セキュリティインシデント対応で考えること

株式会社ラック サイバーリスク総合研究所 取締役所長
JNSA 理事　西本 逸郎

2005年から被害が目立つようになった金銭目的の犯罪は、2008年に入りさらに増加している。起こってはならないことではあるが、ある面、増えているということはそれだけ実社会においてITの利用･活用が推進しているという証左だと思う。例として、ネット活用を徹底的に行い、事業を推進している通販関係のインシデント対応で感じたことを書いてみたい。

1．経営者次第

経営者の視点が重要だ。事態を軽く考えたい意識が働く方もいるが、多くの経営者は、利用者や取引先は大変重要な「財産」であり、それを守ることが第一義であり、生命線であると確信し、そのためにしっかりとした決断を下している。同時に、事業に対する思いやビジョンなどを熱く語る方も多い。苦しい中、さすがだと思う。一方、周りの支える方が、頭をたれてほとんど口を開かないことも、またよく見かける。これは、事件を起こしてしまったという責任感もあるのだろうが、そういう体質なのだろう。

2．がんばるシステム管理者

年商10億以上くらいになると、システムやセキュリティに関しても少しは手を打てると思うが、それ以下では正直辛い。大手の中でも「うまくプログラムを書ける」レベルの自社要員やソフトハウスなど頼っていることは多い。そういう人たちは経営者が推進したいビジネスを一所懸命プログラムで実現している。それだけ機動性も高くコストもかからないため、ビジネスモデルが良ければ、成功していく。素晴らしいと思う。しかし、残念なことにネットワーク、データベース、セキュリティといった基盤技術を持っていないか、あるいは知らないため、インシデントにつながっている。企業がある程度成長すると、継続成長の為にIT戦略とそれを支える基盤技術が必須となるが、そういった人材や機会にめぐり合えるのは経営者の運かもしれない。

結局、経営者のビジョンを支えるIT戦略立案と推進を図れる人材の確保が重要であるが、圧倒的に少ない。そのためには、セキュリティのプロを養成するだけではなく「うまくプログラムを書ける人」にセキュリティを理解してもらうことが、第一歩のように思う。

私たちが提供する、様々なセキュリティサービスやソリューションが本当に社会に根付いていくため、また、今後の高度IT依存社会を勝ち抜いていくためにも、経営者を支える「セキュリティが分かる人材」の確保が重要であり、費用対効果も高い策であると信じる。

JNSAの技術者集団でのボランティア（若しくは原価）ベースで、このような企業をインキュベーションしていく活動や、セキュリティ技術者以外にセキュリティ技術を導入していくような活動など、私たちが対応すべき課題はまだまだ多い。