Adobe Creative Cloud エンタープライズ版 セキュリティ概要

Contents

概要

Adobe Creative Cloud エンタープライズ版では、アドビのクリエイティブデスクトップおよびモバイルアプリ、クラウドサービス、グループでの共同作業機能、およびライセンス管理ツールを大規模な組織内でお使いいただけます。また、柔軟なデプロイメント、シングルサインオンを使用した Federated ID などの ID 管理オプション、年 1 回のライセンス補正、エンタープライズレベルのカスタマーサポートも含まれており、他のアドビエンタープライズツールとも連携して利用することができます。

アドビでは、デジタルアセットのセキュリティを重要視し、ソフトウェア開発プロセスおよびツールへの徹底したセキュリティの統合から、部門の枠を超えたインシデント対応チームに至るまで、先を見越した迅速な対応に努めています。さらに、パートナー、研究者および他の業界団体と協力して、最新の脅威やセキュリティのベストプラクティスを理解し、提供する製品およびサービスに継続的にセキュリティ対策を組み込んでいます。

Creative Cloud エンタープライズ版は、根本的にセキュリティを考慮して設計されています。Creative Cloud エンタープライズ版は、デスクトップアプリケーションからアクセスされる場合も、クラウドサービスからアクセスされる場合も、Admin Console が管理する一意のユーザー ID によって制御され、ユーザーが所属する企業のディレクトリサービスと連携させることもできます。コンテンツは伝送中も保存中も暗号化され、保存中のコンテンツはお客様固有の暗号化キーを利用してさらに保護することができます。

お客様のコンテンツにアクセスするアドビサービスは、SOC 2 認証、ISO27001 認証および PCI 認証（適切な場合）の取得を完了しているか、審査段階にあります。アドビのクラウドサービスは、最高水準のソリューションによって保護され、管理され、監視されています。管理と開発のライフサイクルの両方で、業界標準のソフトウェアセキュリティ手法を活用しています。

アドビでは、Amazon Web Services（AWS）の最善の組み合わせのホスティングを利用して複数の地域で複数のデータセンターを構成し、常に複製されたバックアップデータを用意することで、お客様が必要なときにコンテンツを入手できるようにしています。

このホワイトペーパーでは、Adobe Creative Cloud におけるユーザーエクスペリエンスやデータのセキュリティを強化するために、アドビが実装する事前対応型アプローチおよび手順について説明します。

Creative Cloud エンタープライズ版の概要

Creative Cloud エンタープライズ版は、大規模組織におけるクリエイティブ制作ワークフローのためのソリューションで、組織内のクリエイティブおよびデザインチームが共同作業を容易にします。このソリューションは、1）デスクトップアプリケーション、2）モバイルアプリ、3）Admin Console、4）一連のクラウドサービスという 4 つの要素で構成されています。

デスクトップアプリケーション

Adobe Photoshop、Illustrator といったデスクトップ版はエンドユーザーのワークステーションで動作します。IT 部門でパッケージ化したものを Microsoft SCCM/JAMF Casper Suite などの標準方式でデプロイすることも、エンドユーザーが直接アドビからアプリケーションをダウンロードするセルフサービス方式を採用することも可能です。Admin Console で、各ユーザーの ID（LDAP、Microsoft Active Directory ID など）を基準にライセンスが割り当てられ、その後、同じ Console で各ユーザーにアプリケーションとサービスの利用資格が割り当てられます。ユーザーが Photoshop などのアプリケーションを起動すると、Admin Console で検知され、そのアプリケーションの利用資格の有無が判断されます。データの伝送は暗号化され、ユーザー情報はセキュリティとプライバシーの業界標準とベストプラクティスに従い処理されます。

モバイルアプリ

Adobe Photoshop Sketch CC、Adobe Comp CC などのモバイルアプリは、エンドユーザーのモバイルデバイスで動作し、AirWatch などのモバイルデバイス管理（MDM）ソリューションで管理することもできます。モバイルアプリケーションで作成したコンテンツは、モバイルデバイスだけでなく、クラウド上の暗号化されたストレージでも保持されます（詳しくは、下記の Creative Services 参照）。データの伝送は暗号化され、モバイルサービスへのアクセスは、Admin Console で設定されたユーザー ID により判断されます。

Admin Console

ライセンスとサービスの利用資格の設定は、Admin Console でおこないます。Console は、SAML2.0 準拠のエンタープライズ ID 管理認証システムに組み込むことが可能です。また、一連の API により認証を自動化することもできます。製品ライセンスグループはエンタープライズディレクトリグループにミラーを作成することも、個別に特定のクリエイティブワークグループを指定することも可能です。次項で説明するクラウドサービスにて保存されるコンテンツは、Admin Console で専用暗号鍵を設定でき、必要に応じて、あらゆるコンテンツへのアクセスを無効にすることも可能です。Admin Console との通信は暗号化され、管理者アクセスは契約開始時にご指定いただく限定ユーザーに限られます。

クラウドサービス

クラウドサービスには、クリエイターが効率的に作業し短時間で作品を仕上げるための、様々な生産性向上機能が組み込まれています。たとえば、多様なファイルを使用する、プロジェクト上で共同作業する、フォントやストック画像を活用するなど、高品質の作品を制作できる機能があります。クラウドサービスの利用資格は、Admin Console で管理し、各ユーザー固有の ID に基づき各サービスへのアクセスが許可されるので、利用資格のない人にアクセスされることはありません。クラウドサービスは、Amazon の AWS により構築されたマルチテナントインフラストラクチャー上で運用しています。データの伝送は暗号化され、ユーザーが作成したコンテンツの保存時も暗号化されます。また、上記に示すとおり、専用暗号鍵を使用して、より高度な暗号化の保護を加えることも可能です。

Creative Cloud エンタープライズ版の ID システム

権利付与と ID 管理

システム管理者は、Adobe Admin Console でユーザー指定ライセンスを設定することで、Adobe Photoshop や Adobe Illustrator などの Creative Cloud デスクトップアプリケーションへのアクセスをエンドユーザーに許可したり、クラウドサービスの使用を許可したりすることができます。

3 種類のユーザー指定ライセンスを使用できます。

- **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。システム管理者が Adobe ID アカウントに権限を設定することで、Creative Cloud エンタープライズ版のリソースにアクセスできます。
- **Adobe 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です。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。
- **Adobe Federated ID**：導入先組織が管理するアカウントです。すべての ID プロファイル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、すべての関連するアセットとともにシステム管理部門によって作成、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。

アプリケーションとサービスの権利付与は、Adobe Admin Console でおこないます。

パスワードのロックアウト手順

システム管理部門は、エンタープライズ版リソースにアクセスできる招待された Adobe ID、Enterprise ID および Federated ID に、以下で説明する 3 種類のパスワードポリシーを適用できます。

Adobe ID および Enterprise ID では、SHA 256 ハッシュアルゴリズムを、パスワードソルトと多数の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 Adobe ID アカウントのセキュリティ脅威を迅速に軽減しています。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ないので、アドビによるアカウントの監視はおこなわれません。

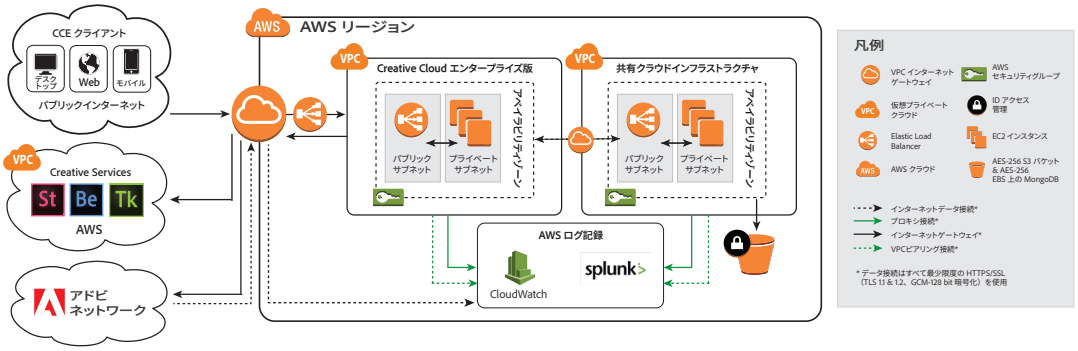
アカウント管理

ユーザー指定アカウントは Adobe Admin Console で管理できます。Adobe Admin Console は使いやすいコンソールであり、これによりシステム管理スタッフは、組織内の権限付与の管理、つまり、どのユーザーとグループを、どの Creative Cloud アプリとサービスにアクセス可能にするかの管理をおこなうことができます。さらに、Adobe Admin Console でユーザーを管理して、Adobe Document Cloud と Adobe Marketing Cloud へのアクセス資格を付与することも可能です。システム管理者は、Console を利用して、カスタマーケアに対する問い合わせケースを作成したり、エキスパートサービスを予約することで素早く問題を解決することができます。

システム管理者は、Adobe Admin Console を利用して Enterprise ID および Federated ID アカウントを作成、管理、削除できます。これらのアカウント用の Cloud ストレージは個別のストレージとして割り当てられるので、システム管理部門はユーザーの Creative 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。ただし、従業員のアカウントを所有し、アクセス権を取り消すことはできます。シェアードサービスストレージが割り当てられている Enterprise ID または Federated ID を削除すると、ユーザーはそのストレージ内のデータにアクセスできなくなり、ユーザーのデータは 90 日後に削除されます。

システム管理者は、Adobe 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。システム管理者は Adobe ID アカウントを制御できませんが、エンタープライズ版上のアカウントを削除し、アカウントに付与したエンタープライズストレージ容量を回収できます。その場合も、データは 90 日後に削除されます。

Creative Cloud エンタープライズ版のアーキテクチャ



Adobe Creative Cloud エンタープライズ版は、デスクトップアプリ、モバイルアプリ、クラウドサービスが組み合わされたものになります。ユーザー指定ライセンスによってプロビジョニングされた Creative Cloud エンタープライズ版ユーザーは、3 つのエンドポイントからクラウドサービスにアクセスすることができます。

- Adobe Photoshop などのデスクトップアプリと Creative Cloud デスクトップアプリケーション
- Web ブラウザー
- Adobe Capture CC、Adobe Photoshop Sketch、Adobe Lightroom Mobile などのモバイルアプリ

使用できるツールとサービスの説明については、https://www.adobe.com/jp/creativecloud/business/enterprise.html を参照してください。

それぞれのエンドポイントで、前述のユーザー指定ライセンスにより ID 認証し、Creative Cloud エンタープライズ版のコンテンツにアクセスします。

ユーザーが Adobe Creative Cloud へのアクセスに使用したエンドポイントによって、利用できるサービスは異なります。たとえば、モバイルアプリからは、Creative Cloud にアクセスして、ユーザー認証、設定の同期、モバイル作品などのコンテンツの共有ができます。また、Creative Cloud デスクトップアプリケーションからは、Photoshop などのクリエイティブデスクトップアプリのダウンロードとアップデート、Adobe Typekit からフォントのダウンロード、ローカルシステムと Creative Cloud のストレージ間のファイルのアップロードとダウンロードができます。

各組織のエンドポイントの種類にかかわらず、Creative Cloud のアクセスはすべて HTTPS/SSL 経由の一般サービスにより制御されます。コンテンツは、伝送中は AES 128 ビット GCM 対称キー暗号化のブロック暗号によって、また保存中は NIST 800-57 推奨に準拠する FIPS 140-2 承認暗号化アルゴリズムを使用する AES 256 ビット対称セキュリティキーで、暗号化されます。Adobe Creative Cloud エンタープライズ版の認証を受けたユーザーは、IT 管理者が Adobe Admin Console で資格を付与したサービスとアプリケーションにアクセスできます。その後、資格を付与され、エンドポイントによって許可されているすべてのアクションを実行できます。たとえば、Photoshop のユーザーは、Creative Cloud ライブラリで共同作業し、カラー、グラフィック、文字スタイルをチームの他のメンバーと共有することができます。

Creative Cloud エンタープライズ版のコンテンツストレージ

Creative Cloud エンタープライズ版はマルチテナントストレージを利用しています。お客様のコンテンツは、Amazon Elastic Compute Cloud（EC2）インスタンスによって処理され、Amazon Elastic Block Store（EBS）上の MongoDB インスタンスによって、Amazon Simple Storage Service（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 S3 バケットに保存され、コンテンツに関するメタデータは MongoDB によって EBS に保存され、その 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。

S3 に保存されているコンテンツとアセットは、お客様ごとおよびお客様のクレーム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。専用キーは、キー管理に制御とセキュリティの追加レイヤーを提供し、アドビが 1 年ごとにキーを自動的にローテーションする Amazon Key Management Service（KMS）によって管理されます。必要なときは、IT 管理者が Admin Console でキーを取り消し、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が可能です。詳しくは、後述の「専用暗号化キー」を参照してください。

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、破損を防いで完全性を保証するため、体系的なデータ検証とチェックサム計算を受けます。最後に、保存されているコンテンツは、その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、2 つの場所でデータが失われた場合で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）：http://www.mongodb.org
- Amazon S3 サービス：https://aws.amazon.com/jp/s3/faqs/
- Amazon KMS サービス：https://aws.amazon.com/jp/kms/faqs/
- Amazon EC2 サービス：https://aws.amazon.com/jp/ec2/

専用暗号化キー

Creative Cloud エンタープライズ版に保存されるコンテンツは、前述したように暗号化されます。IT 管理者は、組織内の一部またはすべてのドメイン用の専用暗号化キーの生成をアドビに依頼することで、制御とセキュリティをさらに強化できます。コンテンツは専用暗号化キーを使用して暗号化されます。この暗号化キーは、必要であれば、Admin Console から無効にすることができます。キーを無効にすると、そのキーを使用して暗号化されているすべてのコンテンツは、エンドユーザーがアクセスできない状態になります。

専用キーを使用した暗号化の管理について詳しくは、以下をご覧ください。

- https://helpx.adobe.com/jp/enterprise/help/encryption.html
- https://helpx.adobe.com/jp/enterprise/help/encryption-faq.html

Creative Cloud サービスの種類

Creative Cloud サービスには SaaS ベースのサービスが含まれています。一部のサービスはユーザーが生成したコンテンツを保存でき、権利が付与されている場合は Creative Cloud のすべてのエンタープライズサービスとエンドポイントで利用できます。IT 管理者は、Adobe Admin Console を使用して、これらのサービスに対するエンドユーザーアクセスと権利の付与を管理できます。Creative Cloud サービスについて詳しくは、以下をご覧ください。

- Adobe Portfolio（英語）：https://www.myportfolio.com/
- Behance：https://www.behance.net/
- Creative Cloud Extract：http://www.adobe.com/jp/creativecloud/extract.html
- Lightroom：https://www.adobe.com/jp/products/photoshop-lightroom.html
- Phonegap Build（英語）：https://build.phonegap.com/
- Publish Online（InDesign）：https://helpx.adobe.com/jp/indesign/using/publish-online.html
- オンライン共有：https://helpx.adobe.com/jp/experience-design/help/share-designs-and-prototypes.html
- Story Plus（英語）：https://creative.adobe.com/products/story-plus
- Typekit：https://typekit.com/

Amazon Web Services

前に説明したように、Creative Cloud エンタープライズ版のコンポーネントは、アメリカ、欧州連合（EU）、アジア太平洋の各地域では、Amazon EC2 および Amazon S3 などの 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です。

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 のセキュリティサイトを参照してください。

AWS とアドビの運用責任

AWS は、ハイパーバイザー仮想化レイヤーから Adobe Creative Cloud エンタープライズ版が運用される施設の物理セキュリティまでを運用、管理および制御します。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

AWS で『セキュリティプロセスの概要ホワイトペーパー』を提供しています。AWS のセキュリティについて詳しくは、AWS ホワイトペーパー（英語）を参照してください。

アドビは Adobe Creative Cloud のすべてのお客様の ID および利用権限に関するデータを Amazon Web Services の米国東部リージョンに保存します。米国内のお客様については、カリフォルニア州サンノゼまたはテキサス州ダラスにある AWS の施設に解析データを保存します。米国以外のお客様については、英国ロンドンの AWS の施設に解析データを保存します。

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。

顧客データの分離／顧客の隔離

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、外部ネットワークとの境界およびネットワーク内の主な境界で通信の監視と制御を行うため、ファイアウォールなどのネットワーク境界をつなぐネットワーク機器を採用しています。これらのネットワーク機器は、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 の 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 Dos（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、Amazon Web サイトの AWS：セキュリティプロセスの概要ホワイトペーパー（英語）をご覧ください。

侵入検知

アドビは、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 Creative Cloud を積極的にモニタリングします。

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 Creative Cloud のお客様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 Creative Cloud 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。また 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。AWS のセキュリティについて詳しくは、AWS：セキュリティプロセスの概要ホワイトペーパー（英語）を参照してください。

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 Console（英語）を通じてお客様に通知します。アドビもまた Adobe Creative Cloud 用の Status Health Console 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 1、Type 2 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：セキュリティプロセスの概要ホワイトペーパー（英語）または Amazon セキュリティ Web サイトをご覧ください。

物理施設のセキュリティ

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、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、引き続き Amazon または Amazon Web Services 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。

火災対策

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消火装置が取り付けられています。この火災検出システムでは、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、煙感知器を使用しています。これらのエリアは、予作動式放水スプリンクラー、またはガス消火設備によって守られています。

空調環境のコントロール

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、空調設備を採用することで、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。

ビデオ監視

専門のセキュリティスタッフが、ビデオ監視カメラ、侵入検出システム、その他の電子的手段を用いて、AWS データセンターの建物の入口とその周辺の両方で物理的アクセスを厳しく管理しています。

障害回復

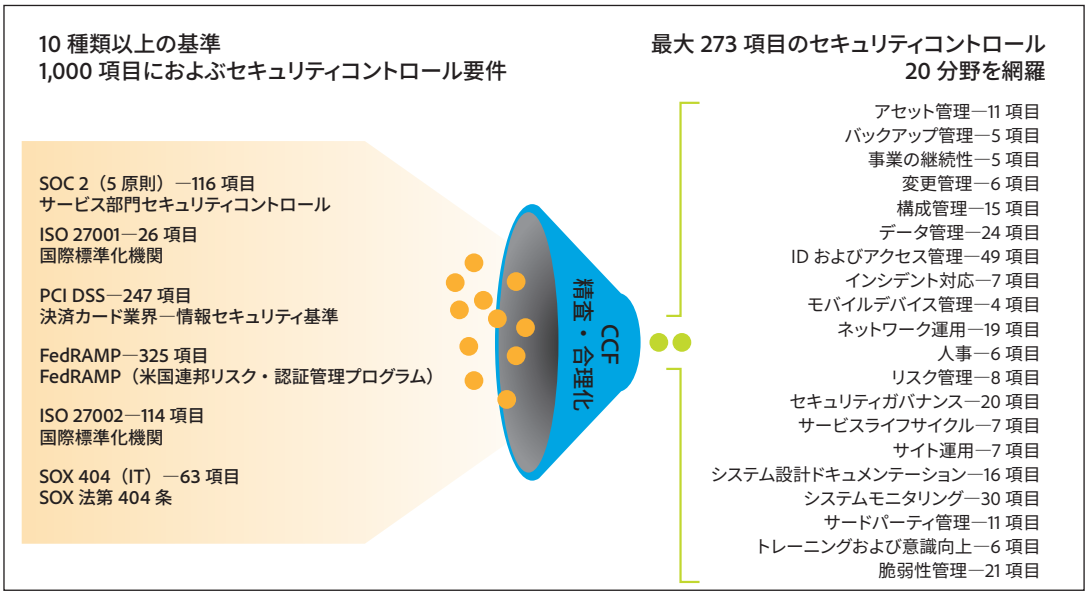
AWS データセンターは、高いレベルの可用性を備え、影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。すべてのデータセンターは、世界各地にクラスターの状態で構築されています。24 時間、365 日体制のサービスをオンラインで顧客に提供しており、「コールド」の状態のデータセンターは存在しません。障害時には、自動プロセスが、影響を受けるエリアから顧客データを移動します。

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、Amazon セキュリティ Web サイトを参照してください。

Adobe Common Controls Framework

ソフトウェア層からセキュリティを保護するために、アドビは Adobe Secure Product Lifecycle を採用しています。これについては次のセクションで説明します。物理層からの保護については、セキュリティ保護プロセスの基本的枠組みを構築して様々なセキュリティ対策を実施。インフラ、アプリケーション、サービスを保護するとともに、業界が認定する数々のベストプラクティス、基準、認証に準拠しています。

Adobe Common Controls Framework（CCF）を作成する際に、一般的に普及している各種セキュリティ認定の内容をアドビで分析したところ、認定基準には重複するものが多いことが判明しました。そこでアドビは、関連性の高いクラウドセキュリティのフレームワークや基準の中で必要とされている 1,000 項目以上の事項を精査したうえで、本当に必要な約 200 項目に絞ってアドビ独自の CCF を策定しました。CCF コントロール担当者は、セキュリティコントロールの実施に関して、アドビの関係者と顧客の期待に応えるために何が必要かを明確に理解しています。

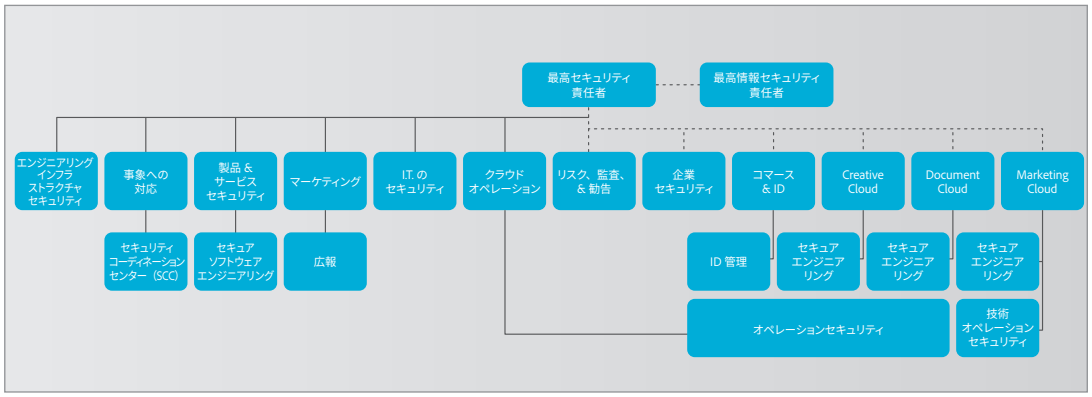


Adobe Common Controls Framework（CCF）

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）も管理します。ASSET は、セキュリティの専門家が集まった専任のチームです。Creative 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担っています。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

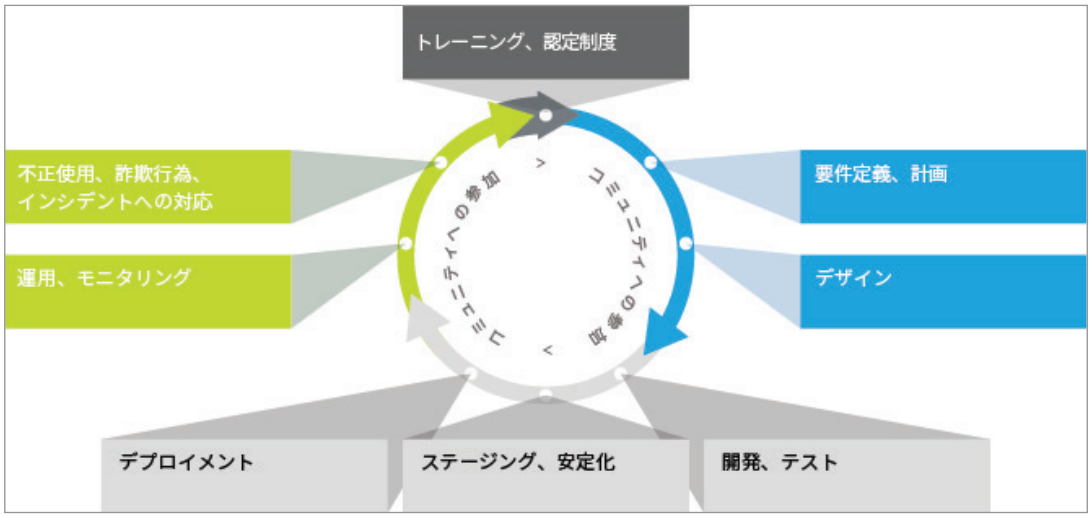
アドビの安全な製品開発

他のアドビの製品およびサービスの関連部署と同様、Creative Cloud 関連部署も 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、デプロイメントに至るまで、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

Adobe SPLC の活動には、それぞれの Creative Cloud サービスに応じて、次のような推奨プラクティス、プロセス、ツールの一部またはすべてが含まれています。

- すべての製品チームに対するセキュリティトレーニング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
- Creative Cloud セキュリティチームが「Open Web Application Security Project（OWASP）Web アプリケーションの脅威 Top 10」と「CWE/SANS 最も危険なプログラミングエラー Top 25」に対処するための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
- ユーザー生成コンテンツの検証
- 静的および動的なコード分析
- 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



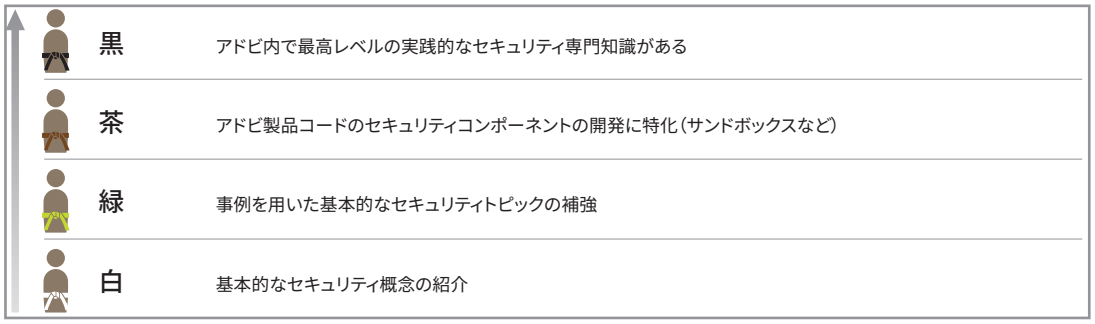
Adobe Secure Product Lifecycle（SPLC）

アドビのセキュリティトレーニング

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トレーニングを実施し、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。

プログラムには 4 つのレベルがあり、それぞれに色付きの「帯」（白、緑、茶、黒）が指定されています。白および緑のレベルは、コンピューターベースのトレーニングを修了すると達成されます。その上の茶および黒のレベルに到達するには、数ヶ月から 1 年にわたるセキュリティプロジェクトの実務を修了する必要があります。茶帯または黒帯を獲得した従業員には、製品チーム内のセキュリティチャンピオンおよびエキスパートの称号が与えられます。アドビでは定期的にトレーニング内容を刷新し、新たな脅威や緩和策、新しい制御方法やソフトウェア言語に対応しています。



Adobe Secure Software Engineering 認定制度

Creative Cloud 関連部署では様々なチームがさらなるセキュリティトレーニングやワークショップに参加し、セキュリティが組織内や企業全体での役割に及ぼす影響について認識を高めています。

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。

アドビのリスクと脆弱性管理

侵入テスト

アドビは、承認した第三者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。当該第三者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。

社内では、Adobe Creative Cloud セキュリティチームが、リリースの前に毎回 Creative Cloud アプリケーションのリスク評価を実行します。このセキュリティレビューは、ネットワークトポロジ／インフラストラクチャのセキュリティ確保に信頼のある、高度な訓練を受けたセキュリティスタッフが実施し、ファイアウォール、ロードバランサー、サーバーハードウェアについてネットワークのセキュリティ設定に問題がないか、アプリケーションレベルの脆弱性はないかということを調べます。セキュリティ対策として、脅威モデリングと脆弱性のスキャニング、アプリケーションの静的分析、動的分析なども実行します。Creative 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。

侵入テストは年 1 回以上、およびメジャーリリースの後に実施します。脆弱性スキャンは毎月、Web とデータベーススキャンは四半期ごとに実施します。

インシデントへの対応

脆弱性や脅威が日々進化する中、アドビは新たに発見された脅威を軽減すべく懸命に取り組んでいます。US-CERT、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。

Creative Cloudがアナウンスされた重大な脆弱性の危険にさらされると、Adobe PSIRT（製品セキュリティインシデント対応チーム）が Creative Cloud 関連部署内の該当するチームに脆弱性について通知し、軽減策を講じます。

Creative Cloud を含むアドビのクラウドベースサービスでは、セキュリティコーディネーションセンター（SCC）でインシデントへの対応や意思決定、外部モニタリングを一元的に管理し、全機能の一貫性と問題の迅速な解決を実現します。

アドビの製品やサービスで問題が発生した場合、SCC は関連するアドビ製品のインシデント対応チームおよび開発チームと連携して、次の実績あるプロセスを使用して問題を特定、軽減、解決します。

- 脆弱性の状態評価
- プロダクションサービスにおけるリスクの軽減
- セキュリティが侵害されたノードの検疫、調査、破棄（クラウドベースのサービスのみ）
- 脆弱性のための修正プログラムの開発
- 問題を阻止する修正プログラムのデプロイ
- アクティビティのモニタリングと解決策の確認

フォレンジック分析

インシデントの調査に関して、Creative 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。

アドビの所在地

アドビは世界中にオフィスがあるため、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。

物理的なセキュリティ

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

マルウェアの影響を受けやすいすべてのシステム（Linux 以外の Windows サーバーなど）と従業員のアセット（ラップトップなど）に対して、マルウェアに対抗するための保護対策を講じています。マルウェアに対抗するには、以下をおこなう必要があります。

- 署名のスキャンを毎日更新する
- スキャンエンジンのバージョンをベンダーがリリースした最新のバージョンに常に更新する
- システム全体のスキャンを毎週実行する
- イベントログとアラートを生成する
- スキャン結果から特定された問題を権限が与えられた関係者またはグループに伝達する
- リアルタイムのスキャンを有効にする
- ウイルス対策の仕組みを無効にできないようにする

アドビの従業員

従業員による顧客データへのアクセス

技術的なコントロールを使用して、稼働しているシステムへのネットワークレベルおよびアプリケーションレベルでのアクセスを制限し、セグメント化された Creative Cloud の開発と生産環境を維持します。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。従業員には最小限のアクセス権限が与えられ、アクセス権限は 3 ヶ月毎に見直されます。

身元調査

アドビは、雇用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、システムを管理したり顧客情報にアクセスしたりすることになる米国の新規の正社員に適用されます。米国の新規の派遣社員には、アドビの身元調査ガイドラインに従って適切な派遣会社を通して身元調査要件が課されます。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おこないます。

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処理フォームを提出します。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。

お客様のデータの秘密保持

アドビは、顧客データを常に機密情報として扱います。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、アドビはお客様から収集した情報のアクセス、使用、共有をおこなうことはありません。アドビのプライバシーへの対応については、アドビプライバシーセンターをご覧ください。

セキュリティコンプライアンス

AWS は、ISO 27001、SOC 1、SOC 2、PCI DSS およびその他のセキュリティフレームワークの認証を取得し維持しています。

アドビのすべてのサービスは、文書化された一連の包括的なセキュリティプロセスによって管理され、様々なセキュリティ監査を受けて品質の維持および改善を図っています。アドビのサービスは ISO 27001 標準の自己レビューを常に受けており、基盤サービスインフラストラクチャは SOC 2 - Security の認定を受けています。

アドビは、SOC 2 信用提供の原則（Trust Services Principles）と ISO 27001 セキュリティ標準に準拠するよう、Creative Cloud 運用のセキュリティプロセスおよびコントロールの開発、実装、改善に取り組んでいます。Adobe Creative Cloud エンタープライズ版は「FERPA 対応」となっています。これは、FERPA ガイドラインに基づき、契約上の合意によりアドビが「学校関係者」とみなされ規制対象の学生データを取り扱うことができるため、教育機関のお客様に定められた FERPA の要件を満たすことを意味します。

セキュリティホワイトペーパーのリストについては、http://www.adobe.com/jp/security/resources.html を参照してください。アドビのコンプライアンスの総合的セキュリティ戦略の詳細については、Adobe Cloud Services Compliance Overview ホワイトペーパー（英語）を参照してください。

まとめ

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ています。本ホワイトペーパーで説明したセキュリティの事前対応型アプローチと厳格な手順によって、Creative Cloud データをセキュリティ保護しています。本ホワイトペーパーで説明されていないセキュリティに関する疑問をお持ちの場合は、アドビの担当者にお問い合わせいただくか、http://www.adobe.com/jp/security.html をご覧ください。

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 Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

3/17