Cashless Security Report

Quarterly Report

（2025年 7-9月版）2026年1月発行

PCI DSS Ready Cloud

2026.1.29

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7-9月版：2026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（2025 年7-9月）

（1）カード情報流出事件数・情報流出件数の推移

2025年7-9月のカード情報流出事件

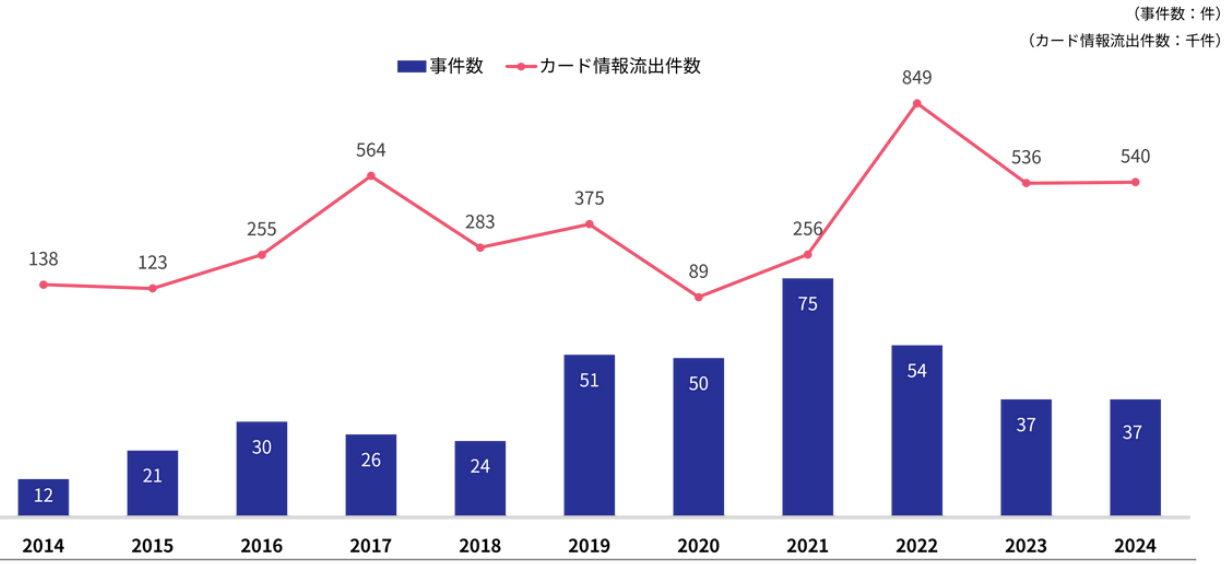
- 事件数　7件
- カード情報流出件数　160,822件

※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



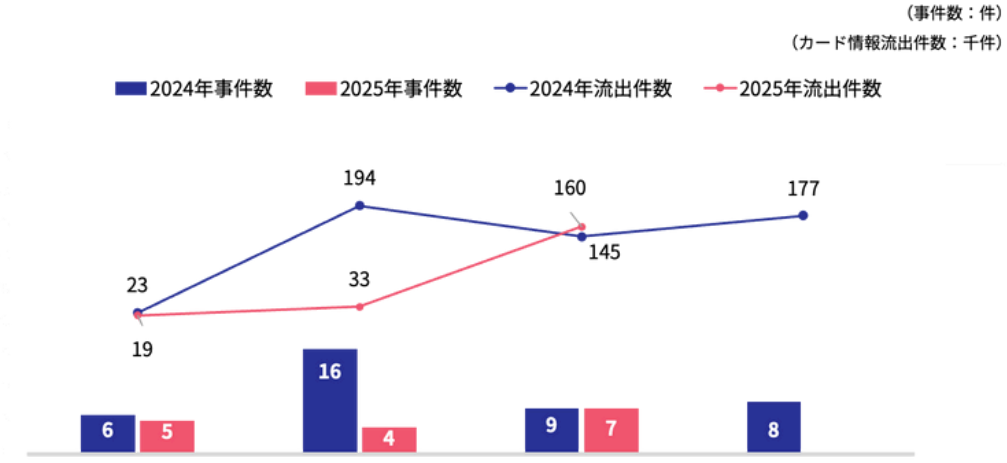
	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
事件数	12	21	30	26	24	51	50	75	54	37	37
カード情報流出件数	138,717	123,527	255,689	564,844	283,374	375,479	89,628	256,822	849,950	536,291	540,722

（Cacco・リンク調べ）

※1 2021年以前のデータはｆｊコンサルティング調べ

※2 2025年12月16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	
	カード情報流出件数	19,635	33,872	160,822	
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 2025年12月16日時点で集計

※2 集計時点で2025年4-6月の事件のうち1件/2025年7-9月の事件のうち2件は詳細が不明のため、カード情報流出件数の集計からは除外

2025年7～9月に公表されたカード情報流出事件は7件となりました。うち2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後、2025年12月時点で詳細が不明な事件です。流出したカード情報の件数は160,822件と4-6月に比べ大幅に増加しました。うち127,263件は、4月に公表された食品スーパーのランサムウェア被害の調査の結果、暗号化・流出した情報に自社のクレジットカード一体型ポイントカードの情報が含まれていたことを7月に公表したものです。この事件は、4月の時点では「個人情報の流出は確認されていません」としてカード情報流出の可能性について言及しておらず、利用者への注意喚起もなかったため、7月のカード情報流出事件として扱いました。

カード情報流出の事件数については7件と前年同期に比べて横ばいとなりました。うち3件は、カード情報流出の発覚から事件発生の公表まで1ヶ月以内となっています。また、7件中5件の事件が、詳細が判明する前に第一報を公表しています。うち2件は自社の点検でカード情報流出の懸念を発見したもので、「早期発見、早期公表」の姿勢が広がり始めている様子が伺えます。

（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		2024年10-12月		2025年1-3月		2025年4-6月		2025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		8	177,772	5	19,635	4	33,872	7	160,822
業種別	アパレル	1	71,943	0	0	1	30,712	1	60
	コスメ	0	0	0	0	0	0	0	0
	食品	3	67,489	3	17,726	1	2,270	3	130,235
	家電・電子機器・PC	1	4,257	0	0	0	0	1	96
	生活雑貨・家具・インテリア	0	0	1	2,460	1	0	0	0
	健康食品	1	4,494	0	0	0	0	0	0
	ホビー	1	0	1	1,909	0	0	1	30,431
	自動車、バイク	0	0	0	0	0	0	0	0
	家具	0	0	0	0	0	0	0	0
	その他	1	16,396	0	0	1	890	1	890
カード会社		0	0	0	0	0	0	0	0

（Cacco・リンク調べ）
※1 2025年12月16日時点で集計
※2 集計時点で2025年4-6月の事件のうち1件/ 2025年7-9月の事件のうち2件は詳細が不明のため、カード情報流出件数の集計からは除外

＜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10-12月		2025年1-3月		2025年4-6月		2025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	1	4,257	0	0	1	2,270	2	30,491
3ヶ月-1年	1	6,929	1	13,094	0	0	1	96
1-3年	0	0	0	0	0	0	1	127,263
3年以上	6	166,586	4	6,541	2	31,602	1	2,972

（Cacco・リンク調べ）
※1 2025年12月16日時点で集計
※2 集計時点で2025年4-6月の事件のうち1件/ 2025年7-9月の事件のうち2件は詳細が不明のため、情報流出期間別の集計からは除外

業種／商材別にみると、「食品」が3件、「ホビー」、「家電・電子機器・PC」、「アパレル」、「その他」が１件ずつとなっています。(「食品」のうち1件と「その他」についてはカード情報の流出件数などの詳細が不明)

警察からの情報流出の指摘により発覚した事件は２件ありました。うち1件はカード情報の流出開始が2021年3月で、流出期間が3年以上に及び、以前から発生している「Water Pamola ※」攻撃と同様の手口が発覚したものと推測されます。もう１件は、カード情報の流出期間が2025年2月から8月と比較的最近の事件でした。

※Water Pamola：ECサイトのクロスサイトスクリプティング（XSS）脆弱性を悪用して、ECサイトを利用するユーザーが入力した個人情報やカード情報を窃取する攻撃

（3）カード情報流出事件トピック

国内初、ランサムウェアにより、大量のカード情報が外部から閲覧された可能性

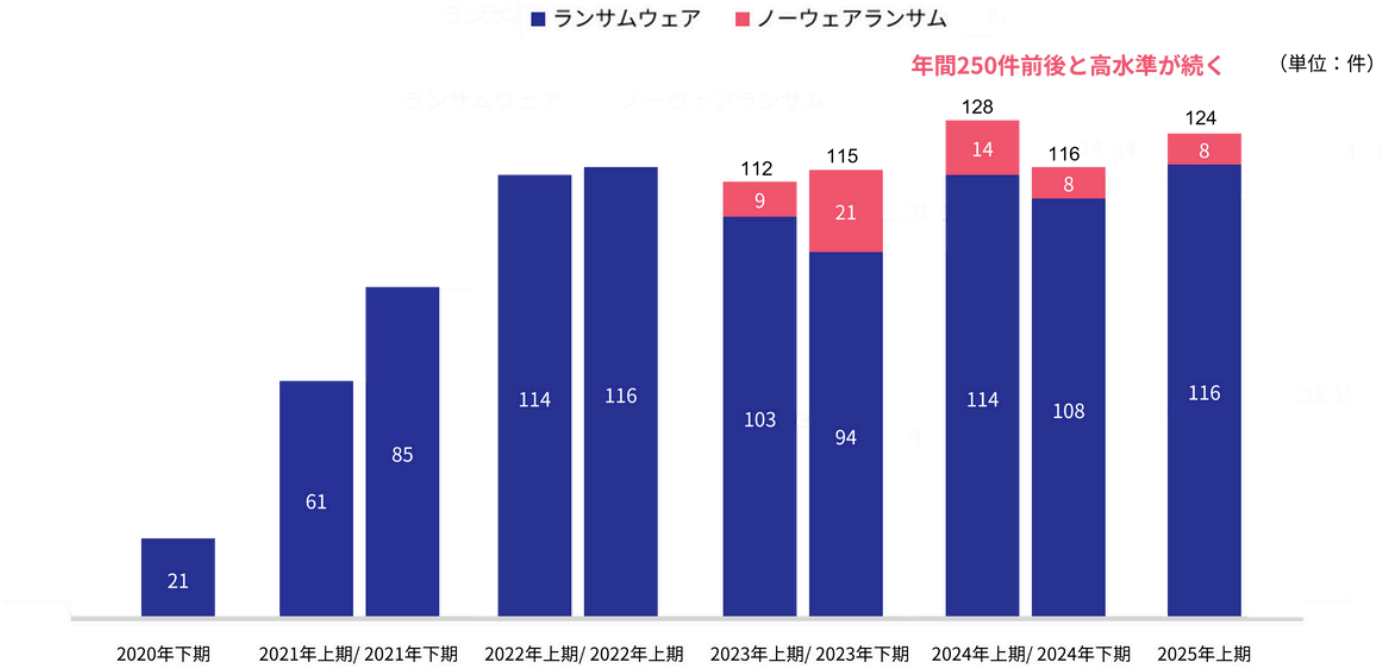
2025年4月、食品スーパーA社が「当社におけるサイバー攻撃被害について」として、ランサムウェア攻撃を受け、グループの複数サーバーが暗号化される被害が発生したことを公表しました。報道によれば、3月30日にシステムの異常を検知した後、基幹システムが停止し、3月31日には展開する23店舗全店が臨時休業しました。4月1日には営業を再開したものの、その後2ヶ月以上クレジットカード決済やポイントの付与が利用できない状況が続きました。A社はクレジットカード一体型ポイントカードを発行しており、カードの入会・再発行手続きも停止する事態となりました。

A社は、4月の時点では個人情報については流出が確認されていないとしていましたが、7月の第2報で、顧客の個人情報延べ約43 万件、取引先情報約4,600件、取引先からの派遣社員の個人情報約3,900件が閲覧された可能性があることを公表しました。カード情報の流出は127,263件で、氏名、住所などの個人情報、2022年4月から2025年3月の購入履歴などと併せて、A社のクレジットカード一体型ポイントカードのカード番号、名義人、有効期限が閲覧された可能性があります。クレジットカード一体型ポイントカードの会員・請求管理システム内のデータが閲覧された上で、暗号化されたことが推測されます。

過去に国内でランサムウェア感染によりクレジットカード情報が暗号化された事例としては、2021年6月に発生したスポーツクラブB社の例があります。B社の会員情報管理システムに登録されていた顧客のクレジットカード情報34,920件が暗号化されましたが、これらの情報は2014年2月以前に登録された情報であり、暗号化された時点では全て有効期限が切れていました。また、情報は暗号化されたものの、外部への流出は確認されていません。今回のA社の事件は、ランサムウェア攻撃による現在有効なカード情報の外部からの閲覧の可能性が報告された国内初の事例となりました。なお食品スーパーなどの業態では、クレジットカード一体型ポイントカードが発行されていることが多くなっています。自社システムにカード情報を保存する場合は、割賦販売法と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』において、PCI DSSの準拠が要請されています。同じ形態でカード情報の取り扱いがある場合は、今一度点検するなど注意が必要です。

警察庁サイバー警察局の統計によると、ランサムウェア攻撃被害は2022年ごろから年間250件前後と高い水準が続いており、2025年上半期にも124件の被害が報告されています。

＜国内におけるランサムウェア被害報告件数の推移＞



※1（『令和７年上半期における サイバー空間をめぐる脅威の情勢等について』警察庁サイバー警察局）2025年9月
※2 ノーウェアランサム：暗号化することなくデータを窃取したうえで対価を要求する手口。2023年上期から集計。2023年以降は合計値を記載

ランサムウェアの侵入経路として多いのが、VPN装置やリモートデスクトップ接続など、インターネットに公開されたシステムの脆弱性を突いた侵入です。単一要素による認証、パスワードの使い回し、セキュリティ更新が行われていないシステムは攻撃者に狙われやすくなります。多要素認証の導入とOS、ファームウェア、ソフトウェアの脆弱性対応を頻度高く行うなどの運用が求められます。

フィッシングメールに添付された不正なファイルや本文中のリンクを利用してマルウェアに感染させる手口も多用されます。業務連絡や請求書を装ったメールは見分けが難しく、利用者が不用意に開封するとマルウェアが実行されてしまいます。この対策としては、DMARCの導入、メールフィルタリングの強化に加え、利用者に対する定期的なセキュリティ教育を行い、不審なメールを開かない訓練を実施するなどの対策が効果的です。

正規のソフトウェアを装った偽のプログラムをダウンロードさせる手口も確認されています。この手口に対しては、ソフトウェアの入手元を公式サイトに限定し、エンドポイントセキュリティ製品で不正な挙動を検知・遮断することが有効です。さらに、万一ランサムウェアに感染し、重要なデータが暗号化された場合に備えて、定期的にオフラインメディアのバックアップやバックアップシステムのアクセス権の分離が重要です。早期に重要なデータを復元し、業務を復旧させることが期待できます。ランサムウェア被害はカード情報の流出にとどまらず、ビジネス全体の停止に直結します。感染しないための対策と、万一感染しても被害を最小限にとどめるための両方の対策が重要です。

≫ 2. ECにおける不正利用の概況（2025年7-9月）

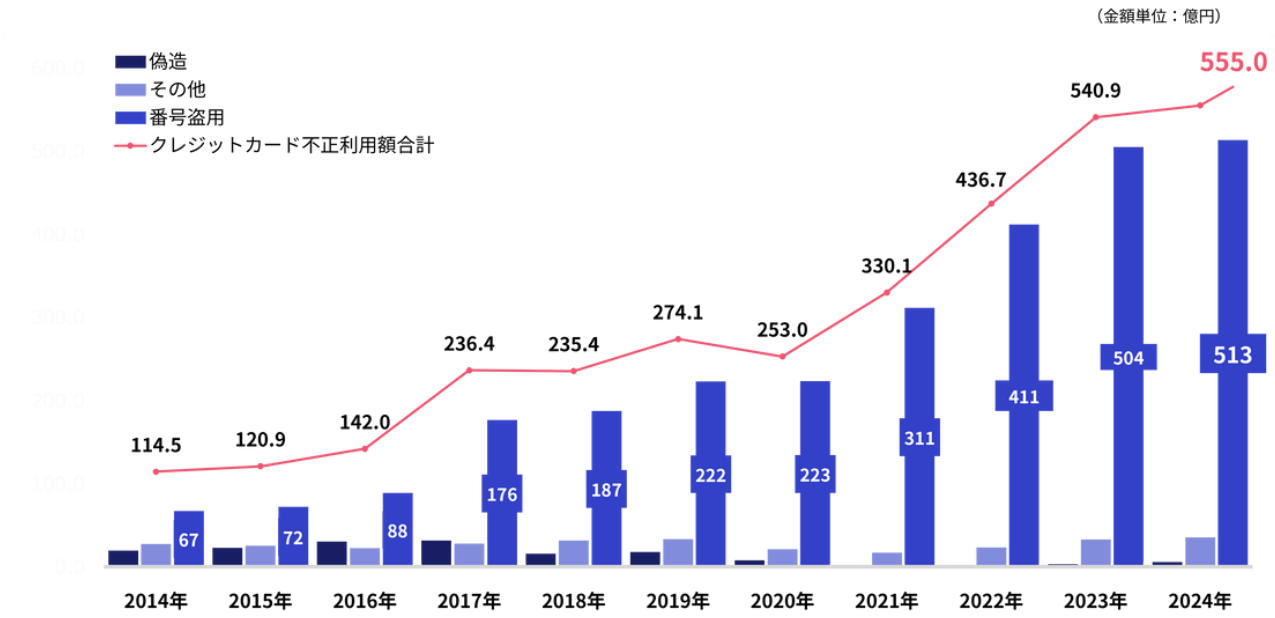
（1） クレジットカード不正利用被害額の推移

2025 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　102.0億円
- 偽造　3.3億円
- 番号盗用　92.6億円
- その他　6.1億円

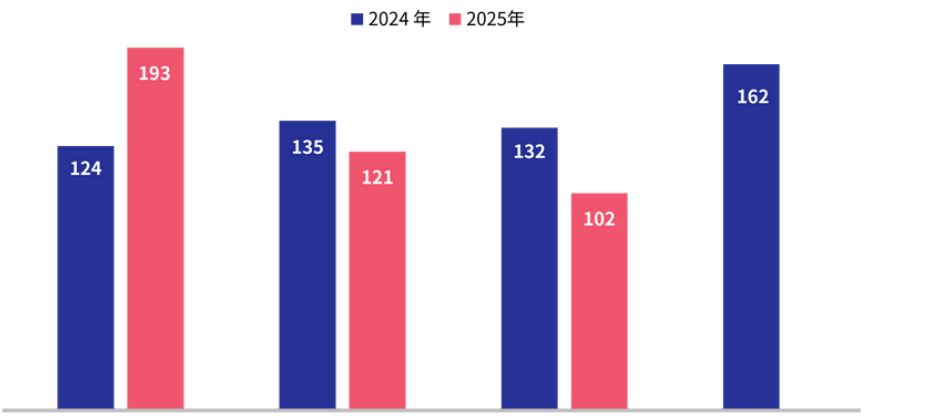
※日本クレジット協会調べ
https://www.j-credit.or.jp/information/statistics/index.html

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12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）



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

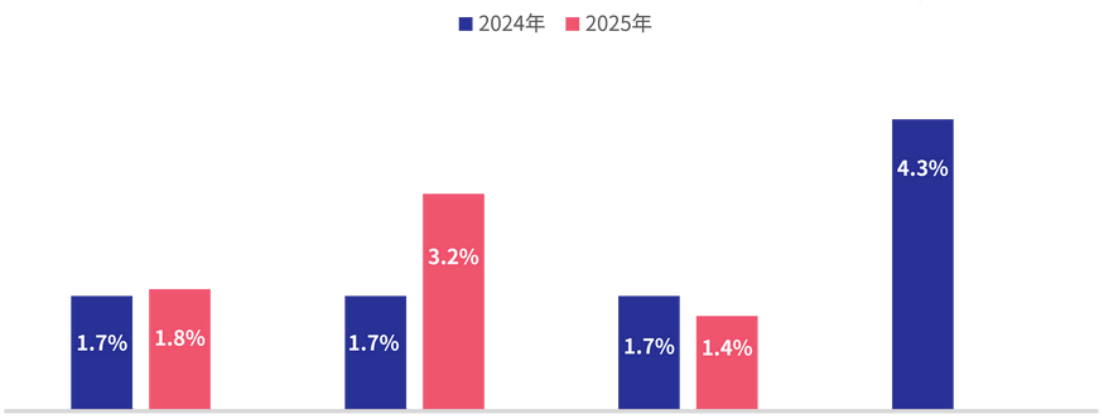
2025年7～9月期におけるクレジットカード不正利用被害額は102億円となり、2025年4-6月に比べて15.8%減、前年同期比で23.1%の減少となりました。2025年3月を期限としたEMV3-Dセキュアの導入義務化の効果が寄与していると推測します。一方で、EC事業者実態調査※によると、「EMV3-Dセキュア」を導入している事業者は、2024年12月時点で61.5%、12月時点では65.2%と導入率はほぼ横ばいの状況です。導入率がそれほど変わらないにもかかわらず不正利用が減少している理由としては、EMV3-Dセキュア導入から時間が経過したことでパラメーターなどのチューニングが進み、不正利用防止効果が高まったことが可能性として考えられます。

※EC事業者実態調査：Caccoがインターネットにて EC事業者で不正注文対策に関わる担当者（24年：550人、25年：553人）を対象に実施

（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

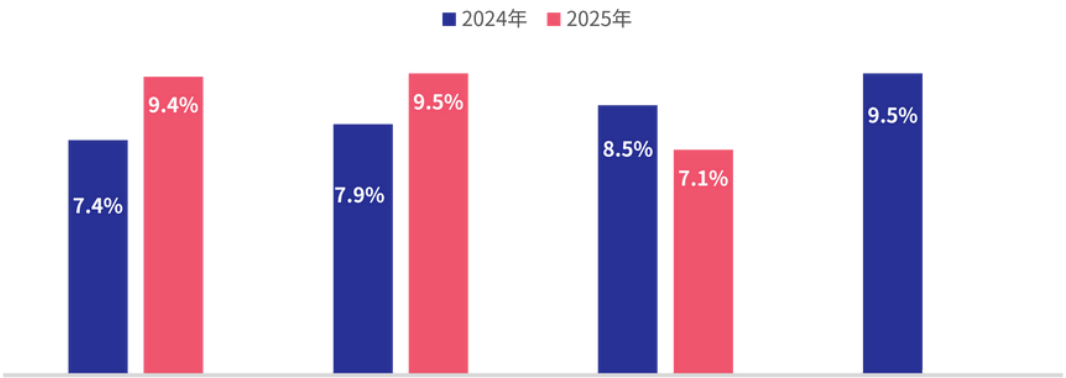
カード不正注文の発生率 （前年同四半期比較）



	1～3月	4～6月	7～9月	10～12月
2025年	1.8%	3.2%	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 2025年12月16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%	
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）
※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 2025年12月16日時点で集計

2025年7～9月期におけるクレジットカード不正注文発生率および転売発生率は、いずれも前年同期比で微減しました。特に4～6月期は、不正注文発生率の増加幅が例年より大きく、一時的に高水準となっていましたが、7～9月期には通常の水準に回帰したと見られます。また、転売発生率についても、2025年1～6月期は9%台と高止まりしていたものの、7～9月期には7.1%まで低下しました。不正・転売リスクは落ち着きを見せつつあるものの、引き続き動向を注視する必要があります。

不正注文検知数の商材別ランキングを見ると、2025年7～9月期は、夏休みや大型連休の影響により人の移動や余暇活動が活発化した結果、コンサートやライブなどのイベント関連が検知数1位となりました。また、レジャー需要の高まりを背景に、スポーツ用品が3位へと大きく順位を上げました。一方で、外出機会の増加と並行して在宅時間も一定程度確保される時期であることから、ホビー・ゲーム関連が4位にランクインしました。さらに、動画配信サービスなどのデジタルコンテンツも前期の10位から6位へと順位を上げました。

＜不正注文に狙われやすい商材ランキング＞

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

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	サブスサービス

※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 2025年12月16日時点で集計

（3）不正利用のトピック

転売対策： プラットフォーマー主導で進むルール厳格化とその背景

2025年7–9月期において、「転売」を巡る動きが改めて注目を集めました。特に10月に発表されたメルカリによる出品ルールの厳格化や、主要CtoCプラットフォーム3社であるメルカリ、LINE ヤフー（Yahoo!オークション、Yahoo!フリマ）、楽天グループ（楽天ラクマ）の人気ゲーム機器を巡る転売問題への対応は、現在の転売対策の方向性を象徴する事例と言えます。以下、転売を取り巻く課題を整理したうえで、プラットフォーマーによる不正抑止の取り組みについて解説します。

■転売の何が問題なのか

転売問題は、これまでも人気キャラクターグッズやゲームソフト、限定商品、スポーツや興業のチケットなどを中心にたびたび話題となってきました。一方で、現状では十分な対策が講じられていないケースも多く、課題が残されているのが実情です。

転売の問題点は、主に以下の3点です 。

① 消費者体験が損なわれること

人気商品発売直後に、転売者によって組織的・大量に買い占められることで、本来の購入希望者が適正価格で商品を入手することができなくなります。「いつも買えない」「転売者ばかりが買っている」という状況が続くことで、消費者の熱量が冷めるのみならず、ブランド価値の毀損にもつながります。

② 転売益を目的とした不正行為が行われること

CtoCプラットフォームでは、転売を目的として、偽造身分証や他人の名義を騙る不正なアカウントの作成が行われます。取引時に商品に問題があったり、正しく引き渡しが行われない場合でも、転売者本人に責任を問うことができなくなります。

③ 犯罪収益のマネーロンダリングに転売が利用されること

特殊詐欺や組織犯罪で得た不正資金を利用して購入した商品を、転売によって現金化することで、資金の出所が隠蔽されます。また、他人のカード情報を悪用して購入した商品を転売することで現金化する手口も多くみられます。

一方で、転売対策の法整備は進んでいません。チケット分野においては、2019年6月に施行された「特定興行入場券の不正転売の禁止等による興行入場券の適正な流通の確保に関する法律」（略称：チケット不正転売禁止法）により、不正転売が罰則付きで禁止されています。一方で、チケット以外の商品については包括的な法規制が存在せず、「不正な転売」と「正当な二次流通」との線引きが極めて難しいのが現状です。そのため、違法性の判断が困難で、規制強化が進みにくい状況が続いてきました。

■大手プラットフォーマーによる転売対策

こうした背景を受け、法規制に依存しない形での不正転売抑止として、CtoCプラットフォーマー側での対策が重要性を増しています。2025年には、人気ゲーム機器を巡る転売問題が大きな注目を集めました。発売前から大きな話題を呼ぶ商品で、高額転売、商品が手元にない状態での詐欺的な出品、誤認購入を狙う空き箱出品などのトラブルが予想されました。これに対しゲーム機メーカーである任天堂とメルカリ、LINE ヤフー（Yahoo!オークション、Yahoo!フリマ）、楽天グループ（楽天ラクマ）は不正転売を防ぐ目的で協力する取り組みを発表しました。各社の利用規約に違反する行為に対しては、フリマサイト側が能動的に出品削除対応を行う他、メーカーとの情報共有を含む連携体制構築を進めるとしました。これに合わせてLINEヤフー（Yahoo!オークション、Yahoo!フリマ）は転売商材として取引環境の混乱を招くおそれがある商品を出品禁止物に指定できるようガイドラインを改訂。当該ゲーム機をこれに指定することで、出品を禁止しました。このように、個社対応にとどまらず、CtoCプラットフォーマー横断で不正抑止に取り組む動きが見られた点は、転売対策の新たな局面を示すものと言えます。

また、最大手のメルカリは、2025年10月に公開した『「マーケットプレイスの基本原則」の考え方と議論の経緯に関するホワイトペーパー』の中で、転売を含む商品の取引についての方針を新たに定めました。「安全・信頼・人道的」というマーケットプレイスの基本原則は維持しつつ、不正出品やトラブルの急増、誹謗中傷の急増、極端な価格の乱高下など、マーケットプレイス内の「安心・安全」が著しく損なわれる可能性がある商品については、出品禁止などを含む対応を行う方針を明示しました。これは、転売に対して「不公正」、「気に入らない」といった主観的な「不快感」を根拠としたルールで禁止するのではなく、利用者が安心してマーケットプレイスに参加できなくなる状況を避けるために、メルカリが経営判断として個別の事案に対する判断の余地を認める試みとして位置づけられています。

>>> 3. 政策の動向

政府機関等における耐量子計算機暗号(PQC)への移行について(中間とりまとめ)公表

カード情報や認証情報の安全な伝送や保存など、キャッシュレスセキュリティの安全性を担保するために、暗号技術は重要な役割を果たしています。2025年11月、内閣官房は『政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ)』（以下『中間とりまとめ』） を公表しました。以下、その背景と『中間とりまとめ』の概要について紹介します。

■暗号の強度と使用期限

データの保存や通信に用いられる暗号の安全性は、計算量的安全性、すなわち現時点で実用化されている計算資源では解くことが極めて困難であるという前提に基づいています。しかし、コンピューターの能力の向上や新たなアルゴリズムの登場によって、この前提が崩れた場合、暗号の安全性は維持できなくなります（暗号の危殆化)。 米国の国立標準技術研究所（NIST）は政府機関などにおける各暗号の使用期限をガイドライン（NIST SP-800-57 ）で示しています。

<NISTが定める暗号強度別の使用期限>

弱 → 強

セキュリティ強度	使用期限	共通鍵暗号	ハッシュ	DSA（デジタル署名）	RSA（公開鍵暗号）
112	新規：2030年 （既存システム利用は当面可能）	3TDEA （3-key Triple DES）	SHA-224	公開鍵：2.048ビット 秘密鍵：224ビット	2,048ビット
128	利用可能	AES-128	SHA-256	公開鍵： 3,072ビット 秘密鍵： 256ビット	3,072ビット
192	利用可能	AES-192	SHA-384	公開鍵： 7,680ビット 秘密鍵： 384ビット	7,680ビット
256	利用可能	AES-256	SHA-512	公開鍵：15,360ビット 秘密鍵： 512ビット	15,360ビット

※1　NISTが定める鍵管理における推奨事項「NIST Special Publication 800-57 Part 1 Revision 5 」を参考に作成
※2　共通鍵暗号：情報の暗号化と復号に共通の鍵を用いる暗号方式で、暗号化と復号に同じ鍵を使用。そのため事前に安全な方法で共通鍵を共有し、管理する必要がある。
※3　ハッシュ：　どんな長さのデータ（文章やファイルなど）からでも、決まった長さのユニークな値（ハッシュ値）を生成する計算方法とその値のこと。
ハッシュ値から元のデータを復元するのは非常に困難なため改ざん検知やセキュリティ強化に役立つ。
※4　公開鍵暗号：公開鍵と秘密鍵というペアになる2つの鍵を使ってデータの暗号化及び復号を行う暗号方式。片方の鍵を使って暗号化したものは、それと対になるもう一方の鍵を使用しなければ復号できない仕組みのため、共通鍵暗号では共通鍵を安全に送ることが課題になっていたが、公開鍵の場合はそういった課題がない。

NISTでは、現在Webサーバーの証明書などに広く使われているRSA-2048（暗号鍵の長さが2,048ビットのRSA公開鍵方式）については2031年以降使用を推奨しないとして、より強度の高い暗号への移行を義務付けています。日本では、CRYPTREC※が『電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)』を策定しています。2022年3月には、CRYPTREC暗号リストに掲載された暗号技術を利用する際に、情報システムでの運用期間を考慮して適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定した『暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準』が公開されました。 NISTと同様に、112ビット強度の暗号については2031年以降の新規生成は不可としており、128ビット強度の暗号についても2051年以降の新規生成は不可としました。

※CRYPTREC：電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。 デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号技術評価委員会で構成される。
https://www.cryptrec.go.jp/system.html

<日本の電子政府システムの調達基準>

想定運用終了・廃棄年/利用期間		2022～2030年	～2040年	～2050年	～2060年	～2070年
112ビット セキュリティ	新規生成	移行完遂期間	利用不可	利用不可	利用不可	利用不可
	処理		許容			
128ビット セキュリティ	新規生成	利用可	利用可	移行完遂期間	利用不可	利用不可
	処理				許容	
192ビット セキュリティ	新規生成	利用可	利用可	利用可	利用可	利用可
	処理					
256ビット セキュリティ	新規生成	利用可	利用可	利用可	利用可	利用可
	処理					

（『暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準 Ver1.0』デジタル庁・総務省・経済産業省）2022年3月

■量子コンピューター実用化によるRSA暗号と楕円曲線暗号の終焉

2030年代を見据えて開発が進められている量子コンピューターが実用化されると、RSA暗号の安全性を支える素因数分解問題や、楕円曲線暗号の安全性を支える離散対数問題が、「ショアのアルゴリズム」により、理論上は効率的に解けることが示されています。その結果、RSA暗号や楕円曲線暗号は、暗号強度の問題ではなくアルゴリズムそのものが危殆化してしまいます。また、共通鍵暗号についても、「グローバーのアルゴリズム」により$\sqrt{N}$の効率で鍵の探索が実行可能になるため、128bit以上の強度を担保するためにはAES-256以上が必要となります。こうした状況を踏まえ、各国は耐量子計算機暗号（PQC）移行時期に関わる方針を検討しています。今回の『中間とりまとめ』は、日本政府機関等におけるPQC移行の方向性を整理し、ロードマップを策定するための作業と位置付けられます。

■採用する技術

PQCの国際的な標準化動向としては、NISTがFIPSとして複数の暗号方式の標準化を進めています。CRYPTECでも、CRYPTEC暗号リストの更新が可能となるよう、これらのPQC暗号方式の安全性評価および実装性能評価を実施しています。

＜NISTで標準化されたPQアルゴリズムの例（抜粋）＞

アルゴリズム	機能	仕様
CRYSTALS-Kyber (ML-KEM)	鍵確立（鍵交換）のための非対称アルゴリズム	FIPS PUB 203
CRYSTALS-Dilithium (ML-DSA)	デジタル署名のための非対称アルゴリズム	FIPS PUB 204
SPHINCS+ (SLH-DSA)	デジタル署名のための非対称アルゴリズム	FIPS PUB 205

（『Announcing the Commercial National Security Algorithm Suite 2.0』米国国家安全保障局）2022年9月を基に作成

■移行の期限

米国、EUなどの諸外国では2035年を移行期限としてPQCへの移行を進めており、日本のPQCへの移行が遅れることで、これらの諸外国との間で安定的なネットワークの構築やサイバーセキュリティの確保、防衛や安全保障などの重要な情報のやりとりに支障をきたします。『中間とりまとめ』では、日本も2035年を目標にPQCへの移行を進めることを検討しています。

暗号方式の提案から普及までは相当の期間が必要となるため、長期間の移行スケジュールを策定する必要があります。一方で、特に機微な情報や長期間の保護が必要となる情報については、すでにHNDL攻撃（Harvest Now, Decrypt Later：暗号化データを保存しておき、量子計算機での暗号解読が可能となった後に解読を行う攻撃）というリスクが存在します。対象によっては、2035年の目標を踏まえつつ、より早期にPQCへの移行を行うことを含め、適切に検討を進めることが重要と整理しました。

■ロードマップの考え方

『中間とりまとめ』では、原則として2035年までの移行を行う前提で、2026年度中にロードマップを策定するとしています。ロードマップには以下を含むとしており、他にも盛り込むべき事項を引き続き検討していくと述べています。

① 移行の対象：主に公開鍵暗号。共通鍵暗号やハッシュ関数についてもセキュリティ強度の担保される鍵長に変更を検討する。

② PQCの安全性確認：安全性と実装性能が確認されたPQCについて、CRYPTEC暗号リストに反映するよう、掲載方法も含めてCRYPTECで検討する。

③ PQCへの移行期限：原則として2035年までを目処とする。

④ 暗号技術の利用に係る停止の時期：量子計算機技術の進展を踏まえた暗号技術の安全性評価、政府機関等におけるPQCへの移行状況、諸外国の状況等を十分に踏まえて検討する。

移行にあたって最初に着手することとして、移行対象把握のための暗号インベントリ（どこで、どのような暗号が使用されているかのリスト）を作成し、移行の必要性や方法などについて検討する必要があります。PQCについては暗号解読手法や安全性評価、実装時のセキュリティ対策などが十分に蓄積されていないことも考慮し、暗号部分は迅速に切り替えられる（クリプト・アジリティ）情報システムを構築する必要があります。また、利用環境によっては、PQCと従来の暗号技術を併用して段階的に量子耐性をつけ、HNDL攻撃に対応することも有効です。

今回の『中間とりまとめ』および2026年度に策定されるロードマップは、政府機関などのPQC移行を対象としています。一方で、PQC移行は政府機関だけでなくクレジットカード分野を含む金融サービスなどの重要インフラ事業者も考慮すべき課題です。これらのロードマップを参考に準備を進めていく必要があります。

【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

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）