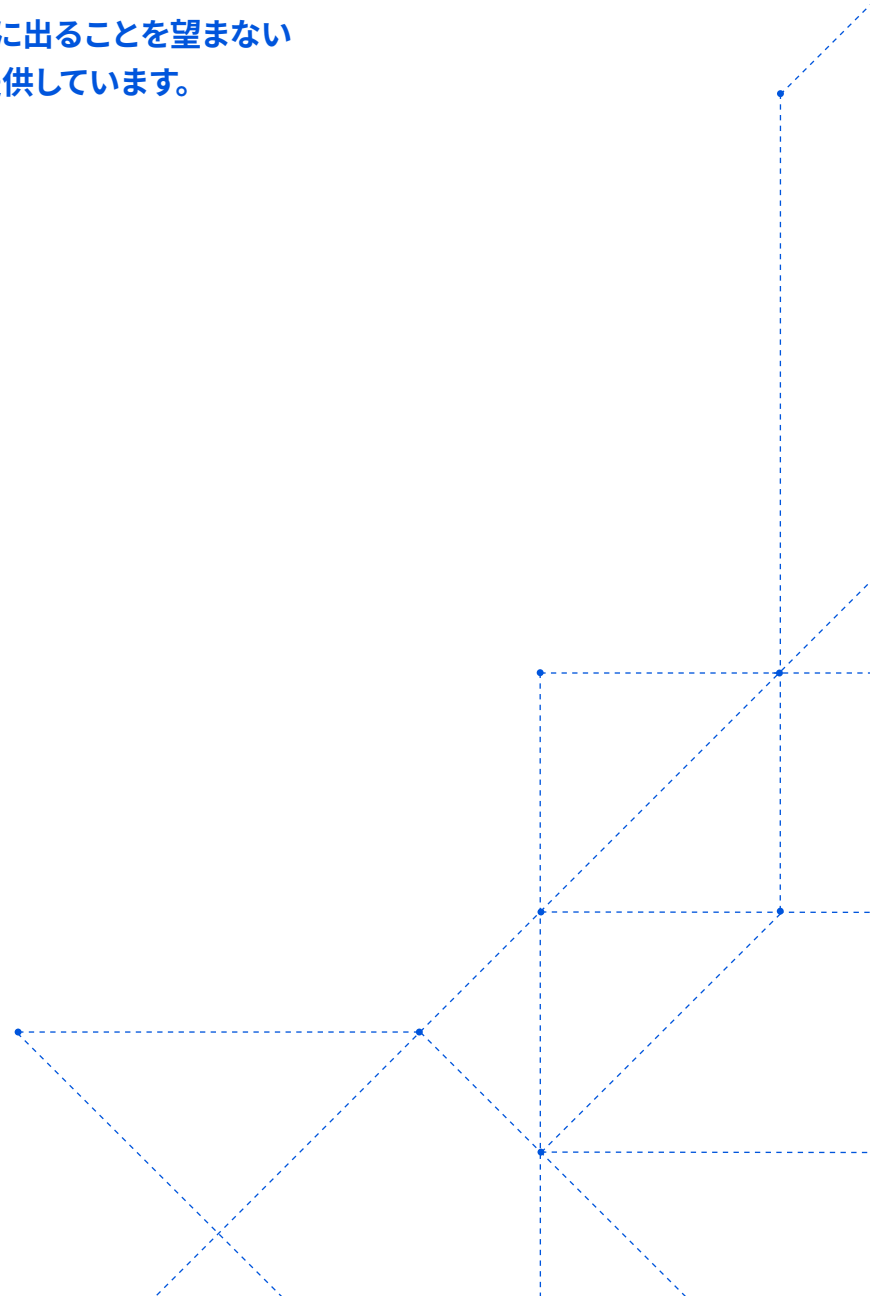
CLOUDFLARE

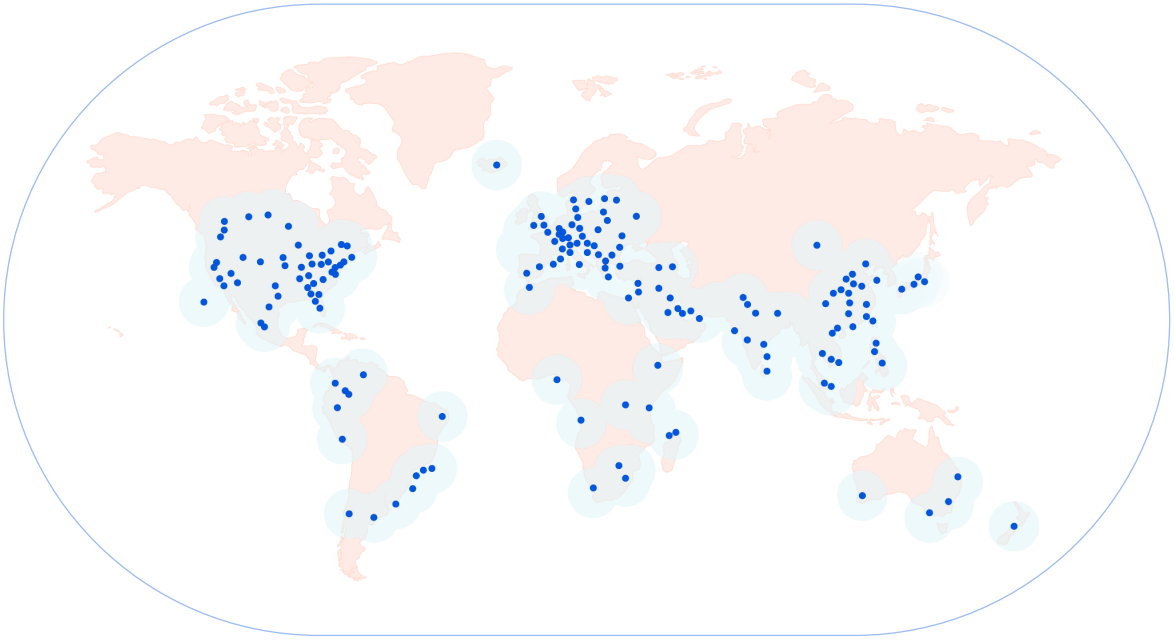
ホワイトペーパー

Cloudflareが、日本におけるデータの保護基準と責務にどのように対応しているか？

概要

- **Cloudflareは、お客様とそのエンドユーザーがインターネット上でより安全であるために構築されています。当社はプライバシー優先の企業であり、当社のネットワークと製品はすべてデータ保護を念頭に構築されています。**
- **Cloudflareは、日本の個人情報保護法（「APPI」）の要件に適合したさまざまな法的・契約的保護措置を講じています。**
- **Cloudflareは、自身のデータが日本国外に出ることを望まないお客様向けの製品機能や技術的保護を提供しています。**





Cloudflareのユニークなグローバルクラウドネットワークは、100か国以上、275都市以上に置かれたデータセンターで構成されています。Cloudflareは、お客様のデータがそれらのデータセンター間をどうルーティングされるかを管理するツールを提供し、安全性、プライバシー、パフォーマンスのニーズに応じた方法でトラフィックを検査する場所をお客様がカスタマイズできるようにしています。

Cloudflareについて

Cloudflareは、より良いインターネットの構築に貢献するというミッションを掲げています。当社は、世界中の個人やあらゆる規模の企業に広範なネットワークサービスを配信するグローバルクラウドプラットフォームを提供しています。Cloudflareのネットワークと拡張する製品ポートフォリオは、インターネットに接続するものすべての安全性、プライバシー、パフォーマンス、信頼性を高めます。お客様へのサービスはもちろん、インターネット自体の改善にも貢献し、常時オン状態で常に高速、安全、プライベートで誰にでも利用できるインターネットにすることもCloudflareの使命です。

Cloudflareのネットワーク、開発者コミュニティ、ビジネスはすべて、究極的にはお客様の信頼を基盤として築かれています。当社は、データプライバシー保護へのコミットメントと当社システムでお客様とエンドユーザーのデータを管理する方法を明確にすることにより、引き続きお客様の信頼を獲得し、維持していきたいと考えています。また、以下の条件を満たす製品を構築してデプロイすることによっても信頼を築きます。(i) 当社システムのセキュリティ向上に役立つ、(ii) 保存中ないし伝送中のデータを暗号化する、(iii) 世界のさまざまな場所におけるトラフィック検査の方法をお客様が決められる。そして、業界指定の認証（ISO 27001と27701、SSAE 18、SOC 2タイプ2など）を取得して維持し、プライバシーを確実に保護するために責任分担についてお客様に伝える契約メカニズム（データ処理契約など）を提供することによって、お客様の信頼を獲得します。

日本におけるCloudflare

現在、数百万に及ぶグローバルインターネットプロパティがCloudflareを利用しています。日本でも、インターネットイニシアチブジャパン、早稲田大学、IDOM、オズ・インターナショナル、信託銀行など、さまざまな分野で多くの組織にご利用いただいています。あらゆる規模の企業や団体が顧客やユーザー、ステークホルダーへのサービス提供に不可欠なプラットフォームとしてインターネットにますます依存する中、インターネット向けのアプリケーション、インフラストラクチャ、人員をあらゆる種類の脅威から保護するために、Cloudflareのような安全で信頼性の高いクラウドネットワークの導入が急速に進んでいます。

日本でのデータ保護に独特の難しさがあることを、当社は承知しています。日本には個人情報保護法（「APPI」）という形の包括的なプライバシー保護規制があります。

Cloudflareのインターネットプラットフォームは、日本でも最もプライバシー意識が高く規制の厳しい業界（金融サービス、電気通信、IT/デジタル、ヘルスケアなど）をサポートするために構築されています。Cloudflareは、セキュリティとユーザープライバシーの最高水準に適った製品を構築し、日本の個々のお客様と緊密に連携しながら、立地や産業部門ごとのデータ保護義務を遵守できるよう支援しています。そのために、当社はさまざまな手段をとっています。

- プライバシー保護に対する包括的コミットメント
- セキュリティとプライバシー保護に関する国際的認証の維持
- APPIを遵守したデータ移転メカニズムの整備
- データローカライゼーションをサポートする製品機能の提供

このホワイトペーパーでは、上記の手段について詳しく説明します。

プライバシー保護に対する当社独自のコミットメント

Cloudflareは、お客様とその顧客がインターネットをより安全に利用できるよう支援するために設立されました。当社はプライバシー優先の企業で、当社のネットワークと製品はすべて、データ保護を念頭に構築されています。当社はプライバシーポリシーの中で、当社がお客様に代わって処理する個人データを販売せず、お客様へのサービス提供以外の目的で使用しないことを約束しています。創業以来、この約束を破ったことは一度もありません。実際、プライバシーに対する当社のスタンスは、政府がプライバシー規制を始め、他の多くのテクノロジー企業が顧客とユーザーのプライバシー保護を然るべく優先するために慣行を変更せざるを得なくなるずっと前に確立されていました。当社は広告から収益を得ず、いかなる目的でもお客様のエンドユーザーやエンドユーザーデータのプロファイリングは行いません。このように、お客様の代わりに当社で処理する個人データの収集と保持には、本来反対の立場をとっているのです。

以下に、他の多くのクラウドサービスプロバイダーとは違う当社のプライバシー保護のコミットメントをいくつか紹介します。

- Cloudflareは、個人データを販売しません。
- Cloudflareは、お客様のエンドユーザーのインターネットプロパティ間の移動を追跡しません。

- Cloudflareは、広告販売目的でお客様のエンドユーザーのプロファイリングを行いません。
- Cloudflareは、お客様にサービスを提供する上で必要な限りにおいてのみ個人データを保持します。
- Cloudflareは、お客様の暗号化キーや当社ネットワークを通過するお客様のコンテンツのフィードを、いかなる第三者や政府にも提供しません。当社には、そうした請求に応じる前にあらゆる法的救済手段を消尽するという長年来のコミットメントがあります。
- Cloudflareは、米国のいかなる政府からのデータ請求であっても、データ保護法の対象であり法の抵触を起こすと当社が判断したものについては、法的救済を申し立てることを公約しています。
- Cloudflareでは、お客様の情報を請求する法的手続きがとられた場合は、法律で禁止されていない限り、情報開示前にお客様に通知することをポリシーとしています。

Cloudflareの国際的セキュリティ認証

Cloudflareは、セキュリティとプライバシー保護の業界最高水準を満たし、そのコミットメントを第三者監査人により、毎年検証しています。

Cloudflareは、個人データの保護とその処理の管理に関するプライバシー保護の新国際規格（ISO/IEC 27701:2019）の認証を取得しています。この規格は2年弱前に定められたもので、情報セキュリティ管理システムの既存概念を基にプライバシー情報管理システム（PIMS）を構築しています。このプライバシー情報管理システムは堅牢でなくてはならず、しかも、定められた目的に適うよう継続的な改善が必要です。この規格は、認証要件がEU一般データ保護規則（GDPR）の要件にうまく整合するように定められています。

簡単に言うと、ISO 27701認証は、世界で最も包括的なデータ保護制度の一つに整合した国際的業界標準に準ずると第三者が評価したプライバシープログラムを当社が整備していることをお客様に保証するものであり、当社はそのプライバシープログラムが常にコンプライアンスを維持するようにしなければなりません。この認証と、お客様がダッシュボードで確認できるようにしているデータ処理補遺条項（DPA）とで、Cloudflareが処理する個人データはすべてAPPIの定めを含めた包括的なデータ保護要件を充足する形で取り扱われるということを、お客様に重ねて保証しているのです。

さらに、CloudflareはISO 27001/27002、ペイメントカード業界データセキュリティ基準（PCI DSS）、SSAE 18 SOC 2タイプ2に適合しています。これらの適合確認は、最も機密性の高いデータを当社のサービスを通して移転する組織に安心感を与え、各々のコンプライアンス義務の継続遵守にも役立っています。

当社はデータ保護を大事にしており、法律で監査を義務づけられたり認証対象になっているものの監査を行うだけに止まりません。当社のセキュリティチームは、内部と外部の厳格なペネトレーションテストを実施していますし、当社はHackerOneを通じてバグバウンティプログラムも運営しています。さらに、当社のプライバシー保護へのコミットメントを確認するための常任独立監査人もいます。そうしたコミットメント確認の一例が、当社の1.1.1.1パブリックDNSリゾルバに関するコミットメントについて実施した、プライバシーに重点を置いた監査です。当社は、プライバシープログラムやポリシー、個人データの処理と保存のしかたに関するさらなる保証として他の認証を取得することに、常に前向きです。

Cloudflareが処理するデータ

Cloudflareは、お客様のエンドユーザーがお客様の許可に従って当社サービスにアクセスした際のログデータを処理します。このログデータには、IPアドレス、システム設定情報、お客様のWebサイト、デバイス、アプリケーション、ネットワークを行き来するトラフィックに関する他の情報が含まれますが、これらに限定はされません。Cloudflareはさらに、当社製品の運用上、サーバーとネットワークのアクティビティデータとログを収集して保存し、トラフィックデータの観察と分析を行います。当社が収集する情報と、収集した情報の用途については、プライバシーポリシーで詳説しています。

当社ネットワーク上のアクティビティからデータを収集して保存するのは、あくまでお客様とインターネットコミュニティ全体にとってより良い製品を作るためです。お客様が思いもかけない方法でこのデータを現金化するようなことはありません。たとえば、世界中のお客様から集めたネットワークトラフィックデータを一時保存して分析し、最も効率的なインターネットパスでリクエストをインテリジェントにルーティングするのに役立てたり、ネットワークデータを保存・分析して新たな脅威ベクトルを検出・識別し、それをセキュリティツールの改善に即時活用したりします。さらに、かなり大規模な顧客セグメントから集めたネットワークデータを集計し（特定可能な個々のユーザーやお客様からは決して集めません）、インターネットコミュニティがインターネット上のトレンドや脅威を理解しやすいようにする場合もあります（Cloudflare Radar参照）。

Cloudflareのデータ移転メカニズム

Cloudflareがデータ処理者として個人データを日本国外へ移転する場合は、標準データ処理契約（DPA）に従って行います。DPAは、お客様のEnterpriseサービス契約やセルフサーブサブスクリプション契約に盛り込まれています。DPAは、APPIに基づく越境移転の許可と同等の基準です。当社のAPPI遵守のコミットメントとDPAについて、詳しい情報はこちらでご確認いただけます。

重要なのは、当社がDPA中で、日本などの他の裁判管轄に属すると当社が判断するデータの開示を米国のいずれかの政府から請求された場合は、法的救済を申し立てることと、お客様の情報を請求する法的手続きがとられた場合は、法律で禁止されていない限り、情報開示前に必ずお客様に通知することを公約していることです。当社が契約上のコミットメントとして加えた追加的安全策については、DPA第7条に記載しています。

データ保護に関する規則や指針は常に進化するため、当社は規制や法制の動向をしっかり監視しています。当社では、新たな指針の制定を常に見越して、お客様とパートナーがCloudflareのメリットを日本で享受し続けられるようにしています。

Cloudflareがいかなる個人データも移転していないことを確認する必要があるお客様に対しては、Data Localization Suiteと呼ばれる一連の技術的手段を提供しています。

データローカライゼーションをサポートするCloudflareの製品機能

Cloudflareは、お客様が個人データを日本に留められるようにすることを約束しています。当社は、お客様が自社のデータの検査・保存場所を制御できるようにするData Localization Suiteを提供しています。

当社のData Localization Suiteには、以下の要素が含まれています。

- Encryption Key Management（Geo Key Managerと Keyless SSL）
- Payload Inspection Boundary（Regional Services）

Encryption Key Management：

データプライバシーはインターネットセキュリティなしには守れず、インターネットセキュリティの大部分は効果的な暗号化によって提供されます。

ネットワークを通過するデータの暗号化には、暗号化キーか、暗号化されたメッセージの送信者と受信者の双方が知っている一連の数値が必要になります。SSL/TLSは暗号化通信を可能にする暗号化プロトコルで、一対のキー（公開鍵と秘密鍵）を用います。

Cloudflareのお客様は、自社の秘密鍵が日本に留まるようにするために、次の2機能の使用を選択できます。

Keyless SSLを使うと、Cloudflareで使う秘密鍵をお客様が保存し管理することができます。お客様は、ハードウェアセキュリティモジュール（「HSM」）、バーチャルサーバー、お客様の制御下の環境に格納されUnix/LinuxやWindowsを実行するハードウェアなど、さまざまなシステムをキーストアとして使用することができます。Keyless SSLはCloudflareの観点から見た場合のみキーレスになっています。つまり、Cloudflareがお客様の秘密鍵を見ることは決してありませんが、お客様は秘密鍵を持ち、それを使用するのです。一方、公開鍵は通常通りクライアントサイドで使われます。

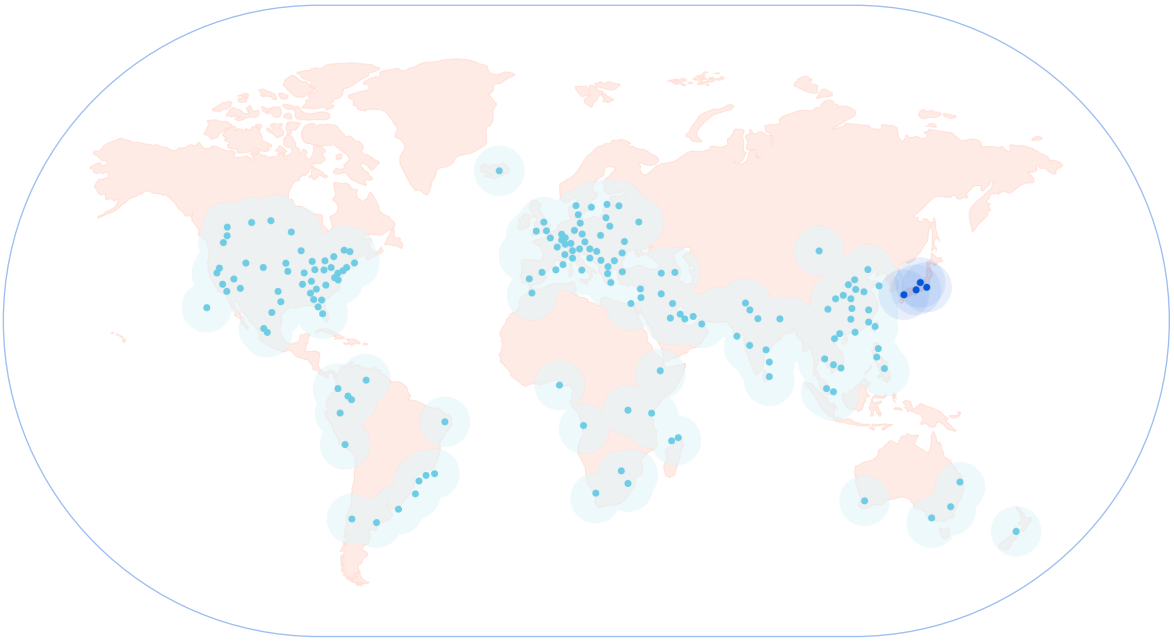
Geo Key Managerは、お客様がご自分の秘密鍵を保存するデータセンターをきめ細かく制御できるようにします。たとえば、日本国内のデータセンターでのみ秘密鍵にアクセスできるようにするなどです。このアプローチであれば、お客様はKeyless　SSLをデプロイしてキーストアを保守するという面倒から解放されます。

Payload Inspection Boundary：

Cloudflareは、お客様のトラフィックをすべて当社ネットワークのエッジからプロキシするため、最も安全で高パフォーマンスのnetwork-as-a-serviceサービスを提供できます。当社のサービスは、認証済みプロキシとしてお客様のトラフィックを確実に検査し、セキュリティ脅威を識別して、当社グローバルネットワーク上の任意のロケーションからルーティングします。Cloudflareは、特定の地域的要件に合わせた設定も可能な統合グローバルプラットフォームとして設計された数少ないクラウドプロバイダーの一つです。このアーキテクチャにより、Cloudflareのお客様はトラフィック検査の場所と方法を完全に制御することができるのです。

CloudflareのRegional Services（地域ごとのサービス）は、お客様がCloudflareネットワークのどこでTLS接続を終了するかを選べるようにします。たとえば、日本国内での終了を選択して、HTTPトラフィックのコンテンツの復号化と検査が日本国内でのみ行われるようにすることができます。この制限は、以下を含む当社のエッジ「アプリケーションサービス」すべてに適用されます。

- コンテンツの保存とキャッシュからの取得
- Webアプリケーションファイアウォール（WAF）による悪性HTTPペイロードのブロック
- Bot Managementによる不審アクティビティの検出とブロック
- Workersスクリプトの実行



想定するユースケースとしては、Cloudflareの日本のお客様がRegional Servicesを有効化しサービスを日本国内に限定することが考えられます。エンドユーザークライアントは世界中のどこでも最寄りのCloudflareロケーションに接続しますが、そのロケーションが日本国外の場合は、トラフィックは検査前にCloudflareの日本国内のロケーションに渡されます。お客様は、低遅延、高スループットで、最大級のDDoS攻撃でさえ撃退可能な当社グローバルネットワークのメリットはそのまま享受できます。

一方、お客様はRegional Servicesでローカルの制御もできます。日本のデータセンターだけが、セキュリティポリシーの適用に必要なアクセスを許されます。このアプローチによって、Cloudflareは日本への最速ルートと、処理に利用できる最寄りの接続点（POP）を選ぶことができるのです。

機会と責任の共有

日本の企業・団体がプライバシーとセキュリティの原則をビジネスの各側面に組み込む必要があることを、当社は承知しています。そこで、このチャートをご用意し、一般的なプライバシー保護要件の充足責任が誰にあるかを理解しやすくしました。

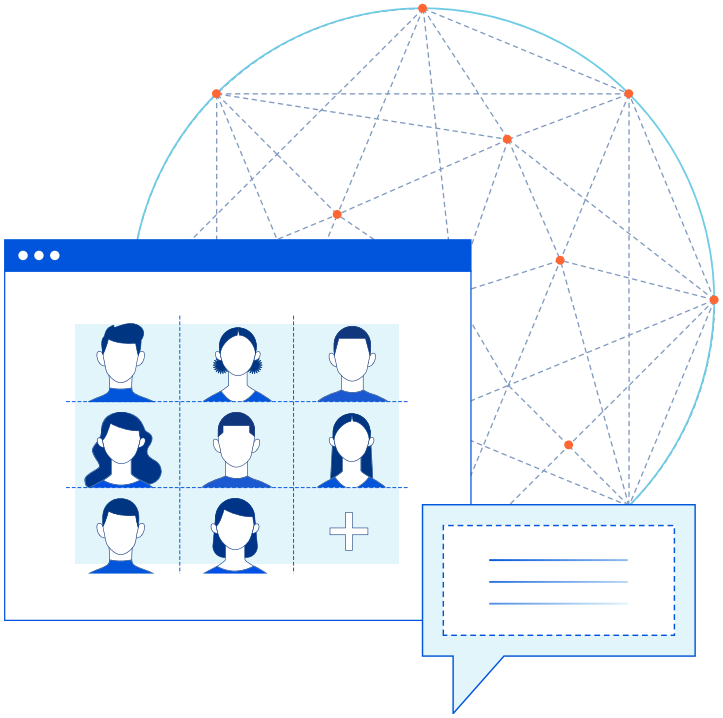
原則	責任	責任の詳細
設計によるデータ保護	共有	Cloudflareが、プライバシー保護を念頭に置いて構築された製品やサービスの提供に責任を持ちます。当社の仕事のしかたにプライバシー意識を確実に植え付けるため、プライバシーチームがレビュー、評価、訓練を行います。 お客様は、ご利用のCloudflareサービスの利用と設定に責任を持ち、利用状況と設定のレビューを定期的に実施して、設計と実装でデータ保護の原則が考慮されていることを確認します。
データ主体によるアクセス請求	共有	Cloudflareは、居住地の裁判管轄にかかわらず、データ主体に個人データのアクセス、修正、削除の権利を与えています。データ主体の要求は、sar@cloudflare.com へ送信することができます。当社がお客様のエンドユーザーらしき人からの要求を受け取った場合は、お客様に直接連絡するようご案内します。
十分なセキュリティ	共有	Cloudflareは、業界標準に従ってセキュリティプログラムを整備します。セキュリティプログラムには、正式なセキュリティポリシーと手続きの整備、適切な論理的アクセス制御と物理的アクセス制御の確立、企業環境と実稼働環境における安全な設定、伝送と接続、ログ記録、監視の確立を含めた技術的安全策の確立、個人データの保護に適した暗号化技術の使用が含まれます。 お客様は、お使いのクラウドプロバイダー（Cloudflareなど）のセキュリティポスチャのレビューを行う責任を負います。これは、当社のコンプライアンス認証とレポートのレビューによって行えます。当社では、お客様がダッシュボードのセキュリティ設定も見直して、自社のセキュリティポリシーと手続きの順守を確認するよう奨励しています。
個人データの漏えい	共有	Cloudflareは、Cloudflareまたはその副処理者が処理する個人データの損失、無許可の開示またはアクセスにつながるセキュリティ侵害に気が付き次第、お客様に通知します。Cloudflareは、漏えいの状況と影響を受ける個人データに関してCloudflareが持つ妥当な情報の提供など、漏えいに見合った妥当な協力と助力をお客様に提供する責任も負っています。 お客様には、個人データ漏えいについてエンドユーザーや政府当局へ通知する規制上または契約上の義務を果たす責任があります。

お客様の信頼を基盤として構築されたグローバルクラウドネットワーク

Cloudflareの第一優先事項は、お客様の信頼を得、それを維持することです。Cloudflareのプライバシー保護へのコミットメントと、当社のネットワークと製品にデータの局所性とプライバシーの安全策を組み込む方法についての透明性確保が、お客様がご自分の義務を果たす上で役に立つことを承知しています。当社は、Cloudflareの業界認証と精巧な契約メカニズムが日本のお客様との強力な信頼関係構築に役立つことも、理解しています。

Cloudflareのプライバシー・セキュリティチームは、お客様がご自身の国や地域、業界で課される極めて厳格な要件を満たすために協力を惜しみません。豊富な知識を持つ当社のアカウントエグゼクティブ、Customer Successマネージャー、セールスエンジニアは、プライバシーとセキュリティのコンプライアンスを扱うチームと常に連携し、お客様が固有のコンプライアンス義務を果たせるようにお使いのCloudflare製品を設定できるよう支援しています。

お使いのサービスをお客様固有の義務を果たせるように設定する方法について、デモまたは専門セッションをご希望の方は、今すぐprivacyquestions@cloudflare.comまたはsecurity@cloudflare.comへメールでご連絡ください。



03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3761.2022SEP14