2011/12/16　第 87 回理事会
資料 1-1

JPNIC プライマリルート認証局
CPS の改定について

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運営委員会は、2011 年度、JPNIC プライマリルート認証局に新たに導入する暗号アルゴリズムを選定し、CPS 改定案を作成した。この CPS 案を JPNIC プライマリルート認証局 CPS とすることを承認いただきたい。

■2. CPS の改定点

利用できるアルゴリズムを追加し、新しいアルゴリズムを用いた認証局証明書を発行できるようにすると共に、古いアルゴリズムの認証局証明書と識別するために、新しい認証局の名称を追加する（表 1）。

表 1. 改定の内容

頁	節	改定前	改定後	理由
22	7.1. 証明書のプロファイル（Certificate Profile）		本認証局は、使用するアルゴリズムを移行するため、証明書プロファイルが異なる複数の証明書を発行する。これらは識別名の末尾につけた「S」＋番号で識別する。	新しいアルゴリズムを使用した証明書プロファイルを追加するため。
23	7.1.3. アルゴリズム OID（オブジェクト識別子）	sha1withRSAEncryption（1.2.840.113549.1.1.5）	sha256WithRSAEncryption（1.2.840.113549.1.1.11） sha1WithRSAEncryption（1.2.840.113549.1.1.5）	使用するアルゴリズムの追加
25	表 7-1	sha1withRSAEncryption	sha1WithRSAEncryption / sha256WithRSAEncryption *3	使用するアルゴリズムの追加
25	表 7-1 の注	※2　C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S1	※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	二種類の証明書を発行するための追加

			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。	
27	表 7-2	sha1withRSAEncryption	sha1WithRSAEncryption / sha256WithRSAEncryption *2	使用するアルゴリズムの追加
27	表 7-2 の注	※1　C=JP, O=Japan Network Information Center, OU=JPNIC Primary Root Certification Authority S1	※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。	二種類の証明書を発行するための追加

■3. 改定後の CPS

改定後の CPS 案を資料 1-2 として添付する。

以上