電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針の一部を改正する告示新旧対照条文

○　電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成十三年総務省・法務省・経済産業省告示第二号）

（傍線部分は改正部分）

改正案	現行
（特定認証業務に係る電子署名の基準）	（特定認証業務に係る電子署名の基準）
第三条　規則第二条の基準を満たす電子署名の方式は、次の各号のいずれかとする。	第三条　規則第二条の基準を満たす電子署名の方式は、次の各号のいずれかとする。
一　ＲＳＡ方式であって、ハッシュ関数としてＳＨＡ－１を使用するもの（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　五）、ＳＨＡ－２５６を使用するもの（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一一）、ＳＨＡ－３８４を使用するもの（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　一二）又はＳＨＡ－５１２を使用するもの（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　一三）のうち、モジュラスとなる合成数が千二十四ビット以上のもの	一　ＲＳＡ方式（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　五）又はＲＳＡ－ＰＳＳ方式（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　一〇）であって、モジュラスとなる合成数が千二十四ビット以上のもの
二　ＲＳＡ－ＰＳＳ方式（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　一〇）であって、ハッシュ関数としてＳＨＡ－１（オブジェクト識別子　一　三　一四　三　二　二六）、ＳＨＡ－２５６（オブジェクト識別子　二　一六　八四〇　一　一〇一　三　四　二　一）、ＳＨＡ－３８４（オブジェクト識別子　二　一六　八四〇　一　一〇一	二　ＥＣＤＳＡ方式（オブジェクト識別子　一　二　八四〇　一〇〇四五　四　一）であって、楕円曲線の定義体及び位数が百六十ビット以上のもの
	三　ＤＳＡ方式（オブジェクト識別子　一　二　八四〇　一〇〇四〇　四　三）であって、モジュラスとなる素数が千二十四ビットのもの

三　四　二　二）又はＳＨＡ－５１２（オブジェクト識別子　二　一六　八四〇　一　一〇一　三　四　二　三）を使用するもののうち、モジュラスとなる合成数が千二十四ビット以上のもの

三　ＥＣＤＳＡ方式であって、ハッシュ関数としてＳＨＡ－１を使用するもの（オブジェクト識別子　一　二　八四〇　一〇〇四五　四　一）、ＳＨＡ－２５６を使用するもの（オブジェクト識別子　一　二　八四〇　一〇〇四五　四　三　二）、ＳＨＡ－３８４を使用するもの（オブジェクト識別子　一　二　八四〇　一〇〇四五　四　三　三）又はＳＨＡ－５１２を使用するもの（オブジェクト識別子　一　二　八四〇　一〇〇四五　四　三　四）のうち、楕円曲線の定義体及び位数が百六十ビット以上のもの

四　ＤＳＡ方式であって、ハッシュ関数としてＳＨＡ－１を使用するもの（オブジェクト識別子　一　二　八四〇　一〇〇四〇　四　三）であり、かつ、モジュラスとなる素数が千二十四ビットのもの

（認定認証業務と他の業務との誤認を防止するための措置）

第十条　規則第六条第七号に規定する利用者その他の者が認定認証業務と他の業務を誤認することを防止するための適切な措置には、次の各号に掲げる措置が含まれるものとする。

一　（略）

二　発行者署名検証符号に係る電子証明書の値をＳＨＡ－１、ＳＨＡ－２５６、ＳＨＡ－３８４又はＳＨＡ－５１２のうち

（認定認証業務と他の業務との誤認を防止するための措置）

第十条　規則第六条第七号に規定する利用者その他の者が認定認証業務と他の業務を誤認することを防止するための適切な措置には、次の各号に掲げる措置が含まれるものとする。

一　（略）

二　発行者署名検証符号に係る電子証明書の値をＳＨＡ－１で変換した値によって認定認証業務を特定すること。

いずれか一以上で変換した値によって認定認証業務を特定すること。