Cashless Security Report

Quarterly Report

（2025年 1-3月版）2025年8月発行

PCI DSS Ready Cloud

2025.8.8

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2025年1-3月版：2025年7月発行ー

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（2025 年1-3月）

（1）カード情報流出事件数・情報流出件数の推移

2025年1-3 月のカード情報流出事件

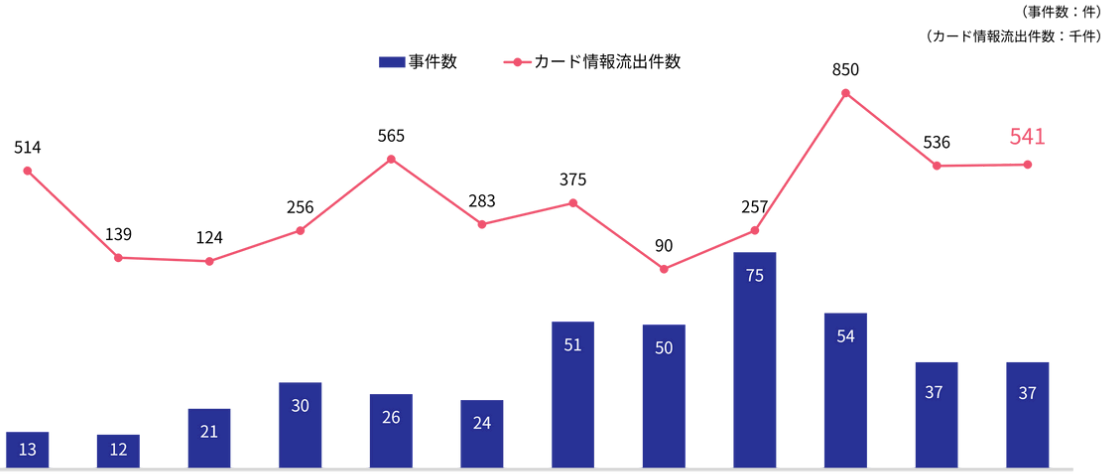
- 事件数　6件
- カード情報流出件数　19,635件

※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

2024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	2024
事件数	13	12	21	30	26	24	51	50	75	54	37	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	540,722

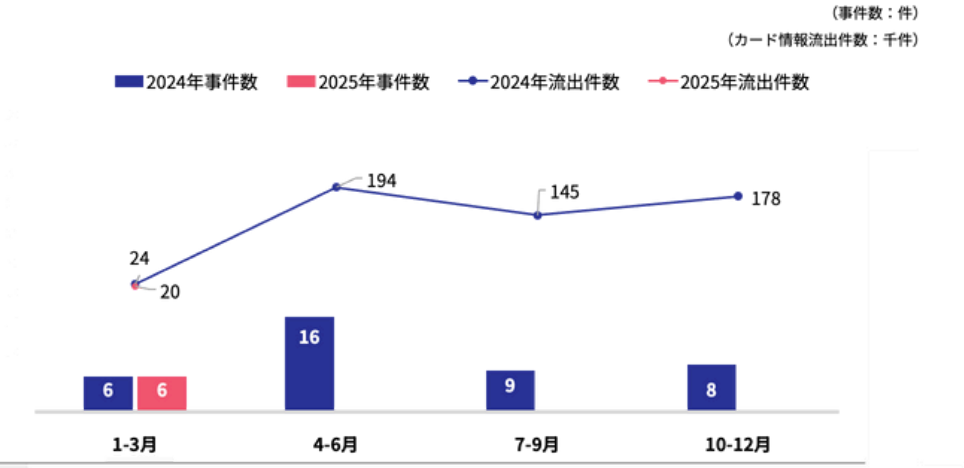
（Cacco・ｆｊコンサルティング調べ）

※1 2021年以前のデータはｆｊコンサルティング調べ

※2 2024年7-9月分の流出事件の追加と、2024年10－12月の流出件数が公開されたことにより2024年の数値を以下の通り訂正
事件数　36→37、流出件数　520,074→540,722

※3 2025年7月11日時点で集計

2025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
2025年	事件数	6			
	カード情報流出件数	19,635			
2024年	事件数	6	16	7	8
	カード情報流出件数	23,677	194,241	145,032	177,772

（Cacco・リンク調べ）

※1 2024年7-9月分の流出事件の追加と、2024年10－12月の流出件数が公開されたことにより2024年の数値を以下の通り訂正
2024年7-9月分 事件数6→7/流出件数137,577 → 145,032、2024年10-12月分 流出件数164,579 → 177,772

※2 2025年7月11日時点で集計

2025年1～3月に公表されたカード情報流出事件は6件です。うち1件は流出件数や流出期間などの詳細が判明する前に一報として事件の発生を公表したものです。流出したカード情報の件数は19,635件となり、前年同期比で約4,000件の減少となりました 。

なお、2024年に公表された事件について、集計時点（2025年7月11日）までに判明した追加情報を踏まえ、関連する数値を更新しました。
1) 2024年7-9月 に事件数1件・カード情報流出件数7,455件を追加（詳細調査後にクレジットカード情報流出が判明した事件を追加）
2）2024年10-12月にカード情報流出の発生は公表していたが、詳細不明となっていた１事件について、判明したカード情報流出件数13,193件を追加

（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		2024年4-6月		2024年7-9月		2024年10-12月		2025年1-3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		16	194,241	7	145,032	8	177,772	6	19,635
業種別	アパレル	3	17,176	0	0	1	71,943	0	0
	コスメ	1	15,198	0	0	0	0	0	0
	食品	8	126,746	5	136,145	3	67,489	4	17,726
	家電・電子機器・PC	0	0	0	0	1	4,257	0	0
	生活雑貨、家具、インテリア	1	0	1	1,432	0	0	1	2,460
	健康食品	0	0	0	0	1	4,494	0	0
	ホビー	1	4,969	0	0	1	0	1	1,909
	自動車、バイク	0	0	0	0	0	0	0	0
	家具	1	3,958	0	0	0	0	0	0
	その他	1	26,467	1	7,455	1	16,396	0	0
カード会社		0	0	0	0	0	0	0	0

（Cacco・リンク調べ）
※1 2024年7-9月分の流出事件の追加と、2024年10－12月の流出件数が公開されたことにより2024年の数値を以下の通り訂正
7-9月分その他の流出件数　0→1/ 流出件数　0→7,455、 加盟店合計 137,577→145,032、10-12月分ホビーの流出件数　0→13,193、加盟店合計 164,579→177,772
※2 2025年7月11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	2024年4-6月		2024年7-9月		2024年10-12月		2025年1-3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	1	8,073	0	0	1	4,257	0	0
3ヶ月-1年	2	5,621	0	0	1	6,929	1	13,094
1-3年	9	113,120	3	25,132	0	0	0	0
3年以上	4	67,427	4	119,900	6	166,586	4	6,541

（Cacco・リンク調べ）
※1 2024年7-9月分の流出事件の追加と、2024年10－12月の流出件数が公開されたことにより2024年の数値を以下の通り訂正
7-9月3年以上　事件数3→4　流出件数112,445→119,900、/　10-12月 3年以上　事件数5→6　流出件数153,393→166,586
※2 2025年7月11日時点で集計

業種/商材別にみると、「食品」が事件数4件（うち1件は詳細なカード情報の流出不明）となっています。カード情報流出件数と流出期間が公表されている全体の5件のうち、流出開始が2021年以前で流出期間が3年以上に及ぶケースは4件を占めています。この4件のうち3件は警察からの情報流出の指摘により調査を開始し、実際に流出したことが確認されたものです。残りの1件も発覚のきっかけは外部機関の指摘によるものとしています。2024年から始まった警察によるカード情報流出事件の調査と個別企業への指摘が続けて成果を上げている様子が伺えます。

（3）カード情報流出事件トピック

インフォスティーラーによる個人情報漏えいの増加

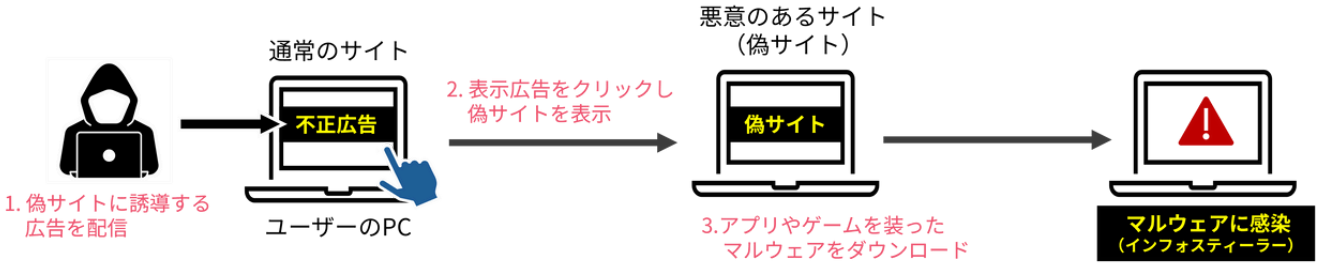
インフォスティーラーとは、情報窃取に特化したマルウェアの総称です。以前から存在は確認されていましたが、2024年頃から被害報告が増えています。一度感染すると自身のパソコンやサーバーのバックグラウンドで動作し、コンピューターやブラウザに保存されている情報、クリップボードデータ、スクリーンショット及びキーロガー機能を使用して入力したログイン認証情報や決済時のクレジットカード情報などを窃取し、外部サーバーに送信します。

フィッシングに注意して偽サイトにログイン認証情報やカード情報などを入力しないように注意していても、インフォスティーラーに感染していると知らないうちに流出することになります。2025年初めごろから急増している証券口座不正利用事件でも、一部はインフォスティーラーによって窃取されたログイン認証情報が悪用されていると言われています。実際に全くフィッシングにあった覚えのない利用者が、証券口座を不正利用されたと申し出ている事例があります。流出した情報は、これまでダークウェブなどの通常の手段ではアクセスできない場所で流通していましたが、2023年以降テレグラム（匿名性の高いメッセージングアプリ）のチャンネルを利用した売買が増えています。

インフォスティーラーの感染経路は多様化しており、メールの添付ファイルを開かせたり、本文に記載されたURLをクリックさせてマルウェアをダウンロードさせる方法以外にも以下のような方法が確認されています。

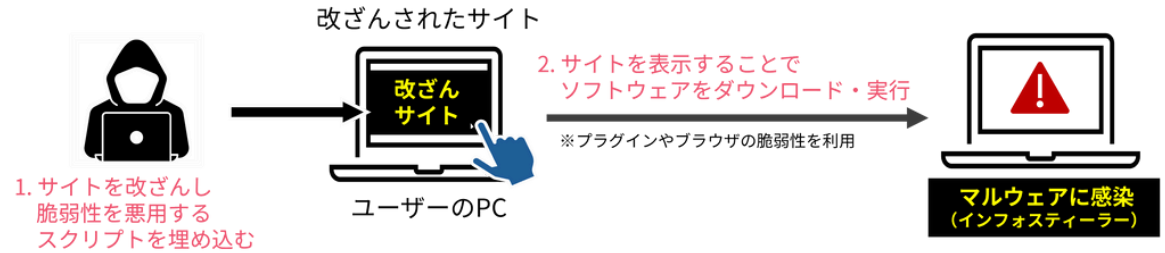
①インターネット広告の悪用（マルバタイジング）

SNS広告などで誘導されたサイトで、ゲームアプリや無料情報をダウンロードするよう促し、マルウェア入りのソフトウェアをダウンロード・実行させる手口です。



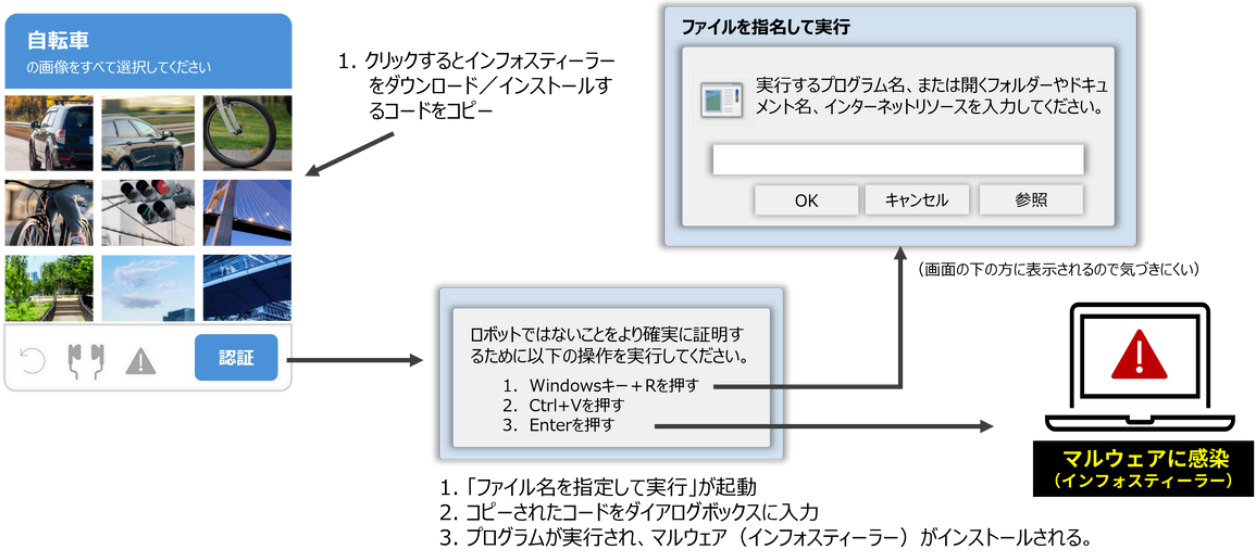
②ドライブバイダウンロード

改ざんされた正規サイトや偽サイトを閲覧するだけで（ページを開くだけで）マルウェアがダウンロード・実行されます。



③Click Fix（偽CAPTCHA）

Webサイトのフォームで、利用者がロボットではないことを確認するために使用する「CAPTCHA認証」を悪用した手口です。CAPTCHA認証では、メッセージに従って表示される画像を選択しますが、ClickFixでは画像を選択するためにクリックすると裏側でJavaScriptが実行され、インフォスティーラーをインストールするためのコードがクリップボードにコピーされます。続けて、「ロボットではないことをより確実に証明するために以下の操作を実行してください」等のメッセージと共に、「Windowsキー＋R」「Ctrl+V」「Enter」の順に押すよう促されます。「Windowsキー+R」はWindowsで「ファイル名を指定して実行」ダイアログボックスを開かせるためのショートカットです。続けて「Ctrl+V」を押すことで開いたダイアログボックスに先の操作でクリップボードにコピーされたコマンドを入力し、「Enter」キーを押すことで実行させます。一連の操作により、インフォスティーラーがPCにダウンロードされ、インストールされてしまいます 。



インフォスティーラーがインストールされた場合、Webサイトに決済のために入力したカード情報がキーロガーによって窃取される可能性があります。それらのカード情報は、ダークウェブで販売されたり、不正利用されるリスクがあります。また、外部サイトの認証情報が窃取されることでクレジットカードを不正利用されるリスクもあります。例えばイシュアの会員向けサイトの認証情報が窃取され場合、不正ログインされ、多要素認証やEMV 3-Dセキュアのワンタイムパスワード送付先を変更されたり、ApplePayなどのスマートフォン決済の支払手段としてカード情報を他人のスマートフォンに不正に登録されてしまう可能性があります。ECサイトの認証情報が窃取された場合は、商品の送付先情報を変更して不正な買い物をされることも考えられます。

インフォスティーラーがバックグラウンドで動作していても、多くの場合パソコンの挙動には変化がなく、気づくのは困難です。情報の窃取実行の直後に自身をアンインストールするものも確認されているため、事象発覚後に調査してもマルウェアの痕跡が発見ができないこともあります。イシュアの会員向けサイトやECサイトなど、サービス提供側が、インフォスティーラーによる被害の可能性を減らすためには、ログイン時だけではなく、上述の連絡先変更や支払手段の追加などのイベント毎に多要素認証を要求することが有効と考えられます。また、利用者に対してはインフォスティーラーのリスクを啓発し、疑わしい添付ファイルやURLを開かない、マルウェア対策ソフトの導入によるファイルダウンロード時のリアルタイムスキャンや定期的なスキャンなどを周知する必要があります。

2. ECにおける不正利用の概況（2025年1-3月）

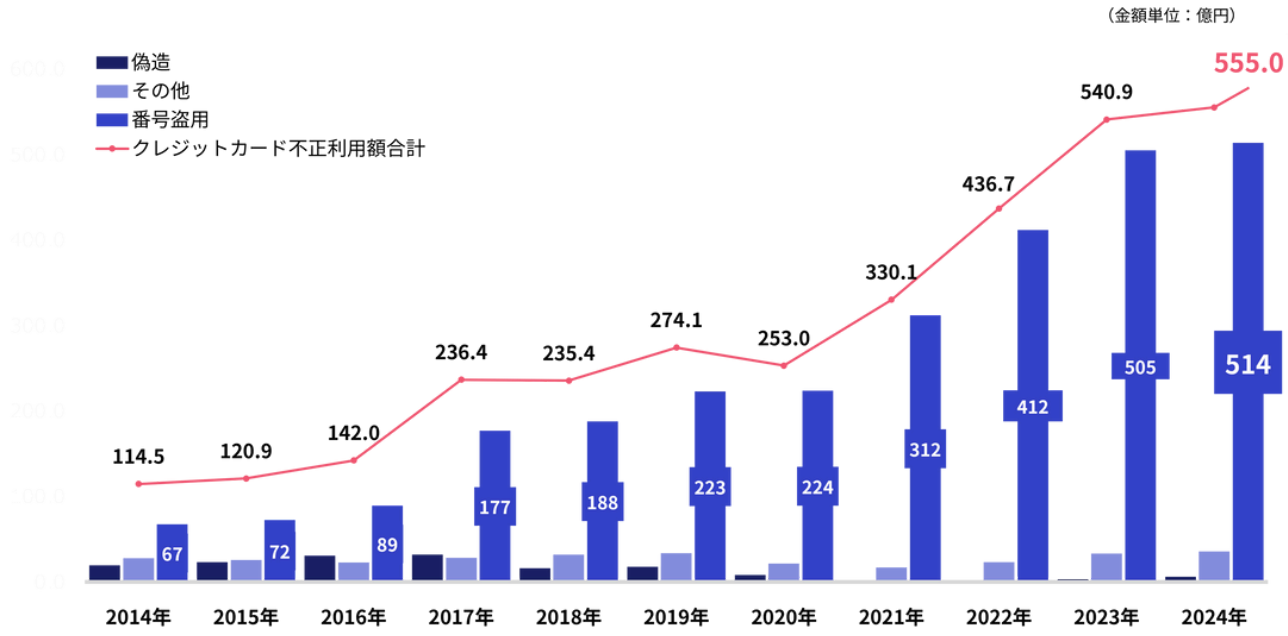
（1） クレジットカード不正利用被害額の推移

2025 年1-3月のクレジットカード不正利用

- 不正利用被害額合計　193.2億円
- 偽造　1.8億円
- 番号盗用　182.9億円
- その他　8.5億円

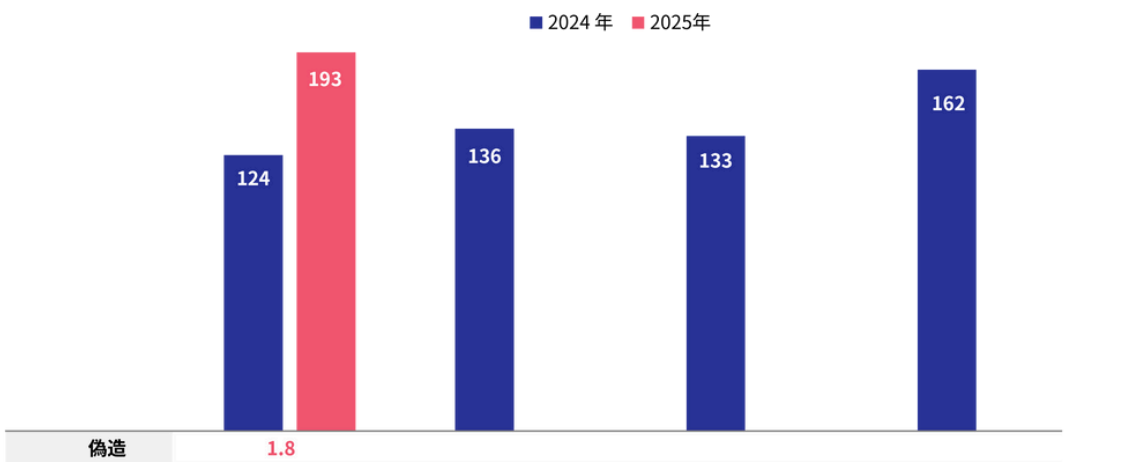
※日本クレジット協会調べ
https://www.j-credit.or.jp/information/statistics/index.html

2024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』 日本クレジット協会）2025年6月

2025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）



2025年	偽造	1.8			
	番号盗用	182.9			
	その他	8.5			
	合計	193.2			
2024年	偽造	0.7	0.9	2.1	2.2
	番号盗用	115.1	126.3	121.4	150.7
	その他	8.3	8.7	9.2	9.4
	合計	124.1	135.9	132.7	162.3

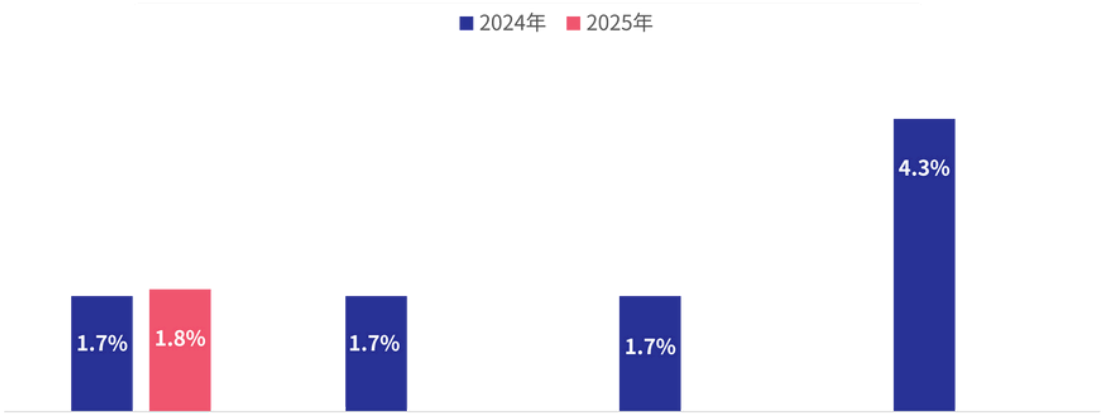
（『クレジットカード不正利用被害額の発生状況』 日本クレジット協会）2025年6月

2025年1～3月期のクレジットカード不正利用被害額は193.2億円となり、前年同期（124.1億円）から約69.1億円、55.7%の増加となりました。「番号盗用」による被害が9割以上を占めている傾向が継続しております。カード加盟店に対するEMV 3-Dセキュア義務化により、導入が進んでいるにもかかわらず、2025年1～3月期の被害額が対前年四半期と比較し大きく増加した理由は、過年度の不正利用被害の期ずれによる計上が要因であることも想定されます。EMV 3-Dセキュア義務化の効果については、今後の動向を慎重に見極める必要があり、次の四半期（2025年4～6月期）の推移に引き続き注視が必要です。

（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 Payment Protection」（Caccoが提供する不正検知サービス）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

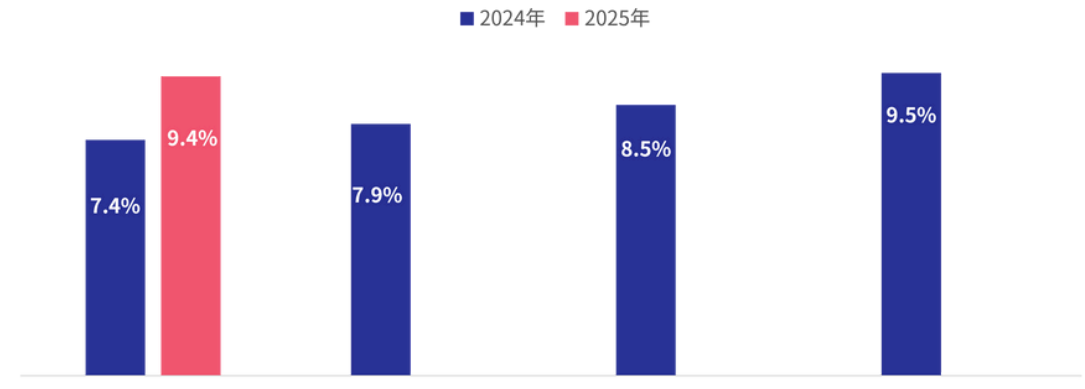
カード不正注文の発生率 （前年同四半期比較）



	1～3月	4～6月	7～9月	10～12月
2025年	1.8%			
2024年	1.7%	1.7%	1.7%	4.3%

※「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。
※2025年5月11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
2025年	9.4%			
2024年	7.4%	7.9%	8.5%	9.5%

※「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。
※2025年7月11日時点で集計

2025年1～3月期におけるクレジットカード不正注文発生率は前年同時期と比べて微増しており、特に「転売不正注文」の割合が依然として高水準で推移しています。加えて、「不正注文に狙われやすい商材ランキング」からは、ライブチケットや遊園地などのエンタテインメント系チケットなどの需要が春休みに増えたこともあり、被害が特に増えたと推測されます。また、ゲーム機器や家電製品といった換金性の高い商材が引き続き標的となっている傾向が見られました。

＜不正注文に狙われやすい商材ランキング＞

2024年（10-12月） 商材別不正注文検知数ランキング			
1位	カメラ・映像機器・音響機器	7位	コスメ・ヘアケア
2位	ホビー・ゲーム	8位	総合通販
3位	イベント	9位	日用品・雑貨・キッチン用品
4位	デジタルコンテンツ	10位	食品・飲料・酒類
5位	ふるさと納税	11位	PC・タブレット・家電
6位	健康食品・医薬品	12位	コンタクト・メガネ

2025年（1-3月） 商材別不正注文検知数ランキング			
1位	イベント	7位	日用品・雑貨・キッチン用品
2位	ホビー・ゲーム	8位	食品・飲料・酒類
3位	健康食品・医薬品	9位	デジタルコンテンツ
4位	総合通販	10位	PC・タブレット・家電
5位	コスメ・ヘアケア	11位	サブスサービス
6位	アパレル	12位	旅行

※「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。
※2025年7月11日時点で集計

（3）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Webサイトで公開されているイシュア242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）242社

【調査実施時期】

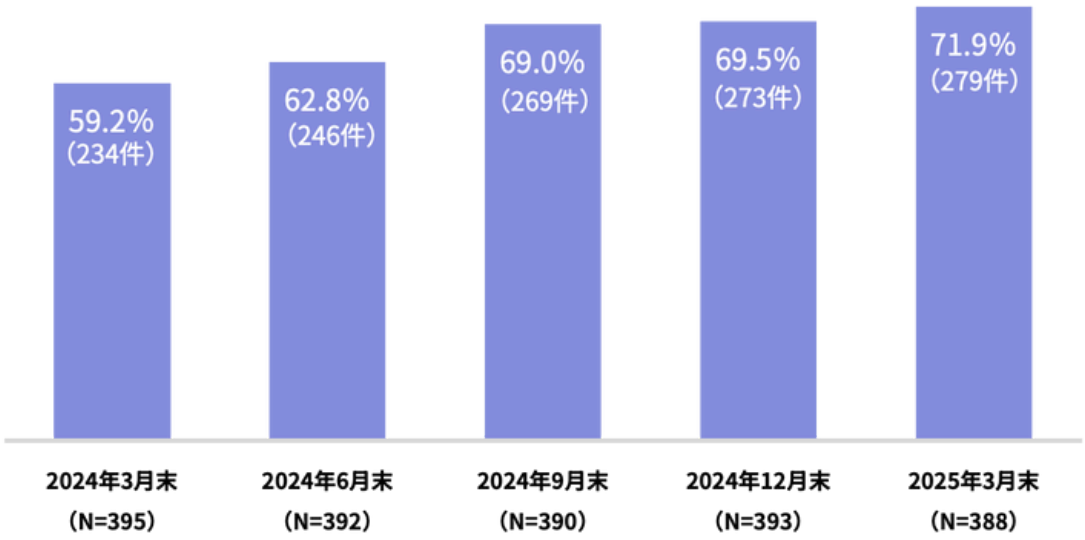
2025年3月末

【調査結果】

①調査対象ドメイン数　388件

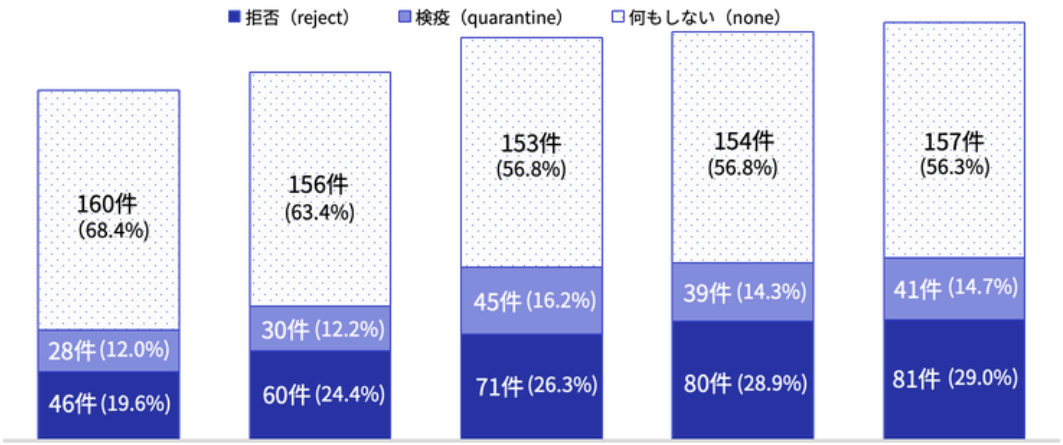
②調査対象ドメインごとのDMARC対応状況と運用ポリシー

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）



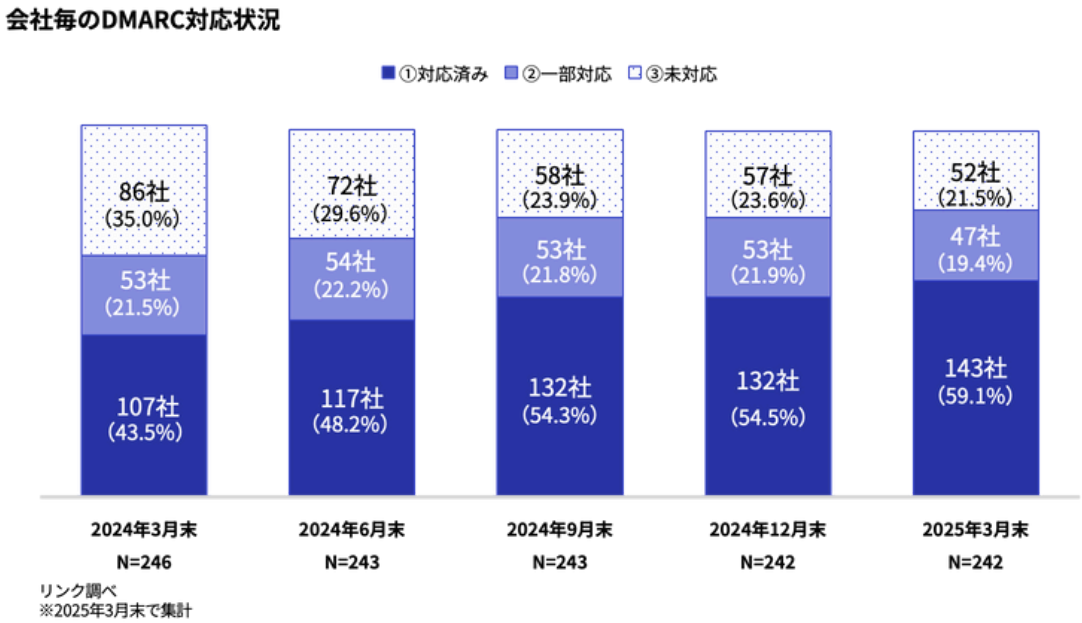
リンク調べ
※2025年3月末に集計

ドメイン毎のDMARCポリシー



リンク調べ
※2025年3月末で集計

③会社ごとのDMARC対応状況



2025年3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388件のうち、有効なDMARCレコードが設定されているのは279件（71.9%）となり、初めて7割を超えました。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81件（29.0%）と微増、ポリシーを「quarantine（検疫）」に設定したドメインが41件（14.7%）と、こちらも微増です。ポリシーを「none（何もしない）」に設定しているドメイン数は157件（56.3%）とほぼ横ばい状態です。

組織別にみると、DMARCを一部でも導入しているイシュアは190社（78.5%）、うち143社（59.1%）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。1年前（2024年3月末）と比較すると、全てのドメインでDMARC導入済みのイシュアの割合は43.5%から59.1%に増加していますが、引き続き未対応のイシュアの導入促進および未対応のドメインのDMARC導入を促進する必要があります。

（4）不正利用のトピック

他人のクレジットカードで「投げ銭」購入

近年、クレジットカードの不正利用が増え続ける中で、インターネットのライブ配信プラットフォームの「投げ銭」用のコインを不正に購入する事件が起きています。投げ銭とは、ライブ視聴者が配信者に対してプラットフォーム内で購入したギフト（コインやアイテム）を送る行為です。ライブ配信者側はギフトを換金することで、金銭的な対価を得ることもできます。

2024年5月から11月にかけて他人のカードを使って約4,600万円分の投げ銭用コインを不正に購入したとして、京都府警にて2025年4月、犯人Aが摘発されました。Aは発覚を避けるため、不正入手した196件のカード情報と複数のアカウントを使いコインを購入し、複数のライブ配信者に投げ銭を繰り返していました。また、AはSNSでカード不正利用に関する情報交換を行うグループに参加していたと報じられており、不正利用されたカード情報はそのグループで入手したものと推測されます。

2025年3月には、他人のクレジットカードでコインを購入し、自らのライブ配信に投げ銭することで金銭的な利益を得ていた高校生Bが逮捕されました。Bは他人になりすまして不正に携帯電話の回線契約を行い、その回線のスマートフォンで作成したライブ配信プラットフォームのアカウントで他人のカードを不正利用してコインを購入。そのアカウントから自分のアカウントのライブ配信に約100万円分の投げ銭を行い、手数料を差し引いた約50万円を得ていました。

投げ銭用のコインは無形のデジタル商材であることから、不正な購入後にライブ配信プラットフォーム側で利用を止めるのは困難です。物理的な配送が不要で配送先住所などの情報がなく、配信者側への提供（投げ銭）もリアルタイムで完了します。サービスを運営する事業者が不正購入に気づいても、コインの取引を止めたり、回収したりする手段がありません。同様にオンラインゲーム内アイテムの不正購入も横行しています。これも無形のデジタル商材であるため、被害に気づきにくく、対応が後手に回ることが多いという問題があります。

今後、こうした無形のデジタル商材を狙った不正利用は更に増える可能性があり、事業者側では、それらの購入の度、EMV 3Dセキュアの導入による本人認証を確実に行うと同時に、新規アカウントの登録時、ログイン時、登録カードの変更時など利用者の活動全体の不正利用検知の強化が求められます。

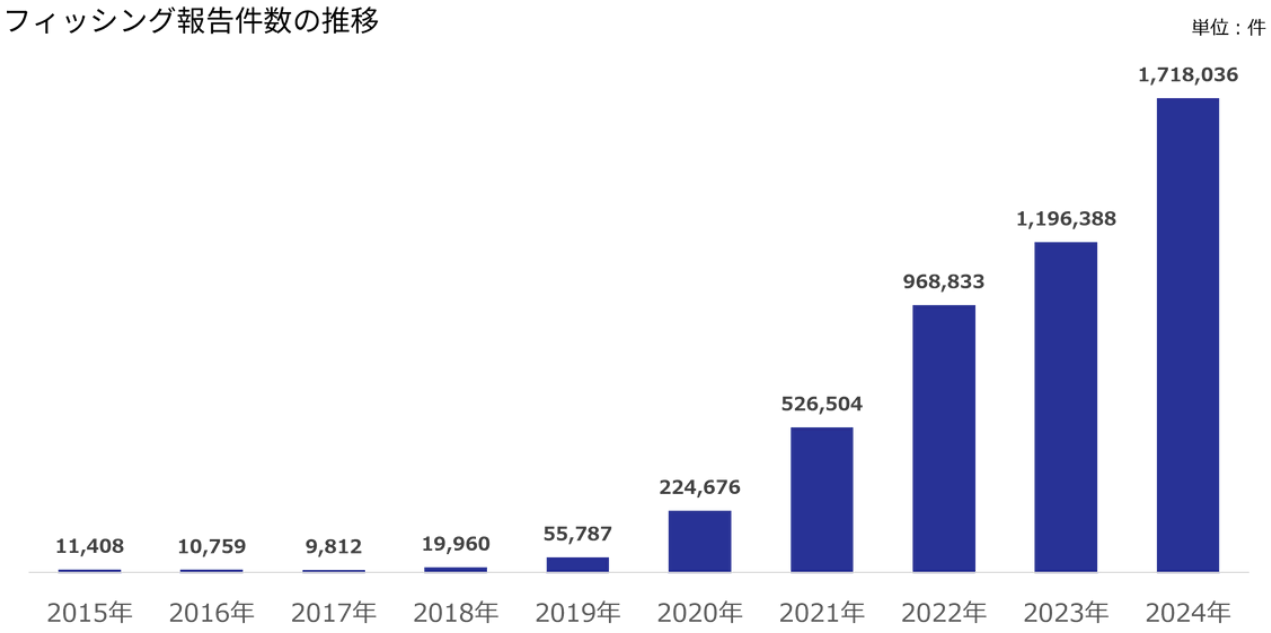
>>> 3. 政策の動向

カード会社と日本クレジットカード協会などが 共同でフィッシングサイト閉鎖の取り組みを開始

カード会社8社（イオンフィナンシャルサービス、NTTドコモ、クレディセゾン、ジェーシービー、三井住友カード、三菱UFJニコス、ユーシーカード、楽天カード）とアクシオン社及び日本クレジットカード協会（JCCA）は、フィッシングメールによるカード情報やログイン認証情報などの詐取を防ぐために、フィッシングサイトを閉鎖（テイクダウン）する取り組みを2025年4月から共同で開始しました。

この取り組みでは、アクシオン社の技術によってフィッシングサイトを能動的に検知することだけではなく、当該サイトを閉鎖す るための各所への届出などを実施します。具体的には、GoogleなどのWebブラウザの提供企業へのフィッシングサイトの申告、当該サーバーをホスティングするインターネットサービスプロバイダー（ISP）へ犯罪行為に利用されていることを通報、ドメイン登録事業者へのドメイン無効申請、フィッシング対策協議会への通知などを実施します。

多くのカード会社は、自社ブランドを騙るフィッシングサイトを閉鎖する取り組みを実施しています。しかし、フィッシングで悪用されるサービスや企業はECサイトや公共インフラ・サービスなどに多様化しています。JCCA、カード会社8社、アクシオンは、フィッシングサイト閉鎖の取り組みを進めると共に、フィッシングサイトが多く報告される企業や業界団体に対し、自主的な閉鎖対応の要請や必要なノウハウの提供を通じてフィッシングサイト閉鎖に取り組む環境整備を呼びかけるとしています。



（『フィッシングレポート2024』 フィッシング対策協議会）2024年6月

日本クレジットカード協会（JCCA）
国内カード発行会社が加盟する業界団体。CCT共同利用端末やネットワークに関する各種ガイドラインの策定、クレジットカードの不正対策の調査・研究、PR、行政や他団体との連携により制度整備などを行なっている。
https://www.jcca-office.gr.jp/

株式会社ACSiON（アクシオン）
セブン銀行と電通総研の合弁で設立されたフィンテック企業。フィッシングサイトの検出・通知・テイクダウン依頼対応をワンストップで提供するフィッシング対応サービスを提供する。
https://www.acsion.co.jp/

【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
担当：相原・滝村
Mail: spdsales@link.co.jp
TEL：03-6704-9090

【編集】
瀬田 陽介（YSコンサルティング株式会社　代表取締役）
板垣 朝子（YSコンサルティング株式会社）
滝村 享嗣（株式会社リンク　セキュリティプラットフォーム事業部長）
前田 亜由美（かっこ株式会社）