２０１５年６月８日

流通システム標準普及推進協議会
技術仕様検討部会

SSLver3.0 脆弱性対応のお願い（改訂版）

拝啓　早春の候貴社益々ご清栄のことと存じます。
平素より流通システム標準普及推進協議会へご協力賜り、誠にありがとうございます。
さて、流通 BMS の暗号化通信で利用している「SSLver3.0」において、セキュリティの脆弱性が確認されました。これに伴い Web ブラウザ等の基本ソフトウェア各社から「SSLver3.0」の利用を停止する対応方針が出されております。
流通 BMS におきましても当該基本ソフトウェアの影響を受けて通信ができなくなる可能性が高いため、下記対応方針に沿ってご対応をお願い致します。

記

【ご対応のお願い】

■概要

「SSLver3.0」における脆弱性対応のため、Web ブラウザ等の基本ソフトウェア各社から「SSLver3.0」の利用を停止する方針が表明されております。その結果、今後「SSLver3.0」を利用した EDI データの送受信ができなくなる可能性があります。
※詳細につきましては IPA から公表されている共通脆弱性識別子「CVE2014-3566」をご参照ください。
https://www.ipa.go.jp/security/announce/20141017-ssl.html

また、2009 年に確認された再ネゴシエーション時における脆弱性への対応につきまして、一部パッケージで未対応のものが見受けられますので、あわせてご対応をお願い致します。
※詳細につきましては IPA から公表されている情報をご参照ください。
https://www.ipa.go.jp/security/fy21/reports/tech1-tg/b_02.html

■対応方針

各パッケージ等において、「TLS」への移行と「再ネゴシエーション」への対策をお願いいたします。

※TLS 移行に関する補足

TLS へ移行する際、お取引先様が TLS 未対応の場合は送受信ができなくなります。
各お取引先様の対応状況に合わせ、SSLv3 の並行期間を設ける等、対応方針の
検討をお願いいたします。
特に「JX 手順」で通信を行われている場合、サーバ側ユーザー様からクライアン
ト側ユーザー様に移行スケジュール等の周知をお願い致します。

■対応期間

・SSLver3.0 の脆弱性対応

⇒　2015 年 10 月 1 日までにご対応をお願い致します。

・再ネゴシエーション時の脆弱性対応

⇒　2015 年中にご対応をお願い致します。

【本件に関するお問い合わせ先】

各ソフトウェア／サービス提供元までお問い合わせください。

敬具