PCI DSS Ready Cloud

Cashless Security Report
Annual Report 2025

2025年10月2日
かっこ株式会社
株式会社リンク

もくじ

もくじ

はじめに

2025年3月に経済産業省が公表したデータによれば、2024年のキャッシュレス決済比率は42.8%と2023年に比べて3.5ポイントの増加となった。政府が掲げた「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%」の目標を前倒しで達成した。

【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 116.9兆円と、前年の105.7兆円から約11.2兆円増加し、伸び率にして約10.6%の増加となった。

・デビットカード

デビットカードの利用額は4.4兆円と、前年（3.7兆円）から約0.7兆円増加し、伸び率は約18.9%となった。全体に占める割合も3.1%（前年2.9%）へとわずかに上昇している。

・電子マネー

電子マネーの利用額は6.2兆円で、前年（6.4兆円）からやや減少した。全体に占める割合も5.1%から4.4%へと低下し、コード決済やクレジットカードの拡大に押される形となっている。

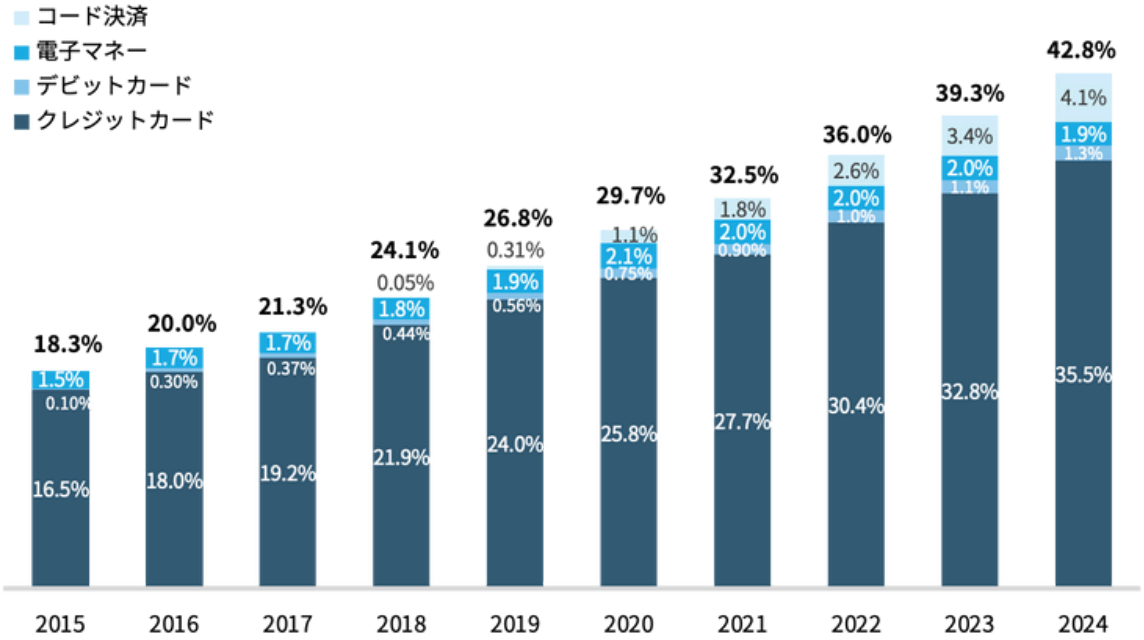
・コード決済

コード決済は13.5兆円と、前年（10.9兆円）から約2.6兆円増加し、伸び率は約23.9%と大幅な成長を記録した。全体に占める割合も9.6%と、前年（8.6%）から1.0ポイント上昇し主要4手段の中で最も高い成長率となった。

2024年は、クレジットカードが依然として8割以上を占める中、コード決済やデビットカードの利用が引き続き拡大した。電子マネーは減少傾向に転じたものの、日常的な少額決済における利用は引き続き根強く、決済手段の多様化が進展していると考えられる（図1-1）。

今後はさらなる利便性向上と安全性確保を図りつつ、将来的には 80% の比率を目標に環境整備を目指している。

▼図1-1　キャッシュレス決済比率の推移



出所：経済産業省プレスリリース『2024年のキャッシュレス決済比率を算出しました』（商務・サービスグループ キャッシュレス推進室　2025年3月31日）

2024年のクレジットカードなどのカード情報流出事件は、2023年に比べると事件数、カード情報流出件数ともほぼ横ばいであった。一方で、クレジットカード不正利用被害は2023年をさらに上回り、年間約555億円と過去最悪の記録を更新した。不正利用されるカード情報は、フィッシングやクレジットマスターなど、加盟店から流出したもの以外の割合が増えていることを裏付ける結果となった。

キャッシュレスセキュリティの重要性が増す中、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とりまとめ、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2025」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、両社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。

1. 2024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

(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。

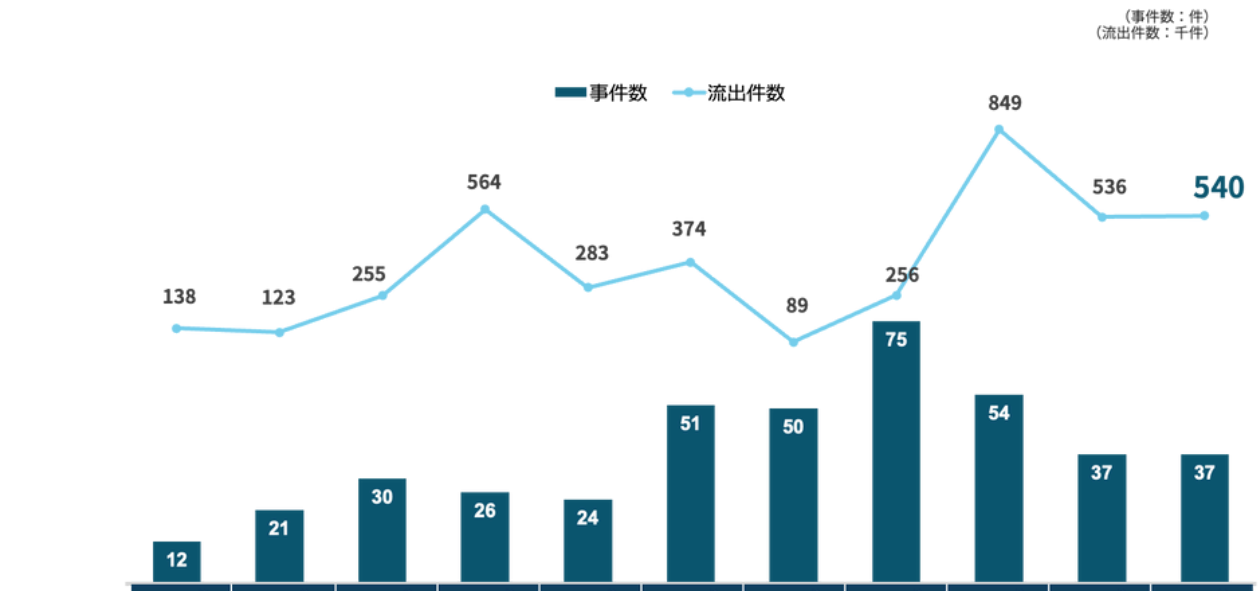
●カード情報流出件数：発表主体により公表された流出件数で、クレジットカード、ブランドデビットカード、ブランドプリペイドカードを含む。公開された件数のうち、最新の情報を正として集計

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2013年から2021年までのデータはｆｊ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ｆｊ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

2024年のクレジットカードなどのカード情報流出事件数は 37件 で、前年と同数となった。流出したカード情報件数は 540,722件 と、前年（536,291件）からわずかに増加した（図1-2）。１事件あたりの平均流出件数は14,614件となり、これもほぼ横ばいとなっている。

▼図1-2　国内のカード情報流出事件発生状況



	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年	2022年	2023年	2024年
事件数	12	21	30	26	24	51	50	75	54	37	37
カード情報流出件数	138,717	123,527	255,689	564,844	283,374	375,479	89,628	256,822	849,950	536,291	540,722
1件あたり平均件数	12,611	7,266	9,470	22,594	12,321	7,344	1,793	3,424	16,345	14,897	14,614

Cacco・リンク調べ（2021年以前のデータはｆｊコンサルティング調べ）

2023年のカード情報流出件数は半数以上をカード会社１社によるダイレクトメール誤印刷が占めていた。その事故を除いたカード情報窃取を目的とした被害のみの合計は、245,520件となり、2022年から大きく減少した。しかし2024年は540,722件が全てカード情報窃取を目的としたものとなり、約2.2倍と大幅に増加した。その流出件数の大半がECサイトをターゲットとした攻撃による被害によるものである。図1-3に示す通り、5万件以上の大規模流出事案は4件確認されている。最大はアパレル販売A社における71,943件の流出で、原因はペイメントアプリケーションの改ざんによるものだった。

これらを含め、37事件中15事件で１事件あたり1万件以上のカード情報が流出している。流出期間が長い事件が多くなったのは、2020年から2021年ごろに多く見られたECサイト改ざんの手口について警察が集中的に調査した結果、被害が新たに発覚したからであると考えられる（詳細は「(3)-1. 警察の指摘によるカード情報流出発覚の増加」）。結果として、2024年のカード情報流出件数の総合計は、昨年とほぼ同じとなり、１事件あたりのカード情報流出件数も横ばいとなった。

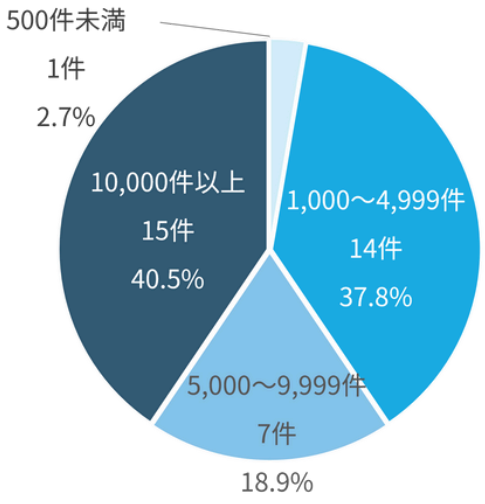
▼図1-3　2024年カード情報流出件数の多かった事件

	サイト名（運営企業）		流出件数	流出期間（日数）	原因
1	アパレル（女性下着）販売	A社	71,943	1,602	オンラインスキミング（可能性高）
2	食品（菓子）販売	B社	65,387	1,168	オンラインスキミング（可能性高）
3	食品（紅茶）販売	C社	58,407	1,487	オンラインスキミング（可能性高）
4	食品（コーヒー関連）販売	D社	52,958	1,036	オンラインスキミング（可能性高）
5	食品（ケーキ・洋菓子）販売	E社	45,335	1,486	オンラインスキミング（可能性高）
6	食品（地方特産品）販売	F社	18,746	1,170	オンラインスキミング
7	食品（地方特産品）販売	G社	18,443	1,117	オンラインスキミング（可能性高）
8	その他（仏壇仏具）販売	H社	18,394	1,149	オンラインスキミング（可能性高）
9	食品（おせち・高級商材）販売	I社	16,682	1,067	オンラインスキミング（可能性高）
10	食品（加工食品）販売	J社	16,407	839	オンラインスキミング（可能性高）

Cacco・リンク調べ

カード情報流出を規模別に見ると、500件未満の事件は、2024年はわずか1件（2.7%）にとどまり、2023年の11件（29.7%）から約10分の1へと大幅に減少している。一方で、流出件数10,000件以上の事件は15件（40.5%）を占めた。流出件数5,000件から9,999件の事件も7件（18.9%）と2割近くを占めている（図1-4）。

▼図1-4　2024年カード情報情報流出規模別事件数



Cacco・リンク調べ

流出件数規模	事件数	割合
500未満	1	2.7%
500～999	0	0.0%
1,000～1,499	2	5.4%
1,500～1,999	1	2.7%
2,000～2,499	3	8.1%
2,500～2,999	2	5.4%
3,000～3,499	0	0.0%
3,500～3,999	2	5.4%
4,000～4,499	2	5.4%
4,500～4,999	2	5.4%
5,000～7,499	6	16.2%
7,500～9,999	1	2.7%
10,000以上	15	40.5%
不明	0	0.0%

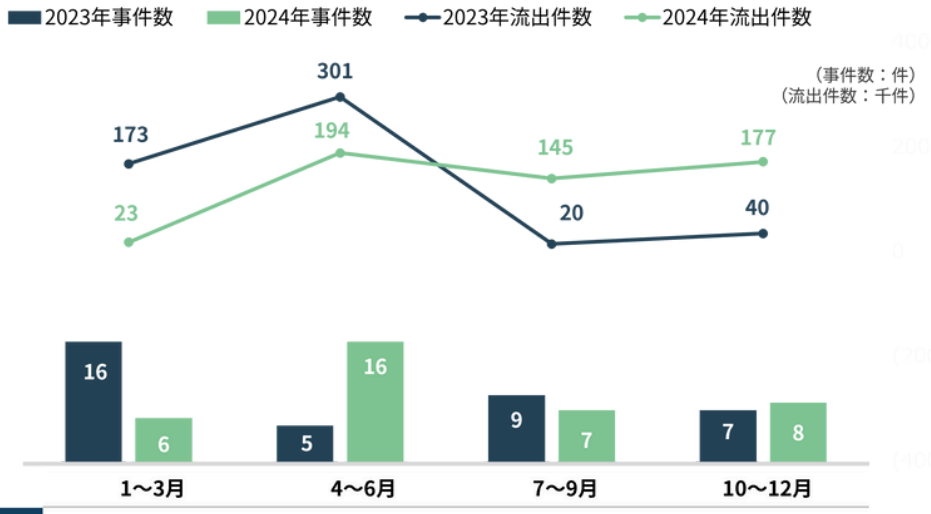
(1)-2. 四半期別推移

2024年の四半期別のカード情報流出動向を2023年と比較すると、特徴的な変化が見られる（図1-5）。

まず1–3月期は、事件数が前年の16件から6件へと大幅に減少し、流出件数も17万件超から2万件台へと急減した。前年同期は特定事業者からの大量流出が統計を押し上げていたが、2024年は同規模の事案が発生しなかったことが主な原因である。

4–6月期は一転して、事件数が5件から16件へと急増し、年間で最も高い四半期となった。一方で、流出件数は30万件超から約19万4千件と減っている。これは前年同四半期の流出件数には前述のカード会社によるダイレクトメール印刷ミスによる約29万件が含まれていることによる。なお、2024年4-6 月期の流出件数には、クラウドサービスプロバイダーL社によるクラウド設定ミスによるカード情報流出約8,000件が含まれている。7-9月期、10-12月期については、いずれも事件数はほぼ横ばいだが、カード情報流出件数は約21,000件から約145,000件、約41,000件から約178,000件と大幅に増加している。

▼図1-5　2023年　と2024年のカード情報流出件数四半期別の推移



		1～3月	4～6月	7～9月	10～12月
2024年	事件数(件)	6	16	7	8
	カード情報流出件数(件)	23,677	194,241	145,032	177,772
2023年	事件数(件)	16	5	9	7
	カード情報流出件数(件)	173,322	301,545	20,593	40,831

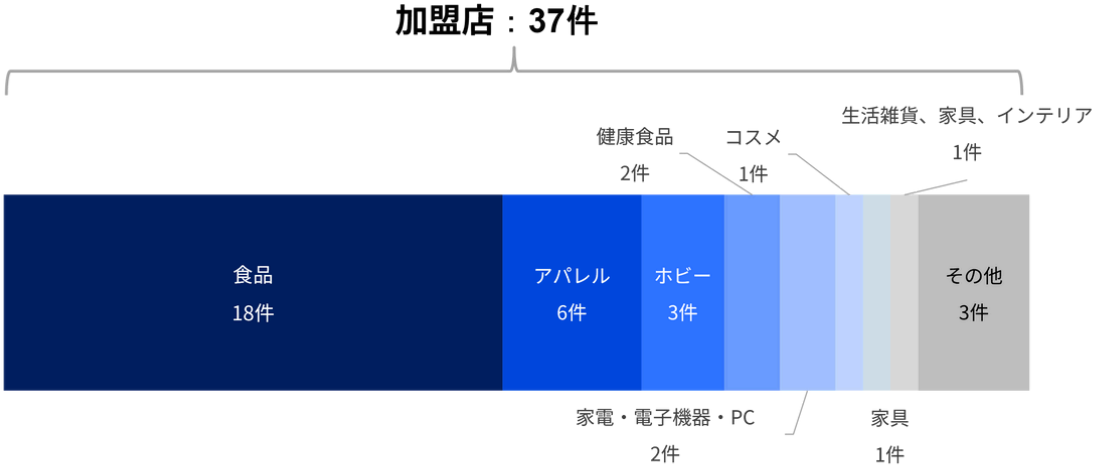
Cacco・リンク調べ

(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数

2024年のカード情報流出事件37件の内訳を図に示す。加盟店の内訳を取扱い商材別に見ると、最も多いのが食品（18件）、次いでアパレル（6件）／ホビー（3件）／健康食品（2件）／家電・電子機器・PC（2件）／コスメ（1件）／家具（1件）／生活雑貨・家具・インテリア（1件）となった。（図1-6）

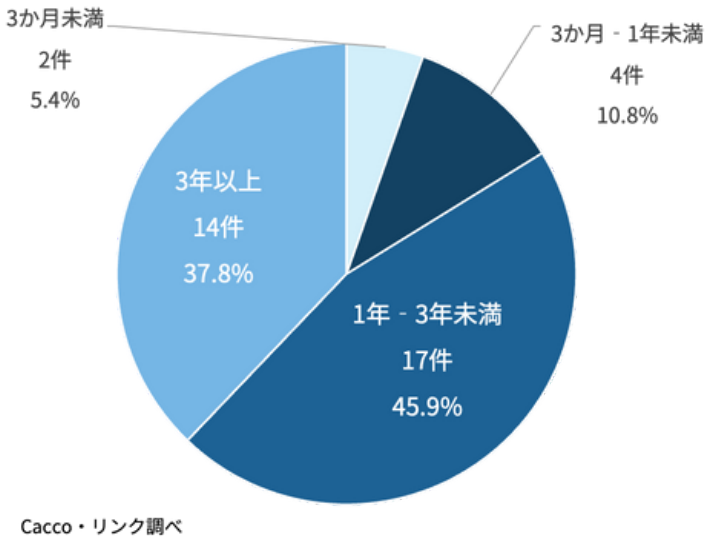
▼図1-6　2024年業種/取扱い商材別カード情報流出件数



Cacco・リンク調べ

流出期間別の割合は以下となる。1-3年未満の事件が17件、45.9%と最も多くを占めた。次いで3年以上が14件（37.8%）、3ヶ月-1年未満が4件（10.8%）、3ヵ月未満が2件（5.4%）だった。（図1-7）3年以上の割合が2023年の2.7%に比べると大きく上昇している。

▼図1-7　2024年流出期間別事件数



Cacco・リンク調べ

業種別・取扱商材別にカード情報流出件数と流出期間を集計した結果が以下の表である。

加盟店1件あたりの平均流出期間は945日で、2023年の417日から大幅に延びた。さらに、加盟店からの1事件あたりの平均流出件数は14,614件と、前年のカード会社の事故を除いた加盟店からの平均流出件数 7,107件の約2倍に増加している。1万件以上の大規模流出事件が15件と全体の約4割を占めたことが平均値を押し上げた。（図1-8）

▼図1-8　2024年業種・取扱い商材別カード情報流出件数/流出期間

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		37	540,722	945	14,614
加盟店取り扱い商材別	食品	18	337,563	944	18,754
	アパレル	6	100,401	1,183	16,734
	ホビー	3	20,615	826	6,872
	健康食品	2	9,687	1,123	4,844
	家電・電子機器・PC	2	9,005	359	4,503
	コスメ	1	15,198	1,080	15,198
	家具	1	3,958	1,038	3,958
	生活雑貨、家具、インテリア	1	1,432	964	1,432
	その他	3	42,863	786	14,288

Cacco・リンク調べ

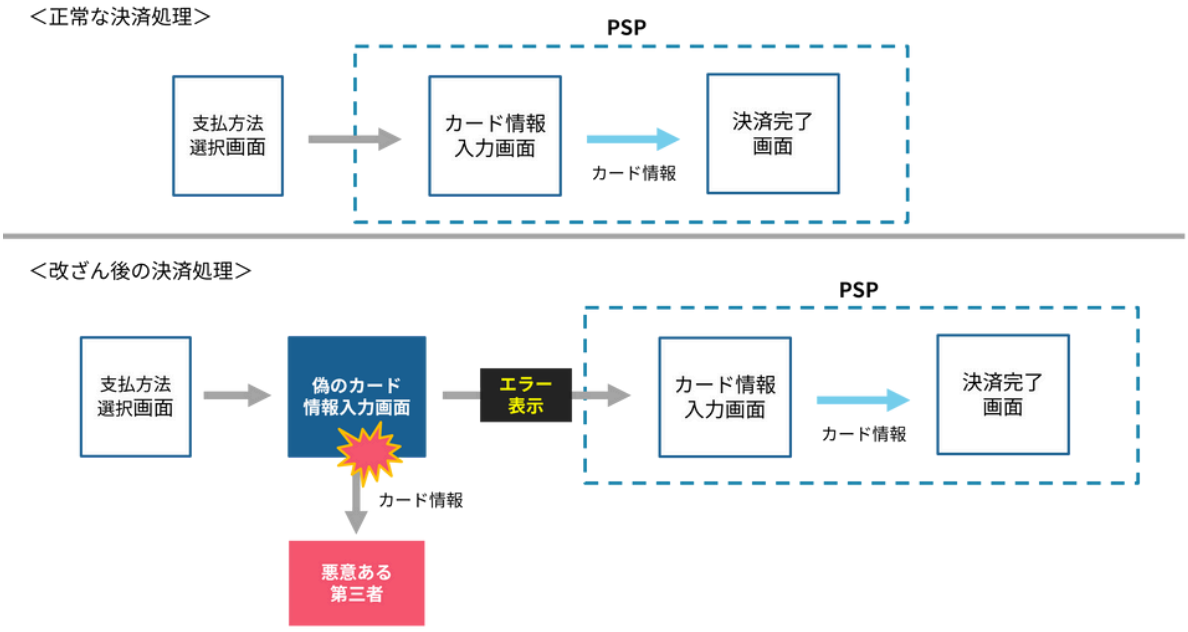
(2)-2. カード情報窃取の手口：オンラインスキミングがいまだ大半を占める

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、ほとんどの場合はセキュリティコードも一緒に流出する。

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【6.0版】』（以下『セキュリティガイドライン6.0』と記載）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事業者が提供する「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を埋め込むことで決済代行事業者にカード情報を送信する「JavaScript型（トークン型）決済」の導入を挙げており、国内のほとんどのECサイトがいずれかを導入している。しかし、オンラインスキミングの手口では、Webブラウザに表示された決済ページに消費者が入力した情報を直接窃取するため、非保持化を達成したECサイトであっても防ぐことは困難である。

一般に、決済代行事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事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い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1-9）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6.0』では、非保持化済みであるかどうかに関わらず、すべてのECサイトに対して、マルウェア対策、管理者権限の管理等の脆弱性対策の実施を指針対策として義務付けている（詳細は「4. 制度・政策の動向 (1)-1. EC加盟店に対する脆弱性対策の義務化」で解説）。

▼図1-9　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



『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、2024年に公表された37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1-10）

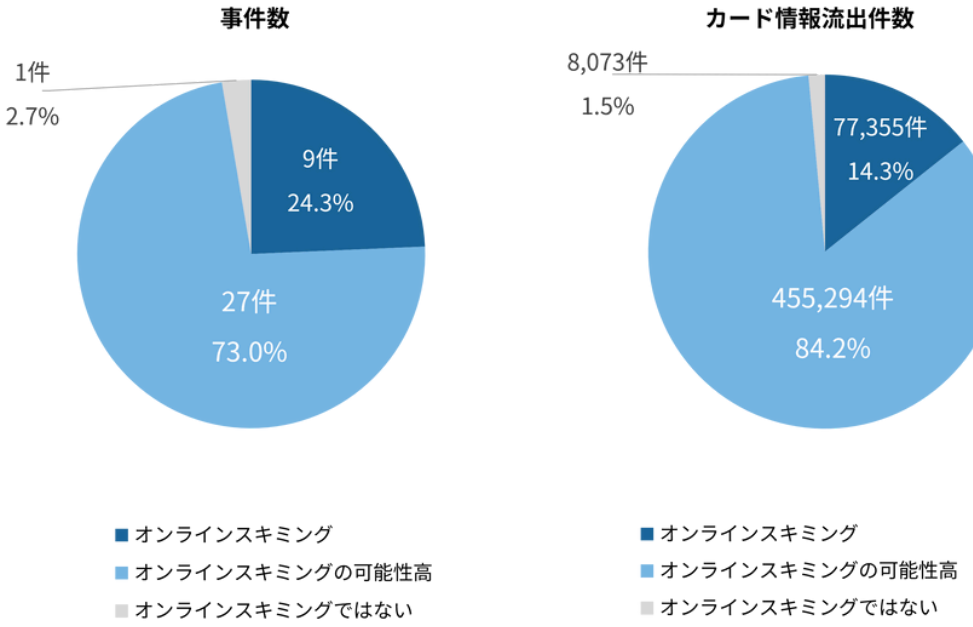
①オンラインスキミング：公式発表で「決済画面が2枚あった」「画面に入力したカード情報が第三者に送信された」等のオンラインスキミングであることがわかる記載がある。

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。

▼図1-10　2024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



リンク調べ

※「オンラインスキミングの可能性低」は、事件数、カード流出件数ともに数値が0なのでグラフから除外

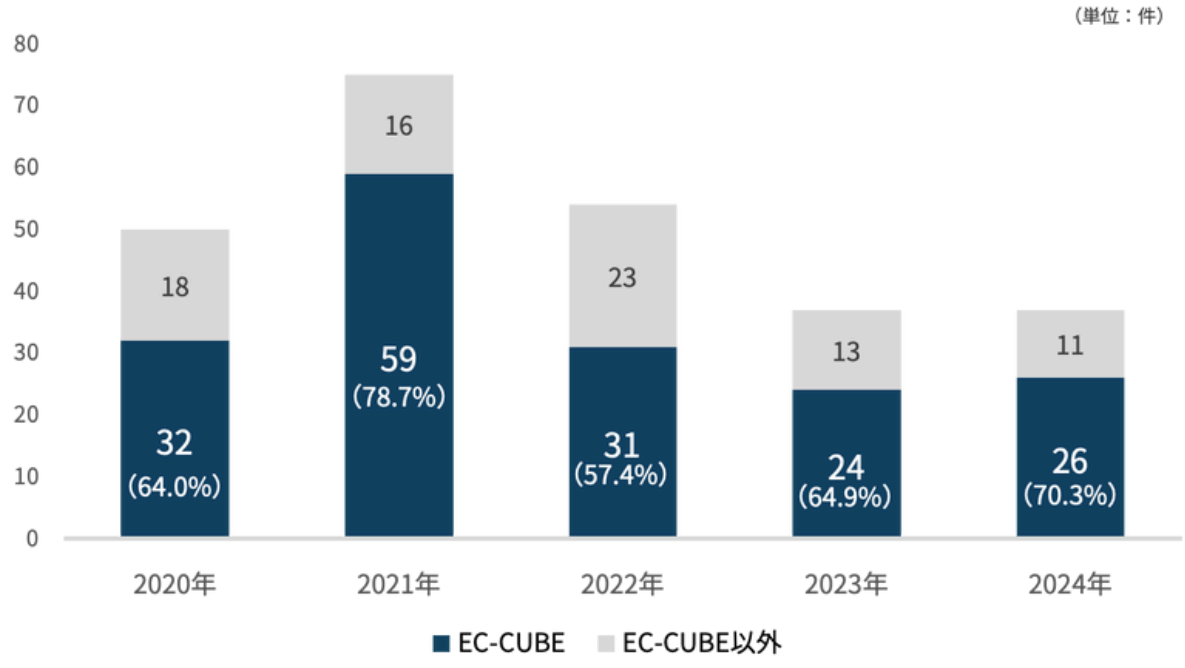
2024年に発生した37件のカード情報流出事件のうち、オンラインスキミングもしくはその可能性が高い事件は36件、97.3%となった。（図1-10）2023年はオンラインスキミング以外の流出事案が6件あったが、2024年は前述のクラウドサービスプロバイダーL社の設定ミスによる流出のみである。

(2)-3. プラットフォーム：引き続きEC-CUBEの割合が高い

オンラインスキミングでカード情報を窃取する攻撃者は、ECプラットフォームの脆弱性を狙うことが多い。国内においては、No.1のシェアを占めるEC-CUBEが攻撃の対象となりやすい。

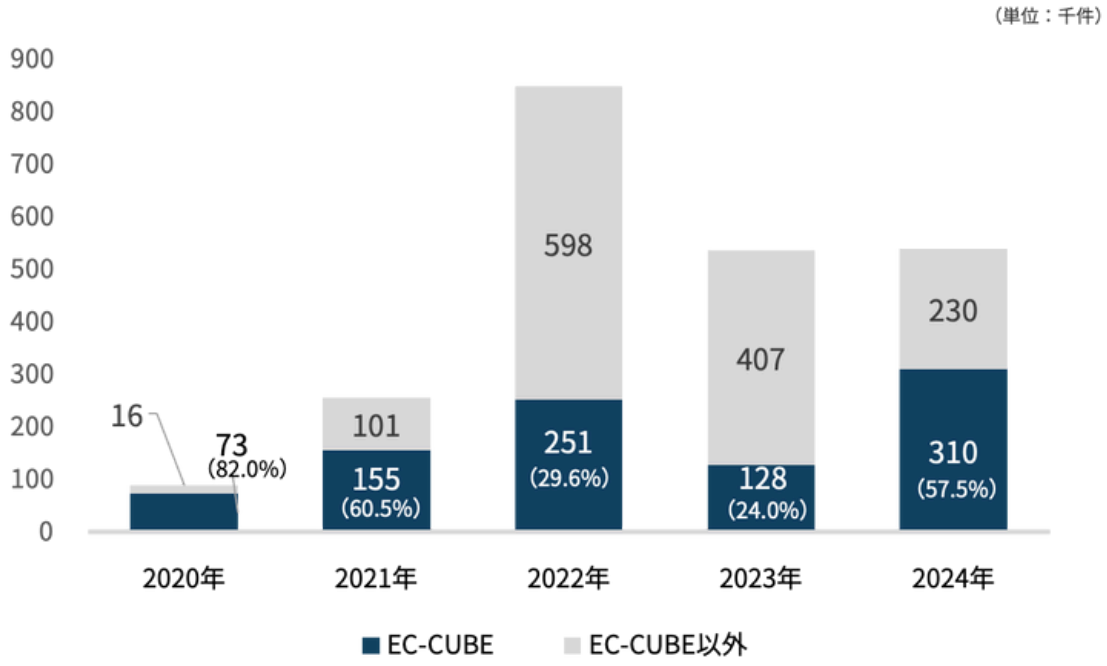
セキュリティ情報サイト「Fox Research」の調査結果をもとに2024年に発生したカード情報流出事件のうちEC-CUBEが占める割合を推計したところ、事件数で26件（70.3%）に達している。（図1-11）カード情報流出件数に占めるEC-CUBEの割合は310,689件（57.5%）と5割を超えている（図1-12）。

▼図1-11　2024年のカード情報流出事件　事件数に占めるEC-CUBEの割合



出所：『Fox Research』調査を元に作成

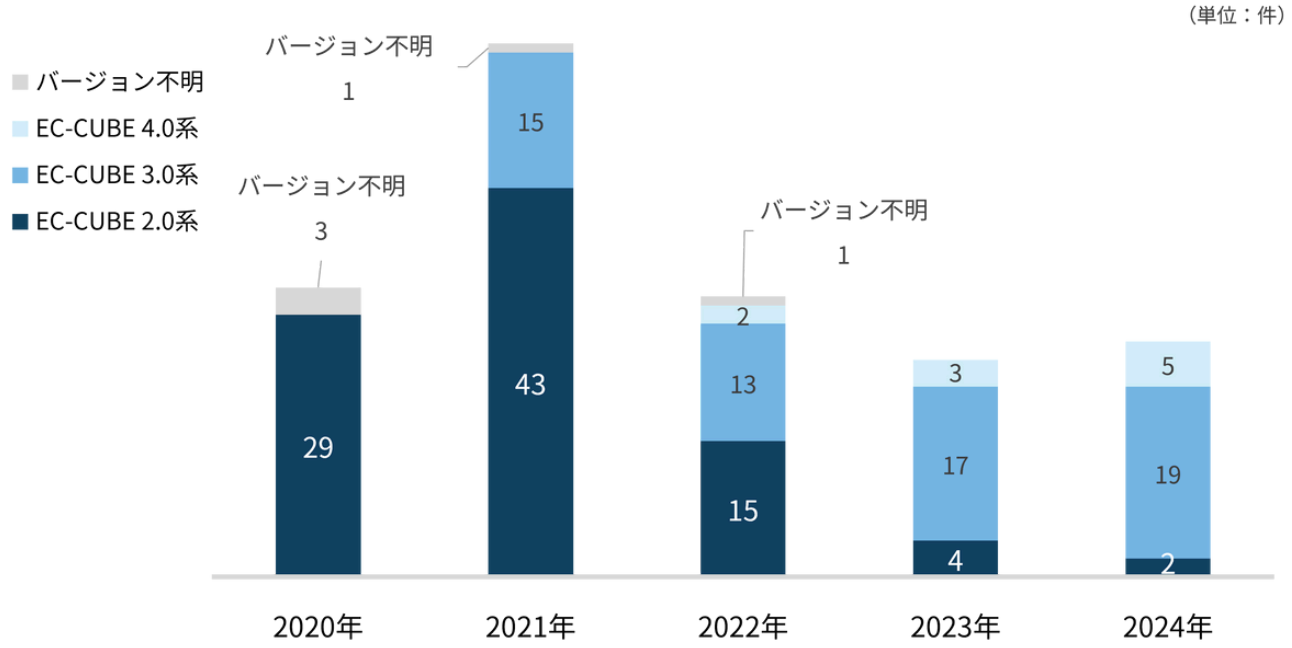
▼図1-12　2024年のカード情報流出事件 流出件数に占めるEC-CUBEの割合



出所：『Fox Research』調査を元に作成

攻撃を受けたEC-CUBEのバージョンについて、2020年から推移を調べたのが図1-13である。最も多かったのはEC-CUBE 3.0系で26件中19件であり、次いでEC-CUBE 4.0系が５件であった。EC-CUBE2.0系は2件まで減っている。2021年5月から6月にかけ、EC-CUBE 3.0系と4.0系で管理画面にクロスサイトスクリプティング（XSS）脆弱性があることが公表されており、これを悪用した攻撃が2024年の発覚時点まで続いていたと推定される。

▼図1-13　カード情報流出事件の発生サイトで使用されていたEC-CUBEのバージョン



出所：『Fox Research』調査を元に作成

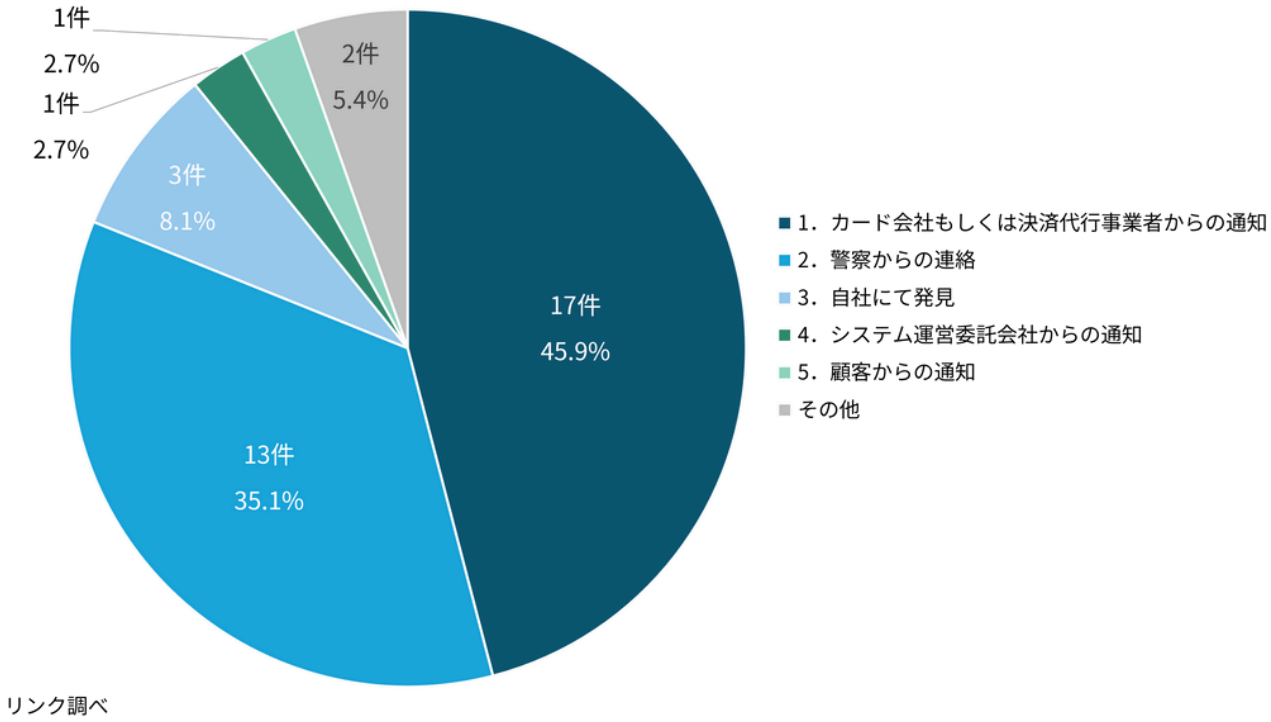
(3)2024年のカード情報流出事件のトピック

(3)-1. 警察の指摘によるカード情報流出発覚の増加

2024年に入り「警察が2021年頃に改ざんによるカード情報流出被害が発生したECサイトと同じプラットフォームで運用されているサイトを集中的に調査し、改ざんを指摘している」と報じられている。従来のカード情報流出事件の発覚は、カード会社や決済代行事業者からの指摘によるものが大半であったが、2024年は警察による指摘で発覚する事件の割合が増えた。

各社の公式発表に記載された事件発覚の経緯を元に、発覚のきっかけを集計したのが図1-14である。カード会社もしくは決済代行事業者からの通知によるものが17件（45.9%）と最も多いが、次いで多いのが警察からの指摘によるもの13件（35.1%）である。「不明」となっている2件についても、「外部機関の指摘」という記載がされており、警察からの指摘である可能性がある。

▼図1-14　2024年に公表されたカード情報流出事件発覚のきっかけ

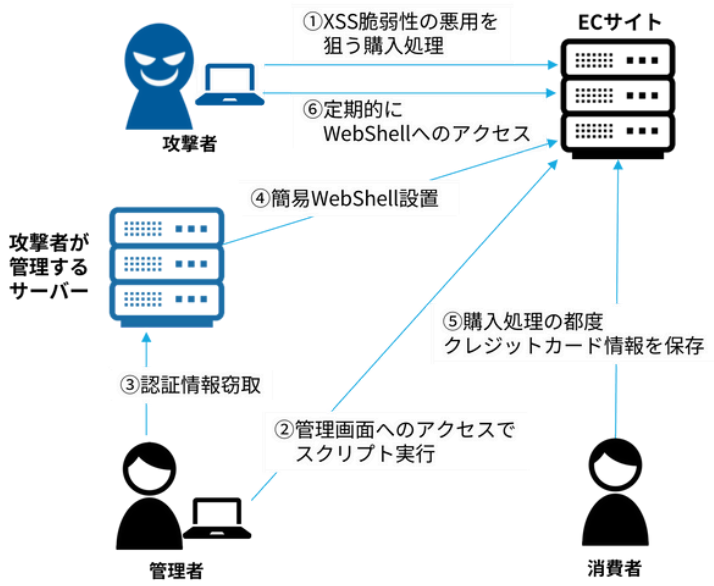


リンク調べ

警察が指摘した13件の事件について、流出開始年（サイトを改ざんされた時期）は全て2021年である。プラットフォームの内訳は、EC-CUBE3.0系が7件、EC-CUBE4.0系が４件、その他のプラットフォームが2件となっている。前述の通り、警察は主にEC-CUBEで確認された犯行手口（以下に詳細）について横断的に調査したと推測される。

2021年5月から6月にかけ、EC-CUBE 3.0系、4.0系で相次いで管理画面にクロスサイトスクリプティング（XSS）脆弱性があることが公表されたが、それに先立つ2021年4月には、トレンドマイクロからECサイトのXSS脆弱性を悪用した攻撃キャンペーン「Water Pamola」が報告されていた。2021年7月には、JPCERT/CCによりEC-CUBEを使用したサイトに対して同様の攻撃を確認したとして、手口が公開されている。まず、攻撃者は、注文フォームから不正なスクリプトを含んだ文字列を入力し、購入処理を行う。ECサイトの購入処理にXSS脆弱性が存在する場合は、管理者がECサイトの管理画面を閲覧することで不正なスクリプトが実行され、管理者の認証情報の窃取が行われる。盗んだ認証情報で管理者ログインした攻撃者は、不正ファイルや不正JavaScriptの設置などを行う。（図1-15）

▼図1-15　XSS脆弱性を悪用した管理画面からの侵入

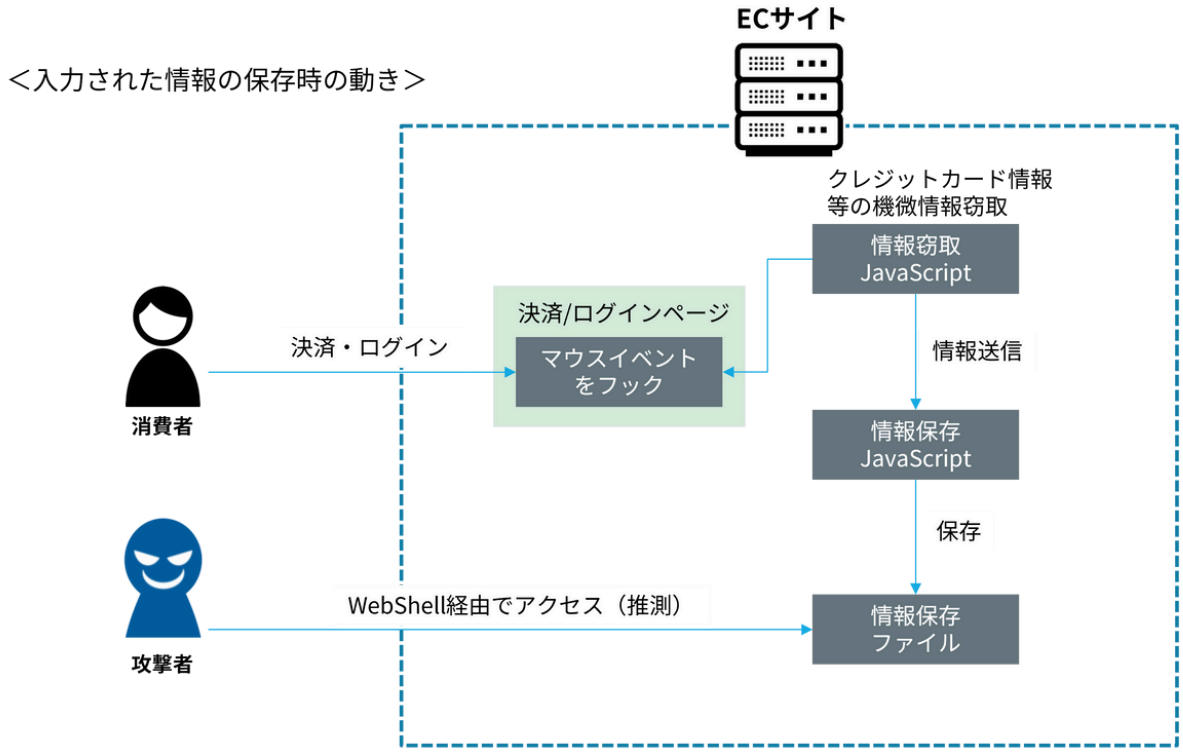


設置されたファイル	内容
WebShell	・多機能なWebShell（中国語をベースとしており、ツール名は不明）
データベース操作ツール	・Adminer version 4.2.4
情報窃取JavaScript	・ボタンをクリックした際にクレジットカード情報などを送信する ・ログインページや決済ページでロードされる
情報保存JavaScript	・“情報窃取JavaScript”からの情報送信先 ・受信したデータを“情報保存ファイル”に保存する
情報保存ファイル	・クレジットカード番号、有効年月、セキュリティコード、メールアドレス、パスワードなどが保存されている
簡易WebShell	・ア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

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

いったん不正なスクリプトが設置されると、消費者による「送信」ボタンのクリックをトリガーとして、入力された情報がECサイト内に作成された情報保存用ファイルに保存される。このファイルを攻撃者がサーバーに定期的にアクセスして取得することで、消費者の認証情報やカード情報を不正に窃取していたと推測されている。（図1-16）

▼図1-16　消費者が入力した情報の保存と窃取



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

2025年に入ってからも警察の指摘をきっかけとしたカード情報流出事件の公表は続いている。こうした事件では、長期間にわたり流出が続いているため、カード情報流出件数も大きくなる傾向がある。

EC加盟店は再度、自社サイトを調査し、改ざんが放置されていないかを調査すると共に、プラットフォーム事業者の提供するパッチの適用やプラットフォーム自体のバージョンアップなどの対応を適切に行う必要がある。

(3)-2. クラウドの設定ミスによるカード情報流出

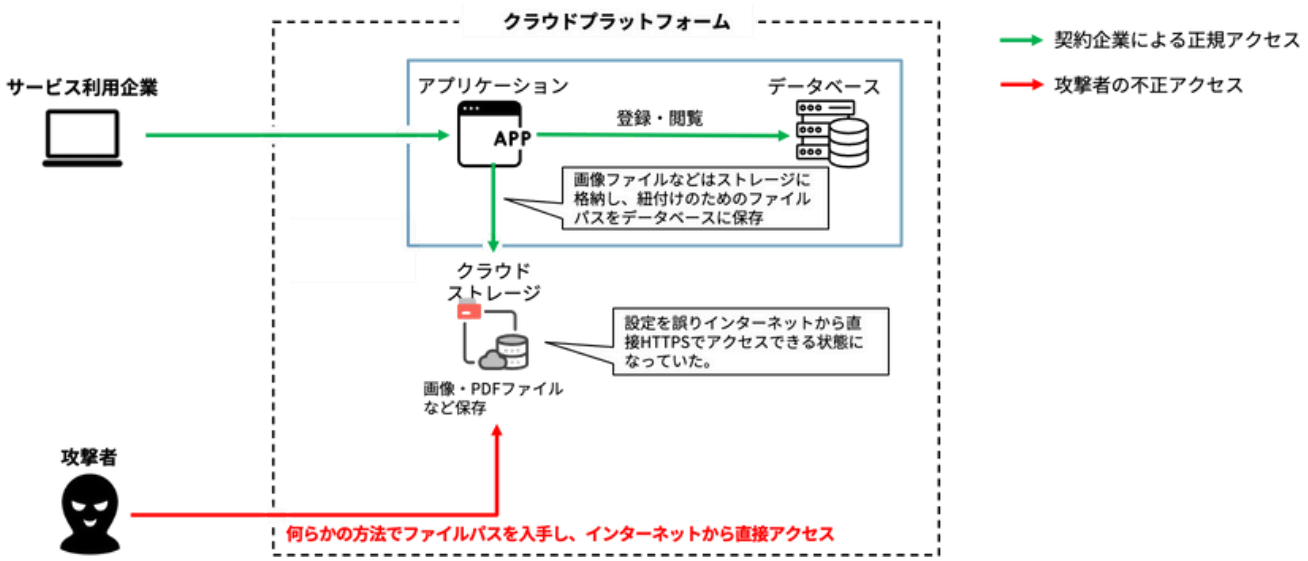
2024年3月、人事労務系SaaSサービスを提供するL社が、自社サービスのプラットフォームとして利用しているクラウドストレージのアクセス権限設定の誤りにより、外部から重要な個人データの閲覧・ダウンロードが可能な状態になっていたことを発表した。2020年1月から2024年3月まで、4年以上にわたって外部からアクセスが可能な状態となっていた。2023年12月28日・12月29日には第三者による不正アクセスの実行も確認されている。

L社が提供していたのは、飲食店や小売店など非正規雇用が多い企業向けの人事労務業務を効率化するサービスである。外部から閲覧可能となっていたクラウドストレージには、ユーザーがアップロードした各種身分証明書等のPDFファイル及び画像ファイルが保存されていた。本来、これらのファイルに対しては、サービス利用企業が、正規のアプリケーションを通してアクセスすることをのみを想定していた。しかし、クラウドストレージのアクセス権限の設定の誤りにより、約16万人分の個人データが外部から閲覧・ダウンロード可能となっており、約15万件がダウンロードされた痕跡が確認された。

流出した個人データには、当該ファイル内の氏名、住所、生年月日、性別、電話番号等の個人情報の他、マイナンバーや要配慮個人情報（健康診断情報、障害情報など）が含まれていた。また、2024年3月の速報時には、L社は流出した情報にカード情報は含まれていないとしていたが、5月の最終的な発表時に8,073人分のカード情報が含まれると訂正した。

設定不備の詳細と流出経路の詳細については公表されていないが、クラウドプラットフォームが提供するストレージサービスの中には、公開設定することでリソースのURLを指定してインターネットから直接アクセス可能になるものがある。そうしたサービスの権限設定ミスを利用され、第三者に個人データを窃取されたと推測される。（図1-17）

▼図1-17　想定される設定不備と流出経路（推測）



クラウドサービスを利用する場合、最小権限の原則に従い、個々のシステムコンポーネントに対するアクセス権を正しく設定する必要がある。また、プラットフォーム側のバージョンアップや新機能リリースにより、意図しない権限の変更や新たな権限の追加が行われる場合があるため、リリースノートを見落とさないよう注意する。

CIS Benchmarks（米国の営利団体CIS（Center for Internet Security）が策定した、システムやソフトウェア、クラウドサービスのセキュリティ設定に関するベストプラクティス集）を参照することで、OS・ミドルウェア・クラウドサービスにおける推奨セキュリティ設定を確認し、網羅的な評価が可能となる。大手のクラウドサービスはAWS Security Hub（AWS）、Microsoft Defender for Cloud（Azure）、Security Command Center（Google Cloud）のような統合セキュリティ評価サービスを提供している。推奨セキュリティ設定には、CIS Benchmarksなどのセキュリティ基準が含まれており、その時点での準拠状況を自動的に短時間で評価し、設定の不備を確認できる。同様の事件を起こさないためにもそれらのサービスを利用することを推奨したい。

2. 2024年のECサイトにおける不正利用の概況

2024年のEC市場は、前年比9.23%増の24.8兆円（消費者向け物販系分野）という高い成長率を記録している。一方、この市場成長に伴い、クレジットカード不正利用をはじめ、転売不正、ポイント不正取得、後払い未払いなど、さまざまな不正注文の手口が確認されている。

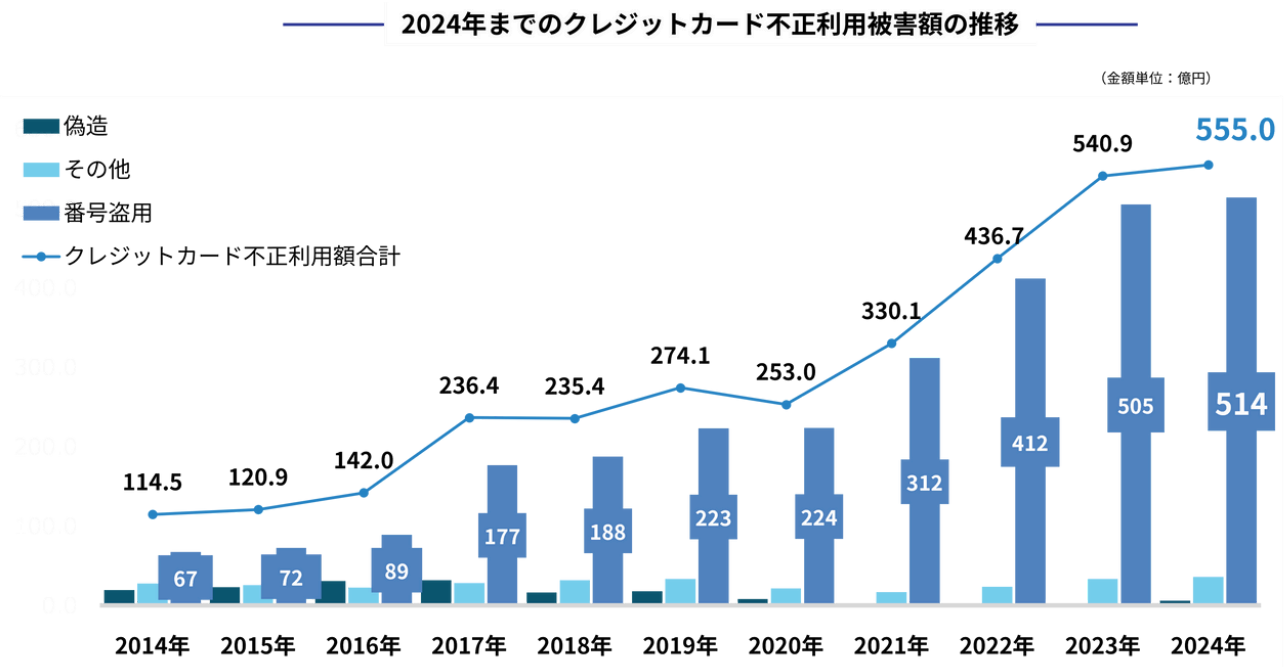
その中でもCaccoのユーザーから特に多くの相談が寄せられているのが、他人のアカウントを悪用した不正ログイン、クレジットカードの不正利用（他人のクレジットカード情報を用い、カード保有者になりすまして決済する行為）と転売不正（転売を目的として、初回限定価格など注文に条件がある商品や数量限定販売の商品などを不正に購入する行為）である。本節では、ECサイトの不正利用被害の概況について述べた後、それらの不正注文について、Caccoが提供する不正検知サービス「O-PLUX」を導入するECサイト（累計12万サイト）のデータを元に詳しく分析していく。

(1)クレジットカード不正利用被害額の推移

(1)-1. クレジットカード不正利用被害額と傾向

2024年の年間クレジットカード不正利用被害額は、555億円で前年に比べて23.9億円の増加 となった。（図2-1）2021年以降は毎年100億円以上の増加となっていたのに比べると増加のスピードは鈍化したが、被害は高止まりしている。内訳としては、「番号盗用」が513.5億円で全体の92.5%を占めている。その多くはECサイトでの不正注文によるものである

▼図2-1　クレジットカード不正利用被害額の推移



出所：（『クレジットカード不正利用被害額の発生状況』 日本クレジット協会）2025年6月

(1)-2 . クレジットカード不正利用被害増加の要因

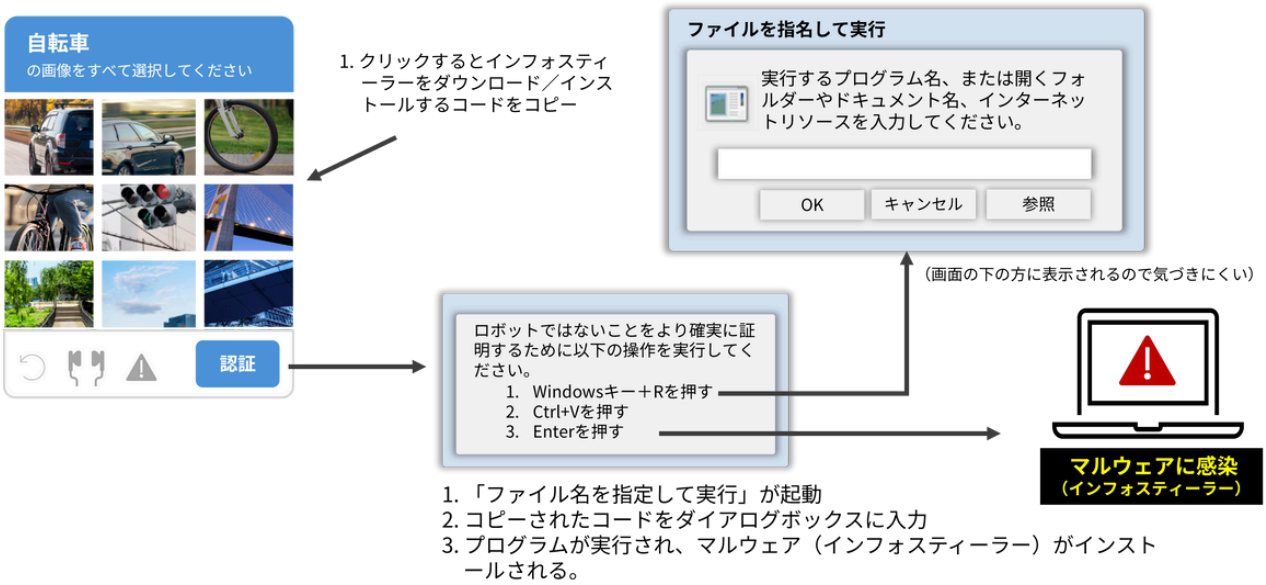
攻撃者は年々巧妙化・多様化する手口でクレジットカード情報を取得している。2023年に引き続き、フィッシングによる情報窃取や、カード番号の規則性を悪用して有効な番号を生成する「クレジットマスター攻撃」が継続的に発生している。

2024年の特徴として、情報窃取に特化したマルウェア「インフォスティーラー」による被害が増加している。（図2-2）IBMの調査 によれば、世界中でインフォスティーラーによる攻撃は増加しており、2024年は前年と比較してインフォスティーラーを感染させる目的のフィッシングメールの数は84%増加した。

感染の手法は、メールやSMSを経由して送信されるURLをクリックしてサイトにアクセスさせる方法の他、インターネット広告を利用して誘導したサイトで無料アプリや無料情報のダウンロードを促しインフォスティーラーをダウンロードさせる手法、CAPTCHA認証に見せかけたClickFixによる方法など多岐にわたる。（図2-3）

▼図2-2　インフォスティーラー

▼図2-3　ClickFix



インフォスティーラーに感染すると、キーロガーにより入力したり、Webブラウザに保存しているカード情報や認証情報が抜き取られる。マルウェア対策ソフトをすり抜け、短時間で情報を奪取した後に、痕跡を消すため自らを削除することがあることから、発見や防止が極めて難しい。流出したカード情報や認証情報は、ダークウェブで販売される他、2023年ごろからはテレグラム（匿名性の高いメッセージングアプリ）のチャンネルを通した売買が増えている。

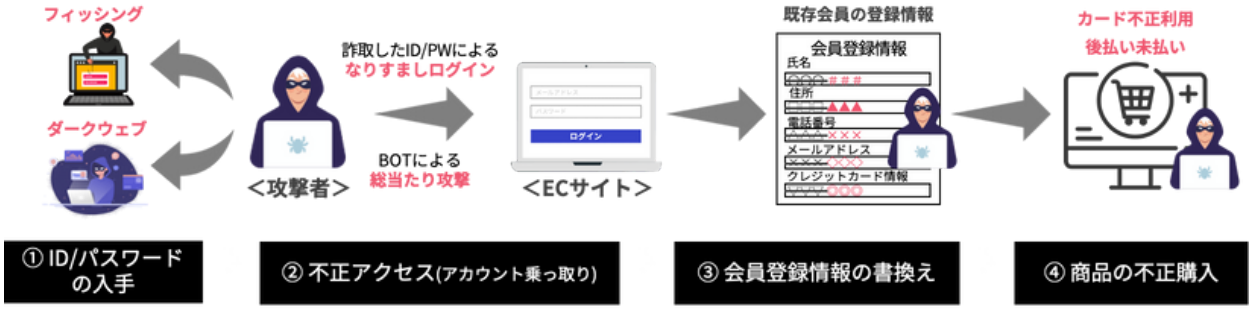
不正に購入した商品の転売や現金化には、以前からフリーマーケットサイト（フリマサイト）などのCtoCマーケットが使用されているが、その傾向は2024年も継続している。特に近年では、SNSや掲示板で募集される「闇バイト」（図2-4）によって、一般人がフリマサイトでの商品の出品、購入、受け取りといった役割を担うケースが増加している。攻撃者は直接関与せずとも商品が市場に流通する分業体制を構築できるため、追跡は一層困難となり、取引の秘匿性が高まっている。これが被害拡大を後押しする構造的要因となっている。

▼図2-4　闇バイト

他人のカード情報などの不正利用に加え、ECサイトのアカウント乗っ取り被害も増加傾向にある。国家公安委員会などが発行したレポートによれば、2024年の不正アクセス禁止法における不正アクセス行為の検挙件数のうち、識別符号窃用型（アカウント乗っ取り）が90%以上を占めている。また、都道府県警察から警察庁に報告された不正アクセス行為のうちインターネットショッピングでの不正購入につながった件数は180件と2023年（93件）の約2倍となっており、ECサイトのアカウント乗っ取り被害が増加していることがうかがえる。これらの数字は、警察への届出や検挙につながったものであり、実際の発生数はそれよりも多い。Caccoの取引先のECサイトからもアカウント乗っ取りに関する相談が実際に増えている。 アカウント乗っ取りは、攻撃者はフィッシングやダークウェブで入手したID・パスワードを悪用して既存会員のアカウントになりすまし、ログインを行う。ログイン成功後に、当該アカウントに予め登録済みのカード情報を悪用して不正注文することで、攻撃者は新たにカード情報を詐取することなく、IDとパスワードのみで効率的に不正注文を行えることになる。（図2-5）

こうした脅威の高まりを受け、『クレジットカード・セキュリティガイドライン【6.0版】』(以下『セキュリティガイドライン6.0』と記載）では、EMV 3-Dセキュア（以下EMV3-DS）の導入や不正ログイン対策などが義務化され、事業者に対してアカウントの登録、購入、配送に至る一連のプロセス全体における多層的な防御策の実装が求められている（詳細は「4. 制度・政策の動向 -(1）クレジットカード・セキュリティガイドライン6.0版について」で解説)。

▼図2-5　アカウント乗っ取り



(2)ECサイトにおける不正注文の傾向

(2)-1.「O-PLUX」導入ECサイトにおける不正注文の傾向

「O-PLUX」を導入するECサイト（累計12万サイト）を対象に、O-PLUXの審査でクレジットカード不正利用と判定された注文の割合、および転売不正と判定された注文の割合を集計した。それらの不正と判定された注文とは、不正注文の種類ごとに判定される「O-PLUX」の審査でNGと判定された注文を指す。2024年のクレジットカード不正利用発生率は2.4%で2023年に比べて0.8ポイント増加した。また転売不正の発生率は8.3%と2023年に比べて2.6ポイント増加、2020年に比べると5年間で6倍以上に増加している。（図2-6）転売不正の内容としては、これまでと同様、コスメやヘアケアなどの初回限定価格の商品が対象となることが多い。

▼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

年度	クレジットカード不正利用発生率
2020年	0.9%
2021年	1.2%
2022年	1.6%
2023年	1.6%
2024年	2.4%

年度	転売不正発生率
2020年	1.3%
2021年	1.4%
2022年	2.5%
2023年	5.7%
2024年	8.3%

※1「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）
※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。

高リスク商材とされるデジタルコンテンツ、チケット、家電はいずれも不正注文において上位を維持した。（図2-7）特にオンラインゲームや動画配信などのデジタルコンテンツは、即時性と換金性の高さから3年連続で3位以内となっている。また、コスメ・ヘアケアや健康食品・医薬品といった低単価ながら需要が安定した商材も継続して上位に入り、CtoCマーケットや闇バイト経由での転売に適しているとを目的に狙われたと考えられる。

2024年は新たに、8位にふるさと納税、12位にサブスクサービスがランクインした。ふるさと納税では返礼品を狙った不正が目立ち、 保存しやすい酒類や小型家電が標的となった。サブスクサービスでは最新家電やカメラなどのレンタルが狙われ、レンタル品を詐取するケースも確認された。

▼図2-7　商材別不正注文検知件数ランキング

順位	2022年	2023年	2024年
1	ホビー・ゲーム	デジタルコンテンツ	カメラ・映像/音響機器
2	デジタルコンテンツ	ホビー・ゲーム	ホビー・ゲーム
3	チケット	旅行	デジタルコンテンツ
4	健康食品・医薬品	コンタクト・メガネ	チケット
5	コスメ・ヘアケア	チケット	健康食品・医療品
6	コンタクト・メガネ	健康食品・医薬品	総合通販
7	食品・飲料・酒類	コスメ・ヘアケア	コスメ・ヘアケア
8	美容機器	食品・飲料・酒類	ふるさと納税
9	MVNO	EC総合通販	家電・PC・タブレット
10	PC・タブレット＆家電	家電・PC・タブレット	日用品・雑貨・キッチン用品
11	EC総合通販	アパレル	食品・飲料・酒類
12	工具	家具	サブスクサービス

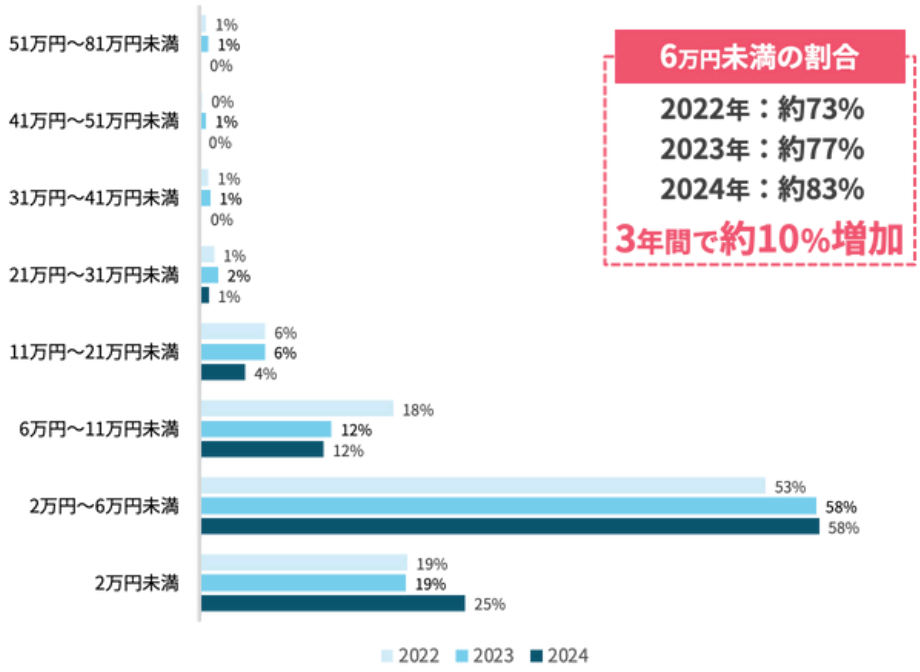
※1「O-PLUX」の審査で、審査件数全体に占める審査結果NGの割合を件数ベースで商材ごとに算出。NGの割合が多い順にランキング（Cacco調べ）
※2 最終的に出荷停止や注文を拒否するなどの対応は、「O-PLUX」加盟店判断により異なる。

(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

2024年のクレジットカード不正利用では、前年に引き続き注文金額の低額化の傾向が見られた。6万円未満に着目すると、3年間で10ポイント増加しており、内訳は2022年が73%、2023年が77%、2024年には83%と、年を追うごとに不正被害の低額化が着実に進んでいることが分かる。（図2-8）低額化の背景には、不正利用を発覚しにくくするという狙いがあると考えられる。高額な取引は事業者やカード会社に検知されやすいが、少額取引は通常の購入行動に紛れ込み、チェックをすり抜けやすい。

さらに、近年は少額取引を複数回に分散させるケースも確認されている。自動化ツール等を用いることで、少額注文を繰り返すことは手間にならず、むしろ検知を回避しつつ、確実に利益を積み上げる合理的な手口になっていると考えられる。

▼図2-8　クレジットカード不正利用注文金額の分布



「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）

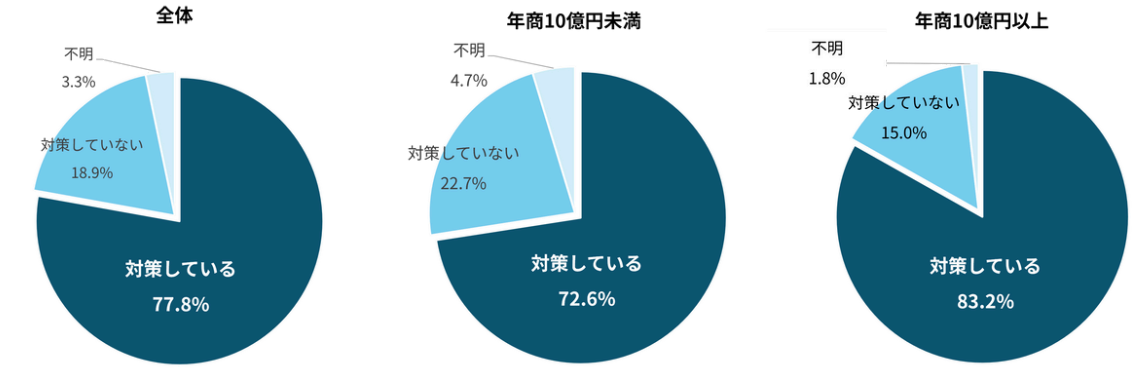
(2)-3. EC事業者の不正注文対策状況とEMV 3-Dセキュアの導入率

Caccoでは、EC事業者の不正被害や対策の実態を把握するため2021年より年に1度「EC事業者実態調査」を実施している。最新の調査は2024年12月、全国のEC事業者550名の不正注文対策に関わる担当者を対象にセキュリティ意識や具体的な対策状況を調べた。

調査の結果、全体の77.8%が何らかの不正注文対策を実施しており、前回（74.9%）から約3ポイント上昇した。年商別では、10億円未満の事業者で72.6%、10億円以上では83.2%が対策を実施しており、企業規模が大きいほど実施率が高い傾向は前年同様である。（図2-9）

▼図2-9　EC事業者の不正注文対策状況

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。

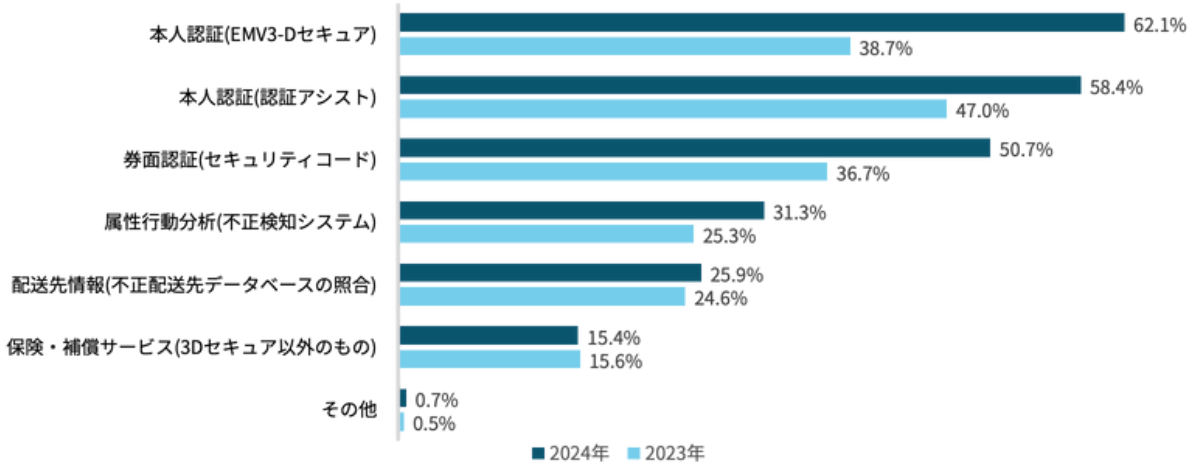


EC事業者実態調査（Cacco調べ）2024年12月調査

導入されている対策の中で最も多かったのは「本人認証（EMV 3-Dセキュア、以下EMV3-DS）」で62.1%と過半数を占めた。2023年に比べると23.4ポイントの増加となっている。これは2024年3月に公表された『セキュリティガイドライン5.0』において、2025年3月までにEMV3-DSの導入が義務化されたことが背景にあるとみられる。次いで「本人認証（認証アシスト）」が58.4%と続き、本人認証系の対策が上位を占めた。「属性行動分析（不正検知システム）」も31.3%で、前年（25.3%）から6.0ポイント増加しており、AIや機械学習を活用した不正検知ツールの導入が進んでいることがうかがえる（図2-10）。その他、券面認証や配送先情報の突合など、多層的な対策も一定数採用されている。

▼図2-10　事業者が実施する対策方法

Q：実施している対策方法はなんですか（複数回答）



※1 3Dセキュア1.0は2022年10月にサービス終了しているため除外
※2 対策をしていると回答した人の中での割合を集計。N=411(2023年)、N＝428(2024年)

EC事業者実態調査（Cacco調べ）2024年12月調査

EMV3-DSの導入は対策の終着点ではない。実際、中間者攻撃（詳細は「3. 他の金融サービスにおける不正取引 (1) オンライン証券取引口座乗っ取りによる不正取引」を参照）などのEMV3-DSをすり抜ける突破する手口も確認されており、ガイドラインでも多層的な対策防御の重要性が強調されている。

EMV3-DSを導入している事業者のうち、不正検知システムを併用する事業者の割合は、2023年は28.0%だったのに対し、2024年は37.6%と9.6ポイント上昇していた。（図2-11）こうした動きからも、本人認証と属性行動分析を組み合わせるなどの複数の対策を重層的に導入する加盟店が今後も増えていくことが推測される。

▼図2-11　EMV3-DSと属性行動分析の不正検知システム併用の割合

	2024年	2023年
EMV3-Dセキュア+不正検知システム	37.6%	28.0%
EMV3-Dセキュアのみ	62.4%	72.0%

EC事業者実態調査（Cacco調べ）2024年12月調査

(3)2024年のECサイトにおける不正利用のトピック

(3)-1. オフライン取引を悪用した カード不正利用が発生

2024年には、カード保有者がカード利用停止した後も数か月にわたって不正利用が継続される事案が多発し、大きな問題となった。クレジットカードの不正利用が発覚した際、通常はイシュア（カード発行会社）への連絡によって利用停止措置がとられ、被害拡大が防がれる。カードの利用を止めても不正利用が止まらないのは、「オフライン取引」が悪用されたことによるものである。

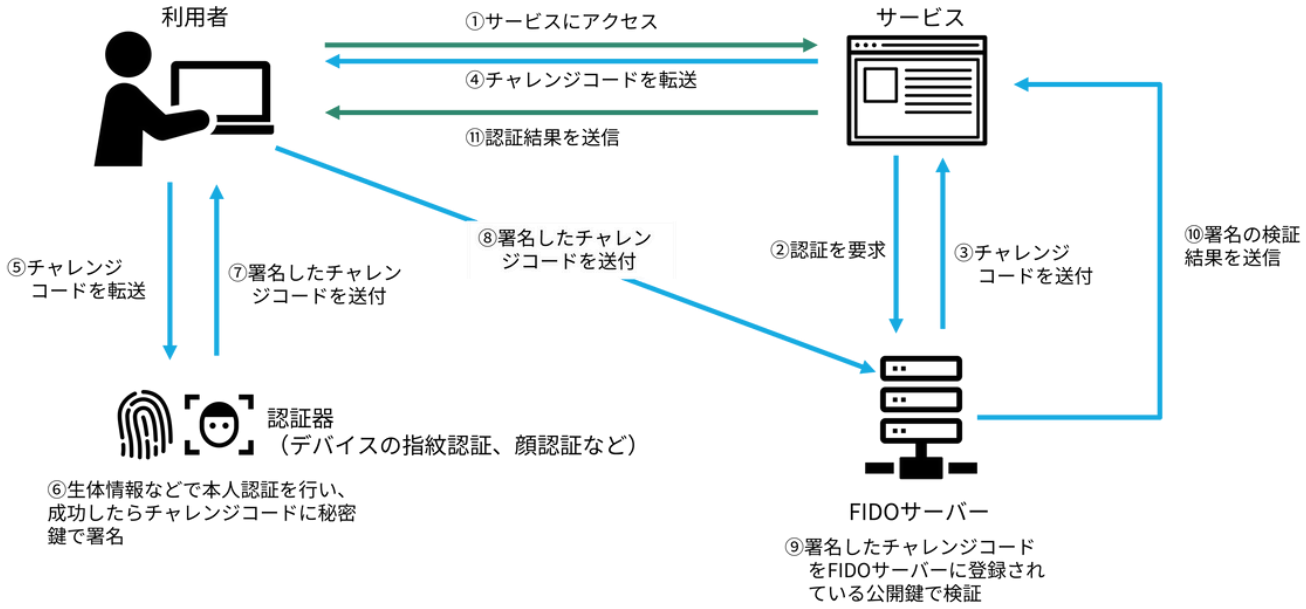
オフライン取引とは、少額決済においてネットワークを通じた即時のオーソリゼーション（与信承認）を省略する仕組みであり、利便性を重視して導入されている。その結果、カード停止後も決済が継続してしまう脆弱性が存在する。

この脆弱性を突く手口として、Apple Payに他人のカード情報を不正に登録し、少額決済を繰り返すケースが報告されている。Apple Payにカードを登録する際、通常はSMS等によるワンタイムパスワード（OTP）などの本人認証が求められる。しかし当該イシュアのカード会員向けスマートフォンアプリでは、会員の利便性を高めるため、アプリにログインした状態でアプリ内メニューからApple Pay登録を行う際に本人認証を省略できる仕様となっていた。攻撃者はこの仕様を悪用して、フィッシング等で取得した認証情報でカード会員向けアプリに不正ログインし、自分のスマートフォンのApple Payに他人のカード情報を登録していたと考えられる。

ひとたび登録に成功すると攻撃者はカード情報を登録したスマートフォンを機内モードにして少額の決済を繰り返す。機内モードにしていても、少額決済はオフライン取引で実行される。なおかつ、機内モードなのでカード会社からの利用停止などのオンライン制御も効かないため、被害者が不正利用に気づいてカード会社に利用停止措置を依頼しても決済が止まらない状態となる 。当該イシュアは、2025年2月期の決算で損失補填のために99億円を計上した。

オフライン取引は、ネットワークに接続せずに処理されるため、カードを停止しても一定額以下の決済が継続してしまうという構造的な脆弱性を抱えている。対策としては、イシュアが自社の会員向けサービスへのログインの際の認証を強化する必要がある。専用スマートフォンアプリのログイン時に多要素認証やパスキー（生体認証等を使用したパスワードレス認証の仕組み・図2-12）を全ての会員に必須化する。さらにApple Pay、Google Payなどにクレジットカードやブランドデビットカードを登録する際には追加で本人認証を必ず求め、不正な登録そのものを防ぐことが重要である。

▼図2-12　パスキー



(3)-2. 不正注文に対する事業者の意識と実態（2024年度版 EC事業者実態調査より）

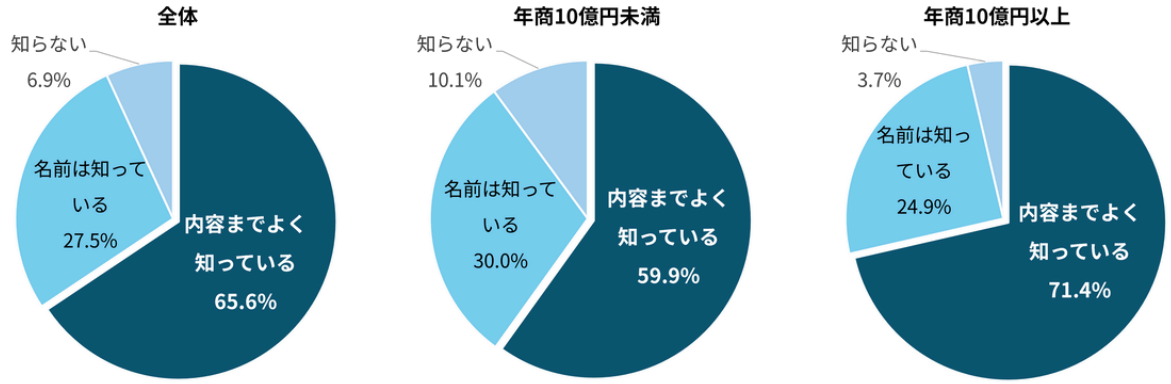
「(2)-3 EC事業者の不正注文対策状況とEMV 3-Dセキュアの導入率」でも一部触れたが、ここでは同調査の中から、クレジットカード不正利用に対する事業者の意識、被害の実態について整理する。

1.不正利用対策の「線の考え方」は9割以上が認知

『クレジットカード・セキュリティガイドライン【5.0版】（2024年3月発行）』では、クレジットカード不正利用への対策の新たな考え方としてカード決済時に加えて決済前、決済後という場面ごとに対策を考える「線の考え方」を初めて提示した。『セキュリティガイドライン6.0』にも継続して記載されている（詳細は「4. 制度の動向(1)-2. 「線の考え方」に基づく不正利用対策への指針対策追加」を参照）。2024年版のEC事業者実態調査においては、「線の考え方」の認知度（「内容までよく知っている」＋「名前は知っている」）は、全体で93.1%となった。65.6%は内容までよく知っており、EC事業者に浸透している様子がうかがえる。年商10億円以上の事業者では71.4%が内容までよく理解しており、規模の大きい事業者ほど理解度が高い傾向がみられる（図2-13）。

▼図2-13　線の考え方」認知状況

Q：2024年に公表された最新の「クレジットカード・セキュリティガイドライン5.0版」にて、EC事業者がとるべき対策として、クレジットマスター、不正ログインなども追加され「線の対策」が推奨されていることを知っていますか。

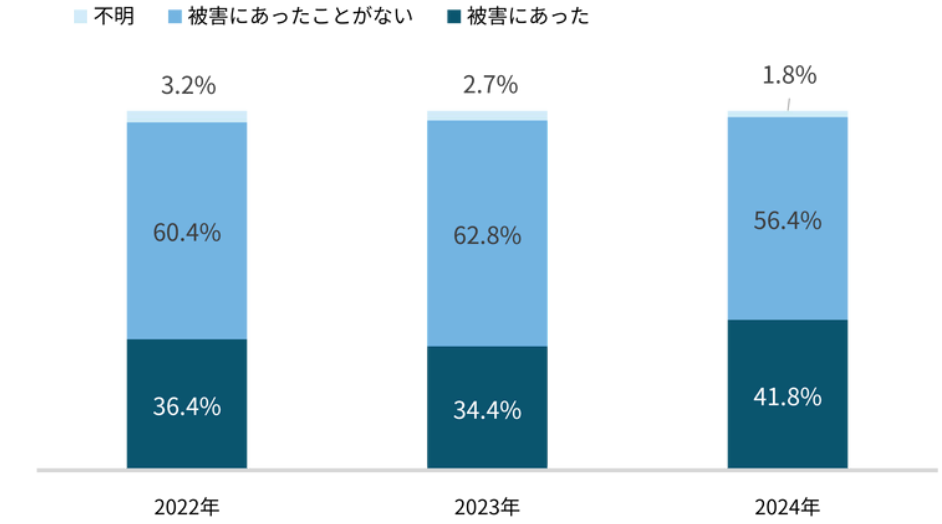


EC事業者実態調査（Cacco調べ）2024年12月調査

2．不正注文被害は4割が経験

2024年版EC事業者実態調査において、不正注文被害にあったと回答したEC事業者の割合は2023年に一時的に若干減少したものの、2024年には再び増加し、全体の41.8%が被害を経験していた。（図2-14）被害内容は、「チャージバック（クレジットカード不正利用）」が52.6%と最多である。（図2-15）被害額は「25～50万円未満」が最も多く、2022年の「50～100万円未満」がボリュームゾーンだった時期に比べれば低額化しているものの、依然として事業者にとって看過できない損失となっている。（図2-16）

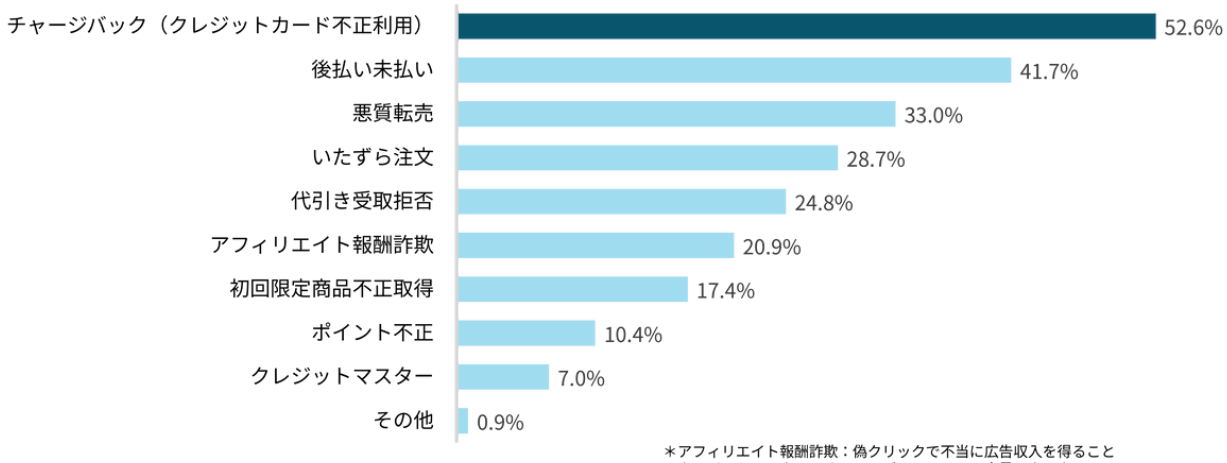
▼図2-14　不正注文被害有無



EC事業者実態調査（Cacco調べ）2024年12月調査

▼図2-15　不正注文被害の種別

Q：今まで受けたことがある不正被害を教えてください。(複数回答)

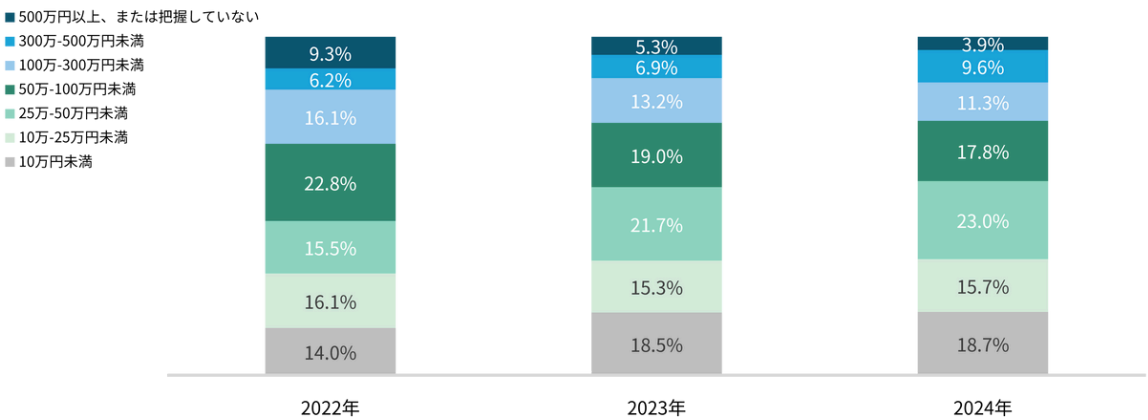


＊アフィリエイト報酬詐欺：偽クリックで不当に広告収入を得ること
＊クレジットマスター：オーソリゼーションへの大量アタック

EC事業者実態調査（Cacco調べ）2024年12月調査

▼図2-16　被害額

Q：直近1年間の不正被害の総額はいくらですか。



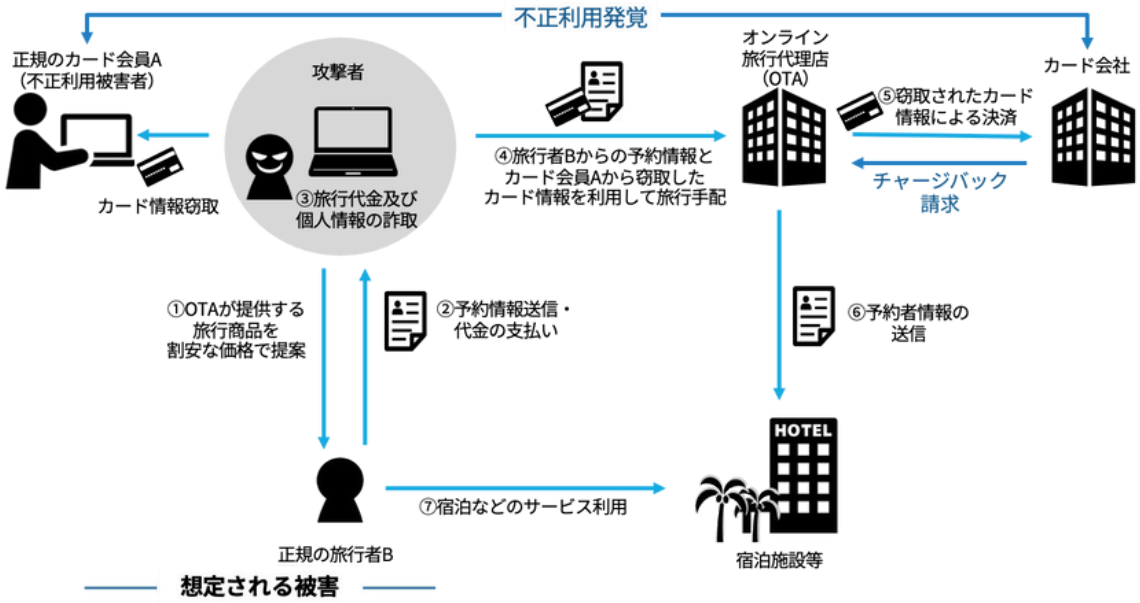
EC事業者実態調査（Cacco調べ）2024年12月調査

(3)-3. 不正トラベルが再び増加傾向に

宿泊施設や航空券など旅行関連サービスを狙った「不正トラベル」が多発していることは2024年に発表した『キャッシュレスセキュリティレポート2024』でも触れた。不正トラベルの手口は巧妙で、まず攻撃者が旅行代理店の商品を偽の予約サイトやSNS経由で正規価格より安く販売し、旅行者に個人情報と旅行代金を入力・送金させる。この時点で旅行代金は攻撃者の手に渡っている。続いて、攻撃者は入手した個人情報を使って正規の旅行代理店に予約を行い、あらかじめ入手していた第三者のクレジットカード情報で決済を行う。旅行代理店はカード会社から代金を受領し、宿泊施設などに予約情報を送付。旅行者は現地でサービスを受けられるため、不正を認識しないまま旅行を終えるケースが多い。（図2-17）

しかし、後日カードの不正利用が判明すると、カード会社は旅行代理店にチャージバック（売上取り消し）を行い、最終的な損害は旅行代理店が負担することになる。旅行者は金銭的被害を免れる一方で、個人情報が攻撃者の手に渡るため、別の詐欺や不正利用に悪用される二次被害のリスクが残る。

▼図2-17　不正トラベル



想定される被害

正規のクレジットカード会員A	カード情報が不正利用される
正規の旅行者B	予約に使用した個人情報が流出、悪用される
旅行代理店	チャージバックにより、旅行代金を得ることができない

出所：『不正トラベルの対策の実施』（日本サイバー対策犯罪対策センター）を参考に作成

Caccoは2023年より、不正トラベルの発生推移を調査している。図2-18は、旅行代理店における「O-PLUX」の審査で不正判定となった注文のうち、旅行代理店自身が不正利用の可能性が高いと判断してブラック登録（※）した取引の合計額の、全体取引額に占める割合である。2023年は0.03％だったが、2024年は0.01％と一時的に減少。しかし2025年上半期は0.18％と再び大幅に増加に転じており、不正トラベル被害の拡大が懸念されている。

※ブラック登録：不正取引のパターンとして登録し、類似注文を検知できるようにすること

▼図2-18　旅行代理店において不正判定した注文の合計金額リスクが高い注文の割合（金額ベース）

	2023年	2024年	2025年 (1-6月)
不正の可能性が高いと判断した取引（金額）の割合	0.03%	0.01%	0.18%

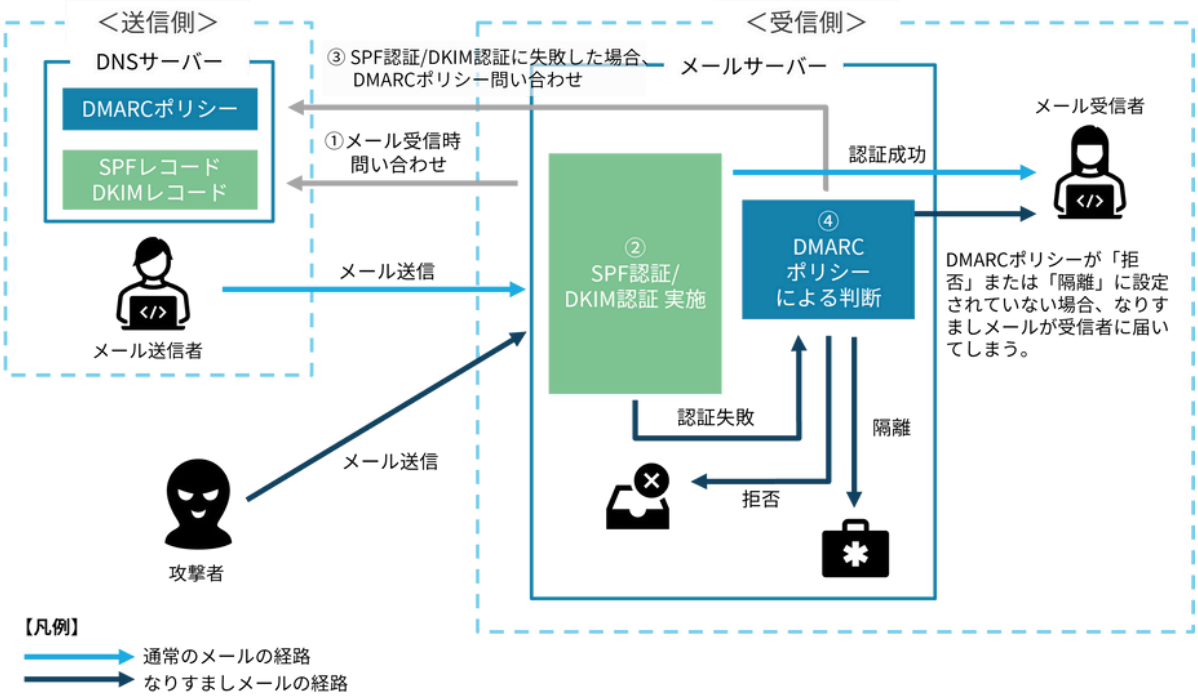
旅行代理店が「O-PLUX」の審査で、不正の可能性が高いと判断した取引（金額）の全体に占める割合（Cacco調べ）

(4)イシュアにおける送信ドメイン認証（DMARC）導入状況

自社になりすましたフィッシング（なりすまし）メールの送信を防止するための対策として有効とされるのが、ドメイン認証技術の一つであるDMARC (Domain-based Message Authentication, Reporting, and Conformance)である。送信元メールサーバーのIPアドレスを利用してドメインを認証するSPF認証や、電子署名を利用して認証するDKIM認証を補完する技術で、これらの認証に失敗したメールの受信側メールサーバーにおける取り扱いを、送信元ドメインのDNSで指定できる。

具体的には、DNSサーバのテキストレコードにDMARCポリシーを記述した「DMARCレコード」を作成する。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。受信側メールサーバーは、受信したメールがSPF認証やDKIM認証に失敗した場合、DMARCレコードの有無を送信元ドメインのDNSに問い合わせる。DMARCレコードが存在し、かつポリシーが隔離または拒否に設定されていると、SPF認証やDKIM認証に失敗したメールはメール受信者のメールボックスに届かない。これにより、イシュア（カード発行会社）になりすましたフィッシングメールが消費者に届くことを防止できる。（図2-19）

▼図2-19　メール送信元によるフィッシング対策(DMARC)



フィッシング被害の増加を受け、2023年2月、経済産業省・総務省・警察庁は、クレジットカード会社等に対し、DMARCの導入をはじめとする、なりすまし（フィッシング）メール対策の導入の要請を連名で行った。「クレジットカード会社等に対し、DMARCを導入すること」および「DMARC導入にあたっては受信者側で、なりすましメールの受信拒否を行うポリシーでの運用を行うこと」、すなわちDMARCを導入し、ポリシーを「拒否（reject）」または「隔離（quarantine）」で運用することを求めている。イシュアは割賦販売法で「登録包括信用購入あっせん事業者」として登録が義務付けられており、一覧が経済産業省のWebサイトで公開されている。イシュアのDMARC導入状況について、リンクでは『キャッシュレスセキュリティレポート　四半期版』の発行にあわせ、四半期ごとの調査を実施している。（2023年末まではｆｊコンサルティング社が実施）

以下、調査の概要と、2023年9月末から2025年3月末までの推移を半年ごとのデータで紹介する。

■調査の概要

＜調査対象＞

経済産業省のWebサイトで公開されている登録包括信用購入あっせん事業者（以下イシュア）

＜調査手順＞

① 調査対象となるドメインの特定

調査対象のイシュアがWebサイト等でメール送信元として公開しているドメイン（サブドメインを含む）を収集し、対象ドメインを確定する。この中には、ワンタイムパスワードサービスやカード会員向けWeb明細提供サービスなどを提供する外部委託先が管理するドメインも含まれる。フィッシング対策の実効性を考えると、これらの外部委託先に対してもイシュアは、自社のカード会員のフィッシング被害を防止するためにセキュリティ対策を求める必要があると考え、対象ドメインに含めることとした。

② ドメインごとのDMARCレコード設定状況の確認
①で収集した全てのドメインのDNSに問い合わせを行い、DMARCレコードの設定有無と、レコードがある場合のポリシーを確認する。

③ 会社ごとのDMARCレコード対応状況集計
会社ごとに、メールの送信元として利用しているドメインのDMARC対応状況を集計し、以下の3カテゴリーに分類する。

1) 対応済み：メール送信元として使用しているドメイン全てにDMARCレコードが設定されている。
2) 一部対応：メール送信元として使用しているドメインの一部にDMARCレコードが設定されている。
3) 未対応：メール送信元として使用している全てのドメインにDMARCレコードが設定されていない。

■調査結果

1. 調査対象イシュアと対象ドメインの数

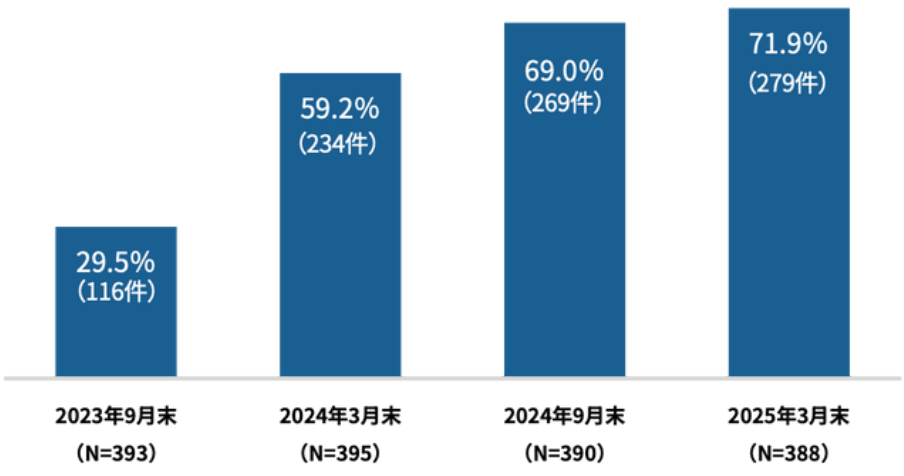
	2023年9月末	2024年3月末	2024年9月末	2025年3月末
調査対象社数	246社	246社	243社	242社
対象ドメイン数	393ドメイン	395ドメイン	390ドメイン	388ドメイン

2. ドメインごとのDMARCレコード設定状況

2025年3月末には、イシュアで利用されているドメイン388件のうち279件（71.9%）にDMARCレコードが存在した。調査期間中の推移を見ると、2023年9月末時点の393件中116件（29.5%）が2024年3月末でおよそ倍増した後も、１年間で少しずつ導入が進んでいる。（図2-20）

2024年3月にDMARC対応ドメインが急増した理由としては、2024年2月のGoogle のメール送信者ガイドラインのアップデート（Gmailアカウントに1日5,000通以上のメールを配信する事業者に対し、DMARC対応を必須とする）が考えられる。

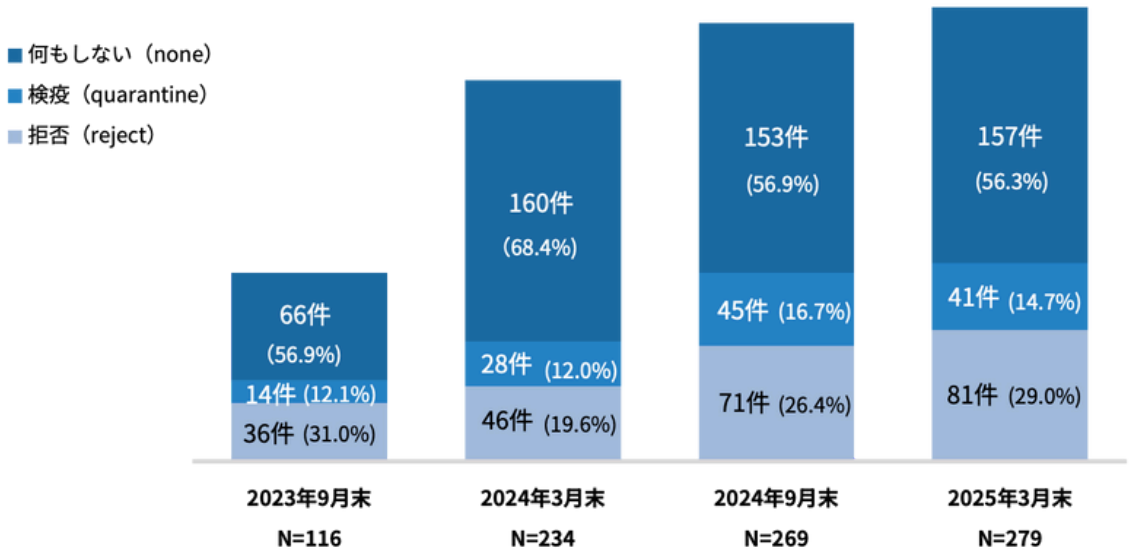
▼図2-20　ドメインごとのDMARC設定率（DMARCを有効にしているドメインの割合）



リンク調べ
※2023年9月のデータはｆｊコンサルティング調べ

DMARCポリシーを最も厳しい「拒否（reject）」に設定しているドメインの数は、2025年3月末には81件（29.0%）となっている。調査期間中の推移を見ると、「拒否（reject）」に設定したドメインの数は増加し続けているが、割合は2024年3月に一度19.6%まで下がった後、再び3割前後まで回復している。前述のGoogleのメール送信者ガイドラインへの対応のため、2024年3月末にひとまずポリシーを「何もしない（none）」に設定してDMARCを導入したドメインが、時間をかけてポリシーを調整し、徐々に厳しくしている様子がうかがえる。しかし一方で、ポリシーを「何もしない（none）」に設定しているドメインが157件（56.3%）と、依然として6割弱存在している。(図2-21)。

▼図2-21　イシュアのメール送信元ドメインのDMARC設定状況率

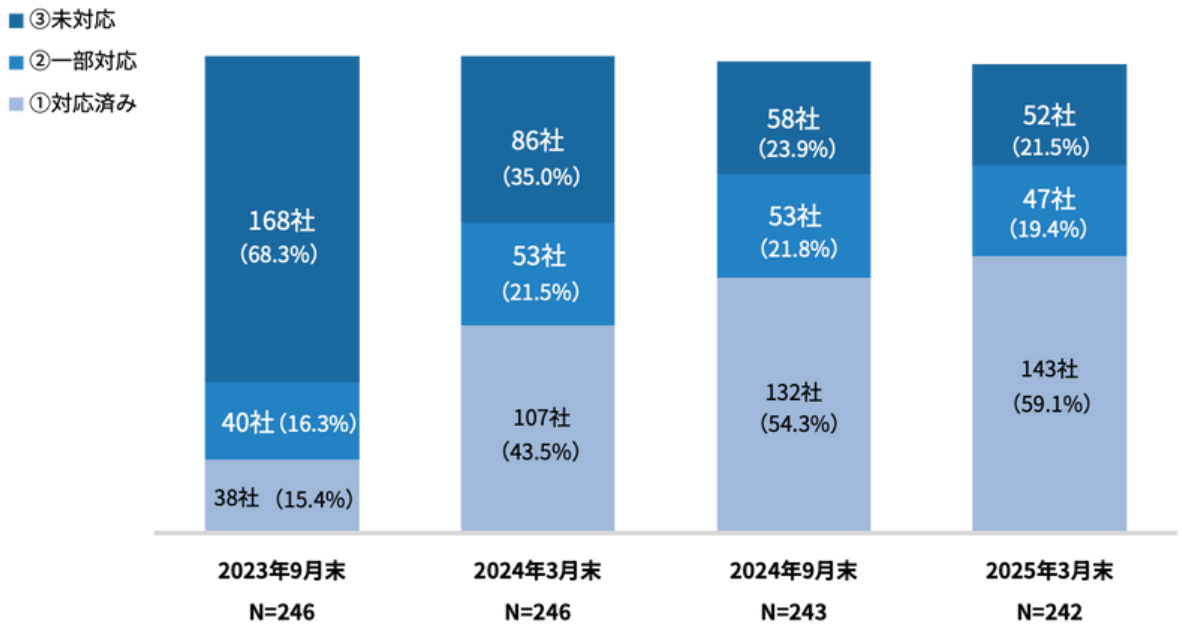


リンク調べ
※2023年9月のデータはｆｊコンサルティング調べ

3. 会社ごとのDMARC対応状況

2025年3月末時点で、①対応済みと②一部対応をあわせて242社中190社（78.5%）がDMARC導入に着手している。うち、143社（59.1%）は委託先も含めメール送信元として使用する全てのドメインにDMARCレコードの設定を完了している。調査期間中の推移を見ると、2023年9月末時点でDMARC対応に着手しているイシュアは３分の1に満たなかったが、2024年3月末には合わせて160社（65.0%）と急増し、2024年9月末には4分の3以上のイシュアがDMARC対応に取り組んでいた。また、2024年9月末には半数以上のイシュアが委託先のドメインを含めた全てのドメインのDMARC対応を完了していた。（図2-22）

▼図2-22　イシュアにおけるDMARC対応状況



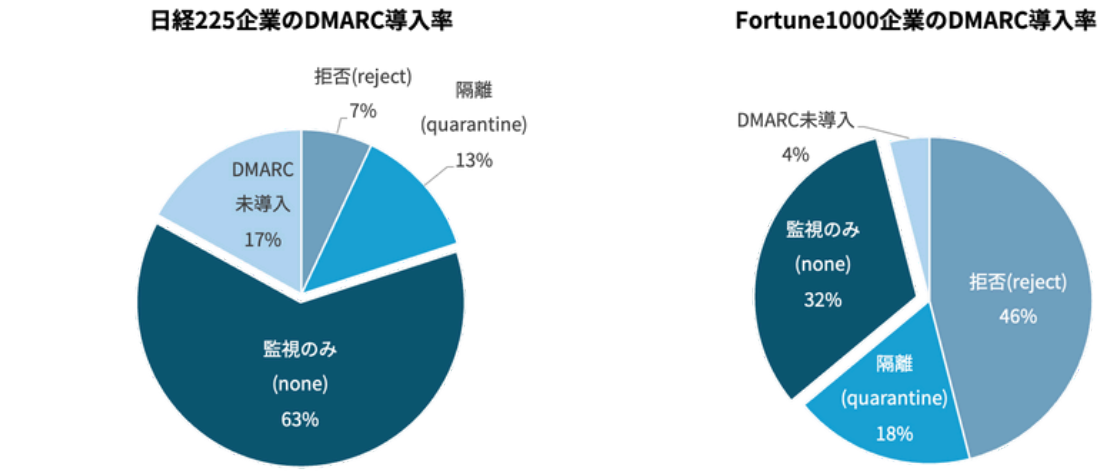
リンク調べ
※2023年9月のデータはｆｊコンサルティング調べ

3. 総括

調査開始からの1年半で、イシュアのDMARC導入は着実に進んできたと言えるが、依然として２割のイシュアが未対応である状況で進捗は鈍化している。また、DMARCポリシーの設定については、依然として６割近いドメインで「何もしない（none）」に設定されており、なりすましメール対策としての実効性を上げるためには課題を残している。

2025年1月、フィッシング対策協議会は、ワーキンググループ報告書 として『送信ドメイン認証技術「DMARC」の導入状況と必要性について』を公開した。この報告書では、日本プルーフポイントによる日経225企業とFortune1000企業を対象とした、日米を比較したDMARC導入状況調査の結果を紹介している。（図2-23）

▼図2-23　DMARC導入状況の日米比較（日本プルーフポイント調べ・2024年8月）



出所：『送信ドメイン認証技術「DMARC」の導入状況と必要性について』(フィッシング対策協議会）)を参考に作成　2024年8月

日経225企業のDMARC導入率は83%に対し、Fortune1000企業の導入率は96%とほぼ全てに近い企業がDMARCをすでに導入している。また、Fortune 1000企業のうちDMARCのポリシーを『拒否（reject)』に設定しているのが46%、『検疫（quarantine)』が設定しているのが18%と、6割以上がなりすましメール対策として実効性のあるポリシーを設定している。対して、日経225企業では63%がDMARCのポリシーを『何もしない（none)』に設定している。DMARC未導入の17%とあわせると、8割もの企業が実効性のあるなりすましメール対策ができていない。

イシュアのDMARC導入率も着実に底上げされてはいるが、監督官庁の要請が出されているにもかかわらず、日経225企業と比較し下回っている。未導入のイシュアは早急に導入することが求められる。また導入済みのイシュアについても、なりすましメール対策として実効性を持たせるために、DMARCポリシーを『拒否』に設定して、なりすましメールを封じ込める必要がある。ポリシーの強化が進まない理由として、DMARC設定が誤っている場合、フィッシングではない正規のメールの受信が拒否される可能性があるなど、業務への影響が大きいと考えられる。フィッシング対策協議会では、DMARCを最初に設定する時は、ポリシーを「何もしない（none)」に設定してレポートを取得し、正規メールとなりすましメールの配信状況を確認しつつ、徐々に強制力のあるポリシーへと調整することを推奨している。

また、イシュアの中にはWeb明細サービスやメール配信を外部に委託している場合があり、その場合は外部委託先ドメインについても受信を「許可」するようにカード会員向けに案内している。イシュアは自社のなりすましメール対策の一貫として、外部委託先に対してもメール送信ドメインにDMARC対応を求めていく必要がある。

一方で、国内企業全体にDMARCの導入が進んできたにもかかわらず、フィッシングに起因すると思われる不正利用被害は減っていないという現状がある。2024年末から2025年前半にかけてのオンライン証券口座乗っ取りによる不正取引では、認証情報を窃取されたのち証券口座に不正ログインされ、不正な取引が実行された（「3. 他の金融サービスにおける不正取引 -(1)オンライン証券取引口座乗っ取りによる不正取引」にて詳述)。これらの金融サービスには、DMARCの導入やポリシー強化を先んじて取り組んできた企業も含まれている。

イシュアの会員サイトの場合は、ポイント交換など金銭的な損失につながる操作がある。ワンタイムパスワードの送付先を攻撃者に変更されてカード利用時の多要素認証を突破されることがある。また、利用状況の通知が届かなくなり、不正利用が行われていることに気づきにくくなる。

前述のオンライン証券口座乗っ取りによる不正取引のような、今まで考えもしなかったような不正手口のイノベーションが起こらないという保証はない。クレジットカード業界においても、次の段階に先手を打つための対策として、イシュアの会員向けサイトへの多要素認証の必須化を進めるべきである。

フィッシングメールやメッセージの誘導先で、実際にカード情報や認証情報を入力させるフィッシングサイトの閉鎖（テイクダウン）も被害の減少には有効な対策である。2025年4月からカード会社8社とアクシオン社、および日本クレジットカード協会は共同でフィッシングサイト閉鎖の取り組みを開始した。アクシオン社の技術でフィッシングサイトを能動的に検知するだけでなく、当該サイトを閉鎖するための各種届出（当該サイトをホスティングするISPへの通報、ドメイン登録事業者へのドメイン無効申請、Google等のWebブラウザ提供企業への申告、フィッシング対策協議会への通知など）を実施する。

(5) EMV 3-Dセキュア導入に伴うカード決済承認率の変化

ECサイト事業者は、消費者が商品をカートに入れても購入に至らない「カゴ落ち」を恐れる。かつて3Dセキュア1.0が普及しなかった理由の1つが、決済の都度、消費者に3Dセキュアの入力画面にパスワードを入力させることで消費者がわずらわしさを感じたり、決済の途中で外部サイトに遷移することに不安を感じたりしたことである。その結果、カゴ落ちが発生することにEC事業者側が強い懸念を示したのである。後継バージョンであるEMV3-DSでは、リスクベース認証によって、優良な買い物客にはなるべくパスワードを追加で入力させずスムーズに取引が済むようにしてカゴ落ちを防いでいる。

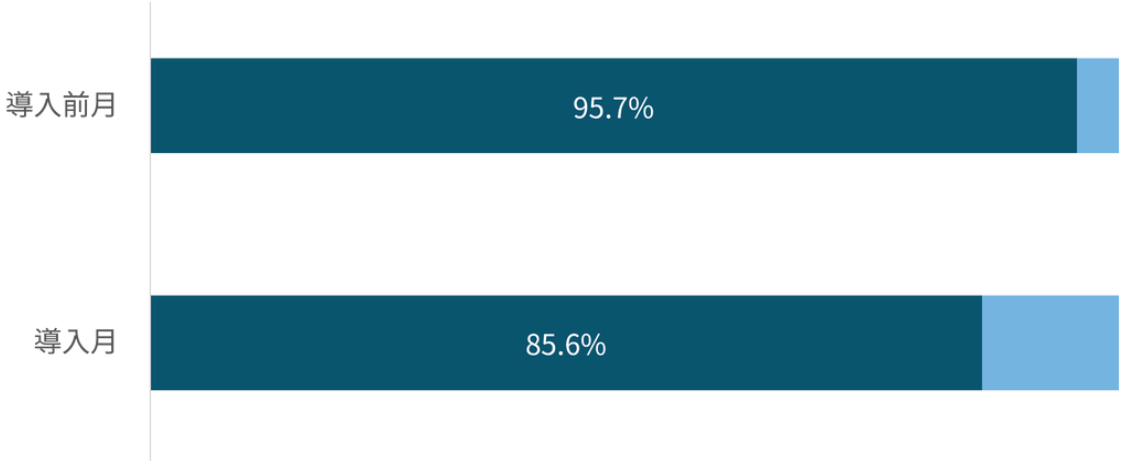
一方で、カード決済承認率（加盟店からのオーソリゼーション要求に対して、イシュアが承認する割合）がEMV3-DS導入前に比べて低下傾向にあると言われている。オーソリゼーションが否認されると決済に失敗して取引が完了できず、カゴ落ちにつながる。

実際の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を、決済承認率改善サービスを提供する株式会社YTGATE（以下YTGATE）の協力を得て調査した。

1. EMV3-DS導入前後での決済承認率の変化

４社のEC加盟店の延べ約22万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95.7%に対し、導入後のカード決済承認率は85.6%と10.1ポイントの低下が見られる。（図2-24）

▼図2-24　EMV 3Dセキュア導入前後の決済承認率の比較



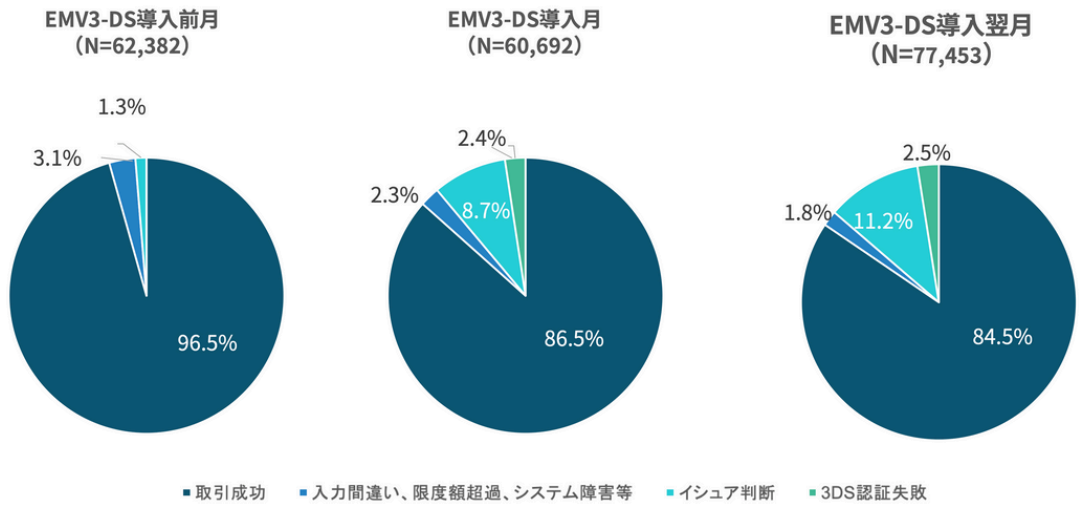
YTGATE提供データを元に作成

2. カード決済承認率低下の要因

４社のうち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。なおEMV3-DS導入日が月途中のEC加盟店も含まれているため、導入月のデータにもEMV3-DSを導入する前の決済が混在している。そのため範囲を広げて、導入翌月のデータについてもカード決済承認率を対比し、否認理由について分析した。

EMV3-DS導入前月の取引と比較すると、EMV3-DS導入翌月のカード決済承認率は95.6%から84.5%と、11.1ポイント低下していた。否認理由で最も増加したのは、イシュア判断による否認であり、その割合は1.3%から11.2%とおよそ9倍に増加している。（図2-25）

▼図2-25　決済否認の理由内訳



YTGATE提供データを元に作成

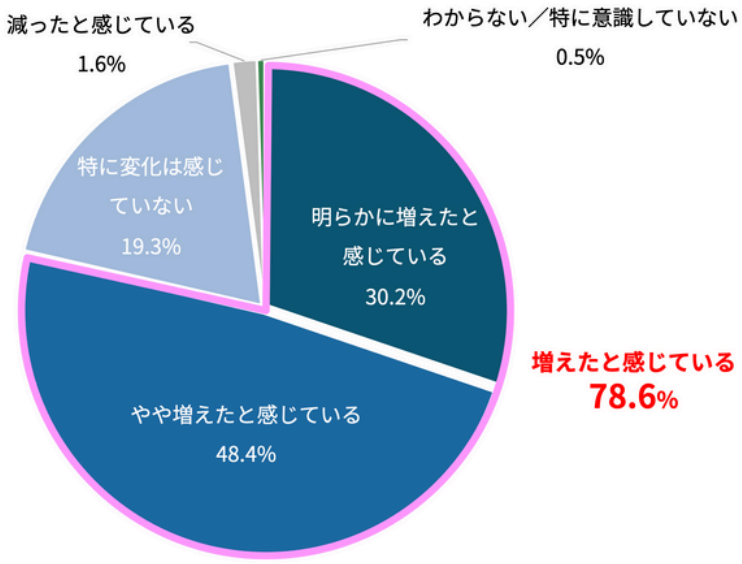
3. 考察

分析した4社のデータからは、EMV3-DS導入前後でカード決済承認率が低下していることが裏付けられた。その要因として、イシュア判断による否認の割合がEMV3-DS導入前に比べて大幅に増加していることが挙げられる。

イシュアの判断による取引否認が増えた大きな理由としては、EMV3-DS導入取引に対するライアビリティシフトが考えられる。従来、カード不正利用による損失は加盟店側の責任としてチャージバック（売上取り消し）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の責任は原則イシュアとなる。そのため、イシュアは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拒否する傾向が強くなっていると想定される。

YTGATEが2025年8月に全国のEC事業者を対象として実施した調査によれば、EMV3-DSの導入率は約70%であるが、導入済みのEC事業者の約8割が「カゴ落ちが増えた」と感じている。（図2-26）

▼図2-26　EMV3-DS導入後、カゴ落ちが増えたと感じているEC事業者の割合



YTGATE調査（2025年8月）を元に作成

消費者から見てもEMV3-DS導入後に決済を完了できない割合は増えている。YTGATEの調査によれば、65%以上の消費者がEMV3-DSの認証エラーによる決済失敗を経験している。そして決済が失敗した消費者の15%以上が購入をあきらめるか、もしくは他のサイト・店舗で商品を探す、すなわちカゴ落ちとなっている。売上向上のために対応した様々なマーケティング施策も、最終的に決済が失敗すれば購買が完了せず、結果売上機会の損失となる。

不正利用を防ぎつつカード決済承認率を上げるためには、まず、EMV3-DSの認証精度を上げることが必要となる。『セキュリティガイドライン6.0』では、EC加盟店に対し、イシュアのリスクベース認証精度向上のために、自社取扱商品や不正利用被害の状況等をふまえて、カード会員のデバイス情報等の情報をより多く提供すること、提供する項目を適宜見直すことを求めている。

より多くのリスク判定項目のデータを加盟店からイシュアに提供することでEMV3-DSの精度を上げ、イシュアが過剰にオーソリゼーション否認を行わないようになることが理想的な姿である。一方で、多くのリスク判定項目のデータをリスクベース認証に適切に活用するノウハウが不十分なイシュアもあり、現実にはイシュアによってカード決済承認率に大きな差がある。

EC事業者は、カード決済承認率向上のためにリスク判定項目のデータを適切に提供すると同時に、イシュアごとのカード決済承認率を分析して、カード決済承認率が低いイシュアに対し個別に情報交換を通じて調整を行うなどの対応も可能である。消費者に対しては、カゴ落ちを減らすために、決済エラーの内容の説明や再購入手続きに必要な解決方法を丁寧にナビゲーションすることが有効である。

3. 他の金融サービスにおける不正取引

(1)オンライン証券取引口座乗っ取りによる不正取引

金融庁の集計によると、2025年1月から7月末までにおけるオンライン証券取引口座（以下証券口座）への不正アクセス件数は 14,069件、そのうち不正取引件数は 8,111件、累計被害額は 6,205億円 に達した。（図3-1）

▼図3-1　オンライン証券取引口座への不正アクセス件数

	2025年1月	2025年2月	2025年3月	2025年4月	2025年5月	2025年6月	2025年7月	合計
不正取引が発生した証券会社数（社）	2	2	5	9	16	7	5	ー
不正アクセス件数	170	114	2,319	5,407	3,330	1,759	970	**14,069**
不正取引件数	95	51	951	2,970	2,375	851	818	**8,111**
売却金額（億円）	約2	約0.9	約168	約1,556	約1,117	約221	約243	**約3,307**
買付金額（億円）	約0.8	約0.8	約145	約1,365	約1,001	約165	約217	**約2,898**

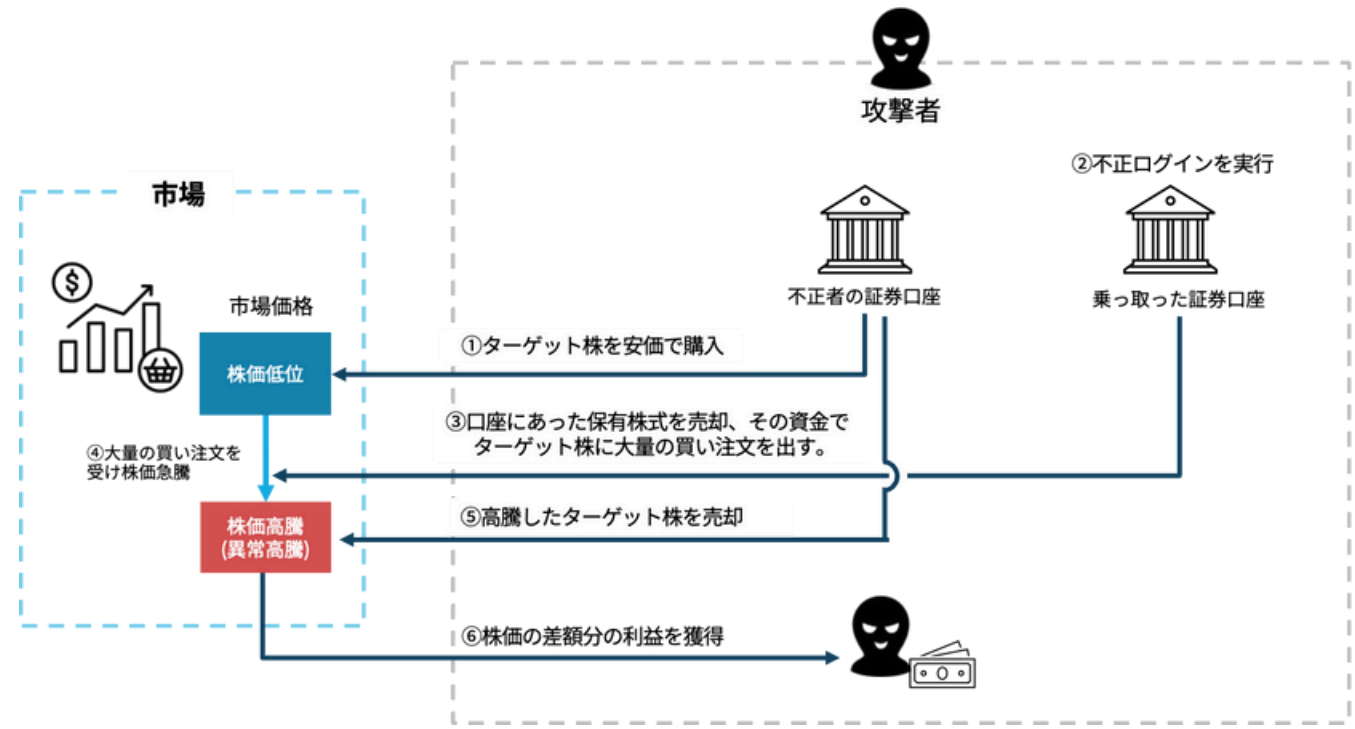
出所：インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています（金融庁）2025年8月7日更新

1. 手法の概要

証券口座乗っ取りによる不正収益入手までの典型的な流れは以下の通りである。（図3-2）

① 攻撃者の証券口座で、市場での取引量が少なく低価格で安定した株式（ターゲット株）を事前に大量に購入
② 攻撃者が他人の証券口座の認証情報（ID、パスワード暗証番号等）を窃取し、不正ログイン実行
③ 不正ログインした口座の保有株式を勝手に売却し、その資金でターゲット株に大量の買い注文を出す。
④ 市場でターゲット株の株価が急騰
⑤ 攻撃者は自身の証券口座から事前に購入したターゲット株を高騰した価格で売却
⑥ 売却利益を確定

▼図3-2　不正収益入手までの流れ



この手法は、攻撃者が金銭を直接奪うのではなく、株価操作などを通じて間接的に利益を得る点が特徴である。クレジットカード不正利用やオンラインバンキングを悪用した不正振込などでは、攻撃者に犯罪収益を移転するために、不当に得た資金を多数の金融機関を転々とさせることで出所をわかりにくくする「マネーロンダリング」が行われる。しかし今回の証券口座乗っ取り事件では、不正に入手した口座情報や資金は株式市場を操作するために利用される。犯罪収益の移転は正規の株式取引によって行われるため、マネーロンダリングが不要であるという点が斬新である。

2. 被害が拡大した理由

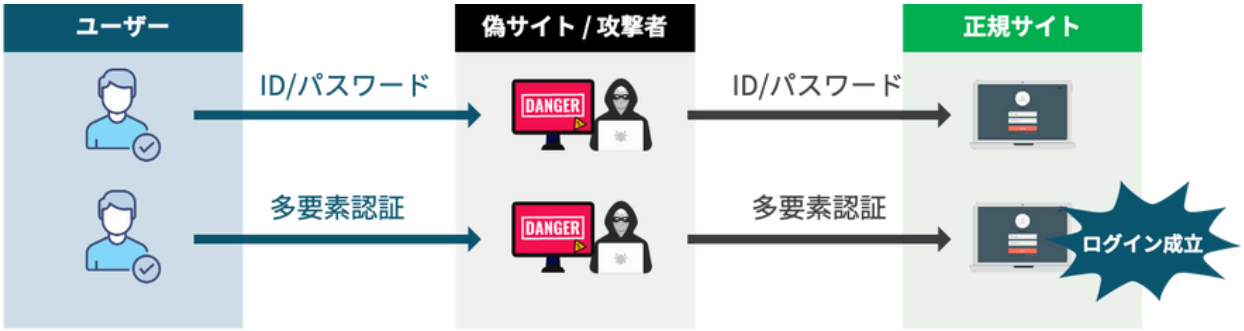
不正にログインする証券口座の認証情報の入手手法としては、フィッシング、マルウェア「インフォスティーラー」(「2.2024年の ECサイトにおける不正利用の概況 (1)-2 クレジットカード不正利用被害増加の要因」参照）の感染、他サービスから流出した認証情報を利用する攻撃などがある。

窃取された認証情報による不正ログインを防止するためには多要素認証の導入が有効である。しかし証券取引では一分一秒を争う取引のタイミングによって利益や損失が変動することから、システム操作時間の短縮に対する利用者のニーズが非常に高い。そのため、証券会社各社は操作に時間のかかる多要素認証の導入に消極的であったり、導入していても必須化までは求めていない場合がほとんどであった。

被害の急拡大を受け、日本証券業協会では多要素認証の必須化を決め、2025年4月25日に『多要素認証の設定必須化を決定した証券会社名』を公表（2025年7月7日現在75社)。対応が進んだ結果、6月以降の不正アクセス被害件数は減少傾向にある。

ただし、多要素認証を導入した場合も、中間者攻撃（ユーザーと正規サイトの通信の間に攻撃者が割り込み、認証情報などを盗み取る攻撃手法）であれば不正ログインができてしまう（図3-3)。実際に、証券口座に多要素認証を設定していても不正ログインされ、不正取引が行われた事例が複数報告されており、2025年7月は不正利用被害件数は減ったものの不正取引被害額は再度増加に転じている。 また、メインのシステムでは多要素認証を必須化していても、システム障害時向けに提供される「バックアップサイト」では多要素認証に対応していない証券会社もあった。

▼図3-3　中間者攻撃（AiTM）



※セッショントークン（Set-Cookieで配られるセッションID等）を入手すれば、IDとパスワードのみで不正ログインされるケースもある。

3. 証券会社の対応

当初、証券会社各社は、約款で証券口座の認証情報の管理は利用者の責任であると定めていること、また侵害されたのは自社の取引システムであり、自社も被害者であることを理由に、乗っ取られた口座で行われた不正取引による損害については「正規の認証情報を用いて行われた取引である」として補償を行わない方針であった。

しかし2025年3月以降の被害急増を受け、4月22日に金融担当大臣より証券会社に対し、補償について「(顧客の）問合せや相談に真摯に対応し、被害の回復に向けて誠実な対応をとるよう指示した」という発言があった。これを受け、日本証券業協会は5月2日に『フィッシング詐欺等による証券口座への不正アクセス等による対応について（10 社申し合わせ)』(以下『10社申し合わせ』）を公表した。

『10社申し合わせ』には、約款の定めにかかわらず不正取引により発生した被害については一定の被害補償を行う方針と共に、実際の対応については利用者の認証情報の管理状況や証券会社の対策等を勘案した上で、個別に対応することが記された。また、利用者向けには「利用している証券会社が多要素認証を提供している場合、必ず設定する」「証券会社のWebサイトはあらかじめブックマークし、アクセスする」「メールやSMSなどに表示されているURLリンクは絶対に使わない」ことが要請された。

7月以降、証券会社各社の補償方針が明らかになった。対面大手証券会社は被害口座の原状回復（不正取引で売られた株を顧客の口座に戻し、買われた株を口座から取り除く）を行う、全額補償に近い対応を公表したのに対し、ネット証券の多くは不正売買で発生した損失の一部を金銭補償する方針を示しており、割合は会社によって異なっている。ネット証券を利用していた不正取引の被害者からは証券会社に対し全額補償を求める訴訟が起こされ、被害者の会が結成されている。

4. 考察

従来、銀行と比較し、証券会社はインターネット取引におけるセキュリティ対策がやや手薄であった。例えばオンラインバンキングサービスでは当然に導入されている多要素認証についても、前述のような理由で証券口座のログインにおいては導入が進んでいなかった。証券口座の収益は取引手数料によるものであり、ユーザー数と取引数がダイレクトに収益に直結する。そのため、セキュリティを厳しくすることで顧客が他の証券会社にスイッチするリスクを恐れ、日本証券業協会からアナウンスが出るまで多要素認証の義務化ができなかった。

「万一証券口座を乗っ取られて株式を売却されたとしても、顧客本人名義の銀行口座に出金されるだけで実際の金銭被害にはつながらない」という油断も、口座乗っ取り対策が手薄になった背景にあったと思われる。今回のような、売却代金を市場に投入して株価を操作し、売却益で収益を得るという手法は証券会社においては想定外の手口であったと言える。

日本の証券会社がターゲットになっていたことが、フィッシングメールの動向からわかる。メールセキュリティ対策を提供する日本プルーフポイント社の調査によると、2025年7月に詳細を分析できた不審メールのうち、日本語で書かれたものが9割以上を占めている。生成AIによって自然な日本語の文を作れるようになったことから、海外の犯罪集団にも日本をターゲットにした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。今回の証券口座乗っ取りの不正アクセスは中国からであった疑いが強いことがわかっている。

フィッシングメールやフィッシングサイトの作成には、雛形を提供する「フィッシング・キット」と呼ばれる犯罪ツールが使われることが多い。トレンドマイクロによると、これまでフィッシングキットが使われたと見られる日本語のフィッシングメールやフィッシングサイトの主な標的は銀行やクレジットカード会社であった。しかし、2024年後半からは証券会社を標的としたものが目立つようになり、2025年6月中旬時点で17社のフィッシングサイトが確認されたという。フィッシング対策協議会の月次レポートでもフィッシング報告のうち証券系ブランドを騙る割合は3月4.1%、4月25.5%、5月32.2%、6月15.5%となっており、ここからも証券会社をターゲットとした攻撃が4月以降急増していたことがうかがえる。

今回の事件では、日本の証券会社のセキュリティ対策の手薄さと、生成AIを中心とした技術の進化による日本向けフィッシング攻撃の難易度低下が重なり、前代未聞の大規模な被害を出すに至ったと考えられる。

日本証券業協会は証券口座乗っ取りへの対策に主眼を置き、2025年7月、『インターネット取引における不正アクセス等防止に向けたガイドライン』の改正案を公表した。ログインや出金などの重要な操作の際に、「フィッシングに耐性のある多要素認証」の実装を必須化する。現状のワンタイムパスワードを用いた多要素認証が中間者攻撃により突破されていることへの対策であり、例として、パスキーやPKI（公開鍵基盤）をベースとした認証が挙げられている。 他にも、フィッシングを未然に防ぐための6項目の対策を証券会社に求めている。

（１）顧客へ送信する電子メールのドメインを特定し、DMARC 等の送信ドメイン認証技術の 計画的な導入を行う。また、DMARC レポート等の確認等を行った上で、ポリシーは 「reject」にする。
（２）SMS送信時には共通ショートコード（※1）を利用し、Web サイト上又はアプリケーション上等で当該共通ショートコードを公開する。
（３）自社を騙るフィッシングサイトについて、そのアクセス制限のためのテイクダウン（閉鎖）活動を行う。
（４）ドメインは自己のブランドと認識し、以下の①から③を中心に適切に管理する。
① 自組織に割り当てられているドメイン名を把握・管理する。
② ドメイン名のライフサイクルを管理する。また、ドロップキャッチ（※2）やサブドメインテイクオーバー等の攻撃に対する対策を実施する。
③ 顧客に対し、サービスで使用するドメインに関する周知を行う。
（５）利用者がアクセスしているWebサイトが真正なものであることの証明を確認できるような措置を講じる。
（６）メールや SMS（ショートメッセージサービス）内にパスワード入力を促すページのURLやログインリンクを記載しない。

金融庁も『金融商品取引業社等向けの総合的な監督指針』の一部改正案を公表している。監督指針の改正案では、日本証券業協会のガイドラインを踏まえた適切なセキュリティ対策を講じることを求めている。

※1 共通ショートコード：「0005」から始まる8～10桁のSMSの送信元表示名。通信会社の審査によって発行されるため、共通ショートコードが送信元のメッセージは正規メッセージと判別することが可能
※2 ドロップキャッチ：既に使用していない等の理由で有効期限が切れたドメインを攻撃者が取得し、以前の使用者になりすます攻撃手法

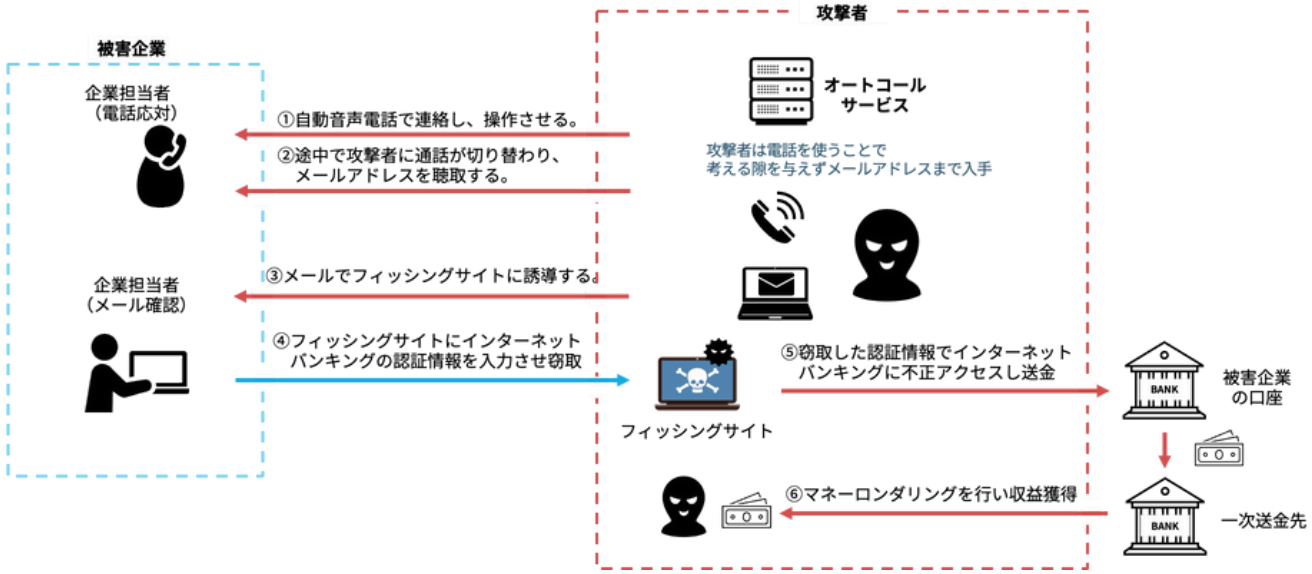
(2)ボイスフィッシングによる法人口座を狙った不正送金

金融機関を装い、企業に電話をかけて偽サイトに誘導し、法人口座の情報を盗み取る「ボイスフィッシング」（Voice Phishing /ビッシングとも略される）という手口による不正送金被害が増えている。報道によれば、2024年11月から2025年4月末までに被害は国内約80社に上り、約28億円が不正送金されていた。2025年4月には全国銀行協会、金融庁、警察庁、日本サイバー犯罪対策センターが連名 で注意喚起を公表している。

ボイスフィッシングの典型的な手口としては以下の通りである。（図3-4）

①金融機関を装った自動音声電話で連絡し、自動音声に従い利用者に操作をさせる。
②自動音声を操作すると攻撃者との通話に切り替わり、理由をつけて会社のメールアドレスを聴取する。
③メールアドレス宛にURLを添付したメールを送信し、フィッシングサイトに誘導する。
④フィッシングサイトで法人のインターネットバンキング口座の認証情報を入力させ、窃取する。
⑤入力された認証情報を利用してインターネットバンキング口座に不正アクセスし、一次送金先に送金する。
⑥送金した資金は、別口座への送金や暗号資産化などによりマネーロンダリングを行う。

▼図3-4　ボイスフィッシング



2025年3月に被害にあった鉄道会社R社の例では、代表番号宛に地元の地方銀行を名乗り、「ネットバンキングの情報更新が必要」という自動音声電話があった。音声ガイダンスに従いボタンを押していくと人の通話に切り替わり、手続きに必要だとして会社のメールアドレスを尋ねられた。まもなく届いたメールにフィッシングサイトのURLが記載されており、担当者が気づかずオンラインバンキングの認証情報を入力した後、口座残高の約1億円が不正送金された。

2024年4月には、地方銀行T銀行インターネットバンキングサービスのヘルプデスクを装った自動音声通話によって、県内の複数企業が、「インターネットバンキングサービスの登録情報を更新するために現在の認証情報を教えて欲しい」等の名目でインターネットバンキングの認証情報を聴取され、不正送金の被害にあった。被害金額の総額は1億円に上る。T銀行は緊急措置として他行宛の即時扱いの振込を停止した。現在は不正送金リスクの高い新規先への即時振り込みを不可としている。

AI音声を悪用した、いわば「標的型ビッシング」とでも言うべき手口も登場している。2024年11月に起こった日本の大手メーカーを標的とした詐欺未遂事件では、社長の声を学習したAI音声が用いられた。学習データとして、IR動画やインタビューなど、インターネット上に公開された社長の声が入った動画が利用されたと考えられる。攻撃者は電話番号も社長のものに偽装して、海外赴任中の幹部に電話をかけ、海外グループのM&Aの名目で即日の送金を命じた。さらに２回目の電話で送金の督促と契約弁護士からの連絡についての確認があり、同じタイミングで当該契約弁護士からのメールを受信した。このことで幹部が不審に思い、電話で直接契約弁護士に確認したところ、メールが偽のものであることが確認でき、詐欺と判明した。

法人をターゲットにしたボイスフィッシングが増えている理由の一つは、電話で直接話しかけることで実在する組織の担当者であると誤認させやすいことがある。メールに比べて、電話はリアルタイムで返答する必要があるため、被害者に考える時間を与えず会話を進めることが可能になる。また、最初に自動音声応答を利用することで警戒心の薄い企業を選別でき、攻撃者にとって効率的である。法人口座が狙われる理由は、1日あたりの送金限度額が高く設定されているからと考えられる。

ボイスフィッシングの被害を防ぐための企業の対策として、警察庁は以下の3点を挙げている。

①知らない電話番号からの着信は信用しない。
②銀行からの電話があった場合、銀行の代表電話番号や問い合わせ窓口で確認する。
③インターネットバンキングにログインする時はメールに記載されたリンクを使用せず、公式サイトやアプリケーションからアクセスする。

銀行側も多要素認証にパスキーなどのフィッシング耐性の高い認証を導入する、銀行からのメールに企業のロゴを表示して正規メールと判別させるBIMIを導入して利用者に周知するなどの対策が求められる。カード会社やECサイトにおいても、サポートセンターを装って個人や法人のカード会員に同様の方法で電話をかけ、認証情報を騙し取るような手口が考えられるので、備える必要がある。

4. 制度・政策の動向

(1)クレジットカード・セキュリティガイドライン【6.0版】について

2025年3月、割賦販売法におけるクレジットカード情報保護および不正利用対策の実務上の指針である『クレジットカード・セキュリティガイドライン【6.0版】』（以下『セキュリティガイドライン6.0』と記載）が公表された。

現在、加盟店からのカード情報流出の主な手口は、ECサイトの改ざんにより消費者が決済画面で入力したカード情報を第三者に送信するオンラインスキミングである。また、クレジットカード不正利用の大半は番号盗用であり、これもECサイトにおいて発生している。『セキュリティガイドライン6.0』では、こうした現状への対応として、EC加盟店に対する指針対策（割賦販売法が求める「クレジットカード番号等の漏えい等の事故及び不正利用を防止する措置」）が新たに追加された。本節では追加された指針対策について解説する。なおこれらの指針対策を実施するための具体的な対応は『ECサイト加盟店におけるセキュリティ対策導入ガイド【附属文書20】』（以下『セキュリティガイドライン附属文書20』）にまとめられており、その内容については現状を踏まえて、今後見直しや表記のブラッシュアップが進められる。

(1)-1. EC加盟店に対する脆弱性対策の義務化

『セキュリティガイドライン』では、EC加盟店のカード情報保護対策は、カード情報を保持しない非保持化、もしくはカード情報を保持する場合はPCI DSS準拠を指針対策（割賦販売法で定める「必要かつ適切な措置」）として求めている。しかし、非保持化だけではECサイトの改ざんによるオンラインスキミングを防ぐことは困難である。

その対策として新規EC加盟店を対象に、自社システムやWebサイトの脆弱性対策を実施し状況を契約するカード会社（アクワイアラ）や決済代行事業者に報告する「セキュリティチェックリスト」が2022年から試行されていた。『セキュリティガイドライン6.0』では、これを全てのEC加盟店向けに拡大し、「脆弱性対策」を指針対策として義務付けた。（図4-1）

また最近は、「クレジットマスター」（クレジットカード番号の規則性を悪用して機械的にカード番号を生成する手法）により大量にカード番号を生成し、ECサイトの決済に利用して番号の有効性を確認する手口（悪質な有効性確認）が多くが発生している。これに対してもEC加盟店で取引の連続回数やIPアドレス制限によって異常な取引であることを検知し、取引を遮断するなどの対策を講じることを求めている。

▼図4-1　EC加盟店の自社システムやWebサイトに求められる脆弱性対策

カテゴリー	対策
①システム管理画面のアクセス制限と管理者のID/パスワード管理	• システム管理画面のアクセス可能なIP アドレスを制限する。IP アドレスを制限できない場合は管理画面にベーシック認証等のアクセス制限を設ける。 • 取得されたアカウントを不正使用されないよう2 段階認証又は多要素認証（2要素認証）を採用する。 • システム管理画面のログインフォームでは、アカウントロック機能を有効にし、10 回以下(PCI DSS ver4.0.1 基準)のログイン失敗でアカウントをロックする。
②データディレクトリの露見に伴う設定不備への対策	• 公開ディレクトリには、重要なファイルを配置しない。（特定のディレクトリを非公開にする。公開ディレクトリ以外に重要なファイルを配置する。） • Web サーバーやWeb アプリケーションによりアップロード可能な拡張子やファイルを制限する等の設定を行う。
③Web アプリケーションの脆弱性対策	• 脆弱性診断又はペネトレーションテストを定期的に実施し、必要な修正対応を行う。 • SQL インジェクションの脆弱性やクロスサイト・スクリプティングの脆弱性対策として、最新のプラグインの使用やソフトウェアのバージョンアップを行う。 • Web アプリケーションを開発又はカスタマイズされている場合には、セキュアコーディング済みであるか、ソースコードレビューを行い確認する。その際は、入力フォームの入力値チェックも行う。
④マルウェア対策としてのウイルス対策ソフトの導入、運用	マルウェア検知/除去などの対策としてウイルス対策ソフトを導入して、シグネチャーの更新や定期的なフルスキャンなどを行う。
⑤悪質な有効性確認、クレジットマスターへの対策	悪質な有効性確認、クレジットマスターに対して、『EC加盟店におけるセキュリティ対策導入ガイド【附属文書20】』別紙aに記載の対策のうちいずれか1つ以上の対策を実施する。

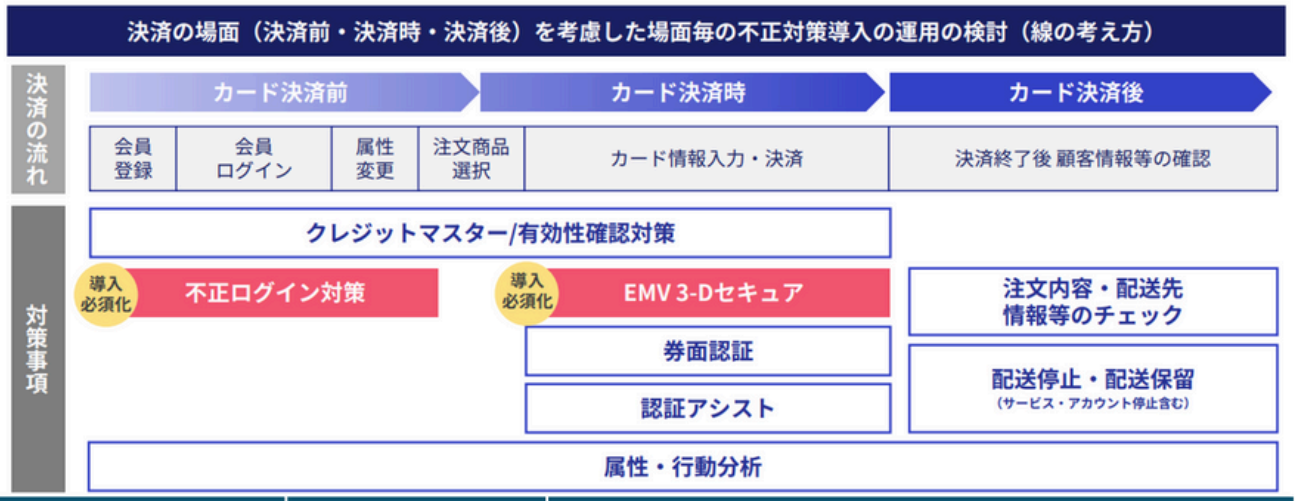
出所：『クレジットカード・セキュリティガイドライン【6.0版】』（2025年3月）をもとに作成

なお、この脆弱性対策は2025年4月時点で「すでに当然実施されている施策」として位置付けられている。アクワイアラや決済代行事業者は、定期的な加盟店途上調査において実施状況を確認し、未実施のEC加盟店に対しては指導することが求められる。対応を行わないEC加盟店は、アクワイアラから加盟店契約を解除されることがある。

(1)-2.「線の考え方」に基づく不正利用対策への指針対策追加

クレジットカード不正利用への対策の新たな考え方として、『セキュリティガイドライン5.0』では、カード決済時に加えて決済前、決済後という場面ごとに対策を考える「線の考え方」を提示し、詳細運用は今後検討するとしていた。『セキュリティガイドライン6.0』では、「線の考え方」のカード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た。また、以前から示されていた全てのEC加盟店に対するEMV 3-Dセキュア（以下EMV3-DS）による本人認証の導入は、カード決済時の対策として位置付け、指針対策として明記された。(図4-2)

▼図4-2 「線の考え方」に基づく不正利用対策



対策が必要な場面	不正手口	不正内容
会員登録	不正アカウント作成	EC加盟店において、窃取した属性情報・カード情報等を利用し、不正なアカウントの登録を行う。
会員ログイン・属性情報変更	アカウント乗っ取り	窃取した正規のアカウントなどのログイン情報などを使用し、不正ログインを行う。

出所：『クレジットカード・セキュリティガイドライン【6.0版】改訂ポイント』（2025年3月）をもとに作成

不正ログイン対策がカード決済前の対策として位置付けられた背景には、最近のECサイトでは、まず消費者がサイトに会員登録してIDとパスワードを作成する会員登録型が主流となっていることがある。会員登録型ECサイトの多くは消費者が買い物の都度決済情報を入力する手間を省くため、予め支払手段を登録できる。その場合、不正ログインが支払手段の不正利用に直結することになる。

『ガイドライン6.0』では、まず、不正ログインの手口を「不正アカウント作成」と「アカウント乗っ取り」の2つに分けた。不正アカウント作成は、ECサイトで他人（または架空）の属性情報を利用してアカウントを作成し、他人のカード情報を支払手段として登録する手口である。防ぐためには、会員登録時に不正な登録をさせない対策が必要である。アカウント乗っ取りは、フィッシングその他の手法で入手した認証情報を利用して既にある正規のアカウントにより不正ログインし、登録済みのカード情報を利用して決済を行う手口である。また、その際に、攻撃者は登録されている連絡先や配送先情報などの属性情報を変更することがある。そのため、ログイン時と属性情報変更時の対策が必要である。

具体的な対策は『セキュリティガイドライン附属文書20』に取りまとめられている。『セキュリティガイドライン6.0』では、その中でも図4-3に示した7つの対策を優先して導入することが望ましい対策として記載している。

▼図4-3　優先して導入することが望ましい不正ログイン対策の内容

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

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

(1)-3. 不正顕在化加盟店、高リスク商材取扱加盟店の対策における変更点

『セキュリティガイドライン5.0』までは、EC加盟店の不正利用対策としてオーソリゼーション処理の体制整備、善管注意義務に加えて「本人認証」「券面認証」「属性・行動分析（不正検知システム）」「配送先情報」の４つの方策を挙げ、高リスク商材取扱加盟店（※1）は1つ以上、不正顕在化加盟店（※2）は２つ以上を導入することを求めていた。

※1　：①デジタルコンテンツ（オンラインゲームを含む）、②家電、③電子マネー、④チケット、⑤宿泊予約サービス を取扱う加盟店

※2　：アクワイアラ各社が把握する不正利用金額が、「3ヵ月連続50万円超」に該当する加盟店

しかし実際には加盟店の取扱商品やスキーム等により手口が異なりこれまでの４方策では実効的な抑止効果が得られなくなっていることから、『セキュリティガイドライン6.0』では、不正顕在化加盟店に対しては指針対策を「線の考え方」に基づく不正利用対策の追加導入を求めるように変更した。類似の不正利用の発生を防止するために、不正利用の発生状況を把握する。取り扱い、取扱商品やスキーム等によって異なる不正利用の手口に応じて「適切な対策の追加導入」や既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングによる「対策の強化」を行う。追加導入する対策については、『セキュリティガイドライン附属文書20』にて、「線の考え方」に基づき決済前・決済時・決済後の場面ごとに取りまとめられている。また、「対策の強化」とは、EMV 3-DSや属性・行動分析を導入している場合に、リスク判定や不正判定レベルの分析に基づき、リスク判定項目の追加・変更や不正判定レベルのチューニングによる精度向上を行うことを指す。対策を導入するだけでなく、精度を上げるために継続した見直しが求められる。

なお、従来の高リスク商材取り扱い加盟店については、「相対的にリスクが高い商材」として、追加導入する対策や既に導入している対策の設定項目の追加・変更、チューニングにおいては、リスクを認識した上で適切な対応を行うと整理された。

(1) -4. MO・TO加盟店の不正利用対策の指針対策の変更

従来は、MO・TO（メールオーダー・テレフォンオーダー）加盟店の不正利用対策としてEC加盟店と同様にオーソリゼーション処理の体制整備、善管注意義務に加えて４方策のうち高リスク商材取扱加盟店は1つ以上、不正顕在化加盟店は２つ以上を導入することを求めていた。『セキュリティガイドライン6.0』では、追加の対策が見直され、リスクベースによる適切な対策の導入に変更された。なお、「相対的にリスクが高い商材」を取り扱う場合は、商材のリスクに応じた適切な不正利用対策をとることが必要となる。また、アクワイアラや決済代行事業者から短期間に不正利用が急増した旨の連絡を受けた場合は、追加の対策導入が必要となる。

MO・TO加盟店の場合、EMV3-DSについては、カード情報を消費者が自ら入力することはないため導入できない。不正利用対策を強化するためには、配送先情報チェックによる配送停止や配送保留など、決済後の対策が必要となる。

(2)警察庁とカード会社の連携強化

クレジットカード不正利用の未然防止に向け警察から国際カードブランドへ流出カード情報の連携を開始

「１．2024年のカード情報流出事件の概況」で解説した通り、2024年のカード情報流出件数は 540,722件 に達し、高止まりの状況が続いている。

こうした事態を受け、警察はクレジットカード不正利用被害の拡大防止に向けた取り組みを強化している。2024年6月18日に閣議決定された「国民を詐欺から守るための総合対策」では、カード不正利用情報の効率的な提供が重点施策に位置付けられ、これを契機に「警察から国際ブランドへの流出カード番号連携」が開始された。

従来、悪用が懸念されるカード番号を警察が把握した場合、都道府県警が約240社のカード発行会社（イシュア）に個別連絡を行っていた。しかし、カード番号だけでは即座にイシュアが特定できないカードもあり、国際ブランドに照会する必要があった。さらにイシュアごとにメール・電話など連絡方法が異なるため、情報共有に時間がかかるという課題があった。

こうした非効率を解消するため、警察庁は2024年12月19日から、国内シェア9割超を占める American Express、JCB、Mastercard、Visa、Diners Club、Discover の6つの国際ブランドと連携を開始した。警察が把握した流出カード番号をこれら国際ブランドに一括提供し、ブランド各社がイシュアに迅速に情報を伝える仕組みである。

これにより、イシュアは速やかに利用停止措置を取り、利用者への連絡やカード差し替えの提案を行える体制が整った。その結果として、情報共有から利用停止までのプロセスが大幅に短縮され、不正利用を未然に防げる可能性が高まった。都道府県警の業務負担も軽減され、他のサイバー犯罪対策に人員や時間を振り向けられる効果も期待できる。

(3)『個人情報の保護に関する法律についてのガイドライン』に関するQ&A追加

2025年6月、『個人情報の保護に関する法律についてのガイドライン』に関するQ&A に、ECサイトにおいて不正な取引が疑われる個人データの取り扱いに関する記載が追加された。ECサイト事業者が警察や公的機関に対し、不正な取引が疑われる取引を行なっている者に関する個人データ提供する場合、本人同意不要で提供できることが明記された。これまでは、EC事業者が不正取引等を把握しても、個人情報に配慮して、疑い段階での警察への情報提供をためらう例があったが、指針に明記して情報提供の可否を判断しやすくすることで、警察との情報連携を強化する。

個人データを第三者に提供する際は原則として、あらかじめ本人の同意を得る必要があるが、「国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき」は、本人の同意は不要である。ECサイト運営事業者が被害にあった顧客の通報や独自の監視により、犯罪の一部となる不正な取引または合理的に不正な取引と疑われる取引（以下、不正取引等）を把握した際に、当該不正取引等を行う者に関する個人データを必要最小限の範囲で警察に提供することは、これに該当すると整理した。また被害にあった顧客から通報があった場合は、同様の特徴をもつ取引についても不正取引等に該当するとした。

個人情報が登録されたアカウントが不正ログインされ、不正取引に使用された場合にも、原則として警察へ個人データを提供する際には当該個人の同意を得る必要がある。その場合も同意を取得するための時間的余裕や費用に照らして事実上不可能な状況下では同意を得る必要がないと整理された。

＜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』（経済産業省商務・サービスグループキャッシュレス推進室　2025年3月31日）
https://www.meti.go.jp/press/2024/03/20250331005/20250331005.html

2.『クレジットカード・セキュリティガイドライン【5.0版】』（クレジット取引セキュリティ対策協議会　2024年3月）
https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_5.0_published.pdf

3.『クレジットカード・セキュリティガイドライン【6.0版】』（クレジット取引セキュリティ対策協議会　2025年3月）
https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_6.0_published.pdf

4.『クレジットカード・セキュリティガイドライン【6.0版】改訂ポイント』（クレジット取引セキュリティ対策協議会　2025年3月）
https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_6.0_revisionpoint.pdf

5.『Fox Research』（フォックスリサーチ）
『【限定記事】クレジットカード情報漏洩事件のまとめ（2024年上半期）』（最終更新 2024/7/21）
https://foxresearch.hatenablog.com/entry/2024/03/14/174125
『【限定記事】クレジットカード情報漏洩事件のまとめ（2024年下半期） その1』（最終更新 2025/1/8）
https://foxresearch.hatenablog.com/entry/2025/01/08/173235
『【限定記事】クレジットカード情報漏洩事件のまとめ（2024年下半期） その２』（最終更新 2025/1/8）
https://foxresearch.hatenablog.com/entry/2024/11/07/201254

6.『「不正注文」で国内オンラインショップサイトを侵害する攻撃キャンペーン「Water Pamola」』（トレンドマイクロ　2021年5月）
https://www.trendmicro.com/ja_jp/research/21/e/water-pamola-attack-campaign-that-infiltrates-japanese-online-shopping-sites-with-malicious-orders.html

7.『ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃』（JPCERT/CC　2021年7月6日）
https://blogs.jpcert.or.jp/ja/2021/07/water_pamola.html

8.『CIS Benchmarks』（Center for Internet Security）
https://www.cisecurity.org/cis-benchmarks

9.『令和5年度電子商取引に関する市場調査の結果を取りまとめました』（経済産業省　2024年9月25日）
https://www.meti.go.jp/press/2024/09/20240925001/20240925001.html

10.『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　2025年6月）
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf

11.『IBM X-Force脅威インテリジェンス・インデックス2025』（IBM　2025年4月16日）
https://www.ibm.com/thought-leadership/institute-business-value/jp-ja/report/2025-threat-intelligence-index#D

12.『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』（警察庁　2025年3月13日）
https://www.npa.go.jp/news/release/2025/R070313_access.pdf

13.『EC事業者実態調査』（Cacco　2024年12月26日）
https://prtimes.jp/main/html/rd/p/000000164.000009799.html

14.『クレジットカード会社等に対するフィッシング対策の強化を要請しました』（経済産業省・総務省・警察庁　2023年2月1日）
https://www.meti.go.jp/press/2022/02/20230201001/20230201001.html

15.『送信ドメイン認証技術「DMARC」の導入状況と必要性について』（フィッシング対策協議会　2025年1月30日）
https://www.antiphishing.jp/report/wg/cert_explaindoc_20250130.html

16.『国内カード会社8社とACSiONと共同でフィッシングサイト閉鎖の取組を開始しました。』（日本クレジットカード協会　2025年3月31日）
https://www.jcca-office.gr.jp/info/1378/

17.『インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています』（金融庁　2025年8月7日更新）
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

18.『本協会において実施したインターネット取引における不正アクセス等への対応等について』（日本証券業協会　2025年5月20日）
『多要素認証の設定必須化を決定した証券会社』（日本証券業協会　2025年7月7日更新）
https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/list_tayouso/index.html

19.『今般のインターネット取引サービスにおけるフィッシング詐欺等による証券口座への不正アクセス等による対応について（10社申し合わせ）』（日本証券業協会　2025年5月2日）
https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/higai/index.html

20.『日本が今、最も狙われている【続編】―プルーフポイントのデータからみる生成AI時代のメール脅威と対策』（米Proofpoint　2025年8月11日）
https://www.proofpoint.com/jp/blog/email-and-cloud-threats/email-threats-and-countermeasures-generative-ai-age

21.『「インターネット取引における不正アクセス等防止に向けたガイドライン」の改正について（案）』（日本証券業協会　2025年7月15日）
https://www.jsda.or.jp/about/public/bosyu/files/20250715_guideline_public.pdf

22.『「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）の公表について』（金融庁　2025年7月15日）
https://www.fsa.go.jp/news/r7/shouken/20250715/20250715.html

23.『サイバー警察局だより』（全国銀行協会、金融庁、警察庁、日本サイバー犯罪対策センター　2025年4月）
https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.1cpal.pdf

24.『国民を詐欺から守るための総合対策』（犯罪対策閣僚会議　2024年6月18日）
https://www.soumu.go.jp/main_content/000953287.pdf

25.『個人情報の保護に関する法律についてのガイドライン」に関するQ＆A』（個人情報保護委員会　2025年7月1日）
https://www.ppc.go.jp/personalinfo/faq/APPI_QA/

キャッシュレスセキュリティレポート2025
2025年10月2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）
