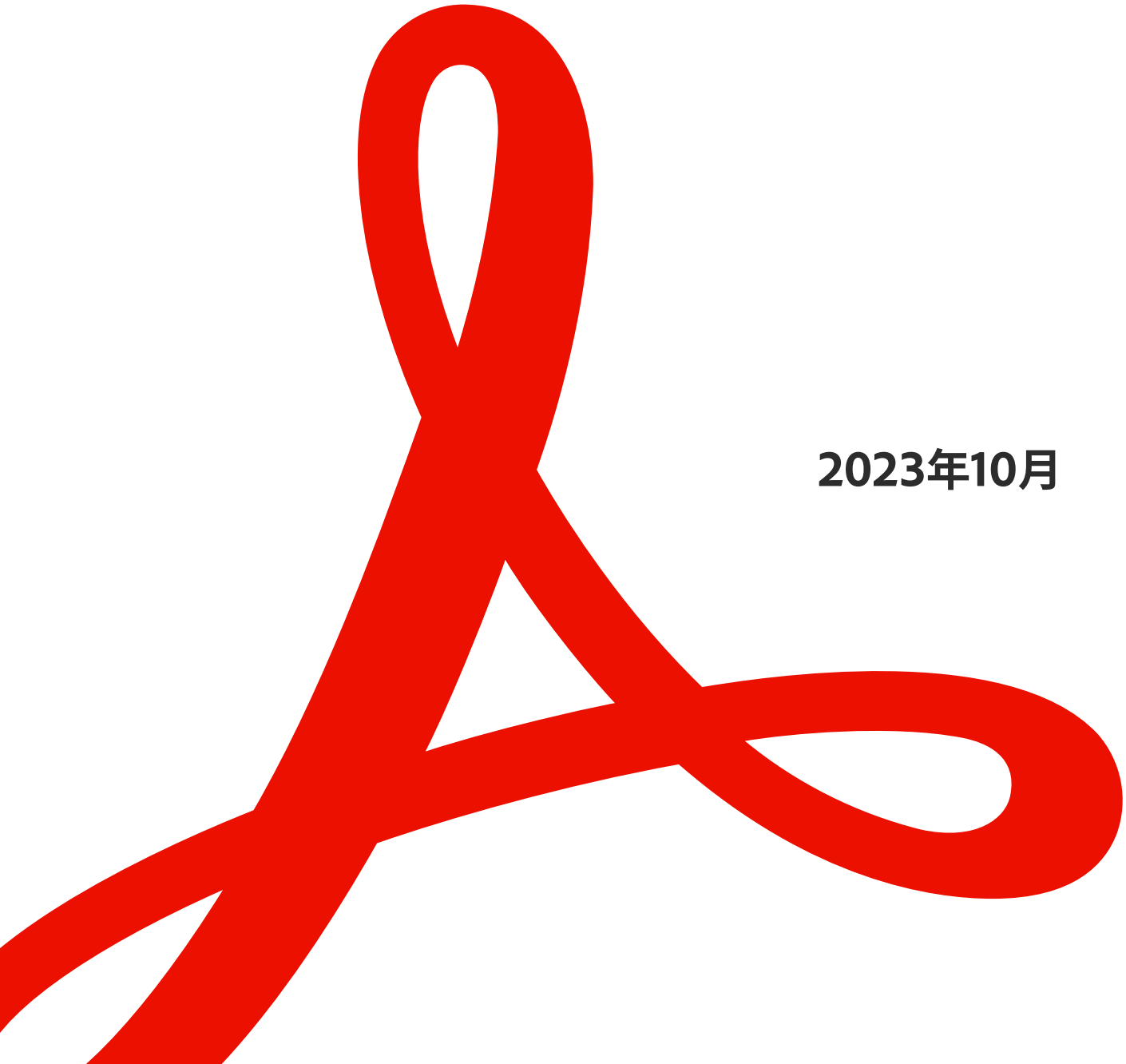
Adobe Document Cloud

Adobe

ホワイトペーパー

Adobe Acrobat Signのセキュリティ概要



2023年10月

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の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 Acrobat 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。

注意：この文書は Acrobat Sign Solutions エンタープライズ版と Acrobat Sign Solutions ビジネス版の機能を対象としています。Acrobat Sign の特定の機能を利用できるかどうかについては、アドビの担当者にお問い合わせください。

Acrobat Sign について

Acrobat 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。クラウドでの基本的な電子サインからデジタル署名（適格電子サイン）まで、あらゆるタイプの署名ワークフローに対応します。Acrobat Sign では、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。Acrobat 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。

Acrobat 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デジタル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。法人向けの堅牢なクラウドベースのソリューションであるため、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、Acrobat Signのクラウド署名は、Cloud Signature Consortium（CSC：クラウド署名コンソーシアム）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にもとづいたリモートデジタル署名を実現します。電子サインのコンプライアンスと各国の電子サイン関連法について詳しくは、Adobe Trust Centerを参照してください。

Acrobat Signソリューションのアーキテクチャ

Acrobat 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、Acrobat Signのトランザクションデータはすべてフェイルオーバーおよびリカバリー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。

アドビはAcrobat Signの可用性、入手性、提供体制を維持するため、ISO 22301認定の包括的な事業継続性と障害復旧（BCDR）プログラムをデプロイおよびサポートし、予期しない中断の影響への対応、緩和、回復力を強化しています。詳しくは、Acrobat Sign BCDR Fact Sheet（英語）をご覧ください（守秘義務契約にご同意いただきます）。

Acrobat Signソリューションの各論理層は、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。

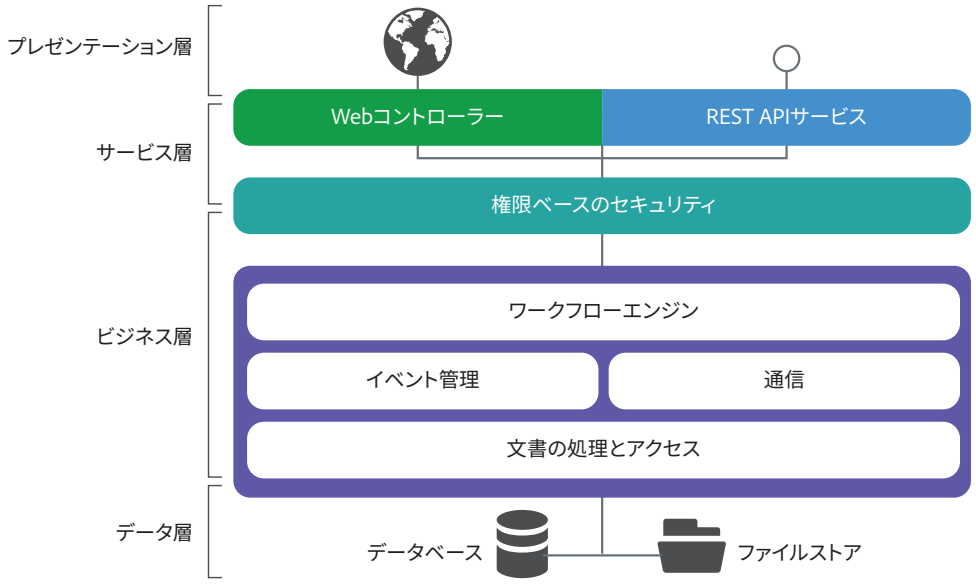


図1：Acrobat Signソリューションのアーキテクチャ

Acrobat 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。

この後のセクションでは、Acrobat Signソリューションアーキテクチャの各層の機能を説明します。

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）の管理、署名の収集やその他のワークフロー（不正改ざん防止シール付きの最終PDFの提示など）のための文書の生成とレンダリングをおこないます。

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を管理します。

Webサーバーは、ビジネス層のAcrobat 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、アクセス制御の強化を支援するファイアウォール保護を組み込んでいます。

ビジネス層

Acrobat 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** — 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クラウドファイルストレージ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Acrobat 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。Acrobat 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、Acrobat Sign で は、Domain Keys Identified Mail（DKIM）、Domain-based Message Authentication、Reporting & 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と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、Acrobat 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

Acrobat Signには、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含まれます。また、Acrobat Signでは包括的REST APIセット（英語）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。Acrobat 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をご覧ください。

一般的なデータフロー

ユーザーが文書の署名プロセスを開始する場合のAcrobat Signの一般的なデータフローを以下に示します。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. **リポジトリの作成：**ユーザーは、Acrobat Signを初めて使用する前に、再利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Acrobat 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から契約書を送信する、ワークフローを開始する、または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. **ワークフローの作成：**Acrobat 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Acrobat Sign API（英語）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：**Acrobat Signでは、アップロードした文書が契約書になります。ライブラリテンプレートフォームから生成した、定義済みのフィールドのある契約書の場合、Acrobat Signがフィールドを契約書内に作成します。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。

   Acrobat 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たり、特定のタイプ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、Acrobat 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が使用するAcrobat Sign APIを通じて、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、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より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Acrobat 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の提示：**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、Acrobat 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、Acrobat 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できます。オプションで、Acrobat 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またはコピーすることもできます。

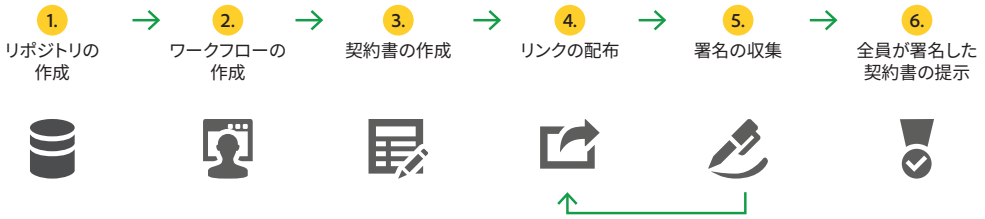


図2：Acrobat Signのデータフロー

Acrobat 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、Acrobat 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。

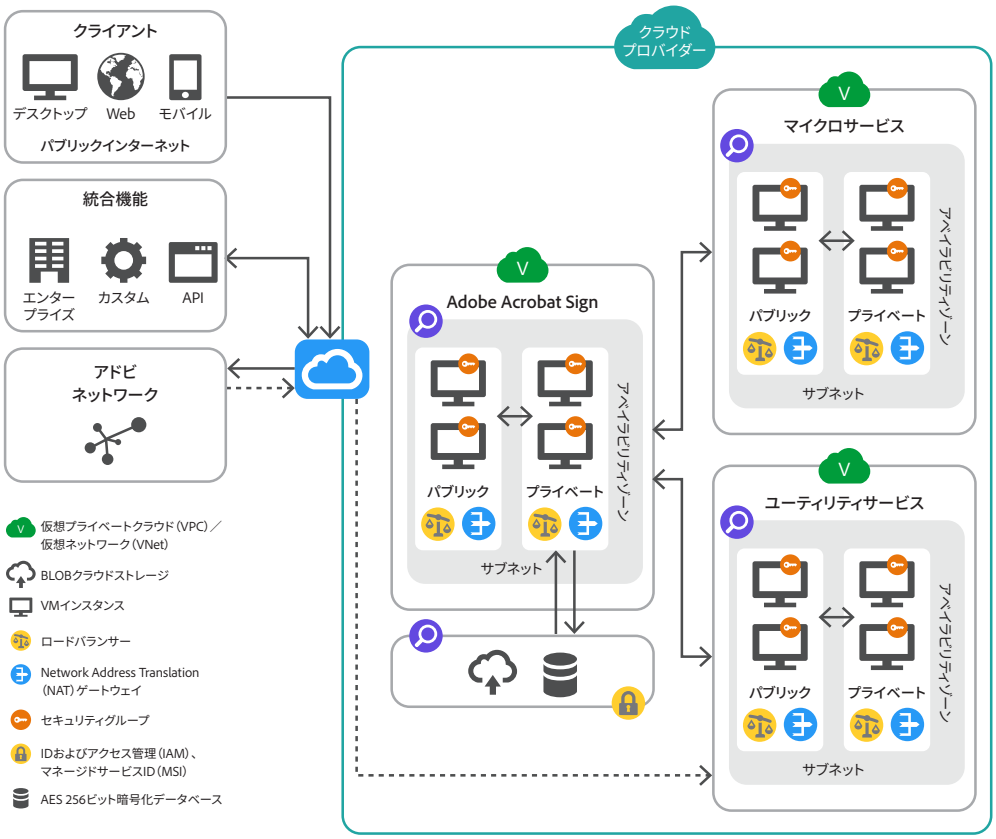


図3：Acrobat Signのセキュリティアーキテクチャ

外部向けサーバー

Webサーバーを含むAcrobat Sign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。Webサーバーには、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

Acrobat Sign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。Acrobat Signサービスでは VPC／VNetを以下の方法で使用します。

- Acrobat Signの中核となる業務プロセスをサポートするコアVPC／VNet。
- Cloud Signature Consortiumによるデジタル署名の統合、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、厳格なサブネットとVPC／VNETネットワークのセキュリティ制限で許可され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、Acrobat Sign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

Acrobat Signには、ブラウザー、REST API、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Acrobat 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TLS v1.2以降によるHTTPSでおこないます。

データの暗号化

Acrobat 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、Acrobat 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、安全な機密管理システムに保管され、管理されます。このシステムへのアクセス権は限定されており、アクセスには多要素認証が必要です。

Acrobat Signの電子メールは通常、SMTPS経由で送信され、最小キー長128 bitの暗号スイートを使用してTLSで暗号化されます。ただし、ごく一部のインターネット電子メールプロバイダーはTLS暗号化をサポートしていないため、確実に届ける必要がある場合、電子メールは暗号化されていないSMTP経由で送信されます。

ID管理

Acrobat Signはロールベースのモデルを使用して、Acrobat Signソリューション全域の認証、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Acrobat Sign管理者が定義し、有効にします。Acrobat 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Acrobat 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。

ライセンス取得済みユーザー認証

Acrobat 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。

ライセンスを持つユーザーは、以下のいずれかの認証方法でAcrobat Signにログインできます。

- **Acrobat Sign ID** — ライセンスを持つユーザーがAcrobat 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アカウント** — Adobe ID、Business ID等を含むAdobeアカウントは、ライセンスされたすべての（Acrobat Signを含む）アドビサービスへのアクセスに使用できます。
- **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（英語）にし、企業IDシステムを使用してAcrobat Signユーザーを管理することができます。

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。

ライセンス取得済みユーザーIDデータの所在地

ライセンス取得済みユーザー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、Acrobat Signを使用する際は、アドビID管理サービス（英語）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）、SG-1（シンガポール）にある可用性の高いデータセンターでも複製されます。

署名者のID

電子サインの署名者が本人確認に使用する方法と種類は、署名者の種類（社内か社外か）によって異なります。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、通常Acrobat Signへの本人確認は、発信者が特定の個人に文書の署名を依頼する電子メールを送信する方法でおこないます。

セキュリティを強化し、電子サインした文書の完全性を保護するには、電話、SMS、ナレッジベース認証（KBA）、デジタル証明書、公的証明書、BankID／eID検証など、署名者の本人確認を追加で要求することができます。また、お客様の所在地に応じて、利用可能なその他のデジタルIDソリューションを追加することもできます。

Acrobat Signはまた、Acrobat Signデジタル IDゲートウェイへの統合が認められたプロバイダーやCloud Signature Consortium（CSC）による技術標準規格を使用するクラウド署名プロバイダーによる数多くのサードパーティーデジタルIDソリューションも提供しています。

Acrobat Signに統合されたデジタルIDソリューションについて詳しくは、Adobe Trust Centerをご覧ください。

Acrobat Signの文書証明

Acrobat Signは、ワークフローの各ステージで文書を保護し、文書の完全性と作成元の証明を確認しています。Acrobat Signは、公開鍵基盤（PKI）を使用してデジタル署名で最終の署名済みPDFと監査証跡を証明した後、その文書を受信者に配布します。

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。このデジタル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、文書の完全性（以下の図4を参照）を確認し、文書がAcrobat Signで生成されたことと、最終的な不正改ざん防止シール付き文書であることの証明に役立ちます。追加で機密保持を必要とする場合は、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：Acrobat Signの文書証明バナー

Acrobat 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Acrobat 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（HSM）に保管されます。

Acrobat Signのホスティングとセキュリティ

Acrobat Signサービスのインフラストラクチャは、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。

世界のホスティング場所について詳しくは、Adobe Acrobat Signデータセンター（英語）を参照してください。

Acrobat Signのコンプライアンス

業界規格と標準規格

Acrobat Signは、ほとんどの場所およびデバイスから、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すように設定できます。お客様は自社の文書、データ、ワークフローについての制御権を保持することができ、また、当該自治体や地域の規則（EUの一般データ保護規則（GDPR）、米国の健康情報保護法（HIPAA）、米国のFDA CFR 21 Part 11など）に従うための最善の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、アドビプライバシーセンターをご覧ください。

特定地域の電子サインに関する法律とAcrobat Signのコンプライアンスの情報について詳しくは、Adobe Trust Centerをご覧ください。

FedRAMP

Acrobat SignはFedRAMPのTailoredレベル認証を取得しています。Acrobat Sign for GovernmentはModerateレベルの認証を取得し、Microsoft Azure Government Community Cloudでホストされています。米国連邦政府、部族、州、地方政府の顧客、米国政府の請負業者のみが使用できるように指定されています。

アドビセキュリティプログラムの概要

アドビセキュリティプログラムは、一体となって機能する5つのCenter of Excellence（CoE）で構成されています。各CoEは、新しいテクノロジーや発展が期待されるテクノロジー（例：自動化、AI、機械学習など）をアドビのリスク検知・予防策に応用するために、それぞれのテーマに従って反復研究と進歩を追求しています。

図5：5つのセキュリティ Center of Excellence（CoE）

アドビセキュリティプログラムを構成する5つのCoEが担当するテーマは以下のとおりです。

- **アプリケーションセキュリティ** — 製品コードのセキュリティに重点的に取り組み、脅威調査やバグ調査報奨制度を実施
- **運用セキュリティ** — アドビのシステム、ネットワーク、実稼働クラウドシステムについて、モニタリングとセキュリティ確保を支援
- **エンタープライズセキュリティ** — アドビの企業環境に関するアクセスセキュリティと認証システムに注力
- **コンプライアンス** — アドビのセキュリティガバナンスモデル、監査／コンプライアンスプログラム、リスク分析体制を統監
- **インシデント対応** — 常時稼働のセキュリティオペレーションセンターと脅威対応チームを運営

アドビの組織においては、最高セキュリティ責任者（CSO）がセキュリティに関する現行の取り組み全体を統括し、セキュリティの将来を見据えたビジョンを示す役割を担います。5つのセキュリティCoEはCSOの直属に位置付けられています。この体制は、製品・サービスのセキュリティをきわめて重視するアドビの姿勢を象徴するものといえます。

アドビのセキュリティ組織

アドビのセキュリティ組織は、透明性の確保、結果責任の明確化、意思決定材料の充実を目的とする共通基盤の上に立ち、総合的なセキュリティサービス群全体を単一のガバナンスモデルで運営する体制をとっています。トップマネジメントを担うCSOは、最高情報責任者（CIO）および最高プライバシー責任者（CPO）と密接に協力し、オペレーションと方針を合わせながらセキュリティ戦略を遂行します。

アドビのセキュリティ組織は、上記のCoEに加えて法律、プライバシー、マーケティング、PRの専門家チームを擁し、セキュリティ関連のあらゆる意思決定に関して透明性の確保と結果責任の明確化を追求する仕組みを内包しています。

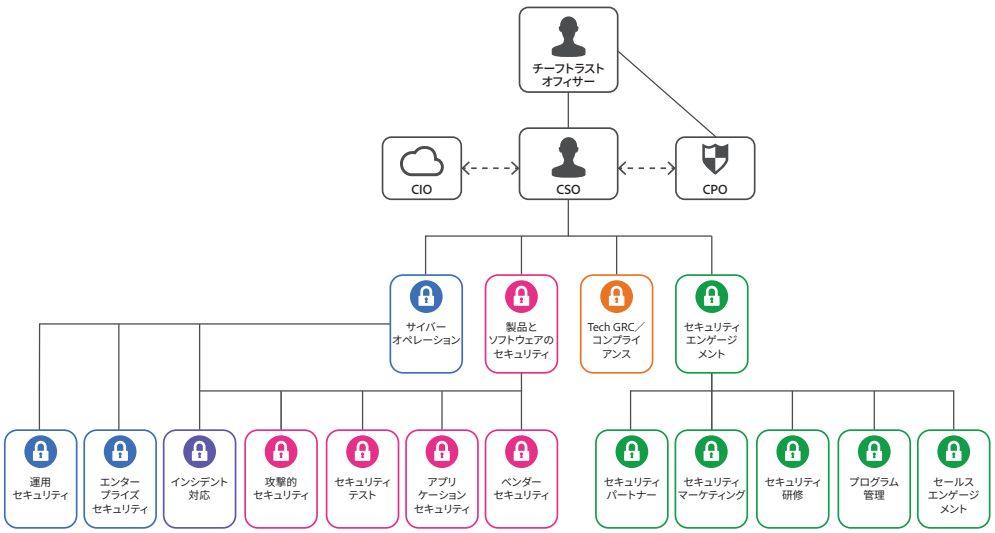


図6：アドビのセキュリティ組織

アドビでは、全社のセキュリティ文化を保つ活動の一環として、すべての従業員に年1回のセキュリティ意識向上およびセキュリティ教育研修の受講・再認定を義務付けています。この規則は、全従業員をあげてアドビの企業資産、お客様データ、従業員データを守る環境づくりに役立っています。技術系従業員は（エンジニアリング、技術運用の両方とも）、人事採用の際、それぞれの職務に最適化された緻密な「格闘技を模した段級位制」の研修プログラムに自動登録されます。

アドビのセキュリティ文化と研修プログラムについては、アドビのセキュリティ文化に関するホワイトペーパー（英語）をご覧ください。

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を構成する様々な段階には、あらゆるセキュリティの基礎となるAdobe Secure Product Lifecycle（SPLC）が組み込まれています。Adobe SPLCは、ソフトウェア開発のプラクティス、プロセス、ツールを幅広く網羅し、数百項目のセキュリティ活動を具体的かつ厳密に示して、明確で反復可能なプロセスを定義したものです。その内容は、開発チームが製品・サービスにセキュリティを組み込む際の指針となり、絶えず最新の業界ベストプラクティスを絶えず取り入れて進歩し続ける活動に役立っています。

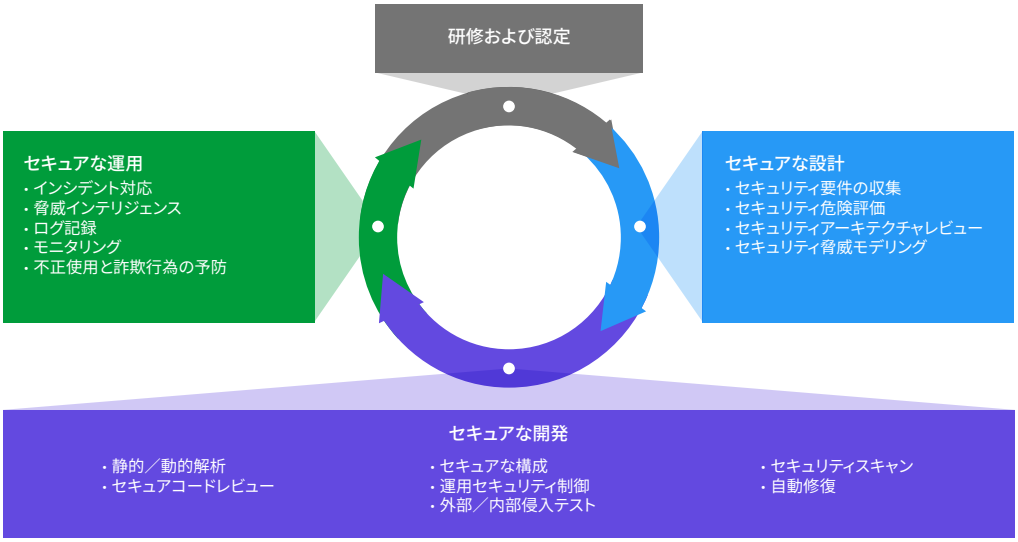


図7：Adobe Secure Product Lifecycle（SPLC）

アドビではSPLC標準のドキュメントを発行・維持しており、ご要望に応じて提供可能です。Adobe SPLCを構成する要素について詳しくは、アドビアプリケーションセキュリティの概要（英語）をご覧ください。

アドビアプリケーションセキュリティ

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）を前提とするアプリケーション開発の出発点は、アドビアプリケーションセキュリティスタックです。このスタックは、実績ある研究成果と経験から導かれた明確で反復可能なプロセスに、一貫したセキュリティ制御を確実に適用する自動化の仕組みを組み合わせて構築されています。これには、開発効率を高め、セキュリティミスの発生リスクを最小限に抑える効果があります。既にテストと承認が済んでいる安全なコードブロック群が含まれているため、開発者は、共通的なパターンやブロックをゼロからコーディングする必要がありません。コードのセキュリティを必要以上に心配することなく開発に取り組み、各自が本来の専門分野に意識を集中できます。アドビアプリケーションセキュリティスタックは、テスト体制、目的に特化したツール整備、モニタリング体制と相まって、セキュア・バイ・デフォルトなコードの作成に役立っています。

図8：アドビアプリケーションセキュリティスタック

また、アドビではアプリケーションセキュリティに関する標準ドキュメントをいくつか発行・維持しています。Amazon Web Services（AWS）とMicrosoft Azureパブリッククラウドインフラストラクチャに関する当社独自の利用方法に特化した内容も含まれます。それらのドキュメントはご要望に応じて提供可能です。アドビアプリケーションセキュリティの概要（英語）には、アドビのアプリケーションセキュリティ対策とプロセスに関する詳細な情報が記載されています。

アドビの運用セキュリティ

すべてのアドビ製品・サービスについて、最初からセキュリティのベストプラクティスを念頭に置いた設計作業がおこなわれる環境を整備するために、運用セキュリティチームはアドビ運用セキュリティスタック（OSS）を作成しました。OSSは、製品開発者とエンジニアによるセキュリティ対策の改善に役立ち、アドビの立場とお客様の立場におけるリスク軽減にも役立つツール群を集約したものです。これは、アドビがコンプライアンス、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うえでも役立ちます。

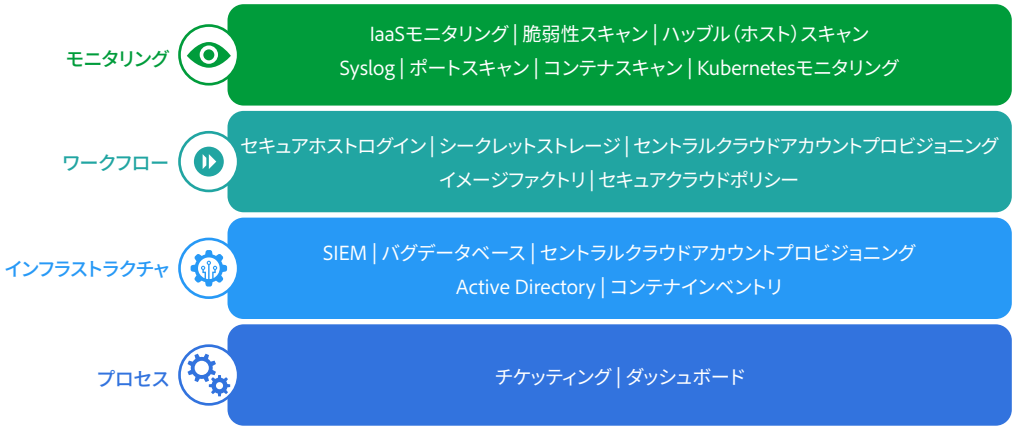


図9：アドビ運用セキュリティスタック（OSS）

アドビでは、継続的なクラウド運用に関する標準ドキュメントをいくつか発行・維持しています。それらのドキュメントはご要望に応じて提供可能です。アドビOSSと、アドビが全社的に利用している具体的なツールについて詳しくは、アドビ運用セキュリティの概要（英語）をご覧ください。

アドビのエンタープライズセキュリティ

アドビでは、製品・サービスとクラウドホスティング運用環境を保護するだけでなく、様々な社内向けセキュリティ対策を導入し、社内のネットワークとシステム、物理的な会社施設、従業員、お客様データのセキュリティを確保しています。

アドビが採用しているエンタープライズセキュリティ管理策の詳細情報と、それらの管理策に関してアドビが策定した標準ドキュメントについては、アドビエンタープライズセキュリティの概要（英語）をご覧ください。

アドビのコンプライアンス

すべてのアドビ製品は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。アドビでは、最先端の自動化プロセスをできるだけ多く活用して、コンプライアンス違反の可能性がある状況を検知し、チームに警告を伝え、状況改善や業務環境見直しの迅速化に役立てています。

アドビ製品・サービスは、適用される法的基準を満たしているか、または、お客様によるサービスプロバイダー利用に関連した法的義務を満たすために役立つ方法で使用できます。お客様は自社の文書、データ、ワークフローについての制御権を保持することができ、また、当該自治体や地域の規則（EUの一般データ保護規則（GDPR）など）に従うための最善の方法を選択できます。

また、アドビではコンプライアンスの研修および関連する標準ドキュメントも作成・維持しており、ご要望に応じて提供可能です。アドビCCFおよび主要な認定資格について詳しくは、アドビのコンプライアンス認定、標準規格、規則リストをご覧ください。

インシデント対応

アドビは、リスクと脆弱性の管理、インシデント対応、問題の緩和、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。脅威の動向を常に注視し、世界中のセキュリティ専門家と知識を共有しています。問題発生時にはすみやかに解決し、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・サービスについて最高レベルのセキュリティを確保するよう努めています。

また、インシデント対応と脆弱性管理に関する内部標準ドキュメントも作成・維持しており、ご要望に応じて提供可能です。

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プログラムの概要（英語）をご確認ください。

事業継続性と障害復旧

アドビ事業継続性と障害復旧（BCDR）プログラムは、アドビ事業継続性プラン（BCP）と各種製品に特有の障害復旧（DR）プランで構成されています。いずれの内容も、アドビ製品・サービスの可用性、入手性、提供体制を維持するためのものです。BCDRプログラムはISO 22301認証取得済みであり、アドビはこれに従って、予期しない事業中断への対処、問題の緩和、影響からの回復能力を強化しています。Adobe BCDRプログラムについて詳しくは、アドビの事業継続性と障害復旧プログラムの概要（英語）をご覧ください。

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、Acrobat 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。

アドビセキュリティについて詳しくは、Adobe Trust Center をご覧ください。

12/23