Cashless Security Report

Quarterly Report

（2025年 10-12月版）2026年4月発行

PCI DSS Ready Cloud

2026.4.21

キャッシュレス・セキュリティレポート

ー2025年10-12月版：2026年4月発行ー

かっこ株式会社
株式会社リンク

>>> 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10-12月）

（1）カード情報流出事件数・情報流出件数の推移

2025年10-12月のカード情報流出事件

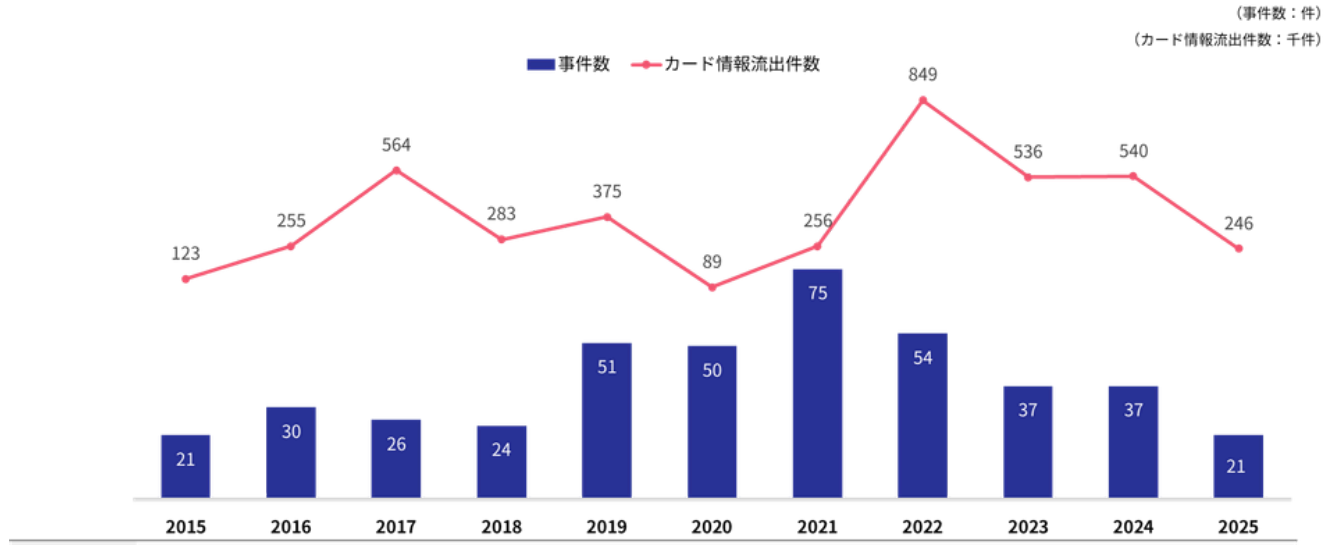
- 事件数　5件
- カード情報流出件数　19,650件

※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

2025年までのカード情報流出事件数・情報流出件数の推移



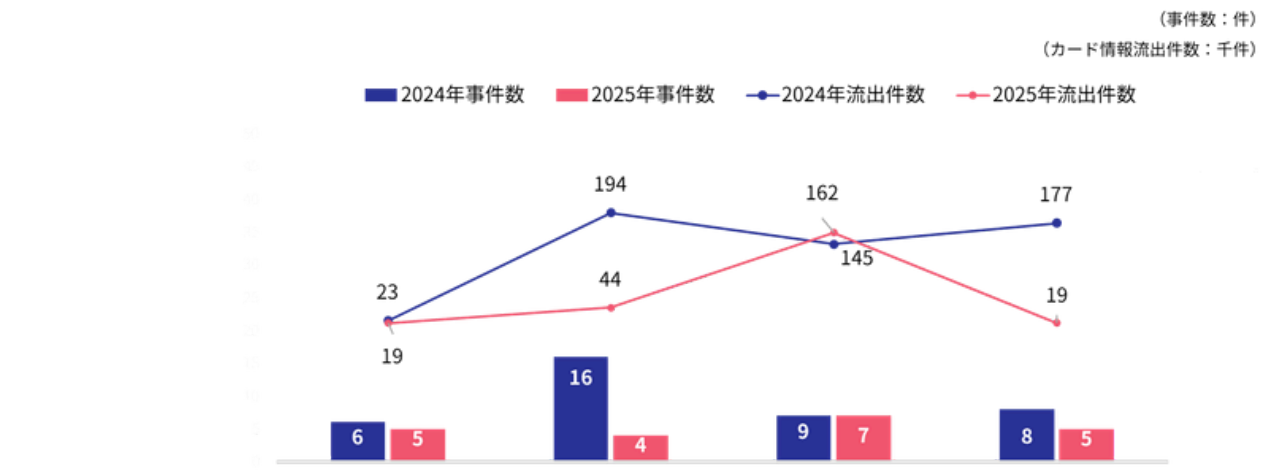
	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
事件数	21	30	26	24	51	50	75	54	37	37	21
カード情報流出件数	123,527	255,689	564,844	283,374	375,479	89,628	256,822	849,950	536,291	540,722	246,474

（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 2026年3月12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	5	4	7	5
	カード情報流出件数	19,635	44,295	162,894	19,650
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 2026年3月12日時点で集計

※2 2025年4-6月、7-9月のカード情報流出件数が公開されたことにより、2025年の数値を以下の通り訂正

- 4-6月 33,872件→44,295件、7-9月　160,822→162,894件

2025年10-12月期に公表されたカード情報流出事件は5件となりました。流出したカード情報の件数は19,650件と前四半期（2025年7-9月期）に比べ大幅に減少しました。前年同期の177,772件に比べても大幅に減少しています。前年同期は8事件のうち流出件数が1万件を超えた事件が5件、うち2件は約5万8千件と7万2千件と大規模な流出が複数発生したのに対し、2025年10-12月期は5事件のうち流出件数が1万件を超えたのは1事件のみとなったことが減少の要因です。5件のうち2件は流出の判明から公表までに1年以上、2件は11ヶ月が経過しており、公表までに時間がかかっています。なお詳細判明前に公表された2025年4-6月期の1事件と7-9月期の2事件のカード情報流出件数が判明しましたので、当該期間のカード情報流出件数を修正しました。

2025年の1年間の累計でみると、カード情報流出事件は21件（2024年の37件から16件の減少）、流出したカード情報の件数は246,474件（2024年の540,722件から294,248件の減少）となりました。 2025年通年で最もカード情報の流出件数の規模が大きかった事件は、7月に公表された食品スーパーのランサムウェア被害による127,263件の流出事案となり、年間のカード情報流出件数の半分以上を占めました。2024年は長期間にわたって大量のカード情報が流出していた事件が複数あり、5万件以上の流出事案も4件ありました。対して2025年は、前述のランサムウェアを除くと5万件以上の流出事案は無く、逆に6件が1,000件未満の流出と比較的小規模な事件が多かったことから、前年に比べて大幅に流出件数が減少しました。

（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		2025年1-3月		2025年4-6月		2025年7-9月		2025年10-12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		5	19,635	4	44,295	7	162,894	5	19,650
業種別	アパレル	0	0	1	30,712	1	60	3	18,592
	食品	3	17,726	1	2,270	3	130,912	1	1,049
	家電・電子機器・PC	0	0	0	0	1	96	1	9
	生活雑貨・家具・インテリア	1	2,460	1	10,423	0	0	0	0
	ホビー	1	1,909	0	0	1	30,431	0	0
	その他	0	0	1	890	1	1,395	0	0
カード会社		0	0	0	0	0	0	0	0

（Cacco・リンク調べ）
※1 2026年3月12日時点で集計
※2 2025年4-6月、7-9月の流出件数が公開されたことにより2025年の「カード情報流出件数」を以下の通り訂正
- 4-6月 カード情報流出件数 加盟店合計 33,872件→44,295件、生活雑貨・家具・インテリア 0件→10,423件
- 7-9月カード情報流出件数加盟店合計 160,822→162,894件、その他 0→1,395件/食品 130,235→130,912件

＜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	2025年1-3月		2025年4-6月		2025年7-9月		2025年10-12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	1	2,270	2	30,491	1	9
3ヶ月-1年	1	13,094	0	0	2	773	0	0
1-3年	0	0	1	10,423	1	127,263	0	0
3年以上	4	6,541	2	31,602	2	4,367	4	19,641

（Cacco・リンク調べ）
※1 2026年3月12日時点で集計
※2 2025年4-6月、7-9月の流出件数が公開されたことにより2025年の「事件数」「カード情報流出件数」を以下の通り訂正
- 4-6月1-3年 事件数：0→1件、カード情報流出件数0→10,423件
- 7-9月3ヵ月-1年　事件数：1→2件、カード情報流出件数96→773件/3年以上　事件数：1→2件、カード情報流出件数2,972→4,367件

2025年10-12月期は、商材別にみると、「家電・電子機器・PC」が1件、「アパレル」が3件、「食品」が1件発生しています。うち、「アパレル」では1事件あたり1万件を超える大規模なカード情報流出が発生しており、全体の数字を大きく押し上げました。一方、「家電・電子機器・PC」や「食品」においてもカード情報流出事件が継続しており、特定の商材に限らず、あらゆるECサイトがターゲットとなっている現状に変わりはありません。

5つの事件のうち4件は、2021年から3年以上にわたってカード情報流出が続いていました。うち2件は神奈川県警サイバー警察本部の指摘により発覚、1件はJPCERT/CCによるカード情報流出懸念の連絡により発覚した事件です。残り1件はカード会社からの指摘により発覚しました。前回（2025年7～9月版）の本レポートでも、2021年3月から3年以上にわたり流出が継続した「Water Pamola（ウォーター・パモラ）」（詳細は1-(3)2025年10-12月　カード情報流出事件トピック『クレジットカード・セキュリティガイドライン』で義務付けられた「脆弱性対策」を参照）が原因と推測される事案を報告しましたが、同様の手口の新たな発覚が続いています。一方で、本四半期（2025年10-12月期）では、流出開始の翌日に自社の決済ページに不正なスクリプトが挿入されていることに自ら気づき、カード決済を停止した事案がありました。このように自社で早期に気づくことができれば、カード情報の流出件数を少なく抑えるだけではなく、不正利用が発生する前にカード会社に流出可能性を報告し、流出したカード番号の利用を停止するなどの措置をとることが期待できます。

（3）カード情報流出事件トピック

『クレジットカード・セキュリティガイドライン』で義務付けられた「脆弱性対策」

2026年3月、『クレジットカード・セキュリティガイドライン【6.1版】』（以下『ガイドライン6.1』）が公表されました。2025年3月に公表された『ガイドライン6.0』から新たな指針対策（割賦販売法への法的対応として義務付けられる対策）の追加はないため、【6.1版】となっています。

『ガイドライン6.0版』では、指針対策としてEC加盟店に義務付けられた脆弱性対策、EMV 3-Dセキュア導入、不正ログイン対策、および「線の考え方」として示された決済時、決済後の対策が示されましたが、『ガイドライン6.1』ではこれらの対策の着実な理解と促進を目的として、具体的な取り組みについての記載が追加されました。

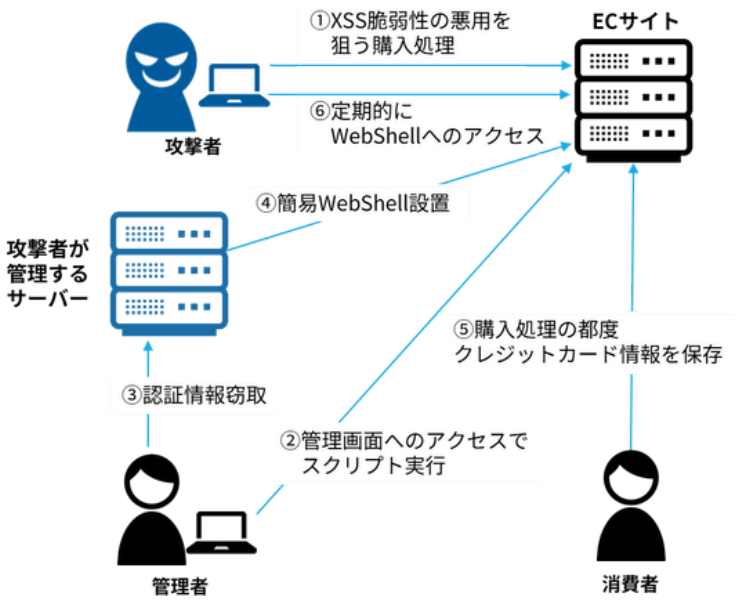
『ガイドライン6.1』の公表とあわせて、これらの指針対策のより具体的な内容を取りまとめた『EC加盟店におけるセキュリティ対策導入ガイド2.1版（付属文書20）』（以下『付属文書20』）が公開されました。この中から「脆弱性対策」について解説します。

■脆弱性対策が必要な理由

ECサイトからのカード情報流出の大半を占める手口である、オンラインスキミングは、オープンソースソフトウェアを主とするECサイト構築パッケージやCMSの設定不備及び脆弱性を狙った攻撃が原因で発生しています。実際にどのような攻撃が行われるのか、2021年ごろに多発した攻撃キャンペーン「Water Pamola」を例に見ていきます。

「Water Pamola」は、ECサイト構築パッケージにおけるクロスサイトスクリプティング（XSS）脆弱性を悪用した攻撃でした。まず攻撃者は、ECサイト内の入力フォームから不正なスクリプトを含む文字列を入力します。管理者がこの入力フォームのデータを確認するために管理画面にアクセスすると、この不正なスクリプトが実行され、管理者の認証情報が攻撃者に窃取されます。攻撃者は窃取した認証情報を利用してECサイト構築パッケージの管理画面にログインし、不正なスクリプトやファイルを設置します。いったん不正なスクリプトが設置されると、消費者が決済ページから入力したカード情報が都度ECサイト内に作成した情報保存ファイルに保存されます。このファイルを攻撃者がサーバーに定期的にアクセスして取得することで、カード情報が流出します。

▼Water Pamolaの概要



設置されたファイル	内容
WebShell	・多機能なWebShell（中国語をベースとしており、ツール名は不明）
データベース操作ツール	・Adminer version 4.2.4
情報窃取JavaScript	・ボタンをクリックした際にクレジットカード情報などを送信する ・ログインページや決済ページでロードされる
情報保存JavaScript	・“情報窃取JavaScript”からの情報送信先 ・受信したデータを“情報保存ファイル”に保存する
情報保存ファイル	・クレジットカード番号、有効年月、セキュリティコード、メールアドレス、パスワードなどが保存されている
簡易WebShell	・アップロードされたPHPファイルを実行する

出所：JPCERT/CC『ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃』（2021年7月）を元に作成

「Water Pamola」による攻撃は、以下の脆弱性に対策ができていれば、カード情報流出を防げた可能性があります。

① ECサイトの脆弱性の悪用
WebアプリケーションのXSS脆弱性が対策できていれば、管理画面の認証情報を窃取される可能性は低かったです。

② 管理画面からの不正なログイン
認証情報を窃取されても、攻撃者がECサイト構築パッケージの管理画面にアクセスできないよう対策していれば、管理者ログインを乗っ取ることはできませんでした。また、もし管理画面にアクセスされても、多要素認証を導入していれば、窃取された認証情報だけでは、不正ログインを許す可能性は低かったといえます。

③ ECサイトへの不正なスクリプトやファイルの設置
管理画面からのなりすましログインを許しても、Webサーバーに不正なスクリプトやファイルのアップロードができないように制限していれば、サーバー内のファイルに消費者が入力したカード情報を保存することはできないので、カード情報が流出するリスクは低減できました。

■過去に行われた攻撃事例をもとにした脆弱性対策
以上はWater Pamolaの例ですが、『付属文書20』では、他にも過去に行われた攻撃事例からリスクを洗い出し、以下の対策を求めています。

①システム管理画面のアクセス制限と管理者のID/パスワード管理

①-1 管理画面にアクセスさせない対策
- システム管理画面にアクセス可能なIP アドレスを制限する。IP アドレスを制限できない場合は管理画面にベーシック認証等のアクセス制限を設ける。
- システム管理画面のURLを推測困難なものへ変更する。

①-2 管理画面にアクセスされてもログインさせない対策
- 取得されたアカウントを不正使用されないよう2 段階認証又は多要素認証（2要素認証）を採用する。
- システム管理画面のログインフォームでは、アカウントロック機能を有効にし、10 回以下のログイン失敗でアカウントをロックする。
- ユーザーID/パスワードをデフォルトから変更する。admin など推測しやすいものでないことを確認し、adminフォルダを削除する。

②データディレクトリの露見に伴う設定不備への対策

②-1 データにアクセスさせない対策

- 公開ディレクトリには、顧客データや決済データ、アクセスログなどの重要なファイルを配置しない。（特定のディレクトリを非公開にする。公開ディレクトリ以外に重要なファイルを配置する。）

②-2 Webサーバーに不正なファイルやスクリプトをアップロードさせない対策

- Web サーバーやWeb アプリケーションによりアップロード可能な拡張子やファイルを制限する等の設定を行う。

③Web アプリケーションの脆弱性対策

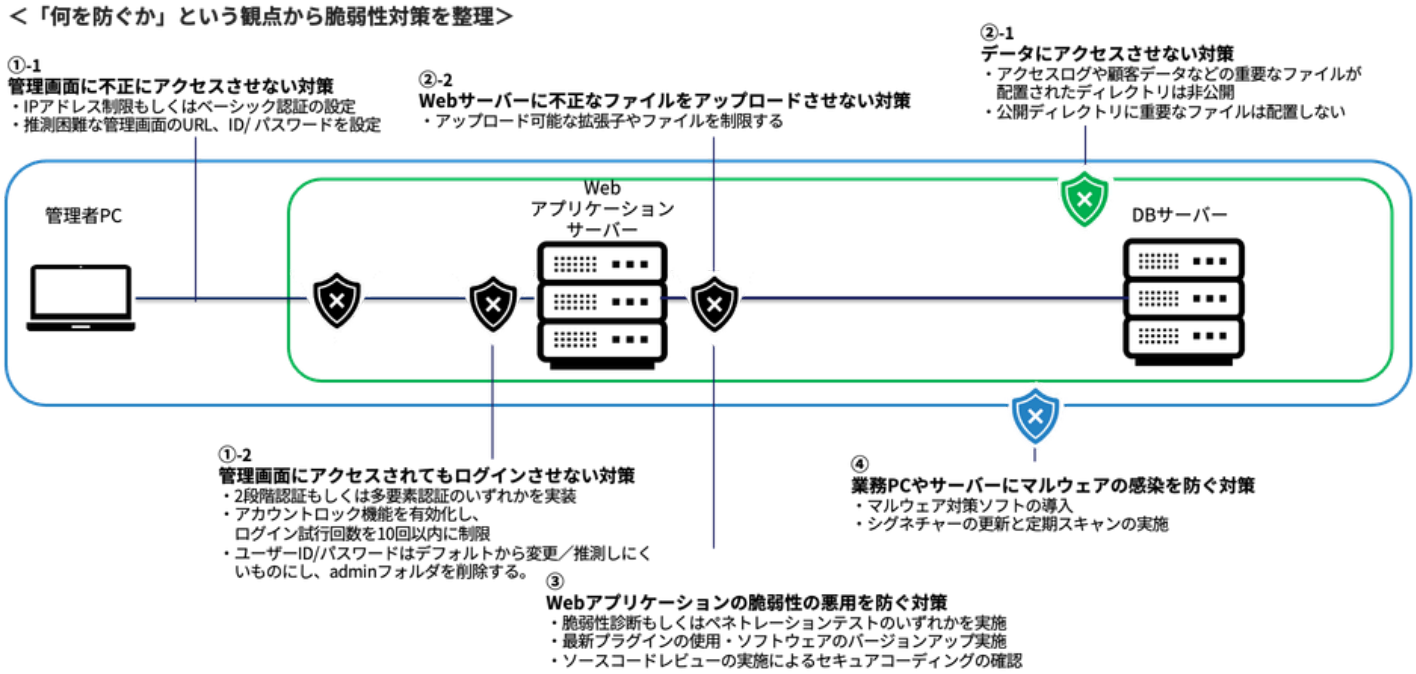
（Webアプリケーションの脆弱性の悪用を防ぐ対策）

- 脆弱性診断又はペネトレーションテストを定期的に実施し、必要な修正対応を行う。
- SQL インジェクションの脆弱性やクロスサイト・スクリプティングの脆弱性対策として、最新のプラグインの使用やソフトウェアのバージョンアップ（必要なセキュリティパッチの適用を含む）を行う。
- Web アプリケーションを開発又はカスタマイズしている場合には、セキュアコーディング済みであるか、ソースコードレビューを行い確認する。コーディングの脆弱性の対処には「安全なWebサイトの作り方」（IPA）を参考に対策を行う。

④マルウェア対策としてのウイルス対策ソフトの導入、運用

（業務PCやサーバーにマルウェアの感染を防ぐ対策）

- サーバーや業務用PCにウイルス対策ソフトを導入して、シグネチャーの更新や定期的なフルスキャンなどを行う。



■クレジットマスター／悪質な有効性確認への対策も脆弱性対策の一部として整理

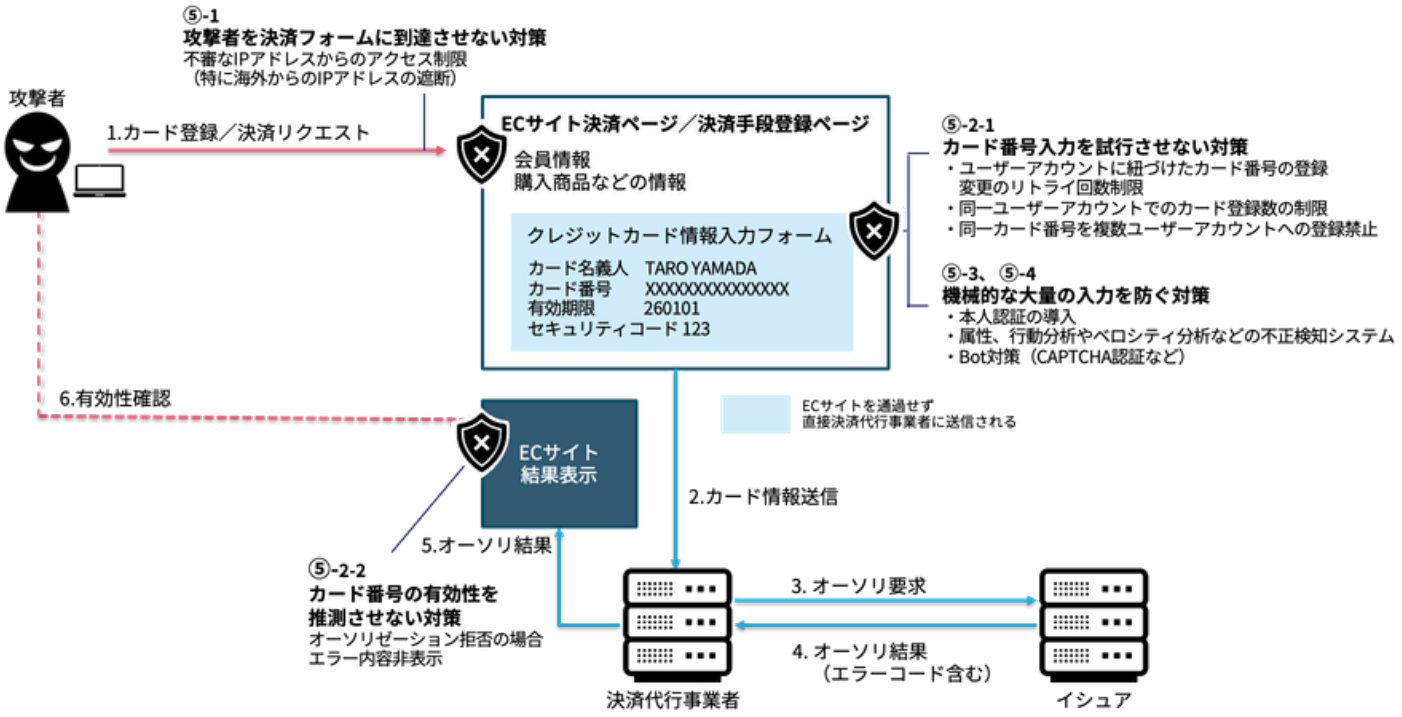
クレジットカード番号の規則性を利用して機械的にカード番号を生成する「クレジットマスター」で生成した大量のカード番号や、フィッシングで窃取したカード番号をECサイトの決済に利用して番号の有効性を確認する手口（悪質な有効性確認）が発生しています。具体的な方法としては、大量のカード番号をECサイトの決済フォームや会員情報の決済手段登録に連続して入力することによって行われます。対策としては、不正なカード番号の入力をECサイト側で防ぐ仕組みが有効です。そのため、ECサイト『付属文書20』では、脆弱性対策の一部として「悪質な有効性確認、クレジットマスターへの対策」を位置付け、以下のいずれかを実施することを求めています。

⑤-1 不審なIPアドレスからのアクセス制限
（攻撃者を決済フォームに到達させない対策）
特に海外からの攻撃が多いので、不要な場合は海外からのアクセスの遮断を求めています。

⑤-2 有効なカード会員データの漏えい対策
⑤-2-1 カード番号入力を試行させない対策
なりすましにより作成されたユーザーアカウントや不正ログインを許したアカウントを利用してカード番号の有効性確認が行われることがあります。同一ユーザーアカウントからの入力制限が有効となります。ユーザーアカウントに紐づけたカード番号の登録・変更のリトライ回数制限、同一ユーザーアカウントでのカード登録数の制限、同一カード番号を複数ユーザーアカウントへの登録禁止を行います。
⑤-2-2 **カード番号の有効性を推測させない対策**
カード番号登録に対してオーソリゼーション(以下、オーソリ)を拒否する場合に、エラー内容を非表示とすることで、攻撃者にカード番号の有効性を推測させることを防止します。

⑤-3 本人認証の導入
（機械的な大量の入力を防ぐ対策）
ユーザーアカウントへカード情報を登録する際に「EMV 3-Dセキュア」、SMS通知などの本人認証が行える対策を導入します。

⑤-4 有効性確認の回数制限
（機械的な大量の入力を防ぐ対策）
前述のカード情報の入力制限の他、属性・行動分析やベロシティ（操作速度）分析などの不正検知システム、CAPTCHA認証などのBot対策を行います。



≫ 2. ECにおける不正利用の概況(2025年10-12月)

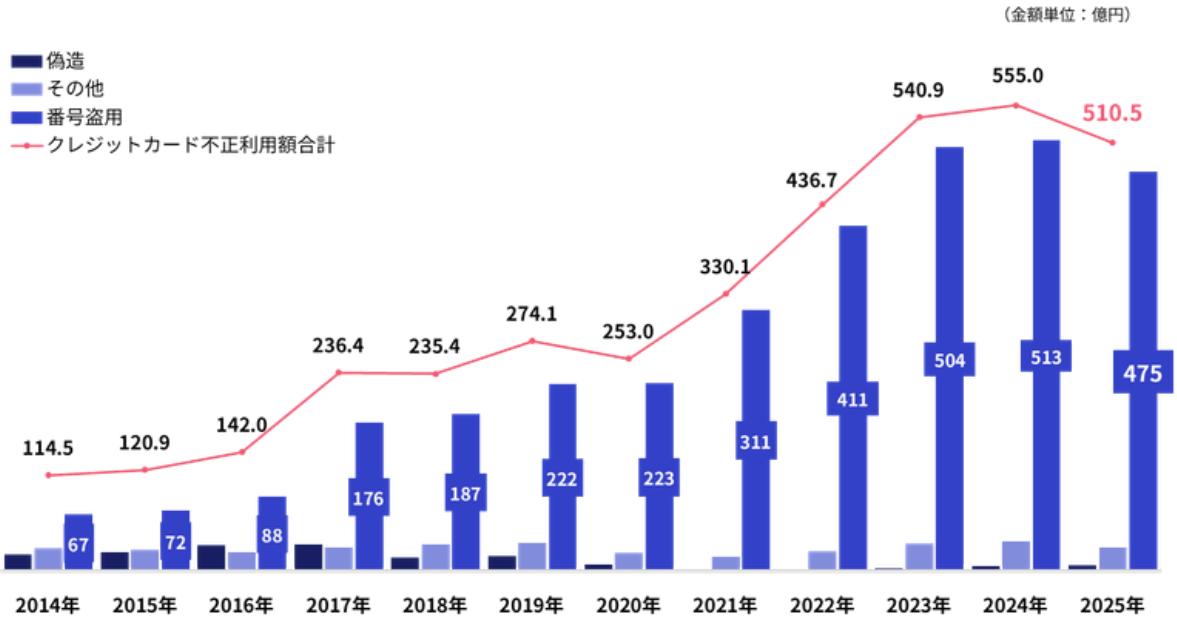
(1) クレジットカード不正利用被害額の推移

2025 年10-12月のクレジットカード不正利用

- 不正利用被害額合計　93.9億円
- 偽造　1.0億円
- 番号盗用　86.6億円
- その他　6.3億円

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

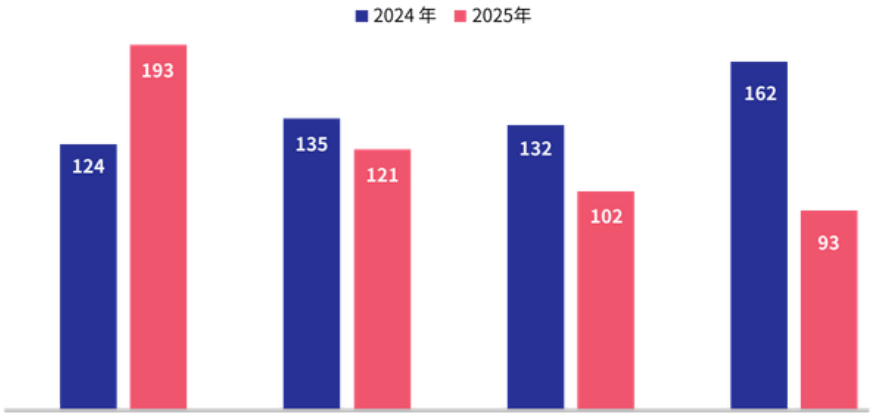
2025年までのクレジットカード不正利用被害額の推移



(『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) 2026年3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）

(金額単位：億円)



		1～3月	4～6月	7～9月	10～12月
2025年	偽造	1.8	1.1	3.3	1.0
	番号盗用	182.9	113.3	92.6	86.6
	その他	8.5	7.0	6.1	6.3
	合計	193.2	121.4	102.0	93.9
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) 2026年3月

2025年第4四半期（10～12月期）のクレジットカード不正利用被害額は93.9億円となり、前年同四半期と比較すると約47%減となりました。また2025年の1年間の累計被害額は約510億円となりました。注目すべきは、前年（2024年)対比でみても約7.4%の減少に転じた点です。被害額が増加の一途をたどっていた2014年以降、11年目で初めての減少を記録しました。

この減少の背景には、国内での「EMV 3-Dセキュア」導入義務化による効果があると考えられます。先行して本人認証の強化が進んだ欧州市場では、SCA（強力な顧客認証※1）への移行期間であった2020年から2021年において、カード決済の不正利用発生率（金額ベース）が4～6割減少したことが欧州銀行監督局（EBA）のレポート（※2）で報告されています。日本国内においても同様のメカニズムで不正利用防止に効果が表れていると推測できます。不正利用被害額が減少に転じたことは大きな進歩ですが、金額自体は依然として3年連続で500億円を上回る極めて高い水準にあります。

「EMV 3-Dセキュア」は強力な武器ですが、それのみで不正利用被害を根絶することは困難です。「EMV3-Dセキュア」による本人認証に加え、不正検知システムによる「属性・行動分析」や「配送先情報の精査」などを組み合わせた「重層的な防御（多層防御）」を構築し、さらなる被害抑制を目指す必要があります。

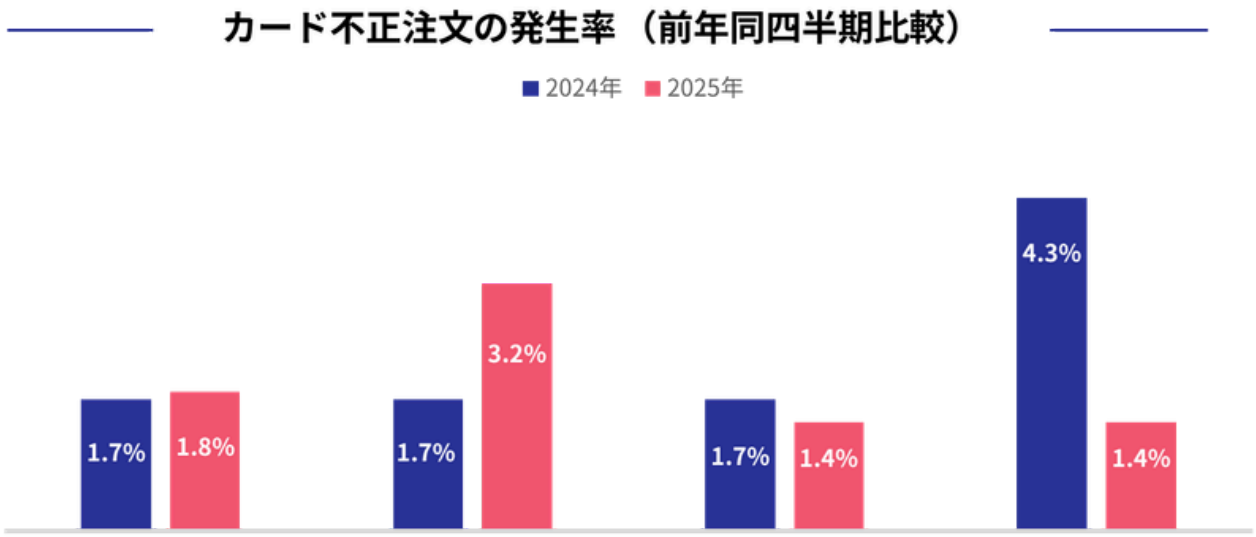
※1 SCA（Strong Customer Authentication）：「強力な顧客認証」を指す欧州の規制要件。知識（パスワード等）、所持（スマホ等）、生体（指紋等）のうち2つ以上を組み合わせた認証（多要素認証）を求める。「EMV 3-Dセキュア」は決済においてSCAの求める多要素認証の要件を満たすための技術として位置付けられる。

※2 欧州銀行監督局（EBA）のレポート：Opinion on new types of payment fraud and possible mitigants (2024年4月29日発表)

（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12万サイト以上）における審査結果をもとに集計



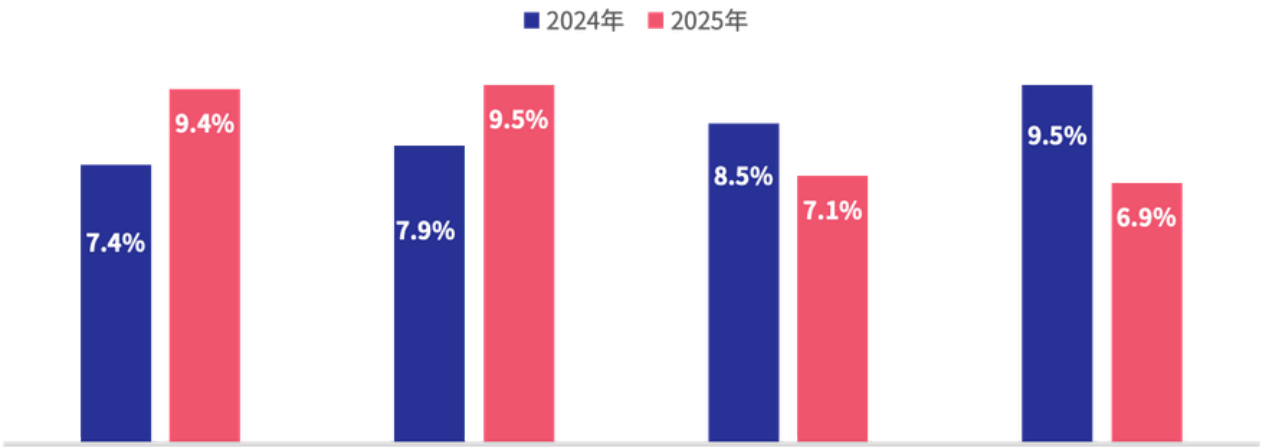
	1～3月	4～6月	7～9月	10～12月
2025年	1.8%	3.2%	1.4%	1.4%
2024年	1.7%	1.7%	1.7%	4.3%

※1「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）

※2 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 2026年3月12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%	9.5%	**7.1%**	**6.9%**
2024年	7.4%	7.9%	8.5%	9.5%

※1「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。（Cacco調べ）
※2 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 2026年3月12日時点で集計

カード不正注文の発生率を前年同四半期と比較すると、2025年10-12月期は1.4%と2.9ポイントの減少となりました。例年、ブラックフライデーやクリスマス、年末年始のセールが重なる第4四半期（10～12月期）は、取引件数の増加に伴い不正注文の発生率も急増する傾向にあります。実際、前年（2024年）の同時期は4.3%と極めて高い水準にありましたが、今期は前四半期（7-9月）から横ばいの1.4%に留まっています。この抑制傾向は、クレジットカード各社によるモニタリングの強化や、加盟店側での「EMV 3-Dセキュア」の導入が進んだことにより、不正利用者による注文が「通りにくい」環境が構築されつつある結果と考えられます。

転売目的の不正注文発生率についても、クレジットカードの不正利用と同様に落ち着きを見せています。2025年10-12月期は6.9%となり、前年同四半期の9.5%から大幅に低下しました。前四半期（2025年7-9月期）の7.1%と比較しても微減しており、年間を通じて高止まりしていた転売被害が、一定の抑制フェーズに入ったと推測されます。

不正注文検知数の商材別ランキングを見ると、2025年10～12月期は、前四半期（2025年7-9月期）に続きランキング1位となった「イベント」は、配送を伴わないデジタルチケットやQRコード形式が主流であり、不正注文直後の転売・換金が容易な即時性を理由に、攻撃者にとって極めて効率の良いターゲットであり続けています。

2025年10-12月期で顕著な動きを見せたのは、2位に浮上した「ホビー・ゲーム」（前回4位）です。これは新作ゲーム機や限定フィギュアなど、年末商戦特有の高単価・希少商材が標的となったものと推測されます。また5位へと順位を上げた「アパレル」についても注視が必要です。同四半期に発生した大規模なカード情報流出事件の背景と歩調を合わせるように、検知数ベースでも不正注文の標的となる割合が高まっています。アパレル事業者は自社サイトの脆弱性対策と併せて、決済における不正対策の強化が急務となっています。

このように、現在はフリマアプリ等の普及により、あらゆる商材が容易に換金可能な対象となっています。「自社商材は狙われにくい」という固定観念を捨て、全カテゴリーの事業者が一貫した警戒態勢を敷くべき局面にあります。

＜不正注文に狙われやすい商材ランキング＞

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

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

※1「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）
※2 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 2026年3月12日時点で集計

（3）不正利用のトピック

フリマアプリを悪用した「空き箱出品」によるスマホ不正取得事件

2024年から2025年にかけて、フリマアプリ等のプラットフォームを悪用し、他人名義のクレジットカード情報を用いて不正に利益を得ていた容疑者が摘発されました。

■ 事件の概要

本事件の容疑者である指示役は、SNS等で募った「闇バイト」を実行役に据え、不正に入手した他人のクレジットカード情報を共有しました。ECサイトでスマートフォンを他人のカード情報を利用して不正に購入させた後、その商品をフリマアプリ上で「スマホの空き箱」と偽って出品・取引させることで、実物のスマートフォンを回収し、転売していました。指示役の容疑者は、この手法で合計約700万円相当の物品を不正に取得していたとされています。

■ 不正の手口

①闇バイトの勧誘
指示役がSNS等で実行役の闇バイトを募集

②ECサイトでの不正購入
指示役が提供した他人のクレジットカード情報を用い、実行役がECサイトでスマートフォンを購入・受取する。

③カムフラージュ出品
実行役がフリマアプリへ「スマホの空き箱」として当該商品を出品する。

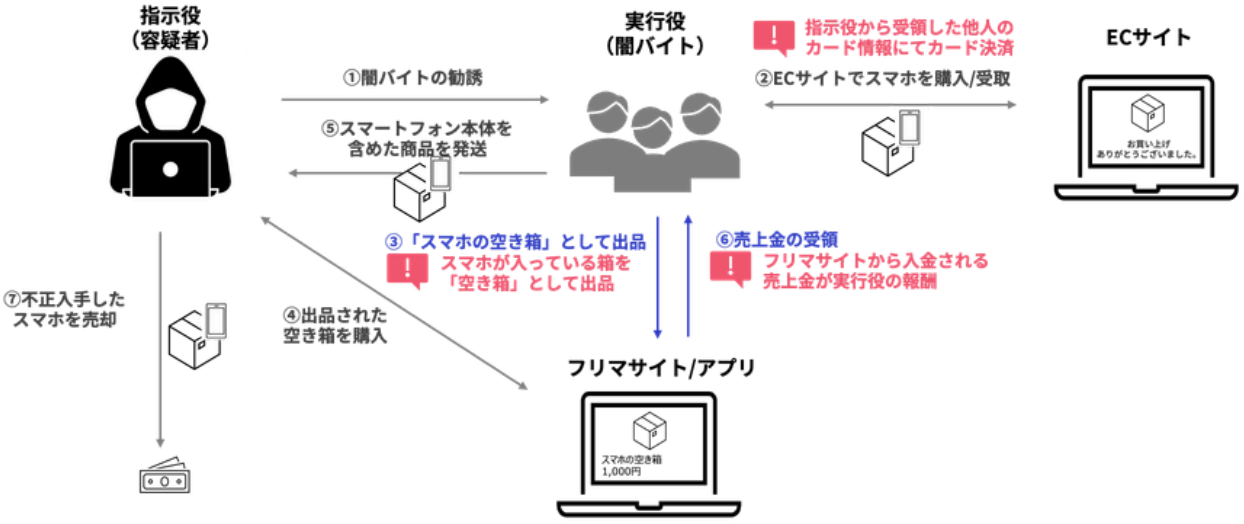
④フリマアプリでの購入
指示役は実行役が出品した「空き箱」を購入する。

⑤現物の発送と取引完了
実行役は「空き箱」名目で、実際にはスマートフォン本体を含めた商品を指示役へ発送し、受取評価を経て取引を完了させる。指示役は、配送履歴の残る正規ルートにより、足がつくことなく実際のスマートフォンを不正に入手できる。

⑥報酬の受取
実行役は、フリマアプリ上の売上金を一連の犯行の報酬として受け取る。

⑦不正入手したスマートフォンの換金
指示役は不正入手したスマートフォンを売却して換金する。

フリマアプリを悪用した「空き箱出品」によるスマホ不正取得事件



本事件の巧妙な点は、「スマホの空き箱」という名目で、実物の高額商品を配送させている点にあります。フリマアプリにおいては空き箱自体の出品は、トラブル防止で制限される場合を除き、規約違反ではないケースが多いため、システムによる不正検知を回避しやすいという盲点を突いています。また、闇バイトを介在させることで、カード情報の不正利用者（実行役）と最終的な受取者（指示役）の間に「正規のフリマ取引」を挟み、捜査の手を逃れようとする意図が見て取れます。

本事件は、単なるクレジットカード決済時の本人認証強化だけでは防ぎきれない「属性や行動の歪み」を捉える重要性を示しています。

- 「新規アカウントによる高額出品・即落札」
- 「出品から購入までの時間が極端に短い」
- 「特定の属性を持つアカウント間での高頻度な取引」

これらをリアルタイムでモニタリングする取引分析の実装が、巧妙化する不正スキームへの対抗策として有効になると考えます。

>>> 3. 政策の動向

『クレジットカード・セキュリティガイドライン6.1版』における不正利用対策の例示

2026年3月に公表された『ガイドライン6.1』の付属文書20別紙dとして『不正利用の抑止を実現する加盟店の事例集 1.0版』（以下『事例集』）が公表されました。

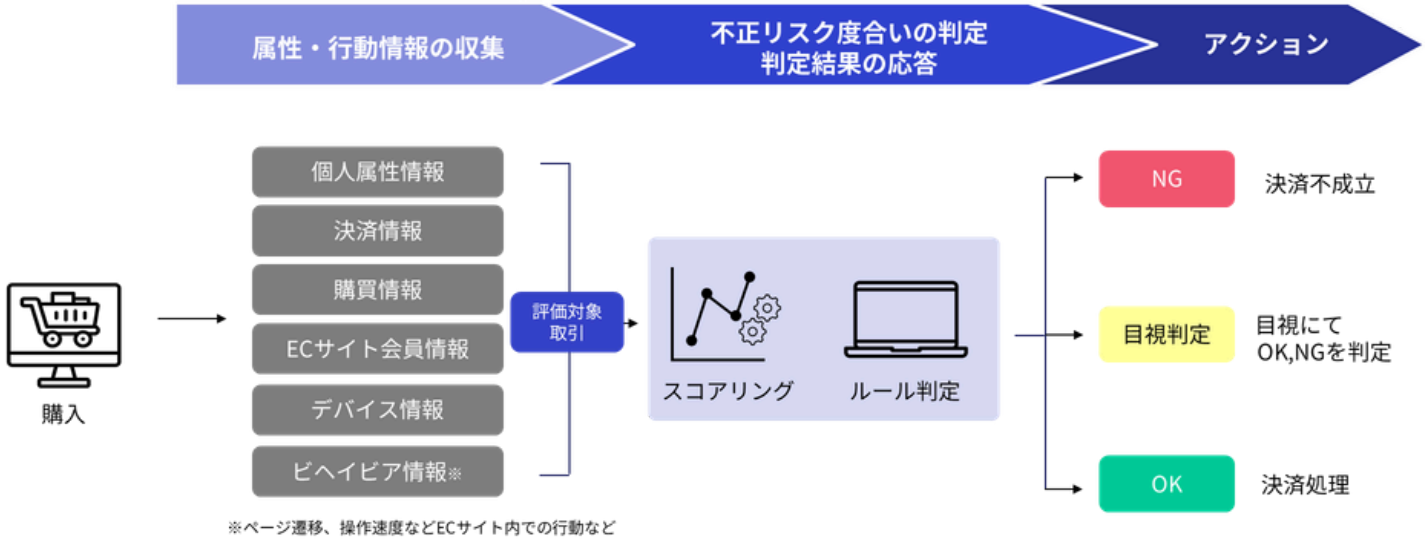
『事例集』は、日本クレジット協会インフラ整備部会の不正利用対策検討ワーキンググループ（以下WG）において実施している調査の結果に基づくものです。調査の結果、不正利用発生率の抑制に対し、組織体制の整備を伴う属性・行動分析の導入が効果的であることが明らかになりました。この結果を受け、同WGでは不正利用の抑制を実現した加盟店に対し、具体的な取り組みについてのヒアリングを実施し、内容を取りまとめました。

■属性・行動分析について

属性・行動分析は、過去の取引情報から不正に関する属性や行動の特徴を見出し、新たな取引と比較することでその取引のリスク評価を行う手法です。不正利用対策の「線の考え方」における「決済前」「決済時」「決済後」の全てのフェーズで効果的な対策です。

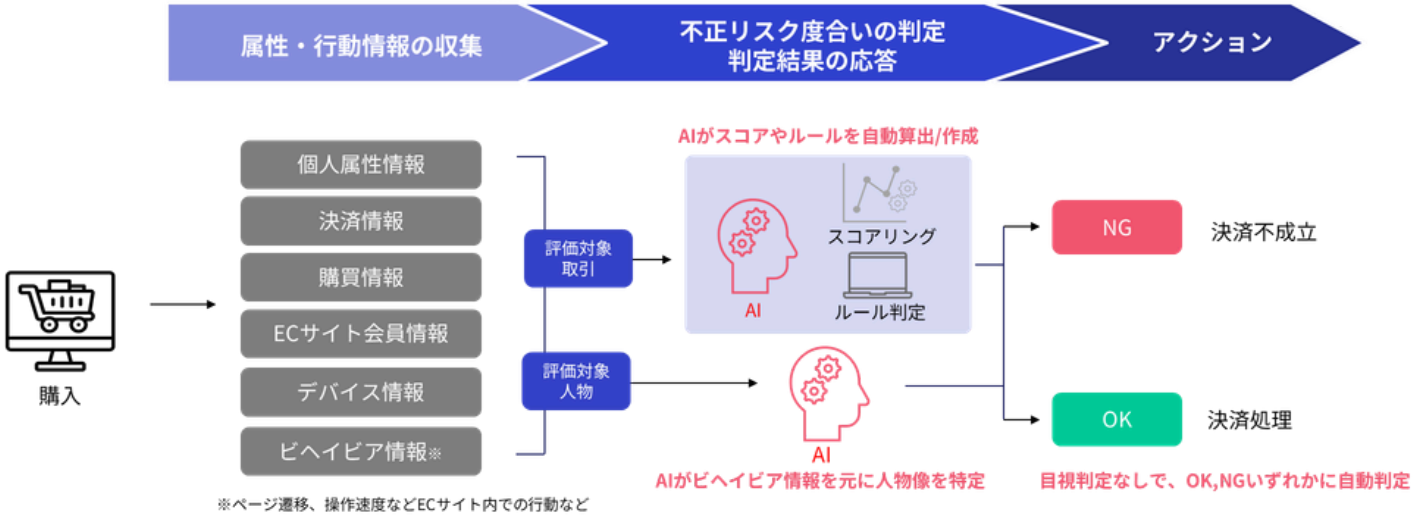
クレジットカードで決済を行おうとする消費者の属性（個人属性、決済情報、購買情報、ECサイト会員情報、デバイス情報など）や、ECサイト内でのふるまい情報（ページ遷移、操作速度などECサイト内での行動）を元にしたスコアリングを行い、その結果を元にルールを用いて不正のリスクを判定します。不正検知スコアリングによって怪しい取引を抽出し、最終的な判断は人間が目視で行うモデル、AIが自動でスコアリングやルールの設定を行い不正な取引を自動判定するモデル、両者のハイブリッドタイプのモデルがあります。

最終判断は人間が目視で行う支援型不正検知モデル



出所：クレジット取引セキュリティ対策協議会『不正利用の抑止を実現する加盟店の事例集1.0版（クレジットカード・セキュリティガイドライン【6.1版】付属文書20別紙d）』（2026年3月）を元に作成

AIが自動でスコアリングやルールの設定を行い不正な取引を自動判定する不正検知モデル



出所：クレジット取引セキュリティ対策協議会『不正利用の抑止を実現する加盟店の事例集1.0版（クレジットカード・セキュリティガイドライン【6.1版】付属文書20別紙d）』（2026年3月）を元に作成

■好事例の共通点

『事例集』では5つの事例が紹介されています。これらの共通点としては以下の3点が挙げられます。

① 不正利用の抑止や承認率向上などのモチベーションを持つきっかけがある。

5つの事例に共通するのが、多額の不正利用被害の発生やそれによるカード決済停止の可能性、不正利用の増加による決済承認率低下など、属性・行動分析導入のモチベーションがあることでした。導入がゴールではなく、導入によって何をどれだけ改善するか、対策の方針やKPIの設定が重要であることを示しています。

② 「属性・行動分析の導入時に留意すべき要素」を実践している。

『EC加盟店におけるセキュリティ対策導入ガイド2.1版（付属文書20）』では、「属性・行動分析導入時に留意すべき要素」として、以下を挙げています。

1）属性・行動分析サービスへの適切な情報提供
不正利用されたカード会員、取引の情報、不審な取引トランザクション、新たな脅威や攻撃パターンに関する情報を属性・行動分析サービスに提供します。情報提供をスムーズに行うために、情報はECサイトと属性・行動分析サービスのシステム間で直接連携します。また自社での不正発生状況を適切に把握するために、「EMV 3-Dセキュア」で認証された取引も含め、アクワイアラ（加盟店契約カード会社）やPSP（決済代行事業者）に対して、イシュア（カード発行会社）から提供される不正利用された取引情報の共有を求めます。これらの情報も属性・行動サービスに情報提供するようにします。

2）ネガティブ情報（過去に不正取引に使用された情報）の蓄積と活用
ネガティブ情報には、不正取引で使用された個人の属性情報、決済情報、購買情報、デバイス情報、位置情報、IPアドレス、振る舞い情報などがあります。これらの情報を蓄積して分析することで、異常なパターンや行動を検知する効果的なルール設定やAIによる学習が可能となり、属性・行動分析の精度向上につながります。

3）継続的な運用の見直し
属性・行動分析の不正利用傾向に応じたルールの見直しや属性・行動分析サービス提供者からのサポートをもとにしたスコアリングの見直しなど、精度向上のための取り組みを継続して行います。

4）トレーニングと教育・体制の整備
属性・行動分析の使用方法、アラートと対応手順、モニタリングの方法、データの収集と報告、プライバシーとコンプライアンスの遵守などについて、必要に応じトレーニングと教育プログラムを整備します。

紹介されている好事例はいずれも、これらの留意点について適切に対応していました。

③ 一定数の人的リソースを確保する（困難な場合は別の方法で補う）

属性・行動分析のルール見直しなど、不正利用対策に専任担当者など十分な人的リソースを充てることが理想とされます。しかし、紹介されている好事例においても、十分な人的リソースを確保できているのは5事例中1事例のみでした。残りの事例では商材ごとにスコアやルールの強度の調整、サービス提供者のサポート活用、AIの活用などで人的リソース不足を補い、不正利用被害の抑制を実現しています。不正利用対策に十分な多くの人員を充てることが難しく、社内にスキルやノウハウが蓄積されていないという事情は多くのECサイトで共通していると考えられ、これらの対応は参考になります。

■重層的な取り組みが効果的

「EMV 3-Dセキュア」と属性・行動分析サービスの併用について紹介されています。一段階目に属性・行動分析を実施し、疑わしいと判定された取引について二段階目で「EMV 3-Dセキュア」による認証を行う事例が紹介されています。第一段階で問題ないと判定された取引には「EMV 3-Dセキュア」のワンタイムパスワードの認証を実施させず、ユーザー体験を向上させることが期待されます。また「EMV 3-Dセキュア」の導入効果が限定的であった、導入後に決済承認率が下がったため不正利用発生率を下げる必要があった、などの理由の場合に「EMV 3-Dセキュア」と属性・行動分析サービスの併用により、効果を上げています。不正利用対策は複数の対策を重層的に導入することが効果的であることが、よくわかる事例となっています。

【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

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）