経済産業省

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て

平成２８年４月
経済産業省

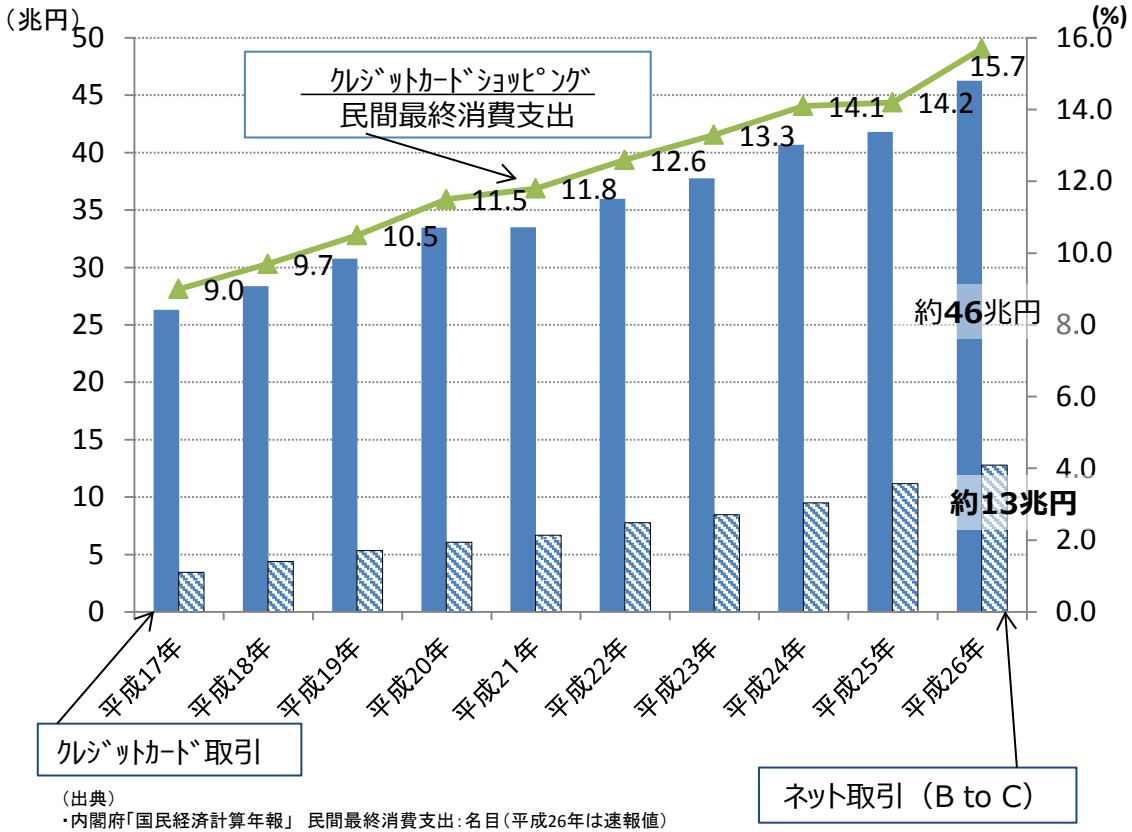
ネット取引の拡大とクレジットカード利用の増加

- ネット取引の急拡大に伴い、近年、**クレジットカード取引高は一貫して増加**。
- 直近では、**４６兆円**（消費全体の**約１６％**）を占める。

（参考）主要各国のカード利用率　韓国：７３％、中国：５６％、米国：３４％

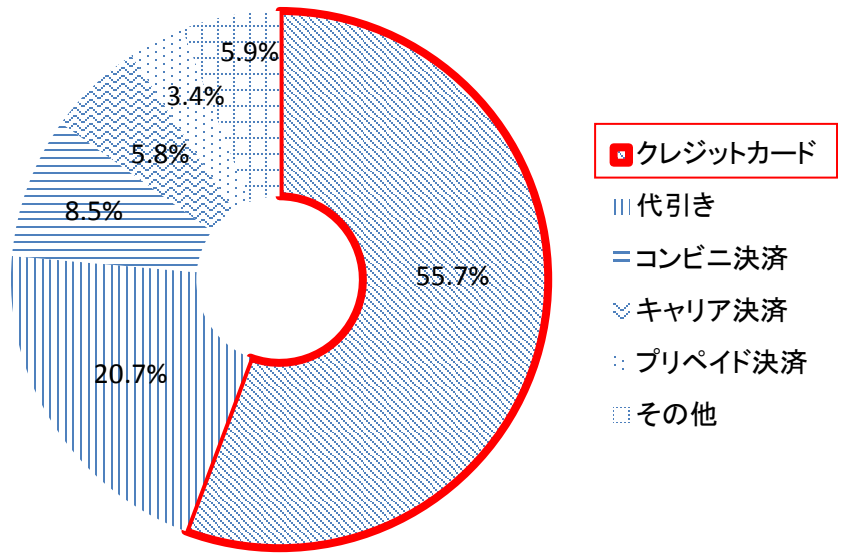
（出所）日本クレジットカード協会による推計

消費に占めるクレジットカード取引とネット取引



（出典）
・内閣府「国民経済計算年報」 民間最終消費支出：名目（平成26年は速報値）
・（一社）日本クレジット協会調査
（注）平成24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、
平成25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。

電子商取引における支払手段の割合【平成24年度】



（出典）矢野経済研究所
電子決済/EC決済サービスの実態と将来予測　2013－2014

日本再興戦略における位置づけ

日本再興戦略改訂2014（平成26年6月24日閣議決定）

5.（3） i）金融・資本市場の活性化 ②資金決済高度化等

・2020年オリンピック・パラリンピック東京大会等の開催等を踏まえ、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。このため、訪日外国人の増加を見据えた海外発行クレジットカード等の利便性向上策、クレジットカード等を消費者が安全利用できる環境の整備（中略）について、関係省庁において年内に対応策を取りまとめる。

キャッシュレス化に向けた方策（平成26年12月26日公表）

2. クレジットカード等を安全に利用できる環境整備

①悪質な加盟店の排除 ②クレジットカード番号等の管理、IC対応などのセキュリティ強化

③消費者教育によるキャッシュレスの理解増進

日本再興戦略改訂2015（平成27年6月30日閣議決定）

5.（3） i）金融・資本市場の活性化等 ⑦キャッシュレス化の推進

・（前略）昨年12月に関係省庁で取りまとめた「キャッシュレス化に向けた方策」に基づき、海外発行クレジットカード等での現金引き出しが可能なATMの一層の普及など訪日外国人向けの利便性向上、クレジットカードのIC化の推進などクレジットカード等を安全に利用できる環境整備（中略）に係る施策を推進する。

インバウンド需要の取り込みのために

- **増加する訪日外国人**は、主な決済手段として、クレジットカードを利用。
- インバウンド需要を更に取り込むためには、**カード利用に関し、訪日外国人の安心を確保**することが必要。

■ **訪日外国人の50%**は、クレジットカードを利用。

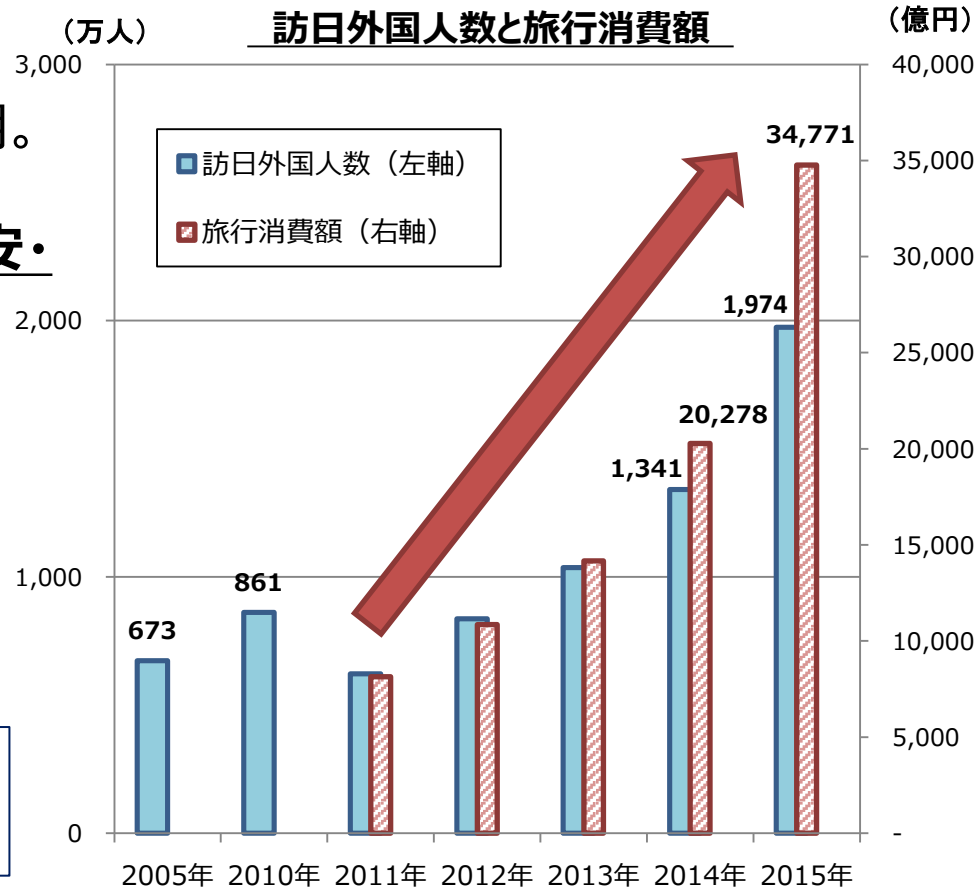
（出所） 観光庁 訪日外国人の消費動向（平成26年報告書）

■ **訪日外国人は**、日本の**カード利用環境に不安・不満**を抱いている。

＜訪日外国人から見た改善すべき点＞
・セキュリティの高いICカード対応の
決済環境を整備すべき：49%

（出所） 日本クレジットカード協会によるアンケート調査

加盟店におけるセキュリティ向上(決済端末のＩＣ化）が求められている。



（出所） ＜観光客数＞ 独立行政法人 国際観光振興機構（JNTO)の統計資料
＜旅行消費額＞観光庁 訪日外国人の消費動向調査（2015年は速報値であり、今後改訂される可能性あり）

「重要インフラ」としての位置づけ

- 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かかる第3次行動計画（2014年5月）」において、「情報システムが障害に至った場合、**国民生活・社会経済活動に多大な影響を及ぼす**おそれがある」として、クレジット分野が**「重要インフラ」に指定**された。（電力、ガス、金融等１３分野の一つ）
- **サイバーセキュリティ基本法**において、「**重要社会基盤事業者**は、そのサービスを安定的かつ適切に提供するため、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国が実施するサイバーセキュリティに関する施策に協力するよう努める」と定められている。

「第3次行動計画」における方針

＜重要インフラ防護の目的＞

- サービスの持続的な提供を行い、サイバー攻撃等に起因するIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、**IT障害発生を可能な限り減らす**とともに、**障害発生時の迅速な復旧**を図る。

＜基本的考え方＞

- 情報セキュリティ対策は、**重要インフラ事業者等が自らの責任において**実施。
- **官民が一丸となった取組**を通じて国民の安心感の醸成、社会の成長等を目指す。

追加的な対応

クレジット分野での取組の方向性（2015年度～）

＜目標＞

- カード情報を保有する事業者のセキュリティ対策を強化。サイバー攻撃等による**情報漏えいを防止**。
- 海外を含め、窃取されたカード情報による**不正使用を最小化**。

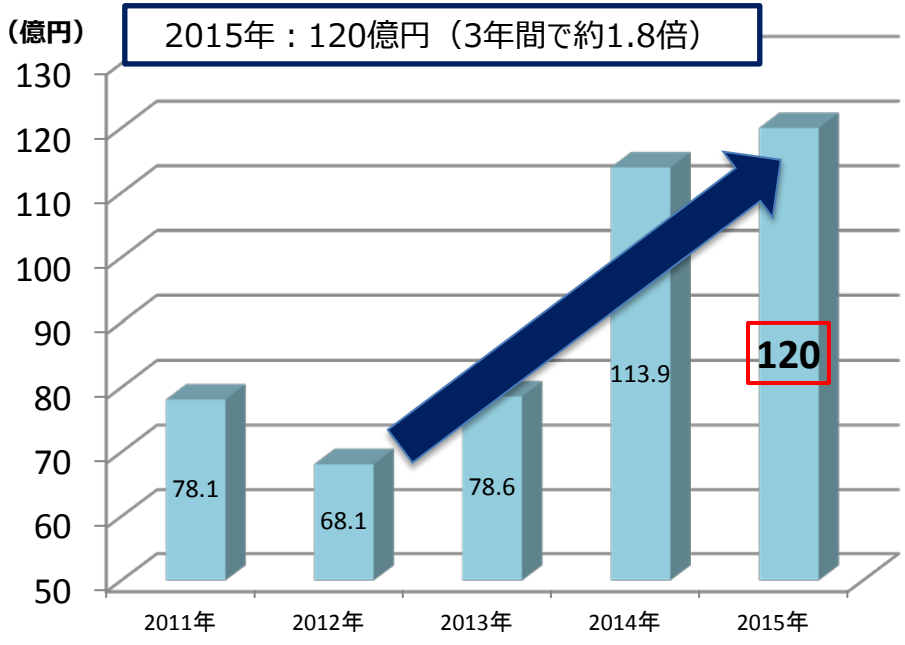
＜具体的な取組＞

- クレジット取引に**関わる幅広い事業者及び行政が連携**した、「クレジット取引セキュリティ対策協議会」において、2020年までの**「実行計画」を策定**。
- 加盟店における情報管理義務等については、**割賦販売法における義務付け**を検討。

クレジット取引の不正使用被害の増加

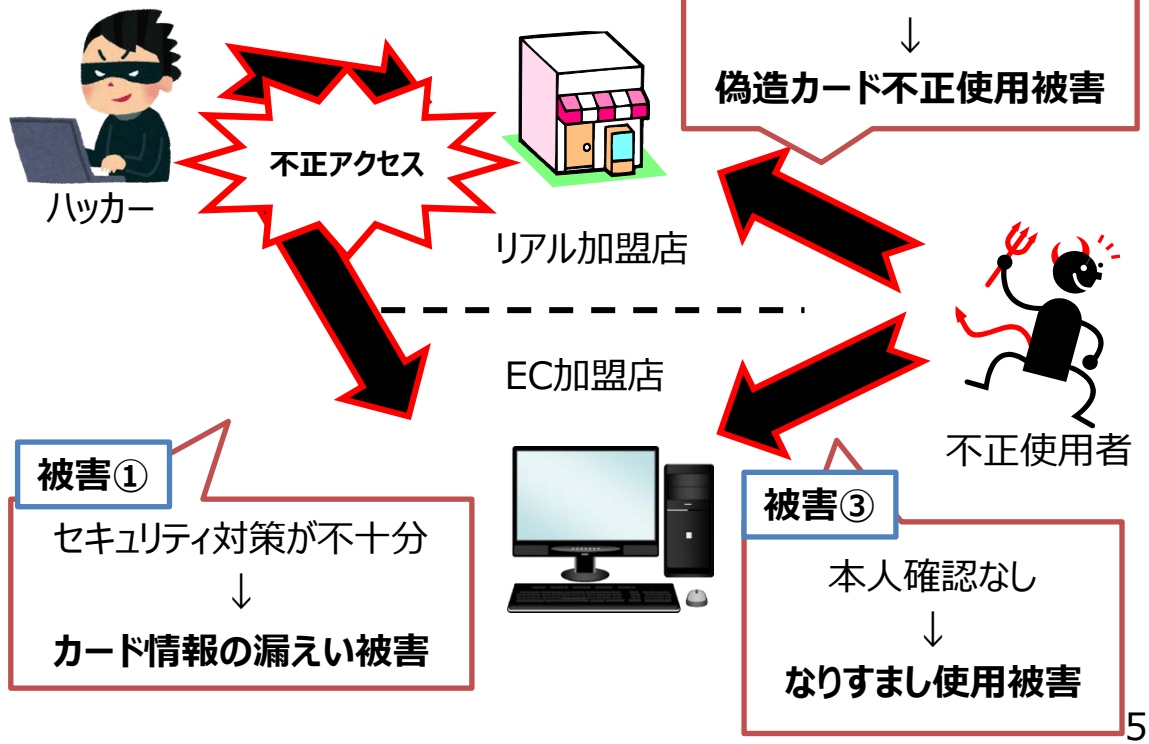
- 昨今、**セキュリティ対策が不十分な加盟店を狙った不正アクセス**により、**カード情報の漏えいが拡大。**
- これに伴い、窃取したカード情報を使って、偽造カードや本人になりすました**不正使用による被害は増加**（2015年**120億円**、3年間で約1.8倍）。
- 不正使用は国境を越えて行われ、換金性の高い商品の購入を通じて、**犯罪組織に多額の資金が流出**しているとの指摘あり。

クレジット取引の不正使用額の推移



（注）不正使用被害額は、国内発行クレジットカードでの不正使用分で、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。）。
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の集計結果について」

クレジット取引での被害イメージ



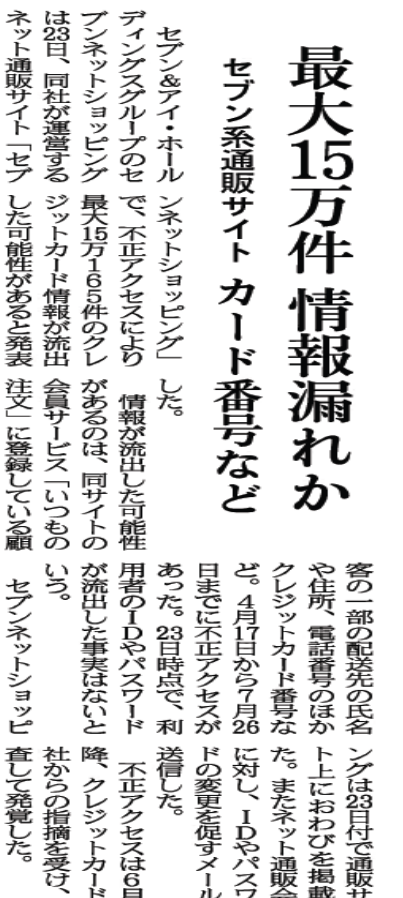
加盟店からのカード情報の漏えい～①ECサイト（日本）

- 近年公表された大規模なカード情報漏えい事案（１万件以上のもの）は、全て（４年間で18件）が**加盟店からの情報漏えい**によるもの。
- カード情報を扱う責任について、加盟店自身に**当事者意識が希薄**なことが問題と指摘されている。

最近の情報漏えい事例

	件名	公表日	流出原因	カード情報の漏えい件数
1	クーコム（株） （宿泊予約サイト「トクー！」）	平成27年 ７月	外部からの不正アクセスにより、**会員氏名、カード番号、有効期限、セキュリティコード、住所、電話番号、メールアドレスが流出**	可能性のある件数 約２万２千件
2	DL Market （音楽、書籍等のネット販売）	平成27年 ９月	SQLインジェクション＊１によって、**会員氏名、カード番号、有効期限、セキュリティコード等が流出**	可能性のある件数 約２万３千件
3	江崎グリコ（株） 「グリコネットショップ」 （菓子・飲料等の通販サイト）	平成28年 ３月	SQLインジェクションによって、**会員氏名、カード番号、有効期限、カード名義、住所、電話番号、メールアドレス等が流出**	可能性のある件数 約４万４千件

＊１　アプリケーションのセキュリティ上の不備を利用し、アプリケーションが想定しない**SQL**文を実行させることにより、システムを不正に操作する攻撃方法のこと



最大15万件 情報漏れか

セブン系通販サイト カード番号など

セブン&アイ・ホールディングスグループのネットショッピング「セブンネットショッピング」で、不正アクセスにより最大15万165件のクレジットカード情報が流出した可能性があると発表した。23日、同社が運営するネット通販サイト「セブン注文」に登録している顧客の一部の配送先の氏名や住所、電話番号のほか、クレジットカード番号など。4月17日から7月26日までに不正アクセスがあった。23日時点で、利用者のIDやパスワードが流出した事実はないという。不正アクセスは6月以降、クレジットカード会社からの指摘を受け、調査して発覚した。セブンネットショッピングは23日付で通販サイト上におわびを掲載し、IDやパスワードの変更を促すメールを送信した。

平成25年10月25日　日経MJ　4面

加盟店からのカード情報の漏えい～②POSシステム（米国）

- 2013年11月に**米国大手スーパーのTarget社**で、**約4000万件**のカード番号等の大規模情報漏えい事案が発生。
- 国際的な犯罪組織がネットを通じてマルウェアを仕掛け、**磁気で読み取られたカード情報を窃取**したもの。セキュリティ強化策として、**2015年にはカード及び端末のIC対応**が完了。
- これにより、同社では、**多額の対策費と損害賠償**が発生し、純利益は大幅減、**CEOも退任**に追い込まれた。

米国TARGET社の事案の概要

・2013年11月27日から12月15日にかけて、Target社の店頭で使用された**4,000万人分のクレジットカード及びデビットカード番号**と**7,000万人分の個人情報（氏名、住所等）**が盗まれた。

・販売店舗の**カード決済端末に不正なプログラムが埋め込まれた**ことが原因。犯人は正体不明だが、地理的拠点としては、ウクライナの約150人のハッカーが集積したデジタル犯罪のシンジケートに辿り着く。

・**情報漏えい対策の費用として6,100万ドル**、損害賠償として顧客に対して1,000万ドルを計上。**銀行（カード会社）からは10億ドルの損害賠償請求**を受けている。

・この影響によって、2013.11-2014.1期の売上高は前年同期比3.8%減、**純利益は半減**した。

出典：各種報道

当時の米国での報道記事

THE WALL STREET JOURNAL.

http://www.wsj.com/articles/SB10001424052702304773104579266743230242538

BUSINESS

Target Hit by Credit-Card Breach

Customers' Info May Have Been Stolen Over Black Friday Weekend

By ROBIN SIDEL, DANNY YADRON and SARA GERMANO
Updated Dec. 19, 2013 7:29 a.m. ET

Target Corp. was hit by an extensive theft of its customers' credit-card and debit-card data over the busy Black Friday weekend, people familiar with the matter said, in what appears to be a brazen breach of a major retailer's information security.

The theft was national in scope and happened in stores, not online, and may have involved tampering with the machines customers use to swipe their cards when making purchases, the people said.

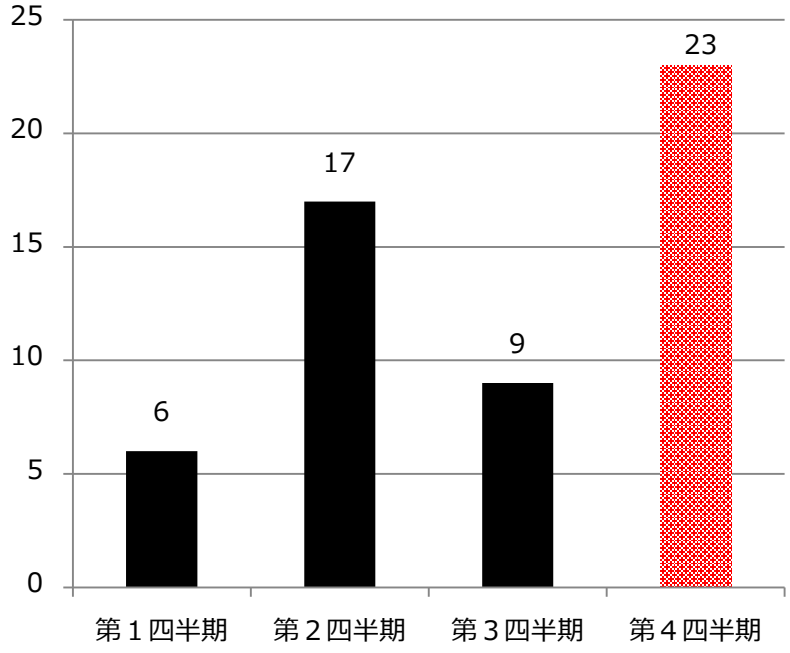
加盟店からのカード情報の漏えい～③POSシステム（日本）

- 大手ホテルチェーンの米ハイアット社が、**決済処理システムでマルウェアの感染**を確認。調査の結果、**日本国内の４拠点**（パークハイアット東京ほか）を含む54の国・地域／250拠点で感染していたことが判明。**国内初のPOSシステムのマルウェア感染による被害**。
- これにより、カード会員**氏名、カード番号、有効期限、セキュリティコード等**が窃取された。
- **POSシステムを標的としたマルウェアの検出台数は世界的に増加傾向**。**日本でも2015年から急増**。（2015年検出台数55台、前年比約７倍、米・フィリピンに続き世界第3位）。

最近のPOSマルウェア被害事例

時期	企業名	被害内容
2015年3月	マンダリンオリエンタル	米国とヨーロッパの拠点でマルウェア感染
2015年4月	White Lodging	北米10拠点のレストランやラウンジで約7ヶ月間POSマルウェア感染
2015年10月	Trump Hotel Collection	北米7拠点のレストランやギフトショップで約1年間にわたりPOSマルウェア感染
2015年11月	ヒルトン	複数のグループホテルで約4ヶ月間にわたりPOSマルウェア感染
2015年11月	スターウッド	北米50拠点のレストランやギフトショップで約11ヶ月間にわたりPOSマルウェア被害
2016年1月	ハイアット	**日本を含む**全世界54ヶ国地域250拠点で約4ヶ月間POSマルウェア感染

2015年POSマルウェア検出台数（日本）

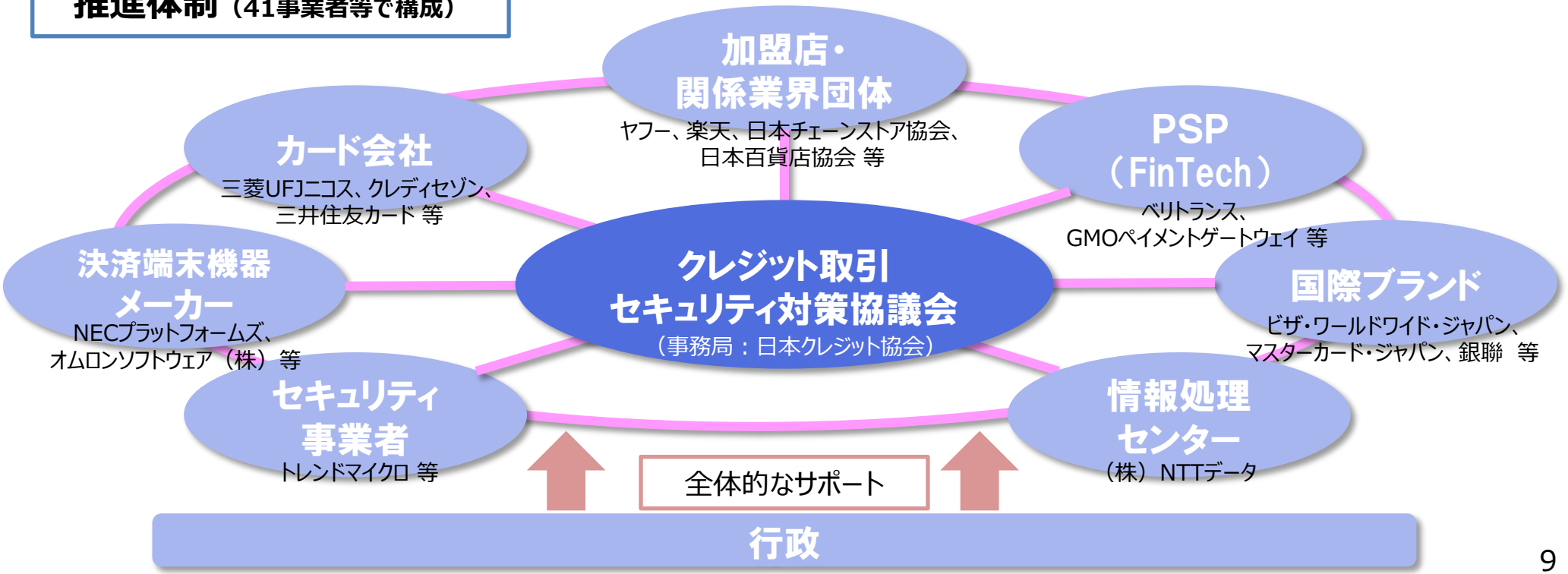


（出典）2016年２月トレンドマイクロ調査

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）。
- **目標**、**各主体の役割**、**当面の重点取組**をとりまとめた「**実行計画**」を策定（2016年2月）。
- **日本クレジット協会**を中心に、**「実行計画」の推進体制を構築**。今後、目標達成に向け、**進捗状況を管理・評価**し、**必要な見直し**を行っていく（2016年4月～）。

推進体制（41事業者等で構成）



［参考］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、ジャックス、ジェーシービー、
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

【ＰＳＰ】ベリトランス

【加盟店】カタログハウス、 ジェイティービー、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

【機器メーカー】ＮＥＣプラットフォームズ、オムロンソフトウェア

【セキュリティ事業者】トレンドマイクロ、Payment Card Forensics

【学識経験者】笠井修・中央大学教授（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

WG1（番号保護）

【カード会社】
イオンクレジットサービス(株)
(株)オリエントコーポレーション
(株)クレディセゾン
(株)ジャックス
(株)ジェーシービー
(株)セディナ
トヨタファイナンス(株)
三井住友カード(株)
三菱UFJニコス(株)
ユーシーカード(株)
楽天カード(株)
【PSP】
GMOペイメントゲートウェイ
【加盟店関係】
(株)カタログハウス
(株)ジェイティービー
(株)高島屋
(株)三越伊勢丹ホールディングス
ヤフー(株)
ユニー株
楽天(株)
【情報処理センター】
(株)NTTデータ
【セキュリティ専業者】
トレンドマイクロ
Payment Card Forensics
【オブザーバ】
（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［DinersClub］
UnionPay International Co.,Ltd［銀聯］
（その他）
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
経済産業省

WG2（偽造防止）

【カード会社】
イオンクレジットサービス(株)
(株)オリエントコーポレーション
(株)クレディセゾン
(株)ジャックス
(株)ジェーシービー
(株)セディナ
トヨタファイナンス(株)
三井住友カード(株)
三菱UFJニコス(株)
ユーシーカード(株)
楽天カード(株)
【加盟店関係】
(株)高島屋
(株)三越伊勢丹ホールディングス
ユニー(株)
(株)ヨドバシカメラ
【情報処理センター】
(株)NTTデータ
【機器メーカー／ソフトウェアメーカー】
NECプラットフォームズ(株)
オムロンソフトウェア(株)
東芝テック(株)
パナソニックシステムネットワークス(株)
富士通(株)
日本NCR
ソリマチ技研
【オブザーバ】
（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［DinersClub］
UnionPay International Co.,Ltd［銀聯］
（その他）
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
経済産業省

WG3（不正防止）

【カード会社】
イオンクレジットサービス(株)
(株)オリエントコーポレーション
(株)クレディセゾン
(株)ジャックス
(株)ジェーシービー
(株)セディナ
トヨタファイナンス(株)
三井住友カード(株)
三菱UFJニコス(株)
ユーシーカード(株)
楽天カード(株)
【PSP】
ソニーペイメントサービス(株)
【加盟店関係】
(株)カタログハウス
(株)ジェイティービー
J. フロント リテイリング株
(株)三越伊勢丹ホールディングス
ヤフー(株)
ユニー(株)
楽天(株)
【情報処理センター】
(株)NTTデータ
【セキュリティ専業者】
トレンドマイクロ
Payment Card Forensics
【オブザーバ】
（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［DinersClub］
UnionPay International Co.,Ltd［銀聯］
（その他）
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
経済産業省

「実行計画」における対策の３本柱

１．カード情報の漏えい対策

◇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PCIDSS準拠

２．偽造カードによる不正使用対策

◇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

３．ECにおける不正使用対策

◇ネットでなりすましをさせない

- 多面的・重層的な不正使用対策の導入

1．クレジットカード情報の漏えい防止（非保持／セキュリティ国際規格準拠）

現 状 ・ 課 題

- 近年、サイバー攻撃によるEC加盟店等からの**カード情報の漏えい事故が頻発**※H27年30件（前年比2.3倍）。
- カード情報を狙うハッカーの**攻撃手口のグローバル化・巧妙化**。
- 加盟店等において、カード情報を取り扱っている**当事者意識が希薄**で対策が不十分。

目 標

○ 加盟店は、原則、**カード情報の非保持化**

○ カード情報を取り扱う事業者は、セキュリティに関する**国際規格（PCIDSS）準拠**

各主体の役割

カード会社・PSP（決済代行業）

・**PCIDSS準拠を完了(2018年3月まで)**
・カード会社は、PCIDSSに準拠していないPSPとの取引を見直し(2018年4月目途)
・加盟店に対して非保持化又はPCIDSS準拠に向けた要請・支援

加盟店

・カード情報の**非保持化又はPCIDSS準拠**を完了
（**EC加盟店は2018年3月**まで）
（**対面加盟店は2020年3月**まで）
・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

行政

・**PSPや加盟店等にもカード情報の適切な管理を義務づけ**（割賦販売法の改正）
・カード情報の適切な保護について、事業者や消費者に情報発信
・NISC、JPCERT等の**セキュリティ関係機関との連携・情報共有**

PCIDSS（ Payment Card Industry Data Security Standard ）

- PCIDSSは、**<u>カード情報を取り扱う全ての事業者</u>**に対して**<u>国際ブランドが共同で定めたデータセキュリティの国際基準</u>**。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。
- PCIDSS準拠の検証方法としては、カード情報の取扱形態や規模によって、①**<u>オンサイトレビュー</u>**（認証セキュリティ評価機関（QSA）による訪問審査）又は②**<u>自己問診</u>**（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。

Ⅰ．安全なネットワークの構築・維持	Ⅳ．強固なアクセス制御手法の導入
要件1：ファイアーウォールによるカードデータ保護	要件7：カード会員データへのアクセスを、業務上必要な範囲に制限する
要件2：デフォルトパスワードの変更	要件8：システムコンポーネントへのアクセスを確認・許可する
Ⅱ．カード会員データの保護	要件9：カード会員データへの物理アクセスを制限する
要件3：カード会員データの保護	Ⅴ．ネットワークの定期的な監視およびテスト
要件4：カード会員データを伝送する場合、暗号化する	要件10：カード会員データへのアクセスを追跡および監視する
Ⅲ．脆弱性管理プログラムの整備	要件11：セキュリティシステムおよびプロセスを定期的にテストする
要件5：マルウェアからの保護	Ⅵ．情報セキュリティポリシーの整備
要件6：安全性の高いシステムとアプリケーション	要件12：すべての担当者の情報セキュリティポリシーに対応するポリシーを整備する

2．偽造カードによる不正使用防止（カードと決済端末のIC対応）

現 状 ・ 課 題

- **偽造カードによる不正使用**に対し、取引のIC化は、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※は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。

※市場の約8割を占め、全体でのIC対応端末は約17%。カードのIC率は約7割、銀行ATMのIC対応は約93%。

目　標

○ 2020年までに**カード**及び**加盟店の決済端末のIC対応100%実現**

各主体の役割

カード会社

・**クレジットカードのIC化**100%を実現（2020年3月まで）
・IC取引時のオペレーションルール（PINレス等）の策定

加盟店

・POS等の**決済システムのIC対応**を完了（2020年3月まで）

低コスト化支援

国際ブランド

・加盟店がIC対応する際の**認証プロセスの効率化**

POS機器メーカー

・POSの接続部分のソフトウェアを共通化
・POSシステムの**IC対応を標準化**

行政

・先行的に取り組む加盟店の**見える化**、未対応による**不正使用の損害賠償ルール**の明確化）

・**実効性確保**の観点から、割賦販売法における更なる措置を検討

・**中小加盟店等への支援**

我が国のクレジットカード及び決済端末のIC対応の現状

- **クレジット取引のIC化**は、現状、国際的にも、**カードの偽造防止の唯一無二の対策**。
- 我が国の**クレジットカードのIC化**は、**7割程度**普及。2020年までに100%IC化を目指す。
- 決済端末について、**決済専用端末のIC対応は約7割**まで普及（約100万台）。他方、大規模加盟店を中心とした**ＰＯＳ端末（※）のIC対応**については、システム改修のコスト負担等がネックとなり、ごく一部を除いて**まだ普及が進んでいない**。※市場全体の８割程度を占める。

カードのIC化

磁気カードの10～200倍の情報を蓄積

偽造カードは、**磁気カードをコピー**して作られる。ＩＣカードは、**ＩＣチップ内に情報を暗号化**して格納しているので、情報のコピー（**偽造**）**ができない**。

決済端末のIC対応化

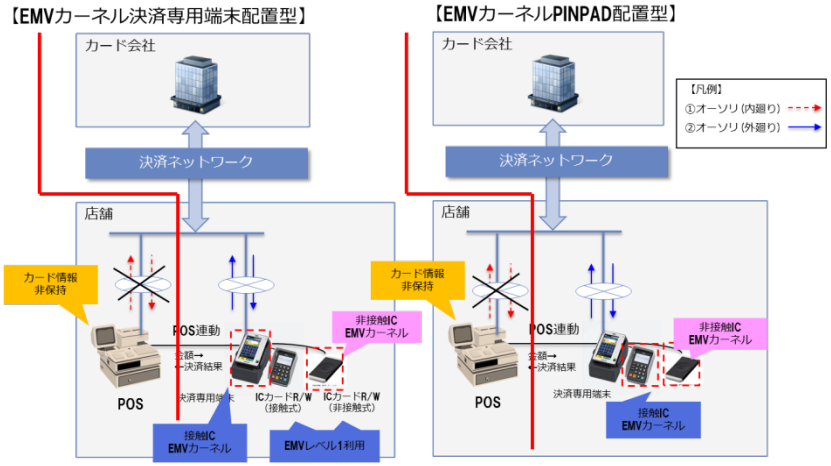
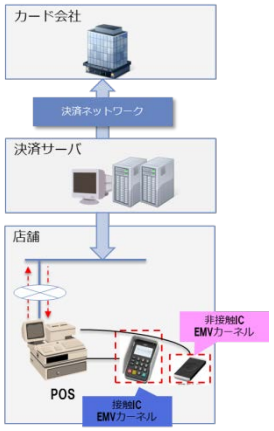
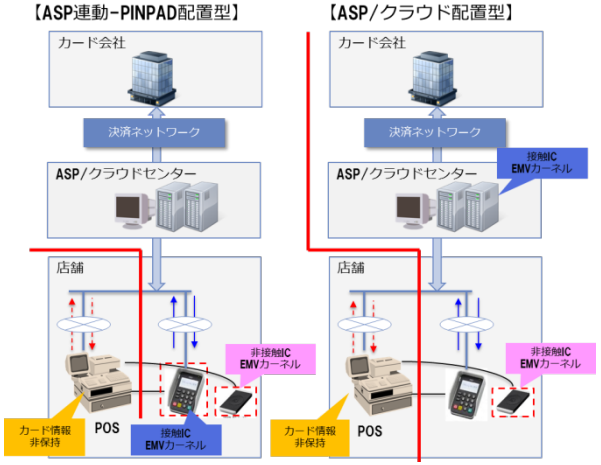
磁気ストライプ対応端末

IC対応端末

磁気ストライプ決済では、**スキミングの恐れ**があるが、**IC対応**によりカード情報の処理が**暗号化**され、カードと端末の間で相互認証されるため、**偽造カードの使用が防止**できる。

IC対応の手法の種類について

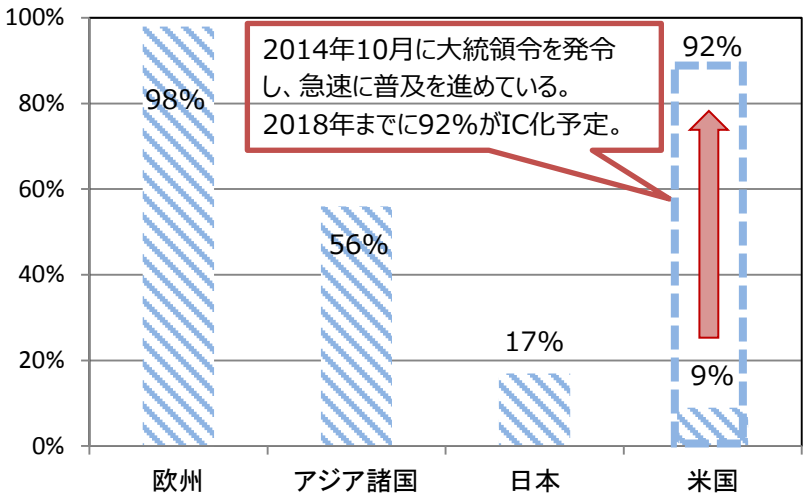
- POSシステムのIC対応を推進するため、EMVカーネルの配置（EMV認定の取得箇所）をPOSシステムの外側にすることでコスト負担の低減を図れる3つの手法に整理し、それぞれ技術面・コスト面での検証及びコスト低減策についての検討を行った。

手法	決済専用端末連動型	決済サーバ接続型	ASPクラウド接続型
	【EMVカーネル決済専用端末配置型】 【EMVカーネルPINPAD配置型】 	【PINPAD配置型】 	【ASP連動-PINPAD配置型】 【ASP/クラウド配置型】 
説明	✓ 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	✓ 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。	✓ 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。
特徴	✓ 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。 ✓ 決済専用端末を新たに追加する必要があるため、設置場所の確保が課題。	✓ EMVカーネルをPOSシステムの外側に置くため、導入時の対応影響は小さい。 ✓ カード情報がPOSシステムのサーバーを通過するため、PCIDSSの準拠は必要。	✓ 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(ただしASP利用料は発生)。
コスト低減策	✓ CCT端末とアプリケーション間で通信を行うミドルウェアの通信手続きを標準化※1 ✓ ブランドテストの効率化について国際ブランドと検討	✓ PINPADとアプリケーション間で通信を行うミドルウェアの通信手続きを標準化※1 ✓ ブランドテストの効率化について国際ブランドと検討	✓ CCT端末とアプリケーション間で通信を行うミドルウェアの通信手続きを標準化※1 ✓ ブランドテストの効率化について国際ブランドと検討

我が国の「セキュリティホール化」の懸念

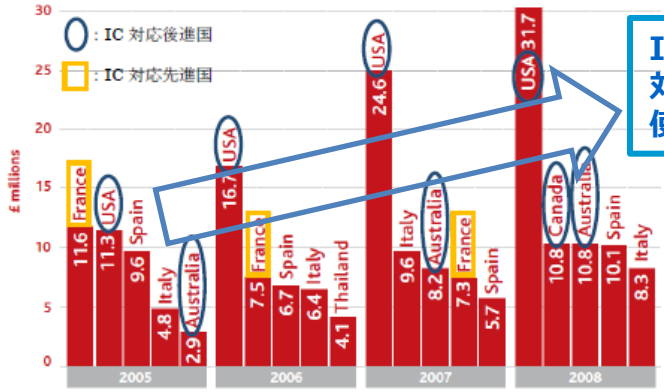
- 従来、クレジット決済端末の**IC対応「後進国」**の代表格が**日米両国**。
- **不正使用大国であった米国**は、最近の大規模漏えい事件をきっかけに、**ＩＣ対応を急速に進め**つつある。 ※2014年10月にクレジット決済のＩＣ化に係る大統領令を発令。2015年中には大手小売業者はIC対応をほぼ完了。
- 欧州や東南アジアの一部の国では**100%近く普及が進んでいる**ほか、**中国や韓国では Chip Mandate（義務化）**等によりIC対応が急速に進んでいる。
- その結果、磁気決済が中心でセキュリティ環境の脆弱な**我が国が「セキュリティホール化」**し、偽造カードの不正使用被害が**国境を越えて流入するリスク**が高まりつつある。

クレジット取引のIC対応比率（※）



（※）クレジット取引全体に占める、IC対応端末での取引の比率
（出所） 2013VisaNet clearing & settlement

イギリス発行カードの海外での不正利用の推移（2005-2008）



出典：APACS Fraud The Facts 2009（2016年2月　日本クレジットカード協会　IC化に関する調査結果）

米国の偽造カード被害額
（2011 - 2015）

出典：Aite Report - EMV Lessons Learned and the U.S. Outlook
（2016年2月　日本クレジットカード協会　IC化に関する調査結果）

3．ネットでのなりすまし等による不正使用防止（本人認証等）

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使用被害が急増**。
  ※不正使用被害額（2015年120億円）の６割はECにおける不正使用に起因。
- なりすましにより不正使用されやすい「**カード番号＋有効期限**」のみで決済可能なEC加盟店が多数存在。

目　標

○ 2020年に向け、**ECにおける不正使用被害の最小化**
○ 2018年3月までに、EC加盟店において、**多面的・重層的な不正使用対策**を導入

多面的・重層的な不正使用対策

※いずれも一つで十分というものでないが、一定の有効性のある代表的な方策として提示。

○本人認証（3Dセキュア）	○セキュリティコード	○属性・行動分析	○配送先情報
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	券面の数字（3～4桁）を入力し、カードが真正であることを確認	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	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

各主体の役割

加盟店

- **各社の被害状況やリスクに応じ、多面的・重層的な不正使用対策を導入（2018年3月まで）**
- 特に、何も不正使用対策を講じていない加盟店はカード会社・PSPの協力を得て、早急に導入

カード会社・PSP

- 本人認証（３Dセキュア）のための**パスワード登録の促進**
- EC加盟店における不正使用対策の導入に向けた要請・支援

行政

- 不正使用対策の必要性や有効性について、事業者等に対し周知・啓発
- 被害の実態や最新手口等について**外部専門機関と連携・情報発信**
- 消費者に対し、不正使用の実態やパスワード等の使い回し等を注意喚起

本協議会の今後の活動方針と体制等について

- 協議会の参加各社等は本実行計画に基づき、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。
- 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。
- 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、進捗管理等の業務を行う。協議会参加各社は支援・協力を行う。

本協議会の今後の活動方針

協議会参加各社等
セキュリティ対策協議会

実行計画の策定

2016/4

本実行計画に基づく具体的な取組を推進

セキュリティ対策の強化に向けた議論を継続
（漏洩事案、被害実態、技術的進展を踏まえた対策の改善）

2020/3

安心・安全なカード利用環境の実現

本実行計画の進捗管理に係る体制と役割

協議会参加各社等

支援・協力

日本クレジット協会
（クレジット取引セキュリティ対策協議会事務局）

① 本実行計画の取組についての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