



## 主なメリット

- 企業データを保護する強固な Web ブラウザを導入し、iOS、Android、Windows Phone デバイスの生産性を向上
- VPNを必要とせずに、社員が企業イントラネットサイトへ保護されてアクセスできる集中管理されたプラットフォームを使用
- きめ細かいセキュリティ・ポリシーで、モバイル・イントラネットのエクスペリエンスをコントロール
- 悪意がある Web サイトからの攻撃やマルウェアを防止
- 幅広い範囲のビジネスニーズを網羅する、モバイル Web の課題を克服

# IBM MaaS360 Secure Mobile Browser

企業データのロックを解除、危険があるウェブサイトに対する脆弱性を低減

## モバイル・デバイスでの Web へのアクセスのコントロール

IBM® MaaS360® Secure Mobile Browser は、VPN を必要とせずに、社員に企業イントラネット・サイトやネットワークへの保護されたアクセスを提供します。

マルウェア、人事 (HR) ポリシー違反、あるいは単なるユーザーの貴重な時間の無駄を含んでいる可能性がある危険な Web サイトに対する、モバイル・デバイスの脆弱性も低減できます。

MaaS360 Secure Mobile Browser を利用する企業は、ソーシャルネットワークワーキング・サイト、ダウンロードサイト、露骨なサイトなどを含めて、ユーザーにアクセスさせたくないコンテンツのカテゴリを指定することができます。フィルタリング基準は 60 を超えるカテゴリがあり、何百万もの URL が分類されています。

特定の URL を設定して、該当する Web サイトへのアクセスをフィルターすることができます。IBM® MaaS360® Device Management のポリシーやブラックリストによって、ネイティブまたはサードパーティのブラウザを無効にすることができます。

MaaS360 Secure Mobile Browser は、ほぼリアルタイムでメールを管理者に送信し、こうしたサイトへのアクセスを警告することができます。

MaaS360 Secure Mobile Browser で、できること:

- クラウドベースの集中管理プラットフォーム
- 使いやすいポリシーの作成、リモートからの over-the-air (OTA) での割り当て
- VPN デバイスなしでの、企業イントラネットサイトやネットワークへの保護されたアクセス
- SharePoint、JIRA、内部 wikis、レガシー ERP システムなどのモバイル化
- ブラウザのトラフィックの傍受による継続的な保護
- カテゴリ別での URL の制限、および特定の URL へのアクセスの許可
- スキャンエンジンやレピュテーションデータベースを使用して、既知のマルウェアや悪意のある Web サイトをブロック
- クッキー、印刷、ファイルのダウンロード、コピーおよび貼り付けの無効化
- カスタマイズ可能なブロッキング、ほぼリアルタイムでの通知、例外やレポートのオプション





図 1: さまざまなモバイル・デバイスでの MaaS360 Secure Mobile Browser の例

## モバイル・イントラネット・エクスペリエンスのコントロール

MaaS360 Secure Mobile Browser は、スマートフォンやタブレット向けの強固な Web ブラウザです。タブ化されたブラウジング、ブックマーク、検索、共有や履歴の機能を備えた、直感的なユーザー・インターフェースです。組織内で MaaS360 Secure Mobile Browser を構築して、モバイル・デバイスの脆弱性を低減し、HR ポリシーの違反を防ぎ、ユーザーの注意をフォーカスさせる方法はたくさんあります。

- **共有ヘルスケア・プロバイダー・デバイス:** 患者記録を保護し、医療参照やポイント・オブ・ケア Web サイトに集中し、VPN 装置接続を必要としないイントラネットサイトへのアクセスを提供することで、医療作業h者による共有デバイスの使用を最適化します。

- **専用小売販売時点管理 (POS) デバイス:** 小売スタッフの生産性を改善し、チェックアウト、在庫照会、Web ストアの利用可能性のための特定の Web サイトに対して POS デバイスをロックすることで、オンデバイスのデータを保護します。
- **共有教育デバイス:** 教室で、共有学習デバイスで露骨な Web サイトへのアクセスを制限することで生徒を集中させ、教育機関のプライオリティを児童インターネット保護法 (CIPA) の規制に適合させます。
- **病院のコンシェルジュ・デバイス:** デバイスをチェックインまたはチェックアウト、施設のアメニティの表示、地域の天気や交通へのアクセスに限定することで、病院スタッフの効率を向上させます。
- **イベント・デモ・デバイス:** わずかな、キオスクで選択した Web サイトへのアクセスだけを許可することで、デモ・スタッフの有用性を高めます。

### ブラウザ構成の設定

- デフォルト・ブラウザとして設定
- MaaS360 コンテナのセキュリティ・ポリシーを適用
- クッキーやファイルのダウンロードを無効化
- コピー、貼り付け、印刷を制限
- ブラウザのキオスク・モードを有効化
- デフォルトのホームページを設定し、ブックマークをカスタマイズ

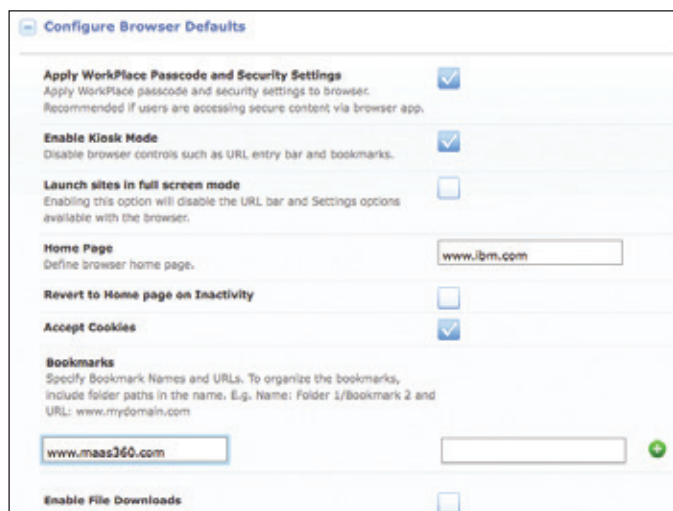


図 2: MaaS360 コンソールでのブラウザ設定の例

### Web サイトのフィルターを設定

- URL カテゴリの選択で、許可、ブロック、追跡
- 60 を超えるカテゴリ、数百万の URL から選択
- ドメイン名または URL に基づいて、例外を許可
- 特定の Web サイトをブラックリスト化

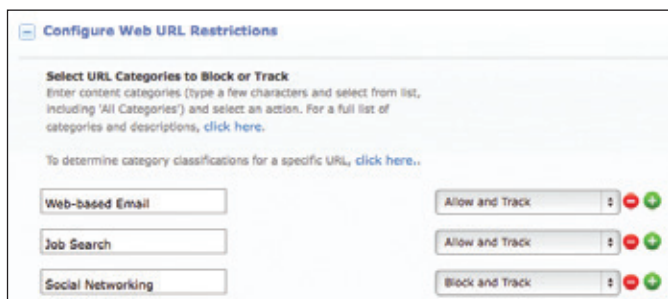


図 3: ポータルでの Web サイト・カテゴリのフィルター設定の例

### ユーザーおよび管理者の通知設定

- 禁止されているブロックされている URL へアクセスしようとした場合に、カスタムのテキストまたは HTML による通知をユーザーへ送信
- ポリシーに違反する場合、特定の URL に限定
- ユーザーがブロックされた場合に、管理者へ通知を送信
- 管理者への通知が送信される前に、ユーザーは何回ブロックが可能であるかを定義

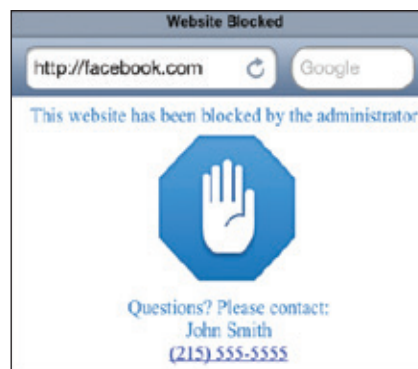


図 4: Web サイトがブロックされている場合のブラウザでのユーザー通知の例

### デバイス固有および会社のレポート

- カテゴリやドメインのブロックや追跡の履歴のサマリーをグラフィカルに表示
- 特定のデバイスブロックおよび追跡されたドメインの履歴の詳細なレポートにアクセス



図 5: デバイスのブラウザ違反レポートの例

## 予防的 Web セキュリティー

MaaS360 Secure Mobile Browser は、データを保護し、iOS や Android デバイスでの公開 Web サイトや企業のイントラネットサイトへのアクセスのコントロールで、生産性を向上

以下を含め、指定したカテゴリに基づいて、Web サイトへのアクセスを制限または許可：

- 広告およびポップアップ
- 匿名化
- ボットネット
- チャット
- 犯罪活動
- 顔合わせやパーソナル
- ダウンロードサイト
- エンターテイメント
- 露骨
- フォーラムおよびニュースグループ
- ギャンブル
- ゲーム
- ハッキング
- 画像共有
- インスタントメッセージング
- マルウェア
- ニュース
- ピア・ツー・ピア
- フィッシングや詐欺
- ショッピング
- ソーシャルネットワーキング
- スポーツ
- ストリーミングメディアおよびダウンロード
- さらに、もっと多く

- 柔軟なポリシー作成のフレームワーク
- カスタマイズ可能なポリシー割り当て
- MaaS360 Mobile Device Management との統合で最適化されたコントロール (オプション)

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](http://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](http://ibm.com/legal/copytrade.shtml) でご覧いただけます。

Apple、iPhone、iPad、iPod touch、および iOS は、米国、その他の国における Apple Inc. の登録商標または商標です。

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。

本書の情報は最初の発行日の時点で得られるものであり、IBM によって予告なしに変更される場合があります。掲載されている製品・サービスは IBM がビジネスを行っているすべての国・地域でご提供可能なわけではありません。

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、保証するものでもありません。

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ー体制への取り組みについて:IT システムのセキュリティーでは、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ー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ー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ー・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