Dropbox Business

共有責任ガイド：データの安全性を確保するための Dropbox とお客様の連携について

Dropbox は、Dropbox Business および Dropbox Education のお客様と協力して、データの安全性の確保に取り組んでいます。インフラストラクチャ、ネットワークおよびアプリケーションの保護、セキュリティとプライバシー対策における社員トレーニング、信頼に応えることを最優先する社風の構築、システムと実践内容に対する厳格な第三者機関によるテストと監査など、Dropbox は包括的なセキュリティ対策を講じています。

弊社の管理下にあるサービスの各要素で安全性を守ることは Dropbox の責任です。一方、チームとそのデータを保護して安全性を確保するという点では、お客様の役割が重要になります。Dropbox は、お客様が組織のセキュリティ、プライバシー、およびコンプライアンス要件を満たせるように、Dropbox Business または Dropbox Education チームの管理者にアカウントの設定、使用、監視に役立つ機能を提供しています。

このガイドでは、アカウントの安全性を確保するために Dropbox が責任を担うこと、そしてチームのデータに対する可視性と制御を維持するためにお客様が実施できることについて説明します。

Dropbox の責任

セキュアなアーキテクチャを採用

世界中の数多くの企業が、社内の最も重要なコンテンツの保護を Dropbox に委ねています。その信頼に応えるために、Dropbox は管理者が安心して使用できる安全なサービスの開発に尽力しています。Dropbox では、アーキテクチャとネットワークに対して以下のようなセキュリティ対策を採用しています。

分散型アーキテクチャ

Dropbox は、複数のサービスにさまざまなレベルの情報を分散するアーキテクチャを採用しています。これにより、同期の迅速化と信頼性の向上だけではなく、セキュリティの強化も実現しています。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や Paper ドキュメントを複製することはできません。

セキュアなネットワーク

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。本番環境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 の本番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。

ユーザー データの暗号化

Dropbox Business および Dropbox Education のお客様は、モバイル、デスクトップ、ウェブ アプリケーション、API を介して Dropbox のシステムとデータをやり取りしています。Dropbox は、お客様が使用しているアプリの種類を問わず、転送中と保管中の両方のファイルおよび Paper ドキュメントを保護します。

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。

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

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。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 Paper ドキュメントも同様に、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。

信頼性の高いサービスの維持

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 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 3 日に 1 回、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 ブロックの格納には、社内のシステムとサード パーティのシステムを使用しており、どちらも 99.999999999 % 以上の年間データ耐久性を提供するように設計されています。

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、停止中、オフライン時は、ユーザーのハード ドライブの Dropbox デスクトップ クライアント/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。

同様に、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、完全バックアップを毎日行うように設定されています。Dropbox では、Paper ドキュメントの格納に、99.9999999999 % 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サードパーティのシステムを使用しています。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。

バックエンド システムへの社員のアクセス制限

Dropbox Business または Dropbox Education のお客様が Dropbox にファイルや Paper ドキュメントを保管するのは、Dropbox が責任を持ってデータを管理するという期待をお持ちであるがゆえだと理解し、この責任の一端として、Dropbox では弊社の社員に対し社内システムへのアクセスを厳しく統制しています。まず、業務ネットワークと本番環境ネットワーク間のアクセスに対して厳しい制限を設けています。たとえば、Dropbox の本番環境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。データ センター、サーバー設定ユーティリティ、本番環境サーバー、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。

セキュリティとプライバシーに対する社員の意識の向上

サービスの安全性を確保する対策の一環として、Dropbox の社員にはセキュリティ意識と不審なアクティビティを認識する能力が求められています。そのため、Dropbox の社員はセキュリティ ポリシーを理解していなければ、システムへのアクセスを許可されません。社員は、新規採用者向けのセキュリティおよびプライバシーの必須トレーニングに参加し、年 1 回のフォローアップ トレーニングを受講しています。それだけではなく、セキュリティ情報に関するメール、ミーティング、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訓練も日常的に受けています。

Dropbox の実践方法の実証

Dropbox では、セキュリティ対策が意図したとおりに実践されていることを証明するために、その有効性の評価を第三者機関に依頼しています。Dropbox の業務環境および本番環境に対して、専門家が定期的に侵入テストと脆弱性テストを実施しています。問題が特定されると、優先事項として、セキュリティ エンジニアリング チームが問題の修正にあたります。さらに、第三者監査機関が Dropbox のセキュリティ実践方法を国際的な業界標準と照らし合わせて評価を行っています。Dropbox の評価の詳細については、SOC 3 レポート、ISO 27001、ISO 27017、ISO 27018、ISO 22301 の各証明書をオンラインで公開しています。また、SOC 2 レポート、HIPAA 要件の対応付けと評価レポート、BSI C5 の評価とレポート（英語とドイツ語のみ）、侵入テストの結果の要旨については、機密保護契約（NDA）の下でご要請いただけます。

問題の通知

サービス状況

Dropbox Business および Dropbox Education のお客様は、サードパーティのサイト(status.dropbox.com)を通じて、Dropbox のサービス状況を確認できます。このサイトにアクセスすることで、いつでも現在のサイト状況、過去の問題とメンテナンス情報を参照できます。

違反の通知

Dropbox では、適用される法律の定めるところにより、データ違反の発生を通知します。Dropbox は、インシデント対応ポリシーや違反通知プロセスなどの手順を定めており、影響の及ぶお客様に必要に応じて連絡を行える体制を整えています。HIPAA 事業提携契約または EU データ処理契約を結ばれている場合は、それらの契約に記載されているように通知が送られます。

セキュリティに必要なツールの提供

Dropbox Business および Dropbox Education の管理者がチームのセキュリティについて情報に基づいた責任のある意思決定を行えるように、Dropbox は必要なツールを提供しています。管理コンソールには、お客様がニーズを満たす形でアカウントの設定、使用、監視を実施できるように、代理操作が可能なセキュリティ機能が搭載されています。また、アカウントの設定や責任について理解を深めていただくために、本書のようなガイド、Dropbox Business のセキュリティに関するホワイトペーパー、ヘルプセンター、サポート チームにより有益な情報を提供しています。

お客様の責任

Dropbox のセキュリティ対策の理解

Dropbox Business または Dropbox Education が社内のニーズに適したソリューションかどうかを判断することは重要なプロセスです。Dropbox では、他のアプリケーションの場合と同じように、お客様に時間を取って Dropbox の実践内容を検証していただくことをお勧めしています。Dropbox のセキュリティ対策を確認する材料として、ISO 27001、ISO 27017、ISO 27018、ISO 22301 の各証明書、SOC 3 保証報告書、CSA STAR Level 1 セルフ アセスメント、Level 2 証明書をオンラインで提供しています。また、お客様が情報に基づく意思決定を行えるように、機密保持契約の下で他のドキュメントも提供しています。これには、SOC 1 および SOC 2 評価レポート、C5 評価レポート（英語とドイツ語）、Dropbox の社内での慣行と推奨事項との対応付け（HIPAA/HITECH のセキュリティ、プライバシー、および違反通知規定の要件順守について確認を求めるお客様向け）、最新のアプリケーション侵入テストの要旨が含まれます。さらに、Dropbox Business または Dropbox Education がお客様のチームに最適なソリューションであることを確認していただけるように、Dropbox の利用規約、適正利用規定、標準の Business 契約書をオンラインで公開しています。

共有許可および閲覧許可の設定

Dropbox Business および Dropbox Education では、セキュリティ、共同作業、およびプライバシー要件に沿ったアカウントを柔軟に設定できます。管理者は、管理コンソールからこれらの設定を確認および変更することで、組織の共有/規制環境に対応できます。たとえば、フォルダ、リンク、Paper ドキュメントがチーム外の人と共有されないようにアカウントを設定することができます。チーム メンバーは、Dropbox でファイルを管理するために共有フォルダを作成し、さらに設定をカスタマイズして、編集可能または読み取り専用といった適切なアクセス レベルを設定できます。

認証の強化

強力な認証対策により、チームのデータの安全性を確保できます。管理者は、認証設定を確認し、アカウントの保護に最適な設定を行う必要があります。Dropbox Business および Dropbox Education のアカウントでは次の設定が可能です。

2 段階認証

チーム管理者は、アカウントへのログインに対しメンバーに 2 段階認証を課すことができます。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。ぜひご利用ください。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、通常のパスワードの他に 6 桁のセキュリティ コードまたはセキュリティ キーが必要になります。

シングル サインオン (SSO)

お客様の会社が 1 つのアイデンティティ プロバイダによる認証とパスワード ポリシー管理を採用されているのなら、Dropbox Business または Dropbox Education チームにシングル サインオンを設定するとよいでしょう。既存の SSO プロバイダを使用するので、チーム メンバーが新たなパスワードを覚える必要がなくなります。さらに有用なのが、Dropbox へのアクセスの認証を社内の他のサービスと同じパスワード ポリシーを使って管理できる点です。

定期的なアクセス確認の実施

チームのアカウントへのアクセス権限は、チームのメンバーシップ、社内の役割、デバイスの変更に応じて更新する必要があります。適切な情報管理を行うために、アカウントへのアクセスを許可するユーザー、デバイス、アプリの適合性を頻繁にチェックしてください。アクセス権限の変更と削除は、管理コンソールから簡単に実行できます。

チーム メンバー

チーム メンバーの追加、削除、確認は、管理コンソールから簡単に行えます。Dropbox Business または Dropbox Education のアカウントに保管された機密データにアクセスできるユーザーを適切に管理するために、メンバー リストを頻繁に確認することをお勧めします。退職するユーザーや、職務の変更によりアクセスが不要になるユーザーがいる場合は、権限を削除できます。また、各ユーザー アカウントのアクセス レベルを適切に保つ手段として、管理コンソールでチーム メンバーの役割を変更することもできます。

デバイス

管理者とチーム メンバーはアカウントにリンクされているデバイスを頻繁に確認し、使用されなくなったデバイスや権限のなくなったデバイスがあれば、そのデバイスのリンクを解除する必要があります。デバイスの解除は、チーム メンバーとチーム管理者のどちらでも実行できます。また、管理者やチーム メンバーは、リンクの解除に伴い、デバイスから Dropbox のコンテンツを遠隔削除することもできます。リンク解除と遠隔削除によって、デバイスの紛失や盗難、あるいはチームを離れるユーザーに対してデータの安全性を確保できます。

サード パーティ製アプリ

サードパーティ製アプリと Dropbox Business または Dropbox Education アカウントをリンクして機能を追加すると、強力なエコシステムを実現できます。SIEM、DLP、アイデンティティ管理などのサービスの統合は、既存のセキュリティ対策を強化する強力なツールになります。なお、これらのサードパーティ製アプリと統合はアカウントを強化できる優れた方法ですが、Dropbox のサービスではありませんので、その点はご留意ください。そのため、これらの内容は、貴社が Dropbox と交わした Dropbox の利用規約、Business 契約書、事業提携契約、データ処理契約などには記載されていません。アプリについては、サービス内容によって、データへのさまざまなレベルのアクセス権限が必要になる場合があります。管理者は、アカウント全体に適用されるように、チームにアプリのリンクや削除を行えます。また、チーム メンバーが自分のアカウントに追加した個々のアプリを削除することができます。サードパーティ製アプリとアクセスについては、管理コンソールから確認して変更することができます。

異常なアクティビティの監視

チーム管理者は、チームのファイル イベント、共有、認証、管理者のアクティビティについて詳細を記録したレポートを閲覧し、それをエクスポートすることができます。管理者は、このアクティビティ レポートを定期的に確認して異常なアクティビティがないかチェックし、チームの安全性を確保する必要があります。サードパーティ製の SIEM やその他の監視ツールと統合して機能を強化することも検討するとよいでしょう。

暗号化ニーズの見極め

Dropbox は、デフォルトでファイルをローカルのパソコンに保管し、必要なファイルをいつでも使える状態にしています。ローカルに保管されたファイルは、コンピュータ上の他のファイルと同じように保護されます。そのファイルの安全性を確保するには、可能な限りデバイスのディスクを暗号化すること、そして Dropbox アカウントにアクセスできるノート パソコン、スマートフォン、タブレットなどのデバイスに強力な固有のパスワードを設定することをお勧めします。デバイスに強力な固有のパスワードを設定することで、Paper ドキュメントへのアクセスも保護できます。

Dropbox は、アカウントにアップロードされたファイルを自動的に複数のブロックに分割し、各ブロックを 256 ビットの Advanced Encryption Standard（AES）で暗号化することでファイルを保護します。同様に、永続的なストレージに保管されている Paper ドキュメントも 256 ビットの AES で暗号化して保護します。Dropbox は、お客様に代わって暗号化キーを管理することで、このプロセスに対するユーザーの負担を軽減し、特定の機能を有効にしています。

Dropbox Business および Dropbox Education のメンバーは、自分で、またはサードパーティ製品との統合によって、Dropbox にアップロードする前にファイルを暗号化することもできます。ただし Dropbox へのアップロード前にデータを暗号化する場合は、ユーザーが暗号化キーの管理に責任を担うことになります。また、Dropbox へのアップロード前にデータを暗号化すると、一部の機能を使用できなくなる可能性もあります。

Dropbox のセキュリティ対策に関する詳細は、セキュリティに関するホワイトペーパーまたは Dropbox ウェブサイト(dropbox.com/business/trust)でご覧いただけます。Dropbox Business や Dropbox Education の詳細、または機密保護契約下での第三者機関による監査レポートが必要な場合は、sales@dropbox.com にお問い合わせください。