Why not Mac?

vol.3

Macは安心・安全なのか？

“ Macの企業導入が進む一つの理由は
セキュリティがしっかりしているから ”

利便性とセキュリティは表裏一体

日常の業務に利用するITシステムに対して、セキュリティ対策を何も講じていない企業はないはずだ。セキュリティポリシーを遵守させることは、企業や従業員を守る上で大事なことである。自分たちだけでなく、クライアントや取引先、社会的立場も含めて、その企業に対する信用に大きく影響するからだ。どれだけ時間をかけて積み上げてきた信用も実績も、一つのセキュリティ事故で失うのは一瞬である。

企業のMac導入の現場では、Macの管理方法の経験やノウハウが少なく、セキュリティ対策についても、Windows PCと同等レベルの設定を行うことが多い。ウィルス対策ソフトのインストール、パスワードポリシーの遵守、アカウントの権限設定など、設定すべき項目は膨大だ。セキュリティ設定を手動で行なっていたり、WindowsだけでなくMacにも対応したセキュリティツールなどで部分的に対処しているような現状だ。

これらセキュリティ設定を行うことは利用者の利便性と反するものも多い。アカウントの権限がなければ自由にアプリケーションを追加することができず、都度、管理者に依頼をして追加のインストール作業を依頼することになる。利用者にとっても管理者にとっても手間ばかりかかって、生産性を高めるはずのMacが、コストになってしまっていることもある。また、企業が定めるセキュリティポリシーが的確に設定されていない状態でセキュリティ事故が発生した場合、その損害は甚大なものになってしまう。企業にとって、セキュリティ対策は信用を守る上でも、企業存続の上でも、誰もが避けて通れないものだ。

Apple製品がエンタープライズ市場で受け入れられている理由の一つとして、「セキュリティがしっかりしているから」という理由が挙げられる。Appleが他の企業と比較してもセキュリティに対する意識が高い企業であることは明白だ。iOSデバイスと同様にMacに対しても、利用者のセキュリティを守るためのシステム保護や暗号化の技術が標準機能として実装されている。ハードウェアとソフトウェアを同じ企業が開発、製造し、サービス部分も含めて統合的にセキュリティを考えているからこそ、安全性と堅牢さを兼ね備えたセキュリティ機能が提供できるのだ。

こうした標準搭載のセキュリティ機能を最大限に活かすためにも、各機能への理解や適用方法、自社のセキュリティポリシーと現在のモバイル中心のビジネスを照らし合わせて、最適なセキュリティ設定を施さなければならない。「Macはウィルスには感染しない」といった通説はもはやエンタープライズ市場では通用しない。会社のデータ資産をしっかり守る上でも、Macのセキュリティ対策は企業にとって重要な責務である。

Macの導入検討段階では、ワイヤレスでファイル共有が可能になるAirDropやiOSデバイスとの連携機能など、様々な標準機能の利用を想定される。しかし、セキュリティを守るためという理由から、最終的に全てのMac特有の生産性を高めるための機能が制限されてしまっているのが現状だ。セキュリティ対策は単に利用するデバイスの機能を制限するだけでなく、システムにアクセスするユーザやネットワーク、扱うデータなど、様々な側面で検討する必要があるため、Macの機能を制限するだけでは、対処しきれない問題も数多く存在する。オンプレミスな環境で自社内のネットワーク内を監視していればデータ資産が守られていた時代はとっくに終わっている。クラウドサービスの利用を前提とした現代においては、従業員がどのようなデバイスを使い、どのネットワークを経由して、会社のデータ資産にアクセスするのかを、モバイル前提で検討を始める必要がある。

AppleはiOSデバイスと同じ管理フレームワーク（MDM）をmacOS向けにも提供している。これにより、Macのセキュリティ対策に必要な設定を、MDMから一括かつ遠隔で適用することが可能だ。iOSデバイスを設定するかのように、Macに対して企業のセキュリティポリシーを適用できる。

会社の資産やデータを守るためとはいえ、何でも制限すれば良いというものではない。セキュリティ設定は業務上適用しなければならないものにしなければ、ユーザの利便性は下がる一方である。しかし、利便性や生産性を優先して、セキュリティ設定は見逃していいというものではない。セキュリティ設定の検討は、現在のビジネスの状況や現場の用途、外的な環境要因の変化など、様々な角度で検討することが望ましい。昔導入したシステム導入時に策定したセキュリティポリシーでは、テクノロジーの進化や変化の激しいビジネスには対応できない。セキュリティポリシーに対しても、柔軟に対応していくための基盤が必要となる。

Macのセキュリティ対策ができれば完璧というものではない。最終的には利用者が扱うデータに対して、日々どれだけリスクを意識して業務が行えているか、だと思う。利用者のミスや故意の事故であったとしても、システムのセキュリティ設定だけでは守りきれない。何よりも大事なことは、日常的にセキュリティに対する意識を高めること、そしてリスクを想定しながら業務を行うこと、そうした日々の教育やリテラシー向上が一番のセキュリティ対策になることは明白だ。