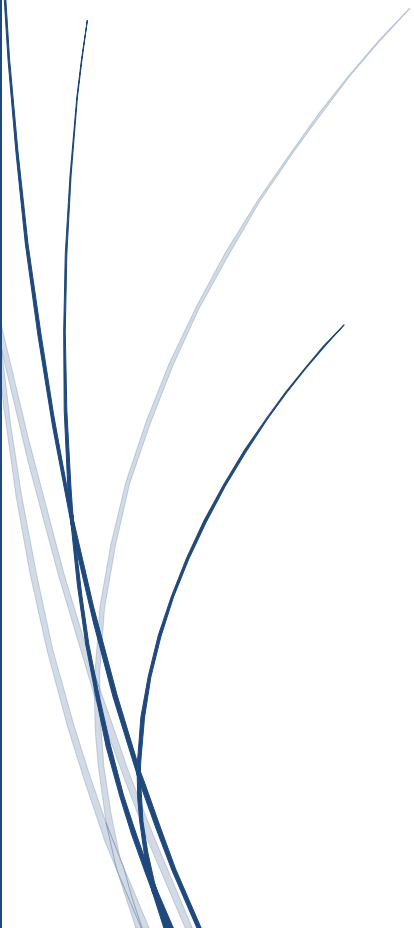




2020年3月

クレジットカード取引等におけるセキュリティ対策の  
現状と2020年度以降の取組について

～実行計画後の取組（ポスト2020）～



クレジットカード取引セキュリティ対策協議会  
事務局 一般社団法人日本クレジット協会

—目次—

はじめに	2
I. クレジットカード市場の現状と不正利用被害の動向	4
1. クレジットカード市場の現状	4
2. 不正利用被害の動向	5
II. 実行計画を踏まえたセキュリティ対策の課題とポスト2020における取組	7
1. クレジットカード情報保護対策	7
2. クレジットカード偽造防止対策	11
3. 非対面取引における不正利用対策	14
4. 新たな決済サービス等におけるセキュリティ対策	19
5. 消費者啓発の実施	21
6. 技術・運用指針の更新	22
III. ポスト2020における協議会の検討体制の再構築等について	23
1. ポスト2020における協議会の目的・役割	23
2. 主な取組事項	24
3. 本協議会の委員構成及び検討のための組織体制	25

## はじめに

「クレジット取引セキュリティ対策協議会（以下「本協議会」という）」は、2015年3月に設立され、2020年に開催される「東京オリンピック・パラリンピック競技大会」に向けて、消費者がクレジットカード等を安全に利用できる環境整備を進めるため、クレジットカード取引に関する幅広い事業者（クレジットカード会社、加盟店、PSP（Payment Service Provider）、機器メーカー、ソリューションベンダー、情報処理センター、セキュリティ事業者、国際ブランド）及び行政、業界団体等の連携によって「国際水準のセキュリティ環境」を実現し、もって我が国のキャッシュレス決済の普及による決済の利便性・効率性の向上を図るために活動を行ってきている。

本協議会では、クレジットカード取引の関係事業者が、各々の役割に応じて取り組むべきセキュリティ対策について検討し、2016年2月に「クレジット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、広く関係事業者等に周知するとともに協力を要請し計画推進に向けた取組を開始した。それから今日まで、毎年度各主体における計画の進捗状況を検証しつつ、実行計画を推進するための追加的な検討や見直し等を行い目標実現に向けて取組を続けてきた。

この間、政府では「日本再興戦略 2014（2014年6月24日閣議決定）」を皮切りにキャッシュレス化の方策を打ち出し、「未来投資戦略 2018（2018年6月15日閣議決定）」では、キャッシュレス推進協議会の設立、キャッシュレス決済比率4割程度を目指すというKPIを掲げ推進を求めている。さらに2019年10月からは、消費税率引上げに伴う需要平準化対策の一環として「キャッシュレス・消費者還元事業」も開始された。

また、2016年10月にはカード会社のみならず、加盟店に対してもセキュリティ対策の義務化等を盛り込んだ割賦販売法が改正され、2018年6月から施行されている。

このような政府のキャッシュレス化推進の動きもあり、クレジットカード取引は、2015年から2018年までの3年間で16兆8,536億円、33.8%の増加と堅調に伸びてきている。一方で、不正利用の被害額は2015年に120.9億円であったものが2018年には235.4億円と94.7%増となり、ほぼ倍増している。

実行計画や割賦販売法の改正により、多くの関係事業者のセキュリティ対策の取組は大きく前進したが、一方で不正犯によるカード情報の窃取、不正利用の手口も多様化している。

また、キャッシュレス化の推進により、新たな決済事業者の参入が進んでいるが、セキュリテ

ィ対策等が不十分な状況で事業を開始し、その脆弱さを狙われて不正利用被害が発生した事例もあった。

不正利用被害は不正犯の資金源に繋がり、不正犯の増加、ひいては新たな不正利用手段の出現にも繋がり得るため、カード会社（イシューアール・アクワイアラー）、加盟店を始めとした関係事業者が一体となって不正利用対策を実施する必要がある。

本協議会の実行計画では、2020年3月末をセキュリティ対策の実施期限として設定し、取組を進めてきたが、新たな手口等によるカード情報の漏えい、不正利用の発生、新たな決済サービスの進展等クレジットカード取引を取り巻く環境も変化している状況を踏まえ、引き続き必要なセキュリティ対策を検討し、実施していくことが必要である。

そこで、本協議会としては、カード情報漏えい、不正利用被害の現状を踏まえ、実行計画後のセキュリティ対策の在り方を検討し、ここに“実行計画後の取組（ポスト2020）”として取りまとめるものである。

なお、関係事業者におけるセキュリティ対策にかかる措置の実務上の指針と位置づけていた実行計画の後継文書となる「クレジットカード・セキュリティガイドライン」も別途策定している。

この“実行計画後の取組（ポスト2020）”に基づき、関係事業者等が一丸となって更なるセキュリティ対策に取り組むことにより、より一層安全・安心なクレジットカード取引環境が実現することを期待する。

2020年3月

## I. クレジットカード市場の現状と不正利用被害の動向

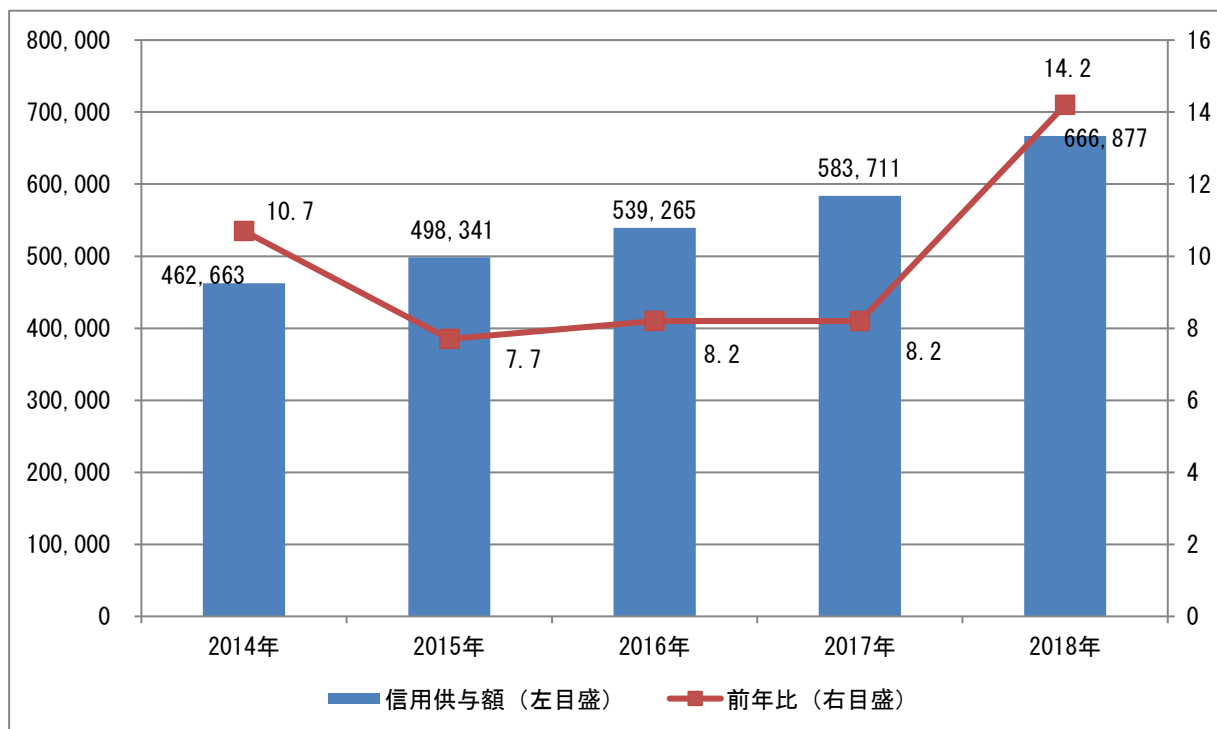
### 1. クレジットカード市場の現状

我が国のクレジットカードショッピングの信用供与額は、本協議会が設置された2015年には49兆8,341億円であったものが、2018年には66兆6,877億円と、16兆8,536億円の増加、33.8%の伸びとなっている。（【図表1】「クレジットカードショッピング信用供与額」参照）

このクレジットカードショッピングの信用供与額が、民間最終消費支出に占める割合を見てみると、2015年の16.6%に対して、2018年は21.9%と5.3%増加している。（【図表2】「民間最終消費支出とクレジットカードショッピング信用供与額の推移」参照）

【図表1】クレジットカードショッピング信用供与額

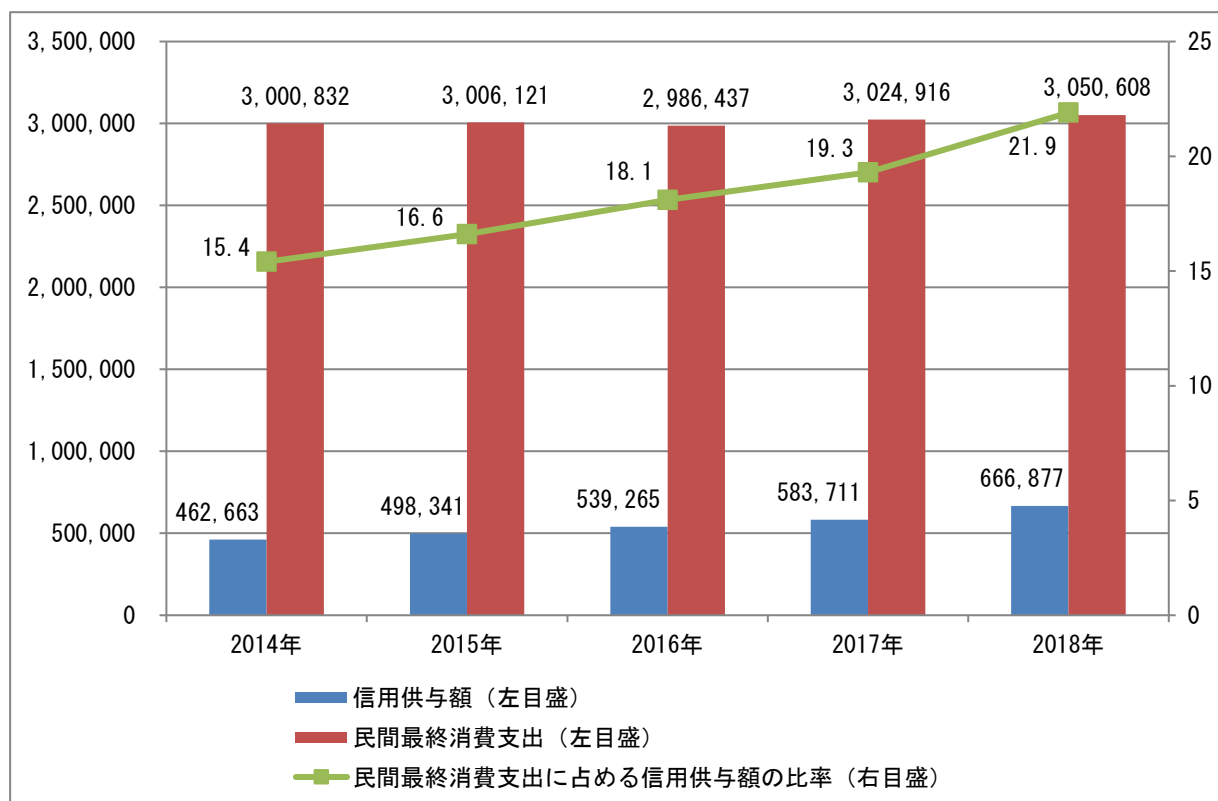
（単位：億円、%）



出所：日本クレジット協会「日本のクレジット統計」

【図表 2】 民間最終消費支出とクレジットカードショッピング信用供与額の推移

(単位: 億円、%)



出所：内閣府「国民経済計算年報」

日本クレジット協会「日本のクレジット統計」

## 2. 不正利用被害の動向

クレジットカードの不正利用被害額は、2015年に120.9億円であったが、2018年には、235.4億円となり、3年間で114.5億円、94.7%の増加となっている。

不正利用の内訳を、①偽造カード被害、②番号盗用被害、③その他不正利用被害（定義は後述を参照）で見ると、「偽造カード被害」については、増減があるものの2015年の23.1億円から2018年の16.0億円と7.1億円減少し、30.7%減となっている。「番号盗用被害」は、2015年の72.2億円が2018年には187.6億円と115.4億円増加、159.8%増と大幅に増加している。

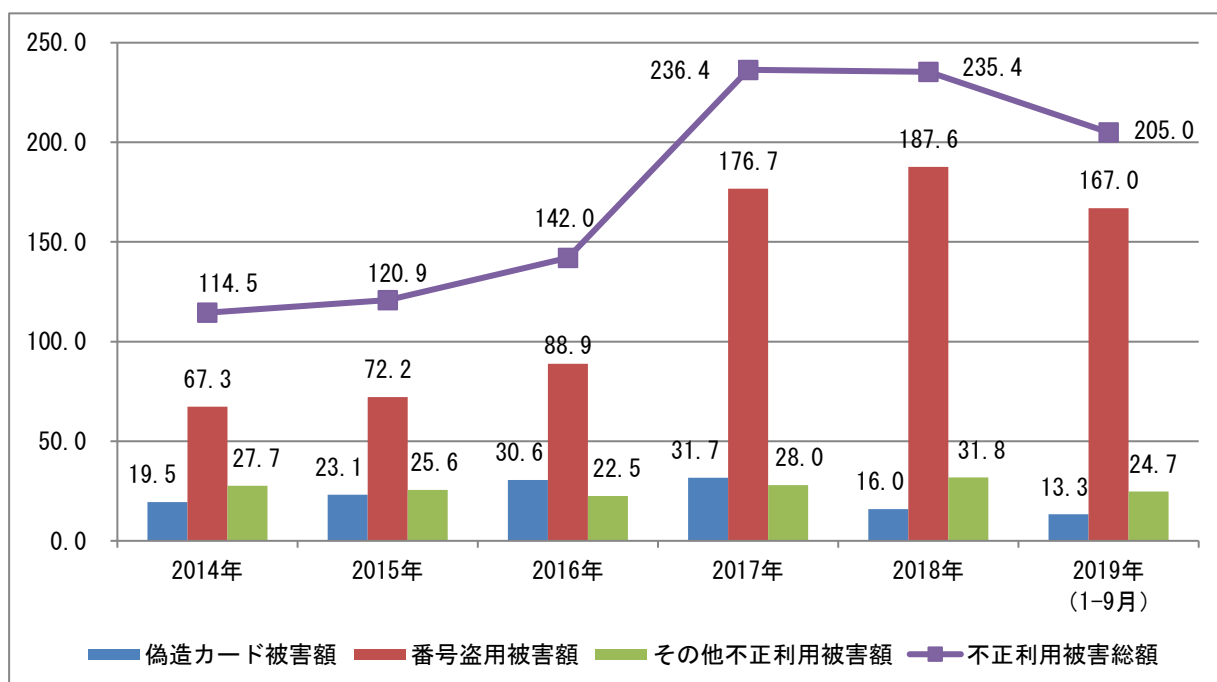
「その他不正利用被害」は、2015年の25.6億円が2018年には31.8億円と6.2億円増加、24.2%増となっている。2019年1-9月を見ても「偽造カード被害」「その他不正利用被害」は前年同期比で微増に止まっているものの、「番号盗用被害」は引き続き増加の傾向にある。（【図表3】「クレジットカード不正利用被害の発生状況」参照）

<不正利用手口の定義>

- ①偽造カード被害：不正に取得されたカード番号等を用いて作成された偽造カードで決済された取引の被害
- ②番号盗用被害：不正に取得されたカード番号等を用いてカード会員本人になりすまされて決済された取引の被害
- ③その他不正利用被害：①及び②以外の不正利用（例えば、紛失したカード、盗難されたカードの不正利用）で決済された取引の被害

【図表 3】クレジットカード不正利用被害の発生状況

(単位:億円)



出所：日本クレジット協会「クレジットカード不正利用被害の発生状況」

## II. 実行計画を踏まえたセキュリティ対策の課題とポスト2020における取組

### 1. クレジットカード情報保護対策

#### (1) クレジットカード情報保護対策の推進状況

本協議会では、カード情報保護対策として、加盟店に対しては、カード情報の非保持化（非保持と同等/相当を含む）又はカード情報を保持する場合には PCI DSS（Payment Card Industry Data Security Standard）準拠、業務上カード情報を保持するカード会社や PSP などの事業者については PCI DSS 準拠を求めている。

また、これら事業者がカード情報を取り扱う業務を外部委託する場合は、委託者である各主体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ることとしている。

さらに、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、必要なカード情報保護対策を行うことが求められている。本協議会ではこれらの対策を推進するため、加盟店の業界団体と協力して傘下の加盟店向けに継続的に説明会等を開催し対応を求めるとともに、実際に個々の加盟店に対して対策の推進にあたるカード会社（アクワイアラー）や PSP 等の実務担当者向けに必要な知識や情報を提供する各種セミナーを開催している。

なお、対策を講じた加盟店へ、近時の漏えい事案の傾向等を踏まえ、自社のシステムについて定期的な点検を行い、システムの脆弱性が発覚した場合は、漏えい防止のための追加的な対策を求めるとともに、カード会社（アクワイアラー）や PSP 等へ新たな攻撃手口への対策の改善や強化についても情報提供等を行っている。

また、PCI DSS 準拠をサポートするため、日本カード情報セキュリティ協議会（JCDS）と連携し、資料や情報の提供、相談窓口の設置等も継続して実施している。

#### (2) カード情報の漏えいの現状

##### ① カード情報漏えい事案及び漏えいしたカード番号数の推移

カード情報の漏えいは、そのほとんどが EC 加盟店からの漏えいである。そこで 2016 年から 2019 年 9 月までに、EC 加盟店から対外公表された漏えい事案について調査したところ、漏えい件数は 2016 年が 13 件であったのに対して、2019 年は 9 月時点で既に 22 件と増加傾向にある。一方で漏えいしたカード番号数は、626,871 件から 243,423 件と 62% の減少となっており、一事案あたりの漏えいカード番号数は減少傾向にある。（【図表 4】「カード情報漏えい事案の件数及び漏えいしたカード番号数」参照）



【図表 4】カード情報漏えい事案の件数及び漏えいしたカード番号数

(単位：件)

	2016年	2017年	2018年	2019年 (9月現在)
1) 漏えい事案件数	13	11	13	22
うち偽の決済画面による漏えい事案件数	0	0	8	13
2) 漏えいカード番号数	626,871	813,492	294,012	243,423

出所：本協議会事務局調べ

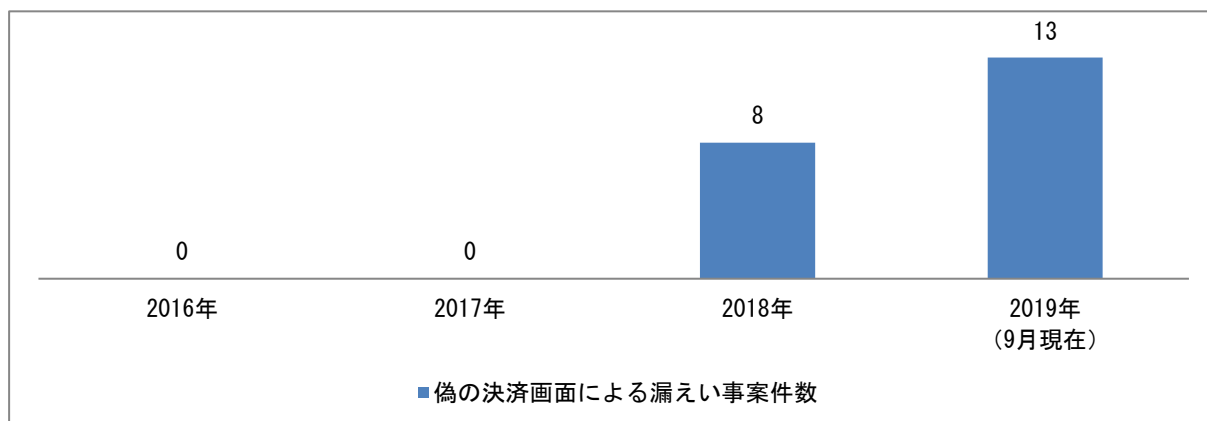
## ②漏えい事案の手口の変化

EC 加盟店の漏えいの原因を調査したところ、ウェブサイトの URL の特定が容易であったり、簡易なログインパスワードを設定したりしていることにより管理画面へのアクセス制御が適切に行われていないなど、ウェブサイトの開発・運用段階での設定の不備や委託先の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）の脆弱性等を狙ってカード会員を偽の決済画面に誘導し、当該偽画面に入力されたカード情報等を窃取するという手口が、2018 年から目立ち始め、2019 年には漏えい事案 22 件の内 13 件（59.1%）がこの手口になっている。（【図表 4】「カード情報漏えい事案の件数及び漏えいしたカード番号数」参照）

この手口により漏えいが発生した加盟店の大多数は非保持化対応を実施済みであるものの、不正犯のつけ入る隙があったことが確認されている。EC 加盟店の非保持化対応により、加盟店自身が保有しているカード情報を窃取することができなくなったことから、ウェブサイトの脆弱性や設定の不備等を狙った手口にシフトしてきたものと考えられる。（【図表 5】「偽の決済画面による漏えい事案の推移」参照）

【図表 5】偽の決済画面による漏えい事案の推移

(単位：件)



出所：本協議会事務局調べ（2019 年は 1 月～9 月の 9 ヶ月間）

### **(3) カード情報保護対策の今後の取組について**

#### **①クレジットカード情報保護対策未対応先の推進加速**

加盟店からのカード情報の漏えい事案が引き続き発生している現状において、対策を講じていない加盟店は早急にカード情報の非保持化（非保持と同等/相当を含む）又は PCI DSS に準拠しなければならない。

また、アクワイアラーは、これら未対応の加盟店のカード情報保護対策を加速するため、必要な措置を講じるよう指導することが求められる。

なお、カード情報を取り扱うカード会社、PSP においては引き続き PCI DSS に準拠し、これを維持・運用することが求められる。

#### **②クレジットカード情報保護対策の維持・運用**

クレジットカード取引に関係する事業者においては、非保持化や PCI DSS 準拠等のカード情報保護対策は一過性のものではなく、その安全性を確保するための維持・管理が重要となる。また、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・向上に向けて継続的な取組が重要である。

PCI DSS の基準を策定する機関である PCI SSC (Payment Card Industry Security Standards Council) は、2020 年後半以降に現行の PCI DSS をバージョン 3.2.1 から 4.0 に改訂する予定であり、対象事業者は新バージョンへの対応が必要となるが、特に準拠検証を自己問診 (SAQ (Self-Assessment Questionnaire)) にて行っているカード会社等は、このような基準の改訂内容についても理解したうえで対応することが必要となる。

PCI SSC では、ペイメントセキュリティ情報における入門レベルの資格である PCIP (Payment Card Industry Professional) を奨励したり、企業内の PCI DSS 要件の専門家である ISA (Internal Security Assessor) を育成したりする取組等も実施している。自己問診 (SAQ) による準拠を行っているカード会社等においては、このような制度を活用することも自社のセキュリティ対策の推進・維持管理や新バージョンへの対応において有効な手段の一つであると考えられる。

#### **③カード情報保護対策の対象事業者の拡大**

本協議会では、カード情報保護対策を、主に加盟店、カード会社（イシューア、アクワイアラー）、PSP に対して求めてきたが、安全・安心なクレジットカード利用環境を実現するためには、クレジットカードに紐づいた決済サービスを利用者に提供するコード決済サービス事業者や EC モール事業者、さらには、それらの事業者から委託を受けて大量のクレジットカード番号等を取り扱う事業者についても、適切なカード情報保護対策が求められる。

### **(4) 多様化・巧妙化する手口等への対応**

カード情報を窃取しようとする不正犯はセキュリティ対策が脆弱な箇所を狙い、その手口は多様化かつ巧妙化している。前述のように管理画面へのアクセス制御が適切に行われていないなど、加盟店のウェブサイトの開発・運用段階での設定の不備や決済ソリューション（ショッピングカート機能等）の脆弱性等があれば、非保持化を行っていたとしても当該箇所からカード情

報が窃取されるリスクが存在する。本協議会ではこのようなカード情報漏えいの手口に関する情報を関係事業者に提供し、注意を促すとともに対応方法等に関するセミナー等を開催してきた。

2020年度以降は、関係事業者に加え、セキュリティの専門機関からシステムの脆弱性や漏えい手口及び対応策に関する情報収集を行い、関係事業者が取組むべき対策を検証し、対策が必要な関係事業者に対して迅速かつ的確な情報提供を行い、対応を促していく。

## 2. クレジットカード偽造防止対策

### (1) クレジットカード偽造防止対策の推進状況

本協議会では、クレジットカードの偽造防止による不正利用対策として、IC取引の実現が現状では最も有効な対策であると位置付け、カード会社に対してはクレジットカードのIC化を、加盟店に対しては決済端末のIC対応を求めてきた。

#### ①クレジットカードのIC化の進捗状況

カード会社（イシューア）は、2020年3月末までに国内で流通する国際ブランド付きのクレジットカードのIC化100%を目指し、クレジットカードの更新時期にかかわらず、磁気カードからICカードへの切替を実施している。

また、日本クレジット協会は、カード会社（イシューア）によるIC化の取組について毎年進捗を管理しその達成状況について公表してきた。行政もまた、その進捗状況を踏まえ、対応が遅れている事業者への個別指導を行う等、カードのIC化100%達成に向けて着実な推進を図ってきた。

この結果、カードのIC化率は、2019年末現在、95.1%の進捗となっている（2020年3月末99.5%見込み）。

#### ②決済端末のIC対応の進捗状況

加盟店は、2020年3月末までに店頭に設置する決済端末のIC対応を完了することとしており、特に、独自のPOSシステムでクレジットカード決済を行っている加盟店においては、カード会社（アクワイアラー）や機器メーカー等と連携し、自社のシステム及びオペレーションに即したIC対応を進めている。本協議会は、このPOSシステムでクレジットカード決済を行っている加盟店のIC対応に必要な手法について、技術面、運用面、コスト面の課題を整理し、各種ガイドラインを策定、関係事業者へその周知を図り、IC対応の加速化をサポートしてきた。

また、我が国固有の商慣習や業務特性、端末の設置環境等により国際的なセキュリティ基準に完全準拠させることが現状困難な特定業界向け（ガソリンスタンドに設置の精算機（ガスPOS）/オートローディング式自動精算機）のIC対応についても、実効性のある対策を推進するため、代替コントロール策による暫定的なIC対応についての指針を示し、関係事業者への周知を図ってきた。

POSシステムでクレジットカード決済を行っている加盟店は、実行計画や各種ガイドラインに基づき、着実にIC対応を進めているところである。また、CCT（Credit Center Terminalの略。共同利用端末として運営される情報処理センターの信用照会端末）のIC対応についても進捗しており、2019年9月末時点でカードの有効性チェックのみを行う端末、撤収予定（長期間未稼働）の端末及びPOSと分類される端末を除くと95.7%となっており、IC対応100%の達成に向けて取組が進んでいる。

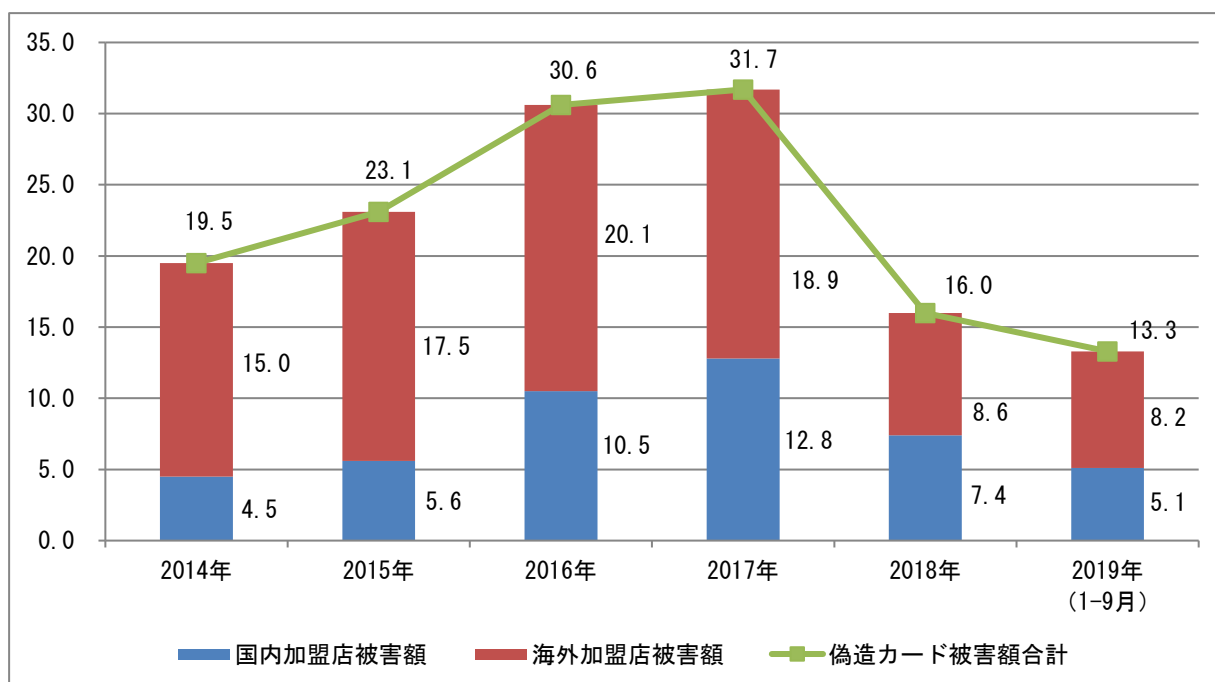
## (2) クレジットカード偽造による不正利用被害の発生状況

日本クレジット協会が実施、公表しているクレジットカードの不正利用被害額調査における偽造カード被害額を見ると、増減を繰り返しながらも、IC取引の実現がかなり進捗した2018年においては、約16億円と前年比で半減（2017年31.7億円）に近い減少傾向となっている。（【図表6】「国内・海外加盟店別クレジットカード偽造被害の推移」参照）

また、偽造カード被害額の国内加盟店・海外加盟店の比率を見ると、海外加盟店は減少（2014年15億円、76.9% → 2018年度8.6億円、53.8%）し、国内加盟店は上昇（2014年4.5億円、23.1% → 2018年度7.4億円、46.3%）している。これは、海外加盟店におけるIC対応が国内加盟店よりも先行して進捗したことによるものと想定される。国内加盟店における偽造カード被害額の総額自体は減少傾向にあるが、グローバルにIC対応が進展している現状において、的確に国内加盟店のIC対応を実施していないと、我が国が偽造カードによる不正利用の標的となるおそれがあり、IC対応未完了加盟店の対応の加速が必須である。

【図表6】国内・海外加盟店別クレジットカード偽造被害の推移

（単位：億円）



出所：日本クレジット協会 「クレジットカード不正利用被害の発生状況」

## (3) クレジットカード偽造防止対策の今後の取組について

### ①IC対応未完了加盟店及びカードのIC化未達カード発行会社の対応加速化

カード偽造による不正利用の防止に向けた対策、「加盟店の決済端末のIC対応」及び「クレジットカードのIC化」については、2020年3月末の期限に向けて加盟店、カード会社が

各々着実に取組んできたが、引き続き、加盟店は IC 対応、カード会社（イシューア）は IC 化、カード会社（アクワイアラー）は加盟店への指導を行うことにより、対策未完了先の対応の更なる加速を図る。

## ②特定業界向けの暫定措置の継続と見直し

我が国固有の商慣習や業務特性、端末の設置環境等により国際的なセキュリティ基準に完全準拠させることが現状困難な特定業界向けの暫定対応（ガソリンスタンドに設置の精算機（ガス POS）/オートローディング式自動精算機）については、未だ暫定対応の解消が可能な環境が整っていないことから、今後の技術面の進展等や市場の動向を注視しつつ、2020年4月以降も当面の間は、ガソリンスタンドに設置する精算機については、「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」に基づく実現可能な方策による IC 対応、オートローディング式自動精算機については、「オートローディング式自動精算機の IC 対応指針と自動精算機の本人確認方法について」に基づく代替コントロール策による暫定的な IC 対応を継続しつつ、方策や代替コントロール策の内容については必要に応じ適宜見直しを図っていくこととする。

## ③PIN バイパスの取扱に関する検討の継続

カード会員による PIN（Personal Identification Number の略。暗証番号）失念の一時的な救済措置としてカード会員の申出に基づき運用されている「PIN 入力スキップ機能（PIN バイパス）」については、当該運用に伴う PIN 入力による本人確認の未実施により、紛失・盗難カード等による不正利用被害が発生していることや、PIN 入力スキップ機能を許容しない海外発行会社のカードが存在していることを踏まえ、日本クレジット協会及びカード会社においては、紛失・盗難カード等第三者による悪用の回避のため、代替策による対応を含め将来的な廃止に向けて検討を継続することとする。

### **3. 非対面取引における不正利用対策**

#### **(1) なりすましによる不正利用対策の推進状況**

本協議会では、なりすましの不正利用を防止するための方策についてその効果を検証しつつ、現時点では「本人認証」「券面認証（セキュリティコード）」「属性・行動分析（不正検知システム）」「配送先情報」の4つの方策を一定の効果が得られるものとして採用している。そのうえで、これら4つの方策をベースに加盟店のリスクや被害発生状況等に応じた方策の導入指針を示している。

これまでの加盟店における方策の導入指針としては、全ての非対面加盟店に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ことと、オーソリゼーション処理のための体制整備を求めたうえで、加盟店の取り扱う商材や不正利用被害の発生状況等を踏まえ、特に不正利用被害の発生が集中している「デジタルコンテンツ（オンラインゲームも含む）」「家電」「電子マネー」「チケット」といった商材を「特定4商材」とし、これら4商材を主たる商材として取り扱っている「高リスク商材取扱加盟店」に該当する加盟店には4つの方策のうち1方策以上、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「3ヵ月連続50万円超」発生している「不正顕在化加盟店」に該当する加盟店には2方策以上の導入を求めてきた。

さらに、これらの方策については、単体で導入するだけでなく、それぞれの方策を組み合わせることで導入することによってより高い効果が得られる場合もあることから、導入に際しての参考とするため、実際に防止効果を上げたケースについても検証を行い、好事例（「2019年版実行計画上の方策導入による不正抑止の好事例の紹介」）として公表してきた。

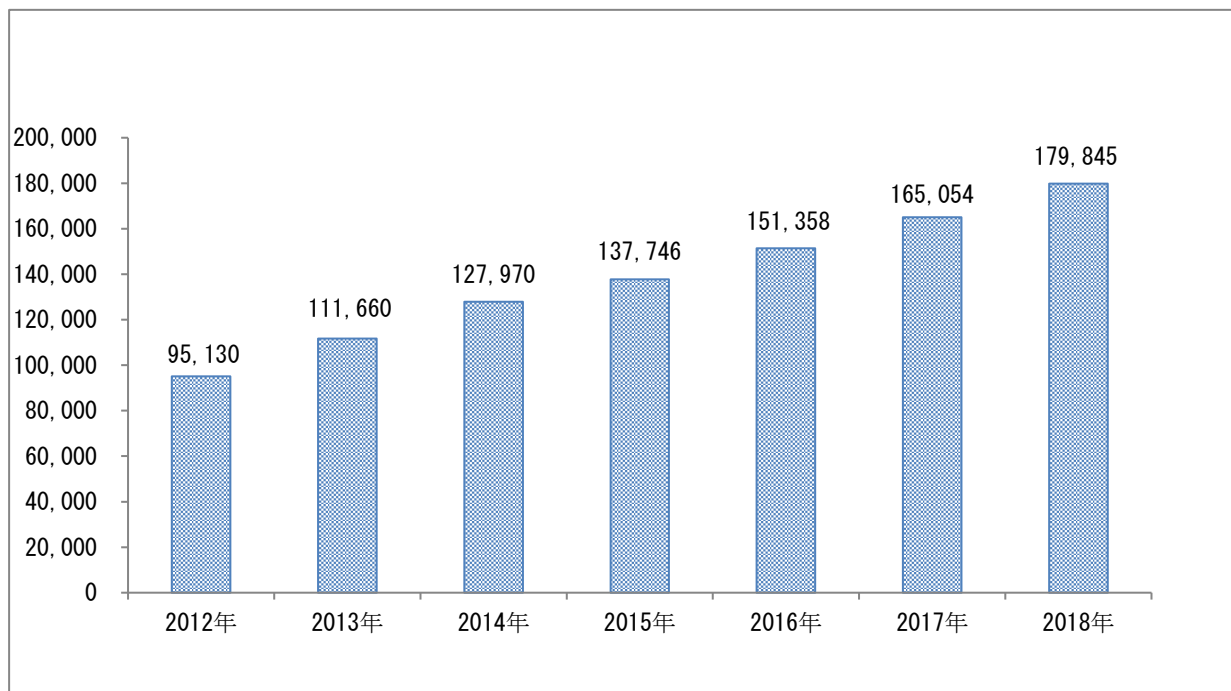
#### **(2) 非対面取引における不正利用被害の発生状況**

##### **① EC市場の取扱高とクレジットカード取引の取扱高推移**

経済産業省の調査によれば、我が国のBtoCのEC市場規模は、物販系分野、サービス系分野を中心に拡大を続けており2015年から2018年の3年間で30.6%増加している（【図表7】「日本のBtoC-EC市場規模の推移」参照）。このEC市場の拡大に伴って、ECにおける決済手段として親和性の高い（【図表8】「インターネットで購入・取引する場合の決済方法の推移」参照）クレジットカードの取扱高も一貫して増加しており、同じ時期におけるクレジットカード取引の取扱高を見ても、3年間で33.8%の増加を示している（【図表1】「クレジットカードショッピング信用供与額（4頁）」参照）。

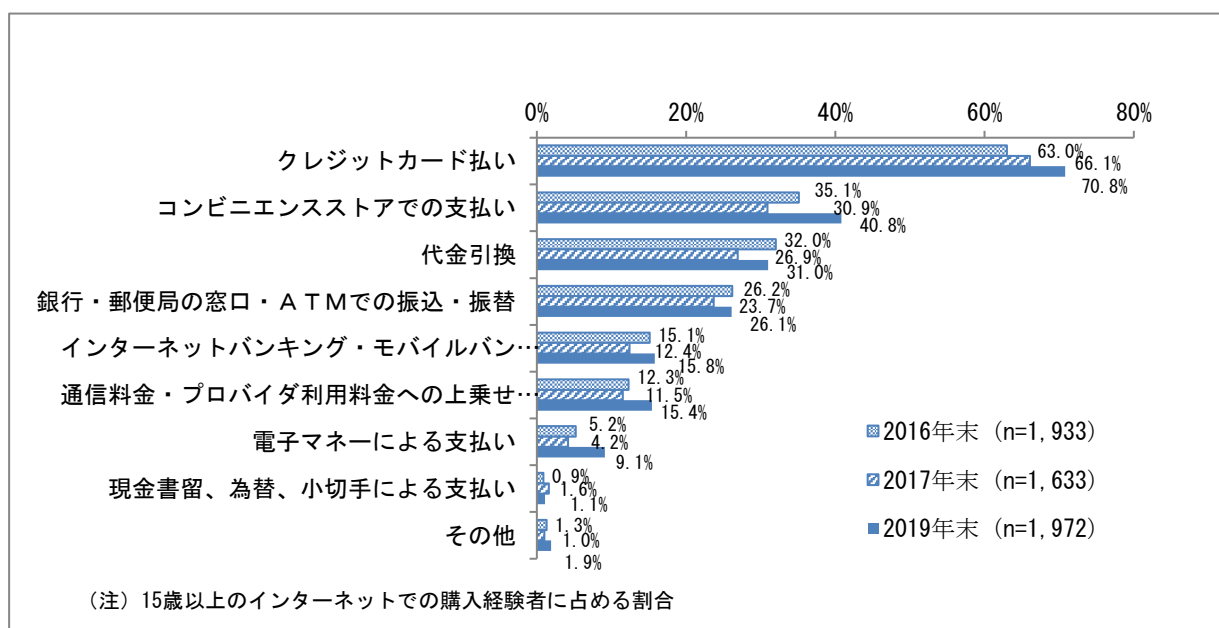
【図表 7】日本の BtoC-EC 市場規模の推移

(単位：億円)



出所：経済産業省情報経済課「平成 30 年度我が国におけるデータ駆動型社会に係る基盤整備（電子商取引に関する市場調査）」

【図表 8】インターネットで購入・取引する場合の決済方法の推移



出所：総務省「平成 30 年通信利用動向調査報告書（世帯編）」

※図表中の「n」は回答者数



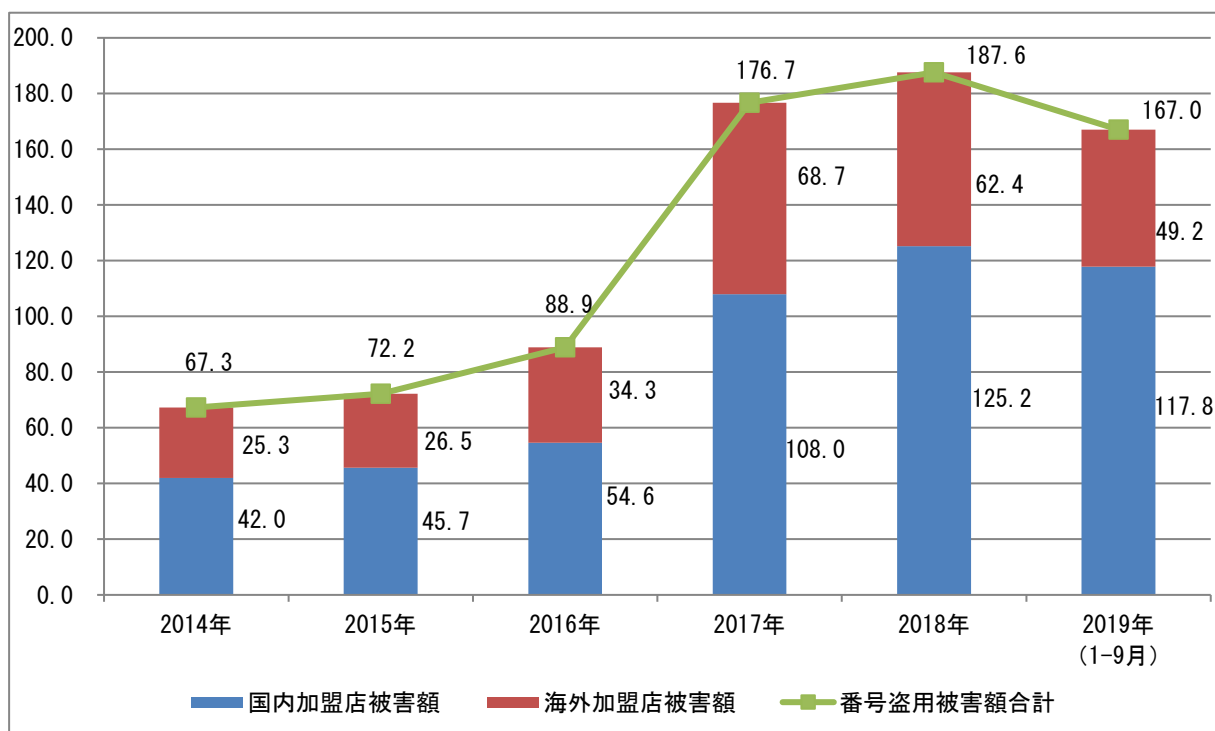
## ②非対面取引における不正利用被害額の推移

### 1) 不正利用被害額調査

日本クレジット協会が四半期毎に実施しているクレジットカードの不正利用被害額調査において、非対面取引の不正利用被害に該当する「番号盗用」の不正利用被害額は、2015年に72.2億円であったものが、2018年には187.6億円と大きく増加しており3年間で159.8%の伸びとなっている。国内加盟店における不正利用被害だけを見ると、2015年に45.7億円であったものが、2018年には125.2億円と174.0%と更に高い伸びとなっている。2019年1-9月においても、「番号盗用」による不正利用被害額は既に167億円を計上しており、引き続き増加傾向にある。(図表9「国内・海外加盟店別クレジットカード不正利用被害(番号盗用)推移」参照)

【図表9】国内・海外加盟店別クレジットカード不正利用被害額(番号盗用)推移

(単位：億円)



出所：日本クレジット協会「クレジットカード不正利用被害の発生状況」

### 2) 高リスク商材取扱加盟店

本協議会では、特に不正利用被害の発生が集中している「デジタルコンテンツ(オンラインゲームも含む)」「家電」「電子マネー」「チケット」といった商材を「特定4商材」とし、これら4商材を主たる商材として取り扱っている加盟店を「高リスク商材取扱加盟店」として注視し、4つの方策のうち1方策以上の導入を求めてきた。

高リスク商材取扱加盟店の根拠となる不正犯に狙われやすい商材の傾向について、毎年妥

当性の検証を行っているが、「特定4商材」の不正利用被害額は、いずれの商材も残念ながら高止まりの中で増減を繰り返しており、不正利用被害額全体に占めるシェアでは上位を占めていることから、引き続き被害発生防止に注力する必要がある商材と位置づけている。

また、宿泊予約サイトにて宿泊施設の予約手配を提供する「宿泊予約サービス」の不正利用被害が2018年度下期の調査結果においては急増している。このため、本協議会としては、今般の不正利用被害の状況を踏まえ、高リスク商材へ追加するとともに、関係事業者に注意喚起を行っている。(【図表10】「2016年度下期以降の不正利用被害商材のシェア推移」参照)  
今後も高リスク商材の該当性を注視し、適時適切な対応を求めていく。

【図表10】2016年度下期以降の不正利用被害商材のシェア推移

商材	2016年度下期		2017年度上期			2017年度下期			2018年度上期			2018年度下期		
	不正被害額 (比率)	シェア	不正被害額 (比率)	シェア	前期比	不正被害額 (比率)	シェア	前期比	不正被害額 (比率)	シェア	前期比	不正被害額 (比率)	シェア	前期比
1. チケット・金券	26	26.1%	32	23.2%	-2.9p	30	21.8%	-1.4p	39	26.6%	+4.8p	38	19.2%	-7.4p
2. 宿泊予約サービス	8	8.5%	28	20.1%	+11.6p	18	13.1%	-7.0p	6	4.3%	-8.8p	28	14.1%	+9.8p
3. 家電	10	9.8%	13	9.2%	-0.6p	15	10.8%	+1.6p	16	11.0%	+0.2p	25	12.8%	+1.8p
4. 電子マネー	10	9.7%	11	7.7%	-2.0p	17	12.2%	+4.5p	10	6.5%	-5.7p	12	6.0%	-0.5p
5. デジタルコンテンツ	11	10.5%	8	6.0%	-4.5p	7	5.2%	-0.8p	10	6.8%	+1.6p	9	4.4%	-2.4p
6. アプリ	4	3.9%	5	3.8%	-0.1p	2	1.4%	-2.4p	4	3.0%	+1.6p	8	4.1%	+1.1p
7. 貴金属・時計	2	1.5%	3	2.0%	+0.5p	3	1.9%	-0.1p	3	2.1%	+0.2p	3	1.7%	-0.4p
8. ブランド品	1	0.6%	1	0.6%	0.0p	2	1.1%	+0.5p	3	1.8%	+0.7p	3	1.5%	-0.3p
9. 通信	2	1.6%	3	2.0%	+0.4p	3	2.4%	+0.4p	1	0.4%	-2.0p	2	0.9%	+0.5p
10. 化粧品	1	0.6%	2	1.2%	+0.6p	2	1.4%	+0.2p	1	0.9%	-0.5p	1	0.7%	-0.2p
11. スポーツ用品	1	0.9%	0	0.2%	-0.7p	1	1.0%	+0.8p	1	0.7%	-0.3p	1	0.7%	-0.2p
12. カー・バイク用品	0	0.0%	0	0.0%	-	1	0.9%	+0.9p	1	1.0%	+0.1p	0	0.0%	-1.0p
13. その他	6	6.3%	11	7.7%	+1.4p	10	7.6%	-0.1p	11	7.7%	+0.1p	10	5.2%	-2.5p
14. 小額分 (101位以下)	20	19.9%	23	16.3%	-3.6p	26	19.2%	+2.9p	40	27.0%	+7.8p	55	28.0%	+1.0p
合計	100	100.0%	140	100.0%	-	137	100.0%	-	147	100.0%	-	196	100.0%	-

出所：日本クレジット協会「実行計画-2019-」記載の非対面取引における不正利用方策にかか  
る調査結果報告書

※図表中の「不正被害額（比率）」は2016年度下期計を「100」とした比率にて表示

### （3）非対面取引における不正利用被害額の減少に向けた取組について

非対面取引においては、特にECの取扱高が大きく伸びており、これに比例するように不正利用被害もECでの発生が増加している。本協議会でも実行計画に基づき、主にECにおけるなりすましによる不正利用を防止するために取組を行ってきたが、不正犯の手口の巧妙化もあり、不正利用被害額を減少させるには至っていない。このため実行計画後においても、不正利用被害を減少させるために引き続き実効性のある取組が求められる。

#### ①加盟店におけるリスクに応じたセキュリティ対策の浸透

ECにおいてクレジットカードの不正利用被害が多発していることもあり、EC加盟店に対策導入が浸透してはいるものの、全く対策を講じていない加盟店が少なからず存在することから、対策が進捗しない要因を分析する必要がある。そのうえで、カード会社（アクワイア

ラー)及びPSPは連携しながら、全ての加盟店に対策を早急に講ずるよう指導するとともに、加盟店が取り扱う商材や不正利用被害の発生状況に応じた措置を求める。

加盟店は不正犯が狙う換金性商品等も日々変化していることを踏まえ、リスクに応じた対策を適宜実施していく必要がある。

## ②不正利用対策の再検証等

これまでの不正利用対策の効果検証の結果、対策の導入によって不正利用被害が大幅に減少したケースがあった一方で、具体的な効果が表れなかったケースも存在していることが判明している。原因としては、対策を導入したものの運用が的確ではない、本人認証や券面認証の追加認証による方策に対して、認証情報がクレジットカード番号や有効期限とともに漏えいしており、それらを不正に利用されているという状況が考えられる。

このように、導入した対策を実効性のあるものにするため、加盟店の対応実績やアクワイアラーの指導実績等も踏まえ、対策の運用について具体的な検証作業を実施し、より有効な対策を実施していく必要がある。

例1) 券面認証(セキュリティコード)について、コードが窃取されたり総当たり攻撃されたりして認証を突破されるケース等の発生状況の確認

例2) 本人認証(3-Dセキュア)について、固定(静的)パスワードを使用している場合、パスワードが窃取され認証を突破されるケース等の発生状況の確認

## 4. 新たな決済サービス等におけるセキュリティ対策

### (1) 新たな決済サービスにおける不正利用被害の発生状況

技術の進展やスマートフォン等のデバイスの普及、さらには各企業の経済圏構想等も相俟って、決済市場に様々な決済サービスが登場してきている。決済サービスの多様化は利用者に各種利便性を提供した一方で、一部の決済サービス事業者のセキュリティ面等の脆弱性を狙われ、クレジットカードを不正に利用される事案が発生した。

具体的には、コード決済サービスで次のような不正利用事案が発生している。

#### ①コード決済サービスに不正に入手したクレジットカード情報が登録され不正利用されたケース

2018年12月、不正に入手したクレジットカード情報が他者のコード決済サービスのアプリに登録され、不正利用された事案が発生。

#### ②不正に入手したID・パスワードでログインし、登録されていたクレジットカード情報で不正なチャージを行ったケース

2019年7月、コード決済サービスにて流出したID・パスワードにより、アプリ内で不正ログインが行われ、アプリと端末との紐付け管理がされていなかったため、登録されているクレジットカードを用いて残高チャージを行い、商品が購入される事案が発生。

### (2) 新たな決済サービスにおける不正利用対策の実施状況

コード決済サービスにおいて不正利用が発生したことを受けて、2019年4月に一般社団法人キャッシュレス推進協議会（以下「キャッシュレス推進協議会」）は「コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン」（以下「コード決済ガイドライン」）を取りまとめ、類似事案のコード決済サービスの不正利用防止に取り組んだ。しかし、一部のコード決済サービスにおいて、コード決済ガイドラインに定められた措置が実施されていなかったため、アカウントへ不正アクセスされ、そのアカウントへの残高チャージにクレジットカードが不正利用される事案が発生した。これを受けて、2019年7月に経済産業省は、コード決済サービス事業者等に対して、コード決済ガイドライン等の遵守を求めるとともに、常に最新のセキュリティ情報を収集し、自己のセキュリティ対策を見直したうえで、セキュリティレベルの向上に努めるよう要請している。

本協議会においても、カード会社（アクワイアラー）に対し、加盟店に向けてコード決済サービス事業者が、コード決済ガイドラインを遵守していることの確認に努めるよう指導することを要請している。

### (3) 新たな決済サービス等におけるカード情報保護

2019年12月に公表された産業構造審議会割賦販売小委員会報告書において、「PSP・コード決済事業者・ECモール事業者・決済システムの中で大量のクレジットカード番号等の取扱いを受託する事業者にも、クレジットカード番号等の適切管理義務を課すことが適当である」とさ

れた。これら事業者は大量のクレジットカード番号等を取り扱っており、漏えいすれば、大規模な情報漏えい事件につながることを懸念されるためである。

こうした状況を踏まえ、新たな決済サービス等事業者におけるカード情報保護の対応についても検討していく必要がある。

#### **(4) 本協議会における今後の取組**

クレジットカードが紐づくコード決済サービスは、クレジットカード番号を登録し、最終的にクレジットカードで決済される仕組みである。キャッシュレスの推進によりコード決済サービスの利用者、利用加盟店も拡大している状況において、なりすましによるクレジットカードの不正利用等が発生していることから、コード決済サービスにおけるクレジットカードの不正利用防止に向けた対策の検討及び取組が必要である。

本協議会では、キャッシュレス推進協議会と連携し、コード決済サービス事業者及びカード会社に対し、引き続きコード決済ガイドラインの遵守等を求めるとともに、コード決済サービスの不正利用の発生状況も踏まえ、クレジットカード業界として必要な対策の検討を行うこととする。

EC サイト内に保有されるアカウントに紐付いているクレジットカード情報が不正利用されるなど、最終的にクレジットカードで決済される決済手段の不正利用対策等についても検討を行っていくこととする。

また、PSP やコード決済サービス事業者、EC モール事業者、さらには、それらの事業者から委託を受けて大量のクレジットカード番号等を取り扱う事業者等におけるカード情報保護の対応を検討する。

## **5. 消費者啓発の実施**

クレジットカード取引におけるセキュリティ対策をより実効性のあるものとするためには、クレジットカード会員の正しい理解に基づく利用が不可欠である。また、不正犯の攻撃手口も巧妙化し、新たな攻撃手口が出現してくる一方で、対策技術も進歩していくことが想定されることから、そうした最新情報等を含め、クレジットカード利用者及び一般消費者を対象とした周知・啓発活動を事業者及び業界団体が継続的に実施していく必要がある。

また、成年年齢を18歳に引き下げることを内容とする民法の一部を改正する法律が成立（2022年4月施行）したことから、クレジットカードを初めて持つことが多いと思われる若年成人に対して、安全・安心なクレジットカードの利用方法やトラブルに巻き込まれた際の対処方等について重点的な周知活動を行うことが求められる。

### **（1）カード情報保護対策分野**

カード情報保護対策においては、従前からのID・パスワード使い回しについての周知・啓発を引き続き実施するとともに、フィッシングや加盟店サイトの改ざんによる偽画面への誘導により、カード会員から直接カード情報を窃取するなど近時増加している手口等について関係事業者、行政等と連携し、各方面への周知・啓発を実施していく。

### **（2）偽造カード被害対策分野**

偽造防止対策においては、不正利用対策の必要性とともに、IC対応加盟店の見える化やIC取引にはPIN入力が必要なこと及びPIN認知向上等について引き続き周知・啓発を実施していく。

### **（3）非対面不正利用対策分野**

なりすまし等による不正利用対策においては、不正利用対策の必要性とともに、インターネットショッピングにおけるカード利用時のパスワード等の入力やセキュリティコードの入力等の具体的な方策について引き続き周知・啓発を実施していく。

## 6. 技術・運用指針の更新

本協議会で取り組んでいるセキュリティ対策について各当事者が実際に取組むため、下記のような技術面、運用面の指針等を策定し、関係事業者を活用されている。これらの指針等は、技術の進歩や業務オペレーション等から適宜見直しが必要になることから、クレジットカード取引の実務実態及び実効性の観点を踏まえ、指針等の見直しの検討及び新たな指針の策定を行うこととする。

### 《本協議会で取りまとめた指針等》

- ①【追補版】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
- ②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
- ③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
- ④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
- ⑤オートローディング式自動精算機の IC 対応指針と自動精算機の本人確認方法について
- ⑥IC カード対応 POS ガイドライン
- ⑦IC カード対応 POS 導入の手引き～全体概要編～
- ⑧IC カード対応 POS 導入の手引き～取引処理フロー解説編～
- ⑨IC カード対応 POS 導入の手引き～認定・試験プロセス概要～
- ⑩ブランドテスト要否一覧
- ⑪非接触 EMV 対応 POS ガイドライン（全体概要編）
- ⑫非接触 EMV 対応 POS ガイドライン（取引処理編）
- ⑬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

### Ⅲ. ポスト2020における協議会の検討体制の再構築等について

#### 1. ポスト2020における協議会の目的・役割

本協議会は、2020年の東京オリンピック・パラリンピック競技大会に向けて、クレジットカード取引において「国際水準のセキュリティ環境」を整備することを目指してきた。このため、クレジットカード取引に係わる各主体がそれぞれの役割に応じて取り組むべき事項を「実行計画」として取りまとめ、2020年3月末を最終的な実施期限とし実現に向けた取組を進めてきた。

本協議会の目的からすれば、2020年3月末までに実行計画が達成され、国際水準のセキュリティ環境が整備されることで、その役割を果たすことになるが、「Ⅱ. 実行計画を踏まえたセキュリティ対策の課題とポスト2020における取組（7頁を参照）」で述べたように、実行計画の推進によりセキュリティ環境は大きく改善され、一定の成果を上げたものの、不正犯の巧妙化した新たな手口によるカード情報漏えいや、不正利用被害も発生し続けている。

このため、本協議会では引き続き「国際水準のセキュリティ環境」の整備とその維持を目標として、次の役割を担っていく必要があるため、存続させることが必要である。

#### (1) 安全・安心なクレジットカード利用環境整備のためのセキュリティ対策等（クレジットカード・セキュリティガイドライン）の取りまとめと公表

各関係事業者が取り組むべきセキュリティ対策等については、実行計画で明確に示してきたが、これらの対策を実行計画の期限経過後も、各関係事業者が最新の状態で維持し続ける必要がある。また、新たにクレジットカード取引を始める事業者についても、必要なセキュリティ対策を講じたうえで参入してもらう必要がある。このため、各関係事業者が講ずべきセキュリティ対策を「クレジットカード・セキュリティガイドライン」として策定し、対外的に周知するとともに、その維持・管理を行う。

また、同ガイドラインの取りまとめにあたっては、実行計画が割賦販売法に規定されるセキュリティ対策の実務上の指針であることから、引き続き同ガイドラインが法令上の実務上の指針としての役割を果たせるよう留意する。

#### (2) 最新のセキュリティ対策の情報収集と関係事業者間の共有

不正利用の手口は年々巧妙化しており、セキュリティ対策も手口の変化に対し適宜見直しや新たな対策の導入が求められることになる。そこで国際ブランド等の協力も得ながら、最新の不正利用の手口やセキュリティ対策の情報を収集し、関係事業者間で共有することでいち早く有効なセキュリティ対策が講じられるようにする必要がある。また、業界全体で取り組むべき事項が生じた場合には、ガイドライン等の見直しや追加等も行う。

#### (3) 関係者の協力体制の確立

本協議会は、クレジットカード取引の関係事業者とその業界団体及び消費者代表、行政などが広く参画し、互いに協力し合いながら実行計画の推進に取り組んでいる。セキュリティ対策や



その技術・運用指針等を最新の状態にし、社会の理解を得ながら推進していくためには、引き続き関係者の相互協力体制を維持していくことが必要である。

## **2. 主な取組事項**

本協議会が、「Ⅱ. 実行計画を踏まえたセキュリティ対策の課題とポスト 2020 における取組（7 頁を参照）」の内容を受けて 2020 年度以降当面取組むべき主な項目としては、次の 4 項目が挙げられる。

### **（1）非対面不正利用への対策**

非対面取引については不正利用被害額が高止まりの状況にあり、特に EC 加盟店に不正利用被害が集中している。EC 加盟店では一定の対策が講じられているにもかかわらず不正利用被害を防ぎきれない場合等もあり、運用面も含めたセキュリティ対策の検証を行うとともに、より実効性のある対策の検討と関係事業者による対策の実施が求められる。

### **（2）関係事業者におけるカード情報保護対策の推進の加速化及び維持管理**

カード情報を窃取しようとする者は、セキュリティ対策の対応が遅れている事業者の脆弱性を狙って攻撃を仕掛けてくることから、未対応先に対しては早急に対応するよう推進を加速する必要がある。なお、新たに市場に参入してくる事業者についても、必要なセキュリティ対策を講じたうえで参入するよう働きかけを行う。また、既に対策を導入した事業者についても、導入した対策が常に効力を発揮できるよう対策の維持・管理に取組む必要がある。

さらに、クレジットカード決済に関わる事業者のウェブサイト構築上の脆弱性を狙った漏えい事案に対しても、関係事業者による適切な対応が求められる。

### **（3）新たな決済サービス等におけるセキュリティ対策**

コード決済サービス等のクレジットカードを紐づけた新たな決済サービスにおいて、不正利用被害が発生したことを踏まえ、キャッシュレス推進協議会の対策も踏まえ対応策を検討し、それぞれの関係事業者が防止に向けた対応策を実施する。

また、PSP やコード決済サービス事業者、EC モール事業者、さらには、それらの事業者から委託を受けて大量のクレジットカード番号等を取り扱う事業者におけるカード情報保護の対応が求められる。

### **（4）実効性のある消費者啓発の実施**

関係事業者が実施するセキュリティ対策の実効性を確保するためには、IC 取引における PIN 入力や 3-D セキュアの認証情報の入力等、カード会員の協力が必要なものや、近年増加しているフィッシングのように消費者を直接狙った手口への自衛のために求められる行動などについて周知・啓発を行う必要がある。

### **3. 本協議会の委員構成及び検討のための組織体制**

#### **(1) 委員の見直し**

新たな決済サービス事業者など、本協議会において、ともにセキュリティ対策を講ずべき関係者の範囲を広げていくことを視野に、実務の実態に合わせ実効性をもって検討、実施ができるよう委員の見直しを図る必要がある。

#### **(2) 取組課題に応じた組織体制の再構築**

##### **①本会議**

本協議会の本会議は、「(1) 委員の見直し等」を行ったうえで、これまでと同様に本協議会の意思決定機関としての役割を果たすこととする。

##### **②ワーキング等**

これまでのワーキンググループでは、「カード情報の保護 (WG1)」「対面取引の不正利用防止 (WG2)」「非対面取引の不正利用防止 (WG3)」というそれぞれの分野ごとに講ずべきセキュリティ対策について検討を行ってきた。このうち、「カード情報の保護」及び「対面取引の不正利用防止 (カードの偽造防止)」については、これまでのワーキンググループの検討により、実施すべきセキュリティ対策及びその導入手法が確定していることから、これらの対策を推進しつつ、維持管理に力点を置いた活動を展開するためのワーキングとして改組する。

また、コード決済サービス等クレジットカードが紐付く新たな決済サービスのセキュリティ対策について、幅広い検討が行われることが想定されることから、新しいワーキンググループを設置する。

さらに、これまで協議会で策定してきた技術的な指針等を適宜最新化するための見直しを行う専門家を中心とした新しいグループを設置する。

具体的には「2. 主な取組事項」に記載した取組むべき主な項目を踏まえ、次のワーキンググループ等を新たに設置し、既存の3つのワーキンググループは解散する。

##### **1) セキュリティ対策推進ワーキンググループ**

カード情報保護及び対面取引の不正利用防止におけるセキュリティ対策の推進と導入先における対策の維持管理に関する事項について対応する。

##### **2) 非対面不正対応ワーキンググループ**

非対面取引の不正利用対策の推進とさらなる実効性のある対策の検討と実施について対応する。

##### **3) 新型決済対応ワーキンググループ**

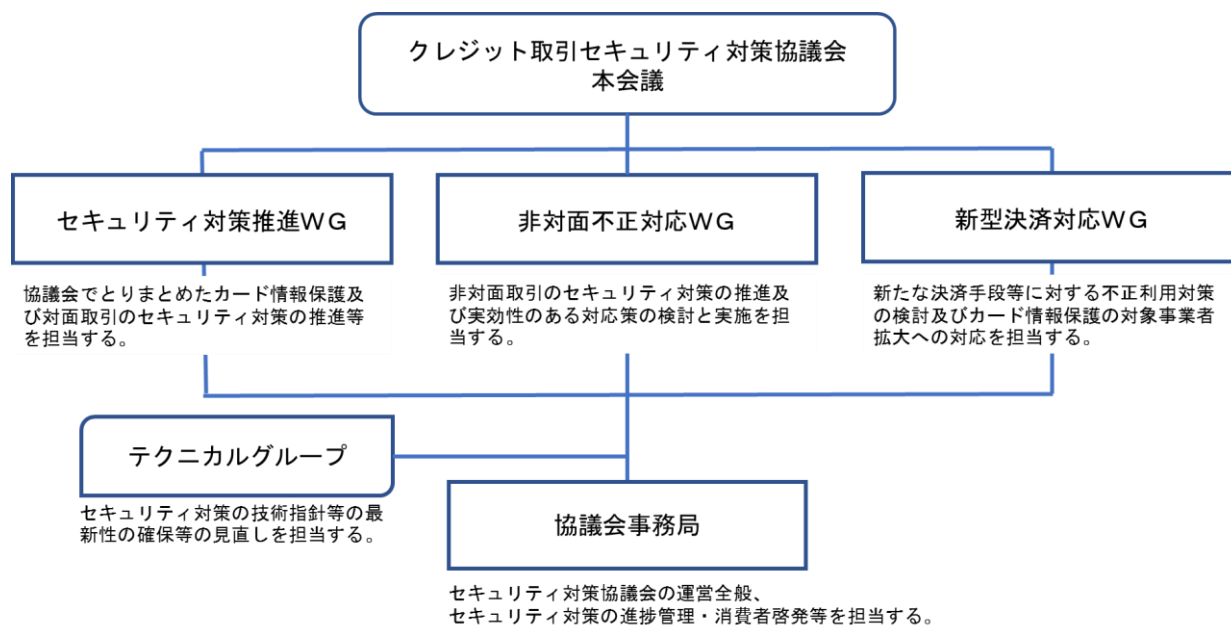
コード決済等クレジットカードが紐付く新たな決済サービスの不正利用対策の検討と、カード情報保護の対象事業者拡大への対応について検討する。

##### **4) テクニカルグループ**

セキュリティ対策の技術面、運用面の指針等について、最新性を確保するための見直し等を行う。ワーキンググループで取りまとめたセキュリティ対策に基づき技術面、運用

面からの検討を機動的に行うため、専門家と事務局によるグループを目的に応じて設置する。

【図表 11】協議会の組織体制



以上