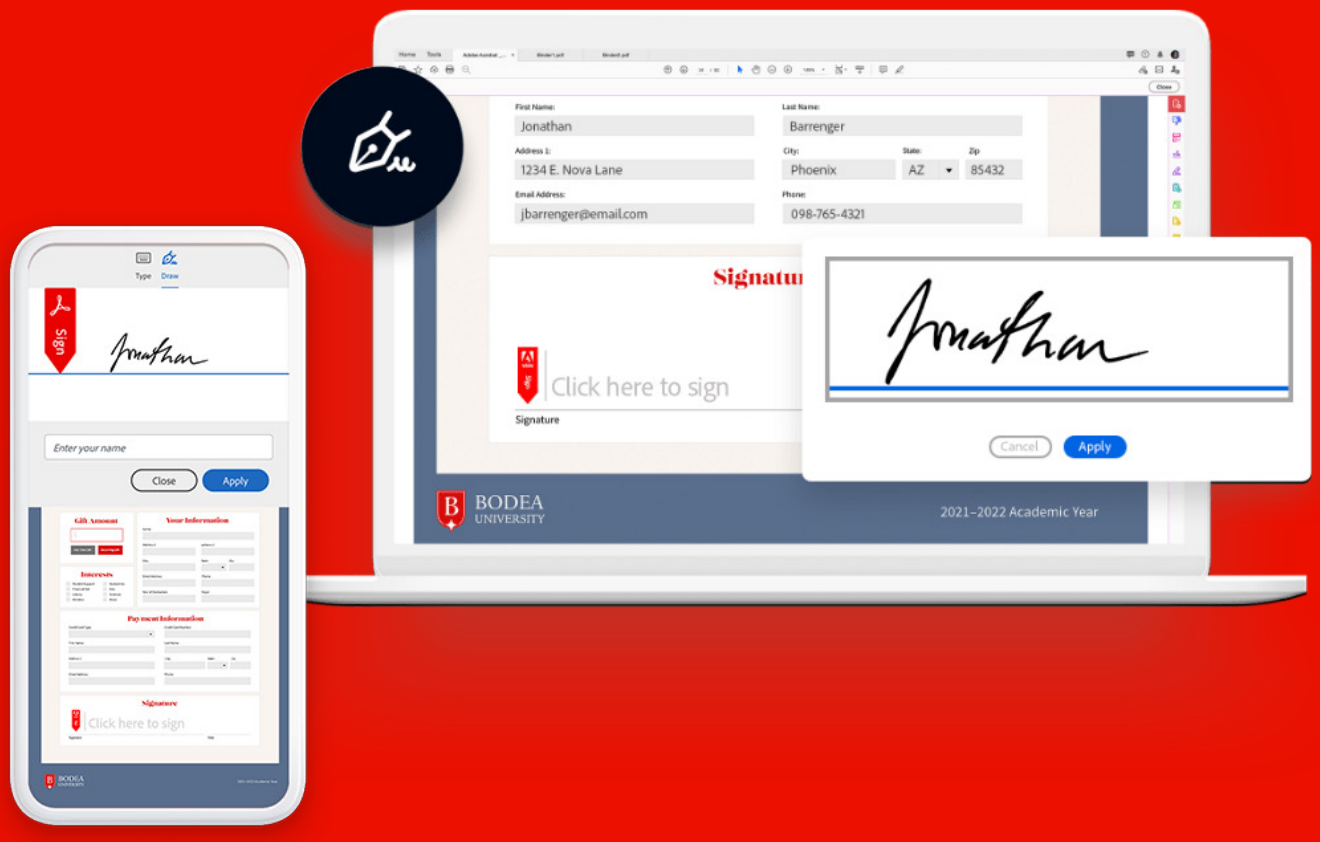
ホワイトペーパー

Adobe Acrobat Sign Solutions

Acrobat Sign Solutions とヘルスケア・ライフサイエンス組織：
21 CFR Part 11 および EudraLex Annex 11 に関するハンドブック



目次

1　はじめに

Acrobat Sign Solutionsは、柔軟かつ信頼性の高いクラウドベースの電子サインサービスです。これを導入すれば、極めてシンプルな標準署名からセキュリティの高い証明書ベースのデジタル署名まで、様々な署名ワークフローを管理できます。

今日、米国食品医薬品局（FDA）の監督下にある多くの組織（食品、薬品、生物製剤、医療機器、化粧品、動物用医薬品）は、従来の手書き署名プロセスに代えて自動電子サインワークフローを導入するにあたりAcrobat Sign Solutionsを選んでいます。FDAは、電子記録を作成、変更、保持または伝達するためのシステムによって電子記録（それらの記録に適用される電子サインを含む）の真正性と完全性が守られるよう、21 CFR Part 11規制を設けています。

欧州連合（EU）では、人用および動物用薬品を管理する規則・規制集はEudraLexです。EudraLexのVolume 4 Annex 11には、コンピューターシステムの使用規則が定められています。

GxP規制下にあるヘルスケア・ライフサイエンス組織にとっては、21 CFR Part 11やEudraLex Annex 11の要件に準拠する方法でAcrobat Sign Solutionsを使用できることが非常に重要です。

このハンドブックでは、適切なシステム実装と手順制御により、Acrobat Sign Solutionsによる電子サインの法的有効性を確保し、組織が21 CFR Part 11の要件に準拠する方法について考察します。また、Acrobat Sign Solutionsで利用できる主な機能と、組織でそれらの機能を実装して21 CFR Part 11およびEudraLex Annex 11の要件を満たす方法をユースケースとともに紹介し、さらに、Acrobat Sign Solutionsのシームレスな導入と継続的な使用をサポートするためにアドビが実施している品質管理プロセスについても説明します。

2　適用範囲

本ハンドブックは、組織において21 CFR Part 11およびAnnex 11の要件を満たす形でAcrobat Sign Solutionsを導入・使用するための情報、指針、推奨事項を提供します。対象とする読者は、GxP規制への対応の一環としてAcrobat Sign Solutionsを使用しているヘルスケア・ライフサイエンス関連企業及び組織のお客様です。

本ハンドブックでは、**Adobe Acrobat Sign Solutions**のエンタープライズレベルまたはビジネスレベルのサービスで提供されるAcrobat Signサービスを使用してGxP対応文書に電子サインを適用するための標準的なシナリオに焦点を当てます。

Acrobat Pro、Acrobat Standard、およびAcrobat ReaderのAcrobat Sign機能は、本ハンドブックでは考慮されていません。

システムをAcrobat Sign Solutionsに接続するAPIや他のアプリケーションを使用してAdobe AcrobatおよびReaderデスクトップアプリで生成される電子サインも、本ハンドブックの適用範囲外です。この形態を実装する場合は、それに先立ち、その適合性やコンプライアンス対応をお客様が別途評価する必要があります。

Acrobat Sign Solutionsにはビジネスプロセスのデジタル化を促進する様々な機能がありますが、テンプレート、カスタムワークフロー、APIの使用をサポートする機能の使用はお客様の実装状況によって異なります。そのため、こうした機能については本書では説明していません。

HIPAAに準拠する保護医療情報（PHI）に関心のあるヘルスケア・ライフサイエンス組織は、Acrobat Sign Solutionsでプライバシーおよびセキュリティ保護対策を実施できますが、本ハンドブックではHIPAAへの準拠については明示していません。

本ハンドブックの情報は、21 CFR Part 11およびEudraLex Annex 11の要件を満たすAcrobat Sign Solutionsの機能についての組織の理解を促すことを意図していますが、それらの要件に準拠するAcrobat Sign Solutionsの導入を計画するにあたり、組織は自社の法律顧問に相談する必要があります。

3 用語集

3.1 一般的な用語

Adobe Admin Console	アドビの製品およびサービスのユーザーとライセンスを管理するために組織が使用する管理ポータル。
契約書	署名を取得するプロセス中にAcrobat Signサービスにアップロードされたファイルから作成されるオブジェクトと、最終的に生成されるPDFの両方を定義する用語。
お客様	（本書の場合）21 CFR Part 11やEudraLex Annex 11の要件に準拠する必要があるプロセスの一部としてAcrobat Signを使用するためにAcrobat Sign Solutionsを導入している組織。
お客様アカウント（またはAcrobat Signアカウント）	お客様に属するAcrobat Sign Solutionsの特定のインスタンス。
ユーザー	一意の電子メールアドレスによって識別され、署名者、送信者、または管理者（アカウント、グループ）の資格でAcrobat Sign Solutionsを使用する個人。
ユーザーアカウント	お客様アカウントに追加された個人がシステムの認証を取得するためのユーザー情報（電子メールアドレスやパスワードなど）。

3.2 グループ、ロール、権限

Admin Console管理者	組織が購入したすべてのアドビ製品およびサービスのユーザーとライセンスを管理する権限を持つAdobe Admin Consoleユーザー。 Admin Console管理者は、Acrobat Sign Solutionsユーザーである必要はありません。
アカウント管理者	アカウント設定の指定やグループ作成の権限を持ち、ユーザーの追加や管理の責任を負う場合があるAcrobat Sign Solutionsユーザー。 アカウント管理者はAcrobat Sign Solutionsお客様アカウントのメンバーである必要があります。
グループ	独自の構成設定を適用できるお客様アカウント内のエンティティ。 内部ユーザーは、単一または複数のグループに割り当てられます。
グループ管理者	グループ設定を指定する限定的な管理機能を持ち、グループに割り当てられたユーザーを管理するAcrobat Sign Solutionsユーザー。 グループ管理者はAcrobat Sign Solutionsお客様アカウントのメンバーである必要があります。1人のユーザーを単一または複数のグループのグループ管理者に指定することもできます。
送信者	署名者に文書を送信して電子サインをもらうための適切な権限を持つAcrobat Sign Solutionsユーザー。文書を承認用に回覧するには、送信者はAcrobat Sign Solutionsの送信ページに文書をアップロードして署名者（受信者）の電子メールアドレスを指定します。 送信者はAcrobat Sign Solutionsお客様アカウントのメンバーである必要があります。

署名者（受信者）	Acrobat Sign Solutionsで文書への電子サインの依頼を受ける個人。署名者は、文書への署名を求めるメッセージと文書へのハイパーリンクが記載された電子メールを受け取ると、任意のデバイスから安全なwebブラウザー経由で文書にアクセスして署名できます。 署名者は、Acrobat Sign Solutionsお客様アカウントの内部または外部の個人です（ユーザーアカウントを持っている必要はありません）。 本書の目的のために、ここではそれらの個人を以下のように内部署名者または外部署名者と呼びます。 ・ **内部署名者**は、契約書の送信元である同一のAcrobat Sign Solutionsお客様アカウント内のアクティブユーザーであり、文書への電子サインの依頼を受ける個人（電子メールアドレスによって識別される）です。「内部署名者」と同義で「内部受信者」が使用される場合があります。内部署名者が契約書の唯一の署名者である場合、自己署名も可能です。 ・ **外部署名者**は、契約書の送信元であるAcrobat Sign Solutionsお客様アカウントのメンバーではない個人であり、Acrobat Sign Solutionsでの文書への電子サインの依頼を受ける個人です。「外部署名者」と同義で「外部受信者」が使用される場合があります。外部署名者はAcrobat Signのユーザーアカウントを持っていなくても契約書に署名できますが、契約書を作成したアカウントとは別のお客様アカウントのメンバーである可能性があります。

3.3 21 CFR Part 11関連用語

デジタル署名	発信者認証の暗号方式にもとづく電子サインであって、一組の規則および一組のパラメーターを用いて計算され、署名者の身元およびデータの完全性を確認することができるもの（参考文献 [1]）。
電子記録	コンピューターシステムによって作成、修正、保守、アーカイブ、検索、または配布され、21 CFR Part 11の要件の対象となるデジタル形式のテキスト、グラフィック、データ、オーディオ、画像、またはその他の情報表現の任意の組合せ（参考文献 [1]）。
電子サイン	個人の手書き署名と同等の法的拘束力を持つものとして、個人により作成、採用、または承認されたシンボル（または一連のシンボル）を編集したコンピューターデータ（参考文献 [1]）。
GxP	医薬品の臨床試験実施基準（GCP）、安全性試験実施基準（GLP）、製造管理・品質管理基準（GMP）、物流・文書化基準（GDP）、および安全性監視基準（GVP）などのコンプライアンス基準の一般的な略称。
従前規則	連邦食品・医薬品・化粧品法、公衆衛生法、または21 CFR Part 11以外のFDA規制に定められている要件。
署名の外観	署名内容に付随し、署名者を識別するグラフィック。
署名内容	署名された電子記録は、以下のすべてを明確に示す署名に関連する情報を含むものとする（参考文献 [1]）。 (1) 署名者の印字氏名 (2) 署名が実行された日時 (3) 署名の意味（審査、承認、責任、作成者など）

注意：「デジタル署名」は「電子サイン」の一種ですが、すべての電子サインがデジタル署名であるわけではありません。本ハンドブックでは、Acrobat Sign Solutionsを使用して適用される署名全般を「電子サイン」という用語で呼びます。「デジタル署名」という用語は、本人確認とデジタル証明書の発行が外部のトラストサービスプロバイダーによって実行される署名プロセスに言及する場合にのみ使用されます。デジタル署名について詳しくは、こちらを参照してください。

4 GxP規制下でのAcrobat Sign Solutions

21 CFR Part 11やEudraLex Annex 11に従って電子サインを適用するためにAcrobat Sign Solutionsを導入する場合、規制要件やビジネスプロセスのニーズに対応できるように機能や手順を制御することが必要となります。Acrobat Sign Solutionsは、使用する機能をお客様が自力で柔軟に判断できるよう設計されています。システム構成や必要なサポートプロセスに関連する意思決定を十分な情報にもとづいておこなうには、Acrobat Sign Solutionsで利用できる機能を理解することが重要です。

4.1 はじめに

Adobe Acrobat Sign Solutionsのエンタープライズレベルまたはビジネスレベルのサービスを購入すると、Adobe Admin Consoleを使用して組織全体のユーザー、製品、およびアドビ製品の使用権限を管理できます。購入後、契約者にはAdobe Admin Consoleにアクセスできることを知らせる電子メールがアドビから届きます。Acrobat Sign Solutionsはユーザー単位のプランまたはトランザクション単位のプランとして購入できます。Admin ConsoleでAcrobat Sign Solutionsがどのように表示されるかは、プランの種類によって異なります。

ユーザー管理とアクセスのプロビジョニングはAdobe Admin Consoleで管理できますが、Acrobat Signに固有の設定はアプリケーション内でおこないます。Acrobat Sign Solutionsを使用するには、管理者が事前にアカウントを設定し、業務のニーズに合わせて構成する必要があります。設定と構成は、Acrobat Sign Solutionsの管理ロールを与えられた個人（または個人のグループ）によって管理されます。

旧製品のお客様はAdobe Admin Consoleを使用しない方法でオンボードした可能性があります。そのようなお客様は、Acrobat Sign Solutionsのアカウントとユーザーの管理をすべてアプリケーションのインターフェイス内でおこないます。

Acrobat Sign Solutionsの使用を開始するための手順について詳しくはこちら：
https://www.adobe.com/go/sign-admin-guide_jp

4.2 バイオ医薬業界標準対応の設定を使用して21 CFR Part 11の要件に対応

4.2.1 概要

Acrobat Sign Solutionsでは、バイオ医薬業界標準対応の設定に、21 CFR Part 11の要件への対応に関連する構成パラメーターが含まれています。

Acrobat Sign Solutionsでの21 CFR Part 11およびAnnex 11の要件への対応方法について詳しくはこちら：
https://www.adobe.com/content/dam/dx-dc/jp/ja/pdf-cards/acrobat-sign-compliance-21cfrpt11-wp-jp.pdf

バイオ医薬業界標準対応の設定は、それだけで21 CFR Part 11の要件すべてに十分に対応できるわけではありませんが、署名者を一意に識別するためには不可欠であり、署名内容に影響する署名の様々な構成要素を制御するのに必要です。バイオ医薬業界標準対応の設定は以下の目的で使用されます。

- IDの要求を有効にし、要求するタイミング（文書を開くとき、署名フィールドをクリックしたとき、署名を完了するとき）を指定する
- 署名の理由の使用を強制し、事前に定義した理由の一覧を管理する

バイオ医薬業界標準対応の設定を使用する場合、署名フィールドの書式が再設定され、署名者の印字氏名、署名の日付とタイムスタンプ、指定された署名の理由が、システムによって署名内容に表示されるようになります。バイオ医薬業界標準対応の設定の使用については、セクション4.10で詳しく説明します。

4.2.2　考慮すべき点

バイオ医薬業界標準対応の設定では、署名プロセス全体を通して署名者の本人確認のために、複数回の認証を署名者に求めるよう設定することができます。これは、ビルに入館するときだけでなく、そのビル内のオフィスや一般立ち入り禁止の場所に入るときにも身分証を提示するようなものです。バイオ医薬業界標準対応の設定を使用すると、文書を開くときだけでなく、その文書内で署名しようとするたびに署名者に認証を求めることができます。

バイオ医薬業界標準対応の設定は、Adobe Acrobat Sign Solutionsのエンタープライズレベルまたはビジネスレベルのサービスのサブスクリプションを購入すると利用できます。

バイオ医薬業界標準対応の設定について詳しくはこちら：
https://www.adobe.com/go/adobesign-bio-pharma-overview_jp

バイオ医薬業界標準対応の設定に加え、HIPAAに準拠する保護医療情報（PHI）に関心のあるヘルスケア・ライフサイエンス組織はAcrobat Sign Solutionsでプライバシーおよびセキュリティ保護対策もおこなえます。パスワードポリシーの適用、非アクティブな期間が続いた後のwebセッションからの自動ログアウト、電子メールの添付ファイルの除外などのオプションがあります。お客様には、Acrobat Sign Solutionsで保護医療情報（PHI）を処理する前に、これらのオプションを検討し、すべてのセキュリティ設定を確認することをお勧めします。

Acrobat Sign Solutionsで保護医療情報を処理するには、アドビと提携事業者契約（BAA）を結ぶ必要があります。

HIPAAへの準拠およびアドビとの提携事業者契約（BAA）について詳しくはこちら：
https://www.adobe.com/go/adobesign-hipaa-settings_jp

4.3　グループの設定

4.3.1　概要

Acrobat Sign Solutionsで、アカウント管理者はアカウント内にグループを作成することができます。グループ構造により、設定をきめ細かく構成できるため、グループのメンバーに独自のエクスペリエンスが作成されます。これは、特定の署名要件を持つ契約書を送信する必要があるユーザーのクラスを定義する場合に非常に役立ちます。

グループの追加と管理について詳しくはこちら：
https://adobe.com/go/sign-groups-overview_jp

新しいグループを作成するとアウントレベルの設定が継承されますが、グループレベルで固有のアカウント設定を上書きできるため、特定のグループについてグループレベルでバイオ医薬業界標準対応の設定を適用することができます。

ビジネスプロセスを21 CFR Part 11の電子サイン要件に対応させる必要がある場合は、専用のグループを作成してバイオ医薬業界標準対応の設定を適用します。このグループの認定メンバーは、内部や外部の受信者に契約書を送信し、バイオ医薬業界標準対応の設定にもとづいて署名を得ることができます。この設定は下図のとおりです。

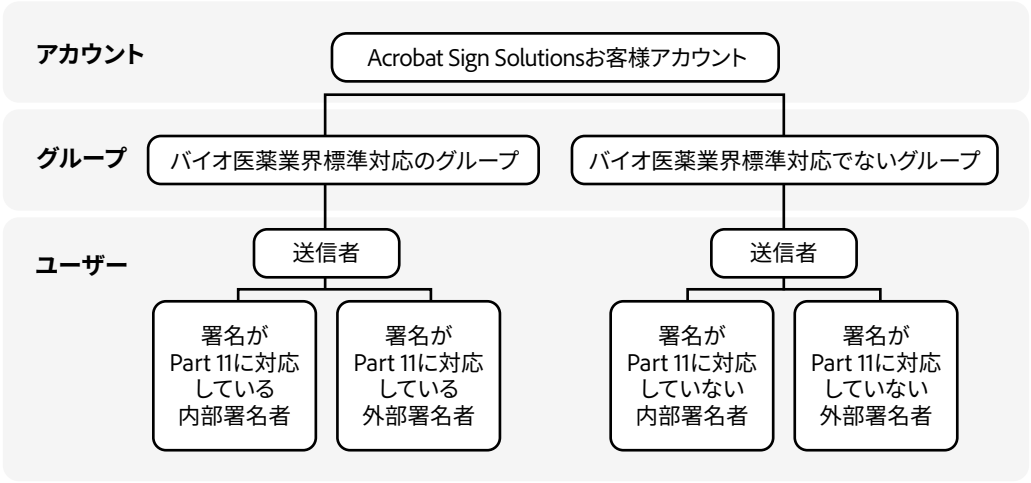


図1 – Acrobat Sign Solutionsお客様アカウントのグループ構造

契約書が、バイオ医薬業界標準対応の設定で、ID認証の強制が有効に設定されているグループから送信された場合、受信者は署名プロセスの複数のタイミングでAcrobat Sign Solutionsへの再認証を求められます。バイオ医薬業界標準対応の設定が適用されているグループのメンバーも、契約書の唯一の署名者である場合は必ずそのグループから開始された自己署名機能を使用して再認証するよう求められます。

署名プロセス中の複数回の再認証は、全体的な生産性とユーザーエクスペリエンスに影響を及ぼします。21 CFR Part 11の電子サイン要件を満たそうとすれば、これは仕方のないことです。ただ、ビジネスプロセスによっては21 CFR Part 11の要件を満たす必要がないこともあります。そのような場合は、バイオ医薬業界標準対応の設定が適用されていないグループにユーザーを追加します。複数のグループにユーザーを追加するオプションも用意されており、21 CFR Part 11署名内容を作成するトランザクションとそれ以外のトランザクションをいつ開始するかを選択できます。

4.3.2　考慮すべき点

21 CFR Part 11規制は、FDAの従前規則（セクション3.3の定義を参照）に従って作成、維持、またはFDAに提出される電子記録および電子サインに対してのみ適用されます。Acrobat Sign Solutionsを使用してバイオ医薬業界標準対応の設定で署名する必要がある文書かそうでない文書かを指定するには、ビジネスプロセスの分析をおこなう必要があります。Acrobat Sign Solutionsを使用するビジネスプロセスの実施を計画する際は、ビジネスプロセスを21 CFR Part 11の影響を受けるものとそうでないものに区別し、それに応じてユーザーをグループ分けします。

最初はビジネスプロセスがひとつしかないとしても、将来的な組織のニーズに対応して拡張できるように、グループ構造を持つアカウントを設計することをお勧めします。

4.4　アカウントとグループにユーザーを追加

4.4.1　概要

Acrobat Sign Solutionsのアカウントとユーザーアクセスは、以下の2種類の管理環境で管理できます。

1. Adobe Admin Console：

お客様がオンボードされると、最初の管理者にAdmin Consoleへのアクセス権が付与され、そこから追加の管理者を割り当てることができます。管理者はアドビの製品およびサービスすべてのユーザー、ユーザーのID、およびライセンスを管理できます。ユーザーの作成は手動で管理することも、組織ディレクトリと同期させて自動的に管理することもできます。

Admin Consoleでは、管理者がAcrobat Sign Solutions製品へのユーザーのアクセスの許可／取り消しをおこない、ユーザー（管理者権限なし）、Signアカウント管理者、Signアカウントおよびプライバシー管理者の3つの権限ロールのうちのひとつを割り当てることができます。Acrobat Sign Solutionsのグループメンバーとユーザー権限の割り当ては、Acrobat Sign Solutionsアカウントの管理環境内で管理する必要があります。

2. Acrobat Sign Solutionsアプリケーション：

アプリケーションでは、Acrobat Sign Solutionsで管理者権限を割り当てられたユーザーがアプリケーションの構成設定や機能を管理できます。また、Acrobat Sign Solutionsの管理者は、グループの作成と編集、グループへのユーザーの割り当て、およびユーザー権限の編集をおこなえます。最初にエンドユーザーまたは管理者がAcrobat Sign Solutionsへのアクセスを許可されると、そのユーザーはアカウントのデフォルトグループに配置されます。ただし、Acrobat Sign Solutionsアカウントの管理者はそのユーザーをアカウント内の別のグループに移動することや、複数のグループに割り当てることができます。Acrobat Signのグループは、Adobe Admin Consoleのユーザーグループとは異なることに注意してください。

Adobe Admin Consoleにアクセスせずにオンボードした旧製品のお客様は、Acrobat Sign Solutionsのアカウントとユーザーの管理をすべてアプリケーションのインターフェイス内でおこないます。このようなお客様がアカウントをAdobe Admin Consoleに移行することをご希望の場合は、アドビにお問い合わせください。また、新規のお客様は、追加のメリットを提供するAdobe Admin Consoleを使用したセットアップのみおこなうことができます。

Admin Consoleの管理者とAcrobat Sign Solutionsアカウントの管理者が同一である必要はありません。これらの管理者権限は相互に排他的です。

ユーザーが作成されると、Acrobat Sign Solutionsでユーザープロファイルが生成され、個人情報が取得されます。ユーザープロファイルは、個人の姓名と有効なメールアドレスを紐付けるものです。ユーザーはAcrobat Sign Solutionsサービスに対する本人確認にこの電子メールアドレスを使用します。ユーザーアカウントを作成すると、ユーザーは、Acrobat Sign Solutionsにログインして利用条件に同意するよう求める通知メールを受け取ります。このとき、ユーザーはパスワードを作成することも求められます（ユーザーがFederated IDを使用してログインしている場合を除く）。

ユーザーの追加と管理について詳しくはこちら：
https://www.adobe.com/go/sign-add-users-to-account_jp

管理者はユーザープロファイルからユーザーを単一または複数のグループに配置できます。「複数のグループユーザー」機能が有効な場合、複数のグループで送信権限を割り当てられているユーザーは、複数のグループから契約書を送信できます。その際、どのグループから契約書を送信するかを決める権限は送信者にあります。送信者のグループに関連する構成設定がシステム制御のプロパティ（認証方法、ブランディング、PDFセキュリティなど）を大きく左右するため、これは非常に重要です。署名者のエクスペリエンスは、署名者が属するグループに関係なく、契約書の送信元であるグループのグループレベル設定によって決まります。規制に準拠した署名を生成するよう設定されているグループから契約書が送信されなかった場合、規制に準拠しない署名が収集されることになります。

複数のグループのユーザーについて詳しくはこちら：https://adobe.com/go/sign-umg-overview_jp

4.4.2　考慮すべき点

Acrobat Sign Solutionsは、ユーザーを一意の電子メールアドレスによって識別します。電子メールアドレスは、単一のAcrobat Sign Solutionsアカウントにのみ関連付けることができます。お客様アカウントでユーザーが作成されると、同一の電子メールアドレスを使用してその個人を別のAcrobat Sign Solutionsアカウントに関連付けることはできません。1人の個人が複数のAcrobat Signアカウントのアクティブメンバーになるには、一意の電子メールアドレスが複数必要になります。ユーザーを登録できないエラーは、大抵この要件が原因となっており、アドビのサポートに連絡してユーザーの電子メールアドレスの競合を取り除くことで解決できます。

管理者は、ユーザーページのユーザープロビジョニングレポートを活用することで、ユーザー作成の問題を把握して解決できます。正常にプロビジョニングされなかったユーザーは保留中としてリストされ、問題を解決するための推奨アクションが提案されます。

ユーザーをお客様アカウントに登録する場合は、一意の電子メールアドレスが1人の個人に属することを確認するためのプロセスを事前に実施する必要があります。

また、各個人が組織の要件すべてを満たし、Acrobat Sign Solutionsでユーザーアカウントを割り当てられる前に必要な研修を完了していることを確認するために、適切な手順制御を実施する必要もあります。

否認防止を実現し、不正な署名のリスクを回避するために、21 CFR Part 11は、個人に電子サインを割り当てる前に本人確認をおこなうことを求めています。組織は、ユーザーをお客様アカウントに登録する前に、身元（本人が主張する人物であること）を確認するための適切な本人確認プロセスを実施する必要があります。通常この確認は、お客様またはトラストサービスプロバイダー（TSP）によって1回だけ実施され、正式な身分証明書（パスポート、運転免許証など）またはその他の個人を特定できる情報を確認することで実行されます。実用的な理由から、多くの組織は、社員の採用および入社の手続きの際に本人確認プロセスを実施しています。

送信者が複数のグループメンバーシップを持っている場合、ひとつのグループをそのユーザーのプライマリグループに設定する必要があります。送信者が送信ページにアクセスすると、プライマリグループのプロパティがデフォルトで適用されます。送信者には、プライマリグループを保持するか、署名者のエクスペリエンスとその結果の署名を管理する別のグループ（および関連するグループレベルのプロパティすべて）を選択する責任があります。慎重を期して、送信者が不適切なグループから契約書を送信して規制に準拠しない署名が収集されるという間違いが起こらないよう、バイオ医薬業界標準対応に設定されたグループを送信者のプライマリグループとして割り当てることをお勧めします。

4.5　ユーザー権限の適用と管理

4.5.1　概要

お客様アカウントでユーザーが作成されると、ユーザー設定を編集し、文書への署名（署名者ロール）および署名用文書の送信（送信者ロール）が可能な権限レベルにユーザーを昇格させることができます。さらに、グループ管理者、アカウント管理者、プライバシー管理者のロールなど、より高いレベルの管理者機能を割り当てることも可能です。

ユーザーが確認できるのは関与している契約書（自らが送信した契約書、受信した契約書）だけですが、共有機能を使用すれば、他のユーザーが指定ユーザーに契約書を見せることができます（セクション4.16を参照）。

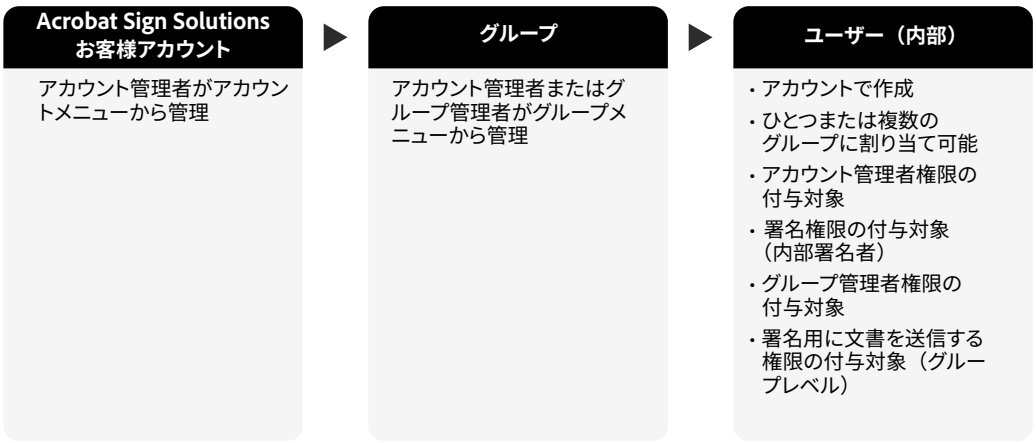


図 2 – Acrobat Sign Solutionsのアカウント、グループ、内部ユーザーの関係

ユーザーの権限レベルの編集について詳しくはこちら：
https://www.adobe.com/go/adobesign-admin-roles_jp

送信者

送信者は、Acrobat Signアプリケーションのインターフェイスを介して1人以上の受信者に契約書を送信する権限を持つユーザーです。送信者のグループに関連付けられた送信設定に応じて文書の署名プロセスが制御されます。送信者が複数のグループのメンバーの場合、送信者はどのグループから契約書を送信するかを指定できます。

署名者

送信者のお客様アカウントのユーザーが電子サインを適用する権限を割り当てられているとき、そのユーザーは内部署名者とみなされます。これらのユーザーのシステムアクセスは制限されています。内部署名者は、Acrobat Signアプリケーションのインターフェイスの管理ページから、自分宛てに送信されたすべての契約書を表示および取得できます。

多くのお客様アカウントでは、署名プロセスにおいて内部署名者がAcrobat Sign Solutionsサービスへの本人確認に組織のIDプロバイダー（IdP）とシングルサインオン（SSO）を使用するよう設定されています。他の認証方法でAcrobat Sign Solutionsサービスへの本人確認を内部署名者に求めるようお客様アカウントを設定することもできますが、そうした認証方法は実用性が低くあまり使用されません。

署名権限を持つお客様アカウントのメンバーでなくても契約書に署名できます。そのため、外部署名者は、別のお客様アカウントのユーザーアカウントを持つ署名者の場合もあれば、Acrobat Signのユーザーアカウントをまったく持っていない署名者の場合もあります。いずれの外部署名者も、Acrobat Sign Solutionsを介して送信された契約書に署名することができます。外部ユーザーは、署名を依頼された契約書にのみアクセスでき、契約書を送信・管理するAcrobat Signのアプリケーションインターフェイスにはアクセスできません。規制に準拠した署名の本人確認を求められた場合、外部署名者はアドビで作成したIDを身分証明として使用できます。外部署名者が利用できる認証方法について詳しくは、セクション4.7を参照してください。

管理者（アカウント、グループ、プライバシー）

アカウント管理者は、アカウント設定とアカウント内の全グループのグループ設定を編集する完全な権限を持っており、また、ユーザーの追加／削除（旧製品のお客様アカウントのみ）、新規グループの作成、グループ管理者の指名をおこなう権限があります。グループ管理者には、グループへのユーザーの追加のほか、グループの設定をアカウントレベルでの設定から変更する権限が与えられます。

グループへのユーザーの追加について詳しくはこちら：
https://www.adobe.com/go/sign-add-users-to-groups_jp

アカウント管理者およびグループ管理者のロールには、複数の個人を割り当てることができます。ただし、グループ管理者は、管理しているグループのメンバーでなければなりません。組織によっては、グループ管理者のロールを使用しないことを選択している場合があります。グループ管理者がいない場合は、アカウント管理者がグループとグループ設定を管理する権限を保持します。

また、アカウント管理者には、アカウントからユーザーや契約書を削除できるプライバシー管理者ロールを割り当てることもできます。プライバシー管理者ロールは、アカウント管理者であるユーザーに対してのみ割り当てられます。

表1：管理者の責任

権限	管理者（Admin Consoleから）	アカウント管理者（Acrobat Sign Solutions内）	グループ管理者
アカウントに新規にユーザーを追加する	X	[x]*	
アカウント内のユーザーを無効化／有効化する	X	[x]*	
アカウントからユーザーを削除する（プライバシー管理者ロールを介して）		X	
ユーザープロファイルを編集する		X	
グループを作成する		X	
グループにユーザーを追加する		X	X

権限	管理者 （Admin Consoleから）	アカウント 管理者（Acrobat Sign Solutions内）	グループ管理者
アカウント管理者ロールをユーザーに割り当てる	X	[x]*	
プライバシー管理者ロールをユーザーに割り当てる	X	[x]*	
グループ管理者ロールをユーザーに割り当てる		X	X
送信者ロールをユーザーに割り当てる		X	X
署名者ロールをユーザーに割り当てる（内部署名者）		X	X
アカウント設定を管理する		X	
グループ設定を管理する		X	X

* Adobe Admin Consoleにアクセスせずにオンボードした旧製品のお客様の場合、ユーザーの追加／削除および管理者権限の割り当てをAcrobat Sign Solutionsのアプリケーションインターフェイス内でおこなえます。

4.5.2　考慮すべき点

GxP対応のビジネスプロセスでは、対象文書に電子サインで署名するためのすべての組織的要件を満たした署名者のみに送信者が署名を要求できるよう、適切な手順制御を実施する必要があります。これらの手順制御には、ユーザー向けの研修や、認証を受けた個人や電子サインの適用が許可された個人を参照できるユーザーアクセスリストの管理などが含まれます。

GxP対応とGxP非対応の両方のビジネスプロセスで契約書の送信にAcrobat Sign Solutionsを使用している場合、21 CFR Part 11の対象となるビジネスプロセスにメンバーが関与する特定のグループに対してバイオ医薬業界標準対応の設定を適用できるようなグループ構造を使用することをお勧めします。署名プロセスでは、送信者のグループに関連付けられた設定が適用されるため、送信者となる個人を、バイオ医薬業界標準対応の設定を使用するグループに割り当てることが重要です。

GxP対応のビジネスプロセスにAcrobat Sign Solutionsを使用している組織では、以下に該当するかどうかを評価することも必要です。

- バイオ医薬業界標準対応の設定が維持され、GxP規制の対象となる文書への署名時に適用されるように、システムの運用とAcrobat Sign Solutionsアカウントの設定の管理方法を制御するための適切なサポートプロセスを実施している。

- バイオ医薬業界標準対応に設定されているグループのユーザーが、GxP対応のビジネスプロセスに関与するための組織の要件すべてを満たすように、制御をおこなっている（例：組織の資格情報を持つユーザー、つまり入社手続きと本人確認を完了しているユーザーにグループメンバーを制限する）。

4.6　署名の種類

4.6.1　概要

Acrobat Sign Solutionsは、ESIGN ACTやeIDAS規制をはじめとする世界中の様々な電子サイン関連規制の要件を満たす電子サインに対応しています。また、証明書によるデジタルIDを使用して署名者の身元を確認する、よりセキュアな適格電子サイン（QES）やデジタル署名にも対応しています。組織は自社のリスク特性やユースケースに最適な署名方法を採用することができます。

電子サインに関する世界の法令について詳しくはこちら：
https://adobe.com/go/trust-compliance-cloud-signatures_jp

証明書ベースのデジタル署名を使用する場合は、外部のトラストサービスプロバイダー（TSP）を選択する必要があります。トラストサービスプロバイダーは、デジタル署名の作成、確認、および検証を担う組織です。Acrobat Sign Solutionsは、Adobe Approved Trust List（AATL）やEuropean Union Trust List（EUTL）で指定されているトラストサービスプロバイダーに対応しています。

認定トラストサービスプロバイダーについて詳しくはこちら：https://www.adobe.com/go/digital-id-providers_jpおよびhttps://adobe.com/go/european-union-trust-lists-govcloud_jp

Acrobat Signアカウントは、クラウド署名、つまり署名者のデジタル証明書がクラウド内に安全に保存されるデジタル署名を受け入れるように設定できます。Acrobat Sign Solutionsは、クラウドベースのデジタル署名のオープンスタンダードを定義する組織であるクラウド署名コンソーシアム（Cloud Signature Consortium）（https://cloudsignatureconsortium.org/）に所属するトラストサービスプロバイダーに対応しています。

クラウドベースのデジタル署名について詳しくはこちら：
https://www.adobe.com/go/adobesign-config-cloud-signature-providers_jp

4.6.2　考慮すべき点

クラウドベースのデジタル署名機能を使用する場合は、外部のトラストサービスプロバイダーを別途選択して料金を支払う必要があります。ベンダー管理手順が品質とサービスの期待値を満たしていることを確認するために、トラストサービスプロバイダーによる正式な評価と適切な調査が必要になる場合もあります。

Acrobat Sign Solutionsのデジタル署名について詳しくはこちら：
https://www.adobe.com/go/adobesign-use-digital-signature_jp

物理的な（紙ベースの）署名を取得せざるを得ないケースもあります。Acrobat Sign Solutionsは、適切にアクセス制御をおこない電子的な処理と監査の利便性を活かしながら、手書き署名の取得に対応するよう設定できます。

手書き署名の取得について詳しくはこちら：
https://adobe.com/go/obtain-written-physical-signature_jp

4.7　電子サインの本人確認方法

4.7.1　概要

本人確認とは、何らかの記録や個人情報を提示して、その人の存在を確認することです。これに対し、ID認証は、本人が主張する人物かどうかを判断するために、その人のIDといくつかの追加情報を検証するプロセスです。最も単純な方法は一要素認証です。これは通常、個人のID要求（ユーザー名など）とひとつの「要素」（通常はパスワード）を照合することで実行されます。多要素認証では、より多くの「要素」を用いることで認証が強化されます。通常、所持情報（トークン、デバイスなど）、知識情報（パスワード、PINなど）、生体情報（指紋、バイオメトリクス）のうち少なくともひとつを必要とします。

Acrobat Sign Solutionsでの本人確認方法について詳しくはこちら：
https://www.adobe.com/go/adobesign-authentication-methods_jp

Acrobat Sign Solutionsは、多様なビジネスプロセスのニーズを満たす柔軟な認証方法を提供するよう設計されています。Acrobat Sign Solutionsでサポートされている本人確認方法は、下表のとおりです。組織は自社のリスク特性やユースケース、予算に最適な認証方法を選択して実施することができます。「プレミアム」認証方法をアプリケーションで使用するには、追加のライセンス条件とサブスクリプション料金が必要です。

表2：ID認証方法

方法	説明	可用性	追加コスト	バイオ医薬業界標準対応の設定による強制認証
一要素				
電子メール認証	受信者が電子メールのリンクにアクセスして、合理的な認証措置を講じる	すべてのサービスプラン	なし	非対応
Acrobat Sign認証	アドビで作成した有効なID（電子メールアドレスとパスワード）でログインして本人確認をおこなうよう受信者に求める	ビジネスレベルとエンタープライズレベルのみ	なし	対応
電子メールによるワンタイムパスコード（OTPvE）	受信者の電子メールの受信トレイから取得した1回限りのパスコードを入力するよう受信者に求める	ビジネスレベルとエンタープライズレベルのみ	なし	対応

二要素				
パスワードベースの認証	契約の設定時に送信者が指定したパスワードを入力するよう受信者に求める	すべてのサービスプラン	なし	非対応
ナレッジベース認証（KBA）	個人的な質問（「あなたの母親の旧姓は？」など）に正しく答えるよう受信者に求める	ビジネスレベルとエンタープライズレベルのみ、米国の受信者のみ	使用に応じた追加料金が必要	非対応
電話認証	SMSまたは音声通話で送信される確認コードを入力するよう受信者に求める	ビジネスレベルとエンタープライズレベルのみ	使用に応じた追加料金が必要	対応
公的証明書	自撮り画像と官公庁発行の証明書（運転免許証、パスポート）の画像を提供するよう受信者に指示する	エンタープライズ版のみ	使用に応じた追加料金が必要	非対応

Acrobat Sign Solutionsは、電子メールアドレスが一意でありパスワード認証されることから、受信者のデフォルトの一要素認証方法として電子メールを使用します。電子メール認証のみを使用して契約書を送信する場合、受信者が電子メールのハイパーリンクをクリックすると契約書が表示され、操作を実行できます（それ以降の認証はなし）。受信者が署名を確定するには、「クリックして署名」ボタンをクリックするだけで済み、それ以降の認証はありません。お客様は適切な管理手順を適用し、情報セキュリティのベストプラクティスに従って電子メールの受信トレイへのアクセスを制御する必要があります。

承認に関連する21 CFR Part 11の要件を満たすには、適切な認証方法が必要となります。電子メール認証は多くのビジネスニーズに対応しますが、署名ごとに認証イベントが必要なビジネスプロセスにはAcrobat Sign認証が適しています。Acrobat Sign認証では、受信者は契約書の内容を表示する前にAcrobat Signへの認証を求められます（Acrobat Sign Solutionsにログイン済みでない場合）。

電子サインで個人を識別する必要がある場合、制御された環境でクラウドベースのデジタル署名を使用することもできます。ビジネスプロセスで証明書ベースのデジタル署名が使用されていない場合、多要素認証を使用するのが賢明です。Acrobat Sign Solutionsは、署名者の本人確認のための二要素認証方法をサポートしています。二要素認証を使用して契約書を送信する場合、ユーザーが電子メールのハイパーリンクをクリックすると、契約書を表示して操作を実行する前に本人確認を求められます。

21 CFR Part 11の対象となるビジネスプロセスでは、署名プロセス中に署名者に有効な資格情報の提供を複数回求めるためにバイオ医薬業界標準対応の設定を使用します。「ID認証を強制」の設定オプションにもとづいて、署名者はまず契約書を開く前、次に署名フィールドをクリックしたとき、最後に「クリックして署名」ボタンを押したときに認証を求められる場合があります。

送信設定で選択したいずれの方法も、契約書の設定時に選択できます。ただし、バイオ医薬業界標準対応の設定にもとづく強制的な認証では、対応している次の認証方法のいずれかが必須であることに送信者は注意する必要があります。

- **電話認証：**電話認証は、署名者を既知の物理的電話デバイスにつなぎ、必要な第2レベルのID認証を提供します。この方法では、署名者がSMSまたは音声通話でスマートフォンに送信されて認証コードを入力することで、契約内容の閲覧と文書への署名が許可されます。電話認証の使用ではコストを考慮する必要があります。この方法を使用すると、追加料金が発生します。この料金はAcrobat Sign Solutionsのライセンス契約に盛り込まれており、サービスのサブスクリプション料金に含まれています。電話認証を使用する前にトランザクションを購入する必要があります。トランザクションは受信者単位で消費されます。

- **Acrobat Sign 認証：**Acrobat Sign 認証は、アカウントの ID プロバイダーを利用するか（SSO が有効な場合）、アドビで作成した ID を認証に使用します。この方法では、署名者が確認済み電子メールアドレスまたは Adobe ID とパスワードから成る有効な資格情報を入力することで、契約内容の閲覧と文書への署名が許可されます。Acrobat Sign 認証の使用に追加料金はかかりません。

- **電子メールによるワンタイムパスワード（OTPvE）認証：**この方法では、署名者が電子メールの受信トレイに送信された認証コードを入力することで、契約内容の閲覧と文書への署名が許可されます。電子メールアドレスはシステムにとって既知であるため、この情報は事前入力されます。OTPvE 認証の使用に追加料金はかかりません。

ID 認証の強制について詳しくはこちら：https://adobe.com/go/enforce-identity-authentication_jp

バイオ医薬業界標準対応の設定では、契約のどのタイミングで署名者に認証を要求するかを指定しますが、エクスペリエンスはアカウントまたはグループの送信設定で指定された ID 認証方法によって決まります。送信設定では、ID 認証や送信ページのその他のパラメーターの基本設定を構成できます。また、送信者が使用できる認証方法を管理者が制御して、デフォルトの方法からの変更を送信者に許可するかどうかを決めることもできます。これらの設定はアカウントレベルに適用されますが、グループレベルで上書きできます。

デフォルトの ID 認証方法は、内部署名者と外部署名者用に定義できます。この 2 種類の署名者ごとにデフォルトの方法を設定し、外部署名者には常に電話認証または Adobe ID の使用を求め、内部署名者には常に SSO を有効にして Acrobat Sign 認証を使用することを求めるといったこともできます。

クラウドベースのデジタル署名機能を使用する場合、選択した ID 認証方法が強制され、署名時にトラストサービスプロバイダーから発行された追加の資格情報（個人識別番号（PIN）、ワンタイムパスワード（OTP）など）を署名者からリクエストされます。

Acrobat Sign Solutions のデジタル ID ゲートウェイは追加の認証オプションを有償で提供しています。デジタル ID ゲートウェイを使用すると、組織は事前設定されたサードパーティのデジタル ID プロバイダー（IdP）を活用し、標準の OpenID Connect（OIDC）認証プロトコルを使用した認証と署名者の ID 検証サービスを利用できます。しかし、現時点ではバイオ医薬業界標準対応の設定による強制的な認証制御をサポートしていないため、デジタル ID ゲートウェイは 21 CFR Part 11 に対応した Acrobat Sign Solutions の実装から除外されています。

Acrobat Sign Solutions のデジタル ID ゲートウェイについて詳しくはこちら：
https://www.adobe.com/go/sign-config-digital-identity_jp

4.7.2　考慮すべき点

適切な ID 認証方法を選択する際にはコストを考慮する必要があります。Acrobat Sign 認証を使用すると、電話認証を実行できないときに、セキュアで費用のかからない方法を提供することができます。Acrobat Sign 認証は、内部署名者と外部署名者の両方に使用できます。

内部受信者は（定義上）お客様アカウントのメンバーであるため、IDを持っています。この場合、プレミアム認証トランザクションに関連する追加コストがかからないため、Acrobat Sign認証を支障なく使用できます。

外部受信者はアドビのIDを持っている場合と持っていない場合があるため、Acrobat Sign認証の使用には独自の課題があります。アドビのIDを持っていない外部受信者は、登録を求められます。これにより、多少の操作の手間が発生し、受信者にフラストレーションが生じる場合があります。外部署名者がIDを持っていない場合は、OTPvE認証（一要素）や電話認証（二要素）が望ましいかもしれません。

シナリオ1：受信者が内部署名者

内部署名者の本人確認には、組織のSSO機能が最適です。Acrobat Sign Solutionsと連携するよう設定された自社のIDプロバイダー（IdP）を使用すれば、ID認証を明確かつ簡潔に実行できます。SSOは、ソフトウェアアプリケーションへのユーザーのアクセスをより厳密に制御する必要があるエンタープライズレベルのお客様や組織にとって、理想的な選択です。詳しくはセクション4.8を参照してください。

組織によっては、SSOの実装を妨げるポリシーや技術的制約があります。そのような場合は、Acrobat Sign認証を使用するよう設定し、確認済み電子メールアドレスとパスワード（アドビのID）を使用して認証するよう受信者に求めることができます。

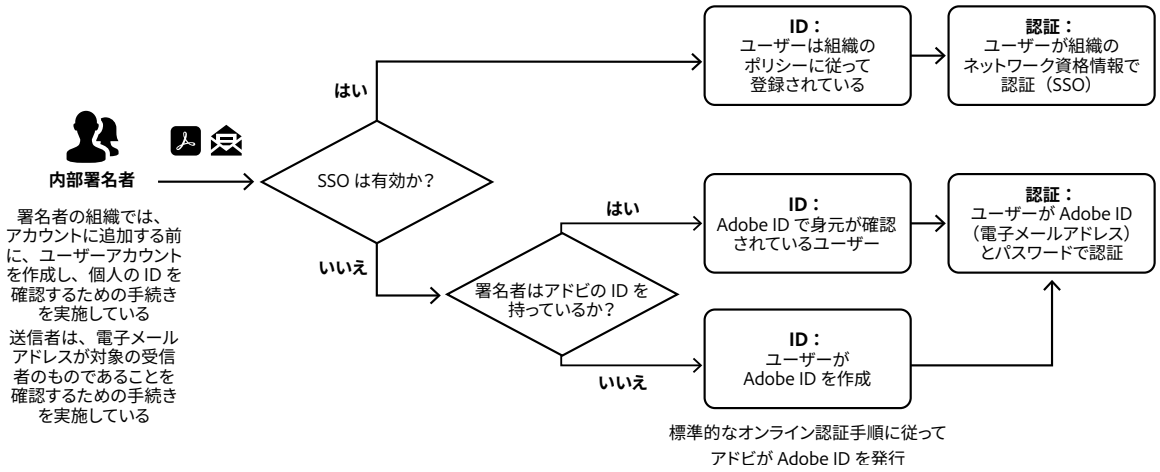


図3 – 内部署名者の認証プロセス

シナリオ2：受信者が外部署名者

外部署名者の電話番号がわかっており、それが本人のものであることが確認されている場合、電話認証の使用が最適です。送信者は、送信時に受信者の電話番号を把握している必要があります。受信者の電話番号は、契約の設定時に送信者によって入力されます。外部署名者が文書に電子的に署名するには、電子メールのリンクから契約書にアクセスする必要があります。受信者の電子メールアドレスは一意でありパスワード認証されるため、電子メールリンクへのアクセスは、本人確認の合理的な手段となります。受信者が契約内容を確認するには、システムによって生成され電話番号に送信される確認コードを入力する必要があります。署名者は、確認コードを受け取る手段としてSMS（テキストメッセージ）または音声通話を選択できます。ユーザー認証が必要になるたびに新しい検証コードがシステムによって生成されるため、電話認証では同じ資格情報の組み合わせが複数の署名アクティビティで使用されることはありません。

受信者が外部署名者で、電話番号がわからない場合や費用の問題がある場合は、Acrobat Sign認証を利用できます。署名時の認証に対応する新しい個人用ID（Adobe ID）をアドビが提供します。署名者がアドビのIDを持っていない場合、契約書を表示する権限を得るためにIDを作成するよう求められます。IDの作成には、個人の電子メールアドレスの登録と確認に加え、アカウントへの電話番号の関連付け（パスワードを復元しやすくするため）が必要です。IDは無料で、必要に応じて他のアドビの製品やサービスにアクセスするために使用することができます。ただし、署名以降にアドビの製品やサービスを利用する義務はありません。これは推奨される方法ではありませんが、一部のお客様では、この方法を適切なプロセスと組み合わせて個人の本人確認をおこなっています。詳しくはセクション4.9を参照してください。

OTPvE認証は、外部署名者向けに利用でき、追加費用がかからないもうひとつの選択肢です。この方法では、ユーザーはアドビでIDを作成する必要がありません。受信者は電子メールの受信トレイにアクセスするだけで済み、Acrobat Sign認証で生じる可能性のある摩擦の多くが解消されます。

個人の場合、契約書の送信元であるお客様アカウント内のライセンスユーザーではないため、外部署名者とみなされます。ただし、個人であっても、異なるお客様エンティティに属するAcrobat Sign Solutionsアカウントのメンバーである可能性があります。署名者が属するアカウントにSSOが設定されていれば、署名者は所属する組織のネットワーク資格情報を使用して認証をおこなうことができます。

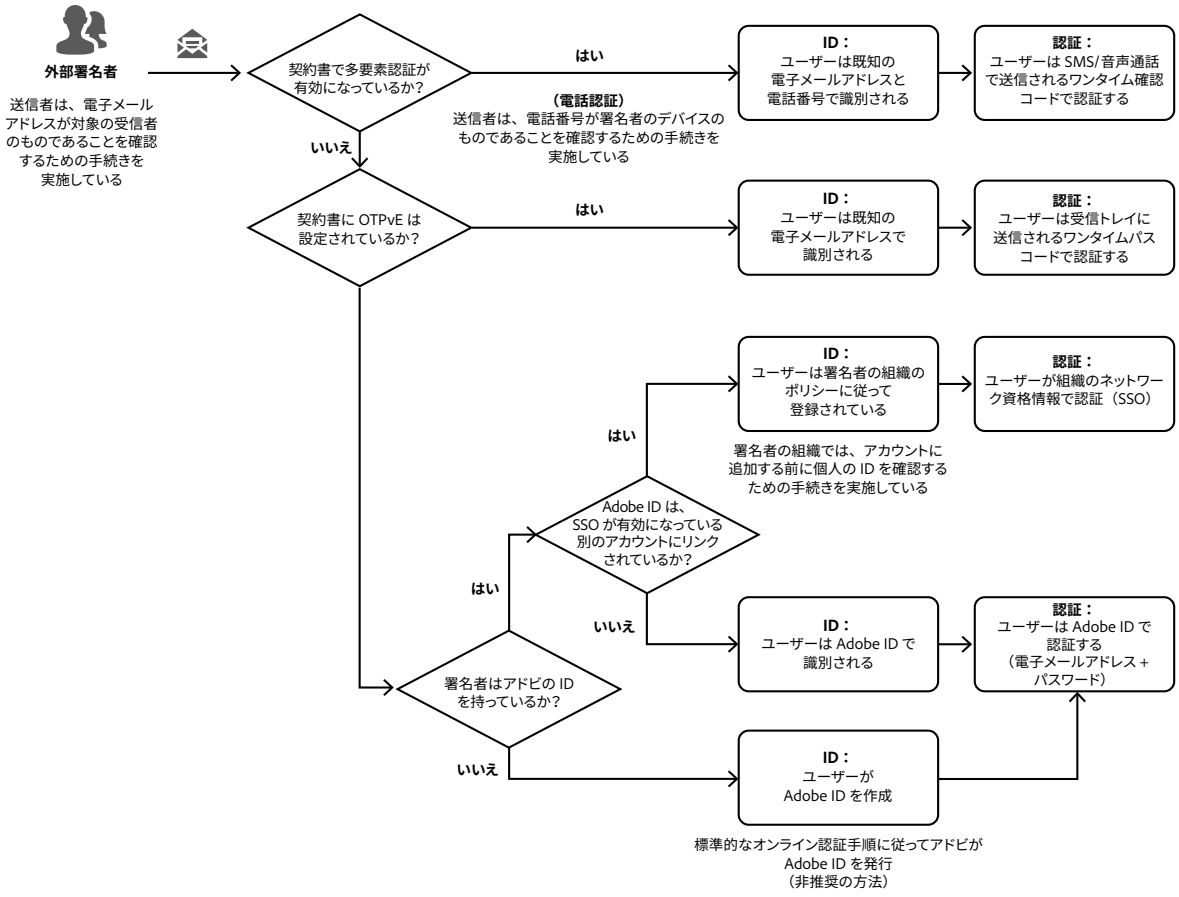


図4 – 外部署名者の認証プロセス

4.8　ユーザー認証にシングルサインオン（SSO）を使用する

4.8.1　概要

Admin Console で Acrobat Sign Solutions アカウントを管理する際、管理者はアカウントを設定して、SSO に使用する Federated ID を介してログインに使用するドメインを設定することができます。ドメインが確認されると、このドメインを含むディレクトリが設定され、Microsoft Azure、Google Federation、Okta などの ID プロバイダー（IdP）を介して、ドメイン内の電子メールアドレスを使用して Acrobat Sign Solutions にログインできるようになります。

Adobe Admin Console での ID の設定について詳しくはこちら：
https://helpx.adobe.com/jp/enterprise/using/set-up-identity.html

既存のディレクトリに対するユーザーアカウントの自動作成は、ジャストインタイム（JIT）プロビジョニングを有効にすることで容易におこなうことができます。有効にすると、お客様は、管理者による追加のアクションなしで、Adobe Acrobat Sign 製品の使用権限をフェデレーションユーザーに割り当てる自動割り当てルールを設定できます。

ジャストインタイム（JIT）プロビジョニングについて詳しくはこちら：
https://helpx.adobe.com/jp/sign/admin/jit-via-sso.html

Adobe Admin Console を使用していない場合、管理者は Acrobat Sign Solutions アプリケーション内の SAML 設定を構成できます。これにより、アカウントのユーザー認証に SSO を使用することができます。SAML 設定はアカウントレベルにのみ適用され、グループレベルでは上書きされません。SAML 設定を適用するには、エンタープライズ版が必要です。

4.8.2　考慮すべき点

Federated ID は、組織で既に使用している ID 管理システムにもとづいて、認証とユーザーを厳格に制御したいお客様に推奨します。組織のディレクトリサービスを使用して、内部ユーザーのパスワードとユーザーアカウントロックアウトポリシーを管理することができます。ログを監視することで、ユーザーアカウントから異常なアクティビティや疑わしいアクティビティを検知し、報告することができます。さらに、エンドユーザーの観点から見ると、エンドユーザーは使い慣れている組織の標準 SSO エクスペリエンスにリダイレクトされるため、ログインプロセスがより迅速かつ簡単になります。

SSO を使用しない場合、Acrobat Sign Solutions サービス内で作成されたユーザーアカウントの資格情報を使用してユーザー認証をおこないます。このモードでは、ユーザーアカウントを作成すると、Acrobat Sign Solutions にログインしてライセンス使用権限に同意するよう求める通知が表示されます。

法人向けサービスプランは SSO をサポートしていません。エンタープライズ版が必要となります。

Adobe Admin Console で ID プロバイダー（IdP）を使ってシングルサインオン（SSO）を設定する方法について詳しくはこちら：
https://helpx.adobe.com/jp/enterprise/using/sso-overview.html

4.9　外部署名者の留意点

4.9.1　概要

Acrobat Sign Solutionsでは、アカウントのメンバーシップにもとづいて、契約書の受信者が組織に属しているかどうかを判断します。外部署名者とは、契約書の送信元であるAcrobat Sign Solutionsアカウントのユーザーではない受信者です。

外部署名者に文書を送信することは、内部署名者に契約書を送信することと何ら変わりはありません。送信者はAcrobat Sign Solutions内の送信インターフェイスにアクセスし、受信者（内部署名者または外部署名者）を識別するための電子メールアドレスを指定し、意図した署名者のリストに追加します。

送信者は、希望する認証方法を指定する必要がありますが、外部署名者が内部署名者と異なる認証方法を要求する可能性があることに留意してください。内部署名者と外部署名者の送信設定で定義されたデフォルトのID認証メソッドを使用すると、このような負担を軽減できます。外部署名者が利用できる認証方法について詳しくは、セクション4.7を参照してください。

4.9.2　考慮すべき点

外部署名者が署名プロセスに参加できるようにするために必要な設定はほとんどありません。ただし、外部署名者はお客様のアカウントのメンバーではないため、外部署名者が規制された署名プロセスに参加するためには、多要素認証方式を使用する必要があります。コスト、リスク、署名プロセスのコンプライアンス要件など、様々な要素に応じて、選択する認証方式は異なります。

公的な臨床試験など、何千人もの外部署名者が参加する場合には、アドビで作成したIDを使用したAcrobat Sign認証が実用的な選択肢だと言えます。より円滑なユーザーエクスペリエンスが求められる場合は、OTPvE認証をお勧めします。この方法では、受信者の電子メールだけがわかっている場合、費用をかけずに受信者の身元を確認することができます。また、既知の受信者の数が少なく、ビジネス価値が高い場合には、電話認証が適切である可能性があります。

特定の個人が、署名リクエストの受信と実行に使用された電子メールアドレスと電話番号（該当する場合）の真の所有者であることを確認するために、所定の手順を実施する必要があります。認証方式にかかわらず、公的な身分証明書やその他の個人を特定できる情報を確認することで、個人の身元を特定する（つまり、その人が本人である）プロセスの実施が必要です。特にこの点に注意して、外部受信者にAcrobat Sign認証方式を使用してください。受信者がまだアドビのIDをお持ちでない場合は、登録が必要です。Adobe IDは、電子メールアドレスがあれば、標準的なオンライン認証の手順に従って誰でも作成できますが、本人確認プロセスはありません。

GxP対応のビジネスプロセスでは、身元確認が完了し、他の組織的要件を満たした署名者のみに送信者が署名を要求するために、適切な手順制御を実施する必要があります。これらの手順制御には、送信者向けの研修や、認証を受けた個人や電子サインの適用が許可された個人を参照できるユーザーアクセスリストの管理などが含まれます。

アカウントや組織を代表して行動する個人（請負業者やベンダーなど）の場合は、外部署名者としてではなく、お客様アカウントにオンボードして、内部署名者として参加することができます。このような個人は、GxPプロセスの一環として文書に署名することを許可するすべてのビジネスおよび規制要件を満たすために、組織のセキュリティポリシーと品質システムの手続きに関する研修を受ける必要があります。この方法は、Acrobat Sign Solutionsを複数のインスタンスで使用することが想定される場合、特に実用的であると考えられます。

4.10　契約書の設定

4.10.1　概要

署名用の文書を送信する権限を持つ承認されたユーザーのみが、Acrobat Sign アプリケーションインターフェイスの送信ページにアクセスできます。このページで、送信者は対象の受信者を指定し、署名のために回覧するファイルを選択します。

お客様アカウントで「複数グループのユーザー」機能が有効になっている場合、グループセレクターが使用できるようになります。送信者には、どのグループから契約書を送信するかを選択する権限と責任があります。21 CFR Part 11の要件に準拠した署名を取得するために、送信者はバイオ医薬業界標準対応の設定を使用して構成されたグループから契約書を送信する必要があります。

契約書の送信について詳しくはこちら：
https://helpx.adobe.com/jp/sign/using/sending/overview.html

標準の送信ページを使用して、1人以上の受信者を指定したり、自分自身を唯一の署名者に設定したりできます。後者は、構造化された自己署名ワークフローの代替方法であり、送信者が他の受信者を設定することなく単独でドキュメントに署名する必要がある場合に使用できます。

Acrobat Sign Solutionsは、送信者が契約書に添付するファイルを選択できる場所を許可または制限するよう設定できます。ファイルは、送信者のローカルシステム、クラウドベースのストレージ（Google ドキュメント、Box、Dropbox、OneDrive）、またはAcrobat Sign ライブラリから添付できます。いくつかのドキュメントおよび画像ファイル形式がサポートされています。

署名用に文書の送信準備をする際、送信者はオーサリング環境にアクセスして文書をプレビューし、署名のプレースホルダーとして必要な署名フィールドを挿入しておく必要があります。様々なタイプの電子サインフィールドを文書上に配置することができますが、適切なタイプを選択し、21 CFR Part 11に従って署名内容に必要なすべての要素が表示されるようにします。

電子サインを使用する場合、送信者は署名タイプまたは署名ブロックタイプの電子サインフィールドを挿入する必要があります。各署名者には、1つの文書に1つ以上の電子サインフィールドを割り当てます。「バイオ医薬業界標準対応の設定」を設定すると、署名ブロックには、署名者の電子メールアドレスのほか、すべての必要な情報（署名者の印字氏名、日付とタイムスタンプ、署名の理由）が表示されるようになります。

証明書ベースのデジタル署名を使用する場合、送信者はオーサリング環境にアクセスし、文書にデジタル署名フィールドを挿入する必要があります。クラウドベースの署名の場合は、受信者ごとに最大10個のデジタル署名フィールドに対応できます。

送信者がオーサリング環境で署名フィールドを配置しない場合、システムによって割り当てられた位置に、署名者用の電子サインブロックフィールドが自動的に設定されます。

フィールドタイプについて詳しくはこちら：https://helpx.adobe.com/jp/sign/using/field-types.html

4.10.2 考慮すべき点

Acrobat Sign Solutionsには、通常の使用量に対応し、適切なパフォーマンスしきい値を確保するためのデフォルトの制限があります。送信者は、アップロードされたファイルが、許容されるファイルサイズの制限と、アドビが適用する総ページ数のしきい値を超えないようにする必要があります。送信者は、トランザクションに追加できる受信者数の割り当てを把握しておく必要があります。

トランザクションの制限について詳しくはこちら：
https://helpx.adobe.com/jp/sign/using/transaction-limits.html

署名のために契約書が送信され、送信後に契約書に何らかの変更を加える必要があることに気付いた場合、契約書の変更や受信者のリストの調整を可能にするいくつかのオプションが用意されています。

- Acrobat Sign Solutionsは、送信者が受信者を置き換えることができるように設定できます。このオプションを使用すると、送信者は受信者の電子メールアドレスを別の受信者の電子メールアドレスに置き換えることにより、契約書に対するアクション（署名、承認、委任、キャンセルなど）をまだ完了していない受信者を更新できます。

- 1人の受信者を単純に削除するオプションはありません。ただし、Acrobat Sign Solutionsは、送信者が代替受信者を追加できるように設定できます。これにより、元の受信者が契約書に参加できる状態のまま、新しい受信者は契約書に対してアクションを実行できます。受信者の置き換えは監査レポートに反映されます。

- Acrobat Sign Solutionsは、送信者が契約書を変更できるように設定できます。これにより、文書やフォームフィールドの追加、削除、並べ替えなど、様々な種類の変更をおこなうことができます。いくつかの制約があることに注意してください。契約書にデジタル署名が含まれている場合、送信中の契約書を変更することはできません。また、受信者が既に契約書に対してアクションを実行した場合も変更できません。

- 送信者は、完了前であればいつでも契約書をキャンセルできます。キャンセルされた場合、契約書は無効となり、これは監査レポートに記録されます。一度無効になると、送信者は契約書をやり直すことはできません。新しい契約書を開始する必要があります。すべての受信者が署名を実行すると、契約書は完了し、キャンセルはできなくなります。

- Acrobat Sign Solutionsは、受信者に署名を拒否するオプションを提供するように設定できます。拒否された場合、契約書は無効となり、これは監査レポートに記録されます。一度無効になると、送信者は契約書をやり直すことはできません。新しい契約書を開始する必要があります。

4.11 バイオ医薬業界標準対応の設定を使用して署名内容を設定する

4.11.1 概要

バイオ医薬業界標準対応の設定を使用する場合、署名内容のレイアウトが暗黙的に変更されます。バイオ医薬業界標準対応の設定では、21 CFR Part 11で義務付けられている次のコンポーネントを各署名内容に含めるように設定できます。

- 署名者の印字氏名
- 署名が適用された日時
- 署名の意味（署名の理由）

これらの情報は、署名済み文書の電子ディスプレイおよび紙の印刷物に、人間が判読できる形で表示されます。

バイオ医薬業界標準対応の設定について詳しくはこちら：
https://helpx.adobe.com/jp/sign/using/bio-pharma-settings-configuration.html

署名者の印字氏名

内部署名者の場合、署名内容に記載される署名者の名前は、Acrobat Signのユーザープロファイルに登録されている氏名に対応します（Acrobat Sign認証方式を使用する場合）。署名者が名前を編集できないように設定することができます。

外部署名者の場合、署名者本人が署名時にフルネームを入力するよう求められます。入力された名前は署名内容に表示されます。契約書を設定するときに送信者が受信者の名前を事前入力し、受信者がその名前を変更できないようにするオプションが用意されています。

受信者の名前について詳しくはこちら：
https://helpx.adobe.com/jp/sign/config/send-settings/require-recipient-name.html

証明書ベースのデジタル署名を使用する場合、署名者の名前は、署名者のデジタルIDと一致します。

署名が適用された日時

署名者が「クリックして署名」ボタンを押すと、署名内容にタイムスタンプが適用されます。この行為は、署名者が肯定的に承認し、署名を意図的におこなっていることを意味します。この時点で、ファイルは「ロック」された状態になり、署名動作を保存するために監査証跡にエントリーが記録されます。1つの契約書に複数の署名をおこなう場合、署名者は契約書の最後の最終署名で、クリックして署名ボタンを1度だけ押します。署名者の署名は文書内の複数の場所に表示されますが、これらの署名内容は実質的に1つの署名イベントを表していることに注意してください。署名フィールドに記載されるタイムスタンプは、クリックして署名ボタンが押された時刻に更新されます。クリックして署名ボタンが操作された時点を反映するため、監査証跡には1件のエントリーのみが記録されます。運用上、署名アクティビティを連続的または時系列的におこなうことが義務付けられている場合、一度に複数回の署名をおこなうことが適切でない場合もあります。そのような場合、Acrobat Sign内蔵のワークフロー機能を活用して署名イベントの順序を強制し、契約を設定する際に送信者が指定する署名順序を制御する方がより適切だと考えられます。

署名内容の日付とタイムスタンプは標準形式で記録されます。日付形式とタイムゾーン設定の管理については、セクション4.14を参照してください。

署名の意味（署名の理由）

バイオ医薬業界標準対応の設定では、署名者に署名の理由を要求するように設定できます。さらに、理由の選択リストを設定でき、ここには、署名者が自分で理由を入力する項目を含めることもできます。署名時に、署名者は署名の理由を入力するよう求められ、理由が入力されない限り署名を完了できません。理由を入力すると、「クリックして署名」ボタンが表示されます。電子サインを適用するには、署名者は「クリックして署名」ボタンを押した後、再認証する必要があります。

署名の理由の要求について詳しくはこちら：
https://helpx.adobe.com/jp/sign/using/reason-for-signature.html

4.11.2　考慮すべき点

バイオ医薬業界標準対応の設定をグループレベルで構成します。バイオ医薬業界標準対応の設定では、アカウントレベルで署名の理由を指定できます。グループレベルで意図的に上書きされない限り、すべてのグループに適用されます。そのため、アカウントレベルで設定された署名の理由は、すべてのグループに適用され、グループレベルで設定された署名の理由はそのリストに追加されることになります。

署名理由のリストを設定するときに、各理由を言語ごとに分類できます。署名時に、署名者のロケールの言語と一致する理由のみが、署名者による選択のために提示されます。送信者が契約書を設定するときに署名の言語を指定することもでき、これにより受信者向けに言語でフィルタリングされた理由のリストが作成されます。固有の言語要件のある異なる地域でデプロイする場合、この機能を利用して複数の言語で理由を指定することができます。

署名理由のテキストの長さには制限があります。署名内容のフォントサイズは署名フィールドに収まるように調整されるため、署名内容のフォントサイズを読みやすくするために、署名理由のテキストはできるだけ短くすることをお勧めします。

署名理由について詳しくはこちら：
https://helpx.adobe.com/jp/sign/using/reason-for-signature.html

以下の手順に従って、正しい名前が署名内容に組み込まれるように制御を実装します。

- 内部署名者の場合、ユーザープロファイル情報を管理するための手順と制御を実装する必要があります。SSO認証に使用するID管理システム内の情報とユーザー名を同期させるツールの利用を検討してください。また、署名時に署名パネルの名前を変更できないよう、「署名の環境設定」を設定することも有効です。

- 外部署名者については、署名時に完全かつ正確な名前を記載することの重要性を、その個人が確実に理解できるように、適切な手順を実施する必要があります。

すべての署名者は、いかなる契約書であっても署名する責任を理解し、21 CFR Part 11に準拠した署名には、署名の理由が必要であることを認識する必要があります。

4.12　署名の委任

4.12.1　概要

委任に関する設定は、グループ設定でおこなうことができ、特定のグループに対して委任を完全に禁止できます。委任は、内部署名者のみ、外部署名者のみ、またはその両方に対して許可されるように制御できます。

内部署名者が委任を許可されている場合、追加の設定を適用することで、署名を次の者に委任できるよう制御することができます。

- お客様アカウントのユーザーのみ（内部署名者）
- お客様アカウント内外のすべてのユーザー

外部署名者が委任を許可されている場合、署名は誰にでも委任することができます。

受信者が署名リクエストを通じて委任するか、または自動委任を設定することもできます。新しい署名者に署名が委任されると、送信者は電子メールで通知を受け取ります。自動委任は、ユーザー、アカウント管理者、グループ管理者のいずれかが設定できます。自動委任が削除されるまで、すべての署名リクエストは委任された署名者に自動的に送信されます。

4.12.2　考慮すべき点

委任が許可されている場合、ビジネスプロセスのどの時点で、誰に署名を委任することができるのか、手順制御を明確にする必要があります。プロセスを制御することで、電子サインを使用して管理文書に署名する権限のない個人に、署名リクエストが委任されるリスクを軽減できます。

4.13　監査証跡機能

4.13.1　概要

Acrobat Sign Solutionsでは、システムが自動で監査レポートを生成しますが、これには電子サインの収集プロセスに関する一連のイベントも含まれます。監査レポートには、手書き署名が提出された時、署名が委任された時、契約書が解除になった時、署名者が署名リクエストを拒否した時などの情報も記録されます。監査レポートの項目は、正常に適用された電子サインに関連付けられており、以下の情報が含まれます。

- 署名者の名前と電子メールアドレス
- 署名日時
- 署名の理由

さらに、各認証イベントは監査レポートに記録され、使用された認証の種類が明示的に反映されます。

署名が拒否または契約書が解除された場合、その理由も監査レポートに記録されます。

送信者には、契約書の受信者に定期的または臨時でリマインダーを送信するオプションが用意されています。必要であれば、監査レポートにイベントのリマインダーを含めるようにお客様アカウントを設定することができます。

監査レポートには、署名された文書を閲覧するために使用したデバイスのIPアドレスと、署名のタイムスタンプを記録するために使用したタイムサーバーのIPアドレスも記録されます。

監査レポートは署名された文書に関連付けられ、管理ページに表示される契約オブジェクトとは別に保存されます。契約書に参加している送信者と内部署名者は、監査レポートと関連する署名済み文書を、管理ページのインターフェイスから2つの異なるPDFとして取得できます。これらは、契約書のトランザクションIDを介してリンクされています。管理ページからは、監査レポートと契約書を1つのPDFに結合した文書を取得することもできます。

オプションとして、契約書が最終的なものになった時点で、参加者に送信する電子メールの添付ファイルとして監査レポートのコピーと関連する署名済みPDFを含めるように設定することもできます。電子メールの添付ファイルを一部の受信者に限定して送信するか、またはすべての受信者（送信者、内部署名者、外部署名者）に送信するかを設定できます。

監査レポートについて詳しくはこちら：
https://helpx.adobe.com/jp/sign/using/audit-reports-transaction-history.html

管理ページでオブジェクトを非表示にしても、監査レポートは削除されません。トランザクションIDがわかっていれば、いつでもその監査レポートを確認できます。

監査レポートに記録されたイベントは、Acrobat Sign Solutionsアプリケーション内で動的に生成されるアクティビティリストにオンライン表示されます。アクティビティリストは契約書の一要素であり、契約を解除する明示的なアクションによって破棄されます。契約書を削除するとアクティビティ履歴も失われ、復元はできません。監査レポートの削除を除き、お客様が定義した保持ルールにもとづいてシステムアクションによって契約書が削除された場合は、例外である可能性があります。詳しくはセクション4.15を参照してください。

4.13.2 考慮すべき点

署名者個人がひとつの契約書内の異なる署名フィールドに複数の署名を適用する必要がある場合、一連の署名に対して署名者が「クリックして署名」ボタンを操作した時点を反映するために、監査証明には1つのエントリーのみが記録されることに注意してください。ユーザーが個別の署名フィールドで異なる理由を選択した場合、監査レポートには複数の理由が選択されたことが表示されますが、それぞれの理由は一覧表示されません。

署名用の複数の文書を1つの契約書の一部としてルーティングすることが可能です。Acrobat Sign Solutionsではデフォルトで、署名者に送信する前に個別のファイルを結合します。契約が完了した時点でファイルを分離するよう設定することができます。ただし、契約書全体に対して生成されるのは1つの監査レポートのみで、個別の文書名は明記されません。独自に署名された文書とその監査レポートを取得したい場合、送信者は、契約書ごとに1つの文書をアップロードする必要があります。

Acrobat Sign Solutionsから署名済み文書と関連する監査レポートを取得するにあたっての注意事項については、セクション4.15を参照してください。

4.14　日付とタイムゾーンの設定

4.14.1　概要

電子サインを適用する場合、すべての日付とタイムスタンプは、アドビサーバーの時刻を使用して記録されます。アドビサーバーでは、NTP プールプロジェクトを使用して、既知の信頼できる外部ソースと時刻同期をおこなっています。

デジタル署名の場合、信頼できるプロバイダーからのデジタル証明書とタイムスタンプを使用して、公開鍵基盤（PKI）によって文書に埋め込まれる署名を作成します。

監査レポートでは、日付とタイムスタンプの形式は「YYYY-MM-DD - HH:mm:ss AM/PM [タイムゾーン]」に設定されており、これを変更することはできません。監査レポートには、デフォルトですべてのイベントがグリニッジ標準時タイムゾーンに標準化されて表示されますが、グローバル設定（アカウントレベル）またはグループ設定（グループレベル）で異なるタイムゾーンを使用するように設定することもできます。

署名内容では、タイムスタンプに表示されるタイムゾーンは署名者のタイムゾーンに対応し（タイムゾーンオフセットを含む協定世界時で表示）、これを変更することはできません。

4.14.2　考慮すべき点

署名内容の日付と時刻の形式はAcrobat Sign Solutionsによって設定されるため、お客様が適用する構成設定に従うことはありません。そのため、Acrobat Sign Solutionsに強制される日付と時刻の形式が、日付と時刻の記録に関する社内ポリシーに従って承認されていることを確認することが重要です。

4.15　署名記録の管理

4.15.1　概要

Acrobat Sign Solutionsを使用してすべての署名が文書に適用されると、署名記録と監査レポートが利用可能になったことを通知する電子メールがすべての関係者に送信されます。この電子メールには、署名記録へのハイパーリンクを含めるように設定することができます。送信者と内部署名者は、電子メール内のハイパーリンクから、またはAcrobat Sign Solutionsインターフェイスの管理ページから直接、署名記録にアクセスできます。外部署名者は、（電子メールに含まれている場合）ハイパーリンク経由でのみ、署名記録にアクセスできます。

コンテンツ保護設定は、内部署名者と外部署名者に対して個別に有効にすることができます。保護された契約書を表示しようとすると、ユーザーは署名された契約書を表示する前に認証を求められます。署名者は、契約書で元々割り当てられていた認証方法を使用して認証するよう求められます。コンテンツ保護を使用する場合、システムから送信される電子メールに添付ファイルは含まれません。これにより、セキュリティが強化され、署名された契約書にアクセスするためのベストプラクティスに従うことができます。

コンテンツ保護について詳しくはこちら：
https://adobe.com/go/sign-config-content-protection_jp

また、グローバル設定（アカウントレベル）またはグループ設定（グループレベル）で、契約完了時に一部またはすべての参加者（送信者、内部署名者、外部署名者）に署名記録と監査レポートを添付して電子メールを送信することもできます。電子メールは署名済み文書にアクセスするための便利な手段ですが、電子メールを介した署名記録のルーティングを禁止する内部情報保護および機密保持のポリシーに留意する必要があります。

Acrobat Sign Solutionsでは、転送中と保存中に文書とアセットを暗号化します。Acrobat Sign Solutionsのすべての文書は、アドビが管理するデータ層（データベースとファイルストア）内に安全に保存されます。バックアップ管理と障害回復プロセスは定期的にテストされています。

Acrobat Sign Solutionsでは、契約書を安全に保管することができますが、このシステムは記録管理に特化しているわけではありません。署名記録と監査レポートを取得して、電子記録の管理に使用している外部システムで保管することができます。ユーザーインターフェイスから直接、またはAPIを利用しておこないます。文書はAcrobat Sign Solutionsインターフェイスから PDF として抽出できます。認証、シールされるため、作成元の証明と完全性が確保されます。

デフォルトでは、お客様アカウントがアクティブである限り、すべてのお客様文書はAcrobat Sign Solutionsに保存されます。契約書を削除する明確なアクションを取るまで、データは削除されません。

アカウント管理者は、データガバナンスポリシーをアカウントに構成することで、保持ルールを作成できます。保持ルールには、契約書、トランザクション、およびそれに伴う監査情報と個人情報がAcrobat Sign Solutionsから自動的に削除されるまでの期間を定義できます。

保持規則を作成する際に、関連する監査証跡の保持期間を明確に定義することができます。このオプションを有効にしない場合、契約書の一部として提供した文書、ファイル、添付ファイルのみが削除されます。監査証跡と個人情報は削除されません。トランザクションIDがわかっていれば、いつでも契約書が交わされたことを確認できます。

データガバナンスと保持について詳しくはこちら：
https://adobe.com/go/adobesign_document_retention_guide_jp

さらに、Acrobat Sign Solutionsでは、一般データ保護規則（GDPR）に準拠するための機能を提供しています。トップレベルのプライバシー管理者権限を付与されたユーザーは、指定された目的を果たしたと判断された後、アカウント内で任意のユーザーが作成した元の契約書を閲覧、削除する権限を持ちます。プライバシー管理者は、Acrobat Sign Solutionsから取消不能の形で元の契約書を削除でき、契約書の履歴もそれに伴って削除されます。お客様は、Acrobat Sign Solutionsの外部で取得および保持される契約書のコピーの安全な保管、配布、および削除を管理するための追加の制御と手順を実装する必要があります。

GDPR要件への準拠について詳しくはこちら：
https://adobe.com/go/sign-gdpr-overview-govcloud_jp

4.15.2 考慮すべき点

Acrobat Sign Solutionsが使用されるGxP対応のビジネスプロセスには、署名後の署名記録と監査レポートの回収を含め、これらの適切なファイリングを保証する必要があります。お客様にはこれらの記録について説明責任があり、記録が適時に回収されるように手続き上の制御を実装する必要があります。

4.16　アカウントと契約書の共有

4.16.1 概要

Acrobat Sign Solutionsは、ユーザーのコンテンツ（契約書、テンプレート、レポート）を他のすべてのユーザーから保護するように設計されています。ただし、これらのコンテンツの閲覧や操作が明示的に求められる場合を除きます。組織のフレームワークによっては、他の個人やロール（ラインマネージャー、文書制御チームなど）が、契約書の参加者（送信者または署名者）にならずに、契約書の進捗を監視することが必要な場合があります。このような場合は、共有オプションを利用してコンテンツを公開することができます。

アカウント共有機能は、あるユーザーのコンテンツを、お客様アカウント内の他のユーザーと共有する必要がある場合に使用します。この機能により、共有ユーザーの契約書を永続的に開示することができます。基本的なアカウント共有機能により、共有者は、共有ユーザーの管理ページのコンテンツ（処理中、完了、解除状態の契約書と監査レポート）に表示専用でアクセスできます。高度なアカウント共有機能では、共有者は、すべてのコンテンツの閲覧、処理中の契約書の変更、共有ユーザーの代理としての契約書の送信がおこなえます。

アカウントの共有について詳しくはこちら：https://adobe.com/go/adobesign-share-accounts_jp

特定のトランザクションについては可視化する必要があるが、共有ユーザーの契約書のリスト全体を常に閲覧する必要がない場合、契約書の共有機能を活用できます。内部ユーザーのみ、外部ユーザーのみ、またはその両方との契約書の共有を許可する制御があります。他の内部ユーザーと契約書を共有すると、共有ユーザーの管理ページに契約書が表示され、進行中の契約書を確認し、監視することができます。契約書を共有する際、受信者は現在の状態の契約書のPDFコピーを含む電子メールを受け取ります。共有した後、契約書の共有を解除することができます。この場合、共有していたユーザーの管理ページからは契約書が削除されますが、共有を解除しても、契約書のPDFコピーが添付された電子メールの送信は取り消されません。この問題は、コンテンツ保護コントロールを使用することで回避できる場合があります。コンテンツ保護が有効になっている場合、添付ファイルは電子メールに含まれず、ユーザーは署名済みの契約書を表示する前に認証手順を実行する必要があります。

契約書の共有について詳しくはこちら：
https://adobe.com/go/adobesign-share-agreement_jp

契約書の共有解除について詳しくはこちら：
https://adobe.com/go/adobesign-unshare-agreement_jp

契約書を共有する他の方法として、契約書の受取人を指定する際に、CCフィールドに個人の電子メールアドレスを入力することもできます。CCフィールドは、契約書を設定する時に送信者だけが入力できます。

4.16.2 考慮すべき点

適切な共有ルールを定義して、記録の機密性と完全性を不正アクセスから保護しない限り、契約書の共有を有効にしないでください。

4.17 入力可能なFDAフォームフィールドへの署名

4.17.1 概要

FDAに提出する入力可能なフォームフィールドの中には、提出前に署名が必要なものがあります（フォーム番号1571、1572、0356hなど）。これらのフォームを使用する場合、フォームがAcrobat Sign Solutionsにアップロードされると、データセキュリティ対策によりフォームからビジネスロジックが削除されることに注意してください。FDAには、様々なツールを使用してフォームからデータやテキストを抽出するチームがあるため、フォームをライブデータのままで要求するFDAにとって、このことは課題になります。

4.17.2 考慮すべき点

Acrobat Sign Solutionsで処理した後、フォームがフラット化されていることが判明した場合、FDAはフォームのコピー2部を提出することを推奨しています。(1) 記入済みかつ電子サイン済みのフォームと (2) 署名されていないオリジナルのフォームが、データ抽出用の作業用コピーとして使用されます。

Adobe Acrobatデスクトップアプリ（利用可能な場合）を使用して、入力可能なFDAフォームにデジタル署名を適用することもできます。

ご不明な点がある場合は、FDAに直接お問い合わせください。

4.18 Webフォームへの署名

4.18.1 概要

Acrobat Sign Solutionsは、入力可能なフィールドを備えた再利用可能なwebフォームを作成する機能を提供します。Webフォームはwebサイトに埋め込んだり、URL経由で共有したりできます。参加者はフォームを表示し、記入して、署名することができます。

Webフォームの作成について詳しくはこちら：
https://helpx.adobe.com/jp/sign/adv-user/web-form/create.html

Webフォームはバイオ医薬業界標準対応の設定に従い、Acrobat Sign認証と共に使用する場合、署名者にID認証を求めるため、21 CFR Part 11の規制に準拠した署名を実現できます。

4.18.2 考慮すべき点

デジタル署名はサポートされていないため、webフォームの設計時に追加しないでください。

4.19 レポート作成

4.19.1 概要

ユーザーはレポートページのダッシュボードを活用して、容易に契約書のデータを閲覧できます。このデータはグラフィカルに表示され、フィルター（日付範囲、グループなど）を使用して絞り込むことができます。データの静的スナップショットをCSVファイルに書き出すと、データのさらなる分析が容易になります。利用できるレポートには多くの種類があります。ユーザーが利用できるレポートの数と種類はユーザーの権限レベルによって異なり、ユーザーレベルで制御できます。

契約書レポートには、生産性に関連するデータが表示されます。このデータは、契約書の完了率や完了までの平均時間など、契約活動の傾向を把握するのに役立ちます。

トランザクション消費レポートには、アカウントの使用状況に関連するデータが表示されます。これは、トランザクションの消費パターンとシステムの使用者を把握するのに役立ちます。

設定アクティビティレポートには、アカウント設定のアクティビティの履歴が表示されます。このタイプのレポートには管理者のみがアクセスできます。これは、ユーザー、グループ、または設定がいつ変更されたかを分析するのに役立ち、定期的な確認活動をサポートするために使用できます。

4.19.2 考慮すべき点

新しいレポートエクスペリエンスはすべてのアカウントに対してデフォルトで有効になるため、お客様は最新の環境を体験し、レポート機能を最大限に活用できます。

5 お客様のコンプライアンスの達成に向けたアドビのサポート体制

アドビは、ヘルスケアおよびライフサイエンス組織が、21 CFR Part 11やEudraLex Annex 11といった規制によって、独自の要件や高品質の標準規格を設けていることを理解しています。アドビはクラウドサービスプロバイダーとして、お客様のコンプライアンス目標の達成をサポートするために、数多くのプロセスやツールを導入しています。

5.1 業界標準規格の準拠

Adobe Document Cloud - Acrobat Sign Solutionsエンタープライズ版とビジネス版は、ISO 27001:2013、SOC 2 Type 2、PCI DSSなど、数多くの認証制度、標準規格、規制に準拠しています。証明書および監査レポートは、アドビが採用した制御の設計、運用、および有効性を証明するものです。アドビが提供するこれらの証明書および監査レポートは、ベンダー管理やサプライヤー評価プログラムの一環として活用していただけます。

利用可能な認定および監査レポートのコピーにアクセスするには、Adobe Trust Centerに接続します。これらの一部は、アドビと合意した機密保持契約の条件にもとづいてのみ利用できます。必要に応じて、ユーザーは機密保持契約に電子サインするよう求められます。

Adobe Trust Centerによるセキュリティ、プライバシー、コンプライアンスについて詳しくはこちら：
https://www.adobe.com/jp/trust.html

Adobe Document Cloudに関連するコンプライアンス標準と認定のリストはこちら：
https://www.adobe.com/jp/trust/compliance/compliance-list.html

アドビでは、社員の専門能力の開発を支援するプロセスを確立しています。すべての社員には、定期的にビジネス行動規範とセキュリティ啓発の研修を修了することが義務付けられています。アドビのシステムの開発とサポートに責任を負う個人には、割り当てられた業務を遂行するための資格を得るために、追加の研修が用意されます。研修の修了記録は文書化され、保存されます。

5.2 Adobe Cloudとインフラストラクチャ制御

アドビは、Acrobat Sign Solutionsのサービスを安全かつ制御された状態で維持します。Acrobat Signアプリケーションをサポートするインフラストラクチャは、厳格な制御を受け、セキュリティ、メンテナンス、およびコンプライアンスのベストプラクティスに従っています。ライフサイクルアクティビティを通して、アプリケーションの要件を満たすようにインフラストラクチャが設計され、テストされていることを確認しています。インフラストラクチャーサービスの委託先であるサードパーティは、アドビにサービスを提供する前に、（アドビのベンダー管理プログラムによる）厳格な検証を受ける必要があります。制御プロセスは、国際的に認められた標準規格（ISO 27001、SOC 2 Type 2など）への準拠を定期的に評価する外部監査人によって検証されます。

5.3 Acrobat Sign Solutionsのソフトウェアライフサイクル

Acrobat Sign Solutions、Acrobat Signアプリケーション、および関連するデータベースは、標準化されたソフトウェアライフサイクルマネジメント（SLC）プロセスに従って開発・保守されています。

アドビのSLCプロセスには、厳格な品質テストの段階が含まれます。テスト範囲には一般的なユースケースが含まれ、ソフトウェアアップデートをリリースする前に、テストを正常に完了させる必要があります。以下のユースケースは、各リリースに対するアドビの品質テストプランに含まれています。

- ユースケース1：**内部署名者への送信** — 複数の内部署名者（外部署名者なし）による文書の署名
- ユースケース2：**自己署名** — 送信者でもある1人の内部署名者による文書の署名
- ユースケース3：**外部署名者への送信** — 1人以上の外部署名者（内部署名者なし）による文書の署名
- ユースケース4：**内部署名者と外部署名者の両方に送信** — 内部署名者と外部署名者による文書の署名

これらのユースケースについて詳しくは、付録1を参照してください。

お客様は、これらのユースケースと使用目的との関連性を評価する必要があります。アドビのSLCプロセスでは、一貫性と信頼性を確保した方法でこれらのユースケースを完了できるよう、暗黙的にテストし、保証しています。このプロセスに依存することで、不必要なテスト作業の重複が発生しないように考慮する必要があります。

5.4　サービスコミットメント

アドビサービスコミットメントは、セールスオーダーに記載のAcrobat Sign Solutionsのサービスについて、アドビのサービスの可用性を説明するものです。

すべてのアドビサービスコミットメント：
https://www.adobe.com/jp/legal/service-commitments.html

Acrobat Sign Solutionsのホスティング環境には、複数のクラウドプロバイダーを利用しています。データは、複数のクラウド地域にある継続的にアクティブなアベイラビリティゾーンに複製されます。この環境は、高いレベルの可用性と拡張性を提供するように設計されています。アドビでは、Acrobat Sign Solutions、Acrobat Signサービス、パフォーマンスに関連するインフラストラクチャを継続的に監視しています。

Adobe Acrobat Signデータセンターについて詳しくはこちら：
https://helpx.adobe.com/jp/sign/using/adobesign-data-centers.html

データセンターの構成には、フェイルオーバー機能と回復機能が組み込まれています。データセンターに障害が発生した場合、トラフィックは障害が発生したアベイラビリティゾーン外の他のデータセンター、またはまったく別のクラウド地域にルーティングされます。

Acrobat Signサービスの可用性ステータス（アップタイムデータ）：
https://status.adobe.com

アドビでは、事業の継続性と障害復旧を目的として、ISO 22301認証取得済みの包括的なプログラムを導入しています。アドビは毎年、Acrobat Sign Solutionsの障害復旧テストを実施し、クロスリージョンのフェイルオーバー機能とフェイルバック機能が、規定の復旧時間と復旧ポイントの目標に反していないかを検証しています。

5.5　セキュリティとインシデントの対応

セキュリティの脅威は常に進化しているため、プロアクティブなセキュリティアプローチを導入しています。アドビは、脅威インテリジェンス情報を管理し、Acrobat Sign Solutionsのサービスを継続的に監視して、セキュリティの脆弱性やインシデントの予防と早期発見に努めています。

アドビは、インシデントの対処、軽減および解決プログラムを導入しています。各セキュリティインシデントは、アドビのインシデント対応チームが調査をおこない、軽減措置を講じています。また、アドビの社員には、セキュリティ啓発研修を年1回受けることが義務付けられています。研修では、アドビの現在のセキュリティポリシーと標準規格、セキュリティインシデントを対応チームに報告する方法などを扱います。

確認されたインシデントには、お客様への影響、損害、または障害にもとづいて重大度レベルが割り当てられます。アドビは、個人データの漏えいが確認された場合、適用される法律に従ってお客様に通知します。セキュリティ侵害通知については、アドビとお客様との間の契約条件に記載されています。

5.6 リリース管理

アドビは、Acrobat Sign Solutionsのリリースを管理、計画、テスト、スケジュールするための明確なプロセスを維持しています。アドビでは、毎年3つの主要な機能リリースの提供を計画しています。メジャーリリースには、新機能や既存の機能への重要な変更が含まれます。お客様が発見した欠陥やシステム処理の問題を解決するために、必要に応じてマイナーリリースを頻繁にリリースする場合があります。マイナーリリースは、新機能の導入やユーザーエクスペリエンスの変更を意図したものではありません。ただし、例外もあります。エンドユーザーエクスペリエンスに影響を与える新機能（メジャーリリースやマイナーリリースでリリースされる）は可能な限り「オフ」に設定されているため、リスクは低くなります。この機能は、管理者が有効にするまで「オフ」モードのままです。

変更のリリースは、月の第2週におこなうように最善を尽くしています。リリース予定日は、Adobe Acrobat Signのリリーススケジュールに公開されます。

Adobe Acrobat Signのリリーススケジュール：
https://helpx.adobe.com/jp/sign/release-notes/adobe-sign/sign-release-schedule.html

スケジュールには、変更によって影響を受けるサービスタイプ（サブスクリプションレベル）の概要が記載されています。また、その機能が標準（構成不可）であるのか、お客様アカウントのアカウントレベルまたはグループレベルで構成可能であるのかについても説明します。

変更はアドビによって計画され、通知されます。すべてのコミュニケーションは情報の提供を目的に特別に作成されており、お客様は変更とコンプライアンスの状態を管理するためのプロセスに使用できます。提供する情報は以下のとおりです。

- プレリリースノート：プレリリース情報は、メジャーリリースとマイナーリリースごとに公開され、Adobe Acrobat Signリリーススケジュールのページで閲覧することができます。リリースの範囲、機能の変更点、強化点、ユーザーインターフェイスのアップデートについて記載しています。プレリリース情報は、製品リリースの8週間前、4週間前、そして当日にも公開されます。

- 設定のアップデートに関するリリース：このドキュメントはメジャーリリースごとに公開されます。リリースの結果、変更される予定の設定について説明します。内部向けとお客様向けの機能に影響を与える新規の設定と変更される設定が対象です。この設定によって、カスタマーエクスペリエンスがどのような影響を受け、アカウントレベルでデフォルトの動作がどのように変わるかを記載します。

- 技術的なお知らせ：これらのアップデートは通常、長期的な視野にもとづいた戦略的変更であり、定期的に予定されるメジャーリリースやマイナーリリースとは別に実施されます。テクニカルアップデートは通常、かなり前から計画され、発表されます。非推奨となるサービスに関連する変更が含まれるのが一般的です。Acrobat Sign の管理者は、技術的なお知らせを電子メールで受け取ります。

- 品質保証レポート：このドキュメントは、ソフトウェアリリースの品質を保証するためにテストが実施されたことを示すアドビの証明書です。メジャーリリースについてのみ公開され、Adobe Trust Center（https://www.adobe.com/jp/trust/resources.html）からダウンロードできます。

- リリースノート：このドキュメントはメジャーリリースとマイナーリリースごとに公開されます。リリースノートはプレリリースノートを改良した最終版です。最新リリースの新機能、エクスペリエンスの変更点、および解決された問題（バグ）に重点を置いています。リリース当日に公開されます。

Acrobat Sign Solutions のリリーススケジュールとプレリリースノート：
https://helpx.adobe.com/jp/sign/release-notes/adobe-sign/sign-release-schedule.html

Acrobat Sign Solutions の現在のリリースと過去のリリースのリリースノート：
https://helpx.adobe.com/jp/sign/release-notes/adobe-sign.html

リリースに関するドキュメントを参照し、機能または構成の変更点を確認することをお勧めします。また、定期的に Acrobat Sign Solutions の技術情報を確認し、アドビの製品ロードマップと予定されているテクニカルアップデートの理解を深めてください。

Acrobat Sign の技術的なお知らせ：https://helpx.adobe.com/jp/sign/using/technical-notifications.html

プレリリースのドキュメントや技術的なお知らせに目を通して、今後の変更点を確認し、予想される影響を考慮して積極的に計画を立てるプロセスを導入し、実施することが重要です。場合によっては、様々な変更によって、ビジネスプロセスのユースケースにも変更が生じます。システム構成の変更が必要な場合、またはシステムの使用目的に影響が及ぶ場合、回帰テストや再検証作業が必要になる可能性があります。アドビは、規制に関するコンプライアンスの遵守や検証の観点から、予定される変更による潜在的な影響を評価し、評価レポートを発行することで、お客様を支援します。

アドビは、可能な限り、新機能をデフォルトで無効化した状態で配信します。新機能を希望するお客様は、意図的に操作をして機能を有効にする必要があります。その場合、社内で変更管理手順を導入して、機能の有効化を監督してください。

5.7 Adobe Acrobat Sign サンドボックス

エンタープライズクラスのお客様は、Adobe Acrobat Sign サンドボックスに登録いただけます。この環境は、本番環境とは切り離されています。サンドボックスから送信される契約書には、「Not for production use」という透かしが入ります。

サンドボックスの目的は、本番環境に影響を与えることなく、管理者が希望する設定を定義、変更、テストできるようにすることです。サンドボックスは、デフォルト構成のクリーンな環境として提供され、お客様の本番環境設定をミラーリングするものではありません。ただし、2つの環境の同期を容易にするために、管理者はいくつかの設定（グループ名、ライブラリテンプレート、カスタムワークフローなど）を本番環境にコピーしたり、本番環境からコピーしたりすることができます。

サンドボックスのアカウントレベルまたはグループレベルの設定は通常、本番環境にある設定オプションと一致しています。ただし、リリース待ちの新規／アップデートされた設定は除きます。サンドボックス環境は、本番環境でのメジャーリリースの4週間前に、新しいコンテンツにアップデートされます。これは、2つの環境に4週間のずれが生じることを意味しますが、本番環境に導入する前に、リリース間近の新機能を評価、テストできるメリットがあります。

サンドボックスと本番環境の機能の違いは完全に開示されていることをご承知おきください（送信メールの抑制、サンドボックスアカウントでは利用できない統合機能など）。本書では、コアとなるAcrobat Signアプリケーションのみのサンドボックス環境について説明し、他のソリューションとのシステム統合については説明しません。

Adobe Acrobatサンドボックスについて詳しくはこちら：
https://helpx.adobe.com/jp/sign/using/adobesign-sandbox.html

5.8　検証のサポート

GxP規制の環境で電子サインの適用にAcrobat Sign Solutionsを使用する場合、Acrobat Sign Solutionsの検証をおこなうことが求められます。その際、使用目的に対して適合しており、システムが一貫性と信頼性を確保した方法で機能し、改ざんまたは無効な記録／署名を識別する能力を提供することを証明する必要があります。

お客様は、適切なレベルと範囲の検証を確立する必要があります。ISPEのGAMP 5（参考文献 [3]）といった規制機関や業界のベストプラクティスでは、検証をリスクベースのアプローチでおこなうことを推奨しています。検証の作業を可能な限り効果的かつ効率的におこなうために、サプライヤーを活用することをお勧めします。

アドビでは、検証の文書テンプレートを提供し、お客様の検証作業をサポートしています。テンプレートパッケージは一連の典型的なユースケースを網羅しています。ただし、その他の想定されるユースケースは、パッケージでは考慮されていません。検証の文書テンプレートパッケージで対応しているユースケースは、コアのAcrobat Sign Webアプリケーションのみに関連しており、他のソリューションとのシステム統合を伴うユースケースには対応していません。お客様には、（ユースケースの範囲を含む）テンプレートの適合性を評価する責任があります。Acrobat Sign Solutionsのインスタンスが使用目的に適合していることを証明する文書化された証拠を確立するために、これらの検証文書を適合させ、実行できます。これらの文書は、検証の観点から潜在的な影響を説明する影響評価報告書とともに、メジャーリリースごとに必要に応じてアップデートされ、再発行されます。

検証文書テンプレートパッケージについて詳しくはこちら：
https://helpx.adobe.com/jp/sign/using/21-cfr-validation-pack.html

サンドボックス環境の対象条件を満たすお客様は、本番前のテストや検証の目的で使用できる制御された環境として、インスタンスの設定を検討することができます。

5.9 カスタマーサービス

よくある質問（FAQ）、ユーザーガイド、チュートリアルの回答は、オンラインのアドビヘルプセンターでいつでも参照できます。

Acrobat Sign ヘルプセンター：https://helpx.adobe.com/jp/support/sign.html

Acrobat Sign Solutions をご利用のお客様は、アドビサポートにケースを送信することで、個別のサポートを受けることができます。サポートを受けるためのケースを提出する権限を持つのは、管理者のみです。アドビサポートに連絡して、Acrobat Sign サンドボックスとプロダクションのインスタンスで見られた問題を報告してください。

また、アドビサポートでは、アプリケーションのインターフェイスを通じて、お客様向けでない設定の変更を要求することもできます。ただし、その場合、リクエストの状況と設定変更による影響をお客様側で追跡するためのプロセス（変更管理や構成管理など）を実施する必要があります。

6 Acrobat Sign Solutions の導入 — 実用ガイド

6.1 導入チェックリスト

このステップバイステップ形式の操作ガイドに従って、Acrobat Sign Solutions のお客様アカウントを作成し、運用を始めてください。

ステップ	アクティビティ	アクション	構成
1.	ビジネスユースケースの特定：使用目的	ビジネスプロセスを検証して、Acrobat Sign を使用して誰が、どのようなタイプの文書に署名する必要があるのかを明確にします。	該当なし
2.	アカウントの作成	セクション 4.1 を参照。 バイオ医薬業界標準対応の設定とその他の高度な機能を利用するには、Acrobat Sign Solutions のエンタープライズ版またはビジネス版のサブスクリプションが必要です。 Acrobat Sign にシングルサインオン（SSO）を導入する場合、またはサンドボックスのサブスクリプションを希望する場合は、エンタープライズ版が必要です。 アドビでは、アカウントのオンボーディングをサポートしており、管理ツールとして Adobe Admin Console を提供しています。 Acrobat Sign Solutions のアカウント管理者として任命されたユーザーを作成します。	該当なし

ステップ	アクティビティ	アクション	構成
3.	グループ管理	セクション4.3を参照。 アカウント管理者として、バイオ医薬業界標準対応の設定の制御を受けるユーザー用のグループ（例：GxPグループ）と、規制された環境で署名する必要がないユーザー用の別のグループ（例：非GxPグループ）を作成します。 GxPグループのグループ管理者となるユーザーを指定します。グループ管理者が、ユーザーを追加し、グループの設定を編集できるように設定します。 グループ管理者として、ビジネスプロセスに関する追加の設定をおこないます。	アカウント／グローバル設定／グループ アカウント／グループ／グループ設定
4.	署名の種類	セクション4.6を参照。 電子サインを選択した場合： ・グループ管理者として、GxPグループに電子サインを許可するように設定します。 証明書ベースのデジタル署名を選択する場合： ・グループ管理者として、GxPグループにデジタル署名を許可するように設定します。 ・トラストサービスプロバイダー（TSP）を選択してオンボーディングし、デジタルIDで署名するための手順書を配布します。	アカウント／グループ／署名の環境設定 アカウント／グループ／デジタル署名
5.	認証設定	セクション4.7を参照。 グループ管理者として、GxPグループの認証方法を構成します： ・内部署名者：Acrobat Sign認証を選択します。 ・外部署名者：Acrobat Sign認証、電話認証、電子メールによるワンタイムパスワード認証を選択します。	アカウント／グループ／送信設定
6.	シングルサインオン	セクション4.8を参照。 Adobe Admin Consoleの管理者として、Federated IDを使用するようにアカウントを設定します（必要な場合）。 アカウント管理者として、シングルサインオンを有効にします（必要な場合）。	Adobe Admin Console または アカウント／アカウント設定／SAML設定
7.	外部署名者の許可	セクション4.9を参照。 グループ管理者として、GxPグループを構成し、外部署名者が契約書への署名に参加できるようにします。 送信者が許可された署名者を識別できるよう、プロセスを実装します。	アカウント／グループ／署名の環境設定 アカウント／グループ／送信設定
8.	承認	セクション4.4と4.5を参照。 ユーザーアクセス管理のプロセスを実装します。 手動で、または組織のエンタープライズディレクトリと同期して、ユーザーを作成します。 Adobe Admin Consoleの管理者として、Acrobat Sign Solutionsにユーザー資格を割り当てます。 アカウント管理者またはグループ管理者として、ユーザーをGxPグループに配置します。 アカウント管理者またはグループ管理者として、ユーザーの権限レベルを割り当てます。	アカウント／ユーザー
9.	バイオ医薬業界標準対応の設定	セクション4.2と4.11を参照。 グループ管理者として、GxPグループのバイオ医薬業界標準対応の設定を有効にして、構成をおこないます。 グループ管理者として、事前に定義した署名の理由のリストを設定します（空白の理由を除く）。	アカウント／グループ／バイオ医薬業界標準対応の設定
10.	委任、アカウントの共有、契約書の共有	セクション4.12と4.16を参照。 グループ管理者として、GxPグループの委任の環境設定をおこないます（必要な場合）。 グループ管理者として、アカウント共有機能と契約書の共有機能の環境設定をおこないます。	アカウント／グループ／グループ設定 アカウント／グループ／セキュリティ設定

6.2　ガバナンス

いかなるシステムも21 CFR Part 11およびEudraLex Annex 11の要件に準拠しなければならないのと同様に、電子記録と電子サインの完全性を確保するための手順と制御を採用する必要があります。Acrobat Sign Solutionsの使用目的がお客様のニーズに合致していることを確認するために、社内のポリシーと手順を精査する必要があります。

以下の表には、Acrobat Sign Solutionsを適切に使用するために、お客様が実施する必要のある主なガバナンスプロセスを記載しています。推奨事項と注意事項も合わせてご確認ください。

トピック	注意事項
システム管理	各リリースに先立ち、アドビのロードマップとテクニカルアップデートの文書を確認するロールと責任を定義します。 アドビは、すべてのメジャーリリースとマイナーリリースの前に、サービスの変更に関する文書を作成します。管理者とその他の関係者は、プレリリースノートやAcrobat Sign Solutionsのサービスの状態に関する通知を受け取ることができます。今後の機能の変更点を評価し、必要に応じて適切な手段を講じるために、これらの情報を確認する必要があります。
ユーザーアクセス管理	ユーザーアカウントを作成し、ユーザーのロールと責任にもとづいて適切なレベルの権限を付与するためのプロセスを定義します。 ユーザーアカウント管理は、既存のIDプロバイダーと統合する（例：自動ユーザー作成）か、手動のユーザー作成プロセスを通じておこなうことができます。
電子サインの使用	各個人がその電子サインのもとで開始したアクションに対する責任と義務を規定した社内ポリシーを定義します。これらのポリシーは、署名の偽造を防止するように設計する必要があります。電子サインの不適切な使用の結果を明確にする必要があります。 米国FDAの21 CFR Part 11とEudraLex Volume 4 Annex 11（必要な場合）の要件に準拠した、電子サインを電子記録に適用するプロセスを定義します。 このプロセスでは、主要な規制対象のユースケースにおける認証要件を重視する必要があります。ただし、電子サインを広範に使用する場合、これらの制御は必ずしも必要ではありません。電子サインのユースケースを判断することは、効果的な導入に不可欠です。
記録管理	署名済みの電子記録とその監査証跡をAcrobat Sign Solutionsから抽出し、お客様が管理する指定の電子記録レポジトリまたはアーカイブに保存するためのプロセスを定義します。

上記の手順に加え、Acrobat Sign Solutionsが制御された方法で検証、導入、管理、使用されるために、以下のトピックに対処するポリシー、手順、またはその他の品質システム文書を実装する必要があることに注意してください。

- コンピューターシステムの検証
- 論理的セキュリティ
- 研修管理
- 文書管理
- 変更と構成の管理
- バックアップと回復
- 障害復旧と緊急時対応計画
- 定期的な検証
- ベンダー評価
- インシデントと問題の管理

7　付録1：ビジネスユースケースの概要

21 CFR Part 11 と Annex 11 に準拠した電子サインを適用するために、Acrobat Sign Solutions の導入方法を示した一般的なビジネスユースケースを以下に紹介します。

ユースケースの説明	例	インサイト
ユースケース1：内部署名者への送信	・検証成果物（検証プラン、検証プロトコルなど）の承認 ・標準作業手順（SOP）の承認	送信ページのインターフェイスは、内部受信者に契約書を送信するために使用します。 送信者が署名者の1人である場合と、そうでない場合があります。
ユースケース2：自己署名	・追加の承認が必要でない、記録やその他のフォーム／レポートの発行者による署名 ・インシデントレポートへの署名 ・自身のステータスレポートへの署名	このユースケースは、単独の内部署名者が送信者となり、文書に署名する場合に関連します。 署名者は「入力と署名」をクリックして、自ら契約書に署名します（自己署名）。また、署名者は送信ページのインターフェイスを使用して契約書を自身に送信できます（自己送信）。
ユースケース3：外部署名者への送信	・同意書への署名 ・情報にもとづく同意書への署名 ・サプライヤーとの契約書への署名	送信ページのインターフェイスは、アカウントのメンバーではない1人以上の署名者に契約書を送信するために使用します。
ユースケース4：内部署名者と外部署名者の両方への送信	・制御された文書への署名（SOP、検証成果物など）。この場合、署名者の1人以上は、組織の Acrobat Sign Solutions アカウントに追加されていないコンサルタントまたは請負業者です。 ・スポンサー（内部）と治験実施医師（外部）が署名する治験施設契約書	送信ページのインターフェイスは、送信者または他の内部メンバーが、外部署名者の署名前または署名後に契約書を送信するために使用します。 送信者が署名者の1人である場合と、そうでない場合があります。

8　参考資料

参考文献 [1] U.S. Food and Drug Administration, Code of Federal Regulations, Title 21 Part 11, Electronic Records; Electronic Signatures, 1997.

参考文献 [2] EudraLex, The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medical Products for Human and Veterinary Use, Annex 11:Computerised Systems, 2011.

参考文献 [3] ISPE, GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems, Second edition, 2022.

9　謝辞

本書は、アドビとMontrium Inc.が共同で作成しました。Montriumについて詳しくはこちらをご覧ください：www.montrium.com

本書は、FDAの規制の対象となる、またはEU内で営業するヘルスケア組織とライフサイエンス組織向けに作成されました。本書は、Acrobat Sign Solutionsの使用に関して独自の決定をおこなうための参考資料として作成されています。本書は法的または専門的な助言を提供するものではありません。各組織は、Acrobat Sign Solutionsがそれぞれの使用目的に合致していることを確認するために、内部プロセスにもとづいて適切な調査をおこなう必要があります。法律や規制は頻繁に変更されるため、本情報は最新かつ正確でない場合があります。アドビは、法律で認められる最大限の範囲において、本資料を「現状のまま」で提供します。アドビは、商品性、特定目的への適合性、正確性の表明もしくは保証を含め、本資料に関して、明示、黙示、法定を問わず、いかなる種類の表明または保証もおこないません。