Adobe Digital Publishing Suite Enterprise Edition セキュリティ概要

目次

アドビのセキュリティ

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、ソフトウェア開発プロセスおよびツールへの徹底したセキュリティの統合から、部門の枠を超えたインシデント対応チームに至るまで、先を見越した迅速な対応に努めています。さらに、パートナー、研究者および他の業界団体と協力して、最新のセキュリティのベストプラクティスを理解し、提供する製品およびサービスに継続的にセキュリティ対策を組み込んでいます。

このホワイトペーパーでは、Adobe Digital Publishing Suite におけるユーザーエクスペリエンスや Digital Publishing Suite で作成したアプリケーションに含まれるデータのセキュリティを強化するために、アドビが実装する事前対応型アプローチおよび手順について説明します。

Adobe Digital Publishing Suite Enterprise Edition について

Adobe Digital Publishing Suite Enterprise Edition は、大手出版社、グローバル企業、高等教育機関にお勧めの統合プラットフォームです。タブレットやスマートフォン向けのデジタルコンテンツのデザイン・発行・販売から、コンテンツ利用状況の追跡把握まで、モバイルコンテンツのパブリッシング関連作業全般をカバーする機能が揃っています。ホスティングサービスと App Builder テクノロジーで構成される Digital Publishing Suite は、Adobe Creative Cloud ソフトウェア（InDesign を含む）および Adobe Experience Manager との緊密な連携により、デジタルマガジン、ブランド好感度向上、販促、マーケティングコミュニケーションの各種アプリケーションのモバイルデバイスへの効率的な公開を実現します。

Adobe Digital Publishing Suite Enterprise Edition および Adobe Content Viewer for Web のすべてのサービスコンポーネントはクラウドでホストされます。Adobe Content Viewer for Desktop などのその他の表示コンポーネントは、それぞれのシステムまたはプラットフォーム上に存在します。

Adobe Digital Publishing Suite Enterprise Edition の主なコンポーネント

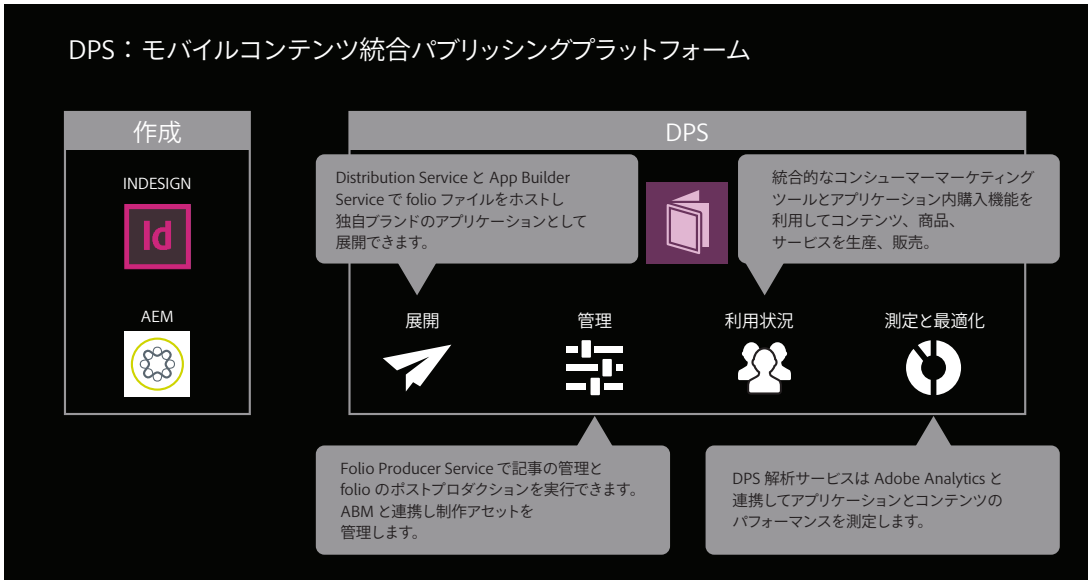
Digital Publishing Suite は、コンテンツ中心のアプリケーションを公開するエンドツーエンドのプラットフォームです。モバイルデバイスにインストールされたアプリケーションへ配信するコンテンツの作成には、Adobe InDesign ソフトウェアを所有しているか Adobe Experience Manager へのアクセスが必要です。

Adobe InDesign を使用している場合：

デスクトップで Adobe InDesign を使用してコンテンツを作成したら、そのコンテンツを .folio ファイルに変換します。.folio ファイルには、コンテンツのほか、コンテンツに関連付けられた画像、フォント、マニフェストが含まれます。.folio ファイルは、セキュアな HTTP 接続（HTTPS）を使用して Digital Publishing Suite へ自動的にアップロードされます。その後、.folio ファイルをコンテンツ閲覧者への配布用アプリケーションとして管理および公開できます。複数の .folio ファイルを一緒にバンドルすることもできます。

Adobe Experience Manager を使用している場合：

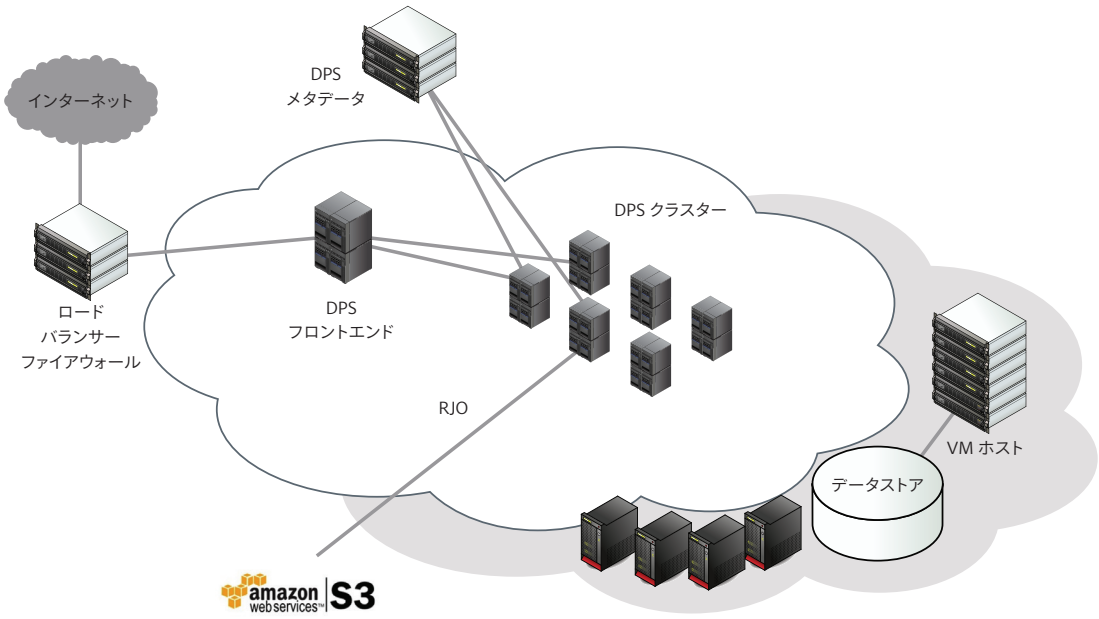
Adobe Experience Manager のドラッグ＆ドロップ対応のインターフェイスを使用して HTML テンプレート形式のコンテンツを作成したら、それらのテンプレートをセキュアな HTTP 接続（HTTPS）で Digital Publishing Suite と同期します。その後、コンテンツ閲覧者への配布用アプリケーションとして .folio ファイルを作成および公開します。複数の .folio ファイルを一緒にバンドルすることもできます。



Adobe Digital Publishing Suite モバイルコンテンツパブリッシングプラットフォーム

Adobe Digital Publishing Suite Enterprise Edition には次のコンポーネントが含まれています。

Folio Producer Service：.folio ファイルを共有、管理、公開します。Folio Producer Service に InDesign から .folio ファイルをアップロードまたは Adobe Experience Manager から HTML テンプレートを同期すると、コンテンツの編成と並べ替え、メタデータの追加、完成した .folio ファイルのプレビューを実行できます。プレビュー機能では、発行後に表示される様子を正確に確認できます。Folio Producer Service は、Amazon Web Services（AWS）のクラウドでホストされ、PDF、JPEG、HTML5 などの各種ファイル形式をサポートしています。



Folio Producer Service のネットワーク図

DPS App Builder：アイコンやアセットをアップロードして独自ブランドのアプリケーションを構築し、主要アプリケーションマーケットプレイス経由で配布または非公開の刊行物として組織内部に配布できます。DPS App Builder では、単一の .folio ファイルまたは複数の .folio ファイルを使用してアプリケーションを作成できます。独自ブランドのアプリケーションのツールバーをカスタマイズして、最大 7 つのオリジナルアイコンを追加することもできます。

Distribution Service：主要なタブレットおよびスマートフォンデバイスで .folio ファイル形式のデジタルコンテンツを安全に保存およびホスティングします。セキュアFolio機能を有効にすると、Distribution Serviceでもデジタルコンテンツの配信セキュリティが強化されます。セキュア Folio の配布について詳しくは、「Digital Publishing Suite のセキュア Folio と制限付き配布」セクションを参照してください。

解析サービス：アプリケーションの合計ダウンロード数やその他の購入指標値など、主なアプリケーション、folio、デバイス、購入、読者に関する指標値のほか、DPS 解析サービスに含まれる作成済みのレポートを使用してインタラクティブコンテンツの利用状況を確認できます。Adobe Analytics をご使用の場合、お客様のビジネス要件に合わせてカスタマイズ可能なドリルダウン形式の詳細なレポートも利用できます。

アカウント管理設定：管理者は、役割に基づくセキュア Folio の有効化など、組織内のすべての DPS アカウントの設定を管理できます。Web フォームを通じて、管理者は Adobe Content Viewer for Web を有効化、無効化、および設定できます。また、適切な場合、DPS 解析サービスと Adobe Analytics アカウントをリンクするために必要な詳細を提供できます。

Adobe Content Viewer：Apple iOS や主要な Android ™ベースのタブレット、スマートフォン、または Microsoft® Windows® 8.1 デスクトップ、タブレット、スマートフォンの各デバイスで魅力的な読書体験を可能にします。また、自社ブランドを冠した Content Viewer を作成し、自社の刊行物らしい外観と操作を提供して読者の意識をコンテンツに集中させることができます。

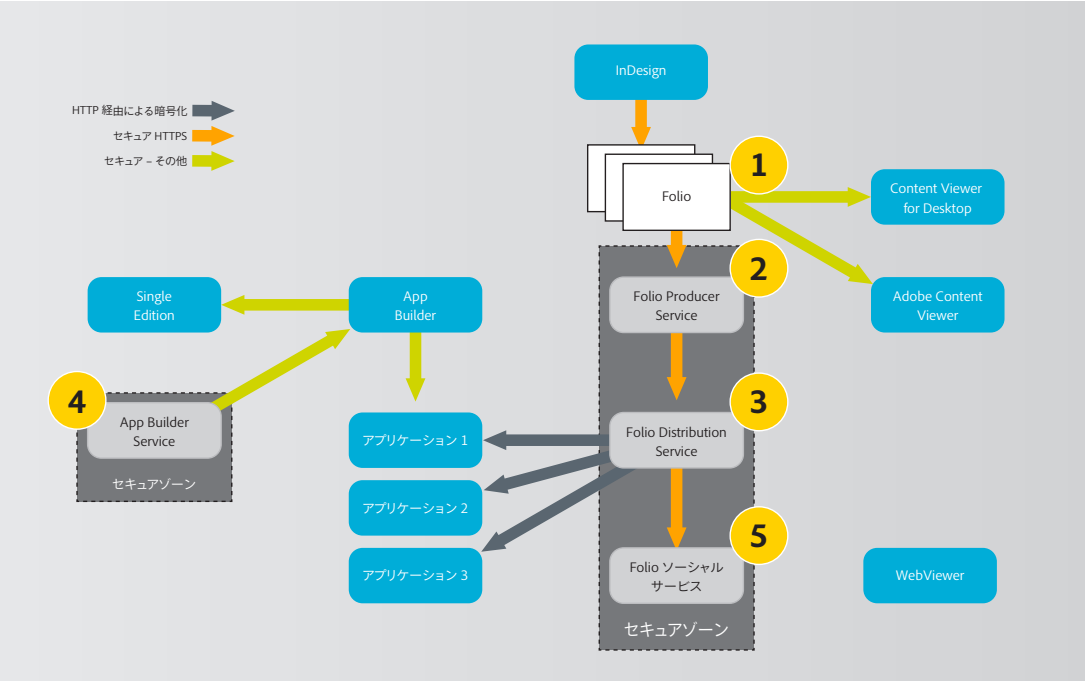
Adobe Digital Publishing Suite のコンテンツフロー

Adobe Digital Publishing Suite とセキュリティの問題を十分に理解するために、コンテンツの開発から配布までのフローについて説明します。

手順 1：前述のように、Adobe InDesign または Adobe Experience Manager を使用して .folio ファイルに収めるコンテンツを作成します。この .folio ファイルにはコンテンツのほか、コンテンツに関連付けられた画像、フォント、マニフェストが含まれます。次に、デスクトップコンピューターで **Content Viewer for Desktop** を使用してコンテンツを表示、更新、プレビューします。ここでは、タブレット、スマートフォン、その他のモバイルデバイス上のアプリケーションに展開したのと同じ状態でコンテンツを操作できます。

InDesign を使用している場合、.folio ファイルは自動的に Folio Producer Service にアップロードされます。Adobe Experience Manager を使用してコンテンツを作成している場合、「同期」ボタンを押すだけで HTML テンプレートが Folio Producer Service に同期され、ワークフローの次の手順に進みます。

注意：.folio ファイルに個人の特定につながる情報（PII）やその他の機密情報を含めないことをお勧めします。もし含める場合は、セキュア Folio 機能を有効にすることを検討してください。ただし、セキュア Folio 機能を有効にすると、Digital Publishing Suite の他の機能が無効になります。セキュア Folio 機能を有効にする前に、妥協すべき点についてよく理解する必要があります。詳しくは、後述の「Digital Publishing Suite のセキュア Folio と制限付き配布」セクションを参照してください。



Adobe Digital Publishing Suite セキュア Folio のコンテンツフロー

手順 2：コンテンツはセキュアな HTTPS 接続を介して InDesign から **Folio Producer Service** へ自動的にアップロード、または Adobe Experience Manager と自動的に同期されます。権限を付与されたユーザーは、アドビブランドのモバイルアプリケーション **Adobe Content Viewer** を使用して、iOS、主要な Android、および Windows 8.1 のモバイルデバイスでコンテンツを表示およびテストできます。

手順 3：コンテンツを公開する準備ができたら、Folio Producer Service で「公開」をクリックするとコンテンツがセキュアな HTTPS 接続で **Distribution Service** に送信されます。

デフォルトでは、Distribution Service はコンテンツを暗号化しない状態で保存します。ただし、セキュア Folio 機能を有効にすると、コンテンツは暗号化されてから保存されます。コンテンツ閲覧者がコンテンツをダウンロードすると、コンテンツデータネットワーク（現在は Akamai）が所有するエッジサーバーにコンテンツがキャッシュされ、Distribution Service と同じ形式（暗号化、非暗号化など）で保存されます。

セキュア Folio 機能を有効にすると、Distribution Service でコンテンツが暗号化され、コンテンツ閲覧者のデバイスにダウンロードされた後、暗号化が解除されます。デバイスに置かれたコンテンツは、OS レベルのセキュリティ機能を使用して保護されます。

手順 4：カスタムの自社ブランドアプリケーションを作成してコンテンツをホストする場合は、**DPS App Builder を使用します。**その後、お客様はアプリケーションから最新のコンテンツをダウンロードできます。

手順 5: Web ブラウザーを使用して Facebook や Twitter などのソーシャルネットワークでコンテンツを共有可能にする場合は、**アカウント 管理 サービス**で機能を有効にできます。有効にすると、ユーザーは記事や記事の一部をリンクで共有することができます。このようなコンテンツは、モバイルデバイスと同様の形式で **Adobe Content Viewer** for Web でもアクセスできます。

* 注意：セキュア Folio 機能を有効にしている場合、ソーシャルシェアリングは自動的に無効になります。詳しくは、後述の「Digital Publishing Suite のセキュア Folio と制限付き配布」セクションを参照してください。

手順 6：公開された .folio ファイルは、契約期間中いつでも削除できます。Digital Publishing Suite のサブスクリプションを解約すると、公開されたコンテンツは解約の日から少なくとも 90 日間、Digital Publishing Suite サーバーに残ります。90 日を経過すると、アドビは必要に応じてサーバーからコンテンツを削除する権利を有します。

Digital Publishing Suite のセキュア Folio と制限付き配布

個人の特定につながる情報（PII）を .folio に含めた場合、または権限を付与したユーザーに特定のコンテンツへのアクセスを許可する場合、Digital Publishing Suite のセキュア Folio 機能が役立ちます。セキュア Folio 機能は、Digital Publishing Suite v30 以降の直接権利付与および市販 folio 権利付与アプリケーションにのみ利用できます。また本書の発行時点で、Apple iOS ベースのアプリケーションのみサポートされます。

セキュア Folio 機能では、ユーザーの資格情報または役割に基づきコンテンツの配布を制限できます。例えば、製薬会社で、医師に対して特定のコンテンツへのアクセスを許可し、営業担当者にはそのコンテンツの一部または完全に別のコンテンツへのアクセスのみ許可することができます。

セキュア Folio 機能を有効にするには、商用のアプリケーションストアを使用してアプリケーションを配布するのではなく、どのユーザーにどのコンテンツの表示を許可するかを定義する独自の権利付与サーバーを構成する必要があります。直接権利付与について詳しくは、*www.adobe.com/devnet/digitalpublishingsuite/entitlement.html* をご覧ください。

安全なアプリケーションの構築と配布のワークフローは、次の 3 つの手順で行います。

1. 事前に、iOS Developer Center で「Data Protection」を有効にします。これにより、ご使用のモバイルデバイスでセキュアモードがオンになり、OS レベルのセキュリティ機能を使用してコンテンツが保護されます。
2. Digital Publishing Suite で、アカウント管理ツールの「セキュリティ保護されたコンテンツ」チェックボックスをクリックします。これにより、Adobe ID にリンクされているコンテンツ発行者のアカウントが承認され、セキュア Folio を作成できます。
3. Folio Producer Service でセキュア Folio を公開する準備ができたら、「Folio を暗号化」オプションを選択し、.folio ファイルを「公開」および「市販」に設定します。

セキュア Folio に有効なセキュリティメカニズム

セキュア Folio を作成する際、次の追加的セキュリティメカニズムが適用されます。

- .folio ファイルを Folio Producer Service にアップロードすると、セキュア AWS S3（Amazon Simple Storage Service）バケットに .folio ファイルが保存されます。つまり、コンテンツが Folio Producer Service にある間、Adobe Content Viewer for Web を使用してコンテンツをテストまたはプレビューすることはできません。
- セキュア Folio をテストまたはプレビューするためには、コンテンツを Distribution Service に公開する必要があります。これを行うには、Folio Producer Service で「Folio を暗号化」オプションを選択し、.folio ファイルを「公開」および「市販」に設定します。そうすると、.folio ファイルとそのコンテンツが暗号化された形式で Distribution Service に公開され、ワークフローのこの時点で、対象のモバイルデバイス上の Adobe Content Viewer を使用する「デバイスでプレビュー」オプションを使用して、.folio のコンテンツをテストおよびプレビューできます。
- セキュア Folio 機能と「Folio を暗号化」オプションを使用するすべての .folio ファイルは、モバイルアプリケーションに配信されるときに暗号化されます。モバイルデバイスがロックされているときや電源がオフのときは、安全な .folio ファイルの暗号化が維持されます。パスコードまたは指紋認証を使用してデバイスのロックを解除すると、.folio コンテンツの暗号化が解除され使用可能になります。この機能は、オペレーティングシステムによって提供される Apple iOS の標準機能を使用します。安全なアプリケーションについて詳しくは、Apple の iOS セキュリティドキュメントを参照してください。

セキュア Folio での制限

セキュア Folio 機能を有効にすると、機密情報や取り扱いに注意を要するコンテンツの配信をユーザーの資格情報または役割に基づいて制限できます。また、Digital Publishing Suite のその他の機能に一定の制限をつけることができます。以下のような制限が設定できます。

- 「市販」ステータスに設定された公開 folio のみを暗号化可能にする
- コンテンツのソーシャルシェアリングを無効にする
- セキュリティの目的で、Adobe Content Viewer for Web を使用した Folio Producer Service での安全な .folio ファイルのワイヤレスプレビューを無効にする。Distribution Service にファイルを安全に保存してから、「デバイスでプレビュー」を使用して安全な .folio ファイルをプレビューします。
- バックグラウンドダウンロードとプログレッシブダウンロードをサポートしない。デバイス上で、.folio ファイル全体を必ずダウンロードしてから暗号化を解除します。

Digital Publishing Suite のストレージとストレージオプション

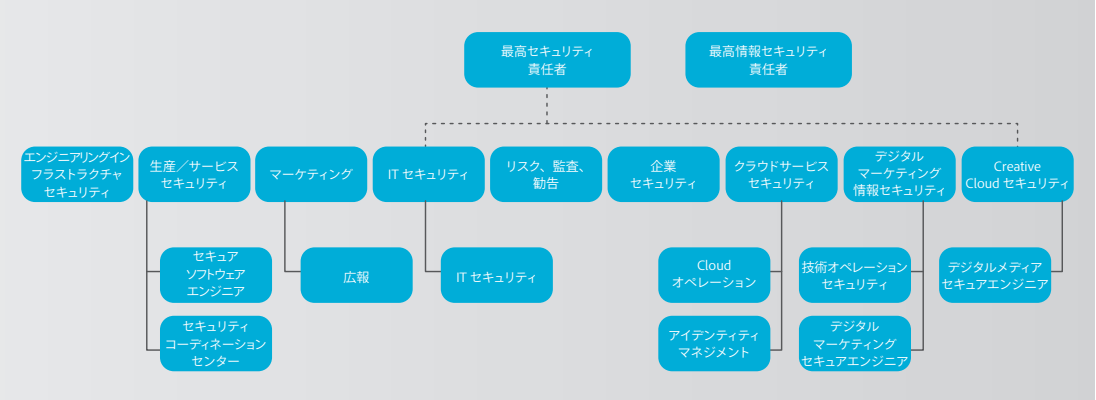
Folio Producer Service にアップロードされたコンテンツは、容量に関係なくデータを保存・取得できるデータストレージインフラストラクチャ、Amazon S3（Amazon Simple Storage Service）のクラウドに保存されます。Adobe Digital Publishing Suite のお客様は、以後もデータの所有権を持ち、自由にご利用いただけます。詳しくは、アドビの利用条件およびプライバシーポリシーをご覧ください。

Folio Producer Service に保存されているすべてのコンテンツは固有の Adobe ID とリンクし、その Adobe ID を使用してストレージ内でコンテンツを事実上区分けします。Folio Producer Service は保存状態のコンテンツを暗号化しませんが、Acrobat.com など他のアドビサービスでアクセスできる形式でも保存しません。Folio Producer Service、Distribution Service、Folio Producer Service API、および InDesign の Folio Builder パネルでのみアクセスできます。

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、セキュリティのスペシャリストが集まった専任のチームです。Adobe Digital Publishing Suite 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担っています。ASSET の研究者は、各アドビ製品のセキュリティおよび運用を担当するチームと協力して、製品やサービスに適切なレベルのセキュリティを実装し、さらに開発、導入、運用、インシデント対応に繰り返し実行できる明確なプロセスのセキュリティプラクティスについて、それらのチームにアドバイスします。



アドビのセキュリティ組織

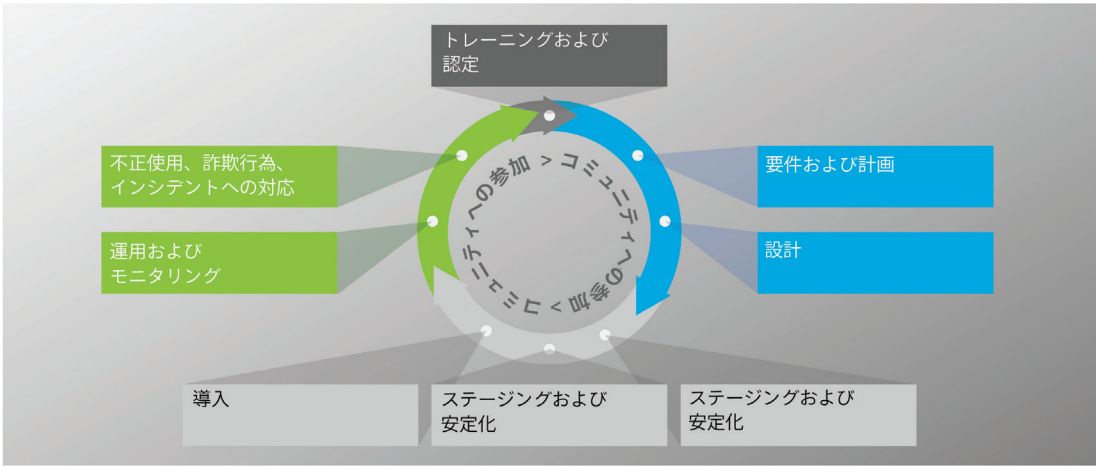
アドビの安全な製品開発

他のアドビの製品およびサービスの組織と同様、Digital Publishing 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、継続的なコミュニティ活動によって補完され、技術、セキュリティプラクティス、脅威の展望に変化が生じても、常に最新状態が保たれるよう進化します。

Adobe Secure Product Lifecycle

Adobe SPLC のコントロールには、それぞれの Digital Publishing Suite コンポーネントに応じて、次のような推奨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のトレーニング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 Digital Publishing Suite 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
- レビュー、レスポンスプラン、開発者向け教材のリリースの準備



Adobe Secure Product Lifecycle（SPLC）

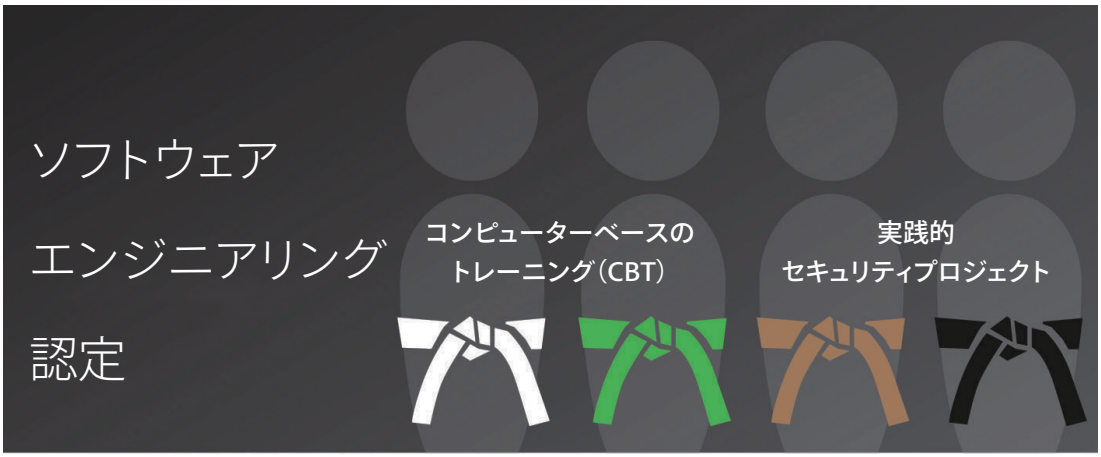
アドビのセキュリティトレーニング

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トレーニングを実施し、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。

プログラムには 4 つのレベルがあり、それぞれに色付きの「帯」（白、緑、茶、黒）が指定されています。白および緑のレベルは、コンピューターベースのトレーニングを修了すると達成されます。さらに上位の茶および黒のレベルは、数か月から 1 年にわたる実務経験を伴うセキュリティプロジェクトを修了する必要があります。茶帯または黒帯を獲得した従業員は、製品チーム内のセキュリティチャンピオンおよびエキスパートになります。新たな脅威や脅威の軽減、さらには新しい規制やソフトウェア言語を反映するために、アドビは定期的にトレーニングを更新します。

Digital Publishing Suite 部門では様々なチームがさらなるセキュリティトレーニング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。



アドビソフトウェアセキュリティ認定プログラム

Adobe Digital Publishing Suite のホスティング

Adobe Digital Publishing Suite のすべてのコンポ―ネントは、アメリカ、ヨーロッパ、アジア太平洋では、Amazon Elastic Compute Cloud（Amazon EC2）、Amazon Simple Storage Service（Amazon S3）などの Amazon Web Services（AWS）でホスティングされています。Amazon EC2 は、クラウド内で規模の変更が可能なコンピューター処理能力を提供し、Web スケールでのコンピューター作業を容易にする Web サービスです。Amazon S3 は、容量に関係なくいつどこでもデータを保存・取得できる冗長性の高いデータストレージインフラストラクチャです。

AWS プラットフォームは、業界標準のプラクティスに従ったサービスを提供し、一般的に業界に認められている認証と監査を受けています。AWS と Amazon のセキュリティ制御について詳しくは、AWS のセキュリティサイトをご覧ください。

AWS とアドビの運用責任

AWS は、ハイパーバイザー仮想化レイヤーから Digital Publishing Suite のコンポーネントが運用される施設の物理セキュリティまでを運用、管理および制御します。一方アドビは、ゲストオペレーティングシステムの管理（アップデート、セキュリティパッチを含む）および AWS が提供するセキュリティグループファイアウォールの設定について責任を負います。

AWS は、アドビが使用するクラウドインフラストラクチャを運用し、処理やストレージをはじめとする様々な基本的コンピューティングリソースを供給します。AWS のインフラストラクチャには、施設、ネットワーク、ハードウェアに加え、それらのリソースの供給と使用をサポートする運用ソフトウェア（ホスト OS、仮想化ソフトウェアなど）が含まれます。Amazon は、業界標準のプラクティスと様々なセキュリティコンプライアンス基準に従って AWS を設計および管理しています。

安全な管理

アドビでは、管理接続用の Secure Shell（SSH）および Secure Sockets Layer（SSL）を使用して AWS のインフラストラクチャを管理しています。

Amazon Web Services（AWS）について

AWS ネットワーク上の顧客データの所在地

AWS で『セキュリティプロセスの概要ホワイトペーパー』を提供しています。AWS のセキュリティについて詳しくは、AWS ホワイトペーパーをご覧ください。

アドビは Digital Publishing Suite のすべての顧客データを Amazon Web Services の米国東部リージョンに保存します。米国内のお客様については、解析データを AWS のカリフォルニア州サンノゼまたはテキサス州ダラスの施設に保存します。米国以外のお客様については、解析データを Amazon Web Services の英国ロンドンの施設に保存します。

Amazon S3 データオブジェクトのデータ複製は、データが保存されるリージョンのクラスター内で行われ、他のリージョンのデータセンタークラスターにデータは複製されません。

顧客データの分離／顧客の分離

AWS は、強力なテナント分離のセキュリティ機能とコントロール機能を使用します。仮想化されたマルチテナント環境として、AWS は、Digital Publishing Suite などの各顧客を他の AWS 顧客から分離するよう設計されたセキュリティ管理プロセスとその他のセキュリティコントロールを実装します。アドビは AWS Identity and Access Management（IAM）を使用してアクセスを制限し、インスタンスを処理および保存します。

セキュアネットワークアーキテクチャ

AWS は、ファイアウォールや他の境界デバイスなどのネットワークデバイスを採用し、ネットワークの外部境界およびネットワーク内の主な内部境界で通信の監視と制御を行っています。これらの境界デバイスは、ルールセット、アクセスコントロールリスト（ACL）、構成を採用し、特定の情報システムサービスに情報を流します。ACL、つまりトラフィックフローポリシーは、各マネージドインターフェイス上でトラフィックの流れを制御します。Amazon Information Security はすべての ACL ポリシーを承認し、AWS の ACL 管理ツールで自動的にそれらを各マネージドインターフェイスにプッシュして、マネージドインターフェイスが最新の ACL を強制するようにします。

ネットワークのモニタリングと保護

AWS は、様々な自動モニタリングシステムを使用して、ハイレベルなサービスパフォーマンスと可用性を提供します。モニタリングツールによって、通信ポイントの入口と出口で異常なアクティビティや承認されていないアクティビティが検出されます。

AWS のネットワークは、次のような従来のネットワークセキュリティの問題に対する強固な保護機能を提供しています。

- 分散サービス妨害（DDoS）攻撃
- 介入者（MITM）攻撃
- IP スプーフィング
- ポートスキャニング
- 第三者によるパケットスニッフィング

ネットワークのモニタリングと保護について詳しくは、Amazon Web サイトの AWS：セキュリティプロセスの概要ホワイトペーパーをご覧ください。

侵入検出

アドビは、業界標準の侵入検知システム（IDS）および侵入防止システム（IPS）を使用して、Folio Producer Service と Distribution Service の両方を積極的に監視します。

ログ記録

アドビは Digital Publishing Suite の顧客行動をサーバーサイドでログ記録し、サービスの停止、顧客に固有の問題、報告されたバグを診断します。ログには、特定の顧客の問題を診断するための Adobe ID のみが保存されます。ユーザー名とパスワードの組み合わせは含まれません。アドビテクニカルサポート認定担当者、主要エンジニア、選定された開発者のみ、起こり得る問題を診断するためにログにアクセスできます。

サービスのモニタリング

AWS は、電気、機械、生命サポートシステムおよび設備をモニタリングし、サービスに関する問題が速やかに特定されるようにしています。また設備の継続的な運用性を維持するために、予防的メンテナンスを実行しています。

データの保管とバックアップ

アドビは Digital Publishing Suite のすべてのデータを、堅牢性の高いストレージインフラストラクチャ、Amazon S3 に保存します。堅牢性を高めるため、Amazon S3 PUT および COPY 操作は、複数の施設で同期をとりながら顧客データを保存し、Amazon S3 のリージョン内で、複数の施設にまたがって、複数のデバイス上で冗長的にオブジェクトを保存します。また Amazon S3 は、すべてのネットワークトラフィックでチェックサムを計算して、データの保存または取得時にデータパケットの破損を検出します。AWS のセキュリティについて詳しくは、AWS：セキュリティプロセスの概要ホワイトペーパーをご覧ください。

変更管理

既存の AWS インフラストラクチャに対する緊急、非定期的、その他の設定の変更は、こうしたシステムで適用される業界基準に従って、認定、記録、テスト、承認を経て、文書化されます。Amazon が AWS を更新するにあたり、顧客への影響は最小限に抑えられます。サービスが悪影響を受ける可能性がある場合、AWS は電子メールまたは AWS Service Health Dashboard を通じて顧客に通知します。アドビもまた Adobe Digital Publishing Suite 用に Status Health Dashboard を保持しています。

パッチ管理

AWS には、ハイパーバイザーやネットワークサービスといった AWS サービスをサポートするシステムにパッチを適用する責任があります。アドビは、ゲストオペレーティングシステム（OS）、ソフトウェア、AWS で実行しているアプリケーションにパッチを適用する責任を負っています。パッチが要求されると、アドビは、実際のパッチではなく、新たに強化した OS およびアプリケーションのインスタンスを供給します。

Adobe Digital Publishing Suite の認証（Adobe ID）

管理者からチームに加わるための招待状を受け取ると、ユーザーは Adobe ID を作成する必要があり、それを Digital Publishing Suite にアクセスするたびに使用します。Adobe ID は、SHA 256 ハッシュアルゴリズムを、様々なパスワードやハッシュイテレーションと組み合わせて使用します。アドビは、異常なアカウントアクティビティがないか継続的に Adobe ID アカウントをモニタリングし、この情報を評価することで Adobe ID アカウントのセキュリティ脅威を迅速に軽減します。

証明書とキーの保管

DPS App Builder は、アプリケーションに署名するため、デジタル証明書とプロビジョニングプロファイルを提供するようユーザーに要求します。すべての証明書は署名するマシンのローカルにあり、この処理中にアドビ（または AWS）に転送されることはありません。

購読の検証プロセスを完了するため、購読のアプリケーション内購入が可能なアプリケーションでは、お客様は構築したアプリケーションごとにアプリケーションストアの共有キーを登録する必要があります。これは秘密キーで、このキーが iOS SDK を使用した購読検証プロセスの一部としてどのように転送、保存、使用されるかに関し、アドビは Apple のガイダンスに従います。

アドビの iOS 向けプッシュ通知サービスの使用を選択したユーザーは、アドビのサーバーにプッシュ証明書をアップロードする必要があります。アドビはプッシュ証明書のサードパーティの管理について、Apple のガイダンスに従います。

アドビのリスク／脆弱性管理

セキュリティテスト

アドビでは、認可された第三者たるセキュリティ企業と協力して侵入テストを実行し、潜在的なセキュリティ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。ベンダーのレポートを受け取り次第、アドビは発見された脆弱性を文書化し、深刻度と優先度を評価した上で、適切な軽減策や修復計画を作成します。

アドビは、リリースの前に毎回Digital Publishing Suiteサービスのセキュリティスキャンを実施します。このセキュリティスキャンは、Digital Publishing Suite だけでなくアドビがホストするすべての製品とサービスのセキュアネットワークトポロジおよびインフラストラクチャの構築に信頼のある、高度なトレーニングを受けた運用スタッフが実施し、ファイアウォール、ロードバランサー、サーバーハードウェアをまたいでセキュリティの弱いネットワーク設定の問題を探します。プレリリースのセキュリティスキャンは、依頼に応じて機密保持契約に基づきご利用いただけます。

アドビのテクニカルサポートに連絡をいただけば、Digital Publishing Suite の外部向けインフラストラクチャに独自の外部セキュリティスキャンを実行することができます。ただし、外部向け Digital Publishing Suite システムでの侵入テストとロードテストは実施できません。これを実施しようとするお客様は Digital Publishing Suite の利用条件に違反し、アドビはこれに対し取引を終了またはサービスを一時停止する権利を有します。

インシデント対応と通知

新しい脆弱性や脅威は進化しているため、アドビは新たに発見された脅威に懸命に対処し、その軽減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。

重大な脆弱性がアナウンスされると、Adobe PSIRT（Product Security Incident Response Team）が Digital Publishing Suite 組織内の該当するチームに脆弱性について通知し、軽減策を講じます。

AWS データセンターに影響を及ぼすインシデントや脆弱性、脅威については、Amazon の事故管理チームが、業界標準の診断手順を用いて、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制でインシデントを検出し、影響と解決方法を管理して、アドビや AWS の他の顧客に知らせます。

Digital Publishing Suite では、セキュリティコーディネーションセンター（SCC）でインシデントへの対応や意思決定、外部モニタリングも一元的に管理し、全機能の一貫性と問題の迅速な解決を実現します。

問題が発生した場合、SCC は Digital Publishing Suite のインシデント対応チームおよび開発チームと連携して、次の実績あるプロセスを使用して問題を特定、軽減、解決します。

- 脆弱性の状態評価
- プロダクションサービスにおけるリスクの軽減
- セキュリティが侵害されたノードの検疫、調査、破棄（クラウドベースのサービスのみ）
- 脆弱性のための修正プログラムの開発
- 問題を阻止する修正プログラムの展開
- 動作のモニタリングと解決策の確認

フォレンジック分析

インシデントの調査に関して、アドビは業界標準のツールと手法を用います。アドビは、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などのフォレンジック分析プロセスに準拠しています。さらに捜査または起訴が必要な場合、アドビは法的機関と協力することもあります。

AWS データセンターの物理統制と環境統制

AWS の物理統制と環境統制については、SOC 1、Type 2 レポートに具体的に記載されています。次のセクションでは、世界各地の AWS データセンターで実施されているセキュリティ対策をいくつか紹介します。AWS のセキュリティについて詳しくは、AWS：セキュリティプロセスの概要ホワイトペーパーまたは Amazon セキュリティ Web サイトをご覧ください。

物理設備のセキュリティ

AWS データセンターは、業界標準の構造的かつ工学的アプローチを採用しています。AWS データセンターは、外部からはそれとはわからないようになっています。専門のセキュリティスタッフ、ビデオ監視カメラ、侵入検出システム、その他の電子的手段を用いて、建物の入口とその周辺の両方で物理的アクセスを制御しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。

AWS は、必要とする正規の手続きを有する従業員や業者に対してのみ特権を与え、データセンターへのアクセスや情報を提供しています。従業員がこれらの特権を必要とする作業を完了したら、引き続き Amazon または Amazon Web Services の従業員であったとしても、そのアクセス権は速やかに取り消されます。AWS 従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。

火災抑制

すべての AWS データセンターには、自動火災検出装置および鎮火装置が取り付けられています。この火災検出システムは、全データセンター環境、機械電気インフラ空間、冷却室および発電機設備室において、煙検出センサーを使用しています。これらのエリアは、充水型、二重連結予作動式、またはガス式スプリンクラーシステムによって守られています。

コントロールされた環境

AWS は、サーバーその他のハードウェアの運用温度を一定に保つために、天候コントロールシステムを採用することで、過熱を防ぎ、サーバー停止の可能性を減らしています。AWS データセンターは、大気の状態を最適なレベルに保つように設定されています。AWS の作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。

バックアップ電源

AWS データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1 日 24 時間、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給します。データセンターは、発電機を使用して施設全体のバックアップ電力を供給します。

ビデオ監視

専門のセキュリティスタッフが、ビデオ監視カメラ、侵入検出システム、その他の電子的手段を用いて、AWS データセンターの建物の入口とその周辺の両方で物理的アクセスを厳しく管理しています。

障害回復

AWS データセンターは、高いレベルの可用性を備え、影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。すべてのデータセンターは、世界各地にクラスターの状態で構築されています。24 時間、365 日体制のサービスをオンラインで顧客に提供しており、「コールド」の状態のデータセンターは存在しません。障害時には、自動プロセスが、影響を受けるエリアから顧客データを移動します。重要なアプリケーションは N+1 設定で配備されるので、データセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。AWS 障害回復プロトコルについて詳しくは、Amazon セキュリティ Web サイトでご覧ください。

アドビの所在地

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全社的に実装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。訪問者には常に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

アドビは、Folio Producer Service に送信されたすべてのコンテンツのウイルスをスキャンしてからアドビのシステムに保存します。

アドビの従業員

従業員による顧客データへのアクセス

技術的なコントロールを使用して、稼働しているシステムへのネットワークレベルおよびアプリケーションレベルでのアクセスを制限し、セグメント化された Digital Publishing Suite の開発と生産環境を維持します。従業員は開発や生産システムにアクセスするための特定の権限を付与されます。

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。アドビが通常調べる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行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。

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。

セーフハーバー

アドビシステムズ社（当社の米国本社）は EU セーフハーバープライバシープログラムを遵守しています。

セキュリティコンプライアンス

Amazon Web Services（AWS）は、ISO27001、SOC2 およびその他のセキュリティフレームワークの認証を取得し維持しています。

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、Digital Publishing Suite データをセキュリティ保護しています。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ています。

アドビの製品とサービス全体へのセキュリティの取り組みについて詳しくは、アドビのセキュリティ情報サイトをご覧ください。

アドビ システムズ 株式会社
〒 141-0032 東京都品川区大崎 1-11-2
ゲートシティ大崎 イーストタワー
www.adobe.com/jp

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

本書の情報は予告なく変更される場合があります。アドビのソリューションとコントロールの詳細については、アドビのセールス担当者にご相談ください。SLA、変更承認プロセス、アクセスコントロール手順、障害回復プロセスを含むアドビのソリューションについて、さらに詳しくご説明します。

5/14