fjconsulting, INC.

Cashless Security Report

Annual Report

2023

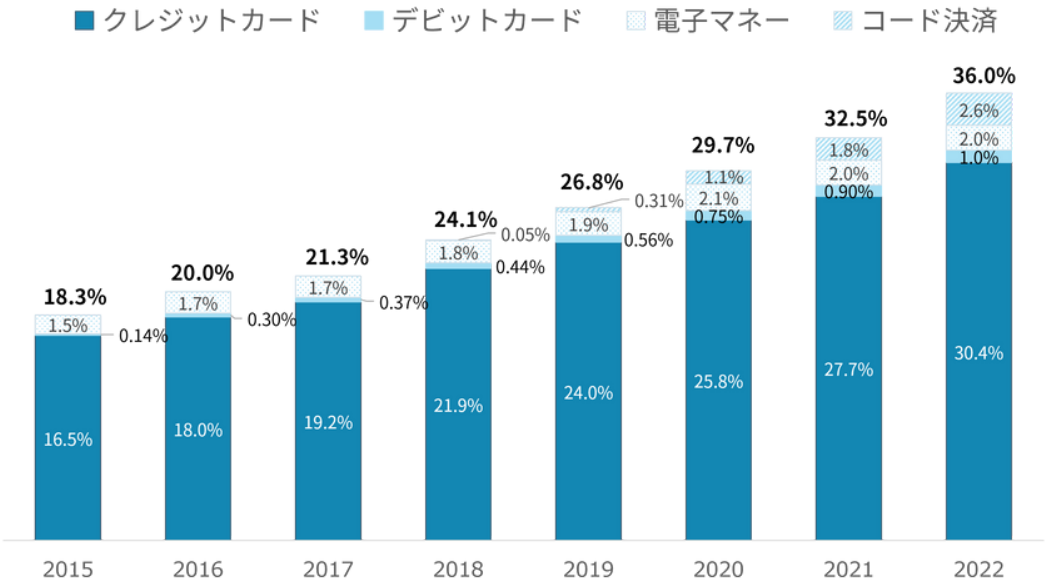
2023年10月26日
かっこ株式会社
ｆｊコンサルティング株式会社

はじめに

2023年6月に経済産業省が公表したデータによれば、2022年のキャッシュレス決済比率は36.0%と2021年に比べて3.5%の増加となった。東京オリンピック・パラリンピックで2021年に加速したキャッシュレス比率の上昇傾向は、2022年以降も継続している。政府は「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%」の目標を掲げているが、前倒し達成がほぼ確実となっている。

2022年の決済手段の内訳は、コード決済の占める割合が電子マネーを上回った。一方、クレジットカードも、タッチ決済など非接触決済対応の広がりもあり、2021年の27.7%から30.4%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84.5%となった。2021年の85.3%からはやや減少しているが、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。

キャッシュレス決済比率の推移

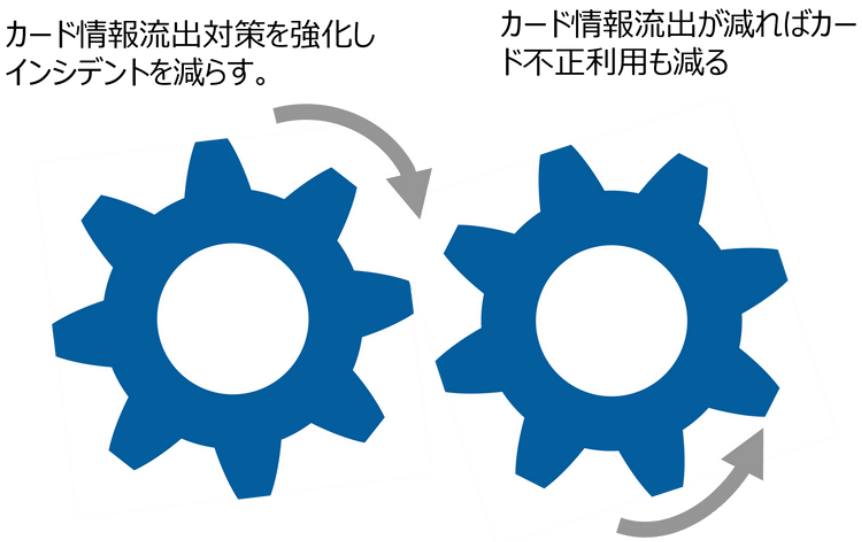


経済産業省プレスリリース『2022年のキャッシュレス決済比率を算出しました』
（商務・サービスグループ キャッシュレス推進室　2023年4月6日）
https://www.meti.go.jp/press/2023/04/20230406002/20230406002.html

キャッシュレス比率が上がる一方で、クレジットカードなどのカード情報を狙った攻撃やキャッシュレス決済の不正利用の被害は増加している。2022年は複数の加盟店が利用するサービスプロバイダを狙った攻撃（サプライチェーン攻撃）が2件、公表された。それらのサービスを利用する多数の加盟店が被害を受け、計40万件以上のカード情報が流出した。

クレジットカード不正利用金額は2021年をさらに上回り、年間でついに400億円を突破し、過去最悪の記録を更新している。不正利用されるカード情報は、不正アクセスなどにより加盟店から流出したもの以外にもフィッシングやクレジットマスターなどの手口で取得されたものの割合が増えつつある。従来のクレジットカードセキュリティは、カード情報流出事件が減れば不正利用も減るという相関を前提としていたが、それ以外の手口にも対応しなければ不正利用被害は減少しない状況に変化している。

カード情報流出対策と不正利用対策の相関



キャッシュレスセキュリティの重要性が増す中、かっこ株式会社とｆｊコンサルティング株式会社とは、2023年7月より、クレジット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2023」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。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。

もくじ

1. 2022年のカード情報流出事件の概況

（1）カード情報流出事件数・流出件数の推移

クレジットカードやブランドデビットカードなどのペイメントカード情報（以下、カード情報）流出事件に関しては業界団体や官公庁などによる統計が存在しない。本レポートをかっこ社とｆｊコンサルティング社の連名で公表するにあたり、カード情報流出事件数およびカード情報流出件数の考え方について協議し、以下の通り定義した。

●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。

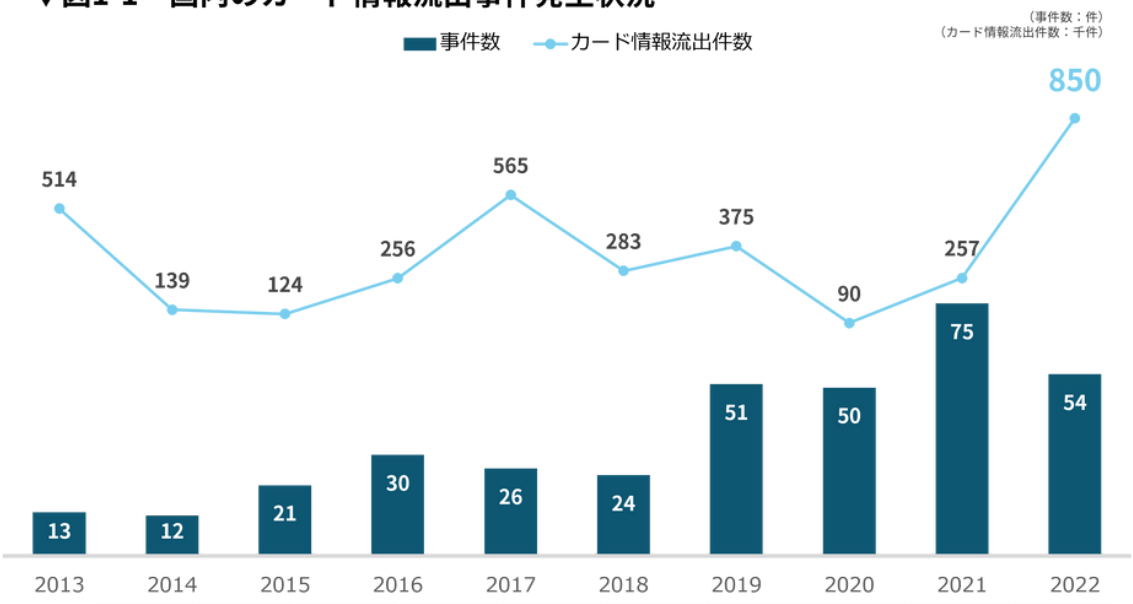
▶ECサイトから委託を受けてカード情報を扱っていた事業者が発表主体として情報公開した場合は、公表された一連の攻撃を1つの事件として扱う。

●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

(1)-1. 年次推移

2022年1月から12月に公表された事件数は54件と、2021年に比べて21件減っている。一方でカード情報流出件数は849,950件と、2013年にｆｊコンサルティング社が調査を開始して以来最多となった。うち、2022年2月に公表された決済代行事業者 A社からの流出が460,829件と半分以上を占めている。

▼図1-1　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
事件数	13	12	21	30	26	24	51	50	75	54
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
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

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）

図1-1の通り、1事件あたりの流出件数は2017年以降減少傾向にあった。2022年は1万件を超えるカード情報が流出した事件が前述の決済代行事業者A社を含め10件公表された。

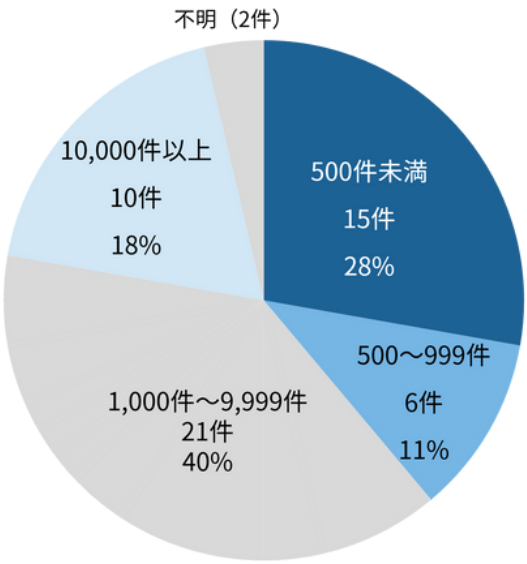
その結果、1事件あたり平均のカード情報流出件数は16,345件、A社を除いた平均も7,630件と2021年の3,424件に比べて約2倍となり、2021年以降2年間続けての増加となった。

▼図1-2　2022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	決済代行事業者 A社	460,829	2021/8/2～2022/1/25	104	SQLインジェクション、バックドアを利用した不正プログラムによる情報窃取
2	コスメ販売 B社	89,295	2020/5/21～2021/8/18	454	オンラインスキミング（可能性高）
3	アパレル（職業制服）販売 C社	63,565	2020/10/9～2022/3/7	515	オンラインスキミング（可能性高）
4	コスメ販売 D社	46,702	2020/12/5～2021/6/24	201	オンラインスキミング
5	カタログギフトサービス E社	28,700	2020/11/14～2021/11/11	363	オンラインスキミング（可能性高）
6	アパレル（子供向け）　F社	18,453	2020/6/26～2021/4/26	369	オンラインスキミング（可能性高）
7	アパレル（ブランド古着）販売　G社	18,136	2020/4/27～2021/12/22	605	オンラインスキミング（可能性高）
8	アパレル（女性向け）販売　H社	16,093	2021/8/10～2022/2/22	197	オンラインスキミング（可能性高）
9	コスメ販売　B社（2とは別サイト）	14,640	2020/5/21～2021/8/18	454	オンラインスキミング（可能性高）
10	和菓子販売　I社	14,127	2021/2/4～2022/1/31	362	オンラインスキミング（可能性高）

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15件（28%）、500～999の事件が6件（11%）となった。合計すると1,000未満の事件が約4割を占めるが、2021年は1,000件未満の事件が約5割を占めていたのに比べると減少した。ここからも、1事件あたりの流出件数が増加に転じている傾向がうかがえる。

▼図1-3　2022年カード情報流出規模別事件数



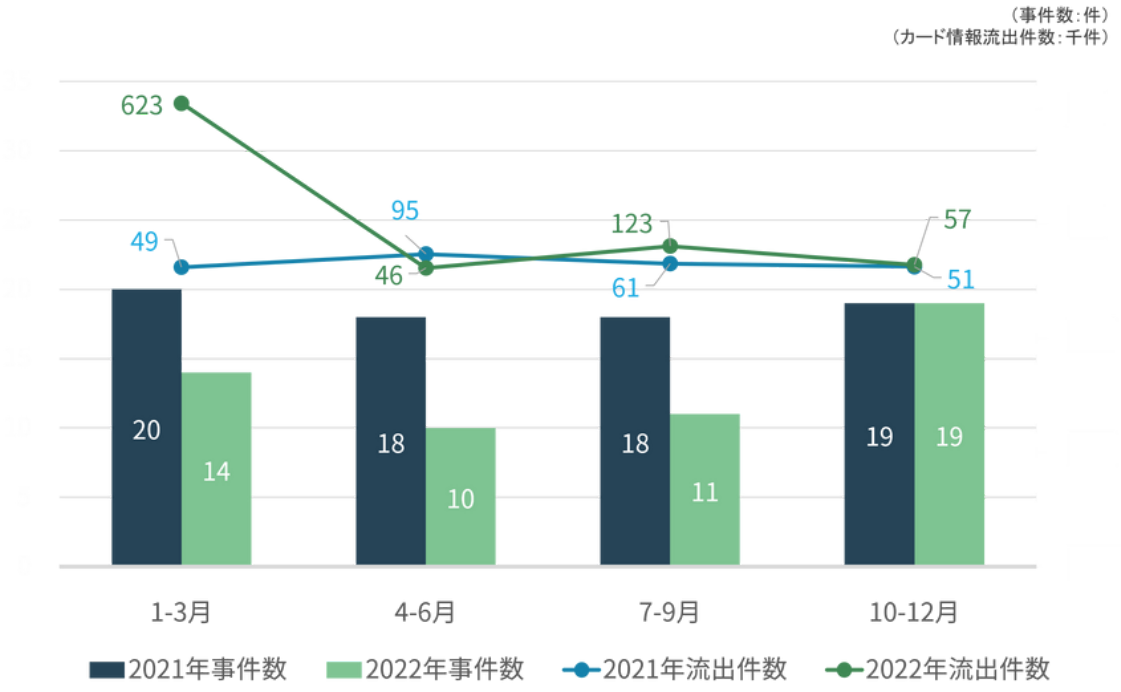
流出件数規模	事件数	割合
500未満	15	26%
500～999	6	11%
1000～1499	4	8%
1500～1999	2	4%
2000～2499	5	9%
2500～2999	2	4%
3000～3499	1	2%
3500～3999	1	2%
4000～4499	0	0%
4500～4999	1	2%
5000～7499	2	4%
7500～9999	3	6%
10,000以上	10	19%
不明	2	4%

かっこ・ｆｊコンサルティング調べ

(1)-2. 四半期別推移

四半期別の事件数を2021年と比較すると、2022年1-3月、4-6月、7-9月はいずれも前年同期よりも少なくなっているのに対し、10-12月は前年と同数となった。これは、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）による事件が8件公表されたことによる（詳細は後述）。四半期別のカード情報の流出件数は、1-3月期に決済代行事業者A社のカード情報流出件数が公表された他にも流出件数が1万件を超える事件が3件公表されたことにより、流出件数が跳ね上がっている。また、7-9月にも1万件を超える事件が3件公表されており、流出件数が若干増加した。

▼図1-4　2021年と2022年のカード情報流出件数四半期別の推移



かっこ・ｆｊコンサルティング調べ

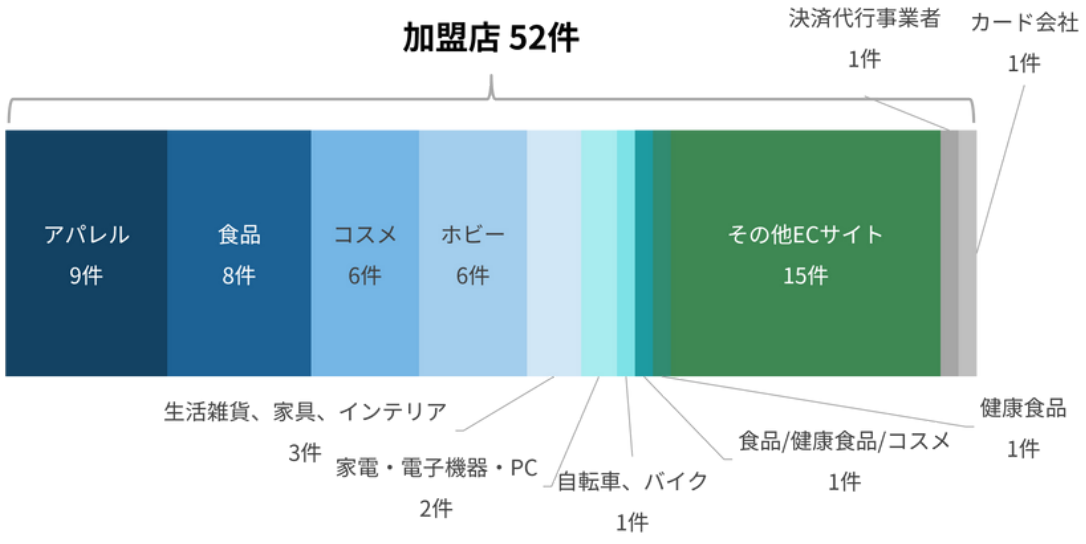
（2）カード情報流出事件の傾向

(2)-1. 業種/取扱い商材別・情報流出期間別事件数

2022年のカード情報流出事件54件の内訳を図に示す。52件が加盟店からの流出、2件が加盟店以外からの流出である。

加盟店の内訳を取扱い商材別に見ると、最も多いのがアパレル（9件）、次いで食品（8件）、コスメ（6件）／ホビー（6件）となる。

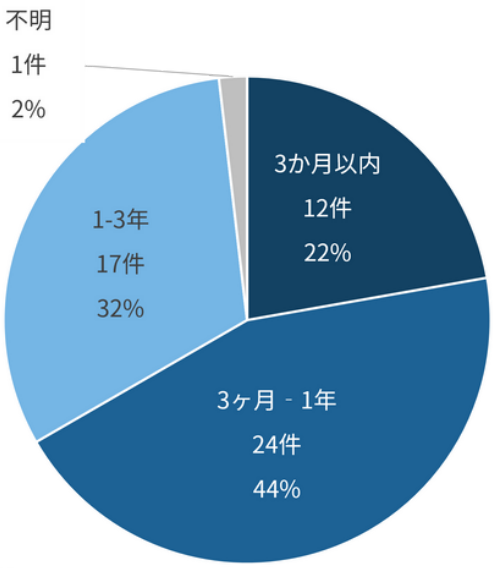
▼図1-5　2022年業種・取扱い商材別カード情報流出件数



かっこ・ｆｊコンサルティング調べ

流出期間別の割合は以下となる。3ヶ月-1年の期間が最も多く24件（44%）を占める。次いで1-3年の17件（22%）となっている。2022年に発生した事件で、3年以上にわたる長期間にわたり流出が継続した事件はなかった。

▼図1-6　2022年流出期間別事件数



かっこ・ｆｊコンサルティング調べ

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以下の表となる。サービスプロバイダ2社（決済代行事業者、カード会社）を除いた、A.加盟店の1事件あたりの平均流出期間は296.9日、1事件で流出したカード情報の平均件数は7,630件となっている。加盟店平均と比較して、コスメ、アパレルの２商材は事件数も多くかつ1事件あたりのカード情報流出件数が多くなっている。結果、加盟店から2022年に流出したカード情報のうち、75%がこの２商材 を取り扱う加盟店から流出しているが、平均流出期間はそれぞれ169.3日、165.8日と比較的短くなっている。

事件数で2位となっている食品は、平均流出カード情報流出件数は4,000件弱に留まっており、加盟店平均と比べると半分強となっている。一方で、平均流出期間は320日と加盟店平均よりも若干長い。

加盟店以外の業種については、図中B. 決済代行事業者が104日間分、460,829件のカード情報を流出させている。C.カード会社については、流出期間は8日間と公開されているが、カード情報流出件数については開示していない。

▼図1-7　2022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		52	389,121	296.9	7,630
加盟店取扱い商材別	①アパレル	9	127,248	169.3	14,139
	②食品	8	31,779	320.0	3,972
	③コスメ	6	164,006	165.8	27,334
	④ホビー	6	8,119	153.8	1,353
	⑤生活雑貨、家具、⑥インテリア	3	4,421	224.7	1,474
	⑦家電・電子機器・PC	2	2,457	184.5	1,229
	⑧自転車、バイク	1	3,360	275.0	3,360
	⑨食品/健康食品/コスメ	1	2,086	369.0	2,086
	⑩健康食品	1	4,636	446.0	4,636
	⑪その他ECサイト	15	41,009	411.6	2,734
B. 決済代行事業者		1	460,829	104.0	460,829
C. カード会社		1	非公開	8.0	非公開

かっこ・ｆｊコンサルティング調べ

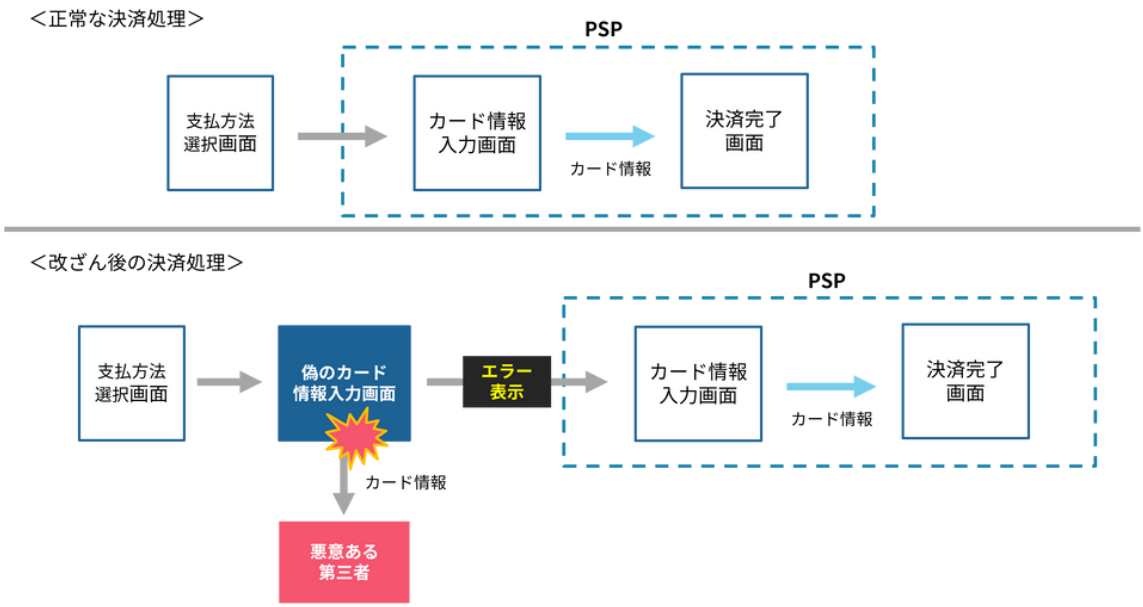
(2)-2. カード情報窃取の手口：カード情報入力画面のCSPを回避するオンラインスキミング

カード情報窃取の手口としては、2018年頃から、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が増えている。対面加盟店でカードを読み取るときに不正な装置を用いて券面の磁気ストライプ情報を盗み取る手法を「スキミング」というが、そのオンライン版ということで「オンラインスキミング」と呼ばれる。

具体的には、ECサイトの決済ページへのリンクを改ざんして偽の決済ページを挿入したり、決済ページに不正なJavaScriptを挿入することで、消費者が入力したカード情報を正規の決済代行事業者以外に、第三者にも送信する。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4.0版』（以下『ガイドライン4.0』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。

図1-8は、リダイレクト（リンク）型決済でオンラインスキミングが行われている例である。正常な決済処理（上）であれば、消費者が支払い方法を選択した後、決済代行事業者のサイトに設置されたカード情報入力画面が表示され、カード情報を入力して決済を完了する。改ざんされたサイト（下）では、支払方法選択画面からサイト内に設置された偽のカード情報入力画面が呼び出される。ここでカード情報を入力すると、悪意ある第三者にカード情報が窃取されるが、同時に「通信エラー」などのエラー画面が表示される。エラー画面で「次へ」等のボタンをクリックすると、決済代行事業者の正規のカード情報入力画面が表示される。そのまま手続きを進めると決済が正常に完了する。

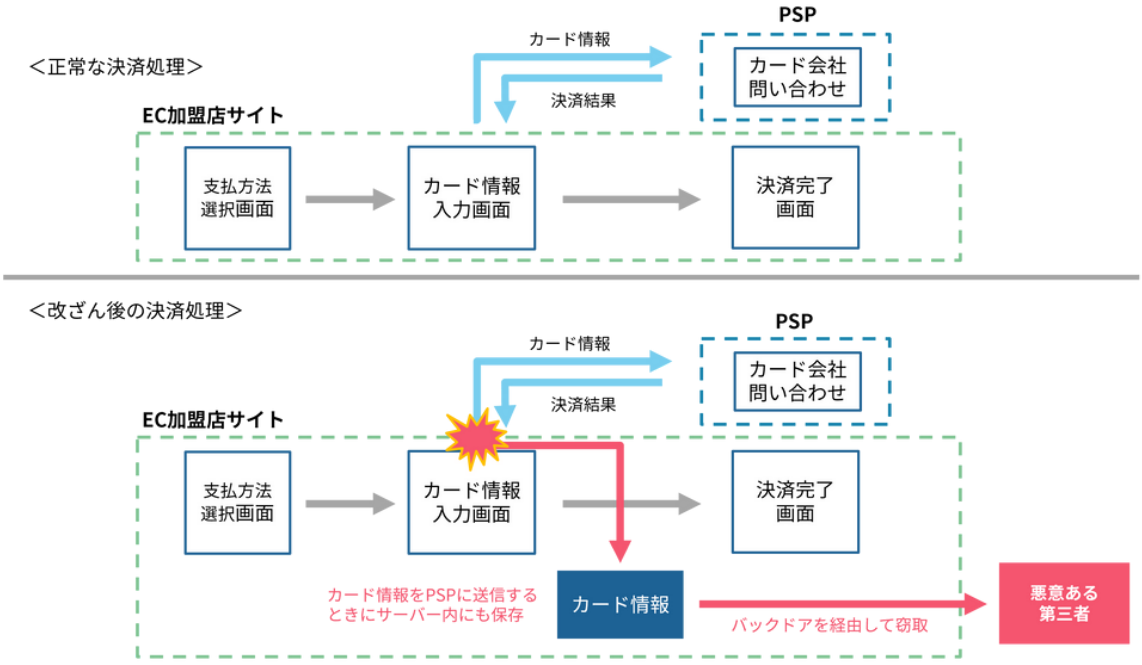
▼図1-8　リダイレクト（リンク）型決済で発生している事案（偽の決済フォームに遷移）



『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ｆｊコンサルティング作成

図1-9は、JavaScript型（トークン型）決済でオンラインスキミングが行われている例である。正常な決済処理（上）であれば、支払方法を選択すると、消費者のWebブラウザに読み込まれた決済代行事業者のJavaScriptによって、入力したカード情報が決済代行事業者に直接送信される。カード情報は決済代行事業者によってトークン情報に変換され、加盟店にはトークン情報をもとに決済が実行される。改ざんされたサイト（下）では、支払方法を選択すると、消費者のWebブラウザに加盟店サーバー内のファイルに書き込み保存する不正なJavaScriptが読み込まれる。消費者がカード情報を入力すると、不正なファイルへの書き込みと同時に決済代行事業者に送信され、正規の決済が実行される。攻撃者は、不正なJavaScriptを埋め込んだ際に使用したバックドアを経由してサーバー内のファイルを抜き取ることでカード情報を窃取する。

▼図1-9　JavaScript型（トークン型）決済で発生している事案
（消費者が入力したカード情報をEC加盟店サーバー内に保存）

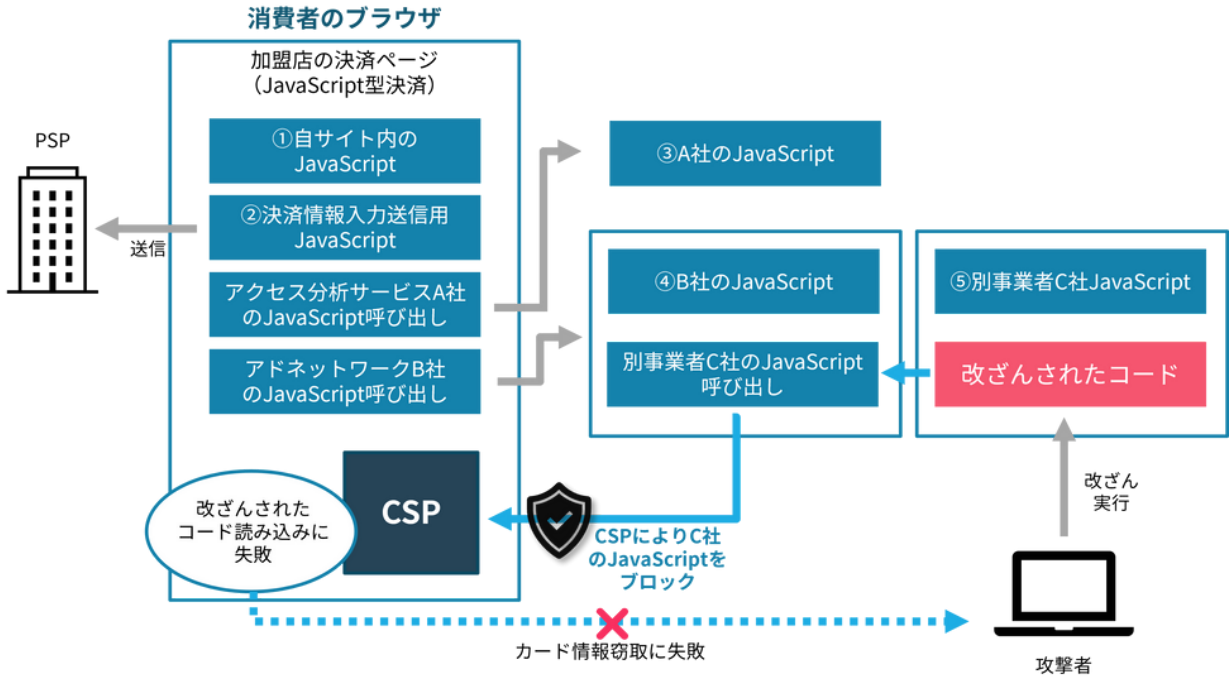


『クレジットカード・セキュリティガイドライン【4.0版】の記載を元にｆｊコンサルティング作成

以前は、決済情報ページに外部サイトの不正なJavaScriptを読み込ませて消費者のWebブラウザ上で実行することで、カード情報を攻撃者に送信する手口がよく見られた。対抗する方法として、CSP（Content Security Policy）のドメイン制御により明示的に許可したドメイン以外からのJavaScriptの読み込みを禁止する方法がある。図1-10は、消費者のWebブラウザに表示された決済ページに読み込まれているJavaScriptの例である。①自サイト内のJavaScriptは、ナビゲーションバーなどのスクリプトである。②決済情報入力送信用JavaScriptは、決済代行事業者が提供するカード情報送信用のJavaScriptである。これら以外にも、③アクセス分析サービスA社のJavaScriptや④アドネットワークB社のJavaScriptなどを決済ページの機能として読み込んでいる。ここで④が、さらに⑤別の事業者C社のJavaScriptを読み込んでいた場合、加盟店が知らないうちに⑤が消費者のWebブラウザ上で実行されることになる。すなわち、⑤が改ざんされてしまうと、加盟店が気づかないうちに消費者のWebブラウザに改ざんされたコードが読み込まれ、カード情報が第三者に送信されるようなことが起こり得る。

CSPのドメイン制御では、決済ページで実行できるJavaScriptとして、①～④の読み込み元のドメインを自ドメイン含め明示的に指定する。これにより、読み込みを意図していなかった⑤のスクリプトはCSPにより読み込みをブロックされる。結果、消費者のWebブラウザに改ざんされたコードが読み込まれることがないので、攻撃者はカード情報の窃取に失敗する。

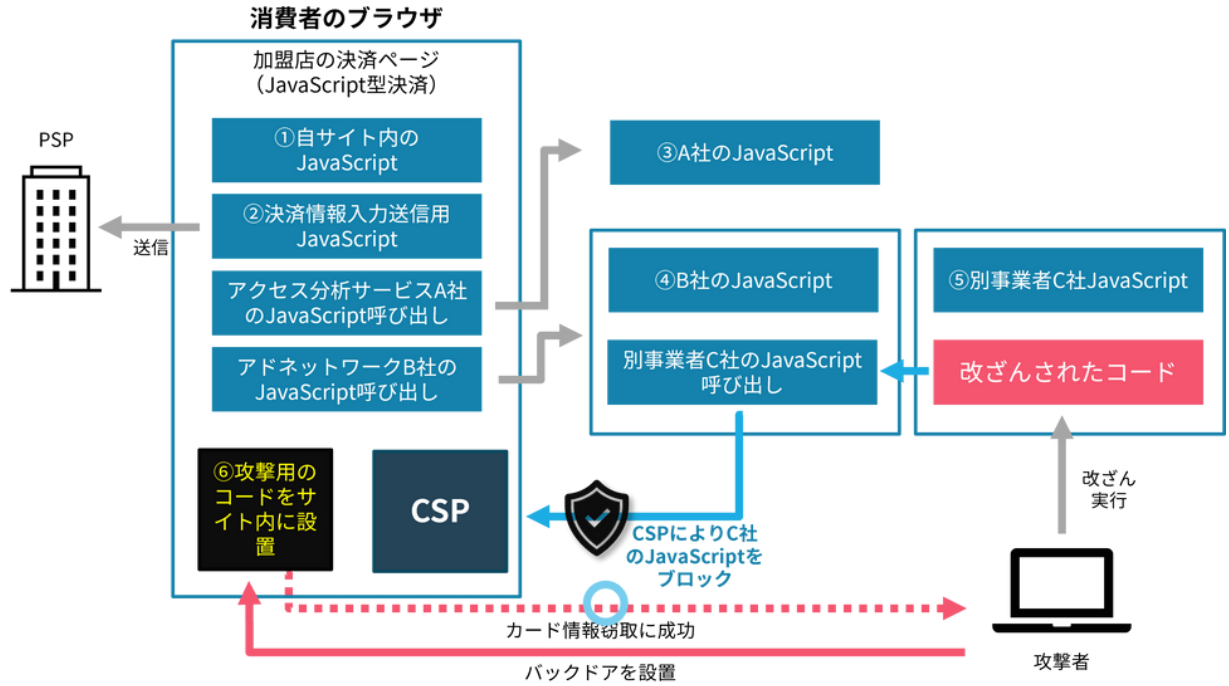
▼図1-10　CSPによるオンラインスキミングの防止



ｆｊコンサルティング作成

CSPの導入が進んだことで、外部JavaScriptを改ざんする形でのカード情報窃取がし難くなったことから、CSPを回避して情報窃取を図るために攻撃用のコードを自サイト内に設置する方法が多く見られるようになっている。図1-11では、攻撃者は加盟店のサーバーに侵入して⑥攻撃用のJavaScriptを設置する。自サイトのドメインはCSPのドメイン制御で許可されているので、自サイト内に設置された⑥のスクリプトも読み込まれ、実行される。これにより、攻撃コードが読み込まれ、カード情報が攻撃者に送信される。

▼図1-11　CSPを回避するオンラインスキミング攻撃



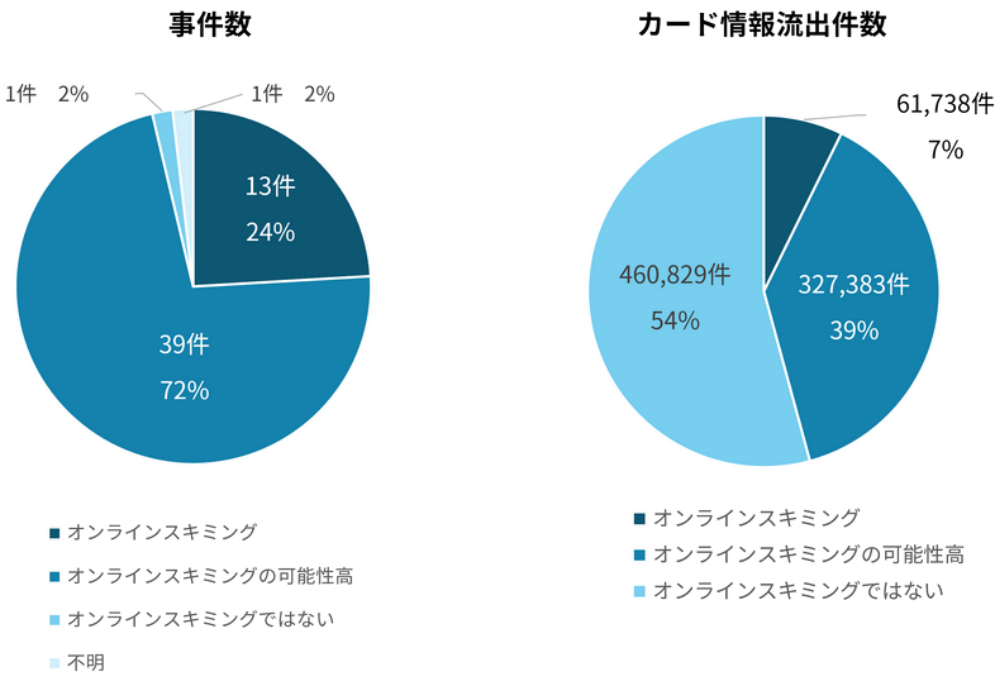
ｆｊコンサルティング作成

これを防ぐには、CSPやSRI（Subresource Integrity）により、スクリプトの読み込み先のドメインを制御するだけでなく、スクリプトの完全性を証明するハッシュ値を併用することにより、改ざんされたスクリプトを読み込まないように制御する対策が挙げられる。

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。そのためｆｊコンサルティングでは、2022年に公表された54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。

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SQLインジェクション等、オンラインスキミング以外の原因が明記されている。

▼図1-12　2022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



ｆｊコンサルティング調べ

2022年度に発生した54件のカード情報流出事件のうち、前述の決済代行事業者A社に対する攻撃、および加盟店のうち流出したカード情報の項目、流出期間、流出件数が不明の1件を除く52件は、全てオンラインスキミングか、もしくはその可能性が高いという結果となった。これらの事件によるカード情報流出件数は合計389,121件である。

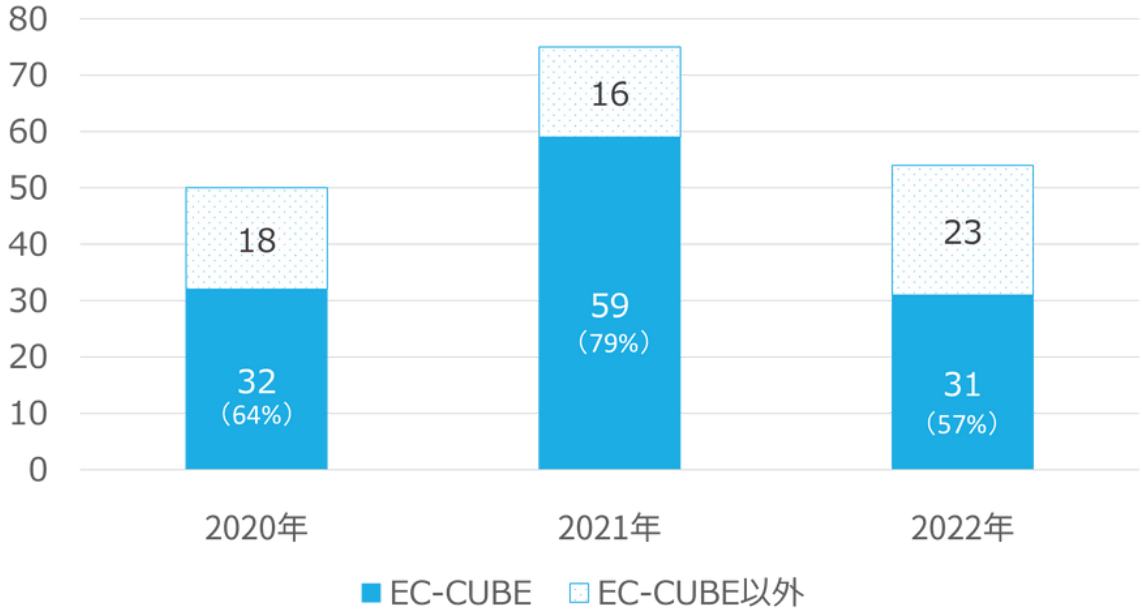
2018年以降、一度に大量のカード情報が流出する事件は減少傾向にあった。非保持化により大型の事件を防ぐ一定の効果があったといえる。一方で、非保持化対応済みのECサイトからもカード情報流出は続いており、非保持化だけではECサイトのセキュリティ対策は不十分である。非保持化対応済みの加盟店であっても、従業員に対するセキュリティ教育や脆弱性対策、ウイルス対策、管理者権限の管理、デバイス管理等の基本的なセキュリティ対策が求められる。

具体的な対策として、独立行政法人情報処理推進機構（IPA）がECサイトを構築・運用する中小企業向けのガイドラインとして、2023年3月に公開した『ECサイト構築・運用セキュリティガイドライン』を取りまとめた（詳細は3章を参照）。

(2)-3. プラットフォーム： EC-CUBE 4.0系にも被害が拡大

オープンソースのECプラットフォームとして国内でNo.1のシェアを占めるEC-CUBEについては、脆弱性が攻撃の対象となりやすいことから2019年12月には経済産業省から注意喚起の文書が公表されている。セキュリティ情報サイト「フォックスエスタ」の調査結果をもとに2022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31件（57%） に達している。2020年、2021年に比べると割合は減ったとはいえ、依然として半数以上を占める。

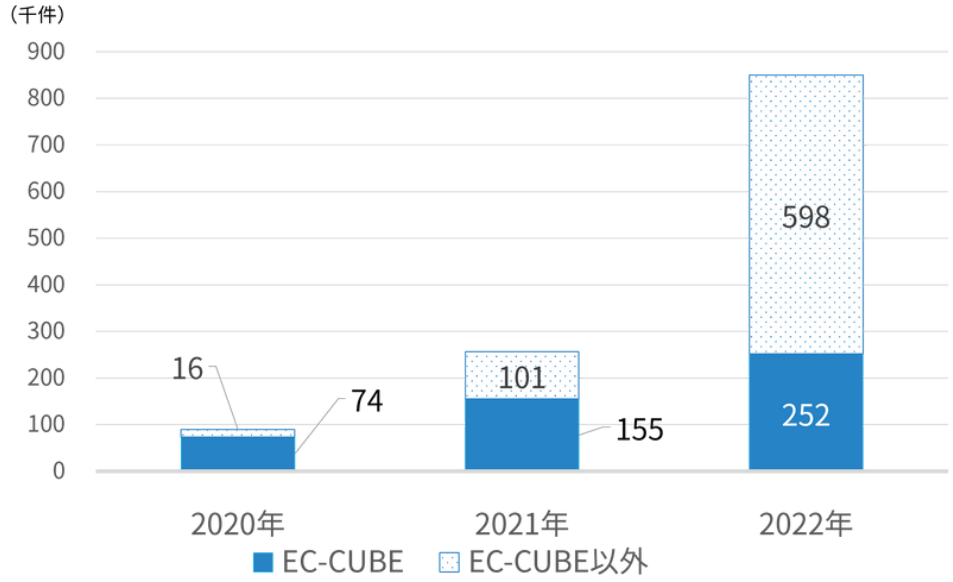
▼図1-13　2022年のカード情報流出事件　事件数に占めるEC-CUBEの割合



『フォックスエスタ』（https://foxestar.hatenablog.com/）調査結果をもとにｆｊコンサルティング作成

カード情報流出件数に占めるEC-CUBEの割合は251,766件（30%）となっている。2022年は決済代行事業者からの流出件数が半分以上を占めるため、一見、EC-CUBEの割合は減っているように見えるが、加盟店からのカード情報流出件数（389,121件）に対する割合は65%に達しており、2021年とほぼ変わらない。

▼図1-14　2022年のカード情報流出事件 流出件数に占めるEC-CUBEの割合

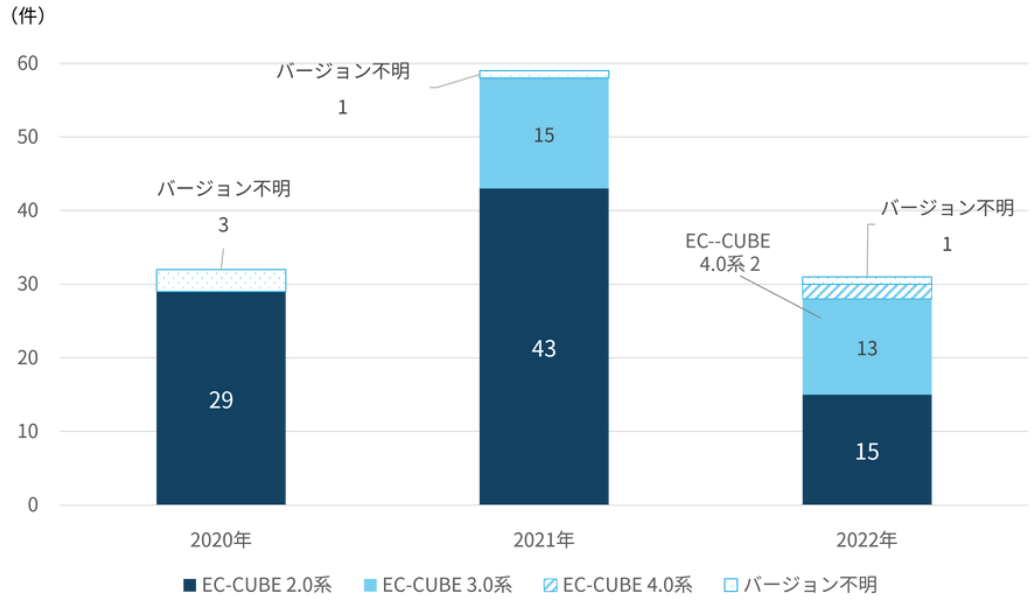


『フォックスエスタ』（https://foxestar.hatenablog.com/）調査結果をもとにｆｊコンサルティング作成

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1-17である。2020年以前は、EC-CUBE2.0系がほとんどを占めていたが、2021年には4分の1程度をEC-CUBE 3.0系が占めるようになった。2021年5月から6月にかけ、EC-CUBE 3.0系と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ており、これを悪用した攻撃と推定される。2022年は、事件数そのものは減っているものの、EC-CUBE 3.0系の割合が増加しており、さらにEC-CUBE4.0系が攻撃された例も出てきている。

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。

▼図1-15　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



『フォックスエスタ』（https://foxestar.hatenablog.com/）調査結果をもとにｆｊコンサルティング作成

(3)　2022年のカード情報流出事件のトピック：カード情報を直接扱わない事業者に対してもサプライチェーン攻撃が発生

加盟店のサイトそのものを攻撃するのではなく、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「サプライチェーン攻撃」が発生している。2022年は、2つのサプライチェーン攻撃が公表されている。

(3)-1. PCI DSS準拠済みの決済代行事業者A社

2022年2月、約46万件のカード情報の流出を公表した。前述の通り、これは2022年に流出したカード情報の半数以上を占める。影響を公表したECサイトなどの数は100を超えている。

決済代行事業者であるA社は、カード情報を取り扱うサービスプロバイダーであり、割賦販売法でPCI DSS準拠が義務付けられている。A社も求められる通りPCI DSSに準拠していたが、2022年6月に公表された第三者委員会報告書によれば、PCI DSS審査時に提出する脆弱性診断の報告書が改ざんされるなど、運用が適切に行われているとは言い難い状態であった。結果、A社はクレジットカード番号等の適切な管理のために必要な措置を講じていたとは認められないとして、経済産業省から業務改善命令を受けた。

『ガイドライン4.0』では、割賦販売法第35条の16第１項で、カード情報保護義務を負うセキュリティ対策の実施主体者として挙げられた1号～7号事業者を図1-18のように定義している。

図1-16にある通り、『ガイドライン4.0』では、２号事業者（加盟店）以外のカード情報保護義務を負う事業者に対してPCI DSS準拠・維持を求めている。カード情報保護対策としてPCI DSSに準拠する事業者は、年１回の外部審査や自己問診のクリアを目的化するのではなく、顧客から預かっているカード情報を保護するという本来の目的を再認識することが求められる。

A社は業務改善命令に対する改善措置を実施しつつ、カード情報を取り扱うシステムについてPCI DSSの再審査を進め、2023年1月以降順次サービスを再開している。

▼図1-16　カード情報保護義務を負うセキュリティ対策の実施内容

	『セキュリティガイドライン』内での名称	業種の例示	認められるカード情報保護対策	
			非保持化	PCI DSS
1号事業者	カード発行会社（イシュアー）	カード発行会社（イシュア）	-	●
2号事業者	加盟店	加盟店（対面/非対面）	●	●
3号事業者	カード会社（アクワイアラー）	加盟店契約カード会社（アクワイアラ）	-	●
4号事業者	決済代行業者等	● 決済代行業者で包括代理契約を締結している事業者（対面/非対面取引双方） ● ECモール事業者（デジタルプラットフォーマーなど） ● SC、百貨店（消化仕入れを除く）ショッピングモール等（対面取引） ● 包括代理を行なっている商店街組合（対面取引）等	対面取引のみ取扱う事業者の一部（※1）	●
5号事業者	QRコード決済事業者等	● QRコード決済事業者 ● スマートフォン決済事業者 ● ID決済事業者等 ※名称にかかわらずカード情報と紐づけた他の決済用番号で決済を行う事業者	-	●
6号事業者	5号事業者の委託会社	第5号事業者からカード情報の管理を受託している事業者	-	●
7号事業者	加盟店向け決済システム提供事業者	● EC システム提供会社（アクワイアラーとの契約有無にかかわらず、決済システムを運営しEC加盟店にサービスとして提供する事業者。ASP/SaaSとしてEC事業者にサービス提供する事業者、EC事業者に購入プラットフォームを提供する事業者）等 ※カード会員データの伝送処理保存を行っている事業者、決済代行会社又はアクワイアラーに接続できる決済モジュールを提供している事業者も含まれる。	-	●

※1 合わせて協議会が定める「セキュリティ対策チェック項目」に基づく対策が必要
『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ｆｊコンサルティング作成

(3)-2. Webマーケティング支援ツール提供会社 J社

もう一つのサプライチェーン攻撃は、2022年10月に公表された、Webマーケティング支援ツール提供会社J社に対する攻撃である。J社が提供するサービスは、会員登録画面や決済画面などの入力フォームのエラーチェックや、PCサイトの表示をスマートフォン用に最適化するものであり、直接カード決済処理には関わらない。しかし、当該サービスのプログラムコードが改ざんされたことで、 入力フォームから送信した内容が悪意のある第三者に送信されるようになっていた。

当該サービスは5,000サイト以上での導入実績があり、個人情報を入力するフォームでサービスを利用していた複数のサイトから個人情報が流出した。うち、カード情報を入力するページで当該サービスを利用していたとして、カード情報の流出を公表したのは2023年8月時点で11社12サイトに上る。

▼図1-17　Webマーケティング支援ツール提供会社J社起因のカード情報流出状況

	公表年月	サイト	流出件数	流出期間
1	2022/10	カード会社 K社（会員向けサイト）	非公開	2022/7/19～2022/7/26
2	2022/10	通信教育サービス L社	200	2022/7/24～2022/7/26
3	2022/10	アパレル販売 M社	2,298	2022/7/24～2022/7/26
4	2022/10	カメラ・写真用品販売 N社	519	2022/7/19～2022/7/29
5	2022/10	写真プリントサービス N社（4.と同じ企業）	851	2022/7/19～2022/7/29
6	2022/11	飲料販売　O社	8,094	2022/7/19～2022/7/29
7	2022/11	食品メーカー公式通販　P社	164	2022/7/19～2022/7/29
8	2022/11	書籍販売　Q社	427	2022/7/19～2022/7/28
9	2023/ 1	コスメ販売 R社	2,259	2022/7/19～2022/7/26
10	2023/ 1	レンタルWi-Fi サービス S社	15	2022/7/24～2022/7/26
11	2023/ 1	コスメ・雑貨販売　T社	37	2022/7/19～2022/7/2
12	2023/ 1	アパレル・コスメ販売　U社	605	2022/7/19～2022/7/29

かっこ・ｆｊコンサルティング調べ

J社は、カード情報処理には関わっていないため、前述の割賦販売法で定める1～6号事業者いずれにも該当しない。さらに当該サービスはクレジットカード決済機能や決済代行事業者に接続する決済モジュールを提供しているわけではないので、７号事業者にも該当するとは言い切れない。

『ガイドライン4.0』では、セキュリティ対策の実施主体者がカード情報を取り扱う業務を外部委託する場合、委託社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準拠等の必要な対策を求めるとしている。とはいえ、J社の提供していたサービスは、フォーム送信前の入力支援や、Webブラウザ にあわせたスタイルシート最適化といった機能を提供するものであり、利用していた加盟店やカード会社には「カード情報を取り扱う業務を外部委託している」という認識はなかったと思われる。 だが現実には、当該プログラムの改ざんにより想定外に不正な者にカード情報が流出することとなった。

このような「直接カード情報は取り扱わないが、カード情報を入力するページのセキュリティに影響を与えるサービス」を提供する事業者に対しても、何らかのセキュリティ対策を求める必要がある。しかし、PCI DSS準拠等のセキュリティ対策を求めることは、現行法やガイドラインの下では難しいと考える。こういった事案に対応するために、どのような対策を求めるのか、法整備やガイドライン改訂など検討していく必要がある。

2．2022年のECサイトにおける不正利用の概況

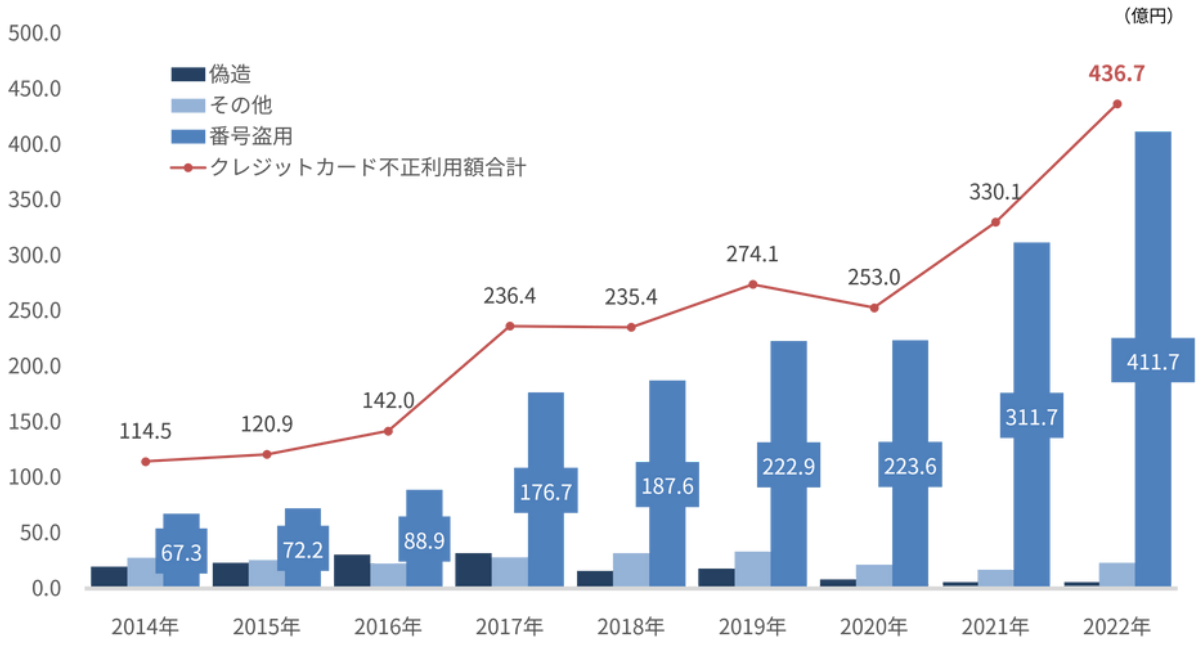
（1）クレジットカード不正利用被害額の推移

(1)-1 2022年のクレジットーカード不正利用被害額と傾向

2022年の年間不正利用額は436億円となり、前年に比べて100億円増加した。これは2014年の不正利用額の3.8倍に相当しており被害は増加を続けている。特に注目すべきは、この被害の94.3%が番号盗用によるものであり、多くはECサイトでの不正注文によるものである。[不正注文とは、クレジットカード不正の場合は、他人のクレジットカード情報を使いECサイトにて、第三者がなりすまして決済する行為で、それ以外にも転売不正、あと払いの未払いなどがある。ECサイトでのクレジットカードの番号盗用被害の増加傾向 に対処するため、経済産業省は「クレジットカード・セキュリティガイドライン」 を策定し、指針対策を定めている。

主なポイントとしては、「高リスク商材取扱加盟店（オンラインゲームを含む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主たる商材として取り扱う加盟店）」および「不正顕在化加盟店（アクワイアラ（加盟店契約カード会社）各社が把握する不正利用金額が３ヶ月連続50万円を超える加盟店）」における対策の強化だ。高リスク商材取扱加盟店は、セキュリティを強化するための4つの方策（券面認証、本人確認、属性・行動分析、配送先確認）の内1方策以上を導入する必要があり、不正顕在化加盟店は2方策以上の導入が求められている。さらに、2023年3月に公開された『ガイドライン4.0』では、高リスク商材取扱加盟店と不正顕在化加盟店以外も含む全ての加盟店に対して、2025年3月末を期限としたEMV 3-Dセキュア(以後EMV3DS)の導入が指針対策として明示された。

▼図2-1　クレジットカード不正利用被害額の推移



日本クレジットカード協会「クレジットカード不正利用被害の発生状況」

(1)-2 クレジットカード不正利用被害増加の要因

オンラインショッピングの利用者が急増している 。市場の成長に伴い、不正注文も増加した。その一方、不正アクセスやフィッシング、クレジットマスターなどによりクレジット カード情報などの流出が増加し、システムの脆弱性対策不足も顕著である。2020年以降、新型コロナウイルス感染症拡大により、クレジットカードにおける2020年から2022年の不正発生率は約2倍になっていた。(図2-2)

市場の成長に伴い、ECサイトの新規事業者も増加している。新規参入事業者の中には、セキュリティ対策が不十分なケースも多く、攻撃者の標的になりやすい傾向がある。また、（2）-2で述べる通り、企業規模によっても不正利用の対策状況に差があるのが実態である。これらの要因が組み合わさり、クレジットカードの不正利用が大幅に増加したと考えられる。新規参入事業者や小規模事業者は、予算やリソースに制約があるため、まず自社のリスクを理解し、最適な対策を考える必要がある。たとえば、現時点では不正被害が少ない場合でも、換金性の高い商品や人気商品、限定商品等に関しては配送先住所が存在するか、電話番号の疎通があるかを確認するなど、自社でできる範囲の対策を検討するべきである。また、自社の対策だけでは不十分な場合、不正検知サービスを利用するなど、状況に応じた対策方法を選択することが、今後のセキュリティ対策のポイントとなる。

（2）ECサイトにおける不正注文の傾向

(2)-1「O-PLUX」導入加盟店における不正注文の傾向

▼図2-2　クレジットカード不正利用発生率及び転売不正発生率

クレジットカード不正利用	年度	転売不正	年度
2020年	0.9%	2020年	1.3%
2021年	1.2%	2021年	1.4%
2022年	1.6%	2022年	2.5%

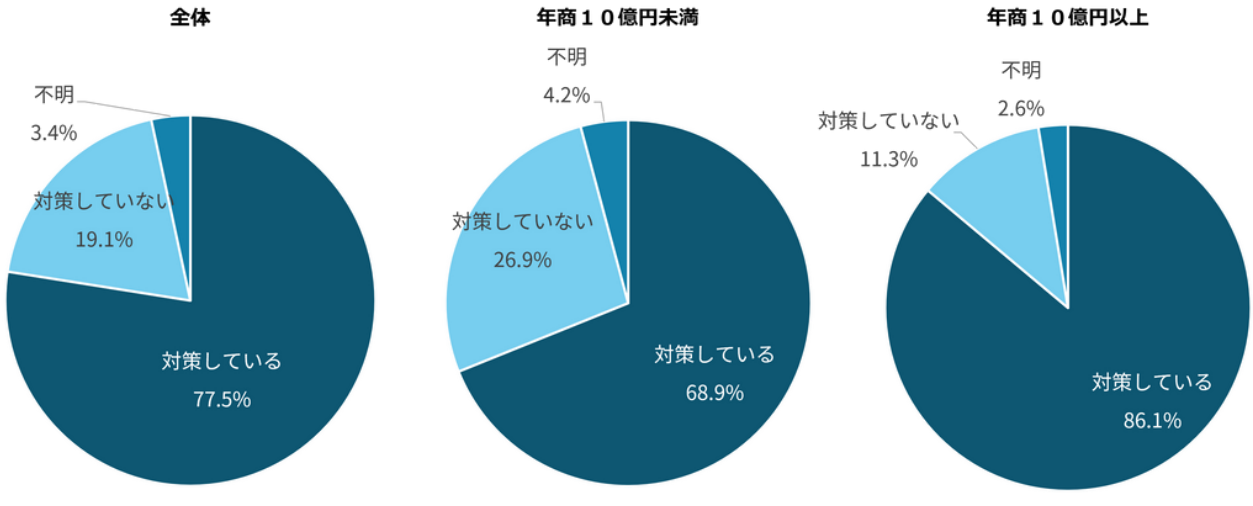
※「O-PLUX」の審査で、審査件数全体に占めるクレジットカード不正注文/不正転売の審査結果NG割合を件数ベースで算出。（かっこ調べ）
※最終的に出荷停止や注文を拒否するなどの対応は、「O-PLUX 」加盟店判断により異なる。

(2)-2 EC事業者の不正注文対策状況

2022年12月、かっこ社では「EC事業者実態調査」として、EC事業者530社で不正利用対策に携わる担当者を対象に、セキュリティ意識や不正対策の実態について調査を実施した。全体で見ると77.5%が不正注文対策をしている。年商別に見ると、年商10億円未満のEC事業者の対策実施率は68.9％にとどまる一方、年商10億円以上の事業者は86.1%が対策を実施している。(図2-3)

▼図2-3　EC事業者の不正注文対策状況

Q：クレジットカード不正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（かっこ調べ）2022年12月調査

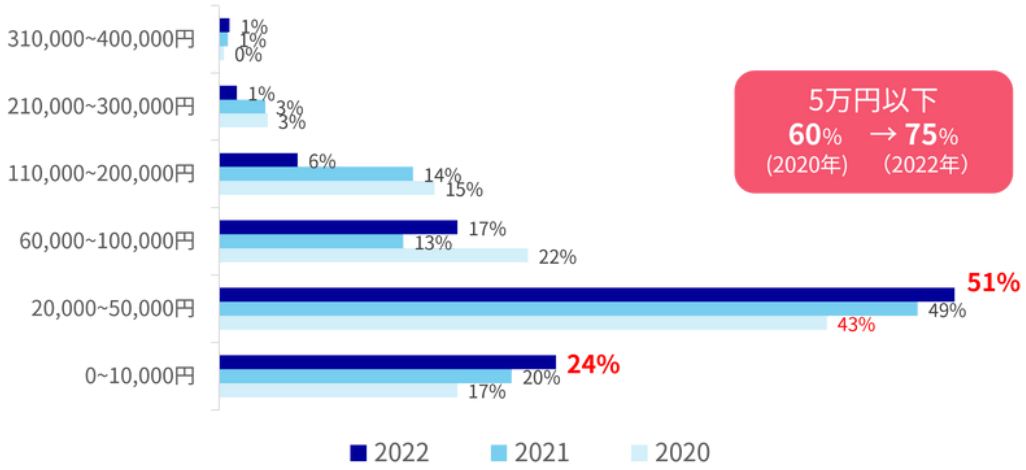
（3）2022年のECサイトにおける不正利用のトピック

(3)-1 クレジットカード不正利用における注文金額の低額化及び狙われやすい商材

2022年はクレジットカード不正利用において、注文金額が低額化している傾向があった。かっこ社の調べによると、2020年は5万円以下が全体の60%だったのに対し、2022年は75%に増加していた。(図2-4)

2022年において、クレジットカード不正利用で狙われやすい商材においては、「クレジットカード・セキュリティガイドライン」で高リスク商材取扱店に指定されているデジタルコンテンツ、家電、旅行などで不正が多い傾向があった。ここ3年で共通するのはホビー・ゲームが毎年上位となっている。巣ごもり需要の高まりもあり、市場における転売価値が上がり不正が増えたと推測ができる。(図2-5)

▼図2-4　クレジットカード不正利用の注文金額



「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（かっこ調べ）

▼図2-5　EC事業者の不正注文に狙われやすい商材ランキング変遷

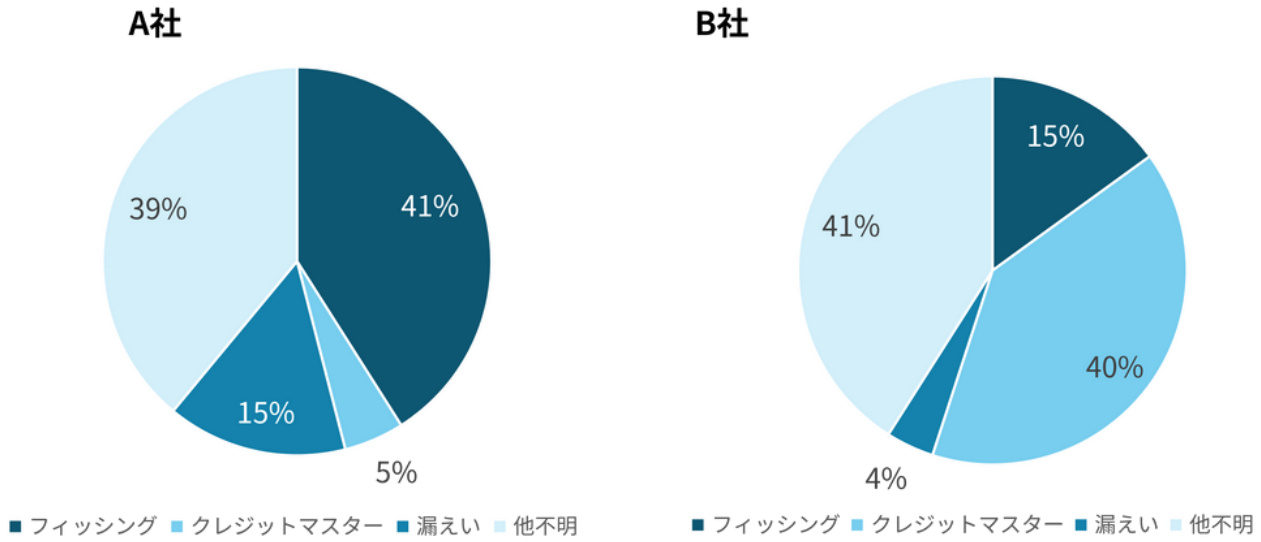
順位	2020年	2021年	2022年
1	MVNO	ホビー・ゲーム	デジタルコンテンツ
2	ホビー・ゲーム	デジタルコンテンツ	ホビー・ゲーム
3	コスメ・ヘアケア	チケット	旅行
4	アパレル	健康食品・医薬品	コンタクト・メガネ
5	家電・PC・タブレット	コスメ・ヘアケア	チケット
6	EC総合通販	コンタクト・メガネ	健康食品・医薬品
7	ベビー用品	食品・飲料・酒類	コスメ・ヘアケア
8	テレビ総合通販	美容機器	食品・飲料・酒類
9	アウトドア	MVNO	EC総合通販
10	サブスクサービス	PC・タブレット＆家電	家電・PC・タブレット
11	ペット用品	EC総合通販	アパレ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

※「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（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。

(3)-2 クレジットカード不正利用の手口の多様化

クレジットカード不正利用の手口においては、多様化、巧妙化の傾向はこれまでと変わらないが、目立った傾向としてはフリマアプリやオークションサイトを悪用した不正注文が急増した。また、クレジットカード不正利用増加の主たる要因は、加盟店や決済代行事業者などからのカード情報流出と考えられていたが、最近ではその傾向に変化が出ている。あるカード会社2社の調査（図2-６）では、カード番号の規則性を利用し総当たりで番号を割り出すクレジットマスターやフィッシングに起因する不正利用がカード情報流出を上回るという報告がされている。

▼図2-6　カード会社2社における番号盗用の不正手口の割合（件数ベース）



※A社2021年暦年、B社は2021年度で集計
※第２回 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（2022年9月） 日本クレジット協会提出資料を元に作成

(3)-3 クレジットマスターによる被害

クレジットマスター（クレマス）は以前からある手口だが、近年被害が増加している。クレジットカード番号の規則性にしたがって、bot等を利用し他人の番号を割り出す手法で、カード情報が使えるかどうかを確認するため、ECサイトの決済ページや会員登録ページが悪用される。事業者にとっての主な被害は以下の3点である。

①カード情報が割り出されればカードの不正利用につながる。
②無駄なオーソリゼーション費用が発生する。
③大量のアクセスが発生するため、ECサイトへの負荷がかかり売上機会の損失が発生する。

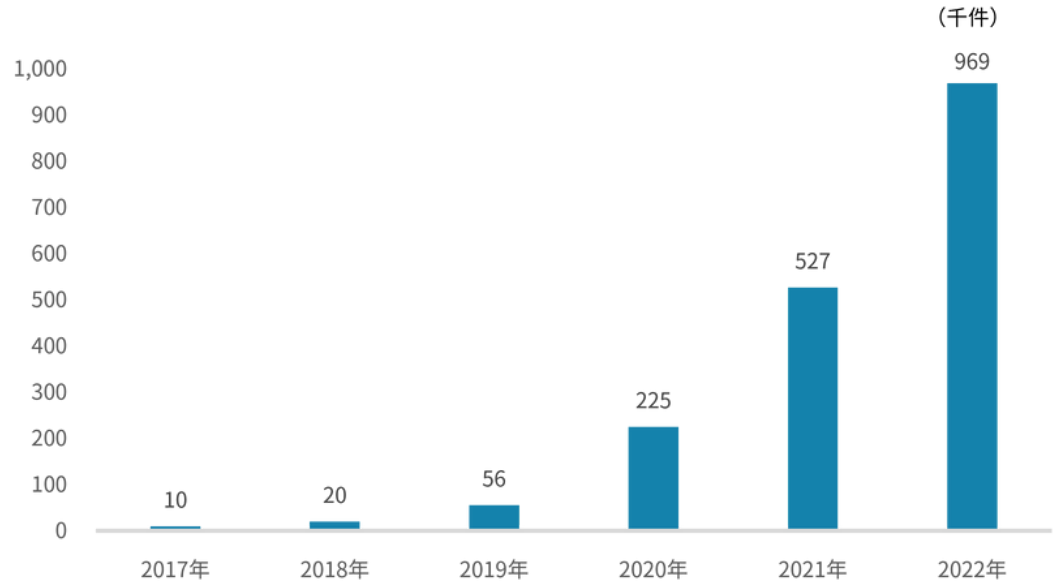
なかには、十数万件のクレマス攻撃や数十～数百万円にも及ぶ無駄なオーソリゼーション費用が発生するケースも確認された。攻撃対象としてECプラットフォームを狙うケース もあり、一度に大量のカード情報を詐取しようとしている傾向があることもうかがえる。現状の対策方法としては、カード決済における利用回数制限、アクセスがbotかどうかを判断するGoogleが提供する無料ツール「reCAPCHA」の導入、外部からの大量アクセスを検知するWAF(Web Application Firewall)の利用、不正検知サービスの利用などが挙げられる。

(3)-4 フィッシングによる被害

フィッシング対策協議会によると、フィッシング被害の報告件数は2017年～2022年の5年間で約100倍に増加している。ターゲットになりやすいサイトで最も多いのはネット通販などのECサイト、続いてキャリアなどの通信事業者、次にクレジットカード会社を装ったフィッシングサイトとなっている。これらに共通するのは、日常的に利用するサービスで利用者が多く、大手企業がサービス提供しているなどユーザーがだまされやすい点である。さらには、こういったサイトにはIDやパスワード等の個人情報やクレジットカード情報が含まれることも多く、不正な者がフィッシングで個人情報やカード情報の詐取を狙っていることが見てとれる。

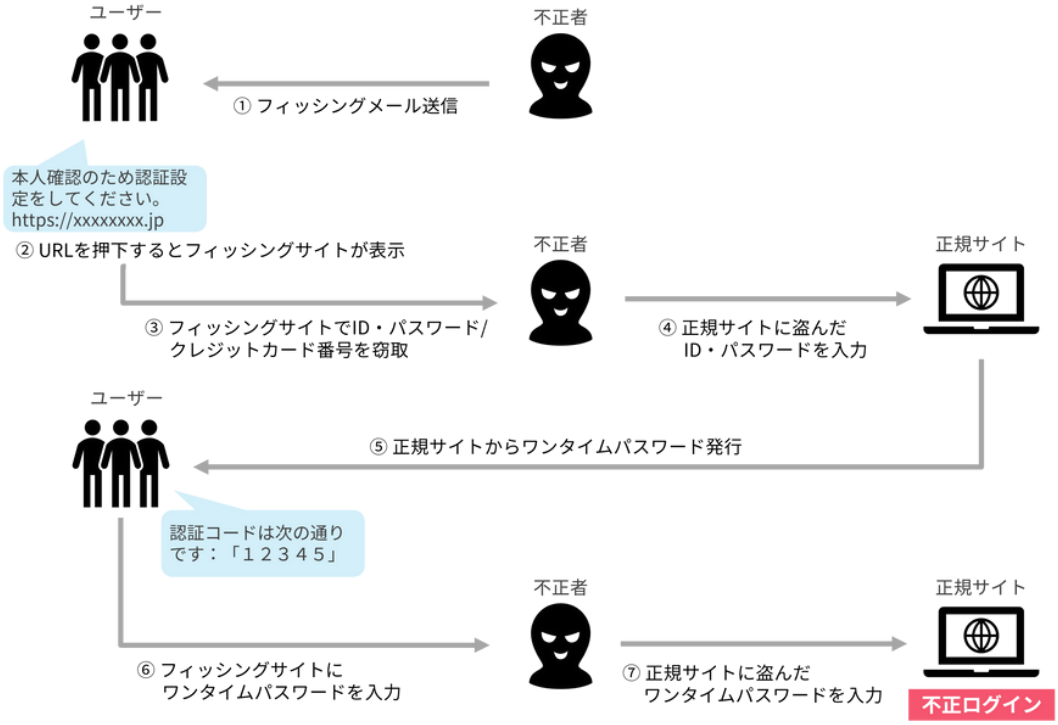
フィッシング手口は巧妙化しており、ワンタイムパスワードですら1万件以上が突破されたケース が確認されている。これは正規サイトとユーザーの間にフィッシングサイトを中継させる中間者攻撃 （図2-8を参照）といわれるもので、入手したIDなどの個人情報を悪用し、不正ログインされ金銭を振り込ませる詐欺も確認されている。

▼図2-7　フィッシング報告件数推移



フィッシング対策協議会「フィッシング報告状況（月次報告書）」を元にかっこ作成

▼図2-8　中間者攻撃



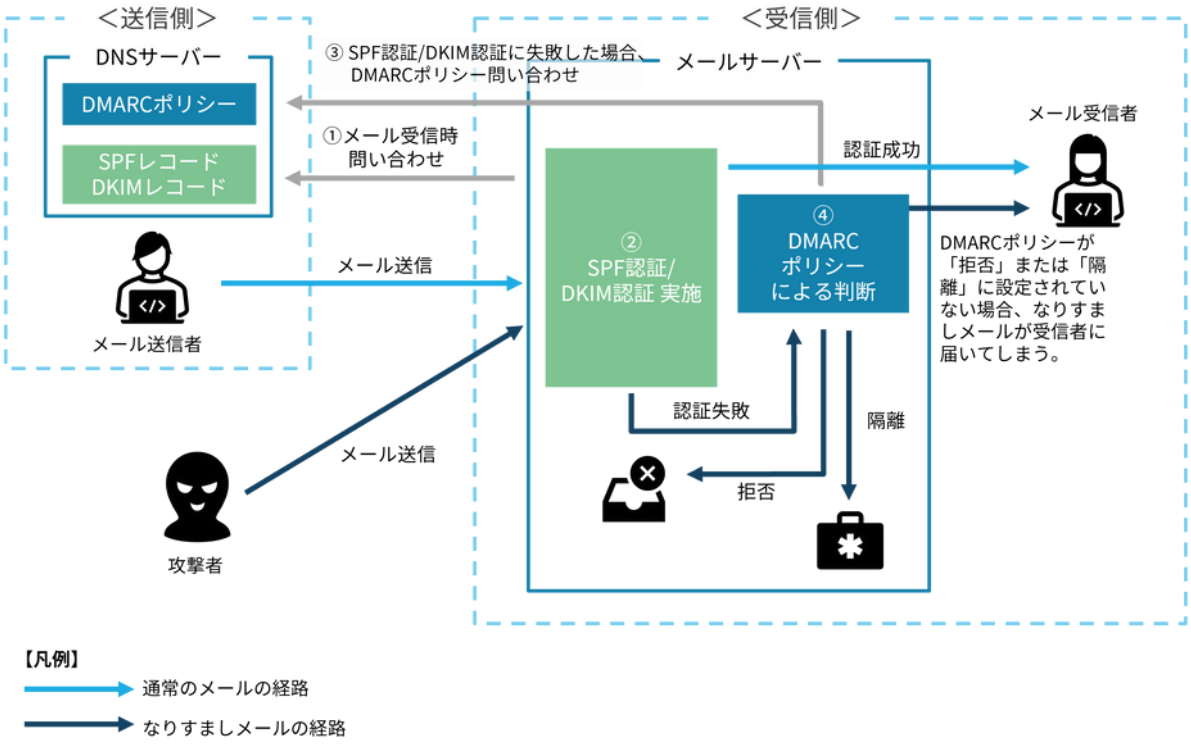
かっこにて作成

（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の取り扱いを、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、送信者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2-9　メール送信元によるフィッシング対策



ｆｊコンサルティング作成

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。フィッシング対策のためにDMARCが効果がある話を先に書く必要がある。

要望の背景には、2023年1月に経済産業省が公表した『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、イシュア（カード発行会社）に対してDMARC導入を含めた、なりすまし対策の強化を求めたことが挙げられる。

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。実際にイシュアがどの程度DMARCを導入しており、どのようなポリシーで運用しているかを調べるために、以下の通り調査を行った。

＜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（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

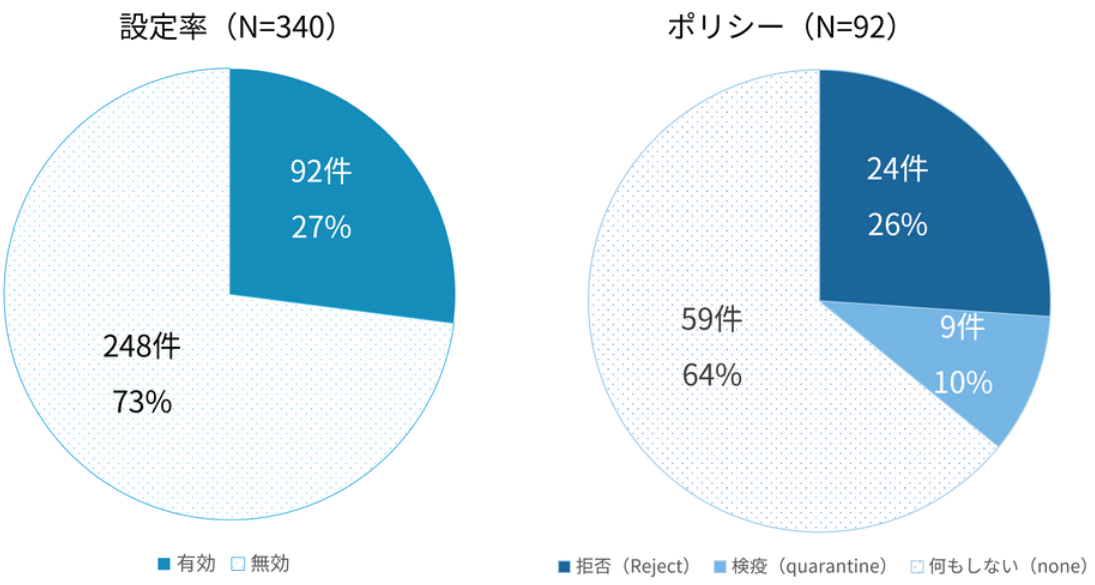
＜調査実施時期＞
2023年8月上旬

＜調査結果＞
1. 対象ドメインの確定
246社のイシュアに対し、コーポレートサイトのドメイン、およびWebサイトなどで「メール受信設定のお願い」等で案内されている「受信許可が必要なドメイン」を「メール送信元として利用しているドメイン」とみなして収集したところ、340ドメインが抽出された。

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、調査対象に含めることとした。

2. ドメインのDMARC対応状況と運用ポリシー
340件の対象ドメインに対してDNSレコードを調査したところ、有効なDMARCレコードが設定されていたのは92件（全体の27%）であった。この92件のDMARCポリシーの内訳は、最も厳しい「拒否（reject）」が24件（実施済み企業の26%）、「検疫（quarantine）」が9件（10%）だった。残りの59件（64%）は、DMARCは設定されているもののなりすましメールの受信拒否はしない「何もしない（none）」に設定されている。

▼図2-10　イシュアのメール送信元ドメインのDMARC設定状況（2023年8月）



ｆｊコンサルティング調べ

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。

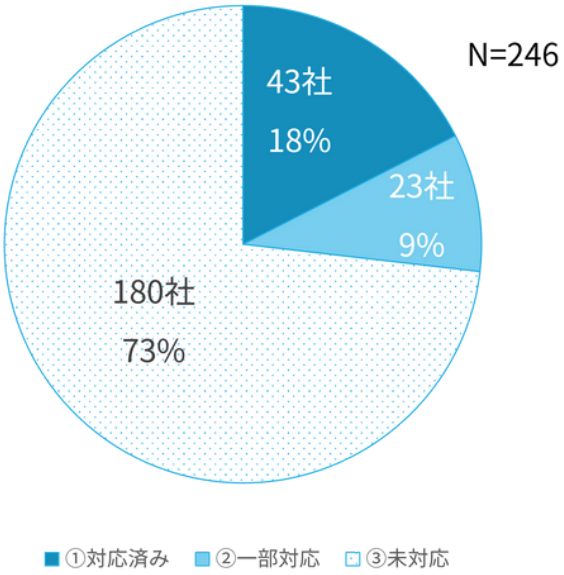
①対応済み：メール送信元として使用しているドメイン全てにDMARCレコードが設定されている。

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。

結果、246社中「対応済み」は43 社（18%）、「一部対応」は23社（9%）であり、7割以上のイシュアがDMARCにまだ対応していない。

▼図2-11　イシュアにおけるDMARC対応状況（2023年8月）



ｆｊコンサルティング調べ

4. 総括

日経225企業を対象としたTwoFive社の調査によれば、対象企業の62%が少なくとも1つのメール送信元ドメインでDMARCを導入しているという。比べるとイシュアのDMARC導入率は半分以下で、監督官庁からの要望が出されているにもかかわらず、比較して低い割合に留まっている。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、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

DMARC設定が不適切な場合、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

今回の調査で、イシュアが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とが明らかとなった。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。DMARCポリシーによって消費者へのフィッシングメールの到達を防いでも、「よく似た紛らわしいドメイン」のメールについては効果が無い。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. 制度・政策の動向

（1）セキュリティ対策強化検討会と クレジットカード・セキュリティガイドライン改訂

クレジットカード不正利用の増加が止まらないことを受け、経済産業省は2022年8月から6回にわたり「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」を開催し、2023年1月に報告書をとりまとめた（以下『セキュリティ対策強化検討会報告書』）。

その内容は、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『ガイドライン4.0』にも反映されている。ガイドライン4.0に追加された新たな施策や『セキュリティ対策強化検討会報告書』から読み取れる今後の方向性について概観する。

(1)-1. 非保持化済みEC加盟店に対する セキュリティ対策チェックリストの導入

国内のEC加盟店のほとんどが、カード情報保護対策として自社のシステムにカード情報を保存・処理・通過しない「非保持化」を選択していることは前述の通りである。

非保持化済達成済みのEC加盟店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加盟店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（加盟店契約カード会社）や決済代行事業者に申告する制度の試行が開始された。『セキュリティ対策強化検討会報告書』ではEC加盟店の脆弱性対策をアクワイアラ等による加盟店管理義務の対象とするため、チェックリストの調査項目EC加盟店全般に拡大し、2024年度末までにガイドラインに追加することを当面の対応とした。セキュリティ対策要件の参考として、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』を挙げている。『セキュリティ対策強化検討会報告書』では併せて、2025年4月以降、アクワイアラ等の加盟店管理の実施状況について監督を監視する方針を示している。

▼図3-1　ECサイトの構築時、運用時それぞれにおけるセキュリティ対策要件

要件No	セキュリティ対策要件（構築時）	区分
1	「安全なウェブサイトの作り方」及び「セキュリティ実装チェックリスト」に準拠して、EC サイトを構築する。	必須
2	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須
3	EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。	必須
4	管理者画面や管理用ソフトウェアへ接続する端末を制限する。	必須
5	管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。	必須
6	クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドラ イン」を遵守する。	必須
7	サイト利用者情報の登録時及びパスワード入力時における、不正ログイン対策を実施する。	必須
8	サイト利用者の個人情報に対して安全管理措置を講じる。	必須
9	ドメイン名の正当性証明と TLS の利用を行う。	必須
10	サイト利用者のログイン時における二要素認証を導入する。	必須
11	サイト利用者のパスワードの初期化及び変更といった重要な処理を行う際、サイト利 用者へ通知する機能を導入する。	必須
12	Web サーバや Web アプリケーション等のログや、取引データ等のバックアップデータを保管する。	必須
13	保管するログやバックアップデータを保護する。	推奨
14	サーバ及び管理端末において、セキュリティ対策を実施する。	推奨

要件No	セキュリティ対策要件（運用時）	区分
1	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須
2	EC サイトへの脆弱性診断を定期的及びカスタマイズを行った際に行い、見つかった脆弱性を対策する。	必須
3	Webサイトのアプリケーションやコンテンツ、設定等の重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う	必須
4	システムの定期的なバックアップの取得及びアクセスログの定期的な確認を行い不正アクセス等があればアクセスの制限等の対策を実施する。	必須
5	重要な情報はバックアップを取得する。	必須
6	WAF を導入する。	推奨
7	サイバー保険に加入する。	推奨

※「ECサイト構築・運用セキュリティガイドライン」独立行政法人情報処理推進機構

(1)-2. モバイルデバイスを利用した決済のセキュリティ対策

対面加盟店では、従来使用されていたPOSレジに代わってスマートフォンやタブレットなどの汎用モバイルデバイスに専用の決済端末を連携してカード決済を実現するmPOSや、決済端末を使用せず市販のスマートフォンやタブレット単体で非接触決済を実現するMPoCの利用が増えている。EC加盟店でも、スマートフォンアプリを提供して、Webサイトを利用せず決済代行業社等が提供するSDKを通してアプリ内で決済を行う方式が増えている。こうした状況を受け、『ガイドライン4.0』の付属文書として『スマートフォン・タブレット等のアプリを利用した決済に関するセキュリティ対策の技術要件について』が関係事業者向けに公表された。汎用モバイルデバイスを利用する際の決済端末や通信のセキュリティについて、技術要件が記載されている。

『ガイドライン4.0』では、EC加盟店の非保持化の方策にスマホアプリ等のSDKを使用する場合は本技術要件を参照することが追記された。また、対面加盟店の非保持化導入方策の内回り方式の導入例に、PCI SSC（PCI DSS等のクレジットカードセキュリティの管理・運用を行う機関）が制定した「PCI MPoC認定ソリューション」が追加された。

(1)-3. 全てのEC加盟店に対し2025年3月末のEMV 3Dセキュア導入義務化へ

『クレジットカード・セキュリティガイドライン』では、EC加盟店における不正利用対策の具体的方策として、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つを挙げ、不正利用発生のリスクに応じて導入を求めていた。しかし、不正利用が増え続けていることを受け、さらなる対策強化として、2025年3月末を期限としてEMV 3Dセキュア（以下EMV3DS）を原則全てのEC加盟店に導入することを義務付けるとした。これまでは善管注意義務とオーソリゼーション処理の体制整備が課されていたのみであった、不正利用が顕在化していないEC加盟店や高リスク商材を取り扱わないEC加盟店についても対応が必要となる。

EMV3DSはデバイス情報や利用者から提供される個人情報等を活用して本人の利用であるかどうかを判定し、リスクに応じた認証を行う「リスクベース認証」がベースとなる本人認証手段である。リスクが低いと判定された取引については、ID・パスワードの追加入力不要で取引が実行できる。一方、リスクが高いと判定された取引にはチャレンジモードとして追加認証を要求する。その際の認証も、生体認証やワンタイムパスワードなど、固定パスワード以外の認証方法を採用することを求めている。EMV-3DS導入の現状と課題についてはこの後詳述する。

(1)-4. 不正利用情報の共有に向けた検討を開始

現状イシュア（カード発行会社）各社は、取引ごとに個別に過去の取引履歴等の情報から不正利用か否かを判断するオーソリゼーションモニタリングのためのシステムを導入しており、不正検知精度の向上が課題となっている。『セキュリティ対策強化検討会報告書』では、イシュア間の不正利用情報の共有化により、不正検知がより精度高く効率的に行えることを期待している。当面の対応としてはAI等による不正利用検知にも活用できるよう、イシュア間で不正利用情報共有に向けた具体的な枠組みの検討と連携の促進を図るとしている。

情報共有の実現のためには個人情報の取り扱いが課題である。今後、クレジットカードセキュリティ協議会等での具体化に向けた検討が期待される。

(1)-5. 警察等との連携強化

偽造カード取締等のクレジットカード決済に関する犯罪については、カード会社と警察組織との連携が古くから行われてきたが、不正アクセス等のサイバー攻撃によるカード情報流出や不正利用などのサイバー犯罪対策の点でも連携を強化することが公表された。『セキュリティ対策強化検討会報告書』では、当面の対応として以下3点を挙げている。

①経産省と警察庁の連携強化

サイバー攻撃によるカード情報流出事件について、経産省から警察庁サイバー警察局に情報提供する。また、クレジットカード会社等のカード情報保護対策の参考になるサイバー攻撃の手口、対策等の情報を警察庁から経産省に提供し、業界に周知する。

②都道府県警等とイシュアの連携強化

現在も個別案件ごとに不正利用されたカード番号などの情報を都道府県警察からイシュアや決済代行事業者に連携しているが、これを継続する。

③攻撃を受けたEC加盟店や不正利用を受けた消費者などの当事者から警察への早期通報および捜査協力の促進

現状、サイバー攻撃を受けカード情報が流出した際に、警察への相談や届出が円滑に受理されていないことがある。また、カード情報を不正利用された消費者に対しても、届出をしてもカード自体が紛失・盗難にあったわけではないことから、被害者であることが認識されず対応が疎かにされることがある。結果、サイバー犯罪全体の傾向や手口を警察が把握することが困難になっているという問題が指摘されている。対策として、業界内でのカード情報流出時のマニュアル整備や捜査協力時の対応フロー等を提示し、警察への早期通報や捜査協力を促進する。

この方針を受け、警察庁と経産省は2023年6月『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（https://www.meti.go.jp/press/2023/06/20230630004/20230630004.html）

（2）「EMV3-Dセキュア」の現状

2022年12月のかっこ社のEC事業者実態調査※1によると、「EMV3DS」を導入している事業者は全体の28.9%にとどまり、従来のバージョンである「3-Dセキュア1.0※2」を含めると、全体の62.9%が対応していた。「3-Dセキュア1.0」から最新版のEMV3DSへの移行は、81.7%が予定していた。

一方、前項でふれた『ガイドライン4.0』では、2025年3月を期限としたEMV3DSの導入義務化がうたわれており、さらに導入が促進されることが想定される。しかし導入を躊躇している加盟店の背景には、利用している決済代行事業者やECシステムにより異なるが、ランニングや導入コストに不安を抱える事業者が多いことが実態調査で分かった。実際の費用は、導入するためのシステム開発に数百万円かかったケースもあれば、費用がほぼかからずに移行できたケースもあり、事業者により大きく異なった。

またEMV3DSを導入する際は、以下の点を考慮すべきである。

①EMV3DSのリスクベース認証の精度不足

EMV3DSはリスクベース認証を行ってから、リスクの高いもののみに追加認証をしていく仕組みである。しかしリスクベース認証をすり抜けるケースも発生しており、EMV3DSを導入していても数百万円のクレジットカード不正利用被害※3が発生した事例が確認されている。そのためEMV3DSだけではなく多面的・重層な対策が必要である。

②ライアビリティシフト（損失の移転）の適用による不正利用情報の把握困難

EMV3DSの導入により、不正利用に関する責任が加盟店からカード会社に移転し、ライアビリティシフトが適用され、加盟店がチャージバック※4を受けることはなくなる。金銭的負担がなくなる一方で、クレジットカード不正利用に関する通知が加盟店には送られなくなり、不正利用の把握が難しくなる。例えば加盟店が不正検知サービスを導入している場合、この状況が検知精度に影響を与える可能性がある。なぜなら、不正検知サービスは、実際の不正利用被害をシステムにフィードバックし、検知精度向上を行っているからだ。そのため、EMV3DSを使用している場合でも、不正利用の発生状況を加盟店自身が把握することは非常に重要である。

※1　EC事業者の不正対策に関する実態調査（かっこ株式会社）
https://prtimes.jp/main/html/rd/p/000000084.000009799.html

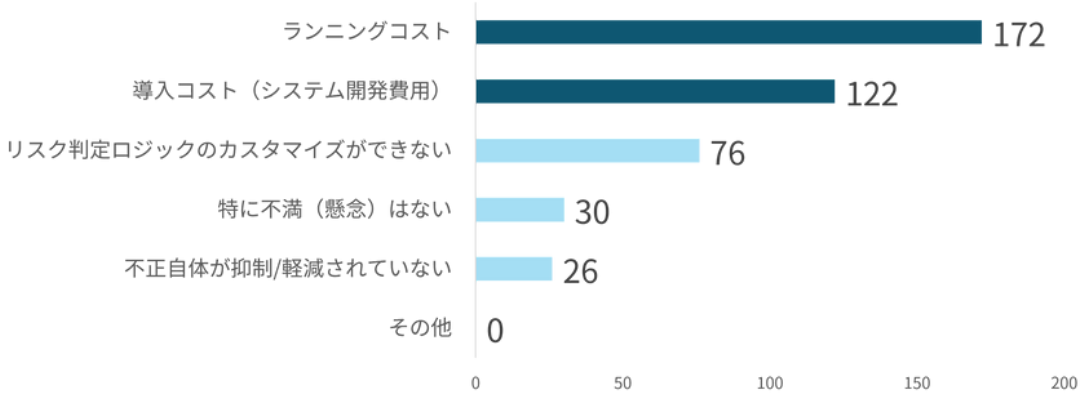
※2　「3-Dセキュア1.0」は、2022年10月でサポートが終了。2022年10月以降、不正利用が発生した場合、基本的にはEC事業者が負担することになる。

※3　EMV3DSを導入しているためEC事業者は補償されるが、カード会社が負担した金額。

※4　チャージバック：クレジットカードの持ち主が決済に対して同意しない場合に、クレジットカード会社がその決済を取り消して持ち主に返金する仕組み。

▼図3-2　EMV3-Dセキュアに関する不満な点（懸念している点）

Q：「EMV3-Dセキュア（3Dセキュア2.0）」に関して不満な点（懸念している点）を教えてください。（複数回答）

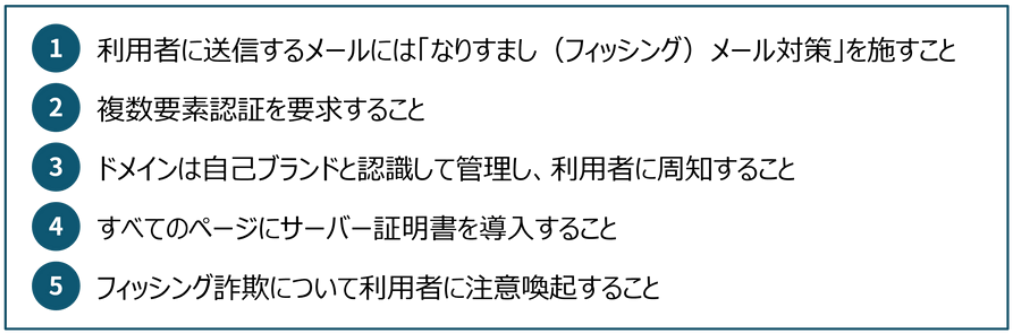


EC事業者実態調査（かっこ調べ）2022年12月調査

（3）フィッシング対策の強化

フィッシング対策協議会が公表している最新の『フィッシング対策ガイドライン（2023年度版）』は、2023年5月31日付で公開された。2022年度版に続き、フィッシングに関する基礎知識、フィッシング対策ガイドライン重要５項目、Webサイト運営者におけるフィッシング対策、利用者におけるフィッシング対策の構成で作成されている。そのなかでも特に重要となる「フィッシング対策ガイドライン重要5項目」の要点を解説する。その他のフィッシング対策については、『フィッシング対策ガイドライン（2023年度版）』を参照されたい。

▼図3-3　フィッシング対策ガイドライン重要5項目



①利用者に送信するメールには「なりすまし（フィッシング）メール対策」を施すこと

送信ドメイン認証技術「DMARC」（Domain-based Message Authentication, Reporting, and Conformance）を導入し、不正者からのメールを利用者に受信させない対策が重要である。また、「DMARC」レポートを活用し現状の不正傾向を把握し、受信制御ポリシーに「reject」を設定することが効果的である。さらに、国内直接接続のSMS を利用し、発信者番号を Webサイトなどで事前に告知することも対策の一環として示されている。

②複数要素認証を要求すること

フィッシングサイトによる個人情報の詐取を防ぐために、ログイン時には複数要素認証を要求することを推奨している。特にポイントやマイルなど資産の移動機能を提供している場合は資産の移動操作時にも複数要素認証を行うことが求められている。但し、複数要素認証はユーザーの使い勝手を阻害する可能性もあるため、認証対象を不正ログインに絞るなどの工夫が実運用では必要となる。

③ドメインは自己ブランドと認識して管理し、利用者に周知すること

フィッシングから利用者を守るために、自社のドメイン名を利用者に正確に周知することが重要となる。正しいドメイン名を繰り返し示すことで、利用者がフィッシングサイトに気づきやすくなるためだ。さらに企業側では、ドメイン名の登録と利用に関するルールと手順を確立し、自社で取得する全てのドメインに対してセキュリティに配慮した管理を徹底する必要がある。

複数の部門でそれぞれの目的のために複数のドメイン管理サービスを利用するような状況は、全容把握ができず、セキュリティ配慮に欠けた運用がされたり管理が放置される原因となる。

④すべてのページにサーバー証明書を導入すること

近年では大半の企業が対応しているが、セキュリティを強化するために、すべてのWebページにサーバー証明書を導入することを推奨している。これにより、利用者がフィッシングサイトにアクセスすることを防ぎ、アクセス先の正当性を確認できるようになるためだ。

また、近年では利用者が検索エンジン等で検索した際、本来のサイトよりもフィッシングサイトの方が上の検索順位になっているケースも報告されており、SEOの観点でもサーバー証明書の導入は必須である。

⑤フィッシング詐欺について利用者に注意喚起すること

不正者はあらゆる手段で利用者をフィッシングサイトへ誘導し、重要情報を詐取しようとするため、企業は利用者に対し、フィッシング詐欺対策啓発活動を行う責任がある。これに加え、フィッシング詐欺に関する報告窓口を設けること、更に一歩踏み込み、フィッシングサイトを検知する体制を整備することが重要である。

(4) FATF第4次審査結果を受けたクレジットカード業界の規制強化の方向性

2021年8月、FATF（Financial Action Task Force：金融活動作業部会）による第4次対日相互審査報告書が公表された。FATFは国ごとのマネーロンダリング（以下マネロン）およびテロ資金供与防止対策の状況を審査する政府間会合である。

FATF第4次相互審査では技術的コンプライアンス（法令等の整備状況）40項目（40の勧告）、有効性（体制の運用面）について11項目の評価が行われた 。日本は「重点フォローアップ国」と評価され、5年後のフォローアップ審査までの間に3回、FATFに改善状況を報告する必要がある。

審査結果において優先して取り組むべき事項として一番に挙げられたのが「事業者ごとのリスク評価導入・実施、リスクベースでの継続的な顧客管理、取引のモニタリング、資産凍結措置の実施、実質的支配者情報の収集と保持」である。また、大手銀行や資金移動業者以外の金融機関（クレジットカード発行会社含む）は、マネーロンダリング・テロ資金供与リスクについての理解が不十分で、リスクに基づいた低減措置を適用していないと評価されている。

審査結果の公表を契機に、政府一体となってマネーロンダリング対策等に取り組むため、警察庁・財務省を共同議長として17省庁が参加する「マネロン・テロ資金供与・拡散金融対策政策会議」（以下「マネロン対策政策会議」）が設置され、『マネロン・テロ資金供与・拡散金融対策に関する行動計画』が確認された。

上記の行動計画には、金融機関向けのガイドライン更新・策定が含まれている。経済産業省でも、2021年11月に『クレジットカード業におけるマネー・ローンダリング及びテロ資金供与対策に関するガイドライン』を改訂した。

改訂前（2019年）のガイドライン に比べると以下の点が強化されている。

①リスクベースアプローチにおける「リスク評価」において、疑わしい取引の届出の状況等の分析を考慮すること
②顧客 管理において、顧客の営業内容、所在地等が取引目的、取引態様等に照らして合理的ではないなどのリスクが高い取引等については、取引開始前、あるいは多額の取引を実施する際などに営業実態や所在地等を把握するなどの追加的な措置を講ずること
③疑わしい取引を検知するためのシナリオや閾値などの基準を含むモニタリング体制を構築し、改善を図ること
④制裁対象取引（経済制裁の対象となる相手型や国、地域との取引や、対象品目の取引）をフィルタリングする体制を構築すること

経済産業省では、上記も含め、ガイドラインで「対応が求められる事項」として挙げている項目について、2024年3月末までに完全実施を求めている。

FATF第5次審査は2025年以降順次実施予定で、FATFでは勧告の改訂を進めている。第5次審査に向けて、マネロン対策政策会議では2022年5月に『マネロン・テロ資金供与・拡散金融対策の推進に関する基本方針』を策定した。日本の第5次審査のスケジュールは未定だが、基本方針にのっとり法改正などの対応を進めていくとしている。

＜参考文献＞

1.『2022年のキャッシュレス比率を算出しました』（経済産業省 2023年4月）
https://www.meti.go.jp/press/2023/04/20230406002/20230406002.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 ）
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【4.0版】』（クレジット取引セキュリティ対策協議会　2023年3月）
https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_4.0_published.pdf

4.『株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について（注意喚起）』（経済産業省 2019年12月）
https://warp.da.ndl.go.jp/info:ndljp/pid/12685722/www.meti.go.jp/press/2019/12/20191220013/20191220013.html

5.『クレジットカード情報漏洩事件のまとめ（2022年上半期）』（フォックスエスタ）
https://foxestar.hatenablog.com/entry/2022/01/19/155606

6.『クレジットカード情報漏洩事件のまとめ（2022年下半期）』（フォックスエスタ）
https://foxestar.hatenablog.com/entry/2023/01/10/121218

7.『EC-CUBE4.0におけるクロスサイトスクリプティングの脆弱性(JVN#97554111)』（株式会社イーシーキューブ 2021年5月）
https://www.ec-cube.net/info/weakness/weakness.php?id=77

8.『EC-CUBE3.0におけるクロスサイトスクリプティングの脆弱性(JVN#95292458)』（株式会社イーシーキューブ 2021年5月）
https://www.ec-cube.net/info/weakness/weakness.php?id=79

9.『クレジットカード番号等取扱業者に対する行政処分を行いました』（経済産業省 2022年6月）
https://www.meti.go.jp/press/2022/06/20220630007/20220630007.html

10.不正アクセスに関するお知らせとお詫び（株式会社ショーケース 2022年10月）
https://www.showcase-tv.com/pressrelease/202210-fa-info/

11.『EC事業者実態調査』（かっこ株式会社　2022年12月27日）
https://prtimes.jp/main/html/rd/p/000000084.000009799.html

12.『クレジットカード不正利用被害のうち 「番号盗用」の内訳について』
（一般社団法人日本クレジットカード協会　第2回クレジットカード決済システムのセキュリティ対策協議会検討会　2022年9月）
https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/002_02_00.pdf

13.『カード決済の不正な大量アタック(クレジットマスター)の増加と対策について（2023/01/13）』（株式会社イーシーキューブ　2023年1月13日）
https://www.ec-cube.net/news/detail.php?news_id=432

14.『From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud』
（米Microsoft　2022年7月12日）
https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

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

16.『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 2023年2月）
https://www.meti.go.jp/press/2022/02/20230201001/20230201001.html

17.『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』（経済産業省 2023年1月）
https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/20230120_1.pdf

18.『登録包括信用購入あつせん業者一覧　令和5年5月31日現在』（経済産業省 2023年5月）
https://www.meti.go.jp/policy/economy/consumer/credit/R5-5tourokuhoukatsuichiran.pdf

19.『ECサイト構築・運用セキュリティガイドライン』（独立行政法人情報処理推進機構 2023年3月）
https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

20.『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』（経済産業省 2023年6月）
https://www.meti.go.jp/press/2023/06/20230630004/20230630004.html

21.『フィッシング対策ガイドライン（2023年度版）』（フィッシング対策協議会　2023年5月）
https://www.antiphishing.jp/report/antiphishing_guideline_2023.pdf

22.『マネロン・テロ資金 供与対策 日本　相互審査報告書　仮訳』（金融活動作業部会（FATF） 2021年8月）
https://www.mof.go.jp/policy/international_policy/amlcftcpf/20221228.pdf

23.『マネロン・テロ資金供与・拡散金融対策に関する行動計画』（マネロン・テロ資金供与・拡散金融対策政策会議　2021年8月）
https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/20210830_2.pdf

24.『クレジットカード業におけるマネー・ローンダリング及びテロ資金供与対策に関するガイドライン』（経済産業省 2021年11月）
https://www.meti.go.jp/policy/economy/consumer/credit/pdf/20211118creditmanerongl.pdf

25.『マネロン・テロ資金供与・拡散金融対策の推進に関する基本方針』（マネロン・テロ資金供与・拡散金融対策政策会議　2022年5月）
https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/20220519_1.pdf

キャッシュレスセキュリティレポート2023
2023年10月26日発行
発行者
かっこ株式会社
https://cacco.co.jp/
ｆｊコンサルティング株式会社
https://www.fjconsulting.jp/