セキュリティおよびリスク管理のプロフェッショナル向け

The Forrester New Wave™：サイバーセキュリティリスクレーティングプラットフォーム、2021年第1四半期

主要プロバイダ7社とその状況

執筆者：Paul McKay、Alla Valente
共同執筆者：Joseph Blankenship、Shannon Fish、Peggy Dostie
2021年2月25日

目次

関連する調査ドキュメント

Cybersecurity Risk Ratings Market Outlook, 2020 And Beyond（2020年以降のサイバーセキュリティリスクレーティング市場の展望）

The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018（The Forrester New Wave™：サイバーセキュリティリスクレーティングソリューション、2018年第4四半期）

レポートを同僚と共有しましょう。
調査共有を使用してメンバーシップを有効活用しましょう。

FORRESTER®
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax：+1 617-613-5000 | forrester.com

サイバーセキュリティレーティングは成熟の途上にある

サイバーセキュリティリスクレーティング（CSR）市場は、信用格付の市場から影響を受けています。CSR市場のソリューションは、企業のオンラインにおける対外的プレゼンスについての社外調査によるデータに基づき、複数のセキュリティリスク要素にまたがる企業のサイバーセキュリティのあり方を一元的に集約して評価します。プラットフォームが収集したデータは、企業のセキュリティへの取り組み姿勢と実際の調査結果の比較について、サードパーティや社内関係者が申告した内容を企業が検証するために活用できる点に価値があります。こうしたソリューションが活用される最も一般的なユースケースとして、サイバーセキュリティの信用度調査やサードパーティリスク管理（TPRM）の継続的モニタリング、全社的セキュリティリスク管理とベンチマーキング、M&A適正評価、経営幹部層のコミュニケーション、サイバー保険契約の引受などがあります。

2018年に発行された前回のForrester New Wave™以降、CSRの多数のプラットフォームによりレーティング精度、アセットアトリビューション、ワークフローなどさまざまな改善が見られました[1]。しかし、市場はまだ成熟したとは言えません。市場が成熟し企業が採用するに足るセキュリティソリューションとして完成を見るためには、なおもいくつかの課題が残っています。今回の調査では、以下のようなことが明らかになりました。

- **CSRプラットフォームの精度の評価は、必ずしも企業のサイバーリスクを反映していない。**今回の調査対象となったベンダーの多くは、アセットアトリビューションに特化した精度評価を行っています。すなわち、アセットを適切な組織に正しく紐付けられているか、という観点です。ベンダーはモデルのレビューを外部機関に委託し、外からの視点で評価を行っています。ただし正確なアセットアトリビューションは重要ではあるものの、そうしたレーティングそのものが企業の現在のセキュリティのあり方を正しく反映していると統計的に確信できるわけではありません。レーティングベンダーは、モデルに使用されるセキュリティデータポイント、変数の重み付け、分析の種類、機械学習モデルの訓練と検証の方法についても、真のリスクを正しく想定したものであるかをさらに詳細に検証する必要があるのです。
  また、自社のモデルについて内部でレビューするだけでなく外部の検証も受けることで、レーティング市場が提供する価値に対し、さらなる自信を持つことができるようになります。

- **ベンダーのモデルやアルゴリズムの透明性の水準がまちまちである。**透明性については前回のForrester New Waveより改善されたものの、CSR企業が解決すべき課題はまだ多くあります。顧客にのみ開示するために多くの情報を秘匿し、他社に比べて詳細情報を公開しない企業もあれば、誰でも確認できるよう自社の手法をホワイトペーパーやポータルで詳細に開示する企業もあります。過誤検知の申告のプロセスに関する透明性が、改善の鍵となる領域です。こうした領域は主にCSR企業が自社内で対処しますが、こうした対応はセキュリティ業界の他企業からCSR企業が「神のように振る舞っている」と批判される事態にもつながります。CSRレーティング企業は自社の過誤検知の申告手順に関する透明性の水準を改善し、企業間の紛争を独立した立場から公平的に見ることのできる業界のオンブズマンを導入し、紛争の結果を公開する努力をする必要があります。

- **ベンダーは関連性の高いセキュリティソリューションとの連携を進める必要がある。**CSRソリューションは主に2つのユースケースに利用されています。CSRソリューションの提供するさらなるデータと継続的な監視機能により、企業が自社のセキュリティのあり方と、サードパーティのエコシステムのセキュリティのあり方の両者の評価を実施できるのです。ベンダーの連携へのアプローチは各社で異なっています。自社のワークフローエンジンやクエスチョネアモジュールを構築している場合もあれば、主要なGRCやTPRMプラットフォーム（また、Splunkなどのセキュリティアナリティクスプラットフォームとも）とネイティブに連携するよう構築されている場合もあります。なかには、十分と言えない品質での連携により、低品質なデータダンプの提供に留まり、サードパーティによるセキュリティレビューや全社的リスク管理といったより幅広いビジネスプロセスの観点でデータのさらなるコンテキストやインサイトを実現する機会を逸しているベンダーもいます。