# 第３回クレジットカード決済システムのセキュリティ対策強化検討会
# 議事要旨

日時：令和４年１０月１１日（火）１４時００分～１６時００分

場所：オンライン会議（Teams）

出席委員：
中川座長、池本委員、大河内委員、大野委員、小川委員、篠委員、二村委員、長谷川委員、松尾委員、三浦委員、森竹委員
※オブザーバー、プレゼンターについては構成員名簿を参照

議題：
１．開会
２．議事
（１）クレジットカード番号等の不正利用対策
３．閉会

議事概要：
■クレジット取引セキュリティ対策協議会より資料３に基づき、株式会社メルカリより資料４に基づき、株式会社髙島屋より資料５に基づき、説明。
■事務局より、資料２に基づき、クレジットカード番号等不正利用対策の強化について御議論いただきたい論点を提示した後、委員による討議を実施。

討議：
EC 加盟店での不正利用防止対策に係る総論
・不正利用対策は、消費者の安心・安全な決済環境の提供という観点だけでなく、犯罪者集団が犯罪収益を得ているという観点からも国が対策を進める必要がある。本来、カード入会時に本人確認を経ているはずが、不正利用で誰が使っているか不明となると、犯収法の基本構造から逸脱することとなり、AML 等の観点からも不正利用対策は重要事項。よって、国の対策が必要であり、各プレーヤーも対策を義務づけられることにつながっていくのだろう。

１．加盟店側での対応
１－１．「利用者であることの適切な確認」の手法の高度化
・カード会社が利用者であることの適切な確認の手法として、カード業界が統一的に推進する対策として、現在有力な手法である EMV-3DS を主眼に進めるべき。原則としてすべての加盟店に導入を求めていく方向に賛成。
・加盟店での EMV3DS 導入に関する効果について、新規導入された２社の事例では効果が非常に顕著であった。

・EC 加盟店側で高度な個人認証を入れていくということは効果が高いということを周知すべき。広めていくために、非保持化の際と同様に、一定の法制による義務化・制度化が必要ではないかと認識。
・導入について法制的に対応しないと、諸外国との比較で日本市場が狙い撃ちになる。その結果、犯罪、マネロンの温床になるという点でも深刻な問題になるのではないか。かご落ちリスクを考えると、当たり前化で導入することが重要。総合的に考えると法的に義務化することには異論がなかった。
・将来的には、クレジットカード番号 16 桁ではないトークナイゼーションがどのように使い得るのか、課題が何かについて、検討課題として視野に入れておくべきではないか。
・EMV3DS の義務付けについては一定の例外もあるべきではないか。PSP では加盟店に対して EMV3DS 以外の個別の不正利用対策ソリューションも提供しており、EMV3DS 同様に認めていくべきではないか。

１－２．EMV 3DS の導入に向けて
・アカウントとクレジットカード番号等の紐付け時の EMV3DS は効果的ではないか。
・アカウントとクレジットカード番号等が紐付いている場合、紐付けの時の高度な本人認証と決済時のリスクベース認証をあわせて検討すべき。決済時でも OS や接続場所、行動時間等からリスクを検知し得る。
・紐付けされている場合、個別決済での認証はリスクベース判定で行うことがよいのではないか。
・一方、取引都度の EMV3DS 認証をしない場合は、加盟店はチャージバックのライアビリティが効かないことに留意すべき。
・加盟店はログイン周りの入口対策に重きをおくとよいのではないか。
・現行の不正利用対策として掲げてある４つの方策には古いものも新しいものも入っているように見える。EMV3DS の導入促進を前提として義務化した場合、EMV3DS の普及が前提となるので、不正利用防止の４つの方策の整理が必要。セキュリティ対策協議会でも検討中。
・EMV3DS だけでなく、加盟店が独自に導入する不正防止対策についても、有効である施策は認められるべき。加盟店の対策が不十分な場合は EMV3DS に移行すべきではないか。
・EMV3DS を導入しても不正利用が止まらない場合は、他の手段も含めた重層的な対策が必要。
・セキュリティサイト対策をしているサイトとそうでないサイトが見分けにくい。サイトのトップページに対策の有無を表記してほしい。
・パスワードを使い回しているケースがあるが、漏えいにより、意図せず不正利用される事例もある。静的パスワードでの EMV3DS の義務化はリスクがある。
・カード決済時にすべての取引にワンタイムパスワードの入力を求めてほしい。カード名義人と加盟店での申込者名義人が異なる場合は、必ずワンタイムパスワードを求めるべきではないか。

１－３．不正利用防止義務とした時の EMV-3DS の導入時期等
・不正利用対策の導入が進む海外と比較すると、導入がまだで円安の日本は不正利用被害の狙い目のマーケットになってきて、非常に危険な状態になってくる。２、３年のうちには導入を進める必要があるが、件数と取扱商材等の定量的・定性的な判定をリスクベースで考えながら順次段階的に実施するのが現実的ではないか。
・時期としては早急に進めるが、一定の期日を目標として進めていくべきではないか。

・導入具合がばらばらだと導入されていない加盟店が狙われてしまう、またかご落ちリスクも高まるので、可能な限り一斉に義務づけをしてくことが望ましい。
・全ての加盟店に導入していくうえでも、システム面、コスト面の課題があるので、段階的な導入が望ましい。
・当面の対応として、新規加盟店にはチェックリストを出されるのであれば、既存の加盟店にも更新のタイミングで効くのではないか。取引規模が大きいところは、優先的に早めに導入してもらうことがよいのではないか。
・かご落ちの問題の捉え方として、EMV3DS の技術的なレベルが向上して、パスワードを求めるブランドの画面が改良されると、一定程度かごオチへの影響は小さくなるのではないか。
・今 3DS が導入されている分野は旅行系や電子マネー、ゲームサイトなどであり、3DS の体験自体、よく使う人は知っているが、使わない人は全く知らないというマイナーな体験になっている。業界全体として導入を進めると、かご落ちの話も減るとみてよいのではないか。

・EMV3DS 導入の費用について、特に中小規模のサイトの場合は投資負担が明らかになると浸透しやすいのではないか。
・個別に EC サイトを運営している加盟店は PSP が提供する EMV3DS 対応のモジュールを導入していく必要がある。ほとんどの会社が外部のベンダーにお願いしていると思うが、初期のシステム導入コストが障壁であり、普及の鍵であると認識。
・導入経費は EC 加盟店のシステムの構成による。中小の EC 加盟店の場合は PSP のシステムを利用していることが多いので、投資という面では PSP の投資の方が大規模。EC 加盟店側でも接続のためのアプリの投入経費は一定程度かかるだろうが、その規模は PSP のシステムによる。
・自社の事例では、自社内にエンジニアを内製しているため、外部に支払う開発コストは大きくならなかった。一般的には中小の EC 加盟店は決済代行会社が導入する者を使えるため、開発コストというより、決済量が多いほど手数料の負担が増えるのではないか。
・通販業界では、特商法改正やインボイス制度の対応で既に負担が大きい状況。なるべく低コストで済むと良い。

２．PSP（EC モール等）での対応
２－１．PSP や EC モール等の対応
・加盟店への法的な義務付けの時には PSP への義務付けも明確にして健全な競争環境の整備を図るべき。
・EC モールでの決済の市場シェアが高いことを考えれば、EC モールも協力すべき。
・当初は、求めるレベルより高いレベルでのセキュリティ対策であれば EMV3DS の例外があっても良いのではないかと考えていたが、やはり消費者への啓発の観点からは、EMV3DS 対応の義務付けは望ましいと考える。

３．イシュアー側での対応
３－１．「利用者であることの適切な確認」の確認主体
・イシュアーが本人認証をするのがあるべき姿。
・現状では、まだ全てのイシュアーが EMV3DS に対応し切れているわけではない。JCA のアンケートによると、大手、中堅のイシュアーは EMV3DS に対応済みだが、一部小規模のイシュアーでは未

対応。ACS サーバ側での準備が整い次第参加したいと聞いている。早いうちに全てのイシュアーは EMV-3DS に対応できるという認識。
・イシュアー側での EMV3DS はかなり対応が進んでいるが、利用者のパスワード登録が追いついていないという印象。動的パスワードの登録率を上げていかないと、不正利用されることから、不正対策上必要。
・利用者がパスワード未設定の場合、イシュアー側が登録を促すべきではないか。
・利用者へのパスワード登録は、イシュアーが 3D セキュアのためだけでなく、自社の web 関連サービスの利用にあたり登録を呼びかけるケースが多く、イシュアー毎に進めているため、各者の web サービスの充実度・進捗度合いによりばらつきがある。今後全ての加盟店に EMV3DS を導入していくことを踏まえ、業界一丸となって取組を進めるべき。
・国際ブランドの提供する EMV3DS のサービスの課題は、加盟店の意見を吸い上げてイシュアーから国際ブランドへ提示してほしい。
・相談現場の感覚では、９割もの利用者が利用明細を確認しているように感じない。決済後に決済の完了メールを利用者に送ってほしい。
・スマホアプリの利用は、直接顧客と会社がつながる通信手段となり、既に銀行でも取り組まれており、望ましい。特にスマホでの認証は生体認証も利用できるため非常に望ましい。利用明細の確認が行いやすくなり被害の認知として気付きやすくなる他、フィッシング対策という点でも企業のアプリ利用は効果が期待できるのではないか。
・マイページのアクセス履歴がないときは確認のメールを聞いてはどうか。

３－２．EMV3DS のリスクベース認証の精度
・リスクベース認証でのイシュアー間等のリスク情報の共有は必要ではないか。
・EMV3DS を導入したが、イシュアーで加盟店からのアプリ経由の情報をすべて受け取れていないためかチャレンジが多い、あるいは EMV3DS 認証後にオーソリでエラーが起きることもあり、イシュアーでリスクベース認証がきちんとできているか疑問。
・EMV3DS のトランザクション数がまだ少なく、イシュアーとして分析が不十分な面もある。イシュアーによってリスクベース認証の精度はばらつきがあるため、イシュアー側のレベルを上げる対策をあげることが急務。

３－３．リスクベース認証の効果の確認
・EMV3DS の取引の大半がリスクベース認証であり、その効果検証は当然必要になってくる。
・高リスクと判定した決済のうち、どのくらいが遮断されたのか／実は正当なものだったのか、ローリスクと判定した決済が実は不正利用のものだったかという情報を、イシュアーによるリスク評価の精度を監督官庁に情報提供し、監督官庁はリスク評価の精度を確認・モニタリングできるようにする形が必要。

３－４．不正利用情報の共有
・不正利用情報の共有化や判断基準についても、イシュアー間で共有するといった連携が重要なことと考える。