

データプライバシーと法執行機 関の要求に関するCloudflare のポリシー

2021年1月28日公開

Cloudflareのネットワークとビジネスは、お客様の皆さまの信用をもとになりたっています。その信頼を維持するために、Cloudflareは自社のシステムセキュリティの向上、データの暗号化、そして世界中のトラフィックの検査方法の設定が可能なきざまな製品を作っています。

しかし、すべての課題がエンジニアリングで解決できるわけではありません。そのため、当社ではシステム上の顧客およびエンドユーザーのデータの管理方法、および行政機関・司法機関から要請への対応に関するポリシーと手順も定められています。

このホワイトペーパーでは、これらのポリシーについて説明し、データプライバシーとコンプライアンスに対する当社のアプローチのさまざまな側面について、より詳細な情報へのリンクを掲載しています。具体的には、次のことを網羅しています。

- 変化するデータプライバシーの情勢に関する当社の視点
- データプライバシーとデータ要求に関する当社のポリシー

変化するデータプライバシーの情勢

クラウドサービスの急増、およびデータを生成したユーザーの居住国以外に保存される可能性があるという事実は、法執行機関の調査を行う行政機関にとって課題となっています。あらゆる種類のオンラインサービスプロバイダは、多くの場合、それらの電子記録のアクセスポイントとして機能します。

Cloudflareのようなサービスプロバイダーに対する、行政機関のデータ要求が非常に多くなることもあります。法執行機関や他の行政機関が行う業務は重要だと認識しています。ただし、当社に求められるデータは、当社が所有するものではありません。当社のサービスを利用するのお客様は、当社を信用してデータを預けていただいています。その信頼を維持することは、当社のビジネスと価値観に必要な不可欠です。

各国の行政機関では、個人データの保護基準が異なるので、さらに対応が難しくなります。たとえば、米国では法的に定義された特定の状況を除き、企業が通信の内容を米国以外の行政機関に対して開示することを禁じています。プライバシーが基本的人権であると以前から認識している欧州連合は、EU一般データ保護規則 (GDPR) を通じて全EU加盟国の個人データを保護しています。これらの保護対策には似ている部分はありますが、範囲と守る対象が異なります。

法的枠組みの違いは、特に、外国の行政機関による情報の法的要求がプライバシー要件に準拠しているかどうかを判断する際に重要です。例えば、近年、欧州連合司法裁判所 (CJEU) は、プライバシーシールド (またはその前身であるUS-EUセーフハーバー) のような一定の自発的なコミットメントとともに、データ収集に関する米国の法的制限がEUのプライバシー要件に準拠するのに十分ではないと何度も結論付けています。これは、法的当局が外国の諜報目的で米国以外の市民に関する情報を収集することを許してしまう米国の法律があるからです。実際、欧州データ保護委員会 (EDPB) は、米国の刑法によりデータを要求する立場をとっています。これは、EU内の国々が収集される情報がある程度コントロールできる法的手続きの場合を除き、GDPRの対象となる個人データの転送を原則的に拒否するというスタンスです。

これはすなわち、どちらかの国の行政機関が法的命令やその他の法的プロセスを介して、他国民に関するデータにアクセスすることが適切かどうかの攻防です。そして、これらはヨーロッパに限った話ではありません。政策対応は違うけれど、現在、国民のデータへのアクセスを国家安全保障上の懸念として重視する国が増えてきている。

Cloudflareのデータプライバシーとデータ要求に関するポリシー

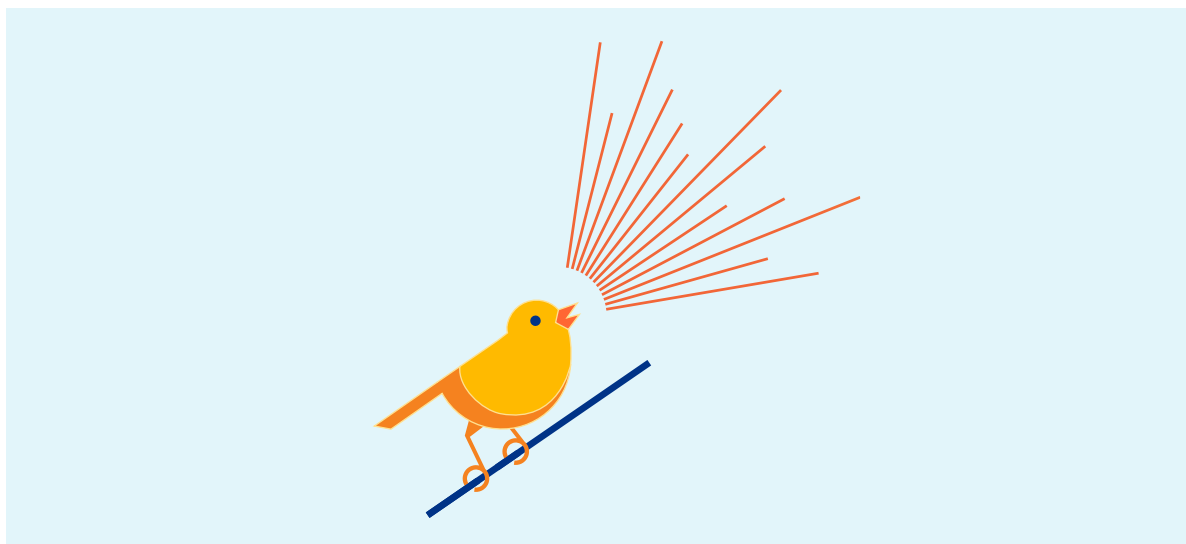
Cloudflareは、個人データへのアクセスに関する懸念に対処するためのポリシーを長く維持してきました。私たちはそれが正しいことだと信じているため、そしてこうした法律の矛盾は避けられないと思えたからです。これらのポリシーには以下が含まれます。

- プライベートデータの取り扱い方法とそのデータに対する法執行機関の要請の処理方法に関する公約について
- データ要求があった際に、お客様に通知する方法。

一般的に、2つの異なる法的基準の間に矛盾がある場合、当社はプライバシー保護が最も高い基準に合わせてるようにしています。そして、データの開示には必ず法的手続きを必要とします。一度データアクセスの例外を許してしまうと、今後のアクセスを拒否しにくくなるからです。

プライベートデータと法執行機関の要請に関する公約について

2013年の法執行機関によるデータ要求の詳細を記載した最初の透明性レポートから、データ要求へのアプローチ方法と、これまで行っていないことに関する公的な声明について公約しました。当社は、これまで行っていないことの公的な声明を「カナリア」と呼んでいます。この状況をCloudflareの外にも知らせるためです。



そうした「カナリア」は2つの機能を果たします。第一に、これらはCloudflareが自らの意思で行わないという公的な声明です。第二に、これらの情報がサイトの声明から削除されることにより、(本来なら開示が制限される可能性のある)情報の伝達メカニズムともなり得ます。

規制機関は、特に契約によって執行できる場合に、プライバシーのコミットメントの価値を認識し始めています。実際、当社が長年にわたって透明性レポートに含めてきたコミットメントは、まさに欧州委員会がGDPRに準拠するための標準契約条項草案に含めることを推奨しているコミットメントと同じようなものです。

本ホワイトペーパーの発行日現在の、当社のコミットメントの主な例は次のとおりです。

- **法執行機関のソフトウェアや機器を当社のネットワークにインストールしたことはありません。**
当社のネットワークを通過するコンテンツのフィードを提供したことはありません。セキュリティ企業として、ネットワークへのアクセスを制御することは絶対的な必須事項であることを認識しています。そのため、セキュリティチームはアクセス制御、ロギング、監視に重点を置き、年間に複数のサードパーティによる監査を受けています。当社は、法執行機関または政府機関の規制に「異例」がないことをお客様に理解していただきたいと考えています。そのため、Cloudflareは当社のネットワーク上に法執行機関ソフトウェアや機器をインストールしたことがないこと、および当社の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政府機関に提供したことがないことを述べています。
- **当社は、認証キーまたは暗号化キーを共有したことはありません。** Cloudflareは、コンテンツとメタデータの両方の強固な暗号化がオンラインプライバシーのために必要であると信じています。どの国であっても、他の国の政府から自国民の個人情報へのアクセスを防ぎたい場合に、最初にやるべきことは、その個人情報の暗号化でなければなりません。しかし、お客様や規制当局はまた、その暗号化自体が信頼できるものであることを確信する必要があります。そのため、当社は、暗号化キーまたは認証キー（またはお客様の暗号化キーまたは認証キー）を誰にも引き渡したことがなく、法執行機関またはその他の第三者の要請により、暗号化を弱体化、侵害、または無効化することは決してないことを約束しています。
- **お客様のコンテンツや DNS リクエストを変更したことはありません。** 当社は、訪問する意図のないサイトにユーザーを導いたり、オンラインで得るコンテンツを変更したりするために、当社のシステムを悪用すべきとは考えていません。そのため、法執行機関または他の第三者の要請により、お客様のコンテンツを変更したり、DNS レスポンスの意図された宛先を変更したりしたことはないことに公に述べています。
- **コミットメントが破られる可能性がある場合に関する透明性。** 当社は、これらのコミットメントを破るよう求める法的命令に（必要であれば法廷で）異議を唱えることを公約します。当社の目標は、お客様だけでなく、世界中の政府と当社の線引きを非常に明確にする事でした。

創業以来、データ保護に関する当社の全体的な理念は変わっていませんが、当社では、製品やポリシーの最新の変更を反映するために、当社のコミットメントを適宜調整しています。これらのコミットメントの最新のリストは、[透明性レポートのページ](#)でご覧いただけます。

行政機関からの要請があった際にお客様に通知する

Cloudflareは兼ねてより、お客様の情報が（法執行機関や他の政府機関を含む何者かによる）法的手続きで求められた場合に知らせられるべきだと信じています。その通知があることで、お客様は懸念がある場合にリクエストに異議を申し立てることができます。

実際、当社では創業期からお客様への通知を行う方針を定めています。2013年1月、従業員が30人未満だったとき、当社はFBIから国家安全保障書簡を受け取りました。その内容は、あるお客様に関する情報を要求するもので、当社にも弁護士以外の人との話し合いを禁じられると書いてました。当時、国家安全保障書簡にはほとんど監視がなく、米国政府の1つの支部によって作成および執行され、それを受け取ったものはそれらについて無期限に話すことを禁じられていました。

当社は、捜査の実行可能性を維持するために、法執行機関が一時的に開示を制限することが適切な場合があることを認識しています。ただし、政府は機密保持契約を正当化する必要があり、機密保持契約は現在の目的に必要な最小限の時間に明示的に制限する必要があると考えています。そのため、当社は電子フロンティア財団と協力して、この国家安全保障書簡に対する法的な異議申し立てを行いました。

結果として生じた訴訟は数年間続き、2017年までそれについて話すことはできませんでした。しかし最終的に、[FBIはその国家安全保障書簡を取り](#)下げる結果になりました。

米国の裁判所は、無期限の非開示命令は憲法上の問題を引き起こすと示唆しているため、[米国司法省](#)は2017年に（例外的な状況を除いて）非開示命令を1年以内に制限するよう、連邦検察官に指示するガイダンスを発行しました。しかし、それはすべての米国の法執行機関が無期限の非開示命令を求めることを阻止していません。このホワイトペーパーの発行日現在、2017年以降に受け取った機密保持契約に終了日が含まれていなかったものは少なくとも28件ありました。Cloudflareはアメリカ自由人権協会（ACLU）と協力して、このような無期限の機密保持契約を受け取るたびに訴訟を起こすと脅迫してきました。いずれの場合にも、行政機関はその後に法的要求の非開示要件に期限を設け、当社にはお客様に要求があったことを通知できるようにしていただけました。

法の抵触への対応

GDPRなどの法律の遵守を維持するには、特に法的な命令により、違反が義務付けられているという困難な立場に追い込まれる可能性がある場合、裁判所を関与させる必要があります。Cloudflareのようなサービスプロバイダーは、法の抵触を理由に裁判所に法的要求を破棄するよう求めることができます。そして当社は、公的な声明と当社のデータ処理補遺条項の両方において、そのような抵触を回避するために必要に応じてその措置を講じることを約束しています。こうした抵触は、情報へアクセスする権利を巡って争う両政府の間で決着をつけるべきだと当社は考えています。

まとめ

この記事は、データプライバシーに対する当社の幅広く深いコミットメントの紹介にすぎません。これらのコミットメントの詳細については、以下をご覧ください。

- [当社の全体的なプライバシーポリシー](#): 当社が収集するデータ、その使用方法、共有するデータ、そしてその他の一般的なプライバシーに関する質問が記載されています。
- [当社の透明性レポート](#): お客様に関する情報を開示するために頂いた法的要請に関する最新情報。
- [当社のデータプライバシー&コンプライアンスホームページ](#): 当社のポリシーと製品が、どのようにプライバシーとコンプライアンスのニーズを満たしているかに関する最新のお知らせ。

最終的に、顧客とエンドユーザーのデータを保護する（そして世界中のさまざまなプライバシー法に準拠する）グローバルネットワークを運営するには、企業としての創業期から提唱してきた価値観（「原則的かつ透明である」、「プライバシーを尊重する」、「適正手続きを必要とする」、そして「お客様が自らのデータに関する判断が行えるように、事前に知らせること」）に立ち返る必要があります。

© 2021 Cloudflare, Inc. All rights reserved. Cloudflareのロゴは、Cloudflareの商標です。その他の会社名および商品名はそれぞれ関連する各企業の商標です。