経済産業省

安全・安心

参考資料１

2022年6月2日　第30回割賦販売小委員会資料2－2より抜粋・一部改変

クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）第1.1版

2022年6月2日

経済産業省　商務・サービスグループ
商取引監督課

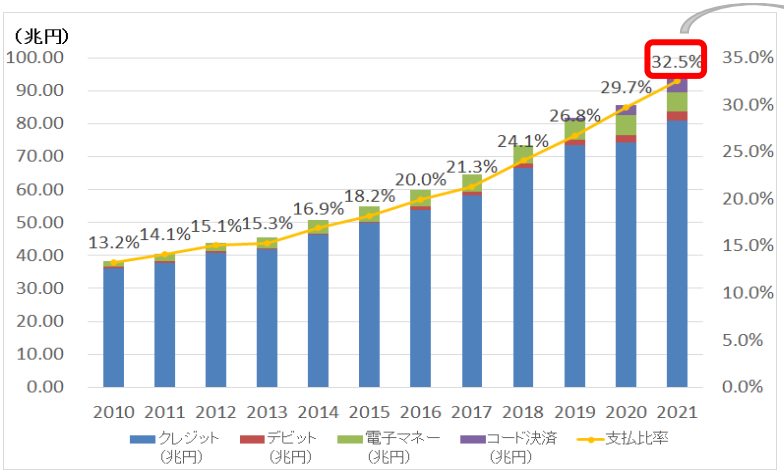
1．背景

2022年6月2日　第30回割賦販売小委員会資料2－2より改変

キャッシュレス決済の伸長

国内キャッシュレス決済額・比率は順調に増加（うちクレジットカード取引は約９割）

キャッシュレス支払額及び決済比率の推移



2025年6月まで
40%
※目標値

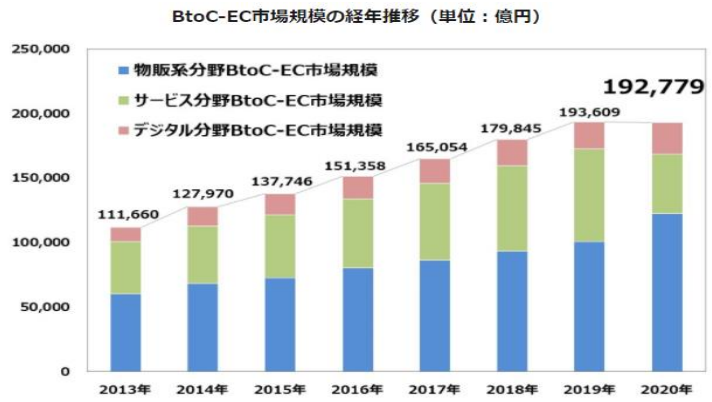
うちクレジット：
約100兆円
※見込み

出典：経済産業省HP

参考：民間(矢野経済研究所)の試算によると、キャッシュレス決済額全体は2025年に約**150**兆円まで拡大するとされている

EC決済サービスの伸長

EC取引の伸長に伴って、消費者のクレジットカード番号の入力機会が増加



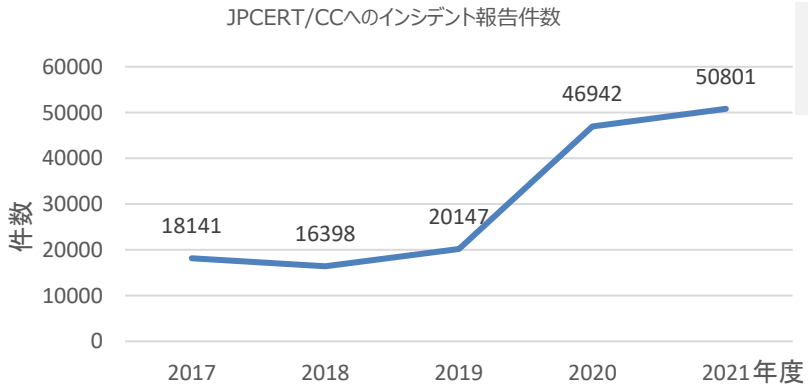
2020年
EC市場規模
約19兆円

出典：令和2年度産業経済研究委託事業（電子商取引に関する市場調査）経済産業省

参考：民間(SBペイメント)の試算によると、EC決済のうち約 **8** 割はクレジットカードを使った決済が行われている

サイバーセキュリティインシデントの発生

全業種的にサイバーセキュリティインシデントへの脅威が高まっている

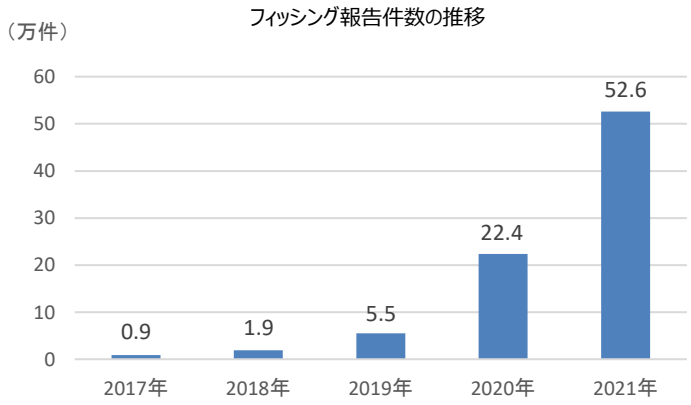


2021年度
報告件数
約 5 万件

出典：JPCERT/CCインシデント報告対応レポート（2022年４月14日）

フィッシング被害の増加

近年、消費者を狙ったフィッシングの報告件数も急増



2021年
フィッシング報告件数
約53万件

フィッシングとは：
メールやSMSを通じて、個人情報等（クレジットカード番号等を含む）をだまし取ること

出典：JC3HP（フィッシングターゲットの変遷）

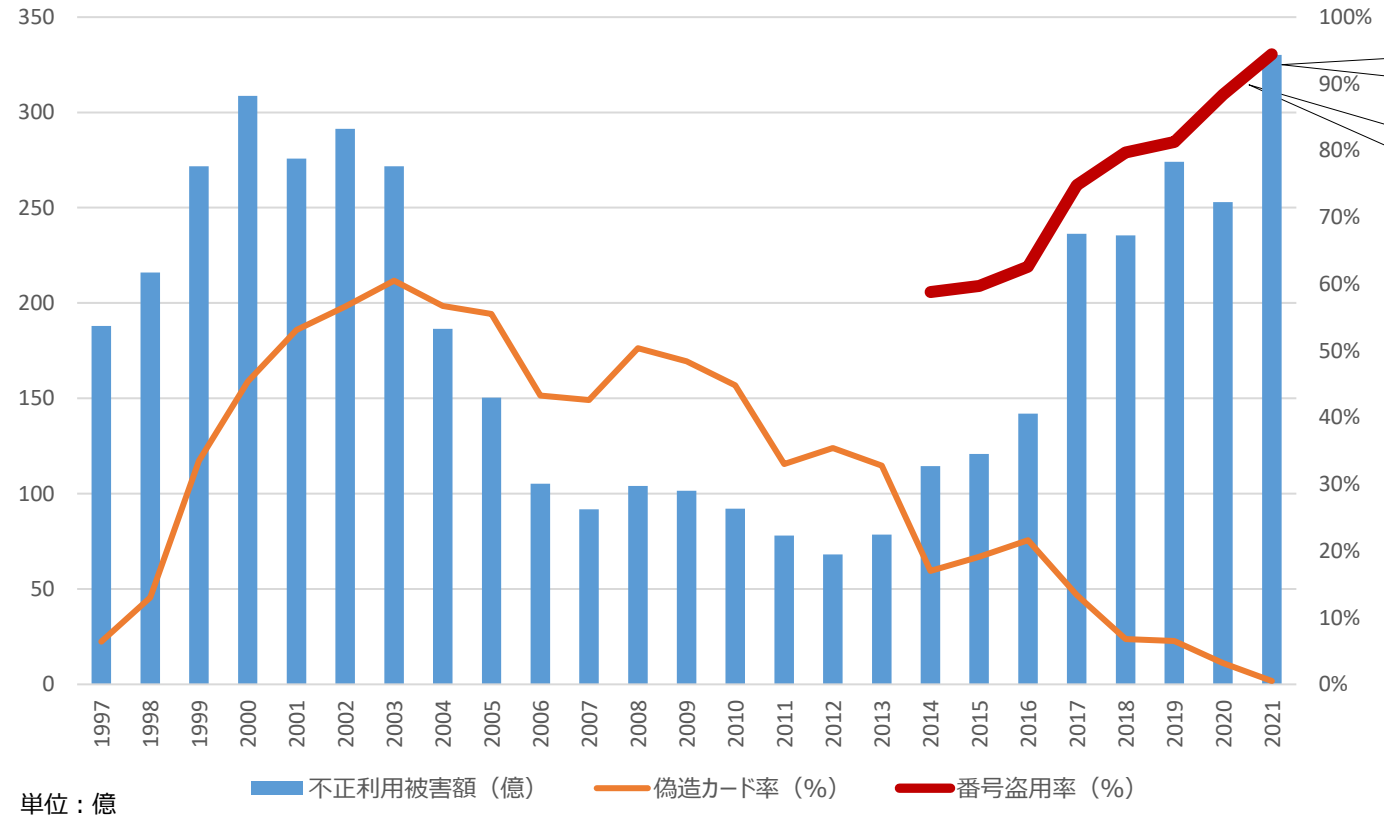
1．背景

2022年6月2日　第30回割賦販売小委員会資料2－2より抜粋

結果として、不正利用被害額は過去最高に、そのうち番号盗用被害額も過去最高に

※　サイバー攻撃やフィッシング等によって漏えい・割り出されたクレジットカード情報を用いて、クレジットカードによる不正利用に使われている

国内発行クレジットカードにおける年間不正利用被害額推移



単位：億

2021年における不正利用被害**総額**
330億円

2021年の不正利用被害総額に対する**番号盗用**の被害割合
94%

想定される番号盗用の原因
- クレジットマスター
  （クレジットカード番号自体は盗まず、他人のクレジットカード番号から確率的に割り出す手法）
- 加盟店等、事業者からの漏えい
- フィッシング
  （メールやSMS等を通じて、利用者からクレジット情報等をだまし取る）

出典：日本クレジット協会（令和４年３月）

補足：ダークウェブでのクレジットカード番号等の取得による不正利用

※　盗まれたクレジットカード情報は、ダークウェブ等において売買され、不正利用に使われることもある

事案１）クレジットカードの情報をダークウェブで入手し、高級腕時計を購入し売却したとして逮捕
事案２）クレジットカードの情報をダークウェブで購入し悪質事業者に売りさばいたとして学生を逮捕

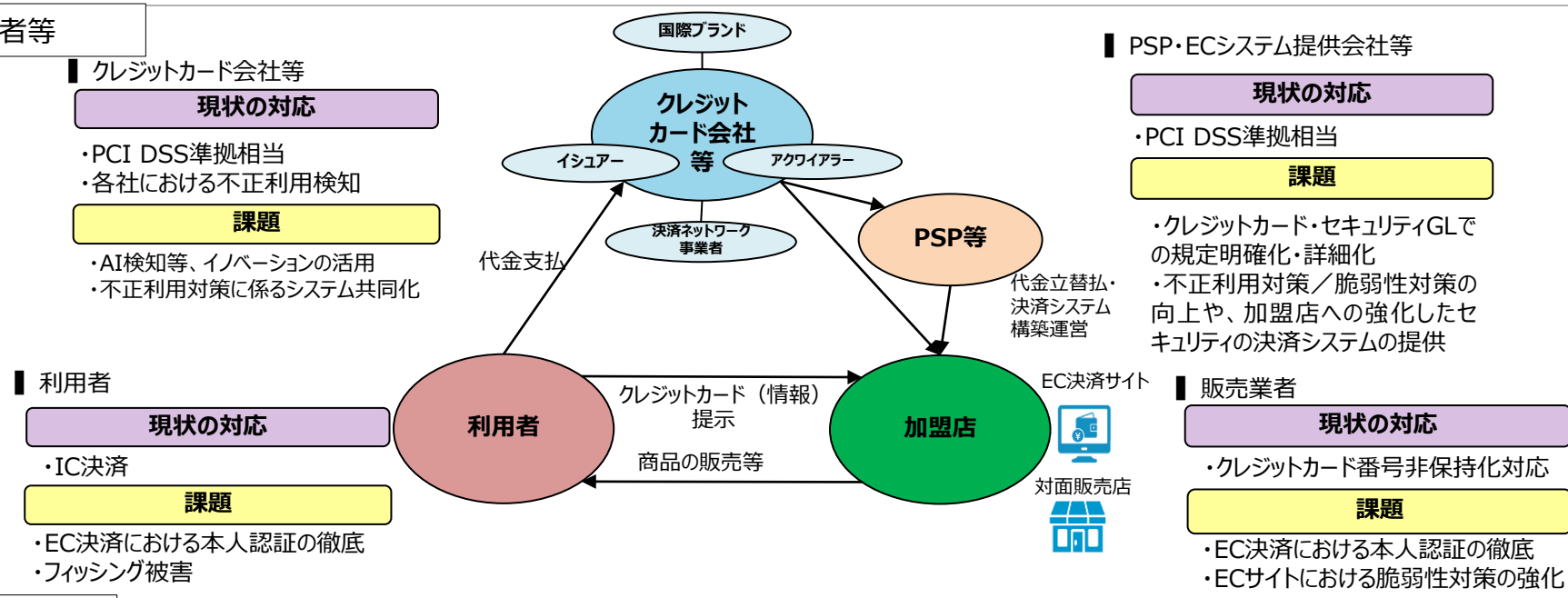
参考：民間セキュリティ会社の調査によると、日本のクレジットカード情報は闇サイトで平均約5200円で販売されているとの情報も（2022/4/4　共同通信社）

2．クレジットカードシステムのセキュリティ対策の現状と課題

2022年6月2日　第30回割賦販売小委員会資料2－2より抜粋

- 加盟店と利用者との決済サービスをクレジットカード会社が提供するという基本的関係をもとに様々な事業者が参画。
- クレジットカードシステムに対するセキュリティは、
  ① 当初は、**クレジットカード会社**によるPCI DSS準拠等の漏えい防止対策。
  ② 一方、キャッシュレス決済の広まりに伴い、**利用者**や**加盟店**といったフロントでの対策も重要。
  ③ 最近では、**決済代行業者（PSP）等**の、クレジットカード会社と加盟店の間にいる事業者が決済情報を集積している場合も多く、これらの事業者におけるさらなるセキュリティ対策強化が課題と認識。
- 今後は、関係事業者・関係省庁・関係団体等の連携がより一層重要になる。

関係事業者等



クレジットカード会社等

現状の対応

・PCI DSS準拠相当
・各社における不正利用検知

課題

・AI検知等、イノベーションの活用
・不正利用対策に係るシステム共同化

PSP・ECシステム提供会社等

現状の対応

・PCI DSS準拠相当

課題

・クレジットカード・セキュリティGLでの規定明確化・詳細化
・不正利用対策／脆弱性対策の向上や、加盟店への強化したセキュリティの決済システムの提供

利用者

現状の対応

・IC決済

課題

・EC決済における本人認証の徹底
・フィッシング被害

販売業者

現状の対応

・クレジットカード番号非保持化対応

課題

・EC決済における本人認証の徹底
・ECサイトにおける脆弱性対策の強化

関係省庁

経済産業省

・割賦販売法に基づく監督・検査
・消費者からの相談受付・相談事例の収集
・消費者被害防止に向けた注意喚起

警察庁

・各種罰則に基づく検挙活動
・サイバーインシデント対応／フィッシング対策
－サイバー警察局

内閣サイバーセキュリティセンター（NISC）

・重要インフラ事業者（クレジット分野で約50社指定）のサイバーセキュリティ対策

消費者庁

・消費者被害防止に向けた注意喚起

関係団体等

日本クレジット協会（JCA）

・認定割賦販売協会
・クレジット取引セキュリティ対策協議会事務局

フィッシング対策協議会

・フィッシングに関する情報収集／提供／動向分析

日本サイバー犯罪対策センター（JC3）

・サイバー犯罪等のサイバー空間の脅威に対し、情報共有や手口分析等

3．クレジットカード番号セキュリティ対策の３つの方向性

クレジットカード会社等　加盟店　利用者　PSP等

2022年6月2日　第30回割賦販売小委員会資料2－2より抜粋

目的意識	これまでの取組	今後の方向性
クレジットカード番号を安全に管理する（漏えい防止）		
▌クレジット決済に関与するプレイヤーは、クレジットカード番号を取り扱う上でシステム等の安全性を確保する	✓ 割賦販売法に基づく対応 （クレジットカード番号等の適切管理規定） － PCI DSS準拠相当 － 非保持化	✓ さらなる制度的措置の検討 －クレジットカード・セキュリティガイドラインでのアップデート ✓ 加盟店やPSP等のECサイト、システムの脆弱性対策の強化
クレジットカード番号を不正利用させない（不正利用防止）		
▌決済を承認する際には本人認証を行い、なりすましをさせない	✓ 割賦販売法に基づく対応 － 対面取引におけるIC決済の推進 － 非対面取引における本人認証の導入 （セキュリティコード・静的パスワード等における認証）	✓ 特に非対面取引における本人認証の原則化 ✓ 本人認証方法の高度化 生体認証・ワンタイムパスワード等といった強力な本人認証方法を推進 ⇒EMV-3Dセキュアの普及
▌決済取引をモニタリングし、不正利用を検知する	✓ クレジットカード会社等における個社での不正検知の取組 ✓ 明細、利用履歴の確認（クレジットカード会社等における明細通知・利用者における確認）	✓ 共同システムの構築・新しい技術や方法に基づく不正利用検知のイノベーション ✓ 明細による確認強化（リアルタイム通知等、利用者へのアラート機能の充実）
クレジットの安全・安心な利用に関する周知・犯罪の抑止		
▌利用者は、悪意を持った第三者からのフィッシング被害に遭わないよう対策を行う	✓ フィッシング対策協議会や日本クレジット協会等における周知啓発	✓ フィッシング対策に向けた多層的な取組（送信ドメイン認証（DMARC）等） ✓ 周知啓発の強化 ✓ 事業者と行政機関等における連携強化
▌漏えい防止・不正利用防止で行き届かない部分については、執行で対応	✓ 割賦販売法第49条の２（クレジットカード番号の不正利用・取得）／不正アクセス禁止法等に基づく執行対応	✓ 経済産業省と警察庁（サイバー警察局等）との連携強化

4．安全・安心なクレジットカード決済環境の進展と今後のロードマップ（イメージ）

2022年6月2日　第30回割賦販売小委員会資料2－2より抜粋