DM7-03-091

情報システムに関する情報セキュリティ対策
実施確認のための点検リスト策定手引書

2009 年 9 月

内閣官房情報セキュリティセンター

改訂履歴

改訂日	改訂理由
2008/12/26	初版
2009/9/14	第２版

目次

1　本手引書の目的

「政府機関の情報セキュリティ対策のための統一基準 第４版」（以下「統一基準」という。）のうち情報システムに関係する遵守事項を情報システムに適切に適用することは、情報を保護するために重要なことである。しかし、様々な形態の情報システムに対して、情報セキュリティ対策を一様に定めることは現実的ではなく、統一基準では主として第 1.5 部と第 2.1 部にて必要となる対策の枠組みを示し、第 2.2 部にて情報システムの構成要素ごとの対策、そして第 2.3 部にて個別に必要となる対策を示した上で、それらを複合して適用することを求めている。

それらのうち、第 1.5 部と第 2.1 部の遵守事項は情報セキュリティ対策の必要性の有無を個々に判断して適用することになっている。

また、第 2.2 部の構成要素ごとの対策については、構成要素として適用しなければならない対策を定めているが、情報システムの構成要素となる製品を選定した後からでは、選定した製品が備えている機能しか適用できない。

このため、第 1.5 部、第 2.1 部、第 2.2 部及び第 2.3 部のうち情報システムに関する遵守事項をどのような観点でどの段階で適用すれば、適切な対策を講じることができるのかを理解しておくことが重要である。

本手引書は、新規に構築する情報システムにおいて、統一基準のうち情報システムに関係する遵守事項の適用方法について解説することを目的とする。なお、説明を簡潔にするため、新規に構築する情報システムを想定するが、既存の情報システムに対して遵守事項を適用する際にも参考にできるものである。

2　本手引書の対象者

2.1　対象者

本手引書は、情報システムの企画や設計を実施する者及び構築や運用時に情報セキュリティ対策基準の遵守方法について計画する者を対象とする。

3　統一基準に準じた対策基準の適用

情報システムに関する遵守事項に漏れがないように、確認表を使って確認する必要がある。

3.1　適用方法の検討

遵守事項のそれぞれについて適用方法を検討すればよいが、役割や情報システムの構成ごとに、ある遵守事項について適用方法を複数検討する必要がある場合もある。そのような場合には、適宜、複数の適用方法を検討しなければならない。

各遵守事項において、対策を実施したか否かの判断基準を決めることにより、検討中の適用方法の具体性が十分であるかを確認するのに役立てることができる。

3.2 点検リストの使い方

統一基準の遵守事項のうち、情報システムに関係するものについて、そのような判断基準を記載した例を付表１の点検リストに示す。

3.2.1 点検リストの構成

点検リストは、統一基準の情報システムに関わる遵守事項（第 1.5 部、第 2.1 部、第 2.2 部及び第 2.3 部のすべての遵守事項）ごとに、以下の項目について記載し、又は情報システムの作業工程に携わる者等が点検・記入する欄を設けている。

- 統一基準項番、基本／強化、遵守事項
  統一基準の遵守事項について、項番、対策レベル（基本遵守事項か強化遵守事項かの別）、遵守内容を記載している。
- 情報システムのライフサイクルへの適用に関わる解説
  情報システムのライフサイクルを「設計・開発」、「運用・保守」、「他」の３つの作業工程に分類し、遵守事項を各作業工程に適用する際に参考可能な情報を記載している。なお、ある作業工程への適用が一般的に想定されない場合は、当該作業工程に対応する欄の記載を「（該当せず）」としている。
  - ○ 設計・開発に関わる解説
    「設計・開発」の作業工程に関わる解説を記載している。例えば、機能の技術的な実現等。
  - ○ 運用・保守に関わる解説
    「運用・保守」の作業工程に関わる解説を記載している。例えば、手順書に記載されるべき内容や、手順書に従った運用の実施等。
  - ○ 他（利用者による対策、省庁対策基準等）
    「設計・開発」、「運用・保守」に該当しない作業工程での実施を記載している。具体的には、利用者向け手順書への反映や、利用者への周知、情報セキュリティ関係規程の確認、組織内セキュリティ管理の確認。
- 当該情報システムの評価
  情報システムの作業工程に携わる者等が点検・記入するための欄を設ける項目である。作業計画時又は作業完了時の点検結果・実施内容等を記載する。なお、「本遵守事項の該当性」の項目については作業工程ごとに点検するよう欄を設けることを想定している。
  - ○ 本遵守事項の該当性
    当該情報システムに遵守事項を適用する必要性の有無を判断し、必要性の有るものを「該当する」（〇）、無いものを「該当しない」（×）

とする。

○ 採用する対策内容

「設計・開発」の作業工程に適用する遵守事項のうち、当該情報システムに該当するとしたものについて、その対策内容を記載する。

○ 納品時・作業完了時の確認結果

「設計・開発」の作業工程に適用する遵守事項のうち、当該情報システムに該当するとしたものについて、納品時・作業完了時に対策されていることを確認し、対策実施状況が「十分」（〇）か「不十分」（×）かを記載する。

3.2.2 点検リストの利用の流れ

点検リストは一例として以下のような利用の流れを想定しているが、これらの利用方法に限るものではない。

（1） 省庁対策基準等に合わせて「点検リスト」の項目・内容をカスタマイズ

（2） 情報システムに携わる者が企画・要件定義時等の出来るだけ早い段階に、点検リスト中の各遵守事項が対象情報システムに該当するかを判断

（3） 「設計・開発」や「運用・保守」の作業計画時に、本点検リストの遵守事項（該当判断済み）を確認し、対策内容について検討

（4） 「設計・開発」の場合には、作業完了時の対策実施状況の確認等を実施