Windows 10

Windows 10 Mobile

セキュリティ ガイド

2016 年 7 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、マイクロソフトは発行日以降に発表される情報の正確性を保証できません。

このホワイト ペーパーは情報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。

このドキュメントで例として使用されている会社、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。提供状況とエクスペリエンスはアプリによって異なります。アプリは Windows ストアで提供されているものです。提供状況は変動する場合があります。一部の機能とサービスでは、Microsoft アカウント、Wi-Fi アクセス、およびデータ接続が必要です。別途、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 ライセンスは別売です。すべての機能を利用するには別途購入する必要があります。

Windows Information Protection (WIP) は、2016 年半ばに一般提供される予定です。

Windows Hello で生体認証を使用するには、指紋リーダー、照明付き赤外線センサー、その他の生体認証センサーを含む、専用のハードウェアが必要です。Windows Hello の資格情報またはキーをハードウェア ベースで保護するには、TPM 1.2 以上が必要です。TPM が存在しない、または構成されていない場合、資格情報およびキーの保護はソフトウェア ベースで行われます。Windows Hello のコンパニオン デバイスは、Bluetooth で Windows 10 PC とペアリングする必要があります。Windows Hello の資格情報のローミングに対応した Windows Hello コンパニオン デバイスを使用するには、Windows 10 PC の Pro または Enterprise エディションにサインインする必要があります。

Windows デバイス正常性構成証明サービスは、モバイル デバイス管理ソリューション (Microsoft Intune など) やその他の種類の管理システム (SCCM など) で実現される条件付きアクセスのシナリオで使用できます。

別途記載されている場合を除き、Windows 10 Mobile が提供されている国においては、すべての機能をご利用いただけます。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。

改訂履歴

本ガイドの PDF 版をお読みの場合は、http://aka.ms/W10Mobile-SecurityGuide で最新版をご確認ください。

2015 年 11 月	Windows 10 Mobile (バージョン 1511) に関する更新
2016 年 7 月	Windows 10 Mobile Anniversary Update (バージョン 1607) に関する更新

スマートフォンは現在、デスクトップ PC やノート PC と同じく、ビジネス ワーカーにとってきわめて重要な生産性向上ツールとしての役割を担っており、マルウェアの攻撃やデータの盗難を防止できるようにセキュリティで保護する必要があります。こうしたデバイスは、オペレーティング システムや構成が多岐にわたり、また多くの従業員が個人所有のデバイスを利用しているため、保護することは容易ではありません。IT 管理者は、すべてのデバイス上にある企業の資産をセキュリティで保護する必要がありますが、一方でユーザーの個人的なアプリやデータのプライバシーも守る必要があります。

Windows 10 Mobile は、従業員が個人所有デバイスと企業所有デバイスのどちらを使用しているかにかかわらず、このようなセキュリティ上の問題に直接対処できます。Windows 10 オペレーティング システムと同じセキュリティ テクノロジを採用しているため、さまざまな経路で発生するセキュリティ上の既知の脅威や新たな脅威から、企業とユーザーのデータを保護することができます。使用しているテクノロジには、次のようなものがあります。

- **Windows Hello。**強化された ID 管理とアクセス制御の機能により、承認済みのユーザーのみが企業のデータとリソースにアクセスできます。Windows Hello では、PIN、コンパニオン デバイス、生体認証といった認証手法が提供されるため、多要素認証 (MFA) を簡単に展開して使用できます。
- **Windows Information Protection。**自動でデータが分離され、企業の情報が個人のデータやアプリに共有されてしまう事態を回避できます。
- **マルウェア対策。**デバイスのハードウェア、起動プロセス、アプリ プラットフォームに組み込まれた多層の保護機能により、従業員のデバイスを侵害する可能性のあるマルウェアの脅威を軽減できます。

本ガイドでは、未承認のアクセス、データ漏えい、マルウェアに対する保護を強化する Windows 10 Mobile のセキュリティ機能について、IT 管理者向けに詳しく説明します。

この記事では次のトピックを扱います。

- Windows Hello
- Windows Information Protection
- マルウェア対策

Windows Hello

Windows 10 Mobile には、シンプルながらも強力な多要素認証ソリューションである Windows Hello が含まれており、企業の機密情報やリソースへのアクセスをユーザーに許可する前に、そのユーザーの ID を確認することができます。多要素認証は、パスワード ベースのデバイス セキュリティに代わる、より安全性に優れた認証方法です。ユーザーは長く複雑なパスワードの入力を嫌い、特にモバイル デバイスのタッチ スクリーンでその傾向が強くなりますが、一方で企業のポリシーでは、パスワードを頻繁に変更することが必要とされています。このような状況は、パスワードを再使用する、紙にメモする、脆弱なパスワードを作成するといったユーザーの行動を誘発し、セキュリティ対策の品質低下につながります。

Windows Hello を利用すると、簡単かつコスト効率に優れた方法で、組織全体に多要素認証を展開することができます。スマート カードとは異なり、公開キー基盤の展開や追加ハードウェアの実装は必要ありません。従業員は PIN、コンパニオン デバイス (Microsoft Band など)、または生体認証を使用して自分の ID を検証することで、Azure Active Directory (Azure AD) に登録した Windows 10 Mobile デバイス上にある企業のリソースにアクセスできるようになります。

Windows Hello はすべての Windows 10 デバイスでサポートされているため、多要素認証を組織内の環境全体にわたって一律に導入できます。Windows Hello を Windows 10 Mobile デバイスに展開するには Azure AD (別売) が必要ですが、Azure AD Connect を使用すると、オンプレミスの Active Directory サービスと同期できるようになります。

Windows Hello では、生体認証センサーを備えたデバイス向けに、虹彩スキャン、指紋認識、顔認識をベースにした認証をサポートしています。

> **メモ**
>
> 初回リリース時の Windows 10 には **Microsoft Passport** と **Windows Hello** が搭載され、これらが連携することで多要素認証を提供していました。マイクロソフトでは、展開方法を簡素化してサポート性を高めるために、2 つのテクノロジを **Windows Hello** の名称で 1 つのソリューションに統合しました。既にこれらのテクノロジを展開している場合、機能面での変更はありません。Windows Hello をまだ試したことがないお客様にとっては、ポリシー、ドキュメント、セマンティクスがシンプルになったことで、より展開しやすくなっています。

セキュリティで保護された資格情報

Windows Hello を利用することで、ログイン用のパスワードが不要になり、攻撃者にユーザーの資格情報を盗まれて再使用されるリスクが低減します。Windows 10 Mobile デバイスは、高度なセキュリティ機能を実現するマイクロチップである、トラステッド プラットフォーム モジュール (TPM) を備えていることが要件となっています。TPM は暗号化キーを作成し、TPM 独自のストレージ ルート キーで「ラップ」します。このキーは、資格情報の流出を防ぐために TPM の内部に保存されます。TPM によって作成された暗号化キーは、同じ TPM によってのみ暗号化を解除できます。このしくみにより、取得と再使用をねらう攻撃者からキー マテリアルが保護されます。

攻撃者が Windows Hello 資格情報を侵害するためには、物理デバイスにアクセスした後、ユーザーの生体認証 ID を偽装するかユーザーの PIN を推定する方法を見つける必要があります。また、これらはすべて、TPM のブルートフォース対策機能がモバイル デバイスをロックするか、盗難に対する保護メカニズムが起動するか、ユーザーまたは企業内管理者によりデバイスがリモートで消去される前に実行しなければなりません。TPM ベースの保護を通じて、攻撃者がユーザーの資格情報を侵害できる可能性は大幅に低下します。

生体認証のサポート

生体認証を利用すると、資格情報の盗難を防止できるほか、ユーザーが自分のデバイスに簡単にログインできるようになります。ユーザーの生体認証 ID は常にユーザー自身の一部であるため、思い出せなくなったり、紛失したり、置き忘れたりすることがありません。攻撃者が企業のリソースにアクセスするには、ユーザーのデバイスにアクセスするだけでなく、ユーザーの生体認証 ID を偽装する必要があり、これはパスワードを盗み出すことよりもはるかに困難です。

Windows Hello では、生体認証センサーについて次の 3 つのシナリオをサポートしています。

- **顔認識:** 特殊な赤外線カメラを使用して写真やスキャン画像と実際の人物の違いを確実に識別します。複数のベンダーが、このテクノロジを組み込んだ外付けカメラの発売を予定しており、主要なメーカーは顔認識テクノロジを内蔵したノート PC を既に出荷しています。Surface Pro 4 と Surface Book は、どちらもこのテクノロジをサポートしています。
- **指紋認識:** センサーを使用してユーザーの指紋をスキャンします。指紋リーダーは、Windows オペレーティング システムを搭載するコンピューターで数年前から利用されていますが、Windows 10 の検出、スプーフィング対策、認識アルゴリズムは以前のバージョンの Windows よりも強化されています。Windows 生体認証フレームワークをサポートしている既存の指紋リーダーのほとんどは、(外付け型か、ノート PC や USB キーボードへの内蔵型かに関係なく) Windows Hello でも動作します。
- **虹彩スキャン:** 特別なカメラを使用して、ユーザーの虹彩をスキャンします。虹彩とは眼球の器官であり、色鮮やかで複雑な模様が付いています。高精度のデータが必要になるため、虹彩スキャンでは赤外線光源と高品質カメラを組み合わせて使用しています。Microsoft Lumia 950 および 950 XL の各デバイスでは、このテクノロジをサポートしています。

ユーザーは、生体認証ジェスチャの登録時にロック解除 PIN を作成する必要があります。この PIN は、デバイスで生体認証ジェスチャを取得できない場合に、フォールバック メカニズムとして使用します。

生体認証のこれら 3 つの要素 (顔、指紋、虹彩) は、いずれも個人個人で異なります。生体認証スキャナーでは、個人を一意に識別するのに十分なデータを取得するために、最初は複数の条件で画像を取得したり、追加情報を伴う画像を取得したりする場合があります。たとえば虹彩スキャナーでは、左右両方の目の画像、または眼鏡やコンタクト レンズを着用したときと着用しないときの目の画像を取得します。

企業環境では生体認証データのスプーフィングが重大な問題になることが多々あります。Windows 10 Mobile には、生体認証デバイスの信頼性を検証すると共に、保存されている生体認証の測定データとの意図的な衝突を防ぐ、いくつかのスプーフィング対策手法が採用されています。これらの手法により、MFA の全体的な操作性と管理性を維持しながら、他人受入率 (なりすましの生体認証データが本人のデータとして承認される確率) を改善することができます。

登録時に収集された生体認証画像は、アルゴリズム形式に変換されるため、元の画像に戻すことができません。アルゴリズム形式のデータだけが保持され、実際の生体認証画像は変換後にデバイスから削除されます。Windows 10 Mobile デバイスは、アルゴリズム形式の生体認証データを暗号化すると共に、暗号化したデータをデバイスにバインドします。この両方の操作により、他者がそのデバイスからデータを削除するのを防ぐことができます。このため、Windows Hello で使用される生体認証情報はローカルのジェスチャとなり、ユーザーのデバイス間を移動することはありません。

コンパニオン デバイス

Windows Hello コンパニオン デバイスは、ユーザーに対してその資格情報へのアクセス許可を付与する前に、そのユーザーの ID を検証するための要素としてウェアラブル デバイスなどの物理デバイスを利用できるようにする機能です。たとえば、ユーザーがコンパニオン デバイスを物理的に所持しているときは、PC のロックを簡単に、また場合によっては自動的に解除し、アプリや Web サイトでの認証を行うことができます。この種のデバイスは、生体認証センサーを内蔵していないスマートフォンやタブレットのロック解除に役立ちます。また、小売業など、ユーザーがすばやく便利にサインインできる機能を必要とする業種にも有用です。

状況によっては、Windows Hello のコンパニオン デバイスを利用すると、スマートフォンやウェアラブル デバイスなどの物理デバイスにユーザーの資格情報をすべて保存できます。モバイル デバイスに資格情報を保存することで、キオスクや家庭の PC などの対応デバイスでそれらの資格情報を使用できるようになり、各デバイスに Windows Hello を登録する必要がなくなります。また、コンパニオン デバイスは、組織が連邦情報処理標準 (FIPS) パブリケーション 140-2 (FIPS 140-2) などの規制要件を満たすためにも利用できます。

標準に基づくアプローチ

Fast Identity Online (FIDO) Alliance は、強力な認証デバイス間での相互運用性の不足や、ユーザーが複数のユーザー名とパスワードを作成および記憶するうえで直面する問題を解消するべく取り組んでいる非営利団体です。FIDO 標準によって、すべてのビジネス ネットワーク、アプリ、Web サイト、クラウド アプリケーションが、既存のものから将来リリースされるものまで、さまざまな FIDO 対応のデバイスやオペレーティング システム プラットフォームと連携できるようになり、オンライン サービスのユーザー認証では、安全性を維持しながらパスワードへの依存度を低減できるようになります。

マイクロソフトは 2014 年に FIDO Alliance の理事会に加盟しました。2014 年に公開された FIDO 1.0 仕様では、パスワードレス認証 (**UAF** とも呼ばれます) と 2 要素認証 (U2F) という 2 種類の認証方式が提供されています。FIDO Alliance は現在、FIDO 1.0 標準の U2F と UAF の優れた部分を組み合わせた 2.0 仕様の提案策定に取り組んでいます。マイクロソフトでは、レビューやフィードバックを受ける目的で FIDO 2.0 仕様のワークグループに Windows Hello テクノロジを提供しており、FIDO 2.0 仕様の進展に合わせて FIDO Alliance と継続的に連携しているところです。FIDO 製品の相互運用性の高さが、FIDO 認証の有効性を実証しています。マイクロソフトは FIDO ソリューションを市場に投入することで、企業と消費者の双方にとって重要なニーズが解決できると考えています。

Windows Information Protection

企業では、個人データと企業データのストレージの統合が大幅に進んでいます。個人データが企業のデバイスに保存され、企業データが個人のデバイスに保存されることは珍しくありません。このようにデータが流動している状況では、企業の機密データが誤って漏えいする危険性も高くなります。

企業が個人所有のデバイスから企業リソースへのアクセスを認めることで、過失による情報開示が急速に増加し、機密データ漏えいの最大の原因となっています。個人所有の携帯電話で仕事用のメール アドレスを使用している従業員が、会社の機密情報が含まれた添付ファイルを意図せずに個人用のクラウド ストレージに保存し、それが承認を受けていない第三者によって共有されてしまうという状況は、容易に想像できます。このような過失による企業データの共有は、職場でモバイル デバイスを使用する場合に共通して見られる問題の一例にすぎません。この種のデータ漏えいを防ぐために、ほとんどのソリューションでは、ユーザーが個別のユーザー名とパスワードを使用して企業のアプリとデータがすべて保存されているコンテナーにログインする必要がありますが、このような操作はユーザーの生産性を低下させます。

Windows 10 Mobile は、企業データの安全性と個人データのプライバシーを透過的な方法で維持するために、Windows Information Protection を備えています。企業データは常に保護されているため、ユーザーが誤ってそれをコピーすることも、承認を受けていないユーザーやアプリと共有することもありません。主な機能として次のものがあります。

- 個人データと企業データに自動的にタグ付けする。
- ローカルまたはリムーバブル ストレージにデータが保存されている間、そのデータを保護する。
- どのアプリが企業データにアクセスできるかを制御する。
- どのアプリが仮想プライベート ネットワーク (VPN) 接続にアクセスできるかを制御する。
- 公開された場所にユーザーが企業データをコピーすることを防止する。
- デバイスがロック状態のときにはビジネス データにアクセスできないようにする。

対応アプリ

通常、サード パーティ製のデータ損失防止ソリューションでは、アプリの開発者がそのアプリをラップすることが要件とされています。これに対し Windows Information Protection では、このインテリジェンスが Windows 10 Mobile に組み込まれているため、大部分のアプリでは、企業データの不適切な共有を防ぐために追加の操作を行う必要はありません。

Windows Information Protection では、アプリが対応アプリと非対応アプリの 2 つのカテゴリに分類されます。対応アプリでは企業データと個人データが区別され、どちらを保護対象とすべきかが内部ポリシーに基づいて正確に決定されます。企業データは管理されているデバイス上で暗号化され、企業の管理対象外のアプリやユーザーにこの情報をコピー/貼り付けまたは共有することができません。非対応アプリでは、それが企業の管理対象アプリに指定されている場合、すべてのデータが企業データと見なされ、既定で全データが暗号化されます。

ユーザー エクスペリエンスの品質を低下させないために、既定で全データを暗号化することは避けたいという場合は、コードを追加して Windows Information Protection アプリケーション プログラミング インターフェイスでコンパイルすることにより、アプリを**対応させる**ことを検討する必要があります。対応させるアプリの候補として最も可能性が高いのは、次のようなアプリです。

- ファイルの保存に共通のコントロールを使用しない。
- テキスト ボックスに共通のコントロールを使用しない。

- 個人データと企業データを同時に操作する (たとえば、個人データと企業データを 1 つのビューに表示する連絡先アプリや、1 つのインスタンス内で個人および企業の Web ページをタブに表示するブラウザーなど)。

ほとんどのアプリでは、Windows Information Protection を使用するために対応化を行う必要はありません。実行すべき手順は、対象のアプリを許可リストに追加することだけです。たとえば基幹業務 (LOB) アプリは企業データのみを扱うため、この方法で問題なく機能します。

どのような場合にアプリの対応化が必須となるか

必須	推奨	不要
個人データと企業データを両方とも扱う必要があるアプリ。	企業データのみを扱うが、起動、アンインストール、更新などのためにファイル (構成ファイルなど) を変更する必要があるアプリ。このようなアプリに対する取り消し操作は、アプリを対応させないと適切に実行できません。 ロック時の保護がアクティブになっている間、企業データにアクセスする必要があるアプリ。	企業データのみを扱うアプリ。 個人データのみを扱うアプリ。

データ漏えいの制御

Windows Information Protection をサポートするモバイル デバイス管理 (MDM) ソリューションで Windows Information Protection を構成するには、承認済みのアプリを許可リストに追加します。Windows 10 Mobile を搭載したデバイスが MDM ソリューションに登録されている場合、未承認のアプリは企業データにアクセスできません。

ユーザーが、未承認のアプリや Web 上の場所から企業データにアクセスしようとしたり、企業データをそれらのアプリや場所に貼り付けようとしたりしない限り、Windows Information Protection はシームレスに機能します。たとえば、承認済みのアプリから別の承認済みのアプリに企業データをコピーする操作は通常どおりに機能しますが、承認済みのアプリから未承認のアプリに企業データをコピーしようとすると、Windows Information Protection によってブロックされます。同様に、未承認のアプリを使用して企業データが含まれているファイルを開こうとした場合もブロックされます。

承認済みのアプリからデータをコピーして未承認のアプリや Web 上の場所に貼り付ける操作がブロックされる場合、その範囲は次のどの保護レベルが設定されているかによって決まります。

- ブロック: Windows Information Protection は、ユーザーの操作が完了しないようにブロックします。
- オーバーライド: Windows Information Protection は、操作が適切でないことをユーザーに通知しますが、ユーザーはポリシーを無視できます。ただし、その操作は監査ログに記録されます。
- 監査: Windows Information Protection はユーザーの操作をブロックせず、ユーザーに通知もしませんが、監査ログには記録します。
- オフ: Windows Information Protection はユーザーの操作をブロックせず、ユーザーに通知せず、監査ログにも記録しません。

データの分離

ほとんどのサード パーティ ソリューションには、パスワードで保護されたコンテナー内に企業データを配置し、個人データをコンテナー外に配置するアプリ ラッパーが必要です。実装によっては、この操作を行うために、デバイス上で実行される 2 種類のバージョン (個人データ用と企業データ用) の同じアプリが必要になります。

Windows Information Protection でもデータの分離機能を提供しますが、コンテナーや、企業データまたは個人データにアクセスするための特別なアプリは必要ありません。また、企業データの表示や企業アプリケーションの起動に個別のログインは必要ありません。Windows Information Protection は、企業での使用のみを目的として企業データの識別と暗号化を行います。データの分離は自動かつシームレスに行われます。

暗号化

Windows 10 Mobile では、BitLocker テクノロジを基にしたデバイス暗号化を使用し、オペレーティング システムとデータ ストレージ パーティションを含むすべての内部ストレージを暗号化しています。ユーザーがデバイス暗号化をアクティブにすることも、企業で管理されるデバイスの暗号化を IT 部門が MDM ツールを通じてアクティブにし、強制的に適用することもできます。デバイス暗号化が有効になっていると、そのデバイスに保存されているすべてのデータが自動的に暗号化されます。Windows 10 Mobile デバイスで暗号化が有効になっていれば、デバイスを紛失した場合や盗まれた場合でも、保存されているデータの機密性は保護されます。Windows Hello によるロックとデータ暗号化の組み合わせにより、未承認の第三者がデバイスから機密情報を取得することは極めて困難になります。

デバイス暗号化のしくみは、企業固有のセキュリティ要件に合うようにカスタマイズできます。また、デバイス暗号化を利用することで、独自の暗号スイートを定義することも可能です。たとえば、Windows 10 Mobile でデータ暗号化に使用するアルゴリズムとキー サイズや、許可するトランスポート層セキュリティ (TLS) 暗号スイートを指定したり、連邦情報処理標準 (FIPS) ポリシーを有効化するかどうかを指定したりできます。以下の表は、Windows 10 Mobile デバイスでデバイス暗号化をカスタマイズするために変更できるポリシーを一覧にまとめたものです。

領域名	ポリシー名	説明
暗号	Allow FIPS Algorithm Policy (FIPS アルゴリズム ポリシーを許可する)	FIPS ポリシーを有効または無効にします。このポリシーを適用するには、再起動が必要です。既定では無効に設定されています。
BitLocker	暗号化方法	BitLocker ドライブ暗号化方法と暗号強度を構成します。既定値は AES-CBC 128 ビットです。指定した値がデバイスで使用できない場合は、別の値が使用されます。
暗号	TLS Cipher Suite (TLS 暗号スイート)	このポリシーには、Secure Sockets Layer 接続で使用できる暗号化の暗号アルゴリズムのリストが含まれています。

外部からの干渉に対するデバイスの安全性をさらに高めるために、現在の Windows 10 Mobile はロック時の保護機能を備えています。これにより、デバイスがロックされるたびに暗号化キーがメモリから削除されるようになります。デバイスがロック状態になっている間はアプリから機密データにアクセスできないため、ハッカーやマルウェアはキーを見つけて盗み出すことができません。ユーザーが Windows Hello でデバイスのロックを解除するまでは、TPM によってすべての機密データがしっかり守られています。

政府の認定

Windows 10 Mobile では、FIPS 140 標準 (英語) と情報セキュリティ国際評価基準 (Common Criteria) (英語) の両方に対応しています。FIPS 140 認定では、Windows 10 Mobile で使用される暗号化アルゴリズムの有効性が検証されます (詳細については、こちらのページ (英語) をご覧ください)。マイクロソフトは、Lumia 950、950 XL、550、635、および Surface Pro 4 で動作する Windows 10 Mobile について Common Criteria の認定 (英語) も取得しており、暗号化機能が適切に実装されていることが保証されているため、お客様には安心してご利用いただけます。

マルウェア対策

マルウェアへの対抗手段として最も有効なのは、感染を防止することです。Windows 10 Mobile には、セキュリティで保護されたハードウェア、スタートアップ プロセスの防御機能、コア オペレーティング システム アーキテクチャ、アプリケーション レベルの保護による強力なマルウェア対策が用意されています。

以下の表に、特定のマルウェアの脅威に対する Windows 10 Mobile の軽減策を示します。

脅威	**Windows 10 Mobile の軽減策**
ファームウェア ブートキットによりファームウェアがマルウェアに置き換えられる。	すべての認定デバイスにはセキュア ブート付きの Unified Extensible Firmware (UEFI) が搭載され、UEFI とオプション ROM を更新するには署名済みのファームウェアが必要になります。
ブートキットにより Windows の起動前にマルウェアが起動される。	Windows の起動前に悪意のあるオペレーティング システムが起動できないように、セキュア ブート付きの UEFI によって Windows ブートローダーの整合性が検証されます。
システムまたはドライバーのルートキット (通常はオペレーティング システムから隠れている悪意のあるソフトウェア) により、Windows の起動中、マルウェア対策ソリューションが起動する前にカーネル レベルのマルウェアが起動される。	Windows トラスト ブートによりマイクロソフトのドライバーを含む Windows ブート コンポーネントが検証されます。メジャー ブートがトラスト ブートと並行して実行され、デバイスの起動状態を検証するリモート サーバーに情報を提供できるため、トラスト ブートやその他のブート コンポーネントがシステムのチェックに成功したことを確認できます。
アプリから他のアプリやオペレーティング システムにマルウェアが感染する。	すべての Windows 10 Mobile アプリは、他のすべてのプロセスや機密性の高いオペレーティング システム コンポーネントから切り離されて、AppContainer 内で実行されます。アプリは AppContainer の外部のリソースにアクセスできません。
未承認のアプリまたはマルウェアがデバイス上で起動を試みる。	すべての Windows 10 Mobile アプリは、Windows ストアまたはビジネス向け Windows ストアからダウンロードされていなければなりません。実行を許可するアプリを正確に判断できるように、Device Guard によって管理ポリシーが適用されます。
ユーザー レベルのマルウェアによりシステムやアプリケーションの脆弱性が悪用され、デバイスが乗っ取られる。	ASLR (Address Space Layout Randomization)、データ実行防止 (DEP)、ヒープ アーキテクチャ、メモリ管理アルゴリズムを強化した結果、脆弱性を悪用される可能性が低下しました。 保護されたプロセスにより個々の信頼されていないプロセスが分離され、機密性の高いオペレーティング システム コンポーネントから切り離されます。
ユーザーがリスクを認識せずに危険な Web サイトにアクセスする。	SmartScreen URL 評価機能により、ブラウザーの脆弱性を悪用してデバイスを制御しようとする、悪意のある Web サイトにユーザーがアクセスするのを防止します。

脅威	Windows 10 Mobile の軽減策
マルウェアによりブラウザーのアドオンの脆弱性が悪用される。	Microsoft Edge は、ユニバーサル Windows プラットフォーム (UWP) を基盤とするアプリであり、Microsoft ActiveX や、ツール バーによく使用されるブラウザー ヘルパー オブジェクトなどの従来のバイナリ拡張機能を実行しないため、これらを悪用されるリスクがありません。
悪意のあるコードが含まれる Web サイトにより Web ブラウザーの脆弱性が悪用され、クライアント デバイスでマルウェアが実行される。	Microsoft Edge に用意されている拡張保護モードでは、AppContainer ベースのサンドボックスを使用し、ブラウザーで実行中の拡張機能 (Adobe Flash、Java など) や攻撃者に発見される可能性のあるブラウザー自体の脆弱性を悪用した攻撃からシステムを保護できます。

メモ

Windows 10 Mobile デバイスには、Qualcomm などの SoC ベンダーから提供された System on a Chip (SoC) 設計が採用されています。SoC ベンダーやデバイス メーカーは、このアーキテクチャを使用して、UEFI 以前のブートローダーと UEFI 環境を提供しています。UEFI 環境には、UEFI 仕様のセクション 27 で説明されている UEFI セキュア ブート標準が実装されています。この UEFI 仕様は、www.uefi.org/specs (英語) でご確認いただけます。この標準では、すべての UEFI ドライバーと UEFI アプリケーションが、UEFI ベースのデバイス内にプロビジョニングされたキーとの照合によって実行前に検証されるプロセスについて説明しています。

セキュア ブート付きの UEFI

Windows 10 Mobile デバイスが起動すると、デバイスはそのストレージ システム上にブートローダーを配置することで、オペレーティング システムの読み込みプロセスを開始します。セーフガードが用意されていないと、デバイスはブートローダーに対して、それが信頼されているオペレーティング システムなのかマルウェアなのかを判断せずに制御を渡す可能性があります。

UEFI は、BIOS に代わる最新型の、標準ベースのソリューションです。UEFI は BIOS と同じ機能に加え、セキュリティ機能やその他の高度な機能を備えています。BIOS と同様にデバイスを初期化しますが、セキュア ブート付きの UEFI コンポーネント (バージョン 2.3.1 以降) には、携帯電話でオプション ROM、UEFI アプリ、オペレーティング システム ブートローダー内の信頼されているファームウェアのみを起動できるようにする機能もあります。

UEFI では、ファームウェアを実行する前に、ファームウェアのデジタル署名を検証する内部整合性チェックを実行できます。有効なファームウェアの署名を作成するために必要なデジタル証明書には携帯電話のメーカーだけがアクセスできるため、Windows 10 Mobile よりも先に読み込まれてオペレーティング システムから隠れて悪意のある動作を実行しようとするファームウェア ベースのマルウェアに対する保護を提供できます。このようなファームウェア ベースのマルウェアは通常「ブートキット」と呼ばれています。

UEFI とセキュア ブートを備えたモバイル デバイスが起動すると、UEFI ファームウェアはブートローダーのデジタル署名を検証し、デジタル署名が行われた後に変更が加えられていないことを確認します。ファームウェアは、ブートローダーのデジタル署名の発行元が信頼されている機関であるかどうかも検証します。このチェックによってブートローダーが信頼されていること、署名後に変更されていないことが両方とも確認されない限り、システムが起動しません。

すべての Windows 10 Mobile デバイスでは、セキュア ブートが常に有効になっています。また、これらのデバイスで信頼されるのは Windows オペレーティング システムの署名のみです。Windows 10 Mobile やアプリはもちろん、マルウェアでさえ UEFI 構成を変更することはできません。セキュア ブート付きの UEFI の詳細については、「UEFI による OS 起動前の環境の保護 (英語)」をご覧ください。

トラステッド プラットフォーム モジュール

トラステッド プラットフォーム モジュール (TPM) は、コンピューティング プラットフォームのセキュリティとプライバシー保護を強化する、改ざん対策を備えた暗号化モジュールです。TPM は、PC、タブレット、スマートフォンのような信頼されたコンピューティング プラットフォームにコンポーネントとして組み込まれています。信頼されたコンピューティング プラットフォームは、ソフトウェアだけでは実現できないプライバシーとセキュリティのシナリオを TPM と連携してサポートできるように設計されています。TPM を使用するには、Windows 10 Mobile デバイスのハードウェア認定を取得する必要があります。

TPM を信頼されたコンピューティング プラットフォームの一部として適切に実装することで、ハードウェアに信頼のルートが備わります。これはつまり、ハードウェアが信頼できる方法で動作するということです。たとえば、TPM からのキーのエクスポートはだれも実行できないというプロパティを持つ TPM 内にキーを作成した場合、そのキーが TPM から持ち出されることは絶対にありません。TPM とプラットフォームを緊密に統合すると、プラットフォームの起動に使用されるソフトウェアについて信頼性の高いレポートを生成できるようになるので、ブート プロセスの透明性が増し、デバイス正常性のシナリオをサポートできます。

次に、Windows 10 Mobile で TPM によって提供される主な機能を示します。

- **暗号化キーの管理。** TPM では、キーを作成および保存できるほか、定義した方法でのキーの使用を許可することもできます。Windows 10 Mobile では、BitLocker ボリューム、仮想スマート カード、証明書、その他の各種キーの暗号化キーを保護するために、TPM を使用しています。
- **整合性の測定値の保護と報告。** Windows 10 Mobile では、メジャー ブート機能の対象となるハードウェアおよび Windows ブート コンポーネントの整合性に関連する測定値を記録し、その保護に役立てるためにも TPM を使用します。このシナリオでは、メジャー ブートによりファームウェアからドライバーまで各コンポーネントが測定され、それらの測定値がデバイスの TPM に保存されます。その測定ログをリモートでテストすることにより、別のシステムで Windows 10 Mobile デバイスの起動状態を検証できます。
- **TPM が本当に TPM であることの証明。** プライバシーとセキュリティを保護するためには暗号化キーの管理と整合性の測定がきわめて重要であることから、TPM は、TPM を偽装しているマルウェアから自身を識別しなければなりません。

Windows 10 Mobile では、2.0 標準に準拠する TPM の実装をサポートしています。TPM 2.0 標準は、いくつかの改善が加えられて 1.2 標準よりもさらに優れたものになっていますが、その中でも特に注目すべき点は暗号化の機敏性です。TPM 1.2 のアルゴリズムは、特定の暗号化アルゴリズムとハッシュ アルゴリズムの組み合わせに制限されています。2000 年代初めに TPM 1.2 標準が登場した時点で、セキュリティ コミュニティではこれらのアルゴリズムが暗号化手法として強力であると考えられていました。それ以来、暗号化アルゴリズムと暗号解読攻撃が共に進歩を続けたことで、これを超える強力な暗号化手法への期待が高まりました。TPM 2.0 では、さらに強力な暗号化による保護を実現する追加のアルゴリズムと、特定の地域または業界で推奨されるアルゴリズムのプラグイン機能がサポートされています。さらに、TPM コンポーネント自体を変更せずに、将来新たなアルゴリズムを追加できる余地も確保されています。

TPM は、相手先ブランド供給業者 (OEM) がハードウェアのマザーボードに個別のモジュールとして埋め込む必要があると思われがちですが、ファームウェアに実装して使用することも可能です。Windows 10 Mobile では、2.0 標準に準拠するファームウェア TPM のみをサポートしています。ディスクリート型ソリューションとファームウェア型ソリューションは、満たす必要のある実装要件とセキュリティ要件が同じであることから、Windows では区別されません。そのため、TPM を活用できる Windows 10 の機能は、Windows 10 Mobile でも使用することができます。

> マイクロソフトでは、いずれかのバージョンの Windows 10 Mobile を実行するデバイスの要件として、TPM 2.0 の実装を求めています。詳細については、「最小ハードウェア要件」をご覧ください。

次に示す Windows 10 Mobile セキュリティ機能には、TPM が必要です。

- 仮想スマート カード
- メジャー ブート
- 正常性構成証明 (TPM 2.0 以降が必要)

その他の機能でも、可能な場合は TPM が使用されます。たとえば、Windows Hello には TPM は必要ありませんが、可能な場合は使用します。組織では、Windows Hello で TPM を要件とするようにポリシーを構成することができます。

生体認証

Windows 10 Mobile では、中心的なセキュリティ機能として生体認証が使用されます。マイクロソフトは、生体認証を (以前のバージョンの Windows のように) 単にプラットフォームに付け加えるのではなく、Windows 10 Mobile のセキュリティ コンポーネントに完全に統合しました。これは大きな変化です。以前の生体認証の実装は、大部分が認証を簡略化したフロントエンド方式でした。内部的には、システムによるパスワードへのアクセスと、その後のバックグラウンドでの認証に、生体認証が使用されていました。生体認証によって利便性は高まりましたが、そのすべてがエンタープライズ レベルの認証かというと、そうではなかったのです。

マイクロソフトでは、Windows 10 Mobile デバイスを製造する OEM に、エンタープライズ レベルの生体認証センサーの重要性を説いてきました。Windows Hello ではこのような顔認識センサーや虹彩スキャン センサーを完全にサポートしています。

マイクロソフトは、OEM が今後さらに進化したエンタープライズ レベルの生体認証センサーを製造し、モバイル デバイスへの統合を推し進めるものと期待しています。それにより、生体認証は MFA システムを構成する一般的な認証方法となるでしょう。

トラスト ブート

セキュア ブート付きの UEFI では、ブートキットからユーザーを保護するために各種ハードウェア テクノロジが使用されています。セキュア ブートはデバイス、ファームウェア、ブートローダーの整合性を検証できます。ブートローダーが起動すると、ユーザーはシステムの残りの部分の整合性の保護をオペレーティング システムに頼らなければなりません。

セキュア ブート付きの UEFI がブートローダーの信頼性を確認して Windows 10 Mobile を起動すると、Windows トラスト ブート機能は、すべての Windows スタートアップ コンポーネントが信頼でき (信頼された発行元によって署名されているなど)、整合性があることを確認することで、残りのスタートアップ プロセスを保護します。ブートローダーは、Windows カーネルのデジタル署名を検証してから、その Windows カーネルを読み込みます。Windows

カーネルは、ブート ドライバーなど、Windows スタートアップ プロセスの他のコンポーネントとスタートアップ ファイルをすべて検証します。

メジャー ブート

以前のバージョンの Windows において、ルートキットやブートキットに対処するうえでの最も大きな課題は、クライアントで検出できないことがよくあるという点でした。ルートキットやブートキットは Windows の防御機能やマルウェア対策ソリューションよりも前に起動する場合が多く、さらにシステム レベルの権限を持っているため、自身を完全に偽装しながらシステム リソースへのアクセスを続けることが可能でした。セキュア ブート付きの UEFI とトラスト ブートによってほとんどのルートキットやブートキットを防ぐことができましたが、わずかながら侵入者に利用できる可能性のある攻撃方法が残されていました (たとえば何者かが、マイクロソフト製以外のドライバーなどのブート コンポーネントの署名に使用された署名を侵害し、悪意のあるコンポーネントの署名に利用するなど)。

Windows 10 Mobile には、TPM ハードウェア コンポーネントを使用して、ファームウェア、Windows ブート コンポーネント、ドライバーなどの重要なスタートアップ関連コンポーネントの一連の測定値を記録する、メジャー ブート機能が実装されています。メジャー ブートでは、測定データを隔離してマルウェア攻撃から保護する TPM のハードウェア ベースのセキュリティ機能が使用されているため、ログ データは高度な攻撃からも十分に保護されます。

メジャー ブートは、測定データの取得と、その改ざんに対する保護に重点を置いた機能です。さらに包括的なセキュリティを提供するには、データの分析とデバイス正常性の判定を行えるサービスと連携させる必要があります。

デバイス正常性構成証明

デバイス正常性構成証明 (DHA) は、低レベルのマルウェアへの感染防止に役立つ、Windows 10 Mobile の新機能です。DHA では、デバイスの TPM とファームウェアを使用して、デバイスの BIOS と Windows スタートアップ プロセスの重要なセキュリティ プロパティを測定します。これらの測定は、カーネル レベルのマルウェアかルートキットに感染しているシステム上であっても同様に行われるため、攻撃者がプロパティを偽装する可能性は低くなります。

DHA を Microsoft Intune (別売) やサード パーティ製の MDM ソリューションと共に使用すると、ハードウェアで測定されるセキュリティ プロパティと他のデバイス プロパティを組み合わせて、デバイスの正常性とコンプライアンス対応状態を全体的に把握することができます。この統合方法は、ジェイルブレイク (脱獄) されたデバイスの検出、デバイスのコンプライアンス状態の監視、コンプライアンス レポートの生成、ユーザーまたは管理者へのアラート、デバイス上での修正操作の実施、Office 365 などのリソースへの条件付きアクセスの管理といったさまざまなシナリオで利用できます。

下記の例は、Windows 10 の保護機能がどのように Intune やサード パーティ製の MDM ソリューションと統合され、連携して機能するかを示しています。Windows 10 Mobile のスマートフォン向けセキュリティ アーキテクチャがいかにコンプライアンス状態の監視と検証に役立つか、またデバイス ハードウェアを基盤とするセキュリティと信頼によっていかに企業リソース全体の保護を実現できるかを具体的に説明しています。

ユーザーがスマートフォンの電源を入れると…

1. Windows 10 Mobile のセキュア ブート機能がスタートアップ シーケンスを保護し、定義済みの信頼された構成でのデバイスの起動を許可し、出荷時点で信頼されたブートローダーを読み込みます。
2. セキュア ブートのプロセスが完了すると、Windows 10 Mobile のトラスト ブートに制御が渡り、Windows カーネルのデジタル署名を検証します。コンポーネントの検証が行われ、スタートアップ プロセス中に読み込まれて実行されます。

3. ステップ 1 と 2 に並行して、ハードウェアで保護されたセキュリティ ゾーン (ブート アクティビティを監視するブート実行パスから分離されたゾーン) で、スマートフォンの TPM が独立して実行されます。TPM は、TPM のみがアクセスできるシークレットを使用して署名され、保護と改ざん証明が施された監査証跡を作成します。
4. DHA 対応のデバイスから、保護、改ざん防止、改ざん証明を備えた通信チャネルを通じて、この監査証跡のコピーをマイクロソフトの正常性構成証明サービス (HAS) に送信します。
5. HAS がこの監査証跡を確認し、署名付きの暗号化されたレポートを発行して、デバイスに転送します。
6. DHA 対応の MDM ソリューションから、保護、改ざん防止、改ざん証明を備えた通信チャネルを通じてレポートを確認することで、デバイスがポリシーに準拠した (正常な) 状態で実行されているかどうかを評価し、組織のセキュリティ要件やポリシーに基づいてアクセスを許可したり修正操作を実行したりすることができます。

このソリューションは、他の方法ではきわめて検出困難であろう低レベルのマルウェアを検出して防止できるため、マイクロソフトは Intune のような DHA 対応の MDM システムの実装を検討することをお勧めします。DHA 対応の MDM システムでは、Windows 10 Mobile のクラウド ベースの正常性構成証明サーバー機能を活用することで、高度なマルウェアに感染したデバイスを検出してブロックできます。

Device Guard

Device Guard は、ハードウェアとソフトウェアの両方のシステムの整合性を強化する機能から構成される機能セットです。これらの機能は、オペレーティング システム全体を「何も信頼しない」ことをベースとしたモデル (trust-nothing model) に移行することにより、Windows オペレーティング システムのセキュリティに変革をもたらしました。

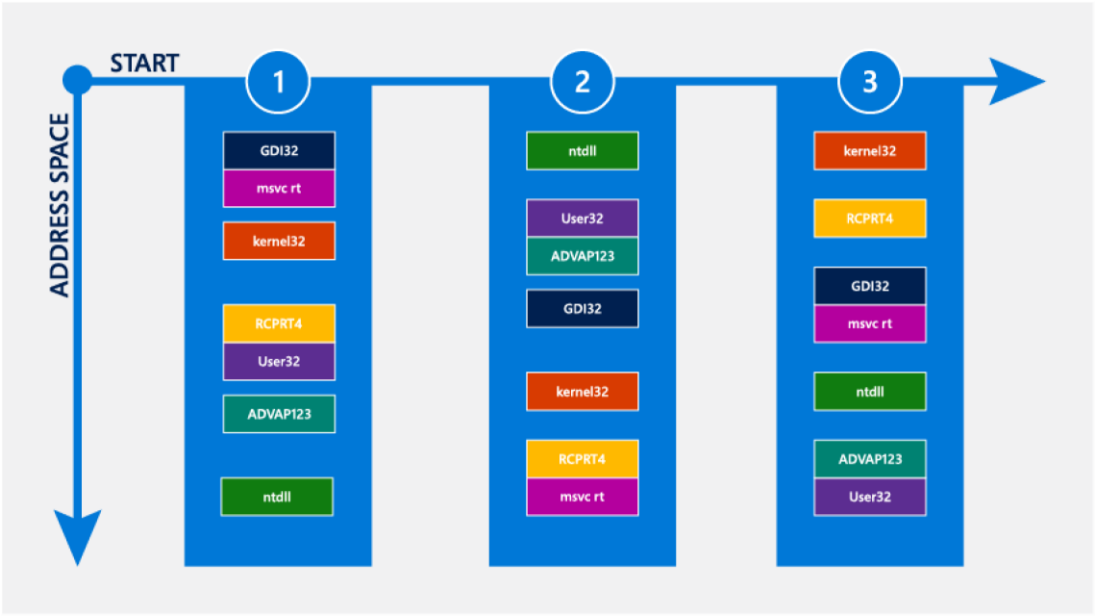
Windows 10 Mobile 上のすべてのアプリは、デジタル署名され、Windows ストアまたは信頼されているエンタープライズ ストアからダウンロードしたものでなければなりません。Device Guard には、この条件をさらに制限するポリシーが実装されています。Windows ストアのアプリはすべて既定でサポートされています。Windows 10 Mobile デバイスで実行できるアプリと実行できないアプリを定義するポリシーを作成することもできます。アプリがデジタル署名されていない場合、ポリシーによって禁止されている場合、または信頼されているストアからのアプリではない場合、そのアプリは Windows 10 Mobile では実行されません。

これらのセキュリティ機能は、前述した高度なハードウェア機能によって支えられています。Windows 10 Mobile では、これらのハードウェア機能をコア オペレーティング システムとさらに高度に統合することにより、新たな形で利用できます。このような新しいセキュリティ機能を提供するために、Device Guard にはセキュア ブート付きの UEFI が必要です。

Address Space Layout Randomization

システムにアクセスするために攻撃者が用いる最も一般的な手法の 1 つは、既に実行されている特権付きプロセスで脆弱性を見つけ、重要なシステム コードやデータが置かれているメモリ内の場所を推定または発見して、その情報を悪意のあるペイロードで上書きする手法です。初期のオペレーティング システムでは、システム メモリに直接書き込むことができるすべてのマルウェアがそのような操作を実行できました。マルウェアは、よく知られた場所や予測しやすい場所にあるシステム メモリを上書きするだけで目的を果たせました。

Address Space Layout Randomization (ASLR) は、メモリ内での重要なデータの保存方法とその場所をランダム化することで、そのような種類の攻撃をはるかに困難にします。ASLR を利用すると、マルウェアにとっては攻撃すべき特定の場所を見つけることがさらに難しくなります。下の図は ASLR のしくみを表したもので、重要な各種 Windows コンポーネントのメモリ内の場所が再起動のたびにどのように変わるかを示しています。



マイクロソフトでは、これまでのバージョンを経て大きく強化された ASLR を Windows 10 Mobile に実装し、特定のアプリだけではなく、システム全体に適用しました。大幅に拡大したメモリ領域を活用できる 64 ビット システムとアプリケーション プロセスも考慮に入れると、Windows 10 Mobile で重要なデータが保存される場所をマルウェアが予測するのは、さらに困難です。ASLR メモリのランダム化は、TPM を備えたシステムで使用するとデバイス間での一意性が増すため、あるシステムで成功した脆弱性の悪用方法を別のシステムに利用することがよりいっそう困難になります。

データ実行防止

マルウェアは、ユーザーが後で気付かずに実行することをねらって、悪意のあるペイロードをメモリに挿入するという方法に頼っています。ASLR による保護がこの方法を困難にする一方で、Windows 10 Mobile はその保護をさらに拡張し、情報の保存だけのために割り当てた領域にマルウェアが書き込まれた場合、それが実行されるのを防止します。データ実行防止 (DEP) は、悪意のあるコードがその目的のために使用できるメモリの範囲を大幅に削減する機能です。DEP では、最新の CPU で NX (No execute) ビットを使用し、メモリ ブロックを読み取り専用としてマークするため、マルウェアは悪意のあるコードの実行にそれらのブロックを利用することができません。すべての Windows 10 および Windows 10 Mobile デバイスが、DEP をサポートしています。

Windows ヒープ

「ヒープ」とは、Windows が動的アプリケーション データを保存するために使用するメモリ内の場所です。マイクロソフトでは、攻撃者にヒープが悪用されるリスクを軽減することにより、これまでの Windows ヒープの設計を継続的に強化しています。

Windows 10 Mobile では、次に示すいくつかの重要な点で、以前のバージョンの Windows よりもヒープのセキュリティが強化されています。

- ヒープで使用される内部データ構造は、メモリ破損に対する保護が強化されています。
- ヒープ メモリの割り当てで場所とサイズがランダム化されるようになったため、攻撃者にとっては、上書きの対象とする重要なメモリの場所を予測することがさらに困難になっています。具体的には、Windows 10 Mobile で新たに割り当てられるヒープのアドレスにランダム オフセットが追加されるので、割り当ての予測がはるかに難しくなります。
- Windows 10 Mobile では、メモリ ブロックの前後に仕掛けとして「ガード ページ」を使用しています。攻撃者は、メモリ ブロックを越えて書き込もうとする場合 (バッファー オーバーフローと呼ばれる一般的な手法)、ガード ページを上書きする必要があります。ガード ページに変更を加えようとする試みは、すべてメモリの破損と見なされるため、Windows 10 Mobile が直ちにアプリを終了することで対応します。

メモリの予約

マイクロソフトでは、オペレーティング システム用に、最小限の 64 KB のプロセス メモリが予約されます。アプリによってメモリのその部分を割り当てることができなくなったため、マルウェアがメモリ内の重要なシステム データ構造を上書きすることはさらに困難になっています。

制御フロー ガード

Windows によりアプリケーションがメモリに読み込まれると、そのアプリケーションにはコードのサイズ、要求されたメモリ、およびその他の要素に基づいてメモリ領域が割り当てられます。アプリケーションがコードを実行し始めると、他のメモリ アドレスにある追加のコードが呼び出されます。各コードの場所間の関係は、コード自体に記述されているため明らかです。しかし、Windows 10 Mobile が登場するまで、これらの場所間のフローがオペレーション システムによって強制されることはなく、攻撃者には必要に応じてフローを変更する機会が与えられていました。つまり、攻撃者はこのしくみを利用して、アプリケーションが通常は実行できないコードを実行することにより、アプリケーションの悪用を達成していたのです。

Windows 10 Mobile では、この種の脅威を制御フロー ガード (CFG) によって軽減しています。作成者によって CFG を使用するようにコンパイルされている信頼済みアプリケーションがコードを呼び出すと、CFG は呼び出されたコードの場所が実行用の場所として信頼されているかどうかを検証します。その場所を信頼できないと判断した場合、CFG は潜在的なセキュリティ リスクとしてアプリケーションを直ちに終了します。

ユーザーが CFG を構成することはできませんが、アプリケーションの開発者は、アプリケーションのコンパイル時に CFG を構成することで、自由に活用できます。ブラウザーは攻撃時の主なエントリ ポイントであるため、Microsoft Edge では CFG を最大限に活用しています。

保護されたプロセス

残念ながら、マルウェアの影響を受けないデバイスというものは存在しません。考えられる最善の予防的制御をすべて試したとしても、マルウェアはいずれオペレーティング システムやハードウェア プラットフォームへの感染経路を見つけ出します。そのため、多層防御の戦略による感染防止は重要ですが、追加のマルウェア制御も必要です。

システム上でマルウェアが実行されている場合は、そのマルウェアが実行できる動作を制限する必要があります。保護されたプロセスは、特別に署名されているプロセスが、信頼されていないプロセスによって改ざんされるのを防止します。保護されたプロセスは、プロセスの信頼レベルを定義します。これにより、信頼性の低いプロセスが信頼性の高いプロセスに干渉し、それが攻撃につながることを回避できます。Windows 10 Mobile では、保護されたプロセスをオペレーティング システム全体にわたって広範に使用しています。

AppContainer

Windows 10 Mobile のセキュリティ モデルは最小権限の原則に基づいており、それを実現するために分離を利用しています。すべてのアプリ、さらにはオペレーティング システム自体の一部も、AppContainer (内部でアプリとそのプロセスを実行できる、セキュリティで保護された分離境界) と呼ばれる独自の分離されたサンドボックス内で実行されます。各 AppContainer はセキュリティ ポリシーによって定義され、実装されます。

一部の AppContainer のセキュリティ ポリシーでは、AppContainer 内からアプリがアクセスできる、地理的な位置情報、カメラ、マイク、ネットワーク、センサーなどのオペレーティング システムの機能が定義されています。

すべての AppContainer には、分離された一意のストレージの場所へのアクセスなど、一連の既定のアクセス許可が付与されています。他の機能へのアクセスは、アプリのコード内で宣言できます。従来のデスクトップ アプリケーションとは異なり、実行時に追加の機能および特権へのアクセスを要求することはできません

AppContainer のコンセプトには、以下の点を実現できるというメリットがあります。

- **攻撃範囲の縮小。**アプリは、アプリケーション コードで宣言され、関数を実行するために必要な機能にしかアクセスできません。
- **ユーザーによる同意と制御。**アプリで使用される機能は、Windows ストアのアプリの詳細ページに自動的に公開されます。機密性の高い情報を公開する可能性のある機能にアプリがアクセスすると、ユーザーに確認と同意を求めるメッセージが自動的に通知されます。
- **アプリの分離。**Windows アプリ間の通信は厳密に制御されます。アプリは互いに分離され、事前に定義された通信チャネルとデータ型を使用している場合にのみ通信できます。

アプリには、正当なタスクの実行に必要な最小限の特権が与えられます。そのため、悪意のある攻撃者がアプリの脆弱性を悪用した場合でも、アプリは特権を昇格できず、また AppContainer 内に収められているため、予想される損害は限定的です。Windows ストアには、アプリに必要なアクセス許可と、アプリの年齢区分、発行元が表示されます。

Device Guard と AppContainer を組み合わせることで、未承認のアプリが実行されるのを防止できます。マルウェアがアプリのエコシステムに紛れ込んだ場合は、AppContainer によってアプリを抑制し、潜在的な損害を抑えることができます。Windows 10 Mobile の「何も信頼しない」ことをベースとしたモデルは、どのコンポーネントも完璧とは限らないという前提に基づいています。しかし、アプリ、AppContainer、Windows 10 Mobile 自体の潜在的な脆弱性が、攻撃者にシステムを侵害する機会を与える可能性もあるため、冗長な脆弱性は軽減する必要があります。以降のトピックでは、Windows 10 Mobile における冗長性の軽減策の一部について説明します。

Microsoft Edge

Web ブラウザーは、セキュリティ戦略の重要な構成要素です。Web ブラウザーはインターネットに対するユーザーのインターフェイスであり、インターネット上には悪意のあるサイトや危険の潜んだコンテンツがあふれかえっています。ほとんどのユーザーは、ブラウザーがなければ少なくとも作業の一部ができなくなり、ブラウザーに完全に頼っているユーザーも数多く存在します。このような現状から、ブラウザーは悪意のあるハッカーが攻撃を開始する、第一の経路となっています。

Windows 10 Mobile には、読み取りビューなどの機能によってブラウジングだけにとどまらず多種多様な用途に利用できる、まったく新しい Web ブラウザー「Microsoft Edge」が搭載されています。Microsoft Edge は、以下のような点で以前のマイクロソフトの Web ブラウザーよりも安全性に優れています。

- **Windows 10 Mobile の Microsoft Edge は、拡張機能をサポートしていません。**Microsoft Edge には PDF 表示機能が組み込まれています。
- **Microsoft Edge は UWP アプリとして設計されています。**内部的に区分されており、また、システムやデータ、その他のアプリに対してブラウザーをサンドボックス化する AppContainer 内で実行されます。
- **Microsoft Edge によりセキュリティ構成タスクが簡略化されます。**Microsoft Edge では、シンプルなアプリケーション構造と単一のサンドボックス構成が採用されているため、必要なセキュリティ設定が少なくなりました。さらに、マイクロソフトではセキュリティ上のベスト プラクティスに沿った Microsoft Edge の既定の設定が確立されているため、設計上も安全性が向上しています。

まとめ

Windows 10 Mobile には、個人所有や企業所有のデバイスを、未承認のアクセス、データ漏えい、マルウェアの脅威から保護するためのセキュリティ機能が数多く備わっています。このドキュメントで取り上げた多要素認証、データの分離、マルウェア対策といった機能のすべてが、オペレーティング システムにシームレスに統合されています。これにより、モバイル デバイスの生産性と使いやすさを損なうことなく企業の保護を実現できるため、さらに多くのユーザーがモバイル デバイスをますます業務に活用できるようになります。Windows 10 Mobile Anniversary Update のセキュリティ機能の詳細については、https://technet.microsoft.com/ja-jp/windows/mt631176 をご覧ください。