経済産業省

資料６－２

クレジットカードの安全・安心な利用環境の整備に向けて

平成２８年６月

商務情報政策局 商務流通保安グループ 商取引監督課

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、（中略）、**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）

※内閣官房、金融庁、消費者庁、経済産業省、国土交通省、観光庁決定

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、（中略）、**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。

日本再興戦略改訂2016（平成28年6月2日閣議決定）

Ⅱ．2－2.（1） iii)活力ある金融・資本市場の実現：キャッシュレス化の推進等

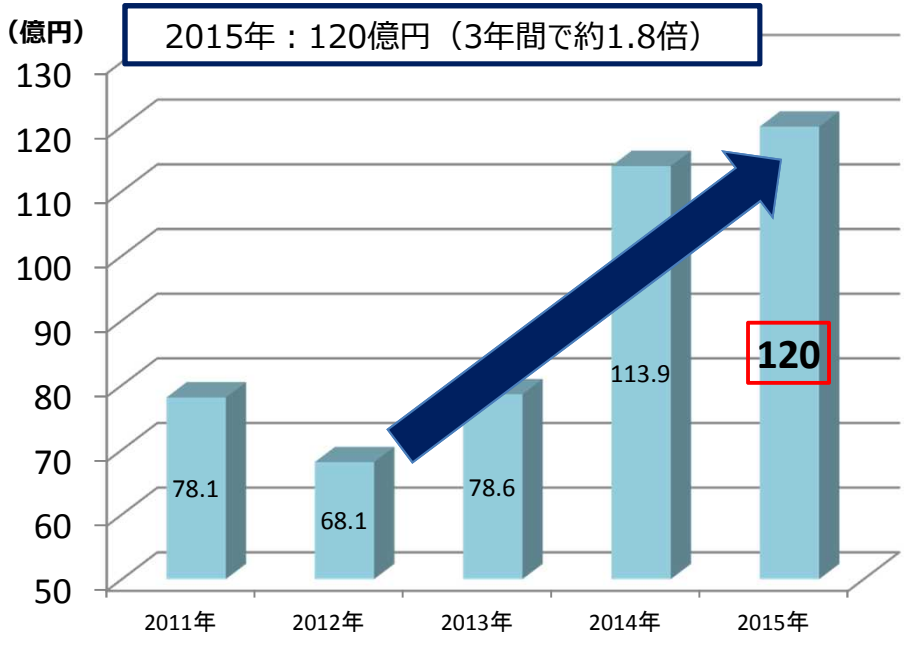
・クレジットカードを安全に利用できる環境整備を推進するため、**2020年までに「クレジット決済端末の100%のIC対応化」**の実現等、国際水準のセキュリティ環境の実現を目指し、クレジット取引に関係する事業者等が策定した**「実行計画」の円滑な実施**を促進するとともに、その実行性を確保するため、**加盟店等におけるセキュリティ対策を義務付ける**ことを含め、必要な法制上の措置を講ずる。

・さらに、**FinTechによるイノベーションを促す新たな規制・制度環境整備を実現**するため、クレジットカード分野において、**技術力・信頼度の高い決済代行業者に新たに法的な位置付けを与える**ことにより、独自のIT技術をいかして効率的に取引の安全確保を図ること等を含め、必要な法制上の措置を講ずる。

クレジット取引の不正使用被害の増加

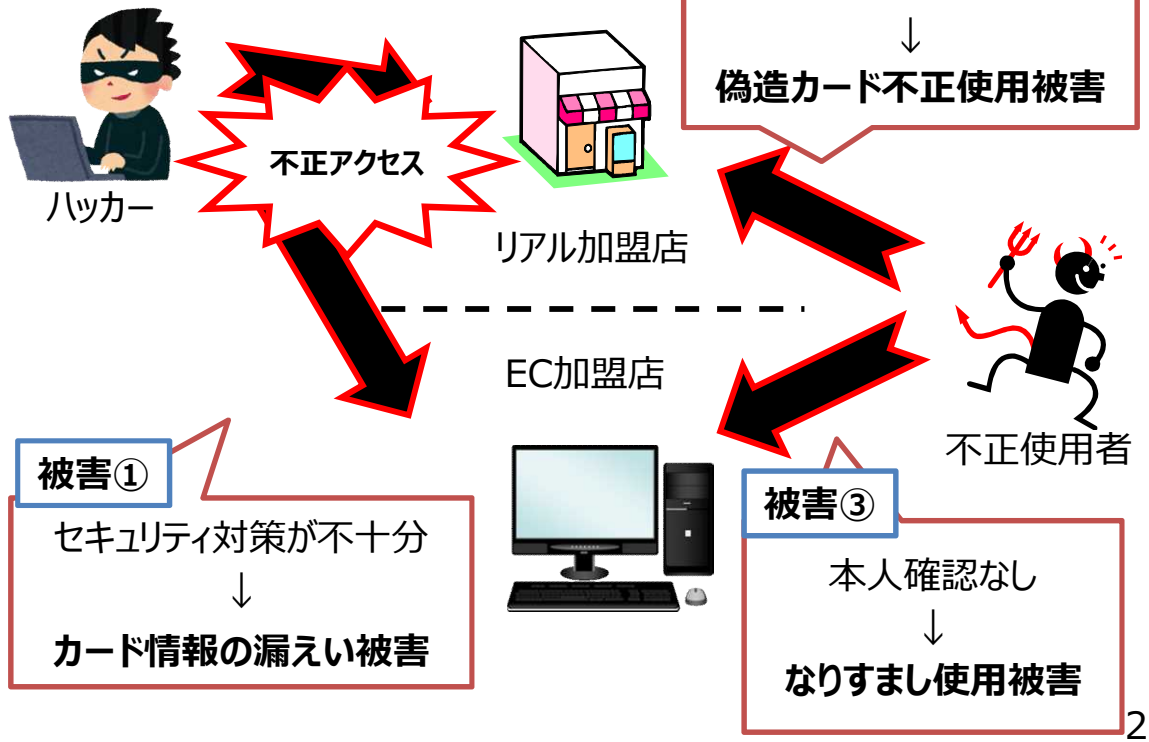
- 昨今、**セキュリティ対策が不十分な加盟店を狙った不正アクセス**により、**カード情報の漏えいが拡大。**
- これに伴い、窃取したカード情報を使って、偽造カードや本人になりすました**不正使用による被害は増加**（2015年**120億円**、3年間で約1.8倍）。
- 不正使用は国境を越えて行われ、換金性の高い商品の購入を通じて、**犯罪組織に多額の資金が流出**しているとの指摘あり。

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



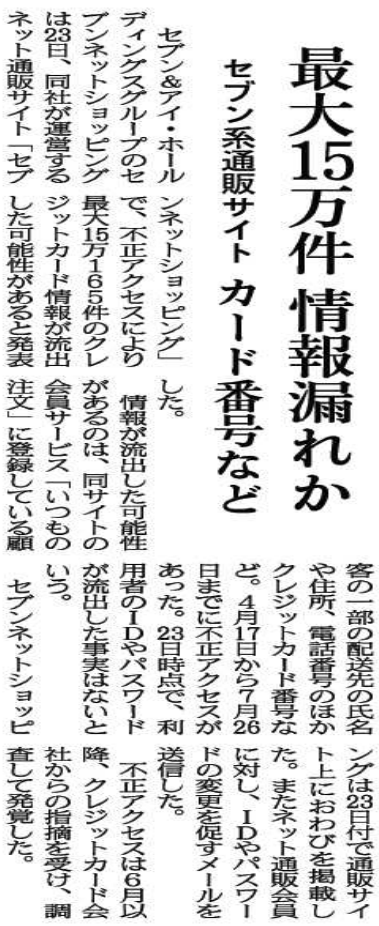
加盟店からのカード情報の漏えい～ECサイト

- 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

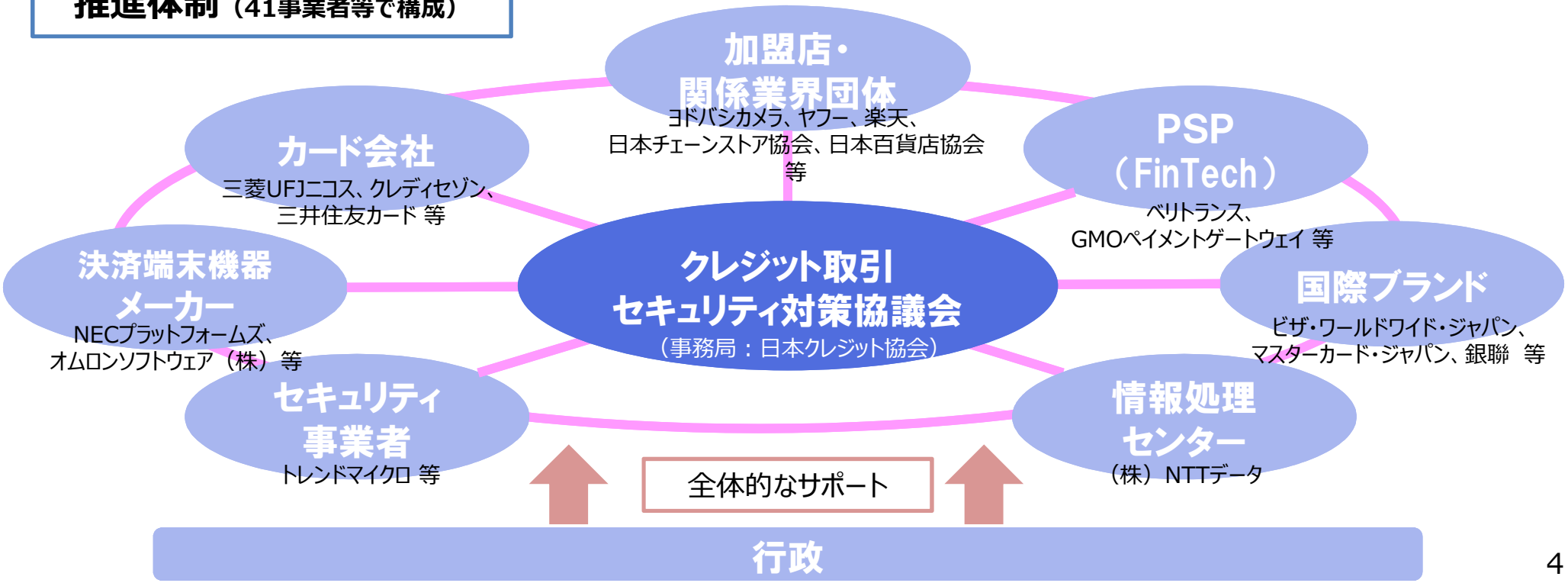
セブン&アイ・ホールディングスグループのネットショッピング「セブンネットショッピング」で、不正アクセスにより最大15万165件のクレジットカード情報が流出した可能性があると発表した。情報が流出した可能性があるのは、同サイトの会員サービス「いつものご注文」に登録している顧客の一部の配送先の氏名や住所、電話番号のほかクレジットカード番号など。4月17日から7月26日までに不正アクセスがあった。23日時点で、利用者のIDやパスワードの変更を促すメールを送信した。不正アクセスは6月以降、クレジットカード会社からの指摘を受け、調査して発覚した。

平成25年10月25日　日経MJ　4面

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）



「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

［実行計画①］クレジットカード情報の漏えい防止（非保持／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**

［実行計画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）

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**

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**

［実行計画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

産構審割賦販売小委員会報告書［追補版］(6月2日公表)について（セキュリティ対策の強化）

● 加盟店からのカード情報の大型漏洩事件の続発、不正使用被害の増加傾向等、セキュリティリスクの高まる中、**「クレジット取引セキュリテイ対策協議会」の実行計画**（本年2月）**の実効性を確保**するため、法制上の措置を講じることを提言。

1．加盟店等へのセキュリティ対策の義務づけ

- **全ての関係事業者**に対し**「リスクに応じた措置」**を義務づけ
  - ①**情報管理**（漏洩対策）：加盟店を含め、カード情報を保有する事業者　※個人情報保護法の特別法的な位置づけ
  - ②**不正使用対策**：加盟店
- 義務履行のための具体的手段については、事業者の創意工夫に委ねる**「性能規定」**の考え方を採用。**技術革新の成果**を取り込んだ多様な手法を許容。

2．加盟店契約会社等による加盟店管理を通じたセキュリティ強化

- 加盟店契約会社等が、**加盟店管理の一環**として、加盟店における**セキュリティ対策の状況を確認**し、是正指導等の適切な対応を行う。　※クレジット取引ネットワークの「ゲートキーパー」としてスクリーニング・モニタリング機能を果たす。

3．認定割賦販売協会（日本クレジット協会）を中心としたセキュリティ推進体制の構築

- **法定業務**として「セキュリティ対策の推進」を追加。
- 協会の役割として、**「実行計画」の実施**を進めるとともに、「性能規定」の下で、**標準的な対策に関する指針**を策定。