Cashless Security Report

Quarterly Report

（2026年 1-3月版）2026年8月発行

PCI DSS Ready Cloud

2026.8.4

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2026年 1-3月版：2026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（2026 年1-3月）

（1）カード情報流出事件数・情報流出件数の推移

2026年1-3月のカード情報流出事件

- 事件数　2件
- カード情報流出件数　3,463件

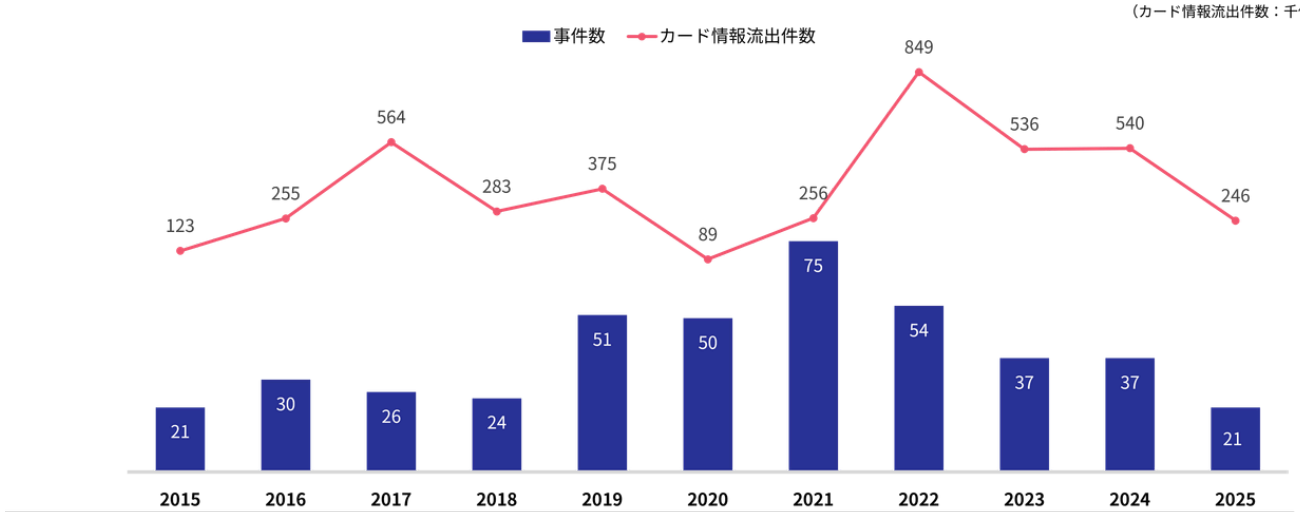
※クレジットカード、ブランドデビットカード、ブランドプリペイドカードを含む

【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

（事件数：件）
（カード情報流出件数：千件）

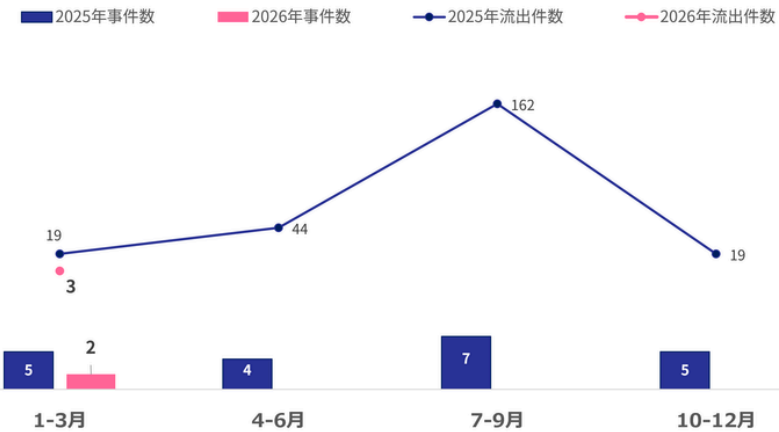


	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
事件数	21	30	26	24	51	50	75	54	37	37	21
カード情報流出件数	123,527	255,689	564,844	283,374	375,479	89,628	256,822	849,950	536,291	540,722	246,474

（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6月4日時点で集計

2026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）

（事件数：件）
（カード情報流出件数：千件）



		1-3月	4-6月	7-9月	10-12月
2026年	事件数	2			
	カード情報流出件数	3,463			
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

（Cacco・リンク調べ）
※1 2026年6月4日時点で集計

2026年1-3月期に公表されたカード情報流出事件は2件となりました。2件のうち1件は詳細判明前となります。判明している流出したカード情報の件数は3,463件と前四半期（2025年10-12月期）に比べ大幅に減少しました。 前年同四半期の19,635件に比べても大幅に減少しています。2025年3月発行のクレジットカード・セキュリティガイドライン【6.0版】（最新版は2026年3月発行の6.1版）でEC加盟店に義務付けられた脆弱性対策への対応が進んできたことが要因の一つと考えられます。

（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		2025年4-6月		2025年7-9月		2025年10-12月		2026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		4	44,295	7	162,894	5	19,650	2	3,463
業種別	アパレル	1	30,712	1	60	3	18,592	0	0
	食品	1	2,270	3	130,912	1	1,049	0	0
	家電・電子機器・PC	0	0	1	96	1	9	0	0
	生活雑貨・家具・インテリア	1	10,423	0	0	0	0	0	0
	ホビー	0	0	1	30,431	0	0	0	0
	コスメ	0	0	0	0	0	0	1	0
	その他	1	890	1	1,395	0	0	1	3,463
カード会社		0	0	0	0	0	0	0	0

（Cacco・リンク調べ）
※1 2026年6月4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	2025年4-6月		2025年7-9月		2025年10-12月		2026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	2,270	2	30,491	1	9	0	0
3ヶ月-1年	0	0	2	773	0	0	0	0
1-3年	1	10,423	1	127,263	0	0	0	0
3年以上	2	31,602	2	4,367	4	19,641	1	3,463

（Cacco・リンク調べ）
※1 2026年6月4日時点で集計

2026年1-3月期は、商材別にみると「コスメ」1件、「その他」が1件発生しています。うち詳細が判明している1件は、自動車部品販売（分類上は「その他」）で、2021年3月から2024年11月までの期間に3,463件のカード情報が流出しました。事件発覚のきっかけはカード会社の指摘によるものです。連絡を受けて2日後には事件発生の第一報を公表し、およそ1ヶ月間でフォレンジック調査を完了。事件発覚から103日後には調査結果を公表しています。

（3）カード情報流出事件トピック

クレジットカード業界における能動的サイバー防御法の対応

2025年5月に成立した「重要電子計算機に対する不正な行為による被害の防止に関する法律」および「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律」（以下、総称して能動的サイバー防御法）が、2026年10月1日に施行されます。この法律は基幹インフラへのサイバーセキュリティ対策を欧米主要国と同等の水準に引き上げることを目的としており、クレジットカードインフラもその対象に含まれます。

■経済安全保障推進法との関係

能動的サイバー防御法において「基幹インフラ事業者」とは、経済安全保障推進法に基づき各主務大臣が個別に指定する「特定社会基盤事業者」を指します。電気・ガス・石油・水道・鉄道・航空・電気通信・放送・郵便・金融・クレジットカードなど15分野が対象となっており、2026年4月時点で計257社が指定されています。クレジットカード分野では、登録包括信用購入あっせん業者（イシュア）のうち、会員数1,000万以上かつ年間信用供与額が4兆円以上である者とされています。2026年4月時点で該当するイシュアは9社ですが、後述の通りそれ以外の事業者にも関係する可能性があります。

経済安全保障推進法には重要インフラの設備導入時に事前審査を行う「基幹インフラの安全性確保」の枠組みがあります。能動的サイバー防御法はこの既存の枠組みを基盤としつつ、新たに「特定重要電子計算機」の届出義務とインシデント報告義務を上乗せするかたちで構成されています。つまり、すでに経済安全保障推進法の対象として指定されている事業者が、そのまま能動的サイバー防御法の義務対象となる構造です。

■クレジットカード業界における特定重要電子計算機

能動的サイバー防御法で新たに導入される「特定重要電子計算機」とは、「特定重要設備の機能の停止または低下をもたらすおそれがある電子計算機」（同法第9条第1項）と定義されます。すなわち、資産届出およびインシデント報告の対象となる「特定重要電子計算機」には、特定重要設備そのものが含まれるほか、それを取り巻く周辺機器も新たに対象となります。

■経済安全保障推進法における特定重要設備

経済安全保障推進法においてイシュアの特定重要設備は、省令により以下の6種類が示されています。

＜イシュアの特定重要設備＞

システムの種類	説明
会員管理システム	カード利用者情報を一元管理する基幹業務系
取引認証システム	ACS・トークンサービスプロバイダ等、EMV 3Dセキュアの中核設備
決済電文受理システム	加盟店からの承認要請の受送信
不正利用検知システム	不正利用を検知する設備 ※利用履歴の確認機能のみを持つ設備は対象外
信用照会システム	オーソリゼーションを行う設備
代行信用照会システム	信用照会システム停止時のバックアップ系

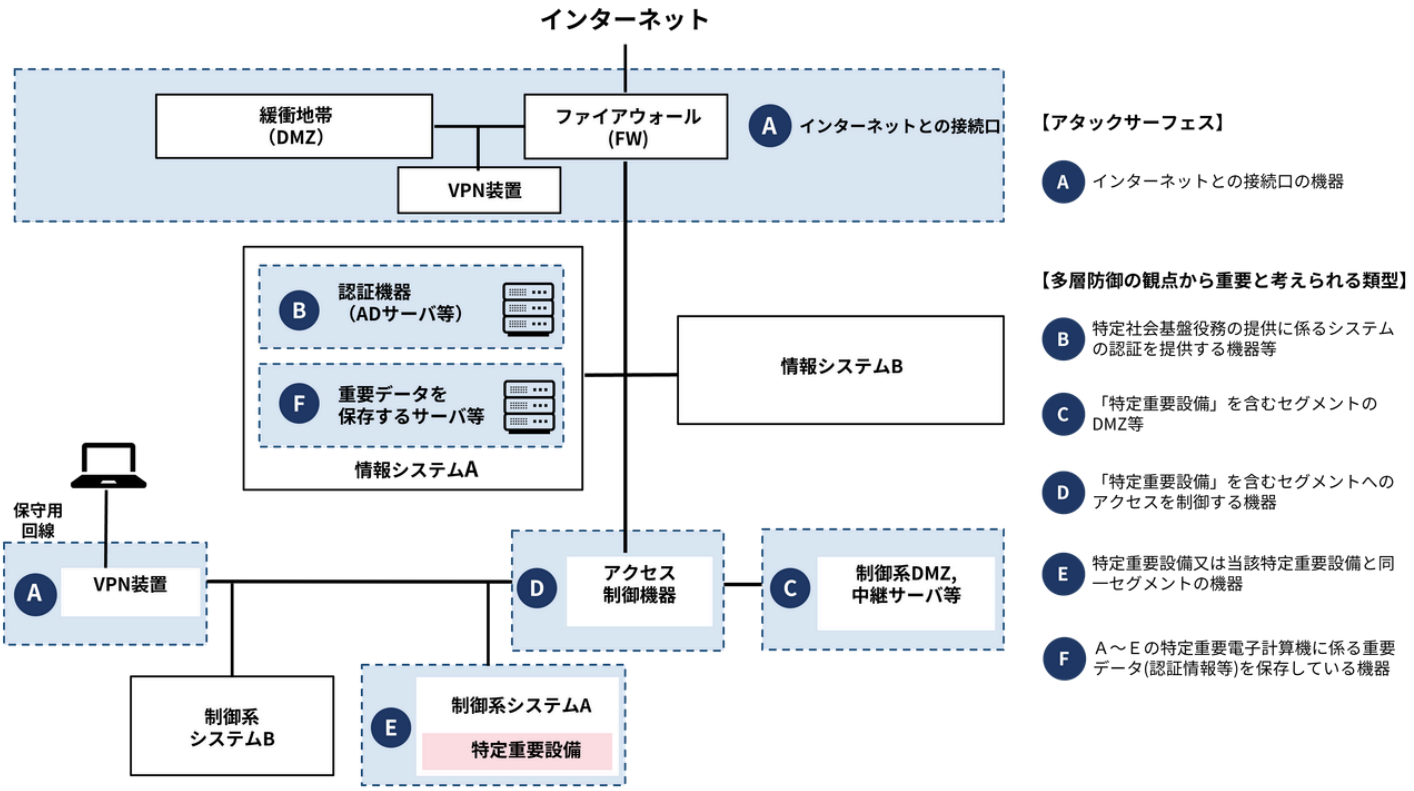
出所：『包括信用購入あっせんの業務を行う事業における経済安全保障推進法の 特定社会基盤役務の安定的な提供の確保に関する制度の解説』（経済産業省）を元に作成
※1 ACS（Access Control Server）：EMV 3Dセキュアにおいて、カード会員の本人認証を実施し、認証結果を返すシステム
※2 トークンサービスプロバイダ：実際のカード番号を安全なトークンに置き換えて管理し、決済時のカード情報漏えいリスクを低減するサービス提供事業者

なお、取引認証システムおよび代行信用照会システムについては、OS・ミドルウェア・サーバーは構成設備に含まれません。

■特定重要電子計算機の6類型

一方で能動的サイバー防御法における特定重要電子計算機の届出対象としては、A～Fの6類型が示されています。

＜届出対象機器の考え方＞



出所：『サイバー対処能力強化法（官民連携）の施行に向けた考え方の案』（2025年12月　内閣府制作統括官（サイバー安全保証担当）を元に作成

類型Aはインターネットとの接続口（アタックサーフェス）となる機器で、グローバルIPアドレスが割り当てられたファイアウォールやVPN装置が該当します。対して、B、C、D、Fは、多層防御の観点から重要と考えられる類型です。類型Eが特定重要設備そのものおよび同一セグメントにある機器となり、類型Dは特定重要設備へのアクセスを制御する機器、類型Cは特定重要設備を含むセグメントのDMZ（※）となります。類型Bはこれらのシステムの認証を提供する機器、類型FはA～Eに係る重要データを保存している機器が該当します。イシュアにおける類型A～Fの具体的な対象は今後政省令やガイドラインで具体化されます。

※DMZ：インターネットからアクセスされるサーバーを配置し、社内ネットワークを外部の脅威から保護するための中間ネットワーク領域

■届出事項とインシデント報告

資産届出で求められる届出事項は、機器の種類によって異なります。アプライアンス機器（特定用途のプログラムが組み込まれた専用機器）については、ハードウェアの製品名・製造者名を届け出ます。それ以外の汎用サーバー等については、ハードウェア名の届出は不要で、ソフトウェア（アプリケーション・ミドルウェア・OS）の製品名・製造者名が届出事項となります。これは、政府として脆弱性情報を把握・提供するうえでソフトウェア情報が重要であるためです。クラウドサービスを利用している場合は、サービス名および提供者名を届け出ます。ただし、特定重要設備がクラウドサービスを利用して実装されている場合は、製品名と製造者名の届出も必要となります。

届出のタイミングは、新規導入から4か月以内が原則です。ただし施行時点で既に導入済みの機器については、施行から6か月以内（初回届出期限：2027年4月1日想定）に届け出ればよいとされています。また、届出事項に変更が生じた場合も、変更日から4か月以内の届出が求められます。

インシデント報告については、特定重要電子計算機において以下の3つの事象の痕跡を認知した場合に報告義務が生じます。①不正指令電磁的記録（マルウェア）が実行可能な状態に置かれた場合、②不正アクセス行為が行われた場合、③サイバーセキュリティを害することによる業務妨害が行われた場合です。

特に特定重要設備等については、サイバー攻撃による機能停止・低下に至る可能性が特に大きいことから、上記の痕跡を認知した場合に加え、それらに繋がるおそれのある事象についても報告対象となります。報告は、認知後速やかに速報を、その後30日以内に詳報を提出する2段階方式が想定されており、いずれも報告時点で把握している事項のみの届出で足ります。報告先は事業所管大臣および内閣総理大臣の両者です。

なお、能動的サイバー防御法の施行に先立ち、2025年10月1日より統一報告様式の先行運用がすでに開始されています。国家サイバー統括室は同年5月28日の関係省庁申合せに基づき、DDoS攻撃およびランサムウェアの2種類の共通様式を公表しました。報告対象となるインシデントの種類はMITRE ATT&CK（※）等のフレームワークも参考に、今後整備予定のガイドラインに追加されます。能動的サイバー防御法に基づくインシデント報告において求められる攻撃技術情報の記載事項は、この共通様式に準拠する形で整理される予定です。報告窓口の一元化と様式の統一により、被害組織の報告負担の軽減が図られています。

※MITRE ATT&CK：実際のサイバー攻撃事例をもとに整理された、攻撃者の行動パターン（戦術・技術）を体系化したナレッジベース。セキュリティ対策の評価や、攻撃の検知・分析に広く利用されている。（ATT&CK = Adversarial Tactics, Techniques, and Common Knowledge）

■能動的サイバー防御法の位置づけ――「先制攻撃できる法律」という誤解

能動的サイバー防御法は、しばしば「攻撃者のサーバーに先制攻撃できる法律」と紹介されますが、基幹インフラ事業者の立場から見ると、この表現は若干実態とは異なります。

法律は①官民連携、②通信情報の利用、③アクセス・無害化措置、④組織・体制整備の4つの柱で構成されており、「先制攻撃」に相当するアクセス・無害化措置は③に該当します。これは警察・自衛隊が攻撃者のサーバーに限定的にアクセスし無害化する権限を定めたものですが、実施にあたっては独立機関であるサイバー通信情報監理委員会の事前承認が必要であり、警察・自衛隊が独自の判断で動くわけではありません。

基幹インフラ事業者に直接課される義務は①官民連携の部分、すなわち資産届出・インシデント報告・協議会への参加です。事業者の役割はあくまで自社システムへの攻撃情報を政府に共有することです。その情報を含む複数の情報源をもとに政府が総合的に判断し、必要に応じて独立機関の承認を経たうえでアクセス・無害化措置が実施されます。資産届出とインシデント報告は、能動的サイバー防御において基幹インフラ事業者が担う役割の中核であり、国全体のサイバー防衛能力を支える情報インフラの一翼を担うものです。

■協議会の設置と脆弱性対応

能動的サイバー防御法は官民間の情報共有をさらに促進するため、「情報共有及び対策に関する協議会」の設置を定めています。内閣総理大臣が関係行政機関の長とともに設置するこの協議会には、基幹インフラ事業者やシステムベンダー等が同意のうえで構成員として参加します。構成員には守秘義務を伴う被害防止情報が共有されるとともに、必要に応じて情報提供を求めることも可能とされています。

また、政府が特定重要電子計算機に用いられる機器やプログラムの脆弱性を認知した場合、事業所管大臣はそのベンダー等に対して必要な措置を講ずるよう要請できる規定も設けられています。これはシステムを構築・提供するベンダーやサービスプロバイダーにとっても直接的な関わりが生じる点です。自社製品が特定重要電子計算機に用いられている場合には、政府からの要請に応じられる体制をあらかじめ整えておくことが求められます。

■今後に向けた対応

本レポート執筆時点（2026年6月）では、クレジットカード業界における具体的な特定重要電子計算機の範囲を定める省令が確定していませんが、2026年10月の法施行に向け各事業者が準備を進める必要があります。

① イシュア（特定社会基盤事業者として指定されている事業者）

直接の義務主体として最も広範な対応が求められます。まず優先すべきは、インシデント報告体制の整備です。資産届出の初回期限（2027年4月1日想定）より前に、インシデント報告義務が施行日（2026年10月1日）から開始されるためです。報告先は事業所管大臣（経済産業大臣）および内閣総理大臣の両者であり、インシデント認知後速やかに速報を、30日以内に詳報を提出できる社内フローを確立しておく必要があります。並行して、特定重要設備6種を起点に特定重要電子計算機A〜F類型に該当し得るシステム・機器の棚卸しを進め、届出対象の候補を絞り込んでおくことで、省令確定後の対応を迅速に行えます。

② システムベンダー・SIer・クラウドサービス事業者

基幹インフラ事業者のシステムを構築・運用する立場として、届出対象となり得る機器の製品名・製造者名・ソフトウェアバージョン情報を整理・提供できる体制を整えておくことが求められます。また、特定重要電子計算機に脆弱性が発見された場合、事業所管大臣からベンダーに対して必要な措置を講ずるよう要請が行われる規定が法律上設けられています。自社製品・サービスが対象となった場合の対応フローをあらかじめ検討しておくことが重要です。

③ PSP（決済代行事業者）

クレジットカード取引においてPSPはアクワイアラと加盟店の間に位置しており、イシュアとは直接接続しない構成が一般的です。現時点で省令に定められているクレジットカード分野の特定重要設備6種はいずれもイシュイング機能に関するものであるため、PSPのシステムが特定重要電子計算機に該当する可能性は現時点では低いと考えられます。ただし、今後の省令改正や業態別の政省令の内容によっては状況が変わる可能性もあるため、動向を注視しておくことが望ましいといえます。

>>> 2. ECにおける不正利用の概況（2026年1-３月）

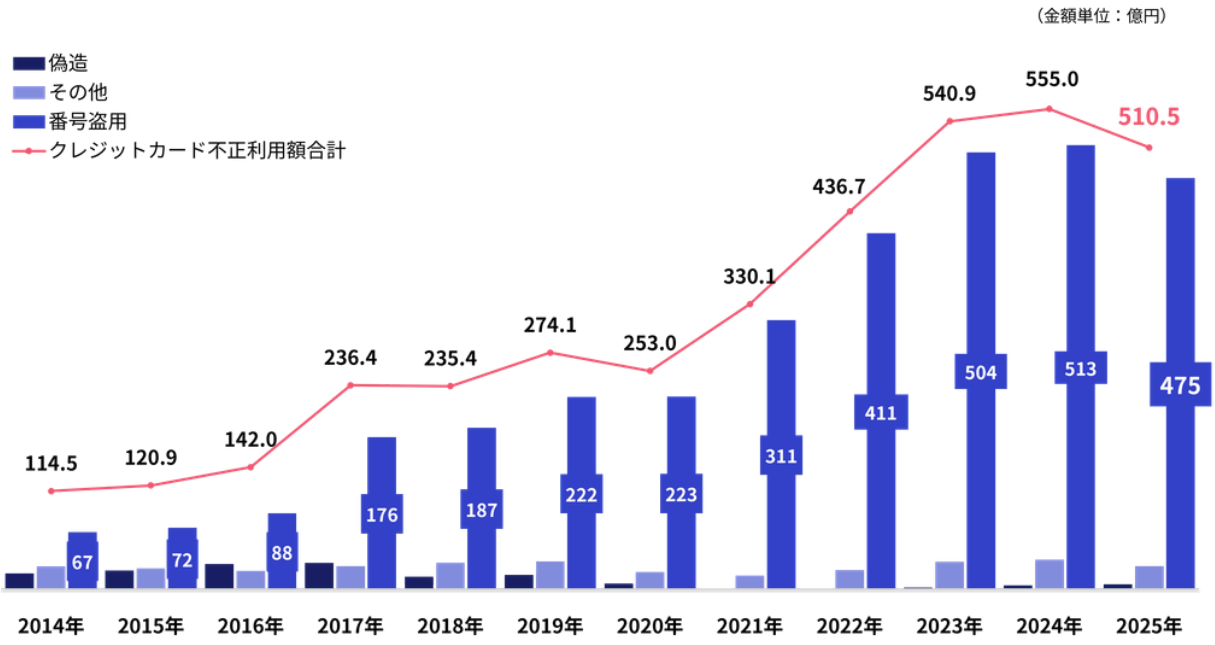
（1） クレジットカード不正利用被害額の推移

2026 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　113.6億円
- 偽造　1.5億円
- 番号盗用　106.0億円
- その他　6.1億円
- クレジットカード不正利用発生率　0.033%

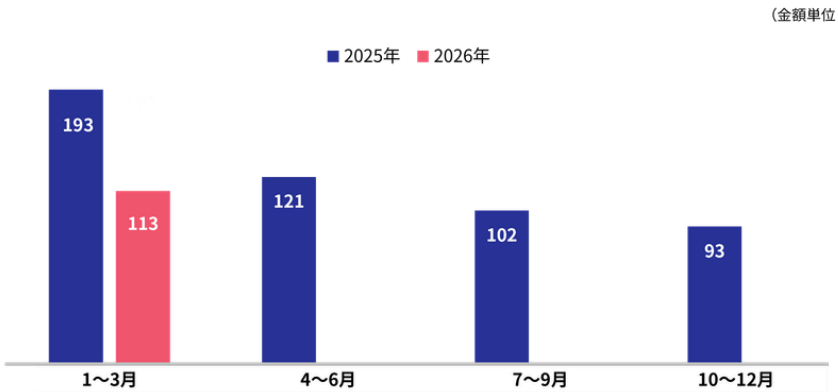
※日本クレジット協会調べ
https://www.j-credit.or.jp/information/statistics/index.html

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

2026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
2026年	偽造	1.5			
	番号盗用	106.0			
	その他	6.1			
	合計	113.6			
	不正利用発生率	0.033%			
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
	不正利用発生率	0.059%	0.036%	0.030%	0.027%

（『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6月

2026年第1四半期（1～3月期）のクレジットカード不正利用被害額は113.6億円となり、前年同四半期と比較すると約41%減となりました。特に、番号盗用（なりすまし）の被害が182.9億円から106.0億円と大幅に減少しており、国内のEMV 3Dセキュア導入義務化の効果が現れていると考えられます。一方で、クレジットカード不正利用発生率は0.033%と前年同四半期に比べると低下しているものの、前四半期である2025年第4四半期（10～12月期）に比べると増加（0.027%→0.033%）に転じており注意が必要です。

なお、2025年9月の『割賦販売法（後払い分野）に基づく監督の基本方針』（経済産業省）の改正を受け、2026年第1四半期（1～3月期）から調査方法が変更されています。変更点は以下の2点です。

1. 四半期調査の調査対象拡大

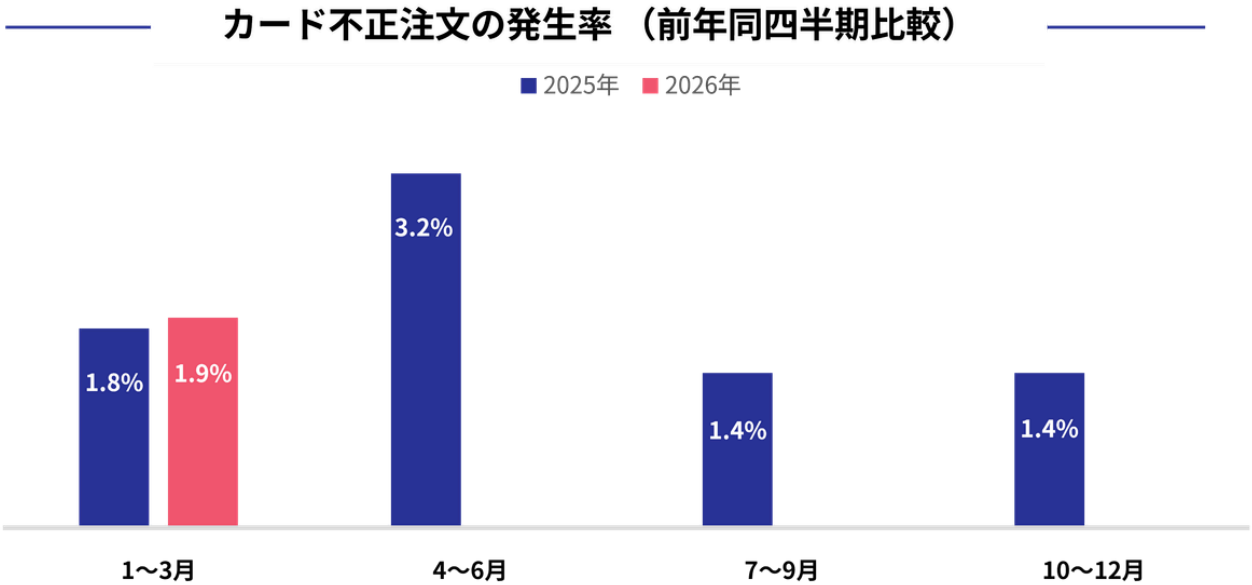
従来は主要イシュア40社を調査対象としていましたが、48社に拡大されました。また、調査対象となる基準が「包括信用購入あっせん業者であり、かつクレジットカード発行枚数100万枚以上であること」と明示され、毎年見直しが行われることになりました。ただし、調査継続性の観点から、一度調査対象となったイシュアは発行枚数が基準を満たさなくなった場合も引き続き調査対象となります（イシュアを廃業した場合を除く）。

2. 年次調査の新設

2026年以降、従来の調査とは別に、全てのイシュアを対象とした年次調査が行われます。調査対象期間は1月から12月の通年となり、取りまとめ結果として年次の不正利用被害額と不正利用発生率が翌年3月末に公表されます。

（2）ECサイト不正利用の傾向

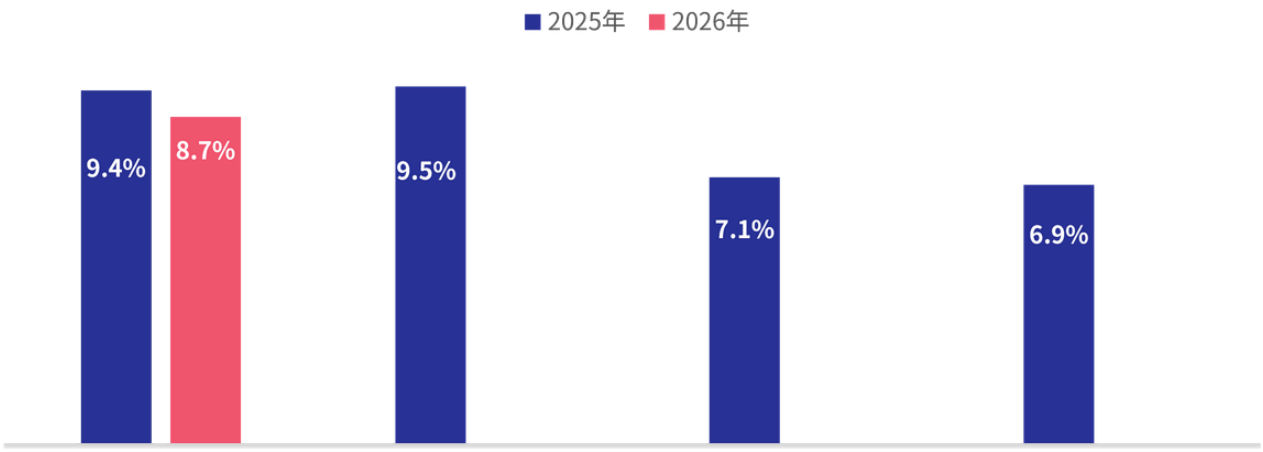
【調査方法】
不正注文検知サービス「O-PLUX Payment Protection」（Caccoが提供する不正検知サービス）をご利用のお客様（累計12万サイト以上）における審査結果をもとに集計



	1～3月	4～6月	7～9月	10～12月
2026年	1.9%			
2025年	1.8%	3.2%	1.4%	1.4%

※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6月4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
2026年	8.7%			
2025年	9.4%	9.5%	7.1%	6.9%

※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6月4日時点で集計

2026年1-3月期におけるカード不正注文の発生率は1.9%となりました。前年同期（2025年1-3月期）の1.8%と比較すると0.1ポイントの微増となり、ECサイトにおけるクレジットカードの不正利用リスクは、引き続き横ばいで推移していると言えます。

一方、2026年1-3月期における転売不正注文の発生率は8.7%となりました。前年同期（2025年1-3月期）の9.4%と比較すると0.7ポイントの減少が見られますが、2025年10-12期の6.9%と比較すると1.8ポイントの増加となっています。全体の注文に対する割合としては依然として9%弱を占めており、カード不正利用（1.9%）と比較しても高い割合となっています。

商材別ランキングでは、前回（2025年10-12月期）トップの「イベント」を抑え、「健康食品・医薬品」（前回6位）が1位となりました。前回圏外だった「チケット（航空・鉄道）」が3位に急上昇しています。この期間は年度末の帰省ラッシュや春休みの旅行シーズンを含んでおり、交通機関のチケットは、即座に高値で現金化したいという不正者側の狙いと合致する商材であるという理由が考えられます。前回8位の「PC・タブレット・家電」が4位となっています。

＜不正注文に狙われやすい商材ランキング＞

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

2026年（1-3月） 商材別 不正注文検知数ランキング			
1位	健康食品・医薬品	7位	ホビー・ゲーム
2位	イベント	8位	アパレル
3位	チケット（航空、鉄道）	9位	コスメ・ヘアケア
4位	PC・タブレット・家電	10位	日用品・雑貨・キッチン用品
5位	デジタルコンテンツ	11位	食品・飲料・酒類
6位	スポーツ用品	12位	総合通販

※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6月4日時点で集計

（3）不正利用のトピック

コード決済を悪用した返金詐欺　消費生活センターへの相談が過去最多に

近年、ECサイトにおけるクレジットカードの不正利用対策が急速に進む一方で、決済手段の盲点を突いた脅威が急増しています。それが、コード決済（QRコード決済、バーコード決済）アプリを悪用した不正手口です。国民生活センターの発表によると、全国の消費生活センターに寄せられたこの手口に関する相談件数は、2025年4月から11月末までの8ヶ月間で過去最多の5,107件に達しています。統計を取り始めた2023年度（通期）と比較すると約2.3倍に急増しています。コード決済アプリの仕組みを悪用した手口と詐欺が成功しやすい理由を解説します。

■「コード決済で返金する」と騙す、返金詐欺の巧妙な手口

この詐欺の最大の特徴は、犯人が「ECサイトのサポート窓口」になりすまして購入者に接触してくる点にあります。主な流れは以下の通りです。

1. 偽の「欠品・キャンセル通知」から始まる接触

犯人は、相場よりも安価に人気商品やブランド商品などを販売する偽ECサイトを作り、SNS広告やフィッシングメールで集客します。広告から誘導されて偽サイトにアクセスした消費者がそこで商品を注文すると、犯人から「注文された商品が欠品したため、代金を返金します」といったメールやSMSが届きます。

2. 「コード決済での返金」へ誘導

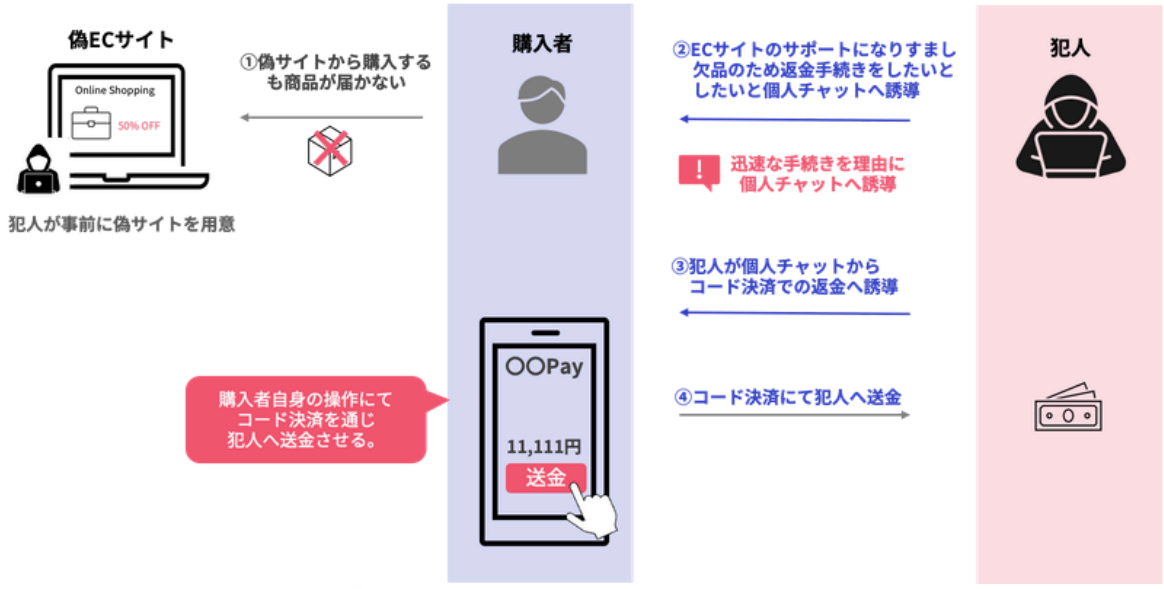
犯人は「手続きを迅速に行うため、銀行振込ではなく〇〇ペイ（コード決済）で返金します」と持ちかけ、購入者を言葉巧みにLINEなどの個人チャットへ誘導します。

3. 「返金」ではなく「送金」をさせる操作を誘導

犯人はLINEなどのチャットで会話をしながら、購入者に「今から言う手順通りにアプリを操作してください」と指示を出します。スマホの画面共有アプリをインストールさせ、購入者のスマホの実際の画面をリアルタイムに確認しながら誘導するケースもあります。指示によって、購入者の本来の目的である「返金手続き」ではなく、実際には個人間送金機能を利用して「犯人へ送金させる手続き」を行わせ、最終的に購入者自身の手で犯人へ送金させてしまいます。

個人間送金機能は、本来は友人同士で割り勘や送金をするための便利な機能ですが、これを悪用した手口です。銀行振込とは異なり、手続きをした瞬間にリアルタイムでお金が相手（犯人）に移動し、即座に引き出されたり別のアカウントへ分散されたりするため、一度送金してしまうと被害金を回収することが極めて困難になります。

＜コード決済を悪用した返金詐欺の流れ＞



■正規のECサイトやメーカーにも被害が及ぶ

購入者が偽サイトを正規のECサイトやメーカーの運営するサイトと誤認していた場合、被害はそちらにも及びます。「自分が利用したECサイト（またはその事業者）が詐欺を働いた、あるいは情報漏洩した」と誤解した購入者のクレームへの対応に時間を取られます。また、商品やショップのレビュー、SNSなどに悪評が書き込まれ、ブランド価値に致命的なダメージを受けます。

■なぜ、この「返金詐欺」が成立するのか

その理由は大きく2つあります。

- **購入者の心理的な隙を突きやすい：** 「買い物をしたECサイトから欠品の連絡が来る」ということ自体は、通常のネットショッピングで起こり得ます。そのため購入者が警戒心を抱きにくく、さらに「早く返金してほしい」という心理に付け込むことで、多少不自然な操作であっても指示通りに動かされてしまいます。

- **正規のECサイトのセキュリティを迂回する手口：** この手口は、そもそも偽ECサイトから注文した消費者に対し、犯人が「返金手続き」という購入後のコミュニケーションを装って金銭を詐取する詐欺です。正規のEC事業者にとっては、どれだけ自サイトの不正利用対策（EMV 3Dセキュア、不正検知システムなど）を強化しても、自社のシステムと接点のないところで行われる行為を防ぐことは困難です。

■EC事業者が今すぐ行うべき対策

EC事業者は、自社と消費者を守るために以下のような対策を検討する必要があります。

1. **購入者への事前の注意喚起：** 「当ショップからの返金手続きにおいて、〇〇ペイなどのコード決済を使った送金指示や、LINEでの個別誘導を行うことは一切ありません」という警告文を、購入完了画面やメルマガ、マイページに目立つように掲載します。
2. **偽広告の発見・通報窓口の整備：** 偽ECサイトの入口となるのが、SNS広告やフィッシングメールです。自サイトを騙る偽サイトや、自社の取扱商品を極度に安く販売するような、詐欺と疑わしい広告をいち早く発見して掲載を差し止めたり、消費者に注意喚起します。消費者が詐欺の被害にあうことや、悪評によるブランド価値の毀損を防止することができます。主要なSNSを定期的に確認し、疑わしい広告を広告事業者に対し通報する、自社と紛らわしい怪しい広告やメールを通報できる窓口を整備し、サイトのトップページなどわかりやすいところに記載するといった対策を実施します。

利便性の高いツールが普及する裏で、その仕組みの隙を狙った手口は常に変化しています。EC事業者側も、購入から決済までだけではなく、購入前、購入後の顧客コミュニケーションまで見据えたセキュリティ意識を持つことが求められています。

3. 政策の動向

サプライチェーン強化に向けたセキュリティ対策評価制度の概要

2026年3月27日、経済産業省および内閣官房国家サイバー統括室は、『サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針』（SCS評価制度の構築方針）を公表しました。2025年12月に公表された方針案へのパブリックコメントを経て成案化されたもので、本方針に基づき、2026年度末頃の制度開始を目指した取組が進められています。カード情報や個人情報を扱うキャッシュレスサービスは、サプライチェーン攻撃の標的になりやすい構造を持ちます。本制度は、イシュア・アクワイアラ・コード決済事業者・PSP（決済代行事業者）・加盟店といった各プレイヤーとその取引先に影響を及ぼす可能性があります。以下では、制度の概要と各事業者が今から取り組むべき準備のポイントを整理します。

■制度創設の背景

近年、セキュリティ対策が強固な大企業を直接狙うのではなく、取引関係にある中小企業を踏み台にして侵入する「サプライチェーン攻撃」が急増しています。IPAが毎年公表する「情報セキュリティ10大脅威」においても常に上位に位置づけられており、社会全体にとって看過できない脅威となっています。キャッシュレスサービスにおいても、加盟店管理業務を担うPSPや決済システムの開発・運用を担うSIerといった周辺事業者が侵入口となるリスクは現実のものとなっており、業界全体でのセキュリティ底上げが急務となっています。

こうした状況を受け、経済産業省および内閣官房国家サイバー統括室は、サプライチェーンにおける各企業が満たすべきセキュリティ対策を提示しつつ、その対策状況を可視化する仕組みの構築に向けた検討を進めてきました。その結果として公表されたのがSCS評価制度です。

■制度の目的と位置づけ

本制度は、企業のサイバーセキュリティ対策状況を客観的な基準で評価し、可視化する仕組みです。対象範囲はサプライチェーンを構成する企業等のIT基盤（メールサーバー・Webサーバー等の公開サーバーや認証基盤、エンドポイント機器、クラウドサービスを含む）です。製造環境等の制御（OT）システムや発注元に提供する製品等は原則として対象外とされています。これにより、企業は自社の対策レベルを取引先に明確に示せるようになり、取引先選定の新たな指標となることが期待されています。

現時点では、評価を受けるかどうかは任意ですが、今後、大企業が取引条件として第三者による評価を求めたり、将来的に必須化されたりする可能性も考えられます。PSPなどキャッシュレス決済に関わる事業者にとっては、PCI DSSによるカード情報保護に加え、SCS評価制度への対応が「取引継続の条件」として実質的に機能する場面が今後増えていくことが推測されます。

■評価レベルの体系（★1〜★5）

本制度では、企業のセキュリティ対策の実施状況を★3・★4・★5の3段階で可視化します。★3は「すべてのサプライチェーン企業が最低限実装すべきセキュリティ対策」、★4は「サプライチェーン企業が標準的に目指すべきセキュリティ対策」、★5は「サプライチェーン企業が到達点として目指すべき対策」と位置付けられています。

＜段階別評価の概要＞

評価レベル	★3	★4	★5
想定される脅威	広く認知された脆弱性等を悪用する**一般的なサイバー攻撃**	• **供給停止**等によりサプライチェーンに**大きな影響**をもたらす企業への攻撃 • 機密情報等、**情報漏えい**により**大きな影響**をもたらす資産への攻撃	**未知の攻撃**も含めた、**高度なサイバー攻撃**
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべきセキュリティ対策**として、**基礎的な組織的対策とシステム防御策**を中心に実施	サプライチェーン企業が**標準的に目指すべきセキュリティ対策**として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等**包括的な対策**を実施（**実地審査および技術検証を含む評価**によって対策実施状況の確認を行う）	サプライチェーン企業等が**さらに目指すべき高度な対策**として、**国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した**上で、**システムに対しては現時点でのベストプラクティスに基づく対策**を実施
脅威に対する達成水準（イメージ）	• **組織内の役割と責任**が定義されている。 • 一般的なサイバー脅威への対処を念頭に、**自社IT基盤**への初期侵入、侵害拡大等への対策が講じられている。 • インシデント発生時に、**取引先を含む社内外関係各所への報告・共有に必要な最低限の手順が定義、実施**されている。	• **取引先のシステムやデータを含む内外**への被害拡大や攻撃者による目的遂行のリスクを低減する対策が講じられている。 • **事業継続に向けた取組や取引先の対策状況の把握**など、自社の位置付けに適合した**サプライチェーン強靭化策が講じられている。**	• 組織において**国際規格等に基づくマネジメントシステム**が確立されている。 • **リスクを適宜適切に把握**した上で、インシデントに対して迅速に検知・対応するなど、**ベストプラクティスに基づくサイバーレジリエンス確保策**が講じられている。 • 取引先への指導や共同での訓練の実施など、**自社サプライチェーン全体の対策水準向上に資する対策**が講じられている。
要求事項数	26件	43件	今後検討することを想定
評価スキーム	**専門家確認付き自己評価**	**第三者評価**	**第三者評価**
有効期間	1年	3年	今後検討することを想定

出所：『サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針』（経済産業省／内閣官房国家サイバー統括室）2026年3月

なお、★1・★2は既存のIPA（独立行政法人情報処理推進機構）が運営するSECURITY ACTION制度における自己宣言・自己点検ベースの枠組みに相当し、専門家の確認や第三者評価を伴わない自己宣言にとどまります。本制度の開始により、専門家の確認や第三者評価を伴う★3以上の取得が取引上の実質的な基準となると見込まれます。

■★3・★4の評価スキーム

本制度のセキュリティ要求事項は、NISTのサイバーセキュリティフレームワーク（CSF）の6分類（統治／識別／防御／検知／対応／復旧）に「取引先管理」を加えた7分類で構成されています。IT資産の把握、多要素認証などのアクセス管理、バックアップ、マルウェア対策、インシデント発生時の対応手順、委託先の管理といった「セキュリティ対策の基本」が網羅されています。

★3については、取得希望組織が26項目の要求事項について自己評価を行い、その内容についてセキュリティ専門家の確認・助言を受ける方式が想定されています。有効期間は1年間の想定です。

★4については、★3に加えて取引先企業の管理、システムへの侵入検知、インシデント対応など包括的な対策を加えた43の要求事項について、認証を受けた評価機関が第三者評価を行います。有効期間は3年間です。

★5については、2026年3月現在で評価基準や評価スキーム等の検討が行われている段階です。今後、ISMSなど既存の認証、評価制度との整合性を取りながら詳細が決定される予定です。

■スケジュール

★3および★4レベルは2026年度末頃（2027年1～3月頃）の申請受付開始が予定されており、多くの企業にとって対応が急務となっています。一方で、★5の開始時期については引き続き検討が進められる予定です。

■今後に向けた対応

本制度は現時点で任意ですが、クレジットカードなどキャッシュレス業界の構造上、上位事業者からの要請が下位事業者へと波及するスピードは速いと考えられます。事業者の立場ごとに、以下のような対応が求められます。

① イシュア

自社システムへの対応に加え、SIer、決済ネットワークやクラウドサービス事業者に対して委託者としてSCS評価取得の対応を求める立場となります。前述の通り、能動的サイバー防御法の特定社会基盤事業者にも該当しうることから、両制度への対応を並行して進める必要があります。調達・委託基準へのSCS評価の組み込みと、取引先への周知・支援体制の整備が急務です。取引先への対応要請にあたっては、経済産業省・公正取引委員会が整理した独占禁止法・下請法上の考え方を確認したうえで進めることが重要です。

② アクワイアラ

自社が委託するSIerやクラウドサービス事業者に対しては委託者としてSCS評価取得を求める立場である一方、加盟店からはサービス提供事業者として取得を求められる可能性がある二重の立場に置かれると考えられます。 本制度への対応は任意ですが、7分類の要求事項に対するギャップ分析と規程・記録の整合を今から進めておくことが、制度開始後の対応を円滑にする近道です。

③ コード決済事業者・PSP（決済代行事業者）

加盟店から決済処理を受託する受託者として、取引先からSCS評価取得を求められる可能性が高い立場です。同時に、自社が委託するSIerやクラウドサービス事業者に対しては委託者として取得を求める立場にもなります。加盟店のカード情報非保持化を支援するインフラとしてサプライチェーン上の重要な位置を占めており、SCS評価取得が取引継続の実質的な条件となる場面が今後増えていくと見込まれます。

④ SIer・クラウドサービス事業者

決済システムの構築・運用を担う受託者として、複数の取引先からSCS評価取得を求められる典型的な立場です。顧客企業のSCS評価取得を支援する立場としても、自社の提供サービスが、どの要求事項に対応しているかを整理するとともに、顧客への技術支援・証跡提供なども可能な体制を整えておくことが求められます。

⑤ 加盟店

決済処理をコード決済事業者やPSPに委託するだけでなく、ECサイトやPOSシステムの構築・運用をSIer・ベンダーに委託する立場でもあります。★4の要求事項では「重要な取引先のセキュリティ対策状況の把握」が求められており、一定規模以上の加盟店にとっては対応が必要になる場面が生じ得ます。またECモール事業者は、顧客に提供しているECプラットフォームが本制度の適用範囲に該当する可能性があり、SCS評価取得主体としての側面も出てきます。

一方、自社IT基盤をほぼ持たない中小規模の加盟店については、利用するPSPやクラウドサービスなど委託先のSCS評価取得状況の確認が対応の出発点と考えられます。

【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）