ALLIANCEBERNSTEIN®

知の広場
Knowledge Forum

企業のサイバーセキュリティを見極める
～なぜ優れたガバナンスが必要か～

2023年1月20日

ダイアナ・リー
アライアンス・バーンスタイン・エル・ピー
コーポレート・ガバナンス　ディレクター
責任投資　ESGアナリスト

ハッカー攻撃やデータ漏えいの増加により、サイバーセキュリティやデータセキュリティはあらゆる組織にとって最優先課題となっている。投資家は、デジタル化された世界で企業がデジタルな防御能力の向上に取り組む中、ガバナンスの問題や増大するビジネスリスクについて把握する必要がある。

サイバーセキュリティやデータセキュリティは、幅広い業界で大きなテーマとなっている。脅威の高まりにより、企業は攻撃を受けた場合の被害を最小限に食い止めるため、防御能力や態勢を常に見直さざるを得なくなっている。サイバーセキュリティへの備えに関する企業の公式な説明が、実際の実力以上に誇張されていることも多い。

企業の意識とは裏腹に、多くの投資家にとってサイバーセキュリティの優先順位は高くない。特に、ガバナンスの問題が環境、社会、ガバナンス（ESG）の重要な要素であることを踏まえれば、それは間違いだとアライアンス・バーンスタイン（以下、「AB」）は考えている。サイバーリスクへの備えが整っていない企業は、財務上の損失や罰則、または評価の落ち込みによって事業やブランドが損なわれることで、株式や社債のリターンも打撃を受ける恐れがある（モーニングスターのレポートご参照）。ABは投資家にサイバーリスク管理の評価に

当資料は、アライアンス・バーンスタイン・エル・ピーのCONTEXTブログを日本語訳したものです。オリジナルの英語版はこちら。

関するガイドラインを提供するため、さまざまな分野のサイバーセキュリティの専門家から知見を得るとともに、規制の状況について調査を行った。

エスカレートする攻撃がもたらす損失

サイバー攻撃は非常に高いコストをもたらす。サイバーセキュリティ企業のソニックウォールによると、2022年上半期に、世界で少なくとも28億件のマルウェア攻撃が報告された。これはそれまでの12カ月間の件数を11%上回る規模だ。

ポネモン・インスティチュートとIBMセキュリティの調査によると、データ漏えいによる1件当たりのコストは2022年に世界平均で440万米ドルと、過去最高に達した。復旧に要するコストは、企業のシステムの性能やリモートワークが要因かどうかなどによって異なる。

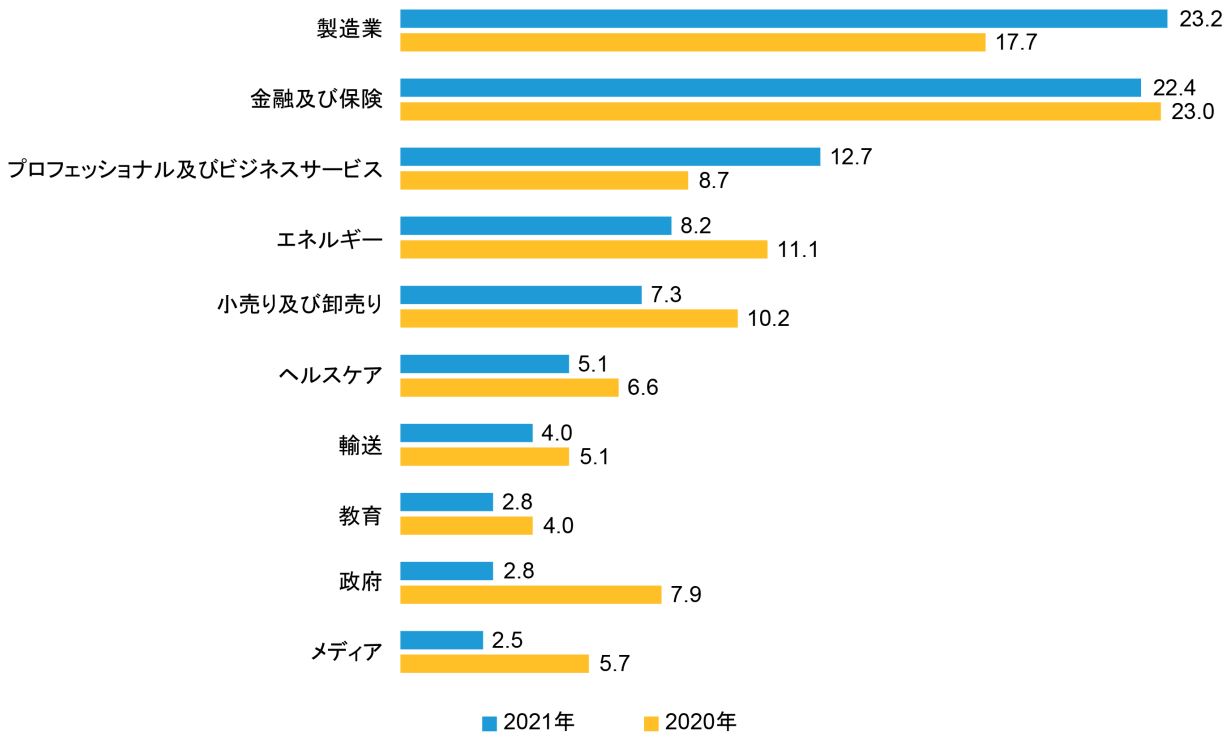
業界によってリスクは異なるものの *(図表)*、オンライン化が進んだ今日の世界では、安全でいられる企業はどこにもない。そしてリスクの増大は規制強化を招いている。米国だけでも、この1年間に「SECサイバーセキュリティ規則」、「重要インフラに関わるサイバー事故報告法」、「2021年ランサムウェア及び金融安定化法」の3つの規制が新たに制定された。一方、ロシアとウクライナの戦争で国家が関与したサイバー攻撃が急増し、各国政府は厳戒態勢を強めている。こうした環境変化の中で、企業はこの問題を無視できなくなっている。

企業にとって何が最大の課題か？

多くの企業は、自社の施設で管理するデータセンターやセキュリティをクラウドベースのソリューションに移行することでリスクに対処している。そのペースが加速しているが、クラウドベースのセキュリティは新たな懸念を生み出している。

インフラの構築：企業は2つの大きなジレンマに直面している。それは、数多くのセキュリティ・プロバイダーやベンダーの中から選択しなければならないことと、それらを管理しなければならないことだ。さまざまなクラウド・セキュリティ・プラットフォームを導入しているあるベンダーは、端末からクラウド・システムまで、さまざまなソリューションを一括で管理する単一のダッシュボードを設けることが共通の課題だと指摘している。同じようなオプションがあまりに多くあることも、一部の企業を困惑させている。彼らはまずインフラを構築した後に随時アップデートするよりも、はじめから完璧に適合するものを作り上げるために時間をかけすぎている。

【図表】　サイバー攻撃と無縁の業界はない
世界全体で攻撃を受けた業界トップ10（%）



過去の実績や分析は将来の成果等を示唆・保証するものではありません。
2021年12月31日現在
出所：IBM Security X-Force

システムの監視、トレーニング、ガバナンス：インフラが完成した後は、システムを監視・運用するための適切なトレーニングを受けたスタッフや、システムの整合性を維持するためのガバナンスが必要となる。さまざまな社内システムとセキュリティ・ベンダーの製品を適切に組み入れるには、時間とリソースが必要になる。また、大手セキュリティ・プロバーダーの多くが小規模な競合他社を積極的に買収しており、統合した管理を維持するのが難しくなる可能性があることも、問題をさらに複雑化している。

サイバーセキュリティに関する強力なガバナンスを作り上げるには何が必要なのだろうか？まず、監督の責を負う取締役委員会への透明性のある報告体制が不可欠で、サイバーセキュリティに関する専門知識を持たない取締役でも容易に理解できる平易な言葉を用いて報告しなくてはならない。同様に、「高、中、低」のリスクに分類したシンプルなマトリックスや、緩和措置に関する報告書や脅威の分類も役に立つ。ガバナンスが成熟するのに伴い、法務責任者、取締役会、ビジネスマネジャーは、情報セキュリティチームとより頻繁に協議する必要が生じる。監督の対象は、システムを運用・監視する従業員まで広げなくてはならない。また、企業は、普及しているサービスであるほどサポートが可能な専門家が多いことなどを踏まえ、選択するベンダーの重要性を認識する必要がある。

コストの上昇：多くの最高情報責任者（CIO）は我々に対し、コストに頭を悩ませていると明らかにした。場合によっては、エンジニアが1台のサーバーに1つの変更を加えるだけで、システム全体のコストが著しく増加することもある。しかも、多くのベンダーは強力なサイバーセキュリティ・インフラの監視や維持に要する将来的なコストの上昇について明確な概要を示していない。特にサイバー専門のリソースが少ない企業は、従業員の増加に目を配り、将来を見越したインフラコストに関するモデルを作成することで、こうした落とし穴を避けることができる。サイバー保険のコストも要因の一つで、新しいベンダーが追加されたり、システムが更新されたりすると保険金が減額されたり、補償範囲が狭くなることがある。例えば、ロイズ・オブ・ロンドンは最近、国家が関与したサイバー攻撃に備えた保険の販売を停止すると発表した。

投資家はサイバーリスク管理をどう評価すべきか？

投資家は企業のサイバー戦略や行動を評価するため、予算に目を配りつつ、適切な質問を投げかける必要がある。例えば、サイバー問題はどのように取締役会に報告されるのか？リスクはどのように監視され、エスカレーションされているか？どのようなシステムテストや対応プランが策定されているか？従業員は攻撃に備えているか？といった問いかけである。

取締役や経営陣と対話することで、サイバーリスクに関する知見について重要な確証を得ることができる。最近のエンゲージメントでは、リスクを強く意識している企業ほど、このテーマについて積極的に議論し、ガバナンス、報告、トレーニングに関する詳細な情報を提供してくれる。曖昧で一般的な回答は、脅威に対する備えが不十分で、同業他社に遅れをとっており、攻撃に対して脆弱であることを示している可能性がある。サイバー予算も、戦略や行動に関する重要な情報を提供してくれる。サイバー保険、リソース管理、ベンダー、社内システムのための支出に関する透明性は、全体像を把握するうえで役に立つ。

複雑な脅威に対処する一貫した戦略

脅威が増大する中、企業は攻撃に対抗し、データやシステムを保護するための取り組みを強化する必要がある。中小規模の企業の多くはサイバーセキュリティへの取り組みが比較的初期段階にあり、攻撃を受ける可能性のあるシステム上の課題を抱えているため、より重大なリスクにさらされる恐れがある。

投資家はあらゆる規模の企業についてサイバーシステムの導入状況を精査し、セキュリティに関するガバナンス、リソース管理、報告体制について掘り下げて分析する必要がある。それぞれの分野で一貫した戦略があれば、企業はサイバー攻撃を食い止めるとともに、それに対処する準備を整えることができる。これらの問題について経営陣と定期的に話し合うことで、投資家は、企業のサイバーセキュリティへの対応状況をポートフォリオ組み入れ候補や保有株式の幅広いリスク評価に取り入れることが可能になる。

アライアンス・バーンスタイン株式会社

金融商品取引業者 関東財務局長(金商)第303号
【加入協会】 一般社団法人投資信託協会／一般社団法人日本投資顧問業協会／日本証券業協会／
一般社団法人第二種金融商品取引業協会
https://www.alliancebernstein.co.jp

当資料についての重要情報

当資料は、投資判断のご参考となる情報提供を目的としており勧誘を目的としたものではありません。特定の投資信託の取得をご希望の場合には、販売会社において投資信託説明書(交付目論見書)をお渡ししますので、必ず詳細をご確認のうえ、投資に関する最終決定はご自身で判断なさるようお願いします。以下の内容は、投資信託をお申込みされる際に、投資家の皆様に、ご確認いただきたい事項としてお知らせするものです。

- 投資信託のリスクについて

  アライアンス・バーンスタイン株式会社の設定・運用する投資信託は、株式・債券等の値動きのある金融商品等に投資します(外貨建資産には為替変動リスクもあります。)ので、基準価額は変動し、投資元本を割り込むことがあります。したがって、元金が保証されているものではありません。投資信託の運用による損益は、全て投資者の皆様に帰属します。投資信託は預貯金と異なります。リスクの要因については、各投資信託が投資する金融商品等により異なりますので、お申込みにあたっては、各投資信託の投資信託説明書(交付目論見書)、契約締結前交付書面等をご覧ください。

- お客様にご負担いただく費用:投資信託のご購入時や運用期間中には以下の費用がかかります
  - 申込時に直接ご負担いただく費用 …申込手数料　上限3.3%(税抜3.0%)です。
  - 換金時に直接ご負担いただく費用…信託財産留保金　上限0.5%です。
  - 保有期間に間接的にご負担いただく費用…信託報酬　上限2.068%(税抜1.880%)です。

その他費用…上記以外に保有期間に応じてご負担いただく費用があります。投資信託説明書(交付目論見書)、契約締結前交付書面等でご確認ください。

上記に記載しているリスクや費用項目につきましては、一般的な投資信託を想定しております。費用の料率につきましては、アライアンス・バーンスタイン株式会社が運用する全ての投資信託のうち、徴収するそれぞれの費用における最高の料率を記載しております。

ご注意

アライアンス・バーンスタイン株式会社の運用戦略や商品は、値動きのある金融商品等を投資対象として運用を行いますので、運用ポートフォリオの運用実績は、組入れられた金融商品等の値動きの変化による影響を受けます。また、金融商品取引業者等と取引を行うため、その業務または財産の状況の変化による影響も受けます。デリバティブ取引を行う場合は、これらの影響により保証金を超過する損失が発生する可能性があります。資産の価値の減少を含むリスクはお客様に帰属します。したがって、元金および利回りのいずれも保証されているものではありません。運用戦略や商品によって投資対象資産の種類や投資制限、取引市場、投資対象国等が異なることから、リスクの内容や性質が異なります。また、ご投資に伴う運用報酬や保有期間中に間接的にご負担いただく費用、その他費用等及びその合計額も異なりますので、その金額をあらかじめ表示することができません。