ペイメントナビ　セミナー講演資料

加盟店における不正使用対策及び改正割賦販売法について

2019年9月4日

ユーシーカード株式会社

UC CARD

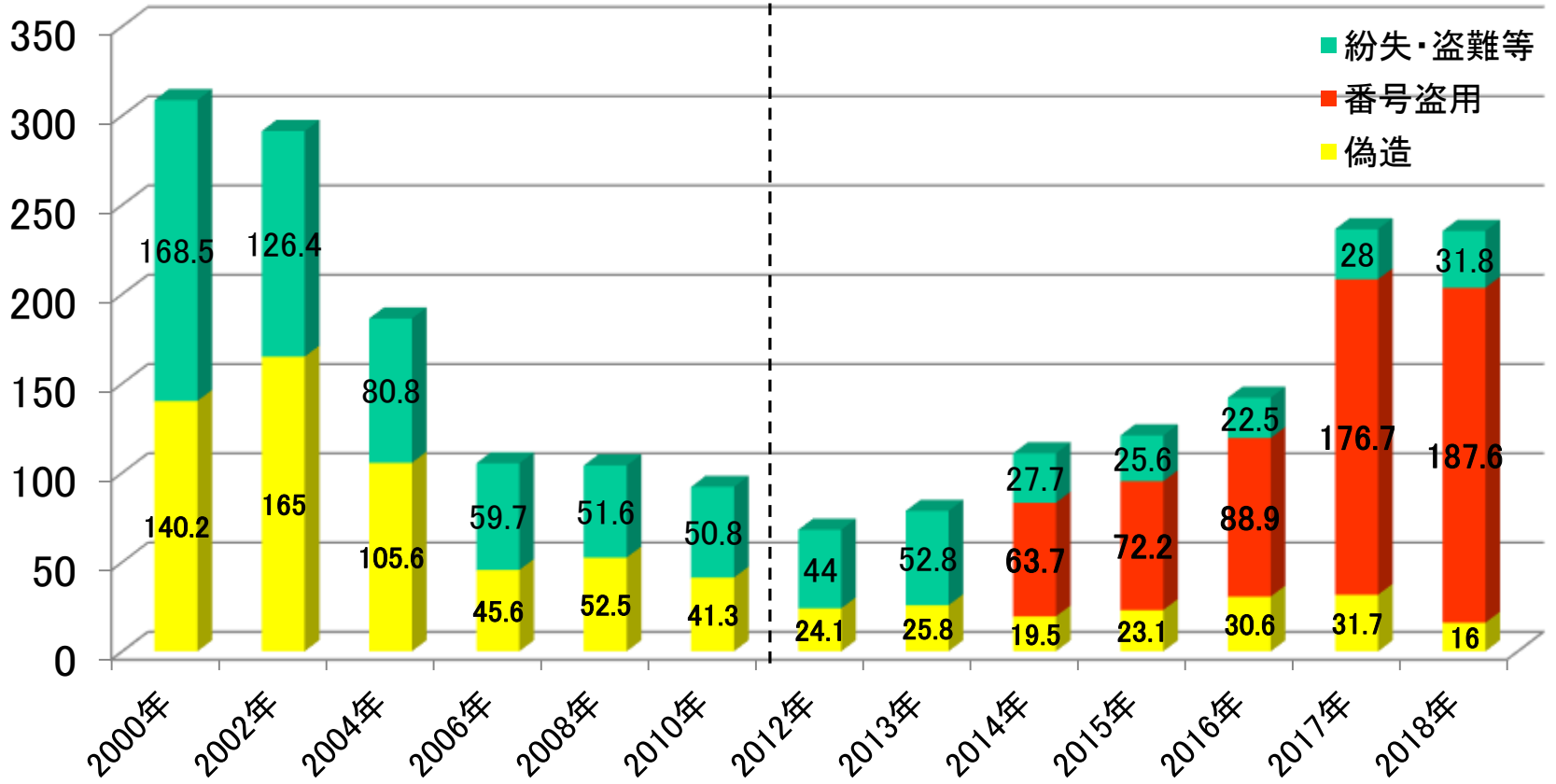
目　次

1. 不正使用の発生状況

UC CARD

＜クレジットカード不正利用被害の発生状況＞

（単位：億円）



出典：一般社団法人日本クレジット協会

1. 不正使用の発生状況

UC CARD

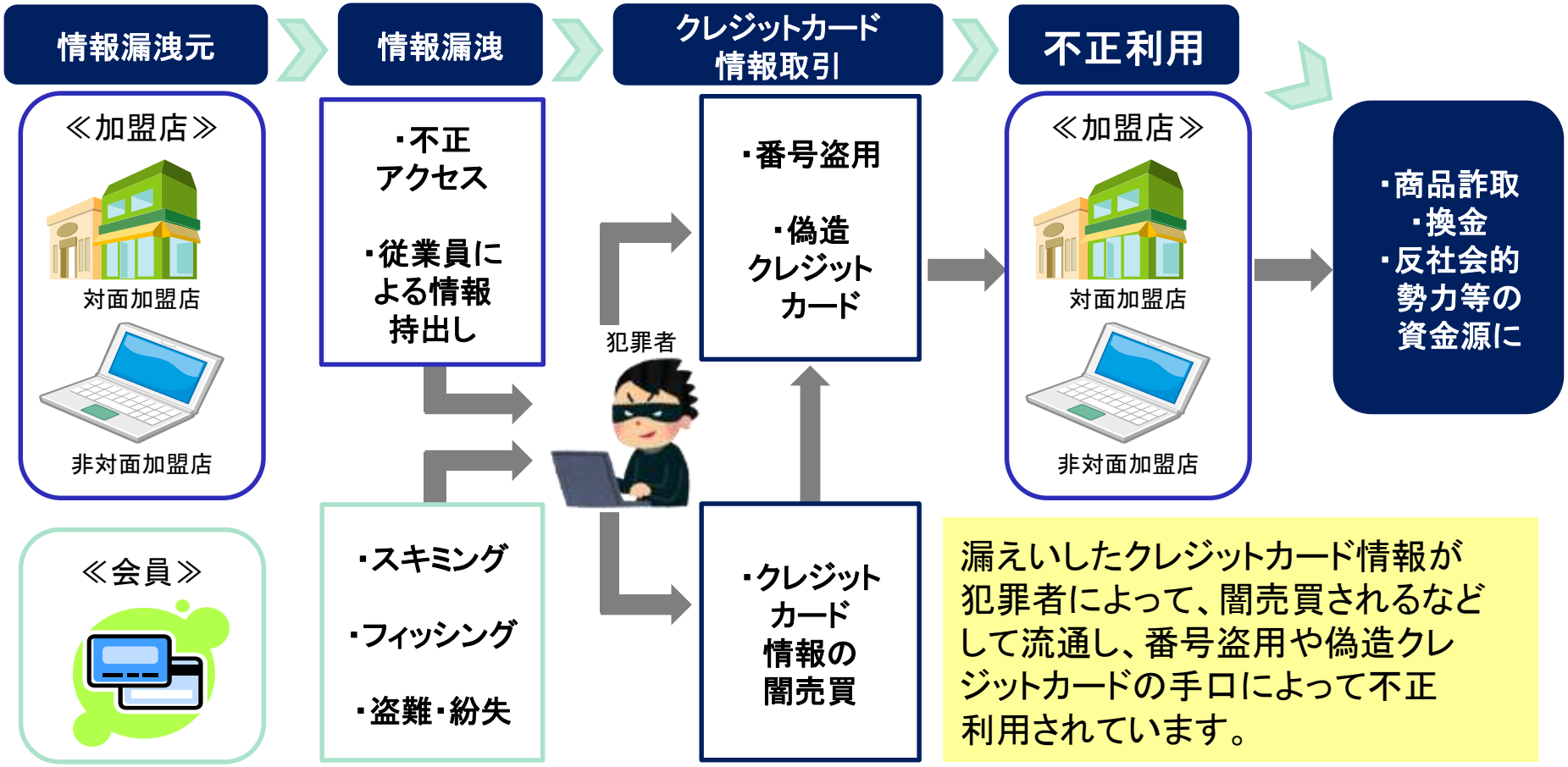
不正使用傾向の比較

時　期	2000～2004年ごろ	2017年～現在
手　口	盗難紛失、偽造	番号盗用
主　な　商　材	ガソリンスタンド、 有料道路通行料、 宝飾・高級ブランド品等	たばこ、化粧品、 デジタルコンテンツ、 旅行系商品等
不　正　使　用　犯	日本人、外国人	外国人が主流

1. 不正使用の発生状況

UC CARD

クレジットカード不正利用の概要



漏えいしたクレジットカード情報が犯罪者によって、闇売買されるなどして流通し、番号盗用や偽造クレジットカードの手口によって不正利用されています。

1. 不正使用の発生状況

UC CARD

主なクレジットカード犯罪の種類（1）

種類	手口	詳細
番号盗用	クレジットカード番号等の情報のみで不正利用する	非対面加盟店（主にインターネット加盟店。通販サイト、オンラインゲーム、電子マネー購入サイト等）において、不正に入手したクレジットカード番号等の情報のみで利用して決済する。
偽造カード	クレジットカードを偽造する	真正クレジットカードの磁気情報を上書きしたり、所要の文字・マーク等を刻印・印刷した生カードに不正に入手した真正クレジットカードの磁気データを入力するなどして偽造クレジットカードを作製し、不正利用する。 IC取引が主流の諸外国に比べ、磁気取引が主流の日本が「セキュリティホール」として狙われている。

1. 不正使用の発生状況

主なクレジットカード犯罪の種類（2）

種類	手口	詳細
盗難・紛失	真正クレジットカードを盗む、拾う	真正クレジットカードを盗む、または紛失した真正クレジットカードを拾って、本人以外の第三者が不正にクレジットカードを利用して決済する。
ぼったくり	不当に高額な代金を請求する	繁華街等において客引き等により会員を巧みに来店させ、不当に高額な飲食代金を請求する。威圧的な態度をとる場合や、近隣のATMへ強引に連れていく場合もある。

1. 不正使用の発生状況

UC CARD

主なクレジットカード犯罪の種類（3）

種類	手口	詳細	
特殊詐欺	カード手交型詐欺など	金融庁や百貨店等を騙って消費者に電話をかけ、自宅を訪問して、クレジットカード等を不正に詐取して、不正利用する。	
その他	真正クレジットカードを騙し取る	虚偽入会	免許証・保険証などを偽造してクレジットカードの入会申込みをして、真正クレジットカードを詐取する。
		なりすまし再発行	第三者が会員の個人情報を盗み、会員になりすまして紛失届・住所変更等をして、再発行される真正クレジットカードを詐取する。

2. 不正使用対策

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

改正割賦販売法の施行（2018年6月）により、**カード会社及び加盟店において、クレジットカード番号等の適切な管理や不正使用の防止といったセキュリティ対策が求められました**。

また、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、「実行計画」が掲げられており、この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ます。

2. 不正使用対策

セキュリティ対策の3つの柱

①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** ・カード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化」の実現
③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 （3Dセキュア等の本人確認、不正利用配送先情報の蓄積等）

出典：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-

2. 不正使用対策

対面加盟店における対策

実行計画では、偽造カードによる不正使用防止のため、以下の対策を掲げており、2020年3月までに対応することが求められています。

＜クレジットカード会社＞
　発行するクレジットカードへのICチップ搭載（IC化）

＜加盟店＞
　クレジットカード決済端末（CCT、POS）のIC読取に対応

偽造が困難なICカードによる決済を普及させるため、クレジットカード、クレジット決済端末の両面からIC化対応を推進しています。

2. 不正使用対策

非対面加盟店における対策①

対　策	概　要
本人認証	（1）3Dセキュア カード会員のみが知るカード会社（イシュアー）に事前に登録したパスワード等をカード利用時にイシュアーが照合することにより、本人が取引を行っていることを確認するもの （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て、カード会員の属性情報等を送信し、カード会社に予め登録されている属性情報等と照合し、利用者本人が取引を行っていることを確認する手法

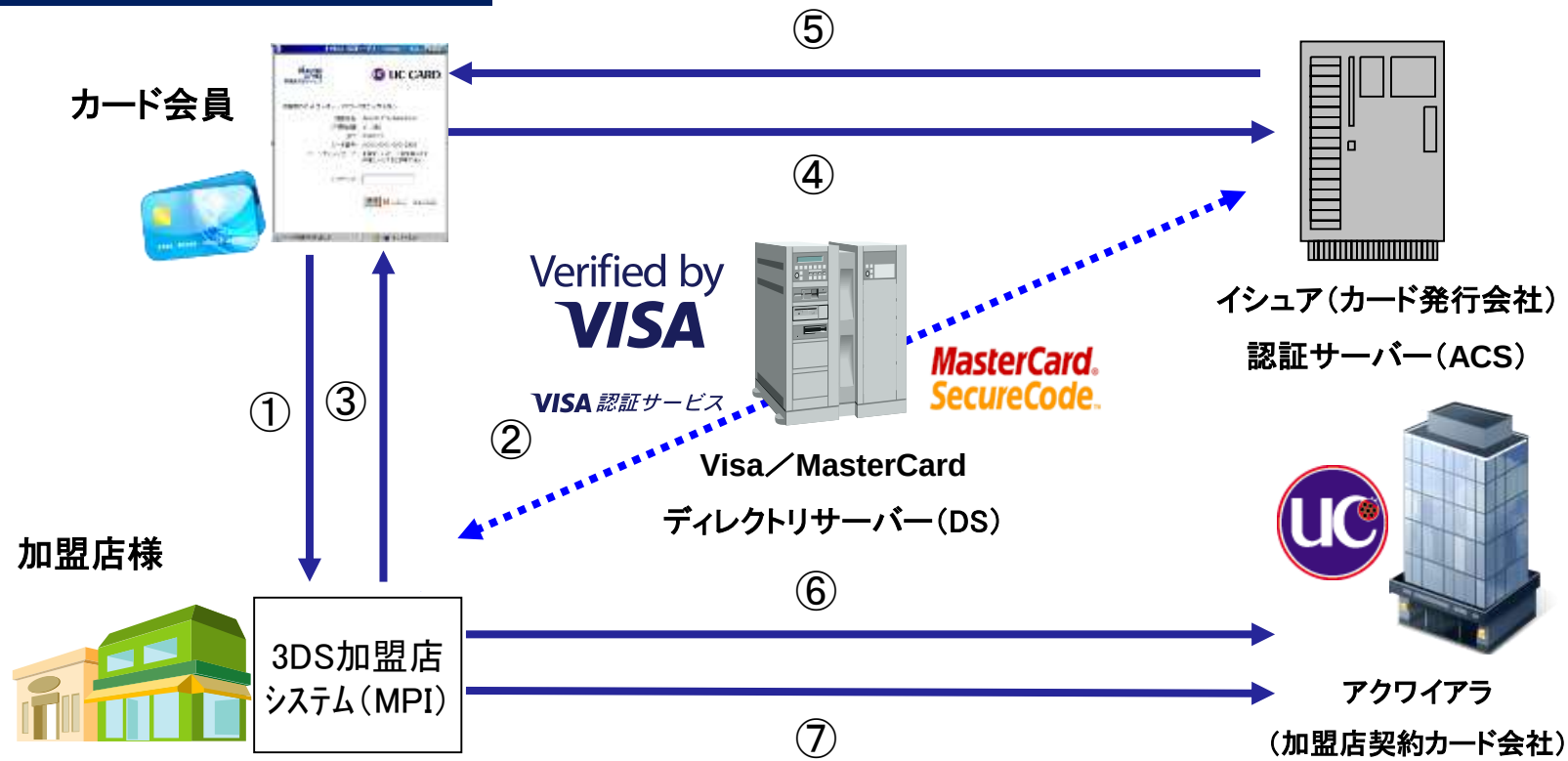
3Dセキュアは静的（固定）パスワードによる認証手法であるため、真正利用の阻害や、情報漏洩、パスワード使い回し等により効果が減退する恐れがあります。

近い将来移行が予定されている3Dセキュア「バージョン2.0」は、個々の取引におけるリスク度合いに応じてパスワード入力を求めるため、真正利用阻害の軽減が見込まれています。

2. 不正使用対策

UC CARD

（参考）3Dセキュア概要図



① 購入申込・決済	③ パスワード入力要求	⑥ カード利用承認（オーソリ）
② 認証サーバーがカード発行	④ パスワード送信	※認証データ含む
会社/会員の登録状況を確認	⑤ 本人確認結果送信	⑦ 売上データ

2. 不正使用対策

非対面加盟店における対策②

対　策	概　要
券面認証 （セキュリティコード）	カード利用時に入力されたカードの裏面又は表面に記載される3桁～4桁の数字をオーソリ時に合わせて送信し、イシュアーが照合することにより、当該カードの真偽を確認する手法

セキュリティコードは自体がカード側に100%普及しているほか、カード会員が忘れる懸念がないことや加盟店側の導入障壁が比較的低いという利点がある一方、前項の「本人認証」同様、情報漏洩や使い回しにより、認証を突破される懸念があります。

なお、セキュリティコードは桁数が限られるため、クレジットマスター（膨大な連続申込みを試み正当なコードを探り当てる手法）により突破される懸念があります。

2. 不正使用対策

UC CARD

非対面加盟店における対策③

対　策	概　要
属性・行動分析 （不正検知システム）	カード会員が操作するブラウザやアプリから抽出するデバイス（PC パソコンやスマートフォン等）情報の組合せ、またはそれらの情報に加盟店等が保有する取引情報等を更に組合せ、システム的に分析の上、リスク度合をスコアリング等によって表し、当該カード取引の不正判別を行う手法

属性・行動分析（不正検知システム）で収集する購入者のデバイス情報は、通常、クレジットカード会社では取得できない情報であり、これを活用することで不正検知精度の向上が期待できます。

なお、不正取引の手口や傾向は変化するため、傾向を分析し検知システムの条件設定を適宜更新し続けていくことがとても重要です。

2. 不正使用対策

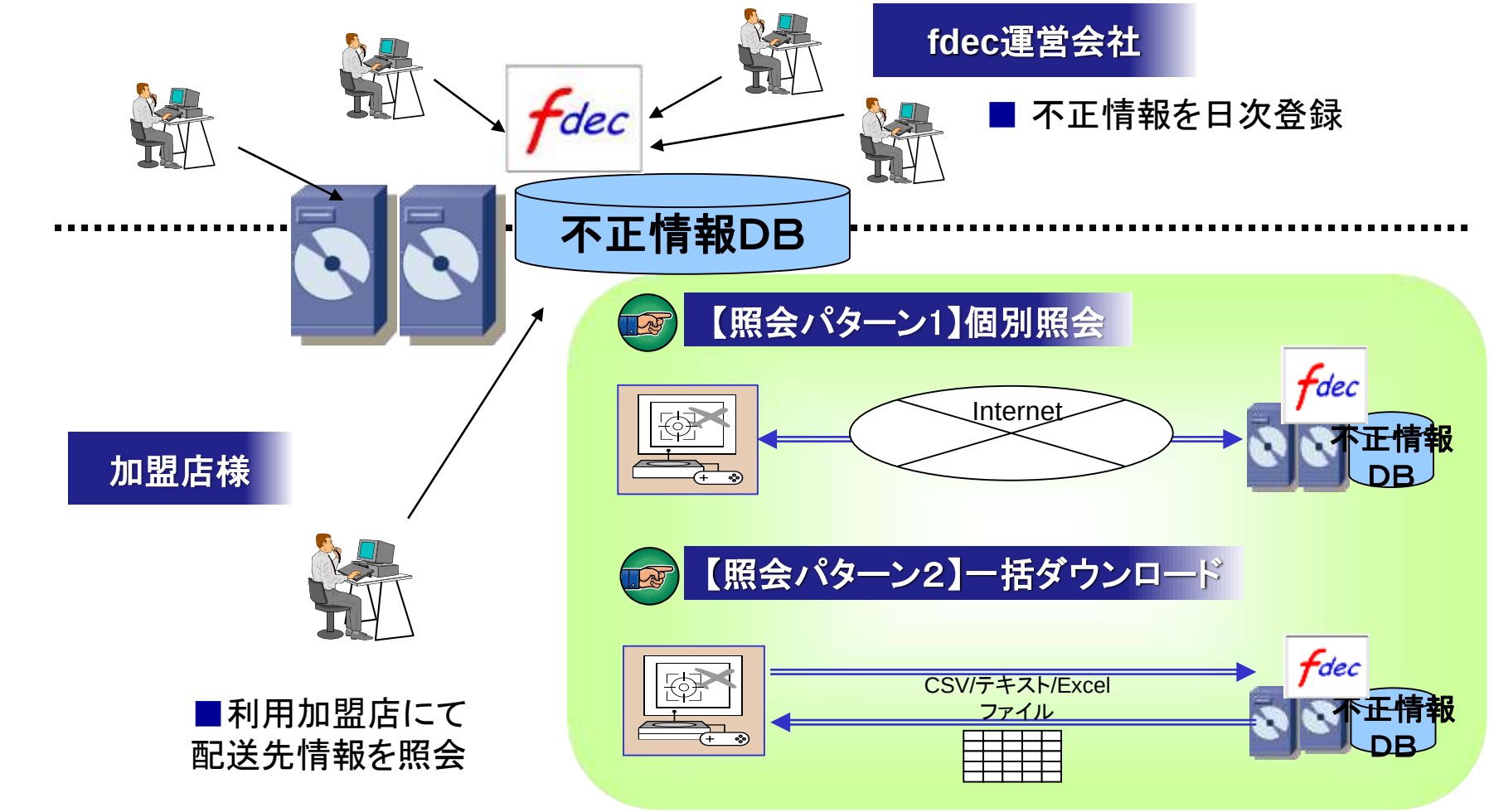
非対面加盟店における対策④

対　策	概　要
配送先情報	不正利用された注文等の配送先情報を蓄積することで、 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 加盟店独自で過去の不正配送先のネガデータを蓄積するほか、 クレジットカード会社が共有する過去の不正配送先情報を照会 する方法（F-dec）もあります。

2. 不正使用対策

UC CARD

（参考）F-dec概要図



2. 不正使用対策

UC CARD

対策の導入基準

（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、オンラインオーソリ
（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扱う加盟店
　　【対策】実行計画が掲げる4方策のうち、1方策以上の導入
（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】実行計画が掲げる4方策のうち、2方策以上（※2）の導入

（※1）デジタルコンテンツ（オンランインゲームを含む）、家電、電子マネー、チケット
（※2）4方策のうち2方策以上を導入しても不正被害が減少せず、引き続き不正顕在化が継続する場合、加盟店はカード会社による不正利用発生状況の情報共有を受け、不正利用防止に向けた追加的な方策導入の継続的な検討が求められる

出典：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-

３．加盟店へのアプローチ（法施行前）

アクワイアラーとして、不正多発先（チャージバック受入上位先）の加盟店を中心にセキュリティ対策の導入を推進。
しかしながら、以下の理由から対策の導入スピードは緩やか。

＜対面加盟店＞
- IC対応端末の導入に向けた費用負担

＜非対面加盟店＞
- なりすまし防止のセキュリティ対策導入に向けた費用負担
- カート落ち等、真正利用阻害の発生懸念

4. 加盟店へのアプローチ（法施行後）

UC CARD

セキュリティ対策が法令要件となり、加盟店の不正対策の導入が進展。
特に不正継続発生時の追加的な対策が進んでいます。

＜事例１＞
【従来】本人認証、券面認証、属性・行動分析、配送先情報
＋
【追加】利用確認（不審取引について商品発送前にカード会社へ利用確認する運用）

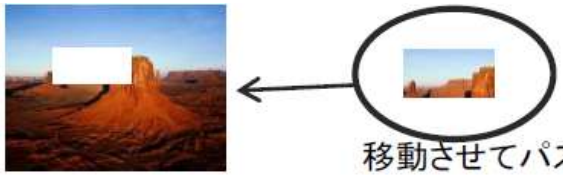
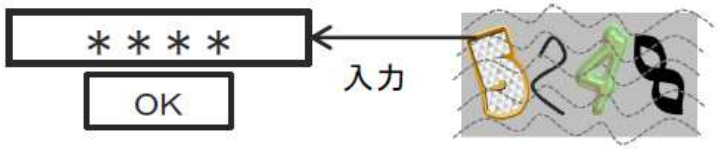
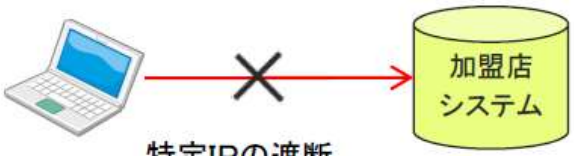
＜事例２＞
【従来】本人認証、券面認証
＋
【追加】加盟店独自で構築したネガDB（申込者・配送先）との照合

実行計画に掲げる4方策に加え、加盟店の取扱商材や配送方法等に応じた追加の方策を導入することで、不正抑止を図っています。

5. アプローチの課題とさらなる取組み

UC CARD

一方で、セキュリティ対策を導入した後も不正が継続する場合も散見されています。
特に非対面取引（なりすまし）は、4方策の全てを導入しても不正が継続する場合があり、前頁に記載の対策のほか以下のような対策が有効です。

対　策	内　容	イメージ
1. パズル認証	サイト上に表示されたパズルを完成させ、人間による操作であることを認証	
2. キャプチャー認証	表示された文字列と同じ文字列を入力させることで、人間によるログイン操作であることを認証	
3. IPアドレスの遮断	クレジットマスター等による攻撃時に特定のIPアドレスを遮断	
4. アカウント停止	不正利用発生アカウントの停止	

６．最後に

改正割販法の施行によって、海外と比較し出遅れていた
クレジットカード不正使用対策は大きく進展することとなりました。

一方で、対策を導入しても不正が継続したり、これまでになかった
新たな不正手口が登場しています。

不正使用を継続して抑止するため、新たな不正手口と対策の
研究が必要です。また、対策の導入に当たっては加盟店と
クレジットカード会社の協力・連携が重要であり、関係者一体と
なり、今後も対応を進めて参ります。

ご清聴いただき、ありがとうございました。