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－

２０１６年２月２３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、クレジットカードの取引高は堅調に拡大を続けており、2014 年（平成 26 年）には取扱高 46 兆円を超えるに至っている。特に、近年は急成長する電子商取引（以下「EC」という）における主要な決済手段としても大きな役割を果たしており、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」において、2020 年（平成 32 年）のオリンピック・パラリンピック東京大会の開催等を踏まえ、訪日外国人の需要の取込を含めて、商取引の活性化に資するキャッシュレス化の推進を重要な政策課題として位置づけているが、クレジットカードを消費者が安全・安心に利用できる環境の整備は、クレジットカードの利用拡大の大前提であることは自明である。また、2014 年（平成 26 年）5 月には政府の情報セキュリティ政策会議が策定した「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」における国の重要インフラとしてクレジット分野が指定されたところである。

クレジットカードの取引においては、加盟店やクレジットカード会社を始め様々な事業者が介在しており、そのシステム全体のセキュリティを強化するためには、それら全ての事業者が連携を図って戦略的な取組を進めることが必要不可欠である。

そのため、本協議会は、2020 年（平成 32 年）のオリンピック・パラリンピック東京大会の開催等に向け、国際水準のセキュリティ環境を整備することを目指し、最新の技術等を活用しつつセキュリティ対策を強化していくため、経済産業省の協力を得て、クレジットカード会社、加盟店、ペイメント・サービス・プロバイダー（以下「PSP[1]」という）、決済端末機器メーカー、情報処理センター、セキュリティ専業者、国際ブランド等のクレジットカード取引に関係する幅広い事業者等の参加をもって発足したものである。

2015 年（平成 27 年）3 月から、我が国におけるクレジットカードの不正使用による被害の実態と世界のセキュリティ環境の進展の状況を踏まえて、クレジットカード情報（以下「カード情報[2]」という）の適切な保護のあり方、対面取引における IC 対応の推進方策並びに EC における不正使用防止の方策等について検討を進めてきた。

本実行計画は、これまでの検討結果に基づき、我が国が 2020 年（平成 32 年）までに達成すべき目標の実現に向け、クレジットカード取引に関係する各主体がそれぞれ役割に応じて取り組むべき事項を取りまとめたものである。クレジットカード取引に関係する全ての主体が本実行計画を尊重し、主体者として行動を起こし目標を達成することを期待する。

2016 年 2 月 23 日

---

[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

[2] カード情報とは、カード会員データ（カード番号、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、PIN 又は PIN ブロック）をいう

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（平成15年）以降漸減傾向にあったが、ECの増加に伴い2013年（平成25年）から再び増加傾向に転じており、（一社）日本クレジット協会の集計によれば2014年（平成26年）には約114億円の被害が確認されている。特に、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割近くを占めている。

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り組むべき責務があることを認識しなければならない。

クレジットカードの不正使用を行う者は、国境を越えてセキュリティの脆弱なところを狙ってくると考えられるが、世界各国においてセキュリティ対策が急速に進められる中で、各主体は、日本の対策が後れを取ることとなれば世界の中で日本がクレジットカード不正使用の温床になりかねないという危機感を持って、相互連携を図りつつ、具体的な取組を進めることが求められる。

不正使用の発生状況であるが、まず、不正使用が発生する原因となるカード情報の漏えいについては、カード情報を保持する全ての事業者に発生する可能性があるが、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の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。

さらに、不正使用は、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が、対面取引においては偽造クレジットカードによる不正使用、ECにおいてはカード会員本人になりすました不正使用が発生しており、これら不正使用の手口に応じた適切な対策をとることが重要である。

なお、海外では、特に不正使用の最大の被害国である米国が、偽造カード使用防止のため急速にIC対応を進めていることや、ECにおける不正使用防止のため、3Dセキュア等の対策の導入が世界的に浸透している。

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超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（平成 32 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）加盟店の取引形態及び不正使用の手口に応じた検討

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具体的な方策の検討を行った。

（２）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た多面的・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。

（３）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、契約関係にあるクレジットカード会社や 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。

（４）消費者に対する情報発信

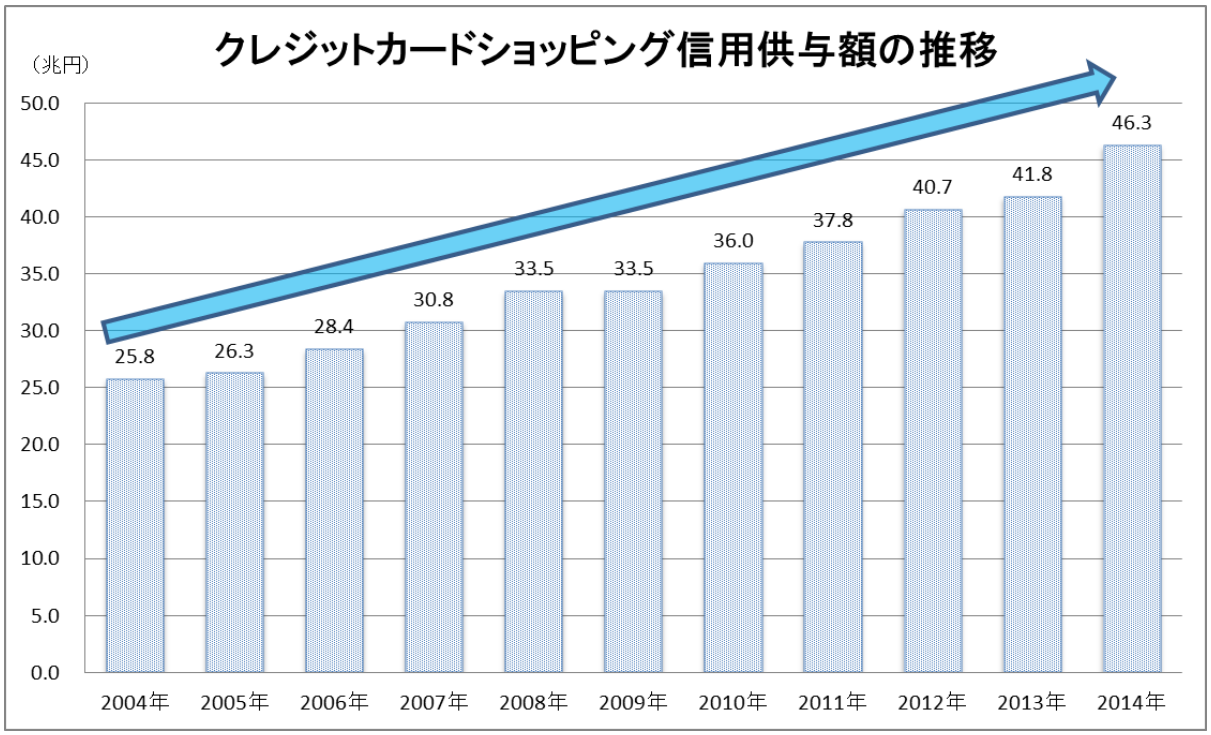
クレジットカード会社や加盟店等の不正使用対策に加えて、消費者自身のクレジットカードの不正使用に対する認知・意識の向上を図るため、より効果的な消費者に対する情報発信等によって理解・協力を得ることも、セキュリティ対策強化の観点から必要な取組である。

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（平成 32 年）3 月末までに不正使用被害額（2014 年（平成 26 年）114 億円）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。

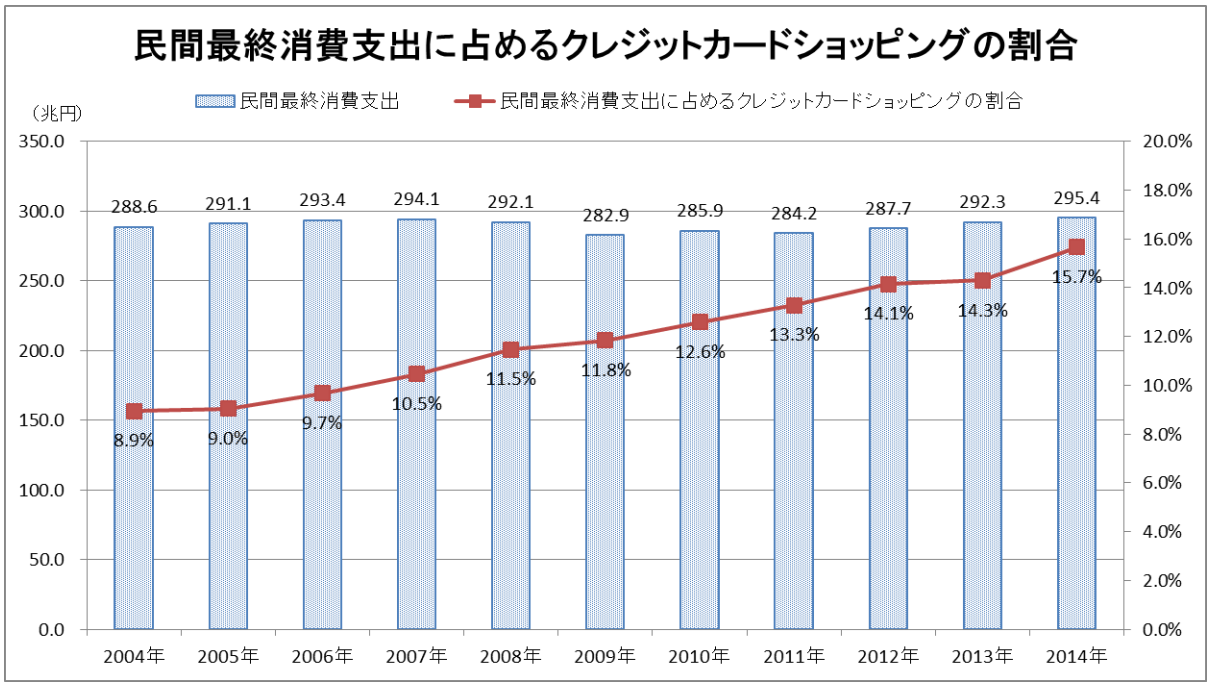
参考資料

（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」

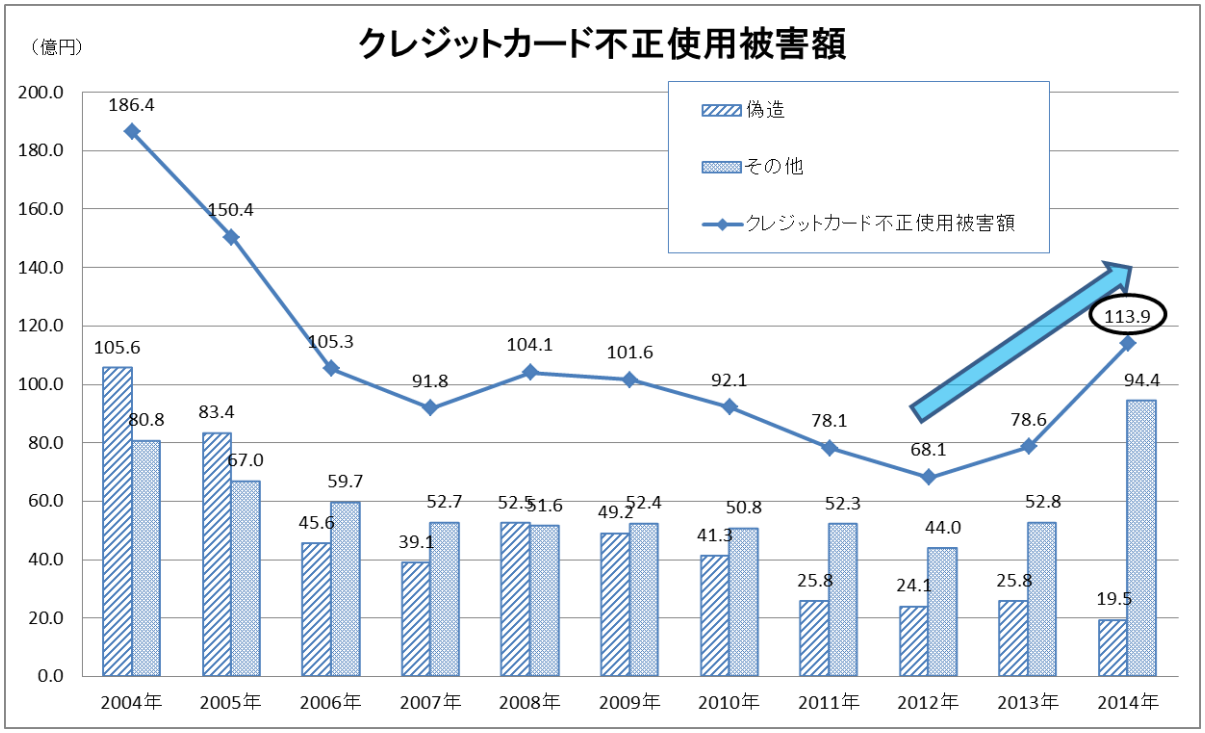
（資料２）



出所：内閣府「国民経済計算年報」民間消費支出：名目

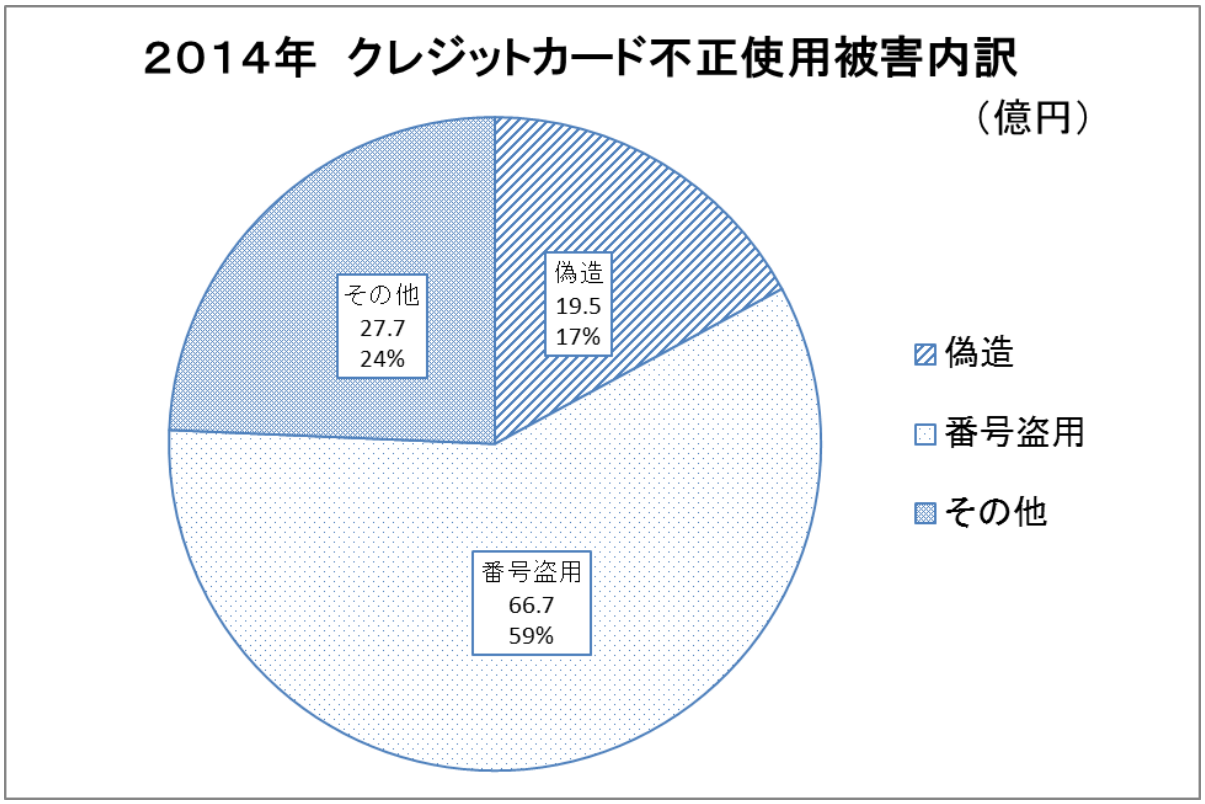
出所：一般社団法人日本クレジット協会「信用供与額」

（資料３）



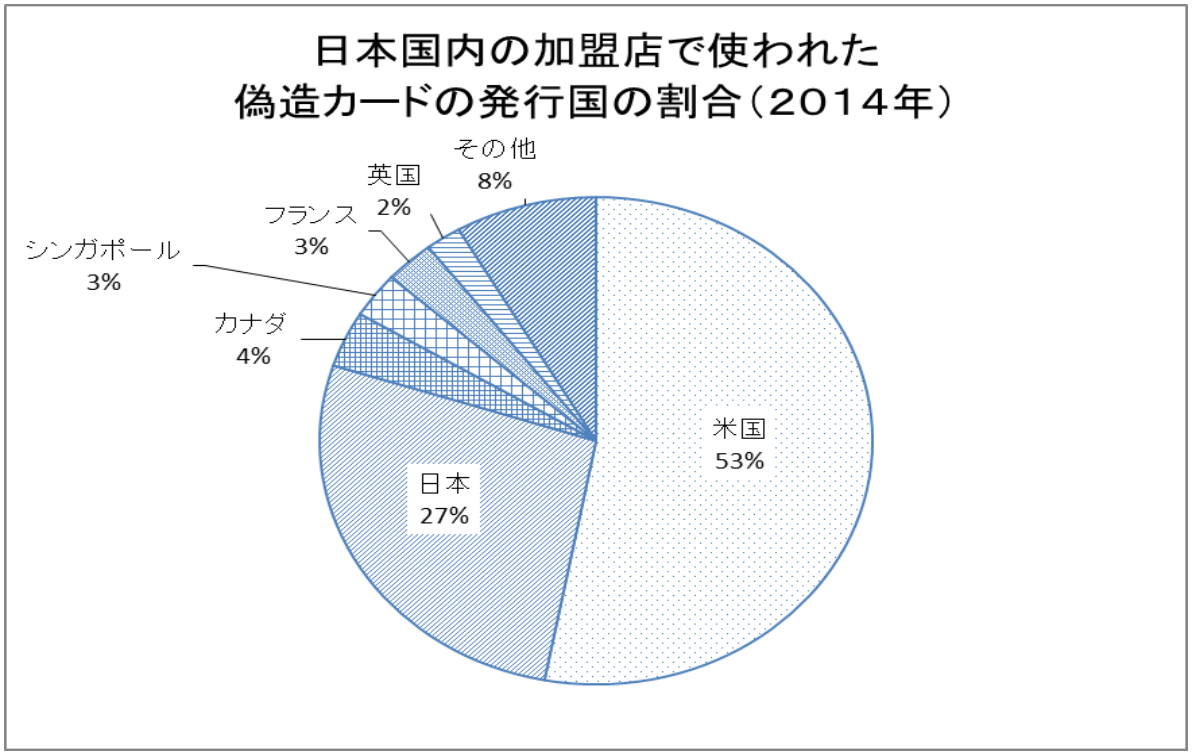
出所：一般社団法人日本クレジット協会「クレジットカード不正使用被害額の発生状況」

（資料４）



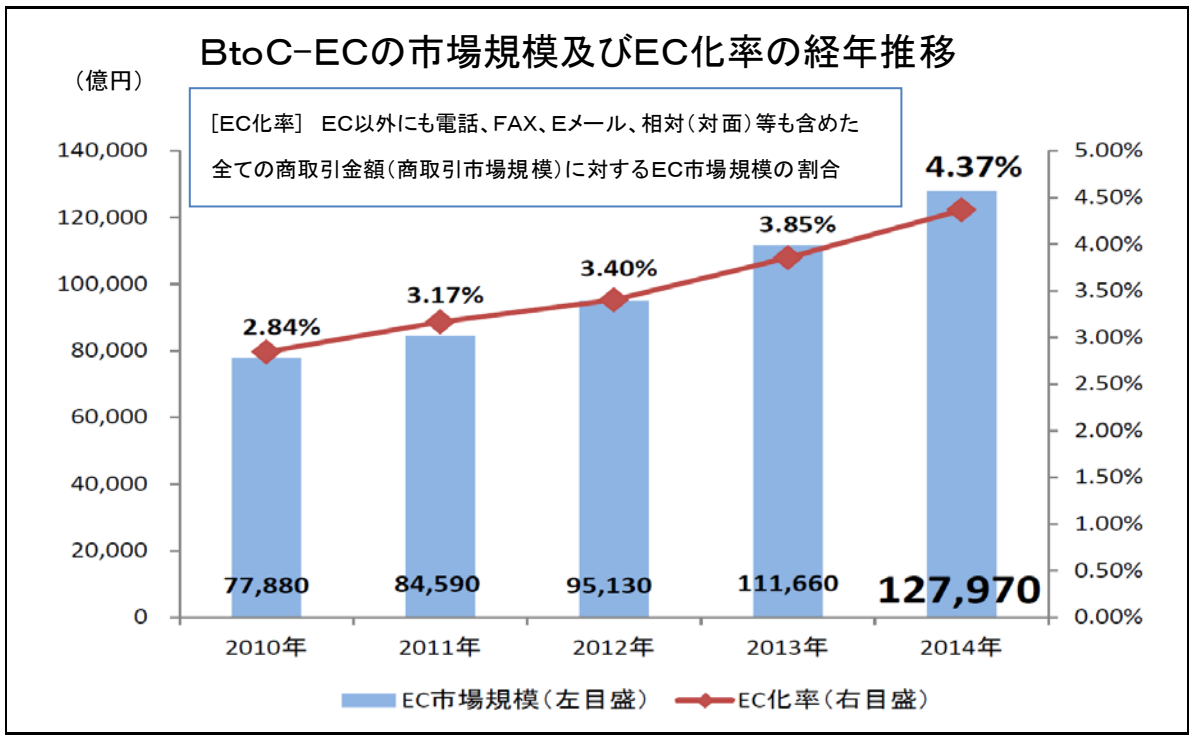
出所：一般社団法人日本クレジット協会「クレジットカード不正使用被害額の発生状況」

（資料５）



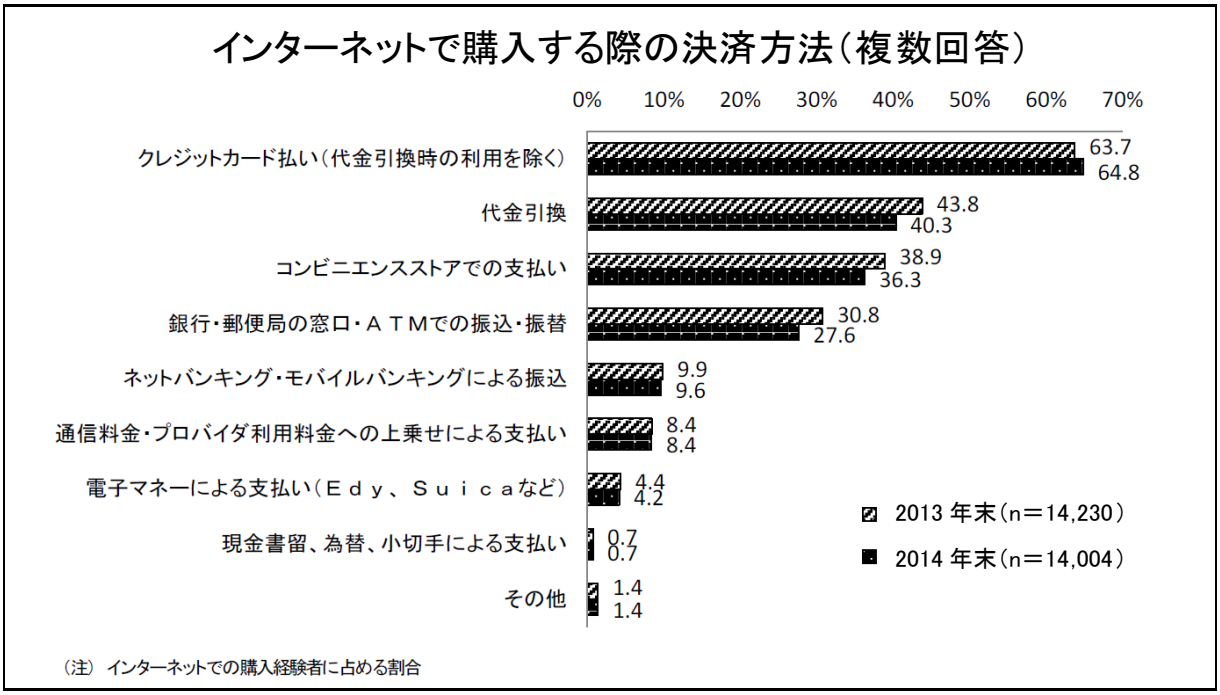
出所：ビザ・ワールドワイド・ジャパン株式会社資料

（資料６）



出所：経済産業省「平成２６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７）



出所：総務省「平成２６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	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。その対策としては、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[3]することを基本とした取組を第一に検討し、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特に情報漏洩リスクの高いEC加盟店におけるセキュリティ対策を進めることが喫緊の課題である。

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Payment Card Industry Data Security Standard（以下「PCIDSS」という）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、PCIDSSへの速やかな準拠[4]が求められるため、事業者がPCIDSS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する。

以上の考え方に基づき、以下の取組を進めることで、2018年（平成30年）3月末までに、特にカード情報の漏えいの頻度が高い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PCIDSS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PCIDSSへの準拠を求める

---

[3] 「非保持」とは、「サーバーにおいてカード情報を『保存』、『処理』、『通過』しないこと」をいう

[4] PCIDSSは、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」とはカード情報を取り扱う業務範囲において、この要求事項にすべて対応できていることをいう。PCIDSS準拠の検証方法としては、カード情報の取扱い形態や規模によって、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PCIDSS準拠の度合いを評価し、報告することのできるツール）による方法がある

こととし、対面加盟店においては 2020 年（平成 32 年）3 月末までにカード情報の適切な保護に関する対応（非保持又は PCIDSS 準拠）を完了することを目指す。

なお、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については非保持化を推進することを基本として、以下の取組を推進する。

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）EC 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サーバーを通過する「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 加盟店のサーバーを「通過」して「処理」されるため、EC 加盟店のシステムにカード情報が「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」されたカード情報や「通過」するカード情報を窃取されるリスクが高い。

一方、非通過型はカード情報が EC 加盟店のサーバーではなく PSP のサーバーを「通過」して「処理」されるため、EC 加盟店はカード情報を「処理」「通過」することはなく、EC 加盟店からのカード情報の漏えいが発生するリスクは低い。

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、PCIDSS 準拠済みの PSP を活用した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。

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 EC 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、PCIDSS 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。

その上で、カード情報を保持する場合は PCIDSS 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は、主に POS システムを導入している加盟店が対象となる。この場合、カード情報を POS システムのサーバーに『通過』させないよう、POS の機能と決済機能を分離すること、分離した決済専用端末からカード情報をサーバーに取り込まないこと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、マルウェア等の感染等により、分離した決済専用端末からカード情報が漏えいする可能性もあることから、非保持化した場合であっても、必要なセキュリティ対策を講ずる必要がある。

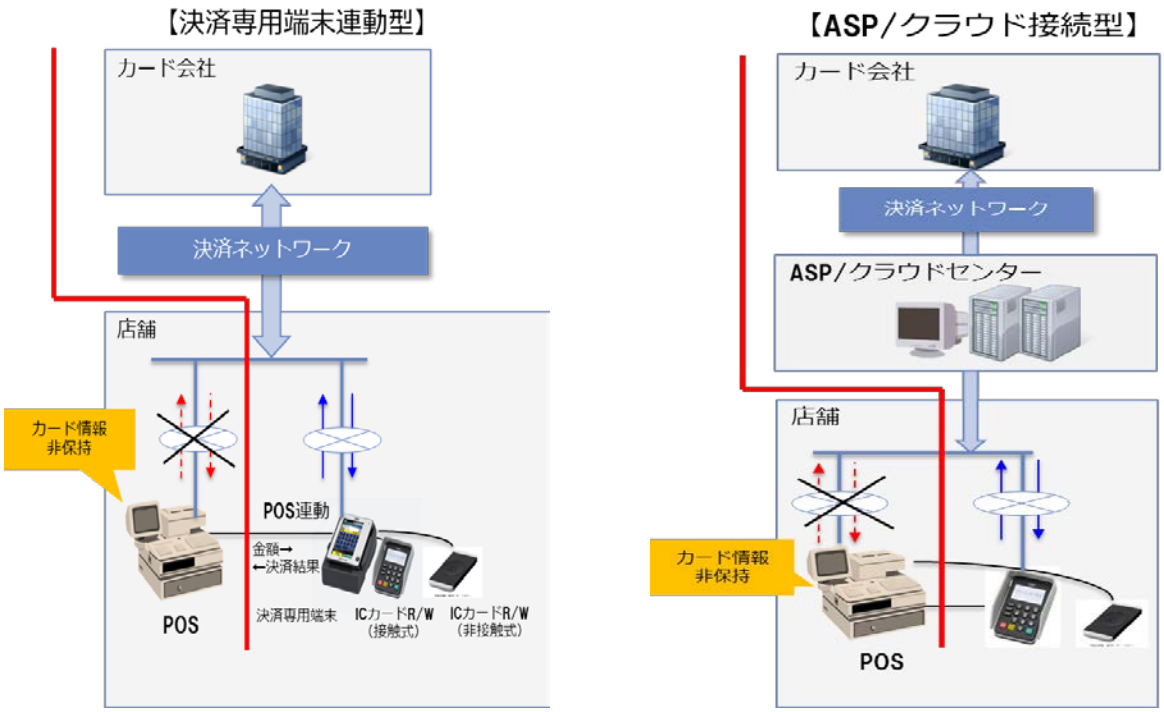
なお、決済機能の分離は、各加盟店の現行システムや店頭オペレーション等の特徴を踏まえ、コスト負担の低減が可能となる方法を検討すべきであることから、後述の POS システムの IC 対応とリンクして検証を行った。

■決済専用端末連動型・ASP／クラウド接続型

「決済専用端末連動型」は IC 対応した決済専用端末（CCT 端末等）と POS システムの間で取引金額や決済結果等を連動させる仕組みであり、「ASP（Application Service Provider）[5]／クラウド接続型」の方式は、POS システムと加盟店の外側の事業者（ASP 事業者）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。

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 POS システムのサーバーを通過せずに行われる。決済結果のうちカード情報を POS システムのサーバーに取り込まないことにより、カード情報の非保持化が実現できるため、PCIDSS 準拠に向けた対応範囲の縮小が期待できる。

[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・仕組み等全般のこと。



（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、既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。

今後、POS システムを導入している加盟店においてカード情報の非保持化を進めるためには、その方法に応じた照会時の課題とその対応策（新たな技術の活用を含む）について検討する必要があるため、引き続き本協議会においてその検討を行う。

３．カード情報を保持する加盟店の PCIDSS 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、PCIDSS への準拠を求める。

しかし、加盟店によっては必ずしも PCIDSS の認知がされていないことや、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（以下「JCDSC」という）の協力を得て、PCIDSS に関する認知度を向上する理解活動の推進と、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）PCIDSS 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 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 PCIDSS 準拠への取組促進のため、PCIDSS に関するセミナーの開催等の周知・啓発活動を行う。

（２）PCIDSS 準拠に向けた加盟店等へのサポート体制について

本協議会は、カード情報を保持する加盟店等が PCIDSS 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、JCDSC の協力を得て以下の対応に取り組むこととする。

① PCIDSS 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 PCIDSS 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。

②PCIDSS に関する理解増進のためのコンテンツの作成・展開

・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。

・PCIDSS に関する FAQ を作成し提供する。

③相談窓口の設置

・PCIDSS 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加盟店向けの PCIDSS 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）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。

４．加盟店以外のカード情報を保持する事業者の PCIDSS 準拠の推進について

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・利用しているが、カード取引に係るインフラの重要な一端を担う重要な役割に鑑み、PCIDSS の準拠は必須である。仮に、このような重要なポジションを占める事業者が PCIDSS 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を求める。

また、カード会社は 2018 年（平成 30 年）4 月を目処に、PCIDSS 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保持する事業者については、PCIDSS 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し、自主的な取組に努めることを求める。

５．カード情報漏えい時の緊急対応について

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おり、同マニュアルの利用範囲を拡大し、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 PCIDSS の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、PCIDSS 準拠等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 で協議の上で対応することとする。

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、カード情報を保持する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している場合は、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 PCIDSS 準拠の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

- EC 加盟店及び EC 以外の非対面加盟店については、2018 年（平成 30 年）3 月末までにカード情報の非保持化又は PCIDSS 準拠完了を目指す。
- 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し、さらに、より安全な非通過

型システムへの移行を進める。

・対面加盟店については、2020 年（平成 32 年）3 月末までにカード情報の非保持化又は PCIDSS 準拠完了を目指す。

・EC 及び対面取引の両方を行う加盟店については、EC に係るシステムについては 2018 年（平成 30 年）3 月末までに、対面取引に係るシステムにおいては 2020 年（平成 32 年）3 月末までに、カード情報の非保持化又は PCIDSS 準拠完了を目指す。

・カード情報を保持する加盟店においては、PCIDSS 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

・カード会社(アクワイアラー)及び PSP は、2018 年（平成 30 年）3 月末までに PCIDSS 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 PCIDSS 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 等への誘導等による早期の準拠が実現できるよう協力する。

また、加盟店の非保持化の完了については、カード会社（アクワイアラー）が確認する。

・カード会社（アクワイアラー）は契約等を有する PSP に対して、包括加盟店契約等を有する EC 加盟店に非保持化（非通過型システムへの移行を含む）させることを要請し、さらに PSP が PCIDSS に準拠していない場合は可及的速やかに準拠するよう必要な指導を行う。なお、カード会社は、2018 年（平成 30 年）4 月を目処に、PCIDSS 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）

・カード会社(イシュアー)は 2018 年（平成 30 年）3 月末までに PCIDSS 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詐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）行政・業界団体等

・行政は、本協議会事務局と協力して、カード情報の適切な保護の必要性やあり方について、事業者向けや消費者向けの情報発信に取り組む。特に、加盟店の業種別団体等に対しては、本実行計画の着実な実行に向けた働きかけ等を積極的に行う。

・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。

・行政は割賦販売法に規定されるカード情報の適切な管理義務について、その対象を PSP や加盟店等にも拡大する方向で見直しを行う。

７．2016 年度（平成 28 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、以下事項について 2016 年度（平成 28 年度）中に特に重点的な取組として進めることで、近年頻発しているカード情報の漏えいを防止し、クレジットカード取引全体の安全・安心の実現を図ることとする。

なお、2017 年度（平成 29 年度）以降の取組については、2016 年度（平成 28 年度）までの進捗状況やカード情報の漏えいの実態、新たな技術の進化等を踏まえて検討を進めることとする。

（１）加盟店におけるカード情報非保持化への移行に向けた取組

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り組む。

（２）「通過型」を採用している EC 加盟店への対応

すでに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に述べたとおり非通過型への移行を推進する。

（３）PCIDSS 準拠に向けた JCDSC のサポート体制の整備とカード会社（アクワイアラー）及び PSP を通じた加盟店等への周知

A．3．に述べたとおり、カード情報を保持する加盟店等が PCIDSS 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、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こと等により、PCIDSS 準拠の早期実現に向けた取り組みを行う。

（４）EC 加盟店と包括加盟店契約を有している PSP の早急な PCIDSS 準拠の完了

EC 加盟店には、非保持化（非通過型システムへの移行を含む）を進めることとするが、今後ますます大量のカード情報が PSP に集約されることとなることから、PCIDSS に準拠していない PSP は早急に準拠完了を目指す。

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等に向けて、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放置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 IC チップそのものが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 7 割弱にとどまっている。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。

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。

本協議会においては、改めて 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の可能性について検討を行った。更に、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について検討を行った。

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。

コスト低減等に資する事項の洗い出し・検討は引き続き行うこととするが、本実行計画を推進することで、決済端末のIC対応について2020年（平成32年）3月末までに完了することを目指す。

２．IC取引時のオペレーションルール・ガイドライン等について

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。今後、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確定させ、我が国のクレジットカード業界としてのルール・ガイドライン等を制定することを目指す。カード会社・加盟店及び機器メーカー等は、当該ルール・ガイドライン等に基づいて対応することとする。

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取引においてオペレーションが異なる場合があることに留意する。

（１）IC取引における本人確認方法

①接触IC取引

接触IC 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）」が我が国の決済システムを考慮すると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、サイン機能の装備を必須とする。
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、本人確認としてPINの取得が売場形態等の事由により困難であり、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、例外として接触IC 取引においてもサインを許容する。
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会員に認められているが、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[6]

非接触 IC は、各国際ブランドルールにより一定金額以下の取引については、本人確認が不要な取引が認められていることを踏まえ、本人確認方法を以下の通りとする。

・CVM リミット金額[7]以下は、本人確認不要とする。
・CVM リミット金額超は、原則サイン、又は 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。
・そのため、日本国内の端末は「サイン機能」「Consumer Device CVM 機能」「No CVM（本人確認不要）機能」の装備が必要となる。

（２）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[8]の実装方式であり、EMV 仕様に準拠しつつ、PIN 対応、サ

---

6 非接触 IC においては、下記のようなケースにおいて非接触 IC から接触 IC への切替・誘導が可能となる点に留意が必要。
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。このため、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。
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。

7 「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。

8 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。

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、CVM リミット金額以下は、本人確認不要取引を実現し、CVM リミット金額超の本人確認方法は原則オフライン PIN の考え方に則り、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、本方式の実現に向けて継続検討を行う。

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

既存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等の考慮も必要である。

具体的な本人確認不要加盟店の対象や除外商品については、今後各国際ブランドと継続協議を行う。

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、今後各国際ブランドと継続協議を行う。

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。

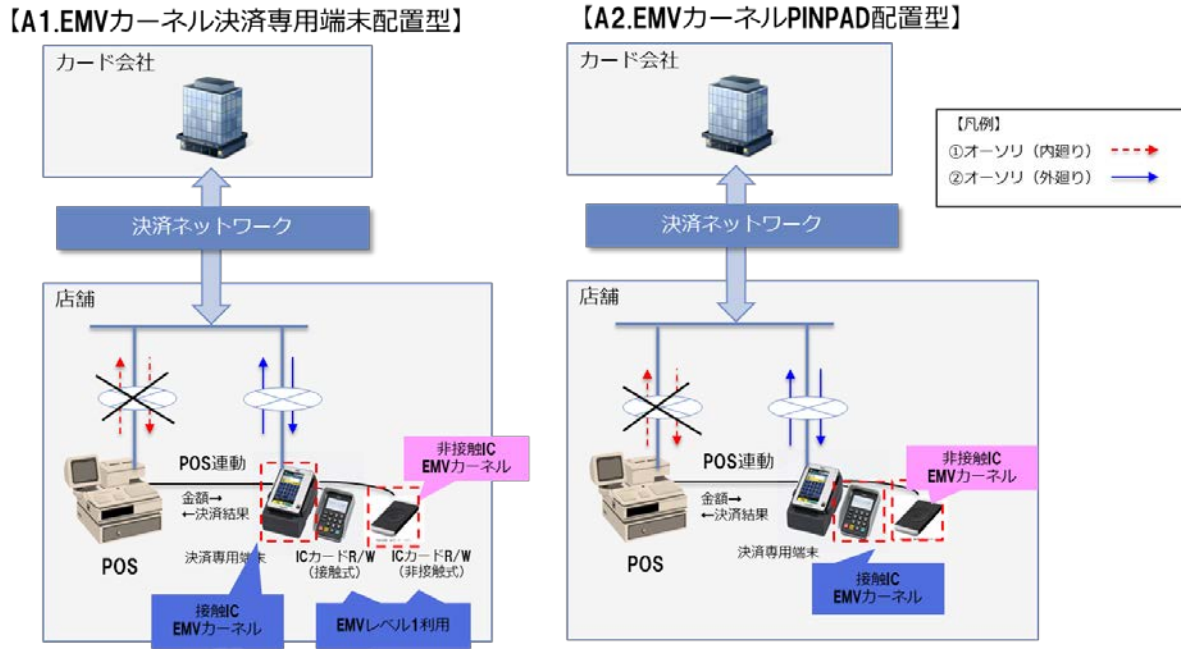
（１）各方策の検証について

IC 対応の方法は、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図れる方法を検討するため、決済専用端末（CCT 端末等）連動型、決済サーバー接続型、ASP／クラウド接続型に大別し、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を行った。

■決済専用端末連動型

IC 対応した決済専用端末（CCT 端末等）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 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。

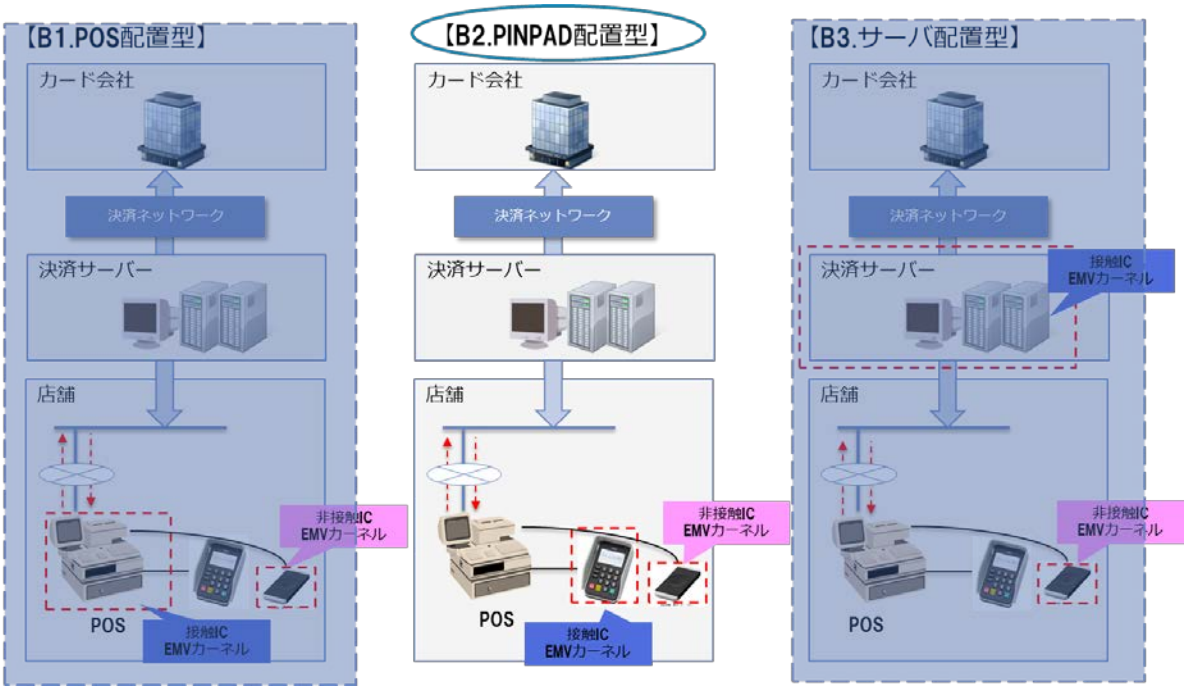
一方で、決済専用端末を新たに追加する必要があるため、設置場所の確保等の課題もある。



■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、導入時における対応の影響は小さい。

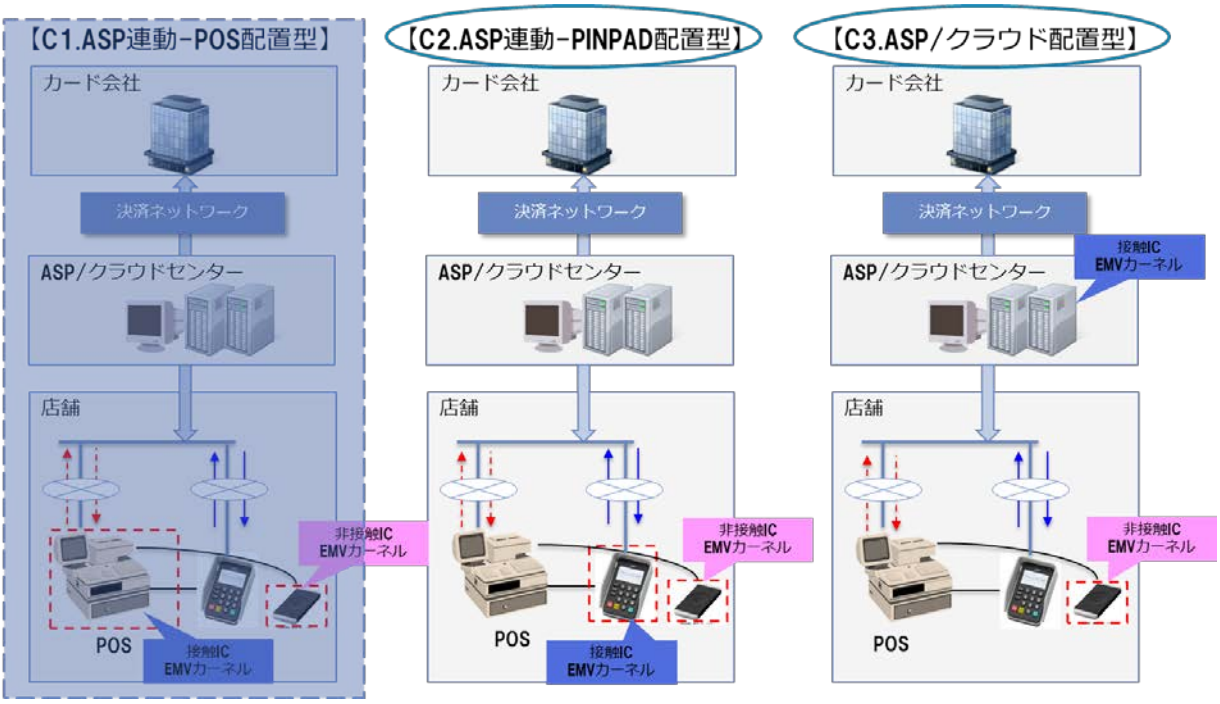
ただし、カード情報が POS システムのサーバーを通過することから、PCIDSS に準拠[9]する必要がある。



9 POS システムの PCIDSS 準拠のために、PA-DSS（ソフトウェアベンダー向けのセキュリティ基準であり、POS 等の決済アプリケーションが守るべきセキュリティ基準。）準拠製品の使用が望ましい。PA-DSS 準拠製品の使用は PCIDSS 準拠の要件ではないが、PA-DSS 準拠製品を使用することで、PCIDSS 準拠をスムーズに進めることができる。

■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 事業者）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、クラウド配置型については社外（ASP 事業者）で開発・EMV 認定・ブランドテスト等の対応を行うため、加盟店の個別負担は少ない（ASP 利用料は発生)。



（２）接続インターフェイス等の共通化・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 のインターフェイ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。

今後、各方法の接続インターフェイス等の共通化・標準化の検討を踏まえ、国際標準仕様を策定している OPOS 技術協議会等と連携し、普及を促進する。

（３）POS システムの IC 対応標準化

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、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、国際ブランドと引き続き調整を行う。

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-CCT 端末の普及に努める。

また、CCT 端末の IC 対応は、現状約 7 割と順調に進捗してきているが、磁気取引しか実行できない 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各主体は必要な支援の検討を行う。

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

・2020 年（平成 32 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 対応の完了を目指す。

・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)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イス等の共通化や 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をしてガイドライン等の策定を行う。

（３）カード会社（イシュアー）

・（一社）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%の実現に向けて取り組む。

・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のルールを制定することに協力する。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。
・加盟店の負担となるブランドテストのコスト低減化を図るため、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、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、カード会社（アクワイアラー）と引き続き検討を行う。

（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法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の必要な情報を提供する。
・POS システムの接続インターフェイス等の共通化等によって、コスト低減化に資する技術的解決策の実現に向けて取り組む。
・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、カード取引の IC 対応の必要性等について事業者向け及び消費者向けの情報発信に取り組む。特に、加盟店の業種別団体等には本実行計画の着実な実行に向けた働きかけ等を積極的に行う。
・行政は、本実行計画の進捗状況を踏まえて、（一社）日本クレジット協会と連携しつつ、加盟店の IC 未対応による不正使用の損害賠償責任に関するルールの明確化や、IC 対応に向けた事業者の取組状況の可視化等の検討を行うとともに、必要に応じて法制化を含む制度的対応に関する検討を行う。
・行政は、投資負担に限界がある中小加盟店等の円滑な IC 対応を進めるため、必要な支援の検討を行う。
・業界団体等は、消費者の PIN 認知度のさらなる向上のための広報等に引き続き取り組む。

６．2016 年度（平成 28 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、以下事項について 2016 年度（平成 28 年度）中に特に重点的な取組として進めることとする。なお、IC 対応には各事業者等に大きな投資コストが発生し得ることに留意し、引き続き、本協議会において実行計画の進捗等について緊密な意見交換を行うこととする。

なお、2017 年度（平成 29 年度）以降の取組については、2016 年度（平成 28 年度）の進捗状況等を踏まえて検討を行う。

（１）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 対応に向けた検討を進める。

（２）加盟店に対する決済システムの IC 対応に向けた取組

・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、協議会事務局の協力を得ながら、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 対応 POS ガイドラインの整備

・ B．2．に述べた IC 取引オペレーションルール及び B．3．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が策定している IC－POS ガイドラインの改訂及び（一社）日本クレジット協会においてその他ルール等を整備することにより、加盟店の POS システムの IC 対応に向けた取り組みを加速する。

（４）行政の業界団体等への働きかけ等

・行政は、協議会事務局と協力して、加盟店の所属する業界団体等に対して、本実行計画の周知と着実な実行に向けた働きかけ等を行う。

・行政は、本実行計画の進捗状況を踏まえて、(一社）日本クレジット協会と連携しつつ、加盟店の IC 未対応による不正使用の損害賠償責任に関するルールの明確化や、IC 対応に向けた事業者の取組状況の可視化等の検討を行うとともに、必要に応じて法制化を含む制度的対応に関する検討を行う。

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

2014 年（平成 26 年）の EC 市場の取扱高は 12 兆円を超える規模となっており、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、一方で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が多く発生している。また、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が拡大している。

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。

不正使用対策を講ずるにあたっては、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になる。また、なりすまし等の不正使用対策としては、一つの手法・対策を導入さえすれば足りるものではなく、不正使用対策に万全を期す観点から多面的・重層的な対策が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、不正使用対策が脆弱な EC 加盟店のうち、不正使用の対象となるリスクが高い「カード番号＋有効期限」のみで決済を行い、本人認証技術等の不正使用対策を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、EC の拡大が今後も続くことに鑑みれば、不正使用の増加・手口の巧妙化等の懸念もあることから、現行の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。

さらに、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、より効果的な消費者に対する情報提供や啓発等も進めることとする。

以上の取組を、不正使用被害額が大きい業種及びリスクの高い業種等の加盟店において集中的に実施することにより、2018 年（平成 30 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に対する具体的な方策について、以下のとおり整理する。

なお、それぞれの方策には有効性・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的な方策を講じる。

■本人認証

・本人認証の手法として、EC におけるなりすまし防止のための既存の本人認証サービスとしては、3D セキュアや認証アシストがあるが、消費者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が確認できる。

・他方、3D セキュアについては、消費者がパスワード等を失念した場合の購入機会の逸失の懸念、パスワード使い回しのリスク、消費者の登録の低調、等の課題がある。そのため、3D セキュアの実効性をより向上させるため、消費者に対する登録に向けた啓発活動の実施、パスワードの使い回しによる不正使用リスクを回避するための方策の実施等のカード会社等の取組を重点的に行う。

・既存の 3D セキュアと連動するリスクベース認証機能や、国際機関（EMVCo）で検討中の 3D セキュア 2.0 へのバージョンアップは、取引内容等の高リスク取引のみ本人認証を行う等の制御が可能になるため、販売機会の逸失等の懸念が相当程度緩和されることが期待されることから、サービス内容やサービス開始時期等について関係事業者や国際ブランドからの情報収集に努めるとともに、できる限り早期に導入できるように検討を進める。

■券面認証

・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、消費者が認証で使用する番号を失念する懸念がないこと、導入コストが低廉であるため加盟店が導入しやすい、等の評価がされている。

・一方、クレジットカードを所持しているのが、真正なカードホルダーかどうかまでは確認できないことに留意が必要である。

■属性・行動分析

・EC を行う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サービスである。そのため、本サービスの活用により、不正取引と判定された場合、取引を中断することができる等のメリットがある。

・一方、過去の取引情報が無い場合は、不正取引との判定が難しく、不正被害を回避できないこともある。

・また、最終的に不正かどうかを判断するのは加盟店自身となるため、加盟店

自身の不正判定業務ノウハウの蓄積や体制構築が必要となる。

■配送先情報

・犯罪組織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おり、安価なコストで導入することができる。

・一方、デジタルコンテンツのような消費者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､不正被害を回避できないこともある。

■その他

・今後、カード利用時におけるＥメール等による消費者への利用通知や、イシュアーによる不正検知精度の向上等、不正防止のための新たなシステムやサービスが明らかになった場合は、有効性と課題等を確認した上で、具体的な方策に取り入れていく。

３．各主体の役割について

EC におけるなりすまし等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広報に努める。

・加盟店における 3D セキュアの導入の加速と不正使用抑制の効果を高める観点から、3D セキュアの利用会員の登録率の向上に努める。

・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、加盟店における 3D セキュアの導入の加速と不正使用抑制の効果を高める観点から、早期の導入を図る。

・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・検知力向上に努める。

（２）カード会社（アクワイアラー）及び PSP

・契約を有する EC 加盟店に対して、本実行計画の内容について周知を行い、これを踏まえた対応を行うよう働きかけを行う。

・不正使用被害額の大きい加盟店に対して、現在どのような不正使用対策を講

じているのか、さらに効果的な不正使用対策としてどのような対策を導入することが適切か等についてヒアリング等を行った上で、加盟店と協働して、C．2．で示した方策を基本として、既存の対策の改善や、より効果的な対策の導入等の取組に向けた必要な措置を講ずる。

・特に、不正使用対策を何ら講じていない加盟店に対しては、当該加盟店と協働して早急に効果的な不正使用対策に取り組むよう必要な措置を講ずる。

・3Dセキュアの仕様やその運用に関する情報を加盟店と共有することに努める。

（３）加盟店

・自社での不正使用被害状況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、具体的な不正使用の手口等最新の情報を入手して対策の強化に反映するよう体制の整備を図ることとする。

・不正使用による被害のリスクを低減するために、対策の強化を図る観点からカード会社（アクワイアラー）及び PSP とも協力して、C．2．で示した方策を基本とした多面的・重層的な対策を講じる。特に、「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について、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、早急に具体的な方策を基本とした不正使用対策の導入を図る。

（４）行政・業界団体等

・不正使用の実態を踏まえて、C．2．で示し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啓発活動に取り組む。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。

・不正使用による被害の実態や最新の犯罪手口等や、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。

４．2016 年度（平成 28 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、2016 年度（平成 28 年度）は、現時点で不正使用による被害が発生している加盟店においては、その不正使用を阻止する具体的な対応を講ずるとともに、同業他社にシフトすることを抑止するため、リスクの高い特定の業種に対して不正使用を防止する取組を合わせて進める。

なお、2017 年度（平成 29 年度）以降の取組みについては、2016 年度（平成 28 年度）の進捗状況や不正使用被害の実態及び新たな技術の進化等を踏まえて、検討を進めることとする。

（１）不正使用被害額が大きい加盟店のうち、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

・不正使用被害額が大きい加盟店のうち、不正使用の対象となるリスクが高い「カード番号＋有効期限」のみで決済を行い、本人認証技術等の不正使用対策を講じていない加盟店に対しては、カード会社（アクワイアラー）及びPSPは、加盟店と協働してC．2．で示した方策を基本として、不正使用によって取引されやすい商材、サービスや業種、規模等に応じて、早急に何らかの方策を導入するよう必要な措置を講ずる。

（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の不正使用対策に係る方策の分析及び有効な対策の導入に向けた取組

・不正使用対策の具体的な方策や、独自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加盟店については、カード会社（アクワイアラー）及びPSPは、加盟店と協働して、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、C．2．で示した方策を基本として、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。

（３）特定の業種のうち、不正使用被害額が小さい加盟店の中で不正使用対策を講じていない加盟店への対応

・クレジットカードの不正使用によって取引されやすい業種については、主要カード会社10社の過去のデータから分析した結果、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業種が全体の被害額の70%超を占めた。

・よって、カード会社（アクワイアラー）及びPSPは、この5業種の加盟店のうち、不正使用被害額は小さいが何ら不正使用対策を講じてない加盟店に対しては、C．2．で示した方策など不正使用対策に関する周知に努め、有効な対策を導入するよう必要な措置を講ずる。

（４）加盟店での不正検知普及のための方策の検討

・EC 決済の際の購入者の属性を分析し異常な取引を検知する等の取組も効果があると考えられるため、本協議会において、加盟店にしか取得できない情報を駆使する等して、最新の統計分析技術で判定する方策について有用性を検証し、普及に向けた検討を行う。

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ており、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。

そのため、クレジットカード取引のセキュリティ対策を強化するためには、消費者の理解・協力が不可欠である。

2014 年（平成 26 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（平成 27 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、クレジット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・協力も重要である。

また、クレジットカード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、本協議会の事務局である（一社）日本クレジット協会によるセキュリティ関係機関との連携や、効果的な情報発信の取組を進める。

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

①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防止の点では、消費者が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、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り組むこととする。

特に、PIN を認知していない消費者（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。

②ID／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、消費者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停止等 ID・パスワードの管理の徹底について業界団体等は広報等に引き続き取り組むこととする。

③EC 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、消費者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消費者の理解・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り組むこととする。

④セキュリティの取組に関する可視化の検討

クレジットカードを安全・安心に利用できる環境を整備する観点から、消費者が加盟店の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にすることで、セキュリティ対策への加盟店のインセンティブを付与することが重要である。

そのため、（一社）日本クレジット協会及び行政は、加盟店が PCIDSS 準拠や決済端末の IC 対応等の取組が完了している場合に、消費者向けの表示スキームのあり方等について検討を行うこととする。

（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、特に、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・発信等に努めるものとする。

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

本協議会の参加各社等は本実行計画に基づき、2020 年（平成 32 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が、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ことから、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（一社）日本クレジット協会にセキュリティ対策に係る専門部署を設置し、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。

【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

◆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

◆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

◆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