資料４

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について（案）

平成 16 年 7 月 26 日
情報セキュリティ対策推進会議幹事会

１　「ガイドライン」の果たした役割と「基準」策定の必要性

「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。以下「ガイドライン」という。）は、各府省庁が当該府省庁における情報セキュリティを確保するための基本方針と具体的な対策について自ら組織的に検討して「情報セキュリティポリシー」を定め、これを職員に遵守させることの重要性と各府省庁における「情報セキュリティポリシー」策定の手続等を示したものであった。ガイドラインは、各府省庁がこれに基づいて「情報セキュリティポリシー」を策定、運用したことにより、各府省庁に情報セキュリティに関する意識を定着させ、各府省庁の情報セキュリティ水準を向上させたという点では、一定の成果を得たと考えられる。

しかし、ガイドラインは、あくまで各府省庁が情報セキュリティポリシーを策定するための参考資料と位置づけられており、また、各府省庁が取るべき具体的な対策も十分に示していないため、「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。このため、各府省庁において実際に取られている対策と各府省庁の情報セキュリティ水準はまちまちであり、政府全体として十分な情報セキュリティ水準が確保されているとは言い難い状況にある。

また、各府省庁の組織や情報システムの運用の実態を十分に踏まえておらず、実際に適用する上で難がある等の問題も指摘されている。

このため、今般、政府として統一的な「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」（以下「基準」という。）を策定し、各府省庁の情報セキュリティの水準の斉一的な引き上げを図ることによって、行政事務の円滑かつ適正な遂行を期すとともに、国民の信頼を確保しようとするものである。

２　基準策定に当たっての留意事項

基準の策定に当たっては、次の事項に留意するものとする。

（１）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確に示すこととする。

（２）「情報」の位置づけと分類

「情報」、「情報システム」及び「これらを取り扱う者」の相互関係を明確にし、守るべきものは「情報」であるという視点から全体を構成する。なお、この「情報」には、情報システムに関係がある限り、紙に記載された情報や情報システム外部の電磁的記録媒体に記録された情報を含めるものとする。

また、「国の安全、外交上の秘密その他の国の重大な利益に関する情報」、「犯罪の捜査、公訴の提起又は維持等に関する情報」、「当該情報の改ざん若しくは破壊又は当該情報が利用できないことにより国民の生命又は身体に危害が及ぶおそれがある情報」、

「個人情報」等、情報の国家的、社会的性質に応じてこれを分類し、同種の情報については政府内で統一的な取扱いを担保する。

（3）統一性と拘束力

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定めることにより、府省庁による情報セキュリティ水準のばらつきを防止し、政府全体として遺漏のない情報セキュリティを確保する。

なお、各府省庁は、策定された基準に基づき、既存の情報セキュリティポリシー、情報システム関係訓令等について必要な見直しを行うものとする。

（4）具体的な対策の明示

情報の入力、編集、保存、出力、廃棄等といった情報のライフサイクル及び情報システムの設計、調達、運用、保守等といった情報システムのライフサイクルの各段階において、情報及び情報システムに関与するそれぞれの者（幹部（管理責任者）、システム管理者、端末利用者、一般職員等）が「自分は何をすべきか。何をしてはならないのか。」を明確に認識できるよう、遵守事項、禁止事項等を具体的に記述する。

（5）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た実効性あるものとする。また、当初の基準策定に当たっては、必要不可欠な最低限の事項は盛り込みつつも、各府省庁の職員が実際に遵守できる内容とする。

（6）明解な語句、表現の使用

可能な限り平易な文言を用い、かつ、言わんとするところが明確な表現を用いるものとする。また、基本的な用語には定義を付し、外来語の安易な使用は戒めることとする。

なお、重要又は難解な部分については、必要に応じ、解説を付すこととする。

（7）監査等の基準としての位置づけ

上述した統一性、具体性、実効性、一義性等を確保することにより、内閣官房等が各府省庁の情報システム及びその運用について監査等を行う場合の基準として活用できるよう配慮する。

（8）段階的見直し

各府省庁の情報セキュリティ対策が段階的に推進されるよう、基準に基づく監査等の結果をも踏まえて、基準の見直しを定期的に行い、項目の追加やその内容の充実等を図ることとする。

3　基準の構成

上記留意事項を踏まえ、基準の構成は、次のとおりとする。

- 政府として横断的かつ統一的な情報の分類を行い、情報の種別ごとに基準を策定するものとする。
- 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いてどのような脅威が存在するかを分析し、当該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する。特に、情報システムから出力された情報が記録された書類や電磁的記録媒体の紛失、盗難等が情報漏洩事案の原因の中で大きい比重を占めているこ

とに鑑み、これらの書類や電磁的記録媒体の管理については、詳細に規定する。

・ 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）を明示する。

4　従来のガイドラインとの関係

従来のガイドライン及びこれに附属した「A省ポリシー（例）」のうち、各府省庁が実施すべき具体的な対策に該当する部分は、これを抽出し、必要な追加、削除、修正を行った上で基準に盛り込むものとする。

他方、従来のガイドライン及び「A省ポリシー（例）」のうち、各府省庁がセキュリティポリシーを策定する上での手続き及び考え方に関する部分は、新しいガイドラインとして再構成する。この場合において、「情報セキュリティ委員会」の設置等、各府省庁において情報セキュリティ対策を推進し、管理するための組織に係る部分については、各府省庁の実態に委ね、必要な要件（情報システム担当部門だけでなく、情報システムを運用する部門や人事、会計部門等を含めた検討体制を確保すること、担当者だけでなく幹部を参加させること等）のみを定めることとする。また、「リスク分析」に係る部分については、実際に適用することが可能な内容に改めるよう検討することとする。