

2026年2月12日
日本クレジットカード協会

EC加盟店におけるクレジットカード不正利用発生時の サイバー窓口を活用した警察通報に関する対応要領

変更履歴

変更日	版数	変更理由	変更者
2026.2.12	1.0	初版作成	日本クレジットカード協会

1. はじめに

(1) 目的

- ・ 本書は、インターネットを通じて商品を販売する電子商取引の加盟店様（以下、EC 加盟店様）がクレジットカードの不正利用による被害に遭われた際の初動対応のポイントを整理したものです。
- ・ 警察への早期通報を促進することで、被害の拡大防止や不正の抑止につなげることを目的としております。本書が、EC 加盟店様の対応の一助となれば幸いです。

(2) 背景

- ・ 日本では、経済産業省が主導するクレジット取引セキュリティ対策協議会（事務局：一般社団法人 日本クレジット協会）策定の「クレジットカード・セキュリティガイドライン」に基づき、カード会社や加盟店等が不正利用防止に関する技術的対策を推進しております。
 - ・ クレジットカード不正利用被害額が増加の一途をたどる状況の中、2024 年 3 月 29 日に、サイバー事案に関する通報・相談等を受け付ける警察の窓口が、警察庁により「サイバー事案に関する相談窓口」（以下、サイバー窓口）へ一本化されました。
 - ・ EC 加盟店様から「警察のどこに通報をすべきかなどがわからず、通報がしづらい」とのお声をいただくこともございましたが、統一窓口を通じて一元的に通報や相談ができるようになり、迅速に対応を受けられる環境が整っております。
 - ・ 2024 年にはクレジットカード不正利用被害額は約 555 億円（前年比+14 億円）と過去最悪を記録しております。
 - ・ 不正動向の把握、対策検討、被害の拡大防止のためには、カード会員を装って商品を注文・詐取する詐欺行為において、刑法上の被害者である EC 加盟店様からの警察への早期通報が極めて重要となります。
 - ・ カード会社は被害届を提出できないケースが多いなか、クレジットカード不正利用の撲滅のためには EC 加盟店様によるご協力が必要不可欠でございます。以上の背景をご理解いただき、ご協力賜りますようお願い申し上げます。
- (※) クレジットカード不正利用の多くが、カード情報（カード番号・有効期限等）の漏えいに起因し発生しております。EC 加盟店様自身の販売サイト等からカード情報が漏えいした懸念がある場合は、速やかに、カード会社やご利用の決済代行会社、最寄りの警察署にご連絡ください。

2. 対応の概要

EC 加盟店様が不正利用の被害に遭われた場合には、以下の基本的な流れ及び留意事項に従い、速やかにご対応くださいますようお願いいたします。

本書では、②通報、③情報収集および④捜査協力についてご案内いたします。

①発覚・検知	カード会社またはカード会員からの連絡等により、および EC 加盟店様にて不正利用の被害を検知
②通報	EC 加盟店様にて、サイバー事案に関する 通報 （詳細を項番 3、4 にて後述）
③情報収集	EC 加盟店様にて、捜査に必要な情報を追加収集・保全（詳細を項番 4 にて後述）
④捜査協力	捜査を担当する 警察署からの連絡・案内に基づき捜査協力 （詳細を項番 6 にて後述）

3. 通報方法

以下の手順に則り、警察への通報をお願いいたします。

(1) e-Gov 電子申請の準備

サイバー窓口への通報は、e-Gov 電子申請（デジタル庁が運営する電子申請のポータルサイト）からオンライン上で申請してください。

申請にあたって、事前に e-Gov アカウントの取得および、「e-Gov 電子申請アプリケーション」のインストールが必要となります。

以下のリンク（※）に記載の手順に従い、事前準備をお願いいたします。

（※）[e-Gov を初めてお使いの方へ | e-Gov 電子申請](#)

(2) 「サイバー事案に関する通報」ページへアクセス

以下のリンク（※）より①「サイバー事案に関する通報」ページへアクセスし、「申請書入力へ」ボタンを押下ください。②遷移先のページで、「e-Gov 電子申請アプリケーション起動」ボタンを押下してください。

（※）[手続情報表示 | e-Gov 電子申請](#)

① 「サイバー事案に関する通報」 ページ

e-GOV 電子申請

トップ | 電子申請について | 利用準備 | **手続検索** | ヘルプ

サイバー事案に関する通報

委任可 GビズID電子署名省略可

手続概要	都道府県警察に対し、サイバー事案に関する通報を行うものです。
根拠法令	-
電子申請方法別利用案内	サイバー事案に関しない悩みやご相談等をご遠慮ください。 一般的な情報セキュリティに関する技術的な相談は、情報処理推進機構（IPA）又は03-5978-7509（情報セキュリティ安心相談窓口）へお問い合わせください。 商品やサービス等、消費生活全般に関する相談は、消費生活センター又は188（消費者ホットライン）へお問い合わせください。 捜査の進捗状況、違法性や法律解釈の判断等については、原則回答いたしかねます。 担当者が受け付けた時点で、ステータスは「手続終了」と表示されます。
告知情報	【通報要件】 被害に遭った具体的な事実の通知を伴う場合にご利用ください。 （これらを伴わない場合は「サイバー事案に関する相談」をご利用ください。） ※殺害予告や犯行予告、自殺をほのめかす書込等、緊急を要する場合は110番通報してください。 【通報先】 お住まいの都道府県の警察本部又は管轄警察署 【手続可能時間】 24時間365日ご利用できます。 ただし、土日、祝祭日及び年末年始は、通報の確認を行っておりません。 お急ぎの場合は、最寄りの警察署に連絡してください。

[戻る](#) [申請書入力へ](#)

② 遷移先ページ



e-Gov電子申請アプリケーション起動

申請等の手続は「e-Gov電子申請アプリケーション」を使って行います。
インストールがお済みの場合は、下のボタンからアプリケーションを起動し、手続に進んでください。

e-Gov電子申請アプリケーションを起動

次回からはこの画面を省略し、直接アプリケーションを起動する。

(3) 「e-Gov 電子申請アプリケーション」へログイン

アプリ起動後、(1) で登録した情報を用いて e-Gov アカウントへログインしてください。

(4) 申請書入力

フォーマットに従って申請書の入力をお願いいたします。「2. サイバー事案に関する通報」への記入内容については項番 4 をご参照ください。

e-GOV 電子申請

お問合せ ヘルプ

申請書入力 申請内容確認 提出完了

申請書入力

基本情報を選択し、申請・届出様式に必要な事項を入力してください。

1. 基本情報

未設定・変更する場合には、それぞれ設定ボタンを押してください。

申請者情報

必須

申請者情報を設定

法人名

申請者氏名

住所

2. サイバー事案に関する通報/サイバー事案に関する通報

申請・届出に関する事項を入力してください。
複数の様式を提出する場合は、左の様式一覧から様式を切り替えてください。

申請する様式一覧

必須

サイバー事案に関する通報

プレビュー

サイバー事案に関する通報

必須 氏名

必須 フリガナ

必須 メールアドレス

必須 電話番号

必須 申請・届出先 北海道函館方面

4. 通報内容

(1) 「申請する様式一覧」への記載内容

(表1) にしたがってご入力をお願いいたします。

(表1) 「申請する様式一覧」への記載内容

項目	記載内容
氏名	ご担当者様の情報をご入力ください。
フリガナ	
メールアドレス	
電話番号	
申請・届出先	EC 加盟店様の法人所在地のある都道府県を選択ください。
郵便番号	EC 加盟店様の法人所在地をご入力ください。
住所	
通報の種別	「ネット上の詐欺・悪質商法等による被害に関するもの」を選択ください。
具体的な内容	本書【別紙①】【別紙②】の記入サンプルを参考にご入力ください。

(2) 「添付書類」への添付内容

(表2) の項目を収集のうえ、添付をお願いいたします。

入力フォーマットについては【別紙③】「クレジットカード不正利用発生時の申出書」をご活用ください。(表2) の項目を満たしていれば、【別紙③】以外のフォーマットでご提出いただいても問題ございません。)

(表2) 通報時の添付情報

項目	
1. 申出者の基本情報	
	会社名
	会社所在地 (住所)
	担当所属 (部署名)
	担当者氏名
	担当者連絡先電話番号
2. 事件概要	
	発覚日 (認知日)
	発覚の経緯
	屋号
	サイト URL
	不正利用と判断した理由
	購入情報
	不正購入日時
	商品名
	数量
	販売価格

(表2)の項目につきましては、可能な限りご入力のうえ添付をお願いいたします。(捜査を担当する都道府県警察の振り分け、捜査にあたってのご連絡等に必要な項目となるため)
 ただし、通報時は速やかな情報連携を最優先とし、すべての情報をそろえていただく必要はございません。

(3) 「提出先選択」の選択内容

EC加盟店様の法人所在地のある都道府県警察本部を選択してください。
 例)：法人所在地が神奈川県の場合、「神奈川県警察本部」を選択

5. 情報収集

通報後の捜査協力の備え、(表2)の項目に加え、以下(表3)に記載の項目についても収集・保全をお願いいたします。なお、その際も【別紙③】「クレジットカード不正利用発生時の申出書」をご活用ください。

(表2)(表3)の項目以外の情報につきましても、警察からの要請がございましたら、適宜カード会社、決済代行業者へのお問い合わせ等をいただき、追加の情報収集をお願いいたします。

(表3) 保全情報

項目	
3.不正購入者情報等	
	発注者住所
	発注者氏名
	発注者電話番号
	配送先住所
	配送先氏名
	配送先電話番号
	配送業者
	購入時のログ情報
	アクセス元 IP アドレス (購入時等)
	アクセス元ポート番号 (購入時等)
	アクセス日時 (購入時等)
	ブラウザ情報 (ユーザーエージェント)
	言語情報
	アクセス先 IP アドレス (EC サイトが管理している IP アドレス)
	不正アクセス疑い有無
	↳有の場合は認証サーバの設置場所
	操作ログの有無 (購入時の画面遷移等)
	当該ECサイトに係る委託業者の有無
	↳有の場合は業者名
	その他参考となる事項

6. 警察からの連絡について

サイバー窓口への通報・相談内容に基づき、捜査を担当する警察から連絡がある場合がございます。その際は、捜査へのご協力をお願いいたします。また、項番5でもご案内いたしました【別紙③】「クレジットカード不正利用発生時の申出書」をご活用の上、可能な範囲でご記入ください。記入いただいたものは、警察による捜査対応の際に、警察署等の捜査員へお渡しいただきますようお願いいたします。

7. 不正利用の未然防止にあたって

不正利用被害の抑止にあたっては、被害発生後の対応はもとより、被害を未然に防止することが極めて重要です。

未然防止のための対策については、クレジットカード取引セキュリティ対策協議会の定める「クレジットカード・セキュリティガイドライン」をご参照ください。

[関連資料 | 安全・安心なクレジットカード取引への取組 | 一般社団法人日本クレジット協会](#)

以上