資料３－３

【神保委員御意見】

第２次情報セキュリティ基本計画に関するコメント
（外交・安全保障分野を中心に）

慶應義塾大学
神保　謙

１．脅威・リスク対応型

（１）サイバーアタックに関するリスクシナリオ策定の必要性

- 悪意のあるアクターによるネットワーク攻撃の可能性について、諸外国の事例の蓄積、考えられうる将来のリスク等についての幅広い検討が必要。検討事項についてのデータベース化、公的機関による共有の促進。

２．実施体制の拡充

（１）情報保持・管理・秘匿・罰則に関する国際的スタンダードを公的機関で共有

- 外交・安全保障に関する情報の国際的相互依存体制は拡大し、日本もそのネットワークの中に入ることにより高い安全を確保する必要がある。
- 重要インテリジェンスを確保するためには、日本国内で信頼できる情報秘匿体制があることが重要。そのためには、情報秘匿に関する法整備、ガイドラインが公的機関（各省庁・政府機関・国会議員含む）で共有されていることが重要。
- 各省庁のセキュリティのクリアランスに関する階層整備を標準化し、情報のアクセス許可・制限に関する権限を徹底する必要がある。
- 国民に対して機密・秘情報はなぜ公開されるべきでないのか、という情報に関する政策カルチャーを醸成することが重要。他方で、国民に対するアカウンタビリティを保つためにも、原則として政策決定に関する情報は公開するというルールのもとに運用されるべき。

（２）国外諸国と共有する情報の標準化

- 外交・安全保障に関するリスク関連情報（災害・人の移動・保健衛生・国際組織犯罪）欧米諸国・アジア諸国との連携を強化。とりわけ基礎データベース、早期警戒情報などのシステム共有を進め、相互補完関係を強化する。
- 以上のシステム構築のためのセミナーの実施、協定の締結、情報インフラの整備、システムの標準化、運用に関する標準手続き、リスク管理などを二国間・多国間の組みで積極的に推進する。

（３）情報セキュリティに関する人材育成・専門機関の拡充

- 社会各層（公的機関・民間機関・非政府組織）における情報セキュリティに関する教育・人材育成を強化する必要。情報セキュリティ専門家の具体的な数値目標を示すことも一案。