資料１１

2007 年 2 月 2 日
富士通株式会社
黒川 博昭

第 10 回情報セキュリティ政策会議への意見書

本日から本会議へ出席させて頂くが、2005年春にNISCと本会議が設置されて以来、わずか2年弱の短期間で、「第一次情報セキュリティ基本計画」「セキュア・ジャパン2006」といった政府戦略の策定、「政府機関統一基準」等の基準公開といった具体的成果が出されている。事務局及び関係者の皆様のご尽力に敬意を表する。

「第一次情報セキュリティ基本計画」には、実現すべき基本目標として、“IT を安心して利用可能な環境の構築”が掲げられている。産業界も、より安全・安心な製品・サービスを提供する責務があると日頃より感じている。

今年度「セキュア・ジャパン2006」で重点指針とされた「官民における情報セキュリティ対策の構築」にむけて、現在、関連する施策が実施されていると認識している。来年度早々には、次期年度計画である「セキュア・ジャパン2007」が策定されることと考えるが、「第一次情報セキュリティ基本計画」のもと、情報セキュリティ問題に対して、官民の各主体(政府機関・地方公共団体、重要インフラ、企業、個人)が自律的に取り組むことを期待している。同時に、これまで実施された施策の整理、各施策との整合性の確認、及び、定着していない施策に関する原因分析並びに対応をお願いしたい。

一方、NISCに対しては、各主体内及び各主体間で連携・協調を促進するための一層のリーダーシップを期待したい。更には、情報セキュリティ分野で世界のトップランナーとなるためのグローバルな取組みを推進して頂きたい。

なお、個別具体的には、以下について更なる対応・推進を頂きたい。

1．情報セキュリティ対策の必要性を共有し、責任分担を明確化

情報セキュリティ対策は、機器や特定の製品の防護だけでは十分でなく、業務・サービスの安定した継続稼動の観点から総合的な対策を講ずる必要がある。業務・サービスのITへの依存度が高まる今日では、これらの停止や機能低下の社会的影響が深刻化してきており、情報システムの信頼性・安全性向上は喫緊の課題である。

そこで、情報システムの構築や運用に当たっては、発注者と受注者の間で、以下の3点を事前に明らかにしておく必要がある。

①情報セキュリティ対策を実施することを基本認識として共有する。
②対象となる情報システムの情報セキュリティ対策の具体的な内容を取り決める。
③それぞれの対策に関する役割と責任分担を明確化する。

②に関しては、対象となる情報システムにおける情報セキュリティ上の脅威の特定や、これら脅威に対する脆弱性の分析、そして、具体的な情報セキュリティ対策の内容を示すことで、情報セキュリティ対策を講ずる上での前提条件と対策の内容を、発注者と受注者が共有することが必要である。③の責任分担は、このような具体的な対策が列記されて始めて可能になる。また、今日のように、高度にネットワーク化された社会では情報システムが相互に接続

されるケースが多いため、それぞれの情報セキュリティ対策のレベルの不整合によって発生する問題も看過できない。

このような観点から、政府は民間企業に対して、情報システムの開発・運用に際して、発注者と受注者間の情報セキュリティ上の責任分担を明確化するよう働きかけると共に、相互接続する情報システムの情報セキュリティ対策のレベルが比較可能となるような一定の基準を示すことが必要と考える。

例えば、重要インフラにおいては、指針を踏まえて各重要インフラの10分野における安全基準等ガイドラインの整備をすすめているが、情報システム相互の依存関係が高まっている現在、これらの安全基準等の策定・見直しを更に進め、重要インフラ間で共通に利用できる安全基準・個別マニュアル等を整備する必要がある。あわせて、民間企業においても共通認識できる基準の策定が期待される。

2．情報セキュリティ対策の演習はＰＤＣＡをベースに実施

重要インフラ分野では、安全基準の策定、相互依存性解析、分野横断的な情報共有体制の構築と、段階的な取り組みが実施されている。加えて、内閣官房及び一部の重要インフラでは、有効性を確認するための机上演習の実施が予定されており、演習の成果が期待される。机上演習を行うに当たっては、定量的な目標を設定し、目標設定⇒演習⇒測定⇒分析・改善といったＰＤＣＡサイクルに着目し、常に対策の有効性を高めることが必要である。

一方、「セキュア・ジャパン2006」では、今後、机上演習を受けた総合演習の実施を検討するとあるが、関係官庁や重要インフラ提供事業者の協力を得た上で、擬似的な環境での実演習の実施が強く期待される。例えば、擬似的なハッキングが発生した場合に、経路の遮断やセキュリティホールの修復にどの程度の時間を要したかを計測し、次の演習までに対応時間をどの程度短縮するかの目標を立て、その目標の実施状況を精査することが肝要である。このような、リアルな場面での演習こそが、情報システムに対する情報セキュリティ対策の向上に効果を発揮するものと考える。

以上