PCI DSS Ready Cloud

# Cashless Security Report
## Annual Report 2024

2024年9月9日
かっこ株式会社
株式会社リンク

# もくじ

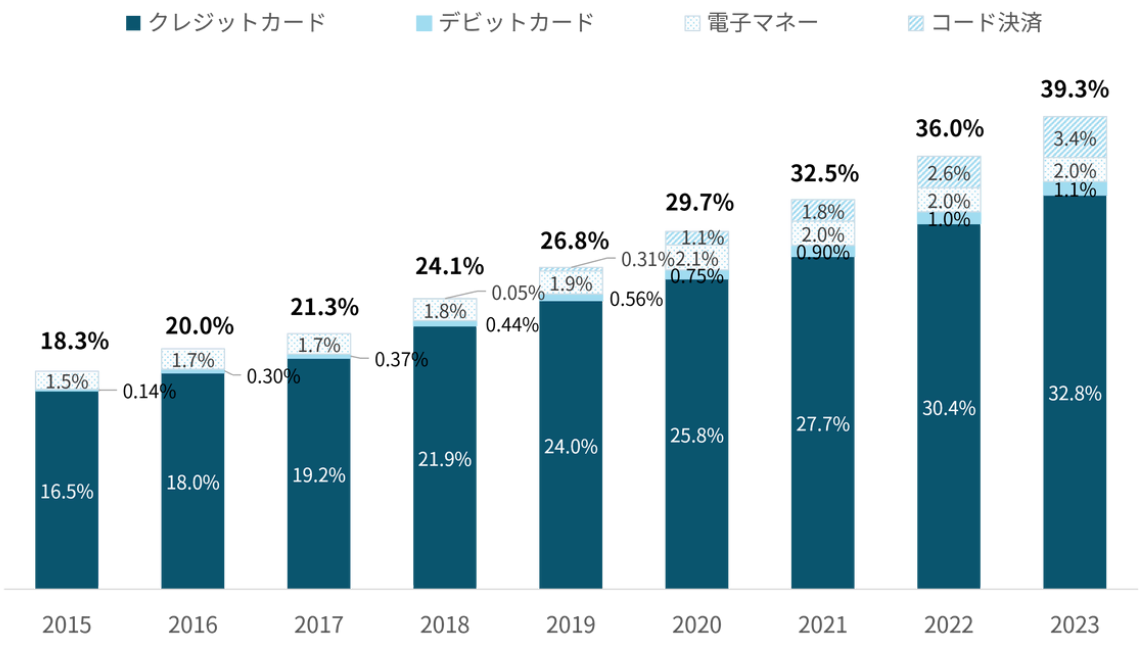
# もくじ

# はじめに

2024年に経済産業省が公表したデータによれば、2023年のキャッシュレス決済比率は39.3%と2022年に比べて3.3ポイントの増加となった（図1-1）。キャッシュレス比率の上昇傾向は継続しており、政府が掲げる「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%」の目標は前倒しで達成できる見通しとなった。

2023年の決済手段の内訳は、コード決済が3.4%と前年に比べて0.8ポイント上回った。前年に比べ３割以上増えており、４つのキャッシュレス決済手段の中で最も伸び率が高い。クレジットカードも、2022年の30.4%から32.8%へと着実に増加している。キャッシュレス決済に占めるクレジットカードの割合は2022年の84.5%から83.5%となり、コード決済の割合は2022年の7.1%から8.6%と増加している。コード決済の割合が増えた分クレジットカード決済の割合が減る構図となっているが、依然日本のキャッシュレスの８割以上をクレジットカードが占めている。

▼図1-1 キャッシュレス決済比率の推移




出所：『2023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)

クレジットカードなどのカード情報を狙った攻撃は、2022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、クレジットカード不正利用被害は2022年をさらに上回り、年間約540億円と過去最悪の記録をさらに更新した。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。また、2023年はオンラインバンキングを悪用した不正送金の被害が急増しており、対策が急がれる。

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に関する統計とECに関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。年次レポート「キャッシュレスセキュリティ2024」は、この取り組みの一環として、国内のキャッシュレス不正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。なお、本レポートは、2023年までCaccoとｆｊコンサルティング株式会社（以下ｆｊコンサルティング）が共同で制作していた「キャッシュレスセキュリティレポート」を継承した内容となる。

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. 2023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。

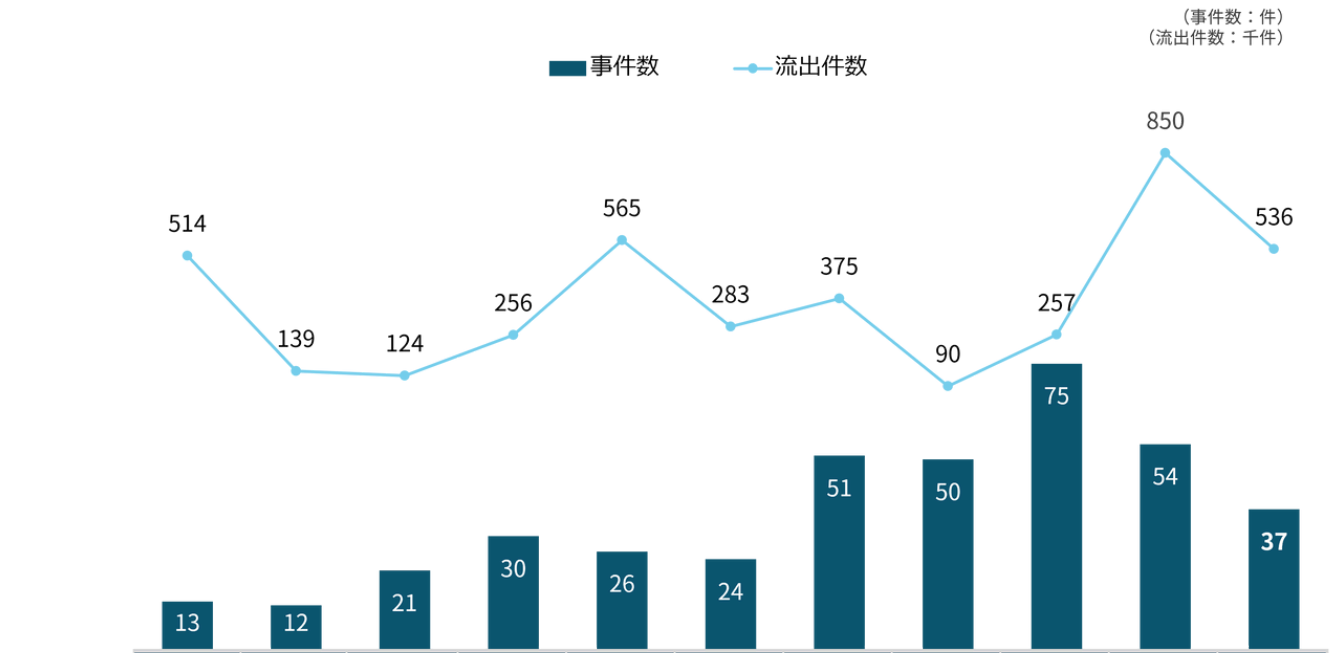
●カード情報流出件数：発表主体により公表された流出件数で、クレジットカード、ブランドデビットカード、ブランドプリペイドカードを含む。公開された件数のうち、最新の情報を正として集計

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）。

### (1)-1. 年次推移

2023年1月から12月に公表された事件数は37件と、2021年に比べて17件減っている。カード情報流出件数は536,291件と、2022年に比べて約31万件の減少となった（図1-2）。１事件あたりの平均流出件数は14,897件となり、調査開始以来4番目に多い数字となっている。

▼図1-2 国内のカード情報流出事件発生状況




| | 2013年 | 2014年 | 2015年 | 2016年 | 2017年 | 2018年 | 2019年 | 2020年 | 2021年 | 2022年 | 2023年 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 事件数 | 13 | 12 | 21 | 30 | 26 | 24 | 51 | 50 | 75 | 54 | 37 |
| カード情報流出件数 | 514,369 | 138,717 | 123,527 | 255,689 | 564,844 | 283,374 | 375,479 | 89,628 | 256,822 | 849,950 | 536,291 |
| 1件あたり平均件数 | 42,864 | 12,611 | 7,266 | 9,470 | 22,594 | 12,321 | 7,344 | 1,793 | 3,424 | 16,345 | 14,897 |

Cacco/ｆｊコンサルティングによる（2021年以前のデータはｆｊコンサルティングによる）

カード情報流出件数のうち、2023年5月に公表されたカード会社A社からの流出が290,771件と半数以上を占めており、平均流出件数を引き上げている (図1-3)。この事案は、カード会員宛のダイレクトメールの表面にお客様番号を印刷すべきところ、カード番号を誤って印刷して発送したことによりカード情報が流出したものであり、カード情報を狙った攻撃の被害ではない。カード情報窃取を目的とした被害に限定すると、カード情報流出件数は245,520件となり、2022年から大きく減少している。

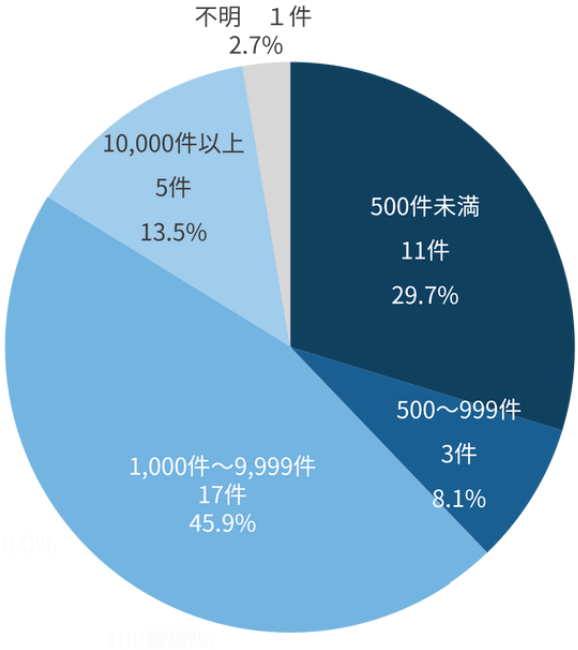
▼図1-3 2023年カード情報流出件数の多かった事件

| | サイト名（運営企業） | 流出件数 | 流出期間（日数） | 原因 |
|---|---|---|---|---|
| 1 | カード会社 A社 | 290,771 | 2 | ダイレクトメール表面へのカード番号誤印刷 |
| 2 | 電子機器・ソフトウェア販売 B社 | 112,313 | 64 | オンラインスキミング（可能性高） |
| 3 | 教育研修サービス C社 | 23,309 | 850 | オンラインスキミング |
| 4 | 手芸素材販売 D社 | 14,256 | 620 | オンラインスキミング |
| 5 | ホビーグッズ販売 E社 | 13,084 | 661 | オンラインスキミング（可能性高） |
| 6 | アパレル（雑貨）販売 F社 | 9,416 | 511 | オンラインスキミング |
| 7 | アパレル（バック・生地）販売 G社 | 8,655 | 755 | オンラインスキミング（可能性高） |
| 8 | レンタルドレスサービス H社 | 8.604 | 243 | オンラインスキミング（可能性高） |
| 9 | コスメ販売 I社 | 7.024 | 520 | オンラインスキミング（可能性高） |
| 10 | 産業用品部品販売 J社 | 6,364 | 616 | オンラインスキミング（可能性高） |

Cacco/ｆｊコンサルティングによる

カード情報の流出規模別の事件数を見ると、流出件数500未満の事件が11件（29.8%）、500～999の事件が3件（8.1%）となった。1,000未満の事件の割合は約4割で、2022年とほぼ変わらなかった。一方で、10,000件以上の事件は前述のカード会社A社の事故も含め、5件（13.5%)となった（図1-4）。加盟店からの流出に限定すると、２位の電子機器・ソフトウェア販売 B社の流出件数が112,131件と突出しているが、それ以外には30,000件を超える流出はなかった。

▼図1-4 2023年カード情報流出件数の多かった事件



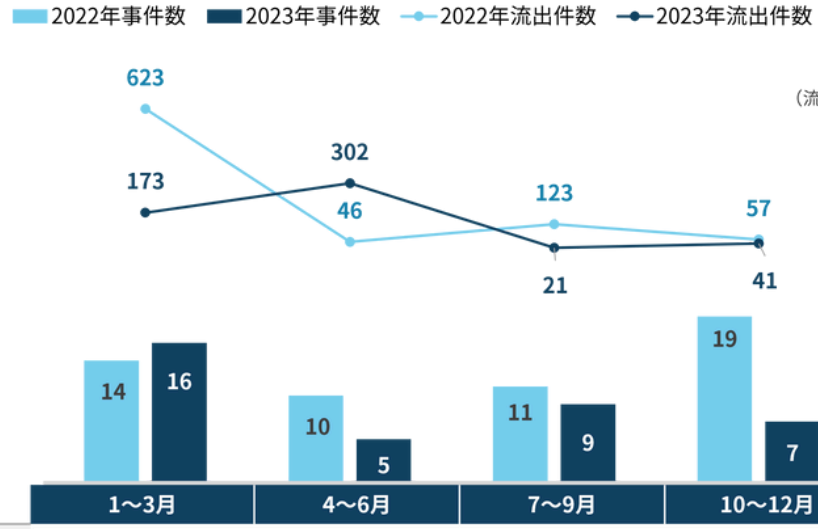

| 流出件数規模 | 事件数 | 割合 |
|---|---|---|
| 500未満 | 11 | 29.8% |
| 500～999 | 3 | 8.1% |
| 1,000～1,499 | 1 | 2.7% |
| 1,500～1,999 | 3 | 8.1% |
| 2,000～2,499 | 1 | 2.7% |
| 2,500～2,999 | 1 | 2.7% |
| 3,000～3,499 | 0 | 0.0% |
| 3,500～3,999 | 1 | 2.7% |
| 4,000～4,499 | 3 | 8.1% |
| 4,500～4,999 | 0 | 0.0% |
| 5,000～7,499 | 4 | 10.8% |
| 7500～9.999 | 3 | 8.1% |
| 10,000以上 | 5 | 13.5% |
| 不明 | 1 | 2.7% |

Cacco/ｆｊコンサルティングによる

### (1)-2. 四半期別推移

四半期別の事件数を2022年と比較する（図1-5）。2023年1-3月は前年よりも2件多く16件となった。うち2件は2022年10月に公表されたサプライチェーン攻撃（加盟店が利用するプラットフォームやサービスを攻撃することで、一度に複数の加盟店から情報を窃取する攻撃）に起因する流出である。また、カード情報流出件数は大幅に減っている。理由は、2022年1-3月期の流出件数に決済代行事業者から約46万件の流出が含まれているためである。4-6月期は、事件数は10件から5件と半減している。しかし流出件数は、5月に前述のカード会社A社による約29万件のカード情報流出が公表されたことにより大幅に増えて30万件を超えている。7-9月期については事件数が11件から9件と2件減少しているが、流出件数が5,000件を超える事件は1件のみと比較的小規模な事件が多かったため、カード情報流出件数は10万件以上減っている。10-12月期は事件数が19件から7件と半分以下に減っているが、教育研修サービスC社（カード情報流出件数 23,309件）とホビーグッズ販売E社（同 13,084件）の2件が含まれており、流出件数は約17,000件の減少に止まった。

▼図1-5 2022年と2023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 |
|---|---|---|---|---|---|
| 2022年 | 事件数(件) | 14 | 10 | 11 | 19 |
| | カード情報流出件数(件) | 623,491 | 46,429 | 122,829 | 57,201 |
| 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/ｆｊコンサルティングによる

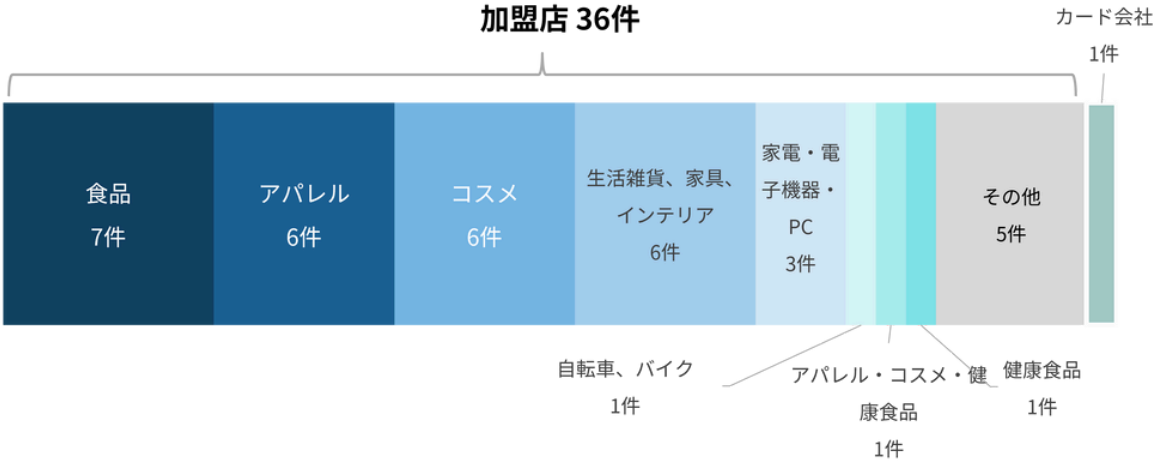
## (2)カード情報流出事件の傾向

### (2)-1. 業種／取扱い商材別・情報流出期間別事件数

2023年のカード情報流出事件37件の内訳を図1-6に示す。36件が加盟店からの流出、1件がカード会社からの流出である。

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（7件）、次いでアパレル（6件）／コスメ（6件）／生活雑貨、家具、インテリア（6件）となる。

▼図1-6 2023年業種/取扱い商材別カード情報流出件数

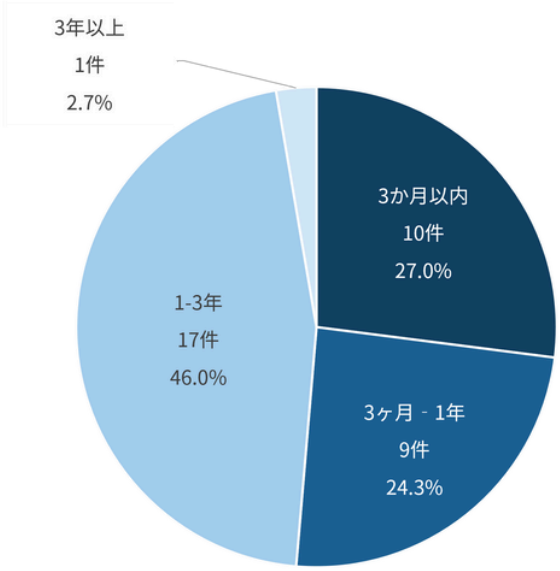



Cacco/ｆｊコンサルティングによる

流出期間別の割合は以下となる。1-3年の事件が46%と最も多く17件（46.0%）を占めた。次いで3ヶ月以内が10件（27.0%）、3ヶ月-1年（24.3%）がほぼ同じ割合を占めている（図1-7）。

なお、流出期間3年以上となっている1件は、ランサムウェアによりサーバーに保存されていたカード情報が流出した酒造会社K社（カード情報流出件数23件）の事件である（詳細は後述）。

▼図1-7 2023年流出期間別事件数




Cacco/ｆｊコンサルティングによる

業種別・取扱い商材別にカード情報流出件数と流出期間についてとりまとめたのが図1-8となる。

加盟店についてみると、1事件あたりの平均流出期間は417.9日、1事件で流出したカード情報の流出件数は7,107件となっている。事件数が最も多い食品は平均流出期間が802.1日と長くなっているが、前述のK社を除くと平均流出期間は573.1日となる。

加盟店からのカード情報流出件数245,520件のうち、家電・電子機器・PCが118,511件と48.2%を占めている。そのほとんどが前述の電子機器・ソフトウェア販売 B社による流出である。次いで多いのはアパレルで47,625件となり、この2業種で加盟店からの流出件数の67.6%と約3分の2を占めている。

▼図1-8 2023年業種・取扱い商材別カード情報流出件数/流出期間

| 業種／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） |
|---|---|---|---|---|---|
| **A. 加盟店合計** | | **36** | **245,520** | **417.9** | **7,017** |
| 加盟店取扱い商材別 | ①食品 | 7 | 13,841 | 802.1 | 1,977 |
| | ②アパレル | 6 | 47,625 | 523.5 | 7,938 |
| | ③コスメ | 6 | 13,774 | 274.2 | 2,296 |
| | ④生活雑貨、家具、インテリア | 6 | 11,156 | 244.2 | 1,859 |
| | ⑤家電・電子機器・PC | 3 | 118,511 | 227,7 | 39,504 |
| | ⑥自転車、バイク | 1 | 2,602 | 370,0 | 2,602 |
| | ⑦アパレル・コスメ・健康食品 | 1 | 605 | 11,0 | 605 |
| | ⑧健康食品 | 1 | 14 | 215,0 | 14 |
| | ⑨その他 | 5 | 37,392 | 380.2 | 9,348 |
| **B. カード会社** | | **1** | **290,771** | **2.0** | **290,771** |

※「その他」のうち1件はカード情報流出件数が不明のため、平均流出カード情報件数の算出からは除外
Cacco/ｆｊコンサルティングによる

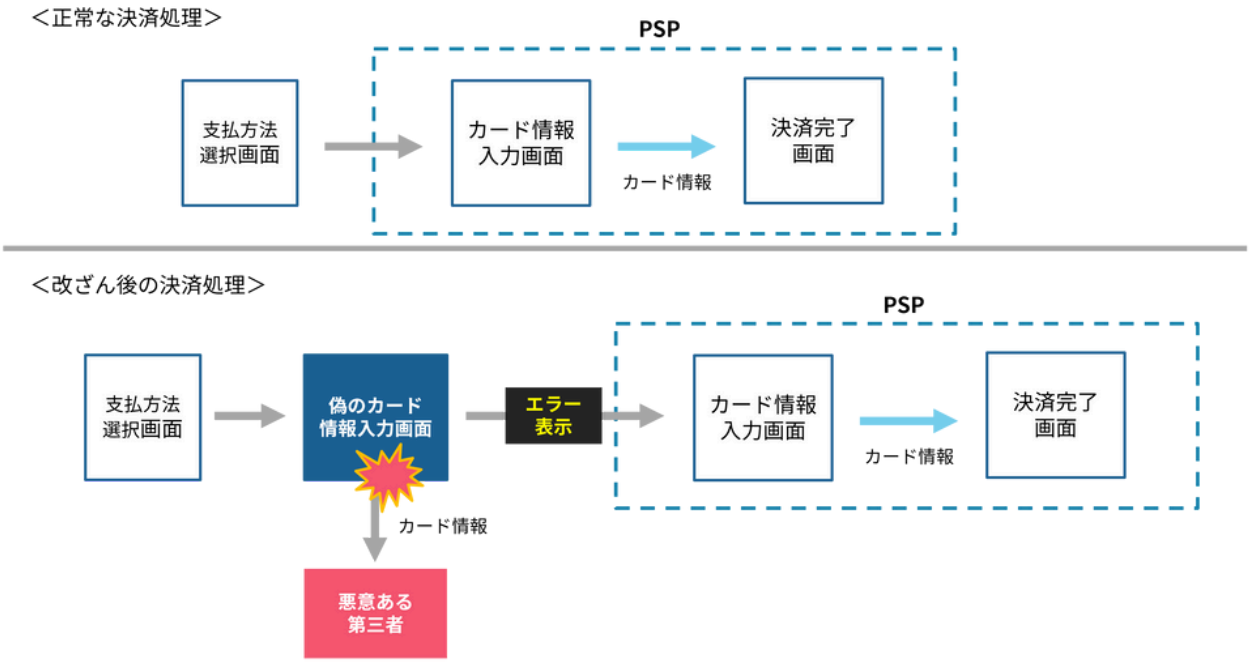
### (2)-2. カード情報窃取の手口：オンラインスキミング以外の手口が増加

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【5.0版】』（以下『ガイドライン5.0』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直接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、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）。非保持化済みのECサイトであっても、脆弱性対策、ウイルス対策、管理者権限の管理、デバイス管理等の基本的なセキュリティ対策により、ECサイトへの侵入を防ぐための方策が必須である。『ガイドライン5.0』では、必要な対策を付属文書『セキュリティ・チェックリスト』に取りまとめている。（4-(1)-2参照）

▼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




出所：『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）を参考に作成

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、2023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）

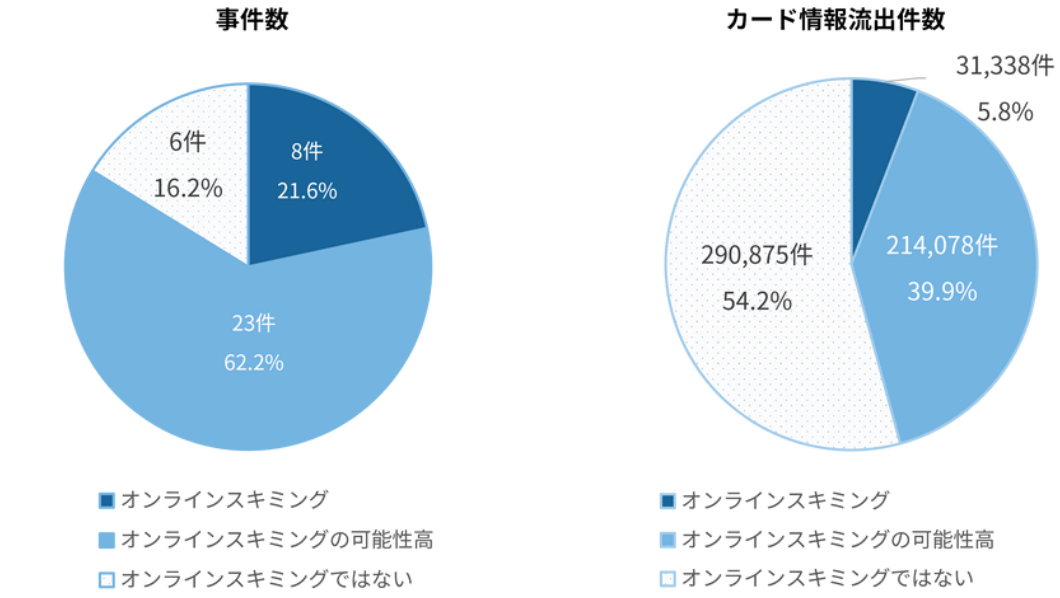
①オンラインスキミング：公式発表で「決済画面が2枚あった」「画面に入力したカード情報が第三者に送信された」等のオンラインスキミングであることがわかる記載がある。

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 2023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




リンクによる

※「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

2023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31件、83.8%となった。

なお、2023年の特筆すべき事項として、京都府警などの合同捜査本部により、オンラインスキミングによるカード情報の不正入手が初めて摘発された。2022年10月から、音楽グループの公式オンラインショップを改ざんして、グッズなどを購入するためにアクセスした利用者3名のカード情報を不正に入手した行為が、不正指令電磁的記録供用と割賦販売法違反の疑いにあたるとされた。

外部からの指摘や内部の調査により、カード情報流出事件が発覚してから公表までには、通常、3ヶ月から9ヶ月程度かかることが多い。一方で、消費者の立場では、調査の結果を待たずとも自身のカード情報が流出している可能性を早く知ることで、未然に不正利用被害を防げる可能性がある。そのため、時に流出したカード加盟店が「カード情報流出の事実を隠蔽していたことで不正利用被害が広がった」という批判に晒されることがある。

事件の公表までに時間がかかるのは、指定された機関によるフォレンジック調査の結果を待って影響範囲を特定し、契約するカード会社などと事後の対応について調整してから情報を公開するという慣習によるものである。混乱を避けるための措置であるが、カード加盟店によっては、流出の可能性の段階であっても自社の顧客に通知、公表したいという要望もある。消費者保護の観点からは、詳細な調査結果を待たず第一報として、情報流出が発覚した段階で公表するべきであると考える。

オンラインスキミング以外の事件6件のうち、1件は前述のカード会社A社によるダイレクトメールへの誤印刷である。残りの5件の内訳は以下の通りであり、いずれもECサイト以外からの流出である。

1) ランサムウェアによる流出（2023年3月公表）

酒造会社K社が2022年9月に公表していたランサムウェア被害において、暗号化されたデータの中に電話で注文を受けた時のクレジットカード情報が記載された注文書やメモの画像が含まれたことが判明した。（流出カード情報件数：23件）。同社が運営するECサイトについてはクレジットカード情報を保持しない形態となっており、電話による注文もクレジットカード情報が記載されたデータファイルについてはサーバー内に保存しないルールとしていた。しかし、運用ルールが徹底されておらず、想定していない場所からカード情報が発見されることとなった。

2) コールセンターからの流出（2023年7月公表）

旅行会社L社が、自社コールセンターへ電話で旅行を申し込んだ顧客のクレジットカードが不正利用されていることを公表した。（流出カード情報件数：非公開）

3) コールセンターシステム運用保守担当者による不正持ち出し（2023年10月公表）

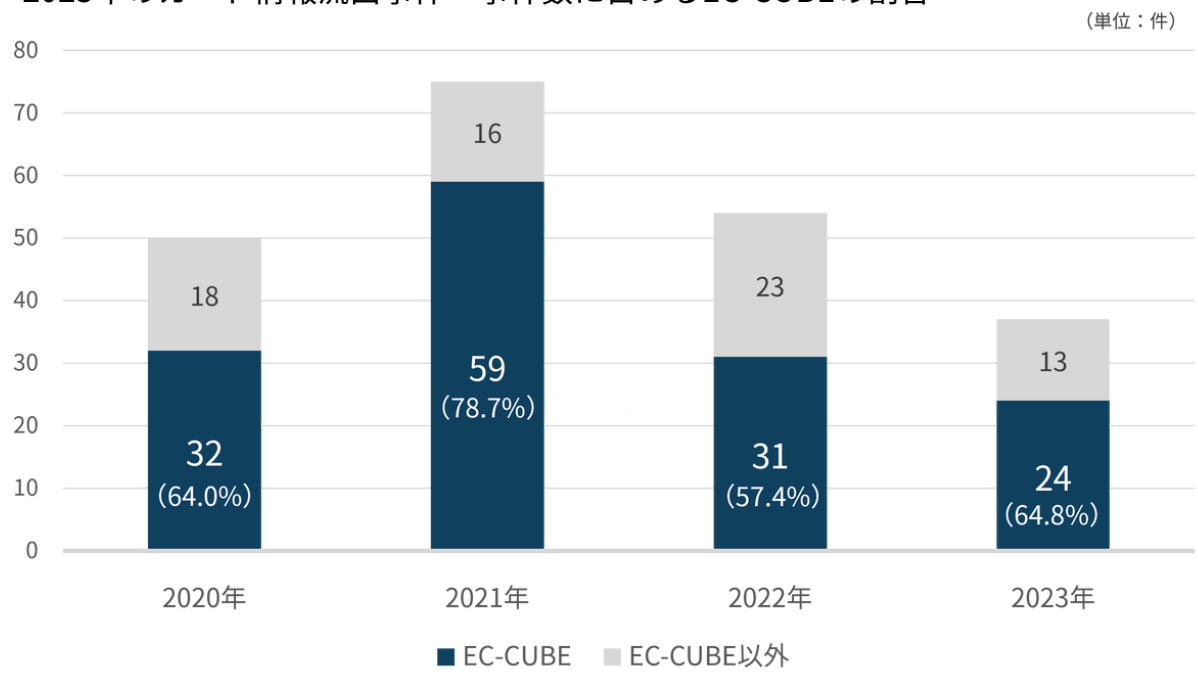
コールセンター業務を受託するM社が、運用保守業務委託先の派遣社員が顧客データを持ち出し、900万件以上の個人情報が流出したことを公表した。カード情報については、3件のECサイトから合計81件が流出した。（詳細は後述）

カード情報流出件数については245,416件（45.8%）がオンラインスキミングもしくはその可能性が高い事件である。カード会社A社からの流出を除く、加盟店からの流出（245,520件）に対するオンラインスキミングもしくはその可能性が高い事件が占める割合は、ほぼ100%となっている。

**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2023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24件（64.8%）に達している（図1-11）。2022年の31件に比べると事件数自体は減っているが、割合は若干増えている。2023年のECサイトからの流出事件（31件）に対するEC-CUBEが使用されている割合は77.4%と 高い割合を占めた。

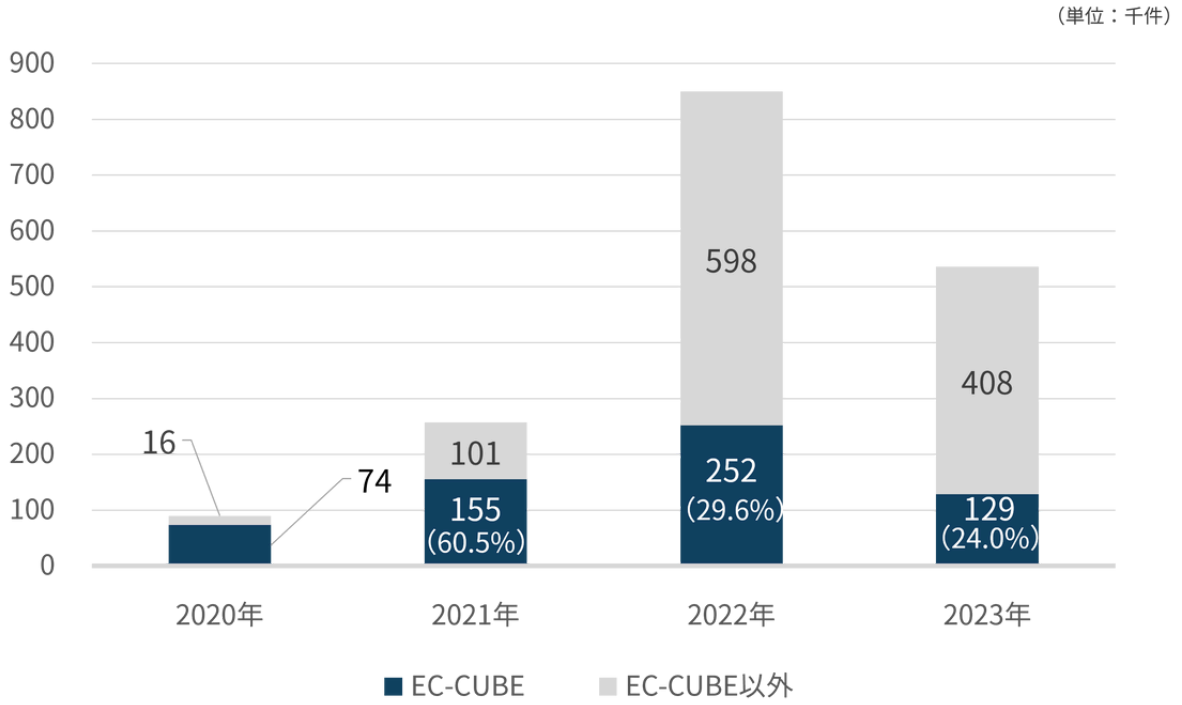
▼図1-11　2023年のカード情報流出事件　事件数に占めるEC-CUBEの割合




出所：『Fox Research』による

カード情報流出件数に占めるEC-CUBEの割合は128,508件（24.0%）となっている（図1-12）。2022年と比較すると割合は若干減っている。2023年のECサイトからの流出件数（245,416件）に対するEC-CUBEが使用されている割合は52.4%であった。

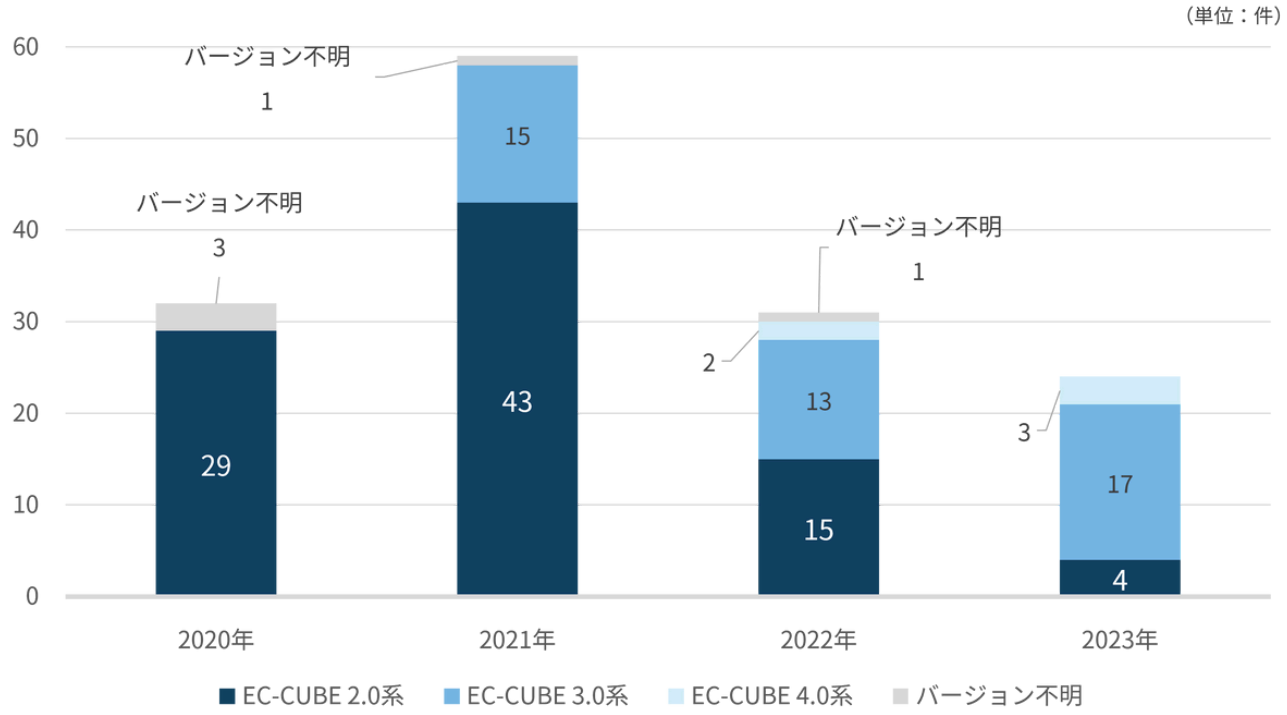
▼図1-12　2023年のカード情報流出事件 流出件数に占めるEC-CUBEの割合




出所：『Fox Research』による

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。2023年で最も多かったのはEC-CUBE 3.0系で24件中17件であり、EC-CUBE2.0系は4件まで減っている。EC-CUBE 4.0系は3件であった。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、3.0系と4.0系についてはこれを悪用した攻撃と推定される。

▼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』による

今後もEC-CUBE3.0系、4.0系の被害が増えることが予想される。EC-CUBEなどオープンソースソフトウェアを利用する際は、セキュリティパッチを迅速に適用して既知の脆弱性に対応する必要がある。

## (3)2023年のカード情報流出事件のトピック

ECサイトへの攻撃によらないカード情報の流出が多数発生している。本レポートでは、その中から、大手宿泊サイトのメッセージ機能を悪用したフィッシング攻撃と、コールセンター業務委託先からの内部不正による持ち出しを取り上げる。

### (3)-1. 大手宿泊予約サイトの機能を悪用したフィッシング攻撃

大手宿泊予約サイトBooking.comで宿泊施設を予約した利用者をターゲットにした、カード情報の窃取を目的としたフィッシングが全世界で多発している。日本でも2023年5月ごろから被害が報告されはじめた。2024年2月末時点で90件以上の宿泊施設が被害を公表していると報じられており、その後も被害は続いている。2023年11月には国土交通省や観光庁から「Booking.com利用者へのフィッシング被害に関する注意喚起」が公表された。また、Booking.com以外の宿泊予約サイトでも、同様の被害が報告されている。

米Secureworks 社の調査によれば、この攻撃は2段階のフィッシングで行われ、いずれもBooking.comが宿泊施設に提供する宿泊客向けのメッセージ送信機能が悪用された。

① 宿泊施設の管理者を対象としたフィッシング

攻撃者は宿泊客を装ってBooking.comで宿泊施設を予約し、サイト内のメッセージ機能を使用して宿泊施設とやり取りする。何度目かのやりとりで添付ファイルを装ってGoogleドライブのリンクを送信し、パスワードを窃取するマルウェアを宿泊施設管理者のパソコンにダウンロードさせる。Secureworks社が入手した攻撃者のメッセージは、宿泊した際に身分証明書を紛失したので捜索に協力して欲しいという宿泊施設への依頼であった。最初は添付ファイルもリンクもないメールだったが、何度目かのやりとりで、「紛失したパスポートの写真とチェックイン情報が保存されている」としてGoogle DriveのURLが送信された。宿泊施設のスタッフがURLをクリックすると、ZIPファイルがダウンロードされ、そのファイルにマルウェアが含まれていた。

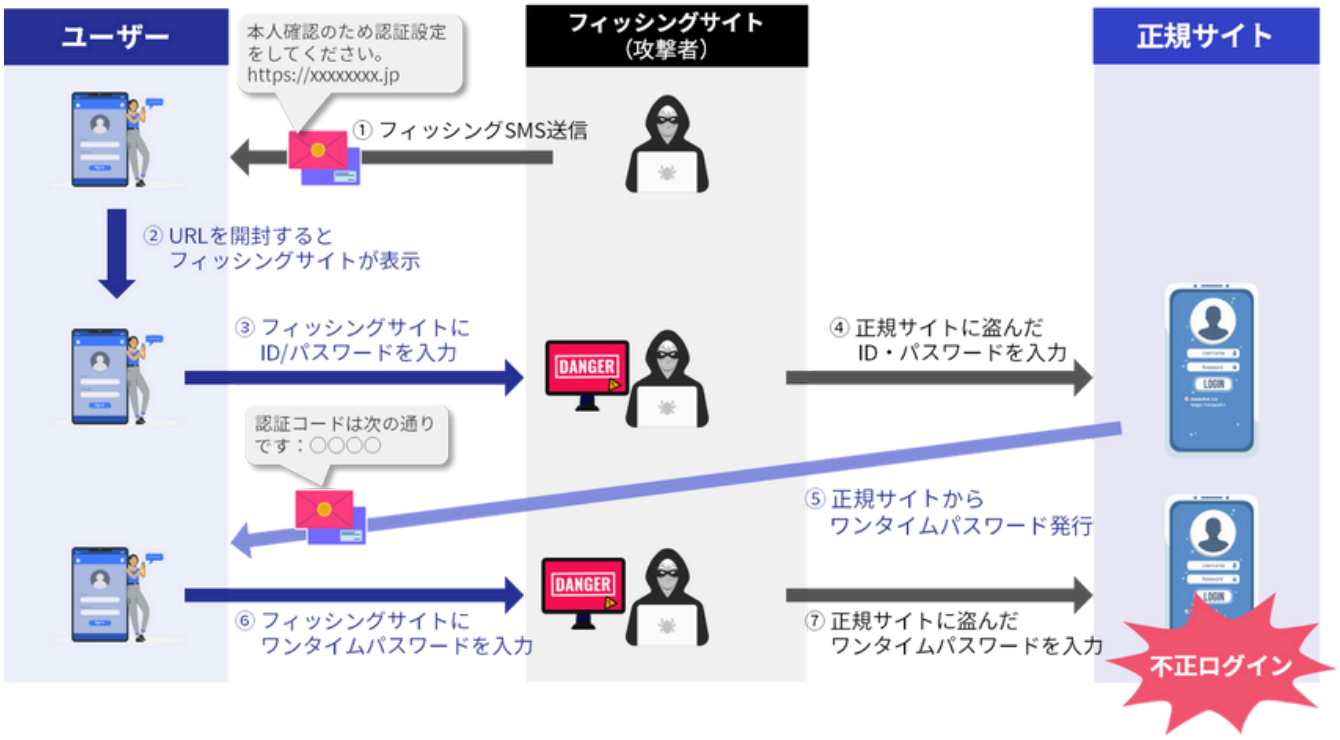
宿泊施設の管理者画面に多要素認証を設定していない場合、窃取された認証情報で宿泊施設の管理画面に不正にログインが可能となる。

②利用者を対象としたフィッシング

宿泊施設の管理者として不正ログインした攻撃者は、宿泊予約客向けのメッセージ機能を利用して「クレジットカード決済に失敗したので確認して下さい」などのメッセージと共にフィッシングサイトのURLを送信する。宿泊予約者がそのサイトにアクセスしてカード情報を入力すると、カード情報が窃取される。

被害を防ぐには、宿泊施設の管理者画面に多要素認証の導入が有効だが、設定していても安全とは言えない。多要素認証を突破する手口としては、攻撃者がBooking.comなどのプラットフォーム事業者を装って管理者をメールなどでフィッシングサイトに誘導し、入力させた認証情報をリアルタイムで正規の管理画面に入力して不正にログインする中間者攻撃（Man In the Browser攻撃）」が考えられる（図1-14）。

▼図1-14　中間者攻撃




また、メールを利用したフィッシング攻撃などで管理者のPCにマルウェアがインストールされると、バックドアによる遠隔操作が可能になる場合がある。その結果、攻撃者が管理者のPCを遠隔で操作し、多要素認証時に管理者にメールで送られるアクセスコードやワンタイムパスワードを窃取して、不正ログインされる可能性がある。多要素認証を設定する場合、ID・パスワードを入力するPCとは独立したスマートフォンなどのデバイスでアクセスコードやワンタイムパスワードを取得する必要がある。

旅行予約サイトに限らず、利用者向けにメッセージ機能を提供するECプラットフォームなどでも、同様の手口で管理画面がフィッシングの踏み台となる可能性が考えられる。管理画面に多要素認証を設定し、２要素目の認証要素はID・パスワードを入力するPCと別のデバイスで取得すること、また管理用に使用するPCがマルウェアなどに感染しないよう、メールのURLを不用意に開かないといったフィッシング対策や、マルウェア検知・EDRなどのソフトウェアのインストールといった基本的な対策が重要である。

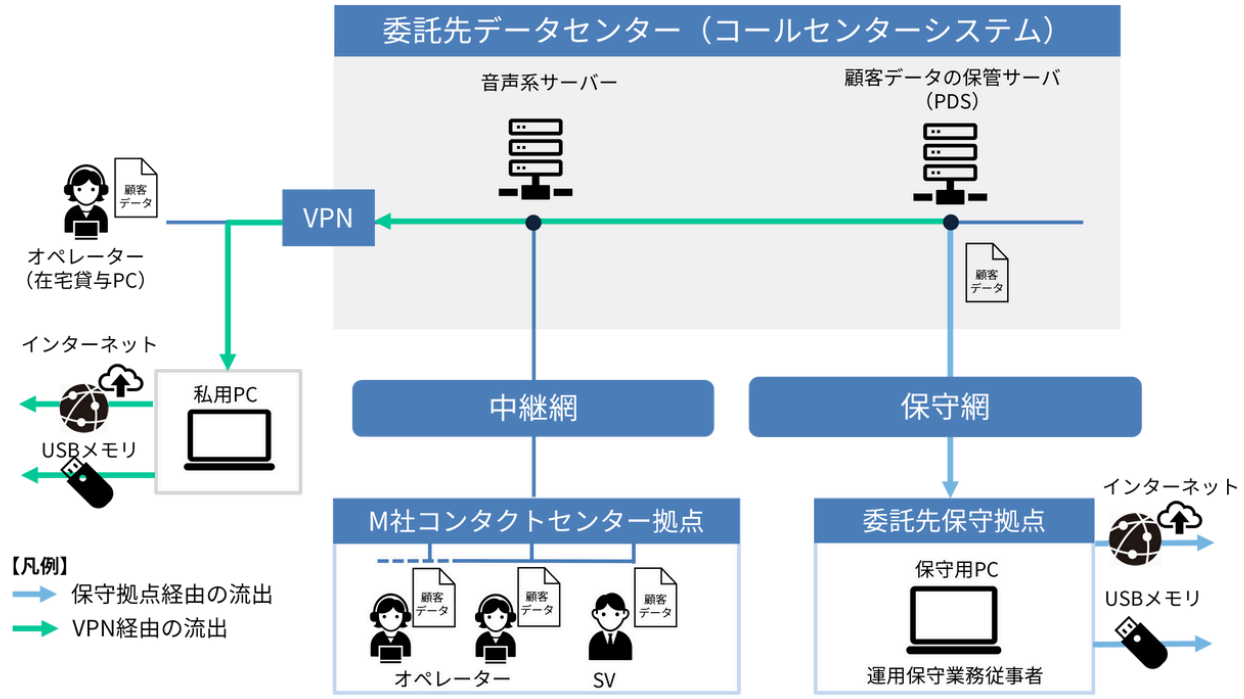
なお、この手口によるカード情報の流出については、直接原因がカード会員を対象にしたフィッシング詐欺によるものであることから、1.のカード情報流出事件の統計には含めていない。

### (3)-2. コールセンター業務委託先における不正持ち出し

2023年10月、コールセンター業務を受託するM社が、コールセンターシステムの運用保守委託先の派遣社員が顧客データを不正に持ち出し、第三者に転売していたことを公表した。流出した個人情報は、69の企業・自治体から取扱を委託された約928万人分に上る。うち、クレジットカード情報を含むのは2社分・81件と公表されている。流出期間は2013年7月頃から2023年2月頃までの約10年間に及び、持ち出された情報は名簿業者に売却されている。

2024年2月に公表された社内調査委員会の調査報告書（以下『調査報告書』）によれば、当該派遣社員は顧客情報保存サーバーの運用保守にあたっており、システム管理者アカウントの使用が許可されていた。当該派遣社員は、貸与されていた保守用PC、もしくは私有PCを使用して、保守拠点（運用保守委託先の企業）もしくはVPN経由でサーバーにアクセスし、個人情報をダウンロードしてUSBメモリーに保存する、もしくはWebメールに添付して外部に送信する方法で持ち出していたと推測されている（図1-15）。

▼図1-15 情報持ち出しの経路




出所：『調査報告書』（NTT西日本グループ 社内調査委員会）を参考に作成

『調査報告書』では、サーバーからの顧客データのダウンロード制限、USBメモリーなどの外部記録媒体への書き出し禁止、保守用PCのインターネット接続禁止、ログ監視、私有PCのネットワーク接続禁止といった基本的なセキュリティ対策がされていなかったことが「内部不正による情報漏洩リスクに対し極めて脆弱」と評価されている。

本件に起因したカード情報流出を公表したECサイトは３サイト（うち2サイトは同一企業が運営）であり、カード情報流出件数の合計は81件であった。

『ガイドライン5.0』では、カード情報を取り扱う業務を外部委託する場合、委託者自身が委託先のセキュリティ状況を確認し、責任を持ってPCI DSS準拠などの対策を求めることを要求している。本件のような内部不正を防止するための対策としては、最小特権の原則（アクセス権限は職務遂行に必要な最小限とする）や、監査ログの定期的なレビューなどのPCI DSSの要件を適用することが有効である。カード情報の取り扱いを外部に委託する場合は、PCI DSS準拠状況を確認し、準拠していない場合は委託先に要請する必要がある。

# 2. 2023年のECサイトにおける不正利用の概況

2023年のEC市場は、前年比9.91%増の22.7兆円（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、クレジットカードなど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。

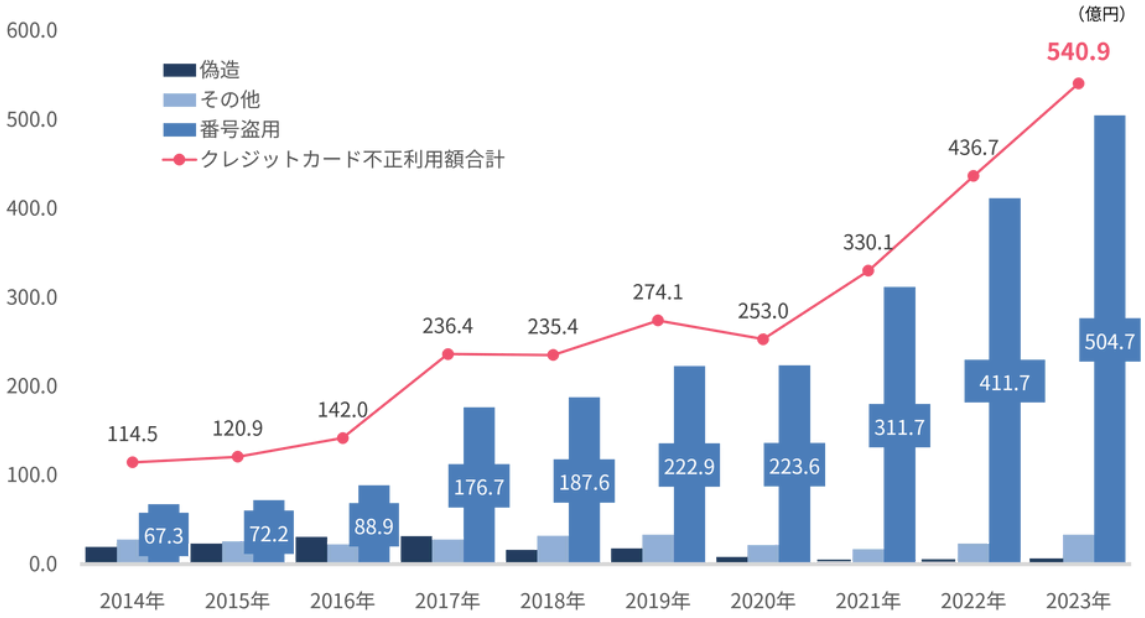
その中でもCaccoの契約先事業者から特に多くの相談が寄せられているのが、カードの不正利用（他人のカード情報を用い、カード保有者になりすまして決済する行為）と転売不正（転売を目的として、初回限定価格など注文に条件がある商品や数量限定販売の商品などを不正に購入する行為）である。本レポートでは、カード不正利用被害の概況について述べた後、これらの不正について、Caccoが提供する不正検知サービス「O-PLUX」導入ECサイト（累計11万サイト）のデータを元に詳しく紹介していく。

## (1)クレジットカード不正利用被害額の推移

### (1)-1. 2023年のクレジットカード不正利用額と傾向

2023年の年間クレジットカード不正利用被害額は、540.9億円で前年比23.9%の増加となった。2018年から増加傾向が続いているが、とりわけ2021年以降は毎年100億円以上の増加となり被害が拡大している。内訳としては、「番号盗用」が504.7億円で全体の93.3%を占めている（図2-1）。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の発生状況』（日本クレジット協会）

### (1)-2 . クレジットカード不正利用被害増加の要因

不正利用されるカード情報は、ECサイト等から流出したものに限らない。フィッシングによるカード情報の窃取や、カード番号の規則性に従って有効なカード番号を機械的に生成するクレジットマスター など、ECサイトからのカード情報流出以外で入手したカード情報の不正利用が増加していることが、被害増加の要因となっていると考えられる。

カード情報の流出に加え、2023年はECサイトのアカウント乗っ取り（図2-2）による不正被害が増加した。会員制のECサイトでは消費者の利便性のため、アカウント情報にカード情報を紐づけているケースが多い。そのため、アカウント乗っ取りに成功した攻撃者はカード情報を入手することなくカード不正利用ができる。

▼図2-2　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」導入ECサイト（累計11万サイト）を対象に、O-PLUXの審査で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。

2023年のカード不正利用の発生率は1.6%で前年同様であった。一方で、転売不正の発生率は5.7%と2022年に比べて2倍以上、2020年に比べると3年間で4倍以上に増加していた（図2-3）。転売不正の内容としては、2022年までと同様、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2-3 カード不正利用発生率および転売不正発生率

| 年 | 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% |

| 年 | 転売不正発生率 |
|---|---|
| 2020年 | 1.3% |
| 2021年 | 1.4% |
| 2022年 | 2.5% |
| 2023年 | 5.7% |

Caccoによる
※「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。
（クレジットカード不正注文には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）
※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。

『ガイドライン5.0』では、不正利用のリスクが高い「高リスク商材」として、デジタルコンテンツ・家電・電子マネー・チケット・宿泊予約サービスを挙げている。そのうちデジタルコンテンツ、チケット、家電は「O-PLUX」が検知した不正注文件数においても上位であった。他に、比較的低単価のコスメ・ヘアケアや健康食品・医薬品が、3年連続して上位となっている（図2-4）。

▼図2-4 商材別不正注文検知件数ランキング

| 順位 | 2020年 | 2021年 | 2022年 | 2023年 |
|---|---|---|---|---|
| 1 | MVNO | ホビー・ゲーム | デジタルコンテンツ | デジタルコンテンツ |
| 2 | ホビー・ゲーム | デジタルコンテンツ | ホビー・ゲーム | ホビー・ゲーム |
| 3 | コスメ・ヘアケア | チケット | 旅行 | チケット |
| 4 | アパレル | 健康食品・医薬品 | コンタクト・メガネ | コスメ・ヘアケア |
| 5 | 家電・PC・タブレット | コスメ・ヘアケア | チケット | 健康食品・医薬品 |
| 6 | EC総合通販 | コンタクト・メガネ | 健康食品・医薬品 | コンタクト・メガネ |
| 7 | ベビー用品 | 食品・飲料・酒類 | コスメ・ヘアケア | 家電・PC・タブレット |
| 8 | テレビ総合通販 | 美容機器 | 食品・飲料・酒類 | サブスクサービス |
| 9 | アウトドア | MVNO | EC総合通販 | 食品・飲料・酒類 |
| 10 | サブスクサービス | 家電・PC・タブレット | 家電・PC・タブレット | 工具 |
| 11 | ペット用品 | EC総合通販 | アパレル | スポーツ用品 |
| 12 | カメラ・映像機器・音響機器 | 工具 | 家具 | 日用品・雑貨・キッチン用品 |

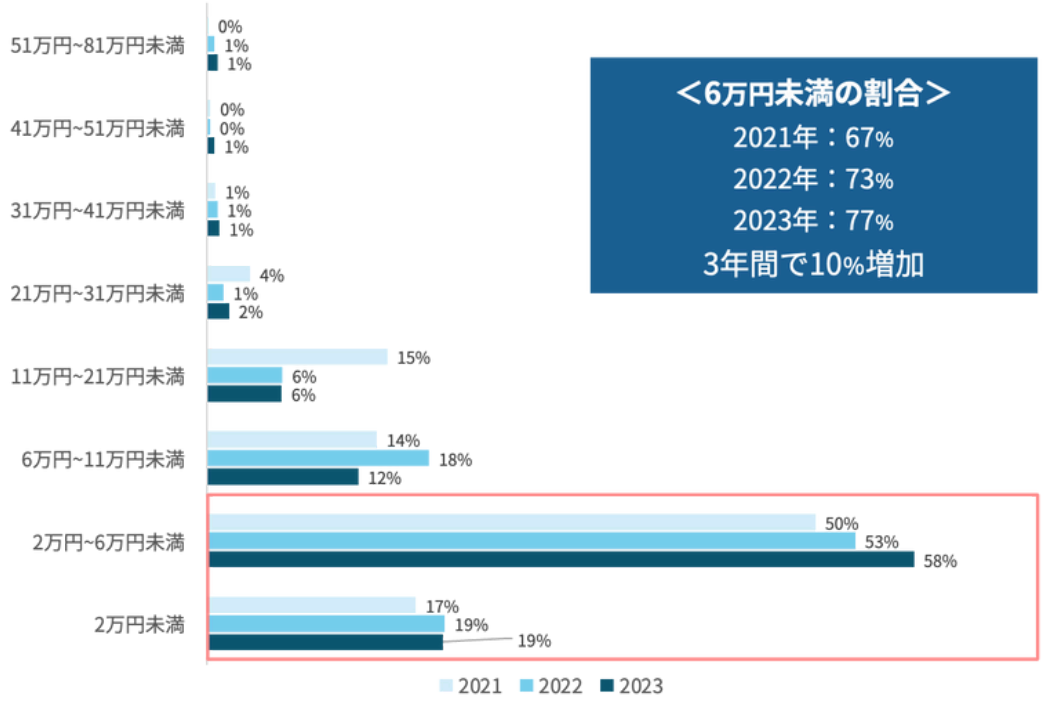
Caccoによる
※「O-PLUX」の審査で、審査件数全体に占める審査結果NGの割合を件数ベースで商材ごとに算出。 NGの割合が多い順にランキング
※最終的に出荷停止や注文を拒否するなどの対応は、「O-PLUX」加盟店判断により異なる。

## (2)-2. カード不正利用における注文金額の低額化

2023年の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。2021年には不正注文のうち注文金額が11万円を越えるものが20%、6万円未満のものが67%を占めていた。2023年には11万円を越えるものが11%、6万円未満のものが77%となっている（図2-5）。

低額化の理由の一つとしては、不正利用を発覚しにくくすることを狙ったと考えられる。さらに、前述の「クレジットマスター」による試行は、金額が少額でもカードの有効性さえ確認できれば良いため、その増加も影響していると推測できる。

▼図2-5 カード不正注文金額の分布



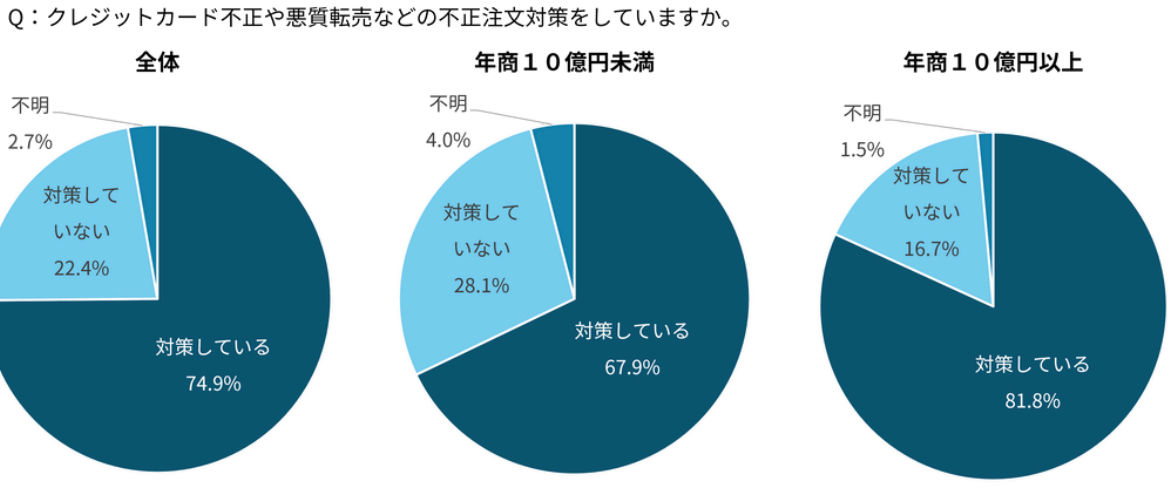

Caccoによる
※「O-PLUX」の審査で、クレジットカード不正対策におけるNG金額の分布から集計
（審査対象にはブランドデビットカード・ブランドプリペイドカードを含む）

## (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事業者の不正利用および不正注文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。2023年11月は、EC事業者549名の不正対策に関わる担当者を対象にセキュリティ意識や対策の実態について調査した。

全体で見ると74.9%が不正対策を行っている。年商別では、年商10億円未満のEC事業者の対策実施率は67.9%にとどまる一方、年商10億円以上は81.8%が対策をしており、年商規模が大きいほど対策している割合が高い傾向にあった（図2-6）。

▼図2-6 EC事業者の不正対策状況

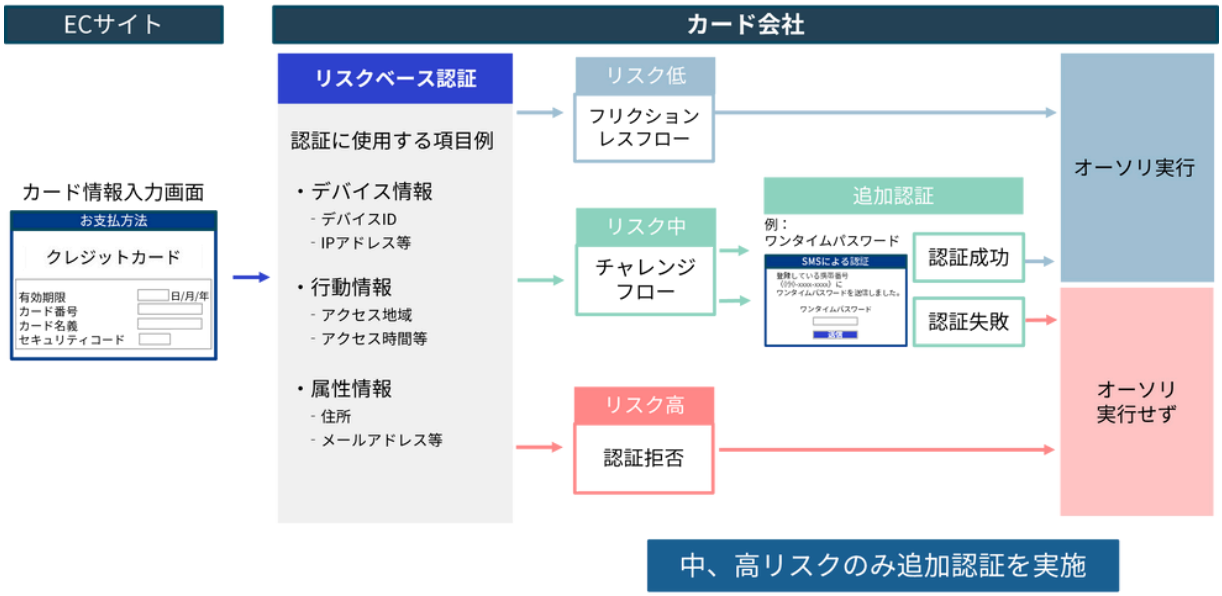



出所：『EC事業者実態調査』（Cacco）

EC事業者の不正利用対策として、『ガイドライン5.0』では、①本人認証 ②券面認証（セキュリティコード ③属性・行動分析（不正検知サービス） ④配送先確認　の４つを指針対策として定め、リスクや不正利用被害状況に応じて導入を求めている。中でも、国際ブランドが推奨する本人認証サービスであるEMV 3-Dセキュア（以下EMV3-DS）については、原則すべてのECサイトに対し2025年3月末までに導入を求めている。

EMV3-DSは、決済時に取引がカード会員本人によるものかどうかの確からしさを、イシュア（カード発行会社）に送信した利用者の情報などを活用してリスクを判定する（リスクベース認証）。リスクが低いと判定された取引については追加の認証を求めない「フリクションレスフロー」が適用されるため、3Dセキュア1.0の普及を妨げる一因となっていた「かご落ち」の懸念は軽減される。リスクが一定以上と判定された取引は、自動で取引を拒否したり、追加の認証を求める「チャレンジフロー」を適用することで安全性を高めている（図2-7）。

▼図2-7 EMV 3-Dセキュア



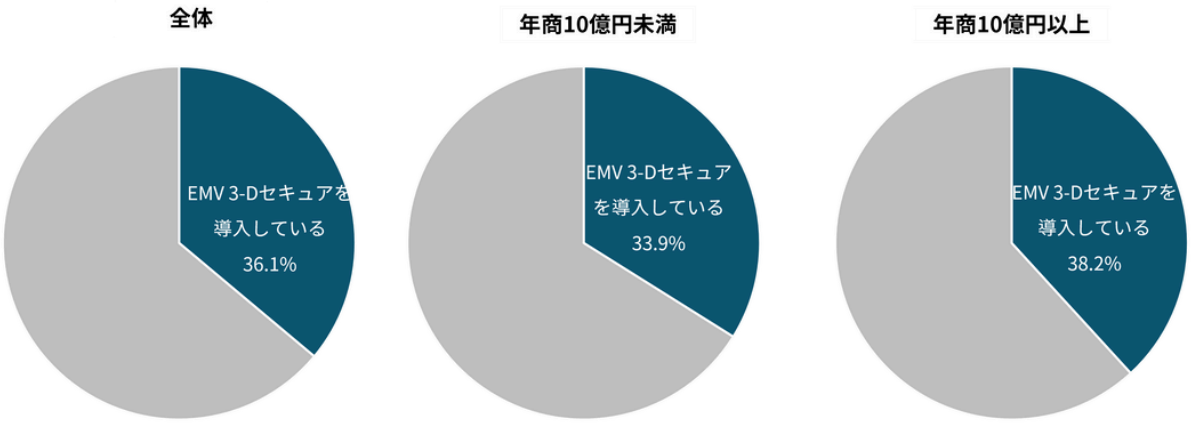

出所：『クレジットカード・セキュリティガイドライン』（日本クレジット協会）を参考に作成

「EC事業者実態調査」によれば、2023年11月の時点でEMV3-DSを導入しているECサイトの割合は、全体の36.1%にとどまっているものの、2022年の28.9%と比較すると導入が進んでいる。内訳を年商別でみると、年商10億円以上では38.2%に対し年商10億円未満では4.3ポイント低い33.9%だった（図2-8）。

EMV3-DSを導入しない理由として最も多く挙げられたのは、「導入コストが高い」であった。3Dセキュア1.0は無償で利用できたが、EMV3-DSは原則有料になることが導入を妨げる要因となっていると考えられる（図2-9）。

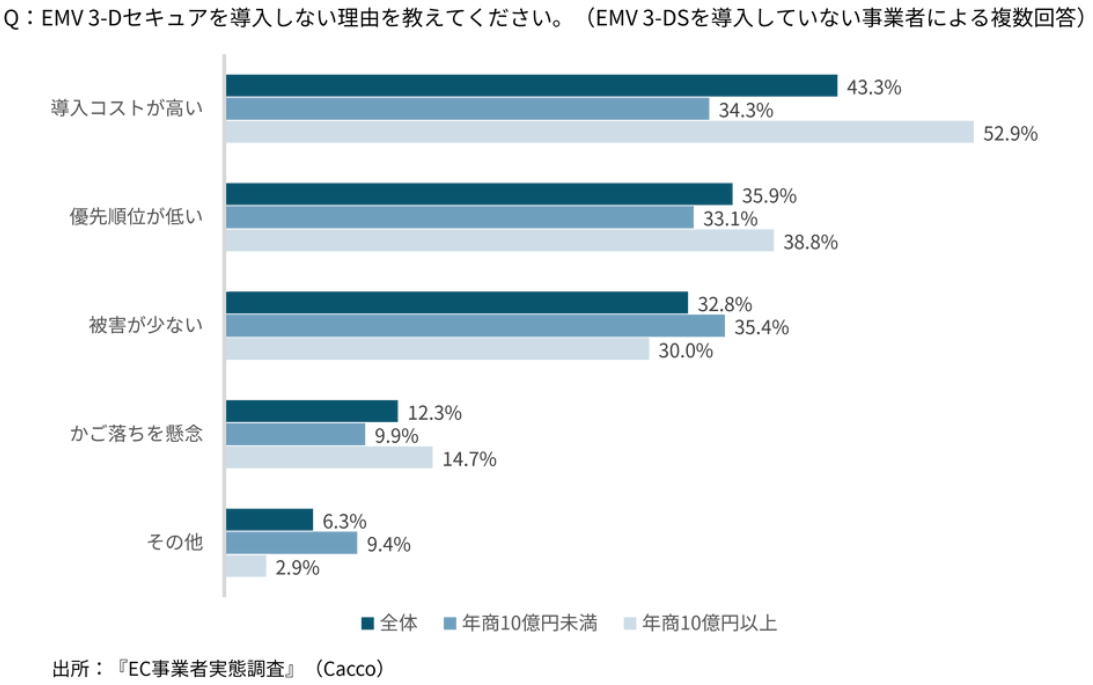
▼図2-8 EMV 3-Dセキュアの導入率

Q：EC決済における本人認証手法である「EMV 3-Dセキュア」を導入していますか。




出所：『EC事業者実態調査』（Cacco）

▼図2-9 EMV 3-Dセキュアを導入しない理由




出所：『EC事業者実態調査』（Cacco）

## (3)2023年のECサイトにおける不正利用のトピック

ECサイトでの決済時に他人のカード番号を入力して換金性の高い商品を購入する以外の方法で、カード情報を不正利用する手法がある。本レポートでは、コード決済を利用した不正利用および不正トラベルを取り上げる。

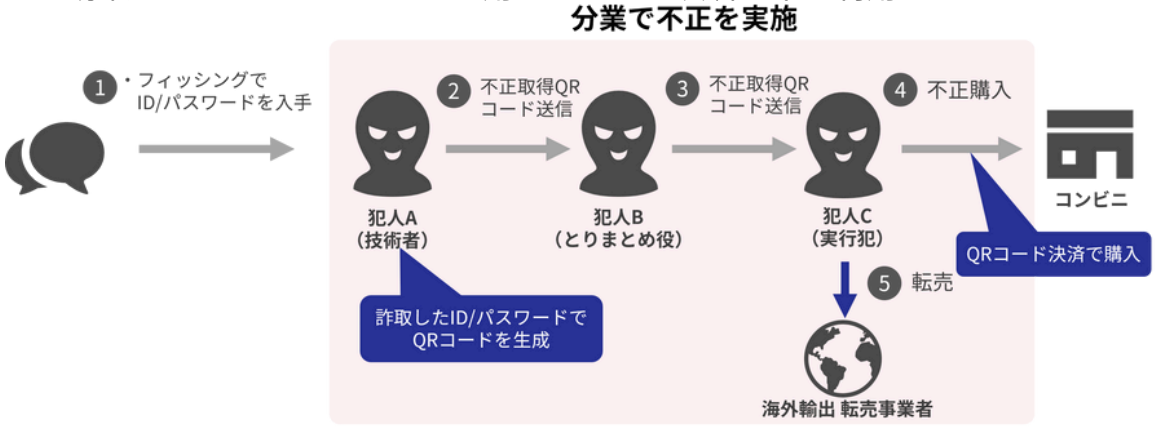
### (3)-1. コード決済を悪用した不正利用

スマートフォンのアプリで生成したバーコードやQRコードをかざすだけで決済ができるコード決済の決済額は、2023年には10.9兆円に達し、利用が急速に拡大している。一方で、コード決済利用者になりすました不正利用も発生している。支払い方法としてクレジットカードが紐づけられていた場合、クレジットカードが不正利用されることになる。

不正の手口は分業化が進んでいる（図2-10）。まず、「技術者」が収集したコード決済サービスのIDやパスワードを使用して、決済用のQRコードを生成する。「とりまとめ役」は、「技術者」が生成したQRコードを不正購入の「実行犯」に共有する。「実行犯」はそのQRコードを用いてタバコやプリペイドカードなどの換金性の高い商品を不正購入し、転売して現金化する。「実行犯」はSNSなどで募集されたアルバイトであり、不正の意識が希薄なことも多い。

また、コード決済を悪用した返金詐欺も確認されている。犯人はSNS広告などで偽のECサイトに消費者を誘導する。そのサイトで購入した消費者が、商品が届かないと事業者（実際には犯人）に問い合わせると、在庫の欠品などを理由に返金対応を提案され、返金のためのコード決済アプリの操作を指示される。指示通りに操作すると犯人に送金される。なお、このようなケースは被害者本人が送金しているため、補償対象にならないことにも注意したい。2023年9月には、国民生活センターがこの手口について注意喚起 を行っている。

▼図2-10　窃取したID・パスワードを悪用したコード決済の不正利用




| 想定される被害 | |
|---|---|
| 不正取得された ID/パスワードのアカウント保持者 | カード不正利用 |
| 販売事業者 | アカウントの不正利用における正規アカウントへの代金補填。不正に悪用されることでのブランディング棄損につながる。 |

### (3)-2. 不正トラベル

2023年5月、WHO（世界保健機関）が新型コロナウイルスの感染拡大を受けて出していた「国際的に懸念される公衆衛生上の緊急事態」の終了を発表した。ほとんどの国や地域で出入国制限が撤廃され、海外旅行がコロナ禍前と同様に行えるようになったことで、訪日外国人の数が急増した。国内でも、新型コロナウイルス感染症が感染症法上の5類に移行した。旅行に関する制度上の制約はなくなり、政府や自治体による旅行支援策もあって、国内旅行者の数も増えている。

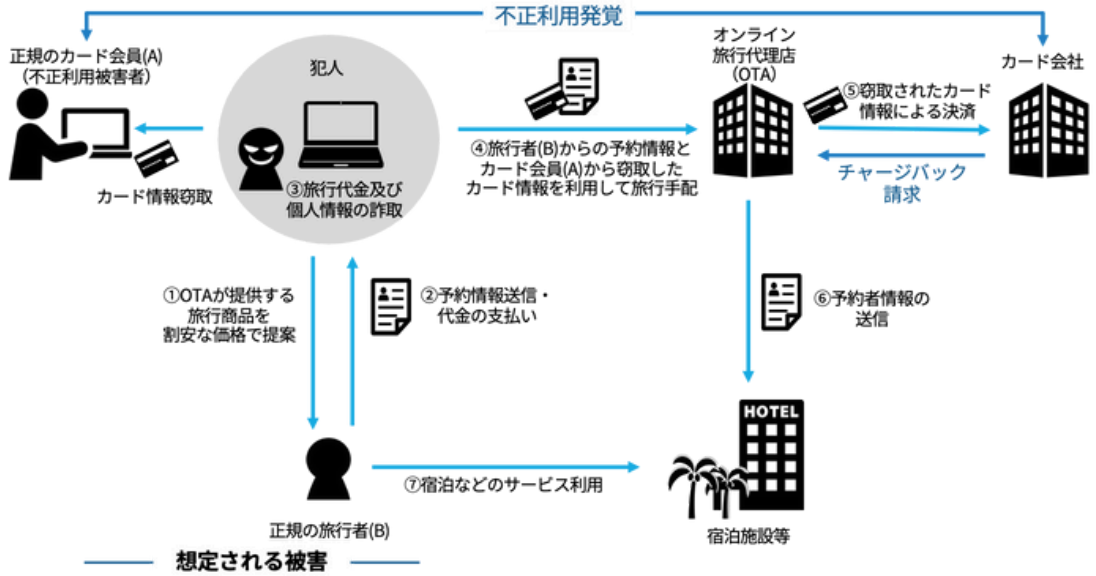
2017年頃から2019年頃にかけ、「不正トラベル」と呼ばれる、宿泊施設や航空券の販売など旅行関連サービスを狙った不正行為が多発し、2019年には日本サイバー犯罪対策センター（JC3）が注意喚起を行った。2020年以降はコロナ禍による旅行需要の低迷で不正トラベルの被害も減少していたが、2023年以降の旅行者急増に伴い再び増加の兆しがあり、Caccoの契約先事業者からも多くの相談が寄せられている。

不正トラベルの具体的な手口は以下となる（図2-11）。

① 犯人は旅行代理店が販売する旅行商品を、偽の予約サイトやSNSなどを通じて正規価格よりも安く販売する。
② 正規の旅行者（B）が申し込み、個人情報を入力して旅行代金を支払う。
③ 犯人は旅行者が支払った旅行代金を詐取する。
④ 犯人は旅行者の個人情報を用いて、旅行代理店に旅行を申し込み、あらかじめ入手していた他人（A）のカード情報で決済する。
⑤ 旅行代理店は不正利用されたカード情報によりカード会社から決済承認をもらう。
⑥ 旅行代理店は宿泊施設などに予約者情報を送信する。
⑦ 旅行者（B）は宿泊などのサービスを利用する。
⑧ 後日カードの不正利用が発覚し、旅行代理店はチャージバックを受ける。

犯人は旅行者が支払った旅行代金を詐取できる。 加えて旅行者の個人情報が犯人の手に渡ることで、個人情報の流出や悪用などの二次被害が想定される。一方で、被害を受けた旅行代理店が正規の旅行者に対して料金を請求することは、法的に困難であると考えられる。

▼図2-11 不正トラベル




**想定される被害**

| | |
|---|---|
| 正規のカード会員(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

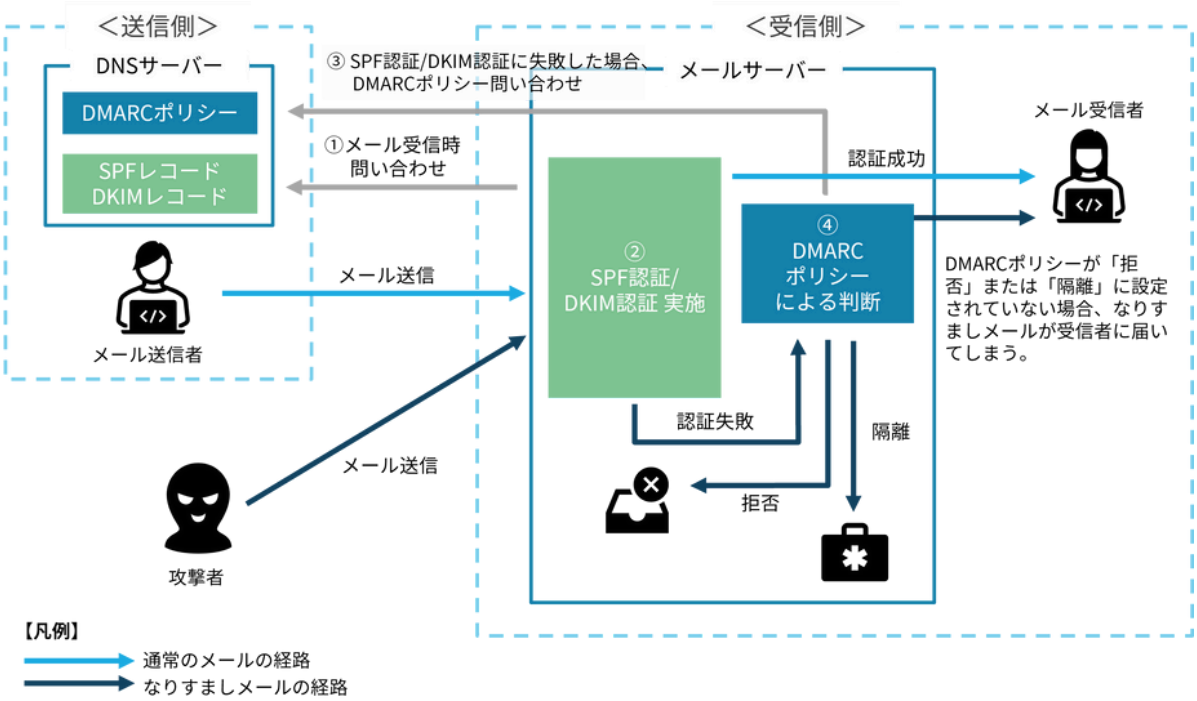
## (4)イシュア（カード発行会社）における送信ドメイン認証（DMARC）導入状況

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、メールの取り扱いを指定する「DMARCポリシー」をテキストレコー

ド（DMARCレコード）に記述する。DMARCポリシーには、「何もしない（none）」「隔離（quarantine）」「拒否（reject）」のいずれかを選択する。

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DMARC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2-12）。

▼図2-12　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コンサルティングが実施）

以下、調査の概要と、2023年9月末、2023年12月末、2024年3月末の調査結果を紹介する。

■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。

＜調査実施時期＞

2023年9月末・2023年12月末・2024年3月末

■調査結果

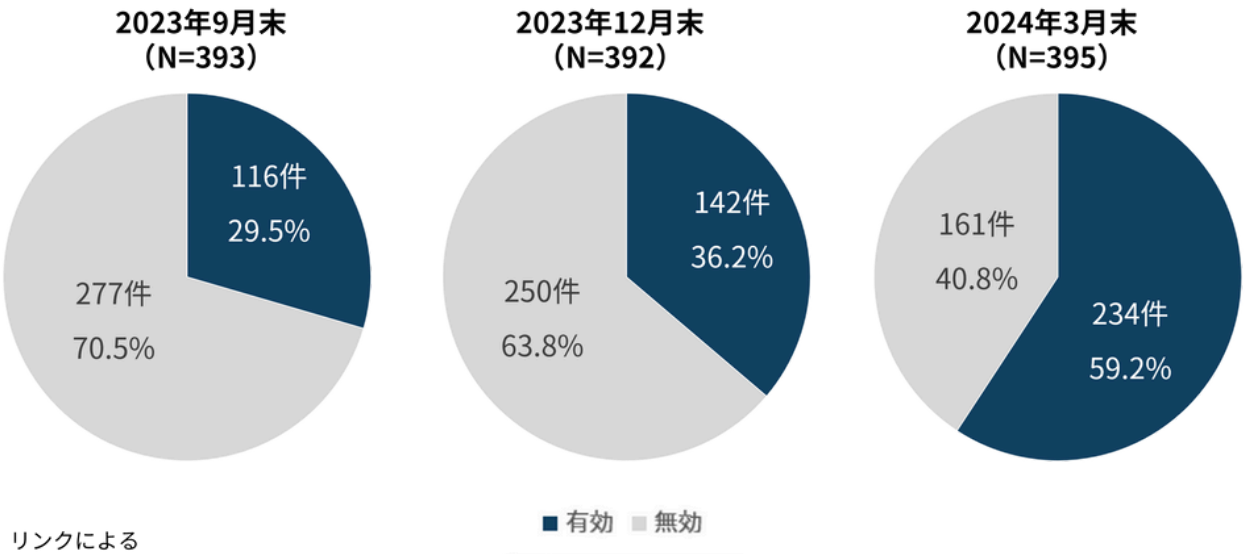
**1. 調査対象イシュアと対象ドメインの数**

| | 2023年9月末 | 2023年12月末 | 2024年3月末 |
|---|---|---|---|
| 調査対象社数 | 246社 | 245社 | 246社 |
| 対象ドメイン数 | 393ドメイン | 392ドメイン | 395ドメイン |

**2. ドメインごとのDMARCレコード設定状況**

2023年9月末にはイシュアで利用されているドメイン393件のうち116（29.5%）件、2023年12月末は392件中142件（36.2%）でDMARCレコードが存在した。2024年3月末はドメイン395件中234件（59.2%）と大幅に上昇した（図2-13）。

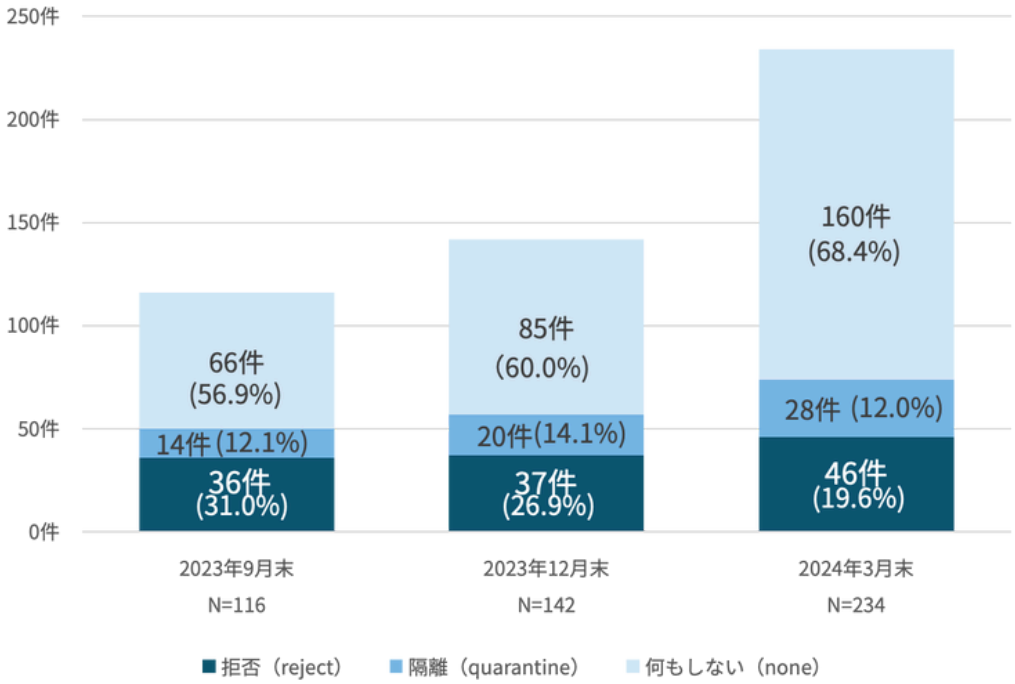
▼図2-13 ドメインごとのDMARC設定率




リンクによる
※2023年12月までのデータはｆｊコンサルティングによる

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、2023年9月末には36件、2023年12月末には37件、2024年3月末には46件と徐々に増加している。「隔離（quarantine）」に設定しているドメインについても、2023年9月末には14件、2023年12月末には20件、2024年3月末には28件と同様に増加している。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は2023年12月末の85件から2024年3月末には2倍弱の160件と大きく増加した。理由は、新規にDMARCを設定するドメインはポリシーをnoneに設定することが多いためと考えられる。その結果、「拒否（reject）」「隔離（quarantine）」に設定しているドメインの割合は2023年9月末から徐々に下がっている（図2-14）。

▼図2-14　イシュアのメール送信元ドメインのDMARC設定状況




リンクによる
※2023年12月までのデータはｆｊコンサルティングによる

### 3. 会社ごとのDMARC対応状況

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カテゴリーに分類した

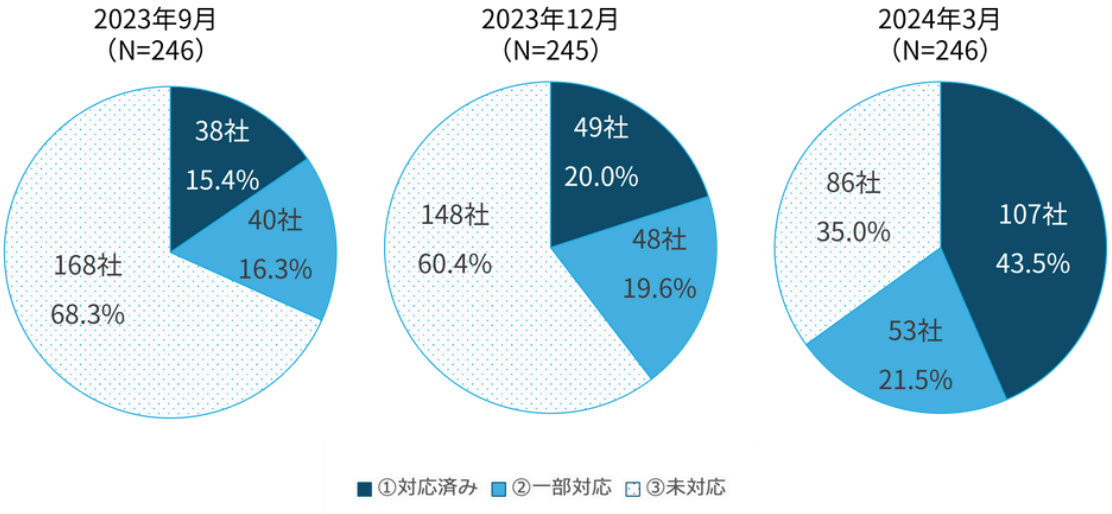
①対応済み：メール送信元として使用しているドメイン全てにDMARCレコードが設定されている。

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。

2023年9月は、①対応済みと②一部対応をあわせて246社中78社（31.7%）と、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月は合わせて160社（65.0%）となっている。うち、107社（43.5%）は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（図2-15）。

▼図2-15　イシュアにおけるDMARC対応状況




リンクによる
※2023年12月までのデータはｆｊコンサルティングによる

### 4. 総括

2023年10月にGoogleのメール送信者ガイドラインがアップデートされ、2024年2月以降、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はDMARC対応が必須とされた。言い換えると、1日5,000通以上のメールをGmailに配信している事業者は、DMARCに対応しない場合Gmailのユーザーにメールが不達となる可能性があるということである。これを受け、DMARC導入に着手する企業が増えている。

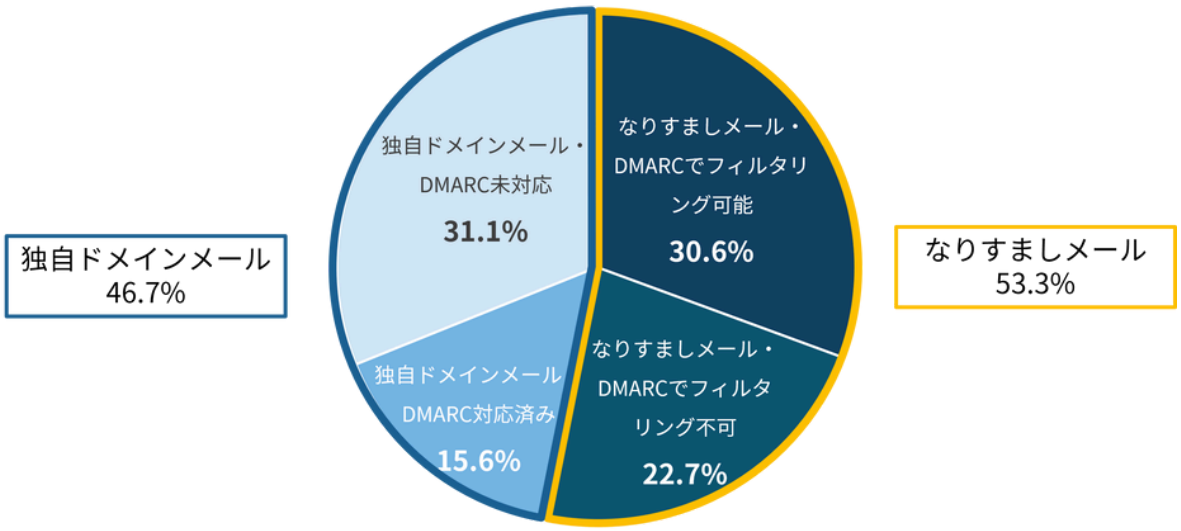
日経225企業を対象としたTwoFive社の調査によれば、2023年12月末時点でメール送信元に使用しているドメインのうち少なくとも1つでDMARCを導入している企業（図2-15の①対応済み②一部対応の合計に相当）の割合は70.7%であったが、2024年2月末には85.8%、2024年5月末には91.6%とこちらも大きく増加している。

イシュアのDMARC導入率も着実に底上げされてはいるが、監督官庁の要望が出されているにもかかわらず、他業界に比べると低い割合（65.0%）にとどまっているといえる。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、フィッシングメール対策として実効性を持たせるために以下の対応が求められる。

#### ① DMARCポリシーを適切に設定すること

フィッシングメールには、第三者が実在するドメインを騙って送信するメールと、第三者が実在するドメインと紛らわしい独自ドメインを使用して送信し、受信者の誤解を誘うメールがある。フィッシング対策協議会では、前者を「なりすましメール」、後者を「独自ドメインメール」として、その割合を調査している。『フィッシング報告状況（2024年6月）』によれば、調査用のメールアドレスにとどいたフィッシングメールのうち、送信元ドメインのDMARCポリシーが「拒否（reject）」もしくは「隔離（quarantine）」に設定されており、フィルタリングが可能な「なりすましメール」の割合は約30.6%と増加傾向にある。一方で、DMARCポリシーが「何もしない（none）」に設定されているか、もしくはDMARCが設定されておらず、フィルタリングができない「なりすましメール」の割合」は22.7%であった。なお、15.6%はDMARCに対応した上で「独自ドメインメール」により、フィッシングメールが送信されている。攻撃者側もメールの到達率を上げるためにGoogleのメール送信者ガイドライン改訂に対応していることが伺える（図2-16）。

▼図2-16 フィッシングメールにおけるDMARC設定状況




なりすましメール　：第三者が実在する他社のドメインを騙って送信するメール
独自ドメインメール：第三者が実在する他社のドメインと紛らわしい独自ドメインを使用し、受信者の誤解を誘うメール

出所：『フィッシング報告状況』（フィッシング対策協議会）を参考に作成

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。しかし、DMARCによるフィッシング対策の実効性を高めるためには導入するだけでなく、適切なポリシーで運用することが必要となる。

フィッシング対策協議会は、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、正規メールとフィッシング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。

**② 委託先企業のドメインに対してもDMARC設定を求めること**

イシュアの中にはWeb明細サービスやワンタイムパスワードサービス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。これらの外部委託先ドメインの中には、DMARCレコードが設定されていないドメインも存在する。イシュアは自社のフィッシング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。

**③ カード会員への継続的な啓発活動**

イシュアを騙るフィッシングメールには、紛らわしいドメインを送信元のドメインやフィッシングサイトのドメインとして使用し、気づかない消費者から情報を窃取する手口も多くある。図2-15 で示したように、フィッシングメールのうち46.7%は「実在のドメインと紛らわしい独自ドメイン」によるものである。正規のドメイン所有者が自社ドメインのDMARCポリシーを「拒否（reject）」もしくは「隔離（quarantine）」に設定していても、自社ドメインと異なる独自ドメインを使用しているメールの到達を防ぐ効果は無い。その結果、実在のドメインと紛らわしい独自ドメインを使用したフィッシングメールは、消費者に届いてしまう。フィッシングの被害を防ぐためには、メールの送信元のドメインをよく確認することや、メールに記載されたリンクを直接クリックせずに検索サイトやブックマークを使用することなど、カード会員への継続的な啓発も欠かせない。

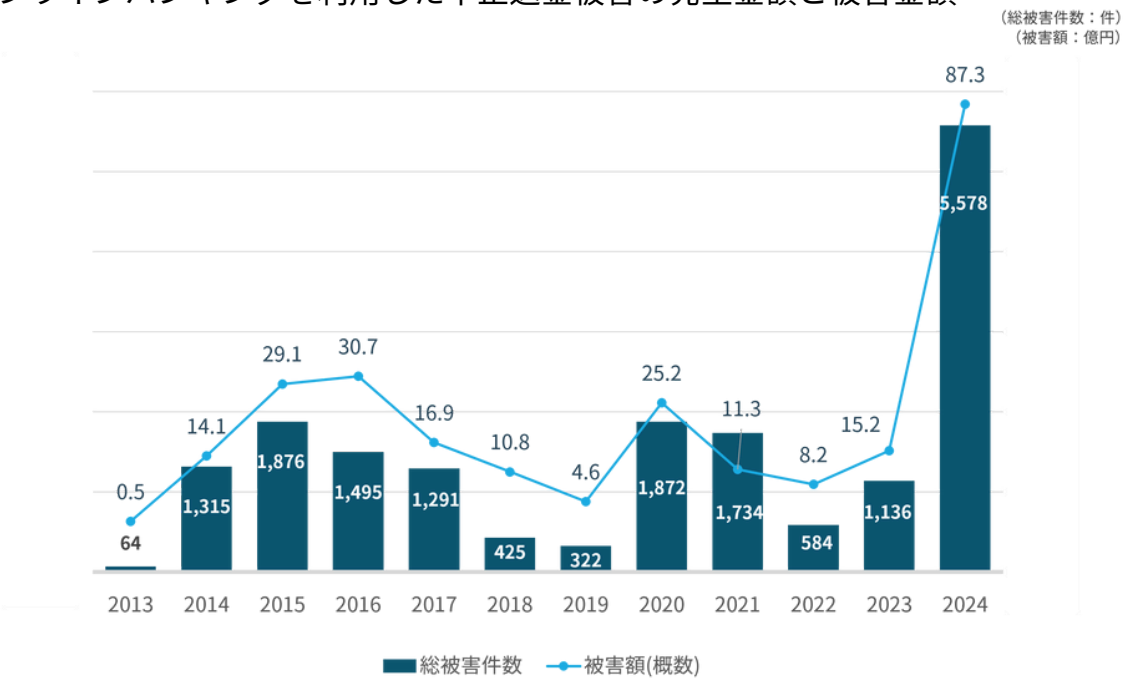
# 3. オンラインバンキングを利用した不正送金の概況

オンラインバンキングを利用した不正送金被害が2023年以降急増している。2023年8月および12月、金融庁と警察庁は連名で『フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）』を発表した。以下、被害の概況と暗号資産を利用したマネーロンダリングの手口を解説する。

## (1)被害の概況

警察庁が公表している『令和５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』によれば、オンラインバンキングによる不正送金被害の発生件数は5,578件と前年比4.9倍、被害総額は約87.3億円と前年比5.7倍でいずれも過去最多となった（図3-1）。被害者のうち97.9%が個人である。

▼図3-1 オンラインバンキングを利用した不正送金被害の発生金額と被害金額




出所：『令和5年におけるサイバー空間をめぐる脅威の情勢などについて』（警察庁）

## (2)分業が進む不正送金犯罪

不正送金の実行犯は、それぞれが不正送金プロセスの一部を担っており、SNSなどで、ゆるく繋がって1つの組織のように活動している。図3-2は、日本国内をターゲットとした一般的な不正送金犯罪のプロセスと分業の一例である。それぞれの役割を持つ者は隣接する工程の者とは繋がりがあるが、全体像は把握していない。

▼図3-2 不正送金犯罪のプロセスと分業される役割

上流

| 犯罪のプロセス | 名称 | 役割 |
|---|---|---|
| 研究・ツール化 | ①フィッシングキット作成者 | フィッシングサイトを作成するためのキット（ソフトウェア）を作成する。 |
| | ②フィッシングサイト作成者 | 日本のインターネットバンキング、送金サービスの詳細を把握し、フィッシングサイトを作成する。 |
| ばら撒き | ③配布役 | 「作成」又は「購入」したフィッシングサイトのURLへ誘導するために、日本に向けてSMSやメールをばら撒く。 |
| 送金準備 | ④不正口座作成者 | 窃取された日本人の個人情報、身分証データを利用するなどして、偽造身分証を作成の上、その偽造身分証で銀行口座を作成する。 |
| 送金実行 | ⑤実行役（指示役も兼ねる場合有り） | 日本の被害者がフィッシングサイトで「ログインID、パスワード、ワンタイムパスワード」などを入力した場合、その情報を使用して、オンランバンキングに不正アクセスし、不正送金を行う。 |
| 現金化準備 | ⑥指示役 | 日本における出し子・買い子に対する指示を行う。 |
| | ⑦不正口座準備役 | 日本で不正送金の一次送金先となる銀行口座を買い集める。（帰国した外国人が以前作成した口座も悪用されている） |
| | ⑧出し子管理者 | 海外製SNSを使用し、「手軽にお金稼ぎしたい人は連絡をください。」などと「出し子・買い子」をリクルートし、指示役などに繋げる。 |
| 現金化 | ⑨買取業者 | 「買い子」が不正購入したゲーム機やタバコなどを換金する業者 |
| | ⑩資金回収者 | 「出し子・買い子・受け子」が集めた現金を回収し、報酬を支払うとともに、指示役に送金する。 |
| | ⑪出し子・買い子・受け子 | 出し子は、ATMから現金を引き出す者。買い子は、コンビニや電気店などで買い物をする者。受け子は、自宅や空き家などで荷物を受け取る者。海外製SNSや日本語学校などでリクルートされた者が多い。 |

下流

出所：『JC3コラム - 悪質な不正送金の実態』（日本サイバー犯罪対策センター（JC3））を参考に作成

①フィッシングキット作成者は、フィッシングサイトの構築を容易にするソフトウェアのテンプレートを作成し、ダークウェブなどで配布する。②フィッシングサイト作成者は、フィッシングキットを使用してフィッシングメールの誘導先となる偽サイトを作成する。

サイトが準備できたら③配布役が実際にフィッシングサイトのURLを記載したメールやSMSを送信する。送信先のリストはダークウェブなどで販売されているメールアドレスや電話番号であることが多い。これらはサイバー攻撃によって企業サイトから流出したデータや、別のフィッシングで窃取された個人情報である。

④は不正送金を集める口座である。日本人名義の偽名の口座を作成するために、窃取した個人情報や身分証データを利用して偽造身分証明書を作成し、銀行口座を作成する。⑤実行役は、フィッシングサイトで被害者が入力したID、パスワード、ワンタイムパスワードなどを使用してオンラインバンキングに不正アクセスし、不正送金を実行する。

上流工程の①から⑤までは技術レベルが高く、インターネット上の作業で完結しており、主に海外で活動していると考えられる。対して、⑥以下は日本国内において不正送金で得た資金の出所をわからなくする（マネーロンダリング）ために現金化するためのプロセスである。不正送金はまず複数の一次送金先に分散して送金されるが、送金先の口座は⑦の不正口座準備役が準備する。この口座はわざわざ偽造身分証明書を使って開設したりせず、他人の銀行口座を買い取り、準備する。帰国した外国人が以前に作成した口座が悪用されることも多い。

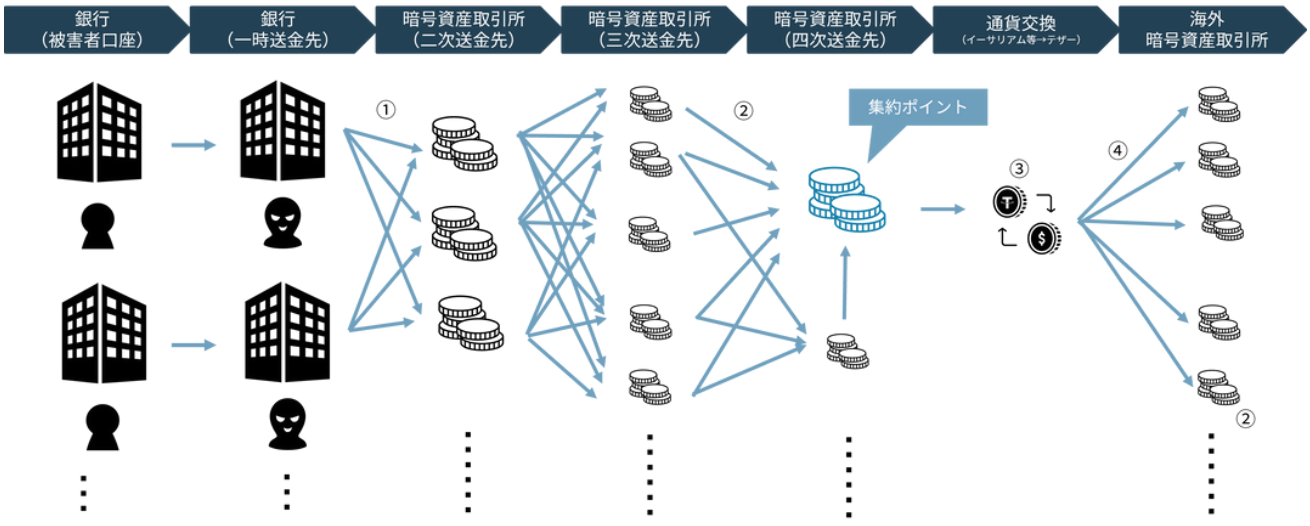
口座に入金された現金は⑪出し子がATMから引き出し、⑩資金回収者に渡す。⑩資金回収者は⑥指示役の指示に従い、④の口座に回収した現金を送金する。上流工程から見ると下流工程はいわば「トカゲの尻尾」的な存在であり、特に⑪出し子・買い子・受け子は逮捕されるリスクが高い。

## (3)暗号資産を利用したマネーロンダリング

オンラインバンキングを利用した不正送金の場合、近年はマネーロンダリングには暗号資産が使用されるケース増えている。暗号資産を使用する場合、図3-2の「現金化」のプロセスが不要となる。『令和５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』によれば、オンラインバンキングの不正送金被害額 約87.3億円のうち、51%の約44.2億円が暗号資産交換業者の金融機関口座に送金されている。

典型的な暗号資産を利用したマネーロンダリングでは、まず、複数ある一次送金先の口座から複数の暗号資産取引所に小分けにして送金を行い、暗号資産を購入する。さらにそこから複数の暗号資産取引所で別の暗号資産に交換することを何度も繰り返す。その際に、本人確認の必要がない海外の取引所を経由したり、匿名で保有できるマイナーなコインを利用することで資金の匿名性が高まる（図3-3）。

▼図3-3　暗号資産を利用したマネーロンダリングの例




お金の流れ(例)
① 一次送金先の銀行から複数の暗号資産取引所（海外含む）へ送金しイーサリアム等の仮想通貨を購入
② 複数の暗号資産取引所に分散して送金を繰り返し集約ポイントとなる取引所に集約
③ 集約ポイントの資金をテザー（法定通貨担保型ステーブルコインの一つ）に交換
④ 海外の暗号資産取引所へ送金

出所：『JC3コラム - 悪質な不正送金の実態』（日本サイバー犯罪対策センター（JC3））を参考に作成
※法定通貨担保型ステーブルコイン：米ドルなどの法定通貨を担保としており比較的価値が安定している暗号資産

# 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改訂

割賦販売法の求めるセキュリティ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【5.0版】』（以下『ガイドライン5.0』）が2024年3月に公開された。4.0版までの「クレジットカード情報保護対策分野」「不正利用対策分野」「消費者及び事業者への周知・啓発について」という3部構成が見直され、割賦販売法によりクレジットカード情報保護を義務付けられた対象事業者ごとに対面取引と非対面取引に分けて、カード情報保護対策と不正利用対策を示す構成へと変更された。また、本文には求められる対策や法令対応として求められる「指針対策」の基本的な考え方や概要を記載し、実装方法や仕様については附属文書に誘導するよう記載内容が整理され、附属文書が整備された。以下に主な改訂のポイントを示す。

### (1)-1. EMV 3-Dセキュアの導入ロードマップ

2-(2)-3で述べた通り、『ガイドライン5.0』では、原則すべてのECサイトに対し2025年3月末までにEMV 3-Dセキュア（以下EMV3-DS）の導入を求めている。クレジット取引セキュリティ対策協議会（以下協議会）は2023年11月に開催された割賦販売小委員会において、『イシュアーにおけるEMV 3-Dセキュア推進ロードマップ』『加盟店におけるEMV 3-Dセキュアの導入推進ロードマップ』を提示しており、『ガイドライン5.0』にも反映された。

イシュア（カード発行会社）に対しては、EMV3-DSの即時導入が求められる。これに関しては、2023年10月末の時点で95%のイシュアが導入済みである。加えて、2025年3月末までに、EMV3-DSの登録率を、ECサイトを利用するカード会員の80%に引き上げ、すべてのEMV3-DS登録会員に対してワンタイムパスワードの導入を求めることが明記された。現状でEMV3-DSの登録が進まないユーザーとしては法人カードやプリペイドカードの他、古いカード会員で携帯電話番号やメールアドレスなどワンタイムパスワードを受信する手段を登録していないケースなどが挙げられる。こうしたカード会員にもEMV3-DSの必要性を周知し、必要な情報の登録を促す必要がある。

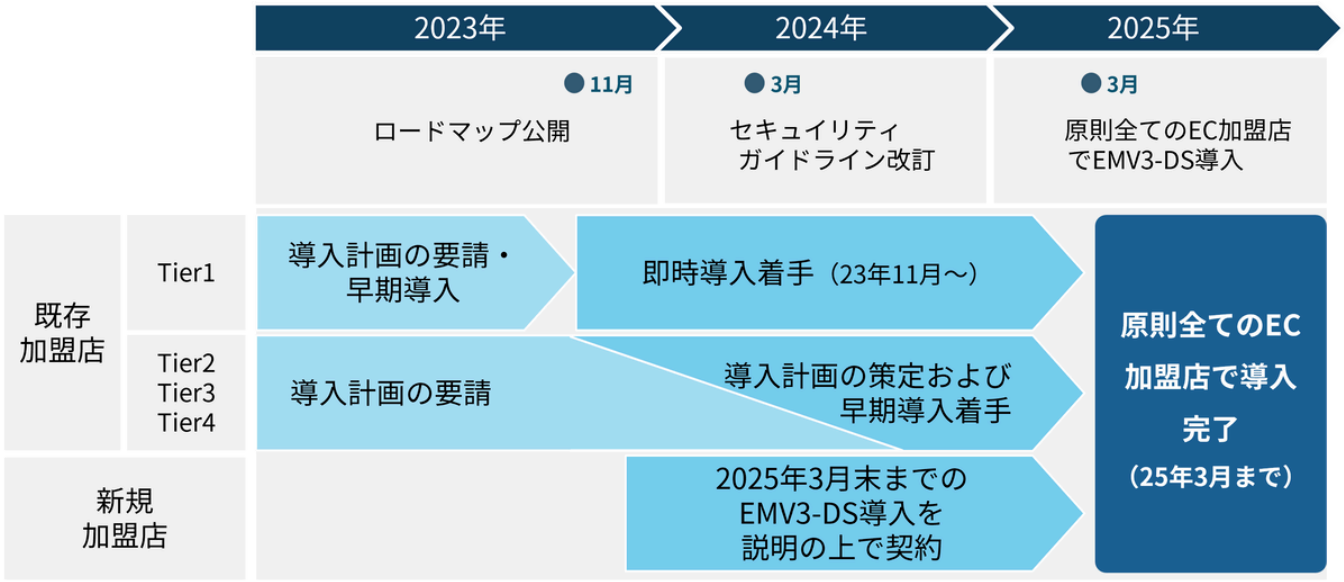
加盟店にはTier 1からTier 4までの優先順位をつけたロードマップが示された。Tier 1である「不正顕在化加盟店」(過去3ヶ月連続で50万円以上の不正利用被害が発生)については、即時導入着手を求める。それ以外の既存加盟店については、Tier 2「不正顕在化加盟店ではないが不正が発生している加盟店」、Tier 3「高リスク商材取り扱い加盟店」、Tier 4「それ以外の加盟店」の優先順位で導入に着手し、2025年3月までに導入完了を目指す。新規加盟店に対しては、アクワイアラ（加盟店契約締結カード会社）や決済代行事業者から、2025年3月末までの導入を説明した上で契約を行うことが明記された（図4-1、図4-2）。

▼図4-1. 既存カード加盟店の分類

| 優先順位 | 対象 |
|---|---|
| Tier 1 | 不正顕在化加盟店<br>3ヶ月連続して50万円以上の不正が発生している加盟店 |
| Tier 2 | 不正顕在化加盟店ではないが不正が発生している加盟店<br>直近2年で、不正が5件以上または累計で10万円以上発生した加盟店 |
| Tier 3 | 高リスク商材取扱加盟店<br>①デジタルコンテンツ、②家電、③電子マネー、④チケット、⑤宿泊予約サービス |
| Tier 4 | 上記以外の加盟店 |

出所：『EMV 3-Dセキュア導入ガイド 1.4版』（日本クレジット協会）

▼図4-2. 加盟店のEMV 3-DS導入ロードマップ




出所：『EMV 3-Dセキュア導入ガイド 1.4版』（日本クレジット協会）を参考に作成

### (1)-2. セキュリティ・チェックリストの改訂と対象範囲の拡大

国内のECサイトのほとんどがカード情報保護対策として「非保持化」を選択している。しかし、非保持化済みのECサイトの設定の不備や既知の脆弱性を悪用して、オンラインスキミングによりカード情報を窃取される被害が発生しているのは前述の通りである。

非保持化済みのECサイトのセキュリティ強化を目的として、2022 年10月より、新規加盟店契約するECサイトがセキュリティ・チェックリストにより自身の脆弱性対策の実施状況をアクワイアラや決済代行事業者に申告する制度の試行が開始された。

『ガイドライン5.0』の付属文書として、『セキュリティ・チェックリスト』がとりまとめられた。『セキュリティチェックリスト』のチェック項目としては、従来の脆弱性対策、ウイルス対策、管理者権限の管理、デバイスの管理に加えて、クレジットマスター、悪質な有効性確認（クレジットマスターやフィッシングなどで窃取したカード情報の有効性をECサイトでの利用等を通じて確認する手口）および不正ログインなどへの対策が追加されている。また、追加的な対策の参考として、独立行政法人情報処理推進機構（IPA）が公表している『ECサイト構築・運用セキュリティガイドライン』が記載された。

『ガイドライン5.0』には、2025年4月から、新規に限らず全てのクレジットカードを取り扱うECサイトにセキュリティ・チェックリストに記載された対策の実施を求めることが明記された。ECサイトを運営する事業者からチェックリストを受領し確認するのは、割賦販売法により加盟店調査義務を負う、クレジットカード番号等取扱契約締結事業者（アクワイアラや決済代行事業者 ）の役割となる。

2023年6月時点で日本国内で稼働中のECサイト・ネットショップの数は約450万店に上る（eccLabによる推計）。膨大な数の加盟店が対象となるため、セキュリティ・チェックリストによる対策にはECプラットフォーム事業者など従来のクレジットカード業界を超えた協力が必要だと考えられる。

### (1)-3. MO・TO加盟店の不正利用対策のとりまとめ

『ガイドライン5.0』から構成を見直したことで、これまでの『クレジットカード・セキュリティガイドライン』に記載がなかったメールオーダー・テレフォンオーダー加盟店（以下MO・TO加盟店）の不正利用対策が新たに記載された。その内容はECサイトと同様で、すべての加盟店に対して善管注意義務とオーソリゼーションを求めるのに加え、「本人認証」「券面認証（セキュリティコード）」「属性・行動分析（不正検知システム）」「配送先情報」の４方策のうち、高リスク商材取扱加盟店では1つ以上、不正顕在化加盟店では2つ以上を実施するというものである。

MO・TO加盟店の場合、カード情報をコールセンターやBPO事業者の担当者が入力し、消費者が直接入力しない。そのため、2方策以上を導入する際に、カード会員本人がワンタイムパスワードを入力する前提となるEMV3-DSは導入できない。EMV3-DS以外の不正利用対策として、属性・行動分析、配送先住所の確認による出荷停止や券面認証の併用などによる対応が必要と考えられる。

### (1)-4. 「線の考え方」導入による不正利用対策指針

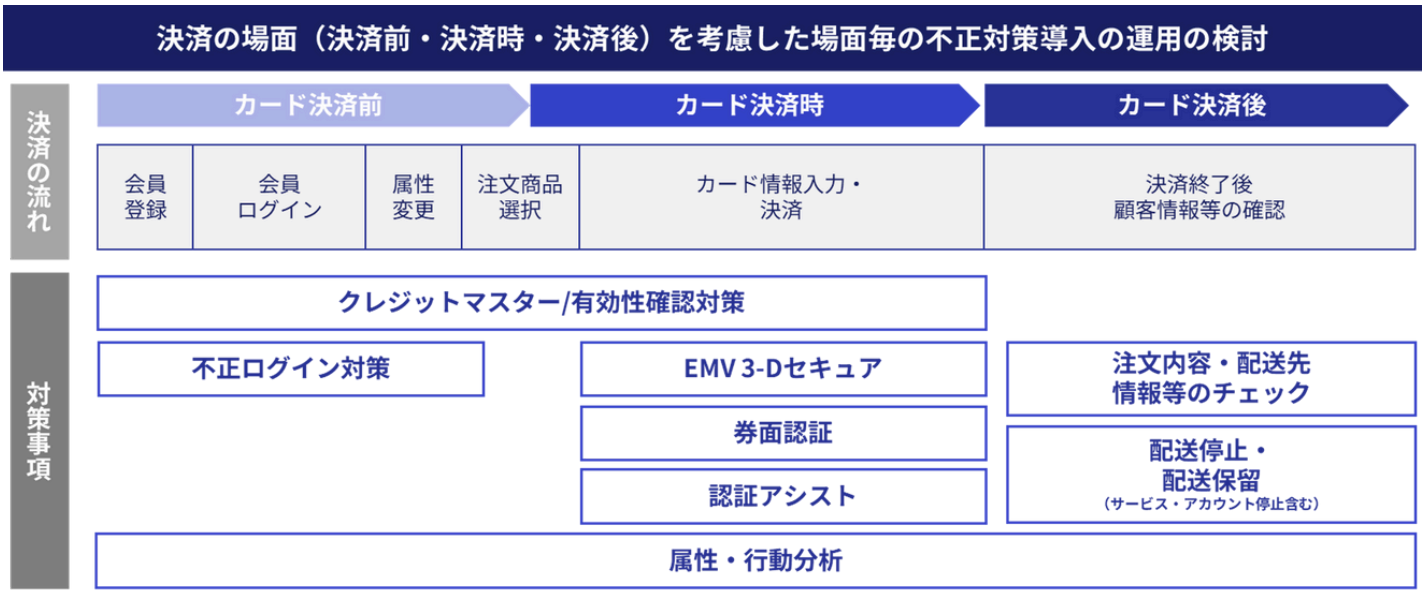
これまでの『セキュリティガイドライン』では、ECサイトの不正利用対策として４方策をベースに複数の方策を導入することを求めてきた。しかし、現状、これらの方策だ

けでは実行的な抑止効果が見られないケースもある。例えば2章(1)-2で紹介したアカウント乗っ取りは既存のECサイト会員のアカウントに不正にログインされ、登録済みの正規のカードで買い物をされるので、EMV3-DSだけでは防ぐことが難しい場合がある。あるいは、不正に新規登録された会員アカウントに、窃取したカード情報を登録する事例もある。その場合は、アカウントの登録時に不正なアカウントであることを検知する仕組みが必要である。

不正利用対策の効果を挙げているECサイトでは、EMV3-DSの導入に加えて、不正ログイン対策や配送先チェック、AIを利用した不正検知サービスなどを併用していることが多い。逆に、EMV3-DSだけを導入しても思ったように不正利用防止の効果があがらないという事例も見られるようになっている。

『ガイドライン5.0』では、2025年3月末のEMV3-DS導入完了後の不正利用対策として、カード決済時に加えて、決済前・決済後という場面ごとに対策を考える「線の考え方」を提示した（図4-3）。

▼図4-3 「今後の不正利用対策（線の考え方）」の概要




出所：『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)を参考に作成

2024年4月以降は、決済時の対策となるEMV3-DSを軸に、不正ログイン対策やクレジットマスター対策などの決済前の対策や、商品配送が伴う場合の配送停止などの決済後の対策も含め、詳細運用を検討するとしている。

## （2）PCI DSS バージョン4.0.1の公開

2024年6月、PCI DSS バージョン4.0（以下PCI DSS v4.0）の改訂版となるPCI DSS バージョン4.0.1（以下PCI DSS v4.0.1）が公開された。同時に、PCI DSS v4.0の有効期限が2024年12月末に設定された。なお、ベストプラクティス対応期限（2025年3月末）に変更はない。

今回の改訂は書式や誤記の修正、一部の要件の明確化を行う限定的な改訂であり、要件の追加や削除はない。

内容としては、PCI DSS v4.0で新規に追加された要件を中心に、用語や適用範囲の明確化がされている。例を挙げると、要件6.4.3（決済ページに含まれるスクリプトのインベントリ管理）に関連して、以下の2点が修正されている。

① 適用に関する注意事項に、決済代行事業者などのサードパーティサービスプロバイダ（TPSP）によって提供されるスクリプトについては、本要件はTPSPが責任を負うことが追記された。

② 目的に、決済ページに含まれるスクリプトの変更や新しいスクリプトの追加が行われる前に承認することが現実的でない場合、変更後にできるだけ早く承認することが追記された。また、本要件の適用対象となる「決済ページ」の定義も改訂され、決済トランザクションの処理とオーソリゼーションを目的とするページであることが明示された。

2024年12月末でPCI DSS v4.0は無効となるため、2025年1月以降にPCI DSS準拠を確認する場合はPCI DSS v4.0.1を使用する必要がある。2025年3月末のベストプラクティス対応期限に向けて準備を進めるPCI DSS 準拠企業は注意が必要である。

## （3）警察庁のキャッシュレスを狙うサイバー犯罪への取り組み

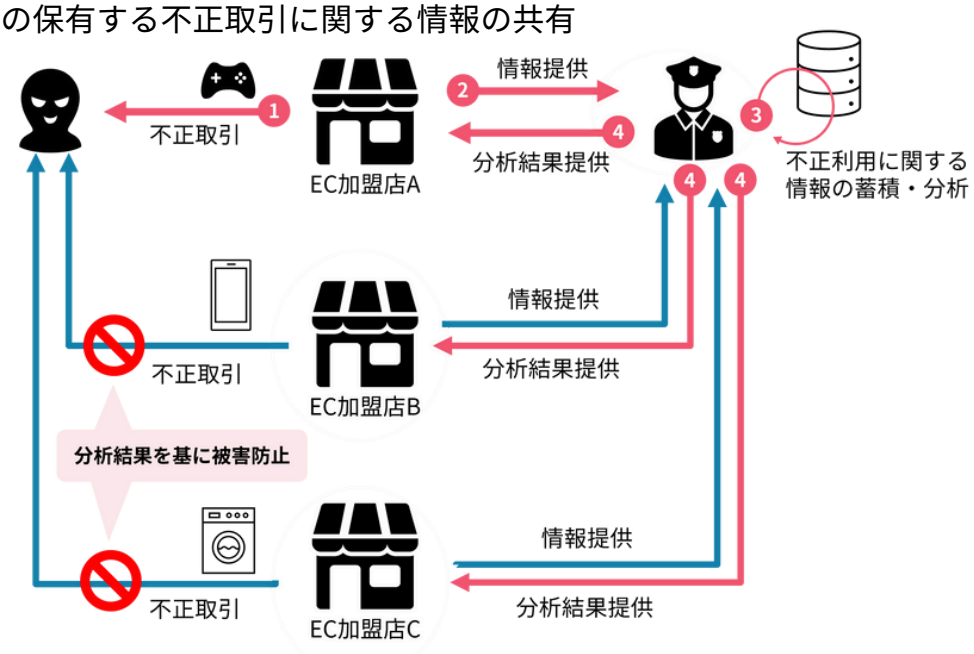
2023年6月、警察庁と経済産業省は、『サイバー攻撃によるクレジットカード番号等の漏えい事案に関する対策の推進に関する覚書』を締結した。本覚書では、カード情報流出事件が発生した際の情報共有や被害実態の把握、攻撃手口の分析等における連携や、平時における攻撃手口や重大な脆弱性に関する情報共有などを定めている。連携の他に、警察組織が独自にECサイトの調査等を通じてサイトの改ざんをECサイトに通知する動きも出始めている。

また警察庁は2023年11月から2月にかけて『キャッシュレス社会の安全・安心の確保に関する検討会』を開催し、報告書 を取りまとめた。本報告書では、フィッシングなどでID・パスワードを窃取された場合でも、不正送金やクレジットカード不正利用などの実質的な被害を水際で食い止めるために、以下のような方策を挙げている。

### (3)-1. EC加盟店との情報連携の強化

ECサイトは不正取引に関連するアカウント情報（氏名、住所、電話番号、メールアドレスなど）クレジットカード番号または、それに変わるトークン情報、配送先住所、取引内容などの情報（以下「不正取引に関する情報」）を保持している。各ECサイトの保有する不正取引に関する情報を警察と共有し、警察がECサイトを横断して分析した結果をフィードバックすることで、ECサイトが独自に実施するよりも、効果的な被害防止対策が可能になると考えられる（図4-4）。

▼図4-4. ECサイトの保有する不正取引に関する情報の共有




出所：『キャッシュレス社会の安全・安心の確保に向けた検討会報告書』（警察庁サイバー警察局）を参考に作成

一方で、不正取引に関する情報には個人データが含まれている。そのため、ECサイトはプライバシー保護への配慮などの観点から、警察に対する情報提供に極めて慎重であるのが現状である。本施策を推進するためには、警察庁において個人情報保護委員会事務局と調整し、個人データの第三者提供について本人同意が得られない場合でも財産の保護のために個人データの提供が可能になるケースを整理することが望ましいとしている。また、提供された不正取引に関する情報は非常に大量になることが予想されることから、分析にあたってはAI等のデジタル技術を活用して高度化・効率化すべきであるとしている。

### (3)-2. 暗号資産交換業者の不正送金防止

3章で述べた通り、オンラインバンキングの不正送金被害額のうち約半分は暗号資産交換業者の金融機関口座に送金されている。

暗号資産交換業者は、アカウントの名義と異なる名義からの送金は受け付けない 。そのため、暗号資産交換業者に送金するためには、依頼人名を送金元の口座の名義から変更して行う必要がある。2024年2月、警察庁と金融庁は連名で全国銀行協会等の団体に対し、送金元口座と異なる依頼人名での暗号資産交換業者への送金を停止するよう要請した 。

### (3)-3. コード決済に関する被害防止

フィッシング等により窃取されたコード決済サービスのアカウントが、実店舗で不正利用されるケースがある。攻撃者に正規のユーザーとしてログインされたコード決済サービスは実店舗では不正利用と見分けがつかないため、特にコード決済にクレジットカードや銀行口座を紐付けて使用している場合は被害が拡大する。

コード決済サービスの不正利用の水際防止を目的として、2023年11月、警察庁は日本フランチャイズチェーン協会に対して具体的な犯罪手口の情報を提供し、店舗における対応を教示した。また、防犯カメラについては、犯罪実行の抑止効果が期待できるとともに、その映像が被害発生時の捜査に重要な証拠となる。本報告書では、業界団体と連携して防犯カメラ設置や映像の保存期間延長について働きかけるべきであるとしている。

## （4）経済安全保障とクレジットカード業界

キャッシュレス社会においては、クレジットカードなど決済に関わるシステムは水道や電気と同等の社会基盤インフラであり、そのセキュリティは安心安全な生活を実現する上で重要である。その安定的な提供に支障が生じた場合は、国家および国民の安全に大きな影響をおよぼす。

経済安全保障推進法は、重要なインフラを提供する事業者を防護し、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることを目的とした法律である。具体的には、①重要物資の安定的な供給の確保 ②基幹インフラ役務の安定的な提供の確保 ③先端的な重要技術の開発支援 ④特許出願の非公開 に関する4つの制度を定めている。

クレジットカード分野にかかわるのは、そのうちの②基幹インフラ役務の安定的な提供の確保のために定められた「基幹インフラ制度」である。具体的には、15の対象分野を基幹インフラとして指定し、その中で「特定社会基盤事業者」を指定する。特定社会基盤事業者は、国に指定された重要設備（特定重要設備）の購入や維持管理の委託をしようとする際は、事前に審査を受ける。国は届け出られた計画書を確認し、特定重要設備が攻撃を受ける恐れがある場合は必要な措置を行うことを命令できる。

クレジットカード分野においては、クレジットカードなどの会員契約数1,000万件以上かつ年間取扱高4兆円以上のイシュアをクレジットカード業における特定社会基盤事業者に指定し、クレジットカード決済の取引承認（オーソリゼーション）にかかわるシステムなどの導入、保守点検、運用については国（経済産業大臣）への届け出および審査を受けることとしている（図4-5）。

▼図4-5 経済安全保障推進法でクレジットカード業において対象とされる特定重要設備

| | |
|---|---|
| **対象分野（法律）** | クレジットカード |
| **特定社会基盤事業の指定（政令）** | 包括信用購入あっせんの業務を行う事業 |
| **特定社会基盤事業者の指定基準**<br>（2019年6月省令） | クレジットカード等の会員契約数： 1,000万以上かつ、年間取扱高：4兆円以上<br>※年間取扱高、会員契約数それぞれのシェアの合計が大半を確保できる数値を目安として設定 |
| **特定重要設備**<br>（2019年6月省令） | クレジットカード決済の承認等に係るシステム<br>①基幹処理<br>②取引認証<br>③決済電文受理<br>④不正利用検知<br>⑤信用照会<br>⑥代行信用照会　等 |
| **重要維持管理等**<br>（2019年9月省令） | ・システムの保守点検<br>・システムの運用 |
| **構成設備**<br>（2019年9月省令） | ・業務アプリケーション<br>・オペレーティングシステム<br>・ミドルウェア<br>・サーバー<br>・その他重要な設備、機器、装置またはプログラム |

出所：『割賦販売法等について（平成28年改正法の評価等について）』
（経済産業省 商務・サービスグループ 商取引監督課 2023年11月）を元に作成

2023年11月、経済産業省はクレジットカード分野の特定基盤事業者としてイオン銀行、NTTドコモ、クレディセゾン、ジェーシービー、三井住友カード、三菱UFJニコス、楽天カードの７社を指定し、2024年5月17日から基幹インフラ制度の運用を開始した。

これらの事業者に加え、決済ネットワークや不正利用検知などの特定重要設備に指定されシステムを提供する事業者も、委託元からの要請という形で間接的に制度の枠組みの中に組み込まれることになる。

## ＜参考文献＞


1.『2023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　2024年3月29日）
https://www.meti.go.jp/press/2023/03/20240329006/20240329006.html

2.『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　2024年6月）
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf

3.『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

4.『カード情報漏洩インシデント調査レポート【2023年上半期】』（Fox Research）
https://foxresearch.hatenablog.com/entry/2023/08/03/153000

5.『カード情報漏洩インシデント調査レポート【2023年下半期】』（Fox Research）
https://foxresearch.hatenablog.com/entry/2024/03/13/090000

6.『Booking.com利用者へのフィッシング被害に関する注意喚起』（国土交通省　2023年11月15日）
https://www.mlit.go.jp/kankocho/page06_000354.html

7.『【重要】お客様へのお願い-フィッシングメールと宿泊施設への宿泊に関する注意喚起』（Booking.com　2023年12月）
https://news.booking.com/ja/-%E3%80%90%E9%87%8D%E8%A6%81-%E3%80%91%E3%81%8A%E5%AE%A2%E6%A7%98%E3%81%B8%E3%81%AE%E3%81%8A%E9%A1%98%E3%81%84-%E3%83%95%E3%82%A3%E3%83%83%E3%82%B7%E3%83%B3%E3%82%B0%E3%83%A1%E3%83%BC%E3%83%AB%E3%81%A8%E5%AE%BF%E6%B3%8A%E6%96%BD%E8%A8%AD%E3%81%B8%E3%81%AE%E5%AE%BF%E6%B3%8A%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E6%B3%A8%E6%84%8F%E5%96%9A%E8%B5%B7/

8.『Vidar Infostealer Steals Booking.com Credentials in Fraud Scam』（米Secureworks　2023年11月30日）
https://www.secureworks.com/blog/vidar-infostealer-steals-booking-com-credentials-in-fraud-scam

9.『調査報告書』（NTT西日本グループ 社内調査委員会　2024年2月29日）
https://www.ntt-west.co.jp/news/2402/pdf/240229a_2.pdf

10.『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　2023年8月31日）
https://www.meti.go.jp/press/2023/08/20230831002/20230831002.html

11.『EC事業者実態調査』（かっこ株式会社　2023年4月23日）
https://prtimes.jp/main/html/rd/p/000000120.000009799.html

12.不正トラベル対策の実施（連携施策）（日本サイバー犯罪対策センター（JC3） 2019年7月5日）
https://www.jc3.or.jp/threats/topics/article-145.html

13.『TwoFive なりすましメール対策実態調査 2024年2月版』（株式会社TwoFive　2024年2月9日）
https://www.twofive25.com/news/20240209_dmarc_report.html

14.『フィッシング報告状況（2024年6月）（月次報告書）』（フィッシング対策協議会）
https://www.antiphishing.jp/report/monthly/

15.『フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）』（金融庁、警察庁　2023年12月25日）
https://www.fsa.go.jp/ordinary/internet-bank_2/13.pdf

16.『令和５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 2024年3月14日）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

17.『JC3コラム - 悪質な不正送金の実態』（日本サイバー犯罪対策センター（JC3）2023年8月31日）
https://www.jc3.or.jp/threats/topics/article-508.html

18.『ＥＭＶ ３-D セキュア導入ガイド 1.4版』（クレジット取引セキュリティ対策協議会 2024年3月14日）
https://www.j-credit.or.jp/security/pdf/secure_installation_guide.pdf

19.『【2023年最新版】国内のECサイト・ネットショップの総稼働店舗数』（eccLab　2023年6月2日）
https://ecclab.empowershop.co.jp/archives/80408

20. 『Payment Card Industry Data Security Standard Requirements and Testing Procedures Version 4.0.1』（PCI Security Standards Council 2024年6月）
https://www.pcisecuritystandards.org/document_library/

21.『キャッシュレス社会の安全・安心の確保に関する検討会報告書』（警察庁サイバー警察局 2024年3月21日）
https://www.npa.go.jp/bureau/cyber/pdf/r5report.pdf

22.『割賦販売法等について （平成28年改正法の評価等について）』（経済産業省 商務・サービスグループ 商取引監督課 2023年11月）
https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/kappu_hambai/pdf/032_02_00.pdf

キャッシュレスセキュリティレポート2024
2024年9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/