Dropbox

プライバシーとデータ保護

はじめに

個人データは社会や経済で大きな部分を占め、組織が利用および保護する際は、これまで以上に個人によるデータ管理への裁量と透明性が求められるようになりました。

Dropbox と世界中にいる数億人もの Dropbox ユーザーや企業との関係性を構築しているのは「信頼」です。私たちは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

私たちはお客様の個人データの保護に真摯に取り組んでいます。Dropbox のサービス利用規約では、Dropbox のサービスご利用の際に守っていただきたい事項について、概要を記しています。プライバシー ポリシーでは、Dropbox におけるユーザーに対するプライバシー責任を記載し、弊社サービスを利用される際の個人データの収集、使用、取り扱い方法について説明しています。北米（米国、カナダおよびメキシコ）にお住まいのお客様については、Dropbox, Inc. がサービス提供者となります。

他のすべてのお客様の個人データは、Dropbox International Unlimited Company が管理します。

Dropbox Business または Dropbox Education をお使いのお客様については、Dropbox Business または Dropbox Education のご使用に関連して Dropbox に提供された個人データは、お客様の所属する組織が管理します。個人データ処理の目的と手段はデータ管理者が決定します。Dropbox はデータ処理者として、Dropbox Business または Dropbox Education を使用するお客様の組織に代わってデータを処理します。弊社のビジネス契約書に、データ処理と国際データ転送に関する弊社の取り組みについて記載しています。

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立証するための効率的な方法です。Dropbox では、セキュリティおよびプライバシーに対する活動が、ISO 27001、ISO 27017、ISO 27018、HIPAA/HITECH、ドイツの BSI C5、SOC 1、2、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。

さらに、Dropbox は、クラウド プライバシーとデータ保護に関する主要な実践として国際的に認められている ISO 27018 を初めて取得したクラウド サービス プロバイダの 1 つです。独立した第三者の監査機関が弊社のデータ管理体制を検証し、報告書と意見書を提出します。これらの文書は可能な限りお客様と共有しています。

なお、弊社の認定や監査報告書は通常、Dropbox Business および Dropbox Education を対象としていますが、弊社のデータ管理体制の大部分は Dropbox Basic、Plus、および Professional のユーザーの皆様にも適用されます。弊社が準拠する基準や活動の検証方法の詳細については、コンプライアンス ウェブ ページをご覧ください。

Dropbox

Dropbox アーキテクチャ：個人データの保護

Dropbox では、個人データの保護はお客様のデータを安全に保つことから始まると考えています。これを達成するため、Dropbox は複数の保護レイヤで設計されています。たとえば、セキュリティ保護されたファイル データ転送、暗号化、アプリケーション単位の管理機能などが拡張性のある安全なインフラストラクチャ全体に装備されています。

Dropbox のインフラストラクチャ：ファイル

Dropbox のファイル用インフラストラクチャは、下の図に示すコンポーネントで構成されます。

メタデータ サーバー

ユーザー データに関する特定の基本情報はメタデータと呼ばれ、独立したストレージ サービスに保管されています。メタデータは、ユーザー アカウントのデータに対するインデックスとして機能します。メタデータには、メール アドレス、ユーザー名、デバイス名などの基本的なアカウント情報とユーザー情報が含まれます。また、ファイル名やファイル形式などファイルに関する基本情報も含まれ、バージョン履歴やファイルの復元、同期などの機能をサポートします。

メタデータ データベース

ファイルのメタデータは、MySQL ベースのデータベース サービスに保存され、パフォーマンスと高可用性に関する要件に対応するため、必要に応じてシャード化および複製されます。

ブロック サーバー

ユーザーのデータを保護するため、Dropbox は、従来の暗号化にとどまらない独自のセキュリティ対策を設計段階から備えています。ブロック サーバーは Dropbox アプリケーションからのファイルを 1 つずつブロック状に分割し、強力な暗号で各ファイル ブロックを暗号化し、変更されたブロックのみ同期することでファイルを処理します。ファイルの新規作成や既存のファイルの編集を検知した Dropbox アプリケーションは、その変更をブロック サーバーに通知し、新規作成または編集されたファイル ブロックを処理しストレージ サービスに転送します。

ブロック ストレージ サーバー

ユーザーのファイルに含まれる実際のコンテンツは、暗号化されたブロックの状態でブロック ストレージ サーバーを使用して保管されます。Dropbox クライアントはデータを転送する前に、ストレージに合わせてファイルをファイル ブロックに分割します。ブロック ストレージ サーバーは Content-Addressable Storage（コンテント アドレス ストレージ：CAS）システムとして機能し、暗号化された各ファイル ブロックはそのハッシュ値に基づいて取得されます。

プレビュー サーバー

プレビュー サーバーは、ファイルのプレビューの作成を担当します。プレビューとは、エンド ユーザーが自分のデバイスですぐに確認できるよう、ユーザーのファイルを別のファイル形式でレンダリングしたものです。プレビュー サーバーは、ブロック ストレージ サーバーからファイル ブロックを取得してプレビューを生成します。ファイルのプレビューが要求されると、まずプレビュー サーバーがプレビュー ストレージ サーバーからキャッシュされたプレビューを取得してブロック サーバーに転送します。最終的にユーザーにプレビューを提供するのはブロック サーバーです。

プレビュー ストレージ サーバー

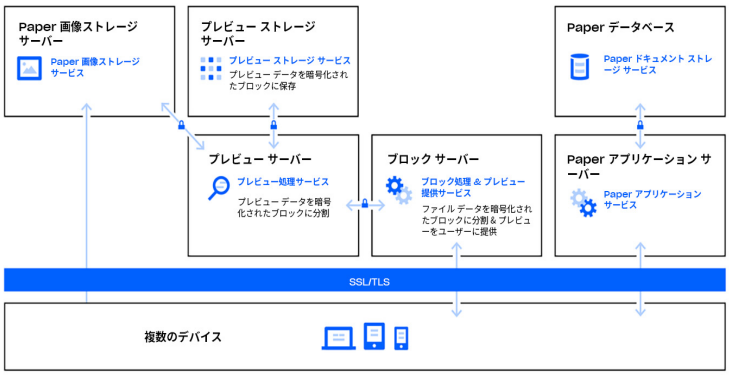
キャッシュ化されたプレビューは、暗号化された形式でプレビュー ストレージ サーバーに保管されます。

通知サービス

Dropbox アカウントに対して変更があったかどうかをモニタリングするための専用サービスです。ファイルやメタデータがこのサービスに保管されたり転送されたりすることはありません。各クライアントは、通知サービスに対してロング ポーリング接続を確立して待機します。Dropbox のファイルが変更されると、通知サービスはロング ポーリング接続を終了することによって、関連するクライアントに変更を通知します。接続の終了を契機に、クライアントはメタデータ サーバーへの安全な接続を確立し、ファイルの変更を同期します。

Dropbox

Dropbox のインフラストラクチャ：Paper
Dropbox Paper（Paper）は、Dropbox 製品が備える機能の 1 つです。ただし、Paper は Dropbox のインフラストラクチャ環境内で、Dropbox とは異なる特殊なシステムを使用します。Paper のインフラストラクチャは、下の図に示すコンポーネントで構成されます。



Paper アプリケーション サーバー
Paper アプリケーション サーバーは、ユーザーからの要求の処理、編集された Paper ドキュメントの出力の表示、および通知サービスを実行します。Paper アプリケーション サーバーは、ユーザーが行った編集を永続的なストレージに配置されている Paper データベースに書き込みます。Paper アプリケーション サーバーと Paper データベース間の通信セッションは、強力な暗号化が行われています。

Paper データベース
ユーザーの Paper ドキュメント自体に含まれるコンテンツに加え、その Paper ドキュメントについての特定のメタデータは Paper データベース上の永続的なストレージで暗号化されます。暗号化される情報には Paper ドキュメントについての情報（タイトル、共有中のメンバーシップと権限、プロジェクトとフォルダの関連など）に加え、Paper ドキュメント内のコンテンツ（コメントやタスクなど）が含まれます。Paper データベースは、パフォーマンスと高可用性に関する要件に対応するため、必要に応じてシャード化および複製されます。

Paper 画像ストレージ サーバー
Paper ドキュメントにアップロードされた画像は、Paper 画像サーバー上に保管され、暗号化されます。Paper アプリケーションと Paper 画像サーバー間の画像データの通信は暗号化されたセッションで実行されます。

プレビュー サーバー
プレビュー サーバーは、Paper ドキュメントにアップロードされた画像、および Paper ドキュメントに埋め込まれたハイパーリンクのプレビューを生成します。Paper ドキュメントにアップロードされた画像の場合は、暗号化チャネル経由で Paper 画像ストレージ サーバーに保存されている画像データを取り出します。Paper ドキュメントに埋め込まれたハイパーリンクの場合は、画像データを取り出し、ソースのリンクで指定された暗号化方式を使用して画像のプレビューを表示します。最終的にユーザーにプレビューを提供するのはブロック サーバーです。

プレビュー ストレージ サーバー
Paper は、Dropbox のインフラストラクチャ図にあるものと同じプレビュー ストレージ サーバーを使用して、画像プレビューのキャッシュを保存します。キャッシュ化されたプレビューのチャンクは、暗号化された形式でプレビュー ストレージ サーバーに保管されます。

Dropbox

Dropbox の情報管理：内部プラクティス

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、ファイルの完全削除などがあります。
また、社員全員に徹底したプライバシーとセキュリティのトレーニングを実施することで、信頼される会社となることが何よりも優先される文化を育んでいます。弊社の情報管理の詳細を以下に示します。

トレーニング
ユーザーの個人データを保護するためには、セキュリティとプライバシーを意識する文化を構築し、それを育むことも大切です。Dropbox の社員は、システムへのアクセス権を付与される前に、ユーザー データのプライバシー ポリシーを含むセキュリティ ポリシーに同意することが求められます。こうしたシステムへのアクセス権が付与されるのは、アクセスする必要がある社員のみです。さらに、社員には毎年セキュリティとプライバシー トレーニングの受講が義務付けられています。

転送中データの暗号化
Dropbox クライアント（現在はデスクトップ/モバイル/API/ウェブ）と Dropbox のフロントエンド サーバー間で転送中のファイル データを保護するため、暗号化接続のネゴシエーションを行い、安全な転送を確保しています。同様に、Paper クライアント（現在はモバイル/API/ウェブ）とホスト サービス間でも、転送中の Paper ドキュメント データを保護するため、暗号化接続のネゴシエーションを行います。これらの接続は、セキュア ソケット レイヤ（SSL）/トランスポート レイヤ セキュリティ（TLS）を使用して暗号化され、128 ビット以上の AES 暗号化で保護された安全なトンネルを作成します。

保存データの暗号化
ユーザーがアップロードしたファイルは、Dropbox のストレージ サーバーに個別のファイル ブロックとして保存されます。各ブロックは、256 ビットの Advanced Encryption Standard（AES）で暗号化されています。ファイルの編集中に変更されたブロックのみが同期対象になります。同様に、Paper データベースに保存された Paper ドキュメント データも、256 ビットの Advanced Encryption Standard（AES）で暗号化されています。

ファイルと Paper ドキュメントの完全削除
Dropbox ユーザー、あるいは Dropbox Business または Dropbox Education のチーム管理者がファイルを完全削除の対象として指定すると、そのファイルを完全に削除する処理がトリガーされます。同じように、ユーザー、あるいは Dropbox Business または Dropbox Education のチーム管理者が Paper ドキュメントを完全削除の対象として指定すると、Paper ドキュメントのデータと画像データを完全削除するための同様の処理が行われます。

個人データへのアクセス リクエスト
Dropbox を使用して保存したファイルや Paper ドキュメント以外の個人データにアクセスするには、Dropbox ウェブサイトにログインし、自分のアカウント ページに移動します。アカウント ページには、アカウントに関連付けられている氏名やメール アドレスなどの情報が表示されます。また、セキュリティ ページやリンク済みアプリ ページから、接続済みセッション、パソコン、モバイル デバイスの IP アドレスに加えて、アカウントにリンクされているアプリを確認することもできます。

Dropbox ユーザーは、Dropbox が収集したその他の個人データへのアクセス権やそれらのデータの削除をリクエストすることもできます。
このプロセスの詳細については、Dropbox ヘルプセンターをご覧ください。

Dropbox におけるプライバシー ガバナンス
Dropbox プライバシー プログラムの運用は、プライバシー プログラム チームが担当しています。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」を実現するための取り組みを行っています。
Dropbox プライバシー プログラムには、複数の法務関連チームも部門の枠を超えて関与しています。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。

DPO（データ保護責任者）チームは他のプライバシー関連職とは独立して活動し、プライバシーのコンプライアンスと監督を担当する組織として、データ保護責任者の任務の遂行を直接的にサポートします。データ保護責任者は EU 域内の代表者であり、連絡先は privacy@dropbox.com です。

Dropbox

政府からのデータ要請に関する指針

Dropbox ではユーザーの皆様からお預かりした個人データを安全に保管し、皆様の信頼と期待に応えることに尽力しております。多くのオンライン サービス会社と同様に、Dropbox は政府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。

政府からの情報開示要請をどのように処理するかについて、以下に原則を説明します。

透明性を保つ

オンライン サービスを提供する企業は、政府による情報公開要請の回数や要請された情報の種類を個人に公開できるべきだと私たちは考えます。このように透明性を保つことで、ユーザーは政府の過度な情報要求の実態と共通の特徴を把握できます。

Dropbox は今後もこのような要請の詳細を公開し、こうした重要情報のさらなる提供の権利を主張していきます。

過度に広範囲な要請に応じない

政府による情報開示要請は、必要とする情報のみに制限され、特定のユーザーの合法的な調査に合わせた狭い範囲に制限されるべきです。Dropbox は一括要請と過度に広範囲な要請には応じません。

信頼できるサービスを提供する

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

居住地と市民権の存在する場所に応じて保護内容が異なる法律は、時代に沿わなくなっており、グローバルな特性を備えたオンライン サービスには適していません。Dropbox は、これらの法律の改定に取り組み続けています。

これらの原則は、弊社の年次透明性レポートとともに Dropbox ウェブサイト（https://www.dropbox.com/transparency）で公開されています。

お客様の個人データの保護に対する弊社の管理とアプローチの詳細については、Dropbox Business のセキュリティに関するホワイトペーパーをご覧ください。

Dropbox と提携している第三者

Dropbox では、サービスの提供に関連するアクティビティの大部分を自社で管理していますが、一部の信頼できる第三者を弊社のサービスに関連して利用する場合もあります（カスタマー サポートや IT サービスのプロバイダなど）。これらの第三者は、弊社のプライバシー ポリシーに遵守しながら、Dropbox の代理として作業を行う目的でのみ、お客様の情報にアクセスします。また、第三者が Dropbox の指示に従ってお客様情報を取り扱うよう、Dropbox が責任を負います。

第三者はそれぞれ、セキュリティに関するレビューや定期的な契約レビューを含む厳格な審査プロセスを受け、弊社のデータ保護の約束を果たす能力が評価されます。

データの国際転送

Dropbox は、欧州連合（EU）から米国への個人データの国際転送について、さまざまな法体系に依拠しています。Dropbox は、EU およびスイスから米国に移転された個人データの収集、使用、保存に関して、EU と米国間ならびにスイスと米国間のプライバシー シールド プログラムの認定を受けています。プライバシー シールドに加えて、Dropbox ではサービスのプライバシーについて堅牢な契約上の保証を取り決めており、国際データ転送を対象に EU 標準契約条項を実践しています。

Dropbox

GDPR：一般データ保護規則

一般データ保護規則（GDPR）は EU の規則であり、EU のデータ主体（情報の持ち主）の個人データの保護に関する法的な枠組みです。

GDPR は、1995 年の EU データ保護指令以来最も重要な欧州データ保護法の構成要素であり、Dropbox を含めて、ヨーロッパで事業を行う多くの企業が GDPR に準拠するため莫大な投資を行っています。

GDPR は、欧州全域のデータ保護法を調和させ、過去 20 年間における技術の急速な変化への対応を目指しています。

GDPR は、EU データ保護指令を含む、EU における過去の法的枠組みに基づいて構築されており、個人データを扱う組織に対して新しい義務と責任を課すと同時に、個人データに関してユーザーに新しい権利をもたらします。

EU で設立された組織、ならびに EU のデータ主体の個人データを処理する組織は、GDPR に準拠する必要があります。

Dropbox が GDPR に準拠するまで

Dropbox は GDPR への準拠に取り組んでいます。プライバシーとセキュリティの尊重は、Dropbox のビジネスに当初より組み込まれていた考え方です。Dropbox は成長を遂げましたが、お客様が信頼して預けてくださるデータの取り扱いと保護については、最優先事項として今でも重要視しています。Dropbox は率先してコンプライアンスを満たしてきた実績があります。上述のように、Dropbox は、法人ユーザー向けに ISO 27018 認定を初めて取得したクラウド サービス プロバイダの 1 つです。こうした強力な基盤があることから、GDPR への準拠は Dropbox における個人データの取り扱いを一歩前進させ、ユーザーの皆様の個人データを常に保護するための継続的かつ進化し続ける一連のイニシアチブを体現するものであると考えています。

GDPR 準拠に向けての準備は、2016 年に規則が採択された直後から始まりました。最初のステップでは、法律顧問、セキュリティとコンプライアンスの専門家、製品エンジニアとインフラストラクチャ エンジニアからなる部署の枠を超えたデータ保護専門チームを立ち上げ、現在のセキュリティとデータ保護の活動を GDPR の要件に照らしてくまなく評価しました。

次のステップでは、個人データ処理のアクティビティを評価し、Dropbox の各種システムで個人データのライフサイクルを追跡しました。こうした実践は、データマッピングの実施やデータ保護影響評価の完了と呼ばれることもあります。

それ以来、Dropbox は、GDPR の要件に則り説明責任の原則を確実に満たすよう、既存の社内プロセスと社内手順を改善しています。GDPR では、個人データに影響する決定事項や実践の文書化に大きな重点が置かれていることを考えれば、これはは重要です。

Dropbox

ユーザーの GDPR 準拠を支援

Dropbox では、GDPR 準拠義務を含めて、お客様のデータ保護義務をより容易に管理できるような機能や可視化機能を提供しています。当然ながら、お客様の組織全体の GDPR の準拠は、Dropbox などのサプライヤーとの関係性だけで完結するものではありません。Dropbox の機能はお客様が義務を果たすお手伝いをしますが、それ自体でコンプライアンスを保証することはできません。GDPR に準拠するには、お客様の組織内でデータがどのように移動し、保護されるかについて、より広い視点で考える必要があります。コンプライアンスを達成するには、サプライヤーを重要なパートナーとして味方に付けながら、各組織が独自の手順を実行する必要があります。

データの最小化

GDPR が定める「Privacy by Design（プライバシー バイ デザイン：設計時にプライバシーの考え方を組み込むこと）」の重要な要素の 1 つが、データを最小化するように組織のサービスを設計することです。これは、組織内のデータに対して優れた可視化と制御を実現し、管理しやすくすることを意味します。Dropbox Business の管理者用ダッシュボードはこのための便利なツールであり、チームのアクティビティの監視、リンク済みデバイスの表示、共有アクティビティの監査を行うことができます。Dropbox では、新しい製品と機能に「プライバシー バイ デザイン」の原則を組み込むための取り組みを進めています。

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、ファイルの復元は、意図しない紛失、損害、または破壊から個人データを保護します。また、インシデントの発生時に、可用性と個人データへのアクセスをすぐに復元することもできます。また 2 段階認証も、お客様のデータ保護のために推奨される重要な対策です。

記録の保持

GDPR では、組織がそのデータ処理アクティビティの詳細な記録を保持することに対して、より大きな義務が定められています。Dropbox の監査ログとアクティビティ ログは、データ処理アクティビティに関する理解を深め、記録するサポートをします。

アクセス管理

Dropbox Business の管理者用ダッシュボードでは、チーム メンバーによるファイルやフォルダ、Paper ドキュメントへのアクセスを簡単に管理できます。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コンテンツへの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。ユーザー間で責任の所在を変更する場合、アカウント移行ツールを使用すると、ファイルや Paper ドキュメントの所有権を別のユーザーに簡単に移行することができます。

管理者は、アカウントへのユーザーのアクセス権を無効にすると同時に、そのユーザーのデータと共有関係を保持することができるため、組織の情報を安全に保つことができます。

最後に、遠隔削除機能では紛失や盗難にあったデバイスのファイルや Paper ドキュメントを削除できます。

EU のインフラストラクチャ

GDPR では個人データを EU 内で保管することは義務付けられていませんが、Dropbox は、対象となる Dropbox Business と Dropbox Education のお客様向けに、ファイル（ブロック）を EU で保管できるようにしています。EU にあるファイル ストレージは、Amazon Web Services（AWS）のインフラストラクチャを利用しています。EU のインフラストラクチャの詳細については、Dropbox の営業チームにお問い合わせください。

Dropbox

個人データの保護に向けた連携

Dropbox はユーザーと連携して個人データを保護しています。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の包括的な対策を講じ、社員向けにセキュリティとプライバシーに関するトレーニングを実施しています。また、信頼を最優先とする文化を育み、システムと活動に対して第三者による厳格なテストと監査を実施しています。

しかし、個人データの保護にはユーザーの役割も重要になります。Dropbox では、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を満たすような方法でアカウントを設定、使用、監視することができます。Dropbox の共有責任ガイドでは、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、より詳しく説明しています。

まとめ

Dropbox では毎日何百万人ものユーザーの皆様のデータをお預かりしています。その信頼に応えるため、Dropbox では今までもこれからも変わらず、セキュリティとプライバシーを重視して成長を続けていきたいと考えています。ユーザーの個人データを保護するという約束は、私たちが意思決定を下す際に何よりも優先されます。詳細については、privacy@dropbox.com までお問い合わせください。GDPR の詳細については、GDPR ガイダンス センターもご覧ください。