Cashless Security Report

Quarterly Report

2023年(7-9月版)2024年1月発行

fjconsulting, INC.

2024.1.16

キャッシュレス・セキュリティレポート
ー2023年7～9月版ー

かっこ株式会社
ｆｊコンサルティング株式会社

はじめに

かっこ株式会社とｆｊコンサルティング株式会社が、カード情報流出とECサイトの不正被害の実態を把握するため、独自調査・データをもとにまとめたレポートです。

コンテンツ

1. カード情報流出事件の概況（2023年7-9月）

（1）カード情報流出事件数・情報流出件数の推移

2023 年7月-9月のカード情報流出事件

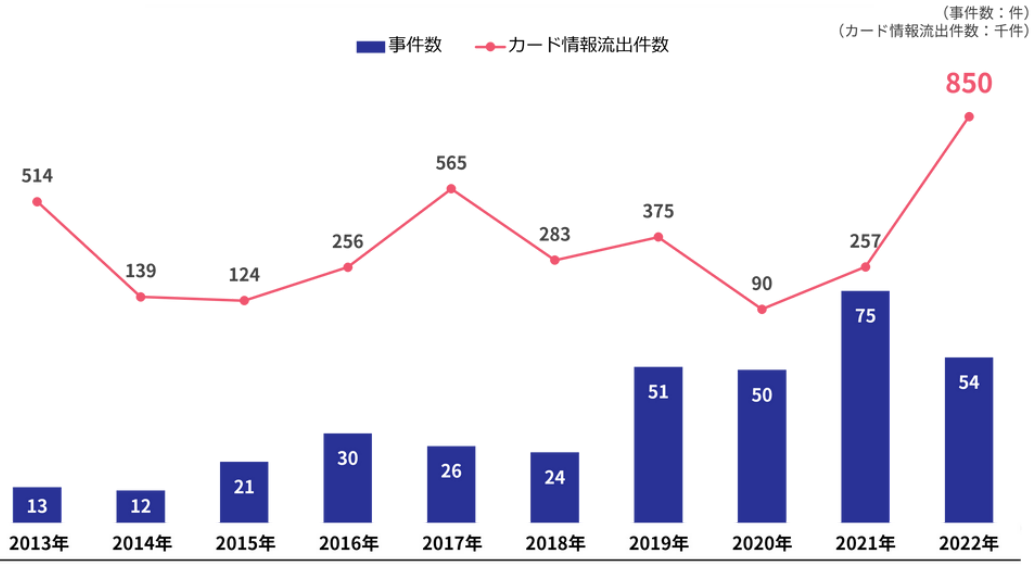
- 事件数　9件
- カード情報流出件数　20,593件

※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】

かっこｆｊコンサルティングが、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

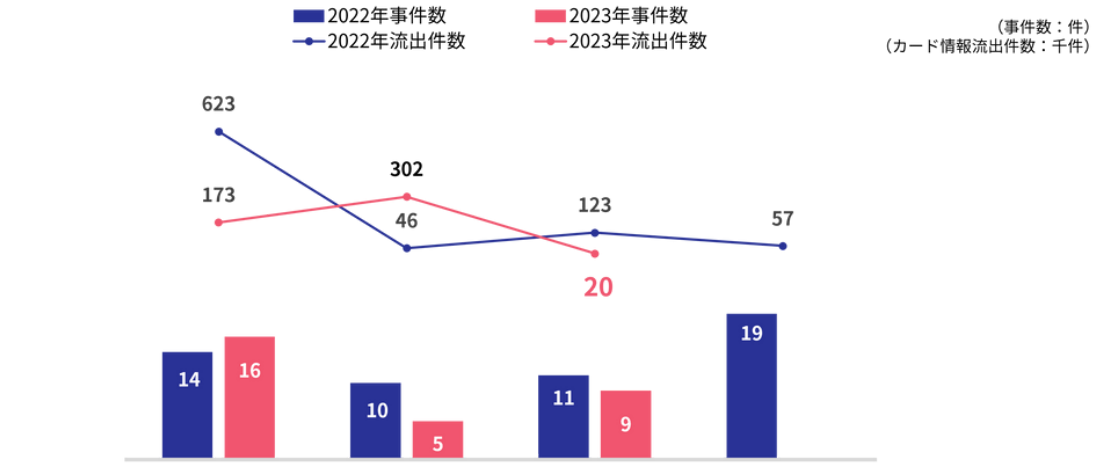
2022年までのカード情報流出事件数・情報流出件数の推移



	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年	2022年
事件数(件)	13	12	21	30	26	24	51	50	75	54
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

（かっこ・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

2023年のカード情報流出事件数・情報流出件数(前年比較)



		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	
	カード情報流出件数(件)	173,322	301,545	20,593	

（かっこ・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9件、カード情報流出件数が20,593件となりました。10,000件を超える大規模な流出事件がなかったため、カード情報流出件数は少なくなっています。9件の流出事件のうち1件は、旅行会社で、ECサイト経由ではなく電話でクレジットカード決済を行なった顧客のカード情報が流出したものとなっており、流出件数は不明です。

（2）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(2023年1-9月)＞

業種/商材カテゴリー		2023年1-3月		2023年4-6月		2023年7-9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）
加盟店合計		16	173,322	4	10,774	9	20,593
業種別	アパレル	5	41,362	1	6,263	0	0
	コスメ	4	13,707	0	0	0	0
	食品	3	5,099	1	1,830	2	5,157
	家電・電子機器・PC	2	112,147	0	0	1	6,364
	生活雑貨、家具、インテリア	1	402	1	1,771	4	8,983
	アパレル、コスメ、健康食品	1	605	0	0	0	0
	その他	0	0	1	910	2	89
カード会社		0	0	1	290,771	0	0

（かっこ・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1-3月		2023年4-6月		2023年7-9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)
3ヶ月以内	5	115,048	2	292,542	3	173
3ヶ月-1年	2	12,819	2	2,740	2	244
1-3年	8	45,432	1	6,263	4	20,176
3年以上	1	23	0	0	0	0

（かっこ・ｆｊコンサルティング調べ）

（3）カード情報流出事件のトピック

旅行予約サイトBookng.comを経由したフィッシングが多発

大手旅行サイトBooking.com経由で宿泊施設を予約した利用者に対し、チャット機能やメールを利用してクレジットカードを盗み取るカード情報の流出が世界中で多発しています。日本でも2023年5月頃から被害が報告されており、11月時点で68件の宿泊施設が被害を公表していると報じられています。2023年11月には国土交通省から「Booking.com利用者へのフィッシング被害に関する注意喚起」が公表されています。

攻撃者はBooking.comの宿泊施設向け管理画面に不正にログインし、宿泊予約客宛のメッセージ機能を利用して利用者にチャットやメールを送信します。メッセージの内容は、「カード決済に失敗したので確認手続きをしてください」「期限までに手続きしないと予約がキャンセルされます」というもので、手続き用のURLとして偽サイトのURLが記載されています。偽サイトではカード番号、有効期限、セキュリティコードなどの入力を求められ、入力するとカード情報が窃取されます。

Booking.comでは宿泊施設に対し、管理画面へのログインに２段階認証の設定を推奨していますが、設定していなかった宿泊施設も多数あり、被害にあっていると推測されます。現在Booking.comは、宿泊施設向けのサポートサイトに、本件に関する注意喚起の文書を公表しています。

同様の被害を防ぐには、宿泊施設の管理者が2段階認証など多要素認証を有効にすることが、まずは必要ですが、設定していた場合でも必ずしも安全とは言い切れません。2段階認証を突破する手口としては、管理者を偽サイトに誘導し、入力させた認証情報をリアルタイムで正規のサイトに入力して不正にログインする「リアルタイムフィッシング（中継型フィッシング）」が被害として、すでに確認されております。また2段階認証のワンタイムパスワードの送信にメールを使っている場合は、マルウェアを管理者のPCにインストールさせ、遠隔操作することで管理者のメールを参照することが可能になってしまいます。そのため、送られている2段階認証のワンタイムパスワードを窃取して使用し、管理画面に不正にログインする手口も想定されます。2段階認証など多要素認証を使用する場合は、実際に管理者がログインするPCでワンタイムパスワードを参照する方法を避け、スマートフォンによるワンタイムパスワードの生成（Google Authenticatorなど）や物理トークンなど独立したデバイスを使用する必要があります。

2. ECにおける不正利用の概況（2023年7-9月）

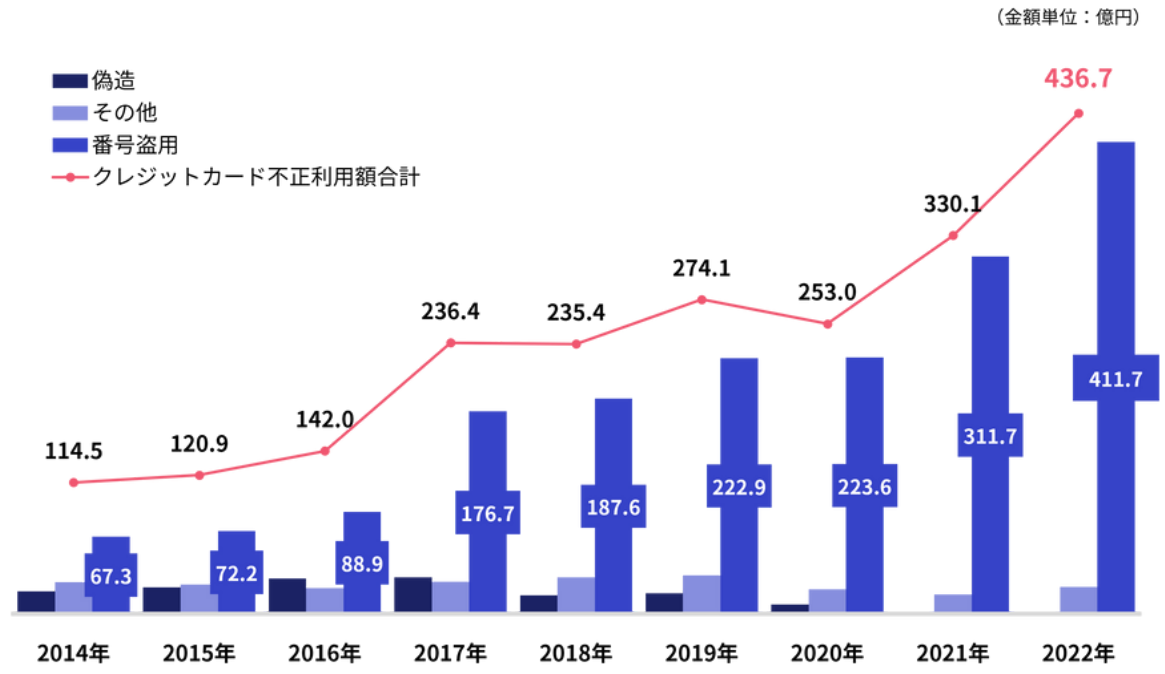
（1） クレジットカード不正利用被害額の推移

2023 年7月-9月のクレジットカード不正利用

- 不正利用被害額合計　139.5億円
- 偽造　0.7億円
- 番号盗用　130.6億円
- その他　8.2億円

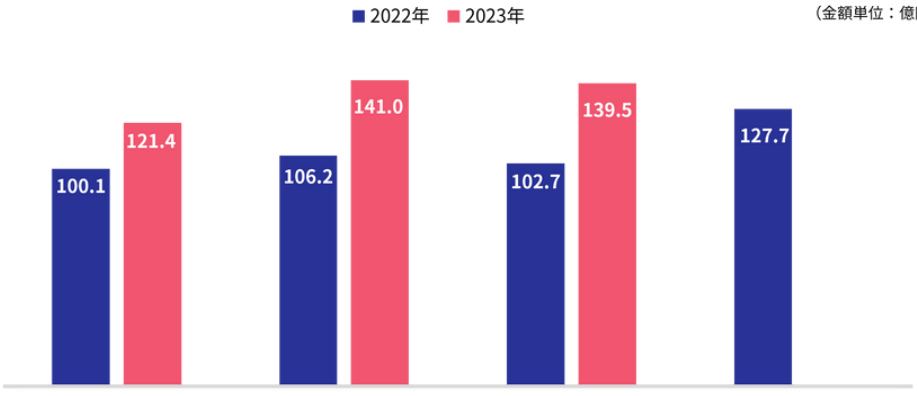
※日本クレジット協会調べ
https://www.j-credit.or.jp/information/statistics/index.html

2022年までのクレジットカード不正利用被害額の推移



（『クレジットカード不正利用被害額の発生状況』日本クレジット協会）

2023年のクレジットカード不正利用被害額（前年比較）



		1-3月	4-6月	7-9月	10-12月
2022年	偽造	0.2	0.2	0.7	0.6
	番号盗用	94.6	100.6	95.9	120.6
	その他	5.3	5.4	6.1	6.5
	合計	**100.1**	**106.2**	**102.7**	**127.7**
2023年	偽造	0.8	0.5	0.7	
	番号盗用	113.3	132.4	130.6	
	その他	7.3	8.1	8.2	
	合計	**121.4**	**141.0**	**139.5**	

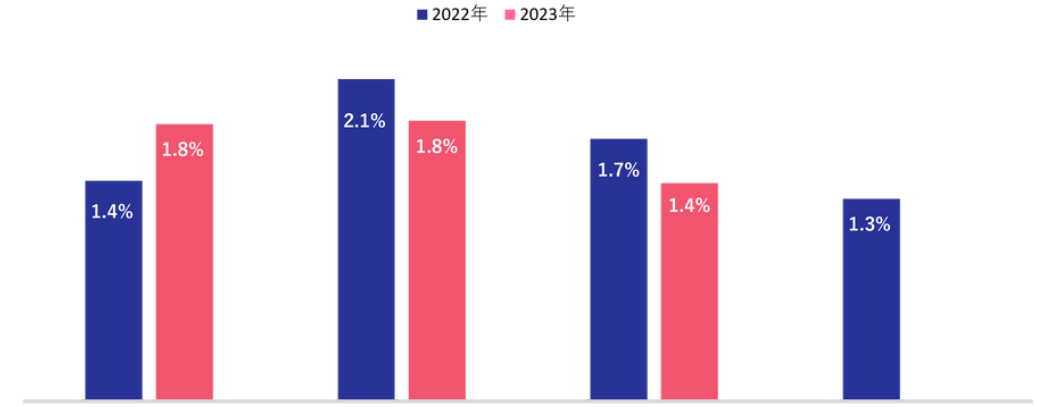
（『クレジットカード不正利用被害額の発生状況』 日本クレジット協会）

2023年7月から9月の間に発生した不正利用被害額は139.5億円で、前年同期比で35.8%増加しました。2022年と同様に番号盗用が9割以上を占め、偽造やその他についても増加傾向が続いています。全体をみると、2023年1－9月の合計不正被害額は既に401.9億円にのぼっており、2023年度は500億円を突破することが予測されます。

（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」（かっこが提供するクレカ不正、悪質転売など不正注文を検知するサービス）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

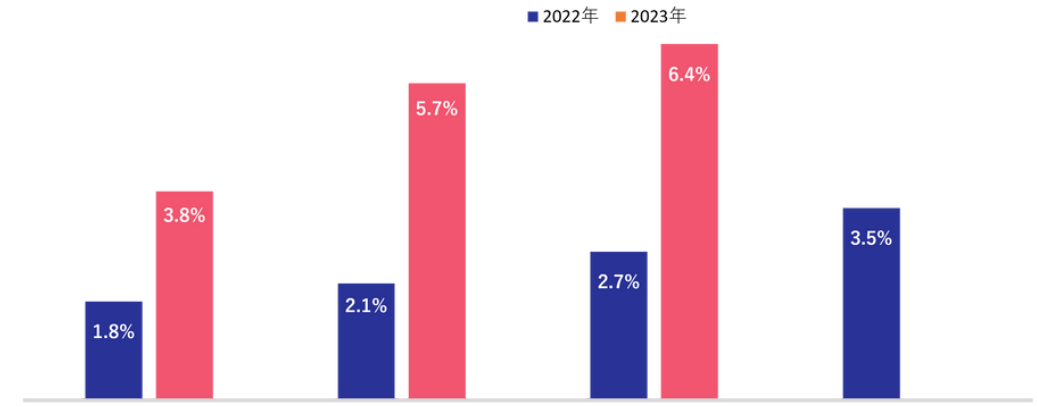
クレジットカード不正注文の発生率



	1～3月	4～6月	7～9月	10～12月
2022年	1.4%	2.1%	1.7%	1.3%
2023年	1.8%	1.8%	1.4%	

※「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。（かっこ調べ）
※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



	1～3月	4～6月	7～9月	10～12月
2022年	1.8%	2.1%	2.7%	3.5%
2023年	3.8%	5.7%	6.4%	

※「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。（かっこ調べ）
※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。

第二四半期に引き続き、健康食品やコスメなど、特定の商品やジャンルを絞った単品通販での不正注文がさらに増加する傾向がありました。

夏休みを利用した小遣い稼ぎを目的とした不正な転売や、企業の販促プロモーションとして行われるアフィリエイターによる活動（※）が活発化し、これが商品への注目を高め、転売価値が上がる結果、不正注文が増加するというケースも見受けられました。

※アフィリエイターが、ブログやSNS等にて消費やサービスを紹介し、そこから購買につなげることで報酬を得る活動

＜不正注文に狙われやすい商材ランキング＞

2023年（4-6月） 商材別不正注文検知数ランキング			
1位	ホビー・ゲーム	7位	食品・飲料・酒類
2位	デジタルコンテンツ	8位	コンタクト・メガネ
3位	チケット	9位	スポーツ用品
4位	コスメ・ヘアケア	10位	家電
5位	健康食品・医薬品	11位	工具
6位	総合通販	12位	レンタルサービス

2023年（7-9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	食品・飲料・酒類
2位	ホビー・ゲーム	8位	PC・タブレット・家電
3位	チケット	9位	スポーツ用品
4位	コスメ・ヘアケア	10位	工具
5位	コンタクト・メガネ	11位	ふるさと納税
6位	健康食品・医薬品	12位	総合通販

※「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。（かっこ調べ）
※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。

ふるさと納税はこれまでランキング圏外でしたが、需要の高まりとともに不正注文も増加したため11位にランクインしました。また、チケットなどはこれまでも狙われやすい傾向にありましたが、旅行・レジャー需要の高まりや「コト消費」のニーズの高まりもあり、不正注文が増加しています。これらは、物販とは異なり配送不要なため換金がしやすく不正注文がしやすい特徴があります。

（3）2023年9月末の国内のカード発行会社（イシュア）におけるDMRAC設定状況

フィッシング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、経済産業省は、2023年1月に公表した『クレジットカード決済システムのセキュリティ対策強化検討会 報告書』で、カード発行会社（以下イシュア）に対してDMARC導入を含めたなりすまし対策の強化を求めています。

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。ｆｊコンサルティングは、経済産業省のWeb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。

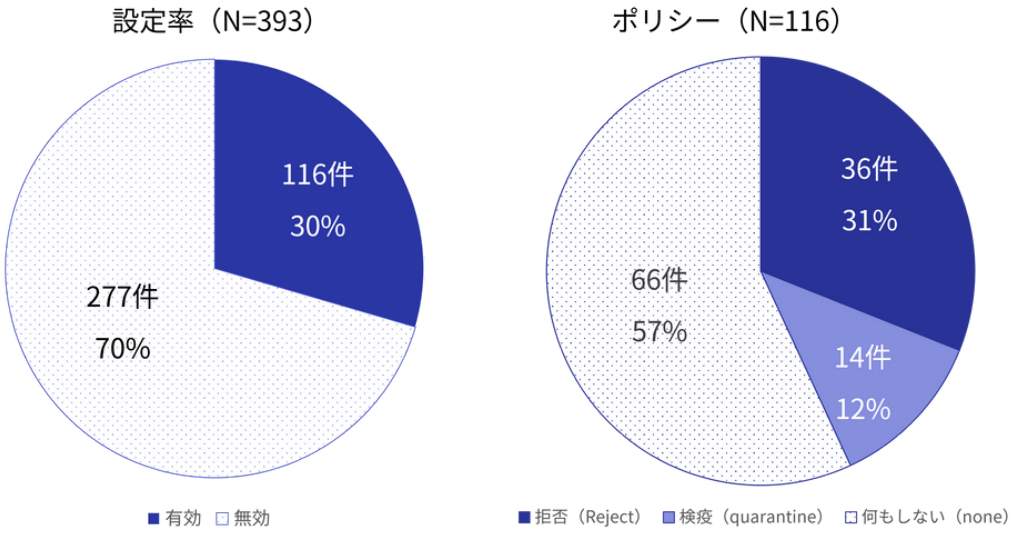
【調査方法】
①　調査対象のイシュアがWebサイト等でメール送信元として公開しているドメイン（外部委託先やサブドメインを含む）を収集し、対象ドメインを確定
②　①で収集した全てのドメインのDNSに問い合わせを行い、DMARCレコードの設定有無と、設定がある場合ポリシーを確認
③　会社ごとのDMARC対応状況を以下の3段階に分類
　１）対応済み：メール送信元として使用しているドメイン全てにDMARCレコードが設定されている。
　２）一部対応：メール送信元として使用しているドメインの一部にDMARCレコードが設定されている。
　３）未対応：メール送信元として使用している全てのドメインにDMARCレ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】
2023年9月末

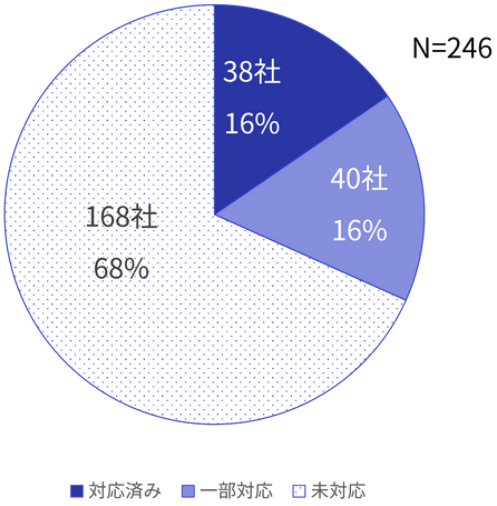
【調査結果（2023年9月30日）】
① 調査対象ドメイン数　393件
② 調査対象ドメイン毎のDMARC対応状況と運用ポリシー

＜調査対象ドメイン毎のDMARC対応状況と運用ポリシー＞



（ｆｊコンサルティング調べ）

＜会社毎のDMARC対応状況＞



（ｆｊコンサルティング調べ）

2023年9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393件のうち、有効なDMARCレコードが設定されているのは116件（30%）となりました。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36件（31%）で、66件（57%）はポリシーを「none（何もしない）」にして運用しています。組織別にみると、DMARCを一部でも導入しているイシュアは32%となっています。

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、導入率を引き上げる、および導入しているドメインにおいても認証結果レポートをふまえ、ポリシーを「reject（拒否）」もしくは「quarantine（検疫）」に設定して適切に運用することが求められます。

（4）不正利用のトピック

Amazonを悪用した不正利用の増加

Amazonを悪用した不正利用が増加しており、特に2023年9月以降、その頻度が上昇しています。被害者は、2段階認証を有効にしているにもかかわらず、不正アクセスやアカウントが乗っ取られAmazonギフトカードを大量購入されるなどの被害を受けています。2段階認証は、Webサービスへのログイン時にIDとパスワードの入力だけでなく、アプリやアクセスコードを使用した追加認証を求め、本人確認を強化する仕組みです。追加認証の手段には、SMSでのワンタイムパスワード、専用アプリ、Google Authenticatorなどがあります。

今回の具体的な手口はまだ明らかになっていませんが、カード情報流出事件トピックのbooking.comでもご紹介した2段階認証が突破されるケースでは、リアルタイムフィッシング（中継型フィッシング） が確認されております。これにより、被害者が気付かずに不正なログインを許してしまいます。

インターネットバンキングにおいても、2023年11月末現在で5, 147件、約80億1000万円と過去最多の不正送金被害が発生しています。金融庁と警察庁は、IDやパスワードに加えてワンタイムパスワード等を窃取する手口への注意喚起をおこなっています。

【本レポートに関するお問い合わせ】

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

ｆｊコンサルティング株式会社
広報・マーケティング担当　板垣
Mail: info@fjconsulting.jp