JPNIC プライマリルート認証局の CPS 変更案について

JPNIC プライマリルート認証局運営委員会

■1. おはかりする内容

JPNIC プライマリルート認証局において古い暗号アルゴリズムの使用を停止したことから、CPS 変更案を作成した。JPNIC プライマリルート認証局運営委員会として、理事会に提案する CPS 案にすることを承認いただきたい。

■2. CPS の変更点

CPS の中から古いアルゴリズムに関する記述を削除する（表 1）。

表 1. 変更の内容

頁	節	変更前	変更後	理由
23	7.1.3. アルゴリズム OID（オブジェクト識別子）	sha256WithRSAEncryption（1.2.840.113549.1.1.11） sha1withRSAEncryption（1.2.840.113549.1.1.5）	sha256WithRSAEncryption（1.2.840.113549.1.1.11）	使用しないアルゴリズムの削除
24	表 7-1 signature の Algorithm	sha256WithRSAEncryption sha1withRSAEncryption	sha256WithRSAEncryption	使用しないアルゴリズムの削除
25	表 7-1 の注	※2　古い認証局証明書に入る値： C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S1 新しい認証局証明書に入る値： C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S2 ※3　JPNIC Primary Root Certification Authority S1 では sha1WithRSAEncryption とし、JPNIC Primary Root Certification Authority S2 では sha256WithRSAEncryption とする。	*2 値は C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S2 とする。	古い認証局証明書の値を削除

26	表 7-2	sha256WithRSAEncryption sha1withRSAEncryption	sha256WithRSAEncryption	使用しないアルゴリズムの削除
26	表 7-2 の注	※1　古い認証局証明書に入る値： C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S1 新しい認証局証明書に入る値： C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S2 ※2　JPNIC Primary Root Certification Authority S1 では sha1WithRSAEncryption とし、JPNIC Primary Root Certification Authority S2 では sha256WithRSAEncryption とする。	*1 値は C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S2 とする。	古い認証局証明書の値を削除
24 26	表 7-1 表 7-2	subject と issuer の行の形式を他の行と合わせる。（内容に変更はなし）		

■3. 変更後の CPS

変更後の CPS 案を資料 8-2 として添付する。

以上