Adobe Creative Cloud グループ版のセキュリティ概要

目次

1: アドビのセキュリティ
1: Adobe Creative Cloud グループ版
1: Creative Cloud グループ版のストレージとストレージオプション
1: Creative Cloud グループ版の管理ツール
2: アドビのセキュリティ組織
2: アドビの安全な製品開発
3: アドビのセキュリティトレーニング
4: Creative Cloud のアーキテクチャ
5: Amazon Web Services（AWS）について
6: Creative Cloud グループ版の認証（Adobe ID）
6: アドビのリスク／脆弱性管理
7: AWS データセンターの物理統制と環境統制
8: アドビの所在地
8: アドビの従業員
9: 顧客データの機密保持
9: セキュリティコンプライアンス
9: まとめ

アドビのセキュリティ

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。

このホワイトペーパーでは、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。

Adobe Creative Cloud グループ版

Creative Cloud グループ版には、すべての Creative Cloud デスクトップアプリケーション（Adobe Photoshop CC、Adobe Illustrator CC など）に加え、グループや小中規模の組織向けのサービスと機能が含まれています。Creative Cloud グループ版は、通常版（フル版）と単体サブスクリプションの 2 つのプランで利用でき、どちらも直感的なアドミンコンソールで購入申請、管理、展開を簡単に行えます。

Creative Cloud グループ版のストレージとストレージオプション

Creative Cloud グループ版では、Amazon S3（Amazon Simple Storage Service）を使用するクラウドベースのストレージを通常版（フル版）の各メンバーに最大 100GB（単体サブスクリプションのメンバーには 20GB）用意し、データを保存して取り出すための信頼性の高いデータストレージインフラストラクチャを提供しています。

デフォルトのストレージオプションではユーザーのデータはクラウドで保存されますが、クラウドで保存しない方法や企業ネットワーク内でのネットワーク接続を遮断する方法を選択することもできます。詳しくは、アドビのサイトをご覧ください。

Creative Cloud グループ版の管理ツール

アドミンコンソール

Creative Cloud グループ版には、IT 管理者がシートの購入申請からユーザーの追加、ライセンスの管理、Creative Cloud アプリケーションの展開とアップデートまでを簡単に行うための Web ベースのアドミンコンソールが含まれています。管理者はユーザーに電子メールを送信して各自の Adobe ID を作成するよう依頼します。

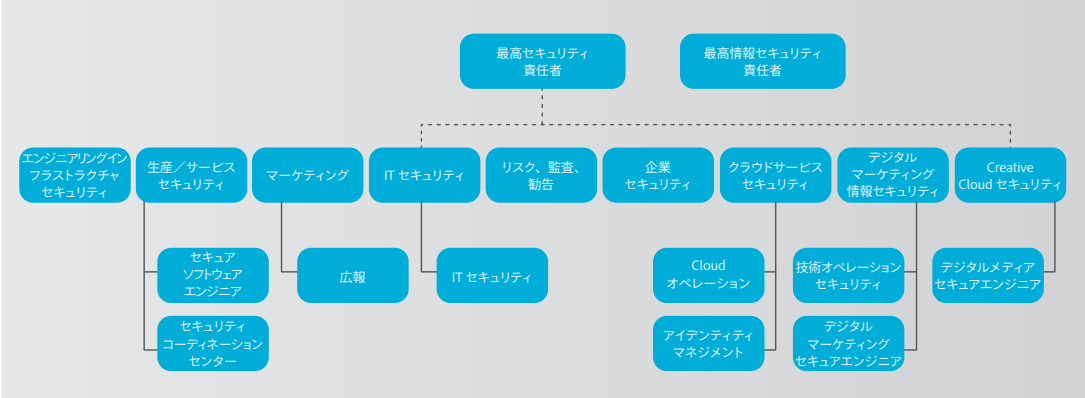
Creative Cloud Packager

Creative Cloud グループ版のアドミンコンソールから利用できる Creative Cloud Packager は、IT 管理者が Creative Cloud のすべてのアプリケーション、または選択したアプリケーションのみを一元的に展開するためのツールです。Creative Cloud Packager を使用すると、全員が確実に同じバージョンのソフトウェアを利用できるため、サポート費用の節減につながり、また多くのユーザーが同じソフトウェアを同時にダウンロードすることがなくなるので、ネットワークの負担を軽減できます。IT 管理者は、Creative Cloud グループ版加入時にまず自分の Adobe ID を作成し、アドミンコンソールの管理者または、サブ管理者として登録しそれを使用して Creative Cloud Packager にログインします。Creative Cloud Packager および展開方法について詳しくは、アドビの Web サイトでご覧ください。

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。CSO のオフィスで、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）の実装について統括しています。

CSO はまた、Adobe Secure Software Engineering Team（ASSET）も管理します。ASSET は、セキュリティのエキスパートが集まった専任のチームです。Adobe 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 の研究者は、各アドビ製品のセキュリティおよび運用を担当するチームと協力して、製品やサービスに適切なレベルのセキュリティを実装し、さらに開発、導入、運用、インシデント対応に繰り返し実行できる明確なプロセスのセキュリティプラクティスについて、それらのチームにアドバイスします。



アドビのセキュリティ組織

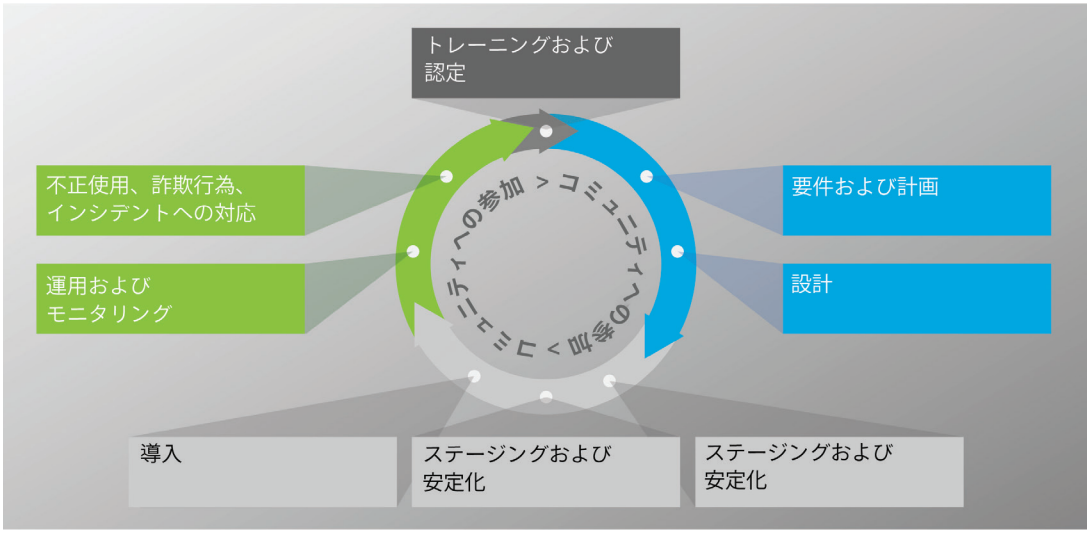
アドビの安全な製品開発

他のアドビの製品およびサービスの組織と同様、Creative Cloud 組織も Adobe Secure Product Lifecycle（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、継続的なコミュニティ活動によって補完され、技術、セキュリティプラクティス、脅威の展望に変化が生じても、常に最新状態が保たれるよう進化します。

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の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
- レビュー、レスポンスプラン、開発者向け教材のリリースの準備



Adobe Secure Product Lifecycle（SPLC）

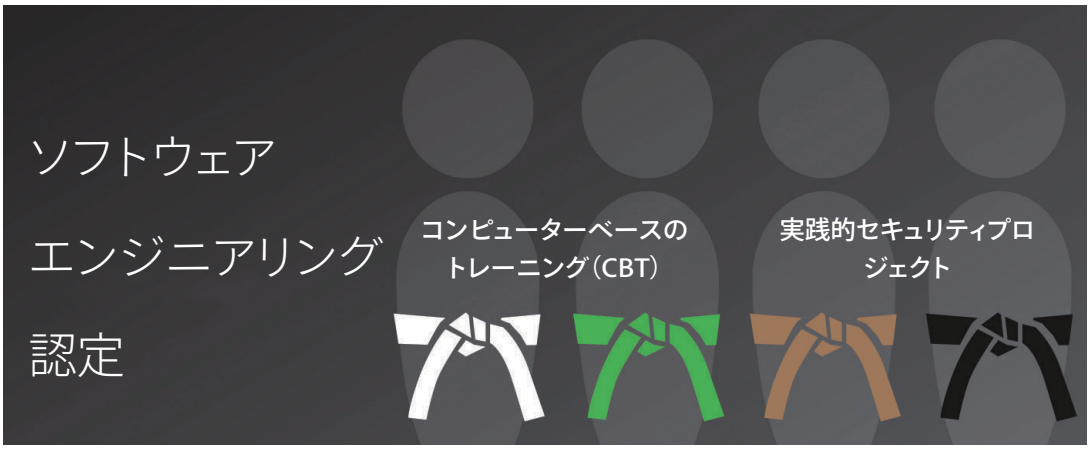
アドビのセキュリティトレーニング

アドビ社内での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。さらに上位の茶および黒のレベルは、数か月から 1 年にわたる実務経験を伴うセキュリティプロジェクト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になります。新たな脅威や驚異の軽減、さらには新しい規制やソフトウェア言語を反映するために、アドビは定期的にトレーニングを更新します。

Creative Cloud 部門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。



アドビ社内でのアドビソフトウェアセキュリティ認定プログラム

Creative Cloud のアーキテクチャ

アドビは Creative Cloud グループ版のコンポーネントすべてに対応する集中型のホスティングインフラストラクチャの構築を目指していますが、現在のところ、Creative Cloud グループ版の様々なコンポーネント向けに主に 2 つのホスティングインフラストラクチャを利用しています。

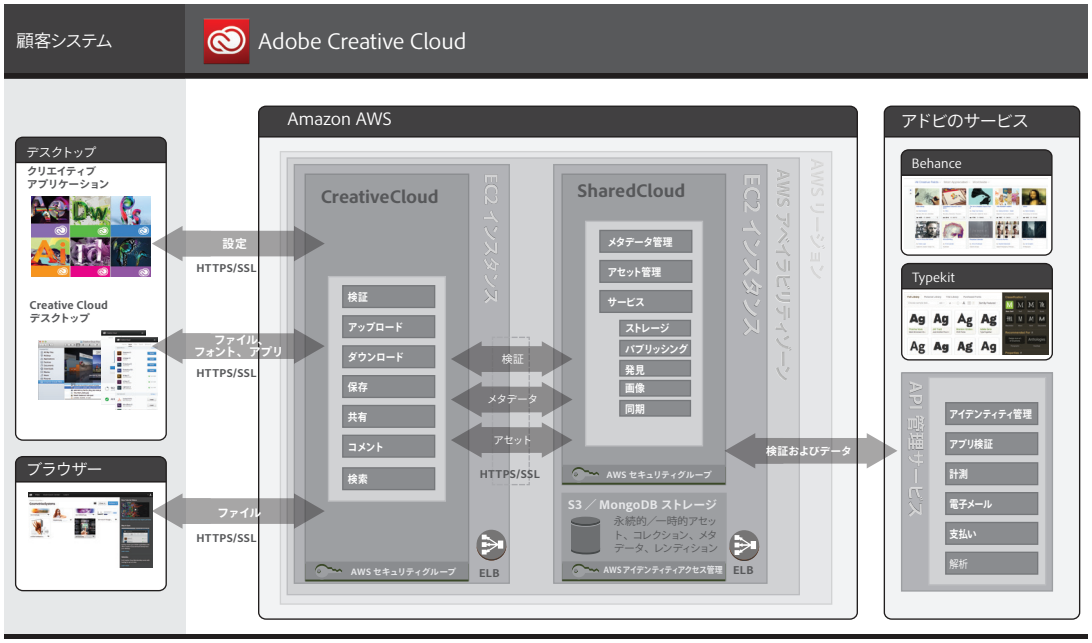
- Amazon Web Services（AWS）：Creative Cloud グループ版のほとんどのコンポーネントは、アメリカ、ヨーロッパ、アジア太平洋では、Amazon Elastic Compute Cloud（Amazon EC2）、Amazon Simple Storage Service（Amazon S3）などの AWS でホスティングされています。Amazon EC2 は、クラウド内で規模の変更が可能なコンピューター処理能力を提供し、Web スケールでのコンピューター作業を容易にする Web サービスです。Amazon S3 は、容量に関係なくデータを保存・取得できる信頼性の高いデータストレージインフラストラクチャです。

  AWS は、世界中の何千もの企業に利用されるソフトウェアサービス向けに信頼できるプラットフォームを提供し、またセキュリティのベストプラクティスに従ったサービスを提供して、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。詳しくは、AWS セキュリティホワイトペーパーをご覧ください。

- 専用データセンター施設：現在アドビは、人目に付きにくい安全な専用データセンター施設で、Adobe ID をはじめとする Adobe Creative Cloud 用のいくつかのサービスをホスティングしています。これらのデータセンターでは、業界標準のインフラストラクチャと物理的なセキュリティ対策を採用しています。

* 作品の展示・共有のためのオンラインプラットフォームである Adobe Behance は、Rackspace が所有する安全な専用データセンターに所在します。

* Typekit は、Rackspace と AWS の両方でホスティングされています。Rackspace は、Typekit Web アプリケーションをシカゴのデータセンターでホスティングしています。同 Web アプリケーションは、AWS に保存されているソースフォントを用いてカスタムフォントの「キット」を作成します。一部の顧客は Rackspace がホスティングするカスタムキット用のオリジンサーバーを持っていますが、多くの場合、作成されたキットは AWS に置かれます。



Creative Cloud グループ版の論理アーキテクチャ

Creative Cloud アプリケーションは、AWS 内の Adobe Shared Cloud プラットフォーム上に構築されています。アップロードされたファイルは、Amazon Elastic Compute Cloud（EC2）インスタンスによって処理され、AWS リージョン内の Identity and Access Management（IAM）ロールによって保護された Amazon Simple Storage Service（S3）バケットに保存されます。S3 の冗長性機能の一部として、ファイルは AWS アベイラビリティゾーンでバックアップ用に複製されます。

Creative Cloud には、正規ユーザーがデスクトップアプリケーションと Web アプリケーションにアクセスできるサービス一式が含まれています。

総じて、それらのサービスとアプリケーションは、ユーザーのシステムから以下の 3 つのエンドポイントを経由してアクセスされます。

- Adobe Photoshop などのアプリケーション
- Creative Cloud デスクトップアプリケーション
- ブラウザー

ユーザーが Adobe Creative Cloud にどのようにアクセスするかによって、利用できるサービスは異なります。例えば、個々のアプリケーションは、Creative Cloud にアクセスしてユーザーの検証、設定の同期のほか、必要に応じて Adobe Behance でコンテンツの共有を行えます。同様に、Creative Cloud デスクトップアプリケーションは、デスクトップアプリケーションのダウンロードとアップデート、Typekit での Web 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／ダウンロードをユーザーに許可します。

ユーザーのエンドポイントとは関係なく、Creative Cloud のアクセスはすべて Adobe.com で一般提供されているサービスによって制御されます。検証されたユーザーは、自分のエンドポイントによって許可されればどんなアクションでも実行できます。利用できるツールとサービスについて詳しくは、こちらをご覧ください。

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 Creative Cloud グループ版のコンポーネント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、セキュリティベスト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設計および管理を行っています。

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。

Amazon Web Services（AWS）について

AWS ネットワーク上の顧客データの所在地

Amazon S3 のクラウドに保存される顧客データについて、アドビは個々の顧客のデータおよびサーバーを配置する物理的リージョンを指定します。アドビはアメリカ、ヨーロッパ、アジア太平洋の 3 つのリージョンで Creative Cloud を運用します。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。ユーザーが Creative Cloud に保存するコンテンツは、他のリージョンの他のデータセンターには複製されません。例えば、初期設定では、Creative Cloud はアップロードされたすべてのヨーロッパのユーザーのコンテンツをヨーロッパで保存します。

顧客データの分離／ AWS 顧客の分離

アドビが AWS で保存する Creative Cloud のデータには、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が含まれています。仮想化されたマルチテナント環境として、AWS は、Creative Cloud などの各顧客を他の AWS 顧客から分離するよう設計されたセキュリティ管理プロセスとその他のセキュリティコントロールを実装します。AWS Identity and Access Management（IAM）は、アクセスを遮断してインスタンスを処理および保存するために使用されます。

安全な伝送

アドビでは、HTTP/HTTPS で REST/ クエリリクエストを送信するか、AWS SDK の 1 つでラッパー関数を呼び出して、AWS アクセスポイントに接続します。HTTPS は、データ漏えい、改ざん、メッセージの偽造を防ぐよう設計された暗号プロトコルである Secure Sockets Layer（SSL）を使用しています。アドビは、SSL 暗号化エンドポイント経由で Amazon S3 にデータをアップロードしたり Amazon S3 からデータをダウンロードしたりします。インターネットと Amazon EC2 のどちらからでもアクセスが可能な暗号化エンドポイントを使用することで、AWS 内でも、AWS 外のソースとの間でも、データを安全に転送できます。

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行っています。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 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。

- 分散サービス妨害（DDoS）攻撃
- 介入者（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 セキュリティホワイトペーパーをご覧ください。

サービスのモニタリング
AWS は、電気、機械、生命サポートシステムおよび設備をモニタリングし、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
Creative Cloud グループ版は Amazon S3 にデータを格納します。Amazon によると、Amazon S3 は、特定の 1 年間、99.999999999% のオブジェクト堅牢性と 99.99% のオブジェクト可用性を提供します。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。

変更管理
既存の AWS インフラストラクチャに対する緊急、非定期的、その他の設定の変更は、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 Creative Cloud 用に Status Health Dashboard 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。パッチが要求されると、アドビは、実際のパッチではなく、新たに強化した OS およびアプリケーションのインスタンスを供給します。

Creative Cloud グループ版の認証（Adobe ID）

管理者からチームに加わるための招待状を受け取ると、ユーザーは Adobe ID を作成する必要があり、それを Creative Cloud グループ版にアクセスするたびに使用します。Adobe ID は、SHA 256 ハッシュアルゴリズムを、様々なパスワードやハッシュイテレーションと組み合わせて使用します。アドビは、異常なアカウントアクティビティがないか継続的に Adobe ID アカウントをモニタリングし、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ます。

アドビのリスク／脆弱性管理

侵入テスト
アドビでは、認可された第三者たるベンダーと協力して侵入テストを実行し、潜在的なセキュリティ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。ベンダーは、業界のベストプラクティスに従ってテストを実行します。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。

インシデントへの対応

新しい脆弱性や脅威は日々進化しているため、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。

Adobe 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（Product Security Incident Response Team）が Creative Cloud 組織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。

AWS データセンターに影響を及ぼすインシデントや脆弱性、脅威については、Amazon の事故管理チームが、業界標準の診断手順を用いて、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制でインシデントを検出し、影響と解決方法を管理して、アドビや AWS の他の顧客に知らせます。

Adobe 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展開
- 動作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、アドビは業界標準のツールと手法を用います。アドビは、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などのフォレンジック分析プロセスに準拠しています。さらに捜査または起訴が必要な場合、アドビは法的機関と協力することもあります。

AWS データセンター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 と Amazon のセキュリティ制御について詳しくは、Amazon セキュリティ Web サイトをご覧ください。

物理設備のセキュリティ

AWS データセンターは、最新の構造的かつ工学的アプローチを採用しています。Amazon は大規模データセンターの設計、構築、運用において長年の実績を有しており、それを AWS のプラットフォームとインフラストラクチャに活かしています。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厳密に管理しています。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を行います。

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 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、二重連結予作動式、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、大気の状態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 サイトでご覧ください。

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全社的に実装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。訪問者には常に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

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。従業員は開発や生産システムにアクセスするための特定の権限を付与されます。

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行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。

顧客データの機密保持

アドビは、顧客データを常に機密情報として扱います。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。

セーフハーバー

アドビシステムズ社（当社の米国本社）は EU セーフハーバープライバシープログラムを遵守しています。

セキュリティコンプライアンス

Amazon Web Services（AWS）と Rackspace は、それぞれ ISO27001、SOC2 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。

現在アドビは、SOC2 Trust 原則と 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。

まとめ

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。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。

詳細情報はこちら：*http://www/adobe.com/jp/security.html*

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