ndards/MPEG-DASH_schema_files/DASH-MPD.xsd" profiles="urn:mpeg:dash:profile:isoff-live:2011" type="dynami tationDelay="PT6S" availabilityStartTime="2019-03-07T06:00:04Z" publishTime="2019-03-07T22:26:16Z" timeSh e="PT6.0S"> <ProgramInformation src="https://preview.tinyurl.com/y6fb2nhr"> </ProgramInformation> <Period e="video" segmentAlignment="true" bitstreamSwitching="true" frameRate="30000/1001"> dwidth="2000000" width="1280" height="720" frameRate="30000/1001"> <SegmentTemplate ="5.967" initialization="1551938403/init-stream\$RepresentationID\$.m4s" media="1551938403/chunk-stream_t_\$ ="1"> </SegmentTemplate> </Representation> </AdaptationSet> <AdaptationSet contentType="audio" segmentAli entation id="1" mimeType="audio/mp4" codecs="mp4a.40.2" bandwidth="96000" audioSamplingRate="48000"> <Aud h:23003:3:audio_channel_configuration:2011" value="2" /> <SegmentTemplate timescale="1000000" duration="6 tion="1551938403/init-stream\$RepresentationID\$.m4s" media="1551938403/chunk-stream_t_\$RepresentationID\$-\$ te> </Representation> </AdaptationSet> </Period> </MPD> <?xml version="1.0" encoding="utf-8"?> <MPD xmlns nce" xmlns="urn:mpeq:dash:schema:mpd:2011" xmlns:xlink="http://www.w3.org/1999/xlink" xsi:schemaLocation= ds.iso.org/ittf/PubliclyAvailableStandards/MPEG-DASH_schema_files/DASH-MPD.xsd" profiles="urn:mpeg:dash:p datePeriod="PT500S" suggestedPresentationDelay="PT6S" availabilityStartTime="2019-03-07T06:00:04Z" publis th="PT18.0S" minBufferTime="PT6.0S"> <ProgramInformation src="https://preview.tinyurl.com/y6fb2nhr"> </Pr ationSet contentType="video" segmentAlignment="true" bitstreamSwitching="true" frameRate="30000/1001"> <R s="avc1.64001f" bandwidth="2000000" width="1280" height="720" frameRate="30000/1001"> <SegmentTemplate ti TimeOffset="5.967" initialization="1551938403/init-stream\$RepresentationID\$.m4s" media="1551938403/chunkrtNumber="1"> </SegmentTemplate> </Representation> </AdaptationSet> <AdaptationSet contentType="audio" se ="true"> <Representation id="1" mimeType="audio/mp4" codecs="mp4a.40.2" bandwidth="96000" audioSamplingRa dUri="urn:mpeg:dash:23003:3:audio_channel_configuration:2011" value="2" /> <SegmentTemplate timescale="10 ="5.979" initialization="1551938403/init-stream\$RepresentationID\$.m4s" media="1551938403/chunk-stream_t_\$ ="1"> </SegmentTemplate> </Representation> </AdaptationSet> </Period> </MPD> <?xml version="1.0" encoding ://www.w3.org/1999/ PSD2 コンプライアンスの es/DASH-MPD.xsd" pr entation id="0" mim オフロードとシンプル化 e="1551938403/chunk-="1551938403/chunktentType="audio" segmentAlignment="true '1" mimeType="audi ="1551938403/chunk-stream_t_\$RepresentationID\$-\$Number%05d\$.m4s" startNumber="1"> </SegmentTemplate> </Re ml version="1.0" encoding="utf-8"?> <MPD xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="urn k="http://www.w3.org/1999/xlink" xsi:schemaLocation="urn:mpeg:DASH:schema:MPD:2011 http://standards.iso.o ndards/MPEG-DASH_schema_files/DASH-MPD.xsd" profiles="urn:mpeg:dash:profile:isoff-live:2011" type="dynami tationDelay="PT6S" availabilityStartTime="2019-03-07T06:00:04Z" publishTime="2019-03-07T22:26:16Z" e="PT6.0S"> <ProgramInformation src="https://preview.tinyurl.com/y6fb2nhr"> </ProgramInformation> <Period e="video" seqmentAliqnment="true" bitstreamSwitchinq="true" frameRate="30000/1001"> <Representation id="0 dwidth="2000000" width="1280" height="720" frameRate="30000/1001"> <SegmentTemplate timescale="1000000" d

目次

tion:2011 " vaPSD2 コンプライアンスのオフロードとシンプル化

はじめに	02	
Akamai と Raidiam の対応	02	
新たな課題と機会	03	
サードパーティへのアクセス権付与	03	
アイデンティティ、同意、認証	03	
カスタマーアイデンティティ	04	
同意と認可	04	
強力な顧客認証	05	
API ガバナンス	05	
相互 TLS	06	
PSD2 成熟度モデル	07	
結論	09	
追加情報	10	

はじめに

改訂版欧州決済サービス指令(PSD2)とオープンバンキング (英国における PSD2 の実装)は、金融機関に対し、決済インフ ラストラクチャを公開して顧客の銀行口座データへのアクセス 権をサードパーティープロバイダー(TPP)に付与することを求 めています。規制機関がこのイニシアチブを推進しているのは、 TPP が消費者に決済サービスと口座情報サービスを提供できる ようにすることで、金融サービスのイノベーション、競争、 効率性が促進されるためです。

PSD2 は規制要件ですが、優れたユーザー体験と顧客重視の金融サービスを提供することで、金融機関は PSD2 を競争優位への好機とすることもできます。しかし、PSD2 の遵守は新たな技術的課題をもたらします。機微な情報の漏洩、誤用、または不適切な共有を確実に防止できる強力なセキュリティ制御が必要です。

このホワイトペーパーでは、PSD2 のコンプライアンス要件、課題、機会について概説し、実装最適化へのロードマップを提示します。比較的規模の大きいエンタープライズ組織のテクノロジーリーダーの方にお役立ていただける内容となっています。

Akamai と Raidiam の対応

Akamai ソリューションは、顧客体験、アプリケーションの安定性、セキュリティコントロールを強化することで、金融機関による PSD2 コンプライアンスを支援します。エンタープライズはそれぞれの組織のニーズに最適なツールを選択します。Akamai のソリューションは、クラウド、オンプレミス、ハイブリッドのいずれの環境にも簡単に統合できるため、総所有コスト(TCO)の低減に役立ちます。

Raidiam は、顧客と IoT のアイデンティティに重点をおいたデジタル変革サービスを提供しているアイデンティティ専門企業です。Raidiam の創業メンバーは、英国のオープンバンキングに対応した初めてのプラットフォームを考え出したアーキテクトであり、OpenID Foundation Financial Grade API(FAPI)標準の開発においても重要な役割を果たしました。そのため、同社は PSD2 に関連した法的な障害、組織における課題、技術オプションについて深い知識と経験を有しています。

改訂版欧州決済サービス指令 (PSD2)

これまで金融機関のみが実施していた電子決済取引のセキュリティ確保を目的とした EU 指令

Electronic Identification, Authentication and Trust Services (eIDAS)

欧州電気通信標準化機構(European Telecommunications Standards Institute)が企業、市民、公的機関の間の電子取引を安全かつシームレスなものとするために定めた基準

サードパーティプロバイダー(TPP) サービス提供を目的とした銀行口座 情報へのアクセスについて認可を受 け、アクセス許可を依頼できる口座 情報サービスプロバイダー(AISP) または決済指図伝達サービスプロバ イダー(PISP)

新たな課題と機会

PSD2 は特定のテクノロジーコンポーネントの使用を義務付けるものでなく、コンプライアンスを達成するために最適な方策は金融機関自身が評価し判断できます。つまり PSD2 は課題であるとともに好機でもあるのです。このエンタープライズアプリケーションのサイロから顧客重視のアプローチへの移行は、ソリューションの導入にも影響します。

PSD2 が提起する技術上およびビジネス上の課題:

- すべての製品でユーザー体験に関する顧客の期待を満たしながら顧客を管理する
- ビジネス機会を最大限に活用できるような戦略を確立する
- ビジネスニーズを満たしつつ、コスト効果が高い形で技術的課題を解決する

PSD2 を遵守してソリューション全体の複雑さとコストを管理した場合に金融機関が得られるメリット:

- 顧客体験の向上
- 顧客のニーズを満たすことによる顧客からの信頼の確立
- 競争力のある新たな金融商品およびサービスの提供

サードパーティへのアクセス権付与

PSD2 は、直接契約を締結していないサードパーティプロバイダー(TPP)に正規の利用法を開示することを求めています。TPP は、金融サービス業界における新しいクラスのプロバイダーです。こうしたことは長年暗黙のうちにおこなわれていましたが、銀行の多くは依然として彼らの顧客との関係の管理にとどまっています。

PSD2 のカスタマーアドボカシーグループや規制当局は、適切にコントロールされたサードパーティが他のサードパーティや従来の金融サービスコミュニティと公正に競争できるような環境の整備を目指しています。

アイデンティティ、同意、認証

顧客の期待と PSD2 における組織の責任を両立するためには、以下の 3 要素が重要です。

- セキュリティ データおよびトラストアグリー メント(信託契約)を確実に保護する
- アイデンティティ 顧客が自らのデータを コントロールできるようにする
- プライバシー 収集された顧客データを 保護する

セキュリティ
PSD2
アイデン
ティティ
プライバシー

図 1: PSD2 の主要 3 要素

カスタマーアイデンティティ

PSD2 に基づいて事業価値を提供しようとする場合、アイデンティティは重要な役割を果たします。アイデンティティの目標は、PSD2 に基づくユーザージャーニー全体を通じて、ユーザーに自らの情報、アカウント、認可に対するアクセス、制御、選択の権限を与えることです。アイデンティティのソリューションと実装を適切なものとするためには、決済サービスユーザー(PSU)とも呼ばれる顧客が、安全で低フリクション(消耗が少ない)のユーザー体験を得ながら、情報に基づいた意思決定を行えるようにする必要があります。

最新のインターネットプロトコルである OAuth2 や OpenID Connect は、最適なアイデンティティソリューションの実現に最適といえます。これらの標準は、現在 Akamai の一部である Janrain と OpenID Foundation が共同で開発したものです。最近標準化されたハイアシュアランス設定によって、これらのプロトコルは PSD2 など金融サービスのユースケースに適した堅牢なものとなっています。最新のインターネットプロトコルを使用することで、顧客の認証情報がシェアされることを防ぐとともに、明示的な顧客の同意に基づいてサードパーティのアクセス権を厳格に制御することができます。

同意と認可

一般的に同意はアイデンティティソリューションとは独立して管理されるものとみなされていますが、両者を統合すれば、認証の過程で同意と認可の収集を行える、より広範なメタデータソリューションを活用できます。この方法には、トランザクションフローのやりとりの中で顧客の同意を得ていくことができるなど、いくつかの利点があります。また認可リクエストの面でも有利です。

PSD2 では、以下に関して PSU の明示的な同意認可が必要とされます。

- 決済口座データを口座情報サービスプロバイダー(AISP)と共 有する
- 決済指図伝達サービスプロバイダー (PISP) が決済口座からの 決済を開始できるようにする
- カードベース支払手段発行者(CBPII)が資金確認(Confirmation of Funds) リクエストを口座保有型決済サービス提供者(ASPSP) に送信できるようにする

ロ座保有型決済サービスプロバイ ダー(ASPSP)

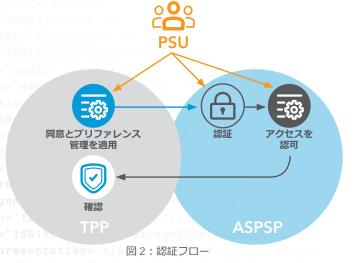
一般的には、口座を保有する銀行

口座情報サービスプロバイダー (AISP)

口座情報統合サービスを提供するプロバイダー

決済サービスユーザー(PSU)

自身の口座へのアクセスに関して TPP に同意を与えるユーザー



たとえば、TPP によって認可のリクエストが開始される場合、PSU は認可のためにその ASPSP に送られる必要があります。認可されると、PSU は TPP にリダイレクトされて戻され、取引が完了します。認可はトークンに保存され、あらゆる API コールに対してトークンが検証されます。

一般的に認可管理においては、PSU による以下の行為を可能にする必要があります。

- 同意の撤回
- すべてのデータまたは特定データへのアクセス の一時的な有効化または無効化

強力な顧客認証

新たな PSD2 ルールには、強力な顧客認証(SCA: Strong Customer Authentication)と呼ばれる要件が 含まれています。顧客に一貫した認証を提供するため、SCA に定められている基準は、ファーストパーティ である銀行であるか、サードパーティの金融サービスインターフェースであるかに関わらず、すべての 当事者に適用されます。また、SCA によって顧客アクセスのセキュリティ強化が推進され、脆弱な認証 プロセスによる詐欺行為が減少するという効果も期待できます。

例外が適用されない限り、当事者による以下の行為には SCA ルールが適用されます。

- 電子決済取引を開始する
- 決済口座にオンラインでアクセスする
- 支払い詐欺のリスクがあるアクションをリモートから実行する。

SCA ソリューションは、スマートフォンを持たない人も含め、あらゆる顧客層に利用可能なものとする必要があります。そのためには、異なる複数の認証手段の提供が必要となる可能性があります。また、SCA の実装によって不必要にカスタマージャーニーが阻害されたり、顧客体験の質が低下したりする事態は避けなければなりません。コンテキストに対応したユーザージャーニーを認証、認可、同意管理に導入すれば、より魅力的なユーザー体験を提供できます。

API ガバナンス

PSD2 および規制技術基準(RTS)は、金融機関に対し、安全な 通信インターフェースを利用できるようにすることを義務付け ています。これらの基準では、インターフェースは、TPP によ る金融サービスの提供を妨げることなく「常に同レベルの可用 性とパフォーマンスを提供」しなければならないとされています。このような要件を満たす最適なテクノロジーが API である ことは業界全体の共通認識となっています。

Akamai API Gateway ソリューションは以下に示す 3 種類の API に対応しています。

- 金融機関内のプライベート API
- 金融機関と外部 TPP の間のパートナー API
- 信頼されているすべての TPP が使用できるオープン API

規制技術基準(RTS)

強力な顧客認証および共通の安全なコ ミュニケーションに関する詳細な基準

強力な顧客認証(SCA)

多要素認証の使用によって電子決済のセキュリティ強化を求める PSD2 要件

ASPSP として機能する金融機関は、地理的所在地、可用性、アプリケーションに依存しない単一もしくは複数の API エンドポイントを、TPP 用に提供します。各 API は、すべての API コールで OAuth アクセストークンが提供されることを求めます。ASPSP は、同意請求など、TPP との限定的なやりとりのためにアクセストークンを発行します。

多くの API はその部門のニーズに応じて個別に開発されているため、類似の API が全社的に同じレベルであるとは限りません。API Gateway の管理機能を利用すれば、認証、レート制限、ロギング、キャッシングなど、すべての API に関連する要件を統一することができます。

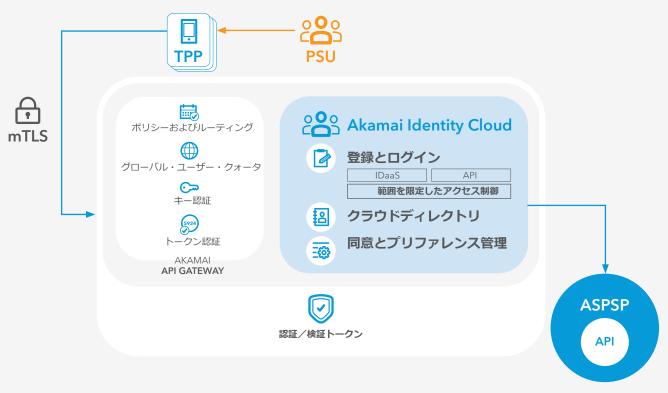


図 3: API Gateway によるトークン検証の管理

API Gateway ソリューションを使用することで、トークンの検証と検査、および OAuth 2.0 アクセストークン行使のタスクをオフロードできるとともに、Akamai Intelligent Edge Platform を通過する API トランザクションのセキュリティを確保できます。API リクエストのボリュームが増大し、リクエストごとに PSD2 に基づく認証が必要になると、トークン検証のスロットリングが予測不能になる可能性があります。この状況では、クラウドまたはオンプレミスのインフラストラクチャにかかるコストを管理することは 困難です。エッジでアクセスをコントロールすれば、API ファースト戦略を維持できます。

相互 TLS

PSD2 およびオープンバンキングに基づくサードパーティの識別には、Electronic Identification, Authentication, and Trust Services (eIDAS) を使用する必要があります。eIDAS は企業が確実に自身のアイデンティティを提示できるようにするために EU が定めた手法です。eIDAS の証明書を TPP が ASPSP に提示する際には、TLS プロトコルが使用されます。ASPSP は、以下のようないくつかのチェックを行う必要があります。

- eIDAS 証明書プロバイダーで eIDAS 証明書のステータスを確認
- 適切な国の機関で elDAS 証明書プロバイダーのステータスを確認
- 適切な国の機関で当該企業の PSD2 認可レベル

Akamai エッジサービスには、相互 TLS(mTLS)ターミネーションと検証を管理する機能があるので、ia="1551938483 金融機関は、こうした複雑なシステムの実装、運用、維持という課題から解放されます。」 contentType="audio" segr

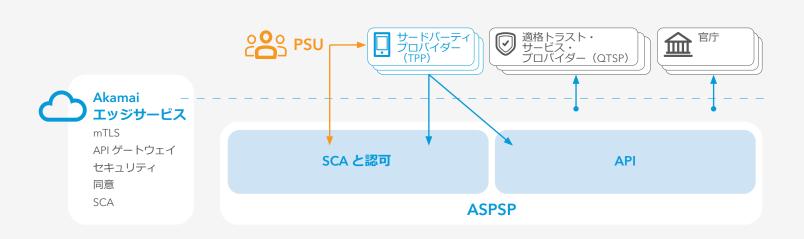


図 4: Akamai が mTLS ターミネーションと検証をオフロード

PSD2 成熟度モデル

規制は複雑で変わりやすいうえに、コンプライアンスを達成し価値を高めるアプローチには異なるさまざまなテクノロジーやプラットフォームが関わっています。PSD2 戦略を成功させるためには、時の経過に伴う変化に対応できるような柔軟性が必要です。以下に 5 段階の PSD2 成熟度モデルを示します。組織にとっての利点や、次の段階への移行方法は段階ごとに異なります。

1. 導入前

PSD2 の導入を開始しようとしている組織は、一般的に言って、調査段階にあるか、または小売コマースなど、PSD2 の影響を受ける隣接業界の組織です。この段階の組織の多くは、「様子見」をしています。もう少し業界のベストプラクティスや標準、規制当局からのサポートを見極めてから PSD2 の要件を満たそうと考えています。

2. 暫定的 (アドホック)

この段階の組織は一定のコンプライアンスレベルにあり、一般的に、数多くのシステムやプロセスが既存ソリューション(多くの場合、独自仕様のソリューション)の周りに構築されています。コントロールされた既知のアイデンティティがサイロ状に存在し、これらのサイロとシステム(SCA への複数のアプローチなど)との間はほとんどまたは全く統合されていません。この段階の組織は通常、PSD2 に準拠しているか、または部分的に準拠しています。

図 5:5 段階の PSD2 成熟度

3. 定義済みで反復可能

この段階では、システムとの統合を深化させる基盤を構築することで、ビジネス価値を高めることに重 点がおかれます。これには、堅牢なカスタマーアイデンティティ管理プラットフォームや、内部および 外部ソースから顧客データを収集できる API、ポリシーベースの SCA の整備が含まれます。

複数の IT 環境を横断して自社開発の異種システムを置き換えるには、統合プラットフォームからどのよ うに価値を創造するかについて明確な戦略が必要となります。この段階のコンプライアンスには、マル チベンダーアプローチが含まれ、自社開発システムを置き換えるか、補強します。ソリューションには 統合用の高度なカスタム実装が含まれます。この段階の組織は通常、PSD2 に準拠していますが、運用の オーバーヘッドが高い状態です。

4. 管理され測定可能

この段階では、より良い顧客体験の構築が重視され、統一的なカスタマー・アイデンティティ・プラット フォームが整備されます。ビジネスリーダーがコンプライアンスのユースケースを超えるソリュー ションを模索するようになると、次の段階への移行が始まります。顧客を中心にした投資が行われるよ うになり、業績が重視され、コンテキストやリスクに基づいてカスタマージャーニーが変更されます。

5. 最適化後

この段階で重視されるのは、組織と顧客の両者にとって戦略的価値を高めることです。通常、この段階 の組織は、最適化を目指してポイントソリューションから脱し、ベストプラクティスソリューションを 提供できるベンダーとの統合によって、カスタマーアイデンティティ、mTLS、API セキュリティがもた らす複雑さと運用コストを軽減します。

目標の達成 最適化後

統合済み、運用パフォ

-マンスの向上

結論

PSD2 コンプライアンスについて検討する際には、エンタープライズが次に示す 5 つのビジネス目標を18000"> <Audi 達成できるようなアプローチを探すことが重要です。

- 1. 規制要件に対応できる
- 2. 可能な最高の顧客体験を提供できる
- 3. 競争優位性を確立できる

tion:2011" vaPSD2 コンプライアンスのオフロードとシンプル化

- 4. 必要なセキュリティ制御を確保できる
- 5. 運用可能かつコスト効果の高い技術ソリューションを提供できる

Akamai のテクノロジーとサービスをご利用いただけば、PSD2 およびオープンバンキング標準の実装を合理化し、持続的なコンプライアンス、顧客体験の改善、運用の複雑さの軽減、コストの削減が可能となります。Akamai は、欧州の大手銀行上位 10 行すべてをはじめ、世界最大規模の企業各社に安全で快適なデジタル体験を提供しています。Akamai Intelligent Edge Platform は、エンタープライズからクラウドまで全てを網羅し、お客様とそのビジネスを高速、スマート、セキュアなものにします。

Raidiam は、PSD2 対応ソリューションの提供を促進し、カスタマーソリューションの成熟度を大きく進化させています。同社は、一般的な Web ソリューションや API ソリューションのアジャイルデリバリーにも対応し、これらのサービスへのアクセスに関連した課題に対処しています。 Raidiam はマネージド・プロキシ・サービスを提供することで、PSD2 相互 TLS の終端と証明書検証に対処するとともに、B2B および B2C ソリューション向けのマネージドアプリケーションおよびインフラストラクチャサービスを提供しています。

PSD2 オープンバンキングを、ユーザージャー二ー再定義や IT 環境統合の好機と捉えて対応していく 金融機関は、この新たな指令がもたらす利点を最大限に活かすことができます。詳細については、akamai.com/psd2 をご覧ください。

schema:MPD:2011 http://standards.iso.org/ittf/Publicly
2011 type="dynamic" minimumUpdatePeriod="PT500S" su
2011 timeShiftBufferDepth="PT18.0S" minBufferTime="

追加情報

- Akamai ホワイトペーパー: PSD2 遵守とリスク緩和のためのセキュリティソリューション Rate= "48000"> <Audi
- 決済サービス指令 2017
- オープンバンキングにおける顧客体験ガイドライン

著者:

Mark Haine, Founding Partner, Raidiam Services Ltd (raidiam.com)

Mayur Upadhyaya, Senior Director, Identity Cloud, Akamai (akamai.com)



Raidiam は、顧客と IoT のアイデンティティに重点をおいたデジタル変革サービスを提供しているアイデンティティ専門企業です。Raidiam の創業メンバーは、英国のオープンバンキングに対応した初めてのプラットフォームを考え出したアーキテクトであり、OpenID Foundation Financial Grade API(FAPI)標準の開発においても重要な役割を果たしました。そのため、同社は PSD2 に関連した法的な障害、組織における課題、技術オプションについて深い知識と経験を有しています。Radiam は最適化されたサービスを提供することで、eIDAS デジタル証明書の検証など、PSD2 に関する顧客の規制課題に対応しています。



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、ウェブ/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 でご紹介しています。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: 2019 年 12 月。