2018 年 10 月 26 日

ご利用企業各位

ｅ－お菓子ねっと
富士通エフ・アイ・ピー株式会社

[再掲]流通 BMS 通信手順の脆弱性対応について（お願い）

拝啓　貴社益々ご清栄の事とお慶び申し上げます。平素は格別のご高配を賜り、厚くお礼申し上げます。
この度、ｅ－お菓子ねっとでは、セキュリティ強化のため、流通 BMS 通信手順（ebXML、JX）の DES 及び 3DES 暗号の無効化作業を下記の通り実施させていただきます。
ｅ－お菓子ねっとから、『流通 BMS 通信手順の脆弱性対応』の依頼があったご利用企業様につきましては、お手数をお掛け致しますが、下記内容をご確認いただき、ご理解とご協力を賜りたく、何卒宜しく御願い申し上げます。

敬具

記

１．対応内容
ｅ－お菓子ねっとＥＤＩサービスで利用可能な流通 BMS 通信手順（ebXML、JX）において、DES 及び 3DES の暗号の無効化を行い、代わりに、AES（AES256、AES128）の暗号化方式を採用します。この対応に伴い、ご利用の通信ソフトや OS が AES（AES256、AES128）の暗号化方式に対応していない場合、通信が出来なくなります。

２．対応理由
ｅ－お菓子ねっとのＥＤＩサービスで利用可能な流通 BMS 通信手順では、クライアントとサーバ間でデータを暗号化するために、ブロック暗号アルゴリズムを利用しています。暗号化アルゴリズムのデータを分割しているブロックの中で、DES 及び 3DES のブロックサイズは 64 ビットの短いブロックサイズのため、sweet32 の誕生日攻撃の影響を受ける可能性があるため。

３．作業予定日時（環境変更対応日）
2018 年 11 月 1 日(木)　01:00 ～ 03:00
（01:00 ～ 03:00 は、オンラインサービスの時間外となります）

４．対象のご利用企業様
下記条件に該当する場合、通信が出来なくなる等の影響を受けます。
・ｅ－お菓子ねっとのＥＤＩサービスで、流通 BMS 通信手順（ebXML、JX）を利用しているご利用企業様で、通信ソフトや OS が AES（AES256、AES128）の暗号化方式に対応していないご利用企業様
※対象の企業様には、既に個別連絡（Ｅメール送付）しており、原則として事前に検証環境での接続テストを実施いただいております。

５．依頼内容
対象のご利用企業様におかれましては、上記の項番３の「作業予定日時（環境変更対応日）」をご認識いただけますよう、お願いいたします。

（以下次葉）

（前頁より）

６．お問い合わせ、及び、アンケート等の提出先

以下の情報をご記入の上、Ｅメールにてお問い合わせをお願い致します。

・タイトル：ｅ－お菓子ねっと 流通 BMS 通信手順の脆弱性対応

・本文　：取引先コード（代表数字８ 桁）、
御社名、
ご担当者様名、
お電話番号、
お問合わせ内容

・問い合わせ先
：富士通エフ・アイ・ピー（株）ｅ－お菓子ねっと運用サポート

・メール宛先
：fip-edic-eokashi@dl.jp.fujitsu.com

以　上