

(イ) 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。

- 事務局から、先進主要国における通信情報利用の実施過程とその制限・監督についてプレゼンテーション及びこれまでのテーマ別会合「通信情報の利用」における議論を整理
- プレゼンテーション及び議論の整理に対する意見交換は主に以下のとおり。
 - トランジット通信（日本を経由する外国から外国への通信）について、周辺情報にも少し目を広げていくことによって全体状況が分かりやすくなるので、他国と同等の分析ができるようにしておく必要があるのではないか
 - 今回は海外に関係する通信に限定した情報のチェックということになるかと思うが、国内サーバを使用した攻撃の監視が手薄になる可能性がある。ウィークポイントがないか確認し、対応を検討していく必要があるのではないか
 - 独立機関の監督の仕組みの制度化が必要。独立機関の在り方につき、英国及びドイツの例は大変参考になるが、諸外国の仕組みや法制度を参考にするときには、司法制度との関係などを考慮に入れておく必要がある。また、公文書管理など日本の情報管理の領域にある組織の仕組みも考慮に入れてはどうか
 - 同意による場合には、通信の秘密の侵害に関する同意の具体的中身が問題となる。今回について言うと、カスタマイズされた同意ではなく、法律等で何らかの裏付けを持たせた規格化された同意という形にすることが適切ではないか
 - 情報処理の各プロセスの中で、処理・分析やフィルタリング等は、通信事業者ではなく、国の機関が実施するものと理解。通信事業者が実施する内容にしても、法制度上の確にカバーする必要があるのではないか

- 能動的サイバー防御に係る議論について、**全て情報公開することは不可能。概ねこういうことをしていると適切に情報公開**し、説明責任を全体として果たしていくことで、国民が理解をし、その結果もう少し踏み込んでやってもよいというような形で、全体として制度の見直しも含めたプロセスを回していく視点を入れるとよい
- 国民の理解を得る方法として、一般に透明性の確保がよく言われるが、本件の性質上、その全てをつまびらかにすることになじまない。透明性で補えない部分を別の方法で補う必要があるところ、例えば、諸外国で行われているような、**信頼性のある独立機関による監督を担保することが、国民の理解を得ることになる**のではない
- インターネットの出現で**通信の在り方はこの20年で大きく変化**。固定電話の時代には、その通信の容量は非常に少なかったが、現代は、サイバースペースにより匿名的な通信が大量に出現。**その変化に対応するための法制を作らなければいけないのだという説得の仕方が必要**
- 国民の理解を得るには、企業や国民に対してどのような便益があるのかが重要。セキュリティクリアランスを持った企業にフィードバックするとともに、あるいは、新組織から、サニタイズした情報を国民に対して還元していくなど、**最終的に企業や国民に便益がある活用、仕組みとすることが重要**