Kong

Powering the API world

APIセキュリティの展望2025年版

AI強化型の脅威とAPIセキュリティ

本レポートについて

Kongの『APIインパクトレポート2024年版』によると、開発者やビジネスリーダーの83%は、AIへの投資を通じて既に新製品や新サービスの機会を手にしたと回答しています。

ではITリーダーは、今後1年についてどのような懸念を抱いているのでしょうか。また、APIセキュリティインシデントやAI強化型の脅威に関して、これまでに何を目にしてきたのでしょうか。

AI強化型の脅威に伴うリスクの高まりに企業が対処し、AIツールや大規模言語モデル（LLM）の導入を進めるにあたって、APIセキュリティが重大な転換点にあることが、700人のITリーダーを対象としたKongの最新の調査で明らかになっています。

回答者の約75%がAI強化型の攻撃に深刻な懸念を示している一方で、注目すべき食い違いも見えてきました。55%の企業が過去1年間にAPIセキュリティインシデントを経験したにもかかわらず、自社のセキュリティ能力に自信があると回答した企業は85%にも上ったのです。

しかし、この自信は恐らく的外れと言えます。というのも、77%の回答者が、自社のAPIエコシステムにAIやLLMを導入することで、重大なセキュリティリスクが生じる可能性があることを認めているからです。

しかも、APIセキュリティインシデントには大きなコストが伴います。過去1年間の修復費用が50万ドルを超えたとの回答が20%ありました。

そのほか、今回の調査で得られた主な結果は次のとおりです。

- AI関連の新たなリスクに対処するうえで、**40%の回答者は現在のセキュリティ投資が十分であるか自信がない**
- AI強化型のサイバー攻撃がセキュリティ脅威の最上位になっている
- **92%の回答者はAI強化型の脅威に対策を講じている**
- シャドーAPIは大半の企業にとって危険な盲点となり得る

多くの企業は、脅威の情勢が変化してきたことを認識しつつも、AI時代のAPIインフラを守るうえで必要となる包括的なセキュリティ対策を講じていません。

認識と現実のギャップには注意が必要です。API攻撃は今後増加する見通しであるだけになおさらです。それに、Gartnerの調査によると、API侵害では一般的なセキュリティ侵害よりも多くのデータが流出します。

AI強化型の脅威とAPIセキュリティインシデント

Kongは、APIセキュリティと、AI強化型脅威のリスクの高まりについて、
700人のITリーダーを対象に調査を実施しました。

88%
APIセキュリティを最優先事項の1つと回答

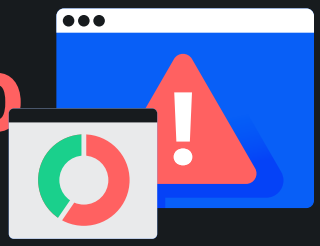
APIセキュリティはITリーダーにとって最大のセキュリティ懸念

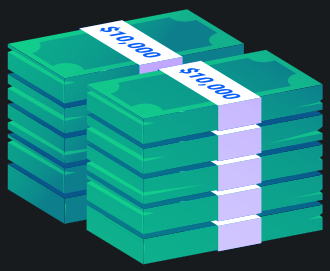
回答者の97%はAPIセキュリティについて、ネットワークセキュリティやエンドポイントセキュリティなど、他のサイバーセキュリティの懸念と同じかそれ以上に重大だと認識しています。

APIセキュリティインシデントは広く見られ、多額のコストが発生

回答者の半数以上は、過去1年間にAPIセキュリティインシデントを経験しています。27%はAPIセキュリティ対策に自信が持てていません。

55%
過去1年間にAPIセキュリティインシデントを経験





インシデント経験者の約半数は修復に

10万ドル

以上を投入

過去1年間にAPIセキュリティインシデントを経験した回答者のうち、
47%は修復費用が10万ドルを超え、20%は50万ドルを超えたとされています。

リーダーはAI強化型脅威の阻止に関して自社の能力に自信が持てず

今日のAPIセキュリティにとって最大の脅威と認識されているのは、AI強化型の攻撃でした。
それ以降に不正なアクセスや侵害、不十分なデータ保護や暗号化が続きます。

74%
AI強化型の攻撃を強く懸念

92%
AI強化型の攻撃に対策を講じている

40%
現在のセキュリティ投資に自信が持てない

APIマネジメントプラットフォームのリーディング企業であるKongは、世界中の企業が「APIファースト」企業となり、AIの導入を安全に加速することを使命としています。世界で最も採用されているAPIゲートウェイ上に構築されたKongの統合クラウドAPIプラットフォームは、APIの構築・運用・管理のライフサイクル全体を一気通貫で提供することで開発者の生産性を高めると同時に、高速かつセキュアで拡張性のある製品とサービスにより、ビジネスのデジタル体験を向上させ、イノベーションを加速します。詳細については、jp.konghq.com をご覧ください。

APIセキュリティとAI強化型脅威のリスクの高まり

API（アプリケーションプログラミングインターフェース）は、今日のデジタル社会の屋台骨です。**AIにはAPIが不可欠**ですが、ピザの注文や乗換案内など、もっと基本的なネット上の連携も、APIを通じて成立しています。

しかし、適切な管理、可視性、プロセスを導入していないAPIは、セキュリティホールになりかねません。

Gartnerの**調査**によると、平均的なAPI侵害では、通常のセキュリティ侵害の少なくとも10倍のデータが流出します。また、API攻撃は件数が増えており、2030年までに548%増加するとKongは**予測**しています。

潜在的なセキュリティ脅威の最上位はAI強化型の脅威

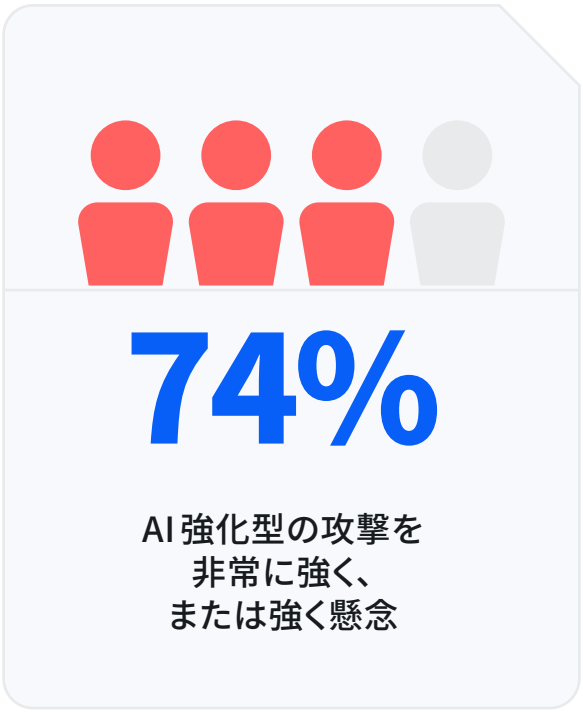
AIによってサイバー攻撃の参入障壁が低くなることが考えられ、企業のAPIセキュリティの防御を打ち破る新たな攻撃経路が生まれます。APIに依拠しているテクノロジは非常に多いため、API攻撃がデータセキュリティにますます大きな影響を及ぼす可能性があります。

テクノロジ分野に従事している人々は、このリスクを明確に認識しています。回答者の74%は、AI強化型の攻撃を非常に強く懸念、または強く懸念しており、32%は今日の企業にとって最大のセキュリティ脅威だと回答しています。今日のAPIセキュリティに対する最も重大な脅威の第1位はAI強化型の攻撃、第2位は不正なアクセスや侵害という結果でした。

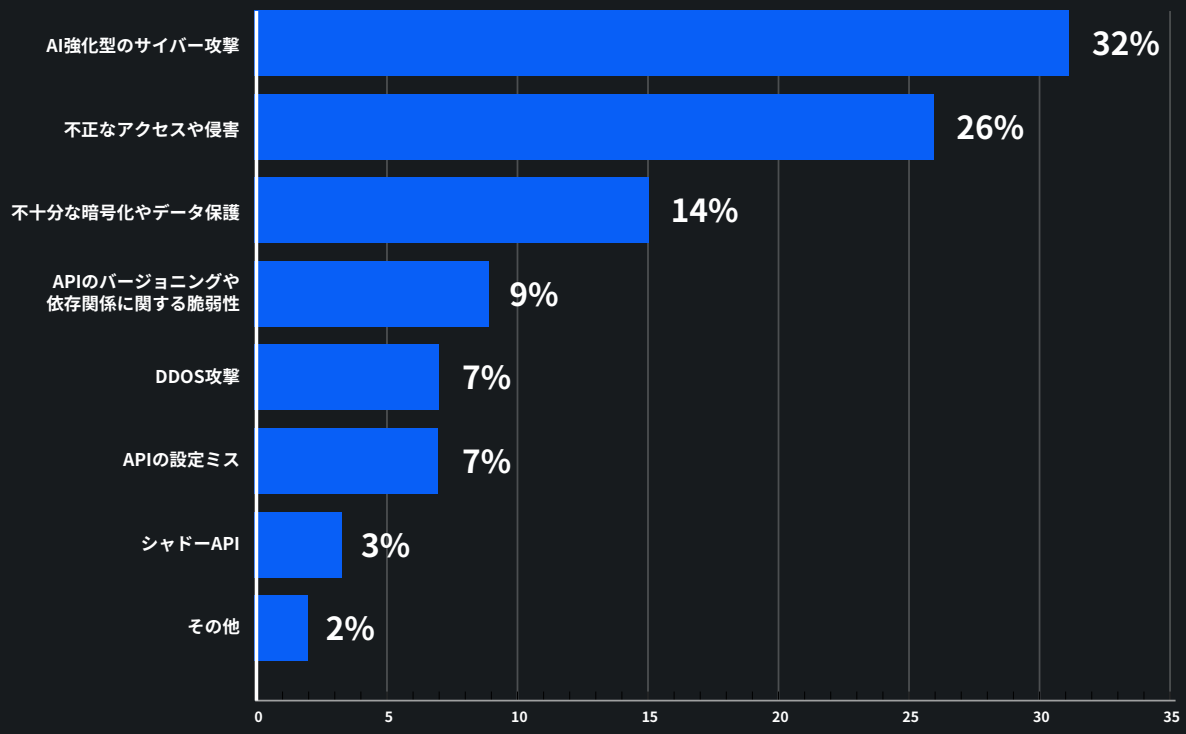
AI技術や大規模言語モデル（LLM）の導入が急速に進んだことで、以前なら想像もできなかったイノベーションが現実になっています。しかし、それに伴って、サイバーセキュリティの脅威の情勢も一変しました。

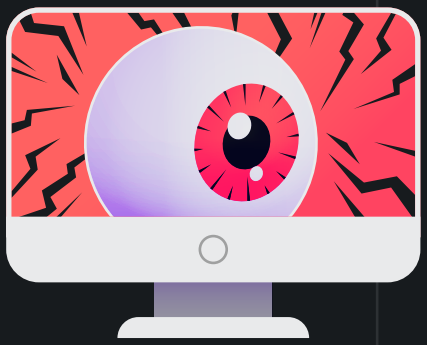
こうしたAI強化型の新たなツールや脅威は、**APIセキュリティ**にどのような影響を及ぼしているのでしょうか。そして、ITリーダーは次の1年についてどのような懸念を抱いているのでしょうか。

その点を探るために、Kongは米国と英国で700人のITリーダーを対象に、今日のAPIセキュリティを取り巻く環境にAIがもたらしている影響についてアンケートを実施しました。



現在の御社にとって
最大のセキュリティ脅威は？





シャドー APIのリスクに注目

シャドー APIは、脅威と目されている項目のリストでは下位にとどまっています。しかし、サービスやAPIに関して最新の記録システムを取り入れていない企業の場合、存在が認識されておらず管理もされていないシャドー APIは、非常に大きなセキュリティリスクとなります。Gartnerは『2024 Market Guide for API Protection』の中で次のように述べています。「API、特にシャドーAPIや休眠APIは、企業にとってデータ侵害の原因となっている。その平均規模は他の侵害を上回る」

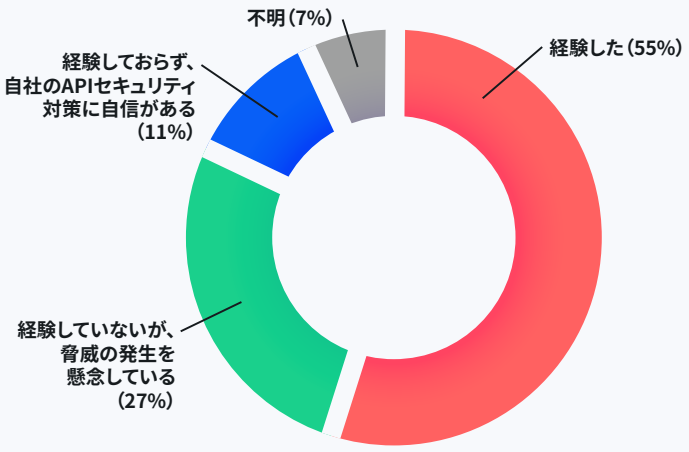
サービスやAPIには可視化が不可欠です。自社のインフラで稼働する数万のAPIエンドポイントは、その1つひとつが固有の攻撃経路になると考えられます。特に、保護の対象から外れたままで、認証や認可、レート制限を適用していないエンドポイントは危険です。

自社のITインフラに潜むシャドー APIに特定する方法について、詳しい情報をご覧ください。

半数が過去1年間にAPIセキュリティインシデントを経験

回答者の55%は、過去1年間にAPIセキュリティインシデントを経験していました。そのうち3分の1は、「深刻」なインシデントだったと回答しています。インシデントを経験しておらず、自社のAPIセキュリティ対策に自信を持っているとの回答は11%にとどまりました。

過去1年間にAPIセキュリティインシデントを経験しましたか？



32%

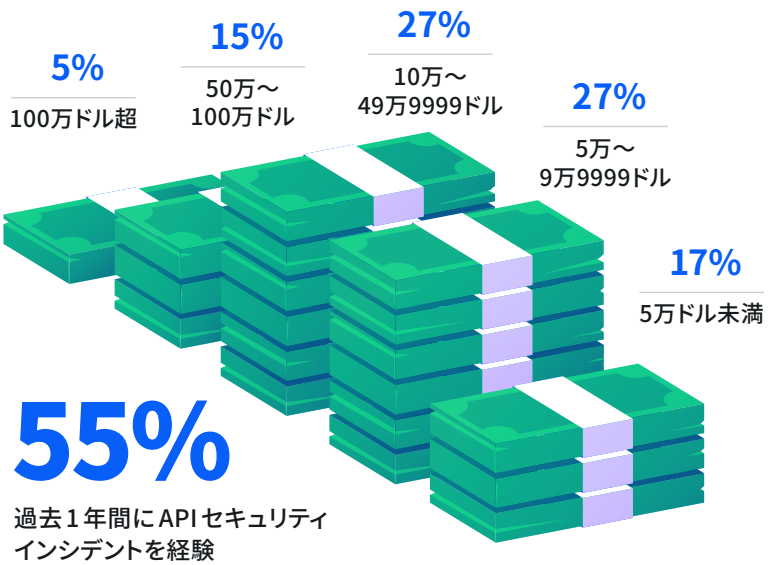
APIインシデントを経験したうちで、「深刻」だったと回答した人の割合

5人に1人はAPIセキュリティインシデントの修復費用が50万ドルを超えたと回答

過去1年間にインシデントを経験した回答者のうち、47%は修復費用が10万ドルを超え、**20%は50万ドルを超えたとされています。**

この費用には、従業員の作業時間などの社内リソースの分と、コンサルティング、セキュリティツール、法務関連の費用などの外部リソースの分が含まれています。

過去1年間のAPIセキュリティインシデントの修復費用



55%

過去1年間にAPIセキュリティインシデントを経験

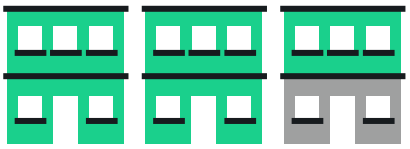
9%は不明または未回答

企業の自信とセキュリティインシデント件数との意外な乖離

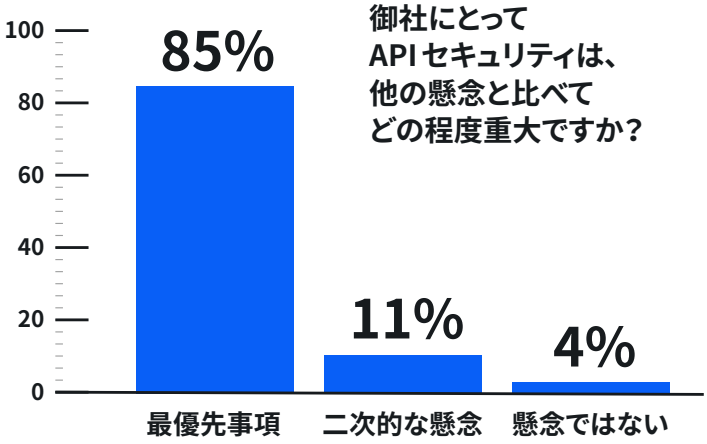
最近攻撃を経験し、その対処に費用を投じた人が増えているにもかかわらず、多くの回答者は、現在と今後の脅威に対する自社のAPI防御能力に自信を示しています。これは偽りの安心感なのでしょうか。それとも、インシデントを経験した後で真剣に取り組んだ結果なのでしょうか。その答えは、時が経てば明らかになるでしょう。

85%

自社のAPI防御能力に自信があると回答



4%は自信なし、11%はどちらでもない



大半の回答者はAPIセキュリティをサイバーセキュリティ上の重大な懸念と認識

回答者の97%は、APIセキュリティの重大性について、ネットワークセキュリティやエンドポイントセキュリティなど、他のサイバーセキュリティの懸念と同じかそれ以上と認識しています。

40%は自社の投資が十分であるか自信なし

45%の回答者が、サイバーセキュリティ予算の20%以上をAPIセキュリティに投じています。また**40%の回答者は、特に新たなAIプロジェクトやAI強化型の脅威への対応という面で、自社の投資がAPIセキュリティリスクを網羅するのに十分であるかについて、自信がないか、または疑念を抱いています。**

40%

自社の投資がAPIセキュリティリスクを網羅するのに十分であるか自信が持てない

継続的な統制は監視とAPIゲートウェイが頼り

APIセキュリティリスクを低減するために企業が講じている予防策は、API監視ツールと異常検知ツールが第1位でした。英国と米国を比較すると、英国の方がAPIゲートウェイの導入との回答が多くなっていました（英国は71%、米国は50%）。この違いは、英国の方がコンプライアンスや規制要件が厳しいことに起因している可能性があります。

APIセキュリティリスクを低減するために講じている手段は？

1. API監視ツールと異常検知ツール（63%）
2. APIゲートウェイソリューションの導入（61%）
3. APIの暗号化とトークン化（58%）
4. 定期的なペネトレーションテストと監査（57%）
5. ゼロトラストアーキテクチャの採用（35%）
6. 具体的な手段は講じていない（6%）

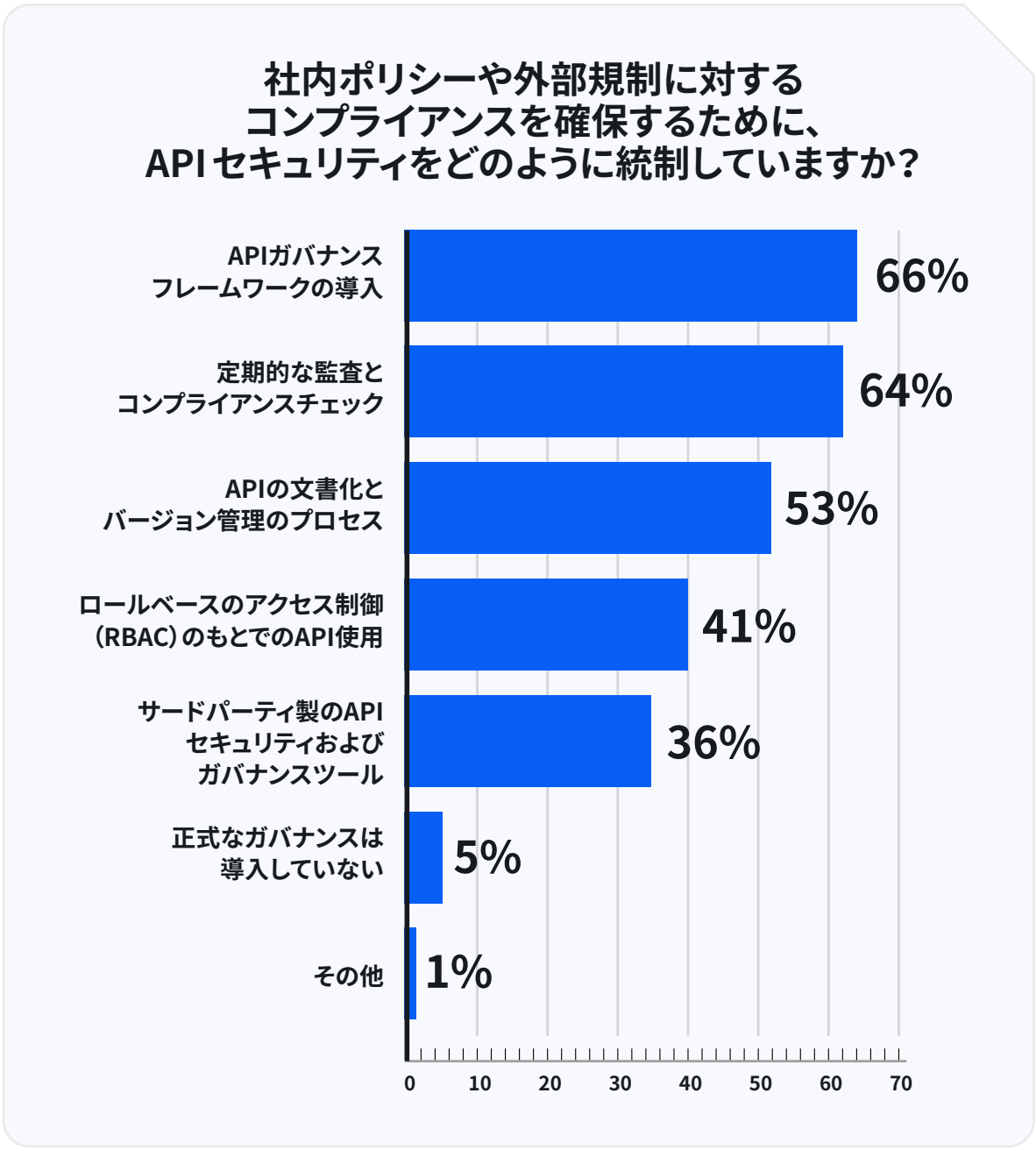
ゼロトラストアーキテクチャの採用という回答はわずか35%でした。APIセキュリティへの包括的なアプローチであるゼロトラストがベストプラクティスとして確立され、広く受け入れられていることを考えると、この数字は意外です。

92%はAI強化型の脅威からAPIを防御するためのセキュリティ対策を実施

AI強化型の脅威からAPIを防御するために企業が講じている策で最も多かったのは、監視とトラフィック分析の強化でした。企業がAI強化型の脅威をどの程度真剣に捉えているかという点で、英国と米国には顕著な違いがあるようです。具体的には、AIの脅威に対して特に策を講じていないとの回答は、米国では13%だったのに対し、英国ではわずか4%でした。

AI強化型の脅威からAPIを防御するために講じている策は？

1. 監視とトラフィック分析の強化（66%）
2. 従業員教育（60%）
3. AIを活用した脅威検知システム（51%）
4. AI/MLの機能を持つAPIセキュリティソリューションの活用（44%）
5. サードパーティのセキュリティサービス企業との提携による脅威の検知と緩和（40%）
6. なし（8%）

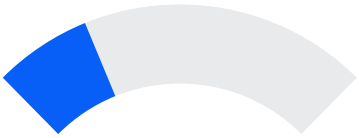


コンプライアンス対策はAPIガバナンスフレームワークや監査が上位に

社内ポリシーや外部の規制（例えばGDPRやHIPAA）に対するコンプライアンスを確保してAPIセキュリティを統制するために企業が導入している主な策には、APIガバナンスフレームワーク、定期的な監査とチェック、APIの文書化とバージョン管理のプロセスがあります。

AIモデルとLLMが加わってセキュリティが複雑化し、脆弱性が発生

77%の回答者は、LLMなどのAIモデルを自社のAPIエコシステムに統合することについて、セキュリティ脆弱性が生じる大きなリスクがあると回答しています。



25%

APIやLLMに関連するAI強化型のセキュリティ脅威を経験

65%

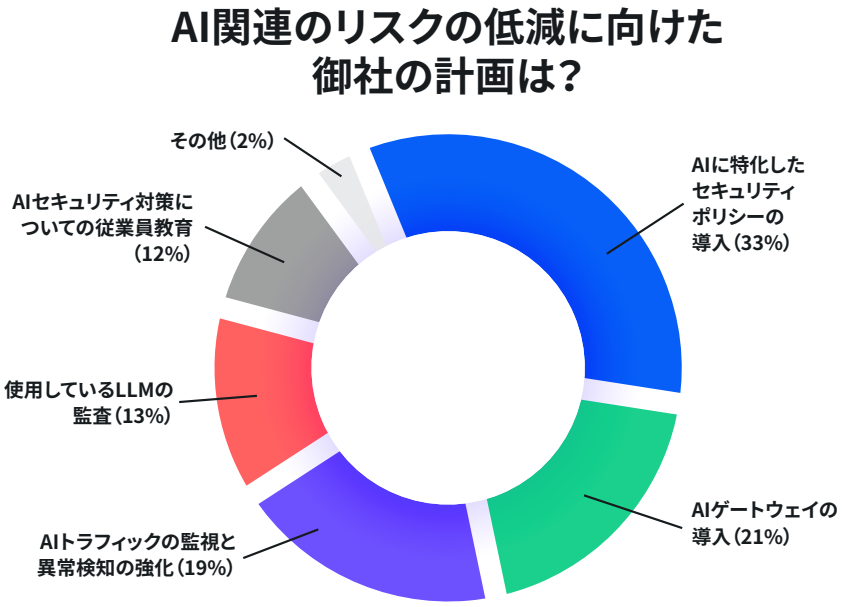
AI強化型のセキュリティ脅威に対する戦略策定や準備を進めている

84%

AIとLLMによってAPIの防御が今後2～3年で複雑化すると回答

企業内でのAI利用の普及にあわせて、外部からのAI強化型の攻撃をブロックすること、そして新たな取り組みの中で発生したAI生成のトラフィックを適切に統制し防御することが重要になります。こうしたリスクを低減するための策として、ITリーダーは、AIに特化したセキュリティポリシーの導入、AIゲートウェイの導入、AIトラフィックの監視と異常検知の強化を挙げています。

AIゲートウェイでは、AIへのアクセスを一元的に管理できます。これは、オブザーバビリティ、セキュリティ、ガバナンスを損なわずにAIの導入を加速させるのに役立ちます。



AIのセキュアな導入と、最大の弱点

人間は依然として、サイバーセキュリティにおける最大の弱点の1つです。したがって、生成AIとLLMに関するベストプラクティスの教育にエネルギーを注ぐのは賢明です。

しかし、教育だけでは十分ではありません。大半の企業はAIに関するガイドラインや規則を設けていますが、60%の人は、自社のAI利用規則を無視している、あるいは回避する方法を発見していると回答しています。

生成AIのテクノロジがもたらす可能性を最大限に引き出すためには、データガバナンスや規制の面での影響など、生成AIに付随する課題への対処方法を企業として理解しておくことが欠かせません。責任ある導入に向けて、堅牢なガバナンスのプレイブックを明確に定義しておくことが鍵となります。

AIを適切に導入するために、AIガバナンスのプレイブックの作成方法に関するeBook「**Navigating AI Innovation: A Playbook for Secure and Governable LLM Integration**」をぜひお読みください。

今すぐダウンロード

まとめ

AI時代は APIセキュリティが かつてないほど重要に

AIとAPIの融合は、過去に例のないチャンスであり、かつリスクでもあります。大半の企業はAI強化型の攻撃を非常に強く懸念しているものの、40%もの企業が、自社の現在のセキュリティ投資が十分であるか自信を持てずにいます。シャドーAPIなどの重大な脆弱性を軽視している企業は依然として多く、AI強化型の脅威に対して特に策を講じていないと回答した米国企業は13%にも上ります。

API攻撃は、2030年までに548%増加する見通しです。今こそ行動を起こさなくてはなりません。Kongの統合APIプラットフォームは、こうした課題に取り組む企業を支えます。堅牢なセキュリティを備えており、完全な可視化が可能で、APIエコシステム全体をシンプルに管理できます。

企業がAPIマネジメントを簡素化し、AIのイノベーションを引き出すうえで、Kongは効果を発揮します。詳しくは[jp.konghq.com](jp.konghq.com)をご覧ください。

調査方法

このレポートは、現在のトレンドと動きに関するエキスパートの見解を分析することで、APIセキュリティを取り巻く環境の変化について考察しています。こうした洞察を得るために、2024年第4四半期、専門の調査会社への委託のもと包括的な調査を実施しました。調査対象は、2つの重要な市場である米国と英国のITプロフェッショナルおよびビジネスリーダー700人です。

Kongについて

APIマネジメントプラットフォームのリーディング企業であるKongは、世界中の企業が「APIファースト」企業になることを使命としています。世界で最も採用されているAPIゲートウェイ上に構築されたKongの統合クラウドAPIプラットフォームは、APIの構築・運用・管理のライフサイクル全体を一気通貫で提供することで開発者の生産性を高めると同時に、高速かつセキュアで拡張性のある製品とサービスにより、ビジネスのデジタル体験を向上させ、イノベーションを加速します。

Kongの詳細については、jp.konghq.com をご覧になるか、Xで @KongJPN をフォローしてください。

詳しく見る

Powering the API world

jp.konghq.com

Kong 株式会社
japanmarketing@konghq.com

東京都港区赤坂 9 丁目 7 － 1
ミッドタウン・タワー 18 階