トレンドマイクロ **Trend Micro Mobile Security**

セキュリティ対策からMDMまで包括提供 スマホ活用の課題をワンストップで解決

不正プログラム対策や危険サイトブロック等のセキュリティ対策と、リモートロック／ワイプや機能制限を行うMDM。スマートフォン／タブレットの業務利用に不可欠なこれらの機能をワンストップで提供するのが「Trend Micro Mobile Security」だ。対応OSも幅広く、安心・安全にモバイルワークを実現するための包括的な環境を整備できる。

スマートフォンやタブレット端末の普及により、社内システムや業務アプリケーションを利用するエンドポイントは多様化していく。これらをどう活用するかは今後、企業の競争力を高めるうえで重要な要素となるだろう。

だが一方で、新たな課題も生まれてくる。社内外のさまざまな場所で活用されるモバイル端末は、その利便性とは裏腹に、情報漏えい等のセキュリティリスクを高め、また管理負荷の増大も招く。iOSやAndroidといった新しいOSは、セキュリティ対策や効率的な管理手法がまだ確立されていない。

幅広いリスク抱えるスマホ 活用法に応じた対策を検討すべき

セキュリティリスクの低減と、効率的なデバイスの管理という、2つの大きな課題をどう解決していくべきか。

トレンドマイクロの転法輪浩昭氏は、「活用の仕方に応じて必要な対策は当然異なってくる。やはり、モバイル端末を何のために使うのかをきちんと定めたうえで、そこから想定されるリスクと対策を考えていくべきだ」と話す。

電話とメール、Web閲覧だけの場合と、社内のメールやスケジューラを利用するユーザー、さらに深く業務システムにアクセスして業務端末として使う場合では、それぞれ求められる対策は異なる。例えば、電話やメールだけであれば、ウィルス対策ソフトを導入し、万一の紛失に備えてリモートロック／ワイプの機能を準備しておけば十分という考え方も成り立つ。一方、業務システムにアクセスするような利用法を広く展開するのであれば、従来のノートPCと同等あるいはそれ以上に厳格な運用ルールを定め、セキュリティポリシーを徹底させるべきだ。

トレンドマイクロ株式会社
マーケティング本部
エンタープライズマーケティング部
プロダクトマーケティングマネージャー
転法輪浩昭氏

スマートフォンの活用法が深くなればなるほど、幅広いリスクを想定し、対策を打つ必要がある。

紛失・盗難時には端末内のデータ漏えいに加え、拾得した第三者からの不正アクセスも防御しなければならない。不正プログラムが増加しているAndroidについては、不正プログラムのインストールや不正サイトへのアクセスを防ぐ仕組みも必要だ。

社員の不正利用も防がなければならない。iOSのJailbreak、Androidのルート化といった不正改造はもちろん、SNSへの書き込みや、Gmail、Dropboxといったクラウドサービスへの同期・転送など、たとえ悪意のない行為であっても情報漏えいのリスクを伴う場合がある。

ウィルス対策も集中管理で徹底 iOS／Android含め4OSをカバー

こうしたリスク対策を行うため、最近では、不正プログラム対策やWeb脅威対策等のセキュリティ対策製品や、端末の管理を効率化するモバイルデバイス管理（MDM）システムが充実してきた。ただし、別々に提供されているそれらの製品をユーザー企業が適切に組み合わせて利用するのは容易ではない。また、複数のツールが混在すれば、運用も自ずと複雑になってしまう。

「Trend Micro Mobile Security（TMMS）」の管理画面（左）。TMMSは「ウイルスバスターコーポレートエディション」のプラグインとして提供されている。拠点や部署等のグループ毎に社内のモバイル端末を集中管理し、セキュリティポリシーの適用等を効率的かつ確実に実行できる。Android端末には、エージェント（右）をインストールし、端末管理のほか、急増する不正プログラム対策やWeb脅威対策等も行える

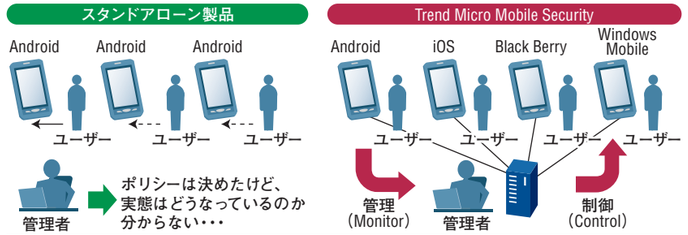
これを解決するため、セキュリティ対策からMDMまでを包括的に提供するというコンセプトで開発されたのが「Trend Micro Mobile Security（TMMS）」だ。トレンドマイクロが得意とするウィルス対策やWeb脅威対策に加え、MDM機能もワンストップで提供する。さらに、従来はWindows MobileとAndroid OSを対象としていたが、1月から出荷を開始したv7.1ではiOSとBlackBerryにも対応。4種類のOSが混在した環境でも、単一のコンソールからセキュリティ対策と端末管理を行うことが可能になった。

さらにもう1つ、大きな利点がある。ウィルス対策やWeb脅威対策も集中管理することで、その確実性を高められるのだ。

MDMは、端末を遠隔から監視・制御し、パスワードの設定をはじめポリシーに則った運用を徹底させることを目的としている。だが、ウィルス対策やWeb脅威対策ソフトウェアはスタンドアロン型が一般的だ。社員に端末を配布した後、パターンファイルの更新やスキャンの実行といった運用は“ユーザー任せ”となる（図表）。極端な場合、ソフトウェアをアンインストールされたり、スキャン機能などをOFFにされても、管理者からはそれを把握し難い。

せっかく有効なソリューションを導入しても、その運用がユーザー任せでは宝の持ち腐れとなりかねない。特に、Androidについては不正プログラムが急増しており、そのリスクは日に日に高まっている。「セキュリティ対策も含めて端末の情報を可視化し、管理者がポリシーを適用できるようにすることが不可欠だ」（転法輪氏）。

図表　スタンドアローン vs 集中管理



	スタンドアローン	集中管理
インストール	ユーザー任せ	管理者がインストール済みデバイスを把握できる
各種設定	ユーザー任せ	管理者が状況の把握や設定の強制ができる
運用	各デバイスにログが残る。ユーザーが確認するだけ	管理者が一元的にログを管理できる

→セキュリティポリシーのコンプライアンスが低い　→モバイル端末の運用、管理にガバナンスを確立

そのためTMMSでは、MDM機能だけでなく、ウィルス対策やWeb脅威対策についても、管理者が遠隔から集中管理できるようにしている。v7.1では、Android向けセキュリティ対策の集中管理機能も大幅に強化した。

例えば、不正プログラム対策については、一定期間ごとにパターンファイルの更新を強制したり、Androidマーケットでアプリをダウンロードする際に対象ファイルをスキャンさせたりといった設定を管理サーバーから行える。社員が設定を勝手に変更できないようにすることも可能だ。

もしウィルスが検出されれば、情報をポップアップして不正プログラムをアンインストールするのはもちろん、管理者はコンソールでログを確認することで、どのデバイスでどのような不正プログラムが見つかったのかを把握できる。

ワンストップ提供で運用負荷軽減 PCとの一元管理も視野に

リモートロック／ワイプやパスワードポリシーの設定、機能ロック（Wi-FiやBluetooth、カメラ等を使用不可にする）といったデバイス管理も、ウィルス対策やWeb脅威対策といったセキュリティ対策も、スマートフォンやタブレットを安心・安全に利用するうえではともに必要不可欠なものだ。これらを1つのインフラにまとめることができれば、運用負荷の軽減にも大きく貢献する。

また、TMMSは、法人用のPC向けウィルス対策で最も広く利用されている「ウイルスバスター コーポレートエディション」のプラグインの形で実装されており、そのユーザーであれば、同じ管理サーバーでTMMSも管理することが可能。PCのセキュリティ対策ソリューションとインフラを共通化できることも利点の1つだ。

現在はスマートフォン／タブレットが普及し始めた段階であり、PCとは別にセキュリティと管理の仕組みを構築する例も多い。だが、いずれは社内リソースを活用して業務を行う多種多様な端末を一元的に管理・運用したいというニーズも強くなるはずだ。

そうした将来を見越してトレンドマイクロでは、「PCもモバイル端末も含めて、多様化するエンドポイントをすべて一元的に管理することをコンセプトに包括的なソリューションを開発していく」（転法輪氏）方針だ。

お問い合わせ先
トレンドマイクロ株式会社
法人お問い合わせ窓口
TEL：03-5334-3601
URL：http://www.trendmicro.co.jp/mobile-security/