Cashless Security Report

Quarterly Report

2023年(4-6月版)

fjconsulting, INC.

2023.10.12

キャッシュレス・セキュリティレポート
ー2023年4～6月版ー

かっこ株式会社
ｆｊコンサルティング株式会社

はじめに

かっこ株式会社とｆｊコンサルティング株式会社が、カード情報流出とECサイトの不正被害の実態を把握するため、独自調査・データをもとにまとめたレポートです。

コンテンツ

1. カード情報流出事件の概況（2023年4-6月）
（1）カード情報流出事件数・情報流出件数の推移
（2）業種/商材別・情報流出期間別事件数・流出件数
（3）2023年4-6月 カード情報流出事件のトピック
　カード情報流出事件が減少する一方、銀行の不正送金被害が過去最高に
（4）クレジットカード情報保護対策に関する考察
　警察庁と経済産業省がサイバー攻撃によるカード情報流出防止対策推進の覚書を締結

2. ECにおける不正利用の概況（2023年4-6月）
（1）クレジットカード不正利用被害額の推移
（2）ECサイト不正利用の傾向
（3）2023年4-6月 不正利用のトピック
①専門知識がなくても、フィッシング詐欺を可能にするフィッシングキット「16SHOP」：
　日本とインドネシアによる国際共同調査で初の逮捕に
②不正注文における分業化、巧妙化が進む：コード決済不正利用

1. カード情報流出事件の概況（2023年4-6月）

（1）カード情報流出事件数・情報流出件数の推移

2023 年4月-6月のカード情報流出事件

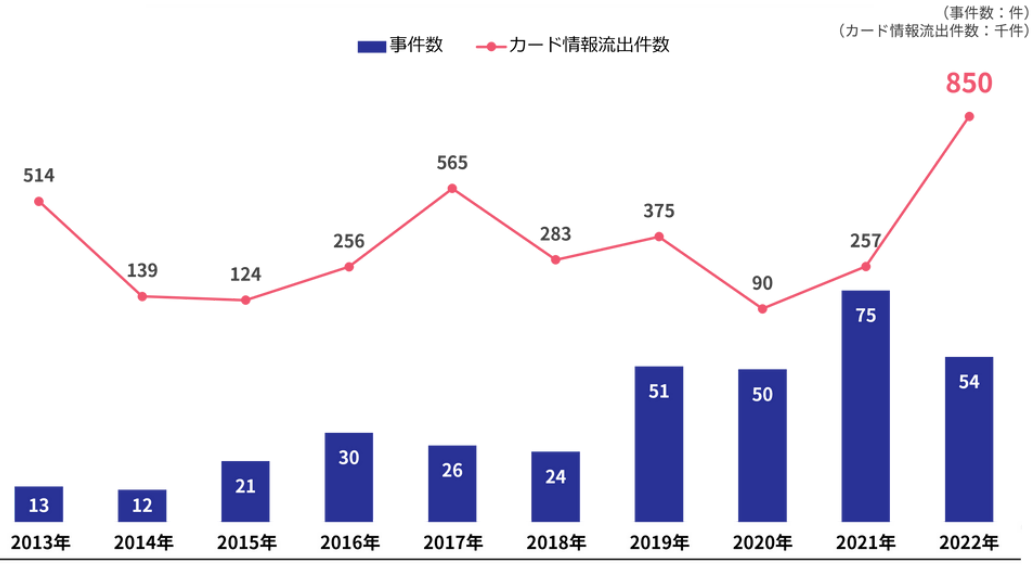
- 事件数　5件
- カード情報流出件数　301,545件

※クレジットカード、ブランドデビットカード、ブランドプリペイドカードを含む

【調査方法】

かっこｆｊコンサルティングが、各社の公式サイトや報道などの公開情報により事件を特定し、集計

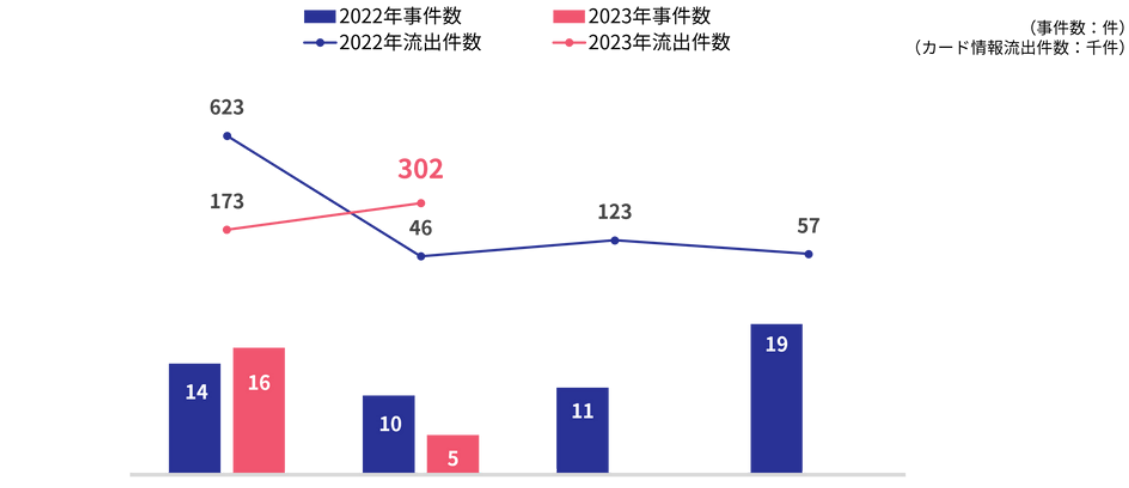
2022年までのカード情報流出事件数・情報流出件数の推移



	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年	2022年
事件数(件)	13	12	21	30	26	24	51	50	75	54
カード情報流出件数(件)	514,369	138,717	123,527	255,689	564,844	283,374	375,479	89,628	256,822	849,950

（かっこ・ｆｊコンサルティング調べ）
※2021年以前のデータはｆｊコンサルティング調べ

2023年のカード情報流出事件数・情報流出件数(前年比較)



		1～3月	4～6月	7～9月	10～12月
2022年	事件数(件)	14	10	11	19
	カード情報流出件数(件)	623,491	46,429	122,829	57,201
2023年	事件数(件)	16	5		
	カード情報流出件数(件)	173,322	301,545		

（かっこ・ｆｊコンサルティング調べ）

期間中のカード情報流出事件の数は5件（うち、ECサイト4件、カード会社1件）と大幅に減りましたが、流出件数は30万件を超えました。2023年4月にカード会社の1社が、自社のダイレクトメールの表面に誤ってクレジットカード番号を印字した状態で送付するという事故があり、本件で合計290,771件と4-6月に流出したカード情報の大部分を占めています。

（2）商材別事件数・情報流出期間別事件数

＜業種/商材別の事件数(2023年1-3月)＞

業種/商材カテゴリー		事件数(件)	カード情報流出件数(件)
加盟店合計		16	173,322
業種別	アパレル	5	41,362
	コスメ	4	13,707
	食品	3	5,099
	家電・電子機器・PC	2	112,147
	生活雑貨、家具、インテリア	1	402
	アパレル／コスメ／健康食品	1	605

（かっこ・ｆｊコンサルティング調べ）

＜業種/商材別の事件数(2023年4-6月)＞

業種/商材カテゴリー		事件数(件)	カード情報流出件数(件)
加盟店合計		4	10,774
業種別	アパレル	1	6,263
	食品	1	1,830
	生活雑貨、家具インテリア	1	1,771
	その他	1	910
カード会社		1	290,771

（かっこ・ｆｊコンサルティング調べ）

＜流出期間別の事件数・カード情報流出件数＞

情報流出期間	2023年1-3月 事件数(件)	2023年1-3月 カード情報流出件数(件)	2023年4-6月 事件数(件)	2023年4-6月 カード情報流出件数(件)
3ヶ月以内	5	115,048	2	292,542
3ヶ月-1年	2	12,819	2	2,740
1-3年	8	45,432	1	6,263
3年以上	1	23	0	0

（かっこ・ｆｊコンサルティング調べ）

（3）カード情報流出事件のトピック

ECサイトからのカード情報流出事件が減少する一方、銀行の不正送金被害が過去最高に

2023年4-6月は、前四半期、対前年四半期と比較し、ECサイトからのカード情報流出事件は4件、カード情報流出件数も1万件余りと大幅に減少しました。対して、2023年2月以降、インターネットバンキングによる預金の不正送金被害が急増しています。2023年上半期（1-6月）の被害件数は過去最多の2,322件、被害金額は約30億円にのぼりました。

その手口は以下と推測されています。

① 銀行を騙ったメールやショートメッセージ（SMS）で「取引が一時的に停止されている」「個人情報の再確認が必要」などの消費者の不安を煽るメッセージを送信する

② 記載したURLからオンラインバンキングのログイン画面に似せた偽のサイト（フィッシングサイト）に誘導し、ID、パスワード、ワンタイムパスワード等のログイン情報を窃取

③ 窃取したログイン情報で正規のオンラインバンキングのサイトに不正アクセスし、預金を不正に送金

2023年8月8日、警察庁と金融庁は連名で『フィッシングによるものと見られるインターネットバンキングに係る不正送金被害の急増について（注意喚起）』を公開しました（※1）。

※1：https://www.fsa.go.jp/ordinary/internet-bank_2/10.pdf

（4）クレジットカード情報保護対策に関する考察

警察庁と経済産業省がサイバー攻撃によるカード情報流出防止対策推進の覚書を締結

2023年1月に経済産業省が取りまとめた『クレジットカード決済システムのセキュリティ対策強化検討会報告書』では、サイバー攻撃によるカード情報流出や不正利用などのサイバー犯罪対策の点で警察との連携強化が必要であるとしています。これを受けて2023年6月、経産省と警察庁は『サイバー攻撃によるクレジットカード番号等の漏えいに関する事案の情報共有等について』という覚書を締結しました（※2）。

覚書では、サイバー攻撃を起因とするECサイトからのカード番号等の漏えい、もしくはそのおそれがある事件が発生した時に、経産省から警察庁に情報提供し、警察庁は提供を受けた情報をもとに被害実態の把握や攻撃手口の分析、注意喚起などを行うとしています。また、警察庁からはカード情報窃取の攻撃手口や重大な脆弱性に関する情報について経産省に情報提供し、経産省は提供を受けた情報をクレジットカード業界のセキュリティ対策に係る指導、監督に活用するとしています。

※2：https://www.npa.go.jp/policies/disclosure/notice/document/cyber/R050630.pdf

2. ECにおける不正利用の概況（2023年4-6月）

（1） クレジットカード不正利用被害額の推移

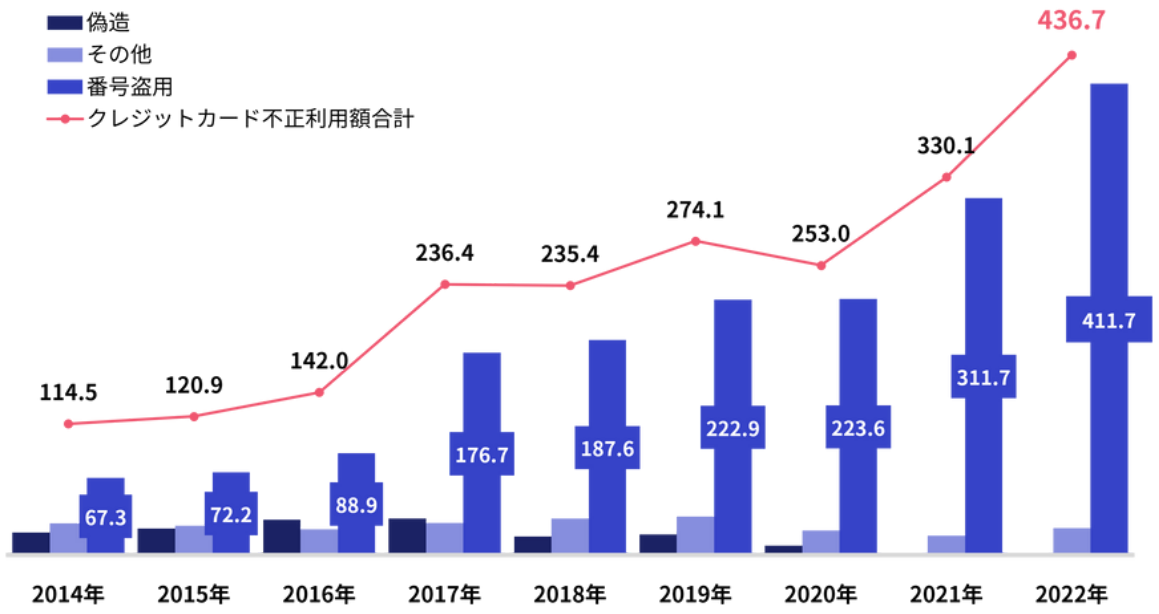
2023 年4月-6月のクレジットカード不正利用

- 不正利用被害額合計　141.0億円
- 偽造　0.5億円
- 番号盗用　132.4億円
- その他　8.1億円

※日本クレジット協会調べ
https://www.j-credit.or.jp/information/statistics/index.html

2022年までのクレジットカード不正利用被害額の推移

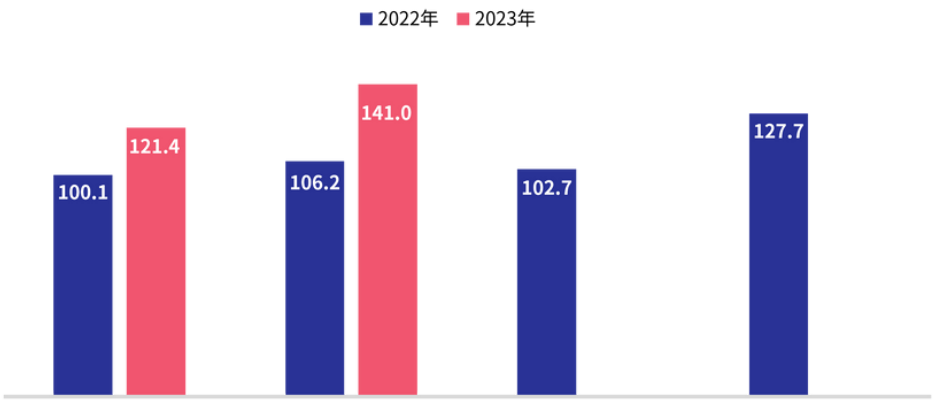
（金額単位：億円）



（『クレジットカード不正利用被害額の発生状況』日本クレジット協会）

2023年のクレジットカード不正利用被害額（前年比較）

（金額単位：億円）



		1～3月	4～6月	7～9月	10～12月
2022年	偽造	0.2	0.2	0.7	0.6
	番号盗用	94.6	100.6	95.9	120.6
	その他	5.3	5.4	6.1	6.5
2023年	偽造	0.8	0.5		
	番号盗用	113.3	132.4		
	その他	7.3	8.1		

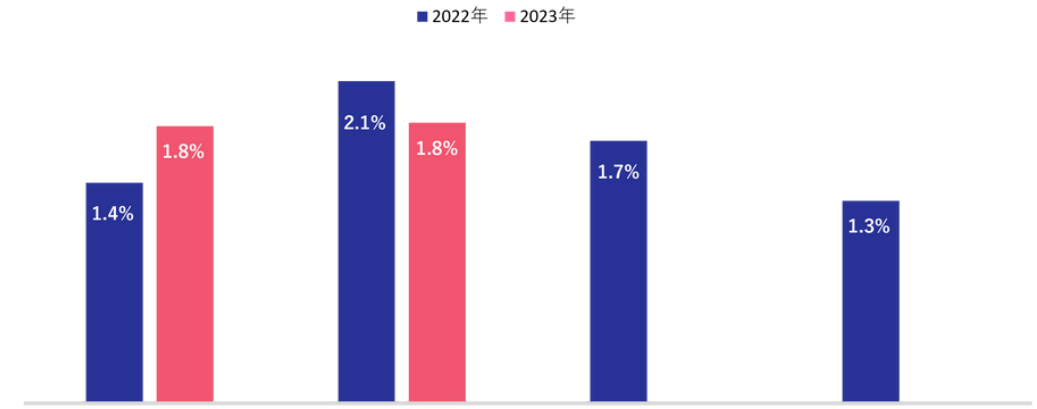
（『クレジットカード不正利用被害額の発生状況』日本クレジット協会）

2023年4月から6月の間に発生した不正利用被害額は141.0億円で、前年同期比で32.8%増加しました。その中でも、番号盗用による被害額は132.4億円で、これは前年より16.9%増加しており、2021年以降、不正利用被害全体の９割以上を占めている状況です。

（2）ECサイト不正利用の傾向

【調査方法】
不正注文検知サービス「O-PLUX」（かっこが提供するクレカ不正、悪質転売など不正注文を検知するサービス）をご利用のお客様（累計11万サイト以上）における審査結果をもとに集計

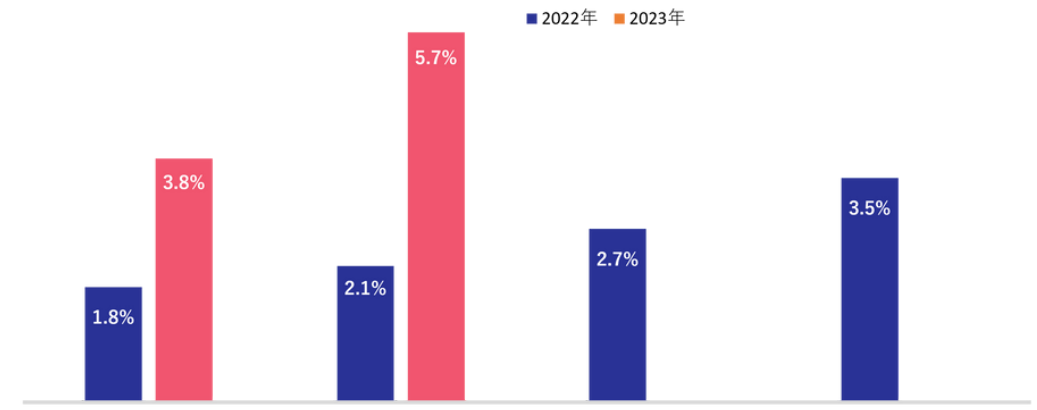
クレジットカード不正注文の発生率



	1～3月	4～6月	7～9月	10～12月
2022年	1.4%	2.1%	1.7%	1.3%
2023年	1.8%	1.8%		

※「O-PLUX」の審査で、審査件数全体に占めるクレジットカード不正注文の審査結果NG割合を件数ベースで算出。（かっこ調べ）
※最終的に出荷停止や注文を拒否するなどの対応は、「O-PLUX」加盟店判断により異なる。

転売不正注文の発生率



	1～3月	4～6月	7～9月	10～12月
2022年	1.8%	2.1%	2.7%	3.5%
2023年	3.8%	5.7%		

※「O-PLUX」の審査で、審査件数全体に占める転売不正注文の審査結果NG割合を件数ベースで算出。（かっこ調べ）
※最終的に出荷停止や注文を拒否するなどの対応は、「O-PLUX」加盟店判断により異なる。

2023年の転売不正注文について、1－3月、4－6月ともに前年比2倍以上の発生率で増加傾向が続いていますが、特に初回限定品を狙った転売不正が継続的に発生しています。

＜クレジットカード不正における狙われやすい商材ランキング＞

2023年（1-3月） 商材別不正注文検知数ランキング			
1位	ホビー・ゲーム	7位	コスメ・ヘアケア
2位	デジタルコンテンツ	8位	アパレル
3位	チケット	9位	スポーツ用品
4位	食品・飲料・酒類	10位	レンタルサービス
5位	健康食品・医薬品	11位	家具
6位	コンタクト・メガネ	12位	PC・タブレット・家電

2023年（4-6月） 商材別不正注文検知数ランキング			
1位	ホビー・ゲーム	7位	食品・飲料・酒類
2位	デジタルコンテンツ	8位	コンタクト・メガネ
3位	チケット	9位	スポーツ用品
4位	コスメ・ヘアケア	10位	家電
5位	健康食品・医薬品	11位	工具
6位	総合通販	12位	レンタルサービス

※「O-PLUX」の審査で、審査件数全体に占める不正注文の審査結果NG割合を件数ベースで算出。（かっこ調べ）
※最終的に出荷停止や注文を拒否するなどの対応は、「O-PLUX」加盟店判断により異なる。

3）不正利用のトピック

①専門知識がなくても、フィッシング詐欺を可能にするフィッシングキット「16shop」日本とインドネシアによる国際共同捜査で初の逮捕に

「16shop」は、ブラックハッカー向けのプラットフォームで、フィッシング詐欺を行うためのツールキットです。フィッシングの技術や専門知識があまりない人でもフィッシング詐欺を行うことができるのが特徴です。インドネシアのハッキンググループ「Indonesian Cyber Army」によって作成され、Apple、Amazon、Paypalなどのグローバル企業を含む、43カ国以上の７万以上の企業のアカウントになりすますためのツールキットが提供されてきました。

仕組みとしては、PDFファイルが添付された電子メールを送付し、その添付ファイル内のリンクをクリックするとフィッシングサイトに遷移し、個人情報を詐取するというものです。

2021年秋頃から行われた警察庁とインドネシア国家警察による国際共同捜査により、2023年8月、インドネシアで1名の容疑者（容疑者A）が逮捕されています。警察庁が他国との共同サイバー捜査で容疑者を摘発した初の事例となりました。容疑者Aは「16shop」で、カード情報を詐取し、そのカード情報を不正利用してECサイトでパソコンなどの商品を不正に購入していました。その商品は2022年に日本で逮捕された別の容疑者（容疑者B）に配送され、容疑者Bが商品を転売して利益を容疑者Aに送金していました。

トレンドマイクロの調査（※1）によると、「16shop」によるフィッシング攻撃検出数の国別分布において、半分以上が日本をターゲットにしていたことが確認されています。2023年8月、国際刑事警察機構（ICPO）は、「16shop」の根本的な問題を根絶したことを発表しました。(※2)

※1:『フィッシングキット16shopの分析、トレンドマイクロとインターポールのパートナーシップ』（トレンドマイクロ　2023年9月）
https://www.trendmicro.com/ja_jp/research/23/i/revisiting-16shop-phishing-kit-trend-interpol-partnership.html
※２：https://www.interpol.int/en/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation

②不正注文における分業化、巧妙化が進む：コード決済不正利用

不正注文を実施する際の分業が進んでいます。これまでも実行者らが摘発されていましたが、2023年5月にコード決済不正の主犯格ともいえる「技術者」が逮捕されたことにより、分業化が進んでいる実態が明らかになりました。

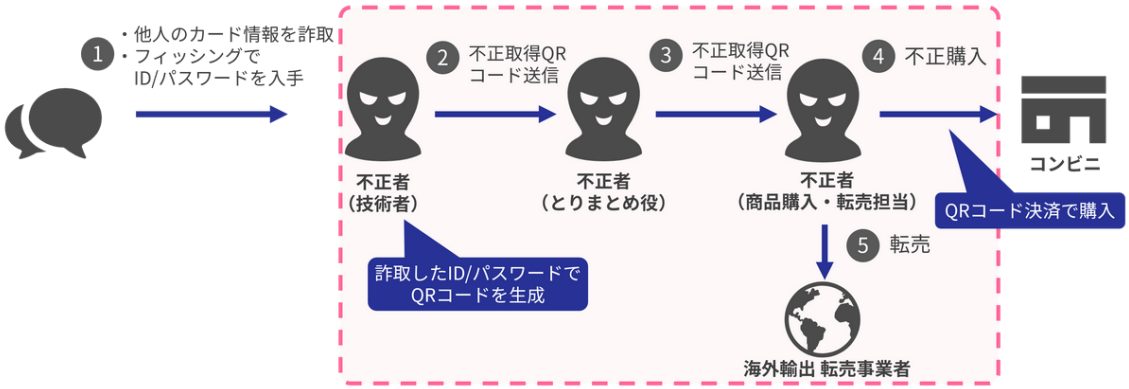
役割としては、以下のようになります。

- 技術者：コード決済サービスのID・パスワードを収集し、決済用のQRコードを生成する
- とりまとめ役：実行グループをとりまとめる。生成したQRコードを実行者である商品購入・転売担当に転送する
- 商品購入・転売担当：実際にQRコードを利用して商品を不正購入し、転売事業者に持ち込む

このように役割を細分化することにより、なるべく身元を隠匿できるようになっています。

また、最近ではこういった分業をSNSなどでアルバイトとして募集するケースも増えており、気づかぬうちに不正注文に加担してしまう可能性もあります。このリスクを避けるため、各自治体や警察庁は注意喚起を行っています。

コード決済の不正事例：分業で不正を実施



想定される被害	
ID/パスワードのアカウント保持者	カード不正利用
販売事業者	アカウントの不正利用における正規アカウントへの代金補填。 不正に悪用されることでのブランディング棄損につながる。

【本レポートに関するお問い合わせ】

かっこ株式会社
広報担当　前田
Mail: pr@cacco.co.jp
Mobile : 050-3627-8878

ｆｊコンサルティング株式会社
広報・マーケティング担当　板垣
Mail: info@fjconsulting.jp