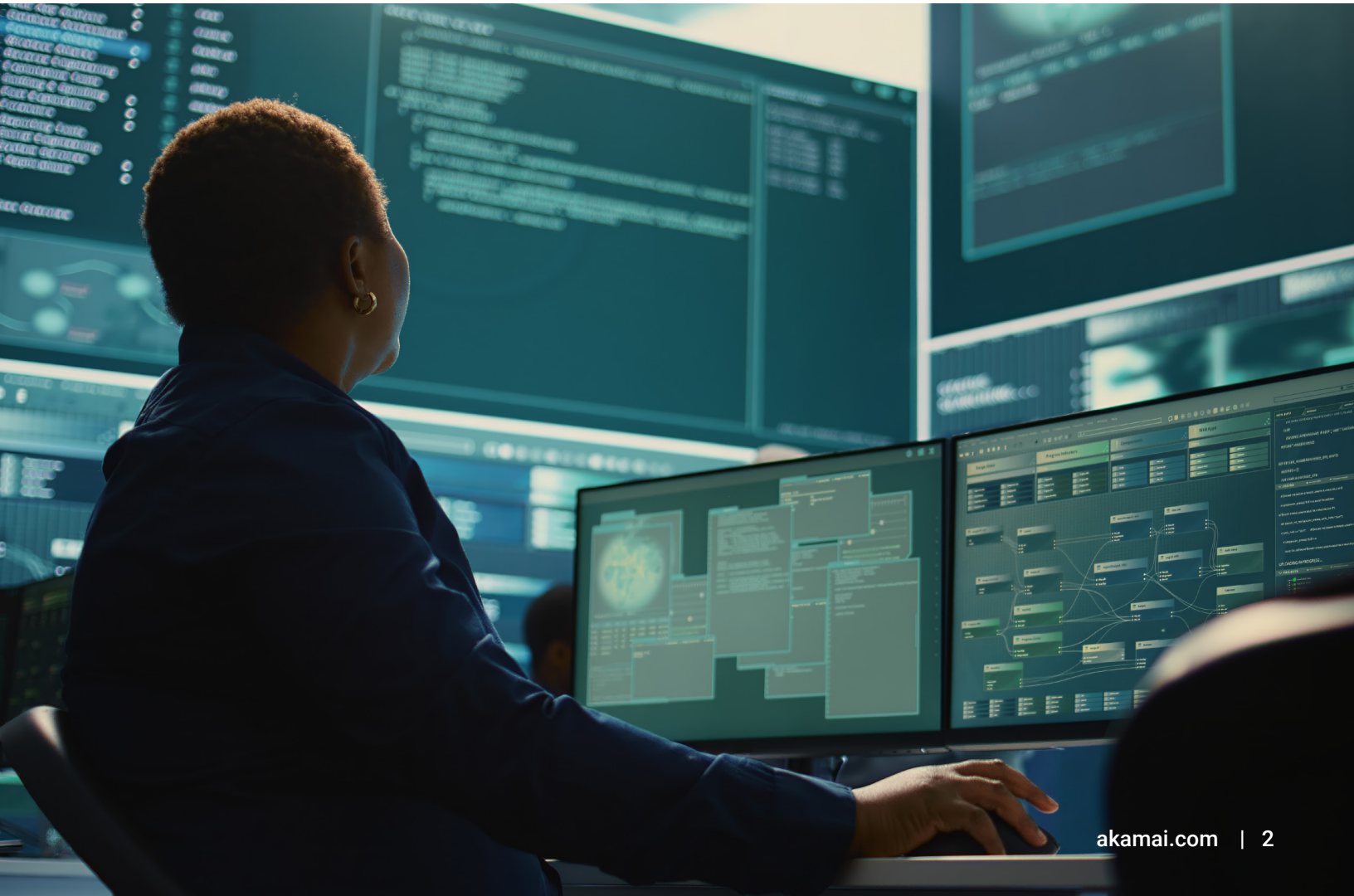
Akamai

ホワイトペーパー

API セキュリティとコンプライアンス

データ保護の暗黙的および明示的な要件

目次



はじめに

従来、データ保護規制へのコンプライアンスを実証するためには、莫大なエネルギーとリソースを投じて、ほぼすべての一般的なリスクに対応できなければなりませんでした。しかし、それが変わりつつあります。現在、アタックサーフェスが急速に進化し、多くのエンタープライズ・コンプライアンス・プログラムでは完全に対応しきれない脅威が現れています。その理由のひとつは、侵入を防止するために必要な範囲について規制機関自体が常に把握し、明確にできるわけではないためです。

これは API 保護にもあてはまります。顧客、パートナー、ベンダーとの間でデジタル処理が行われるたびに、各処理の背後で情報のやり取りを迅速かつスムーズに行うための API が機能しており、これらの情報に機微な情報が含まれることも少なくありません。そして、手っ取り早くデータを窃取するためには戦略をシンプル化して API を直接ターゲットにすればよいことが、攻撃者の間で周知の事実となっています。

すでにお気づきのとおり、規制において、API のインベントリ、評価、セキュリティ確保の必要性に関する言及が新たに登場しています。たとえ「API」と具体的に表現されていなくても、API が明確な攻撃ベクトルになっているという事実が、適切な保護の必要性を示していると言えます。

重要なコンプライアンス問題に API が出てくることも、意外なことではありません。それは、公開された API や設定ミスのある API は至るところにあり、簡単に侵害でき、多くの場合保護されていないということです。また、API がたった 1 つ侵害されただけで、数百万件ものレコードが窃取されるおそれがあります。数字が物語っています：

- 組織の 78% が API セキュリティインシデントを経験[1]。
- 44% が API セキュリティインシデントに関して規制当局に罰金を課された経験あり[2]。

これは、企業のコンプライアンスプログラムにどのような影響を与えるのでしょうか？規制当局は、機微な情報へのすべてのアクセスポイントを保護するための対策を組織が講じているかどうかを確認する必要があります。つまり、次のことを実証することが組織に求められています。

- 見つけにくいシャドウ API など、あらゆる API の動きを把握する
- API の脆弱性を検知して修正する
- カスタム制御を適用し、API を中心としたデータ漏えいを防止する

このホワイトペーパーでは、高まる API リスクの性質について解説し、API 保護を求める（明示的または暗黙的）規制やフレームワークの 6 つの例に焦点を当てて、API セキュリティのベストプラクティスでコンプライアンス要件を満たす方法に関するアドバイスを提供します。

1.、2.Akamai Technologies「The API Security Disconnect」（2023 年）

API リスクについて

API は、エンタープライズのデジタル製品、サービス、クラウド環境の中核となります。データに常時アクセスするため、API は収益作用因にも運用上のリスクにもなります。問題は、成熟したセキュリティプログラムを有するエンタープライズであっても、ほとんどのエンタープライズが、フィッシングやランサムウェアなどの脅威を重視するのと同じようには API 関連の脅威を重視していないことです。

組織によっては、API ゲートウェイや Web アプリケーションファイアウォール（WAF）をベースライン API の保護に使用しているところもあります。しかし、これらのツールは、専用の API セキュリティソリューションのような可視化、リアルタイム保護、継続的なテストを提供する設計になっていません。これらのツールだけでは不十分な理由は次のとおりです。

- API ゲートウェイや WAF は、これらを経由してルーティングされるマネージド型 API トラフィックしか監視できません。
- 管理されていない API は保護できません。しかし、2025 年までには、一般的なエンタープライズの API エコシステムにおいてこのような API が約半分を占めることになるとアナリストの間で予測されています。
- その結果、セキュリティチームは、API のルーティングや構成、やり取りされる機微な情報の内容、生じる可能性のあるリスクなどをほとんど把握できず、最も急速に拡大しているアタックサーフェスに対して保護の準備が十分にできなくなります。

規制当局において、ユーザー情報の保護は優先事項であり、顧客データを不正アクセスから適切に保護できない企業には厳しい罰金が科されます。API インベントリを完全に把握しているセキュリティ専門家 10 人中 4 人しか、機微な情報を返す API を把握していません[3]。また、API の呼び出し元が、脆弱性をテストしている攻撃者であることも少なくありません。これらを考慮すると、API を介したデータ侵害は増加の一途を辿るのみとなるでしょう。とりわけ今は、API 攻撃が非常に実行しやすくなっているのです。

3.Akamai Technologies「The API Security Disconnect」（2023 年）

コンプライアンスに関わる 4 つの API 攻撃

API 侵入は企業のコンプライアンス状況にどのような影響を与える可能性があるでしょうか？いくつかの例を紹介します。

- 一般的なプロジェクト管理アプリケーションが、認証制御のない API エンドポイントを悪用した攻撃者によって侵害されました。攻撃者は API に侵入して、数百万人のユーザー情報に不正アクセスし、数か月後にはメールアドレスや取締役会の情報など、21GB 以上のデータがインターネット上に漏えいしました。

- 大手通信会社が有する 1,100 万件以上の顧客レコードが露出しました。これは、API が知らないうちにインターネット上に露出し、認証が不要な状態だったことが原因です。攻撃者は API に侵入して固有の識別子がないことを確認し、ID 番号を推測して、機微な情報を簡単に要求することができてしまったのです。

- ある SNS 企業では、ここ数年で 2 回もスクレイピング攻撃に遭ったと報告されています。原因として、API の不正使用が考えられています。1 回目は、5 億人のユーザープロファイルから個人データが収集され、販売されてしまいました。2 回目は、7 億人のユーザーからデータがスクレイプされ、電話番号や給与データなどのデータベースが攻撃者によって作成されてしまいました。

- この手法は、他の SNS 企業に対しても用いられ、何百万人ものユーザーのデータが窃取されていました。サードパーティベンダーが企業の API を使用して機微な情報を収集していたため、50 億ドルの罰金が企業に科されました。問題とされたのは、ベンダーが API を悪用したことではなく、企業がアプリケーションを監視できなかったことでした。そのため、企業自体に罰金が科されました。

API セキュリティを課す規制やフレームワークに関する 6 つの例

多くの規制やフレームワークでは、必ずしも「API」と明確に言及されるわけではありません。しかし、各要件では、API が動作するアプリケーションやインフラのセキュリティ保護に対して明確に焦点が当てられています。以下に例を示します。

- Payment Card Industry Data Security Standard（PCI DSS）v4.0 では、組織のソフトウェアが外部コンポーネントの機能を安全に使用していることを確認するためのガイダンスを提供しています。これには、モバイルアプリから銀行のシステムに支払いデータを送信する API が含まれます。
- NIST セキュアソフトウェア開発フレームワークでは、適切に保護されたソフトウェアの作成、継続的な保護、脆弱性への対応に関するガイダンスを提供しています。API はソフトウェア開発の中核を担っています。

多くの場合、規制では、一般データ保護規則（GDPR）の「適切なセキュリティ対策」の要件など、データ保護に関する明確な目標が提示されています。ご使用の API は、データを提供するために、顧客だけでなく攻撃者からの呼び出しも含め、1 日に数百万件の呼び出しを受信しているかもしれません。どのようなセキュリティ制御が必要なのかを判断し、それがどのように機能するのかを実証するのは、企業自らの責任です。

API エコシステムに直接影響する規制やフレームワークについて詳しく見ていきます。

1. PCI DSS v4.0

PCI DSS は、Payment Card Industry Security Standards Council によって策定されたもので、決済データ保護の世界標準となっています。主要なクレジットカードを受け入れて、カード所有者データを電子的に処理、保存、送信するエンタープライズ組織は、この標準に準拠しなければなりません。

元のバージョンの要件はセキュリティの中核に対応し、これらは PCI DSS が 2006 年に公開されたときと同様に重要視されています。たとえば、システムおよびカード所有者データへのアクセス権は、関係者以外極秘で割り当てを行い、職務ごとにアクセス要件を定義します。

しかし、PCI DSS v4.0 が施行されると、エンタープライズは、決済テクノロジー内に存在する数千もの API を頻繁に狙う脅威アクターを考慮に入れてコンプライアンスプログラムを適応させる必要があります。全体的に、PCI DSS v4.0 は、主に次の 4 つの目的を中心に据えています。

1. 決済業界のセキュリティニーズを引き続き満たすこと
2. セキュリティが継続的なプロセスであることを認識してもらうこと
3. 要件を満たすうえで、エンタープライズ組織に柔軟性（新しいツール、新しい制御など）を持たせること
4. 検証方法とプロセスを強化すること

PCI DSS v4.0 の要件 6.2.3 では、組織がカスタム・アプリケーション・コード（標準的な市販の商用アプリケーションではない、サードパーティベンダーによって開発されたコード）を確認し、脆弱性が本番環境に入り込まないようにすることの必要性に重点が置かれています。特に API に関して、この要件は、組織のソフトウェアが外部コンポーネントの機能（ライブラリー、フレームワーク、API など）を安全に使用していることを確認するためのガイドラインを提示しています。これらの要件では、幅広いソフトウェア・サプライ・チェーンで API が担う重要な役割と、それを保護するために必要なことが明確に示されています。

API は、最新のアプリケーション環境での接続やデータのやり取りの方法としてデフォルトになっています。そのため、攻撃時にデジタルビジネスの耐障害性を確保するためには、本番環境の前（シフトレフト）と後（シールドライト）の両方で API を保護することが不可欠です。ここでは、要件 6.2.3 への準拠に役立つ API セキュリティのベストプラクティスについて、いくつか説明します。

- API ベースのコンポーネントの使用とそのセキュリティ対策を確認する（脆弱な暗号化アルゴリズムの使用をはじめ、脆弱性につながる不適当な設定を見つけるなど）。
- 使用する API に期待される正常なふるまいを検証し、攻撃者によるシステムの悪用を阻止するための制御を実装する（アプリケーションのふるまいをチェックして論理的な脆弱性を検知するなど）。
- API の強化に使用されているサードパーティフレームワークを検知して、古くなっていないか、あるいは脆弱になっていないかを判断する。
- 実行しているさまざまなバージョンを含め、すべての API の完全なインベントリを作成する。これにより、バックドアをはじめ、管理が必要なマニュアル化されていない潜在的機能に関する知見が得られます。
- API コードのセキュリティを検証し、API 関連の脆弱性が本番環境に紛れ込むことを回避する。
- API の安全なコーディングのベストプラクティスを実装する。これにより、コードを継続的かつ安全に配信できるプログラム的アプローチを採用できるようになります。

2. 一般データ保護規則（GDPR）

GDPR は、欧州連合内の個人のデータ保護を強化および統一することを目的とした欧州連合の法律です。欧州連合の法律ではありますが、GDPR の対象は EU を拠点とする企業だけではなく、EU で消費財やサービスを提供するあらゆる組織が遵守しなければなりません。

この規制では、個人データを、個人に紐づけられている情報または関連している情報と規定しています。GDPR に基づく規制対象のデータには、個人の氏名、連絡先情報、銀行および財務データ、医療情報が挙げられます。より技術的な見方になると、IP アドレスや Web の Cookie などのジオロケーションデータも対象データに含まれます。

これは API セキュリティにおいてどのような意味を持つのでしょうか？アプリケーション、マイクロサービス、モノのインターネット（IoT）デバイスのいずれを開発している場合でも、API はこれらのテクノロジーの中心的存在となり、GDPR で規制されたデータのやり取りが行われる可能性が高くなります。そのため、インターネットアクセス可能な API を開発する組織で API 設計を行う場合、データ保護は事後ではなく最初から考慮する必要があります。

最小権限の原則を考慮します。ここでは、ユーザーがジョブを実行するために必要最小限の権限しか持たないようにすることが求められます。

GDPR 第 25 条は最小権限という概念に根差しており、「デフォルトで、個々の特定の目的に必要な個人データしか処理されないようにする技術的措置及び組織的措置」を実装することが企業に求められています。そのため、API 開発者は、API を通過する機微な情報を保護するために、ユーザー認証と認可の制御を実装する必要があります。また、API 開発チームは、セキュアな通信プロトコルでクライアントとサーバー間での情報のやり取りを暗号化して、転送中においてもデータの機密性を維持する必要があります。

しかし、組織がこれまでに数年または数十年かけて構築してきた API の既存エコシステムについてはどうでしょうか？エンタープライズ API の大部分は、管理されていないか、忘れられているか、チェック・アンド・バランスもなく絶えず実行されています。このような場合、GDPR のコンプライアンスでは以下が求められます。

- IT 環境内 API をすべて検知すること
- リスク要因の評価（やり取りしているデータの種類、データにアクセスできる人やアクセス元など）
- 不適当な設定や脆弱な認証メカニズムなどの脆弱性の修復
- 新旧いずれの攻撃手法に対する耐障害性を目的とした API テストの継続的な実施

3. デジタル・オペレーショナル・レジリエンス法（DORA）

DORA の要件は、重要なインフラ事業者としての EU 金融部門の役割を考慮して、サイバー攻撃に耐え、攻撃から復旧できるよう EU 加盟国の組織をサポートすることを目的としています。DORA の採用により、情報通信テクノロジー（ICT）を対象とした、拘束力のある包括的なリスク管理のフレームワークが部門で構築されることになります。現在の状況では規制や規格が無数にあるため、EU 金融企業の要件を統一して強化することが法令の目的となります。

DORA の影響を受ける EU の金融機関および IT サービスプロバイダーは、合計 22,000 社以上に及びます。これには、クラウド・サービス・プロバイダーなど、EU の金融企業に ICT システムおよびサービスを提供するサードパーティも含まれます。この法令では、ICT のサードパーティリスク戦略を策定し、デューデリジェンスを実施してプロバイダーの適性を精査することが金融機関に求められています。

DORA では、デジタル運用の安定性など、API のセキュリティに関連する要件がいくつか規定されています。そのため、デジタル運用の安定性における潜在的なギャップ、脆弱性、欠陥を特定する定期的なテストプログラムを実施することが組織に求められています。ネットワーク・セキュリティ・テスト、侵入テスト、Web アプリテストなどを見てみます。金融系エンタープライズの規模、リスク、ビジネスプロファイルに応じて、脅威ベースの侵入テスト（TLPT）に基づく義務的レビューを実施することが重要です。同様に、API の脆弱性を定期的にテストすることも重要です。

DORA では、Web ベースのアプリケーションや API のテストなどのセキュリティテストの例を概説しています。これには、Open Worldwide Application Security Project（OWASP）などの公開リソースの利用も含まれます。特に、OWASP Top 10 API セキュリティリスクは、攻撃者に組織のリソースへのアクセス、操作、制御を許す設定エラー、脆弱性、ロジックの欠陥、コードの問題を組織で特定するのに役立ちます。

4.Health Insurance and Portability and Accountability Act（医療保険の携行性と責任に関する法律、HIPAA）

HIPAA では、データプライバシー規則やセキュリティ規則に重点を置き、電子カルテ（EHR）の保護医療情報（PHI）、電子化された医師の発注プラットフォーム、その他のヘルスケア IT システムを保護しています。PHI を電子的に保存または送信する米国のヘルスケアプロバイダー、保険管理業者、クリアリングハウスは、HIPAA を遵守する必要があります。これには、PHI の機密性、完全性、可用性を確保し、不正な開示や不適切な使用から保護することが含まれます。

HIPAA は、要件の中で「API」と明確に言及していなくても、API に重大な影響を及ぼす規制の一例と言えます。

24 時間対応のヘルスケアクリニック向けの患者ポータルを構築するテクノロジーベンダーを見てみます。これらのポータルの基本的な機能は、患者が医師の診察、検査結果、支払いなどに関するデータに効率的かつ安全にアクセスできるようにすることです。API は、こうしたデータのやり取りのファシリテーターとなります。病院とベンダーの両方が HIPAA 要件への準拠を義務付けられています。

HIPAA のプライバシー規則では、対象となる事業体に対して、「保護対象の保健情報へのアクセスや使用を従事者の特定の役割に基づいて制限するポリシーや手順を策定および実装しなければならない」と定めています。そのため、組織の API 開発者は、認証、一意のユーザー ID、ロールベースのアクセス制御などの技術的な保護手段を組み込み、最小権限が適用されるようにする必要があります。

また、IT チームが独自の API を構築するプロバイダーや、プロバイダー向けの API を開発するベンダーなどを含め、HIPAA の対象となる組織では可視性も重要となります。送信する PHI のタイプなど、各 API のリスク状況に関するリアルタイムの評価やレポートが組織に求められます。これは、コンプライアンスの遵守や HIPAA 要件の達成にも該当し、PHI が開示された時間、場所、理由、開示先に関する情報を個人が要求した場合、これに対応できることが求められます。

5.Network and Information Security Directive（ネットワークおよび情報セキュリティ指令、NIS2）

EU は、2023 年 1 月に NIS 指令のバージョン 2.0（v2.0）を採択しました。この指令は、IT インフラのセキュリティ確保とインシデントの報告に関する元のバージョンのガイドラインに基づいて作成されています。v2.0 では「API」と明確に言及していませんが、指令の対象となる組織が有する数多くのデジタルサービスの機能に API は不可欠なため、指令の要件は API の保護や管理においても大きな影響を及ぼします。NIS2 には以下の内容が含まれます。

- 広範に及ぶさまざまな部門：たとえば、クラウド・サービス・プロバイダーや SNS 企業などが既存のリストに加わります。これには重要なインフラ事業者も含まれます。これらの部門では、API が統合やサービス提供で広範に使用されるため、API セキュリティが優先事項となります。
- サプライチェーンの保護を新たに重視：エンタープライズはリスクを評価して、IT サプライチェーンやサードパーティサプライヤーとの関係を保護する必要があります。API は外部サービスの統合で使用されることが多いため、セキュリティを確保することがコンプライアンスの鍵となります。
- 情報セキュリティ管理システムを構築する要件：人材、ポリシー、テクノロジーを評価して機密性の高いリソースを保護し、運用上の耐障害性を確保します。API は攻撃ベクトルとして急成長しているため、リスク管理戦略に含める必要があります。
- API 侵入など、重大なサイバーセキュリティインシデントの報告：組織は、API 関連のインシデントを監視、検知、報告する体制を採り入れる必要があります。

6. 米国の金融サービス規制当局向けのガイダンス

FFIEC（連邦金融機関検査協議会）では、米国の金融業界を監督する連邦規制当局向けのガイダンスおよび基準を作成します。これには、連邦準備金制度、FDIC、OCC、NCUA が含まれます。同協議会の使命は、消費者と投資家を詐欺、悪用、不正行為から保護することです。FFIEC のガイダンスは、規制ではないものの、推奨されるセキュリティ対策への対応方法を金融会社に認識してもらう手掛かりとなります。

以下はドキュメントの重要例です。API のセキュリティを確保して消費者を不正や ID の盗難から保護する方法に関する具体的なガイダンスが記載されています。概要は次のとおりです。

- **インベントリ：**FFIEC では、API をはじめとするあらゆる情報システムのインベントリを構築して、認証やアクセス制御を義務付けることを推奨しています。これは、金融機関だけでなく、クラウド・サービス・プロバイダーなどのサードパーティにも適用されます。
- **認証：**API は、許可されたユーザーのみにアクセスを許可する必要があります。アクセス制御が必要なユーザー（顧客など）をすべて特定できるようにすることが重要です。また、多要素認証など、拡張制御が必要なユーザーを特定することも重要です。
- **認可：**API は、許可されたユーザーのみに特定のリソースへのアクセスを許可する必要があります。そのため、FFIEC では、階層化されたセキュリティの実装を推奨しています。たとえば、アクティビティの監視、ロギング、報告を実施して不正アクセスを特定および追跡することが一例として挙げられます。
- **リスク管理：**最新のガイダンスでは、FFIEC が数多くの効果的なリスク管理手法を明らかにしています。ただし、情報システムのインベントリのカテゴリで API が明示的に出てくるため、API のインベントリは正確に作成する必要があります。

フィッシングやランサムウェアなどの既知の脅威であれば迅速に対処できる組織もあることでしょう。しかし、FFIEC では、企業のデータや「金融機関情報システムに影響を与える可能性があると考えられる」場合には、あらゆるサイバー脅威を特定することが求められます。「はじめに」で説明したように、組織の 78% が API セキュリティインシデントを経験しています。したがって、金融規制機関の要件が絶えず進化する中、API 保護がコンプライアンス上の必須事項であることは有効であると言えます。

API 保護のベストプラクティスでコンプライアンスの問題に対応

今日の脅威状況では、API 探索、対策管理、ランタイム保護、API セキュリティテストを提供する完全な API セキュリティソリューションが求められています。この包括的なアプローチでは、すでに導入されている WAF または API ゲートウェイを補完することができます。

1.API 探索

多くの企業が自社の API を完全には把握していないのは、珍しいことではありません。ほとんどの組織では、API トラフィックの大部分が可視化されていません。多くの場合、API はすべて API ゲートウェイ経由でルーティングされると想定されているからです。しかし、必ずしもそうではありません。インベントリが完全かつ正確なものでなければ、エンタープライズはさまざまなリスクにさらされてしまいます。必要なコア機能：

- 設定やタイプに関係なく、すべての API を検索してインベントリを作成する
- 休眠 API、レガシー API、ゾンビ API を検知する
- 忘れられているドメイン、見落とされているドメイン、またはその他の不明なシャドードメインを特定する
- 盲点を解消し、潜在的な攻撃経路を明らかにする

2.API 対策管理

完全な API インベントリを導入した場合、API を通過するデータフローのタイプを把握し、規制要件への準拠に与える影響を理解することが重要になります。API 対策管理では、トラフィック、コード、設定が包括的に示され、組織の API セキュリティ対策を評価することができます。必要なコア機能：

- インフラを自動的にスキャンして、設定ミスや隠れたリスクを把握する
- カスタムワークフローを作成して、主要関係者に脆弱性を通知する
- 機微な情報にアクセスできる API と内部ユーザーを特定する
- 検知した問題に重大度のランクを付けて、修復の優先順位を設定する

3. API ランタイムセキュリティ

「データ侵害を想定する」という概念については周知のことでしょう。API 固有の侵入や攻撃は、必然の域に達していると言えます。本番環境で稼働しているすべての API において、攻撃をリアルタイムで検知してブロックできる必要があります。必要なコア機能：

- データの改ざんや漏えい、ポリシー違反、不審なふるまい、API 攻撃を監視する
- ネットワークの変更や面倒なエージェントのインストールを行うことなく、API トラフィックを分析する
- 既存のワークフロー（チケット発行、SIEM など）と統合して、セキュリティ／運用チームに警告する
- 攻撃や悪用をリアルタイムで阻止し、修復の一部または全部を自動化する

4.API セキュリティテスト

API 開発チームでは、1 秒でも早く作業する必要に迫られています。あらゆるアプリケーションの開発において、スピードは非常に重要です。しかし、急ぐあまり脆弱性や設計上の欠陥が発生しやすくなったり、検知されないまま進行してしまったりするものです。開発中の API は、本番環境にリリースする前にテストを実施しておくことで、リスクだけでなく、脆弱な API を修正するコストも大幅に軽減することができます。必要なコア機能：

- さまざまな自動テストを実行して、悪性トラフィックをシミュレーションする
- API を本番環境に展開する前に脆弱性を発見し、攻撃が成功するリスクを緩和する
- 定められたガバナンスポリシーやルールに照らして、API の仕様を確認する
- API に特化したセキュリティテストをオンデマンドで、または CI／CD パイプラインの一環として実行する

Akamai API Security が API コンプライアンスの複雑さを合理化する仕組み

API は侵入の主要な原因となっています。これを防止するために、現在の規制が策定されています。API の増加に伴いリスクも増大していく中、エンタープライズを保護するために何が必要でしょうか？多くの組織がベースライン API 保護に使用している既存のツールは、ある程度の保護を提供しますが、十分ではありません。組織の API を保護し、コンプライアンスを実証できるより良い方法をお探しであれば、ぜひご相談ください。

このホワイトペーパーで取り上げたあらゆる要件やガイダンスについては、Akamai API Security が、エンタープライズに必要な保護を強化します。規制を遵守するだけでなく、お客様のデータと信頼を保護するニーズにも対応します。

Akamai の包括的なソリューションにより、開発の初期段階から本番環境移行後までのあらゆる段階において API が保護され、中核となるベストプラクティスを遵守できるようになります。

- API 探索
- 対策管理
- ランタイム保護
- セキュリティテスト

API と攻撃から API を保護する方法について詳しくはこちらをご覧ください。

Akamai API Security が組織にどのように役立つのか、詳しくはこちらをご覧ください。