第２回総合セキュリティ対策会議
（平成１４年３月１日）
発言要旨

（事務局から「総合セキュリティ対策会議報告書概要（案）」について説明）

○　業者は通信の秘密や顧客の秘密の保持義務といった制約があるので、情報交換・提供を行っていくためには、現在の仕組みを変えていく必要がある。

○　法律上通信の秘密は犯してはならないこととされている。所管官庁による法解釈の整理についても検討する必要がある。

○　犯罪に関係しない情報が取得されているのではないかとの懸念がある。省庁間での横の連携も必要である。ハイテク犯罪とサイバーテロを区別する必要がある。

○　プライバシー保護に対する考え方は変わってきている。

○　報告書の読者として誰を想定しているのかを明確にする必要がある。この報告書について産業界の同意があるとされるのは困る。各施策について警察としてのプライオリティ付けが必要。

○　民側の協力やセキュリティ対策について、どのような利益があるのか、どのような場合に免責されるのかといった点を明らかにしないと、誰が何をやったらいいのかが明確にならない。

○　ソフトウエアベンダーの責任をどう考えるかも議論すべきである。民側の免責を広く認めると、民間の努力が無くなってしまう。

○　市民のプライバシーを一番持っているのは自治体である。

○　多くの地方自治体のセキュリティレベルはあまり高くない。実際に捜査を行っている警察の立場から思い切った提言を考えても良いのではないか。

○　官の内部での協力・連携についても議論すべきである。

○　報道の自由への影響にも配慮する必要がある。

○　多面的な利害があるということに配意する必要がある（例えば、ログの保存におけるコスト負担等）。

○　技術の進歩がコストに影響を与えることもある。

○　マスコミへの指摘（マスコミにおけるセキュリティ等）も報告書に盛り込むべきである。

○　自治体職員の意識向上・教育の面では、民側に後れをとっている。

○　ネットワークの時代において情報を管理することは難しい。必要のない情報を作らないという考え方が必要。

○　一般論としての情報提供だけでなく、官庁、ビジネス界、ＮＰＯ等による個別の対応についての認識も必要である。防御側のレベルを上げるためには教育

が必要。

○　フィジカルなセキュリティサービスにおいては一定の場合に警察に通報することについて了解ができているが、サイバーセキュリティにおいてはビジネスにおいて得た情報を公表・通報することができない。セキュリティベンダーと顧客、警察との関係を考えていく必要がある。

○　サイバーセキュリティ産業と警察との関係を考えていく必要がある。

○　ハイテク犯罪は地域を問わない犯罪であり、警察の組織整備についても検討する必要がある。犯罪捜査のために個人情報が必要であるとしても、いかなる個人情報を企業が保持し得るかについては社会的コンセンサスが必要である。技術の発展が早いので、立法による対応だけでなくできるだけ現行法で対応していくことが必要である。法律の国外への適用についても検討する必要がある。

○　警察の役割には犯罪の捜査と犯罪の予防があるが、この会議においては予防の観点を優先すべきである。

○　民間やＮＧＯにおいても相談を受理している。民間と一緒に対応を行うという視点が必要である。また、ナショナルレベルでの相談対応体制の整備が必要である。

○　将来的な被害者を無くすために企業がすべきことは、①蓄積された個人情報を漏洩させないことと、②個人が攻撃されないハードウエアを構築することである。②については欠陥についての情報公開が必要だが、一方で公開しすぎることによってその情報が悪用される危険性もある。

○　セキュリティに関して、企業としては他社との競合という点からの関心が強く、犯罪への対応という意識はあまりない。また、技術者の教育が必要である。

○　少年の被害が大きく、少年保護の視点を強調すべきである。

○　セキュリティを誰が担うのかという問題がある。サイバーセキュリティにおいては、防犯という観点が重要である。

（以上）