平成２７年度　流通ＢＭＳドキュメント

「流通業界共通認証局　証明書ポリシー」の改訂内容

２０１５年１月２８日
技術仕様検討部会　事務局

本資料では、「流通業界共通認証局　証明書ポリシー（ＣＰ）」の改訂事項を以下に記載します。

1.　RSA 鍵長のサイズに関するＣＰの改訂について

変更の理由	(1) 2015 年時点において RSA 暗号鍵の長さについては、NIST の勧告等により 1,024 ビットは脆弱とされることから、鍵長を 2,048 ビット以上に変更すること。
変更の概要	(1) 利用者の証明書は 2,048 ビット以上の鍵長の RSA 暗号アルゴリズムを明記する。また句読点を補完する。

上記の変更にともない、6.1.5 項を次の通り改訂を行う。

【改定前】
6.1.5. 鍵サイズ
各流通業界共通認証局はその全ての階層構造中の認証局について、2,048 ビット以上の鍵長の RSA 暗号鍵アルゴリズムを使用しなければならない（ただし、別途認められた場合は除く）。
利用者は 1,024 ビット以上[1]の鍵長の RSA 暗号アルゴリズムを使用しなければならない

【改定後】
6.1.5. 鍵サイズ
各流通業界共通認証局はその全ての階層構造中の認証局について、2,048 ビット以上の鍵長の RSA 暗号鍵アルゴリズムを使用しなければならない（ただし、別途認められた場合は除く）。
利用者は 2,048 ビット以上[1]の鍵長の RSA 暗号アルゴリズムを使用しなければならない。

なお、脚注 1 についてはそのまま残すものとする。

2.　使用する暗号アルゴリズムに関するＣＰの改訂について（別添：移行スケジュール案）

変更の理由	(1) 認証局ならびに利用者証明書で使用する署名アルゴリズムで使用するハッシュアルゴリズムを sha1 から sha2 に変更する。本件により署名アルゴリズムでの sha1 の利用について発行並びに利用について期限を設定する。 (2) CRL の署名アルゴリズムで使用するハッシュアルゴリズムを sha1 から sha2 に変更する。本件により、sha1 を利用した署名アルゴリズムでの利用者証明書の有効期限まで sha1 を利用した CRL への署名を継続し、上記の期限をまで有効であるものとする。
変更の概要	(1) 証明書の署名アルゴリズムならびにそれを意味する OID を変更し期限を設定する。具体的には sha1WithRSAEncryption の新規発行はそれぞれの認証局が定めるものとするが、最大でも 2015 年 9 月 30 日まで、どの利用は 2018 年 12 月 31 日までとする。なお一般に SHA2 と分類されるハッシュアルゴリズムには以下のものがあることから、どちらかを選択可能とするように記載する。 • sha256WithRSAEncryption • sha384WithRSAEncryption • sha512WithRSAEncryption • sha224WithRSAEncryption また subjectPublicKeyInf は subjectPublicKeyInfo の誤りであるので修正する。 (2) CRL の署名アルゴリズムについて、上記と同様の変更を行う。 ただし、認証局の定めるタイミングまで、署名アルゴリズムが sha1RSAEncryption

	である利用者証明書が有効である間は、同じく CRL についても sha1RSAEncryption を継続使用するものとする。

上記の変更にともない、7.1.3 項および 7.2 項の表 8 を以下の通り改訂を行う。

【改定前】
7.1.3. アルゴリズムオブジェクト識別子
本項では、証明書への署名形式と証明書で証明される公開鍵の形式を規定する。基本領域の signature フィールドには sha1WithRSAEncryption (1.2.840.113549.1.1.5)が設定されなければならない。また、基本領域の subjectPublicKeyInf フィールドには rsaEncryption(1.2.840.113549.1.1.1)が設定されなければならない。

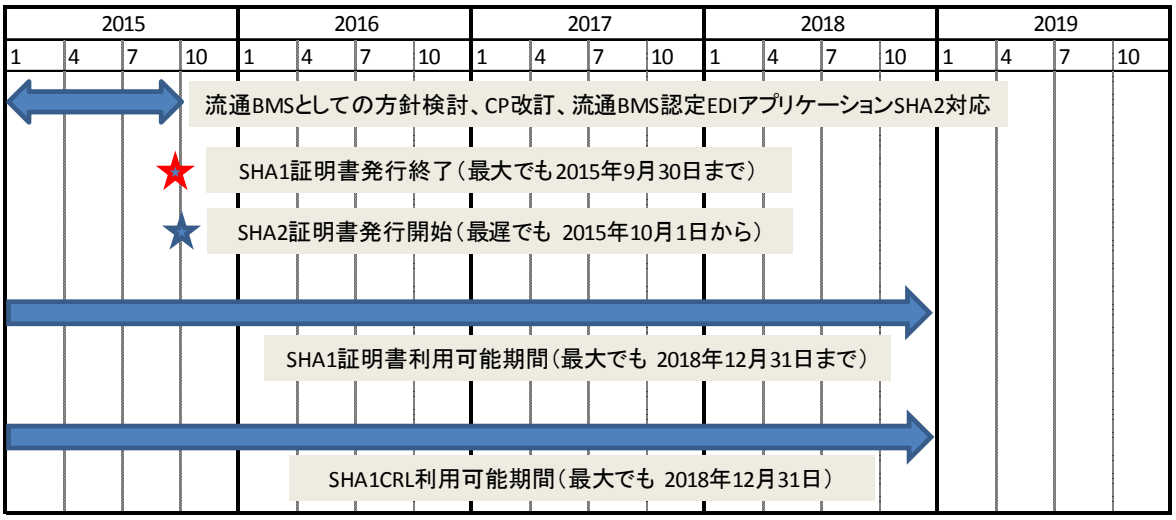
7.2 CRL のプロファイル
表 8
項番 2 signature　sha1withRSAEncryption

【改定後】
7.1.3. アルゴリズムオブジェクト識別子
本項では、証明書への署名形式と証明書で証明される公開鍵の形式を規定する。基本領域の signature フィールドには、**各認証局が定める日まで、または最大でも 2015 年 9 月 30 日まで sha1WithRSAEncryption (1.2.840.113549.1.1.5)が利用可能である。かつ sha1RSAEncryption を設定する利用者証明書は 2018 年 12 月 31 日を超えて利用してはならない。**
各認証局が定める日でかつ遅くとも 2015 年 10 月 1 日以降は sha256WithRSAEncryption (1.2.840.113549.1.1.11) 、 sha384WithRSAEncryption (1.2.840.113549.1.1.12) 、 sha512WithRSAEncryption (1.2.840.113549.1.1.13) 、 および sha224WithRSAEncryption (1.2.840.113549.1.1.14)のいずれかが設定されなければならない。
また、基本領域の subjectPublicKeyInfo フィールドには rsaEncryption(1.2.840.113549.1.1.1)が設定されなければならない。

7.2 CRL のプロファイル
表 8
項番 2 signature　sha1withRSAEncryption
sha256withRSAEncryption
sha384withRSAEncryption
sha512withRSAEncryption
sha224withRSAEncryption
のいずれか
但し、利用者は検証において CRL を利用する際 sha1withRSAEncryption で署名した CRL を 2018 年 12 月 31 日を超えて利用してはならない。

以上

別添


2015
2016
2017
2018
2019
1 4 7 10 1 4 7 10 1 4 7 10 1 4 7 10 1 4 7 10
流通BMSとしての方針検討、CP改訂、流通BMS認定EDIアプリケーションSHA2対応
SHA1証明書発行終了（最大でも2015年9月30日まで）
SHA2証明書発行開始（最遅でも 2015年10月1日から）
SHA1証明書利用可能期間（最大でも 2018年12月31日まで）
SHA1CRL利用可能期間（最大でも 2018年12月31日）