



主なメリット

- デバイスの VPN がなくても、セキュリティー保護された状態でモバイルから企業データにアクセスすることが可能
- SharePoint、Windows File Share、企業イントラネット・サイトをモバイル化
- エンタープライズ・システムへのアプリ内 VPN トンネルを使用
- 外出時でもコラボレーションを実現
- 認証、暗号化、DLP 制御など、堅固なセキュリティー・ポリシーで企業の機密データを保護
- ネットワークまたはファイアウォールのセキュリティー構成を変更することなく、アクセスを提供

IBM MaaS360 Gateway Suite

エンタープライズ・システムとコンテンツの可能性を解放

SharePoint、Windows File Share、イントラネットをモバイル化

IBM® MaaS360® Gateway Suite は、ネットワーク、ファイアウォール・セキュリティー構成、デバイスの VPN を変更することなく、SharePoint、Windows File Share コンテンツ、イントラネット・サイト、アプリ・データなど、ファイアウォールで保護されたビジネス・リソースに簡単、安全にアクセスすることを可能にします。

認可、暗号化、コンテナ化のポリシーでコンテンツを保護しながら、外出先でもコラボレーションを行うことができます。IT 環境にハードウェアを追加したり、LAN 外部のデバイスやサービスからのインバウンド TCP/IP 接続を使用したりすることなく、簡単にセットアップ、構成、維持できます。

堅固なモバイル・エンタープライズ・コラボレーションを実現

ユーザーはモバイル・デバイス上の IBM® MaaS360® Content Suite または IBM® MaaS360® Secure Mobile Browser によって、SharePoint、Windows File Share などから企業コンテンツのアクセス、表示、共有を行うことができます。企業所有または個人所有のデバイスかは問わず、ドキュメントの共同作業に先取り組めます。

MaaS360 Secure Mobile を使用すると、JIRA、内部 Wiki、ナレッジベース、レガシー ERP システムなど、イントラネット・サイトや内部アプリの可能性を安全に解放することができます。

データは、データ漏えい防止 (DLP: Data Leak Prevention) 制御機能のある、暗号化されたコンテナ内で保護されます。従業員が組織を辞めた場合は、デバイスを選択的にワイプして企業データや企業アプリのみを削除したり、完全にワイプしてデバイスを工場出荷時の設定に戻したりすることができます。



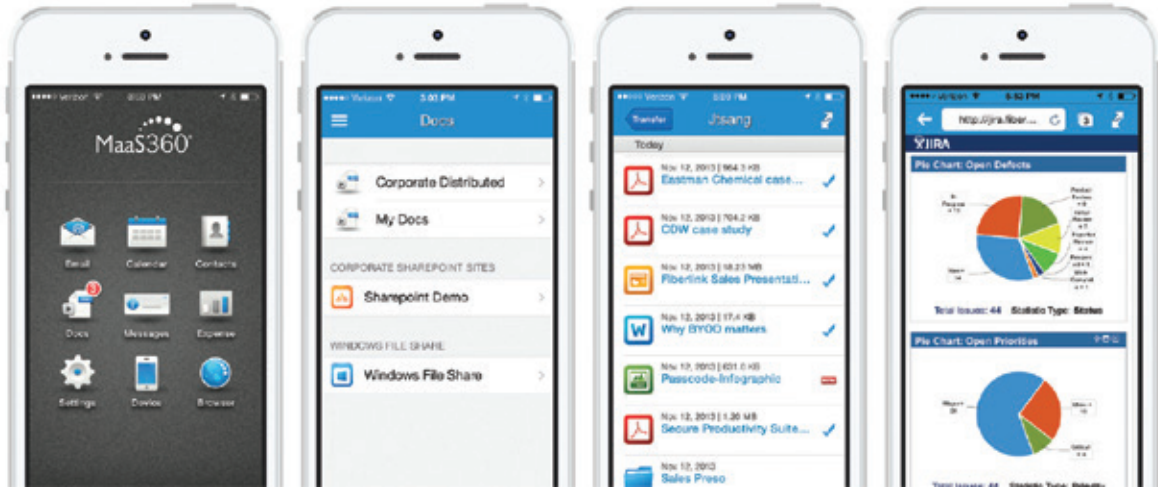


図 1: モバイル・デバイス上の MaaS360 コンテナー、データ・リポジトリ、ドキュメント、イントラネット・サイトの例

外出先でもエンタープライズ・リソースにアクセス

- IBM MaaS360 Gateway for Documents およびモバイル・デバイス上の MaaS360 Content Suite により、SharePoint、Windows File Share などから企業コンテンツを取得、表示、編集、共有することが可能
- 企業所有のデバイスか個人所有のデバイス (BYOD) かを問わず、ドキュメントの共同作業を出先で行うことが可能
- IBM MaaS360 Gateway for Browser および MaaS360 Secure Mobile Browser を使用して、JIRA、内部 Wiki、ナレッジベース、レガシー ERP システムなど、イントラネット・サイトや内部アプリケーションの可能性を安全に解放
- IBM MaaS360 Gateway for Apps により、エンタープライズ・システムとアプリ・データベースへのアプリ内 VPN トンネルを実現

システムと容易に統合

- IT 環境へのハードウェアの追加は不要
- デバイス VPN は不要 (アプリ・レベルの「インスタント」VPN)
- ネットワークの変更は不要
- LAN 外部のデバイスまたはサービスからのインバウンド TCP/IP 接続は不要
- ファイアウォールのセキュリティー構成は不要

認可および詳細アクセスを制御

- 許可されたモバイル・デバイスでのみ企業データを表示することが可能
- ゲートウェイとデバイス間の通信を完全に暗号化
- 組織内の個々のデバイスとユーザーを有効化またはブロック
- 選択したコンテンツとアプリケーションのみをパートナー、請負業者、コンサルタントなどに公開

企業の機密データの流出を抑制

- 暗号化されたコンテナーでデータを保護
- 詳細なポリシーを設定、適用して強力なモバイル・セキュリティーと DLP 制御を提供
- 認証を実施し、認可を有効にすることで、部外者による機密データへのアクセスを阻止
 - 企業データは必ず暗号化してからモバイル・デバイスに格納
 - 紛失または盗難にあった場合、デバイスと機密データを完全にワイプ
 - MaaS360 により、暗号化データを読み取ることなく、ゲートウェイとデバイス間のトラフィックを移動
 - モバイル・アプリケーション・サーバーがパブリック・インターネットに公開された際に発生する可能性のあるプローブや攻撃に対するネットワークの脆弱性を阻止
 - 不正アプリによる企業 LAN へのアクセスを許可する可能性のある VPN の使用は不要

モバイル・イントラネット・アクセス

MaaS360 Gateway Suite は、SharePoint, Windows Files Share、イントラネット・サイト、アプリ・データベースなどを、モバイルデバイスでモバイル・デバイス上のシームレスで保護されたアクセスのために解放して、出先での企業コラボレーションを実現します。

主な特長

- モバイル・デバイスの企業リソースに安全にアクセス
- SharePoint と Windows File Share のコンテンツを表示および共有
- イントラネット・サイトの情報を閲覧および取得
- 内部データベースへのアプリ内 VPN トンネルを有効化
- FIPS 140-2 準拠の AES 256 暗号化コンテナを使用
- 認証と認可を施行
- コピー/貼り付け、個人アプリでのドキュメントの表示、印刷および画面キャプチャへの制限など、DLP 制御を構成

IBM MaaS360 の詳細と 30 日間の無料トライアルのご利用については、次の Web サイトをご覧ください:

www.ibm.com/maas360



© Copyright IBM Corporation 2016

IBM Systems and Technology Group
Route 100
Somers, NY 10589

Produced in Japan
February 2016

IBM, IBM ロゴ、ibm.com、および X-Force は、世界の多くの国で登録された International Business Machines Corporation の商標です。BYOD360™、Cloud Extender™、Control360®、E360®、Fiberlink®、MaaS360®、MaaS360® およびデバイス、MaaS360 PRO™、MCM360™、MDM360™、MI360®、Mobile Context Management™、Mobile NAC®、Mobile360®、MaaS360® Productivity Suite™、Simple. Secure. Mobility.®、Trusted Workplace™、Visibility360®、および We do IT in the Cloud.™ およびデバイスは、IBM 社の一員である Fiberlink Communications Corporation の商標または登録商標です。他の製品名およびサービス名等は、それぞれ IBM または他社の商標である場合があります。現時点での IBM の商標リストについては、次の Web サイトをご覧ください。ibm.com/legal/copytrade.shtml でご覧いただけます。

Microsoft, Windows, Windows NT、および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

性能データとお客様の事例は、説明目的のみのために提示しています。実際の性能結果は、特定の設定や運用条件によって異なる場合があります。他社の製品またはプログラムと IBM の製品またはプログラムを併用した場合の操作の評価および検証は、お客様の責任で行ってください。

本資料の情報は「現状のまま」提供され、商品性、特定目的への適合性に対する保証、および非侵害の保証または条件を含め、いかなる明示的または黙示的な保証も行いません。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。

適用されるすべての法令と規則の順守は、お客様の責任範囲とします。日本 IBM は、法律上の助言を提供することはいたしません。また日本 IBM のサービスまたは製品が、お客様においていかなる法を順守していることの裏付けとなることを表明し、保証するものではありません。

IBM の将来の方向性および指針に関する記述は、予告なく変更または撤回する場合があります。

確実なセキュリティ体制への取り組みについて:IT システムのセキュリティでは、社内外の不適切なアクセスの防止策、検出、対応に取り組むことで、システムと情報を保護しています。不適切なアクセスにより、情報が改ざん、破壊、または不正流用される可能性があり、システムへのダメージや他者への攻撃といったシステムの悪用が生じることがあります。IT システムまたは製品によってセキュリティ対策が万全になると考えることは危険であり、1 つの製品またはセキュリティ対策で不正アクセスを完全に有効に防ぐことはできません。IBM のシステムと製品は、包括的なセキュリティ・アプローチの一部として設計されています。そのため、運用手順を追加することがどうしても必要となり、効果を最大限に高めるには、他のシステム、製品、サービスが必要になることがあります。IBM は、システムと製品が他者による悪意のある行為または不正行為から免れることを保証するものではありません。



Please Recycle