

商談の軌跡

所在地:東京都世田谷区
長:大谷哲夫
設立:1904年
学生数:学部14969人、大学院276人(2004年10月時点)
教員数:930人(非常勤を含む)
事業内容:仏教学部、文学部、経済学部、法学部などの各学部、および研究科(大学院)

駒沢大学

発注

アイ・オー・エス

飛び込み営業でセキュリティ商談獲得 大手による囲い込みの間隙を突く

顧客の要望を先読みした情報提供が決め手に

アイ・オー・エスが、飛び込み営業をきっかけに駒沢大学のセキュリティシステムを受注した。飛び込み不毛地帯である大学市場に食い込めた勝因は、顧客の要望を先読みした提案だ。(文中敬称略)

「多い月は20人の飛び込み営業と会う。ただし、合格する営業担当者は20～30人に1人」——。駒沢大学 総合情報センターで係長を務める徳本克彦が実践するITベンダーとの付き合い方だ。

駒沢大学は2006年に、ネットワークのセキュリティ対策を大幅に刷新する。目的は、教員や学生が、ウイルスに感染したパソコンを学

内に持ち込んでウイルスがまん延するといった事態を防ぐこと。徳本が飛び込み営業を受けるのは、新しいセキュリティ対策の検討材料を収集するためなのだ。

セキュリティ強化の第一歩として駒沢大学は昨年3月、ファイアウォールやウイルス対策、IPS(侵入防止システム)などの機能を備えた統合型セキュリティシステムを

導入した(図1)。ウイルスに感染したパソコンが学内の無線LANに接続した場合でも、基幹ネットワークに被害を広げずに済む。そして、この商談を受注したのは、徳本の厳しい飛び込み営業審査を通り抜けたアイ・オー・エス(IOS)の井上倫文だった。

通常、大学は特定のベンダーに囲い込まれており、飛び込み営業の不毛地帯ともいえる。駒沢大学もインフラ部分を伊藤忠テクノサイエンス(CTC)が、がっちり握っており、2006年の大刷新もCTC主

システム導入前の課題

- 教員や学生が外部から、ウイルスに感染したパソコンを持ち込んで学内ネットワークに接続してしまう
- 学内に約300拠点の無線LANアクセスポイントを設置したため、持ち込みパソコンの接続が増えた
- 個々の教員や学生にセキュリティ対策を強制するのは困難

システム概要

学内にある無線LANからの攻撃を防ぐセキュリティシステム

稼働時期

2004年3月

受注金額

約500万円

システム導入による効果

- 大学内の無線LANにウイルスが持ち込まれたとしても、基幹ネットワークは攻撃されない
- 教員や学生に負担をかけることなく、セキュリティ対策ができた

導で進んでいる。一見、食い込むのが不可能な状況に思えるが、井上は顧客の要望を先読みした提案を地道に続け、数少ないチャンスをモノにした。

飛び込み営業でいきなり受注

井上が飛び込み営業をかけたのは2002年6月(34ページの図2)。当時、駒沢大学は、セキュリティ対策の強化を検討し始めていた。教員や学生が、悪意のあるWebサイトにアクセスしてウイルスに感染するとか、持ち込みパソコンからウイルスが広がるとかいった問題が発生したのだ。

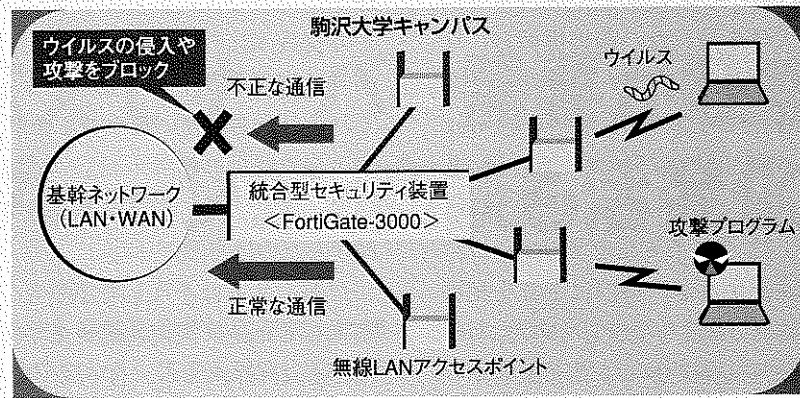
企業とは違い、大学には教員や学生の私物パソコンがたくさん存在する。その上、駒沢大学は私物パソコンでも、学内各所に設置された無線LANのアクセスポイントやインターネットを介して学内ネットワーク「KOMAnet」に接続できるようにしていた。便利な反面、大学内でのウイルス感染は増える一方だった。

セキュリティ強化が必要なことを痛感しつつも、システム畑出身ではない徳本たちには、知識や情報が足りない。そのため、飛び込み営業も情報収集の一環として断らなかった。ただし、使えない営業担当者には、30分で「帰ってくれ」と言い渡す。付き合いが続く営業担当者のごくわずかだった。

井上も最初は、数多くやってくる飛び込み営業の一人。その際にはURLフィルタリングソフトの提

図1 ●駒沢大学が導入したセキュリティシステムの概要

教員や学生はキャンパス各所に設置された無線LANのアクセスポイントを使って、学内ネットワーク「KOMAnet」に接続できる



案を行った。「小中学校ではURLフィルタリングが必須。同じ教育機関の大学でも必要とされるかもしれない」。こう考えた末の選択だった。

ところが、総合情報センター副所長の中山文法から、「大学は学びの機会を広く提供するところで、研究、学習情報を収集できることの方が優先する」と諭された。当ては外れ、この提案はあえなく却下されてしまう。ただし、井上はそこで引き下がらなかった。大学のセキュリティ全体に関する話に変えたのである。すると、ウイルス対策ソフトのライセンス更新が翌月に迫っているという。井上はその場で、安価な教育機関用のライセンスを紹介した。

「そんなに安くなるのか」。徳本たちの目の色が変わった。従来のベンダーは、教育機関用のライセンスを提案していなかったのだ。ライセンス変更であれば、手間を

かけずにコストを削減できる。なにより徳本は、井上が要望を持ち帰ったりせず、その場で新たな提案を出してきたことが気に入った。井上は受注とともに、顧客の信頼を獲得した。これがセキュリティシステム受注の布石となった。

予算の把握が決め手に

コストは低減できたものの、根本的なセキュリティ対策は見つからない。「内部からの感染をなんとか防止できないものか」。徳本たちは2003年に新たなセキュリティ対策のための予算を確保し、構築に向けて本格的に動き出す。CTCにもセキュリティシステムの提案を依頼。しかし、出てきた見積もりは徳本たちが確保していた予算と、大きくかけ離れたものだった。自分たちでもシステムを探したが、予算と機能の両方を満足するものは見つからなかった。

「仕方がない。対策予算は次年度

に持ち越すか」。このような考えが徳本の頭をよぎった。まさにその時、井上が新たな提案を持って駒沢大学を訪れた。その提案が、今回導入した米フォーティネットの統合型セキュリティ装置「FortiGate」を使ったシステムである。これが、予算にピッタリと合った。井上は「タイミングがよかった」と謙遜するが、事前に予算を把握した上で製品を選択していた。

「持ち込みパソコン対策として完全ではないが、コストに見合った働きをしてくれそうだ」。駒沢大学から委託を受けてシステム担当者として常駐しているSRAの分銅淳至はひと目で気に入った。複数の

機能が1台にまとまっていて導入や運用が容易な点など製品自体の評価は高かった。問題は、開発元が外資系ベンチャーということだ。当時は管理ソフトも英語版しかなく、自分たちに使いこなせるのか、購入した後のサポートは大丈夫なのか、駒沢大学の担当者に不安が浮かんできたのは当然だった。

だが、井上はそうした不安を先読みしていた。説明に当たっては機能面だけでなく、IOS自身がFortiGateの運用をどれだけサポートできるかなど、内部事情を含めて情報を提供した。徳本たちは井上の説明を受けるうちに、サポートが信頼できると確信できた。

トラブルも信頼を高める結果に

無事、商談は成立し3月、セキュリティシステムを導入した。しかし、導入直後にトラブルが発生する。「Webサイトが見られない」というのだ。井上は、「原因も対策も分からないのに、顔を出しても顧客にとっては邪魔なだけ」と割り切った。井上の営業スタイルの真骨頂だ。

電話やメールで現場の状況を確認しつつ、技術担当者と連絡を取って、原因の究明に走った。だが、設定変更などの対処策をいくら試しても、うまく動作しない。原因が分かったのは、連絡から1週間以上たってからだった。駒沢大学に納入した機器に、メモリーチップの不具合があることがようやく判明した。

「新しい機器に交換すれば問題は解決するはず」。顧客への説明材料ができて初めて、井上は駒沢大学を訪れ、徳本たちに改めて謝罪した。予想通り、新たな機器に取り替えるとネットワークは正常になった。徳本は、自らの営業スタイルを貫いた井上のトラブル対応に満足し、FortiGateの増設にも前向きという。


駒沢大学のキャンパスは各所に分散しており、センターで一括してセキュリティを処理すると、拠点間を結ぶ回線コストがかかり過ぎる。井上は、離れた拠点のセキュリティシステムに3度目のチャンスがあると考え、駒沢大学に足を運び続ける。 (鈴木 孝知) 

図2 ●駒沢大学のセキュリティ強化の取り組みとIOSの提案プロセス

