RSA

サード パーティー リスク向け RSAリスク フレームワーク

サード パーティーとの関係から生じるリスクをコントロールする組織の能力を成熟させます

世界中の組織がデジタル トランスフォーメーションを推進する中、新しいテクノロジーが急速に採用され、業務プロセスの統合が進んでいます。デジタル トランスフォーメーションは、効率性と柔軟性をもたらし、より革新的で優れた製品とサービスの提供を可能にします。その一方で組織は、サイバー リスクとデジタル リスクの新しいクラスが出現したことを認識しています。デジタル トランスフォーメーションは、セキュリティ、アイデンティティー、およびリスクの従来の課題に根ざしているものの、それらの課題の規模、複雑さ、結果が拡大する原因となっています。

RSAは、組織がこれらのリスクを管理する能力を向上させるのを支援するため、RSAリスク フレームワークを開発しました。RSAリスク フレームワークは、サイバー インシデント リスクとサード パーティー リスク、動的ワークフォースとマルチクラウド トランスフォーメーションなど、デジタル トランスフォーメーションの影響を受ける特定の領域での成熟度を最適化したいと考えている組織向けのアドバイザリー契約です。RSA Risk & Cybersecurity Advisory Practice（RCAP）によって提供されるリスク フレームワーク契約では、数千件に及ぶ過去の契約を通じて開発されたサイバーセキュリティとリスク管理のための実証済みベスト プラクティスに基づく、高度なアセスメント ツールが活用されます。お客様は、ギャップ分析および成熟度を高めるためのロードマップを使用して、サイバー リスクに対する自分の組織の成熟度の現状を把握することができます。

デジタル トランスフォーメーションの最大の影響の1つは、企業とそのパートナー（データ ソースを含む）の間の潜在的なやり取りの数が急増していることです。相互のつながりとアウトソーシングが盛んに行われる今日の動的環境では、企業が組織内部のリスクのみに集中するだけでは不十分です。企業は、パートナー、クラウド プロバイダー、ソフトウェア ホスティング会社、サービス プロバイダー、その他のデータ パートナーなどのサード パーティーからなるエコシステム全体でリスクを管理する必要があります。

図1：RSAサード パーティー リスク フレームワーク（概略図）

サード パーティー リスク向けRSAリスク フレームワークは、ビジネス中心のコンサルティング モデルを促進して、内部および外部の両方のエコシステム全体でリスクを管理する組織の現在の対応状況を評価できるようにします。これによって多大な成果が得られる可能性があります。サード パーティー エコシステムにおけるデータ リスクを調査したPonemon Instituteの2018年の報告書では、回答者の42%が過去12か月にサード パーティーによるデータ侵害があったと報告し、さらに22%はそのような侵害に遭ったかどうかわからないと答えました[1]。

RSAサード パーティー リスク フレームワークは、リスクとサイバーセキュリティの分野におけるRSA独自の専門知識に基づいており、組織の制御が及ばないが、効果的なパフォーマンスのために管理する必要のあるデジタル脅威から企業を保護するという、難しいが重要なタスクを対象としています。この委託調査では、ITセキュリティとビジネス リスクの担当者の69%が、「ビジネス リスクとITセキュリティの間の関係を調整するのは難しい」という記述に対して、同意または強い同意の姿勢を示しました。さらに、「セキュリティ侵害の検出とセキュリティ侵害への対応に必要なITおよびビジネス リスク管理スキルの点で組織になんらかの弱点がある」という記述に対しては、同意または強い同意の姿勢を示した回答者が60%以上に達しています[2]。

サード パーティー ガバナンス向けRSAリスク フレームワークは、組織がリスク管理の各カテゴリー、つまり、エコシステム、契約、アイデンティティーとガバナンスにおける成熟度を自己評価し、それを向上させるのを支援します。RSAは、これらの各領域について、独自のサード パーティー リスク定量化ツールを適用することで、サード パーティー リスクにおける企業の成熟度プロファイルに加え、理想状態プロファイル（リスク管理ライフサイクル全体にわたるサード パーティー ガバナンス成熟度ステータスの長期目標）を生成します。現状と理想状態を比較すると、組織が要改善領域に優先順位を付けるのに役立つギャップ分析が作成されます。

RSAリスク フレームワークがすべてそうであるように、Cyber Risk Practiceでは、CEO、COO、CCO、CIOなどの経営幹部の視点をサポートする成熟度モデルを使用して、組織の従来の職能的境界にとらわれないアプローチで、このリスクを管理するための企業の現在の対応状況を評価できます。

RSA Third Party Risk Assessmentでは、以下のサービスが提供されます。

- ビジネス部門の目標、目的、既存のリスク状況を深く理解するための、ビジネス部門の主要な関係者を対象としたインタビューとドキュメント化
- 企業のエコシステム全体の成熟度のベースラインを設定するための、RSA独自のサード パーティー リスク成熟度定量化ツールの管理
- 業界のベスト プラクティスに基づく、サード パーティー ガバナンス成熟度の理想状態と現状のギャップ分析
- 理想状態のサイバー リスク管理成熟度に移行するために利用できるロードマップの開発

RSA GLOBAL SERVICESについて

650名のサイバー セキュリティ ビジネス/テクニカル コンサルタントで構成されるRSA Global Servicesチームは、100か国以上で事業を展開しており、デジタル フォレンジックおよびインシデント対応サービス プロバイダーのForrester Wave™において「Strong Performer」の評価を獲得しています[3]。RSA Global Servicesは、数千件を超える契約業務を通じて、包括的なリスク/セキュリティ管理プログラムを設計して導入することによって、さまざまな種類の組織のセキュリティ保護に貢献しています。

RSA Global Servicesは、高度なビジネス セキュリティ スキルと幅広いリスク管理知識を組み合わせて、組織がサード パーティー ガバナンス成熟度ステータスを評価および改善するのを支援します。RSA Risk and Cybersecurity Practiceでは、次の3つのグループから重要なセキュリティ サービスが提供されます。

- RSA Risk and Cybersecurity Advisory Practice（RCAP）は、サイバー インシデント管理、サード パーティー ガバナンス、データ プライバシー、デジタル ビジネス回復力の分野で、コア ビジネス分析、ビジネス インパクト アセスメント、サイバー リスク アセスメントに焦点を当てたビジネス主導のサイバー セキュリティ サービスを提供します。
- RSA Advanced Cyber Defense（ACD）は、データ漏洩への対応状況を評価するサービス、Security Operations Center（SOC）またはCyber Incident Response Team（CIRT）のアセスメントと設計、インシデント対応の計画とテスト、「エキスパート オンデマンド」サービスを提供します。
- RSA Incident Response（IR）は、事前対応型サービスと事後対応型サービスの両方で、インシデント対応機能の設計、管理、および実行を支援します。RSA IRは、継続的なサービスまたは単発的なサービスで利用でき、組織のセキュリティ スキルを拡張して、あらゆるタイプと重大度のセキュリティ インシデントに対処します。

[1] Ponemon Institute、『Data Risk in the Third-Party Ecosystem』（2018年11月）
[2] ESG Custom Research、『Cybersecurity and Business Risk Survey』（2018年6月）
[3] 『The Forrester Wave™: Digital Forensics and Incident Response Service Providers』（2017年第3四半期）