Adobe Sign 技術概要

セキュリティ、コンプライアンス、ID 管理、管理方法、文書処理

目次

1: エグゼクティブサマリー
2: アーキテクチャ
4: ID管理
4: 文書の証明
5: セキュリティ
7: コンプライアンス
8: オペレーション
9: ガバナンス
11: 詳細情報

エグゼクティブサマリー

Adobe Sign は信頼性の高い法的効力のある電子サインで、法人向け Document Cloud ソリューションです。エンドツーエンドのデジタル文書エクスペリエンスが可能になります。Adobe Sign を使用すれば、web、モバイルアプリ、自社のエンタープライズシステムからも、デジタル文書の署名プロセスの開始、追跡（トラッキング）、承認、保管（アーカイブ）が容易にできます。Adobe Sign は各地域や業界の規格に数多く準拠しどのデバイスでも利用できます。クラウドベースのサービスであるため、高いセキュリティで以下に示すような大容量の電子サインプロセスを安全に処理できます。

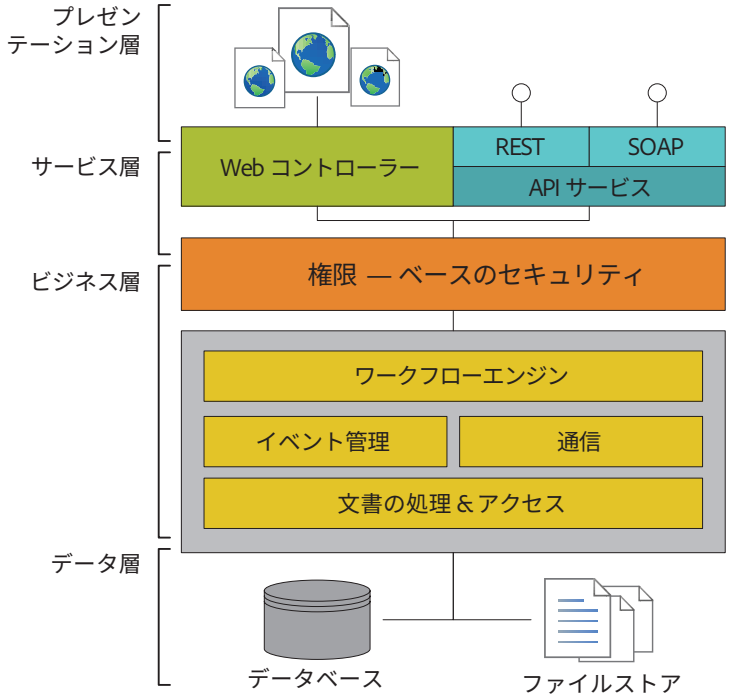
- 権限ベースの認証によるユーザー識別の管理
- 文書の完全性の証明
- 電子サインの検証
- 受信者の受諾または文書受信確認のログ記録
- 監査証跡の保管
- 基幹業務アプリケーションやエンタープライズシステムへの組み込み

Adobe Sign は電子サインと電子署名の両方をサポートしています。電子サインは、デジタル文書やデジタルフォームによる同意や承認を示す方法です。世界の多くの先進国において法的に有効であり、法的強制力があります。一方、電子署名は、証明書ベースのデジタル ID を使用して署名者の同一性を検証し、署名を暗号化された文書と紐付けるという限定的な電子サインの実装方法です。Adobe Sign は、スマートカード、USB トークン、クラウドベースのハードウェアセキュリティモジュール（HSM）などに保存されたデジタル ID に対応しています。また、デスクトップ、web、モバイルのいずれでも、クラウド署名コンソーシアム（Cloud Signature Consortium）仕様によるデジタル ID を使用したオープン標準ベースの署名をサポートしています。

このホワイトペーパーでは、Adobe Sign のアーキテクチャ、セキュリティ、コンプライアンス、ID 管理、文書処理、ネットワーク保護、パフォーマンスのモニタリング、サービス管理、ガバナンス、その他の主要な技術項目の概要を示します。その他、電子サインおよび、電子署名に関する詳しい情報については、アドビの「電子サインおよび電子署名ソリューションで業務プロセスを改革」をご覧ください。

アーキテクチャ

Adobe Sign のアーキテクチャは、パフォーマンスを低下させることなく、大規模なトランザクションを処理できるように設計されています。高い可用性と拡張性を維持するために、Adobe Sign のトランザクションデータはすべて、自動障害回避と復元機能のある複数の分散冗長データベースクラスターに保管されています[1]。次の階層式アーキテクチャの図で、Adobe Sign のコンポーネントと機能の論理区分を示します。



Adobe Sign の論理アーキテクチャ概要

Adobe Sign の各論理層は、広範なツール群によりモニタリングされ、文書の PDF 変換にかかる時間、リソースの利用率などの主なインジケーターが記録されます。Adobe Sign のオペレーションエンジニアは、監視ダッシュボードを使って容易にサービス全体の状態を確認できます。主なインジケーターが、指定したしきい値を超えると、リアルタイムでオペレーションエンジニアに警告が通知されます。問題を回避できない場合は、詳細な診断および分析ログが作成されます。これは、エンジニアが問題を早急に解決し、根本原因に対応して、再発を回避するために役立ちます。

プレゼンテーション層

プレゼンテーション層では、web ユーザーインターフェイス（UI）のほか、署名の必要な文書、最終の承認済み PDF、ワークフローコンポーネントの生成、表示、レンダリングを管理します。

サービス層

サービス層では、クライアントサービスと web サービス API インターフェイス（REST Gateway や SOAP API など）に必須の制御機能を果たします。外部向けシステム web サーバーがブラウザーと API のリクエストを処理し、電子メールサーバーが送受信されるメールのトラフィックを管理します。web サーバーは、Adobe Sign アプリケーションサーバーのビジネス層に、ロードバランサーを使用して複雑な動的リクエストを分配します。また、サービス層 web サーバーには、一般的な web 攻撃を阻止するセキュリティフィルタリングルールとアクセス制御を強化するファイアウォール保護も組み込まれています。

[1] 自動復旧は Amazon Web Services インフラストラクチャに限られます。

ビジネス層

Adobe Sign のビジネス層は、ワークフロー、権限ベースのセキュリティ、文書の変換、イメージングサービス、イベント管理、ログ作成とモニタリング、ファイルアクセスと操作、通信の各機能を果たします。

ワークフローエンジン

Adobe Sign のワークフローエンジンは、文書の署名に必要なすべてのビジネスプロセスと手順を実行し、管理します。ワークフローエンジンは、宣言型 XML ベースの定義言語を使用して、署名または承認プロセスの完了に必要なお客様各社固有のフローおよびイベントシークエンスを実行するための前提条件を記述します。

権限ベースのセキュリティ

Adobe Sign の権限ベースのセキュリティは、どのリソースが利用可能であり、認証されたユーザーまたはアプリケーションがそのリソースで実行できるのはどのオペレーションかを定義、制御、監査します。リソースには、文書、データ、メタデータ、ユーザー情報、レポート、API 形式のあらゆる情報が含まれます。

イベント管理

Adobe Sign のイベント管理は、ワークフロープロセスの各手順において、各ユーザーと文書の関連情報の監査証跡を記録し、保管します。ワークフローで各ステージが発生するたびに、Adobe Sign はイベントを生成し、非同期メッセージングシステムにより、適切なシステムリソースにメッセージを配信します。

通信

Adobe Sign では、署名イベント通知に電子メールを使用し、オプションで、サイン入りの承認済み文書をプロセス終了時に配布します。迷惑メールとフィッシング詐欺を防止するために、Adobe Sign では、Domain Keys Identified Mail（DKIM）、Domain-based Message Authentication, Reporting and Conformance（DMARC）、Sender Policy Framework（SPF）による電子メールの認証が可能です。

文書の処理とアクセス

パフォーマンスを向上させるために、Adobe Sign の文書処理エンジンは完全なステートレス機能を備えており、様々なファイル形式の PDF への変換、ファイルの暗号化と復号化、web ブラウザー表示用の画像のラスタライズが可能です。文書処理アクションについては、非同期でキューベースのメッセージングシステムを使用してシステムリソース間の通信を実行します。また、すべての文書処理とネットワーク接続ストレージ（NAS）へのアクセスがバックグラウンドで実行されるため、ユーザーには、ワークフローの各段階で Adobe Sign の各手順が瞬時に処理されるように見えます。

データ層

データ層は、トランザクションデータベースアクセス、非同期メッセージングシステムデータベース、文書ストアの機能を果たします。データアクセス層に保管されるトランザクションデータには、対象となるオリジナルの文書、署名プロセス中に生成された中間文書バージョン、文書のメタデータ、ユーザー、イベント、Adobe Sign で処理された最終のサイン済み PDF 文書があります。

インテグレーション

Adobe Sign は広範なビジネスアプリケーションおよびエンタープライズシステムとのターンキー統合が可能です。これには、Salesforce、Apttus、Workday、Ariba のほか、SharePoint、Dynamics、Office アプリケーションなどの Microsoft 製品も含まれます。また、Adobe Sign では包括的 API セットを使用できるため、各社独自のビジネスシステムや自社 web サイトとの、セキュア HTTPS、SOAP、REST web サービスを介したカスタム統合が可能です。Adobe Sign でサポートされる統合の一覧については、代表的な業務システムとの連携ページをご覧ください。

ID 管理

Adobe Sign はロールベースのモデルを使用して、Adobe Sign システム全域の認証、承認、アクセス制御による ID 管理をおこなっています。権限ベースのセキュリティと認証プロセスは、組織の Adobe Sign 管理者が定義し、有効にします。Adobe Sign では、以下の一般的なユーザーロールを定義します。

- **送信者** — 管理者から特定の Adobe Sign アクセス権を付与されたライセンスを持つユーザー。文書の署名ワークフローを作成し、署名、承認、参照用に文書を送信することができます。
- **署名者** — 特定の文書に署名するために送信者からアクセス権を与えられた確認済みユーザー。デフォルトでは、署名する文書への一意の URL が電子メールで署名者に送信されます。この URL は、各トランザクションに固有の専用識別子で構成されます。
- **承認者** — 特定の文書を承認するために送信者からアクセス権を与えられた確認済みユーザー。
- **その他** — 文書または監査証跡を表示するために送信者から限定アクセス権を与えられた確認済みユーザー。

ユーザー認証

Adobe Sign は、単一要素認証と多要素認証の両方に、その他のユーザー ID 検証方法を加えた複数の方式でユーザー ID を認証します。通常、ライセンスを持つユーザーは、Adobe ID などの認証 ID に対応する確認済み電子メールアドレスとパスワードを使用して Adobe Sign にログインします。管理者は、パスワードの強度と複雑さ、変更頻度、過去のパスワードとの比較、ロックアウトポリシー（ログイン更新期限など）も必要に応じて設定できます。

Adobe Sign への基本認証は、対象者に電子メールでリクエストを送信する方法でおこないます。ほとんどのユーザーは、1 つの電子メールアカウントを 1 人で使用しているため、これが第 1 レベルの認証と考えられます。第 1 レベルの認証は、署名者、承認者、その他のユーザータイプでよく使用されます。セキュリティを強化し、悪意のある個人によるシステムのスプーフィングを阻止するために、対応地域では、電話、SMS テキスト、ナレッジベース認証（KBA）などの多要素認証方式を追加することもできます。

Adobe Sign では、以下のタイプのユーザー認証をサポートしています。

- **Adobe Sign ID** — ライセンスを持つユーザーが Adobe Sign アカウントに安全にログインするために使用する、確認済み電子メールアドレスとパスワードの組み合わせ。
- **Adobe ID** — Adobe ID は、ライセンスされたすべての（Adobe Sign を含む）アドビサービスへのアクセスに使用できます。アドビは、通常と異なる不審なアクティビティがないかどうかをすべての Adobe ID で継続的にモニタリングし、セキュリティの潜在的脅威に迅速に対処します。
- **Google ID** — Gmail や G Suite など、Google が認証するユーザー ID。
- **シングルサインオン（SSO）** — さらに厳格なアクセス制御の仕組みを求める企業は、Security Assertion Markup Language（SAML）SSO を有効にし、企業 ID システムを使用して Adobe Sign ユーザーを管理することができます。Adobe Sign は、Okta、OneLogin などの主要な ID 管理ベンダー方式を認識し、統合するよう設定できます。

文書の証明

Adobe Sign は、ワークフローの各ステージでセキュアチェックサムを維持し、文書の整合性と機密性を確認しています。Adobe Sign は、公開鍵方式（PKI）を使用して電子署名で最終の署名済み PDF を証明した後、その文書をすべての参加者に配信します。

電子署名はハッシュアルゴリズムで作成されます。このアルゴリズムは、最終の署名済み PDF 内の特定の固有情報を使用して、16 進数表記の数字と文字からなる固定長の暗号化文字列を出力します。電子署名が、最終のサイン済み PDF の上部に青いバナーと証明バッジとしてグラフィカルに表示され、文書の整合性（下の図を参照）を確認し、証明書が適用された後には文書が改ざんされていないことを証明します。最終の証明済み PDF は、必要に応じて、さらにパスワードで保護することもできます。

Acrobat DC 版 — ブラックバッジ

Acrobat X および XI — ブルーバッジ（バージョン 10、11）

Adobe Sign 文書証明バナーとバッジ

Adobe Sign は、最終の署名済み PDF をロックし、証明するためのキーを生成するために、信頼された認証機関（CA）とタイムスタンプ機関（TSA）が発行した特定の証明書を使用します。一部の環境では、スイス、ブラジル、インドでの場合のように、政府が指定する CA を使用して証明済み文書を発行できるように Adobe Sign を設定できます。最終 PDF の証明に使用した PKI キーは、オンラインでの攻撃や改ざんを防ぐためにハードウェアセキュリティモジュールに保管されます。

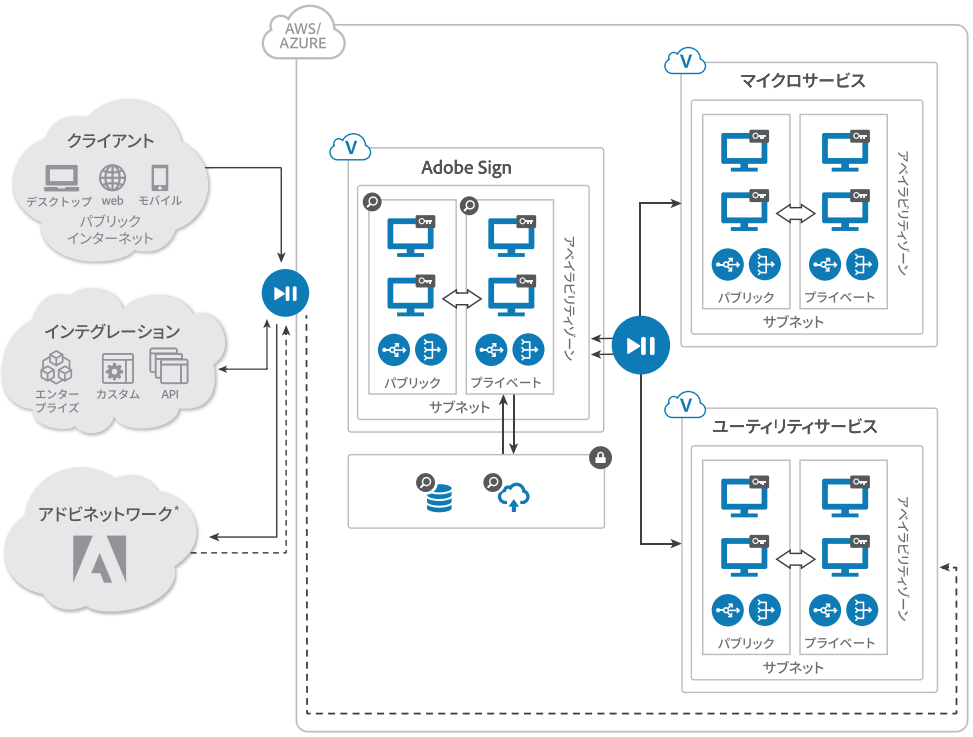
セキュリティ

アドビでは、企業文化、ソフトウェア開発、およびサービスオペレーションプロセスにセキュリティとプライバシー対策が深く根づいています。Adobe Sign では、文書、データ、個人情報を保護するために、業界標準のセキュリティ対策（ID 管理、データの機密保持、文書の整合性）を採用しています。Adobe Sign サービスのインフラストラクチャは、委託先クラウドサービスプロバイダーである Amazon Web Services（AWS）および Microsoft Azure[2] が管理する米国規格協会（ANSI）tier 4 データセンターにあります。Adobe Sign インフラストラクチャはすべて、データセンターアクセス、耐障害性、環境統制、ネットワークセキュリティについて厳格なコントロールを維持しています。承認された、権限のあるアドビの従業員、クラウドサービスプロバイダーの従業員、正規の文書で契約している請負業者以外は、北米、日本、オーストラリア、インドおよび EU 内にある保護されたサイトにアクセスできません。

アドビはセキュリティに対する取り組みの一環として、SOC 2 Type 2、ISO 27001 レポートなどのコンプライアンス認定を定期的に確認するとともに、業界標準の侵入検知システム（IDS）および侵入防止システム（IPS）を使用して、Adobe Sign のあらゆるコンポーネントを頻繁にモニタリングしています。アドビのセキュリティプロセス、コミュニティ活動、Adobe Secure Product Lifecycle について詳しくは、*www.adobe.com/jp/security* をご覧ください。

ネットワークセキュリティアーキテクチャ

外部向けサーバー、クラウドサーバーおよびクライアントアクセスを含めた、Adobe Sign セキュリティアーキテクチャのネットワーク概略図を示します。



凡例

仮想プライベートクラウド（VPC）/ 仮想ネットワーク（VNet）
VM インスタンス
ネットワークアクセス変換（NAT）ゲートウェイ
ID およびアクセス管理（IAM）、マネージドサービス ID（MSI）
Amazon S3/BLOB クラウドストレージ
Elastic Load Balancer
セキュリティグループ
AES 256-bit 暗号化データベース

* ソフトウェアアップデートの配信やAdobe ID管理など他のソフトウェアサービスに使用する、アドビのネットワークへの安全な接続を示します。

[2] 2018 年第 3 四半期に公開予定

外部向けサーバー

web サーバーを含む Adobe Sign サービスのホストネットワークアーキテクチャ内の外部向けシステムがブラウザーと API のリクエストを処理し、電子メールサーバーが電子メール通信の入出トラフィックを管理します。web サーバーはハードウェアロードバランサーを使用して、アプリケーションサーバーに複雑な動的リクエストを分配します。web サーバーには、一般的な web 攻撃を拒否するセキュリティフィルタリングルールとアクセス制御を強化するファイアウォール保護も組み込まれています。

仮想クラウドネットワーク

Adobe Sign ネットワークのセキュリティアーキテクチャは、いくつかの仮想クラウドネットワークを使用しています。AWS 環境では仮想プライベートクラウド（VPC）、Microsoft Azure では仮想ネットワーク（VNet）と呼ばれるものです。VPC/VNet は論理的に隔離されたネットワークであり、Adobe Sign の他のインスタンスからは分離され、アクセスできません。各 VPC/VNet 内に一連の IP アドレスを含むサブネットがあります。サブネットにはパブリックとプライベートがあります。パブリックサブネットはインターネットに接続されますが、プライベートサブネットは接続されません。Adobe Sign サービスでは VPC/VNet を以下の方法で使用します。

- Adobe Sign のプライベートおよびパブリック VPC/VNet ネットワークが Adobe Sign サービスのビジネスプロセスに対応します。Adobe Sign のビジネスロジックは、スケーラブルでセキュアな仮想クラウドサーバーで実行するプライベートサブネットで管理します。このプライベートサブネットにはパブリックサブネットを発信元とする接続を経由した場合にのみアクセス可能です。
- マイクロサービス VPC/VNet は区分化されたコンテナアーキテクチャを使用することで、基盤となるシステムインフラストラクチャに影響を及ぼさず、非常に高い拡張性と性能を持つ「内部のみの」サービスの提供が可能となります。Adobe Sign では、電子署名のクラウド署名コンソーシアム（Cloud Signature Consortium）統合、署名検証、署名画像の背景削除などの特定のアクションでマイクロサービスを使用します。
- ユーティリティサービス VPC/VNet はイベントモニタリングとログ作成およびサービスアーティファクトの複製リポジトリを管理します。

ネットワークアーキテクチャから見ると、アベイラビリティゾーン（AZ）VPC/VNet インスタンス内にあります。物理的には各 AZ に複数の異なる冗長データセンターが存在します。すべてのデータがすべてのデータセンターで複製され、各データセンター内の複数のサーバーでも複製されます。

VPC/VNet インスタンスはセキュリティグループにロックダウンされています。仮想ファイアウォールと同様に、セキュリティグループではアドビはさらに細かく VPC/VNet インスタンスの送受信トラフィックをコントロールできます。そのため、検証されたユーザーのみが権限のあるアクションを実行できるように確実に制限できます。また、Adobe Sign ネットワークセキュリティアーキテクチャでは主要なロケーションに侵入検知 / 保護センサーを設置し、サービス全体でシステムの整合性と可視性を確保しています。

クライアントアクセス

Adobe Sign サービスには、ブラウザー、モバイルアプリ、電子メール経由など、様々なクライアントエンドポイントからアクセスできます。クライアントをその指定地域の Adobe Sign に接続すると、インターネットゲートウェイを通じていくつかの VPC/VNet に接続されます。クライアント接続は、AES 128 ビット以上で暗号化された TLS1.2（2018 年 6 月現在）による HTTPS 接続でおこないます。

ネットワーク保護

Adobe Sign のサービスプロバイダーはすべて、ネットワークデバイスを使用して、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をモニタリングし、制御しています。これらのファイアウォールとその他の境界デバイスは、ルールセット、アクセスコントロールリスト（ACL）、設定により、特定の情報システムサービスに情報が流れるようにします。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、自動プロセスで常に最新を維持しています。

両方のプロバイダーでは、様々な自動モニタリングシステムも使用して、高水準のサービスパフォーマンスと可用性を強化しています。モニタリングツールは、ネットワーク通信ポイントの出入口で、異常や不正なアクティブティ、状態を検出し、以下のような従来型ネットワークセキュリティの脆弱性を保護するために役立ちます。

- 分散サービス妨害（DDoS）攻撃
- 中間者（MITM）攻撃
- インターネットプロトコル（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

アドビでは、Secure Shell（SSH）および Secure Sockets Layer（SSL）を使用して、Document Cloud サービスのホスティングインフラストラクチャを管理するためのセキュアな接続を確立しています。

暗号化

Adobe Sign は PCI DSS 準拠の暗号アルゴリズムのみを使用して、保存中の文書とアセットを AES 256 ビットで暗号化しています。また、HTTPS TLS v1.2（および旧バージョン）のサポートにより、転送中のデータを保護します。保存中の文書は暗号化されたストレージコンテナで保護され、適切な権限ベースのセキュリティアクセス権でプライベートサブネットのアプリケーションデータアクセス層を介してのみアクセスできます。さらに、Adobe Sign の送信者がプライベートパスワードを設定して、文書の保護を強化することもできます。

文書暗号化キーは、Adobe Key Management Standard（アドビキー管理基準）に従い、アクセス権が限定された安全な環境に保管され、必要に応じてローテーションされます。各委託先ホスティングでは強力な多要素暗号化を採用しています。例えば、オブジェクトごとにユニークキーで暗号化するほか、さらにキー自体もマスターキーで暗号化して定期的にローテーションするなどをおこなっています。

コンプライアンス

Adobe Sign は、どこのどのデバイスからでも、確認済み署名者が電子文書を操作できるように設計されたグローバル電子サインソリューションであるため、多くの業界規格や標準規格のコンプライアンス要件を満たしています。または、満たすように設定できます。文書、データ、ワークフローについては各社がコントロールでき、EU の一般データ保護規則（GDPR）など、各自治体や地域の規則に従う最も良い方法を選択できます。アドビのプライバシーへの対応については、*www.adobe.com/jp/privacy* をご確認ください。特定地域の電子サインに関する法律については、電子サイン関連法グローバルガイド：法律とその強制力に関する国別のまとめをご覧ください。

ISO 27001

ISO 27001 は、国際標準化機構（ISO）および国際電気標準会議（IEC）によって発行されている規格です。情報セキュリティ管理システム（ISMS）に関する要件を規定し、システムの監査は認定された独立認証機関によっておこなわれます。Adobe Sign は、ISO 27001: 2013 の認定を受けています。

SOC

SOC（Service Organization Controls）は、セキュリティ、可用性、処理の整合性、機密性、プライバシーに関する一連の IT コントロール（Type 2）です。Adobe Sign は、SOC 2 Type 2（セキュリティと可用性）認証を受けています。

PCI DSS

決済カード業界データセキュリティ基準（PCI DSS）は、主要なカードスキームによるブランド化されたクレジットカードを処理する組織向けに規定された、機密情報のセキュリティ標準です。カード所有者データの管理機能を強化し、不正行為を削減することを目的としています。Adobe Document Cloud に含まれる Adobe Sign は、PCI DSS に準拠する加盟店 / サービスプロバイダーの認定を受けています。

FedRAMP

米国連邦リスク・認証管理プログラム（FedRAMP）は、政府機関が使用するクラウド製品やクラウドサービスのセキュリティ評価、権限付与、継続的なモニタリングについて、標準的なアプローチを策定したものです。FedRAMP Tailored は、Low-Impact Software-as-a-Service（LI-SaaS）システムを使用するクラウドサービスプロバイダー向けの基準です。Adobe Sign は、FedRAMP Tailored 認定済みです。

SAFE-BioPharma

SAFE-BioPharma® は、製薬業界、バイオテクノロジー業界、医療業界の電子商取引において、世界的に保証レベルの高い認証をおこなえるように、業界とその規制機関が策定した電子認証と電子署名の標準規格です。Adobe Sign は、SAFE-BioPharma の認定を受けています。

HIPAA[3]

米国医療保険の携行性と責任に関する法律（HIPAA）では、秘密にすべき患者情報の保護を目的として、電子的医療情報処理の基準を定めています。米国保健福祉省（HHS）によって示された対象事業者の定義に合致し、アドビと提携事業者契約（BAA）を締結している組織が使用する場合、Adobe Sign は HIPAA 準拠となります。

21 CFR Part 11[3]

Code of Federal Regulations, Title 21, Part 11: Electronic Records; Electronic Signatures（21 CFR Part 11）では、電子記録および電子署名に対する米国食品医薬品局（FDA）の規制を定めています。

GLBA[3]

米国のグラム・リーチ・ブライリー法（GLBA）では、顧客の個人情報を保護するために、金融機関に対する規制が定めています。Adobe Sign は、GLBA に準拠しています。

FERPA[3]

米国家庭教育の権利とプライバシーに関する法（FERPA）は、米国の学生の教育記録と名簿情報の秘密保持を目的としています。FERPA ガイドラインのもと、Adobe Sign は契約上の合意によって「学校関係者」として規制対象の学生データの処理機能を果たすことができるため、教育機関は FERPA の義務を遵守することができます。

オペレーション

パフォーマンスのモニタリングなど、標準のオペレーション対策を実施し、Adobe Sign サービスの状態を管理しています。

パフォーマンスのモニタリング

アドビは Adobe Sign サービスの良好な状態を維持するため、可用性、ボリューム、パフォーマンスのチェックなどの詳細なモニタリング活動を実施しています。状態のチェックはすべて、予防措置に必要な先制インジケーターである、定義済みの測定可能なしきい値に基づいています。状態チェックのしきい値とプロセスは、定期的に見直されます。

また、サーバー側で顧客行動のログを記録し、サービスの停止、顧客に固有の問題、報告されたバグを診断します。ログには、パスワードや名前などの個人を識別できる情報（PII）は含まれません。ただし、Adobe ID がある場合は記録されます。アドビテクニカルサポート認定担当者、主要なエンジニア、選定された開発者にのみ、起こり得る問題を診断するためにログへのアクセス権が与えられます。

サービス管理

アドビは、変更、インシデント、問題の管理など、業界標準のサービス管理コンセプトを活用しています。また、アドビのプロセスと制御は、多数のコンプライアンスフレームワークをサポートするように設計されています。

変更管理

アドビは、標準に準拠した包括的変更管理プロセスを実施しており、Adobe Sign サービスの変更による影響とメリットの可能性を査定する厳重な検査を実施しています。ほとんどの変更はサービスに影響を及ぼしませんが、まれに例外があります。例えば、災害復旧手順の年次点検は、顧客体験に影響を及ぼす場合があります。そのような特殊なケースについては、アドビが、影響する可能性のある Adobe Sign ユーザーに事前に通知します。

インシデント管理

万一サービス停止が発生した場合は、Adobe Sign オペレーションチームがアドビのインシデント管理プロセスを開始します。このプロセスが開始されると、オンコールエンジニアがオンラインコラボレーションツールにより呼び出され、優先順位を決定し、原因を突きとめ、問題の解決に当たります。また、インシデント管理プロセスには、インシデントの解決につながる一連のイベントのデータのほか、サービスレベル契約（SLA）への影響の評価に使用するタイミングと影響度の情報を取得する規定も含まれます。未解決の事項は問題管理チームに渡され、プロセスが続行されます。

問題管理

アドビのインシデント管理プロセスの一環として、インシデントの原因究明と防止措置の提案を目的とした、正式な事後問題管理会議が予定されます。サービス停止中には他の問題が偶発的に発見される可能性があるため、それらについて、問題管理プロセスを使用して対応します。また、サーバー停止の原因の一端となったものや、将来の停止の原因となるリスクが高いものなど、あらゆる脆弱性にも対応します。問題管理プロセスの結果、インシデントの分析とまとめ、根本的原因の詳細な説明、影響分析、および必要な是正措置が得られ、問題の完全解決に役立ちます。

[3] アドビの GLBA 対応サービス、FERPA 対応サービス、FDA 21 CFR Part 11 準拠サービス、HIPAA 準拠サービスとは、サービスプロバイダーの利用に関する法的義務を顧客が遵守しやすくなるよう支援するものです。法的義務を確実に遵守すること、アドビのサービスがコンプライアンスに関する自社ニーズに合っていること、そのサービスのセキュリティを自社で適切に保護することについては、顧客が最終的な責任を負うものとします。

担当者

アドビは、世界各地に専任テクニカルオペレーションエンジニアチームを分散させており、通常の営業時間内の対応をリレーする方式を取っています。このグローバルサポートチームはオンコール対応を提供し、一刻も早くサービスを再開できるように、法人向けアドビインシデント対応チームを補佐します。アドビのオンコールテクニカルオペレーションエンジニアの主要な拠点は、米国とインドのノイダです。

ガバナンス

新たな脆弱性のモニタリング、潜在的脅威の軽減のいずれに対しても、アドビは業界標準の対策を実施し、Adobe Sign のリスク管理、軽減、インシデント解決プロセスが迅速かつ徹底的に実行されるようにしています。

リスク管理

アドビは、リスクと脆弱性の管理、インシデント対応、軽減、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。継続的に脅威の動向をモニタリングし、世界中のセキュリティ専門家と知識を共有して、インシデントの迅速な解決に取り組んでいます。すべての Adobe Sign インフラストラクチャプロバイダーは、いくつかのツールを用いて、ネットワーク全体のトラフィック、その他の潜在的脅威となる異常、サービス妨害攻撃（DoS）などを積極的に検出、評価、トレースしています。

侵入テスト

アドビは、承認したサードパーティ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。アドビは、サードパーティ企業から提出されたレポートに基づいて脆弱性を文書化し、深刻度と優先度を評価した上で、Adobe Sign サービスのリスク軽減戦略または改善計画を作成します。

セキュリティチームは Adobe Sign の各リリースに先立ち、サービスのリスク評価を実施して、ファイアウォール、ロードバランサー、サーバーハードウェアから、アプリケーションレベルの脆弱性まで、ネットワーク設定に安全性の問題があるかどうかを調べます。リスク評価は、ネットワークトポロジー、インフラストラクチャ、および Adobe Sign サービスのセキュリティに精通した、高度な訓練を受けたセキュリティスタッフが実施します。セキュリティタッチポイントには、脅威モデリングの実施のほか、脆弱性のスキャニング、アプリケーションの静的 / 動的分析が含まれます。

脅威の軽減

日々生み出される新たな脆弱性と脅威を軽減するため、アドビは、US-CERT、Bugtraq、SANS などの業界規模での脆弱性アナウンスリストに加え、主要なセキュリティベンダーが発行するセキュリティ警告リストも利用しています。Adobe Sign などのクラウドベースサービスでは、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。

Adobe Sign のリスクとなる重大な脆弱性がアナウンスされると、Adobe Document Cloud 組織内のすべての担当チームに通知され、各チームが協力して軽減策を講じます。また、Adobe Sign サービス内でインシデントが発生した場合は、インシデント対応チームと開発チームが連携して、以下の例に示すような業界標準の対策を講じてインシデントを特定、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デプロイ
- アクティビティのモニタリングと解決の確認

Adobe Sign チームは、インシデントのフォレンジック分析のため、影響を受けるマシンの完全なイメージ（またはメモリダンプ）、証拠の保全、分析過程の管理記録を確保します。

データの分離 / 隔離

すべてのクラウドサービスパートナーは、テナントを分離する強力なセキュリティとコントロール機能を使用して、マルチテナントサービス内にある Adobe Sign のお客様データを隔離しています。セキュリティ管理プロセス、その他のセキュリティコントロールも併用して、お客様データの適切な分離と保護をおこなっています。

詳細情報

ソリューションの詳細：*www.adobe.com/go/adobesign-jp*

電子サインの法的効力：
https://acrobat.adobe.com/jp/ja/sign/capabilities/electronic-signature-legality.html

アドビのセキュリティ：*www.adobe.com/jp/security*

Adobe Trust Center：*www.adobe.com/jp/trust.html*

Microsoft Azure のセキュリティ：*azure.microsoft.com/ja-jp/services/security-center*

Amazon Web Services のセキュリティ：*https://aws.amazon.com/jp/security*

Adobe Sign のヘルプ /SAML を使用したシングルサインオンの有効化：
https://helpx.adobe.com/jp/sign/help/SAML_Configuration.html

Adobe

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

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

© 2018 Adobe Systems Incorporated. All rights reserved. Printed in Japan.

6/18