Autodesk® Fusion 360™ セキュリティ

ホワイトペーパー

2018 年 12 月 28 日

目次

概要

Autodesk® Fusion 360™ は、3D CAD、CAM、CAE ツールを 1 つにまとめ、Mac と Windows のどちらでも動作する、他に類を見ないソフトウェアです。1 つのクラウドベース プラットフォームを使い、関係者全員で連携して製品開発を進めることができます。セキュアで統合されたコンセプトから製造まで対応できるこのツールセットは、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おり、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。

この文書の目的

このドキュメントは、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。
Fusion 360 は、Fusion 360 クライアント ソフトウェアと Fusion 360 ブラウザ アクセス ソフトウェアの両方を意味します。

Fusion 360 の開発

Fusion 360 の開発チームは、Fusion 360 のクライアント側のソフトウェアおよびクラウド 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。

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、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、機能の単体テストが含まれており、品質保証担当者が受入と完了の定義(Definition of Done)の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。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 Fusion 360 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。

オートデスクの従業員トレーニング

オートデスクのすべての従業員は、新入社員研修の一部として情報セキュリティの重要性を確認する必要があります。従業員は、会社の行動規範を読み、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ています。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 プラクティスを実装するために、オートデスクではエンジニアリングおよびクラウド インフラストラクチャ部門の全従業員に対し、毎年 Software Security Certification Program (SSCP)を実施しています。

Fusion 360 製品セキュリティ

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および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

Fusion 360 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 接続が必要です。

暗号化と暗号

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

Fusion 360 にアクセスするには、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、ソルト付きハッシュとしてのみ格納されます。

Fusion 360 では、ログイン時に多要素認証を使用するオプションをエンド ユーザーに提供しています。この機能を有効にしたユーザーは、認証済みのセキュアな個人デバイス(携帯電話など)で、パスワードと組み合わせて使用するためのコードを受信できます。

データ セキュリティ

すべての Fusion 360 の設計は、クラウ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。

設計のバージョン管理

Fusion 360 は、すべての設計のバージョン履歴を保持します。バージョン管理によって、旧バージョンへのロールバックが可能となり、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、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、メンバーによる新しいユーザーへのアクセスの付与を厳密に制御できます。

加えて企業ユーザーは Team Hub を使用することもできます。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。Team Hub では、メンバーはプロジェクトに招待されている共有メンバーへのアクセスを制限するかどうかを選択できます。また、顧客の管理者が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すこともできます。

パブリック共有

パブリック共有により、ユーザーは 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ことができます。Fusion 360 ユーザーは、設計への読み取り専用アクセスを提供するリンクを作成します。ダウンロード/エクスポート機能を有効にすることもできます。このリンクで提供されたパブリック共有は、いつでも破棄することができます。

クラウド インフラストラクチャ

オートデスクのクラウド インフラストラクチャ 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、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

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。

データの複製と冗長性

顧客データの複製は、Amazon Web Services (AWS) のアベイラビリティ ゾーン (AZ) 間で実行されます。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再開の遅延を抑制します。

電源システムの冗長性

AWS 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。
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

Fusion 360 アプリケーションは、AWS の安全なデータ 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。いくつかの物理制御と環境制御の概要を以下に示します。AWS セキュリティ プロセスの概要については、https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf を参照してください。

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、その他の装置は保護されます。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、将来の対応が累積された知識によって推進されるようにすることも含まれます。

パッチ管理

クラウド インフラストラクチャ チームには、効果的なパッチ配備を実現できるパッチ管理ポリシーがあります。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 インフラストラクチャ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 インフラストラクチャ 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。

- 変更要求(RFC)フォーム。すべての変更について RFC フォームを提出する必要があります。RFC フォームには、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が含まれます。

- 復元計画。クラウド インフラストラクチャ 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。

- 定義された保守期間。クラウド インフラストラクチャ チームは、定期、緊急、および延長保守期間を指定します。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 インフラストラクチャ チームは、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一連のテストを定義します。

- テストの実行。配備が完了した後、クラウド インフラストラクチャ チームおよび 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 インフラストラクチャ 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。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。

- キャパシティの計画。クラウド インフラストラクチャ チームは、キャパシティ管理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。

- リソースの割り当て。計算されたリソースは、顧客の要求に応じて割り当てられます。暖機された計算リソースは常に利用できます。アクティビティが急増すると、新しいリソースがインスタンス化されます。たとえば、Fusion 360 ブラウザ リソースの可用性は、通常 10 分未満で達成されます。

- アクティビティの監視。アクティビティ ダッシュボードとアラートはバックエンド サービス全体で定義されるため、エンジニアはシステム アクティビティを観察して、事後インシデントの調査と分析を実行できます。

警告と監視

平均修復時間をできる限り短くするために、オートデスクでは自動システムを使用して Fusion 360 を監視し、サービスの正常性を確認します。データベースからサービスまで、単一の各コンポーネントが個別に監視されます。サービスに影響を与えるイベントが発生した場合、警告が生成され、エスカレーション プロセスを通じてクラウド インフラストラクチャ チームに通知されます。

サービスの正常性は、オートデスク サービス間の相互関係も表します。Fusion 360 などのサービスは ACM サービス(アクセス制御)に非常に影響を受けやすくなっています。各サービスは、依存するサービスで障害が発生した場合に早急に回復が可能で、動作できなくなった場合には顧客のデータを失うことなく適切に停止する必要があります。

Fusion 360 サービスの状態は、オートデスクの正常性ダッシュボード サービス (https://health.autodesk.com) に公開されています。

配備中のゼロ ダウンタイム

パッチがプロダクション環境に適用されると、ブルーグリーン配備アプローチが Fusion 360 ブラウザおよびその他の Fusion 360 サービスで実施されます。これにより、顧客側でサービスのダウンタイムは生じなくなります。

Fusion 360 運用制御

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、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。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。

オートデスク セキュリティ

オートデスク 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、オートデスク クラウド環境内のセキュリティ プラクティスの特定と実施を主に担当しています。オートデスク セキュリティ チームの責務には以下があります。

- 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。
- 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

Fusion 360 サービスは、毎年侵入テストと、セキュリティ上の脅威や脆弱性に対する定期的なスキャンを実施しています。アプリケーションは静的な分析とサードパーティのライブラリ スキャンも実施します。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。また、AWS は物理的なデータ センターを保護するネットワーク セキュリティ制御も提供します。詳細については、AWS のセキュリティ ホワイトペーパー (https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf)を参照してください。

暗号化

すべてのネットワーク トラフィックは、インターネット経由でオートデスク クラウド環境の周囲に送信されるときに暗号化されます。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 プロファイルなどの機密情報は安全に暗号化されます。

プライバシー

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。詳細は、オートデスク プライバシー ステートメント (https://www.autodesk.com/company/legal-notices-trademarks/privacy-statement-jp) をご覧ください。

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.com をご覧ください。（日本語ページは 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。
- Fusion 360 - Fusion 360 サービスに関する情報は、https://www.autodesk.co.jp/products/fusion-360/overview をご覧ください。