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-2019-
概要版

【2019年3月1日】

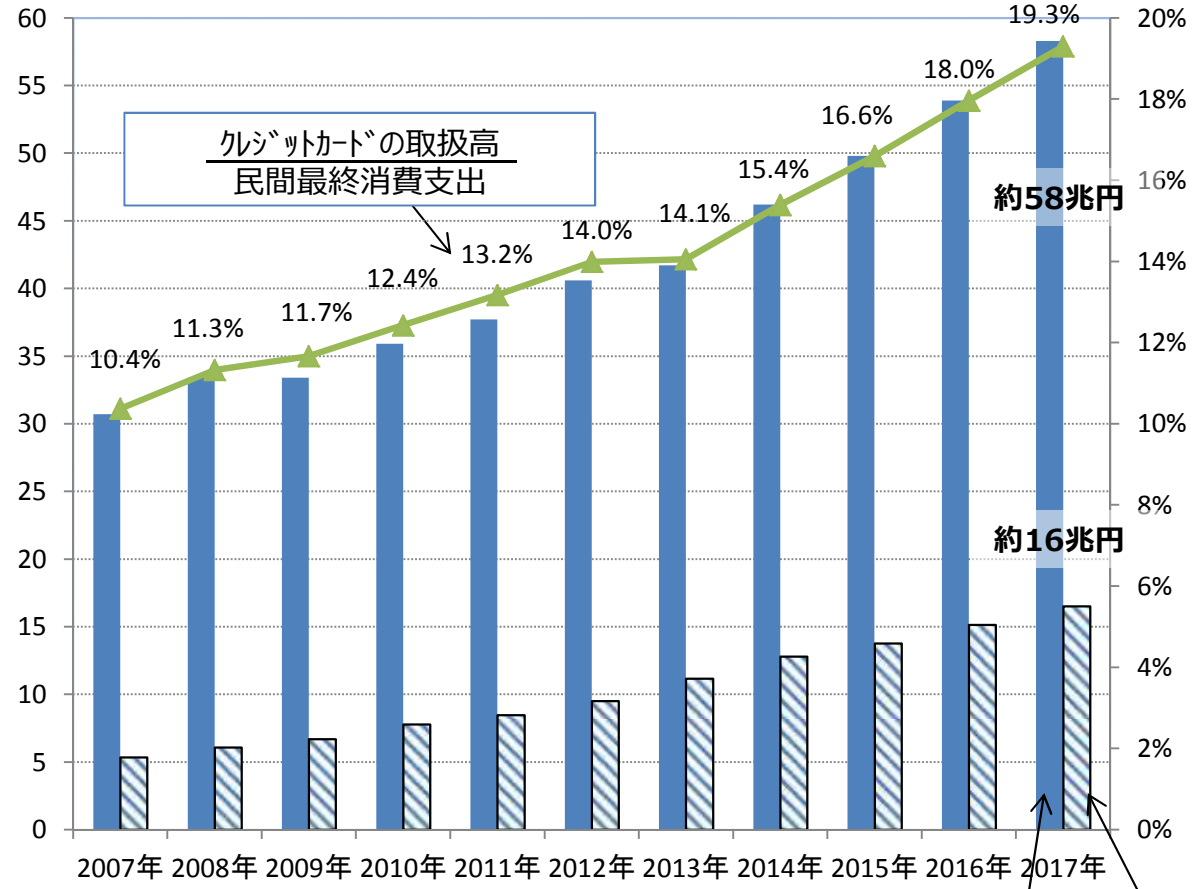
クレジット取引セキュリティ対策協議会
（事務局　一般社団法人日本クレジット協会）

はじめに

1-1. ネット取引の拡大とクレジットカード利用の増加

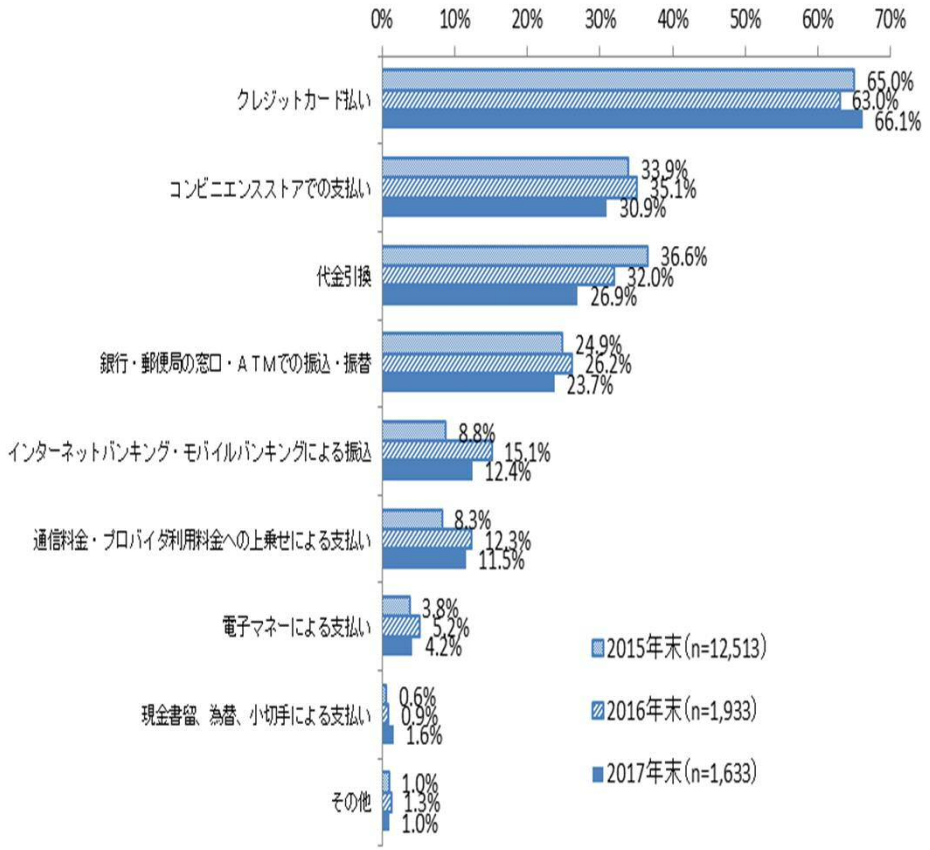
- 近年、電子商取引（EC）の拡大に伴い、**クレジットカードの取扱高は一貫して増加。**
- 2017年のクレジットカード取扱高は**約58兆円**で民間最終消費支出の**約19%**を占める。

消費に占めるクレジットカード取引とネット取引



（出所）
・内閣府「国民経済計算年報」 民間最終消費支出：名目（2017年は速報値）
・日本クレジット協会調査
（注）2012年までは加盟クレジット会社へのアンケート調査結果を基にした推計値、
2013年以降は指定信用情報機関に登録されている実数値を使用。
・Eコマース市場規模（BtoC）は経済産業省「電子商取引に関する市場調査」を使用。

インターネットで購入・取引する場合の決済方法の推移



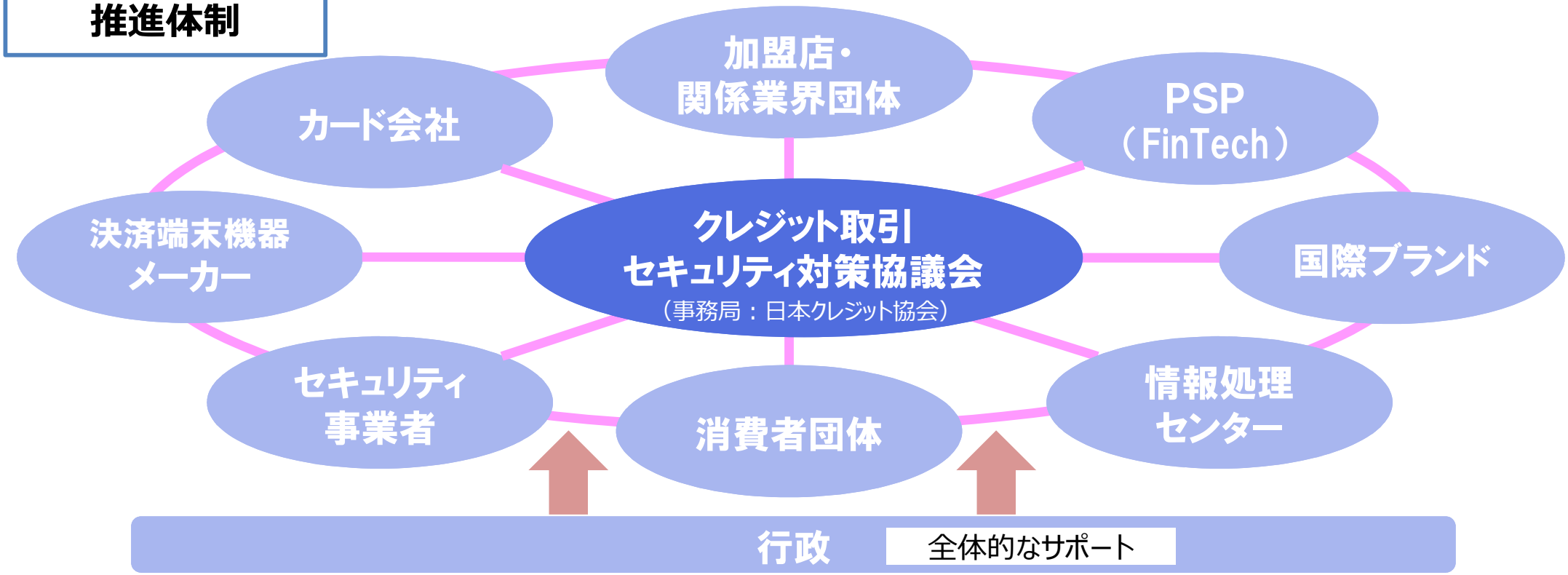
(注)15歳以上のインターネットでの購入経験者に占める割合

（出所）総務省「平成29年通信利用動向調査報告書（世帯編）」

1-2. クレジット取引セキュリティ対策協議会

- 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、クレジット取引に関わる**幅広い事業者及び行政が参画**して設立（2015年3月）。
- 本協議会では、**対策、期限、各主体の役割、当面の重点取組**等をとりまとめた**「実行計画」**（初版は2016年2月）を策定し、毎年度、実行計画の進捗を踏まえ、**改訂を行っている**（日本クレジット協会（事務局）を中心に、「実行計画」の推進体制を構築）。
- 実行計画を推進することで、**2020年3月末までに不正利用被害額の極小化を目指し**、我が国のキャッシュレス社会の**安全・安心なクレジットカード利用環境の実現**を図る。

推進体制



1-3．協議会　本会議メンバー

【カード事業者】 イオンクレジットサービス、オリエントコーポレーション、クレディセゾン、ジェーシービー、ジャックス
セディナ、トヨタファイナンス、三井住友カード、三菱UFJニコス、ユーシーカード、楽天カード
【決済代行業者（PSP）】 EC決済協議会
【加盟店】 オルビス、JTB、Ｊ.フロントリテイリング、三越伊勢丹ＨＤ、ヤフー、ユニー、ヨドバシカメラ、楽天
【情報処理センター】 NTTデータ
【決済端末機器メーカー】 NECプラットフォームズ、オムロンソーシアルソリューションズ
【セキュリティ事業者】 トレンドマイクロ、P.C.F. FRONTEO
【消費者団体】 全国消費者団体連絡会
【学識経験者】 笠井修・中央大学法科大学院教授（本会議議長）、田中良明・早稲田大学教授
【オブサーバー】
（国際ブランド） アメリカン・エキスプレス・インターナショナル、ビザ・ワールドワイド・ジャパン、
マスターカード・ジャパン、三井住友トラストクラブ[Diners Club]、
UnionPay International Co.,Ltd[銀聯]
（団体事務局） 日本チェーンストア協会、日本通信販売協会、日本百貨店協会
（官庁） 経済産業省

Ⅰ．基本的な考え方

2．クレジットカード取引における不正利用被害の実態等①

- 昨今、**情報漏えい対策が不十分な加盟店等を狙った不正アクセス**により、**カード情報の漏えい被害が拡大。**
- これに伴い、窃取したカード情報を使って、偽造カードや本人になりすました**不正利用による被害は増加。**（2017年**236.4億円**と5年間で約3.5倍）
- 不正利用は国境を越えて行われ、換金性の高い商品の購入を通じて、犯罪組織に多額の資金が流出しているとの指摘あり。

クレジットカード取引での被害イメージ

ハッカー

不正アクセス

対面加盟店

被害②

磁気ストライプでの決済
↓
偽造カード不正利用被害

不正利用者

被害①

情報漏えい対策が不十分
↓
カード情報の漏えい被害

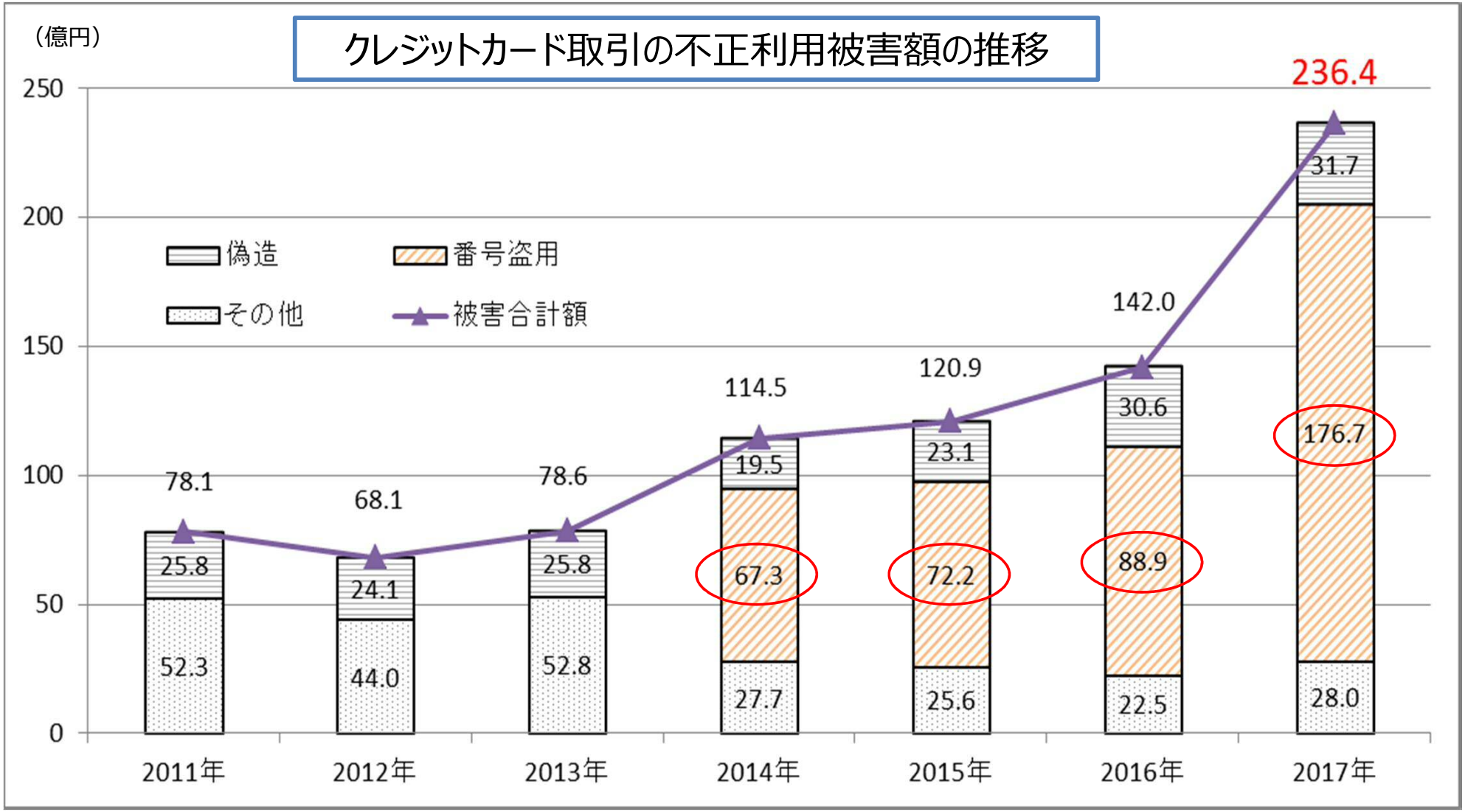
EC加盟店

被害③

本人確認なし
↓
なりすまし不正利用被害

2．クレジットカード取引における不正利用被害の実態等②

- 近年、**番号盗用**による不正利用被害額が増加傾向にある。



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」
（注）不正利用被害額は、国内発行クレジットカードでの不正利用分で、カード会社が把握している分を集計（海外発行カード分は含まれない）。
2013年調査までは「その他」に「番号盗用」を含む。

３．セキュリティ対策の強化に向けた基本的な考え方①

（１）「実行計画」の位置付け

改正割賦販売法

❶クレジットカード番号等の適切な管理
（改正法第35条の16第1項）
❷クレジットカード番号等の不正利用の防止
（改正法第35条の17の15）
のために必要な措置

必要な措置とは何か？

実行計画は実務上の指針

「実行計画」に掲げる措置
又はそれと同等以上

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

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

以上の観点から、本実行計画を指針とした取組を着実に進めていく必要がある。

※1 「クレジットカード番号等取扱契約締結事業者」（改正割賦販売法第35条の17の2）のこと
※2 改正割賦販売法においては、クレジットカード番号等の適切な管理についてはカード会社（イシュアー）、カード会社（アクワイアラー）等及び加盟店に課された義務であり、不正利用の防止については加盟店に課された義務である

３．セキュリティ対策の強化に向けた基本的な考え方②

（２）不正利用リスクに応じたセキュリティ対策の実施

- 実行計画では、**不正利用リスクに応じたセキュリティ対策**を求めている。
- 加盟店については、取引形態、取扱商材等によって不正利用リスクは異なるため、対策の実施にあたり留意すべきである。

□国際ブランド付きのクレジットカード

世界中で共通に使用できるため不正利用リスクが高い。

⇒実行計画では、**国際ブランド付きのクレジットカード**を**対象**としている。

□国際ブランドが付いていないクレジットカード

使用範囲が限定されるため国際ブランド付きのクレジットカードよりは不正利用リスクは低い。

⇒実行計画では、**国際ブランドが付いていないクレジットカード**は**対象とはしていない。**
しかしながら、**リスクに応じたカード情報保護対策**及び**不正利用対策**が**必要**となる点に留意する。

３．セキュリティ対策の強化に向けた基本的な考え方③

（３）セキュリティ対策の検証と改善

- セキュリティに係る方策は100%の安全性を担保するものではないという認識に立つ。

⇒ **リスクに応じた多面的・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。

（４）加盟店に対する情報提供等

- カード会社（アクワイアラー）・PSP、加盟店間の相互連携が重要。

⇒ 加盟店における対策の導入にあたり、契約関係にあるカード会社（アクワイアラー）やPSPは**加盟店に対するサポートを行い**、加盟店は契約関係にあるカード会社（アクワイアラー）等に対し**必要な情報提供を求める**。

（５）消費者に対する情報発信

- 消費者自身のクレジットカードの不正利用に対する認知・意識の向上を図る。

⇒ **消費者に対する情報発信**によって**セキュリティ対策に係る理解・協力**を得る。

Ⅱ．分野別の具体的な実行計画

４．分野別の具体的な実行計画

■「実行計画」における対策の３本柱

A. クレジットカード情報保護対策

◇カード情報を盗らせない

- 加盟店におけるカード情報の「非保持化」
- カード情報を保持する事業者のPCI DSS準拠

B. クレジットカード偽造防止による不正利用対策

◇偽造カードを使わせない

- クレジットカードの「100%IC化」の実現
- 決済端末の「100%IC対応」の実現

C. 非対面取引におけるクレジットカードの不正利用対策

◇なりすましをさせない

- リスクに応じた多面的・重層的な不正利用対策の導入

A. クレジットカード情報保護対策

5-1. クレジットカード情報保護対策

現 状 ・ 課 題

- 改正割販法の施行により、カード会社のみならず、加盟店にもカード情報保護対策が義務化
- ECサイト改ざん・偽画面への誘導など、不正犯の巧妙化した新たな攻撃手口による被害発生

対　策

○ 加盟店は**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準拠**

非保持化: 自社で保有する機器・ネットワークにおいて、保存、処理、通過しないこと

○ カード情報を保持する事業者は**PCI DSS準拠**

○ 新たな脅威への警戒と**セキュリティ対策への継続的な取組**

各主体の役割・取組

カード会社・PSP

・**PCI DSS準拠の維持・運用**
・PCI DSS未準拠のPSPとの取引を見直し
・加盟店に対し、非保持化（非保持と同等/相当を含む）又はPCI DSS準拠完了を推進

加盟店

・カード情報の**非保持化（非保持と同等/相当を含む）が基本**（又は**PCI DSS準拠**）
・非保持化実現加盟店についても、**自社システムの定期的な点検やその結果に基づく追加的な対策が重要**
・**最新の攻撃手口に対応したセキュリティ対策の改善・強化を不断に実施**

業界団体等

・アクワイアラーと連携し、加盟店にカード情報保護対策の必要性の周知を徹底、業界団体や消費者団体等との連携を強化し事業者や消費者に情報発信
・カード会社やPSP、加盟店業界団体の加盟店の非保持化実現への取組をサポート

【注１】カード情報について

クレジットカード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）及び機密認証データ（カード情報を含む全トラックデータ、CAV2/CVC2/CVV2/CIDいわゆるセキュリティコード、PIN又はPINブロック）をいう。ただし、クレジットカード会員データのうち、クレジットカード番号以外のデータのみであれば「カード情報」ではない。また、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**。

①**トークナイゼーション**（自社システムの外でクレジットカード番号を不可逆的に別の番号等に置き換え、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）
②**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）
③**無効処理されたクレジットカード番号**

【注２】カード情報の保持とならない例について

本実行計画において、以下においてカード情報を保存する場合には、**「保持」にはならない**。

①紙（クレジット取引伝票、カード番号を記したFAX、申込書、メモ等）
②紙媒体をスキャンした画像データ
③電話での通話（通話データを含む）

※1 ①～③以外において**非保持化（非保持と同等/相当を含む）が実現されていることが前提**
※2 PCI DSS準拠を目指す加盟店においては、本実行計画の内容にかかわらず、PCI DSSに則って取組むことに留意する必要がある

5-2. 加盟店におけるカード情報保護対策

□加盟店における対策（指針）一覧

（いずれの対策（指針）を選択するかは各事業者に委ねられる）

形 態		対策（指針）	
		外回り(非通過型) 自社で保有する機器・ネットワークにカード情報を「保存」「処理」「通過」しない方式	**内回り(通過型)** 自社で保有する機器・ネットワークにカード情報を「保存」「処理」「通過」する方式
非対面加盟店	EC加盟店	非保持化※	PCI DSS準拠
	メールオーダー・テレフォンオーダー(MO・TO)加盟店	非保持化※	非保持と同等/相当※　又は　PCI DSS準拠
対面加盟店		非保持化※	非保持と同等/相当※　又は　PCI DSS準拠

※非保持化 又は 非保持と同等/相当を実現した場合でも、事業者の選択によりPCI DSSに準拠することを否定しない

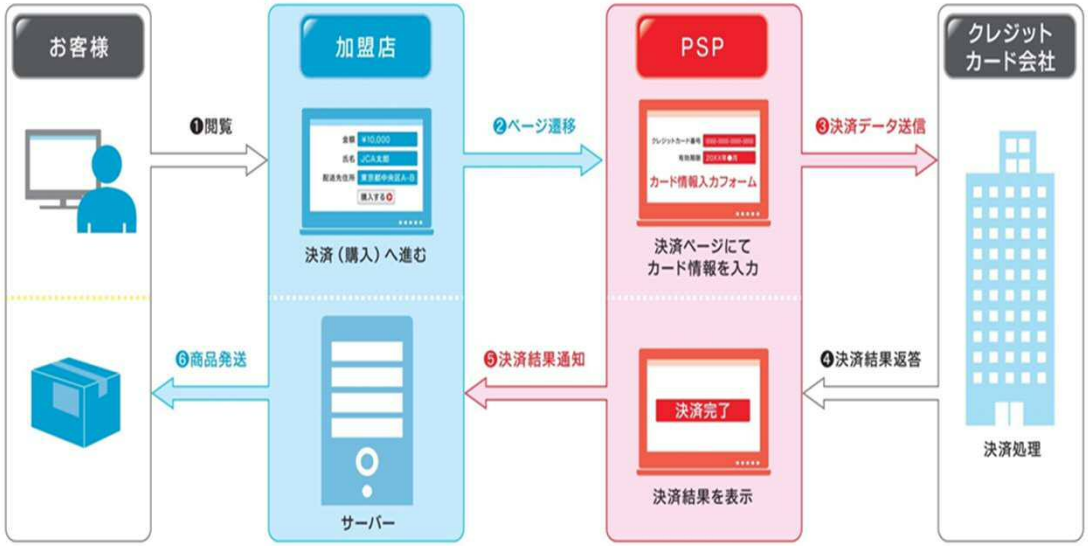
5-3．非対面加盟店における非保持化・非保持と同等/相当①

- 非対面加盟店における非保持化の推進は、不正アクセスによる外部への情報漏えい被害の極小化に有効。
- 本実行計画において例示する方式により、非保持化の実現が可能である。また、PCI DSSに準拠した外部委託先が提供するカード情報保護対策ソリューションを活用し、非保持化を実現することも有効な対策となり得る。

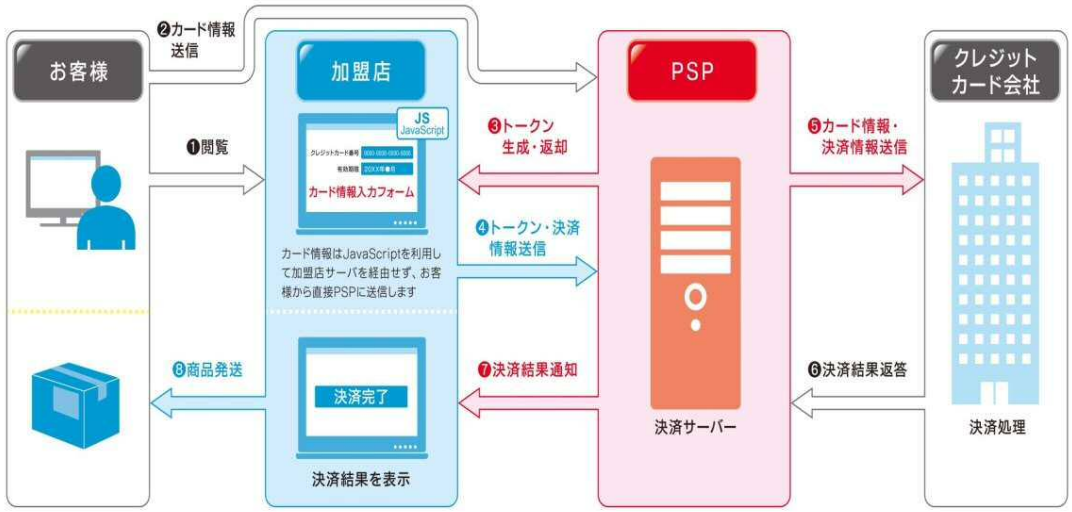
（1）EC加盟店における非保持化を実現するセキュリティ措置

◆非保持化：非通過型（「リダイレクト（リンク）型」又は「Java Script型（トークン型）」）の決済システムの導入

➢非通過型（リダイレクト（リンク）型）



➢非通過型（Java Script型（トークン型））



※トークンは、クレジットカード情報を代替するパラメータです。加盟店はお客様がPSPに送信したカード情報を元に生成されたトークンを利用して決済を行います。

近時のカード情報漏えい事案を踏まえ、以下に対するセキュリティレベルの向上が重要

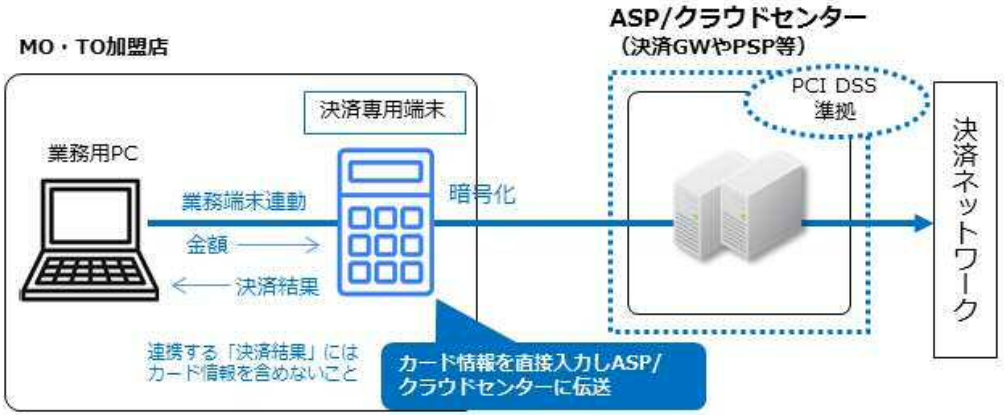
- ECサイトの脆弱性や設定の不備
- 委託先事業者が提供する決済ソリューション（ショッピングカート機能等）の脆弱性等
- ウェブサイト開発・運用段階での不十分なセキュリティ対応
- ECサイトの改ざん、偽画面への誘導など不正犯の巧妙化した新たな攻撃手口

5-3．非対面加盟店における非保持化・非保持と同等/相当②

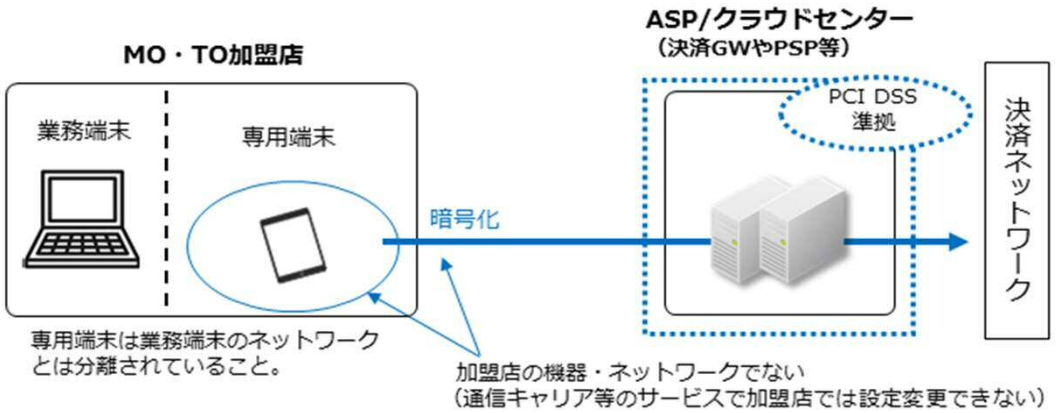
（2）MO・TO加盟店における非保持化又は非保持と同等/相当を実現するセキュリティ措置※

◆非保持化：要件を満たした決済専用端末やタブレット端末を活用した外回り方式の導入

➢外回り方式（決済専用端末を利用した方式）

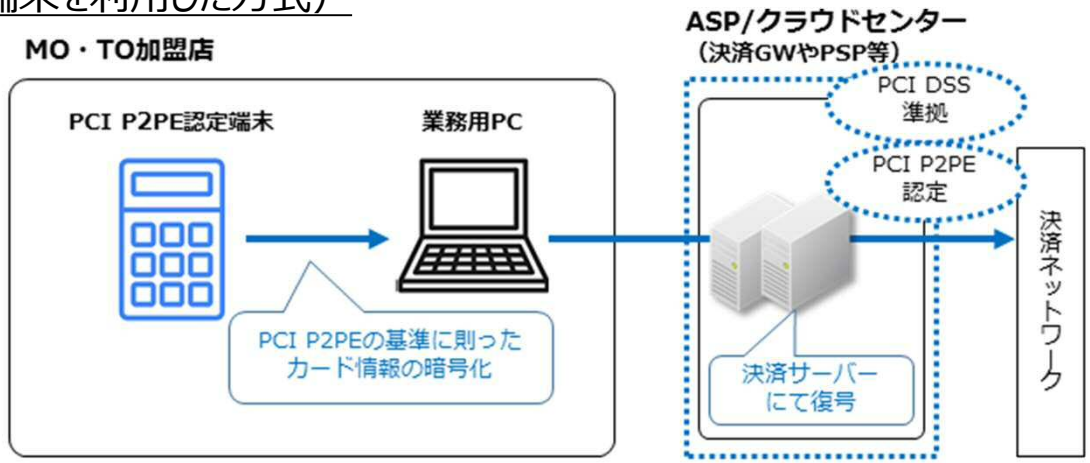


➢外回り方式（タブレット端末を利用した方式）



◆非保持と同等/相当：PCI P2PE認定ソリューションの導入

➢内回り方式（PCI P2PE認定端末を利用した方式）



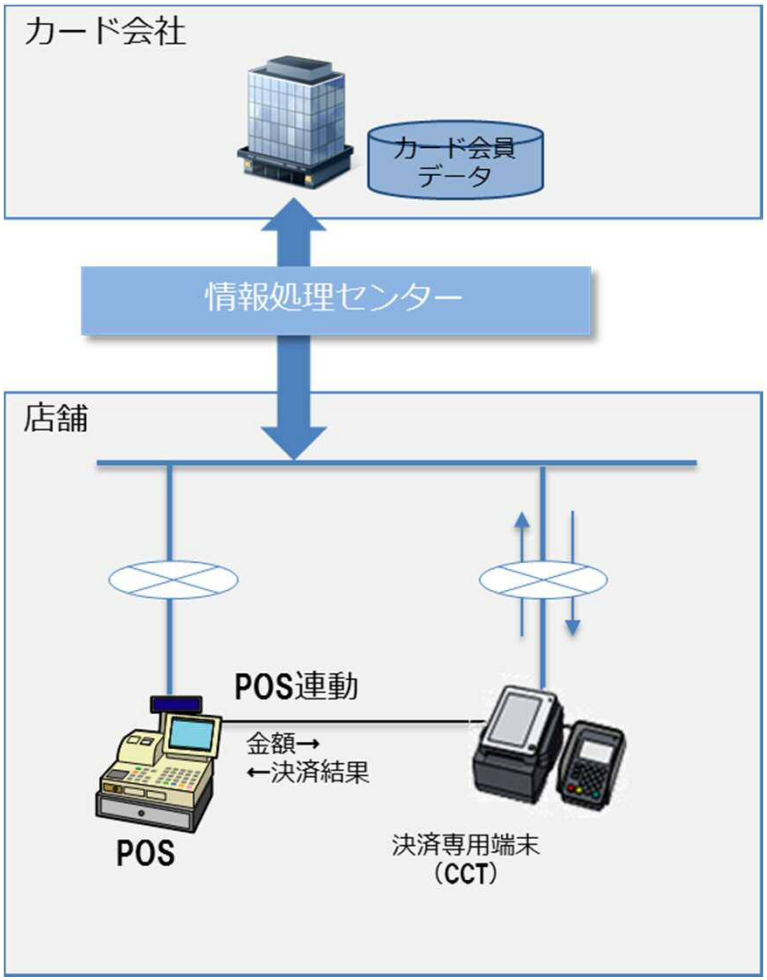
※これら非保持化、非保持と同等/相当の詳細については、「【追補版】メールオーダー・テレフォンオーダー加盟店における非保持化ソリューションについて」を参照

5-4. 対面加盟店における非保持化・非保持と同等/相当①

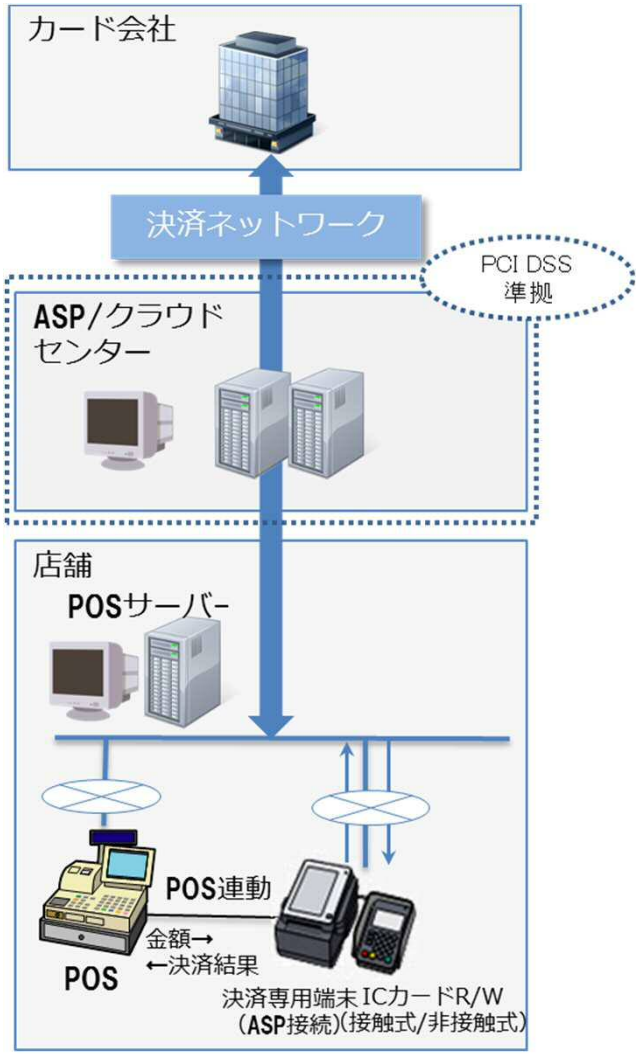
(1)対面加盟店における非保持化を実現するセキュリティ措置

◆非保持化：決済専用端末から直接外部の情報処理センター又はASP/クラウドセンター等に伝送される方式
POSに連動する決済結果には「カード情報」は含めないことが前提

➢決済専用端末（CCT）連動型（外回り）



➢ASP/クラウド型（外回り）

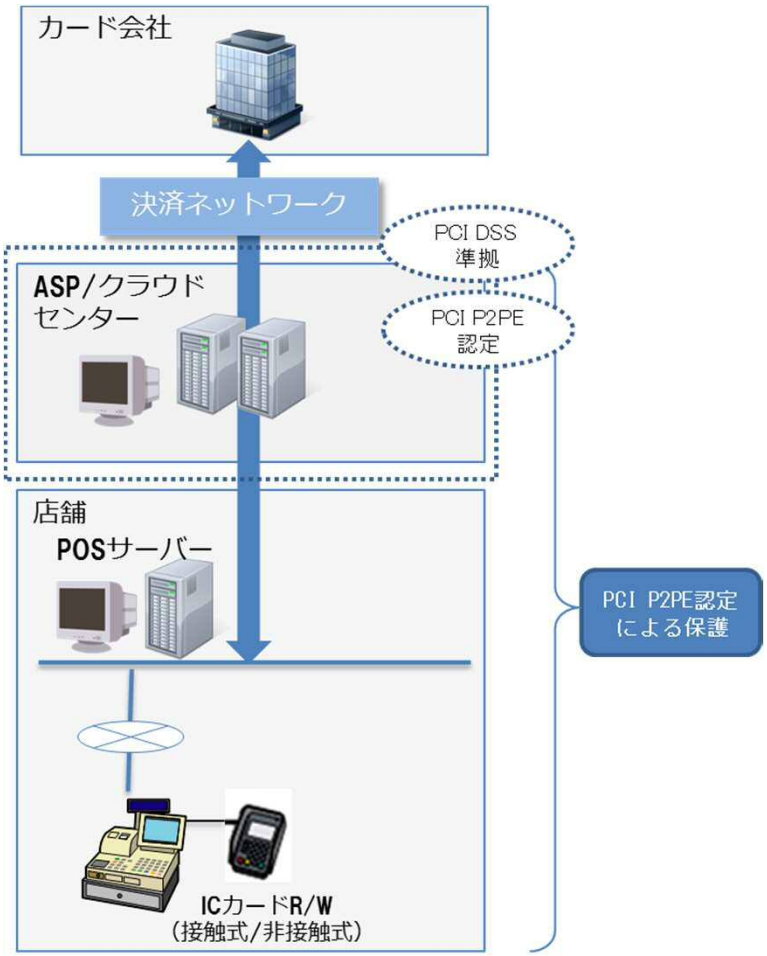


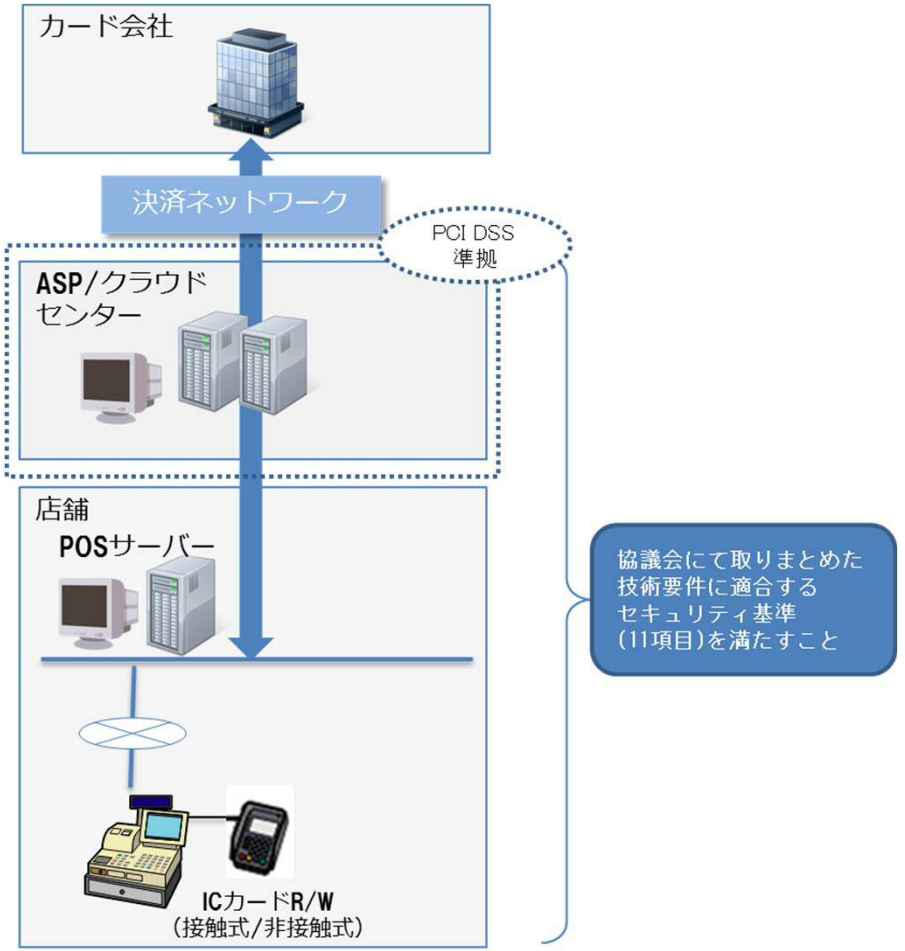
5-4．対面加盟店における非保持化・非保持と同等/相当②

（2）対面加盟店における非保持と同等/相当を実現するセキュリティ措置

◆非保持と同等/相当：PCI P2PE認定ソリューションの導入又は本協議会において取りまとめた技術要件に適合するセキュリティ基準（11項目）※を満たすこと

➢ASP/クラウド接続型（内回り）





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

5-5．非保持化実現加盟店における留意点

□非保持化を実現した加盟店における情報漏えい防止対策

非保持化実現後も以下の情報漏えい防止のための継続的なセキュリティ対策が求められる。
・情報保護に関する従業員教育
・ウィルス対策
・デバイス管理　等

□非保持化を実現した加盟店における顧客対応

顧客照会等の際、以下を利用して一時的にクレジットカード番号を入手・利用することが認められる。
①クレジットカード取引にかかる紙伝票（加盟店控え、お客様控え）等の紙媒体
②紙媒体をスキャンした画像データ
③電話での通話（通話データを含む）
④PCI DSSに準拠したASP事業者が提供するセキュリティ対策が施された環境へのアクセスによる照会
※運用上の課題については各加盟店、カード会社、必要に応じてASP事業者等が連携し、個別に検討すること

□非保持化を実現した加盟店における過去のカード情報保護対策

過去のカード情報が以下要件を全て満たす場合、当該カード情報をテキスト形式等の電子帳簿として保存することが認められる。
①電子帳簿保存法に基づく管理を求められている
②非保持化対応完了以前に取り扱った過去のカード情報である
③本協議会にて定めたセキュリティ対策※が行われている
※ネットワークを利用しない「スタンドアローン環境」で保管・利用することが必須条件。詳細については、「非保持化実現加盟店における過去のカード情報保護対策」を参照

5-6．PCI DSS準拠推進/カード情報漏えい時対応

□PCI DSS準拠の推進について

本協議会は、日本カード情報セキュリティ協議会等とともに、PCI DSSに関して以下の事項に取組む。
①セミナー開催等による周知・啓発活動の推進
②PCI DSS準拠に向けた加盟店等の取組をサポートするための体制構築

□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

業務上大量のカード情報を管理・利用するカード会社、PSP、その他事業者は、以下の取組が求められる。
①PCI DSS準拠
②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

□カード情報漏えい時の対応について

◆加盟店

・「クレジットカード情報漏えい時および漏えい懸念時の対応要領」を参考にしつつ、二次被害の防止に努めること。
・被害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、カード決済の一時停止等の措置及びPCI DSS準拠等再発防止のための適切な措置を講じること。

◆カード会社（アクワイアラー）等

・カード決済の再開については、再発防止のための措置等の対応状況を十分に確認すること。
・再発防止措置の内容は、当該加盟店と契約カード会社（アクワイアラー）等で協議の上で決定すること。

5-7．カード情報保護対策に関する附属文書一覧

No	文書名	目的・概要
1	「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」	メールオーダー・テレフォンオーダー（MO・TO）加盟店における「非保持化（非保持と同等/相当を含む）」の取組を推進するため、具体的な方策例について取りまとめたもの。
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」	内回り方式を採用する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実現するため求められる11の想定リスクに対応したセキュリティ対策措置（暗号化、アクセス制限等）を取りまとめたもの。
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」	電子帳簿保存法に基づき、過去のカード情報を含む電子帳簿について非保持化が困難な場合があることを踏まえ、「スタンドアローン環境」での保管・利用などの措置内容を取りまとめたもの。

Ｂ．クレジットカード偽造防止による不正利用対策

6-1. クレジットカード偽造防止による不正利用対策

現 状 ・ 課 題

- **偽造カードによる不正利用**に対し、IC取引の実現は、現状では**唯一無二**の対策
- 海外でのIC対応が進む中、国内加盟店のPOSシステムのIC対応が進んでおらず、「**セキュリティホール化**」するリスクが高まっている

対　策

○ **クレジットカードの100%IC化**及び**加盟店の決済端末の100%IC対応**

各主体の役割・取組

カード会社

・2020年3月末までの**クレジットカードの100%IC化**の実現
・消費者へのPIN認知
・加盟店へのIC対応に向けた必要な情報提供（ガイドライン等）

加盟店

・POS等の**決済システムのIC対応**（最終的には2020年3月までに完了）

業界団体等

・**消費者への周知活動**（IC取引の安全性、PIN認知度の向上等）
・**IC加盟店の「見える化」の取組**

低コスト化等の支援

国際ブランド

・協議会との調整
・制定ルール推進に向けた協業した取組

POS機器メーカー

・IC対応推進のため加盟店へ必要な情報の提供
・POSシステムの**IC対応を標準化**

6-2. IC取引における本人確認方法

◆接触IC取引

・ 本人確認は原則、「オフラインPIN（Personal Identification Number、暗証番号のこと）」とする 。

◆非接触IC取引

・ CVMリミット金額（本人確認不要上限金額）以下は、本人確認不要とする。
・ CVMリミット金額超は、次のとおりとする。
　1）モバイル型等での取引では、原則Consumer Device CVM（モバイルPIN/指紋等）とする。
　2）カード型等での取引では、原則、接触IC取引のオフラインPIN入力とする。ただし、オフラインPIN機能環境に対応できない、カード型等での取引でサインを要求する場合 、これを許容する。

IC取引方法		CVMリミット	本人確認方法
接触IC		CVMリミット以下	不要
		CVMリミット超	**PIN** （サインを許容※1）
非接触IC取引	モバイル型等	CVMリミット以下	不要
		CVMリミット超	**Consumer Device CVM** **（モバイルPIN/指紋等）**
	カード型等	CVMリミット以下	不要
		CVMリミット超	**接触ICへ切替（PIN）** （切替不可の場合、サインを許容※2）

※1：一部の海外発行カードでは、オフラインPIN環境では利用を許容しないカードが存在するため
※2：接触IC取引への切替を許容しないカードが存在するため

【注意事項】 本人確認不要加盟店では、紛失・盗難対策の観点から、接触IC取引は全件オーソリゼーションを必須とする。

6-3. IC取引に関する附属文書一覧

No	文書名	目的・概要
1	「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」	国内のガソリンスタンドにおける商慣習上の制約を考慮し、2020年3月までのIC対応に向けて、実現可能な代替策を取りまとめたもの。
2	「オートローディング式自動精算機のIC化対応指針と自動精算機の本人確認方法について」	オートローディング式自動精算機の国際的なセキュリティ準拠が技術的に困難なことから、2020年3月までに実現可能な自動精算機のIC対応とそれに伴うセキュリティリスク及び代替コントロール策を示したもの。
3	「ICカード対応POSガイドライン」	接触IC取引を対象としたPOS加盟店でのIC対応を円滑に進める具体的な方策として策定したもの。
4	「非接触EMV対応POSガイドライン」	今後の非接触EMV決済の普及、及び接触型と非接触型のPOS端末の同時導入を志向するニーズに応えるために策定したもの。
5	「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」	IC取引時のオペレーションルールとして、国内加盟店でのIC取引における本人確認方法の業界統一的な考え方を示すとともに、加盟店の円滑なIC対応に資するよう取りまとめたもの。

6-4. 加盟店におけるIC対応の取組支援

□接続インターフェース等の共通化・標準化

- 各種端末（CCT、IC-PINパッド、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、汎用的なPOS搭載ミドルウェアの使用
  ⇒ POS改修コストの低減化、対応期間の短縮化が可能

□POSシステムのIC対応標準化

- 今後開発・製造するクレジット機能を有するPOSシステム
  ⇒IC対応可能なシステムを標準化

□国際ブランドテストの効率化

- 加盟店の負担となる国際ブランドのテストコスト低減化と導入までの期間の短縮化、端末(ハード/ミドルウェア)やサーバー等ごとの国際ブランドテストの効率化

＜主な取組事項＞

・ネットワーク会社によるブランドテストの実施枠の拡張等

・国際ブランドテストの要否一覧の整理（シナリオ・パターンを明確化）
  ⇒「ICカード対応POSガイドライン」への反映

※詳細については、契約先のカード会社(アクワイアラー)やPOS機器メーカー等に照会のこと

C. 非対面取引におけるクレジットカードの不正利用対策

7-1. 非対面取引におけるクレジットカードの不正利用対策

現 状 ・ 課 題

- 近年、**ネット取引（EC）におけるなりすまし等による不正利用被害が急増**

※不正利用被害額（2017年236億円）の約3/4はECにおける不正利用に起因

対　策

○ **非対面加盟店(EC、MO・TO等)**において、**リスクに応じた多面的・重層的な不正利用対策**を導入

各主体の役割・取組

カード会社（イシュアー）

・オーソリモニタリングの検知精度向上・強化
・３Dセキュアのパスワード登録促進
・リスクベース認証導入の検討

カード会社（アクワイアラー）・PSP

・加盟店における不正利用対策の具体的方策の導入に向けた要請・支援

加盟店

・**各社の被害状況やリスクに応じ多面的・重層的な不正利用対策の具体的方策の導入**
・自社の課題解決、リスク低減等のため、アクワイアラー及びPSPとの情報共有に努める

業界団体等

・事業者等に対する、不正利用対策の必要性・有効性についての周知活動
・消費者に対するパスワード等の使い回し等についての注意喚起
・**不正の傾向調査、基準や方策の有効性の検証**

加盟店における不正利用対策の具体的方策

○本人認証（3Dｾｷｭｱ等）
消費者に特定のパスワードを入力させることで本人を確認

○券面認証(ｾｷｭﾘﾃｨｺｰﾄﾞ)
券面の数字を入力し、カードが真正であることを確認

○属性・行動分析(不正検知ｼｽﾃﾑ)
過去の取引情報等に基づくリスク評価によって不正取引を判定

○配送先情報
不正配送先情報の蓄積によって商品等の配送を事前に停止

7-2. 加盟店におけるリスク・被害発生状況に応じた方策の導入

□加盟店における方策導入の指針

- 非対面加盟店は、当該加盟店の取り扱う商材等に応じた不正利用の被害発生状況等を踏まえ、必要な対策を導入することが求められる（具体的な指針内容については以下参照）。

（１）「全ての非対面加盟店」

【定義】全ての非対面加盟店

【対策】カード取引に対する善管注意義務の履行、オーソリゼーション処理

（２）「高リスク商材取扱加盟店」

【定義】実行計画で定める４つの商材※１を主たる商材として取り扱う加盟店

【対策】実行計画の掲げる４方策の内、１方策以上

（３）「不正顕在化加盟店」

【定義】継続的に一定金額を超えた不正利用被害が発生している加盟店

【対策】実行計画の掲げる４方策の内、２方策以上※２

※１　デジタルコンテンツ(オンラインゲームを含む）、家電、電子マネー、チケット

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

【実行計画に掲げる４方策】

○本人認証（3Dｾｷｭｱ等）
消費者に特定のパスワードを入力させることで本人を確認

○券面認証(ｾｷｭﾘﾃｨｺｰﾄﾞ)
券面の数字を入力し、カードが真正であることを確認

○属性・行動分析(不正検知ｼｽﾃﾑ)
過去の取引情報等に基づくリスク評価によって不正取引を判定

○配送先情報
不正配送先情報の蓄積によって商品等の配送を事前に停止

7-3．不正利用対策の具体的な方策について①

□なりすまし等不正利用を防止するための４つの方策

- 不正利用を防止するための具体的な方策について、現状における主なものを以下のとおり整理。
- それぞれの方策には特徴があり、加盟店が取り扱う商材や販売手法に応じた有効な方策を講じることが重要。

（１）本人認証

①3Dセキュア

・カード会員のみが知るカード会社に事前に登録したパスワード等により利用者本人の取引を確認する手法（国際ブランドが推奨）

・パスワード等の入力を省略した結果、不正利用被害が発生しているため、3Dセキュア導入加盟店において本人認証が要求される対象取引全てに実施されることが重要

・「リスクベース認証」導入により、パスワード入力を求める取引を最小限にすることも期待可

②認証アシスト

・カードのオーソリゼーション電文を用い、カード会員の属性情報を送信し、カード会社に予め登録されている属性情報と照合し利用者本人の取引を確認する手法（カード会社と直接契約が必要）

（２）券面認証（セキュリティコード）

・カード券面のセキュリティコードを認証することにより真正なカードが利用されていることを確認する手法

・100%普及しており、パスワードのように利用者の失念懸念なし

・イシュアー側で、多数回連続アクセスに対して早期に検知し取引不成立とする対策が必要

7-3．不正利用対策の具体的な方策について②

□なりすまし等不正利用を防止するための４つの方策（続き）

（３）属性･行動分析（不正検知システム）

- 非対面でのカード利用時、購入者の入力情報、利用端末情報、IPアドレス、過去の取引情報、取引頻度等、加盟店が収集できる情報に基づいたリスク評価を行い、不正取引であるか否かを判定する手法
- 不正取引の手口や傾向の変化に基づき、不正判定の条件設定を更新・変更する機能を有することが必要であり、常に条件設定を最新化しておくことが望ましい
- 個々の取引を人的対応による判定ではなく、上記条件設定による自動判定が行われることが重要

（４）配送先情報

- 不正利用された注文等の配送先情報を蓄積し、取引成立後であっても商品等の配送を事前に止めることで不正利用被害を防止する手法
- 情報の蓄積には時間がかかることから、外部の実績のあるサービスの利用等が有効（現在、複数のカード会社が共同で運用しているサービスやシステムベンダーが提供するサービスが存在）

⇒ **各方策導入の参考とするため、「好事例」を取りまとめた（業界団体、アクワイアラーに配布）**

7-4. 非対面取引の不正利用対策に関する附属文書一覧

No	文書名	目的・概要
1	「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」	カード会社、決済代行会社、加盟店の協力を得て、実行計画に掲げる４つの不正利用防止方策を導入した際の不正抑止効果について好事例集として取りまとめたもの（2019年版）。
2	「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」	加盟店のリスクや被害発生の状況等に応じ、実行計画に掲げる４つの不正利用防止方策を導入する際の指針として、具体的な基準・考え方を取りまとめたもの。

Ⅲ．消費者及び事業者等への情報発信等について

８．消費者及び事業者等への情報発信①

（１）消費者向け周知活動

①加盟店におけるセキュリティ対策の「見える化」への取組

改正割賦販売法の附帯決議を踏まえ、消費者が加盟店のクレジットカード取引におけるセキュリティ対策を「見える化」できる方策の推進を図る。

- **ICクレジットカード対応済加盟店であることを示す共通シンボルマーク等掲出**

「IC対応」・「暗証番号の認知度向上」
共通シンボルマーク

「IC対応デザイン」

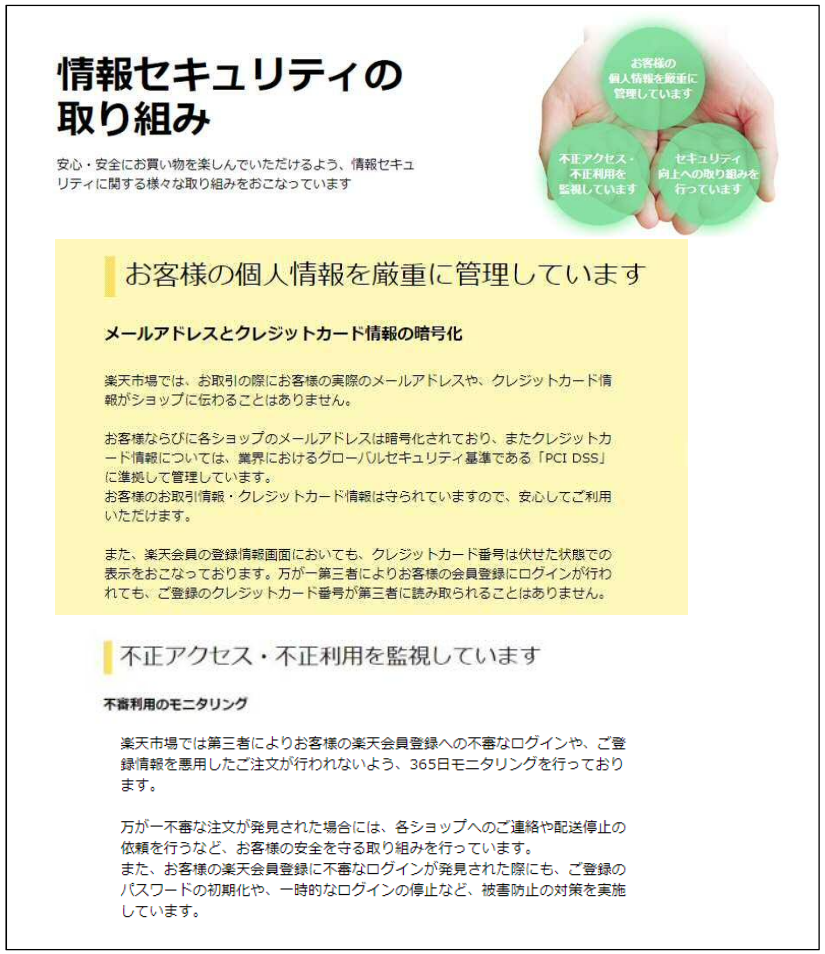
● クレジットカードのセキュリティ対策を講じたEC加盟店による自己宣言

EC加盟店が実行計画で求めるクレジットカードの情報保護対策及び不正利用対策を講じている場合には、自社ECサイトにおいて実行計画に取組んでいることを宣言。

（自己宣言：参考例）

『割賦販売法に基づき、クレジット取引セキュリティ対策協議会の定める実行計画に取り組んでおります。』

『割賦販売法に基づき、クレジットカード取引のセキュリティ対策に取り組んでおります。』



情報セキュリティの取り組み

安心・安全にお買い物を楽しんでいただけるよう、情報セキュリティに関する様々な取り組みをおこなっています

お客様の個人情報を厳重に管理しています

メールアドレスとクレジットカード情報の暗号化

楽天市場では、お取引の際にお客様の実際のメールアドレスや、クレジットカード情報がショップに伝わることはありません。

お客様ならびに各ショップのメールアドレスは暗号化されており、またクレジットカード情報については、業界におけるグローバルセキュリティ基準である「PCI DSS」に準拠して管理しています。
お客様のお取引情報・クレジットカード情報は守られていますので、安心してご利用いただけます。

また、楽天会員の登録情報画面においても、クレジットカード番号は伏せた状態での表示をおこなっております。万が一第三者によりお客様の会員登録にログインが行われても、ご登録のクレジットカード番号が第三者に読み取られることはありません。

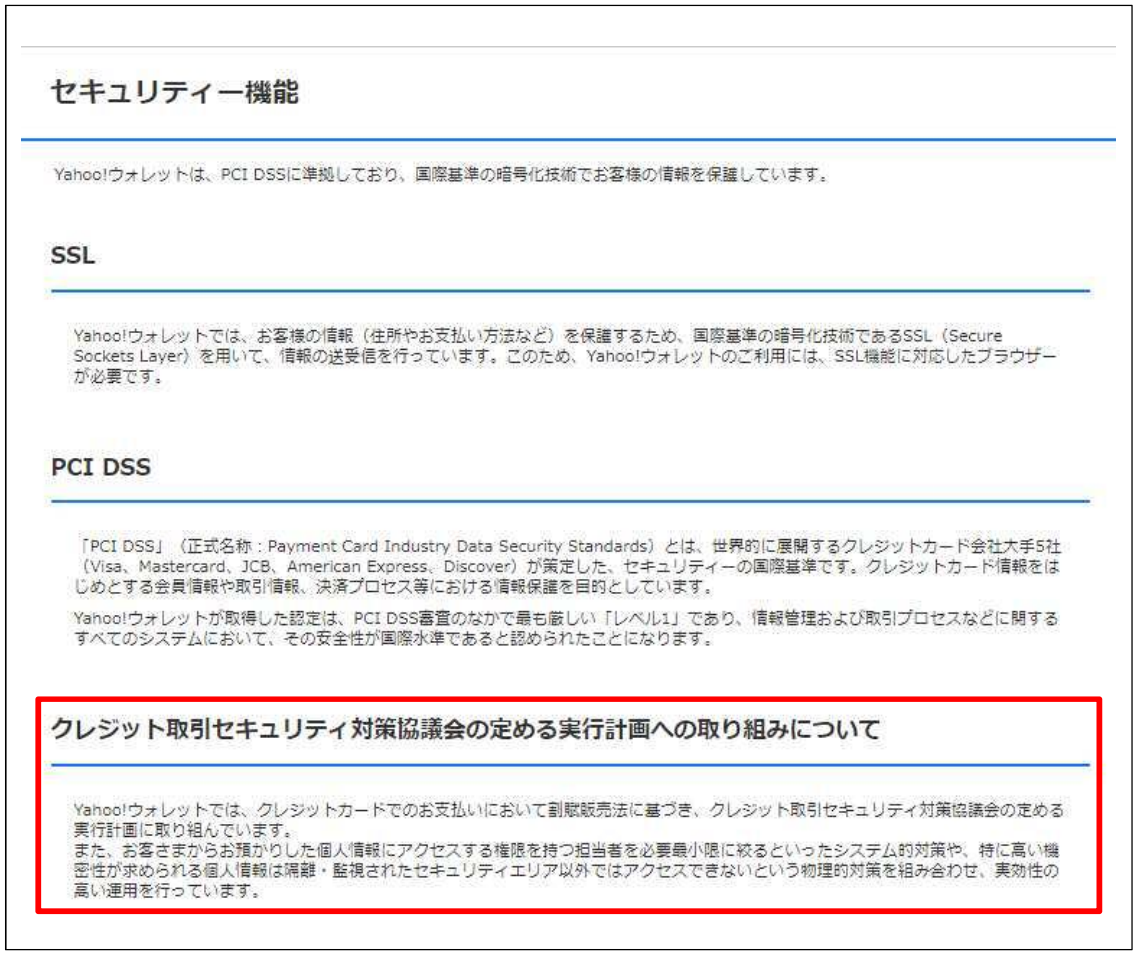
不正アクセス・不正利用を監視しています

不審利用のモニタリング

楽天市場では第三者によりお客様の楽天会員登録への不審なログインや、ご登録情報を悪用したご注文が行われないよう、365日モニタリングを行っております。

万が一不審な注文が発見された場合には、各ショップへのご連絡や配送停止の依頼を行うなど、お客様の安全を守る取り組みを行っています。
また、お客様の楽天会員登録に不審なログインが発見された際にも、ご登録のパスワードの初期化や、一時的なログインの停止など、被害防止の対策を実施しています。

2019年3月1日現在（URL　https://event.rakuten.co.jp/anshin/security）



セキュリティー機能

Yahoo!ウォレットは、PCI DSSに準拠しており、国際基準の暗号化技術でお客様の情報を保護しています。

SSL

Yahoo!ウォレットでは、お客様の情報（住所やお支払い方法など）を保護するため、国際基準の暗号化技術であるSSL（Secure Sockets Layer）を用いて、情報の送受信を行っています。このため、Yahoo!ウォレットのご利用には、SSL機能に対応したブラウザーが必要です。

PCI DSS

「PCI DSS」（正式名称：Payment Card Industry Data Security Standards）とは、世界的に展開するクレジットカード会社大手5社（Visa、Mastercard、JCB、American Express、Discover）が策定した、セキュリティーの国際基準です。クレジットカード情報をはじめとする会員情報や取引情報、決済プロセス等における情報保護を目的としています。

Yahoo!ウォレットが取得した認定は、PCI DSS審査のなかで最も厳しい「レベル1」であり、情報管理および取引プロセスなどに関するすべてのシステムにおいて、その安全性が国際水準であると認められたことになります。

クレジット取引セキュリティ対策協議会の定める実行計画への取り組みについて

Yahoo!ウォレットでは、クレジットカードでのお支払いにおいて割賦販売法に基づき、クレジット取引セキュリティ対策協議会の定める実行計画に取り組んでいます。
また、お客さまからお預かりした個人情報にアクセスする権限を持つ担当者を必要最小限に絞るといったシステム的対策や、特に高い機密性が求められる個人情報は隔離・監視されたセキュリティエリア以外ではアクセスできないという物理的対策を組み合わせ、実効性の高い運用を行っています。

2019年3月1日現在（URL　https://wallet.yahoo.co.jp/guide/about/security/index.html）

８．消費者及び事業者等への情報発信②

②クレジットカードのPINの認知度向上

カード会社（イシュアー）及び業界団体等は、IC取引が進展している状況において、更にPIN認知を浸透させるための周知活動に取組む。

③ECにおける不正利用対策の認知度向上

ECにおける不正利用対策の導入・普及にはカード会員の理解・協力を得ることが重要であるため、カード会社（イシュアー）及び業界団体等は、その対策に関する周知活動に取組む。

④ID・パスワードの使い回しの防止

カード会員が複数のインターネットサイトで同一のID・パスワードを使い回している場合、一つのサイトでカード情報が漏えいすれば、他のサイトに不正ログインされ、登録されているカード情報等が不正利用される可能性があるため、カード会社（イシュアー）及び日本クレジット協会は、その使い回し防止等に関する周知活動に取組む。

⑤フィッシング対策への取組

フィッシングが増加傾向にあるため、カード会社（イシュアー）及び業界団体等は、その手口等に関する周知活動に取組む。

⑥利用明細のチェックに関する周知

不正利用被害を防止するためには、カードの利用明細を確認し、不正利用の発生に早期に気付くことが重要であるため、カード会社（イシュアー）及び業界団体等は、その確認の重要性に関する周知活動に取組む。

８．消費者及び事業者等への情報発信③

（２）クレジットカード取引関係事業者への情報発信

- 加盟店をはじめとするクレジットカード取引関係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。

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