第３回総合セキュリティ対策会議
（平成１４年３月２８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（案）」について説明）

○　６名の委員の連名で意見書を提出した。今回の報告書は３回の会議しか経ておらず、十分な議論がなされていない。プライバシー、産業界のコスト負担、インターネットの発展と適正な規則の調和に係る社会的コンセンサスなどについて、事業者として報告書の内容に同意していると受け取られることは問題であり、報告書の内容が成熟したものでないことが明記されるべきである。取り締りの必要性は、事業者の自主的な対応ではまかなえない部分について議論すべきである。我が国全体としてのセキュリティ対策は、関係省庁や産業界が広く参加した場において議論されるべきである。国際的な議論を踏まえれば、データ保存の義務付けや民間側のコンタクトポイントの設定を前提とした議論は有益ではない。

○　本会議は警察庁の会議であり、情報セキュリティ全般を対象としたものではない。犯罪現象があり国民が困っているということにどう対処するかという切り口で議論を行っている。

○　コンタクトポイントの件を例に挙げると、議論はされているが現実はそれに対応していない。産業界といっても多数の業界があり、それをまとめて議論するのは、出発点の詰めが甘いのではないか。

○　希望する委員については漏れなく「委員有志からのコメント」として報告書の結語という形で記載することとしてはどうか。
（本提案については、委員の間で合意された。）

○　報告書の内容が、制度として強制力を持つように読めるのが問題なのではないか。表現ぶりを工夫して誤解を避ける方法があるのではないか。

○　産業界側の２４時間コンタクトポイントは、国際会議では議論そのものをしないこととされている。データ保存の「奨励」という表現も適切ではない。国際会議の議論に合わせた内容とする必要がある。

○　「犯人の追跡性の向上等」において、産業界と警察の連携強化だけが強調されているが、プライバシーや通信の秘密に係る問題点も存在するので、これら考慮すべき点も多いということも記述すべき。

○　様々な意見があることを明らかにしておくべき。

○　一定限度のログの保存の必要性についての議論は必要。ログは、被害を受けた国民の保護のために、民事裁判においても必要とされる。データ保存は国民の裁判を受ける権利の確保に資するものである旨を記述すべき。また、保存の

在り方やコスト負担の点についても記述すべき。

○　技術的な見地から、データ保存等が犯人追跡のために果たして有効なのかという議論がある。技術、制度、法律、運用といった多面的な議論をすることが望ましい。

○　数でいえば、ログが保存されていたので捕まった事例の方が多い。

○　ログそのものを消去してしまうような高度な知識・技術を有する者が問題であり、そのような者の行為を阻止すべき。

○　ログによる追跡は難しいが、ログがなければ追跡できない。技術的な対応により、追跡性とプライバシーが両立する可能性もある。技術的な検討についても記述すべき。

○　Ｇ８での議論もそうだが、制度の議論に偏っており、技術的対応に関する感覚が薄い。

○　官民の協力、意見交換の必要性を改めて感じた。産業界はコストに対する意識が強く、他方、犯罪現場においてはログがあったほうが犯人検挙に資する。両者がお互いの立場をより理解することが必要。

○　データ保存等に関して、Ｇ８では「奨励」という語は用いられていない。リアルタイム・トレーシングは、どのように行うのか明確でなく、技術的な観点からさらなる議論の必要がある。産業界からは追跡を可能とするネットワーク構成については、犯人だけではなく全員の追跡になるとの指摘もある。コンタクトポイントの設定は、Ｇ８官民合同会合等では全く合意が得られなかった事項の一つ。産業界側に統一的な窓口はなく、議論するのであれば、少なくとも具体的に何の目的で誰とコンタクトするのかを明確にすべき。「今後の課題」の「プライバシーとの関係」については、ＥＵ等の国際的動向との整合性をとる必要がある。「ハードウェア、ソフトウェアベンダの役割」にある製品に不具合があった場合に関する記述は、犯罪に関係した問題なのか疑問。

○　自治体における電子政府の実現について言及しているが、自治体については「電子自治体」という言葉が使われている。また自治体の大小に関する記述は不要ではないか。

○　教育機関に関する記述においては、中学の技術・家庭科の授業で情報教育が必修となり、高校で「情報」という科目が必修となったこと、これら指導要領のなかでセキュリティに関して触れられていないことについて記述してほしい。ドメイン名の不正取得等の記述では、すでに JPNIC における紛争解決の体制が確立されたものについては記述しなくてよいのではないか。情報管理の部分は記述が足りない。

○　情報管理、教育の問題についてはもっと具体的に書くべき。

○　都道府県警の対応能力のレベルの差が大きいと思うので、地方の警察の能力を向上させる方策を示してもよいのではないか。

○　サイバーテロの現状については、日本ではサイバーテロは発生していないので、削除すべきではないか。もしサイバーテロについて言及するなら、９／１１の米国同時多発テロを例にとり、現実世界のテロからサイバーテロに発展する危険性を指摘する方がよいのではないか。

○　内閣における会議などにおいても、サイバーテロの脅威が高まっていることの事例として中央省庁ホームページ書き換え事案等を挙げている。

○　この報告書の内容が今後立法、法改正等に使われるものではないことを確認したい。

○　セキュリティホールの存在といった犯罪の方法論を公にすることに関する議論が書かれていない。

○　セキュリティ対策を担う主体として、法曹界を加えてほしい。

（事務局から「平成１４年検討事項（案）」について説明）

○　１４年度の検討課題としては、「脅威の実態把握」でよいのではないか。「産業界等と警察との連携の在り方」の各項目名は内容に対応したものとすべき。「連携の主体」の中の「電気通信事業者以外の各種事業者」については分類して書いた方が分かりやすくなる。

（以上）