Adobe Signのセキュリティ概要

目次

アドビのセキュリティ

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重要な課題です。ソフトウェア開発・運用のプロセスおよびツールに徹底した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厳密なセキュリティ基準に従ってインシデントの防止、検知、および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、および他の業界団体と協力して、最新の脅威や脆弱性を把握し、提供する製品およびサービスに常に高度なセキュリティ技術を組み込んでいます。

このホワイトペーパーでは、Adobe Signとユーザー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 Signについて

Adobe Signを使用すれば、既存の紙の署名をおこなうようなワークフローをデジタル化し、完全なデジタルエクスペリエンスへと移行することができます。クラウドでのシンプルな署名から、高度なコンプライアンス基準を満たした電子サインまで、あらゆるタイプの署名ワークフローに対応します。Adobe Signを利用すると、送信、署名、トラック、署名プロセス管理が、ブラウザーやモバイルデバイスでいつでもどこでも簡単にできます。Adobe Signのシステム連携プラグインとAPIにより、組織の電子サインワークフローを、エンタープライズサービスや文書管理システム、Microsoft 365などの生産性を向上する一般的なクラウドソリューションに組み込むこともできます。

Adobe Signは、署名者の本人確認やセキュリティを強化するために証明書ベースの電子署名をサポートするなど、各地域の規格や業界規格、標準規格に数多く準拠しています。堅牢なクラウドベースのサービスであるため、以下に示すような大容量のオンライン署名プロセスを安全に処理できます。

- ユーザーの識別、認証、アクセス制御の管理
- 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

また、Adobe Signのクラウド署名は、クラウド署名コンソーシアム（CSC）の標準統合規格への準拠が認められており、トラストサービスプロバイダー（TSP）によるデジタル証明書（英語）にもとづいたリモート電子署名を実現します。

世界各地域の電子サインの法的効力については、Adobe Trust Centerの国／地域ごとの電子サインの法的効力（英語）をご覧ください。Adobe Signについて詳しくは、www.adobe.com/go/adobesign-jpをご覧ください。

Adobe Signソリューションのアーキテクチャ

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。

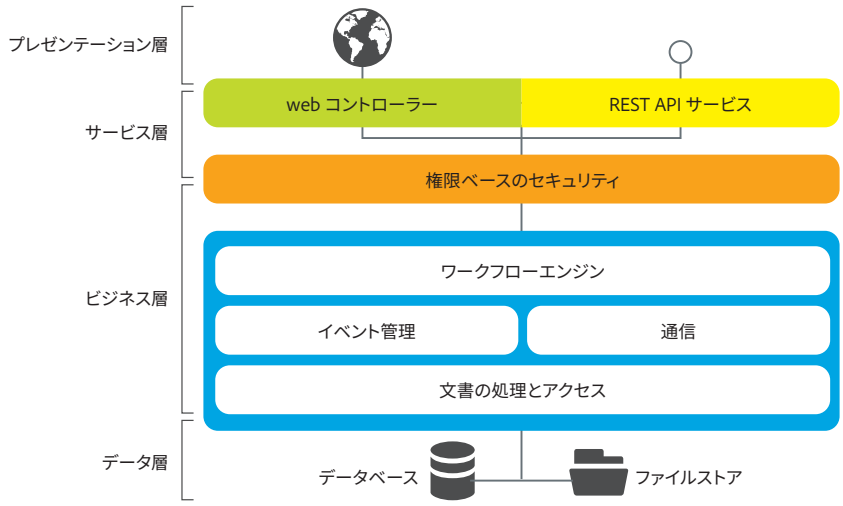

図1：Adobe Signソリューションのアーキテクチャ

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、署名の収集やその他のワークフロー、最終の承認済みPDFに必要な文書の生成と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REST APIサービスに必須の制御機能を果たします。外部向けシステムの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、ビジネス層のAdobe Signアプリケーションサーバーに、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、サービス層のwebサーバーでは、一般的なweb攻撃を阻止するための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を組み込んでいます。

[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、以下の各機能を果たします。

- **ワークフローエンジン** — 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** — 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制御し、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。
- **文書の処理とアクセス** — 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から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。
- **イベント管理** — 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。Adobe Signはワークフローの各ステージでイベントを生成し、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** — 署名イベントについてユーザーに通知し、オプションで、プロセス終了時にサイン入りの承認済み文書の配布を通知します。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。

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、ユーザー情報、イベント情報、Adobe Signで処理された最終のサイン済みPDFがあります。

REST APIサービスを介した統合

Adobe Signは、広範なビジネスアプリケーション、エンタープライズシステム、トラストサービスプロバイダー（TSP）とのターンキー統合が可能です。また、Adobe Signでは包括的REST 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でサポートされるビジネスアプリケーションとエンタープライズシステムの一覧については、Adobe Document Cloud法人版の代表的な業務システムとの連携に関するページをご覧ください。トラストサービスプロバイダーの一覧については、https://www.adobe.com/trust/document-cloud-security/cloud-signatures-compliance.html（英語）をご覧ください。

Adobe Signのデータフロー

ユーザーが文書の署名プロセスを開始する場合のAdobe Signの利用手順を以下に示します。ステップの番号は以下の図2の番号に対応しています。

1. **リポジトリ項目の定義：**ユーザーは、Adobe Signを初めて使用する前に、再使用可能なカスタムワークフロー定義、ライブラリテンプレート、webフォームを作成してAdobe Signリポジトリに保存できます。これらのアセットにアクセスする権限を持ったユーザーは、ライブラリテンプレートを送信するか、ワークフローを開始するか、webフォームを投稿して署名プロセスを開始することができます。

2. **構成：**Adobe Signで契約書送信ワークフローを開始するには、参加者とその参加順序を定義し、参加の詳細を設定する各種オプションを定義します。また、アドビが提供する統合アプリケーションか、パートナーまたはカスタマーがAdobe Sign APIを使用して開発したアプリケーションを介して、契約書ワークフローを開始することもできます。アップロードした電子メールアドレス一覧にもとづいて契約書を一括送信することもできます。

   次に、ユーザーは契約書に関するソース文書をアップロードします。文書のアップロードは、サードパーティのクラウドストレージシステム、カスタマーやパートナーの統合機能、既存のライブラリテンプレート、またはユーザーのデスクトップから実行できます。

3. **契約書の作成：**Adobe Signでは、アップロードした文書が契約書になります。契約書が定義済みのフィールドのあるライブラリテンプレートフォームである場合、Adobe Signがそれらのフィールドを契約書内でインスタンス化します。契約書がライブラリテンプレートフォームでない場合、署名者が署名プロセスをスムーズに進めることができるように、ユーザーが必要なフィールドを契約書に配置する必要があります。

   Adobe Signでは、ユーザーが契約書内の適切な位置にフォームフィールドを配置し、入力式のフォームフィールド（電子メールアドレス、姓、名、役職名など）を使用して契約書に情報やコンテキストを追加できます。このプロセスを「オーサリング」といいます。

   どのような契約書であれ、少なくとも署名フィールドは必要です。署名フィールドは、オーサリングで配置するか、Adobe Signで自動的に配置することができます。署名フィールドを自動的に配置する場合、署名フィールドは契約書の一番下（余白が十分にある場合）に配置されるか、契約書に署名ページが追加されて配置されます。この情報は、下流プロセスで使用することができます。

4. **リンクの配布：**契約書のオーサリングが完了すると、電子メール、webフォーム、またはカスタムアプリケーションのAdobe Sign APIを使用して、指定した参加者全員に契約書が送信されます。

5. **署名の収集：**契約書のパラメーターにもとづき、署名者には、承認の送信、署名、フォームフィールドへの値の入力が依頼されます。フォームフィールドは、作成したユーザーの指示にもとづき任意または必須にできます。また、フォームフィールドをマスクしたり、フォームフィールドに様々な書式を適用したりできます。値はすべて、契約書の現在の状態（誰が署名し、次に誰が署名する必要があるかなど）とともにクラウド内のAdobe Signデータストレージに保存されます。この段階で、添付文書を収集できます。

6. **全員が署名した契約書：**すべての署名者が署名ワークフローを完了すると、全員が署名した契約書は、署名プロセスの参加者全員で利用できるようになり、Adobe Signクラウドストレージに自動的に保存されます。ユーザーは、Adobe Signクライアントを使用して、署名済みの契約書（承認済みPDF）、監査レポート（承認済みPDF）、フォームフィールドのデータ値を記録した別のレポート（CSVフォーマットで書き出し可能）など、署名に関連するすべての作成物をダウンロードしたり、オプションで、Adobe Sign APIまたはパートナーの文書保管サービスにより、選択した記録システムに契約書を移動／コピーしたりできます。

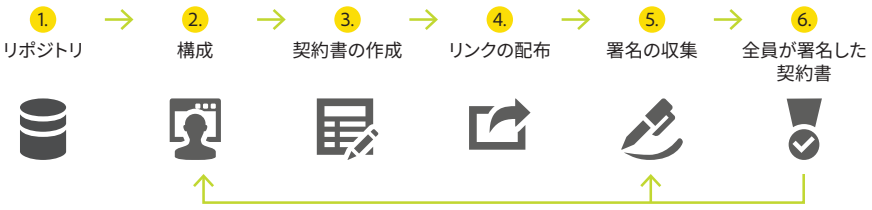

図2：Adobe Signのデータフロー

Adobe Signの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図を示します。

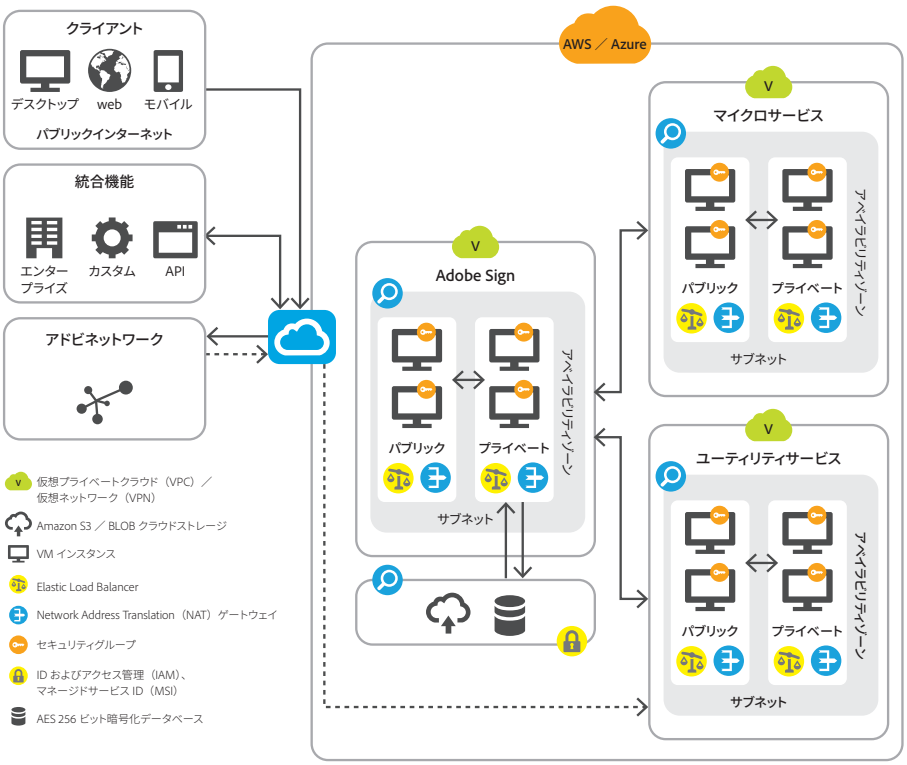

図3：Adobe Signネットワークのセキュリティアーキテクチャ

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サーバーとその関連ロードバランサーは、アプリケーションサーバーに動的リクエストを分配します。また、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、厳格な制約のある出入口を介した場合を除き、外部からは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の中核となる業務プロセスをサポートするコアVPC／VNet。
- クラウド署名コンソーシアム（Cloud Signature Consortium）による電子署名の統合、署名検証、署名画像の背景削除などのセカンダリサービスをサポートするマイクロサービスVPC／VNet。
- イベントモニタリングなどの管理機能を制御するユーティリティサービスVPC／VNet。

これらのサービスはすべて、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されます。この仮想クラウドサーバーは、厳格に保護されたサブネットとVPC／VNETネットワーク制限を経由した場合にのみアクセス可能です。

高可用性をサポートするために、VPC／VNetインスタンスは複数の冗長なアベイラビリティゾーン（AZ）に分割されます。AZは相互に物理的に分離されているため、いずれかのAZで電力やネットワークなどのインフラストラクチャに障害が発生しても、他のAZのオペレーションは影響を受けません。すべてのデータがすべてのAZ間で複製され、各AZ内の複数のサーバーでも複製されます。

VPC／VNetインスタンス内におけるネットワークアクセスは、セキュリティグループルールを介して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特定の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によるHTTPS接続でおこないます。

データの暗号化

Adobe SignはPCI DSS準拠の暗号アルゴリズムを使用して、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を使用して、転送中のデータを保護します。

保存中の文書には、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追加して、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、アクセス権が限定された安全な環境に保管されて管理されます。

Adobe Signの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、以下のような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、文書の署名ワークフローを作成し、署名、承認、または表示するための文書を送信することができるライセンスを持つユーザー。
- **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では、単一要素認証や多要素認証など、複数の方式でユーザーIDを認証できます。

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。
- **Google ID** — GmailやGoogle Apps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。

Adobe SignでSAMLを使用したシングルサインオンを有効にする方法について詳しくは、http://www.adobe.com/go/adobesign-saml-configuration（英語）をご覧ください。

Adobe ID管理サービス（IMS）については、https://www.adobe.com/content/dam/acom/en/security/pdfs/AdobeIdentityServices.pdf（英語）をご覧ください。

IDデータの所在地

通常、Adobe Signを使用する際は、Adobe Admin Consoleを使用してユーザー管理をおこないます。この場合、ユーザーIDデータは、Adobe Signがホストされているデータセンターに保存され、お客様の所在地に関係なくAdobe IMSの情報を処理するすべてのデータセンターに複製されます。このようなデータセンターは、米国東部（バージニア州）、米国西部（オレゴン州）、EU西部（アイルランド）、シンガポールの各リージョンにあり、負荷分散されています。

注意：ユーザーIDデータは、お客様の所在地に関連のある同一のデータセンター内に保存されます。通常、Adobe Signを使用する際は、Adobe IMSとAdobe Admin Consoleを使用してユーザー管理をおこないます。この場合、ユーザーIDデータは、米国東部（バージニア州）、米国西部（オレゴン州）、EU西部（アイルランド）、シンガポールにある可用性の高いAdobe IMSデータセンターでも複製されます。

署名者の本人確認

Adobe Signへの本人確認は、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レベルの確認と考えられます。第1レベルの確認は、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、お客様の所在地に応じて、電話、SMSテキスト、ナレッジベース認証（KBA）、公的証明書による確認などの多要素認証方式を追加することもできます。署名者の本人確認をおこなう最新の方法について詳しくは、https://helpx.adobe.com/jp/sign/using/signer-identity-authentication-methods.htmlをご覧ください。

Adobe Signの文書証明

Adobe Signは、ワークフローの各ステージで文書を保護し、文書の整合性と作成元の証明を確認しています。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と監査証跡を証明した後、その文書を参加者に配信します。

認証署名はSHA-256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から固有の暗号化文字列を算出します。この電子署名が、最終の署名済みPDFの上部に証明バッジ付きの青いバナーとしてグラフィカルに表示され、文書の整合性（以下の図4を参照）を確認し、文書がAdobe Signで生成されたことと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。機密保持が必要な文書の場合、最終の承認済みPDFをさらにパスワードで保護することもできます。

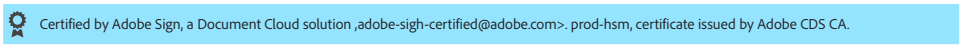

図4：Adobe Signの文書証明バナー

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、複数の信頼された認証機関（CA）とタイムスタンプ機関（TSA）が発行した証明書を使用します。一部の環境では、地域的な要件やコンプライアンス要件にもとづき、特定の証明書を使用して認証署名を適用できるようにAdobe Signを設定できます。最終PDFの証明に使用したPKIキーは、最高レベルのセキュリティとコンプライアンスに対応する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。

Adobe Signのホスティングとセキュリティ

Adobe Signサービスのインフラストラクチャは、委託先クラウドホスティングプロバイダーであるAmazon Web Services（AWS）およびMicrosoft Azure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。アドビのクラウドサービスインフラストラクチャパートナーは、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、保護されたサイトにアクセスできません。Adobe Signサービスに使用されるデータセンターについて詳しくは、アドビのサポートwebサイトをご覧ください。

Amazon Web Servicesのセキュリティについて詳しくは、https://aws.amazon.com/jp/securityをご覧ください。

Microsoft Azureのセキュリティについて詳しくは、https://azure.microsoft.com/ja-jp/services/security-center/をご覧ください。

Adobe Signのネットワーク管理

Adobe Signネットワークでは、データの収集、コンテンツの供給、レポート作成のセキュリティを確保することが重要です。この目的のために、ネットワークアーキテクチャは、開発／生産環境のセグメント化、認証済みロールベースのアクセス制御（RBAC）など、セキュリティを最優先に考えて設計されています。

安全な管理

サーバーに対するすべての管理接続は、暗号化されたチャネルでおこなわれ、アドビの社内ネットワーク以外からはアクセスできません。アクセスには常に2要素認証が必要です。

サービスのモニタリング

アドビは、Adobe Signネットワーク上のすべてのサーバー、ルーター、スイッチ、ロードバランサーおよびその他の重要なネットワーク機器を年間365日24時間休みなくモニタリングしています。アドビネットワークオペレーションセンター（NOC）は様々なモニタリングシステムから通知を受け取り、迅速に問題の修正を試みるか、その問題を適切な関係者に報告します。さらに、アドビは複数の第三者企業と外部モニタリング契約を結んでいます。

加えて、Adobe Signは最先端のテクノロジーと業界をリードするプロバイダーを利用して、アプリケーション専用のモニタリングとアラート通知をおこなっています。SLIとSLOは常にトラックされ、違反があった場合は深刻度に応じたアラートが通知されます。

データの可用性

Adobe Signのデータは、データベースとクラウドストレージリポジトリの両方を組み合わせて保存されます。データベースは、複数のアベイラビリティゾーン間で複製された上で、定期的にバックアップされます。クラウドストレージリポジトリは、非常に高レベルの堅牢性を備えた独自の冗長性メカニズムにより、1年間で99.999999999%（9 x 11）の堅牢性を実現します。また、災害復旧機能を備えたAdobe Signリージョンの場合、データはすべて、セカンダリリージョンに複製されます。

変更管理

アドビは変更管理ツールを使用し、変更をスケジュールすることで、リソースの依存関係を共有するチーム間でのやり取りを増やしたり、保留中の変更を関係者に通知したりします。さらに、変更管理ツールを使用して、ネットワークトラフィックが多くなる期間を避けるように、保守による機能の一時停止をスケジュール設定します。

パッチ管理

Adobe Sign組織内のホストコンピューターへのパッチ配信を自動化するために、アドビでは社内のパッチおよびパッケージリポジトリと業界標準のパッチおよび構成管理を使用しています。ホストの役割と保留中のパッチの重要性に応じて、導入時と定期的なパッチスケジュールでホストにパッチを配信し、必要な場合は、ただちに緊急パッチをリリースおよびデプロイします。

セキュリティアップデートを含む、Adobe Signのインスタンスと製品アップデートは、デプロイメントパイプラインに従って適用されます（詳しくは、デプロイメントモデルに関する上記の節を参照してください）。

アクセスコントロール

管理ツールにアクセスできるのは、アドビのイントラネット内の認定ユーザーまたはVPN接続作成の複数要素の認証プロセスを完了したリモートユーザーのみです。さらに、アドビは監査のためにすべてのAdobe Signプロダクションサーバーの接続を記録しています。Adobe Sign環境では、組み込みのセキュリティ機能を利用することで、グループと権限を使用してアクセス権とアクセスコントロールを実装できます。

お客様の問題をトラブルシューティングするために必要な場合などの限定的な状況を除き、アドビの管理者はお客様の契約書にはアクセスできません。アクセスが可能な役割を割り当てることができるのは、職務上そのようなアクセスが必要な管理者のみです。アクセス時には常に、お客様の承認と、指定の承認権限を持つ管理者による承認の両方が必要です。また、このアクセスには2要素認証が必要で、アクセスは記録されます。

ログ記録

不正なアクセスや改ざんを防ぐために、アドビは業界標準ツールとアドビ独自のツールを組み合わせて使用することで、ネットワークログ、OS関連ログを取得して管理し、侵入検知をおこなっています。また、定期的にログのストレージ容量を確認し、必要に応じてストレージ容量を拡大しています。ログを生成するすべてのシステムは強化され、ログおよびログ作成用ソフトウェアへのアクセスは認定を受けたアドビの担当者に限定されています。取得したログデータは1年間アドビで保管され、すべてのログの管理とアクセスはアドビの担当者のみがおこないます。

データセンターの物理統制と環境統制

データセンターの物理的および環境的なアクセス制御に関する以下の記述は、アドビのデータセンターの拠点すべてに共通の統制を説明するものです。データセンターによっては、本書に記述されている内容を補完する統制が追加されている場合があります。

物理施設のセキュリティ

アドビが所有またはリースしているホスティング施設にあるすべてのハードウェアは、物理的に不正アクセスから保護されています。Adobe Signのプロダクションサーバーが設置されているすべての施設には、専任の現場セキュリティ担当者が24時間常駐しており、これらの担当者が施設に入るには有効な証明書が必要です。アドビは、データセンターにアクセスするためには暗証番号またはバッジ型証明書（場合によっては両方）を運用するように取り決めています。認可されたアクセスリストに表示された担当者のみが施設に入ることができます。一部の施設ではトラップを使用して、不正な人物が認可された担当者の後ろについて施設に入ることができないようにしています。

火災抑制

すべてのデータセンター施設に、空気サンプリング方式の即応性に優れた煙探知システムを採用し、火災の最初の兆候が見られた時点で施設担当者に警告することを義務付けています。さらに、各施設に必ずダブルインターロック方式の予作動式ドライパイプスプリンクラーシステムを設置して、煙探知機が起動したり熱が検知されたりしなければ、サーバー領域に放水されないようにしてあります。

空調管理

すべてのデータセンター施設は、温度湿度コントロールや液体検知を含め、環境的にコントロールされている必要があります。アドビは、完全に冗長構成の冷暖房換気空調（HVAC）システムを備え、24時間体制の施設チームにより、発生する可能性のある環境問題に即座に対応できる体制を整えるように取り決めています。環境パラメーターがアドビによって定義された値から外れると、環境モニターがアドビと施設のネットワークオペレーションセンター（NOC）の両方に警告を発します。

ビデオ監視

Adobe Signのプロダクションサーバーが設置されているすべての施設では、ビデオ監視をおこなってポイントアクセスの出入りを最小限モニタリングする必要があります。アドビは、データセンター施設に対し、機器への物理アクセスをモニタリングするように求めています。問題が発生すると、ビデオログを確認してアクセスを特定します。

バックアップ電源

独立した配電器からの複数の電力供給によって、アドビが所有またはリースしているすべてのデータセンター施設に継続的に電力を供給できます。アドビでは、主要電源からバックアップ電源に自動的に移行することとされており、この移行はサービスを中断することなくおこなわれます。また、各データセンター施設にあらゆるレベルで発電機やディーゼル燃料契約などの冗長性を維持するよう取り決めています。さらに、各施設では負荷をかけて発電機を定期的にテストして機器の可用性を確認する必要があります。

可用性と通知

Adobe Signは、Amazon Web Services（AWS）とMicrosoft Azureの常時アクティブなアベイラビリティゾーン（AZ）データセンター構成でホスティングされています。Adobe Signのすべてのデータセンターは非常に回復力が高く、高い可用性を備え、影響を最小限に抑えてシステムまたはハードウェアの障害に耐えられるように設計されています。各データセンターは、システム停止時にも事業の継続が支援できるよう、それぞれ独自の物理的に異なる独立したインフラストラクチャ上で動作しています。アドビの復旧ポイント目標（RPO）や復旧時間目標（RTO）の取り組みなど、データセンター構成について詳しくは、アドビのサポートwebサイトをご覧ください。

Adobe Signのアップタイムデータは、Adobe Status webサイトで入手できます。また、定期および計画外のいずれのシステム停止についても、所定の手順でAdobe Signのサービスの状態をお客様にお知らせいたします。万一、運用サービスをプライマリサイトから災害復旧サイトに移行する必要が生じた場合は、以下のような特定の通知をお客様に送信いたします。

- 災害復旧サイトへのサービス移行の意思の通知
- サービス移行中の毎時進捗状況
- 災害復旧サイトへの移行完了の通知

通知には、クライアントサポートとお客様担当者の連絡先と対応状況も記載します。移行中および移行後に関するお客様からのご質問とお問い合わせには、この担当者が対応し、別地域のサイトに移行した後、運用をスムーズに開始できるように支援いたします。

アドビのセキュリティ組織

製品および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、アドビは最高セキュリティ責任者（CSO）の下にすべてのセキュリティ活動を統合しています。すべての製品・サービスのセキュリティ戦略とAdobe Secure Product Lifecycle（SPLC）の実装は、CSOのオフィスで統括しています。

CSOはまた、Adobe Secure Software Engineering Team（ASSET）も管理します。ASSETは、セキュリティのエキスパートが集まった専任のチームです。Adobe Signチームをはじめ、主要アドビ製品のセキュリティと運用を担うチームのコンサルタントとしての役割を果たしています。ASSETの調査担当者は、各アドビ製品チームや運用チームと協力して製品やサービスが適切なレベルのセキュリティで保護されるよう尽力するとともに、明確かつ再現可能なプロセスで開発、デプロイメント、運用、インシデント対応をおこなえるように、セキュリティに対する取り組みについて各チームにアドバイスしています。

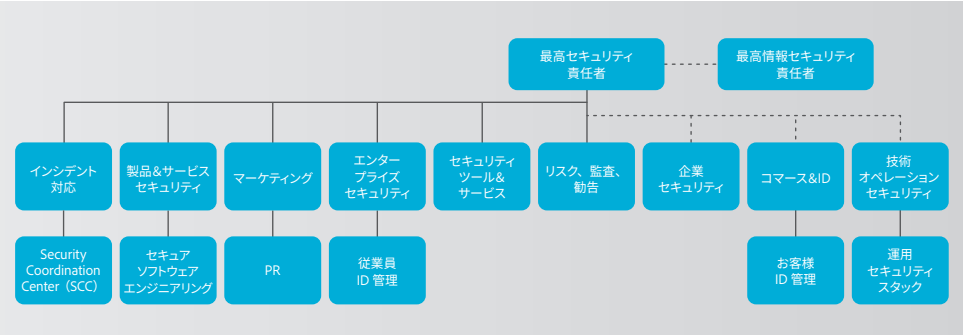

図6：アドビのセキュリティ組織

アドビの安全な製品開発

他のアドビの製品およびサービスの組織と同様、Adobe Sign組織もAdobe Software Product Lifecycle（SPLC）プロセスを採用しています。ソフトウェア開発のプラクティス、プロセス、ツールにわたる数百もの特定のセキュリティコントロールを厳選したAdobe SPLCは、設計や開発から品質保証、テスト、導入に至るまで、製品ライフサイクルの様々な段階に組み込まれます。ASSETのセキュリティ研究者は、潜在的なセキュリティの問題点に基づいて、主要な製品またはサービスについて個別にSPLCをアドバイスします。Adobe SPLCは、アドビ外部のセキュリティコミュニティに継続的に参画することによって補完され、テクノロジー、セキュリティプラクティスおよび脅威の変化に応じて最新の状態が保たれるよう進化し続けます。

Adobe Secure Product Lifecycle

Adobe SPLCの活動には、個々のAdobe Sign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。

- すべての製品チームに対するセキュリティ研修および認定制度の実施
- 製品の正常性、リスクおよび脅威の分析
- 安全なコーディングガイドライン、ルール、分析
- Adobe Signセキュリティチームが「Open Web Application Security Project（OWASP）webアプリケーションの脅威Top 10」と「CWE／SANS最も危険なプログラミングエラーTop 25」に対処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方法
- セキュリティアーキテクチャレビューと侵入テストの実施
- 脆弱性の原因となりかねない既知の問題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
- 安全かつ順応性の高いレビュー、対応計画、開発者向け教材のリリース準備

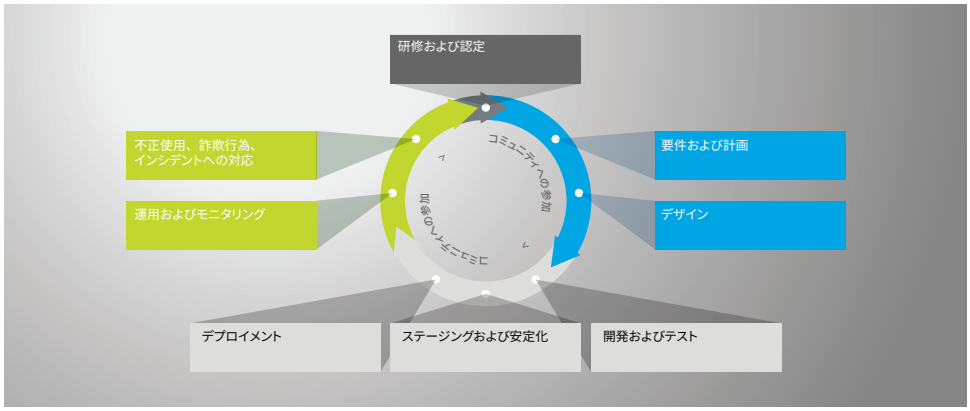

図7：Adobe Software Product Lifecycle（SPLC）

アドビのセキュリティ組織とSPLCについて詳しくは、
www.adobe.com/jp/securityをご覧ください。

アドビソフトウェアセキュリティ認定プログラム

Adobe SPLCの一環として、アドビでは、開発チームで継続的にセキュリティ研修を実施し、企業全体でセキュリティの知識を高め、製品およびサービスの包括的なセキュリティ向上を図っています。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に到達します。

Adobe Sign組織では様々なチームがさらなるセキュリティ研修やワークショップに参加し、セキュリティが組織内や企業全体での役割に及ぼす影響について認識を高めています。詳しくは、アドビセキュリティ文化ホワイトペーパー（英語）をご覧ください。

Adobe Signのコンプライアンス

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をご覧ください。

特定地域の電子サインに関する法律とAdobe Signのコンプライアンスの最新情報について詳しくは、www.adobe.com/jp/trust.htmlをご覧ください。

Adobe Common Controls Framework（CCF）

Adobe Sign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。CCFを策定するにあたり、アドビはクラウドビジネスにおける主なセキュリティ認証の基準を分析。十数種類の業界標準にまたがる1,350項目以上の要件を、アドビ独自の対策に落とし込みました。

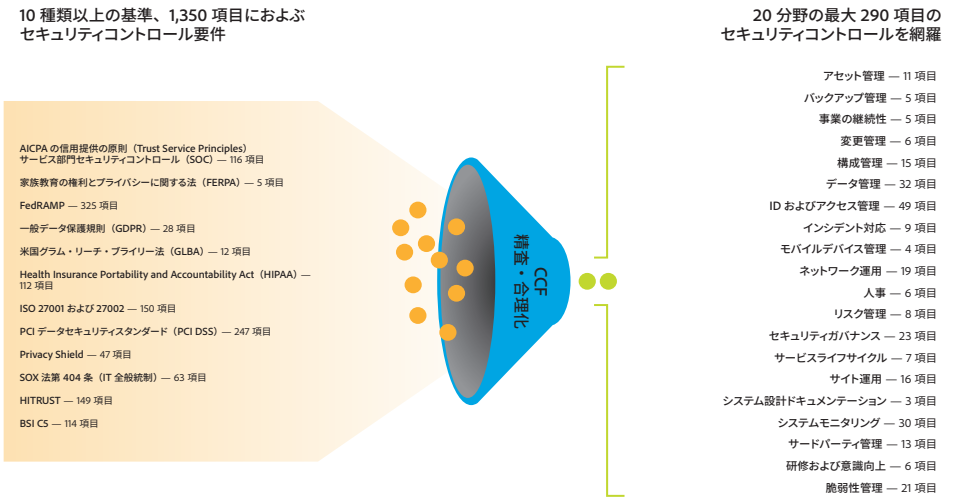

図8：Adobe Common Controls Framework（CCF）

アドビのリスク／脆弱性管理

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尽力しています。継続的に脅威の動向をモニタリングしながら、世界中のセキュリティ専門家と知識を共有して問題が発生したらすぐに解決し、この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およびサービスにおいて最高レベルのセキュリティを確保します。

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。当該第三者から提供されたレポートを受け取り次第、アドビはこれらの脆弱性を文書化し、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。侵入テストは年1回、およびメジャーリリースの前に実施します。脆弱性スキャンは毎月、Webとデータベーススキャンは四半期ごとに実施します。

社内では、Adobe Signセキュリティチームが、年1回およびリリースの前に毎回すべてのAdobe Signコンポーネントのリスク評価を実行します。Adobe Signセキュリティチームは、技術オペレーションおよび開発チームと連携し、リリースの前にリスクの高い脆弱性を軽減するための措置を講じます。アドビの侵入テスト手順について詳しくは、アドビセキュアエンジニアリング概要ホワイトペーパー（英語）をご確認ください。

インシデントの対応と通知

脆弱性や脅威が日々進化する中、アドビは新たに発見された脅威を軽減すべく懸命に取り組んでいます。US-CERT、Bugtraq、SANSなどの業界規模での脆弱性アナウンスリストの利用に加え、主要な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ます。

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概要（英語）をご確認ください。

フォレンジックス分析

インシデントの調査に関して、Adobe Signチームは、必要に応じて、すべての画像取り込み、影響を受けるマシンのメモリダンプ、証拠の安全な保持および分析過程の管理記録をはじめとするアドビのフォレンジックス分析プロセスに準拠しています。アドビは、契約書の完成後にお客様が指定した間隔でAdobe Signの契約書データを自動的に削除するのに役立つ、データ保持機能を提供しています。また、お客様がデータを選択して手動で削除できる管理用インターフェイスを提供しています。

アドビのオフィス

アドビは世界中にオフィスがあるため、次のプロセスと手順を企業全体に導入してセキュリティの脅威から会社を守っています。

物理的なセキュリティ

アドビのすべてのオフィス所在地では、現地の警備員を採用して敷地を24時間体制で保護しています。アドビの従業員は、建物に入るためのキーカード型IDバッジを携帯しています。訪問者は正面入口から入り、受付で署名して一時的な訪問者IDバッジを提示します。訪問者には従業員が同伴します。サーバー機器、開発マシン、電話システム、ファイルサーバーとメールサーバーおよびその他のデリケートなシステムは、環境が制御されたサーバールームに常時設置されており、そのサーバールームには認可されたスタッフメンバーのみがアクセスできます。

ウイルス対策

アドビでは、送受信されたすべての企業電子メールを対象に既知のマルウェアによる脅威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、稼働している生産システムへのアクセスをネットワークレベルとアプリケーションレベルで制限する技術対策を講じ、Adobe Signの開発環境と生産環境を分離された状態に保っています。開発システムや生産システムにアクセスする従業員には特定の権限が付与され、業務上の正当な目的がない従業員はそれらのシステムにアクセスできません。

身元調査

アドビは、雇用目的で身元調査レポートを取得します。アドビが通常調査をおこなう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、職歴、犯罪歴などの裁判記録、同僚や友人への身元照会が含まれます。これらの身元調査要件は、システムを管理したり顧客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、アドビの身元調査ガイドラインに従って適切な派遣会社を通して身元調査要件が課されます。米国以外では、アドビの身元調査ポリシーと適用される現地法に従って、特定の新入社員について身元調査を行います。

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おこなうように通知します。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。

アドビの企業セキュリティ担当は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やオフィスにアクセスできないようにします。

- 電子メールアクセスの削除
- リモートVPNアクセスの削除
- オフィスおよびデータセンターの入退出バッジの無効化
- ネットワークアクセスの終了

要求に応じて、上司はアドビのオフィスまたは建物から退職する従業員に警備員を同伴させることができます。

施設のセキュリティ

アドビのすべてのオフィス所在地では、現地の警備員を採用して敷地を24時間体制で保護しています。アドビの従業員は、建物に入るためのキーカード型IDバッジを携帯しています。訪問者は正面入口から入り、受付で署名して一時的な訪問者IDバッジを提示します。訪問者には従業員が同伴します。サーバー機器、開発マシン、電話システム、ファイルサーバーとメールサーバーおよびその他のデリケートなシステムは、環境が制御されたサーバールームに常時設置されており、そのサーバールームには認可されたスタッフメンバーのみがアクセスできます。

顧客データの機密保持

アドビは、顧客データを機密情報として扱います。お客様との契約で許可されている場合、およびアドビ利用条件とアドビプライバシーポリシーに規定されている場合を除き、アドビはお客様の代わりに収集した情報を使用または共有しません。

まとめ

本ホワイトペーパーで説明したセキュリティの事前対応型アプローチと厳格な手順によって、Adobe Signおよび機密情報を保護しています。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。

詳しくは、Adobe Trust Centerをご確認ください。

Adobe

アドビ株式会社
〒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 Inc.
345 Park Avenue
San Jose, CA 95110-2704
USA
trust.adobe.com