



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方式であつて、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)

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 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方式であつて、ハッシュ関数としてSHA-1を用するもの(オブジェクト識別子 一 二 八四〇 一〇〇四五 四 三)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

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)であつて、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 一〇〇四五 四 三)であつて、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で変換した値によって認定認証業務を特定すること。

2012