

ファームウェアコード制御とパッチ適用の困難さ

組み込みシステムは、サプライチェーンのリスクを慎重に管理する必要がある理由の1つを示しています。FPGAで実装されるプログラミングロジックとファームウェアコードにはバックドアが含まれないようにする必要があります。ファームウェアのパッチ適用は、ホストOSのソフトウェアを最新に保つのと同じくらい重要ですが、多くの組み込みシステムにとって、それは大きな課題となっています。

- 組み込みシステムとIoTデバイスの多くは、低成本のファームウェアチップが使用されており、ベンダーがセキュリティの問題を修正する更新を作成することはないか、比較的短い製品サイクルで更新を作成します（一方でデバイスはそれよりも長期的に使用され続けます）。
- 組み込みシステムの多くでは、手動による更新が必要になりますが、ほかに実施するべき優先事項があるセキュリティ部門にとって、多大な時間のかかる作業であると認識されています。
- 可用性はほとんどの組み込み展開の重要な属性です。サービスを中断することなくパッチを適用することは不可能な場合があり、サービスのダウントIMEの機会は非常に限られています。



Cisco Liveでは、組み込みシステムのセキュリティ要件に関する役立つ概要を提示しています (cisco.com/c/dam/r/cisco/live/us/docs/2018/pdf/BRKIOT-2115.pdf)。

レビュー アク ティビティ：

組み込みシステムのセキュリティのリスク

次の質問にお答えください。

1. コンピューターとネットワーキングに関して、コスト以外に組み込みシステムを制約する主要な要因は何ですか。
2. 次の記述は正しいですか、誤りですか？組み込みシステムは、お客様によって完全にカスタマイズ可能ですが、Raspberry PiまたはArduino設計のいずれかに基づいています。
3. NB-IoTには、どのアドレス指定コンポーネントをインストールまたは構成する必要がありますか。
4. あなたは、組み込みシステムの特定の実装に合わせた組み込みシステムに関するセキュリティブリーフィングの準備を手伝っています。CompTIA Security+シラバスに従って、工場、産業、製造、エネルギーのセクターについて業界固有のアドバイスを作成しました。
他にアドバイスを作成する必要があるのはどれですか。
5. 企業でIoTデバイスの使用を許可する前に、ベンダーと製品の詳細な評価が必要なのはなぜですか。

レッスン12

概要

ホストのハードニングポリシーとテクノロジーを適用して、サードパーティのサプライチェーンと組み込み/IoTシステムのリスクを評価できる必要があります。

ホストのセキュリティソリューションを実装する際のガイドライン

エンドポイントセキュリティの導入や、組み込みシステムまたはIoTシステムと統合を展開したり再評価を行なう際には次のガイドラインに従います。

- サードパーティリスクを評価して、テクノロジーおよびソリューションのプロバイダーとして承認済みのベンダーとパートナーをオンボードするために適切な手順と合意（MOU、NDA、SLA、BPA、MSA）が使用されるようにします。
- 各ホストの種類別に構成ベースラインを確立します。ホストは構成ベースラインに従って展開されるようにし、コンプライアンスを遵守できるように監視を設定します。
- セキュアポートオプションを構成して、ネットワークアクセスコントロールメカニズムのベースとして構成証明とポリシーサーバーを使用することを検討します。
- フルディスクまたは自己暗号化ドライブを使用してストレージの暗号化を構成します。
- マルウェア対策、ファイアウォール、IDS、EDR、DLPなどのセキュリティ要件を満たす機能を持つエンドポイント保護ソリューションを展開します。
- パッチ管理手順を確立して、さまざまなホストグループの更新をテストし、OSとサードパーティ製ソフトウェアを確実に管理します。
- 職場で使用するIoTデバイスの管理計画を作成し、管理されていないアプライアンスに「シャドーIT」が展開されていないようにします。
- ICSやSCADA組み込みシステムのセキュリティ要件を評価します。
 - セキュアなSoC、RTOS、FPGAコントローラーシステムの調達。
 - 認証、完全性、耐性のための暗号化制御の使用。
 - 専門の通信技術の使用。
 - OTネットワークのアクセス制御とセグメント化。
 - パッチ管理のベンダーサポート。

レッスン13

セキュアなモバイルソリューションの実装

レッスン概要

現在、モバイルデバイスは数多くの一般的な業務タスクを行う上で好まれているクライアントであり、ネットワーク管理とセキュリティシステムをそれらに対応するよう改良する必要があります。またモバイルへのシフトは、統合化されたエンドポイント管理への動きと、企業アプリとデータ処理をプロビジョニングするさらに優れたモデルとして、仮想ワークスペースを使用することの前触れともなっています。

レッスンの目的

このレッスンの内容は、以下のとおりです。

- モバイルデバイス管理を実装する。
- セキュアなモバイルデバイス接続を実装する。

トピック13A

モバイルデバイス管理を実装する



対象試験範囲

3.5与えられたシナリオに基づいて、セキュアなモバイルソリューションを実装することができる。

モバイルの使用がありとあらゆる組織に浸透する中、そうしたモバイルデバイスが管理されていない攻撃ベクトルとして悪用されることがないよう、ネットワーク管理とセキュリティのスイートが開発されてきました。あなたはセキュリティのプロフェッショナルとして、そうした管理スイートを構成し、デバイスのオンボーディング処理によってユーザーを支援することを頻繁に求められるでしょう。

モバイルデバイスプロイモデル

モバイルデバイスは、メール管理やスケジュール管理を行う多数のタスクにおいてすでにコンピューターに取って代わっています。また、その他多くのビジネスプロセスやクラウドベースのアプリケーションにアクセスする上で不可欠な存在になっています。モバイルデバイスプロイモデルは、モバイルデバイスとアプリケーションが従業員にどう提供されるかを説明するものです。

- **デバイス持ち込み(Bring Your Own Device, BYOD)**— モバイルデバイスを従業員が所有しているモデルです。そのモバイルデバイスは（OSのバージョンや機能性に関して）企業の求める仕様をすべて満たす必要があり、また従業員は企業アプリのインストールと、一定水準の監督と監査に同意する必要があります。通常はこのモデルが従業員に一番好まれていますが、セキュリティやネットワークの管理者にとっては最も厄介です。
- **企業所有、業務使用のみ(Corporate owned, business only, COBO)**— デバイスは企業の所有物であり、業務に限って使用できるというモデルを表します。
- **企業所有、私的使用可(Corporate owned, personally-enabled, COPE)**— デバイスの選定と供給は企業が行い、引き続きその企業の所有物となるモデルです。従業員は個人のメールアカウントやソーシャルメディアアカウントへアクセスするために、または私用でWebを閲覧するためにデバイスを使用できます（実施されているすべての利用規定の対象となります）。
- **デバイス選択可(Choose your own device, CYOD)**— COPEとほぼ同じですが、従業員はリストからデバイスを選ぶことができるモデルです。

仮想化によってさらに別のデプロイモデルが可能になります。仮想デスクトップインフラストラクチャ(VDI)では、互換性のあるハードウェアにOSデスクトップがプロビジョニングされます。ハードウェアはVDIクライアントビューアーを実行できればそれでよく、またはブラウザにクライアントレスHTML5ソリューションをサポートさせても構いません。そのインスタンスはセッションごとに「新規」で提供され、リモートアクセスが可能です。スマートフォンやタブレットなどのモバイルデバイスからも同じテクノロジーにアクセスできます。企業のアプリとデータはそのデバイス上の他のアプリからセグメント化されているので、BYODにまつわるセキュリティ上の一部の懸念が取り除かれます。

エンタープライズモビリティ管理

エンタープライズモビリティ管理(EMM)は、エンタープライズ環境におけるモバイルデバイスとアプリの使用にセキュリティポリシーを適用するよう設計された、管理ソフトウェアの一種です。接続されたデバイスの識別と管理にまつわる課題は、しばしば可視性と呼ばれます。EMMソフトウェアは、企業が所有するデバイスだけでなくBYODの管理にも使用できます。EMM製品スイートには2つの主な機能があります。

- **モバイルデバイスマネジメント(MDM)**—認証、機能の使用（カメラやマイクなど）、接続に関するデバイスピリシーを定めます。またMDMにより、デバイスのリセットとリモートワイプも可能になります。
- **モバイルアプリケーションマネジメント(MAM)**—企業データを処理する可能性があるアプリ向けのポリシーを定め、個人のアプリへのデータ転送を防止します。このタイプのソリューションは、企業が管理するコンテナまたはワークスペースを構成します。

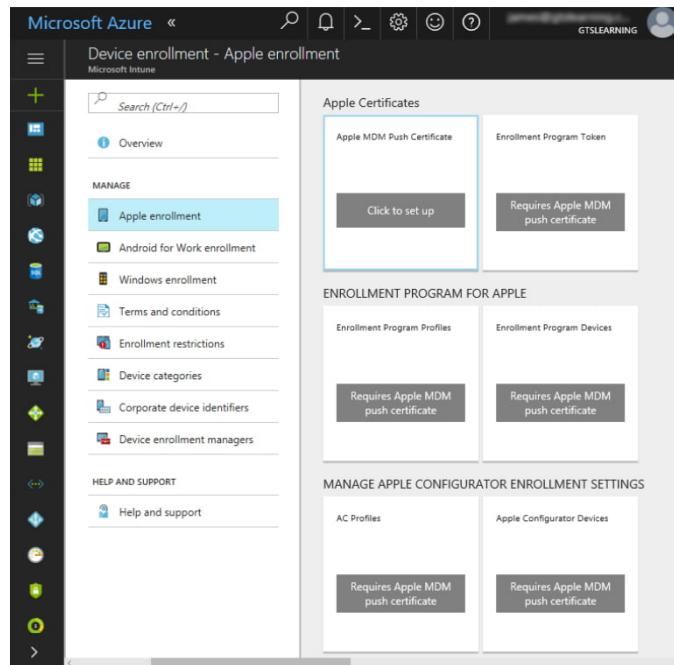
さらに、そうした管理タスクの多くにおいては、クライアントエンドポイントがモバイルか固定式かは実際には重要な要素でなく、結果として最新のスイートは、PC、ラップトップ、スマートフォン、タブレット、さらにはIoTデバイスにまたがる可視性を視野に入れています。そうしたスイートは統合エンドポイント管理(UEM)と呼ばれます(redmondmag.com/Articles/2017/10/01/Unified-Endpoint-Management.aspx)。

エンドポイント管理スイートの中核機能は、ネットワークアクセス制御(NAC)ソリューションの概念を拡張するものです。管理ソフトウェアはネットワーク上のデバイスの使用を記録し、管理者が設定したパラメータをもとに接続の許可を決定します。管理ソフトウェアに登録したデバイスは、アプリや企業データ、ビデオカメラやマイクなどの内蔵機能の使用を許可もしくは制限するポリシーで設定することができます。

EMM/UEMソリューションとして Microsoft Intune (microsoft.com/en-us/microsoft-365/enterprise-mobility-security/microsoft-intune)、Symantec/Broadcom (broadcom.com/products/cyber-security/endpoint/end-user/protection-mobile)、Citrix Endpoint Management (旧称XenMobile) (citrix.com/products/citrix-endpoint-management)などがあります。

企業におけるiOS

AppleのiOSエコシステムにおいて、サードパーティの開発者は、MacOSでのみ利用可能なAppleソフトウェア開発キットを用いてアプリを制作できます。アプリはAPP Store経由でユーザーにリリースする前にAppleに提出し、承認を受ける必要があります。企業によるiOSデバイスの管理と、企業版およびB2B (Business-to-Business)アプリの配信は、Device Enrollment Program (support.apple.com/business)、Volume Purchase Program、Developer Enterprise Program (developer.apple.com/programs/enterprise)に参加することで容易に行えます。別の選択肢として、EMMスイートとその開発ツールを使用し、企業アプリ用の「ラッパー」を作成するというものがあります。



MicrosoftのIntune EMMスイートにおけるiOSデバイスの登録設定。
(スクリーンショットはMicrosoftからの許可を得て使用。)

iOSに対する攻撃のほとんどは、ユーザーに悪意のあるリンクをクリックさせる、またはフィッシングサイトに情報を入力させるなど、他のあらゆるシステムへの攻撃と同じです。iOSはクローズドのプロプライエタリシステムであり、すべてのコードはAppleのサーバーからのみ更新されるので、マルウェアがiOSデバイスに感染するのは不可能なはずです。それでもなお、iOSやアプリにおける脆弱性が発見され、悪用されるリスクは残っています。その場合、ユーザーはiOSまたはアプリを、そうした悪用を軽減するバージョンに更新する必要があるでしょう。

企業におけるAndroid

Androidはオープンソースが基本であり、そのことはベンダーごとのバージョンに広い余地があることを意味します。アプリモデルの規制は緩く、Google Playから、またはAmazonのApp Storeなどのサードパーティサイトからもアプリを利用できます。SDKはLinux、Windows、macOSで使用できます。Android Enterprise (android.com/enterprise)プログラムはEMMスイートの使用と、企業ワークスペースのコンテナリゼーションを容易にします。さらに、SamsungはKNOX (samsung.com/us/business/solutions/samsung-knox)と呼ばれるワークスペースフレームワークを用意しており、デバイスの機能に対するEMMコントロールを容易にしています。



Company Access Setup

We'll help you set up your device to access the Company Portal, internal apps and other company resources.

Work Profile Setup

Your work profile is managed by your company and gives you access to company resources.

Device Enrollment

Sign in, approve Terms and Conditions, and enroll your device.

Device Compliance

You might need to set a passcode or change your email configuration.



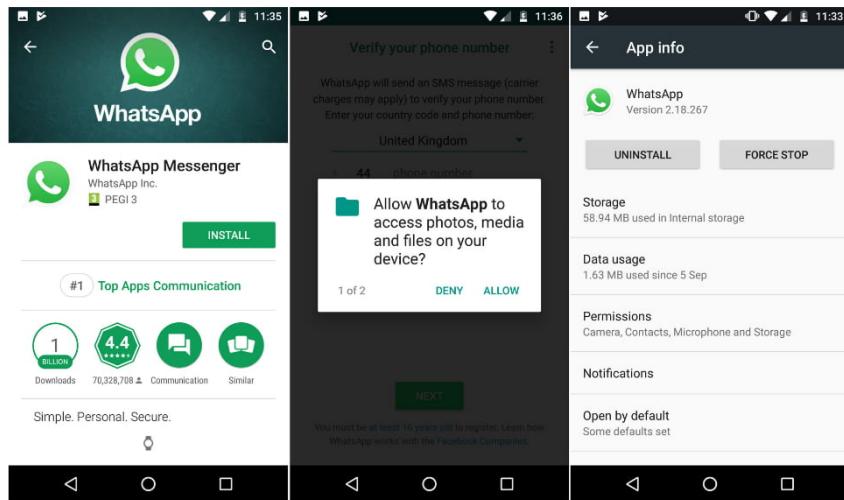
*IntuneでAndroidスマートフォンを登録する。
(AndroidはGoogle LLCの商標)*

通常、iOSデバイスは非常に素早く更新されます。Androidにおいては、新バージョンを完成させるにあたり、または各社のAndroidに合わせたパッチを発行するにあたり、更新がしばしば携帯電話のベンダーに依存しているため、状況はそれほど一貫していません。Android OSの方がよりオープンであり、Androidのマルウェアが存在していますが、Appleと同様、未熟なハッカーやスパマーが主要なアプリのリポジトリに侵入するのは困難です。



用いられるテクニックの1つにステージペイロードと呼ばれるものがあります。マルウェアの制作者は無害に見えるアプリをストア内でリリースしていますが、ひとたびインストールするとマルウェアに感染した追加コンポーネントをダウンロードしようとします(zdnet.com/article/android-security-sneaky-three-stage-malware-found-in-google-play-store)。Googleはサーバーサイドのマルウェアスキャニング製品(Play Protect)を実装しており、アプリが危険と思われる場合はユーザーに警告した上で購入済みのアプリをスキャンすると共に、セキュリティ上の問題が検出された場合もユーザーに警告を行います。

バージョン4.3以降、AndroidはSecurity-Enhanced Linuxがベースになっています。
SEAndroid (source.android.com/security/selinux)は強制アクセス制御(MAC)ポリシーを使用し、サンドボックス内でアプリを動作させています。アプリがインストールされると、連絡先情報、SMSテキスト、およびメールなど、特定の共有機能へのアクセスが許可される（または許可されない）ことになります。



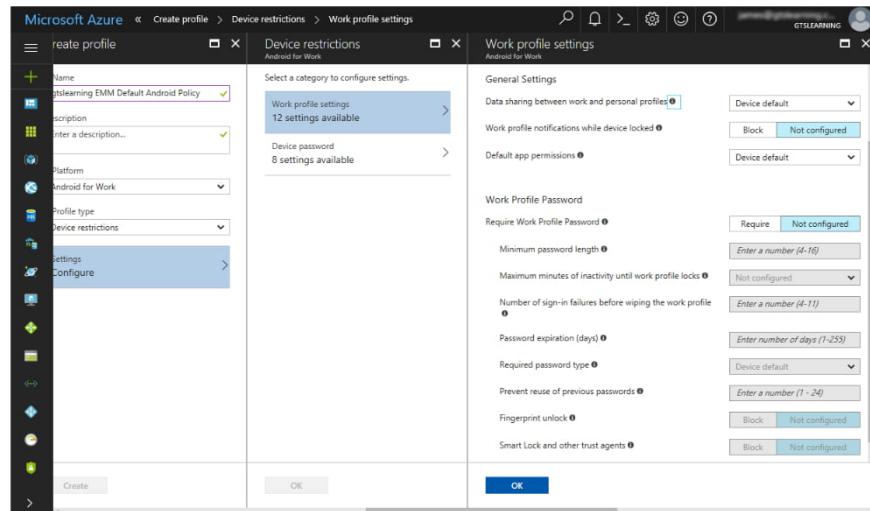
Android OSでアプリのパーミッションを構成する。(AndroidはGoogle LLCの商標)

モバイルアクセス制御システム

脅威アクターは、スマートフォンやタブレットにアクセスできた場合、膨大な量の情報を入手して、それを武器にさらなる攻撃を仕掛けることができます。多くの場合、デバイスに保存されている可能性のある機密データファイルとはまったく別に、電子メールやリモートアクセスVPN、Webサイトなどのサービスのパスワードがキャッシュされています。

スマートフォン認証

スマートフォンやタブレットの多くは、一人のユーザーだけが利用するシングルユーザーデバイスです。アクセス制御は、正しいパスワード、PIN、またはスワイプパターンでのみ解除できる画面ロックを設定することで実装できます。現在では多くのデバイスが生体認証をサポートしており、通常は指紋リーダーですが、顔認識や音声認識が使用されることもあります。



Intune EMMを用いて認証とプロファイルのポリシーを構成する – このポリシーにより、企業のアプリとデータをホストしているワークスペースに対して、ユーザーが異なる種類の認証を行える（または認証がまったく行われない）ことに注意してください。（スクリーンショットはMicrosoftからの許可を得て使用。）



単純な4桁のPINコードは簡単にブルートフォースされるので、モバイルデバイスには必ず強力なパスワードを設定しなければなりません。スワイプパターンも、ユーザーの選択がまざい(文字や四角形のパターンを選ぶ)場合、またはスマッシ攻撃を可能にする指紋汚れの跡がある場合は脆弱になります(arstechnica.com/information-technology/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns)。

画面ロック

画面ロックはまた、ロックアウトポリシーで設定することも可能です。これは、間違ったパスコードが入力されると、一定の時間デバイスがロックされることを意味します。また、徐々に時間が長くなるように設定することも可能です（例えば、最初の失敗ではデバイスが30秒間ロックされるだけだが、3回失敗すると10分ロックされる）。これにより、パスコードを推測することを阻止します。

コンテキスト対応の認証

コンテキスト対応の認証など、より新しい認証モデルを検討することも重要です。一例を挙げると、現在のスマートフォンは、自宅など信頼できる場所にいることをデバイスが検知した際に画面ロックを無効にするよう、ユーザーが設定できるようになっています。それとは逆に、企業はデバイスの悪用を防ぐべく、より厳格なアクセス制御を求めているかもしれません。例えば、デバイスがロックを解除されても、企業のワークスペースへアクセスするにあたり、ユーザーに再度認証を求めるといったことが挙げられます。また、そのネットワーク接続が信頼できるかどうかをチェックすることもあります（オープンWi-Fiホットスポットではない、など）。

リモートワイプ

リモートワイプまたはキルスイッチは、携帯電話が盗難に遭った場合に、工場出荷時設定に戻したり、個人データをすべて消去（サニタイズ）したりできることを意味します。また、ユーティリティによっては、プラグインメモリカードも消去できる場合があります。リモートワイプは、パスコード入力の数度の失敗によってトリガーさせたり、エンタープライズ管理ソフトウェアによってトリガーさせたりできます。他に、電話からデータをサーバーにバックアップした後、「この電話は紛失物です／盗難に遭いました。XXに返却してください」といったメッセージをハンドセットに表示できる機能もあります。

The screenshot shows the 'User Settings' page for a user named James Pengelly. On the left, there's a sidebar with navigation links: 'HOME', 'USERS', 'SERVICES', 'ACCOUNT', and 'gtslearning'. A search bar at the top right contains the placeholder 'Search users, pages and...'. The main content area is titled 'User Settings' and shows 'James Pengelly' with the email 'james.pengelly@gtslearning.com'. Below this, there's a section titled 'ActiveSync devices' with a table listing the following data:

Device name	Device model	Latest sync date	Wipe	Erase
Outlook for iOS and Android	Outlook for iOS and Android	10/09/2017, 21:38:41	Wipe	Erase
XT1032	XT1032	31/05/2017, 08:49:03	Wipe	Erase
Outlook for iOS and Android	Outlook for iOS and Android	22/05/2017, 04:13:57	Wipe	Erase
Moto G (5)	Moto G (5)	16/05/2017, 14:44:57	Wipe	Erase
White iPad mini	iPad2CS	19/06/2016, 19:19:59	Wipe	Erase
Outlook for iOS and Android	Outlook for iOS and Android	24/08/2015, 22:22:20	Wipe	Erase
unknown	iPhone	12/06/2012, 10:17:06	Wipe	Erase

Below the table, it says '7 items found (7 total)'.

大半の企業向けメッセージングシステムにはリモートワイプ機能（この例のように、*Intermedia*メールホスティングと共に提供されるものなど）があり、電子メールやカレンダー、連絡先情報をモバイルデバイスから削除できます。（スクリーンショットは*Intermedia*からの許可を得て使用。）

理論上、窃盗犯はまず電話がネットワークに接続できないようにし、次に電話をハッキングしてセキュリティを無効にすることで、リモートワイプを阻止することが可能です。

デバイスのフル暗号化と外部メディア

初期のOSバージョンでない限り、スマートフォンやタブレットにはデバイスのフル暗号化が導入されています。iOSには、さまざまなレベルの暗号化があります。

- デバイス上のすべてのデータが常に暗号化されていますが、鍵はデバイス上に保存されています。これは主に、デバイスをワイプする手段として使用されます。OSは、各保存場所をワイプするのではなく、鍵を削除するだけで、データにアクセスできなくすることができます。
- 「データ保護」オプションを使用している電子メールデータやアプリも、ユーザーの認証情報から派生し、それによって保護されている鍵を使用して第2の暗号化が行われます。これにより、デバイスが盗難に遭った場合でも、データの安全が確保されます。すべてのユーザーデータが「データ保護」オプションを用いて暗号化されるわけではなく、連絡先やSMSメッセージ、写真などは暗号化されません。

iOSではデバイスのパスワードロックを設定すると、データ保護の暗号化が自動的に有効になります。Androidの暗号化オプションは、バージョンごとにかなりの違いがあります(source.android.com/security/encryption)。Android 10の時点では、パフォーマンスに悪影響を与えるすぎると考えられているため、フルディスクの暗号化は行われていません。デフォルトでは、ユーザーデータはファイルレベルで暗号化されます。

モバイルデバイスにはソリッドステート（フラッシュメモリ）ドライブが備わっており、アプリとデータの永続的な保存を可能にしています。Android携帯電話の中には、プラグインMicro SecureDigital (SD)カードスロットなど、外部メディアを用いたリムーバブル記憶装置をサポートしているものもあり、またUSB方式の記憶装置への接続をサポートしているものもあります。モバイルOSの暗号化ソフトウェアによってリムーバブル記憶装置を暗号化できる場合もありますが、常に可能なわけではありません。必要に応じてサードパーティのソフトウェアを用いてカードを暗号化し、機密データはその中にのみ保存するよう留意する必要があります。

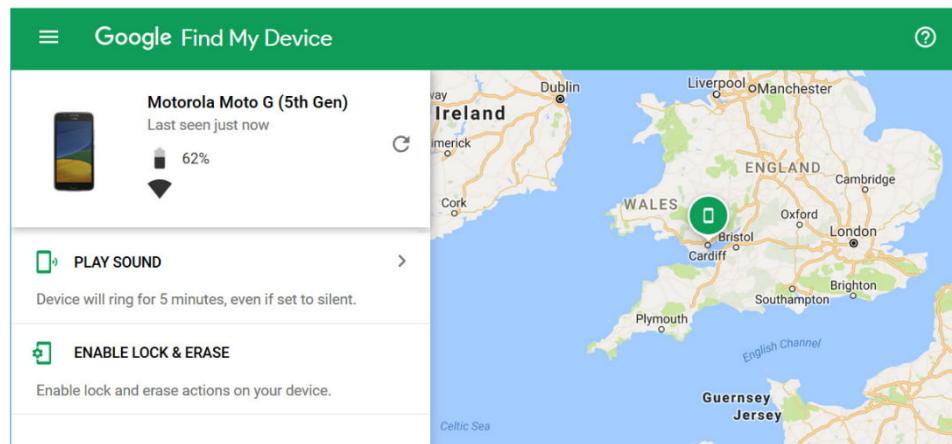
MicroSD HSMは、暗号化鍵を安全に保存することを目的とした小型のハードウェアセキュリティモジュールです。これにより、ラップトップやスマートフォンなどさまざまなデバイスで暗号化マテリアルが使用できます。

ロケーションサービス

位置情報とは、ネットワーク属性を用いてデバイスの物理的位置を識別する（または推定する）ことです。デバイスはロケーションサービスを用いて現在位置を判断します。ロケーションサービスは次の2つのシステムを活用できます。

- 全地球測位システム(GPS) – GPSセンサーを介して人工衛星から受信した情報を基に、デバイスの緯度と経度を判断する方法です。
- 屋内測位システム(IPS)** – 携帯電話の基地局、Wi-Fiアクセスポイント、Bluetooth/RFIDビーコンなど、他の電波源までの近さを三角測量することでデバイスの位置を特定します。

ユーザーがアプリに使用を許可していれば、ロケーションサービスはどのアプリでも利用可能です。

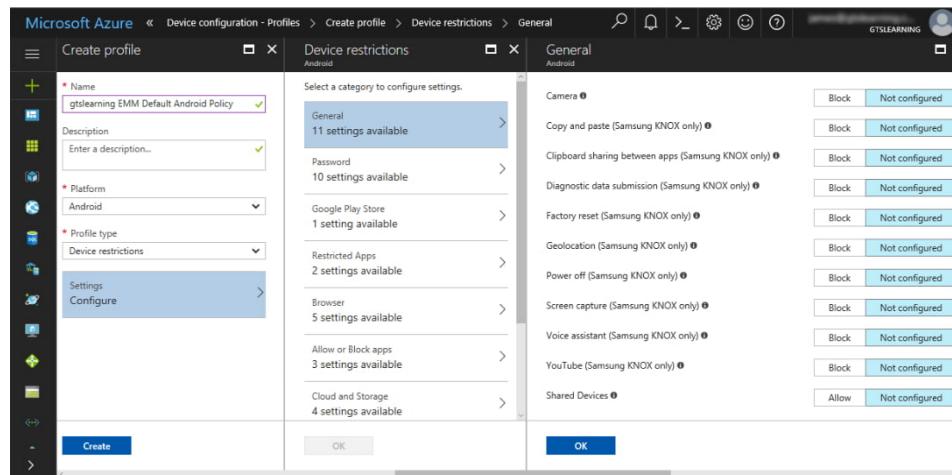


Find My Deviceを使ってAndroidスマートフォンの位置を特定する。(AndroidはGoogle LLCの商標)

ロケーションサービスにまつわる主な懸念にプライバシーの問題があります。ロケーションサービスは地図や進路誘導ナビゲーションに極めて有益ですが、個人の行動を追跡し、そこからその人の社会的習慣やビジネス上の習慣をトラッキングするメカニズムとなります。多数のモバイルアプリがロケーションサービスへのアクセスを必要とし、アプリケーションのデベロッパーにその情報を送信すると同時に、デバイスのファイル構造の中にそれを保存していることで、問題はさらに複雑になっています。脅威アクターがそのデータにアクセスできると、ストーキング、ソーシャルエンジニアリング、さらには個人情報の盗難が現実のものとなります。

ジオフェンシングとカメラ/マイクの使用制限

ジオフェンシングは、実世界の地理に基づいて仮想境界を作成する方法です。カメラまたはビデオ機能の使用をコントロールする、もしくはコンテキスト対応の認証を適用することに関して、ジオフェンシングは有益なツールになり得ます。自社の敷地周辺に境界を設定し、その境界を越えたすべてのデバイスの機能を制限するために、組織がジオフェンシングを使用する場合があります。ロックが解除されているスマートフォンをロックし、敷地へ立ち入る際に再認証を求める、あるいはカメラとマイクを無効化するといったことが可能です。デバイスの位置はロケーションサービスから取得されます。



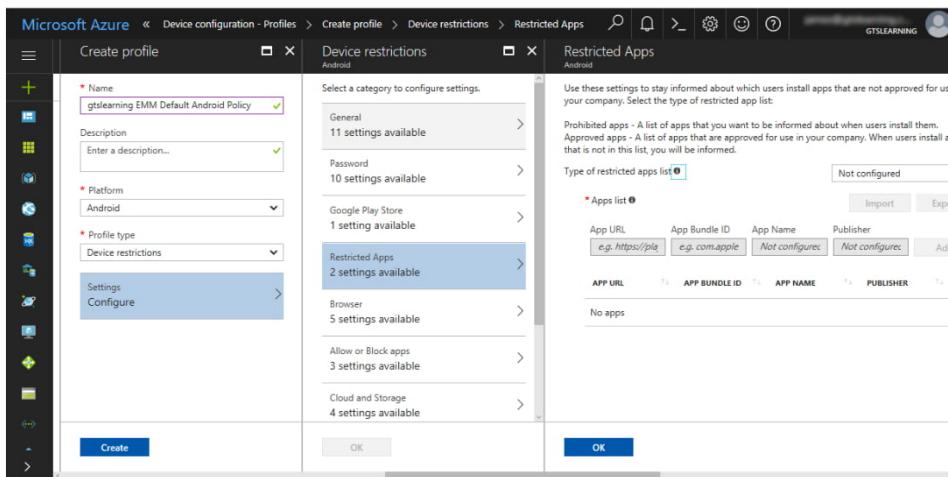
Intuneを使ってカメラや画面キャプチャなどのデバイスパーミッションを制限する。
(スクリーンショットはMicrosoftからの許可を得て使用。)

GPSタギング

GPSタギングは、デバイスがそのとき位置していた緯度と経度などの地理識別メタデータを、写真、SMSメッセージ、ビデオといったメディアに追加するプロセスです。それにより、アプリはそのメディアを緯度と経度の明確な座標に位置づけることができます。GPSタギングは非常に機密性が高い個人情報であり、また組織の機密データである場合もあります。GPSタギングされた上でソーシャルメディアにアップロードされた写真が、個人の行動や位置を追跡するために用いられることがあります。一例を挙げると、あるロシア人兵士がGPSタギングされた自撮り写真をInstagramにアップロードしたせいで、部隊の位置が明らかになるということがありました(arstechnica.com/tech-policy/2014/08/opposite-of-opsec-russian-soldier-posts-selfies-from-inside-ukraine)。

アプリケーション管理

デバイスが管理ソフトウェアへの登録を通じて企業ネットワークに加わる場合、一定数の許可されたアプリケーションだけを実行できるエンタープライズワークスペースモードに設定することができます。



Microsoft Intuneなどのエンドポイント管理ソフトウェアを使用することで、アプリの承認や禁止が行えます。（スクリーンショットはMicrosoftからの許可を得て使用。）

信頼できるアプリの発行元とは、サービスプロバイダーが管理しているものを指します。サービスプロバイダーは有効な開発者の認証および承認を行い、アプリへの署名とアプリの信頼性の保証に使用する証明書を発行します。また提出されたコードを分析して、ユーザーにセキュリティやプライバシーに関するリスクを及ぼしていないか確認することもあります（また、こういたリスクがあると判明したアプリを削除する場合もあります）。コンテンツが成人向けのアプリや、コアOSのアプリと機能が重複しているアプリを許可しないなど、開発者が満たすべきその他のポリシーを適用することもあります。

モバイルOSの既定の設定では、アプリのインストールは関連するストア（iOSではApp Store、AndroidではPlay）に制限されています。このモデルは一般ユーザーの間では受け入れられていますが、企業では問題になることがあります。誰でもダウンロードできるパブリックストアから、企業独自のアプリを配信するのが適切ではない場合があります。Appleはエンタープライズ版のデベロッパープログラムとディストリビューションプログラムを運営することでこの問題に対処しており、プライベートなアプリをApple Business Manager経由で配布できるようにしています（developer.apple.com/business/distribute）。またGoogle PlayストアにはManaged Google Playと呼ばれるプライベートチャネルのオプションがあります。いずれの選択肢でも、EMM/UEMスイートによってプライベートチャネルからデバイスにアプリをプッシュ配信できます。

iOSと違い、Androidではさまざまなストアからの選択が可能であり、あらゆるサードパーティが配信する信頼できないアプリをインストールすることができます（このオプションがユーザーによって有効になっている場合）。不明な発行元を有効にすると、.apkのファイル形式でWebサイトから信頼できないアプリをダウンロードしインストールてしまいます。これを**サイドロード**と呼びます。

逆に、サードパーティのストアやサイドロードが使用されるのを防止し、許可されていないアプリ発行元をブロックするために、管理スイートが用いられることもあります。

コンテンツ管理

コンテナリゼーションを行うことで、雇用者はデバイスのうち企業ネットワークと連動する部分を管理・維持できるようになります。規定されたアプリ群と個別のコンテナを持つエンタープライズワークスペースが作成されます。このコンテナは企業アプリをデバイスの残りの部分から隔離します。ワークスペースへアクセスするために追加の認証が必要になる場合もあります。

またコンテナはストレージセグメンテーションを行うこともできます。ストレージセグメンテーションを行った場合、コンテナは、その中に含まれていないアプリでは読み書きできない永続ストレージ装置のディレクトリと関連付けられることになります。逆に、アプリは外部メディアなどコンテナ外の領域に書き込むことができず、コピー・アンド・ペーストを使ってコンテナ外のアプリに書き込むこともできません。アプリのネットワークアクセスは、組織のセキュリティシステムを通じてトンネリングされたVPNに制限されます。

それにより、企業は個人使用、アプリ、またはデータに影響を及ぼすポリシーを実施することなく、必要とするセキュリティを維持できます。

またコンテナリゼーションはコンテンツ管理システムやデータ損失防止(DLP)システムを支援します。コンテンツ管理システムは企業データもしくは機密データをタグ付けし、共有不正な外部のメディアまたはチャネル（企業外のメールシステムやクラウド保管サービスなど）へのコピーを防止します。

root化とジェイルブレイク（脱獄）

WindowsやLinuxと同じく、OSのインストールとカーネルレベルの処理に使用されるアカウントは、デバイスの所有者が用いるアカウントと同じではありません。一部のOSベンダー、携帯電話OEM、通信事業者（キャリア）がデバイスに課している制限を回避したい場合、ユーザーは何らかのタイプの特権エスカレーションを用いなければなりません。

- **root化** – この用語はAndroidデバイスに関連するものです。一部のベンダーはユーザーが自分のデバイス上でrootアカウントにアクセスできるよう、承認済みのメカニズムを提供しています。デバイスによっては、脆弱性を悪用したりカスタムファームウェアを使用したりするためにルート化が必要になります。カスタムファームウェアは本質的に、そのデバイスに適用される新規のAndroid OSイメージです。これはファームウェアの保持に用いられる読み取り専用メモリーチップにちなみ、カスタムROMとも呼ばれます。
- **ジェイルブレイク** – iOSはAndroidに比べて制限が強いので、ユーザーによるroot特権の取得、アプリのサイドロード、キャリアの変更または追加、インターフェイスのカスタマイズを可能にするエクスプロイトを指す用語として、「ジェイルブレイク」が一般的になりました。iOSのジェイルブレイクは、パッチされたカーネルを持つデバイスを起動することにより行われます。大半のエクスプロイトについて言えば、ジェイルブレイクはデバイスが起動する際、コンピューターに接続している場合にのみ可能です（紐付きジェイルブレイク）。
- **キャリアアンロック** – iOSとAndroidどちらの場合でも、これはデバイスを単一のキャリアに縛りつける制限を取り除くことを意味します。

モバイルデバイスのroot化やジェイルブレイクには、デバイスのセキュリティ対策を回避し、そのデバイスへの管理者アクセスを取得することが含まれています。そこには、セキュリティ対策の多くが永久に無効化されたままになるという副作用もあります。ユーザーがrootパーティションを有していると、そのデバイスで動作している事実上すべての管理エージェントソフトウェアが侵害されます。ユーザーがカスタムファームウェアイメージを適用した場合、セグメンテーションを実行する保護機能が消去された可能性があります。するとそのデバイスは、信頼できるOSを実行しているとはもはや見なされません。

EMM/UEMには、root化またはジェイルブレイクされ、有効なデベロッパーコード署名がないデバイスもしくはカスタムファームウェアを検出し、エンタープライズアプリ、ネットワーク、またはワークスペースへのアクセスを防ぐルーチンがあります。コンテナリゼーションとエンタープライズワークスペースは暗号化を用いることにより、たとえroot化またはジェイルブレイクされたデバイスからであっても、ローカルエージェントに比べて侵害をはるかに難しくする形で、そのワークスペースを保護することができます。

レビュー アク ティビティ： モバイルデバイス管理

次の質問にお答えください。

1. ユーザーがモバイルデバイスのメーカーとモデルを選択できるのは、どのタイプのデプロイモデルですか？
2. VDIはモバイルデプロイモデルとしてどのように機能しますか？
3. あなたは会社のポリシーにより、紛失や盗難に備えて自分のスマートフォンを不正なアクセスから確実に保護するよう求められています。電源を入れた何者かがデバイス上のデータへただちにアクセスするのを防ぐには、どのようなセキュリティ管理を用いるべきですか？
4. 最近、ある従業員の自家用車が荒らされ、大量の機密データを保持している会社のタブレットが盗まれました。あなたはすでに、そのデータの大量のバックアップを保護するという予防策をとっています。データが渡ってはいけない人の手に渡っていないことを絶対確実に保証するため、あなたは何をすべきですか？
5. コンテナリゼーションとは何ですか？
6. サイドロードのプロセスはどういったものですか？
7. 自社の敷地内で記録用デバイスが使用されるを防ぐデバイス管理ソフトウェアに企業が投資するのはなぜですか？
8. root化またはジェイルブレイクされたデバイスが企業のセキュリティにとって脅威なのはなぜですか？

トピック13B

セキュアなモバイルデバイス接続を実装する



対象試験範囲

1.4 与えられたシナリオに基づいて、ネットワーク攻撃に関する可能性のあるインジケーターを分析することができる。

3.5 与えられたシナリオに基づいて、セキュアなモバイルソリューションを実装することができる。

管理スイートは機能やアプリの認証と許可だけでなく、モバイル向けのネットワークオプションを支援することもできます。ローカルネットワークにとってセキュアでない通信タイプを無効にし、デバイスをリモートで使用するユーザーに通信セキュリティに関するアドバイスをできるようになる必要があります。

携帯ネットワーク接続方式とGPS接続方式

ローカルネットワークやパーソナルエリアネットワークで通信を確立するために、またはサービスプロバイダー経由でインターネットのデータにアクセスするために、モバイルデバイスはさまざまな接続方式を使用します。

Setting	Status
Data roaming (Samsung KNOX only)	Block / Not configured
SMS/MMS messaging (Samsung KNOX only)	Block / Not configured
Voice dialing (Samsung KNOX only)	Block / Not configured
Voice roaming (Samsung KNOX only)	Block / Not configured
Bluetooth (Samsung KNOX only)	Block / Not configured
NFC (Samsung KNOX only)	Block / Not configured
Wi-Fi (Samsung KNOX only)	Block / Not configured
Wi-Fi tethering (Samsung KNOX only)	Block / Not configured

IntuneでAndroidの接続方式をロックダウンする – 大半の設定はSamsung KNOXに対応したデバイスにしか適用できないことに注意してください。(スクリーンショットはMicrosoftからの許可を得て使用。)

携帯データ接続

スマートフォンと一部のタブレットは携帯電話ネットワークを用いて通話やデータアクセスを行います。携帯データ接続が監視やフィルタリングの対象になることは多くありません。データの流出に使用されることを避けるため、デバイスが企業のネットワークやデータにアクセスする際はそれを無効化する必要があります。

通信会社のネットワークを支える主要なインフラストラクチャやプロトコルに対して攻撃または悪用が成功した例もあり、有名なものとしてSS7ハック([theregister.com/2017/05/03/hackers_fire_up_ss7_flaw](http://www.theregister.com/2017/05/03/hackers_fire_up_ss7_flaw))が挙げられます。そうした脆弱性に対して企業や個人ができるることはほとんどありません。攻撃には高度な知識が必要とされ、頻度は比較的高くありません。

全地球測位システム(GPS)

全地球測位システム(GPS)センサーは、軌道周回GPS衛星からの信号を用いてデバイスの位置を三角測量します。この三角測量プロセスに時間がかかることがあるので、大半のスマートフォンは補助GPS(A-GPS)を用いることで最も近い携帯基地局から座標を取得し、その基地局との相対関係でデバイスの位置を調整します。A-GPSは携帯データネットワークを使用します。GPS衛星は合衆国政府によって運用されています。GPSセンサーの中には、EU (Galileo)、ロシア (GLONASS)、および中国(BeiDou)が運用しているその他の衛星からの信号を使用できるものもあります。

GPS信号はジャミングされることがあります。専用の無線装置を用いて偽装されることさえあります。これは例えればジオフェンシングメカニズムを打ち破るために用いられます([kaspersky.com/blog/gps-spoofing-protection/26837](https://www.kaspersky.com/blog/gps-spoofing-protection/26837))。

Wi-Fi接続方式とテザリング接続方式

Wi-Fi接続が存在している場合、デバイスは通常それを用いてデータ通信を行うようデフォルト設定されています。ユーザーが強力なWPA3セキュリティを用いて企業ネットワークへの接続を確立した場合、盗聴や中間者攻撃のリスクは極めて低くなります。Wi-Fiに由来するリスクは、ユーザーがオープンアクセスポイントに、また場合によっては企業ネットワークを装った不正アクセスポイントに接続することから生じます。これにより、そのアクセスポイントの所有者はいくらでも攻撃を仕掛けることができ、(DNSスプーフィング攻撃などを用いて)セキュアなサーバーとのセッションを侵害できる可能性さえあります。

パーソナルエリアネットワーク(PAN)

パーソナルエリアネットワーク(PAN)は、モバイルデバイスと周辺機器との接続を可能にします。モバイルデバイス同士、またはモバイルデバイスとその他のコンピューティングデバイスとのアドホック（またはピアツーピア）ネットワークを確立することもできます。企業セキュリティの点から言えば、そうしたピアツーピア機能は一般的に無効にすべきです。脅威アクターが誤って構成されたデバイスを悪用し、企業ネットワークへブリッジ接続する可能性があるからです。

アドホックWi-FiとWi-Fi Direct

ワイヤレスステーションはアクセスポイントを使用するのではなく、互いにピアツーピア接続を確立することができます。これは**アドホックネットワーク**とも呼ばれ、そのネットワークが永久的に利用できるようになっていないことを意味します。しかしアドホックネットワークには、標準ベースの確立されたサポートがありません。Androidスマートフォンがアドホックネットワーク内で自身を構成できるようにするプロジェクトが、MITREによって進められています(mitre.org/research/technology-transfer/open-source-software/smartphone-ad-hoc-networking-span)。

またWi-Fi Directによってステーション間の1対1の接続が可能になりますが、この場合、実際にはデバイスの1つがソフトアクセスポイントとして機能します。Wi-Fi DirectはWPS (Wi-Fi Protected Setup)に依存していますが、そこには数多くの脆弱性があります。AndroidはWi-Fi Direct APとして動作することをサポートしていますが、iOSはプロプライエタリのマルチピア接続フレームワークを用いています。とは言え、Wi-Fi DirectソフトAPが動作している別のデバイスにiOSデバイスを接続することも可能です。

またNetgearやGoogleなどのベンダーがワイヤレスメッシュ製品を提供しており、あらゆるタイプの無線デバイスがピアツーピアネットワークに参加できるようにしています。これらの製品は相互運用が不可能な場合もありますが、現在ではさらに多くの製品がEasyMesh標準をサポートしています(wi-fi.org/discover-wi-fi/wi-fi-easymesh)。

テザリングとホットスポット

スマートフォンはPCなど別のデバイスとインターネット接続を共有することができます。こうしたインターネット接続がWi-Fi経由で複数のデバイスと共有されている場合、そのスマートフォンは**ホットスポット**と呼ばれます。スマートフォンをUSBケーブルでPCへ接続することによって、またはBluetoothを介して単一のPCへ接続することによってインターネット接続が共有されている場

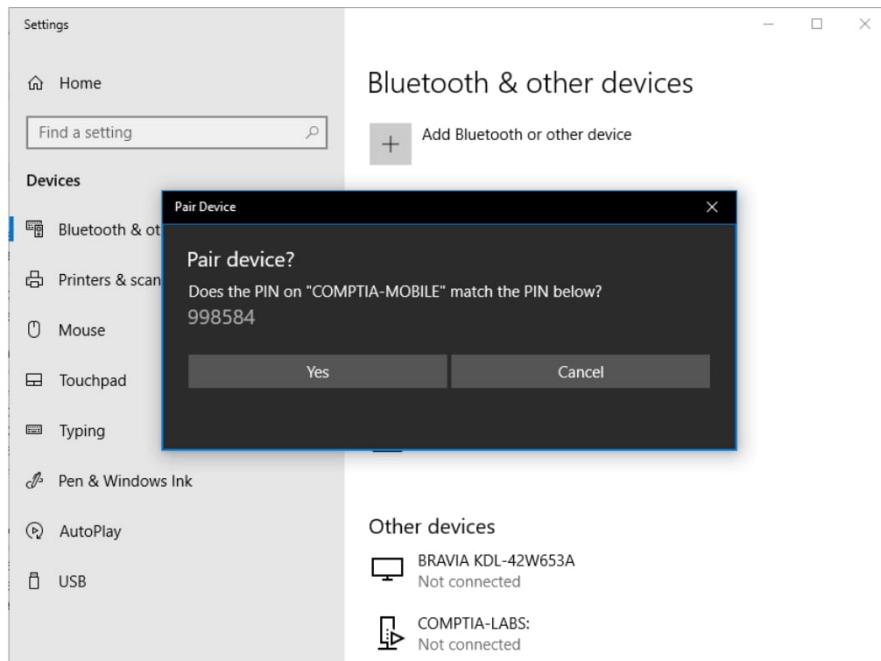
合、これは**テザリング**と呼ばれます。しかし「Wi-Fiテザリング」という用語が、ホットスポットを意味するものとしても極めて広く用いられています。通常このタイプの機能は、デバイスを企業ネットワークに接続するときは無効にされます。データ損失防止やWebコンテンツのフィルタリングポリシーなど、セキュリティメカニズムを回避するために用いられる場合があるからです。

Bluetooth接続方式

BluetoothはPANの実装において最も人気のあるテクノロジーの1つです。ネイティブBluetoothそのもののデータ転送速度は極めて低いものの、別のデバイスとペアリングし、Wi-Fiリンクを用いてデータ転送を行うために使用することができます。この種の接続はiOSのAirDrop機能によって実装されます。

Bluetoothデバイスには既知のセキュリティ問題がいくつかあります。

- デバイスの検出 – デバイスを検出可能モードにすると、近くにある他のあらゆるBluetoothデバイスに接続することになります。残念ながら、検出可能モードになっていないデバイスであっても検知は極めて容易です。
- 認証と許可 – デバイスは両方のデバイスに設定された単純なパスキーを用いて認証（「ペアリング」）を行います。これは必ず何らかの安全なフレーズに変更し、デフォルトのままにしては絶対にいけません。また、リストされているデバイスが有効であることをペアリングリストで定期的に確認してください。
- マルウェア – 概念実証段階のBluetoothワームやアプリケーションエクスプロイトが存在しています。その中で最も有名なのがBlueBorneエクスプロイト(armis.com/blueborne)であり、検知が有効になっているか否かにかかわらず、またユーザーによる介入を一切必要とせず、パッチされていないアクティブなシステムを侵害することができます。また多くのデバイスの認証スキームにも脆弱性が存在しています。最新のファームウェアで常にデバイスを更新するようにしてください。



コンピューターをスマートフォンにペアリングする。
(スクリーンショットはMicrosoftからの許可を得て使用。)