資料１－３

政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針の改定（案）

新旧対照表

No.	改定案		現行	
1		平成 20 年 4 月 22 日 情報セキュリティ政策会議決定 平成　年　月　日改定 情報セキュリティ対策推進会議決定		平成 20 年 4 月 22 日 情報セキュリティ政策会議決定
2	2　対象機関	内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、金融庁、消費者庁、復興庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省及び防衛省とする。	2　対象機関	内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、金融庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省及び防衛省とする。
3	3（1)(ア)	政府認証基盤（GPKI）　及び電子認証登記所（商業登記認証局）	3（1)(ア)	政府認証基盤（GPKI）　及び商業登記認証局
4	3（3)	キ　総務省及び法務省は、2014 年 9 月下旬以降の早期に、政府認証基盤及び電子商業登記所（商業登記認証局）において、電子証明書の発行に使用する暗号アルゴリズムを SHA-256 及び RSA2048 の組合せに変更するとともに、電子証明書の発行対象者の鍵ペアに使用される暗号アルゴリズムを RSA2048 に切り替える。 ク　総務省及び法務省は、2015 年度	3（3)	(新規追加)

No.	改定案	現行
	までに、政府認証基盤及び電子商業登記所（商業登記認証局）において、暗号アルゴリズム SHA-1 又は RSA1024 を用いた電子証明書の検証を終了する。ただし、発行済み電子証明書の有効期間が 2015 年度末を超え、その検証の終了が制度や費用の観点で困難であり又は合理的で無い場合は、2019 年度を超えない範囲で SHA-1 又は RSA1024 を用いた電子証明書の検証を行うことも可能とする。	