



Windows 10 Mobile

モバイル ファーストの世界に最適化された
多層セキュリティ

2015 年 11 月

このドキュメントに記載されている情報は、このドキュメントの発行時点におけるマイクロソフトの見解を反映したものです。市場の変化に対応する必要があるため、このドキュメントは記載された内容の実現に関するマイクロソフトの確約とはみなされないものとします。また、発行以降に発表される情報の正確性に関して、マイクロソフトはいかなる保証もいたしません。

このホワイトペーパーは情報の提供のみを目的としており、明示または黙示にかかわらず、このドキュメントに記載されている情報について、マイクロソフトはいかなる責任も負わないものとします。

お客様ご自身の責任において、適用されるすべての著作権関連法規に従ったご使用をお願いいたします。このドキュメントのいかなる部分も、マイクロソフトの書面による許諾を受けることなく、その目的を問わず、どのような形態であっても、複製または譲渡することは禁じられています。ここでいう形態とは、複写や記録など、電子的な、または物理的なすべての手段を含みます。ただしこれは、著作権法上のお客様の権利を制限するものではありません。

マイクロソフトは、このドキュメントに記載されている内容に関し、特許、特許申請、商標、著作権、またはその他の無体財産権を有する場合があります。別途マイクロソフトのライセンス契約上に明示の規定のない限り、このドキュメントはこれらの特許、商標、著作権、またはその他の知的財産権に関する権利をお客様に許諾するものではありません。

このドキュメントの例で登場する企業、組織、製品、ドメイン名、電子メール アドレス、ロゴ、人物、場所、出来事は架空のものです。実在する企業、組織、製品、ドメイン名、電子メール アドレス、ロゴ、人物、場所、出来事とは一切関係ありません。

このプレゼンテーションで使用されている画面はハメコミ合成です。一部のアプリは別売りです。出荷状況とエクスペリエンスは変動する場合があります。アプリは Windows ストアで提供されているものです。出荷状況は変動する場合があります。一部の機能とサービスには、Microsoft アカウント、Wi-Fi アクセス、データ接続が必要です。通信事業者の料金がかかります。アプリとコンテンツの提供状況は変動する場合があります。Office ライセンスは別売りです。すべての機能を使用する場合は購入が必要です。

EDP は「間もなく」Windows Insider Preview に追加され、2016 年夏には提供される範囲が拡大される予定です。

特に記載がない限り、すべての機能は Windows 10 Mobile が提供されているすべての国で利用できます。アジアの一部の国では、画面のレイアウトが異なる場合があります。

© 2015 Microsoft Corp. All rights reserved.

Windows 10 Mobile が実現する 最新のセキュリティ脅威からの保護

従業員の高度なモバイル化に対応するべく IT プラクティスを調整する際、どのような規模の組織でも最優先事項として挙がるのは、強力なセキュリティ対策の実装です。企業の経営陣、ビジネス パートナー、顧客は皆、どのような手段でアクセスされる場合であれ、重要なデータがセキュリティ保護され、機密性が保たれることを望んでいます。しかも組織のモバイル デバイスは、増え続けるデータ保護関連法令に常に準拠している必要もあります。

セキュリティ脅威に関する状況は絶えず変化しているため、残念ながらこれらの要件を満たすことは容易ではありません。悪意のあるコードやソーシャル エンジニアリング攻撃の新たな変種は毎日のように登場し、モバイル デバイスを含め、考えられるあらゆる手段を駆使して企業データへの不正アクセスが試みられています。ユーザーと情報を攻撃から保護するには、組織に多層防御型のモバイル セキュリティを実装する必要があります。

Windows 10 Mobile が実現する多層化されたセキュリティを利用すれば、組織はセキュリティ態勢を妥協することなく、時間と場所の制約を受けずにネットワークに接続できる環境を整え、ユーザーの生産性を維持することができます。Windows 10 Mobile が備えるエンタープライズ レベルのセキュリティ制御機能は、企業の情報とリソースを保護するための厳格な要件を満たしているうえ、IT 部門によるアクティブ化と管理も容易で、企業ポリシーへの確実な遵守を実現できます。

Windows 10 Mobile の多層保護は、次の要素で構成されています。

- **ID とアクセス制御。**

Windows 10 Mobile デバイスは、Active Directory と統合された ID とアクセス制御の機能を備えており、ユーザーを認証してから企業のネットワーク、アプリケーション、データへのアクセスを許可するセキュリティ対策を簡略化したうえで強化します。この要素には、Azure Active Directory、シングル サインオン (SSO)、低コストの多要素認証、生体認証サポート¹、ポリシーの強制適用、簡素化された VPN アクセスが含まれます。

- **情報の保護。**

モバイル デバイス、企業クラウド、オンプレミス データ ストアのいずれに情報が格納されている場合でも、Windows 10 Mobile がデータ盗難に対する柔軟かつ効果的な保護対策を提供します。組み込み型のデバイス暗号化と情報権管理の機能により、Windows デバイス上のデータを従来よりも包括的にセキュリティ保護することができます。

¹ 生体認証サポートは Windows Hello を通じて提供されます。顔認識または虹彩スキャン用の特殊な照明付赤外線カメラか Windows 生体認証フレームワーク対応の指紋リーダーが必要です。

- **マルウェア対策。**

Windows 10 Mobile デバイスは暗号化を使用して重要なシステム リソースとアプリを保護し、マルウェアの脅威を軽減します。この機能は、Windows デバイスの安全性を保つための実績のある堅固な保護手段を複数組み合わせ、ルートキット、ジェイルブレイク、感染アプリの実行を防ぎ、オンライン詐欺とマルウェアをブロックします。

ID とアクセス制御

Windows 10 Mobile には Windows Hello と Microsoft Passport が導入されており、企業リソースへの安全なアクセスの確保と資格情報の保護をこれまでよりも容易に実現できます。これらの機能をデバイスに組み込まれた生体認証サポートと組み合わせることで、組織は脆弱なパスワードに伴うリスクを最小限に抑制できます。ユーザーはエンタープライズレベルのセキュリティと利便性の恩恵を受けながら、シンプルでパーソナルな操作性が得られます。キーまたは証明書ベースの認証を使用するため、企業の資格情報をモバイルデバイスに格納する必要がなく、デバイスが盗難された場合でもデータやリソースに不正にアクセスされるおそれはありません。Windows 10 Mobile デバイスは多層防御型のセキュリティ アプローチもサポートしており、可能な場合には常に多要素認証が使用されます。

多要素認証とシングル サインオン

Windows 10 Mobile を導入することで、組織はセキュリティや生産性に妥協することなく、エンタープライズレベルの要求を満たす企業リソースへの安全なアクセスを実装できます。多要素認証を通じて、特に Windows 10 Mobile では認証要素の 1 つとして生体認証を使用できるため、ハッカーによるソーシャルエンジニアリングやブルートフォース攻撃が困難になります。また、生体認証²を使用すれば、ユーザーはデバイスに即座にアクセスでき、生産性を発揮しやすくなります。

Windows 10 Mobile デバイ스에搭載された強力な認証により、組織は、アクセスの制御、未承認ユーザーのブロック、企業リソースへの接続の効率化が容易になります。ユーザーは、虹彩スキャン²などの資格情報を入力し、業務に必要な情報とアプリへの SSO アクセス権を取得できます。

また、Microsoft Passport の機能により、Windows 10 PC にサインインする際のリモート資格情報として Windows 10 Mobile デバイスを使用できます。サインイン プロセスでは、Windows 10 PC がユーザーの Windows 10 Mobile デバイス上の Microsoft Passport に Bluetooth を介してアクセスすることで、スマートフォンへの接続が実現されます。ユーザーは常にスマートフォンを携帯しているため、Microsoft Passport による多要素認証の実装は他のソリューションによる場合に比べてコストと複雑さが低く抑えられます。

² 生体認証サポートは Windows Hello を通じて提供されます。顔認識または虹彩スキャン用の特殊な照明付赤外線カメラか Windows 生体認証フレームワーク対応の指紋リーダーが必要です。

生体認証サポート

Windows Hello¹ は Windows 10 向けの新しい生体認証サインイン オプションで、ユーザーは顔認識、指紋認識、虹彩認識のいずれかを使用してデバイスのロックを解除できます。デバイスへの認証はユーザーごとに一意の生体認証 ID を通じて有効になるため、複雑なパスワードを記憶したり、書き留めておいたりする必要がありません。

Windows 10 Mobile では、生体認証は後から付け足されたものではなく、デバイスのセキュリティ コンポーネントに統合されています。Windows Hello で使用されるユーザーの生体認証データは、ユーザーのデバイス間で引き継がれたり、クラウド上に一元的に格納されたりすることはありません。センサーによって読み取られた生体画像はアルゴリズム形式に変換され、元の画像は破棄されて復元不可能になります。これにより、生体画像をデバイスから盗み、それを使用して他のデバイスから企業リソースに不正にアクセスすることはできなくなります。また、なりすまし対策が組み込まれているため、ユーザーの眼の写真などを使用してデバイスにアクセスすることもできません。保護をさらに強化するために、ユーザーはカメラが故障した場合に、生体認証スキャンと共に暗証番号 (PIN) を入力してデバイスを解除することが求められます。デバイスごとに設定される暗証番号 (PIN) 自体も、デバイス上でセキュリティ コンポーネントを使用して保護されます。

リソースに対する安全でシンプルな認証

Windows 10 に組み込まれている [Microsoft Passport](#) は、企業のアプリケーションやオンライン リソースへのアクセスをユーザーに許可する前に、非対称キーによる暗号化を使用してユーザー認証を行います。これは、スマート カードの利用による証明書ベース認証やスマートフォンによるネットワーク検証を実現している実証済みの技術と同様の手法です。盗難のおそれがありいたる所で使用可能なパスワードとは異なり、Microsoft Passport キーはデバイス上で[トラステッド プラットフォーム モジュール \(TPM\)](#) を使用して生成され、デバイスにバインドされています。そのため攻撃者はデバイスを盗むだけでなく、何らかの方法でユーザーの指紋、虹彩、顔のいずれかを作成しない限り、デバイスのロックを解除して企業のリソースにアクセスすることはできません。

Microsoft Passport では、Azure Active Directory に対してユーザーの認証を行い、ユーザーが使用を許可されている業務用アプリケーション、システム、データへのアクセス権を付与します。Azure Active Directory を使用しているため、2,500 個を超えるオンライン アプリにも SSO が可能です。SSO を利用することで、ユーザーは 1 度のログインで、組織の SharePoint チーム サイト、DropBox、salesforce.com はもちろんのこと、社内用の基幹業務 (LOB) アプリケーションにもアクセスできます。

VPN

社内ネットワークへのモバイル接続の提供は、モバイル ワーカーを擁する組織にとって不可欠な要素です。Windows 10 Mobile には VPN プラットフォームが組み込まれているため、ユーザーは内部システム、イントラネット サイト、アプリケーションにすばやくアクセスできます。VPN ベンダーは、企業顧客のニーズに対応するプラットフォームを容易に拡張、構築することができます。Cisco、Pulse Secure、F5、SonicWALL、Check Point、MobileIron をはじめとする数多くのベンダーが、Windows ストアからダウンロード可能な Windows 10 向けアプリを販売しています。

Windows 10 Mobile には常時接続 VPN が搭載されているため、IT 部門は VPN を構成してユーザーが Microsoft Passport の資格情報でスマートフォンやタブレットのロックを解除したときに VPN に自動的に接続されるよう設定できます。また、アプリが備える VPN 機能を使用した企業リソースへの接続を、Windows 10 Mobile デバイス上のどのアプリに許可するかを定義することもできます。たとえば、IT 部門はユーザーがスマートフォンで社内用 LOB アプリを選択したときにアプリが VPN “A” プロファイルのみを使用して接続するように指定できます。

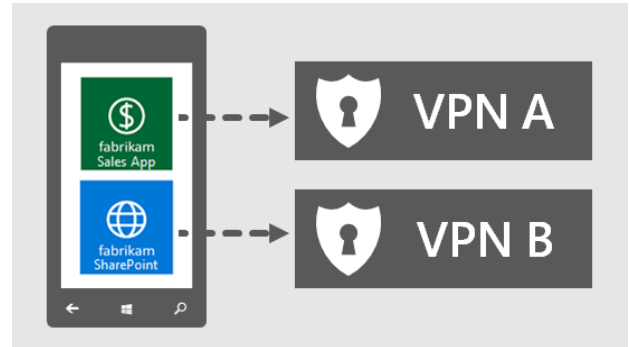


図 1: IT 部門は特定の VPN を経由して接続するアプリを定義できる

同様に、ユーザーがスマートフォンで SharePoint チーム サイトを選択した場合は、デバイスが VPN “B” プロファイルのみを使用して接続するように指定できます (図 1 参照)。これらの VPN 接続はすべてバックグラウンドで自動的に処理されるため、ユーザーは作業をすぐに開始できます。遅延は生じず、別のパスワードを入力する必要もありません。VPN が多要素認証と SSO をサポートしているため、企業のオンプレミス リソースへの安全なアクセスが確保されます。IT 部門は、管理対象外のアプリケーションが VPN 接続を経由して企業のリソースにアクセスするのを防ぎ、データの漏えいを抑止できます。

デバイス アクセス ポリシー

デバイスは常に IT 部門の管理下に置かれます。IT 部門は[モバイル デバイス管理 \(MDM\)](#) ポリシーまたは Exchange ActiveSync (EAS) ポリシーを適用することで、Windows 10 Mobile 搭載のスマートフォンやタブレットによるデバイス アクセスをセキュリティ保護できます。デバイスに生体認証センサーが搭載されていない場合は、暗証番号 (PIN) または英数字のパスワードの使用を強制でき、長さや複雑さのパラメーターなどを要件として指定できます。Windows Hello³ は、MDM を使用して直接管理することもできます。

³ 生体認証サポートは Windows Hello を通じて提供されます。顔認識または虹彩スキャン用の特殊な照明付赤外線カメラか Windows 生体認証フレームワーク対応の指紋リーダーが必要です。

情報の保護

ID とアクセスの保護以外にも、Windows 10 Mobile には、保存中および送信中の企業データを保護する際に役立つ手段がいくつも備わっています。アプリがデバイスに格納する情報は、業界トップクラスの暗号化によって盗難から保護されます。また、従業員と顧客の間でやり取りされる情報のためのデータ漏えい保護技術が Windows 10 Mobile に追加されており、承認されたユーザーのみが企業のデータにアクセスできるようになっています。

知的財産とクライアント データの保護は事業を健全な状態に維持するうえで不可欠ですが、それによって従業員の生産性に悪影響が生じては意味がありません。新たなモバイル アプリの作成に要するコストや時間が増加する事態も組織としては避ける必要があります。Windows 10 Mobile に組み込まれた分離セーフガードは、ユーザー エクスペリエンスに支障をきたすことなく、個人の情報と企業の情報の間に明確な境界を構築します。ユーザーは面倒な手順を踏まなくても、フォルダー間やコンテナ間を移動して企業の情報にアクセスできます。データ保護技術はモバイル プラットフォームに初めから埋め込まれており、企業のシステムやアプリから取得されたデータは自動的に暗号化されます。これらの処理を補完するために、組織は MDM から適用できるポリシーを使用して、リスクにさらされたデータの格納と共有の方法を管理できます。

デバイスの暗号化

Windows 10 Mobile では BitLocker 技術を使用して、オペレーティング システムとデータ ストレージのパーティションも含めたすべての内部ストレージを暗号化します。デバイスの暗号化はユーザーが直接有効にできるほか、企業の管理対象デバイスは IT 部門が暗号化を有効にして強制適用できます。デバイスの暗号化を有効にすると、スマートフォンに格納されたすべてのデータが自動的に暗号化されます。保護された Windows 10 Mobile デバイスが紛失または盗難にあった場合でも、デバイス ロックとデータ暗号化を併用しているため、未承認の第三者がスマートフォンから機密情報を取得することはほぼ不可能です。

加えて、外部からの干渉に対してデータの安全性をさらに向上させるために、Windows 10 Mobile には Protection Under Lock (ロックによる保護) 機能が追加されています。この機能では、デバイスがロックされるたびに暗号化キーが RAM から削除されるため、ハッカーやマルウェアは、ダイレクト メモリ アクセス (DMA) 攻撃を通じて暗号化キーを探し出すことができません。デバイスがロック状態にある間、アプリからデータへのアクセスは不能になります。ユーザーがデバイスのロックを解除するまで、すべての要素が厳重に保護されます。

エンタープライズ データ保護⁴

スマートフォンやタブレットが個人的な用途と業務用途の両方に使用されることは珍しくありませんが、IT 部門がデータ漏えい防止ポリシーを適用する際には、この点が課題になります。社内のデータが個人的なメール、ソーシャル メディア、クラウド ベース アプリを通じて未承認のユーザーに開示されることがあってはなりません。企業のデータに対して禁止された機能でも個人的な目的で使用する分にはまったく問題ない場合、スマートフォンを完全にロックダウンするわけにもいきません。たとえば、組織のドキュメントを個人の Dropbox に保存するのは望ましくありませんが、休暇中のプライベート写真を保存するのはまったく問題ありません。

組織のデータと個人のデータの分離を維持する一般的な解決策は、業務関連の活動時にユーザーがログインする専用のコンテナをデバイス上に作成することです。コンテナ内のすべてのデータに対してデータ共有に関する企業ポリシーを適用することで、データがコンテナから持ち出される事態を防止できます。ところがこの方法では、ユーザーがデバイスで作業するたびにコンテナにログイン/ログアウトをする必要があるため、生産性が低下し、煩雑さが増すおそれがあります。Windows 10 Mobile では、上記とは異なるエンタープライズ データ保護 (EDP) というアプローチが採用されています。EDP は間もなく Windows Insider Preview で提供され、2016 年の夏には提供範囲がさらに拡大される予定です。データの分離と封じ込めがプラットフォーム レベルで統合されるため、シームレスな操作性が実現し、ユーザーは単一の環境で作業できます。企業のリソースにアクセスする際に、分離されたコンテナにログインする必要はありません。企業のシステムやアプリから取得されたファイルとデータに、ポリシーの適用と暗号化が自動的に実行されます (スクリーンショット 1 参照)。



スクリーンショット 1:
DP で保護されたアプリには
データ保護を示すアイコンが
付加される

たとえば、Excel ファイルが添付された電子メールがユーザーの業務用 Office 365 受信ボックスに届いた場合、Windows 10 Mobile デバイスは、そのコンテンツが企業のデータであることを自動的に判別し、デバイスに格納されている間、そのデータを暗号化します。組織が設定した保護レベルによって個人のアプリやストレージとの共有がブロックされている場合、ユーザーは添付ファイルの内容をコピーして Word ドキュメントに貼り付け、OneDrive for Business にそのドキュメントを保存できます。しかし、添付ファイルから取得した情報を個人のアプリにコピーすることはできません。また、信頼された Word ドキュメントを信頼されていない個人のクラウド ストレージ アカウントに保存することもできません (図 2 参照)。

⁴ EDP は、間もなく Windows Insider Preview に追加され、2016 年の夏には提供範囲がさらに拡大される予定です。

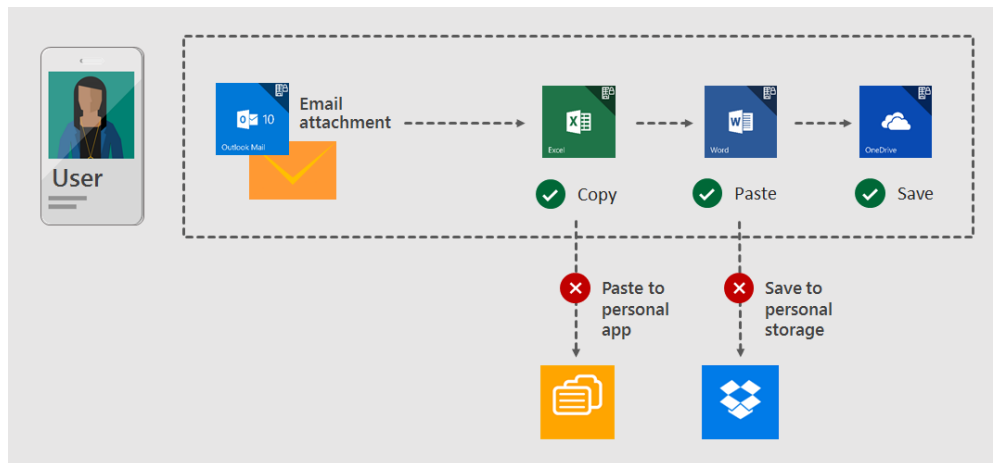


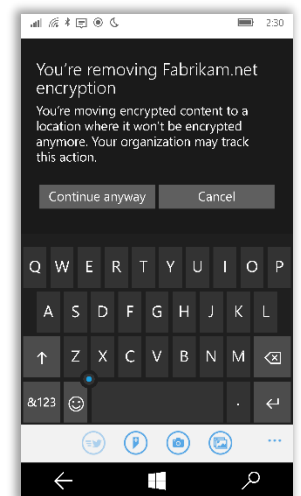
図 2: この例は、個人のアプリやストレージとの共有をブロックするように組織によって保護レベルが設定されているシナリオで、暗号化されたデータが保護されるようすを示している

追跡の適用

組織は EDP⁵ を使用して、不適切なデータ共有に対するブロックと監査を実行できます。ユーザーに制限の無効化を許可することはできませんが、ポリシー違反を通知する警告が表示され、ユーザーの操作が MDM システムに記録されます (スクリーンショット 2 参照)。またユーザーは、ドキュメントを新規作成する際に、対応アプリ内でドキュメントの分類を企業用から個人用に手動で変更することもできます (次項参照)。新規ドキュメントを個人用に分類すると、企業のドキュメントから取得した情報を個人用の新規ドキュメントにコピーして貼り付けることはできなくなります。これらの分類操作は、後で確認できるように記録されます。

アプリケーション データの安全性確保

EDP では、業務用途専用に指定されたアプリが「信頼済み」に分類され、提供する保護レベルが決定されます。信頼済みのアプリは管理対象となり、すべてのデータが自動的に暗号化されて保護されます。EDP は、これらのアプリが信頼された場所内のデータにアクセスし、信頼された場所にデータを格納することを許可します。このアプローチでは、アプリケーションがコンテナ内で実行しているかのように扱われつつも、実際にはデバイス内の別の領域にログイン/ログアウトする必要がありません。しかも、アプリケーション開発時のコード変更や「アプリ ラッパー」の作成も必要がなく、開発に要する時間とコストを大幅に節約できます。



スクリーンショット 2:
データを侵害した場合
ユーザーに警告が表示される

⁵ EDP は、間もなく Windows Insider Preview に追加され、2016 年の夏には提供範囲がさらに拡大される予定です。

対応アプリとは、個人用途と業務用途の両方に使用できるアプリを指します。対応アプリは EDP による制限に対応しており、データの取得元に基づいて企業のデータのみを暗号化し、個人のデータは暗号化しません。たとえば、ユーザーは対応アプリである Outlook メールを業務用途と個人用途のどちらにも使用できますが、業務用の電子メールを個人の電子メール受信ボックスに移すことはできません。Outlook は、企業の Exchange Server⁶ または Office 365 アカウントから受信したメールを企業の暗号化キーで暗号化する必要があると認識します。Yahoo アカウントから受信した個人の電子メールは暗号化されません。

信頼されたアプリ一覧にないアプリは、EDP の保護を受けません。また、デバイスや共有上に格納された企業の情報にアクセスすることも、その他の企業のリソースにアクセスすることもできません。

データ アクセスとストレージのセキュリティ保護

管理者は EDP⁷ を利用して、どのオンプレミスの場所、クラウドの場所、データ ストア、ネットワークが信頼されているかを定義できます。これらのストアに保存されたデータとドキュメントは、承認された企業ユーザーのみがアクセスするため、暗号化する必要がありません。IT 部門は、企業用の IP アドレス範囲や、ネットワークに含めるコンピューターを定義するドメインの一覧を設定できます。これらの信頼できるソースから取得されたデータは企業のデータの一部とみなされ、承認された資格情報を持つ企業ユーザーであれば誰でもアクセスできます。つまり暗号化は、ユーザーがデータをモバイル デバイス上に格納するか、信頼されていない場所に移動する場合にのみ適用されます。個人の Dropbox など信頼されていない場所では、企業のデータはすべてユーザーのエンタープライズ キーで自動的に暗号化されるため、そのユーザー以外はアクセスできなくなります。

暗号化キーと EDP による制限は常に MDM システムによって管理されます。そのため、企業はデータを完全に制御下に置くことができ、信頼されていない場所にユーザーが格納したデータの暗号化を解除することもできます。

選択的ワイプとフル ワイプ

管理者は EDP を利用して、管理対象のデバイスから個人のデータのみを残したまま企業のデータをリモートで消去することもできます。この機能を使用すると、従業員が企業を退職する際や業務用デバイスを新しく購入する際に、元のデバイスを個人が使用できるようにすることができます。

⁶ Windows 10 Mobile は、Exchange Server 2010 以後のバージョンと互換性があります。

⁷ EDP は、“間もなく” Windows Insider Preview に追加され、2016 年の夏には提供範囲がさらに拡大される予定です。

Windows 10 Mobile には、紛失したデバイスを探し出せるように、リモートでロック、呼び出し、検索を実行できる機能が組み込まれています。ユーザーは紛失したスマートフォンや盗難されたスマートフォンを見つけるために、Web ベースのツールを使用してデバイスをリモートでロックしたり、デバイスの位置を特定したりできます。スマートフォンの着信音がオンかオフかにかかわらず、大きな音を鳴らすこともできます。IT 部門が MDM システムを使用してこれらの措置を行い、ユーザーをサポートすることも可能です。さらに、盗難防止機能により、デバイスのリセットは阻止されます。紛失や盗難の報告の後でスマートフォンやタブレットが発見された場合も、ロックの解除には特別なコードが必要になります。

Microsoft Rights Management

Microsoft Rights Management (RMS) は Azure クラウド テクノロジーの 1 つで、[Microsoft Enterprise Mobility Suite](#) に含まれています。コンテンツの作成者はこの技術を使用して、ユーザーが第三者に送信する Microsoft Office ドキュメント、PDF、電子メール メッセージなどにアクセス権限を割り当てることができます。IT 部門または承認されたユーザーは、権利が保護されたドキュメントや電子メール メッセージを暗号化し、暗号化されたコンテンツには承認されたユーザーのみが特定の権限を使用してアクセスできるように指定できます。この権限を利用して、読み取り専用アクセス権の強制適用、ドキュメントやメッセージ内でのコピーとペーストの防止、ドキュメントやメッセージの印刷のブロックを実行できます。また、RMS を使用して電子メールの転送を禁止したり、組織内でのみ転送を許可したりすることもできます。

権限管理を活用すると、組織の全体的なデータ セキュリティの水準が向上し、組織の内外で業務データを保護する手段の幅が広がります。RMS をネイティブでサポートしている点は、Windows 10 Mobile 搭載デバイスだけが備える特長です。ユーザーは RMS で保護された電子メールを制約を受けずにやり取りし、スマートフォンやタブレットで RMS で保護されたドキュメントにアクセスできます。その一方で、RMS によるドキュメント セキュリティの有効範囲は Windows 以外のデバイスにも拡張できます。iOS や Android デバイスを使用している顧客やビジネス パートナーは、ブロックされていない限り、ドキュメントにアクセスできます。

マルウェア対策

マルウェアによる攻撃は絶えず巧妙さを増しています。資金の潤沢な犯罪組織は、詐欺、ゆすり、知的財産の窃盗などの悪事を働くために、個人や企業の価値ある情報にアクセスしようと企んでいます。

モバイル デバイスの利用が増えるにつれてそのような資産への侵入口となる攻撃範囲も拡大しており、悪意のあるモバイル プログラムが毎年何十万個も世に放たれています。従業員に企業リソースへのアクセス権を与えることで企業はメリットを得られますが、その一方、システム、アプリ、モバイル デバイス上に格納されているデータを確実に保護できる方法でこれを実現する必要があります。

Windows 10 Mobile には、デバイスとアプリの整合性を損なう脅威への対策が組み込まれています (図 3 参照)。ハードウェアベースの保護機能は、起動プロセスの改ざんを防止するように設計されています。また、デバイス プラットフォームとアプリを保護するために、署名済みの信頼されたアプリのみが実行を許可され、オンライン マルウェアとオンライン詐欺のブロックに効果を発揮します。これらのデバイス レベルのセキュリティ対策によって組織は重大な侵害を防止できるため、顧客の信頼を失ったり、取引の逸失や訴訟によって多額の損失を被るなどのリスクを回避できます。

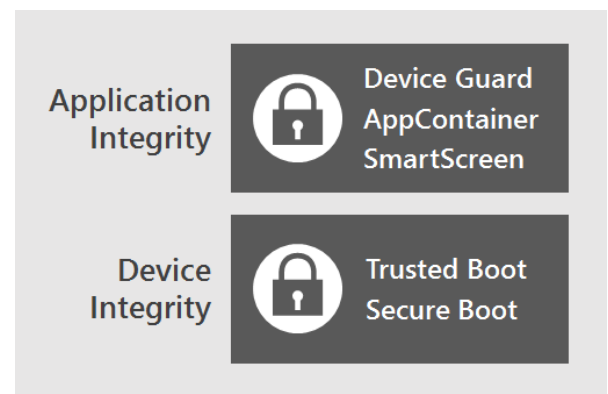


図 3: Windows 10 Mobile のプラットフォーム セキュリティ アーキテクチャ

デバイスの整合性

すべての Windows 10 Mobile デバイスには、ファームウェアを検証するセキュア ブート テクノロジーが搭載されています。このアプローチでは、暗号化によって検証されたデジタル署名がすべての起動コンポーネントに付加されます。こうすることで、承認されたコード以外はデバイスの起動と Windows オペレーティング システムのロードを実行できなくなり、デバイスのハードウェアとファームウェアからオペレーティング システム (OS) までを信頼でつなぐ重要なリンクが確立されます。

この初期セキュリティ チェックが完了すると、トラスト ブートが処理を引き継いで OS の起動プロセスを完了し、ユーザーはスマートフォンを使用できるようになります。トラスト ブートでは、OEM ドライバーやアプリケーションを含め、オペレーティング システム内のすべてのコードがマイクロソフトによって署名済みであることを求められます。この措置により防御の厚みが増し、プラットフォームの整合性が確保されます。Windows ストアから追加されたアプリや信頼されたビジネス アプリも、実行するには適切に署名されている必要があります。

Device Guard

Windows 10 Mobile は、感染アプリケーションを通じてマルウェアがデバイスに侵入するのを防ぐよう設計された保護機能を備えています。各種保護機能が連携することで、ユーザーは信頼されたアプリケーションのみにアクセスでき、デバイスによってアプリケーションの整合性が確認されてから他のアプリケーションやデータとのやり取りが許可されます。

Device Guard では Windows 10 Mobile デバイスをロックダウンし、マイクロソフト、Windows ストア、または組織がポリシーで定義したその他の信頼済みソースによって署名されたアプリのみが実行されるようにします。OS は、ウイルス対策などのセキュリティ ソリューションによってブロックされない限りアプリを信頼するのではなく、企業によって承認されたアプリのみを信頼します。信頼されていないアプリがデバイスにプロビジョニングされたりサイドロードされたりすると、Device Guard はそのアプリの実行を防止し、システム、アプリ、データをセキュリティ侵害から保護します。

アプリケーション サンドボックス

Windows 10 Mobile に組み込まれている AppContainer を使用すると、各アプリは専用のサンドボックス内で実行され、特権の付与は最小限に抑えられます。こうすることで、悪意のあるアプリが不正な特権昇格によってデバイスのシステム、アプリ、データにアクセスするのを防止し、業務用アプリに信頼できるコンテナを提供できます。また、アプリケーション サンドボックスにより、意図せずアプリが競合する可能性が軽減し、ユーザー エクスペリエンスの信頼性が向上します。

セキュリティ保護されたアプリへのアクセス

企業は、Windows ストアまたは会社のポータルを介してユーザーにモバイル アプリへのアクセス権を付与することができます。スマートフォンに配布されたすべてのアプリは、配布方法にかかわらず、Windows 10 Mobile デバイスでの実行に関するセキュリティ制限が強制的に適用されます。Windows ストア アプリはマイクロソフトによって署名されており、不正な改造が行われていないことが確認されています。また、LOB アプリはユーザーが所属する組織によって署名されていないと実行することができません。この署名を行うには、IT 部門がアプリをビジネス向け Windows ストアにアップロードし、登録済みのユーザー デバイスのみに公開します。登録されていないユーザーとデバイスにはこれらのアプリは表示されません。また、MDM システムを介してアプリを配布し、企業の証明書で署名することもできます。

ブラウザー ベースの保護

Microsoft Edge の SmartScreen フィルターは、ユーザーが Windows 10 Mobile で訪問したサイトの評判チェックを実行し、フィッシング詐欺サイトに対する防御を講じます。サイトに疑わしい点がある場合は、SmartScreen によってアクセスが完全にブロックされます。また、ユーザーをだまして悪意のあるソフトウェアをダウンロードさせ、デバイスへのセキュリティ侵害を引き起こすサイトからもユーザーを保護します。Microsoft Edge のコンテンツ処理はすべて、悪意のある実行可能ファイルがデバイスにアクセスできないよう設計された AppContainer で実行されます。また、MDM による制限を通じてブラウザーを管理し、アクセスするサイトを限定したり、検査のためにプロキシ経由でトラフィックをリダイレクトしたりすることもできます。

まとめ

Windows 10 Mobile は、強力な透明性の高い多層防御アプローチを通じて、あらゆる組織や企業のニーズに適したレベルの保護をスマートフォンとタブレットに提供します。ID とアクセス制御、情報の保護、マルウェア対策のすべてにおいて高度な技術が導入されており、ユーザーと組織の両方がその恩恵を受けることができます。ユーザーは、デバイス、アプリ、オンライン リソースへのアクセスがシンプルかつ便利になり、データのセキュリティ侵害に対する懸念が払拭されます。組織は、デバイスによる企業のアプリとデータのやり取りを IT 部門が高いレベルで制御できるようになり、個人のデバイス (BYOD) 向けプログラムや企業デバイス向けプログラムを安心して社内に導入できます。

Windows 10 Mobile が備えるエンタープライズ レベルのセキュリティは、実装が容易なうえに、組織にコスト削減の効果をもたらします。Windows Hello⁸ と Microsoft Passport の導入により、全社規模の多要素認証の実装は大幅に簡略化され、コストも削減されます。Windows Insider Preview に間もなくリリースされ、2016 年夏には提供範囲がさらに拡大される予定のエンタープライズ データ保護は、企業のデータを自動的に暗号化し、安全なモバイル アプリの開発を容易にします。マルウェア対策はデバイスとアプリケーションに組み込まれており、ユーザーが攻撃の標的となるのを防ぎます。エンタープライズ レベルのセキュリティが Windows 10 Mobile 搭載のスマートフォンとタブレットで手軽に実現できるため、IT 部門の効率向上はもちろんのこと、ユーザーの生産性も飛躍的に向上します。

Windows 10 Mobile のセキュリティ機能の詳細については、
<https://www.microsoft.com/business/mobile> でご確認いただけます。

⁸ Windows Hello には、顔認識または虹彩スキャン用の特殊な照明付赤外線カメラか Window 生体認証フレームワーク対応の指紋リーダーが必要です。