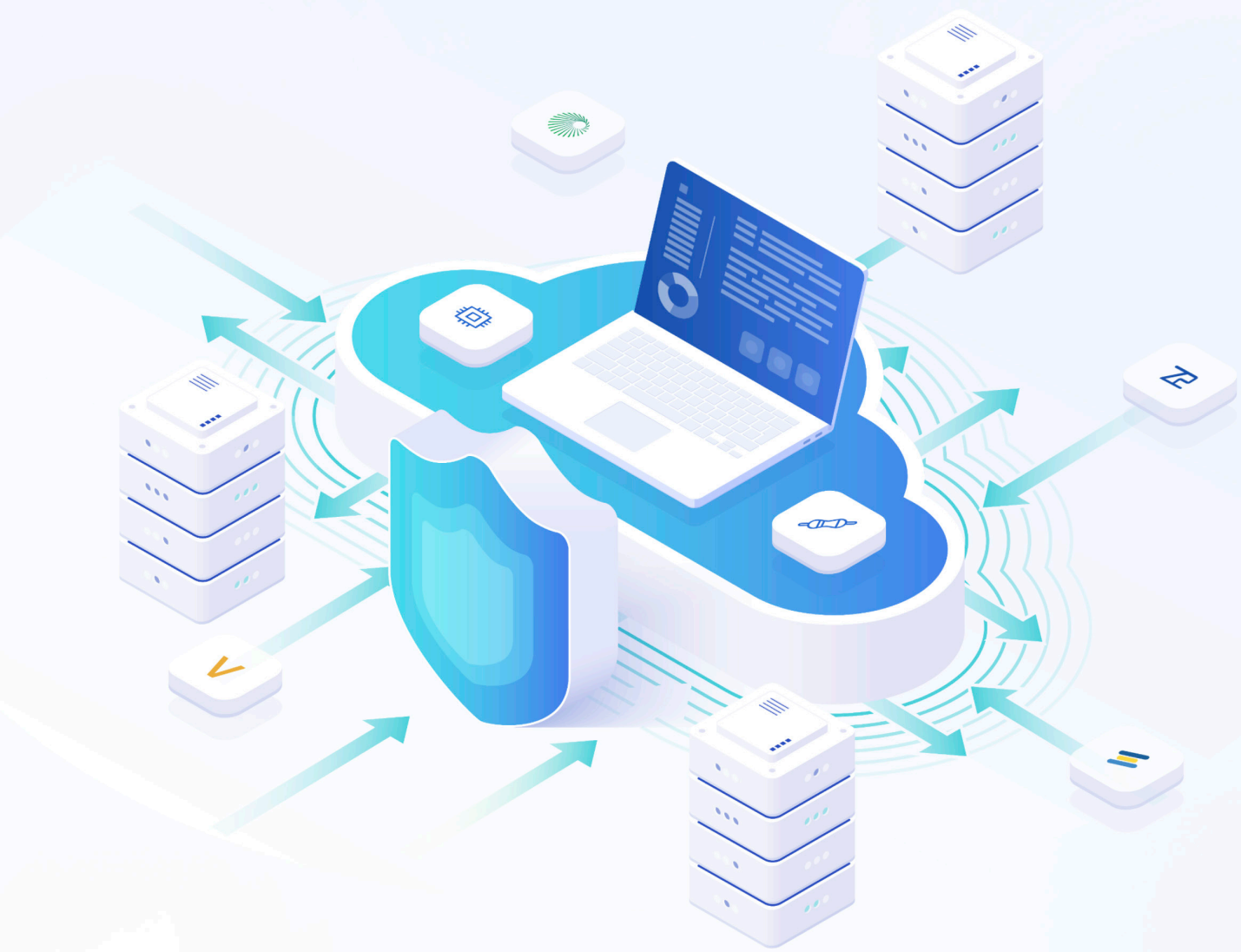
ALTIUM 365

セキュリティへの取り組みと実践



CONTENT

はじめに

Altium 365は、設計、データ、共同作業を単一の安全なクラウド環境に統合する電子機器開発プラットフォームです。電子機器開発の全ライフサイクルを対応するように構築されており、エンジニアリングチームがより迅速、かつ効率的に、そして大規模に作業するために必要な最新のインフラストラクチャを提供します。Altium Agile、およびAltium Developに含まれるこのプラットフォームは、ワークフローを効率化し、生産性を向上させ、製品の提供を加速します。

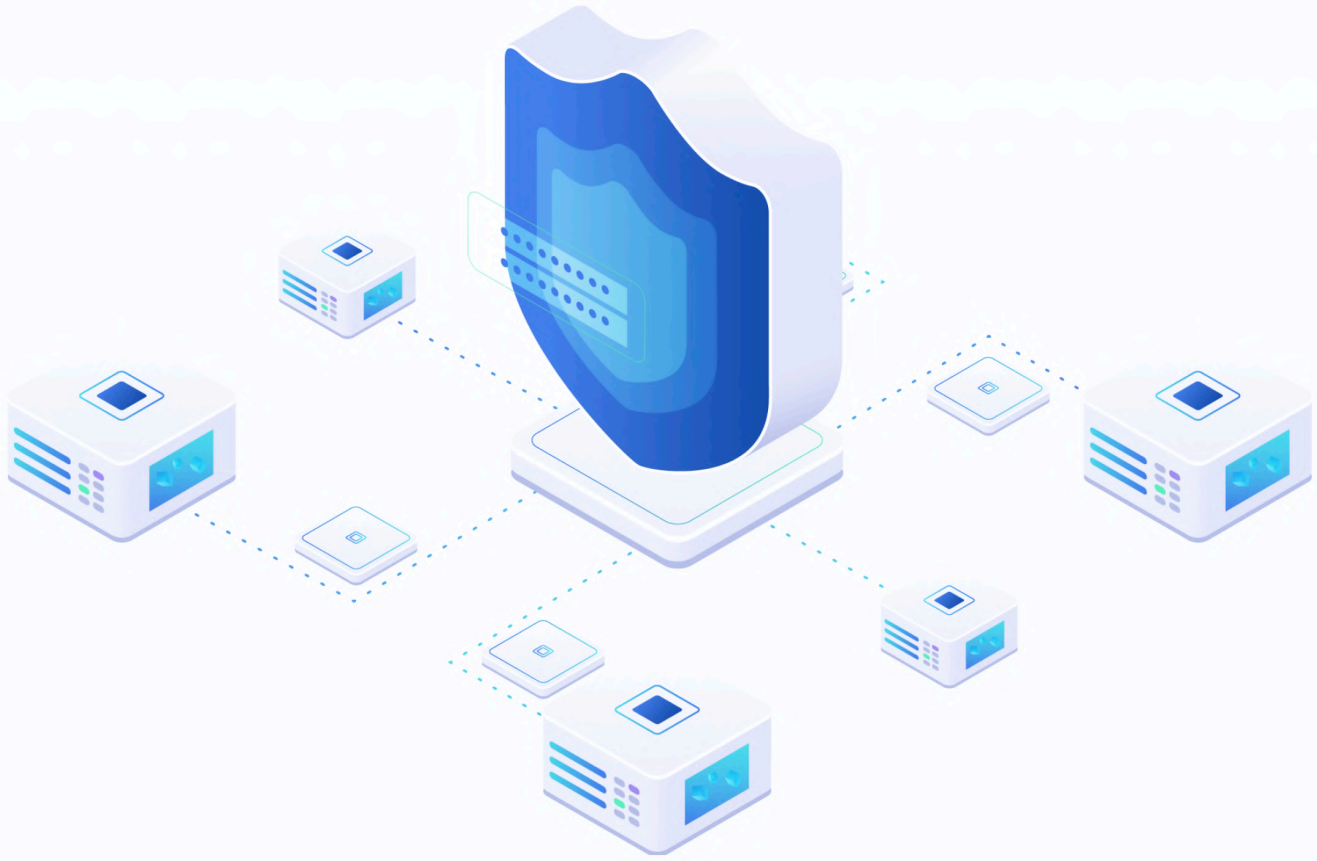
Altiumでは、クラウドプラットフォームの真の価値は、それによって何が可能になるかだけでなく、託された作業をどれだけ安全に保護できるかによっても測られると考えています。セキュリティはAltium 365のアーキテクチャの中核に組み込まれており、プラットフォームの設計、構築、運用の指針となっています。この取り組みにより、私たちは最新のサイバーセキュリティ基準を満たし、継続的に上回ることを目指しています。

このホワイトペーパーでは、Altium 365を支える広範なセキュリティ対策を明確かつ透明性の高い形で説明します。私たちの目標はシンプルです。皆様のデータがどのように保護されているか、保護対策がどのように設計されているか、新たな脅威に先んじるためにセキュリティ体制がどのように進化しているかをお伝えすることです。

これらのページを読み進めることで、安全な開発手法からプラットフォーム全体に組み込まれた多層制御に至るまで、Altiumの方法を形作る計画、プロセス、保護メカニズムについて理解を深めることができます。Altiumの厳格なエンジニアリング、運用規律、クラウドネイティブアーキテクチャがどのように連携し、あらゆる段階でお客様のデータを保護しているかをご覧いただけます。

最終的に私たちが目指しているのは、堅牢で継続的に進化するセキュリティフレームワークによってAltium 365での共同作業が保護されているという安心感を提供することです。共同作業を保護するセキュリティは私たちに任せ、皆様には創造と革新に専念していただきたいと考えています。

本書では、プラットフォームレベルでのAltium 365のセキュリティ方法と実践について説明します。具体的な機能は、サブスクリプション、導入環境 (GovCloudなど)、お客様の構成によって異なる場合があります。



Altium 365 セキュリティ対策

セキュリティは信頼の基盤です。お客様は、最も価値のある資産であるデータ、設計、知的財産の保護をAltium 365に委ねています。セキュリティは、初期のアーキテクチャと開発から、展開、継続的な運用に至るまで、プラットフォームのあらゆる層に組み込まれています。Altiumの方法は、綿密、かつ積極的で、継続的に進化しており、共同での電子機器開発に安全で強靭な環境を提供します。

セキュリティ駆動型開発

私たちは、ユーザーのセキュリティを念頭に置いて、Altium 365プラットフォームとその特長、および機能を開発しました。開発の各段階で、導入されているセキュリティ対策を厳格に検証しています。これには、広範なアーキテクチャレビュー、依存関係のスキャン、コードレビュー、動的アプリケーションセキュリティテストが含まれます。私たちの目的は、潜在的なセキュリティ脆弱性を開発当初から事前に特定し、対処して、防止することです。さらに、独立した第三者機関によるテストを実施し、セキュリティフレームワークの堅牢性を確保しています。

信頼性の高いデータ保護

Amazon Web Services (AWS) は、Altium 365の物理的なセキュリティと信頼性を支える基盤となっています。お客様のデータはAWSリソース内にのみ保存し、データベースにはRelational Database Service (RDS) を使用しています。標準的なバイナリデータの保存にはAWS S3を使用し、高性能なバイナリストレージが必要な場合にはFSxを使用しています。高性能な検索機能を提供するため、専用のElasticsearchクラスターを使用しています。

Altium 365内の保存データは、AWS Key Management Service (KMS) を使用して暗号化されます。これらの鍵では、暗号モジュールの承認に使用される米国政府のコンピューターセキュリティ規格であるFIPS 140-2規格に基づいて検証されたハードウェアセキュリティモジュールを使用しています。これらの暗号鍵の使用は、ログに記録され、監視されます。その後、ログは私たちのセキュリティ情報イベント管理 (Security Information and Event Management (SIEM)) システムに送信され、暗号鍵がいつ使用されたかを追跡できるようになります。

お客様のデータを管理するAltium 365インフラストラクチャへのアクセスは、最小権限の原則に基づき、権限を付与された担当者のみに制限されています。すべてのアクセスはログに記録され、監査可能な状態にあり、Altiumの専任セキュリティチームによって継続的に監視されます。

セキュア通信

Webブラウザー、Altium Designer、モバイルアプリケーションなどのAltium 365クライアントとAltium 365クラウドプラットフォームとの通信は、安全で信頼できる接続を確保するため、標準ポートを介したインターネット通信の標準的な手法であるHTTPSプロトコルを使用する場合にのみ許可されます。

認証とアイデンティティ管理

機密性の高い顧客データを管理するAltium 365のサービスにアクセスするには、ユーザーはリクエストごとに認証プロセスを経る必要があります。この認証は、従来のユーザー名とパスワードの入力に限定されるものではなく、シングルサインオン (SSO) システムや、GoogleやFacebookのようなIDプロバイダー (Identity Providers (IdPs)) とも統合されています。これらのシステムでは、ハードウェアキー、スマートカード、指紋などの生体データを含むさまざまな認証情報が使用される場合がありますが、これらは当社が直接管理するものではありません。どの方法であっても、セキュリティ上の理由からすべてのセッションには期限が設けられており、機密性の高いログイン情報は送信中に安全に暗号化されます。

Altium 365は、SAML 2.0プロトコルを使用したSSOを対応しています。この機能は、OneLogin、Okta、Microsoft Azure AD、Google Identityなど、最新の主要なIdPと統合できます。SCIMプロトコルの拡張対応により、ユーザーとグループのプロビジョニング、およびプロビジョニング解除を一元的に管理できます。IdPによっては、多要素認証 (multi-factor authentication (MFA)) による強化された保護を選択できます。

分散と制御

Altium 365では、Webアプリケーションファイアウォールや管理されたロードバランシングなどの多層的な境界防御を採用し、受信トラフィックをコントロール、および検査しています。これらの管理策により、インターネットに接続するエンドポイントを保護するとともに、アプリケーションサービス全体にトラフィックを分散して可用性を確保しています。本番システムへの管理アクセスは、最小権限の原則に基づいて権限を付与された担当者のみに制限され、ログに記録されて監視されます。

シングルテナント、およびマルチテナントアーキテクチャー

Altium 365はマルチテナントアーキテクチャで運用されており、現在ワークスペースの概念に対応している各テナントには、分離された独自のデータベーススキーマが割り当てられます。このモデルでは、共有クラウドインフラストラクチャを活用して効率性と拡張性を確保しながら、データを確実に分離します。より高度な分離、カスタマイズ、運用管理を必要とする組織向けに、AltiumはSingle Tenant Environment (STE) を提供しています。これは、アプリケーションとそのサポートインフラストラクチャの専用インスタンスです。STEは、高度なデータ分離、予測可能なパフォーマンス、テナント固有の構成オプションを提供し、管理されたサービスの利便性と、従来はオンプレミス環境でしか得られなかったコントロールを兼ね備えています。

脆弱性スキャン

Altium 365の製造環境への展開では、リリースプロセスの一環として脆弱性スキャンが実施されます。検出された問題は、Altiumの脆弱性管理方針と定められた修正期限に従って、修正が完了するまで追跡されるか、リスクの受容がドキュメント化されます。

第三者機関による試験

私たちは、絶えず進化する脅威に対して最高水準のセキュリティを維持するため、外部の第三者機関と連携して毎年侵入テストを実施しています。開発チームは侵入テストで得られたすべてのフィードバックを確認し、アプリケーション、サービス、インフラストラクチャに必要な更新を実施します。秘密保持契約 (Mutual Non-Disclosure Agreement (MNDA)) を締結している場合、ご関心のある方には、侵入テストレポートの最新の要約を提供いたします。

セキュリティ監視、およびインシデント管理

私たちは、セキュリティインシデントを早期に検出し、効果的に対応できるよう、包括的なログ記録と監視の手法を導入しています。NISTサイバーセキュリティフレームワークを基盤として、ログ記録と監視を「検知」機能と「対応」機能の主要な構成要素としています。これらの機能は、セキュリティイベントと脆弱性を特定して把握し、Altium 365の正確性と精度を高めるうえで不可欠です。インシデントの特定は、私たちのインシデント対応プロセスの基盤です。このプロセスでは、セキュリティチーム、システム、ツールが連携して、潜在的なセキュリティインシデントを認識し、確認します。セキュリティインシデントが特定されると、組織のセキュリティ目標とビジネス目標に沿って迅速、かつ効果的に対応できるよう、インシデント対応計画を実行します。

セキュリティ意識向上、およびトレーニング

Altiumは、全新入社員がオンボーディング中にセキュリティ意識向上トレーニングを受け、全スタッフが毎年復習トレーニングを受けることを保証しています。人事チームは、コンプライアンスを確保するため、トレーニングを完了していない従業員に対してフォローアップを行います。さらに、新しいプロトコルや潜在的な脅威についてスタッフに知らせるため、セキュリティ意識向上に関する通知を定期的に送信しています。当社の研究開発チームは、セキュアコーディングの実践に関する専門的なトレーニングを受けています。トレーニング教材は、コーディングの実践やプログラミング言語を反映させるために、定期的に見直しと更新が行われています。

データプライバシー

当社のAltium一般利用規約とプライバシーポリシーには、お客様のデータのプライバシーとセキュリティを確保するために当社が講じる措置が記載されています。これらの文書と社内の関連手順は、GDPRやカリフォルニア州消費者プライバシー法 (California Consumer Privacy Act (CCPA)) など、世界各国のデータ保護規制に準拠しています。この準拠により、お客様やビジネスパートナーから当社に託された情報を含め、Altiumが管理するすべてのデータの機密性、完全性、可用性が確保されます。今日の競争の激しいグローバルビジネス環境では、エラー、損失、不正、スパイ行為などを防ぎ、保存データのプライバシーを維持することが極めて重要です。当社の方法は、当社が取り扱うデータのセキュリティ侵害を防止するように設計されています。

クッキーポリシー

クッキーの設定は、ブラウザーの設定を通じて管理できます。一部のブラウザーでは、クッキーを受け入れるサイトをホワイトリストに登録できます。クッキーの設定の管理の詳細については当社のクッキーポリシーをご覧ください。

データ保持ポリシー

Altium 365の使用を停止した場合、お客様のデータは、データ保持ポリシーに定められた期間に従って保持されます。この期間が終了すると、お客様のデータはAltiumのシステムから消去されます。

バックアップと災害復旧

Altium 365は自動バックアップシステムを採用しており、Altium 365に保存されたすべてのデータがバックアップリジョンにコピーされるため、手動による介入は不要です。当社は、製造サービス、およびプラットフォームの事業継続を対応するための包括的な災害復旧計画を策定しています。システム障害が発生した場合、目標復旧時点 (Recovery Point Objective (RPO))、および目標復旧時間 (Recovery Time Objective (RTO)) をそれぞれ24時間以内とすることを目標としています。この計画は120日ごとに見直しとテストが行われ、その有効性が確認されています。また、災害時にサービスを復旧させるための詳細な方針と手順が含まれています。

詳細については、Altium 365 Trust Centerにアクセスして、よくある質問への回答をご確認ください。

Altium 365 GovCloud

Altium 365 GovCloudは、米国内にあるAltium 365クラウドプラットフォームの専用領域であり、AWS GovCloudリージョンの米国人のみが運営しています。GovCloud領域のAltium 365 workspaceを選択することで、組織はITARやEARなどの米国政府の規制に準拠しやすくなります。

米国人

Altium側でのGovCloudリジョンの運用は、米国人 (US Persons) のみに制限されています。Altiumのお客様は、workspaceに追加するユーザーと、workspaceに保存されているデータへのアクセス権を付与するユーザーを決定、および管理できます。

データ保護

送信トラフィック制御

不正なデータのエクスポートを防ぐため、環境外への不正な送信トラフィックをコントロール、および阻止するアウトバウンドプロキシを使用しています。

機能の制限

米国外への意図しないデータ流出につながる可能性のある機能はデフォルトで無効にし、ユーザーエラーに伴うリスクを軽減しています。

- **Workspace外との共有。**デフォルトでは、Altium 365 GovCloud workspaceに属していないユーザーとプロジェクト、リリース、ライブラリ、製造パッケージを共有する機能 (「製造元に送信」機能) は無効になっています。この設定は、必要に応じて管理者が変更できます。
- **Altium 365 Personal Space。**Altium 365 GovCloud workspaceに追加されたユーザーは、自分のAltium 365 Personal Spaceにデータを保存できません。
- **PLM統合。**サードパーティのPLMシステムへの接続は管理者が制御し、必要な設定を行います。
- **クライアントシステム。**Altiumの責任は、Altium 365 GovCloudに接続するブラウザーやCADツールなど、お客様側のシステムの構成、セキュリティ、保守には及びません。お客様は、これらのシステムを最新の状態に保ち、必要な更新とパッチをすべてインストールする必要があります。

米国内

AWS GovCloudのUS-EastおよびUS-Westリージョンは、米国国内に所在する米国市民である従業員によって運営されています。

アクセス制御

米国外からのワークスペースへのアクセス

米国外からworkspaceへのアクセスは明示的にブロックされます。これには、米国人が他国からworkspaceにアクセスしようとする場合も含まれます。VPNアクセスの詳細については、こちらをご覧ください。

詳細については、Altium 365 GovCloudをご覧ください。

コンプライアンス: 認証と規制

コンプライアンスは、単にチェックボックスにチェックを入れることではありません。卓越性への取り組みであり、信頼性を保証するものです。Altium 365では、この責任を真摯に受け止め、プラットフォームが最高水準のコンプライアンス基準と認証基準を満たすよう徹底しています。

CSA STAR Level 1: 自己評価

Security、Trust、Assurance、Risk (STAR) プログラムは、クラウドコンピューティング向けの堅牢な保証フレームワークを提供するためにCloud Security Alliance (CSA) が策定した取り組みです。Altium 365はCSAのSTAR Level 1を取得しています。これは、一般にConsensus Assessment Initiative Questionnaire (CAIQ) として知られる質問書を使用して、Cloud Controls Matrix (CCM) の統制への準拠を自己証明するものです。そのため、Altium 365はSTARレジストリに掲載されています。

SOC 2 Type 2保証報告書

Altium 365はService Organization Control (SOC) 2 Type 2保証報告書を取得しており、セキュリティ原則に関して、データ、およびシステムのセキュリティに関する最高水準の基準を維持していることが確認されています。このサイバーセキュリティコンプライアンスフレームワークは、米国公認会計士協会 (American Institute of Certified Public Accountants (AICPA)) によって策定されたもので、企業はAICPA認定の外部監査人による監査を受ける必要があります。Altium 365は、SOC 2 Type 2監査を毎年、実施しています。

GDPR

私たちはデータプライバシーの重要性を認識し、一般データ保護規則 (General Data Protection Regulation (GDPR))で定められた厳格な要件を遵守して、お客様のデータが細心の注意と敬意をもって取り扱われるよう徹底しています。

ITARコンプライアンス

Altium 365 GovCloudは、お客様が国際武器取引規則 (International Traffic in Arms Regulations (ITAR)) に準拠できるよう支援します。この専用領域は、規制の厳しい業界で活動するユーザーの特定の要求を満たします。

Altium 365のセキュリティ、およびガバナンス機能

Altiumは、組織が機密性の高い設計データを保護し、コンプライアンスを維持し、大規模にアクセスを管理できるよう支援する、高度なセキュリティ、ID、ガバナンス機能を提供します。

アクセスコントロール

- **基本データ権限**
  プラットフォーム全体でユーザーがファイル、フォルダー、プロジェクトをどのように操作できるかを定める、基本的な表示、および編集権限です。
- **高度なデータ権限**
  組織レベルの共有ルール、きめ細かな権限設定、高度な継承オプションなど、基本的なアクセス権限を超えるコントロールにより、チーム間でデータにアクセスする方法やアクセスを制限する方法を定めます。
- **グループ管理**
  定義された役割に基づいてアクセス権を割り当てることで、権限、ライセンス、workspaceの可視性を標準化し、組織全体で一貫性と拡張性のある制御を実現します。
- **外部ゲストの対応**
  可視性ルールと適用されるワークフローにより、外部の共同作業者を招待してグループ化し、そのアクセスを制限する方法を管理して、ゲストアクセスを限定された安全な範囲に維持します。
- **アクセスフィルター**
  すべてのプロジェクトで実効アクセス権を検索、および監査し、すばやく調整したり、ワンクリックでゲストを削除できます。

認証とユーザープロビジョニング

- **組織管理**
  ユーザーが組織に参加する方法、役割を割り当てる方法、ドメインベースのルールによって内部リソースへのIDとアクセスを管理する方法を定義します。
- **シングルサインオン (SSO)、およびSCIM**
  既存のIDプロバイダーと統合して認証を一元化し、SCIMを通じてユーザーのプロビジョニングとプロビジョニング解除を自動化します。
- **多要素認証 (Multi-Factor Authentication (MFA))**
  追加の認証ステップを要求することでアカウントのセキュリティを強化し、資格情報が漏洩した場合でも不正アクセスのリスクを低減します。
- **グループ管理**
  オンボーディング中、およびライフサイクル全体を通じて、ユーザーを事前定義された役割やアクセスプロファイルに合わせることで、IDプロビジョニングを対応します。

高度なセキュリティ

- **IPホワイトリスト**
  承認されたIPアドレス、またはIP範囲にプラットフォームへのアクセスを制限し、信頼できるネットワークのみが機密性の高い組織データにアクセスできるようにします。
- **イベントログ**
  workspace全体のユーザー、およびシステムの動作を可視化し、明確なタイムスタンプ付きの活動記録によって、監査、セキュリティレビュー、コンプライアンス報告を支援します。
- **SIEM (API)**
  Altium Agileのイベントデータを既存のSIEMに接続し、組織全体での一元的な分析、アラート通知、コンプライアンス追跡を可能にします。

当社の最新のセキュリティ更新に関する情報をご確認ください

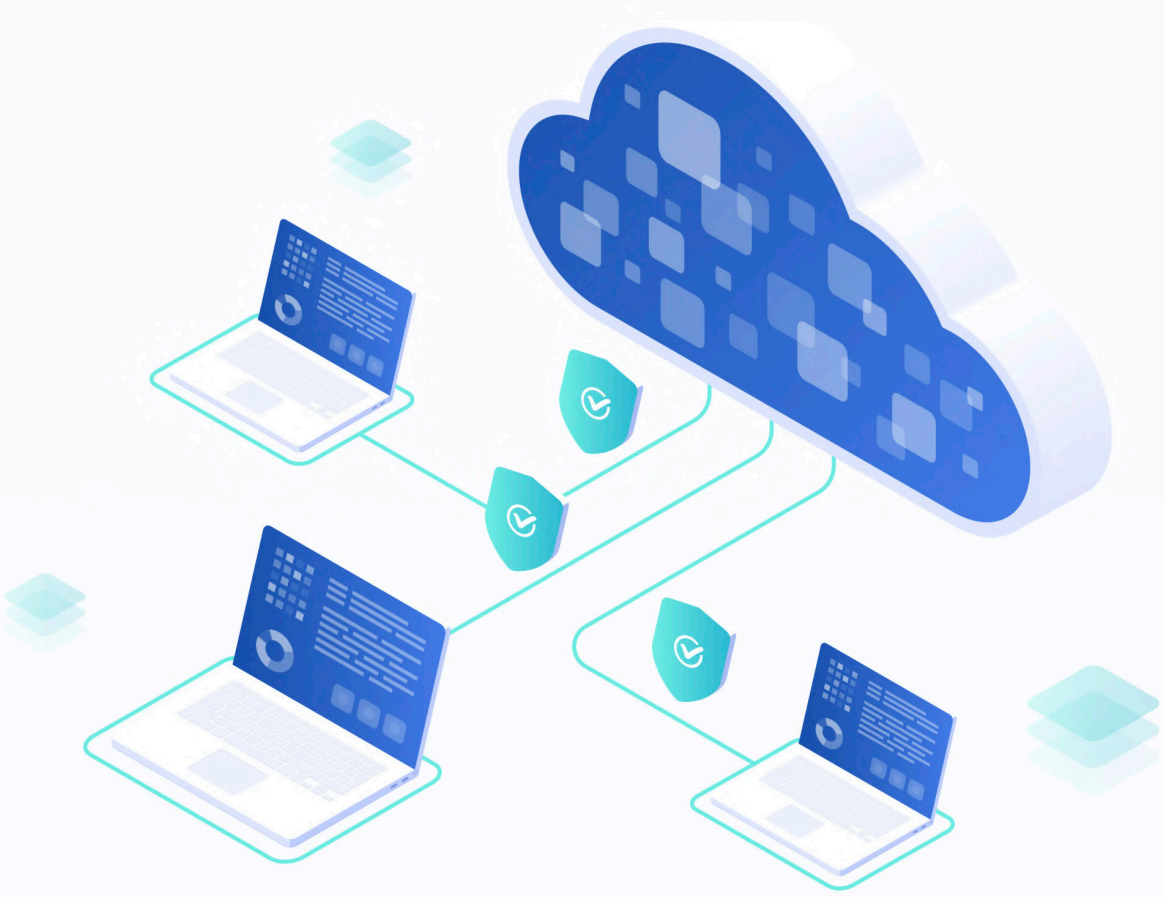
当社のプラットフォームは、ガバナンスを強化し、可視性を高め、現代のエレクトロニクス組織のセキュリティ要件をサポートする新しい機能によって進化を続けています。セキュリティは基盤であり、すべてのアップデートは、機密データや規制対象データのコントロールを維持しながら、チームが迅速に作業を進められるように設計されています。

電子機器開発とデータ保護を取り巻く環境の変化に合わせて、私たちも進化を続けています。私たちが重視しているのは、現在の要求に対応しながら、組織が今後の変化に備えられる、実用的で拡張性のある改善を提供することです。

セキュリティと革新の整合性を維持できるよう、管理策の拡充、監視の強化、保護の強化を進めています。今後も継続的な機能強化にご期待ください。

詳細、および関連リソースについては、altium.com

詳細は、こちらをご覧ください。 www.altium.com/platform/trust



このホワイトペーパーに記載されている情報は、2026年2月時点のものです。Altium 365は進化を続けるプラットフォームです。本書の最新版については、このページをご覧ください。