Adobe Experience Platformのセキュリティ

目次

アドビでは、デジタル体験におけるセキュリティを、極めて重要と認識しています。セキュリティの取り組みは、社内のソフトウェア開発やオペレーションプロセス、ツールに深く根差しています。また、部門を超えたチームによって厳密にチェックされ、適切な手法を用いてインシデントの防止、検出、対応をおこなっています。さらに、パートナーや一流の研究者、セキュリティ研究機関、業界組織などと協力して、最新の脅威や脆弱性に対応できる態勢を常に整えています。アドビでは、高度なセキュリティ技術を、継続的に製品やサービスに組み込んでいます。

この資料では、Adobe Experience Platformと企業のデータのセキュリティを強化するために、アドビが実装している多層防御アプローチとセキュリティ手順について説明します。

ADOBE EXPERIENCE PLATFORMの概要

現代の人々は、スマートフォン、タブレット、デジタルTV、車載情報端末など、数えきれないほどのデバイスを使い分けながら、企業とやり取りしています。コンテンツやデータに対する人々の期待はかつてないほど高まり、リアルタイムでパーソナライズされた適切な体験が提供されることを期待しています。そうした体験の創出は有意義ですが、同時に企業は、的確な相手に最適なコンテンツをタイミングよく、より迅速に提供しなければならないという、大きな課題に直面しています。膨大な量のデータ、数えきれないほどのデバイスやスクリーン、高まり続ける顧客の期待により、企業は、顧客とどのようにやり取りするのかを改めて検討する必要に迫られています。

その際に大きな課題となるのが、行動データやCRMデータ、製品の使用状況、コマースデータなど、顧客に関するあらゆるデータを集約した「顧客プロファイル」を構築する必要があることです。そこで、Adobe Experience Platformが役立ちます。過去のやり取りから導き出されたインサイトでデータを補強し、リアルタイムで活用できるため、適切でパーソナライズされた顧客体験をチャネルをまたいで提供できます。

Adobe Experience Platformは、あらゆる顧客データの一元化と標準化を実現するデータ基盤で、Adobe Experience Cloudの共通基盤でもあります。この製品により、リアルタイムの顧客プロファイルを構築して活用し、よりパーソナライズされた顧客体験を瞬時に提供できます。あらゆる属性データと、webやモバイル、IoT、SoR（PoSやCRMなどの記録システム）の行動データを一元化することで、膨大な量のエクスペリエンスデータをリアルタイムで処理し、顧客に関する理解を深め、適切な体験を提供できるようになります。

Adobe Experience Platformは、オープンかつ拡張可能な基盤です。APIを通じて、エンタープライズデータレイクを含めたテクノロジースタック全体と連携して活用できます。これらのAPIを使用し、企業やパートナー、開発者は、アドビ製品の機能を拡張したり組み込んだりすることで、まったく新しい顧客体験アプリケーションを構築できます。

Adobe Experience Platformはオープンソースの標準規格と、最新のフレームワークおよびテクノロジーを活用しています。これにはJava Content Repository（JCR）APIと、Adobe I/Oの堅牢で構造化されたREST（Representational State Transfer）アーキテクチャが含まれます。

Adobe Experience Platformを使用すれば、企業は次のことが可能になります。

- 実用的かつインテリジェントなリアルタイムの顧客プロファイルの構築
- データクエリやAI（人工知能）モデル、マシンラーニング（機械学習）モデルを使用した、データの強化とインサイトの拡充
- マルチチャネルに対応した、リアルタイムの顧客体験の配信とパーソナライゼーションの強化
- ガバナンス、セキュリティ、プライバシー制御に関する顧客からの信頼獲得
- オープンかつ組み立て可能なコンポーネントを利用した顧客体験の改善

機能の概要

Adobe Experience Platformは、パーソナライズされたデジタル体験をリアルタイムで構築するために、データを整備し、様々なシステムに配信するサービスを提供します。これらのサービスは、分散型データストアとファイルシステムを組み合わせて活用します。オープンソースで最新のフレームワークとテクノロジー、データをやり取りするための拡張可能なREST APIのセット（データセットAPIやインジェストAPI、インフラストラクチャAPI、計算APIなど）、堅牢なデータアクセスSDKを備えています。

Adobe Experience Platformは、次のような概念をもとに構築されています。

データ

データに関する機能は、Adobe Experience Platformの中核を成します。データは、Adobe Analytics CloudやAdobe Experience Cloud、Adobe Advertising Cloudを通じて収集し、基盤に取り込まれます。Adobe Experience Platform Launchは、アドビやパートナーのツールを容易に統合し、データを収集することのできる、次世代型のタグ管理システムおよびクライアントサイドプラットフォームです。また、Adobe Experience Platformでは、組み込みコネクタのセットやストリーミングAPI、バッチAPI、データ統合ツールの豊富なエコシステム（Informatica、SnapLogic、Unifiなど）を利用できます。これらを活用して、CRMやコマース、ロイヤルティ、顧客の声、オフラインでの購入など、企業の様々な情報源をまたいでデータを収集し、顧客の全体像を把握できます。

他のアドビソリューションのデータを利用する、またはデータを基盤に取り込むことを選択した場合は、Microsoft Azureのデータレイクが利用されます。Microsoft Azureではデフォルトで、保存中のデータが暗号化されます。データレイクは、顧客体験データの様々なタイプのデータストアの組み合わせを提供します。データレイクに保存されているデータを使用して、ビジネスのスピードに合わせてデータのクエリ、設定、管理をおこなうことができます。

データガバナンス

Adobe Experience Platformは、Experience Data Model（XDM）と呼ばれる共通のスキーマセットにもとづいています。XDMは、オープンで標準化された、拡張性を備えたスキーマで、あらゆるエクスペリエンスデータを表すことが可能なため、クロスチャネルデータのセマンティックを即座に理解できます。また、インサイトやサービスの既存エコシステムを発展させることもできます。XDMは、Adobe Experience Platformでのデータの相互運用を実現する、JSONスキーマで公開された正式な標準です。スキーマレジストリおよびスキーマ設計ツールを利用すれば、ニーズに合わせてXDMを管理したり、拡張したりできます。

また、Adobe Experience Platformは、データの使用方法を制御および管理するのに役立ちます。今日の世界において、データは政府の規制、契約上の制限、およびデータの使用を制限する社内ポリシーの影響を受けます。これらの規制に違反した場合、罰則や悪影響が発生することがあります。ビジネスにおけるデータの価値は、利用できるデータの種類とデータの出所を把握できるかどうかによって決まります。データのカタログを作成して分類し、データ使用に関する様々な規制や契約、ポリシー上の制限を管理することが重要です。Adobe Experience Platformは、これらの考慮事項を念頭に置いて構築されており、一般データ保護規則（GDPR）などの法的規制や制約要件、データ使用ポリシーなどに準拠できる、堅牢で強力なデータガバナンスフレームワークを備えています。Adobe Experience Platformを利用すれば、データのカタログを作成して分類し、様々なカテゴリによるデータの使用方法に関するポリシーを定義できます。

クエリ、マシンラーニング、AIの統合

Adobe Experience Platform Data Science Workspaceは、AIやマシンラーニングのフレームワークであるAdobe Senseiを利用し、データセットからの予測によって顧客プロファイルを補完するのに役立ちます。

共通のマシンラーニングフレームワークとランタイムをもとに構築されたData Science Workspaceは、高度なワークフロー管理、モデル管理、および拡張性を備えています。さまざまなスキルレベルのデータサイエンティストが、柔軟に独自のカスタムモデルを作成し、独自のモデルを構築できます。また、あらかじめ構成済のアドビのモデルを使用して、アドビ製品データやその他のデータを用いて、シームレスにトレーニングやデプロイメントをおこなうこともできます。

Adobe Experience Platformが無かったなら、通常、データレイクにデータを取り込み、データを標準化して、モデリングを実行し、結果をエンゲージメントシステムに取り込んで顧客体験に反映させるには、数日から数週間かかります。しかしAdobe Experience Platformを使用すれば、顧客データは既に取り込まれて標準化されているため、データサイエンティストは、追加でデータの準備をおこなうことなくモデルを抽出し、価値創出までの時間を短縮することができます。

さらに、Adobe Experience Platform Query Serviceを利用すれば、データアナリストは、データレイクのXDM上にある、使いやすいSQLクエリツールを使用できます。これにより、フィルター処理されたデータセットや集計されたデータセット、結合されたデータセットに対して、オムニチャネルやマルチプラットフォーム、サーバーレスの環境で、ペタバイト規模のクエリをアドホックに実行できます。そのため、アドビ製品からデータを取り込む必要がなくなり、短時間でより深いインサイトを得られるようになります。TableauやPower BIなど、好みのビジネスインテリジェンス（BI）ツールをネイティブで使用できるので、クエリを視覚化し、データの詳細な検査や評価を追加して、顧客プロファイルを拡充することも容易になります。

プロファイル管理

パーソナライズされた顧客体験を提供するには、顧客の全体像をリアルタイムで把握する必要があります。この全体像は、顧客プロファイルを構築するProfile Serviceによって実現されます。Profile Serviceは、1stパーティデータや3rdパーティデータを含む、様々なエンタープライズリポジトリーからデータを取り込むことができます。それらのデータは、CRMデータやeコマースのトランザクション、オフラインのトランザクション、ロイヤルティプログラムのデータ、モバイルの行動データ、webの行動データ、電子メールの行動データ、ソーシャルインタラクションデータなど、多岐に渡ります。

複数のデータソースからのデータをつなぎ合わせることで、顧客の全体像を把握できます。各データソースには、それぞれ独自の顧客IDの概念があります。これらのIDは互いに照合されます。1stパーティデータをつなぎ合わせる場合は、重複排除、データ結合、およびサバイバーシップルールが必要となります。オンライン行動データの場合、IDはcookieをもとにしていることが多く、cookieを照合するための手法が必要となります。モバイルとIoTには、デバイスにもとづいた独自のIDの概念があります。Adobe Experience Platform Identity Serviceでは、決定論的アルゴリズムおよび確率論的アルゴリズムを使用して、IDを照合し、これらの関係をグラフとしてモデル化します。

データフローの概要

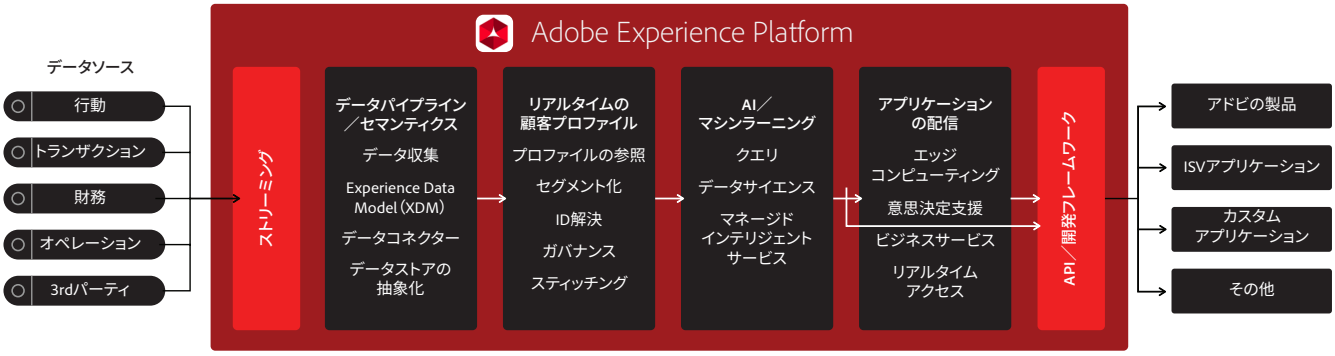
Adobe Experience Platformは、顧客体験データの信頼できる永続的な単一リポジトリーです。容易にアクセスでき、常に最新に保たれた、高速かつ完全なデータストアが提供されます。アクティベーションシステムは、このデータストアを使用して、データへのアクセスやクエリ、構成、管理をおこないます。Adobe Experience Platformは、複数のタイプのデータベース（アドビのデータレイク、NoSQL、グラフなど）を提供し、ユースケースに応じて様々な形式でデータを保存し、複数のデータアクセスパターン（リアルタイム、ニアリアルタイム、バッチ）をサポートします。データベースは組み込まれているので、データベースを新しく構築する必要はありません。

Adobe Experience Platformは、ストリーミングやBulk Ingestion API、ネイティブの3rdパーティ接続、Adobe Experience Platform Mobile SDK、Adobe Experience Platform Launchなどの様々な方法を用いて、様々な手段で、ほぼすべてのソースから構造化データ、半構造化データ、および非構造化データをオンボーディングすることができます。Adobe Experience Platformは、取り込む前にあらゆるデータを評価し、関連するXDMスキーマで指定された属性と制約によってオンボードデータをクエリできるようにします。データの取得中、データセット、スキーマ、サンプルデータ、系統、および指標に関する情報が、アドビのカタログに一覧表示されます。

Adobe Experience Cloud製品を使用している企業であれば、Adobe Experience Platformにデータを自動的に取り込み、リアルタイムで活用することができます。XDMを使用することで、アドビ製品から収集した顧客データとその他の顧客データを容易に組み合わせることができます。

Adobe Experience Platformでデータの標準化と取り込み、保存をおこなえば、APIを介して、ほぼすべてのチャネルで顧客プロファイルを構築して活用できます。Adobe Experience

Platform Data Science WorkspaceやAdobe Experience Platform Query Serviceなどのサービスを使用して顧客プロファイルを強化できます。さらに、Adobe Experience Platformの強力なデータカタログは、基盤内に保存されているあらゆるメタデータを管理し、データの検出やデータガバナンスを可能にします。データレイクに保存されているデータは、セキュリティのために暗号化されます。



Adobe Experience Platformデータワークフロー図

セキュアなアーキテクチャ

Adobe Experience Platformは「共有アーキテクチャ」にもとづき、エンゲージメントシステムから収集したあらゆるエクスペリエンスデータを結合し、Experience System of Record（顧客体験のためのSoR）を構築します。Adobe Experience Platformが使用するサービスモデルは、セキュリティに対するアプローチを合理化します。単一のアクセスゲートウェイ（Adobe.io）を使用することで、意図したトラフィックと意図しないトラフィックをすばやく把握することができます。Adobe Experience Cloud全体を通じてセキュリティ制御を適用できるように、オペレーションレベルのセキュリティとアプリケーションレベルのセキュリティの両方のセキュリティモデルを標準化しています。

Adobe Experience Platformでは、Azure Blob Storageとネットワークセキュリティ機能を活用することで、堅牢なセキュリティ制御、プログラム、およびプロセスにもとづいて、アドビ製品と顧客企業のセキュリティ体制を継続的に改善しています。

ADOBE EXPERIENCE PLATFORMのセキュリティ

Adobe Experience Platformは、エンタープライズクラウドインフラストラクチャサービスを使用して、セキュリティインフラストラクチャ、データ、およびシステムを提供します。データの取得や入力は、認証ユーザー、システム、およびサービスに制限されます。これらの入力接続は、UIやセキュアなREST APIを介しておこなわれます。次に、データはデータレイクに保存されます。このデータレイクは、データやアルゴリズムのサンドボックスとして機能します。あらゆるデータ、スキーマ、構成、およびプロファイルは認証層経由で保護され、適切に承認されたユーザーのみがアクセスできます。

それぞれの顧客のデータは、個別のサブスクリプションに格納されます。ロールベースのアクセス制御は、データへのアクセスを許可されたユーザーのみに制限するのに役立ちます。データレイク内のデータは、企業が定義したルールによって管理されます。また、Adobe Experience Platformはデフォルトで、保存中のデータを暗号化します。

アドビのセキュリティ

認証とアクセス管理

アドビでは、IMS認証をサポートしています。これにより、Adobe Enterprise IDを使用できるようになりますが、Adobe Experience Platformへのアクセスに関する制御項目を追加したい企業は、Federated IDを選択することもできます。Federated IDを使用すれば、企業は既存のIDプロバイダーを活用して、Adobe Experience Platformの認証をおこなうことができます。Adobe Experience Platformは、Adobe Identity Management Service（IMS）を活用して、レガシーLDAP準拠、SAML準拠、およびSSOシステムをサポートします。Adobe IMSの詳細は別途ご確認ください。

クラウドインフラストラクチャプロバイダーのオペレーション上の責任

アドビでは、認定クラウドインフラストラクチャプロバイダーと契約を結び、コンポーネントの運用、管理、および制御をおこないます。契約の範囲は、ハイパーバイザービジュアライゼーション層から、Adobe Experience Platformを実際にデプロイする施設の物理的なセキュリティに至るまで、多岐にわたります。

これらのプロバイダーは、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、様々な基本的なコンピューティングリソース（処理やストレージを含む）のプロビジョニングをおこないます。このインフラストラクチャには、これらのリソースのプロビジョニングや使用をサポートする施設、ネットワーク、ハードウェア、運用に使用するソフトウェア（ホストOS、仮想化ソフトウェア）が含まれます。アドビには、「Guardrails」と呼ばれるサードパーティベンダーのセキュリティ評価プログラムがあり、これらのプロバイダーが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標準規格を順守しているかどうかを評価しています。

サービスモニタリング

アドビのクラウドサービスプロバイダーは、サービスの問題を即座に特定できるよう、電気設備、機械設備、ライフサポートシステム、装置、および環境の状態を監視しています。アドビのクラウドプロバイダーには設備の運用性を維持するために、定期的な予防保守の実行が求められます。

物理制御と環境制御

SOCレポートには、必須の物理制御と環境制御について具体的に明記されています。以下に、世界中にあるアドビのクラウドサービスプロバイダーのデータセンターで採用されているセキュリティ対策と制御の一部を解説します。

物理施設のセキュリティ

クラウドインフラストラクチャパートナーのデータセンターは、業界標準の構造的アプローチとエンジニアリングアプローチを活用しています。これらのデータセンターは目立たない施設に格納されており、パートナーは専門のセキュリティスタッフ、監視カメラ、侵入検知システム、およびその他の電子的手段を使用して、周辺や建物の入口で物理アクセスを制御します。許可されたスタッフがデータセンターのフロアに入るためには、二要素認証で2回以上承認される必要があります。あらゆる訪問者と請負業者は、受付でIDを提示して氏名を記入し、常に許可されたスタッフの付き添いを必要とします。

インフラストラクチャパートナーから、データセンターへのアクセス権や情報の提供を受けることができるのは、これらの特権を業務上必要とする従業員や請負業者だけです。従業員が業務においてこれらの特権を使用する必要がなくなった際には、引き続きパートナーの従業員であったとしても、ただちにアクセス権が取り消されます。データセンターへのあらゆる物理的なアクセスは記録され、定期的に監査を受けます。

消火

クラウドアーキテクチャプロバイダーは、では、自動火災検知設備と消火設備をあらゆるデータセンターに備えています。自動火災検知設備は、あらゆるデータセンター環境、機械および電気インフラストラクチャスペース、冷却室、発電機室で煙検知センサーを活用します。これらのエリアは、ダブルインターロック方式の予作動式（湿式）スプリンクラーシステムまたはガス系スプリンクラーシステムのどちらかで保護されています。

空調管理環境

クラウドサービスプロバイダーは、サーバーやその他のハードウェアの動作温度を一定に保つために空調管理システムを採用してオーバーヒートを防ぎ、サービス停止の可能性を低減しています。データセンターでは、最適なレベルで大気条件が維持されます。担当者およびシステムにより、適切なレベルで温度と湿度が監視および制御されています。

バックアップ電源

データセンターの電源システムは、完全な冗長性を備え、24時間365日、運用に影響を与えずにメンテナンスできるよう設計されています。無停電電源装置（UPS）装置は、停電発生時にバックアップ電源として、施設の重要および不可欠な負荷に対応します。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提供します。

監視カメラ

専門のセキュリティスタッフが、監視カメラや侵入検知システムなどの電子的手段を使用して、データセンターの周囲や建物入口での物理的なアクセスを厳密に制御します。

障害回復

データセンターには高度な可用性が備わっており、システム障害やハードウェア障害の際、影響を最小限に抑えることができます。すべてのデータセンターが、世界中の様々な地域でクラスター状に構築され、24時間365日、顧客にサービスを提供し続けます。停止状態になるデータセンターはありません。障害が発生すると、顧客データトラフィックは、影響を受けた地域から自動的に移動されます。主要アプリケーションはN + 1構成でデプロイされているので、データセンターに障害が発生した場合でも、残りのサイトにトラフィックの負荷を分散できる十分な容量を有しています。

セキュアなネットワークアーキテクチャ

アドビでは、クラウドサービスプロバイダーに対し、ネットワークの外部境界と主要な内部境界での通信を監視および制御するため、ファイアウォールやその他の境界デバイスなどのネットワークデバイスを導入することを要求しています。これらの境界デバイスは、ルールセット、アクセス制御リスト（ACL）、および構成を用いて、特定の情報システムサービスへの情報の流れを強化します。ACLまたは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に存在し、トラフィックフローを管理および強化します。アドビでは、クラウドプロバイダーと連携し、最新のACLを使用しています。

ネットワークの監視と保護

クラウドインフラストラクチャプロバイダーは、高度なサービスパフォーマンスと可用性を確保できるよう、様々な自動監視システムを採用しています。監視ツールは、通信の出入り口で、異常または不正なアクティビティや状況を検出するのに役立ちます。これらのツールでは、優れた保護機能を利用することができ、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応可能です。

- 分散型サービス妨害（DDoS）攻撃
- 中間者（MITM）攻撃
- IPスプーフィング
- ポートスキャン
- 他のテナントによるパケットスニッフィング

データストレージとバックアップ

デフォルトでは、アドビはクラウドインフラストラクチャパートナーから提供された、高耐久性ストレージサービスを使用して、Adobe Experience Platformのあらゆるデータを保存します。また、PUTおよびCOPYオペレーションにより、複数の施設をまたいで顧客データを同期的に保存し、プロバイダーの地域にある複数の施設の複数のデバイスにオブジェクトを冗長的に保存することで、耐久性を実現します。さらに、プロバイダーは、データを保存または取得する際にあらゆるネットワークトラフィックでチェックサムを計算し、データパケットの破損を検出します。

変更管理

クラウドサービスプロバイダーには、同様のシステムの業界標準に従って、既存のインフラストラクチャに対する所定の変更、緊急の変更および設定の変更を認証、記録、テスト、承認および文書化する責任があります。また、顧客企業への影響が最小限になるようにアップデートのスケジュールを設定する必要があります。

パッチ管理

Adobe Experience Platformのクラウドインフラストラクチャプロバイダーは、IaaSサービス（ハイパーバイザーやネットワークサービスなど）の提供をサポートするシステムのパッチ適用をおこなっています。

アドビのリスク管理と脆弱性管理

アドビでは、リスクと脆弱性の管理、インシデントの対応、軽減および解決プロセスが迅速かつ正確に実施されるよう取り組んでいます。アドビでは、脅威の状況を継続的に監視し、世界中のセキュリティ専門家と知識を共有して、発生したインシデントをすばやく解決します。さらに、Adobe Experience Platformだけでなく、アドビのすべての製品とサービスで最高レベルのセキュリティを実現できるよう、この情報を開発チームにフィードバックしています。

侵入テスト

アドビでは、承認した社外の大手セキュリティ組織と協力して侵入テストを実行しています。これによって、潜在的なセキュリティ脆弱性を発見し、アドビの製品とサービスの全体的なセキュリティの向上に役立てています。セキュリティ組織から提供されたレポートを受け取ると、アドビは、これらすべての脆弱性をドキュメント化し、重大度と優先度を評価して、軽減戦略や修復計画を作成します。また、アドビには、Adobe Experience Platformの侵入テストを定期的に実施する社内の侵入テストチームがあります。

セキュリティレビュー

Adobe Experience Platformのセキュリティチームは、あらゆるコンポーネントのリスク評価を定期的に実施しています。経験豊富なセキュリティエンジニアとAdobe Experience Platform専門のアーキテクトによって実施される詳細なセキュリティレビューでは、スタック全体の設計上の欠陥、脆弱性、および安全性の低い構成を確認します。セキュリティ検出アクティビティには、脅威モデリングの実施のほか、脆弱性スキャン、アプリケーションの静的および動的分析が含まれます。セキュリティチームは、オペレーションおよび開発チームと連携して、リスクの高い脆弱性を迅速に軽減しています。

インシデントへの対応および通知

新しい脆弱性と脅威が、毎日のように出現しています。アドビは、新たに発見された脅威を即座に軽減するよう努力しています。アドビでは、US-CERT、Bugtraq、SANSなどの業界全体の脆弱性アナウンスリストの利用に加え、大手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ています。

脆弱性によってAdobe Experience Platformがリスクにさらされた場合、アドビのProduct Security Incident Response Team（PSIRT）が組織内の適切なチームにその脆弱性を報告し、軽減に向けた取り組みを調整します。

クラウドベースのサービスの場合、アドビではインシデント対応、意思決定、および外部モニタリングをSecurity Coordination Center（SCC）に一元化し、部門の枠を超え、一貫性を持って問題の迅速な解決に取り組みます。

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、次のような実績あるプロセスを使用して問題を特定、軽減、解決できるよう支援します。

- 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強制隔離、調査、破棄（クラウドベースサービスの場合のみ）
- 脆弱性に対する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

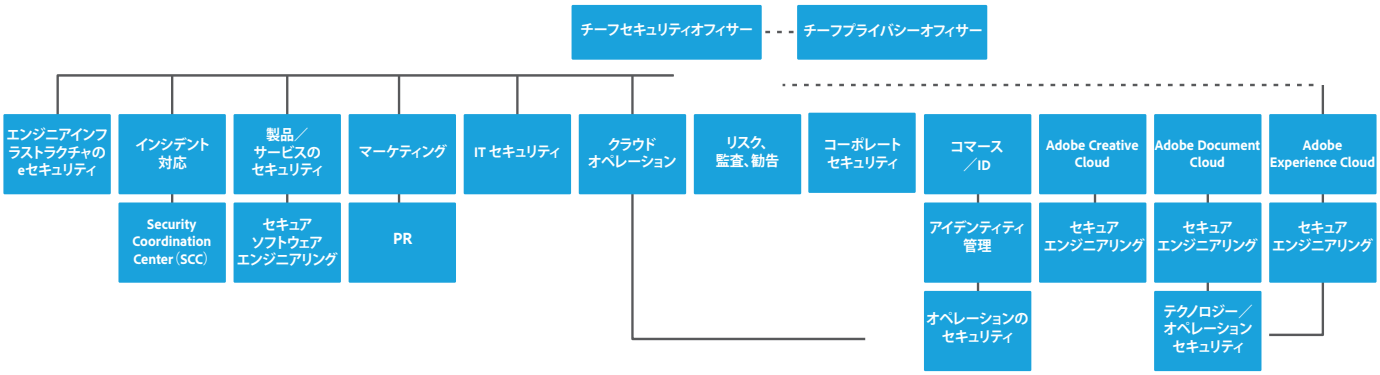
フォレンジック分析

インシデントの調査にあたり、Adobe Experience Platformチームは、アドビのフォレンジック分析プロセスに従います。これには、影響を受けたマシンの完全なイメージキャプチャまたはメモリダンプ、証拠保全、過程を管理および追跡できる記録などが含まれます。必要であると判断された場合、アドビは法的機関や社外のフォレンジック専門企業と協力することがあります。

アドビのセキュリティ組織

製品と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、アドビでは、チーフセキュリティオフィサー（CSO）の下にあらゆるセキュリティ活動を統合しています。CSOは、製品とサービスのセキュリティ対策とAdobe Secure Product Lifecycle（SPLC）の実装を取りまとめています。

また、CSOは、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から成る専任のチームです。Adobe Experience Platformチームをはじめ、主要なアドビ製品チームおよびオペレーションチームに対する役割を担っています。ASSETのセキュリティ研究者は、それぞれの製品チームおよびオペレーションチームと協力して、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ます。さらに、開発、導入、運用、インシデント対応のための再現可能なわかりやすいプロセスのセキュリティプラクティスについて、チームにアドバイスします。



アドビのセキュリティ組織

アドビのセキュアな製品開発

他の主要なアドビ製品およびサービス組織と同様に、Adobe Experience Platform組織ではSPLCプロセスを使用します。ソフトウェア開発のプラクティスやプロセス、ツールなどを含む数百もの特定のセキュリティアクティビティを厳選したAdobe SPLCは、設計や開発から品質保証、テスト、デプロイに至るまで、製品ライフサイクルの複数の段階に組み込まれています。

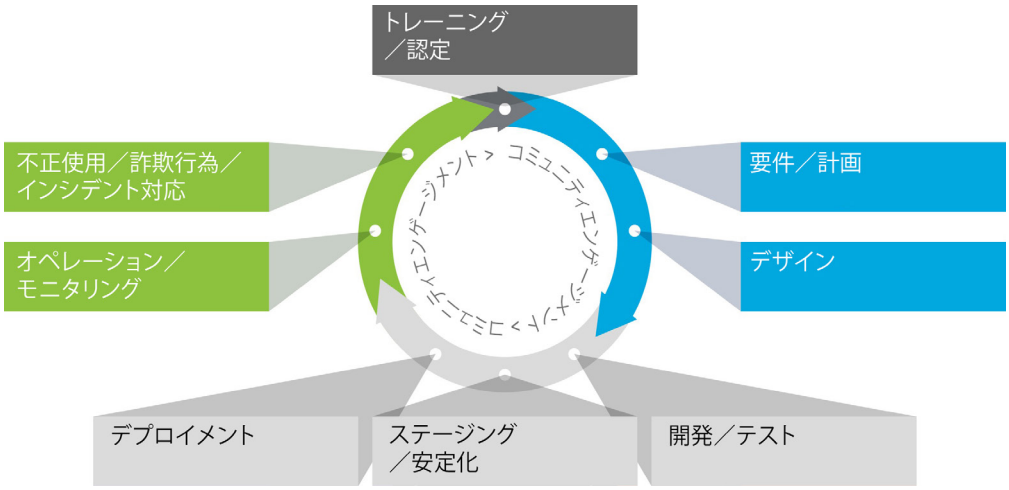
ASSETのセキュリティ研究者は、潜在的なセキュリティ問題の評価にもとづいて、各主要製品またはサービスに対する具体的なSPLCガイダンスを提供します。Adobe SPLCは、継続的なコミュニティ活動によって補完され、テクノロジーやセキュリティプラクティス、脅威の状況に変化が生じても、常に最新の状態が保たれるようになっています。

Adobe SPLC

Adobe SPLCのアクティビティには、それぞれのAdobe Experience Platformコンポーネントに応じて、次のようなベストプラクティス、プロセス、ツールの一部またはすべてが含まれています。

- 製品チーム向けのセキュリティトレーニングと認定
- 製品の健全性、リスク、脅威の状況分析
- セキュアなコーディングガイドライン、ルール、分析

- Open Web Application Security Project（OWASP）の最も重大なwebアプリケーションのセキュリティリスク上位10件と、CWE/SANSの最も危険なソフトウェアエラー上位25件に、Adobe Experience Platformセキュリティチームが対処できるように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手法
- セキュリティアーキテクチャのレビューと侵入テスト
- 脆弱性を引き起こす可能性がある既知の不具合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
- レディネスに関する包括的なレビュー、対応計画、開発者向け教材のリリース



Adobe SPLCプロセス

アドビのソフトウェアセキュリティ認定プログラム

アドビでは、Adobe SPLCの一環として、開発チームに対して継続的なセキュリティトレーニングを実施し、全社を挙げてセキュリティの知識を高め、製品とサービスの包括的なセキュリティの強化に取り組んでいます。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を取得できます。

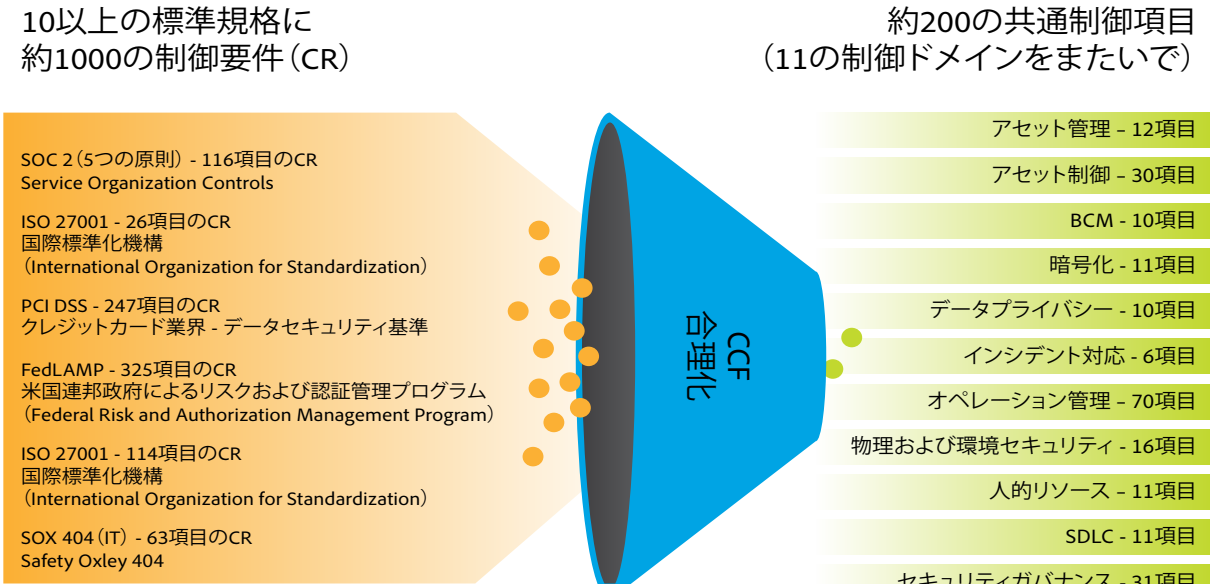
プログラムには4つのレベルがあり、それぞれに「ベルト」の色（白、緑、茶、黒）が指定されています。白と緑のレベルは、コンピューターベースのトレーニングを修了することで取得できます。さらに上位の茶と黒のレベルを取得するには、数ヶ月から1年に及ぶ実務経験を伴うセキュリティプロジェクトを修了する必要があります。茶または黒のベルトを獲得した従業員は、製品チーム内のセキュリティ責任者およびエキスパートになります。新たな対策方法やソフトウェア言語を学んだり、新しい脅威や軽減方法に対応するために、トレーニング内容は定期的に更新されています。

また、Adobe Experience Platform組織の各チームは、追加のセキュリティトレーニングやワークショップに参加し、組織および企業内で自分たちに割り当てられた特定の役割にセキュリティが及ぼす影響について、意識を高めています。

Adobe Common Control Framework

ソフトウェア層から下のレイヤーに向けてセキュリティを保護するために、アドビでは前述のとおり、Adobe SPLCを使用しています。物理層から上のレイヤーに向けてセキュリティを保護するためには、セキュリティプロセスと制御の基礎となるフレームワークを実装しています。このフレームワークは、企業のインフラストクチャ、アプリケーション、およびサービスを保護し、多数の業界認証済みベストプラクティス、標準規格、および認定制度を順守するのに役立ちます。

Adobe Common Control Framework（CCF）を構築するにあたり、アドビでは、最も一般的なセキュリティ証明の基準を分析し、重複している項目が多数あることに気付きました。関連するクラウドセキュリティフレームワークと標準規格の1,000を超える要件を分析した結果、これらを合理化し、約200のアドビ独自の制御項目にまとめることができました。このCCF制御項目を見れば、制御機能の実装において、アドビの関係者や顧客の期待に応えるために何が必要かを正確に把握することができます。



Adobe CCF

アドビのオフィス

世界中にオフィスを構えているアドビでは、セキュリティの脅威に立ち向かうため、全社を挙げて次のようなプロセスと手順を実装しています。

物理的なセキュリティ

アドビのすべてのオフィスでは、オフィス内を24時間体制で警備しています。アドビの従業員は、オフィスに入室するためのキーカード型IDバッジを携帯しています。訪問者は正面玄関から入り、受付で氏名を記入して、一時的な訪問者IDバッジを受け取り、提示します。訪問者には従業員が同伴します。アドビでは、サーバー機器や開発マシン、電話システム、ファイルサーバー、メールサーバーなどの慎重に扱うべきシステムは、環境制御されたサーバールームに常時設置され、そのサーバールームへのアクセスは認可されたスタッフメンバーのみに制限されています。

ウイルス対策

アドビでは、既知のマルウェアによる脅威を見つけるため、送受信されたすべての企業電子メール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

アドビでは、技術的な制御機能を使用して、稼動中の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、Adobe Experience Platform用に分割された開発環境と本番環境を維持しています。従業員は、開発システムと本番システムにアクセスする際に専用の認証が義務付けられており、ビジネス上の正当な理由なしに、これらのシステムにアクセスすることは禁じられています。

身元調査

アドビは、雇用目的で身元確認レポートを取得しています。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、学歴や職歴、犯罪歴などの裁判記録の照会と同僚や友人による身元保証が含まれます。これらの身元確認要件は、システムを管理したり企業の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、アドビの身元確認ガイドラインに従って適切な派遣会社を通して身元確認要件が課されます。米国以外では、アドビの身元調査ポリシーと適切な現地の法律に従って特定の新入社員について身元調査を実施しています。

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、アドビの人事担当者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実施するように通知します。アドビが従業員を解雇する場合は、人事担当者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。

その後、コーポレートセキュリティ担当者が、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にアクセスしたり、オフィスに入室したりできないようにします。

- 電子メールアドレスの削除
- リモートVPNアクセス権の削除
- オフィスおよびデータセンターバッジの無効化
- ネットワークアクセスの停止

必要に応じて、上司は、退職する従業員がオフィスまたは建物から退去するまで警備員に同伴させることができます。

顧客データの守秘義務

アドビは常に、顧客企業のデータを機密情報として扱います。顧客企業との契約で許可されていて、なおかつアドビの利用規約およびアドビのプライバシーポリシーで定められている場合を除き、アドビが収集した情報を使用したり共有したりすることはありません。

標準コンプライアンス

あらゆるアドビのサービスは、文書化された包括的なセキュリティプロセスによって管理され、品質を保持および向上させるため、数多くのセキュリティ監査を受けています。アドビのサービスに対しては、ISO 27001標準規格に照らし合わせて継続的に社内レビューが実施されています。また、サービスインフラストラクチャの基礎となる共有クラウドは、SOC 2セキュリティ認証を取得しています。

アドビが選ばれる理由

アドビは、企業がより優れたサービスや体験を顧客に提供できるように支援します。Adobe Experience Platformは、企業やパートナーが、合理化されたシームレスな顧客体験管理に取り組むための道を切り拓きます。それは、データとプロファイル管理の課題を解決することから始まります。続いて、Adobe Senseiのサービスと独自のマシンラーニングモデルを使用して、実用的なインサイトで顧客のプロファイルを強化し、Adobe Experience Cloud、Adobe Creative Cloud、Adobe Document Cloudのアプリケーションで活用します。さらに、シームレスな統合を実現する機能とオープンAPIを利用して、独自のソリューションや統合を構築することができます。

これまでに解説したセキュリティへのプロアクティブなアプローチと厳密なプロセスは、顧客企業の機密データのセキュリティを保護するのに大きく役立っています。アドビでは、顧客企業のデジタルエクスペリエンスのセキュリティを重視しているため、最も厳しいセキュリティを念頭に置いてAdobe Experience Platformを開発しました。さらに、不正なアクティビティの先を行き、データのセキュリティを確保できるよう、変化を続ける驚異の状況を継続的に監視しています。

詳しくは、こちらをご覧ください。

本書の情報は事前の告知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と制御項目の詳細については、アドビの営業担当者にお問い合わせください。SLAや変更承認プロセス、アクセス制御プロセス、障害回復プロセスなど、アドビのソリューションの詳細をご説明します。

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

5/19