2012 年 9 月 14 日

第 6 回「国際共同声明を読み込む講座」
国連総会決議　サイバーセキュリティ関係

１．　サイバーセキュリティの基礎（背景）知識

(1)「インターネット」とは

a）ネットワークの構造（専用回線か公衆回線か）

b）セキュリティは階層で分けて（インフラの話なのか、利用面（アプリケーション）の話なのか（＝物理的な破壊なのかウィルス等によるものか））

c）現実にどのような被害が生じているか（あるいはその蓋然性)。

(2) 議論する際のポイント

(a) サイバー一元論か二元論か

一元論であれば、既存の法制度を適用。二元論であれば新たな、個別の法制度が必要。

(b)「サイバーセキュリティ」の意義の相違

(c) 具体例

「サイバー戦争」

エスピオナージュなどは基本的に既存の法制度での対応。

基本の法制度を適切に運用する場合の（サイバー特有の）論点

従前の攻撃形態と比べて

- 攻撃元の特定が困難
- 非国家主体による攻撃の可能性も大きい
- 攻撃先が非軍事施設等におよぶことも一般的
- 容易にエスカレートしやすい 等

→

a）いかなるサイバー攻撃が国連憲章に基づく自衛権の行使を正当化する 「武力の攻撃」たりうるか

b）非国家主体がサイバー攻撃を実施した場合の自衛権の 行使の余地

c）自衛権の行使にあたっての比例原則の適用のあり方

といったことが論点になりうる。

２．　国連総会の決議（2003 年時点）

現在も続いている議論（2011 年 G8 サミット（仏:ドーヴィル）～2012 年サイバーセキュリティ会議（ハンガリー）など）