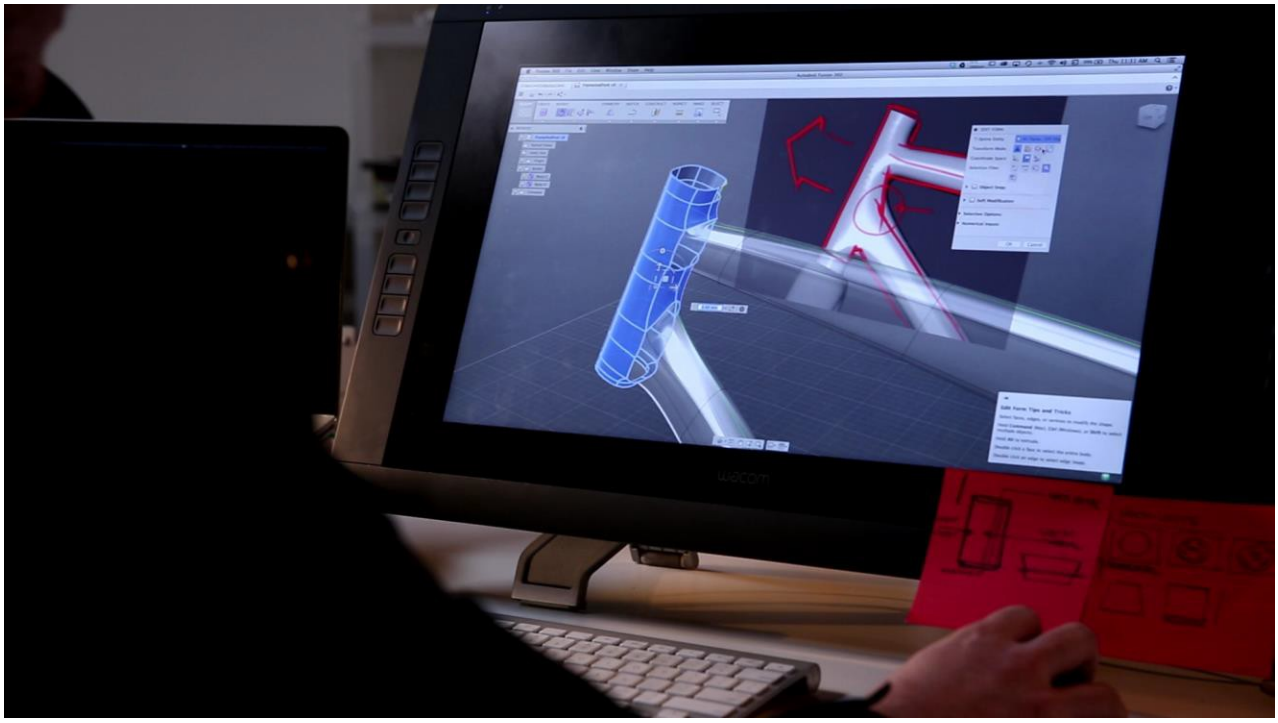
Autodesk Fusion 360
セキュリティ ホワイトペーパー



公開: 2015 年 8 月
最新情報は以下の Autodesk Trust Center でご確認ください。
http://www.autodesk.com/trust/overview

AUTODESK.

目次

概要

Autodesk® Fusion 360 ™ サービスは、製品開発のためのクラウドベースの 3D CAD/CAM ツールです。1 つのパッケージに工業設計と機械設計、コラボレーション、機械加工のツールが集約されています。Autodesk Fusion 360 のセキュアで統合されたコンセプトから製造までのツールセットなら、オートデスクのクラウド コンピューティング プラットフォームを通じた Web ブラウザやモバイル デバイスにも対応しているので、設計アイデアを高速かつ容易に探究することができます。

顧客データの高可用性を維持するため、Autodesk Fusion 360 は、要求が増加してもサービスが応答を継続することができる、拡張性の高いインフラストラクチャで実行されています。

この文書の目的

この文書は、Autodesk Fusion 360 の運用、ソフトウェア開発プロセス、およびセキュリティ対策について説明することを目的としています。

Autodesk Fusion 360 エンジニアリング

Autodesk Fusion 360 エンジニアリング チームは、Autodesk Fusion 360 のクライアント側のソフトウェアおよびクラウドで提供されるクラウド サービス アプリケーションの設計、実装、テストを行います。

Autodesk Fusion 360 アプリケーションの設計、コーディング、テスト、保守はアジャイル ソフトウェア開発プロセスに基づきます。デザイン スプリントでは、詳細な設計ドキュメントが作成され、アーキテクトがレビューして設計の機能性や拡張性を評価します。実装スプリントでは、ソフトウェア エンジニアおよびアーキテクトによるコードのピア レビューが実施され、Autodesk Fusion 360 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。このプロセスで生成されるすべてのコードには、機能単位のテストが含まれており、品質保証担当者が受入基準を検証するまでユーザー ストーリーは完成しません。Autodesk Fusion 360 のパフォーマンス テストも、開発ライフサイクルに統合されています。開発スプリントを通じてチームは負荷テストを行い、パフォーマンスにマイナスの影響を与える変更をプロセスのできるだけ早い段階で特定します。

Autodesk Fusion 360 製品セキュリティ

Autodesk Fusion 360 には、クラウド サービスとの通信から、ユーザーが制御できる製品レベルのセキュリティ/コラボレーション機能まで、さまざまなセキュリティ機能が組み込まれています。

通信セキュリティ

Autodesk Fusion 360 クライアント ソフトウェアとクラウド サービスの間のすべての通信は、セキュアな HTTPS 接続を必要とします。

暗号化 & 暗号

Autodesk Fusion 360 とバックエンド サービスの間の通信、およびバックエンド サービス内での通信は、暗号化されたチャンネルを介しており、セキュアな通信を実現します。

認証

Autodesk Fusion 360 にアクセスするには、Autodesk ID、ユーザー ID、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、SHA-2 の暗号学的ハッシュ関数によって生成された salt 付きハッシュとしてのみ格納されます。

データ セキュリティ

Autodesk Fusion 360 の設計はすべて、クラウンド上の暗号化されたストレージに保存されます。ストレージ ソリューションは、256 ビットの Advanced Encryption Standard (AES-256)を使用してデータを暗号化します。

ローカルにキャッシュされた設計のアクセス制御には、オペレーティング システムのユーザー レベルのアクセス権が使用されます。

設計項目の バージョニング

Autodesk Fusion 360 は、すべての項目のバージョン履歴を保持します。バージョニングによって、旧バージョンのプロモートによる変更のロールバックが可能となり、データの整合性が保護されます。また、各ファイル修正に関する情報が含まれた監査可能なリストが提供されます。

ハブおよびグループ ベースのコラボレーション セキュリティ

プロジェクトには、Autodesk Fusion 360 の設計へのアクセス権を一連の共有メンバーに対して付与または制限するためのシンプルな基本機能が備わっています。プロジェクトへの招待はプロジェクトのオーナーまたはモデレータが承認します。このため、招待を受けたメンバーによる他の人々の招待を厳しく制御することができます。

企業はチーム ハブを選ぶこともできます。この場合、メンバーが作成するすべてのプロジェクトに対して所有権とアクセスの制御を実行できます。オープンプロジェクト、クローズドプロジェクト、シークレットプロジェクトなどのプロジェクト プライバシー設定によって、制御されたコラボレーションが可能になります。チーム ハブでは、メンバーは招待されたプロジェクトにのみ共有メンバーを追加できます。これらの共有メンバーは、自分が招致されたプロジェクトにのみアクセスできます。チーム ハブではまた、企業のハブ管理者は退職従業員のアカウントを無効にしたり、プロジェクトの所有権をチームの他のメンバーに移したりすることもできます。

パブリック共有

パブリック共有は、Autodesk ID や Fusion 360 の使用権を持っていない外部関係者とコラボレーションするための方法です。ユーザーは、設計に対して読み取り専用のアクセス権を提供するリンクを作成できます。また、必要であれば、このリンクを介してダウンロード/エクスポートのアクセス権を提供することもできます。さらにユーザーは、このリンクで提供されたパブリック共有をいつでも破棄することができます。

クラウドの運用

オートデスクのクラウド運用チームは、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、システム正常性の監視、Autodesk Fusion 360 の保守に必要なその他のアクティビティの手順を定義し、実施します。

高可用性

Autodesk Fusion 360 は、基盤となる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ることで、高度な可用性を達成するよう設計されています。

データ複製

さまざまな場所にあるデータ センター間で顧客データの複製が行われます。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再開の遅延を抑制します。

データ センターの冗長性

異なるデータ センターに同様の物理インフラストラクチャを保持することで、データ センターの故障などの事象に備えています。

電源システムの冗長性

データ センターは、24 時間 365 日の稼働を維持するため、冗長な電源システムを備えています。障害が発生した場合は、無停電電源装置(UPS)によって自動的に一次電力系統にバックアップが提供されます。停電が発生した場合は、各データ センターの発電機によって長時間のバックアップ電力が提供されます。

インターネット接続の冗長性

冗長なマルチベンダー システムを使用することで、各データ センターへのインターネット接続を維持しています。

Autodesk Fusion 360 クライアント ソフトウェアは、オフライン モードも備えており、ユーザーはインターネットに接続されていないときでも、設計のローカル コピーにアクセスして作業することができます。

物理インフラストラクチャのセキュリティ

Autodesk Fusion 360 アプリケーションは、安全なデータ センターで実行されており、さまざまなセキュリティ制御によって未承認の物理アクセスや環境危険から保護されています。

施設へのアクセス制御

データ センターは、24 時間 365 日、専門のセキュリティ スタッフによって警備されています。各データ センターの周囲、ならびにコンピューティング装置や支援装置のある部屋は、ビデオ監視によって保護されています。ビデオ監視映像はデジタル メディアに保存され、要求があれば最近のアクティビティを確認することができます。データ センターの入り口は、入場を一度に 1 人だけに制限するマントラップ方式で警備されています。すべてのビジターおよび契約業者は、いかなる場合も身分証明書を提示して、権限を持つ担当者から入室許可を得る必要があり、その担当者の案内で入室しなくてはなりません。業務上正当な必要性を持つ従業員だけがデータ センターへのアクセスを許可され、すべての訪問は電子的に記録されます。

火災の防止

各データ センターの随所に煙警報器や熱作動のスプリンクラーといった火災検知および鎮火システムが設置されており、コンピューティング装置や支援システムのある部屋が保護されています。火災検知センサーは、天井および高床の下に設置されています。

室内気候制御

データ センターの室内気候制御によって、厳密な環境範囲を超えた場合に故障する可能性があるサーバー、ルーター、その他の装置を保護します。システムと人員の両方で監視することで、オーバーヒートなどの危険な状況を防止します。気温やその他の環境計測値は、制御システムによって自動的に許容範囲内に調整されます。

運用インシデント管理

オートデスクには、インシデント解決を推進するためのベスト プラクティスを定義したインシデント管理ポリシーがあります。オートデスクのインシデント管理ポリシーは、すぐに実施可能な手順のナレッジ ベースを構築するため、修復手順の記録と原因分析の使用を重視しています。オートデスクのインシデント管理ポリシーの目標には、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、インシデント情報を収集および配布することでプロセスを継続的に改善し、累積された知識によって将来の応答を推進することも含まれます。

パッチ管理

可能な場合は、新しいパッチのチェックと、権限を持つクラウド運用担当者が承認するための配備リストの準備が自動的に行われます。また、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が定義されます。パッチの影響が大きい可能性があると判定された場合、そのパッチを配備する前に回帰テストが行われます。プロダクションシステムへのパッチの配備は、変更管理によって追跡されます。

変更管理

クラウド運用チームの変更管理ポリシーには、以下の活動が含まれています。

- 変更イニシエータの名前、変更の優先度、変更に対する業務上の正当性、要求する変更の実施日を含む変更要求(RFC)フォームの提出を要求します。
- クラウド運用チームは、変更によってサービスの中断が発生した場合にシステムの状態を復元できるよう、配備の前に復元計画を作成します。復元計画には、最小限の手動手順でシステム状態を復元するスクリプトで定義された実行可能指示が含まれます。
- 保守期間を定義します。クラウド運用チームは定常、緊急、および延長の保守期間を指定します。定期的に行われる定常保守はオフピーク時間帯にスケジュールされます。
- 変更の配備後、機能にアクセスできるかどうかを検証するテストを定義します。
- 配備が完了した後、クラウド運用チームおよび Autodesk Fusion 360 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を維持しているかどうかをチェックするテストを実行します。

キャパシティ管理

クラウド サービスへの顧客のアクセスは、セルフサービス モデルを通じてオンデマンドで準備されるため、トラフィック パターンは非常に変わりやすく、使用量が突発的に急増しがちです。突発的に使用量が急増し、サービスを駆動するコンピューティング リソースのプールが使い果たされた場合、サービスの可用性にマイナスの影響があります。高度な可用性を維持するため、クラウド運用チームはキャパシティ管理ポリシーを実施します。これらの実施には以下が含まれます。

- リソース使用を頻繁に記録 - Autodesk Fusion 360 のリソース使用を、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 コンポーネントで頻繁に収集します。使用に関する統計情報は、キャパシティ管理リポジトリに格納されます。
- 現在のリソース使用と将来の必要量の予測を文書化したキャパシティ計画を作成 - クラウド運用チームは、キャパシティ管理リポジトリを使用して詳細なキャパシティ計画を生成します。現在の使用レベルを文書化し、統計分析に基づく将来のレベルと、次回のビジネス機能の改善による影響をモデル化します。キャパシティ計画は、必要に応じて、または使用パターンの大きな変更が検出された場合に更新されます。

Autodesk Fusion 360 運用制御

Autodesk Fusion 360 は、機密性の高い顧客データを未承認のアクセスから保護します。

- **データ センターへの物理的な規制** - データ センターを物理的に規制することで、未承認の関係者が、Autodesk Fusion 360 が使用するハードウェアや支援システムにアクセスするのを防止します。
- **バックグラウンド チェック** - Autodesk Fusion 360 が使用するコンピューティング リソースおよび支援システムに物理的にアクセスする従業員には、バックグラウンド チェックが要求されます。
- **データの複製** - 施設間でフェイルオーバーが発生した場合でも、ビジネスの継続を維持できるよう、データ複製によって顧客データを複数のデータ センターにコピーします。
- **冗長**化- 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軽減します。

クラウド セキュリティ

クラウド セキュリティ チームは情報セキュリティの専門家グループで、Autodesk Fusion 360 クラウド環境内のセキュリティの特定と実施を主に担当しています。

クラウド セキュリティ チームの責務には以下があります。

- クラウド インフラストラクチャのセキュリティの設計と実装をレビューします。
- 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。
- 情報セキュリティアセスメントを実施するため、サードパーティのセキュリティ専門家を採用します。
- 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。
- セキュリティ ポリシーについて年に 1 度レビューを行います。

脆弱性スキャンと侵入テスト

クラウド セキュリティ チームは、Autodesk Fusion 360 サービスの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、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、システム強化手順など、物理的制御および論理的制御の組み合わせを使用して実施されます。クラウドの周囲にはスタンドアロンのハードウェア ファイアウォールが配備されます。顧客要求に使用する必要があるポートを除く、すべてのポートがブロックされます。

暗号化

資格情報、アプリケーション セッション情報、アクセス トークン、ユーザー プロファイルなど、機密性の高い情報を含むネットワーク トラフィックは、インターネットを介して環境の周辺まで安全に転送されます。

セキュリティ基準と証明書

Autodesk Fusion 360 セキュリティ制御は、将来、独立の監査者によってレビューされ、AT Section 101 SOC 2 監査レポートにリストされる予定です。

リソース

以下のリソースは、オートデスクおよびこのドキュメントの本文中で言及されているその他のトピックに関する一般情報を提供しています。

- オートデスク - オートデスクに関する情報は、http://www.autodesk.co.jp をご覧ください。
- Autodesk Trust Center - Autodesk Trust Center に関する情報は、http://trust.autodesk.com をご覧ください。
- Autodesk Fusion 360 - Autodesk Fusion 360 サービスに関する情報は、http://fusion360.autodesk.com をご覧ください。

このドキュメントに含まれる情報は、公開日時点での Autodesk, Inc. の見解を表しており、オートデスクはこの情報を更新する責任を負いません。オートデスクは、製品やサービスに改善やその他の変更を加えることがあり、ここに含まれる情報は、公開日時点で提供されているバージョンの Autodesk Fusion 360 にのみ適用されます。

このホワイト ペーパーは、情報提供のみを目的としています。オートデスクは、このドキュメントについて一切の明示的または黙示的保証を行いません。また、このホワイト ペーパー内の情報は、オートデスクの側に拘束力のある義務または責務を作成するものではありません。

Autodesk Fusion 360 サービスは、上記を制限または変更することなく、http://www.autodesk.com/company/legal-notices-trademarks/terms-of-service-autodesk360-web-services に記載されている適用可能なサービス利用規約の下で提供されます。