

米国セキュリティベンチャー事情 と日本のセキュリティビジネス

住商情報システム株式会社
JNSA 幹事・技術部会長 二木 真明



この数年、米国のベンチャー企業を訪問し、日本で売れそうな製品を探してローカライズするなど、日本での販売まで持ち込む仕事を中心にしてきました。しかし、最近、そうした仕事に困難を感じるようになってきました。それは、かつて、夢と希望にあふれてIPO（株式上場）を夢見たベンチャー企業が、ITバブルの崩壊なども経験し、短期間でリターンを求める投資家の志向もあって、特定の狭い範囲の技術に特化してしまうようになってきたからです。これは、自ら新しい市場を切り開き、そのリーダーとなることを目標とするのではなく、既存の市場で優位性を確保する道具となりそうな要素技術に特化し、その技術をメジャープレイヤーに買ってもらうという方向にほかなりません。IPOを目指すには長い期間を要し、IPO後にはさらに大きな社会的責任が待ち受けています。より安易な道を目指す方向は、経営的な視点からは正しいのかもしれませんが。我々もかつては特徴ある製品を開拓し、日本で市場を開拓し、時間をかけて育て上げる余裕がありましたが、今はもうそんな余裕はありません。実際、こうした形で製品開拓をしてきた企業の多くが、同じ困難を感じているはずで、つまり、競争力のある製品をいち早くみつけ、先行利益を確保するようなビジネスモデルは難しくなりつつあり、大手のベンダが提供する製品やサービスを同業他社と競争して売りながら、自分たちの付加価値をつけ、それをいかにお金にしているのか、ということ、いままで以上に真剣に考えなければいけなくなっているわけです。

一方、セキュリティという世界も様変わりしつつあります。かつては、セキュリティといえば、専門性の高いビジネスであり、それ単独で成り立つと考えられてきました。しかし、実際は、ITのいたるところにセキュリティは必要で、それらのセキュリティはITの各分野と密接に関連しています。たとえばアプリケーションシステムの開発に業務知識が不可欠なように、セキュリティにおいても、その分野ごとに必要な知識が異なりますし、こうした知識がまったくない状態では、セキュリティを語るものが難しくなっています。たとえば、ネットワークを知らないファイアウォール技術者はもはや通用しませんし、Webセキュリティを語るには、データベースやプログラミングの知識や経験、開発プロセスの知識が不可欠です。そういう意味では、セキュリティというかつて独立していた世界の多くの部分が、ITというより大きな領域と融合しつつあると言えるでしょう。ITメジャー企業がセキュリティ企業を買収するという動きが激しくなっているのも、こうしたことを裏付ける現象では

ないかと思えます。こうした中で、ITの総合力をつけていくのか、もしくは、より専門特化した方向を目指すのか、米国のベンチャー企業と同じ選択を我々は迫られているのかもしれません。

ユーザとの関係も変化しつつあります。米国では、ユーザ企業の多くに、ベンダのカウンターパートとなりうる専門家がいます。これによって、おのずとユーザ、ベンダの責任範囲が決まり互いの仕事のバランスがうまくとれているように見えます。日本ではまだまだ、ユーザ側にそうした人材が少ないこともあり、ベンダが多く仕事をユーザにかわってしなければいけないケースも多くあります。しかし、セキュリティの要求が多様化する中で、ベンダ側にはセキュリティのみならずITの総合力も求められるようになる上、ユーザ側の担当者と共通する土俵がないために、意識や認識の違いが浮き彫りになってしまうことも少なくありません。こうした問題の解決には、ユーザ側にも我々のカウンターパートとなる専門家が重要なのではないかと思えます。これは、私自身がこの2年ほどのあいだで、自社のセキュリティに主体的にかかわるようになって特に感じ始めたことです。

現在、教育サービスで提供されているトレーニングは、どちらかといえば業界側の技術者を育成するものが中心です。(本来はそうでなくても、現実にはそうなってしまっているのではないかと思えます。)しかし、これからは、ユーザ側でプロジェクト全体を統括できる、ジェネラルなセキュリティ知識をもった専門家の育成も重要なのではないかと思えます。こうした方向での教育サービスを提供できないだろうか、提供できたとして、ユーザにうまく受け入れてもらえるのだろうか、など、なかなか悩みは尽きません。業界のこれからの方向を見極めていく上でも、大いに議論してみてもうだろうかと考えているこのごろです。