ホワイトペーパー

Akamai Security でコンプライアンスをビジネスの強みに

セキュリティの強化と監査対応への準備を支える
4 本柱のアプローチ

コンプライアンス実現の焦点となるセキュリティの 4 本柱

現在、GDPR や HIPAA、PCI DSS、地域的な要件の増加など、ますます規制が厳しくなり、世界中の組織が複雑に入り組んだ規制という迷路の中を進んでいます。しかし、コンプライアンスへの対応を実証することは、規制当局の基準を満たすことだけが目的ではありません。顧客や上級管理職、取締役会などの内部関係者との信頼を維持するうえでも不可欠となっています。

実際、コンプライアンス違反の影響は、直接的な規制上の罰則をはるかに超えています。コンプライアンス違反の代償には、調査および修復の段階での業務の中断、評判の低下、法的リスクの高まりなどが含まれます。組織がコンプライアンス要件に抵触すると、顧客離れによる収益損失のリスクが生じ、イノベーションではなく問題是正にリソースが割かれることで、運用コストが大幅に増加する可能性があります。Forrester によると、2024 年に発生した世界最大規模の侵害事案 35 件において、罰金総額が 30 億ドルに達し、そのうち 23 件は欧州連合（EU）の一般データ保護規則（GDPR）に関連する違反が原因として挙げられています。

かつては、規制が新たに策定されるたびに、セキュリティチームがコンプライアンスへの対応を行っていました。しかし、テクノロジーが急速に進歩し、攻撃の規模や苛烈さが増している現在では、ツールや成熟度モデルを評価する際に、コンプライアンスについても検討する必要があります。チームは、「今どのようなセキュリティの選択をすれば、現在および将来のコンプライアンス要件を満たすことができるだろうか」と自らに問いかける必要があります。

Akamai では、セキュリティのベストプラクティスにおける 4 つの柱を中心に話し合いを進めることで、コンプライアンス対応の重要な領域を無理なく強化し、セキュリティの選択に関する問いにお客様が答えを見いだせるように支援しています。4 つの柱は次のとおりです。

- IT 環境全体の可視性を実現
- ネットワーク、アプリケーション、API 間のラテラルムーブメント（横方向の移動）を防止
- 不正アクセスの防止
- 顧客に関する機微な情報およびアカウント情報を保護

この結果、明確な競争上の優位性がもたらされます。セキュリティの強化だけでなく、規制上の課題を乗り越え、対処する力が向上します。セキュリティとコンプライアンスが強化されると、顧客の信頼と社内のリーダーシップも獲得しやすくなります。

第1の柱
IT 環境全体の可視性を実現

コンプライアンスへの対応の基盤は、すべてのデジタル資産を包括的に可視化することから始まります。可視化されていないものを保護することはできないためです。規制当局は、完全な資産インベントリの証明、継続的な監視、脅威に対する認識をますます求めるようになっていますが、

これは簡単なことではありません。Forrester が実施した最近の調査によると、金融機関の半数以上（52%）が、**自社の IT 資産を完全に把握できていない**ことについて、「そう思う」または「非常にそう思う」と回答しています。残念ながら、いかなる業界においても、コンプライアンス違反には大きなリスクがあります。**10 万米ドルを超える規制上の罰金を支払った**組織の数は、2023 年から 2024 年で 20% 近く急増しました。

多くの組織にとって、可視性の課題は、ネットワークトラフィックと API の監視にあります。リスクに対する明確な可視化を求めるいくつかの規制と基準を以下に示します。

- Payment Card Industry Data Security Standard（PCI DSS）には、企業のソフトウェアが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 などの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が含まれています。
- 国際標準化機構（ISO）の IEC 27001 などの規格では、攻撃者がネットワークに侵入した場合に、データおよびデータ処理施設を分離する必要があります。
- 中華人民共和国のデータセキュリティ法では、さまざまな IT システム間で機微な情報を交換する技術を通じて、顧客の個人情報へのアクセスを保護するための堅牢なセキュリティ管理を求めています。

多くの企業は、これらの要件の一部を満たすツールやプロセスを有しています。しかし、企業がハイブリッドコンピューティング環境や複数の地域にわたって拡大していくにつれ、監視ははるかに困難になってきています。API では特に顕著です。Akamai の調査によると、API インベントリを完全に把握しているセキュリティ担当者のうち、**自社のどの API が機微な情報を返すのかを実際に把握している**のはわずか 27% にとどまりました。これは、すでに懸念されていた 2023 年の 40% からさらに減少しています。

最終的には、何をセキュリティの取り組みの中心にすべきか判断するために、組織は機微な情報の場所と情報のアクセス元を把握する必要があります。そのためには、下記について可視化が必要です。

- ハイブリッドクラウドおよびオンプレミス環境全体で、レイヤー 7 プロセスやエッジトラフィックなど、ネットワークと通信している（リアルタイムビューと履歴ビュー）IT 資産
- トラフィックソースやコードとの統合場所を示すシャドウ API やゾンビ API などの API インベントリ
- クライアントサイド JavaScript（最新の PCI DSS 要件において特に重要です）

Akamai のポートフォリオは、セキュリティチームが必要な可視性を得るのに役立ちます。

Akamai Guardicore Segmentation は、レイヤー 7 プロセス、ハッシュ、コマンドラインの詳細など、IT 環境全体においてネットワーク内で通信する資産を特定し、可視化できます。また、コンプライアンス監査時に、対象範囲の資産が侵害されていないことを証明するための履歴情報も可視化します。さらに、垂直方向（North ／ South）および水平方向（East ／ West）のトラフィックの可視化により、アクセスがどこで発生しているかも示します。

API Security は、組織がコンプライアンスに必要とする API のリアルタイムインベントリを提供し、暗号化されていないデータが API を通過する場所と時期を特定するのに役立ちます。

App & API Protector は、API インベントリ、機微な情報の流出検知、リアルタイムのトラフィック分析など、アプリケーションレベルの可視性を提供します。

Client-Side Protection and Compliance は、PCI DSS v4 に必要なクライアントサイドのスクリプトを可視化できます。

ある**ヘルスケア機関**は、HIPAA および SOC 2 のコンプライアンス要件に対応するため、Akamai Guardicore Segmentation を導入しました。当製品は、さまざまなアプリケーション間のトラフィックフローに関して有益な視点を提供しました。セキュリティチームは、レイヤー 4 ログだけでなく、ユーザー ID、コマンドライン入力、さらにはサービス間の関連性まで詳細を確認できました。

第 2 の柱

ラテラルムーブメントの阻止

セキュリティチームと同様に、多くの規制当局は、強固なセキュリティポスチャを敷いていてもデータ侵害が発生する可能性があることを認め、その際に被害を最小限に抑えられることの確証を企業に求めています。次に例を示します。

- GDPR **第 32 条**では、「処理システムおよびサービスの継続的な機密性、完全性、可用性、および回復力を確保する能力」と「物理的または技術的なインシデントが発生した場合に、個人データの可用性とアクセスを適時に復元する能力」が求められています。
- PCI DSS v4 でも同様に、ファイアウォールを実装して、クレジットカード所有者のデータを保護し、信頼できるネットワークと信頼できないネットワーク間の接続を制限するようにファイアウォールが設定されていることを確認することを求めています。
- **国際標準化機構／国際電気標準会議（**ISO **／ IEC）27001** などの規格では、攻撃者によるネットワーク侵入の発生時に、データおよびデータ処理施設を分離することを求めています。

ほとんどの組織でなんらかのファイアウォールが設置されていますが、攻撃者がネットワーク内にいる場合にラテラルムーブメント（横方向の移動）を制限するためには、より高度な制御が必要です。このため、マイクロセグメンテーション（できればソフトウェア定義）がコンプライアンスを実現するための重要なツールとなります。Akamai は、監査の懸念事項であるラテラルムーブメントに対応するための体制を整えています。

Akamai Guardicore Segmentation は、組織がコンプライアンスを維持するために必要なラテラルムーブメントを制限します。すぐに使用できるポリシーテンプレートにより、きめ細かなレイヤー 7 制御で、コンプライアンス関連のイニシアチブを迅速に実施できます。また、ソフトウェア定義であるため、資産の場所に関係なく、同じレベルのきめ細かな保護を提供できます。さらに、ネットワーク内で通信するアプリとセグメント化されたゾーン間での通信試行を識別する機能により、監査担当者は、脅威を緩和する能力にさらなる自信を持てるようになります。

攻撃者は、API の急増により、ラテラルムーブメントを行う新たな機会を得ています。特に、壊れたオブジェクトレベル認可（BOLA）攻撃に対して脆弱な API エンドポイントが狙われています。脅威アクターは、API リクエストのオブジェクト ID を操作して、ネットワーク内でラテラルムーブメントを実行します。そして、内部に侵入すると、認可をバイパスし、権限をエスカレートして、顧客データにアクセスします。

Akamai API Security は、適切な認証を行わずに機微な情報を公開する API にフラグを付けることや、不正なデータアクセスやラテラルムーブメントの引き金となる可能性のある、脆弱であるか設定に誤りがあるアクセス制御を使用している API を特定することが可能です。また、Akamai Web Application Firewall（WAF）との統合により、API Security は悪性の脅威をリアルタイムでブロックすることもできます。

Akamai をご利用いただいている、ある**グローバル金融サービス組織**は、環境内の未知の API で苦労していたため、API Security を実装しました。この導入により、API の乱立が大幅に減少し、コンプライアンスが向上しました。Akamai API Security は機微な情報を分類し、GDPR や HIPAA などの規制要件の順守を支援しています。規制監査中、これらの実装は、会社が適切な技術的措置を講じたことを示す直接的な証拠となります。

Akamai Security

今日の AI の脅威が、将来の規制上の課題に

今日では、組織のサイバーセキュリティ防御を評価する際には、AI という脅威を必ず考慮に入れる必要があります。AI 搭載のアプリケーション、大規模言語モデル（LLM）、および生成 AI と連動した API の急速な普及により、多くの組織がまだ認識していない新たな脆弱性が生じています。このようなアプリケーションの例としては、AI 搭載のチャットボット、小売企業向け推奨エンジン、健康診断ツール、リスク決定エンジンなどがあります。一方、脅威アクターは AI を活用して、より高度な攻撃を開始しています。

事業運営や公共事業への脅威が生じた場合、規制が適用される可能性が高くなります。

AI、データ、顧客への投資を保護したいと考えている組織は、Akamai に支援を求めています。可視性、ラテラルムーブメント、アクセス制御に関する今日の要件を満たしてきた実績のあるセキュリティプロバイダーとして、Akamai は将来の AI 要件を満たすためにプロアクティブに投資してきました。Akamai では、セキュリティソリューションを強化するために高度な AI 機能を開発し、組織独自の AI への投資を保護するためのソリューションを導入しました。

Akamai Firewall for AI は、従来のセキュリティツールでは対処できない AI 特有の脅威や攻撃を特定し、緩和することで、AI を活用するアプリケーションに包括的なセキュリティを提供します。Firewall for AI 専用の保護機能には、次のものがあります。

- **プロンプトインジェクションの防御** — 攻撃者が不正な入力によって AI モデルを操作することを防ぎます
- **データ損失防止（DLP）** — AI が生成する応答内の機微な情報の漏えいを検知してブロックするとともに、リクエスト内で機微な情報を受け取ることからも保護します
- **有害コンテンツフィルタリング** — 配信前に、ヘイトスピーチ、誤情報、攻撃的なコンテンツを検出してフラグを付けます
- **敵対的 AI 攻撃への対策** — リモートコード実行、モデルバックドア、データポイズニング攻撃から保護します
- **サービス拒否攻撃の緩和** — クエリの過剰な使用やモデルの過負荷を制御することで、AI を利用した DoS 攻撃を緩和します

さらに、Firewall for AI は、組織が既存のプライバシー、安全性、およびセキュリティのガイドラインを順守できるよう支援します。AI 固有のセキュリティポリシーを適用することで、企業はデータ保護規制、倫理的な AI の使用、および企業ガバナンスの要件に関連するリスクを緩和できます。

第 3 の柱

不正アクセスの防止

機密性の高いシステムや機微な情報へのアクセスを制御することは、ほぼすべての規制フレームワークにおけるコンプライアンスの基盤となります。組織は、アプリケーションと API のセキュリティポスチャを理解し、不正アクセスや不正行為を防止する必要があります。これには、ユーザーの適切な認証、必要に応じたアクセスの承認、すべてのアクセスアクティビティの詳細な記録の維持が必要となります。

規制要件を満たす完全なアクセス制御を実現するためには、組織は 3 つの重要な課題に対処する必要があります。Akamai のセキュリティポートフォリオは、それぞれに対処する徹底的な防御を実現するのに役立ちます。

1. アプリと API のセキュリティポスチャについて包括的に理解する

Akamai の App & API Protector を使用すると、実行中のすべての環境でトラフィックポリシーを適用できます。一方、Akamai API Security では、異常なアクティビティや不正なデータアクセス、または設定ミスの警告を受け取ることができます。これらはすべて監査における重要な考慮事項です。また、Akamai Guardicore Segmentation は、ネットワーク内で通信するすべてのアプリを追跡し、アクティビティのベースラインを確立します。

2. ユーザーのふるまいを監視し、機密情報へのアクセスを制限する

Akamai Guardicore Segmentation は、ユーザー ID に基づいてネットワーク内のアクセスを制限します。**App & API Protector** は、AI を利用した脅威検知機能を使用してトラフィックポリシーを適用し侵害を防止します。最後に、**Client-Side Protection & Compliance** は、JavaScript の実行動作を監視して、クライアントサイドの攻撃を緩和します。

3. 不正行為を検知して制限する

API Security は、API の異常なふるまいや誤って設定された認証制御を検知することで高リスクの攻撃をブロックするのに役立ちます。Akamai Guardicore Segmentation は、不正行為を示す可能性のある疑わしい接続にフラグを付けてブロックすることで、ネットワークを保護します。App & API Protector は、OWASP によって特定された脅威を検知して緩和し、不正行為のリスクをさらに軽減します。

NIS2 とアクセスのセキュリティ確保

更新されたネットワークおよび情報セキュリティ指令（NIS2）は、EU 加盟国全体で共通レベルのサイバーセキュリティを構築するために設計されています。NIS2 の最近の追加事項のひとつとして、企業は、人材・ポリシー・テクノロジーを評価して機微な情報を保護し、運用の回復力を確保する情報セキュリティ管理システムを構築しなければなりません。また、IT サプライチェーンとサードパーティサプライヤーとの関係のセキュリティ強化にも重点を置いています。

第 4 の柱

顧客に関する機微な情報およびアカウント情報を保護

包括的な規制対応アプローチの最後の柱として、組織は機微な情報に関する計画を策定する必要があります。顧客、患者、パートナーなどのデータのセキュリティを確保することは、セキュリティを重視するほとんどの規制の中心的な課題です。

たとえば、日本の個人情報保護法では、大量の個人データの処理や、リスクの高いデータ処理活動を伴うテクノロジーのリスクを特定して緩和できるデータ保護の影響評価が必要とされます。

米国の金融機関の場合、連邦金融機関審査委員会（FFIEC）は、監視、ロギング、レポートなどの階層化されたセキュリティを介して、承認されたユーザーの特定のデータへのアクセスのみを API が許可するように管理する必要があります。

この柱に対処するためには、まず脅威の検知から始めます。Akamai の Web アプリケーションおよび API 保護ソリューションである **App & API Protector** は、防御の第 1 レイヤーを提供します。**Akamai Guardicore Segmentation** は、垂直方向（North ／ South）および水平方向（East ／ West）のトラフィックを監視してセグメント化します。Akamai の**ボット不正利用防止ポートフォリオソリューション**により、自動化された脅威や人為的な攻撃に対してセキュリティレイヤーが追加されます。

ただし、脅威を適切に特定するためには、ネットワーク内のベースラインのふるまいも理解する必要があります。以下に、Akamai Security の機能がこれらの重要な知見を提供する仕組みについて説明します。

- Akamai API Security と Akamai Guardicore Segmentation は、それぞれネットワーク内で通信している API およびアプリの標準的な状態を把握し、異常なふるまいを検知できるようにします。
- App & API Protector のコアテクノロジーである Adaptive Security Engine は、ローカルデータとグローバルデータを使用して攻撃パターンを学習し、顧客特有の保護調整を行いながら、将来の脅威に対応します。
- Akamai Hunt は、Akamai のエキスパート・リサーチ・チームを活用したマネージド脅威ハンティングサービスです。企業がより積極的な防御アプローチを取ることができるよう支援します。

DORA とデータセキュリティ

デジタル・オペレーショナル・レジリエンス法（DORA）は、EU 加盟国の金融サービス機関がサイバー攻撃に耐え、そこから回復できるよう支援することを目的としています。DORA により、金融サービス業界は、情報通信技術（ICT）を対象とした、拘束力のある包括的なリスク管理フレームワークを備えることになります。DORA の第 3 条は、ICT ソリューションやプロセスの活用において、以下の要件を満たすことを要求しています。

- データ関連のリスク、不正アクセス、技術的な欠陥を最小限に抑える
- データの可用性の喪失、データ損失、完全性と機密性の欠陥を防止する
- データ転送のセキュリティを確保する

単なるコンプライアンスから競争優位性へ

効果的なコンプライアンスプログラムは、単に規制要件を「チェックするだけ」にとどまらず、その取り組みがビジネスに与える影響を示さなければなりません。Akamai のコンプライアンス重視のセキュリティソリューションを導入している組織は、3 つの重要な側面にわたって測定可能な改善点を報告しています。

コンプライアンスコストの削減

成熟したコンプライアンスプログラムを導入している組織では、通常、アドホックアプローチの場合よりもコンプライアンス活動に費やすコストが少なくなります。統合されたセキュリティプラットフォームを介して証拠収集を自動化することで、ポイントソリューションを包括的なプラットフォームに統合できるため、監査の準備にかかる時間を大幅に短縮できます。

リスクポスチャの改善

コンプライアンスの改善により、コスト削減に留まらず、大幅なリスク削減も実現する可能性があります。Akamai のセグメンテーションソリューションを導入した組織では、脆弱なラテラルムーブメント（横方向の移動）経路を制限し、リスクを軽減しながら主要なコンプライアンス要件に直接対応できます。

包括的な監視機能により、コンプライアンス違反が検知されない可能性がある盲点を排除することで、リスクの軽減に直接つながる可視性が向上します。

運用効率

コンプライアンスへの影響の 3 つ目の側面は、運用効率の改善です。事前に承認された制御と一貫したセキュリティパターンにより、新しいアプリケーションのセキュリティ承認が大幅に高速化されます。これにより、セキュリティ・レビュー・プロセスの障壁が減り、新しいアプリケーションの市場投入までの時間が短縮されることで、開発者の満足度が向上します。

コンプライアンスの微調整

規制要件の進化と組織の成長に伴い、それに適合するコンプライアンスアプローチが求められています。Akamai の統合セキュリティポートフォリオは、規制の傾向を予測し、組織の成長に合わせて拡張できるコンプライアンス戦略の基盤を提供します。

- 構成可能なポリシーフレームワークは、大幅な再設計を行わずに新しい要件に適応できます。また、拡張可能なレポート機能により、規制の進化に伴う新たな証拠要件にも対応できます。
- 新しいアセットのポリシー展開を自動化することで、ビジネスの拡大に合わせてコンプライアンスの適用範囲を自動的に拡張できます。
- 一元管理機能は、規模に関係なく包括的な可視性を維持します。また、包括的な API サポートにより、コンプライアンスプロセスを自動化して、複雑さの増大に対応することができます。

さらに組織は、定期的に規制を確認し、それに応じてコンプライアンス管理を更新していくよう積極的に取り組む必要があります。Akamai は、進化するコンプライアンス要件に対応できるよう特別に設計されたセキュリティソリューションを定期的に更新し、お客様が規制の変更にかかわらず継続的にコンプライアンスを維持できるようにします。

結論：競争上の差別化要因としてのコンプライアンス

効果的なコンプライアンスは、規制要件を満たすだけではありません。組織のパフォーマンス、顧客の信頼、競争上の位置づけに直接影響を与える戦略的なビジネス上の必須事項です。業界や地域にかかわらず、コンプライアンスに対する積極的なアプローチにより、強力でアジャイルなセキュリティポスチャを確保できます。

IT 環境全体の可視性、ラテラルムーブメントの阻止、不正アクセス防止、顧客に関する機微な情報やアカウント情報の保護という、コンプライアンス対応の 4 つの柱にわたる統合的なセキュリティアプローチを導入することで、組織は規制遵守にとどまらず、測定可能なビジネス価値をもたらす持続可能なコンプライアンス基盤を確立できます。

最大の成功を収めているのは、コンプライアンスをビジネスに必要なコストから戦略的な利点に転換し、デジタルトランスフォーメーションを可能にすると同時に、顧客の信頼、データの整合性、ビジネスの評判など、最も重要なものを保護している組織です。

Akamai がお客様の組織をどのように支援できるかについて、ぜひご相談ください。

お問い合わせ

 | 公開日：2025 年 7 月