資料12

2005.09.15

意見書

村井　純

政府統一的基準について、分散システムとして機能する本システムの観点から次のような検討を実施することが必要である。

1．各省庁の自律的な責任感の確立

政府保有情報処理システムの構築･運用に責任をもつ各省庁が、内閣官房が定めた統一基準があるから情報セキュリティ対策を行うという姿勢ではなく、主体的に各省庁の責任と捉え、主体的に率先して対策の実施と改善に取り組むようにするための方策が必要である。この自律的な責任感の確立プロセスが無いままでは、政府内の情報セキュリティ対策高度化は望めない。

2．情報セキュリティに取り組む各省庁の方針決定と意思決定の透明性確保

各府省庁において、情報セキュリティ対策についてどのような方針を持つのか、さらには、その方針に基づく情報セキュリティ対策の策定･実施の意思決定プロセスの透明性を確保することが大切。特に、国民に対する各省庁の説明責任を果たすという観点からも重要である。

3．情報セキュリティ対策についての検査と改善義務の明確化

情報セキュリティ対策の実施状況について、内閣官房情報セキュリティセンターがアクセスできることを現在の枠組みの中で確保すべき。さらに、このアクセスによって問題点が発見され、情報セキュリティ政策会議からの改善勧告が行われた場合には、対象となる省庁は改善を行うことに責任を持つ、ということについての政府内のコンセンサスが必要だと考える。
また、状況に対する情報提供の要求に応えるシステムも確立しなければならない。

4．各省庁が持つシステム運用記録の保持

各府省庁が保有する情報システムの運用記録（いわゆるログ）について、各府省庁が責任を持って保存し、トラブル等発生時の原因解明に利用できるようにすること。特にログ保存の基準、およびその開示の基準については、内閣官房情報セキュリティセンターにおいて策定し、各府省庁に実施させること。

5．組織を越えた緊急避難構造の準備

内閣官房情報セキュリティセンターが主導して、各省庁の情報システムのサービス継続性計画（あるいはＢＣＰ）を各省庁に策定させ、実施が可能な環境構築をする。この際、各省庁の異議、および新しい課題への迅速な対応などのために、組織を越えて総合的にサービスの緊急避難ができるような構造を確立しなければならない。

以上