資料８

前回の検討を踏まえた対応の方向性について（案）
（クレジットカード取引のセキュリティ強化）

平成 28 年４月 21 日
経済産業省

１．前回の委員各位のご意見

○　クレジットカード取引におけるセキュリティ対策については、現下の状況に鑑み、カード番号等情報管理及び不正使用対策いずれについても、加盟店等に対する義務づけを含めた強化を図るべきであるとのご意見が多数を占めた。

・セキュリティについては、消費者の自助努力では対応のしようがないため、規制による対応も必要。

○　その上で、義務づけの対象範囲や具体的内容については、以下のご意見があった。

- 個別業界の実態を踏まえ、中小企業等の負担軽減に関し、配慮が必要。
- 消費者の立場からは、加盟店等に対するセキュリティ対策の義務付けについて、その対象となる主体の範囲を限定することは望ましくない。
- 加盟店ごとのリスクに応じた対応が許容されるようにすべき。
- 一定の基準を示した上で、各事業者の創意工夫の中で実効的な方策を見出すことを許容すべき。
- 法律で詳細なセキュリティ水準を規定するのではなく、具体的内容は政省令等の下位ルールで定め、随時見直せるようにすべき。
- 過度な対応をとると、加盟店の数が減り、消費者利便が低下するおそれもある。キャッシュレス推進に逆行しないよう、加盟店等にとって現実的な対応が可能となるように配慮すべき。
- セキュリティの問題については、コストと利便性を両立させなければならないが、FinTech 等の技術がそうした課題を解決していく。
- 義務の中身が示されないと混乱するので、具体的なセキュリティ対策について、業界でスタンダードの開発と推奨を行うことが望ましい。
- 技術中立性の観点から、PCI DSS 等の具体的な対策を法律に規定することには違和感あり。事業者に表示させることも一つの選択肢。

○　義務違反に対する措置については、制裁金を検討してはどうかといったご意見や、直罰とするよりは行政指導や改善命令による対処の方が望ましいのではないかといったご意見があった。

○　また、クレジットカードのセキュリティ強化に係る割販法における措置の前提として、個人情報の保護に関する法律（以下「個人情報保護法」という。）との関係については、以下のご意見があった。

・　平成２０年改正における割賦販売法改正の趣旨を再確認し、個人情報保護法に委ねてその目的が実現できるのか、キャッシュレス社会を目指すうえで割販法に何ができるのか再整理すべき。
・　個人情報保護法は、個人のプライバシーの観点から措置するものであり、カード番号のように決済のために転々流通するものは想定していないため、割販法の中で必要な措置を講じるべき。
・　カード番号について改正個人情報保護法を適用した場合、実務上支障が生じることが懸念されるため、クレジット業界としては、カード番号が個人情報保護法の対象となることには反対の立場。

○　アクワイアラーによる加盟店調査については、以下のようなご意見があった。
・　アクワイアラーにとって履行困難な義務とならないよう慎重に検討すべき。
・　多数のアクワイアラーの対応にばらつきが生じないよう、最低限の線引きをして取組を後押しする必要がある。
・　「加盟店等への義務づけ」と「加盟店調査」の間に論理的関係があるのではないか。加盟店に直接の義務がかかっていない場合でも、アクワイアラーによる加盟店調査義務の対象にできるのかという点について整理が必要。

○　消費者教育等については、日本の消費者はセキュリティに関する認識が甘いので、加盟店の取組を「見える化」する等により、認識を高めていくことが必要とのご意見があった。

これらのご意見を踏まえ、残された主な論点について、以下のように考えてはどうか。

２．加盟店等のセキュリティ対策について

まず、加盟店等における「セキュリティ対策」とは、以下の２つの対策を総称するものとする。
① クレジットカード情報の保護（不正アタック等による漏洩防止）
② 正当な権利者（本人）以外の者による不正使用防止（対面取引における偽造カードの使用防止と非対面取引におけるなりすましの防止）

（２）個人情報保護法と割賦販売法との関係の再確認

①保護法益等

個人情報保護法は、プライバシー等の人格権や財産権等広く個人の権利利益の保護を目的としており、個人情報を取り扱う民間事業者に対して、個人情報について利用目的の範囲内での取り扱いや個人データの第三者提供の制限と安全管理措置を講じ

ること等の規律を定めている。個人情報の取り扱いに当たってはその有用性に配慮することとされ、例外規定等も設けられている。

これに対し、割賦販売法（以下「割販法」という。）におけるクレジットカード番号等の適切管理義務は、取引インフラとしてのクレジットカードの信用秩序を維持し、利用者の信頼を確保する観点から、クレジットカード番号等の不正使用・流出を防止する必要性が特に高いものであるという理由に基づき、平成２０年の割販法改正により導入されたものである。

割販法は、クレジットカード番号の不正使用・流出による個々の利用者の財産被害の防止のみならず、クレジットカード取引システムの信頼性維持という個人の権利利益にとどまらない社会的法益を保護している点で、個人情報保護法とは保護法益が異なるものと言えるのではないか。

また、特に不正使用被害防止については、個人情報保護法においては特段の措置は規定されていない。

②検討の方向性

個人情報保護法において、個人情報としての適正な取り扱いの確保の観点からクレジットカード番号を「個人識別符号」として政令指定するか否かが議論されているが、個人情報保護法と割販法の上記のような保護法益や措置内容の違いや、決済のために転々流通するカード番号の特性を踏まえ、クレジットカード番号等の情報漏洩及び不正使用の防止を図るにあたっては、個人情報保護法の適用関係の如何にかかわらず、割販法で措置することが必要ではないか。

（２）義務主体の範囲と義務の水準について

クレジット取引は、サイバーセキュリティ基本法に基づく「重要インフラ」として指定されており、キャッシュレス社会の主要な取引インフラとしての重要性も増している。

加盟店からのカード番号等の大型漏洩事件の続発や不正使用被害額の増加傾向、我が国のセキュリティホール化の懸念、近時のPOSシステムに対するサイバー攻撃の増加等、我が国のクレジットカード取引に対するセキュリティリスクの高まりに対し、クレジット取引システムの信頼性を確保するため、実効的な対応措置を講じることが喫緊の課題である。

まずは、２０２０年に向けて国際水準のセキュリティ環境の整備を目指して、幅広い関係事業者が参画したクレジット取引セキュリティ対策協議会で策定された「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－」（以下「実行計画」という。）の実効性を確保するため、割販法において加盟店等に対するセキュリティ対策の義務づけを行うべきではないか。

なお、個人情報保護法において義務づけられる「安全管理措置」については、「本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ

適切な措置を講ずるものとする。」（経済産業分野のうち信用分野における個人情報保護ガイドライン）として、リスクベースの考え方が採用されている。キャッシュレス社会の実現に向け、「コストと安全性」の適切なバランスを図るためにも、割販法においても、義務の水準の検討に当たっては、キャッシュレス推進の観点も踏まえ、特に中小企業等の事業者負担に配慮しつつ、このような「リスクに応じた措置」を求める考え方が妥当ではないか。

以上を踏まえ、具体的には、たとえば以下のような措置を検討してはどうか。

① 番号等情報管理については、個人情報保護法の改正により取扱個人情報の件数による裾切りがなくなり、中小企業も含め全ての事業者に安全管理が義務づけられたこととのバランスも考慮し、クレジットカード番号等を保有する全ての事業者（加盟店、PSP 等）に対し、リスクに応じた法的義務を課すこととする。

② 不正使用対策義務については、取扱い商材や業種業態、取扱件数等を勘案し、それぞれのリスクに応じた対応を加盟店に求めることとする。

（３）具体的な義務内容の在り方について

上記３．の通り、加盟店等に対しセキュリティ対策を義務付けるに当たっては、上記の通り「リスクベース」の考え方を基本とし、「不正を企図する攻撃者に対し、多面的かつ一般には公開できない取組を行うことが必要であり、技術自体も日々進歩するものであるから、法令等により特定の技術的手段を求めることにはなじまない面がある」という点にも留意し、例えば、以下のような製品安全・保安分野における「性能規定」的な考え方に基づく制度設計を検討してはどうか。

① 「性能規定」的な考え方

製品安全・保安分野においては、技術進歩や新製品へのより柔軟な対応を可能とするため、製品等が満たすべき技術基準について国が寸法・数値、形状、材質、計算式等の詳細を定める「仕様規定」から、製品安全・保安に不可欠な性能のみを定め、当該性能を実現するための具体的な手段・方法など問わないとする「性能規定」への転換が図られている。

これにより、従来、法令等により規定されていた材料の規格、数値、計算式などの詳細については、各事業者の自主的判断に委ねられ、技術開発の促進にもつながるとされている。

また、「性能規定」である基準に適合しているか事業者が判断する際の指針として、最新の技術を活用して民間が定める規格を「整合規格」として積極的に採用し、公表することとしている。

② 検討の方向性

クレジットカード取引のセキュリティ分野においても、「利便性と安全性」あるいは「コストとセキュリティ」の両立という課題を、技術の力で解決することが重要であ

り、技術革新の果実を迅速に取り込んでいくダイナミックな仕組みを作ることが求められるのではないか。

こうした観点から、上記のような「性能規定」の考え方を取り込むことにより、法令においてはセキュリティ確保に不可欠な機能（一定水準の情報漏洩防止と不正使用防止）のみを定め、その実現手段・方法は各事業者の創意工夫によることとし、各事業者の判断に基づき、より適切なセキュリティ対策を講ずることができるようにする必要があるのではないか。

他方、事業者にとっては予測可能性が確保されることも重要であるため、「このやり方であれば、法令上の義務を満たす」ものとして、例えば自主規制機関のガイドラインとして標準的な対策を示すとともに、技術進化の状況に応じ、機動的にこれを見直していくことが求められるのではないか。

まずは、関係事業者による実務的な検討を経て策定された「実行計画」のうち具体的な措置に関する部分を、セキュリティ対策に係る義務の履行方法に関する事業者向け指針として位置付け、国としてもその着実な実施を後押ししていくことが必要ではないか。

（４）義務に関する担保措置

セキュリティ対策について、事業者における義務の履行を担保するため、情報漏えい事故や不正使用が発生した場合等における報告徴収や改善命令等の行政処分から、命令違反の場合の罰則規定まで、段階的な措置を講じられるようにしておくべきではないか。

３．アクワイアラーによる加盟店調査について

昨年の報告書において、アクワイアラーによる加盟店調査は「悪質加盟店の是正・排除を通じた加盟店網における適正なクレジットカード利用環境維持に向けた公法上の措置」とされている。これは、アクワイアラーがいわば「加盟店網のゲートキーパー」として、加盟店に対する適切なスクリーニング機能あるいはモニタリング機能を担うという考え方といえる。

クレジットカード取引システム全体のセキュリティを確保することも「加盟店網における適正な利用環境維持」のための重要な要素であることに鑑みれば、加盟店等に対するセキュリティ対策の義務付けに併せて、アクワイアラーによる加盟店調査において、加盟店等における対応状況を確認し、必要に応じて、是正指導や加盟店契約の見直し等の適切な対応を求めていくことが必要ではないか。

セキュリティ対策に関する加盟店調査の具体的な在り方については、「リスクベース」の考え方に基づいて、加盟店ごとのリスクに応じた対応が求められると考えられるのではないか。

また、具体的な調査方法の検討に当たっては、現状における国内アクワイアラーにおけ

る加盟店審査実務や対応コスト等に十分配慮しつつ、悪質加盟店排除のための加盟店調査と同様、「特定の調査項目を法令上列挙してこれについての調査のみを求めるという考え方よりは、各アクワイアラー等が自社の営業実態やノウハウに応じ、初期審査と途上審査を柔軟に組み合わせた調査体制を整備できるよう、双方を総合して一定水準を確保することを許容する」という性能規定的な考え方をとってはどうか。

その上で、整備する体制についての具体的な指針（ガイドライン）として、例えば、必須事項とともにベストプラクティスから抽出した推奨事項を示すことにより、必要最小限の水準を確保しつつ、各アクワイアラーがこれに基づくセルフチェックにより自社の対応状況を客観的に認識できるようにすることで、継続的なレベルアップを促していくことが重要ではないか。

なお、この加盟店調査義務については、加盟店における情報漏えい事故等の発生について、アクワイアラーに結果責任を求めるものでないということを確認しておく必要があるのではないか。

４．認定割賦販売協会の役割について

クレジットカード取引のシステム全体のセキュリティを確保するためには、取引に関わる多様なステークホルダーが目標を共有しつつ連携し、最新の技術動向やリスク環境の変化に応じて継続的に取り組んでいくことが不可欠である。

こうした観点から、割販法上の自主規制機関であり、かつ、クレジット取引セキュリティ対策協議会の事務局として「実行計画」の策定においても中心的役割を果たしてきた認定割賦販売協会（日本クレジット協会）の法定業務として「セキュリティ対策の推進のために必要な業務」を追加し、２０２０年に向けた実行計画の確実な実行と、その後の更なるセキュリティ強化の取組を推進する体制の中核として位置づけることが必要ではないか。

また、上記の通り、加盟店等に対してセキュリティ対策を義務づけることとした場合、その具体的な内容については、「性能規定」的な考え方に基づき、最新の技術を活かした多様な手法に対してオープンなものとすることが求められるのではないか。

他方、事業者に対して「どのような対策を講じれば十分か」について具体的な指針を示すため、認定割賦販売協会において、関係事業者の実務的検討によるガイドラインあるいは民間規格の策定を行うことが求められるのではないか。

アクワイアラーに求める加盟店調査についても、認定割賦販売協会において同様の役割が求められるのではないか。