

TeamViewerを使用したIBM MaaS360のリモート・サポート

TeamViewerとMaaS360ソリューションでリモート・デバイスのサポートと制御を効率的に提供します

特長

数秒間で接続して実際の無線（OTA）デバイスの状況を把握してリモート制御機能を実行します

Apple iOS、Google Android、macOS、Microsoft Windowsプラットフォームでデバイスに迅速なITサポートを提供します

リモートでデバイスを構成、接続性を設定、接続性に関する問題を解決します

ITヘルプデスクへの通話とサポート担当者への電子メールによる問い合わせの量を削減します

IT管理者とユーザーの生産性を向上させます

モバイル・デバイスへのITサポートは、ITチームとユーザーのどちらにとっても、時間を浪費し、不満が募ることになる場合があります。両者の所在地が異なるオフィスや国であっても、直接会ってサポートすることは現実的でない、または不可能な場合があります。電子メールによる指示やヘルプ・デスクのコーチングでさえも、混乱を招くことがあるでしょう。ユーザーは問題またはその解決方法を理解できず、管理者はユーザーをサポートするためにそのユーザーのデバイスを操作できる状態ではないかもしれません。そのために、全員の生産性が低下します。

IBM MaaS360 Remote Support with TeamViewerにより、ITメンバーはデバイスのインターフェースをまるで直接見ているかのように、ユーザーのiOSやAndroidのモバイル・デバイス、WindowsやmacOSのラップトップやデスクトップをリモートで確認できるようになります。このような現実的な視点を持つことで、IT担当者は即座に必要な変更、設定を変更するためのユーザーへの指示、アプリケーションの追加、または接続性の問題の修復を実行して、できるだけ早く従業員が自分の仕事に戻れるようにします。デバイスにユーザーがいない場合やデバイスがキオスク端末の場合、管理者は無人モードでそのデバイスを表示し、制御することができます。このソリューションは、MaaS360統合エンドポイント管理（UEM）プラットフォームの堅牢な機能と同時に動作し、組織が全社的に効率性を向上させながら、ダウンタイムとITサポート・コストを削減できるように支援します。

企業がIBM MaaS360 Remote Support with TeamViewerを使用するためには、MaaS360のサブスクリプションを持っている必要があります。これで、企業はまったく異なるエンドポイントとモバイル・デバイスの制御を維持するための闘いにおいて一歩先に進むことが可能になります。最近の調査で、従業員の58%が、これから在宅勤務を主とするか、ハイブリッド・ワークを受け入れるということが分かっています。¹

MaaS360ユーザーは、多数のUEM機能を利用して、スマートフォン、タブレット、ラップトップ、モノのインターネット（IoT）のデプロイメントをサポートすることができます。そのUEMの機能には、集中管理と監視、管理者、デバイス、アプリケーション、およびコンテンツにわたる強力なセキュリティ制御機能などがあります。

OTA構成機能により、管理者は従業員が基本的にはどこからでも必要になるプロファイル、資格情報、設定を提供できるようになります。

MaaS360の機能

- エンドポイントやモバイル・デバイスの迅速なOTA登録
- 電子メール、連絡先、カレンダー、VPN、WiFiのプロファイルのセットアップ
- 内部や公共のアプリケーションを含む、組織のドキュメントやコンテンツへのアクセス
- ネットワークにアクセスする新しいモバイル・デバイスの承認または検疫
- 画面キャプチャーやクラウド・バックアップのようなアプリケーションや機能へのアクセスの制限
- デバイス共有やキオスク・モードの機能の有効化

IBM MaaS360 Remote Support with TeamViewerで、IT担当者はこれらの機能をすべて活用して、リモート・デバイスに数秒で接続し、ユーザーのインターフェースの完全な可視化を実現し、リモート制御機能を使用して問題解決に導きます。



ユーザーがデバイスの完全な可視化を実現

IBM MaaS360 Remote Support with TeamViewerを使用して、ユーザーが直面している問題を可視化し、リモートでユーザーに指示を出すこともできます。管理者はアプリケーションの機能性を実演し、トラブルシューティングやサポートのために直接デバイスにアクセスし、必要な変更を実行できます。以下でその一部を紹介します。

- セキュリティー・ポリシーの構成
- アプリケーションのドラッグ・アンド・ドロップまたはアプリケーション・データの取得
- デバイスをコンプライアンスに適合させるために、必要な機能の実行

TeamViewer内で、管理者とユーザーはそれぞれにインスタント・メッセージを送信できます。また、必要に応じて管理者はアプリケーション内で発生するリモート・セッションを記録したり、必要性があればユーザーにファイルを転送したりすることができます。



堅牢なリモート・デバイス・セキュリティーに期待

MaaS360ソリューションは、安全なコンテンツ・コンテナ、ID管理、脅威管理、クラウド・セキュリティーといった幅広いエンタープライズ・グレードのエンドポイント・セキュリティー機能を備えています。TeamViewerのセキュリティー機能には、以下のようなものがあります。

- 完全なクライアントからのデータの暗号化といったRSA-2048の秘密鍵/公開鍵交換とAES256ビット・セッション暗号化
- リモート・セッション毎の固有のセッション・コードによるアクセス保護
- トラストド・デバイスのリストを通じてサインイン時の新しいデバイスの確認

IBM MaaS360 Remote Support with TeamViewerの使用を開始するための9つの手順

1. MaaS360のサブスクリプションを取得します。
2. TeamViewer.comでTeamViewerプロファイルを作成します。
3. MaaS360ソリューションでTeamViewerを有効化します。
4. リモート・サポート用のTeamViewerをダウンロードします。
5. MaaS360ソリューションのデバイス・インベントリーのエンドポイントを選択します。
6. TeamViewerは、MaaS360ソリューションを通じてユーザーにリモート接続性の要求を送信します。
7. ユーザーはデバイス上のリンクをクリックすることで要求の承認ができます。新しいユーザーは、はじめにTeamViewerアプリケーションをダウンロードする必要があります。
8. 数秒以内に、IBM MaaS360 Remote Support with TeamViewerのインターフェースがユーザーのデバイスで起動します。
9. IT管理者は、これで接続されたデバイスのインターフェースの全体を把握し、完全なリモート制御機能を活用することができます。

MaaS360ソリューションをお勧めする理由

あらゆる業界のあらゆる規模の何千もの組織が、モバイルによるデジタル変革の基盤としてMaaS360ソリューションを信頼しています。IBM Watson®とともに、MaaS360ソリューションは、ユーザー、デバイス、アプリケーション、コンテンツ全体の強力なセキュリティー制御を備えたAI搭載のUEMを提供し、基本的にはすべてのエンドポイントつまりモバイル・デバイスメントをサポートします。IBM MaaS360 Remote Support with TeamViewerにより、組織は生産性を向上させ、ITサポートや従業員のダウンタイムのコストを削減するために必要な実際のデバイスの状況を把握することができます。

詳細情報

IBM MaaS360 Remote Support with TeamViewerの詳細は、IBM 担当員またはIBMビジネス・パートナーにお問い合わせいただくか、ibm.com/jp-ja/maas360をご覧ください。

さらに、IBM グローバル・ファイナンスは、お客様がビジネスの成長に必要とするテクノロジーの取得を支援する豊富な支払いオプションをご用意しております。当社は、取得から廃棄にいたるまで、IT製品とサービスへの完全なライフサイクル管理を提供しています。詳しくは、ibm.com/jp-ja/financingをご覧ください。

© Copyright IBM Corporation 2022

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19-21

米国で制作
2022年1月

IBM、IBMロゴ、IBM Security、IBM Watson、MaaS360、with Watsonは、米国およびその他の国におけるInternational Business Machines Corporationの商標または登録商標です。その他の製品名およびサービス名は、IBMまたは他社の商標である可能性があります。IBMの最新商標リストについては、ibm.com/trademarkをご覧ください。

MicrosoftおよびWindowsは、Microsoft Corporationの米国、その他の国またはその両方における商標です。

本書は最初の発行日時点における最新情報を記載しており、IBM により予告なしに変更される場合があります。IBMが事業を展開しているすべての国で、すべての製品が利用できるわけではありません。

IBM製品およびプログラムと他の製品またはプログラムとの動作を評価したり、検証する場合は、お客様の責任で行ってください。本書の情報は“現状のまま”で提供されるものとし、明示または黙示を問わず、商品性、特定目的への適合性、および非侵害の保証または条件を含むいかなる保証もしないものとします。IBM製品は、IBM所定の契約書の条項に基づき保証されます。

適切なセキュリティーの実践に関するステートメント。ITシステム・セキュリティーには、企業内外からの不適切なアクセスに対する防止、検出および対応などにより、システムと情報を保護することが含まれます。不適切なアクセスは、情報の改ざん、破壊、悪用、誤用、または他者への攻撃への使用を含む、システムの損傷または誤用につながるおそれがあります。ITシステムや製品は完全に安全であると捉えるべきではなく、不適切な使用やアクセスを防止する上で絶対に効果のある、製品、サービス、セキュリティー対策は1つもありません。IBMのシステム、製品およびサービスは、合法的で包括的なセキュリティー・アプローチの一部として設計されているため、必然的に運用手順が追加されることとなります。また、他のシステム、製品、またはサービスが最も効果的である場合もあります。IBMでは、いずれの当事者による不正行為または違法行為により、いかなるシステム、製品もしくはサービス、またはお客様の企業に対して影響が及ぶことはないことを保証するものではありません。

¹ Future of Work – How Long-Term Digital Workplace Strategies and Business Priorities Have Changed、Omdia社、2021年8月