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
－２０１８－
【公表版】

２０１８年３月１日

クレジット取引セキュリティ対策協議会

－目　次－

はじめに

我が国の国内消費が横ばいで推移する中にあって、急成長する電子商取引（以下「EC」という）の拡大とともに、クレジットカードの取扱高は堅調に拡大を続けており、2016 年には取扱高 53 兆円を超えるなど、クレジットカードが社会における取引インフラとして重要な機能を担っている。

政府は「未来投資戦略 2017」（2017 年 6 月 9 日）において、これまでの 2020 年のオリンピック・パラリンピック東京大会の開催に向け、「クレジット決済端末の 100%の IC 対応化」の実現等、国際水準のセキュリティ環境の実現を目指すとの方針に加え、新たに今後 10 年間（2027 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方針を示した。また、「明日の日本を支える観光ビジョン」（2016 年 3 月）においても、外国人が訪れる主要な商業施設、宿泊施設及び観光スポットにおいて、「100%の決済端末の IC 対応」等、キャッシュレス環境の飛躍的な改善を行うこととしている。

サイバーセキュリティの観点からも、クレジット分野は、2014 年 5 月には政府の情報セキュリティ政策会議において国の重要インフラの一つとして指定されており、セキュリティ強化に向けた更なる取組が求められている。

このように、商取引の活性化に資するキャッシュレス化の推進とともに、IC 対応化の実現等による安全・安心なクレジットカードの利用環境整備は、国の重要な政策課題となっている。一方、2016 年 7 月に内閣府が実施した「クレジットカード取引の安心・安全に関する世論調査」によれば、クレジットカードの利用について約 6 割が消極的と回答しており、その多くは、不正利用や情報漏えいに対する懸念があるとして、政府に対し、「不正使用に対する取締りの強化」（57.4%）や「セキュリティ対策の規制に係る法整備」（52.3%）を求めている。

本協議会は、2020 年に向け、「国際水準のセキュリティ環境」を整備することを目指し、クレジットカード取引に関わる幅広い事業者（クレジットカード会社、加盟店・関係業界団体、PSP[1]（Payment Service Provider）、決済端末機器メーカー、情報処理センター、セキュリティ事業者、国際ブランド等）及び行政が参画して 2015 年 3 月に設立された。その後 1 年間検討を重ね、2016 年 2 月 23 日付けで「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（以下「実行計画」という）」を策定し、毎年度、各主体における実行計画の進捗及び達成度等を踏まえ、これを改訂することになっている。関係各主体は互いに連携し、本実行計画に基づく取組の推進により、我が国が 2020 年までに達成すべき目標の実現に向け、セキュリティ対策の取組を進めているところである。

政府は、安全・安心なクレジットカード利用環境を実現するため、2016 年 10 月 18 日に、加盟店に対してセキュリティ対策を義務付ける等の措置を盛り込んだ「割賦販売法の一部を改正する法律案」を国会に提出し、本法案は、衆参両院において全会一致で可決された。「割

[1] 本実行計画では、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をいう。

賦販売法の一部を改正する法律」（以下「改正割賦販売法」という）は、同年 12 月 9 日公布、2018 年 6 月 1 日に施行される。

本実行計画は、改正割賦販売法に規定するセキュリティ対策義務の実務上の指針となるものである。本実行計画に掲げる措置又はそれと同等以上の措置を講じている場合には、セキュリティ対策に係る法的基準を満たしていると認められる。

今般改訂された 2018 年度の実行計画は、2017 年度の実行計画の下での取組の進捗を踏まえ、関係事業者における取組を更に推進するため、各対策に関する記載事項の具体化・明確化を行い、課題の解決を図った結果を反映した。また、引き続き、本協議会で検討を進めるべき課題について整理の上、2018 年度の重点取組事項を取りまとめたものである。

本実行計画は、クレジットカード取引に関係する各主体がそれぞれの役割に応じて取組むべき事項を取りまとめたものであり、関係各主体が本実行計画を踏まえ、主体者として着実な取組を進め、目標を達成することを期待する。

2018 年 3 月 1 日

Ⅰ．基本的な考え方

１．クレジットカード取引における不正利用被害の実態等

我が国のクレジットカードの不正利用被害は 2003 年以降漸減傾向にあったが、EC の増加に伴い 2013 年から再び増加傾向に転じている。一般社団法人日本クレジット協会（以下「日本クレジット協会」という）の集計によれば 2016 年には約 142 億円の被害が確認されている。2017 年は 1 月から 9 月までに、既に 177 億円の被害が発生しており、前年を上回る勢いとなっている。なお、こうした不正利用被害は、高額な家電製品・宝飾品等、デジタルコンテンツやチケット類といった換金性・流通性の高い商材を取り扱っている業種の加盟店において多発している。

窃取されたカード情報等を不正に利用したなりすましによる被害額は、対面、非対面加盟店で発生する不正利用被害額全体の 73.7%を占めるに至っており、特に EC 加盟店における不正利用被害の伸びが顕著になっている。これを踏まえ、カード会員本人になりすました不正利用の様々な手口に対して実効的に対処するため、リスクが高い加盟店においてはより多面的・重層的な対策を講じる必要がある。

対面取引においては、偽造カードによる不正利用被害を防止するため、クレジットカードの IC 化とともに、決済端末の IC 対応を進めていく必要がある。我が国と同様に、IC 対応が遅れている米国では、大手スーパーマーケットでの大規模情報漏えい事件が契機となり、2014 年 10 月に IC 対応を進める大統領令が発令されたことを踏まえ、IC 対応が急速に進められている。こうした中、我が国の IC 対応の取組が遅れると、米国で発生していた不正利用被害が我が国にシフトし、セキュリティホール化するリスクが高まることは、10 年ほど前に欧州で IC 対応が進んだ際に不正利用被害が米国にシフトしてきた歴史の教訓からも十分想定されることである。実際、大型商業施設等で偽造カードを使用したショッピングの被害が報告されている状況を踏まえても、対面加盟店における IC 対応を進めていくことは喫緊の課題である。

また、これら不正利用により得られた資金は犯罪組織の活動資金源となっている可能性もあることから、クレジットカード取引に関係する事業者は社会的責任の観点からも不正利用対策に取組むべき責務があることを認識しなければならない。

さらに、不正利用が発生する原因となるカード情報の漏えい対策についても重点的に取組む必要がある。カード情報が漏えいするリスクは、カード情報を取り扱う全ての事業者に生じる可能性があり、近年の傾向としては、外部からの攻撃に対してセキュリティ対策が脆弱な EC 加盟店（委託先を含む）からの漏えいの増加が顕著となっている。また、海外では、大手加盟店の POS 端末を標的としたサイバー攻撃によってウィルスに感染し、当該端末で決済されたカード情報を含む顧客情報が大量に窃取されるという事案が発生している。我が国においても同様のウィルスが検出されたとの情報もあり、早急な対応が必要となっている。

各主体は、我が国がセキュリティホール化し、不正利用被害が国境を越えて流入するリスクが高まっていることへの危機意識を共有した上で、本実行計画を早急に実行することが求

められる。

２．セキュリティ対策の強化に向けた基本的な考え方

本協議会においては、2020 年に向け、国際水準のセキュリティ環境を整備し、安全・安心なクレジットカードの利用環境を実現するため、以下の点に留意しつつ、取組を進めている。

（１）本実行計画の位置づけ

改正割賦販売法の施行により、①カード会社（イシュアー）、②カード会社（アクワイアラー）等[2]、③加盟店においては、クレジットカード番号等の適切な管理や不正利用の防止といったセキュリティ対策が求められることとなる[3]。本実行計画は、改正割賦販売法で求められるセキュリティ対策の実務上の指針として位置づけられるものであり、本実行計画に掲げる措置又はそれと同等以上の措置を講じている場合には、セキュリティ対策に係る法令上の基準を満たしていると認められる。

また、改正割賦販売法では、カード会社（イシュアー）に加え、カード会社（アクワイアラー）等について「登録制」が導入され、カード会社（アクワイアラー）等は契約先加盟店の調査等を実施することが求められることとなる。調査の結果、セキュリティ対策が不十分な加盟店については、契約先のカード会社（アクワイアラー）等からの指導により合理的な期間内に法令上の基準に適合することが求められる。

以上の観点から、本実行計画を指針とした取組を着実に進めていく必要がある。

（２）加盟店のリスクに応じた方策の導入

対面加盟店では偽造されたクレジットカードによる不正利用、非対面加盟店では窃取されたカード情報による不正利用と、販売方法によってその攻撃手口は異なることから、セキュリティ対策の強化に向けては取引形態の違い・不正利用の手口の違い等を考慮した上で、それぞれのリスクに応じた具体的な方策を導入することが必要である。

なお、本実行計画では、クレジットカードのうち世界中で共通に使用できるがゆえに不正利用リスクの高い国際ブランド付きのカードを対象としている。一方、国際ブランドが付いていないカードについては、使用範囲が限定される点ではリスクは低いため本実行計画の対象としていないが、リスクに応じたカード情報保護対策及び不正利用対策が必要である点には留意すべきである。

（３）セキュリティ対策の検証と改善

対面取引・非対面取引ともにセキュリティ面では様々な技術やサービスが既に提供されているが、どの方策も 100%の安全性を担保するものではないという認識に立って、クレ

---

[2] 「クレジットカード番号等取扱契約締結事業者」（改正割賦販売法第 35 条の 17 の 2）のこと。

[3] 改正割賦販売法においては、クレジットカード番号等の適切な管理についてはカード会社（イシュアー）、カード会社（アクワイアラー）等及び加盟店に課された義務であり、不正利用の防止については加盟店に課された義務である。

ジットカード取引に関係する事業者においては、その業種・業態、特に加盟店においては取扱商材や販売方法と、不正利用被害の傾向と最新の攻撃手口等を踏まえ、それぞれのリスクに応じて多面的・重層的な対策を講じ、その実効性を不断に検証し、必要な改善を図ることが求められる。

（４）加盟店に対する情報提供等

加盟店における具体的な対策の導入にあたっては、契約関係にあるカード会社（アクワイアラー）や PSP が加盟店に対する必要な情報提供や具体的な方策の導入等へのサポート等を行うことが重要である。

（５）消費者に対する情報発信

カード会社や加盟店等の不正利用対策に加えて、消費者自身のクレジットカードの不正利用に対する認知・意識の向上を図るため、より効果的な消費者に対する情報発信等によって理解・協力を得ることも、セキュリティ対策強化の観点から必要な取組である。

以上の点に加えて、不正利用の攻撃手口は刻々と巧妙化すること及びセキュリティ対策の技術的進展も著しいことを踏まえ、本実行計画については、不正利用被害の実態と技術的な進展等を踏まえて適時見直しを図ることとする。

本協議会は、本実行計画を推進することで、2020 年 3 月末までに不正利用被害額の極小化を目指し、もって我が国のキャッシュレス社会の安全・安心なクレジットカード利用環境の実現を図るものである。

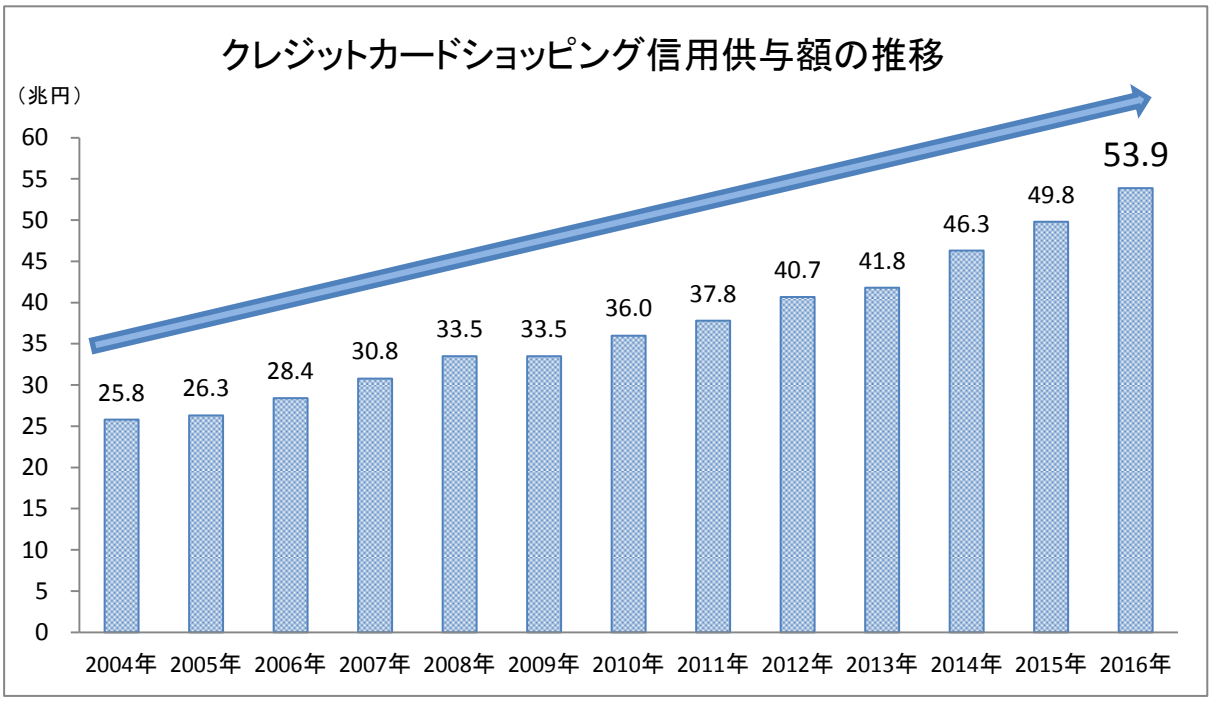
Ⅱ．分野別の具体的な実行計画

具体的な実行計画の策定にあたっては、取引の類型及び想定される不正手口について以下の分類を行い、それぞれ未然防止対策と不正利用対策に分けて適切な方策の検討を行った。

	想定される不正手口	未然防止対策	不正利用対策
対面取引	偽造カード、紛失・盗難カードによる不正利用	カード情報保護　→WG1 カードの IC 化　→WG2	決済端末の IC 対応　→WG2
非対面取引	盗用されたカード情報を用いたなりすまし	カード情報保護　→WG1	本人認証・不正利用検知の強化 →WG3

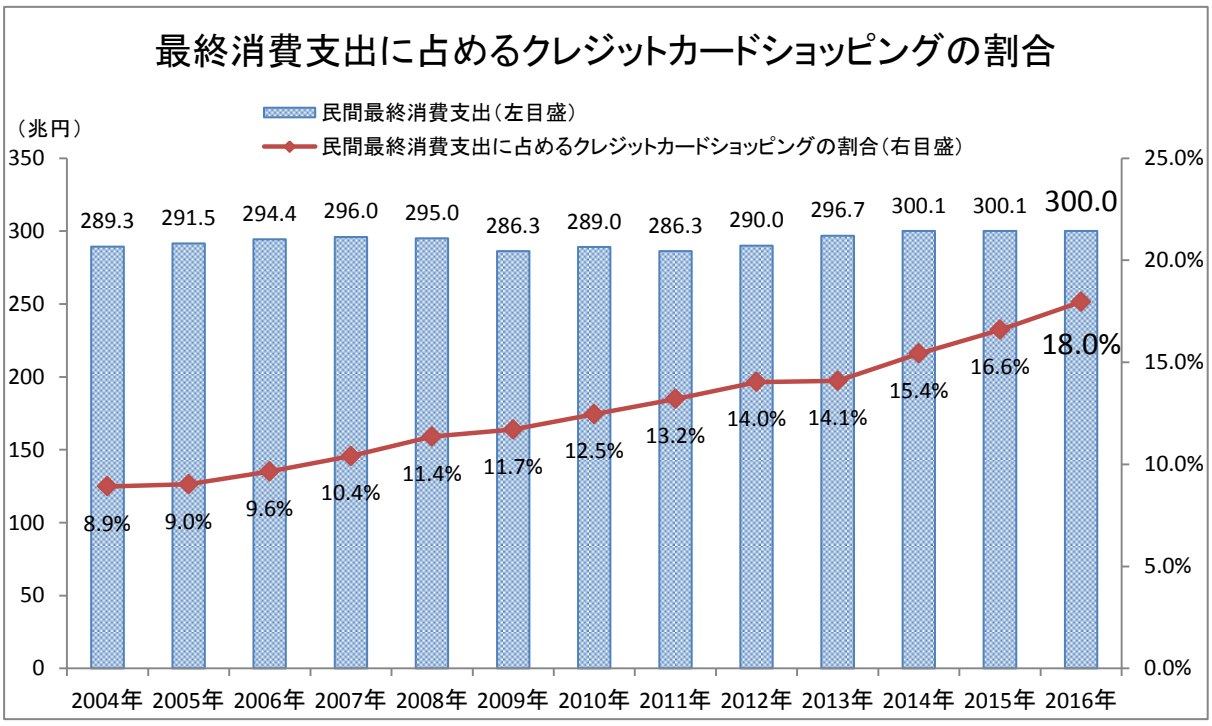
参考資料

（資料１）



出所：一般社団法人日本クレジット協会「信用供与額」

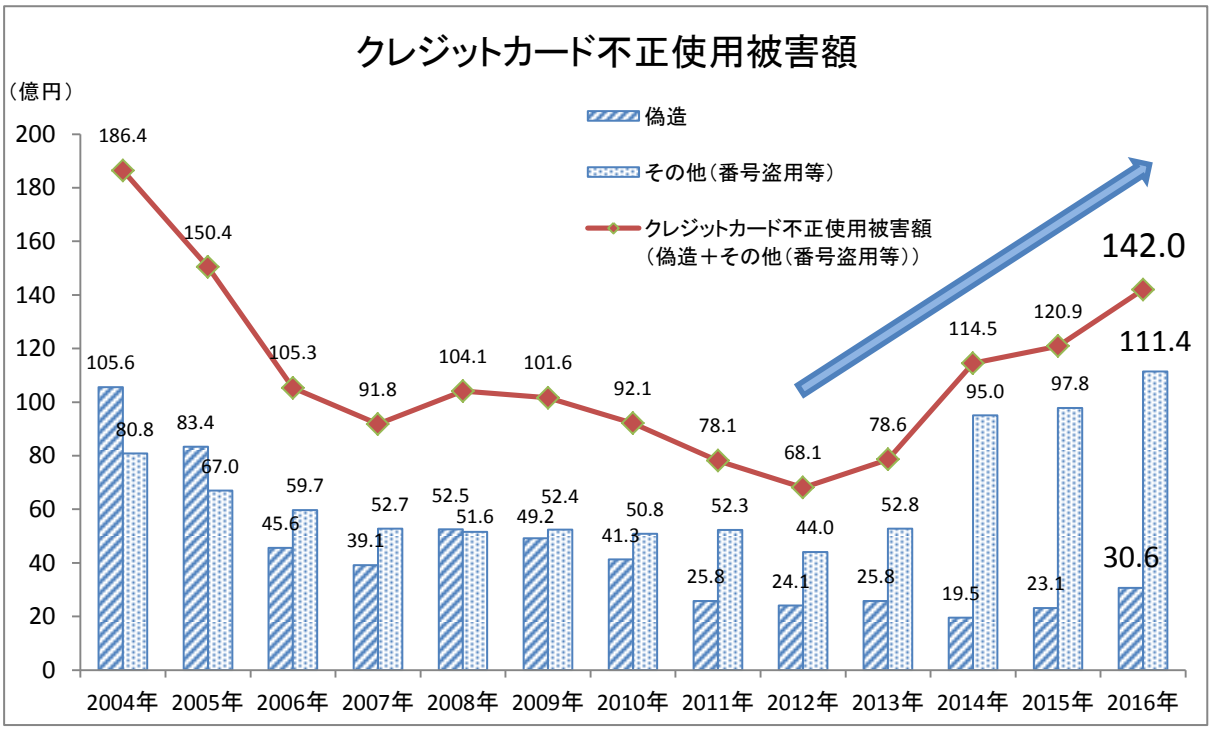
（資料２）



出所：内閣府「国民経済計算年報」民間最終消費支出：名目

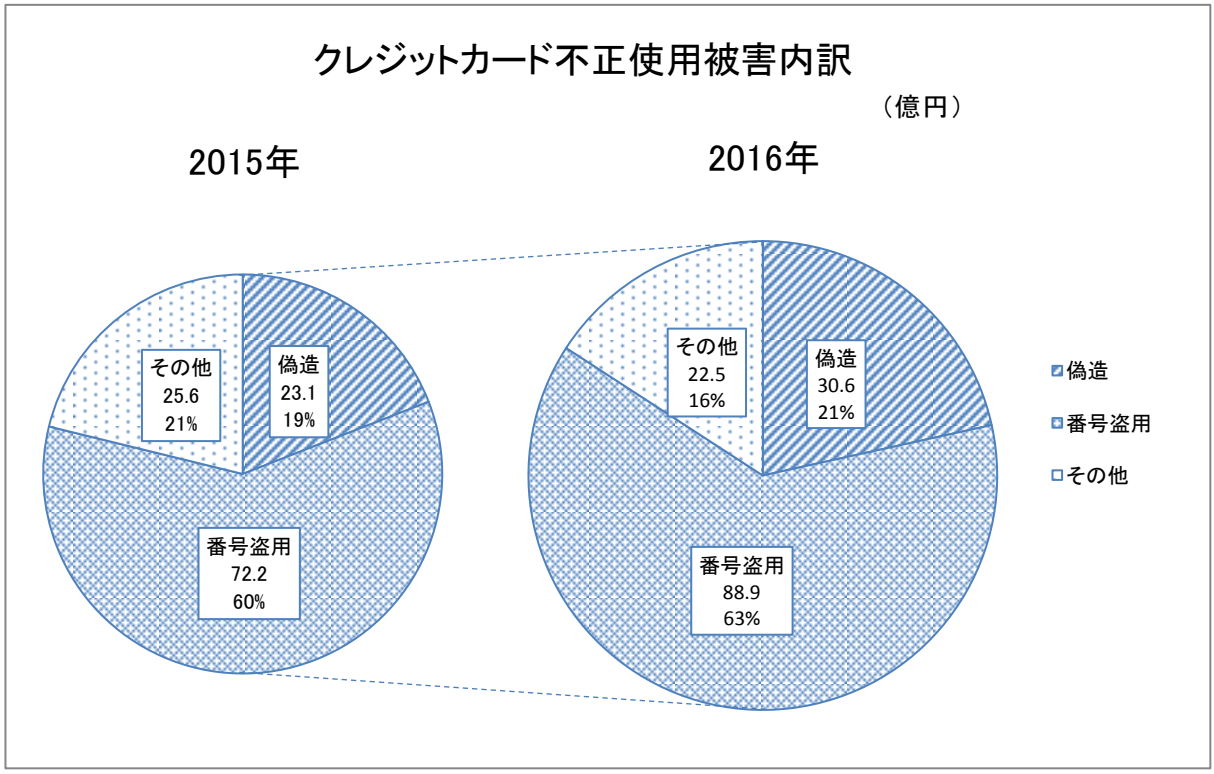
出所：一般社団法人日本クレジット協会「信用供与額」

（資料３）



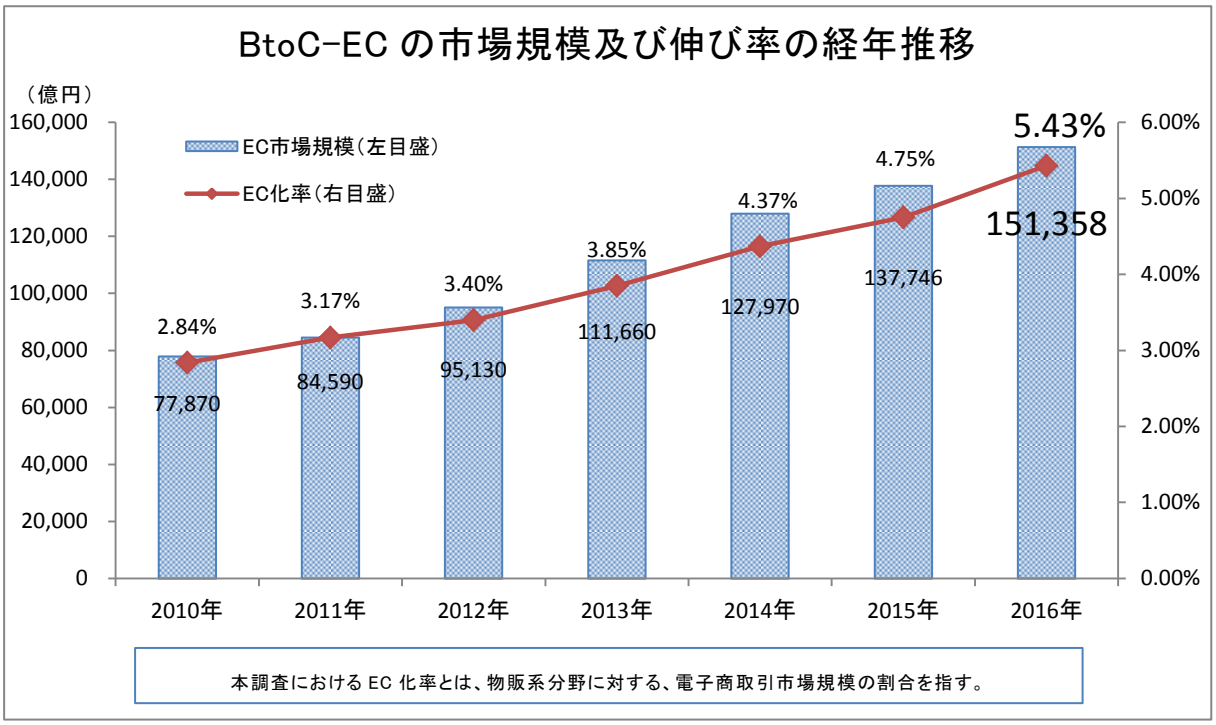
出所：一般社団法人日本クレジット協会「クレジットカード不正使用被害額の発生状況」

（資料４）



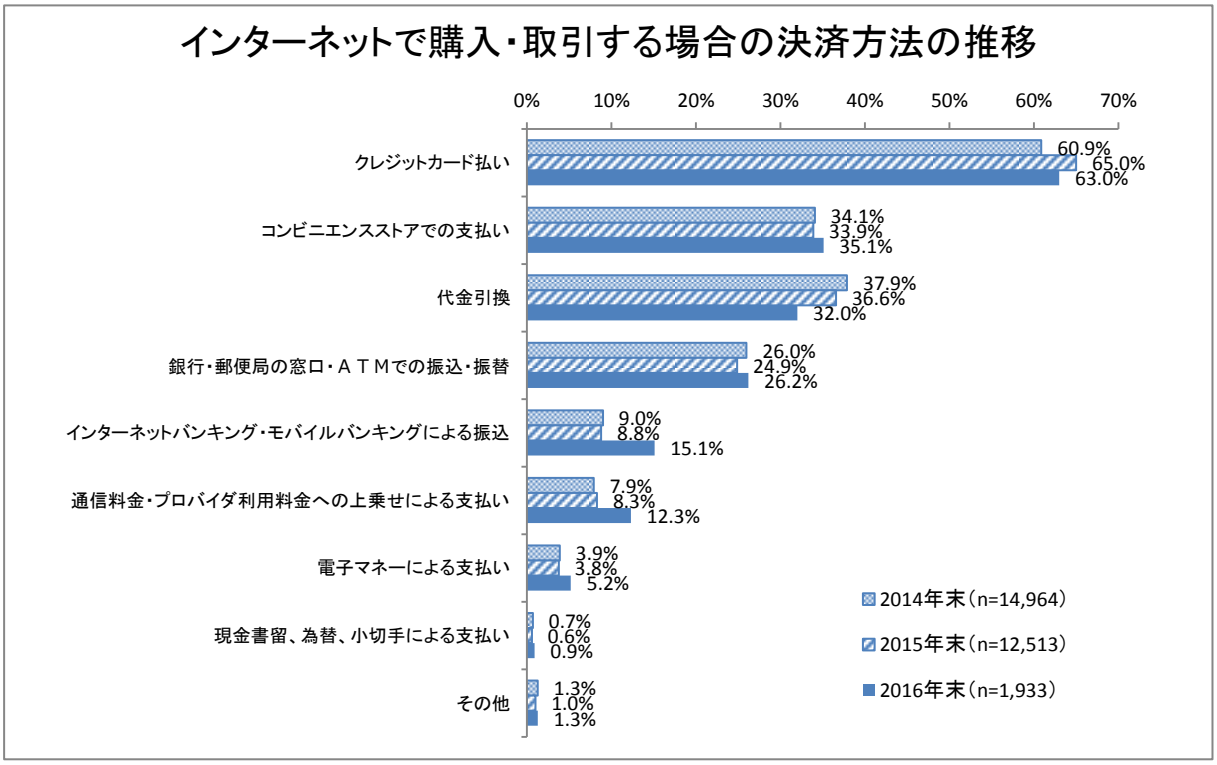
出所：一般社団法人日本クレジット協会「クレジットカード不正使用被害額の発生状況」

（資料５）



出所：経済産業省「平成 28 年度我が国経済社会の情報化・サービス化に係る基盤整備（電子商取引に関する市場調査）」

（資料６）



出所：総務省「平成２８年通信利用動向調査の結果（概要）」

Ａ．クレジットカード情報保護対策の強化に向けた実行計画

１．クレジットカード情報の適切な保護に関する取組について

カード情報[4]の保護は、クレジットカード取引に関わる全ての事業者の責務である。割賦販売法においては、従来カード会社に義務が課されていたが、2018 年 6 月 1 日施行の改正割賦販売法では、加盟店にも義務が課されることになった。

近年、企業や個人を狙ったマルウェアや標的型攻撃によって個人情報やカード情報を窃取し、特殊詐欺や盗んだカード情報を不正に利用する事件が発生している。特にクレジットカードは世界中で利用できることから、カード情報を取り扱う事業者からの情報漏えいにより、偽造カードやなりすましによる不正利用が引き起こされることとなり、その範囲は国内にとどまるものではない。

2017 年においても情報漏えいに起因する偽造被害・なりすまし被害が依然として増加していることから、本実行計画に基づくカード情報保護の取組を加速化させていく重要性がさらに増している。

そもそもカード情報を自社で保持していなければ、カード情報を窃取されるリスクが払拭され、情報漏えいの観点からも最も有効なセキュリティ対策と考えられる。しかし、カード情報を保持しなくても事業を運営できる事業者と、保持しなければ事業を運営できない事業者があるため、各事業者の実態を踏まえた対策を検討することが重要である。具体的には、加盟店においてはカード情報を非保持化することを基本とした取組を第一に検討し、カード情報を取り扱うカード会社及び PSP においては、カード情報保持を前提とした適切な対策の構築が必要である。

加盟店における非保持化に向けた具体的対策を進めるにあたっては、対面取引加盟店と非対面取引加盟店に分けたアプローチをする必要があるが、近時のカード情報漏えい事案の発生状況を鑑みれば、非対面取引の中でも情報漏えいリスクの高い EC 加盟店におけるセキュリティ対策を進めることは、引き続き喫緊の課題である。また、EC 加盟店の委託先事業者が提供する決済ソリューション（ショッピングカート機能等）の脆弱性を要因とした漏えい事案が発生していることに留意が必要である。

カード情報の保護については、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が共同でデータセキュリティの国際基準である PCI DSS[5]（Payment Card Industry Data Security Standard）を策定し、カード情報の安全性が確保できる環境を整えている。カー

---

[4] 「カード情報」とは、クレジットカード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）及び機密認証データ（カード情報を含む全トラックデータ、CAV2/CVC2/CVV2/CID いわゆるセキュリティコード、PIN 又は PIN ブロック）をいう。なお、以下の処理がなされたものはクレジットカード番号とは見做さない。
・トークナイゼーション（自社システムの外で不可逆な番号等に置き換え、自社システム内ではクレジットカード番号を特定できないもの）
・トランケーション（自社システムの外でクレジットカード番号を国際的な第三者機関に認められた桁数を切り落とし、自社内では特定できないもの）
・無効処理されたカード番号

[5] PCI DSS については別紙参照のこと。

ド情報を保持する加盟店やカード会社及び PSP については、PCI DSS への速やかな準拠が求められ、事業者が PCI DSS の内容を正しく理解し効率的に対応する必要がある。そのため、本協議会は、きめ細かい理解増進の取組や具体的な手続き等に対するサポート体制を構築することで、カード情報を保持する事業者における準拠に向けた取組の加速を図る。

さらに、カード情報の漏えいは不正利用につながる可能性が高いことから、漏えいした際の二次被害の防止を図るため、カード情報を漏えいした加盟店等の事業者が必要な対応を速やかに図るためのマニュアル等を整備した。

本実行計画では、2018 年 3 月末までを目標期限として、特にカード情報の漏えいの頻度が高い非対面（EC）加盟店については原則として非保持化（保持する場合は PCI DSS 準拠）を推進するとともに、カード会社及び PSP については PCI DSS 準拠を求めてきた。引き続き、改正割賦販売法の施行を踏まえ、その取組を継続していくこととする。また、対面加盟店については、改正割賦販売法の施行までの対応を基本とし、最終的には、全加盟店が 2020 年 3 月末までにカード情報の適切な保護に関する対応（非保持化又は PCI DSS 準拠）が完了している状態になっていることを目指す。

加盟店は次項に定める非保持化を実現した場合であっても、継続的な情報保護に関する従業員教育やウィルス対策、デバイス管理等について必要なセキュリティ対策が求められる。

また、フィッシングやウィルス感染など、カード会員から直接カード情報等を窃取する手口も存在するため、消費者に対する啓発等も併せて行うことも必要である。

２．加盟店におけるカード情報の非保持化の推進について

本協議会は、加盟店におけるカード情報保護のための第一の対策として非保持化を基本とした取組を推進する。

非保持化は PCI DSS 準拠とイコールではないものの、カード情報保護という観点では同等の効果があるものと認められるため、実行計画においては、PCI DSS 準拠に並ぶ措置として整理する。

実行計画で示す加盟店における「非保持化」とは、カード情報を保存する場合、それらの情報は紙のレポートやクレジット取引にかかる紙伝票、紙媒体をスキャンした画像データ等[6]のみであり、電磁的に送受信しないこと、すなわち「自社で保有する機器・ネットワークにおいて「カード情報」を『保存』、『処理』、『通過』しないこと」をいう（ただし、決済専用端末（CCT（Credit Center Terminal））及びそれと同等以上のセキュリティレベルのもの。以下同じ。）から直接外部の情報処理センター等に伝送している場合を含む。）。

非保持化実現により、仮にマルウェアや標的型攻撃を受けた場合でもカード情報の漏えいを防ぐことができることから、偽造カードやなりすましといったカード不正利用の未然防止

[6] 本実行計画において、①紙（クレジット取引伝票、カード番号を記した FAX、申込書、メモ等）、②紙媒体をスキャンした画像データ、③電話での通話（通話データ含む）においてカード情報を保存する場合には、「保持」とはならない。
注 1）①～③以外において非保持化（同等/相当含む）が実現されていることが前提。
注 2）PCI DSS 準拠を目指す加盟店においては、本実行計画の内容にかかわらず、PCI DSS の基準に則って取組むことに留意する必要がある。

が可能となる。

特に、EC 加盟店の中には、自社サイトにカード情報を含む決済情報等のログが蓄積される等のシステム的課題を認知できていないケースもあることから、これら加盟店に対する注意喚起を行い、さらに、カード情報を保持しないシステム（カード情報非通過型）への移行を強く推奨していくものである。

なお､非保持化(後述の非保持と同等/相当を含む)ソリューションを提供する事業者等は、非保持化を実現した加盟店における顧客照会等の運用実態を踏まえたサービスの提供に留意する必要がある（後述「（３）非保持化実現加盟店における顧客対応」参照)。

（１）非対面加盟店におけるカード情報の非保持化について

①EC 加盟店への対応

PSP を利用する EC 加盟店におけるカード決済システムにおいては、カード情報が EC 加盟店の機器・ネットワークを通過する「通過型」と、通過しない「非通過型」に大別される。

通過型は、カード情報が EC 加盟店の機器・ネットワークを「通過」して「処理」されるため、EC 加盟店に意図せずカード情報が「保存」されることがある。このため、外部からの不正アクセスやマルウェア等により「保存」されていたカード情報又はシステム改ざんや機器の脆弱性により「通過」するカード情報を窃取されるリスクが高く、経済産業省によると 2017 年の 1 年間で報告されたカード情報の漏えい事故（2015 年からの 2 年間で 1.8 倍（※報告ベース））の大半が、この「通過型」の EC 加盟店からのものであった。

一方、非通過型は、カード情報が EC 加盟店ではなく、PSP の機器・ネットワークを「通過」して「処理」され、EC 加盟店はカード情報を「通過」､「処理」､「保存」することはないため、EC 加盟店における非保持化を実現するセキュリティ措置として推奨されるものである。ただし、非通過型の決済サービスを提供する PSP が PCI DSS 準拠済みであることが前提である。

よって、EC 加盟店におけるカード情報の非保持化を推進するため、PCI DSS 準拠済みの PSP が提供するカード情報の非通過型（「リダイレクト（リンク）型」又は「Java Script 型」）の決済システムの導入を促進することとする。なお、非通過型を導入した EC 加盟店において、業務の都合上、PSP 等より還元されたカード情報を保持する場合には PCI DSS 準拠が必要である。

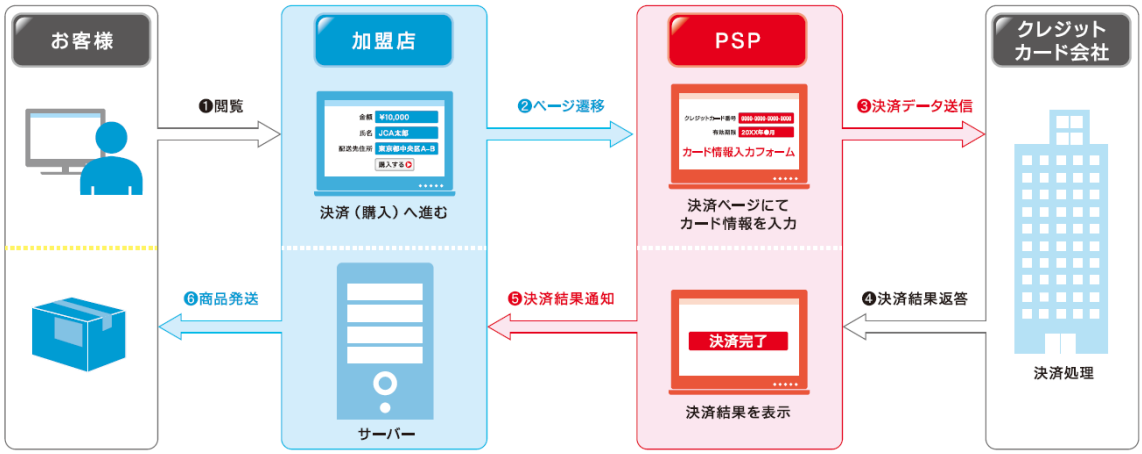
■新規の EC 加盟店

カード会社（アクワイアラー）及び PSP は、新規にクレジットカードを利用して EC 取引を始める加盟店に対して、非通過型の決済システムの導入を強く推奨し、通過型を導入する場合は、カード情報を保持することになるため、PCI DSS 準拠を求める。

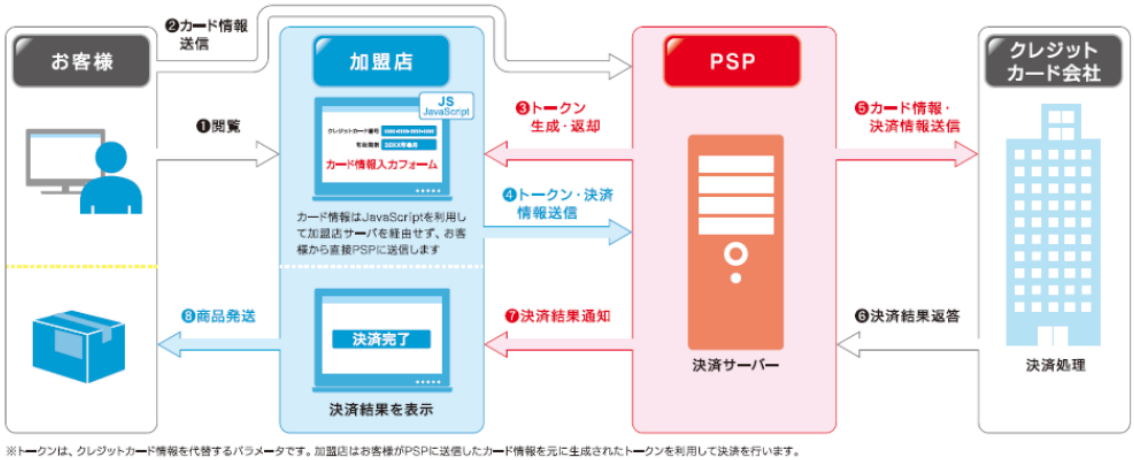
■通過型システムを導入している EC 加盟店

既に通過型を導入している EC 加盟店は、自社サイトにカード情報を含む決済情報等のログが蓄積される等のシステム的課題を認知できていないケースもあることから、カード会社（アクワイアラー）及び PSP は、引き続き加盟店に対する注意喚起を行い、システムログ等の消去を求める。さらに、カード情報を保持しない非通過型への移行を強く推奨する。なお、EC 加盟店において、通過型か非通過型の認識がなく、カード情報の漏えい事故が発覚してから、通過型を採用していたことを認識した事例もあることから、注意が必要であり、カード情報を保持しない非通過型への移行又はカード情報を保持する場合は PCI DSS 準拠を求める。

【非通過型（リダイレクト（リンク）型)】



【非通過型（Java Script 型 ※トークン型の場合)】



②メールオーダー・テレフォンオーダー等の非対面加盟店における非保持化について

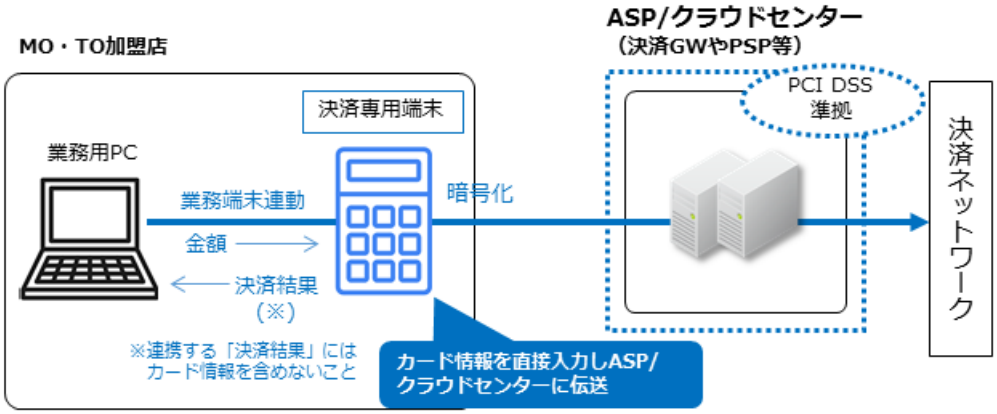
メールオーダー・テレフォンオーダー等の EC 加盟店以外の非対面加盟店（以下「MO・TO 加盟店」という）においては、顧客から電話・FAX・はがき等でカード情報を入手し、MO・TO 加盟店の機器においてカード情報を入力し決済を行うため、カード情報を電磁的情報で自社内に「通過」させない外回り方式を導入することにより、

カード情報の非保持を実現することが可能となる。また、カード番号を特定できない状態とし、自社内で復号できない仕組みとすれば、仮に窃取されてもカード情報として不正に利用することは極めて困難であるため、PCI P2PE[7]（PCI Point to Point Encryption）認定ソリューションを導入することにより、非保持と同等/相当のセキュリティ措置を実現することが可能となる（この場合には、PCI DSS 準拠までは求めないこととする。）。

■外回り方式

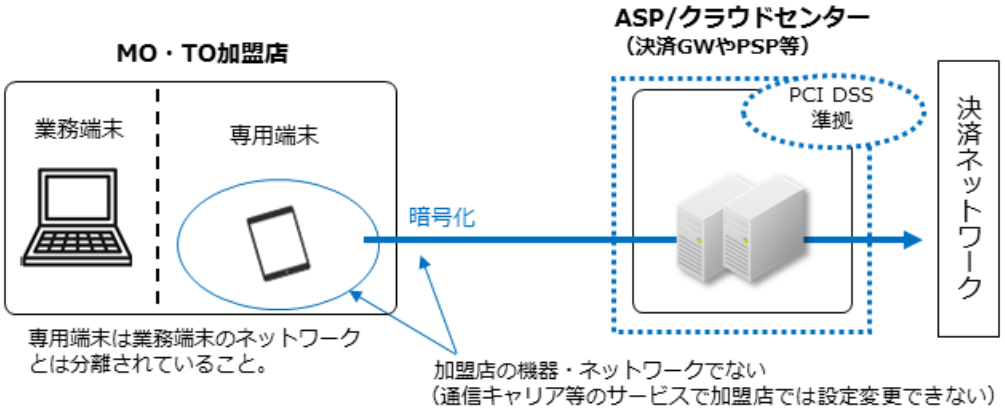
カード情報を紙媒体のまま保存する場合や要件を満たした決済専用端末やタブレット端末を活用した外回り方式[8]（自社で保有する機器・ネットワークにおいて、カード情報を「保存」、「処理」、「通過」しない）にて決済を行う場合には、非保持となる。

【外回り方式（決済専用端末を利用した方式）】



※ASP は Application Service Provider の略

【外回り方式（タブレット端末を利用した方式）】



[7]「PCI P2PE」とは、カードリーダーデバイスから決済処理ポイントまでカード会員データを安全に伝送処理する仕組みで、PCI SSC（Payment Card Industry Security Standards Council）に認定されたソリューション。

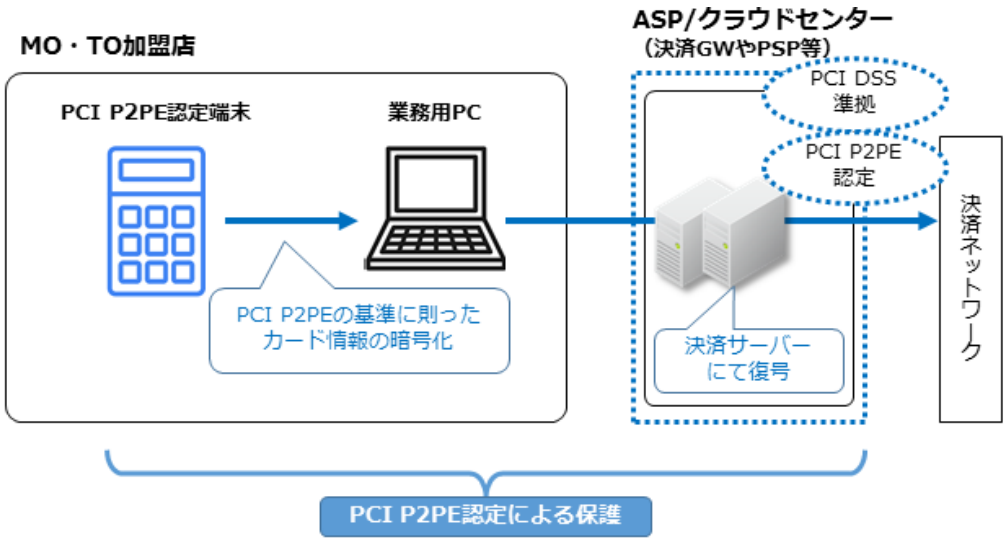
[8] 詳細については「メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて」等を参照のこと。

■内回り方式

MO・TO 加盟店において、PCI P2PE 認定ソリューションを導入した場合には、非保持と同等/相当のセキュリティ措置となる。

なお、カード情報を電磁的情報として、自社で保有する機器・ネットワークにおいて「保存」、「処理」、「通過」する場合においては、PCI DSS 準拠を求める。

【内回り方式（PCI P2PE 認定端末を利用した方式）】



（２）対面加盟店におけるカード情報の非保持化について

対面加盟店におけるカード情報の非保持化の推進は、特に POS システムを導入している加盟店において課題となる。カード情報を電磁的情報で自社内に「通過」させないよう、POS の機能と決済機能を分離すること、IC 対応した決済専用端末からカード情報を電磁的情報で自社内に取り込まない外回り方式（決済専用端末連動型・ASP/クラウド接続型（外回り方式））を導入することにより、カード情報の非保持化を実現することが可能となる。また、カード番号を特定できない状態とし、自社内で復号できない仕組みとすれば、仮に窃取されてもカード情報として不正に利用することは極めて困難であるため、PCI P2PE 認定ソリューションの導入又は本協議会において取りまとめた技術要件に適合するセキュリティ基準（11 項目）[9]を満たすことにより、非保持と同等/相当のセキュリティ措置を実現することが可能となる（この場合には、PCI DSS 準拠までは求めないこととする。）。

ただし、カード会社や ASP/クラウドセンター等を運営する事業者より、カード情報の還元を受け自社で保有する機器・ネットワークにおいて「保存」、「処理」、「通過」している場合（決済以外の目的の場合も含む）には、カード情報を保持している扱いとなる。

■決済専用端末連動型・ASP/クラウド接続型(外回り方式)

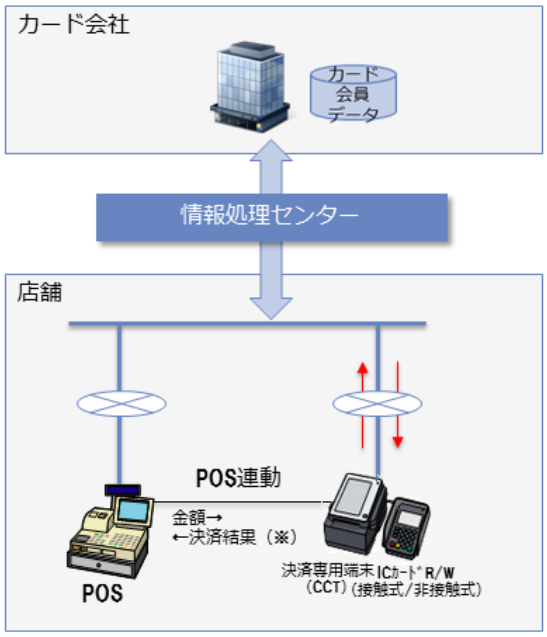
[9] 詳細については「対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について」を参照のこと。

「決済専用端末連動型」・「ASP/クラウド接続型」（外回り方式）は、加盟店あるいはカード会社等が所有する決済専用端末から直接外部の情報処理センター又は ASP/クラウドセンター等に伝送される方式である。

両方式とも、決済機能は POS システムの外側となるため、オーソリゼーションやクレジットカードの売上処理は、カード情報を POS 端末や POS システムの機器・ネットワークに「保存」、「処理」、「通過」せずに行われ、カード情報の非保持化が実現できる。

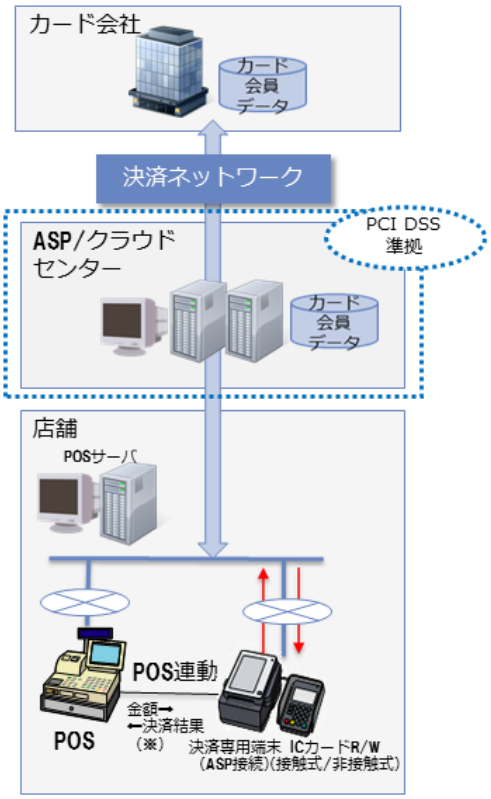
なお、POS システムを導入せず「IC 対応した決済専用端末」のみを使用し、直接外部の情報処理センター等に伝送している加盟店も非保持となる。

【決済専用端末（CCT）連動型（外回り）】



※POS 連動する「決済結果」にはカード情報を含めないこと

【ASP/クラウド接続型（外回り）】



■ASP/クラウド接続型（内回り方式）

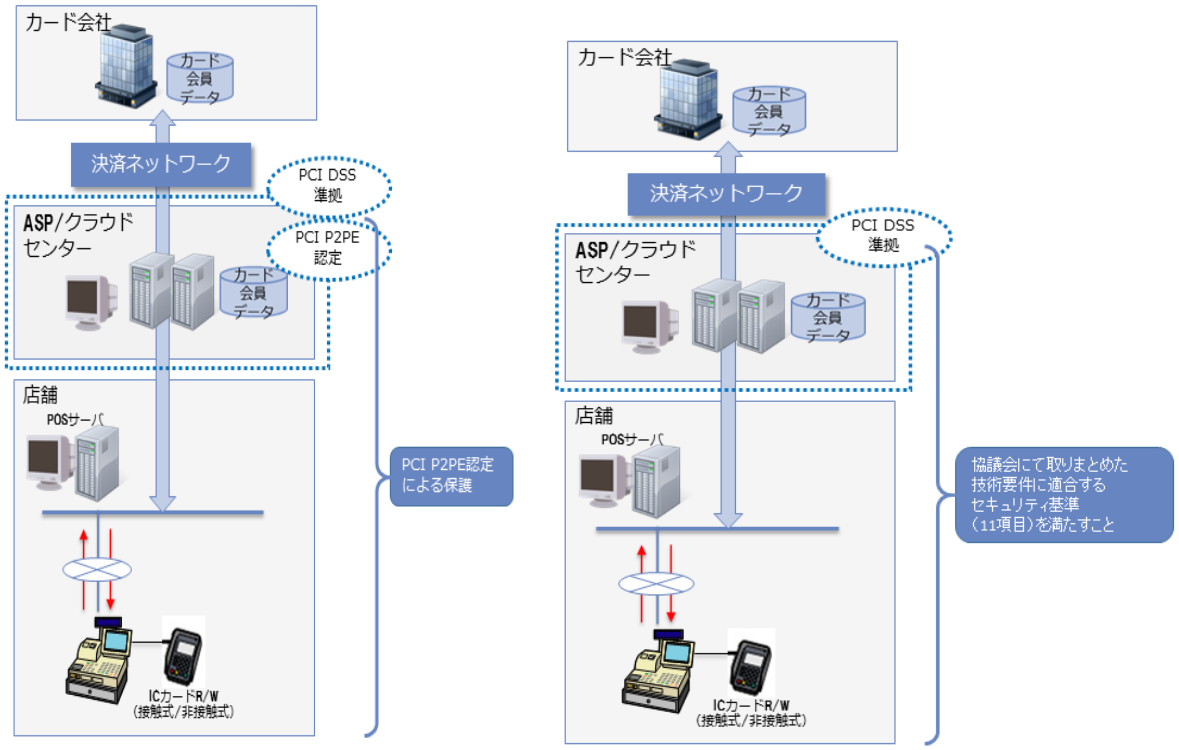
オーソリゼーションやクレジットカードの売上処理のため、カード情報が決済端末から POS システム又は社内システムを介して外部の情報処理センター又は ASP/クラウドセンター等を運営する事業者等外部事業者へ伝送される方式である。

この場合、カード情報が自社内機器・ネットワークを「保存」、「処理」、「通過」するため、PCI DSS 準拠が必要となる。

非保持と同等/相当のセキュリティ措置としては、PCI P2PE 認定ソリューションの導入又は本協議会において取りまとめた技術要件に適合するセキュリティ基準（11

項目）を満たすことが求められる。

【ASP/クラウド接続型（内回り）】



（３）非保持化実現加盟店における顧客対応

現在、クレジットカードを利用した顧客からの返品や購入金額の訂正等の照会に対しては、カード番号等を用いて加盟店とカード会社間で対応している。

非対面加盟店においては、通常 PSP がカード情報を保有しているため、カード情報を非保持化した場合でも、PSP が仲介を行うことで従来どおり対応が可能である。

対面加盟店のうち決済専用端末を導入している加盟店においては、カード番号の一部非表示化が図られており、一部非表示化されたカード番号に加え、利用日、利用金額、端末番号、伝票番号等による照会が行われている。

非保持化実現時の照会等対応において、伝票番号、取引日時、金額等その他カード番号以外の取引を特定するための照会キーはあるものの、カード番号以外の照会キーのみでは対象取引を特定できないこともある。また、全ての加盟店・カード会社が一律、同レベルの対応を行うことは現状困難であるため、カード番号を基本として双方照会する必要がある。

実行計画上の非保持化（非保持と同等/相当を含む）を実現した加盟店が顧客照会等の際、クレジットカード取引にかかる紙伝票（加盟店控え、お客様控え）等の紙媒体を利用する方法や、PCI DSS に準拠した ASP/クラウドセンター等を運営する事業者が提供するセキュリティ対策が施された環境に加盟店がアクセスし、一時的にカード番号を入手・利用する方法は、非保持化後も認められる。なお、各加盟店の運用実態は異なり、顧客対応

についても一律的な対応とすることは困難であることから、運用上の課題については各加盟店、カード会社、必要に応じて ASP 事業者等が連携の上、個別に検討を進めることが重要である。

（４）非保持化実現加盟店における過去のカード情報保護対策

非保持化（非保持と同等/相当を含む）を実現した加盟店において、電子帳簿保存法に基づく管理が求められ、非保持化対応完了以前に取り扱った過去のカード情報を画像データ以外のテキスト形式等で電子帳票として保存する場合、本協議会にて定めたセキュリティ対策[10]を行う必要がある。

３．PCI DSS 準拠の推進について

本協議会は、日本カード情報セキュリティ協議会等（以下「JCDSC 等」という）とともに、PCI DSS に関する認知度を向上させるためのセミナー開催等による周知・啓発活動の推進と、その準拠に向けた加盟店等の取組をサポートするための体制の構築に継続して取組む。

（１）PCI DSS に関する認知度の向上及び準拠への取組促進に向けた情報提供

本協議会は JCDSC 等の協力を得て、クレジットカード取引に関係する各事業者の PCI DSS 準拠への取組促進のため、PCI DSS に関するセミナーの開催等の周知・啓発活動を行う。

（２）PCI DSS 準拠に向けた加盟店等へのサポート体制について

JCDSC 等は本協議会と協力して、カード情報を保持する加盟店等が PCI DSS 準拠に向けた円滑な対応を図ることをサポートするため、以下の対応に取組むこととする。

①PCI DSS に関する理解促進のための講師派遣

カード会社向け、関係業界団体・加盟店等向けに PCI DSS の内容や準拠に向けた手続き等に関する理解促進を図るための講師派遣を行う。

②PCI DSS に関する理解促進のためのコンテンツの提供・展開

・加盟店等向けの PCI DSS に関する基礎的資料（規格内容、解説、FAQ 等）を提供する。

・各種説明会等で使用する資料（コンテンツ）を作成し提供する。

・自社システムの現状理解に資する簡易な自己診断票を作成し提供する。

③相談窓口の設置

・PCI DSS に関する質問や意見、問い合わせ等を送付できる専用窓口（http://www.jcdsc.org/inquiry.php）を JCDSC サイトに開設し、関係業界団体、加盟店等の問い合わせ、説明会の開催依頼等の要望に応えられるようにする。

④加盟店等向けの PCI DSS 準拠に向けた分かりやすいツール等の用意

[10] ネットワークを利用しない「スタンドアローン環境」での保管・利用することが必須条件。詳細については、「非保持化実現加盟店における過去のカード情報保護対策」を参照のこと。

・相談者が理解しやすいよう認定審査機関（QSA[11]（Qualified Security Assessor））各社の特徴等を記載したリスト等を作成し、JCDSC サイト（http://www.jcdsc.org/qsa-asv.php）を通じて提供する。

⑤専門人材の育成

・PCI DSS 準拠に取組む加盟店等へのサポートニーズの拡大に対応するため、QSA の人員体制の整備・拡充を図る。

・PCI DSS 準拠に関し、QSA による審査に代替し得る内部監査を行うことのできる専門人材として、**ISA**[12]（Internal Security Assessor）等の人材育成を支援する。

4．カード情報を取り扱う事業者の PCI DSS 準拠の推進について

カード情報を取り扱うカード会社及び PSP については、業務上大量のカード情報を管理・利用しており、クレジットカード取引に係るインフラの一端を担う重要な役割に鑑み、PCI DSS 準拠は当然の責務である。仮に、このような重要なポジションを占める事業者が PCI DSS に準拠しない場合、クレジットカード取引システム全体への脅威ともなりかねないことから確実な対応が必要である。なお、カード会社・PSP 以外のカード情報を取り扱っている事業者も同様である。

これらカード情報を取り扱う事業者については、PCI DSS 準拠に加えて、巧妙化するサイバー攻撃への対応を含むセキュリティ対策の改善・向上・維持に向けた継続的な取組が重要であることを認識する必要がある。

5．カード情報漏えい時の対応について

加盟店からカード情報が漏えいした際に被害の拡大を防ぐために、取引に関係するカード会社及び PSP は早急にリスク回避に向けた行動を起こす必要がある。具体的には、日本クレジット協会において策定した加盟店におけるカード情報漏えい時の緊急対応マニュアルを有事の際の参考にしつつ、二次被害の防止に努めることとする。

また、カード情報の漏えい事案が発生した加盟店は、被害の拡大を防止するために初動対応として漏えい元（データベース等）のネットワークからの切り離し、一旦カード決済を停止する等の措置及び PCI DSS 準拠等再発防止のための適切な措置を講じる。

カード決済の再開については、契約カード会社（アクワイアラー）は、再発防止のための措置等の対応状況を十分に確認する必要がある。なお、PCI DSS 準拠等の再発防止のための適切な措置の具体的な内容は、当該加盟店と契約カード会社（アクワイアラー）及び PSP で協議の上で決定することとする。

---

[11] PCI SSC に認定された認定セキュリティ評価機関。加盟店やサービス・プロバイダーへのインタビューやドキュメント、サーバーなどの訪問審査を正式に行うことができる。

[12] PCI SSC によるトレーニングと証明書を受領して、組織の内部の PCI DSS 自己評価を行うことができる内部監査人のこと。ISA の資格を取得している内部監査人がいる企業は、QSA の審査を受けずに PCI DSS の準拠が可能となる。

６．各主体の役割について

カード情報の適切な保護を推進するためには、カード情報を取り扱う事業者全てが自主的な取組を進めることが重要である。

なお、各主体がカード情報を取り扱う業務を外部委託する場合は、委託者自身が委託先のセキュリティ状況を確認し、責任を持って PCI DSS 準拠等の必要な対策を求めていくこととする。また、複数の委託者からカード情報を取り扱う業務を受託する又はショッピングカート機能等のシステムを提供する事業者は、自社システムにおけるカード情報の保持状況について確認の上、PCI DSS 準拠等の必要な対策を行うことが求められる。

以下、各主体に求められる役割等について整理する。

（１）加盟店

・非対面加盟店は、カード情報の適切な保護に関する対応（非保持化又は PCI DSS 準拠）が求められ、引き続き、改正割賦販売法の施行を踏まえ、その取組を継続する。対応済みの非対面加盟店においては、情報漏えい防止のためのセキュリティ対策を維持・運用する。

・対面加盟店においても、改正割賦販売法施行までの対応を基本とし、最終的には、全加盟店が 2020 年 3 月末までにカード情報の適切な保護に関する対応（非保持化又は PCI DSS 準拠）が完了している状態になっていることを目指す。なお、各加盟店において、PCI DSS 準拠に向けて対応を進めるにあたっては、情報漏えいやそれに伴う不正利用が発生している現状を鑑み、早急に対処する必要があることから、カード会社（アクワイアラー）や QSA と連携しつつ、情報漏えいリスクの高いところから優先的にカード情報保護対策の強化に取組むことが重要である。対応完了後は情報漏えい防止のためのセキュリティ対策を維持・運用する。

・非対面及び対面取引の両方を行う加盟店における対面取引に係るシステムについては、上述のとおり、最終的には、全加盟店が 2020 年 3 月末までにカード情報の非保持化又は PCI DSS 準拠が完了している状態になっていることを目指す。

・カード情報の保護においては、カード情報の窃取を企図する者の最新の攻撃手口等の情報を踏まえて、不断に自社のセキュリティ対策の改善・強化を図る。

（２）カード会社

・カード情報を取り扱うカード会社は、外部からの不正侵入やカード情報の外部への漏えい等といった外的脅威によるリスクを極小化し、かつ予見される様々なリスクに厳格に対処するため PCI DSS に準拠し、これを維持・運用する。このほか、関係法令・ガイドライン等を参照し、リスクに応じた必要なセキュリティ対策を講じるとともに、適切な管理・運用を行う。

・カード会社（アクワイアラー）は、PSP と連携の上、加盟店に対しカード情報保護対策について必要な助言や情報提供等を行い、非保持化又は PCI DSS 準拠完了を推進する。

・カード会社（アクワイアラー）は、PCI DSS 準拠を完了していない PSP がある場合に

は可及的速やかに準拠を完了するよう必要な指導を行う。なお、カード会社（アクワイアラー）は、PCI DSS に準拠していない PSP との取引の見直しについて検討を進める。

・なお、EC 加盟店や決済サービスを提供する PSP の中には、セキュリティ対策に関する意識が低い者も少なくないことから、本実行計画の推進にあたっては、これら加盟店、PSP への丁寧な対応に留意する。

・カード会社（イシュアー）は、フィッシングやウィルス感染など、カード会員から直接カード情報等を窃取する手口も存在するため、消費者に対する注意喚起及びセキュリティ対策の必要性等の啓発を行う。

（３）PSP

・カード情報を取り扱う PSP は、カード会社（アクワイアラー）と同様、PCI DSS に準拠し、これを維持・運用する。

・PSP は、カード会社（アクワイアラー）と協力して、加盟店に対しカード情報保護対策について必要な助言や情報提供等を行い、その取組を支援する。

（４）国際ブランド

・我が国のクレジットカード取引の実態を踏まえ、本実行計画に掲げるカード情報保護対策の実現に向け、国際ブランドの各種ルール等との調整を行い、各種課題の解決に向けて関係事業者と協働して取組む。

・グローバルな観点から、海外におけるカード情報保護に関するリスクや各種課題、我が国における国際水準のセキュリティ環境の整備の必要性等について、事業者向けや消費者向けの情報共有・発信に取組む。

（５）行政・業界団体等

・行政は、改正割賦販売法によりカード情報の適切な管理が加盟店にも義務付けられることを踏まえ必要な措置が確実に導入されるよう、カード会社（アクワイアラー）等を通じた加盟店に対する指導を徹底する。また、国際ブランド等と協力して、本実行計画の着実な実施に向け、事業者向けや消費者向けの情報発信に取組む。

・日本クレジット協会は、カード会社（アクワイアラー）と連携し、改正割賦販売法の施行を踏まえ、本実行計画に掲げるカード情報保護対策の必要性について加盟店に対する周知活動を徹底するとともに、加盟店の業界団体、消費者団体等との連携を強化し、事業者・消費者向けの情報発信に取組む。

・日本クレジット協会は、行政と連携の上、他の情報セキュリティに係る関係機関との連携・情報共有を図り、クレジット取引に関係する事業者等に対して適時情報発信を行う。

・政府の情報セキュリティ政策会議において、クレジット分野は、国の重要インフラの一つに指定されており、「重要インフラ情報セキュリティ第 4 次行動計画」（2017 年 4 月 18 日付）に基づき、官民連携による重要インフラ防護を推進していく。具体的な取組としては、「クレジット CEPTOAR における情報セキュリティガイドライン」に基づき、重要インフラ事業者における安全基準等の整備・浸透、情報共有体制の強化等を図るこ

ととする。

7．2018 年度中に重点的に実施すべき具体的な取組について

2018 年度では、以下の具体的な取組により、各主体における取組を加速化させていくこととする。

（1）非対面加盟店向けのカード情報保護対策の推進、周知活動の強化

・EC 取引におけるカード情報の漏えいの発生状況等を踏まえ、EC 加盟店においては非通過型の導入を基本とする取組を確実に実施し、委託先事業者については PCI DSS 準拠等必要な対策を講じる。

・非対面加盟店は、カード会社（アクワイアラー）・PSP と連携の上、必要に応じて日本クレジット協会が開催する説明会・セミナー等を活用しつつ、カード情報保護対策の取組を推進する。

・日本クレジット協会は、2018 年度版の実行計画で追記された MO・TO 加盟店におけるカード情報保護対策の具体的内容について、公益社団法人日本通信販売協会や PSP 等サービスプロバイダーと連携し、MO・TO 加盟店への周知活動の強化に努める。日本通信販売協会に属さない中小事業者等への周知活動にも留意する。

・日本クレジット協会は、行政と連携し、非対面加盟店向けに決済ソリューションを提供する PSP 等サービスプロバイダー向けの説明会・セミナーを開催し、改正割賦販売法及び本実行計画に基づくカード情報保護対策を引き続き推進する。

（2）対面加盟店向けのカード情報保護対策の推進、周知活動の強化

・対面加盟店は、カード会社（アクワイアラー）と連携の上、必要に応じて日本クレジット協会が開催する事例セミナー等を活用しつつ、カード情報保護対策の取組を推進する。

・日本クレジット協会は、加盟店業界団体や情報処理センター等の協力を得て、対面加盟店向けのカード情報保護対策を推進するための事例セミナー等を開催し、最新の動向について情報共有を行う場を提供することを通じて、改正割賦販売法及び本実行計画に基づくカード情報保護対策を引き続き推進する。

（3）本実行計画と PCI DSS 基準の関係についての理解促進

・本実行計画では、加盟店におけるカード情報保護対策として「非保持（同等/相当を含む）」を達成した場合には PCI DSS 準拠を不要としているが、非保持（同等/相当を含む）に加え、事業者の判断で PCI DSS 準拠することを否定するものではない。

・カード情報を取り扱う事業者が PCI DSS に準拠する場合には、本実行計画の内容にかかわらず、全ての PCI DSS 要件（12 要件）を満たすことが求められる。関係事業者においては、こうした本実行計画と PCI DSS 基準の関係性についても理解の上、カード情報保護の対策を推進する。

（４）カード情報保護対策に関する状況把握と新たな共有すべき課題への対応

日本クレジット協会は、カード会社、PSP 及び加盟店におけるカード情報保護対策の取組状況の把握に努める。加盟店におけるカード情報保護対策の状況把握については、カード会社（アクワイアラー）及び PSP と連携の上、これを実施する。また、実行計画を推進する上での新たな共有すべき課題等がある場合には、本協議会において必要な検討を行う。

B．クレジットカード偽造防止による不正利用対策の強化に向けた実行計画

１．クレジットカードの IC 取引の実現に向けた取組について

我が国のクレジットカード取引は、いまだ磁気情報での取引が大半を占めており、犯罪組織等がその情報を窃取し偽造カードを生成して不正に利用される被害が後を絶たず、その対策として IC 取引を推進することが喫緊の課題である。また、海外では大手加盟店の POS システムがウィルスに感染し、そこで決済したカード情報を含む顧客情報が大量に窃取されるという事案が頻発していることを受け、特に最大の被害国である米国では偽造カードによる不正利用対策として IC 対応が急速に進められている。

今後、2020 年のオリンピック・パラリンピック東京大会に向けて、訪日外国人の更なる増加が見込まれるが、海外、特に欧州等ではほぼ 100%が IC 取引となっており、磁気情報による取引の継続は我が国のクレジットカード取引のセキュリティ対策が脆弱であるとの印象を与え、安全・安心を求める訪日外国人の需要の取込を阻害する要因にもなりかねない。

加盟店等においてカード情報を窃取されたとしても窃取された情報を用いて偽造 IC チップを生成することが困難であること等の利点から、現状では、IC 取引の実現が、カードの偽造防止の唯一無二の対策である。

クレジットカード業界においては2000年代からICクレジットカードの発行を進めているが、クレジットカードの IC 化率は 2017 年 12 月末時点で、2020 年 3 月までに 100%IC 化する目標に対し、77.3%[13]となっており、2020 年 3 月に向けて早急に取組を進めていくべきである。改正割賦販売法により、加盟店における不正利用防止措置が義務づけられ、その具体的措置として IC 対応が求められることとなるが、偽造カードによる不正利用を防止するためには、カードの IC 化も伴ってその効果が最大限に発揮されることから、IC カードへの切替えを加速化していくことが強く求められる。

また、加盟店における IC 端末の整備においても、CCT（Credit Center Terminal）等の決済専用端末の IC 対応により中小の加盟店[14]を中心に順調に進捗しているものの、POS システムを導入している比較的大型の流通業の加盟店における IC 対応が課題となっている。POS システムが各加盟店によってカスタマイズされた仕様になっていることから、決済システム・店頭の端末の IC 対応への移行費用や業務運用等の対応が負担となる点が大きな課題となっている。

しかし、前述の諸外国における IC 対応の普及状況を踏まえれば、各事業者においては、これ以上、我が国の IC 対応が遅れれば、世界の中で日本がセキュリティホールとなる蓋然性は極めて高いとの危機感を持って早急に IC 対応を進める必要がある。

---

13 日本クレジット協会が会員企業 234 社に対して国際ブランド付きカードを対象として行った調査の結果、2017 年 12 月末時点で 100%IC 化を達成している企業は 84 社。

14 平成 27 年度予備費により、IC 対応の決済端末の導入も支援対象とする「軽減税率対策補助金」を措置しており、その活用促進に向けた周知を図ることで、中小加盟店における IC 対応を支援する。
（平成 28 年度第 2 次補正予算では、「地域未来促進事業（うち、商店街・まちなか集客力向上支援事業）」や「小規模事業者販路開発支援事業（小規模事業者持続化補助金）」においても支援の対象としている。）

なお、POS システムの IC 対応の改修を図る際に、カード情報保護対策を同時に行うことで、加盟店におけるシステム投資のコスト低減が期待できる。

改正割賦販売法が 2018 年 6 月 1 日に施行されることを踏まえ、決済端末の IC 対応についても、その時までの対応を基本とし、最終的には、全加盟店が 2020 年 3 月末までに IC 対応が完了していることを目指す。

２．IC 取引時のオペレーションルール・ガイドラインについて

（１）IC 取引時のオペレーションルール

本協議会では、IC 取引の普及の前提となる接触・非接触の IC カード及び IC 対応決済端末による取引におけるオペレーションルールの検討を行った。本協議会での検討結果を踏まえ、国際ブランドとの最終調整を経てルールが確定し、我が国のクレジットカード業界としてのルールとして「IC 取引時のオペレーションルール」を策定した。カード会社・加盟店及び機器メーカー等は、当該ルールに基づいて対応することとする。

また、これを受け、クレジットカード業界では、日本クレジット協会により、会員カード会社向けのガイドラインとして「IC 取引における本人確認方法に係るガイドライン」及び「本人確認不要（サインレス/PIN レス）取引に係るガイドライン」を策定している。

なお、訪日外国人が使用する海外発行のクレジットカードの場合、海外カード会社（イシュアー）のセキュリティ設定により、国内の加盟店での IC 取引において本人確認方法等についてオペレーションが異なる場合があることに留意する。

（２）IC カード対応（EMV）POS ガイドライン

本協議会では、POS の IC 対応に係る具体的な方策ごとに技術面・コスト面の観点からコスト構造を可視化し、その上で、ソフトウェアの共通化等によるコスト低減策を取りまとめるとともに、今後 IC 対応を図る加盟店等の円滑な移行に資するため、IC 取引におけるオペレーションに関するルールを策定した。

これらの成果を含め、POS 端末を製造する機器メーカー向けに、「接触型 IC 取引」を対象とした「IC カード対応 POS ガイドライン」（初版）を策定した（今後、本ガイドラインを順次改訂予定)。さらに、今後の接触型と非接触型の POS 端末の同時導入を志向するニーズに応えるため、「非接触型 EMV 対応 POS ガイドライン」を新たに策定し、関係カード会社、加盟店等に周知した。

（３）IC 取引における本人確認方法

①接触 IC 取引

接触 IC 取引の導入の目的はセキュリティ向上であり、カード偽造防止のみならず、紛失・盗難カード被害の抑制のためには、「オフライン PIN（Personal Identification Number、暗証番号のこと)」[15]が我が国の決済システムを考慮すると現状では最適な本

[15] 「オフライン PIN」とは、カード利用時に会員が入力した数字と、カードの IC チップ内に保存された

人確認方法である。また、現在 130 万台を超える IC-CCT 端末設置加盟店では、「オフライン PIN」をクレジットカード業界として推進してきたことを踏まえ、接触 IC 取引における本人確認方法を以下のとおりとする。

・原則オフライン PIN とする。そのため、日本国内の端末はオフライン PIN 機能及び（磁気カードへの対応のため）サイン機能の装備を必須とする[16]。また、国内（国内イシュアー発行カード）取引については、原則オフライン PIN での取引を実現するために、日本国内のイシュアーは、IC チップの設定上、オフライン PIN を必須とする。

・ただし、PIN の取得が売場形態等の事由により、PIN による本人確認をただちに行うことは困難であり、IC 取引普及の阻害要因となりうるケースにおいては、PIN 対応への措置を継続検討していくことを前提に、当面の間、例外として接触 IC 取引においてもサインによる本人確認を許容する。

例 1）飲食店等のテーブル決済 等

例 2）既にサインを前提とした端末設置加盟店 等

・PIN 入力スキップ機能（PIN バイパス）は、会員の PIN 忘れ等の一時的な救済機能としてカード会員の申し出に基づいて行われているが、海外カード会社（イシュアー）のカード等の利用では、PIN バイパスを許容しないカードも存在し利用阻害が発生することや、PIN バイパスによって本人確認を実施しない場合において不正利用の被害が発生していることを踏まえ、本協議会では、目的外の利用制限、代替策による対応を含め将来的な廃止に向け継続検討する。

②非接触 IC 取引

非接触 IC 取引の形態は「モバイル型」や「カード型」に限らず、「キーホルダー型」「ウェアラブル型」等がある。

非接触 IC カードの取引の多くは CVM[17]リミット金額以下になることが想定されるため、消費者の利便性も勘案し、以下のとおりとする。

・CVM リミット金額以下は、本人確認不要とする。

・CVM リミット金額超は、以下のとおりとする。

1）モバイル型等での取引では、原則 Consumer Device CVM（モバイル端末等における認証（モバイル PIN/指紋等））とする。

2）カード型等での取引では、日本国内の端末・ネットワークが現状オフライン PIN 機能環境[18]にあり、非接触 IC 取引におけるオンライン PIN 入力に対応できないことを考慮し、当面の間、サインとする。

PIN とを照合するものであり、一方、オンライン PIN は、オンラインネットワークを経由してカード会社(イシュアー)のシステム上で照合するものである。

16 現在 POS で読み取りしている磁気カード処理は IC カード R/W 処理を行うこととする。

17 「CVM（Cardholder Verification Method）リミット金額」とは、本人確認不要上限金額のこと、当該金額までの取引であれば本人確認を不要とする。

18 接触 IC 取引、非接触 IC 取引共に「オンライン PIN」の導入については、国際的な決済インフラの状況を見つつ、将来的な課題とする。

ただし、セキュリティ確保の観点から、PIN 入力が望ましいことを踏まえ、接触 IC 取引の PIN 入力に誘導する仕様の実効性について、技術的・運用的な観点等により継続して検討するものとする[19]。

・そのため、日本国内の端末は「No CVM（本人確認不要）機能」「Consumer Device CVM 機能」「サイン機能」の装備が必要となる。

（４）本人確認不要（サインレス/PIN レス）加盟店のオペレーション

①本人確認不要加盟店の是非

取引の安全性が確保できる環境であることを前提に、例外的な取引として既存の磁気取引におけるサインレス売場での IC 対応推進の観点において、接触 IC 取引についても、本人確認不要取引を認める。

なお、接触 IC での本人確認不要取引を実現させるための具体的な端末の実装方式としては、セレクタブルカーネルコンフィグレーション方式を採用する。セレクタブルカーネルコンフィグレーション方式とは、決済アプリケーションの機能により取引単位で端末の機能（本人確認方法）を切り替える EMV カーネル[20]の実装方式であり、EMV 仕様に準拠しつつ、PIN 対応、サイン対応の両方の取引を一つの装置で実現する方式である。

本方式により、原則オフライン PIN の考え方に則り、CVM リミット金額以下は本人確認不要取引を認めつつ、CVM リミット金額超ではオフライン PIN での本人確認が実現可能となる。

今後、機器メーカー等において、本方式の実装に取組むこととする。

②本人確認不要加盟店の対象及び本人確認不要加盟店での除外商品

従来の磁気取引において、一部例外的に実施しているサインレス取引の売場等を前提に、本人確認を求めることがクレジットカード取引の阻害要因となり、また本人確認が不要となることにより決済処理の迅速性が増し、クレジットカード取引（キャッシュレス化）の普及に寄与する業種/業態を本人確認不要加盟店の対象とする。

ただし、不正利用のリスクが低い業種/売場等であることを前提とし、不正利用防止の観点から換金性の高い商品を除外する。

③CVM リミット金額

磁気取引・接触 IC 取引・非接触 IC 取引の種別による CVM リミット金額の差異が加盟店オペレーションの混乱を誘発しないよう、本人確認不要加盟店における CVM リミット金額は統一することが望ましい。

---

[19] 接触 IC 取引の PIN 入力に誘導する以下の仕様の実効性について以下の検討が必要。
①カード会社（イシュアー）のセキュリティ設定により、非接触 IC カードの IC チップの設定上、非接触 IC から接触 IC へ切替させる設定が可能だが、端末機能として、EMV 仕様に基づき、接触 IC へ切替（誘導）するガイダンスを表示する等対応が必要であること。
②CVM リミット金額超において、加盟店が「同一カードに非接触と接触 IC の両方が搭載されたカード」は、「接触 IC 機能を有する端末」で、「接触 IC 取引へ誘導」することを選択可能とすること。

[20] 「EMV カーネル」とは IC クレジット決済処理を行うために必要な処理等を行うためのソフトウェア。

よって、現在の磁気取引において一部例外的に実施しているサインレス取引の売場等の既存加盟店における設定金額に一定の配慮をしつつ、各国際ブランドと協議を行った結果、上記②の換金性の高い商品を除き CVM リミット金額の基準となる金額を定め、それ以下は本人確認不要とすることとした。

④本人確認不要加盟店でのオーソリゼーションの要否

紛失・盗難のリスクを踏まえたセキュリティの確保の観点から、オーソリゼーションを実施すべきであるため、接触 IC 取引は全件オンラインオーソリゼーションを必須とする。

（５）特定業界向けの IC 対応指針の策定

ガソリンスタンドにおける IC 対応については、フルサービススタンドでの車内精算等日本固有の商慣習、セルフスタンドでの給油機一体型の自動精算機、その他防爆準拠（消防法等）の課題があり、現行の決済インフラやオペレーションの全てを国際基準に則った環境とすることは、現状困難[21]であることを踏まえ、2020 年時点での IC 対応における実現可能な方策を示した「国内ガソリンスタンドにおける IC クレジットカード取引対応指針」を取りまとめた。

また、国内での業務特性や設置環境等のため広く普及しているオートローディング方式の自動精算機については、国際的なセキュリティ基準である PCI PTS[22]に準拠することは技術的に難しいことから、代替コントロール事例を示す「オートローディング式自動精算機の IC 化対応指針と自動精算機の本人確認方法について」を取りまとめた。（別途、鉄道事業者向けの指針を取りまとめた）。

３．コスト低減を踏まえた POS システムの IC 対応に関する方策について

POS システムの IC 対応を推進するため、IC 対応手法について技術面、コスト面からの整理を行った。

（１）各方策の検証について

IC 対応に関し、各加盟店の現行システムや店頭オペレーション等の特徴を踏まえ、コスト負担の低減が図れる方法について、決済専用端末（CCT）連動型、決済サーバー接続型、ASP/クラウド接続型に大別[23]し、EMV カーネルを加盟店のシステムの外側に置くことで IC 対応しやすくするものとして、各パターンのコストを可視化し、各方法の技術面等の検証・整理した。

---

[21] セルフスタンドでの給油機一体型自動精算機の PCI PTS 準拠機器、及びフルサービススタンドでの車内精算時使用の防爆準拠（消防法等）ハンディ型端末機器が存在しないこと。

[22] 「PCI PTS（Pin Transaction Security）」とは、PCI SSC が定めた、PIN 取引を保護する PIN 入力装置の国際的なセキュリティ基準。

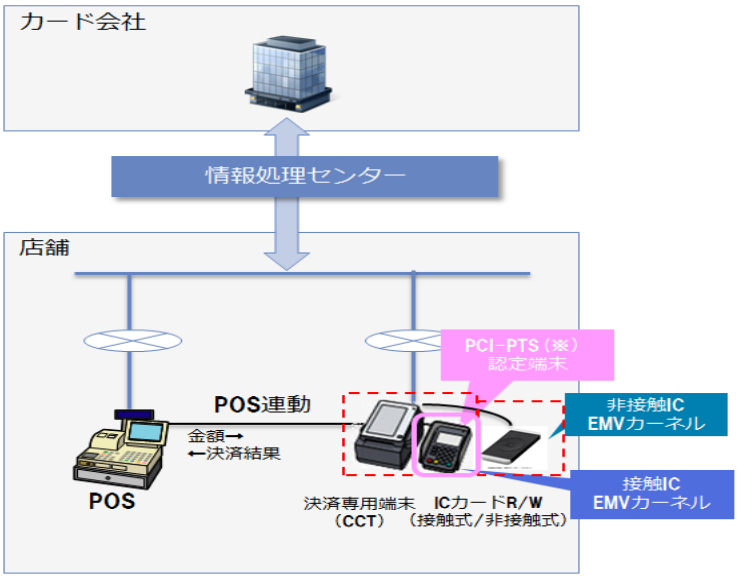
[23] IC 対応手法の構成図は、コスト削減を目的としたインターフェースの標準化、ブランド認定/テストの簡素化の観点からの推奨例を示したもの。詳細は、「IC カード対応 POS ガイドライン」を参照、また、カード情報保護の観点からのパターン別構成図は、『A.クレジットカード情報保護対策の強化に向けた実行計画』（P14～P20）の記載内容を参照のこと。

■決済専用端末（CCT）連動型

IC 対応した決済専用端末（CCT）と POS システムの間で取引金額や決済結果等を連動する仕組みである。EMV カーネルを決済専用端末や PIN パッド等に置くことで、POS システムの外側となるため、決済専用端末側で開発・EMV 認定・ブランドテスト等の対応を行えばよく、POS システム側で対応する必要がないことから、導入時における対応（開発・EMV 認定・ブランドテスト等）の影響が最も小さい。また、カード情報が IC 対応の決済専用端末から直接カード会社に伝送されるため、加盟店におけるカード情報の非保持化が同時に実現できる[24]。

一方で、決済専用端末を新たに追加する必要があるため、設置場所の確保等の課題はある。

【決済専用端末（CCT）連動型】

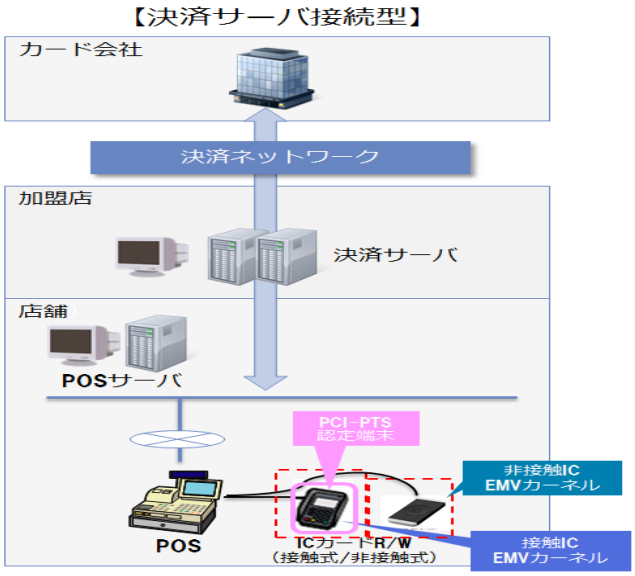


■決済サーバー接続型

POS システムで決済を行うが、EMV カーネルが PIN パッドにある仕組みである。EMV カーネルを POS システムの外側に置くため、POS 本体で開発・EMV 認定等を取る必要がなく、ブランドテスト等の対応で済むため、導入時における対応の影響は小さい。

この場合、カード情報は POS システムを通過してカード会社に伝送されるため、カード情報が自社内機器・ネットワークを「保存」、「処理」、「通過」するため、「非保持」とならず、PCI DSS 準拠が必要となる。

[24] 非保持化は決済専用端末（CCT）より POS へ連動する「決済結果」にはカード情報を含めないことが前提。

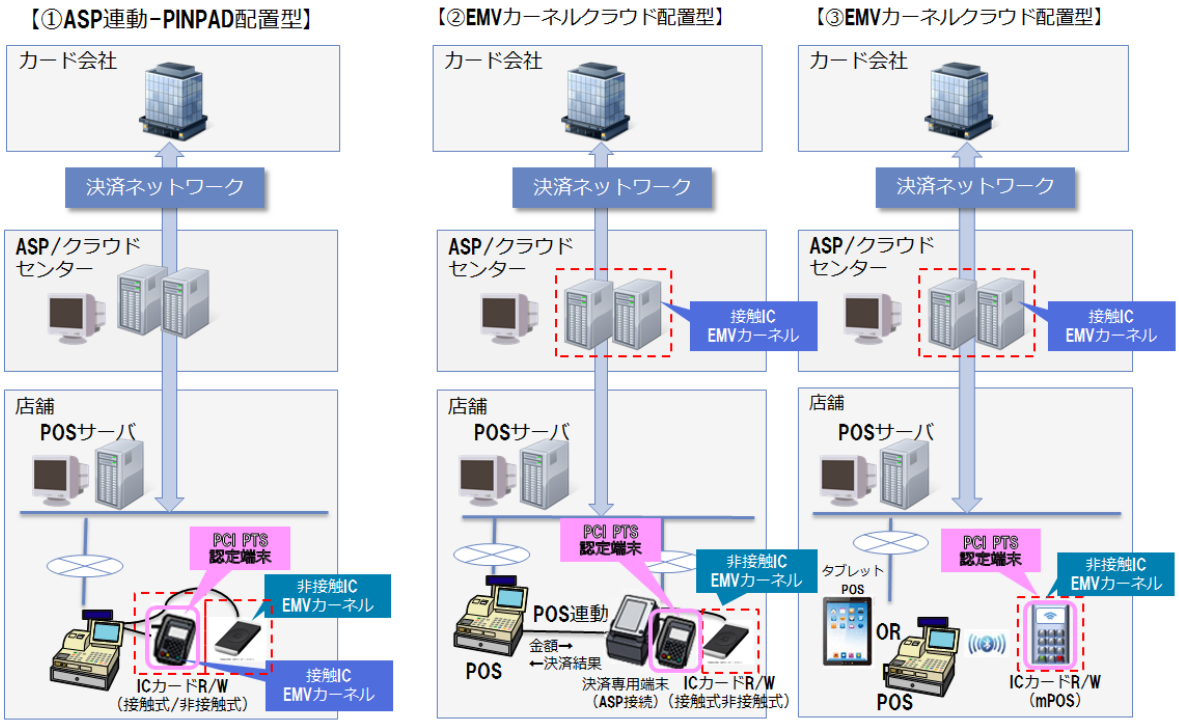


■ASP/クラウド接続型

POS システムと加盟店の外側の事業者（ASP）との間で取引金額や決済結果を連動させる仕組みである。基本的には上記決済サーバー接続型と同じ構造であるが、ASP/クラウド配置型での EMV 認定・ブランドテストの対応については社外（ASP）で行うため、加盟店の個別負担は少ない。

この中で、EMV カーネルクラウド配置型のうち決済専用端末を POS システムと連動させる場合（下記②）については、カード情報が IC 対応の決済専用端末から直接社外の ASP/クラウドセンターに伝送されるため、加盟店におけるカード情報の非保持化が同時に実現できる[25]。下記①及び③の場合には、カード情報は POS システムを通過するため、加盟店は PCI DSS 準拠が求められる。なお、非保持化を実現する場合は、非保持化と同等/相当のセキュリティ措置（PCI P2PE 認定ソリューションの導入又は本協議会において取りまとめた技術要件に適合するセキュリティ基準（11 項目）[26]）を満たすことが求められる。

[25] 非保持化は POS 連動する「決済結果」にカード情報を含めないことが前提。
[26] 詳細については、「対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について」を参照のこと。



（２）接続インターフェース等の共通化・標準化について

接続機器（CCT、IC-PIN パッド、非接触 R/W 等）を接続するための POS のインターフェースの標準化や汎用的な POS 搭載ミドルウェアを使用することで、POS 改修コストの低減や、各加盟店での対応期間の短縮を図ることが可能となる。

各方法の接続インターフェース等の共通化・標準化の検討結果について、国際標準仕様を策定している OPOS 技術協議会による確認の結果、標準化可能との回答が得られたため、今後、IC カード対応 POS ガイドラインへ記載し、機器メーカー等への連携、普及を図る。

（３）POS システムの IC 対応標準化

機器メーカーは、IC 対応端末のコスト低減化や加盟店での IC 対応を円滑に行うために、今後開発・製造するクレジット機能を有する POS システムについては、IC 対応可能なシステムを標準とする。

（４）その他 IC 対応 POS システムのコスト低減策

加盟店の負担となる国際ブランドごとのテストコスト低減化と導入までの期間を短縮するため、端末（ハード/ミドルウェア）やサーバー等が同一の構成である場合においては、国際ブランドと調整の上、端末やサーバー等ごとにブランドテストのプロセスの明確化あるいは簡略化による効率化を図るよう、IC カード対応 POS ガイドラインへ記載した。このコスト低減化等の考え方は、新たに策定した「非接触 EMV 対応 POS ガイドライン」にも応用されるものであり、引き続き両ガイドラインを機器メーカー等への連携・普及を図る。

４．IC-CCT 端末の普及について

カード会社（アクワイアラー）は、前述の IC 取引オペレーションルールに基づき、加盟店に対し店頭での運用について周知しつつ、IC 対応した CCT 端末の普及に努める。

また、CCT 端末の IC 対応は、2017 年 12 月末時点で 71.9%となっていることから、IC 未対応の CCT 端末については、稼働状況を踏まえて、稼働率の高い端末を優先的に IC 対応への切り替えを進めるものとする。また長期間未稼働の端末については登録抹消等を行うなど、IC 対応すべき対象の整理も行う。

５．IC 対応加盟店の「見える化」の方策について

日本クレジット協会は、行政と連携し、改正割賦販売法の国会附帯決議を踏まえ、加盟店のクレジットカード取引におけるセキュリティ対策を「見える化」する方策について検討を行い、以下の内容を取りまとめた。

（１）シンボルマーク等

消費者が IC クレジットカード対応加盟店であることを認識・識別できるよう、IC 対応済みであることを示す「共通シンボルマーク」、「IC 対応デザイン」（以下「IC 対応デザイン等」という）を策定した。また、IC 取引の必要性や特徴を理解してもらうための「IC 取引啓発デザイン」も策定[27]し、周知活動に使用することとした。

「IC 対応」・「暗証番号の認知度向上」
共通シンボルマーク

「IC 対応デザイン」

「IC 取引啓発デザイン」

[27] ニュースリリース『IC クレジットカード取扱店「見える化」のためのロゴマークを決定しました』
日本クレジット協会　http://www.j-credit.or.jp/download/171127_news_a.pdf
経済産業省　http://www.meti.go.jp/press/2017/11/20171127002/20171127002.html

（２）シンボルマーク等の普及

2018 年 4 月からの「見える化」活動の本格展開を見据え、カード会社（アクワイアラー）から IC 対応済み加盟店に対する「見える化」の取組及び「IC 対応デザイン等」を周知し、掲出等を依頼する。また、IC 対応済み加盟店が独自の「見える化」の取組が行えるよう日本クレジット協会のホームページに「IC 対応デザイン等」が掲載されていること、ダウンロードの上、活用いただくことについて周知する。

６．各主体の役割について

クレジットカード取引の IC 化を推進するためには、カード取引に関係する事業者全てにおいて、それぞれの役割に応じて取組を進めることが重要である。

なお、加盟店における IC 対応の早期完了に向けての統一的な経済的支援はできないものの、様々なセキュリティ対策とそれに伴う運用面の変更等が効果的かつ実効性のある取組として行われるよう、各主体は協力していくこととする。

以下、各主体に求められる役割等について整理する。

（１）加盟店

・改正割賦販売法が 2018 年 6 月 1 日に施行されることを踏まえ、その時までの対応を基本とし、最終的には、全加盟店において 2020 年 3 月末までに IC 取引が可能となるよう自社のクレジット決済システムの IC 対応が完了している状態になっていることを目指す。

・特に、POS システムを導入している加盟店においては、B. 3.（1）（各方策の検証について）を参考にし、自社対応方策検討時には、必要に応じてカード会社（アクワイアラー）や機器メーカー等に情報を求めることとする。

・IC 対応済み加盟店は、「IC 対応デザイン等」や「IC 取引啓発デザイン」の掲出、あるいは自社独自の「見える化」への取組に努めることとする。

（２）カード会社（アクワイアラー）

・契約を有する加盟店の IC 対応を推進するため、本実行計画で整理された各方策について加盟店に対して理解を進めるよう活動するとともに、必要に応じて機器メーカーとも連携して情報を提供する。

・POS システムの接続インターフェース等の共通化や IC 取引オペレーション等を踏まえて、機器メーカー等と連携して作成した「IC カード対応 POS ガイドライン」及び「非接触 EMV 対応 POS ガイドライン」について、機器メーカーや加盟店等への周知を行う。

・契約を有する IC 対応済み加盟店に「IC 対応デザイン等」の掲出を行うなどの取組に努める。

（３）カード会社（イシュアー）

・カード会社（イシュアー）においては、日本クレジット協会が策定した計画に基づき 2020 年 3 月末までにクレジットカードの IC 化 100%の実現に向けて、引き続き、IC カードへの切替えを加速していくこととする。

・カード会員等に対し、IC 取引では本人確認のため PIN 入力が必要になることから、B. 5. (1)の「共通シンボルマーク」を使用しカード会員の PIN 認知に向けた周知活動を行うとともに、PIN を認知していないカード会員には、特に丁寧な対応を図ることとする。

（４）国際ブランド

IC 取引オペレーションルールについて、本協議会での検討結果を踏まえ、本協議会と調整を行い、我が国のクレジットカード業界として制定したルールを推進することに協働して取組む。また、技術の向上や環境の変化等により新たな措置等が必要になった場合は、カード会社（アクワイアラー）と調整を行う。

（５）機器メーカー

・加盟店の IC 対応を推進するため、IC 対応の必要性及び本実行計画で整理された各方策について加盟店への周知活動等を進めるとともに、カード会社（アクワイアラー）とも連携をして加盟店へ必要な情報を提供する。

・本協議会における検討結果である POS システムの接続インターフェース等の共通化や国際ブランドテストの簡略化等を活用し、コスト低減化に資する技術的解決策の実現に向けて積極的に取組む。

・IC 対応端末のコスト低減化や加盟店での IC 対応を円滑に行うために、今後開発・製造するクレジット機能を有する POS システムについては、IC 対応可能なシステムを標準とする。

（６）行政・業界団体等

・行政は、改正割賦販売法により加盟店に対してカードの不正利用防止措置が義務付けられることを踏まえ、対面加盟店において決済端末の IC 対応が確実に図られるよう、カード会社（アクワイアラー）等を通じた加盟店に対する指導を徹底する。また、国際ブランド等と協力して、本実行計画の着実な実施に向け、事業者向けや消費者向けの情報発信に取組む。

・日本クレジット協会及び業界団体等は、行政と連携の上、消費者に対し、IC 取引の安全性及び IC 対応の「見える化」の方策である「IC 対応デザイン等」を周知するとともに、PIN 認知度のさらなる向上のための周知に引き続き取組む。

・また、クレジットカード業界全体で IC 取引を推進していること、IC 取引では本人確認のため PIN の入力が必要になることの周知に引き続き取組む。

7．2018 年度中に重点的に実施すべき具体的な取組について

2018 年度では、以下の具体的な取組により、各主体における取組を加速化させていくこととする。

（1）クレジットカード IC 化に向けた取組

・カード会社（イシュアー）は、2020 年 3 月末までに国内で流通する国際ブランド付きクレジットカードが 100%IC 化されていることを目指し、IC カードへの切替えを加速する。また、カード会員からの要望があれば、当該カードの更新時期を待たず、IC カードへの切替えを可能とする環境を早急に整える。

・日本クレジット協会は、行政と連携の上、カード会社（イシュアー）によるクレジットカード IC 化 100%の実現に向けた取組について進捗管理を行うとともに、カード会社（イシュアー）ごとの進捗状況について公表することを検討する。

・行政は、2017 年末時点でのカード会社（イシュアー）ごとのカードの IC 化の進捗状況を踏まえ、進捗の遅れている事業者への個別指導を行う等、カードの IC 化率を 100%に近づけられるよう着実な推進を図る。

（2）加盟店に対する決済システムの IC 対応に向けた取組

・加盟店は、各主体の協力を得ながら本実行計画に基づいて IC 対応に向けた方策を実施する。

・カード会社（アクワイアラー）は、対面取引の契約加盟店に対して、IC 対応に向けた本実行計画の周知を行う。

・特に、クレジットカードの取扱額の大きい加盟店に対し、日本クレジット協会は、IC 対応に向けた本実行計画の周知を行う。さらに、加盟店の特性に応じた IC 対応への個別の課題の抽出とその対応策について、機器メーカー等の専門事業者の協力を得ながら、加盟店の IC 対応に向けた検討を進める。

（3）IC カード対応 POS ガイドライン・非接触 EMV 対応 POS ガイドラインの周知

カード会社（アクワイアラー）は、日本クレジット協会やシステムベンダー等と連携して、B．2.（IC 取引時のオペレーションルール・ガイドラインについて）に述べた IC 取引オペレーションルール及び B．3.（コスト低減を踏まえた POS システムの IC 対応に関する方策について）に述べたコスト低減を踏まえた POS システムの IC 対応に関する方法を踏まえ、日本クレジットカード協会策定のガイドラインをもとにして策定した「IC カード対応 POS ガイドライン」及び「非接触 EMV 対応 POS ガイドライン」並びに日本クレジット協会において策定したその他ガイドライン[28]を関係者に周知することにより、加盟店の POS システムの IC 対応に向けた取組を加速する。

[28]「IC 取引における本人確認方法に係るガイドライン」及び「本人確認不要（サインレス/PIN レス）取引に係るガイドライン」。

C．非対面取引におけるクレジットカードの不正利用対策の強化に向けた実行計画

１．非対面取引における不正利用対策の取組について

非対面取引の中にはEC加盟店、MO・TO加盟店等による取引が有るが、非対面取引における不正利用被害のほとんどは、EC加盟店において発生している状況にある。

2016年のEC市場の取扱高はおよそ15兆1千億円となり、前年比9.9%増と引き続き拡大傾向である。その主な決済手段としてクレジットカードが重要な役割を担っているが、不正アクセス等による加盟店からのカード情報漏えい事案や消費者を狙った悪用者によるマルウェアやフィッシングでのカード情報の窃取による情報漏えい事案も発生している。

この結果、窃取されたカード情報等を不正に利用したなりすましによる被害額は2016年に約88億円（前年比23.1%増)、また2017年1月から9月の9ヶ月間には約130億円（前年同期比 92.2%増）発生し、この額は対面/非対面加盟店で発生する不正利用被害額全体の73.7%を占めるに至っており、なりすましによる年間での被害額はEC市場規模の伸びを大幅に超える状況になると想定される。この背景には、カード情報漏えい事案が依然多発しており、不正利用の単価や商材を真正利用と類似させるなど、不正利用自体が執拗且つ巧妙化していることが挙げられる。

このような非対面加盟店、特にEC加盟店におけるなりすましによるクレジットカードの不正利用被害額を極小化するため、犯罪組織や悪意のある第三者による不正な取引を検知・停止する取組を加速することが喫緊の課題である。

本協議会において、非対面加盟店における不正利用被害の状況について調査を行い分析したところ、2015年度においては不正利用被害額全体の75%をデジタルコンテンツ（オンラインゲーム含む)、家電、ECモール、電子マネー、チケットの5業種が占めることが判明した。このうちECモールは、業種ではなく販売形態であり、自身が特定の高リスク商材の販売を担っている訳ではないこと、また、2017年に実施した大手 ECモールに対するヒアリングの結果、モール傘下の店子における不正利用被害の発生状況も同様に他4業種（以下「特定4業種」という）が過半を占めていることが判明したことから、特定業種からECモールを除くこととする（ECモールについては、傘下の店子単位の取扱商材により特定4業種に該当するか否かを判別する。)。

不正利用被害が発生している加盟店では、本実行計画に掲げる不正利用対策の具体的方策を導入し、一定程度の防止効果をあげているが、不正利用被害が増加している現状を鑑み、不正利用の減少に向け、被害が多く発生している特定4業種を中心に取組を強化していく必要がある。

不正利用が多発している加盟店においては、契約先のカード会社、PSP、セキュリティ事業者等と連携し、不正利用の発生状況等を分析・把握するとともに、業種及び商材等のリスクの状況等に応じて、多面的・重層的な対策を講じていくことが有効である。

一方、加盟店が不正利用対策の具体的方策を導入していても、加盟店以外の要因により対策が有効に機能しない問題も生じている。例えば、①加盟店が 3Dセキュアを導入していて

も、カード会員がカード会社（イシュアー）に対してパスワード登録を行わない場合には、「本人認証」の処理が行われないこと、②カード情報とともにセキュリティコードが同時に漏えいした場合には、窃取された情報を基に「券面認証」が不正に行われる可能性があること、③過去の不正利用事案について十分に情報共有されていない場合、不正利用の傾向に対応できず、カード会社や加盟店においての不正利用対策の精度向上につながらないおそれがあること、などである。

このうち、①については、消費者自身のクレジットカードの不正利用の状況や不正利用対策等に関する認知・意識の向上も重要であり、消費者に対する情報提供や周知活動等を進めていく。②についてはカード情報保護対策の問題として取組む（Ⅱ．A.参照）。③については、関係事業者の創意・工夫により、不正検知システムの開発・導入や不正配送先情報の蓄積・活用が進んでおり、こうした最新の技術やノウハウを活用することが考えられる。

また、EC が拡大傾向にある中、クレジットカード決済の利便性を図りつつ、不正検知能力を高めていくためには、新しい技術・仕組みの開発・導入が必要であり、関係事業者によってこうした取組がさらに進むことが期待される。

本実行計画では、2018 年 3 月末までを目標期限として、EC 加盟店での不正利用対策の導入を推進してきたが、改正割賦販売法の施行を踏まえ、この取組は非対面加盟店全体を対象として継続していくこととする。

２．不正利用対策の具体的な方策について

なりすまし等不正利用を防止するための具体的な方策について、現状における主なものを以下のとおり整理する。

それぞれの方策には一定の効果が得られており、加盟店において方策の特徴等に対する理解を深め、方策導入の参考とするため、本協議会において不正利用被害抑止の好事例[29]を取りまとめた。好事例調査の取組は継続して実施し、更に方策毎の効果、方策の組合せによる効果について検証することとする。

また、それぞれの方策には特徴があり、加盟店の業種（商材）や販売手法に応じた有効な方策を講じることが重要である。加盟店はカード会社（アクワイアラー）、PSP と協働し、リスクの状況に応じた不正利用対策を適切に講じることにより、不正利用防止効果を高めていく。

なお、不正利用被害防止に資する新たな技術が検証され、その効果が認められると判断した場合は、本協議会においてさらに方策の追加を行うこととする。

■本人認証

- EC 加盟店におけるなりすまし不正利用防止のための本人認証の具体的手法として、3D セキュアや認証アシストがある。これらは、カード会員に特定のパスワードや属性情報等を入力させることで、利用者本人が取引を行っていることを確認するものである。
- 「3D セキュア」とは、カード会員のみが知るカード会社（イシュアー）に事前に登録し

[29] 詳細については「実行計画上の方策導入による不正抑止の好事例の紹介」を参照のこと。

たパスワード等を、カード利用時に当該カード会社（イシュアー）が照合することにより、本人が取引を行っていることを確認するものであり、国際ブランドが推奨する本人確認手法である。

・一方、加盟店が「3D セキュア」を導入していても、パスワード未登録のカード会員の利用に対しては本人認証の処理が行われず、その結果、不正利用被害を回避できない事例が発生している。カード会員のパスワードの登録なくしては、認証処理ができないため、カード会社（イシュアー）によるパスワードの登録率向上に向けたカード会員への周知活動を強化していくことが必要である。

・また、「3D セキュア」は、カード会員が「静的（固定）パスワード」を失念した場合の販売機会の逸失の懸念もあるため、消費者へのパスワードの管理に関する周知活動も重要である。

・カード会社（イシュアー）とカード会員のみが認知している情報の照合は、その情報の漏えいがない限り有効であるが、「3D セキュア」については、カード会員によるパスワード使い回しやパスワードの漏えいにより、その効果が発揮できない状況も発生している。

・現在、「3D セキュア」において主に利用されている「静的（固定）パスワード」の課題に対する解決策としては、「動的（ワンタイム）パスワード」や「指紋等の生体認証」が有効である。

・「動的（ワンタイム）パスワード」や「指紋等の生体認証」の利用は国際ブランドも推奨しており、特に「動的（ワンタイム）パスワード」については国内においても既に採用しているか、もしくは採用を検討しているカード会社（イシュアー）が存在している。今後、新たに「動的（ワンタイム）パスワード」を採用するカード会社（イシュアー）の増加等により、パスワード漏えいによる不正利用対策の強化やパスワード失念による販売機会逸失の回避が図られることが期待される。

・なお、「3D セキュア 2.0」の仕様については、国際ブランドが設置した国際機関 EMVCo より 2016 年 10 月下旬に公表されているが、「3D セキュア」に係るステークホルダーへの影響及び移行について、引き続き、国際ブランドに情報の提供及び説明を求め、移行にあたっての課題及び必要な対応について検討することとする。

【3D セキュア 2.0 仕様の特徴について】

①1.0 のブラウザベース（PC 利用）に加え、2.0 ではアプリケーションベースも対象となる。これによりスマートフォンのアプリケーションを利用した取引においても、3D セキュアによる認証が活用できるようになる。

②カード会員のネット接続端末情報や購入時にカード会員が入力した属性等、加盟店から ACS[30]（Access Control Server）に提供される情報が 1.0 に比較して 2.0 では増加する。これら情報の活用により、リスク判別力の高いモデルの設定が可能になり、パ

[30] 3D セキュアにおいて、カード会社（イシュアー）が加盟店からの本人確認要求に対して、本人であることを確認するためのサーバー。

スワード入力を求める取引が格段に少なくなることが期待できる。

・「認証アシスト」とは、カードのオーソリゼーション電文を用いて、カード会員の属性情報を送信し、カード会社に予め登録されている属性情報と照合し、利用者本人が取引を行っていることを確認する手法である。本人の属性情報を用いるため、カード会員のパスワード失念などの懸念が無いのが特徴である。

・一方、「認証アシスト」を導入する場合、加盟店は当該サービスを利用するカード会社との間で直接契約が必要であり（日本国内のカード会社のみが対象）、利用者全てのカードが対象とならない可能性がある。

・「3D セキュア」と同様、カード情報とともに当該属性情報が漏えいした場合には不正利用被害発生のリスクが生じることとなる。

■券面認証（セキュリティコード）

・「セキュリティコード」による認証は、使用するクレジットカード番号が真正であることをカード会社（イシュアー）が確認できること、セキュリティコード自体がカード会社（イシュアー）及びその顧客のカードに 100%普及していること、カード会員が認証で使用する番号を失念する懸念がないこと、既存のオーソリゼーション電文の活用で導入できること等の点で評価されている。

・カード番号とともに「セキュリティコード」が窃取されることにより、券面認証を突破される被害が一部確認されているが、こうしたことがなければ、好事例で示すように、セキュリティコードの不正利用防止効果が確認されている。

■属性・行動分析

・非対面でのカード利用時、加盟店が購入者のデバイス情報、IP アドレス、過去の取引情報、取引頻度等に基づいたリスク評価（スコアリング等）を行い、不正な取引であるか判定する手法である。なお、加盟店が独自で「属性・行動分析」のモデルを構築するには相当量の不正利用被害実績を把握する必要があり、小規模加盟店においてこれを独自で構築するのは簡単ではないため、外部の実績があるサービスの利用等が有効である。現在、複数の PSP やシステムベンダー等からサービスが提供されている。

・「属性・行動分析」を他の手段と組合せて導入した加盟店において、前年より不正利用被害が減少している好事例がある。これは、加盟店が独自に把握できるデバイス情報等を活用した不正判定モデルと、過去の不正利用実績における配送先情報の組合せが功を奏したものとして評価される。

■配送先情報

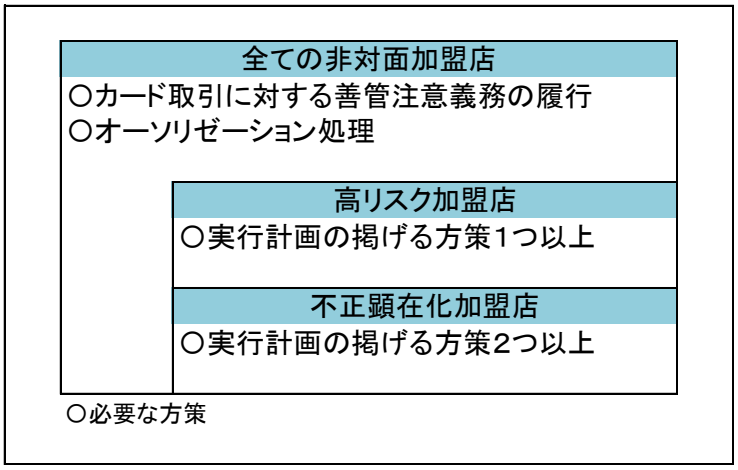
・不正利用された注文等の配送先情報を蓄積することで、取引成立後であっても商品等の配送を事前に止めることで不正利用被害を防止することが可能である。ただし、その情報の蓄積には時間がかかることから、新規に取組を始めて直ちに効果が発揮されることは困難であるため、外部の実績があるサービスの利用等が有効である。現在、大手加盟店が独自のデータベースを運用しているほか、カード会社複数社が共同で運用しているサービスが一部の加盟店に対して提供されている。

・過去に不正利用の配送先に用いられた住所情報を契約加盟店に提供するサービスが存在するが、複数のカード会社が共同で運用しているサービスについては、関係事業者を増やし情報量を増加させるとともに、「属性・行動分析」等の他の方策と組合せ、不正検知能力を高めることが重要である。
・「配送先情報」による不正利用対策では、送付先の不自然さ等から、不正な取引かどうかの判断を行うことも必要となるため、加盟店においては不正判断ノウハウの蓄積や態勢構築も必要となる。

３．加盟店におけるリスク・被害発生状況に応じた方策の導入

加盟店の業種及び商材等に応じた不正利用の被害発生状況等を踏まえ、各加盟店は不正利用対策の具体的方策を導入することとする。本実行計画では不正利用防止のための方策として、４つの方策（①本人認証、②券面認証、③属性・行動分析、④配送先情報）を掲げており、この４つの方策をベースに、加盟店のリスクや被害発生の状況等に応じた指針を示すこととする[31]。

加盟店分類表



（１）全ての非対面加盟店

リスクや被害発生の状況にかかわらず、全ての非対面加盟店において導入を求める不正利用防止のための方策としては、加盟店契約における善良なる管理者の注意をもって不正利用の発生を防止するとともに、カード会社が不正利用のリスクを評価するためのオーソリゼーション処理の態勢整備を図ることである。この上で、以下の加盟店については、リスクや被害発生の状況に応じた方策の導入を求める。なお、昨今の不正犯の手口として、リスト型攻撃（システムを利用し短時間に大量の購入申し込みを行う）が発生しており、継続的（連月）ではなくとも単発的（単月）で高額な不正被害が発生する加盟店に対して、カード会社（アクワイアラー）は早急に追加的な方策を導入する必要があると判断する場合があり、当該加盟店には方策の導入を含めた不正利用防止策の検討を求める。

[31]「非対面加盟店における不正利用対策の具体的な基準・考え方について」を参照のこと。

（２）高リスク（業種）加盟店

特定 4 業種（①デジタルコンテンツ（オンラインゲームを含む）、②家電、③電子マネー、④チケット）に属する加盟店は、「高リスク（業種）加盟店」として、本実行計画の掲げる 4 つの方策のうち、1 方策以上の導入を求める。

なお、EC モールのように多数の店子によって構成されるのではなく、一つの加盟店が様々な商品等を取り扱っているいわゆる「総合通販」についても、総合通販事業者における主たる取扱い商材が特定 4 業種に該当する場合には、高リスク加盟店と同様の方策の導入を求める。

（３）不正顕在化加盟店

不正利用被害が多発状況にあるとカード会社（アクワイアラー）等が認識する加盟店は「不正顕在化加盟店」として、本実行計画の掲げる 4 つの方策のうち、2 方策以上の導入を求める。なお、「不正顕在化加盟店」については、カード会社（アクワイアラー）各社が把握する不正利用金額が継続的に一定金額を超えた場合に該当する。（なお、当該基準については、毎年度の不正利用被害の状況等により、必要に応じて見直しを行うこととする。）

また、4 つの方策のうち 2 方策以上を導入していても不正利用被害が減少せず、引き続き、「不正顕在化加盟店」と認識される加盟店は、カード会社（アクワイアラー）等より不正利用の発生状況等の情報共有を受け、不正利用防止についての追加的な方策の導入等のため継続的な検討が求められる。

４．各主体の役割について

2017 年における非対面加盟店での「なりすまし不正利用被害」の継続的な増加状況を踏まえ、不正利用被害防止を 2018 年に更に具現化するため、特に不正が多発（不正顕在化）している加盟店への対策の導入について、協議会に関わる全てのステークホルダーの協力のもと、強力に推進する。EC におけるなりすましの不正利用被害を極小化するためには、EC に関係する事業者全ての積極的な対応が求められる。以下、各主体に求められる役割について整理する。

（１）カード会社（イシュアー）

- 過去の取引履歴等の様々な情報から、不正取引か否かを判断する不正検知システムの導入・検知精度の向上に努める。
- 不正利用の被害防止に関する消費者への周知を図る。
- カード会社（イシュアー）自体が「3D セキュア」未導入の場合は、早期に導入を図り、また導入カード会社においては「3D セキュア」の利用拡大のため、カード会員のパスワード登録率の向上を図る。
- 「3D セキュア」のパスワード登録率向上の施策推進にあたっては、カード情報とともに「静的（固定）パスワード」が窃取されるリスクがあり、これら情報の流用によるなりすまし被害を防止するため、「動的（ワンタイム）パスワード」の導入促進に努める。

・加盟店（オフアス取引の場合はアクワイアラー経由）からの真正利用確認照会件数の増加を想定した対応態勢を整備する。
・取引が不正か真正かの最終確定はカード会社（イシュアー）であることから、迅速に判断するとともに、カード会社（アクワイアラー）、加盟店、PSP との不正情報の共有が重要である。迅速な判断及び情報連携について、課題の特定とともに解決を図る。
・「カード利用時におけるカード会員向け利用確認メール等通知」は、カード会員がメール等通知内容を確認し、利用の覚えがない場合はカード会社（イシュアー）に連絡することにより、早期の不正利用の確定とカードの無効手配・処理が可能となるため、有効な不正利用対策となる。
・一方、メール等受信に関するカード会員の同意が必要なことや、メールアドレス等の登録・管理（メールアドレス等の情報の最新化）等、カード会社（イシュアー）が採用する場合の課題も考慮しつつ、検討すべき方策である。

（２）カード会社（アクワイアラー）及び PSP

・本実行計画 C. 2.（不正利用対策の具体的な方策について）で示す不正利用対策の具体的な方策について、カード会社（アクワイアラー）は、加盟店に対して適切な方策の導入の助言・協力ができるよう態勢の整備をするとともに、本実行計画 C. 3.（加盟店のリスク・被害発生状況に応じた方策の導入）の確実な実施のため加盟店に対する指導を適切に実施する。
・国際ブランドから提供される「3D セキュア 2.0」の仕様及びそれに係る運用ルールや導入メリット等の情報について収集することに努める。
・併せて、加盟店に対し、不正利用対策の参考となるよう、なりすまし不正利用の傾向や事例等の情報（本協議会で取りまとめた「好事例」等）について共有を図る。
・PSP は、C. 2.（不正利用対策の具体的な方策について）に列挙した「本人認証」「券面認証」「属性・行動分析」「配送先情報」の各方策を提供できる態勢を構築し、契約先の加盟店に対して導入の推進に努める。
・オフアス取引において、カード会社（アクワイアラー）は、加盟店における不正利用対策の更なる向上のため、カード会社（イシュアー）から提供された不正情報について加盟店と迅速な情報共有に努める。
・各加盟店における不正利用対策の課題の特定とともにその解決を図るため、各加盟店との間で迅速な情報共有に努める。

（３）国際ブランド

・本実行計画の確実な実施を図るため、我が国における非対面加盟店でのクレジットカード取引の実態を踏まえ、各種課題の解決に向けて関係事業者と協働して取組む。
・「3D セキュア 2.0」に係るステークホルダーへの影響（運用ルール等）及び 2.0 への移行について、情報の提供及び説明を行う。

・非対面加盟店における不正利用対策の取組を推進するため、海外のカード会社や加盟店における取組事例について情報提供を行うとともに、我が国における国際水準のセキュリティ環境の整備の必要性等について、事業者向けや消費者向けの情報発信に取組む。

（４）加盟店

・本実行計画 C．3.（加盟店のリスク・被害発生状況に応じた方策の導入）に基づき、加盟店のリスク、被害状況に応じたなりすまし不正利用対策の具体的方策を確実に実施する。

・自社での不審なカード利用の把握に努めるとともに、不正利用の実態やその手口は日々巧妙化することから、カード会社における不正利用対策の更なる向上のため、当該情報（不審利用）を契約先のカード会社（アクワイアラー）や PSP と迅速な情報共有に努める。

・自社の不正利用対策の課題の特定とともにその解決を図るため、契約先のカード会社（アクワイアラー）や PSP との間で迅速な情報共有に努める。

・自社の不正利用被害のリスクを低減するために、不正利用対策の強化を図る観点から、カード会社（アクワイアラー）や PSP とも協力して、C．2.（不正利用対策の具体的な方策について）で示した方策を基本としたリスクに応じた不正利用対策を講じる。

（５）行政・業界団体等

・行政は、改正割賦販売法により、カードの不正利用防止措置が加盟店に義務付けられることを踏まえ、必要な措置が確実に導入されるよう、カード会社（アクワイアラー）等を通じた加盟店に対する指導を徹底する。また、国際ブランド等と協力して、本実行計画の確実な実施に向け、事業者向けや消費者向けの情報発信に取組む。

・日本クレジット協会は、他の業界団体に協力を要請し、不正利用の実態を踏まえ、加盟店において本実行計画に掲げるリスクに応じた方策を導入する必要性及び各方策の有効性等について、消費者や事業者向けの周知活動の強化に取組む。ID・パスワードの使い回しへの注意喚起などの周知活動を行うことを含め、消費者における不正利用対策への理解・認知度の向上に取組む。

・日本クレジット協会は、カード会社（イシュアー）と連携の上、「3D セキュア」のパスワード等の登録推進、カード会社（イシュアー）からの真正利用確認に対する協力について、消費者等に対して周知活動を行う。

・日本クレジット協会は、最新の不正発生状況を踏まえた「不正顕在化加盟店」の基準や「高リスク加盟店」の特定商材の継続的な検討、不正被害が継続的に発生する加盟店の不正発生状況の分析・評価、加盟店の業種（商材）に応じた各方策の有効性の検証や方策の組合せ効果の検証を行う。このため、日本クレジット協会にカード会社としての取組としての新たな会合等を組成して、不正利用被害額の抑止に実効的な取組を行う。

・日本クレジット協会は、不正利用による被害の実態や最新の犯罪手口、不正利用対策に

対する取組の成功事例等について、関係機関との連携・情報共有を図り、クレジット取引に関係する事業者等に対して適時情報発信を行う。

５．2018 年度中に重点的に実施すべき具体的な取組について

2018 年度では、以下の具体的な取組により、各主体における取組を加速化させていくこととする。

（１）加盟店による不正利用被害減少への取組

・加盟店は、本実行計画 C. 3.（加盟店のリスク・被害発生状況に応じた方策の導入）で示す指針に基づき、カード会社（アクワイアラー）及び PSP と連携し、必要な方策を確実に導入する。

・不正顕在化には至っていないが、不正利用被害が発生している加盟店は契約先のカード会社（アクワイアラー）及び PSP と連携し、不正利用被害の実情を共有し、追加対策の必要性も含め、協働して不正利用被害を防止するための対策に努める。

（２）カード会社による不正利用被害減少への取組

・カード会社は、不正検知システムの更なる検知精度の向上に努める。

・「3D セキュア」の更なる活用を促進するため、カード会員のパスワード等の登録率の向上を図る。登録率向上のための施策実施にあたっては、セキュリティの高い「動的（ワンタイム）パスワード」の導入や「生体認証」等の新たな認証方法の導入に努める。

・「3D セキュア」において、ACS ベンダーが新たにカード会社（イシュアー）版の属性・行動分析（以下「リスクベース認証[32]」という）の提供を開始した。本機能は過去の不正実績とデバイス情報等を活用したリスク評価モデルにより、不正利用の判別精度を高めることを目的としたものである。カード会員にパスワード入力を求める取引を最小限にすることも期待できることから、カード会社（イシュアー）は「リスクベース認証」の導入を検討する。

・「3D セキュア 2.0」への移行について、国際ブランドに情報提供・説明を要請し、協働して関係者への周知等を図り、早期の対応が図れるよう努める。

・不正顕在化までには至っていないが、不正被害が発生している加盟店と協働して不正の手口、方策の有用性等の検証を行い、被害額の減少に向けた有効な対策を提案する。

・配送先情報の利用拡大、情報共有について検討を行う。

（３）業界団体等による不正利用対策の効果検証に係る取組

日本クレジット協会は、カード会社（アクワイアラー）及び PSP 等と連携の上、不正利用防止効果を高めるため、①高リスク加盟店の根拠となる「不正犯に狙われやすい商材」の傾向の検証、②不正顕在化加盟店の基準の検証、③不正顕在化加盟店における導入済対策の効果検証等を行う。検証結果を踏まえ基準改訂が必要な場合には、本協議会

[32]リスクベース認証は「3D セキュア」のバージョンが 1.0 の環境下でも導入することができる。

において検討を行う。

（４）業界団体等による不正利用対策への理解・認知度を高める取組

日本クレジット協会は、行政と連携の上、消費者が EC 加盟店等で導入される不正利用対策への理解・認知度を高める取組について検討を行うとともに、本取組の実施を通じて、事業者側の取組・努力を分かりやすく伝えていく。

Ⅲ．消費者及び事業者等への情報発信等について

１．基本的な考え方

日本クレジット協会の調査結果[33]によれば、2017 年 3 月末時点のクレジットカード発行枚数は 2 億 7,200 万枚で、成人人口比では、1 人当たり 2.6 枚保有しているなど、今や消費者にとってなくてはならない便利な決済インフラとして重要な役割を果たしている[34]。

他方、クレジットカードのセキュリティレベルをより向上することは、時として消費者の利便性に影響を及ぼすことも事実であることから、消費者の理解・協力を得つつ、クレジットカード取引のセキュリティ対策を強化することが不可欠である。

こうした観点より、消費者への情報発信等は様々な機会を捉えて積極的に行うことが必要であり、カード会社のみならずカード取引に関わる各事業者等の取組・協力や消費者団体等との連携も重要である。

改正割賦販売法により加盟店におけるセキュリティ対策が義務化され、本実行計画を実務上の指針としていることを踏まえ、行政は、日本クレジット協会とともに、加盟店業界団体、消費者団体等と連携の上、本実行計画の内容に関する消費者及び事業者向けの周知活動等に引き続き取組むものとする。また、カード会社（イシュアー）はカード会員向け、カード会社（アクワイアラー）及び PSP は契約先加盟店向けの周知活動等を強化するものとする。

２．具体的な取組について

（１）消費者向け周知活動について

日本クレジット協会では、一般消費者向けのホームページ（安全・安心なクレジットカード取引への取組み）において啓発チラシ（「クレジットカードがより安全・安心な IC 取引に変わります！」「インターネットショッピングのカード決済には「本人確認等」が必要になります！」）の掲載、セキュリティ対策に係る動画の提供を行い、ラジオ CM の放送などの情報発信を行っている。

そのほか、周知の一環として、行政とともに、新聞広告の実施、講演会での対応、プレス取材協力を通じた情報発信等を行っている。

2018 年度は、各主体において、以下の取組により、さらに積極的な周知活動・情報発信を行っていくものとする。

①IC 対応の「見える化」への取組

消費者がセキュリティ対策を導入済の安全･安心な加盟店を選択できる環境を整備する観点から、IC 対応加盟店を認識・識別できる方策として IC 対応シンボルマーク・デ

---

[33] 出所:日本クレジット協会「クレジットカード発行枚数調査結果の公表について」(2017 年(平成 29 年)11 月 30 日）https://www.j-credit.or.jp/download/toukei_03_a_171130.pdf

[34] 2014 年 8 月に消費者委員会が公表した「クレジットカード取引に関する消費者問題についての建議」において、「クレジットカード取引における被害の発生・拡大防止及び回復等を図るため、」「クレジットカードの利用に関する知識について消費者教育及び消費者への情報提供を一層積極的に推進すること。」が消費者庁及び経済産業省に対し建議された。これを受けて、2015 年 2 月に経済産業省からクレジットカード業界に対して同旨の要請文が発出された。

ザイン、IC 取引啓発デザイン（以下「マーク等」という）の普及に努める。このため、カード会社（アクワイアラー）は、IC 対応加盟店に対して当該マーク等を周知することとする。

②クレジットカードの PIN の認知度向上

紛失・盗難によるカードの不正利用を防止するためには、加盟店のクレジット決済端末が IC 対応するだけでなく、カード会員が PIN（暗証番号）入力による本人確認の重要性（カード会員自身が設定した暗証番号を入力する方がサインよりもさらに安全であること）を理解し、自らのクレジットカードの PIN を認識していることが必須要件である。日本クレジットカード協会のアンケート調査によれば、PIN の認知率は 86.6%、また「安全性を重視すると暗証番号入力は必要」と 9 割強が回答している。今後 IC 取引が進展していく中、更に PIN 認知を浸透させるため、カード会社（イシュアー）及び業界団体等は引き続き広報等に取組むこととする。

なお、PIN を認知していないカード会員については、どのように PIN を再確認すればよいか不明な者も多いことから、カード会社（イシュアー）はカード会員への丁寧な周知等に留意すべきである。

③ID・パスワードの使い回しの防止

EC 加盟店における不正利用を防止するために本人認証サービス等の方策をとることが有効であるが、カード会員が複数のインターネットサイトで同一の ID・パスワードを使い回している場合は、一つのサイトでカード情報が漏えいすれば、他のサイトに不正ログインされ、登録されているクレジットカード情報等が不正利用される可能性がある。

このため、ID・パスワードの使い回しの防止等について、カード会社（イシュアー）及び日本クレジット協会は引き続き周知活動に取組むこととする。

④EC 加盟店における不正利用対策の認知度向上

EC 加盟店における不正利用対策の導入・普及には、カード会社、PSP、加盟店等カード取引に関係する事業者による取組のみならず、カード会員の不正利用対策の必要性やその具体的な方策に関する理解・協力を得ることが重要であり、日本クレジット協会は、関係事業者と協力し、EC 加盟店における不正利用対策に関する消費者向けの周知活動に取組むこととする。

⑤利用明細のチェックに関する周知

不正利用による消費者被害を防止するためには、消費者自身がカードの利用明細をチェックし、不正利用の発生に早期に気付くことが重要である。このため、日本クレジット協会は、毎月の利用明細を確認することの重要性について、引き続き、積極的な消費者への周知活動を行うこととする。

（２）クレジットカード取引に関係する事業者等への情報発信について

クレジットカード取引に対する不正を企図する攻撃者の手口は日々巧妙化していくため、加盟店をはじめとするカード取引に関係する事業者は最新の手口やセキュリティ技術等に関する情報を常に収集することが求められる。

特に各加盟店におけるセキュリティ対策については、多額の投資や業務の変更等を要することもあり、適切な情報の収集と分析等が必要となるが、個社の取組のみでは限界もある。

こうした事情を踏まえ、行政及び日本クレジット協会は、本実行計画の内容を広く周知するとともに、セキュリティ対策について必要な助言や情報提供を行い、その取組を支援していくものとする。

Ⅳ．本協議会の今後の活動方針と体制等について

１．今後の活動方針

本実行計画は各主体における2017年中の活動状況等を踏まえ、2018年版として改訂した。本協議会の参加各社等は実行計画 2018 年版に基づき、2020 年に向けたセキュリティ対策の強化に向けた具体的な取組を進めることとする。

なお、各事業者等が連携を図って戦略的に実行していくことが実効性の観点から必要であるため、今後も本会議又は各 WG において、継続検討事項の検討を進めるとともに、さらなるセキュリティ対策の強化に向けた議論を継続することとする。

具体的には、カード情報の漏えい事案や不正利用の被害の実態、さらにセキュリティ対策の技術的進展を踏まえて、本実行計画の内容の改善・見直し等を図ることとする。特に、各主体における本実行計画の進捗及び達成度等について報告を受け、その評価を踏まえて、翌年度に重点的に実施すべき具体的な取組等について検討を行い、本実行計画の見直し等を図ることとする。

２．本実行計画の進捗管理等に係る体制について

本協議会の事務局である日本クレジット協会を中心に、①本実行計画の取組について、各主体へのヒアリング等を通じた進捗管理及び実行計画の内容の改善・見直し等、②本実行計画に基づく具体的な取組に関する各事業者等との連携、③不正利用被害の実態、諸外国のセキュリティ環境、最新の攻撃手口及びセキュリティ技術等の情報収集・発信、④消費者に向けた周知活動、⑤その他セキュリティ対策の強化に資する関係機関との意見交換等を行うこととする。

本協議会事務局の円滑な活動のため、協議会に参加する各事業者等はその活動に対して支援・協力することとする。

別紙

PCI DSS 準拠について

本実行計画に定める非保持化（それと同等のセキュリティが確保できる措置を含む。）を実現した場合は、PCI DSS 準拠を求めるものではない。

１．PCI DSS とは

PCI DSS は、カード情報を扱う全ての事業者に対して国際ブランドが定め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など、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（認証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。

各国際ブランドにおいて、①を求める対象範囲について、カード情報の取扱形態や規模による基準を定めている。

なお、日本国内における PCI DSS 準拠の取組については、日本クレジット協会が策定した『PCI DSS 準拠にかかる基準及び検証方法等に関する実施要領』に基づいて行うものとする。

２．PCI DSS 12 要件

（１）PCI データセキュリティ基準-概要（バージョン 3.2）

Ⅰ	安全なﾈｯﾄﾜｰｸｼｽﾃﾑの構築と維持	1.	ｶｰﾄﾞ会員ﾃﾞｰﾀを保護するために、ﾌｧｲｱｳｫｰﾙをｲﾝｽﾄｰﾙして構成を維持する
		2.	ｼｽﾃﾑﾊﾟｽﾜｰﾄﾞ及び他のｾｷｭﾘﾃｨﾊﾟﾗﾒｰﾀｰにﾍﾞﾝﾀﾞｰ提供のﾃﾞﾌｫﾙﾄ値を使用しない
Ⅱ	ｶｰﾄﾞ会員ﾃﾞｰﾀの保護	3.	保存されるｶｰﾄﾞ会員ﾃﾞｰﾀを保護する
		4.	ｵｰﾌﾟﾝな公共ﾈｯﾄﾜｰｸ経由でｶｰﾄﾞ会員ﾃﾞｰﾀを伝送する場合、暗号化する
Ⅲ	脆弱性管理ﾌﾟﾛｸﾞﾗﾑの維持	5.	すべてのｼｽﾃﾑをﾏﾙｳｪｱから保護し、ｳｲﾙｽ対策ｿﾌﾄｳｪｱ又はﾌﾟﾛｸﾞﾗﾑを定期的に更新する
		6.	安全性の高いｼｽﾃﾑとｱﾌﾟﾘｹｰｼｮﾝを開発し、保守する
Ⅳ	強力なｱｸｾｽ制御手法の導入	7.	ｶｰﾄﾞ会員ﾃﾞｰﾀへのｱｸｾｽを、業務上必要な範囲内に制限する
		8.	ｼｽﾃﾑｺﾝﾎﾟｰﾈﾝﾄへのｱｸｾｽを識別・認証する
		9.	ｶｰﾄﾞ会員ﾃﾞｰﾀへの物理ｱｸｾｽを制限する
Ⅴ	ﾈｯﾄﾜｰｸの定期的な監視及びﾃｽﾄ	10.	ﾈｯﾄﾜｰｸﾘｿｰｽ及びｶｰﾄﾞ会員ﾃﾞｰﾀへのすべてのｱｸｾｽを追跡及び監視する
		11.	ｾｷｭﾘﾃｨｼｽﾃﾑ及びﾌﾟﾛｾｽを定期的にﾃｽﾄする
Ⅵ	情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの維持	12.	すべての担当者の情報ｾｷｭﾘﾃｨに対応するﾎﾟﾘｼｰを維持する

業態、システム・ネットワーク構成により対象となる範囲において上記の各要件に適合していることを自己問診（SAQ）もしくは第三者の確認（QSA による訪問審査）によって証明する。

３．タイプ別 SAQ

本実行計画においては、A.2.（加盟店におけるカード情報の非保持化の推進について）に定める「非保持化」あるいは「非保持化と同等/相当のセキュリティ確保できる措置」を実現した場合は、PCI DSS 準拠を求めるものではない。

カード情報を保持するため PCI DSS 準拠を選択した場合、PCI DSS ではその業態、システム・ネットワーク構成に応じたタイプ別自己問診（SAQ）が示されており、該当する SAQ に応じて評価することとなる。

下表はあくまで参考であり、準拠項目は業務、システム・ネットワーク構成実態による。

SAQ の詳しい内容等に関しては、日本カード情報セキュリティ協議会（JCDSC）http://www.jcdsc.org/を参照。

	加盟店の業態	ｶｰﾄﾞ情報の取扱い形態	求められる PCI DSS SAQ タイプ V3.2 Rev1.1	準拠項目数（付録含）
非対面 EC／通信販売加盟店	・PSP のﾘﾝｸ（ﾘﾀﾞｲﾚｸﾄ）型の決済ｻｰﾋﾞｽを使用する EC 加盟店 ・ｶｰﾄﾞ情報の全ての処理を外部委託する EC/通信販売加盟店	EC 又は通信販売の加盟店でｶｰﾄﾞ情報をｼｽﾃﾑ又は加盟店内で電子形式で通過、処理、保存しない	SAQ A	22
	・PSP の JavaScript 型の決済ｻｰﾋﾞｽを使用する EC 加盟店	EC の決済を PCI DSS 準拠済みのｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞｰに部分的に委託している EC の加盟店でｶｰﾄﾞ情報をｼｽﾃﾑ又は加盟店内で電子形式で通過、処理、保存しない	SAQ A-EP	193
対面/通信販売加盟店 ※EC 加盟店には適用されない	CCT などの決済端末をﾀﾞｲｱﾙｱｯﾌﾟ接続する主に対面加盟店	ｲﾝﾌﾟﾘﾝﾀ、ｽﾀﾝﾄﾞｱﾛﾝ型のﾀﾞｲｱﾙｱｯﾌﾟの決済端末のみによってｶｰﾄﾞ情報を処理する加盟店であり、ｶｰﾄﾞ情報を保存していない。	SAQ B	41
	CCT などの決済端末を IP 接続する主に対面加盟店	決済ﾈｯﾄﾜｰｸ又は ASP/ｸﾗｳﾄﾞ事業者に IP 接続されるｽﾀﾝﾄﾞｱﾛﾝ型の PCI PTS 認定の決済端末のみによってｶｰﾄﾞ情報を処理する加盟店であり、ｶｰﾄﾞ情報を保存していない。	SAQ B-IP	88
	POS をｲﾝﾀｰﾈｯﾄに接続してｶｰﾄﾞ処理する主に POS 加盟店	POS ｼｽﾃﾑ又はその他のｲﾝﾀｰﾈｯﾄに接続されているﾍﾟｲﾒﾝﾄｱﾌﾟﾘｹｰｼｮﾝ経由でｶｰﾄﾞ情報を処理するが、ｶｰﾄﾞ情報をｺﾝﾋﾟｭｰﾀｼｽﾃﾑに保存しない加盟店	SAQ C	162
	電話やﾊｶﾞｷ/FAX でｶｰﾄﾞ処理する主に通信販売加盟店	Web ﾌﾞﾗｳｻﾞなどの仮装端末のみでｲﾝﾀｰﾈｯﾄを経由して、1 件ずつｶｰﾄﾞ情報を処理し、ｶｰﾄﾞ情報をｺﾝﾋﾟｭｰﾀｼｽﾃﾑに保存しない。決済に利用する Web ｱﾌﾟﾘｹｰｼｮﾝは PSP、ｱｸﾜｲｱﾗｰなどｻｰﾄﾞﾊﾟｰﾃｨｰから提供される必要がある。	SAQ C-VT	85
	PCI P2PE ｿﾘｭｰｼｮﾝを導入した主に POS 加盟店	PCI P2PE に認定されたｿﾘｭｰｼｮﾝを導入し、それらに含まれる決済端末のみでｶｰﾄﾞ情報を	SAQ P2PE	33

		処理する加盟店であり、ｶｰﾄﾞ情報を保存していない		
対面/非対面加盟店	・PSP のﾓｼﾞｭｰﾙ（ﾌﾟﾛﾄｺﾙ）型を使用する EC 加盟店 ・ｶｰﾄﾞ情報をｻｰﾊﾞｰや PC で保存する POS や通信販売加盟店 ・ｶｰﾄﾞ情報を POS ｼｽﾃﾑで通過、処理、保存する加盟店	・ｶｰﾄﾞ情報を自社のｻｰﾊﾞｰで処理する加盟店 ・ｶｰﾄﾞ情報を電子形式で保存する加盟店 ・ｶｰﾄﾞ情報を電子形式で保存しないが他の SAQ ﾀｲﾌﾟの基準を満たさない加盟店 ・他の SAQ ﾀｲﾌﾟを満たす環境にあるが、自社の環境に他の PCI DSS 要件が適用されるような加盟店	SAQ D Marchant	331

【参考】クレジット取引セキュリティ対策協議会の検討経緯

◆本会議

第 1 回　2015 年 3 月 25 日

議題：クレジット取引における不正被害の状況とクレジット業界のこれまでの取組について
ＷＧの設置について　等

第 2 回　2015 年 7 月 23 日

議題：中間論点整理と今後の検討の方向性について

第 3 回　2016 年 2 月 23 日

議題：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（案）について

第 4 回　2017 年 3 月 8 日

議題：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－に基づく協議会並びに各主体の活動状況等について
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－2017－について

第 5 回　2018 年 3 月 1 日

議題：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－2017－に基づく協議会並びに各主体の活動状況等について
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 - 2018 - について

◆カード情報保護 WG（WG1）

第 1 回　2015 年 5 月 1 日

議題：クレジット取引における不正被害の状況とクレジット業界のこれまでの取組について
カード情報保護ＷＧの検討課題と検討の進め方について

第 2 回　2015 年 5 月 29 日

議題：カード情報保護の取り組みを進める上での課題について①

第 3 回　2015 年 6 月 15 日

議題：カード情報保護の取り組みを進める上での課題について②　等

第 4 回　2015 年 7 月 6 日

議題：本会議に向けた中間論点整理と今後の検討の方向性について

第 5 回　2015 年 9 月 18 日

議題：2020 年のあるべき姿及び優先的に取り組む課題と具体的な論点等について

第 6 回　2015 年 11 月 20 日

議題：決済代行業者との非保持化方式のリスク低減に向けた対応について
対面取引での非保持化の検討状況について
QSA との検討状況について

第 7 回　2015 年 12 月 21 日

議題：WG1 実行計画（案）について①　等

第 8 回　2016 年 1 月 26 日

議題：WG1 実行計画（案）について②

第 9 回　2016 年 4 月 20 日

議題：今後の進め方について

非保持化実施加盟店における問合せ対応について

通過型 EC 加盟店におけるトランザクションログ消去等の要請実施について

第 10 回　2016 年 5 月 19 日

議題：非保持化の実現方策及び問合せ対応方法について

第 11 回　2016 年 12 月 19 日

議題：「非保持化」の定義について

実行計画の見直しについて

第 12 回　2017 年 1 月 18 日

議題：実行計画 2017 について

第 13 回　2017 年 1 月 31 日

議題：実行計画 2017 について

第 14 回　2017 年 2 月 13 日

議題：実行計画 2017 について

第 15 回　2017 年 2 月 23 日

議題：実行計画 2017 について

第 16 回　2017 年 4 月 27 日

議題：非保持化と同等/相当のセキュリティ措置について

第 17 回　2017 年 7 月 25 日

議題：メールオーダー/テレフォンオーダー等の非対面加盟店の対応について

2017 年度中に重点的に実施すべき具体的な取組の進捗報告

第 18 回　2017 年 11 月 9 日

議題：メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて

2017 年度中に重点的に実施すべき具体的な取組の進捗状況及び実行計画 2018 策定の方向性について

「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」ガイドライン（暫定版）について

第 19 回　2017 年 12 月 21 日

議題：「POS-IC 化推進に向けたシステム構成～対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について～」の一部修正について

非保持化実現加盟店における過去のカード情報保護対策

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 - 2018 - （案）について

第 20 回　2018 年 1 月 30 日

議題：メールオーダー・テレフォンオーダー加盟店におけるカード情報保護対策について
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 - 2018 - （案）について

第 21 回　2018 年 2 月 9 日

議題：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 - 2018 - （案）について

◆クレジットカード偽造防止対策 WG（WG2）

第 1 回　2015 年 4 月 21 日

議題：クレジット取引における不正被害の状況とクレジット業界のこれまでの取組について
カード偽造防止対策 WG の検討課題と検討の進め方について

第 2 回　2015 年 5 月 18 日

議題：IC カード対応への取り組みを進める上での課題について①

第 3 回　2015 年 6 月 11 日

議題：IC カード対応への取り組みを進める上での課題について②

第 4 回　2015 年 7 月 1 日

議題：本会議に向けた中間論点整理と今後の検討の方向性について

第 5 回　2015 年 9 月 18 日

議題：2020 年のあるべき姿及び優先的に取り組む課題と具体的な論点等について
SWG の設置及び座長会社の選任等について

第 6 回　2015 年 11 月 17 日

議題：オペレーション SWG の検討状況について
実現方式検討 SWG の検討状況について
WG の今後の進め方について

第 7 回　2015 年 12 月 18 日

議題：WG2 実行計画（案）について①　等

第 8 回　2016 年 2 月 2 日

議題：WG2 実行計画（案）について②

第 9 回　2016 年 4 月 22 日

議題：今後の進め方について
国際ブランドルールの確認結果と IC 取引のオペレーションの考え方の取りまとめについて

第 10 回　2016 年 12 月 16 日

議題：残課題の検討状況について
実行計画 2017 について

第 11 回　2017 年 1 月 17 日

議題：実行計画 2017 について
残課題の現状報告

第 12 回　2017 年 2 月 3 日

議題：実行計画 2017 について

第 13 回　2017 年 2 月 17 日

議題：実行計画 2017 について

第 14 回　2017 年 6 月 16 日

議題：実行計画 2017 重点的に実施すべき具体的な取組状況について

第 15 回　2017 年 11 月 1 日

議題：実行計画 2017 取組み報告

実行計画 2018 について

実行計画ガイドラインについて

第 16 回　2018 年 1 月 24 日

議題：クレジットカード IC 化向けた取組報告

加盟店に対する決済システムの IC 対応に向けた取組

IC 対応に向けた加盟店周知活動報告

◆不正使用対策 WG（WG3）

第 1 回　2015 年 4 月 27 日

議題：クレジット取引における不正被害の状況とクレジット業界のこれまでの取組について

不正使用対策 WG の検討課題と検討の進め方について

第 2 回　2015 年 5 月 13 日

議題：EC サイトでの不正使用対策を進める上での課題について①

第 3 回　2015 年 6 月 9 日

議題：新たな本人認証の方策について

EC サイトにおける不正発生被害状況等について

第 4 回　2015 年 7 月 9 日

議題：本会議に向けた中間論点整理と今後の検討の方向性について

第 5 回　2015 年 9 月 16 日

議題：2020 年のあるべき姿及び優先的に取り組む課題と具体的な論点等について

検討課題に対する具体的な進め方について

不正使用対策を講じていない加盟店等に対する具体的な対策等について①

第 6 回　2015 年 10 月 19 日

議題：不正使用対策を講じていない加盟店等に対する具体的な対策等について②

既存の本人認証手法の課題を踏まえた普及に向けた具体的な方策について

第 7 回　2015 年 11 月 12 日

議題：グローバルでの不正利用と対策の動向

非対面取引におけるクレジットカードの不正使用対策の強化に向けた実行計画について①

第 8 回　2015 年 12 月 4 日

議題：EC 取引におけるクレジットカードの不正使用対策の強化に向けた実行計画について②

第 9 回　2016 年 2 月 6 日

議題：ＥＣ取引におけるクレジットカードの不正使用対策の強化に向けた実行計画について③

第 10 回　2016 年 6 月 2 日

議題：今後の進め方について

3D セキュア 2.0 の概要について

第 11 回　2016 年 8 月 9 日

議題：実行計画におけるなりすまし防止対策の推進状況等について（報告）

3D セキュア 2.0 の影響と今後の対応等について

第 12 回　2016 年 10 月 17 日

議題：カード会社による加盟店への現状確認の結果と判明した課題への対応について

3D セキュア 2.0 の状況について

第 13 回　2016 年 11 月 16 日

議題：3D セキュア 2.0 の対応について

不正被害の多い業種の検証について

第 14 回　2016 年 12 月 14 日

議題：実行計画 2017 について

第 15 回　2017 年 1 月 13 日

議題：実行計画 2017 について

第 16 回　2017 年 2 月 6 日

議題：実行計画 2017 について（継続審議）

第 17 回　2017 年 2 月 21 日

議題：実行計画 2017 について（継続審議）

第 18 回　2017 年 5 月 15 日

議題：2017 年度の重点取組課題の進め方について

SWG（サブワーキング）の組成について

第 19 回　2017 年 7 月 28 日

議題：なりすまし防止対策の基準の検討状況について

第 20 回　2017 年 10 月 12 日

議題：なりすまし防止対策の基準について（SWG の取りまとめ案）

実行計画 2018 に向けての取組みについて

第 21 回　2017 年 12 月 26 日

議題：好事例のレポートについて　（SWG の取りまとめ案）

消費者への情報発信等について

実行計画 2018 に向けての取組みについて

第 22 回　2018 年 1 月 25 日

議題：実行計画 2018 について

第 23 回　2018 年 2 月 6 日

議題：実行計画 2018 について（継続審議）

第 24 回　2018 年 2 月 13 日

議題：実行計画 2018 について（継続審議）

実行計画 2018（案）について（共通部分）

消費者における不正利用対策への理解・認知向上のための取組について