視点を変えて可能性を広げるITの新活用術（第11回）

社外モバイル機器管理の要「MDM」。一体何だろう？

2024.03.14

オフィスでも自宅でもどこでも働けるハイブリッドワークが普及している。この自由な働き方を支えているのがモバイル通信環境だ。そこではノートパソコンやタブレット、スマートフォンなどのモバイルデバイスが活用される。ただし、自由な反面リスクもある。悪意を持ったプログラムに感染したり、盗難や紛失によって情報が漏えいしたりすることなどだ。これらのリスク対策として注目されているのがMDM（モバイルデバイス管理）である。

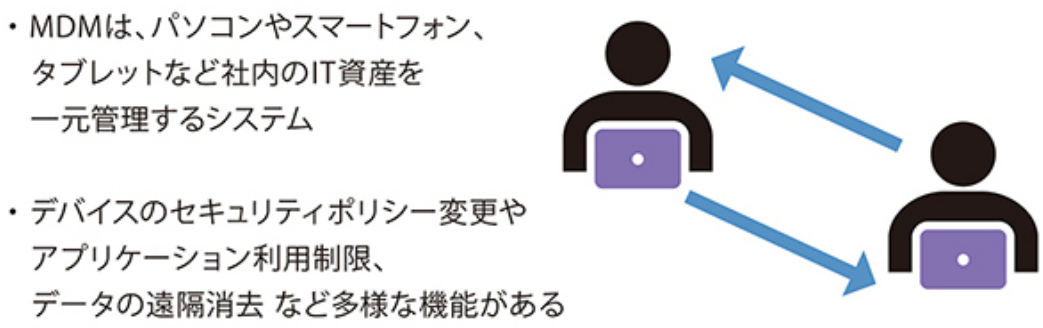
働き方の環境が変わるとセキュリティリスクも変わる

社外でも仕事ができる環境になると、企業が支給したモバイルデバイスや従業員個人が保有するモバイルデバイスを企業内のシステムに接続して業務をこなすようなケースも増えてくる。しかし、なんの対策も講じることなくモバイルデバイスの利用を許してしまうことでリスクも増大する。

従業員が私的にWebを閲覧したことでウイルスに感染して、そこから社内のシステムに侵入されて情報を盗まれるケースや、モバイルデバイスそのものが盗まれて、内部のデータが抜き取られたりすることもある。不用意にフリーWi-Fiに接続して業務をすることで、通信内容をのぞき見されてしまうという危険もある。

こうしたリスクを回避するために、ノートパソコンやタブレット、スマートフォンなどさまざまなモバイルデバイスを一元的に管理するソフトウエアがMDMである。一般的にはモバイルデバイスのセキュリティ保護、モバイルデバイスのデータの保護、アプリケーションの管理、モバイルデバイスそのものの管理などの機能が提供されている。

自社で使われているモバイルデバイスに対応しているか、必要な機能が提供されているか、提供形態はどうなっているのか、などチェックした上でMDMを導入し、登録されたデバイスだけが社内のシステムに接続できるようにすることで、モバイルデバイスを安全に利用できるようになる。



MDMのメリットを生かして安心して自由に働くことのできる環境を… 続きを読む