資料３

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

報告書（案）

２０２３年１月２０日

目次

はじめに

電子商取引及びキャッシュレス決済の普及に伴い、クレジットカード決済市場の規模は継続的に増加している。一方、サイバー攻撃の増加等を背景に、クレジットカードの不正利用被害額が増加しており、2021 年には、不正利用被害額は過去最高の約 330 億円となった。また、クレジットカード決済機能の分化により多様なプレイヤーがクレジットカード決済網に関与していく傾向にある。2025 年に向けて、政府としてキャッシュレス決済の拡大を目指している中、これらの状況に鑑み、安全・安心なクレジット決済を確保するための在り方の再考が求められている。

産業構造審議会商務流通情報分科会第 30 回割賦販売小委員会（2022 年６月２日）では、クレジットカード業界をめぐる課題として、セキュリティ対策については優先して取り組んでいくべき課題と示された。

クレジットカード業界では、これまでにもクレジットカード・セキュリティガイドライン」を毎年改訂し、クレジットカード取引の関係事業者が実施すべきセキュリティ対策を示し、その実行を推進してきたところである。しかしながら、サイバー攻撃等のセキュリティリスクが年々高まり、実際に不正利用被害額も増加している現状に鑑み、国としては、業界の取組に加え、更に追加的な対策の実行を促進すべく、「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」を立ち上げた。本検討会（2022 年８月～2023 年１月）では、割賦販売小委員会で報告された「クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性」を踏まえ、（１）クレジットカード番号等を安全に管理する（漏えい防止)、（２）クレジットカード番号等を不正に利用させない（不正利用防止)、（３）クレジットの安全・安心な利用に関する周知・犯罪の抑止の３本柱に沿って、技術的な観点も含め、より詳細な検討が行われた。

本提言は、本検討会での議論を踏まえ、クレジットカード決済のセキュリティ対策強化に向けた具体的な取組と今後の課題について取りまとめたものである。

第１章　クレジットカード決済システムをめぐる環境

１．クレジットカード決済システムをとりまく環境

（イ）クレジットカード決済システムをとりまく環境

我が国では、2025 年６月までに、キャッシュレス決済比率を倍増し、４割程度とすることを目指す（成長戦略フォローアップ(令和元年６月 21 日閣議決定)）こととしているが、2021 年には 32.5%に達しており、今後も引き続き増加することが見込まれている。このキャッシュレス決済のうち、2021 年においてはクレジットカードの取引が約９割を占めている（約 85%)。また、社会のデジタル化・新型コロナウィルス禍を受けた巣ごもり需要の拡大等により、電子商取引が伸張し、2021 年の EC の市場規模は約 21 兆円にまで拡大している。これらに伴い、EC サイトでの非対面取引における主要な決済手段としてクレジットカードが利用される機会も増加している。

一方、サイバー攻撃の手法の変化、消費者のオンラインツールの利用機会の増加等により、クレジットカード番号等の不正利用を招く原因となる手法についても、巧妙化しているものの、その手法自体は一定程度定型化しており、それぞれのプレイヤーが講じるべき対策が見えてきた状況になりつつあると考えられる。決済インフラとしての持続可能性を維持するためにも対策の実行や強化が喫緊の課題である。

（ロ）非対面取引におけるクレジットカード決済の取引の仕組み

クレジットカード決済は、クレジットカード会社による利用者に対するクレジットカード番号等の付与、加盟店に対するクレジットカード取引の許諾により可能となっており、これがクレジットカード取引の基本的構造である。しかし、EC サイト自体の増加や EC サイトでのクレジットカード決済の利用の拡大等に伴い、クレジットカード決済の取引構造において、対面取引と非対面取引[1]でのクレジットカード決済の取引の仕組みの差異が顕著となってきたように見受けられる。

対面取引では、アクワイアラーを通じて供給される決済端末等を設置し、アクワイアラーに接続する。通常、当該端末は、既に PCI SSC が定める基準に準拠した仕様で大手メーカーにより製造・販売されており、加盟店では当該端末を設置・接続さえすれば、クレジットカード番号等を加盟店から分離して処理し、クレジットカード決済が可能となるほか、複数のアクワイアラー等にクレジットカード番号等を仕分けることもできるため、保守も含め特段の対応は不要となる。クレジットカード決済の仕組みは、従前、こうした対面取引を前提に構築され、アクワイアラーは加盟店での当該端末の設置の有無を確認し、クレジットカード決済機能を把握することで、セキュリティ面を含めた加盟店管理を直接行い易い構造となっていた。

一方、非対面取引では、EC 加盟店は、自社で EC サイトや決済環境の構築が必要ではなく独自のカスタマイズができない設定となっているような EC モールを利用した構築パターン[2]を選ばない限りは、インターネット環境下で、各 EC サイトが選択した構築パターン[3]のなかにクレジット

---

[1] 本報告書では、加盟店が EC サイト上で販売及びクレジットカード決済を行っている場合の取引を対象としている。

[2] EC サイトのコンテンツ自体も第三者となる EC モールのサービスを利用するサービス利用型の構築パターンの１つ。

[3] 自社構築型（決済モジュール以外すべてを自前で構築するスクラッチ型、EC サイトの構築自体は汎用的なパッ

カード決済のモジュールを埋め込むカスタマイズを行い、インターネット回線を通じてPSP[4]に接続し、PSPがアクワイアラーに専用線で接続するため、アクワイアラーとの接続は間接的となる。また、カスタマイズを行う過程では、EC加盟店自身ではECサイト等の構築・設定ができない場合や自身より優れたカスタマイズを提供する事業者を利用したい場合には、加盟店のECサイト上でクレジットカード決済を行うためのシステムやサービスを提供する事業者や、ECサイトとクレジットカード決済の利用が可能なプラットフォームを構築する事業者などEC加盟店のニーズに応じたクレジットカード決済サービスを提供する多様な事業者のサービスを利用するようになっており、EC加盟店となる参入障壁が低くなっている。

クレジットカード決済のモジュール自体には特段のセキュリティの基準はないほか、その埋め込みはECサイトに任されているところ、PSPでクレジットカード番号等が保存等されていたとしても、クレジットカード番号等をPSPに送信させる決済モジュールを組み込んだECサイトに対する保守も含めたセキュリティ対策はEC加盟店自らが継続的に対応する必要がある。アクワイアラーにとっては、EC加盟店でのクレジットカード決済処理や環境を直接把握することは困難であり、事業者としてのセキュリティ体制や方針を確認することにならざるを得ない。EC加盟店にとっても、立替払いやアクワイアラーへの決済システムの接続だけでなく、複数のアクワイアラー等にクレジットカード番号を仕分けてくれるPSPは必要不可欠な存在となっており、機能分化と業務の専門性が深化してきている。非対面取引でのクレジットカード決済の仕組みにおいては、アクワイアラーとしてのクレジットカード会社がすべてのEC加盟店と直接かつ日常的な接点を有する状況にはなく、EC加盟店とアクワイアラーの間に介在し、EC加盟店とクレジットカード決済システムやサービス提供に係る契約を締結しているPSPが実務的な加盟店管理を実施している場合が多い。

２．クレジットカード決済のセキュリティ対策の経緯

クレジットカード決済のセキュリティ対策自体は、2000 年前後の偽造カードによるクレジットカード番号等の盗用への対策に向けて、クレジットカード業界や全国クレジットカード犯罪対策連絡協議会の一丸となっての対応や、偽造カード不正作出の罰則化等により、一時はクレジットカードの不正利用被害額の水準も低くなっていた。

平成 20 年割賦販売法改正では、イシュアー（委託先含む）等の従業員の持ち出し等によるクレジットカード番号等の漏えい事案の発生を踏まえ、大量のクレジットカード番号等を取り扱う事業者の漏えいに対する懸念から、イシュアー・アクワイアラー（立替払取次業者）に対してクレジットカード番号等の適切管理の措置が求められた。また、インターネット取引等の規制強化として、フィッシングを含む不正アクセスによるクレジットカード番号等の不正取得について罰則の対象とした。2010 年代半ば以降、当該罰則化のほか業界での一部の事業者による決済端末の IC 対応の自主的な取組により、偽造カードによる不正利用が減少してきたのとは対象的に、番号盗用による不正利用が増加してきた。

ケージを利用するパッケージ利用型）やサービス利用型（ECサイトのコンテンツは自前で構築するもののECサイトアプリは第三者サービスを利用するASP/SaaS）がある。

[4] 本報告書において、PSPとは、決済代行業者のほかECモール等「インターネット上の取引において、EC加盟店にクレジットカード決済スキームを提供し、カード情報を処理する事業者」としている。

このような状況の中、クレジットカード業界においては、クレジットカード取引の IC 化が既に国際水準の偽造対策として普及していたこと及び不正利用額が再び増加してきたことを踏まえ、業界の自主的な取組を推進すべく、2015 年３月、我が国のクレジットカード取引において、「国際水準のセキュリティ環境」を整備することを目的として、クレジット取引に関わる幅広い事業者及び行政等が参画する「クレジット取引セキュリティ対策協議会」を設立し、2020 年３月までに関係事業者が実施するべきセキュリティ対策を定めた「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」（2016 年２月～2019 年３月）を策定してきた。

一方、国としては、平成 20 年割賦販売法改正後も加盟店からのクレジットカード番号等の漏えい、偽造カードやなりすましによる不正利用の増加に歯止めがかからないこと、国際的にクレジットカード取引の IC 化等のセキュリティ対策が進展している中、国内のクレジットカード決済環境が脆弱性を有した状態であることは、我が国がセキュリティホール化するリスクが高まることから、平成 28 年割賦販売法改正では、クレジットカード番号等の適切管理義務主体者を加盟店にも拡大し、加盟店に対して不正利用防止義務を課すとともに、これら義務に基づく措置の実務上の指針として実行計画を位置づけた。具体的には、加盟店に対して、クレジットカード番号等の非保持を推奨し、非保持化している場合は PCI DSS 準拠は求めていない。また不正利用防止措置として、対面取引を行う加盟店に対しては、IC カードと暗証番号の入力によりクレジットカード会員本人の利用であることの確認を行うことができるよう決済端末の IC 対応を求めた。これにより、偽造カードによる不正利用被害は大きく減少した。一方、非対面取引を行う加盟店に対しては、必ずしも単一の対策で不正利用を防止することができるものではないため、不正利用リスクに応じて多面的・重層的な措置を講じることを求めた。このため、クレジットカード会員本人の利用を確認するための対策は、事業者の業種や取扱商材等に応じて不正利用リスクの高い EC 加盟店が任意に選択できる対策の一つであり、すべての EC 加盟店に対して実施を求めてはいなかった（すべての EC 加盟店共通では、各イシュアーのオーソリゼーション処理（クレジットカードの有効性確認）の体制整備及び加盟店契約上の善良なる管理者の注意を求めていた）。

また、同改正により、認定割賦販売協会（一般社団法人日本クレジット協会）の業務に「クレジットカード番号等の適切な管理等に資する業務」が追加され、同協会は当該実行計画の策定のための支援や加盟事業者に対するセキュリティ対策の指導等を法定業務として実施することとなった。また、同実行計画は 2020 年３月末を対応期限としていたところ、2020 年４月以降は、「クレジットカード・セキュリティガイドライン」（2020 年３月～。最新の 3.0 版は 2022 年３月）として策定され、毎年改訂されている。

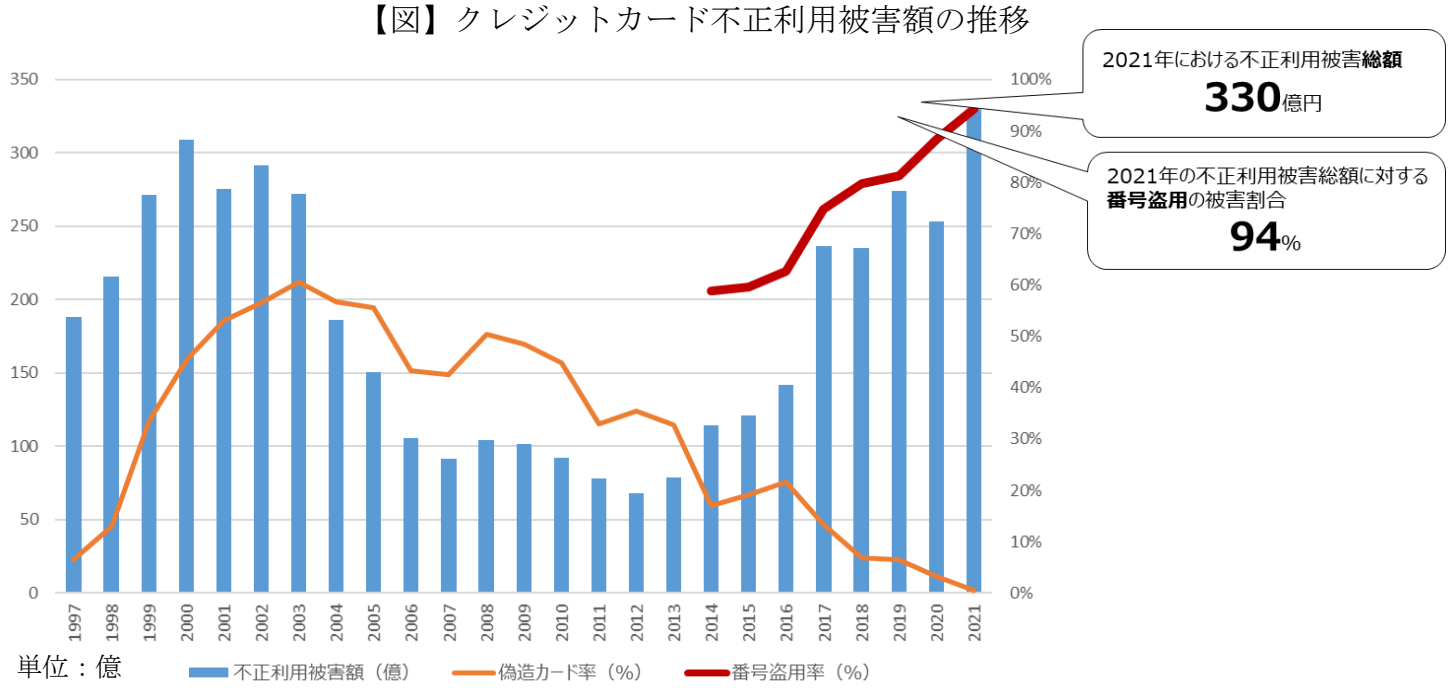
令和２年割賦販売法改正では、ICT の進展に伴い、決済テクノロジーが進化するなか、決済システムにおいて、イシュアー・アクワイアラー・加盟店以外にも大量のクレジットカード番号等を取り扱う事業者が現れ、大規模なクレジットカード番号等の漏えい事案の発生リスクが高まったことから、クレジットカード番号等の適切管理義務の主体を、EC モールを含む PSP や QR コード決済事業者、EC 決済システム提供業者等まで拡大した。

３．クレジットカードの不正利用の現況

我が国のクレジットカードの不正利用被害総額は近年増加傾向にあり、2021 年には過去最高となり、330 億円を超えた（【図】参照）。このうち、クレジットカード番号等の盗用の割合が 94%

を占めており、主に非対面取引でのクレジットカード番号等のなりすましによる不正利用が主要な要因である。これらの不正利用の対象となっているクレジットカード番号等は、EC 加盟店を始めとしたクレジットカード決済網に存在する事業者からの漏えいだけでなく、EC 加盟店のクレジットカード決済処理の仕組みを悪用してクレジットカード番号等を割り出すクレジットマスター、電子メールや SMS 等を通じて利用者からクレジットカード番号等を騙しとるフィッシングにより詐取されていると想定されている。

【図】クレジットカード不正利用被害額の推移



（出典）クレジットカード不正利用被害額の発生状況（2022 年３月　日本クレジット協会）より事務局作成

不正利用の対象となる取引のほとんどが非対面取引であり、換金性があり転売しやすい商品や配送を伴わない商品が不正利用の標的となっていたが、昨今では、その時々の商品の需要の状況によって不正利用で購入される商品が変化することから、不正利用の対象となる商品は多様化し、また比較的低価格な商品の不正利用も増えてきている。

第２章　基本的考え

本検討会では、非対面取引における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に向け、（１）クレジットカード番号等を安全に管理する（漏えい防止）、（２）クレジットカード番号等を不正に利用させない（不正利用防止）、（３）クレジットの安全・安心な利用に関する周知・犯罪の抑止の３つの方向性に向けて、具体的な対策について検討を行ってきた。

その結果、本検討会の議論として、①まずは、現行法の規制の範囲内で、技術的なアップデートをすること、②現行法の規制の在り方そのもののアップデートを今後考えるべきことの課題に整理された。規制の在り方そのものを考えるにあたり、クレジットカードが国民生活の決済インフラの役割を担っていることを踏まえ、セキュリティ対策は消費者利益の根幹としての責務であることを前提にしたうえで、消費者の利便性も念頭においた消費者利益の保護の観点と、クレジットカード決済システムの信頼性確保の観点の２つの観点を意識しながら検討する必要性がある。

また、今般、これらの対策を検討していく過程で、クレジットカード決済システムの対策を強化していくうえでは、以下の意識をもって臨むことが肝要である。

〇クレジットカード決済網の全プレイヤーによる実効的な対応

クレジットカード決済は今や経済活動の重要インフラとなっている。クレジットカード会社やPSP の供給側のセキュリティはもとより、これらをビジネスとして利用する EC 加盟店、EC モール等も、重要インフラを担うクレジットカード決済網のプレイヤーとして、的確なセキュリティ対策をビジネスの根幹として捉える必要がある。クレジットカード被害の実額の損失を事業者が負担することにより、利用者に経済的被害を生じさせなければよいというものではなく、不正利用そのものの未然防止を図ることを目的として、全てのプレイヤーのセキュリティ対策のレベルを上げていくための実行が不可欠である。

〇セキュリティ対策を継続する責任とボーダーレスなサイバー攻撃への対応

セキュリティの情報・サイバー攻撃は日々刻々と進化するものである。ボーダーレスなインターネット環境において自由なビジネスを行うためには、継続的な情報収集とセキュリティ対策を行う責任が伴うことを自覚する必要がある。クレジットカード決済システムは多数の事業者のネットワークによって成立しているだけでなく、非対面取引はインターネットを通じて世界中で使える利便性がある一方、サイバー攻撃等もボーダーレス化しており、セキュリティリスクも高まっている。こういった状況において、クレジットカード番号等を直接保持（保存・処理・通過）しているプレイヤーだけでなく、インターネットを介してクレジット決済を可能にするネットワークに接続するプレイヤーには常にサイバー攻撃のリスクが存在しているものと認識し、セキュリティ対策を継続的に実施する責任がある。既知の脆弱性を悪用するサイバー攻撃は未然防止が可能であり、的確に対処することが肝要である。また、国もグローバルなサイバー攻撃の蓋然性も踏まえたセキュリティ対策を打つために、国際ブランドから定期的にその有する知見や情報の提供を受ける仕組みを構築するなどして、グローバルな状況を踏まえた対策を継続的に検討する等国内の対策レベルを引き上げることが必要である。

○利用者目線での対応

情報化社会においては、瞬時に利用者間で情報が共有されるが、特にインシデントに関連する情報は、憶測レベルの不正確な情報であっても拡散され不安が広がりやすい。インシデントが発生した際の利用者への情報提供は、無用な混乱を招かないために確定した情報を提供することも大切であるが、利用者が今後発生し得る不利益に対する防御の取組を行うことができるよう適時適切にインシデントの状況を情報提供することも重要である。また、利用者に対する情報提供が遅れ、クレジットカード取引に対する不信感が生じ、ひいてはクレジットカード決済システムの信頼性を低下させることにもなりかねない。したがって、インシデント発生時の情報提供は、利用者目線に立ち、随時的確な情報提供を行うことも求められる点に留意が必要である。

○データに基づく状況の把握

これまで、クレジットカード業界において不正利用の総額については把握されてきたものの、不正利用の対象となっている加盟店や商材、不正利用に使われたクレジットカード番号等の漏えい原因等の詳細な分析は実施していない。状況の変化が激しくなってきているサイバー攻撃や不正利用に対して、実効的なセキュリティ対策を検証し、実施していくうえでは、クレジットカード番号等の漏えいや不正利用の状況について、より詳細に状況を分析し、発生原因に適した効率的な対策を行っていくことが必要である。国は、適確なセキュリティ対策の実施及び不正利用被害の減少を目的とした監督を行うにあたり、対策の検討に必要なデータを持つ当事者から状況を把握し、適切な行政上の措置を講ずるとともに、対策の随時の見直しにより、クレジットカード決済システムの信頼性を確保していくことが重要である。

第３章　３つの方向性について

第１節の１．クレジットカード番号等の適切管理の強化

○位置づけ

クレジットカード番号等の不正利用に悪用されるクレジットカード番号等の漏えい原因の１つとされるのは、クレジットカード決済網の事業者からの漏えいである。その漏えい対策となるクレジットカード番号等の適切管理は、クレジットカード決済システムの信頼性を確保するため、同システムに携わるすべての事業者による責務であり、クレジットカード番号等の不正利用の未然防止に直接寄与するものである。今回は、事案の増加から、特にサイバー攻撃により事業者からクレジットカード番号等が漏えいするものを対象としている。

１．加盟店での漏えい対策の強化

（イ）EC 加盟店側での対応

割賦販売法では、平成 28 年改正により、EC 加盟店に対し、クレジットカード番号等の漏えい対策として、クレジットカード番号等の適切管理義務（法第 35 条の 16）を課している。また、アクワイアラー等[5]による加盟店管理の対象項目に、クレジットカード番号等の漏えい防止の措置状況を挙げている（法第 35 条の 17 の８）。当該防止措置の法的水準としては、「クレジットカード・セキュリティガイドライン（以下「ガイドライン」という。）」により示された、クレジットカード情報を保持しない非保持化[6](非保持と同等/相当を含む)若しくはクレジットカード情報を保持する場合は PCI DSS[7]準拠の措置、又はそれらと同等以上の措置を求めた。多くの EC 加盟店が漏えい対策として非保持化を選択したことにより、EC 加盟店が保持しているクレジットカード番号等の漏えい被害は極小化し、１事案あたりのクレジットカード番号等の漏えい件数は減少した。一方、従前の EC サイトの保存サーバーに蓄積されていたクレジットカード番号等を窃取していた手法から、非保持化だけでは防止することができない EC サイトのコンテンツを改ざんする手法への変化により、クレジットカード番号等を不正に窃取するクレジットカード番号等の漏えい事案は増加傾向にある。EC 加盟店での漏えい事案の多くは、オープンソースソフトウェア（OSS）を利用し、自社や委託先において適切な設定、ソフトウェアのアップデートや既知の脆弱性対策を実施しないなど十分なセキュリティ対策を講じていない EC サイトを狙った不正アクセス等による漏えい事案であり、国からも注意喚起（2019 年）がされている[8]が、増加している。OSS の利用をしていない EC 加盟店でも漏えい事案は存在しており、漏えい対策は OSS の利用の有無にかかわらず、非保持化による対

---

[5] 本報告書では、「アクワイアラー等」は、法第 35 条の 17 の２に規定するクレジットカード番号等取扱契約締結事業者である、いわゆるアクワイアラー・PSP の一部を想定している。

[6] 非保持化とは、自社で保有する機器・ネットワークで非処理・非保存・非通過の３要件をすべて満たした状態である。

[7] PCI DSS とは、Payment Card Industry Data Security Standard の略。カード情報を取り扱う全ての事業者に対して国際ブランド（VISA、Mastercard、JCB、American Express、Discover）が共同で策定したデータセキュリティの国際基準。安全なネットワークの構築やカード会員データの保護等、12 の要件に基づいて約 400 の要求事項から構成されており、「準拠」とは、このうち該当する要求事項に全て対応できていることをいう。PCI DSS 準拠の検証方法としては、①オンサイトレビュー（認定セキュリティ評価機関（QSA）による訪問審査）又は②自己問診（SAQ、自己評価によって PCI DSS 準拠の度合いを評価し、報告することができるツール）による方法がある。

[8] 株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について（注意喚起）（2022 年 12 月 20 日経済産業省） https://www.meti.go.jp/press/2019/12/20191220013/20191220013.html

策だけでは不十分であり、更なる漏えい対策が必要である。

（１－１）EC 加盟店における対策の実効性の確保

昨今のクレジットカード番号等の漏えい事案では、EC サイトの設定不備や既知の脆弱性の悪用事案が多いことから、クレジットカード決済網に参入する EC 加盟店は、非保持化等の漏えい対策に加え、EC サイトの脆弱性対策を実施していることが必須である。また、セキュリティ対策は常に適切にアップデートする必要があることから、特に EC システムの導入やサイト構築の時点だけでなく、運用開始後も EC 加盟店自らがセキュリティ対策の実施状況を適時適切に確認する運用も重要である。

昨今の漏えい事案の増加及び非対面取引でのクレジットカード決済の利用の広がりを踏まえ、今後、EC 加盟店に対し、クレジットカード番号等を適切に管理すべき内容として、非保持化か否かにかかわらず、その前提となる EC サイト自体の脆弱性対策について自ら責任をもって対応することを求めていくべきである。

EC 加盟店では、セキュリティ対策を外部の事業者に委託し、自らが EC サイトのセキュリティ対策の実施、管理を行っていないケースも多くあることから、セキュリティリテラシーが低い EC 加盟店も多く、自主的な取組のみでは実効性を確保することは困難と考えられる。EC 加盟店における対策の実効性の確保に向けて、クレジットカード番号等の適切管理義務の主体者としてすべての EC 加盟店が公平・平等に守るべき義務とすることが適切である。また、不正アクセスの手段は変化している一方、EC 加盟店での非保持化以外の対応の必要性を認知しておらず、これらの攻撃の狙いは EC サイトの脆弱性であるところ、すべての EC 加盟店が既知の脆弱性対策を実施することで漏えい防止の効果が期待できる。このため、EC 加盟店に対して、クレジットカード番号等の適切管理義務の履行主体者として、脆弱性対策を求めることが適切である。

EC サイトにおけるクレジットカード決済の利用は、国内取引に止まらず、海外からも自由にアクセスが可能であり、越境取引も行われる場でもあること、サイバー攻撃の手法や被害の動向は日々変化していることを踏まえ、EC 加盟店の脆弱性対策は継続的かつ適切なアップデート及びこれを担保するための措置も必要である。

更に、不正アクセス発生後の被害拡大防止のためには、EC 加盟店が早期に漏えいを検知するための不正アクセスの早期検知等も重要であり、EC 加盟店に求めていくことが望ましい。一方、不正アクセスの早期検知等を、脆弱性対策自体も十分に実施できていない中小 EC 加盟店に対して義務付けることについては、時期尚早との意見もあった。

漏えい原因の一つであるクレジットマスターは、EC 加盟店の決済フォームが悪用され、クレジットカード番号の有効性が確認され、利用可能なクレジットカード番号等が割り出されることから、実質的にクレジットカード番号等が漏えいするものである。このため、EC 加盟店において大量のデータが流れることを検知してクレジットマスターを未然に防止する対策も有効ではないかという見解もあった。

また、EC 加盟店が EC サイト上で第三者のサービスを利用する場合には、決済ページの変更・改ざんへの対応として、警告表示なく不正アクセス者にスキミングコード等を追加されないよう EC サイトを表示するブラウザの通信を制限する仕組み[9]等により、予期しないスクリプトの埋め込

[9] 例えば、コンテンツセキュリティポリシー（CSP）等がある。CSP とは、クロスサイトスクリプティングのリ

みを防止・検知することも追加的な漏えい対策として重要である。なお、PCI DSS の最新のバージョンでも明記され、ベストプラクティスとして位置づけられている[10]。

昨今では、EC 加盟店との委託関係が不明確な取引先事業者やクレジットカード番号等の取扱いの該当性が判然としない事業者等を起因とした漏えいもあることを踏まえると、クレジットカード番号等取扱業者のセキュリティ対策の義務範囲、当該 EC 加盟店の取引先事業者との責任分岐点、クレジットカード番号等取扱業者の対象の適切性についても、検討が必要である。

これらに加え、EC 加盟店での漏えい対策の実効性の確保として、どのように適切管理義務の履行を担保するかが課題となる。これまで、EC 加盟店の適切管理義務の履行については、基本的にはアクワイアラー等による加盟店調査、管理により担保されるものとし、加盟店を改善命令等の行政処分の対象としていない。しかしながら、アクワイアラー等が加盟店契約を根拠として EC 加盟店にセキュリティ対策の徹底を図ることは限界があり、EC 加盟店の行動変容が起きることは期待しづらい。このため、EC 加盟店のセキュリティ対策の実施を担保するため、加盟店も改善命令の対象とすること等を検討する必要性はあるが、その発動要件等義務付けの在り方には工夫が必要であるとされた。

なお、将来的にはクレジットカード番号 14～16 桁ではないトークナイゼーションをどのように使い得るか、検討課題として視野に入れておくべきという意見もあった。

（１－２）具体的な措置

上記を踏まえ、以下の当面の対応を措置するとともに、更なる検討が必要である。

＜当面の対応＞

対応①：EC 加盟店でのクレジットカード番号等の適切管理義務の水準の引き上げ

⇒基本的なセキュリティ対策として、EC 加盟店のシステム、EC サイト自体の脆弱性対策※を必須とする。

※システム上の設定の不備への対策（PW 管理等）、脆弱性診断・対策、ウイルス対策等

【セキュリティ GL に追記】（2022 年度末～2024 年度末）

＜更なる制度的措置の必要性の検討＞

論点①：EC 加盟店での漏えい対策の実効性の担保

⇒EC 加盟店におけるシステムや・サイトの脆弱性等を原因とした漏えい事案への対応として、必要な措置及びそれを担保するための制度の在り方についての検討。（2023 年度）

（法的論点例）EC 加盟店の適切管理義務に対する改善命令の導入

EC 加盟店でのセキュリティ対策状況・登録契約先の事業者等の表示

＜参考＞EC サイト全般のセキュリティ対策要件の確認（「EC サイト構築・運営セキュリティガ

スクを軽減するブラウザの標準機能。組み込むコンテンツが改ざん等を受けた場合にも、事前に指定したサイト以外との通信等を禁止出来る。これにより、管理者権限の奪取やクレジットカード番号等の外部送信等の抑止が可能となる。EC 加盟店のウェブサイトへのヘッダー設定が必要。

[10] PCI DSSver.4.0 は 2024 年３月末まで移行が求められているとなるが、ベストプラクティス要件として位置づけられている項目は 2025 年３月末までの準拠が求められている。

イドライン（仮称)」(2023 年度末)）[11]

（ロ）アクワイアラー側の対応

割賦販売法では、アクワイアラー等に対し、EC 加盟店に対する加盟店管理（EC 加盟店のクレジットカード番号等の適切管理）を求めており（法第 35 条の 17 の８)、EC 加盟店側の適切管理義務水準の引上げに伴い、アクワイアラー等による EC 加盟店に対する加盟店管理（セキュリティ基準）を強化するアプローチが考えられる。

（１－１）アクワイアラー等の加盟店管理（セキュリティチェック）の強化

クレジットカード番号等の適切管理義務として、EC サイト自体の脆弱性対策についても、アクワイアラー等の加盟店管理義務の対象としていくべきである。

現在、アクワイアラー等から新規 EC 加盟店に対し、セキュリティチェックリストによる EC サイト自体の脆弱性対策の実施状況の申告を求め、その内容を確認する試行運用が 2022 年 10 月から開始されたところである。現在のチェック項目がどの程度実態に即して抑止効果があるかについて、2023 年度中に判断する。

特に、EC サイトの脆弱性対策を含むセキュリティ対策は、継続的な対応が求められるものであり、その実効性を担保するためには、EC 加盟店の対策に加え、アクワイアラー等による EC 加盟店調査・管理においても確認が求められる。一方、現状、EC 加盟店に直接対峙していないアクワイアラー等の EC 加盟店のセキュリティ対策の確認は形式的な非保持化か否かの確認になっていること、EC 加盟店からの申告ベースでの確認であること、アクワイアラー自体に脆弱性診断について知見を有している人材が不足していること等から、どの程度の有効性が期待できるのは不明である。更に、アクワイアラー等がすべての EC 加盟店に対して、サイバー攻撃や漏えい事案の発生状況を踏まえた適時適切のセキュリティ対策を求め、実施状況を調査、管理することの業務負担の増加についても留意が必要である。また、クレジットカード番号等のセキュリティ対策の管理として、現在の加盟店管理の在り方が効率的で妥当なものとなっているかについて検証を要する点から、国の加盟店管理に対する監督の手法についてもより柔軟かつ実効的な方法や監督体制の人的強化について検討を行うほか、加盟店管理が実効的なものとなるよう加盟店管理の在り方についても検討が必要である。

（１－２）具体的な措置

上記を踏まえ、以下の当面の対応を措置するとともに、更なる検討が必要である。

＜当面の対応＞
対応①：アクワイアラー等による加盟店管理として加盟店調査対象事項の対象の拡大
⇒アクワイアラー等から新規 EC 加盟店に対し、セキュリティチェックリストによる

[11] クレジットカード決済にかかわらず、EC サイトの構築・運用そのものについて、独立行政法人情報処理推進機構（IPA）から「EC サイト構築・運用セキュリティガイドライン（仮称)」が策定されているところである（2022 年度末公表予定)。EC サイト開設時にセキュリティ保守・運用コストを見積もらないサイトが被害にあっているという事実の啓発に加え、オープンソースやパッケージソフト等を活用して構築する EC サイトにおいて、構築時及び運用時の最低限満たすべき脆弱性対策要件や、応急措置としての WAF（Web Application Firewall）等の導入指針等が挙げられている)。

EC サイト自体の脆弱性対策の実施状況の申告を求め、その内容を確認する試行運用を開始。【アクワイアラー等の運用】（2022 年 10 月～2023 年度末（予定））

⇒EC 加盟店のクレジットカード番号等の保持・非保持の有無／ PCI DSS の準拠の状況に加え、EC 加盟店のシステムやサイト自体の脆弱性対策について、加盟店の適切管理の措置として加盟店管理義務の対象とするため加盟店調査項目を拡大する。【セキュリティ GL に追記】（2022 年度末～2024 年度末）

対応②：アクワイアラー等の加盟店管理に対する国の監督

⇒アクワイアラー等の加盟店管理が実施されているか、監督を開始。EC 加盟店の定期調査（初期調査と同じ項目の調査）については、調査対象となる既存 EC 加盟店数が膨大にあり、2025 年４月からどのように監督していくか、優先順位や実施時期の工夫をする。【国の運用】（2025 年４月）

（運用上の論点）調査の頻度等運用方法（法の運用・監督）
アクワイアラー等の管理能力

＜更なる制度的措置の必要性の検討＞

論点①：加盟店管理の仕組みの在り方

⇒現在の加盟店管理の手法が妥当なのか、特にマルチアクワイアリングによる仕組みのもと管理業務の対象事業者が多いこと、管理手法のデジタル化による効率化等が図れないのか、加盟店管理の実効性を担保するための制度的措置の必要性を検討する。【国の検討】（2023 年度）

（法的論点例）マルチアクワイアリング下での加盟店管理の在り方
管理手法のデジタル化、リスクベースに基づく定期調査の可能性

（２－１）PSP（決済代行・EC モール等）を通じた加盟店に対する管理の在り方

アクワイアラー等による EC 加盟店に対する加盟店管理を実効的に行っていくうえでは、現在の非対面取引での取引の仕組みの実態にも留意する必要がある。法的にはアクワイアラー等であるクレジットカード番号等取扱契約締結事業者に対して加盟店管理義務が規定されているが、現在のクレジットカード業界の取引の仕組みでは、非対面取引を行う EC 加盟店の加盟店管理は、これら加盟店へのクレジットカード決済機能やシステムの提供等の業務により、EC 加盟店と直接かつ日常的な接点を有する決済代行業者や EC モール事業者等の PSP が、実質的に対応していると考えられる。

このような状況において、EC 加盟店に対して脆弱性対策等のセキュリティ対策の義務を強化した場合、セキュリティ対応の義務主体者は EC 加盟店であることには変わりはないが、そのセキュリティ対策の実効性を担保するための加盟店管理の主体者について検討が必要である。その際には、多様な PSP の機能や役割に応じて、PSP とアクワイアラーとの責任の分界点について留意すべきである。

（２－２）具体的な措置

上記を踏まえ、更なる検討が必要である。

＜更なる制度的措置の必要性の検討＞

論点①：PSP の実態把握

⇒PSP の加盟店管理における機能、実務実態について把握し、制度的措置の必要性を検討する。【国の検討】（2022 年度末～2023 年度）

（法的論点例）PSP の登録（実効的な加盟店管理）

２．決済代行業者等関連事業者における漏えい対策の強化

（イ）PSP

EC 加盟店の非保持化を実現するためのサービスを提供している PSP は、EC 加盟店の非保持化の進展、クレジットカード決済を利用する EC 加盟店の増加等から、保持するクレジットカード番号等が蓄積されていくため、厳格なセキュリティ対策の要請は更に強まっている。2021 年には、クレジットカードの決済代行業者の大量の情報を保有するデータベースへの外部からの不正アクセスにより、同社が運営する複数の決済サービスにおいて、決済情報の漏えいが発生する事案が生じた。本事案では、クレジットカード番号等の漏えい件数及び漏えい対象者がクレジットカード決済を行っていた EC 加盟店数も多いいだけでなく、漏えいされたクレジットカード番号等の不正利用による被害が実際に発生し、影響は深刻なものとなった。同社では、基本的なセキュリティ対策や業務運営体制について軽視されていた。

割賦販売法では、PSP に対し、クレジットカード番号等の適切管理義務が事後規制として課されている（法第 35 条の 16 第１項第４号・第７号）が、国による市場に参入する前の審査やアクワイアラー等による契約先としての管理の対象にはなっていない。

割賦販売法で規定するクレジットカード番号等取扱業者としての PSP は、決済代行、EC モール、EC システム提供等の機能を提供しており、多様な事業形態が存在しているところ、組織のセキュリティ体制や組織文化、人的資源等は事業者ごと差異があり、漏えい対策の措置である PCI DSS の準拠自体が目的となり、継続的な基本的なセキュリティ対策の実施やセキュリティ対策の運営体制の整備が措置されていない事業者も存在する。基本的なセキュリティ対策は PCI DSS の要件に入るものも多く、PCI DSS 準拠下で業務運営が行われていることが必須であるが、PSP が PCI DSS 審査の対象となるシステム、アプリケーション、ネットワーク等の範囲や状況を適確に把握したうえで審査を受け、準拠しなければ安全性は担保されない。PSP の漏えい対策として、単に PCI DSS を準拠しているという事実だけでなく、セキュリティ対策運用に係る体制整備の状況の確認及びセキュリティ対策の実効性の担保をどこまで求めるかが課題となる。

（１－１）PSP のセキュリティレベルの担保の在り方

現状、PSP には業界横断的な業界団体が存在しないことから、業界全体での取組による網羅的な業界の底上げは困難である。PSP のセキュリティレベルを担保するにあたり、クレジットカード決済網のゲートキーパーとして、加盟店管理と同様に、アクワイアラー等が PSP に対し、セキュリティ状況について調査・指導する方策が考えられる。アクワイアラー等が法に基づく調査・指導を PSP に実施することとなったとしても、PSP 内部の組織体制・業務運営体制までを民間企業であるアクワイアラー等が調査・指導することには限界がある。そのため、法律に基づく登録義務を課し、国による PCI DSS 準拠を含むセキュリティ対策の実施に係る体制整備確認を受けた

事業者のみ市場への参入が可能となる制度を構築も考えられる。さらには、漏えい等のインシデント発生時における被害拡大防止、利用者保護の観点から業務停止等の措置についても検討が必要である。検討が必要である。また、登録の際には、一定のレベル以上の PSP は、第三者による審査を必ず受けてその結果を公表する等追加的な方策も考えないと機能しないではないかという意見もあった。

（１－２）具体的な措置

上記を踏まえ、更なる検討が必要である。

＜更なる制度的措置の必要性の検討＞

論点①：PSP の実態把握

⇒４号・７号事業者は所謂 PSP、EC モールを始めとした多様な形態の事業者が対象となるところ、これらの事業者の実態を踏まえ、役割及びその役割に応じたセキュリティレベルの再検討、国の監督の在り方や等の制度的措置の必要性を検討する。【国の検討】（2022 年度末～2023 年度）

（法的論点例）PSP の登録制（事前のセキュリティ体制等のチェック）

論点②：クレジットカード番号等適切管理義務の明確化

⇒クレジットカード番号等の適切管理として、求められるべき基本的なセキュリティ対策や業務運営体制の措置について検証する。【国の検討・監督指針等の明記】（2022 年度末～2023 年度）

（法的論点）適切管理義務における基本的セキュリティ対策・体制整備の位置づけの検証

（ロ）EC 決済システム提供者

昨今の EC 加盟店のクレジットカード決済スキームを含む EC サイトの構築は、必ずしも自社構築で完結するものだけでなく、第三者のサービスを利用しているケースが多く存在している。このため、EC 加盟店が利用する決済モジュールを含む EC サイト構築・運用サービスを提供する事業者のサーバーが不正アクセスを受け、結果、EC 加盟店の顧客のクレジットカード番号等が漏えいする事案が発生している。また、これらの事業者は複数の EC 加盟店に同サービスを提供していることから、一事案につき、複数の EC 加盟店の顧客のクレジットカード番号等が漏えいし、被害範囲、規模は大きくなることとなる。

割賦販売法では、クレジットカード番号等取扱業者として「大量のクレジットカード番号等を取り扱う者として経済産業省令で定める者」（法第 35 条の 16 第１項第７号）を定めており、省令において「特定のクレジットカード等購入あつせん関係販売業者又はクレジットカード等購入あつせん関係役務提供事業者のために、クレジットカード番号等を特定の立替払取次業者に提供（当該立替払取次業者以外の者を通じた当該立替払取次業者への提供を含む。）することを業とする者」（施行規則第 132 条の２）と定めており、加盟店向けに決済システムを提供する事業者も対象としている。

EC 加盟店向けに、決済モジュールを含む EC サイトを構築・運用をするサービスプロバイダーなどは、自らクレジットカード決済システムを提供しているにもかかわらず、クレジットカード

番号等を提供していないとして、これらの事業者は自らが適切管理義務の対象事業者ではない、加盟店から委託を受けている場合には、適切管理義務として加盟店と同様、非保持化対応を行っていればよいと誤認しているケースも散見される。現在、アクワイアラー等による自主的な取組として、EC 加盟店が委託・利用する EC 決済システム提供業者やその他サービス提供業者を加盟店から申告してもらい、実態を把握し始めているところであるが、まずはクレジットカード番号等の取扱いや提供の範囲について、解釈を明確化する必要がある。

（１－１）EC 加盟店に対して EC 決済システムを提供する者の法的位置づけ

割賦販売法第 35 条の 16 第１項第７号に規定する「クレジットカード番号等の取扱い」には、必ずしもクレジットカード番号等を物理的に取り扱うことのみを対象としているものではなく、他社が提供するサービスやシステムを利用することにより間接的にクレジットカード番号等を取り扱うことも含んでいること、利用者が、クレジットカード番号等を、EC 決済システム提供者のネットワークを介さず、自身の PC 等に表示される加盟店の決済画面から決済代行業者に対して直接伝送し、さらに当該決済代行業者が立替払取次業者にクレジットカード番号等を提供するようなスキームであったとしても、EC 決済システム提供者が提供するサービスにより立替払取次業者に対してクレジットカード番号等が提供されているのであれば、「当該立替払取次業者以外の者（決済代行業者）を通じた立替払取次業者への提供」を行っていると考えられる。

しかしながら、義務主体者として該当する事業者となるか自覚しにくいだけでなく、取引先が義務主体者として対象となっているか認識しづらいことから、解釈や具体例の提示等により対象範囲を明確化するための措置が求められる。

（１－２）具体的な措置

上記を踏まえ、更なる検討が必要である。

＜更なる制度的措置の必要性の検討＞

論点①：クレジットカード番号等を取り扱う者の範囲の明確化

⇒加盟店におけるクレジットカード決済のためにクレジットカード番号等を間接的に取り扱う事業者が法第 35 条の 16 第１項第７号に規定する事業者の対象となること等を明確化する。【監督指針等に明記】（2022 年度末～2023 年度）

（法的論点例）「取り扱う」（法第 35 条の 16 第１項第７号）の解釈・「提供」（施行規則第 132 条の２）の範囲の明確化（監督指針等）

３．クレジットカード番号等取扱業者（共通）での漏えい対策の強化

（１－１）クレジットカード番号等適切管理義務の明確化

クレジットカード番号等の適切管理義務として PSP に求められる基本的なセキュリティ対策や業務運営体制の措置は、PSP に限らず割賦販売法第 35 条の 16 に規定するすべてのクレジットカード番号等取扱業者に共通する課題と位置づけられる。

（１－２）具体的な措置

上記の検討を踏まえ、更なる検討が必要である。

＜更なる制度的措置の必要性の検討＞

論点①：クレジットカード番号等適切管理義務の明確化【再掲】

⇒クレジットカード番号等の適切管理として、求められるべき基本的なセキュリティ対策や業務運営体制の措置について検証する。【国の検討・監督指針等の明記】（2022 年度末～2023 年度）

（法的論点例）適切管理義務における基本的セキュリティ対策・体制整備の位置づけの検証

（２－１）登録対象外の取扱業者（EC 加盟店等）でのセキュリティ対策等の見える化による市場の健全化

現状の EC 取引では、消費者が利用する EC 加盟店のサイトが、クレジットカード番号等の漏えい防止としてどのようなセキュリティ対策を講じているかは表示されておらず、適切なクレジットカード番号等の漏えい対策が講じられている EC 加盟店を見分けることができない。利用前に事前に把握したいと思っている利用者が大半であり、利用者が安全なクレジットカード決済の利用を提供する EC 加盟店を選択するための情報提供として、EC サイトの閲覧しやすい箇所に、EC 加盟店のセキュリティ対策を表示する等の見える化を求める方策が考えられる。また、結果として、十分なセキュリティ対策を講じない EC 加盟店への行動変容も期待し得る。もっとも、表示すべき内容として、セキュリティ対策の詳細を開示することは安全性の観点から適切ではなく[12]、基本的な事項として PCI DSS 準拠の有無や非保持化等の割賦販売法に基づくセキュリティ対策としてセキュリティ GL で求められる措置を表示することが想定される。

見える化を図ることは、EC 加盟店以外にも、登録により事前審査の対象となっていないクレジットカード番号等取扱業者すべてにも共通する方策とも考えられる。利用者への情報提供だけでなく、キャッシュレス化が進展し、EC 加盟店等が新たな取引先を選択する際にも、自社が決済網において直接・間接的につながる取引先の判断の目安となることも期待される。

（２－２）具体的な措置

上記を踏まえ、更なる検討が必要である。

＜更なる制度的措置の必要性の検討＞

論点①：EC 加盟店等でのセキュリティ対策の表示

⇒利用者への情報提供・事業者の選択の確保、漏えい対策の実効性の担保（事業者の行動変容）の観点から、EC 加盟店でのセキュリティ対策の表示等、制度的措置の必要性を検討する。【国の検討】（2023 年度）

（法的論点例）EC 加盟店等でのセキュリティ対策状況

登録契約先の事業者等の表示

12 見える化を図ることにより、虚偽の表示をする第三者への対策や攻撃者に狙われるデメリットもあるのではないかとの意見も一部あった。

４．業界全体での体制強化

現在、クレジットカード決済のセキュリティ対策は、クレジット取引セキュリティ対策協議会（事務局：一般社団法人日本クレジット協会）が措置の具体的内容として実務的な措置及び技術水準を検討し、ガイドラインとして公表し、国はこれらの措置及び技術水準を法令上のセキュリティ対策の実務指針として、その実施状況を国として監督している。漏えいや不正利用のインシデントに対して、適確な対策を検討し、その実施を推進するためには、漏えい事案や不正利用の実態把握、原因分析が必須であるところ、これを実施するための仕組み、実施体制を構築するとともに、類似事案の発生の防止のための周知活動やセキュリティ対策の推進への取組が必要である。

（１－１）クレジットカード業界のセキュリティ対策に関する体制強化に向けて

現状、クレジットカード・セキュリティ対策協議会において、クレジットカード決済の関係事業者が集まり、セキュリティ対策の水準や実施するべき対策等を議論している。類似事案の再発防止や業界全体としての対策を進める観点からも、国や業界団体がより関与していくべきである。従前と比べ、クレジットカード決済には、クレジットカード会社以外の多様なプレイヤーが参画する構造となってきており、これらの事業者におけるセキュリティ対策の実施が重要であることから、クレジット取引セキュリティ対策協議会においても、これらの事業者が講じるべき取組を含めて実効性のある取組・施策をまとめていくべきである。

また、セキュリティ情報は関係機関や事業者から発出されているが、数や頻度が多くこれらの情報の取得・活用の状況に差違がある。業界内の事業者が取得する情報のレベル感を合わせるための情報共有も必要であるほか、クレジットカードの漏えいや不正利用の動向については常時継続的なの動向の把握も必要となる。特に、クレジットカード決済網は国際ブランドの仕組みを前提としたものであり、業界全体でのセキュリティ対策を強化していくうえでは、他国の法制も参考にしながら、海外動向を含め国際ブランドの持つデータを国が恒常的に、かつ適時に取得できるような枠組みを構築し、これにより得られた情報を基に、国が継続的に対策を講じていくことが合理的である。

（１－２）具体的な措置

上記を踏まえ、以下の当面の対応を措置するとともに、更なる検討が必要である。

＜当面の対応＞

対応①：業界内の周知・再発防止の対策強化としての業界側の体制強化

⇒クレジットカード番号等の漏えい事案に対する実効性な対策を検討するための実態把握、不正利用の詳細原因の分析を継続的に実施するため認定割賦販売協会日本クレジット協会の体制・専門性の強化、活動方針について検討する。【JCA・国】（2022 年度末～2023 年度）

対応②：業界内の周知・再発防止の対策強化として国の監督強化

⇒国による監督の強化、漏えい事案の速やかな把握を実現する制度を検討する。

また、警察等との連携によるサイバー犯罪の手口の共有だけでなく、国際ブランドからの情報提供を受け、業界のセキュリティ対策を底上げすることを検討する。【国の運用・検討】（2022 年度末・2023 年度運用開始）

第１節の２．インシデント対応・漏えい防止に係る利用者保護

１．漏えい時の利用者への連絡・公表の早期化

現状、EC 加盟店においてクレジットカード番号等の漏えいが発生した場合の業界ルールでは、イシュアーが対象顧客を把握し、対象顧客からの問い合わせ対応を準備したうえで個別の通知、公表を行うことが、顧客の混乱回避と事態の早期収束に資するとして、通知・公表の内容、タイミング、方法等についてイシュアーと調整することを求めている。このため、実態上、フォレンジック調査が完了し、漏えいの対象となったクレジットカード番号等が確定してから通知・公表が行われており、漏えいの可能性があるとわかった時点から、実際に利用者に個別通知または公表されるまでの期間が長く、数ヶ月以上かかる事案がほとんどである。一方、利用者の不正利用被害拡大防止の観点からは、利用者への早期の個別通知または公表を担保すべきと考えられる。

（１－１）漏えい時の利用者への早期の個別通知または公表の在り方

利用者への個別通知・公表までの期間が長期化している要因は、イシュアーと EC 加盟店間での交渉や調整、フォレンジック調査等に時間がかかるとされている。また、クレジットカード番号等を特定しないまま漏えい当事者が公表すると、不安になった利用者からの連絡が、漏えい当事者との間で対処方針の固まっていない状態のクレジットカード会社に殺到することが懸念されている。

しかしながら、インターネットや SNS の普及する情報化社会にあって、漏えいのおそれのある状況に関する情報は、他の利用者にも瞬時に伝わりやすい。また、事業者の社会的責任として、また消費者安全の領域では、原因不明であっても事故情報そのものについては一刻も早く伝えることが社会の総意となってきている[13]。クレジットカード番号等の特定ができない段階での利用者に周知・公表した場合、イシュアーによるモニタリングの強化やカード交換等の対応が実施される状況にはないものの、利用者自身のクレジットカード番号等が不正利用されていないかを確認し、二次被害となる不正利用の防止のための注意喚起となる。漏えいのおそれが発覚した際の通知・公表については、どの段階で、どういった情報を伝えるべきなのか、また、それぞれのタイミングでの通知・公表において、その後の事業者の対応として何をするべきなのかを実務を踏まえた検討を行い、利用者への通知・早期化を実現することが必要である。また、漏えい当事者の公表については、自社サイトの見つけにくい場所で公表されている、公表した内容を早期に削除しているケースが見受けられるとの指摘もあり、公表の持続期間や方法も課題となる。特に PSP 等の利用者と直接契約関係がない漏えい当事者の場合には、利用者への連絡手段も限られるほか、利用者は、自身のクレジットカード決済に PSP 等の事業者が関与していることを認識していないことも多いことから、広く公表をする等の工夫を要する。

利用者保護または利用者の被害拡大防止という観点から、漏えい事業者の対応の実効性を確保するため、制度的に措置することも考えられるが、漏えい事業者による国に対する漏えい報告を義務化（第１節の２．２．（１－２））した場合、事案に応じて行政による注意喚起としての公表を行うこともあり得るのではないかという意見もあった。

[13] 個人情報保護法の令和２年改正により、個人データの漏えいがあった際は利用者本人への通知、通知が困難な場合には代替措置としての公表が求められるようになった。

（１－２）具体的な措置

上記を踏まえ、以下の当面の対応を措置するとともに、更なる検討が必要である。

＜当面の対応＞

対応①：漏えい時の利用者への通知・早期化

⇒現状、全ての漏えいカード番号の特定に至ってから初めて公表される漏えい事案の公表について、漏えい発覚時から長期間が経過していることから、利用者保護または被害拡大防止のため、クレジットカード番号等の漏えい時の利用者への通知・対外公表の早期化に向けて、参考となる通知のタイミングや周知案文等を追記する。【加盟店向け「クレジットカード情報の漏えい時および漏えい懸念時の対応要領」（JCA）の改訂・周知】（2023 年度）

＜更なる制度的措置の必要性の検討＞

論点①：漏えい時の利用者への通知・早期化

⇒利用者保護または被害拡大防止、注意喚起のため、クレジットカード番号等の漏えい時の利用者への通知の在り方・早期化等について、制度的措置の必要性を検討する。【国の検討】（2023 年度）

（法的論点例）漏えい時の利用者への個別通知または公表
被害拡大防止のための国等による注意喚起（公表）

２．利用者保護を図るための国の監督の整備

現状、EC 加盟店での漏えい報告は、業界自主ルールのもと、アクワイアラー等から関係行政機関に報告することの一環で、事実上、国（経済産業局）に報告する運用がなされており、国への明示的な報告義務はない。加盟店以外のクレジットカード番号等取扱業者（法第 35 条の 16）での漏えいは、当該業者が登録業者であれば官公庁も含めた関係先への迅速な連絡体制の整備は求めているが、登録業者の有無にかかわらず、報告義務自体はない。また、漏えいが起きた場合であっても、クレジットカード番号等取扱業者に対し、行政はクレジットカード決済サービスを即座に停止させる権限はない。

クレジットカード番号等の漏えいが発生した際、事業者が利用者保護のための対応を実施しているかを監督する観点からは、国への早期の報告、クレジットカード決済サービスの即時停止や適切なセキュリティ対策を講じたうえでの決済の再開を求められるよう、国の監督に必要な整備をすべきと考えられる。

（１－１）国における漏えい事案の把握

現状、アクワイアラー等から国（経済産業局）に漏えい事案を事実上報告しており、法的義務化の必要性はないという意見もあった。一方、漏えい事案の国への報告は、漏えい原因となるサイバー攻撃手法も変化し、現況の漏えい事案が深刻化しているなか、国としても、クレジットカード番号等の適切管理として、被害拡大防止または再発防止のための対応を適時適確に実施しているかを監督するため、また利用者に被害を生じさせるような重大な漏えい時や新たなサイバー

攻撃の手法が判明した場合の注意喚起等を実施するため、早期に漏えい事案の状況を把握できる体制を確保するべきという意見もあり、制度的な措置の必要性について検討が必要である。

（１－２）具体的な措置

上記を踏まえ、更なる検討が必要である。

＜更なる制度的措置の必要性の検討＞

論点①：クレジットカード番号等の漏えい時の国への報告

⇒利用者保護・被害拡大防止のため、クレジットカード番号等の漏えい時の国への報告について制度的措置の必要性を検討する。【国の検討】（2023 年度）

（法的論点例）漏えい時の国への報告

（２－１）漏えい時の被害拡大の防止の在り方

現状、クレジットカード番号等を漏えいした際には、EC 加盟店の決済は多くの場合、アクワイアラー等により即日停止しているが、EC 加盟店から拒否される場合もなくはない。漏えい原因や再発防止策の確認ができるまでの間の決済停止に強制力を持たせたほうが実効的であるほか、PSP のような大規模な漏えい事案でも強制力が必要な場面がある。一方、日常生活においてクレジットカード決済が利用されている現状においては、クレジットカードの決済停止は影響も大きいことから、どのような場合に決済を止めるべきか、再開してよいかについては精査が必要である。

（２－２）具体的な措置

上記を踏まえ、更なる検討が必要である。

＜更なる制度的措置の必要性の検討＞

論点①：クレジットカード決済サービスの即時停止・再開の判断の明確化

⇒クレジットカード決済サービスの即時停止や漏えい時の決済サービスの停止や再開について、制度的措置の必要性を検討する。【国の検討】（2023 年度）

（法的論点例）漏えい時の決済サービスの即時停止

漏えいに伴う決済サービスの停止／再開の要件の明確化

第２節．クレジットカード番号等の不正利用防止

○位置づけ

クレジットカード番号等の不正利用防止は、クレジットカード番号等の漏えいや割り出しにより、クレジットカード番号等がなりすまされて使われる財産被害によるクレジットカード決済システムの信頼性確保だけでなく、クレジットカード決済の仕組みを通じて社会犯罪に資金が流入することの抑止、ひいてはテロ資金供与対策にも寄与するものである。

１．非対面取引での利用者本人の適切な確認

割賦販売法では、加盟店に対し不正利用防止措置として、①利用者によるものであるかの適切な確認等、②その他の不正利用を防止するために必要かつ適切な措置を講ずることとされている（法第 35 条の 17 の 15)。非対面取引においては、不正利用リスクに応じた対策として、①利用者の適切な確認については、高リスク商材取扱 EC 加盟店や不正顕在化 EC 加盟店に対しては任意で求める扱いとし、すべての EC 加盟店に対しては求めてこなかった。

一方、昨今、不正利用額が増加しているだけでなく、不正利用商材が多様化、金額が低廉化するなかで、商材の指定の限界、対策の選択の任意性、そもそもの利用者の適切な確認がないなかでのクレジットカード決済によるシステムの信頼性への毀損、犯罪組織への資金供与にもつながることから、制度として、非対面取引における利用者の適切な確認として、本人認証を実施すべきと考えられる。

（１－１）利用者の適切な確認に向けた環境整備

非対面取引においても、すべての EC 加盟店に対し、「利用者であることの適切な確認」としてイシュアーによる本人認証を求めることとする。その手法として、クレジットカード業界が統一的に推進する対策としては、国際ブランドが共通で規格し、現在有力な手法である EMV3DS[14]の導入を進める。新規に EMV3DS を導入した EC 加盟店の不正利用防止の効果は顕著でもあったことから、2024 年度末（2025 年の３月）を期限として、公平・平等の観点から、原則、すべての EC 加盟店に導入を求めていくべきである。その際には、かご落ちリスクを懸念する EC 加盟店に対し、個々の EC 加盟店の不正利用を防止する実効性の観点だけでなく、不正利用対策の導入が進む諸外国に比べ日本市場が狙い撃ちされ、犯罪やマネロンの温床として非常に危険になることを防ぐ観点からも、不正利用防止措置の義務水準の引き上げとして位置づける。

未導入加盟店が狙われる点、認知やかご落ちリスクの点からは、一斉の導入が望ましいが、件数・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の段階的な導入が現実的である。まずはリスクや取引規模の大きいところは優先的に早めの導入を目指すべきである。なお、導入に伴う EC 加盟店の経済的負担として、EMV3DS の導入に伴う経費は、利用の手数料より

[14] EC 加盟店からイシュアーに、利用者のデバイス・行動・属性情報等を提供し、イシュアーでのルール設定によるスコアリング・リスク判定を踏まえ、取引の拒絶・チャレンジ（パスワードの要求)・取引認証（パスワード不要）を判断する。従来の旧３-D セキュアの更新版として、リスクベース認証のほか、ワンタイムパスワードの標準化によるセキュリティ強化及びの入力負荷の軽減、スマホ対応による対象取引の拡大や加盟店からイシュアー（ACS：アクセスコントロールサーバー）への提供情報の拡大が可能となった。

も初期のシステム導入コストの方が障壁となる可能性が高く、導入には一定の時間がかかることが想定される[15]。

EMV3DS を義務化しても、固定パスワードによる本人認証では、パスワード自体が漏えいしている場合には、不正利用リスクが高いことから、イシュアーは、固定パスワード以外のワンタイムパスワードや生体認証も活用した利用者本人しか知り得ない・持ち得ない情報での入力を求めるようにすべきである。

更に、キャッシュレスサービスや EC モールのアカウントと紐付けられたクレジットカード決済が普及している状況下では、これらのアカウントの入力等だけでクレジットカード決済ができることに鑑みれば、アカウント自体がクレジットカード番号等と同等の情報となる。このため、アカウントにクレジットカード番号等の紐付けの登録をする時及び登録後に個別の決済をする時のなりすまし対策が必要となる。まず個別に決済をする前にアカウントをクレジットカード番号等と紐付ける登録を行う場合には、EMV3DS により、本人認証を行う必要がある。そのうえで、登録後に個別の決済を行う際にも、ログイン時のアカウントの本人認証が EMV3DS と同程度のなりすまし防止策を実施しており、EC 加盟店側が取引の不正利用リスクの分析、判断を適切に行うことができる場合にあっては、ログイン後の個別の決済時の EMV3DS による本人認証については、柔軟な運用を認めることも考えられる。

ただし、十分なアカウントのなりすまし対策等が行われていない場合には、EMV3DS の本人認証を実施するべきと考えられる。

また、個別の決済ごとに EMV3DS による本人認証をしない場合は、チャージバックのライアビリティがあることに留意すべきである。

アカウントの紐付けがなされていない場合であっても、継続課金等様々なクレジットカード決済の利用の状況に鑑みた実効的・効果的な検討も必要である。

なお、これらの仕組みは、①イシュアーの EMV3DS システムの導入、②加盟店の EMV3DS システムの導入、③利用者のパスワード設定が必要となってくる。現状、①については対応しつつあるが、②の導入の義務化だけでなく、③についてはイシュアーの web サービス等の充実・進捗度合いによるところが多く、ばらつきがあり、業界一丸となっての呼びかけが必要である。

非対面取引では、EC モールでの決済市場のシェアが高いことを考えれば、②の導入を進めるにあたり、EC 加盟店を抱える EC モール等の PSP も EC 加盟店の不正利用防止について対応することが求められる。特に EC 加盟店に対し、クレジットカード決済機能を提供し、EC 加盟店の一存では仕組みを導入できない場合には、PSP に対して同様に不正利用防止の措置を求め、一律に適正なクレジットカード決済環境の整備を図る必要が生じてくる。

そして、国は、性能規定を採用する割賦販売法に基づく不正利用防止対策の効果検証を行う必要がある。EMV3DS については、イシュアーによるリスクベース認証の運用状況を監督官庁に報告し、監督官庁がその運用により不正利用防止が図られているのかを確認・モニタリングできる形が必要となってくる。また、国として、不正利用の総額は把握しているものの、具体的な不正利

[15] PSP のシステムを利用している場合は PSP 側の投資、自社で EC システムを構築している場合は加盟店側の投資であり、外部ベンダーを利用している場合は EC システムの構成による。義務化に際し、財政上の支援が必要ではないかという意見もあった。

用の状況・類型等を把握するための整備がなされておらず、関係事業者から提供されるべきである。

現状、EMV3DS の導入に伴うイシュアーの運用として、イシュアーのパスワードを求める判断にばらつきがあるだけでなく、システムの安定稼働に課題があると指摘されており、イシュアー側のリスクベース認証の精度を上げること等が急務となっている。

今後、利用者であることの適切な確認として本人認証をすべての EC 加盟店に求めていくことを踏まえると、セキュリティ GL に定めている４つの EC 加盟店の不正利用防止の方策について、イシュアーによる利用者本人の適切な確認として本人認証を義務化することを念頭に置いた見直しが必要となってくる。

また、EC 加盟店や EC モールにおいて、その他の不正利用防止措置として、性能規定のもと実施されてきた属性・行動分析等による従前の不正利用防止措置も引き続き組み合わせて行われるべきである。

インターネット環境でビジネスを行うためには、継続的な情報収集と対策が不可欠であることを踏まえれば、EMV3DS を導入すればそれで足りるものではなく、状況の変化に応じて EMV3DS の運用の改善を図ること、さらに場合によっては、他の手段も含めた重層的な対策が必要となってくることに留意しなければならない。

（１－２）具体的な措置

上記を踏まえ、以下の当面の対応を措置するとともに、更なる検討が必要である。

＜当面の対応＞

対応①：非対面取引における利用者本人の適切な確認として、本人認証の義務化

⇒EC 加盟店の不正利用防止措置として、2025 年３月までに、固定パスワード以外のワンタイムパスワードなど利用者本人しか知り得ない・持ち得ない情報により、利用者本人の認証を行うための仕組みを順次導入する【セキュリティ GL に追記】（2022 年度末～2023 年度末）

⇒イシュアーとして、利用者本人の適切な確認を実現するための仕組みを導入、利用者に呼びかける。【イシュアーの運用】（2022 年度・2023 年度）

対応②：非対面取引における本人認証として EMV3DS の導入・運用

⇒当面の対応としては、まずは原則すべての EC 加盟店で、EMV3DS の導入を進める。【セキュリティ GL に追記】（2022 年度末～2024 年度末）

（論点）導入の順序

EMV3DS の運用（アカウント紐付けや継続課金等の取引における本人認証の実施方法）

⇒リスクや取引規模が大きい加盟店においては、利用者の行動分析等、EMV3DS 以外の方策による不正利用防止措置も必要であり、現状の不正利用防止４方策や具体的運用について、更に検討する。【協議会】（2022 年度末・2023 年度）

（論点）既に行動分析を実施している EC モール等における取組の継続

４方策の優先順位の変更

対応③：利用者の適切な確認の実効性の担保

⇒イシュアーによるEMV3DSのリスクベース認証が効果的に実施されるようリスクベース認証の精度を向上させる。【協議会・イシュアーの運用】（2022年度～2023年度）

対応④：非対面における利用者の適切な確認の監督に向けた準備

⇒生体認証を活用したモバイルデバイストランザクション等のEMV3DS以外の本人認証手法についても、効果及び実効性を踏まえ、必要かつ適切な利用者本人の適切な確認措置として監督上取り扱うことの検討。【協議会・国の検討・運用】（2022年度末～2023年度中）

（運用上の論点）その他本人認証手法の精査

対応⑤：業界内の周知・再発防止の対策強化としての業界側の体制強化【再掲】

⇒クレジットカード番号等の漏えい事案に対する実効性な対策を検討するための実態把握、不正利用の詳細原因の分析を継続的に実施するため認定割賦販売協会日本クレジット協会の体制・専門性の強化、活動方針について検討する。【JCA・国】（2022年度末～2023年度）

＜更なる制度的措置必要性の検討＞

論点①：不正利用防止措置の主体

⇒不正利用防止対策に関しては、イシュアーによる本人認証の実効性担保に加え、EC加盟店が本人認証を適切に行うにあたっては、決済機能サービスを提供する決済代行やECモール等のPSPによる本人認証に関するサービス提供及び運用が必要であることから、これらの事業者の不正利用防止措置の制度的措置の必要性を検討する。また、アクワイアラー等による加盟店管理におけるEC加盟店の不正利用防止対策の確認に加え、EC加盟店での不正利用防止対策に資するため、アクワイアラー等を通じた不正利用情報の提供が行われる環境整備も重要である。【国の検討】（2023年度）

（法的論点例）イシュアーの不正利用防止（EMV3DS導入・利用者の適切な確認のできない決済の禁止等）決済代行・ECモール等のPSP（※EC加盟店ではEMV3DSが導入できない仕組みの場合）のEC加盟店への不正利用防止措置サービス（利用者本人の適切な確認）の提供

論点②：利用者の適切な確認の実効性の担保として国の監督のための整備

⇒不正利用防止措置として利用者の適切な確認の実施状況のモニタリングの制度的措置の必要性を検討する。【国の検討】（2023年度）

（法的論点例）イシュアーの不正利用防止

イシュアー・アクワイアラーの不正利用防止措置の実施状況、不正利用被害の発生状況の報告

２．不正利用情報の共有化と活用

現在、各イシュアーにおいて、オンラインモニタリングによる不正検知がなされているが、各イシュアーが保有する不正利用情報をイシュアー間で共有化することで、不正検知の精度向上し、効果的な不正利用防止が期待される。クレジットカード決済網の当事者間で、不正利用に関する情報を共有・集積することで、より高度な不正検知を実現する取組が進められることが必要と考えられる。

業界では、既存のネットワークを活用した共同利用等による不正利用情報の共有が検討されている。各イシュアー間を越えた個人情報の共有にあたっては、現行の関連法令の運用との関係に留意する必要がある。

（１－１）不正利用情報の共有化と活用

イシュアーによる不正検知は、各イシュアーでシステム導入している。顧客属性や過去の経験値、情報の量や質等から、不正のリスクを判断し、個社の責任において決済を止めている。一方、効率的な不正検知の観点からは、イシュアー間で共有する連携が重要であるが、不正利用情報の共有化について、法令の確認や裏付けが必要である。

（１－２）具体的な措置

上記を踏まえ、以下の当面の対応を措置するとともに、更なる検討が必要である。

＜当面の対応＞

対応①：不正利用情報の共有化

⇒AI 等による不正利用の検知にも活用できるよう、イシュアー間での不正利用情報の共有に向けた具体的な枠組みの検討・連携の促進。【イシュアーの運用】（2022 年度～2023 年度）

＜更なる制度的措置の必要性の検討＞

論点①：制度上の整理

⇒イシュアー間での不正利用情報の共有化及び活用を推進するため、現行の関連法令を含む制度上の整理を行う。【国の検討】（2022 年度末・2023 年度）

（法的論点例）個人データの第三者提供

第３節．クレジットの安全・安心な利用に関する周知・犯罪の抑止

○位置づけ

クレジットカードの安全・安心な利用には、クレジットカード決済網の事業者による対策だけでなく、利用者自身の対策も必要となる。また、クレジットカード番号等の不正搾取・不正利用に関する犯罪は増えており、犯罪の取締りの強化を図るべきものであり、警察との連携を推進し、更に犯罪抑止を目指すべきである。

１．フィッシング対策

クレジットカード番号等の不正利用の原因の１つとされるフィッシングでは、誘導された偽サイトに、消費者自身がクレジットカード番号や ID・パスワード等を入力することにより、クレジットカード番号等を不正取得されるものである。

フィッシング自体は従前より存在するが、昨今、フィッシングの報告[16]件数が増加しており、フィッシングサイト数（URL 数）もこの３年で 10 倍以上増加している。これらのフィッシングサイトの大半は、クレジットカード番号等を取得することを目的としており、対策の実施が急務である。また、フィッシングメール技術の巧妙化により、利用者がフィッシングメールか否かを見分けることは困難であり、従前の利用者への注意喚起による利用者自身の対応を促す対策では十分ではなく、なりすまされるサイトを運営している事業者自らがフィッシング対策を実施することが求められる。このような状況から、クレジットカード業界として、フィッシングサイトのテイクダウンや送信メールのドメイン管理等によるフィッシング被害の未然防止策を多面的・重層的に実施するための環境整備が必要である。

（１－１）フィッシングに対するイシュアー・加盟店の自衛に向けた環境整備

現在、フィッシング対策としては、利用者への注意喚起も含め、クレジットカード会社各社の対応に委ねられている。事業者のフィッシング対策としては、フィッシングメールや偽サイトの検知した際、テイクダウンの要請を行うことが求められるが、そもそも、自社のメールをなりすまされないようにする対策も重要であるところ、送信ドメイン認証（DMARC[17]）が有効な手段とされている。現在のイシュアーの DMARC の導入状況は、主要なクレジットカード会社[18]であっても約３割のみの対応に留まっている。また、導入済みのイシュアーであっても、なりすましメール対策に効果を発揮する正式運用（受信者側でなりすましメールを拒否等とする設定）を行っているイシュアーは約半数となっている。フィッシングによるクレジットカード番号等の漏えいの未然防止の観点からも、国として、DMARC の積極的な導入を含め事業者自らの自衛に向けたフィッシング対策を推奨すべきである。フィッシングによるクレジットカード番号等の漏えいは、イシュ

---

[16] フィッシング対策協議会に寄せられる情報提供。フィッシング詐欺へ誘導するメールや SMS、フィッシングサイトの情報を報告の増加は、消費者が詐欺被害にあう危険性が高くなっていることを意味する。

[17] DMARC（Domain-based Message Authentication, Reporting, and Conformance）は、送信者をドメイン名単位で認証する仕組みで、受信したメールが正規の送信元から送られてきたかを検証できる技術の一つ。ドメイン管理者は、受信者が認証に失敗した場合のポリシー（メールの取り扱い）、その検証結果をドメイン管理者へレポートしてもらうためのメールアドレスを DNS（Domain Name System）に事前に登録・公開し、検証失敗した受信者のメールの扱いを指定する（ポリシーとして、迷惑メールフォルダーへ配信(p=quarantine)、拒否（p=reject）を宣言することとなるが、拒否とする設定が本来の正式運用である)。

[18] 事務局で把握している 30 社程度のイシュアー。

アーに限らず、クレジットカード決済を利用し、利用者にクレジットカード番号等の情報の入力を求めているEC加盟店等、自社の業務においてメールを利用しているすべての事業者の問題である。まずは利用者にクレジットカード番号等を付与し、業務上メール等の連絡をとるイシュアーにおいて、積極的な導入を求める。なお、国としては、フィッシングの対象に狙われやすい事業者に対して、導入を求めている[19]。

一方、イシュアーのDMARCの導入を自主的な対応でどこまで普及させることができるか、特にDMARCの運用は、導入した事業者が、なりすまされたメールを受信者側で拒絶する設定を行った正式な運用にしなければ、フィッシング対策の効果は弱まることから、この正式運用の実施の徹底が課題となる。まずはDMARCの導入を推奨したうえで、更に措置の実効性の観点から法的な義務づけの必要性について検討すべきか見極める。また、利用者には自身が利用するサービス、事業者を選択する自由があるところ、DMARCの導入含めた安全なサービスを提供している事業者を選択する重要性を利用者に周知することも必要な取組ではないかとの意見もあった。

（１－２）具体的な措置

上記を踏まえ、以下の当面の対応を措置するとともに、更なる検討が必要である。

＜当面の対応＞

対応①：フィッシングからの自衛

⇒クレジットカード会社をかたるフィッシングサイトの検知・テイクダウンやクレジットカード会社の送信メールのドメイン管理等による未然防止による多面的・重層的な自衛・推奨【イシュアーの対応・国の推奨】（2022年度末）

２．警察等との連携による犯罪抑止

これまでも、偽造カードの取締り等、クレジットカード決済に関する犯罪について警察等と連携してきた。しかしながら、サイバー攻撃によるクレジットカード番号等の漏えいや不正利用等のサイバー犯罪が増加しており、サイバー犯罪対策の観点でも連携を強化することが重要である。既に警察において、クレジットカード番号等の不正取得や不正利用について取り締まられている事案もあるが、警察による捜査・検挙は効果のある対策であり、不正行為の取締りを加速するため、官官、官民で、より詳細かつ実効的な情報共有等の連携を強化等していく。

（１－１）警察等との連携

現状、大手のイシュアーを中心に、クレジットカード犯罪対策連絡協議会を通じて、現場の都道府県警察と情報連携等を行っている。EC加盟店と契約関係にあるPSPも、個別事案を通じて警察と連携している。

しかしながら、不正アクセスによるEC加盟店等での漏えいや不正利用においては、不正アクセスを受けたEC加盟店等と通報・相談を受ける都道府県警察間において円滑な通報・相談、これら

[19] フィッシング対策の推進：警察が把握したフィッシングサイト等に関する情報をウイルス対策ソフト事業者等に提供するほか、関係団体等と連携し、民間事業者に対して、送信ドメイン認証技術（DMARC、SPF、DKIM等）の導入等のなりすましメール対策を講じるよう働き掛ける。（「世界一安全な日本」創造戦略2022（2022年12月20日閣議決定））

の受理等がなされていない現状も見受けられる[20]。結果、サイバー犯罪全体の傾向や手口端緒を警察において把握することが困難となっている。そこで、漏えいが発生したEC加盟店等が漏えいの可能性を認識した時点で、都道府県の警察に通報・相談が行われるような取組が必要である。また、警察からの捜査協力の要請に対し不安のあるEC加盟店等もいることから、捜査の流れの概要を事前に伝え、不安を払拭するよう情報提供する等積極的な捜査協力の働きかけを行う必要がある。また、利用者が情報漏えい等を通じて不正利用され、警察に相談した場合、クレジットカードの紛失・盗難ではないことや利用者が被害者とは判定できないなどとして対応が疎かになることがないよう、警察側でも、現場での適切な対応に向けた対策を講じることが求められる。警察側においても現場においてサイバー犯罪に係る通報・届出への対応、捜査協力への働きかけに関して、適確な対応が実施されるような取組がなされる必要がある。

国の行政機関においても、割賦販売法を監督する経済産業省と都道府県警察に対する指導を行う国家公安委員会では、それぞれの所掌から、クレジットカードに関するサイバー犯罪の最新の動向の把握が十分にできているわけではない。そこで、サイバー犯罪の防止等に資するため、それぞれの持つ情報を連携し、対策の打ち出しにつなげていくことが重要である。

また、サイバー攻撃による情報の不正取得に関しては、事業者がこれを犯罪であることの認識がないことも多い。クレジットマスターを受けたことを認知したEC加盟店であっても、そもそもクレジットマスターが犯罪である[21]ことを認識しないEC加盟店も存在する。EC加盟店等への周知が課題である。

フィッシングサイトのテイクダウン要請にスピーディーに対応してくれないホスティング事業者や同じIPアドレスで複数のクレジットカード会社になりすましメールを送信する不正行為者もいるほか、フィッシングは海外から敢行されているケースも多く捜査が困難な一方、2022年4月に発足したサイバー警察局が中心となって国際連携を進めていく必要がある。

（１－２）具体的な措置

＜当面の対応＞

対応①：経産省・警察庁との連携強化

⇒不正アクセスを契機とするクレジットカード番号等の漏えい事案について、経産省から警察庁（サイバー警察局）に情報提供する。【国の運用】（2023年度中開始）

⇒クレジットカード会社等の防衛の参考になる、サイバー攻撃の手口・対策等の情報を、警察庁から経産省に情報提供し、業界に周知する。【国の運用】（2023年度中開始）

対応②：都道府県警等とイシュアーの連携強化

⇒個別事案で発覚した不正利用されたクレジットカード番号等のイシュアーへの情報提供を継続する。【都道府県警の運用】

---

[20] 警察においても同様の問題意識を持ち、「サイバー事案の被害の潜在化防止に向けた検討会」（警察庁）において、サイバー事案の被害の潜在化を防止するため、関係省庁と連携した情報共有や被害者が自発的に通報・相談をしやすい環境の整備に向けた方策について、2022年12月より議論を開始しており、2022年度内に報告書の取りまとめ及び公表を予定している。

[21] クレジットマスターは、電子計算機使用詐欺や偽計業務妨害等に問われ得る犯罪である。

⇒クレジットカード番号等が流通しているサイト情報をイシュアーに情報提供する試行を 2023 年２月まで実施する。【日本サイバー犯罪対策センターの運用】

対応③：漏えい当事者からの警察への早期の通報・捜査協力の促進

⇒業界内での漏えい時のマニュアルの整備、捜査協力時の対応フロー等を提示し、警察への早期の通報や捜査協力を促進する。【国の検討・運用、加盟店向け「クレジットカード情報の漏えい時および漏えい懸念時の対応要領」（JCA）の改訂の修正】（2023 年度中開始）

＜更なる制度的措置の必要性の検討＞

論点①：クレジットカード番号を取得しようとするフィッシングサイトの取締り

⇒現状、割賦販売法ではクレジットカード番号等が不正に取得したことを立証できた場合に取締りが可能。クレジットカード番号等を取得しようとするフィッシングサイト自体の摘発に向け、制度的措置の必要性を検討する【国の検討】（2023 年度）

３．利用者への周知

クレジットカード決済網においては、利用者もプレイヤーの一人であり、安全・安心なクレジットカード決済には、利用者自身の対応も必要不可欠である。今般、不正利用対策として業界で推進している EMV3DS は、利用者がイシュアーの web サービスにおいて、認証用パスワードの利用設定等が必要である。従前、業界からも注意喚起している利用明細の確認も、今ではイシュアーのサービスによっては、スマホアプリ等のダウンロードによりリアルタイムで利用通知を受けることができることから、不正利用を即座に認知し、被害防止に有効である。また、スマホアプリの導入により真正なサービス提供者であるイシュアーへの接続が確保されていることから、イシュアーをなりすますフィッシングへの対策としても効果が期待できる。こうした非対面取引におけるセキュリティに対策として効果的なサービスやアプリを提供するイシュアーを利用者が選んで利用できる環境を整備することも重要である。利用者には、クレジットカードの安全・安心な利用に向けて、個人情報等の漏えい実態や傾向、セキュリティ対策として実施するべき対応（EMV3DS の認証用パスワードの設定や送信認証技術（DMARC 等）、フィッシング等の対策を取っている事業者の選択）等、セキュリティ対策に関する情報をアップデートして、周知啓発することが必要である。

また、周知啓発に当たっては、利用者の情報収集の手法や場面を考慮し、効果的に行うことが必要である。一般的には、業界団体のホームページにコンテンツを掲載するといった手法が採られるが、これらのサイトに能動的にアクセスして情報収集する利用者は多くはないことから、若い利用者向けの動画サイトやニュースに掲載する等の工夫も考えられる。また、現在も学校教育現場を通じたクレジットカード取引に関する情報提供・周知を行っているところ、成年年齢の引下げ等も踏まえ、これをさらに強化する必要がある。効果的な周知の方法の明示は難しい課題であるが、業界団体・民間事業者だけでなく、国としても実施し、利用者の行動変容を促すような広報の効果をあげるため試行錯誤を続けていくこととする。

＜当面の対応＞

対応①：セキュリティの観点での利用者への周知・注意喚起

⇒昨今の漏えい実態や利用者自身が取るべき対応を広報・周知する。【JCA・イシュアー・国の実施】（～2024 年度末）

おわりに

本検討会は、クレジットカード決済システムに関わるすべての当事者それぞれ及びこれらの当事者を監督する国において、本報告書で示した具体的な措置を実施することを求める。

本報告書では、クレジットカード決済システムのセキュリティ対策に特化して、これまで実行してきた対策を振り返りながら、現在起きていることとのギャップを踏まえ対策の水準の引き上げ等の見直しを求めている。

これまでもクレジットカード決済システムの信頼性を確保するため、割賦販売法の改正等を通じ、各種の措置がとられてきたところではある。しかしながら、社会のデジタル化等に伴い、クレジットカード決済網における各プレイヤーがインターネット上で接続し、自由な空間で取引が行われているなか、サイバー攻撃等によるクレジットカード決済システムへの脅威は増す一方、キャッシュレス社会の進展で国民の日常生活を支えるインフラとしての役割の色合いも濃くなっている。特に非対面取引においては、安全・安心なクレジットカード決済の実現のためセキュリティ対策の重要性がとりわけ高まっている。また、セキュリティ対策には終わりがないことからすると、今後も不断の見直しが求められるものと位置づけられる。

クレジットカード決済はその仕組み故に、元来、関係するプレイヤーが多い業界ではあったが、非対面取引では、影響を及ぼすプレイヤーがさらに多くなっており、脆弱性を有した状態での決済サービスの提供は許容されず、決済システム全体としてセキュリティ対策を前に進めるうえでは、各プレイヤーの個社の自主的な対応に委ねるだけでは限界があり、業界全体で底上げをする必要がある。そのため、各当事者が、クレジットカード業界が講ずべきセキュリティ対策の同じ絵姿を見据えて初めて、業界全体として、安全・安心なクレジットカード決済システムを再構築することができるものと考える。また、取組を進めていくうえでは、インシデントが発生した際に、当事者間、特に利用者との関係で公正な負担となるよう留意することも必要である。

本検討会を通じて、クレジットカード決済システムに関わるすべての当事者が、クレジットカード決済システムのセキュリティ対策として対応が求められることを自覚して、実現に向け準備していくことが肝要である。

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
構成員名簿

１．委員

池本　誠司	日本弁護士連合会消費者問題対策委員会 幹事
大河内 貴之	Ｓｅｃｕｒｅ・Ｐｒｏ株式会社 代表取締役
大野　克巳	一般財団法人日本サイバー犯罪対策センター　経済・金融犯罪対策担当部長
小川　睦世	一般社団法人日本クレジットカード協会　事務局長
篠　　寛	ＥＣ決済協議会 会長（株式会社ＤＧフィナンシャルテクノロジー 代表取締役社長共同ＣＯＯ 兼 執行役員ＳＥＶＰ）
○中川　丈久	神戸大学法学研究科・法学部 教授
二村　浩一	山下・柘・二村法律事務所 弁護士
長谷川 ゆかり	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会
松尾　健一	大阪大学大学院高等司法研究科　教授
三浦　千宗	公益社団法人日本通信販売協会 理事 事務局長
森竹　由美子	ＢＳＩグループジャパン株式会社 認証事業本部金融セクター部 部長

（五十音順・敬称略）

○は座長。

２．オブザーバー

・日本クレジット協会
・クレジット取引セキュリティ対策協議会
・情報処理推進機構セキュリティセンター
・警察庁サイバー警察局サイバー企画課
・金融庁資金決済モニタリング室
・経済産業省商務情報政策局サイバーセキュリティ課

３．事務局

経済産業省商務・サービスグループ商取引監督課

検討経過

第１回　2022 年８月４日

議事

（１） 検討会の設置等

（２） 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に向けた方向性

（３） 今後の検討に向けて

（４） 自由討議

第２回　2022 年９月 13 日

議事

（１） クレジットカード番号等の漏えい対策

第３回　2022 年 10 月 11 日

議事

（１）クレジットカード番号等の不正利用対策

第４回　2022 年 11 月 15 日

議事

（１－１） クレジットの安全・安心な利用に関する犯罪の抑止（フィッシング対策）

（１－２） クレジットの安全・安心な利用に関する犯罪の抑止（警察等との連携）

（２） クレジットカード番号等の漏えい対策（インシデント対応・漏えい防止に係る利用者保護）

（３） クレジットの安全・安心な利用に関する周知

第５回　2022 年 12 月 23 日

議事

（１）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報告書（骨子案）

（２）自由討議

第６回　2023 年１月 20 日

議事

（１）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報告書（案）

（２）自由討議