ホワイトペーパー

設計に組み込まれたプライバシー

EU プライバシー要件への対応を念頭に設計された Akamai Bot Manager Premier サービスと Page Integrity Manager サービス

概要

Akamai は、個人データを保護し、プライバシー要件へのコンプライアンスを維持することが、当社のテクノロジーとサービスに対する信頼を確立する上で重要であることを理解しています。このホワイトペーパーでは、Bot Manager Premier[1] および Page Integrity Manager が EU の ePrivacy 指令および一般データ保護規則（GDPR）[2] にどのように準拠していて、これらのサービスの運用に伴うリスクをどのように評価できるかについて説明します。

Bot Manager Premier は、（ロ）ボットによって生成された Web プロパティへの自動アクセス要求を検知するように設計されています。このようなボットは、人間のふるまいを模倣してエンドユーザーのログインデータを収集し、悪用します。Page Integrity Manager は、これらのプロパティに不正な目的で挿入された JavaScript を検知します。ボットやスクリプトが検知されると、Akamai は、ユーザーの指示、一般的な知識、当社の脅威インテリジェンスに従って、悪性アクティビティと非悪性アクティビティに分類します。悪性アクティビティはブロックされ、非悪性のボットやスクリプトのみがオリジンサーバー、インフラ、データにアクセスできます。

いずれのサービスも、エンドユーザーが提供する個人データを窃盗や不正使用から保護します。このような脅威から保護することの重要性は、British Airways および The North Face で最近発生したセキュリティ侵害／データ漏えいで実証されています。

Bot Manager Premier のアーキテクチャ

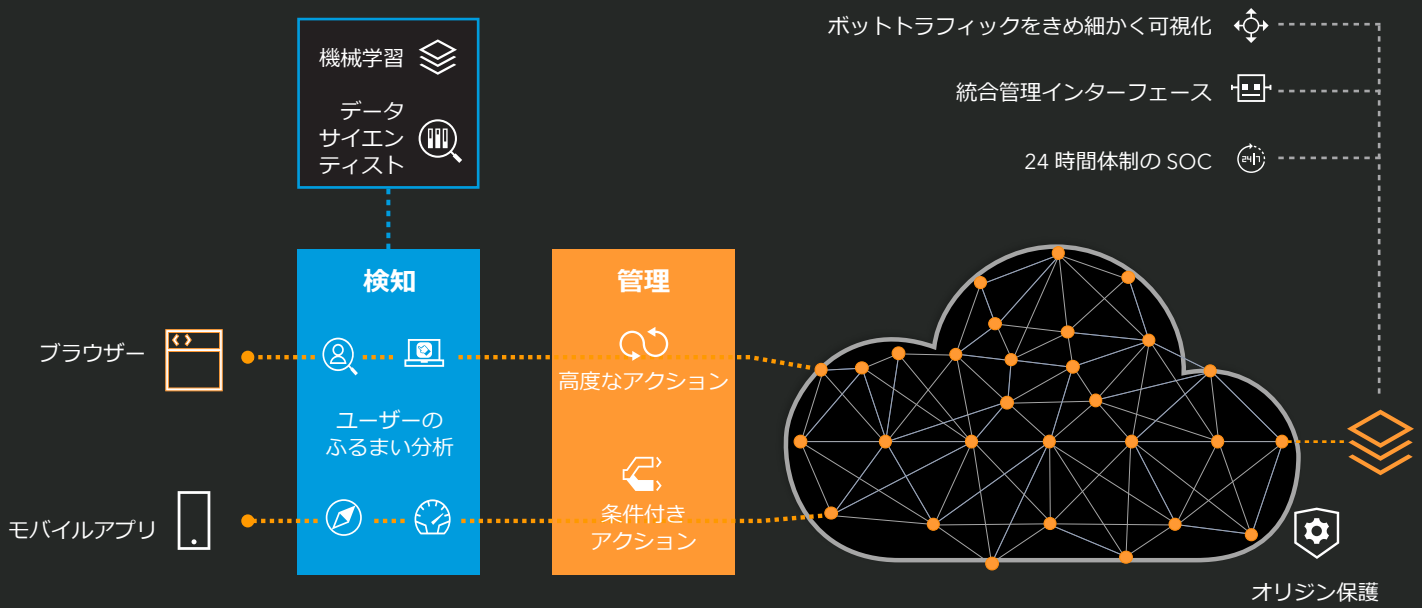


図 1：Bot Manager Premier のアーキテクチャ

Page Integrity Manager のアーキテクチャ

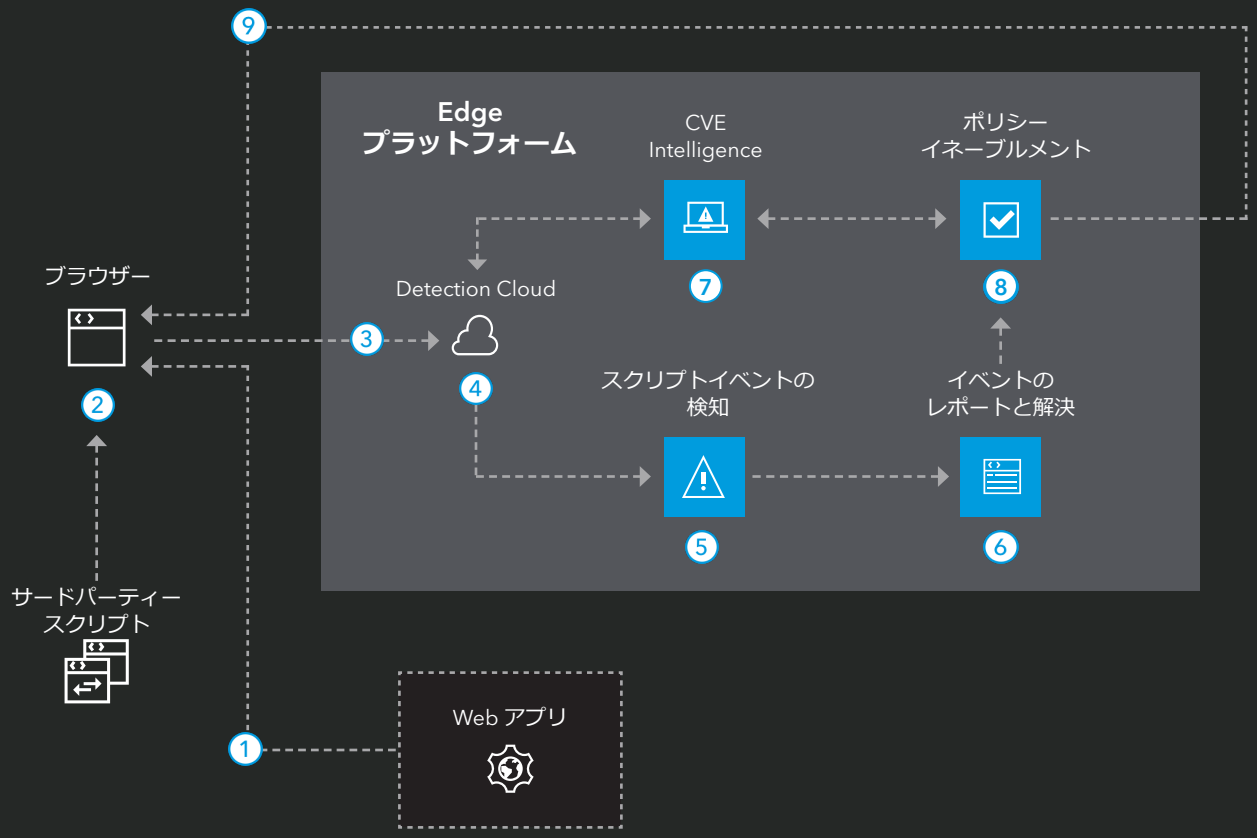


図 2：Page Integrity Manager のアーキテクチャ

技術面においては、JavaScript インジェクションを用いて、またはモバイルアプリのソフトウェア開発キット（SDK）を統合して、ネットワークデータ、ブラウザーデータ、ふるまいデータを収集して分析することにより、ボットとスクリプトを検知します。Bot Manager Premier がデータを分析して、アクティビティを実行したのがボットなのか人間なのかを判断し、Page Integrity Manager が Web プロパティに挿入されたすべてのスクリプトを識別します。検知したボットおよびスクリプトのアクティビティを悪性アクティビティまたは非悪性アクティビティのいずれかに分類し、悪性アクティビティをブロックすることで、データ窃盗を回避します。

プライバシー面においては、JavaScript インジェクションと SDK 統合は、EU の法律では「cookie テクノロジー」に分類され、ePrivacy 法の適用対象となります。さらに、エンドユーザーの IP アドレスなど、収集するデータ要素の一部は個人データとして分類され、GDPR の適用対象となります。

EU ePrivacy 法の遵守

Bot Manager Premier および Page Integrity Manager の cookie テクノロジーを EU のプライバシー法に従って使用する際には、2 つの一般的なルール（同意およびオプトアウトメカニズム）が免除となります。これらの免除により、Bot Manager Premier および Page Integrity Manager を Web プロパティに配置して、すぐに運用できます。

同意免除の適用

元来、ePrivacy 指令では、cookie テクノロジーおよび cookie テクノロジーを用いて収集したデータを使用する際には、エンドユーザーの同意を得ることを義務付けています。加入者またはユーザー（エンドユーザ）から明示的に要求された情報社会サービスを（Web プロパティ上で）提供するためには、cookie が必要不可欠な場合に限り、cookie の使用に関する個人の同意を必要とすることなく、cookie テクノロジーを使用することができます。[3]

EU 加盟国の多くは、ePrivacy 指令を国内法化する際に、この免除を取り入れています。

Bot Manager Premier および Page Integrity Manager で使用される cookie テクノロジーは、サービスの運用に必要不可欠です。JavaScript インジェクションがなければ、データを収集して分析することはできず、ボットやスクリプトが検知され、ブロックされることはありません。データ収集の目的は、Web プロパティ経由で提供される個人データを、侵害、窃盗、不正利用から保護することです。不正防止などのセキュリティサービスのために cookie テクノロジーを使用することは同意免除の対象であると、現地データ保護当局が認めています。[4] 次の表は、英国プライバシー監視機関（ICO）がセキュリティサービスに適用される同意免除について示した概要です。[5]

アクティビティ	免除の対象か？
セキュリティ	**目的の制限によって異なる。** セキュリティ目的で使用されるファーストパーティー cookie（繰り返し発生したログイン試行の失敗を検知するための cookie など）は必要不可欠であるため、免除の対象となります。また、このようなファーストパーティー cookie には、セッション cookie よりも長い時間を設定することもできます。 ただし、他社のオンラインサービスのセキュリティに関連する cookie については、同意が必要です。なぜなら、ユーザーが要求した機能は、他社サービスではなく、自社サービスに関連しているからです。 特定のセキュリティ目的のためにデバイスのフィンガープリント技術を使用する場合も、必要不可欠であるため、免除の対象となります。ただし、cookie と同様に、情報を二次的な目的（ユーザーが要求していないオンラインサービスのセキュリティなど）のために処理する場合は、同意が必要です。 不正防止のために情報を処理する場合、具体的には、複数のオンラインサービスが単一の不正防止サービスを使用し、それらすべてのオンラインサービス訪問者の情報を処理する場合は、同意が必要です。

オプトアウト免除の適用

ePrivacy 法は、cookie テクノロジーによるデータ収集からオプトアウトするメカニズムをエンドユーザーに提供することを企業に義務付けています。この要件は、GDPR 第 21 条に基づく異議を唱える権利を反映したものです。[6]

ただし、この制御権が悪用され、オプトアウトによってデータ保護活動（cookie テクノロジーに基づくセキュリティサービスなど）の実施が妨げられる場合があります。このコーナーケースは、cookie テクノロジーに基づくセキュリティサービスのパフォーマンスです。

悪性ボット／スクリプトを検知するための cookie テクノロジーからオプトアウトすると、個人データへの不正アクセスを防止するセキュリティサービスが停止してしまいます。cookie テクノロジーがセキュリティ目的のみに使用されている場合は、cookie テクノロジーによるデータ収集を制御するためのオプトアウトメカニズムをエンドユーザーに提供しなくても、権利や自由を侵害したことにはなりません。むしろ、このオプトアウトメカニズムを提供しないことにより、cookie テクノロジーを継続的に運用し、個人データを不正アクセスから保護できます。

世界中のプライバシー専門家が、このオプトアウト免除の要件に賛同しています。個人（エンドユーザー）に提供されるデータ制御メカニズムを悪用してデータに不正アクセスできる場合、そのデータ制御メカニズムは無意味であり、そのようなメカニズムは導入してはなりません。つまり、cookie テクノロジーに関連するデータ制御（オプトアウト）メカニズムを提供することよりも、最先端のセキュリティサービスを円滑に運用することの方が優先度が高いと一般的に考えられています。[7]

EU データ保護法の遵守

Bot Manager Premier および Page Integrity Manager は、収集する個人データの種類や収集の目的を含め、GDPR などのデータ保護法やプライバシー法を遵守しながらデータを処理します。

個人データの種類

Bot Manager Premier および Page Integrity Manager は、ネットワークデータ、ブラウザーデータ、ふるまいデータ（TCP セッション、TLS セッション、セッション ID、ユーザーエージェント、リクエストヘッダー、アクセスした URL、タイムスタンプ、エンドユーザーの IP アドレス、ブラウザー設定、エッジサーバーの地理位置データ、画面のタッチ、マウスの動き、キー押下など）を収集します。

目的

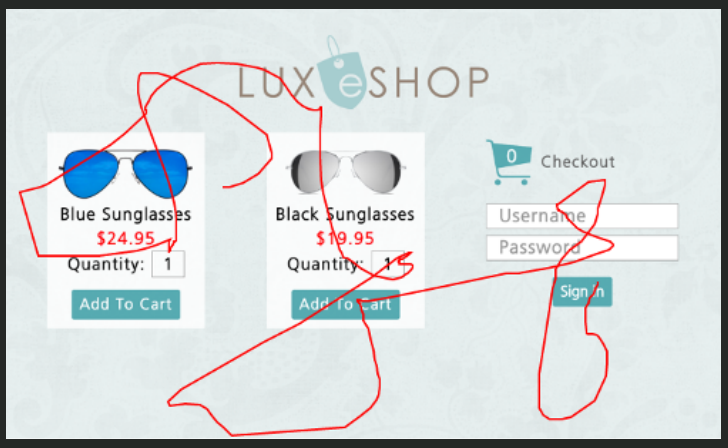
データを収集および分析する目的は、人間のふるまいを模倣する、悪性ボット／スクリプトを Web プロパティ内で検知して、データの窃盗や不正利用を防止することです。

この目的を達成するために、Akamai は Web プロパティにアクセスする際のデバイスの使用方法を分析しています。この分析を実行する際、Akamai は、エンドユーザーを特定したり、エンドユーザーのプロファイルを作成したりすることはありません。また、収集したふるまいデータが、個人を一意に特定するために使用されることもありません。そのため、これらのデータは、GDPR が定める生体認証データには該当しません。[8] したがって、機微なデータ（米国の条項）にも、特別なカテゴリーのデータ（EU の条項）にも該当しません。

Akamai は、以下の図に示すように、ユーザーの Web プロパティへのアクセスがボットと人間のいずれによって行われているかを判断するために、ふるまいデータを収集および分析しています。

マウスイベント

人間の例



ボットの例

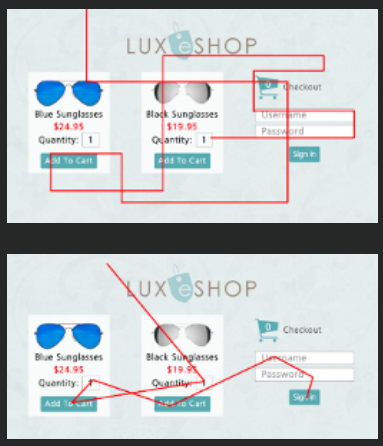
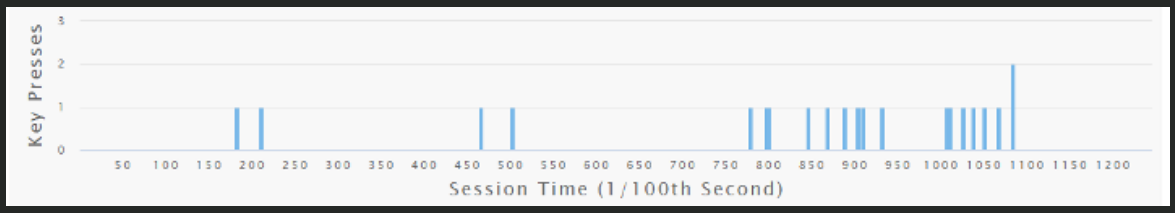


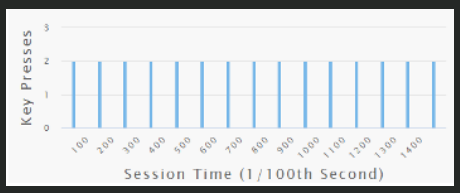
図 3:高度なボットは、マウスの動きをトリガーすることにより、ボットであることを隠そうとします。これは、人間による操作をエミュレートするように設計されています。しかし、一定の数を超えると、動きにパターンが出現します。Akamai は、これらのパターンを検知してボットを識別できます。

キー押下のパターン検知

人間によるキー押下



ボットによるキー押下の例



ボットによるキー押下の例

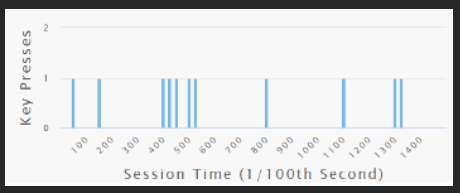


図 4：人間によるキー押下は通常、巧妙なボットと比べても、はるかにランダムです。人間によるキー押下の速度とリズムを調べることで、Akamai はユーザーがボットかどうかをさらに判断できます。

法的根拠

悪性ボット／スクリプトを検知してブロックするネットワーク／情報セキュリティサービスを提供することが Akamai の正当な利益であり、この正当な利益がデータ処理の法的根拠となります。正当な利益は、セキュリティサービスを実施するための法的根拠として GDPR で認められています。[9]

Akamai は、すべてのインターネットトラフィックの最大 30% を配信および保護しています。ボット／スクリプト管理サービスがなければ、オンラインデータの窃盗や悪用が現在よりも大幅に増え、エンドユーザーの権利や自由が損なわれることになります。

必要性および相応性の評価

Akamai のネットワーク／情報セキュリティサービスが、プライバシー法に基づいて最先端と見なされるためには、データ処理が必要不可欠です。収集したネットワークデータ、ブラウザーデータ、ふるまいデータを分析することで、Akamai はボットのアクションか人間のアクションかを正確に判断し、Web プロパティに挿入されたスクリプトを検知することができます。

今日の巧妙なボットとスクリプトに対応するために相応のデータ要素を収集および分析しています。収集するデータ量を減らすと、分析の精度に影響が及び、悪性アクティビティを効果的に検知できなくなります。エンドユーザーの IP アドレスを分析するだけでは、ボットを検知することはできません。ブラウザーとネットワークの詳細情報はデバイスの使用状況を示すものの、パッシブなシグネチャベースのメカニズムに限定されており、フォールス・ポジティブ（誤検知）やフォールス・ネガティブ（検知漏れ）が発生しやすい傾向があります。Web プロパティのための最新セキュリティ [10] には、高度なボット検知が必要です。人間のふるまいを模倣するアクティブなボットを検知するためには、ふるまいデータの分析が不可欠です。

収集するデータ量が増えても分析が改善しない場合は、過剰なデータ収集と見なされます。

リスク評価

Bot Manager Premier および Page Integrity Manager のデータ処理によって、エンドユーザーの権利と自由が損なわれるリスクは、低いと言えます。ブラウザーデータ、ネットワークデータ、ふるまいデータは、機密データ、機微なデータ、特別なカテゴリーの個人データには分類されていません。[11] Bot Manager Premier および Page Integrity Manager に関連する Akamai の処理活動については、Akamai のプライバシー保護方針に記載されており、当事者に公開されています。Akamai は、データ最小化原則に従って、ボットと JavaScript の検知に必要なデータのみを収集します。

Akamai は、処理対象の個人データを第三者による不正アクセスから保護するための適切な技術的かつ組織的な対策を講じています。この対策については、以下の Web サイトで公開しています。Akamai の情報セキュリティプログラムおよび Akamai の技術的かつ組織的な対策。

ボット／スクリプト検知の分析は、米国に展開された Akamai システムで実行されます。したがって、EU のエンドユーザーが Bot Manager Premier および Page Integrity Manager で保護された Web プロパティにアクセスする場合は、分析時に EU の個人データを米国内で処理する必要があります。米国での処理時に適切なデータ保護を確保するために、Akamai は、Akamai グループ、お客様、サブプロセッサーを対象に EU 標準契約条項を設け、米国で処理する個人データを第三者アクセスから保護するための追加の技術的保護対策を導入しています。

Akamai は、Akamai 組織の所在地に関係なく、すべてのグループ組織に同じデータ保護要件を適用しています。当社は、転送データを第三者アクセスから保護するための補足対策を導入しています。さらに、Akamai の見解では、Bot Manager Premier および Page Integrity Manager に関連して Akamai が米国に転送するデータは、（米国の）監視機関が監視業務を実施する際に関心を持つ種類のデータではありません。[12] ほとんどのデータは、インターネット接続を確立するための要件として自由にアクセスできる状態になっており、サードパーティーがそのようなデータを収集するために Akamai を経由する必要はありません。第三者がこのようなデータにアクセスするための効果的な方法は他に数多く存在します。したがって、Akamai では、Bot Manager Premier および Page Integrity Manager に関連して米国に転送されるデータがサードパーティーによってアクセスされるリスクは最小限であると評価しています。詳細については、Akamai Privacy Trust Center にあるデータ転送に関する Akamai の声明をご覧ください。

Akamai では、データ最小化とデータセキュリティの原則に従って、データの保持期間を 90 日に設定しています。これは、特定の期間および複数の地域にわたってネットワークデータ、ブラウザーデータ、ふるまいデータを分析し、最も効果的なボット／スクリプト検知を実現するための適切な期間です。

Akamai が提供するボット／スクリプトの検知／管理サービスにより、Web プロパティのセキュリティを確保できるだけでなく、インターネット全体の状態を改善できます。Akamai Intelligent Edge プラットフォームでボットやスクリプトを検知してブロックすることで、エンドユーザーの個人データの窃盗や不正利用を防止できるだけでなく、ネットワークやセキュリティサービスのための脅威インテリジェンスを獲得して、そのメリットを数百万人ものエンドユーザーに提供できます。

緩和策

Akamai は、Bot Manager Premier サービスおよび Page Integrity Manager サービスの運用によって発生するデータ主体の権利と自由に関するリスクを特定し、これらのリスクを緩和しています。ふるまいデータの収集時にエンドユーザーが特定されることはありません。また、Akamai は個人データを適切に保護しており、転送データを第三者アクセスから適切に保護するための対策も追加しています。

まとめ

Akamai Bot Manager Premier および Page Integrity Manager は、EU のデータ保護法に準拠しています。両サービスの運用に使用される cookie テクノロジーは、エンドユーザーの個人データを保護するために必要不可欠であるため、同意要件およびオプトアウトメカニズムの免除が適用されます。

両サービスの運用に必要なデータ収集は、正当で、必要で、相応のものです。また、緩和措置により、処理活動がエンドユーザーの権利や自由にもたらすリスクを非常に低く抑えています。Bot Manager Premier および Page Integrity Manager により、すべてのユーザーがより安全なインターネットを享受できるようになるため、両サービスのパフォーマンスがエンドユーザーやその他のオンラインユーザーにもたらすメリットは、リスクを上回ります。

Akamai Technologies
Dr. Anna Schmits、EMEA DPO

出典：

1. 本書の記載内容は　Akamai Service Bot Manager Standard にも当てはまります。ただし、Akamai Service Bot Manager Standard　で収集するデータはネットワークデータとブラウザーデータのみです。Akamai Bot Manager の詳細：https://learn.akamai.com/en-us/products/cloud_security/bot_manager.html
2. 次の URL にある「デジタルプライバシー」を参照してください。https://ec.europa.eu/digital-single-market/en/online-privacy
3. 指令 2006 ／ 24 ／ EC による ePrivacy 指令 2002 ／ 58 ／ EC 第 5 条（3）の改正を参照してください：https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN。
4. 英国 ICO の cookie ガイドライン：https://ico.org.uk/for-organizations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9、フランス CNIL のガイドライン：https://www.cnil.fr/en/cookies-and-other-tracking-devices-council-state-issues-its-decision-cnil-guidelines、ドイツ当局委員会のガイドライン（ドイツ語のみ）：https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf を参照してください。
5. ICP の cookie ガイダンス：https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply16。
6. GDPR 第 21 条（1）：https://gdpr-info.eu/art-21-gdpr/。
7. ICO のガイダンス：https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules9。
8. GDPR 第 9 条（1）：https://gdpr-info.eu/art-9-gdpr/。
9. GDPR 備考 49：https://gdpr-info.eu/recitals/no-49/
10. GDPR 第 32 条に基づく要件：https://gdpr-info.eu/art-32-gdpr/
11. GDPR 第 9 条：https://gdpr-info.eu/art-9-gdpr/
12. Schrems II（2020 年 9 月）以後の EU - 米国間のデータ転送に関する SCC およびその他の EU の法的根拠に関連する米国のプライバシー保護措置。URL：https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

Intelligent Security Starts at the Edge

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、Web ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日 /24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com、blogs.akamai.com および Twitter の @Akamai で紹介しています。全事業所の連絡先情報は、www.akamai.com/locations をご覧ください。公開日：2021 年 3 月。