



(52) 高まる情報セキュリティの必要性

野村総研(上海)咨询有限公司

◇不正アクセスの8割以上が中国から

NR Iセキュアテクノロジーズはさまざまな情報セキュリティ関連サービスを日本国内で提供し、お客様のシステムの情報セキュリティ対策を支援させていただいている。弊社のデータセンターで通信ログをモニターしていると、お客様や弊社自身のシステムが外部からさまざまな不正アクセスを受けていることが分かる。その不正アクセスは毎月数千件規模に達しているが、実は何とその80 - 90%が中国国内からの発信なのである（発信元のIPアドレスグループから中国発だと判断できる）。

中国国内の多くのサーバーまたは端末が直接不正アクセスを掛けている。悪意ある者によって“踏み台”にされ（被害を受け）てアクセスしている - のいずれかが考えられる。これは中国からの“攻撃”が多いという事実だけでなく、“踏み台”となるセキュリティの弱いサーバーまたは端末が中国に多くあることをうかがわせる。

◇限られたリソースで対策進める日系企業

情報セキュリティ対策で企業にとっての眼目は基本的には外部からの攻撃（不正アクセス・ウイルス・スパムメール等）からシステムを守ること、内部からの情報漏えいを防止することにある。

上海と北京の日系企業約30社を最近訪問し、情報セキュリティ対策の状況についてIT部門マネジャーの方々からお話をうかがった。その結果としては、ITマネジャーの方々には予想以上に情報セキュリティに対する意識が高く、日本本社からの内部統制や情報セキュリティに関する「指導」が思いのほか順守されている印象を受けた。

情報セキュリティ対策についての各社共通の課題は、大別すると以下のようである。

1) ガイドラインに従い必要な対策を進めているが、具体的な実施内容が十分かどうか漠然とした疑問や不安を抱えている

2) 情報セキュリティ対策の必要性は認識しているものの、IT部門で専門知識のあるスタッフが不足しており、運用管理を一部の担当者に任せ放しにしている

3) 何をどこまでやったらいいのが決めきれず、「予算範囲内で」「取りあえず」という感じになっていて、妥当性についてはあいまいである

4) サーバーや端末の台数や設置場所も把握できていない

これらの状況は、2005年に個人情報保護法が施行される以前の日本の状況に似ている。インターネットを基本とした情報システムそのものの利用は中国と日本で何も変わりはないが、中国においては必要なスタッフの確保が難しく、システム対策に必要なツール類や外部のサービス提供企業が少ないなど、ITマネジャーにとっては日本より厳しい環境にあると言える。つまり日本以上に要注意ということになる。

◇内販拡大で高まる情報セキュリティの必要性

中国では、これまでの製造拠点という位置付けから、中国国内市場をターゲットとした内販化の動きがある。従来型の業務システムのみならず、消費者との接点であるBtoCのEコマース、中国各地の販社や代理店との接点となるBtoBの企業間ネットワークが求められるであろうことは容易に想像できる。

社外に門戸を開くことになることで、情報セキュリティ対策の重要性はこれまで以上に高くなるのだが、それ自体は直接的には富を生む仕組みではないので、やっかいな課題となり、しこりとなってITマネジャーの頭に残り続けそうだ。

情報セキュリティがほかと大きく違うのは、問題が徐々に顕在化するのではなく、突然降り掛かってくる点にある。日本の情報システム部門の基準を中国国内の実情に合わせて、という基本方針はいいとしても、充実の度合いは日本以上としておくべきである。

せっかく努力して販売や営業を行って中国事業を拡大させるなら、情報セキュリティがクリティカルポイントにならないような方策が必要となるだろう。

(野村総研(上海) 咨询有限公司 黄晓春 / NRIセキュアテクノロジーズ 工藤真一)