Autodesk
Construction Cloud®

AUTODESK

セキュリティ ホワイトペーパー

はじめに

Autodesk Construction Cloud® は、プロジェクトのライフサイクル全体に渡ってパフォーマンスを改善できるように設計されたクラウドベースの設計および建設プロジェクト管理プラットフォームです。セキュアなクラウドベースのプラットフォームとして、Autodesk Construction Cloud® は、顧客データの保護に貢献しながら、設計および建設現場でコラボレーションするメリットを提供します。

Autodesk Construction Cloud® は、最先端のクラウドソフトウェア技術を活用して設計および構築されており、Amazon Web Services（AWS）を利用し ています。オートデスクは、お客様がオートデスクを信頼し、頼りにしていることを理解しており、その責任を重く受け止めています。そのため、オートデスクのサービスは、セキュリティとレジリエンスを維持しながら拡張性を確保できるよう、基盤から設計されています。

本ドキュメントでは、Autodesk Construction Cloud® の運用、ソフトウェア開発、およびその環境に実装されているセキュリティ対策の概要を説明します。

ドキュメントの目的と範囲

内容

このホワイトペーパーには、Autodesk Docs、Autodesk Build（PlanGrid Build を含む）、Autodesk Takeoff、および Autodesk BIM Collaborate Pro（Revit® Cloud Worksharing、Collaboration for Civil 3D®、および Collaboration for Plant 3D® を含む）内のすべてのモジュールおよびサービスが含まれます。

本書に含まれない内容

このホワイトペーパーには、Assemble、BuildingConnected、Pype、ACC Connect、BIM 360 Field、BIM 360 Glue、BIM 360 Plan、BIM 360 Ops、および BIM 360 Team、ならびに本書に記載されていない製品は含まれません。
次のサービスに関する情報が含まれています。

- クラウド サービス
- エンジニアリング
- 製品セキュリティ コントロール

オートデスク製品のセキュリティ プラクティスの詳細については、

- 「Autodesk Trust Center」をご覧ください
- 「Autodesk Trust Center コンプライアンス」をご覧ください

クラウド サービス

エンジニアリング
製品セキュリティ コントロール

クラウド サービス* チームは、アプリケーション リリース管理、コア システムのアップグレード、システムの正常性監視、Autodesk Construction Cloud® のメンテナンスに必要なその他のアクティビティの手順を定義および実行します。

高可用性

オートデスクは、堅牢で高可用性のサービスをお客様に提供することに注力しています。土木・インフラ計画および設計において冗長性を重要な原則とすることで、オートデスクは業界をリードする稼働率とデータ保護レベルを維持しています。Autodesk Construction Cloud® は、Web サーバーおよびアプリケーション サーバー、バックグラウンド ジョブ処理システム、レポート実行システム、ならびにデータ ストレージ システムで構成されています。

オートデスクは、データ ストレージに Amazon Web Services（AWS）を活用しています。各リージョン内では、データのコピーが常に複数の物理的な AWS アベイラビリティ ゾーンに保存されます。これらの取り組みにより、オートデスクのお客様をデータ損失から保護します。プロジェクト データ（場合によっては「対象コンテンツ」とも呼ばれる）のプライマリ ストレージの格納場所は、お客様のアカウントを管理しているデータ格納リージョンです。対象となるサービスについては、Autodesk Construction Cloud® 製品を使用するお客様は、対象コンテンツのプライマリ ストレージのリージョンを選択できます**。プロジェクト データには、お客様またはお客様が許可したユーザによって本サービスに送信またはアップロードされた、プロジェクト ファイル、モデル、図面、データ セット、画像、ドキュメント、またはこれらに類する資料が含まれます。また、オートデスク サービスが、お客様自身の未処理データまたは情報を基に生成した特定の出力や、バイナリ データや設計オブジェクト自体には含まれない、プロジェクト ファイルに関連付けられたメタデータも含まれます。たとえば、個人データ（作成者名など）、タイムスタンプ、アクティビティ ストリームなどが該当します。

* クラウド サービス チームは、オートデスクではクラウド インフラストラクチャ チームまたはクラウド オペレーション チームと呼ばれる場合もあります。
** 対象となるサービスおよびリージョン別ストレージの場所の一覧については、「地域データ ストレージに関する FAQ」を参照してください。

クラウド サービス

エンジニアリング
製品セキュリティ コントロール

ビジネスの継続性およびデータ センターの冗長性

オートデスクの事業継続計画および災害復旧計画は、Amazon Web Services（AWS）を活用し、高い稼働率と低い中断率を実現するサービスと、業界をリードするデータ保護をお客様に提供しています。

データの安全性を確保するため、オートデスクはインフラストラクチャを複数の地理的リージョンに分散して展開し、同時に複数の物理データ センターへデータのコピーを保存しています。さらにオートデスクでは、事業継続計画および災害復旧計画を定期的にテストし、導入されているポリシーや手順が最新であり、業界のベスト プラクティスに準拠していることを確認しています。複数の AWS アベイラビリティ ゾーン（AZ）に渡る配置の一環として、 24 時間 365 日の運転を維持するために冗長な電力システムが設置されています。これには、停電が発生した場合に備えた長期的なバックアップ電源用の無停電電源装置（UPS）および発電機も用意されています。冗長なマルチベンダー システムが、AWS の各データ センターへのインターネット接続を維持するために使用されています。

クラウド サービス

エンジニアリング
製品セキュリティ コントロール

データ複製

顧客データは、別々の AWS AZ にあるデータ センター間で複製されます。複製は、バックアップ データ センターへのフェイルオーバーが必要となった場合に、データ損失や遅延のリスクを低減します。データは通常、15 分以内に複製されます。また、個々のデータベースのバックアップは少なくとも毎日行われます。

物理インフラストラクチャのセキュリティ

Autodesk Construction Cloud® アプリケーションは、AWS を所有および利用している安全なデータ センター内で実行されます。AWS データ センターは、さまざまなセキュリティ コントロールによって許可されていない物理アクセスや環境破壊から保護されています。

施設へのアクセス制御

物理的なアクセスは、専門のセキュリティ スタッフによって、監視システム、検出システム、およびその他の電子的手段を使用して、施設の入館管理を厳格管理し制御されます。許可されたスタッフは、多要素認証メカニズムを使用して AWS データ センターにアクセスします。サーバー ルームへの入口は、ドアが無理やり開かれたり、開いたままになった場合にインシデント対応を開始するためのアラームを鳴らすデバイスで安全が確保されています。

ビデオ監視

AWS サーバー ルームへの物理的なアクセスは、閉回路テレビカメラ（CCTV）によって記録されます。画像は、法的要件およびコンプライアンス要件に従って保持されます。

火災の防止

AWS データ センターには、自動火災検知および消火装置が備えられています。火災検知システムでは、ネットワーキング領域、機械領域、およびインフラ領域内に煙感知器が使用されています。これらのエリアは、消火システムによっても保護されています。

室内気候制御

AWS データ センターでは、室内気候を制御し、サーバーやその他のハードウェアの適切な動作温度を維持するためのメカニズムを使用し、過熱を防止して、サービス停止の可能性を低減しています。作業者およびシステムにより、温度と湿度が適切なレベルで監視および制御されています。

クラウド サービス

エンジニアリング
製品セキュリティ コントロール

運用インシデント管理

Autodesk Construction Cloud® には、インシデントの解決を推進するためのベスト プラクティスを定義しているインシデント管理ポリシーがあります。運用インシデント管理プロセスは、IT インフラストラクチャ ライブラリ（ITIL）バージョン 4 のフレームワークに従っています。

Autodesk Construction Cloud® のインシデント管理ポリシーでは、インシデントの修復手順の記録と根本原因分析の実行を重視し、すぐに実施可能な手順のナレッジ ベースを構築しています。このポリシーの目標は、インシデントを迅速かつ効果的に解決することだけではなく、プロセスを継続的に改善し、蓄積されたナレッジによって将来の対応が推進されるように、インシデント情報を収集および配布することです。

「Autodesk Trust Center」をご覧ください

パッチ管理

クラウド サービス チームは、効果的なパッチの展開を支援するオートデスクのパッチ管理ポリシーに従います。新しいパッチの確認や、権限を持つクラウド サービス担当者によって承認された展開リストの作成が自動化されているところもあります。

また、Autodesk Construction Cloud® のパッチ適用ポリシーによって、システムの安定性に対するパッチの影響を決定するための基準も定義されています。パッチがかなり大きな影響を持つ可能性があると認識された場合は、パッチを展開する前にクラウド サービス担当者が十分なリグレッション テストを実行します。

クラウド サービス チームが、本稼働システムへのパッチの展開を追跡します。品質保証には、開発および展開プロセス全体に渡る自動テストと手動テストが含まれます。

クラウド サービス

エンジニアリング
製品セキュリティ コントロール

変更管理

クラウド サービス チームの変更管理ポリシーには、以下のプロセスと手順が含まれます。

変更要求 (RFC)
アプリケーションをサポートしているシステムに対して行われる変更はすべて、正式な変更管理プロセスに従います (適切に署名された変更チケットおよび RFC を介して証拠を入手できます) 。

復元計画
クラウド サービス チームは、変更を展開する前に詳細な復元計画を作成します。これにより、変更によってサービスが中断された場合にシステムの状態を復元できるようになります。復元計画には、スクリプトに定義された、最小限の手動手順でシステム状態を復元する実行可能な指示が含まれています。

定義された保守期間
クラウド サービス チームは、定期、緊急、および延長メンテナンス期間を指定します。可能な限り、これらはオフピーク時間帯にスケジュールされます。

テスト計画
クラウド サービス チームは、一連のテストを定義して、変更の展開後、機能にアクセスが可能であることを確認します。

ステージング環境
本稼働システムのレイアウトと類似したステージング環境が保持されます。すべての本稼働環境に対する変更は、まずステージング環境に配置されます。機能テストを含む広範なテストは、変更をステージング環境から本稼働環境に展開する前に実行します。

テストの実行
展開が完了した後、クラウド サービス チームおよび製品 QA チームは、リスクがある機能が使用可能な状態になっていないか確認するテストを実行します。

クラウド サービス

エンジニアリング
製品セキュリティ コントロール

キャパシティ管理

時間の経過に伴い、Autodesk Construction Cloud® のリソース ニーズがお客様の需要に基づいて変化する可能性があります。オートデスクのエンジニアは、Autodesk Construction Cloud® のクラウド リソースに対するニーズを慎重に評価し、リソースの使用状況の計測やクラウド インフラストラクチャの柔軟性を活用します。

Autodesk Construction Cloud® のリソースの使用状況は、仮想インスタンス、仮想ストレージ ボリューム、仮想ネットワーク デバイスなどの一連のインフラストラクチャ用コンポーネント全体から頻繁に収集されます。使用状況統計は解析のために保存され、お客様の需要に基づいて仮想インスタンスの規模を事前に拡大または縮小するために使用される場合もあります。

処理性能/拡張性/可用性

高い可用性とパフォーマンスを確保するため、ソフトウェア開発ライフサイクル全体を通じて、パフォーマンス テストおよび負荷テストが実施されます。現在および過去の可用性が、今後予定されているメンテナンスとともに、Autodesk Health Dashboard でレポートされます。

「Autodesk Health Dashboard」をご覧ください

クラウド サービス

エンジニアリング
製品セキュリティ コントロール

Autodesk Construction Cloud® の運用セキュリティ コントロール

Autodesk Construction Cloud® 製品には、お客様のアカウントおよびデータへの不正なアクセスを防ぐために複数のセキュリティ コントロールが用意されています。

素性調査
オートデスクでは、Autodesk Construction Cloud® によって使用される計算リソースおよびサポート システムへのアクセスを従業員に許可する前に、必要に応じて従業員の素性調査を求めます。

アクセス管理
オートデスクは、アクセス管理ポリシーおよびプロセスを定義しています。このポリシーおよびプロセスにより、オートデスクの情報およびシステムへのアクセスを割り当てられたジョブの履行に必要な範囲のみに限定し、時間通りのアクセス終了で、アカウントのプロビジョニングに取り組みます。オートデスクのアクセス管理ポリシーは、オートデスク セキュリティ チームによって少なくとも年に 1 回レビューされます。

テストの実行
展開が完了した後、クラウド サービス チームおよび製品 QA チームは、危険性があると判定された機能が使用可能な状態のままであるかどうかを確認するテストを実行します。

管理機能
Autodesk Construction Cloud® の管理ツールには、ユーザ、役割ベースの権限、およびエンドユーザ向けのその他のアクセスを管理者がコントロールするための柔軟な方法が用意されています。

組み込み冗長性
ロード バランサやクラスタ化されたデータベースなどの技術により、単一障害点を最小限に抑えるようインフラが構築されています。

エンジニアリング

Autodesk Construction Cloud® エンジニアリング チームには、Autodesk Construction Cloud® のアプリケーションを設計、実装、およびテストする責任があります。Autodesk Construction Cloud® の設計、コーディング、テスト、およびメンテナンスは、必要に応じてセキュリティ プロセスが含まれるソフトウェア開発プロセスに基づいて行われます。

設計ステージでは、ユーザ ストーリーの詳細な設計ドキュメントが作成され、設計者によってレビューされ、設計の機能性や拡張性が評価されます。設計フェーズでは、共同アプリケーション設計プロセスを使用します。このプロセスでは、設計者とソフトウェア エンジニアがユーザ ストーリーの機能性、拡張性、およびパフォーマンス特性を評価します。

実装フェーズでは、エンジニアおよび設計者によるコードのピア レビューが実施され、Autodesk Construction Cloud® アプリケーションの開発プラクティスからの逸脱が検出されます。

プロセス時に作成されるすべてのコードには、単体テスト、統合、および QA 検証が含まれます。品質保証担当者が受け入れ基準を検証するまでは、新しいリリースが開始されることはありません。

開発ライフサイクルの一環として、Autodesk Construction Cloud® のパフォーマンス チームは、パフォーマンスに悪影響を及ぼす可能性のある変更をできるだけ早い段階で検出するため、負荷テストを実施しています。

従業員トレーニング

オートデスクでは、すべての従業員と派遣社員が一般情報、セキュリティ ポリシー、および意識向上のための トレーニングを定期的に利用できるようにしています。

オートデスクの行動規範では、すべての従業員に対し、法令を遵守し、倫理的かつ誠実に業務を遂行するとともに、互いに敬意を払い、会社のユーザ、パートナー、競合他社を尊重することを厳格に求めています。

オートデスクの従業員は、機密性、企業倫理、適切な慣習、職業上の基準に関する会社のガイドラインを順守する必要があります。新しい従業員は機密保持契約に署名する必要があります。オートデスクの新入社員向けオリエンテーションでは、顧客データの機密性およびプライバシーの重要性が強調されており、従業員は年次のサイバーセキュリティおよびプライバシー トレーニングを受講することが義務付けられています。

セキュリティのベスト プラクティスを導入するには、各開発チームが専任のセキュリティ チャンピオンと密接に連携して業務を遂行する必要があります。セキュリティ チャンピオンには専門的なトレーニングが提供されており、安全な開発に対するオートデスクの取り組みをさらに強化しています。

製品セキュリティ コントロール

クラウド サービス
エンジニアリング

Autodesk Construction Cloud® には RBAC（役割ベースのアクセス制御）が備わっており、お客様は詳細な ID およびアクセス管理ポリシーを作成できます。お客様の管理者およびユーザは、Autodesk Construction Cloud® のセキュリティ ツールを使用して、ワークスペースの所有権やドキュメントを管理したり、共有権限を設定できます。

認証

ユーザ データのセキュリティと完全性を確保するため、オートデスクは認証におけるベスト プラクティスを最優先しています。オートデスクのプラットフォームはシングル サインオン（SSO）統合に対応しており、Okta、Azure AD などの各種 ID プロバイダー（IdP）の資格情報を使用して、サービスへシームレスにアクセスできます。このアプローチにより、認証とポリシーを一元管理することでセキュリティを強化すると同時に、複数のアプリケーションへワンクリックでアクセスできる、シンプルなユーザ エクスペリエンスを実現します。業界基準に準拠し、堅牢な認証メカニズムを採用することで、オートデスクは安全かつ使いやすい環境をお客様に提供しています。

SSO を使用していないお客様向けには、アプリベースの MFA などの強力な制御機能が用意されており、不正アクセスからアカウントを保護するため、これらの有効化を強く推奨しています。SMS ベースの MFA も利用可能ですが、オートデスクでは、アプリケーション ベースの認証システムの使用を強く推奨しています。

SSO の詳細

転送中の暗号化

クライアントとバックエンド サービスの間の通信は、通信セキュリティを提供する暗号化されたチャンネルで行われています。このサービスは、高度な基準を確実に満たし続けることができるように、業界最高のツールによって定期的にスキャンされます。これらのサービスでは、最低限として TLS v1.2 と安全な暗号スイートが使用されています。

保存されたデータの暗号化

Autodesk Construction Cloud® のお客様によってアップロードされたファイルはすべて、暗号化されたストレージ上のクラウド内に保存されます。このストレージ ソリューションは、利用可能な最強のブロック暗号の 1 つである 256 ビットの高度な暗号（AES-256）を使用しています。

製品セキュリティ コントロール

クラウド サービス エンジニアリング

管理者の管理権限

Autodesk Construction Cloud® は、ID およびアクセス管理ポリシーを作成するためのセキュリティ機能をお客様の管理者に提供します。

ユーザの管理
管理者は、ユーザを作成および非アクティブ化できます。

役割ベースのセキュリティの使用
管理者は、Autodesk Construction Cloud® の役割を使用することで、アクセス コントロールのレベルをカスタマイズし、アクセスを制限するためにきめの細かいコントロールを実現できます。役割は、業務に関連するデータや機能に対する権限の集合です。

役割に基づいて権限を割り当てるという柔軟な方法を提供することで、Autodesk Construction Cloud® は、最小限の権限という原則を遵守しています。この原則では、各ユーザによるデータと機能へのアクセスを、ユーザに割り当てられたタスクを完了するために必要な権限に限定することが求められます。

ユーザ コントロール

ユーザは、管理上の制約を例外として、所有している項目、レポート、およびファイルへのアクセスをコントロールできます。ユーザはまた、ファイルのバージョニングを使用して、ワークスペース項目に添付したファイルの以前のバージョンを復元することもできます。

脆弱性スキャンと侵入テスト

オートデスクは、Autodesk Construction Cloud® のサービスに対して、定期的にセキュリティ スキャンおよび侵入テストを実施しています。これらのテストは、社内および外部の第三者の双方によって実施されます。

製品セキュリティ コントロール

クラウド サービス
エンジニアリング

セキュリティ基準とコンプライアンス

- Autodesk Construction Cloud® は、セキュリティ体制を検証するために業界基準の SOC2 認定を採用しました。
- Autodesk Construction Cloud® は、ISO 27001、ISO 27017、ISO 27018 の認証を取得しています*。

Autodesk Construction Cloud® および関連サービスの最新の認定ステータスの詳細については、Autodesk Trust Center の「コンプライアンス」 セクションをご覧ください。

「Autodesk Trust Center コンプライアンス」をご覧ください

プライバシー ポリシー

オートデスクは、顧客の個人データの収集と使用について明らかにしています。詳しくは、オートデスク プライバシー ステートメントをご覧ください。また、Autodesk Trust Center の「プライバシー」セクションをご覧いただくこともできます。

*ISO 27017 および ISO 27018 は、ISO 27001 監査認証の一部として含まれています。

以下のリソースは、オートデスクに関する一般情報、およびこのドキュメントで言及されているトピックに関する参考情報を提供しています。

リソース

オートデスクの詳細については、**autodesk.com/jp** をご覧ください

包括的なセキュリティ フレームワークの詳細については、
autodesk.com/jp/trust/security をご覧ください

Autodesk Construction Cloud® アプリケーションは、AWS でホストされています。このため、セキュリティとインフラストラクチャに対する責任は、オートデスクと Amazon の間で共有されます。Amazon のセキュリティの詳細については、次のリソースをご覧ください。

- **AWS コンプライアンス**
- **AWS データ センター管理**
- **共有責任モデル**

米国
+1 (866) 475-3802
construction.autodesk.com

オーストラリアおよび APAC
AUS +611800 314 435
acs.apac@autodesk.com
construction.autodesk.co.jp

英国および EMEA
+44 808 1892 253
acs.emea@autodesk.com
construction.autodesk.com.uk