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

目次

Adobe SignはDocument Cloud PDFサービスの一部ですが、セキュリティ機能は独立しています。

概要

アドビでは、デジタルエクスペリエンスのセキュリティを重要視し、ソフトウェア開発から、オペレーションプロセス、ツールに至るまで、セキュリティ対策が深く根づいています。また、その対策は部門横断型チームが厳重にチェックし、臨機応変にインシデントの保護、検出、対応をおこなっています。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、常に最新の脅威と脆弱性を把握し、提供する製品およびサービスに高度なセキュリティ技術を組み込んでいます。

ユーザーのコンテンツにアクセスするアドビのサービスは、業界で高く評価されています。現在アドビ製品およびソリューションでサポートされ、準拠している認証、規格、政府規制については、最新の準拠認証、規格、規制の一覧（英語）をご確認ください。GDPRへの対応については、GDPRへの対応に記載されています。

このホワイトペーパーでは、Adobe Acrobat DC、Acrobat Reader DC、Document Cloud、Document Cloudサービスおよび関連データを利用する際のセキュリティを強化するために、アドビが実行している厳重な対策とセキュリティ手順について説明します。

Document Cloudサービスがプラスされた Acrobat DC概要

Adobe Acrobat DCには、最新のAcrobatデスクトップ版に加えて、高度な機能を備えたAcrobat Readerモバイル版アプリとAdobe Document Cloudオンラインサービスが付属しています。このため、あらゆるデバイスを通じてセキュリティを確保しつつ、接続性と生産性を維持するというエンドユーザーのビジネスニーズを満たすことができます。Adobe Acrobat DCとDocument Cloudサービスを使えば、コンテンツを電子文書に変換でき、アドビのどのクラウドサービス、デスクトップアプリケーション、モバイルアプリでも他者と共有し、簡単にPDFを生成、操作、変換できます。

Acrobatの文書セキュリティ機能

墨消し

Adobe Acrobat DCには機微情報や秘密情報を保護するための一連の墨消しツールが含まれ、文書内のテキストとグラフィック画像の両方を完全に削除（復元不可能）してから配布することもできます。また、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パターンによって検索し、コンテンツの墨消しをおこなうこともできます。墨消しした情報は、他の削除方法を使用した場合のように単にマスクされるのではなく、ファイルから完全に情報が削除されます。文書の非表示情報の削除機能では、非表示情報やグラフィック以外のオブジェクト（PDF内のメタデータといった関連情報）も削除できます。

ファイルの共有

Document Cloudファイルをクラウドに保存すると、アップロードしたユーザーのみが表示可能であることを示す、「プライベート」というラベルがすべてのファイルに付加されます。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コンテンツの共有は、電子メール、テキスト、その他の共有ソフトウェアを使用して、受信者にDocument Cloudコンテンツへのリンクを送信することでおこないます。

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」か「レビュー」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、受信者は読み取り専用文書としてコンテンツを表示できます。これに対して、文書をレビュー用に送信した場合、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。

アセット設定と共有の制限

アセット設定を使用することで、従業員による組織外とのアセット共有を制御できます。制限的設定では、従業員によるDocument Cloud内の共有機能の使用を制限できます。例えば、招待を受理してアクセスを要求し、ホワイトリストに登録された信頼できるドメインの受信者のみとの共有に制限することができます。このポリシーを設定すれば、ユーザーは許可されたドメインリストにない外部のユーザーとは組織が所有するアセットを共有できなくなります。

Admin Consoleでのアセット設定

Microsoft Information Protection（MIP）

Acrobat DCまたはAcrobat Reader DCを使用し、DRM（デジタル著作権管理）が施されたPDFを開くことができます。Microsoft Information Protectionソリューション（MIP）（Azure Information Protection（AIP）およびOffice 365による情報保護を含む）で保護されたファイルを開く場合は、こちらの文書をご確認ください。

Acrobat Reader DCの保護モード

悪意のあるコードには、PDF形式を使用してコンピューターのファイルシステムに対し書き込みまたは読み取りを試みるものがあります。このようなコードからお客様を保護するために、アドビではAdobe Reader X以降の製品に保護モードと呼ばれるサンドボックス技術を実装しています。

サンドボックスとは、セキュリティ手法のひとつで、隔離した環境の中で権限またはセキュリティ特権を低下させた状態でプログラムを実行することを指します。サンドボックスを使用すると、実行可能コードを含む信頼されないドキュメントによる損害から、ユーザーのシステムを保護できます。Acrobat Reader DCの場合、あらゆるPDFと、それによって起動されるあらゆるプロセスが、信頼されないコンテンツに該当します。Acrobat Reader DCは、あらゆるPDFを潜在的に有害であると見なし、PDFの処理をサンドボックス内で実行します。

Acrobat Reader DCの保護モードは、攻撃者がユーザーのシステムにマルウェアをインストールできないようブロックすることで、悪意の実行者がネットワーク上の機密情報や知的財産にアクセスし、情報を引き出すことを防ぎます。Acrobat Reader DC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、プログラムに付与されるアクセスレベルを制限することで、コンピューターのファイルシステムに対する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悪意のあるPDFから、Microsoft Windowsを実行中のシステムを保護します。

Windows 8以降の保護モードではWindows AppContainerでの実行もでき、保護モードを有効にした環境をのセキュリティをさらに強化します。

Acrobat DCの保護されたビュー

保護されたビューとは、Acrobat Reader DC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 DCの豊富な機能セットに対応しています。Acrobat DCでは、保護モードの機能が拡張されており、PDFを利用してコンピューターのファイルシステムで悪意のあるコードを実行する書き込みベースの攻撃だけでなく、PDFを通じて機密情報や知的財産を盗み出す読み取りベースの攻撃もブロックできます。

保護されたビューも、保護モードと同様に、信頼されないプログラム（例えば、あらゆるPDFとそこから起動されるプロセスなど）を、機能制限されたサンドボックスの中に隔離して実行します。この仕組みが、PDF形式を利用した悪意あるコードによってコンピューターのファイルシステムへの書き込みまたは読み取りが実行されるのを防ぎます。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、ユーザーがPDFを単体のAcrobat DCアプリケーション上で開く場合と、ブラウザー上で開く場合の両方をサポートしています。Windows 8.1以降では、保護されたビューは常にAppContainerで実行されます。したがって、保護されたビューを有効にすることで、さらにセキュリティが強化された環境での作業が可能になります。

信頼できないファイルを保護されたビューで開くと、Acrobat DCの表示ウィンドウの上部にメッセージが表示されます。それが信頼できないファイルであり、現在は保護されたビューで表示されているため、Acrobat DCの機能の多くが無効化され、ファイルに対する操作が制限されていることを通知するメッセージです。基本的にファイルは「読み取り専用」モードのため、埋め込みコンテンツや付随コンテンツによるシステムの改ざんを防御できます。

ファイルを信頼してAcrobat DCのあらゆる機能を有効にするには、メッセージバー上の「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、Acrobatでセキュリティ特権付きとして扱われる場所のリストにそのファイルが追加されます。ファイルに永続的な信頼が設定され、以降、その信頼されたPDFを開くときには、保護されたビューによる制限は適用されません。

Document Cloudサービスのアーキテクチャ

Adobe Document Cloudサービスの詳細：

- **ページを整理**－PDF内のページを挿入、削除、並べ替え、回転
- **PDFを作成**－Word、Excel、PowerPoint文書、画像や写真をPDFに変換
- **PDFを書き出し**－PDFを編集可能なMicrosoft Word、Excel、PowerPoint、RTFファイルに簡単に変換
- **PDFを編集**－モバイルデバイスやラップトップで既存のPDFを簡単に編集
- **ファイルを結合**－どこからでも複数のファイルをひとつのPDFに結合し、ドキュメントパッケージを構築
- **送信とトラック**－文書を送信、トラック、配信確認
- **Adobe Scan**－対象を問わず取り込み、検索可能で高品質なPDFに変換
- **Adobe Sign**－どのデバイスでも利用できる、安全で信頼でき、法的拘束力のある電子サイン用の文書を作成し、送信

Document Cloudサービスのセキュリティ

権利付与とID管理

IT管理者は、Adobe Admin Consoleの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 Document Cloudは、次の3種類のユーザー指定ライセンスをサポートしています。

- **Adobe ID**－個々のユーザーが作成、所有、管理し、アドビがホストするユーザー指定ライセンス。Adobe IDアカウントは、IT管理者がアクセスを有効にした場合にのみ、Acrobat Document Cloudサービスへのアクセス権が得られます。
- **Enterprise ID**－導入先組織のシステム管理者が作成、管理し、アドビがホストするユーザー指定ライセンス。ユーザーアカウントおよび関連するすべてのアセットは、組織が所有して管理します。
- **Federated ID**－導入先組織が管理するアカウント。すべてのIDプロファイルおよび関連するアセットは導入先組織で運用されているシングルサインオン（SSO）ID管理システムによって提供され、そのIT部門によって作成、所有、管理されます。ほとんどのSAML 2.0準拠IDプロバイダーとの統合に対応します。

ほとんどの大規模組織では、会社ドメインの電子メールアドレスが付与された従業員、契約スタッフ、フリーランサー用にEnterprise IDかFederated IDを使用しています。この方法を使用すれば、権利付与とユーザーIDで保存したユーザー生成コンテンツ（UGC）の両方を常にコントロールできるからです。各IDについて詳しくは、アドビカスタマーサポートサイトをご確認ください。

Adobe IDとEnterprise IDのパスワードの保存には、SHA 256ハッシュアルゴリズムを、パスワードソルト、膨大なハッシュイテレーションと合わせて使用しています。アドビは、アドビがホストするアカウントに対して異常な活動がないか継続的に監視し、この情報を評価することでセキュリティに対する脅威を直ちに封じています。Federated IDアカウントの場合、アドビはユーザーのパスワードを管理しません。詳しくは、アドビID管理サービスのセキュリティ概要（英語）をご確認ください。

電子サインと電子署名

Document Cloudサービスには、安全に署名する機能として次の2つのツールがあります。

- **入力と署名ツール**－Adobe Signの機能により、エンドツーエンドの署名プロセスをユーザー自身で管理できます。米国、欧州、その他世界中ほとんどの先進国の電子サイン関連法規に準拠するよう設計されています。このツールを使用すると、署名の依頼や署名プロセスの追跡が可能になるほか、署名済み文書と監査証跡を自動的に長期保管できます。プロセス全体にセキュリティ対策が施され、アドビの不正改ざん防止シールによって文書と監査証跡の整合性が確保されます。

モバイル版にはトラッキング機能はありません。

Adobe Signとそのセキュリティ機能について詳しくは、Adobe Sign技術概要をご確認ください。

- **署名者認証ツール**－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サービスプロバイダーが発行する証明書ベースの電子署名を使用して、文書に署名できます。信頼できるサードパーティの認証機関（CA）から発行された証明書ベースのIDを使用する署名は、安全性の高い電子署名方法として広く認められています。このIDは署名者と一意に紐付けされており、このIDによって署名者が特定されます。署名者のみが持つ秘密鍵を使用した署名プロセスにより、暗号化された署名者の認証情報が文書に付加されます。

  Acrobat DCは自動的に認証機関に接続し、署名者の署名と文書の真正性を検証します。この種の署名は、PDF長期署名標準（PDF Advanced Electronic Signature（PAdES）Parts 2、3および4、AES-256、RSA-4096、SHA-512、RSA-PSSを使った暗号化および公開鍵基盤（PKI）のU.S. Department of Defense Joint Interoperability Test Command（JITC）使用など）に準拠します。また、証明書ベースの署名では、文書にタイムスタンプを追加できるほか、不正改ざん防止シールで文書の整合性を確保することもできます。

Document Cloudサービスのコンテンツストレージ

管理者はAdobe Admin Consoleを通じてEnterprise IDおよびFederated IDアカウントに個別のクラウドストレージを割り当てますが、ユーザーのDocument Cloudストレージ内のファイルに直接アクセスすることはできません。シェアードサービスストレージがあるEnterprise IDまたはFederated IDを削除すると、エンドユーザーはそのクラウドストレージ内のデータにアクセスできなくなり、そのユーザーのデータは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。管理者はAdobe IDのアカウント自体を削除することはできませんが、付与したエンタープライズストレージの割り当てと、アプリケーションとサービスへのアクセス権の両方解除できます。そのアカウントに関連付けられたデータは90日後に削除されます。

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います。顧客コンテンツは、Amazon Elastic Compute Cloud（Amazon EC2）インスタンスによって処理され、Amazon Elastic Block Store（Amazon EBS）上のMongoDBインスタンスによって、Amazon Simple Storage Services（Amazon S3）バケットの組み合わせに保存されます。コンテンツ自体はAmazon S3バケットに、コンテンツに関するメタデータはMongoDBによってAmazon EBSに保存され、そのAmazon Web Services（AWS）リージョン内のIdentity and Access Management（IAM）ロールによってすべて保護されます。

Amazon EBSに保存されたメタデータと補助アセットは、National Institute of Standards and Technology（NIST）800-57の勧告に準拠するFederal Information Processing Standards（FIPS）140-2承認済みの暗号化アルゴリズムを利用して、AES 256ビットで暗号化されます。

データはすべて複数のデータセンターで保存され、さらに各データセンターでも複数のデバイスに重複して保存されます。すべてのネットワークトラフィックは体系的なデータ検証とチェックサム計算を経るため、破損を防ぎ、完全性が保証されます。最終的に、保存されているコンテンツは、お客様のリージョン内の他のデータセンター施設に同期的かつ自動的に複製され、万一2つの場所でデータが失われたとしてもデータの整合性が維持されます。

Amazonサービスプラットフォームについて詳しくは、以下をご覧ください。

- MongoDB（英語）
- Amazon S3
- AWS Key Management Service（KMS）
- Amazon EC2サービス

専用の暗号化キー

初期設定では、Amazon S3に保存されているコンテンツとアセットは、顧客ごとおよび顧客が要求したドメインごとに固有のAES 256ビット対称セキュリティキーで暗号化されます。組織内の一部またはすべてのドメイン用に制御とセキュリティの追加レイヤーを希望する場合は、AWS KMSによって管理し、1年ごとにキーを自動的にローテーションする専用暗号化キーを使用できます。

管理者はAdmin Consoleで専用暗号化キーを取り消し、そのキーにより暗号化されたデータにエンドユーザーがアクセスできないようにすることも可能です。これにより、暗号化キーを再度有効にするまでコンテンツのアップロードとダウンロードを防止できます。

注意：専用暗号化キーではAdobe Document Cloudファイルは暗号化できますが、メタデータの暗号化はできません。

専用キーを使用した暗号化の管理について詳しくは、以下のアドビヘルプページをご確認ください。

- 暗号化の管理
- 専用暗号化キーのよくある質問

*アセット設定と共有の制限、専用暗号化キーによる保護機能は、Enterprise IDおよびFederated IDでサポートしています。なおAcrobat DC個人版およびグループ版では、Adobe IDのみサポートしています。

Amazon Web Services

前述のとおり、Adobe Document Cloudサービスのすべてのコンポーネントは、Amazon EC2およびAmazon S3を含む、米国内のAWSでホストされています。Amazon EC2は、クラウド内で規模の変更が可能なコンピューター処理能力を提供し、Webスケールでのコンピューター作業を容易にするWebサービスです。Amazon S3は、容量に関係なくデータを保存・取得できる信頼性の高いデータストレージインフラストラクチャとして広く認められています。

AWSプラットフォームは、業界標準のプラクティスに従ったサービスを提供し、一般的に業界に認められている認証と監査を受けています。AWSとAmazonのセキュリティ対策について詳しくは、AWSクラウドセキュリティwebサイトをご確認ください。

AWSとアドビの運用責任

コンポーネントの運用、管理、制御については、AWSがハイパーバイザー仮想化レイヤーからAdobe Document Cloud services運用施設の物理セキュリティまでを担当します。一方アドビは、ゲストオペレーティングシステムの管理（アップデート、セキュリティパッチを含む）およびAWSが提供するセキュリティグループファイアウォールの設定について責任を負います。

AWSは、アドビが使用するクラウドインフラストラクチャを運用し、処理やストレージをはじめとする様々な基本的コンピューティングリソースを供給します。AWSのインフラストラクチャには、施設、ネットワーク、ハードウェアに加え、それらのリソースの供給と使用をサポートする運用ソフトウェア（ホストOS、仮想化ソフトウェアなど）が含まれます。Amazonは、業界標準のプラクティスと様々なセキュリティコンプライアンス基準に従ってAWSを設計および管理しています。

安全な管理

アドビでは、管理接続用のSecure Shell（SSH）およびSecure Sockets Layer（SSL）を使用してAWSのインフラストラクチャを管理しています。

AWSネットワーク上の顧客データの所在地

Document Cloudにアップロードしたすべての UGCは、AWS米国東部リージョン（バージニア州）データセンターに保存されます。コンテンツは、負荷分散と冗長化のため、各データセンターとリージョン内の他のデータセンターでバックアップされます。

AWSネットワーク上のIDデータの所在地

IDデータは、バージニア州（米国東部）、オレゴン州（米国西部）、アイルランド（EU西部）、シンガポール（アジアパシフィック南東部）の各リージョンに負荷分散されたAWSデータセンターに保存されます。IDデータはすべてのデータセンター間で複製されます。アドビは域外データ移転に関して適用される法令を遵守しています。詳しくは、https://www.adobe.com/jp/privacy/eudatatransfers.html をご確認ください。

顧客データの分離／顧客のセグメント化

AWSは、強力なテナント分離のセキュリティ機能とコントロール機能を使用します。仮想化されたマルチテナント環境のAWSにはセキュリティ管理プロセスや他のセキュリティ対策が実装されており、AWSのお客様がそれぞれ分離されるようになっています。アドビはAWS Identity and Access Management（IAM）を使用してアクセスを制限し、インスタンスの処理と保存をおこないます。

セキュアネットワークアーキテクチャ

AWSは、ファイアウォールや他の境界デバイスなどのネットワークデバイスを採用し、ネットワークの外部境界およびネットワーク内の主な内部境界で通信の監視と制御をおこなっています。これらの境界デバイスは、ルールセット、アクセスコントロールリスト（ACL）、構成を採用し、特定の情報システムサービスに情報を流します。ACL、つまりトラフィックフローポリシーは、各マネージドインターフェイス上でトラフィックの流れを制御します。

Amazon Information SecurityはすべてのACLポリシーを承認し、AWS ACL管理ツールで自動的にそれらを各マネージドインターフェイスにプッシュして、マネージドインターフェイスが最新のACLを強制するようにします。

ネットワークのモニタリングと保護

AWSは、様々な自動モニタリングシステムを使用して、ハイレベルなサービスパフォーマンスと可用性を提供します。モニタリングツールによって、通信ポイントの入口と出口で異常なアクティビティや承認されていないアクティビティが検出されます。AWSのネットワークは、次のような従来のネットワークセキュリティの問題に対する強固な保護機能を提供しています。

- 分散サービス妨害（DDoS）攻撃
- 中間者（MITM）攻撃

- IPスプーフィング
- ポートスキャニング
- 第三者によるパケットスニッフィング

ネットワークのモニタリングと保護について詳しくは、AWSクラウドセキュリティwebサイトをご確認ください。

侵入検知

業界標準の侵入検知システム（IDS）および侵入防止システム（IPS）を使用して、Adobe Document Cloudサービスを能動的にモニタリングしています。

ログ記録

アドビはサービスの停止、お客様の特定の問題および報告されたバグを診断するために、サーバー側でAdobe Document Cloudサービス利用者のアクティビティを記録します。ログには、特定の顧客の問題を診断するためのAdobe IDのみが保存されます。ユーザー名とパスワードの組み合わせは含まれません。アドビテクニカルサポート認定担当者、主要エンジニア、選定された開発者のみ、起こり得る問題を診断するためにログにアクセスできます。

サービスのモニタリング

AWSは、電気、機械、サポートシステムおよび設備をモニタリングし、サービスに関する問題が速やかに特定されるようにしています。また、設備の継続的な運用性を維持するために、予防的メンテナンスを実行しています。

データの保管とバックアップ

アドビは、Adobe Document Cloudサービスのすべてのデータを、堅牢性の高いストレージインフラストラクチャを提供するAmazon S3に保存します。堅牢性を高めるため、Amazon S3 PUTおよびCOPY操作は、複数の施設で同期をとりながら顧客データを保存し、Amazon S3のリージョン内で、複数の施設にまたがって、複数のデバイス上で冗長的にオブジェクトを保存します。

Amazon S3は、すべてのネットワークトラフィックでチェックサムを計算して、データの保存または取得時にデータパケットの破損を検出します。Amazon S3データオブジェクトのデータ複製は、データが保存されるリージョンのクラスター内で行われ、他のリージョンのデータセンタークラスターにデータは複製されません。

メタデータはAmazon EBSボリュームのスナップショットを作成することで複製され、Amazon S3と同様に保存されます。AWSのセキュリティについて詳しくは、AWSクラウドセキュリティwebサイトをご確認ください。

変更管理

既存のAWSインフラストラクチャに対する日常的な変更、緊急の変更、設定の変更については、こうしたシステムで適用される業界基準に従って、認定、記録、テスト、承認を経て、文書化されます。AmazonがAWSを更新するにあたり、顧客への影響は最小限に抑えられます。サービスが悪影響を受ける可能性がある場合、AWSは電子メールまたはAWS Service Health Dashboardを通じて顧客に通知します。アドビもまたAdobe Document Cloud用のAdobe System Statusを保持しています。

パッチ管理

AWSには、ハイパーバイザーやネットワークサービスといったAWSサービスをサポートするシステムにパッチを適用する責任があります。アドビは、ゲストオペレーティングシステム（OS）、ソフトウェア、AWSで実行しているアプリケーションにパッチを適用する責任を負っています。パッチが要求された場合、アドビは実際のパッチではなく、新たに強化したOSやアプリケーションのインスタンスを提供します。

AWSの物理統制と環境統制

AWSの物理統制と環境統制については、SOC Type 1およびType 2のレポートに具体的に記載されています。次のセクションでは、世界各地のAWSデータセンターで実施されているセキュリティ対策をいくつか紹介します。AWSのセキュリティについて詳しくは、AWSクラウドセキュリティwebサイトをご確認ください。

物理設備のセキュリティ

AWSデータセンターは、業界標準の構造的かつ工学的アプローチを採用しています。AWSデータセンターは、外部からはそれとはわからないようになっています。専門のセキュリティスタッフ、ビデオ監視カメラ、IDS（侵入検出システム）、その他の電子的手段を用いて、建物の入口とその周辺の両方で物理的アクセスを制御しています。権限を付与されたスタッフが2要素認証を最低2回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添います。

AWSは、必要とする正規の手続きを有する従業員や業者に対してのみ特権を与え、データセンターへのアクセスや情報を提供しています。従業員がこれらの特権を必要とする作業を完了したら、たとえ彼らが引き続きAmazonまたはAWSの従業員であったとしても、そのアクセス権は速やかに取り消されます。AWS従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。

火災抑制

すべてのAWSデータセンターには、自動火災検出装置および鎮火装置が取り付けられています。この火災検出システムは、全データセンター環境、機械電気インフラ空間、冷却室および発電機設備室において、煙検出センサーを使用しています。これらのエリアは、充水型、予作動式ダブルインターロック方式、またはガス式スプリンクラーシステムによって守られています。

コントロールされた環境

AWSは、サーバーその他のハードウェアの運用温度を一定に保つために、天候コントロールシステムを採用することで、過熱を防ぎ、サーバー停止の可能性を減らしています。AWSデータセンターは、室内空気環境を最適なレベルに保つように設定されています。AWSの作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。

バックアップ電源

AWSデータセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1日24時間、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給します。データセンターは、発電機を使用して施設全体のバックアップ電力を供給します。

災害復旧

AWSデータセンターは、高いレベルの可用性を備え、影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。すべてのデータセンターは、世界各地にクラスターの状態で構築されています。24時間年中無休体制のサービスをオンラインで顧客に提供しており、「コールド」の状態のデータセンターは存在しません。障害時には、自動プロセスが、影響を受けるエリアから顧客データを移動します。

重要なアプリケーションはN+1設定で配備されるので、データセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。AWS障害回復プロトコルについて詳しくは、AWSクラウドセキュリティwebサイトをご確認ください。

アドビのリスクと脆弱性管理

アドビは、リスクと脆弱性の管理、インシデント対応、軽減、解決プロセスを迅速かつ正確に実行するために力を尽くしています。継続的に脅威の動向をモニタリングしながら、世界中のセキュリティ専門家と知識を共有して問題が発生したらすぐに解決し、この情報をアドビの開発チームにフィードバックすることで、すべてのアドビ製品およびサービスにおいて最高レベルのセキュリティを確保します。

侵入テスト

アドビは、承認したサードパーティの大手セキュリティ企業と提携して侵入テストを実行し、潜在的なセキュリティの脆弱性を明らかにしてアドビの製品とサービスの総合的なセキュリティの強化を図っています。当該サードパーティから提供されたレポートを受け取り次第、アドビはこれらの脆弱性を文書化し、深刻度と優先度を評価した上で、軽減策や修復計画を作成します。アドビは毎年完全な侵入テストをおこない、毎月脆弱性スキャンを実施しています。

社内では、Adobe Document Cloudセキュリティチームが、すべてのリリース前と四半期ごとにすべてのDocument Cloudコンポーネントとサービスのリスク評価を実行します。Document Cloudのセキュリティチームは、技術オペレーションおよび開発チームと連携し、リリースの前にリスクの高いあらゆる脆弱性を軽減するための措置を講じます。アドビの侵入テスト手順について詳しくは、アドビセキュアエンジニアリング概要（英語）をご確認ください。

インシデントの対応と通知

脆弱性や脅威が日々進化する中、アドビは迅速な対応と新しく発見された脅威の軽減に努めています。US-CERT（米国コンピューター緊急事態対策チーム）、Bugtraq、SANSなどの業界規模での脆弱性アナウンスリストの利用に加え、主要なセキュリティベンダーが発行する最新のセキュリティ警告リストも利用します。

アドビのインシデントの対応と通知について詳しくは、アドビインシデント対応概要（英語）をご確認ください。

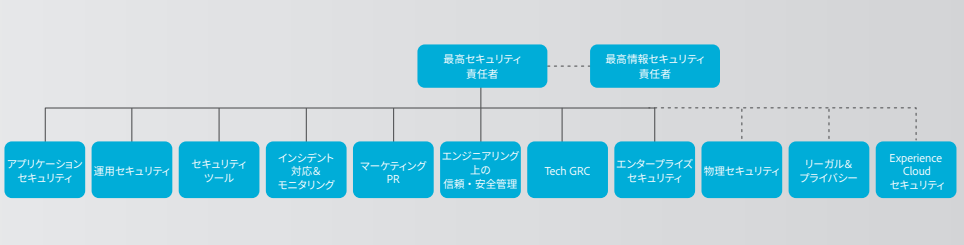
フォレンジック分析

インシデントの調査に関して、Document Cloudチームは、すべての画像取り込み、影響を受けるマシンのメモリダンプ、証拠の安全な保持および分析過程の管理記録をはじめとするアドビのフォレンジックス分析プロセスに準拠しています。

アドビのセキュリティ組織

製品およびサービスのセキュリティに対する取り組みの一環として、アドビは最高セキュリティ責任者（CSO）の下にすべてのセキュリティ活動を統合しています。すべての製品・サービスのセキュリティ戦略とAdobe Secure Product Lifecycle（SPLC）の実装は、CSOのオフィスで統括しています。

CSOはまた、Adobe Secure Software Engineering Team（ASSET）も管理しています。ASSETは、セキュリティのエキスパートが集まった専任のチームです。Adobe Document Cloudチームをはじめ、主要アドビ製品のセキュリティと運用を担うチームのコンサルタントとしての役割を果たしています。ASSETの調査担当者は、各アドビ製品チームや運用チームと協力して製品やサービスが適切なレベルのセキュリティで保護されるよう尽力するとともに、明確かつ再現可能なプロセスで開発、デプロイメント、運用、インシデント対応をおこなえるように、セキュリティに対する取り組みについて各チームにアドバイスしています。



アドビのセキュリティ組織

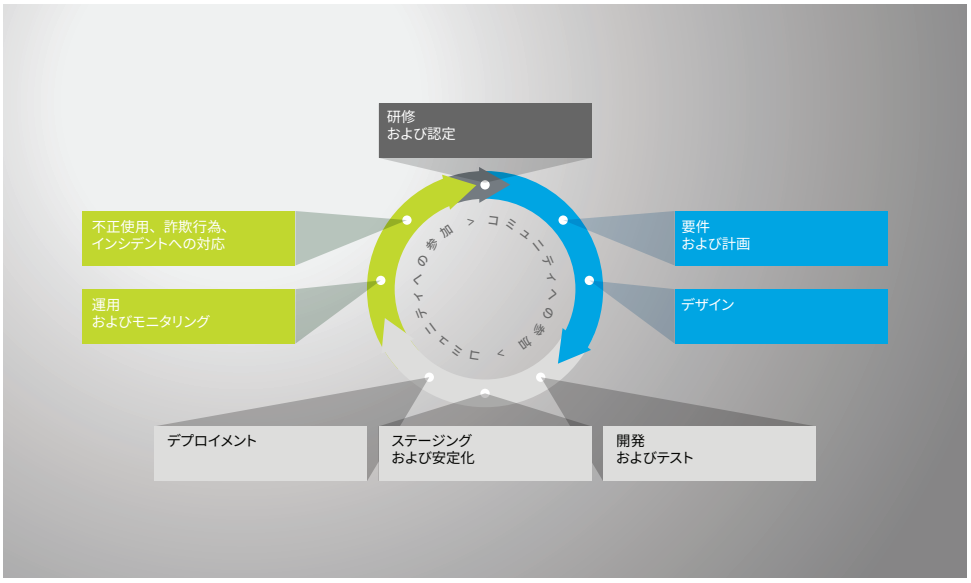
アドビの安全な製品開発

他のアドビの製品およびサービスの組織と同様、Adobe Document Cloud組織もAdobe SPLCプロセスを採用しています。ソフトウェア開発のプラクティス、プロセス、ツールにわたる数百もの特定のセキュリティコントロールを厳選したAdobe SPLCは、設計や開発から品質保証、テスト、導入に至るまで、製品ライフサイクルの様々な段階に組み込まれます。ASSETのセキュリティ研究者は、潜在的なセキュリティの問題点に基づいて、主要な製品またはサービスについて個別にSPLCをアドバイスします。Adobe SPLCは、アドビ外部のセキュリティコミュニティに継続的に参画することによって補完され、テクノロジー、セキュリティプラクティスおよび脅威の変化に応じて最新の状態が保たれるよう進化し続けます。

Adobe Secure Product Lifecycle

個々のAdobe Document Cloudコンポーネントによって、以下のベストプラクティス、Adobe SPLCプロセス、ツールの一部をAdobe SPLCの活動として取り入れている場合もあれば、全部を実施している場合もあります。

- すべての製品チームに対するセキュリティ研修および認定制度の実施
- 製品の正常性、リスクおよび脅威の分析
- 安全なコーディングガイドライン、ルール、分析
- Open Web Application Security Project（OWASP）が発表しているWebアプリケーションの重大なセキュリティリスクトップテンと、CWE/SANSの最も危険なソフトウェアエラー上位25への対策を講じるために、Adobe Document Cloudセキュリティチームが指針とするサービスロードマップ、セキュリティツールおよびテスト方法
- セキュリティアーキテクチャレビューと侵入テストの実施
- 脆弱性の原因となりかねない既知の問題を解消するためのソースコードレビュー
- UGC対応検証
- アプリケーションとネットワークのスキャン
- 安全かつ順応性の高いレビュー、対応計画、開発者向け教材のリリース準備



Adobe Secure Product Lifecycle

アドビソフトウェアセキュリティ認定プログラム

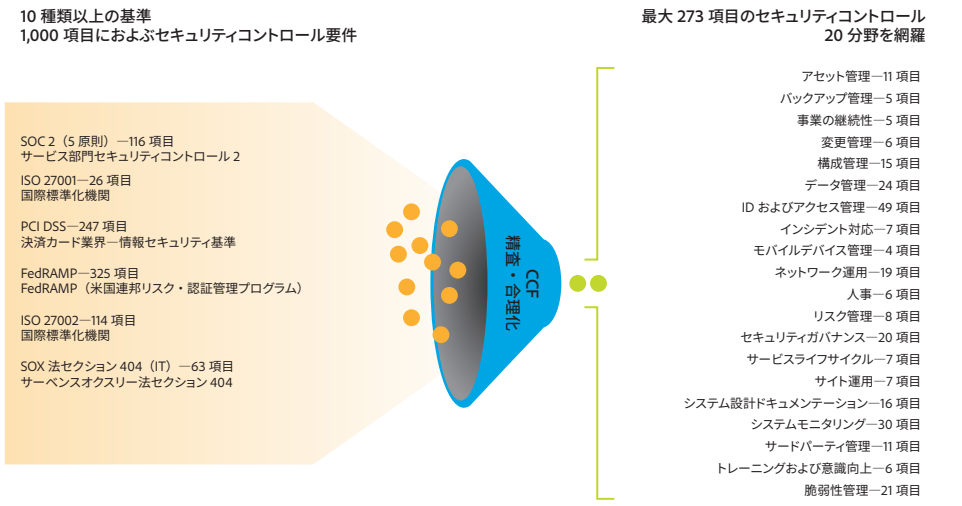
Adobe SPLCの一環として、アドビでは、開発チームで継続的にセキュリティ研修を実施し、企業全体でセキュリティの知識を高め、製品およびサービスの包括的なセキュリティ向上を図っています。アドビのソフトウェアセキュリティ認定プログラムに参加した従業員は、セキュリティプロジェクトを修了することで様々な認定レベルに到達します。アドビの製品セキュリティ対策について詳しくは、アドビセキュアエンジニアリング概要（英語）をご確認ください。

アドビソフトウェアセキュリティ認定プログラムについて詳しくは、アドビセキュリティ文化ホワイトペーパー（英語）をご確認ください。

Document Cloudサービスのコンプライアンス

Adobe Common Controls Framework（CCF）は、様々なセキュリティ対策とコンプライアンス対策をひとつにまとめたもので、アドビの製品運用チームをはじめ、インフラやアプリケーションを担当する様々なチームにも導入されています。

CCFを策定するにあたり、アドビはクラウドビジネスにおける主なセキュリティ認証の基準を分析。十数種類の業界標準にまたがる1,000項目以上の要件を、アドビ独自の対策に落とし込みました。



Adobe Common Controls Framework（CCF）

Adobe Document Cloudサービスに関連する現在の規制とコンプライアンス

SOC 2は、セキュリティ、機密性、プライバシーに関連する主要な実施制御を定義する、一連のセキュリティ原則です。Adobe Document CloudサービスはSOC 2 Type 2（セキュリティと可用性）に準拠しています。

ISO 27001は、顧客情報の機密性、整合性、可用性を管理する体系的な対策を講じていることを示す厳格な要件を定める基準であり、世界的に浸透しています。Adobe Document CloudサービスはISO 27001:2013に準拠しています。

決済カード業界データセキュリティ基準（PCI DSS）は、専有情報のセキュリティ基準として、クレジットカード番号などの決済カード情報を扱う組織向けに規定されたものです。アドビはPCI DSSに準拠したサービスプロバイダーとして、顧客がPCI要件を満たしてカード所有者の個人情報を安全に扱えるようサポートしています。

米国グラム・リーチ・ブライリー法（GLBA）は、金融機関に顧客の個人情報保護を義務付けています。Adobe Document CloudサービスはGLBAに対応しているため、金融機関の顧客はサービスプロバイダーを使用する際のGLBA要件を遵守できます。

米国連邦リスク・認証管理プログラム（FedRAMP）は、米国政府のプログラムで、クラウド製品やクラウドサービスのセキュリティ評価、権限付与、継続的なモニタリングについて、標準的なアプローチを策定したものです。Adobe Document CloudサービスはFedRAMP向けに設計されているため、顧客はFedRAMP要件を遵守できます。

米国家庭教育の権利とプライバシーに関する法（FERPA）は、米国の学生の教育記録と名簿情報の秘密保持を目的としています。FERPAガイドラインのもと、契約上の合意によってアドビが「学校公認」として規制対象の学生データを取り扱うことができるため、教育機関はFERPAの義務を遵守することができます。

SAFE-BioPharma基準は、ID認証または電子署名の認証を標準化するための要件です。Adobe Document CloudはSAFE-BioPharmaデジタルID標準規格準拠の認証を受けています。Adobe Acrobat DCは、SAFE-BioPharmaに準拠し、そのワークフロー内で安全に使用できます。また、Adobe Document CloudサービスとAdobe SignはSOC 2 Type 2にも準拠しています。

Adobe Signの現在のコンプライアンス体制について詳しくは、Adobe Sign技術概要をご確認ください。

法的義務を確実に遵守すること、アドビのソリューションが自社のコンプライアンスニーズに合致し、自社で運用の安全を適切に保護することについては、顧客が最終的な責任を負います。

アドビの従業員

アドビは世界中に従業員とオフィスが存在するため、次のプロセスと手順を企業全体に導入してセキュリティの脅威から会社を守っています。

従業員による顧客データへのアクセス

アドビでは、稼働している生産システムへのアクセスをネットワークレベルとアプリケーションレベルで制限する技術対策を講じ、Adobe Document Cloudの開発環境と生産環境を分離された状態に保っています。開発システムや生産システムにアクセスする従業員には特定の権限が付与され、業務上の正当な目的がない従業員はそれらのシステムにアクセスできません。

身元調査

アドビは、雇用の目的で身元調査レポートを取得します。アドビが通常調べるレポートの内容および範囲には、適用される法令で許可される範囲において、学歴、職歴、犯罪歴などの裁判記録、同僚や友人への身元照会が含まれます。これらの身元調査要件は米国の新規採用の正社員が対象となり、システム管理または顧客情報へのアクセスを担当する者が含まれます。米国の新規の派遣社員は、アドビの身元調査ガイドラインに準拠した、対象となる派遣会社による身元調査要件の対象となります。米国以外では、アドビの身元調査ポリシーと適用される現地法に従って、特定の新入社員について身元調査を行います。

従業員の退職

従業員がアドビから退職する場合、従業員の上司が退職届を提出します。承認されると、アドビの人事担当が電子メールワークフローを開始して関係者にその従業員の退職日までに特定の処理をおこなうように通知します。アドビが従業員を解雇する場合は、人事担当が従業員の退職日時を示した同様の電子メール通知を関係者に送信します。

アドビの企業セキュリティ担当は次の処理のスケジュールを設定して、従業員の退職日に、今後その従業員がアドビの機密情報ファイルやオフィスにアクセスできないようにします。

- 電子メールアクセスの削除
- リモートVPNアクセスの削除
- オフィスおよびデータセンターの入退出バッジの無効化
- ネットワークアクセスの終了

要求に応じて、上司はアドビのオフィスまたは建物から退職する従業員に警備員を同伴させることができます。

施設のセキュリティ

アドビのすべてのオフィス所在地では、現地の警備員を採用して敷地を24時間体制で保護しています。アドビの従業員は、建物に入るためのキーカード型IDバッジを携帯しています。訪問者は正面入口から入り、受付で署名して一時的な訪問者IDバッジを提示します。訪問者には従業員が同伴します。サーバー機器、開発マシン、電話システム、ファイルサーバーとメールサーバーおよびその他のデリケートなシステムは、環境が制御されたサーバールームに常時設置されており、そのサーバールームには認可されたスタッフメンバーのみがアクセスできます。

ウイルス対策

アドビでは、送受信されたすべての企業電子メールをスキャンして既知のマルウェアによる脅威をスキャンしています。

顧客データの機密保持

アドビは、すべての顧客データを常に機密情報として扱います。お客様との契約で許可されている場合、およびアドビ利用条件とアドビプライバシーポリシーに規定されている場合を除き、アドビはお客様の代わりに収集した情報を使用または共有しません。

まとめ

このホワイトペーパーで説明したセキュリティに関するアドビの事前対応型アプローチと厳格な手順によって、Adobe Acrobat DC、Acrobat Reader DC、Document Cloudサービスのセキュリティとお客様の機密情報は保護されています。アドビでは、デジタルエクスペリエンスのセキュリティを重要視し、継続的に脅威の動向をモニタリングして悪意のある行為を防ぐとともに、顧客データのセキュリティ確保に努めています。

詳しくは、Adobe Trust Centerをご確認ください。

Adobe

アドビ システムズ 株式会社
〒141-0032 東京都品川区大崎 1-11-2
ゲートシティ大崎 イーストタワー
www.adobe.com/jp

Adobe Inc.
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

5/19