ホワイトペーパー

# アジア太平洋地域の金融サービスを発展させるための堅牢なAPIセキュリティ

# エグゼクティブサマリー

国際通貨基金によると、アジア太平洋（APAC）地域では大幅な経済成長が続き、2024 年の成長率は 4.2% となる見込みです。このように日々進化を続ける成長の中で、特に金融サービスセクターでは、アプリケーション・プログラミング・インターフェース（API）が業界のデジタルトランスフォーメーションを促す主要な原動力となっています。API は銀行システムのさまざまなコンポーネントを技術的につなげる架け橋のような役割を担っており、これによってデータと機能のシームレスなやりとりが実現します。API によって金融サービスの提供方法が一変し、顧客に多くのメリットを提供しています。

API の利用の急速な拡大には、課題がないわけではありません。IDC の予測によると、APAC におけるセキュリティ支出が 2026 年までに 550 億ドルに達する見込みです。API によってデジタルサービスを拡大したため、金融機関は迂闊にも数多くのセキュリティ上の脆弱性にさらされることとなってしまったのです。このように API の利用急増により、サイバー犯罪の対象となり得るアタックサーフェスが飛躍的に拡大しています。攻撃者は金融データの本質的な価値を認識しており、戦術を変化させ、API という新たなエントリーポイントを悪用するようになりました。

このように増大する脅威の状況に対応するために、金融機関はサイバーセキュリティ対策に大々的に投資せざるを得ませんでした。金融機関は、自社のシステムを守るだけでなく、顧客の機微な情報や資産を保護することにも注力しています。そのため、サイバー攻撃によるリスクを緩和するために、脅威検知、対応戦略、同業他社やサイバーセキュリティ専門家との連携が、ますます重視されるようになりました。

API を原動力とした APAC 金融サービス業界のデジタルトランスフォーメーションは、同業界の、顧客ニーズの変化に対応する適応力とコミットメントの証しです。しかし、このトランスフォーメーションが進行するなか、同業界は気を緩めることなくその取り組みを継続し、サイバーセキュリティ体制を強化し、セキュリティ上の脆弱性に対処し、絶えず存在するサイバー攻撃の脅威によってデジタルイノベーションの恩恵が損なわれないようにしなければなりません。

# 高まる API の重要性

APAC 地域では、金融サービスセクターでデジタル革命が起こっています。API は銀行の商品やサービスを利用したい顧客にかつてないほどの利便性、スピード、セキュリティを提供する原動力となりました。顧客は今や、口座残高の確認から、送金、ローン申請、投資管理まで、さまざまな金融活動を即座に行えます。この利便性により、顧客体験が一変しただけでなく、金融業界はデジタル時代に突入しました。API はシンプルなシステム間通信ツールからインターネットトラフィックの根幹へと進化し、さまざまなアプリケーションやサービスを支える存在になりました。

Polaris Market Research のレポートによると、全世界におけるオープンバンキングの市場規模は 2021 年時点で 161.4 億ドルであり、2030 年までに 1,281.2 億ドルに達し、当該予測期間中の複合年間成長率は 26.8% となる見込みです。また、Polaris の調査では、当該予測期間中に最も大きな成長を遂げる地域は APAC であることが明らかにされています。APAC の金融サービス業界がオープンバンキングの将来性を生かすためには、協力して API セキュリティの課題に対処しなければなりません。

その先頭に立っているのがシンガポールであり、シンガポール金融管理局（MAS）は API プレイブックを公開しています。また、2018 年には MAS の主導により API Exchange（APIX）が設立されました。これは、世界銀行グループの国際金融公社と ASEAN 銀行協会が共同で実現した新たな取り組みであり、金融機関と金融テクノロジー機関のコラボレーションのためのグローバルなオンラインマーケットプレイスおよびサンドボックスです。

他のアジア諸国も長きにわたってオープンバンキングの発展に取り組んできました。インド国内には銀行口座を所有していない人が数多く存在しており、この膨大な非銀行利用者層向けにファイナンシャルインクルージョン（金融包摂）の改善が進められています。

同国政府の初期の取り組みの 1 つとして、2016 年の統合決済インターフェースが挙げられます。これにより、認可されたサードパーティを通じて一般人が API プロトコルを使用し、銀行口座にアクセスして取引を実行できるようになりました。2021 年にはインド準備銀行が Account Aggregator を立ち上げました。これは、同意管理機能を作成し、消費者が自身の金融データにデジタルでアクセスして管理できるようにし、金融サービスプロバイダーとのデータ共有プロセスを簡略化するフレームワークです。

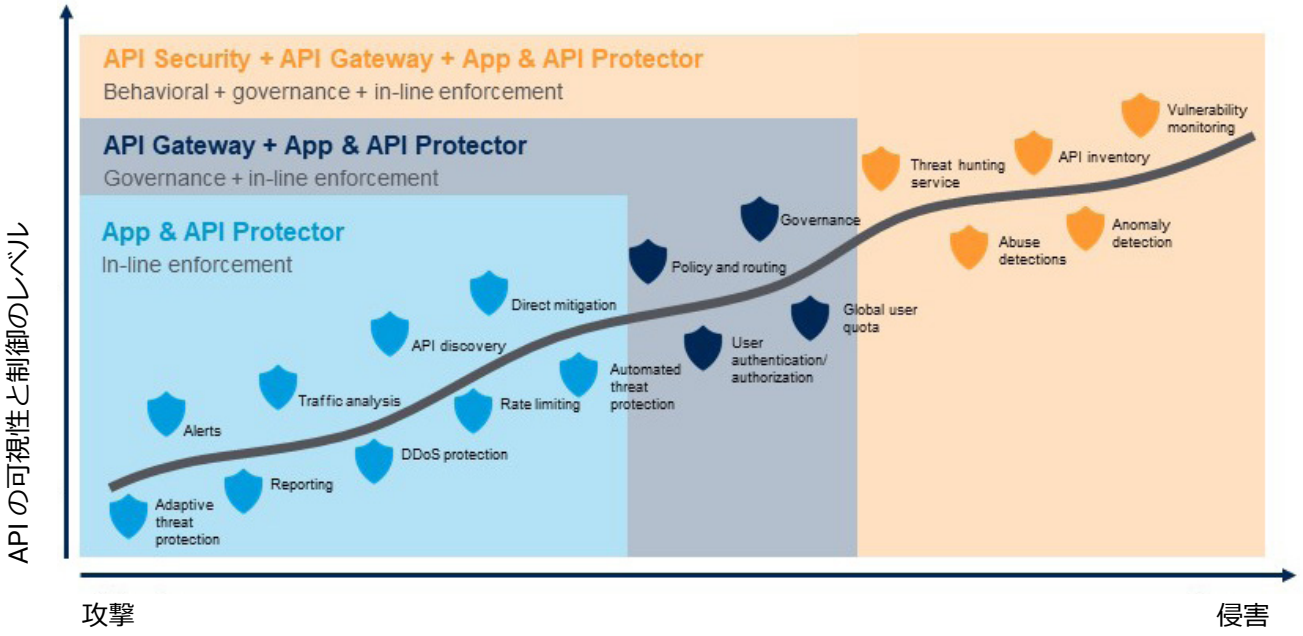
このような重点的な取り組みを行っているにもかかわらず、APAC の金融サービス業界は依然として世界で最も多くの攻撃にさらされている業界であり、2022 年第 2 四半期から 2023 年第 2 四半期の間に Web アプリケーションおよび API 攻撃が 36% 増加し、18 か月間で 37 億件という驚異的な数の攻撃を受けました。数多くの金融ハブがある APAC 地域で、Web アプリケーションおよび API 攻撃が急増したのです。

## APAC における API 関連の脅威

APAC 地域では Web アプリケーションおよび API 攻撃が急激に増加しており、2021 年から 2022 年の間に金融サービスに対する攻撃が 248% 増加しました。オーストラリアでの Optus のデータ漏えいや米国での T-mobile の API データ漏えいなど、注目を浴びた数々の大規模侵害の原因は、API の脆弱性でした。そして、このようなインシデントにより、エンドポイントの保護と認証情報の確認を行うだけではない堅牢な API セキュリティソリューションの必要性が浮き彫りになりました。

このホワイトペーパーでは、この極めて重要なアタックサーフェスに対処し、効果的に API のセキュリティを確保することができる戦略について説明します。また、プロアクティブなアプローチで API セキュリティに取り組むことによってどのようにコンプライアンスとデータ保護を確立できるかについて論じます。

## API 攻撃の進化



# API セキュリティの主なリスク

API は幅広いセキュリティリスクに対して脆弱な可能性があり、データ漏えいや不正アクセスなどの攻撃を招きかねません。API セキュリティの主なリスクとして、シャドウ API、脆弱な API、API の悪用、機微な情報の過度な共有、Credential Stuffing 攻撃が挙げられます。

- **シャドウ API：**多くの金融機関には、すべての API を管理する責任を担っている人やチームが存在しません。このように管理体制が欠如しているため、重大なセキュリティギャップが生まれます。API を管理しセキュリティを確保するためには、組織全体の API を探索しカタログ化することが不可欠です。開発者とセキュリティチームの間のギャップを埋め、環境内のシャドウ API を検知することが重要です。継続的な探索により、新たに探索された API や既存の API への変更に関する最新情報を常に把握し、シャドウ API を排除することができます。

- **脆弱な API：**金融機関は、API を探索した後に、特に機微な情報を保有している API に関してリスク状況を評価し、脆弱性を特定しなければなりません。このステップは、効果的にセキュリティに関する取り組みの優先順位を決定するために不可欠です。

- **API の悪用：**デジタル化の加速に伴い、APAC 全体で Web 攻撃の件数が増加し続けています。攻撃者は絶え間なく API をターゲットにしているため、堅牢なセキュリティ対策によって悪用や乱用を阻止する必要があります。

- **機微な情報の過度な共有：**現代のアプリは機微な情報を過度に共有することが多いため、新たな攻撃ベクトルとなっています。攻撃者はトラフィックを傍受し、機微な情報に不正にアクセスする可能性があります。

- **Credential Stuffing 攻撃：**攻撃者は API を利用し、金融機関を標的とした Credential Stuffing 攻撃を自動化しています。

# API セキュリティに関する課題

## 攻撃が検知されず報告されない

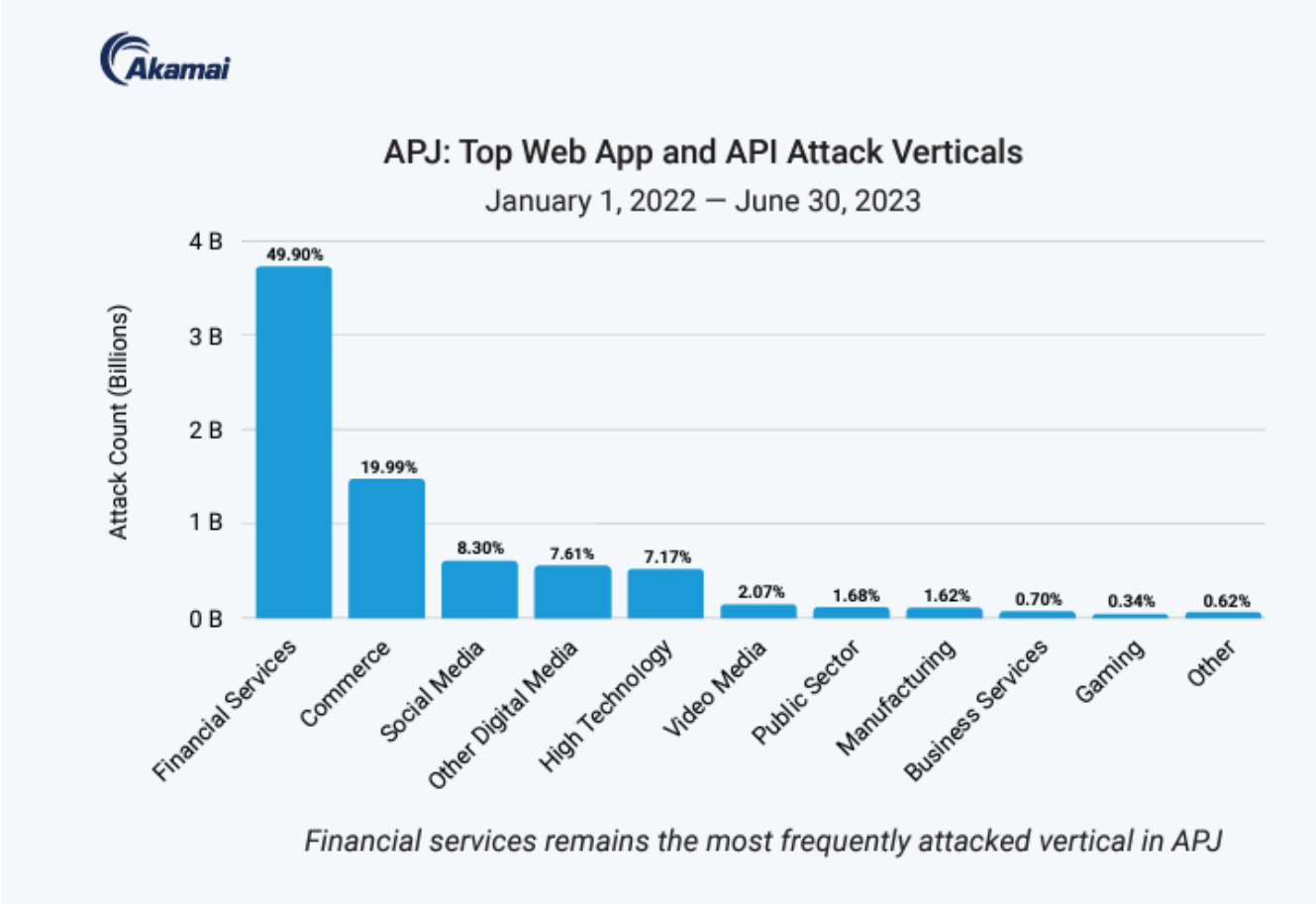
最近の SANS の調査結果によると、API インベントリーは依然として金融機関にとって重大な問題となっています。金融機関は自社のインフラ内にあるすべての API を把握してさえいない場合があり、これによってガバナンスとセキュリティの盲点が生まれます。このように可視化されていないことが、API 攻撃が検知されず報告されないことが多い主な原因の 1 つである可能性があります。API のセキュリティを確保するための第一歩は、API を徹底的に探索し、カタログ化することです。

## 破壊的な API 攻撃の影響

Web アプリケーションと API の可用性が損なわれると、顧客満足度とブランドロイヤルティに深刻な影響が生じる可能性があります。デジタルファーストのアプローチの採用が拡大し、特にフィンテック企業や従来の銀行がオープンバンキングを受け入れるようになったことに伴い、API は金融機関が成功を収めるためにますます重要なものになりました。

## API トラフィックの急増

金融セクターでは API トラフィックが急増し、トラフィック量が 3 桁に達しました。このトラフィックの増加により、API 関連の脅威の発展に応じたセキュリティコントロールが求められるようになっています。




*Financial services remains the most frequently attacked vertical in APJ*

# 規制とセキュリティ

API などの革新的なテクノロジーの力を利用している金融機関では、公益という目的と金融の安定という目的が交錯しています。APAC 地域の多様な金融規制機関の間では、顧客の成果を増進するというコミットメントが共有されています。重要な目標は、金融の選択肢を増やして、競争の拡大とアクセシビリティの向上を促し、フィナンシャルインクルージョンを促進することです。APAC 地域の金融機関は、金融サービスの範囲を広げ、個人と組織の両方に利益をもたらすことを目指しています。

世界銀行によると、世界には銀行口座を所有していない成人が 17 億人もいます。注目すべきは、銀行口座を所有していない個人の割合が多い国のトップ 3 は、中国（13%、約 2.25 億人）、インド（11%、1.9 億人）、インドネシア（6%、9,600 万人）で、いずれもアジアの国であるということです。このように、APAC 地域には銀行口座を所有していない個人やエンタープライズが数多く存在しており、この巨大な未開拓市場の規模は 550 億～1,150 億ドルと推定されています。

## API セキュリティに関する規制の役割

改正決済サービス指令（Revised Payment Services Directive、PSD2）などの規制によって従来の金融機関に外部組織とのデータ共有が義務づけられると、透明性が高まります。このような規制の目的は、エンドユーザーのデータとプライバシーを保護し、セキュリティを確保することです。金融機関はこのような規制を遵守しながらイノベーションを起こし続けなければなりません。

また、規制によってデータ共有が促進されるだけでなく、企業によるデータの保存方法やデータとデータアクセスの保護方法が決定づけられます。Akamai のソリューションは、金融機関がイノベーションの取り組みを阻害されることなくこのような規制を遵守するために役立ちます。

# 堅牢な API セキュリティ戦略を構築するための 6 つのステップ

API ベースの攻撃を防ぐためには、もはやエンドポイントの保護と認証情報の確認だけでは不十分です。次の 6 つのステップからなる堅牢な API セキュリティ戦略を実行しなければなりません。

## 1. パートナーとのコラボレーション

金融機関とセキュリティパートナーは緊密に協力して、人、プロセス、テクノロジーを連携させ、API セキュリティリスクに対する堅牢な防御を確立しなければなりません。このコラボレーションには、開発チーム、ネットワークおよびセキュリティオペレーションチーム、アイデンティティチーム、リスクマネージャー、セキュリティアーキテクト、法務／コンプライアンスチームが関与します。

## 2. API の探索とカタログ化

API のセキュリティを確保するための第一歩は、組織全体の API を探索し、カタログ化することです。このプロセスを実行することで、セキュリティエンジニアはアタックサーフェスの範囲と機微な情報がリスクにさらされる可能性を把握することができます。

## 3. 脆弱性テストとリスク評価

金融機関は、API を探索した後に脆弱性テストとリスク評価を実行し、脆弱性を適時に特定して対処しなければなりません。このプロセスを API の開発サイクルとアップグレードサイクルに組み込み、継続的にセキュリティを確保する必要があります。

## 4. ふるまい検知の実装

API 保護は、アプリケーション・セキュリティ・フレームワーク全体の重要な要素です。ふるまい検知は、脆弱な API が悪用されるのを防ぐための鍵となる戦略です。このアプローチによって API のふるまいを継続的に監視、分析し、潜在的な脅威を特定します。

## 5. OWASP Top 10 の優先的管理

金融機関は、Open Worldwide Application Security Project（OWASP）Top 10 に含まれる API セキュリティリスクに優先的に対処し、総合的な保護を確立する必要があります。そうすることで、API に影響を及ぼす極めて重要な脆弱性と攻撃ベクトルを管理します。

**OWASP API Top 10 coverage by Akamai**

- ☑ **API1:2023 — Broken Object Level Authorization:** BOLA vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs.
- ☑ **API2:2023 — Broken Authentication:** BA refers to broad vulnerabilities in the authentication process, exposing the system to attackers that can exploit these weaknesses to compromise API object protection.
- ☑ **API3:2023 — Broken Object Property Level Authorization:** BOPLA is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.
- ☑ **API4:2023 — Unrestricted Resource Consumption:** This is a type of vulnerability, sometimes called API resource exhaustion, where APIs do not limit the number of requests or the volume of data they serve within a given time.
- ☑ **API5:2023 — Broken Function Level Authorization:** BFLA can occur when access control models for API endpoints are incorrectly implemented.
- ☑ **API6:2023 — Unrestricted Access to Sensitive Business Flows:** This risk arises when an API exposes critical operations like business logic without sufficient access control.
- ☑ **API7:2023 — Server Side Request Forgery:** SSRF allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing.
- ☑ **API8:2023 — Security Misconfiguration:** This refers to the improper setup of security controls, which can leave a system vulnerable to attacks.
- ☑ **API9:2023 — Improper Inventory Management:** This is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including deprecated, legacy, and/or outdated APIs — may be left unpatched and vulnerable to attack.
- ☑ **API10:2023 — Unsafe Consumption of APIs:** This refers to the risks associated with the use of third-party APIs without putting proper security measures in place.

## 6. 同業他社からの学習

金融機関は同業他社から学び、ベストプラクティスを共有する必要があります。Financial Services Information Sharing and Analysis Center（FS-ISAC）の加盟団体は、同組織の情報プラットフォーム、リソース、専門家どうしの信頼性の高いネットワークを活用し、サイバー脅威の予測、緩和、対応を行うことができます。他の組織が API セキュリティの課題にどのように対処しているかを明確に把握することで、業界全体のセキュリティ対策を強化することができます。

# 結論

幅広いソフトウェア、デバイス、データソースに柔軟かつ迅速にコスト効率良く統合できるよう設計された API が幅広く導入され、急速にデジタルトランスフォーメーションが推進されているこの時代に、APAC 地域の金融機関にとって API の保護は最重要事項です。しかし、API セキュリティは複雑かつ困難であり、さまざまな機能や企業の要望が関わっています。API セキュリティを無視すると、サイバー攻撃、データ漏えい、法令違反、組織の評判の失墜など、深刻な結果につながる可能性があります。

Akamai のデータによると、攻撃方法を継続的に進化させて順応させる攻撃者にとって、API の機能は最も魅力的なターゲットの 1 つです。そのため、API セキュリティをエッジに移し、インフラから遠ざけて、顧客とデータやアプリケーションの接点であるデジタルタッチポイントの近くに配置することが不可欠です。デジタル資産をしっかりと保護するためには、このような戦略的適応が極めて重要です。

**Akamai の金融サービス向けソリューションについて、詳しくは akamai.com/finserv でご確認ください。**

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティ体制の適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。公開日：2024 年 2 月