2008.7.28

『電子政府推奨暗号の利用方法に関するガイドブック』正誤表

報告書等	項目等	頁	改訂内容
電子政府推奨暗号の利用方法に関するガイドブック	2.1.4 通信相手の認証で利用される対策技術 (1)SSL (エ)暗号アルゴリズムの安全性と SSL の安全性の関係 (iv)暗号通信	12	(誤)暗号通信には共通鍵暗号と、(ウ)と同様に・・・→(正)暗号通信には共通鍵暗号と、(iii)と同様に・・・ (誤)完全性の検証に利用されている HMAC およびハッシュ関数については、(ウ)同様。→(正) 完全性の検証に利用されている HMAC については、(iii)同様。
〃	2.1.4 通信相手の認証で利用される対策技術 (オ)推奨される利用方法 (ii)鍵共有」	13	(誤)公開鍵暗号(署名)、ハッシュ関数:(ア)と同様→(正)公開鍵暗号(署名)、ハッシュ関数:(i)と同様
〃	2.1.4 通信相手の認証で利用される対策技術 (オ)推奨される利用方法 (iv)暗号通信	13	(誤)HMAC、ハッシュ関数:(ウ)と同様→(正)HMAC:(iii)と同様
〃	6.1.4 公開鍵の証明で利用される対策技術 (1)X.509v03 (オ)推奨される利用方法	127	(追加)署名の推奨される CRYPTREC 暗号とセキュリティパラメータに RSA-PSS(2048 bit 以上)を追加
〃	6.1.4 公開鍵の証明で利用される対策技術 (2)CRL(Certification Revocation List)	127	(誤)CRL (Certification Rivocation List) →(正)CRL (Certification Revocation List)
〃	6.1.4 公開鍵の証明で利用される対策技術 (2)CRL(Certification Revocation List) (オ)推奨される利用方法	128	(追加)署名の推奨される CRYPTREC 暗号とセキュリティパラメータに RSA-PSS(2048 bit 以上)を追加