2017 年 4 月 4 日

※改訂履歴は最終ページに記載

お客様各位

株式会社 セゾン情報システムズ
HULFT 事業部

流通 BMS ガイドライン改定に対する HDC-EDI Base の対応

拝啓　貴社益々ご清栄のこととお慶び申し上げます。
平素は格別なるご高配を賜り誠にありがとうございます。

HDC-EDI Base をご利用いただいているお客様へのご連絡です。
流通システム標準普及推進協議会 技術仕様検討部会からの依頼に対し、弊社では下記のとおり対応しておりますので、何卒、ご確認の程お願い申し上げます。

■【１】署名アルゴリズムの SHA-1 から SHA-2 への変更

■ 告知日：2015 年 3 月 30 日
http://www.dsri.jp/ryutsu-bms/standard/data/CP_20150330.pdf

■ 製品別対処方法
●対象製品：HDC-EDI Base E2X / HDC-EDI Base B2B / HDC-EDI Base B2B LE
●SHA-2 への対応：SHA-224※1、SHA-256、SHA-384、SHA-512 の SHA-2 に対応
※1：SHA-224 を使用する場合は HDC-EDI Base サーバが Java8 で稼動している必要があります。

[対処方法]
認証局による SHA-2 版証明書の発行が開始された後、以下の作業を行っていただく必要があります。なお、SHA-2 版証明書の入手可能時期や入手方法は認証局各社にご確認ください。

1. SHA-2 版証明書の入手

(1) 現在ご使用のサーバ証明書の SHA-2 版を入手
相手先がサーバ証明書の事前交換を求める場合は、SHA-2 版を送付してください。
（HDC-EDI Base E2X / HDC-EDI Base B2B / HDC-EDI Base B2B LE は、事前交換は不要です。）

(2) 現在ご使用のクライアント証明書の SHA-2 版を入手
相手先がクライアント証明書の事前交換を求める場合、SHA-2 版を送付してください。
（HDC-EDI Base E2X / HDC-EDI Base B2B / HDC-EDI Base B2B LE は、事前交換は不要です。）

(3)認証局 3 社のルート証明書および中間証明書の SHA-2 版を入手

2015 年 10 月より認証局から入手が可能になりましたので、各認証局リポジトリより早急に入手してください。

2. keystore に各証明書をインポート

インポート方法は keytool のコマンドヘルプ、ドキュメント、および HDC-EDI Base E2X/ HDC-EDI Base B2B/ HDC-EDI Base B2B LE に同梱されている「AdditionalGuide.pdf」の「2.1. SSL プロトコルを使用した通信」をご参照ください。

(1) SHA-2 版サーバ証明書を keystore にインポート

SHA-2 版サーバ証明書をインポートする際、SHA-1 版サーバ証明書は削除します。

本作業は、すべての取引先クライアント環境において SHA-2 版のルート証明書および中間証明書の適用が完了している必要があります。

適用が未完了の取引先とは通信が行えないため、取引先の適用状況を必ずご確認いただいてからインポート作業を行ってください。

(2) SHA-2 版クライアント証明書を keystore にインポート

SHA-2 版クライアント証明書を入手した場合は、SHA-1 版クライアント証明書を削除してからインポートを行います。

(3) 認証局 3 社のルート証明書および中間証明書の SHA-2 版を keystore にインポート

「流通業界共通認証局証明書適用のご案内.pdf」に従いインポートを行います。

すべての通信相手先が SHA-2 への対応が完了するまではクロス期間となりますので、keystore 内に SHA-2 と SHA-1 の両方のルート証明書および中間証明書がインポートされている必要があります。

【２】SSLver3.0 脆弱性対応（TLS への移行対応）

流通開発標準普及推進協議会の告知「SSLver3.0 脆弱性対応のお願い」に記載された脆弱性対応へのご案内です。

流通 BMS の暗号化通信で使用される SSL プロトコルバージョンについては「SSL3.0」を廃止し「TLS」を使用することが義務付けられています。

■ 告知日：2015 年 4 月 21 日

http://www.dsri.jp/ryutsu-bms/standard/data/SSLv3_201504.pdf

■ 製品別対処方法

●対象製品：HDC-EDI Base E2X / HDC-EDI Base B2B / HDC-EDI Base B2B LE

[対処方法]

HDC-EDI Base サーバが使用する Java を以下のバージョン以降を使用してください。

なお、HDC-EDI Base Ver.3.5.0 以下のバージョンをご使用の場合は Java6、Java 7 および Java 8 は未サポートです。動作保障済みのバージョンへのアップグレードをご検討ください。

・Java 6 update 91 以降（Java 6 は HDC-EDI Base Ver.3.6.0 以降にて動作保障）
なお Java 6 update 45 より以降は有償サポート版となります。
・Java 7 update 76 以降（Java 7 は HDC-EDI Base Ver.3.9.0 以降にて動作保障）
・Java 8 update 31 以降（Java 8 は HDC-EDI Base Ver.4.2.0 以降にて動作保障）

動作環境の Java の仕様により、HDC-EDI Base は次のように動作します。この場合、HDC-EDI Base での設定はありません。

① HDC-EDI Base が発信の場合、ネゴシエーション時に TLS 1.0 を使用し、かつ、サーバ側が SSL3.0 を選択した場合に拒否します。
② HDC-EDI Base が着信の場合、相手からのネゴシエーションが SSL3.0 の場合に拒否します。
③ SSL3.0 を許容する場合は、<JRE_HOME>/lib/security/java.security の以下の設定から"SSLv3" を削除してください。

jdk.tls.disabledAlgorithms=SSLv3

【３】再ネゴシエーション時における脆弱性への対応

流通開発標準普及推進協議会の告知「SSLver3.0 脆弱性対応のお願い」に記載された脆弱性対応へのご案内です。

■ 告知日：2015年4月21日
http://www.dsri.jp/ryutsu-bms/standard/data/SSLv3_201504.pdf

■ 製品別対処方法
●対象製品：HDC-EDI Base E2X / HDC-EDI Base B2B / HDC-EDI Base B2B LE

[対処方法]
HDC-EDI Base サーバが使用する Java を Java 7 もしくは Java 8 にしてください。

【３】再ネゴシエーション時における脆弱性への対応

■ 告知日：2015 年 4 月 21 日

http://www.dsri.jp/ryutsu-bms/standard/data/SSLv3_201504.pdf

■ 製品別対処方法

●対象製品：HDC-EDI Base E2X / HDC-EDI Base B2B / HDC-EDI Base B2B LE

[対処方法]

HDC-EDI Base サーバが使用する Java を Java 7 もしくは Java 8 にしてください。

上記内容にてご不明な点がありましたら、契約しているサポート窓口へお問い合わせください。

以上

【改訂履歴】

2015 年 7 月 10 日	新規作成しました。
2017 年 4 月 4 日	SSLver3.0 脆弱性対応に Java6 の情報を追記しました。 再ネゴシエーション時における脆弱性への対応を追記しました。