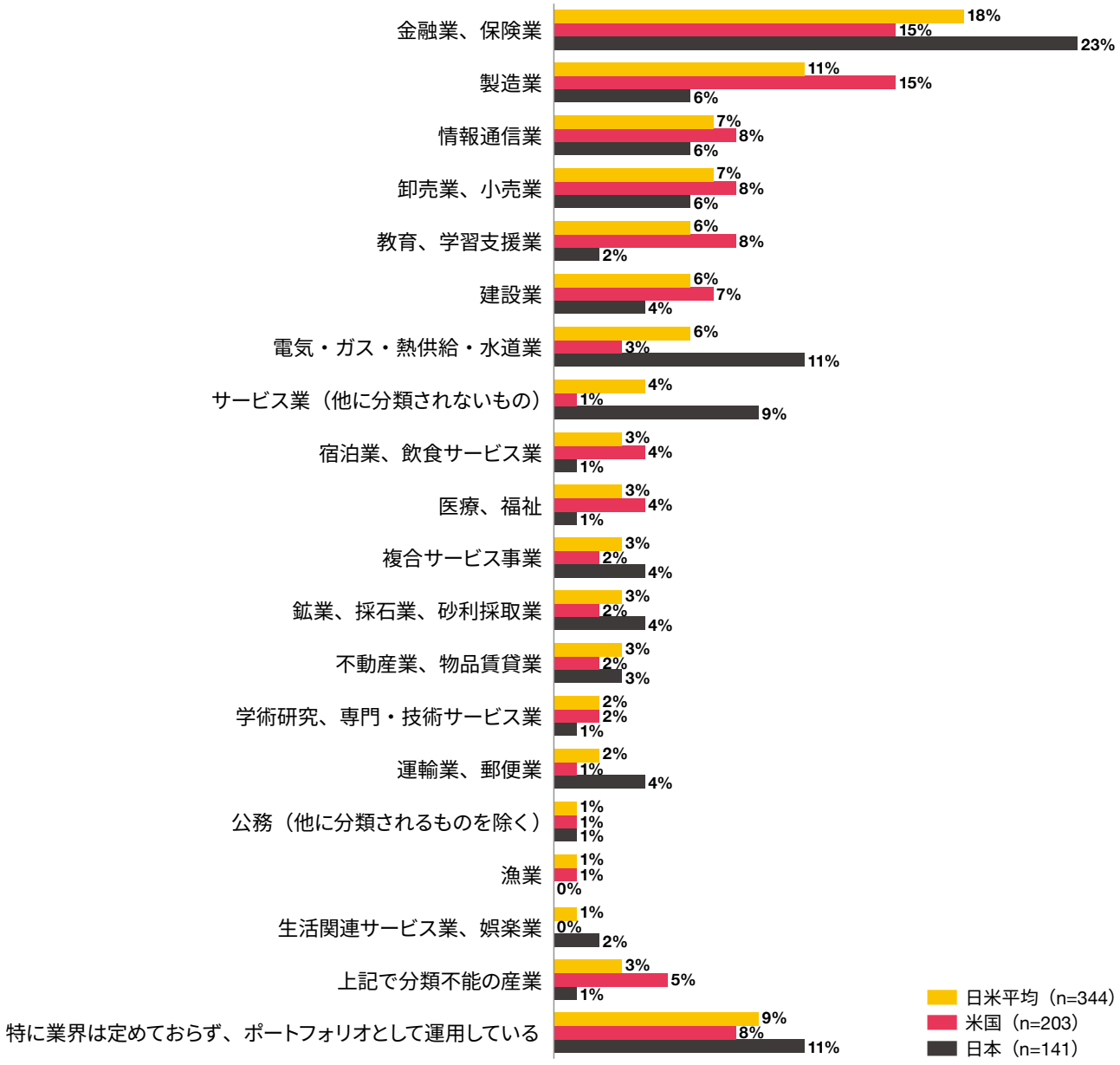


本調査では、「①機関投資家として、仕事で株式を運用する者」「②機関投資家でアナリストとして企業を分析・評価する者」を調査対象としています。
本レポートでは、それぞれの国において①②のグループでは有意な差が見られなかったため、1つのグループ「機関投資家」として分析結果をまとめています。

図表38：回答者の属性（投資規模）

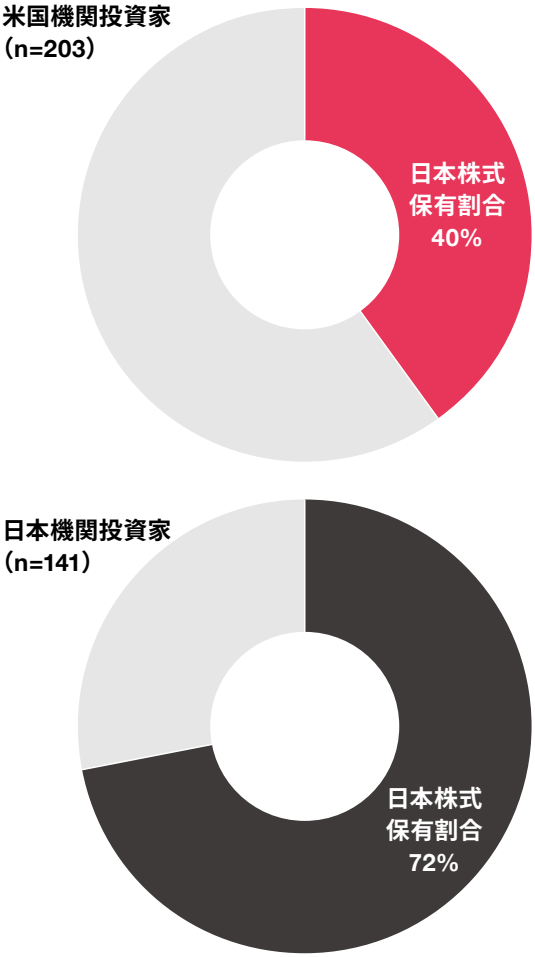


図表39：回答者の属性（最も多く投資する業界）

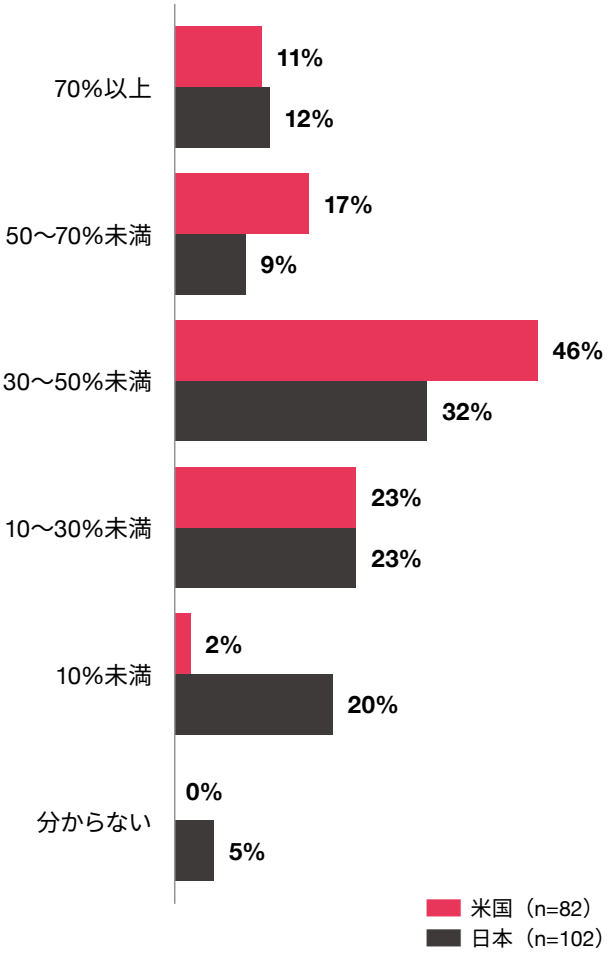


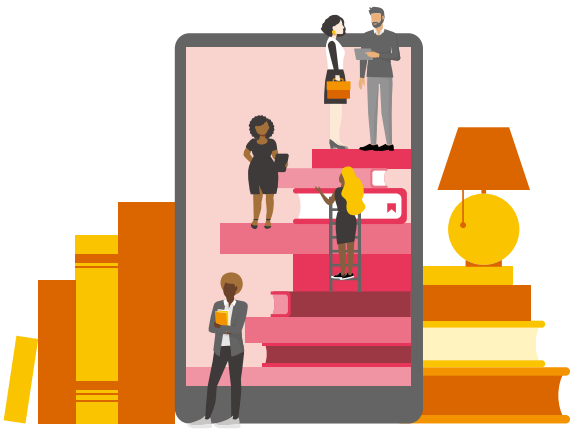
図表40：回答者の属性（日本株式保有有無および日本株式への投資割合）

日本株式保有の有無（n=344）

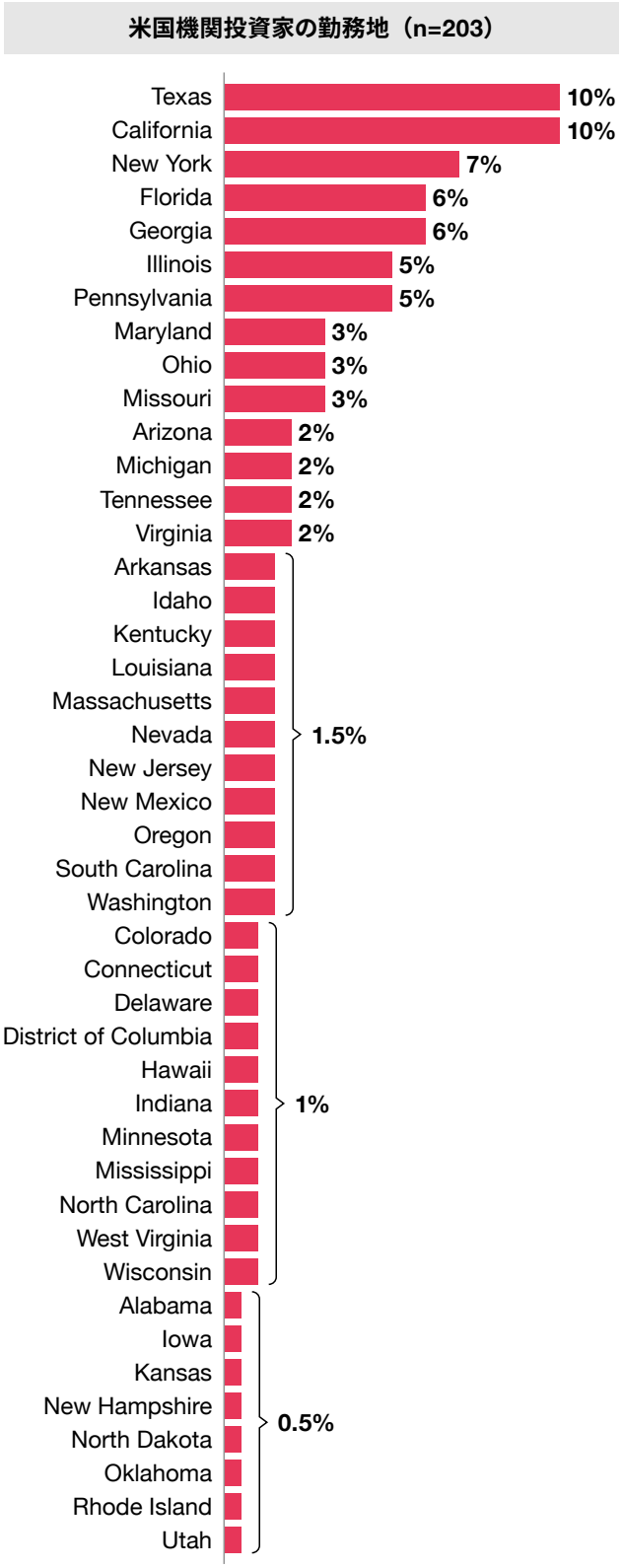


日本株式保有する機関投資家における日本株式への投資割合（n=184）

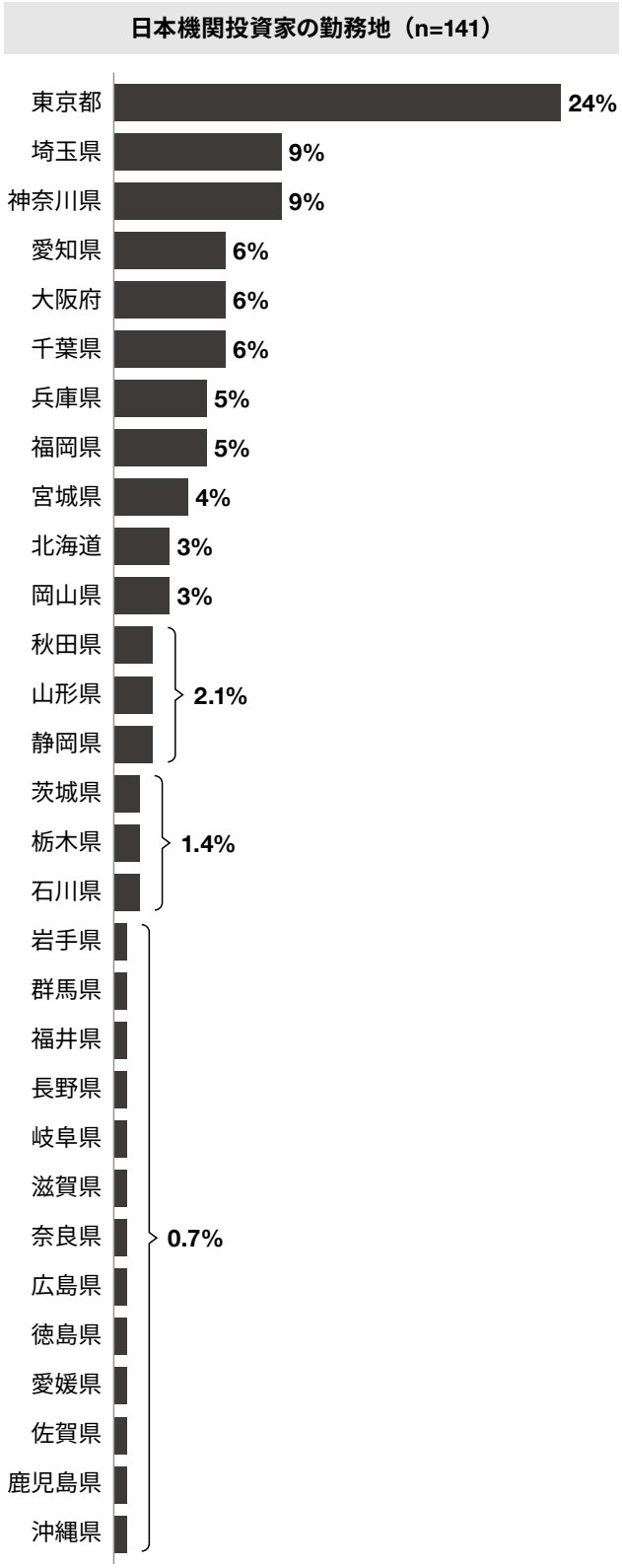




図表41：回答者の属性（主な勤務地：米国）



図表42：回答者の属性（主な勤務地：日本）



執筆者

丸山 満彦
PwCコンサルティング合同会社
パートナー

上杉 謙二
PwCコンサルティング合同会社
ディレクター

愛甲 日路親
PwCコンサルティング合同会社
マネージャー

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約11,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界151カ国に及ぶグローバルネットワークに約364,000人のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。

発刊年月：2024年4月　　管理番号：I202401-22