第5回総合セキュリティ対策会議
（平成15年1月20日）
発言要旨

【ハイテク犯罪の被害状況に関する調査】
（事務局より前回の議論を踏まえて改訂した調査項目について説明）
○　情報セキュリティに関連した脅威の分類は、著作権侵害と商標権侵害を分けた方がよい。
○　誹謗中傷、著作権侵害は、情報セキュリティに対する脅威ではなく、対策が充分に行われていないことによって生じる脅威であるので、その旨を注記すべき。
○　認証方法の選択肢のうち「ICカード」は、「方法」ではないので、その使用方法に関する質問として整理すべき。

【社会における情報セキュリティ対策について】
（委員より発表）
・ 社会（政府機関、企業、国民）の情報資産（施設、組織、情報）を分類して、それぞれに対する具体的脅威を分類し、これらの脅威を脆弱性やCIA（情報の機密性・完全性・可用性）の視点から分析して対処する。このようなサイクルに対して公共サービスや民間サービスが提供されているが、それらサービスについても情報資産の分類、脅威の分類、分析、対処というサイクルが存在している。
・ リスクを分析、評価、対処しても残余リスクが存在する。１００％守ることは、現実的には困難であり、この残余リスクをどこまで許容するかが経営トップの判断。個人の場合は、自己の判断で残余リスクを認識しながらインターネットを利用することとなる。
・ BS7799ガイドラインのリスク分析においても、資産の識別及び査定、脅威のアセスメント、脆弱性のアセスメントを行ってセキュリティ対策を講じ、それに対してもう一度リスクアセスメントを行い、残ったリスクが許容可能か不可能かを識別するという方法がとられている。
・ 脅威を幅広くとらえると、①災害（テロ等を含む）、②故障・障害、③無権限（不正アクセス等）、④過失、⑤準拠違反（関連法規違反等）、⑥要員（労働争議、欠員（健康障害））に分類できる。
・ 不正侵入検知サービスは、意識が高い一部の企業への導入に止まっているが、 今後は、不正アクセス手段の巧妙化や24時間監視が必要となることで、インターネット環境が整っているあらゆる企業での需要が見込まれる。
・ 不正アクセスの状況は、ワームの出現といったインシデントの出現によりダイナミックに変動する。これを早めに分析して検知して対処する必要がある。
・ 官のサービスと民のサービスの連携をどのように行っていくかということが課題である。
・ 何を守るべきか、何が脅威かということを絶えず考えて、分析して対処する仕組みが社会のリスクマネジメントになっていくのであり、これをもっと明確にしていく必要がある。
（質疑応答）

・　(不正侵入検知サービスにおいて、これまでに対応できなかった事案はあるのか、との問に対して)どこかでインシデントを把握すれば、すぐに対応できるようになっている。
・　(不正侵入検知サービスにおいて把握したインシデントについて、不正アクセス禁止法違反として実際に警察との連携はあったのか、との問に対して)全体的な統計などについては情報交換をしているが、具体的な事案については犯罪行為に当たるかという判断はしておらず、警察へも通報していない。
・　(窃盗などについては通報を行っているのではないか、との問に対して)インターネットの場合、現時点では、当事者が被害届を出すかどうかという問題と認識している。
(討論)
○　ソフトウエアのバージョンアップがなされていなかったり、パッチが当たっていないという状況が脅威となっている。
○　原因が分かっていても対策がとられていない場合がある。

【情報セキュリティに関する脅威について】
(委員より発表)
・不正アクセスに関する最近の動向は5点ある。
①ポートスキャン:頻繁に(ほぼ毎日)発生。重大なセキュリティインシデントの前兆行為として認識しておくべき。
②侵入行為(不正侵入):以前はパスワードクラックが主だったが、最近はバッファオーバーフローの弱点を利用したものが主流。
③DoS:重大な脅威となっており、実際にサービスが落とされる被害が出ている。
④スパム:不正中継によって、メールサーバーがエラー処理で止まってしまう場合があり、ある意味でDoS攻撃の一つの形態となっている。
⑤ネットワーク伝搬型ウイルス:着実に増えてきている。
・高度なツールが簡単に入手できる状況であり、攻撃手法の高度化が著しい。
・DoS攻撃によりシステムが落とされており、これをどうやってマネージするかについて、非常に興味を持っている。
・ブロードバンドの急速な進展により、通常の家庭のマシンが攻撃の道具として利用される可能性がある。大手企業・法人レベルから個人ユーザ・ホームユーザ・中小企業まで、セキュリティ対策をきちんとやらないといけない。
・単に制度を作るだけではなく運用との整理をやらないと実効がない。警察が作る制度についても、運用において、ほかのグループ(民間等)から孤立するのではなく、協力が必要。
・技術的な観点からの脅威の評価はこれまでもなされているが、システムに対する被害インパクトの観点からの評価はなされていない。このような評価は、セキュリティサービス企業の料金体系や保険による補償に反映されることが期待される。
・犯罪行為と非犯罪行為の区別を行うべきではない。現実には、グレーゾーンが多い。
・内部者によるトラブルの脅威が大きい。システムの得意不得意を知っているので、一番弱い側から攻撃されてしまう。また、トラブルは内部に隠蔽されてしまう。これに対して行政はどのような役割を果たせるのか。

・ ソフトウエアトラブル（バグ）も大きな問題。ソフトウエア評価、サービスのガイドライン、認定制度といった社会的なメカニズムが必要。

〈討論〉

○ ハッキングツール、クラッキングツールには簡単に使えるものが出回っている。これらをどう位置づけるべきか。届出、試験、資格といった規制が必要かもしれないが、どこまで必要か。

○ ツールの所持に関する規制には反対である。銃や薬物とは異なり、あくまでもソフトウエアであり、所持を規制すると進歩が止まる。

【報告書骨子（案）について】

（事務局より説明）

○ 3，4年後になってこの報告書の中身を再利用されることがないよう、あくまでも本年度の報告書ということで「賞味期限」を書くべき。

○ 5「情報セキュリティ対策への活用」においては、様々な脅威とそれに対応する既存の法律との関係、すなわち取締りの可否について、言及するのか。明らかな犯罪行為よりもむしろ、DoS 攻撃のような迷惑行為に対して、警察がどこまで対応するのかという問題がある。

○ 3「脅威として把握すべき対象」のまとめ方として、事後的な取締りが中心となるもの（児童ポルノ、わいせつ物の頒布、マルチ商法、ネズミ講）と、予防・防止に力点を置くもの（ウイルス、不正アクセス）とは、分けた方がいいのではないか。

○ 追跡性が完全でないという状況がある。追跡によってどこまでできるのか、追跡が切れた先にどのような対策があるかという視点から提言をしたい。

○ IT化が進んで利用者が増えて、無意識のうちに犯罪者になってしまうようなことになると、発展を阻害してしまうおそれがある。

○ 技術的な対策（追跡性の研究等）、経済的な解決（保険等）に対する期待は、警察側からの発言としては注目されるものであり、うまく書く必要がある。

（以上）