Cashless Security Report

Quarterly Report

2024年(1-3月版)2024年7月発行

PCI DSS Ready Cloud

2024.7.25

かっこ株式会社
株式会社リンク

キャッシュレス・セキュリティレポート

ー2024年1～3月版：2024年7月発行ー

>>> はじめに

　かっこ株式会社（以下Cacco）と株式会社リンク（以下リンク）が、カード情報流出とECサイトの不正被害の実態を把握するため、独自 調査・データをもとにまとめたレポートです。本レポートは、2023年よりかっこ株式会社とｆｊコンサルティング株式会社が四半期ごとに取りまとめてきた『キャッシュレスセキュリティレポート（四半期版）』を継承した内容となります。

>>> コンテンツ

1. カード情報流出事件の概況（2024 年1-3月）

（1）カード情報流出事件数・情報流出件数の推移

2024年1-3 月のカード情報流出事件

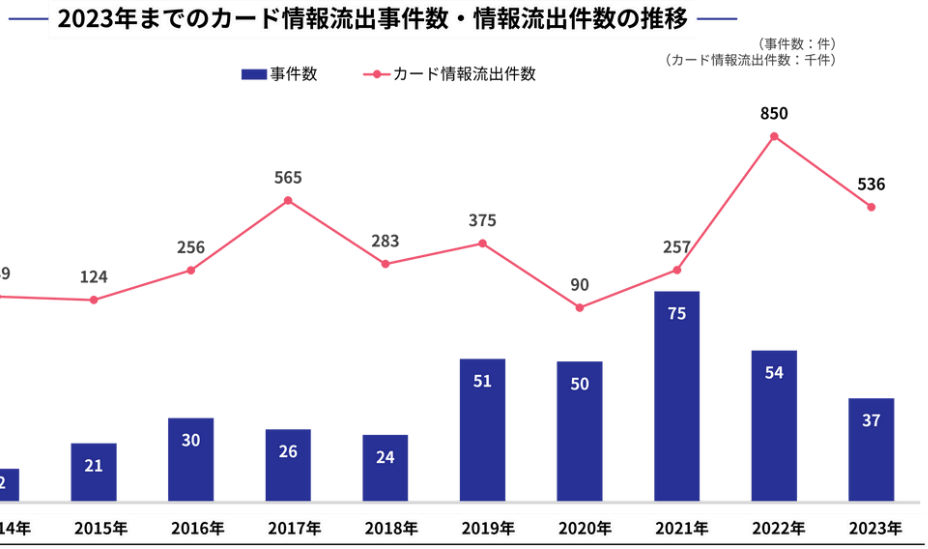
- 事件数　7件
- カード情報流出件数　23,680件

※クレジットカード、ブランドデビットカード、ブランドプリペイドカードを含む

【調査方法】

Caccoとリンクが、各社の公式サイトや報道などの公開情報により事件を特定し、集計

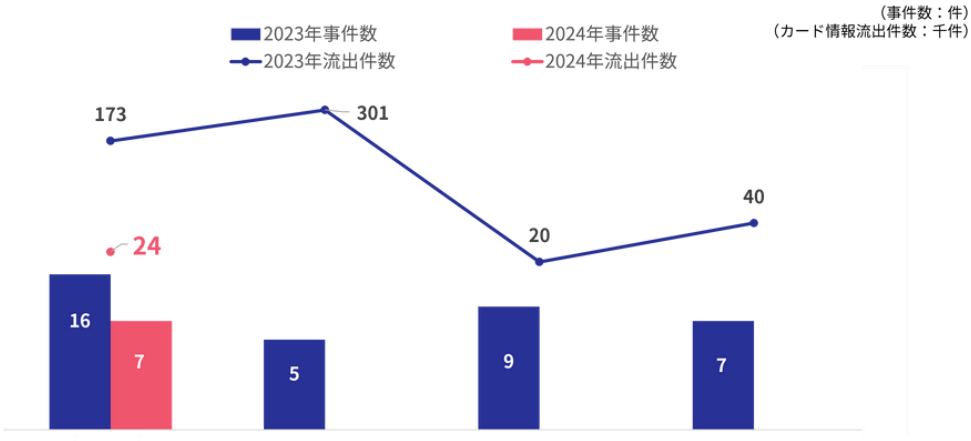
2023年までのカード情報流出事件数・情報流出件数の推移



	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(件)	13	12	21	30	26	24	51	50	75	54	37
カード情報流出件数(件)	514,369	138,717	123,527	255,689	564,844	283,374	375,479	89,628	256,822	849,950	536,291

（Cacco・ｆｊコンサルティング調べ）
※2021年以前のデータはｆｊコンサルティング調べ

2024年のカード情報流出事件数・情報流出件数(前年同四半期比較)



		1～3月	4～6月	7～9月	10～12月
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
2024年	事件数(件)	7			
	カード情報流出件数(件)	23,680			

（Cacco・リンク調べ）
※2023年12月末までのデータはCacco・ｆｊコンサルティング調べ

期間中のカード情報流出事件の数は7件、カード情報流出件数は23,680件となりました。7件の事件のうち1件は、Booking.comの管理画面の不正ログインを起点として送信されたフィッシングメールにより、4,000件以上の個人情報がフィッシングサイトに入力された事件です。4,000件のうち3件で、入力された情報にカード情報が含まれていたことが公表されました。

（2）業種/商材別事件数・情報流出期間別事件数

＜業種/商材別の事件数＞

業種/商材カテゴリー		2023年4-6月		2023年7-9月		2023年10-12月		2024年1-3月	
		事件数（件）	カード情報流出件数（件）	事件数（件）	カード情報流出件数（件）	事件数（件）	カード情報流出件数（件）	事件数（件）	カード情報流出件数（件）
加盟店合計		4	10,774	9	20,593	7	40,831	7	23,680
業種別	アパレル	1	6,263	0	0	0	0	1	3,827
	コスメ	0	0	0	0	2	67	0	0
	食品	1	1,830	2	5,157	1	1,755	2	7,183
	家電・電子機器・PC	0	0	1	6,364	0	0	1	4,748
	生活雑貨、家具、インテリア	1	1,771	4	8,983	0	0	0	0
	健康食品	0	0	0	0	1	14	1	5,193
	ホビー	0	0	0	0	0	0	1	2,726
	自動車、バイク	0	0	0	0	1	2,602	0	0
	その他	1	910	2	89	2	36,393	1	3
カード会社		1	290,771	0	0	0	0	0	0

（Cacco・リンク調べ）
※2023年12月末までのデータは、Cacco・ｆｊコンサルティング調べ

※7-9月の「その他」のうち1件はカード情報流出件数不明

＜流出期間別の事件数・カード情報流出件数＞

情報流出期間	2023年4-6月		2023年7-9月		2023年10-12月		2024年1-3月	
	事件数(件)	カード情報流出件数(件)	事件数(件)	カード情報流出件数(件)	事件数(件)	カード情報流出件数(件)	事件数(件)	カード情報流出件数(件)
3ヶ月以内	2	292,542	3	173	0	0	1	3
3ヶ月-1年	2	2,740	2	244	3	81	1	2,726
1-3年	1	6,263	4	20,176	4	40,750	5	20,951
3年以上	0	0	0	0	0	0	0	0

（Cacco・リンク調べ）
※2023年12月末までのデータは、Cacco・ｆｊコンサルティング調べ

※7-9月の「その他」のうち1件はカード情報流出件数不明

（3）カード情報流出事件のトピック

旧サイトのバックアップ保存の重要性

2024年2月にカード情報の流出を公表した美容家電販売サイトは、2023年4月にサイトのリニューアルを実施し、2ヶ月後の2023年6月1日にクレジットカード会社から利用者のカードが不正利用されている懸念について連絡を受けました。調査の結果、2021年4月から旧サイトを閉鎖した2023年4月3日までの間、旧サイトからカード情報が流出していた痕跡が発見されました。

攻撃の手口は旧サイトの脆弱性を利用して不正な注文を入力してサイトを改ざんし、消費者が入力した個人情報やカード情報などを窃取するものでした。フォックスエスタ（※1）の調査によると、旧サイトはEC CUBE 3.0系で動作していた形跡があります。このバージョンには2021年6月に公開されたクロスサイトスクリプティング脆弱性が存在しており、この脆弱性を攻撃された可能性があります。

今回のケースでは、旧サイト閉鎖後もバックアップが保存されていたことから、旧サイトを調査し、攻撃の手口や被害状況を把握することができたと考えられます。過去に旧サイトにおいて情報流出が発生し、新サイトへの移行後に発覚するケースも多くあるため、サイトリニューアル後も、旧サイトのバックアップを一定期間保存しておくことが重要です。その際には外部から接続されていない安全な環境に保管することが必須となります。またサイトリニューアルの際は、旧サイトを閉鎖するまではセキュリティパッチの適用などを確実に行う必要があります。

※1 フォックスエスタ https://foxestar.hatenablog.com/

（4）カード情報保護　国内政策の動向

2025年4月から全てのEC加盟店を対象に実施する『セキュリティ・チェックリスト』をとりまとめ

2024年3月に公表された『クレジットカード・セキュリティガイドライン【5.0版】』（※2）の付属文書21として、『セキュリティ・チェックリスト』が追加されました。2022年10月から、新規に加盟店契約を締結するECサイトを対象に試行されている「セキュリティ・チェックリスト」を取りまとめたものです。ECサイトの管理画面の保護、ECサイトの設定、既知の脆弱性対策、マルウェア対策、クレジットカードマスター対策、不正ログイン対策について具体的な対策が記載されており、新規加盟店は加盟店契約締結時にこれらの対策の実施状況をアクワイアラーやPSPに申告する必要があります。

『クレジットカード・セキュリティガイドライン【5.0版】」には、2025年4月から既存店を含む全てのEC加盟店に対して、これらの対策の実施を求めることが明記されました。

※2 『クレジットカード・セキュリティガイドライン【5.0版】』
https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_5.0_published.pdf

2. ECにおける不正利用の概況（2024年1-3月）

（1） クレジットカード不正利用被害額の推移

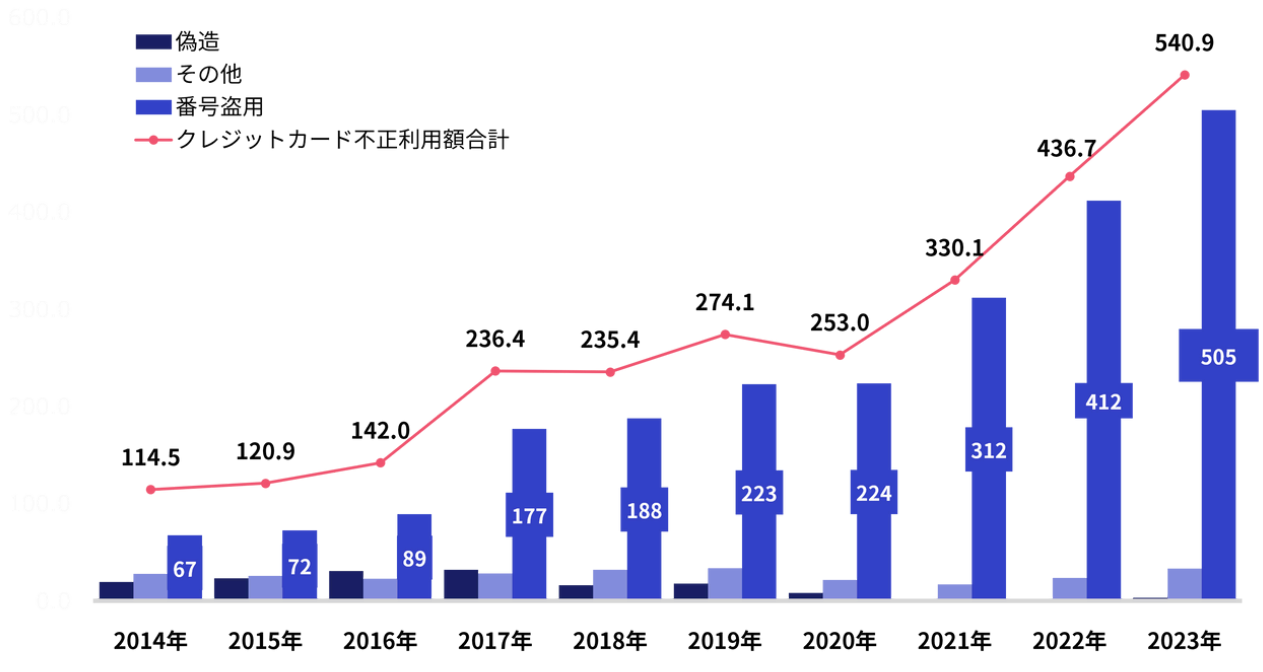
2024 年1-3月のクレジットカード不正利用

- 不正利用被害額合計　121.4億円
- 偽造　0.7億円
- 番号盗用　112.4億円
- その他　8.3億円

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

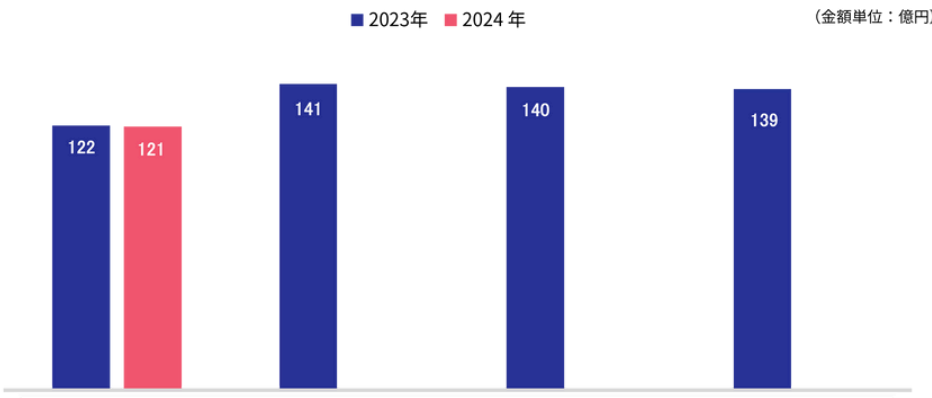
2023年までのクレジットカード不正利用被害額の推移

（金額単位：億円）



（　『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）

2024年のクレジットカード不正利用被害額（前年同四半期比較）



		1-3月	4-6月	7-9月	10-12月
2023年	偽造	0.8	0.5	0.7	1.1
	番号盗用	113.6	132.4	130.6	128.1
	その他	7.4	8.1	8.2	9.4
	合計	121.8	141.0	139.5	138.6
2024年	偽造	0.7			
	番号盗用	112.4			
	その他	8.3			
	合計	121.4			

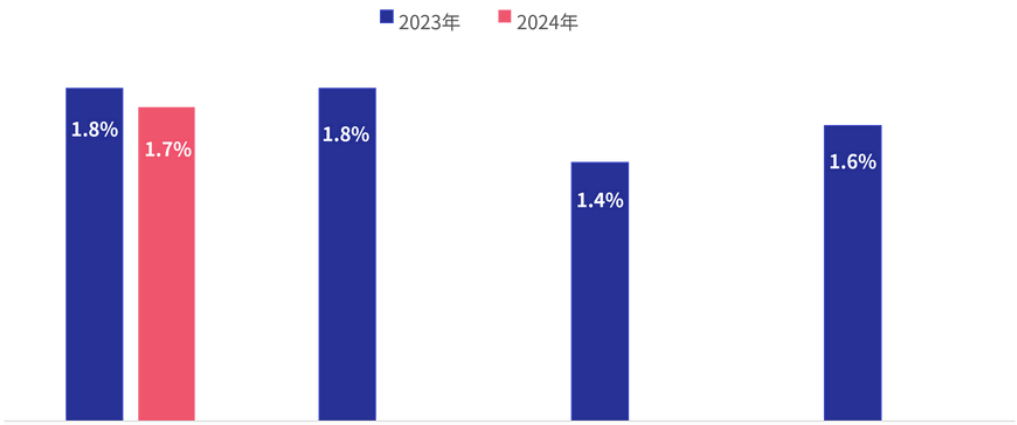
（『クレジットカード不正利用被害額の発生状況』 日本クレジット協会）

2024年1～3月の不正利用被害額は121.4億円と昨年同期とおおよそ同額となりました。2023年の被害額は年間で540億円を超えており、このままのペースでは今年も同様の被害となる恐れがあります。2025年3月を期限としたEMV 3-Dセキュア対応の義務化により、番号盗用による不正利用被害額が減少することが期待されます。

（2）ECサイト不正利用の傾向

【調査方法】
不正注文検知サービス「O-PLUX」（Caccoが提供する不正注文検知サービス）をご利用のお客様（累計11万サイト以上）における審査結果をもとに集計

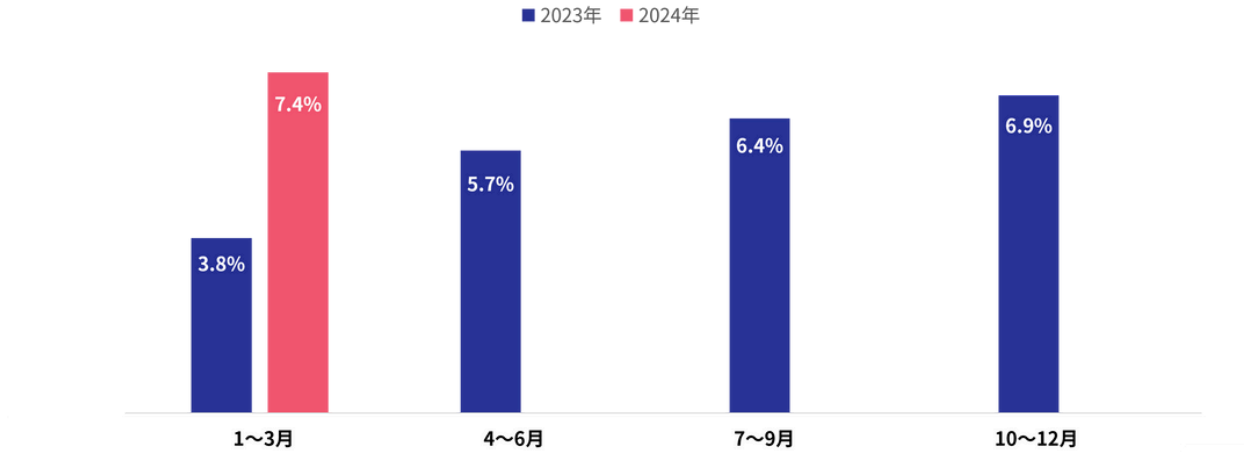
クレジットカード不正注文の発生率 （前年同四半期比較）



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

※「O-PLUX」の審査で、審査件数全体に占めるクレジットカード不正注文の審査結果NG割合を件数ベースで算出。（Cacco調べ）
※最終的に出荷停止や注文を拒否するなどの対応は、「O-PLUX」加盟店判断により異なる。

転売不正注文の発生率（前年同四半期比較）



	1〜3月	4〜6月	7〜9月	10〜12月
2023年	3.8%	5.7%	6.4%	6.9%
2024年	7.4%			

※「O-PLUX」の審査で、審査件数全体に占めるい転売不正注文の審査結果NG割合を件数ベースで算出。（Cacco調べ）
※最終的に出荷停止や注文を拒否するなどの対応は、「O-PLUX」加盟店判断により異なる。

＜不正注文に狙われやすい商材ランキング＞

2023年（10-12月） 商材別不正注文検知数ランキング			
1位	チケット	7位	日用品・雑貨・キッチン用品
2位	デジタルコンテンツ	8位	コンタクト・メガネ
3位	ホビー・ゲーム	9位	ふるさと納税
4位	コスメ・ヘアケア	10位	食品・飲料・酒類
5位	健康食品・医薬品	11位	レンタルサービス
6位	PC・タブレット・家電	12位	工具

2024年（1-3月） 商材別不正注文検知数ランキング			
1位	デジタルコンテンツ	7位	総合通販
2位	ホビー・ゲーム	8位	食品・飲料・酒類
3位	健康食品・医薬品	9位	工具
4位	コスメ・ヘアケア	10位	コンタクト・メガネ
5位	日用品・雑貨・キッチン用品	11位	サブスクサービス
6位	PC・タブレット・家電	12位	チケット

※「O-PLUX」の審査で、審査件数全体に占める不正注文の審査結果NG割合を件数ベースで算出。（Cacco調べ）
※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。

全体の傾向としては、転売不正率が前回の23年10-12月の数値と比較すると、0.5ポイント増加し、2023年から継続して転売発生率が増加しています。これは、不正利用者が様々なサイトで繰り返し注文を試行しているためと推測できます。商材別に見ると、これまで同様コスメやヘアケアなどの定期購入の初回限定価格を設けている商品が転売不正被害に狙われやすい傾向がみられました。

（3）2024年3月末の国内のカード発行会社（イシュア）におけるDMARC設定状況

フィッシング攻撃により窃取されたカード情報の不正利用が増加していることを受け、2023年3月に経済産業省、警察庁、総務省が連名で、カード発行会社（以下イシュア）に対してDMARC導入をはじめとしたメールによる、なりすまし対策を要請しました。

イシュアは割賦販売法で「登録包括信用購入あっせん事業者」として登録が義務付けられており、その一覧が経済産業省のWEBサイトで公開されています。リンクは、経済産業省のウェブサイトで公開されているイシュア246社を対象に、DMARCの導入状況を調べました。

【調査方法】

① 調査対象のイシュアがWebサイト等でメール送信元として公開しているドメイン（外部委託先やサブドメインを含む）を収集し、対象ドメインを確定

② ①で収集した全てのドメインのDNSに問い合わせを行い、DMARCレコードの設定有無と、設定がある場合ポリシーを確認

③ 会社ごとのDMARC対応状況を以下の3段階に分類

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

2）一部対応：メール送信元として使用しているドメインの一部にDMARCレコードが設定されている。

3）未対応：メール送信元として使用している全てのドメインにDMARCレコードが設定されていない。

【調査対象】

登録包括信用購入あっせん事業者（イシュア）246社

【調査実施時期】

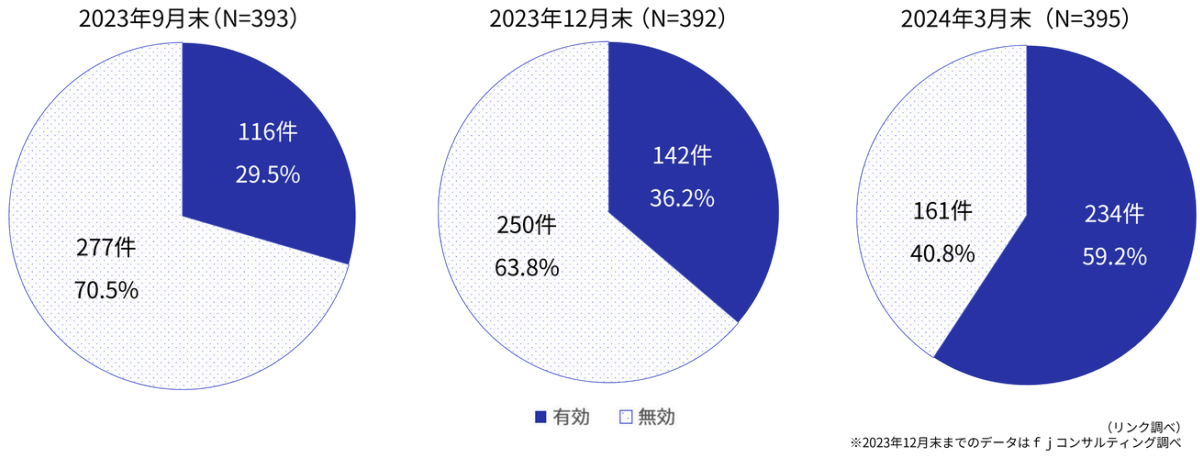
2024年3月末

【調査結果（2024年3月31日）】

① 調査対象ドメイン数　395件

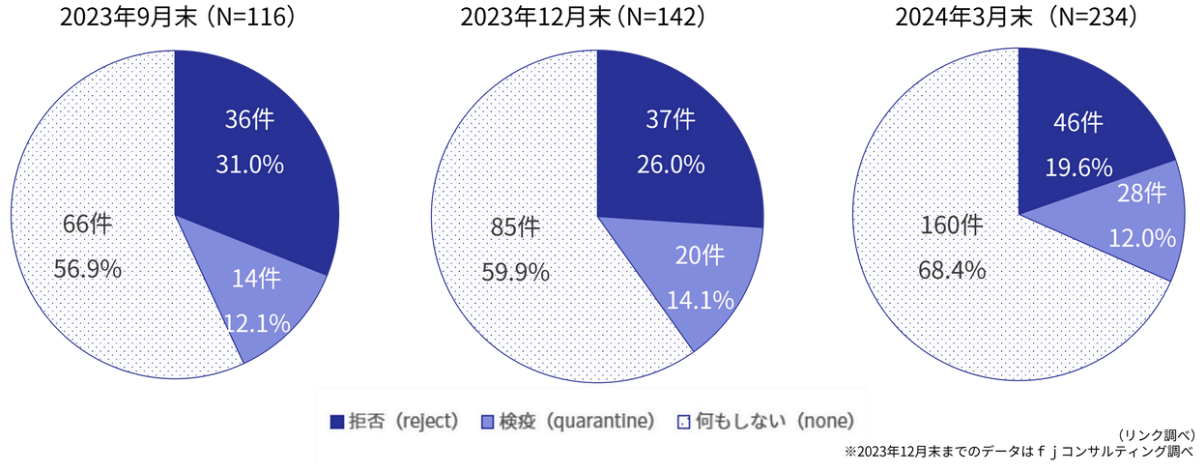
② 調査対象ドメインごとのDMARC対応状況と運用ポリシー

＜ドメインごとのDMARCの設定率＞



（リンク調べ）
※2023年12月末までのデータはｆｊコンサルティング調べ

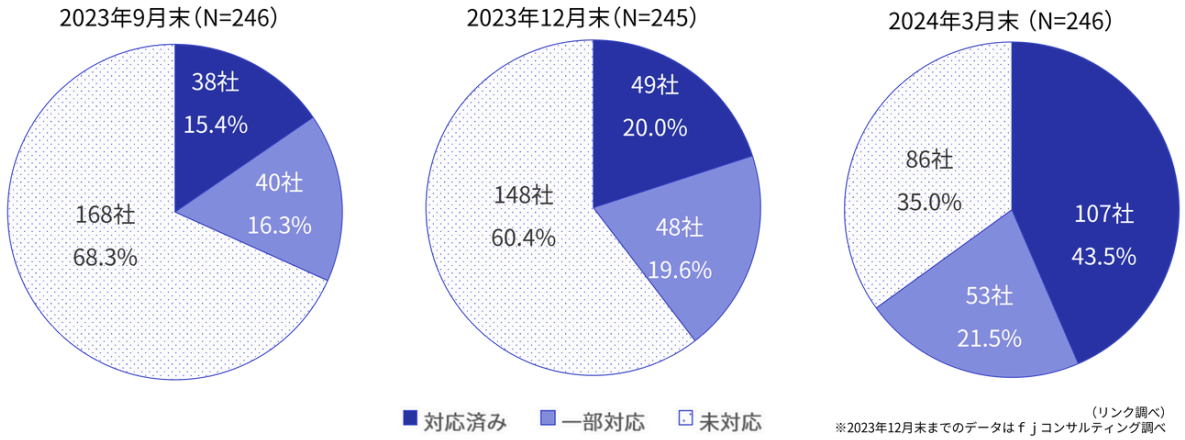
＜ドメインごとのDMARC設定ポリシー＞



（リンク調べ）
※2023年12月末までのデータはｆｊコンサルティング調べ

2024年3月末時点で、イシュアがメール送信に利用しているドメイン395件のうち、有効なDMARCレコードが設定されているのは234件（59.2%）と、2023年8月の調査開始以来、初めて5割を超えました。DMARCレコードが有効なドメインのうち、最も厳しい「reject（拒否）」ポリシーが設定されているドメインは46件（19.6%）で、160件（68.4%）はポリシーを「none（何もしない）」にして運用しています。新規にDMARCを導入したドメインはポリシーを「none（何もしない）」に設定しているケースが多いため、「reject（拒否）」もしくは「quarantine（検疫）」にしているドメインの割合は2023年12月末に比べて下がっていますが、件数自体は増えています。

③会社ごとのDMARC対応状況



会社ごとにみると、DMARCを一部でも導入しているイシュアは160社（65.0%）となっており、107社（43.5%）はコーポレートドメインおよび委託先も含めたメール送信に使用する全てのドメインでDMARC導入済みとなっています。経済産業省、警察庁及び総務省からの要請に基づきDMARC導入を進めてきた企業により、導入率が底上げされたと思われます。

一方でフィッシングメール対策としてのDMARCの実効性を持たせるためには、導入しているドメインにおいてもポリシーを「reject（拒否）」もしくは「quarantine（検疫）」に設定して運用することが求められています。

（4）不正利用のトピック

生成AI活用による不正手口の巧妙化

2022年11月から、生成AIブームのきっかけともなった「ChatGPT」が公開され、今では文章、画像、音声など様々な分野で活用されるようになりました。その一方でそれを悪用した、フェイクニュースや詐欺、不正行為について世界的にも問題になっています。

代表的な例で言えば、マルウェア（コンピューターウイルスなどの悪意のあるソフトウェア）やフィッシングメールの作成などがあげられます。OpenAI、Google、マイクロソフトなどの大手ベンダーが提供する生成AIは、倫理的に問題があるような悪質なプロンプトに対して回答を制限する対策（ガードレール）が実装されています。しかし、「WormGPT」や「FraudGPT」と呼ばれる、ガードレールのない生成AIが確認されており、サイバー犯罪に悪用されるケースが増加しています。

生成AIを利用して実在する人物の画像や音声を結合し、偽の映像を合成するディープフェイク技術が詐欺に悪用される事例も発生しています。2024年2月には、香港の多国籍企業の会計担当者が生成AIで作られた偽のCFO（最高財務責任者）に騙され、計2億香港ドル（日本円約38億円）を不正送金してしまった事件が報じられました。この手口の巧妙な点は、会計担当者をビデオ会議に参加させた点です。その会議に出席していたCFOをはじめとする参加者は、全てディープフェイク技術により声や見た目が本人とそっくりに偽装されていました。当初は詐欺を疑った会計担当者も、会議に参加したことで複数の知人の顔や声が本物だと信じて疑いを捨て、送金に同意してしまいました。

（5）不正利用対策　国内政策の動向

①　MO・TO加盟店の不正利用対策を取りまとめ

『クレジットカード・セキュリティガイドライン【5.0版】』では、メールオーダー・テレフォンオーダー加盟店（MO・TO加盟店）のクレジットカードの不正利用対策が記述されました。その内容はECサイトと同様で、全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す。

ただし、MO・TO加盟店の場合、カード情報はコールセンターやBPO事業者の担当者が代理で入力するため、消費者が直接カード情報を入力することが前提となるEMV 3-Dセキュアによる本人認証は導入できません。そのため、EMV 3-Dセキュア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の対応が必要と考えられます。

②クレジットカード不正利用防止における警察庁とECサイト間の連携

警察庁サイバー警察局は、「キャッシュレス社会の安全・安心の確保に関する検討会」において検討された報告書を2024年3月に公表しました（※3）。本報告書では、EC事業者との不正取引に関する情報共有を推進することが提言されました。EC事業者は不正取引に利用されたアカウント情報（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」）を保持しています。

本報告書では、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が不正利用防止に有効と述べています。

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おり、現状はプライバシー保護への配慮などの観点から、ECサイトは警察に対する情報提供に極めて慎重であるとも述べています。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ます。

※3 『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』（2024年3月）
https://www.npa.go.jp/bureau/cyber/pdf/r5report.pdf

【本レポートに関するお問い合わせ】

かっこ株式会社
広報担当：前田
Mail: pr@cacco.co.jp
Mobile : 050-3627-8878

株式会社リンク
セキュリティプラットフォーム事業部　担当：滝村・加藤・相原
Mail: spdsales@link.co.jp
Tel:03-6704-9090