

各府省庁の情報システム及びその運用に関する安全基準の策定に係る基本方針及び各府省庁の情報セキュリティ対策の評価に係る基本方針について（案） （概要）

1 課題

「情報セキュリティポリシーに関するガイドライン」（平成12年7月18日情報セキュリティ対策推進会議決定）は、各府省庁が取るべき具体的な対策を十分に示していない。

また、「情報セキュリティポリシー」にどのような事項を規定するかは各府省庁に委ねられている。

内閣官房が実施した各府省庁の情報システムの脆弱性に関する検査の結果、各府省庁の情報セキュリティ水準にはばらつきがあることが判明。

技術的セキュリティに関する事項だけでなく、物理的、人的セキュリティに関する事項をも含めた対策がなされていない。

各府省庁の「自己点検」や「外部委託監査」だけでは、客観性に欠け、複数の府省庁に係る結果の比較も困難。

2 対策

（1）各府省庁の情報システム及びその運用に関する安全基準の策定

政府の基本方針の明示

情報セキュリティに関する政府の基本方針を明示することとする。

統一性と拘束力

情報の国家的、社会的な性質に応じて政府として横断的かつ統一的に分類。その分類に応じて全ての府省庁が情報セキュリティの確保のために必ず取らなければならない対策を規定。

総合的な対策

技術的セキュリティに関する事項だけでなく、物理的・人的セキュリティに関する事項も含んだ基準とする。

具体的な対策の明示

情報のライフサイクル及び情報システムのライフサイクルの各段階における脅威に対処するため取るべき対策について具体的に提示。

また、各対策を行うべき者は誰であるか（幹部（管理責任者）、システム管理者、端末利用者、一般職員等）を明示。

実効性の確保

各府省庁の組織及び情報システムの運用の実態を踏まえ、各府省庁の職員が実際に遵守できる実効性あるものとする。

（2）各府省庁の情報セキュリティ対策の評価

上記「安全基準」に基づき、内閣官房が総合的、客観的、統一的な視点で評価を実施。