資料４－２

最近の主な漏えい事案

令和４年８月４日

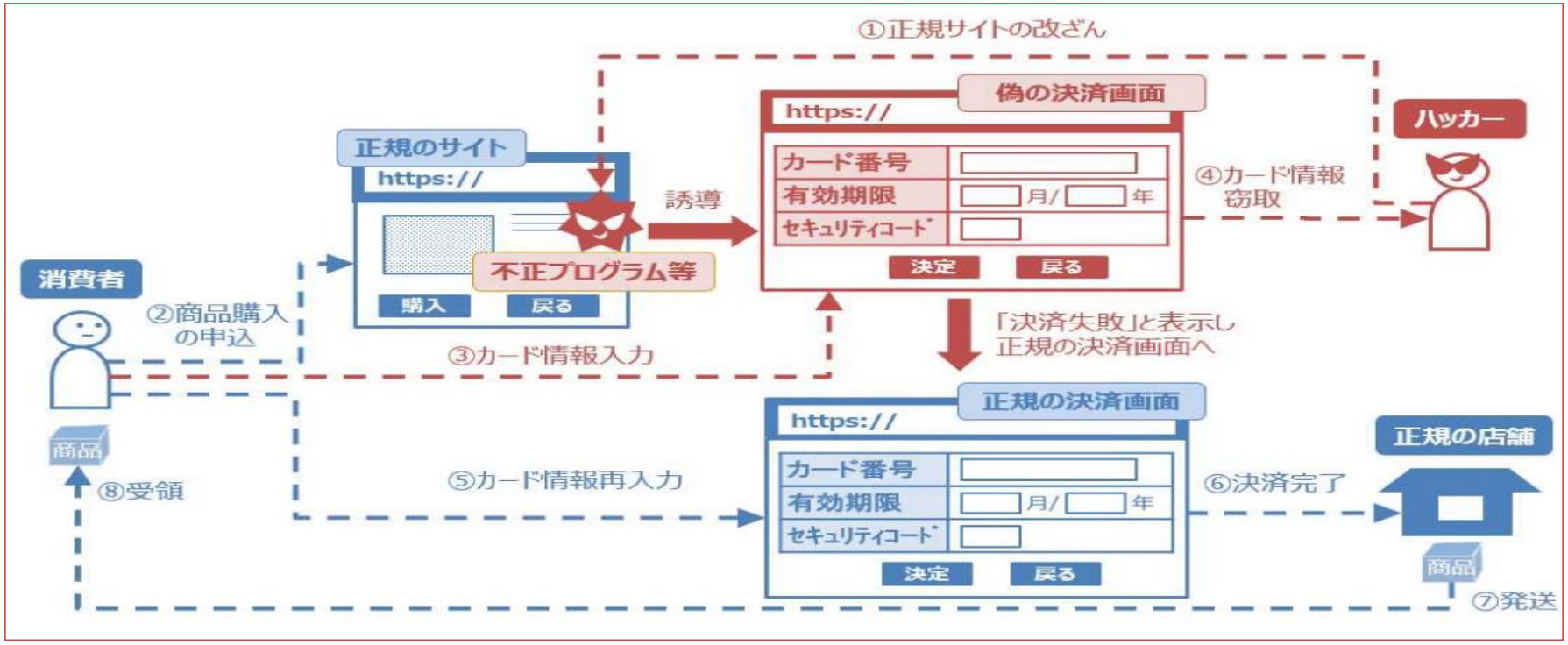
経済産業省　商務・サービスグループ

商取引監督課

漏えい事案①：ECサイト加盟店

2022年6月2日開催第30回割賦販売小委員会資料2－1より抜粋

- 特にオープンソースにより構築され、自社（委託先含む）で適切なアップデートを行わないなど、十分なセキュリティ対策を講じていないECサイトの脆弱性を狙った不正アクセス等による漏えい事案が増加。クレジットカード番号等を保持していなくとも、**ECサイト自体が改ざんされることで、不正ファイルの設置や偽の決済サイトへの誘導でクレジットカード番号等が流出。**
- 当省でも加盟店に対する注意喚起を実施(令和元年12月）。IPAとも連携。
- しかしながら、**ECサイトでのサイバー攻撃によるクレジットカード番号漏えい事案は増加**（約２割増（うちオープンソース関連は、約４割増加）。



消費者庁・経済産業省「インターネットショップでのクレジットカード番号の漏えい・不正利用に注意しましょう」（令和２年２月13日）
https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/pdf/consumer_policy_cms104_200218_01.pdf

(追補)漏えい事案①：ECサイト加盟店の非保持化の限界

- 平成28年法改正以降、**ほぼ全てのECサイト**が、クレカ番号等の**非保持化を選択。**
- 非保持化により、漏えい時の**被害は小規模化**したがと想定されるが、**漏えい事案は増加傾向。**
- **非保持化だけでは漏えい対策は不十分**との認識がなく、サイトの脆弱性対策等が喫緊の課題。

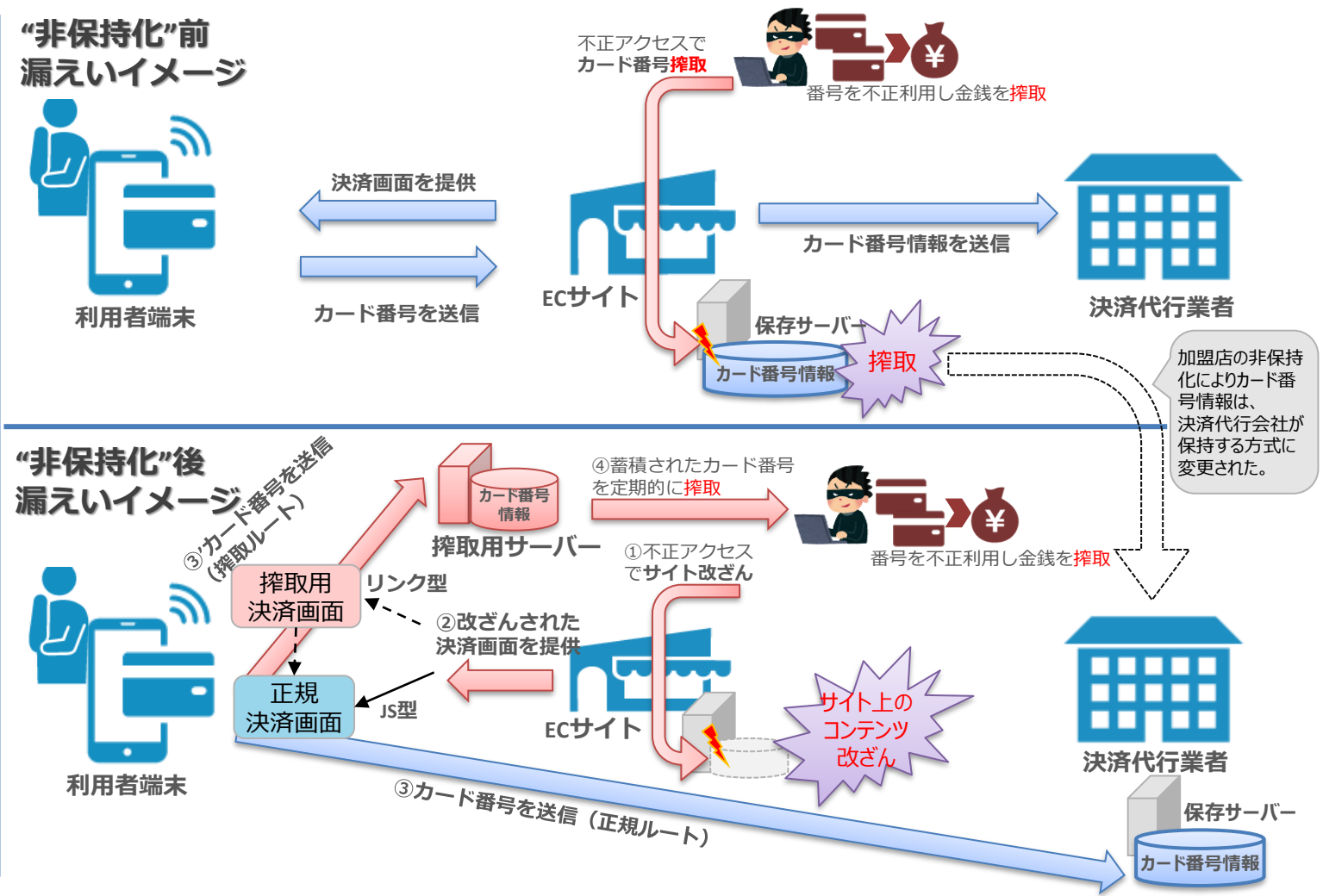
“非保持化”を実現する決済処理方式は「リンク型」と「JS型」の２種類が存在

・「リンク型」改ざん遷移例

②決済画面
（ECサイト：リンク先が改ざん）
↓
③’カード番号入力画面
（搾取用決済画面）
③’搾取用サーバにカード番号送信
↓
③カード番号入力画面
（正規決済画面
（決済代行業者提供））
③ 決済代行サーバにカード番号送信
↓
②決済完了画面
（ECサイト）

「JavaScript(JS)型」改ざん遷移例

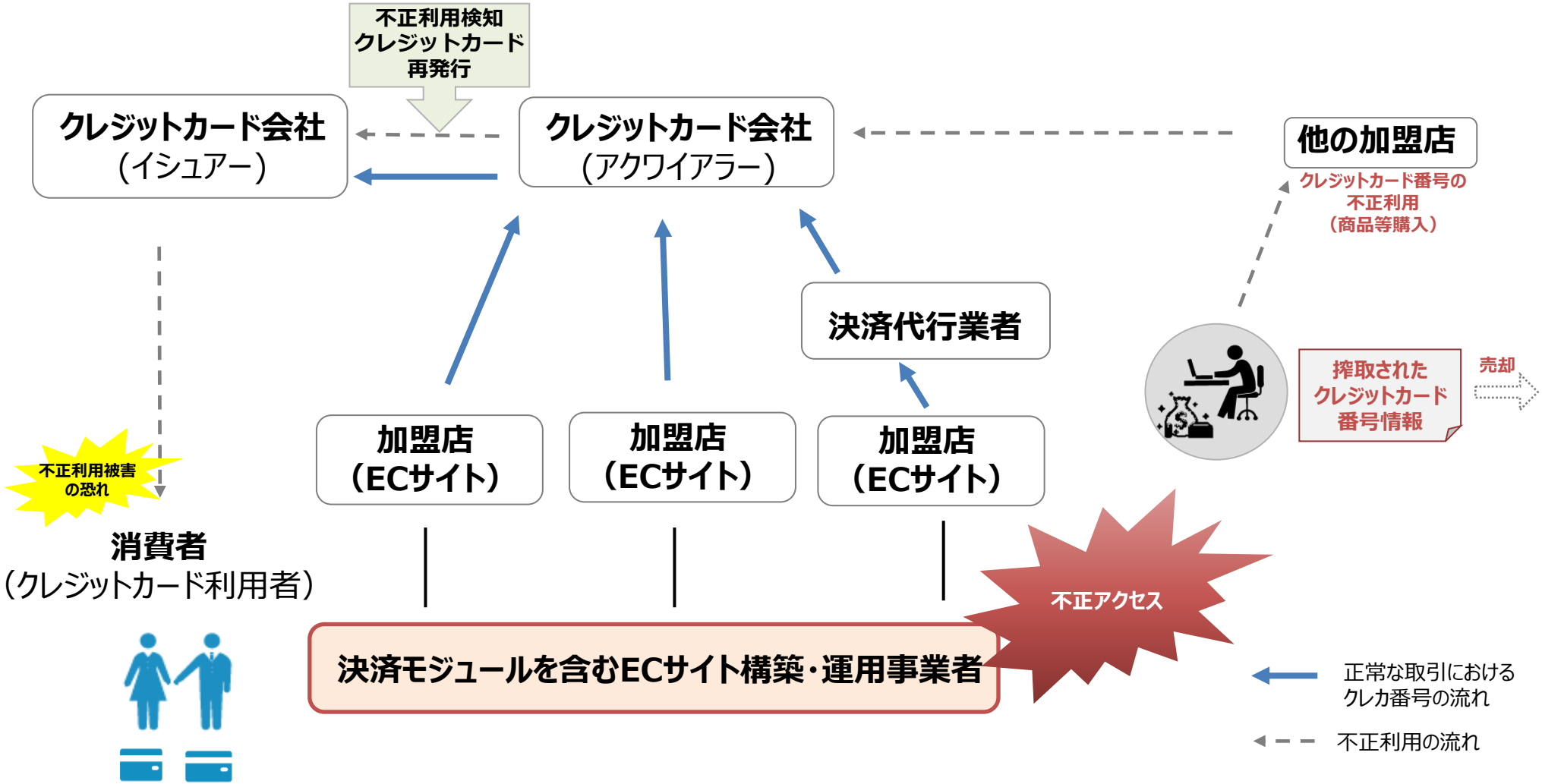
②決済画面
（ECサイト：送信処理が改ざん）
↓
③カード番号入力画面
（正規・搾取用決済画面）
③’搾取用サーバにカード番号送信
③ 決済代行サーバにカード番号送信
↓
②決済完了画面
（ECサイト）



漏えい事案②：ECシステム提供者

2022年6月2日開催第30回割賦
販売小委員会資料2－1より抜粋

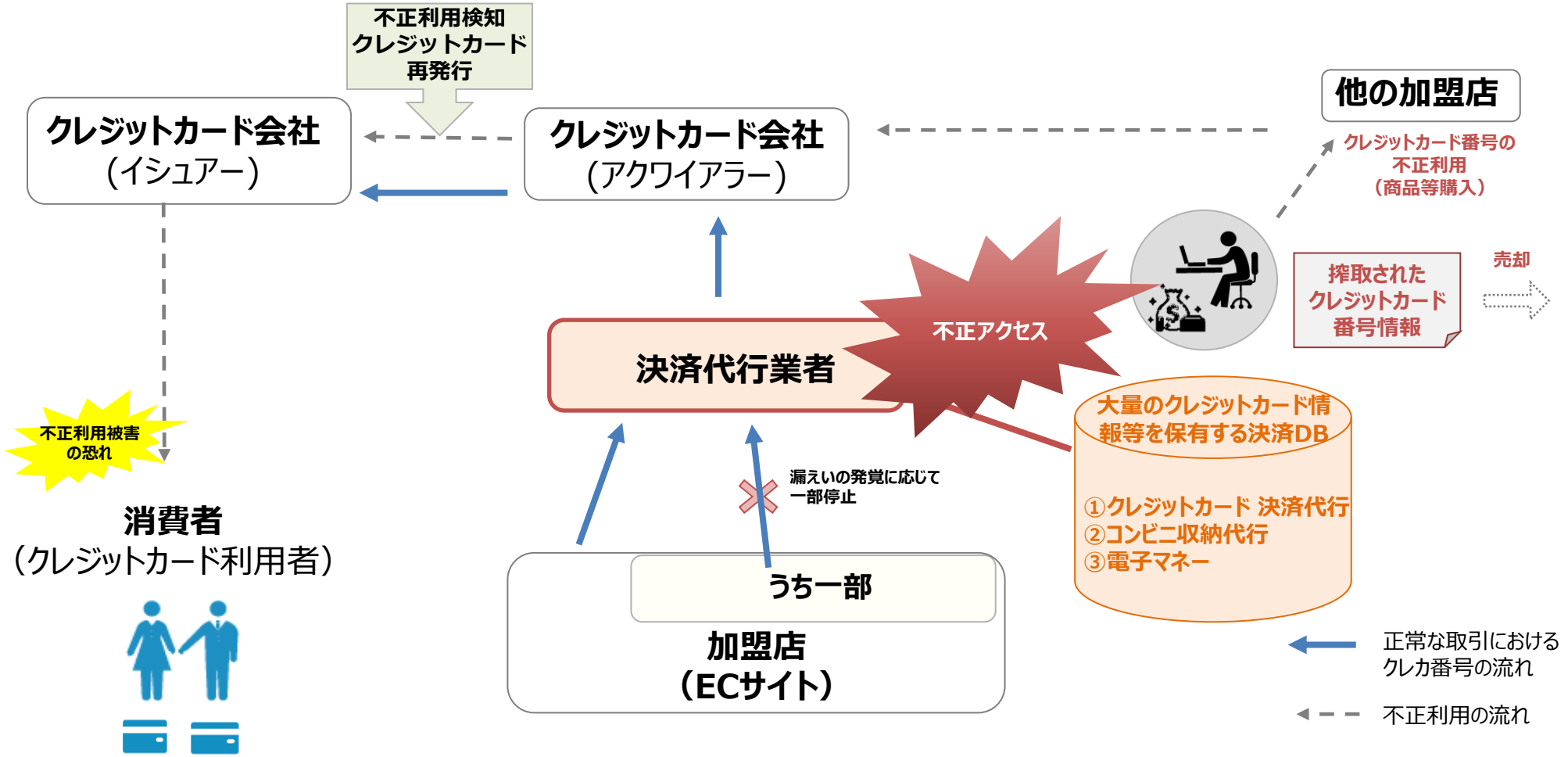
- ECサイトでの漏えいは、決済モジュールを含むECサイトを構築・運用する事業者のサーバーへの不正アクセスを起因とするものも発生。この場合、**一事案であっても、漏えいの規模が広くなる**（関連するECサイトは約９事業者）。



漏えい事案③：決済代行業者

2022年6月2日開催第30回割賦販売小委員会資料2－1より抜粋

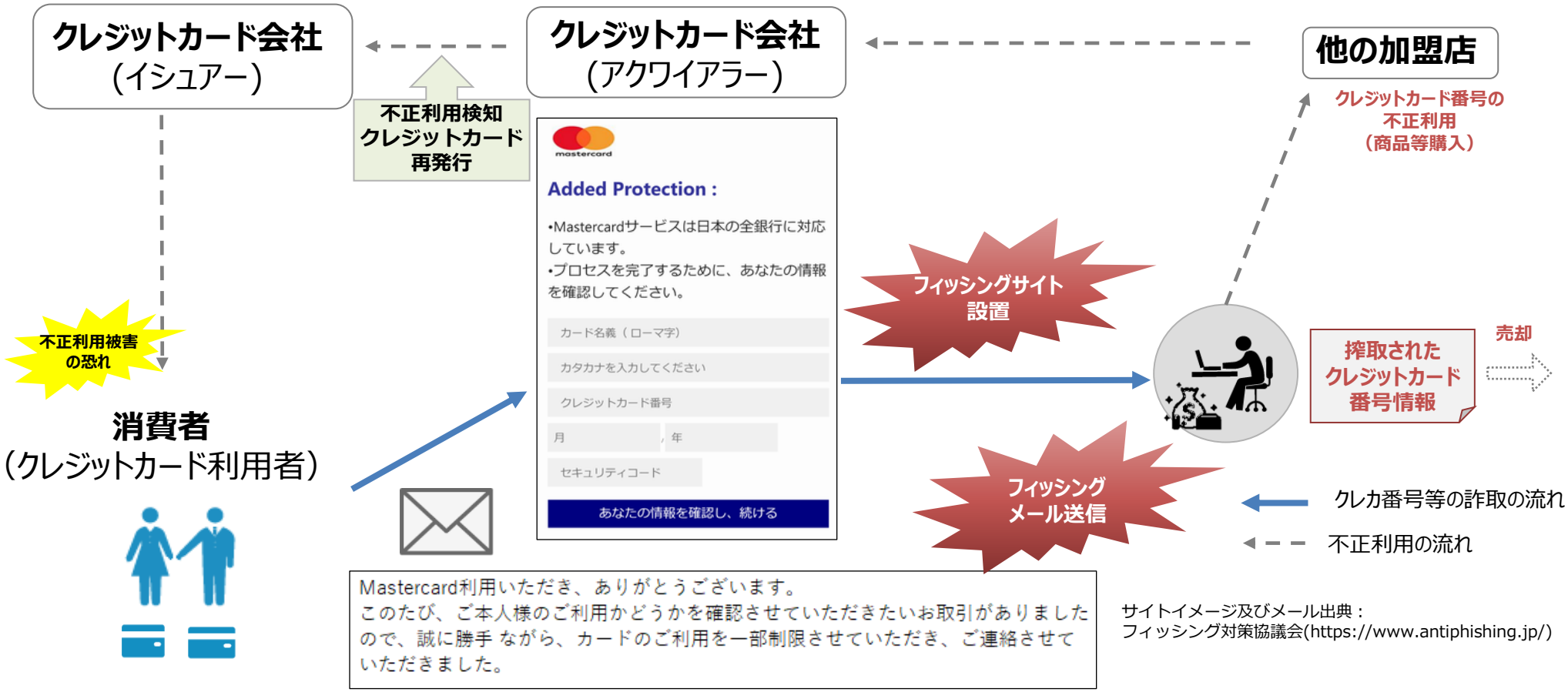
- クレジットカードの決済代行業者の**大量の情報を保有するデータベース**（約46万件のクレジットカード番号等を含むトークン方式クレジットカード決済情報データベース、約240万件のクレジットカード番号等が含まれる決済情報データベース）**への外部からの不正アクセス**により、同社が運営する複数の決済サービスにおいて、決済情報の大規模な漏えいが発生。令和２年法改正後、初めての事案。



漏えい事案④：消費者（フィッシング被害）

2022年6月2日開催第30回割賦
販売小委員会資料2－1より抜粋

- サイバー攻撃によるクレジットカード番号盗用以外にも、**消費者自身が偽サイトにクレジットカード番号やID・パスワード等を入力する**フィッシングによるクレジットカード番号等の漏えい事案も存在。



サイトイメージ及びメール出典：
フィッシング対策協議会(https://www.antiphishing.jp/)