資料９

第１回情報セキュリティ政策会議に当たっての意見

KDDI 株式会社
小野寺　正

１．「重要インフラにおける対策の強化（安全基準・ガイドライン）」について

各重要インフラを構成する事業体（個々の通信事業、個々の電力事業など）は、それぞれの事業体のための安全基準・ガイドラインを保有しており、各事業体において一定のレベルでそれらが有効に機能しているという認識を持つ。従って、今回の重要インフラ横断的な「安全基準・ガイドライン」の策定指針による各重要インフラでの見直し、策定は、第 2 次提言で触れられている「重要インフラの連携（現状の重要インフラの安全基準等に欠けているもの）」に重点を置くべきである。すなわち、各重要インフラを構成する事業体を有機的に連携させるための施策を具体的に打ち出すべきである。そのためには、今後の必要となる重要インフラの連携モデルなどの具体化を優先して検討することが望ましい。

２．「国際連携の強化」について

情報セキュリティに関し、国際的なグローバルな連携を進めるために、POC（Point Of Contact）の確立に着手することは賢明と考えるが、単純に POC を開設しても機能しない。すなわち、セキュリティ対応（障害復旧、国家機能継続性確保、インシデントハンドリングなど）に必要となる国家間の具体的な手順・ガイドラインの標準策定が重要となると考える。サミットなどの主要国協議の議題として、日本から「情報セキュリティ国際連携に関わる提言」を具体的に実施することも一考である。

３．セキュリティ教育　人材の確保

情報セキュリティ確保を継続的に安定化するためには、人材育成、セキュリティトレーニングが必須であることは自明である。情報セキュリティ技術は多岐に渡っていることから、総合的な情報セキュリティ技術を広く習得している人材、セキュリティを十分に配慮したシステム設計、構築ができる人材、情報セキュリティ事案（インシデント）に迅速に対応できる人材等が不足していることも明らかである。このような事態を改善するための手始めとして、日本のセキュリティ教育プログラムにどのような抜本的な問題、課題があり、今後、どのような施策（特に、国として）を打つべきかといった基礎検討を早期に実施する必要がある。

４．その他の視点（情報保護に関する費用対効果）

情報セキュリティの保護レベルについては様々な観点があり、設備・費用も大きく異なる。ガイドラインの策定に関しては、際限のない費用の高騰を避けるため情報保護の要求レベルについては、実務的な観点からの検討も必要である。

以上