Gartner

2024 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

最高情報セキュリティ責任者 (CISO) は、急速に変化する優先事項、脅威、要求、規制圧力、テクノロジなど、複雑で多岐にわたる課題に直面しています。セキュリティ／リスク・マネジメント・リーダーには、今日のセキュリティ環境に対する体系的なアプローチが必要です。以下の 4 つのステップを踏むことで、2024 年以降の戦略的計画を立てる上での指針となります。

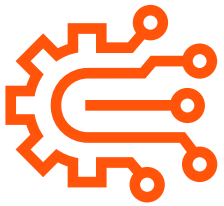
- **ステップ 1：**サイバーセキュリティ・プログラムで直面している主要な緊急課題について意見をまとめます。例えば、以下のような課題が考えられます。
  - CISO 役割の進化に伴うオペレーティング・モデルの変化と、リスク決定の分散化を図りつつ中央での監視を強化する
  - AI に内在するリスクと機会
  - 人間の行動に関連する継続的なセキュリティ上の課題
- **ステップ 2：**緊急課題がサイバーセキュリティ・プログラムのビジョンに反映されていることを確認します。
- **ステップ 3：**重要課題に対処するために必要な具体的なアクションを特定します。
- **ステップ 4：**特定したアクションをサイバーセキュリティ・プログラムに織り込むべく、サイバーセキュリティ戦略を更新します。

セキュリティ／リスク・マネジメント・リーダーは、2024 年以降の戦略プランを策定する際の手引きとして、本 eBook を活用できます。

2027 年までに、**従業員の 75%** が IT 部門の認知範囲外でテクノロジを取得、修正、または構築するようになる **(2022 年の 41% から増加)**

出典：Gartner

セキュリティ／リスク・マネジメント・リーダーに影響を及ぼす 3 つの主要トレンド



サイバーセキュリティの意思決定権の変化

テクノロジの取得／開発／デリバリは、中央集権的な IT 部門から離れ、ビジネス部門や本社部門へと移行し続けています。

このため、セキュリティ／リスク・マネジメント・リーダーは、中央集権的な管理モデルの実行が困難な状況でセキュリティを維持するという難しい立場に置かれています。

さらに、CIO の半数近くが、サイバーセキュリティ・リスクに取り組むことで、デジタル化の実行が妨げられていると考えています。

AI に関するセキュリティの課題

ChatGPT や Bard のような大規模言語モデルを利用したツールは、生成 AI が多くのビジネス・プロセスをどのように形成していくかをいち早く示しています。

生成 AI アプリケーション (モデルやプロンプトなど) を保護するための新しいセキュリティ・ツールは未熟で、生成 AI アプリケーション・アーキテクチャに大きく左右されます。

このような環境でベスト・プラクティスや推奨事項を策定するのは困難です。

効果の低いセキュリティへのフォーカス

Gartner の調査では、回答者の 93% が、自分たちの行動で組織のサイバーセキュリティ・リスクを高くすることが分かっていながらも、実行したことを認めています。

実際、Verizon 社のデータ漏洩／侵害調査報告書によると、セキュリティ侵害全体の 74% に人的要因が含まれています。

また、エンドユーザーに重点を置いたセキュリティ・プログラムを実施していても、データ侵害につながるエラーのほとんどは、開発者やシステム管理者が引き起こしたものです。

セキュリティ／リスク・リーダーの 3 つの優先課題とアクション

1 デジタル・オペレーティング・モデルに適応する

サイバーセキュリティ・リーダーの 4 分の 3 近くが、過去 12 カ月間だけでもリスクに関する意思決定権や説明責任が変化したと認識しています。

2 AI を積極的に活用する

2025 年末まで、生成 AI の安全性を確保するために必要とされるサイバーセキュリティのリソースが急増し、アプリケーションとデータ・セキュリティへの支出が 15% 以上増加すると予測されています。

3 人間中心のセキュリティへ方向転換する

サイバーセキュリティ部門の 90% 以上で意識向上プログラムが実施されていますが、従業員の 69% は意図的に企業のサイバーセキュリティ・ガイダンスに沿わない行動を取っていることを認めています。

アクション

セキュリティ機能を、「イノベーションの障壁」から「安全なデジタル・イノベーションを実現する立役者」へと変更します。

組織が生成 AI を構築／利用する際の安全性を確保するとともに、生成 AI がサイバーセキュリティに及ぼす影響にうまく対処します。

サイバーセキュリティ戦略を評価し進化させるために、専門家チームの設立が推奨されます。このチームは、現在のセキュリティ状況を詳細に分析するとともに、将来のセキュリティニーズを予測します。さらに、セキュリティ強化の新しい機会を探索し、リスクと利益のバランスを慎重に考慮しながら具体的な施策を提案します。専門家チームは定期的に報告を行い、組織のセキュリティ戦略の継続的な改善を支援します。

出典：Gartner

現代のサイバーセキュリティ・オペレーティング・モデルを理解する

現代のサイバーセキュリティ・オペレーティング・モデルの主要な要素には、以下のような重要な影響があります。

財務：テクノロジ／セキュリティ投資の予算権限が、ビジネス部門やプロダクト部門の責任者に移行します。これにより、セキュリティ投資がビジネス・ニーズにより密接に結びつくようになります。

意思決定権：セキュリティに関する決定権が、IT 部門から事業部門の責任者に移っています。この決定は、協調的なリスク意思決定プロセスによってサポートされます。また、セキュリティ・ポリシーがより柔軟で原則ベースになり、セキュリティ対策の選択においてビジネス部門の自律性が高まります。

パフォーマンス管理：運用上のセキュリティ指標から、ビジネス成果を重視した指標へと重点が移行しています。また、ビジネス価値を測定する手法の採用が進んでいます。これにより、セキュリティの効果をビジネス貢献度で評価できるようになります。

人材管理：生成 AI などの新しいテクノロジの採用により、これらのテクノロジのリスク影響を理解するスキルの開発が求められています。さらには、セキュリティ・サービス・マネジャーといった新しいリレーションシップ・マネジメント・スキルのほか、セキュリティ行動／文化を変革するための行動科学スキルも必要とされます。

生成 AI がもたらす影響を理解する

防御に使用する	攻撃を受ける	構築する	利用する
• 低い成熟度 • ベンダーの急増によるリスク • プライバシーと有効性の課題	• スキルの増強 • 攻撃の自動化 • コンテンツ生成	• 段階的な展開が可能 • ほかのプログラムで再利用可能	• 複数の利用オプション • シャドー AI • データのプライバシーと著作権
セキュリティ／リスク・マネジメントの改善、リソースの最適化、新たな攻撃手法に対する防御、場合によってはコスト削減のために、生成 AI の機会を活用する権限を得ます。	攻撃者は、生成 AI ツール／手法の開発によって攻撃手法を進化させ、場合によっては新たな攻撃経路を活用しています。そのため、新しい攻撃方法や手段に対して、防御側が自らの戦略やテクノロジを調整し、効果的に対抗できるようにします。	AI アプリケーションではアタック・サーフェス (攻撃対象範囲) が拡大し、潜在的リスクが新たに生じるため、既存アプリケーションのセキュリティ・プラクティスを調整する必要があります。	最初に登場したのは ChatGPT でしたが、今後は既存アプリケーションに生成 AI アシスタントが組み込まれるようになるでしょう。そうしたアプリケーションには、従来のセキュリティ対策では満たせない独自のセキュリティ要件があります。

出典：Gartner

「シフト・レフト」によってセキュリティ行動を変える

「シフト・レフト (Shift Left) 」というアプローチは、セキュリティを開発プロセスのより早い段階 (左側) に組み込むことを意味します。セキュリティ行動を変えるための取り組みでは、デジタルの「サプライチェーン」全体を対象とする必要があります。これはつまり、行動変革イニシアティブの対象者を、エンドユーザーだけでなく、デジタル・ソリューション開発に関与するすべての役割にまで拡大するということです。この取り組みの対象者は組織の最上層から始める必要があります。CEO や取締役といった明確なリーダー層から始めることで、行動や文化の変更を促しやすくなります。

行動変革イニシアティブの対象者

出典：Gartner

Gartner

Gartner のコンファレンスに参加して、サイバーセキュリティ／リスク・マネジメントのための戦略的思考を加速させましょう

セキュリティ・リーダー同士で協力しながら、サイバーセキュリティ／リスク・マネジメントの手法とテクノロジの柔軟性と対応力を向上させて、ミッション・クリティカルな目標を達成するための価値ある知見を共有します。

ぜひご参加ください

今すぐコンファレンス・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。

→ Gartner のコンファレンス・スケジュールを確認する








実用的で客観的な知見

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。

Roadmap

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)

How We Help

Gartner for CISOs - 最高情報セキュリティ責任者 (CISO) 向けサービス

Gartner が CISO とそのチームに、ミッション・クリティカルな優先課題の解決に必要な知見、ガイダンス、ツールをどのように提供しているかを確認できます。

詳細を見る

Webinar

セキュリティ：新たな闘い

高まる脅威とデジタル環境の急速な変化の中で、疲弊することなくセキュリティの課題に挑み続けるためには、旧来のスタイルを改め、新たな格闘スタイルを身に付ける必要があります。

今すぐ視聴

Research

セキュリティ・ガバナンス (集約と分散) の進め方

セキュリティ侵害のインシデントはいつ発生してもおかしくない状況であり、企業はインシデントに備えた取り組みを今すぐに開始する必要があります。

今すぐダウンロード

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

Connect With Us

Gartner は、お客様のミッション・クリティカルな課題について、
より優れた意思決定と大きな成果へと導く実行可能かつ客観的な
知見を提供します。

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 のコンファレンスにご参加ください
コンファレンスの最新情報を見る

Gartner