Android Enterprise対応 だからこそできた MDMの堅実性と省力化の両立

各店舗や事務所に散在するスタッフ間の
社内コミュニケーションに活用していたモバイル端末が、MDMのサポート外に。
後継のMDMを「SPPM」にすることで、セキュリティ対策と管理・運用の省力化を実現。

課題　MDMの変更に伴う端末600台のセキュリティやアプリの設定、その後の管理を省力化したい。

解決　SPPMを選択。強固なセキュリティとAndroid Enterpriseの柔軟性により、端末の管理・運用を格段に省力化。

事業者プロフィール

1980年設立。関東一円でパチンコホールやカフェなど33店舗※を展開するレジャーグループ企業。「ピーくん」をキャラクターに、健全で親しみやすい雰囲気づくりとともに、業界に先駆けて遊技フロア完全禁煙ホールや１円パチンコなど、革新的な店舗戦略も展開している。
※2019年12月時点

コーポレート戦略部
中條 宏章さま

MDMによりセキュリティの高いモバイルネットワークを運用

― 以前からMDMを活用していた理由を教えてください。

中條さま　もともと、フィーチャーフォンを IP電話で内線運用して、低コストの社内電話網を構築しようと考えていたんです。しかし、スマートフォンの方が利用価値が広がるんじゃないかと考え直して、スマホベースの社内向けモバイルネットワークを構築しました。また、当社は、セキュリティ対策を特に重視しており、その一環として、MDMを導入して端末を運用していたのです。

― MDMによるセキュリティ対策を具体的に教えてください。

中條さま　テザリングや Wi-Fi接続の通信制限、 USBやSDカードスロットに加え、スクリーンショット機能の無効化などを必須として運用しています。当社は大手キャリアさんが提供するオフィスネットワークサービスに加入しているので、社内の電話は内線番号でかけられるのですが、そこにチャットベースのコミュニケーションアプリを加え、社内の取り組みを迅速に共有するなどしています。スクリーンショット機能を無効化しているのは、こういったアプリ画面からの情報流出を防ぐためです。

MDMの変更に伴う端末600台の新たな設定作業が課題に

― SPPMを導入するに至った経緯を教えてください。

中條さま　端末更改時、それまで使用していた端末がMDMのサポート外になるという問題が発生したのです。そこで、急きょ新しいMDMを探すことになりました。選定にあたっては、同じ轍を踏まないためにも、端末や環境に幅広く対応できるものを探し、キャリアさんにも相談したところ、SPPMをご紹介いただきました。機能を見てみると、望んでいたことが全てできるうえ、利用しているビジネスサービスバックから利用できるのも便利だったため、導入を決定しました。

― MDM変更にあたって不安だったことはありましたか。

中條さま　気がかりは、およそ600台もの端末の設定作業（キッティング）でした。ある程度覚悟はしていましたし、スタッフと手分けして作業することを前提に、更新手順のマニュアルを作るなど準備もしていましたが、時間内に終わるだろうかという不安がありました。だからといって、端末の設定を社員各自にさせるわけにもいかず……。アプリのリストを渡して「これをインストールしてIDとパスワードを設定してください」なんて無理ですよね。できたとしてもサポートは必要になるし、セキュリティの都合上、社員には教えられない情報もあります。結局、こちらで設定してから渡さざるを得なかったんです。

― その不安は解消されたのでしょうか？

中條さま　それが、設定作業の1週間前に「SPPMがAndroid Enterprise（以下、AE）に対応した」という情報が入ってきたんです。その知らせを聞いて「あぁ、これで助かった！」と思いましたね。というのも、AE対応のMDMは、端末を1台ずつ手にとって設定する必要がないんです。設定は、PCの管理画面から端末ごとに設定情報を一括で配信するだけ。せっかくの準備が無駄になっちゃうのか…という考えも頭をよぎりましたが、そこは冷静に（笑）、AEで行こうと決めました。

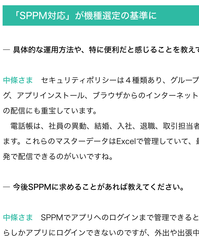
Android Enterpriseで設定も運用も効率的に

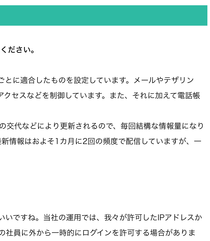
― Android Enterpriseによる一括設定の効果は？

中條さま　とにかくラクで、想定していた半分以下の時間と手間で済みました。端末をMDMからまとめてIDで管理できるので、それぞれにGoogleアカウントを取得・設定する手間が不要なんです。また、Googleアカウントは一定期間使わないと自動失効してしまうため、以前は「久しぶりに使ったらアプリをインストールできない」とか「サービスにログインできない」といったケースがあったのですが、今後はこれらのトラブルもなくなるでしょう。さらに、端末を柔軟にハンドリングできるため、初期状態でインストールされている不要なアプリも容易に削除できる。これも大変便利でした。
　また、AEは、設定時だけでなく運用面でも大きなアドバンテージがあると感じます。

― 運用面での利点を教えてください。

中條さま　当社では、ユーザーをいくつかのグループに分け、それぞれに合わせたアプリやセキュリティポリシーの設定、電話帳の配信を行っています。たとえば、店長以上の役職にはグループウェアやデータベースへのアクセスを許可しています。ここでやりとりされる情報はファイルを含めて重要なものが多く、アクセス権の管理は非常に重要です。
　その点、SPPMはこれらをしっかりコントロールできるので安心です。グループウェアへのアクセス権限を失った社員の端末に対して、そこにログインするためのアプリを直接アンインストールするとかね。当人へのアプリ削除のお願いや削除完了の確認が不要で、非常に便利です。何より、早くて確実なのがいいですね。





「SPPM対応」が機種選定の基準に

― 具体的な運用方法や、特に便利だと感じることを教えてください。

中條さま　セキュリティポリシーは４種類あり、グループごとに適合したものを設定しています。メールやテザリング、アプリインストール、ブラウザからのインターネットアクセスなどを制御しています。また、それに加えて電話帳の配信にも重宝しています。
　電話帳は、社員の異動、結婚、入社、退職、取引担当者の交代などにより更新されるので、毎回結構な情報量になります。これらのマスターデータはExcelで管理していて、最新情報はおよそ1カ月に2回の頻度で配信していますが、一発で配信できるのがいいですね。

― 今後SPPMに求めることがあれば教えてください。

中條さま　SPPMでアプリへのログインまで管理できるといいですね。当社の運用では、我々が許可したIPアドレスからしかアプリにログインできないのですが、外出や出張中の社員に外から一時的にログインを許可する場合があります。そのとき、自動的にログイン状態にできるとうれしいです※。
　とはいえ、AE対応のSPPMはとにかく便利です。次に端末を入れ替える時も、必ずこの環境で使える製品を選びます。そう言い切れるくらい、機能性と使い勝手がいいものだと思っています。

※SPPMはIDやパスを送るという機能を持っており、現時点でもアプリ側の対応次第で実現可能。