別紙２

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－
【公表版】

２０１７年３月８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引高は堅調に拡大を続けており、2015 年には取扱高 49 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「日本再興戦略 2016」（2016 年 6 月 2 日）において、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）では、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た。

また、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、我が国が 2020 年までに達成すべき目標の実現に向け、関係事業者が連携し、「実行計画」に基づく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

[1] 本実行計画では、インターネット上の取引において EC 店舗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。

において全会一致で可決され、同年 12 月 9 日に公布された（施行期日：公布日から 1 年 6 ヶ月以内の政令で定める日）。

2018 年 6 月までに予定される「割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）」の施行に向け、本実行計画は、加盟店等がセキュリティ対策に関する義務を履行する際の実務上の指針となるものでもあり、その重要性はますます高まっているものといえよう。

今般改訂された 2017 年度の実行計画は、2016 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、対策に関する記載の具体化・精緻化や課題の解決を図った結果を反映するとともに、引き続き検討を進めるべき課題や 2017 年度の重点取組事項を整理したものである。

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。

2017 年 3 月 8 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使用被害の実態等

我が国のクレジットカードの不正使用被害は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 2015 年には約 120 億円の被害が確認されている。2016 年は 1 月から 9 月までに、すでに 106.8 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、こうした不正使用被害は、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。

非対面取引においては、漏えいしたカード情報の EC 加盟店における不正使用の伸びが顕著となっており、全体の 6 割以上を占めていることを踏まえ、カード会員本人になりすました不正使用の様々な手口に対して実効的に対処するため、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使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 化を進めていく必要がある。特に、我が国と同様に、IC 対応化が遅れていた米国の動向に目を向けることが重要である。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 月には IC 対応を進める大統領令が発令され、2018 年までに 92%の決済端末を IC 対応化する方向で急速に取組を進めている。こうした状況を踏まえれば、これまで米国で発生していた年間 1 兆円超（世界の不正使用の約 6 割を占める）の不正使用が我が国にシフトしてくることは、10 年ほど前に欧州で IC 対応が進んだ際に不正使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り、我が国において対面加盟店における IC 対応化を進めていくことは喫緊の課題となっている。

2016 年 5 月には南アフリカの銀行で発行されたカードの偽造による不正キャッシングが日本国内のコンビニの ATM で一斉に行われ、約 3 時間の間に 18 億円超の被害が生じた。この事件は、国際的な犯罪組織がセキュリティの甘い日本を狙ったものではないかとする見方もあり、我が国の「セキュリティホール化」の一つの兆しとも言える。こうした国境を越えた不正取引被害を防ぐためには、本実行計画に基づく取組を早急に進めていくことが必要である。また、これら不正使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正義の観点からも不正使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、不正使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頻発している。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。

我が国がセキュリティホール化し、不正使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各主体は共有した上で、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 年に向けたセキュリティ対策の強化の具体的な方策を検討するにあたり、消費者が享受しているクレジットカードの利便性を勘案しつつ、以下の点に留意し進めた。

（１）加盟店におけるセキュリティ対策の義務化とその履行確保のためのカード会社（アクワイアラー）等の加盟店管理

現行割賦販売法では、カード会社（イシュアー及びアクワイアラー）に対してカード情報の適切な管理が義務づけられているところ、今般の法改正により、加盟店についても、カード情報の適切な管理及び不正利用防止のための措置が義務づけられ、契約先のカード会社（アクワイアラー）等がその履行状況を確認し、是正指導や契約解除等の必要な措置を講じることとされた。

また、セキュリティ対策が不十分であったために加盟店契約を解除された場合､その事実は認定割賦販売協会における加盟店情報交換制度（データベース）に登録され、カード会社（アクワイアラー）間で広く共有されるため、実効的な再発防止策を講じない限り、クレジットカード決済を継続することは困難となる。

この改正割賦販売法の施行に向け、加盟店において、本実行計画に基づく取組を加速化させていく必要がある。

（２）加盟店の取引形態及び不正使用の手口等リスクに応じた方策の導入

対面取引では偽造されたクレジットカードによる不正使用、EC 加盟店では窃取されたカード情報による不正使用と、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・不正使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

がゆえに不正使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。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ためリスクは低いと想定され、本実行計画の対象としていないものの、リスクに応じたカード情報保護及び不正使用対策が必要である点に留意する。

（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すで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、不正使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

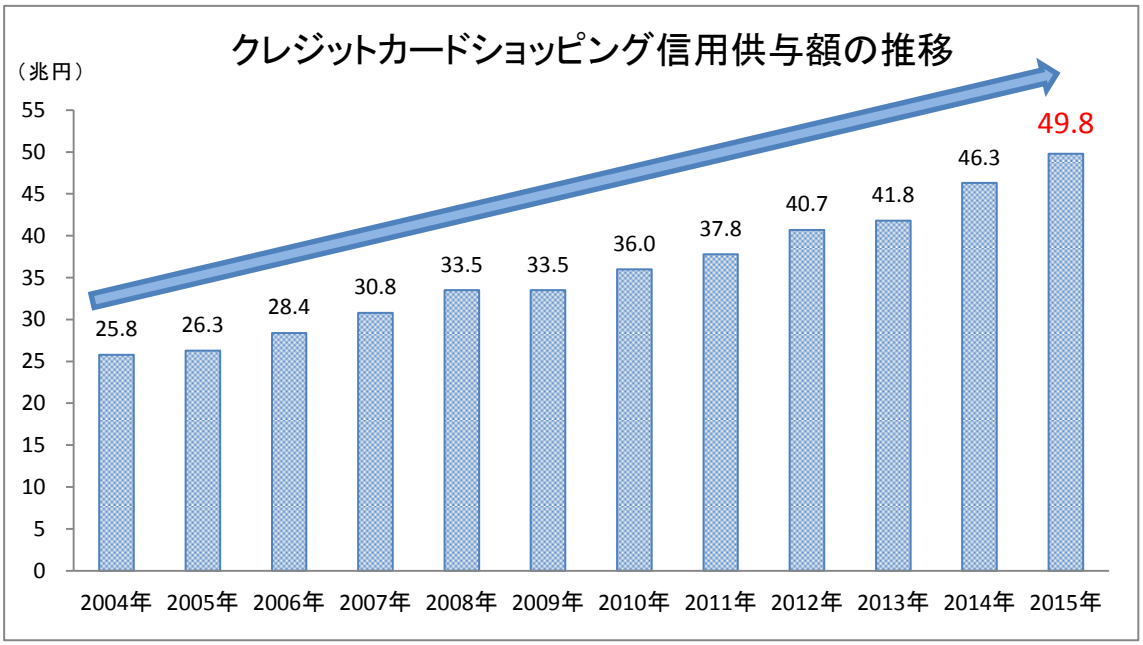
カード会社や加盟店等の不正使用対策に加えて、消費者自身のクレジットカードの不正使用に対する認知・意識の向上を図るため、より効果的な消費者に対する情報発信等によって理解・協力を得ることも、セキュリティ対策強化の観点から必要な取組である。

以上の点に加えて、不正使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、不正使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 月末までに不正使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・安心なカード利用環境の実現を図るものである。

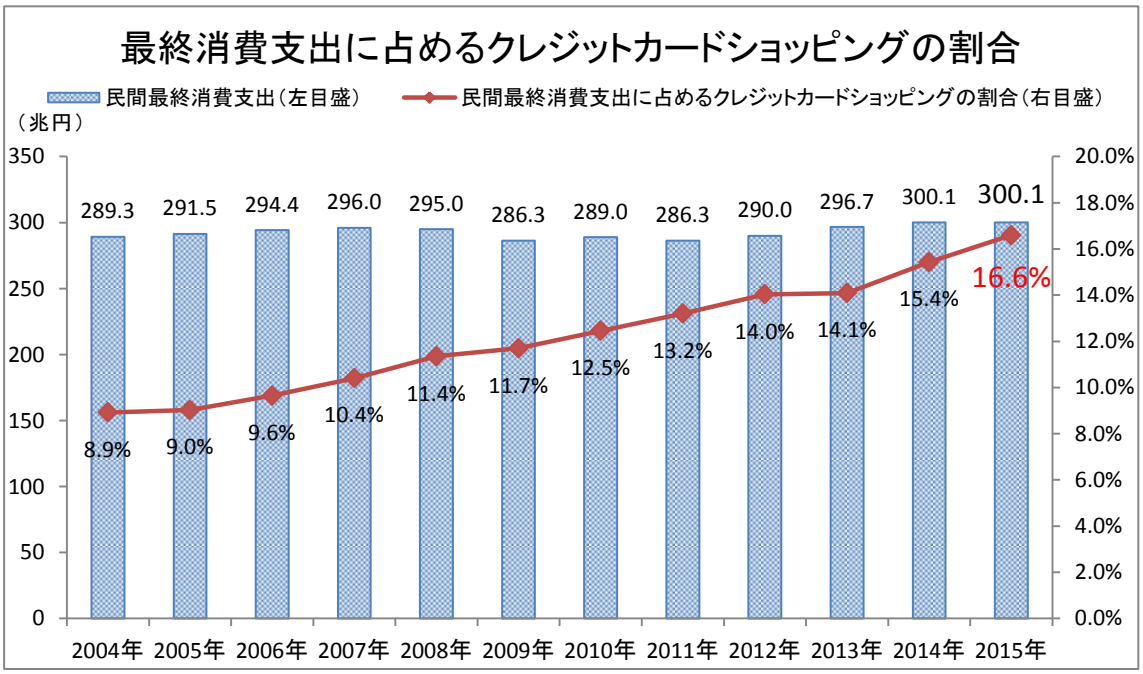
参考資料

（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」

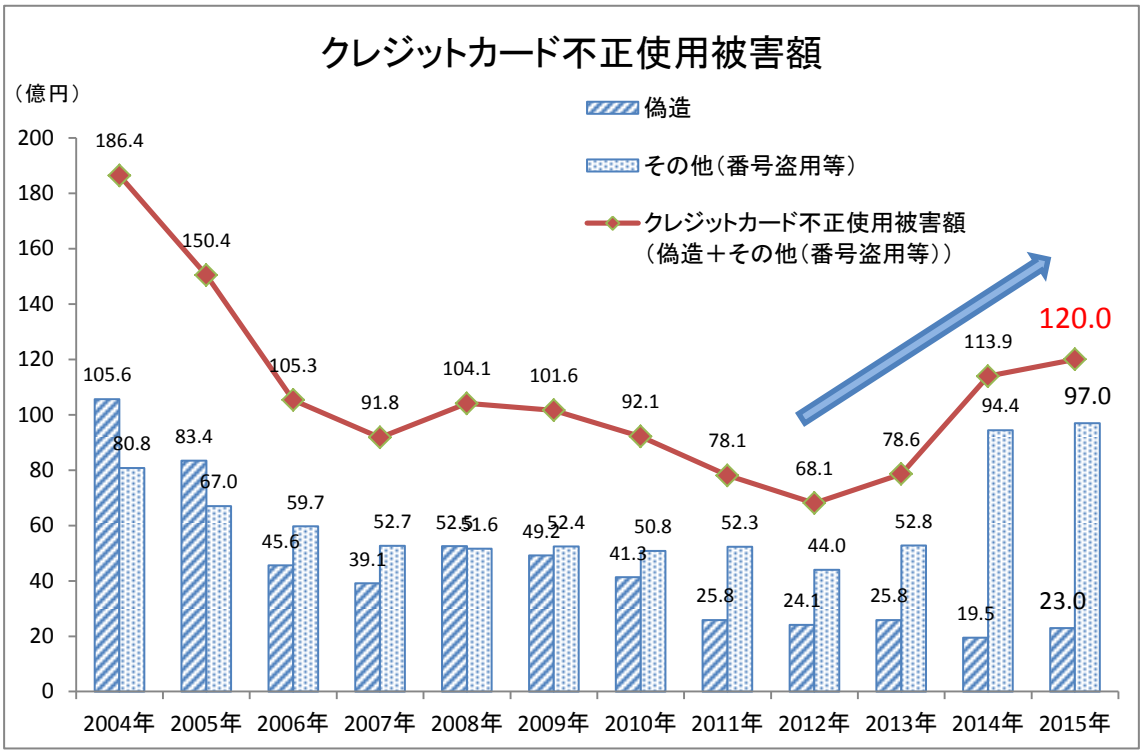
（資料２）



出所：内閣府「国民経済計算年報」民間最終消費支出：名目

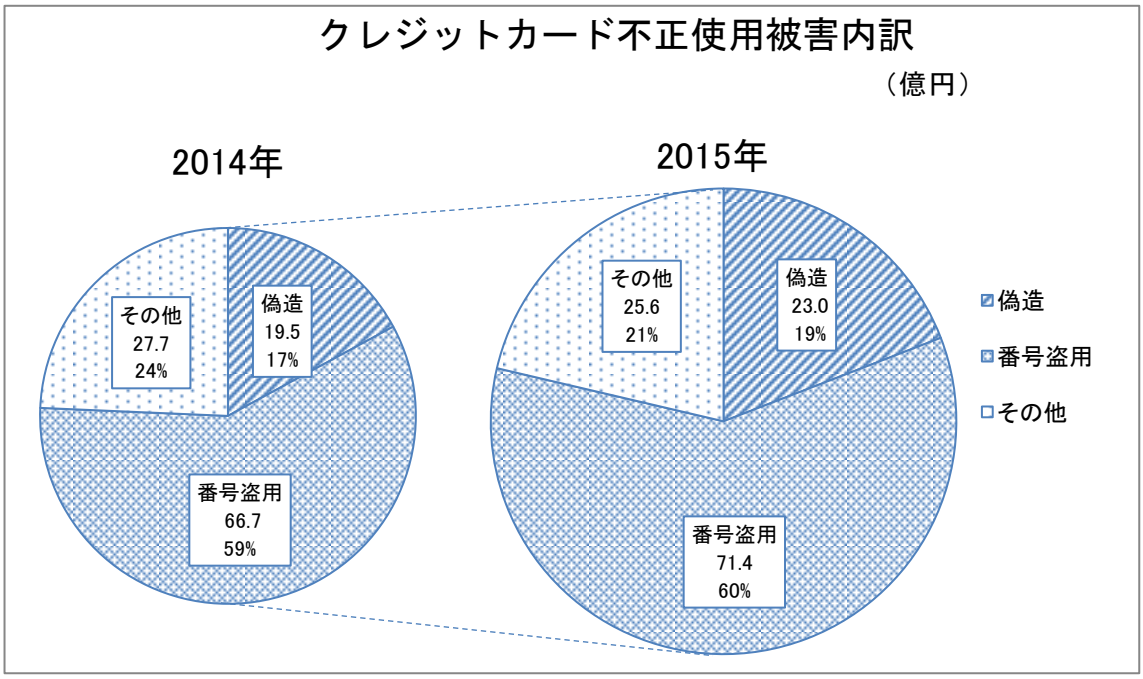
出所：一般社団法人日本クレジット協会「信用供与額」

（資料３）



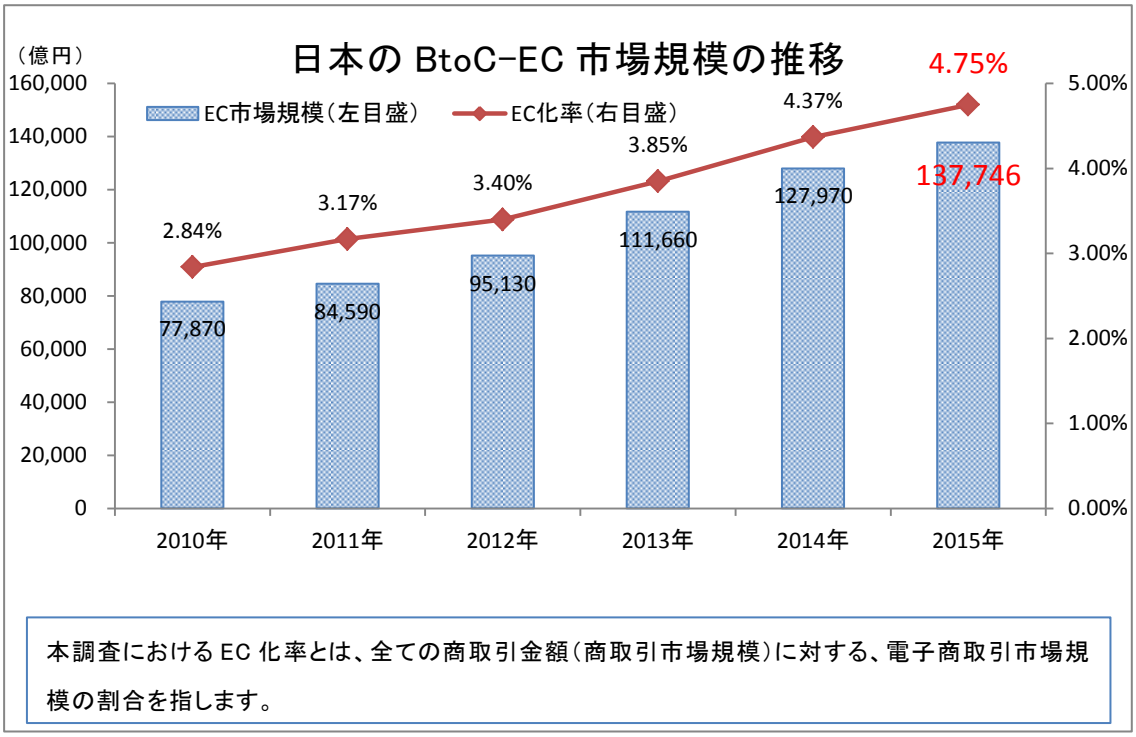
出所：一般社団法人日本クレジット協会「クレジットカード不正使用被害額の発生状況」

（資料４）



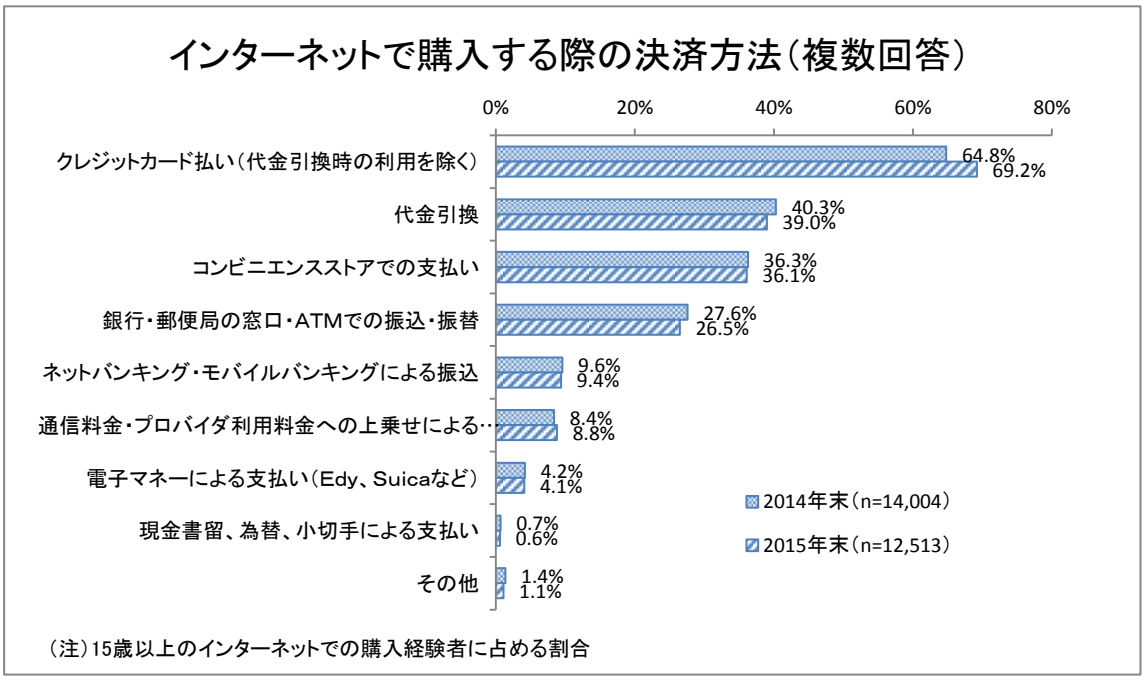
出所：一般社団法人日本クレジット協会「クレジットカード不正使用被害額の発生状況」

（資料５）



出所：経済産業省「平成２７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２７年通信利用動向調査の結果（概要）」

Ⅱ．分野別の具体的な実行計画

具体的な実行計画の策定あたっては、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使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	不正使用対策
対面取引	偽造カード、紛失・盗難カードによる不正使用	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・不正使用検知の強化 →WG3

Ａ．クレジットカード情報保護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[2]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せられていたが、2016年 12 月に公布された改正割賦販売法において、加盟店にも義務が課せられることとなった。

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使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。

2016 年においても情報漏えいに起因する偽造被害・なりすまし被害は増加していることから、本実行計画でのカード情報保護を目的としたセキュリティレベルの向上はさらに重要性を増している。

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（イシュアー・アクワイアラー）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特に喫緊の課題である。

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

---

[2] 「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（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）

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[3]（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るため、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、準拠に向けた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使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。

以上の考え方に基づき、2018 年 3 月末までに、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（イシュアー・アクワイアラー）及び PSP については PCI DSS 準拠を求めることとする。また、改正割賦販売法が遅くとも 2018 年 6 月に施行されることから、対面加盟店においても、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。

加盟店等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、IC 対

[3] PCI DSS については別紙参照。

応した決済専用端末（CCT 及びそれと同等以上のセキュリティレベルのもの[4]。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。後述「A.2.（2）対面加盟店におけるカード情報の非保持化について」参照）。

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使用の未然防止が可能となる。

なお、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。

（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

①現状の課題と対策に関する整理

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 2016 年の 1 年間で報告されたカード情報の漏えい事故（前年比約 1.5 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、カード情報の窃取を抑止するためには、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必要である。

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 を使用した非通過型」）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 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。

---

[4] CCT とは、Credit Center Terminal の略。IC 対応した決済専用端末のセキュリティレベルに関しては、後述の「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」を策定する際に、併せて整理する。

②EC 加盟店への対応

■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

すで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、これら加盟店に対する注意喚起を行い、早急に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システム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とする事例もあり、注意が必要である。

その上で、カード情報を保持する場合は PCI DSS 準拠を求める。

③メールオーダー、テレフォンオーダー等の非対面加盟店への対応

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においては、その際に用いられるカード情報を電話・FAX・はがき等での顧客からの注文によりカード決済をする場合がある。紙媒体のまま保存する場合は非保持となるが、それら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。

（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を「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こと（外回り方式）によってカード情報の非保持化を実現することが可能となる。

ただし、カード会社や ASP[5]（Application Service Provider）事業者等より、クレジットカード番号を含む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」している場合や決済以外の目的でカード情報を同様に保持している場合は非保持とはならない。

[5] アプリケーションソフト等のサービスをネットワーク経由で提供する事業者・仕組み全般のこと。

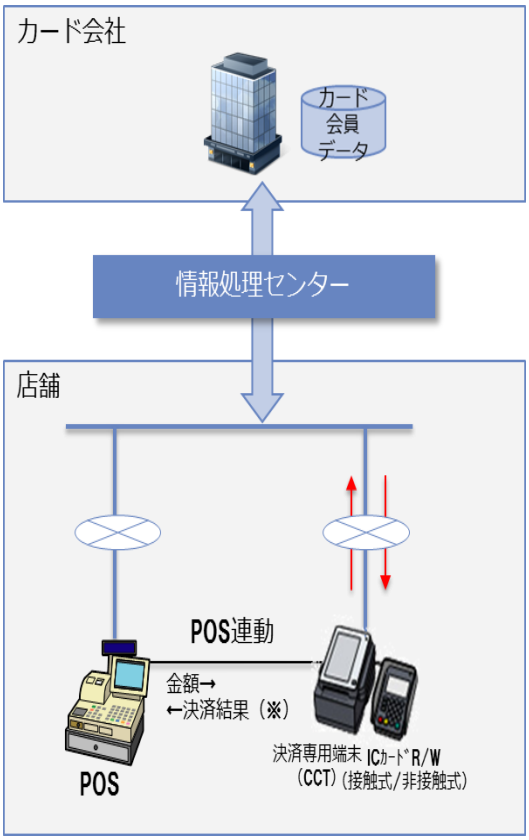
なお、決済機能の分離は、各加盟店の現行システムや店頭オペレーション等の特徴を踏まえ、コスト負担の低減が可能となる方法を検討すべきであることから、後述の POS システムの IC 対応とリンクして検証を行った。

■決済専用端末連動型・ASP/クラウド接続型(外回り方式)

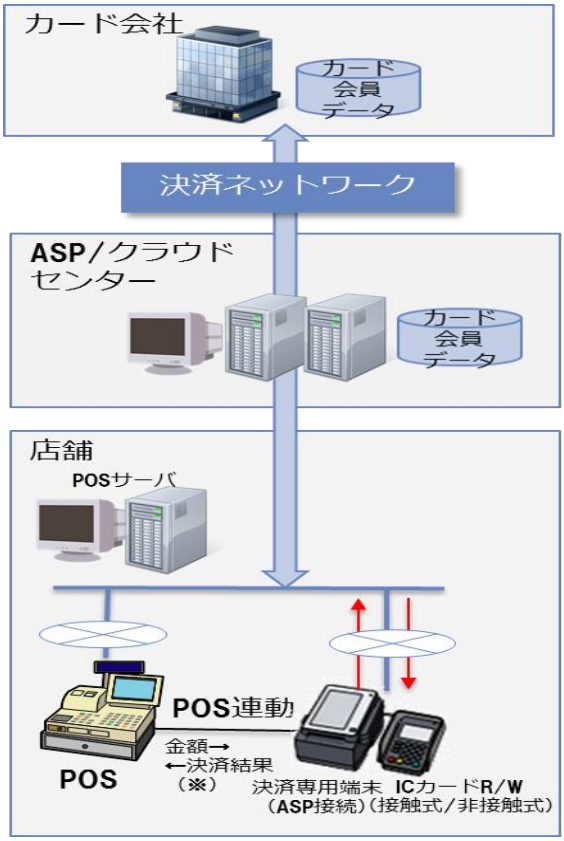
「決済専用端末連動型」・「ASP/クラウド接続型」（外回り方式）は、加盟店あるいはカード会社等が所有する IC 対応した決済専用端末から直接、外部の情報処理センター又は ASP/クラウドセンター等に伝送される仕組みである。

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。

【決済専用端末（CCT）連動型（外回り）】



【ASP/クラウド接続型（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

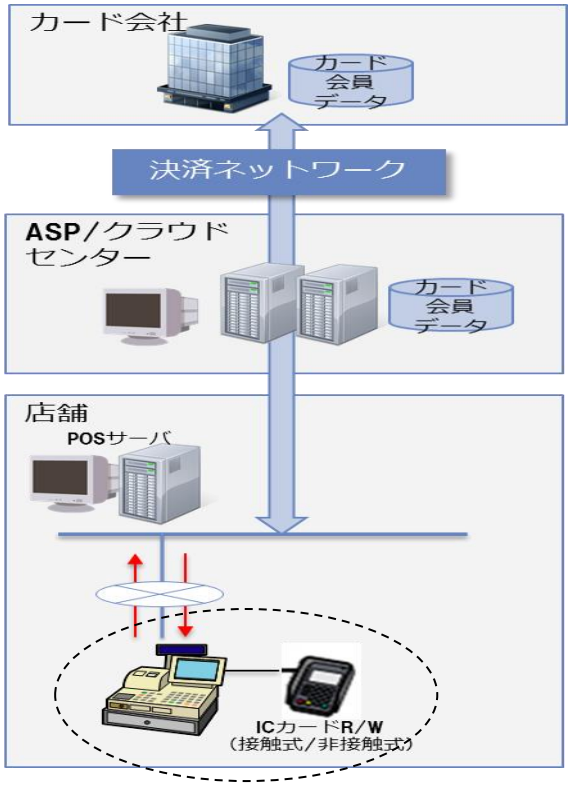
なお、POS システムを導入せず「IC 対応した決済専用端末」のみを使用し、直接、外部の情報処理センター等に伝送している加盟店は非保持となる。

■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 ASP 事業者・情報処理センター等外部事業者へ送られる方式である。

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、「非保持」とならず、原則として PCI DSS 準拠が必要となる。ただし、暗号化等の処理により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使用することは極めて困難であり、非保持と同等/相当のセキュリティが確保できるため、本実行計画においては、これを「非保持化」と同等/相当のセキュリティ措置として扱うものとする。こうした措置の一例として、PCI P2PE[6]（PCI Point to Point Encryption）がある。（「非保持化」と同等/相当のセキュリティ措置については後述（４）を参照）

【ASP/クラウド接続型（内回り）】



（POS（決済機能内蔵型））

6 「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。加盟店自社内を伝送処理したとしても DUKPT（暗号キーがそれぞれ違う）という暗号鍵管理の仕組みにより、仮に漏えいし解読された場合でも解読されたカード番号だけが使用可能なため（暗号キーがそれぞれ違うため、解読方法もそれぞれ違う）、漏えいした場合にでも不正使用されるリスクは極めて小さくなる。

（３）カード情報の非保持化を実現した場合の顧客対応

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

EC 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、すでに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、全ての加盟店・カード会社がカード番号以外のキーにて一律に同レベルでの対応は現状困難であり、カード番号を基本として双方照会する必要があると考えられる。

実行計画上の「非保持化」を実現した加盟店がカード番号を照会キーとして利用する方法としては、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 等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して利用する方法が考えられる。

なお、加盟店での運用実態に即した具体的な対応方法については、継続して検討していくこととする。

（４）「非保持化」と同等/相当のセキュリティ措置について

前述（２）の「ASP/クラウド接続型（内回り方式)」等のように「非保持」とならない場合においても、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検討するため、本協議会の下に本件を扱う「サブ・ワーキンググループ」を設置し、技術要件を定め、対面加盟店における具体的なソリューションの検討を促すこととする。

３．カード情報を保持する加盟店の PCI DSS 準拠の推進について

加盟店によっては、実務上の都合から非保持化が困難な場合もあることから、このようなカード情報を保持する全ての加盟店に対しては、PCI DSS 準拠を求める。

しかし、PCI DSS については加盟店によっては必ずしも十分な認知が進んでいないことや、準拠への社会的要請が十分に認識されていないことが大きな課題であることから、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周知・啓発活動の推進と、その準拠に向けた加盟店の取組をサポートするための体制を構築

する。

（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 準拠に向けた対応を円滑に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 に関する理解増進のための講師派遣

・カード会社向け、関係業界団体等・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増進を図るための講師派遣を行う。

②PCI DSS に関する理解増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

・相談者が理解しやすいよう認定審査機関（QSA[7]（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**[8]（Internal Security Assessor）等の人材育成を支援する。

---

[7] 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。

[8] 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。

（３）カード情報を保持する対面加盟店の PCI DSS 準拠の推進

加盟店によっては、実務上の都合から非保持化が困難な場合もあり、この場合には PCI DSS 準拠が必要となる。

改正割賦販売法により、加盟店におけるカード情報保護が義務化されることを踏まえ、PCI DSS 準拠の対象範囲（スコープ）を最小化することで負担軽減が図られた事例を共有することにより、加盟店側の対応を推進していくことが有効策の一つになると考えられる。

このため、本協議会は、関係事業者の協力を得て情報収集を行い、2017 年度の協議会活動の中で、いくつかのモデルケースをとりまとめ・公表することにより、加盟店側の具体的な取組を進めやすい環境をつくっていくことが重要である。

４．加盟店以外の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、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 の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早急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。

また、カード会社は 2018 年 4 月を目処に、PCI DSS に準拠完了していない PSP との取引の見直しについて検討を進める。

なお、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。日本クレジットカード協会では、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策定し、有事の際の参考に供している。

本協議会は、日本クレジットカード協会の協力を得て、同マニュアルの利用範囲を協議会参加者へ拡大し、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。

また、カード決済を停止させた場合、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したうえでカード決済を再開させることとする。

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。

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の自主的な取組を進めることが重要である。

なお、カード情報保護の対策は、目前のリスクを排除するために早急に着手すべき課題であり、事業者の個別事情を考慮しつつも各主体は本実行計画に示す期限を待つことなく、可能な限り前倒しで対応を進める。

また、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。

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、2018 年 3 月末までにカード情報の非保持化又は PCI DSS 準拠完了を目指す。なお、通過型システムを導入している EC 加盟店は、自社のシステムのトランザクションログ等においてカード情報のログが蓄積されていないか、至急確認を行い、蓄積されている場合は削除するものとする。

・改正割賦販売法が遅くとも 2018 年 6 月に施行されることから、対面加盟店においても、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、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セキュリティ対策の強化に取組むことが重要である。

・EC 及び対面取引の両方を行う加盟店は、EC に係るシステムについては 2018 年 3 月末までに、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。

・カード情報を非保持化していない加盟店においては、PCI DSS 準拠に加えて、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（アクワイアラー）及び PSP

・カード情報を取り扱うカード会社（アクワイアラー)及び PSP は、2018 年 3 月末までに PCI DSS 準拠完了を目指す。

・カード会社（アクワイアラー）及び PSP は、加盟店のカード情報の非保持化又は PCI DSS の準拠に向けて、必要となる技術的な情報提供や、サポート体制を構築する JCDSC 等への誘導等により、早期の準拠が実現できるよう協力する。

・カード会社（アクワイアラー）と PSP は、協力して EC 加盟店の非保持化（非通過型システムへの移行を含む）又は PCI DSS 準拠完了を推進する。

・加盟店の非保持化又は PCI DSS 準拠の完了については、カード会社（アクワイアラー）及び PSP が確認する。

・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 に対して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、2018 年 4 月を目処に、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、これら加盟店等への丁寧な対応に留意する。

（３）カード会社（イシュアー）

・カード情報を取り扱うカード会社（イシュアー）は、2018 年 3 月末までに PCI DSS 準拠完了を目指す。

・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・啓発等を行う。

（４）国際ブランド

・PCI DSS 準拠に向けた加盟店の取組を推進するため、対象範囲（スコープ）を最小化することで負担軽減を図った海外加盟店の事例（モデルケース）について適宜情報提供を行う等、関係事業者への周知に協力する。

・実行計画の着実な実施を図るため、我が国のクレジットカード取引の実態を踏まえ、加盟店及び PSP の PCI DSS 準拠に関する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、海外での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、改正割賦販売法の施行までに必要な措置が導入されるよう、カード会社（アクワイアラー）等を通じた加盟店に対する周知を徹底するとともに、加盟店の業種別団体等に対する働きかけを積極的に行う。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。

・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 3 月策定予定）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。

７．2017 年度中に重点的に実施すべき具体的な取組について

本実行計画を踏まえて、安全・安心なクレジットカードの利用環境の実現を図ることとする。平成 28 年度経済産業省委託調査（平成 28 年 10 月時点）によれば、対面加盟店のカード情報保護について、非保持化対応完了は全体で 17.5%、PCI DSS 準拠完了は全体で 3.6%にとどまっており、取組が遅れている状況にある。また、非対面加盟店では、79.5%が PSP を活用しているが、うち 70%が「通過型」となっており、「非通過型」への移行が進んでいない状況にある。

2016 年 12 月 9 日に公布された改正割賦販売法により、加盟店におけるクレジットカード番号等の適切な管理が義務化されることを踏まえ、改正割賦販売法の施行に向け、カード情報の非保持化又は PCI DSS 準拠を早急に進めていく必要がある。

こうした観点から、2017 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にする。

（１）非対面加盟店におけるカード情報非保持化又は PCI DSS 準拠に向けた取組

本実行計画上、非対面加盟店については、2018 年 3 月末までにカード情報の非保持化又は PCI DSS 準拠完了を目指すことになっており、日本クレジット協会は、カード会社（アクワイアラー）、PSP 業界団体等と連携の上、非対面加盟店におけるセキュリティ対策の進捗状況を管理し、当該目標に向けた取組を強化する。

（２）対面加盟店におけるカード情報非保持化等に向けた取組

カード情報の適切な保護を推進するために、加盟店における非保持化を推進することを基本として、その方策の具体的説明や導入方法等について、各主体が協働して取組む。

また、対面加盟店においてカード情報の適切な保護を推進するため、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、「サブ・ワーキンググループ」において早急に検討を行い、今春を目途に結論を得て、関係事業者に対して周知する。

（３）「通過型」を採用している EC 加盟店への対応

カード情報が通過する「通過型」を採用している EC 加盟店については、トランザクションログ等においてカード情報が蓄積されている可能性があるため、カード会社（アクワイアラー）及び PSP は、早急にシステムログ等の消去を求めるとともに、A．2.（1）．②（EC 加盟店への対応について）に述べたとおり非通過型への移行を強く推奨し、その上でカード情報を保持する場合は、PCI DSS 準拠を求める。

また、日本クレジット協会は、カード会社（アクワイアラー）、PSP 業界団体等と連携の上、EC 加盟店向けの広報資料を作成し、EC 加盟店に対するこうした取組を促進していくこととする。

（４）PCI DSS 準拠に向けた加盟店に対するサポート体制

A．3.（カード情報を保持する加盟店の PCI DSS 準拠の推進）に述べたとおり、カード情報を保持する加盟店等が PCI DSS 準拠に向けた対応を円滑に図ることをサポートするため、本協議会は、PCI DSS 準拠の対象範囲（スコープ）を最小化することで負担軽減が図られた事例に関して情報収集を行い、これをモデルケースとして取りまとめて関係事業者に共有し、PCI DSS 準拠の早期実現に向けた取組を行う。

また、PCI DSS 準拠に関する加盟店側の理解増進のため、カード会社（アクワイアラー）及び PSP は、クレジットカード関係業界団体や JCDSC 等が開催するカード情報保護に関するセミナー等へ誘導する。

（５）カード会社と PSP における早急な PCI DSS 準拠の完了

カード情報を取り扱うカード会社及び PSP は、2018 年 3 月末までに確実に PCI DSS 準拠を完了することを目指すとともに、未だ準拠していない場合には、目標期限に向け、早急に取組を進める。

特に、EC 加盟店における非保持化（非通過型システムへの移行を含む）に伴い、今後ますます大量のカード情報が PSP に集約されることになることを踏まえ、PCI DSS に準拠していない PSP については早急に準拠完了を目指す。

日本クレジット協会は、行政と連携の上、カード会社及び PSP による PCI DSS 準拠の実現に向けた取組について進捗管理を行う。

B．クレジットカード偽造防止対策等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

現在の我が国のクレジットカード取引は、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使用する被害が後を絶たず、その対策として取引の IC 化を進め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使用対策として 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カード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。

カード業界においては2000年代より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 2016 年 12 月末時点で、目標の 80%に対し、75.4%[9] にとどまっている。80%目標が達成できなかった要因としては、一部カード会社（イシュアー）において、提携カード発行先との調整やシステム改修の遅延等によりICカードへの切替えが予定通り進まなかったこと等が挙げられる。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、改正割賦販売法施行に向け、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 対応については、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を中心に順調に進捗しているものの、全体としては IC 対応が諸外国と比して遅れている。特に、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いては、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、決済システムや店頭の端末の IC 対応への移行費用や接客オペレーション等の対応が負担となる点が大きな課題となっている。

---

[9] 日本クレジット協会が会員企業 231 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、2016 年 12 月末時点の目標 80%を達成している企業は 179 社、うち、100%達成済みの企業は、73 社。

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。

なお、POS システムの IC 対応の改修を図る際に、カード情報保護に資する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。

改正割賦販売法が遅くとも 2018 年 6 月に施行されることから、決済端末の IC 化についても、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状態になっ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 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、「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である。初版では、カード及び端末の普及状況を踏まえ「接触型 IC 取引」を対象とした記載となっているが、今後は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も想定されることから、「非接触型 IC 取引」につ

いての記載を追加する。

（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）」[10]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人確認方法である。また、現在 100 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通りとする。

・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[11]。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）すで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、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 による本人確認を実施しないことで不正使用が発生する可能性があることを十分に認識し、将来的な廃止を継続検討する。

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。

---

[10] 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 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。

[11] 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 処理を推奨する。

非接触 IC カードの取引の多くは CVM[12]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、以下の通りとする。

・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、以下の通りとする。

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[13]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。

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[14]。

・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[15]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。

---

12 「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。

13 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。

14 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」に限定して、「接触 IC 取引へ誘導」することを選択可能とすること。

15 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。

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、不正使用のリスクが低い業種/売場等であることを前提とする。

また、不正使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。

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、CVM リミット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なった。今後、運用開始時期について継続協議を行う。

④本人確認不要加盟店でのオーソリの要否

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を必須とする。

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、決済サーバー接続経由型、ASP/クラウド接続型に大別[16]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

[16] 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の強化に向けた実行計画』（P14～P16）の記載内容を参照。

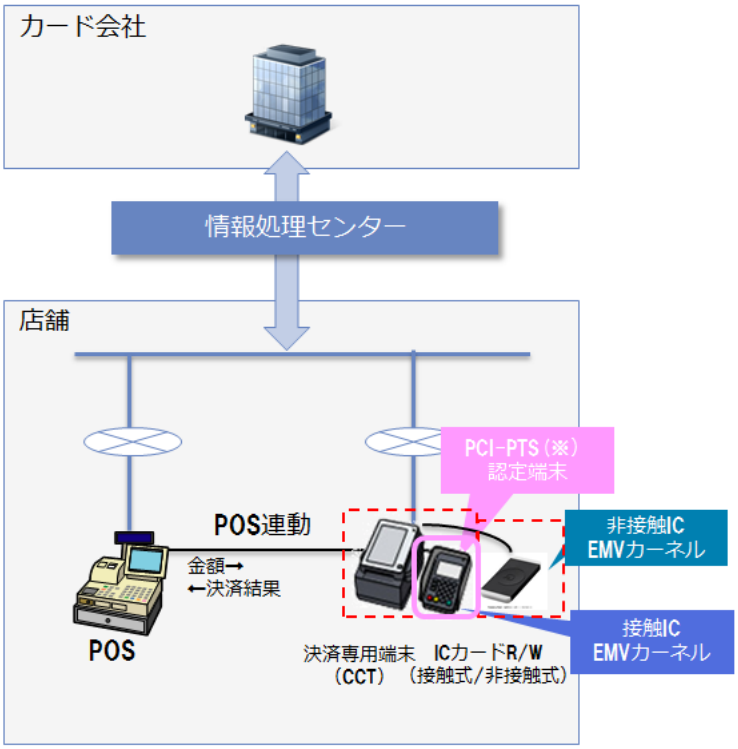
ターンのコストを可視化し、各方法の技術面等の検証・整理した。

■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 PINPAD 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が同時実現できる。

一方で、決済専用端末[17]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】

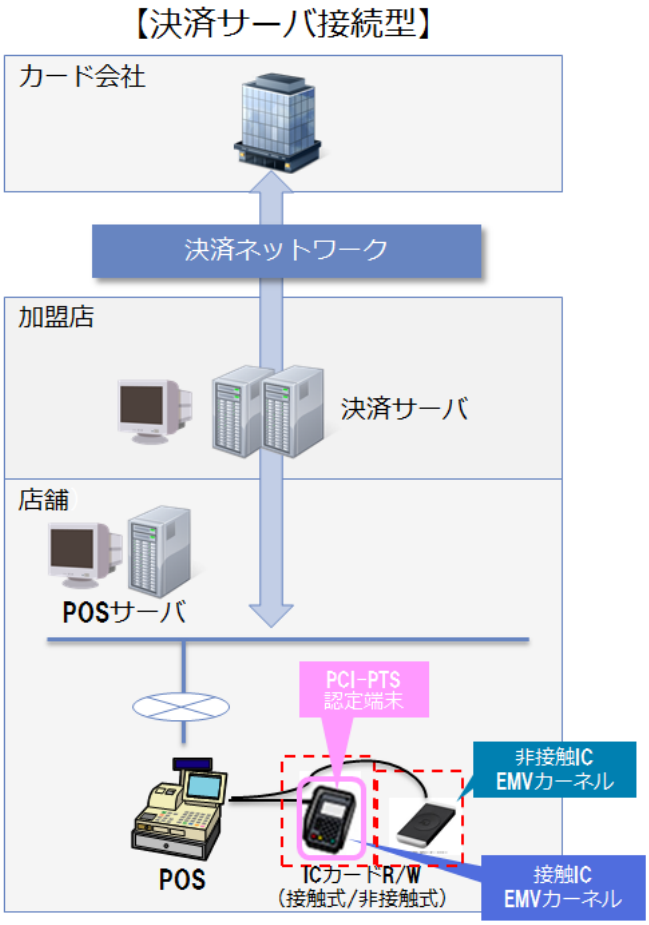


[17]※PCI PTS（Pin Transaction Security）とは、PCI SSC が定めた、PIN 取引を保護する PIN 入力装置の国際的なセキュリティ基準。

■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 PINPAD 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、PCI DSS 準拠又は非保持化と同等/相当のセキュリティ措置[18]を講じることが必要となる。

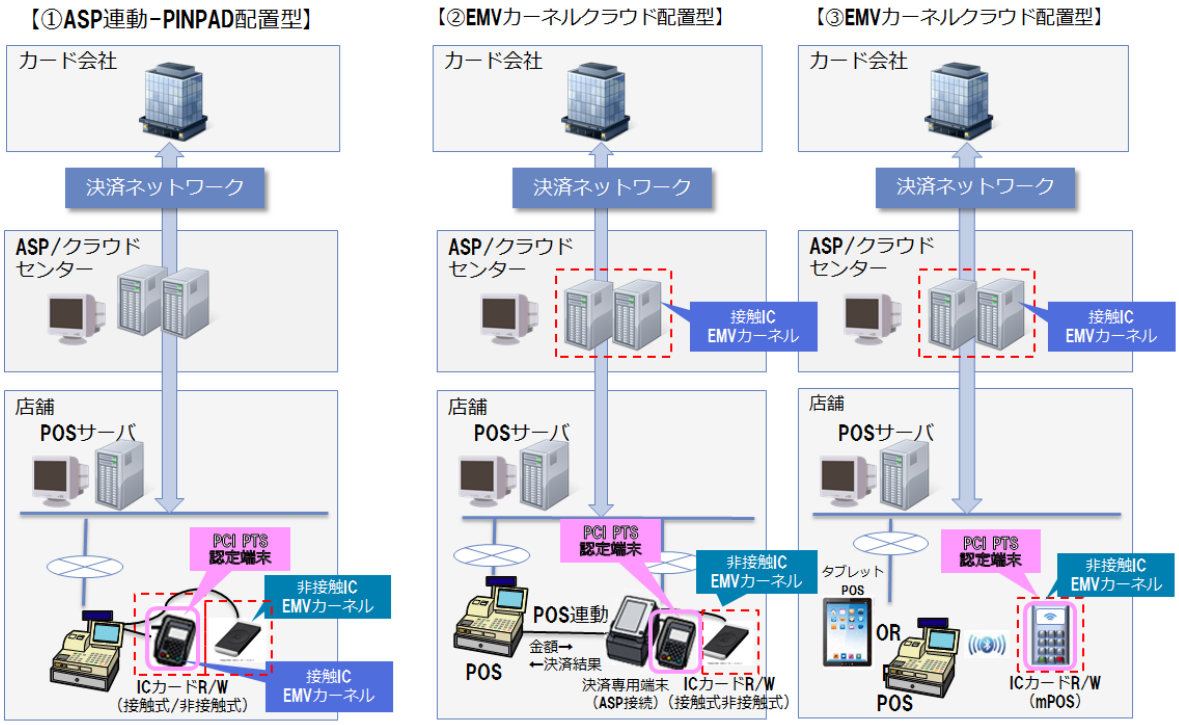


18 対面加盟店において非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件については、「サブ・ワーキンググループ」にて検討予定（A.2.（4）参照）。

■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実現できる。下記①及び③の場合には、カード情報は POS システムを通過し ASP/クラウドセンターを経由してカード会社に伝送されるため、PCI DSS 準拠又は非保持化と同等/相当のセキュリティ措置[19]を講じることが必要となる。



（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-PINPAD、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。

19 対面加盟店において非保持と同等/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は、「サブ・ワーキンググループ」にて検討予定（A.2.（4）参照）。

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（Open Point of Servise）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。さらに、POS システムを導入する際に IC 対応しない加盟店でも、後から簡易に IC 機能を活性化できる仕組みを搭載する。

（４）その他 IC 対応 POS システムのコスト低減に向けた検討について

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。今後、本ガイドラインを機器メーカー等への連携し、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、2016 年 12 月末時点で 71.2%と順調に進捗してきているが、加盟店における不正利用防止措置が義務付けられる改正割賦販売法の施行に向け、IC 対応していない 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．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

・改正割賦販売法が遅くとも 2018 年 6 月に施行されることから、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、自社に最適な対応方策を検討する必要があるが、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。

（２）カード会社（アクワイアラー）

・契約等を有する加盟店の 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をして必要な情報を提供する。

・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」について、機器メーカーや加盟店等への周知を行う。

（３）カード会社（イシュアー）

・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、改正割賦販売法の施行までに可能な限り 100%に近づけられるよう、IC カードへの切替えを加速させる。

・カード会員の PIN 認知に向けて引き続き啓発活動を行うとともに、PIN を認知していない会員に対しては、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理解活動を進めるとともに、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。さらに、POS システムを導入する際に IC 対応しない加盟店でも、後から簡易に IC 機能を活性化できる仕組みを搭載する。

（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、改正割賦販売法の施行までに決済端末の IC 対応化が図られるよう、カード会社（アクワイアラー）等を通じた加盟店に対する周知・指導を徹底するとともに、加盟店の業種別団体等に対する働きかけを積極的に行う。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。

・行政は、改正割賦販売法の円滑な施行及びセキュリティ対策の強化の観点から、加盟店契約に関するガイドライン（加盟店の IC 未対応による不正使用があった場合の損失負担の在り方に関する内容を含む）を策定・公表する。

・行政及び日本クレジット協会は、IC 対応に向けた事業者の取組状況を見える化するため、IC 対応済の加盟店を公表するとともに、消費者向けの分かりやすい表示方法を検討する。

・行政は、以下の支援措置を講ずるとともに、加盟店での IC 対応化の取組を促進する。

①平成 28 年度第 2 次補正予算による「クレジット取引におけるセキュリティ対策推進事業」において、POS 加盟店での IC 対応を進めるため、業界単位で取組む IC 対応のための共同決済システムの導入・実証を支援する（採択先（業種）：ホテル、食品スーパー）。

②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 対応化を支援する。

（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。）

・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

取引の安全性を周知するとともに、PIN 認知度のさらなる向上のための広報等に引き続き取組む。

６．2017 年度中に重点的に実施すべき具体的な取組について

本実行計画を踏まえて、安全・安心なクレジットカードの利用環境の実現を図ることとする。平成 28 年度経済産業省委託調査（平成 28 年 10 月時点）によれば、加盟店の決済端末の IC 対応完了は全体で 16.7%であり、規模の大きい加盟店ほど対策が遅れている結果が得られている。

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化されることを踏まえ、その施行に向け、決済端末の IC 対応を早急に進めていく必要がある。

2017 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。

なお、2018 年度以降の取組については、2017 年度の進捗状況等を踏まえて検討を行う。

（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、改正割賦販売法の施行までに可能な限り 100%に近づけられるよう、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。

（２）加盟店における 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。

（３）加盟店に対する決済システムの IC 対応に向けた取組

・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。

・なお、ガソリンスタンドにおける IC 対応については、精算場所ごとの取引オペレーションや、給油機一体型の自動精算機等において課題[20]があり、現行サービスを踏まえながらどのようにインターフェース対応をしていくのか、継続的に有識者と検討を進める。

（４）IC カード対応 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等[21]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。

（５）行政の業界団体等への働きかけ等

・行政は、日本クレジット協会と協力して、改正割賦販売法の円滑な施行に向け、加盟店の所属する業界団体等に対して、本実行計画及び本協議会の活動内容を周知するとともに、加盟店における着実な実行に向けた働きかけ等を引き続き行う。

・行政は、2016 年末時点での IC 化率が目標の 80%を達成できなかったことを受け、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、進捗の遅れている者への個別指導を行う等、改正割賦販売法の施行までにカードの IC 化率を 100%に近づけられるよう、着実な推進を図る。

---

20 ガソリンスタンド内で使用する決済端末等情報通信・決済機器にかかる各種法規制（防爆等）対応や、給油機一体型オートローディング式自動精算機の PCI PTS 認定、店員による給油サービス後の車内精算における PIN 入力方式等の課題がある。

21 「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．EC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

1．ECにおける不正使用対策の取組について

2015年のEC市場の取扱高はおよそ13兆8千億円となり、前年比7.6%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機能を担っているが、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使用したECにおけるなりすましによる被害は2015年に約71億円（前年比7.0%増）、2016年1月から9月に約67億円（前年同期比32.0%増）発生し、年間では市場規模の伸びを超える状況が想定される。近時、カード情報流出事案が依然多発しており、不正に使用されるカード情報のストックが増加していること、不正使用の単価や商材が真正利用と類似するよう不正使用自体が巧妙化していることもあり、被害額が増加傾向にある。

このようなクレジットカードの不正使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。

こうした状況を踏まえ、本協議会においてEC加盟店における不正使用被害の状況について調査を行い分析したところ、不正使用被害額全体の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（以下「特定5業種」という）が占めることが判明した。また、不正使用被害額上位の加盟店が特定されるとともに、こうした加盟店の大半では何らかの不正使用対策を講じているものの、大半が被害額の減少までには至っていない現状が明らかになった。

何らかの不正使用対策を導入していても不正使用被害を防ぐことができていない要因としては、①加盟店等からのカード情報漏えいの際に真正利用の照合要素（セキュリティコード等）が同時に窃取されていること、②3Dセキュアのパスワード等の登録率が向上しておらず本人認証の処理が行われないケースがあること、③不正使用被害に関する各当事者間における情報共有が不十分であり、その後の被害発生防止に役立ってないこと（その結果、不正判定精度が不十分であること）などがあげられる。

以上の点を踏まえ、実行計画2016で掲げられた具体的措置の実効性について分析・評価を進め、実効性の高い不正使用対策の普及を図っていく必要がある。そのためには、第一に、加盟店、カード会社、PSP及びその他セキュリティ事業者等の総合的な取組が重要であること、第二に、特定5業種のように、不正使用リスクの高い業種や加盟店においては、一つの方策を導入さえすれば足りるもの

ではなく、他の方策との併用により、より万全な不正使用対策を講じること、つまり多面的・重層的な対策が特に必要である点を認識しておく必要がある。

まず、カード会社（アクワイアラー）及び PSP は、不正使用被害が顕在化している加盟店のうち、「カード番号＋有効期限」のみで決済を行い、何らの不正使用対策も講じていない加盟店に対して、本実行計画で整理した具体的な方策を中心とした不正使用対策の導入を促進することとする。

また、すでに何らかの不正使用対策を講じているが、不正使用被害が顕在化しており、不正使用に対する十分な抑止効果が見られない加盟店に対しては、従来の対策を見直し、必要な追加策を講じる等の対応を求めていくこととする。

また、EC の拡大が今後も続くことを鑑みれば、不正使用対策について不断の見直しを図るとともに、新しい本人認証技術やその他サービスの有効性の実証・導入の推進を継続的に検討していくこととする。

カード会社や加盟店等による不正使用対策に加えて、消費者自身のクレジットカードの不正使用の状況や対策等に関する認知・意識の向上も重要であることから、行政・業界団体等は、消費者に対する情報提供や啓発等を進めていくこととする。

以上の取組を着実に進めるとともに特に不正使用被害額が大きい加盟店及びリスクの高い業種等の加盟店に対して重点的に実施することにより、2018 年 3 月末までに多面的・重層的な不正使用対策が講じられることを目指す。

２．不正使用対策の具体的な方策について

なりすまし等不正使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が、以下に記載の方策に限られるものでないことも認識していくことが必要である。

また、それぞれの方策に課題等があるため、加盟店の業種及び商材等に応じた有効な方策を講じることが重要であり、それぞれのリスクの状況に応じて、以下の方策を基本としつつ、追加的な対策をとることを含め、多面的・重層的な対策を講じていくことで不正使用防止効果を高めていくことが求められる。

■本人認証

- EC におけるなりすまし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が、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）に事前に登録したパスワード等を利用時に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、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、パスワード等未登録の

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、不正使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等の情報登録なくしては、認証処理ができないため、カード会社（イシュアー）によるパスワード等の登録率向上に向けたカード会員への周知・啓発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等の管理に関する広報活動も重要である。

・カード会社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。

・このような認証方法は国際ブランドも推奨しており、国内においてもすでに採用しているカード会社が存在する。今後、新たに動的パスワードや生体認証を採用するカード会社の増加等により、パスワード漏えいによる不正使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[22]（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、カードのオーソリ電文上にカード会員の属性情報を同時に送信し、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

[22] 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。

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、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)、「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使用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、既存のオーソリ電文の活用で導入できること等の点で評価されている。
・一方、クレジットカードを利用しているのが、カード会員本人か否かまでは確認できないことに、留意が必要である。
・不正使用被害額上位の加盟店の中には、「セキュリティコード」による券面認証を実施しているにもかかわらず、不正使用被害が発生している加盟店があり、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確認されている。
・したがって、券面認証のみによる不正使用対策では万全ではなく、他の方策と併用することにより、効果的に不正使用の防止を図る必要がある。

■属性・行動分析

・EC を行うカード会員のネット接続端末機器について、加盟店が通信時の IP アドレス等のいわゆるデバイス情報や、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）を行い、不正な取引であるか判定する手法である。
・「属性・行動分析」を他の情報・手段と組み合わせて導入した加盟店において、前年より、不正使用被害が減少している例がある。これは、加盟店が独自に把握できる通信情報等を活用し、過去の不正特性を反映させたモデルが功を奏したものとして評価される。
・「属性・行動分析」では、デバイス情報を判断材料として活用でき、またカード会員が提供したメールアドレスや商品送付先情報と、他の属性情報とを組み合わせることでモデル精度の向上を図ることが可能である。
・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使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が、これを提供する PSP やベンダーから、サー

ビスの提供を受けることが考えられる。
・属性・行動分析による不正使用対策では、購入商品やその購入頻度の不自然さ等から、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体制構築も必要となる。

■配送先情報

・不正使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使用被害を防止することが可能である。現在、大手加盟店が独自のデータベースを運用している他、カード会社複数社で共同で運用しているサービスが、限定的ではあるが加盟店に対して提供されている。
・一方、デジタルコンテンツのようなカード会員がダウンロードを行って商品等を購入し、配送を伴わない取引には利用できず、また、過去に不正な取引と判定されていない住所への配送の場合は、不正使用被害を回避できないこともある。
・賃貸物件の空屋を配送先に指定する場合には、不正行為のおそれがあることが考えられるが、空屋に入居者が現れる可能性があり、その場合には不正を確定する情報にはならないが、他の情報・手段との併用により、この情報を活用することは可能である。
・過去になりすまし不正使用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、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」等の他の方策と組み合わせ、不正検知能力を高めることが重要である。
・「配送先情報」による不正使用対策では、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体制構築も必要となる。

■その他

・「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、カード会社（イシュアー）の採用により導入可能な方策であり、国際ブランドの一部には、カード会社（イシュアー）の採用を義務付ける動きもある。
・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、早期の不正使用の確定とカードの無効手配・処理が可能となるため、有効な不正使用対策となる。
・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。

・加盟店に対し多面的・重層的な方策を求めるとともに、カード会社のオーソリゼーションモニタリングによる不正検知精度の向上についても、不断の努力が必要である。

３．各主体の役割について

EC におけるなりすましの不正使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）

・不正使用の被害抑止に資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」の利用会員の登録率の向上を図る。
・「3D セキュア」の利用会員の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、「動的パスワード」や「生体認証」等の導入促進に努める。
・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。
・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、その迅速な判断を行うとともに、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。

（２）カード会社（アクワイアラー）及び PSP

・本実行計画に基づき、2018 年 3 月末までに多面的・重層的な不正使用対策を講じることについて、契約先の加盟店への周知を徹底する。
・特に、不正使用被害額の大きい加盟店に対しては、既存の不正使用対策の実態、不正使用被害発生推移と対策実施前後の状況変化等の調査を基に評価を行い、不正使用対策として更に効果が期待できる適切な方策等について提案を行う。
・加盟店に対し不正使用対策に関する提案を行う場合には、C．2.（不正使用対策の具体的な方策について）で示した方策を基本とするが、既存の不正使用対策の改善点やより効果的な不正使用対策の導入等について、併せて必要

な助言を行う。
・不正使用被害額の大きい加盟店の中で、不正使用対策を何ら講じていない加盟店に対しては、当該加盟店に対して早急に効果的な不正使用対策を導入するよう要請する。
・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、加盟店と共有することに努める。
・併せて、加盟店に対し、不正使用対策の参考となるよう、なりすまし不正使用の傾向や事例等の情報について共有を図る。
・PSP は C．2.（不正使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」等の各方策を提供できる体制を構築し、契約先の加盟店に対して導入の推進に努める。
・取引が不正か真正かの最終確定を行うのはカード会社（イシュアー）である。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使用防止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使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

・実行計画の着実な実施を図るため、日本の EC 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（オペレーションルール等）及び 2.0 への移行について、情報の提供及び説明を行う。
・EC における不正使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

・自社での不審なカード利用の把握に努めるとともに、不正使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使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。
・自社の不正使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。
・自社の不正使用被害のリスクを低減するために、不正使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

正使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多面的・重層的な不正使用対策を講じる。

・特に、不正使用被害が顕在化しているにもかかわらず、「カード番号＋有効期限」のみで決済を行い、何ら不正使用対策を講じていない加盟店は、契約先のカード会社（アクワイアラー）や PSP の関係事業者の協力を得ながら、早急に C．2.（不正使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多面的・重層的な不正使用対策の導入を図る。

（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、改正割賦販売法の施行までに必要な措置が導入されるよう、カード会社（アクワイアラー）等を通じた加盟店に対する周知・指導を徹底するとともに、加盟店の業種別団体等に対する働きかけを積極的に行う。

・不正使用の実態を踏まえ、加盟店において本実行計画に掲げる多面的・重層的な不正使用対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啓発活動に取組む。消費者に対しては、特に ID・パスワードの使い回しへの注意喚起について周知活動を行う。

・日本クレジット協会は、カード会社と連携の上、「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、業界団体等は、不正使用による被害の実態や最新の犯罪手口、不正使用対策に対する取組の成功事例等について、外部機関とも連携して情報収集を行い、関係事業者に対して逐次情報発信を行う。

・行政は、改正割賦販売法の円滑な施行及びカード取引におけるセキュリティ強化の観点から、加盟店契約に関するガイドライン（非対面加盟店において必要な不正使用防止措置が講じられていない場合の不正使用被害に係る損失負担の在り方に関する内容を含む）を策定・公表する。

４．2017 年度中に重点的に実施すべき具体的な取組について

本実行計画を踏まえて、安全・安心なクレジットカードの利用環境の実現を図ることとする。平成 28 年度経済産業省委託調査（平成 28 年 10 月時点）によれば、EC 加盟店におけるなりすまし防止対策は 29.1%が未実施であり、企業規模が小さくなるほど未実施率が高まるといった状況にある。

他方、何らかのなりすまし防止対策を導入している加盟店においても、不正使用を完全に防止するには諸課題が残っていることが明らかになっている。このため、2017 年度は、不正使用被害が大きく減少又は増加している加盟店を対象に重

点的な調査を行い、被害の増減の要因を分析、評価し、その成果を関係事業者間で共有することにより不正使用対策の推進に反映させていくこととする。

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化されることを踏まえ、本実行計画に基づき、多面的・重層的な不正使用対策の導入及び強化に向けた取組を早急に進めていく必要がある。

こうした観点から、2017 年度では、以下の通り、各主体における取組を加速化させていくこととする。

（１）カード会社による不正使用対策強化への取組

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加え、以下の取組を行い、加盟店側の不正使用対策を強化する

・「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。登録率向上の施策実行にあたっては、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 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。
・配送先情報の利用拡大、情報共有について検討を行うこととする。
・不正使用被害額が大きい加盟店及び特定 5 業種の加盟店に対し、以下の（２）で示した活動を行う。

（２）加盟店による不正使用被害減少への取組

・日本クレジット協会は、不正使用が集中する特定 5 業種における不正使用被害の減少に向け、カード会社（アクワイアラー）及び PSP と連携の上、当該業種における不正使用被害及び対策の状況について分析・評価を行い、行政とも連携の上、特定 5 業種の関連団体・加盟店への情報発信を強化する。
・カード会社（アクワイアラー）及び PSP は、加盟店における以下の取組をサポートすることを通じて、不正使用被害の減少に取組むこととする。

①不正使用対策を講じていない加盟店の不正使用対策に係る方策の導入に向けた取組

・不正使用被害額が大きい加盟店のうち、「カード番号＋有効期限」のみで決済を行い、不正使用対策を何ら講じていない加盟店は、契約先のカード会社（アクワイアラー）や PSP からの必要な助言・協力を得て、その取り扱う商材、サービスや業種、規模等に応じた有効な方策を検討し、早急に導入を図る。
・特定 5 業種の加盟店のうち、不正使用被害額は小さいが何らの不正使用対策も講じてない加盟店は、契約先のカード会社（アクワイアラー）や PSP から

の必要な助言・協力を得て、早急に導入策を図る。

②何らかの不正使用対策を行っているが、不正使用被害額が大きい加盟店における不正使用対策の改善・強化に向けた取組

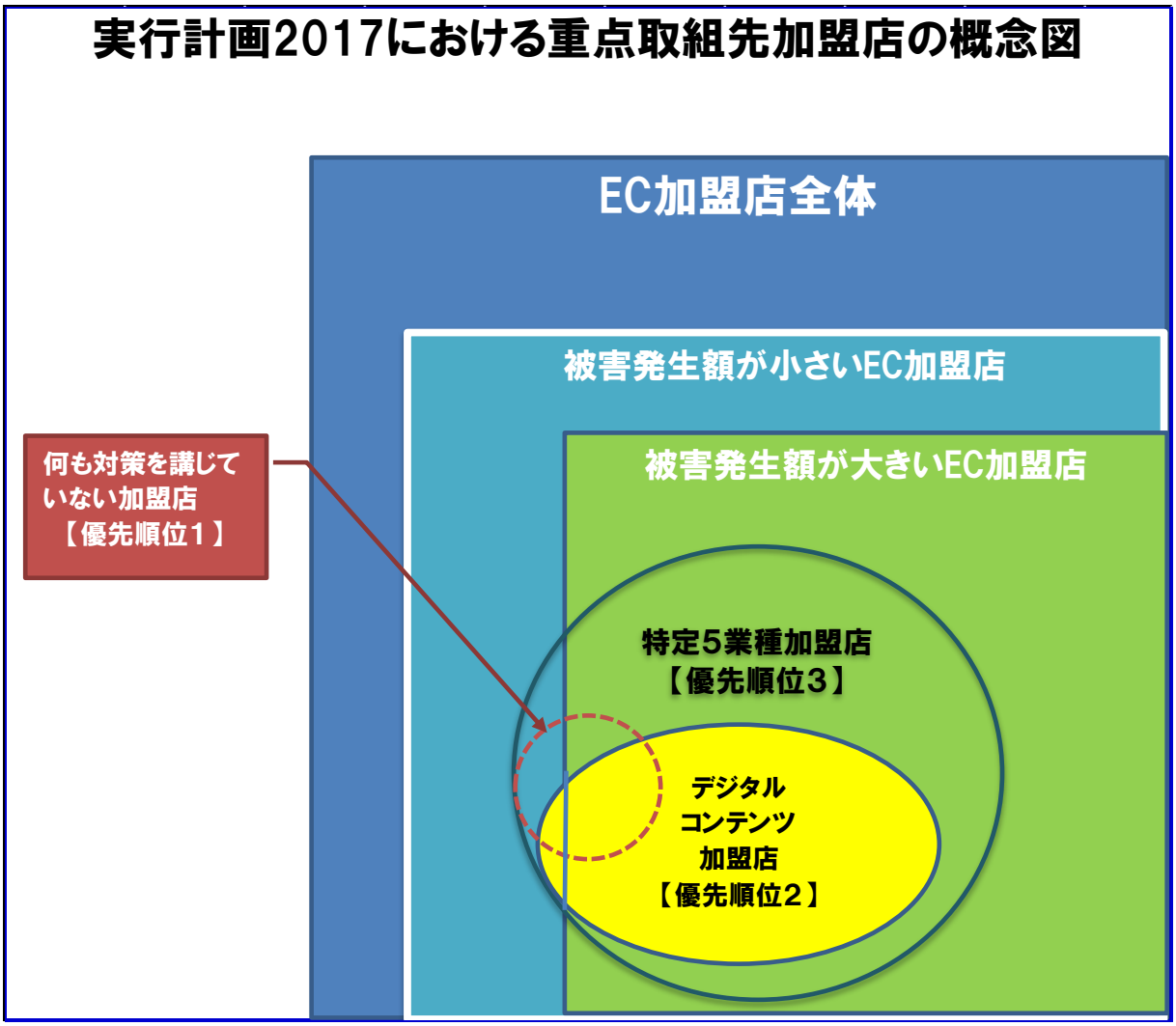
・何らかの不正使用対策を講じているものの、不正使用被害額が大きい（減少していない）加盟店は、契約先のカード会社（アクワイアラー）や PSP からの必要な助言・協力を得て、その対策の有効性や不正使用被害の手口等の検証を行い、③の成果も活用しつつ、既存の方策の改善やより強力な方策の導入等の取組を早急に進めるよう改善策を図る。

・特に、不正使用被害の大きい特定 5 業種のうち、もっとも被害額の多いデジタルコンテンツを取り扱う加盟店は､契約先のカード会社(アクワイアラー)や PSP からの必要な助言・協力を得て、③の成果も活用しつつ、被害額の減少に向けた有効な対策を検討の上、早急に導入を図る。

③不正使用対策が効果を上げている事例の分析・評価及びその成果の共有

・不正使用被害額が大きい加盟店のうち、対策導入後に被害額が減少傾向にあるものは好事例として他の加盟店の不正使用対策にも応用できる可能性があることから、加盟店は、契約先のカード会社（アクワイアラー）や PSP が実施する被害額減少要因の分析・評価に協力することに努める。また、カード会社（アクアイアラー）及び PSP は、その成果について関係事業者間での共有・普及を図る。

・また、何らかの不正使用対策を講じている特定 5 業種の加盟店のうち、不正使用被害額が小さい加盟店についても、導入されている方策が奏功している好事例として他の加盟店にも応用できる可能性があることから、加盟店は、契約先のカード会社（アクアイアラー）や PSP が実施する方策効果の分析・評価に協力することに努める。また、カード会社（アクアイアラー）及び PSP は、その成果について関係事業者間での共有・普及を図る。



（３）行政による業界団体への働きかけ等

・行政は、日本クレジット協会と協力して、加盟店の所属する業界団体等に対して、改正割賦販売法の円滑な施行に向け、本実行計画及び本協議会の活動内容を周知するとともに、加盟店における着実な実行に向けた働きかけ等を引き続き行う。

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

クレジットカードの取扱高は年々増加し、また、日本クレジット協会の調査結果によれば、2016 年 3 月末時点のクレジットカード発行枚数は 2 億 6,600 万枚で、成人人口比では、1 人当たり 2.5 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。

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。

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。」と建議されており、これを受けて 2015 年 2 月には、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ているところである。

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有効であることから、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。

また、加盟店等においては、最新の攻撃手口やセキュリティ技術等の情報を収集することが不可欠であるが、個社単位でこれら情報を収集・分析等するには限界があることから、日本クレジット協会及び行政は、セキュリティ関係機関や国際ブランドとの連携により効果的な情報発信に取組むものとする。

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

2016 年には、日本クレジット協会において、同協会ホームページにセキュリティ対策関連情報を掲載した「安全・安心なクレジットカード取引への取組み」を開設し、また、IC カード取引及びなりすましによる不正使用防止対策についての啓発チラシを作成、全国自治体の消費生活センター及び国民生活センター、日本消費生活アドバイザー、コンサルタント協会などの消費者行政機関約 860 箇所への配布を実施するなどの情報発信を行っている。

その他、行政及び日本クレジット協会において新聞広告、テレビや雑誌のセキュリティ特集への取材協力等も行っている。

2017 年は、各主体において、以下の内容により、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。

①加盟店におけるセキュリティの取組に関する啓発と進捗状況の可視化

カード会員がカード情報の適切な管理や不正使用防止措置が講じられている安全・安心な加盟店を選択できる環境を整備する観点から、加盟店におけるセキュリティ対策の取組を分かりやすく識別できるよう可視化する方策を講じることとする。

そのため、行政及び日本クレジット協会は、セキュリティ対策に関する意識やリテラシー向上のための消費者啓発を行うとともに、加盟店が非保持化又は PCI DSS 準拠、決済端末の IC 対応等の取組が完了している場合に、当該加盟店が安全・安心な加盟店であることや進捗状況を見える化する方策を検討する。

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使用を防止するためには､カード会員が PIN（暗証番号）入力による本人確認の重要性（サインよりも安全であること）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 の認知率は約 7 割、さらに「何となく覚えている」も合わせると認知率は 9 割近いことが明らかになっているが、今後 IC 取引がますます進むと見込まれる中、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。

特に､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るべきである。

③ID・パスワードの使い回しの防止

EC における不正使用対策のうち本人認証サービスは有効な方策であるが、カード会員が他のサービスで使用している ID･パスワードを使い回している場合は、一旦漏えいすれば、本人認証サービスも突破される可能性が高くなるため､このような使い回しの防止等 ID･パスワードの管理の徹底についてカード会社（イシュアー）及び業界団体等は広報等に引き続き取組むこととする。

④EC における不正使用対策の認知度向上

EC における不正使用対策の導入が拡大することは、カード会員の利便性に影響を及ぼす場合もあるが、これら取引の健全な発展の観点から、不正使用対策の必要性やその具体的な方策に関するカード会員の理解・協力を得ることが重要である。特に、本人認証サービスを充実させるためには、カード会員自ら登録することが必要である。

そのため、カード会社（イシュアー）及び業界団体等は本実行計画に記載した不正使用対策の具体的な方策等に関する広報等に引き続き取組むこととする。

⑤利用明細のチェックに関する啓発

不正使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、不正使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、積極的な消費者啓発を行うこととする。

（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とから、行政・業界団体等においては、本実行計画の内容を広く周知するとともに、他のセキュリティ関係機関や国際ブランドからのセキュリティに関する情報や各社のベストプラクティス等の収集・発信等を行うものとする。

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 2016 年中の活動状況等を踏まえ、2017 年版として改定した。本協議会の参加各社等は実行計画 2017 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 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使用の被害の実態、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に設置したセキュリティ対策専門部署を中心に、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不正使用被害の実態、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消費者に向けた広報活動、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（日本クレジット協会）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『改訂版「日本におけるクレジットカード情報管理強化に向けた実行計画」』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およ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.	ｳｨﾙｽ対策ｿﾌﾄｳｪｱまたはﾌﾟﾛｸﾞﾗﾑを使用し、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.	ｺﾝﾋﾟｭｰﾀにｱｸｾｽできる各ﾕｰｻﾞｰに一意の ID を割り当てる
		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およびﾃｽﾄ	10.	ﾈｯﾄﾜｰｸﾘｿｰｽおよびｶｰﾄﾞ会員ﾃﾞｰﾀへのすべてのｱｸｾｽを追跡および監視する
		11.	ｾｷｭﾘﾃｨｼｽﾃﾑおよ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ﾎﾟﾘｼｰを整備する。

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 または通信販売の加盟店でｶｰﾄﾞ情報をｼｽﾃﾑまた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 型の決済サービスを使用する 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 の加盟店でカード情報をｼｽﾃﾑまた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	決済ﾈｯﾄﾜｰｸまたは 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 ｼｽﾃﾑまたはその他のｲﾝﾀｰﾈｯﾄに接続荒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、カード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 P2PE	33
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

◆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：「非保持化可」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

◆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

◆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５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　２０１６年2月２１日
　議題：実行計画２０１７について（継続審議）