Cashless Security Report

QUARTERLY REPORT

2023年(1-3月版)

fjconsulting, INC.

2023.7.6

キャッシュレス・セキュリティレポート
ー2023年1～3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1-3月）

（1）カード情報流出事件数・情報流出件数の推移

2023 年1月-3月のカード情報流出事件

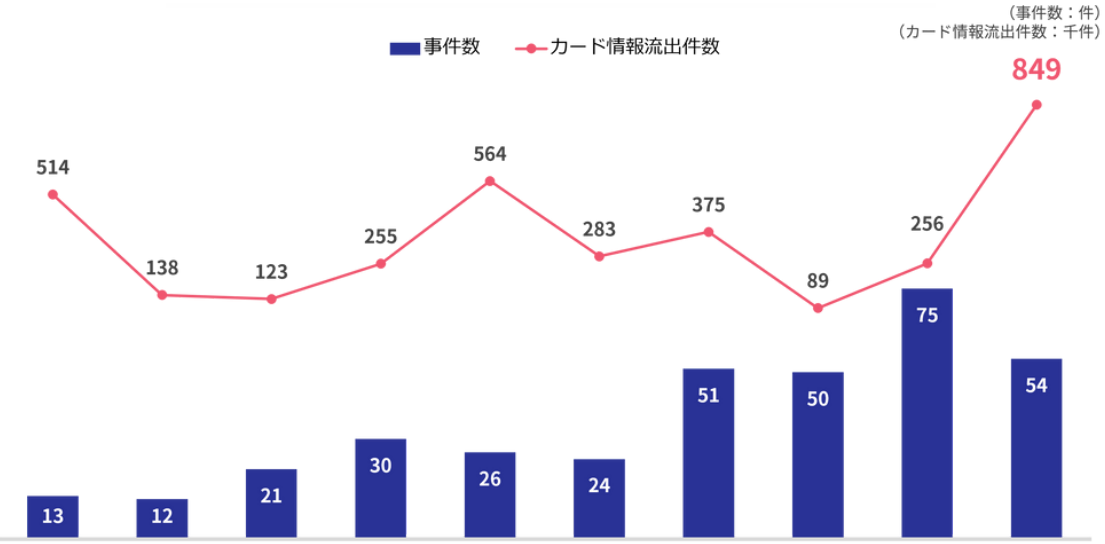
- 事件数　16件
- カード情報流出件数　173,332件

※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】

かっこと f j 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

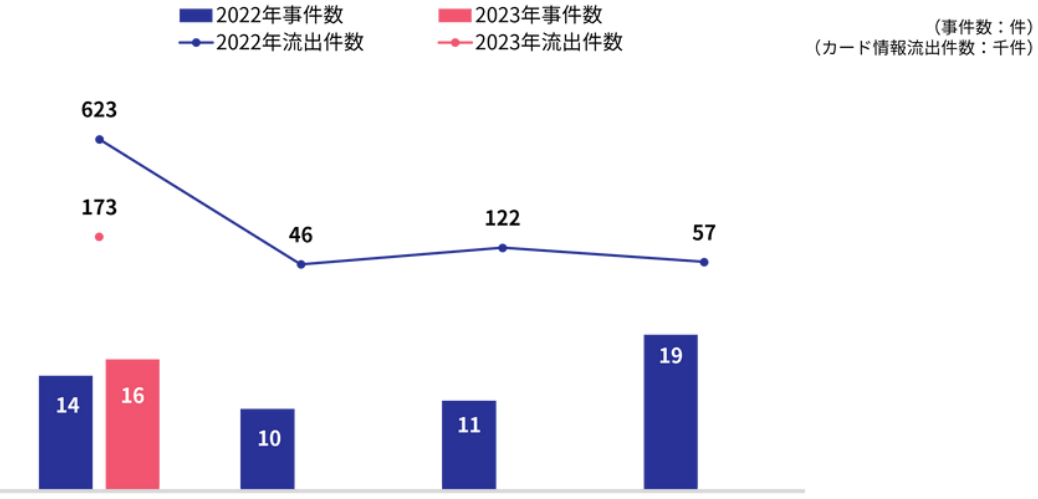
2022年までのカード情報流出事件数・情報流出件数の推移



	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	849,165

（かっこ・f j 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			
	カード情報流出件数(件)	173,322			

（かっこ・f j コンサルティング調べ）

fjconsulting, INC.

（2）商材別事件数・情報流出期間別事件数

＜商材別の事件数(2023年1-3月)＞

商材	事件数(件)	カード情報流出件数(件)
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）

＜情報流出期間別の事件数(2023年1-3月)＞

情報流出期間	事件数(件)	カード情報流出件数(件)
3ヶ月以内	5	115,048
3ヶ月-1年	2	12,819
1-3年	8	45,432
3年以上	1	23

（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

決済機能を持たないサービス事業者へのサプライチェーン攻撃により、
国内で初めてカード情報流出事件が発生

2022年11月に公開された、入力フォーム最適化支援を提供するSaaSの脆弱性を突く攻撃を原因とするカード情報流出事件が、2023年1-3月に4件公表されました。昨年中に公表された事件とあわせると合計で12件、カード情報流出件数は15,469件となります。

広告サービスを提供する事業者の脆弱性を攻撃することで、一度に複数のECサイトからカード情報が流出する「サプライチェーン攻撃」の事例は海外では2019年に報告されていました。国内でもECのカートサービスや決済代行事業者など決済機能を持つサービス事業者を攻撃したサプライチェーン攻撃はこれまでにもありましたが、決済機能を持たないサービス事業者を攻撃してカード情報が流出したのは国内では初めてとなります。

（4）クレジットカード情報保護対策に関する考察

2021年に改正された割賦販売法により、決済機能を提供するECシステム会社などに新たにカード情報保護を義務付けられました。その実務上の指針である『クレジットカード・セキュリティガイドライン』（※1）では、これらの事業者に対し、PCIデータセキュリティ基準（PCI DSS ※2）への準拠を求めています。

しかし、上記（3）で攻撃を受けたような決済機能を持たないサービスは、現状規制の対象であるかは判然としません。このような「 決済機能を持たないがカード決済ページのセキュリティに影響を与えるサービス」を提供する事業者への規制が今後の課題となります。

※1：https://www.meti.go.jp/press/2022/03/20230315001/20230315001.html
※2:PCI DSS:クレジットカードなど国際ブランドのカード会員データを安全に取り扱う事を目的として策定された、カード業界のデータセキュリティに関する国際基準

>>> 2. ECにおける不正利用の概況（2023年1-3月）

（1） クレジットカード不正利用被害額の推移

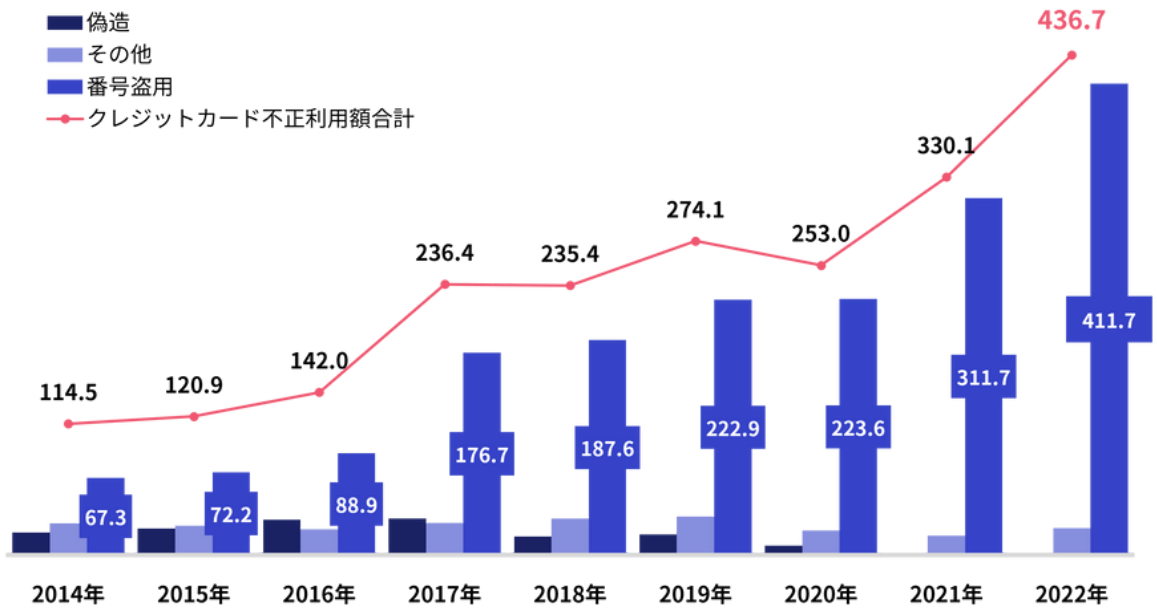
2023 年1月-3月のクレジットカード不正利用

- 不正利用被害額合計　120.4億円
- 偽造　0.7億円
- 番号盗用　133.3億円
- その他　7.3億円

※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

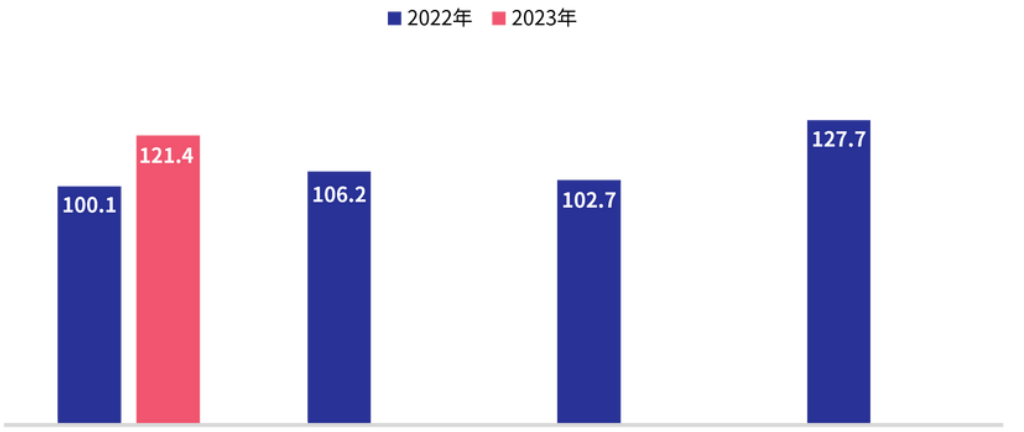
（金額単位：億円）



（『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）



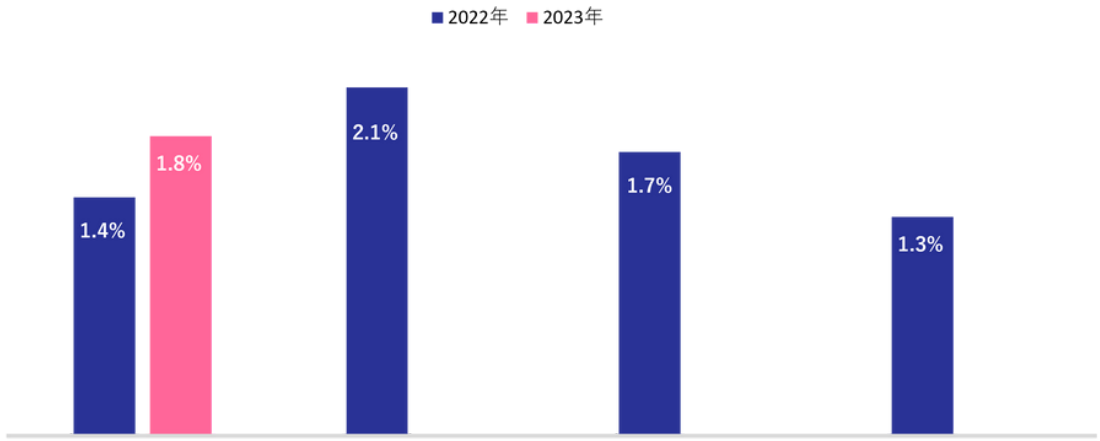
		1～3月	4～6月	7～9月	10～12月
2022年	偽造	0.2	0.2	0.7	0.6
	番号盗用	94.6	100.6	95.9	120.6
	その他	5.3	5.4	6.1	6.5
2023年	偽造	0.8			
	番号盗用	113.3			
	その他	7.3			

（『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）

（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

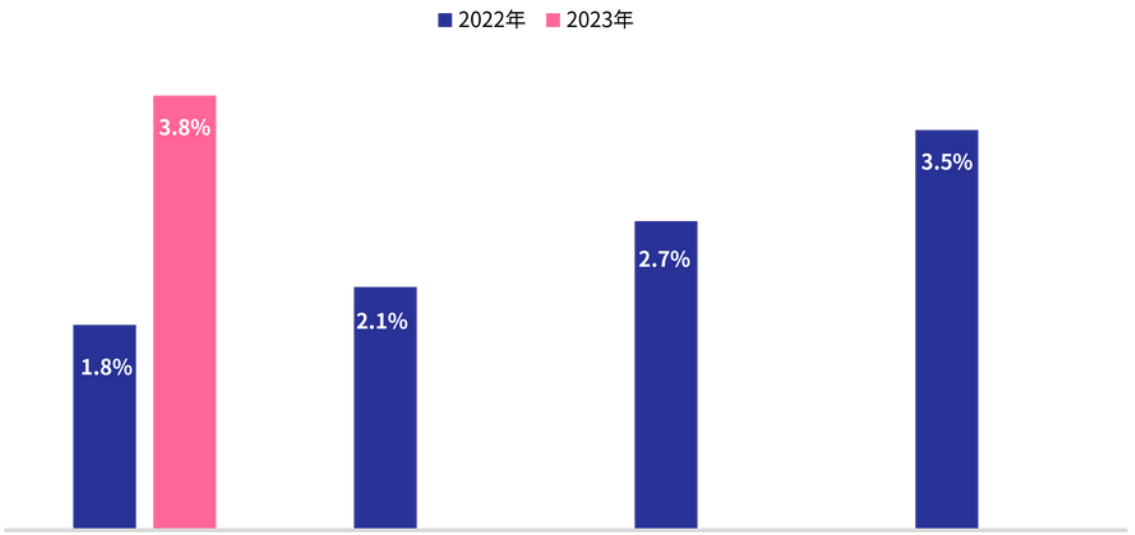
クレジットカード不正注文の発生率



	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%			

※「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%			

※「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。

＜不正注文に狙われやすい商材ランキング＞

2022年（1-12月） 商材別不正注文検知数ランキング			
1位	デジタルコンテンツ	7位	食品・飲料・酒類
2位	ホビー・ゲーム	8位	EC総合通販
3位	旅行	9位	家電・PC・タブレット
4位	コンタクト・メガネ	10位	アパレル
5位	健康食品・医薬品	11位	家具
6位	コスメ・ヘアケア	12位	レンタルサービス

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

※「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クレジットマスター（クレマス）

手口としては以前からありましたが、昨年頃から被害が急増しています。クレジットカード番号の規則性にしたがって、bot等を利用し他人の番号を割り出す行為です。カード情報が使えるかどうかを確認するため、ECサイトの決済ページや会員登録ページが悪用されます。

クレマスが発生すると、事業者への影響としては、大きく4つあげられます。①大量のアクセスがくるため、ECサイトへの負荷がかかる、②無駄なオーソリゼーション費用が発生する、③入手したカード情報でカード不正利用につながる、④カード情報が割り出され不正利用された場合に、カードが使えなくなり、カード保持者からクレームが入るなど顧客の信用喪失につながります。
消費者への影響としては、普段使っていないクレジットカードなので、カード情報が盗まれる機会が全くない場合でも、クレマスで割り出されると不正利用の被害にあいます。

② 置き配を悪用した不正

様々な宅配業者が、対面で荷物を受け取る必要がない「置き配」サービスに対応する傾向にあります。置き配を利用したことがある割合も、2019年から3年間で2.3倍に増加しており、6割以上が利用したこと※1があるほど一般化しています。それを悪用した者が、不正利用により買い物した荷物を週末のオフィスなど人がいない場所を指定し受け取る手口が増えています。

※1:株式会社ナスタ「置き配に関する実態調査」 2022年11月

③ SIMスワッピング(SIMスワップ)

SIMスワップとは、金融機関を狙った不正送金被害に使用される手口の一つです。この手口では、悪意のある第三者があなたのスマートフォンの契約者になりすまし、新しいSIMカードを再発行し不正利用に活用しています。

具体的な流れは以下の通りです：
1. フィッシング: まずフィッシングで、あなたの氏名、電話番号、ネットバンキングのID、パスワードなどの個人情報を盗みます。
2. 身分証明書の偽造: 盗んだ個人情報を元に、悪意のある者は身分証明書として偽造した免許証などを用意します。
3. SIMの再発行: 悪意のある者は、偽造した身分証を使い、紛失したと偽って携帯ショップに行き、新しいSIMカードを再発行してもらいます。このとき、悪意のある者はあなたの電話番号を乗っ取ります。
4. 不正送金: 悪意のある者があなたの電話番号を乗っ取ると、金融機関からの本人確認のためにワンタイムパスワードがその携帯に届きます。悪意のある者は、事前に入手したネットバンキングの情報を使用して、不正送金を行います。

このようにSIMスワップは、フィッシングから始まり、個人情報の盗難と身分証明書の偽造、そしてSIMカードの再発行といった手順を経て、最終的に不正送金が行われる手口です。

（4）クレジットカード不正利用対策に関する考察

『クレジットカード・セキュリティガイドライン』では2025年3月末までに原則、全てのEC加盟店に国際ブランドが推奨する本人認証サービスである「EMV 3-Dセキュア」の導入を求めています。
「EMV 3-Dセキュア」は、カード利用者の決済情報等を基にリスクベース認証を実施し、高リスクと判断される取引にのみ、ワンタイムパスワード等の追加認証を実施します。事業者は、「EMV 3-Dセキュア」を導入することで、従来懸念されていたかご落ちのリスクを低減した上で、クレジットカード不正利用の金銭被害を減らすことが期待できます。

その一方、「EMV 3-Dセキュア」のすり抜けが発生し、事業者より相談を受けることがあります。これは、審査に使用するデータの連携が少ないことや、推奨されているワンタイムパスワードではなく、固定パスワードを利用していること(フィッシングで固定パスワードが流出)に起因していると考えられます。不正利用の被害を減少させるためには、「EMV 3-Dセキュア」だけに頼るのではなく、複数のセキュリティ対策を組み合わせた重層的な対策を取ることが重要です。不正利用被害が続くと、カード会社からの与信条件の厳格化や、決済手数料の引き上げ交渉など、様々な事業への影響が出る可能性がある点にも留意する必要があります。

【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