Windows 10

Windows 10 Mobile

モバイル ファーストの世界を支える多層セキュリティ

2016 年 8 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。マイクロソフトは市場の変化に対応する必要があるため、このドキュメントの内容に関する責任を問われないものとします。またマイクロソフトは記載事項について発行日後にその正確さを保証することはできません。

このドキュメントに記載された内容は情報の提供のみを目的としています。明示または黙示にかかわらず、この内容に関し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願います。著作権法による制限に関係なく、マイクロソフトの書面による許可なしに、このドキュメントの一部または全部を複製したり、検索システムに保存または登録したり、別の形式に変換したりすることは、手段、目的を問わず禁じられています。ここでいう手段とは、複写や記録など、電子的、または物理的なすべての手段を含みます。

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、またはその他の知的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的に規定されていない限り、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。

このドキュメントで使用している会社、組織、製品、ドメイン、電子メール アドレス、ロゴ、人物、場所、出来事などの名称は架空のものです。実在する会社名、団体名、商品名、ドメイン名、電子メール アドレス、ロゴ、人物、場所、出来事などとは一切関係ありません。

このドキュメントで使用している画面は模擬的に再現されたものです。一部のアプリは別途販売され、提供状況やエクスペリエンスは異なる場合があります。Windows ストアのアプリは、提供状況が異なる場合があります。一部の機能やサービスでは、Microsoft アカウント、Wi-Fi アクセス、およびデータ接続が必要となる場合があり、別途通信事業者の料金が掛かります。アプリおよびコンテンツの提供状況は異なります。Office ライセンスは別途販売され、完全な機能を使用するには Office ライセンスが必要になります。

特に記載がない限り、すべての機能は Windows 10 Mobile を入手可能なすべての国で利用できます。アジアの一部の国では、画面レイアウトが異なる場合があります。

最新のセキュリティ脅威に対抗する Windows 10 Mobile

モバイル ワーカーの増加に伴い、あらゆる規模の企業が IT 業務の見直しを進める中で、最優先課題となっているのが強力なセキュリティ対策の導入です。企業の経営陣、ビジネス パートナー、お客様のだれもが、アクセス手段に関係なく、機密データの安全性が確保されることを求めています。さらに企業では、増え続けるデータ保護関連の法令や規制を遵守するように自社のモバイル デバイスを管理しなければなりません。

残念ながら、私たちを取り巻くセキュリティ脅威は日々変化し続けており、こうしたニーズへの対応はますます難しくなっています。悪意あるコードやソーシャル エンジニアリングを用いた攻撃は、毎日のように新しい種類が生み出されています。企業データに対する不正アクセスがありとあらゆる手段で試みられ、モバイル デバイスが利用されるケースも例外ではありません。こうした攻撃からユーザーや情報を守るには、多層防御のモバイル セキュリティが必要です。

Windows 10 Mobile は、企業のセキュリティ方針を妨げることなく、ユーザーがいつでもどこからでも企業のデータにアクセスして生産的に作業できるように、複数の層から成るセキュリティ機能を提供します。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、企業の情報やリソースを保護するための厳格な要件を満たすほか、IT 部門がアクティブ化や管理を簡単に行えるので、企業ポリシーを確実に遵守できます。

Windows 10 Mobile の多層保護は、以下のカテゴリで構成されます。

- **ID 管理とアクセス制御**
  Windows 10 Mobile デバイスには、Azure Active Directory と統合した ID 管理とアクセス制御が搭載され、ユーザー認証におけるシンプルかつ強化されたセキュリティ ソリューションを通じて、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権を付与します。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]、ポリシー適用、シンプルな VPN アクセスといった機能が含まれます。

- **情報の保護**
  スマートフォン、企業クラウド、オンプレミスのデータ ストアなど、情報がどこに保管されてい

[1] 生体認証サポートは Windows Hello を通じて提供されます。Windows Hello を利用するには、顔認識や虹彩スキャンに対応した特殊な照明付き赤外線カメラ、または Windows 生体認証フレームワークをサポートしている指紋リーダーが必要です。

ても、Windows 10 Mobile を利用すれば、柔軟で効果的な保護手段を講じてデータ盗難に対抗できます。デバイスの暗号化と Information Rights Management が組み込まれており、Windows デバイス上のデータをこれまで以上に包括的に保護します。

- **マルウェア対策**
  Windows 10 Mobile デバイスでは、重要なシステム リソースやアプリを暗号化によって保護し、マルウェアによる脅威を軽減します。実績ある一連の堅牢な保護機能を連携させ、Windows デバイスのセキュリティを確保することで、ルートキット、ジェイルブレイク (脱獄)、ウイルスに感染したアプリの実行を防ぎ、オンライン フィッシングやマルウェアをブロックします。

ID 管理とアクセス制御

Windows 10 Mobile には Windows Hello と Windows Hello for Business が導入されており、企業リソースへのアクセスや企業の資格情報を簡単に保護できます。組み込みの生体認証機能を併用することで、パスワードの脆弱性にまつわるリスクを最小限に抑えながら、エンタープライズ レベルの安全性と利便性を備え、1 人ひとりに適したシンプルなユーザー エクスペリエンスを可能にします。キーや証明書ベースの認証を利用しているので、モバイル デバイスに企業の資格情報を保管する必要がなくなり、デバイスが盗まれた場合でもデータやリソースへの不正アクセスを防止できます。さらに、Windows 10 Mobileは多層防御のセキュリティ アプローチを採用しているため、可能な場合には多要素認証を利用できます。

多要素認証とシングル サインオン

Windows 10 Mobile では、安全性も生産性も損なうことなく、企業リソースに対するエンタープライズ レベルの安全なアクセスが可能になります。多要素認証が利用されていると、ハッカーにとってはソーシャル エンジニアリング攻撃やブルート フォース攻撃を使用することが難しくなります。特に、認証要素の 1 つとして生体認証が利用できるようになったことは大きなポイントです。また、生体認証[2] ではユーザーがすばやく簡単にデバイスにアクセスできるので、生産性が損なわれないというメリットもあります。

Windows 10 Mobile デバイスの強力な認証機能によって、企業は簡単にアクセス権を制御した

[2] 生体認証サポートは Windows Hello を通じて提供されます。Windows Hello を利用するには、顔認識や虹彩スキャンに対応した特殊な照明付き赤外線カメラ、または Windows 生体認証フレームワークをサポートしている指紋リーダーが必要です。

り、未承認ユーザーをブロックしたり、企業リソースに効率的に接続できるようになります。ユーザーは、自身の資格情報、たとえば虹彩スキャン[3] などの情報を入力することで、業務に必要な情報やアプリにシングル サインオンでアクセスできます。

さらに、Windows Hello for Business を利用すれば、Windows 10 PC にサインインするときに、Windows 10 Mobile デバイスをリモート資格情報として利用することも可能です。このサインイン プロセスでは、Windows 10 PC が Bluetooth を使用してユーザーの Windows 10 Mobile スマートフォンに接続し、スマートフォン上の Windows Hello for Business にアクセスします。ユーザーはスマートフォンを常に携帯しているので、多要素認証を全社的に導入する場合に Windows Hello for Business を利用すると他のソリューションよりもコストを抑えながらスムーズに導入できます。

生体認証サポート

Windows Hello[3] は、Windows 10 で新たに導入された生体認証によるサインイン オプションです。顔、指紋、虹彩の認証機能を利用してデバイスのロックを解除できます。ユーザーを一意に識別する生体認証識別子を使用して認証できるので、複雑なパスワードを記憶したり書き留めたりする必要がなくなります。

生体認証は、Windows 10 Mobile デバイスのセキュリティ コンポーネントに統合された機能であり、後付けされたものではありません。また、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ローミングされたり、クラウド上で一元的に保管されたりすることはありません。センサーが読み取った生体認証イメージはアルゴリズム形式に変換され、元のイメージは破棄されて復元できなくなります。そのため、あるデバイスから生体認証イメージを盗み出し、別のデバイスを使用して企業リソースに不正にアクセスすることは不可能です。また、スプーフィング対策が組み込まれているので、ユーザーの目の写真などを利用してもデバイスにアクセスすることはできません。

さらなる保護機能として、カメラが故障した状態でユーザーがデバイスのロックを解除しようとすると、生体認証スキャンに加え PIN の入力が求められます。PIN もデバイスのセキュリティ コンポーネントによって同様に保護され、デバイスごとに設定されます。

---

[3] 生体認証サポートは Windows Hello を通じて提供されます。Windows Hello を利用するには、顔認識や虹彩スキャンに対応した特殊な照明付き赤外線カメラ、または Windows 生体認証フレームワークをサポートしている指紋リーダーが必要です。

リソース利用のための安全でシンプルな認証

Windows 10 で導入された Windows Hello for Business は、非対称キー暗号化を用いてユーザー認証を行った後、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権をユーザーに付与します。これは、証明書ベースの認証にスマート カードを利用したり、スマートフォンでネットワークを検証したりといった、これまで使用されてきた実績あるテクノロジと類似したものです。盗難され、どこでも使用されるおそれのあるパスワードとは異なり、Windows Hello for Business のキーはトラステッド プラットフォーム モジュール (TPM) を使用してデバイス上で生成され、デバイスにバインドされます。そのため、攻撃者はデバイスを盗み出したとしても、何らかの方法でユーザーの指紋や虹彩、顔を模したものを作成しなければ、盗んだデバイスのロックを解除して企業リソースにアクセスすることはできません。

Windows Hello for Business は、Azure Active Directory に対してユーザー認証を行い、使用を承認された企業アプリケーション、システム、データへのアクセス権をユーザーに付与します。さらに、Azure Active Directory を利用することで、2,500 を超えるオンライン アプリへのシングル サインオンも可能です。シングル サインオンを利用すれば、ユーザーは一度ログインするだけで SharePoint のチーム サイト、DropBox、salesforce.com、さらには社内の基幹業務 (LOB) アプリケーションにもアクセスできます。

VPN

企業ネットワークにモバイルで接続できるようにすることは、モバイル ワーカーを抱える企業にとって必要不可欠です。Windows 10 Mobile を利用すると、ユーザーは組み込みの VPN プラットフォームを通じて、社内システム、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、顧客企業のニーズに応じてプラットフォームを簡単に拡張、構築することが可能です。Cisco、Pulse Secure、F5、SonicWALL、Check Point、MobileIron など、数多くのベンダーが Windows 10 向けのアプリを作成し、Windows ストアからダウンロードできるように公開しています。

Windows 10 Mobile では VPN の常時接続を利用できるので、IT 部門はユーザーが Windows Hello for Business の資格情報を使用してスマートフォンやタブレットのロックを解除すると VPN に自動接続するように設定できます。さらに、IT 部門はアプリ単位の VPN 機能を使用して Windows 10 Mobile デバイス上のどのアプリを企業リソースに接続できるようにするかを定義することも可能です。たとえば、ユーザーがスマートフォンで社内用の LOB アプリを選択した場合に LOB アプリが「VPN A」のプロファイルのみを使用して接続するように指定する一方で、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にはスマートフォンが「VPN B」のプロファイルのみを用いて接続するように指定することができます (図 1 を参照)。

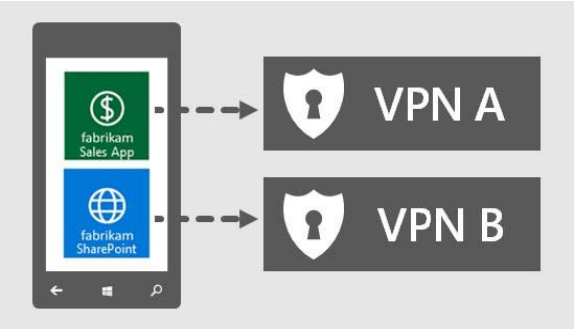


図 1: IT 部門は、アプリがどの VPN を介して接続するかを定義できます

これらの VPN 接続はすべてバックグラウンドで自動的に制御されるので、遅延が生じることも追加のパスワード入力を求められることもなく、すぐに作業を開始できます。VPN では多要素認証やシングル サインオンがサポートされるため、オンプレミスの企業リソースにも安全にアクセスできます。さらに IT 部門では、管理対象外のアプリケーションが VPN 接続を介して企業リソースにアクセスすることを禁止して、データの漏えいを防止できます。

デバイス アクセス ポリシー

Windows 10 Mobile を搭載したスマートフォンやタブレットは、常に IT 部門の管理の下にあり、モバイル デバイス管理 (MDM) ポリシーや Exchange ActiveSync (EAS) ポリシーの適用を通じてデバイス アクセスが保護されます。生体認証用のセンサーが搭載されていないデバイスでは、PIN または英数字のパスワードの使用を強制できると共に、パスワードの長さや複雑さなどの要件を設定できます。Windows Hello[4] は MDM を使用して直接管理することも可能です。

情報の保護

Windows 10 Mobile では、ID やアクセスの保護に加えて、保管中および転送中の企業データを保護す

[4] Windows Hello を利用するには、顔認識や虹彩認識に対応した特殊な照明付き赤外線カメラ、または Windows 生体認証フレームワークをサポートしている指紋リーダーが必要です。

るためにもさまざまな手段が用意されています。アプリがデバイス上に保管する情報は、業界最先端の暗号化機能によって盗難から保護されます。従業員や顧客の間でやり取りされる情報については、追加のデータ漏えい防止テクノロジを搭載して、承認されたユーザー以外は企業データにアクセスできないように制限しています。

企業が正常に事業運営を継続するうえで、知的財産やクライアント データの保護は不可欠ですが、こうした保護機能によって従業員の生産性が損なわれたり、新しいモバイル アプリの開発時に余分なコストや時間が掛かったりすることは企業にとって望ましくありません。Windows 10 Mobile にはデータを分離する保護機能が組み込まれており、ユーザーの業務を妨げることなく、個人の情報と企業の情報を明確に切り離せます。ユーザーが企業の情報にアクセスする際、フォルダーやコンテナー間を移動するという面倒な操作は必要ありません。データ保護テクノロジはモバイル プラットフォームにネイティブに組み込まれており、企業のシステムやアプリから取得したデータは自動的に暗号化されます。こうした処理は、MDM を通じて適用可能なポリシーで補完されるので、企業はリスクに晒されているデータをどのように保管し共有するかを管理できます。

デバイスの暗号化

Windows 10 Mobile では BitLocker テクノロジを使用して、オペレーティング システム パーティションやデータ ストレージ パーティションを含む内部ストレージ全体を暗号化します。デバイスの暗号化をユーザーが直接アクティブ化することはもちろん、IT 部門が会社の管理対象デバイスの暗号化をアクティブ化したり強制的に適用したりすることも可能です。デバイスの暗号化を有効にすると、スマートフォンに保管されているすべてのデータが自動で暗号化されます。保護された Windows 10 Mobile デバイスを紛失したり盗まれたりしても、デバイス ロック機能とデータ暗号化機能を併用していれば、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のはきわめて困難です。

Windows Information Protection

スマートフォンやタブレットは個人目的と業務目的の両方で使用されることが多いので、IT 部門がデータ漏えい防止ポリシーを適用しようとしても一筋縄ではいきません。企業は、個人用の電子メール、ソーシャル メディア、クラウド ベースのアプリを通じて未承認のユーザーに企業データが開示されるようなケースを確実に防ぎたいと考えています。しかし、スマートフォンを完全にロックダウンすることが必ずしも適切とは限りません。ある機能は企業データに対して使用することが禁じられているものの、個人的には利用してもかまわないという場合もあるからです。たとえば、個人用の Dropbox に業務資料を保存するのは好ましくありませんが、休暇の写真を保存するのはまったく問題ないといったケースです。

企業データと個人データを切り離しておくための方法としては、デバイス上にコンテナーを作成し、業務関係の作業を行う際には必ずそこにログインするというやり方が一般的です。コンテナー内のあらゆるデータが企業のデータ共有ポリシーで管理されるので、データがコンテナー外部に持ち出されることはありません。しかし、デバイスで仕事を進めようとするたびに、コンテナーへのログインとログアウトが必要になるため、手間が増え、生産性が損なわれるおそれがあります。

スクリーンショット 1: WIP で保護されたアプリには、データ保護を表すアイコンが表示されます

Windows 10 Mobile では、Windows Information Protection (WIP) を活用した異なるアプローチを採用しています。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ので、シームレスなエクスペリエンスが実現され、ユーザーは単一の環境で作業できるようになります。WIP によってポリシーが自動で適用され、企業のシステムやアプリから取得したファイルやデータが自動で暗号化されるため、企業リソースにアクセスするたびに隔離されたコンテナーにログインする必要はありません (スクリーンショット 1 を参照)。

たとえば、Excel が添付された電子メールを企業用の Office 365 の受信トレイで受信した場合、Windows 10 Mobile デバイスはその中身を企業データだと自動で判断し、暗号化した状態でデバイスに保管します。企業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から情報をコピーして Word ドキュメントにペーストし、そのドキュメントを OneDrive for Business に保存することは可能ですが、添付ファイルの情報を個人のアプリにコピーしたり、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 アカウントに保存したりといったことはできません (図 2 を参照)。

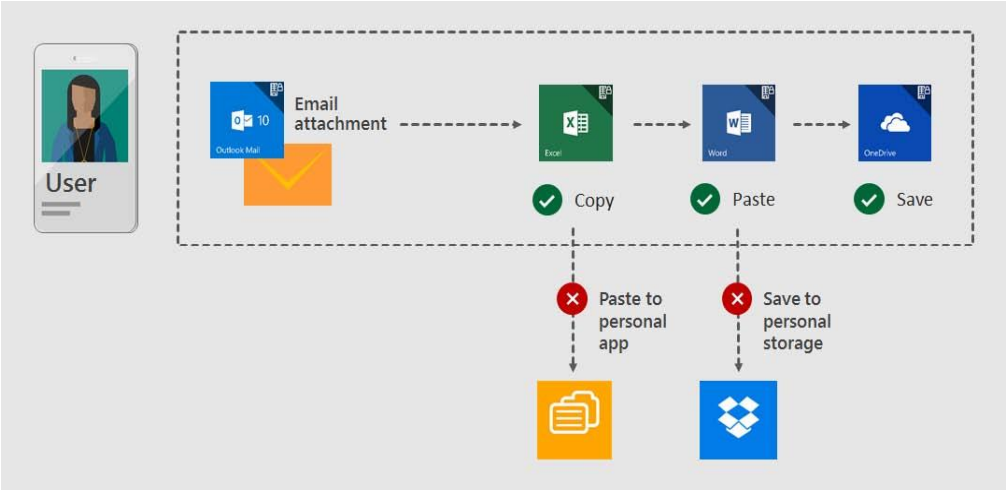
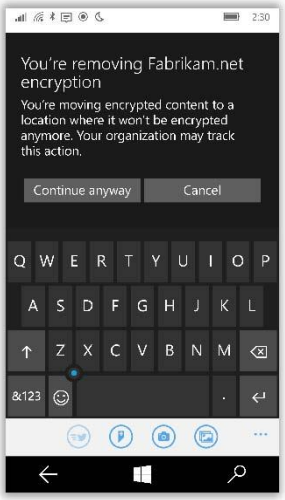


図 2: 企業が設定した保護レベルによって個人のアプリやストレージとの共有がブロックされている場合、暗号化されたデータがどのように保護されるかを例示しています

追跡の適用

企業は WIP を利用して不適切なデータ共有のブロックや監査を行えます。ユーザーは制限を無視することもできますが、その際には、ユーザーの行為がポリシー違反に当たること、その行為がログとして記録されることを通知する警告が表示されます (スクリーンショット 2 を参照)。また、ドキュメントを新規作成した場合、ユーザーは対応アプリ (次のセクションを参照) 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可能です。ただし、新規ドキュメントを個人用として分類すると、企業のドキュメント内の情報をコピーして貼り付けることはできません。分類に関する操作は、後から確認できるようにログとして記録されます。



スクリーンショット 2: データ保護ポリシーに違反すると、警告が表示されます

アプリケーション データの安全性の確保

WIP では、社内使用限定として指定されたアプリを「信頼された」アプリに分類し、適用する保護レベルを判断します。信頼された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。また、WIP によって、こうしたアプリが信頼された場所に格納されているデータにアクセスしたり、信頼された場所にデータを保管したりすることが許可されます。このようなアプローチを取ることで、アプリケーションをコンテナー内で実行しているときと同様に処理しながら、デバイス上の隔離された領域へのログイン、ログアウトを繰り返す必要がなくなります。さらに、アプリケーション開発時のコード変更やアプリ ラッパーの作成が不要になるので、開発に掛かる時間とコストを大幅に節減できます。

対応アプリとは、個人使用と業務使用の両方に対応したアプリを指します。WIP が定める制限を認識し、データの取得先に応じて、企業データは暗号化しますが、個人データは暗号化しません。たとえば、対応アプリである Outlook メールは企業のメールと個人のメールの両方に利用できますが、企業のメールを個人のメールの受信トレイにコピーすることはできません。Outlook は、企業の Exchange Server[5] や Office 365 の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が、Yahoo アカウントから受信した個人のメールは暗号化しません。

信頼されたアプリの一覧に登録されていないアプリは、WIP の保護機能の対象外となります。また、これらのアプリはデバイス上や共有上に保管された企業の情報にアクセスすることも、その他の企業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安全性の確保

WIP では、オンプレミスやクラウド上の場所、データ ストア、ネットワークなど、どこを信頼された場所と見なすかを管理者が定義できます。信頼された場所に保存されたデータやドキュメントは暗号化されず、他の承認された企業ユーザーがアクセスできるようになっています。IT 部門は、ネットワーク内のコンピューターの中から企業用の IP アドレス範囲やドメイン リストを設定できます。こうした信頼された場所から取得するデータは企業に帰属するものと見なされ、承認済みの資格情報を持つ企業ユーザーであればだれでもアクセス可能となります。そのため、暗号化が適用されるのは、ユーザーがデータをモバイル デバイス上に保管したとき、または信頼されていない場所に移動するときだけです。個人用 DropBox などの信頼されていない場所では、あらゆる企業データが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、そのユーザーしかアクセスすることができません。

暗号化キーと WIP の制限は常に MDM システムによって管理されているので、企業はデータを完全に制御でき、ユーザーが信頼されていない場所に保管したデータの暗号化を解除することもできます。

セレクティブ ワイプとフル ワイプ

管理者は WIP を利用することで、個人データはそのまま残しながら、管理対象デバイス上から企業データだけをリモートで消去できます。社員が退職するときや、新しい業務用デバイスを購入

[5] Windows 10 Mobile は Exchange Server 2010 およびそれ以降のバージョンと互換性があります。

したときでも、以前のデバイスを個人用途で使い続けられるので便利です。

Windows 10 Mobile には、デバイスを紛失しても探し出せるように、ロック、呼び出し、検索をリモートで行う機能も組み込まれています。紛失したスマートフォンや盗難に遭ったスマートフォンの所在を特定するには、Web ベースのツールを使用してリモートでデバイスをロックしたり、デバイスの場所を地図上に表示したり、スマートフォンの呼び出し音がオフになっていても大きな音量で鳴らすことができます。これらの操作は IT 部門が MDM システムを使用してユーザーの代わりに実行することも可能です。また、盗難防止機能を利用して、デバイスのリセットを阻止できます。なお、紛失または盗難が報告された後でスマートフォンやタブレットが発見された場合、ロックを解除する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 Cloud テクノロジの 1 つであり、Microsoft Enterprise Mobility Suite (英語) に含まれます。コンテンツ作成者はこの機能を利用して、ユーザーが他のユーザーに送信する Microsoft Office ドキュメント、PDF、電子メール メッセージにアクセス権を割り当てられます。IT 部門や承認済みユーザーは、ドキュメントや電子メール メッセージ内のデータを暗号化し、その暗号化されたコンテンツに承認済みのユーザーだけが特定の権限を通じてアクセスできるように指定することができます。こうした権限を利用して、ドキュメントに対して読み取り専用アクセス権を適用したり、ドキュメントやメッセージ内でのコピーやペーストを防止したり、ドキュメントやメッセージの印刷をブロックしたりできます。RMS では、電子メール メッセージの転送を防止したり、転送を許可する範囲を社内に限定したりすることも可能です。

RMS を利用すれば、全社的なデータ セキュリティの向上につながると同時に、企業データを社内外で保護するための広範な手段が利用できるようになります。Windows 10 Mobile デバイスは、RMS をネイティブにサポートしている点で他とは一線を画しており、ユーザーは RMS で保護された電子メールを制約なくやり取りし、RMS で保護されたドキュメントにスマートフォンやタブレットでアクセスできます。一方、Windows 以外のデバイスにも、RMS によるドキュメントの安全性が幅広く提供されます。iOS や Android デバイスを使用する顧客やビジネス パートナーに、RMS を利用しなければブロックされていたドキュメントに対するアクセス権を付与できます。

マルウェア対策

マルウェア攻撃は日々、巧妙化し続けています。潤沢な資金を持つ犯罪組織は、詐欺、恐喝、知的財産のあからさまな窃盗を目的として、個人や企業の価値ある情報にアクセスしようと企てています。

モバイル デバイスの普及に伴い、そうした資産への侵入につながる攻撃対象領域も拡大しており、毎年、数十万件もの悪意あるモバイル プログラムが出回る事態となっています。企業にとっては、従業員が企業リソースにアクセスできるというメリットがあるものの、デバイス上に保管されたシステム、アプリ、データの安全性を確保しなければなりません。

Windows 10 Mobile では、デバイスやアプリの整合性に影響を及ぼす脅威への対応策が組み込まれています (図 3 を参照)。起動プロセスの改ざん防止には、ハードウェア ベースの保護機能が用意されています。また、署名済みの信頼されたアプリだけを実行可能にして、オンラインのマルウェアやフィッシングをブロックすることで、デバイス プラットフォームやアプリの安全性をさらに高めています。こうしたデバイス レベルのセキュリティ対策を講じることで、顧客の信頼を失ったり、ビジネス チャンスの逸失や訴訟によって多額の損失にもつながりかねない重大なセキュリティ侵犯を防止できます。

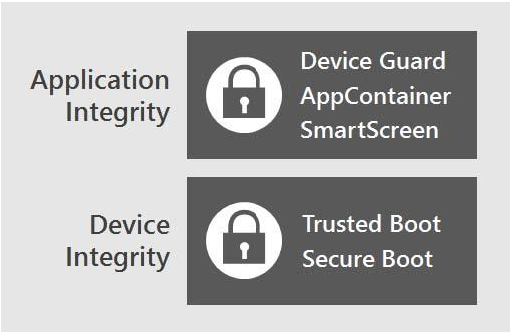


図 3: Windows 10 Mobile プラットフォームのセキュリティ アーキテクチャ

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 テクノロジが搭載されています。このアプローチによって、すべてのブート コンポーネントに、検証されたデジタル署名が付加されます。承認済みのコードだけを使用してデバイスの初期化と Windows オペレーティング システムの読み込みが実行されることになるので、デバイスのハードウェアやファームウェアからオペレーティング システム (OS) に至るまで、信頼の連鎖によって基本となる関係が確立されます。

この最初のセキュリティ チェックが完了し、続くトラスト ブートによって OS のブート プロセスが完了すると、ユーザーがスマートフォンを使用できる状態になります。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 システム内の全コードにマ

イクロソフトの署名が必要になるので、プラットフォームの整合性を確保するためのさらなる防御層が追加されます。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、適切に署名されていなければ実行することはできません。

Device Guard

Windows 10 Mobile には、感染したアプリケーションを通じてデバイスにマルウェアが侵入するのを防ぐための保護機能が備わっています。複数の保護機能を連携させることで、ユーザーは信頼されたアプリケーションだけにアクセスできるようになり、デバイスで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て、マイクロソフト、Windows ストア、またはポリシーを通じて企業が定義したその他の信頼されたソースによって署名されたアプリだけを実行するように制限します。OS は、ウイルス対策などのセキュリティ ソリューションでブロックされなければその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だけを信頼します。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ディングされたりした場合、Device Guard によってそのアプリの実行が阻止されるので、システム、アプリ、データに対するセキュリティ リスクが回避されます。

アプリケーションのサンドボックス化

Windows 10 Mobile では AppContainer を利用することで、各アプリケーションが専用のサンドボックス内でアクセス権を最小限に抑えて実行されるようになっています。これにより、悪意あるアプリがアクセス権を不正に昇格させてデバイス上のシステム、アプリ、データにアクセスしようとするのを阻止できると共に、ビジネス アプリ用の信頼できるコンテナーが提供されます。アプリのサンドボックス化により、意図しないアプリの競合も減らせるので、より信頼性の高いユーザー エクスペリエンスが提供できます。

アプリケーション アクセスの安全性の確保

企業は Windows ストアや企業ポータルを通じてユーザーにモバイル アプリに対するアクセス権を提供できます。スマートフォンに配信されたアプリは、その配信方法を問わず、Windows 10 Mobile デバイス上での実行に必要なセキュリティ制限を満たしていなければなりません。Windows ストア アプリには、改ざんされていないことを保証するマイクロソフトの署名が付加されています。LOB アプリも、ユーザーが所属する組織によって署名されていなければ実行でいません。そのためには、IT 部門がビジネス向け Windows ストアに LOB アプリをアップロード

して、登録済みのユーザー デバイスだけに提供するようにします。こうしたアプリは登録されていないユーザーやデバイスに表示されることはありません。また、企業で MDM システムを通じてアプリを配信し、企業の証明書による署名を付加することもできます。

ブラウザー ベースの保護

Microsoft Edge の SmartScreen フィルターでは、Windows 10 Mobile デバイス上でユーザーが訪問したサイトの評価をチェックすることで、フィッシング サイトからユーザーを保護します。疑わしいサイトだと判断されると、SmartScreen によってアクセスが完全にブロックされます。また、SmartScreen では、ユーザーを騙してソーシャル エンジニアリング型マルウェアをダウンロードさせ、デバイスのセキュリティを侵害しようとするサイトからもユーザーを保護します。
Microsoft Edge のコンテンツ プロセスはすべて、AppContainer 内で実行されます。
AppContainer は、悪意ある実行ファイルがデバイスにアクセスすることを確実に防ぐように設計されています。また、MDM の制限によってブラウザーも管理でき、アクセス可能なサイトを制限したり、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といったことも可能です。

まとめ

Windows 10 Mobile は、強力で透明性の高い多層防御のアプローチを採用し、あらゆる組織や企業のニーズに適したレベルでスマートフォンやタブレットを保護します。ID 管理とアクセス制御、情報の保護、マルウェア対策といった分野で大幅な機能強化が施されており、ユーザーと企業の双方にメリットをもたらします。ユーザーは、データのセキュリティ リスクを心配することなく、より簡単、便利にデバイス、アプリ、オンライン リソースにアクセスできます。企業のアプリやデータをデバイスでどう扱えるようにするかを IT 部門がこれまで以上に細かく制御できるので、企業は安心して個人デバイス用 (BYOD) のプログラムや企業デバイス用のプログラムを職場に導入することができます。

Windows 10 Mobile が備えたエンタープライズ レベルのセキュリティ機能は、簡単に導入できるだけでなく、コストの削減にも貢献します。多要素認証を全社的に導入する場合に Windows Hello[6] と Windows Hello for Business を利用すれば、コストを抑えながらきわめてスムーズに導入できます。Windows Information Protection (WIP) では企業データを自動的に暗号化できるほか、安全性の高いモバイル アプリを簡単に開発できるようにもなります。さらに、マルウェア対策がデバイスとアプリケーションに組み込まれており、攻撃による被害を回避できるようにユーザーを保護します。Windows 10 Mobile を搭載したスマートフォンやタブレットでエンタープライズ レベルのセキュリティが簡単に利用できるので、IT 部門の効率が高まるだけでなく、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/ja-jp/WindowsForBusiness/windows-for-mobile をご覧ください。

---

[6] Windows Hello を利用するには、顔認識や虹彩認識に対応した特殊な照明付き赤外線カメラ、または Windows 生体認証フレームワークをサポートしている指紋リーダーが必要です。