Part2 BYODを実現する新技術

多要素認証で管理負荷低減

BYODを実現するには、セキュリティの担保と管理負荷の軽減を両立するポリシーベース認証などの仕組みが不可欠となる。柔軟なワークスタイルを支える新たな要素を取り入れ、企業ネットワークが進化する。

スマートデバイスを業務に活用する目的で、社内の無線LAN、あるいは社外から3G網などを経由してイントラネットにアクセスさせる環境を整備する企業が増えている。

この場合、セキュリティ対策が重要になることは言うまでもないが、今後は会社支給と私物端末の混在環境を前提とする新たな企業ネットワークが求められるようになる。

こうしたニーズに対応すべく、セキュリティベンダーはBYODを見据えたソリューションの提供、機能拡張に注力している。

「マルチデバイス化」が加速

BYODとは、社員が使い慣れた端末、あるいはその時々の業務の特性によって最適な端末を選んで業務を行うことができる手段だ。これまでデスクトップPCやノートPCから、よりモビリティ性の高い携帯電話やPDAへと業務端末が広がってきた「マルチデバイス化」の一環と捉えられる。

こうした変化は、ネットワークの多様化と合わせて考えるべきだ。例えば、自宅のPCやスマートデバイスを操作端末として、インターネット経由で社内システムを使う在宅勤務の場合、自宅の固定回線や公衆無線LANなどのネットワークが使われる。つまり、BYODは「マルチデバイス化」と「マルチネットワーク化」が共に進むものといえるだろう。

ポリシーベースのアクセス制御を可能にする「Cisco Identity Services Engine（ISE）」の画面（左）と、セキュリティクライアント「Cisco AnyConnect Secure Mobility Cilent」

こうしたアクセス手段の多様化を見据えて昨年、トータルセキュリティソリューション「Cisco Secure X」をリリースしたのがシスコシステムズだ。

BYOD実現の鍵はコンテキスト

Secure Xは、マルチデバイス対応のセキュリティクライアント「Cisco AnyConnect Secure Mobility Cilent」や、ポリシーベース認証プラットフォーム「Cisco Identity Services Engine（ISE）」等の同社の製品やサービスを統合して構成される。さらに、モバイルアイアンが提供するMDM（モバイルデバイス管理）、サイバートラストや日本ベリサインのデジタル証明書ソリューションなどと連携し、包括的なセキュリティ対策が行える。

BYOD対応という点での最大の特徴は、「いつ、誰が、どこから、何へ」というコンテキストに基づいた制御により、ダイナミックにポリシーを管理できる点だ。このポリシーベースのアクセスコントロールがBYODではキーポイントとなる。

会社支給端末を前提とした管理とは異なり、私物端末も混在する環境では、ユーザー情報（誰が）に加えて、端末やアクセスポイント（どこから）、利用しているコンテンツ（何を）といっ