

2015 年 11 月 30 日

お客様各位

株式会社データ・アプリケーション

流通業界共通認証局の SHA-2 版のルート証明書と中間証明書のインポートのお願い

このたびは流通業界共通認証局の SHA-2 版証明書適用ファイルをダウンロードしていただきありがとうございます。流通システム標準普及推進協会からの告知のとおり、ACMS 製品に対して SHA-2 版の証明書を適用していただく必要があるため、下記の製品別の手順に従いインポートを実施していただけますようお願い致します。

記

1. ACMS E2X / ACMS B2B / ACMS B2B LE をご利用の場合

1.1.インポート方法

以下の手順に従いインポートを行ってください。

- (1)「ACMSE2XB2B」配下の 5 つの証明書ファイル（拡張子"cer"が 3 つ、"pem"が 2 つ）の存在を確認
- (2)これらを既存の ACMS が使用する SSL キーストアが存在する稼働ホスト上にコピー
- (3)keytool -import コマンドにより SSL キーストアへ各証明書をインポート

コマンド実行例：

```
keytool -import -alias [*1] -keystore [*2] -storepass [*3] -file [EINSPKI-EDI-CHAIN_v2.cer のパス]
keytool -import -alias [*1] -keystore [*2] -storepass [*3] -file [EINSPKI-EDI-ROOT_v2.cer のパス]
keytool -import -alias [*1] -keystore [*2] -storepass [*3] -file [rootcacertsha2.cer のパス]
keytool -import -alias [*1] -keystore [*2] -storepass [*3] -file [SymantecJapanBMSOnlineCA.pem のパス]
keytool -import -alias [*1] -keystore [*2] -storepass [*3] -file [SymantecJapanBMSRootCA.pem のパス]
```

*1…証明書のエイリアス名

*2…キーストアファイルのパス

*3…キーストアのパスワード

1.2.反映タイミングについて

キーストア更新の反映タイミングはクライアントとサーバの立場により異なります。

【クライアントの場合】

発信時（サーバへの接続時）に、キーストアを都度ロードするため、常に最新の状態で通信を行います。

【サーバの場合】

着信回線をいったん停止し、開始とすることで反映されます。

詳細は「AdditionalGuide」の「2.1.14. キーストアファイル更新後の反映タイミング」を参照してください。

2. ACMS Lite Neo をご利用の場合

2.1.インポート方法

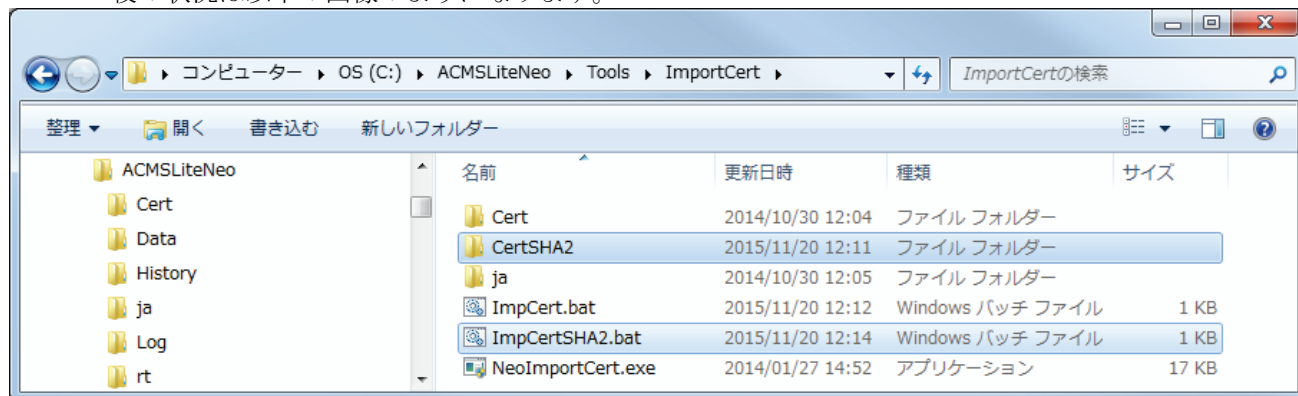
以下の手順に従いインポートを行ってください。

(1)「ACMSLiteNeo」配下の「CertSHA2」フォルダと「ImpCertSHA2.bat」ファイルの存在を確認

(2)これらを既存の ACMS Lite Neo の以下のフォルダにコピー

コピー先：[ACMSLiteNeo_HOME]¥Tools¥ImportCert

コピー後の状況は以下の画像のようになります。



(3)コピーした「ImpCertSHA2.bat」をダブルクリック

※途中 UAC（ユーザアカウント制御）の警告が出力されることがありますが、すべて「はい」とする

1.2.反映タイミングについて

発信時（サーバへの接続時）に、Windows ストアを都度参照するため、常に最新の状態で通信を行います。

2.参考情報 同梱証明書の詳細

本ダウンロードに同梱している証明書の詳細は以下のとおりです。

以下の証明書は、各認証局のリポジトリからも入手が可能となっております。

<Symantec PKI BMS Certificate>

ファイル	SymantecJapanBMSRootCA.cer SymantecJapanBMSRootCA.pem
説明	Symantec PKI BMS Certificate ルート証明書
有効期間(開始日)	2015/04/22 00:00:00 GMT
有効期間(終了日)	2035/04/22 23:59:59 GMT
フィンガープリント(SHA-2)	0b 87 9e 39 61 2b b4 60 b8 54 a9 af a3 1c 67 75 32 87 c8 d4

ファイル	SymantecJapanBMSOnlineCA.cer SymantecJapanBMSOnlineCA.pem
説明	Symantec PKI BMS Certificate 中間証明書
有効期間(開始日)	2015/04/22 00:00:00 GMT
有効期間(終了日)	2035/04/21 23:59:59 GMT
フィンガープリント(SHA-2)	53 81 27 b8 72 91 84 72 fa 22 57 bf 21 d3 7b e8 7a e2 6a 17

<GlobalSign EDI(流通 BMS)用電子証明書サービス>

ファイル	rootcacertsha2.cer
説明	GlobalSign EDI(流通 BMS)用電子証明書サービス ルート証明書
有効期間(開始日)	2015/06/17 00:00:00 GMT
有効期間(終了日)	2025/06/17 00:00:00 GMT
フィンガープリント(SHA-2)	08 00 64 2d 99 99 cb d0 81 e9 b2 a6 7c b3 d3 58 9e 33 40 9b

<EINS/PKI for EDI>

ファイル	EINSPKI-EDI-ROOT_v2.cer
説明	EINS/PKI for EDI ルート証明書
有効期間(開始日)	2015/04/28 13:51:02 GMT
有効期間(終了日)	2035/04/23 13:51:02 GMT
フィンガープリント(SHA-2)	9b 74 13 6a d5 a5 2a 94 0e 36 a6 9f 8a 68 f9 74 fe 23 c8 0f

ファイル	EINSPKI-EDI-CHAIN_v2.cer
説明	EINS/PKI for EDI 中間証明書
有効期間(開始日)	2015/04/28 13:58:26 GMT
有効期間(終了日)	2035/04/23 13:51:02 GMT
フィンガープリント(SHA-2)	a1 ad 8a 80 9b 5d 2d ea ea f9 21 26 6d 51 65 97 e2 e6 7f 7e