PIQUE SOLUTIONS

Windows 10 と Android 6

ラボ環境における機能比較: Windows 10 と Android 6 のセキュリティおよび管理

PIQUE SOLUTIONS

2016 年 7 月

このホワイト ペーパーは、マイクロソフトの後援により作成されました。本書の基盤となっているラボ環境でのテスト、調査、分析は、Pique Solutions が単独で実施したものです。

795 Folsom Street, 1st Floor | San Francisco, CA 94107 | Tel.: 415.685.3392 | www.piquesolutions.com

目次

要旨

サイバー脅威防止は、組織が攻撃される可能性を低減することを目標とするものですが、一方でサイバー脅威からの回復 (サイバー レジリエンス) とは、リスク管理を通じ、こうした攻撃によって生じる影響を軽減することを目指しています。サイバー レジリエンス プログラムでは、攻撃を検出・防止する技法を考慮しつつも、侵害は起こり得るものであることを前提としています。このアプローチで重視されるのは、予測力、機動力、適応力です。

サイバー レジリエンスで最優先されるのは、資産に対して適切なセキュリティ機能を活用することです。セキュリティ スタックは、さまざまな脅威、特にビジネス資産に影響を及ぼす脅威から、企業を保護する必要があります。しかし現状では、セキュリティに関する意思決定に活用できるデータが不足しているために適切なセキュリティが利用されておらず、企業がそれに気付いていないことが少なくありません。また、サイバー脅威に直面した際の回復力の強化に活用できるテクノロジやアーキテクチャ関連のプラクティスは数多く存在していますが、それらを利用することでメリットを得られる反面、コストもかかります。

Pique Solutions では、マイクロソフトの Windows 10 と、Android for Work 搭載の Android 6 の回復機能の比較分析をラボ環境で実施しました。この分析では、回復機能が組織にもたらす保証レベル、回復機能の実用性、ユーザー エクスペリエンスへの影響を評価しました。

マイクロソフトは、Windows 10 と Windows 10 Mobile を通じて、PC、タブレット、スマートフォンのオペレーティング システムを単一の OS に統合しました。一方 Android は、モバイル専門のオペレーティング システムです。Windows 10 と Windows 10 Mobile は共同開発されており、同一のコアと同一のアプリ モデルを共有し、同一のアプリ ストアにアクセスします。Windows 10 にはさまざまなエディションが用意されていますが、このホワイト ペーパーでは Windows 10 Pro、Windows 10 Enterprise、Windows 10 Mobile、Windows 10 Mobile Enterprise を検証しました。基盤のチップセットによって特別な機能 (x86 プロセッサ上での仮想化のサポートなど) が提供される場合や、コアに関連する特別な機能 (Windows 10 Mobile のテレフォニーなど) が装備されている場合がありますが、その点を除けば、ユニバーサル Windows プラットフォーム (UWP) に組み込まれているセキュリティ、管理、アプリは、PC、タブレット、スマートフォン全体で共通です。本書では、このオペレーティング システムを「Windows 10」と呼び、エディションや違いについては適宜説明します。

この回復機能の分析ではセキュリティ保証とユーザビリティを主要な基準として測定し、その結果 Pique Solutions は Windows 10 の方がセキュリティ保証のレベルが高く、ユーザビリティに対する影響は低いと結論付けました。Windows 10 は、

PC とモバイル デバイスにコスト効率の良い 2 要素認証を提供し、ユーザー パスワードを不要にすることにより、資格情報の盗難に起因する侵害発生のリスクを軽減しています。Windows 10 では、ユーザーにとって透過的な方法で企業データが保護され、ユーザーは同一のアプリを個人的なタスクにも仕事にも使用できます。また Windows 10 は、デバイスの正常性構成証明に基づいて企業リソースへの条件付きアクセスを提供します。デバイスの種類にかかわらず統合された 1 つの OS アーキテクチャとアプリ開発プラットフォームを活用することで、重要なセキュリティ更新プログラムや修正プログラムの配布を含むデバイスとアプリのプロビジョニングを合理化しています。

Android for Work は、基盤の Android 環境に待ち望まれていた機能で、以前よりも高度なレベルの保護を企業の Android 環境に提供します。Android for Work は、個人データと業務データの分離、ハードウェア ベースのデバイスの完全暗号化、業務用アプリの管理の効率化など、Android 環境において大きな悩みとなっていたセキュリティ上の問題に対応します。ただし、Android for Work が追加されても、ますます厳しくなる企業のセキュリティ要件を満たす十分な保護を Android が提供できるのかという疑問は残ります。今回のテストの結果、Android for Work を搭載する Android 6 は、業務用のスペースから個人用のスペースを分離できるなど、組織にとって有用な機能を提供していますが、ユーザビリティとリソースに顕著な影響が及ぶことがわかりました。

総合的に見ると、Android 6 は Windows 10 と同じレベルのセキュリティ保証やユーザビリティを提供していません。Android の大きな問題は、Google Nexus デバイス以外は、デバイス製造元の OS 更新に一貫性がなく、一部のデバイスはまったく更新を受信しない点です。さらに、(Good Technology を買収した) BlackBerry、Samsung KNOX などのテクノロジ パートナーが Android for Work 上に拡張機能を構築しているため、Android for Work には企業に最低限必要な機能しか搭載されていません。マイクロソフトが提供しているような製品ロードマップが発行されなければ、どの Android ベンダーが長期的な価値を提供するか見極めることが困難です。

豊富な資金を持つ攻撃者によって実際に執拗な標的型攻撃が仕掛けられている現在のサイバー環境では、所有するアーキテクチャを使用してどの程度のサイバー レジリエンス目標を達成できるのか、どの程度効率的にサイバー レジリエンス技法を取り入れられるのかを考慮しなければなりません。Windows 10 は、最も厳しいセキュリティ要件および企業管理要件を満たす回復性の高いデバイスを提供できます。しかも、エンド ユーザーにとって透過的に、生産性を低下させるどころか高める方法でこうした制御を実現します。

テスト手法

Pique Solutions によって開発された総合的なテスト手法を以下に示します。

1. デバイスから企業リソースへのアクセスに関するリスクを低減するために必要なセキュリティ特性とセキュリティ機能を特定する (企業データの保管、転送、使用といった機能を含む)。
2. ディレクトリ サービスなど、大半の組織に共通するコンポーネントを含む、簡易なエンタープライズ アーキテクチャをシミュレートする環境を構築する。
3. Windows 10 Mobile、 Windows 10 Mobile Enterprise、 Windows 10、 Windows 10 Pro、 Windows 10 Enterprise、 Android for Work を搭載する Android 6 の評価に使用するモバイル デバイスと管理システムを選定する。
4. 選定したデバイスがテスト フレームワークに定義されたタスクをどのように実行するかを手作業で確認する。
5. 結果の詳細な評価を公表する。

業界で認知されている標準と定義を使用して Windows 10 と Android 6 を評価するために、Pique Solutions では、アメリカ国立標準技術研究所 (NIST) 発行のサイバーセキュリティ プラクティス ガイド Special Publication (SP) 1800-4b に記載されているセキュリティ特性と必要な機能を参考にしました。NIST は、NIST SP 800-124、NIST SP 800-164、米国家安全保障局 (NSA) モバイル機能パッケージ、適切な米国家情報保証パートナーシップ (NIAP) プロテクション プロファイルなどに記載されている複数の標準の内容と概念を分析して、必要なセキュリティ特性を導き出しています。Pique Solutions は、参考にした NIST のセキュリティ特性を適宜変更、更新することによって、不足している機能に対応すると共に、セキュリティ特性とベンダーが主張する機能を相関付け、本書全体の内容と流れを改善しました。

わかりやすく説明するために、セキュリティ機能を次の 4 つの領域に分類しました。

ID と承認

- 認証: デバイスとアプリに対するユーザーのローカル認証、ユーザーのリモート認証、デバイスのリモート認証
- 信頼モデル: 認証のためのユーザーとデバイスのロールの使用、資格情報およびトークンの保管と使用
- 生体認証のサポート: 方法、格納、使用

情報保護

- ストレージの保護 – 保存中のデータ (DAR): デバイス暗号化、安全なキー格納、ハードウェア セキュリティ モジュール
- 通信の保護 – 転送中のデータ (DIT): 仮想プライベート ネットワーク (VPN)、アプリごとの VPN
- 作業中のデータ保護 – 使用中のデータ (DIU): 保護された実行環境、データ管理、データ共有

脅威対策

- デバイス整合性: ブート/OS/アプリ/ポリシー検証、信頼された整合性レポート
- アプリ保護: メモリ隔離、信頼された実行、ブラウザー保護

管理

- デバイス登録: 検出、証明書、プロビジョニング
- デバイス構成とサポートされるポリシー: ネットワーク、デバイス リソース管理、ジオフェンシング
- アプリ管理: 配信、更新、構成、アプリのブラックリスト/ホワイトリスト
- リモート アシスタンス: 資産管理、OS とセキュリティの更新、紛失したデバイス、リモート ワイプ
- 監視: 異常な動作の検出、コンプライアンス、原因の検出

テスト環境では、世界中の企業で広く利用されている一般的なソフトウェア、具体的には Microsoft Windows Server、 Microsoft Active Directory、 Office 365 (ドキュメントと電子メール)、「企業アプリ」(企業が提供するアプリをシミュレートするための、機能が制限された軽量アプリ)、「個人用アプリ」(個人用アプリをシミュレートするための、機能が制限された軽量アプリ)、および OneDrive を使用しました。

モバイル デバイス管理 (MDM) システムは、マイクロソフトのツール、Google Apps、 MobileIron と統合された Microsoft Intune を使用しました。

使用したデバイスは次のとおりです。

a. Lumia 950 ― Windows 10 Mobile
b. Surface Pro 3 ― Windows 10 Enterprise
c. Nexus 5x―Android for Work 搭載の Android 6

d. Nexus 9—Android for Work 搭載の Android 6

テスト環境とデバイスの構成、定義されたすべてのシナリオの実行、およびこの比較分析の発行は、エンタープライズ モビリティ スペシャリストが担当しました。Pique Solutions では、OS 管理機能を実際の環境で分析するために MDM ベンダーを活用しました。たとえば、Microsoft Intune は Android のアプリ ラッピング機能を提供します。アプリ ラッピングはデータを保護する強力な機能ですが、他のベンダーが提供するアプリ ラッピング機能と比較分析する必要があります。また、Intune の Android for Work サポートはまだ開発段階であり、Google の MDM ソリューションは Windows 10 を管理できる十分な機能を備えていません。同等の機能と比較するために、Pique Solutions は幅広い組織に導入されているサード パーティ製 MDM ツールとして MobileIron を選定しました。MDM の分析は、この調査プロジェクトの当初の意図および範囲には含まれていません。

OS の回復力の評価では、ISA-99.01.01 で導入された概念であるセキュリティ保証レベル (SAL) に照らしてセキュリティおよび管理の機能の分析を行いました。以下に SAL の説明を示します。

> セキュリティ レベルは、ゾーンのセキュリティに対処する定性的なアプローチを提供します。セキュリティ レベル定義は定性的な手法であるため、組織内の複数のゾーンに対するセキュリティの比較と管理に適用できます。利用できるデータが増加し、リスク、脅威、セキュリティ インシデントの数学的表現が開発されれば、この概念は、セキュリティ レベル (SL) の選択および検証の定量的なアプローチに移行するでしょう。セキュリティ保証レベルは、エンド ユーザー企業だけでなく、産業用オートメーションおよび制御システム (IACS) やセキュリティ製品のベンダーも利用できるようになります。また、ゾーン内で使用する IACS デバイスと保護対策の選定や、さまざまな業界セグメントのさまざまな組織においてゾーンのセキュリティの特定と比較にも使用されるでしょう。

ISA99 では、定性的に 4 つの SAL が定義されています。

- SAL1 – 不用意または偶発的な侵害からの保護
- SAL2 – 単純な手段を利用した意図的な侵害からの保護
- SAL3 – 高度な手段を利用した意図的な侵害からの保護
- SAL4 – 幅広いリソースと高度な手段を利用した意図的な侵害からの保護

スコア付けでは、SAL に数値が割り当てられ、組織のセキュリティに対する機能の実用性に基づいて重み付けされています。実用性とは、その機能が組織に必要な特性を提供しているかどうかを意味します。合計スコアは、OS の総合的な回復力レベル、つまり OS がどれだけ効果的に、どのレベルまで攻撃に対抗できるかを表しています。Pique Solutions は、セキュリティがユーザビリティにもたらす影響も評価しました。メトリックには、タスク完了までの時間、エラー率、ユーザー満

足度が使用されました。情報セキュリティは、優れたユーザー エクスペリエンスを提供できなければ、必ず人為的なエラーを招くことになります。

主な結果

Pique Solutions がラボ環境で実施した Windows 10 と Android 6 のセキュリティおよび管理性に関する機能の比較評価を通じ、Windows 10 は Android for Work 搭載の Android 6 よりも高いセキュリティ保証レベルを提供し、ユーザビリティに対する影響も低く抑えられることがわかりました。この結論は、以下に示す主な結果に基づいて導き出されました。

ID と承認

- Windows 10 は、登録デバイスと生体認証または PIN の組み合わせによるネイティブな 2 要素認証を提供しており、パスワードが不要になっている。
- Android 6 は、リモートの 2 要素認証を実現するためにサード パーティ製のアプリを使用する必要がある。
- Windows Hello は、指紋認識、顔認識、虹彩スキャンを含む生体認証をサポートするフレームワークで、今後登場する他の生体認証形式もサポートできる。
- 認証用にベンダーが提供しているさまざまな指紋スキャナーを統合するために、Android 6 で Android 指紋認証 API が導入された。
- Windows 10 は FIDO 2.0 を実装した初の OS である。FIDO 2.0 は、多要素認証と非対称キーをサポートし、ハードウェア ベースの構成証明を利用してキーの正当性を保証する。

情報保護

- Windows Information Protection (WIP) は、セキュア コンテナーやアプリ ラッピングによるユーザビリティへの影響をまったく受けずに、ビジネス データを透過的に管理する。
- Android for Work はセキュア コンテナー テクノロジで、個人用と仕事用に重複してアプリが必要になるため、システム リソースとユーザビリティに悪影響が及ぶ。

脅威対策

- Windows 10 のメジャー ブートは、ハードウェアを使用してシステム ブート プロセスの整合性を測定する。

- Android デバイスは、Trusted Execution Environment を使用して整合性を検証する機能を提供するが、この機能の実装状況はデバイスやベンダーによって異なる。
- Windows 10 は、制御フローの整合性、制御フロー ガード (CFG) によってメモリ保護を強化し、メモリを破損させる脆弱性に対抗する。

管理

- Windows ストアはあらゆる Windows 10 デバイスに更新プログラムをプッシュできるため、Windows 10 デバイスは常に最新のセキュリティ更新プログラムを適用した状態を維持できる。
- Android デバイスでは製造元がアクティブ デバイスの更新を担当するため、すべてのデバイスにセキュリティ更新が配信される保証がない。
- マイクロソフトは、脆弱性にタイムリーに対応する一貫性の高い修正プログラム更新スケジュールを維持している。修正プログラム管理は組織のセキュリティにとって非常に重要なプロセスである。
- Windows 10 は、リモート正常性構成証明に基づいて、ハードウェアからソフトウェアまでデバイスのコンプライアンス状態を確保し、条件付きアクセスによって非準拠デバイスのアクセスを制限する。
- Android 6 は、Windows 10 と同様のリモート正常性構成証明機能を提供していないため、デバイスのルート化を検出する機能が制限される。ルート化は、ベンダーの付属ソフトを排除する手法として Android エコシステムで広く行われている。

テストのスコア

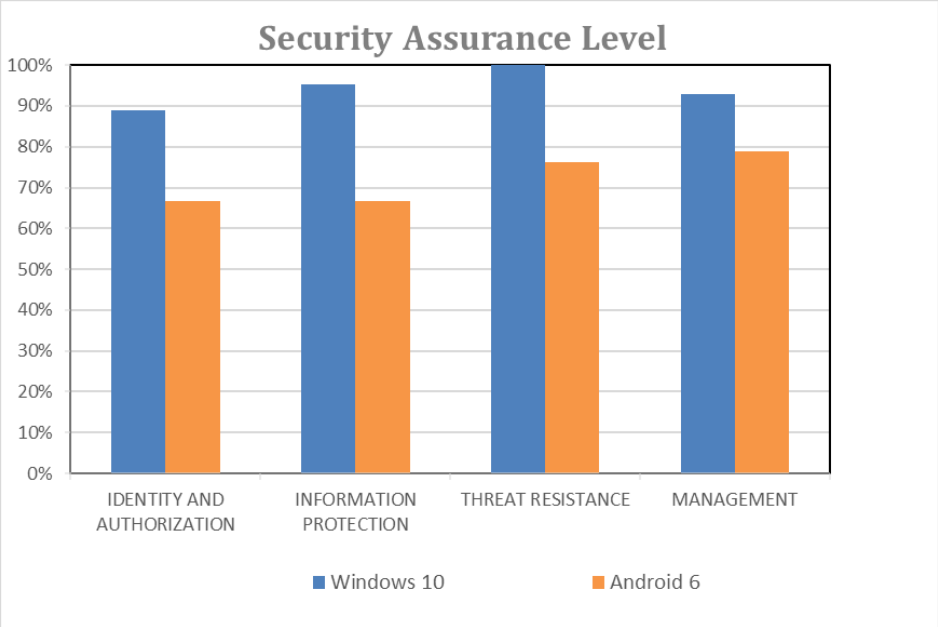

図 1.Windows 10 と Android 6.0 のセキュリティ保証に関するラボ テストのスコア

総合すると、Windows 10 の方が高いレベルのセキュリティ保証を提供していました。特に ID 管理では、統合認証アーキテクチャによって FIDO 2.0 を含むあらゆるレベルの認証がサポートされています。Google は現在 FIDO 2.0 への対応を進めていますが、対象は Web 認証のみです。Windows 10 は、ドメイン、デバイス、アプリ、Web 向けに FIDO 2.0 を実装しています。データ保護の面では、Android for Work 搭載の Android 6 はアプリとデータの分離にコンテナーを使用していますが、この手法では多くのシステム リソースが消費されます。また、メールや予定表などの主要な機能のアプリを重複して用意する必要があります。Windows 10 はデータに制御機能を適用しますが、適用されていないときと同じレベルのユーザビリティを維持します。脅威対策としては、Windows 10 はメモリ制御手法を活用してメモリの不正使用を困難にしています。マイクロソフトは、長期にわたってエンタープライズ管理機能を提供していますが、Windows 10 によっていっそう多様で統合的な機能の構築が可能になっています。そして最も重要なこととして、Android は信頼性の高いセキュリティ プロセスを提供した経験がないため、万一修正プログラムが適用できない重大な欠陥が発生した場合に組織の業務が妨害される可能性があります。

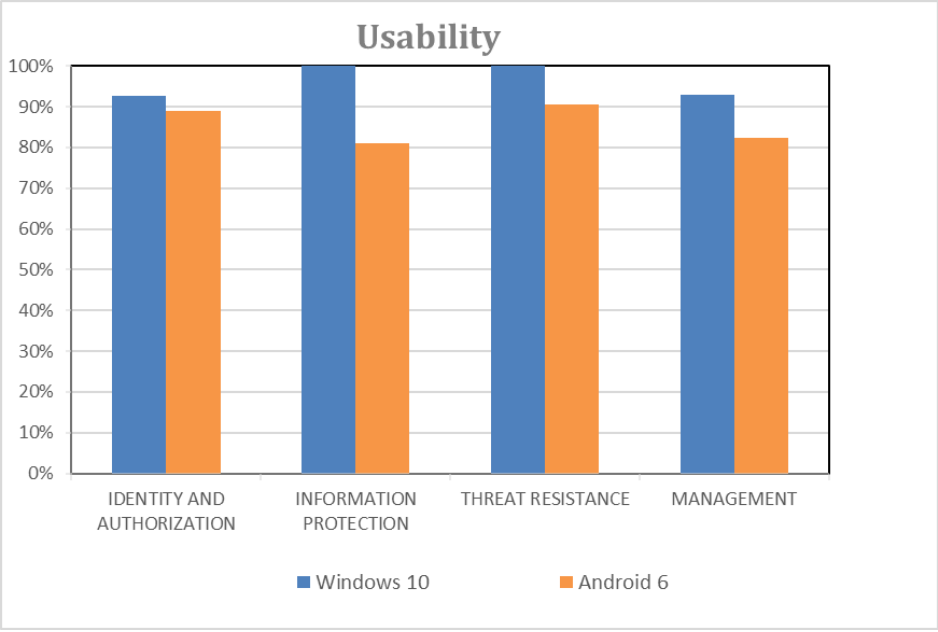

図 2.Windows 10 と Android 6.0 のユーザビリティに関するラボ テストのスコア

ID と承認

ID とアクセスの管理 (IAM) は、必要とするユーザーに必要なときに適切なすべてのリソースへのアクセスを提供する機能です。企業は、ユーザーがさまざまなデバイスにアクセスする分散システムを管理する際に機動力を実現できる IAM 機能を必要としています。IAM は、IAM インフラストラクチャのコストを考慮しながら、各ユーザーの ID の整合性と信頼性を保証する必要があります。さらに重要なこととして、IAM は認証制御の強力さとユーザーにとっての使いやすさを両立する必要があります。

最も一般的な ID の形態は、ユーザー名とパスワードです。大半のユーザーは、平均して 3 つ以上のパスワードを記憶しておく必要があるため、非常に複雑なパスワードを設定してしまうと、多くのユーザーは記憶しようという気が起こらず、実際にも記憶するのが困難です。しかし複雑なパスワードを用意しても、最新のコンピューターを使用すれば、数秒とは言わずとも、数分で侵害される可能性があります。ユーザーの資格情報を知っているだけで、第三者がそのユーザーになりすますことができるのです。シンプルで低リスクの個人デバイスと思われていたモバイル デバイスは、利便性を考慮して単純な 4 桁 PIN で標準化されたため、複雑さの要素が大幅に少なくなっています。パスワードと PIN は、強力とは言えませんが、比較的便利で、実装しやすく、ユーザーにとって個人的なものであるという理由から現在も使用されています。多要素認証戦略の一環として、パスワードと PIN は効率的かつ便利に活用できる可能性があります。より効果的な方法として、生体認証を活用すれば、ユーザー ID は一意性が高まり、個人との結び付きが強くなり、ユーザーと企業にとって便利なものなります。

認証

Windows 10 は、ユーザーからデバイスやアプリへのリモート認証のために 2 要素認証を提供します。Windows Hello は、パスワードに取って代わるテクノロジで、特定のデバイスと生体認証ジェスチャまたは PIN の組み合わせを利用します。Windows Hello は、Microsoft アカウント、Active Directory (AD)、Azure AD、または Fast ID Online (FIDO) 2.0 認証に準拠したサード パーティのサービスもサポートしています。Windows 10 は、エンタープライズ環境で FIDO 2.0 を活用する初の OS であり、FIDO 2.0 の採用は大きな前進と言えます。FIDO 2.0 は、非対称キーをハードウェア ベースの構成証明と組み合わせてキーの正当性を検証することで、多要素認証に対応しています。

Windows Hello の登録時に行われる最初の 2 段階検証の後、ユーザーはデバイスに Windows Hello をセットアップし、ID を検証するためのジェスチャ (生体認証または PIN) を設定します。トラステッド プラットフォーム モジュール (TPM) チップ

は、デバイス上で認証キーを生成し、デバイスにバインドします。キーは、オプションで証明書に基づいて生成することもできます。これにより、デバイスはエンタープライズ ドメイン アカウントに関連付けられた ID の 1 つになります。非対称キー暗号化では、企業のアプリやオンラインの企業リソースへのアクセスを許可する前にユーザーが認証されます。これは、スマート カードを使用して証明書ベース認証を強化する方法や、携帯電話によってネットワークを検証する方法に似ていますが、追加のハードウェアは必要ありません。また、Windows 10 では、デバイス上にある個人の Microsoft アカウントを Azure AD や社内 Active Directory ドメインに参加させる必要はありません。

Windows 10 Enterprise は、Credential Guard と呼ばれるアクセス制限された仮想コンテナー内で認証を実行することによって、認証システムの保護を強化します。すべてのアクセス トークンとチケットをこのコンテナーに格納し、最大長のハッシュで完全にランダム化して管理することで、ブルートフォース攻撃を回避します。

Android 6 は、エンタープライズ ドメイン 2 要素認証のためにサード パーティ製のアプリを必要とします。Android では、デバイスへのアクセスを提供する前に、ユーザーが入力する PIN、パターン、パスワード、または指紋を使用して認証することができます。これは基本的なローカル ユーザー認証です。Android 6 でサポートされる 2 つの認証コンポーネントは、ゲートキーパー (PIN/パターン/パスワード) と指紋です。これらのコンポーネントは、認証されたチャネルを通じて自身の認証状態を KeyStore サービスに通知します。デバイス認証は Trusted Execution Environment (TEE) で行われます。ゲートキーパーは、ハードウェアでサポートされている秘密キーを使用して、パスワードの登録と検証を行います。ユーザーがパスワードの検証を行う際、ゲートキーパーは TEE で生成された共有シークレットを使用して認証用の構成証明に署名し、ハードウェアでサポートされる KeyStore に送信します。TEE の実装はデバイス製造元によって異なり、TPM チップへの実装も可能です。TPM は最も安全な手段で、Windows 10 デバイスも TPM を提供しています。分離された環境内の System on a Chip (SoC) ファームウェアにも実装できます。この方法が最も一般的で最もコストがかかりません。TPM は Windows 10 では必須ですが、Android では必須ではありません。

Android 6 は、ゲスト アカウント、仕事用のアカウント、2 つ目のホーム ユーザー アカウントなど、複数のユーザー プロファイルをサポートしています。ユーザー プロファイルは、デバイスとアプリの単一要素のローカル認証で使用されます。管理対象アカウント (Azure AD など) を使用したリモート認証はサポートされていません。ユーザー プロファイルは Android for Work の認証の基盤です。この管理対象プロファイルによって、Android ユーザーが、管理に関する追加のプロパティと視覚的な要素と共に定義されます。複数のユーザー アカウントを使用すると、ユ

ーザー データが区分化され、他のローカル ユーザーへのデータの公開が制限されます。ユーザー プロファイルごとに、新しいワークスペース セッションと、ユーザーに関連するアプリおよびリソースが生成されます。1 台のデバイス上で複数のユーザー プロファイルを有効にして実行すると、システムのパフォーマンスとリソースに影響が及びます。特にシステム メモリが少ないデバイスまたはメモリ効率の低い旧式デバイスでは、その傾向が顕著です。Android ユーザー プロファイルは、デスクトップ クラスの OS が提供するマルチ ユーザー サポートと同等のものではなく、真の価値を提供するかどうかは現時点では不明です。

生体認証のサポート

Windows Hello フレームワークは、生体認証を使用した強力な 2 要素認証を提供するため、企業 ID を保護すると共に、パスワードの必要性や使用を最小限に抑えることができます。Windows Hello コンパニオン デバイス フレームワークにより、Windows 10 スマートフォンを使用して Windows 10 PC のロックを解除したり、他のコンパニオン デバイスを使用して Windows 10 Mobile デバイスのロックを解除したりできます。

Windows Hello は、指紋認識、顔認識、虹彩スキャン含む生体認証をサポートしており、今後登場する他の生体認証形式もサポートできます。

Windows 10 は、生体認証とデバイスのセキュリティ コンポーネントを統合します。ユーザーの生体認証データは、ユーザーのデバイス以外の場所に移動されることも、クラウドに一元的に格納されることもありません。Windows 10 は、センサーによって取得された生体認証イメージをアルゴリズム形式に変換します。元のイメージは破棄され、復元できなくなります。このアルゴリズム形式のイメージは、すべての Windows 10 Mobile デバイスに必須で搭載されている TPM に格納されます。生体認証イメージが格納されないため、他のデバイスから企業リソースへの不正なアクセスにこれらのイメージが使用されるリスクが排除されます。また、組み込みのスプーフィング対策や生体検知機能により、偽の生体認証データ (ユーザーの目の写真など) を使用してデバイスにアクセスすることはできません。

Android 6 では、Android 指紋認証 API が導入されています。Android 6 デバイスに指紋センサーが搭載されている場合、ユーザーは 1 つ以上の指紋を登録し、これらの指紋を使用してデバイスをロック解除したり、その他のタスクを実行したりできます。Android 6 では、ハードウェアによってサポートされる KeyStore をデバイスに実装すること、および TEE で指紋照合を実行することがベンダーに義務付けられています。その際、個人を特定できるすべての指紋データを暗号化し、TEE 内で暗号を使用して認証しなければなりません。

Android 6 指紋認証 API が登場する前は、ハードウェア製造元は独自の指紋認識機能を提供していましたが、その多くに脆弱な認証システムが搭載されていたこと

がわかっています。ベンダーが実装した Android セキュリティ制御が不十分であったために、デバイスに指紋がクリア テキストで保管されていたケースもありました。現在 Google は製造元に対してデバイスに指紋センサーを実装するよう推奨しているだけですが、センサーを実装する製造元は、相互運用性のために Google の指紋標準に準拠する必要があります。

テストのスコア

ID 管理	セキュリティ保証レベル (SAL)	ユーザビリティ
Windows 10	**89**	**93**
Android 6	**67**	**89**

Windows 10 の方が高いレベルのセキュリティ保証を提供していました。特に ID 管理では、統合認証アーキテクチャによって FIDO 2.0 を含むあらゆるレベルの認証がサポートされています。Google は現在 FIDO 2.0 への対応を進めていますが、対象は Web 認証のみです。Windows 10 は、ドメイン、デバイス、アプリ、Web 向けに FIDO 2.0 を実装しています。Windows 10 は、生体認証などのジェスチャとデバイスを使用する 2 要素ドメイン認証機能を備えており、パスワードを使用する必要があります。この 2 要素アーキテクチャは、トークン ベース システムと同等のセキュリティ保証レベルを提供しますが、高いレベルのユーザビリティも維持します。また、関連するサポート インフラストラクチャ (バックエンド サーバーやユーザー トークンなど) を必要としないため、非常にコスト効率にも優れています。キー ストアはハードウェア ベースで、TPM モジュールが使用されます。Windows 10 と Android 6 は共に、システム全体に生体認証を提供する統合プラットフォームを目指していますが、複数の認証手法をサポートし、他人受入率が低く、スプーフィングに対する重要なメトリックを活用し、パスワードも排除するフレームワークを提供する Windows 10 が、生体認証では明らかに Android 6 をリードしています。

情報保護

データ損失防止では、データのライフサイクルに対応する 3 つの機能グループでデータを制御するように定義されています。その 3 つとは、デバイスや他の形式のメディアに格納されているデータを指す「保存中のデータ (DAR)」、ユーザーと情報共有手段の間で共有されているデータを指す「転送中のデータ (DIT)」、デバイス上のアプリ、ドキュメント、システム メモリ内にあり、作成または操作されているデータを指す「使用中のデータ (DIU)」です。どのようなデータ保護戦略で

も、制御はできるだけデータの近くに配置されます。最も効率的なデータ保護手法は制御をデータ上に配置する方法、次いで管理アプリ上に配置する方法、デバイスおよびネットワーク上に配置する方法です。これらすべての場所に制御を配置すれば、データのライフサイクル全体にわたる包括的な管理を行うことができます。

ストレージの保護 (DAR)

デバイスの紛失、盗難、不正使用に起因する機密情報の損失や侵害を防止する主要な手段として、暗号化が使用されます。暗号化に使用される暗号化キーは、ソフトウェア、ファームウェア、またはハードウェア内の保護された場所に格納する必要があります。最も高度な保護を提供するのはハードウェアです。改ざん防止機能付きハードウェアも暗号化処理によく使用されています。

Windows 10 は、OS とデータ ストレージ パーティションを含むディスク全体を暗号化する BitLocker を備えています。BitLocker は、ポリシーで指定されている場合やユーザーが Windows 設定で有効にしている場合に、自動的に暗号化を適用します。Windows 10 は、デバイスのパフォーマンス低下を回避するために、プロセッサ拡張機能を使用して暗号化を高速化します。Windows 10 Mobile の既定の暗号化アルゴリズムは 128 ビット AES ですが、システム管理機能を通じて有効にすると構成可能になります。Windows 10 Enterprise は 128 ビットおよび 256 ビットの XTS-AES をサポートしており、暗号化されたテキストを操作してプレーン テキストに予測可能な変更を発生させるタイプの攻撃からも暗号を保護します。

必要なサポート ハードウェアが搭載されている Android 6 デバイスは、既定で暗号化が有効にされています。Android 6 にアップグレードしたデバイスは、暗号化を既定で有効にする要件を満たしていません。また、高速フラッシュ ストレージを搭載していないローエンド デバイスや、高速な AES 暗号化をサポートしていない 32 ビット チップを使用するローエンド デバイスも要件を満たしていません。デバイスは、リムーバブル メディアを使用し、そのメディアにブロックレベルの暗号化を適用できます。Android ディスク暗号化の基盤は dm-crypt です。これはブロック デバイス レイヤーで動作するカーネルの機能です。既定の暗号化アルゴリズムは 128 ビット AES です。

以前の Android では、ユーザーのロック画面パスワード、またはソフトウェアに格納された PIN を使用して生成されたキーを使用して、マスター キーを暗号化していました。このキーは、オフボックスのブルートフォース攻撃に対して脆弱でした。Android 6 はこの脅威に対処するために、サポート対象のデバイス上で、ハードウェア ベースで保管されている TEE キーを使用して、このシンプルなキーにもう一度署名します。さらに、暗号化レイヤーを追加して適用して、キー長を適切に調整し、マスター キーの暗号化/暗号解除を行う最終キーを生成します。サポー

トハードウェアが搭載されていないデバイス (最新のハイエンド Android デバイスを除くデバイス) は、今後もソフトウェアにキーを格納することになります。

なお、最新の合理的なプロセスを使用して 128 ビット キーの全数キー探索を行うには、現在の能力をはるかに超えるリソース (MIPS、メモリ、処理能力、時間) が必要となります。また、画期的な手法が開発されれば、128 ビットだけでなく 256 ビットにも適用可能になると考えられます。256 ビット キーの活用は必ずしも効果的とは限りません。キー アルゴリズム処理のためにシステムのリソースと使用率に悪影響を与える可能性もあります。

通信の保護 (DIT)

DIT 制御の目的は、ユーザーがデバイスと信頼される企業リソースや企業アプリとの間で、保護された接続を確立できるようにすることです。通常は VPN が使用されます。VPN のメリットは、デバイスのインターネット接続を暗号化してリモートから企業に安全にアクセスできることです。VPN を使用するとネットワーク パフォーマンスにわずかに影響がありますが、最新のパフォーマンス レベルでは感知されない程度です。一方で、VPN アクセスを使用すると、組織のリソースがデバイス上の他の管理対象外アプリに不必要に公開されてしまいます。そのため VPN アクセスは、特定のアプリにアクセスを限定するようにきめ細かく設定できる必要があります。

Windows 10 は、次の 2 つのタイプの VPN 接続を提供する VPN プラットフォームを備えています。

1.) インボックス プロトコル
   a. IKEv2、PPTP、L2TP (L2TP は PSK と証明書の両方) をベースとした VPN がサポートされています。
   b. インボックス VPN は認証に EAP を使用します。以下の EAP メソッドがサポートされています。
      i. MSCHAPV2
      ii. TLS (Windows Hello、仮想スマート カード、証明書などの証明書ベース認証を使用)
      iii. TTLS (外部メソッド)
      以下の内部メソッドを使用できます。
         1. PAP/Chap/MSCHAP/SCHAPv2
         2. EAP MSCHAPv2
         3. EAP TLS
      iv. PEAP
      以下の内部メソッドを使用できます。
         1. EAP MSCHAPv2
         2. EAP TLS

2.) TLS/SSL 向け VPN プラグイン プラットフォーム
サード パーティ開発者は、VPN プラグイン プラットフォームを使用して、Windows アプリ ストアに対応したダウンロード可能な VPN アプリを作成できます。現在ストアでは、Pulse Secure、Cisco、SonicWALL、Check Point、MobileIron、F5 製のアプリが提供されていますが、2016 年後半にさらに多くのアプリがリリースされる予定です。

Windows 10 は、VPN 接続の簡略化と保護のために、多くのオンデマンド手法と強制適用手法をサポートしています。「常時オン」では、ユーザーがスマートフォンの電源を入れたときやネットワークに変更があったときに自動的に VPN 接続が行われます。「ロックダウン VPN」は、VPN トンネルを介したネットワーク トラフィックのみを許可することでポリシーを強化します。「アプリ トリガー VPN」では、アプリの起動時に自動的に接続が開始されます。「トラフィック フィルター」を利用すると、アプリごとに動作を管理できるため、許可されたアプリからのトラフィックのみを VPN 接続に転送できます。またトラフィック フィルターは、追加レイヤーとして、ホスト宛先属性に基づいてトラフィックをフィルターすることができます。ルールは、アプリ ベースとトラフィック ベースの両方を指定できます。

Android 6 デバイスは、以下のプロトコルと認証方式をサポートする VPN サーバーと通信できます。

- IKEv2/IPsec と、共有シークレット、証明書、PEAP-MSCHAPv2、EAP-TLS、または EAP-TTLS によるユーザー認証
- Pulse Secure、Cisco、SonicWALL、Check Point、Open VPN、AirWatch、MobileIron、F5 Networks SSL-VPN (Google Play アプリ ストアで取得できる適切なクライアント アプリを使用)
- L2TP/IPSec と、MS-CHAPV2 パスワード、仮想スマート カード、ワンタイム パスワード、または証明書によるユーザー認証、共有シークレットによるコンピューター認証
- PPTP と、MS-CHAPV2 パスワード、仮想スマート カード、ワンタイム パスワード、または証明書によるユーザー認証

Android は常時接続 VPN をサポートしており、VPN 接続が確立されるまでアプリからネットワークへのアクセスは許可されません。マルチユーザー デバイスでは、VPN はユーザーごとに適用されるため、デバイスは他のユーザーに影響を与えずに、ユーザーに固有のネットワーク トラフィックを VPN を経由して転送します。プロファイルごとの VPN では、業務用プロファイルを構成し、企業ネットワーク トラフィックのみに業務用プロファイル VPN の通過を許可します。Android 6 は、許可されているアプリ上での VPN 接続をサポートし、許可されていないアプリで

の VPN 接続を防止します。

作業中のデータ保護 (DIU)

作業中のデータ保護の目的は、個人のアプリやサービスとの企業データの共有を制限し、データ損失を防止することです。この目的は、データの暗号化、アプリ管理、セキュア コンテナーなど、複数の方法で達成できます。この 3 つの方法の中で、システム リソースとユーザビリティに与える影響が最も小さいのは、データ暗号化です。セキュア コンテナーとアプリの分離は影響が大きくなります。アプリ内の企業データを管理する手法に加え、メモリ内のデータを保護されたメモリ領域のみで実行することも必要です。

Windows 10 の WIP は、きわめて効率的にデータを保護する手段を提供します。WIP は OS に統合されているため、セキュア コンテナーを利用する必要も、アプリを複製する必要もありません。WIP は定義済みの企業ポリシーに基づいてデータを動的に暗号化します。アプリの種類にかかわらず、企業データの管理に焦点を当てることにより、個人のユーザー エクスペリエンスに影響を与えずに、企業データの可視性と制御を実現します。WIP は、データとアプリを個人用か業務用に分類し、ビジネス データにアクセスできるアプリを判断できます。この分類によって、どのデータを暗号化し、ユーザー間でどのように共有するかも決定されます。AppLocker は、MDM で使用される構成サービスの一部であり、許可するアプリと許可しないアプリを指定できます。アプリの分類は AppLocker によって管理されるので、SDK を使用したアプリの修正やアプリ ラッピングは不要です。管理者が企業情報をワイプするときも、分類されたアプリをデバイスに追加または削除する必要はありません。また、WIP によって既存の個人アプリやデータに変更が加えられることもありません。

Windows 10 における信頼されたアプリとは、業務で使用できるように指定され、保護されている業務データと個人データにアクセスできるアプリです。信頼されたアプリのリストに含まれないアプリは、デバイスや社内共有に格納されている企業情報にアクセスできません。信頼されたアプリから入手したデータは、USB ドライブや個人のクラウド ストレージ アカウントなどの信頼されない場所に保存されると、暗号化されたままになります。また、キーは組織で制御されているため、ユーザーが退職する際には無効化され、ユーザーはデータの格納場所にかかわらずデータの暗号を解除できなくなり、組織のリソースにリモートからアクセスすることも不可能になります。WIP の重要な機能の 1 つは、Windows 10 アプリ (People (連絡先)、Outlook など) が個人データと業務データの両方を同時にサポートできるようにし、業務データには必要な制御や暗号化を提供できることです。たとえば、Microsoft Word の業務用ドキュメントではコピーと貼り付け操作を制限し、個人用ドキュメントでは共有を許可することができます。

IT 部門は WIP を使用して、企業リソースを共有するデバイスに次の 4 つの保護レベルを設定できます。

1. **ブロック:** WIP は不適切なデータ共有を検出すると、ユーザーによる操作を停止します。
2. **オーバーライド:** WIP は不適切なデータ共有を検出すると、操作のポリシー違反についてユーザーに警告します。この保護レベルでは、ユーザーはポリシーを無視してデータを共有でき、その操作が監査ログに記録されます。
3. **サイレント:** WIP はサイレント モードで実行されます。ユーザーが許可されていない操作を行うと、データを暗号化してログに記録しますが、ユーザーへの通知や操作のブロックは行いません。
4. **オフ:** WIP がオフになり、デバイス上のデータは保護されません。

企業は、許可されていないデータ共有 (コピーや貼り付けなど) を完全にブロックするか、監査下での共有を許可するかを選択できます。監査下での共有を許可する場合、ユーザーは WIP 定義の制限をオーバーライドできますが、ユーザーが未許可のデータ共有を試みると、警告がユーザーに表示され、MDM システムによってこの行動がログに記録されます。ユーザーは、この操作を続行するかキャンセルするかを選択できます。新しいドキュメントを作成する際、許可されているアプリ内では、分類を業務用から個人用に手動で変更できます。新しい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この新しい個人用ドキュメントに情報をコピーして貼り付けることはできません。分類イベントはログに記録され、レビュー対象になります。

Office 365 にバンドルされている Microsoft Rights Management (RMS) を使用して、WIP の機能を拡張できます。印刷の許可、ドキュメントや電子メールの転送制御などの RMS による制御を使用して、WIP のアプリ制御、コピーと貼り付けの制御を補完できます。こうした制御は、Windows 10 に加え、Android を含むその他のオペレーティング システムにも拡張できます。

Android for Work は、Android 5 で初めて導入されたセキュア コンテナーであり、Android 6 で刷新されました。このコンテナーによって、仕事用プロファイルと呼ばれる隔離されたワークスペースが作成され、ここに管理対象データが格納されます。プロファイルの管理者は、データの範囲、送受信、ライフタイムを完全に制御できます。Android の旧バージョンでは、管理 API でアプリを「ラップ」する必要がありました。管理対象プロファイルのアプリ、通知、ウィジェットは、個人用アプリと区別しやすいように赤のバッジでマークされ、プライマリ ユーザー インターフェイスに表示されます。プライマリ ユーザーおよび管理対象プロファイルに同一のアプリが存在する場合、アプリはそれぞれの隔離されたデータ空間

を継承します。アプリどうしは、組織に許可されていない限り、プロファイル-ユーザーの境界を越えて直接相互に通信することはできません。また、プロファイル構成設定を通じて管理者に許可されている場合を除き、互いに独立して動作します。管理対象プロファイルのアカウントは、プライマリ ユーザーとは異なります。プロファイルとユーザーの境界を越えて資格情報にアクセスすることはできません。それぞれのコンテキストにあるアプリのみが、それぞれのアカウントにアクセスできます。仕事用アプリが個人用アプリのコピーである場合は、ネットワーク接続、ストレージ、メモリが複製されるため、非常に高性能なデバイスを使用しているのでなければ、ユーザーはリソース管理に注意を払う必要があります。

テストのスコア

情報保護	セキュリティ保証レベル (SAL)	ユーザビリティ
Windows 10	**95**	**100**
Android 6	**67**	**81**

Windows 10 と Android 6 は、Android が強力なキー格納用ハードウェアを実装する Google Nexus デバイスで動作する場合、同様のデータ暗号化レベルを達成しました。ただし Android 6 でも機能の実装状況はベンダーによって異なり、ハードウェアによるキー ストレージとして TPM チップが装備されていない場合もあります。Windows 10 では、PC とモバイル デバイスの両方で一貫した暗号化を達成できます。Windows 10 と Android 6 の VPN 通信にも、特別な長所や短所は確認されず、どちらも高度なセキュリティ保証レベルとユーザビリティを提供しました。データをきめ細かく暗号化できる点を考慮すると、ビジネス データ管理では Windows 10 の方が保証レベルが優れていると考えられます。Android は、コンテナーに暗号化とデータ制御を適用するアプローチを採用しています。WIP はほとんどのユーザーに対して透過的に動作するため、ユーザーは未承認の操作を試みて通知を受けるまで WIP が動作していることに気付かないかもしれません。

脅威対策

どのようなシステムであっても、欠陥がなく、あらゆる外部の脅威から保護されていると考えるのは現実的ではありません。攻撃者は、マルウェアを使用して脆弱性を悪用し、デバイスを感染させます。その手段となるのが、プログラムのエラーと、意図された機能です。プログラム エラーは、攻撃者がアクセス制御を回避して不正なコードをシステムに送り込む手段を提供するため、攻撃者はリモー

トからシステムにアクセスできるようになります。こうした不正コードは、その後このアクセスを悪用して他のマルウェアをダウンロードして実行し、ネットワーク内のシステムに伝搬します。意図された機能は、意図されない用途で使用されてしまいます。たとえばブラウザーは、ローカル オペレーティング システムでのコードの実行を許可します。この手段によって、ウイルスやワームなどの脅威がシステムへのリモート アクセスを取得できるようになります。

セキュリティ侵害されたシステムにおけるデータ損失とマルウェア伝搬の影響を低減するために、OS は回復力を備えるだけでなく、新しいアプリや不明のアプリから、デバイスのメモリやデバイスで実行中のアプリに格納されたファイルへの広範なアクセスや完全なアクセスが不当に取得されないように設計されている必要があります。

デバイスの整合性

Windows 10 デバイスは、セキュア ブート付きの Unified Extensible Firmware Interface を通じ、暗号化された検証済みのデジタル署名を使用して、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します。このプロセスによって、デバイス ハードウェアやファームウェアから OS にまで拡張される信頼チェーンのルートが確立されます。OS ローダーの起動後、トラスト ブートによって残りの Windows ブート関連コンポーネントの信頼性と整合性が検証されます。続いて、Windows カーネルが Windows スタートアップ プロセスの他のすべてのコンポーネント (ブート ドライバー、スタートアップ ファイルを含む) を検証します。改ざんされたファイルがあればトラスト ブートが検出し、Windows の起動前に既知の有効な構成への復元を試みます。トラスト ブートを実行するには、OEM ドライバーやウイルス対策ソリューションなど、オペレーティング システム内のすべてのコードにマイクロソフトの署名が必要です。これがもう 1 つの整合性検証レイヤーとして機能します。すべての Windows 10 アプリには、Windows ストアまたは信頼されたエンタープライズ ストアのデジタル署名が必要です。

マイクロソフトは、「メジャー ブート」という 2 つ目のハードウェア支援プロセスによって、1 つ目の整合性検証プロセスを拡張します。メジャー ブートでは、TPM ハードウェアを使用して、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ベースラインを測定します。TPM は、ベースライン データを切り離して、改ざん攻撃から保護します。Windows 10 は、条件付きアクセスのシナリオで、このベースライン データと共に追加のセキュリティと構成基準を活用します。条件付きアクセスでは、Windows 正常性構成証明 (DHA) クラウド ベース サービスをデバイスの完全な整合性を証明する手段として利用します。DHA サービスを使用する管理システムは、このチェックに基づいてリソースへのデバイス アクセスを許可または拒否しま

す。この機能は、高度でない整合性制御を回避できるルート化されたデバイスを検出するうえで特に重要です。

Android 6 には、デバイスの整合性を検証するために、ベリファイド ブートと定義されている機能が実装されています。Linux カーネルの dm-verity をベースとする Android のベリファイド ブートは、各ブート シーケンスでマルチステージ プラットフォームの検証を実行します。ベリファイド ブートでは各ステージが検証されます。信頼のルートである TEE のハードウェア キーから開始され、次の段階のコードが実行される前に、すべてのバイトの整合性と信頼性が確認されます。この検証はシステム パーティションまで行われます。ベリファイド ブートが実装されずに出荷されたデバイスは、その時点で完全に信頼されたデバイスではないため、サポートされるバージョンにアップグレードすることはできません。

Android はデバイスの整合性を検証しますが、アプリの場合は、アプリの提供元、つまりアプリを検証する証明書に署名したベンダーが信頼のソースになります。Android ではだれでもアプリに署名できます。つまり、だれも明示的に信頼することはできないため、Android アプリ マーケットは悪質なアプリにさらされる可能性があります。Google は Android Play ストアに一定の制御を適用しているものの、Google による規制の対象外であるさまざまな国と地域に多くのアプリ マーケットが存在するためです。アプリにはサード パーティが署名することも、自己署名することもできます。Android は、外部の支援や許可を必要とせずに開発者が生成できる自己署名証明書を使用するコード署名を提供しています。中央の機関がアプリに署名する必要はありません。Android は、アプリの証明書に対して CA による検証を行いません。ユーザーが Android デバイスにアプリ (APK ファイル) をインストールすると、Package Manager によって、この APK が APK に含まれている証明書によって適切に署名されているかどうかが検証されます。証明書の公開キーが、デバイス上の他の APK の署名に使用されているキーと一致した場合、新しい APK は、同様に署名された他の APK とユーザー ID を共有することをマニフェストに指定できます。これは整合性の信頼できるソースにはなりません。

アプリの保護

Windows 10 ではアプリと OS の一部が、AppContainer と呼ばれる専用の分離されたサンドボックス内で実行されます。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機能が定義されています。その機能とは、地理位置情報、カメラ、マイク、ネットワーク、センサーなどの Windows 10 デバイス リソースです。アプリは互いに分離されており、事前定義された通信チャネルとデータ型を使用してのみ相互に通信できます。

多くの不正コードとマルウェア攻撃は、メモリ内のどこに特定のプロセスやシステム関数が存在するかを把握しなければなりません。Address Space Layout Randomization (ASLR) 機能は、実行可能コード、システム ライブラリ、関連プログラミング構成要素のメモリ アドレスをランダム化することで、不正コードによってコードとデータの場所が把握される可能性を低減します。マイクロソフトでは、Windows 10 の ASLR 実装を以前のバージョンよりも強化しており、メモリ空間の予測はさらに難しくなりました。TPM を活用すると、デバイス間での ASLR メモリのランダム化の一意性が高まり、あるシステムで機能している不正コードが別のシステムで機能することはこんなんです。ASLR はアプリ向けの機能ですが、Windows 10 は OS 全体に ASLR を適用してサンドボックスが回避されるリスクを低減します。

Windows 10 には、ユーザーが書き込み可能なメモリ領域に配置されたコードの実行を拒否するデータ実行防止、保護されたランダム ヒープ メモリ割り当て、メモリ管理アルゴリズムが実装されています。この一連のテクノロジによって、脆弱性が悪用の成功につながる可能性をさらに低減しています。こうした防御メカニズムに対抗するために、攻撃者は Return Oriented Programming (ROP) を通じて、システムで既に使用可能なコードを利用します。Windows 10 は OS として初めて、メモリに読み込まれたアプリの制御フローを強制的にロックダウンする、CFG と呼ばれる手法を実装しました。この脆弱性軽減の手法は、ROP 攻撃の防止に役立つだけでなく、ブラウザーにとっても重要な機能です。Microsoft Edge では CFG が有効になっています。これらの一連のテクノロジには、世界で最も多くの企業とコンシューマーに使用されている OS である Windows プラットフォームが数十年にわたって繰り広げてきたマルウェアとの戦いの経験と成果が活かされています。

Microsoft Edge は、AppContainer ベースのサンドボックスを使用して脆弱性からシステムを保護します。Microsoft Edge は、Microsoft ActiveX、Java、Silverlight、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を実行しないため、リスクが大幅に低減されます。SmartScreen は、フィッシング対策 URL フィルターを提供するほか、アプリケーション評価を使用してダウンロードをチェックし、ドライブバイ攻撃の防止にも効果を発揮します。SmartScreen は、サイトで悪質なコンテンツを検出したとき、そのサイト自体をブロックでき、状況によってはサイト内の特定のコンテンツのみをブロックすることもできます。

Android アプリは、カーネル レベルのアプリ サンドボックスで実行されます。各 Android アプリには、Android システムによって一意のユーザー ID が割り当てられ、そのユーザーとして独立したプロセスで実行されます。Android サンドボックスは、Security Enhanced Linux を使用してすべてのプロセスに強制アクセス制御 (MAC) を適用します。既定では、Android アプリはシステム リソースの限定的な範囲にしかアクセスできません。Android アプリからリソースへのアクセスは、シス

テムによって管理されます。リソースが不正にまたは悪意をもって利用されると、ユーザー エクスペリエンス、ネットワーク、デバイス上のデータに悪影響を与える可能性があります。アプリの機能を制限するために、特定の API を意図的に用意しない、役割の分離を使用する、特定の API の使用を信頼されたアプリに限定するなど、さまざまな手法が使用されています。

ただし、サード パーティ製アプリを導入する場合は、ユーザーがアプリのアクセス許可を手動で承認または拒否します。Android 6 を初めて使用する場合、アクセス許可はインストール時にアプリに付与されるのではなく、実行時にアプリが要求します。Android for Work の場合は、組織の管理者が、ユーザーの仕事用プロファイルに展開されているアプリのアクセス許可を管理できます。また、ユーザーがいつでもアプリのアクセス許可のオンとオフを切り替えられるようになりました。十分に理解せずにユーザーがアプリにアクセスを承認するケースがよく見られますが、アプリの整合性を保証するためのアプリ プロバイダーの署名で証明書が検証されていないため、デバイスと情報が悪意のある第三者にさらされる危険性があります。

テストのスコア

脅威対策	セキュリティ保証レベル (SAL)	ユーザビリティ
Windows 10	**100**	**100**
Android 6	**76**	**90**

Windows 10 は、Android 6 よりも優れた 2 つの脅威対策を提供します。Windows 10 のメジャー ブートは、ハードウェアを使用してシステム ブート プロセスの整合性を測定します。Android には、ハードウェアの信頼のルートがありますが、この機能は、ルート化されたデバイスの暗号化ドライブの認証を制限するなどの条件を定義するリモート構成証明には対応していません。もう 1 つは、メモリを破損させる脆弱性に対抗する制御フロー ガード (CFG) という制御フローの整合性機能を通じたメモリ保護強化です。Windows 10 はテストで、最高レベルのセキュリティ保証とユーザビリティを示しました。しかもこうした機能は、日常的にユーザーに意識されることはありません。

管理とレポート

ニーズやデバイス ポリシーは組織によって異なりますが、以下の 3 つのシナリオのいずれかに該当する傾向にあります。

1. デバイスはユーザーの所有物であるという理由や、ポリシーで厳格な制御

が求められていないという理由で、デバイスのパーソナライズをユーザーに許可する組織

2. 組織がデバイスを所有しており、セキュリティが重要な考慮事項であるという理由で、ユーザーにデバイスのパーソナライズを許可しないか制限付きで許可する組織
3. 個人デバイスと企業デバイスの組み合わせをサポートし、両方のシナリオに対応するポリシーの混在を必要とする組織

デバイス管理の目的は、コストとダウンタイムを最小限に抑えながら、モバイル通信ネットワークの機能とセキュリティを最適化することです。デバイス管理は、可視化、デバイス構成、アプリ管理、運用サポートという 4 つの重要な機能を提供します。デバイス管理によって、企業リソースへのアクセスを要求するモバイル デバイスを認識できます。企業はだれがどのデバイスを所有し、所有者にどのアプリが提示されるかを把握できるようになり、管理者はデバイスの構成と保守を行い、企業ポリシーに従った企業リソースへのアクセスを提供できるようになります。さらに、モバイル オペレーティング システム製造元によってサポートされている操作を使用して、リモートからデバイスの管理とサポートを行うことができます。こうしたデバイス管理を通じて、モバイル デバイスは常に最新の状態に更新されるようになり、ユーザーは緊急時にもデバイスにアクセスでき、組織はデバイスの紛失や盗難が発生しても責任を負う必要がなくなります。

デバイスの登録

管理ツールの最新バージョンは、Windows 10 を実行するあらゆるタイプのデバイスを管理できます。グループ ポリシー、Windows Management Instrumentation、PowerShell スクリプト、Orchestrator Runbook、System Center ツールなどの既存のエンタープライズ管理ツールは、引き続き PC 上の Windows 10 で使用できます。Windows 10 を実行するデバイスにも、デバイスの登録と管理のために MDM エージェントが組み込まれています。MDM ベンダーは、Windows 10 デバイスとの通信に Microsoft MDM プロトコルを使用し、Windows 10 デバイスは Open Mobile Alliance の Device Management プロトコル 1.2.1 をサポートしています。MDM クライアントは、ポリシー設定の構成、アプリと更新プログラムの展開、その他の管理タスクの実行を MDM に許可します。MDM は、MDM クライアントを通じて構成要求を送信し、インベントリを収集します。

表 1: Windows 10 と Android 6 における MDM サポート状況

	Windows 10	Android for Work
BlackBerry	√	√
Citrix	√	√

	Windows 10	Android for Work
Google		√
IBM MaaS 360	√	√
Lightspeed Systems	√	
Matrix 42	√	
Microsoft Intune	√	√
MobileIron	√	√
SAP	√	√
Soti	√	√
Symantec	√	
VMWare AirWatch	√	√

個人所有の Windows 10 デバイスには、職場の Microsoft アカウントを使用します。これは企業による管理とリソース アクセス専用のデバイスのサブ アカウントとして機能します。管理者がプロビジョニング パッケージを作成し、ユーザーにパッケージへのアクセスを提供します。ユーザーはこのパッケージを適用し、企業環境にデバイスを登録します。企業所有デバイスは、プライマリ デバイス認証としてドメイン アカウントを使用して企業に登録されます。Azure AD との統合によって、メール、Word、OneDrive などのネイティブ アプリ、Azure AD Web アプリ、オンプレミス リソース、ビジネス向け Windows ストアへのシングル サインオンが可能になります。管理者がプロビジョニング パッケージを作成し、適用してからデバイスをユーザーに配布することも、ユーザーが初期構成時にプロビジョニング パッケージを適用することもできます。

Android の登録では、ユーザーは Google Play ストアからエージェント アプリをダウンロードする必要があります。ユーザーにデバイスへの Device Policy アプリのインストールを義務付ける組織もあります。その場合は、このアプリをインストールしないと、デバイスとのメール、予定表、連絡先の同期がブロックされることがあります。

デバイス構成

Windows 10 では、組み込みの MDM クライアント機能を使用することで、以下に示すような MDM で管理された制限を複数の項目に適用できます。これらの機能は、互換性のあるすべての MDM システムに公開されています。

- デバイスのパスコードの要求と要件の指定
- 内部ストレージ暗号化の強制
- SD カード使用の有効化と無効化
- 開発者ロック解除の無効化
- モバイル データやデータ ローミングに対する VPN の許可
- ActiveSync 設定の構成と配布
- Wi-Fi および Wi-Fi センサー ホットスポット自動接続の使用の許可
- ルート、CA、発行者証明書など、さまざまな種類の証明書の構成
- カメラ、Cortana、位置情報データ、利用統計情報、Bluetooth、インターネット共有、Microsoft アカウント以外のアカウントの追加に対する制限
- 検索での位置情報の使用の禁止
- Microsoft アカウントの接続認証の拒否
- 複数のデバイス間での [設定を同期] の禁止
- Windows ストア以外のアプリの制限
- デバイスの検索と、階層リンク履歴の確認
- 紛失したデバイス、盗難に遭ったデバイス、非準拠のデバイスの選択的ワイプまたはフル ワイプ
- デバイスの手動での使用停止の制限

Android 6 では、管理者は以下のセキュリティ ポリシーを設定できます。

- デバイスのパスワードの強度
- デバイスのパスワードの長さ
- デバイスがワイプされるまでの無効なパスワードの入力回数
- 最近失効し、ブロックされるパスワード数
- デバイスのパスワード失効日までの日数
- デバイスが自動的にロックされるまでのアイドル時間 (分)
- アプリケーションの監査
- リモートからのデバイス アカウント削除
- デバイスのリモート ワイプ
- Device Policy アプリ バージョンの要件
- 最後の同期からワイプまでの日数
- セキュリティが侵害されたデバイスのブロック

管理者は、MDM エージェント アプリを使用して、Wi-Fi ネットワークの構成やネットワーク アクセス用証明書の管理も行うことができます。ネットワーク名とパスワードを知っているユーザーのみがネットワークに接続できるように、ネットワークの詳細を隠すこともできます。

アプリケーション管理

Windows 10 は、アプリの展開のためにビジネス向け Windows ストアのサブスクリプションと MDM の統合をサポートしています。MDM システムを使用してデバイスに基幹業務 (LOB) アプリを直接展開するには、すべてのソフトウェア パッケージが証明機関によってデジタル署名されている必要があります。企業は最大 20 個の自己署名付き LOB アプリを Windows 10 Mobile デバイスに配布できます。組織のデバイスが Windows 10 Mobile Enterprise を実行していれば、20 個以上のアプリを配布できます。Windows 10 の WIP で AppLocker を使用して、許可するアプリと許可しないアプリを指定し、アプリの分類を管理できます。アプリ管理では、Windows ストア、プライベート ストア、自動更新、サイド ローディングを制限したり、同一アプリで複数のユーザーがデータを共有したりすることも制限できます。

Android は、Google Play またはサード パーティ アプリ ストアを通じたアプリの展開をサポートしています。すべてのトランザクションは、企業が管理するモデルで匿名で行われます。Android では、すべてのアプリ管理トランザクションに Google Play の使用を義務付けており、サイドローディングを禁止しています。MDM のアプリ管理機能には、アプリのインストールと削除、特定のアプリのインストールの制限、アプリの有効化と無効化、現在のアプリ状態の照会、アプリの動作の制御、アプリ通知の制御などがあります。

リモート管理

MDM は、Windows 10 デバイスに、ハードウェア インベントリ、デバイス名、ユーザー名、メール アドレス、オペレーティング システムとバージョン、証明書、位置情報、Wi-Fi MAC アドレス、デバイス ID、所有者の指名、基本入出力システム、画面の解像度、OS の言語、Windows ストア アプリとそれ以外のアプリのインベントリを照会できます。

Android 6 デバイスでも、ハードウェアのシリアル番号、デバイス名、Wi-Fi MAC アドレスなど、同様のさまざまな情報を照会できます。また、デバイスのバージョンと制限事項、デバイスにインストールされたアプリのリストなど、ソフトウェア情報も照会できます。

マイクロソフトでは、年間 2 ～ 3 回のペースで Windows 10 更新プログラムを提供するように予定しており、新しい機能も継続的に提供していきます。Windows 10 は、Windows Update から直接ソフトウェア更新プログラムを取得します。Windows 10 Mobile では、展開前に更新プログラムを選択することはできませんが、Windows 10 Mobile Enterprise では、広範囲のユーザーに配布する前に、企業が更新プログラムの選定と検証を行うことができます。

Google は、Android のネイティブ無線メカニズムを使用して、セキュリティ更新プログラムを毎月、OS 更新プログラムはそれより少ない頻度で提供しています。ただし Google の Nexus Android デバイス以外の更新状況は、ハードウェア製造元やモバイル キャリアによる実装ごとに異なります。そのため Android デバイスは、デバイス自体が Android の最新バージョンをサポートしていても、Google の更新発行時に更新プログラムを受け取れない可能性があります。2016 年 5 月時点では、セキュリティ更新プログラムをリリース時に常に提供している OEM 製造元は BlackBerry のみです。ただし BlackBerry も、OS 機能の更新には 6 か月かかっています。

診断と監視

Windows 10 は、問題の追跡や修復操作の実行に役立つ監査情報を提供します。この情報により、デバイス構成を組織の標準に準拠させることができます。Windows 10 のリモート デバイス正常性構成証明は、測定されたブート データを使用してデバイスの正常性状態を検証します。MDM はこの正常性状態を活用し、クライアント ポリシーと関連付けて、デバイスの現在の状態に基づいて条件付きアクセスを許可します。デバイスは、マルウェアに感染していないこと、セキュリティ ツールがアクティブであること、最新のパッチ レベルまで完全に更新されていることを証明する必要があります。証明できなければ、指定のリソースへのアクセスが拒否されます。Android 6 は、デバイス上でリモート正常性構成証明を実行する手段を提供していません。また、同様の機能も装備されていません。

マイクロソフトは、Windows 10 の利用統計情報を定期的に収集しています。利用統計情報は、Connected User Experience and Telemetry コンポーネントによってアップロードされるシステム データです。これは、基本的には OS の診断とユーザー エクスペリエンスの向上のために使用される匿名データです。Windows 10 Mobile で利用統計情報機能を無効にするには、Windows 10 Mobile Enterprise エディションにアップグレードする必要があります。Windows 10 Mobile ではこの機能を無効にできません。Windows 10 Mobile Enterprise では、企業は、「セキュリティ」レベルなど、サポートされる 4 つのレベルで利用統計情報を構成できます。「セキュリティ」レベルでは、最新のセキュリティ更新プログラムで Windows デバイスの安全性を維持するために必要な利用統計情報のみが収集されます。Windows からマイクロソフトにデータが送信されないようにするには、Windows Defender 利用統計情報と悪意のあるソフトウェアの削除ツールのレポートを無効にし、Microsoft サービスへのその他のすべての接続を無効にします。

Google は、広告を配置するために、Google アカウントに関する情報に加え、位置情報やさまざまな個人情報を収集しています。この設定は、Android の個人用アカウントで構成できます。企業がデバイスからのデータ収集を管理できる設定はあ

りません。

テストのスコア

管理	セキュリティ保証レベル (SAL)	ユーザビリティ
Windows 10	**93**	**93**
Android 6	**79**	**82**

管理面では、Windows 10 の方がユーザーと管理者のユーザビリティへの影響が低く抑えられています。Windows 10 は、Azure AD 認証を活用した単一ステップでのドメイン認証、プロビジョニング、デバイス管理をサポートしています。Android 6 では、ドメイン アカウントのアプリ認証はサポートされていますが、デバイスはサポートされていません。この方法は効果的ですが、単一のステップで一貫したユーザー認証を行うことはできません。また、デバイス全体に提供する保証を強化するわけではありません。Windows 10 では、リモート正常性構成証明によって、ハードウェアからソフトウェアまでデバイスのコンプライアンス状態を確認し、条件付きアクセスによって非準拠デバイスのアクセスを制限します。Android は、同様のリモート正常性構成証明機能を備えていないため、デバイスのルート化を検出する機能が制限されています。ルート化は Android エコシステムで広く行われています。その目的は多くの場合、ベンダーの付属ソフトを排除することや、デバイスを新しい Android ビルドに更新することです。マイクロソフトもセキュリティ修正プログラムの一貫したスケジュールを維持しており、Windows 10 にはセキュリティ修正プログラムを OS 更新プログラムとは別に提供する手段を備えています。修正プログラム管理は組織のセキュリティにとって非常に重要なプロセスです。

結論

2 つの OS の回復力と管理機能について、ラボ環境で包括的な比較分析を実施した結果、Pique Solutions は Windows 10 の方が Android for Work 搭載の Android 6 よりも高いレベルのセキュリティ保証とユーザビリティを企業に提供しているという結論に至りました。

Windows 10 は Android 6 よりも認証機能で高いスコアを記録しました。主な理由は、パスワードやセカンダリ トークンを必要としない 2 要素認証機能が搭載されていること、そしてデバイス、アプリ、ドメイン認証で FIDO 2.0 がサポートされ

ていることです。FIDO 2.0 は、非対称キー、ハードウェア ベースのキー ストア、構成証明を使用する多要素認証をサポートします。FIDO のメンバーである Google は、Android で FIDO のサポートを計画していますが、最初は Web アプリのみが対象です。パスワード不要の 2 要素認証と FIDO 2.0 という 2 つの認証方式は、企業の ID 管理に、現在達成可能な最高レベルのセキュリティ保証を提供します。パスワードが排除されると、攻撃者は攻撃を仕掛けるためにデバイス自体が必要になります。生体認証が採用されれば、そのスプーフィング手法も必要になります。パスワードの排除は、セキュリティ保証とユーザビリティの両方を改善するセキュリティ手段となります。

Windows Hello フレームワークは、生体認証を使用した強力な 2 要素認証を提供するため、企業 ID を保護すると共に、パスワードの必要性や使用を最小限に抑えることができます。Windows Hello コンパニオン デバイス フレームワークにより、Windows 10 スマートフォンを使用して Windows 10 PC のロックを解除したり、他のコンパニオン デバイスを使用して Windows 10 Mobile デバイスのロックを解除したりできます。認証に 2 つ目の要素を追加するだけで、組織では大幅な効率化とコスト削減を図ることができます。Android 6 では、Android 指紋認証 API が導入されました。現在の OEM デバイスの生体認証機能には差があるため、この API は非常に重要です。マイクロソフトのハードウェア要件は、他人受入率 (FAR) 100,000 件中 1 件ですが、Android 6 では 50,000 件中 1 件です。FAR は、生体認証がスプーフィングされる可能性を特定するために最も重要な単独のメトリックです。

Windows 10 と Android 6 は共に、デバイス暗号化で AES-128 を使用していますが、Android 6 の場合はハードウェア キー ストレージが実装されているかどうかがベンダーによって異なります。Google Nexus デバイスには、ハードウェア キー ストレージが搭載されています。Windows 10 デバイスの場合、TPM チップの搭載が要件になっています。Windows 10 と Android 6 の VPN 通信には、特別な長所や短所は確認されませんでした。どちらの OS でも、アプリ単位やオン デマンドなど、同じレベルの接続オプションが用意されています。

Windows 10 も Android for Work も強力な AES 暗号化機能を提供しますが、ポリシーをベースに動的なデータ暗号化を行う Windows 10 の方が高度なセキュリティ保証を提供しています。Android は暗号化されたセキュア コンテナーを使用します。おそらくポリシー ベースのデータ暗号化を使用する最大のメリットは、企業データを保護しながら、デバイスのユーザビリティに与える影響を低く抑えられる点です。ユーザーは、企業に許可されていない操作を行うまで、ポリシー ベースの暗号化の存在に気付かないかもしれません。

Windows 10 は、リモート正常性構成証明によって、ハードウェアからソフトウェアまでデバイスのコンプライアンス状態を確保し、条件付きアクセスによって非

準拠デバイスのアクセスを制限します。Android デバイスは、Trusted Execution Environment を使用して整合性を検証する機能を提供しますが、機能の実装状況はデバイスやベンダーによって異なります。リモート チェックや条件付きアクセスは提供していません。Windows 10 の制御フロー ガード (CFG) は、メモリ内の想定された場所でアプリが実行されるかどうかを検証します。CFG がなければ (Android 6 に CFG はなし)、攻撃者は良性のアプリを使用してメモリ保護を迂回し、マルウェアを実行できます。これらの機能はどちらもエンド ユーザーに対して透過的に実行されますが、企業リソースへのアクセスが拒否された場合はユーザーに通知されます。

総合すると、Windows 10 は、最高レベルのリスク許容要件に対応できる高度な回復力を備えています。さらに重要なこととして、エンド ユーザーに透過的にセキュリティ保証が提供されます。ユーザビリティに与える影響は、あるとしても非常に低く抑えられており、認証などの機能はむしろユーザビリティを高めています。

管理面では、Windows 10 はデバイス登録時に個人所有デバイスと企業所有デバイスの両方でドメイン アカウントを活用する「ワン ステップ認証プロセス」を使用するため、ユーザビリティに対する影響が少なくなっています。あらゆるセキュリティ戦略で重要となるセキュリティ修正プログラムへの対応では、Windows ストアがすべての Windows 10 デバイスに更新プログラムをプッシュできるため、Windows 10 デバイスは常に最新のセキュリティ更新プログラムを適用した状態を維持できます。Android デバイスでは製造元がアクティブ デバイスの更新を担当するため、すべてのデバイスにセキュリティ更新プログラムが配信される保証がありません。Google は OEM 製造元に、Google 以外のデバイスでもこのプロセスも改善するよう働きかけていますが、現在タイムリーにセキュリティ更新を受信できるのは Google Nexus デバイスのみです。

今回の Android for Work 搭載の Android 6 との比較分析を通じて、Windows 10 は 4 つすべての領域で Android よりも高度なセキュリティ保証とユーザビリティを提供していることが実証されました。