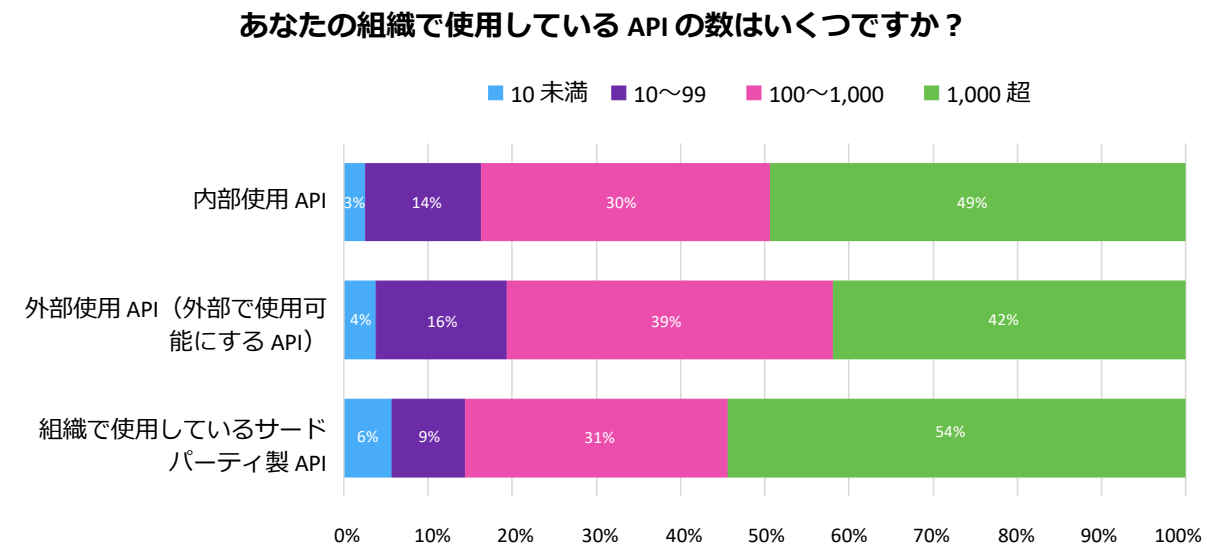
図 1：使用中の API の数



注：n = 160

出典： Omdia

API の使用が増加しています。同時に、回答者の多くが、社内記録の窃取や大規模なデータスクレイピングなどの具体的な問題を生じる API セキュリティインシデントを報告しています。

このシナリオに対応するため、企業は API セキュリティの取り組みを今すぐ改善する必要があります。API は今後も増え続ける一方であり、このような手段を講じない限り、セキュリティ上の問題は大きくなります。API の数が増加すると、攻撃のアタックサーフェスが拡大し続け、攻撃の可能性がさらに高まります。

API セキュリティのクイックガイド

API セキュリティの一般的なフローは、DevOps で使用される構築／共有／実行／監視のサイクルと似た、無限に繰り返し実行される 4 つの主なユースケースを中心に構成されます。

- **環境全体で使用されている API の探索：**これは、OpenAPI（Swagger）定義のインジェスト、コードリポジトリのスキャン、環境のアクティブスキャンなど、さまざまな方法で実行できます。ほとんどの API は、トラフィックを分析することで探索されます。API 仕様ファイルのアップロードはあまり使用されていない方法で、組織がすでにどの API を使用しているかを把握している場合に限られます。さらに、1 つの手法だけでは十分ではありません。トラフィックとリポジトリの継続的なスキャンを組み合わせることで、組織内での API 使用状況を包括的に把握できるようになります。