Cashless Security Report

Quarterly Report

2023年(10-12月版)2024年4月発行

fjconsulting, INC.

2024.4.16

キャッシュレス・セキュリティレポート
ー2023年10～12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10-12月）

（1）カード情報流出事件数・情報流出件数の推移

2023 年10月-12月のカード情報流出事件

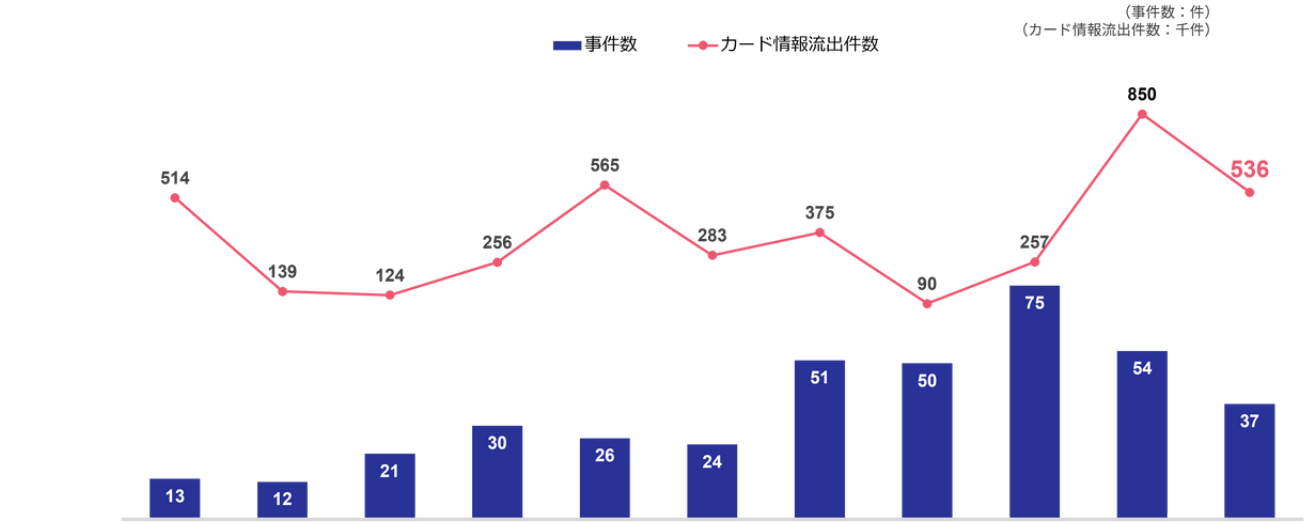
- 事件数　7件
- カード情報流出件数　40,831件

※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ｔｆｊ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

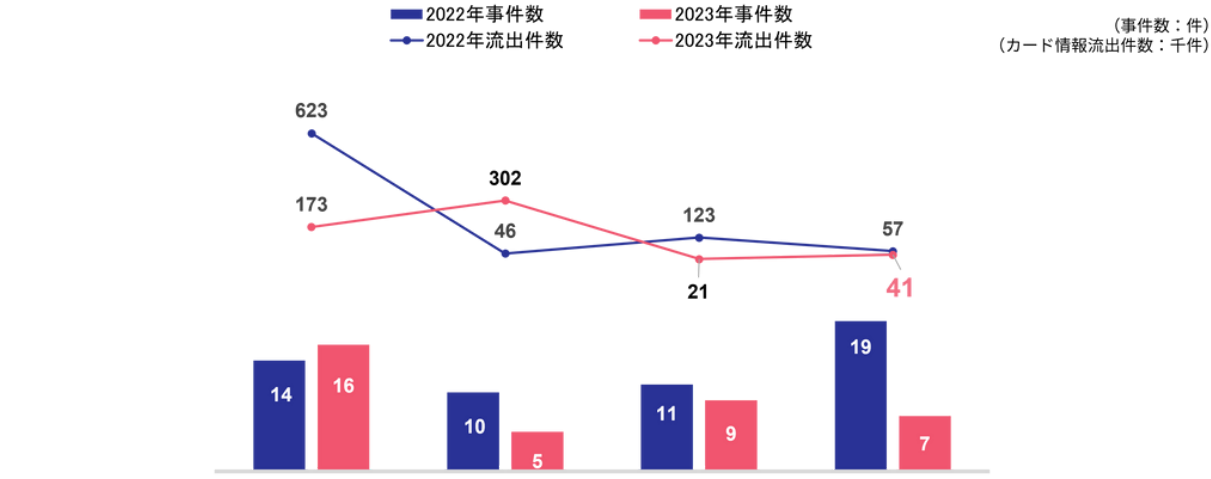
2023年までのカード情報流出事件数・情報流出件数の推移



	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年	2022年	2023年
事件数(件)	13	12	21	30	26	24	51	50	75	54	37
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	536,291

（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	9	7
	カード情報流出件数(件)	173,322	301,545	20,593	40,831

（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7件、カード情報流出件数は40,831件となりました。事件のうち3件は後述するコールセンター業務委託先の担当者（派遣社員）による不正持ち出しによるものです。
2023年通年のカード情報流出事件数は37件、カード情報流出件数は536,291件となり、前年に比べると事件数で17件、カード情報流出件数で約31万件の減少となりました。流出したカード情報のうち290,771件はカード会社1社が自社のダイレクトメール表面に誤ってカード番号を印字した状態で送付したものとなります。

（2）業種/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1-12月)＞

業種/商材カテゴリー		2023年1-3月		2023年4-6月		2023年7-9月		2023年10-12月	
		事件数（件）	カード情報流出件数（件）	事件数（件）	カード情報流出件数（件）	事件数（件）	カード情報流出件数（件）	事件数（件）	カード情報流出件数（件）
加盟店合計		16	173,322	4	10,774	9	20,593	7	40,831
業種別	アパレル	5	41,362	1	6,263	0	0	0	0
	コスメ	4	13,707	0	0	0	0	2	67
	食品	3	5,099	1	1,830	2	5,157	1	1755
	家電・電子機器・PC	2	112,147	0	0	1	6,364	0	0
	生活雑貨、家具、インテリア	1	402	1	1,771	4	8,983	0	0
	アパレル、コスメ、健康食品	1	605	0	0	0	0	0	0
	自動車、バイク	0	0	0	0	0	0	1	2,602
	その他	0	0	1	910	2	89	2	36,393
カード会社		0	0	1	290,771	0	0	0	0

（かっこ・ｆｊコンサルティング調べ）

※7-9月の「その他」のうち1件はカード情報流出件数不明

＜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		2023年4-6月		2023年7-9月		2023年10-12月	
	事件数(件)	カード情報流出件数(件)	事件数(件)	カード情報流出件数(件)	事件数(件)	カード情報流出件数(件)	事件数(件)	カード情報流出件数(件)
3ヶ月以内	5	115,048	2	292,542	3	173	0	0
3ヶ月-1年	2	12,819	2	2,740	2	244	3	81
1-3年	8	45,432	1	6,263	4	20,176	4	40,750
3年以上	1	23	0	0	0	0	0	0

（かっこ・ｆｊコンサルティング調べ）

※7-9月の「その他」のうち1件はカード情報流出件数不明

（3）カード情報流出事件のトピック

コールセンター業務委託先における不正持ち出しでカード情報が流出

2023年10月、コールセンター業務を提供しているサービスプロバイダーの1社が、コールセンターシステムの運用保守委託先の派遣社員による顧客データの不正持ち出しを公表しました。当該派遣社員は持ち出した顧客情報を名簿業者に売却しています。データの流出期間は約10年間と長期にわたっており、流出した個人情報は69の企業・自治体から取り扱いを委託された約928万人分にのぼります。流出した情報の中に、クレジットカード情報は81件含まれていました。

2024年2月に公表された社内調査委員会の調査報告書では、サーバーからの顧客データのダウンロード制限をはじめとするUSBメモリーなどの外部記録媒体への書き出し禁止、保守用PCのインターネット接続禁止、ログ監視、私有PCのネットワーク接続禁止といった基本的なセキュリティ対策がされていなかったことが「内部不正による情報漏洩リスクに対し極めて脆弱」と評価されています。

割賦販売法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』では、カード情報を取り扱う業務を外部委託する場合、委託者自身が委託先のセキュリティ状況を確認し、責任を持ってPCI DSS準拠などの対策を求めることを要求しています。コールセンター業務などを外部に委託する場合、委託先に対しPCI DSS準拠を求めることは、カード情報を取り扱うための必要最低限のセキュリティ対策といえます。

2. ECにおける不正利用の概況（2023年10-12月）

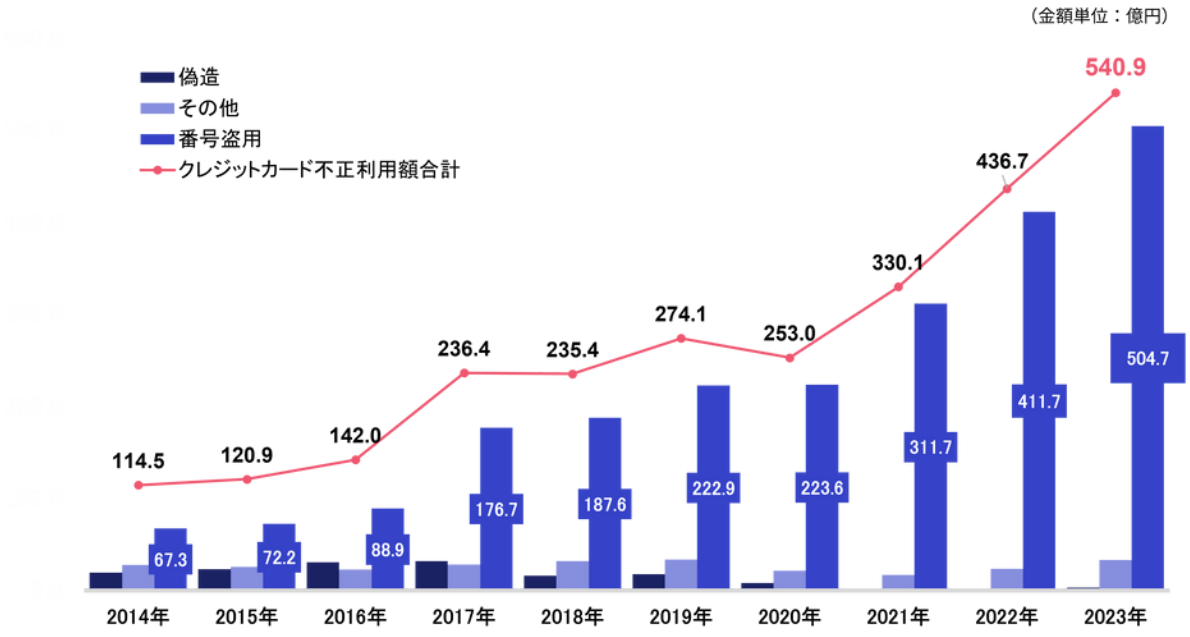
（1） クレジットカード不正利用被害額の推移

2023 年10月-12月のクレジットカード不正利用

- 不正利用被害額合計　138.6億円
- 偽造　1.1億円
- 番号盗用　128.1億円
- その他　9.4億円

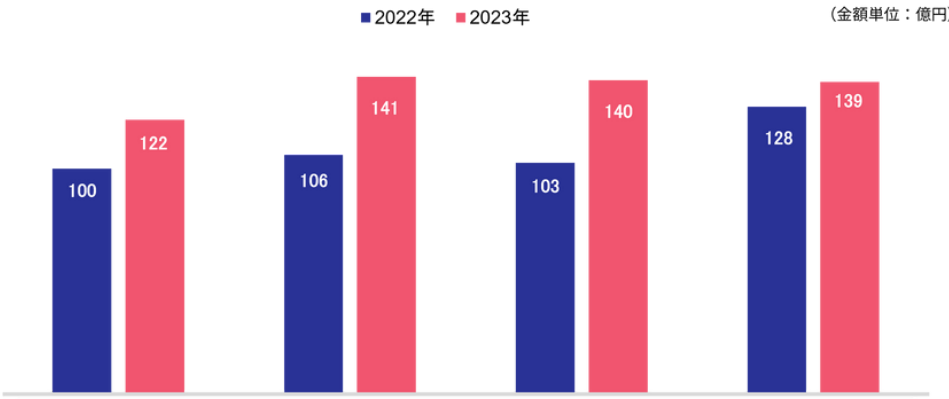
※日本クレジット協会調べ
https://www.j-credit.or.jp/information/statistics/index.html

2023年までのクレジットカード不正利用被害額の推移



（『クレジットカード不正利用被害額の発生状況』 一般社団法人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）



		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
	合計	**100.1**	**106.2**	**102.7**	**127.7**
2023年	偽造	0.8	0.5	0.7	1.1
	番号盗用	113.6	132.4	130.6	128.1
	その他	7.4	8.1	8.2	9.4
	合計	**121.8**	**141.0**	**139.5**	**138.6**

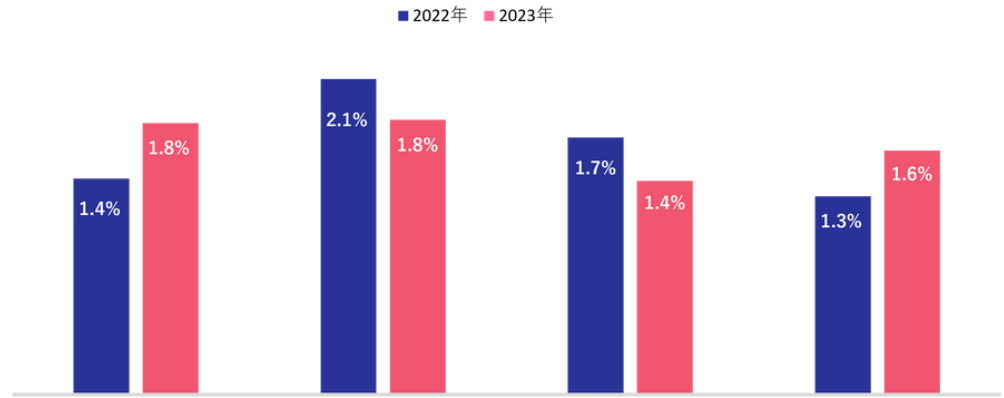
（『クレジットカード不正利用被害額の発生状況』 日本クレジット協会）

2023年1-12月までのクレジットカード不正利用被害額は、合計540.9億円で過去最多を記録しています。これは、前年と比較すると104億円増加しており、2年連続で100億円以上の被害が増加していることになります。内訳としてはクレジットカード情報だけで決済ができる主にECサイトでの不正利用「番号盗用」が全体の93.3%を占める504.7億円になりました。

（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

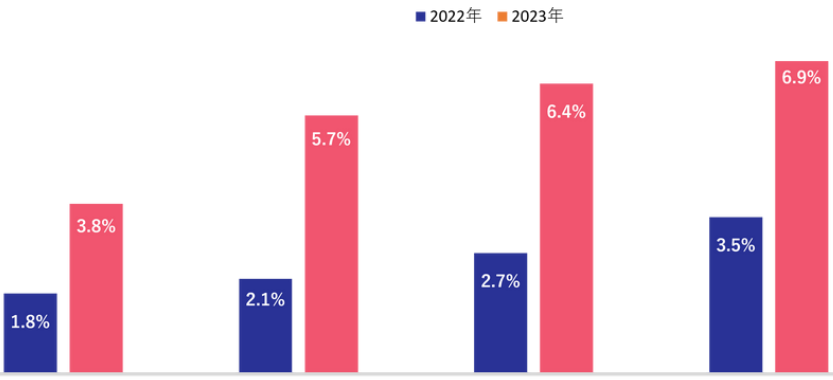
クレジットカード不正注文の発生率



	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%	1.4%	1.6%

※「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%	6.4%	6.9%

※「O-PLUX」の審査で、審査件数全体に占めるい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。

傾向としては、7-9月と比較し10-12月ではクレジットカード不正は0.2%、転売不正は0.5%、不正発生率がともに微増しました。これは、ブラックフライデーや年末セールの時期であり、商品の購買意欲が高まる時期に合わせて転売が増加するため、不正も多く発生したと考えられます。

＜不正注文に狙われやすい商材ランキング＞

2023年（7-9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	PC・タブレット・家電
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	工具
5位	コンタクト・メガネ	11位	ふるさと納税
6位	健康食品・医薬品	12位	総合通販

2023年（10-12月） 商材別不正注文検知数ランキング			
1位	チケット	7位	日用品・雑貨・キッチン用品
2位	デジタルコンテンツ	8位	コンタクト・メガネ
3位	ホビー・ゲーム	9位	ふるさと納税
4位	コスメ・ヘアケア	10位	食品・飲料・酒類
5位	健康食品・医薬品	11位	レンタルサービス
6位	PC・タブレット・家電	12位	工具

※「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。

ふるさと納税は7-9月版では初ランクインで11位でしたが、今回は9位にランクアップとなりました。ふるさと納税の申請期日が12月末までになるため、特に年末は需要が高まる傾向にあります。そこを不正者は狙ってきたと推測できます。

（3）2023年12月末の国内のカード発行会社（イシュア）におけるDMARC設定状況

フィッシングにより窃取されたカード情報の不正利用が増加していることを受け、経済産業省は、2023年1月に公表した『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、カード発行会社（以下イシュア）に対し、DMARC導入を含めた、なりすまし対策の強化を求めています。

イシュアは割賦販売法で「登録包括信用購入あっせん事業者」として登録が義務付けられており、その一覧が経済産業省のWebサイトで公開されています。ｆｊコンサルティングは、経済産業省のWebサイトで公開されているイシュア245社を対象に、DMARCの導入状況を調べました。

【調査方法】
①　調査対象のイシュアがWebサイト等でメール送信元として公開しているドメイン（外部委託先やサブドメインを含む）を収集し、対象ドメインを確定
②　①で収集した全てのドメインのDNSに問い合わせを行い、DMARCレコードの設定有無と、設定がある場合ポリシーを確認
③　会社ごとのDMARC対応状況を以下の3段階に分類
　1）対応済み：メール送信元として使用しているドメイン全てにDMARCレコードが設定されている。
　2）一部対応：メール送信元として使用しているドメインの一部にDMARCレコードが設定されている。
　3）未対応：メール送信元として使用している全てのドメインにDMARCレコードが設定されていない。

【調査対象】
登録包括信用購入あっせん事業者（イシュア）245社

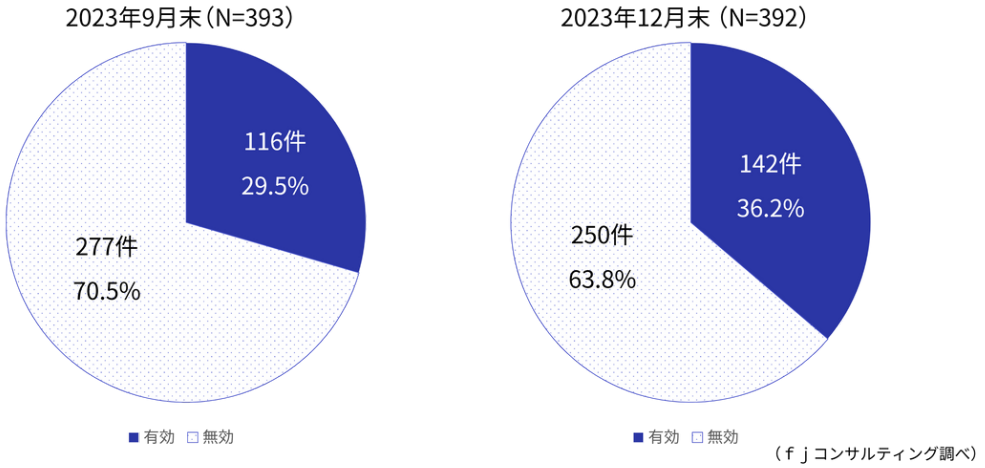
【調査実施時期】
2023年12月末

【調査結果（2023年12月31日）】

① 調査対象ドメイン数　392件

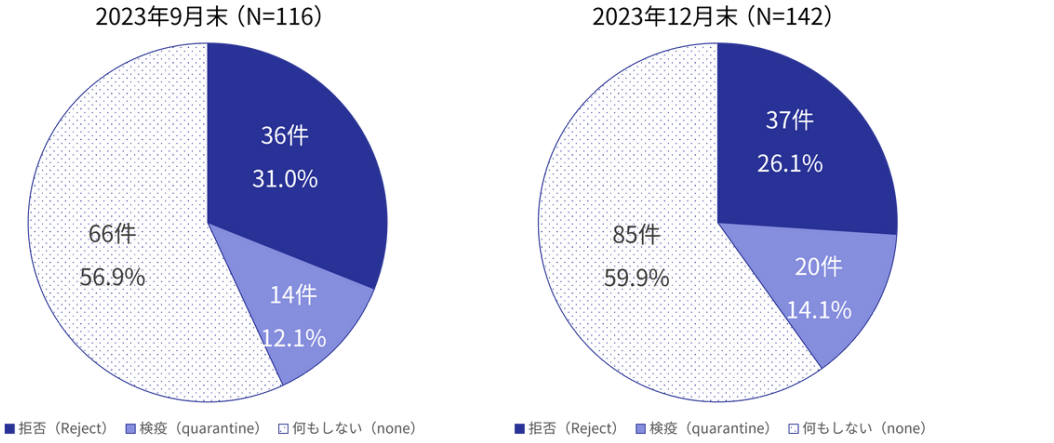
② 調査対象ドメイン毎のDMARC対応状況と運用ポリシー

＜ドメイン毎のDMARCの設定率＞



（ｆｊコンサルティング調べ）

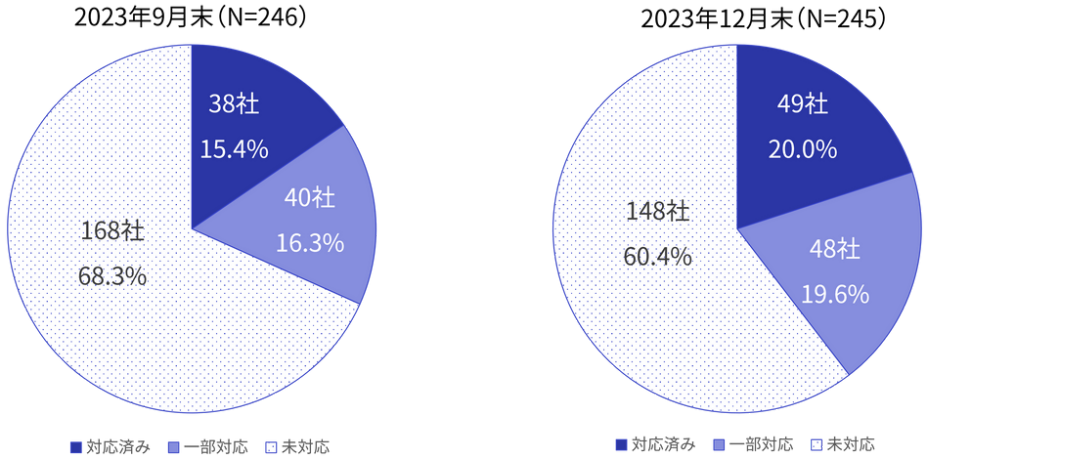
＜ドメイン毎のDMARC設定ポリシー＞



（ｆｊコンサルティング調べ）

③会社ごとのDMARC対応状況

＜会社毎のDMARC対応状況＞



（ｆｊコンサルティング調べ）

2023年12月末時点で、イシュアがメール送信に利用しているドメイン392件のうち、有効なDMARCレコードが設定されているのは142件（約36%）となりました。DMARCレコードが有効なドメインのうち、最も厳しい「reject（拒否）」ポリシーが設定されているドメインは37件（約26%）で、85件（約60%）はポリシーを「none（何もしない）」にして運用しています。組織別にみると、DMARCを一部でも導入しているイシュアは97社（約40%）となっています。

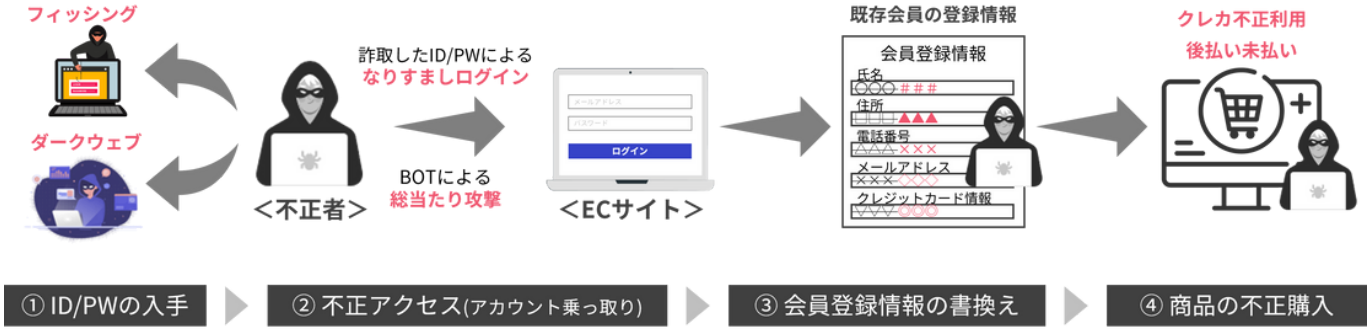
フィッシングメール対策としてのDMARCの実効性を持たせるためには、導入率を引き上げる、および導入しているドメインにおいてもポリシーを「reject（拒否）」もしくは「quarantine（検疫）」に設定して運用することが求められます。

（4）不正利用のトピック

①アカウント乗っ取りによる不正購入

昨年末より、ECサイトにおけるアカウント乗っ取りによる不正注文被害の相談が増加しています。手口としては、まずはダークウェブやフィッシングからECサイトの会員アカウントのIDやパスワードを詐取します。つづいて、詐取したIDやパスワードを用いて、ECサイトにログインした際に、マイページから氏名、住所、クレジットカード情報等の会員情報を書き換え、不正注文をするという流れで行われます。（後払い決済での不正注文も増加中です）この手口の巧妙な点は、既存顧客に対する不正対策が甘くなりがちなところを狙っている点です。さらに会員情報にクレジットカード情報を紐づけている場合には、不正者はクレジットカード情報を盗む手間もなく、容易に不正注文ができてしまいます。

ECサイトを運営する事業者は、会員アカウントが乗っ取られることで事業者責任が問われる可能性があります。さらに、個人情報漏洩の事案として扱われるため、個人情報保護委員会や関連する団体への報告が求められます。このため、EC事業者は、会員アカウントを守る対策を強化する必要があります。



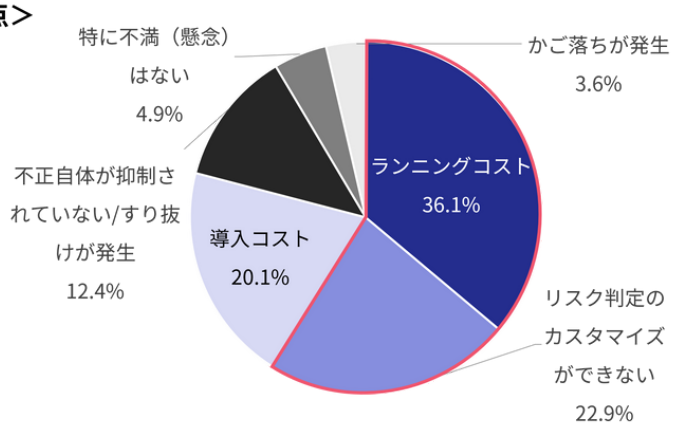
②EC加盟店におけるEMV 3-Dセキュアの導入率

『クレジットカード・セキュリティガイドライン【5.0版】』（2023年3月公表）では、増加し続けるクレジットカード不正利用被害への対策として、全てのEC加盟店に対し2025年3月までに「EMV3-Dセキュア」（以下、EMV3DS）の導入を求める方針が示されています。

かっこが2023年11月に実施したEC事業者実態調査において、「EMV3DS」の導入率は36.1%にとどまっている状況です。「EMV3DS」の懸念点としては、ランニングコストが最も多くなっています。従来の「3Dセキュア」は無償で利用ができましたが、最新版の「EMV3DS」は原則有償になりました。また、高価格帯の商品や換金性の高い商品を扱う場合でも、加盟店リスク判定のカスタマイズができない点を懸念する声が多くなっています。※グラフ<EMV3-Dセキュアの懸念点>参照。

導入率をより高めるには、運用コストと使い勝手において更なる支援をすることがポイントになると考えます。また、精度の面では、「EMV3DS」は不正利用被害の軽減には有効ですが、突破されるケースも発生しています。『クレジットカード・セキュリティガイドライン』にもある通り、リスクに応じ多面的・重層的な対策を実施することが重要になります。

＜EMV3 -Dセキュアの懸念点＞



（かっこ調べ）

【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