# セキュリティ十大ニュースで見るこの 10 年

セキュリティ十大ニュース選定委員会委員長
工学院大学　情報学部　教授　大木　榮二郎

衝撃的な同時多発テロで、ワールドトレードセンタービルが崩れ落ちる映像はいまだに脳裏から離れない。その年、2001年に始めた「セキュリティ十大ニュース」が10周年を迎えた。毎年その年を振り返る、心待ちにしてきた年末行事であるが、10年続けると「10年間の100大ニュースが集まれば、何か時代の動きがつかめるのではないか」と思えてくる。そんな思いで、十大ニュース選定委員が集まって意見交換をした。

結論から言えば、意外なことに委員の多くの意見は「何も変わっていないように感じる」であった。もちろん様々な変化はあり、新たな脅威が次々と現れ、対策も進化してきた10年であることは間違いなかろう。技術と管理の間の大きなうねりもあった。しかし、「変わっていない」と感じるのは、そこに何かセキュリティの本質が潜んでいるのではないだろうか。

「何が変わっていないと思わせるのか」を考えながら、この座談会のまとめに目を通していただけると幸いである。

2月1日、工学院大学新宿校舎にて、セキュリティ十大ニュース10周年座談会が開催され、10年間を振り返っての変化や今後の課題について、セキュリティ十大ニュース選定委員会の各委員間で活発に意見が交わされました。

## ◇10年間全体を振り返って

これまでの10年の十大ニュースを振り返ってみて、表面上出てくる事件はあまり変わっていないという意見が多く、また、元来セキュリティを考えられていないインターネットのほころびを管理して使ってきた10年との意見も出されました。

## ◇10年間で見られた変化

まず、多くの委員から、2005年の個人情報保護法施行が潮目だったとの意見が上がりました。

個人情報保護法施行が変化の潮目となった背景として、2002年辺りまでは技術的なセキュリティ対策によって外部からの脅威に対抗することが主でしたが、情報漏洩など内側からの脅威が増加し、またISMS認証制度がスタートしたことで、管理系のセキュリティへの対策も必要となり、2005年頃までには技術系と管理系がせめぎ合う状況が生まれていたとの指摘が出ました。

こうした状況での個人情報保護法施行により、一般の人々まで情報セキュリティ意識が広がり、情報を1bitでも逃してはならないという風潮が生まれました。このため、企業は情報の取り扱いに非常に気を遣わなければならなくなり、加えてJ-SOXにより、対策に費やす軸足を管理系に大きく移すという流れになったと指摘がなされました。

実際に、2005年辺りを潮目として、ソフトハウスに委託されるものの質も、技術系のものを作るところから、管理系に変化したとの意見も出されました。

不正アクセス対策という観点では、2003年までは被害に遭った時に対策をした方が安いという風潮もありましたが、Blaster／Slammerの流行により、そうした風潮が変化したとの指摘もありました。また、この年は、マイクロソフト社がセキュリティ対策に本腰を入れ始めた年との意見も出ました。

他に、セキュリティを脅かす側の動機が、自己顕示欲を満たすことから、金銭を搾取することに移り、さらに原子力施設を狙うなど政治的なものにまで変化してきているとの意見も出されました。

## ◇今後の課題

管理系のセキュリティ対策に軸足が置かれた結果、この数年、様々な課題が生まれていることが各委員から指摘されました。

- 管理面でのセキュリティ対策をやったと言っても、形だけのことが多く、技術に投資がなされていない。また、技術をマネジメントに取り込むことが出来ていない組織も多い。
- 2002年に教科書通りに作ったポリシーが残っていて、改訂できていない企業が多い。そのため、ドキュメントと実際が乖離しているが、違うのが当たり前という認識が出来ており、誰も直さない。また、直そうという提案は嫌がられてしまう。
- 管理系のソフトウエアを国内の法律に合わせて作るにあたり、法律は分かるがプログラムを知らなかった人たちがシステムを作り出している。また、発注者や現場は明日動かすことや工数を優先して考えてしまうため、セキュアなシステムを開発するというスタンスで取り組めていない。
- ID管理やログ管理、インシデント管理など、根本的な部分に顧客が取り組むようになり、管理系から技術系に軸足が戻る傾向も最近見られるが、景気に大きく左右されてしまっている。
- リスクアセスメントをきちんとやらなければならない時期が来ている。導入するべき技術とそうでないものを見極め、導入すべき技術はしっかりと導入して行く必要がある。

- 企業内でセキュリティを担当する部門が、情報システム部門から経営企画室やセキュリティ管理部などの部門に移ったが、両者の間での連携が全くとれていないことが多い。
- 企業内でのセキュリティ教育をどの部門がやるのか、明確に線引きされていない。

一方で、以前までは隠されていた情報漏洩の事実を外部に発表するようになったことなどが、管理系のセキュリティ対策に軸足が置かれた結果の利点として指摘されました。

また､上記の他に次の様な課題もあげられました。

- 情報漏洩などを恐れて連絡網や名簿を作成できないといった後ろ向きな、過度に反応する風潮が進んでしまって、本当はどこまでの情報が出ることが問題なのかといった議論が進んでない。
- SQLインジェクションが最もたちが悪く、今後も今のDBの仕組みだとなくならないだろう。また、この穴をついてくるのではないかと思う。
- PCではなくスマートフォンやウェブアプリ全盛になってきており、それを使う子どもたちのモラル教育をやらなくてはならない。

今回の座談会の議論から、いかに管理系と技術系の対策を一体として行っていくのか、今後の大きな課題として議論していくことが確認されました。

これからも、10年スパンの長期的・大局的視点から情報セキュリティの取り組みを考える機会を持ちたいと思います。皆様からもご意見やご感想をお寄せいただけるのを、セキュリティ十大ニュース選定委員会では心よりお待ち申し上げております。

## 10年間を振り返ってみて注目されるトピックス

10年間合計100のニュースの内、振り返ってみて注目されるトピックスとして各委員からあがったのは以下の通りで、これを元に意見が交わされました。

2001年
　技術面：「W32/CodeRed」世界に蔓延
　管理面：9.11NY同時多発テロの発生
2002年
　技術面：クロスサイトスクリプティング脆弱性蔓延
　管理面：ISMS 認証制度スタート、住民基本台帳ネットワーク運用開始
2003年
　技術面：Blaster／Slammerの流行
　管理面：情報セキュリティ監査制度始まる
2004年
　技術面：Winny作者逮捕の衝撃
　管理面：IT戦略本部　国家情報セキュリティセンター設置へ
2005年
　技術面：SQLインジェクション、猛威を振るう
　管理面：個人情報保護法全面施行
2006年
　管理面：J-SOX内部統制実施基準案が発表される
2007年
　管理面：食品偽装事件多発、消えた年金記録問題
2009年
　技術面：クラウド台頭、Gumblerによる改ざん被害拡散
　管理面：政権交代