PIQUE SOLUTIONS

Windows 10 と iOS 9

ラボ環境における機能比較: Windows 10 と iOS 9 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 Apple の iOS 9 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。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、モバイル デバイス全体で共通です。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、スマートフォン、タブレット、PC 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すると共に、使いやすさも実現しています。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。

iOS 9 は、これまでの iOS バージョンで段階的にエンタープライズ環境向けに改善を図ってきました。iOS 9 は、ハードウェア ベースのセキュア ブート チェーンや、アプリ管理に対する厳格な制御を導入することで強力なレベルの保証を提供していますが、2 要素認証を利用するにはサード パーティ製品との統合が必要です。また Windows 10 と比較すると、企業データの管理と保護に伴ってユーザビリティに大きな影響が発生します。

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、iOS 9 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 iOS 9 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 (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 (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 (DIU): 保護された実行環境、データ管理、データ共有、メモリ暗号化

脅威対策

- デバイス整合性: ブート/アプリ/OS/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

デバイス/アプリ管理

- 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、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
- リモート管理: 資産管理、OS とセキュリティの更新プログラム、紛失したデバイス、リモート ワイプ
- 診断/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および 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。

1. Lumia 950 — Windows 10 Mobile
2. Surface Pro 3 — Windows 10 Enterprise
3. iPhone 6s — iOS 9.3
4. iPad Mini 4 — iOS 9.3

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テストするために MDM ベンダーを活用しました。たと

えば、Microsoft Intune は iOS 9 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。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独立系 MDM プロバイダーである 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 iOS 9 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 iOS 9 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 iOS 9 に比べ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 の 2 要素デバイス認証は、スマート カード トークン ベースの認証と同レベルのセキュリティ保証を提供するが、追加のインフラストラクチャ コストはかからない。
- iOS 9 デバイスの認証は、1 つの要素しか使用しない。
- Windows 10 の生体認証はパスワードに取って代わる機能で、ユーザビリティにもセキュリティ保証にもプラスの効果をもたらす。
- iOS Touch ID は、ユーザーの利便性向上のためにパスワードの代わりに使用できるが、パスワードに完全に取って代わるわけではなく、パスワードも使用される。
- Windows 10 は、FIDO 2.0 を実装した初のエンタープライズ向けオペレーティング システムであり、現在利用可能な認証のうち最も高度なセキュリティ保証レベルを提供する。FIDO 2.0 では非対称キーを使用した複数要素認証とハードウェアベースの正常性構成証明が採用されている。

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。
- iOS 9 は、個人用アプリとの企業データの共有を制限する制御機能を提供するが、デバイス レベルのファイル共有には対応していない (AirDrop は、ハードウェア制御として別途構成されている)。

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。
- iOS 9 では、ハードウェアの信頼のルートがチップ製造時に書き込まれ、無条件に信頼される。
- 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 10 は、Azure AD の統合を活用して 1 つのステップでドメイン認証、プロビジョニング、管理を行う。
- 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。
- iOS 9 は、リモート正常性構成証明のような機能を備えていないため、ジェイルブレイク検出機能が制限される。

- 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パッチ更新スケジュールを維持している。パッチ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。

テストのスコア

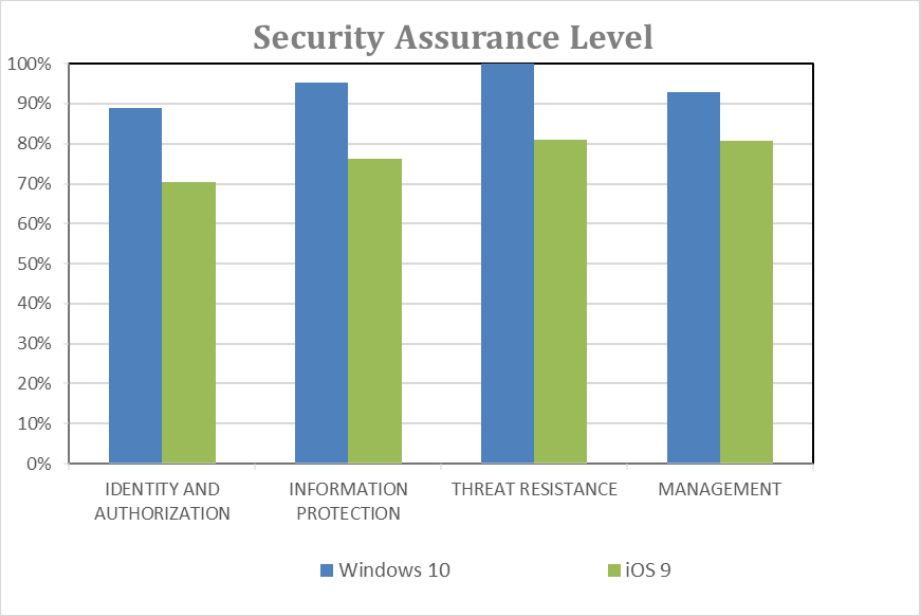

図 1.Windows 10 と iOS 9 のセキュリティ保証に関するラボ テストのスコア

総合すると、Windows 10 は測定されたすべてのカテゴリで iOS 9 よりも一貫して高いスコアを記録しました。特に ID 管理では、Windows 10 はユーザーとエンタープライズに統合認証エクスペリエンスを提供できます。データ保護の面では、Windows 10 がデータに適用する暗号化と制御機能は iOS 9 よりも効率的であり、ユーザー エクスペリエンスに対して透過的であることがわかりました。脅威対策としては、Windows 10 には iOS に見られない新しいメモリ保護機能が追加されており、この機能もユーザーに完全に透過的でした。管理面では、Windows 10 は非常に幅広い OS 管理手法と、ドメイン アカウントを使用した合理的なデバイスのプロビジョニングおよび構成のプロセスを提供しています。また Windows 10 は、リモート正常性構成証明に基づいた条件付きアクセスをデバイスに提供します。

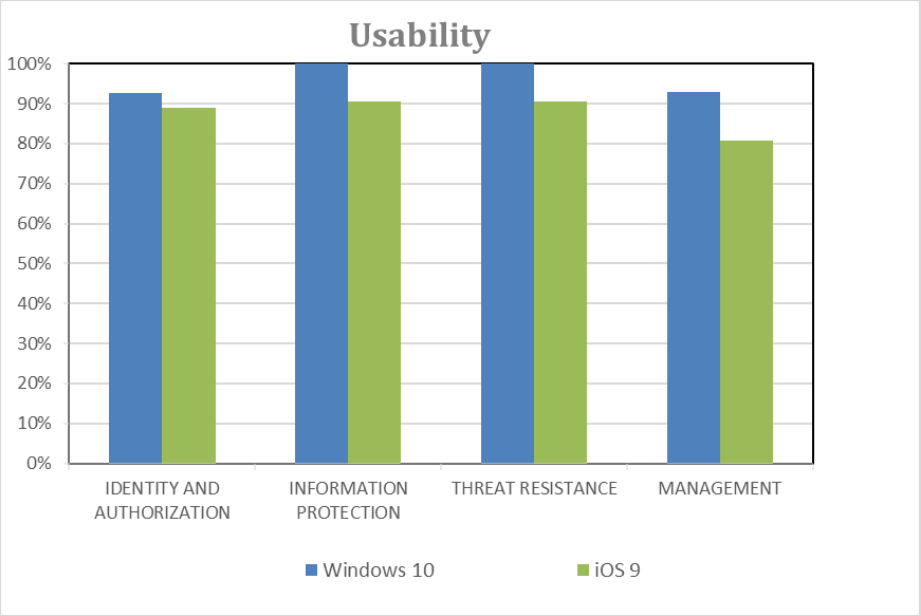

図 2.Windows 10 と iOS 9 のユーザビリティに関するラボ テストのスコア

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 エンタープライズ ドメイン認証に対して 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 Active Directory のほか、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。

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。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。

Apple は iOS 9 で 2 要素認証を提供していますが、これは Apple ID 向けの機能です。エンタープライズ レベルの 2 要素認証ではありません。Apple ID の 2 要素認証では、ユーザーは新しいデバイスに初めて Apple ID とパスワードを入力するときに、6 桁の確認コードで ID を検証するように求められます。このコードは、サポートされている他のデバイスか電話番号に届きます。認証されたユーザーは、指定されたタイムアウト期間中と、このデバイスの全情報を消去した場合やパスワードを変更する必要がある場合を除いては、再びこのデバイスで認証を行う必要がありません。これは大きな第一歩ではありますが、オプションのプロセスであるため、ユーザーは必ずしもこの機能を理解したり使用したりしません。この認証方法によってパスワードが完全に排除されるわけではなく、パスワードが主要な認証手段であることは今後も変わりません。

iOS 9 では、iOS アプリのエンタープライズ ドメイン 2 要素認証を使用するためにサード パーティ製のアプリが必要です。デバイスのエンタープライズ 2 要素認証にはまだ対応していません。iOS 9 では、証明書ベースのシングル サインオン (SSO) を使用したエンタープライズ ネットワークへの認証をサポートしています。Safari は、標準の iOS ネットワーキング API を使用するサード パーティ製アプリへの SSO をサポートしています。サード パーティ製アプリは 2 要素認証をサポートしていますが、これはまだパスワード ベースの 2 要素システムです。

生体認証のサポート

Windows Hello は、Windows 10 で生体認証サインイン オプションを使用するための拡張フレームワークです。ユーザー固有の生体認証 ID によってデバイスへのアクセスを認証しま

す。現在 Windows Hello は、指紋、顔認識、虹彩スキャンをサポートしていますが、現在サポートされている生体認証が新しいハードウェアによって拡張される可能性があります。

Windows 10 は、生体認証とデバイスの他のセキュリティ コンポーネントを統合します。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。

Touch ID は Apple の指紋認証テクノロジです。このテクノロジを有効にすると、ホーム ボタンをタッチするだけで、iOS 9 デバイスのロックを解除したり、iTunes Store での購入時の認証を行ったりすることができます。アプリ ストアで配布されているアプリも、認証のために Touch ID と統合できます。静電容量式の金属リングは、指の接触を検出したときにスキャナーを起動し、高解像度の指紋写真を撮ります。iOS 9 は指紋を数式に変換して暗号化し、ハードウェア チャネルを介して Apple ハードウェア チップセット上の Secure Enclave に転送します。

アプリ ストアのアプリの場合は、認証状態が確認されるか、パスワードが使用されるか、すべてがキャンセルされた場合のみにのみ制御が戻ります。iOS 9 では、ACL で保護されている項目はバックアップされず、デバイス間での同期も行われません。開発者はアプリのユーザー指紋データに一切アクセスできません。注意すべき点は、Touch ID はデバイスへの代替アクセス方法を提供する便利な機能ではありますが、パスワードを使用すると指紋認証を迂回できてしまうことです。

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**
iOS 9	**70**	**89**

Windows 10 の 2 要素デバイス認証は、スマート カード トークンベースの認証と同レベルのセキュリティ保証を提供しますが、追加のインフラストラクチャ コストはかかりません。デバイスとユーザーを 2 つの要素として使用できます。さらに、この 2 要素認証は OS に限定されず、アプリと Web サイトもサポートします。セキュリティの視点で言うと、攻撃者が攻撃を仕掛けるには、ユーザーの物理デバイスとユーザーの生体認証情報が必要になるわけです。ユーザーの生体認証データは Windows 10 内のどこにも格納されていないた

め、攻撃者にはユーザーも必要になります。ユーザビリティの視点で言うと、ユーザーは何も記憶する必要がなく、一般的な管理作業であるユーザー パスワードのリセットも不要になります。また、コストの節約にも貢献できます。

Windows 10 と iOS 9 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、パスワードを完全に排除できるフレームワークを提供する Windows 10 が明らかに iOS 9 をリードしています。iOS 9 が現在サポートしているのは指紋認証のみです。指紋認証も PIN の代替オプションとして使用できますが、PIN に置き換わるものではありません。

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。

iOS 9 は、スマートフォンのハードウェアに格納されている 256 ビットのデバイス固有の秘密キーを使用します。これらの値が他の場所に格納されることはありません。このキーを読み取れるソフトウェアやハードウェアはありません。デバイス固有のキーとパスコード

の組み合わせによって、デバイス内のデータを保護するパスコード キーが生成されます。これは、攻撃者はリモートからデバイス固有のキーを抽出できることはないという考えに基づいています。

ファイルのコンテンツはファイルごとのキーによって暗号化され、クラス キーでラップされ、ファイル システム キーで暗号化されたファイルのメタデータに格納されます。クラス キーはハードウェア キーによって保護されます。また、一部のクラスではユーザーのパスコードも保護されます。iOS 9 は、メッセージ、写真、連絡先、通話履歴など、さらに多くのアイテムにこの機能を拡張しています。

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、最新のネットワーク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。

- インボックス プロトコル
  - 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。
  - 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。
    - MSCHAPV2
    - 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)
    - TTLS (外部メソッド)
      - 以下の内部メソッドを使用できます。
        - PAP/Chap/MSCHAP/SCHAPv2
        - EAP MSCHAPv2
        - EAP TLS
    - PEAP
      - 以下の内部メソッドを使用できます。
        - EAP MSCHAPv2
        - EAP TLS

- 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、ストアから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 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。

iOS 9 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: IPv4 と IPv6 の両方と、以下をサポートします。
  - 認証方式: 共有シークレット、証明書、EAP-TLS、EAP-MSCHAPv2
  - Suite B 暗号化: ECDSA 証明書、GCM を使用した ESP 暗号化、Diffie-Hellman グループの ECP グループ
  - 追加機能: MOBIKE、IKE フラグメンテーション、サーバー リダイレクト、スプリット トンネル
- L2TP over IPSec: MS-CHAP v2 パスワード、2 要素トークン、証明書によるユーザー認証、共有シークレットまたは証明書によるコンピューター認証
- SSL VPN: パスワード、2 要素トークン、サード パーティ VPN クライアントを使用した証明書によるユーザー認証
- Cisco IPSec: パスワード、2 要素トークンによるユーザー認証、共有シークレットと証明書によるコンピューター認証
- PPTP: MS-CHAP v2、パスワード、証明書、2 要素トークンによるユーザー認証
- Pulse Secure、Cisco、Aruba Networks、SonicWALL、Check Point、Palo Alto Networks、OpenVPN、AirWatch、MobileIron、NetMotion Wireless、F5 Networks SSL-VPN (アプリストアの適切なクライアント アプリを使用)

iOS 9 は、プロファイル構成を通じて定義された証明書ベースの認証を使用するネットワークに対して VPN オンデマンドをサポートしています。また、アプリごとに使用する VPN を指定できる機能もサポートしており、VPN 接続を極めて細かく設定できます。MDM を使用すると、管理対象アプリごとや Safari の特定のドメインごとに接続を指定できます。さら

に、VPN 常時接続もサポートしています。MDM で管理され、Apple Configurator または Device Enrollment Program で監視されているデバイスに対して構成できます。VPN 常時接続では、組織に戻るすべての IP トラフィックがトンネリングされます。既定のトンネリング プロトコルである IKEv2 は、転送されるトラフィックをデータの暗号化によって保護します。

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 Windows Information Protection (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。

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。企業情報は、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、企業リソースにアクセスするデバイスに次の 4 つの保護レベルを設定できます。

- **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。
- **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。
- **サイレント:** WIP はサイレント モードで実行されます。ユーザーが不適切な操作を行うと、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。
- **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、EMM 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、iOS 9 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。

iOS 9 は、管理対象アプリを使用して企業データの共有を制限します。無償アプリ、有料アプリ、企業アプリを管理対象アプリに含めることができます。管理対象アプリには、以下の制限と機能があります。

- Managed Open In
  - 管理されていないソースから管理されている場所にドキュメントを出力することをを許可します。この機能を制限すると、管理対象の場所で個人的なソースとアカウントを使用してドキュメントを開くことができなくなります。
  - 管理されているソースから管理されていない場所にドキュメントを出力することを許可します。この機能を制限すると、個人で使用している場所で管理対象のソースとアカウントを使用してドキュメントを開くことができなくなります。
- アプリ開発者は、管理対象アプリとしてアプリをインストールした後に、設定可能な構成を特定できます。
- アプリ開発者は、MDM を使用して読み取り可能なアプリ設定を特定できます。
- 管理対象アプリの iCloud または iTunes へのバックアップの作成を防止します。

- Safari で管理対象ドメインからダウンロードしたドキュメントは管理対象と見なされます。
- 管理対象アプリから iCloud へのデータの格納を防止します。

個人で使用したいアプリが管理対象と見なされた場合、ユーザーは個人用ドキュメントを管理する別の方法を見つける必要があります。ユーザーが Adobe Acrobat Reader DC などの最新の管理対象外アプリを使用している場合に、企業がこのアプリを管理対象アプリとして分類し直すと、このアプリでは未承認データの使用がサポートされなくなります。その結果、関連するアプリで添付ファイルを開くというモバイル デバイスでは一般的な操作を行うのに、余計な手間が発生します。また iOS 9 には、管理対象アプリから iCloud や iTunes へのデータのバックアップを防止する制限もあるため、ユーザーが管理対象アプリを再インストールしても、データを復元することができません。

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**
iOS 9	**76**	**90**

デバイス暗号化機能の比較では、ハードウェア ベースのキー格納の使用など、Windows 10 と iOS 9 の機能は同等という結果が出ました。どちらのプラットフォームも、この分野では強力な機能を提供しています。Windows 10 と iOS 9 の VPN 通信にも、特別な長所や短所は確認されませんでした。どちらのプラットフォームの VPN 機能も強力と言えます。

Windows 10 と iOS 9 は同程度の強力な暗号化機能を提供しますが、データ レベルできめ細かく暗号化できる点を考慮すると、Windows 10 の方が優れていると考えられます。iOS 9 のアプローチでは、アプリに暗号化を適用します。アプリ レベルの暗号化は、WIP を使用してデータ レベルでデータ保護を提供する Windows 10 の機能の一部です。WIP は、OS や企業アプリ内で高度に統合されているため、ユーザー エクスペリエンスに与える影響も抑えられていますが、iOS 9 ではアプリを個人用か業務用として指定しなければならず、両方の用途に使用できる機能を搭載していません。

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、その後このエラー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。

iOS 9 では、セキュア ブート チェーンがデバイス、ファームウェア、ブートローダーの整合性も検証します。デバイスの電源を初めて入れると、デバイス アプリケーション プロセッサによってブート ROM と呼ばれる読み取り専用メモリからコードが実行されます。これは、チップ製造時に書き込まれるハードウェアの信頼のルートで、無条件に信頼されます。ブート ROM コードには、Apple ルート CA の公開キーが含まれており、このキーを使用して、LLB (Low-Level Bootloader) の読み込みを許可する前に LLB が Apple によって署名されていることが確認されます。それ以降の各ステップでは、ブート プロセスの次のレイヤーが Apple によって署名されていることが確認されます。LLB がタスクを終了すると、次の

段階のブートローダーである iBoot が検証されて実行されます。その後 iBoot によって iOS カーネルが検証を経て実行されます。

iOS 9 のカーネルが起動すると、どのユーザー プロセスとアプリを実行するかがカーネルによって制御されます。すべてのアプリが承認済みの既知のソースから提供されていることと、改ざんされていないことを保証するために、iOS ではすべての実行可能コードが Apple 発行の証明書を使用して署名されている必要があります。既定のアプリは署名済みです。サード パーティ製アプリも、Apple 発行の証明書を使用して署名と検証が行われます。こうしたコード署名の強制は、OS からアプリへ整合性検証を拡張したもので、サード パーティ製アプリによって未署名のコード リソースが読み込まれたり、自己書き換えコードが使用されたりするのを防いでいます。Apple では 1 台のデバイス上で管理対象アプリと非対象アプリのリストを定義することを許可しており、企業は承認に基づいて実行可能なアプリを指定できます。

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困難です。ASLR はアプリ向けの機能ですが、Windows 10 では 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 (DEP)、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、制御フロー ガード (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。

iOS 9 では、サード パーティ製のすべてのアプリがアプリ サンドボックスで実行されるため、他のアプリによって保存されたファイルにアクセスしたり、デバイスに変更を加えたりすることはできません。これにより、アプリによって保存された情報を他のアプリが収集または変更するのを防止できます。サード パーティ製アプリは、自身の情報以外の情報にアクセスする必要がある場合、iOS 9 によって明示的に提供されるサービスを使用することでその情報にアクセスできます。システム ファイルとリソースもユーザーのアプリから保護されます。iOS の大部分は、すべてのサード パーティ製アプリと同様に、特権のないユーザー "mobile" として実行されます。OS のパーティション全体は、読み取り専用としてマウントされます。アプリは API を使用して自身の権限を昇格させたり、他のアプリや iOS 9 自体を変更したりすることはできません。

Safari は、すべての iOS 組み込みアプリと同様に、ASLR を使用して起動時にメモリ領域のランダム化を行います。実行可能コード、システム ライブラリ、および関連する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、多くの高度な攻撃が発生する可能性を低減します。iOS 9 では、メモリ ページを実行不可能としてマークする ARM の Execute Never (XN) 機能 (DEP の 1 種) を使用します。書き込み可能と実行可能の両方としてマークされたメモリ ページは、厳しく条件が管理されたアプリのみが使用できます。カーネルによって Apple 独自の動的コード署名エンタイトルメントの有無が確認されます。Safari では、JavaScript JIT コンパイラでこの機能が使用されます。

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**
iOS 9	**81**	**90**

Windows 10 は、iOS よりも優れた 2 つの注目すべき脅威対策を提供します。まずは Windows 10 メジャー ブートです。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。iOS 9 には、無条件に信頼される、ハードウェアの信頼のルートがチッ

プ製造時に書き込まれ、ハードウェアからアプリまで強力な整合性検証機能を提供しますが、この機能はジェイルブレイク (脱獄) されたデバイスの暗号解除を許可しない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) という機能を通じた Windows 10 のメモリ保護強化です。

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

どのシナリオでも、組織はデバイスを管理する必要があります。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。また、Windows Information Protection によるアプリへのポリシー適用などを通じて、企業で承認されたアプリの配布と保守を行うことができます。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。

Apple iOS デバイスの場合、MDM は Apple Push Notification Service (APNS) を使用して公衆ネットワークとプライベート ネットワークの両方でデバイスとの永続的な通信を維持します。MDM では、デバイスと通信するための APNS 証明書、安全に通信するための SSL 証明書、構成プロファイルに署名するための証明書など、多くの証明書が必要です。組織は、毎年 APNS 証明書を更新する必要があります。証明書が失効すると、MDM ソリューションは組織が証明書を更新するまで Apple デバイスと通信できなくなります。

表 1: Windows 10 と iOS 9 における EMM ベンダーのサポート状況

	Windows 10	iOS 9
BlackBerry	√	√
Citrix	√	√
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。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、Azure AD Web アプリを含むネイティブ アプリへのシングル サインオンが可能になります。また Azure AD に参加することで、オンプレミス リソースへのシングル サインオンと、ビジネス向け Windows ストアの認証も可能になります。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。

iOS 9 デバイスは、監視対象にするか自己所有にするかが指定されます。デバイスを監視対象としてセットアップできるのは、アクティブ化前 (設定アシスタントが新しいデバイスまたは完全に消去済みのデバイスに表示される前) のみです。Apple Deployment Program では、初期セットアップ中に自動的に監視対象デバイスが MDM に登録されます。自己所有のデバイスでは、通常は MDM に登録するかどうかをユーザーが決定します。またユーザーは、デバイスと管理サーバーとの関連付けをいつでも解除できます。自己所有デバイス

では、一般設定でプロファイルが削除できないように設定されていても、ユーザーがパスコードを知っていればプロファイルを削除できます。組織は、MDM への登録を強制する要件を新たに考える必要があります。たとえば、企業 Wi-Fi ネットワーク アクセスなどの企業リソースに制限を設けることができます。ただしこの手法は、Windows 10 の正常性構成証明と同等ではありません。

iOS 9 は、MDM のプロビジョニング パッケージをサポートしており、電子メールの添付ファイルまたは Web ページのダウンロードを介して配布できます。また iOS 9 の MDM では、暗号化署名、プロビジョニング パッケージの暗号化、パスワード ベースのユーザー アクセスがサポートされています。MDM では、メールやその他のユーザー アカウントを自動的にセットアップできます。ユーザー名、メール アドレス、認証と署名のための証明書 ID もアカウント ペイロードにあらかじめ入力しておくことができます。iOS 9 デバイスは、通常 Simple Certificate Enrollment Protocol を使用して組織のサービスの認証用に一意の ID を作成します。ただし、iOS 9 の登録で Windows 10 の単一ステップによる MDM 登録と同じメリットを得るには、Azure AD 用の Microsoft Azure Authenticator アプリや MDM 用のサード パーティ製クライアントを使用するなど、複数のステップでプロセスを実行する必要があります。

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

iOS 9 は、デバイスを MDM にロックするために、監視対象デバイス向けに削除不可能な

MDM プロファイルを作成できます。これによって、ユーザーは、管理を迂回したり、登録を解除したりすることができません。以下に iOS 9 で使用可能な管理タスクを示します。監視対象デバイスでのみサポートされているデバイス管理機能や、使用に特別な要件がある機能もあります。

- アクティベーション ロックの有効化/許可/削除
- 診断および使用レポートの有効化/無効化: **共有 iPad でのみ使用可能**
- パスコードのクリア
- 機能制限パスワードの無効化: **監視対象デバイスでのみ使用可能**
- ユーザーのログアウト/削除: **共有 iPad でのみ使用可能**
- 紛失モードの有効化/無効化: **監視対象デバイスでのみ使用可能**
- デバイスの位置情報の取得: **監視対象デバイスでのみ使用可能**
- デバイス名の変更
- リモート ワイプ: **共有 iPad では未サポート**
- デバイスのロック
- 設定のプッシュ/削除
- アプリとブックのプッシュ/削除
- AirPlay ミラーリングの要求/停止
- 情報の更新
- デバイスの登録/削除
- iOS 更新プログラムのインストール: **Apple Deployment Program (ビジネス向け) に参加しているデバイスのみ**
- DEP プロファイルの更新: **Apple Deployment Program (ビジネス向け) に参加しているデバイスのみ**

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 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、許可するアプリと許可しないアプリを指定し、アプリ ラッピングやアプリの変更を必要とせずにアプリの分類を管理できます。管理者は、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がありません。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はありません。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。

Apple では、組織がエンド ユーザー向けアプリを購入できる Volume Purchasing Program (VPP) を提供しています。従業員は、IT 部門から提供される引き換えコードを使用して自分でアプリをダウンロードする必要があります。iOS 9 では、組織は VPP を通じてアプリを購

入し、ライセンスの所有権を維持した状態で従業員にライセンスを割り当てられることができます。これにより、従業員の離職や役割変更に応じて、アプリを再配布することができます。

iOS 9 では、MDM がインストールされたアプリを管理対象アプリと定義しています。MDM では、ユーザーが登録を解除するときに管理対象アプリとデータをデバイスに残すかどうかを指定します。MDM により、管理対象アプリから iTunes または iCloud へのデータのバックアップを防止できます。iOS 9 では、アプリを再インストールしなくても、ユーザー データを保持したまま、MDM で管理対象外アプリを管理対象アプリに変換できます。監視対象デバイスであれば、ユーザーの操作を必要とせずに、管理対象外アプリを管理対象アプリに変換できます。監視対象外のデバイスの場合は、ユーザーが管理を正式に受け入れる必要があります。

管理対象アプリは、リモートから、またはユーザーがデバイスを削除したときに、MDM によって iOS 9 デバイスから削除できます。アプリを削除すると、関連するデータも削除されます。管理対象アプリが MDM によって削除された後もユーザーに割り当てられたままにすると、ユーザーはそのアプリをアプリ ストアから管理対象外アプリとしてダウンロードできます。MDM がアプリのライセンスを無効にしても、アプリの機能は一定期間継続します。最終的にこのアプリは無効になるため、ユーザーが使用を続けるにはコピーを購入する必要があります。

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。

iOS 9 デバイスにでも、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。

Windows 10 には、Windows 10 as a Service という、過去の Windows リリースよりも速いペースで OS 機能の更新を提供するモデルが導入されています。以前は、新しい Windows が 3 年ごとにリリースされてきました。現在ではリリースの頻度が高くなり、絶えず進化するセキュリティの脅威に対処すると共に、定期的に新しい機能を求めるユーザーの期待に応えることを目的としています。マイクロソフトでは、年間 2 ～ 3 回のペースで更新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。

Apple はソフトウェアやセキュリティの更新スケジュールを公開していませんが、ほぼ毎年 iOS のメジャー バージョンの更新を行っています。Apple はモバイル キャリアに関係なく、直接更新プログラムを提供します。Apple は、セキュリティの不具合に応じて OS のマイナ

ー バージョンの更新プログラムとしてセキュリティ更新プログラムをさまざまな時期に提供することがありますが、通常は iOS のメジャー バージョン更新時にまとめてセキュリティ更新プログラムを提供しています。

Windows 10 Mobile は、ヘルプ デスクがデバイスに物理的にアクセスできない場合でも、ユーザーの問題解決を支援するリモート アシスタンスをサポートしています。この機能によって、リモート ロック、PIN リセット、電話着信、検索などに関する問題に対応します。iOS 9 も同様の機能を提供しています。

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。iOS 9 は、システム情報の照会機能は提供しますが、デバイスの正常性情報に基づいた条件付きアクセスは提供できません。

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 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。

Apple にも、製品とサービスの向上に使用される匿名技術データを収集する機能があります。このデータは、デバイスとアプリに関する匿名情報を送信する診断および使用状況プログラムで使用されるオプトイン プロセスです。データを送信するにはユーザーが明示的に同意する必要があります。ユーザーはデバイス上で送信されるデータを確認でき、いつでも送信をやめることができます。

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**
iOS 9	**81**	**81**

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。iOS 9 は、ビジネス アプリのプロビジョニングとドメイン アカウント認証のために SCEP をサポートしています。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。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。iOS 9 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、リモートのジェイルブレイク (脱獄) 検出機能が制限されています。マイクロソフトは、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

Windows 10 と iOS 9 のセキュリティと管理の機能について、ラボ環境で包括的な比較テストを実施した結果、Pique Solutions は Windows 10 の方が iOS 9 よりも企業に優れたソリューションを提供するという結論に至りました。

Windows 10 は、モバイル デバイス、タブレット、PC 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 はエンタープライズ環境で FIDO 2.0 を活用する初の OS です。多要素認証と非対称キーをサポートすると共に、ハードウェア ベースのデバイスの構成証明を利用してこれらのキーの正当性を確認します。Windows Hello は、生体認証サインイン オプションを使用するための拡張フレームワークです。ユーザー固有の生体認証 ID によってデバイスへのアクセスを認証します。現在 Windows Hello は、指紋認識、顔認識、虹彩スキャンをサポートしていますが、現在サポートされている生体認証が新しいハードウェアによって拡張される可能性があります。

さらに Windows 10 では、WIP を利用して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業務にも個人的なタスクにも使用できます。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。Windows 10 は、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し、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。

iOS 9 は、これまでの iOS バージョンで段階的にエンタープライズ環境向けに改善を図ってきました。セキュア ブート チェーンやアプリへの署名で強力な制御を提供していますが、2 要素認証にはサード パーティとの統合が必要です。また Windows 10 が提供している企業データの管理と保護の機能を装備していません。

総合すると、Windows 10 は測定されたすべてのカテゴリで iOS 9 よりも一貫して高いスコアを記録しました。特に ID 管理では、Windows 10 はユーザーとエンタープライズに統合認

証エクスペリエンスを提供できます。データ保護では、Windows 10 はデータに暗号化と制御を適用しますが、その方法は iOS 9 の管理対象アプリに対するアプローチよりも効率的であり、ユーザー エクスペリエンスに対して透過的であることがわかりました。

脅威対策としては、Windows 10 には iOS に見られない新しいメモリ保護機能が追加されています。CFG は、メモリに読み込まれたアプリの制御フローのロックダウンと強制適用を実行する手法を提供します。この機能もユーザーにとっては完全に透過的に実行されます。管理面では、Windows 10 は非常に幅広い OS 管理手法と、ドメイン アカウントを使用した合理的なデバイスのプロビジョニングおよび構成のプロセスを提供しています。

Windows 10 と iOS 9 は同等のレベルの強力な暗号化機能を提供しますが、データ レベルできめ細かく暗号化できる点を考慮すると、Windows 10 の方が優れていると考えられます。iOS 9 のアプローチでは、アプリに暗号化を適用します。アプリ レベルの暗号化は、WIP を使用してデータ レベルでデータ保護を提供する Windows 10 の要素の 1 つです。WIP は、OS や企業アプリ内で高度に統合されているため、ユーザー エクスペリエンスに与える影響も抑えられていますが、iOS 9 ではアプリを個人用か業務用として指定しなければならず、両方の用途に使用できる機能を搭載していません。

Windows 10 は、iOS 9 よりも優れた 2 つの脅威対策も提供します。まずはリモート正常性構成証明です。ルート化されたデバイスの強力な検出など、現在のデバイスの状態に応じて、信頼された企業ネットワークへの条件付きアクセスをデバイスに提供します。リモート正常性構成証明に基づいたこのタイプの条件付きアクセスの付与は、iOS では提供されていません。もう 1 つは新しいメモリ保護機能で、攻撃者によるメモリ攻撃を通じたシステムの侵害を防止できます。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、デバイスからネットワークへのアクセスが拒否された場合にはユーザーに通知されます。

つまり、Windows 10 は、最も厳しいセキュリティ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。さらに、ドメイン アカウントを使用して単一ステップでデバイスの登録と構成を行う Windows 10 の方が、いっそうシームレスなデバイスの管理とプロビジョニングのエクスペリエンスをデバイス全体に提供すると考えられます。以上の理由から、Pique Solution は、Windows 10 の方が優れた管理エクスペリエンスと統合ソフトウェア環境を提供するという結論に至りました。企業の購入担当者の皆様はこの点を考慮されることをお勧めします。