２０１５年3月３０日

流通システム標準普及推進協議会
技術仕様検討部会

流通 BMS　流通業界共通認証局証明書ポリシー改訂に伴うご対応のお願い

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。
この度、流通 BMS の流通業界共通認証局証明書ポリシー（CP）に対するチェンジリクエストが当協議会にて承認されました。本決定に伴い、貴社にてご利用いただいております流通 BMS 適合製品/サービスにおけるセキュリティ対応をお願いさせていただきたく、ご案内申し上げます。

記

１．変更点
◎署名アルゴリズムの SHA-1 から SHA-2 への変更
・チェンジリクエストの概要（背景と内容）
SHA-1、SHA-2 とは、ハッシュ関数の種類で、改ざん検知に利用される署名アルゴリズムのことです。SHA-1 と SHA-2 でハッシュ値の長さが異なり、SHA-1 は 160 ビット、SHA-2 は 224 ビット・256 ビット・384 ビット・512 ビットです。ハッシュ値が短いと同一のハッシュ値を持つデータが発見される可能性が高くなり、安全性が低下します。コンピュータの計算能力の向上により、SHA-1 の安全性が危ぶまれるようになったため、よりハッシュ値の長い SHA-2 の利用が推奨されます。
SHA-1 において、衝突の問題は、クラウド リソースを利用した攻撃の可能性が研究されるなど（Marc Stevens, Cryptanalysis of MD5 & SHA-1 ）、現実の脅威として改ざんされた証明書が発生してもおかしくはない状況になってきています。すでに、公的機関などでは、SHA-1 の利用を停止し、より安全なアルゴリズムへ移行することが呼びかけられています。たとえば、米国国立標準技術研究所（NIST）では、2013 年末までに SHA-1 の使用を停止することを勧告しており、日本においても、2013 年頃より、SHA-1 を廃止して SHA-2 への移行を推奨し、SHA-1 廃止に向けた措置（スケジュールを含む）等が公開されています。
この様なセキュリティ技術動向を背景とし、流通ＢＭＳにおける「流通業界共通認証局　証明書ポリシー（ＣＰ）」について改訂をおこない、利用者へセキュリティの高いサービスの提供を規定する事となりました。

ＣＲの詳細については、下記サイトをご確認ください。
http://www.dsri.jp/ryutsu-bms/standard/standard04.html

・検討結果　…　２０１５年１０月１日以降に発行される流通 BMS 証明書から
SHA-1 には対応しない。
・対応方針　…　各流通 BMS 適合製品およびサービスにおける SHA-2 対応
※全お取引先様の SHA-2 対応状況を考慮のうえ、
ご対応をお願い致します。
・具体的な対応　…　クロス期間中は SHA-1/SHA-2 が混在するため、
下記対応をお願い致します。

(1)【全利用者】
10 月 1 日までに現在使用中のルート／中間証明書に加え、認証局各社が新たに発行する SHA-2 に対応したルートおよび中間証明書をシステムに取り込んでください。

(2)【サーバ証明書/クライアント証明書について事前交換を必要としているシステム/サービスをご利用の場合】
接続先と切り替え時期について調整のうえご対応ください。

【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