# 働き方に起きているパラダイムシフトは社内ネットワークのあり方も変えつつある

企業内のオフィス・ネットワークは、多様な働き方を求めWi-Fiの導入、スマートフォンの普及など、ワイヤレス化、マルチデヴァイス化の浸透により変革が求められている。そこでは保護されて安全なネットワークというのは存在しないという「ゼロトラスト」をベースに、新しい企業内ネットワークの再構築が必要だと、IBMの山下克司は断言する。

山下　克司| 日本IBM グローバル・テクノロジー・サービス事業本部 Distinguished Engineer。ネットワークおよびクラウド分野でIBMのテクノロジーを牽引する。

## 企業ネットワークに変革が求められている

ネットワーク技術や構築手法は、めまぐるしく進歩しています。企業のオフィス・ネットワークを見ても、有線LANのみという時代はとっくに終わり、Wi-Fiが当たり前に使われるようになっただけでなく、スマートフォンの普及という新たなワイヤレスネットワークの波が訪れています。
ところが、2000年代の初頭あたりから大半の企業ではネットワーク管理の仕方というものがあまり変わっていません。テクノロジーが先行してしまい、企業側の体制や管理技術の導入が追いついていない状況なのです。

どうして新たな技術の導入が進まないのかといえば、ネットワーク管理をIT部門ではなく、総務部門や施設部門、購買部門といった部署が担ってきたことが影響していると考えています。有線LANは、内線電話などと同じように扱われていることが多いのです。

オフィスの移転や組織変更などに伴い、ネットワーク設備にも変更や修正が発生します。こうした業務は、総務・施設部門の担当者が、オフィス施設の事業者に、家具と一緒にネットワークまわりもまとめて丸投げしているケースも少なくありません。これでは、最新のネットワーク技術を検討することも、細かな要望を把握することもできないケースがあります。

有線LANだけで企業内ネットワークが構成されていた時代なら、オフィス内の島ごとに必要なポート数のネットワークハブを設置し管理していれば問題はありませんでしたが、オフィスの環境は大きく変化しています。

スマートフォンのようなモバイルデヴァイスを多くの社員が持ち込み業務に利用するような時代では、もはや有線LANのポート数を数えるだけではネットワーク管理とはいえません。なぜなら、スマートフォンのように生まれながらにしてインターネットに直接繋がっているデヴァイスが、大量に社内ネットワークにも繋がることを意味しているからです。

## オフィス・ネットワークセキュリティーの根底思想が、性善説から性悪説へシフト

これまで、多くの企業において社内のネットワークのセキュリティーは「ゾーニング」を基本に設計されてきました。インターネットからの入口にはファイヤーウォールを設置して、内部のネットワークを保護し、外部からアクセスする必要があればVPNを用いる。社内のネットワークには、社内のPCから社員だけがアクセスする、だから安全。これがゾーニングの考え方です。

しかし、スマートフォン時代においては、もはやゾーニングでは十分なセキュリティーを担保できないのです。企業内のネットワークに有線と無線が混在し、社員は複数のデヴァイスから複数の経路で社内のネットワークやイントラ向けのサーヴィスを利用します。そして、いまの時代にモバイルデヴァイス、すなわちスマートフォンを業務で使わないという選択肢は非現実的です。

そこで、社内、特にオフィス・ネットワークのセキュリティーに「ゼロトラスト」という新たな考え方が登場しました。社員性善説で成り立っていたゾーニングではなく「誰がどの端末を使ってアクセスしてもセキュリティーを守る」という、インターネット上のアプリケーションと同じ考え方をオフィス・ネットワークで利用される企業内アプリケーションにも取り入れる考え方です。

> 多様なワークスタイルやビジネス・コラボレーションの推進が、企業の競争力や信頼性に繋がるようになったいま、ネットワークというインフラを武器にすることが、新しいビジネスのイノヴェイションになる

セキュリティー的にも社内ネットワークを信用してはならない時代です。いくら社員教育を進め、社員が正しくデヴァイスを使ったとしても、デヴァイスが常に正常とは限りません。セキュリティー保護の側面から考えれば、オフィス・ネットワークはもはやインターネットと大差ない、信頼できないものだと考えるべきです。そして、社内向けのサーヴィスであっても、アプリケーションやデヴァイス自身がセキュリティー保護のための特化した機能を持ち、自らの業務とデータを守ることが重要です。

オフィス・ネットワークにゼロトラストの考え方を導入すると、コスト上のメリットもあります。それはネットワークの設計がシンプルになり、フラットなネットワークとすることができるためです。

そして、ネットワークはフラットにする一方で、アプリケーション・サーヴィスは厳密に管理されたユーザーIDによって、厳密にアクセスコントロールを施します。さらにアクセスする端末のデヴァイス情報や回線番号等を組み合わせて多要素認証をかけることで、高度なセキュリティーを担保します。そしてアプリケーションやデータは、データセンター内部で、インターネット接続しているアプリケーションと同様に厳重に保護、管理します。

## フラットなネットは低コスト、かつ多様なワークスタイルを可能にする

こうした新しいオフィス・ネットワークの考え方を導入することで、社内からだけでなく社外のネットワークからも企業内システムが安全に利用できるようになります。こうしたネットワーク管理のもとでは、在宅勤務やリモートオフィスから企業内システムへの接続がしやすくなり、多様なワークスタイルを実現できるようになります。

オフィス・ネットワークにゼロトラストの考え方を導入すると、コスト上のメリットもあります。それは社内ネットワークの設計がシンプルになり、フラットなネットワークとすることができるためです。

IBMでは、以前からノートPCだけでなく、スマートフォンなどの通信機器とリモートアクセスの手段を社員に提供しており、多くの社員がマルチデヴァイスから社内のシステムへアクセスしていました。このため、東日本大震災の発生時には、約95パーセントの社員が出社できなかったにもかかわらず、自宅などから通常通りの業務を行うことができました。

被害に遭われたお客さまから、システムの復旧や対応について多くの問い合わせがありましたが、それに迅速に対応することができました。この震災によるIBMの出社状況は想定を越えるものでしたが、ゼロトラストに基づいたネットワーク設計と普段からの運用により、耐えることができました。

ネットワーク環境だけでなく、社員の働き方の多様化や非常時の事業継続性など、時代の要請は高度化していきます。それに合わせて社内ネットワークに求められるものも、変化していきます。これまでのゾーニング設計から脱却しゼロトラストネットワークを構築することは、現時点においてその変化の際たるものです。

そしてゼロトラストをベースにネットワークやシステムを再設計していくことは、日常の働き方のなかにレジリエンシー、すなわち柔軟性や回復性を潜ませることです。わたしたちが3・11で学んだ事は、非常時に役に立つのは平常時に利用できているものだけでした。それによって、いざというときでもいつもと同じように働くことができるのです。

出典：Webサイト「INNOVATION INSIGHTS」(2015年11月 掲載)

モバイル・ネットワーク環境の設計・構築をご支援します

**IBM 無線LAN マネージド・サービス**
http://www-935.ibm.com/services/jp/ja/it-services/networking-services/cisco-meraki/index.html

**日本アイ・ビー・エム株式会社**
グローバル・テクノロジー・サービス
〒103-8510 東京都中央区日本橋箱崎町 19-21

IBM、IBM ロゴ、ibm.comは、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。 現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。