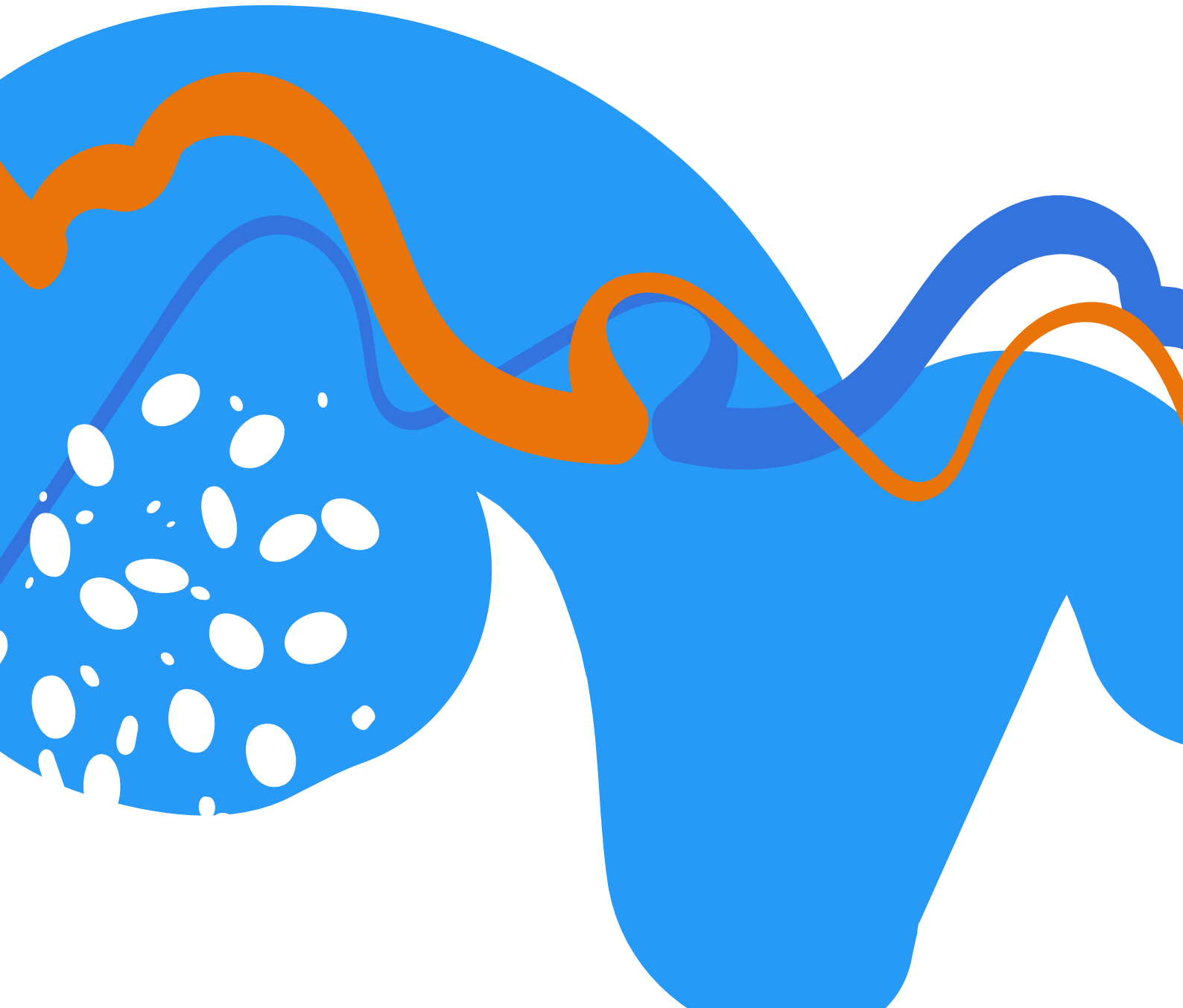
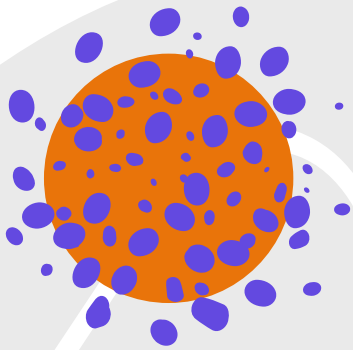
ホワイトペーパー

アドビアプリケーション セキュリティの概要



目次



はじめに

アドビはセキュアなアプリケーション開発を重要課題とし、セキュリティに関する研究および技術に多大な投資をおこなってきました。アドビのアプリケーションセキュリティチームは、製品やサービスに最も効果的なセキュリティ対策を組み込みながらイノベーションを推進し続けることに重点を置き、製品およびサービスチームと協力して「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）を前提としてアプリケーションを開発しています。また、データ収集やリスクにもとづく意思決定に様々な自動化アプローチを採用し、会社全体のセキュリティ対策の強化を図っています。

このホワイトペーパーでは、アドビのアプリケーションセキュリティ戦略について説明します。この戦略では、開発サイクルの初期段階でセキュリティ管理を導入することによって、拡張性を高め、全体的なコストを削減し、実際のセキュリティリスクの可能性を最小限に抑えることに重点を置いています。これらはすべて、アドビとお客様のデータおよびワークフローを保護するための最新のセキュリティ対策に対する弊社の取り組みを強化するものです。

アドビのアプリケーションセキュリティ戦略

アドビのアプリケーションセキュリティ戦略は、セキュリティ問題に対処することよりも、根本的に解決することを重視しており、アプリケーション開発ライフサイクルの初期段階でセキュリティ対策を導入する「シフトレフト」によって、これを実践しています。具体的には、開発の要件、アーキテクチャ、設計、コーディングの各段階でセキュリティの制御とメカニズムを確立することにより、セキュリティ管理を開発に組み込んで、後のテスト段階で生じる変更コストを削減します。このアプローチは、実際のセキュリティリスクの可能性を最小限に抑えるため、お客様のセキュリティ向上にもつながります。

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には、あらゆるセキュリティへの取り組みの基礎となるAdobe Secure Product Lifecycle（SPLC）が組み込まれています。数百に及ぶ厳格なセキュリティ対策を取りまとめたSPLCには、開発チームが製品やサービスにセキュリティを組み込む際に役立つ明確で反復可能なプロセスおよび機能が定義されています。

Adobe SPLCは全社的に導入され、アプリケーションセキュリティチームのセキュリティ研究者によって検証されます。同チームは、アドビの製品およびサービスの各チームに対して、セキュリティ管理のベストプラクティスを提言するとともに、自動化によってセキュリティ管理を検証します。Adobe SPLCのコントロールには、セキュリティチームが「Open Web Application Security Project（OWASP）アプリケーションの脅威Top 10」と「CWE／SANSプログラミングエラーTop 25」に対処するためのロードマップ、セキュリティツールおよびテスト方法が含まれています。Adobe SPLCについて詳しくは、Adobe Trust Centerをご覧ください。

アドビアプリケーション セキュリティスタック

アドビでのセキュアなアプリケーション開発の出発点は、アプリケーションセキュリティスタックです。製品チームは、セキュア・バイ・デフォルトのプラットフォームを使用することから始め、様々な自動セキュリティ機能でアプリケーションを検証し、仕上げにセキュリティレビューと手動でのテストをおこないます。

3層から成るこのスタックには、顧客データとワークフローの保護に重点を置いた最新のセキュリティ対策にもとづく幅広いツールとサービスが含まれており、アドビの製品チームは開発プロセスでこれを使用して、すべてのアドビアプリケーションにセキュリティを確実に組み込むことができます。

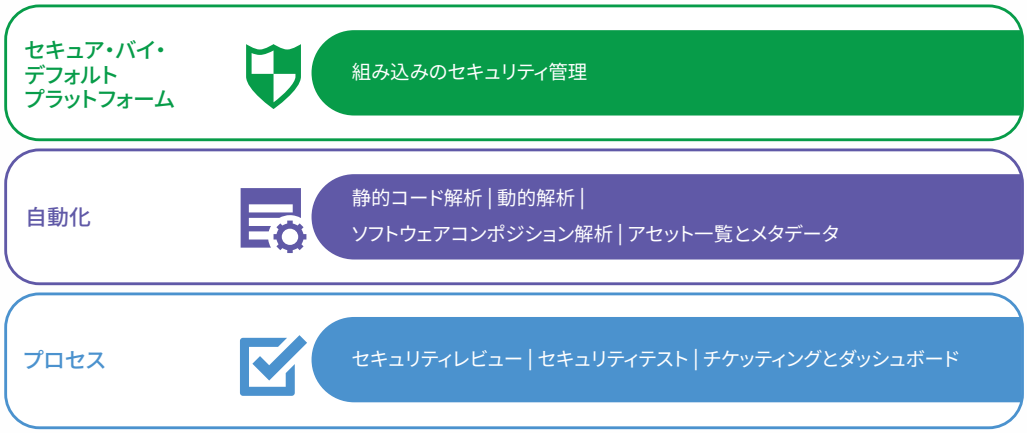


図2：アドビアプリケーションセキュリティスタック

セキュア・バイ・デフォルトプラットフォーム

アドビの開発者は、事前承認済みのセキュア・バイ・デフォルトプラットフォームを使用して、アドビの製品およびサービスの開発を迅速かつ安全に進めるための環境を整えます。これには、検証および承認済みのIDサービスや承認サービス、APIゲートウェイ、メッセージングシステム、SDK、フレームワークなどが含まれます。

セキュア・バイ・デフォルトプラットフォームを使用すると、拡張が容易なだけでなく、セキュリティの機能と構成が正しく実装されていることを確認できます。このプラットフォームには、検出と予防という2大原則にもとづいて、安全でない可能性のある使用パターンを特定する継続的検出ソリューションと、製品およびサービスのセキュリティをあらかじめ確保するための体制実現に役立つ予防的制御が組み込まれています。

セキュア・バイ・デフォルトプラットフォームにより、以下が確保されます。

- **安全な使用** — 大量の構成データ、ログ、ソースコードの継続的な解析により、製品やサービスのセキュリティ構成の不備を迅速に特定し、逸脱を見つけて、適切な製品チームに警告することができます。
- **組み込みのセキュリティ管理** — 最小限の権限、デフォルト拒否、組み込み認証などのベストプラクティスに従ったセキュリティ管理への投資を活かすことで、アドビの製品チームは、顧客データやワークフローを保護しながら製品の開発に専念できます。

セキュリティの自動化

アドビでは、自動化によってアプリケーションのセキュリティを全社規模に拡大し、急速なイノベーションに合わせて常に適切なセキュリティを提供しています。また、ソフトウェアコード、構成データ、リクエスト／レスポンスのトラフィック、アプリケーションログを対象とする静的および動的な解析により、ソフトウェア開発のライフサイクル全体のセキュリティを確保しています。

- **静的コード解析** — アドビの自動コード解析プラットフォームでは、オープンソースと市販ツールの両方を利用してコードリポジトリをスキャンし、問題が最も軽減されやすい開発ワークフロー中に、フィードバックを開発者に直接提供します。これらのツールを環境に固有の機能と併用することで、ソースコードのセキュリティを最大限に高めることができます。
- **動的解析** — 静的コード解析の手法と同様、カスタマイズしたツールと市販のツールを使用して、実行時のセキュリティ脆弱性を特定します。
- **ソフトウェアコンポジション解析** — アドビの製品やサービスにおけるサードパーティコンポーネントの使用を厳重にモニタリングし、社内と市販のソリューションを併用して、それらのコンポーネントのセキュリティ体制を定期的に見直します。脆弱なコンポーネントやサポートが終了するコンポーネントが見つかると、即座に対策を講じることができるよう開発者に警告します。
- **アセット一覧とメタデータ** — 企業規模の大量のメタデータは、アプリケーションセキュリティチームがアドビの製品およびサービスについて理解を深めるのに役立ちます。

プロセス

アドビのセキュリティ戦略の基盤を形成するのは、社内のセキュリティの専門知識とプロセスです。アドビでは、セキュリティチームのメンバーとセキュリティチャンピオンの両方に対して、最先端のテクノロジーやアプローチに関する研修を継続的に実施しています。また、チケッティング、ダッシュボード、および攻撃者情報と脅威モデリングによる効果的なリスク軽減を組み合わせて、セキュリティ戦略を効果的に進める仕組みを作っています。

セキュリティレビュー

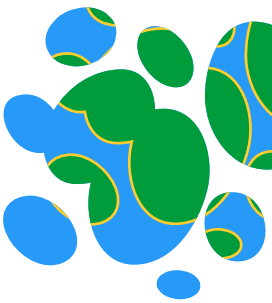
アドビの製品およびサービスのセキュリティを保証するために、アドビは、セキュリティに関する問題の特定、それらの問題に関連するリスクレベルの判定、リスクの軽減や承認についてのデータにもとづく意思決定に共同作業で取り組み、以下のことをおこなっています。

- **脅威モデリング** — 設計段階で脅威モデリングを実行することで、開発ライフサイクルの早期にセキュリティ上の欠陥を特定し、アドビの製品およびサービスそれぞれについて強力なセキュリティ基盤を築きます。脅威モデリングでは、既知の脅威を回避するのにアーキテクチャ上の変更が必要となる可能性を洗い出します。脅威モデリングプロセスを自動化すると、セキュリティ要件を自動的に生成して効果的に拡張できるため、レビュープロセスが効率化します。
- **的を絞ったコードレビュー** — 機密データを扱う特定部分のコードや複数のサーバーで再利用されるコンポーネントを対象に、アドビのセキュリティ研究者が手動のコードレビューを実行し、コードがセキュリティのベストプラクティスに従っていることを確認します。
- **焦点を絞ったテスト** — 攻撃者の関心や既知の攻撃パターンなどの様々な要因にもとづいて、アドビのセキュリティ研究者が製品やサービスの定期的なセキュリティテストを実行します。

セキュリティテスト

アドビでは、定期的なセキュリティレビューに加え、製品やサービスの侵入テストをおこなって脆弱性が特定された部分の強化を図り、ユーザーコミュニティをバグバウンティプログラムに参加させて問題の検出と報告を促しています。アドビのセキュリティテスト活動には以下が含まれます。

- **内部侵入テスト** — アドビの社内セキュリティチームは、セキュリティレビューで指摘された脆弱な部分を対象に、自動と手動の手法を併用してコードベースの侵入テストを実行します。
- **外部侵入テスト** — 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。第三者によるレポートを受け取り次第、指摘された脆弱性を文書化し、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。問題が解決したら、問題の修復を確認するために侵入テストを再度実行します。
- **バグバウンティ** — アドビは、社内外でバグバウンティプログラムを継続的に実施し、ソフトウェアバグを発見・報告した個人を表彰したり、報奨金を支払ったりしています。社内のバグバウンティでは、セキュリティに詳しい社内の人材を活かして、エンジニアリングチーム全体のアプリケーションセキュリティ意識を高めます。また、社外のセキュリティ研究者コミュニティを活用し、アドビやアドビのお客様に影響を及ぼすセキュリティの脆弱性を責任を持って開示します。特定製品に関する問題の責任ある開示は、手続きを踏むと報奨金を授与されます。



チケッティングとダッシュボード

自動チケッティングは、製品チームが即座に問題を軽減できるように、既知の悪用されたセキュリティ脆弱性や悪用可能なセキュリティ脆弱性を通知します。チケットは、チームのスキルや経験、製品に関する知識にもとづいて自動的に割り当てられます。アプリケーションセキュリティチームは、ダッシュボードと主要業績評価指標（KPI）を使用して、アドビアプリケーションセキュリティスタックの全社への導入状況を評価するとともに、セキュリティ自動化ソリューションの効果を判断することができます。

まとめ

アドビの製品およびサービスチームは、アドビアプリケーションセキュリティスタックを使用し、「セキュア・バイ・デフォルト」を前提としてアプリケーションを開発しています。また、アプリケーションセキュリティチームは、開発サイクルの早期にセキュリティ管理を導入することで、セキュリティリスクの未然防止と、製品およびサービスのエンドツーエンドのセキュリティの維持を促進しています。アドビは、自動化を活用すると同時に、レポート、ダッシュボード、四半期ごとのコンプライアンスレビューによりセキュリティ体制を継続的にモニタリングすることで、この成果を確保します。

11/22