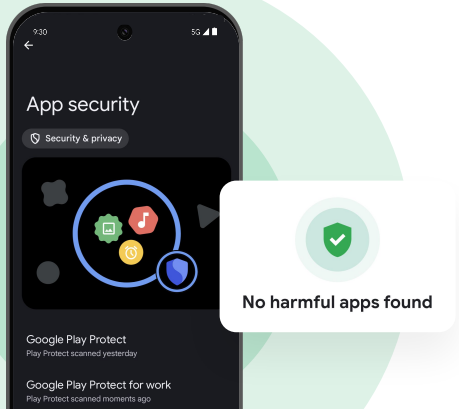
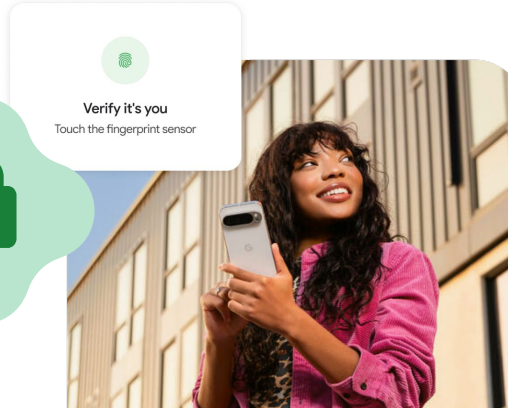
Android

SMB 向け モバイル セキュリティ ガイドブック





はじめに

堅牢なデータ セキュリティの導入は、小規模企業にとって特に重要です。Hiscox[1]によると、セキュリティ侵害を受けた小規模企業の 25% が廃業に追い込まれ、その平均損害額は 20 万ドルにのぼるということです。

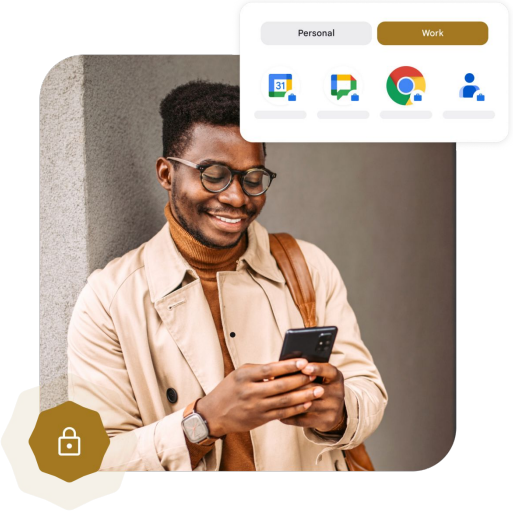
あらゆるものがインターネットに接続されている現代社会では、スマートフォンやタブレットは強力なツールであると同時に、適切に管理されなければセキュリティ上のリスクにもなり得ます。

モバイル ユーザーにとって最大の脅威の一つがフィッシングです。フィッシング サイトの 83% がモバイル デバイスを標的にしています[2]。攻撃者は、AI を使用して、経験豊富なユーザーも騙されるような巧妙な攻撃を仕掛けています。

ビジネス デバイスのライフサイクル全体を管理し、従業員や企業のデータのセキュリティとプライバシーを確保することは、複雑な作業に思えるかもしれませんが、適切なツールを使用すれば、簡単で単純な作業にすることができます。

Android は、シンプルで目立たないセキュリティ保護機能を提供し、企業のデバイスとデータを保護してフィッシング攻撃から防御します。これは、デバイスのセキュリティと管理を行う専任の IT サポート担当者が存在しない企業にとって特に重要です。

このガイドでは、企業データを保護するためのベスト プラクティスを紹介し、Android を堅牢で安全なプラットフォームにしている要素を強化します。



[1] Hiscox Cyber Readiness Report
[2] 2024 Global Mobile Threat Report（Zimperium 社）

Android のデバイス登録モデルについて

デバイスとデータを保護するうえで企業が取り得る具体的な方向性、つまりモデルは 3 つあります。各モデルとも、IT チームがデバイスを管理できる範囲を広げます。

01

1 つ目のモデルは、企業向けモバイル管理（EMM）や管理機能を持たないため、ユーザー主導型に分類されます。このモデルでは、ユーザーのデバイスで特定のセキュリティ設定とプライバシー設定を構成するためのベスト プラクティスについて、企業の IT チームがユーザーを教育および指導します。

02

2 つ目のモデルである Device Trust from Android Enterprise は、ゼロトラストに基づくモデルを提供することでセキュリティを強化します。このアプローチにより、信頼できるソリューション プロバイダは、デバイスが EMM で管理されているかどうかに関係なくデバイスのセキュリティ状態を検査する能力が高まります。これには、ID プロバイダ（IdP）、モバイル脅威防御（MTD）、企業向け検出および対応（EDR）、仮想プライベート ネットワーク プロバイダ（VPN）など、幅広いソリューションが含まれます。Android Enterprise と統合することで、これらのパートナー ソリューションは、企業のリソースへのアクセスを許可する前に、特定のデバイス基準が満たされていることを確認できます。

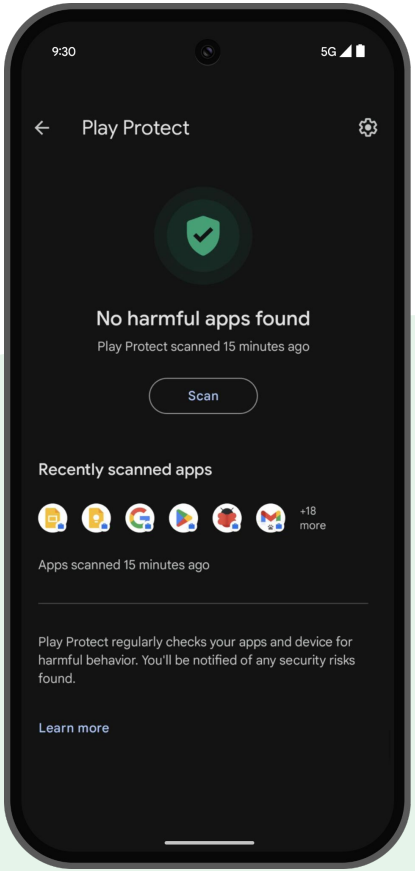
03

3 つ目のモデルは、企業向けモバイル管理（EMM）の管理機能を利用しており、企業は会社所有のデバイスか、個人所有のデバイス（BYOD）であるかにかかわらず、ユーザーのデバイスをより強力に管理できます。個人所有のデバイスの場合、企業が仕事用プロファイルを登録し、個人用エリアのユーザーのプライバシーは保護しながら、IT 部門がこのプロファイルのあらゆる側面を包括的に管理できるようにします。

Android Enterprise は SMB のお客様のニーズに対応する複数のデバイス登録モデルを提供

モデルは統合可能で、SMB は柔軟に選択できるため、ビジネス上のニーズに合わせ、組み合わせて使用できます。Android の堅牢なセキュリティ機能を活用し、後述のベスト プラクティスを導入することで、モバイル環境でも安心して事業を運営できます。

セキュリティの強化に対する Android の取り組みは、その柔軟性と費用対効果とともに、Android が中小企業にとっての最適な選択肢である理由となっています。



各登録モデルのセキュリティ ポリシーと推奨設定

ユーザー主導、デバイス トラスト、EMM の各モデルのガイダンス。

これらのモデルはそれぞれ、要件レベルに基づく、ユーザーのプライバシーと企業の管理策のレベルを念頭に設計されています。

01 ユーザー主導のセキュリティ設定

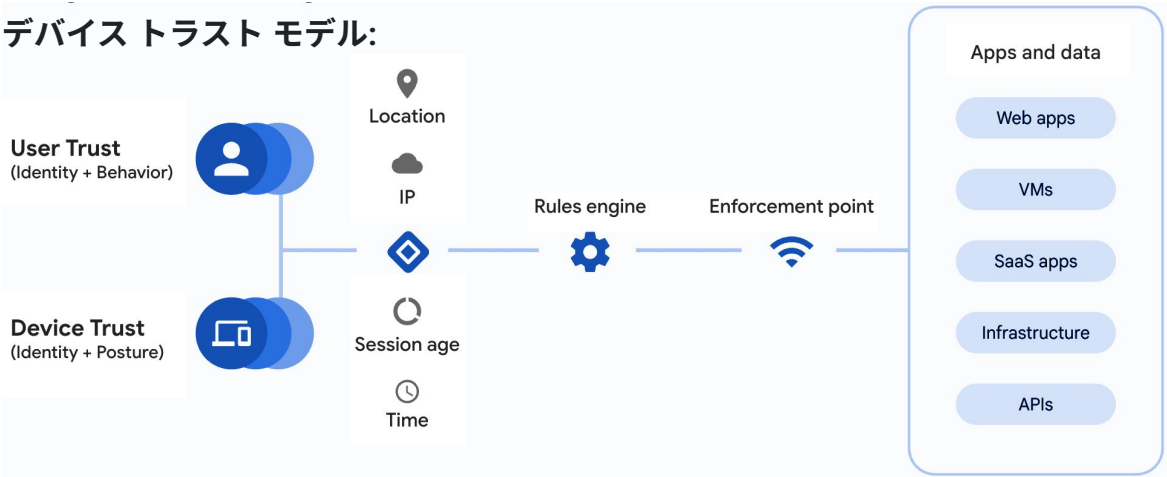
IT チームが、ユーザーのデータと企業のデータを保護するために、Android デバイスで次の設定を手動で行う方法とその理由をユーザーに説明します。

- 盗難検出ロックを有効にする
- リモートロックを有効にする
- オフライン デバイスロックを有効にする
- ID チェックを有効にする
- プライベート スペースを有効にする
- 6 文字以上で繰り返しのない PIN またはパスコードを設定する
- Google Play プロテクトが有効になっていることを確認する
- Google Play からのみアプリをインストールする

02 ゼロトラスト モデル

Device Trust from Android Enterprise で利用可能な管理機能と制限に加えて、IT 部門がセクション 1 のユーザー主導のセキュリティ機能のすべてを設定して活用するようユーザーに指示する必要があります。

デバイス トラスト モデル:



企業の資産に対するアクセスを許可する前に実施するチェックを、以下のリストから選びます。設定の選択はデバイス トラスト パートナーによって異なりますので、パートナーのドキュメントを参照してください。

02 Device Trust from Android Enterprise

企業の資産に対するアクセスを許可する前に実施するチェックを、以下のリストから選びます。設定の選択はデバイス トラスト パートナーによって異なりますので、パートナーのドキュメントを参照してください。

シグナル	説明
デバイスのモデルまたはブランド	デバイスのモデルとブランドを返します。
管理ステータス	管理と管理アプリを返します。
ネットワーク ステータス	デバイス上のすべてのアクティブなネットワークに関する情報を返します。
デバイスのセキュリティ パッチレベル	デバイスの現在のセキュリティ パッチレベル（Google Play システム アップデートのパッチレベルを含む）を返します。
公開済みセキュリティ パッチレベル	デバイス上の対応する更新可能なコンポーネントについて、Google が公開しているセキュリティ パッチレベルを返します。
ディスクの暗号化ステータス	デバイスのストレージが暗号化されているかどうかを返します。
OS バージョンと保留中の OTA	デバイスの OS バージョンと、保留中の OS アップデートの有無を返します。
画面ロックと品質チェック	ユーザーの現在の画面ロックの複雑さを返します。
Play プロテクトのステータス	Google Play プロテクトが有効かどうかを返します。

03 EMM ポリシーの活用

IT 管理者は、これらの最小限のポリシーセットを設定する方法に関する EMM のドキュメントを参照して、ユーザーを保護することができます。EMM を使用すると、IT 部門は、デバイスを仕事用プロファイルのみ、個人利用可能な会社所有（COPE）、または完全管理対象に設定できます。仕事用プロファイルと COPE の場合は、会社が仕事用プロファイルを管理する手段を提供しますが、COPE のみの場合は、デバイス全体をより詳細に管理できます。以下に、考慮すべきセキュリティ管理策の例を示します。

- パスワードの最小文字数 = 6 文字
- デバイスのロック解除の最大試行回数 = 10 回
- Google Play Integrity を有効にする
- スクリーンショットを無効にする
- 仕事用プロファイルへのアカウントの追加を禁止する
- 開発者向けオプションを無効にする
- 提供元不明のアプリのインストールを禁止する
- プロファイル間のコピー / 貼り付けを無効にする
- Android Debug Bridge（ADB）を禁止する
- 許可リストに managed Google Play を使用する
- Chrome: セーフ ブラウジングの無効化を阻止する

企業に Android デバイスを導入する際のベスト プラクティス

01 組み込みのセキュリティ機能を有効にするよう従業員を教育および指導する

ベスト プラクティス

機密性の高いビジネス情報を保護するように作られた追加の組み込み機能により、盗難や不正アクセスからデータを保護します。
以下に例を示します。

A

盗難検出ロックを有効にする。AI、デバイスのモーション センサー、Wi-Fi、Bluetooth を使用して、ひったくり動作を検知し、自動的にデバイスをロックします。

B

リモートロックを有効にして使用する。デバイスを紛失した場合や、盗難にあった場合は、確認済みの電話番号でリモートロックを使用して画面をすばやくロックできます。

C

オフライン デバイスロックを有効にする。デバイスがオフラインになると、オフライン デバイスロック機能によってデバイスの画面が自動的にロックされ、データを保護できます。たとえば、スマートフォンが盗まれてインターネットから切断され、「デバイスを探す」でデバイスを探すことができなくなった場合、オフライン状態がしばらく続くと、デバイスがロックされます。

01 組み込みのセキュリティ機能を有効にするよう従業員を教育および指導する

ベスト プラクティス

機密性の高いビジネス情報を保護するように作られた追加の組み込み機能により、盗難や不正アクセスからデータを保護します。
以下に例を示します。

D

ID チェックを有効にする。ID チェックで本人確認を行うには、生体認証データやその他の安全保護対策が必要です。デバイスで機密情報に関する操作を行うときや、信頼できる場所以外で Google アカウントに変更を加えるときに、本人確認が行われます。

E

プライベート スペースを使ってプライベートなアプリを隠す。Android には、プライベートなアプリケーションを不正アクセスから保護するための「プライベート スペース」機能があります。これを使うことで、デバイス上に隠された専用領域を作成し、そこに個人用アプリを整理できます。ロック解除されたスマートフォンが盗難の被害に遭っても、プライベート スペース内のプライベートなアプリケーションは保護されます。

F

また、Google は、フィッシング対策機能を Google メッセージに直接統合しており、高度な手法のフィッシングからユーザーを保護しています。さらに、ユーザーの保護を強化するスパム対策や Android 発信者番号などの新機能も追加されています。

02 Android Enterprise Recommended ソリューション ディレクトリを使用する

ベスト プラクティス

職場での利用に関して認定を受けたデバイスのリストを、Android Enterprise Recommended ソリューション ディレクトリから作成します。

ソリューション ディレクトリに掲載されているデバイスは、厳格なセキュリティ テストを受け、適切なタイミングでアップデートを受け取ります。

Android Enterprise Recommended により検証されているため、ビジネスニーズに最適化されたセキュリティ強化やセキュリティ機能が組み込まれたデバイスを利用できます。

03 デバイス管理ソリューションを導入して一元管理する

ベスト プラクティス

EMM（企業向けモバイル管理）ソリューションを利用して、セキュリティ ポリシーの適用、デバイスのリモートワイプ / ロック、アプリケーションのインストールの管理を行います。確認済みおよび認定済みの EMM パートナーの一覧は、Android Enterprise Recommended EMM ソリューション ディレクトリでご確認いただけます。

Android と EMM ソリューションが緊密に統合されるため、あらゆる規模の企業で、きめ細かな制御と効率的なセキュリティ管理が可能になります。

04 適切なタイミングでのセキュリティ アップデート

ベスト プラクティス

EMM を通じて Android Enterprise のデバイス ポリシーを使用することで、すべてのデバイスに最新の Android セキュリティ パッチが適用されるようにします。Android Enterprise により、管理者は企業のニーズに合った OS アップデート ポリシーとアプリケーション アップデート ポリシーを適用できます。

Android は、デバイス メーカーと通信事業者のエコシステムで迅速にアップデートが配信されるように、30 日ごとの定期セキュリティ アップデートの提供を約束しています。また、ソリューション ディレクトリの掲載されているデバイスの場合、少なくとも 90 日ごとにアップデートを提供することが要求されています。Google Pixel や Samsung などのデバイス メーカーは、OS アップデートとセキュリティ アップデートを 7 年間提供しています。これにより、潜在的な脆弱性が迅速に修正されます。

05 厳格な認証を実装する

ベスト プラクティス

Android Enterprise の管理機能では、デバイスのロックを解除するパスコードの要件を設定できます。PIN、パターン、パスコードなどがあり、任意で指紋認証や顔認証と組み合わせることもできます。管理者は、組織のニーズを満たす具体的な要件を設定するようユーザーに要求できます。NIST SP 800-53 の最新のガイドラインに従って、少なくとも 6 桁の数字（重複なし）を設定してください。

Android の生体認証サポートと安全な鍵ストレージを組み合わせることにより、ユーザー エクスペリエンスがシームレスになり、ハードウェアを活用した堅牢で安全な認証でデバイスを保護できるようになります。

06 アプリケーションの安全な配備と管理

ベスト プラクティス

Google Play ストア以外からのアプリのインストールを禁止し、Google Play プロテクトを常に有効にすることを必須とします。managed Google Play を使用すると、管理者が承認済みアプリのリストと照合して権限を設定できるようになります。

managed Google Play は、承認されていないアプリのサイドローディングを阻止し、Google Play プロテクトは、インストールされているすべてのアプリをスキャンしてマルウェアがあれば検知します。

07 転送中のデータの保護

ベスト プラクティス

社外からビジネス サービスに安全に接続するには VPN を使用し、すべてのサービスに HTTPS が使用されるようにします。また、企業ネットワークへの Wi-Fi 接続を適切に構成します。

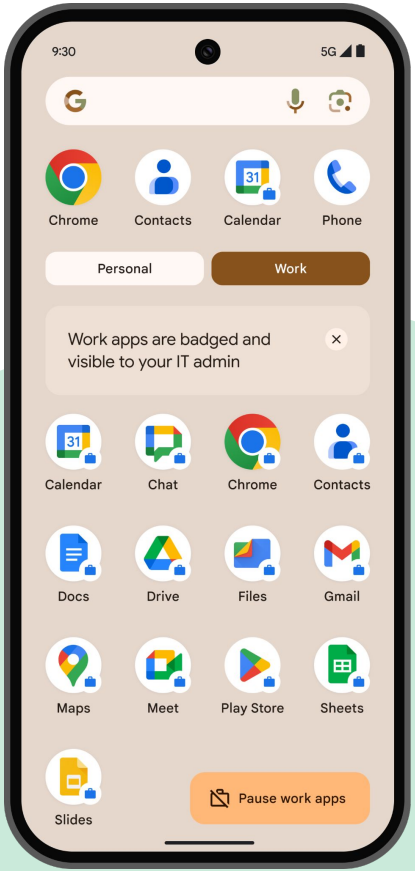
Android が備える暗号化と VPN のサポートにより、デバイスに保存されているデータと、ネットワークで送信されるデータの両方が保護されます。

08 Android 仕事用プロファイルの活用

ベスト プラクティス

従業員が個人用デバイスを使用している場合（BYOD）、管理者が仕事用プロファイルを導入して、1 台のデバイス上で企業データと個人データを分離することを推奨します。

Android 仕事用プロファイルは Android 独自の機能であり、隔離された安全な環境を作成して、企業データの安全性を確保し、個人データのプライバシーを保護します。



重要なポイント

IT 部門やヘルプデスクへの問い合わせを最小限に抑えるには、ユーザーを教育し、3 つのモデルのそれぞれについて、設定に関するわかりやすいガイダンスを提供することが重要です。

認定済みのデバイスとパートナーの選択については、AE ソリューション ディレクトリを参照してください。この情報は、特定の要件に基づいて最適なプロダクトを選択する際に役立ちます。

セキュリティの導入を優先してください。それが基本的なアプローチであってもです。業務用デバイスの保護にかかるコストは、採用するモデルによって異なります。必要なセキュリティと、実装やメンテナンスの費用との間でバランスが取れたモデルを選択しましょう。

Android

詳しくはこちら

www.android.com/enterprise/security