2018 年 7 月 6 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

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
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

５．依頼内容
対象のご利用企業様は、以下のご対応をお願いします。
－対象の企業様には、本依頼を個別連絡（Ｅメールでのご送付）致します。
（1）事前アンケートの提出
対応内容：「【資料Ａ】事前アンケート」にございます現時点での『暗号化方式の対応状況』と『接続テスト希望日』をご記入、ご回答をお願いします。
提出期限：2018 年 8 月 8 日（水）
提出先　：項番 6 をご参照下さい。
（2）検証環境での接続テスト
対応内容：検証環境における接続テストの実施をお願いします。

テスト時は、「【資料Ｃ】接続テスト手引書」をご参照下さい。

テスト期間：2018 年 7 月 23 日（月）～2018 年 10 月 19 日（金）

※検証環境における接続テストは、アンケートにて「AES（AES256、AES128）の暗号化方式に対応している」とご回答いただいたご利用企業様であっても、可能な限り接続テストを実施いただけますようご協力をお願いします。

※終了時期は、混み合うことが予想されます。9 月 28 日(金)までにテストを終了していただけますよう、ご協力をお願いします。

（3）完了報告の提出

対応内容：テスト完了時に、「【資料Ｂ】完了通知書」をご記入いただき、下記の日時までにご提出をお願いします。

提出期限：2018 年 10 月 19 日（金）

提出先　　：項番６をご参照下さい。

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

富士通エフ・アイ・ピー株式会社　行

【資料A】事前アンケート

下記の現時点での『暗号化方式の対応状況』と『接続テスト希望日』をご記入の上、本資料のご提出をお願いいたします。
ご提出納期は、2018年8月8日（水）までとさせていただきます。

1. 暗号化方式の対応状況

ご利用の通信ソフトが、AES（AES256、AES128）の暗号化方式　に対応しているかどうかを、
通信ソフト提供メーカーのサポートにご確認下さい。

確認結果を以下にご記入下さい。（①～③の中から1つ選び、□の中にチェックしてください。）

□　①AES（AES256、AES128）の暗号化方式に対応している。
□　②AES（AES256、AES128）の暗号化方式に対応していない。
□　③不明

2. 接続テスト希望日

暗号化方式対応後の検証環境を準備しております。
検証環境で、接続テストを実施頂けますようお願いします。
・項番1の回答が②の場合は、暗号化方式対応後に接続テストを行なって下さい。
・項番1の回答が③の場合は、接続テストを必ず行ってください。
・該当する□を1つ選び、□の中にチェックしてください。

□　接続テストを実施する
テスト期間：2018年7月23日（月）～2018年10月19日（金）
終了時期は、混み合うことが予想されます。9月28日(金)までにテストを終了していただけますよう、
ご協力をお願いします。

第一希望日　開始時刻～終了時刻

	月		日		:		～		:	

第二希望日　開始時刻～終了時刻

	月		日		:		～		:	

第三希望日　開始時刻～終了時刻

	月		日		:		～		:	

土・日・祝祭日を除く平日の10：00～17:00までの2時間程度の時間帯をご記入下さい。

□　接続テストを実施しない

理由：

3. ご利用企業様の情報

記入日			年		月		日
取引先コード （代表）							
貴社名							
御担当者様							
連絡先 電話番号							
メールアドレス							
通信欄※							

※テスト担当者が異なる場合や連絡事項などありましたら、通信欄にご記入下さい。

【この連絡票の返信先】

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

富士通エフ・アイ・ピー株式会社　行

【資料A】事前アンケート（別紙）

複数の取引先コードをお持ちのご利用企業様で、取引先コード（代表）以外の
取引先コードにて接続テストをご希望の場合は、以下の記入欄に取引先コードをご記入下さい。

取引先コード記入欄（接続テスト希望）

取引先コード	社名

【この連絡票の返信先】

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

富士通エフ・アイ・ピー㈱　e－お菓子ねっと担当　行
（送信先:fip-edic-eokashi@dl.jp.fujitsu.com）

【資料B】完了報告書

記入日付	2018 年　　月　　日

1. 対応完了日（テスト完了日）

完了日
2018　年　　月　　日

2. ご利用企業様の情報

	ご利用企業様の情報
貴社名	
御担当者様	
連絡先 電話番号	
メールアドレス	
取引先コード （代表）	
通信欄	

接続テストが完了したことを連絡します。

e-お菓子ねっと

FUJITSU
shaping tomorrow with you

流通BMS脆弱性対応

―【資料C】接続テスト手引書―

第1.0版

2018年6月22日

富士通エフ・アイ・ピー株式会社

《 目 次 》

FUJITSU

■接続テスト手引き

１．接続テスト概要

■接続テストの概要は以下の通りです。

（１）目的

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暗号の無効化を行い、代わりにAES（AES256、AES128）の暗号化方式の採用します。
AESを使用してのデータ通信が可能であることを確認するために、接続テストを行います。

（２）テスト実施環境

検証環境

（３）テスト内容

①データ受信テスト
②データ送信テスト

（４）接続テスト可能期間

2018年7月23日（月）～2018年10月19日（金）

終了時期は、混み合うことが予想されます。9月28日(金)までにテストを終了していただけますよう、ご協力をお願いします。

2．事前準備

■接続テスト実施前にしていただきたいご準備は以下の通りです。

（１）データ送信テストを行う場合

・送信用データをご用意ください。

ご用意が難しい場合は、データ受信テストでの実施確認をお願いします（データ送信テストの代わりとして）。

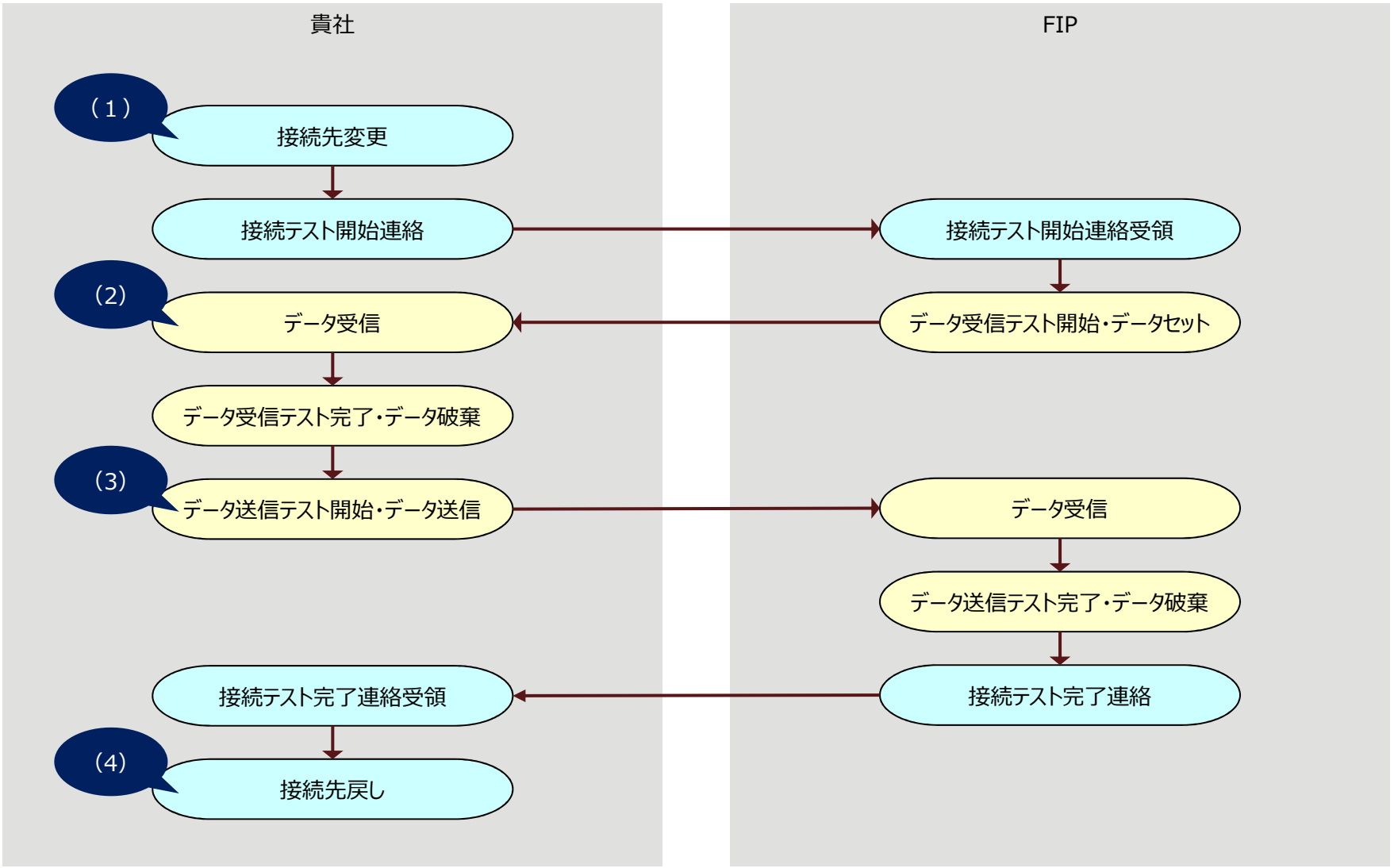
データ受信テストが不可の場合、「5.お問合せ先」にご連絡ください。

（２）データ受信テストを行なう場合

・受信したテストデータは貴社にて処理対象外とし、データ破棄していただけますよう、事前確認をお願いします。

3．当日のテスト手順

■接続テスト当日の手順は以下の通りです。



3．当日のテスト手順

■接続テスト当日の手順は以下の通りです。

（１）接続先の変更

ご利用の通信手順に従い、接続先をセンター本番機からセンター検証機に変更していただきます。

通信手順	変更箇所	変更先（検証機）
JX	接続先URL	https://oskeksbmsbs.tradefront.ne.jp/JX
ebXML	エンドポイントURI	https://oskeksbmscl.tradefront.ne.jp/ebMS/CER

（２）データ受信テスト

FIPがデータをセットし、貴社に受信していただくテストです。

－JXの場合、貴社からセンターへデータを取りに来ていただきます。

－ebXMLの場合、センター（FIP）から貴社へデータを送信します。

通信結果が正常であればテスト完了となります。受信したテストデータは貴社にて処理対象外とし、データ破棄をお願いします。

異常の場合は、後日日程を調整の上、再テストを行います。

・複数のデータ種を利用している場合、いずれか１データ種のみテストします。

・利用しているデータ種が無い場合、データ受信テストは不要です。

・テストデータは、データ種に関わらず発注データを使用します。

・通信がうまく行かない場合は、「5.お問合せ先」にご連絡下さい。

3．当日のテスト手順

■接続テスト当日の手順は以下の通りです。

（3）データ送信テスト

ご用意いただいたデータを貴社から送信していただき、FIPが受信するテストです。
通信結果が正常であればテスト完了となります。テストデータはFIPで処理せず、破棄いたします。
異常の場合は、後日日程を調整の上、再テストを行います。

・複数のデータ種を利用している場合、いずれか１データ種のみテストします。
・利用しているデータ種が無い場合、データ送信テストは不要です。
・テストデータは、ご準備いただいたデータをご使用ください。
・通信がうまく行かない場合は、「5.お問合せ先」にご連絡下さい。

（4）接続先の戻し

ご利用の通信手順に従い、接続先をセンター検証機からセンター本番機に変更していただきます。

通信手順	変更箇所	変更先（本番機）
JX	接続先URL	https://eksbmsbs.tradefront.ne.jp/JX
ebXML	エンドポイントURI	https://eksbmscl.tradefront.ne.jp/ebMS/CER

４．テスト完了後

■テスト完了後の手順は以下の通りです。

・お渡ししたテスト完了報告書の必要項目にご記入いただき、
「5.お問合せ先」記載のメールアドレスへお送りください。

５．お問合せ先

■接続テストに関する技術・運用・テスト面に関するサポート窓口、お問合せ方法は以下の通りです。

お問合せ先

ＥＤＩサービスセンタ

e-お菓子ねっと 担当者宛（９：００～１７:００　土・日・祝祭日を除く）

電話番号　　：０４４－７５２－９２１２

メールアドレス　　：fip-edic-eokashi@dl.jp.fujitsu.com

お問合せ時の必要情報

案件名：e-お菓子ねっと　流通BMS脆弱性対応の接続テスト

お客様情報

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

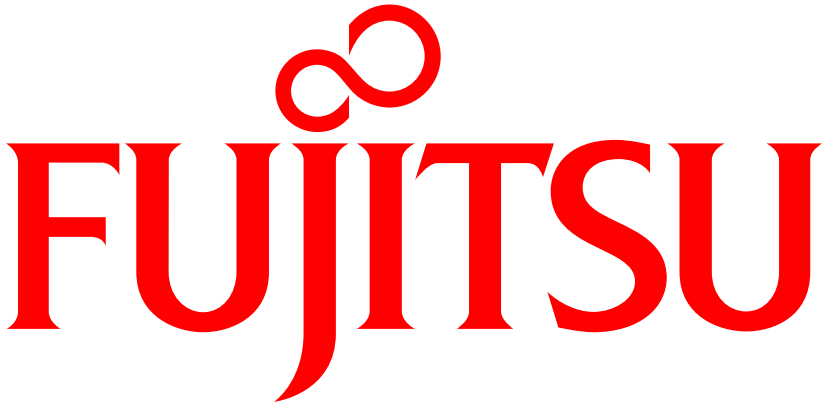
お問合せ方法

－電話でのお問い合わせ時は、案件名、お客様情報をお知らせください。

－メールでのお問合せ時は、案件名をメールタイトルにご指定いただき、お客様情報を本文にご記入下さい。

更新履歴

版数	更新日	更新概要
1.0	2018.06.22	初版作成



shaping tomorrow with you