プライバシーとデータ保護

個人のデータは社会活動や経済活動において重要な役割を果たします。最近では、企業や組織は、ユーザーから入手した個人データに対する管理の厳格化、利用方法と保護方法の明確化がより求められるようになりました。

Dropbox は、信頼という基盤の上に、世界中にいる数億人ものユーザーや企業との関係を築いています。皆様にご利用いただいていることを誇りとし、個人データ保護の責任を第一に考えています。

皆様へのお約束

Dropbox はお客様の個人データの保護を第一に考えています。Dropbox のプライバシー ポリシーでは、Dropbox のプライバシーへの取り組みと、Dropbox のサービスをご利用になる際に個人データがどのように収集、使用、取り扱いされるかについて説明しています。Dropbox はまた、Dropbox のプライバシー慣行について理解しやすい形で情報共有することにも取り組んでおり、よくある質問に対応するためにプライバシー ポリシー：よくある質問および本ドキュメントを入手できるようにしています。

お客様が北米地域（米国、カナダおよびメキシコ）にお住まいの場合、Dropbox, Inc. がお客様のサービス プロバイダとして機能します。その他の地域にお住まいのお客様の場合、Dropbox International Unlimited Company がお客様の個人データの「管理者」となります。データ管理者は、個人データの処理の目的と手段を判断します。

お客様がチーム向け Dropbox プランのいずれかをお使いの場合（Dropbox Business または Dropbox Education など）、お客様の組織は、Dropbox の使用に関連して Dropbox に提供されたあらゆる個人データのデータ管理者として機能します。この場合、Dropbox はデータ処理者として機能し、お客様の組織の代わりに Business 契約書に従ってデータを処理します。Business 契約書にはデータ処理と国際データ転送に関連する Dropbox の責任が記載されています。

プランにかかわらず、Dropbox はお客様の個人データの取り扱いに関して同じ原則を適用しています。以下のセクションでは、Dropbox の企業原則を説明し、Dropbox がグローバルな認証基準をどのように満たし、プライバシー規制を遵守しているのかを紹介します。

政府データ要請原則

ユーザーが個人データを Dropbox に委ねるのは、Dropbox がそのデータの機密性を守ることを期待しているからであり、それを Dropbox は理解しています。大半のオンライン サービス会社と同様に、Dropbox は政府および法執行機関からユーザー情報開示の要請を受領することがあります。Dropbox は各要請を綿密に調査し、ユーザーのアカウントが特定されている場合は、法律で許可されている範囲でユーザーに通知するよう尽力しています。

Dropbox は透明性レポートを維持し、以下の一連の政府データ要請原則を確立しています。

透明性の維持

オンライン サービス会社には、政府より受けた要請の件数と種類を公開し、対象となっているユーザーに情報の要請を受けていると通知することが許可されるべきです。この種の透明性を高めることは、政府による行き過ぎた行為の事例やパターンに関するユーザーの理解を深めるための一助となります。Dropbox は継続的に、こういった提供要請に関する詳細な情報を公開し、これらの重要情報を提供する権利を主張していきます。

過度に広範な要請に応じない

政府機関によるデータ提供要請は、必要とする情報に限定され、特定のユーザーに的を絞り、合法な調査に基づいて行われるべきです。Dropbox は、包括的かつ過度に広範な要請には応じません。

信頼できるサービスを提供

政府はユーザー データを取得するためにオンライン サービスにバックドアを設置したり、インフラストラクチャを危険にさらしたりすべきではありません。Dropbox は、このような活動が違法であることを明確にするため、弊社システムの保護と法律改定に取り組み続けています。

すべてのユーザーの保護

居住地や市民権の存在する場所に応じて異なる方法で人々を保護する法律は、時代に沿わなくなっており、グローバルに展開されるオンライン サービスの可用性を阻害する可能性があります。

これらの原則と年次透明性レポートは、Dropbox ウェブサイトの Dropbox の透明性の概要でご覧いただけます。

人工知能の原則

Dropbox の一部の機能には人工知能（AI）が活用されています。Dropbox は、AI イノベーションがお客様の役に立つだけでなく、お客様の権利と安全も尊重するものとなるように取り組みます。

Dropbox チームは以下の原則を指針として、責任をもって AI を活用する製品と機能を開発します。

- AI を活用してお客様にサービスを提供する
- 常にお客様がデータを管理できるようにする
- AI の使用方法について透明性を保つ
- AI テクノロジーにおける公平性を擁護する
- お客様に対して説明責任を果たす
- 人々とその安全および権利を尊重する

これらの原則については、Dropbox ウェブサイトの Dropbox の AI 原則で詳しく説明しています。

Dropbox の管理：Dropbox の内部慣行

私たちは、インフラストラクチャ、ネットワーク、アプリケーションを保護するために包括的な対策を講じています。実施中のセキュリティ対策として、保存中のデータの暗号化、転送時の暗号化、アクセス制御などがあります。これらの対策については、Dropbox のセキュリティに関するホワイトペーパーで詳しく説明しています。

Dropbox の堅牢なセキュリティ制御は、一連のプライバシー制御によって補完されます。次のような例があります。

プライバシー トレーニング

プライバシーを重視する文化の構築と醸成は、Dropbox におけるユーザーの個人データを保護する対策の一部を占めています。そのため、Dropbox の社員は、ユーザー データ プライバシー ポリシーおよびデータ分類に関するポリシーに同意していなければ、システムへのアクセスを許可されません。そのようなシステムには、特定のニーズを持つ社員だけがアクセスできます。また、社員は年に一度、プライバシーに関する必須トレーニングを受講しています。こうした研修ではプライバシー法の基本を扱い、Dropbox における個人データの取り扱いについて、ベスト プラクティスを説明しています。

ファイルと Paper ドキュメントの完全削除

Dropbox ユーザーや、チーム向け Dropbox のアカウント管理者がファイルを完全削除の対象としてマークすると、そのファイルを完全に削除するプロセスが起動します。同様に、ユーザーや、チーム向け Dropbox のアカウント管理者が Paper ドキュメントを完全削除の対象としてマークすると、Paper ドキュメントのデータと画像データを完全に削除するプロセスが起動します。

匿名化と仮名化

データを個人に結びつける必要がなくなった場合は、匿名化や仮名化などの手法を使用して、データから個人を特定できないように処理します。匿名化は、個人データを完全に削除または変更して、個人の特定に使用できないようにするものです。仮名化は、個人データを一時的に削除または変更するものですが、追加情報へのアクセスを持っている人物に限り、このプロセスを元に戻すことができます。仮名化を使用する場合の例としては、Dropbox の製品やサービスの改善に使用するお客様からのフィードバックを処理して、個人を特定できないようにすることが挙げられます。

プライバシー ガバナンス

プライバシー チームは、Dropbox プライバシー プログラムの運用を担当しています。このチームは主要なプライバシーの取り組みを実施するとともに、データライフサイクルで「プライバシー バイ デザイン」の実現を後押ししています。Dropbox プライバシー プログラムには、法務やセキュリティの部門にまたがる、部門を超えた複数のサブチームが関与しています。こうしたチームは、プライバシー プログラムの日常的なタスクを実施し、監督するために必要となる補助的な専門知識を提供します。

データ保護責任者のオフィスは、他のプライバシーチームとは別個で業務を行い、プライバシー コンプライアンスおよび監督機能を推進しています。お問い合わせは privacy@dropbox.com へお願いいたします。

Dropbox の実績：コンプライアンス

コンプライアンスは、サービスの信頼性を確保するための有効な手段です。Dropbox では、セキュリティとプライバシーの対策が、**ISO 27001**、**ISO 27017**、**ISO 27018**、**ISO 27701**、**HIPAA/HITECH**、**SOC 1**、**SOC 2**、**SOC 3** など広く受け入れられている基準や規制に適合していることを独立機関を通じて積極的に検証し、その結果を提供しています。

また、Dropbox は大手クラウド サービス プロバイダとして、クラウドにおけるプライバシーとデータ保護の先進的な慣行に関する国際規格である ISO 27018 の認証基準をいち早く満たしました。独立した監査機関が Dropbox の管理機能をテストし、レポートと見解を提供しています。そのレポートと見解は、発表され次第、公開いたします。なお、Dropbox に関する認証と監査レポートは通常、チーム向け Dropbox を対象にしていますが、Dropbox の制御の大部分はすべての Dropbox プランに適用されます。

加えて、Dropbox は **EU クラウド行動規範**を遵守しています。EU クラウド行動規範は、Dropbox などのクラウド サービス プロバイダが GDPR コンプライアンスへの取り組みを実証できるようにする自発的手段です。チーム向け Dropbox は、EU クラウド行動規範の遵守を宣言しており、「レベル 2」のコンプライアンス マークを取得しています。これはつまり、サービスが EU クラウド行動規範の要件に沿って技術、組織、契約に関する対策を実施していることを意味しています。詳しくは、EU クラウド行動規範の公式ウェブサイトをご覧ください。

Dropbox が遵守している基準と、Dropbox の慣行を検証している方法の詳細ついては、Dropbox のトラスト センターおよびコンプライアンスに関するウェブ ページをご覧ください。

国際データ転送

Dropbox は、欧州連合、欧州経済地域、英国、およびスイスからデータを転送する場合、Dropbox のお客様や関連会社との契約、標準的契約条項、欧州委員会の十分性決定など、該当するさまざまな法的枠組みに依拠します。

Dropbox は、EU 加盟国、欧州経済地域、英国ならびにスイスから米国に転送される個人データの処理に関して、米国商務省により定められている EU/米国間およびスイス/米国間のデータ プライバシー フレームワークと、EU/米国間データ プライバシー フレームワークの英国拡張版を遵守しています。Dropbox は当該データに関してこれらのデータ プライバシー フレームワークを遵守する旨を米国商務省に対して保証していますが、FormSwift のサービスに関してはこれに含まれません。

データ プライバシー フレームワークと Dropbox の認証の詳細については、https://www.dataprivacyframework.gov/ をご覧ください。

Dropbox のデータ プライバシー フレームワークのコンプライアンスに関する苦情と申し立ては、独立した第三者機関である JAMS を通して調査と解決が行われます。詳細については、Dropbox のプライバシー ポリシーをご覧ください。

Dropbox のパートナー

Dropbox では、サービスの提供に関連する活動のほとんどを自社で管理していますが、一部のサービスについては信頼できるサード パーティ（カスタマー サポートや IT サービスのプロバイダなど）に業務を委託しています。これらのサード パーティがお客様の情報にアクセスするのは、Dropbox のプライバシー ポリシーを遵守して、Dropbox に代わってタスクを実行する場合に限定されます。また、Dropbox はこれらのサード パーティが Dropbox の指示に従ってお客様の情報を処理することについて、引き続き責任を持ちます。

各サード パーティは、セキュリティ レビューやプライバシー レビュー、契約上の審査といった厳格な事前審査プロセスを通して、Dropbox のデータ保護責任を果たす能力があると評価されています。Dropbox はこの事前審査プロセスに基づき、信頼できるサード パーティが Dropbox に代わって個人データを処理する際に、適用されるデータ保護法が確実に遵守されることを確認しています。お客様は、Dropbox が ISO 27001 認証および 27018 認証を受けていることを確認することで、Dropbox が信頼するサード パーティを監視することができます。またこれは、適切な守秘義務を遵守した上で、Dropbox の制御と監査の結果について SOC 2 タイプ II レポートの Trust サービス基準 P6.1、P6.4、CC.9.2 を調べることによっても可能です。

加えて Dropbox は、チーム向け Dropbox のお客様にサービスを提供できるようにするために、お客様の個人データへのアクセス権を持つ復処理者を起用することがあります。復処理者を起用する前に、Dropbox は復処理者のプライバシー、セキュリティ、機密性の慣行についてデュー デリジェンスを実施し、個人データの保護に関して適切な契約上の措置を講じます。Dropbox の復処理者リストで、復処理者のリストをご確認いただき、復処理者の変更をお申込みいただけます。

一般データ保護規則

一般データ保護規則（GDPR）は、EU 域内のデータ主体の個人データ保護に関する法的枠組みを定めた EU の規則です。GDPR は 1995 年以降の EU データ保護指令に代わる欧州データ保護法令の最も重要な部分で、Dropbox をはじめ欧州で事業を展開する企業が GDPR コンプライアンスに多大な投資をしています。

プライバシーとセキュリティの重視は Dropbox 設立時からの社是であり、企業成長の過程においても、ユーザーから委ねられたデータの取り扱いと保護に注力することは常に高い優先順位を保ってきました。Dropbox はコンプライアンス曲線を上回る実績があり、先述のとおり、ビジネス ユーザー向けに ISO 27018 認証をいち早く取得したクラウド サービス プロバイダでもあります。このような強固な基盤があったことから、GDPR のコンプライアンスは、Dropbox がすでに行っていた慣行と制御が自然に進化したものとなりました。

Dropbox の GDPR コンプライアンスへの取り組みは、2016 年に規則が採択された直後に始まりました。Dropbox の取り組みは、法律顧問、セキュリティとコンプライアンスの専門家、製品とインフラストラクチャのエンジニアで構成されるデータ保護の専門家チームを組織することから始まりました。その専門家チームにより、セキュリティおよびデータ保護慣行の GDPR 要件に対する評価をすべて完了しました。次のステップとしたのは、Dropbox が扱う個人データ処理活動の評価を行い、Dropbox のシステム全域での個人データのライフサイクルを追跡することでした。このような実地での検証を、データ マッピングの実行およびデータ保護影響評価の完全実施と呼ぶこともあります。

それ以来 Dropbox では、既存のプロセスをベースとして、GDPR 要件下での責任原則を確実に満たす内部プロセスと手順を構築し続けてきました。これには GDPR 第 30 条に従って処理の記録を維持することなどが含まれます。

GDPR の詳細については、Dropbox の GDPR ガイダンス センターをご覧ください。

データ主体の権利

GDPR は個人に対し、個人データにアクセスし、修正、削除し、処理に対して異議を申し立てる権利を与えます。こうした消費者の権利は、カリフォルニア州消費者プライバシー法（CCPA）をはじめとする多くの他のプライバシー法にも見られます。Dropbox がこうしたプライバシーの権利にどのように準拠しているのかを紹介します。

アクセスおよび修正する権利

ユーザーは https://www.dropbox.com にログインしてアカウント ページに進むことで、自分自身に関するデータにアクセスしたり、修正したりできます。[全般] タブには、アカウントに関連付けられている名前やメール アドレスなどの情報が表示されます。[セキュリティ] タブには、接続されたセッション、パソコン、モバイル デバイスの IP アドレスが表示されます。[アプリ] タブには、アカウントに接続されているアプリのリストが表示されます。

また、[プライバシー] タブも利用できるようになりました。ユーザーはこのタブでアクセス レポートを生成できます。アカウントにログインできない方やアカウントがない方は、こちらのデータ主体リクエスト フォームに記入してリクエストを送信できます。

削除する権利

アカウントのコンテンツの削除を希望するユーザーは、アカウント内から直接削除することができます。コンテンツの削除方法の詳細についてはこちらをご覧ください。

ユーザーは［プライバシー］タブでアカウントに関連しないデータ（マーケティング システムの連絡先情報など）を削除できます。アカウントにログインできない方やアカウントがない方は、こちらのデータ主体リクエストフォームに記入してリクエストを送信できます。

異議を申し立てる権利

処理の種類によっては、個人は Dropbox による個人データ処理の停止または制限をリクエストすることができます。個人データの処理に対する異議申し立てを希望される場合は、privacy@dropbox.com までメールでお知らせください。

個人は、アカウントの［通知］セクションで設定を変更するか、マーケティング メールのフッターにある配信停止リンクをクリックすることで、マーケティング資料の受信をいつでもオプトアウトできます。

また、Dropbox の Cookie バナーで設定を更新することで、Cookie を通じた個人データの収集をオプトアウトすることもできます。Dropbox による Cookie や類似テクノロジーの使用に関する詳細については、こちらのページをご覧ください。

ユーザー支援

Dropbox は、GDPR での遵守義務を含むデータ保護義務の管理がより簡単になる制御と可視化の機能を提供します。当然ながら、ユーザーの企業や組織全体での GDPR の遵守と、Dropbox などのサプライヤーとの関係の開始や終了とは無関係です。Dropbox の機能はユーザーの企業や組織が果たすべき義務の管理に役立ちますが、義務の遵守自体を保証するものではありません。GDPR を遵守するためには、組織内でのデータの移動と保護の状況について、より広範に検討する必要があります。GDPR コンプライアンスを達成するため、それぞれの企業や組織は重要なパートナーであるサプライヤーと協力して、独自の手順を確立し実行する必要があります。

データの最小化

企業や組織は利用するデータを最小限に抑えてサービスを設計する必要がある、という点が、プライバシー バイ デザインの要件に関する GDPR の重要な要素です。つまり、組織におけるデータの可視性の高さが、容易なデータ管理につながる、ということです。チーム向け Dropbox の管理者用ダッシュボードは、チームのアクティビティの監視、接続デバイスの表示、共有アクティビティの監査を可能にする便利なツールで、そういった高い可視性の実現に役立ちます。Dropbox は、新製品や新機能にプライバシー バイ デザインの原則を反映させるべく取り組んでいます。

データの保護と復元

紛失したデバイスの保護、バージョン履歴、およびファイルの復元は、個人データの偶発的な紛失、破損、破壊からの保護と、インシデントが発生した場合の速やかな可用性の回復、個人データへのアクセスを可能にするものです。データを保護するために推奨されるもう 1 つの重要な手段は、2 要素認証です。

記録の保存

また、GDPR により、処理アクティビティの詳細な記録を企業や組織が保持する義務も増加します。Dropbox の監査ログとアクティビティ ログは記録保持に役立ち、処理アクティビティがより理解しやすくなります。

アクセス管理

チーム向け Dropbox の管理者用ダッシュボードを利用することで、チーム メンバーのファイル、フォルダ、Paper ドキュメントへのアクセス管理が容易になります。共有ファイル リンクの場合、リンクの権限設定を利用すれば、共有リンクのパスワード保護、有効期限を設定した一時的なアクセス許可、組織内のユーザーに対するアクセス制限も行えます。ユーザー間で役職が変更された場合は、アカウント移行ツールを使用すれば、ユーザー間でファイルと Paper ドキュメントの所有権を簡単に移行できます。管理者は、ユーザーのデータと共有関係を維持しつつユーザーのアカウントへのアクセスを無効にすることで、企業や組織の情報を守ることができます。また、遠隔削除機能を使用すれば、紛失したり盗難に遭ったデバイスからファイルや Paper ドキュメントを消去できます。

EU 域内でのインフラストラクチャ

GDPR では、個人データを EU 域内でホストすることは必須ではありませんが、対象となるチーム向け Dropbox のお客様が EU 域内でのファイル（ブロック）の保存をご希望の場合、保存が可能です。EU ベースのファイル ストレージは、Amazon Web Services（AWS）インフラストラクチャによって提供されます。EU 域内でのインフラストラクチャの詳細については、セールス担当にお問い合わせください。

お客様と共に取り組む個人データ保護

Dropbox は、お客様と協力して個人データの保護に取り組んでいます。インフラストラクチャ、ネットワーク、アプリケーションの保護、セキュリティとプライバシー対策についての社員トレーニング、信頼に応えることを最優先する社風の構築、システムと慣行に対する厳格な第三者機関によるテストと監査など、Dropbox は包括的な対策を講じています。

ただし、お客様も個人データの保護で重要な役割を持ちます。Dropbox の利用規約で、Dropbox のサービスをご利用いただく際のお客様の責任を説明しています。Dropbox では、お客様が組織のプライバシー、セキュリティ、コンプライアンスのニーズに合致した方法でアカウントを設定、使用、監視できるようにしています。Dropbox の共有責任ガイドをご覧いただくことで、アカウントを安全に保つために Dropbox が取り組んでいること、個人データの可視化と制御を維持するためにお客様ができることについて理解しやすくなります。

本ドキュメントのコンテンツに関する詳細については、privacy@dropbox.com までメールでお問い合わせください。