第１回総合セキュリティ対策会議
（平成１３年１２月２１日）
発言要旨

（事務局から「情報セキュリティに関する脅威等」について説明）

○　ハイテク犯罪については、本来、法執行機関、産業界、ユーザーの利害が一致するはずであるが、現実には利害調整に困難な面がある。一方で、ハイテク犯罪捜査には民間の協力が不可欠。こうした問題について議論がＧ８のスキームで行われている。５月の東京での会合では、データ保存、データ保全、脅威の分析・予防、電子商取引の保護、ユーザー認証、トレーニングの５つの分科会が設けられ、活発な議論がなされた。また、ハイテク犯罪の場合には、脅威の全貌が把握できていない、というのが国際的に一致した認識であった。日本においては、ハイテク犯罪に関する一般の認識・企業のトップの関心が十分高くないということがあり、会議を通じて警察と民間・産業界の連携の必要性について痛感した。東京会合では、今後、各国が国内においてこれらの課題について検討をしていき、必要に応じて国際的な会議を開催していくこととされた。

○　電子署名に関連した犯罪も今後増加が見込まれるので考えていく必要がある。

○　司法機関と民間の希望が異なっている。Ｇ８官民合同会合では、これを国による制度の違いがあり、犯罪が国際的になる中でこの隔たりをどのようにすりあわせていけばいいのかについてもっと具体的に議論ができればよかった。

○　プライバシーや法執行機関への協力についての民側の態度は、日、独が一番堅い。Ｇ８で確立したルールを作るのは困難。各国でベストプラクティスを出しあって、それぞれの国で参考にしながらやっていくというのが一つのアイデアだと思う。

○　この会議では、日本のベストプラクティスを考えてもらいたい。

（事務局から「脅威に対する産業界と警察の連携の現状の在り方」について説明）

○　法執行機関としては、犯罪の抑止という観点から、インターネット上のデータ保存を求めている。また、保全は、犯罪が行われたときの対応において必要。

○　犯罪捜査のためのデータ保存が法律に照らして認められるのかという解釈問題がある。ログの保全は、法執行機関が手続きを迅速にすればよいというのが産業界側の立場。

○　常時接続サービスが増加すると課金のためのログの保存が必要なくなってくる。データ保全については、捜査機関から要求があったときデータを残すということ。コストと脅威のバランスの中でどう考えるかがポイント。

○　米国では、テロに対しては厳しくやる法律になっている。インシデントの態様により大きな違いがある。

○　脅威に関して、現象と被害、関係する人といった点について分類して議論を進めてはどうか。また、セキュリティ対策については、一般的な基準、ガイドライン作りの動きやコストのバランスも踏まえながら犯罪との関係での協力について考えていくことになると思う。
○　それぞれの機関がその責任を担いつつ、みんなで協力していかなければならない。いろいろな立場で捉えていく必要があり、この場はその中の一部であろう。
○　ホームページ書換えが目立つのでいたずらの方に意識がいってしまうが、犯罪組織や内部犯行の方が社会に対する被害が大きい。ただ、犯罪組織や内部犯行は、自慢しないし、目立たないので、どうしても目立つ方に意識がいってしまって、その対策ばかりに注意しているケースが多い。警察の方でデータを利用することが可能であれば、どういう犯罪によって、どのくらいの被害があって、どういうプライオリティをつけるべきかということをどこかで議論が必要だと思う。それを総合的に見ているこういう会議が一つのチャンスである。
○　このような観点は必要。まだ、実際のデータの蓄積、特に脅威に対するデータの蓄積というのがない。ある程度それらを整理し、分析しなければならないと思う。
○　警察としては、脅威に全部対応するということではあろうが、どういうことを中心としてやっていくかといった方向が検討課題。
○　インターネット上の問題は、すべての関係者が協力することが重要。
○　報告書の作成については、その使われ方などを考慮に入れて、戦略的に会議を進めるべき。
○　匿名性が犯罪対策においてネックになっているが、発信者の個人情報も保護しなければならない。これらを踏まえ、国際的にも先例となるようなベストプラクティスを皆で日本において作っていきたい
○　電子政府に向けて、地方公共団体において一斉に情報セキュリティポリシーを策定している。緊急時の対応について警察との連携が重要。
○　プライバシーの問題は、Ｇ８の会合でも大きな柱。また、脅威の実態把握や類型化が重要。
○　脅威の実態が分からないことが最大の問題。セキュリティの脅威の範囲と類型、種類を挙げ、それへの解決策を検討することが重要な作業。プライバシーに関しても、個人のプライバシーは大切だが、電子商取引における事業者にはプライバシーはないという感覚がある。問題を考える際、個人の視点が必要。
○　動いている実態を見据えつつ、脅威を類型化し、そのレベルを考えながら、プライバシーが犠牲にされる程度等を議論していく必要がある。この会議では、問題点を指摘してもらい、この場でも政策を発信し、また関係省庁等にも情報を提供し問題の対策につなげていくことが重要。

○　プライバシーは、非常に深い問題。個人を特定するための情報の管理が不十分なセキュリティレベルであれば問題。こうした点について、関係者の教育も行い、意識も高め、技術的にも穴のないシステムで犯罪を防止していかなくては危ない。また、犯罪組織による犯罪についてデータもあるのではないか。

　一方、国際的にも、プライバシーとセキュリティの話は逆方向に向いており、これをどこかで合わせる必要がある。

○　ベンダーとしては、犯人を捕らえることよりシステムを早く復旧させることが重要。

○　国民のリテラシーは、文化の違いでもある。海外の考えがそのまま国内でも受け入れられるとは限らない。それを踏まえてあるべき姿を検討することが必要。

○　今は、警察にも産業界にもショートタームなソリューションが必要。それをこの場で出して、警察庁として実行すべきことは実行してもらい、また他に発信していくといったことも短期間で成果が目に見える対策が必要。例えば保険制度など。

○　電気通信事業者以外の事業者の官民連携における役割という切り口も考えてもらいたい。

○　将来起こりうる脅威、例えば、電子署名を利用した犯罪などについてどう検討していくかも考えていくことが必要。

○　被害の届出を出したくても警察側の知識が低い場合がある。被害者、被疑者、犯罪の舞台となった事業者の３者がバラバラの都道府県警察になった場合、各都道府県警察間の連携が重要である。

（以上）