AUTODESK
CONSTRUCTION
CLOUD™

セキュリティ
ホワイトペーパー

目次

概要

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、顧客データを保護しながら、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、クラウドソフトウェアのベストプラクティスを使用して設計および構築されており、クラウドインフラストラクチャ業界のリーダー的存在である Amazon Web Services(AWS)を利用しています。オートデスクは、拡張性が高くセキュアなサービスを設計し、それによって回復力の高い安全なアプリケーションをお客様に提供しています。オートデスクは、お客様のビジネスがオートデスクに依拠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。

ドキュメントの目的と範囲

本書の目的は、Autodesk Construction Cloud の運用、ソフトウェア開発、および環境に導入されているセキュリティ対策の概要を示すことにあります。

本書に含まれる内容:

このホワイトペーパーの範囲には、Autodesk Docs、Autodesk Build(PlanGrid Build を含む)、Autodesk Takeoff、Autodesk BIM Collaborate、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の範囲からは、Assemble、BuildingConnected、Pype、ACC Connect、BIM 360 Field、BIM 360 Glue、BIM 360 Plan、BIM 360 Ops、および BIM 360 Team は除外されます。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。

クラウド サービス

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、ハードウェアおよびオペレーティング 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。

「クラウド サービス チーム」、「クラウド インフラストラクチャ チーム」、および「クラウド運用チーム」という用語はすべて、オートデスク内の同じチームを指しています。

高可用性

オートデスクの高可用性への取り組みによって、お客様は Autodesk Construction Cloud を最大限にご利用いただけます。高度な可用性を実現するため、Autodesk Construction Cloud では、支援インフラストラクチャ.に冗長システムを採用し、拡張性のあるインスタンス群に負荷を分散させています。Autodesk Construction Cloud システムは、複数のウェブ サーバーとアプリケーション 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、およびデータ ストアとファイル ストレージで構成されています。

- 各 Autodesk Data Center は、複数の AWS リージョンおよびアベイラビリティ ゾーン(AZ)に渡って分散されています。各 AZ は、テリトリ内の独立した物理データ センターであるため、複数の AZ を使用することで、Autodesk Construction Cloud のアプリケーションの停止が起こらないように保護します。
- スコープ内で Autodesk Construction Cloud 製品を使用しているお客様は、米国または欧州のデータ センターを Autodesk Construction Cloud のプロジェクト データのプライマリ ストレージとして選択できます。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 センターです。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オートデスクの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、または同様の資料、お客様独自の生データまたは情報に基づくサービスから生成された特定の出力、およびバイナリではないまたは設計オブジェクトそのものにあるプロジェクト ファイルの関連メタデータ(個人データ(作成者名、電子メールなど)、タイム スタンプ、およびアクティビティ ストリームなど)が含まれます。

ビジネスの継続性およびデータ センターの冗長性

オートデスクには、ビジネスの継続性計画、および AWS アベイラビリティ ゾーン(AZ)を利用する障害回復プロセスがあります。このプロセスをサポートするために、Autodesk Construction Cloud は、複数の AWS アベイラビリティ ゾーン(AZ)に渡って配置されています。各 AWS AZ は、個別の物理データ センター内にあり、データはこれらの間で複製されます。複数の AWS 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。

データ複製

顧客データは、別々の場所にあるデータセンター間で複製されます。複製によって、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になった場合のデータ損失の可能性やサービスの遅延が回避できます。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、Amazon 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、建物の入口ポイントで制御されます。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。

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 3 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。詳細については、「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、本稼動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。

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。チームは、オフピーク時間に計画メンテナンスをスケジュールします。
- **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。**本稼動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。すべての本稼動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動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。

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、顧客の需要

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。

処理性能とスケーラビリティ

高度な可用性を実現するために、ソフトウェア開発ライフサイクル全体に渡ってパフォーマンス テストと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 (https://health.autodesk.com/)でレポートされます。

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、顧客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。**配置が完了した後、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管理するための柔軟な方法が用意されています。
- **冗長テクノロジー。**ロードバランサやクラスタ化したデータベースなどの冗長構成によってサービス停止を低減します。

Autodesk Construction Cloud 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、建築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、建築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、エンジニアおよび建築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 チームが、開発スプリント全体に渡って負荷テストを実施することで、プロセス内のできるだけ早い段階でパフォーマンスに悪影響を及ぼす変更を捕捉します。

従業員トレーニング

オートデスクでは、すべての従業員と臨時社員が一般情報、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。また、従業員は、オートデスクの行動規範を読み、理解し、それに関するトレーニングを受けることを求められます。行動規範では、すべての従業員が合法的かつ倫理的に、誠実さを持ち、他の従業員、お客様、取引先、競合他社への尊敬の姿勢を持って業務を遂行することを求めています。

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。新人研修では、顧客データの機密保持と保護を重点的に説明します。

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 チャンピオンには特別なトレーニングが必要です。また、オートデスクでは、すべてのエンジニアがセキュア開発ライフサイクル トレーニングを受けることができるようにしています。エンジニアは、(ISC)^2 ソフトウェア セキュリティ実務者認定の獲得を目指すことができます。

また、オートデスクでは、従業員向けに、定期的な模擬フィッシング演習などさまざまなトレーニング演習およびランチミーティングを実施しています。

Autodesk Construction Cloud 製品のセキュリティ コントロール

Autodesk Construction Cloud には、お客様が詳細な ID およびアクセス管理ポリシーを作成できるビルトイン セキュリティ機能が用意されています。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を管理したり、共有権限を設定できます。

転送中の認証および暗号化

Autodesk Construction Cloud にアクセスするには、ユーザ ID とパスワードで構成される資格情報が必要です。資格情報は、ネットワーク転送中は保護され、salt 付きハッシュとしてのみ格納されます。

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。このサービスは、セキュアな暗号スイートを使用した TLS v1.2 接続をサポートしています。

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。全体的な暗号化、キー管理、および復号化プロセスは、既存の監査プロセスの一環として定期的に内部で検査および検証されます。

管理者のコントロール権限

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。

- **ユーザのプロビジョニング**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、ジョブ機能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。

ID フェデレーション基準

Autodesk Construction Cloud は、すべてのユーザを対象として顧客システムに対するシングル サイン オン(SSO)をサポートしています。

クラウド セキュリティ

オートデスクの専任のセキュリティ チームは、Autodesk Construction Cloud 環境内のセキュリティの特定と強化に注力しています。次の責任があります。

- オートデスクのクラウド インフラストラクチャの設計と実装のセキュリティ体制をレビューします。
- ID およびアクセス管理、パスワード管理、脆弱性管理などのセキュリティ ポリシーを定義し、確実に実装します。
- 社内レビューおよび監査を実施することにより、確立されたセキュリティ手順への準拠を推進します。
- 顧客データの安全を確保するテクノロジーを特定して実装します。
- 必要に応じて、サードパーティのセキュリティ専門家によるセキュリティ アセスメントを実施します。
- クラウド サービスで発生する可能性があるセキュリティの問題を監視し、必要に応じてインシデントに対応します。

脆弱性スキャン、侵入テスト、および外部監査

オートデスクのセキュリティ チームは、SOC2 認定の範囲内である Autodesk Construction Cloud サービスの定期的なセキュリティ スキャンと侵入テストを実施します。セキュリティ スキャンと侵入テストは、SOC2 認定の一環として Open Web Application Security Project(OWASP)およびSANS Top 25 によって定義された幅広い脆弱性をカバーします。

ネットワーク セキュリティ

ネットワーク セキュリティは、暗号化、ファイアウォール(物理的または論理的)、および強化手順など、物理的コントロールおよび論理的コントロールの組み合わせを使用して実施されます。オートデスクのクラウド環境の境界には、標準的なハードウェアのファイアウォールが配備されています。顧客のリクエストに応えるために必要なポートを除き、すべてのポートがブロックされています。

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 SSAE-16 AT 101 SOC2 認定を選択しました。Autodesk Construction Cloud は、オートデスクの次の年次 SOC2 監査に含まれることが予定されています。
- Autodesk Construction Cloud は、監査および認定された後、ISO 27001、ISO 27017、および ISO 27018 認定として BIM 360 モジュールおよびサービスを加えます。

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。

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。

リソース

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。

- オートデスクの詳細については、https://www.autodesk.co.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、次のサイトをご覧ください。https://www.autodesk.co.jp/trust/security
- 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 コントロール
    - AWS 責任共有モデル

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

オーストラリアおよび APAC
AUS +61 1800 314 435
acs.apac@autodesk.com
construction.autodesk.com/au

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