Cashless Security Report

Quarterly Report

（2024年 10-12月版）2025年4月発行

PCI DSS Ready Cloud

2025.4.24

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10-12月版：2025年4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（2024 年10-12月）

（1）カード情報流出事件数・情報流出件数の推移

2024年10-12 月のカード情報流出事件

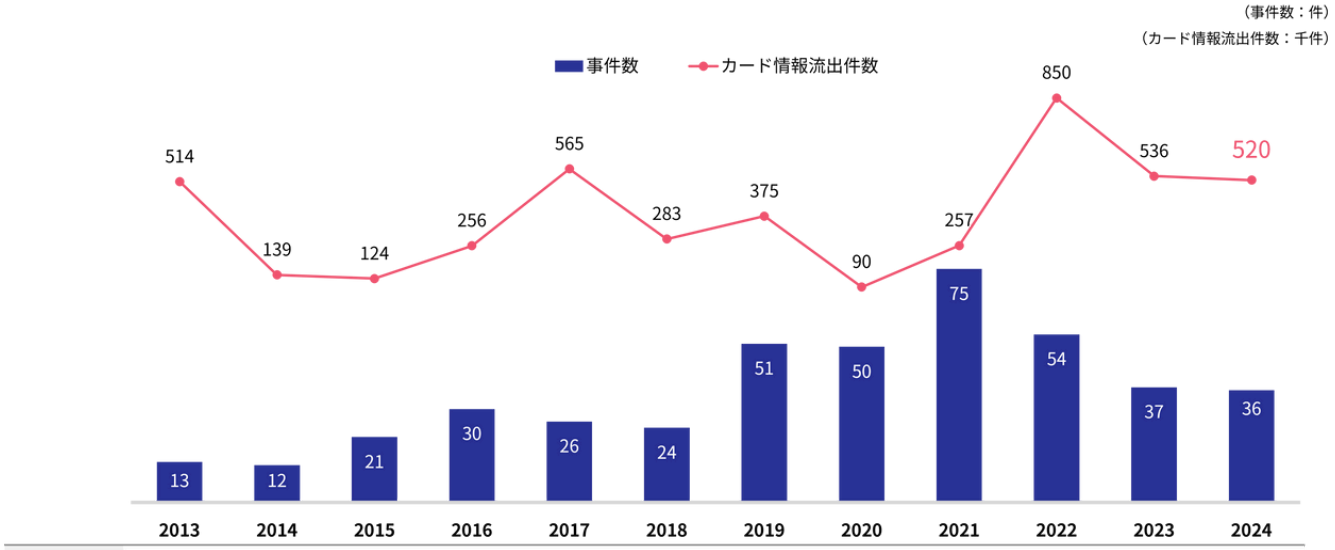
- 事件数　8件
- カード情報流出件数　164,579件

※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

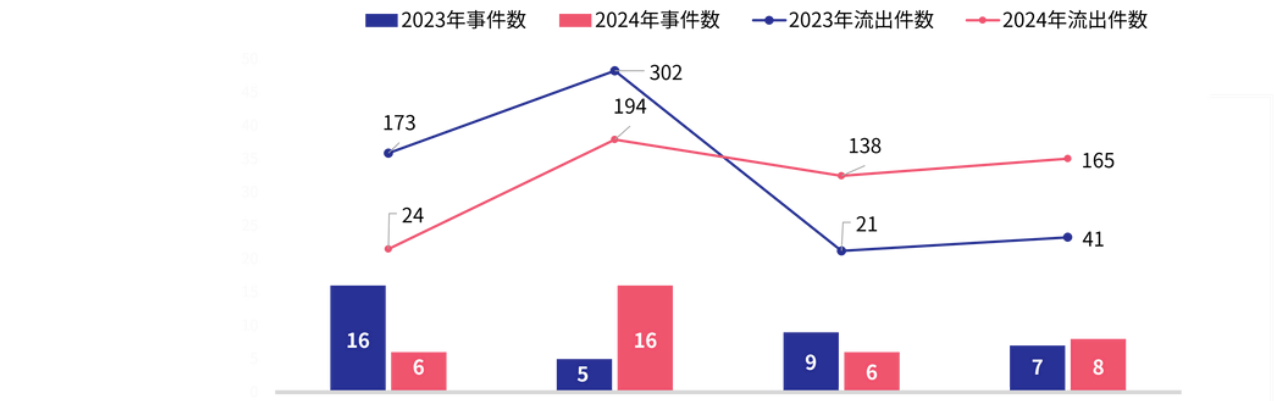


	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
事件数	13	12	21	30	26	24	51	50	75	54	37	36
カード情報流出件数	514,369	138,717	123,527	255,689	564,844	283,374	375,479	89,628	256,822	849,950	536,291	520,074

（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	16	6	8
	カード情報流出件数	23,677	194,241	137,577	164,579
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、7-9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

事件数　4-6月 15→16、2025年7-9月 5→6/ 流出件数 4-6月分：175,847 → 194,241、7-9月分：120,895→137,577

※3 2024年3月31日時点で集計

2024年10-12月に公表されたカード情報流出事件は8件です。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もので、事件発生の公表が早まっていることが伺えます。なお、2件のうち2024年12月に第一報が公表された1件については、2025年3月24日に詳細が公表されたため、2024年10-12月のカード情報流出件数と流出期間別集計に情報を反映しています。

流出したカード情報の件数は164,579件となりました。1事件あたり約50,000件を超える大規模な流出が2件発生したことから、前年同期比で約3.8倍に増加しました。流出期間が公表されている7件のうち、3年以上に及ぶケースは5件を占めており、7-9月期に続き高い割合を占めています。

年間の動向を見ると、2023年のカード情報流出件数は536,291件、事件数は37件であったのに対し、2024年はカード情報流出件数520,074件、事件数36件と、事件数・カード情報流出件数とも、ほぼ横ばいとなりました。特に2024年4月以降、流出期間の開始が2021年以前で長期にわたって大量のカード情報が流出している事件の公表が増えており、今後も同様の傾向が続くか、注意が必要です。

（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1-3月		2024年4-6月		2024年7-9月		2024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		6	23,677	16	194,241	6	137,577	8	164,579
業種別	アパレル	1	3,827	3	17,176	0	0	1	71,943
	コスメ	0	0	1	15,198	0	0	0	0
	食品	2	7,183	8	126,746	5	136,145	3	67,489
	家電・電子機器・PC	1	4,748	0	0	0	0	1	4,257
	生活雑貨、家具、インテリア	0	0	1	0	1	1,432	0	0
	健康食品	1	5,193	0	0	0	0	1	4,494
	ホビー	1	2,726	1	4,969	0	0	1	0
	自動車、バイク	0	0	0	0	0	0	0	0
	家具	0	0	1	3,958	0	0	0	0
	その他	0	0	1	26,467	0	0	1	16,396
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、7-9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
4-6月分その他の流出件数　8,073→26,467、7-9月分食品の流出件数　119,463→136,145
4-6月その他 事件数0→1、7-9月食品 事件数4→5
※3 2025年3月31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1-3月		2024年4-6月		2024年7-9月		2024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	8,073	0	0	1	4,257
3ヶ月-1年	1	2,726	2	5,621	0	0	1	6,929
1-3年	5	20,951	9	113,120	3	25,132	0	0
3年以上	0	0	4	67,427	3	112,445	5	153,393

（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、7-9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
4-6月 1-3年事件数7→9　流出件数60,920→113,120、3年以上　事件数3→4　流出件数49,033→67,427　/　7-9月 1-3年事件数2→3　流出件数8,450→25,132
※3 2025年3月31日時点で集計

2. ECにおける不正利用の概況（2024年10-12月）

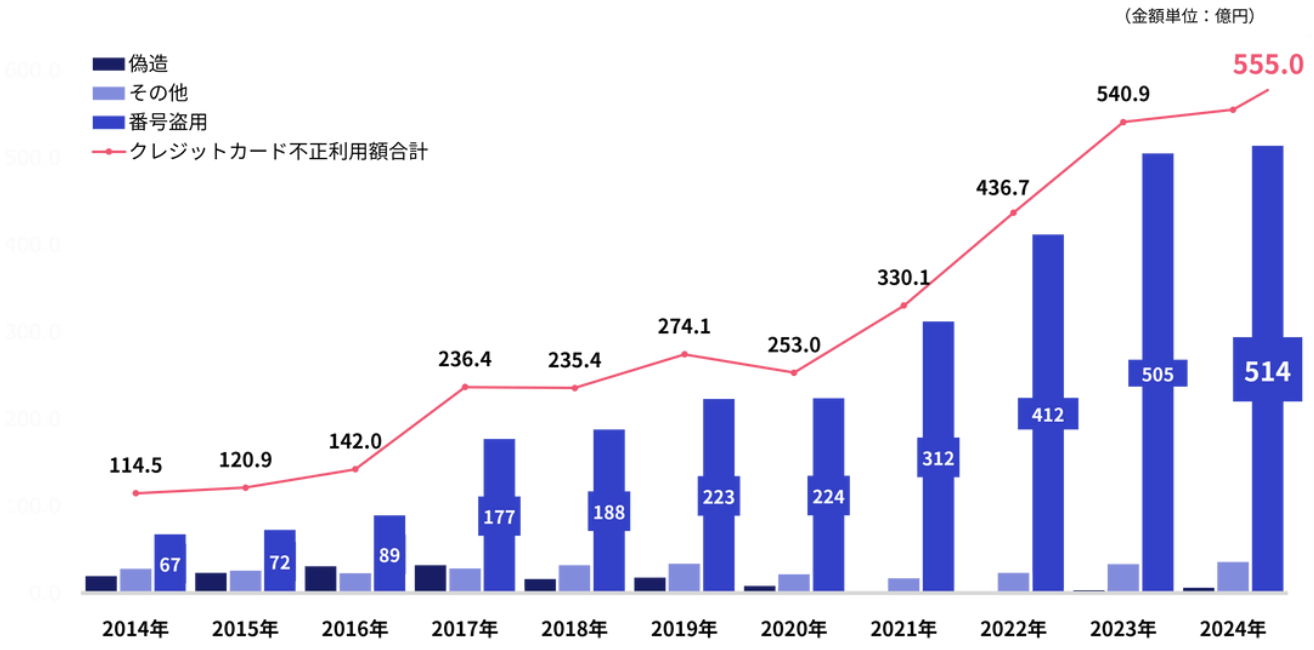
（1） クレジットカード不正利用被害額の推移

2024 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　162.3億円
- 偽造　2.2億円
- 番号盗用　150.7億円
- その他　9.4億円

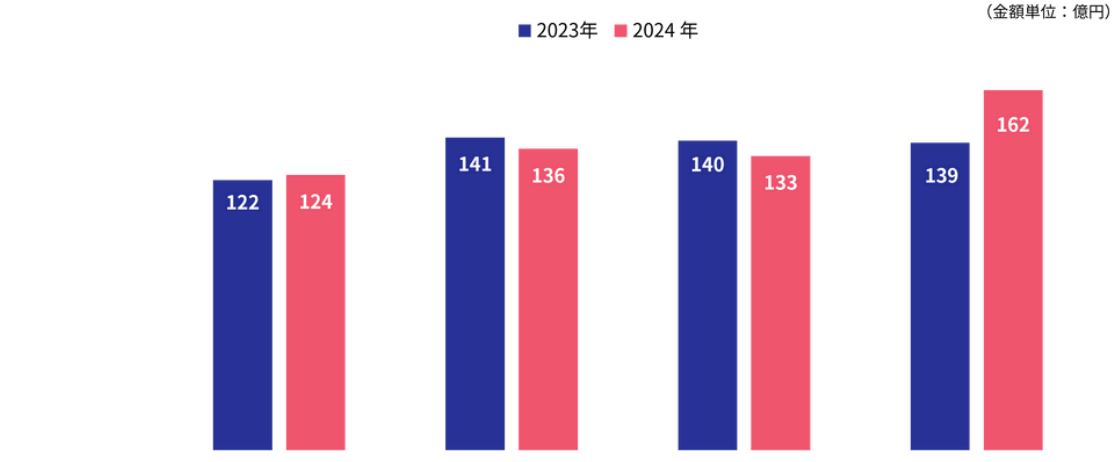
※日本クレジット協会調べ
https://www.j-credit.or.jp/information/statistics/index.html

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3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）



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
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）2025年3月
※2024年1−6月の数値変更を加味して修正（日本クレジット協会より2025年3月時点）

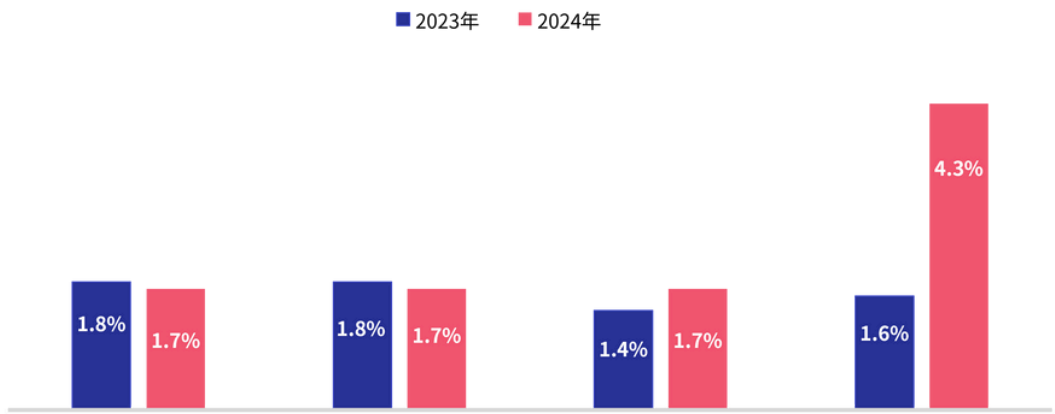
2024年10-12月のクレジットカード不正利用被害額は162.3億円となり、前年同期比で17.1%増加しました。年間ベースでは2020年以降5年連続で増加傾向が続いています。しかし、注目すべき点として、増加率は過去と比べて大幅に鈍化しています。2023年と2024年の年間増加額は14.1億円（+2.6%）にとどまり、これまでの約100億円規模（+20%台）の増加と比べると、明らかな減速が見られます。

この要因のひとつとして、2024年3月に導入期限を迎えた「EMV 3-Dセキュア」のEC加盟店への導入が進んだことが考えられます。この施策により、不正被害額の抑制につながった可能性が高いと推測されます。しかし懸念されるのが、2024年4-６月、7-9月は前年同期に比べて若干減っていた不正利用被害が、10-12月には前年同期比17.1%増と再び増加に転じたことです。今後の動向を慎重に見守る必要があります。

（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

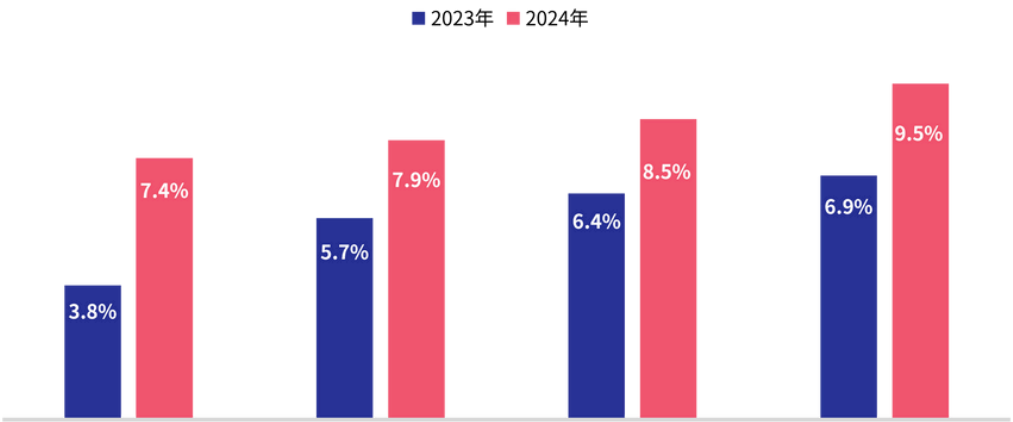
カード不正注文の発生率 （前年同四半期比較）



	1～3月	4～6月	7～9月	10～12月
2024年	1.7%	1.7%	1.7%	4.3%
2023年	1.8%	1.8%	1.4%	1.6%

※「O-PLUX Payment Protection」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 Payment Protection」加盟店判断により異なる。
※2025年3月31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%	9.5%
2023年	3.8%	5.7%	6.4%	6.9%

※「O-PLUX Payment Protection」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 Payment Protection」加盟店判断により異なる。
※2025年3月31日時点で集計

＜不正注文に狙われやすい商材ランキング＞

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	サブスサービス

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

※「O-PLUX Payment Protection」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 Payment Protection」加盟店判断により異なる。
※2025年3月31日時点で集計

2024年10月-12月期におけるクレジットカード不正利用の発生率は、年末にかけて大幅に上昇し、2022年から開始している調査で最も高い「4%」を記録しました。同様に、転売を目的とした不正注文の発生率も「9.5%」に達し、いずれも過去最高の結果となりました。不正が集中した商材としては、カメラやゲーム機といった高額な電子機器に加え、ライブやテーマパークなどのチケット類が上位に挙がっています。これらはいずれもクリスマスや年末年始に向けたギフト需要やレジャー需要が高まるタイミングと重なっており、転売目的での不正注文が発生しやすくなったと考えられます。

（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、経済産業省のウェブ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】

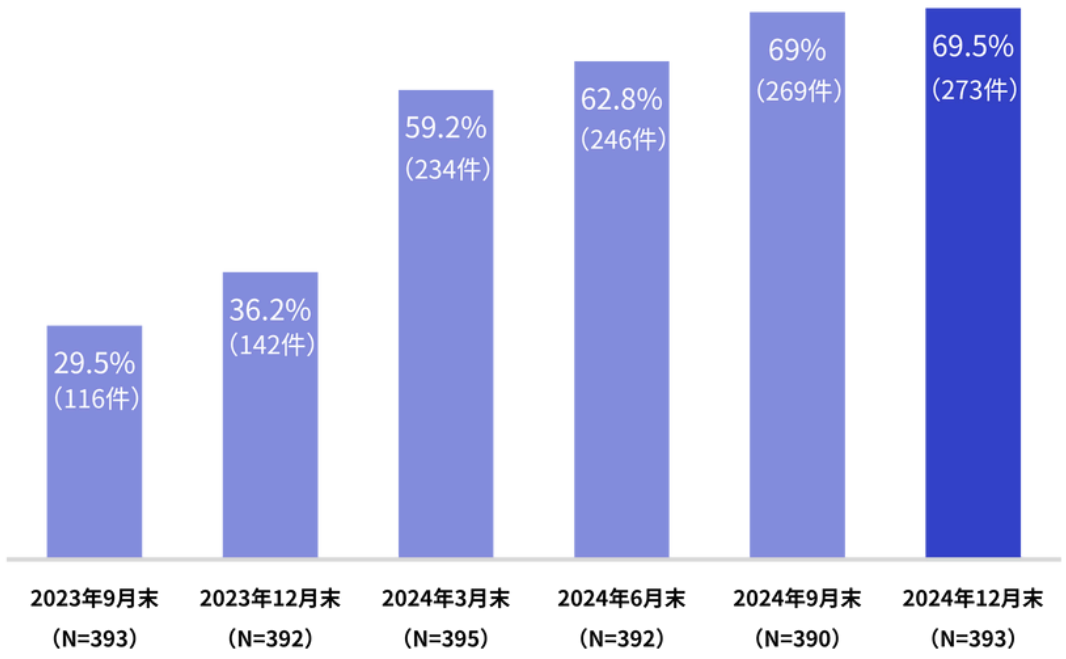
2024年12月末

【調査結果】

①調査対象ドメイン数　393件

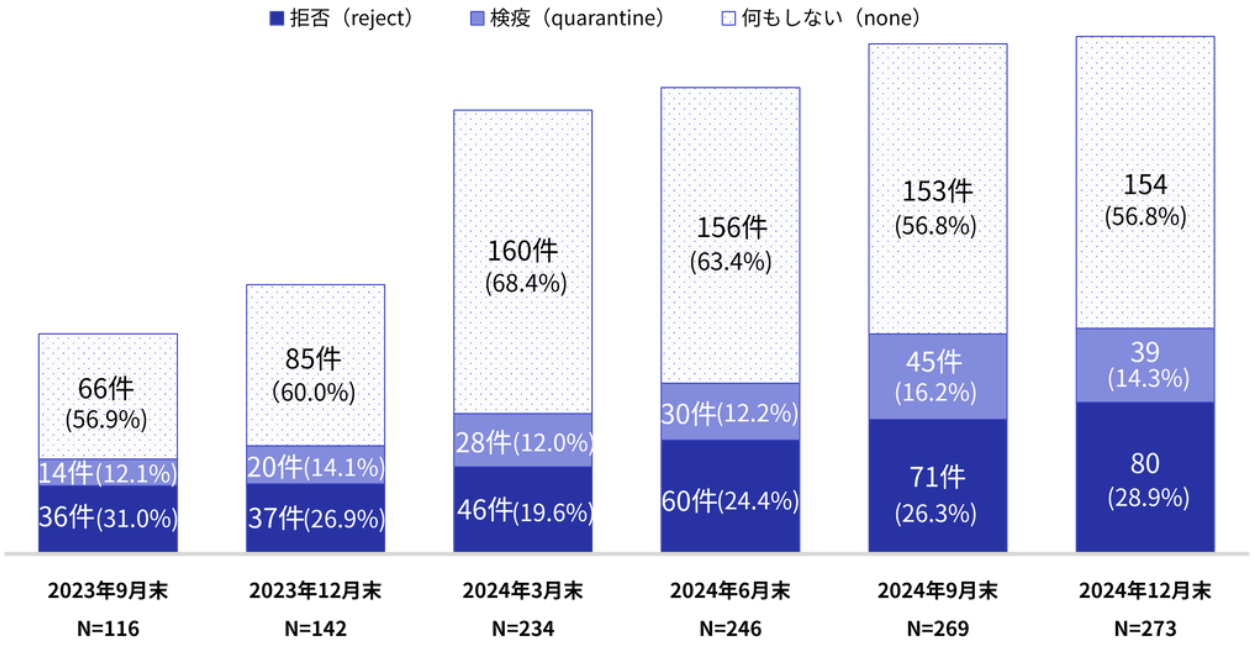
②調査対象ドメインごとのDMARC対応状況と運用ポリシー

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）



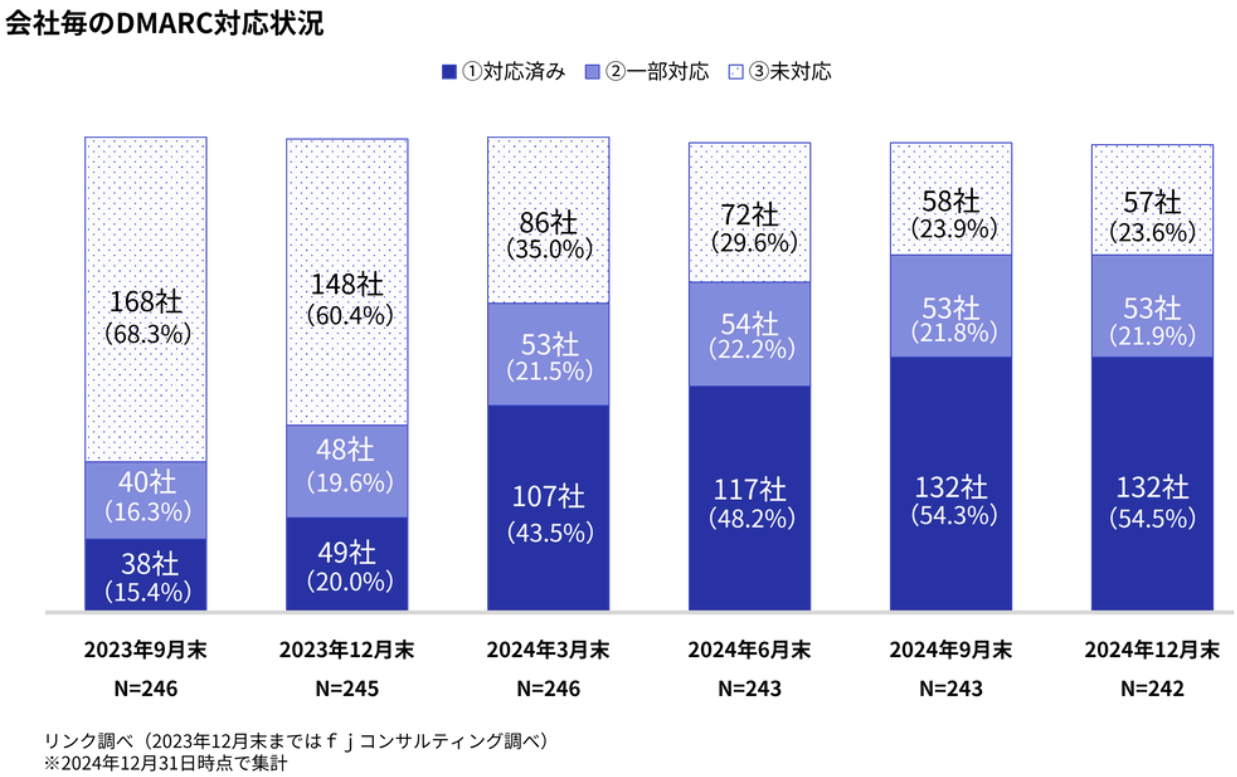
リンク調べ（2023年12月末まではｆｊコンサルティング調べ）
※2024年12月31時点で集計

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12月31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12月31日時点で集計

2024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393件のうち、有効なDMARCレコードが設定されているのは273件（69.5%）となりました。2024年9月末からほぼ横ばいで7割を目前に足踏みしている状態となっています。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80件（28.9%）に増加し、ポリシーを「quarantine（検疫）」に設定したドメインが39件（14.３%）に減っています。ポリシーを「none（何もしない）」に設定したドメイン数は154件（56.8%）とほぼ横ばいとなりました。ポリシーが「quarantine（検疫）」から最も厳しい「reject（拒否）」に移行が進んでいる状況が確認されているものの、ポリシーをnoneに設定しているドメインを、より厳しいポリシーに移行することが望まれます。また引き続き未だDMARCが導入されていないドメインが減少していない状況を改善する必要があります。

組織別にみると、DMARCを一部でも導入しているイシュアは242社中185社（76.4%） となっています。うち132社（54.5%）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。こちらの導入状況も、ほぼ横ばいとなっています。

（4）不正利用のトピック

総額1億円以上のクレジットカード不正利用事件、指示役を逮捕

2024年10月、警察庁サイバー特捜部などは他人名義のクレジットカード情報を不正利用して代金をフリーマーケットアプリ（以下フリマアプリ）運営者から騙し取った疑いで、グループの指示役と見られる男を逮捕しました。

本件では、実行犯となる「闇バイト」をX（旧Twitter）などで募集し、応募者に対してして秘匿性の高い通信アプリ「テレグラム」で犯行を指示していました。2023年6月以降17名の実行役が摘発され、実行役の携帯電話や関連口座の解析により指示役の特定に至りました。サイバー特捜部はSNSなどでゆるくつながり、特殊詐欺などの犯行を繰り返す「匿名・流動型犯罪グループ（トクリュウ）」による事件とみています。

実行犯は、指示役からの命令に従い、出品役と購入役として以下の手順でフリマアプリ運営者から立替払いで入金される代金を詐取していました。

①指示役がダークウェブ等で他人のカード情報を入手
②指示役から実行役（出品役と購入役）に指示
③出品役が商品を架空出品し、購入役が架空出品された商品を購入し、指示役から伝えられた他人名義のクレジットカード情報を使用し不正に決済
④売買の成立を装い、出品役にフリマアプリ運営者から立替払いで入金された代金を詐取
⑤入金された商品代金を暗号資産に交換して指示役に送金

グループは、フリマアプリの悪用に加えて、オークションサイトで他人名義のクレジットカード情報を利用した購入と入手した商品の転売・換金を行う方法でも不正に利益を得ており、少なくとも900件、1億円以上を詐取したとみられます。

フリマアプリ・オークションサイトを利用した不正の流れ

実行役は詐取した代金の5%を取り分として、残りを指示役の暗号資産口座に送金していました。指示役は不正に得た収益を匿名性が高い暗号資産「Monero」に換えて複数の口座に分散させていました。

これまでの摘発では、実行役のみが逮捕されるケースが多く、組織の指示役にまで捜査が及ぶことは稀でした。しかし、近年ではフィッシングサイトを仕掛ける技術者や、送金役など、より上流の関係者まで逮捕されるケースが増えています。今回の指示役逮捕も、警察の取り締まり強化の成果の一つといえるでしょう。

3. クレジットカード・セキュリティガイドライン【6.0版】の改訂ポイント

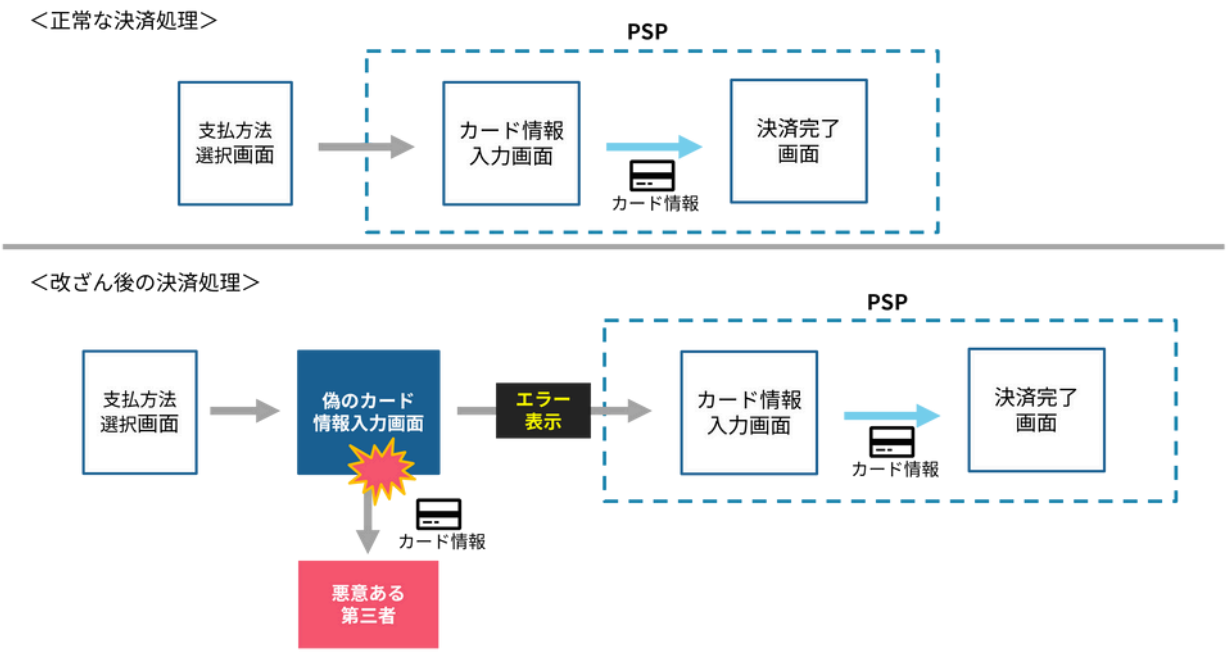
2025年3月、割賦販売法におけるクレジットカード情報保護および不正利用対策の実務上の指針である『クレジットカード・セキュリティガイドライン【6.0版】』（以下セキュリティガイドライン6.0版）が公表されました。改訂のポイントを解説します。

（1）EC加盟店のシステムおよびWEBサイトの「脆弱性対策」の義務化

クレジットカード・セキュリティガイドラインでは、EC加盟店のカード情報保護対策は、カード情報を保持しない非保持化、もしくはカード情報を保持する場合はPCI DSS準拠を指針対策（割賦販売法で定める「必要かつ適切な措置」）として従来から求めています。大半のEC加盟店は、決済代行事業者が提供する非通過型決済サービス（ECサイトの機器・ネットワークをカード情報が通過することがない）を利用して非保持化を実現しています。

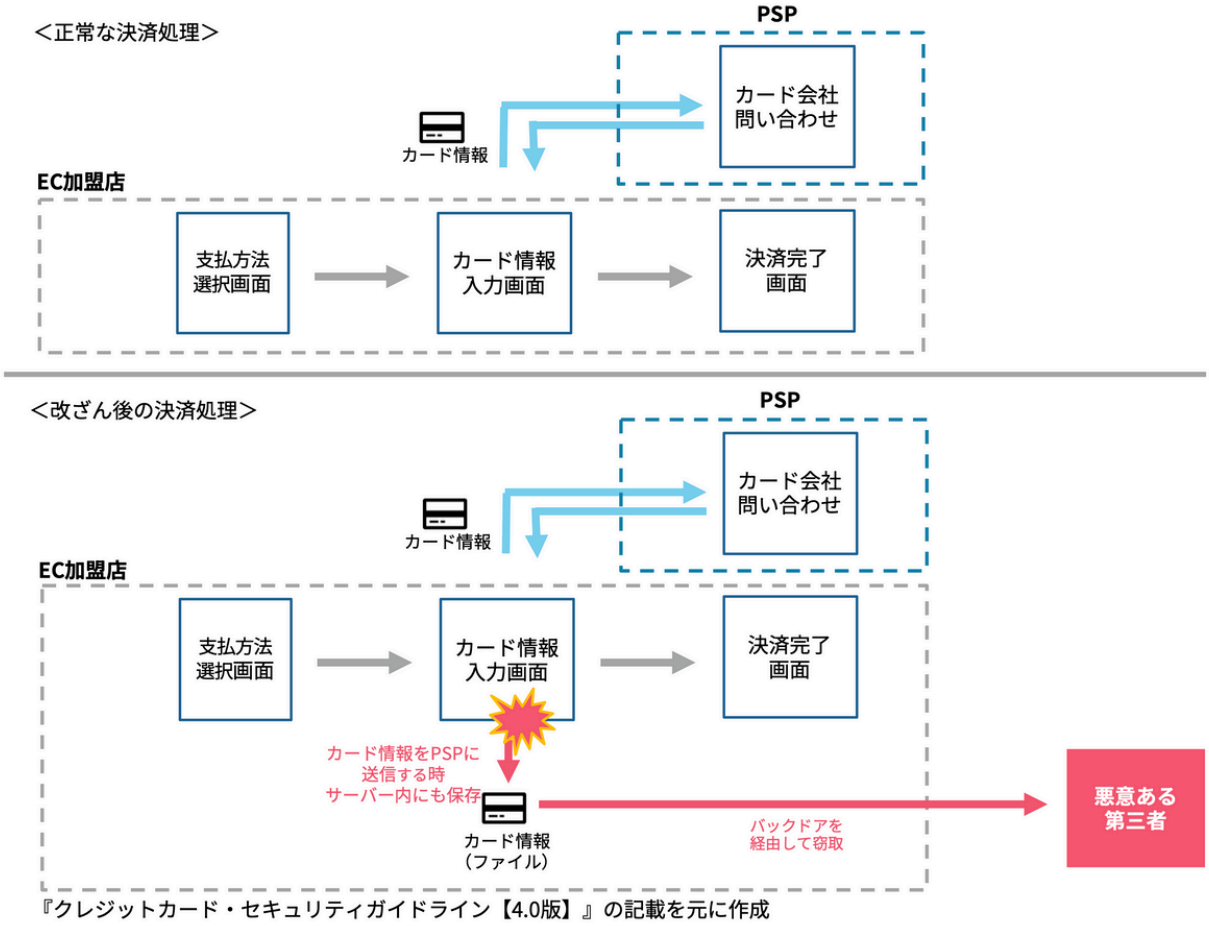
非保持化により、ECサイトのデータベースに保存された大量のカード情報をSQLインジェクション等の手口で抜き取られるような事案はほぼなくなっています。一方で、2018年ごろから見られるようになった、ECサイトの決済ページで消費者が入力したカード情報をそのまま盗み取る「オンラインスキミング」という手口によって、非保持化済みのEC加盟店からもカード情報の流出が続いています。具体的には、ECサイトの決済ページへのリンクを改ざんして偽の決済ページを挿入したり、決済ページに不正なJavaScriptを挿入することで、カード情報を正規のPSP（EC加盟店向けの決済代行業者）以外に第三者にも送信する手口です。

オンラインスキミング（リダイレクト（リンク）型決済の場合）



『クレジットカード・セキュリティガイドライン【4.0版】』の記載を元に作成

オンラインスキミング（JavaScript（トークン）型決済の場合）



『クレジットカード・セキュリティガイドライン【4.0版】』の記載を元に作成

オンラインスキミングをはじめとする、EC 加盟店のシステムやWeb サイトのウイルス対策、管理者の権限の管理、デバイス管理等の脆弱性対策の不備を原因としたカード情報流出を防止するための対策として、これまでは新規加盟店を対象に、自社システムやWebサイトの脆弱性対策を実施し状況をカード会社（アクワイアラ）や決済代行事業者に報告する「セキュリティチェックリスト」が試行されていました。『セキュリティガイドライン6.0版』では、これを全ての加盟店向けに拡大し、「脆弱性対策」を指針対策（割賦販売法で定める「必要かつ適切な措置」）として義務付けました。

また、最近はクレジットカード番号の規則性を悪用して機械的にカード番号を生成する手法「クレジットマスター」により、大量にカード番号を生成し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。これに対してもEC加盟店で取引の速度や連続性によって異常な取引であることを検知し取引を遮断するなどの対策を講じることを求めています。

具体的に求められる対策の内容は『ECサイト加盟店におけるセキュリティ対策導入ガイド【附属文書20】』に取りまとめられており、EC加盟店は全ての対策を実施する必要があります。概要は以下となります。

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

- システム管理画面のアクセス可能な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。
- 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(PCI DSS ver4.0.1 基準)のログイン失敗でアカウントをロックする。

②データディレクトリの露見に伴う設定不備への対策

- 公開ディレクトリには、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。）
- 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

- 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を行う。
- WEB アプリケーションを開発又はカスタマイズされている場合には、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。その際は、入力フォームの入力値チェックも行う。

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

- マルウェア検知/除去などの対策として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。

⑤悪質な有効性確認、クレジットマスターへの対策

- 悪質な有効性確認、クレジットマスターに対して以下のいずれか1つ以上の対策を実施する。
  - I. 不審なIPアドレスからのアクセス制限
  - II. 同一アカウントからの入力制限とオーソリ拒否時のエラー内容非表示
  - III. EMV 3-DセキュアやSMS通知などの本人認証
  - IV. 有効性確認の回数制限を設けるなどの対策

（2）「線の考え方」に基づく不正利用対策への指針対策追加

増え続けるクレジットカード不正利用への対策として、『セキュリティガイドライン5.0版』では、全てのEC加盟店が2025年3月末までにEMV 3-Dセキュア（以下EMV3-DS）による本人認証を導入することを求めていました。また、新たな考え方として、カード決済時に加えて決済前、決済後という場面ごとに対策を考える「線の考え方」を提示し、詳細運用は今後検討するとしていました。

『セキュリティガイドライン6.0版』では、全てのEC加盟店に対して、EMV3-DSの導入が指針対策として義務付けられました。また、「線の考え方」に基づき、決済前の対策として適正な不正ログイン対策の実施が指針対策とされました。

不正ログイン対策が必要な場面として具体的に「会員登録」と「会員ログイン」、「属性情報変更」を挙げ、それぞれの場面に適した対策を1つ以上導入するものとしています。

＜決済前の不正利用対策＞

対象項目	対策が有効な場面		
	会員登録	会員ログイン	属性情報変更
① 不正なIPアドレスからのアクセス制限	○	○	○
② 2段階認証又は多要素認証（2要素認証）による本人確認	－	○	○
③ 会員登録時の個人情報確認 （氏名・住所・電話番号・メールアドレス等）	○	○	－
④ ログイン試行回数の制限強化（アカウント/パスワードクラッキングの対応）、スロットリング	○	○	－
⑤ 会員登録時/属性情報変更時のメールやSMS通知	－	○	○
⑥ 属性・行動分析	○	○	○
⑦ デバイスフィンガープリント	○	○	○
⑧ その他の対策 （「EC加盟店におけるセキュリティ対策一覧_3.不正ログイン対策（決済前の対策）」記載の対策）			

※『クレジットカード・セキュリティガイドライン【6.0版】』(クレジット取引セキュリティ対策協議会）2025年3月

（3）不正顕在化加盟店・高リスク商材取扱加盟店における指針対策の変更

『セキュリティガイドライン5.0』までは、EC加盟店の不正利用対策として「本人認証」「券面認証」「属性・行動分析（不正検知システム）」「配送先情報」の４つの方策を挙げ、高リスク商材取扱加盟店（※1）は1つ以上、不正顕在化加盟店（※2）は２つ以上を導入することを求めていました。

※1:①デジタルコンテンツ（オンラインゲームを含む）、②家電、③電子マネー、④チケット、⑤宿泊予約サービス を取扱う加盟店
※2:カード会社（アクワイアラー）各社が把握する不正利用金額が、「3ヵ月連続50万円超」に該当する加盟店。

しかし実際には加盟店の取扱商品やスキーム等により手口が異なり、これまでの４方策では実効的な抑止効果が得られなくなっていることから、以下の通り指針対策を変更しました。

①従来の高リスク商材は、「相対的にリスクが高い商材」として、追加導入する対策や既に導入している対策の設定項目の追加・変更、チューニングにおいては、リスクを認識した上で適切な対応を行う。

②不正顕在化加盟店については、類似の不正利用の発生を防止するために、不正利用の発生状況等に応じて、「線の考え方」に基づき本ガイドラインが掲げる不正利用対策を追加導入する。

具体的な「線の考え方」に基づく決済前・決済時・決済後の場面ごとの対策については、『ECサイト加盟店におけるセキュリティ対策導入ガイド【附属文書20】』にて取りまとめられています。

【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）