Cashless Security Report

Quarterly Report

2024年(7-9月版)2025年1月発行

PCI DSS Ready Cloud

2025.1.30

かっこ株式会社
株式会社リンク

キャッシュレス・セキュリティレポート
ー2024年7-9月版：2025年1月発行ー

PCI DSS Ready Cloud

はじめに

かっこ株式会社（以下Cacco）と株式会社リンク（以下リンク）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（2024 年7-9月）

（1）カード情報流出事件数・情報流出件数の推移

2024年7-9 月のカード情報流出事件

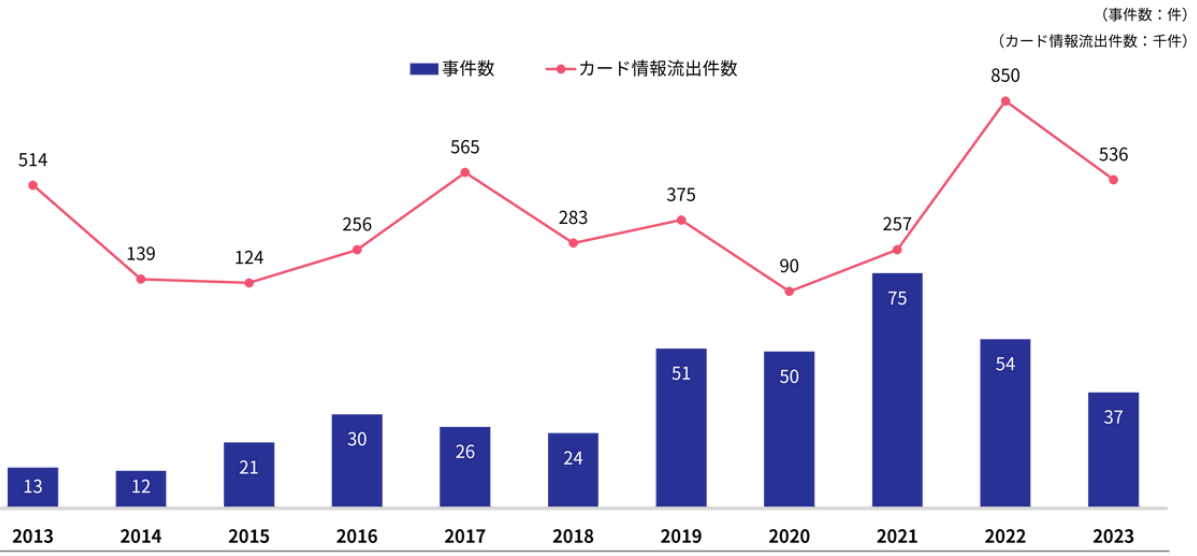
- 事件数　5件
- カード情報流出件数　120,895件

※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】

Caccoとリンクが、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

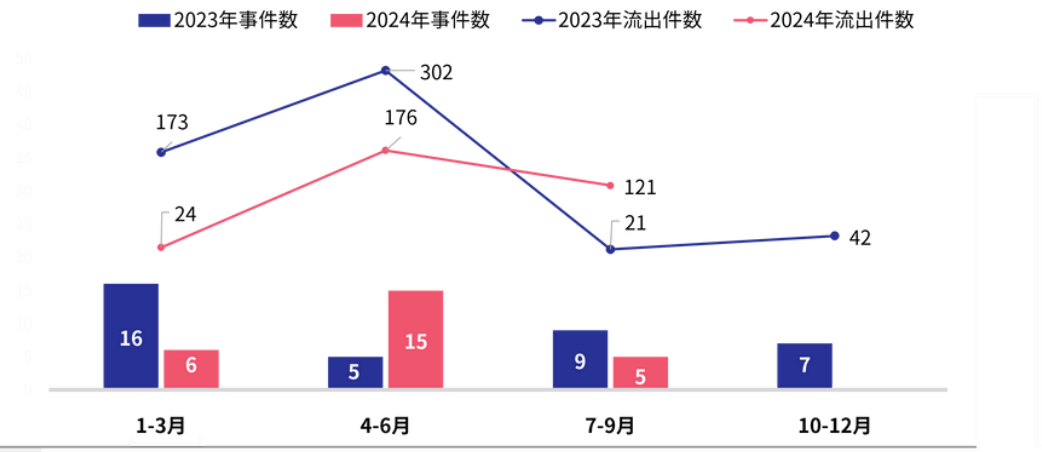


	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
事件数	13	12	21	30	26	24	51	50	75	54	37
カード情報流出件数	514,369	138,717	123,527	255,689	564,844	283,374	375,479	89,628	256,822	849,950	536,291

（Cacco・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

2024年のカード情報流出事件数・情報流出件数（前年同四半期比較）



		1-3月	4-6月	7-9月	10-12月
2024年	事件数	6	15	5	
	カード情報流出件数	23,677	175,847	120,895	
2023年	事件数	16	5	9	7
	カード情報流出件数	173,322	301,545	20,593	40,831

（Cacco・リンク調べ）

※1 2023年12月末までのデータはCacco・ｆｊコンサルティング調べ

※2 2024年4-6月分の流出件数が公表されたため、流出件数を以下の通り訂正

流出件数　120,727 → 175,847

※3 2024年12月27日時点で集計

2024年7～9月の流出事件数は、前四半期（4～6月）と比べて３分の１となりました。事件数は少ないものの、流出件数が約45,000件及び約65,000件となる大規模な事件が含まれていることから、カード情報流出件数は12万件を超えました。当該四半期に発生した5件の事件は、いずれも流出開始時期が2020年または2021年となっており、流出が長期に渡っています。5件のうち2件は警察の指摘により被害が発覚したとされています。2020年から2021年ごろに多く見られた改ざんの手口について警察が集中的に調査した結果、窃取されたカード情報が不正利用されていないもののカード情報が流出し続けていたことが確認されています。

また、4～6月に事件発生が公表されていたもののカード情報流出件数が不明だった2事件について、流出件数が公表されました。これにより、2024年4～6月の流出事件数は5件、カード情報流出件数は175,847件となりました。この2件についても、流出開始時期は2021年となっており、警察庁の指摘により被害が発覚しています。今後、同様に警察の指摘で長期にわたる流出が明らかになり、公表されるケースが増える可能性があります。

（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＞

（単位：件）

業種/商材カテゴリー		2023年10-12月		2024年1-3月		2024年4-6月		2024年7-9月	
		事件数	カード情報流出件数	事件数	カード情報流出件数	事件数	カード情報流出件数	事件数	カード情報流出件数
加盟店合計		7	40,831	6	23,677	15	120,727	5	120,895
業種別	アパレル	0	0	1	3,827	3	17,176	0	0
	コスメ	2	67	0	0	1	15,198	0	0
	食品	1	1,755	2	7,183	8	126,746	4	119,463
	家電・電子機器・PC	0	0	1	4,748	0	0	0	0
	生活雑貨、家具、インテリア	0	0	0	0	1	3,958	1	1,432
	健康食品	1	14	1	5,193	0	0	0	0
	ホビー	0	0	1	2,726	1	4,969	0	0
	自動車、バイク	1	2,602	0	0	0	0	0	0
	その他	2	36,393	0	0	1	8,073	0	0
カード会社		0	0	0	0	0	0	0	0

（Cacco・リンク調べ）
※1 2023年12月末までのデータはCacco・ｆｊコンサルティング調べ
※2 2024年4-6月分の流出件数が公表されたため、流出件数を以下の通り訂正
　アパレルの流出件数　15,014→17,176　食品の流出件数　73,788 → 126,746
※3 2024年12月27日時点で集計

＜流出期間別の事件数・カード情報流出件数＞

（単位：件）

情報流出期間	2023年10-12月		2024年1-3月		2024年4-6月		2024年7-9月	
	事件数	カード情報流出件数	事件数	カード情報流出件数	事件数	カード情報流出件数	事件数	カード情報流出件数
3ヶ月以内	0	0	0	0	1	8,073	0	0
3ヶ月-1年	3	81	1	2,726	2	5,621	0	0
1-3年	4	40,750	5	20,951	7	60,920	2	8,450
3年以上	0	0	0	0	3	49,033	3	112,445

（Cacco・リンク調べ）
※1 2023年12月末までのデータは、Cacco・ｆｊコンサルティング調べ
※2 2024年4-6月分における2件の流出時期と流出件数が公表されたため、流出件数を以下の通り訂正
　1-3年　58,000→60,920
※3 2024年12月27日時点で集計

（3）カード情報流出事件のトピック

攻撃キャンペーン「Water Pamola」の対象と思われる事件が相次いで発覚

前述の通り、2020年から2021年頃にカード情報流出が始まった事件の発覚が相次いでいます。2024年1月から9月末までに発覚した22件の事件のうち、流出開始時期が2020年の事件が2件、2021年の事件が20件を占めています。（表1）

▼表1：2024年9月末までに発覚したカード情報流出事件のうち、漏洩開始が2020年-2021年の事件

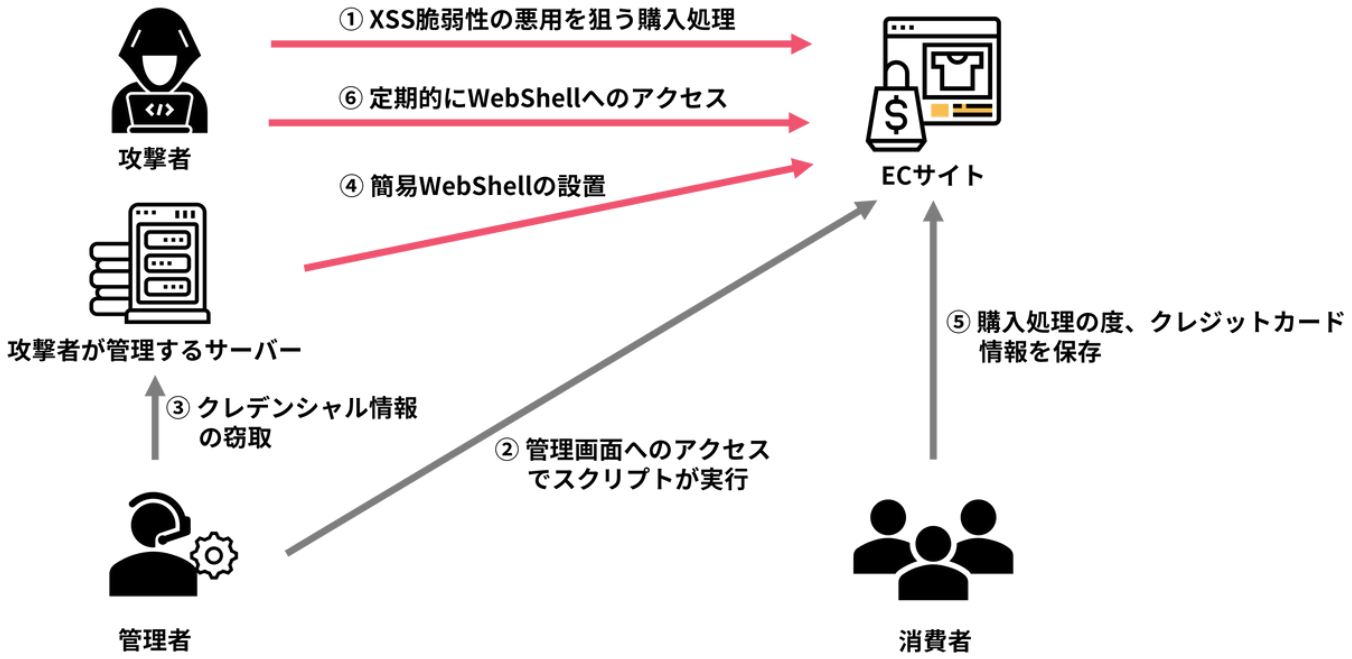
No		取り扱い商材	公表日	発覚日	発覚のきっかけ	漏洩件数	漏洩発生年月
1	A社	健康食品	2024年1月	2023年12月	カード会社	5,193	2021/1/5 ～ 2023/11/15
2	B社	食品	2024年2月	2023年9月	カード会社	2,114	2021/5/30 ～ 2023/9/13
3	C社	美容機器	2024年2月	2023年6月	カード会社	4,748	2021/4/21 ～ 2023/4/3
4	D社	食品	2024年2月	2023年9月	カード会社	5,069	2021/4/22 ～ 2023/7/11
5	E社	アパレル	2024年3月	2023年9月	カード会社	3,827	2021/4/25 ～ 2023/8/21
6	F社	食品	2024年4月	2023年6月	カード会社	16,407	2021/1/27 ～ 2023/5/15
7	G社	スポーツ用品	2024年5月	2024年2月	カード会社	13,960	2021/2/24 ～ 2024/1/17
8	H社	ホームセンター	2024年5月	2024年1月	自社	3,958	2021/3/17 ～ 2024/1/18
9	I社	食品	2024年5月	2024年5月	警察	11,844	2021/4/22 ～ 2024/5/14
10	J社	業務用物販	2024年5月	2023年9月	カード会社	15,198	2020/12/24 ～ 2023/12/8
11	K社	地方特産品	2024年5月	2024年5月	警察	18,746	2021/3/10 ～ 2024/5/22
12	L社	食品	2024年5月	2024年1月	警察	2,727	2021/6/10 ～ 2024/1/18
13	M社	食品	2024年5月	2024年5月	警察	52,958	2021/7/20 ～ 2024/5/20
14	N社	アクセサリー	2024年6月	2024年5月	警察	2,162	2021/6/28 ～ 2024/5/30
15	O社	業務用物販	2024年6月	2024年1月	警察	1,054	2021/5/21 ～ 2024/1/2
16	P社	楽譜販売	2024年6月	2024年1月	警察	4,696	2021/4/10 ～ 2024/1/14
17	Q社	地方特産品	2024年6月	2024年4月	カード会社	18,443	2021/3/30 ～ 2024/4/19
18	R社	食品	2024年7月	2024年1月	警察	1,432	2021/5/27 ～ 2024/1/15
19	S社	食品	2024年7月	2024年3月	カード会社	1,703	2021/5/27 ～ 2024/1/15
20	T社	食品	2024年7月	2024年5月	警察	65,387	2021/3/18 ～ 2024/5/28
21	U社-①	食品	2024年8月	2024年5月	外部	45,355	2020/4/27 ～ 2024/5/21
22	U社-②	食品	2024年8月	2024年5月	外部	7,018	2021/6/17 ～ 2024/5/19

長期間にわたってカード情報流出の発生を加盟店は気づくことができず、契約するアクワイアラ以外の警察など外部機関から発生を指摘されている理由は、窃取されたカード情報が不正利用されていないためと推測されます。カード情報が不正利用されないとカード会社はCPP（※）が特定できないため、カード情報流出事件の発生に気づくことはできません。従来、カード情報流出事件の多くはCPPの特定を起点に、カード会社が加盟店に詳細調査を依頼するにより、発覚することが大半でした。しかし2024年5月以降に公表された事件では、16件のうち9件と半数以上が警察からの指摘により発覚しています。2024年4～6月期の本レポートで、警察によるカード情報流出事件の指摘が徐々に増加していることに触れましたが、同年7月～9月期は、その傾向が裏付けられた結果となりました。

※CPP（Common Purchase Point）：不正利用された複数のカードが共通して使用されていた加盟店

2020年から2021年にかけては、EC-CUBEの脆弱性を狙ってサイトを改ざんする「Water Pamola」（次ページに概要を記載）と呼ばれるオンラインスキミング攻撃のキャンペーンが行われ、多くのECサイトでカード情報流出事件が発生しました。警察庁サイバー特別捜査部が、2021年頃に被害にあったものと同じプログラムで運用されている国内のECサイトを調査し、40以上の企業や団体でWebサイトの改ざんを見つけたとされており、上記表中の事件の多くが該当すると推測されます。

＜Water Pamolaの概要＞



出所：JPCERT CC ブログ記事をもとにリンクにて作成
https://blogs.jpcert.or.jp/ja/2021/07/water_pamola.html
※1 XSS脆弱性（クロスサイトスクリプティング）：Webサイトの脆弱性を利用し、記述言語であるHTMLに悪質なスクリプトを埋め込む攻撃
※2 WebShell：主にサイバー攻撃を目的として犯罪者がWebサーバー遠隔操作をするために使用するもの

（4）カード情報保護　国内政策の動向

警察庁が国際ブランドに流出クレジットカード情報の情報連携を開始

2024年12月、警察庁は流出したクレジットカードの情報を国際ブランドであるAmerican Express、Diners club、Discover、JCB、MasterCard、Visaに提供する取り組みを始めました。ダークウェブ等で情報の流出が判明したカード番号を都道府県警察から警察庁が集約し、警察庁が一括して国際ブランドに提供します。提供された情報を元に、国際ブランドはイシュアに連絡してカードの利用停止を求めます。

これまでは、ダークウェブ等でカード情報の流出が判明した場合、 各都道府県警がカード番号を元にカードを発行するイシュアを調査し、会社ごとに情報を提供して利用停止を求めていました。国内のイシュアは約240社あり、調査や連絡に手間と時間がかかっていました。窓口を一本化することで都道府県警の負担が減り、カード利用停止までの時間が短くなることが期待できます。

2. ECにおける不正利用の概況（2024年7-9月）

（1） クレジットカード不正利用被害額の推移

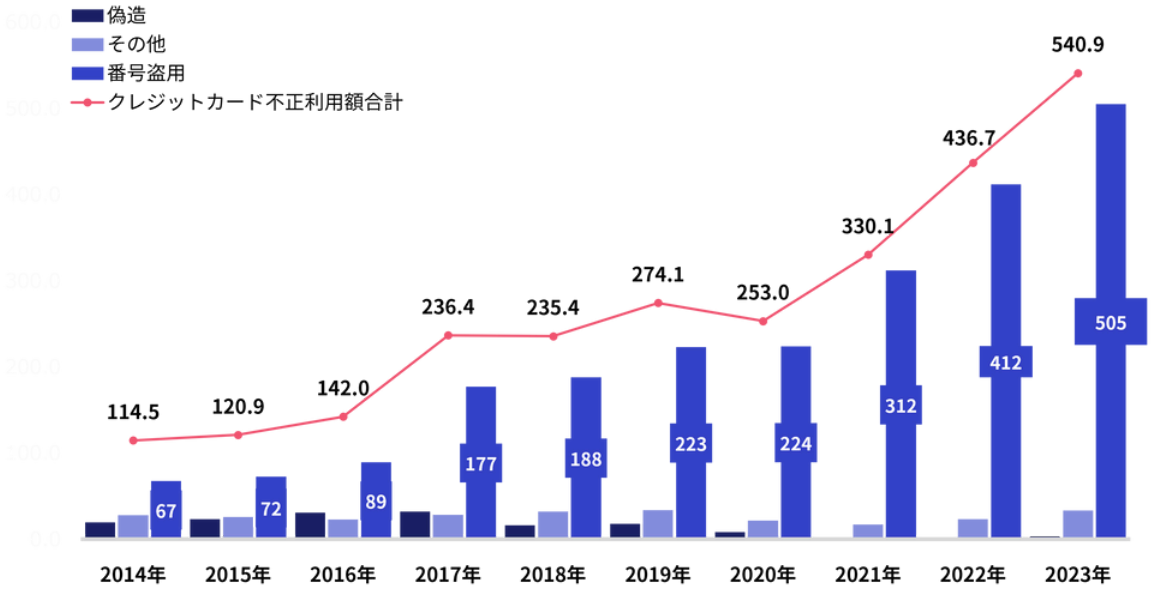
2024 年7-9月のクレジットカード不正利用

- 不正利用被害額合計　132.7億円
- 偽造　2.1億円
- 番号盗用　121.4億円
- その他　9.2億円

※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

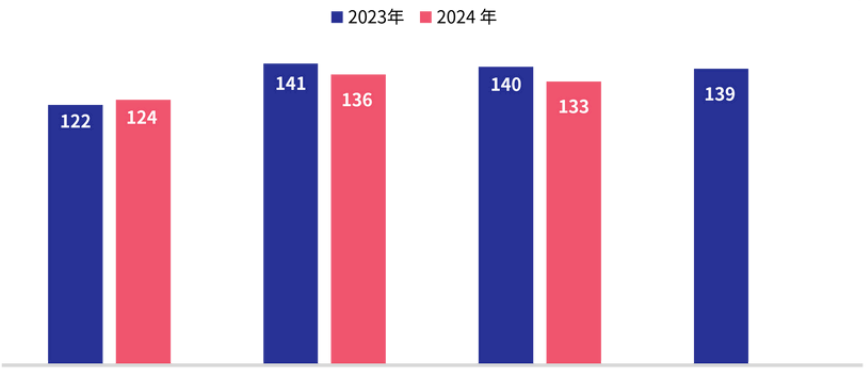
（金額単位：億円）



（『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）2024年9月

2024年のクレジットカード不正利用被害額（前年同四半期比較）

（金額単位：億円）



		1-3月	4-6月	7-9月	10-12月
2024年	偽造	0.7	0.9	2.1	
	番号盗用	115.1	126.3	121.4	
	その他	8.3	8.7	9.2	
	合計	124.1	135.9	132.7	
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

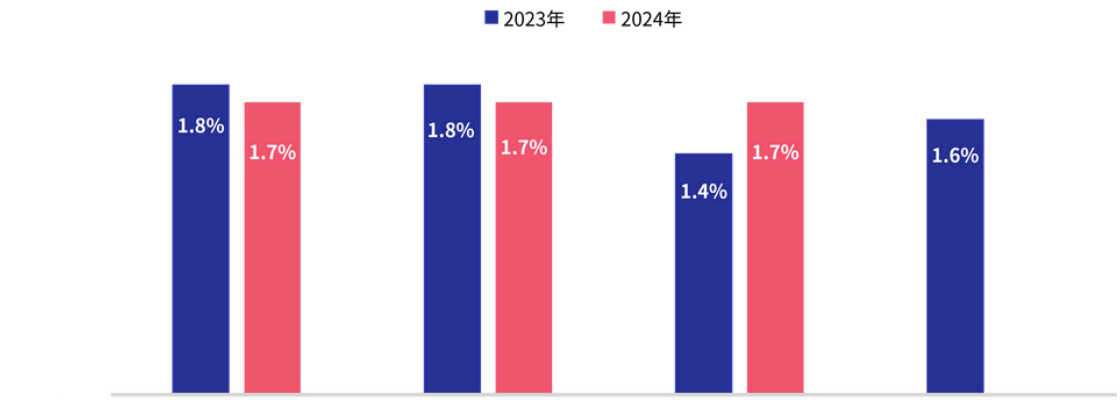
（『クレジットカード不正利用被害額の発生状況』 日本クレジット協会）2024年9月
※2024年4-6月の数値変更を加味して修正（日本クレジット協会より2024年12時点）

2024年7～9月の不正利用被害額は132.7億円と前期（2024年4～6月）比で若干の減少となりました。昨年同期比では4.9%減少しています。内訳としては、番号盗用（なりすましによる不正利用)が全体の9割を占める一方で、偽造による被害額が、全体に占める割合は1.6%と小さいものの被害額が2.1億円と前期同期比で3倍に増加しています。2020年3月末のクレジットカードIC化対応期限以降で初めて四半期で2億円を超える結果となりました。

（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」（Caccoが提供する不正注文検知サービス）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

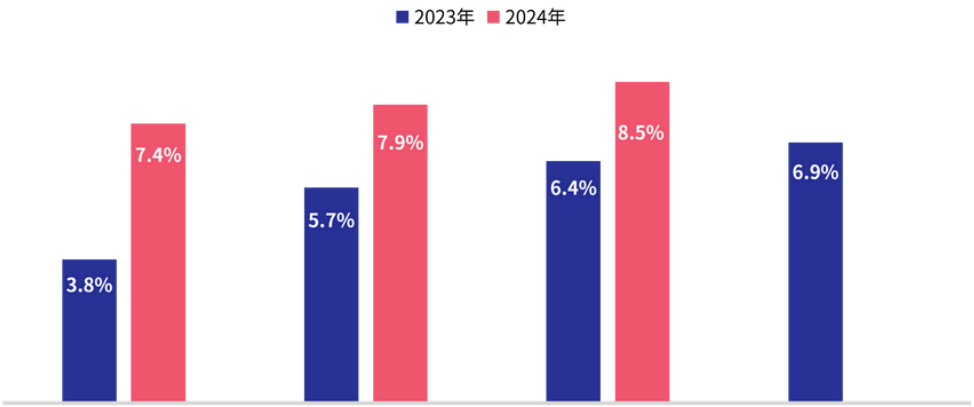
カード不正注文の発生率 （前年同四半期比較）



	1～3月	4～6月	7～9月	10～12月
2024年	1.7%	1.7%	1.7%	
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カード不正注文の審査結果NG割合を件数ベースで算出。（Cacco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。
※2024年12月27日時点で集計

転売不正注文の発生率 （前年同四半期比較）



	1～3月	4～6月	7～9月	10～12月
2024年	7.4%	7.9%	8.5%	
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。（Cacco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。
※2024年12月27日時点で集計

カードの不正注文の発生率は1.7%とこれまでと変わらず、特に大きな変動は見られませんでした。転売不正の発生率は2023年1月から増加傾向が続いています。今回は8.5%と、2020年 に調査を開始して以来最も高くなりました。内訳としては、これまでと同様にコスメ、健康食品、日用品などの分野で多く発生しています。

＜不正注文に狙われやすい商材ランキング＞

2024年（4-6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	総合通販
2位	チケット	8位	日用品・雑貨・キッチン用品
3位	ホビー・ゲーム	9位	食品・飲料・酒類
4位	健康食品・医薬品	10位	工具
5位	PC・タブレット・家電	11位	ふるさと納税
6位	コスメ・ヘアケア	12位	サブスクサービス

2024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	日用品・雑貨・キッチン用品
2位	イベント	8位	PC・タブレット・家電
3位	ホビー・ゲーム	9位	食品・飲料・酒類
4位	健康食品・医薬品	10位	コンタクト・メガネ
5位	総合通販	11位	工具
6位	コスメ・ヘアケア	12位	サブスクサービス

※「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。（Cacco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。
※2024年12月27日時点で集計

（3）2024年9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

フィッシング攻撃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、2023年3月に経済産業省、警察庁、総務省が連名で、カード発行会社（以下イシュア）に対してDMARC導入をはじめとしたメールによる、なりすまし対策を要請しました。

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。リンクは、経済産業省のウェブサイトで公開されているイシュア243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）243社

【調査実施時期】

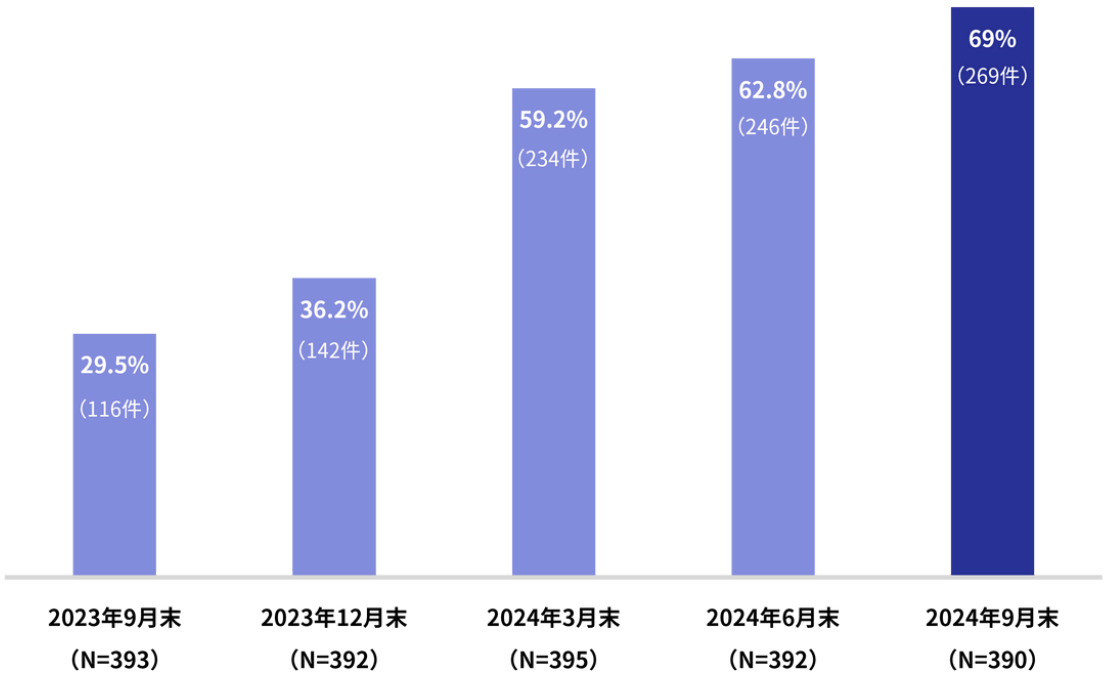
2024年9月末

【調査結果】

① 調査対象ドメイン数　390件

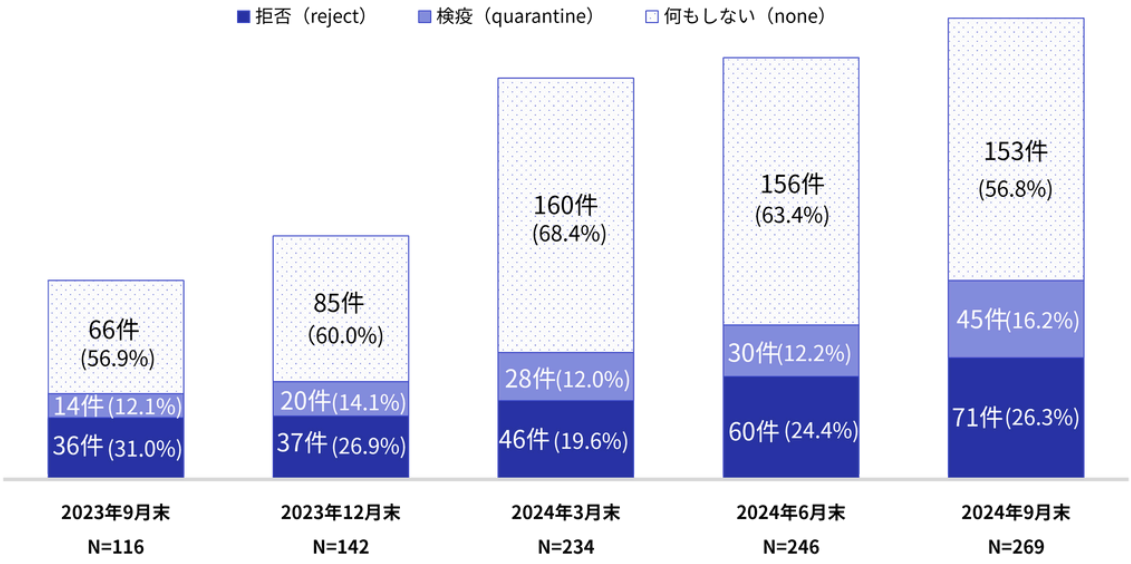
② 調査対象ドメインごとのDMARC対応状況と運用ポリシー

ドメインごとのDMARC設定率（DMARCを有効にしているドメインの割合）



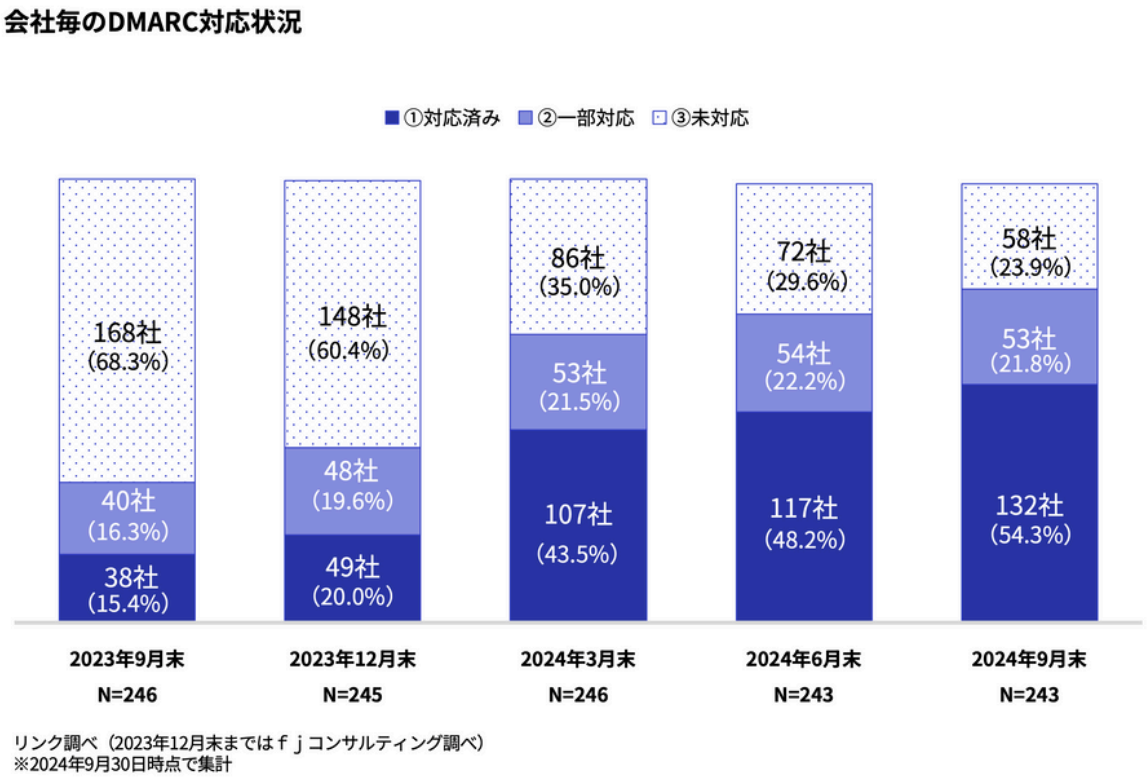
リンク調べ（2023年12月末まではｆｊコンサルティング調べ）
※2024年9月30日時点で集計

ドメイン毎のDMARCポリシー



リンク調べ（2023年12月末まではｆｊコンサルティング調べ）
※2024年9月30日時点で集計

③会社ごとのDMARC対応状況



リンク調べ（2023年12月末まではｆｊコンサルティング調べ）
※2024年9月30日時点で集計

2024年9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390件のうち、有効なDMARCレコードが設定されているのは269件（69.0%）と引き続き増加し、7割に迫っています。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71件（26.3%）と4分の１を超えました。ポリシーを「quarantine（検疫）」に設定したドメインが45件（16.2%）に増えており、ポリシーを「none（何もしない）」に設定したドメイン数は153件（56.8%）となりました。noneのドメインの数自体も153件から156件とわずかにですが減少しており、DMARCレコードを設定するだけにとどまらず、ポリシーを見直し実効性を持たせた運用が進んできていることがうかがえます。

組織別にみると、DMARCを一部でも導入しているイシュアは185社（76.1%）となっており、132社（54.3%）はコーポレートドメインおよび委託先も含めたメール送信に使用する全てのドメインでDMARC導入済みとなっています。全てのドメインにDMARC導入済みのイシュアの割合が５割を超えました。

（4）不正利用のトピック

①Apple Payに不正登録されたカードが不正利用され続ける理由

クレジットカードの不正利用が発覚した際、カード会社に連絡し、カードの利用を停止することで被害の拡大を防ぎます。しかし、カードを止めた後も不正利用被害が続く事件が確認されました。中には、停止後に数か月間にわたって被害が続くケースもありました。なお、この場合でも、不正利用被害はカード保有者が負担することなく、全てイシュアによって補償されるとのことでした。

カードを停止しても不正利用が止まらないのは、「オフライン取引」が悪用されているからと推測されます。オフライン取引とは、決済時にネットワークを通じてカードの利用可否を確認する「オーソリゼーション（与信確認、以下オーソリ）」を即時に行わない取引のことです。この仕組みは、一定以下の少額決済において、決済のスピードや利便性を高めるために導入されているという背景があります。一方で、オーソリを省略する場合があるため、停止されたカードでも決済が可能となるという脆弱性があります。国際ブランドでは、原則、全取引に対しオーソリを必須にするなど、オフライン取引のリスクを最小限に抑えるシステムの見直しや対策が進められています。

この脆弱性を悪用して、Apple Payの支払手段として他人のカードを不正登録し、一定以下の少額で不正利用を繰り返す手口が多発しました。Apple Payに直接クレジットカードを登録する場合は、SMSなどへのワンタイムパスワードなど本人認証が追加で求められるため、他人のカードを登録することは困難です。しかし、あるイシュアでは、カード会員の利便性を高めるため、自社のスマートフォンアプリにログインさえすれば、カード番号や有効期限のみならず、SMSなどに送信するワンタイムパスワードによる本人認証も実施せずにApple Payにカードを登録できてしまう仕様となっていました。犯人はこれを悪用して、フィッシング等で取得した認証情報でカード会員向けアプリにログインし、自分のスマートフォンのApple Payにカード情報を登録したと推察されます。ひとたび登録に成功すると、一定以下の少額決済はオフライン取引で行われるため、カード会社に連絡してカードを停止しても決済が止まらない状態が続きました。

こうした手口を防ぐために、イシュアは、カード会員向けのアプリのログインに多要素認証やパスキー（生体認証などを使用した、パスワードを使用しない認証）を導入して不正ログインを防止することと合わせて、Apple PayやGooglePayへのカードの登録時にはSMSによるワンタイムパスワードなど追加の本人認証を要求し、不正な登録を防ぐことが必須であると考えます。

②EC事業者の不正利用対策状況と主な取り組み

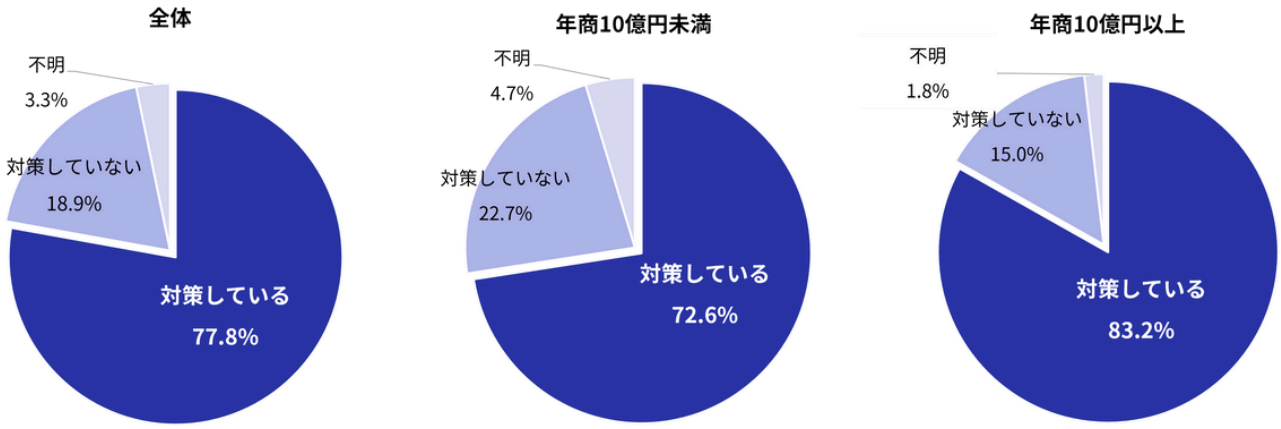
Caccoは、EC事業者における不正注文や不正アクセスなどのセキュリティ意識や不正対策の実態について、独自に調査を実施しました。調査結果の中から、不正利用対策状況と取り組みについてご紹介します。

【調査概要】
•調査時点：2024年11月
•調査対象：EC事業者※で不正対策に関わる担当者
•有効回答数：550件
•調査方法：ネット方式によるアンケート調査
※ 年商規模10億円未満：277件（50.4%）、10億円以上：273件（49.5%）

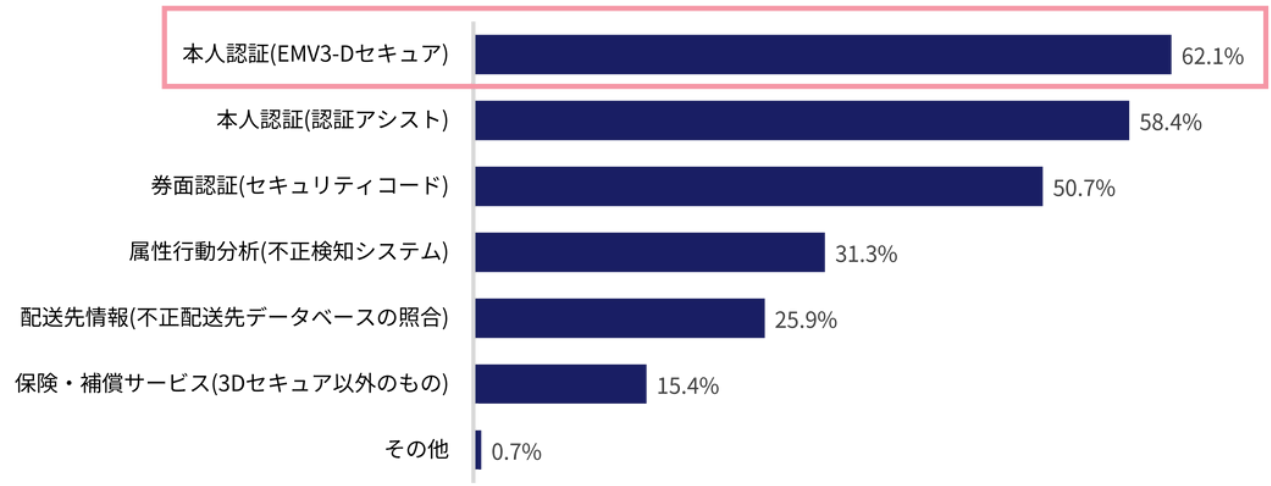
【調査結果】
不正利用対策を実施しているEC事業者は全体の77.8%に達しており、前年同様、多くの事業者が対策を講じていることがわかります。特に、年商10億円以上の事業者では、不正利用対策の実施率が81.8%とさらに高くなっており、対策意識がより高い傾向がみてとれます。

実際に取り組んでいる不正対策の手法としては、本人認証のEMV 3-Dセキュアが最も多く利用されており、不正対策を実施している事業者の62.1%と過半数を占めています。2025年3月にすべてのEC事業者に導入が必須化されていることも相まって、今後より導入が進むことが期待されます。

Q：クレジットカード不正や悪質転売などの不正注文対策をしていますか。



Q：実施している対策方法はなんですか（複数回答）



一方で、不正手口の巧妙化によりEMV 3-Dセキュアだけでは防ぎきれないケースも出てきており、複数の対策を併用することが重要となっています。EMV 3-Dセキュアを導入している事業者のうち、37.6%と3分の1以上がEMV 3-Dセキュアと属性行動分析を基盤とする不正検知システムを併用しています。

このようにEC事業者の重層的な不正利用対策が少しずつ進んでいるにもかかわらず、ここ3年は毎年約100億円ずつクレジットカード不正利用被害額が増加しています。「クレジットカード・セキュリティガイドライン5.0版」では、決済前・決済時点・決済後の場面ごとに不正利用対策を導入する「線の考え方」を示しています。決済時点における対策のEMV3-Dセキュアの導入をもって対策が完了したと考えるのではなく、決済前の会員登録やログインにおける対策、決済後の顧客情報等の確認など、一貫した不正対策に継続的に取り組んでいくことが重要です。

【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

株式会社リンク
セキュリティプラットフォーム事業部　担当：滝村・加藤・相原
Mail: spdsales@link.co.jp
Tel:03-6704-9090