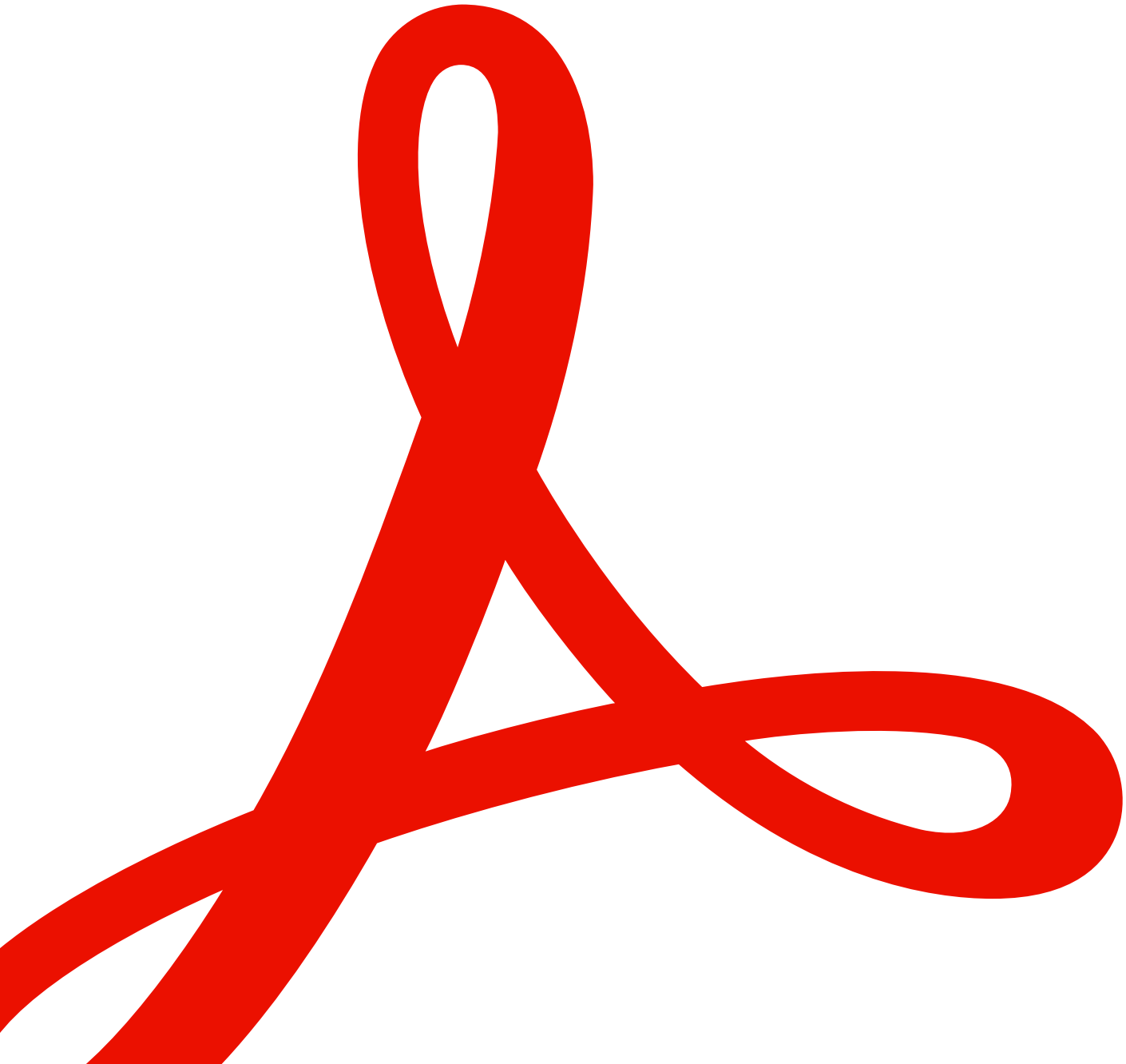
Adobe Document Cloud

Adobe

ホワイトペーパー

Document Cloud サービスがプラスされた Adobe Acrobat のセキュリティ概要



目次

アドビセキュリティ

アドビにとって、デジタルエクスペリエンスのセキュリティは重要な課題です。ソフトウェア開発・運用のプロセスおよびツールに徹底したセキュリティ対策を施すとともに、部門の枠を超えたチームが厳密なセキュリティ基準に従ってインシデントの防止、検知、および迅速な対応に努めています。さらに、パートナー、第一線の研究者、セキュリティ研究機関、その他の業界団体と協力して、最新の脅威や脆弱性を把握し、提供する製品・サービスに高度なセキュリティ技術を随時組み込んでいます。

このホワイトペーパーでは、Adobe Acrobat、Document Cloudサービスと関連データのセキュリティ強化策について、アドビが採用している多層防御アプローチとセキュリティ手順を説明します。

Document Cloudサービスがプラスされた Acrobatの概要

Document Cloudサービスがプラスされた Acrobatは、すべてがネットワークでつながる現代のマルチデバイス環境に最適な、PDF活用のトータルソリューションです。Acrobatデスクトップ版、Adobe Acrobat Readerモバイル版アプリ（有償のプレミアム機能が利用可能）、Document Cloudサービスを組み合わせて利用すると、スマートな文書ワークフローを構築し、様々なデバイスを併用する環境全体のセキュリティを確保しつつ、エンドユーザーのモバイルソリューション需要に対応できます。

Acrobatと Document Cloudサービスには、事実上あらゆるコンテンツを電子文書に変換して共有可能にする力があります。Acrobatのクラウドサービス、デスクトップアプリ、モバイルアプリを使って、PDFの自動生成、加工、変換を簡単に実行できます。

Acrobatのユーザーエクスペリエンス

Document Cloudサービスは多彩な Acrobatユーザーエクスペリエンスと組み合わせて活用できます。

- Acrobat Pro — ノートパソコン／デスクトップユーザー向けのデスクトップ版アプリ
- Acrobatオンライン — Chrome、Microsoft Edge、Firefox、Safariなど、デスクトップ用／モバイルデバイス用の対応ブラウザーで動作するwebアプリ
- Acrobat Readerモバイル版クライアント — Apple App Storeと Google Playから無料でダウンロードできる、モバイル用／タブレット用アプリ

また、Acrobatは各種の Microsoft生産性向上ツールとも連携して機能します。そうした連携ソリューションのドキュメントストレージは、スタンドアロンの Acrobatで利用できるストレージとは異なる形で機能します。連携ソリューションごとのセキュリティに関しては、「Acrobatと Microsoftの連携」セクションに詳しい情報を示します。

Document Cloudサービス

Adobe Document Cloudサービスは以下のサービス要素で構成されています。

- PDFの送信 — 電子メールクライアントを使用し、PDFを送信
- PDFの整理 — PDF内のページを挿入、削除、並べ替え、回転
- PDFの作成 — Word、Excel、PowerPointの文書、画像、写真をPDFに変換
- PDFの書き出し — PDFを変換し、編集可能なMicrosoft Word、Excel、PowerPoint、RTFファイルとして書き出し
- PDFの編集 — 既存のPDFをモバイルデバイスやPCで編集
- PDFの結合 — 複数のPDFを1つに結合する操作やドキュメントパッケージの構築操作を、どこからでも実行
- 入力と署名 — フォームに記入し、署名を追加
- Adobe Scan — 種類を問わずコンテンツを取り込み、高品質な検索可能PDFに変換
- Adobe Acrobat Sign — 信頼できる電子署名処理に対応した文書の作成、送信を実現し、従来の署名ワークフローをクラウド対応のデジタル署名に切り替え

アドビは現在もDocument Cloudサービスの内容を拡充し続けています。Document Cloudサービスの最新の詳しい内容については、Adobe.comでお確かめください。

Acrobatの文書セキュリティ機能

墨消し

Adobe Document Cloudサービスには機微情報や秘密情報を保護するための墨消しツールが含まれており、保護が必要なテキストとグラフィック画像の両方を復元不可能な形で完全に削除してから文書を配布することができます。また、パターンにもとづいて電話番号、クレジットカード番号、電子メールアドレスなどを検索し、墨消し処理することもできます。単に削除マークを付けて見かけ上のマスクをかける一般的なツールの場合と違い、墨消しの対象となった情報はファイル内から完全に削除されます。非表示情報の削除機能により、PDF内のメタデータなど、見えない形で格納されている非表示情報やグラフィック以外のオブジェクトも削除できます。

ファイル共有

Document Cloudファイルをクラウド内に保存すると、アップロードしたユーザー本人のみが表示可能であることを示す「プライベート」というラベルが付加されます。アップロードしたエンドユーザーが明示的にそのコンテンツを共有する操作をおこなわない限り、プライベートのままとなります。Document Cloudコンテンツの共有操作は、そのDocument Cloudコンテンツへのリンクを共有相手に送信するという方法で実行されます。

Document Cloudサービスのユーザーは、ファイルの共有オプションとして「表示のみ」、「レビュー」のいずれかを選択できます。「表示のみ」の制限付きでリンクを送信した場合は読み取り専用文書となり、受信者にはコンテンツの閲覧だけが許可されます。一方、「レビュー」用に文書を送信した場合、受信者は文書に注釈を加えることができます。ただし、コンテンツ自体の編集や変更はできません。受信者へのリンク送信手段としては、電子メール、テキストメッセージ、任意のコラボレーションソフトウェアを使用できます。

図1：Document Cloudサービスのアセット設定

Document Cloudに保存したコンテンツに対しては、Adobe Admin Consoleのアセット設定から共有制限を適用することもできます。この機能を利用すると、公開リンク共有の無効化と、DC共同作業機能の有効範囲を自社ドメインおよび許可された外部ドメインのみに制限する管理操作がエンタープライズIT部門レベルで可能になります。共有制限を適用すると、リンクの受信者がアクセスするにはログインが必要になります。「ドメインユーザーとのみ共有する」モードを有効にすると、ユーザーがコンテンツを共有できる相手は、組織内の他のユーザーと信頼できる外部ドメインのユーザーのみに限定され、外部との共有は完全に無効化されます。

Microsoft Purview情報保護

Microsoft Purview情報保護（MPIP）は、Microsoftが提供している権利保護ソリューションの1つです。Azure Information Protectionと他のMicrosoft Purview情報保護ソリューションを利用するユーザーは、AcrobatまたはAcrobat Readerで、ラベル付きコンテンツや保護されたコンテンツを閲覧できます。Acrobat Pro／Standardの最新のデスクトップバージョン（バージョン22.003.20258以降）からは、プラグインや個別のインストールをおこなわなくても、ネイティブ環境でPDFに情報保護の秘密度ラベルとポリシーを適用および編集できるようになりました。

保護モード

ある種の悪質なコードには、PDF形式を利用してコンピューターファイルシステムの書き込みや読み取りを試みる機能が組み込まれています。そのようなコードからユーザーを保護するために、アドビはサンドボックス技術を最先端の方法で実装した「保護モード」を提供しています。

Acrobat Readerの保護モードには、ユーザーのコンピューターシステムにマルウェアをインストールする挙動をブロックする能力だけでなく、悪意ある個人によって企業内ネットワークの機密データや

知的財産がアクセスされ抽出されることを防ぐ能力も備わっています。Acrobat Readerの起動時、保護モードは初期設定で常に有効になっています。このモードでは、プログラムに付与するアクセスレベルを制限することでMicrosoft Windowsシステムを保護する手法により、悪意あるPDFを利用してコンピューターファイルシステムの書き込みまたは読み取り、ファイルの削除、システム情報の改ざんなどを試みる挙動がブロックされます。

Acrobat Readerの保護モード（Windows 8.1以降）はAppContainer内での隔離実行に対応しています。

保護されたビュー

サンドボックスとは、隔離された環境の中にプログラムを封じ込め、権限やセキュリティ特権を低下させた状態で実行する重要なセキュリティ手法です。サンドボックスは、実行可能コードを内蔵した信頼されない文書からユーザーのシステムを保護し、損害を防ぐための手段として役立ちます。Acrobat Readerの場合、すべてのPDFファイルとそこから起動されるすべてのプロセスが「信頼されない」コンテンツとして扱われます。すべてのPDFファイルが潜在的に有害なものと見なされ、PDFファイルから起動されるすべての実行プロセスがサンドボックス内に封じ込められます。保護されたビューは、Acrobat Readerの保護モードと同じくサンドボックス技術の実装の一種で、Acrobatの豊富な機能に対応しています。

Acrobatの保護されたビューは機能が拡張されており、書き込みベースの攻撃（PDFファイルを利用してコンピューターシステムに悪意あるコードを実行させる攻撃）だけでなく、読み取りベースの攻撃（PDFファイルを通じて機密データや知的財産を盗み出す攻撃）もブロックできます。保護モードと同様に、保護されたビューでも、信頼されないプログラム（すべてのPDFとそこから起動されるプロセスなど）は機能制限されたサンドボックス内に封じ込められます。この仕組みにより、PDF形式を利用してコンピューターファイルシステムの書き込みや読み取りを試みる悪質なコードの実行が防止されます。保護されたビューは、悪意あるコードがどのPDFにも含まれる潜在的な可能性があることを前提に機能するので、ユーザーが具体的な個別のファイルを信頼できると判断した場合以外は、サンドボックス内で処理を実行します。

保護されたビューは、PDFが単体のAcrobatアプリ内で開かれる場合とブラウザー内で開かれる場合の両方に対応しています。Windows 8.1以降では、保護されたビューは常にAppContainerで実行され、保護されたビューの隔離効果がいっそう強化されています。悪意を含んでいる可能性があるファイルを保護されたビューで開くと、Acrobatの表示ウィンドウの上部に黄色のメッセージバー（YMB）が表示されます。これは、信頼できないファイルが開かれていることと、現在Acrobatは保護されたビューで動作しているため、多くの機能が無効化され、ファイルに対する操作が制限されていることを示します。つまり、簡単にいえば「読み取り専用」モードであり、悪意ある埋め込みコンテンツや付随するコンテンツがシステムに手を加えることもできないという意味です。

ファイルを信頼してAcrobatの機能をすべて有効にするには、YMBの「すべての機能を有効にする」ボタンをクリックします。このボタンをクリックすると保護されたビューが終了し、現在開いているファイルは、Acrobatで「セキュリティ特権扱いの場所」として扱う対象のリストに加えられます。同じPDFを再度開くときには、持続的な信頼を与えた対象として扱われるため、保護されたビューによる制限は適用されません。

Adobe Document Cloudサービスのセキュリティ

ユーザー認証

システム管理者は、Adobe Admin Consoleでユーザー指定ライセンスを使用して、エンドユーザーにAdobe Document Cloudサービスへのアクセス権を付与します。AcrobatとDocument Cloudサービスの利用に関しては、Adobe ID、Enterprise ID、Federated IDの3種のユーザー指定ライセンスがサポートされています。これらのIDタイプと、Adobe ID管理サービスについて詳しくは、Adobe ID管理サービスのセキュリティ概要に関するホワイトペーパー（英語）をご覧ください。

文書とユーザー生成コンテンツ（UGC）のストレージ

Adobe Document Cloudサービスはマルチテナントストレージを利用して機能します。ユーザー生成コンテンツ（UGC）を複数のデータセンターに送り、各データセンター内でも複数のデバイスに保存する冗長化構成が採用されています。データの破損を防いで完全性を維持するため、すべてのネットワークトラフィックに体系的なデータ検証とチェックサム計算がおこなわれます。さらに、保存されたコンテンツは、お客様と同じ地域に設置された別のデータセンター施設にも同期的に自動複製されます。この体制により、万一2か所でデータ損失が発生した場合にもデータの整合性は維持されます。

Document Cloudにアップロードされたユーザー生成コンテンツとドキュメントは、通常、IDタイプに関係なく、データをアップロードするユーザーに関連付けられた国コードに対応する地域のデータセンターに保存されます。

- 北米、中米、南米の国コードを持つユーザーの場合、コンテンツはバージニア州（米国）のデータセンターに保存されます。
- ヨーロッパまたはアフリカの国コードを持つユーザーの場合、コンテンツはダブリン（アイルランド）のデータセンターに保存されます。
- アジア太平洋または中東の国コードを持つユーザーの場合、コンテンツは東京（日本）のデータセンターに保存されます。

一部のEnterprise IDアカウントやFederated IDアカウントに、管理者がAdobe Admin Consoleで個別のクラウドストレージを割り当てることもできます。管理者はDocument Cloudストレージに保存されたエンドユーザーのファイルには直接アクセスできませんが、ユーザーアカウントの所有権を引き取ることや、アクセス権を取り消すことができます。これらの種類のアカウントがシェアードサービスのクラウドストレージを既に使用している場合、アカウントを削除すると、エンドユーザーは保存したデータにアクセスできなくなり、データは90日後に削除されます。

管理者は、Admin ConsoleでAdobe IDアカウントにストレージを割り当てることもできます。Adobe IDアカウント自体のコントロールはできませんが、アカウントを除去し、エンタープライズストレージクォータの割り当てと、アプリケーションおよびサービスに対するアクセスを両方ともエンドユーザーアカウントから削除することができます。その場合、データも90日後に削除されます。

データの暗号化

Document Cloudサービスでは、UGCとドキュメントの転送時にはデフォルトでHTTPS TLS 1.2暗号化が適用されます。また、Document Cloudサービス内にコンテンツが保持されている間はAES 256ビット対称セキュリティキーで暗号化されます。このキーは、お客様ごと、およびお客様の申請ドメインごとに固有です。これらの暗号化方式は、永続的および一時的なドキュメントストレージの両方に適用されます。

専用の暗号化キー

管理者は、標準で組み込まれている暗号化機能に加えて、保存中のドキュメントの制御とセキュリティをさらなる追加レイヤーで強化できます。このレイヤーは、お客様組織の一部ドメインまたは全ドメインに適用される専用の暗号化キーを使用して実現されます。この機能では、専用暗号化キーを使用してDocument Cloudサービスのコンテンツを暗号化できるのに加え、必要に応じてAdmin Consoleからコンテンツを失効させることもできます。管理者が暗号化キーを失効させると、キーを再度有効化するまでは、そのキーで暗号化されたデータにエンドユーザーがアクセスすることや、コンテンツをアップロードまたはダウンロードすることは不可能になります。

注意：専用暗号化キーによる暗号化処理は、Adobe Document Cloudのファイルにのみ適用され、メタデータには適用できません。

専用キーを使用した暗号化の管理について詳しくは、Adobe.comの情報をご覧ください。

電子サインとデジタル署名

Document Cloudサービスには、ユーザーが署名を扱うための手段として以下のツールが用意されています。

- **入力と署名ツール** — PDFを開いて、フォームのフィールドに情報を記入し、電子的な署名を文書に付与できます。
- **証明書ツール** — 暗号技術で署名フィールドに関連付けられたデジタル証明書により、有効性の根拠がある電子サインを文書に付与できます。デジタル証明書（デジタルID）は個別の署名者を識別するものであり、Adobe Approved Trust List（AATL）またはEuropean Union Trusted Lists（EUTL）のトラストリストに掲載されたトラストサービスプロバイダー（TSP）、認証機関（CA）によって発行されます。また、証明書ツールでは文書にタイムスタンプを付加できるほか、不正改ざん防止シールで文書の整合性を確保できます。

AcrobatとMicrosoftの連携

アドビはMicrosoftと提携して、Microsoftの有力な生産性向上ツールとの連携ソリューションを構築し、以下のツール環境内からAcrobatとDocument Cloudサービスへのネイティブアクセスを実現しました。

- Microsoft SharePointおよびOneDrive
- Microsoft Teams
- Microsoft Word、Excel、PowerPoint（PDFの作成と保護のみ）

いずれのソリューションにおいても、連携は一時的なPDFを作成することで実現されており、アドビが当該ユーザーのお客様情報や個人を特定できる情報を収集することはありません。

Acrobat（SharePointおよびOneDrive向け）

Acrobat（SharePointおよびOneDrive向け）を導入すると、ユーザーがMicrosoft 365内からPDFワークフローにアクセスし、クラウド内のPDFを閲覧、作成、加工できるようになります。

この連携機能付きAcrobatでは、SharePointまたはOneDrive内にある元の作業場所にドキュメントが保存されます。閲覧、注釈、検索などのアクションはユーザーのコンピューターで実行されます。ユーザーがドキュメントに変更を加えると、そのドキュメントは再びSharePointまたはOneDriveアカウントに保存されます。

ドキュメントの作成、整理、結合、書き出しがユーザーによって実行された場合、そのドキュメントは、一時的な処理のためにユーザーの国コードに対応する地域のAdobe Document Cloudサーバーに送信され、24時間以内に削除されます。そのプロセスの間も、ドキュメントの転送と保存の両方に暗号化が適用され続けます（「データの暗号化」セクションを参照）。変更後のドキュメントは、ユーザーのSharePointまたはOneDriveアカウントに保存されます。

Acrobat（SharePointおよびOneDrive向け）の具体的な機能について詳しくは、Adobe.comの情報をご覧ください。

Acrobat（Microsoft Teams向け）

Acrobat（Microsoft Teams向け）を導入すると、ユーザーがMicrosoft Teams内からPDFワークフローにアクセスし、クラウド内のPDFを閲覧、作成、加工できるようになります。Acrobat（Microsoft Teams向け）は、個人用タブ、ボット、タブ、メッセージアクション、またはメッセージ拡張機能として使用可能です。

デフォルトでは、Microsoft Teamsのチャットまたはチャネルで共有されたPDFは、ユーザーのOneDriveまたはSharePointに保存されます。閲覧、注釈、検索などのアクションはユーザーのコンピューターで実行されます。ユーザーがドキュメントに変更を加えると、そのドキュメントは再びSharePointまたはOneDriveアカウントに保存されます。

ドキュメントの作成、整理、結合、書き出しがユーザーによって実行された場合、そのドキュメントは、一時的な処理のためにユーザーの国コードに対応する地域のAdobe Document Cloudサーバーに送信され、24時間以内に削除されます。そのプロセスの間も、ドキュメントの転送と保存の両方に暗号化が適用され続けます（「データの暗号化」セクションを参照）。変更後のドキュメントは、ユーザーのSharePointまたはOneDriveアカウントに保存されます。

Microsoft Teamsとの連携ソリューションで利用できる具体的な機能について詳しくは、Adobe.comの情報をご覧ください。

Acrobat（Word、Excel、PowerPoint向け）

ユーザーは、Create PDFアドインを使用してMicrosoft 365ドキュメントを高品質のPDFに簡単に変換し、そのPDFをOneDriveに保存することや個人用ハードディスクにダウンロードすることができます。また、パスワードを設定してPDFを保護し、ドキュメントの不正利用を防ぐことができます。

まとめ

Document Cloudサービスがプラスされた Acrobatとお客様の機密情報を保護するにあたっては、本ホワイトペーパーで説明した事前対応型セキュリティアプローチと厳格な手順が効果を発揮しています。アドビはデジタルエクスペリエンスデータのセキュリティをきわめて重要視しており、新たな脅威の動向を常に注視して攻撃者の先手を打つ対策に努めながら、お客様のデータセキュリティを確保し続けています。

エンタープライズ、製品、運用のセキュリティプロセス、セキュリティテストプログラム、コンプライアンスと認定制度、インシデント対応プログラム、事業の継続性と災害復旧（BCDR）プロセスなどのアドビのセキュリティについて詳しくは、Adobe Trust Centerをご覧ください。

本書の情報は予告なく変更される場合があります。アドビのソリューション、利用制御方法、ライセンス購入方法について詳しくは、アドビのセールス担当者にご相談ください。

03/24