



Cashless Security Report Annual Report 2026

2026年10月9日
かっこ株式会社
株式会社リンク

目次

はじめに	1
1. 2025年のカード情報流出事件の概況	3
(1) カード情報流出事件数・流出件数の推移	3
(1)-1. 年次推移	3
(1)-2. 四半期別推移	5
(2) カード情報流出事件の傾向	5
(2)-1. 業種/取扱い商材別・情報流出期間別事件	5
(2)-2. カード情報窃取の手口：オンラインスキミングが引き続き大半を占める	7
(3) 2025年のカード情報流出事件のトピック	9
(3)-1. ランサムウェア攻撃によるカード情報流出とランサムウェア対策	9
2. 2025年のカード不正利用の概況	11
(1) クレジットカード不正利用被害額の推移	11
(1)-1. 2025年のクレジットカード不正利用額と傾向	11
(1)-2. 年間500億円超の高止まりが続く要因と今後の課題	12
1. 本人認証を迂回した不正利用へのシフト	12
2. 中間者攻撃の増加	12
3. アカウント乗っ取り（ATO）やbotの増加	13
4. 今後の課題	14
(2) ECサイトにおける不正注文の傾向	15
(2)-1. ECにおけるクレジットカード不正利用発生率及び転売不正発生率の傾向	15
1. ECにおけるクレジットカード不正利用発生率と転売不正発生率の推移	15
2. 不正に狙われやすい商材ランキング	16

(2)-2. クレジットカード不正利用における注文金額の低額化	17
1. 1万円未満の不正注文割合が2025年には約30%まで上昇	17
2. クレジットカード不正利用における注文金額が低額化する背景と要因	17
3. 低額取引についてEC事業者に求められる対策	18
(2)-3. EC事業者の不正注文対策状況とEMV 3-Dセキュアの導入率	18
1. EMV 3-Dセキュアの導入率	18
2. 年商規模における不正注文対策の実態	19
3. EMV 3-Dセキュア導入に伴う現場の課題：カゴ落ちと決済承認率の低下	20
4. 今後のEC事業者に求められる対策：EMV 3-Dセキュア運用パターンの最適化	21
(3) カード決済承認率改善の取り組み	22
(3)-1. EMV 3-Dセキュア導入後のカード承認率低下と対策による改善効果	22
1. EMV 3-Dセキュア導入前後の決済承認率の変化	22
2. カード決済承認率低下の要因	22
3. 承認率改善対策の効果	23
(3)-2. ジュエリーブランドECサイトにおける決済承認率改善事例	24
(4) カード不正利用のトピック	25
(4)-1. なりすまし広告を入り口とした本人認証の悪用による不正利用	25
(4)-2. 集客フェーズに潜むもう一つの脅威：アドフラウド（広告不正）	28
3. その他のキャッシュレスセキュリティのトピック	30
ニセ社長詐欺：メッセージングアプリを利用するビジネス詐欺の手口	

4. 制度・政策の動向 34

 (1) SCS評価制度の概要と必要な対策 34

 (1)-1. 制度創設の背景 34

 (1)-2. 制度の全体像 34

 (1)-3. 対象となる組織 35

 (1)-4. 対象となる範囲 35

 (1)-5. 要求事項と評価基準の構成 36

 (1)-6. 実務上の影響が大きい要求事項 37

 (1)-7. 対応の進め方 39

 (2) 生成AIの進化とキャッシュレスセキュリティ 41

 (2)-1. 攻撃側の変化：不正の「量産化」と「精密化」 41

 (2)-2. 防御側の変化：フロンティアAIによる脆弱性対策の加速 42

 (2)-3. 新領域：エージェンティックコマースと決済の変化 44

 (2)-4. 考察 45

参考文献 46

はじめに

2026年3月に経済産業省が公表したデータによれば、2025年のキャッシュレス決済比率は58.0%（162.7兆円）となった。なお、この数値は新たに設定された「国内指標」によるものである。2025年12月に公表されたキャッシュレス推進検討会の取りまとめにおいて、従来指標の分母（民間最終消費支出）には持ち家の帰属家賃等が約57兆円（約17%相当）含まれていることから、これを除いて、より消費者実感に即した「国内指標」へと見直しが行われた。従来の指標は継続性や国際比較可能性の観点から「国際比較指標」として併用されることとなった。このため、キャッシュレスセキュリティレポート2025までに掲載してきた比率（2024年の「国際比較指標」：42.8%）とは算出基準が異なり、単純比較はできない点に留意してほしい。

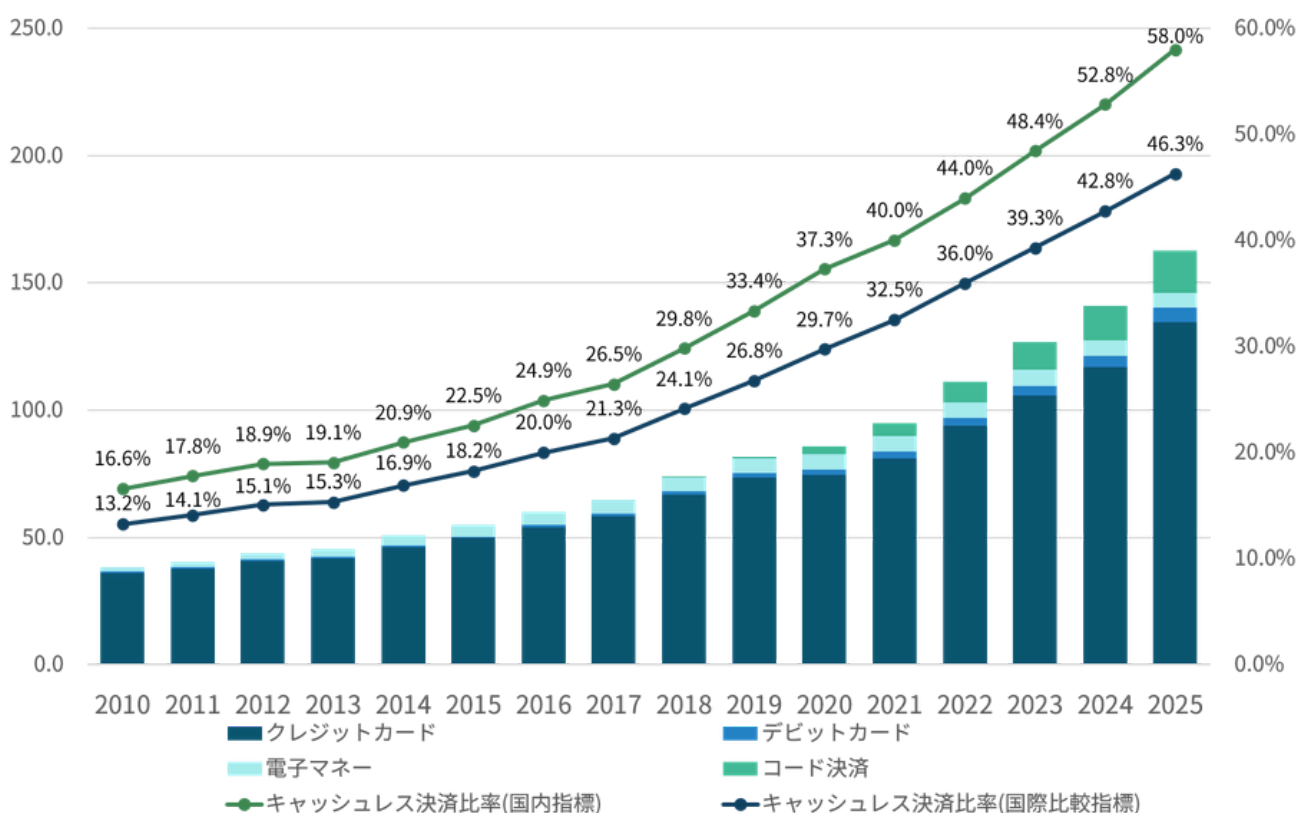
政府目標も見直された。「2025年に民間最終消費支出に占めるキャッシュレス決済比率40%」という従来目標を前倒しで達成したことを踏まえ、将来的な目標であるキャッシュレス決済比率80%は「国内指標」で80%と再設定され、可能な限り早期の達成を目指すこととされた。あわせて中間目標として、2024年実績と将来目標の中間値である国内指標65%（国際比較指標で55%）を2030年までに達成することが新たに掲げられている。

【決済手段別の推移】

- ・ **クレジットカード**：クレジットカードは134.6兆円と、キャッシュレス決済額全体の82.7%を占めた。前年の116.9兆円から約17.7兆円増加し、引き続きキャッシュレス決済の主役となっている。
- ・ **デビットカード**：利用額は5.5兆円と、前年（4.4兆円）から約1.1兆円増加した。全体に占める割合は3.4%であった。
- ・ **電子マネー**：利用額は6.0兆円で、前年（6.2兆円）から引き続き減少傾向にある。全体に占める割合は3.7%と、コード決済やクレジットカードの拡大に押される構図が続いている。
- ・ **コード決済**：コード決済は16.6兆円と、前年（13.5兆円）から約3.1兆円増加し、高い成長が続いている。全体に占める割合は10.2%と初めて1割を超えた。

2025年は、クレジットカードが8割超を占める構造は変わらない中、コード決済が全体の1割を超えるなど、決済手段の多様化が一層進展した。今後は2030年の中間目標（国内指標65%）の達成に向け、さらなる利便性向上と安全性確保の両立が求められる（図1-1）。

▼図1-1 キャッシュレス決済額および比率の推移（2025年）



出所：経済産業省プレスリリース『2025年のキャッシュレス決済比率を算出しました』（2026年3月31日）

2025年のクレジットカードなどの情報流出事件は、2024年に比べると事件数・カード情報流出件数とも大幅に減少した。一方で、ランサムウェア攻撃による有効なカード情報の大量流出の可能性がある国内初の事件も発生した。カード不正利用についても、510.5億円と、2024年の555億円を下回った。2014年以降増加を続けていた不正利用被害額が10年ぶりに減少に転じたことになる。2025年3月末を期限としたEMV 3-Dセキュアなどの不正利用対策の義務化の効果が徐々に現れつつあると推測される。一方で、SNS、インターネット広告、フリーマーケットサイトなど、多様なツールを用いてカード情報の不正入手・不正利用・換金・マネーロンダリングまでを行

う、組織的な攻撃が行われるようになっている。各所での多面的なセキュリティ対策が重要となっている。

かっこ株式会社（以下 Cacco）と株式会社リンク（以下 リンク）は、カード情報流出事件の統計とECやキャッシュレスに関連する不正利用傾向に関するレポートを共同で取りまとめ、四半期ごとに公表している。『キャッシュレスセキュリティレポート2026』は、この取り組みの一環として、国内のキャッシュレスに関連するサイバー攻撃や不正利用被害の現状と対策について、両者が共同で取りまとめた年次レポートである。本レポートが安全安心なキャッシュレス社会の実現に貢献できれば幸いである。

本レポートに記載された統計、数字などの情報を引用される際は、必ず出典元として「キャッシュレスセキュリティレポート2026」（Cacco、リンク）と明記ください。出典を明記されない形での転載および複製を禁じます。

1. 2025年のカード情報流出事件の概況

(1) カード情報流出事件数・流出件数の推移

クレジットカードやブランドデビットカードなどのペイメントカード情報（以下、カード情報）流出事件に関しては業界団体や官公庁などによる統計が存在しない。Caccoとリンクは、カード情報流出事件数およびカード情報流出件数について以下の通り定義し、各社公式発表や報道をもとに独自に集計を行っている。

・**カード情報流出事件数**：カード情報流出を発生させた事業者（発表主体）による公表情報に基づき集計

▶加盟店が発表主体で、同時に複数のECサイトからカード情報が流出した場合は、流出元となったサイトごとに1つの事件として扱う。

▶ECサイトから委託を受けてカード情報を扱っていた事業者が発表主体として情報公開した場合は、公表された一連の攻撃を1つの事件として扱う。

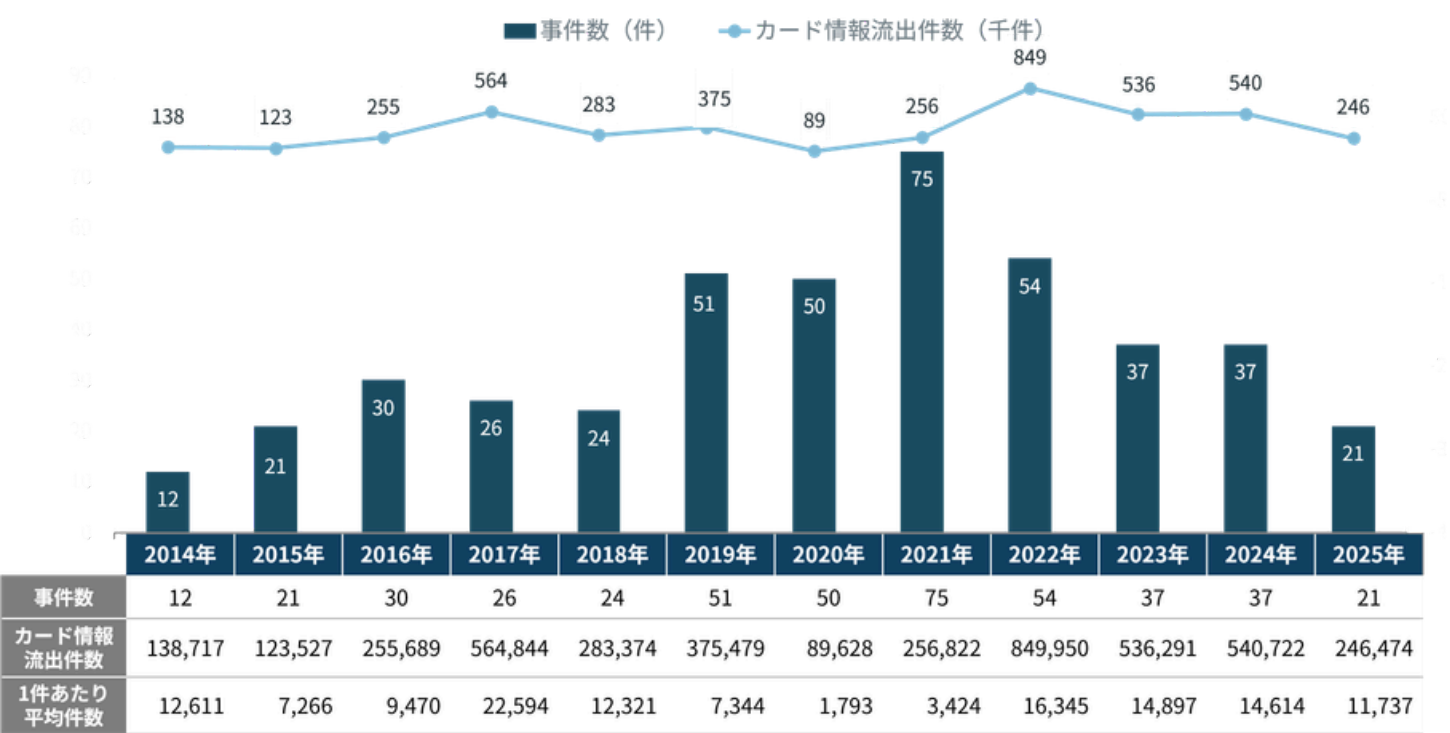
・**カード情報流出件数**：発表主体により公表された流出件数で、クレジットカード、ブランドデビットカード、ブランドプリペイドカードを含む。公開された件数のうち、最新の情報を正として集計

以下、本節で引用するデータは特に断りがない限り、Caccoとリンクの調査によるものである。（ただし2014年から2021年までのデータはf j コンサルティングによる独自調査／2022年・2023年のデータはCaccoとf j コンサルティングによる調査、2024年以降はCaccoとリンクによる調査）

(1)-1. 年次推移

2025年のクレジットカードなどのカード情報流出事件数は21件で、前年（37件）から16件、約43%減少した。カード情報流出件数は246,474件と、前年（540,722件）から約54%減少した（図1-2）。事件数・流出件数がそろって大幅に減少するのは2023年以降で初めてであり、いずれも2021年以降で最も低い水準となった。1事件あたりの平均流出件数も11,737件と、前年の14,614件から約2割減少した。

▼図1-2 国内のカード情報流出事件発生状況



※1件あたり平均件数はカード情報流出件数非公開の事件を除いたもの
Cacco・リンク調べ（2021年以前のデータはf j コンサルティング調べ）

図1-3に示す通り、最大となったのは食品（スーパーマーケット）運営A社における127,263件の流出で、年間のカード情報流出件数全体の51.6%を占めた。ECサイトの改ざんではなく、ランサムウェア攻撃によって、現在有効なカード情報が大量に流出した可能性がある国内初の事案である（詳細は「1-(3)-1. ランサムウェア攻撃によるカード情報流出とランサムウェア対策」）。

2位以下はいずれもオンラインスキミングによるもの、その可能性が高いもので、アパレル販売B社が30,712件（流出期間1,696日）、ホビー（ゲーム・玩具）販売C社が30,431件（同17日）と続いた。上位3件で年間流出件数の76.4%を占めており、少数の大規模事案が全体を大きく左右する構図は前年と変わらない。

▼図1-3 2025年カード情報流出の多かった事件

順位	取扱商材	運営企業	流出件数	流出期間（日数）	原因
1	食品（スーパーマーケット）運営	A社	127,263	1	ランサムウェア感染
2	アパレル販売	B社	30,712	1,696	オンラインスキミング（可能性高）
3	ホビー（ゲーム・玩具）販売	C社	30,431	17	オンラインスキミング
4	食品（茶）販売	D社	13,094	184	オンラインスキミング（可能性高）
5	アパレル（作業着）販売	E社	12,630	1,228	オンラインスキミング（可能性高）
6	生活雑貨（カーテン）販売	F社	10,423	390	オンラインスキミング（可能性高）
7	アパレル販売	G社	5,754	1,133	オンラインスキミング（可能性高）
8	食品（地方特産品）販売	H社	2,972	1,147	オンラインスキミング（可能性高）
9	生活雑貨販売	I社	2,460	1,151	オンラインスキミング（可能性高）
10	食品（テイクアウト）販売	J社	2,270	8	オンラインスキミング（可能性高）

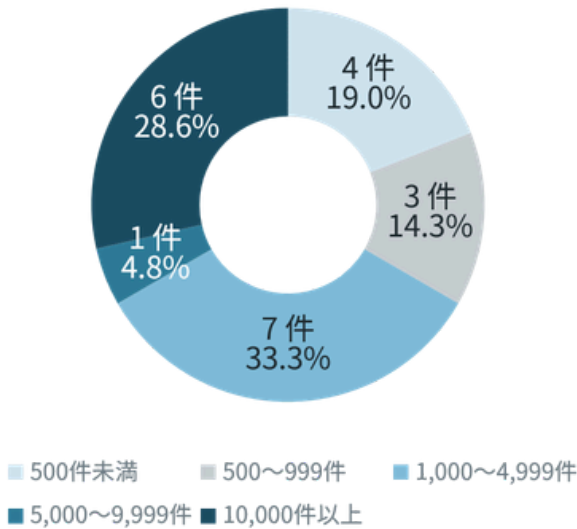
Cacco・リンク調べ

流出規模別に見ると、流出件数10,000件以上の事件は6件（28.6%）で、前年の15件（40.5%）から件数・割合ともに減少した。

一方、500件未満の事件は4件（19.0%）と、前年のわ

ずか1件（2.7%）から増加している。500～999件が3件（14.3%）、1,000～4,999件が7件（33.3%）、5,000～9,999件が1件（4.8%）であり、中小規模の事案が全体の7割を占める分布へと変化した（図1-4）。

▼図1-4 2025年カード情報流出規模別事件数



Cacco・リンク調べ

流出件数規模	2024年	2025年
500未満	1	4
500～999	0	3
1,000～1,499	2	3
1,500～1,999	1	1
2,000～2,499	3	2
2,500～2,999	2	1
3,000～3,499	0	0
3,500～3,999	2	0
4,000～4,499	2	0
4,500～4,999	2	0
5,000～7,499	6	1
7,500～9,999	1	0
10,000以上	15	6

(1)-2. 四半期別推移

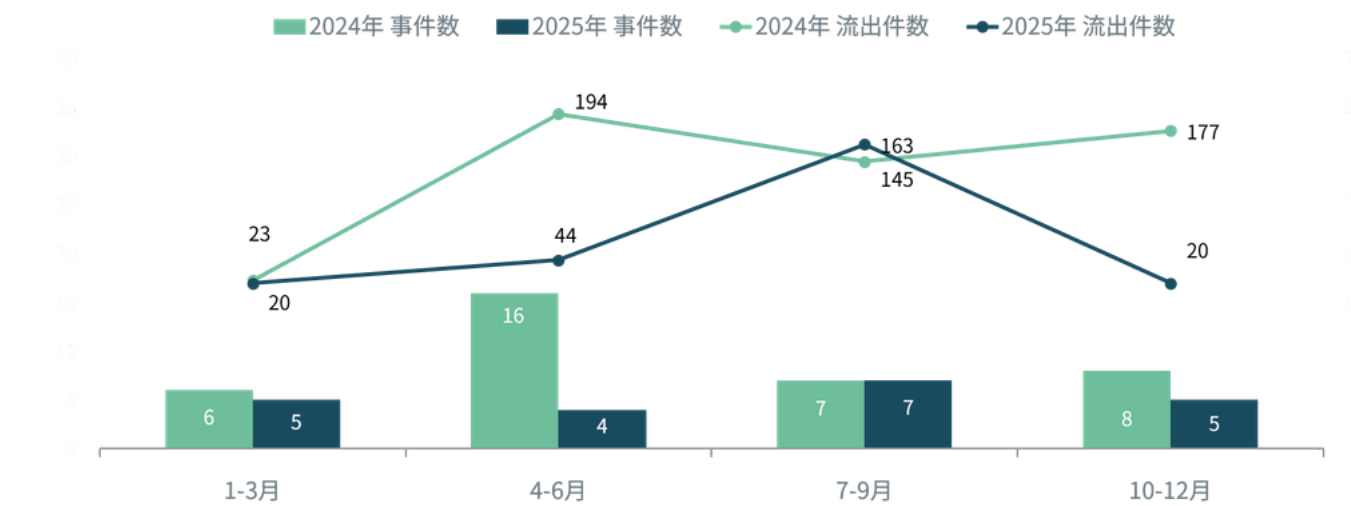
2025年の四半期別のカード情報流出動向を2024年と比較すると、流出事件数は通年で低い水準に落ち着いた一方、流出件数は特定の四半期に集中した（図1-5）。

1-3月期は流出事件数5件（前年同期6件）、流出件数19,635件（同23,677件）と、いずれも前年並みで推移した。4-6月期は流出事件数が前年同期16件から4件へと4分の1に減少し、年間で最も少ない四半期となった。流出件数も3年以上の長期にわたる流出が複数公表された前年同

期（2024年4-6月期）の約19万4千件に比べ、44,295件へと大幅に減少した。

7-9月期は流出事件数7件と前年同期（2024年7-9月期）と同数ながら、流出件数は162,894件と年間の66%を占めた。前述のA社によるランサムウェア攻撃によるカード情報流出の可能性の公表が、この四半期に含まれたことが主な要因である。10-12月期は流出事件数5件（前年同期8件）、流出件数19,650件（同177,772件）と、事件数・流出件数ともに大きく減少した。

▼図1-5 2024年と2025年のカード情報流出件数 四半期別の推移



Cacco・リンク調べ ※流出件数は千件単位（四捨五入）

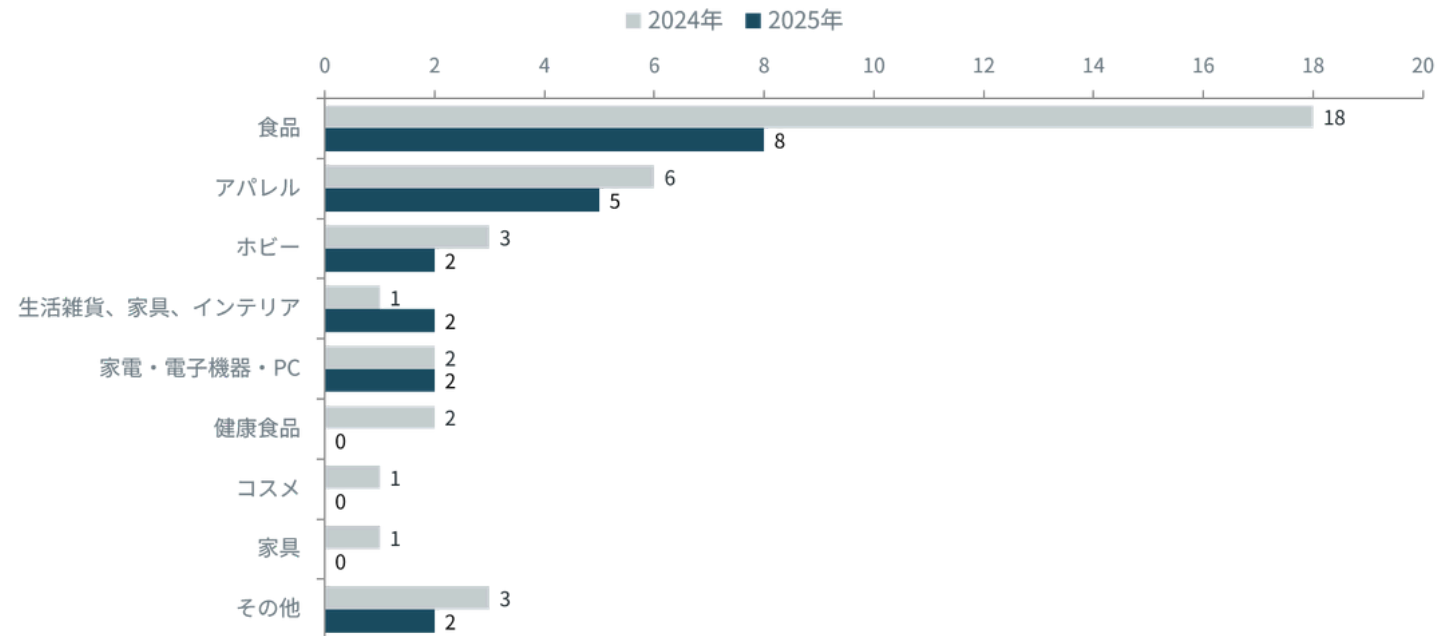
(2) カード情報流出事件の傾向

(2)-1. 業種/取扱い商材別・情報流出期間別事件

2025年のカード情報流出事件数21件の内訳を取扱い商材別に見ると、最も多いのが食品（8件）、次いでアパレル（5件）、ホビー（2件）、生活雑貨・家具・インテリア

（2件）、家電・電子機器・PC（2件）、その他（2件）となった（図1-6）。食品が最多である点は前年と共通しており、比較的小規模な事業者が自社ECを運営するケースが多い商材にリスクが集中している傾向がある。

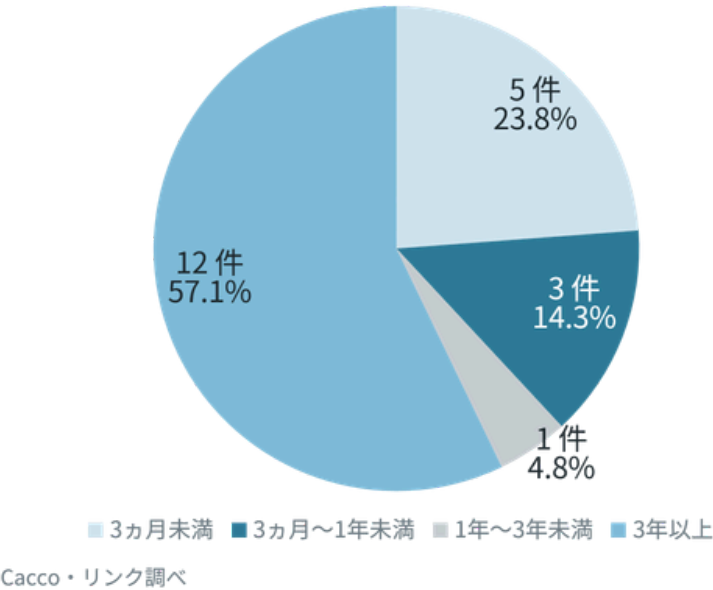
▼図1-6 2025年業種／取扱い商材別カード情報流出事件数



Cacco・リンク調べ

流出期間別に見ると、3年以上の流出事件数が12件（57.1%）と最多を占め、前年の14件（37.8%）から割合が大きく上昇した。次いで3ヵ月未満が5件（23.8%）、3ヵ月～1年未満が3件（14.3%）、1年～3年未満が1件（4.8%）であった（図1-7）。

▼図1-7 2025年流出期間別事件数



加盟店1件あたり平均流出期間

780日

▼ 17%

2024年：945日

1事件あたり平均流出件数

11,737件

▼ 20%

2024年：14,614件

※ランサムウェア攻撃被害を受けたA社1件を除くと
平均流出期間 **819日**／平均流出件数 **5,961件**

流出期間3年以上の12事件について、事件発覚のきっかけを調べると、うち7件が警察の指摘によるものであった。また、「その他」となっている2件についても、公式発表では「外部機関による指摘」という記載であり、警察による指摘である可能性がある。『キャッシュレスセキュリティレポート2024』では、警察により2020年～2021年頃にかけて情報流出被害が多発したECサイトと同じプラットフォームが集中的に調査され、改ざんが指摘されていることを報告したが、2025年も引き続きその捜査活動が継続していたと推測される。

一方で、流出期間3ヵ月未満の5事件のうち4件が自社による発見であった。割賦販売法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【6.1版】』（以下『セキュリティガイドライン6.1』と記載）では、EC加盟店に対して脆弱性対策の実施を義務付けている。徐々にEC加盟店自身による定期的な点検や対策が広がりつつあることで、自社による短期間での発見と対応が可能になってきていると推測される。（図1-8）

▼図1-8 発覚のきっかけ別 流出期間区分・平均流出期間

発覚のきっかけ	3ヵ月未満	3ヵ月～1年未満	1年～3年未満	3年以上	計	平均流出期間(日)
警察からの連絡	—	1	—	7	8	1,082
カード会社/決済代行事業者	1	—	1	3	5	909
自社にて発見	4	—	—	—	4	7
その他	—	1	—	2	3	991
システム運営委託会社	—	1	—	—	1	184
計	5	3	1	12	21	780

Cacco・リンク調べ

加盟店における流出事件1件あたりの平均流出件数は11,737件と、前年の14,614件から約2割減少した。なお、ランサムウェア攻撃による流出事案であるA社（127,263件）を除く20事件で見ると、合計119,211件、平均流出期間819日、平均流出件数5,961件となり、オンラインスキミングによる被害規模は前年から大きく縮小したことがわかる（図1-9）。

商材別に流出件数と流出期間を集計すると、食品が8件・149,497件（平均流出期間648日／平均流出件数18,687件）と件数・流出件数ともに最多となった。ただし、これはA社の127,263件を含む数値であり、同社の事案を除くと22,234件となった。次いでアパレルが5件・49,364件（同1,084日／9,873件）、ホビーが2件・32,340件（同760日／16,170件）と続いた。アパレルの5件は平均流出期間がその他に続いて1,084日と長く、長期にわたるWebサイトの改ざんの放置が被害を拡大させた。

▼図1-9 2025年業種・取扱い商材別カード情報流出件数／流出期間

食品は事件数最多だが、流出件数の大半はランサムウェア攻撃を受けたA社1件によるもの

商材	事件数（件）	カード情報 流出件数（件）	平均流出期間 （日）	平均流出 カード情報件数（件）
加盟店合計	21	246,474	780	11,737
食品	8	149,497	648	18,687
アパレル	5	49,364	1,084	9,873
ホビー	2	32,340	760	16,170
生活雑貨、家具、インテリア	2	12,883	771	6,442
家電・電子機器・PC	2	105	90	53
その他	2	2,285	1,271	1,143

※A社（ランサムウェア感染・127,263件）を除く20事件では、合計119,211件／平均流出期間819日／平均流出件数5,961件

Cacco・リンク調べ

(2)-2. カード情報窃取の手口：
オンラインスキミングが引き続き大半を占める

カード情報窃取の手口として2018年頃から増えている「オンラインスキミング」は、ECサイトを改ざんし、消費者が入力したカード情報を直接消費者から窃取する手法である。入力された情報がそのまま送信されるため、ほとんどの事案はセキュリティコードも一緒に流出する。セキュリティコードは、PCI DSSにおいて認証後の保存が原則認められない「機密認証情報」に位置付けられており、本来、加盟店側に保存されているデータには含まれない。オンラインスキミングは保存済みデータではなく入力時点の情報を窃取するため、「保存しない」という統制では防げず、セキュリティコードが揃った形で流出する点に深刻さがある。PCI DSS v4.0（現行はv4.0.1）ではオンラインスキミングへの対策として、決済ページで読み込まれるスクリプトの管理・承認（要件6.4.3）と、決済ページの改ざん検知（要件11.6.1）が新たに要件化されている。『セキュリティガイドライン6.1』は、国内の加盟店のカード情報保護については、自社で保有する機器・ネットワークにおいて「カード情報」を「保存」、「処理」、「通過」しない「非保持化」が有効なセキュリティ対策の一つであるとしている。非保持化を達成

するための方策としては、決済代行業者（PSP）が提供する「リダイレクト（リンク）型決済」、もしくはECサイト内にある決済画面にJavaScriptを埋め込むことでPSPにカード情報を送信する「JavaScript型（トークン型）決済」の導入を挙げている。国内のほとんどのECサイトが、どちらかを導入している。しかし、オンラインスキミングの手口では、Webブラウザに表示する決済ページに消費者が入力したカード情報を攻撃者が直接窃取するため、非保持化を達成しただけでは防ぐことはできない。

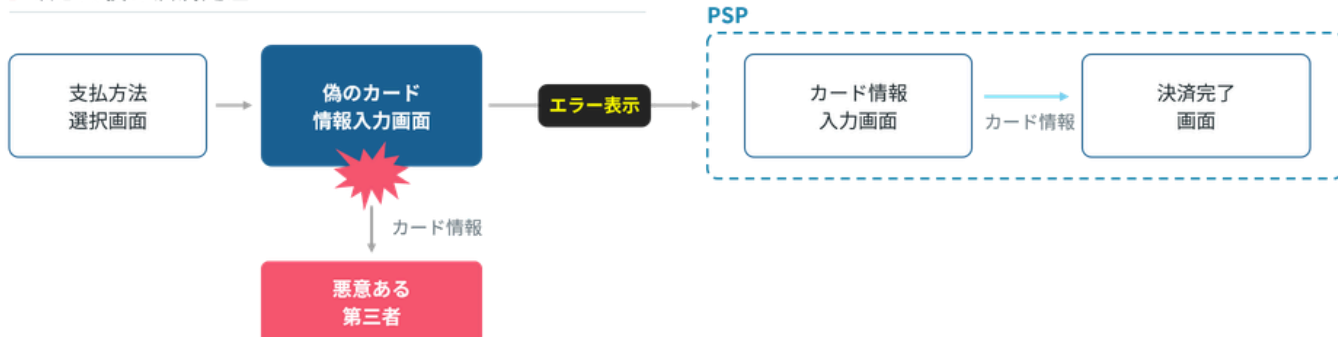
一般に、決済代行業者のリダイレクト（リンク）型決済は、決済ページが決済代行業者のサイトに設置されているため、ECサイト内に決済ページがあるJavaScript型（トークン型）決済に比べて安全であると思われるがちである。しかし実際には、リンク型決済であっても、ECサイトを攻撃されて支払方法の選択画面から決済ページへのリンクを改ざんされることで、偽のカード情報入力画面に誘導され、カード情報を窃取されるケースがある（図1-10）。非保持化後の加盟店においても事件が発生していることから、『セキュリティガイドライン6.1』では、すべてのECサイトに対して、ウイルス対策、管理者権限の管理、デバイス管理などの脆弱性対策の実施を指針対策として義務付けている。

▼図1-10 リダイレクト（リンク）型決済におけるオンラインスキミングの流れ

■ 正常な決済処理



■ 改ざん後の決済処理



『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

カード情報流出事件の原因については被害企業の公式発表では明確に言及されないことが多い。リンクは、2025年に公表された21件のカード情報流出事件の原因がオンラインスキミングである可能性を公表内容から以下の観点で推定し、その割合を集計した。（図1-11）

- ①**オンラインスキミング**：公式発表で「決済画面が2枚あった」「画面に入力したカード情報が第三者に送信された」等のオンラインスキミングであることがわかる記載がある。
- ②**オンラインスキミングの可能性高**：公式発表でオンラインスキミングであることがわかる記載はないが、セキュリティコードが流出している。
- ③**オンラインスキミングの可能性低**：公式発表で原因が明確にわかる記載がないが、セキュリティコードが流出していない。

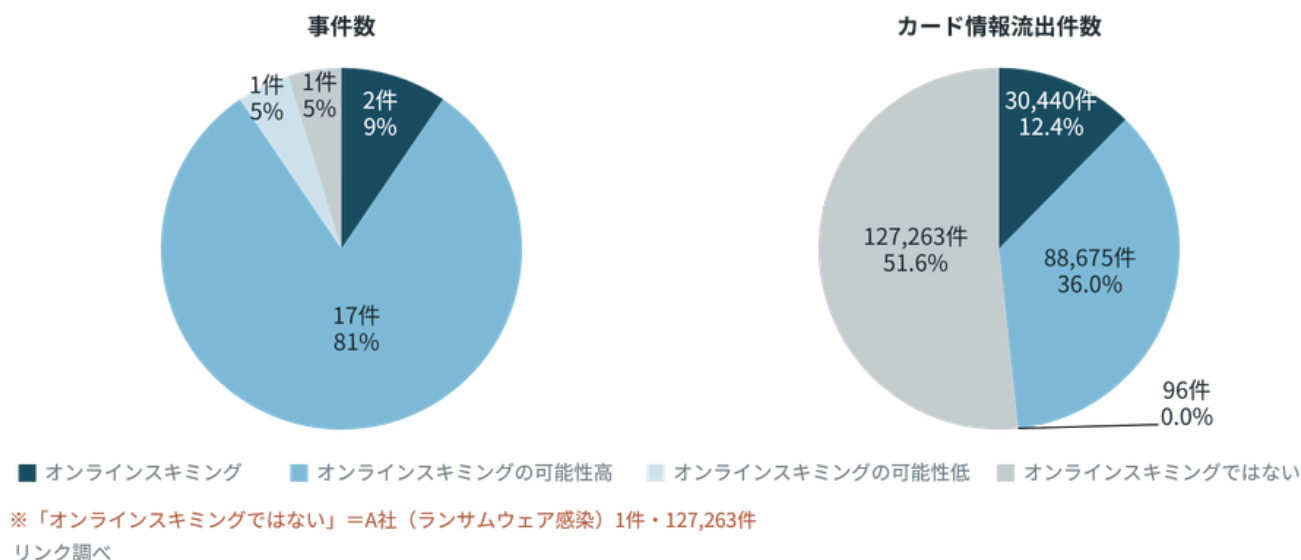
④**オンラインスキミングではない**：公式発表でオンラインスキミング以外の原因が明記されている。

2025年に発生した21件のカード情報流出事件のうち、オンラインスキミングもしくはその可能性が高い事件は19件、90.5%となった（図1-11）。内訳は①オンラインスキミングが2件（9.5%）、②オンラインスキミングの可能性が高いものが17件（81.0%）、③オンラインスキミングの可能性が低いものが1件（4.8%）、④オンラインスキミングではないものが1件（4.8%）である。流出事件数ベースでは、ECサイトの改ざんによるカード情報窃取が引き続き大半を占めている状況である。

一方、カード情報流出件数ベースで見ると、前述のA社のランサムウェア攻撃による流出事案が127,263件（51.6%）と過半を占めている。

▼図1-11 2025年のカード情報流出事件に占めるオンラインスキミングの割合

事件数では19件（90.5%）がオンラインスキミングもしくはその可能性が高い。流出件数ベースの構成はA社1件の影響で反転する。



(3) 2025年のカード情報流出事件のトピック

(3)-1. ランサムウェア攻撃による

カード情報流出とランサムウェア対策

2025年7月、食品（スーパーマーケット運営）A社が、ランサムウェア攻撃によって、自社が発行するポイントカード一体型クレジットカードの情報が閲覧・流出された可能性があることを公表した。本件はランサムウェア攻撃により現在有効なカード情報について外部からの閲覧の可能性が報告された、国内で初めての事案である。本事件の流出件数127,263件は、2025年のカード情報流出件数の半分以上を占めた。

■事件の経過

A社は2025年3月30日にシステムの異常を検知し、複数のサーバーが暗号化される被害を受けた。基幹システムが停止したことにより、翌31日には展開する23店舗の全店が臨時休業した。4月1日に営業は再開したが、クレジットカード決済とポイント付与が利用できない状態はその後2ヵ月以上続き、その間はカードの新規入会と再発行手続きも停止する事態となった。4月に公表された第1報の時点では、個人情報の流出は確認されていないとされていた。

流出の全容が明らかになったのは、約3ヵ月後の7月に公表された第2報である。顧客の個人情報延べ約42万5千件、取引先情報約4,600件、取引先が雇用する派遣社員の個人情報約3,900件、従業員及びその扶養家族の個人情報約1万5千件が閲覧された可能性があることが公表された。顧客の個人情報のうち、カード情報と合わせて流出した件数は127,263件で、氏名・住所などの個人情報および2022年4月から2025年3月までの購入履歴とあわせて、ポイントカード一体型クレジットカードのカード番号、名義人、有効期限が不正に閲覧された可能性があるとされている。同カードの登録会員及びポイントの管理システムが暗号化され、その過程で情報が閲覧されたものと推測される。なお同社はセキュリティコードを保持しておらず、流出の対象には含まれていない。

■決済システム以外の場所からカード情報が流出

今回の事件の特徴は、加盟店において、決済システム以外のシステムから、カード情報が流出したことである。前述の通り、『セキュリティガイドライン6.1』では、自社で保有する機器・ネットワークにおいて「カード情報」を「保存」、「処理」、「通過」しない「非保持化」が有効なセキュリティ対策の一つであるとしており、具体的に非保持化を達成するための決済システムの方式を業態別に定義している。

一方で、加盟店の中でもスーパーマーケットや百貨店などの業態では、A社のようにポイントカード一体型クレジットカードを自社で発行している例は多く、登録会員やポイントの管理のために自社システムでクレジットカード情報を保持する構造になりやすい。『セキュリティガイドライン6.1』は、クレジットカード情報を保存する場合にはPCI DSSへの準拠を要請している。しかし加盟店は決済システム以外の場所に保存されているカード情報を意識できていないことが多く、自社にPCI DSS準拠が必要なことに気づいていないケースもあると考えられる。

A社と同様の形態でクレジットカードなどのカード情報を取り扱っている加盟店は、保存の要否とPCI DSSの準拠状況を改めて点検する必要がある。あわせて、全ての加盟店は、受注管理システム、コールセンターの対応記録、バックアップデータ、業務端末のファイル、委託先の保有データなど、業務全体のデータフローを見渡して、カード情報が意図せず残置されている箇所を洗い出すことが求められる。

■ランサムウェア攻撃の被害を防ぐために

警察庁サイバー警察局の統計によれば、ランサムウェア攻撃の被害報告は2022年頃から年間200件台の高い水準が続いており、2025年も226件が報告されている。カード情報を取り扱う事業者にとって、A社の事案は決して特異な例外ではない。ランサムウェア対策として求められる基本的な事項には図1-12のようなものがある。

▼図1-12 基本的なランサムウェア対策の例

対策のカテゴリ	具体的な例
VPN経由の侵入防止	• VPN機器のソフトウェアのアップデート • 多要素認証の導入 • 接続元IPアドレスの限定 • IPS/IDSの導入
フィッシング対策	• DMARC導入によるなりすましメールの防止 • URLフィルタリング機能によるフィッシングサイトへのアクセス防止
サーバー・PCへの対策	• 多要素認証の導入 • EPP（マルウェア対策ソフト）の導入と常時パターン更新 • EDRの導入 • ソフトウェアのアップデートによる脆弱性対応
バックアップ	• 複数バックアップ保存 • 3-2-1-1-0のバックアップ • リストアテストの定期的な実施
対応手順と体制の整備	• インシデント対応計画の策定と定期的な見直し • インシデント発生時の外部への報告手順の検討 • フォレンジック調査体制の整備

なお、対策の一覧とは別に1点強調しておきたいのが、身代金の支払いに応じるべきではないという点である。身代金を支払ったからといって、暗号化されたデータの復号が保証されるわけではない。さらに、支払った身代金は犯罪グループなどの活動資金となることが懸念される。また、ひとたび支払いを行うと、攻撃者の間で「身代金支払いに応じる企業」としてマークされ、繰り返し攻撃のターゲットにされる可能性がある。加えて二重恐喝では、窃取されたデータが削除されたことを検証する手段がなく、支払い後にリークサイトへ掲載される可能性も残る。

カード情報が対象となった事案において、支払いによって漏えいリスクが消滅することはない。支払わずに復旧する手段も整備されつつある。「No More Ransom」プロジェクトでは一部のランサムウェアに対応する復号ツールが無償公開されている。警察庁も2024年2月にLockBit、2025年7月にPhobos／8baseの復号ツールを公開している。被害時はまず端末を隔離し、警察へ通報・相談すべきである。支払いという選択肢を排除できるかどうかは、平時の備えで決まる。

用語解説：3-2-1-1-0バックアップ

「3つのコピー、2つの異なるメディア、1つのオフサイト（遠隔地）」という3-2-1ルールを、バックアップ製品を提供するVeeam Softwareが拡張した考え方。バックアップ自体を標的とするランサムウェアが増えたことを背景に、3-2-1に加えて「1つのオフラインもしくは不変（変更不可）の状態」と、「0のエラー（リストアテストによって復元時にエラーが発生しない）」を求めている。

オンラインスキミングを想定した脆弱性対策が「ECサイトを改ざんさせない」ことに主眼を置くのに対し、ランサムウェア対策は「社内ネットワークに侵入させない、侵入されても被害を広げない」という、より広い範囲のセキュリティ対策を必要とする。

A社の事案が示したように、被害はカード情報の流出にとどまらず、全店臨時休業や2ヵ月以上に及ぶカード新規及び再発行業務の停止といった形で事業活動そのものを直撃する。ランサムウェアに感染させないための対策と、感染しても被害を最小限にとどめるための対策の両立が、カード情報を取り扱う事業者のみならず全ての事業者に求められている。

2. 2025年のカード不正利用の概況

(1) クレジットカード不正利用被害額の推移

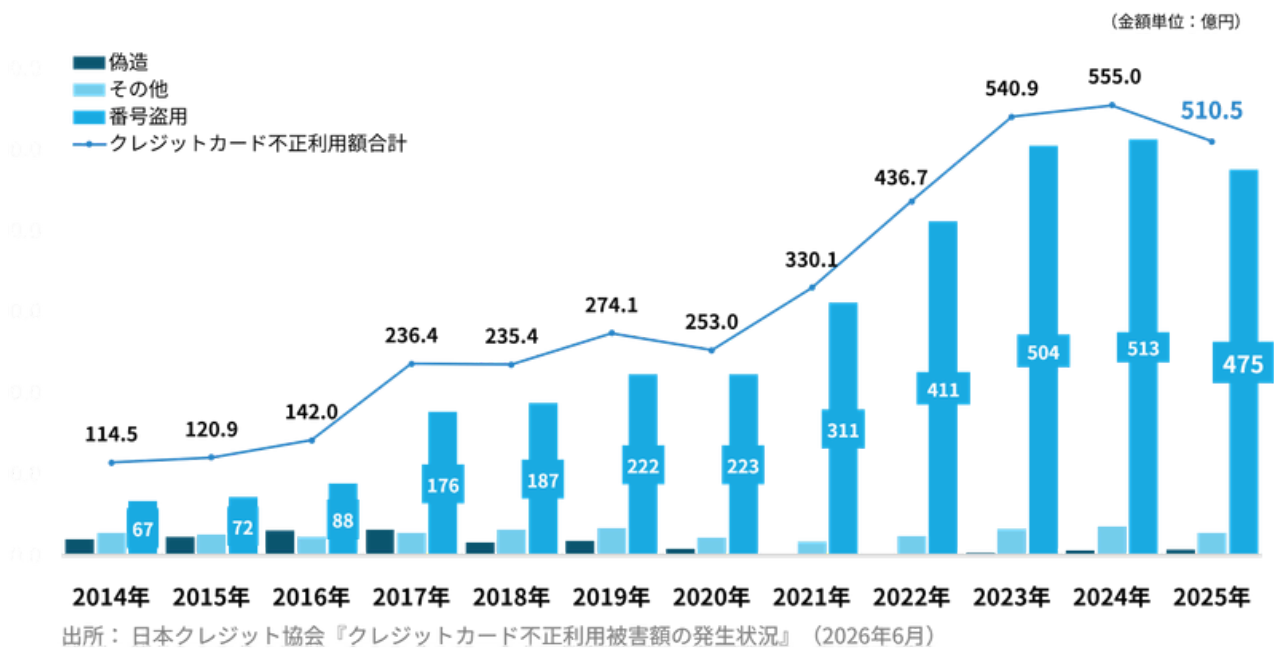
(1)-1. 2025年のクレジットカード不正利用額と傾向

一般社団法人日本クレジット協会（JCA）の発表によると、2025年のクレジットカード不正利用被害額は年間合計で510.5億円に達した。2024年の555.0億円から減少したものの、依然として500億円を超える高止まりの状況が

続いている。

内訳を見ると、2025年の全被害額の約93%を「番号盗用（カード番号や有効期限などの情報が窃取され、ECサイト等で不正にカード決済される手口）」が占めており、EC事業者における非対面取引での対策が最重要課題である状況に変わりはない。（図2-1）

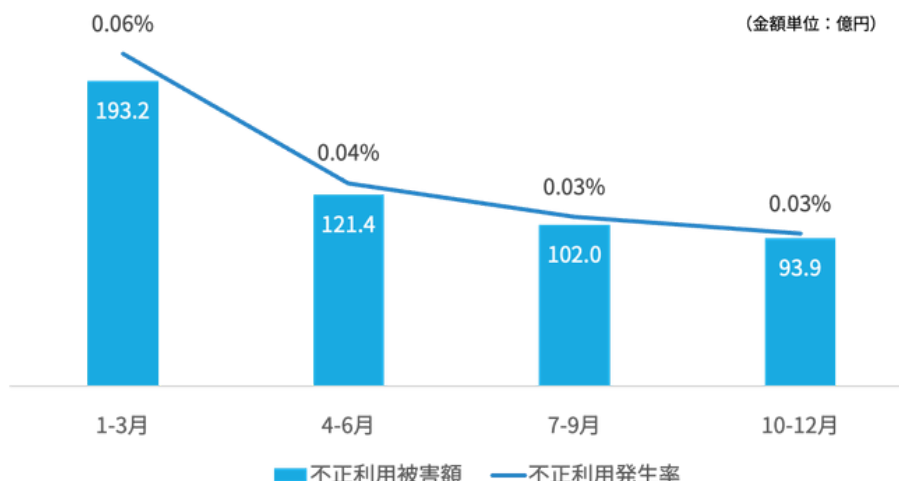
▼図2-1 2025年までのクレジットカード不正利用被害額の推移



四半期別のクレジットカード不正利用額とクレジットカードの決済全体に対する不正利用の発生割合を示す「不正利用発生率」は、図2-2のように推移している。従来、クレジットカードの不正利用被害は、年末年始の大型セール

や繁忙期にあたる第4四半期（10-12月）に増加する傾向があった。しかし、2025年は第1四半期（1-3月）の193.2億円をピークに、期を追うごとに不正利用被害額および不正利用発生率が減少・下落する動きを見せている。

▼図2-2 四半期別のクレジットカード不正利用額と不正利用発生率



出所：日本クレジット協会『クレジットカード不正利用被害額の発生状況』（2026年6月）

2025年の年末にかけて不正利用が減少している背景には、2025年3月末を期限として推進された「EMV 3-Dセキュア（以下EMV3-DS）」の義務化によるEC加盟店への導入が大きな影響を与えていると考えられる。不正利用対策で先行する欧州（EU）では、決済サービス指令「PSD2（Payment Services Directive 2）」に基づき、欧州銀行監督局（EBA）は2020年末を移行期限として、強力な顧客認

証（SCA：Strong Customer Authentication）を非対面のカード決済に適用することを求めた。SCAの一つの手段としてEMV3-DS等の導入が進み、本格的な普及に伴いカード不正利用被害が大幅に減少した実績がある。日本国内においても、2025年にかけて加盟店へのEMV3-DSの導入が進んだことで、欧州と同様の不正利用の減少が顕在化し始めたと推察される。

用語解説：EMV 3-Dセキュア

オンラインでのカード決済時にカード会員の本人認証を行う国際標準のセキュリティ対策の技術。決済のたびに固定パスワードの追加入力を一律で求めていた従来の方式とは異なり、決済時のデバイス情報や購買リスクを判定し（リスクベース認証）、リスクが高いと判断された取引の場合にワンタイムパスワードやパスキーによる追加の本人認証（チャレンジ認証）を求める。これにより、離脱率（カゴ落ち）を抑えつつ安全な取引を実現する。

(1)-2. 年間500億円超の高止まりが続く

要因と今後の課題

四半期ごとの不正利用被害額は減少傾向を見せる一方、年間の不正利用被害額は500億円を超える高い水準に留まっている。この要因として、以下の点が挙げられる。

1. 本人認証を迂回した不正利用へのシフト

EMV3-DSが導入されたECサイトを避け、未導入のEC加盟店へ攻撃がシフトしている可能性が考えられる。EMV3-DSによる認証が及ばない取引へ不正利用が集中する傾向は、欧州でも観測されている。欧州銀行監督局（EBA）と欧州中央銀行（ECB）が2025年12月に公表した共同レポート『2025 Report on Payment Fraud』によれば、SCAで認証された取引は、認証のない取引よりも不正利用率が低く、その差はカード決済で特に顕著であった。2024年のEEA（欧州経済領域）域内のカード決済では、適用除外規定によりSCAが適用されなかった取引の不正利用率は、SCAが適用された取引の約2倍であり、取引の相手方

がEEA域外にある場合は金額ベースで約3倍、件数ベースで約4倍であった。同報告書は地理的区分の分析でも、SCAの適用が法的に義務付けられていないEEA域外の相手方との取引におけるカード決済の不正利用率が国内取引と比較して金額ベースで約17倍に達したとしている。本人認証の強化が進むほど、その網の外側へ攻撃が移動するという構図であり、国内でも同様の展開が考えられる。

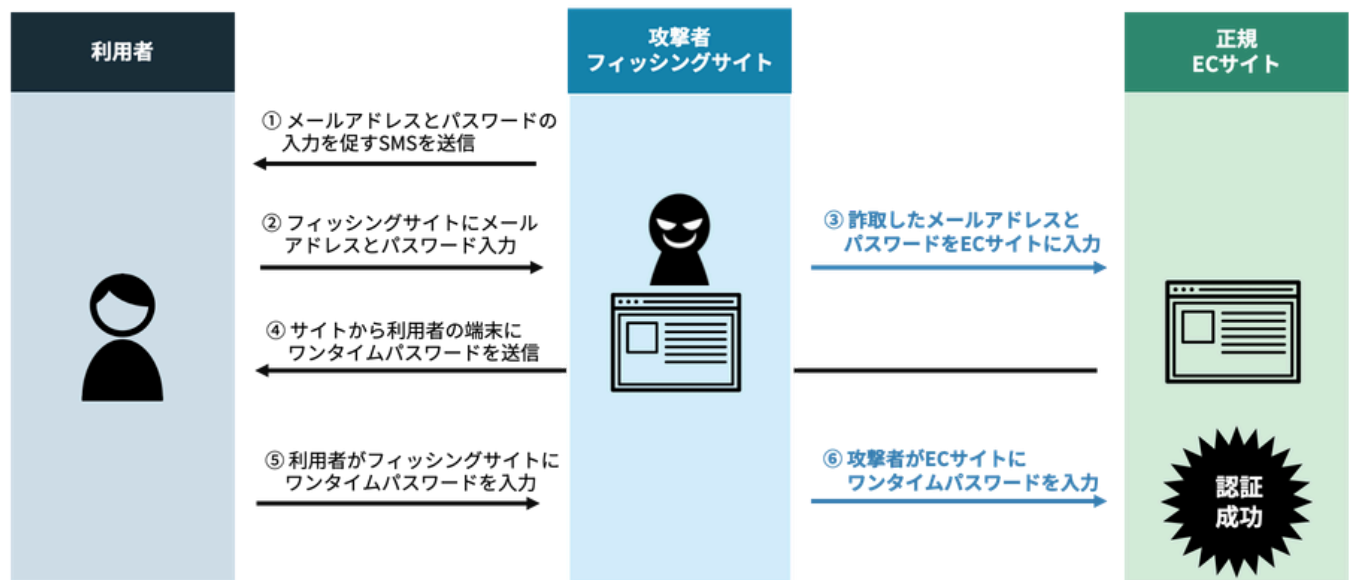
2. 中間者攻撃の増加

フィッシングによって消費者をフィッシングサイトに誘導し、認証情報とワンタイムパスワードをリアルタイムで窃取する手口（中間者攻撃）が発生している。フィッシングの手口は従来よく見られたメールやSMSでフィッシングサイトのURLを送付するものに加え、SNS広告を用いるものなど多様化が進んでいる。（詳細は「2-(4)-1. なりすまし広告を入り口とした本人認証の悪用による不正利用」）

用語解説：中間者攻撃

利用者と正規のサービスの間に攻撃者が割り込み、認証のやりとりをリアルタイムで中継することで本人認証を突破する手口。AiTM（Adversary-in-the-Middle）、リアルタイムフィッシングとも呼ばれる。攻撃者はSMSやメール、SNS広告などで利用者を本物そっくりのフィッシングサイトへ誘導し、入力されたIDとパスワードを即座に窃取して正規サイトへログインする。正規サイトが利用者のスマートフォンアプリやSMSへワンタイムパスワードを送ると、攻撃者はフィッシングサイト上で利用者にその入力を促し、得られたワンタイムパスワードをそのまま正規サイトへ入力して認証を成立させる（図2-3）。利用者は正規の手続きを踏んでいるつもりで操作しているため気づきにくい。ワンタイムパスワードは有効期限内にそのまま使われるため、認証手段を追加するだけでは防ぎきれない点が特徴である。

▼図2-3 中間者攻撃（AiTM）による本人認証突破の流れ



【ポイント】

攻撃者はID・パスワードだけでなく、その瞬間に発行されたワンタイムパスワードまでもフィッシングサイト経由でリアルタイムに中継して正規のECサイトへ入力するため、従来のワンタイムパスワード認証だけでは不正ログインを防ぐことができない。

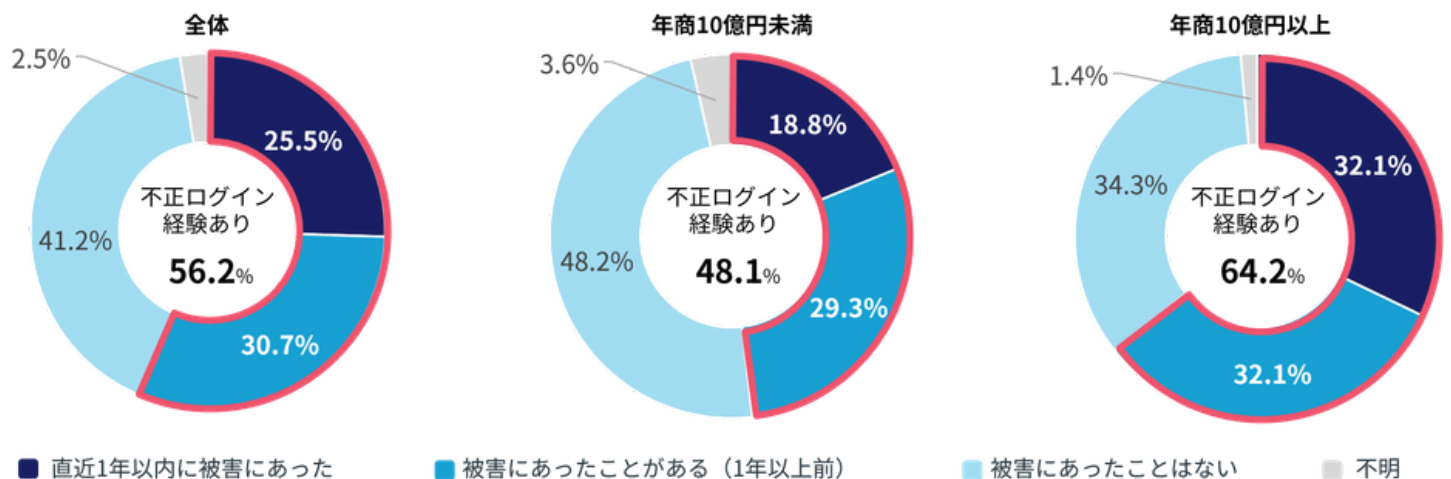
3. アカウント乗っ取り（ATO）やbotの増加

窃取したログイン情報を用いて会員アカウントを乗っ取る手口（ATO: Account Takeover）が拡大している。アカウントを乗っ取るだけでなく、botなど自動化ツールを用いて、乗っ取ったアカウントで大量の不正な注文を行う手口も確認されている。警察庁等が公表した統計によると、2025年に認知された不正アクセス行為は7,190件で、前年

の5,358件から34.2%増加した。このうち、不正アクセス後に「インターネットショッピングでの不正購入」が行われたケースは228件で、前年の180件から26.7%増加している。Caccoによる国内EC事業者を対象とした調査では、56.2%の事業者が不正ログイン被害を経験している（図2-4）。

▼図2-4 国内EC事業者における不正ログイン被害の経験

Q：不正ログイン（なりすましログイン、アカウント乗っ取り）の被害にあったことがありますか。（単一回答）



出所：「EC事業者実態調査2025」Cacco 2025年11月

用語解説：アカウント乗っ取り（ATO: Account Takeover）

悪意ある第三者がフィッシング詐欺や過去の流出データから入手したログインID・パスワードを用いて、正規ユーザーになりすまして会員ページへ侵入する行為。登録された決済手段の悪用、ポイントの不正利用、個人情報の閲覧・改ざんなどの被害が発生する。

アカウント乗っ取りによるキャッシュレスセキュリティにおける問題は、攻撃者がカード情報を新たに窃取しなくても、乗っ取ったアカウントに既に登録されている決済手段を悪用して、不正注文を行える場合があることである。ECサイトのアカウントは毎回カード情報を入力する必要をなくするためにカード情報が紐づけられていることが多い。その場合、攻撃者はカード情報そのものを不正に取得しなくても、配送先住所等を変更して不正注文を完結させることができる。不正利用対策を決済時の対策のみに依存していると、アカウント乗っ取りを十分に検知できないことがある。カード情報が未登録の場合であっても、乗っ取ったアカウントの氏名、住所、購入履歴等を利用し後払い決済などで注文を完結させ、未払いのまま商品をだまし取る手口も確認されている。なお、アカウントが一定の利用実績を持つ場合、新規利用者よりも不正注文が発見しにくくなる傾向がある。

アカウント乗っ取りの増加の背景の一つが、フィッシング等による認証情報の窃取と、それを利用したログイン試行の自動化である。フィッシング対策協議会によると、

2025年に国内で報告されたフィッシング件数は約245万件に達し、過去最多となった。フィッシングサイトではカード情報だけでなく、ECサイトや各種サービスのID・パスワードなどの認証情報も窃取対象となる。

情報窃取に特化したマルウェアを用いて、パソコンやスマートフォンから直接認証情報を窃取する手口もある。Kasperskyが情報窃取型マルウェア（インフォスティーラー）のログを分析した調査では、感染したデバイス1台から窃取されるログイン情報は平均50.9件に上り、2023年には日本に関連する「.jp」ドメインのアカウントだけでも約95万件の認証情報の漏えいが確認されている。こうした手口で窃取された認証情報は、直接不正利用されるだけでなく、ダークウェブ上の掲示板やTelegramのグループチャットなどを通じて売買・配布することが可能である。大量のID・パスワードを攻撃者が容易に入手できる環境が形成されており、ECサイトへの不正ログイン試行には、こうした認証情報のリストが悪用される。複数のサービスで同一のID・パスワードを使い回している利用者を狙い、認証情報を自動的に試行する「クレデンシャルスタッフィング」に用いられることもある。

用語解説：インフォスティーラー

感染したパソコンやスマートフォンから、ID・パスワード、ブラウザに保存された認証情報やCookie、クレジットカード情報、暗号資産ウォレットの鍵などを自動的に収集し、外部の攻撃者に送信する情報窃取に特化したマルウェア（情報窃取型マルウェア）。フィッシングメールの添付ファイル、正規ソフトウェアを装った配布サイト、不正広告などを経路として感染し、窃取された情報はダークウェブの市場やTelegramのグループチャットを通じて売買・配布される。

さらに近年では、生成AIを利用してプログラムやスクリプトを作成することが容易になったことで、高度なプログラミング知識を持たない者でも、大量のID・パスワードによるログインを自動的に試行し、不正利用可能なアカウントを選別する仕組みが構築しやすくなっている。実際に、国内では未成年者が不正に入手した大量のID・パスワードを利用し、生成AIを活用して不正アクセスや不正な契約を自動化するプログラムを作成したとされる事件が発生し、複数検挙されている。

4. 今後の課題

認証情報が大量に流通し、それを利用した攻撃が容易に自動化されることで、一度流出したID・パスワードが多数のECサイトへの不正ログインに利用されるリスクが高まっている。『セキュリティガイドライン6.1』では、「線の考え方」という多層防御の考え方を掲げ、決済前の対策として不正ログイン対策を指針対策として義務付けている。

用語解説：「線の考え方」

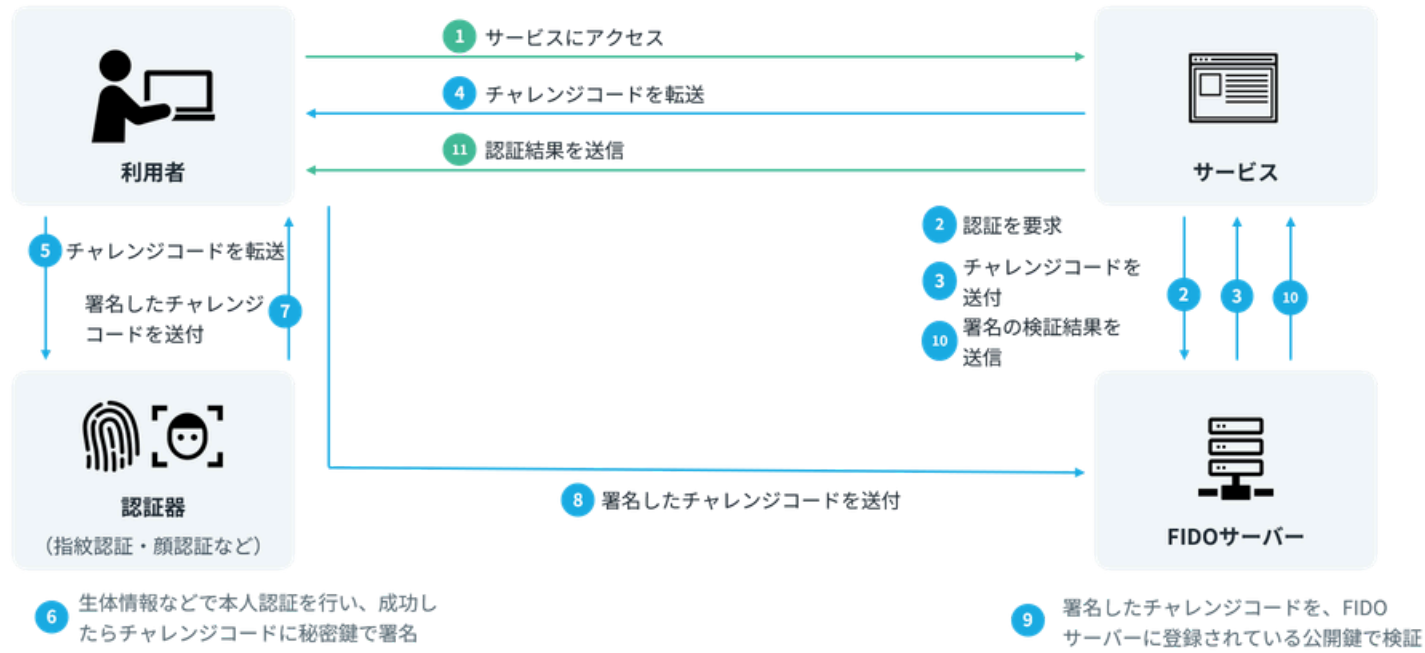
クレジットカード決済の瞬間（点）だけでなく、決済前（会員登録・会員ログイン・属性変更）・決済時（注文・カード情報入力・決済）・決済後（注文内容および顧客情報の確認・配送）という一連のプロセスを「線」としてとらえ、それぞれの場面で不正利用対策を行うという多層防御の考え方

『セキュリティガイドライン6.1』では不正ログイン対策として、不審なIPアドレスや端末からのアクセスの検知、短時間での大量のログイン試行に対する制限（スロットリング）、多要素認証の導入などを挙げている。

その中でも多要素認証は普及しつつあるが、ワンタイ

ムパスワードを利用者が入力する方式では、前述の中間者攻撃により突破されてしまう。対策としては、フィッシング耐性のある多要素認証であるパスキー（生体認証などを使用したパスワードレス認証の仕組み・図2-5）を用いた方式に移行することが有効である。

▼図2-5 パスキーによる認証



アカウント乗っ取りも含めた不正利用対策のためには、EC加盟店はEMV3-DSの導入による本人認証の強化や不正ログイン対策に加え、「属性・行動分析（不正検知システム）」などを組み合わせた重層的な対策の導入により、線の考え方を実践することが重要である。

(2) ECサイトにおける不正注文の傾向

(2)-1. ECにおけるクレジットカード不正利用発生率及び転売不正発生率の傾向

Caccoが提供する不正検知サービス「O-PLUX」の審査データに基づき、2025年のECにおける不正注文（クレジットカード不正発生及び転売不正発生）の傾向について解説する。

1. ECにおけるクレジットカード不正利用発生率と転売不正発生率の推移
審査件数全体に占める不正注文の審査結果（NG判定）の割合は図2-6の通りである。

▼図2-6 クレジットカード不正利用発生率及び転売不正発生率（年間推移）

年	クレジットカード不正利用発生率	転売不正発生率
2020年	0.9%	1.3%
2021年	1.2%	1.4%
2022年	1.6%	2.5%
2023年	1.6%	5.7%
2024年	2.4%	8.3%
2025年	1.9%	8.2%

※ 「O-PLUX」の審査で、審査件数全体に占めるクレジットカード不正注文/不正転売の審査結果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。

▼図2-7 クレジットカード不正利用発生率及び転売不正発生率（四半期別推移）

時期	クレジットカード不正利用発生率	転売不正注文発生率
2025年1-3月	1.8%	9.4%
2025年4-6月	3.2%	9.5%
2025年7-9月	1.4%	7.1%
2025年10-12月	1.4%	6.9%
2026年1-3月	1.9%	8.7%

※「O-PLUX」の審査で、審査件数全体に占めるクレジットカード不正注文/不正転売の審査結果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。

ECにおけるクレジットカード不正利用発生率は2025年4-6月（3.2%）に一時的に大きく高まったが、下半期にかけては1.4%と落ち着きを見せ、2026年1-3月には1.9%へと微増している。

一方、転売目的の不正注文の発生率（転売不正発生率）は年間を通じて約7%～9%台の高い水準で推移しており、EC事業者にとってカード不正利用のみならず悪質転売への対策も急務であることが浮き彫りとなっている（図2-7）。

【一般社団法人日本クレジット協会（JCA）の不正利用発生率とO-PLUX集計データの違いについて】

JCAが発表するカード不正利用発生率と、「O-PLUX」のカード不正利用発生率では数値に大きな開きがある。この違いは集計の母数と集計のタイミングが異なることに起因する。

●JCAの算出方法

母数を「クレジットカードショッピング信用供与額（全体の決済取引総額）」とし、分子を「カード会社に不正利用被害として届け出・認定された額」として計算している。全決済額（対面取引含む）が非常に大きいこと、また被害届が出た金額のみが集計されるため、発生率自体は非常に小さなパーセンテージとなっている。

●O-PLUXの算出方法

母数を「O-PLUXで審査を行った全注文件数」、分子を「O-PLUX」の審査により不正（NG）と判定した注文件数として算出している。O-PLUXを利用するECサイトを母数として、注文が行われる直前・審査段階でリスクの高い取引を捉えているため、実際のECサイト現場における不正注文の比率を反映した数値となる。

2. 不正に狙われやすい商材ランキング

「O-PLUX」の不正注文検知数に基づく商材別ランキングの推移は図2-8の通りである。

▼図2-8 商材別不正注文検知件数ランキング（2023年・2024年・2025年）

順位	2023年	2024年	2025年
1	デジタルコンテンツ	カメラ・映像/音響機器	チケット
2	ホビー・ゲーム	ホビー・ゲーム	ホビー・ゲーム
3	旅行	デジタルコンテンツ	健康食品・医薬品
4	コンタクト・メガネ	チケット	ふるさと納税
5	チケット	健康食品・医薬品	コスメ・ヘアケア
6	健康食品・医薬品	総合通販	日用品・雑貨・キッチン用品
7	コスメ・ヘアケア	コスメ・ヘアケア	アパレル
8	食品・飲料・酒類	ふるさと納税	デジタルコンテンツ
9	EC総合通販	家電・PC・タブレット	スポーツ用品
10	家電・PC・タブレット	日用品・雑貨・キッチン用品	レンタルサービス
11	アパレル	食品・飲料・酒類	総合通販
12	家具	サブスクリプション	食品・飲料・酒類

※「O-PLUX」の審査で、審査件数全体に占める審査結果NGの割合を件数ベースで商材ごとに算出。NGの割合が多い順にランキング（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。

【データから見える商材傾向と背景の考察】

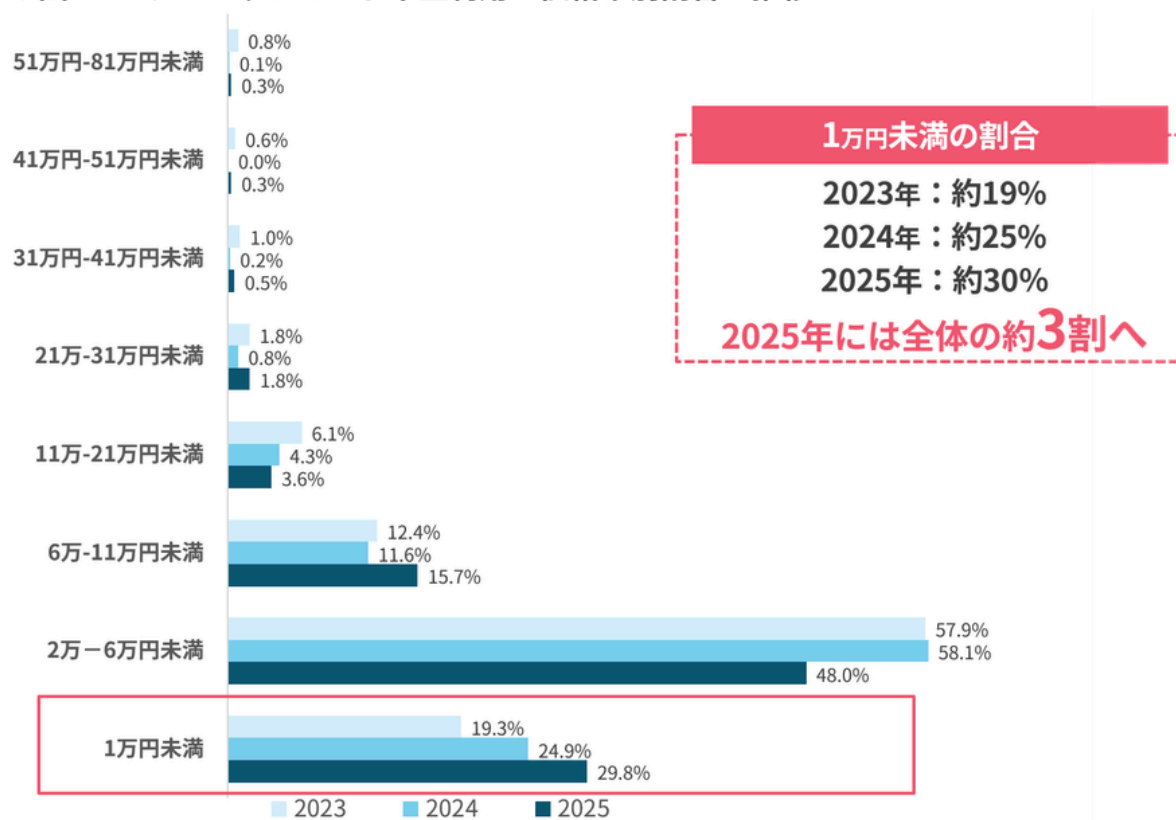
2025年の年間データでは、例年通り「チケット」や「ホビー・ゲーム」といった換金性の高い商材が上位を維持している。特筆すべき傾向として、2025年に「ふるさと納税」が4位へ浮上した。「健康食品・医薬品」がこの3年間で順位を少しずつ上げ、3位となっている。アパレルやスポーツ用品、限定ホビー商品に加え、健康食品などの初回限定割引商品を狙った不正注文が拡大している。これらは、フリマ（フリーマーケット）アプリ等の二次流通（個人間売買）市場において手軽かつ高値で転売できる環境が整っていることが背景にあると推察される。従来の「金券・高級ブランド品」といった高価格帯商材だけでなく、生活密着型や転売需要の高い商材全般へと不正のターゲットが分散・拡大している。

(2)-2. クレジットカード不正利用における注文金額の低額化

1. 1万円未満の不正注文割合が2025年には約30%まで上昇

「O-PLUX」におけるクレジットカード不正利用の価格帯別データを分析したところ、1回あたりの決済金額が低額化している傾向が確認された。具体的には、1万円未満の注文が占める割合が、2023年の19.3%から、2024年には24.9%、2025年には29.8%へと年々増加している。2年間で10ポイント以上上昇しており、2025年は不正利用件数全体の約3割を1万円未満の取引が占める状況となった。一方で、主流である「2万円～6万円未満」の価格帯の割合は、2023年の57.9%から2025年には48.0%へと約10ポイント減少した（図2-9）。

▼図2-9 クレジットカード不正利用の価格帯別割合の推移



「O-PLUX」の審査で、クレジットカード不正対策におけるNG金額の分布から集計（Cacco調べ）

2. クレジットカード不正利用における注文金額が低額化する背景と要因

このようにクレジットカード不正利用における注文金額が低下している背景には、攻撃側の手口の進化とターゲットの変更が影響していると推察される。主な要因として以下の2点が挙げられる。

① 検知回避を狙ったカードの有効性確認の増加

イシュー（カード発行会社）による不正利用検知ロジックの高度化や、ユーザーへのリアルタイム利用通知機能の普及に伴い、高額な決済を行うと即座に取引が保留され、カードが利用停止される傾向が強まっている。

そのため攻撃者は、入手したカード番号が現在も利用可能かを確認する目的の「カードの有効性チェック」や、カード会員やイシューの監視を回避するために、数千円～1万円程度の低額決済を複数回に分けて試行する手口へと移行していると考えられる。

② 初回限定品や低単価商材を狙う「悪質転売」との複合化

前項の商材ランキングでも示した通り、健康食品やコスメなど初回限定割引（無料～数千円程度）が適用される低単価商品へと不正注文の対象が拡大している。このような低単価商品の集中的な不正注文が増加したことも、全体として注文金額の平均を引き下げる要因になっていると推測される。

用語解説：カードの有効性チェック

加盟店や決済事業者が決済を実行する前に、そのカードが利用可能か（有効期限内か、利用停止されていないか、与信枠が残っているか）をカード会社に照会する手続きを指し、一般に「オーソリゼーション（オーソリ）」と呼ばれる。定期購入の登録時など、実際の売上を伴わない場面では、1円といった少額のオーソリだけを行って有効性を確認する運用が広く使われてきた。この運用は2026年10月以降、国際ブランドのルールにより禁止され、金額0円の「アカウント検証（Account Verification）」への移行が必要となっている。攻撃者はこれを逆用し、フィッシング詐欺等で不正に入手したカード番号や、規則性から推定して生成した番号のリストを、ECサイトの決済機能を利用し、大量に試行する。低額の決済を用いればカード会社やカード会員に気づかれにくいため、この方法で実際に使える番号だけを選別し、選別後のカード情報を高額の不正利用やリストとして転売に回す。すなわち有効性チェックの試行自体が不正利用の兆候となるため、加盟店側ではオーソリの失敗回数に上限を設けるなど、大量の試行を繰り返させない対策が求められる。

3. 低額取引についてEC事業者に求められる対策

従来の不正利用対策では高額商品（家電、高級ブランド品、金券類など）を重点的に監視する傾向があったが、今回の分析結果は、低額商品であっても不正利用の標的になり得るという現実を示している。単価が低いから被害が出ても影響が少ない、高額注文だけチェックしていれば安全という前提は成り立たなくなりつつある。注文金額にかかわらず、前述の「線の考え方」を取り入れた多層防御を導入することが、被害拡大を防ぐ鍵となる。

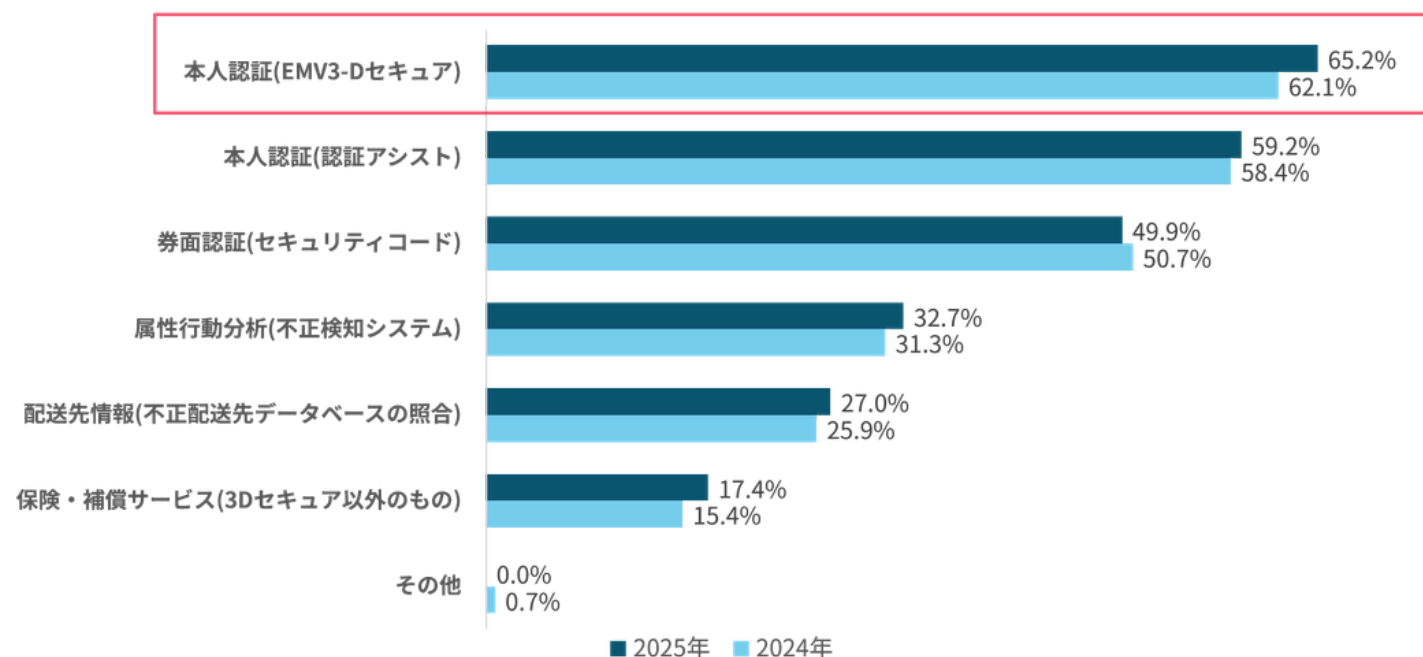
(2)-3. EC事業者の不正注文対策状況とEMV 3-Dセキュアの導入率

1. EMV 3-Dセキュアの導入率

Caccoが実施した「ECサイトにおける不正注文対策の実態調査（2025年版）」によると、EC事業者が導入している不正利用対策として最も多かったのは2024年と同様に「EMV3-DS（65.2%）」であった（図2-10）。

▼図2-10 EC事業者の不正注文対策の導入状況

Q：実施している対策方法は何ですか。（複数回答）



EC事業者実態調査（Cacco調べ）2025年6月調査

2. 年商規模における不正注文対策の実態

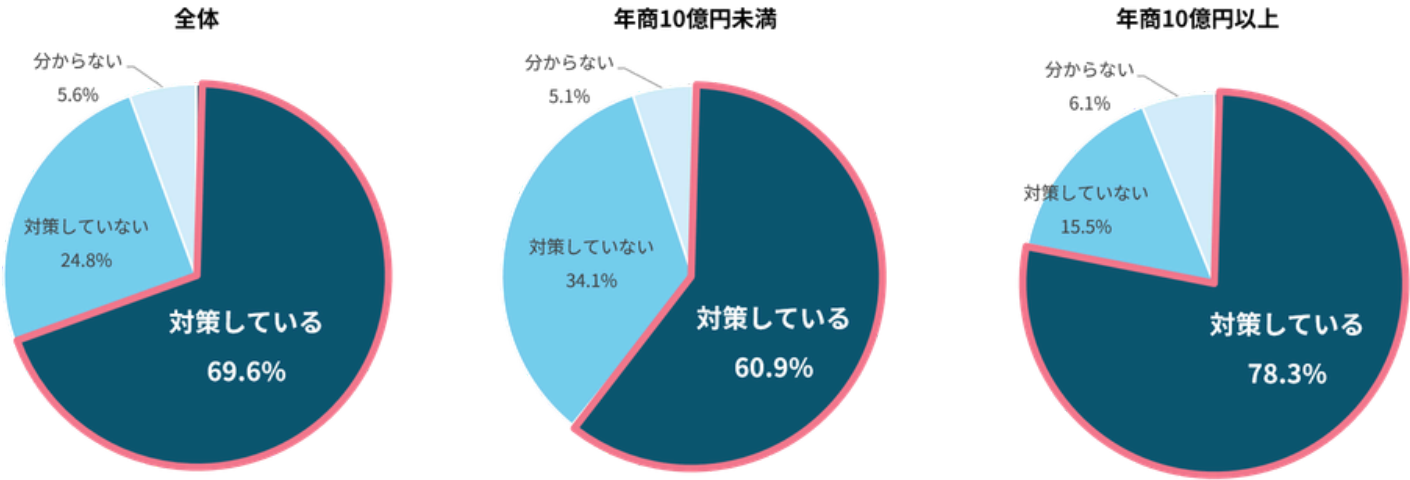
Caccoが実施した「ECサイトにおける不正注文対策の実態調査（2025年版）」の集計結果より、EC事業者が直面している決済環境の変化および企業規模による不正注文対策の実態を解説する。

① 年商規模別の不正注文対策の実施状況

カードの不正利用や悪質転売に対する「不正注文対策を実施している」と回答したEC事業者は全体で69.6%であった（図2-11）。しかし、企業規模別に見ると、年商10億円以上の企業では78.3%が対策を講じているのに対し、年商10億円未満の企業では60.9%に留まっている。

▼図2-11 年商規模別の不正注文対策実施率

Q：クレジットカード不正利用や悪質転売などの不正注文対策をしていますか。



EC事業者実態調査（Cacco調べ）2025年6月調査

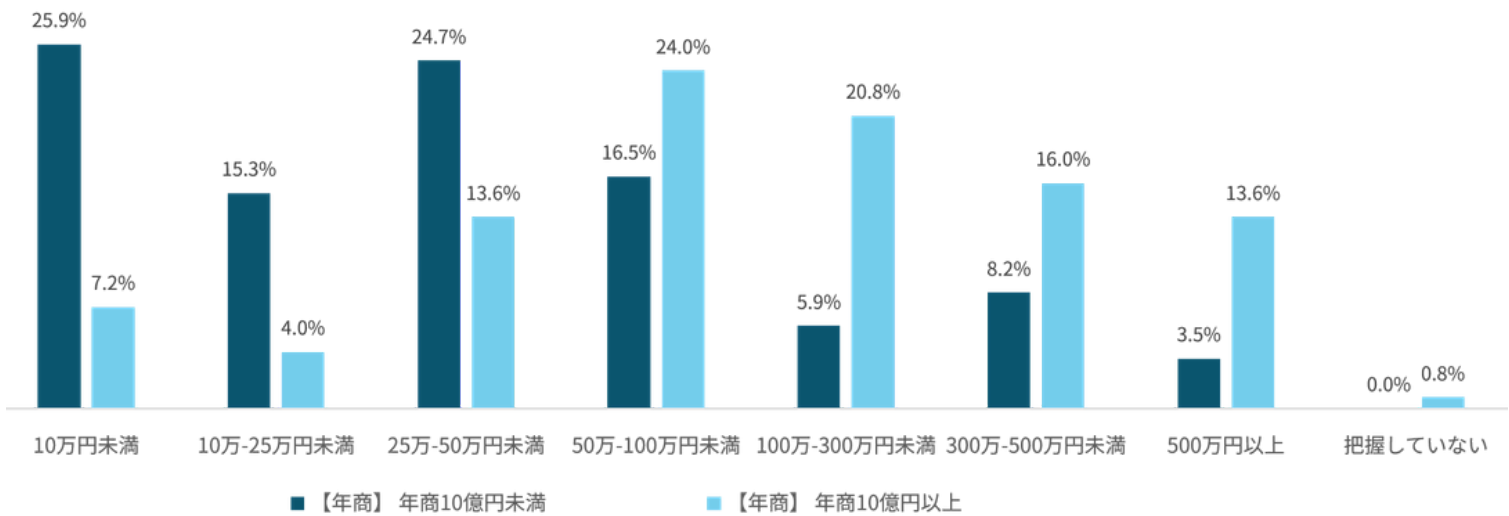
② 年商規模別のクレジットカード不正利用被害額の分布

クレジットカード不正利用被害を受けたことのあるEC事

業者を対象に被害の規模を年商別に分析すると、大手事業者と中小事業者で違いが確認できる（図2-12）。

▼図2-12 年商規模別の年間不正利用被害額の分布

Q：直近1年間の不正被害の総額はいくらですか。（単一回答）



EC事業者実態調査（Cacco調べ）2025年6月調査

年商10億円未満（中小規模EC）の年間不正利用被害額
「10万円未満」が最多の 25.9% を占め、次いで「25万～50万円未満（24.7%）」、「50万～100万円未満（16.5%）」となっている。

年商10億円以上（大手・大規模EC）の年間不正利用被害額
最多は「50万～100万円未満」の 24.0% であり、次いで「100万～300万円未満（20.8%）」、さらに「500万円以上」の深刻な被害を受けた事業者も 13.6% 存在している。

大手事業者はターゲットにされやすく被害総額が大きくなる傾向がある。これに比べると中小事業者は概ね被害総額は少ない傾向だが、それでも1割強は年間300万円以上の

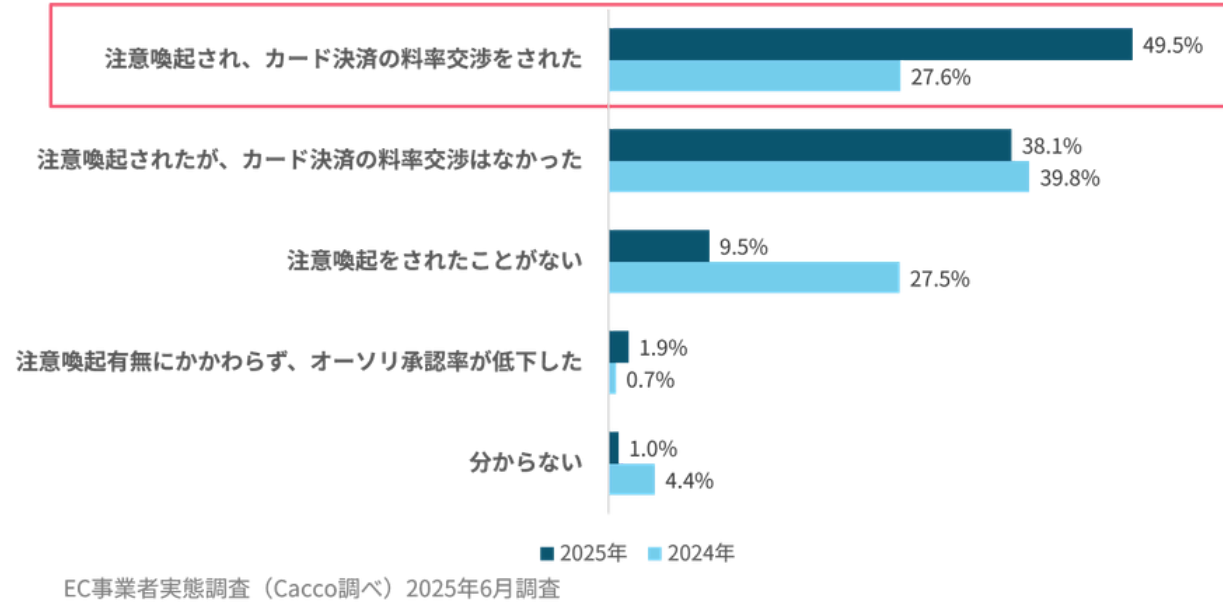
被害額となっている。

③加盟店契約カード会社からの「手数料値上げ交渉」が49.5%へ急増
クレジットカード不正利用被害が発生した経験のあるEC事業者のうち、加盟店契約カード会社（アクワイアラ）や決済代行事業者（PSP）から不正利用被害が多いことに対する注意喚起を受け、決済手数料（料率）の値上げ交渉をされた事業者が約半数の 49.5% に達した。2024年調査と比較して約2倍の割合へ急増した（図2-13）。

クレジットカード不正利用被害が発生すると、単に商品がだまし取られるだけでなく、将来的な決済手数料の増加という形でEC事業の収益性を直接圧迫するリスクが顕在化している。

▼図2-13 決済手数料の値上げ交渉を受けた事業者の割合

Q：クレジットカード会社または決済代行会社から、不正被害が多いと注意喚起されたことがあるまたは、料率交渉など何らかの働きかけをされたことがありますか。（単一回答）



3. EMV 3-Dセキュア導入に伴う現場の課題：カゴ落ちと決済承認率の低下

EMV3-DSの導入拡大が進む一方で、運用を開始したEC事業者の現場では新たなビジネス課題が表面化している。

課題1：カゴ落ち（購入途中の離脱）による売上機会損失
EMV3-DSの導入によりセキュリティレベルは向上するものの、決済時にワンタイムパスワードの入力画面などの追加認証が発生することで、購入者が途中で買い物を諦めてしまう「カゴ落ち（離脱）」が発生する。株式会社YTGATEの調査によると、EMV3-DSを導入済みのEC事業者のうち78.6%が「導入後にカゴ落ちが増えたと感じている」と回答している。

課題2：カード会社（イシュー）側での不正利用検知強化による「決済承認率の低下」
EMV3-DS導入前後で、カード会社判断による決済否認が増え、決済承認率が低下している。これにより、取引が承認されるべき正規ユーザーの決済まで拒否され、加盟店にとっては売り上げの損失につながる事が想定される。（詳細は「2-(3)-1. EMV 3-Dセキュア導入後のカード承認率低下と対策による改善効果」）従来、カード不正利用による損失負担は加盟店側の責任としてチャージバック（売上取消し）が行われることが大半であったが、EMV3-DSによる認証を行った取引で不正利用が発生した場合の損失負担の責任は、原則イシューとなる。そのため、イシューはEMV3-DS認証を行った取引の場合、少しでも不正利用リスクがあると、与信枠が足りている場合でも取引を保留したり拒否したりする傾向が強くなっていると想定される。

用語解説：決済承認率

クレジットカードなどの決済要求のうち、カード会社や決済事業者によって承認され、正常に決済が成立した割合を指す。一般には「承認された決済件数 ÷ 決済要求件数」で算出する。カードの利用限度額超過や有効期限切れ、不正利用検知などによって承認されない場合、承認率は低下する。EC事業者にとっては売上機会に直結する指標であり、不正対策を強化しすぎると正規利用者の決済まで拒否され、承認率が低下することがある。そのため、不正利用の抑止と決済承認率の維持を両立させることが重要となる。

4. 今後のEC事業者に求められる対策：EMV 3-Dセキュア運用パターンの最適化

『セキュリティガイドライン6.1』では、EC加盟店に対して原則として決済の都度EMV3-DSによる認証を行うことを求めている。だが、運用上はEMV3-DS以外に導入する不正

利用対策の内容や効果に応じて、加盟店の不正リスク判断のもと一部の取引にのみEMV3-DSによる認証を行うことも認めている。『セキュリティガイドライン』の附属文書である『EMV 3-Dセキュア導入ガイド』では、導入パターンを図2-14のように整理している。

▼図2-14 EMV 3-Dセキュアの導入パターン

パターン	EMV 3-Dセキュアの具体的な運用	
	カード番号登録時	決済の都度
①	加盟店のリスク判断によりEMV 3-Dセキュアによる認証を行う場合	加盟店が網羅的に行う不正利用対策が、EMV 3-Dセキュアと同等以上の不正抑止効果があることを前提として、加盟店の不正リスク判断によって必要な場合にEMV 3-Dセキュアによる認証を行う。
②	カード番号登録時にEMV 3-Dセキュアによる認証を行う場合	アカウント等の厳格な管理及び不正ログイン対策を講じた上で、ログインが行われる際にアカウント等の利用者であることの確認を行う。 EMV 3-Dセキュアによる認証を行う。 加盟店の不正リスク判断によって必要な場合にEMV 3-Dセキュアによる認証を行う。
③	決済の都度、EMV 3-Dセキュアによる認証を行う場合	EMV 3-Dセキュアによる認証を行うことを推奨する。 EMV 3-Dセキュアによる認証を行う。
-	加盟店起点の取引における例外	初回決済時やカード番号登録時等にEMV 3-Dセキュアによる認証を行う。ただし、顧客からの契約内容の変更の申出、購入商品・サービスの追加等の顧客接点が生じた場合には認証を行う。

※加盟店起点の取引：初回にカード情報を顧客が登録した後、加盟店側のトリガーで行われる取引。継続課金、オートチャージ、事前予約後の金額確定時の決済などが該当する。

パターン① 加盟店のリスク判断によりEMV3-DSによる認証を行う場合

カード番号登録時・都度決済時とも加盟店の不正リスク判断によって必要な取引にのみEMV3-DS認証を行う。以下を満たすことが条件となる。

- 1) 決済前・決済時・決済後の全ての場面で、網羅的な不正利用対策を講じる。
- 2) 自社のデータを用いた属性・行動分析による不正リスク判断を行う。
- 3) 24時間365日継続的なセキュリティ対策の実施を行うための専門部署設置や専任担当者の配置などを行う。
- 4) 契約している全てのアクワイアラおよびPSPの理解を得る。

EC事業者にとって、カゴ落ちなどの売上損失リスクは最も低い形態だが、前提となるセキュリティ対策の負担が重いパターンとなる。特にセキュリティ対策専門部署や専

任担当者の配置は多くのEC加盟店にとって困難であることが想定される。

パターン② カード番号登録時にEMV3-DSによる認証を行う場合

不正ログイン対策およびアカウントの厳格な管理を講じることを前提とする。初回カード登録時にはEMV3-DSによる認証を行い、都度決済時には加盟店の不正利用へのリスク判断によって必要な取引にのみEMV3-DS認証を行う。初回カード登録時の本人認証を確実にすることで不正利用のリスクを減らし、決済時のEMV3-DSの認証を最小限とすることができる。EC加盟店にとっては、セキュリティ強化と売上損失リスク低減のバランスを取りやすい。

パターン③ 決済の都度EMV3-DSによる認証を行う場合

原則通り全ての取引にEMV3-DSによる認証を行うパターンである。EC加盟店にとっては、最も不正利用防止の観点で安全だが、カゴ落ちなどの売上損失リスクは他パターンと比較し大きい。

EMV3-DSを一律に導入・運用するだけでは、セキュリティ強化とカゴ落ちなど売上損失の回避を両立することが困難になっている。セキュリティを強化しつつ売上損失を

最小化するために、ログイン時の認証強化、不正利用検知システムの活用、社内体制整備と併せて対策することにより、パターン①やパターン②の運用が可能となる。

(3) カード決済承認率改善の取り組み

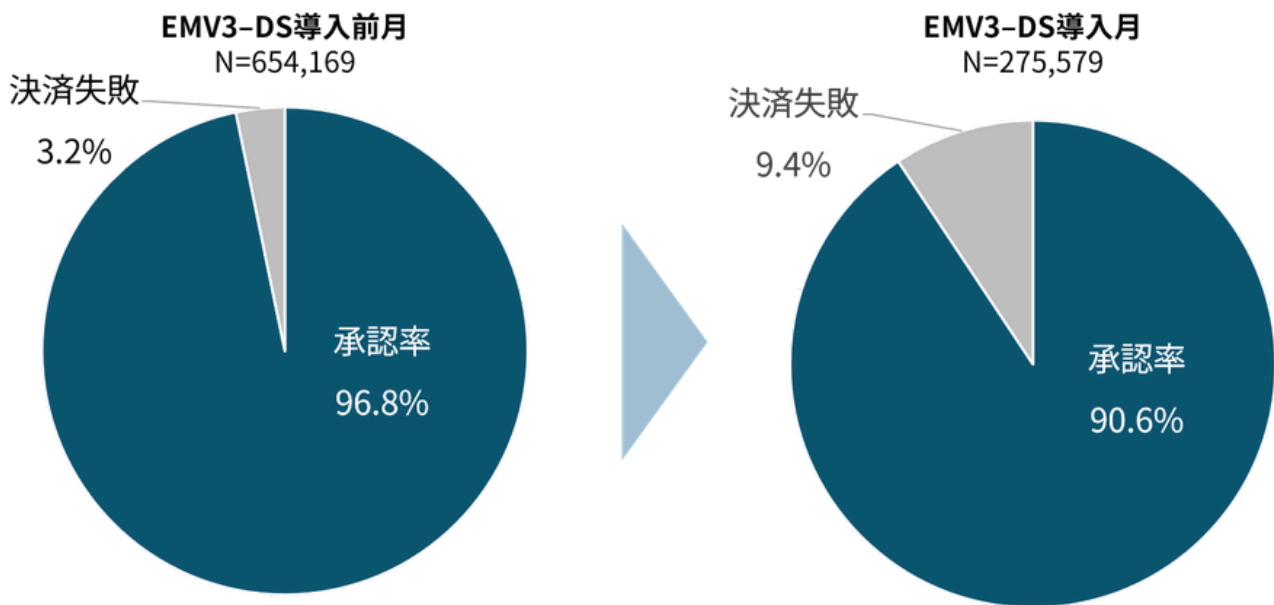
(3)-1. EMV 3-Dセキュア導入後のカード承認率低下と対策による改善効果

株式会社YTGATE（以下YTGATE）の協力を得て、EMV 3-Dセキュア（以下EMV3-DS）導入前後のEC加盟店におけるカード決済承認率の変化について分析する。

1. EMV 3-Dセキュア導入前後の決済承認率の変化

2社（P社・Q社）のEC事業者の延べ約170万件の決済データのうち、EMV3-DS導入月とその前月のカード決済承認率を比較した。EMV3-DS導入前月のカード決済承認率は96.8%に対し、導入月のカード決済承認率は90.6%と6.2ポイントの低下が見られた（図2-15）。

▼図2-15 EMV 3-Dセキュア導入前後の承認率の変化



YTGATE提供データをもとに作成

2. カード決済承認率低下の要因

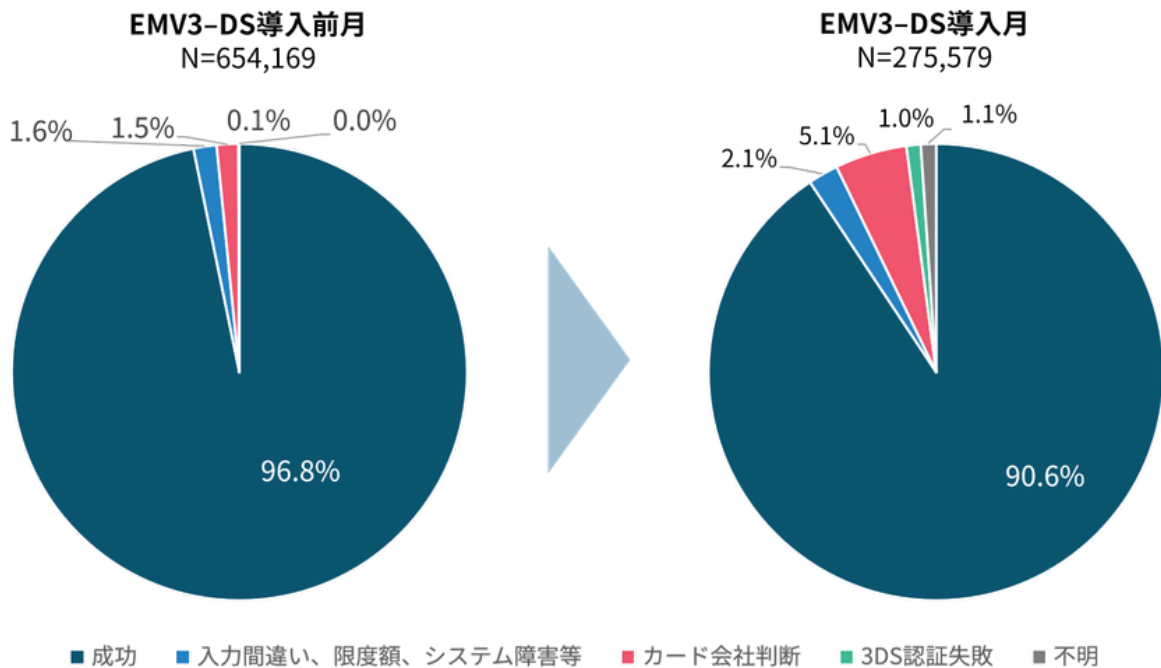
この2社について、決済失敗時のエラーコード（オーソリゼーション要求に対して決済代行事業者から返送されるコード）別にオーソリゼーション否認の理由について分析した。EMV3-DS導入前月と導入月を比較すると、否認理由で最も増加したのは、カード発行会社（イシュア）判断による否認であり、その割合は1.5%から5.1%とおおよそ3.5倍に増加した。

また、EMV3-DS導入月には、エラーコードが得られな

った取引の割合が1.1%を占めた（グラフ中では「不明」として表示）。これは決済が行われたにもかかわらずエラーコードの戻り値が得られなかったもので、EMV3-DSのワンタイムパスワードの未入力など、決済操作の途中で離脱した「カゴ落ち」によるものである可能性が高いと推測される（図2-16）。

以上から、EMV3-DS導入後にはカード決済承認率が低下することがわかる。その主な要因は、カード会社判断による否認の割合の上昇である。

▼図2-16 決済エラーの理由内訳の変化



YTGATE提供データをもとに作成

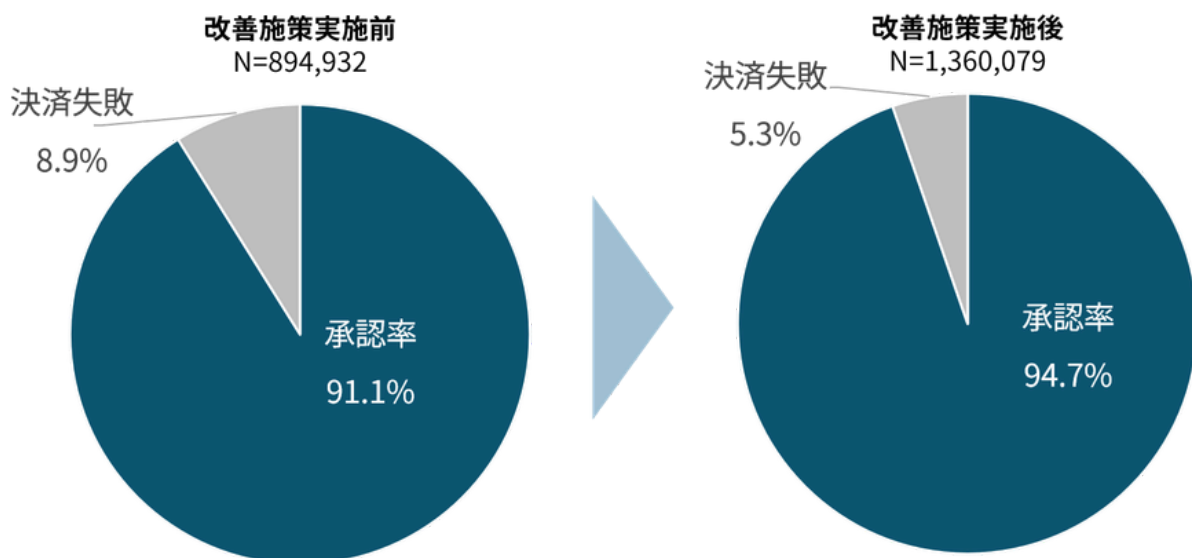
3. 承認率改善対策の効果

加盟店にとって決済承認率は売上機会に直結する重要な指標である。YTGATEでは、EC加盟店向けの決済承認率改善サービスとして、決済承認率を 이슈ア別に集計、分析し、承認率が低下した 이슈アに重点的な働きかけを行い、承認率の改善の助言を行っている。今回、同社のサービスを利用した3社（R社・S社・T社）の延べ約226万件の決済データについて分析した。

■決済承認率改善施策実施前後の比較

3社の改善施策の導入前の3ヵ月間の決済件数・承認件数と施策導入後の3ヵ月間の決済件数・承認件数を用いて、決済承認率を比較した。施策導入前の決済承認率は91.1%であったのに対し、施策導入後の決済承認率は94.7%と、3.6ポイントの改善が見られた（図2-17）。

▼図2-17 決済承認率改善施策実施前後の承認率の変化



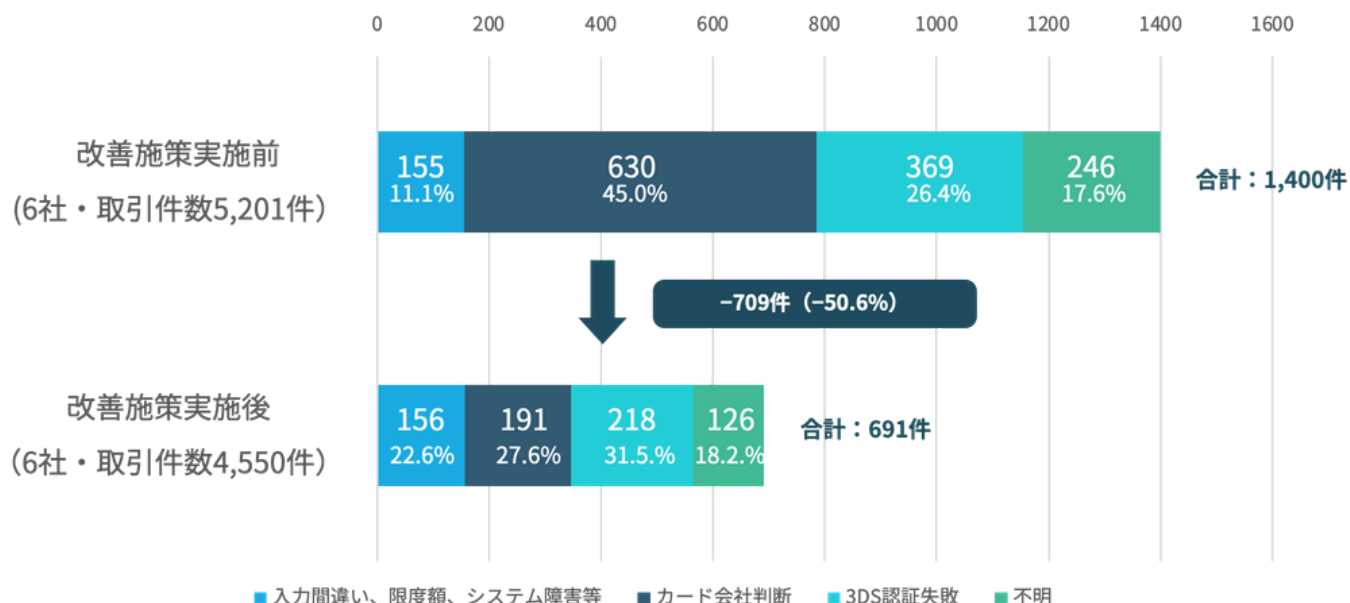
YTGATE提供データをもとに作成

■調整を行った 이슈アにおける決済エラー内訳の変化

3社のうち2社（R社・S社）については、調整を行った 이슈ア延べ6社のエラー内訳の変化についても分析した。決済承認率の改善対策実施前の「カード会社判断」の割合

は、630件から191件に減った。エラーに占める割合も45.0%と半分近くを占めていたが、実施後は27.6%と3分の1弱まで低下している。また、EMV3-DS認証失敗、およびカゴ落ちと推測される「不明」についてもそれぞれ件数が減っている（図2-18）。

▼図2-18 調整を行ったイシューにおける決済エラー内訳の変化



YTGATE社では、イシューとの調整時に、イシュー判断によるEMV3-DS認証エラーを減らすための処置を依頼している。また、EC加盟店に対しても、ECサイトのユーザーインターフェイス上での挙動を確認し、カゴ落ちを防ぐための改善点についてアドバイスを行なっている。

結果、入力間違い等のエラー件数がほぼ同じにもかかわらず、イシュー判断、EMV3-DS認証失敗、カゴ落ちによる決済エラー件数が大きく減少した。イシューとの調整では、加盟店が不正利用対策を行い、それを説明する必要がある。EMV3-DSに加えて、不正利用検知システムなどの重層的な対策を行い、不正利用の抑止効果を確認した上でイシューと調整を行うことが求められる。

(3)-2. ジュエリーブランドECサイトにおける決済承認率改善事例

Caccoの「O-PLUX」ユーザー企業である株式会社エフ・ディ・シー・プロダクツ（以下FDCP社）における決済承認率改善事例を紹介する。同社はジュエリーブランド「4℃」などを展開する。ファッションジュエリーからプラチナやダイヤモンドを使用したブライダルリングまで幅広いラインナップを持ち、20代から50代の幅広い年齢層の顧客に支持されている。

金、銀、プラチナを使用するジュエリー製品は換金性が高く、不正利用のターゲットになりやすい。FDCP社では2018年から3Dセキュア1.0を導入して不正利用対策に取り組み、EMV3-DSの導入にもいち早く対応した。一方で、決済承認率の低下はEC加盟店にとって気づきにくい課題である。カード決済に失敗した顧客の多くはその場で購入を諦めて離脱（カゴ落ち）してしまうため、事業者側から見れば売上機会の損失が可視化されないまま進行していることが多い。また、不正利用対策の効果はチャージバック金額

の抑制で評価されることが多く、決済が通らなかった取引には目が向きにくいという事情もある。同社では、カスタマーサポート（以下CS）に寄せられる「注文が完了しない」「クレジットカードエラーが出る」といった問い合わせが増加していた。そして同時にEC業界全体でクレジットカード不正利用被害が拡大傾向にあった市場環境もふまえ、これらCSへの声と業界的な不正増加トレンドという二つの兆候を捉え、両者の関連性を検討するところから取り組みを開始した。

■CSの問い合わせを日々把握・連携する体制で問題を把握

同社ではチーム内にメール・電話のCS窓口を持ち、毎朝の会議や定例ミーティングの中で問い合わせ事例が共有されていた。担当者はその中から決済関連の問い合わせの増加を察知し、詳細の調査に着手した。特別な不正利用対策という枠組みを超えて、CSに届く顧客の声を日々把握し、関係者間で連携していたことが早期の気づきにつながった点は、多くのEC事業者にとって参考になる。

■不正利用被害の抑制と売上向上をセットで説明し、社内合意形成

対策の実施に先立ち、担当者は社内の合意形成に取り組んだ。まず前提として自社の現状の決済の内訳を整理するとともに、EC市場全体でクレジットカード不正利用被害が右肩上がりに増加して業界課題となっている背景やカード決済においては個別の取引ごとにカード発行会社による決済承認が必要であるといった一般的な知識を社内に説明した。そのうえで、自社の商材が不正利用に狙われやすいことや、CSに実際に届いている顧客の声を具体例として提示した。その帰結として、セキュリティ対策（不正利用被害の抑制）と決済承認率の改善（売上向上）を一体のものと

して説明することで、経営層や関連部署の理解を得た。

セキュリティ強化を単独のコストとしてではなく、CVR（コンバージョン率）の改善と結び付けて位置付けた点が、合意形成を進めるうえでの要点となった。

■不正検知サービス「O-PLUX」の導入で決済承認率が約10ポイント向上

不正利用の増加と決済関連の問い合わせ増加に関連性があると考えた同社は、まず、不正利用対策として、不正検知サービス「O-PLUX」を導入した。オーソリゼーションやEMV3-DSによる認証の前段で、「O-PLUX」の属性・行動分析のロジックを用いて不正利用のリスクが高い取引を遮断している。導入の結果、不正利用被害が大幅に減少すると同時に、決済承認率も約10ポイント向上した。あらかじめ不正利用リスクが高い取引を除外することで、EMV3-DSのリスクベース認証で追加認証が必要と判定される取引の割合が相対的に低下し、顧客の利便性向上とカゴ落ちの抑制につながったことが要因として考えられる。今後は不正利用対策と顧客利便性の両立に向け、不正リスクに応じた柔軟な認証フロー（前述のEMV3-DSの最適な運用パターン）への継続的な改善を目指している。

■カード会社への個別交渉を実施

決済承認率を詳細に分析するために 이슈アごとに決済承認率を確認したところ、一部の 이슈アで承認率が低下していることが明らかになった。そこで、当該 이슈アに対して個別に対応を求める交渉を行った。この交渉が可能になったのは、不正利用検知システムを導入していたからといっても過言ではない。加盟店側で不正利用対策を講じ、その実績をデータとして示せることが、 이슈アとの建設的な協議の出発点となった。

■考察

不正利用対策と売上向上は、いずれか一方を優先すればもう一方が犠牲になるトレードオフとして語られやすい。しかしFDCP社の事例では、不正利用対策によってまず取引の健全性を高めたことが、決済承認率の向上につながり、結果として 이슈アとの協議を可能にした。顧客接点であるCSからの情報を起点に、社内合意形成、不正利用検知システムの導入、 이슈アとの協議までを一つの流れとしてつないだ点は、多くのEC事業者にとって参考になる。

(4) カード不正利用のトピック

ECにおける不正利用対策というと、決済時の本人認証や不正注文の検知が注目されがちである。しかし、ECをめぐる不正は、利用者がECサイトにアクセスした時点から始まるとは限らない。なりすまし広告を入口として、本人認証情報の窃取を経て、正規ECサイトでカードの不正利用を成立させるスキームを取り上げる。続いて、広告主側の資金流出につながるアドフラウドについて解説する。

(4)-1. なりすまし広告を入り口とした本人認証の悪用による不正利用

SNSや検索サービスなどのインターネット広告を悪用し、実在する企業やブランドなどになりすまして利用者を偽サイトへ誘導する「なりすまし広告」が大きな問題となっている。こうした広告は、偽の商品を購入させたり、商品代金をだまし取ったりするためだけに利用されるものではない。偽ECサイトで利用者にカード情報を入力させ、攻撃者が中間者攻撃によってカード情報やログイン情報を詐取するとともに、EMV3-DSのワンタイムパスワードなどカ

ード決済の本人認証を窃取し、不正利用する手口も存在する。EC事業者にとって、なりすまし広告はブランド保護や消費者保護だけの問題ではなく、カード情報の窃取や不正利用につながる上流リスクとしても捉える必要がある。

■政府のモニタリングでも「なりすまし広告」が重点課題に

なりすまし広告の問題は、政府においてもデジタル広告市場の重要な課題の一つとして継続的に取り上げられている。経済産業省は、デジタルプラットフォーム取引透明化法に基づき、Google、Meta、LINEやフーなどの大手デジタル広告プラットフォームに対して、広告主など利用事業者との取引やサービス運営の透明性・公正性を継続的に評価する「モニタリング・レビュー」を実施している。2025年度には「なりすまし広告への対応」が重点的な検討テーマの一つとなり、広告主の本人確認や広告審査、広告掲載後の対応などについて、プラットフォーム事業者への質問や評価が行われた。2026年度もモニタリングが継続されている。

用語解説：デジタルプラットフォーム取引透明化法

正式名称は『特定デジタルプラットフォームの透明性及び公正性の向上に関する法律』（2021年2月1日施行）。経済産業省が所管し、一定規模以上のデジタルプラットフォーム提供事業者を「特定デジタルプラットフォーム提供者」として指定したうえで、利用事業者に対する提供条件等の情報開示、苦情処理を含む手続・体制の整備、および運営状況の年次報告を義務付ける。総合物販オンラインモール分野とデジタル広告分野が対象であり、アプリストア分野は2025年12月にスマホソフトウェア競争促進法へ移管された。

経済産業省がモニタリングのために実施した広告主等へのアンケートでは、1,000回答のうち169回答、16.9%が過去1年程度の間に「なりすまし広告」の被害を受けたと回答した。また、経済産業省が設置するデジタルプラットフォーム取引相談窓口が2024年度に受け付けた1,274件の相談のうち、138件がなりすまし広告に関するものであった。なりすまし広告というと、著名人を騙って投資詐欺へ誘導する広告が目立ちがちである。しかし、経済産業省が2025年度に公表した『2025年度 デジタルプラットフォームの透明性・公正性に関する評価（デジタル広告分野）』では、実在する企業や法人の役員になりすます広告も存在することが述べられている。また著名企業や商品のロゴ・ブランドを無断で広告に使用し、その企業とは無関係なECサイト等へ誘導して、利用者に正規の商品であると誤認さ

せて購入させる事例も確認されているという。デジタルプラットフォーム取引相談窓口には、広告だけでなくリンク先のWebサイトまで偽装されているケースについて、広告とリンク先コンテンツ双方の審査強化を求める相談も寄せられている。つまり、不正な広告と偽サイトを組み合わせることで利用者を誘導する手口は、広告主やブランド企業にとって現実の問題となっている。

国民生活センターが2025年7月に公表した『国民生活センターADRの実施状況と結果概要について』では、SNS広告から誘導された偽通販サイトでカード情報とEMV3-DSのワンタイムパスワード（OTP）を入力させ、それらを別の正規オンラインストアでの取引にリアルタイムで利用するという中間者攻撃の手口が示されている。（2-(1)-2. 用語解説を参照）

用語解説：国民生活センターADR

正式名称は「重要消費者紛争解決手続」。独立行政法人国民生活センター法に基づき2009年4月に設置された「紛争解決委員会」が実施する裁判外紛争解決手続（ADR）で、消費者と事業者の間の紛争のうち、全国的に重要性を有するもの（重要消費者紛争）を対象とする。当事者の申請を受け、消費生活や法律の分野に知見を持つ委員が「和解の仲介」または「仲裁」を行い、訴訟によらない迅速・簡便な解決を図る。手続自体は非公開であるが、同種被害の防止・救済に資する観点から、事案の内容と結果の概要は公表することとされている。

この事案では、消費者がSNS上の広告から通販サイトへアクセスし、通常価格の半額で販売されている商品を購入しようとした。カード情報を入力したものの注文は完了せず、別のカード情報を入力すると、カード発行会社（イシュー）からSMSでEMV3-DSのワンタイムパスワードが届いたため、それも当該通販サイトに入力した。しかし、やはり注文は成立しなかった。その後、2回目に入力したカードが不正利用され、本人に身に覚えのない約3万円のテーマパークのチケットが別のオンラインストアで購入されていたことが判明した。

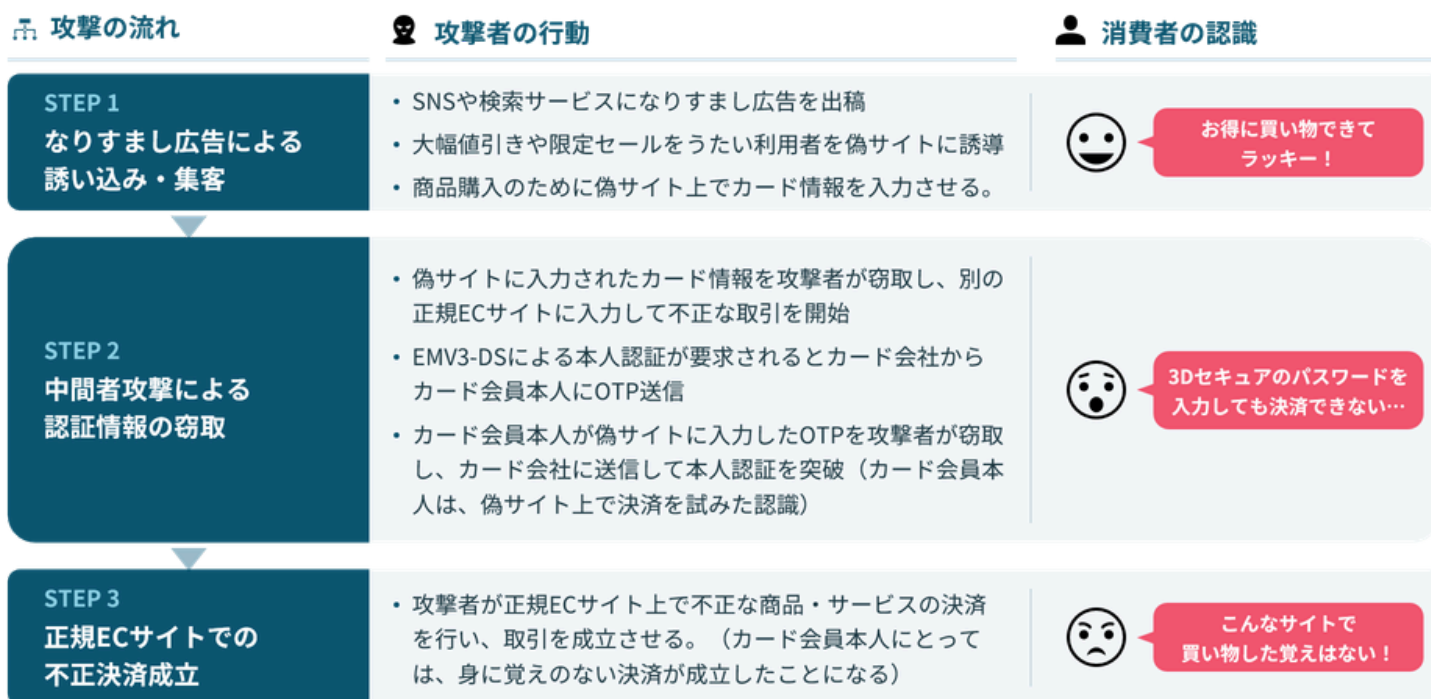
本件については、利用したカード会員が申請人となってイシューに対して決済キャンセルの申立てが行われた。しかし当該イシューは、SMSで送付したEMV3-DSのOTPが正しく入力されていることから、カード利用者がパスワード管理責任に違反したとしてキャンセルを認めないとしてい

た。一方で当該イシューからカード利用者に送られたSMSには、カード会社の名称、OTPとその有効期限は記載されていたものの、決済金額が記載されていなかった。このことから国民生活センターADRの仲介委員は、カード会員が決済金額を確認することができないまま、偽通販サイトにOTPを入力したと考えた。そのためイシュー側にも一定の責任はあるとして、カード会員とイシューで不正利用金額を半額ずつ負担するという解決案を示し、両者はこれを受け入れ、和解した。

■なりすまし広告から不正利用に至る流れと各段階における注意点

なりすまし広告を起点としてカード不正利用につながる流れと、EC事業者の対策ポイントについて整理する（図2-19）。

▼図2-19 なりすまし広告から不正利用への流れ



ステップ1：なりすまし広告による誘い込み・集客

攻撃者は、SNSや検索サービスなどに、実在する企業やブランドを装った広告を掲載し、大幅な値引きや限定セールなどをうたって利用者を偽のECサイトへ誘導する。広告だけでなく、誘導先のWebサイトも正規の通販サイトに似せて作られることがあり、利用者が正規サイトであると誤認したまま商品の購入手続へ進んでしまう。この段階の目的は、単に偽商品を購入させたり商品代金をだまし取ったりすることだけではない。商品の購入手続に見せかけてカード情報を入力させ、さらにカード決済に必要なEMV3-DSなどの本人認証を行わせるための入口として利用される場合がある。

⚠️ EC事業者の対策ポイント

自社名、ブランド名、ロゴ、商品画像などが偽広告や偽サイトに悪用されていないかを把握し、発見した場合には広告プラットフォーム等への削除申請を行うことが重要である。また、自社の公式サイトやSNS等を通じて、偽広告・偽サイトについて利用者に注意喚起することも有効である。

ステップ2：中間者攻撃によるカード情報、本人認証情報の窃取

偽ECサイトに入力されたカード情報を取得した攻撃者は、その情報を別の正規ECサイトに入力して不正な取引を開始する。正規サイト側でEMV3-DSの本人認証が要求されると、イシュアからカード会員の予め登録した携帯電話番号にOTPが送信される。攻撃者は、このOTPも偽ECサイト上で利用者に入力させ、即座に正規ECサイトへ中継する。

利用者は偽ECサイトでの商品購入の決済のため、本人認証しているつもりであるが、実際には攻撃者が別の正規ECサイトで行っている取引の本人認証を成立させている。

⚠️ EC事業者の対策ポイント

カード決済の本人認証を導入していても、EMV3-DSのOTPがリアルタイムに中継されることで、本人が意図していない取引の認証が成立する場合がある。そのため、EMV3-DSの本人認証の成功だけをもって取引を安全と判断せず、不正利用検知システムと組み合わせた重層的な対策が有効である。

⚠️ カード会社（イシュア）の対策ポイント

EMV3-DSの本人認証にOTPを利用する場合、中間者攻撃によってOTPが攻撃者へ中継される可能性がある。このため、EMV3-DSの本人認証にOTPではなく、パスキーなどのフィッシング耐性のある認証方式を採用することが有効である。パスキーによる認証では、中間者攻撃は理論上成立しない。また、OTPを通知する場合には、決済金額や加盟店名などの取引情報を併せて表示することで、利用者が自分の意図した取引と異なることに気づきやすくなる。前述の事案でも、イシュアから送信されたSMSに決済金額が記載されていなかったことが、国民生活センターADRの仲介委員の判断材料となった。

ステップ3：正規ECサイト側での不正利用成立

ステップ2でEMV3-DSのOTPの窃取に成功すると、攻撃者は正規ECサイト上で不正な商品・サービスの購入を成立させる。この手口で重要なのは、正規ECサイト側ではEMV3-DSの本人認証が正常に完了しているように見える点である。正しいカード情報が入力され、カード会員本人に送信されたEMV3-DSのOTPも正しく入力されている。そのため、本人認証に成功したという事実だけでは、不正利用を判別することは難しい。しかし実際には、カード会員が認証したつもり取引と、正規ECサイトで成立した取引は異なっている。すなわち、「本人認証に成功したこと」と「本人がその取引を意図していること」は必ずしも一致しない。

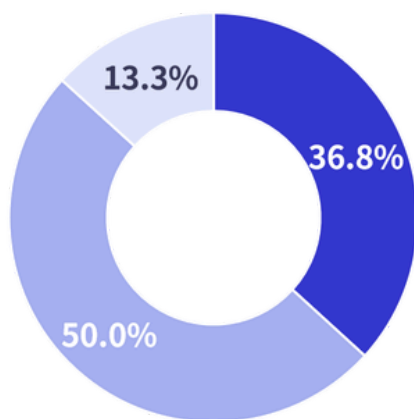
⚠️EC事業者の対策ポイント

本人認証の成功だけをもって安全な取引と判断せず、不正利用検知システムを利用し、IPアドレス、端末情報、配送先住所、電話番号、購入商品、購入金額、過去の取引履歴などを組み合わせて取引リスクを判定することが有効である。特に高額商品や換金性の高い商品の注文では、決済が正常に完了している場合でも、通常とは異なる取引であれば出荷保留や追加確認などを行う決済後の対策も求められる。

このように、なりすまし広告や偽ECサイトを利用した攻撃では、カード情報を詐取されるだけでなく、EMV3-DSのOTPも攻撃者の不正取引に利用される場合がある。

▼図2-20 アドフラウドの被害経験

n=400 | SA(単一回答)



■ 経験あり ■ 経験なし ■ 分からない

アドフラウド実態調査（Cacco調べ）2026年4月

被害経験者がアドフラウドによって詐取されたとする広告費の割合は、「1～5%未満」が27.9%、「5～10%未満」が26.5%、「10～20%未満」が23.8%であり、これらを合わせると約8割を占めた。広告費の一部が不正な広告トラフィックに対して支払われている可能性があることを示す結果である。

そのため、本人認証に成功しているという事実だけで、その決済が本人の意思によるものと判断することは難しい。EMV3-DSなどによる本人認証は不正利用対策の重要な要素である一方、利用者が意図した取引とは別の決済の認証に悪用される可能性も考慮し、ログイン、注文から決済、出荷までの情報を組み合わせて不正利用を検知することが有効である。

(4)-2. 集客フェーズに潜むもう一つの脅威：アドフラウド（広告不正）

アドフラウドとは、botなどを用いて、人が実際に閲覧・クリックしていないにもかかわらず、インプレッション（表示）やクリック、偽のコンバージョン（会員登録や申込）を機械的に大量発生させたり、不正なサイトへの広告配信を発生させることで、広告主が支払う広告費を不正に詐取する手口である。日本インタラクティブ広告協会（JIAA）は、アドフラウドを「広告費を欺瞞的に詐取することを目的とした不正」と位置付けており、個人や国内外の悪質事業者への不正な広告費の流出を防ぐ必要性を指摘している。

■独自データで見るアドフラウドの実態

Caccoが2026年4月にWeb広告運用に携わる担当者400名を対象として実施した『2026年版 ネット広告不正（アドフラウド）に関する実態調査』では、Web広告を出稿しているEC事業者のうち、36.8%が「アドフラウドの被害を経験したことがある」と回答した（図2-20）。

36.8%

被害経験あり

回答者の約3人に1人が経験

- 経験したことがある（36.8%・147件）
- 経験したことがない（50.0%・200件）
- 分からない（13.3%・53件）

「分からない」13.3%は、被害に気づいていない可能性を含む潜在リスク層

アドフラウドによる直接的な被害は広告費の損失であるが、それだけにとどまらない。不正なクリックやインプレッションが広告実績に混入すれば、広告効果を示す指標も実態から乖離し、広告予算の配分や施策の評価を誤らせる可能性がある。

■広告費が犯罪収益となるケースも

さらに注意すべきなのは、詐取された広告費の行き先である。インターネット広告は国境を越えて配信・取引されており、日本の企業が広告主であるからといって、不正を行う主体や広告費の流出先が国内にあるとは限らない。海外では、大規模なアドフラウドによって得た収益が、複数国の銀行口座を介して移転・洗浄された事件も摘発されている。代表的な事例が、2014年から2016年にかけて行われ、2018年に米司法省が摘発・起訴を公表した「Methbot」と呼ばれるデジタル広告詐欺である。攻撃者は広告ネットワークを運営しているように装い、データセンター上のコンピュータなどを使って、人間が広告を閲覧しているかのような大量の偽トラフィックを生成した。米国の広告主、広告メディア、広告プラットフォームなどが実際には人間に閲覧されていない広告に対して、700万ドルを超える広告費を支払っていた。

主犯は、その犯罪収益をブルガリア、ロシア、英国、チェコ、ラトビア、キプロスなど複数国の個人・法人銀行口

座を介して移転していた。起訴状では、広告ネットワークからチェコの法人銀行口座に入金された資金の一部を不正スキームの運営費に支出するとともに、540万ドルをニュージーランドの法人銀行口座へ移転していたことも明らかにされている。主犯は通信詐欺に加えて、マネーロンダリング共謀およびマネーロンダリングでも有罪となり、2021年に禁錮10年の判決を受けた。

■「広告の無駄」ではなく、不正な資金流出として捉える

アドフラウドは、カードの不正利用などとは異なり、キャッシュレス決済そのものを直接攻撃する手口ではない。しかし、企業が正規の取引として支払った資金が犯罪者側へ流出し、その収益がさらに移転・洗浄される可能性があるという点では、不正な資金流出という側面を持つ。EC事業者には、決済領域だけでなく、広告を含む事業活動全体を通じて、不正な主体への資金流出を防ぐ視点が求められる。

3. その他のキャッシュレスセキュリティのトピック

ニセ社長詐欺：メッセージングアプリを利用するビジネス詐欺の手口

2025年のインターネットバンキングに係る不正送金の被害総額は約103億9,700万円、発生件数は4,747件であり、手口の約9割をフィッシングが占める。

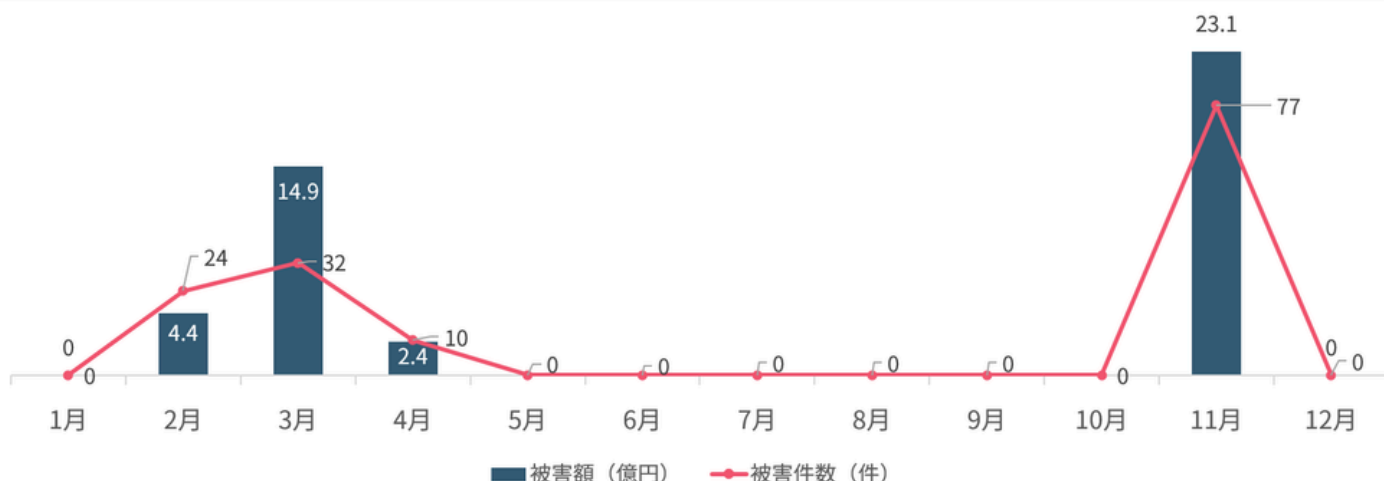
このうち法人の被害額は47億円と前年の約4倍に達し、

被害総額に占める法人の割合は前年の約13%から約45%へと大きく上昇した。警察庁は、この背景として、ボイスフィッシングによる法人口座の不正送金被害が急増したことを挙げている（図3-1）。

用語解説：ボイスフィッシング

電話を用いて金融機関や官公庁、取引先の担当者などを装い、認証情報の聴取や送金操作を誘導する手口。英語のVoiceとPhishingを合わせたvishing（ビッシング）とも呼ばれる。法人口座を狙うケースでは、銀行の担当者やセキュリティ部門を名乗る電話で、法人インターネットバンキングのID・パスワードやワンタイムパスワードを聞き出したり、電子証明書の再発行や特定のソフトウェアの導入を指示したりする。メールやSMSと組み合わせて用いられることも多く、先にSMSで偽サイトへ誘導してから電話でワンタイムパスワードを聞き出すといった使い分けが見られる。電話はメールと異なり、本文の内容を基にしたフィルタリングで機械的に遮断することが難しい。また、相手とリアルタイムにやりとりしながら心理的に圧力をかけられるため、有効期限の短いワンタイムパスワードであってもその場で使われてしまいやすい。認証手段を追加するだけでは防ぎきれず、電話で認証情報を尋ねられても伝えないという社内ルールの周知と、送金時の第三者確認プロセスが対策の要となる。

▼図3-1 ボイスフィッシングによる法人口座の不正送金被害件数と被害額（2025年）



出所：警察庁サイバー警察局『令和7年におけるサイバー空間をめぐる脅威の情勢等について』（2026年3月）

2025年11月には新潟県内の企業で約1億9,000万円、滋賀県内の19事業所で計約3億5,000万円の被害が発生した。滋賀の事件では、2026年7月までに犯罪収益移転防止法違反等の容疑で5人が逮捕されており、盗まれた資金が法人名義の口座を経由した後、暗号資産に変換されて海外の取引所へ送金されるという資金洗浄の手口も明らかになっている。

こうした電話を起点として法人を狙うボイスフィッシングが継続する一方、2025年12月以降、CEOや社長になりすましたメールを起点にLINEなどのメッセージングアプリへ誘導する新しい法人を狙う詐欺が国内で急増した。警察庁は「ニセ社長詐欺」として注意をよびかけている。

■被害の発生状況

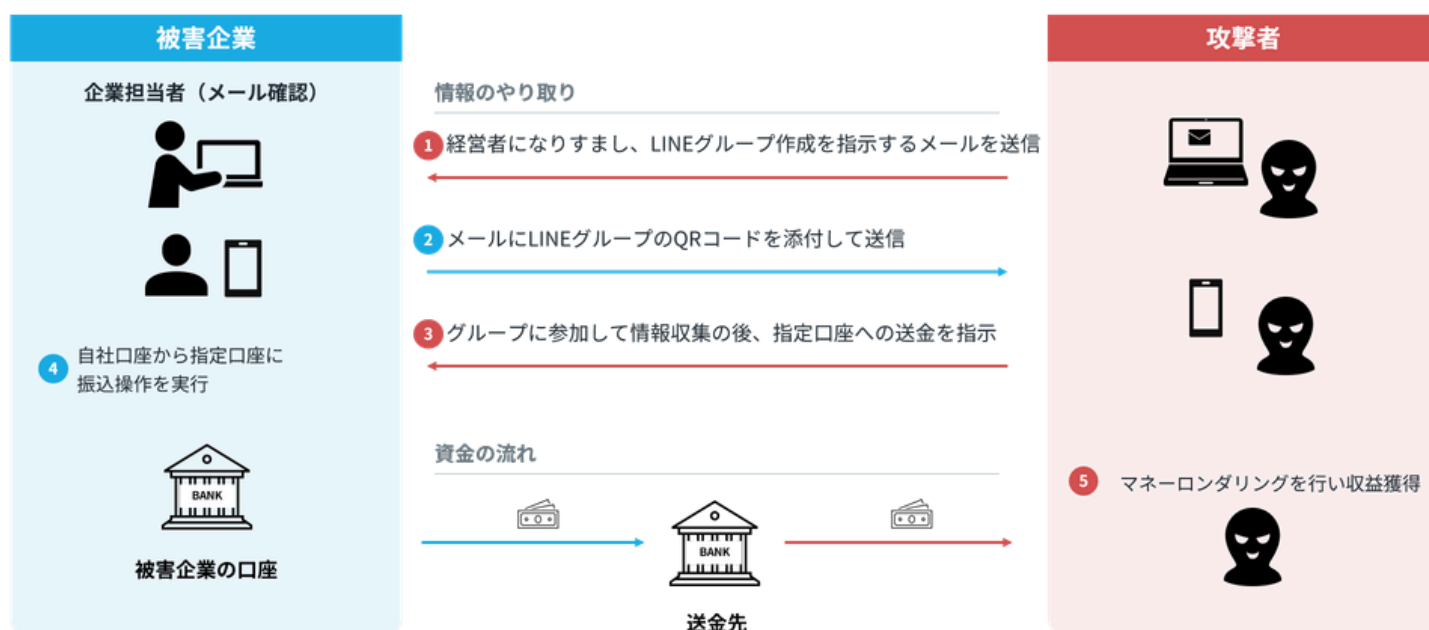
2025年12月に確認され始めて以降、ニセ社長詐欺による被害は全国で相次いでいる。警察庁の『令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について』によれば、2026年1月から6月までの半年間で認知件数127件（未遂も含む）、被害額は約38億8,000万円に上る。既遂1件あたりの被害額は約3,100万円であった。独立行政法人情報処理推進機構（IPA）には2025年12月16日から2026年3月10日までの間だけで106件の相談が寄せられている。

2026年1月上旬に公表された旅行関連プラットフォーム事業者のX社の事例では、同社代表者を装った第三者から従業員宛てにメールが届き、社外のメッセージングアプリ

のグループチャットへ誘導された。グループチャット上で虚偽の送金指示が行われ、経理担当者である従業員が銀行届出印を持ち出して銀行窓口で振込手続を行った結果、約5,000万円が第三者の指定口座へ送金された。同社グループは原則としてネットバンキングを標準的な業務フローとしていたが、例外処理である銀行窓口での振込と、それに用いる銀行届出印の管理に関する詳細な規程・承認フローが未整備であったことを根本原因として挙げている。非対面ツールを用いた緊急指示に対する真偽確認プロセスの欠落も、要因として指摘されている。

2026年3月19日に公表された金融情報メディアを運営するY社の事例では、社外関係者も参加できるビジネスチャット上で同社役職員を装った第三者から不正な送金指示が行われ、担当者が同社の従来のルールとプロセスに沿って処理した結果、9,600万円が外部口座へ送金された。X社の事案が「例外処理の規程不備」を突かれたものであったのに対し、本件は正規の業務フローを通過してもなお防げなかった点が異なる。高額送金時には電話・対面・オンラインなどによる指示の真正性の確認が、承認フローとは独立した工程として組み込まれていない限り、フローを整備するだけでは防げないことを示す事例である。

▼図3-2 典型的なCEO詐欺の流れ



■手口の流れ

この手口の典型的な流れは以下となる（図3-2）。

①経営者などになりすました攻撃者から、インターネット等で公開されている法人のグループメールアドレス宛て（例：info@company.co.jp）に電子メールでLINEなどのSNSのグループを作成するように指示が行われる。メールのFromには法人ドメイン（company.co.jp）のメールアドレスや法人名が設定されており、内容は「新規プロジェクトのため」など業務を装う。振込権限を持つ担当者をグループに含めるよう指示を受ける場合もある。

②被害企業の担当者が作成したグループへのQRコードをメールへの返信に添付する。

③攻撃者がグループに参加し、担当者とのやりとりで法人口座情報や残高などの情報収集を行う。

その後、「事業資金が至急必要だ」「取引先への支払いを至急実行してほしい」などとして、指定した口座に送金を指示する。

④振込権限を持つ担当者が自社口座から指定口座に振込操作を実施する。

⑤受け取った資金を暗号通貨に変換するなどマネーロンダリングを行い、攻撃者が収益を獲得する。

情報収集のやりとりでは、「取引先から会社に入金がある予定なので口座情報を送って欲しい」「入金があったかを確認したいので現在の口座残高を教えて欲しい」など、不自然ではないやりとりで必要な情報を聞き出す。トレンドマイクロ社の検証では、途中で関係のない雑談を挟んでも自然な応答が数分程度で返ってくることから、リアルタイムにメッセージを送れる人物もしくはシステムが関与していると推測している。

■従来型ビジネスメール詐欺との違い

ニセ社長詐欺は、従来型のビジネスメール詐欺（BEC）と比べて以下の3点で異なっている。

①メール本文の情報量を意図的に絞っている

最近のメールサーバーやセキュリティ製品は本文の内容からフィッシングメールを判別する。メールでのやりとりを最小限にして、「送金」「至急」といったフィルターにかかりやすい表現を避けることで、フィルターのすり抜けを図っていると考えられる。

②主なやりとりは組織の管理外のツール（LINE等）を利用する

LINEやChatworkなどの外部ツールでは、メールと違ってフィルタの適用が難しく、社内のシステム管理者がやりとりの内容を確認することも難しい。そのため、被害に気づきにくくなる。

③標的が無差別化している

トレンドマイクロ社は、国内で少なくとも6,000以上の法人ドメインにニセ社長詐欺のメールが送付されたことを確認しており、業種は建築、サービス業、製鉄、商社など多岐にわたる。従業員数万人規模の組織から数人規模の組織まで、規模を問わず標的になっている。

■生成AIによる攻撃の自動化で標的企業が無差別化

従来のBECは、標的企業の事前調査や継続的なやりとりに一定の対応工数を要するため、詐欺によって得られる金額の大きい大企業を標的とする手口であった。ニセ社長詐欺で標的が無差別化した背景には、攻撃側の自動化があるとみられる。トレンドマイクロ社は、本手口を行っている攻撃者グループや関連する国を断定できる情報はないとした上で、多くのメールで中国製メールソフト「Supmailer」

が使われていることを確認している。また、AI悪用の証跡として、実在の組織と社名が若干異なる宛先への送信（同社宛に「マイクロトレンド」という誤った社名で送付されていた例）や、From表示名に簡体字で「代表者未找到（代表者が見つかりません）」と表示されるケースを挙げている。組織情報の自動収集の過程で生じたエラーが、そのままの状態で送信されたものと推測されるという。こうしたエラーの痕跡そのものが、事前調査・文面作成・やりとりの自動化が進んだことを示唆している。Caccoの観測でも、生成AIにより違和感のない日本語で届くケースが増えており、文面だけで詐欺メールを判別することは困難であった。

■実際の詐欺メールの検証

実際に届いたニセ社長詐欺メールの解析から見られた特徴を紹介する。一つは、「Reply-To」ヘッダーの悪用である。Reply-Toは、返信先を送信者本人とは別のアドレスに指定するためのヘッダーで、メーリングリストの返信を運営アドレスに集約する場合など、本来は正当な目的で使われるものである。通常、メールの「返信」ボタンを押すと、表示されている送信元（From）のアドレスが宛先に入る。しかし、Reply-Toが設定されている場合、返信は送信者ではなく、そこで指定されたアドレスへ送られる。この仕組みを悪用すれば、Fromには実在するアドレスを表示させたまま、返信だけを別のアドレスに誘導することができる。

Caccoが受信した不審メールでは、表示される送信元（From）は代表者の正しいアドレスであった。しかし、実際の返信先（Reply-To）には、攻撃者が用意したフリーメールが設定されていた（図3-3）。送信元が本物に見えても、返信ボタンを押した瞬間に宛先がすり替わる仕組みであり、送信直前に宛先アドレスが、それまで表示されていたものと一致しているかを確認することが重要になる。

▼図3-3 Caccoに届いたニセ社長詐欺メール



送信元が本物に見えても、返信ボタンを押した瞬間に宛先がすり替わる。
送信直前に、宛先アドレスが「さっき表示されていたもの」と一致しているか、確認することが大切

もう一つは、プレスリリース連動型と呼べる事例である。Caccoが2025年9月に取引先（以下、Z社）と連名で公表したプレスリリースに登場した、Z社の社長名を騙るメールが、公開メールアドレス宛に2026年2月に送信された。メールの題名はZ社の社名になっており、メールソフトの画面で一覧を見ると「会社名」「社長名」が並んであたかも正規のメールのように見える。攻撃者が組織の公開情報を「なりすましのネタ」として収集し、悪用している実態がうかがえる。

■承認フローの整備と指示の真偽を確認する工程が必要

警察庁は、ニセ社長詐欺への対策として、①社内での情報共有、②送金に関するルールの再確認、③SNSグループ

の利用を指示された場合の警戒、の3点を挙げている。SNSグループに誘導された場合は、通報機能があれば通報した上で速やかにグループから退出することを推奨している。

トレンドマイクロ社は、送金など重要業務の実行時に通常の担当者以外の承認を得る、第三者確認プロセスの導入を推奨している。また、ニセ社長詐欺は名称の通り自社の社長やCEOを偽ってメールが送られてくるため、経営層に意見を言いづらい組織風土があると、何かおかしいと感じても見破ることが難しくなる可能性を指摘している。こうした運用ルールや組織風土の見直しとあわせて、DMARCなどの送信ドメイン認証を導入して自社ドメインのなりすましメールを受信側で見分ける仕組みを整えることが基本の対策となる。

用語解説：DMARC

メールの送信元ドメインが偽装されていないかを受信側で検証する仕組み。送信元のIPアドレスの正当性を検証するSPF、電子署名により送信者とメールの改ざんの有無を検証するDKIM、これらの検証に失敗したメールの取り扱い方針をドメイン所有者が宣言するDMARCの3つを組み合わせで運用する。DMARCのポリシーには「何もしない（none）」「隔離（quarantine）」「拒否（reject）」のいずれかを指定する。あわせて、自ドメインを名乗るメールの認証結果を集計したレポートを受け取ることができ、なりすましメールの送信状況を把握できる。

SPFとDKIMが検証するのは、それぞれエンベロープFromのドメインと署名ドメインであり、いずれも利用者の画面に表示されるFromヘッダーとは一致しない場合がある。この差を埋め、表示上の送信元ドメインの詐称を防ぐ役割を担うのがDMARCであり、フィッシングメール対策として特に有効とされる理由もここにある。2023年2月、経済産業省・警察庁・総務省はクレジットカード会社等に対し、DMARCの導入と、拒否ポリシーでの運用を連名で要請している。

前述の2事例からは、より実務的な示唆も得られる。X社の事案からは、例外処理（窓口振込等）にこそ承認フローの規程が及んでいないリスクがあること、Y社の事案からは、正規の業務フローを整備するだけでは防げず、指示の真正性確認を独立した工程として持つ必要があることが読み取れる。コールバックを行う場合は、相手が指示してきた電話番号ではなく、あらかじめ把握している番号にかけ直すことが基本となる。

IPAの相談件数の推移を見ると、ニセ社長詐欺の認知度は着実に広がっているものの、社内での実践的な対策（詐欺メール訓練やセキュリティ教育の実施）はいまだ一部にとどまるとの調査結果もある。周知だけでなく、承認フローの見直しや訓練といった実務的な対策へとつなげることが課題である。

4. 制度・政策の動向

(1) SCS評価制度の概要と必要な対策

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）を公表した。企業のセキュリティ対策の実施状況を星（★）の数で可視化し、取引先の選定や委託先管理の判断材料とする仕組みであり、2026年度末頃の申請受付開始が予定されている。

カード情報や個人情報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つ。本制度は、イシュー・アクワイアラ・コード決済事業者・決済代行事業者（PSP）・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る。本節では制度の概要を整理したうえで、特にキャッシュレスサービスに関係する各事業者にとって実務上の影響が大きい事項について解説する。

(1)-1. 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として侵入するサプライチェーン攻撃が増加している。独立行政法人情報処理推進機構（IPA）の「情報セキュリティ10大脅威」で

も、組織向けの脅威として上位に位置づけられ続けている。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Sler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る。

この状況に対して、加盟店など委託元とPSPやSlerなどの委託先の双方が課題を抱えてきた。まず、委託元にとっては、委託先のセキュリティ対策が可視化されていない。なおかつ、対策を要求したくとも、その要求が妥当なものであるかを判断することが難しい。委託先にとっては、複数の委託元からそれぞれ異なる内容の対策を求められ、その対応が過重な負担となる。とりわけ中小企業にとって、この負担は小さくない。企業ごとに満たすべき対策を提示し、その実施状況を共通の物差しで可視化する仕組みが求められていた。

(1)-2. 制度の全体像

SCS評価制度は、企業のセキュリティ対策の実施状況を★3・★4・★5の3段階で可視化する（図4-1）。

▼図4-1 段階別評価の概要

評価レベル		★3		★4		★5（検討中）
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 ・ 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 ・ 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		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 ・ 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、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
要求事項数	有効期間	26件	1年	43件	3年（毎年自己評価を実施し結果を評価機関に提出）	今後検討
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

出所：経済産業省・内閣官房国家サイバー統括室『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』（2026年3月）をもとに作成

★3は「すべてのサプライチェーン企業（2社間の契約における受注側の企業）が最低限実装すべきセキュリティ対策」と位置づけられ、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を想定脅威とする。★4は「サブ

チェーン企業が標準的に目指すべきセキュリティ対策」であり、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、機微情報の漏えい等により大きな影響をもたらす資産への攻撃を想定脅威とする。

★5は「到達点として目指すべき対策」とされ、未知の攻撃も含めた高度なサイバー攻撃を想定脅威とするが、その評価基準や評価スキームは引き続き検討中である。

留意すべきは、本制度は任意の制度であり、★取得自体を法令で義務付けるものではないという点である。また、すべての要求事項を満たさなくても直ちに商取引を止めることを求めるものではない。事業者間で求めるセキュリティ水準を分かりやすく提示し、サプライチェーン全体の底

上げを図ることが目的であって、事業者の対策レベルを競わせる「格付け制度」ではない。

(1)-3. 対象となる組織

本制度で定めるセキュリティ対策の実施主体として想定されているのは、前述のサプライチェーン企業である。ただし、対策の実施にあたり、発注者による協力が必要な場合があることから、制度が想定する制度利用者の範囲には発注企業も含む（図4-2）。

▼図4-2 制度の対象事業者（制度利用者）の範囲



出所：経済産業省・内閣官房国家サイバー統括室『制度構築方針』（2026年3月）をもとに作成

本制度は発注企業が取引先に★の取得を要請することによってサプライチェーン全体のセキュリティレベルを底上げていくことを想定している。しかし、要請にあたって価格交渉に応じない、一方的に費用を負担させるといった対応は、独占禁止法および中小受託取引適正化法（旧下請法）上、問題となり得る。要請にあたっては発注企業・受注企業の双方が必要性を理解した上でパートナーシップを構築し、セキュリティ対策に要したコストに関して価格交渉を実施することが求められる。

る。IT基盤にクラウドサービスを利用している場合は、責任共有モデルに基づき、自社の責任範囲については対策を行う。クラウド事業者側の責任範囲については、★を取得する主体がサービス提供者の対策状況を確認する必要がある。

一方、製造環境等の制御システム、発注した企業に販売する製品等はSCS評価制度の対象に含まれない。すなわち、発注企業として本制度を利用する場合、受注企業のSCS評価は、その事業者が業務のIT基盤に一定の対策を講じていることを示すものであり、納品される製品そのものの安全性を示すものではないことに留意する必要がある。ECサイトやPOSシステムなどの構築を委託する場合、成果物の安全性は従来どおり別途の確認を要する（図4-3）。

(1)-4. 対象となる範囲

対象となる範囲は、サプライチェーンを構成する企業等のIT基盤と、外部ネットワークとの境界にあたる機器であ

▼図4-3 制度の対象範囲

区分	説明
適用範囲に含まれる	IT基盤 - 特定の業務領域によらず全体の業務に共通するIT基盤を構成するサーバ群 ※インターネットに公開されたシステムは必ず含める。 ※ただし以下の「適用範囲に含めないもの」を除く。 - エンドポイント機器(パソコン、スマートデバイス等、人が使用するインターフェースを持つもの) - IT基盤を構成する親会社のシステム、クラウドサービスなど ※責任共有モデルに基づく確認を行う。
	外部ネットワーク機器 適用範囲の境界を定義するネットワーク機器（ファイアウォール、ルータ、VPN装置等） ※他組織の内部システムへ接続する際の境界を構成する機器を含む。
適用範囲に含まれない	製造環境等の制御(OT)システム 発注元等に提供する製品等

用語解説：責任共有モデル

クラウドサービスにおけるセキュリティ上の責任を、クラウド事業者と利用者で分担する考え方。一般に、クラウド事業者側はデータセンターやネットワーク、物理サーバーなど基盤部分の安全性を担う。一方、利用者側はアカウント管理やアクセス権限、データ保護、各種設定などに責任を持つ。どの範囲を事業者側が担当するかは、IaaS、PaaS、SaaSなどサービス形態によって異なる。利用するサービスごとにクラウドサービス事業者と自社の責任範囲を確認する必要がある。

PCI DSSの適用範囲はカード会員データ環境（CDE）を起点として、CDEにアクセスできるデバイスやネットワーク及びセキュリティに影響を及ぼすシステムとなるが、SCS評価制度の適用範囲はそれよりも広くなることが想定される。PCI DSSに準拠している事業者であっても、その適用範囲の外側にある資産について別途の整理が必要となる。

(1)-5. 要求事項と評価基準の構成

SCS評価制度のセキュリティ要求事項は、NISTサイバーセキュリティフレームワーク（CSF）2.0の6機能（統治・識別・防御・検知・対応・復旧）に「取引先管理」を加えた7つの大分類と16の中分類で構成されている（図4-4）。★3の取得には26項目、★4の取得には43項目の要求事項に対応する必要がある。

▼図4-4 要求事項の全体像

NIST CSF	大分類	中分類	★3	★4
統治	1. ガバナンスの整備	1-1 組織の状況	0	1
		1-2 役割、責任、権限	2	3
		1-3 ポリシー	1	1
		1-4 監督	0	1
	2. 取引先管理	2-1 サイバーセキュリティサプライチェーンリスクマネジメント	3	5
識別	3. リスクの特定	3-1 資産管理	4	5
		3-2 リスクアセスメント	0	1
防御	4. 攻撃等の防御	4-1 アイデンティティ管理、認証、アクセス制御	7	9
		4-2 意識向上とトレーニング	1	2
		4-3 データセキュリティ	1	4
		4-4 プラットフォームセキュリティ	3	5
		4-5 技術インフラのレジリエンス	1	1
検知	5. 攻撃等の検知	5-1 継続的監視	1	2
		5-2 有害事象の分析	0	1
対応	6. インシデントへの対応	6-1 インシデント管理	1	1
復旧	7. インシデントからの復旧	7-1 インシデント復旧計画の実行	1	1
合計			26	43

出所：IPA『SCS評価制度 ★3・★4 要求事項・評価基準』をもとに作成

用語解説：NISTサイバーセキュリティフレームワーク

米国国立標準技術研究所（NIST）が策定した、組織がサイバーセキュリティリスクを体系的に管理・軽減するためのガイドライン。業種や企業規模を問わず、自社のセキュリティ対策の現状を把握し、優先順位をつけて改善するために世界中で広く活用されている。最新版はバージョン2.0（2024年2月公開）

要求事項ごとに実施すべき具体的なセキュリティ対策が「評価基準」として定められている。評価基準は★3（最低限実施すべきセキュリティ対策：81項目）と★4（標準的なセキュリティ対策：72項目）に分類されている（図4-5）。

★3の取得には、★3の81項目の評価基準を全て実施し、認定を受けた専門家の評価を受ける必要がある。★4の取得には、★3（81項目）に加えて★4（72項目）の評価基準を全て実施し（合計153項目）、第三者機関による評価を受ける必要がある。

▼図4-5 要求事項と評価基準の関係

大分類	中分類	要求事項	評価基準		
3. リスクの特定	3-1. 資産管理	3-1-2. ネットワークに 関する情報の把握	★3	3-1-2-1	ネットワークを把握するための仕組みを整備すること。 その際、把握すべき情報の中に各ネットワークの所在地 及び用途に関する情報を含めること。
			★3	3-1-2-2	ネットワーク機器を把握するための仕組みを整備するこ と。その際、把握すべき情報の中に各機器の製造元、モ デル及び保守事業者に関する情報を含めること。
			★4	3-1-2-3	ネットワークを対象として、ネットワーク図を作成する こと。
			★4	3-1-2-4	年1回以上の頻度でNo.3-1-2-3で作成したネットワーク図 の記載内容について点検すること。

☐ ★3レベルの達成に必要：No.3-1-2-1～2の2要件 ☐ ★4レベルの達成に必要：★3に加えNo.3-1-2-3～4（計4要件）

出所：IPA『SCS評価制度 ★3・★4 要求事項・評価基準』をもとに作成

要求事項の分布には特徴がある。★3の26件のうち7件が「4-1 アイデンティティ管理、認証、アクセス制御」に集中しており、突出している。制度が★3の水準として、初期侵入の防御を重視していることがうかがえる。次いで「3-1 資産管理」が4件、「2-1 サイバーセキュリティサブライチェーンリスクマネジメント」と「4-4 プラットフォームセキュリティ」がそれぞれ3件である。

(1)-6. 実務上の影響が大きい要求事項

★4の43項目の要求事項と153項目の評価基準には、割賦

販売法の実務上の指針となる『セキュリティガイドライン 6.1』やPCI DSSなどで求められ、すでに各事業者が対応済みの項目も多く含まれる。ここでは、対応が困難であったり、実務上の影響が大きいと思われる要求事項をいくつか取り上げ、解説する。

①4-4-4. セキュリティパッチ・アップデートの手続

情報機器、OS及びソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続を定めることを求める要求事項である（図4-6）。

▼図4-6 要求事項4-4-4「セキュリティパッチ・アップデートの手続」に含まれる評価基準

番号	区分	内容
4-4-4-1	★3	・システム、情報機器及びソフトウェアは以下の状態とすること。 - ライセンスが付与され、サポートされている。 - サポートが終了した場合に削除されるか、又はインターネットとの全てのトラフィックを遮断することで適用範囲から削除される。 - 可能であれば、自動アップデートが有効化されている。
4-4-4-2	★3	・利用している機能又は設定に関して、以下のいずれかに該当するアップデートプログラムがリリースされてから14日以内に、アップデートすること。 - 当該アップデートが、ベンダーにより「重大」(Critical)又は「高リスク」(High Risk)と説明される脆弱性を修正するものである。 - 当該アップデートが、CVSSの基本値が7.0以上の脆弱性を修正するものである。 - 当該アップデートが修正する脆弱性のレベルの詳細がベンダーから提供されていない。 ・やむを得ず上記のとおりアップデートができない場合(例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合)は、アップデート適用までの間、以下のいずれかにより脆弱性悪用のリスクを低減する対策を実施すること。 - 脆弱性悪用の対象となる機能を無効化すること。 - ベンダーが推奨する回避策を実施すること。 - 対象となる情報機器を適用範囲内のネットワークから分離すること。 - 対象となる情報機器と適用範囲内のネットワークとの通信を監視し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェアを導入すること。 [対象] - 会社支給のパソコンのOS、ブラウザ及びOfficeソフト - サーバのOS及びミドルウェア - 会社支給のスマートデバイスのOS及びアプリ - インターネットとの境界に設置されているネットワーク機器のOS及びファームウェア
4-4-4-3	★4	・インターネットとの境界に設置されているネットワーク機器のOS及びファームウェアについては、CVSS基本値7.0以上の脆弱性を有していないこと。

出所：IPA『SCS評価制度 ★3・★4 要求事項・評価基準』をもとに作成

本要求事項への対応の中で特に影響が大きいと思われるのは4-4-4-2にある「ベンダーが「重大（Critical）」または「高リスク（High Risk）」と評価した脆弱性、あるいはCVSS基本値7.0以上の脆弱性を修正するアップデートプログラムがリリースされてから14日以内にアップデートすること」である。実際にアップデートを実行するためには業務システムや他のソフトウェアとの互換性確認、動作検証、利用部門との調整、メンテナンス時間の確保などが必要である。特にサーバーやネットワーク機器では再起動やサービス停止を伴う場合もある。このため、リリースから14日以内に検証から本番適用までを完了することは、対象システムの規模や運用体制によっては相当に厳しい条件となる。対象には会社支給PCのOS、ブラウザ、Officeソフト、サーバーOS、ミドルウェア、スマートデバイスのOSやアプリ、インターネットとの境界に設置されたネットワーク機器のOS・ファームウェアなど、多種多様な製品が含まれている。これらについて、使用している製品・バージ

ョンを正確に把握したうえで、各ベンダーが公開する脆弱性情報やアップデート情報を継続的に収集し、自社環境が影響を受けるかを判断する必要がある。この活動そのものも、大きな運用負荷となる。

本要件への対応を実現するためには、単にパッチ適用作業を迅速化するだけでは不十分である。資産情報の一元管理、脆弱性情報との自動的な照合、標準化された検証・展開手順、例外時の代替対策と承認プロセスを一体として整備する必要がある。製品やバージョンの標準化、エンドオブライフ（EOL）製品の使用停止によって管理対象そのものを削減することも検討してほしい。

② 2-1-3. 取引先のセキュリティ対策状況

事業継続リスク及び情報管理リスクの観点から自社に影響を及ぼす可能性のある取引先のセキュリティ対策状況を把握することを求める要求事項である。（図4-7）

▼図4-7 要求事項2-1-3「取引先のセキュリティ対策状況」に含まれる評価基準

番号	区分	内容
2-1-3-1	★4	・以下に示す条件のいずれかが若しくは複数に該当する子会社又は取引先を対象に、年1回以上の頻度で、以下の例を参考にセキュリティ対策状況を把握すること。
		[対策状況把握の対象とする子会社又は取引先の条件]
		- 自社の重要な機密情報を提供・共有する
		- 自社の事業継続にとって重要な位置づけを持つ
		- 当該取引先の環境から発注者の内部システムへのアクセスが可能
		[対策状況の把握方法(例)]
		- 本制度が定める★の取得状況について取引先から回答を受領する、又は本制度の運用主体が管理するWebサイト等で確認する
		- 取引先に訪問し点検を実施する
		- セキュリティ対策チェックシートを作成して回答を受領する

出所：IPA『SCS評価制度 ★3・★4 要求事項・評価基準』をもとに作成

『セキュリティガイドライン6.1』は、キャッシュレスサービスに関係する各事業者に対し、カード情報を取り扱う業務を外部委託する場合に、委託先管理として「PCI DSSに準拠している等の必要なセキュリティ対策を講じた事業者を選定すること」および「委託契約の締結後にその実施状況を確認すること」を求めている。対して、SCS評価制度の評価基準2-1-3-1は、★4の取得を目指す事業者に対し、カード情報を取り扱うかどうかにかかわらず、条件に該当する取引先に対して年1回以上セキュリティ対策状況を把握することを求めている。委託先管理の対象には「自社の事業継続にとって重要な位置づけを持つ」という条件が含まれる。例えば加盟店にとってのPSPは、その条件にあてはまるといえるだろう。また、「当該取引先の環境から発注者の内部システムへのアクセスが可能」という条件には、システム開発や運用を委託している事業者が該当することがある。すなわち、多くの事業者にとって、委託先管理の対象が増えることになると想定される。

「必要なセキュリティ対策を講じている」と判断する基準としては、本制度が定める★の取得状況について取引先から回答を受領すること、または本制度の運用主体であるIPAが管理するWebサイト等で確認することが、まず挙げられている。取引先への訪問による点検、セキュリティ対策チェックシートによる回答受領がこれに続く。★の確認が、従来の個別チェックシートに代わる手段として制度自身に位置づけられている。

③ 7-1-1. 事業継続要件に沿った復旧準備

事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うことを求める要求事項である。また、これに関連した要求事項として、4-3-4「適切なバックアップ」がある（図4-8、図4-9）。

「1-(3) 2025年のカード情報流出事件のトピック」でも触れたが、ランサムウェア攻撃を受けると事業活動そのものが停止してしまう。

重要なデータのバックアップは行っている、実際に攻撃を受けた際にバックアップデータを使ってシステムを復旧できず、事業やサービスの停止が長期間にわたるケースは少なくない。7-1-1-1は、★3の対策として、事業継続上重要なシステムについて、「業務の目標復旧レベル」と、

「そこまで回復するための対策」をあわせて整備しておくことを求めている。7-1-1-2は、★4の対策として、実際のバックアップデータを使用して、手順通りに目標復旧時間内に、目標復旧時点までの復元ができることの確認を必要としている。

▼図4-8 要求事項7-1-1「事業継続要件に沿った復旧準備」に含まれる評価基準

番号	区分	内容
7-1-1-1	★3	・事業継続上重要なシステムについて、サイバー攻撃を念頭に、業務の目標復旧レベルを定めたうえで、当該レベルまで業務を回復するために必要な対策を、以下の例を参考として整備すること。 [復旧のための対策(例)] - システムによる業務継続(例:予備機、クラウド環境等により待機系を整備する。) - 人手による業務継続(例:電話、FAX等による連絡又は業務の実施に備え、影響のある取引先の連絡先及び複数の連絡手段を整備する。)
7-1-1-2	★4	・事業継続上重要なシステムについて、サイバー攻撃を念頭に、以下の対策を構じること。 - 目標復旧時点への復旧ができるようにNo.4-3-4-1及びNo.4-3-4-2で取得したバックアップを保管すること。 - No.4-3-4-3で定めたリストア手順書どおりに、かつ、目標復旧時間内でバックアップの復元ができることを確認すること。

出所：IPA『SCS評価制度 ★3・★4 要求事項・評価基準』をもとに作成

▼図4-9 要求事項4-3-4「適切なバックアップ」に含まれる評価基準

番号	区分	内容
4-3-4-1	★3	・取得対象、取得頻度及び保管期間を定めて自社で取り扱うデータのバックアップを取得すること。
4-3-4-2	★3	・重要な機密情報については、No.4-3-4-1におけるバックアップに加えて、遠隔地バックアップを実施すること。
4-3-4-3	★3	・バックアップ対象ごとにリストア手順書を整備すること。

出所：IPA『SCS評価制度 ★3・★4 要求事項・評価基準』をもとに作成

この要求事項を満たすためには、まずはインシデント発生時の「目標復旧レベル」「目標復旧時点」「目標復旧時間」を、事業継続の観点から定義する必要がある。その上で、バックアップデータの保管方法を再度見直し、リストア手順を定義し、テストすることになる。

(1)-7. 対応の進め方

★取得を目指す事業者にとって、対応の出発点は現状把握とギャップ分析である。自社でギャップ分析やセキュリティ対策の実施が難しい中小企業向けの★取得支援策とし

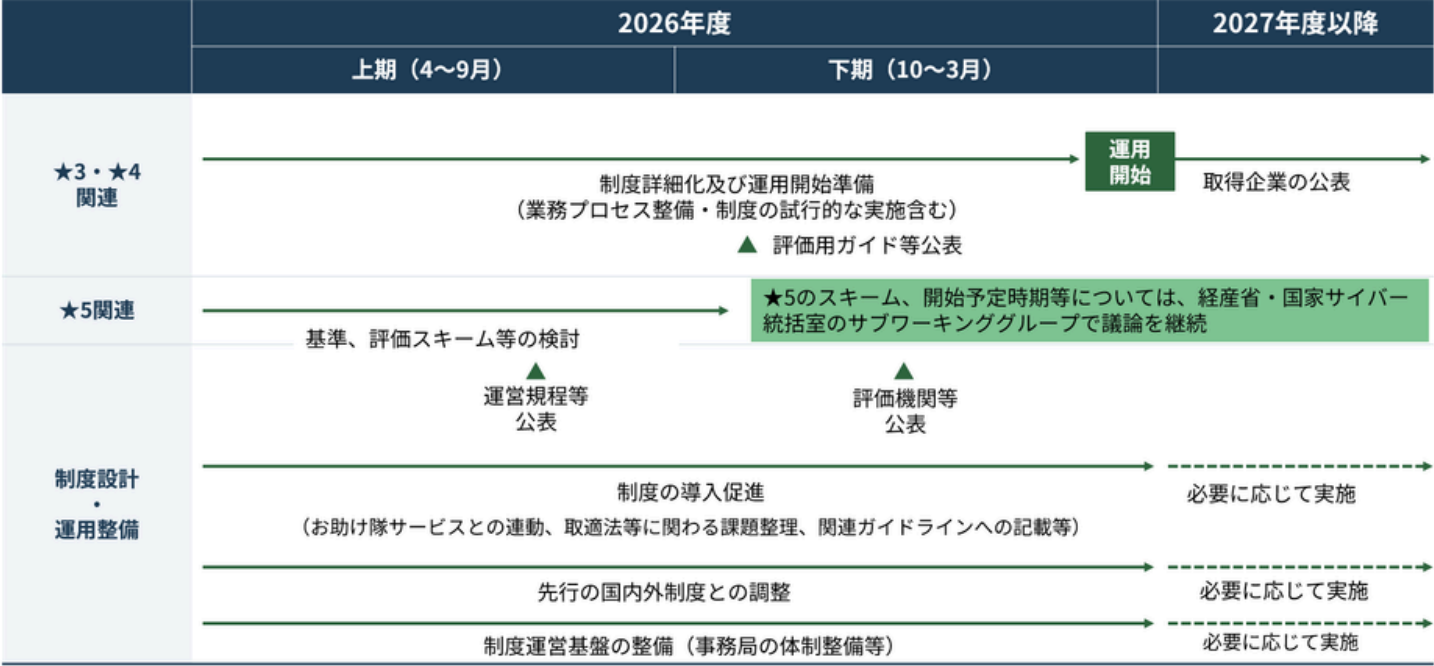
て、経済産業省は「サイバーセキュリティお助け隊サービス（新類型）」の新設を予定している。★3および★4の申請受付開始は2026年度末頃（2027年1～3月頃）が予定されている。★5の開始時期は引き続き検討が進められる（図4-10）。

2026年秋頃には評価用ガイド等の公表が予定されている。取得を予定している企業は、本評価制度に関する情報収集と並行して、現状把握とギャップ分析を進めておくことが望ましい。

用語解説：サイバーセキュリティお助け隊サービス

主に中小企業のサイバーセキュリティ対策に必要な見守り・駆けつけ・保険をワンパッケージで有償提供する。経済産業省が策定した基準に基づき、IPAが認定・登録した民間サービス。サービス利用料はデジタル化・AI導入補助金の支援対象となる。

▼図4-10 制度運用開始までのスケジュール



※上記は制度運営基盤の整備状況等により変更となる可能性がある。
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』2026年3月（国家サイバー統括室・経済産業省）

(2) 生成AIの進化とキャッシュレスセキュリティ

生成AIの急速な進化は、キャッシュレスセキュリティにおける攻防両面を大きく変えつつある。攻撃側では、フィッシングをはじめとする既存の不正手口の「量産化」と「精密化」が進む。防御側では、フロンティアAIによる脆弱性発見能力の飛躍的な向上が、脆弱性管理の前提を変え始めている。

さらに、AIエージェントが人間に代わって商品を検索し決済まで行う「エージェントックコマース」の登場は、「人間が画面上の購入ボタンを押す」ことを前提に構築されてきた不正利用対策そのものに再考を迫っている。本節では、2025年から2026年前半にかけてのこれらの動向を整理する。

用語解説：フロンティアAI

最先端の汎用AIモデル（基盤モデル）のうち、その時点で最高水準のモデルの能力に匹敵またはこれを上回り、安全保障等への影響が懸念される水準のものを指す呼称。2023年11月の英国AI安全性サミットで採択された「ブレッチリ宣言」を契機に定着した用語で、特定の製品名ではなく、技術水準の進展に伴って対象が移り変わる相対的な概念である。

(2)-1. 攻撃側の変化：

不正の「量産化」と「精密化」

警察庁の『令和7年におけるサイバー空間をめぐる脅威の情勢等について』（以下、『サイバー空間をめぐる脅威の情勢2025』）によれば、2025年のフィッシング報告件数は245万4,297件と右肩上がりの増加が続いた。同年のインターネットバンキングに係る不正送金事案は発生件数4,747件、被害総額約103億9,700万円にのぼり、その手口の約9割をフィッシングが占める。また、2025年に急増した証券口座への不正アクセスでは、年間の不正アクセス件数1万7,668件、不正売買金額約7,408億円、証券会社をかたるフィッシングメール報告件数31万6,414件という深刻な被害が確認された。

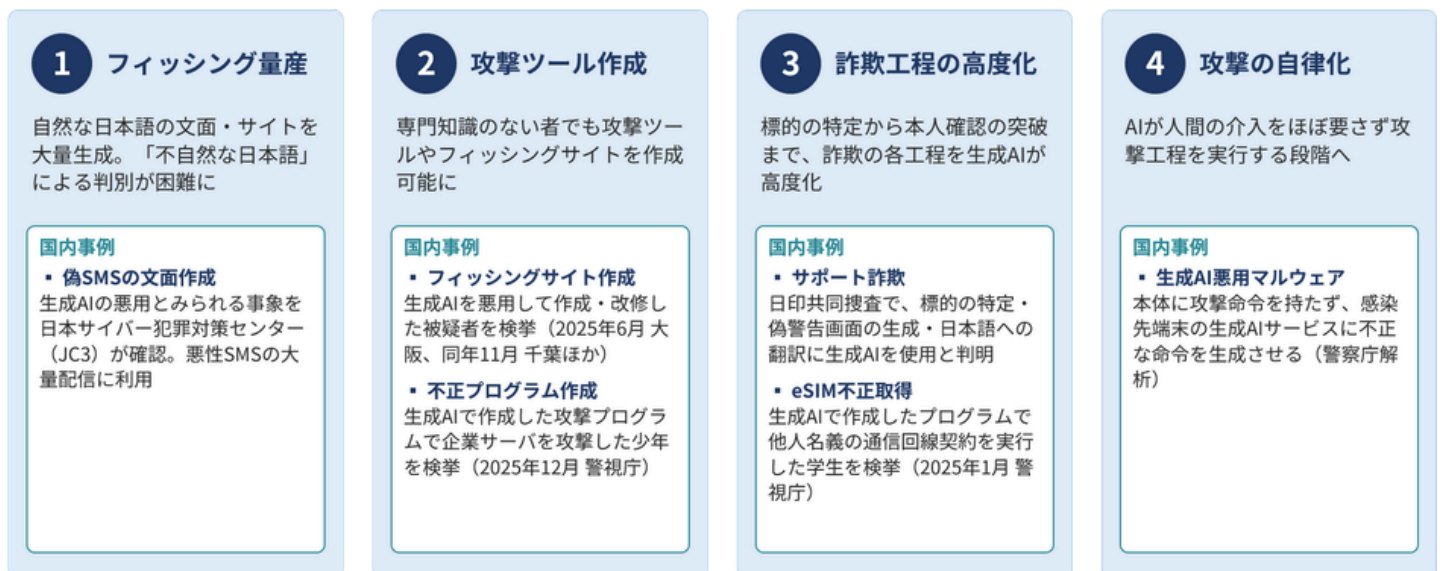
こうした被害拡大の背景に、生成AIによる攻撃の変質がある。生成AIにより自然な日本語のフィッシングメールやフィッシングサイトの作成が容易になったことで、「不自然な日本語で見分ける」という従来の判別法は通用しなくなった。海外の犯罪集団にとって日本市場を狙う際の言語障壁が事実上消失した結果、日本を対象とした攻撃が相対的に増加したと考えられる。

2025年は、生成AIの悪用が報告や推測の段階を越え、国内の検挙事案として相次いで確認された年でもあった。フィッシングの量産から攻撃ツールの作成、詐欺工程の高度化、攻撃の自律化まで、その悪用は攻撃の各局面に広がっている（図4-11）。さらに、『サイバー空間をめぐる脅威の情勢2025』では、国家を背景とする攻撃グループが生成AIを利用し、人間の介入をほぼ要せずにサイバー攻撃の全工程を実行したとの民間企業の報告にも言及している。

これらの事案に共通するのは、生成AIが全く新しい不正の手口を生んだというより、フィッシング、マルウェア作成、なりすましによる不正ログインといった既存の手口の実行に必要なスキルとコストを劇的に引き下げた点である。

これらの事案に共通するのは、生成AIが全く新しい不正の手口を生んだというより、フィッシング、マルウェア作成、なりすましによる不正ログインといった既存の手口の実行に必要なスキルとコストを劇的に引き下げた点である。

▼図4-11 生成AIを悪用した攻撃の類型



出所：警察庁『令和7年におけるサイバー空間をめぐる脅威の情勢等について』（2026年3月）よりCacco・リンク作成

る。専門知識のない者が高度な攻撃に参入できるようになったことは、「1. 2025年のカード情報流出事件の概況」で扱ったカード情報流出や「2. 2025年のカード不正利用の概況」の不正利用被害が今後も高止まりし得る構造的要因といえる。

(2)-2. 防御側の変化：

フロンティアAIによる脆弱性対策の加速

攻撃側の変化と同時に、2026年に入り防御側にも大きな転換点が訪れた。2026年4月7日、米Anthropic社はフロンティアAIモデル「Claude Mythos Preview」を発表した。同モデルは主要なOSやWebブラウザなど重要ソフトウェアにおいて、数千件の高深刻度の脆弱性を自律的に発見しており、発見のみならず、それを悪用するコードの作成まで可能とされる。その能力の高さを理由に、発表時点では一般公開されず、管理された研究プレビューとして限定提供された。

同社は発表と同時に、この能力を防御側で活用する取り組み「Project Glasswing」を開始した。Amazon Web Services、Apple、Cisco、CrowdStrike、Google、Microsoft、Linux Foundation、そして金融機関のJPMorganChaseを含む12組織が立ち上げパートナーとなり、重要なソフトウェア基盤を構築・保守する40超の組織を加えた約50組織で、攻撃者に悪用される前に脆弱性を発見・修正することを目的とする。Anthropic社によれば、開始から約1ヵ月で高・重大深刻度の脆弱性1万件超が発見された。

またプロジェクト参加銀行の1行では、メールアカウント侵害となりすまし電話を組み合わせた150万ドルの不正送金の検知・阻止に同モデルが寄与したという。同プロジェクトの対象は急速に広がっている。Anthropic社は2026年6月2日、参加組織に新たに約150組織を追加し、約200組織規模へ拡大すると発表した。追加された組織は15を超える国にまたがり、初期には十分にカバーされていなかった電力・水道・医療・通信などの重要インフラ分野や、多数の組織が依存するソフトウェアを保守するベンダー、オープンソースのメンテナーが含まれる。同社は新規参加組織の名称を公表していないが、日本については、日本政府および国内の一部金融機関の参加が、同日の財務大臣兼内閣府特命担当大臣（金融）の会見や、その後のデジタル担当大臣の会見で明らかにされている。フロンティアAIによる脆弱性対策が、一部の巨大IT企業の取り組みから、日本を含む重要インフラ事業者の実務へと広がり始めたことを示す動きである。

さらに2026年6月9日には、Project Glasswingのパートナー向けに限定提供された「Claude Mythos 5」に加え、同一の基盤モデルに安全対策を付した「Claude Fable 5」が一般公開され、Mythos級の能力は、限定提供から安全策付きの一般提供へと段階を進めた。もっともその3日後の6月12日、米商務省は輸出管理規則に基づき外国籍者へのアクセス停止を指示し、Anthropic社の自主的な判断により、両モデルは全世界で一時停止された。同月30日の指示解除を経て7月1日に提供が再開されている。この経緯は、フロンティアAIが輸出管理の対象となり得ることを先例として示すものである。日本の事業者にとっては、こうした能力へのアクセスが地政学的要因で変動し得るという可用性リスクの論点も残した。

一方で、Mythosの攻撃能力については英国AISI（AI Security Institute）が2026年4月13日時点での評価を報告している。Mythos Previewが32ステップの企業ネットワーク攻撃シミュレーションを完遂した初のモデルであり、防御の弱いシステムに対しては自律的な攻撃が可能であるという。一方、演習環境の制約から十分に防御されたシステムを攻撃できるかどうかは確言できないとしている。金融庁・日本銀行の要請文（後述）もこの評価を引用して、基本的な対策をより迅速かつ着実に実行することが引き続き重要であるとしている。フロンティアAIの登場は防御の前提を変えるが、基本的な対策を着実に実行しているシステムの防御力を直ちに無効化するものではない、というのがこの時点での評価である。

日本では、これらの動向を受けた政策対応が急速に進んだ。2026年5月18日、内閣官房国家サイバー統括室など計14の関係省庁・関係機関は、政府全体の対応パッケージ「Project YATA-Shield」を公表した。同文書はClaude Mythos Previewを名指しで挙げた上で、高性能AIについて、攻撃者による悪用リスクを前提としつつ、脆弱性の発見・修正等のサイバー防御に積極的に活用していく方針を示している。これを受けて同年5月22日、金融庁と日本銀行は連名で「フロンティアAIによる脅威変化を踏まえた金融機関等の短期的な対応」を金融機関等に向けて要請した。従来発見が困難だった脆弱性が短期間に大量に発見され、脆弱性の発見から攻撃までの期間が大幅に短縮され得るという認識の下、経営トップが直接関与すべき9項目の取り組みへの対応を求めている（図4-12）。この9項目への対応は概ね1ヵ月程度を目途に進めることが期待されるとしている。対応すべきシステムの絞り込みとリスクベースのパッチ適用、仮想パッチ等による多層防御、能動的なサービス停止も選択肢に含めた事業継続計画の点検などが柱で、これらは応急的措置と位置づけられ、中長期的には脆弱性対応の自動化への移行が必要と明記されている。

▼図4-12 金融庁・日本銀行による9項目の短期的対応の全体像



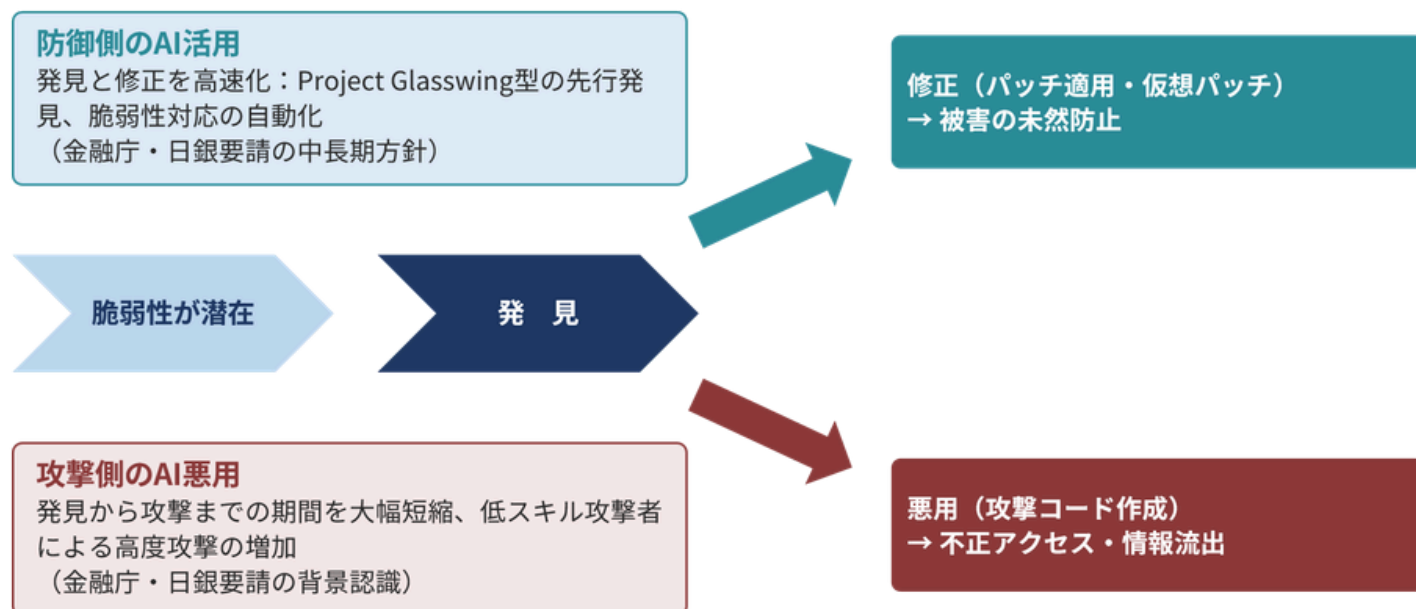
2026年5月22日要請。経営トップの直接関与の下、概ね1ヵ月程度を目途に実施。短期対応は応急的措置であり、中長期的には脆弱性対応の自動化等への移行が必要（要請文より）

出所：金融庁・日本銀行「フロンティアAIによる脅威変化を踏まえた金融機関等の短期的な対応」に係る要請（金総政第3245号ほか）より Cacco・リンク作成

重要インフラの中でも金融分野は先行的な取組と位置づけられている。クレジットカード分野など経済産業省の所管の重要インフラについて官民の意見交換が行われるなど、他分野への展開も始まっている。

攻撃者が脆弱性を発見するコストが下がる環境では、「攻撃者に見つけられる前に自ら見つけて修正する」体制の重要性が、すべての事業者において増すことになる（図4-13）。

▼図4-13 脆弱性のライフサイクルとAIの介入点



同じ「発見」能力が攻防どちらに使われるかで帰結が分かれる——攻撃者より先に発見・修正する体制の意義

(2)-3. 新領域：エージェンティックコマースと決済の変化

生成AIの進化がもたらすもう一つの大きな変化が、AIエージェントが利用者に代わって商品の検索から決済までを行う「エージェンティックコマース」の登場である。2025年後半から、これを支える決済枠組みの整備が国際的に進んだ。

その代表が「AP2（Agent Payments Protocol）」である。2025年9月にGoogleが発表した同プロトコルの仕様策定には、Mastercard、PayPal、American Express、Coinbaseなど60を超える企業・団体が参画しており、日本からはJCBが名を連ねている。AP2の課題認識は明快である。現在の決済システムは、人間が信頼できる画面上で「購入」ボタンを直接クリックすることを前提に設計されているが、自律的なエージェントによる決済は、この前提が崩れる。そこで、利用者がAIエージェントに特定の購買権限を与えたことの証明（認可）、エージェントの要求が利用者の真の意図を反映していることの確認（真正性）、不正・誤発注が起きた際の責任の所在（説明責任）という3つの問いに答える必要がある。暗号署名付きの改ざん不可能な指示記録「Mandate」によって、AIエージェントを利用者の正規の代理人と認めるという考え方となる。

2026年4月には、同プロトコルはGoogleからFIDO Alliance（パスキー等の認証標準を策定する業界団体）へ移管され、業界共通の標準として策定が進む体制に移行した。移管と同時に公開された新版では、利用者が事前に承認した指示に基づき、利用者がその場にいらなくてもAIエージェントが決済を実行する「Human Not Present」決済のフローが新たに整備された。利用者が承認したAIエージェ

ントの行動を改ざん不能な形で記録・証明するMastercard開発の規格「Verifiable Intent」（Googleと共同開発）が、AP2と連携動作する別規格としてMastercardからFIDO Allianceへ同時に提供され、両者は同じ作業部会で一体的に仕様策定が進められている。

このほか、2025年4月～10月には、ChatGPTでの購入機能の基盤となるStripe・OpenAIの「ACP」、AIエージェントと加盟店間の通信をリクエスト単位で暗号的に検証するVisaの「Trusted Agent Protocol」、トークン化されたカード情報を特定のAIエージェントと利用範囲に紐付けるMastercardの「Agent Pay」など、複数の枠組みが立ち上がっている（図4-14）。各枠組みはアプローチこそ異なるが、「AIエージェントの身元と権限を暗号的に検証可能にする」という方向性は共通している。

注目されるのは、各社独自の枠組みから中立的な標準化団体での仕様策定へと重心が移り始めたことである。前述の通りFIDO Allianceの決済技術作業部会にはAP2とVerifiable Intentの2件の仕様が提供されており、同部会の議長はMastercardとVisaのメンバーが務めている。VisaもTrusted Agent Protocolについてインターネット技術の標準化団体IETF、デジタルID認証仕様を策定するOpenID Foundation、カード決済の技術仕様を策定するEMVCoとの整合とACP等との補完を掲げている。枠組みの乱立から相互運用の確保へと、業界の焦点は移りつつある。米国では2026年2月、NIST（国立標準技術研究所）内のCAISI（Center for AI Standards and Innovation：AI標準・イノベーションセンター）が「AI Agent Standards Initiative」を立ち上げ、AIエージェントのアイデンティティと認可を含む標準の整備に着手した。

▼図4-14 エージェント決済を支える主要な枠組み

	AP2 (Agent Payments Protocol)	ACP (Agentic Commerce Protocol)	Trusted Agent Protocol	Agent Pay
主導	Google発。2026年4月にFIDO Allianceへ移管	Stripe・OpenAI	Visa	Mastercard
発表	2025年9月	2025年9月	2025年10月	2025年4月
仕組みの要点	暗号署名付き指示記録「Mandate」で認可・真正性・説明責任を担保。決済手段非依存	ChatGPT内購入の基盤。チェックアウト・決済トークン委譲・OAuth認可委譲を定義	エージェントと加盟店間の通信をリクエスト単位で暗号的に検証（単回有効の制限署名）	トークン化したカード情報を特定エージェント・利用範囲・同意ポリシーに紐付け
主な参画	60超の企業・団体（JCB, Mastercard, PayPal, AmEx等）	Stripe, OpenAI, Meta	Microsoft, Shopify, Stripe, Anthropic, OpenAI等	Microsoft, IBM, Braintree（初期）

出所：Google Cloud（2025/9/16発表）、Stripe公式ドキュメント、Visa・Mastercard各社発表・報道よりCacco・リンク作成

不正対策の観点から重要なのは、エージェントックコマー্সが既存対策の前提を変える点である。EMV 3-Dセキュアのリスク評価や不正検知システムの行動分析は、人間の操作パターンを前提としてきた。しかし正規のAIエージェントによる購買でも、従来のbot検知と行動は類似す

る。攻撃者がAIエージェントになりすます、あるいはプロンプトインジェクションにより正規のAIエージェントに意図しない購買を行わせるといった新しい不正利用の形も想定される。

用語解説：プロンプトインジェクション

AIへの入力に不正な指示を紛れ込ませ、開発者が与えた指示や制約を上書きさせることで、開発者や利用者の意図しない動作を引き起こさせる攻撃手法。利用者が直接不正な指示を入力する「直接型」と、AIが読み込むWebページや商品説明、メール等に指示を埋め込んでおく「間接型」に大別され、AIエージェントが外部の情報を読みながら自律的に操作を行うエージェントックコマー্সでは後者が主要なリスクとなる。

少額の定型的な購買は自律実行を許容しつつ、高額・不可逆な取引には人間の明示的な確認を求めるといった、権限委譲の粒度設計がEC加盟店・PSP双方の課題となる。

AP2の「Human Not Present」決済のように、事前承認に基づく自律実行を仕様として定義する動きは、この課題に対する一つの解であるといえる。国内では、JCBのAP2仕様策定への参画のように国際的な枠組みへの関与が始まっているが、割賦販売法やセキュリティガイドラインといった国内制度がAIエージェントによる決済をどう位置づけるかは、今後の重要な論点である。

(2)-4. 考察

生成AIの進化とキャッシュレスセキュリティの動向を次の3点に整理する。第一に、生成AIは現時点では攻撃側にとって、新たな手口の発明というより、既存手口の参入障壁とコストの劇的な引き下げとして作用している。フィッシングメールやフィッシングサイトの量産、マルウェア作成の容易化、自然な日本語による日本人の標的化は、いずれも従来から存在する手口の実行可能性を広げたものであり、その帰結が2025年の統計に表れている。

第二に、脆弱性をめぐる攻防の時間軸が変わりつつある。フロンティアAIは攻防双方の脆弱性の発見速度を高速化するが、Project YATA-Shieldが示す通り、この能力は悪

用リスクを前提としつつ防御に積極活用すべきものである。Project Glasswingのように一般公開前のモデルを防御側が先行利用する枠組みや、金融庁・日本銀行の要請が示す「大量の脆弱性発見を前提とした態勢整備」は、その具体化といえる。この要請の対象は金融分野における重要インフラ事業者等（サイバーセキュリティ基本法における重要インフラ事業者および経済安全保障推進法における特定社会基盤事業者）であると考えられ、銀行等にとどまらず、大手資金移動業者や前払式支払手段発行者を含む幅広い金融機関等のキャッシュレス決済の担い手が含まれる。加えて、重要インフラ分野に該当するクレジットカード会社や、脆弱性を起点とするカード情報流出が続くEC加盟店にとっても、同じ規律を自主的に適用する意義は大きい。一方、英国AISIの評価（2026年4月時点）が示す通り、フロンティアAIによる十分に防御されたシステムに対する攻撃は達成可能とは確認されておらず、基本的対策の迅速かつ着実な実行の重要性はむしろ高まっている。

第三に、エージェントックコマー্সは、これまでの不正利用対策が前提とした「正規の購入は人間によって操作される」という仮定そのものを置き換える変化である。これはキャッシュレスセキュリティの枠組みに中期的に大きな影響を与える可能性がある。国際的な枠組み整備が始まったばかりであり、国内の制度・実務がこれをどう取り込むか、継続的に注視する必要がある。

<参考文献>

1. 『2025年のキャッシュレス決済比率を算出しました』（経済産業省 2026年3月31日）
<https://www.meti.go.jp/press/2025/03/20260331006/20260331006.html>
2. 『キャッシュレス推進検討会 とりまとめ』（経済産業省 2025年12月26日）
https://www.meti.go.jp/shingikai/mono_info_service/cashless_promotion/pdf/20251226_1.pdf
3. 『クレジットカード・セキュリティガイドライン【6.1版】』（クレジット取引セキュリティ対策協議会 2026年3月）
https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_6.1_published.pdf
4. 『令和7年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 2026年3月）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf
5. 『No More Ransom』プロジェクト（欧州刑事警察機構（ユーロポール）等 2016年開始）
<https://www.nomoreransom.org/ja/index.html>
6. 『クレジットカード不正利用被害の発生状況』（一般社団法人日本クレジット協会）
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf
7. 『クレジットカード不正利用被害の集計結果について』（一般社団法人日本クレジット協会 2026年3月6日）
https://www.j-credit.or.jp/download/news20260306_a1.pdf
8. EBA Opinion on new types of payment fraud and possible mitigants（欧州銀行監督局 2024年4月29日）
<https://www.eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf>
9. Card payment fraud report（欧州中央銀行 2023年5月）
<https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html>
10. 『2025 Report on Payment Fraud』（欧州銀行監督局・欧州中央銀行 2025年12月）
<https://www.eba.europa.eu/sites/default/files/2025-12/1709846a-84d9-47cf-86a0-b155efb34d66/EBA%20and%20ECB%20Report%20on%20Payment%20Fraud.pdf>
11. 『不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況』（国家公安委員会・総務大臣・経済産業大臣 2026年3月12日）
https://www.soumu.go.jp/main_content/001059979.pdf
12. 『フィッシングレポート2026』（フィッシング対策協議会 技術・制度検討ワーキンググループ 2026年6月1日）
https://www.antiphishing.jp/report/report/phishing_report2026.html
13. 『Kaspersky、情報窃取型マルウェアによる感染デバイス数を調査、3年間で約7.4倍に』（株式会社カスペルスキー 2024年4月18日）
<https://www.kaspersky.co.jp/about/press-releases/vir18042024>
14. 『【EC事業者実態調査2025】3-Dセキュア導入義務化後も不正被害は減らず。「決済手数料値上げ」要請は昨対約2倍へ急増する事態に』（かっこ株式会社 2025年12月24日）
<https://prtmes.jp/main/html/rd/p/000000204.000009799.html>
15. 『EMV 3-Dセキュア導入ガイド2.1版』（クレジット取引セキュリティ対策協議会 2026年3月）
https://www.j-credit.or.jp/security/pdf/secure_installation_guide.pdf

16. 『2025年度 デジタルプラットフォームの透明性・公正性に関するモニタリング会合 資料』(経済産業省 2025年度)
https://www.meti.go.jp/shingikai/mono_info_service/digital_platform_monitoring/pdf/2025_001_s02_03.pdf
17. 『2025年度 デジタルプラットフォームの透明性・公正性に関する評価 (デジタル広告分野)』(経済産業省 2025年12月17日)
https://www.meti.go.jp/policy/mono_info_service/digitalplatform/pdf/2025_hyouka3.pdf
18. 『国民生活センターADRの実施状況と結果概要について (令和7年度第1回)』(独立行政法人国民生活センター紛争解決委員会 2025年7月2日)
https://www.kokusen.go.jp/pdf/n-20250702_4.pdf
19. 『アドフラウドに対するJIAAステートメント』(一般社団法人日本インタラクティブ広告協会 2017年8月)
https://www.jiaa.org/katudo/gdl/adfraud_statement/
20. 『【2026年版 アドフラウド実態調査】 Web広告不正クリック対策、広告運用担当者の約4割が“見かけのCPA悪化”を理由に対策を躊躇・中止していることが判明』(かっこ株式会社 2026年5月12日)
<https://prtimes.jp/main/html/rd/p/000000222.000009799.html>
21. Russian Cybercriminal Sentenced to 10 Years in Prison for Digital Advertising Fraud Scheme (米国司法省 ニューヨーク東部地区連邦検事局 2021年11月10日)
<https://www.justice.gov/usao-edny/pr/russian-cybercriminal-sentenced-10-years-prison-digital-advertising-fraud-scheme>
22. 『令和8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 2026年9月10日)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf
23. 『「ニセ社長詐欺」全国で20億円被害 企業狙う手口に注意を』(NHK 2026年4月15日)
<https://news.web.nhk/newsweb/na/na-k10015099411000>
24. 『社長等をかたる詐欺メールに注意!』(独立行政法人情報処理推進機構 2026年3月12日)
<https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20260312.html>
25. 『社長を騙りLINEに誘導する「CEO詐欺」の手口を解説』(トレンドマイクロ 2026年2月6日公開/2026年6月23日更新)
https://www.trendmicro.com/ja_jp/jp-security/26/b/trendnews-20260210-01.html
26. 『「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』(経済産業省・内閣官房国家サイバー統括室 2026年3月27日)
<https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html>
27. 『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 (SCS評価制度)』(経済産業省)
<https://www.meti.go.jp/policy/netsecurity/scs.html>
28. 『情報セキュリティ10大脅威 2026』(独立行政法人情報処理推進機構 2026年1月29日)
<https://www.ipa.go.jp/security/10threats/10threats2026.html>
29. ★3・★4 要求事項・評価基準 (独立行政法人 情報処理推進機構)
<https://www.ipa.go.jp/security/scs/requirements-criteria.html>
30. Project Glasswing (Anthropic 2026年4月)
<https://www.anthropic.com/glasswing>
31. Project Glasswing: An initial update (Anthropic 2026年5月22日)
<https://www.anthropic.com/research/glasswing-initial-update>

32. Expanding Project Glasswing (Anthropic 2026年6月2日)
<https://www.anthropic.com/news/expanding-project-glasswing>
33. Claude Fable 5 / Claude Mythos 5 へのアクセスについて (Anthropic 2026年6月12日)
<https://www.anthropic.com/news/fable-mythos-access>
34. Redeploying Claude Fable 5 (Anthropic 2026年7月1日)
<https://www.anthropic.com/news/redeploying-fable-5>
35. Our evaluation of Claude Mythos Preview's cyber capabilities (英国AI Security Institute 2026年4月13日)
<https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities>
36. 『AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について ～Project YATA-Shield～』(内閣官房国家安全保障局・国家サイバー統括室ほか 2026年5月18日)
https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Package.pdf
37. 『「フロンティアAIによる脅威変化を踏まえた金融機関等の短期的な対応」に係る要請について』(金融庁・日本銀行 2026年5月22日)
<https://www.fsa.go.jp/news/r7/sonota/20260522-5/01.pdf>
38. 『片山財務大臣兼内閣府特命担当大臣(金融) 記者会見』(金融庁 2026年6月2日)
<https://www.fsa.go.jp/common/conference/minister/2026a/20260602-2.html>
39. Announcing Agent Payments Protocol (AP2) (Google Cloud 2025年9月16日)
<https://cloud.google.com/blog/products/ai-machine-learning/announcing-agents-to-payments-ap2-protocol>
40. Agent Payments Protocol contributed to the FIDO Alliance (Google 2026年4月28日)
<https://blog.google/products-and-platforms/platforms/google-pay/agent-payments-protocol-fido-alliance/>
41. FIDO Alliance to Develop Standards for Trusted AI Agent Interactions (FIDO Alliance 2026年4月)
<https://fidoalliance.org/fido-alliance-to-develop-standards-for-trusted-ai-agent-interactions/>
42. Agentic Commerce Protocol (Stripe Documentation)
<https://docs.stripe.com/agentic-commerce/acp>
43. Visa Introduces Trusted Agent Protocol: An Ecosystem-Led Framework for AI Commerce (Visa 2025年10月14日)
<https://corporate.visa.com/en/sites/visa-perspectives/newsroom/visa-unveils-trusted-agent-protocol-for-ai-commerce.html>
44. Mastercard unveils Agent Pay, pioneering agentic payments technology to power commerce in the age of AI (Mastercard 2025年4月29日)
<https://newsroom.mastercard.com/news/press/2025/april/mastercard-unveils-agent-pay-pioneering-agentic-payments-technology-to-power-commerce-in-the-age-of-ai>
45. Announcing the "AI Agent Standards Initiative" for Interoperable and Secure Innovation (NIST／CAISI 2026年2月17日)
<https://www.nist.gov/news-events/news/2026/02/announcing-ai-agent-standards-initiative-interoperable-and-secure>
46. 『高性能AIへの対応に関して赤澤経済産業大臣が重要インフラ事業者との意見交換を実施しました』(経済産業省 2026年5月1日)
<https://www.meti.go.jp/press/2026/05/20260501001/20260501001.html>
47. 『特定社会基盤事業者一覧』(金融庁)
<https://www.fsa.go.jp/news/r5/economicsecurity/tokuteishakaikiban.pdf>

本レポートに記載された統計、数字などの情報を引用される際は、必ず出典元として「キャッシュレスセキュリティレポート2026」（Cacco、リンク）と明記ください。出典を明記されない形での転載および複製を禁じます。

キャッシュレスセキュリティレポート2026

2026年10月9日発行

発行者

かっこ株式会社

<https://cacco.co.jp/>

株式会社リンク

<https://pcireadycloud.com/>

【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）

文中の会社名、商品名、サービス名は各社の登録商標です。
