顕在化する取引先のサイバーインシデントに起因する「ビジネス上の紛争リスク」

――企業が見直すべき「サプライチェーンリスク管理」とは

目次

はじめに

世界的かつ急速なデジタル化の浸透により、企業は取り扱うデータや提供サービス、生産システムなどの開発・運用・破棄といった工程の一部または全てを取引先企業やシステム運用企業に任せるようになり、他社との「サイバーリスクの相互依存関係」がますます拡大しています。

この結果、サイバーインシデントが発生すれば、その影響は瞬く間に取引先など利害関係にある複数の企業へと波及することは近年周知の事実となりました。とりわけ海外においては、サイバーインシデントの一部において、企業同士が損害賠償をめぐり法廷で争うなどの法務リスクにまで発展しています。グローバルなビジネス環境においては、サイバーインシデントに起因するビジネス上の紛争リスクが一段と高まっていると言えるでしょう。そのため、国内のグローバル企業のセキュリティ責任者は、インシデントへの技術的対応だけでなく、法的対応も求められ始めています。

昨今、各国でサイバーセキュリティやプライバシー関連法規制が急速に整備されており、サイバーインシデントに起因するビジネス上の紛争リスクには、企業間の問題にとどまらず、消費者や株主から訴訟を起こされるリスクを内包しています。国内企業は、このようなリスクに対して、適切かつ十分な備えができているでしょうか。

PwCコンサルティング合同会社（以下、PwCコンサルティング）は、国内企業が今後、直面するであろうサイバーインシデントによるビジネス上の紛争リスクの実態把握を目的に、国内外で発生する訴訟を机上調査した上で、国内企業の管理職以上に対しアンケート調査を実施し12,074名から回答を得ました。また、サイバーインシデントに起因するビジネス上の紛争の対応経験のある専門家へのインタビュー調査も実施しました。それらの結果を踏まえて、企業がリスクにどう対処すべきかについて考察します。

実態調査からみる「取引先のサイバーインシデントに起因する『ビジネス上の紛争リスク』11の傾向」

取引先のサイバーインシデントに起因するビジネス上の紛争リスクの実態調査に先立ち、PwCコンサルティングは、国内企業に従事する管理職・経営層を対象としたアンケート調査を実施し、12,074名から回答を得られました。さらにサイバーインシデントに起因するビジネス上の紛争経験を有する6名の有識者（国内外企業におけるサイバーセキュリティ責任者〈CISOなど〉および弁護士など）インタビュー調査を分析した結果、国内企業における「取引先のサイバーインシデントに起因する『ビジネス上の紛争リスク』11の傾向」が明らかになりました（図表1）。

図表1：取引先のサイバーインシデントに起因する「ビジネス上の紛争リスク」11の傾向

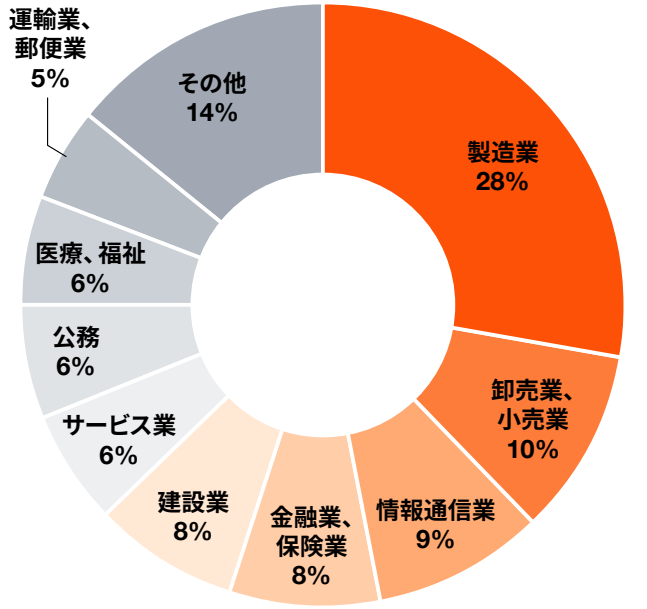
カテゴリー	傾向
サプライチェーンリスクの実態	1. 「自社の顧客情報や機密情報」を取引先企業で取り扱う国内企業は半数 2. インシデント経験を有する国内企業において、取引先企業を起因としたインシデントは3割
損害賠償請求を伴う「ビジネス上の紛争」の発生状況	3. インシデント経験企業の半数が「自社に対する損害賠償請求」を経験 4. 損害賠償請求金額は1,000万円以上が4割、10億円以上は1割存在 5. 取引先企業との紛争解決手段の6割が「示談交渉」で和解、1割が訴訟へ発展 6. インシデント起因のビジネス上の紛争について取引先企業が有責だったとする割合は6割
紛争経験を踏まえたサプライチェーン管理の見直し	7. インシデント経験後サプライチェーン管理を見直した企業は9割、うち9割が「委託先選定基準」を改定 8. 委託先選定基準として特に評価する項目は「セキュリティ教育」「法令順守状況」
サイバーセキュリティ関連法の動向把握	9. インシデント経験企業の6割がサイバーセキュリティ関連法を確認 10. インシデント経験企業の半数がサイバーセキュリティ関連法を「3カ月ごとに確認」 11. セキュリティ関連法動向の把握手法について自社専門部門だけでなく「コンサルタント」や「法律事務所」など、外部専門家をうまく活用する割合が上位

出所：PwC作成

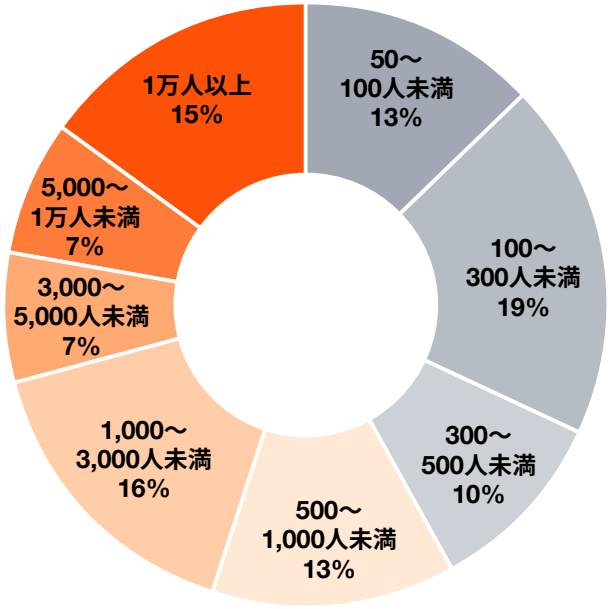
今回のアンケート調査対象となった回答者の属性は図表2のとおりです。

図表2：アンケート調査における回答者属性

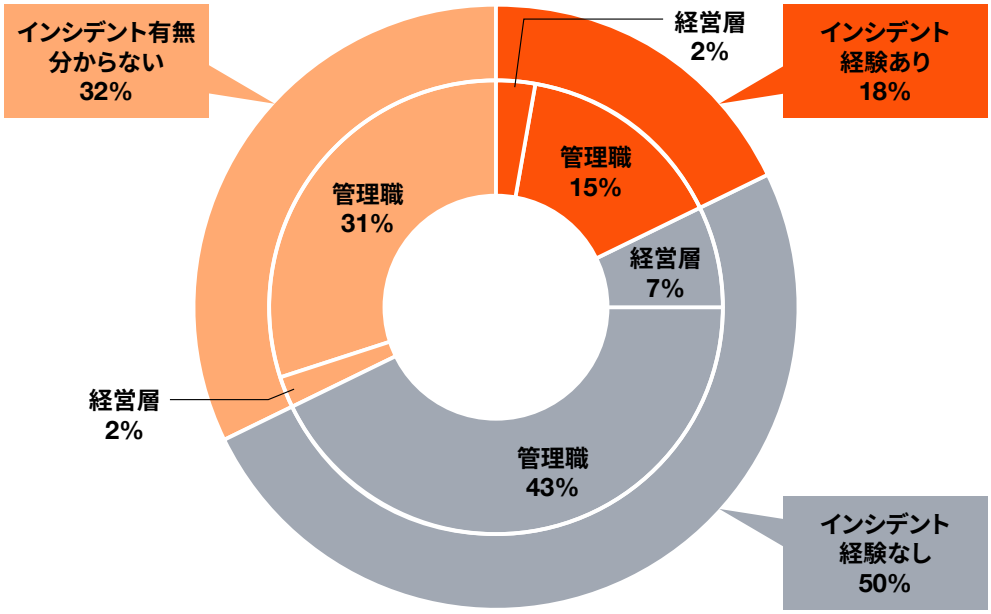
勤務先の業界（n=12,074）



従業員規模数（n=12,074）



インシデント経験有無および役職（n=12,074）



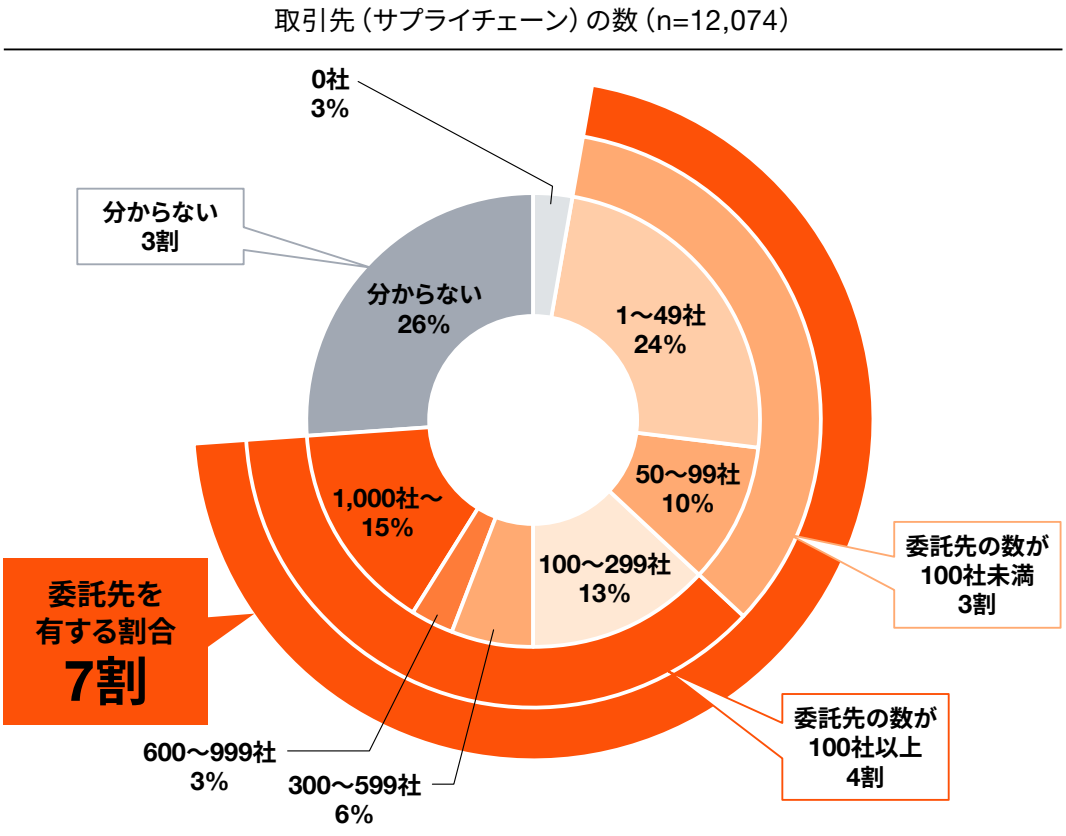
※四捨五入しているため、内訳の合計が親セグメントの比率と一致しない場合があります。
出所：PwC作成

サプライチェーンリスクの実態

昨今、取引先のサイバーインシデントに起因する企業の情報漏えいが大きく報道されています。アンケート調査の結果を踏まえ、国内企業の管理職以上が、自社の守るべき情報である「顧客情報」や「機密情報（製品の開発情報など）」の在りかを正しく把握しているか、また、実際に、取引先を起因としたサイバーインシデントが発生しているかについて確認していきます。

なお、今回のアンケート調査対象が所属する国内企業（n＝12,074）に対し、取引先の有無を確認したところ、71%が「取引先がある」と回答しました（図表3）。

図表3：アンケート調査における回答者属性（取引先の数）

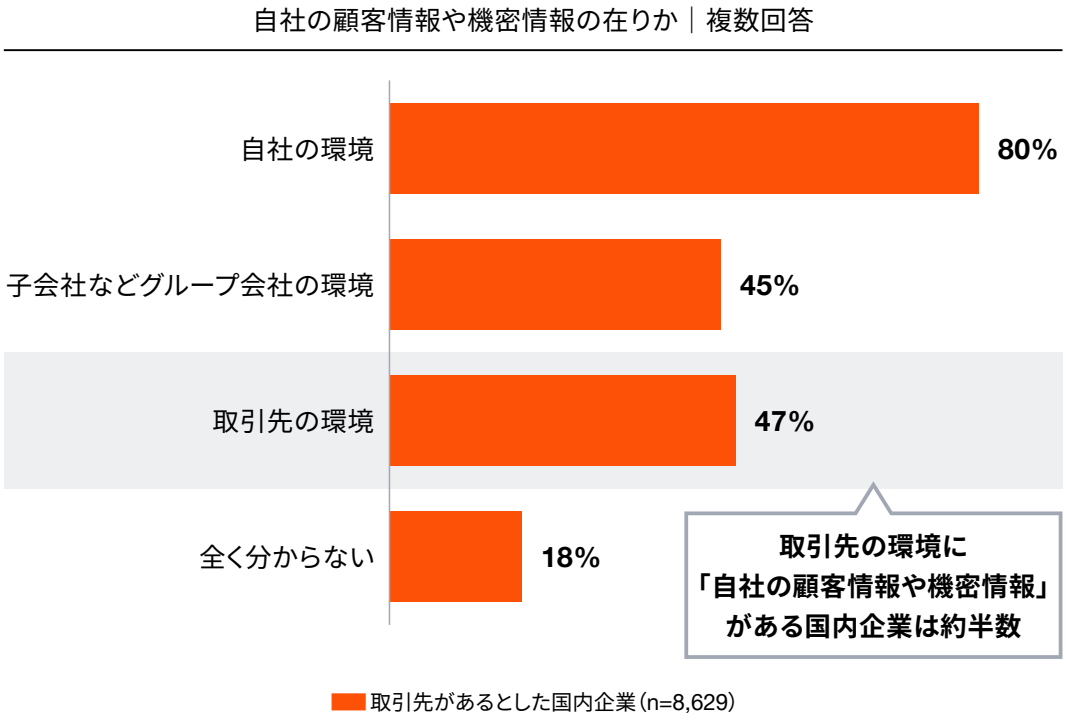


出所：PwC作成

傾向1 「自社の顧客情報や機密情報」を取引先企業で取り扱う国内企業は半数

取引先を有する国内企業（n＝8,629）に対し、「自社の顧客情報や機密情報の在りか」の把握状況を確認したところ、「自社の環境」が80%、「子会社などグループ会社の環境」が45%、「取引先の環境」が47%、「全く分からない」が18%となり、半数近くの企業が自社の顧客情報や機密情報を取引先の環境で取り扱うことが明らかになりました（図表4）。

図表4：自社の顧客情報や機密情報の在りかの把握状況



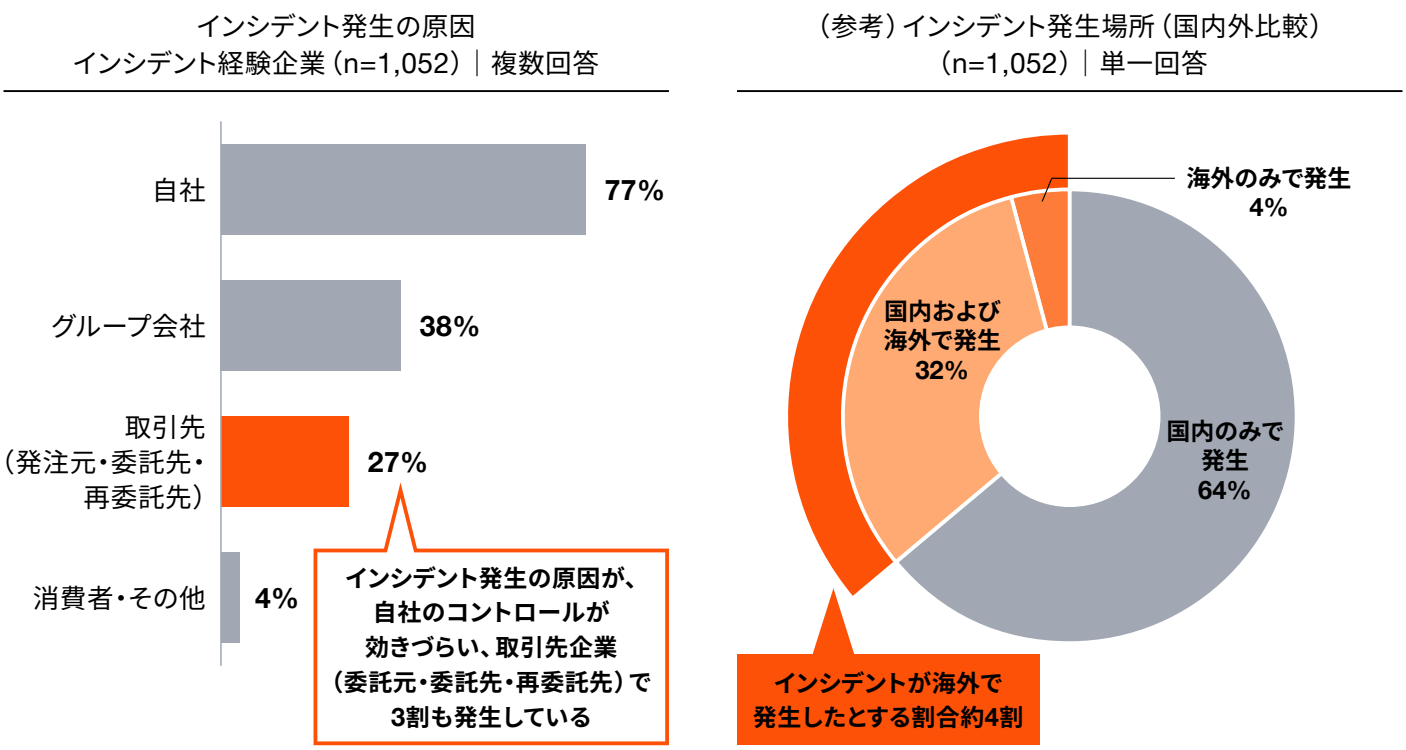
Q. あなたの勤務先が保有する「顧客情報」や「機密情報（製品の開発情報など）」は、どこに格納されているかお知らせください。あてはまるもの全てお知らせください。

出所：PwC作成

傾向2　インシデント経験を有する国内企業において、取引先企業を起因としたインシデントは3割

次に、実際に取引先企業に起因するサイバーインシデントは発生しているのかについて確認していきます。サイバーインシデントを経験したとする企業（n＝1,052）に対し、「サイバーインシデントについて、原因はどこで発生したか」と質問したところ、「自社」が最も多く77%、次いで「グループ会社」が38%、「取引先（発注元・委託先・再委託先）」が27%でした（図表5）。インシデント経験企業の約3割が、自社のセキュリティガバナンスが効きづらい取引先を原因としたサイバーインシデントを経験していることから、インシデント発生時に影響範囲を明確にするためにも、自社の個人情報管理台帳や情報資産管理台帳などでの情報管理が徹底されているか、改めて管理体制を見直す必要があります。特に海外居住者の個人情報が漏えいした場合は、各国当局へのインシデント報告が求められる可能性があることから、インシデント発生時の対応も異なってくるため、現状把握は重要です。

図表5：インシデント発生の場所および原因（n=1,052）



Q. 現在の勤務先において、業務に影響のあるサイバーインシデントを経験された方に伺います。経験した情報セキュリティ事故（サイバーインシデント）について、原因はどこで発生しましたか。あてはまるものを全て選んでください。

出所：PwC作成

損害賠償請求を伴う「ビジネス上の紛争」の発生状況

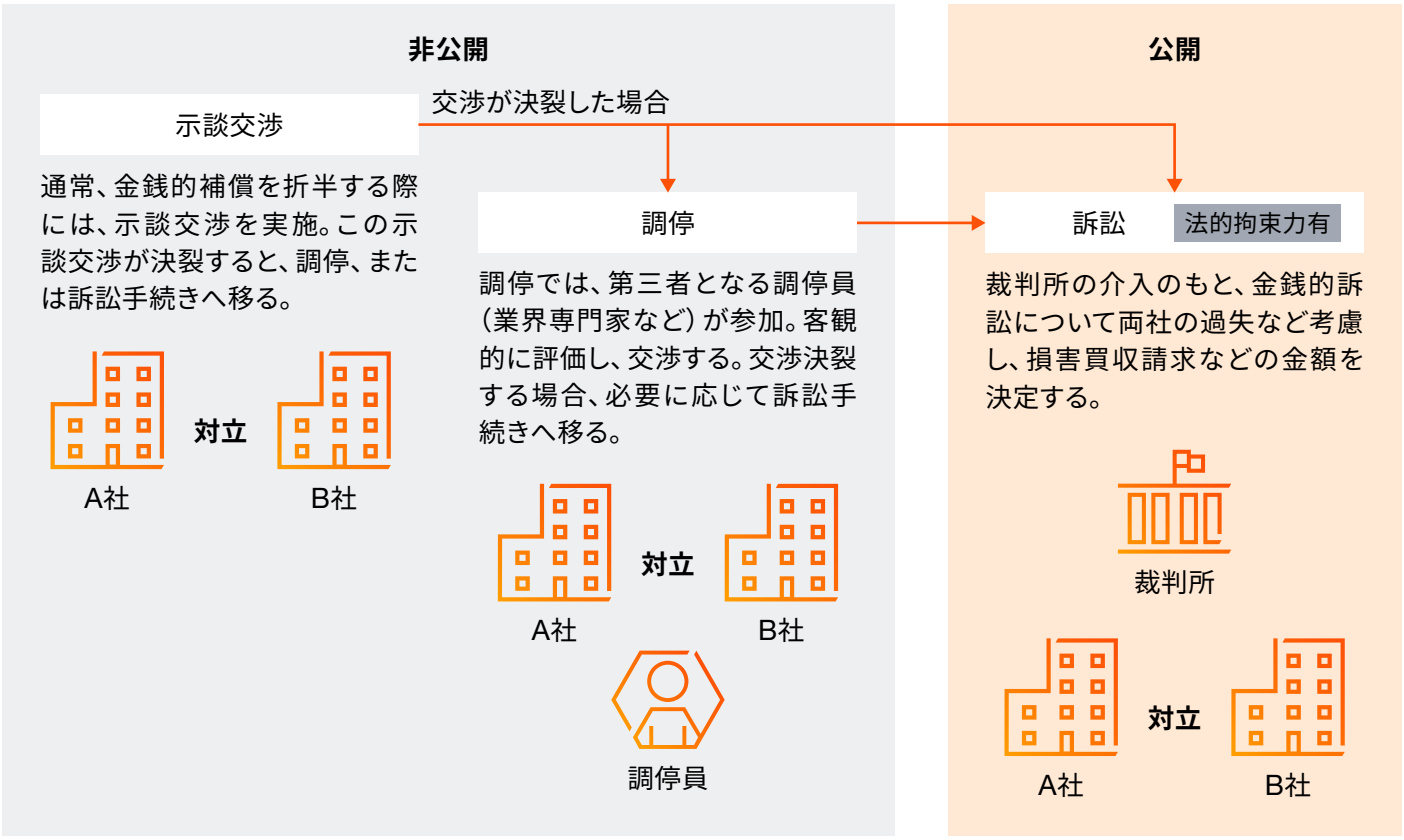
ここからは、サイバーインシデント後に生じるビジネス紛争の発生状況を掘り下げます。

紛争の類型

サイバーインシデント関連の紛争対応経験を有する弁護士および企業の紛争対応経験者にインタビューしたところ、サイバーインシデントに起因する紛争解決手段には、主に「示談交渉」「調停」「訴訟」の3つの手段※がとられ、中でも「示談交渉」が多く、「訴訟」も少ないながら増加傾向にあることが分かりました（図表6・図表7）。特に米国においては、ここ10年で提訴しやすくなり、訴訟が増加傾向にあることが指摘されています。

※なお、紛争解決手段において「仲裁」の選択肢もあります。もっとも国内弁護士および海外有識者へのインタビューにおいて、サイバーインシデントに起因する紛争において「仲裁」を選択するケースは極めてまれで、その背景に、通常仲裁は、国際仲裁を指す場合が多く、当該仲裁には仲裁機関へ付託し1年程度の時間を有し、さらにそれらに係る費用は少なくとも1億円かかるためだと指摘がありました。

図表6：主な紛争解決手段と一般的な紛争解決手段の流れ



出所：PwC作成

図表7：（参考）主な紛争解決手段

紛争解決手段	示談交渉	調停	訴訟
概要	示談交渉は当事者同士が直接話し合い、互いに納得できる解決策を見つける手法です。非公式かつ迅速で、時間や費用を抑えられます。一方で、感情的な対立や信頼関係の欠如により、合意に達しづらい場合もあります。交渉の柔軟性を生かし、弁護士の助言を得ることで進展を図ることが望ましいです。	調停は中立の第三者が介入し、当事者間の対話を支援して解決案を導く方法です。合意に基づく解決を目指し非公開で行われます。法的拘束力はありませんが、進行は迅速で費用も比較的少なく済みます。調停者がコミュニケーションを促し、両者の立場を尊重しながら柔軟に問題を解決します。	訴訟は裁判所で法律に基づき正式に紛争を審理し、裁判官が強制力のある判決を下します。公に行われるため公正性が確保されますが、時間と費用がかかる傾向があります。法的手続きが整備されており、最終的な解決を求める場合に適切です。
関係者	• 当事者（および、弁護士）	• 当事者（および、弁護士） • 調停員	• 当事者（および、弁護士） • 裁判官（裁判所）
解決までに要する期間	短い	短い	長い （規模によるが数年程度）
費用	低	低～中	高
法的拘束力	無	無	有
公開／非公開	非公開	非公開	公開
サイバー関連紛争発生頻度 ※サイバーインシデント関連の紛争対応経験者（弁護士含む）ヒアリング結果より	多い	少ない	まれ

出所：PwC作成

傾向3　インシデント経験企業の半数が「自社に対する損害賠償請求」を経験

それではアンケート調査結果をみていきます。

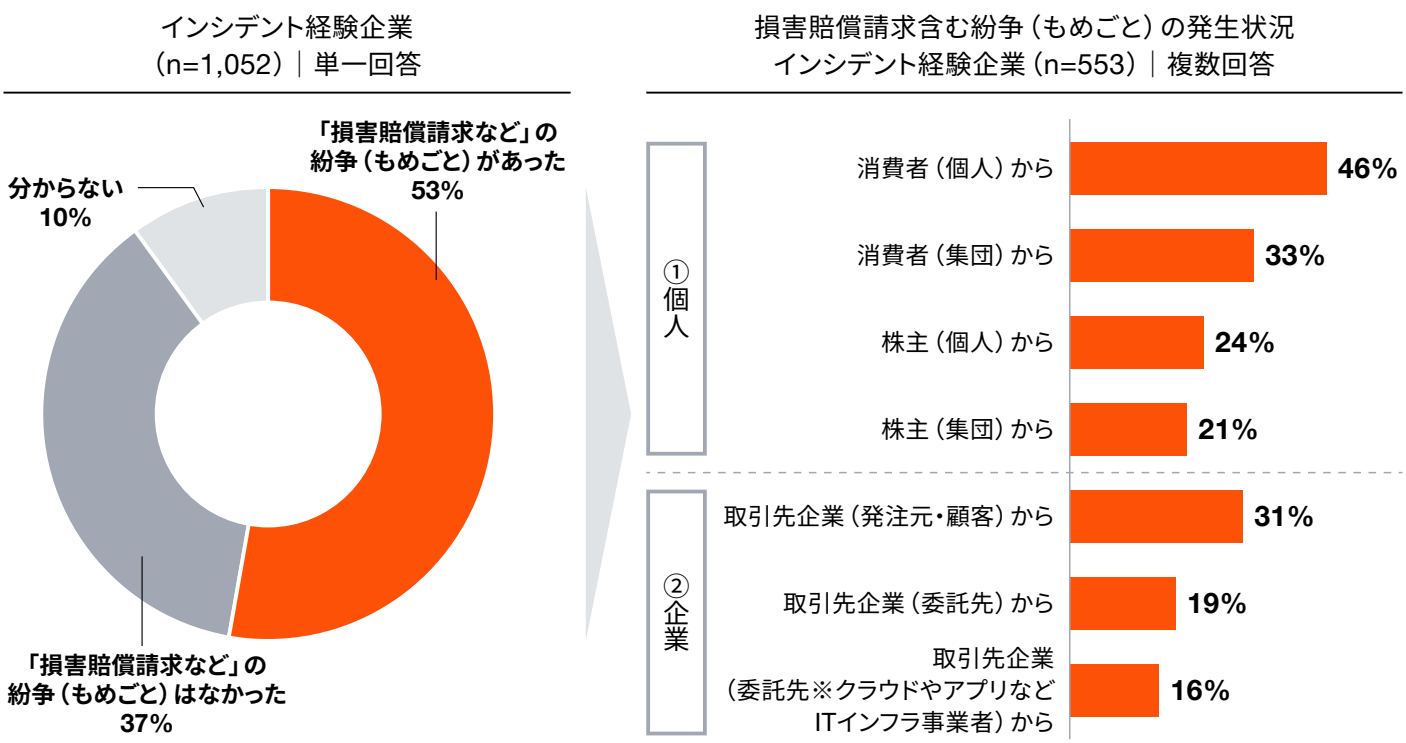
今回の調査において最も注視したいことは、サイバーインシデント経験企業の5割が、当該インシデントに起因する損害賠償請求を受けたと回答したことです（図表8：左）。

具体的にみると、サイバーインシデント経験企業（n＝1,052）に対し、「経験したサイバーインシデントについて、損害賠償請求などを伴うビジネス上の紛争（もめごと）があったか」を確認したところ、「損害賠償請求などの紛争（もめごと）があった」が53％で最も多く、次いで、「損害賠償請求などの紛争（もめごと）はなかった」が37％、「分からない」が10％の順となりました。

さらに「損害賠償請求などの紛争（もめごと）があった」とする回答者（n＝553）に対し、「誰からの金銭的要求があったか」を質問したところ、「①個人」カテゴリーにおいては、「消費者（個人）から」が最も多く46%、次いで「消費者（集団）から」が33%、「株主（個人）から」が24%、「株主（集団）から」が21%となりました（図表9：右）。「②企業」カテゴリーにおいては、「取引先企業（発注元・顧客）から」が最も多く31%、「取引先企業（委託先）から」が19%、「取引先企業（委託先※クラウドやアプリなどITインフラ事業者）から」が16%の順になりました。

これらのことから、サイバーインシデントが発生した際に、企業は、消費者や株主である個人、または取引先企業（例えば発注元、委託先、ITインフラ提供企業）などから「損害賠償請求をされるリスク」が実際にあることがデータとして裏付けられました。

図表8：損害賠償請求額を伴う紛争の発生状況



Q. 現在の勤務先において、業務に影響のあるサイバーインシデントを経験された方に伺います。経験した情報セキュリティ事故（サイバーインシデント）について、「損害賠償請求など」の紛争（もめごと）はありましたか？あった場合は誰からの金銭的要求があったかをお知らせください。

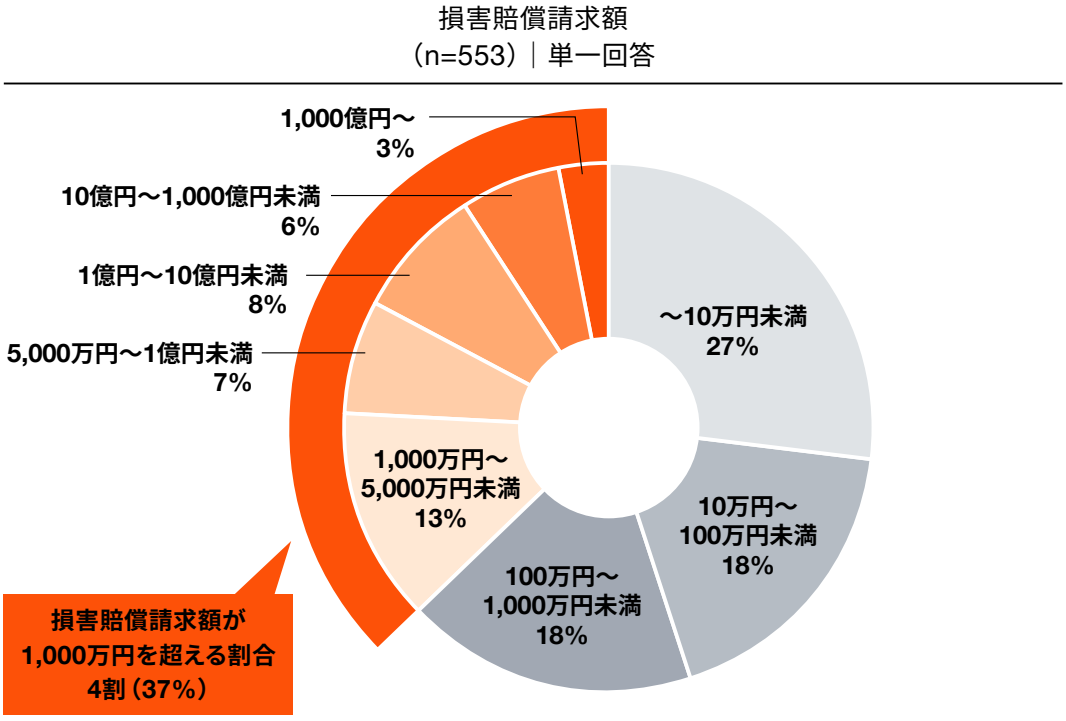
出所：PwC作成

傾向4　損害賠償請求金額は1,000万円以上が4割、10億円以上の割合は1割存在

損害賠償請求をされたと回答した企業（n＝553）に対し、「損害賠償請求額はいくらだったか」確認すると、「1,000万円以上請求」が4割となりました（図表9）。また請求額上位をみると「10億円以上請求された割合」が1割近く存在し、多くの企業にとって、サイバーインシデントを金銭的損失リスクと位置づけざるを得ない段階に達しつつあります。

実際、国内においても、サイバーインシデントに起因する判例で、1,000万円～数億円相当の損害賠償請求が争われた事案が確認されています。

図表9：損害賠償請求額



Q. 業務に影響のあるサイバーインシデントを経験された方で、消費者や取引先から金銭的要求があったと回答された方に伺います。サイバーインシデントを原因とする、消費者や取引先企業からの金銭的要求（損害賠償請求）の規模はどのくらいでしたか。複数該当する場合は、最も大きな損害額をお知らせください。

出所：PwC作成

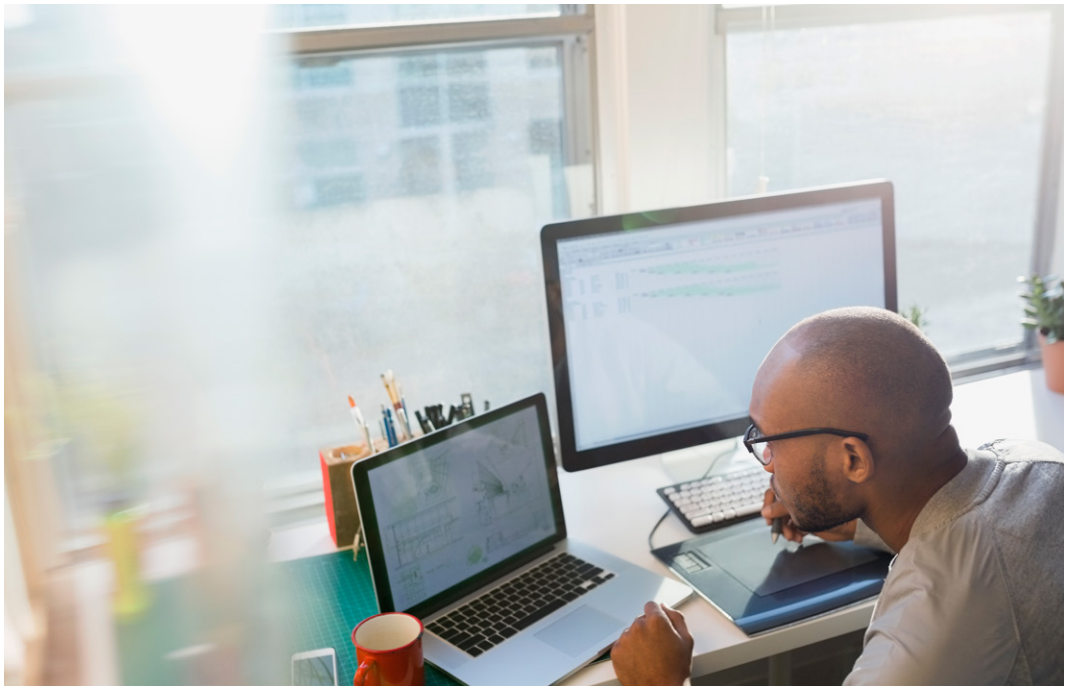
傾向5 取引先企業との紛争解決手段の6割が「示談交渉」で和解、1割が訴訟へ発展

では、国内企業はどのような紛争解決手段をとっているのでしょうか。

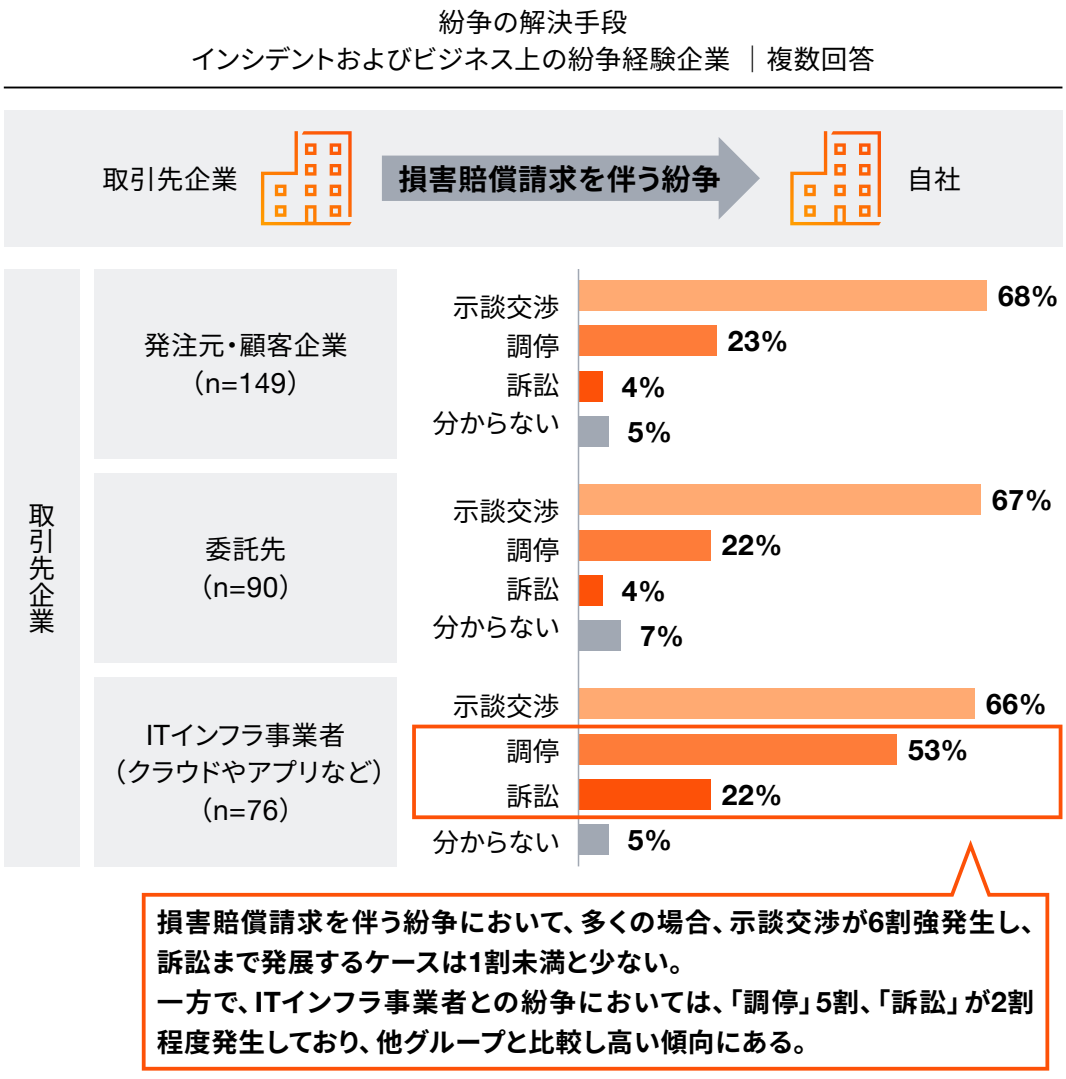
■取引先企業からの損害賠償請求を伴う紛争

取引先等の企業から損害賠償請求をされたと回答した企業（n＝259）に対し、「どのように解決したか」質問したところ、取引先企業（発注元、委託先、ITインフラ事業者など）では、58%が「示談交渉」、40%が「調停」、14%が「訴訟」に発展したと回答しました。

具体的にみると（図表10）、「発注元・顧客企業」から損害賠償請求されたグループ（n＝149）では、「示談交渉」が68%で最も多く、次いで、「調停」が23%、「訴訟」が4%、「分からない」が5%の順となりました。「委託先」に損害賠償請求されたグループ（n＝90）では、「示談交渉」が67%で最も多く、次いで、「調停」が22%、「訴訟」が4%、「分からない」が7%の順となり、「発注元・顧客企業」に損害賠償請求されたグループと同じ傾向がみられました。次に「ITインフラ事業者（クラウドやアプリなど）」に損害賠償請求されたグループ（n＝76）を確認すると、「示談交渉」が66%で最も多く、「調停」は53%で他グループと比較して30ポイント程度高くなり、「訴訟」も22%と他グループと比較し18ポイント高くなりました。これらから、ITインフラ事業者との取引の中で生じたサイバーインシデントでは、損害賠償請求を伴う紛争発生リスクが、他取引先企業よりもやや高いと言えます。



図表10：紛争の解決手段（相手方からの損害賠償請求を伴う紛争）



Q. 現在の勤務先において、業務に影響のあるサイバーインシデントを経験された方に伺います。情報セキュリティ事故に起因した「損害賠償請求など」の紛争（もめごと）について、どのように解決手段を取りましたか？

出所：PwC作成

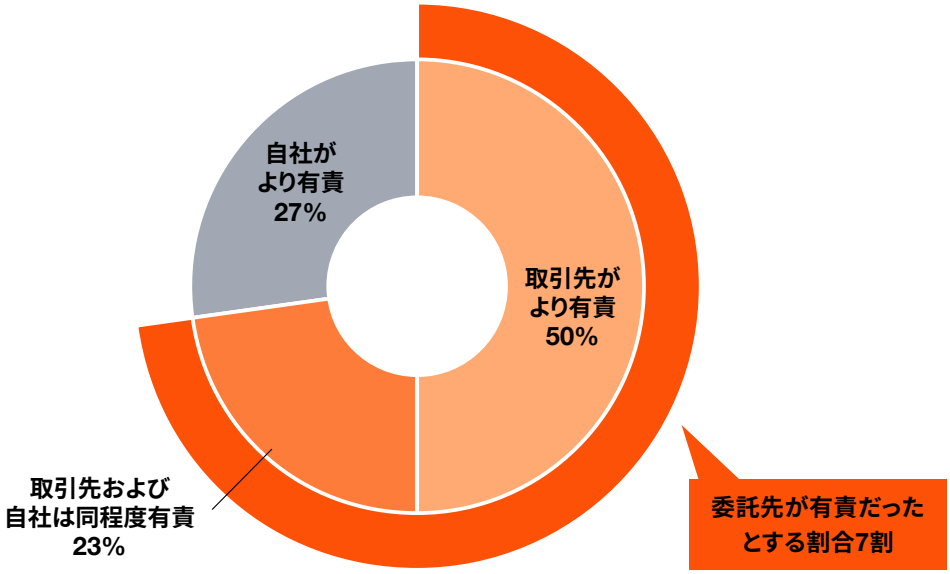
米国の有識者へのインタビューにおいても、ほぼ全ての有識者が「取引先との関係性悪化やブランドイメージ低下などのネガティブな側面を考慮し訴訟はできるだけ避けたい」と述べています。一部企業の事例では、「インシデント100件あたり、クレームがない割合は55%、20%が示談交渉に発展し、5～10%が調停となり、5%程度が訴訟まで発展する」とされており、最終的に訴訟まで発展するケースは1割弱にとどまることから、訴訟発生の割合については実態に即していると言えそうです。なお、インタビューの中には、インシデントを起こしたにもかかわらず示談交渉に全く応じなかった取引先企業（先進国）に対し、自国だけでなく意図的に当該企業が上場する国において訴訟を起こしたケースも確認できています。

傾向6　インシデント起因のビジネス上の紛争について取引先企業が有責だったとする割合は6割

次に、取引先間で損害賠償請求があり、有責の割合を回答できるとした企業（n＝259）にインシデントにおける有責の配分について確認したところ、「取引先がより有責」「取引先および自社は同程度有責」と回答した割合は7割に達し、セキュリティ観点からサプライチェーン管理の重要性が明らかとなりました（図表11）。

図表11：インシデント起因のビジネス上の紛争において、取引先が有責とする割合

インシデント起因のビジネス上の紛争において、取引先が有責とする割合
インシデント経験企業（n=259）｜単一回答



Q. 業務に影響のあるサイバーインシデントを経験された方で、取引先間で損害賠償請求があったと回答された方に伺います。損害賠償請求の割合は、当事者間でどのくらいの割合で決定しましたか。最も近しいものを一つお知らせください。

出所：PwC作成

なお、弁護士へのインタビューでは、損害賠償請求における原告・被告の「過失」の程度は、契約内容や日々のリスクに関するコミュニケーションでの当事者間の合意事項など、状況に応じて異なるとの指摘がありました。ただし「内部不正によるインシデント」については、たとえ行為者が契約社員や個人事業主であっても、その者を採用した企業が有責となる可能性が非常に高いとされており、従業員の管理が必要です。

このため企業は、取引先企業に対面する従業員に対し、日々のコミュニケーションにおいて、適切なサイバーリスクについて議論し、証跡として残すことの重要性を伝える必要があります。例えば、ユーザー企業においては、取引先に対しサイバーリスクについて懸念がある場合には相談すること、また取引先から提示されたリスクを安易に現場の判断だけで許容しないこと（必要に応じてエスカレーションし、追加予算を得るなど）が挙げられます。他方、システム提供企業といった委託先においては、提案時などに「セキュリティは万全」「100%セキュア」など不確かな情報を容易に言わないこと、システム・アプリケーション開発時・運用時にセキュリティリスクが専門家としてみたときに当然認められる場合、仕様書になかったとしても、専門家としてユーザー企業へ当該リスクと対応方法および対応に係る費用を掲示すること、またそれらに対するユーザー企業の判断を仰ぎ、合意内容を証跡として残すことが重要です。これは、万が一議論されたリスクを起因としたインシデントが発生した際に、当該リスクの許容をした主体はどちらか、その責任の所在を明確できるからです。加えて、内部不正の対策においてもデータの機密性に応じたラベルを厳格に付与することの徹底や教育対象の範囲拡大、Need to Knowの原則に基づくアクセス権の最小権限を徹底する必要があります。

紛争経験を踏まえたサプライチェーン管理の見直し

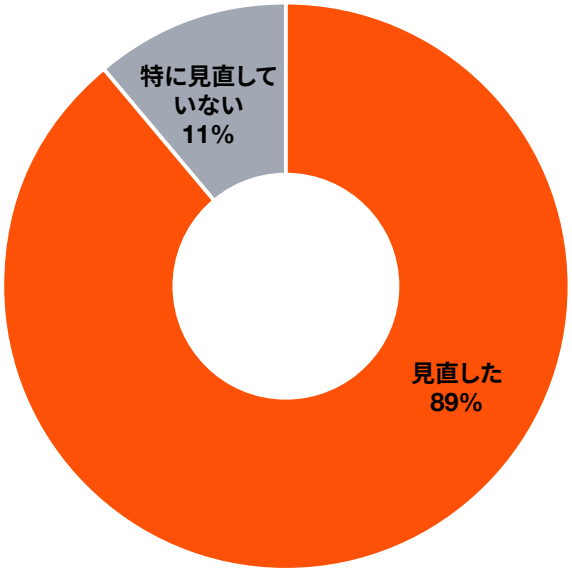
傾向7 **インシデント経験後サプライチェーン管理を見直した企業は9割、うち9割が「委託先選定基準」を改定**

インシデント経験企業（n＝1,052）にインシデント発生後の改善策について確認すると、9割が「サプライチェーン管理を見直した」と回答しました（図表12）。サプライチェーン管理を見直した企業（n＝940）の内訳をみると「委託先の選定基準の見直し」が90%と最も高く、次いで「運用の見直し」が57%、「契約書の見直し」が39%、「仕様書の見直し」が34%でした。サプライチェーン管理を見直したとする企業の9割が「委託先選定基準を見直した」と回答したことから、多くの企業で委託先選定時点でのサイバーリスクを考慮した適切なセキュリティ評価が不足していたことが読み取れ、「セキュリティ上懸念のある企業へ委託可能」な状況が常態化していたことが推察されます。

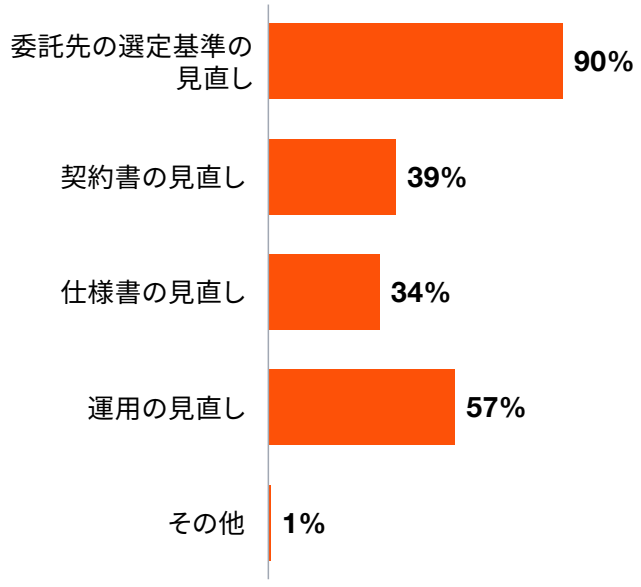
インタビュー調査においても、①ビジネス上の力関係（資本関係含む）や②特許など、その希少性から特定企業に頼らざるを得ない状況の企業、③委託先が小さな町工場で能力的に対応ができない、④対策費用を追加で求められるなど、さまざまな理由から、「セキュリティ要件を満たしていないが委託せざるを得ない状況」があり、サプライチェーン上の全ての企業に一律のセキュリティ要件を求めることは難しく、サプライチェーンリスク管理の課題の一つと言えます。

図表12：サプライチェーン管理を見直した割合と具体策

インシデント発生後のサプライチェーン見直し有無
インシデント経験企業（n=1,052）｜単一回答



インシデント発生後のサプライチェーン見直し対象
インシデント経験企業（n=940）｜複数回答



Q. 現在の勤務先において、業務に影響のあるサイバーインシデントを経験された方に伺います。情報セキュリティ事故（サイバーインシデント）を経験後、取引先企業を対象としたセキュリティ管理の見直しをしましたか。あてはまるものを全てお知らせください。

出所：PwC作成

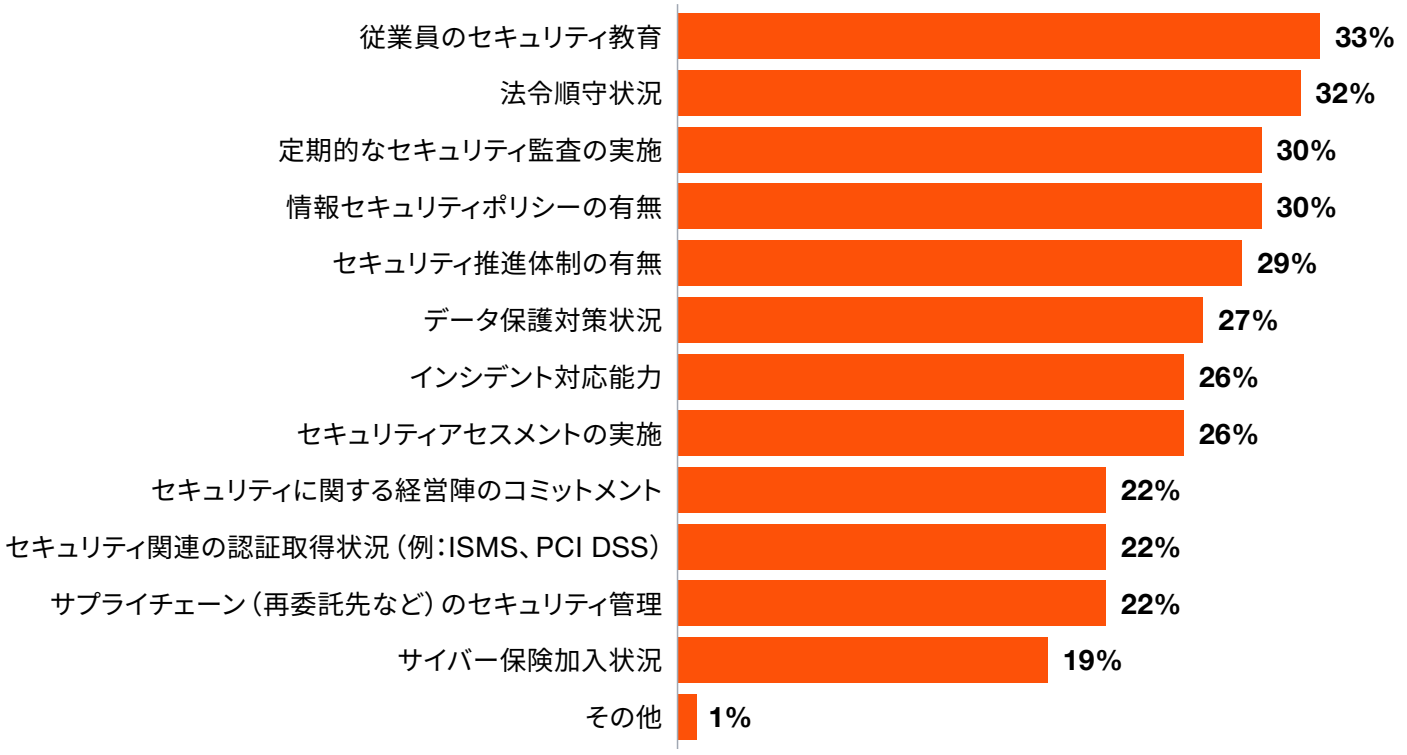
傾向8 委託先選定基準として特に評価する項目は「セキュリティ教育」「法令順守状況」

さらに、インシデント経験企業（n＝1,052）に「委託先選定基準に盛り込んでいる項目」を確認したところ、「従業員のセキュリティ教育」が最も高く33%、次いで「法令順守状況」32%、「定期的なセキュリティ監査の実施」「情報セキュリティーポリシーの有無」が30%、「セキュリティ推進体制の有無」29%という結果でした（図表13）。

インタビュー調査においては、サイバーインシデントに起因する紛争を数多く手がける弁護士は、「契約書の見直し」や「日々のコミュニケーションでリスクについて議論し、当該議事録をとり、証跡として残すこと」も重要としています。特に海外企業や消費者からのビジネス上の紛争リスクに備え、タイムリーな「各国の法規制動向のモニタリング」も必要になっており、これは前述のアンケート調査結果の「法令順守状況」を適切に評価する上で評価側の企業が把握し、かつ運用に盛り込むことが重要となってきます。

図表13：委託先選定基準の具体例

「委託先選定基準」の具体例
インシデント経験企業（n=1,052）｜複数回答



Q. あなた、またはあなたの勤務先では、取引先を選定する際に、どのようなセキュリティ項目を確認しますか。あてはまるものを全て教えてください。

出所：PwC作成

コラム 【インタビュー】サイバーインシデントを起因としたビジネス紛争経験企業

ビジネス上の紛争を経験した企業（ユーザー企業）でも、委託先管理の見直しを実施していることが明らかになりました。図表14に見直し観点のインタビュー結果を紹介します。

図表14：インタビューにおけるビジネス上の紛争リスクに対する見直し

	ビジネス上の紛争リスクに対する見直し
A社 （インフラ事業者）	・得意分野の異なる弁護士との契約 サイバーインシデントを起因としたビジネス紛争が多く発生しており、その対応として、さまざまな分野に強みを持つ弁護士を探し「顧客情報保護分野に強みを持つ弁護士」「テクノロジー分野に強みを持つ弁護士」「物理セキュリティ分野に強い弁護士」と契約しました。 ・自社セキュリティガバナンスを強化および自社専門家の確保（セキュリティおよび法務） セキュリティ部門の人数を20人まで増やし、さまざまなスキルを持つチーム体制を構築しました。また、セキュリティ戦略は大手コンサルティング会社の支援を受け、作成しました。規程類については、サイバーセキュリティの内部プロセスの手順書やルールを文書化して確立しました。具体的には、顧客の責任（どのような責任があり、インシデント発生時に何をして、どのように対処すべきなのか）を明記し、さらには、ISO／IEC 27001のISMS認証取得により、内部プロセスを確立しました。 これらに加え、従業員への教育も強化しています。規程類が整備されても従業員が正しく行動できなければ意味がないからです。特に物理媒体については頭を抱えており、印刷時は適切に削除しないと漏えいにつながります。ISMS認証を取得しようと、例えば出張時などで安全でないホテルの無料ネットワークを使用して機密情報を扱ったり、SNSで扱ったりするため、セキュリティ教育が重要と考え強化しています。 サイバーインシデントが発生した際は、法務部門が対応に当たります。当社では米国、カナダなどの個人情報を取り扱っているため、各国の法規制を理解した職員を法務部門に配属し、示談交渉へ当たらせています。交渉が決裂すれば法廷で争うことになりますが、訴訟を5%に抑えられていることは良いと考えています。

	ビジネス上の紛争リスクに対する見直し
B社（金融）	・契約書に盛り込むセキュリティ要件の見直し 契約書にはセキュリティ要件を記載していましたが、その要件が最初に契約を締結した10年前と同じ文言となっており、急速に変わるテクノロジーにおいて現在のサイバーセキュリティ要件が適切とは言いがたい状況で、紛争において当社側にとって不利となりました。このため、毎年、契約書において適切なセキュリティ要件となっているか見直しを行うことにしました。 ・選定時に取引先企業側の体制・セキュリティプログラムを確認、また責任範囲を明確にする インシデントを発生させた取引先企業に有効な「サイバーセキュリティプログラム」体制の構築と文化の醸成に取り組んだ他、取引先および当社の責任範囲をはっきりさせるようにしました。 ・取引先企業におけるシステム上のセキュリティ強化を要求 当社では、まずインシデントリスクを低減するため、取引先企業に「弊社と同等のセキュリティレベルを求める」こととしました。さらに、「取引先企業のシステムと弊社システムの接続にある二つのレイヤーのセキュリティ強化」を実施しています。具体的には、ファイヤーウォール（FW）などの境界防御とActive Threat Huntingによる強化（アノマリ検知を強化し、リスクが上がったら即分離できるようにするなど）です。 なお、要求することで追加費用を請求する事業者も今後あるかもしれませんが、当社としては、最低限講じるべきセキュリティ対策は、取引先および弊社双方が実装すべきと考えており、現時点では議論となっていません。 ・取引先のリスクアセスメントの実施 取引先のリスクアセスメントは主に2種類あります。 1）アンケートベースのアセスメント： 一つは、パートナー会社にアンケートを送って回答をもらうことと、オンゴーイングなモニタリングシステム（取引先企業のセキュリティに対する姿勢を継続的に監視する仕組み）を導入しました。 2）外部リスクサービスの導入： 当社ではサプライチェーンリスク評価サービスを新たに導入し、取引先企業のリスクの浮き沈みにより判断できるようにしました。コストはかかりますが、必要経費と考えています。 3）（補足）契約上の監査権： 契約上監査を実施する権利は持っていますが、取引先企業を監査したのは2回のみです。理由は業務支障とコスト（第三者期間による監査）です。

出所：PwC作成

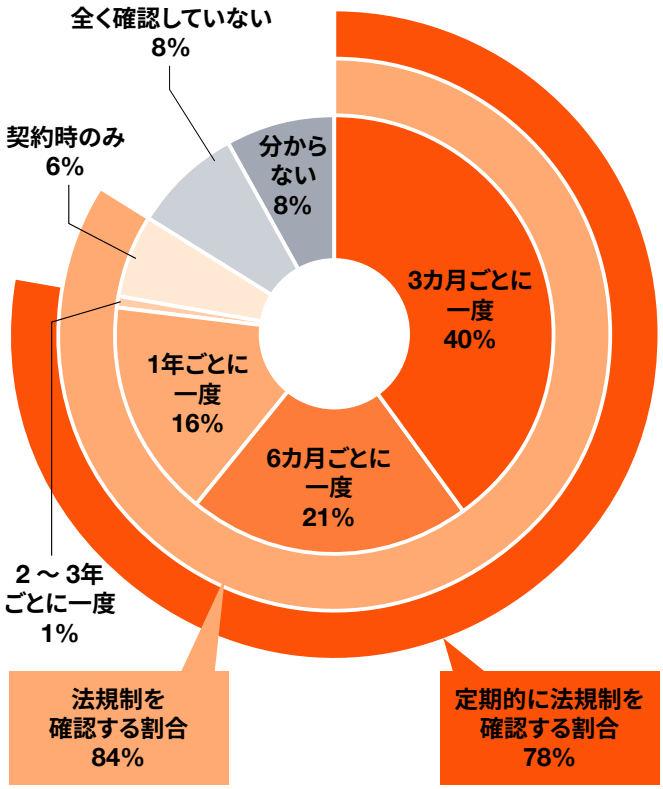
サイバーセキュリティ関連法の動向把握

傾向9 インシデント経験企業の6割がサイバーセキュリティ関連法を確認

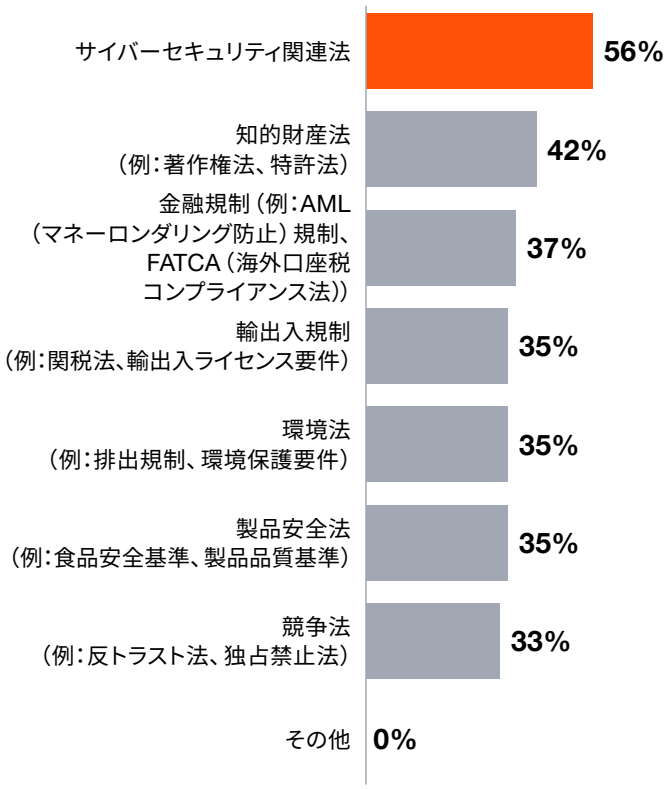
インシデント経験企業（n＝1,052）において、「法規制動向の確認頻度」を質問すると、「定期的に法規制を確認する」と回答した割合は8割と高く（図表15：左）、そのうち半数以上が「サイバーセキュリティ関連法」を確認するとしています（図表15：右）。

図表15：法規制の確認状況と、法規制の種類

法規制動向の確認頻度
インシデント経験企業（n=1,052）｜単一回答



法規制動向を確認するとした
インシデント経験企業（n=883）｜複数回答



Q. 業務に影響のあるまたは取引先企業の所在する国の「法規制の動向」を確認しているとご回答の方に伺います。確認する対象の法規制を具体的にお知らせください。あてはまるものを全てお選びください。

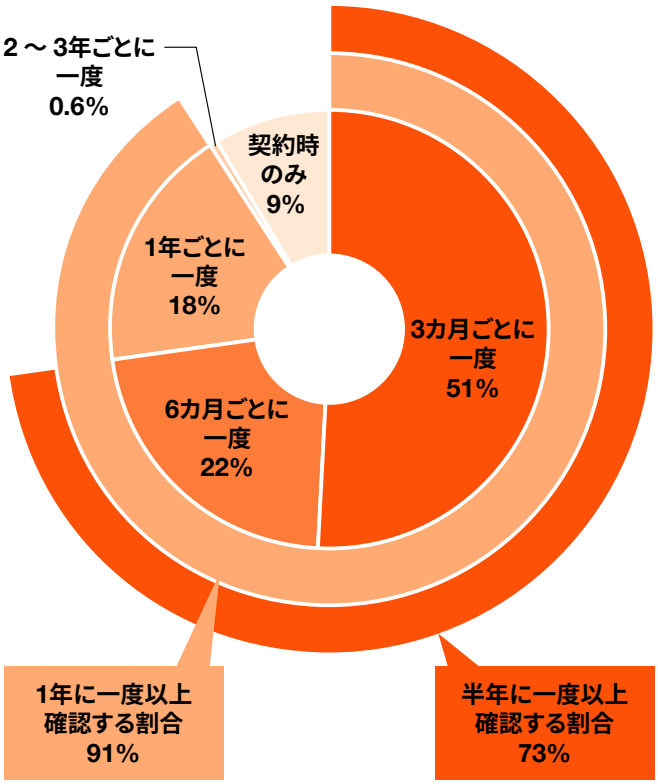
出所：PwC作成

傾向10 **インシデント経験企業の半数がサイバーセキュリティ関連法を「3カ月ごとに確認」**

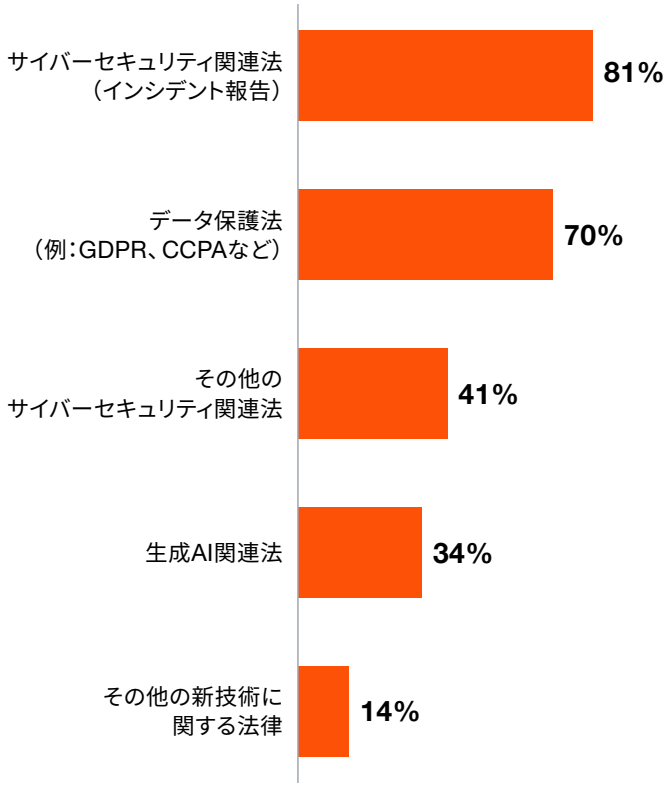
さらに、サイバーセキュリティ関連法を確認するとしたインシデント経験企業（n＝492）に「確認頻度」を確認したところ、「3カ月ごとに一度」が最も高く51%、「6カ月ごとに一度」が22%、「1年ごとに一度」が18%、「2～3年ごとに一度」が0.6%の順となり、「契約時のみ」確認するとした割合は9%となりました。このことから、サイバーセキュリティ関連法を確認するとした企業のほとんどは、定期的に動向を追っている状況が明らかになりました（図表16：左）。この背景に、ここ数年でサイバーセキュリティ関連法、特にインシデント報告に関する各国の法規制の成立・施行が相次ぎ、国内企業にとっても対応を余儀なくされるケースが増加傾向にあり、事実、PwCコンサルティングへの依頼もこれに呼応して急増しています。

図表16：サイバーセキュリティ法規制確認頻度と具体的なサイバーセキュリティ関連法（n=492）

サイバーセキュリティ関連法の確認頻度
サイバーセキュリティ関連法を確認するとした
インシデント経験企業（n=492）｜単一回答



具体的なサイバーセキュリティ関連法
サイバーセキュリティ関連法を確認するとした
インシデント経験企業（n=492）｜複数回答



Q. 前問にて「セキュリティや個人情報保護に関する法律」を確認すると回答した方へ質問します。確認頻度をお知らせください。また「セキュリティや個人情報保護、テクノロジーに関する法律」について、どのような法令を確認していますか。あてはまるものを全てお選びください。

出所：PwC作成

さらに、サイバーセキュリティ法規制を確認するとした回答者（n＝492）に対し、「具体的にどのようなサイバーセキュリティ関連法を確認しているか」と質問したところ、「サイバーセキュリティ関連法（インシデント報告）」が最も多く81%、次いで「データ保護法（例：GDPR[1]、CCPA[2]など）」が70%、「その他のサイバーセキュリティ関連法」41%となりました（図表16：右）。

インタビューした企業においても、確認するとした法規制では、GDPRやCCPAなどプライバシー関連法を挙げ、さらには、顧客の求める法規制の動向や、米国でビジネス展開をする企業においては米国証券取引委員会（SEC）のセキュリティ規則や米国国防分野などで求められる認証の動向を追っていることが分かりました（図表17）。中でも、契約するITシステム企業がビジネス領域（例えば、金融業）の各州法を順守しているかは不明な場合があり、契約書に盛り込むよう注意している企業も確認できました。海外の委託先と契約する場合は、委託先の規制順守状況も確認する必要があると言えそうです。

1 一般データ保護規則
2 カリフォルニア州消費者プライバシー法

図表17：インタビューにおける、確認するとしたサイバーセキュリティ関連法

	確認するとしたサイバーセキュリティ関連法
A社（インフラ）	1)データ・プライバシーに関する規制 欧州であればGDPRなどです。特にポリシー、データの所在、データの取り扱い、ユーザーへの通知やそのタイミング、利用方法について理解を深めます。 2）認証（欧州・北米において、軍事系は特に） いくつかの業界の団体の認証であったり、重要インフラであったり、軍事・防衛関連のシステムについては、特定の認証を要件として示されることがあります。 3）テクノロジーデータに関する規制 一部のテクノロジーデータの取り扱いは、ローカルを使わなくてはならず、クラウドで使ってはいけないことになっています。また地理的な制限が入ることもあります。 4）顧客企業が求める法規制 北米や欧州では、顧客企業が機密情報の取り扱いを気にする場合は、追加で関連する法規制も追う必要があります。
B社（金融）	大きく3点あります。 1）SECのインシデント報告義務 2）プライバシー関連法（GDPRやカリフォルニア州独自のプライバシー法〈CCPA〉） 補足：州独自のプライバシー法があるため、米国の法律に明るい弁護士からアドバイスをもらう体制を整えています。 3）ビジネス領域における州の規制 州によってはセキュリティ情報のトラッキングを求めることもあります。 補足：取引先企業が参照する法規制がそれぞれ異なるため、契約書に盛り込むことが重要です。 例えばITシステム企業は必ずしも私たちのビジネス領域である金融業界の法規制を順守しているわけではないため（テクノロジーに関するものはしていると思うが）、私たちのビジネス領域における州の規制を順守しているかは分かりません。このため、必要な法規制について、セキュリティ要件などを契約に記載する必要があります。 なお、州の規制なので流動的に変わることを意識し、トラッキングすることが重要です。特にAIについて変わることが多いです。
C社（金融）	当社では以下個人情報保護関連の法規制動向を追っています。 1）GDPR 2）各国の消費者保護の法規 補足：米国在住の顧客に対し、米ドルで返金する場合、米国当局規程・プロセスを守らないと、米国当局から指摘を受ける恐れがあるため注意が必要です。

出所：PwC作成

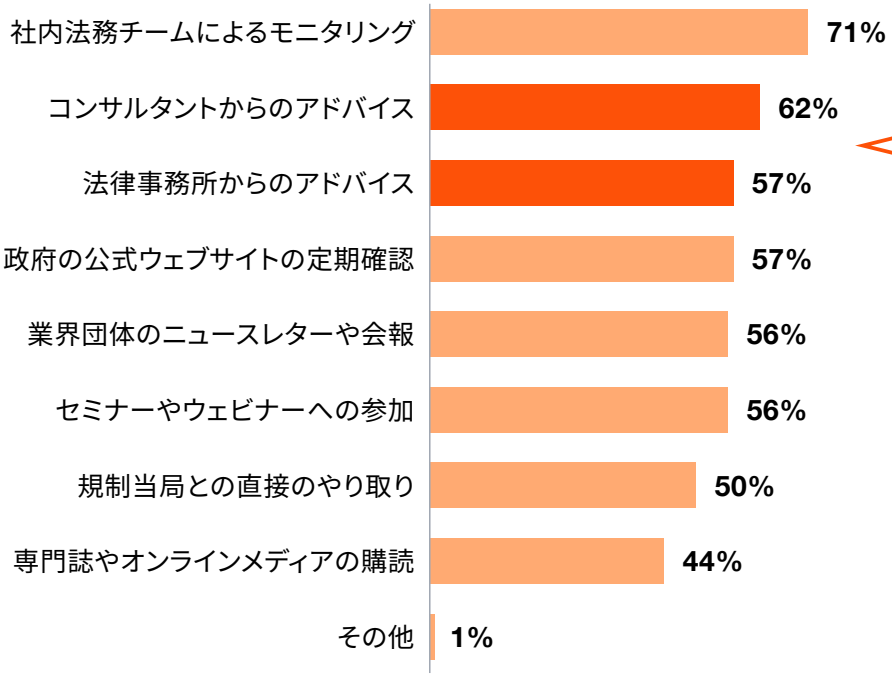
傾向11 セキュリティ関連法動向の把握手法について自社専門部門だけでなく「コンサルタント」や「法律事務所」など、外部専門家をうまく活用する割合が上位

では、企業はどのようにサイバーセキュリティ法規制を確認しているのでしょうか。

サイバーセキュリティ関連法の確認を行っているとするインシデント経験企業（n＝492）に、「サイバーセキュリティ関連法の動向をどのように確認しているか」を確認しました。結果は「社内法務チームによるモニタリング」が71%で最も高く、次いで「コンサルタントからのアドバイス」62%、「法律事務所からのアドバイス」および「政府の公式ウェブサイトの定期確認」が各57%となり、国内企業は自社専門部門に加えて技術や法律などさまざまな分野を考慮したアドバイスを可能とするコンサルティング会社や法的な知識に特化した法律事務所などの外部専門家も活用している実態が明らかになりました（図表18）。実際にインタビュー調査においても、法律事務所だけでなく、コンサルティング会社に動向調査を依頼する海外企業も複数確認できています。コンサルティング会社に動向調査を依頼する理由として、「法規制の知見」だけでなく「テクノロジーの知見（実装・運用・インシデント対応経験などを含む）」を有することから両領域から相談・アドバイスが受けられることを利点として挙げています。

図表18：サイバーセキュリティ関連法の確認方法

サイバーセキュリティ関連法を確認するとしたインシデント経験企業（n=492）｜複数回答



半数以上の企業が、自社専門部門だけでなく、「コンサルタント」や「法律事務所」など、外部専門家をうまく活用し、セキュリティ関連法の動向を把握していることが分かる

インタビュー

法律事務所ではなく、コンサルティング会社に動向調査を依頼する理由は「法規制の知見」だけでなく「テクノロジーの知見（実装・運用・インシデント対応経験など含む」を有するため、両領域からのアドバイス提案がなされるためである

Q. あなた、またはあなたの勤務先では、「法規制の動向」について、どのように確認しますか？あてはまるものを全てお選びください。

出所：PwC作成

取引先(サプライチェーン)を持つ企業への推奨事項

本調査から、「取引先のサイバーインシデントに起因する『ビジネス上の紛争リスク』11の傾向」を示しました。これらの傾向を受けて、サプライチェーンを持つ、特に海外の取引先やビジネス展開をする国内企業は、以下3点を実施することを推奨します。

・サプライチェーンの取引状況や共有する機密情報の現状把握

取引先企業(必要に応じてシャドーIT・クラウド・AIなども含む)を特定し、取引先企業が取り扱う自社の機密データの在りかを定期的に棚卸し

・ビジネス上の紛争リスクに備えた委託先選定・契約・運用となっているか見直し

企業間のビジネス上の紛争リスクが海外だけでなく国内でも顕在化しているため、リスクに備え、契約書の別紙などに具体的なセキュリティ要件を記載、責任範囲や損害賠償上限、当事者間の合意事項の書面化に加え、セキュリティ教育やセキュリティ監査の実施などを見直すこと

国内においては、契約書だけでなく、RFP、提案書など含めた全体で評価し、契約書に未記載だったとしても専門性責任を認めた判例もあることから、提案の段階から表現について、問題ないか社内法務部門に確認をとること

ユーザー企業委託先担当窓口に対し、サイバーリスクに関する合意事項について、日々のコミュニケーションで発生した場合は議事録など証跡として残すことを教育・徹底させること

ビジネスを展開し、かつビジネス上の紛争リスクの高い国において、プライバシー、セキュリティまたはテクノロジーに明るい弁護士との契約を検討すること

・国内外の「サイバーセキュリティ関連法規制」のモニタリング

海外委託先企業や海外にビジネス展開する場合は、定期的なセキュリティ関連法規制を確認し、必要に応じて契約書などに反映すること

特にセキュリティ関連法規制の動向把握方法については、各国政府や主要な業界団体主催の検討委員会などへ積極的に参加することも重要。参加が難しい場合には早期に意図を汲み取れる仕組みを作ること(規制動向を事前に把握することで企業は時間に余裕をもって対応でき、さらに規制に対し実務目線での落としどころを提案する機会があるため)

インシデント発生後には、各国法規制へ適切に対応できるよう平時より備える(インシデント報告先となる対象国の当局連絡先や報告期限、報告フォーマットの整理)

特に製造業においては、生産国／仕向国も考慮して法規把握が重要

調査概要

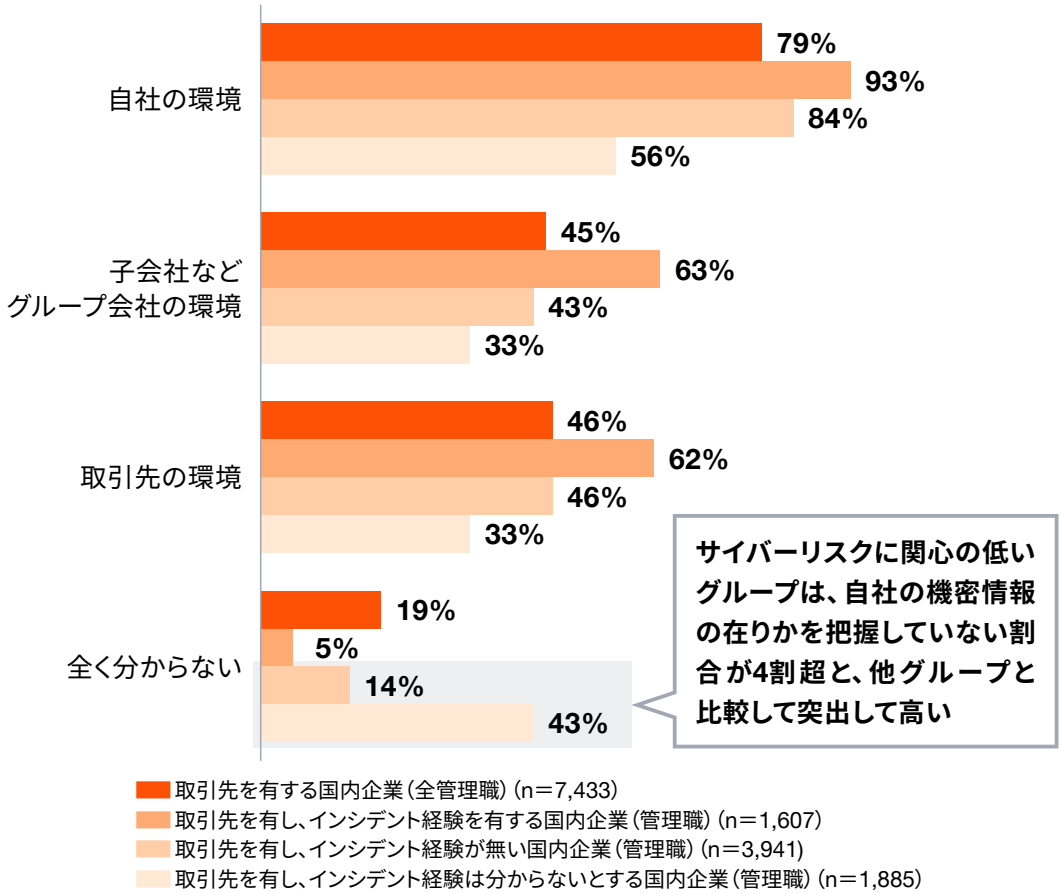
調査名	取引先のサイバーインシデントに起因する「ビジネス上の紛争リスク」に関する調査
調査対象	アンケート調査 国内企業における以下業務従事者 課長職以上の管理職および経営層（12,074名） 課長職以上の管理職および経営層かつ、現職において、インシデント経験者（1,052名） インタビュー調査 国内外企業のサイバーセキュリティ責任者であって、インシデント起因とする紛争対応経験者（3名） 弁護士であって、インシデント起因とする紛争対応経験者（3名）
調査方法	インターネットによるアンケート調査、および有識者へのインタビュー調査
調査期間	アンケート調査：2025年6月10日～6月13日 インタビュー調査：2025年5月～6月
回答者数	アンケート調査：12,074名（分析軸：インシデント経験企業1,052） インタビュー調査：6名（セキュリティ関連の紛争担当経験のある国内外企業のセキュリティ責任者および弁護士など）

その他データ

■ サイバーリスクに対する関心が低い一部管理職グループは半数が機密情報の所在が「全く分からない」と回答

図表19：自社の顧客情報や機密情報の在りかの把握状況（インシデント経験有無比較：管理職）

自社の顧客情報や機密情報の在りかの把握状況｜複数回答



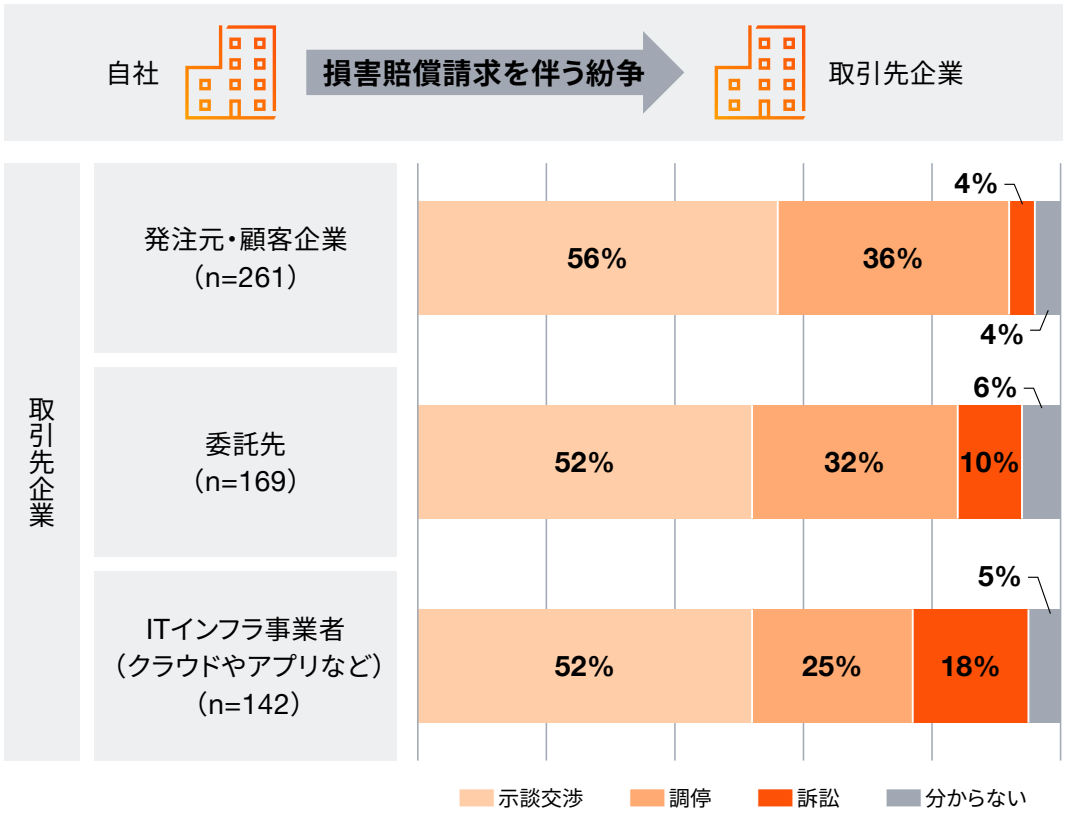
Q. あなたの勤務先が保有する「顧客情報」や「機密情報（製品の開発情報など）」は、どこに格納されているかお知らせください。あてはまるもの全てお知らせください。

出所：PwC作成

■ 自社から提起した損害賠償請求を伴う紛争

図表20：紛争の終結手段（自社から提起した損害賠償請求を伴う紛争）

紛争の解決手段｜複数回答



取引先（発注元、委託先、ITインフラ提供企業など）において、6割程度が示談交渉で和解しており、調停が3割程度存在。訴訟に発展したのは1割未満

Q. 現在の勤務先において、業務に影響のあるサイバーインシデントを経験された方に伺います。情報セキュリティ事故に起因した「損害賠償請求など」の紛争（もめごと）について、最終的にはどのように解決しましたか？

出所：PwC作成

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、監査およびブローダーアシュアランスサービス、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13,500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、クライアントが複雑性を競争優位性へと転換できるよう、信頼の構築と変革を支援します。私たちは、テクノロジーを駆使し、人材を重視したネットワークとして、世界136カ国に364,000人以上のスタッフを擁しています。監査・保証、税務・法務、アドバイザリーサービスなど、多岐にわたる分野で、クライアントが変革の推進力を生み出し、加速し、維持できるよう支援します。

発刊年月：2025年11月　　管理番号：I202507-06