正誤表

報告書等	項目等	頁	改訂内容
2008 年度版リストガイド(電子署名)	1.2 用語および略称 DSA	2	(誤)DSA Digital Signature Algorithm (specified in this standard)。 →(正) DSA Digital Signature Algorithm
〃	1.2 用語および略称 RSA	3	(誤)RSA Algorithm developed by Rivest, Shamir and Adelman →(正)RSA Algorithm developed by Rivest, Shamir and Adleman
〃	1.3.3 評価観点と比較 表 1(注 4)	6	(誤)(注 4)DSA,ECDSA はハッシュ関数として SHA-1 を利用する。 →(正)(注 4)FIPS 186-3 は、Draft 版であるため、CRYPTREC としては当面 DSA,ECDSA を利用する場合には SHA-1 を利用することを推奨する。
〃	1.4.5RSASSA-PKCS1-v1_5 EMSA-PKCS-v15(*M,emLen*) 手順 2.	22	(誤)2.ハッシュ関数のアルゴリズムIDとハッシュ値を、以下に占める ANS.1 の・・・→(正)2.ハッシュ関数のアルゴリズムIDとハッシュ値を、以下に占める ASN.1 の・・・