

## 意見書

2007.10.03 村井 純

**1. 情報セキュリティセンターの整備拡充の必要性**

情報システムの根本的な役割は業務機能の全体的な統制(コントロール)にある。政府における情報セキュリティ政策では、単に政府内部での情報セキュリティ対策だけでなく、国民生活に直結する重要インフラにおける情報システムの役割の同定とセキュリティ対策強化、広く企業や国民における情報セキュリティへの取組の向上といった、幅広い横断的な政策実施が必要。各省庁が単独でバラバラに行うのではなく、官邸主導で全体を設計し、各省庁において整合性がとれ有効性の高い政策実施を行い、官邸が監理することが重要なのはそのため。情報セキュリティ政策の実施で、実作業を担当する内閣官房情報セキュリティセンターで、最新の技術と知識を理解する最高で最強の人材を、安定して確保し続けることが必要であることは重要課題。現状の情報セキュリティセンターの運用においては、この問題が十分に考えられているとは言い難く、より積極的な検討と解決が必要である。

**2. 評価基準について**

各省庁が取組む情報セキュリティ対策の評価においては、日常的な運用体制がどのようになっているのか(特に24時間、365日の運用責任という観点からの評価)、日常的な運用に投入されている人的資源(人員数、人材の質、確保の方法)、さらに、情報セキュリティ対策に用いられている技術についての評価が必須である。また、政府統一基準において、運用体制、人材、技術に関する基準も提示すべきである。

**3. イベントドリブンの課題解決の必要性**

これまで、何度か本会議でも述べてきたが、今後早急に「イベントドリブン」(event driven)で問題解決する体制を NISC 内に実現することが、必須かつ喫緊の課題であることを再度指摘したい。「イベントドリブン」の問題解決とは、ある刻限に事象(イベント)が発生することが分かっている状況で、事前準備(preparedness)、イベントの観測(watch)、そして問題発生時の対応(response)を、合理性を保ちながら確実に実施することである。例えば「Y2K」問題の取り扱いは、まさにイベントドリブンの問題解決の典型である。このようなイベントの取り扱いの経験が継続的に継承され、次のイベントに対する対策に活用されるように、NISC が中心的な役割を負うべきである。

**4. 国際の観点からの日本の役割の認識と実行**

今回の政策会議において議論・決定される、情報セキュリティ政策の国際展開では、日本の特徴のある先端的な事例を中心に具体的取組を構成し、諸外国、特にアジアへの展開を戦略的に考えるべきである。同時に、欧米各国に対しても、この取組を積極的に紹介し、より多くの活動が国際的に行われることを喚起すべきである。

以上