米国投資家は「投資先企業のサイバーセキュリティ開示情報」の何を評価しているのか

PwC コンサルティング合同会社 マネージャー
愛甲　日路親

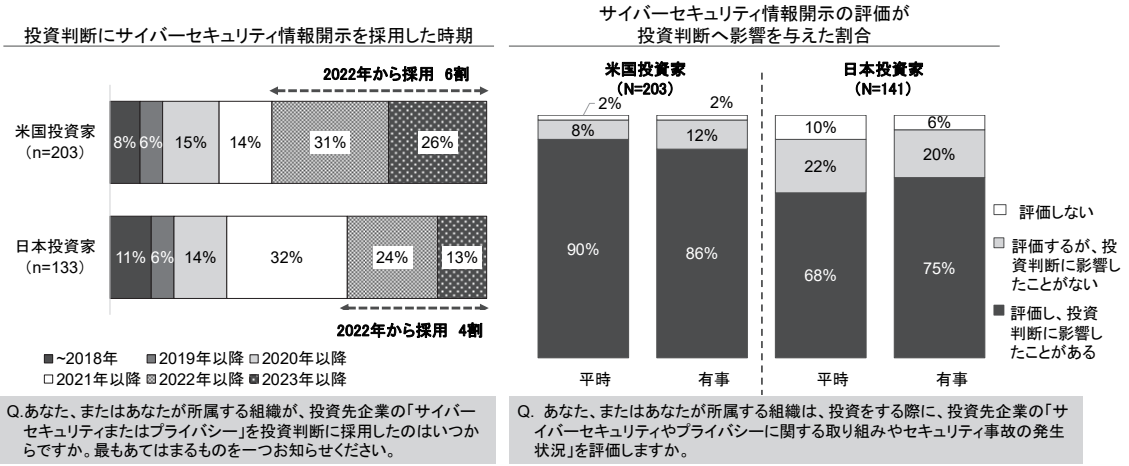
▌要　約▐

1. 今日、投資先企業におけるサイバーリスク懸念が高まり、米国証券取引委員会（SEC）をはじめ海外では上場企業において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開示の法規制強化が進んでいる。一方、企業のサイバーセキュリティ管理体制を適切に評価することは難しい。PwC コンサルティング合同会社では、世界的にサイバーセキュリティ業界を牽引する米国の投資家が企業のどのようなサイバーセキュリティ開示情報を評価するかを把握すべく、アンケート調査を実施した。米国投資家 203 名（および日本投資家 123 名）から回答が得られ、有識者 6 名のインタビュー調査も踏まえ、日米投資家間で意識や着眼点が異なることが明らかになった。
2. 本アンケート調査では、米国投資家全体の 9 割がサイバーセキュリティ評価は投資判断に影響すると回答したが、日本投資家の割合（同 6 割）よりも高い背景として、規制強化と損失顕在化があることが読みとれる。米国投資家の多くは、米国 SEC がサイバーセキュリティ情報開示を義務化した 2022 年からサイバーセキュリティ評価を採用している。そして、直近半年間に投資先企業のサイバーリスクやセキュリティ事故の情報開示不備による損失経験を有する米国投資家は全体の 9 割に上り、うち 3 割は 100 万米ドル（約 1.6 億円）を超える損失を経験するなど、無視できない状況と言える。
3. 米国投資家が最も重視する企業のサイバーセキュリティ評価項目は、取締役会の関与状況で全体の約 6 割（日本投資家は同約 3 割）、また平時において最も確認するとした情報源は「Form 8-K、6-K」が同約 5 割（日本投資家は同約 2 割）と、評価材料が日本投資家と必ずしも共通していないことが読みとれる。また、米国投資家の場合、チームにセキュリティ有識者がいる割合は全体の約 6 割（外部有識者を含むと約 9 割）に対して、日本投資家の場合、残念ながら同 1 割（外部有識者を含むと同 5 割）にとどまり、日本は適切な評価のための体制が整っていないという実態が浮き彫りとなった。
4. 今後、特にサステナビリティ投資家においては、サイバーセキュリティ評価を投資判断に反映させなければならないことは明らかである。セキュリティ情報開示が義務化されていない国内上場企業の開示情報や取材を基に浮き彫りとなった課題は、セキュリティ有識者が不在のチームで「企業のセキュリティ取組を適切に評価できるか」という点である。近い将来、日本投資家においてもサイバーセキュリティ評価の力量の強化およびセキュリティ評価者の力量の標準化は重要な検討事項となるだろう。

Ⅰ　なぜ投資先企業のセキュリティ情報開示を評価しなければならないのか

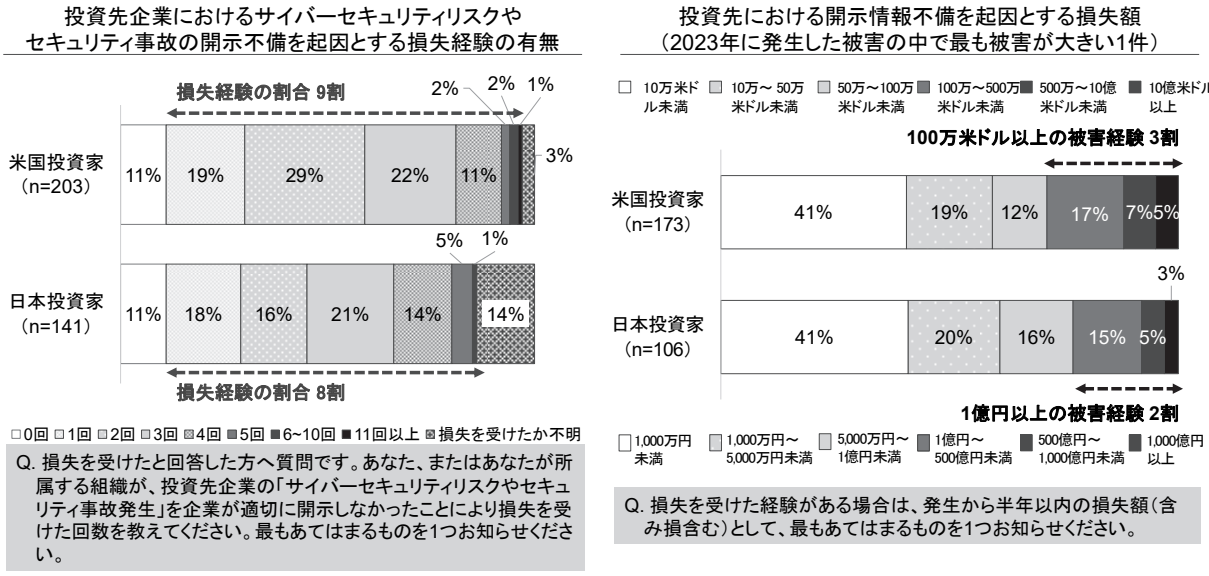
今日、米国証券取引委員会（SEC）などを筆頭に、サイバーセキュリティに関する管理体制やリスクなど投資家との対話のため情報開示義務化に関する法規制の強化が進んでいる。そして、投資先企業のセキュリティ事故や開示不備による投資家の損失・訴訟顕在化といった背景も踏まえ、米国投資家や格付会社では投資先企業のセキュリティ評価を投資判断の一つとして採用する傾向が高まっている。実際に、後述する PwC コンサルティング合同会社が 2024 年 4 月に公開したアンケート調査では、米国投資家の 6 割が、SEC の新しいサイバーセキュリティ情報開示規則案が公表された 2022 年から投資判断の一つとして評価を採用したとしており、投資先企業のサイバーセキュリティ取組の評価が投資判断へ影響を与えた割合に至っては 9 割に上る（図表 1）。また、アンケート調査実施の直近半年間（2023 年 4〜9 月）において、米国投資家全体の 9 割が投資先企業のセキュリティ事故やリスクの開示不備を起因とした損失を経験しており、1 件当たりの被害総額が 100 万米ドル（約 1.6 億円）を超えると回答した者は全体の 3 割も占める。日本投資家においても同じ傾向が確認できており、約 8 割が損失経験を有し、うち 2 割が 1 億円を超える損失を経験していることが明らかになった（図表 2）。

図表 1　「サイバーセキュリティ情報開示の評価」を投資判断に採用した時期、および投資判断へ影響を与えた割合



（出所）PwC コンサルティング合同会社「『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」2024 年 4 月 21 日より PwC 作成

図表 2　投資先企業におけるサイバーセキュリティリスクやセキュリティ事故の情報開示不備による損失経験数、1 件当たりの被害総額



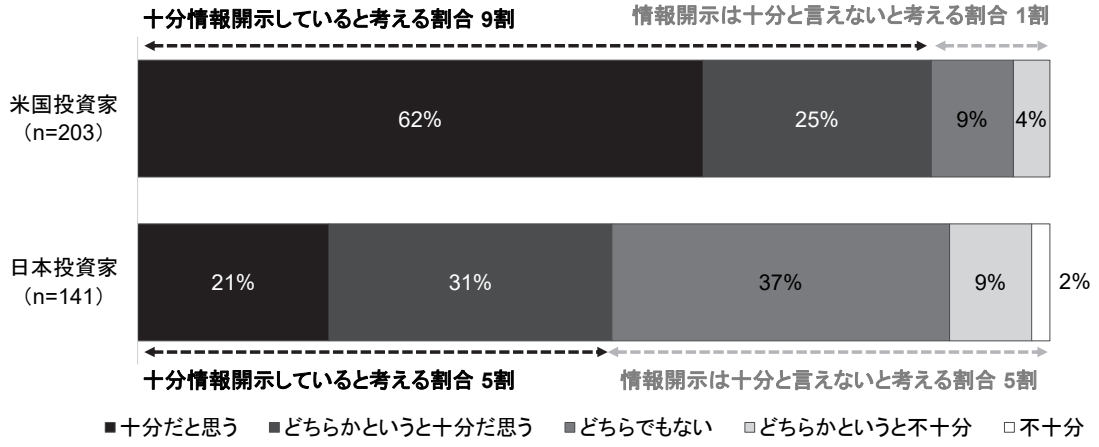
（出所）PwC コンサルティング合同会社「『サイバーセキュリティおよびプライバシー情報開示』に関する日米投資家の意識調査 2024」2024 年 4 月 21 日より PwC 作成

これらのことから、投資先企業におけるサイバーセキュリティの取り組みを適切に評価することは、全ての業界がサイバーの恩恵を受けると同時にセキュリティ事故によるビジネスリスクの可能性も拡大する状況を踏まえると、日本投資家にとっても、今後ますます重要になると想定される。

一方で、米国では情報開示の規制強化により上場企業のサイバーセキュリティに関する開示情報が十分に行われるのに対し、日本では情報開示が義務化されていないこともあり、半数に上る日本投資家が「企業の開示情報は不十分」と回答している（図表 3）。日本投資家は少ない開示情報から企業のサイバーセキュリティの取り組みを読みとり、評価しなければならない。このような環境下での適切な評価は正直なところ難しいと言わざるを得ず、課題と考えられる。

次章より、当該課題に対し、日本投資家が参照できるよう、米国投資家が何を評価しているか、アンケート調査結果に基づき概観する。

図表 3 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係る情報開示が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。

（出所）PwC コンサルティング合同会社「『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」2024 年 4 月 21 日より PwC 作成

Ⅱ 米国投資家は、企業との対話において何を確認しているのか

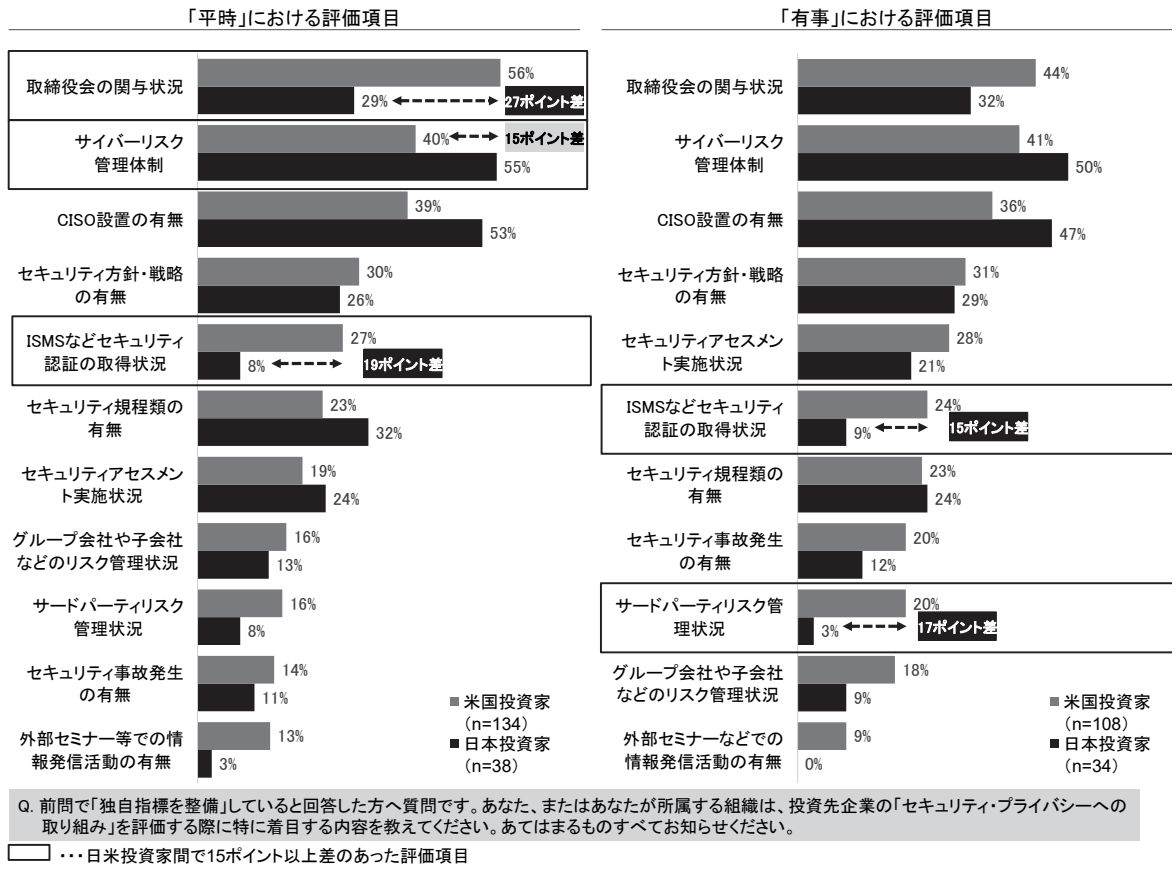
具体的に、米国投資家は投資先企業の開示情報や取材において何を評価しているのか。PwC では、企業のサイバーセキュリティ評価に関して、日米投資家が投資先企業のサイバーセキュリティおよびプライバシー情報開示に関する日米投資家の着目点を明らかにすることを目的にアンケート調査およびインタビュー調査を実施した。同アンケート調査では、米国機関投資家およびアナリスト 203 名、日本機関投資家 141 名、計 344 名から回答を得られた。また、日米投資家や格付会社など有識者 6 名のインタビュー調査も行い、日米投資家間で意識や着眼点が異なることが明らかになった。

１．米国投資家が最も評価するのは「取締役会の関与状況」

アンケート調査では、米国投資家（n=203）全体の 7 割が投資先企業のサイバーセキュリティ情報開示評価の「独自指標」を持ち、他 3 割は外部の指標等を参照すると回答した。なお、日本投資家（n=141）の「独自指標」を持つ割合は全体の 3 割未満と、米国投資家の傾向と乖離がみられる。

当該独自指標を持つと回答した米国投資家（n=134）に対し、投資先企業の評価項目を確認したところ、「取締役会の関与状況」が最も回答の割合が多く 56%、次いで「サイバーリスク管理体制」が 40%、「最高情報セキュリティ責任者（CISO）設置の有無」が 39%、「セキュリティ方針・戦略の有無」が 30%、「情報セキュリティマネジメントシステム（ISMS）などセキュリティ認証の取得状況」が 27%の順に高い（図表 4）。独自

図表 4　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（日米投資家比較）



（出所）PwC コンサルティング合同会社「『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」2024 年 4 月 21 日より PwC 作成

指標を持つ日米投資家（n=38）を比較すると最も差が現れたのは「取締役会の関与状況」29%で、米国投資家と比較し 27%ポイントも低く、必ずしも重要視されていないことが分かる。

有識者インタビューでは、全ての有識者が企業のセキュリティに関するガバナンスを重要視しており、特に（1）取締役におけるセキュリティ知見者の有無、（2）取締役会の関与・報告体制の有無、（3）CISO などセキュリティ責任者名および関連する実務経験の公表を挙げていた。外資系格付会社の有識者からは特に注視する点として「セキュリティ責任者が取締役会で権限や発言力を有するか」を挙げ、影響力のある他の役員がセキュリティ施策遂行を妨げるような体制であればネガティブ評価とするとの見解が示された。

この他、特筆したい点として「ISMS などセキュリティ認証の取得状況」を評価するかについても、米国投資家（27%）と比較して日本投資家は 8%と、19%ポイントの乖離が見られた。有識者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一方、公開情報や取材などからは実態が伴うかまでは確信が持てない。このため、ISMS 認証などの第三者機関の認証を評価対象にする」というコメ

ントが得られた。また、「投資先企業においてセキュリティ事故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浸透していなかったことが明らかになることがある」ため、「企業の過去のセキュリティ事故を必ず確認する」といった声も複数聞かれた。

さらに、有事の評価項目においては「サードパーティリスク管理状況」も日米投資家間で 17%ポイントの乖離が見られた。有識者インタビューにおいても、海外投資家は、昨今のセキュリティ事故がサプライチェーンやサードパーティに起因して生じていることから取り組み状況を評価するとの回答が得られた。日本企業は世界的にサプライチェーンが長い企業も多く、近年、事業継続に大きな影響を与えるサプライチェーンを起因とするセキュリティ事故が顕在化している。これを踏まえると、サプライチェーンリスクマネジメントの一環にセキュリティ対策項目が含まれているかを確認する必要があると言える。

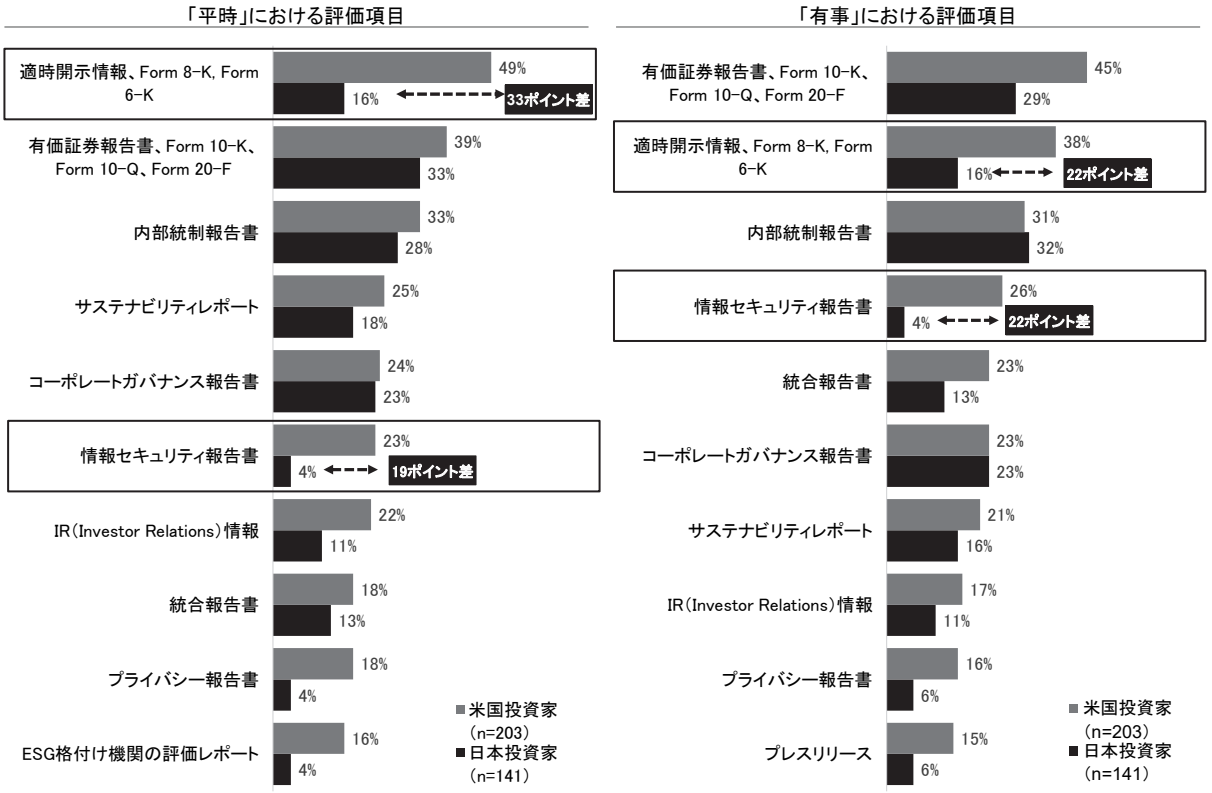
２．評価対象として最も参照する情報源は Form 8-K

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全体の約半数（49%）は「適時開示情報、Form 8-K、Form 6-K」と回答した。これは日本投資家よりも 33%ポイントも高く、特徴的といえる（図表 5）。前述の有識者インタビューでも明らかになったとおり、米国投資家は企業の実態を把握するため、（1）過去のセキュリティ事故での再発防止策から、それらが今どのように継続・強化されているか、（2）取締役会においてリスク認識はどの程度かを図るために、過去の企業のセキュリティ事故にどのように対応してきたか、を必要な情報源としていることが示唆された。

米国投資家が評価対象として参照する情報源は、回答が最も多かった Form 8-K 等に次いで「有価証券報告書、Form 10-K、Form 10-Q、Form 20-F」が全体の 39%、「内部統制報告書」が同 33%、「サステナビリティレポート」が同 25%、「コーポレートガバナンス報告書」が同 24%となった。一方、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%の順となった。

この他、有識者インタビューでは、セキュリティ事故などの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とのコメントが得られた。すなわち、業界専門誌、メディアにて投資先企業を定期的に確認することは有効な手段と言える。

図表 5　サイバーセキュリティ開示情報の情報源（米国投資家の上位 10 項目）



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、どこで確認しますか。あてはまるものすべてお知らせください。／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

□ ・・・日米投資家間で15ポイント以上差のあった評価項目

（出所）PwC コンサルティング合同会社「『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」2024 年 4 月 21 日より PwC 作成

3．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、うち過半数が事前に質問項目を準備

1）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いことが分かった（図表 6 左）。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）」が同 69%、「年に 3 回以上質問する（4 カ月ごと）」が同 41%、「年に 4 回以上質問する（四半期ごと）」が同 28%となった。

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）」が同 72%、「年に 3 回以上質問する（4 カ月ごと）」が同 41%、「年に 4 回以上質問する（四半期ごと）」同 19%となった。すなわち、質問頻度については日米投資家間において、有意な差は確認できなかった。

２）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、米国投資家では全体の過半数を占め、日本投資家（同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った（図表 6 右）。

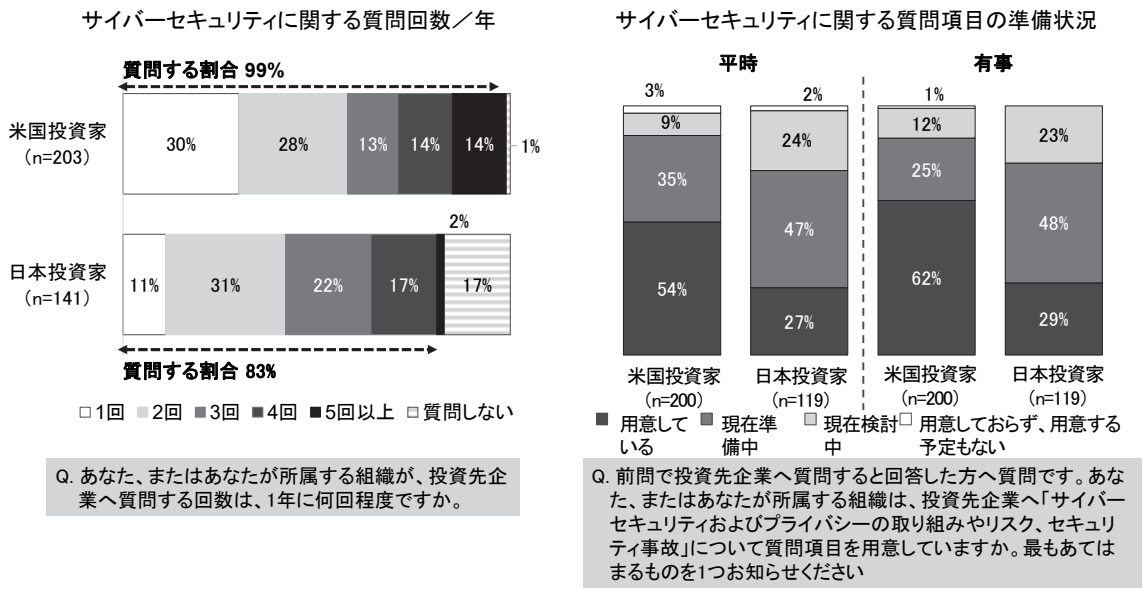
（１）平時における投資先へのサイバーセキュリティ関連質問項目の準備状況

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」が同 35%、「現在検討中」が同 9%、「用意しておらず、用意する予定もない」は同 3%となった。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」が同 47%、「現在検討中」が同 24%、「用意しておらず、用意する予定もない」は同 2%となった。

（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」が同 25%、「現在検討中」が同 12%、「用意しておらず、用意する予定もない」は同 1%となった。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

図表 6　サイバーセキュリティに関する質問回数、質問項目の準備状況



（出所）PwC コンサルティング合同会社「『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」2024 年 4 月 21 日より PwC 作成

備中である」が同 48%、「現在検討中」が同 23%となった。なお、「用意しておらず、用意する予定もない」との回答は 0%だった。

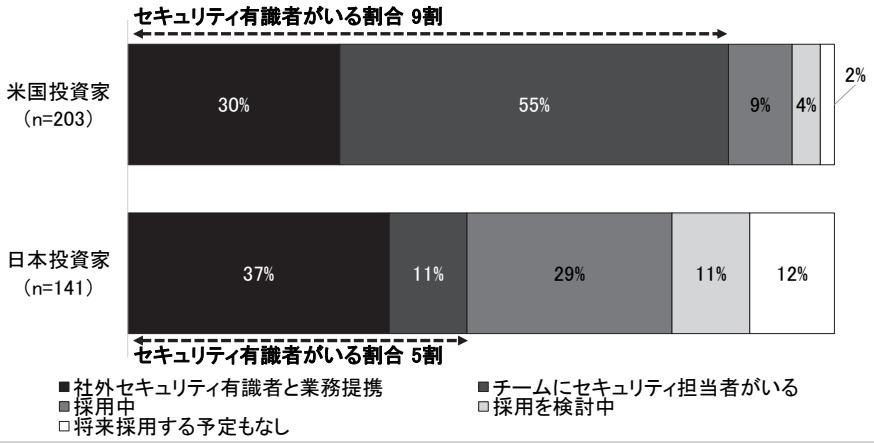
米国投資家はサイバーセキュリティ関連の質問項目を準備しており、特に有事において準備状況の割合が高い傾向にあることが明らかになった。日本投資家においては、準備済みの割合は全体の約 3 割と低いものの、「現在準備中」である割合が同約半数を占めている。これらのことから、今後、国内においても、投資家と企業において、サイバーセキュリティ関連の対話が進む可能性があると考えられる。

4．米国投資家は「チームにセキュリティ有識者がいる」が半数超え、日本投資家は 1 割にとどまる

日米投資家に「投資先企業へのヒアリング実施にあたり、チームにサイバーセキュリティまたはプライバシーの有識者（以下、セキュリティ有識者）がいるか」と確認したところ、米国投資家全体の過半数が「チームにセキュリティ有識者がいる」としており、日本投資家（同 11%）と比較して 44%ポイントも高いことが明らかになった（図表 7）。

具体的に見ると、米国投資家では、「チームにセキュリティ有識者がいる」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」は同 30%となり、セキュリティ有識者がいるとする割合が同 85%と高いことが分かる（図表 7 上）。さらにチームにセキュリティ有識者が不在とする米国投資家（同 15%）においても、「現在採用中である」が同 9%、「採用を検討中である」が同 4%と、体制を強化する傾向にあることが見込まれる。

図表 7　ヒアリング実施にあたり、チームに「セキュリティ有識者」がいる割合



外資系格付け機関へのインタビュー結果

技術的な専門知識がなければ「投資家」も理解できない

例えばアニュアルレポートなどの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、一般投資家などです。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ります。

一方、分かりやすい内容は横比較しづらくなります。

（出所）PwC コンサルティング合同会社「『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」2024 年 4 月 21 日より PwC 作成

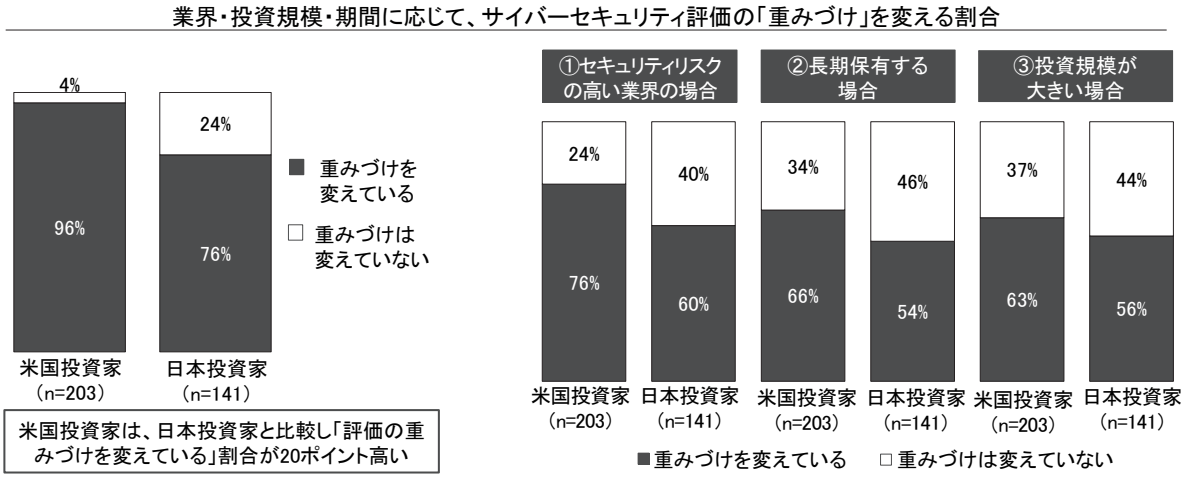
次に、日本投資家を見ると、「チームにセキュリティ有識者がいる」とする割合は全体の 11%、「社外セキュリティ有識者と業務提携している」は同 37%であり、セキュリティ有識者がいるとする割合が 48%と半数に留まる（図表 7 下）。一方、チームにセキュリティ有識者が不在とする日本投資家（同 52%）においては「現在採用中である」とする割合が同 29%、「採用を検討中である」が同 11%となっており、数字を読みとると今後、日本投資家においても、セキュリティに関する専門的な評価体制が整備されることが見込まれる。

５．米国投資家の投資状況による評価の重みづけとリスクの高いと評価される業界

１）投資状況に応じて評価の重みづけ

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全体の 9 割超、日本投資家は同約 8 割と日米投資家ともに高くなった（図表 8）。とりわけ、「セキュリティリスクの高い業界」に応じて最も重みづけを変えるとした米国投資家は 76%「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は 66%、「投資規模」においては、「100 万米ドル以上」とする割合は半数程度存在し、これらの傾向は日本投資家にもみられた。

図表 8　投資状況に応じて、評価の重みづけを変える割合



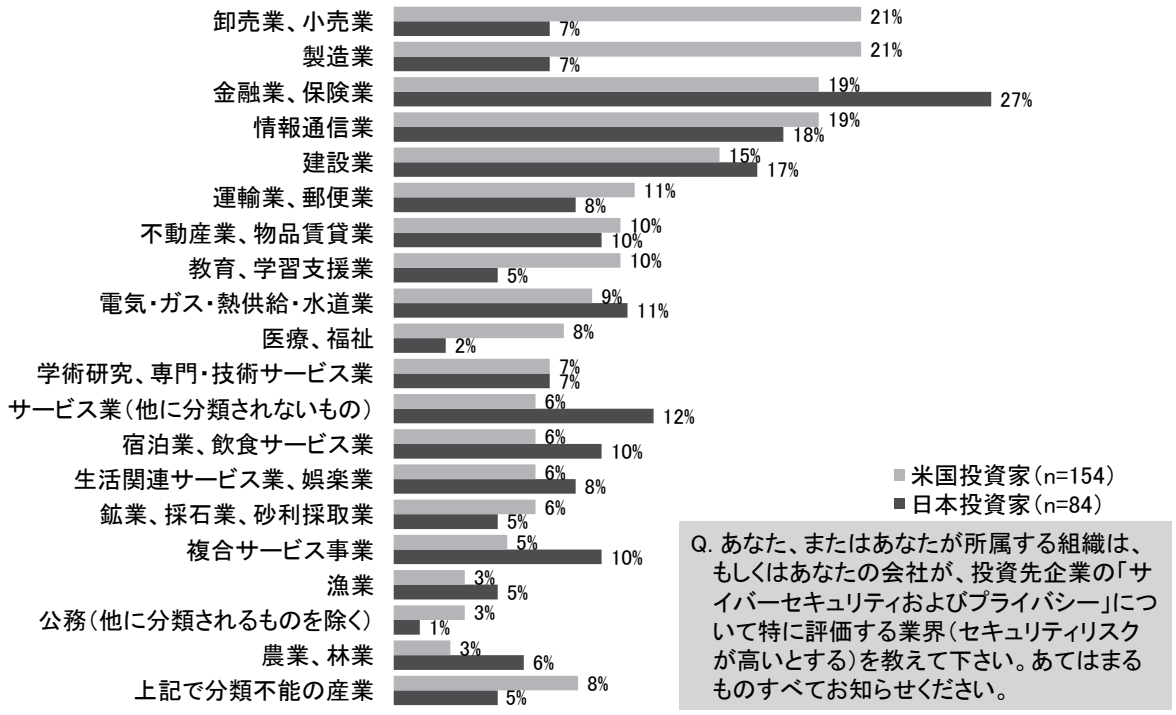
（出所）PwC コンサルティング合同会社「『サイバーセキュリティおよびプライバシー情報開示』に関する日米投資家の意識調査 2024」2024 年 4 月 21 日より PwC 作成

2）米国投資家が考えるセキュリティリスクの高い業界

「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（n=154）においては、「卸売業、小売業」「製造業」が最も高く（ともに全体の 21%）、次いで「金融業、保険業」「情報通信業」がともに同 19%、「建設業」が同 15%の順となった（図表 9）。一方、日本投資家（n=84）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%の順となった。

有識者インタビュー調査においては、セキュリティリスクが高い業界として、ほぼ全有識者が情報通信・テクノロジー業界、金融業界を挙げた。加えて、業界に限らず個人情報取り扱い事業者、クレジットカード決済事業者、またベンチャー企業もセキュリティリスクが高いため、M&A などでこのような企業買収を進める上場企業を厳しく評価するとの言及もあった。

図表 9　セキュリティリスクの高い業界



（出所）PwC コンサルティング合同会社「『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」2024 年 4 月 21 日より PwC 作成

６．投資状況により「1 社ずつ個別評価する」米国投資家の割合は日本投資家より多い

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 社ずつ個別評価する」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、米国投資家は全体 7 割に対し、日本投資家は 3 割との結果となった（図表 10）。

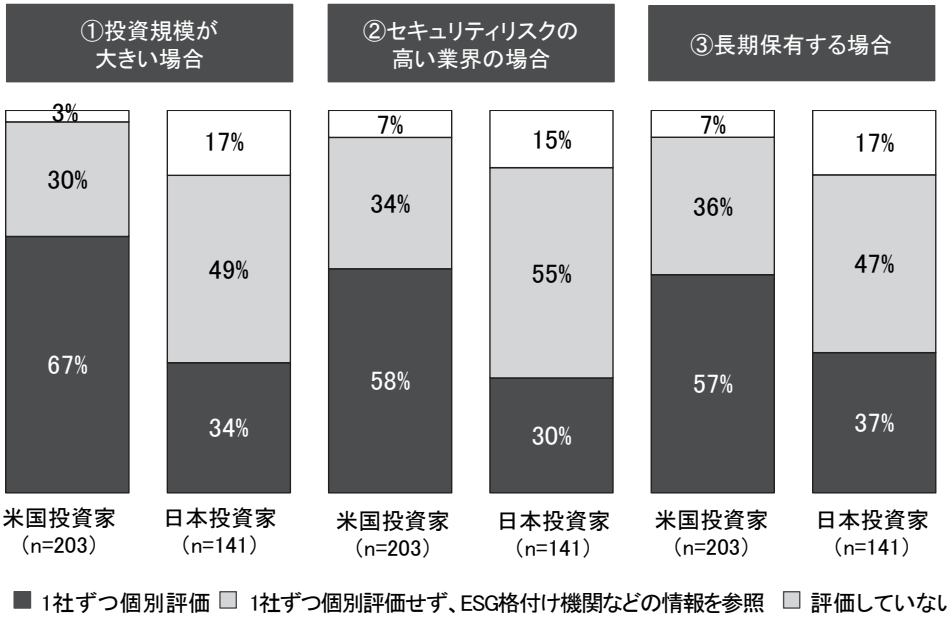
１）投資規模が大きい場合

米国投資家においては、「1 社ずつ個別評価する」が全体の 67%、「1 社ずつ個別評価せず、ESG 評価機関などの情報を参照」が同 30%、「評価していない」が同 3%となった。一方、日本投資家においては、「1 社ずつ個別評価する」が全体の 34%、「1 社ずつ個別評価せず、ESG 評価機関などの情報を参照」が同 49%、「評価していない」が同 17%となった。

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 社ずつ個別評価する」が全体の 58%、「1 社ずつ個別評価せず、ESG 評価機関などの情報を参照」が同 34%、「評価していない」が同 7%

図表 10　投資状況に応じて 1 社ずつ個別評価する割合



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」について1社ずつ評価していますか。それぞれ最もあてはまるものを1つお知らせください。

（出所）PwC コンサルティング合同会社「『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」2024 年 4 月 21 日より PwC 作成

となった。一方、日本投資家においては、「1社ずつ個別評価する」が同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」が同 55%、「評価していない」が同 15%となった。

3）長期保有する場合

米国投資家においては、「1 社ずつ個別評価する」が全体の 57%、「1 社ずつ個別評価せず、ESG評価機関などの情報を参照」が同36%、「評価していない」が同7%となった。一方、日本投資家においては、「1社ずつ個別評価する」が同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」が同 47%、「評価していない」が同17%となった。

これらの結果から、米国投資家では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「1 社ずつ評価」する傾向があると言える。また、日本投資家では、個別評価よりも「評価機関などの評価」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った。

Ⅲ セキュリティ評価者の力量標準化が今後の課題に

インタビューでは、すべての投資家が「企業の開示情報は美しいが、実態が伴っているかまでは見えない。取材をしても IR 担当者から模範的な回答があるにとどまる」と、実態が把握できないことを課題として挙げた。

企業のセキュリティにおける取り組みを適切に評価するには長年の知見・経験やテクノロジーに関する専門知識が必要となるため、正直なところ、唐突にセキュリティ専門家ではない投資家の方にセキュリティ評価を強いるのは酷なことだとも考えられる。何故ならば、新たなテクノロジーの誕生、攻撃手法の確立により、長年の知見を有する企業でもセキュリティリスク評価は難しいからである。

このため、投資家においては、まずは ISMS 認証などの第三者認証組織の認証取得状況や第三者組織によるセキュリティアセスメントやペネトレーションテスト[1]実施状況を評価対象として取り入れることから始めると良いのではないかと思われる。将来的には、国際的なセキュリティガイドライン、例えば ISMS 認証のベースとなる国際規格 ISO/IEC 27000 ファミリーや米国立標準技術研究所（NIST）が提供するセキュリティフレームワーク（NIST CSF V2.0）などの項目を投資家のセキュリティ評価指標に盛り込むことが求められよう。さらに、投資先企業の評価をデータベース化し、投資家ならでは、また日本独自のリスク観点でのセキュリティ評価制度を構築し、国内投資家が適切にセキュリティ評価ができる環境を整備していく必要もあると言える。

[1] 組織の IT システムへの疑似的サイバー攻撃を通じ、セキュリティ対策機能の技術面での有効性を検証するセキュリティテスト手法の1つ。