Dropbox Business のセキュリティ
Dropbox ホワイトペーパー

Contents

はじめに

Dropbox は、写真や動画、ドキュメントなどのファイルをさまざまなデバイスから簡単に保存し、確実に同期・共有できるツールとして、世界中で数億ものユーザーに信頼されています。Dropbox Business は、これと同じシンプルな操作性をビジネスでもご利用いただくためのツールです。さらに高度な機能が用意されており、チームのメンバーは組織間でファイルをスピーディに共有でき、管理者は必要な可視性と制御を獲得できます。Dropbox Business は、ファイルの保管や共有のための使いやすいツールとしてだけでなく、重要な業務ファイルのセキュリティを守るために設計されています。Dropbox が開発した高度なインフラストラクチャにより、アカウント管理者は独自のポリシーを追加したりカスタマイズしたりできます。本ホワイトペーパーでは、バックエンド ポリシーの詳細や管理者が利用できるオプションなど、信頼できるビジネス ツールとしての Dropbox の詳細についてご説明します。

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以下の全製品に適用されます。

- Dropbox Business
- Dropbox Enterprise
- Dropbox Education

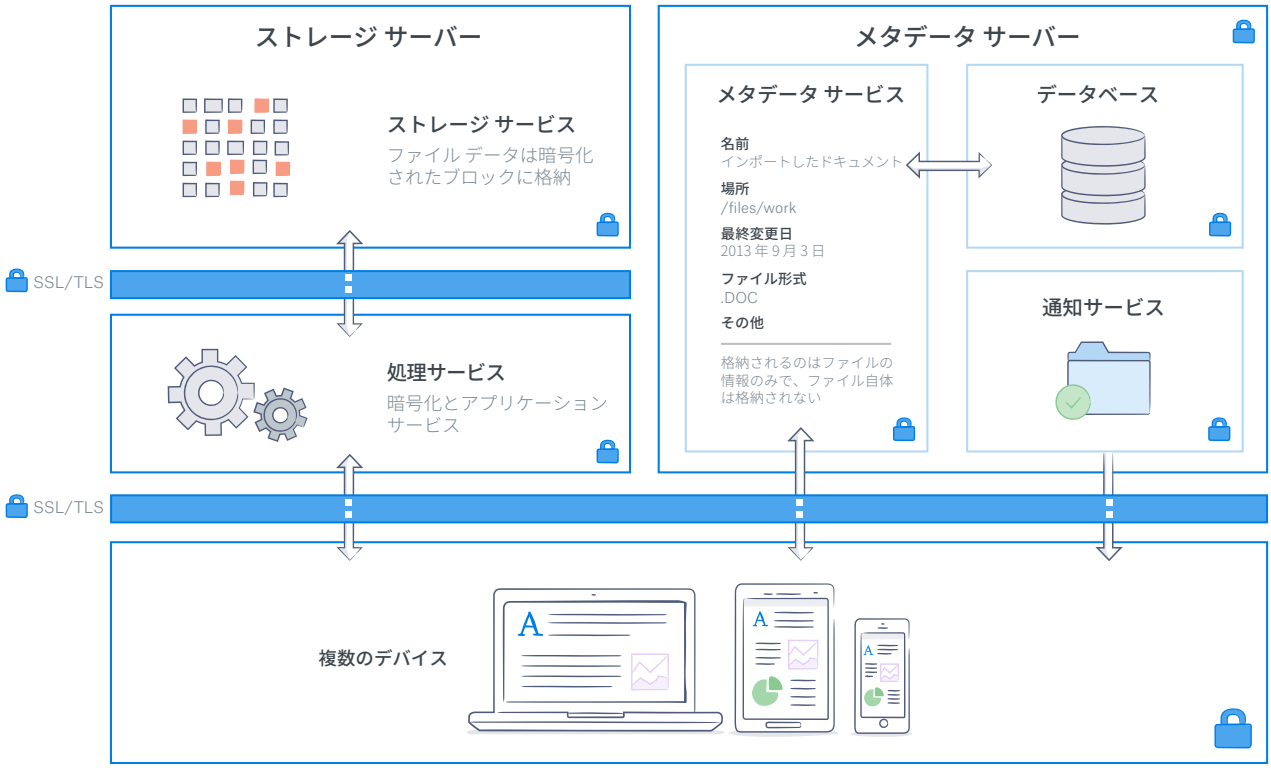
機能の詳細

Dropbox のインターフェースは使いやすく、ファイルをすばやく確実にアップロード、ダウンロード、同期、共有できるように、バックグラウンドで動作するインフラストラクチャでサポートされています。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、安全性を維持しながらデータがどのように転送、保管、処理されているかをご説明します。

アーキテクチャ

Dropbox は、データ転送、暗号化、ネットワーク設定、アプリケーション レベルの管理などを対象とする複数の保護レイヤーを備えており、これらの保護は拡張可能で安全なインフラストラクチャ全体に適用されています。

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 アーキテクチャは以下のサービスで構成されています。

- **処理サービス:**Dropbox は従来の暗号化を超える独自のセキュリティの仕組みを利用して設計され、ユーザーのデータを保護しています。暗号化とアプリケーション サービスでは、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暗号化とアプリケーション サービスに通知します。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ストレージ サービスに転送されます。これらのサービスが使用する暗号化の詳細については、「**暗号化**」のセクションをご覧ください。
- **ストレージ サービス:**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、ストレージ サービス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、ブロック ストレージ サービスに合わせてファイルをファイル ブロックに分割します。ストレージ サービスは 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。
- **メタデータ サービス:**ユーザー データに関する特定の基本情報 (ファイル名やファイル形式など) 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。Dropbox 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、必要に応じて共有 / 複製されます。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。
- **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。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。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 サービスに安全に接続して、ファイルの変更を同期する必要があります。

Dropbox では、社内のセキュリティ専門チームがサードパーティのセキュリティ スペシャリストと協力し、脆弱性を特定して対策を講じることにより、リスクを最小限に抑えながら、これらのサービスを保護しています。セキュリティ担当のグループは、アプリケーション、ネットワーク、その他のセキュリティについて定期的にテストや監査を行い、Dropbox のバックエンド ネットワークのセキュリティを確保しています。

さまざまなレベルの情報を前述のサービスに分散することにより、同期速度と信頼性だけでなく、セキュリティも向上しています。Dropbox アーキテクチャの特性により、個別のサービスにアクセスしてもファイルを複製することはできません。暗号化の種類の詳細については、後述の「**暗号化**」のセクションをご覧ください。

ファイル データの保存

Dropbox は、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）を保管します。ファイルのメタデータは、Dropbox サーバーに保管されます。ファイルのコンテンツは、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。

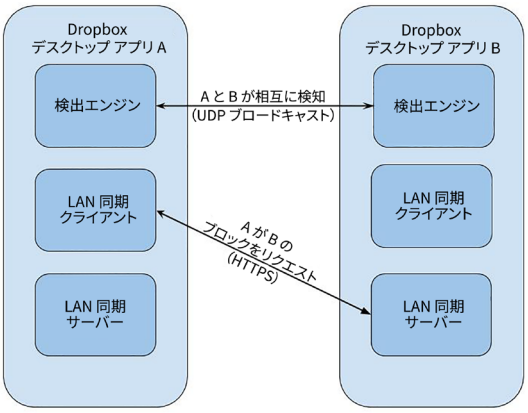
同期

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 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、クライアントは操作を再開します。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、安定した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 つ目のデバイスがファイルのアップロードを完了する前に、2 つ目のデバイスがダウンロードを開始します。別々のコンピュータが 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。
- **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）上の別のコンピュータ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、同期対象となるコンピュータをネットワーク上で見つける機能を担っています。検出対象となるコンピュータは、同じ個人用 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マシンに限られています。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

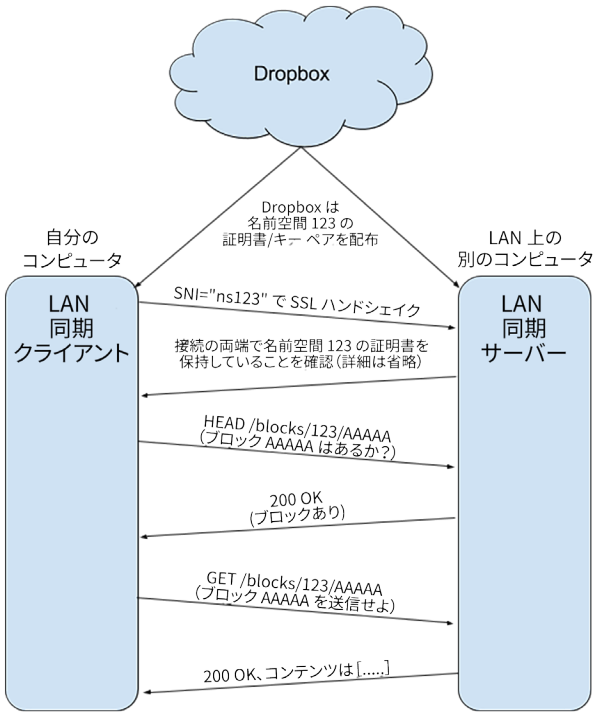
LAN に接続されている各マシンは、ポート 17500 上で UDP ブロードキャスト パケットの送信や受信を定期的に行います（このポートは LAN 同期用に IANA で予約済み）。このパケットには、マシンが使用しているプロトコルのバージョン、対象となる Dropbox の個人 / 共有フォルダ、LAN 同期に使用される TCP ポート（ポート 17500 が使用できない場合は別のポート）、およびランダムに生成されたマシンの ID が含まれています。このパケットを受け取ったマシンは、Dropbox の個人 / 共有フォルダに対応する同期先のリストに IP アドレスを追加します。

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、サーバーはどの証明書を使用するか判断できます。



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のリストを維持します。LAN 同期では、ブロックのダウンロード要求があると、検出結果からピアを任意に抽出して Dropbox の個人 / 共有フォルダへの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に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。

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。

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、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、1 時間ごとの増分バップアップと 1 日 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サーバー上に保管されます。

ファイル コンテンツ

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に独立して格納され、各領域内で確実に複製されます（注：お客様がヨーロッパ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 ブロックはヨーロッパ内でのみ複製されます。後述の「**データ センター**」のセクションをご覧ください）。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、リンクしているコンピュータ上のローカル Dropbox フォルダから最後に同期したファイルのコピーにアクセスすることができます。ダウンタイム中、停電中、オフライン時は、ユーザーのハード ドライブから Dropbox デスクトップ クライアント / ローカル フォルダ内の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次第 Dropbox に反映されます。

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。

- 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および保存する
- 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 27001、およびその他のコンプライアンス監査の一環として監査を受けています。

ビジネスの継続性

Dropbox はビジネス継続計画システム（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、ビジネス継続計画（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。

- **ビジネス継続計画：**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ために役立ちます。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、ビジネス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 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 のインフラストラクチャ 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、解決策が見つかるまで追跡されます。

Dropbox のディザスター リカバリ計画（DRP）では、耐久性と可用性に関す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 コンテンツ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 コンテンツ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、ビジネスの継続性、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。

データ センター

Dropbox の業務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 プロバイダに格納されています。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的 / 環境上 / 運営上の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弊社のインフラストラクチャにおける論理的 / ネットワーク上 / アプリケーション上のセキュリティの管理を担当しています。

Amazon Web Services（AWS）は、一部のファイル コンテンツの処理や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。

ヨーロッパのインフラストラクチャ

ヨーロッパのお客様は、ヨーロッパ内に配置されたストレージにファイル コンテンツを保管できます。インフラストラクチャは、ドイツのフランクフルトに存在する Amazon Web Services によってホスティングされており、冗長性の確保と情報漏洩の防止のためにフランクフルト地域内で複製されています。

製品の機能（セキュリティ、制御、可視性）

Dropbox は IT 担当者とエンド ユーザーがビジネスやデータを効果的に管理できるよう、制御機能と可視性機能を備えています。ここでは、チーム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統合の例を紹介します。

管理者向け機能

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

制御機能

- **管理者役割の階層化：**アカウント管理者に次の 3 つのアクセス レベルを割り当てることで、チームをさらに効果的に管理できるようになります。
  - **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。他のチーム メンバーを管理者にしたり、管理者の役割を変更したりでき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担当できます。チーム メンバーであれば誰でもユーザー管理者になることができます。
  - **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を行うこともできます。
- **ユーザーのプロビジョニング方法**
  - **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（現在は一部のお客様にベータ版として提供）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たり、アカウントを削除したりできます。この機能を統合すると、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 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、作業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 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 統合」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 統合**」のセクションをご覧ください。
- **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:**(Dropbox Enterprise をご利用のお客様のみ)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:**(Dropbox Enterprise をご利用のお客様のみ)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。
- **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。
- **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。SSO 実装により、その他の多要素認証の要件を定めることもできます。
- **パスワードのリセット:**プロアクティブなセキュリティ対策として、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。
- **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を簡単に許可することができます。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、ユーザーが自分のグループを作成して管理できるかどうかを選択できます。管理者は、いつでもユーザー管理グループを企業管理グループに変更して管理することができます。
- **コンピュータ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コンピュータに別の 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。
- **共有の許可:**チーム管理者は、チームが Dropbox を使用して次のような共有を行えるかどうか、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 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。
  - **きめ細かなアクセスと共有管理機能:**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アクセス権限を管理し、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。
  - **同期管理機能:**管理者は会社のコンピュータに自動的に同期するコンテンツを制御できます。
- **完全削除の許可:**Dropbox Business アカウントのチーム管理者は、ファイル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。
- **ウェブ セッション:**管理コンソールと各メンバーのアカウント設定からアクティブなブラウザのセッションを追跡でき、セッションを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コンピュータやモバイル デバイスのリンクを解除できます。コンピュータのリンクを解除すると認証データが削除され、次回そのコンピュータ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あります(詳細は「**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。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。
- **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、コンピュータとモバイル 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、そのユーザーのアカウントに含まれるファイルを他のチーム メンバーに移行できます。
- **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。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。
- **ネットワーク トラフィックの分割（NTS）：**（Dropbox Enterprise をご利用のお客様のみ）管理者は、社内ネットワークでの Dropbox の使用を Enterprise チーム アカウントに限定することができます。この機能を会社のネットワーク セキュリティ プロバイダと統合することにより、社内ネットワーク上の Dropbox トラフィックを検査し、認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することができます。
- **エンタープライズ モビリティ管理（EMM）：**（Dropbox Enterprise をご利用のお客様のみ）Dropbox はサードパーティ EMM プロバイダと連携しているため、Dropbox Enterprise の管理者は、チーム メンバーがモバイル デバイスで Dropbox をどのように利用しているか、より詳細に管理できます。管理者はモバイル アプリで Dropbox Enterprise アカウントにアクセスして使用することを管理対象デバイスのみに制限でき（会社提供または個人用）、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、紛失したデバイスや盗難に遭ったデバイスを遠隔削除することができます。
- **デバイスの承認：**Dropbox の管理者は、ユーザーが Dropbox と同期できるデバイスの数を制限したり、承認の管理をユーザーまたは管理者のどちらが行うかを選択したり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。

可視性

- **アクティビティ フィード：**Dropbox Business は、ユーザーと管理者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に対するユーザーの操作を検証したり、チームのすべてのアクティビティを特定の期間で表示したりできます。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、次のイベントが記録されます。
  - **ログイン：**Dropbox ウェブサイトへのログインの成功または失敗。
    - 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
    - EMM 経由でのログイン試行の失敗またはエラー（Dropbox Enterprise のみ）
    - 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の承認 / 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参加（Dropbox Enterprise のみ）
- アカウント キャプチャによるドメインからのユーザー退会（Dropbox Enterprise のみ）
- チーム メンバーによる新規メンバー提案の有効化 / 無効化
- 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：**コンピュータまたはモバイル 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 コンピュータまたはモバイル デバイス用 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
  - メンバーによる 2 段階認証の無効化のブロック / 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行うチームへの参加リクエストの承認 / 拒否
  - 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 メンバーの名前の変更
  - 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

- チーム外のメンバーが所有する共有フォルダへのメンバー追加のブロック / ブロック解除
- メンバーによるチーム外部のユーザーとのフォルダ共有のブロック / 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たときに表示される警告の有効化
- チーム外のメンバーによる共有リンクの閲覧のブロック / ブロック解除
- 共有リンクの閲覧をチーム メンバーのみにデフォルト設定
- ユーザーによるファイルへのコメント追加のブロック / ブロック解除
- チーム メンバーによるファイル リクエスト作成のブロック / 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 フォルダの管理

- チーム フォルダの作成
- チーム フォルダの名前の変更
- 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ロード

ドメイン管理

- ドメイン検証のテスト、またはドメインの検証 / 削除
- Dropbox Support 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 Enterprise のみ）
- Dropbox Support によるアカウント キャプチャ機能の付与 / 取り消し（Dropbox Enterprise のみ）

エンタープライズ モビリティ管理（EMM）（Dropbox Enterprise のみ）

- 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 リストのチーム 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
- コンピュータへの複数アカウント リンクのブロック / 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 メンバーによるファイル完全削除のブロック / ブロック解除
- リセラーに対する Dropbox Support セッションの開始 / 終了

- **共有：**ファイル、フォルダ、リンクの共有に関するイベント。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の権限の変更
  - グループの追加 / 削除
  - ユーザーの Dropbox への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閲覧
  - ユーザーの Dropbox への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要求
  - 共有フォルダの親フォルダの変更
  - 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 への共有フォルダの追加、または共有フォルダに対するユーザー アクセスの削除
  - 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請求
  - 共有フォルダへのアクセスのリクエスト
  - 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のフォルダへの追加のブロック / ブロック解除
  - フォルダへのユーザー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 アクセスの変更

共有リンク

- リンクの作成または削除
- リンクを持つすべてのユーザーにリンク済みコンテンツの閲覧を許可するか、またはチーム メンバーのみに許可するかの選択
- リンクのコンテンツのパスワード保護
- リンクの有効期限の設定または削除
- リンク済みコンテンツの表示
- リンク済みコンテンツのダウンロード
- ユーザーの Dropbox へのリンク済みコンテンツのコピー
- API アプリによるファイル 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
- チーム外部のユーザーによる共有フォルダ内のリンク済みファイル閲覧のブロック / 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、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

- **グループ:** グループの作成、削除、メンバーシップ情報の変更
  - グループの作成、名前変更、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
  - グループの管理主体をチームまたは管理者に変更
  - グループの外部 ID の変更
- **ファイル イベント:** 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
  - ファイルまたはフォルダの名前の変更
  - ファイルを以前のバージョンに戻す
  - 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
  - ファイルやフォルダの完全削除

- **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ったりアカウント情報を提供したりする前に、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。

ユーザー管理者向け機能

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も用意されています。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。

復元とバージョン管理：Dropbox Business では失われたファイルを復元でき、ファイルの過去のバージョンを無制限に回復できます。重要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。

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、または新しいコンピュータ / 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、通常のパスワードのほかに 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のみに、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 では、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。U2F 準拠のセキュリティ キーでは、暗号通信技術を使用して、フィッシングのような資格情報の盗難からの保護を強化しています。

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、他のユーザーから共有されている個々のファイルも表示されます。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（後述の説明を参照）。
- **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、他のユーザーから共有されているすべてのリンクも表示されます。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（後述の説明を参照）。
- **イベント ページ：**ファイルやフォルダの編集、追加、削除が行われるたびに個々の操作を記録しているログは、このページで確認できます。メンバーシップに関するアクティビティや他のメンバーによる変更など、共有フォルダのアクティビティもこのページで追跡できます。
- **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コンピュータやモバイル デバイスのリストが表示されます。各コンピュータの名前、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、次回オンラインに接続したときにコンピュータ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などが表示されます。アカウントのセキュリティ設定では、任意のセッションを遠隔から終了できます。
- **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、アプリのアクセス許可を取り消すこともできます。

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 と Android デバイスの指紋認証（サポートされている場合）を有効にすることができます。
- **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。
- **内部ストレージと保管されたファイル：**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管されません。Dropbox のモバイル クライアント機能を使うと、ファイルをデバイスに保管して、オフライン状態でも閲覧できるようにすることができます。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、保管したファイル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。

共有ファイルとフォルダの権限

- **共有フォルダの権限：**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、フォルダに対する権限を持たないユーザーへのリンク共有の権限を有効化または無効化することもできます。
- **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。
- **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。

Dropbox Business API 統合

Dropbox Business API とパートナー企業のソリューションを通じて、データやアカウント管理のための以下のセキュリティ ツールを追加できます。

- **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、警告やレポート処理、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ために役立てます。
- **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、電子透かし、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統合することで、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。

Dropbox Business のチーム レベルの機能へのアクセスを開発者に許可することで、管理者はビジネスに欠かせないアプリケーションをチームに導入して管理できるようになります。Dropbox Business では既存のサードパーティ製ソリューションにシームレスに統合する能力が強化されています。特に企業のお客様を意図した便利な機能です。Dropbox Business API の詳細については、後述の「**Dropbox 向けアプリ**」のセクションをご覧ください。

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。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、コンピュータ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 アプリケーションを使用して、Dropbox アカウントに制限なくアクセスできます。Windows/Mac/Linux の各オペレーティング システムに対応しており、各 OS のファイル ブラウザからファイルを直接閲覧したり、共有したりできます。
- **モバイル:**Dropbox アプリは、iOS、Android、Windows、BlackBerry のスマートフォンやタブレット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、オフラインでファイルにアクセスできるように、ファイルをローカル ストレージに保管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。

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、常に 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、強力な暗号を使用し、完全な前方秘匿性（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 cookie に secure 属性を付け、includeSubDomains パラメータ付きで HSTS（HTTP Strict Transport Security）機能を有効にしています。

注意：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が安全に転送されます。

保管されているデータ

Dropbox に保管されているファイルは、256 ビットの Advanced Encryption Standard （AES）によって暗号化されます。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。Dropbox が同期するのは、リビジョン間で変更されたブロックのみです。

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 のファイル暗号化キー管理はユーザーの利益を意図して設計されており、複雑さを排除して、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。ファイル暗号化キーは、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 ポリシーにより作成され、保管、保護されます。

- **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。
- **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、想定されるほとんどの状況や実装環境におけるデスクトップ / モバイル 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なりすましによるものではないことを確認するため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資格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を遅くしています。この手法を採ることで、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。さらに追加の事前対策として、データベースに別途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、共有リンク機能を通じてマルウェアが拡散することを防止する自動スキャン システムを開発しました。このシステムでは、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ています。

Dropbox 向けアプリ

Dropbox 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。Dropbox プラットフォームを基盤として、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が 30 万以上開発されています。

Dropbox API

Dropbox API を使用することで、ユーザーがアプリ内から Dropbox のファイルにアクセスできる機能の開発が可能になり、柔軟な方法で Dropbox の読み取り / 書き込みを行えるようになります。認証、ファイルやメタデータの操作、共有ファイル / フォルダ / リンクの操作、ファイルの操作などは、すべて Dropbox API を通じて処理できます。

Dropbox API を使用するアプリには、次の許可レベルのいずれかを設定できます。

- **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 / 書き込みアクセスが許可され、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をリクエストすることもできます（後述を参照）。
- **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 / フォルダへのアクセスをリクエストすることもできます（後述を参照）。

Chooser と Saver：Chooser と Saver を使用すると、コードを数行記述するだけで Dropbox に簡単にアクセスできます。Chooser は Dropbox のファイルを選択するための機能で、Saver はファイルを直接 Dropbox に保存するための機能です。従来の［開く］、［保存］ダイアログ ボックスに代わって同じ機能を果たし、アプリは、ユーザーが明示的に選択したファイルやフォルダのみに 1 回限りアクセスできます。

Dropbox は業界標準プロトコルの OAuth を認証に使用しているので、ユーザーはアカウントの資格情報を提供しなくても、アプリにアカウント アクセスを許可できます。Dropbox は、すべての 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 Business API

Dropbox Business API を使えば、Dropbox Business アカウント全体をアプリで管理できます。チーム メンバー全員に対して Core API による操作を実行することもできます。アプリは、プログラムを通じて Dropbox Business の管理機能にアクセスできます。具体的には、Dropbox Business の監査ログ、チーム利用状況の統計情報、グループや共有フォルダの管理などの機能を実行できます。

また、Core API コールに加えて、Dropbox Business API には特に企業向けに設計されたエンドポイントが追加されています。ユーザーとグループの情報取得と管理、監査、ウェブフック通知用のエンドポイントなどがあります。

アプリのアクセス許可の種類

Dropbox Business API には 4 種類のアクセス許可があり、それぞれチームとユーザーのデータにアクセスできるレベルが異なります。開発者は、アプリが必要とする最小限のアクセス許可のみをリクエストしてください。

- **Team Information（チーム情報）：**チームと総使用量データに関する情報の閲覧
- **Team auditing（チーム監査）：**チーム情報とチームの詳細なアクティビティ ログの閲覧
- **Team Member File Access（チーム メンバーのファイル アクセス）：**チーム情報と監査情報の閲覧、チーム メンバーとしての任意の操作の実行
- **Team Member Management（チーム メンバーの管理）：**チーム情報の閲覧、チーム メンバーの追加、編集、削除

Dropbox API と同様、Dropbox Business API では API リクエストの認証に OAuth 2.0 を使用しています。Dropbox Business API の OAuth トークンを使用することで、アカウント データに対する広範なアクセスを実現できます。OAuth レスポンスには team_id フィールドが追加されます。OAuth トークンをサーバー側で適切に保護し、トークンが安全でない環境にキャッシュされたりクライアント デバイスにダウンロードされたりしないようにするのは開発者の責任です。開発者は標準的な OAuth 2.0 フローに基づき、Dropbox Business アカウントにアプリケーションをインストールする指示を Dropbox Business アカウントの管理者に伝える必要があります。

Dropbox API の詳細については、**dropbox.com/developers** をご覧ください。

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、Dropbox 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、Dropbox 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および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。

API パートナーシップ

Dropbox はこれまでパートナーと緊密な連携を図り、普及しているソフトウェア パッケージとの統合機能を開発してきました。こうした統合機能によって実現したインターフェースを通じて Dropbox 内のデータにアクセスできるので、エンド ユーザーは両方のサービスをシームレスかつ安全に利用できます。

- **モバイル / ウェブ版 Microsoft Office：**Dropbox の Microsoft Office 統合機能を利用すれば、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 および Acrobat Reader：**Dropbox はデスクトップ版およびモバイル版（Android および iOS）Acrobat アプリと統合されており、Dropbox に保存された PDF ファイルを閲覧、編集、共有することができます。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。PDF の変更内容は自動的に Dropbox に保存されます。

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
- 業務ネットワーク

Dropbox のプロダクション環境へのアクセスは承認された IP アドレスのみに限定されており、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 の業務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、承認されたユーザーのみに限定されています。

インターネットから Dropbox プロダクション環境へ向かうトラフィックは、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、同様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 のラップトップ / デスクトップ コンピュータとプロダクション 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 ログはすべて 1 か所に集められ、業界標準の保持ポリシーに従って、フォレンジック解析とインシデント対応が行われます。

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 がホストするポイント オブ プレゼンス（PoP）を、カリフォルニア、テキサス、バージニア、ニューヨーク、ワシントン、英国、オランダ、ドイツ、日本、シンガポール、および香港で活用しています。これらの場所にはユーザー データはキャッシュされず、転送されるすべてのデータは 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

Dropbox は自律システム AS19679 を使用して運用されており、インターネット サービス プロバイダとの間でネットワーク ピアリングに関する協定を結んでいます。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。

Dropbox とのピアリングでは、お客様のネットワークを宛先とするか、またはネットワークを経由する 50 Mbps 以上の大陸内トラフィックが必要です。また、すべてのパブリック ピアリング リクエストについて、適切な書式で記述されたファブリックのパブリック アドレス、AS 番号、NOC またはピアリング先の連絡先情報など、データ交換のための情報を最新の PeeringDB に登録する必要があります。

Dropbox では、各ピアにプライベート ピアリング施設の詳細情報を保持するように求めています。この情報をプライベート ピアリング（PNI）の宛先設定に使用するためです。

脆弱性の管理

Dropbox のセキュリティ チームは、自動および手動によるアプリケーションのセキュリティ テストを定期的に実施し、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て修正しています。

セキュリティ担当者はこれらのアクティビティによって得られた情報を評価し、セキュリティ チームの評価に基づいて優先順位を割り当てます。Dropbox では、情報セキュリティ管理システムのひとつの要件として、上記すべてのセキュリティ評価アクティビティの調査結果と推奨事項をマネジメント チームに報告し、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 / 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

Dropbox エンジニアリング チームは公式な変更管理ポリシーを定義し、すべてのアプリケーション変更は承認を得なければプロダクション環境に導入できないと定めました。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は、ソース コードを変更します。すべての変更はバージョン管理システムに保管され、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すべての変更は、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すべての変更内容はログに記録されるとともにアーカイブされ、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守り、業界標準に基づいて、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の状態に保つ責任があります。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、モバイル用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、業務環境および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 リサーチ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、これ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、および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。

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ほかに、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、責任を持ってソフトウェアのバグを開示し、報告の一元化に協力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。

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。

- セキュリティの問題の詳細を Dropbox と共有します。
- 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。
- Dropbox サービスのパフォーマンス低下（サービス妨害を含む）が生じないよう、誠実な対応をお願いします。

問題は、HackerOne（**hackerone.com/dropbox**）経由で報告できます。

Dropbox の情報セキュリティ

Dropbox は、情報セキュリティの管理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、内部および外部からのリスク評価も行っています。

Dropbox のポリシー

Dropbox では、情報セキュリティ、物理セキュリティ、インシデント レスポンス、論理アクセス、物理プロダクション アクセス、変更管理、およびサポートの領域を対象とした綿密なセキュリティ ポリシーを設けています。これらのポリシーは年に 1 回以上見直し / 承認され、Dropbox セキュリティ チームにより施行されます。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:** ユーザーおよび Dropbox の情報に関するポリシーで、主にデバイス セキュリティ、認証要件、データとシステムのセキュリティ、ユーザー データのプライバシー、社員によるリソースの使用に関する制限とガイドライン、潜在的な問題への対処方法などを含みます。
- **ユーザー データのプライバシー:** Dropbox のプライバシー ポリシーに従い、ユーザーの情報とデータを保護し、取り扱う上での要件が定められています。
- **物理セキュリティ:** Dropbox がユーザーやアセットを保護し、安全性を維持するための手順が含まれています（後述の「**物理セキュリティ**」のセクションをご覧ください）。
- **インシデント レスポンス:** セキュリティの潜在的な問題に対応するための Dropbox の要件で、評価、コミュニケーション、調査の手順などが含まれます。
- **論理アクセス:** Dropbox のシステム、ユーザー情報、Dropbox の情報を保護するためのポリシーで、Dropbox の業務環境およびプロダクション環境へのアクセスを制御する手順が含まれます。
- **物理プロダクション アクセス:** 物理プロダクション ネットワークへのアクセスを制限するための手続きで、管理者による社員の審査や退職した社員の認証取り消しなどを行うための手順が含まれます。
- **変更管理:** コード審査や変更管理を行うためのポリシーで、認定を受けている開発者が、アプリケーションのソース コード、システム設定、プロダクション リリースに対してセキュリティに影響を与える変更を行った際などに適用されます。
- **サポート:** アカウント情報の閲覧、サポート提供、対応などのために Dropbox サポート チームがユーザーのメタデータにアクセスする際のポリシーです。

- **ビジネスの継続性：**障害が発生したときにビジネスに不可欠な機能を維持または復元するためのポリシーと手続きです。計画から文書化、実施までが含まれます。
- **危機管理：**Dropbox の最も重要な業務を停止させるか、または戦略的目標を脅かす恐れのある異常事態が広範囲に及ぶ場合に、どのように対処するかを示したポリシーと手続きです。

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 の業務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 要素認証、OTP トークンの組み合わせが使用されます。リモート アクセスする場合は 2 要素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。

業務環境およびプロダクション環境の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許可が付与されます。アクセス許可のリクエスト、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許可が付与されます。

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 ファイルの保管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許可が取り消されます。

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。

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 が承認したユーザーが職務のために必要な場合にのみ制限されています。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ユーザーには、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。

アクセス許可のリクエスト、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許可が付与されます。承認後はインフラストラクチャ チームの責任者が該当するサブサービス組織に連絡し、承認されたユーザーのアクセス許可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ユーザーの情報を入力し、承認された Dropbox ユーザーにバッジ アクセス（可能であれば、生体認証によるアクセス）を付与します。承認されたユーザーにアクセスが許可された後は、データ センターが責任を持って、そのアクセス許可が承認済みユーザーのみ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 の業務環境およびプロダクション環境への物理的なアクセス許可を承認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。

コンプライアンス

企業に適用されるコンプライアンスの規格や規制は多数ありますが、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し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、テクノロジー、システム、アプリケーション、人員、およびプロセスは、オランダを拠点とするサードパーティの独立企業、EY CertifyPoint からの ISO 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）からの ISO 認定を取得しています。

ISO 27001（情報セキュリティ）

ISO 27001 は世界中で認められている情報セキュリティ管理システム（ISMS）の最高基準で、ISO 27002 で詳細に規定されているベスト プラクティスを活用しています。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、および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、Dropbox Enterprise、および Dropbox Education の ISO 27001 証明書は、こちらでご覧になれます。

ISO 27017（クラウド セキュリティ）

ISO 27017 は、クラウド セキュリティに関する新しい国際規格です。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基準については、「**共有責任ガイド**」をご覧ください。

Dropbox Business、Dropbox Enterprise、および Dropbox Education の ISO 27017 証明書は、こちらでご覧になれます。

ISO 27018（クラウド プライバシーとデータ保護）

ISO 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新たな国際規格です。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、Dropbox Enterprise、Dropbox Education の ISO 27018 証明書は、こちらでご覧になれます。

ISO 22301（ビジネスの継続性）

ISO 22301 は、ビジネスの継続性に関する国際規格です。組織のサービス中断の発生を抑え、万が一サービスが中断する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、ビジネス継続計画システム（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、Dropbox Enterprise、Dropbox Education の ISO 22301 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、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、運用、プロセス、およびテクノロジーに関する認証を受けています。

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 つの信用提供原則であるセキュリティ、機密性、処理の完全性、可用性、プライバシー（TSP セクション 100）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、Dropbox Enterprise、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 つの信用提供原則であるセキュリティ、機密性、処理の完全性、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。SOC 2 レポートには、Dropbox がお客様のデータを保護する上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に対するテスト手順とそれらの結果報告も記載されています。Dropbox Business、Dropbox Enterprise、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 16/ISAE 3402（旧 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、Dropbox Enterprise、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。独立した第三者機関による監査は、保証業務基準書第 16 号（SSAE 16）および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、廃止予定の監査基準書第 70 号（SAS 70）に代わって取り入れられています。Dropbox Business、Dropbox Enterprise、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**。

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、Dropbox Enterprise、Dropbox Education は CSA STAR のレベル 2 認証を受けています。これは ISO 27001 の要件およびクラウド サービスの性能レベルの測定条件である CSA Cloud Controls Matrix(CCM)v.3.0.1 に則って行われる、独立した第三者機関(EY CertifyPoint)による Dropbox のセキュリティ管理に関する評価です。Dropbox Business は CSA の Consensus Assessments Initiative Questionnaire（CAIQ）に基づいた厳しい調査である CSA STAR レベル 1 の自己評価も完了しています。これは CCM に則って、クラウドの利用者やクラウドのセキュリティ監査法人からの約 300 の質問に対する回答を紹介しています。

Dropbox の CSA STAR レベル 1 の自己評価およびレベル 2 証明書は CSA ウェブサイトでご覧になれます。

HIPAA/HITECH

Dropbox は、事業提携契約書（BAA）を、必要とする米国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。

Dropbox は、Dropbox Enterprise、Dropbox Enterprise、または Dropbox Education の使用において HIPAA/HITECH のセキュリティおよび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、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は、Dropbox のセールス チーム（**sales@dropbox.com**）にお問い合わせください。また、現在お客様が Dropbox Business チームの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。

詳細については、Dropbox の **HIPAA スタート ガイド**をご覧ください。

学生と児童（FERPA と COPPA）

Dropbox Business、Dropbox Enterprise、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（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づ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、Dropbox Enterprise、Dropbox Education を利用することができます。

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 Enterprise、Dropbox Education はクレジット カードの取引を処理または保管するように設計されていません。Dropbox では、お客様のリクエストに応じてマーチャント ステータスの PCI 準拠証明書（AoC）を提供しています。ご希望のお客様は、Dropbox のセールス チーム（**sales@dropbox.com**）または**管理コンソール**の［アカウント］ページを通じて行うことができます。

Dropbox Business、Dropbox Enterprise、Dropbox Education のコンプライアンスについての詳細

dropbox.com/business/trust/compliance でご覧になれます。

プライバシー

Dropbox は重要なファイルの日常的な保存先として、多くのユーザーと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ファイル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、業務契約、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

ISO 27018

Dropbox Business 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に関する新たな国際規格である ISO 27018 の認定基準をいち早く満たしました。ISO 27018 は、特にユーザーのプライバシー保護を目的に策定され、2014 年 8 月に公開されました。この規格では、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 に保存するファイルの追加、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、Dropbox が介入することはありません。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の削除に伴う情報の取り扱い方法についてお知らせします。これらの内容が変更された場合も通知いたします。
- **お客様のデータは安全に保護されます。**ISO 27018 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 27001 を強化するために策定されました。Dropbox は 2014 年 10 月に ISO 27001 認証を受けており、さらに、暗号化や社員の厳格なアクセス管理など ISO 27018 におけるセキュリティとプライバシーに関する要件にも並行して準拠しています。
- **Dropbox の実践方法は実証されています。**ISO 27018 と ISO 27001 に準拠するための実践の一環として、Dropbox では、認定を維持するために年に 1 回、独立した第三者機関による監査を実施いたします。Dropbox の ISO 27018 証明書は、**こちら**でご覧になれます。

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 サービス会社には、政府から受け取ったデータ開示要請の件数、要請により影響を受けるアカウントの数、および要請の根拠となる法律について、正確に報告することが許可されるべきです。Dropbox はこれらの重要情報を提供するために、この権利を継続的に主張しています。
- **一括要請の拒否：**政府によるデータ要請は、特定のユーザーおよび調査に限定されるべきです。Dropbox は、大規模なユーザー集団を対象にした要請や、特定の調査に関連しない情報を求める要請には応じていません。
- **すべてのユーザーの保護**オンライン サービス会社に対して政府がユーザー データを要請することを許可する法律では国籍や居住場所に基づいてユーザーの扱いが区別されるべきではありません。Dropbox は、このような法律の改定を求めるために尽力しています。
- **信頼されるサービスの提供：**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。

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。

EU - 米国間のプライバシー シールド / 米国 - スイス間のセーフ ハーバー

Dropbox は、欧州連合、欧州経済地域、およびスイスからデータを転送する場合、ユーザーとの契約を含むさまざまな法的枠組みを遵守しています。また、Dropbox は、欧州連合に居住するユーザーの個人データの収集、使用、保持に関してアメリカ合衆国商務省および欧州委員会により定められている欧州連合 / 米国間のプライバシー シールド プログラム（「プライバシー シールド」）フレームワークの認証を受け、同原則に準拠しています。上記に加えて、Dropbox は、アメリカ合衆国商務省およびスイスの連邦データ保護および情報委員会により定められている米国 / スイス間のセーフ ハーバー（「セーフ ハーバー」）フレームワークの認証を受け、これに準拠しています。Dropbox のプライバシー シールド証明書は **www.privacyshield.gov/list**、セーフ ハーバー証明書は **safeharbor.export.gov/swisslist.aspx** でご覧になれます。また、プライバシー シールドの詳細については **www.privacyshield.gov**、セーフ ハーバーの詳細については **2016.export.gov/safeharbor/swiss/** でご覧になれます。

組織は、プライバシー シールドとセーフ ハーバーの原則を遵守することにより、EU データ保護指令に基づいて十分なプライバシー保護を提供していることを証明できます。Dropbox のプライバシー シールドおよびセーフ ハーバー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 を通して調査および解決されます。

詳細については、プライバシー ポリシー（**dropbox.com/privacy**）をご覧ください。

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、コンプライアンス、プライバシー保護を強化して Dropbox を機能拡張し、今後も成長し続けます。

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、処理の完全性、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。

まとめ

Dropbox Business は、チームで効率良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、セールス チーム（**sales@dropbox.com**）にお問い合わせください。

Dropbox Business について

Dropbox を利用すれば、ドキュメント、写真、動画をどこにでも持ち歩け、簡単に共有することができます。複数のデバイスで常に最新のファイルを利用でき、チームとの同期も容易に行うことができます。Dropbox Business には管理ツールも用意されており、ビジネスが必要とする十分な容量をご提供します。