

AutoCAD® WS

AutoCAD WS のセキュリティ – クラウド コンピューティング、ほか



このホワイトペーパーでは、AutoCAD WS でいかにセキュリティが重視されているか、また、セキュリティ管理においてクラウド コンピューティングが果たす役割を解説します。

クラウド コンピューティングの台頭

後に「人工知能」という言葉を生み出すことになる John McCarthy 氏は、1961 年、マサチューセッツ工科大学での講演で、コンピュータの力が、水やガスと同じように公共サービスとして提供されるようになる可能性を示唆しました。同氏の提案は、その後長い間大きな関心と呼ぶことはありませんでした。そして 1999 年になって、Salesforce と呼ばれる新会社が、定期購入タイプの CRM(顧客管理)ソフトウェアを市場に投入しました。



それが、今、クラウド コンピューティングと呼ばれているものの始まりです。現在では、Google、Microsoft、Amazon といったさまざまな企業が、クラウド コンピューティングを活用して多くのサービスを提供しています。2002 年に Amazon は、初のクラウドベースのサービス(ストレージサービスと計算処理サービス)として、Amazon Web Services(AWS)を立ち上げました。

クラウド コンピューティングのメリット

価格

クラウド コンピューティングでは、使った分だけ料金を支払う従量課金モデルを採用しています。オートデスクでは、クラウド コンピューティングの料金システムのメリットをユーザに還元し、AutoCAD WS を iOS と Android のスマートフォン/タブレット用と、Web 用のアプリケーションとして無償で提供しています。

リソースの仮想化

クラウド コンピューティングでは、さまざまなユーザ グループによるリソースの共有が不可欠です。これによって、スケールメリットを実現し、各顧客が必要なときに必要なサービスを受けることができます。オートデスクのユーザは、アカウントの規模に関係なく、クラウド上に用意されたアカウント専用領域の図面に常時アクセス可能です。

モビリティ

ユーザはどこからでも重要な情報へのアクセスが可能です。その際、複数の場所にソフトウェアをインストールして管理する必要はありません。AutoCAD WS では、クラウド コンピューティングのリソースが持つあらゆる可能性を有効に活用し、モバイル環境専用の移動性の高い設計環境を提供します。



図 1. 建設現場で使用される AutoCAD WS

自動更新

クラウド コンピューティングは、論理的にはアウトソーシングととらえることができます。企業側がソフトウェアの更新に時間を費やしたり、新リリースへの移行計画を行う必要はまったくありません。すべてクラウド上で自動的に管理されるため、ユーザが利用する製品は常に最新のバージョンに維持されます。

AutoCAD WS にアップロードしたデータの安全性は？

HTTP/1.1 は、現在最も一般的に使用されているプロトコルです。しかし、HTTP は、それ自身だけでは安全とはいえません。HTTP を別の安全なプロトコルと組み合わせることによって、初めて、機密データの転送に必要な厳重なセキュリティが実現できます。この一体化されたプロトコルが HTTPS です。HTTPS では、すべての転送データは送信前にしっかりと暗号化され、受信側で解読されます。

Web ブラウザを利用する AutoCAD WS Web アプリケーションや、モバイル端末で利用する AutoCAD WS モバイル アプリケーションからの通信内容は、すべて完全に暗号化され、HTTPS プロトコルで転送されます。これは、データや文書のインターネット セキュリティにおいて、広く認められている業界標準の手順で、国際銀行やインターネット支払いサービスでは、機密性の高い業務データを安全に転送するために利用されています。

しかしながら、解読されたデータの保管場所が十分に安全でなければ、HTTPS の安全性が無駄になってしまいます。

AutoCAD WS におけるユーザ データの保管場所は？

AutoCAD WS にアップロードされたデータは、すべて Amazon Simple Storage Service (S3) に保管されます。Amazon がクラウド コンピューティング基盤として提供する Web サービスは、業界で広く認められたデータ ホスティングとセキュリティが大きな特徴となっており、AutoCAD WS ユーザはセキュリティに関する恩恵を受けることができます。Amazon Web サービスは、最良のセキュリティ実践モデルに従って、末端に至るまで、セキュリティとプライバシー保護を提供しています。Amazon S3 サーバのセキュリティは、最高レベルであることが認められ、認定を取得しています。

Amazon Web サービスは、インフラストラクチャ、データ センター、Amazon S3 などのサービスにおいて、Information Security Management System (ISMS) の ISO 27001 認定を取得しました。

「ISO 27001/27002 は、広く採用されている世界規模のセキュリティ標準で、企業情報や顧客情報の管理における体系的なアプローチに関する要件と最も効果的な実践方法を設定しています。そこでは、常に形を変えていく脅威発生シナリオに適した定期的なリスク評価をベースとしています」

さらに Amazon Web サービス は、米国監査基準書 70 号 (SAS70) Type II 監査を無事終了し、独立監査人から公平かつ高い評価を受けています。SAS70 認定は、サービス提供企業が顧客データ保護のためのパフォーマンスとセキュリティに関連する制御機能の総合的な監査を行ったことを証明するものです。Amazon Web サービス では、高いセキュリティを維持するために、定期的な監査を継続していきます。

2011 年 1 月の時点で、Amazon の S3 サーバには、2,620 億以上のファイルが保管されており、過去 12 ヶ月と比較して約 150% 増加しています。

Amazon のサーバ本体は、世界中にある安全なデータ センターに設置されています。

「データ センターの実地の所在地を知っているのは、Amazon 社内でも業務上、情報を合法的に必要とする社員のみに限られており、データ センター自体も、不正アクセスを阻止するために、さまざまな物理的バリアによって保護されています」

Amazon のサーバ セキュリティに関する詳細については、<http://aws.amazon.com/security/> を参照してください。

注意: 2011 年 4 月の 2 日間にわたる Amazon のサービス停止の際にも、AutoCAD WS には影響はありませんでした。AutoCAD WS 上の図面にユーザがアクセスできない時間はありませんでした。

Amazon サーバに個人の作業データを保管したくない場合は？

AutoCAD WS では、「サービスへの接続」機能によって、Amazon サーバへのデータ保存への懸念に対処しています。この機能では、Dropbox、Box.net、Buzzsaw、Egnyte、iCloud (旧 MobileMe) などの外部ストレージ サービス、または自社でホスティングしている SharePoint サイトやファイル サーバにファイルを格納することができます。どの場合でも、iOS や Android のモバイル端末や Web ブラウザから AutoCAD WS を利用して、図面ファイルの閲覧や編集を行うことが可能です。「サービスへの接続」では、既に確立されているセキュリティ、役割、アクセス権限をそのまま維持することができます。

「サービスへの接続」機能の使用に関する詳細については、以下のチュートリアルを参照してください。

- [AutoCAD WS と Box.net の接続 \(Connect AutoCAD WS with Box.net\)](#)

- [AutoCAD WS と Buzzsaw の接続 \(Connect AutoCAD WS with Buzzsaw\)](#)
- [AutoCAD WS と Dropbox の接続 \(Connect AutoCAD WS with Dropbox\)](#)
- [AutoCAD WS と Egnyte の接続 \(Connect AutoCAD WS with Egnyte\)](#)
- [AutoCAD WS と SharePoint その他の Windows サーバの接続 \(Connect AutoCAD WS with SharePoint or other Windows Server\)](#)

AutoCAD WS と他の転送方式の比較

AutoCAD WS が提供する安全なデータ転送とデータ格納の組み合わせは、最強の方法といえます。

File Transfer Protocol (FTP) のような他の一般的なファイル転送方式と比較しても、AutoCAD WS の方が、機密性の高い図面データのアップロードや転送をより安全に行うことができます。もともと、FTP は機密性や安全性を意図したプロトコルとして作られたものではなく、HTTPS の提供する最新のセキュリティ レベルとは比べ物になりません。FTP にはセキュリティの問題点が多く確認されており、その中には、「スプーフ攻撃」、「バウンス攻撃」、「スニффイング」に対する脆弱性などがあります。

元来 FTP が開発されたのは、SSL や TLS といった最新の暗号化標準が確立される前なので、HTTPS に内蔵されているような暗号化セキュリティを提供することは不可能なのです。

AutoCAD WS では、セキュリティ標準に HTTPS を採用することで、Gmail、Hotmail、Microsoft Exchange などのオンラインの電子メール クライアントと同等のセキュリティ レベルを実現しています。これまで電子メール経由でクライアントに図面ファイルを送付していたユーザにとっては、同等レベルのセキュリティが AutoCAD WS でも確保されます。

AutoCAD WS にアップロードした図面にアクセスできるのは誰か？

AutoCAD WS は、きわめて安全で、共同作業がしやすいように設計されています。図面ファイルをアップロードした本人以外で図面にアクセスできるのは、共有プロセスの一環として明示的に定義されたメンバーに限られます。

AutoCAD WS で図面を共有する際には、電子メール アドレスによってアクセスを許可するユーザを指定します。

共有設定では、運用方法によって、共有期間も限定できます。特定の会議中に、クライアントや同僚を招くことができます。それらの人々に対しては、会議の間だけ図面の閲覧やコメント添付を

有効にし、会議終了時には、それらの共有設定を取り除き、図面へのアクセスを不可にすることができます。

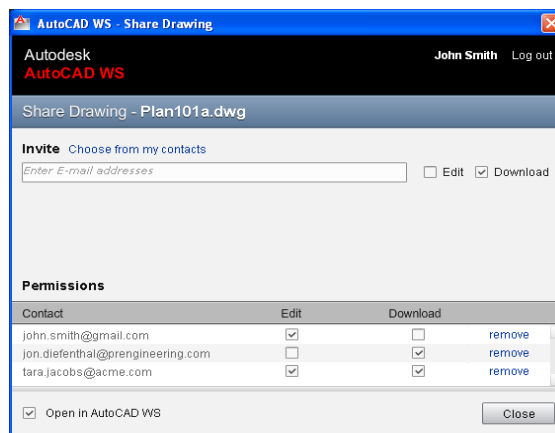
常時、図面を共有しているユーザの名前の確認やアクセス権の制御が可能です。また、図面を共有しているユーザ同士で同時に図面を閲覧しているかどうかを確認できます。

権限の設定

図面の作成者は、その図面に関する共有権限を細かく設定することができます。設定可能な権限は、[編集]と[ダウンロード]です。

権限の組み合わせには、次の 4 つがあります。

- [編集とダウンロード] - この共有通知を受け取ったユーザは、その図面の編集が可能で、また図面をダウンロードしてオフラインで編集することもできます。
- [編集のみ] - この共有通知を受け取ったユーザは、その図面の編集は可能ですが、図面をダウンロードしてオフラインで編集することはできません。
- [ダウンロードのみ] - この共有通知を受け取ったユーザは、そのオリジナル図面を編集することができません。ただし、既存のオブジェクトに変更を加えずに、図面に付け加えたり、マークアップを追加することは可能です。さらに、自分の追加したマークアップと一緒に図面をダウンロードして、オフラインで編集することもできます。
- [編集・ダウンロード不可] - この共有通知を受け取ったユーザは、既存のオブジェクトに変更を加えずに、図面に付け加えたり、マークアップを追加することができます。これらのマークアップは、AutoCAD WS のアプリケーション内でのみ実行できます。ユーザは、どのバージョンの図面もダウンロードできません。



図面に対する制御は継続的に行うことができ、いつでも共有権限の変更および無効化が可能です。

まとめ

AutoCAD WS は、ドキュメントの作成から転送、格納まで、すべての段階において最も効果的な実践方法を組み合わせたサービスです。AutoCAD WS では、クラウド コンピューティングを活用することによって、最高レベルのセキュリティを維持しながら、無限の拡張性を備えながら、設計環境に新しい運用方法を提供します。

これまで存在したどんなメディアよりも優れたセキュリティと協調ツールを提供する AutoCAD WS によって、今や CAD ユーザは、世界中のどこからでも効率的かつ安全にクライアントや同僚と一緒に仕事をすることができます。

AutoCAD WS による設計データの安全な保管に関する詳細については、feedback@autocadws.com までお問い合わせください。

Autodesk, AutoCAD, DWG は、米国および／またはその他の国々における、Autodesk, Inc.、その子会社、関連会社の登録商標または商標です。その他のすべてのブランド名、製品名、または商標は、それぞれの所有者に帰属します。
オートデスクは、通知を行うことなくいつでも該当製品およびサービスの提供、機能および価格を変更する権利を留保し、本書中の誤植または図表の誤りについて責任を負いません。
© 2011 Autodesk, Inc. All rights reserved.