暗号危殆化の危険度判定及び対応フローについて（概要）

資料5-1

- NISCにて危険度を判定して各省に伝達。
  - **危険度1、2の場合**、NISC主催の**各省説明会**において説明。
  - **危険度3と判断**され、政府として緊急に対処する必要性がある場合には、**CISO連絡会議等で決定**し、各省に伝達　　※ 危険度2の場合でも、影響度を踏まえCISO連絡会議等にて決定する可能性がある。

役割と判定の流れ

総務省・経済産業省

暗号の安全性に関する監視

情報交換

NISC

情報システムにおける暗号の危険度の判定、及び各省への伝達

NISCで判定を実施

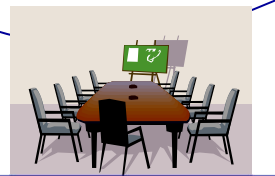
【危険度1、2の場合】

※影響が限定的又は軽微な場合

各省説明会

【危険度3の場合】

※影響が広範囲かつ深刻な場合



CISO連絡会議等

対処の必要性に関する判断

各省

危険度に応じた対処を行うとともに、関係機関へ情報提供 ※

※　必要に応じて、事後、情報セキュリティ政策会議に報告

危険度の判定に当たっては、
- **総務省・経済産業省から提供される情報**
- **NISCで把握している各省のシステムにおける暗号利用状況等**から、

各府省庁のシステム及びシステムで取り扱う情報への影響の程度と範囲を踏まえ、総合的な観点でこれを実施する。
判定した危険度に応じて、**CISO連絡会議等での対処の必要性の判断**や各省説明会での状況説明を行う。

暗号の「急激な危殆化」が発生した場合に備えた「緊急対応計画」の策定

- 緊急対応計画とは、新たな暗号方式への移行が完了する前に、暗号の急激な危殆化が発生した場合に備えて策定する計画。
- SHA-1及びRSA1024の安全性がどの程度かということを「危険度」によって表現し、現状は危険度1と想定。
- 新たな暗号方式への移行完了以前に
  安全性低下による支障が発生した場合に備え、官民連携した緊急対応計画を策定

危険度があがる判断はNISCより発信

危険度0 ： 安全	暗号として十分に利用できる状態	
危険度1 ： 危険（現在はここ）	理論的な暗号解読アルゴリズムが公開された状態	体制整備
危険度2 ： Y年で危殆化	高性能計算機等の利用によって危殆化が実証された状態	状況判断 対策の周知 システム対応
危険度3 ： 危殆化	十分に短い時間で署名の偽造ができる状態	利用停止 若しくは 別の業務を利用する方法

緊急対応計画をそれぞれの段階ごとに事前に策定