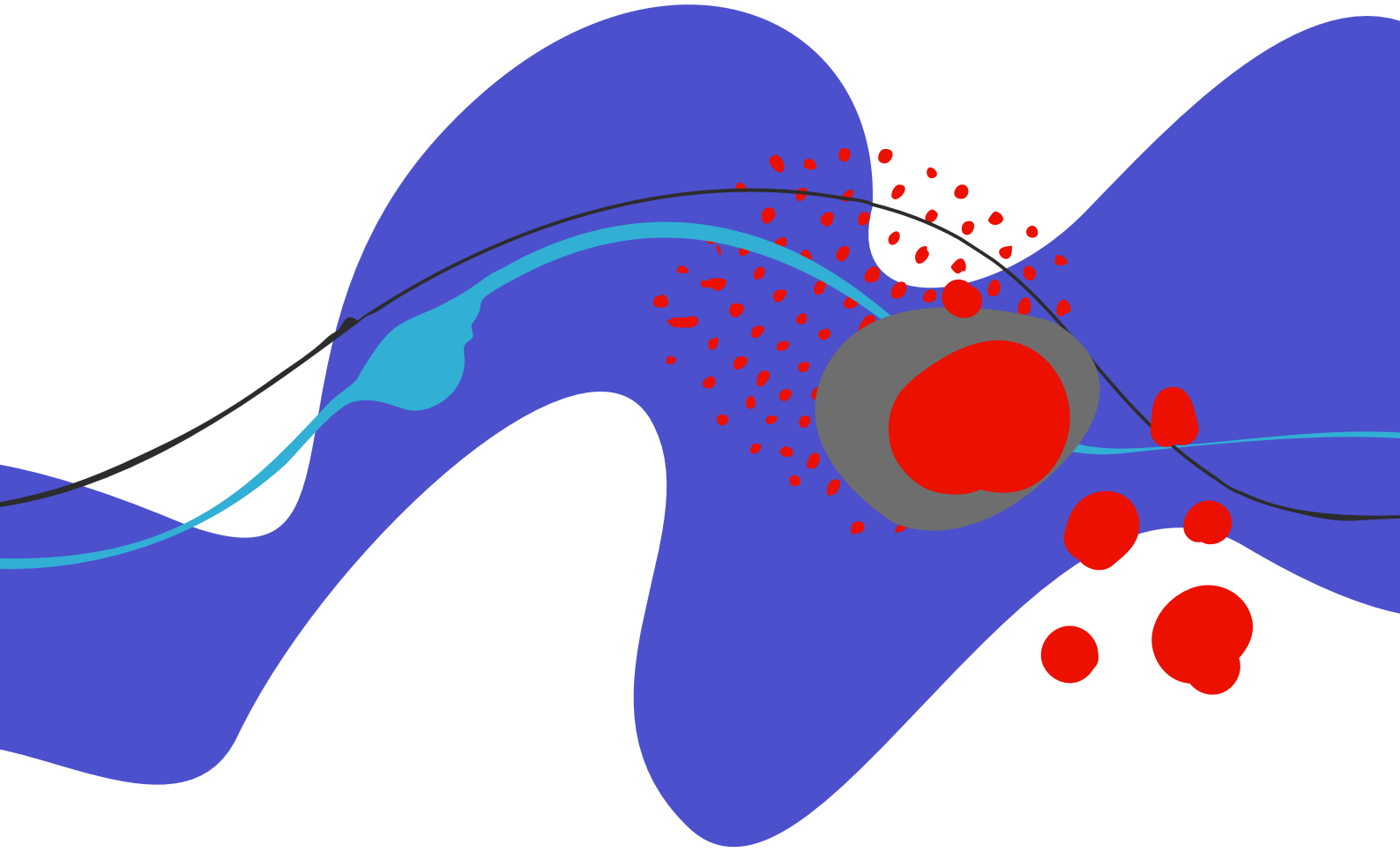
ホワイトペーパー

Adobe ID 管理サービス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におけるセキュリティは最優先の課題です。アドビでは、ソフトウェア開発・運用のプロセスおよびツールに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Adobe Secure Product Lifecyle（SPLC）コントロールを導入してインシデントの防止、検知、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や対策を継続的に組み込んでいます。

このホワイトペーパーでは、Adobe ID管理サービスの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。

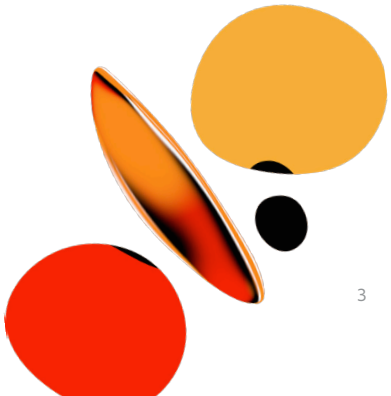
Adobe ID管理サービスについて

Adobe ID管理サービス（IMS）は、以下の3つのコンポーネントから成り、アドビのすべてのソリューションに対するエンドユーザー認証を処理します。

- **Adobe IDサービス** — エンドユーザーの認証および検証を処理します。これにはフェデレーションおよびランタイムのシングルサインオン（SSO）が含まれます。
- **Adobe Admin Console** — 組織全体のアドビ製品の使用権限を一元的に管理し、ユーザー管理、クラウドサービスおよびデスクトップライセンスの使用権限、フェデレーション設定、データ損失防止対策を処理します。
- **Adobe User Management API（UMAPI）** — 導入先組織がAdobe Admin Consoleでのユーザーと使用権限の管理をAPIレベルでおこなえるようにします。

ユーザー指定ライセンス

Adobe IMSプラットフォームは、「ユーザー指定ライセンス」と呼ばれる使用権限と一意の識別子を管理します。これにより、エンドユーザーはデプロイされているアドビのデスクトップアプリケーションとクラウドサービスに対する認証をおこなうことができます。



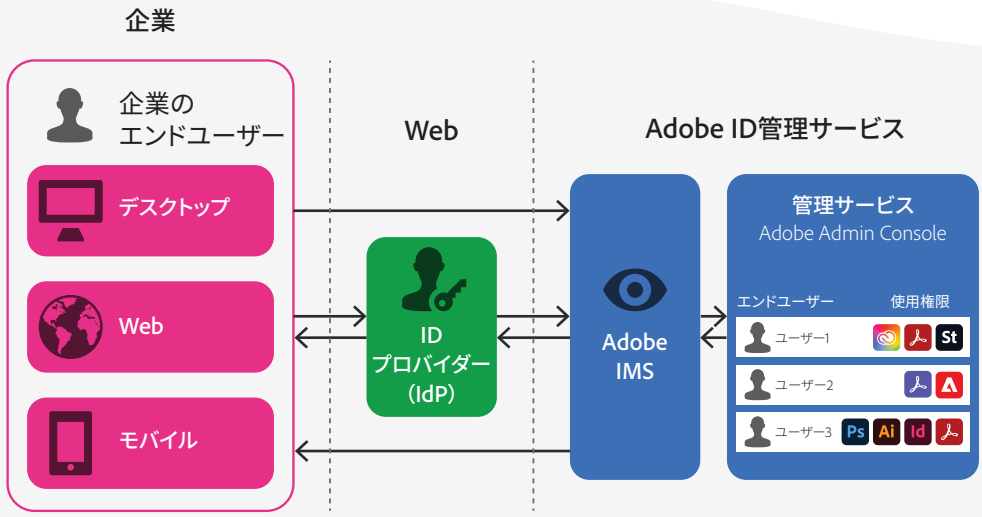


図1：Adobe ID管理サービスのアーキテクチャ

上の図1は、ユーザー指定ライセンスを使用したエンドユーザーとAdobe IMSとのインタラクションを表しています。この例では、エンドユーザーはデスクトップまたはモバイルデバイスにアドビアプリケーションをインストール済みです。エンドユーザーがアドビのデスクトップアプリケーションやモバイルアプリをアクティベートまたは起動するか、アドビのクラウドサービスにアクセスすると、エンドポイントがAdobe IMSと通信します。

指定されたユーザーIDタイプ（次のセクションを参照）に応じて、Adobe IMSはエンドユーザーが直接ログインすること、またはIDプロバイダー（IdP）に制御を渡すことを許可し、それによってフェデレーションSSO認証がおこなわれます。認証が成功すると、Adobe IMSがエンドユーザーの使用権限を検証して要求されたアクションを実行し、エンドユーザーは使用権限を付与されたソフトウェアやサービスを使用できるようになります。

ユーザーIDタイプ

エンタープライズデプロイメントでは、アドビは3種類のユーザーIDタイプをサポートしています。

Business ID — ユーザーのIDとして、またはID目的でドメインを申請していない場合に独自ドメイン以外の電子メールアドレスを使用する組織が管理し、アドビがホストするID。組織のIDや電子メールを持たない外部の請負業者またはフリーランサーに業務を委託する組織にお勧めです。

Enterprise ID — 導入先組織のIT管理者が作成、管理し、アドビがホストするID。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。ユーザーアカウントの管理は、Adobe Admin ConsoleやUMAPIでおこなわれます。管理者は、ユーザーの認証ポリシーを設定できますが、ユーザーの認証および資格情報はアドビが全面的に管理します。

Federated ID — 導入先組織が管理するアカウント。すべてのIDプロファイルは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、システム管理部門によって作成、所有、管理されます。任意のSAML 2.0準拠IDプロバイダーとの統合に対応します。ユーザーアカウントは、IDプロバイダーによって認証され、Adobe Admin Consoleで権限付与されます。導入先組織のIDプロバイダーが認証ポリシーの設定と施行を全面的に管理します。またアドビは、フェデレーションIDサービスのOpenID Connectを介して、Microsoft Azure Active Directoryサービスや Google Workspace Directoryサービスとの接続および同期をサポートします。

電子メールを独自ドメインで運用している場合、ほとんどの組織は従業員、請負業者、フリーランサー用にEnterprise IDまたはFederated IDを使用します。エンドユーザーの電子メールが企業ドメインで運用されていない場合は、Business IDの使用をお勧めします。詳しくは、Adobe HelpXのIDの概要ページを参照してください。

個人での使用の方が適している場合、エンタープライズデプロイメント用のIDタイプの使用はお勧めしません。

ユーザーID管理

ユーザーIDは手動または自動で管理できます。

手動でのID管理

管理者がユーザーを手動で管理する場合、Adobe Admin Consoleでユーザーを1人ずつ個別に追加、削除、変更するか、ユーザーデータのCSV表計算シートをアップロードして一括管理します。

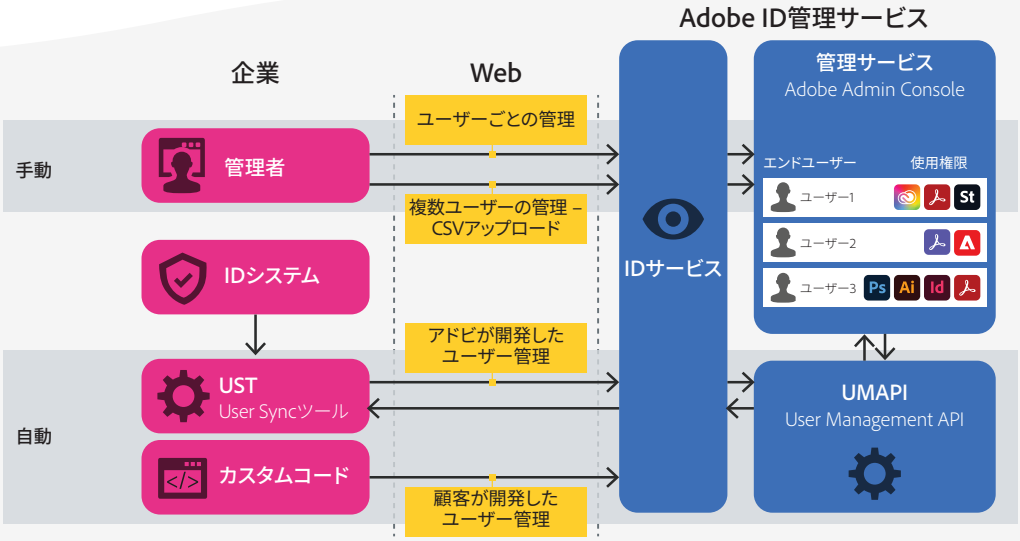


図2：ユーザーID管理のオプション

自動ID管理

管理者は以下の3通りのいずれかの方法でユーザーを自動管理できます。

- **UMAPI**を使用したカスタム開発コードにより、プログラム的にユーザーを追加、更新、削除する。
- クラウドベースの同期のためのオープンスタンダードである**SCIM（System for Cross-domain Identity Management）**を使用して、すべてのユーザーをMicrosoft Azure Active Directoryサービスや Google Workspace Directoryサービスと同期する。
- アドビが開発・保守するPythonスクリプトである**Adobe User Syncツール（UST）**を使用して、エンタープライズディレクトリの特定のユーザーを同期し、Adobe Admin Consoleの適切なライセンスプールにユーザーを追加したり、そこからユーザーを削除したりする。

User Syncツール

USTは、エンタープライズディレクトリサービス（OpenID Connectにサポートされた Microsoft Active Directoryやその他のディレクトリ）のすべてのLightweight Directory Access Protocol（LDAP）グループからIDデータを読み取ります。

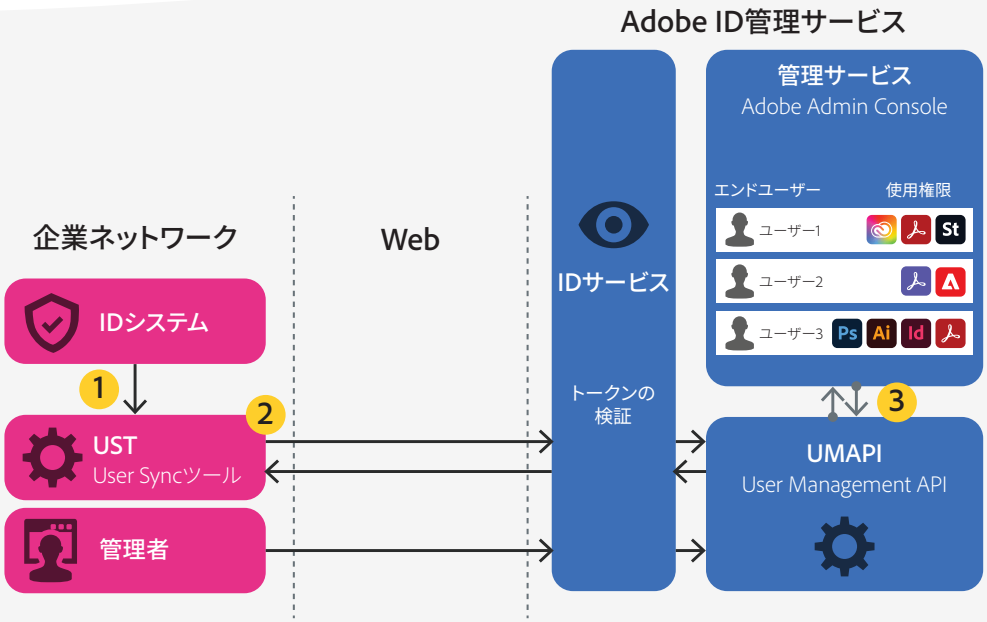


図3：User Syncツール（UST）

USTは、実行するたびに次の処理をおこないます。

1. エンタープライズディレクトリ内のグループから従業員レコードを要求する。グループおよびLDAPクエリは、エンタープライズの固有の環境に合わせてカスタマイズできます。
2. Adobe Admin Consoleから現在のユーザーおよび関連付けられている製品構成を要求する。また、署名、エンコードされたJWT（JSON Web Token）から生成された検証済みの期限付きアクセストークンを利用して、HTTPS経由のREST呼び出しによってUMAPIに接続する。
3. 構成ファイルで定義されたルールにもとづいて作成、削除、または更新が必要なユーザーを決定する。
4. UMAPIを使用してAdobe Admin Consoleに必要な変更をおこない、適切なソフトウェアやサービスの使用権限をユーザーに付与する。

USTは、エンタープライズユーザーのアドビ製品の使用権限とディレクトリサービスのグループとの同期を自動的に保ちます。例えば、あるユーザーがLDAPディレクトリに追加された場合、USTの次回実行時に、UMAPIがディレクトリからユーザーの情報を取得して、その情報をAdobe Admin Console内の適切なグループに追加します。ユーザーが変更またはLDAPディレクトリから削除されると、USTはUMAPIを呼び出して、Adobe Admin Consoleで適切なアクションを実行します。

USTのインストール、登録、実行の詳細な手順については、Adobe HelpXのUser Syncツールの設定ページを参照してください。

ユーザー管理について詳しくは、Adobe HelpXのAdobe Admin Consoleユーザーページを参照してください。

ユーザーの認証および承認のデータフロー

アドビはユーザーの認証および承認を以下の2通りの方法で実行します。

インタラクティブな認証および承認 — ユーザーがアドビのデスクトップアプリケーションまたはクラウドサービスに明示的にサインインして、ユーザーインターフェイス内のダイアログボックスに情報を入力すると実行されます。この場合、承認はシームレスに実行されるため、エンドユーザーには認証プロセスの一部のように見えます。

アドビは多要素認証（MFA）もサポートしています。MFAでは、まずUIで2要素認証をおこない、その後に本人しか知らない追加情報の入力をエンドユーザーに求めてセキュリティを強化します。アドビは、Adobe IDおよびBusiness IDのユーザーにMFAを実行するためのポリシーを提供しています。MFAが導入されている場合でも、承認はシームレスに実行されるため、エンドユーザーには認証プロセスの一部のように見えます。

自動的な認証および承認 — インタラクティブな認証によってエンドユーザーが最初に認証された後に実行されます。自動的な認証では、一意のIDトークンを利用するため、エンドユーザーはセッション期間中に再度ログインする必要がなく、承認もシームレスにおこなわれます。エンドユーザーがアプリケーションやサービスを利用しているとき、明示的なログインを求められない限り、自動的な認証は有効です。ユーザーがセッションをログアウトすると、次回ログイン時にアクセス権を検証するために承認が再確認されます。

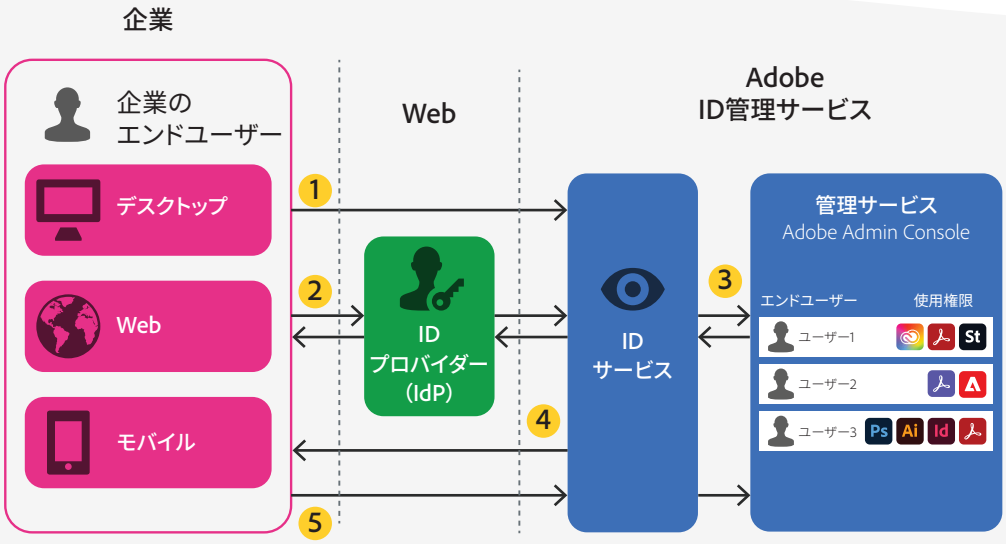


図4：アドビのユーザー認証データフロー

ユーザー認証データフローはユーザーIDタイプによって異なりますが、認証プロセスには通常、以下の手順が含まれます。手順の番号は、上の図の番号と対応しています。

1. エンドユーザーがデスクトップアプリケーションを起動するか、初めてアドビのクラウドサービスへのアクセス権をリクエストします。Business IDまたはEnterprise IDを使用している場合は、Adobe IMSを使用してログインします。

2. 組織でFederated IDが使用されている場合、エンドユーザーがユーザー名フィールドに電子メールアドレスまたはドメインのみ（例：@companydomain）を入力すると、Adobe IMSがSAMLリクエストを開始します。エンドユーザーはIDプロバイダーにリダイレクトされ、会社の資格情報を使ってログインします。

3. ユーザーが正常に認証されると、Adobe IMSが必要な使用権限とポリシーの実行チェックをおこない、ユーザーを適切なアドビのクラウドサービスにリダイレクトするか、適切なデスクトップアプリケーションのライセンスを有効にします。

4. Adobe IMSがエンドユーザーのコンピューター上にデバイストークンを保存し、それを使用してアクセストークン（アプリケーションのセッショントークンに類似）を生成します。また、これら2つのトークンを使用してアプリケーションの署名付きライセンスが生成され、暗号化された上でデバイストークンとともにエンドユーザーの設定に保存されます。トークンはオペレーティングシステムに依存しないため、ユーザーがシステムを再起動しても、アドビのデスクトップアプリケーションやクラウドサービスに対する再認証は必要ありません。

5. これでエンドユーザーは、アプリケーションごとに手動で再認証することなく（つまり自動認証）、アドビのデスクトップアプリケーションやクラウドサービスを同時に使用できます。ユーザーが同じセッションで新しいデスクトップアプリケーションを起動すると、Adobe IMSに伝えられ、デバイスIDおよびデバイストークンがアクセストークンと交換されます。この過程で、ポリシーのチェックと使用権限の確認がおこなわれます。何らかの理由で、ユーザーのアクセス権や使用権限が変更または取り消された場合、アクセストークンとデバイストークンは無効になります。

アドビは、より頻繁に認証を要求してアクセストークンの有効期限をさらに短くするオプションの管理ポリシーを用意しており、一部のAdobe Experience Cloudアプリで有用な場合があります。しかし、特定のセキュリティ要件がない限り、こうしたポリシーの使用はお勧めしません。

IDデータ

収集するデータの種類とその理由

アドビは、各エンドユーザーが一意のIDを持っていることを保証するIDデータを収集して、ライセンス使用権限があることを検証し、それらの使用権限およびユーザーによって生成・保存された内容をパスワード保護できるようにします。アドビは以下のIDデータを収集します。

- **ユーザー名とドメイン** — ユーザーの識別子。通常は、user@domainという形式のプライマリメールアドレスです。Business IDおよびEnterprise IDの場合、アドビのアプリケーションやクラウドサービスにログインするには完全なユーザー名が必要です。ただし、ユーザー名と電子メールアドレスが異なる（例：firstnamelastnameとuser@domain）従業員については、企業が管理します。Federated IDの場合、IDプロバイダーに制御を渡すには、完全な電子メールアドレスまたは@domain部分のみが必要です。

- **UID（Federated IDのみ）** — ユーザーに関連付けられている一意の識別子（通常は電子メールアドレス）。アドビは、UIDをIDプロバイダーからの鍵として使用して、Adobe IMSでエンドユーザーを検索します。

- **パスワード（Business IDおよびEnterprise IDのみ）** — パスワードは格納前に業界のベストプラクティスに従ってハッシュ化されます。アドビがプレーンテキストパスワードへの復号化が可能な形式でユーザーのパスワードのコピーを保管することはありません。

- **生年月日（Adobe IDのみ）** — 児童オンラインプライバシー保護法（COPPA）、一般データ保護規則（GDPR）およびwebサイトへのアクセス時の年齢確認に対応するために必要です。

- **国コード** — IDプロファイル作成時にユーザーのISO Alpha-2およびISO Alpha-3国コードが収集されます。通常アドビは、国コードを使用してユーザー生成コンテンツのアセット保存場所を決定します。Enterprise IDおよびFederated IDの場合、場所は組織が決定します。

- **名と姓** — IDプロファイル作成時に収集されます。Enterprise IDおよびFederated IDの場合、UID、国コード、名、姓のフィールドは、IT管理者がユーザーアカウント作成時に設定できます。これらのフィールドに入力されるユーザー情報の量も管理者が決定できます。

IDデータの保管場所

お客様の所在地にかかわらず、すべてのIDデータは、北米（オレゴン州およびバージニア州）、ヨーロッパ（アイルランド）、APAC（シンガポール）の各リージョンデータセンターを持つ負荷分散されたクラウドインフラストラクチャプロバイダーに保管されます。信頼性を高めるために、IDデータはすべてのデータセンター間で複製されます。

IDデータのセキュリティ対策

IDデータは、保管中はAdobe Common Compliance Framework（CCF）に従いAES 256ビット暗号化によって保護され、機密情報の暗号化と保管に関するアドビ社内のポリシーを満たしています。

IDデータの保管期間

コンテンツは複製され、負荷分散と冗長化のため、各データセンター、リージョン内の他のデータセンター、クロスリージョンデータセンターでバックアップされます。IDデータはデータセンターに毎日バックアップされ、7日間保管されます。アドビは国境を越えたデータ移転に関する法令にも準拠しています。

Adobe IDアカウントは、個々のユーザーによって作成、所有、管理されます。したがって、4年以上使用されていないAdobe IDおよびBusiness IDは保存されず削除されると規定する消費者個人情報保存基準（CPIR）の保存ポリシーとは別に、個々のユーザーがアカウントのライフサイクルを管理します。アドビは、個々のユーザーの要求に応じて、または連続48か月間使用されなかった場合に、Adobe IDアカウントを非アクティブ化し、個人情報、ハッシュ化されたパスワードおよび関連する支払いデータを削除します。

Enterprise IDとFederated IDのどちらのIDタイプでも、アカウント削除のスケジュールは組織が決め、Adobe Admin Consoleで管理できます。組織のアカウントに関連付けられた特定のEnterprise IDまたはFederated IDが必要なくなったら、権限のある管理者がAdobe Admin Consoleで削除できます。詳しくは、Adobe HelpXのAdobe Admin Consoleユーザーページを参照してください。

ログの処理方法

アドビは以下のようなユーザーのアクションを記録します。

- アドビのアプリケーションまたはサービスをアクティベートする
- アドビのアプリケーションまたはサービスにサインインする
- デスクトップまたはモバイルデバイスでアドビのアプリケーションを開く
- クラウドストレージまたはクラウドサービスを使用する

収集されるログデータには、ユーザーID、電子メールアドレス、ユーザーのIPアドレスおよびイベントトラッキングデータが含まれることがあります。またアプリケーションおよびサービスの使用に関する分析データをアドビが記録する場合があります。ユーザーはいつでも分析データの収集をオプトアウトできます。

IDデータへのアクセス権

アドビのISO 27001認定に従い、権限のあるアドビの担当者のみが、必要な場合に限り最小権限の原則にもとづいてIDデータにアクセスできます。Adobe IMSによって記録されたデータは、（Adobe Data Classification and Handling Standardで）「最も特権的」とみなされ、アクセスできるアドビの担当者がさらに制限されます。

アドビセキュリティプログラムの概要

アドビセキュリティプログラムは、一体となって機能する5つのCenter of Excellence（CoE）で構成されています。各CoEは、新しいテクノロジーや発展が期待されるテクノロジー（例：自動化、AI、機械学習など）をアドビのリスク検知・予防策に応用するために、それぞれのテーマに従って反復研究と進歩を追求しています。

図5：5つのセキュリティ Center of Excellence（CoE）

アドビセキュリティプログラムを構成する5つのCoEが担当するテーマは以下のとおりです。

- **アプリケーションセキュリティ** — 製品コードのセキュリティに重点的に取り組み、脅威調査やバグ調査報奨制度を実施
- **運用セキュリティ** — アドビのシステム、ネットワーク、実稼働クラウドシステムについて、モニタリングとセキュリティ確保を支援
- **エンタープライズセキュリティ** — アドビの企業環境に関するアクセスセキュリティと認証システムに注力
- **コンプライアンス** — アドビのセキュリティガバナンスモデル、監査／コンプライアンスプログラム、リスク分析体制を統監
- **インシデント対応** — 常時稼働のセキュリティオペレーションセンターと脅威対応チームを運営

アドビの組織においては、最高セキュリティ責任者（CSO）がセキュリティに関する現行の取り組み全体を統括し、セキュリティの将来を見据えたビジョンを示す役割を担います。5つのセキュリティCoEはCSOの直属に位置付けられています。この体制は、製品・サービスのセキュリティをきわめて重視するアドビの姿勢を象徴するものといえます。

アドビのセキュリティ組織

アドビのセキュリティ組織は、透明性の確保、結果責任の明確化、意思決定材料の充実を目的とする共通基盤の上に立ち、総合的なセキュリティサービス群全体を単一のガバナンスモデルで運営する体制をとっています。トップマネジメントを担うCSOは、最高情報責任者（CIO）および最高プライバシー責任者（CPO）と密接に協力し、オペレーションと方針を合わせながらセキュリティ戦略を遂行します。

アドビのセキュリティ組織は、上記のCoEに加えて法律、プライバシー、マーケティング、PRの専門家チームを擁し、セキュリティ関連のあらゆる意思決定に関して透明性の確保と結果責任の明確化を追求する仕組みを内包しています。

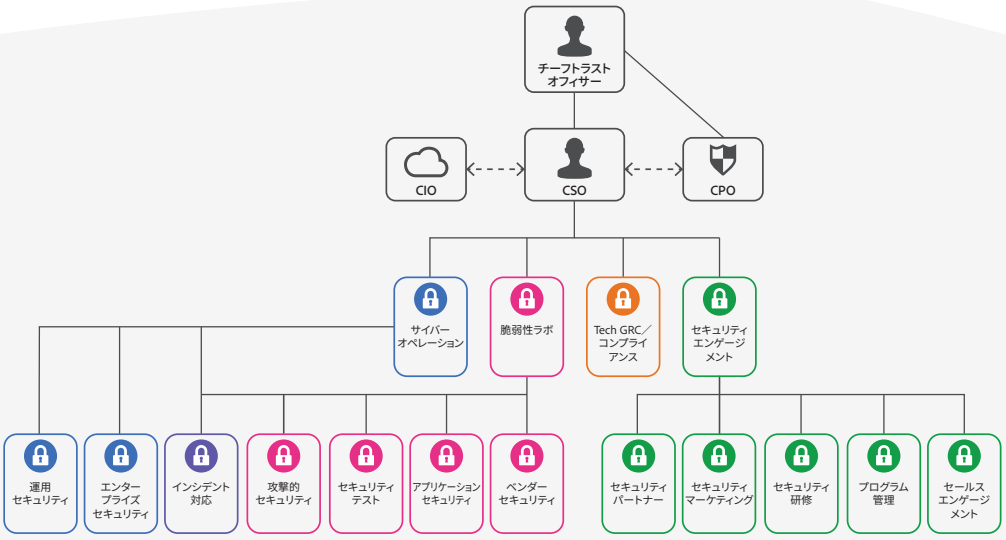


図6：アドビのセキュリティ組織

アドビでは、全社のセキュリティ文化を保つ活動の一環として、すべての従業員に年1回のセキュリティ意識向上およびセキュリティ教育研修の受講・再認定を義務付けています。この規則は、全従業員をあげてアドビの企業資産、お客様データ、従業員データを守る環境づくりに役立っています。技術系従業員は（エンジニアリング、技術運用の両方とも）、人事採用の際、それぞれの職務に最適化された緻密な「格闘技を模した段級位制」の研修プログラムに自動登録されます。

アドビのセキュリティ文化と研修プログラムについては、アドビのセキュリティ文化に関するホワイトペーパー（英語）をご覧ください。

Adobe Secure Product Lifecycle（SPLC）

設計、開発、品質保証、テスト、展開まで、アドビの製品ライフサイクルを構成する様々な段階には、あらゆるセキュリティの基礎となるAdobe Secure Product Lifecycle（SPLC）が組み込まれています。Adobe SPLCは、ソフトウェア開発のプラクティス、プロセス、ツールを幅広く網羅し、数百項目のセキュリティ活動を具体的かつ厳密に示して、明確で反復可能なプロセスを定義したものです。その内容は、開発チームが製品・サービスにセキュリティを組み込む際の指針となり、絶えず最新の業界ベストプラクティスを絶えず取り入れて進歩し続ける活動に役立っています。

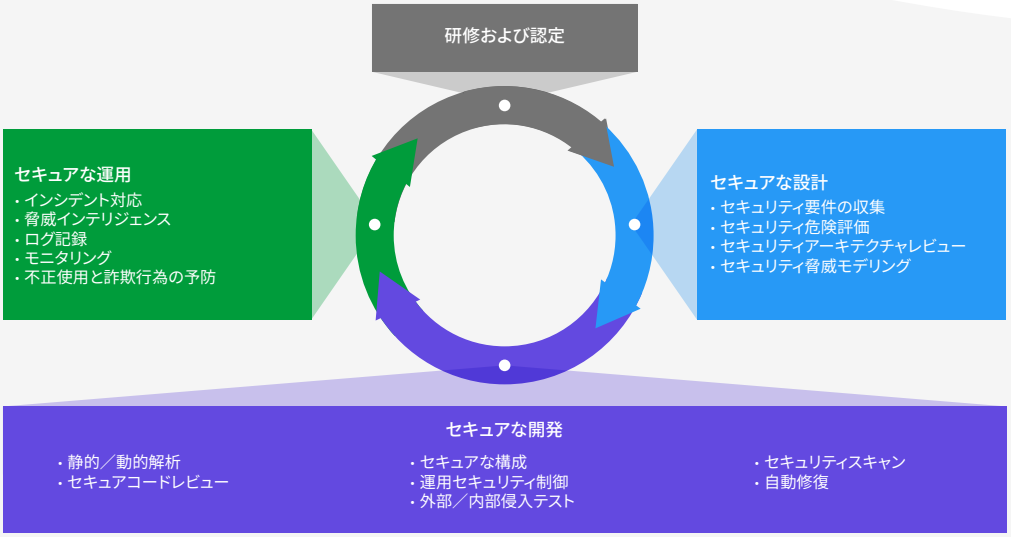


図7：Adobe Secure Product Lifecycle（SPLC）

アドビではSPLC標準のドキュメントを発行・維持しており、ご要望に応じて提供可能です。Adobe SPLCを構成する要素について詳しくは、アドビアプリケーションセキュリティの概要（英語）をご覧ください。

アドビアプリケーションセキュリティ

セキュア・バイ・デフォルト（あらかじめ確保されたセキュリティ）を前提とするアプリケーション開発の出発点は、アドビアプリケーションセキュリティスタックです。このスタックは、実績ある研究成果と経験から導かれた明確で反復可能なプロセスに、一貫したセキュリティ制御を確実に適用する自動化の仕組みを組み合わせて構築されています。これには、開発効率を高め、セキュリティミスの発生リスクを最小限に抑える効果があります。既にテストと承認が済んでいる安全なコードブロック群が含まれているため、開発者は、共通的なパターンやブロックをゼロからコーディングする必要がありません。コードのセキュリティを必要以上に心配することなく開発に取り組み、各自が本来の専門分野に意識を集中できます。アドビアプリケーションセキュリティスタックは、テスト体制、目的に特化したツール整備、モニタリング体制と相まって、セキュア・バイ・デフォルトなコードの作成に役立っています。

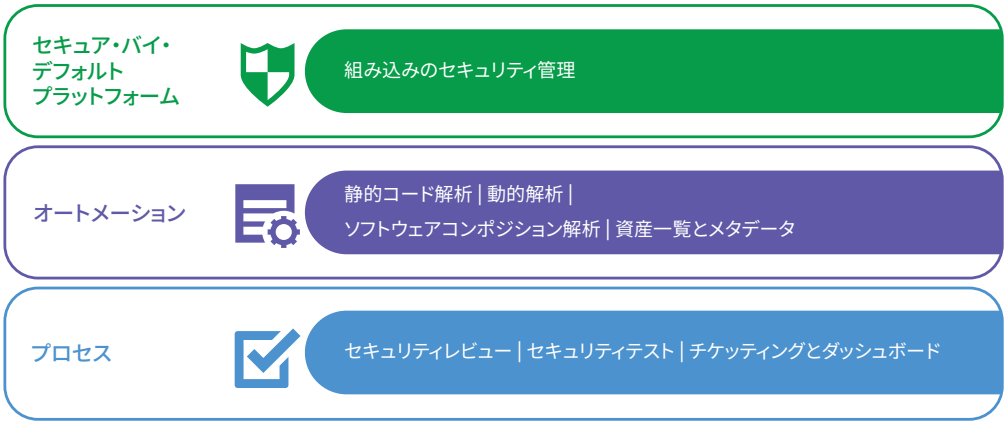


図8：アドビアプリケーションセキュリティスタック

また、アドビではアプリケーションセキュリティに関する標準ドキュメントをいくつか発行・維持しています。Amazon Web Services（AWS）とMicrosoft Azureパブリッククラウドインフラストラクチャに関する当社独自の利用方法に特化した内容も含まれます。それらのドキュメントはご要望に応じて提供可能です。アドビアプリケーションセキュリティの概要（英語）には、アドビのアプリケーションセキュリティ対策とプロセスに関する詳細な情報が記載されています。

アドビの運用セキュリティ

すべてのアドビ製品・サービスについて、最初からセキュリティのベストプラクティスを念頭に置いた設計作業がおこなわれる環境を整備するために、運用セキュリティチームはアドビ運用セキュリティスタック（OSS）を作成しました。OSSは、製品開発者とエンジニアによるセキュリティ対策の改善に役立ち、アドビの立場とお客様の立場におけるリスク軽減にも役立つツール群を集約したものです。これは、アドビがコンプライアンス、プライバシー、その他のガバナンスフレームワークを全社レベルで遵守する体制を強化するうえでも役立ちます。

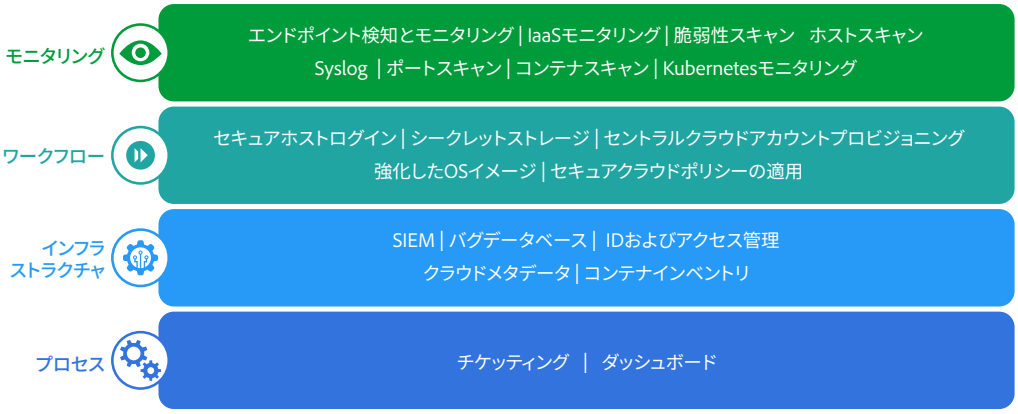


図9：アドビ運用セキュリティスタック（OSS）

アドビでは、継続的なクラウド運用に関する標準ドキュメントをいくつか発行・維持しています。それらのドキュメントはご要望に応じて提供可能です。アドビOSSと、アドビが全社的に利用している具体的なツールについて詳しくは、アドビ運用セキュリティの概要（英語）をご覧ください。

アドビのエンタープライズセキュリティ

アドビでは、製品・サービスとクラウドホスティング運用環境を保護するだけでなく、様々な社内向けセキュリティ対策を導入し、社内のネットワークとシステム、物理的な会社施設、従業員、お客様データのセキュリティを確保しています。

アドビが採用しているエンタープライズセキュリティ管理策の詳細情報と、それらの管理策に関してアドビが策定した標準ドキュメントについては、アドビエンタープライズセキュリティの概要（英語）をご覧ください。

アドビのコンプライアンス

すべてのアドビ製品はAdobe Common Controls Framework（CCF）を満たしています。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。アドビでは、最先端の自動化プロセスをできるだけ多く活用して、コンプライアンス違反の可能性がある状況を検知し、チームに警告を伝え、状況改善や業務環境見直しの迅速化に役立てています。

アドビ製品・サービスは、適用される法的基準を満たしているか、または、お客様によるサービスプロバイダー利用に関連した法的義務を満たすために役立つ方法で使用できます。お客様は自社の文書、データ、ワークフローについての制御権を保持することができ、また、当該自治体や地域の規則（EUの一般データ保護規則（GDPR）など）に従うための最善の方法を選択できます。

また、アドビではコンプライアンスの研修および関連する標準ドキュメントも作成・維持しており、ご要望に応じて提供可能です。アドビCCFおよび主要な認定資格について詳しくは、アドビのコンプライアンス認定、標準規格、規則リストをご覧ください。

インシデント対応

アドビは、リスクと脆弱性の管理、インシデント対応、問題の緩和、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。脅威の動向を常に注視し、世界中のセキュリティ専門家と知識を共有しています。問題発生時にはすみやかに解決し、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・サービスについて最高レベルのセキュリティを確保するよう努めています。

また、インシデント対応と脆弱性管理に関する内部標準ドキュメントも作成・維持しており、ご要望に応じて提供可能です。

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プログラムの概要（英語）をご確認ください。

事業継続性と障害復旧

アドビ事業継続性と障害復旧（BCDR）プログラムは、アドビ事業継続性プラン（BCP）と各種製品に特有の障害復旧（DR）プランで構成されています。いずれの内容も、アドビ製品・サービスの可用性、入手性、提供体制を維持するためのものです。BCDR プログラムは ISO 22301 認証取得済みであり、アドビはこれに従って、予期しない事業中断への対処、問題の緩和、影響からの回復能力を強化しています。Adobe BCDR プログラムについて詳しくは、アドビの事業継続性と障害復旧プログラムの概要（英語）をご覧ください。

まとめ

アドビのソリューション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。

アドビセキュリティについて詳しくは、Adobe Trust Centerをご覧ください。

© 2022 Adobe. All rights reserved.

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.

12/22