

脅威の変化

内部規律違反(ファイル共有ソフトの使用、USBメモリの紛失等)による情報漏えい

外部からの攻撃(標的型攻撃等)による情報窃取等

社会経済環境の変化

IT依存度の一層の高まり

厳しい財政状況(限られた人員・予算)

従来の統一基準の役割

情報セキュリティ水準の全体的な底上げ

今後の対策強化(統一基準見直し)の方向性

統一基準の見直し
リスク評価手法の策定

- 実施すべき対策のベースラインを明確化し、全体的な底上げ対策を着実に実施
- **各府省庁が業務で扱う情報の機密性の要求度等に応じた対策を重点強化**
 - ・ 機微な取扱いが必要な情報等を扱う業務領域について、リスク評価を行い、外部の脅威(標的型攻撃等)から重要な情報を守るために必要な対策を検討
 - ・ 各府省庁のCISO(最高情報セキュリティ責任者)が残存リスクを把握し、限られた人員、予算の中で講ずるべきセキュリティ対策(投資)を計画的・重点的に実施