# Dropbox Business のセキュリティ

Dropbox ホワイトペーパー

©2023 Dropbox. All rights reserved. V2023.01

Dropbox

# 目次

# はじめに

さまざまな業種でデジタル トランスフォーメーションが定着しつつあり、データ、チーム、デバイスが、どこにあっても保護されることが大変重要になっています。Dropbox Business などのクラウド ソリューションを活用してテレワークや分散ワークを行っている組織は、共同作業を効率化し、クラウドのリスクに先手を打って対処しつつ、効果的な管理を行う必要があります。言い換えると、管理機能と耐障害性に優れたクラウド サービスを使うことで、組織の知的財産（IP）の機密性、保存データや共有データの完全性、そしてデータの可用性を確保することが求められています。

Dropbox Business は、テレワークで働くチームが安全に共同作業できるソリューションとして、60 万以上の企業や組織に採用されています。Dropbox Business の中核をなすソリューションは、コラボレーションのためのスマート ワークスペース、そしてファイルの同期と共有の機能です。高度なエンタープライズ セキュリティ、チームとコンテンツのセキュリティ、電子署名、安全なファイル送信、そしてデータ ガバナンスを実現するための各種の機能に加えて、業界最先端のインフラストラクチャが Dropbox のソリューションを支えています。別段の記載がある場合を除き、このホワイトペーパーの情報はすべての Dropbox Business 製品（Standard、Advanced、および Enterprise）と Dropbox Education に適用されます。Paper は、Dropbox Business および Dropbox Education の機能です。

Dropbox Business の中核にあるのは、Dropbox 信頼プログラムと呼ばれる包括的なセキュリティ プログラムです。このプログラムでは、複合的なセキュリティ対策を講じており、世界中でリモート ワークが盛んに行われるようになった今、このようなアプローチが非常に重要になっています。

このホワイト ペーパーでは、Dropbox Business 製品のセキュリティ機能、Dropbox の運用面でのセキュリティ対策、プライバシーと透明性に関するコミットメントの他に、バックエンド ポリシー、独立機関による認証、規制準拠の施策について詳しく解説します。これらはどれも、Dropbox を組織にふさわしいセキュアなソリューションにするための基盤となっています。

**別段の記載がある場合を除き、このホワイトペーパーの情報はすべての Dropbox Business 製品（Standard、Advanced、および Enterprise）と Dropbox Education に適用されます。Paper は、Dropbox Business および Dropbox Education の機能です。**

# 機能の詳細

Dropbox の使いやすいインターフェースは、同期、共有、共同作業をスピードアップできるように、バックグラウンドで動作するインフラストラクチャで支えられています。Dropbox では、製品やアーキテクチャを常に進化させ、データ転送の高速化、信頼性の向上、環境変化への適合を図っています。このセクションでは、セキュリティを維持しつつデータがどのように転送、保管、処理されているかを説明します。

## ファイル インフラストラクチャ

ユーザーは、デスクトップ、ウェブ、モバイル クライアント、Dropbox にリンクしているサードパーティ製アプリなどから、Dropbox のファイルやフォルダにいつでもアクセスできます。すべてのクライアントでは、セキュリティで保護されたサーバーに接続して、ファイルへのアクセスや、他のユーザーとのファイル共有を行うことができます。ファイルが追加、変更、削除された場合は、Dropbox にリンクしているすべてのデバイスで最新のファイルが保持されます。

Dropbox のファイル インフラストラクチャは、次のコンポーネントで構成されています。


- **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するのに役立ちます。

- **メタデータ データベース**

  ファイルのメタデータは複数バージョンの並行処理制御を備えたトランザクション キー バリュー ストアに保管され、パフォーマンスと高可用性の要件を満たすよう、必要に応じてシャーディングと複製が実行されます。

- **ブロック サーバー**

  Dropbox は、従来の暗号化を超えて設計された独自のセキュリティの仕組みを利用して、ユーザーのデータを保護しています。ブロック サーバーでは、Dropbox アプリケーションからのファイルをブロックに分け、強力な暗号を使用して各ファイル ブロックを暗号化し、リビジョン間で変更のあったファイル ブロックのみを同期します。Dropbox アプリケーションが新しいファイルや既存ファイルに対する変更を検知すると、変更があったことをブロック サーバーに通知します。新規または変更されたファイル ブロックは、前述のように処理されてブロック ストレージ サーバーに転送されます。さらに、ブロック サーバーはファイルやプレビューを配信するために使用されます。これらのサービスが転送や保管の際に使用する暗号化の詳細については、以下の「暗号化」のセクションをご覧ください。

- **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を作成します。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個別のサービスです。ファイルやメタデータがこのサービスに保管または転送され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、通知サービスがロング ポーリング接続を終了することで、関連するクライアントに変更を通知します。ロング ポーリング接続の終了を検知したクライアントは、メタデータ サーバーに安全に接続して、ファイルの変更を同期する必要があります。

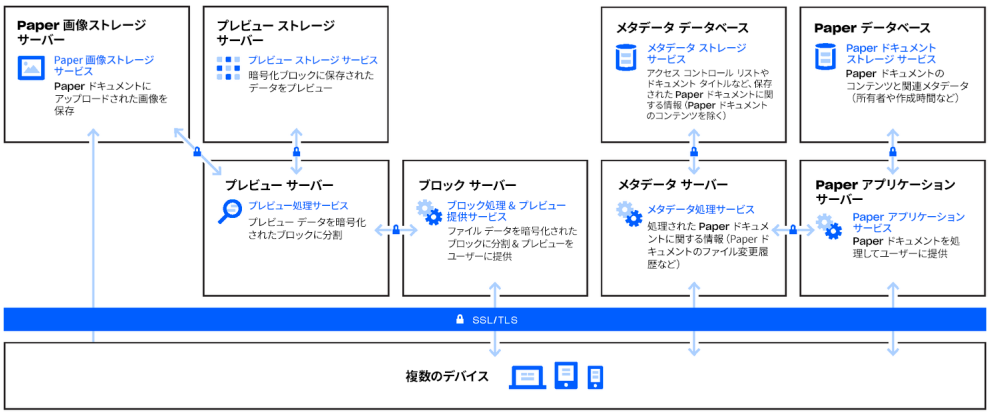
## ファイル データ ストレージ

Dropbox には基本的に、ファイルに関するメタデータ（ファイルが最後に変更された日時など）とファイルの実際のコンテンツ（ファイル ブロック）という 2 種類のファイル データが保管されます。ファイルのメタデータは、Dropbox サーバーに保管されます。ファイル ブロックは、Amazon Web Services（AWS）または Dropbox の社内ストレージ システムである Magic Pocket の 2 つのシステムのいずれかに保管されます。Magic Pocket は独自のソフトウェアとハードウェアで構成されており、高い信頼性と安全性を確立するために新規に設計されています。Magic Pocket と AWS の両方で、ファイル ブロックは暗号化された状態で保管され、両方のシステムとも高い信頼性基準を満たしています。詳細については、後述の「信頼性」のセクションをご覧ください。

## Paper インフラストラクチャ

ユーザーは、ウェブやモバイル クライアント、Dropbox Paper にリンクしているサードパーティ製アプリなどから、Paper のドキュメントにいつでもアクセスできます。すべてのクライアントでは、セキュリティで保護されたサーバーに接続して、Paper のドキュメントへのアクセスや、他のユーザーとのドキュメントの共有を行うことができます。ドキュメントが追加、変更、削除された場合も、Dropbox にリンクしているすべてのデバイスで最新の状態が維持されます。

Dropbox Paper のインフラストラクチャは、次のコンポーネントで構成されています。



- **Paper ドキュメント ストレージ**

  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、Secure Hypertext Transfer Protocol（HTTPS）によって安全が保たれています。

- **Paper データベース**

  Paper ドキュメントに関するメタデータとユーザーの Paper ドキュメントの実際のコンテンツは、Paper データベースの永続的なストレージ上で暗号化されています。Paper コメントやタスクなどのドキュメント内のコンテンツだけでなく、その Paper ドキュメントについての情報（タイトル、所有者、作成日時など）も暗号化されます。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を満たすために、必要に応じてシャード化/複製されます。

- **メタデータ サーバー**

  Paper は、Dropbox インフラストラクチャ図で解説されているのと同じメタデータ サーバーを使用して、Paper ドキュメントに関する情報を処理します。こうした情報にはファイルの変更履歴、共有フォルダのメンバーシップなどがあります。Dropbox は、サードパーティのコロケーション データ センターに置かれているメタデータ サーバーを直接管理します。

- **メタデータ データベース**

  Paper は、Dropbox インフラストラクチャ図で解説されているのと同じメタデータ データベースを使用して、Paper ドキュメントに関する情報を保存しています。こうした情報には、共有、権限、フォルダの関連付けなどがあります。Paper ドキュメントのメタデータは MySQL ベースのデータベース サービスに保管され、パフォーマンスと高可用性に関する要件を満たすために、必要に応じてシャード化/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した画像は、Paper 画像ストレージ サーバーに暗号化されて保存されます。Paper アプリケーション サーバーと Paper 画像ストレージ サーバー間の画像データの転送は、暗号化されたセッションを介して行われます。

- **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。

### Paper ドキュメントのストレージ

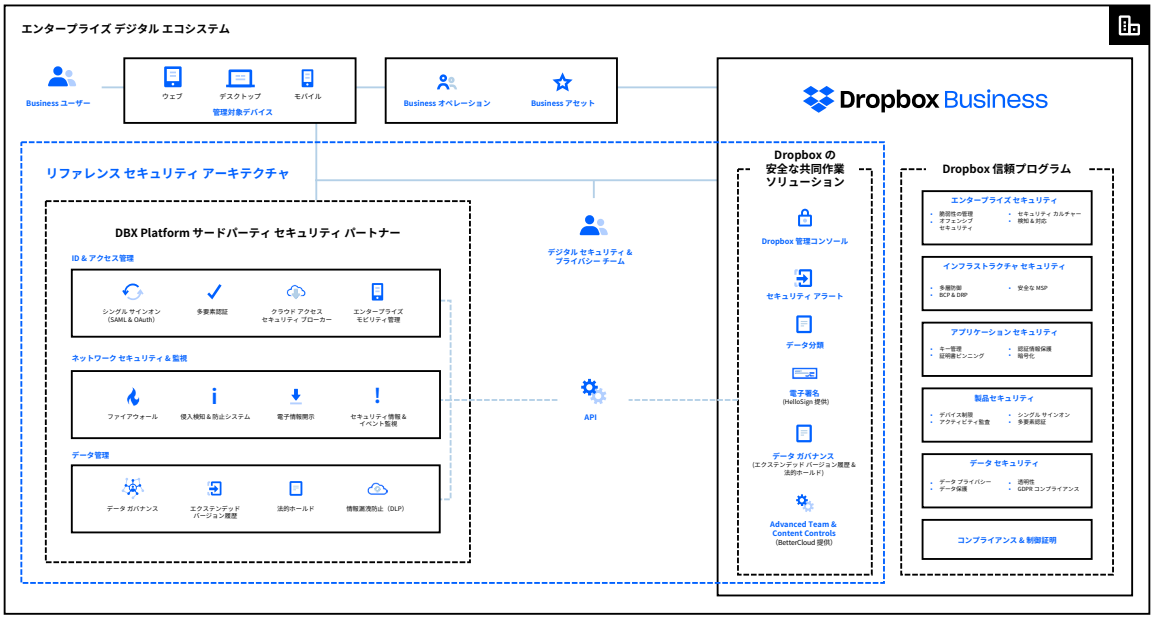
Dropbox では Paper ドキュメントに主に次の種類のデータを格納します。1 つは Paper ドキュメントに関するメタデータ（ドキュメントの共有権限など）、もう 1 つはユーザーによってアップロードされた Paper ドキュメントの実際のコンテンツです。これらをまとめて Paper ドキュメント データと呼び、Paper ドキュメントにアップロードされた画像は Paper 画像データと呼びます。この種のデータは、Amazon Web Services（AWS）に保存されます。Paper ドキュメントは、AWS で静的に暗号化されており、AWS は高信頼性基準を満たしています。詳細については、後述の「信頼性」セクションを参照してください。

# Dropbox 信頼プログラム

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、情報保護の責任を第一に考えています。皆様の信頼に応えられるよう、セキュリティ、プライバシー保護、透明性、コンプライアンスに重点を置いて Dropbox を構築しました。今後もこの方針のもとで Dropbox を成長させていきます。

Dropbox 信頼プログラム ポリシーでは、リスク評価プロセスを確立しています。このプロセスは、システムのセキュリティ、機密性、完全性、可用性、プライバシー保護などに影響する可能性のあるさまざまなリスク（環境、物理的条件、ユーザー、サードパーティ、適用法、契約要件などに関するリスク）に対応するために設計されたものです。対応状況の見直しは、年に 1 回以上実施されます。Dropbox 信頼プログラムの詳細については、dropbox.com/business/trust をご覧ください。

Dropbox では、組織にとって重要な、事業、インフラストラクチャ、アプリケーション、製品のセキュリティを確保するために、多層的なアプローチを採用しています。



# エンタープライズ レベルのセキュリティ

Dropbox は、情報セキュリティ マネジメント フレームワークを確立しています。このフレームワークは、信頼性を維持するための目的、方向性、原則、基本規則を表し、Dropbox Business システムのリスクを評価し、セキュリティ、機密性、整合性、可用性、プライバシーを継続して改善することによって実現されています。Dropbox は定期的にセキュリティ ポリシーの見直しや更新、セキュリティ トレーニングの提供、アプリケーションやネットワークのセキュリティ テスト（侵入テストを含む）を実施しています。また、セキュリティ ポリシーのコンプライアンスを監視し、内部と外部からのリスク評価も行っています。

## Dropbox のポリシー

Dropbox はセキュリティ ポリシーを完備し、Dropbox セキュリティおよび不正防止チーム（Dropbox Security and Abuse Team）がこれを適用しています。ポリシーは少なくとも年に 1 度は見直され、承認されています。Dropbox の社員、インターン、契約社員は入社時にセキュリティ トレーニングへの参加が義務付けられており、さらにはセキュリティ認識トレーニングを継続的に受講しています。

- **情報セキュリティ**
  ユーザーと Dropbox の情報を安全に保ちます。
- **認証**
  Dropbox 社員が情報システムとデータにアクセスする際に自分自身を認証する方法について説明しています。
- **デバイス セキュリティ**
  企業情報にアクセスするために使用するモバイル デバイスの最小セキュリティ要件を定めています。
- **論理的アクセス制御**
  Dropbox のシステム、ユーザー、情報へのアクセスを安全に保ちます。企業環境とプロダクション環境へのアクセス制御について取り決めています。
- **データ セキュリティ**
  Dropbox が特定のストレージ、アクセス、および使用の要件を設けてデータをどのように保護しているかを説明します。
- **出張時のセキュリティ**
  Dropbox 社員が国外へ出張する前にすべきことについて定めています。
- **営業とお客様向けサポート（CX）のセキュリティ ガイドライン**
  ユーザーの情報と Dropbox 社員を保護し、ユーザーにサポートを提供します。
- **物理セキュリティ**
  Dropbox の社員や資産が安全に守られる環境を維持します。
- **プロダクション環境の物理的なセキュリティ ガイドライン**
  プロダクション施設への物理的なアクセスを管理します。

- **インシデント レスポンス**

  セキュリティ、プライバシー、サイトに関する事象が報告されたときに、Dropbox がどのように対処し、それぞれに対するインシデント レスポンス計画を策定するかをまとめています。

- **著作物の不正使用**

  社員が Dropbox や自社のシステムを使用して、権利のないコンテンツを保存または共有することを禁止します。

- **変更管理**

  プロダクション システムへの変更を管理します。システムへのアクセス権を持つすべての Dropbox 社員、契約社員、インターンが対象となります。

- **ユーザー データのプライバシー**

  自社のプライバシー ポリシーに従って、Dropbox でのユーザー情報とユーザー データを保護および処理します。

- **事業継続ポリシーおよび危機管理**

  人（Dropbox 社員）、資産、（ビジネス）プロセスの維持、保護、安全について説明しています。

- **Dropbox プライバシー プログラム**

  Dropbox プライバシー プログラムの目的、原則、説明責任。

- **Dropbox 信頼プログラム**

  Dropbox がどのように運営されているか、そしてなぜ信頼に値するかを説明しています。

- **支払環境のセキュリティ**

  クレジット カードによる支払いを受け付けられるよう、Dropbox で使用されている専用の支払環境を保護し維持するためのセキュリティです。

## 社員ポリシーおよびアクセス

Dropbox の社員は採用時にバックグラウンド チェックを受け、セキュリティ ポリシーの承認と機密保護契約に署名し、セキュリティに関するトレーニングを受けることが求められます。これらの手順を完了した社員だけが、職務における必要性に従って、Dropbox の企業環境およびプロダクション環境への物理的/論理的アクセスが許可されます。また、全社員が年 1 回のセキュリティ トレーニングを修了することが求められ、社員はセキュリティ情報に関するメール、講演、プレゼンテーション、社内イントラネットで閲覧可能な資料を通じてセキュリティ意識に関するトレーニングを日常的に受けています。

社員による Dropbox 環境へのアクセスは中央ディレクトリにより管理されており、認証には、強力なパスワード、パスフレーズで保護された SSH キー、2 段階認証の組み合わせが使用されます。リモート アクセスを使用する場合は 2 段階認証によって保護されている VPN を使用する必要があり、特別なアクセスがあった場合はセキュリティ チームが見直しおよび入念な検査を行います。企業ネットワークやプロダクション ネットワークへのアクセスは、明確なポリシーに基づいて厳しく制限されています。たとえば、Dropbox のプロダクション ネットワー

クへのアクセスは SSH キー ベースであり、業務の一環としてアクセスが必要なエンジニアリング チームのみに限られています。ファイアウォール設定も厳格に管理され、ごく少数の管理者のみがアクセスできます。

また、Dropbox の内部ポリシーでは、Dropbox のプロダクション環境や企業環境にアクセスする社員に対して、SSH 秘密鍵の作成および保管に関するベスト プラクティスを遵守するように指示しています。データ センター、サーバー設定ユーティリティ、プロダクション サーバー、ソース コード開発ユーティリティなど、その他のリソースについては、適切な管理者による明示的な承認によりアクセス権が付与されます。アクセス権のリクエスト、正当性、承認に関する記録は管理者が行い、適切な担当者によってアクセス権が付与されます。

Dropbox は技術的なアクセス制御と内部ポリシーを使用して、社員が独自の判断でユーザー ファイルにアクセスすることを禁止し、ユーザーのアカウントについてのメタデータやその他の情報にアクセスすることを制限しています。エンド ユーザーのプライバシーとセキュリティを保護するために、Dropbox のコア サービスを開発している少数のエンジニアのみがユーザー ファイルの保存されている環境にアクセスできます。社員が退職した場合は、退職後すぐにアクセス権が取り消されます。

Dropbox はお客様のインフラストラクチャ拡張としてサービスを提供しているため、お客様は安心して Dropbox にデータ保護を任せることができます。詳細については、後述の「プライバシー」のセクションをご覧ください。

## 脆弱性の管理

Dropbox のセキュリティ チームは、定期的に自動および手動でセキュリティ テストとパッチ管理を行うとともに、サードパーティの専門家と協力して潜在的なセキュリティ脆弱性とバグを特定し、修正しています。

Dropbox では、情報セキュリティ マネジメント システムの 1 つの要件として、上記すべてのセキュリティ評価の調査結果と推奨事項をマネジメント チームに伝達し、評価を受けます。その後、必要に応じて適切な方法で対処します。重大性の高い項目は、記録および追跡され、指定されたセキュリティ担当エンジニアが解決します。

### 変更管理

開発、問題の修正、パッチ適用のプロセスは、すべて Dropbox エンジニアリング チームが定めた公式な変更管理ポリシーに従って行われます。その結果、システム変更はテストされ承認を得なければプロダクション環境に導入できないようになっています。ソース コードの変更を開始するのは、Dropbox アプリケーションやサービスの機能向上を希望する開発者です。変更はバージョン管理システムに保存され、セキュリティ要件が満たされているかどうか確認するため、自動化された品質管理テスト手順を完了することが求められます。品質管理手順が正常に完了すると、変更適用の段階に進みます。品質管理で承認された変更は、自動的にプロダクション環境に適用されます。Dropbox のソフトウェア開発ライフサイクル（SDLC）では、セキュア コーディング ガイドラインに従う必要があります。また、品質管理および手動による審査プロセスを通じて、コード変更に対するスクリーニングを行い、セキュリティの潜在的な問題がないか確認することも求められます。プロダクション環境にリリースされた変更内容はログに記録されるとともにアーカイブされます。この際、Dropbox エンジニアリング チームの管理者にアラートが自動的に送信されます。

Dropbox インフラストラクチャに対する変更は、承認された社員のみに制限されています。Dropbox のセキュリティ チームは、インフラストラクチャのセキュリティを保護し、サーバー、ファイアウォール、その他のセキュリティ関連の設定を最新に保ち業界標準に準拠させる責任があります。ファイアウォール ルールと、プロダクション サーバーへのアクセス許可を持つ社員は、定期的にチェックされ見直されます。

### 脆弱性のスキャンおよびセキュリティ侵入テスト（社内および社外）

Dropbox のセキュリティ チームは、アプリケーションのセキュリティ テストを自動/手動で定期的に実施し、デスクトップ用、ウェブ用（Dropbox と Paper）、モバイル用（Dropbox と Paper）の各アプリの潜在的なセキュリティ脆弱性やバグを特定し、修正しています。

また、Dropbox はサードパーティのベンダーと契約し、プロダクション環境に対して定期的な侵入テストと脆弱性テストを実施しています。そしてサードパーティのセキュリティ専門家、業界の他のセキュリティ チーム、セキュリティ研究のコミュニティと協力して、Dropbox のアプリケーションを安全な状態に維持しています。Dropbox は脆弱性を見つけるために複数の自動解析システムを使っていますが、このプロセスには社内で開発したシステムや Dropbox のニーズに合わせてカスタマイズしたオープン ソースのシステム、継続的な自動解析業務を委託している社外ベンダーのシステムが含まれます。

### 有害なコンテンツから Dropbox を保護

Dropbox には、有害なコンテンツが Dropbox に保存され、拡散されるのを防ぐためのスキャン機能があります。このスキャン機能では、Microsoft や Google などのパートナーから提供された業界最先端の機能に加えて、自社で開発したテクノロジーを駆使することで、Dropbox をお客様にとって安全な場所にしています。

### バグ発見の奨励金

Dropbox では、専門の会社に委託した侵入テストと自社のテストの他に、バグ発見の奨励金（脆弱性の報告に関する報酬プログラム）を提供することにより、幅広いセキュリティ コミュニティの専門知識を活用しています。Dropbox のバグ発見の奨励金プログラムは、ソフトウェアのバグを発見し責任を持って開示する研究者に対して報奨金を提供します。このように社外コミュニティを関与させることで、Dropbox のセキュリティ担当チームはアプリケーションを独立した立場で精査し、ユーザーの安全性確保に役立てることができます。報奨金額でも、対処や修正の早さでも、Dropbox は業界をリードするべく努力しています。

Dropbox では、報奨金プログラムの対象となる申請内容と Dropbox アプリケーションの範囲を設定し、さらに、セキュリティの脆弱性の発見と報告を促進し、ユーザーの安全性を高めるための責任ある公開ポリシーを設けています。このポリシーのガイドラインは、次のとおりです。

- セキュリティ問題の詳細をご連絡ください。
- 既存のアプリケーションを尊重していただきます。脆弱性の自動スキャンによって生まれるスパム行為は、明確に範囲外とされているため、報奨金や賞金の対象となりません。
- Dropbox がセキュリティの問題に対処するための相応の時間を取ってから、問題に関する情報を一般公開します。
- アカウント所有者の許可なしに、ユーザー データへのアクセスおよび変更は行わないでください。
- データの閲覧、変更、保存、保管、転送、その他の方法でのアクセスは禁じられています。また、Dropbox に脆弱性を報告した後はただちに、ローカルにあるすべての情報を消去する必要があります。
- プライバシーの侵害、データの破壊、サービスの妨害やパフォーマンスの低下（サービス拒否攻撃を含む）が生じないよう、誠実な対応をお願いします。

問題は、Bugcrowd（bugcrowd.com/dropbox）経由で報告できます。

## 物理セキュリティ

### インフラストラクチャ

Dropbox のプロダクション システムが設置されているサブサービス組織の施設への物理的なアクセスは、Dropbox が承認した担当者が職務のために必要な場合のみに限定されています。それ以外に Dropbox のプロダクション環境施設へのアクセスを必要とする担当者には、しかるべき管理者が明示的に承認してアクセス許可を付与します。

アクセス権のリクエスト、正当性、承認に関する記録は管理者が行い、適切な担当者によってアクセス権が付与されます。承認後はインフラストラクチャ チームの承認されたメンバーが該当するサブサービス組織に連絡し、承認された担当者のアクセス権をリクエストします。サブサービス組織は社内システムに担当者の情報を入力し、承認された Dropbox 社員にバッジ アクセス（可能であれば、生体認証によるアクセス）を許可します。承認された担当者にアクセス権が付与された後は、データ センターが責任を持って、そのアクセス権が承認済みの担当者に制限されるようにする必要があります。

## Dropbox オフィス

- **物理セキュリティ**

  物理的なセキュリティ ポリシーを施行し、Dropbox オフィスのセキュリティを監督する責任は、Dropbox の物理セキュリティ チームが担っています。

- **訪問者とアクセスに関するポリシー**

  Dropbox の施設（一般用エントランスとロビーを除く）への物理的なアクセスは、承認された Dropbox 社員と、Dropbox 社員が同伴する登録済みの訪問者のみに制限されています。バッジ アクセス システムにより、承認された人物のみが Dropbox 施設内の制限区域にアクセスできます。

- **サーバーへのアクセス**

  Dropbox のサーバーやネットワーク機器が設置されているサーバー ルームなどの区域へのアクセスは、バッジ アクセス システムから上位の権限を付与された承認済みの担当者のみに制限されます。Dropbox の企業環境とプロダクション環境への物理的なアクセス権を付与された社員のリストは、四半期に 1 回以上の頻度で見直されます。

## インシデント レスポンス

Dropbox では、次のようなインシデント レスポンス ポリシーと手順を定め、サービスの可用性、完全性、セキュリティ、プライバシー保護、機密性の問題に対応しています。当社には、インシデント レスポンス手順の一環として、専門に訓練を受けたチームが存在します。

- インシデントが疑われる警告に迅速に対応する
- インシデントの重大性を判定する
- 必要に応じて軽減措置や抑制措置を講じる

- 社内外の関係者と連絡を取り合う（違反やインシデントに関する通知を行う契約義務を履行し、関連する法律や規制を遵守するために、影響を受ける顧客に通知することも含む）
- 調査のために証拠を収集し保存する
- 事後の分析結果を文書にまとめ、恒久的なトリアージ計画を策定する

インシデント レスポンスのポリシーと手順は、SOC 2、ISO/IEC 27001、およびその他のセキュリティ評価の一環として監査を受けています。

# インフラストラクチャのセキュリティ

## ネットワーク セキュリティ

Dropbox は、バックエンド ネットワークのセキュリティ維持に懸命に取り組んでいます。ネットワーク セキュリティと監視に関する Dropbox の技術は、複数の階層で保護と防御を提供するように設計されています。Dropbox には、ファイアウォール、ネットワークの脆弱性スキャン、ネットワーク セキュリティの監視、侵入検出システムなど、業界標準の保護技術が導入されており、承認済みで悪意のないトラフィックのみが Dropbox のインフラストラクチャに到達できます。

Dropbox の内部プライベート ネットワークは、用途とリスク レベルに基づいてセグメント化されています。主要なネットワークは次のとおりです。

- インターネット接続 DMZ
- 優先インフラストラクチャ DMZ
- プロダクション ネットワーク
- 企業ネットワーク

Dropbox のプロダクション環境へのアクセスは承認された IP アドレスに限定されており、すべてのエンドポイントで多要素認証が必要です。アクセス許可のある IP アドレスは、Dropbox の企業ネットワークまたは承認された Dropbox 社員と関連付けられています。安全なプロダクション環境を維持するため、承認された IP アドレスは四半期ごとに見直されます。IP アドレス リストを変更するためのアクセスは、承認された担当者のみに限定されています。

インターネットから Dropbox プロダクション ネットワークへのトラフィックは、複数階層のファイアウォールとプロキシによって保護されています。

Dropbox の社内ネットワークと公共のインターネットの間には、厳格な制限が設定されています。プロダクション ネットワークとインターネットの間でやり取りされるトラフィックは、専用プロキシ サービスで入念に管理され、さらに、厳格なファイアウォール ルールによって保護されています。

Dropbox は高度なツール セットを利用して、Mac または Windows のノート パソコンやデスクトップ パソコン、プロダクション システムに有害なイベントが発生していないかどうかを監視しています。セキュリティ ログは、業界標準の保持ポリシーに従って 1 か所に集約され、フォレンジック解析とインシデント レスポンスに役立てられます。

Dropbox では、社内のセキュリティ専任チームとサードパーティのセキュリティ専門家が、ネットワーク セキュリティ テストや監査を定期的に行い、リスクを識別して軽減します。

### ポイント オブ プレゼンス（PoP）

Dropbox では、ユーザーがウェブサイトを利用する際のパフォーマンスを最適化するため、サードパーティのコンテンツ デリバリ ネットワーク（CDN）と、Dropbox が世界中の 31 か所に展開してホストしているポイント オブ プレゼンス（PoP）を活用しています。これらの場所でユーザー データのキャッシュは行われません。また、転送されるすべてのユーザー データは SSL/TLS で暗号化されています。また、Dropbox がホストする PoP への物理的/論理的アクセスは承認された Dropbox 社員のみに制限されています。さらに Dropbox は、トランスポート（TCP）レイヤーとアプリケーション（HTTP）レイヤーの最適化を行っています。

### ピアリング

また、オープン ピアリング ポリシーを採用しており、すべてのお客様からのピアリングを受け入れています。詳細については、dropbox.com/peering をご覧ください。

## 信頼性

優れたストレージ システムには信頼性が不可欠です。Dropbox は幾重もの冗長性を持たせることでデータ紛失を防ぎ、可用性を確保しています。

### ファイル メタデータ

メタデータの冗長コピーは、データ センター内にある独立した複数のデバイスにわたって、少なくとも N+2 の可用性モデルを使用して分散されています。すべてのメタデータに対して、少なくとも 1 時間に 1 回の増分バックアップと 36 時間に 1 回の完全バックアップが行われます。メタデータは、Dropbox がホストし管理する、米国内に置かれたサーバーで保管されます。

### ファイル ブロック

ファイル ブロックの冗長コピーは、2 つ以上の別々の地理的領域で独立して格納され、各領域内で確実に複製されます（**注：**お客様がドイツ、オーストラリア、日本、英国のインフラストラクチャにファイルを保存することを選択した場合、ファイル ブロックはそれぞれの領域内でのみ複製されます。詳細については、後述の「データ センターおよびマネージド サービス プロバイダ」をご覧ください）。Magic Pocket と AWS はいずれも、99.999999999 % 以上の年間データ耐久率を提供するよう設計されています。

Dropbox では、アーキテクチャ、アプリケーション、同期メカニズムが一体となって、ユーザー データの保護と高可用性を実現しています。まれにサービスを利用できない事態が発生しても、Dropbox ユーザーは、リンクしているパソコン上のローカル Dropbox フォルダで最後に同期したファイルのコピーにアクセスできます。ダウンタイム中、停止中、オフライン時は、ユーザーのハード ドライブの Dropbox のデスクトップ クライアントやローカル フォルダで同期済みファイルにアクセスできます。ファイルやフォルダへの変更は、サービスまたは接続が復旧し次第 Dropbox に反映されます。

### Paper ドキュメント

Paper ドキュメントの冗長コピーは、データ センター内にある独立した複数のデバイスにわたって、N+1 の可用性モデルを使用して分散されています。Paper ドキュメントのデータは、完全バックアップも毎日実行されます。Dropbox では、Paper ドキュメントのストレージに、99.999999999 % 以上の年間データ耐久性を提供するよう設計されている、米国に置かれた AWS インフラストラクチャを使用しています。まれにサービスが利用できない事態が発生しても、Dropbox ユーザーは、モバイル アプリケーション内で「オフライン」モードを使用して最後に同期した Paper ドキュメントのコピーにアクセスできます。

### ファイルの同期

Dropbox は、業界で認められた最高水準のファイル同期を提供しています。Dropbox の同期の仕組みにより、高速で応答性に優れたファイル転送が確立され、さまざまなデバイスであらゆる場所からデータにアクセスできます。また、Dropbox の同期は回復性にも優れています。Dropbox サービスとの接続に失敗した場合、接続が再確立され次第、クライアントでの同期処理が再開します。ローカル クライアントのファイルが更新されるのは、Dropbox サービスと完全に同期され、正常に検証された場合のみです。複数のサーバーに負荷を分散することで冗長性を確保し、一貫性の高いファイル同期をエンド ユーザーに保証します。

### 差分同期

この同期方法を使用すると、ファイルの変更された部分だけがダウンロード/アップロードされます。Dropbox はアップロードされた各ファイルを暗号化された個々のブロックとして保管し、変更されたブロックだけを更新します。

### ストリーミング同期

ストリーミング同期では、ファイルのアップロードが完全に終了するのを待つのではなく、1 つ目のデバイスがすべてのブロックのアップロードを完了する前に、2 つ目のデバイスが同期されたブロックのダウンロードを開始します。別々のパソコンが 1 つの Dropbox アカウントにリンクされている場合や、異なる Dropbox アカウントでフォルダを共有している場合、この方法が自動的に採用されます。

### ハード ドライブの容量を節約

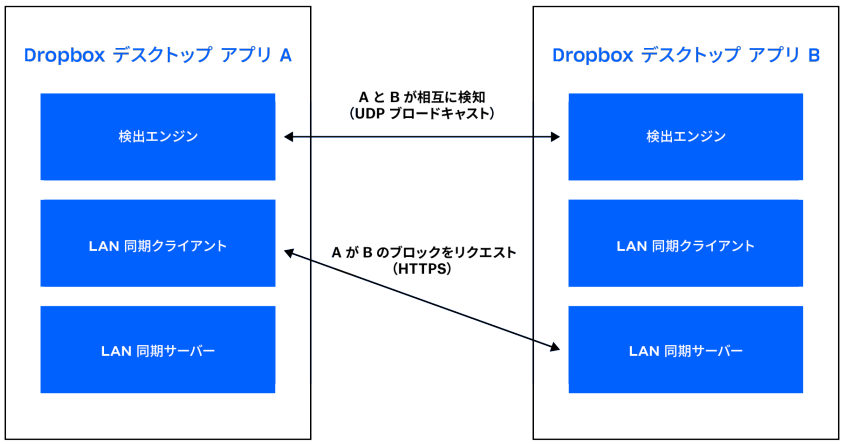
オフラインで使用したいファイルのみをハード ディスクに保存し、それ以外のファイルはすべて「オンラインのみ」として dropbox.com に保存することで、パソコンの空き容量を増やせます。

### LAN 同期

この機能を有効にすると、同じローカル エリア ネットワーク（LAN）上の別のパソコンにある新しいファイルや更新されたファイルがダウンロードされます。そのため、Dropbox サーバーからファイルをダウンロードするのに比べて時間や帯域幅が少なくて済みます。

### アーキテクチャ

LAN 同期システムは、デスクトップ アプリで動作する検出エンジン、サーバー、クライアントという 3 つの主要コンポーネントで構成されます。検出エンジンは、同期対象となるマシンをネットワーク上で見つけます。検出対象となるマシンは、同じ個人 Dropbox フォルダまたは共有 Dropbox フォルダにアクセスすることが承認されているものに限られています。サーバーは、ネットワーク上の他のマシンからのリクエストを処理し、リクエストされたファイル ブロックを提供します。クライアントは、ネットワークに対してファイル ブロックをリクエストします。




**検出エンジン**

LAN に接続されている各マシンは、ポート 17500 上で UDP ブロードキャスト パケットの送信やリッスンを定期的に行います（このポートは LAN 同期用に IANA で予約済み）。このパケットには、そのマシンが使用しているプロトコルのバージョン、対象となる Dropbox の個人/共有フォルダ、サーバーの実行に使用される TCP ポート（ポート 17500 が使用できない場合は別のポート）、およびランダムに生成されたマシンの ID が含まれています。このパケットを受け取ったマシンは、Dropbox の各個人/共有フォルダに対応する同期先のリストに IP アドレスを追加します。

**プロトコル**

実際のファイル ブロックの転送は HTTPS 経由で行われ、各マシンはエンドポイントを備えた HTTPS サーバーを実行します。クライアントは、ブロックが存在するピアを特定するために、複数のピアに対してポーリングを行いますが、ブロックのダウンロード元となるサーバーは 1 つだけです。

ユーザー データの安全を確保するには、認証されたクライアント以外はフォルダに対してブロックをリクエストできないようにする必要があります。また、管理下にないフォルダのデータを配布できないようにする対策も必要です。そのため Dropbox では、個人および共有フォルダごとに SSL キー/証明書ペアを生成しています。このペアは、フォルダに対して認証されたマシンに Dropbox サーバーから配布され、フォルダに参加するメンバーが変更になるたびに更新されます（共有フォルダからメンバーを除外した場合など）。Dropbox の個人/共有フォルダの認証に用いる証明書は、HTTPS 接続の両側で同一でなければなりません。同一の証明書を使用することで、接続の正当性が保証されます。

LAN 同期サーバーに接続する際、クライアントは Server Name Indication（SNI）を用いて接続先をサーバーに通知します。これにより、サーバーは正しい証明書を使用できます。


**サーバー/クライアント**

前述のプロトコルを使用する場合、サーバー側で必要となるのは存在するブロックとその場所の情報だけです。

クライアントはエンジンの検出結果に基づいて、Dropbox の個人/共有フォルダごとに同期先（ピア）のリストを維持します。LAN 同期システムは、ファイル ブロックのダウンロード要求があると、Dropbox の個人/共有フォルダ用に検出されたピアから任意に抽出されたピアにリクエストを送信し、ブロックを所有していると最初に応答したピアのブロックを要求します。

Dropbox では、接続プールを使用して確立済みの接続を再利用することで、遅延を回避しています。接続は必要になったときに初めて確立されますが、一旦確立された接続は再利用に備えて維持されます。また、1 つのピアの接続数には制限があります。

ブロックが見つからない場合や正常にダウンロードされない場合、または接続した結果速度が遅すぎた場合、システムはフォールバックして Dropbox サーバーにブロックを要求します。

## データ センターおよびマネージド サービス プロバイダ

Dropbox の企業システムとプロダクション システムは、米国内のさまざまな地域にあるサードパーティのサブサービス組織のデータ センターおよびマネージド サービス プロバイダに収容されています。セキュリティ制御が十分に行われるように、サブサービス組織のデータ センターの SOC レポートとベンダーのセキュリティ アンケート、および契約上の義務は年に 1 回以上見直されています。これらのサードパーティ サービス プロバイダは、Dropbox のインフラストラクチャと外部との境界における物理、環境、運用に関わるセキュリティの管理を担当しています。Dropbox は、サードパーティのデータ センターに収容されている自社のインフラストラクチャにおける論理、ネットワーク、アプリケーションに関わるセキュリティの管理を担当しています。

Amazon Web Services（AWS）は処理とストレージを扱っているマネージド サービス プロバイダであり、インフラストラクチャを経由して提供している Dropbox サービスの論理的およびネットワーク上のセキュリティの管理を担当しています。接続は AWS のファイアウォールにより保護されており、デフォルトではすべて拒否（deny-all）モードに設定されています。Dropbox は、AWS の環境にアクセス可能な IP アドレスの数や社員数を制限しています。

**ドイツ、オーストラリア、日本、英国のインフラストラクチャ**

条件を満たしたお客様は、米国以外の領域に配置されたストレージにファイル ブロックを保管できます。Dropbox のインフラストラクチャは、ドイツ、オーストラリア、日本、英国の Amazon Web Services（AWS）によってホスティングされており、冗長性の確保とデータ消失防止のため、各領域内で複製されます。ファイルのメタデータは、米国にある Dropbox の専用サーバーに保管されます。Paper ドキュメントとプレビューは、どのお客様のものかに関係なく、すべて米国内に保管されます。

## 事業継続

Dropbox は事業継続マネジメント システム（BCMS）を確立しており、ビジネスに不可欠のプロセスやアクティビティが中断した場合でも、ユーザーに対するサービスの提供を再開または継続する方策を立て、さらに企業として機能する方法も講じています。この計画に基づき、Dropbox では次の段階で構成されるプロセスを周期的に実施します。

- **ビジネスへの影響とリスクの評価**

  Dropbox は 1 年に 1 回以上の頻度でビジネスへの影響評価（BIA）を実施し、Dropbox に不可欠なプロセスの特定、サービス停止による潜在的な影響の評価、優先的な復旧スケジュールの設定、重要度の非常に高い依存関係およびサプライヤの特定を行います。また、全社的なリスク評価も年 1 回以上行っています。このリスク評価を行うことで、Dropbox に対する破壊的な事象が生じた場合のリスクを体系的に特定し、分析、評価することができます。リスク評価と BIA を併せて実施することで、サービス継続の優先順位を認識し、事業継続計画（BCP）における影響軽減と復旧のための戦略を立てることができます。

- **事業継続計画**

  BIA によって Dropbox のサービス継続に不可欠であると特定されたチームは、この情報に基づいて、不可欠なプロセスに関するビジネス継続計画を立案します。この計画を立てることで、緊急時にプロセスを再開させる責任が誰にあるかを把握し、サービス停止時に Dropbox のどのオフィスまたは事業拠点がプロセスを引き継ぐことができるかを特定し、継続性に関する事案が発生したときにどのような方法で連絡を取るべきかを確認できます。また、復旧プランやその他の重要な情報（プランの適用時期および方法、連絡先やミーティングに関する情報、重要なアプリ、復旧戦略など）を一元的に管理することで、障害のインシデントに備えることができます。Dropbox のビジネス継続プランは全社的な危機管理計画（CMP）に結び付いており、その計画に基づいて Dropbox の危機管理およびインシデント対応チームが設立されています。

- **計画のテスト/演習**

  Dropbox では、事業継続計画の中からいくつかの項目を選んで、少なくとも年に 1 回テストしています。テストは BCMS の適用範囲と目標に従って行われ、適切なシナリオを元に、明確に定義された目的に応じて適切に設計されます。テストの対象範囲は、机上での演習から実際のインシデントに関する本格的なシミュレーションまで多岐にわたります。チームは、テスト結果と実際のインシデントの経験に基づいて、問題への対応計画を更新し改善して、チームの対応力を高めます。

- **BCMS の見直しと承認**

  Dropbox のエグゼクティブ スタッフは、信頼プログラムの見直しの一環として、BCMS を少なくとも年に 1 回見直します。

## ディザスター リカバリ

重大な危機や災害によって Dropbox Business の運用に影響があった場合に情報セキュリティ要件に対応するため、Dropbox ではディザスター リカバリ計画を設けています。Dropbox の技術チームはこの計画を毎年見直し、いくつかの項目を選んで、少なくとも年に 1 回テストしています。テスト結果は文書化され、解決されるまで追跡されます。

Dropbox のディザスター リカバリ計画（DRP）は、耐久性に関わる災害と可用性に関わる災害のどちらにも対応しています。これらの災害は次のように定義されます。

- 耐久性に関する災害とは、次のような問題が発生するもののことです。
  - メタデータを保管するプライマリ データ センターまたはファイル ブロックを保管する複数のデータ センターの完全な（または永続的な）損失
  - メタデータを保管するデータ センターから、またはファイル コンテンツを保管する複数のデータ センターからの通信機能またはデータ提供機能の損失

- 可用性に関する災害とは、次のような問題が発生するもののことです。
  - 10 日間を超える停電
  - メタデータを保管するストレージ サービス/データ センターから、またはファイル ブロックを保管する複数のストレージ サービス/データ センターからの通信機能またはデータ提供機能の損失

Dropbox では、目標復旧時間（RTO）と目標復旧時点（RPO）を定めています。RTO とは、災害後のビジネス プロセスやサービスの復旧にかかる時間とサービス レベルのことで、RPO とは、サービスの停止によるデータ損失が許容される最長期間のことです。また、Dropbox では、年に 1 回以上実施しているディザスター リカバリ テストの間に、実際の復旧時間（RTA）も測定しています。

Dropbox のインシデント レスポンス、事業継続、ディザスター リカバリの計画は、一定期間ごとに、および組織や環境に大きな変化があったときにテストを受けるように定められています。

# アプリケーションのセキュリティ

## Dropbox ユーザー インターフェース

Dropbox サービスには多数のインターフェースからアクセスできます。各インターフェースは、ユーザー データに簡単にアクセスできるだけではなく、データを処理し保護するうえでのセキュリティ設定やセキュリティ機能を個別に備えています。

- **ウェブ**
  ウェブ インターフェースには、すべての最新ウェブ ブラウザからアクセスできます。ファイルのアップロード、ダウンロード、閲覧、共有が可能で、パソコンのローカルにある既存のファイルをデフォルト アプリケーションで開くこともできます。

- **デスクトップ**
  Dropbox デスクトップ アプリケーションはパワフルな同期クライアントで、同期したファイルはローカルに保存され、オフラインでアクセスできます。デスクトップ アプリケーションから Dropbox アカウントに制限なくアクセスできます。また、Windows や Mac に対応しており、各 OS のファイル ブラウザからファイルを直接閲覧し、共有できます。

- **モバイル**
  Dropbox アプリは、iOS や Android デバイスに対応しているので、外出先でもすべてのファイルにアクセスできます。また、モバイル アプリでは、ファイルをオフラインでアクセス可能にすることもできます。

- **API**
  Dropbox API を使用すると、Dropbox ユーザー アカウントの読み取り/書き込みや、ファイルの検索、改訂、復元などの高度な機能へのアクセスを柔軟な方法で行うことができます。また、Dropbox Business アカウントのユーザーに関するあらゆる管理作業を API 経由で行うことができ、チームのメンバー全員に対するアクションを実行したり、Dropbox Business の管理機能へのアクセスを有効化したりすることも可能です。

## Paper ユーザー インターフェース

Paper サービスには多数のインターフェースからアクセスできます。各インターフェースは、ユーザー データに簡単にアクセスできるだけではなく、データを処理し保護する上でのセキュリティ設定やセキュリティ機能を個別に備えています。

- **ウェブ**
  ウェブ インターフェースには、すべての最新ウェブ ブラウザからアクセスできます。Paper ドキュメントの作成、表示、編集、ダウンロード、共有が可能です。

- **モバイル**
  Paper モバイル アプリは、iOS および Android のモバイル デバイスやタブレットで利用でき、外出先でもあらゆる Paper ドキュメントにアクセスできます。モバイル アプリは、内部の WebView ブラウザをラップする（iOS や Android の）ネイティブ コードから構成されるハイブリッド アプリとして作成されています。

- **API**

  上記で説明した Dropbox API には、権限の管理、アーカイブ、完全削除などの機能のサポートを含む、Dropbox Paper 内のドキュメントとフォルダを管理するエンドポイントとデータ型が含まれています。

## 暗号化

### 転送中のデータ

転送中のデータを保護するために、Dropbox アプリと Dropbox サーバーとの間で行われる転送では、128 ビット以上の AES 暗号化で保護されている安全な SSL/TLS トンネルが使用されます。Dropbox クライアント（デスクトップ/モバイル/API/ウェブ）とホストされているサービスとの間で転送されるファイル データは SSL/TLS で暗号化されます。同様に、Paper クライアント（現状ではモバイル/API/ウェブ）とホストされているサービスとの間で転送中の Paper ドキュメントのデータは、SSL/TLS で暗号化されます。Dropbox が管理するエンドポイント（デスクトップ/モバイル）と最新バージョンのウェブ ブラウザでは、強力な暗号化を使用し、前方秘匿性（Perfect Forward Secrecy）と証明書ピンニングをサポートしています。さらに、ウェブ上ではすべての認証クッキーに「安全」とフラグを付け、includeSubDomains パラメータ付きで HSTS（HTTP Strict Transport Security）を有効にしています。

**注：** Dropbox では TLS のみを使用しています。SSLv3 には脆弱性があることが知られているため、使用を取りやめていますが、TLS は慣習的に「SSL/TLS」と呼ばれているため、ここではこの表記を使用しています。

中間者攻撃を防止するため、Dropbox のフロントエンド サーバーの認証は、クライアントが保持する公開証明書を使用して行われます。ファイル転送前に暗号化接続がネゴシエートされ、この接続によって Dropbox のフロントエンド サーバーにファイルや Paper ドキュメントが安全に転送されます。

### 保存データ

ユーザーによって Dropbox にアップロードされたファイルは、256 ビットの Advanced Encryption Standard（AES）によって暗号化して保存されます。ファイルは個々のファイル ブロックに分割され、複数のデータ センターに格納されます。各ブロックは断片化され、強力な暗号によって暗号化されます。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。Dropbox に保管されているファイルも同様に、256 ビットの Advanced Encryption Standard（AES）によって暗号化されます。Paper ドキュメントは、サード パーティのシステムを使用して複数のアベイラビリティゾーンに保管されます。

### キーの管理

Dropbox のキー管理インフラストラクチャは、操作、技術、手順におけるセキュリティ管理を意図して設計されており、キーへの直接アクセスが必要最小限に抑えられています。暗号化キーの生成、交換、保管の処理は分散して行われます。

- **ファイル暗号化キー**

  Dropbox はユーザーに代わってファイル暗号化鍵を管理するように設計されており、複雑さを排除しつつ高度なサービス機能と強力な暗号化制御を実現しています。ファイル暗号化鍵は、プロダクション システム インフラストラクチャのセキュリティ管理とセキュリティ ポリシーに従って作成、保管、保護が行われます。

- **内部 SSH キー**

  プロダクション システムへのアクセスは、一意の SSH キー ペアで制限されており、SSH キーを保護するためのセキュリティ ポリシーと手順が定められています。公開鍵の交換プロセスのセキュリティは内部システムで管理され、秘密鍵は安全に保管されています。内部の SSH キーは、別個の二要素認証なしでは、プロダクション システムへのアクセスには使用できません。

- **キーの配布**

  Dropbox は扱いに注意を要するキーの管理と配布を自動化しており、操作に必要なシステムにキーを配布します。

### 証明書ピンニング

Dropbox は、HTTP 公開鍵ピンニング仕様をサポートしている最新のブラウザと、デスクトップやモバイルのクライアントで証明書ピンニングを実行します。証明書ピンニングは、接続先のサービスが意図したものであってなりすましではないことを確認するための追加のチェック機能です。また、巧妙なハッカーがユーザー アクティビティを監視するために用いるさまざまな方法からユーザーを守るためにも、証明書ピンニングを使用しています。

### 認証データの保護

Dropbox では、ユーザーのログイン認証情報を保護するために、通常のハッシュ化では行われない保護対策を講じています。Dropbox は業界のベスト プラクティスに従い、ランダムに生成されたユーザー固有のソルトを付与して各パスワードをソルト化するとともに、このハッシュ化を繰り返して処理に時間を要するようにしています。この手法は、ブルート フォース（総当たり）攻撃や辞書攻撃、レインボー攻撃などからの保護に役立ちます。さらに追加の予防措置として、データベースとは別の場所に保管されるキーによってハッシュ値を暗号化しています。これにより、データベースのみが侵害された場合にパスワードの安全を確保できます。

### マルウェア スキャン

Dropbox は、コンテンツが発信元のユーザー アカウントから外部に共有されるタイミングでマルウェアを自動的にスキャンするシステムを開発しました。このシステムは、Dropbox 独自のテクノロジーと業界標準の検出エンジンを活用し、マルウェアの拡散を阻止するよう設計されています。

## 製品のセキュリティ

Dropbox は IT 担当者とエンド ユーザーがデータを効果的に管理し保護できるよう、制御機能と可視性機能を備えています。Dropbox なら、仕事に必要なすべてのツール、コンテンツ、共同作業の場を 1 か所に集約できます。Dropbox が提供するのは安全なストレージだけではありません。これまでのワークフローを最適化する、スマートでスムーズな方法を提供します。

ここでは、管理者とユーザーが利用できる機能と、主要な IT プロセスを管理するためのサードパーティ製品との連携の例を紹介します。

**注：**使用できる機能は加入プランによって異なります。詳細については、dropbox.com/business/plans をご覧ください。

## コンテンツの管理

知的財産（IP）や個人を特定可能な情報（PII）といった機密性の高いビジネス資産を保護することは、IT チームとデータ セキュリティ チームにとっての最重要課題です。コンテンツの詳細な権限設定、データ保持ポリシー、そして法的ホールドにいたるまで、Dropbox は業界最先端のソリューションを使用してお客様のコンテンツを管理、監視、保護しています。以下に、コンテンツ管理をサポートする主要な Dropbox 製品と機能を紹介します。

### コンテンツおよび共有ファイルや共有フォルダに対する詳細な権限

- **共有ファイルの権限**

  共有ファイルを所有するチーム メンバーは、特定ユーザーのアクセス権の削除や、ファイルへのコメント機能の無効化を行えます。

- **共有ファイルの権限**

  共有フォルダを所有するチーム メンバーは、特定ユーザーのフォルダへのアクセス権の削除、特定ユーザーの閲覧/編集権限の変更、フォルダの所有権の移行を実行できます。また、各共有フォルダの所有者は、チームのグローバル共有権限に応じて、チーム外のユーザーとの共有、編集権限を持つ他のユーザーによるメンバーシップの管理、フォルダ メンバー以外のユーザーとのリンクの共有に関する権限を有効化または無効化することもできます。

- **共有リンクのパスワード**

  共有リンクは、所有者が指定したパスワードで保護できます。ファイルまたはフォルダのデータが転送される前に、アクセス管理レイヤーにより、正しいパスワードが送信されており、他のすべての要件（チーム、グループ、フォルダの ACL など）が満たされていることが検証されます。検証されると、ユーザーのブラウザにセキュアな cookie が保存され、パスワードが検証済みであることが記憶されます。チーム管理者は共有管理機能を使うことで、デフォルトのパスワードを設定することもできます。この場合、パスワードをオプションにしたときよりも、チームのコンテンツに対する保護を強化できます。

- **共有リンクの有効期限**

  共有リンクに有効期限を設定して、ファイルやフォルダへのアクセスを一時的に許可できます。チーム管理者は共有管理機能を使うことで、デフォルトの有効期限を設定することもできます。この場合、有効期限をオプションにしたときよりも、チームのコンテンツに対する保護を強化できます。

### Paper ドキュメントと共有 Paper フォルダの権限

- **Paper ドキュメントと共有 Paper フォルダの権限**

  Paper ドキュメントや共有 Paper フォルダを所有しているチーム メンバーは、特定のユーザーのアクセス権の削除や、Paper ドキュメントの編集機能の無効化が行えます。

- **Paper ドキュメントの権限**

  Paper ドキュメントを所有しているチーム メンバーは、共有パネルに記載されている特定のユーザーのアクセス権を削除できます。Paper ドキュメントの所有者と編集者はどちらも、特定のユーザーの表示/編集権限の

変更が可能で、ドキュメントのリンク ポリシーも同様に変更できます。リンク ポリシーは、ドキュメントを開くことのできるユーザーと付与される権限を制御するものです。チーム管理者は、リンクとドキュメントの共有のポリシーをチーム規模で設定できます。

- **Paper フォルダの権限**

  フォルダ メンバーになっているチーム メンバーは、フォルダの共有ポリシーを変更でき、フォルダに明示的に追加された特定のユーザーのアクセス権を削除できます。

**ファイルとフォルダのアクション**

- **ファイル用チーム フォルダ**

  管理者はチーム フォルダを作成することができます。このフォルダによって、グループや他の共同作業者に必要なコンテンツへの適切なアクセス レベル（表示または編集）が自動的に付与されます。

- **アクセスと共有の詳細な管理機能**

  管理者は共有管理機能を使用して、トップ レベルやサブフォルダ レベルでメンバーシップや権限を管理し、社内外のメンバーやグループに対して、特定のフォルダのみへのアクセス権を与えることができます。

- **チーム フォルダ マネージャー**

  管理者は、すべてのチーム フォルダの表示や共有ポリシーのカスタマイズを単一のツールで行うことができるので、機密資料を誤って共有してしまうといったトラブルを防ぐことができます。

- **Paper ドキュメント用共有フォルダ**

  管理者は共有 Paper フォルダを作成でき、このフォルダによって他の共同作業者に必要なコンテンツへの適切なアクセス レベル（コメント付記または編集）が自動的に付与されます。

- **遠隔削除**

  社員がチームから外れた場合やデバイスを紛失した場合、管理者は Dropbox のデータとファイルのローカル コピーを遠隔削除できます。デバイスがオンラインに接続され、Dropbox アプリケーションが起動すると、パソコンとモバイル デバイスの両方からファイルが削除されます。

- **アカウント移行**

  管理者は、ユーザーのプロビジョニングを（手動またはディレクトリ サービスを通じて）取り消した後で、以前のチーム メンバーによって作成された Paper ドキュメントのファイルと所有権をそのユーザーのアカウントから他のチーム メンバーに移行できます。アカウント移行機能は、ユーザーを削除しているときだけではなく、ユーザー アカウントを削除した後でもいつでも利用できます。

以下の機能は、アドオンとして利用可能です（詳細はセールス担当までお問い合わせください）。

- **コンテンツのスキャン**

  アドオン機能の Advanced Team & Content Controls（チームとコンテンツの高度な管理）を追加することで、Dropbox Business Advanced と Enterprise のお客様は、Dropbox 内の新規および既存のコンテンツをスキャンし、データの脆弱性を発見および防止できます。

- **カスタマイズしたワークフローの設定とトリガー**

  Advanced Team & Content Controls アドオンを使用すると、管理者は、企業ポリシーに違反するファイルに対してカスタマイズ可能なアクションを実施できます。

- **アラートの設定**

  管理者は、セキュリティ上の問題をリアルタイムで監視し、データの脆弱性を未然に防ぐことができます。ファイルが外部に共有されたときや、機密性の高いデータがスキャンされたときに、アラートを受け取ることができます。

## コンテンツの可視性

### セキュリティに関するアラートと通知

Dropbox Enterprise の管理者は、不正なアクティビティやリスクのあるアクティビティ、データ漏洩の可能性が自分のアカウントで検知されたときにリアルタイムで通知を受け取ることができます。以下のイベントを監視できます。

- 一括削除
- データの一括移動
- 機密性の高いコンテンツの外部との共有
- チーム外からのマルウェアの共有
- チーム内でのマルウェアの共有
- 上限を超える回数のログイン失敗
- リスクが高い国からのログイン
- ランサムウェアの検出

アラートのしきい値や通知の受信者の設定、機密性の高いファイルを含むフォルダが外部と共有された場合のアラート送信が可能です。また管理者は、「進行中」、「解決済み」、「却下済み」というマークをアラートに設定することもできます。ダッシュボード ウィジェットを使えば、チーム全体のアラート状況や過去 1 週間の傾向を見ることも可能です。

### 外部との共有に関するレポートとページ

Dropbox では、外部との共有に関するレポートとページを使って、外部共有の状況を詳しく把握できます。管理者は、［インサイト］ページまたは［外部との共有］ページからレポートを作成できます。レポートでは、外部と共有されたチームのファイルおよびフォルダと共有リンクのすべてを確認できます。［外部との共有］ページは管理コンソールに追加されたページで、チーム外と直接共有されたファイルおよびフォルダと共有リンクを、ファイル形式、共有相手、リンク設定などの条件でフィルタリングして参照できます。

### 共有の管理

チーム管理者は共有設定を使用して、チーム コンテンツの共有とアクセスをきめ細かく管理できます。管理者は、有効期限とパスワードのデフォルトをチームレベルで設定できます。これらの設定を行うと、有効期限やパスワードの設定をユーザーに依存せずに済むようになるため、情報漏洩のリスクが軽減されます。

### データ分類

Dropbox Enterprise のチームは、個人データや機密データに自動でラベルを付けることで、情報漏洩リスクを軽減できます。機密性の高い情報を含む、チーム フォルダ内のファイルやフォルダがチーム外に共有された場合、管理者は、情報漏洩防止（DLP）のアラートをメールと管理コンソールで受け取ることができます。また管理者は、共有フォルダやチーム メンバーの個人フォルダに保存された機密性の高いデータを自動で検出し、機密情報として分類できます。自動データ分類は、管理コンソールから有効にできます。

### データ ガバナンスのアドオン

データ ガバナンスとは、プロセス、テクノロジー、チームの全体が一体となって組織のデータ資産を管理、保護することをいいます。データ ガバナンスを実現するためには、企業のデータを保存し、必要に応じて特定、発見、取得できることが必要です。

Dropbox データ ガバナンス アドオンには、組織が保有するデータの管理と保護を強化しつつ、規制準拠やコンプライアンス対策に伴うリスクとコストを低減するための機能がまとめられています。現在、このアドオンには、チーム管理者とコンプライアンス管理者のための 4 つの主要機能が含まれています。

- **エクステンデッド バージョン履歴**
  デフォルトのファイルのバージョン履歴は、Dropbox アカウントの種類によって異なります。Dropbox Business では、エクステンデッド バージョン履歴（EVH）のアドオンを個別に購入するか、データ ガバナンス アドオンのバンドルの一部として購入すると、削除または変更されたファイルの復元を過去 10 年までさかのぼって行えます。

- **法的ホールド**
  あるチーム メンバーに法的ホールドを設定することで、チーム管理者とコンプライアンス管理者はそのメンバーが作成や変更を行ったすべてのコンテンツを確認し、エクスポートできます。法的ホールドの対象となったメンバーに、法的ホールドの対象となっていることは通知されません。また、ファイルの作成、編集、削除を行う権限は引き続き維持されます。

- **データ保持**
  データ保持機能を使用すると、チーム管理者とコンプライアンス管理者は、規制により一定期間の保持が義務付けられているコンテンツが誤って削除されることを防止できます。この機能では、最終更新日から 10 年間にわたってデータを保持できます。

- **データ処理機能**
  データ処理機能を使用すると、チーム管理者とコンプライアンス管理者は、データ保持と破棄の要件に従って、指定した日にデータを完全に削除できます。管理者は、今後のファイル削除日を通知するレポートでアクティビティを監視できます。

### 復元とバージョン管理

Dropbox Business では、削除されたファイルを復元でき、ファイルと Paper ドキュメントの過去のバージョンを回復できます。その際、重要なデータへの変更を追跡して、任意の時点のファイルを取得することができます。

### モバイル デバイスでのデータ セキュリティ

- **データ消去**

  セキュリティ強化のため、パスコードの入力に 10 回失敗した場合はデバイスから Dropbox データをすべて消去できるオプションがあります。

- **内部ストレージとオフライン ファイル**

  デフォルト設定では、ファイルはモバイル デバイスの内部ストレージに保存されません。Dropbox のモバイル クライアント機能を使うと、個々のファイルやフォルダを保存することで、オフライン状態でもそのデバイスから閲覧可能になります。モバイル インターフェースまたはウェブ インターフェースから Dropbox アカウントとデバイスのリンクを解除すると、ファイルやフォルダはそのデバイスの内部ストレージから自動的に削除されます。

- **オフライン Paper ドキュメント**

  Dropbox アカウントのセキュリティのページで、デバイスと Paper のリンクを解除すると、ユーザーはログアウトされ、オフライン Paper ドキュメントは自動的にデバイスの内部ストレージから削除されます。

## チームの管理機能

組織のニーズは同じではありません。Dropbox では、組織の管理者が Dropbox Business をカスタマイズしてチーム独自のニーズを満たせるように、数多くのツールを開発しています。Dropbox Business には、エンド ユーザーがアカウントやデータを保護するためのツールが用意されています。Dropbox のさまざまなユーザー インターフェースから、以下の認証、復元、ログ記録、その他のセキュリティ機能を利用できます。

Dropbox Business の管理コンソールから利用できる管理機能や可視性機能には、次のようなものがあります。

### コンテンツの詳細な権限

- **管理者階層**

  Dropbox では、管理者階層を導入することで、より効果的なチーム管理を実現しています。アカウント管理者には 3 つのアクセス レベルのいずれかが割り当て可能です。チーム内の管理者数には上限はなく、どのチーム メンバーにも管理者の役割を割り当てることができます。

- **チーム管理者**

  チーム全体のセキュリティ権限と共有権限の設定、管理者の作成、メンバーの管理を行うことができます。チーム管理者は、利用可能なすべての管理権限を持ちます。管理者の役割の割り当てや変更が行えるのはチーム管理者のみです。Dropbox Business アカウントには 1 名以上のチーム管理者が必要です。

- **ユーザー管理者**

  チーム メンバーの追加や削除、グループの管理、チームのアクティビティ フィードの閲覧など、チーム管理に関連するタスクのほとんどを実行できます。

- **サポート管理者**

  削除したファイルの復元、2 段階認証でロックアウトされたチーム メンバーに対するサポートなど、チーム メンバーから寄せられる一般的なサービス リクエストに対応できます。また、管理者以外のパスワードのリセットや、特定チーム メンバーのアクティビティ ログのエクスポートも行えます。

- **お支払い管理者**

  管理コンソールの［お支払い］ページにアクセスできます。

- **コンテンツ管理者**

  コンテンツ マネージャーでチーム フォルダを作成、管理できます。

- **レポート管理者**

  管理コンソールでレポートを作成でき、［アクティビティ］ページにアクセスできます。

- **セキュリティ管理者**

  セキュリティ アラート、外部共有、セキュリティ リスクを管理できます。

- **コンプライアンス管理者（データ ガバナンス アドオンを導入しているチームのみ）**

  ［データ ガバナンス］の各ページ（法的ホールド、データ保持、データ処理機能）を管理でき、コンテンツ マネージャーにもアクセスできます。

- **グループ**

  チームは Dropbox のメンバーをグループに分けてリストで管理し、特定のフォルダへのアクセス権を簡単に付与できます。Dropbox では、Active Directory Connector を使用して Active Directory グループを同期することもできます。

- **企業管理グループ**

  この種類のグループのメンバーシップを作成、削除、および管理できるのは管理者のみです。ユーザーは、企業管理グループへの参加または企業管理グループからの退会をリクエストすることはできません。

- **ユーザー管理グループ**

  管理者はユーザーにグループの作成と管理の権限を付与するかどうかを選択できます。また、いつでもユーザー管理のグループを企業管理のグループに変更して、自分の管理下に置くことができます。

- **パソコン上での複数アカウントの使用制限**

  管理者は、チーム メンバーが仕事用の Dropbox アカウントをリンクしているパソコンに別の Dropbox アカウントをリンクできないようにすることが可能です。

- **ユーザーの使用停止**

  管理者は、企業の情報を守るために、ユーザーのデータと共有関係を保持したまま、ユーザーがアカウントにアクセスできないようにすることができます。管理者は、このアカウントは後で再度アクティブにすることも、削除することも可能です。

- **ユーザーの代理ログイン**

  チーム管理者は、チーム メンバーの代理としてログインすることができます。この方法でログインすると、管理者はチーム メンバーのアカウントに保存されているファイルやフォルダ、Paper ドキュメントに直接アクセスして、ファイルやフォルダを変更したり、チーム メンバーの代わりに共有したり、ファイルレベルのイベントに関する監査を実行したりできます。「ユーザーの代理ログイン」イベントはチームのアクティビティ ログに記録され、このイベントをメンバーに通知するかどうかは管理者が決定できます。

- **共有権限**

  チーム管理者は、チームが Dropbox を使用して次のような共有ができるかどうかを包括的に管理できます。

  - チーム メンバーがチーム外のユーザーとファイルやフォルダを共有できるかどうか
  - チーム メンバーがチーム外のメンバーの所有するフォルダを編集できるかどうか
  - チーム メンバーが作成した共有リンクをチーム外のユーザーが使用できるかどうか
  - チーム メンバーがファイル リクエストを作成して、チーム メンバーまたはチーム外のユーザー（もしくはその両方）からファイルを収集できるかどうか
  - ユーザーがチームの所有するファイルを参照し、コメントを追加できるかどうか
  - チーム メンバーがチーム外のユーザーと Paper ドキュメントや Paper フォルダを共有できるかどうか
  - 完全に削除する権限を付与するかどうか

Dropbox Business アカウントのチーム管理者 は、ファイルおよび Paper ドキュメントを完全に削除する機能をチーム管理者のみに制限できます。

### オンボーディングとユーザー プロビジョニング

#### ユーザー プロビジョニングと ID の管理方法

- **メールによる招待**

  Dropbox Business の管理コンソールには、管理者が招待メールを手動で送信できるツールがあります。

- **Active Directory**

  Dropbox Business の管理者は、Dropbox の Active Directory Connector またはサードパーティ アイデンティティ プロバイダを通じて、既存の Active Directory システムからアカウントを自動で作成し、削除できます。この機能と連携すると、Active Directory を使用してメンバーシップを管理できます。

- **シングル サインオン（SSO）**

Dropbox Business では、1 つのアイデンティティ プロバイダにログインすることでチーム メンバーによる Dropbox へのアクセスが許可されるように設定できます。Dropbox の SSO 実装では業界標準の Security Assertion Markup Language 2.0（SAML 2.0）を使用しています。信頼性の高いアイデンティティ プロバイダが認証を管理しており、チーム メンバーは別のパスワードを使わなくても Dropbox にアクセスできるため、プロビジョニングがよりシンプルかつ安全になります。Dropbox は主要なアイデンティティ管理プロバイダとも連携し

ており、ユーザーのプロビジョニングとその解除を自動で行うことができます。後述の「Dropbox Business API インテグレーション」のセクションをご覧ください。

- **API**
  お客様は Dropbox Business API を使用して、ユーザー プロビジョニングとアイデンティティ管理のためのカスタム ソリューションを構築することができます。後述の「Dropbox Business API インテグレーション」セクションをご覧ください。

**2 段階認証**

ユーザーの Dropbox アカウントの保護を強化するためのセキュリティ機能です。Dropbox では本機能の利用を推奨しています。2 段階認証を有効にすると、ログインする際、または新しいパソコン、スマートフォン、タブレットをアカウントにリンクする際に、通常のパスワード以外に 6 桁のセキュリティ コードが必要になります。

- 管理者は、チーム メンバー全員または特定のメンバーに限って、2 段階認証を必須にすることができます。
- アカウント管理者は、どのチーム メンバーに対して 2 段階認証が有効になっているか追跡できます。
- Dropbox の 2 段階認証コードは、テキスト メッセージで受信するか、Time-based One-Time Password（TOTP）アルゴリズム標準に対応するアプリで取得できます。
- これらの方法でセキュリティ コードを取得できない場合は、1 回限り有効な緊急バックアップ コード（16 桁）を使用することもできます。また、予備の電話番号を使用して、テキスト メッセージでバックアップ コードを受信することもできます。
- Dropbox は、オープン スタンダードの FIDO Universal 2nd Factor（U2F）にも対応しています。この標準に準拠することで、6 桁のコードではなく USB セキュリティ キーをセットアップして認証を受けることができます。

**エンタープライズ インストーラー**

管理者には、企業の規模に合わせたプロビジョニングが必要となる場合があります。Windows 版エンタープライズ インストーラーを使用すれば、マネージド ソフトウェア ソリューションや導入メカニズムを通じて、離れた場所から Dropbox デスクトップ クライアントをサイレント インストールできます。

**管理対象デバイスとログイン**

- **エンタープライズ モビリティ管理（EMM）**
  Dropbox はサードパーティ EMM プロバイダと連携しているため、Enterprise プランの Dropbox Business の管理者は、チーム メンバーがモバイル デバイスで Dropbox を利用する方法について、より詳細に管理できます。管理者は Dropbox Enterprise アカウントによるモバイル アプリの利用を管理対象デバイス（会社提供または個人所有）に制限でき、アプリの使用状況（使用可能なストレージやアクセス場所など）をより詳細に参照できます。また、紛失したデバイスや盗難に遭ったデバイスのデータを遠隔で削除することができます。Paper モバイル アプリは、EMM で管理できないことに注意してください。

- **デバイスの承認**
  Dropbox では、Advanced プランおよび Enterprise プランの Dropbox Education および Dropbox Business の管理者は、1 人のユーザーが Dropbox と同期できるデバイスの数を制限し、承認の管理をユーザーが行うか管理者が行うかを選択することができます。また、デバイスの数が制限されないユーザーの例外リストを作成することもできます。Paper モバイル アプリは、デバイス承認に含まれていないことに注意してください。

- **2 段階認証の使用**

  管理者は、チーム メンバー全員または特定のメンバーのみに、2 段階認証を必須にすることができます。チームで SSO 実装することで、その他の多要素認証の要件を定めることもできます。

- **パスワード管理**

  Education、Advanced および Enterprise チームの管理者はメンバーに対して、アカウントのパスワードに強力で複雑なものを使用するよう強制できます。この機能を有効にすると、チーム メンバーはウェブ セッションからログアウトされ、ログイン時に新しいパスワードを作成するように要求されます。組み込みツールによって、一般的に使用される単語、名前、パターン、および番号のデータベースとパスワードが比較され、その強度が分析されます。よく使用される一般的なパスワードを入力したユーザーに対しては、より一般的でなく推測が困難なものにすることを求めるメッセージが表示されます。管理者はチーム全体またはメンバーごとにパスワードをリセットできます。

- **ドメイン管理**

  Dropbox には、企業がユーザーのオンボーディング処理と Dropbox の使用状況の管理を簡単にして、作業をスピーディにするためのツールがいくつか用意されています。

  - **ドメイン認証**
    企業は、自社のドメインの所有権を要求したり、他のドメイン管理ツールを使用することができます。

  - **移行指示**
    管理者は、会社の Dropbox チームに招待された個人ユーザーに対して、チームのアカウントに移行するか、個人用アカウントに指定しているメール アドレスを変更するように要求できます。

  - **ドメイン インサイト**
    管理者は、会社のメール アドレスを個人用 Dropbox アカウントに指定しているユーザーの数など、主な情報を参照することができます。

  - **アカウント キャプチャ**
    管理者は Dropbox ユーザー全員に対して、会社のメール アドレスを使用してチームに参加するか、個人用アカウントに指定しているメール アドレスを変更することを強制できます。

- **ウェブ セッション管理**

  管理者は、チーム メンバーが dropbox.com に対してログイン状態を維持できる期間を制御できます。管理者は、すべてのウェブ セッションまたはアイドル状態のセッションの継続時間を制限できます。上記の制限に達したセッションは自動的にログアウトされます。管理者は、個々のユーザーのウェブ セッションを追跡し、終了することもできます。

- **アプリによるアクセス**

  ユーザーがサードパーティ製アプリを使用してアカウントにアクセスしている場合、管理者はそのアクセスを閲覧でき、無効にすることができます。

- **デバイスのリンク解除**

  管理者は管理コンソールから、ユーザーは個人用アカウントのセキュリティ設定から、ユーザー アカウントにリンクしているパソコンやモバイル デバイスのリンクを解除できます。パソコンのリンクを解除すると認証データが削除され、次回そのパソコンがオンラインになったときに、ファイルのローカル コピーを削除するオプションが表示されます（詳細は以下の「**遠隔削除**」をご覧ください）。モバイル デバイスのリンクを解除した場合は、お気に入りに登録したファイル、キャッシュ データ、ログイン情報が削除されます。また、オフラ

インの Paper ドキュメントも Paper モバイル アプリから削除されます。2 段階認証をオンにしていた場合は、デバイスを再リンクする際にもう一度認証を行う必要があります。また、ユーザーのアカウント設定で、デバイスがリンクされたことを自動的にメールで通知するように設定することもできます。

- **ネットワーク制御**

  Enterprise プランの Dropbox Business の管理者は、Enterprise チームのアカウントだけがお客様の社内ネットワークにある Dropbox を利用できるように制限できます。この機能をお客様の会社のネットワーク セキュリティ プロバイダと連携することで、パソコンの許可されたアカウント以外のすべてのトラフィックをブロックできます。現状では、ネットワーク制御による Paper の管理は行われないことに注意してください。

### モバイル セキュリティ

- **指紋認証**

  Dropbox モバイル アプリのロックを解除する方法として、iOS デバイスの Touch ID や Face ID、Android デバイスの指紋認証（サポートされている場合）を有効にできます。

### アクセスの可視性

- **テクニカル サポートによる ID 確認**

  Dropbox サポートがトラブルシューティングを行うか、アカウント情報を提供する前に、アカウントの管理者は本人であることを証明するため、1 回限り有効でランダムに生成されるセキュリティ コードを提示する必要があります。この PIN は管理コンソールでのみ取得できます。

### ユーザー アカウントのアクティビティ

ユーザーはアカウント設定から以下のページにアクセスして、自分のアカウントのアクティビティに関する最新情報を取得できます。

- **共有ページ**

  このページには、現在ユーザーの Dropbox に含まれている共有フォルダと、ユーザーが追加できる共有フォルダが表示されます。また、ユーザーはフォルダとファイルの共有解除と、共有権限の設定を実行できます。

- **ファイル ページ**

  このページには、共有済みのファイルが、共有したユーザーと各ファイルの共有された日と一緒に表示されます。ユーザーはこれらのファイルへのアクセス権を削除することもできます。他のユーザーから共有されている Paper ドキュメントを表示するには、Paper ドキュメントのナビゲーション インターフェースにある［共有中］ページに移動します。

- **リンク ページ**

  このページには、ユーザーが作成したすべてのアクティブな共有リンクとそれぞれの作成日が表示されます。また、他のユーザーが作成した共有リンクもすべて表示されます。ユーザーはリンクの無効化と権限の変更を実行できます。

- **メール通知**

  自分の Dropbox アカウントに新しいデバイスやアプリがリンクされると、すぐにメールで通知されるように設定できます。

### ユーザー アカウントの権限

- **リンク済みのデバイス**

  ユーザー アカウントのセキュリティ設定にある［**デバイス**］セクションに、そのユーザーのアカウントにリンクしているすべてのパソコンやモバイル デバイスのリストが表示されます。各パソコンの名前、IP アドレス、国、最近のアクティビティのおおよその時間も表示されます。ユーザーはリストに含まれる任意のデバイスのリンクを解除できます。その際、次回オンラインになったときにパソコンのファイルを削除するオプションを設定することもできます。

- **アクティブ状態のウェブ セッション**

  ［**セッション**］セクションには、ユーザー アカウントに現在ログインしているすべてのウェブ ブラウザが表示されます。ブラウザごとに、IP アドレス、国、最近のセッションのログイン日時、最近のアクティビティのおおよその時間が表示されます。ユーザー アカウントのセキュリティ設定から、任意のセッションを遠隔操作で終了できます。

- **リンク済みのアプリ**

  ［**リンク済みのアプリ**］には、アカウントへのアクセスが許可されているすべてのサードパーティ製アプリのリストと、各アプリが使用するアクセス タイプが表示されます。ユーザーは、Dropbox にアクセスされないように、アプリの権限を取り消すこともできます。

### アクティビティ フィード

Dropbox Business は、ファイルのアクションをチームのアクティビティ フィードに記録します。このアクティビティ フィードには管理コンソールからアクセスできます。管理者は柔軟に条件を指定してアクティビティ フィードを検索できるので、アカウントやファイル、Paper ドキュメントのアクティビティについて的を絞って調査を行うことができます。たとえば、任意のファイルの完全な履歴を表示してそのファイルや Paper ドキュメントに対するユーザーの操作を検証することも、期間を指定してチームのアクティビティをすべて表示することもできます。アクティビティ フィードは、ダウンロード可能なレポートを CSV 形式でエクスポートすることも、サードパーティのパートナー ソリューションを通じて SIEM（セキュリティ情報/イベント管理）製品やその他の分析ツールに直接統合することもできます。アクティビティ フィードには、次のコンテンツ イベントが記録されます。

- **ファイル、フォルダ、リンクの共有**

  該当する場合、アクションにチーム外部のユーザーが関与したかどうかがレポートに明示されます。

  **共有ファイル**

  - チーム メンバーまたはチーム外のメンバーの追加/削除
  - チーム メンバーまたはチーム外のメンバーが持つ権限の変更
  - グループの追加/削除
  - ユーザーの Dropbox に対する共有ファイルの追加
  - ファイルまたはフォルダへの招待を通じて共有されたファイルのコンテンツの閲覧
  - ユーザーの Dropbox に対する共有コンテンツのコピー
  - 共有コンテンツのダウンロード
  - ファイルへのコメント

- コメントの解決/解決の取り消し
- コメントの削除
- コメント通知機能の設定/解除
- チームが所有するファイルへの招待の請求
- チームが所有するファイルへのアクセス権のリクエスト
- ファイルの共有解除

**共有フォルダ**

- 新しい共有フォルダの作成
- チーム メンバー、チーム外のメンバー、またはグループの追加/削除
- ユーザーの Dropbox に対する共有フォルダの追加、またはユーザー自身による共有フォルダ アクセス権の削除
- リンクによる共有フォルダの追加
- チーム メンバーまたはチーム外のメンバーの権限の変更
- 別のユーザーへのフォルダ所有権の移行
- フォルダの共有解除
- 共有フォルダへのメンバーシップの要求
- 共有フォルダへのアクセス権のリクエスト
- リクエストしているユーザーの共有フォルダへの追加
- チーム外のメンバーをフォルダへ追加する操作のブロック/ブロック解除
- フォルダへのユーザーの追加をすべてのチーム メンバーに許可するか、所有者のみに許可するかの選択
- 共有フォルダへのグループ アクセス権の変更

**共有リンク**

- リンクの作成または削除
- リンク先のコンテンツの閲覧を、リンクを知っているすべてのユーザーに許可するか、チーム メンバーのみに許可するかの選択
- リンク先のコンテンツのパスワードによる保護
- リンクの有効期限の設定または削除
- リンクの表示
- リンク先のコンテンツのダウンロード
- ユーザーの Dropbox に対するリンク先のコンテンツのコピー
- API アプリによるファイルへのリンクの作成
- チーム メンバー、チーム外のメンバー、またはグループとのリンクの共有
- チーム外のメンバーが共有フォルダ内のファイルへのリンクを閲覧する操作のブロック/ブロック解除
- アルバムの共有

**ファイル リクエスト機能**

- ファイル リクエストの作成、変更、完了、取り消し
- ファイル リクエストへのユーザーの追加
- ファイル リクエストの期限の追加/削除
- ファイル リクエストのフォルダの変更
- ファイル リクエストを通じたファイルの受信
- 「Email to Dropbox」機能経由でのファイルの受信

**個々のファイルやフォルダのイベント**

- Dropbox へのファイルの追加
- フォルダの作成
- ファイルの閲覧
- ファイルの編集
- ファイルのダウンロード
- ファイルまたはフォルダのコピー
- ファイルまたはフォルダの移動
- ファイル名またはフォルダ名の変更
- 旧バージョンのファイルの復元
- ファイル内の変更のロールバック
- 削除したファイルの復元
- ファイルまたはフォルダの削除
- ファイルまたはフォルダの完全削除

**ログインの成功と失敗**

- ログイン試行の成功または失敗
- シングル サインオン（SSO）経由でのログイン試行の失敗またはエラー
- EMM 経由でのログイン試行の失敗またはエラー
- ログアウト
- ウェブ セッション用 IP アドレスの変更

### パスワード

パスワードや 2 段階認証の設定の変更。管理者は、メンバーの実際のパスワードを閲覧できません。

- パスワードの変更またはリセット
- 2 段階認証の有効化、リセット、または無効化
- SMS またはモバイル アプリを使用するための 2 段階認証の設定または設定変更

- 2 段階認証で使用するバックアップ用電話番号の追加、編集、削除
- 2 段階認証用セキュリティ キーの追加または削除

**メンバーシップ**

チーム メンバーの追加/削除

- チーム メンバーの招待
- チームへの参加
- チーム メンバーの削除
- メンバーシップの一時停止または再開
- 削除したチーム メンバーの復元
- アカウント ドメインに基づくチームへの参加リクエスト
- アカウント ドメインに基づくチームへの参加リクエストに対する承認/拒否
- 既存のドメイン アカウントへのドメイン招待の送信
- アカウント キャプチャによるユーザーのチームへの参加
- アカウント キャプチャによるユーザーのドメインからの退出
- チーム メンバーが新規メンバーを提案する操作のブロック/ブロック解除
- 新規チーム メンバーの提案

**アプリ**

サードパーティ製アプリと Dropbox アカウントのリンク設定

- アプリケーションの承認または削除
- チーム アプリケーションの承認または削除

**デバイス**

パソコンまたはモバイル デバイスと Dropbox アカウントのリンク設定

- デバイスのリンクまたはリンク解除
- 遠隔削除の使用と、全ファイルの削除成功または一部ファイルの削除失敗
- デスクトップ パソコンまたはモバイル デバイスの IP アドレスの変更

**管理者の操作**

管理コンソールでの設定の変更（共有フォルダの権限など）

- **認証およびシングル サインオン（SSO）**
  - チーム メンバーのパスワードのリセット
  - すべてのチーム メンバーのパスワードのリセット

- チーム メンバーが 2 段階認証を無効化する操作のブロック/ブロック解除
- SSO の有効化または無効化
- SSO によるログインの必須化
- SSO 用 URL の変更または削除
- SSO 証明書の更新
- SSO アイデンティティ モードの変更

- **メンバーシップ**
  - アカウント ドメインに基づいてユーザーがチームへの参加をリクエストする操作のブロック/ブロック解除
  - チームのメンバーシップ リクエストを自動で承認するか、管理者による手動での承認を求めるかの設定

- **メンバー アカウントの管理**
  - チーム メンバー名の変更
  - チーム メンバーのメール アドレスの変更
  - 管理者ステータスの付与/削除、または管理者の役割の変更
  - チーム メンバーとしてのログイン/ログアウト
  - 削除されたメンバーのアカウント コンテンツの移行または削除
  - 削除されたメンバーのアカウント コンテンツの完全削除

- **グローバル共有設定**
  - チーム メンバーがチーム外のメンバー所有の共有フォルダを追加する操作のブロック/ブロック解除
  - チーム メンバーがチーム外のメンバーとフォルダを共有する操作のブロック/ブロック解除
  - ユーザーがチーム外のメンバーとフォルダを共有しようとするとユーザーに表示される警告の有効化
  - チーム外のメンバーが共有リンクを閲覧する操作のブロック/ブロック解除
  - 共有リンクをチーム専用にする設定のデフォルト化
  - ユーザーがファイルへコメントを追加する操作のブロック/ブロック解除
  - チーム メンバーがファイル リクエストを作成する操作のブロック/ブロック解除
  - 共有リンク ページへのロゴの追加、変更、削除
  - チーム メンバーがチーム外のメンバーと Paper ドキュメントおよび Paper フォルダを共有する操作のブロック/ブロック解除

- **ファイル用チーム フォルダの管理**
  - チーム フォルダの作成
  - チーム フォルダ名の変更
  - チーム フォルダのアーカイブ/アーカイブ解除
  - チーム フォルダの完全削除
  - チーム フォルダの共有フォルダへのダウングレード

- **ドメイン管理**
  - ドメインの検証の試行またはその完了、またはドメインの削除
  - Dropbox サポートによるドメインの検証または削除
  - ドメイン招待の送信の有効化または無効化
  - 「新規ユーザーを自動的に招待する」機能の有効化または無効化
  - アカウント キャプチャ モードの変更
  - Dropbox サポートによるアカウント キャプチャ機能の付与/取り消し
- **エンタープライズ モビリティ管理（EMM）**
  - テスト モード（オプション）または導入モード（必須）での EMM の有効化
  - EMM トークンの更新
  - EMM 除外ユーザー リストに対するチーム メンバーの追加/削除
  - EMM の無効化
  - EMM 例外リスト レポートの作成
  - EMM モバイル アプリ使用状況レポートの作成
- **その他のチーム設定の変更**
  - チームのマージ
  - チーム アカウントの Dropbox Business へのアップグレードまたは無料アカウントへのダウングレード
  - チーム名の変更
  - チーム アクティビティ レポートの作成
  - チーム メンバーがパソコンに複数アカウントをリンクする操作のブロック/ブロック解除
  - すべてのチーム メンバーまたは管理者のみに対するグループ作成の許可
  - チーム メンバーがファイルを完全削除する操作のブロック/ブロック解除
  - リセラーに対する Dropbox サポート セッションの開始/終了

### グループ

グループの作成、削除、メンバーシップ情報の表示

- グループの作成、名前の変更、移動、または削除
- メンバーの追加/削除
- グループ メンバーのアクセス タイプの変更
- グループの管理をチームに移管、もしくは管理者に移管
- グループの外部 ID の変更

### Paper アクティビティ ログ

管理者は、アクティビティ フィードの Paper アクティビティの種類を選択して、一部またはすべてのアクティビティ レポートをダウンロードできます。以下の Paper のイベントが記録されます。

- Paper の有効化または無効化
- Paper ドキュメントの作成、編集、エクスポート、アーカイブ、完全削除、復元
- Paper ドキュメントへのコメントの追加と解決
- Paper チーム メンバーおよびチーム外のメンバーとの Paper ドキュメントの共有/共有解除
- Paper チーム メンバーおよびチーム外のメンバーによる Paper ドキュメントへのアクセス権の要求
- Paper ドキュメントにおける Paper チーム メンバーおよびチーム外のメンバーによるメンション
- Paper チーム メンバーおよびチーム外のメンバーによる Paper ドキュメントの表示
- Paper ドキュメントのフォロー
- Paper ドキュメントに対するメンバーの権限の変更（編集、コメント、または閲覧のみ）
- Paper ドキュメントの外部共有ポリシーの変更
- Paper フォルダの作成、アーカイブ、および完全削除
- Paper ドキュメントのフォルダへの追加、またはフォルダからの削除
- Paper フォルダ名の変更
- Paper ドキュメントおよびフォルダの転送

# Dropbox Passwords

Dropbox Passwords を使えば、ユーザー名、パスワード、クレジット カード、デビット カードなどの情報を保存して、複数のデバイス間で同期し、自動入力できます。オンライン認証情報を保護するための安全でシンプルな方法です。Dropbox Passwords はオンラインの機密情報であるアカウント ユーザー名、パスワード、クレジット カード、デビッド カードの情報をゼロ知識暗号化を用いてクラウド内やデバイス上で保護します。Dropbox の製品は日常的に活用できるように構築され、安全が確保される設計になっています。

## ゼロ知識暗号化

Dropbox Password では、暗号化されたデータがクラウドに保管されていますが、その解読に必要な鍵はお客様のデバイスにのみ保管されます。**Dropbox がその鍵にアクセスすることはありません。**デバイスで生成された長いランダムな鍵が使用されます。新しいデバイスをペアリングしたり登録したりする場合を除いて、鍵がデバイス外に転送されることはありません。転送の際には、公開鍵暗号を用いて暗号化署名と鍵の保護が行われるため、他人が復号することは不可能で、内容が真正であることも検証されます。Dropbox を始め、鍵を持っていない者には暗号化されたデータは役に立たないため、この特性はしばしば、ゼロ知識暗号化と呼ばれています。言い換えると、**本人の情報は本人しか見ることができません。**万一 Dropbox がハッキングされても、その情報は引き続き安全です。暗号化されたデータは表示されている Dropbox フォルダとは別のところに保管され、Dropbox のクライアントや API を用いて覗き見ることはできません。

## 暗号化の詳細

Dropbox では、XChaCha20-Poly1305 を結合モードで使用して暗黙的に認証することで、データを暗号化しています。Dropbox のブラウザ拡張機能とモバイル アプリケーションはすべて libsodium を基盤とする暗号化を実装しています。この暗号化は NaCl の派生版で、監査を受け広く配布されています。

暗号化を実行するたびに 192 ビットのランダムなナンス値が生成されて暗号化されたペイロードとともに保存され、後に復号するときに使用されます。AES-GCM と異なり、XChaCha20-Poly1305 ではランダムなナンス値が利用できます。復号するときには、192 ビットのナンス値がペイロードから読み出され、暗号化されたペイロードの復号に用いられます。以降の暗号化では、以前に使用したナンス値とは無関係な 192 ビットのランダムなナンス値が生成されます。Dropbox Passwords は libsodium を用いてランダムなナンス値を生成します。これは暗号学的に安全な乱数発生器として Dropbox がサポートする各プラットフォームでデフォルトで採用されています。

## 鍵と復元ワード

Dropbox では、Blake2 ハッシュ化によって 128 ビットのエントロピー（ユーザー鍵）から 256 ビットの対称鍵（暗号化鍵）が生成されます。この暗号化鍵は所有者のデバイスのみに保管されていて、可能な限り、そのデバイス上でアクセスできる最も安全なストレージに保管されます。たとえば iPhone であれば、iOS キーチェーンの中に保管されます。

128 ビットのエントロピーをソースとして用いる理由は、十分なセキュリティが確保される一方で、BIP-39 標準を用いれば 12 の復元ワードのみでバックアップができるからです。BIP-39 は、桁の多いランダム鍵を 12 個のワードからなるリストに変換することで、人間にとって扱いやすい方法で表現します。任意の 128 ビットの鍵には 12 個のワードからなるリストが対応し、12 個のワードからなるリストにはそれぞれ、128 ビットが一意に対応します。なお、実際には 12 個のワードには 132 ビットが対応します。そこで、残りの 4 ビットをチェックサムとして使用してエラーを識別しています。復元ワードを用いれば、デバイスを紛失したり盗まれたりした場合に、暗号化鍵を復元することができます。復元ワードを印刷し安全な場所に保管しておくことをお薦めします。また、信用のおける友人や家族に知らせておくか、USB ドライブに保管することも検討してください、

## デバイスの登録

新しいデバイスから Dropbox Passwords にログインする場合、そのデバイスで安全な登録プロセスを完了していないと、ユーザーの Passwords データにアクセスすることはできません。このプロセスによって、ユーザーの秘密鍵と Passwords データへのアクセスがそのユーザーの登録済みデバイスに限定されます。さらに、既存の登録済みデバイスにアクセスできる場合と、復元ワードがわかっている場合にのみ、追加のデバイスを登録できるようになります。デバイスの登録プロセスは以下のようになります。

登録対象の新しいデバイスが 256 ビットのデバイス公開鍵とデバイス秘密鍵のペアをランダムに生成し、公開鍵を Dropbox サーバーにアップロードします。次に、シナリオ **A**、**B**、**C** のいずれかが実行されます。

**A：**ユーザーが以前にデバイスを登録したことがない場合、登録対象のデバイスが 128 ビットのユーザー秘密鍵をランダムに生成します。ユーザー鍵とデバイス鍵のペアが、以下の「鍵の保管」セクションで説明するように、OS ごとの安全な場所に保管されます。デバイスは、ユーザーの Passwords データを初期化して暗号化した後、暗号化されたペイロードを Dropbox サーバーにアップロードします。

**B：**ユーザーが以前にデバイスを登録したことがある場合、登録承認リクエストが登録済みデバイスのそれぞれに送られます。このリクエストには、登録対象のデバイスの公開鍵が添付されています。次に、ユーザーはこのリスエストを登録済みデバイスのいずれかを用いて承認する必要があります。承認されると、登録済みデバイスがユーザー鍵を自分の秘密鍵と登録対象のデバイスの公開鍵を用いて暗号化します。この際、X25519 ECDH と XSalsa20-Poly1305 の組み合わせが用いられます。登録済みのデバイスは、暗号化されたユーザー鍵を登録対象デバイスに送るために Dropbox サーバーにアップロードします。登録対象デバイスはユーザー鍵をダウンロードし、自分の秘密鍵と登録済みデバイスの公開鍵を用いて復号します。次に、登録対象デバイスが暗号化された Passwords ペイロードデータをダウンロードし、ユーザー鍵を用いて復号します。

**C：**ユーザーが以前にデバイスを登録したことがあるものの、それらのデバイスにアクセスできない場合、12 個の復元ワードを入力することで、ユーザー鍵をローカルで再構築できます。次に、登録対象デバイスが暗号化された Passwords のペイロードデータをダウンロードし、ユーザー鍵を用いて復号します。

## 鍵の保管

### ブラウザ拡張機能

ウェブ ブラウザでは、ユーザー鍵はブラウザ拡張機能のローカル ストレージ エリアに保管されています。ブラウザ拡張機能のローカル ストレージに保管された値にアクセスできるのはその拡張機能のみです。ユーザーがアクセスしているウェブサイトで実行されているコードがブラウザ拡張機能のローカル ストレージ エリアにアクセスすることはできません。さらに、ブラウザ拡張機能は、署名された拡張パッケージに含まれていないコードの実行を禁止しています。こうすることで、XSS 脆弱性を利用してローカル ストレージの値にアクセスされるリスクを排除しています。

ユーザーのデバイスに自由にアクセスできる攻撃者がディスク上にあるローカル ストレージのファイルを読み出すことでユーザー鍵にアクセスできる可能性があります。このような脅威が生じるケースとしては、攻撃者がデバイスに物理的にアクセスできる場合や、攻撃者がデバイス上で悪意のあるマルウェアを実行している場合などがあります。このようなシナリオに対抗するために、ローカル デバイスにパスフレーズを設定することができます。

パスフレーズが設定された場合、ユーザー鍵はブラウザ拡張機能のローカル ストレージに暗号化されて保管されます。この場合の暗号化鍵は Argon2 パスワード ハッシュ化によってパスフレーズから生成されます。暗号化には XChaCha20-Poly1305 が使用されます。ブラウザ拡張機能を再起動するたびにパスフレーズを入力し、ユーザー鍵の復号とデータのロック解除を実行する必要があります。その結果、パスフレーズを知らない攻撃者はディスク上にあるローカル ストレージのファイルに保管されたユーザー鍵を復号することができません。

### iOS

iOS では、ユーザー鍵は iOS キーチェーンに保管されます。キーチェーンはディスク上の暗号化されたデータベース ファイルです。このファイルは Secure Enclave と呼ばれるハードウェア モジュールに保管された秘密鍵を用いて暗号化されます。暗号化方式としては AES256-GCM が採用されています。Dropbox Passwords の署名された iOS アプリのみが、そのアプリによってキーチェーンに保管されたデータ項目にアクセスできます。そのため、ユーザーのデバイスで実行されている他のコードがユーザー鍵にアクセスすることはできません。

**Android**

Android では、ユーザー鍵は EncryptedSharedPreferences オブジェクトに保管されます。このオブジェクトはディスク上の暗号化された設定ファイルです。このファイルは Android Keystore と呼ばれる安全なハードウェアに保管されたマスター鍵を用いて暗号化されます。暗号化方式としては AES256-GCM が採用されています。Dropbox Passwords の署名された Android アプリのみが、設定ファイルの復号に必要なマスター鍵にアクセスできます。

### ローカル認証

Dropbox Passwords では、オプションでローカル認証手段を使用し、物理デバイスにあるユーザーの Passwords データに対するアクセスをさらに制限できます。モバイル アプリの場合、ローカル OS に対する認証操作（パスワードと補助的な生体認証）を再利用できます。ブラウザ機能拡張の場合、オプションでパスフレーズを設定できます。これらのメカニズムは、デバイス OS のロックが解除された場合に、アプリケーションを保護する追加のセキュリティの機能を果たします。こうすることで、家族や同僚など自分以外のユーザーが自分のデバイスにアクセスする可能性があっても、Passwords のデータを保護できます。

### 強力なパスワードの提案

Dropbox が構築したオープン ソースのツール zxcvbn を用いて、いくつかのパスワード マネージャーがパスワードの強度を評価しています。このツールは、入力されたパスワードをデータベースと照合します。このデータベースには、3 万件のよく使われるパスワード、米国国勢調査に基づくよくある氏や名、Wikipedia や米国のテレビ、映画で使われる一般的な英単語に加えて、よく使われるパターンとして、日付、繰り返し（aaa）、順列（abcd）、キーボード配列（qwertyuiop）、Leet（1337）Speak などが登録されています。ユーザーが設定しようとしたパスワードが一般的なものである場合、独自性の強い、推察されにくいパスワードを設定するよう促します。「**非常に強力**」の設定を使用すれば、ユーザー アカウントのセキュリティを最高レベルに維持できます。

# データ セキュリティ、プライバシー、透明性

Dropbox は重要な業務成果の日常的な保存先として、多くのユーザーと企業や組織に支持され信頼されており、Dropbox は責任ある企業としてこれらの情報の機密性の保護に最善を尽くしています。

### プライバシー ポリシー

Dropbox のプライバシー ポリシーは、dropbox.com/privacy でご覧になれます。Dropbox のプライバシー ポリシー、サービス契約、サービス規約、利用規約では、以下の条項について通知しています。

- Dropbox が収集するデータの種類と収集する理由
- Dropbox が情報を共有する可能性のある相手

- データの保護方法と保持期間
- データの保管場所と送信先
- ポリシーが変更された場合や質問が寄せられた場合の対応

**透明性**

Dropbox では、ユーザー情報に関する法執行機関からの要請を取り扱う方法と、そのような要請の件数および種類について、透明性の確保に努めています。Dropbox はすべてのデータ要請が法律を遵守していることを綿密に調査し、法執行機関の要請によりユーザーのアカウントが特定された場合は、法律で許可されている範囲で、ユーザーにその旨を通知するよう尽力しています。

Dropbox のこうした取り組みは、ユーザーのプライバシーとデータの保護を保証する弊社のコミットメントを裏付けています。この目的を達成するために、Dropbox では透明性レポートを提供し、政府によるデータ要請原則を確立しています。ユーザー データに対する政府からの要請を Dropbox が受け取り、調査し、返答する際の手順については、以下の原則が適用されます。

- **透明性の維持**
  オンライン サービス企業は、政府から受け取った要請の数と種類を公開すること、さらには個人情報の提供が要請された際に本人にそのことを通知することが許されるべきであると、Dropbox は考えます。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**
  政府によるデータ要請は、特定のユーザーと合法な調査に限定されるべきです。Dropbox は、包括的かつ過度に広範な要請には応じません。

- **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。Dropbox は、これらの法律の改定に取り組み続けています。

- **信頼できるサービスを提供**
  政府がユーザー 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することや、インフラストラクチャを危険にさらすことがあってはなりません。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。

Dropbox の透明性に関するレポートは、dropbox.com/transparency でご覧になれます。

## プライバシーに関する認定、基準、規制準拠

毎日、多くのユーザーと組織が Dropbox を信頼して重要なデータを保存しています。このため、Dropbox はお客様のファイルを保護し外部に漏洩しないよう責任を持って取り組んでいます。Dropbox におけるすべての意思決定の中核には、お客様のプライバシーを守るという当社のコミットメントがあります。

### ISO/IEC 27018（クラウドにおける個人データ保護のための行動基準）、および ISO/IEC 27701（プライバシー情報管理のための ISO/IEC 27001 と ISO/IEC 27002 に対する拡張）

Dropbox Business は大手クラウド サービス プロバイダとして、ISO/IEC 27018 と ISO/IEC 27701 の認定をいち早く取得しました。

ISO/IEC 27018 は、クラウドにおけるプライバシー保護とデータ保護のための国際規格であり、ユーザーのプライバシーとデータの保護を目的に 2014 年 8 月に公開されました。

ISO/IEC 27701 は、プライバシー情報管理のための最初の国際的な認定規格であり、2019 年に公開されました。ISO/IEC 27001 における情報セキュリティ管理システム（ISMS）にデータ プライバシーに関する考慮事項を追加して、プライバシー情報管理システム（PIMS）に拡張するためのフレームワークを提供することを目的としています。

両規格では、Dropbox による組織情報の使用/不使用に関して多くの要件が定められています。

- **お客様のデータを管理するのはお客様です。**

  お客様から提供された個人情報を Dropbox が使用する目的は、お客様が登録したサービスを提供することに限られます。お客様は必要に応じて、Dropbox に対してファイルや Paper ドキュメントの追加、変更、削除を行うことができます。

- **Dropbox はお客様のデータに関する透明性を守ります。**

  Dropbox サーバー上のお客様データの保管場所について、透明性を守ります。また、Dropbox は信頼するパートナー企業に関する情報をお客様に開示し、アカウントの解約やファイルまたは Paper ドキュメントの削除に伴う情報の取り扱い方法についてもお知らせします。これらの内容が変更された場合も通知いたします。

- **データを安全に保管します。**

  ISO/IEC 27018 と ISO/IEC 27701 は、世界で最も信頼されている情報セキュリティ基準の 1 つである ISO/IEC 27001 を強化、拡張するために策定されました。Dropbox は、2021 年 10 月に ISO/IEC 27001 認定の更新を受けています。

- **Dropbox の実践は定期的に審査されています。**

  ISO/IEC 27018、ISO/IEC 27701、ISO/IEC 27001 に従い、Dropbox では認定を維持するために年に 1 度、独立した第三者法人による監査を実施いたします。Dropbox が取得しているすべての ISO 認定は、こちらでご覧になれます。

### 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、当社のお客様や関連会社との契約、標準的契約条項、特定の国の適切性に関する欧州委員会の決定など、該当するさまざまな法的枠組みを遵守しています。

Dropbox は、欧州連合、欧州経済地域、英国、およびスイスから米国に転送される個人情報の収集、使用、保持に関して米国商務省により定められている欧州連合/米国間とスイス/米国間のプライバシー シールド フレームワークに準拠しています。ただし Dropbox は、個人情報を転送する法的根拠を、欧州連合/米国間とスイス/米国間のプライバシー シールド フレームワークに置いてはいません。Dropbox は、自社が当該データに関してプライ

バシー シールド原則に準拠していることを米国商務省に対して証明しています。なお、プライバシー シールドの詳細は https://www.privacyshield.gov をご覧ください。

Dropbox のプライバシー シールド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（dropbox.com/privacy）をご覧ください。

**EU 一般データ保護規則（GDPR）**

一般データ保護規則（GDPR）は、2018 年に施行された欧州連合の規則であり、個人データの取り扱いと保護に関する包括的な枠組みを確立するものです。

Dropbox は、ユーザーのデータのセキュリティと保護に関して、法的要件とベスト プラクティスに常に則ることを第一に考えています。この約束のもと、弊社は Dropbox の GDPR 準拠を徹底すべく、データ保護担当者の任命、プライバシー保護プログラムの見直しを介したユーザーによるデータ主体の権利行使の担保、弊社のデータ処理業務の文書化、セキュリティ侵害が発生した場合の社内プロセスの強化を図っています。今後も、データ保護当局からのさらなる指示に応じて、弊社のプロセスと慣行が新しい規則の個々の要素を満たし、ときにはそれを超えるように調整を続けていきます。

**EU クラウド行動規範**

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コミットメントを実証できるようにする自発的手段です。チームを対象とした Standard、Advanced、Enterprise、Education のプランで構成される Dropbox Business 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、これらのサービスがこの規範の要件に沿って技術、組織、契約において対策を実施していることを意味しています。EU クラウド行動規範と、この規範に関する Dropbox のコンプライアンスについて詳しくは、この規範の公式ウェブサイトをご覧ください。

Dropbox のプライバシー保護に関する実践とポリシーの詳細については、Dropbox のプライバシーとデータの保護に関するホワイトペーパーをご覧ください。

# コンプライアンス

企業に求められるセキュリティやプライバシーに関する規制や業界基準は多数ありますが、Dropbox では、最も広く認められている規格を、お客様のビジネスや業界固有のニーズに適合させたコンプライアンス対策と組み合わせるという手法を採用しています。

## ISO

国際標準化機構（ISO）は、情報セキュリティと社会セキュリティに関する国際的な一連の標準を作成し、企業が信頼性の高い革新的な製品とサービスを開発できるようにしています。Dropbox のデータ センター、システム、アプリケーション、人員、プロセスは、オランダを拠点とする独立した第三者機関である、EY CertifyPoint による一連の監査を通じて認証を取得しています。この企業は、Raad voor Accreditatie （オランダ認定評議会）から ISO 認定を取得しています。

**ISO/IEC 27001（情報セキュリティ）**

ISO/IEC 27001 は世界中で認められている情報セキュリティ マネジメント システム（ISMS）の最高基準で、ISO/IEC 27002 で詳細に規定されているベスト プラクティスも活用しています。Dropbox ではお客様からご信頼をいただけるように、情報セキュリティを物理的、技術的、法的に管理する方法を、包括的に改善し続けています。

Dropbox Business と Dropbox Education の ISO/IEC 27001 証明書は、こちらでご覧になれます。

**ISO/IEC 27017（クラウド セキュリティ）**

ISO/IEC 27017 は、クラウド セキュリティに関する国際規格です。クラウド サービスの提供と使用におけるセキュリティ管理のガイドラインが定められています。Dropbox とお客様がともに満たす必要があるセキュリティ、プライバシー、コンプライアンスのさまざまな基準については、「共有責任ガイド」をご覧ください。

Dropbox Business と Dropbox Education の ISO/IEC 27017 証明書は、こちらでご覧になれます。

**ISO/IEC 27018（クラウド プライバシーとデータ保護）**

ISO/IEC 27018 は、お客様の代わりに個人情報を処理する Dropbox のようなクラウド サービス プロバイダに適用される、プライバシーとデータを保護するための国際規格です。この認証は、お客様が一般的な規制や契約上の要件あるいは疑問に対応するための基盤となるものです。

Dropbox Business と Dropbox Education の ISO/IEC 27018 証明書は、こちらでご覧になれます。

**ISO/IEC 22301（事業継続）**

ISO/IEC 22301 は、事業の継続性に関する国際規格です。組織におけるサービス中断の可能性を抑え、万一サービスが中断した際に適切に対応して損害を最小限に抑えるための指針が示されています。Dropbox では、事業継続計画システム（BCMS）が全体的なリスク管理戦略に組み込まれており、危機的な問題が発生したときに人員と業務を保護します。

Dropbox Business と Dropbox Education の ISO/IEC 22301 証明書は、こちらでご覧になれます。

**ISO/IEC 27701（プライバシー情報管理）**

ISO 27701 は、プライバシー情報管理に関する国際規格です。ISO 27001 に基づく情報セキュリティ管理システムをプライバシー情報管理システム（PIMS）に強化、拡張するためのフレームワークを提供します。Dropbox Business と Dropbox Education は、PII 処理業者としてこの認定を受けています。

Dropbox Business と Dropbox Education の ISO 27701 証明書は、こちらでご覧になれます。

## SOC

Service Organization Controls（SOC）レポートは、SOC 1、SOC 2、SOC 3 とも呼ばれ、企業や組織内で実装されている内部管理を報告するために米国公認会計士協会（AICPA）により確立されたフレームワークです。Dropbox は、独立した第三者監査法人である Ernst & Young LLP による一連の監査を通じて、システム、アプリケーション、人員、プロセスに関する検証を受けています。

**SOC 3：セキュリティ、機密性、処理の完全性、可用性、プライバシー**

SOC 3 保証レポートは、5 つの信用サービス基準であるセキュリティ、機密性、完全性、可用性、プライバシー（TSP セクション 100）のすべてを対象としています。Dropbox の汎用レポートには、SOC 2 レポートの要旨と、Dropbox の管理下にあるデザインとオペレーションの効率の高さに関する独立した第三者監査法人による見解が含まれています。

Dropbox Business と Dropbox Education の SOC 3 レポートは、こちらでご覧になれます。

### SOC 2：セキュリティ、機密性、処理の完全性、可用性、プライバシー

SOC 2 レポートは、管理機能に関する詳細なレベルの保証を提供するもので、5 つの信用サービス基準であるセキュリティ、可用性、処理の完全性、機密性、プライバシー（TSP セクション 100）のすべてを対象としています。SOC 2 レポートには、Dropbox がお客様のデータを保護するうえで使用するプロセスや、100 を超える管理機能に関する詳細が含まれています。Dropbox の管理のデザインとオペレーションの効率の高さに関する独立した第三者監査法人による査定評価の他に、本レポートには監査法人の各管理機能に対するテスト手順とテスト結果も記載されています。Dropbox の SOC 2 レポート（SOC 2+ とも呼ばれます）には、弊社の管理と前述の ISO 標準との監査済み対応付けも記載されており、内容をわかりやすくする工夫がなされています。Dropbox Business と Dropbox Education の SOC 2 レポートをご希望のお客様はこちらからお問い合わせください。

### SOC 1 / SSAE 18 / ISAE 3402（旧 SSAE 16 または SAS 70）

SOC 1 レポートは、お客様の財務報告に係る内部統制（ICFR）プログラムにとって Dropbox Business または Dropbox Education が重要な要素であるとお考えのお客様に保証を提供するものです。お客様はこの保証を Sarbanes-Oxley（SOX）コンプライアンス向けに使用できます。独立した第三者法人による監査は、保証業務基準書第 18 号（SSAE 18）と国際保証業務基準第 3402 号（ISAE 3402）に従って実施されます。これらの規格は、廃止された保証業務基準書第 16 号（SSAE 16）と監査基準書第 70 号（SAS 70）に代わって取り入れられています。Dropbox Business と Dropbox Education の SOC 1 レポートをご希望のお客様はこちらからお問い合わせください。

## CSA

### クラウド セキュリティ アライアンス：セキュリティ、信頼性、保証登録（CSA STAR）

CSA Security, Trust Assurance Registry（STAR）は、クラウド サービス向けのセキュリティ保証プログラムを提供します。誰でもアクセスすることができ、登録は無料です。ユーザーが現在使用中、または契約を検討中のクラウド プロバイダのセキュリティを評価する際にこれらの情報が役立ちます。

Dropbox Business と Dropbox Education は CSA STAR のレベル 2 認証（Certification）とレベル 2 証明（Attestation）を受けています。CSA STAR のレベル 2 は、ISO/IEC 27001、SOC 2 Trust Services Criteria、CSA Cloud Controls Matrix（CCM）v.4.0.2 に則って行われる、独立した第三者法人（認証は EY CertifyPoint、証明は Ernst & Young LLP）による Dropbox のセキュリティ管理に関する評価を必要とします。

Dropbox の CSA STAR レベル 2 の認証と証明は、CSA ウェブサイトでご覧いただけます。

## HIPAA/HITECH

Dropbox は、事業提携契約書（BAA）を、これを必要とする Dropbox Business または Dropbox Education のお客様との間で締結しています。BAA は米国の医療保険の携行性と責任に関する法律（HIPAA）と経済的および臨床的健全性のための医療情報技術に関する法律（HITECH）を遵守するために必要な文書です。詳しくは、「Dropbox と HIPAA/HITECH」をご覧ください。

Dropbox は、Dropbox Business または Dropbox Education の使用において HIPAA/HITECH のセキュリティとプライバシーに関する規定が満たされていることを示す必要のあるお客様向けに、HIPAA/HITECH のセキュリティ、プライバシー、違反通知の規定に対する Dropbox の管理を評価するサードパーティによる保証レポートと、Dropbox の社内での慣行と推奨事項との対応付けが記載されている文書を提供しています。

これらの文書が必要なお客様、または Dropbox Business や Dropbox Education の購入について詳しい情報をお求めのお客様は、Dropbox のセールス チームにお問い合わせください。また、現在お客様が Dropbox Business や Dropbox Education のチーム管理者である場合は、管理コンソールから［アカウント］ページに移動し、BAA に電子署名することができます。

管理コンソールで BAA に電子署名可能なユーザーは、米国に拠点を置くお客様に限定されていますのでご留意ください。

## NIST 800-171

米国立標準技術研究所（NIST）は、情報システムの保護を支援するための規格およびガイドラインの普及と管理に取り組んでいます。NIST 特別刊行物（SP）800-171 改訂 2 版（R2）には、連邦政府以外の情報システムおよび組織で扱う「管理すべき非機密情報（CUI）」を保護するためのガイドラインが記載されています。米国政府の CUI を処理、保存するすべての組織（研究機関や教育機関など）は、NIST SP 800-171 R2 に準拠する必要があります。Dropbox の CUI 関連のシステム、プロセス、および管理機能は、独立した第三者監査機関である Ernst & Young LLP による検証を受けています。

Dropbox Business および Dropbox Education の NIST SP 800-171 R2 レポートをご希望の場合は、Dropbox のセールス チームまでご請求いただくか、現在 Dropbox Business をご利用のお客様はサポート チームまでお問い合わせください。

Dropbox Paper は NIST SP 800-171 R2 レポートの範囲に含まれないことにご注意ください。

## FERPA と COPPA（学生と児童）

Dropbox Business と Dropbox Education は米国の家庭教育の権利とプライバシーに関する法律（FERPA）により課せられるベンダーの義務に従って、お客様のサービス利用を認めています。13 歳未満の児童が在籍する教育機関も、サービスの利用に関して保護者の同意を得ることを教育機関に義務付ける特定の契約条項に同意した場合、児童オンライン プライバシー保護法（COPPA）に従って Dropbox Business と Dropbox Education を利用できます。

### 米食品医薬品局（FDA）連邦規則集（CFR）第 21 章第 11 条

連邦規則集（CFR）第 21 章は、米食品医薬品局（FDA）、米麻薬取締局、全米麻薬撲滅対策室向けに、米国における食品と医薬品に関する規則を定めたものです。第 21 章第 11 条に明記された基準に基づいて、FDA では電子記録および電子署名は信頼性が高く、一般的に、用紙による記録および書面上の手書きの署名に相当するものであると認めています。

CFR 第 21 章第 11 条に基づくお客様組織のコンプライアンスに関して Dropbox が提供する支援の詳細については、Dropbox と FDA CFR 第 21 章第 11 条に関するホワイトペーパーとヘルプセンターの記事をご覧ください。

### PCI DSS

Dropbox は、PCI データ セキュリティ基準（PCI DSS）に準拠していますが、Dropbox Business、Dropbox Education、Dropbox Paper はクレジット カードの取引を処理または保存するように設計されていません。Dropbox のマーチャント ステータスの PCI 準拠証明書（AoC）をご希望のお客様は、こちらからお問い合わせください。

Dropbox Business と Dropbox Education のコンプライアンスについての詳細については、dropbox.com/business/trust/compliance をご覧ください。

## Dropbox 向けアプリ

DBX プラットフォームは、柔軟性を備えたアプリケーション プログラミング インターフェース（API）を利用する開発者の強力なエコシステムから成り立っています。このプラットフォームでは、75 万人以上のデベロッパーが生産性向上、共同作業、セキュリティ、管理などのためのアプリケーションやサービスを構築しています。

### プリビルトされたコンポーネント

Chooser、Saver、Embedder は、プリビルドされているウェブおよびモバイル用のコンポーネントで、サードパーティのアプリやサイトからわずか数行のコードで Dropbox に簡単にアクセスできるようにするものです。

- Chooser を使用すると、Dropbox からファイルを選択できます。
- Saver を使用すると、Dropbox にファイルを直接保存できます。
- Embedder を使用すると、Dropbox にあるファイルやフォルダを表示できます。

これらのコンポーネントに対する認証は、Dropbox のみを通じて行われます。Dropbox の共有リンクや有効期限の短いダウンロード リンクを通じて、Chooser で選択されたファイルへのアクセス許可がアプリに与えられます。これらの事前定義コンポーネントは単独で使用することも、以下に説明する API とともに使用することもできます。

## Dropbox Business API インテグレーション

サードパーティのデベロッパーは Dropbox の公開 API を使用することで、アプリから Dropbox にアクセスし、Dropbox と連携できるようになります。これには、ファイルやメタデータのやり取り、共有、チームに関連する機能などがあります。

### 認証

Dropbox は業界基準プロトコルの OAuth を認証に使用しているため、アカウントの認証情報を公開せずに、ユーザーはアカウントのアクセス権をアプリに付与できます。Dropbox は、API リクエストの認証で OAuth 2.0 をサポートしています。リクエストは Dropbox ウェブサイトまたはモバイル アプリ経由で認証されます。Dropbox は、有効期限が短いアクセス トークンや分散アプリのための PKCE など、OAuth のベスト プラクティスをサポートしています。

### ユーザーの権限

Dropbox API を使用すると、エンド ユーザーの Dropbox に以下のレベルでのコンテンツ アクセスが可能なアプリを開発できます。

- **アプリ フォルダ**
  Dropbox の「アプリ」フォルダには、アプリ名が付いた専用フォルダが作成されます。アプリには、このフォルダに対してのみ読み取り/書き込みアクセス権が付与され、ユーザーはこのフォルダにファイルを移動することにより、アプリでコンテンツを使用できます。また、アプリから Chooser または Saver 経由でファイル/フォルダへのアクセス権をリクエストすることもできます。

- **Dropbox へのフル アクセス**
  アプリは、Dropbox 内にあるすべてのファイルやフォルダに無制限にアクセスできるようになります。Chooser または Saver 経由でファイルやフォルダへのアクセス権をリクエストすることもできます。

アプリは特定のスコープをリクエストすることも可能で、API エンドポイントのサブセットへのアクセスによって挙動を制限できます。たとえば、ファイルへの読み取り専用アクセスやコンテンツのアップロードを可能にするものの、共有の作成は禁止するなどしてアプリを制限できます。

### チームの権限

Dropbox Business の管理者は、チームの管理コンソールに表示されている管理機能にアプリからアクセスできるように許可できます。チームがリンクしたアプリが実行できるアクションは、スコープによって制限できます。具体的には、アプリに読み取りまたは管理を認めるチーム設定を指定します。

スコープの一般的な組み合わせの例を以下に挙げます。

- **Team Information（チーム情報）**
  チームと使用状況の概要に関する読み取り専用の情報

- **Team auditing（チーム監査）**
  チーム情報および詳細なイベント ログへの読み取り専用アクセス

- **Team Member File Access（チーム メンバーのファイル アクセス）**
  チーム内のユーザーの代理として、ファイルやフォルダの管理などのアクションを実行する機能

- **Team Member Management（チーム メンバーの管理）**
  チームへのメンバーの追加とチームからのメンバーの削除

### ウェブフック

ウェブフックを使用すると、ウェブ アプリはユーザーの Dropbox に変更が発生した場合に、それに関する通知をリアルタイムに取得できます。ウェブフックを受信するために URI を登録すると、アプリの登録ユーザーのいずれかに変更が発生したとき、HTTP リクエストがその URI に送信されます。Dropbox Business API とウェブフックを組み合わせて使用すると、チーム メンバーシップの変更に関する通知も生成できます。多くのセキュリティ アプリでウェブフックを使用することで、管理者はチーム アクティビティの追跡と管理ができるようになります。

### Extensions

アプリは拡張 URI を登録することが可能で、Dropbox の UI の［共有］と［開く］のメニューにアクションが表示されます。Dropbox Extensions を使うことで、ユーザーは Dropbox 内にあるファイルから直接サードパーティのカスタム ワークフローを開始できます。アクションがトリガーされると、Dropbox は指定された URI にユーザーをリダイレクトします。そのときに渡されたファイル識別子を API とともに使用することで任意のファイル操作を実行できます。登録した拡張機能をユーザーに表示するには、事前にアプリの認証を行う必要があります。Dropbox では一部の拡張機能のインテグレーションを［共有］と［開く］のメニュー内でユーザーに宣伝目的で表示する場合がありますが、ユーザーが承認するまでアプリがコンテンツにアクセスすることはできません。

### Dropbox 開発者向けガイドライン

Dropbox は開発者向けにさまざまなガイドラインや実践方法を示して、ユーザーのプライバシーを尊重し保護しながら Dropbox のユーザー エクスペリエンスを向上する API アプリの開発に貢献しています。

- **アプリ キー**
  開発するアプリごとに一意の Dropbox アプリ キーを使用する必要があります。また、DBX プラットフォームを意識させないサービスやソフトウェアを実現するアプリが開発者向けに提供される場合、そのアプリを利用する開発者は独自の Dropbox アプリ キーを申し込む必要があります。

- **アプリの権限**
  開発者は、アプリに付与する権限を最小限に留める必要があります。開発者がアプリをプロダクション段階に昇格する承認を申請すると、Dropbox はアプリが提供する機能を考慮し、必要以上に幅広い権限を要求していないかどうか確認します。

- **アプリの審査プロセス**

  - **開発段階**
    新たに作成された Dropbox API アプリには、最初に、開発段階が割り当てられます。アプリはその他のプロダクション段階のアプリと同様に機能しますが、リンクできる Dropbox ユーザー数は最大 500 人に制限されます。アプリを Dropbox ユーザー 50 人にリンクしたら、開発者は 2 週間以内にプロダクション段階の承認を求める申請を行う必要があります。申請を行わないと、追加の Dropbox ユーザーをリンクする機能は凍結されます。

  - **プロダクション段階と承認**
    プロダクション段階の承認を得るには、すべての API アプリが、DBX プラットフォーム使用上の禁止事項など、開発者向けのブランドの取り扱いガイドラインと利用規約を遵守している必要があります。禁止事項には、知的所有権または著作権の侵害の助長、ファイル共有ネットワークの構築、コンテンツの不正ダウンロードなどが含まれます。開発者は、アプリの機能に関する追加情報や、アプリによる Dropbox API の使用方法などを審査前に提出することが求められます。プロダクション段階の承認を受けたアプリは、リンクできる Dropbox ユーザー数の制限が解除されます。

### チームのアプリ管理

チームの管理コンソール内で、Dropbox Business の管理者は、チームでリンクしているアプリとインテグレーションを管理できます。

## API パートナーシップ

Dropbox はこれまでテクノロジー パートナーと緊密な連携を図り、パートナーの使い慣れたソフトウェア パッケージとのインテグレーションをパートナーが開発できるよう支援してきました。これらのパートナーは Dropbox API を使用してアプリを開発し、Dropbox のアーキテクトと協力してセキュリティや UX のベスト プラクティスを採り入れています。以下に示すように、開発されるアプリにはセキュリティや管理のツール以外にも、エンド ユーザー向けの生産性向上アプリなどがあります。

- **セキュリティ情報/イベント管理（SIEM）と分析**

  Dropbox Business アカウントを SIEM や分析ツールに接続することで、ユーザーによる共有、ログイン試行、管理操作などをモニターし、評価できます。中央ログ管理ツールを使えば、社員のアクティビティ ログとセキュリティ関連のデータにアクセスして、それらを管理できます。

- **情報漏洩防止（DLP）**

  ファイルのメタデータとコンテンツを自動的にスキャンして、Dropbox Business アカウントに重要な変更が加えられたときに、アラートやレポート処理、アクションをトリガーします。企業のポリシーを Dropbox Business の導入環境に適用し、規制準拠の要件を満たすのに役立ちます。

- **電子情報開示（eDiscovery）と法的ホールド**

  Dropbox Business アカウントのデータで、訴訟や調停、規制に関する調査に対応できます。電子的に保管された情報の中から関連性のある情報を検索/収集し、電子情報開示プロセスでデータを保存するので、時間と経費を節約できます。

- **デジタル著作権管理（DRM）**

  サードパーティ製のコンテンツ保護機能を追加して、社員のアカウントに保管された機密データや著作権のあるデータの保護を強化できます。クライアント側での暗号化、透かし、監査証跡、アクセス取り消し、ユーザー/デバイスのブロックなど、パワフルな DRM 機能を利用できます。

- **データ移行とオンプレミス バックアップ**

  既存のサーバーや他のクラウドベース ソリューションから Dropbox へデータを移行することで、時間、経費、労力を節約できます。Dropbox Business アカウントからオンプレミス サーバーへ自動でバックアップすることもできます。

- **アイデンティティ管理とシングル サインオン（SSO）**

  プロビジョニングとプロビジョニング解除の処理を自動化して、新入社員のオンボーディングを迅速化できます。Dropbox Business を既存のアイデンティティ管理システムと連携することで、管理業務の合理化とセキュリティの強化が実現します。

- **カスタム ワークフロー**

  Dropbox を既存のビジネス プロセスに統合する社内アプリを構築して、社内のワークフローを強化できます。

テクノロジー パートナーの一覧については、Dropbox アプリ インテグレーションのページをご覧ください。エンド ユーザーは、App Center で Dropbox 製およびサードパーティ製のアプリとインテグレーションを見つけることができます。

# Dropbox インテグレーション

他にも、一流のテクノロジー パートナーと協力して、Dropbox の UI 内に組み込むインテグレーションを開発しています。こうしたより密接なインテグレーションは、Dropbox とパートナーが共同で開発しています。以下にご紹介します。

### Dropbox Extensions

このインテグレーションではさまざまなタイプのアプリ拡張機能を使用して、動画の公開、メールやチャットへのファイルの追加、電子署名をリクエストするためのファイル送信などの操作を Dropbox の画面からシームレスに実行することができます。これらのアプリケーションはパートナーによって開発されていますが、Dropbox は［次で開く］と［次で共有］のメニューで一部の Extensions パートナーを表示することで、ユーザーが発見しやすいよう支援しています。

### Slack、Zoom、Trello

このインテグレーションは Dropbox によるファースト パーティ製です。ユーザーは Dropbox の画面から切り替えることなく、Slack の会話や会議を開始し、タスクを作成できるようになります。エンド ユーザーはこれらのツールを OAuth で認証します。

### モバイル/ウェブ版 Microsoft Office

Dropbox の Microsoft Office インテグレーションを利用すれば、Dropbox に保存されている Word/Excel/PowerPoint ファイルを直接開くことができます。また、Office モバイル アプリやウェブ アプリでファイルを編集して、Dropbox に直接保存できます。Office モバイル アプリやウェブ アプリで Dropbox ファイルを初めて開くと、アクセス許可を求める画面が表示されます。リンクが保持されるため、2 回目以降はこの画面が表示されません。

### Adobe Acrobat と Acrobat Reader

Dropbox はデスクトップ版とモバイル版（Android と iOS）Acrobat アプリと連携しており、Dropbox に保存された PDF ファイルの閲覧、編集、共有が可能です。アプリで Dropbox ファイルを初めて開くと、アクセス権を求める画面が表示されます。PDF の変更内容は自動的に Dropbox に保存されます。

# まとめ

Dropbox Business は、チームで効率よく共同作業するための使いやすいツールを提供するとともに、組織が必要とするセキュリティ対策やコンプライアンス認定を実現しています。堅牢性を備えたバックエンド インフラストラクチャとカスタマイズ可能なポリシー セットを組み合わせてマルチレイヤー化されたアプローチにより、Dropbox はお客様の固有のユーズに合わせることができる強力なソリューションをお客様に提供します。Dropbox Business の詳細については、Dropbox（sales@dropbox.com）にお問い合わせください。