

クレジットカード被害をブロック！

大量アタック 遮断サービスのご案内



IFLAG PAYMENT SERVICE

株式会社アイフラッグ

 0120-953-677

受付時間：9：00～18：00（土日祝日除く）

「クレジットカードマスター」とは

悪意のある第三者により行われるネット上の犯罪行為です

クレジットカードマスターは、クレジットカード番号生成の規則性を悪用するプログラムを用いて、有効なクレジットカード番号を割り出し、ECサイトの決済フォームから該当のカード有効期限とセキュリティコードが判明するまで機械的にリクエスト（攻撃）を繰り返すという手口で行われます。

こうして得られた有効なクレジットカード情報は不正取引に利用され、加盟店様のECサイトの決済フォームやカード登録ページ等が悪用されることから、加盟店様は知らず知らずのうちに犯罪に巻き込まれている、と捉えることができます。

カード番号の規則性に従い、
大量リクエストによる総攻撃を実施



カード番号	有効期限	セキュリティコード	
1234567890123456	01/28	111	×
1234567890123456	02/28	111	×
1234567890123456	03/28	111	×
1234567890123456	04/28	111	×
1234567890123456	05/28	111	×
1234567890123456	06/28	111	×
1234567890123456	07/28	111	×
1234567890123456	08/28	111	○

実在するカード番号の割り出しに成功



悪意のある第三者は以下の罪に問われる可能性があります

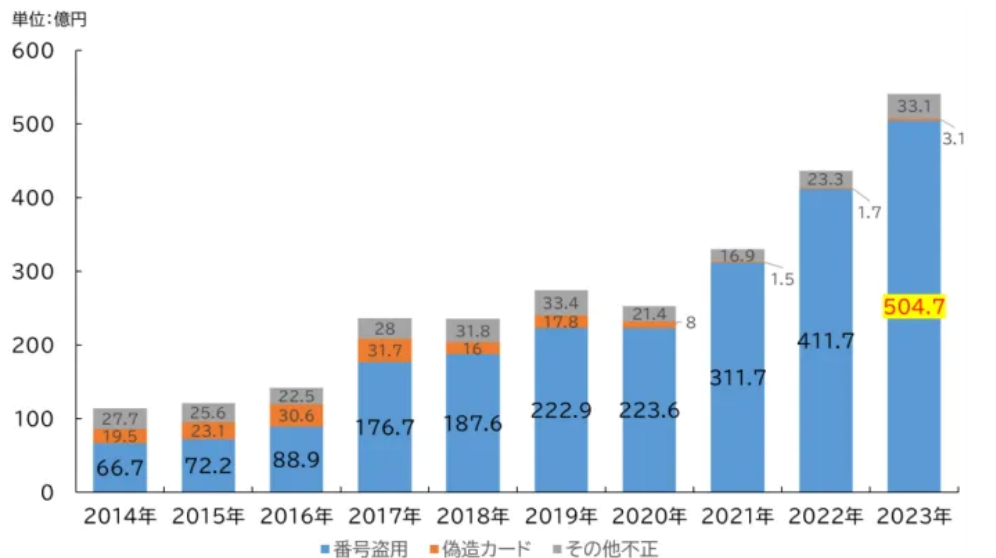
- ・偽計業務妨害罪：大量の攻撃により加盟店様のシステムに障害が発生し、サービスの停止を余儀なくされた場合等に適用
- ・電子計算機使用詐欺罪：加盟店様の決済システムへカード名義人になりました第三者が不正にアクセスし、財産上不法の利益を得た場合等に適用

「クレジットカードマスター」による被害状況

2023年(1月～12月)に発生した クレジットカードの不正利用の総額は540.9億円と過去最悪

日本クレジット協会によると**2023年のクレジットカードの不正利用の総額は540.9億円**、2022年は436.7億円であったため、この1年で約100億円も被害額が増加しています。また、クレジットカード不正利用被害額の内訳を見ると「**番号盗用被害**」は**504.7億円であり、全体の93.3%**となっています。クレジットカードマスターによる攻撃はこの「番号盗用被害」に含まれます。全てがクレジットカードマスターによるものではありませんが、近年の傾向を見ると今後も「番号盗用被害」による被害は増加していく可能性が高いです。

クレジットカード不正利用被害の発生状況



参考：日本クレジット協会

日本経済新聞

お申し込み ログイン

トップ 朝刊・夕刊 速報 マーケット

この記事は会員限定記事です

クレカ不正利用率が最悪 昨年被害額、10年で5倍

官民で監視体制 本人認証の強化促す

2024年4月4日 2:00 [会員限定記事]

解説 クレカ被害「過去最悪」巧妙化する手口 どう防ぐ?

クレジット
去最悪と
ると2023
は540億円
トカード
を立ち上

急増 クレカ不正利用過去最多 背景に手口巧妙化

不正トラベルで被害額4万1402円

ふるさと納税で被害額36万円

クレジットカード不正利用による被害は過去最大

経済産業省も、クレジットカード会社とEC店舗に対し、2025年3月末までに3Dセキュア導入を求めるなど、官民一体となった対策が必要に

クレジットカードを扱うEC事業者は、顧客を守るためにも不正利用への対策が法令で義務付けられています。では、クレジットマスターに有効な対策とはどのようなものかをご紹介します。

クレジットカード不正利用による被害 過去最大540億円超に 9割超が番号盗みネットショッピング

4/9(火) 16:54 配信 1081

テレ朝 news



クレジットカードの不正利用による被害額が去年過去最大となり、経済産業省はカード会社などと不正利用防止に向けた対策状況を確認しました。

【動画】番号表示なしクレジットカード“安心感”で人気

クレジットカード不正利用被害 過去最大で対策状況確認

去年1年間のクレジットカードの不正利用による被害額は過去最大の541億円で、このうち9割以上がカード番号が盗まれネットショッピングなどで利用されたものだという事です。

経産省は不正利用を防ぐため「EMV3Dセキュア」と呼ばれる「ワンタイムパスワード」による本人認証システムの導入を進めていて、今回カード会社などを集めた対策会議を開き、システムの導入状況などを確認しました。

経産省は改めてカード会社とともに利用者本人による設定を促していくことにしています。

テレビ朝日報道局

●クレジットカードマスターへの主な対策

本人認証サービス「3Dセキュア」を導入

ワンタイムパスワードや生体認証などによる本人確認を行う本人認証システムで、経済産業省は、カード会社とEC店舗に対し、2025年3月末までに3Dセキュア導入を求めている

bot対策を導入 (reCAPTCHAの導入)

多くのサイトで導入されるGoogle提供の認証システム、botなどによる悪質なアクセスからWebサイトを守る

入力制限を導入

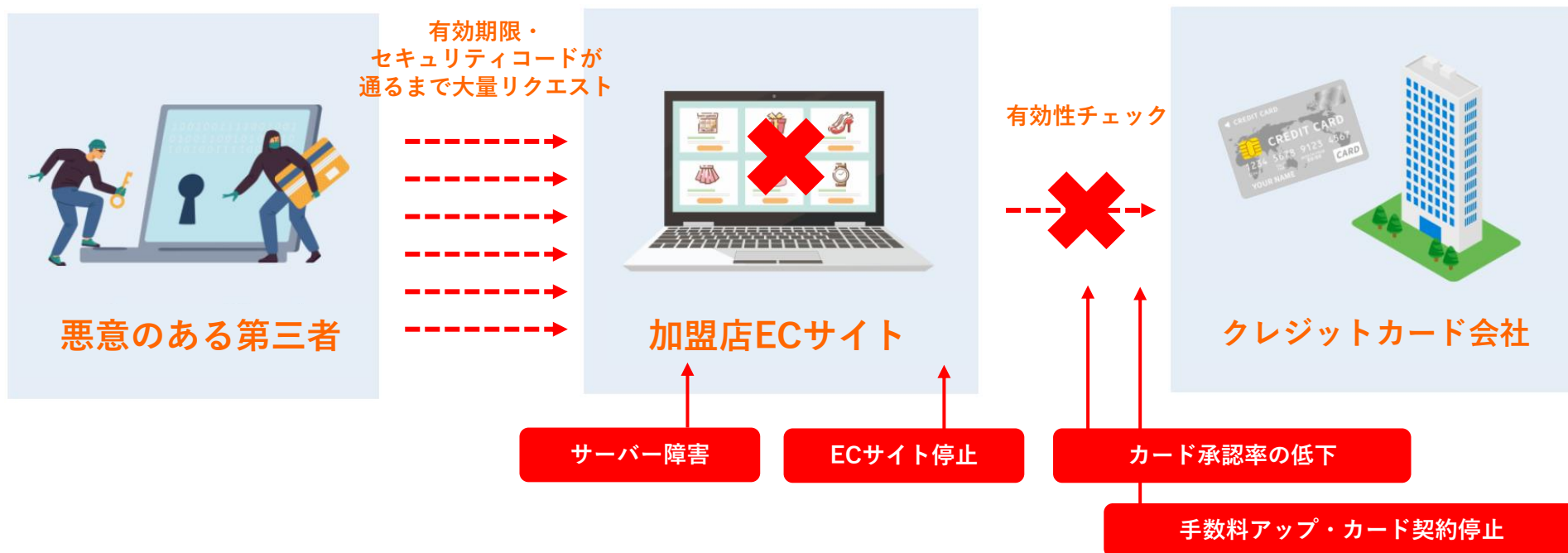
繰り返し実行されるリクエスト（攻撃）を遮断条件に応じてブロック ※今回のご案内です

クレジットカードマスター対策には、複合的な対策が効果的となります

クレジットマスター被害時のリスクとは

加盟店様の主なリスク

ECサイトの停止	短時間に数万単位でリクエスト（攻撃）が発生する場合もあるため、トラフィック量増加に伴うサーバー障害により、サイトダウンをはじめ、一時的なサービス提供・商品販売停止を余儀なくされる可能性があります。
クレジットカード承認率の低下	クレジットマスターの被害が拡大すると、クレジットカード会社が決済の承認率を低下させ、正規のユーザーにもかかわらず、カードが承認されず商品が購入ができない、といった影響が出る可能性があります。
手数料アップ・カード契約の停止	大量リクエスト（攻撃）の影響により、クレジットカード会社より手数料率アップや、クレジットカード会社との契約停止（クレジットカード利用の停止）等の措置を取られる可能性があります。



「大量アタック遮断サービス」とは

大量のオーソリ・リクエストを遮断し クレジットマスターの被害を予防するサービスです

繰り返し実行されるリクエスト（攻撃）を遮断条件に応じてブロックすることにより、クレジットマスター被害を防ぎます。
人的・機械的なアタック両サイドに有効かつ効果的に不正アタックをブロックしますので、安心してEC事業に取り組む事が可能です。

●ご利用料金

月額 **2,000**円（税抜）

- ・契約月は無料、契約月の翌月より課金となります。
- ・当社提供の決済代行サービスご導入のお客様向けのオプションです。



●大量アタック遮断サービスのメリット

1	不正取引につながる可能性のあるリクエストを遮断 「クレジットマスター」の手口である大量アタックを遮断し、購入者様、加盟店様を守ります
2	チャージバック被害のリスクを抑制 大量アタックにより発生する不正取引による、加盟店様のチャージバック被害のリスクを軽減します
3	無駄なトラフィック発生を防ぐ クレジットマスターは短時間に数万単位でリクエスト（攻撃）が発生する場合がありますが、本サービスを導入する事で、無駄なトラフィック発生を抑止し、安心したECサイト運営が行えます

※本サービスによりすべてのクレジットマスター被害を防ぐものではありません

※本サービスは、チャージバックが発生しない、チャージバックを免責するサービスではございません

サービス申込方法と利用開始までの流れ

ご利用にはお申し込みが必要です 専用の申し込みフォームよりお申し込みください

STEP 1

イープレスデザイン顧客サポートサイト内のオプション申し込み画面を表示します

「顧客サポートサイトトップページ」→「有料サービス」→「大量アタック遮断サービス」→「お申込みはこちら」

STEP 2

必要事項を入力し「Z.大量アタック遮断サービスのご案内」にチェックを入れ、規約を確認し、お申し込みをお願いします

「規約」は必ず目を通して頂きますようお願いいたします

STEP 3

当社側にて、クレジットマスター攻撃に対する有効な“遮断方式”と“条件”を設定します。

初期設定では厳しめの設定を行います

STEP 4

設定後、クレジットマスター攻撃に対する遮断が始まります

検知できた事案のみ、照会を受け付けております
詳細はサポート担当までご連絡ください


●遮断方式と条件のイメージ

チェックタイプ	処理区分	取引状態	期間(分)	件数	説明
同一カード番号取引	全て	エラー取引のみ			直近5分間以内にチェックタイプ【同一カード番号取引】に対して、2件以上の処理区分【全て】のエラー有無【エラー取引のみ】のリクエストがある場合にブロックします。
同一カード番号取引	全て	エラー取引のみ			直近1440分間以内にチェックタイプ【同一カード番号取引】に対して、3件以上の処理区分【全て】のエラー有無【エラー取引のみ】のリクエストがある場合にブロックします。
同一カードID取引	全て	エラー取引のみ			直近5分間以内にチェックタイプ【同一カードID取引】に対して、2件以上の処理区分【全て】のエラー有無【エラー取引のみ】のリクエストがある場合にブロックします。
同一カードID取引	全て	エラー取引のみ			直近1440分間以内にチェックタイプ【同一カードID取引】に対して、3件以上の処理区分【全て】のエラー有無【エラー取引のみ】のリクエストがある場合にブロックします。
チェックタイプ	期間(分)	件数	説明		
同一会員IDカード登録			直近5分間以内にチェックタイプ【同一会員IDカード登録】に対して、2件以上のリクエストがある場合にブロックします。		
同一会員IDカード登録			直近1440分間以内にチェックタイプ【同一会員IDカード登録】に対して、3件以上のリクエストがある場合にブロックします。		

お問い合わせ先

株式会社アイフラッグ

〒108-0023 東京都港区芝浦4-16-25

 **0120-953-677**

受付時間 9:00 - 18:00 (土日祝除く)