Gartner

2023年のリーダーシップ・ビジョン

セキュリティ／リスク・マネジメント・リーダーの
戦略的優先課題トップ3

はじめに

今日の組織は、長引くインフレ、希少で高価な人材、そしてロシアによるウクライナ侵攻、新型コロナウイルス感染症によるロックダウン、エネルギー不足によってもたらされた世界的な供給不足により、不確実な状況に直面しています。この 3 つの困難は、世界中のビジネスだけでなく、2023 年のサイバーセキュリティの脅威環境にも直接影響を及ぼしています。

このような困難な時代にサイバーセキュリティ・リーダーとして下す決断は、その企業が不必要なサイバーセキュリティ・リスクを負うか、それとも繁栄に向けてテクノロジ・イノベーションを活用できるかを決めることになります。リーダーとそのチームは、俊敏に方向転換できなければなりません。

2023 年に経済の不確実性と逆風が予想されているにもかかわらず、最高情報セキュリティ責任者 (CISO) への調査結果からは、現在の計画ではサイバーセキュリティへの投資を継続する予定であることが分かります。また、テクノロジに関する意思決定の民主化が進むにつれて、サイバーセキュリティ・リスクも高まっています。

優れた CISO は、新しいアイデアを試す勇気を持っています。CISO は、自身の能力を高め、企業文化の変革を推進することに注力し、サイバージャッジメントの導入を支持する必要があります。

企業がイノベーションを起こし、競合他社と差別化するためのテクノロジへの投資を続ける中、セキュリティ／リスク・マネジメント (SRM) リーダーは、リスクの測定と管理を徹底するとともに、セキュリティのベスト・プラクティスについて、新たに企業全体を教育／指導する方法を実行することが求められます。

Gartner のリーダーシップ・ビジョンでは、データ・ドリブンなリサーチに基づいて、注力すべき領域を明確にできるようトップレベルのガイダンスを提供します。Gartner は、さまざまな職務領域に関する詳細な知見をお客様に提供していますが、今回はその抜粋版をご紹介します。チーム・メンバーや他部門のリーダーと討議する機会に、優先課題やアクションをよりスピーディかつ効果的に診断したり、2023 年の戦略プランを策定したりする際に、ぜひご活用ください。

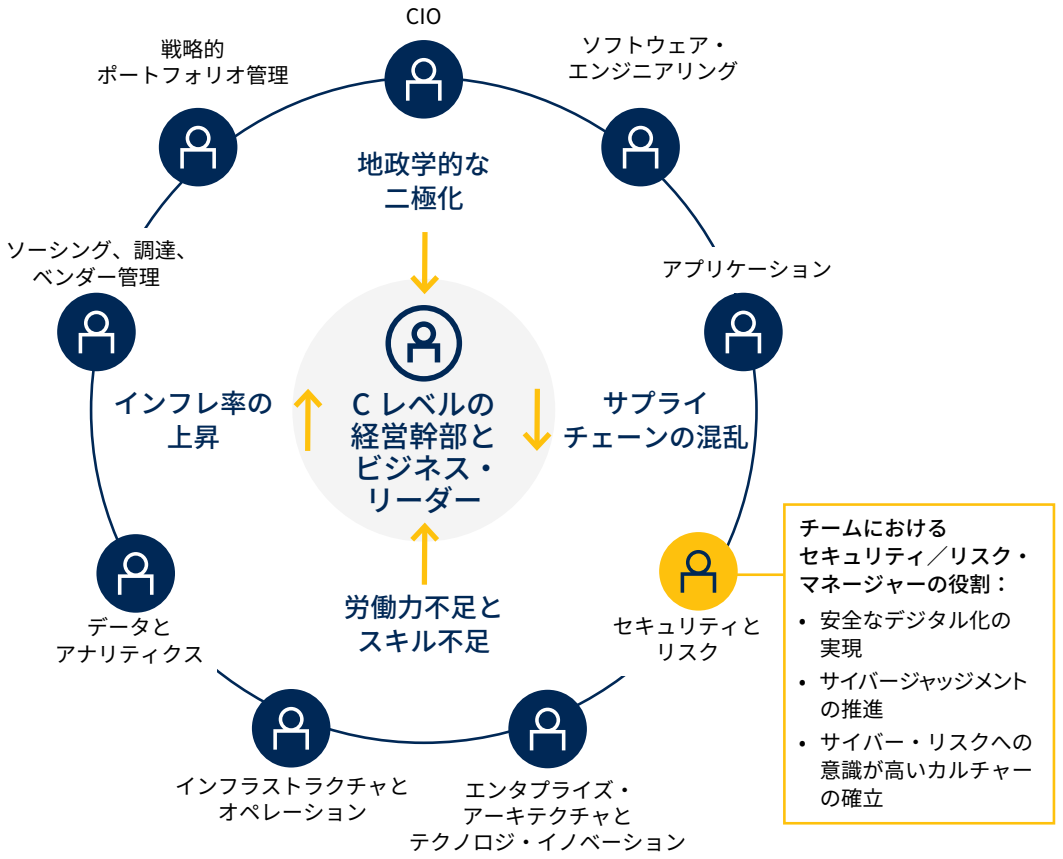
Tom Scholtz
Distinguished VP Analyst

予測不可能なビジネス環境では、チームでの取り組みが必要

SRM リーダーは、複雑化し危険性が増す環境の中で、セキュリティのデジタル化の実現に取り組んでいます。

企業は、予測不可能な状況に対処する一方で、競争上の差別化をもたらす革新的テクノロジを求めているため、当面の間はリスク許容度を高め、セキュリティに投資をすることに前向きです。

社内外の課題を理解し対応するためには、SRM リーダーが組織全体のステークホルダーと連携し、ビジネス・リーダーが十分な情報に基づいて質の高いセキュリティ・リスク判断を下すために必要な知識と能力を身につけることがこれまで以上に重要となっています。



出典：Gartner

SRM リーダーに影響を及ぼす 3 つの主要トレンド

IT部門以外で活動するテクノロジストが増加

デジタル・アクセラレーション (デジタル化の加速) を実現するために、CEO の 67% がビジネス部門におけるテクノロジ・ワークを拡大したいと考えています。このトレンドは、SRM リーダーの直接的な管理下にないチームにおいて、「ビジネス・テクノロジスト」(IT 部門以外の事業部内で、社内外向けのシステムの構築や情報分析といった従来の IT 業務をこなす従業員) が増加することを意味します。

サードパーティのセキュリティ・リスクへの注目の高まり

最近のサイバーセキュリティ・インシデントにより、サプライチェーンの弱点が浮き彫りになっています。2025 年までに、組織の 60% は、情報、システム、インフラストラクチャの侵害を防ぐために、サードパーティとの取引における重要な要因としてサイバーセキュリティ・リスクを用いるようになるでしょう。

サイバーセキュリティ・メッシュが進化

エンドポイント、デジタル市民、IT 資産がどこにでも配置できるのであれば、サイバーセキュリティ・コントロールもそれに追随する必要があります。サイバーセキュリティ・メッシュのアプローチとは、コンポーザブルな分散型ツール／コントロールから成る柔軟性と協調性に優れたエコシステムであり、組織全体および世界中の資産を保護するためにうまく適用されています。

SRM リーダーの課題と実行すべきアクション

1 人的要素に対応する

以前と変わらず、データ侵害の大半には人的要因が絡んでいます。Gartnerの最近の調査では、従業員が、複数のアカウントでパスワードを使い回していたり、送信元不明のメールを仕事用の端末で開いたりするなど、セキュリティ上の危険な行為に、故意に関与していることが明らかになりました。

2 SRMの有効性を高める

現在、ステークホルダーの期待を超えるSRMリーダーは、12%にすぎません。リーダーは、サイバーセキュリティの優先事項を実現する能力を示すために、すべての責任領域において自身の能力を向上させる必要があります。

3 サイバージャッジメントのプロセスを加速させる

SRMリーダーは、組織全体の意思決定者が、SRMチームや自動化に依存することなく、十分な情報に基づいたリスク判断 (サイバージャッジメント) を独自に行えるように支援する必要があります。

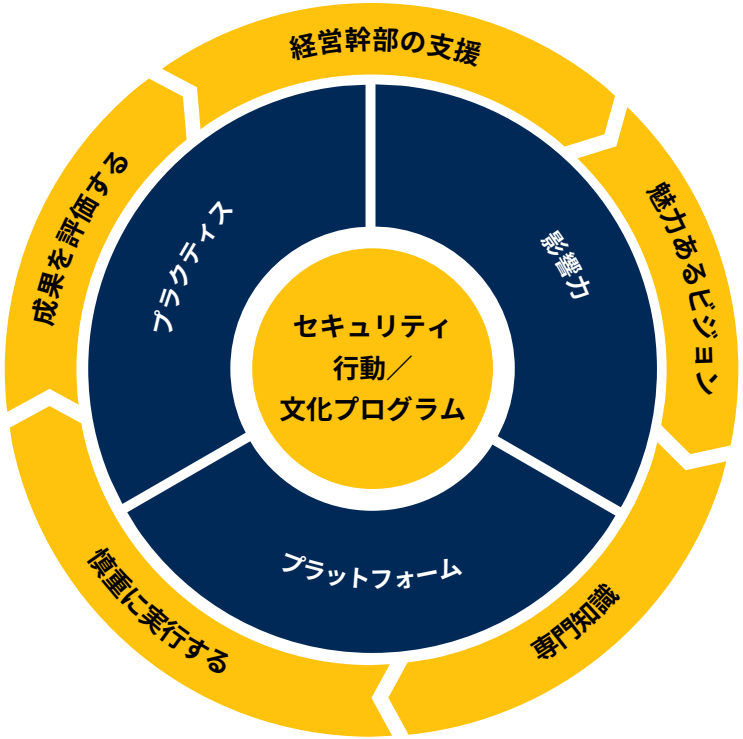
SRMリーダーが実行すべきアクション

GartnerのPIPE (実践、影響、プラットフォーム、実現要素) フレームワークを、セキュリティ行動／文化プログラムを成功させるための指針として活用します。

特定されたカテゴリにおける有効性の向上に注力することによって、ビジネス上の優先課題との整合性を高め、組織のセキュリティを保護します。

自己認証やグループ・トラスト・スコアリングなどの戦略を通じて自律性をサポートし、企業全体のサイバージャッジメントを推進します。

セキュリティ・リスクに関する人的要素を削減する



出典：Gartner

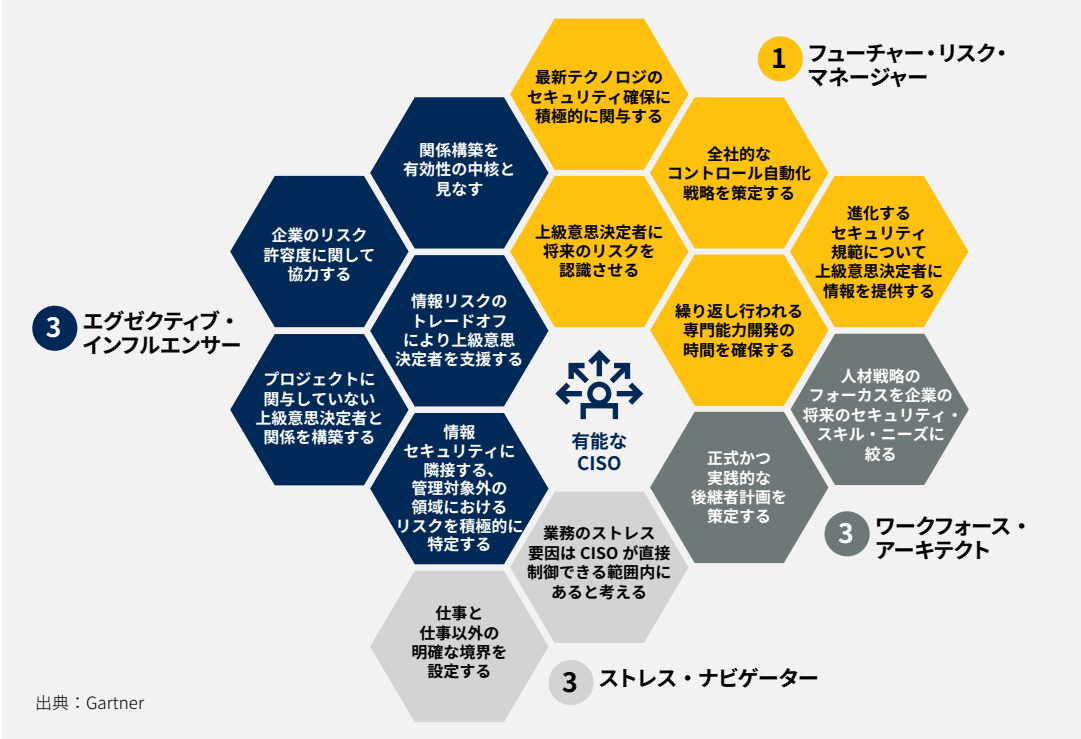
人間の行動がサイバーセキュリティのリスク・レベルに及ぼす悪影響を軽減するには、SRM リーダーは従来とはまったく異なるアプローチでセキュリティ・トレーニング・プログラムを行う必要があります。Gartner の PIPE フレームワークは、その実行の指針となります。また、リーダーは、サードパーティとのインタラクションに関するベスト・プラクティスを策定することによって、デジタル・サプライチェーンのリスクを低減する必要があります。

推奨される次のステップ

1. ユーザー・エクスペリエンスを考慮した制御設計を行う
2. 役割に応じたサイバーセキュリティの学習体験を設計する
3. 組織がどの程度保護されているかを判断するため、成果指向の評価指標に重点を置く
4. サプライチェーン・ベンダーと関わる際に、以下を実行する
   - 共有データ／インフラストラクチャに潜むセキュリティ・リスクを特定する
   - 新たな規制要件を満たしていることを確認する
   - ステークホルダー間で主要なパートナーシップを構築し、共同ガバナンスを展開する
   - 新たなベスト・プラクティスを評価し、導入する

リーダーシップの有効性を高める

SRM リーダーの役割が進化と拡大を続ける中、カテゴリを超えたリーダーシップの有効性を継続的に評価・改善することは極めて重要です。SRM リーダーは、企業価値を高め、企業を保護するために、自らの優先事項をビジネスの優先事項と一致させる必要があります。



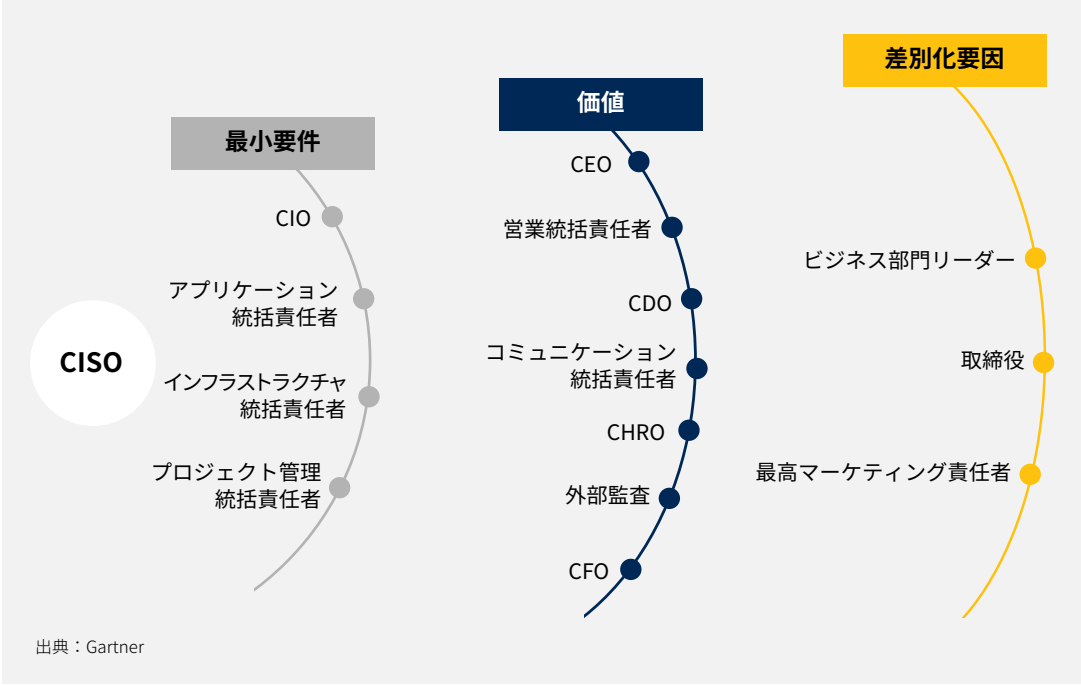
出典：Gartner

推奨される次のステップ

1. IT 部門以外の上級リーダー職との関係を構築する
2. 新しいセキュリティ規範についての最新情報を意思決定者に提供することで、将来のリスクを防御する
3. ビジネスへの AI 活用を積極的に確保する
4. 従業員のパフォーマンスを追跡し、創造的な方法でスキル・ギャップを解消する
5. 仕事とプライベートの境界線を守り、ストレスを管理する

全社のセキュリティ・ケイパビリティを拡充する

SRM リーダーの直接的影響が及ばないグループ単独でのサイバーセキュリティ活動を支援することで、組織全体の能力が高まり、SRM チームはより価値の高い活動に集中できるようなります。サイバーセキュリティ・メッシュ戦略を開始することで、統合システムのセキュリティが強化され、資産が配置されている場所に関係なく、アクセス、設定、データを保護することができます。



出典：Gartner

推奨される次のステップ

1. QP Express* プログラムを通じてリリースされるアプリケーションを自己認証できるように、デリバリ・チームを強化する
2. グループ・トラスト・スコアリングを導入して、サイバーセキュリティ活動を実行できるチームを特定する
3. サイバーセキュリティ・メッシュ戦略を開始して、以下を実行する
   - 導入済みのツールの成熟度を評価する
   - チームの統合能力を調査する
   - 妥当な投資レベルを決定する
   - 独自の統合とオープン・スタンダードの組み合わせ、統合プラットフォーム、階層型コンポーザブル製品、複合的アプローチなど、構築方法を決定する

*Qualification Process Express: Schlumberger 社の DevSecOps プログラムの名称

実用的で客観的な知見

企業の皆様は、以下のようなセキュリティ・リーダーのための リソース／ツールを無償でご利用いただけます。

Webinar

セキュリティ：新たな闘い

ITとセキュリティのリーダーにとって重要となる課題解決のための推奨事項を解説します。

今すぐ視聴

Roadmap

The IT Roadmap for Cybersecurity

レジリエンス、スケーラビリティ、俊敏性に優れたサイバーセキュリティ戦略を構築できます。

今すぐダウンロード (英語)

eBook

サイバーセキュリティ・インシデントへの対応プランに不可欠な3つの事項

インシデントに対する組織の準備能力が向上します。

今すぐダウンロード

eBook

Four Facets of Effective CISO Leadership

トップレベルのリーダーたちが、拡大する自身の権限にどのように取り組んでいるのかをご紹介します。

今すぐダウンロード (英語)

Gartnerのお客様はクライアント・ポータルでさらに多くのリソースをご利用いただけます。ログイン

Gartner

Gartner のコンファレンスに参加して、2023 年の IT 戦略を前進させましょう

2022 年、Gartner は世界中で 34 のコンファレンスを開催し、4 万 6,000 人以上のビジネス／テクノロジ・プロフェッショナルに参加いただきました。Gartner のコンファレンスは、先進的なリーダーが集い、学びを加速させ、意思決定の指針となり、重要なトレンドを把握できる場です。

ぜひご参加ください

今すぐ2023年のコンファレンス・カレンダーで、
最適なコンファレンスを見つけてください。

→ カレンダーを確認する








Connect With Us

ガートナーは、経営幹部およびそのチームに対し、実行可能かつ客観的な知見を提供しています。ガートナーの深い専門知識によるガイダンスやツールは、組織のミッション・クリティカルなビジネス課題についてより迅速でスマートな意思決定を下し、より大きな成果を獲得することを可能にします。

リサーチサービスに関するお問い合わせ

サイバーセキュリティ・リーダーを成功に導くGartnerのサービス
gartner.co.jp/ja/cybersecurity

最新の知見をご確認ください

Gartner