AUTODESK

Autodesk® Fusion 360 セキュリティ ホワイトペーパー

2022 年 10 月

目次

1. はじめに

Autodesk® Fusion 360™ は、この種のツールとしては初めての 3D CAD、CAM、および CAE ツールです。Mac と PC の両方に対応した単一のクラウドベースのプラットフォームで、製品開発プロセス全体を連携できます。Fusion 360 ツールは、Web ブラウザやモバイル デバイスにまで拡張された安全で統合されたコンセプトから製造までの統合ツールセットにより、デザイン アイデアを迅速かつ容易に検討することができます。

1.1 ドキュメントの目的と範囲

このドキュメントの目的は、オートデスクの操作、ソフトウェア開発プロセス、および環境内に実装されるセキュリティ対策について説明することです。このドキュメントでは、Autodesk 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指します。

オートデスクのセキュリティ フレームワークは、顧客情報の機密性、完全性、および可用性を保護するための業界標準に基づいています。

Fusion 360 は高い可用性と拡張性を実現するように設計されており、お客様に高速かつ強化されたクラウド サービスを提供します。オートデスクのクラウド ホスティング プロバイダは、クラウド インフラのリーダーである Amazon Web Services(AWS)です。オートデスクは、AWS ホスティング プロバイダの共有責任モデルを活用しています。このモデルには、AWS クラウド サービスを実行するハードウェア、ソフトウェア、ネットワーク、および設備で構成されるインフラが含まれています。(詳細については、https://aws.amazon.com/jp/compliance/shared-responsibility-model/ を参照してください)。

2. Autodesk セキュリティ

オートデスクのセキュリティ フレームワークは、一貫性のあるセキュリティ プラクティスを確保するために業界標準に沿って設計されており、安全の構築、安全の実行、安全の維持を可能にしています。

- **安全の構築:** セキュリティを一から製品に埋め込むことは、オートデスク製品およびサービスに対するお客様の投資を保護するための重要な要素です。オートデスクは、ソフトウェア開発のあらゆるフェーズにセキュリティを組み込んでいます。

- **安全の実行:** オートデスクはインフラに直接セキュリティを組み込んでいます。当社の総合的なアプローチには、エンドポイント保護ツールの配置、標準化されたパッチ適用と強化された要件、ID とアクセス管理コントロール、および攻撃的なセキュリティ活動が含まれます。
- **安全の維持:** オートデスクのセキュリティは、情報の機密性、完全性、および可用性(CIA)を保護する 3 つの主な目的に焦点を当てています。
    - 機密性: 情報は、許可された者のみアクセス可能であること
    - 完全性: 情報が完全で正確であること
    - 可用性: お客様がデータにアクセス可能で、入手可能であること

最高セキュリティ責任者(CSO)は、セキュリティ戦略およびプログラムの開発、実装、およびガバナンスに関する責任を負い、すべてのオートデスク製品や環境においてセキュリティ方針と標準が適用されていることを保証します。CSO とセキュリティ チームは、オートデスクのエグゼクティブ ディレクターおよび取締役会によってサポートされています。

3. Fusion 360 エンジニアリング

Fusion 360 エンジニアリング チームは、Fusion 360 クライアント 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、テストを担当しています。

Fusion 360 の設計、コーディング、テスト、メンテナンスは、アジャイル ソフトウェア開発プロセスに基づいています。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 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。

3.1 従業員トレーニング

オートデスクの全従業員は、新入社員オリエンテーションの一環として、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、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 プラクティスを実現するため、オートデスクでは、エンジニアリング&クラウド インフラ機能のソフトウェア セキュリティ認定資格プログラム(SSCP)を、全員を対象に毎年導入しています。

4. 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、製品レベルのセキュリティ、ユーザがコントロールできる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。

4.1 通信セキュリティ

Autodesk 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 接続を必要とします。

4.2 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 サービス内の通信は、暗号化されたチャンネルで行われています。

4.3 認証

Autodesk Fusion 360 にアクセスするには、Autodesk ID、ユーザ 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、salt 付きハッシュとしてのみ格納されます。

Fusion 360 では、エンド ユーザがログインする際に、多段階認証を使用するオプションが用意されています。この機能を有効にすることを選択したユーザは、承認された安全な個人デバイス(例: 携帯電話)を使用して、パスワードと組み合わせて使用するコードを受け取ることができます。

4.4 データ セキュリティ

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 レベルのアクセス権が使用されます。

4.5 設計のバージョニング

Autodesk Fusion 360 は、すべての設計のバージョン履歴を保持します。バージョニングによって、旧バージョンへ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。

4.6 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。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。

4.7 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。Fusion 360 ユーザは、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、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。ユーザは、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。

5. クラウド インフラ

クラウドインフラ 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。

5.1 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。

5.2 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ー 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。

5.3 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。

5.4 インターネット接続の冗長性

冗長なマルチベンダー システムが、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。

また、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。

5.5 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、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。物理的なコントロールと環境的なコントロールの一部を以下に示します。AWS セキュリティ プロセス全体の概要については、こちらを参照してください。

5.6 施設へのアクセス制御

AWS データ センターは、プロフェッショナルな物理的セキュリティ スタッフによって 24 時間、週 7 日の間警備されています。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。ビデオ監視はデジタル メディアに保存されており、最近の活動をオン デマンドで見ることができます。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。

5.7 防火設備

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。

5.8 気象コントロール

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。

6. 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。

7. パッチ管理

クラウド サービス チームには、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、パッチを配備する前にリグレッション テストを実行します。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。

8. 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)の取得元。**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。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。

- **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、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。

- **保守期間の定義。**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 インフラストラクチャ 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。

- **テスト実行。**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 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。

9. 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。

- **リソースの使用の頻繁な記録。**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。

- **キャパシティ計画。**クラウド インフラ チームは、キャパシティ管理を使用して、現在の使用レベルを文書化し、統計的分析およびビジネス機能に対する今後の強化による影響に基づいて将来のレベルをモデル化した詳細なキャパシティ計画を作成します。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。

- **リソースの配分。**コンピューティング リソースは、お客様からの要望に応じて割り当てられます。事前計算リソースは、いつでも使用可能です。アクティビティの急増が発生した場合、新しいリ

ソースがインスタンス化されます。たとえば、Autodesk Fusion ブラウザのリソースは通常 10 分以内に使用可能になります。

- **アクティビティの監視。**アクティビティ ダッシュボードと警告はバックエンド サービス全体で定義されているため、エンジニアはシステム アクティビティを観察し、インシデント後の調査や分析を実行できます。

10. 警告と監視

オートデスクは、最短の平均修復時間を提供するために、自動化されたシステムで Fusion 360 を監視し、サービスの健全性を検証します。データベースからサービスに至るまで、各コンポーネントは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は、警告が生成され、エスカレーション処理を通じてクラウド インフラストラクチャ チームに通知されます。

サービスの健全性は、オートデスク サービス間の相互関係についても説明します。Autodesk Fusion 360 のようなサービスは、ACM サービス(アクセス制御)に非常に敏感です。各サービスは、依存サービスに障害が発生した場合に回復力を備えている必要があり、サービスが運用できなくなった場合には顧客にデータを失わせずに適切に障害を発生させる必要があります。

Fusion 360 サービスの状態は、オートデスクの Health Dashboard Service: https://health.autodesk.com によって公に表示されます。

11. 配置時のダウンタイムをゼロに

パッチが本番環境に適用されると、Autodesk Fusion ブラウザやその他の Fusion 360 サービスに対して青緑色の配置アプローチが採用されます。これにより、お客様がサービスを中断せずに継続する場合に役立ちます

12. Autodesk Fusion 360 の運用管理

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。
- **素性調査。**Autodesk Fusion 360 によって使用される計算リソースおよびサポート システムへアクセスでは従業員の素性調査が求められます。
- **データ複製。**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。

13. Autodesk セキュリティ

Autodesk 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 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。Autodesk セキュリティ チームの責務は、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。

13.1 脆弱性スキャンと侵入テスト

Fusion 360 サービスでは、年 1 回の侵入テストと、セキュリティの脅威と脆弱性をチェックするための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、静的解析およびサードパーティのライブラリスキャンも実行します。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。

13.2 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、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。さらに、AWS は、ネットワーク セキュリティ コントロールによって物理的なデータ センターを保護しています。詳細については、「セキュリティ、ID、コンプライアンスに関するベスト プラクティス」を参照してください。

13.3 暗号化

すべてのネットワーク トラフィックは、インターネットを介してオートデスク クラウド環境の周辺まで転送される際に暗号化されます。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 プロファイルなど、機密情報は保管中に暗号化されます

13.4 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。詳細については、オートデスクのプライバシー ステートメントを参照してください。

14. 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を表示するには、https://www.autodesk.co.jp にアクセスしてください。
- **Autodesk Trust Center:** Autodesk Trust Center に関する情報を表示するには、https://www.autodesk.co.jp/trust/overview にアクセスしてください。
- **Autodesk Fusion 360:** Fusion 360 に関する情報を表示するには、https://www.autodesk.co.jp/products/fusion-360/overview にアクセスしてください。