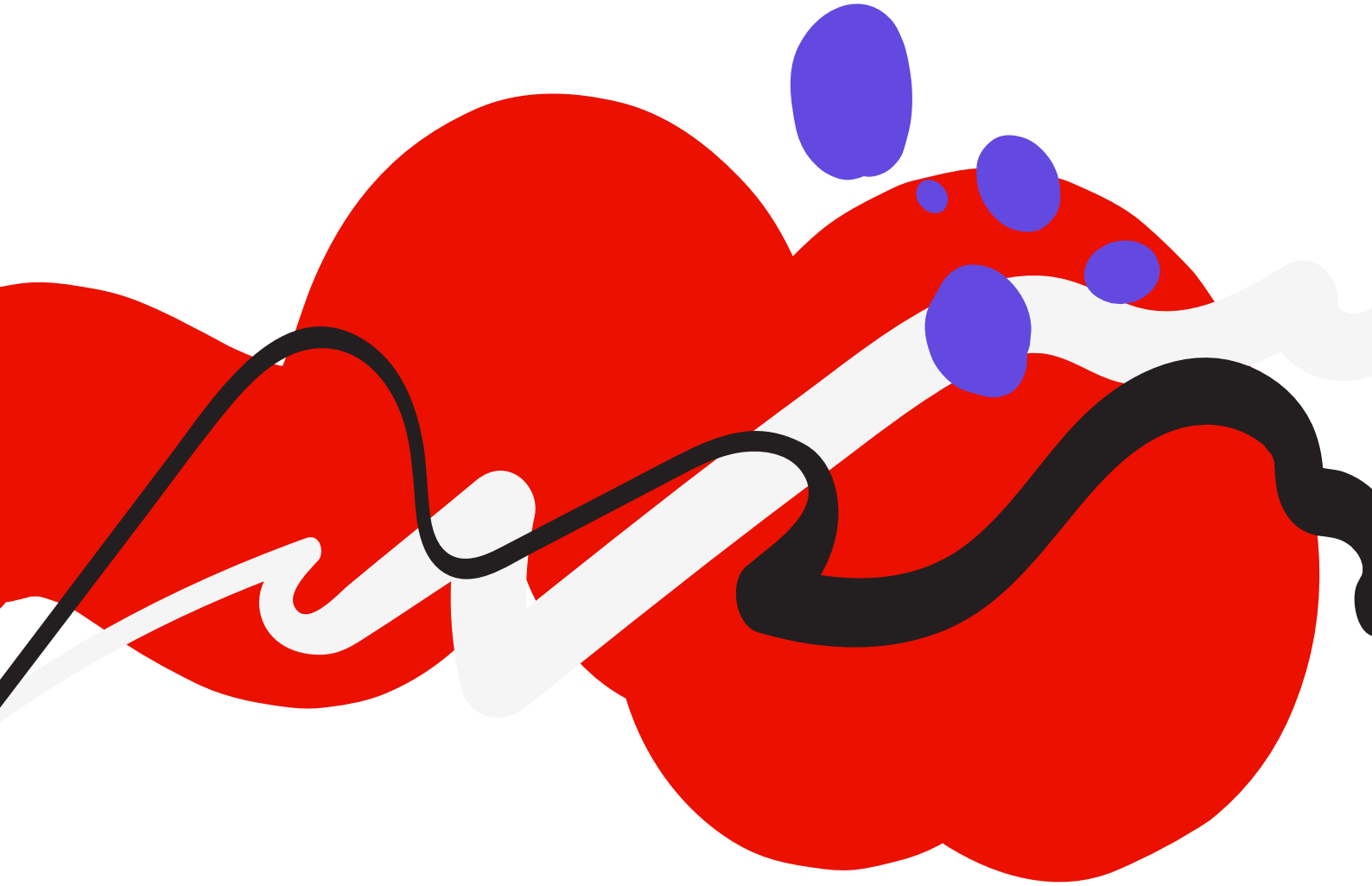
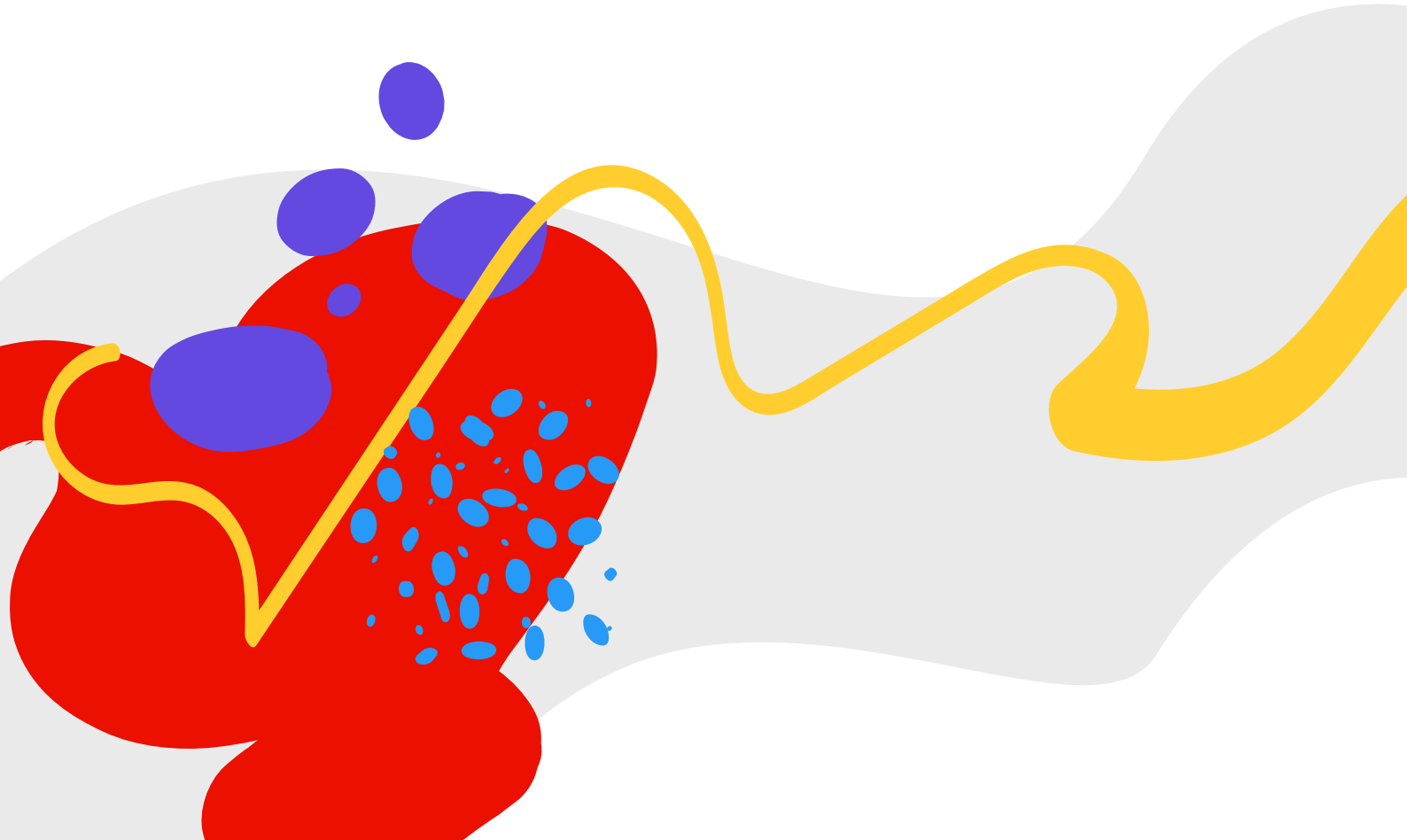
ホワイトペーパー

アドビ運用セキュリティの概要



目次



はじめに

パブリッククラウドやプライベートクラウドを含むクラウドフットプリントは様々なプロバイダーに散在しているため、Adobe®マルチクラウド戦略には、製品チームとサービスチームがすぐに利用できる、一貫性のある反復可能なガードレールが必要です。そのため、アドビの専任の運用セキュリティチームは、継続的に進化するクラウドインフラストラクチャ運用において、大規模なクラウドリソースの保護と、お客様のアプリケーションとデータの安全性とセキュリティの確保を支援することに重点を置いています。

このホワイトペーパーでは、アドビのセキュアクラウド運用戦略について説明するほか、製品開発者とエンジニアがセキュリティ体制を改善し、アドビとお客様の両方のリスクを軽減し、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ために開発したプロセスとツールについて説明します。

アドビのセキュアクラウド運用戦略

アドビは、クラウドプロセスの中核にセキュリティを組み込むことで、複雑なセキュリティ環境で生じる可能性のある潜在的な問題を未然に防いでいます。アドビのクラウドフットプリントは拡大を続けており、マルチクラウド環境や、コンテナ、オーケストレーターなどの新興テクノロジーを使用しています。標準の構成とポリシー、自動化ツールを使用することで、ヒューマンエラーが減り、インフラストラクチャ全体の複数のレイヤーが潜在的な弱点から保護されていることをお客様に保証できます。自動化によるセキュリティの拡張と、セキュリティ体制の定期的なモニタリング、四半期ごとのコンプライアンスレビューにより、アドビはセキュリティドリフトやその他の問題が重大になる前に検出できます。

開発者が専門分野に集中し、偶発的なセキュリティミスを回避できるように、クラウドにデプロイするすべてのサービスに適用する標準の構成とセキュリティポリシーを作成しました。開発ライフサイクルの初期段階にセキュリティコントロールを組み込むことで、アドビは設計からデプロイまでのサービスのセキュリティ体制を強化するだけでなく、修復がより困難になる開発の後期段階でセキュリティホールが発生するリスクを減らすことができます。セキュリティコントロールとクラウドセキュリティポリシーの自動適用により、アドビ全体のセキュリティ体制が向上するとともに、お客様のセキュリティがアドビの最優先事項であることを保証できます。

アドビ運用セキュリティスタック（OSS）

アドビの専任の運用セキュリティチームによって開発されたアドビ運用セキュリティスタック（OSS）は、セキュリティのベストプラクティスを念頭に置いてアドビの製品やサービスを設計するための統合ツールセットです。アドビのマルチクラウドセキュリティのニーズを考慮し、Adobe OSSは標準化と予防という2つの基本原則にもとづいています。Adobe OSSには継続的なモニタリングとワークフローソリューションの標準化されたセットが含まれており、サービスチームはセキュリティを念頭に置いてプライベートクラウドとパブリッククラウドの環境を一から設計でき、セキュリティリスクを未然に防ぐことができます。

様々なクラウドリソースで動作するAdobe OSSは、大規模なセキュリティと組織全体に対して標準化された機能を提供し、アドビのセキュリティ、監査、コンプライアンスの各チームが運用環境のセキュリティを確認するのに役立ちます。アドビは、製品チームとサービスチームが同じツールとプロセスを使用することで、セキュリティエラーを予防し、労力をかけずにアプリケーションがセキュリティソリューションに適応できるようにします。

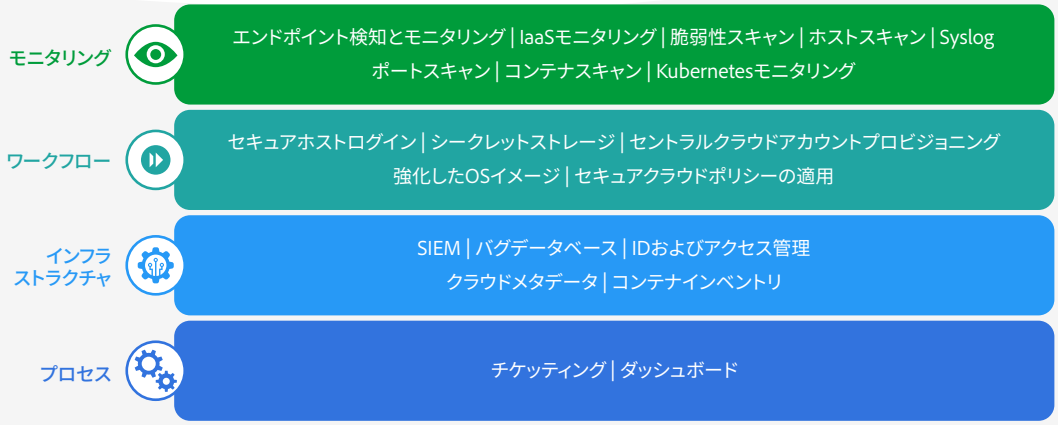


図1：アドビ運用セキュリティスタック（OSS）

安全な選択を既定の選択にすることを目的として、Adobe OSSには4つの異なるレイヤーが含まれています。各レイヤーには、アドビのどの製品チームでも活用できる幅広い一般的なツールとサービスが含まれており、目まぐるしく変化するセキュリティのベストプラクティスを常に把握することができます。

モニタリング

モニタリングレイヤーには、アドビのすべてのクラウド環境および地域のログと構成データを一元的なデータウェアハウスに取り込むためのツールが含まれています。取り込みが完了すると、アドビのセキュリティチームとコンプライアンスチーム、およびAdobe Security Operations Center（SOC）がこのデータを分析し、セキュリティドリフトの測定とセキュリティギャップの検出に役立てることができます。ギャップは、セキュリティチームによるデータの手動レビューまたはセキュリティ自動検出ツールによって検出される場合があります。

また、アドビのセキュリティチームは脆弱性の検出を支援するために、アプリケーションとネットワークの観点から、クラウド環境全体のホストとコンテナのスキャンを定期的に実施しています。このような脆弱性スキャンと侵入テストによって見つかった脆弱性については、評価と優先付けがおこなわれ、必要な場合には修復計画への割り当てがおこなわれます。

Adobe OSSのモニタリングレイヤーには、次のツールが含まれています。

- **エンドポイント検出および応答** — CrowdStrike Falconは、アドビのすべてのエンドポイント（サーバーを含む）にインストールされている軽量の次世代エンドポイント検出および応答（EDR）エージェントです。リアルタイムの継続的なモニタリングと収集によってデータとシステムを保護し、脅威を迅速に特定して対応できるようにします。
- **IaaSモニタリング** — MAVLinkはアドビが開発したパブリッククラウドデータ収集ツールで、Amazon Web Services（AWS）やMicrosoft Azure APIに照会してログや環境構成データを取得し、その情報をSplunkデータウェアハウスに取り込みます。開発者がMAVLinkを使用することで、アドビのセキュリティエンジニアリングチームはセキュリティの観点からパブリッククラウドの状態を一度に確認できるようになります。また、アドビの内部監査およびコンプライアンスチームは、このデータを使用して、AWSとAzureの両方のセキュリティ基準の様々な要素に準拠しているかどうかを判断できます。
- **脆弱性スキャン** — 商用および社内開発の様々なツールを使用して、アドビのデータセンターとクラウド全体を定期的にスキャンし、潜在的な脆弱性が発生する前に特定します。
- **ホストスキャン** — Hubbleは、社内で開発され外部コミュニティにオープンソースで提供されている（英語）、モジュール化されたPythonベースのセキュリティコンプライアンスフレームワークです。これを使用して、アドビは次の3つのアクティビティを実行します。
  - 監査 — Center for Internet Security（CIS）基準にもとづいて、ホストシステムをポリシーファイルと照合
  - クエリ — osqueryを介してシステム情報を収集し、侵入を検出
  - ファイルの整合性 — キーディレクトリ内のファイルの変更をトラック
- **Syslog** — アドビは様々なマシンからシステムログとイベントメッセージを収集し、モニタリングとレビューのためにSplunkに保存します。

- **ポートスキャン** — 数十万のアドビのIPアドレスを継続的にスキャンし、最初の露出から修復までの時間枠を短縮します。nmapスキャンパイプラインを使用すると、チームは境界ポートの露出をすばやく検出できます。

- **コンテナスキャン** — アドビはビルド時と実行時の両方で、既知のCVE（Common Vulnerabilities and Exposures）のコンテナイメージを登録およびスキャンします。スキャンはSplunkにアップロードされ、チームは修復が必要な問題についてJiraチケットを受け取ります。

- **Kubernetesのモニタリング** — アドビのセキュリティエンジニアは、Kubernetesクラスターをモニターするために設計された社内セキュリティツールを使用して、事前に定義された時間にクラスターの読み取り専用の構成スナップショットを取得し、セキュリティギャップに対するカスタム評価を実行できます。その後、調査結果をSplunkにプッシュして分析とチケット発行をおこないます。

ワークフロー

Adobe OSSのワークフローレイヤーは、製品開発者やエンジニアがアドビ製品と同社のインフラストラクチャにエンドツーエンドのセキュリティを提供するためのツールで構成されています。チームが効率的にセキュリティポリシーを実装できるように、ワークフローレイヤーで提供されているツールを使用すると、次のようなセキュアな運用を簡単に実行できます。

- **セキュアホストログイン** — 資格情報とアクセスを一元管理することで、多要素認証（MFA）ポリシーと最小権限の原則を適用し、アドビがクラウド仮想マシンを厳密に管理できるようになります。また、すべての管理セッションを監査目的でログに記録します。

- **シークレットストレージ** — アドビは、主要なサードパーティ製のSecure Vault製品を使用して、トークン、パスワード、証明書、APIキー、その他のシークレットへのアクセスを保護、保存し、厳密に制御します。

- **セントラルクラウドアカウントプロビジョニング** — アドビのクラウドフットプリントの管理とガバナンスを効率化するために、製品チームはセントラルサービスを通じてクラウドアカウントを作成および管理できるため、アドビのガバナンスチームはクラウドアカウントの課金をより簡単に管理し、セキュリティポリシーと運用ポリシーを一元的に適用できます。クラウドアカウントメタデータの信頼できる唯一の情報源は、クラウドフットプリントのサイズとセキュリティ体制を理解するために不可欠であり、一元的なアカウントプロビジョニングにより、アカウントの正しい所有権とその意図された目的を理解できます。

- **強化したオペレーティングシステムイメージ** — Center for Internet Security（CIS）ベンチマークに準拠し、CIS承認のセキュリティ更新プログラムと最新のセキュリティツールの両方を適用する一元的な強化したイメージを提供することで、アドビはすべての製品チームに安全ですぐに使用できるエクスペリエンスを提供します。イメージは、イメージファクトリと呼ばれる社内開発アプリケーションに格納され、エンジニアリングチーム用にリリースされる前に社内セキュリティツールによってスキャンされます。さらに、製品チームはImage Factory APIを使用して、最新のマシンイメージをビルドパイプラインに直接統合できます。

- **安全なクラウドポリシーの適用** — ほとんどのクラウドサービスプロバイダーはデフォルトのセキュアポリシーを提供しますが、アドビは、社内で開発された補完的なツールを使用して、ポリシーの適用と修復を自動化するだけでなく、偶発的なセキュリティドリフトや、クラウドにデプロイされる安全でないサービスに対して追加の保護レイヤーを提供します。このツールは、Azure Policy、AWS Service Control Policy、AWS Config Rulesなどのクラウドネイティブサービスを使用して、すべてのアドビパブリッククラウドアカウントでポリシーとリソースの両方のコンプライアンス要件を適用します。パブリッククラウドアカウント内の非準拠リソースは、適切なポリシーアクションを自動的にトリガーします。その後、アクションがログに記録され、影響を受けたチームに通知されるため、チームは修復イベントをトリガーしたものを特定できます。

アドビのポリシーでは、よくある誤設定から保護するために、攻撃者が最も頻繁に使用する侵害手段を含むカテゴリに焦点を当てています。

- クラウドIDと権限
- データのプライバシーと整合性
- ネットワークエンドポイントの露出
- DNSの整合性

また、アドビのクラウドポリシー運用モデルでは、プロビジョニング時にアクティブなすべてのポリシーは新しいアカウントに含まれます。アドビが新しいポリシーをリリースすると、自動適用プロセスによって、既存のアカウントが新しいポリシーに準拠するように強制されます。新しいポリシーをリリースした後の適用プロセスを迅速化するために、リリース後のベーキング期間（約30日）後にアカウントを自動適用します。非準拠のアカウントは、アカウントを準拠させる期限を含め、修正のために自動的にチケットが発行されます。

自動適用により、開発者はポリシーに準拠するためにより高いレベルの作業に集中できる一方で、プロセスによってポリシー自体の適用が保証されます。自動化されたプロセスは、定期的に新しく準拠したアカウントをチェックし、ポリシーを自動的に適用します。

インフラストラクチャ

定期的に更新されるリッチなメタデータは、Adobe OSSのインフラストラクチャレイヤーの重要なコンポーネントであり、モニタリングレイヤーとワークフローレイヤーの基盤となります。Adobe OSSはこのメタデータを使用して、検出されたセキュリティギャップを、問題のあるクラウドリソースを所有するチームに自動的に割り当てることができます。インフラストラクチャレイヤー内のその他のツールとして、次のものがあります。

- **セキュリティ情報とイベント管理（Security Information and Event Management／SIEM）** — Adobe SOCは、モニタリングレイヤーで収集された集約ログデータをSplunkを使用して検索、モニター、視覚化、分析することで、セキュリティ関連のイベントやインシデントについてより深く分析できます。

- **バグデータベース** — 唯一の情報源を提供できるよう、アドビは説明責任とトラッキングのためにチケット自動発行によってJiraのバグを記録しています。
- **IDおよびアクセス管理（IAM）** — アドビは、Microsoft Active Directoryを他の標準ツールと組み合わせて使用し、認証を管理しています。
- **クラウドメタデータ** — アドビは、すべてのパブリッククラウドアカウントのメタデータをトラックおよび監査し、四半期ごとにこのデータを監査して、アカウントのセキュリティとポリシーのガバナンスの確保に役立てています。クラウドメタデータポータルは、製品チームとセキュリティチームが規定のワークフローに従って新しいクラウドアカウントを追加するのに役立ちます。また、チームはデータウェアハウス内のメタデータにアクセスしてノイズを除去し、誤検出をなくして、重要な脅威を適切に優先付けできます。
- **コンテナインベントリ** — アドビのコンテナエコシステムの豊富なメタデータセットにより、製品チームはコンテナオーケストレーションについてより深いインサイトを得ることができます。さらに、チームはコンテナメタデータを使用して、メトリックをモニターおよび視覚化したり、Kubernetes環境を完全に可視化したりできます。

プロセス

プロセスレイヤーにより、アドビは継続的にセキュリティ体制を改善し、セキュリティのベストプラクティスを実装できます。Adobe OSSの他の3つのレイヤーからのデータは、一元的なデータウェアハウスに格納され、Jira（セキュリティギャップの低減と解決のため）、ダッシュボード（管理の可視性のため）、その他の社内パートナーによって取り込まれます。

アドビは主要業績評価指標（KPI）を使用して、Adobe OSSが社内全体でどれだけ効果的にデプロイされているかを測定し、異常値を特定します。Jiraチケットの自動発行により、強化したセキュリティ状態からサービスが逸脱した場合に製品チームに通知され、エンジニアリングチームと運用チームが構成管理や資産管理など Adobe Common Controls Framework（CCF）（英語）のいくつかの制御ドメインに適合できるようにします。

アドビ運用セキュリティスタック（OSS）の動作

自動化、システムレベルの制御、標準化により、Adobe OSSの各レイヤーは他のレイヤーと協調して動作し、デプロイされたクラウドリソースに対してセキュリティを提供します。

資格情報とアクセスコントロールツールによって、マネージドクラウドサービス全体でIDとアクセス管理ポリシーを統一的に適用でき、ユーザーアクティビティを記録することで、適用ポリシーを改善するための潜在的な領域をより深く把握できます。開発者はその後、イメージファクトリインフラストラクチャからの強化したOSイメージを使用して、セキュア・バイ・デフォルトなクラウドサービスを作成、デプロイ、管理します。

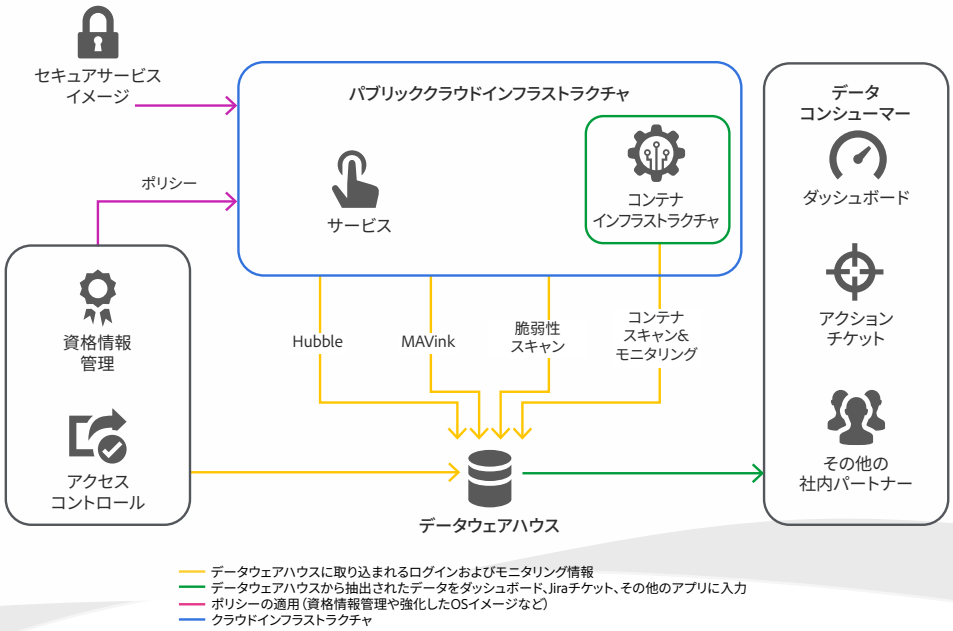


図2：Adobe OSSのデータフロー

デプロイ後、モニタリングツールにより、クラウドまたはコンテナプラットフォームにデプロイされているサービスが継続的に監視され、ログやその他の関連情報が一元的なデータウェアハウスに送信されます。ダッシュボード、Jiraチケット、社内のその他のアプリケーションは、このウェアハウスからデータを抽出して、ユーザー側のアプリケーションにデータを入力します。

まとめ

アドビの運用セキュリティ戦略は、アドビの製品チームとサービスチームに一貫性のある反復可能なガードレールを提供します。それにより、アドビのお客様向け製品がセキュリティを念頭に置いて構築され、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に準拠していることを保証します。セキュリティの自動化と、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るセキュリティ体制の継続的なモニタリングにより、アドビはセキュリティリスクを未然に防ぎ、製品と会社のインフラストラクチャの両方についてエンドツーエンドのセキュリティを維持します。

2/23