資料２－１

暗号危殆化の危険度判定及び対応フローについて（案）

平成 24 年４月○日
情報セキュリティ対策推進会議決定

暗号危殆化の危険度判定及び対応フローは次のとおりとする。

１　総務省及び経済産業省は、SHA-1 及びRSA1024 の安全性に関する監視を行い、内閣官房情報セキュリティセンター（以下「NISC」という。）への情報提供を行う。

２　NISC は、前項１により総務省及び経済産業省から情報提供を受けた場合は、提供された情報及びNISC で把握している各府省庁の情報システムにおける暗号利用状況等から、各府省庁の情報システム及び情報システムで扱う情報への影響の程度と範囲等を総合的に勘案し、その安全性を別表に示す「危険度」の０～３により判定する。

３　NISC は、前項２の判定の結果、「危険度」に変更がある場合は、変更後の「危険度」に応じて以下の対応を行う。

(1)　変更後の「危険度」が１又は２である場合、各府省庁に対する説明会を開催し、情報提供を行う。

(2)　変更後の「危険度」が３である場合、情報セキュリティ対策推進会議（以下「CISO 等連絡会議」という。）等を開催し、情報提供を行う。CISO 等連絡会議において、対処の必要性に関する判断を行う。

４　各府省庁は、前項３により情報提供を受けた場合は、「危険度」に応じて緊急対応計画の発動等必要な対処を実施するとともに、関係機関へ情報提供を行う。実施した対処内容については、必要に応じて、情報セキュリティ政策会議及びCISO 等連絡会議に報告する。

（別表）「危険度」の定義

危険度	状態	危険度に応じた対処の例
0	安全：暗号として十分に利用できる状態	なし
1	危険：理論的な暗号解読アルゴリズムが公開された状態	緊急対応計画の策定等体制を整備
2	一定年限後に危殆化：高性能計算機など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、システム対応を実施
3	危殆化：十分に短い時間で署名の偽造ができる状態	情報システムの利用停止若しくは別の業務を利用する