## Part2 セキュリティ対策と端末管理の効率化

# MDMで運用負荷を改善

**ユーザー企業の管理者にとって最大の悩みの種は、セキュリティ対策と端末・アプリの管理だ。課題と対策を整理し、iOS端末とAndroid端末を安全に使い、かつ効率的に管理するための方法を探っていこう。**

「お客様のAndroid端末への期待の大きさは感じるが、現時点での引き合いはiPhoneとiPadが中心」

こうした声がよく聞かれる。今後OSの勢力図が大きく変化する可能性もあるが、今のところスマートデバイスの企業導入を牽引しているのがiOS端末であることは間違いない。

これには、iPhone／iPadのプロダクトとしての完成度の高さ、アップルのブランド力もあるが、企業が安心して導入できる安定度の高さも大きく影響しているようだ。つまり、セキュリティ対策と端末・アプリ管理の効率性の面で、iOSはAndroidに比べて安心して導入できる端末と評価されているのだ。

セキュリティ対策と端末・アプリ管理にかかる負荷を軽減し、安全かつ効率的に利用する仕組みは、スマートフォン／タブレット導入の必須の要件となる。

### 鍵は安全と利便性の両立

まず、企業にとって必要な対策を整理しておこう。

基本となるのが、端末自体のセキュリティ対策だ。盗難・紛失時の情報漏洩防止と、マルウェアからの防御がスタートになる。

これまでの事例では、Webサイトやローカルに保存した資料・データの閲覧など、業務システムや社内データとは関わらない形でスマートフォン／タブレットが利用されるケースが多かった。だが今後は、顧客データをはじめとする機密性の高い情報を扱う業務にも活用されるケースが増えていく。その場合、端末内のデータ保護が必須となる。

次に考慮すべきなのが、端末とアプリの管理だ。端末に十分なセキュリティ対策を施しても、社員が正しい使い方をしていなければ意味がない。遠隔から利用状況を監視して、不正な利用法や不要なアプリのインストールを抑制し、ポリシーに沿った使い方を徹底させるための仕組みが必要だ。

また、端末の台数が多い場合には、OSのバージョンアップや業務アプリのインストール等を遠隔から一括で行う仕組みがあると、管理負荷は大きく軽減できる。

これらを実現するソリューションとして、端末とアプリを遠隔から管理する「モバイルデバイス管理（MDM）サービス」が次々と登場してきている。セキュリティ対策と管理負荷軽減の両方の意味で、MDM導入は必ず検討すべきだ。

NTTドコモの「スマートフォン遠隔制御サービス」は、紛失時の遠隔ロック（左）やデータ削除、不正利用を防止するためのデバイス利用制限などが行える。管理者は専用Webサイト（右）にアクセスして複数の端末を一括して管理できる