なりすまし EC サイト
対策マニュアル

なりすまし EC サイト対策協議会
一般社団法人セーファーインターネット協会
2015 年 3 月　発行

目次

1. はじめに

本マニュアルは、EC サイト運営者の方向けに作成されたもので、「なりすまし EC サイト」の特徴やアンケートに基づき得られた被害実態、当事者たちの責任関係、被害にあった際の対処法や予防法等の一連の情報をまとめたものとなっております。

本マニュアルを参考に、なりすまし EC サイトの現状や問題を知っていただき対策を推進していただくことで、被害を少しでも減らすことができれば幸いです。

2. なりすまし EC サイトとは

「なりすまし EC サイト」とは、実在するサイトの外観（屋号、商標、サイト意匠・構成、使用している画像等）を模倣することにより、あたかも当該サイトである又は当該サイトと関係のあるサイトであるかのように消費者を誤認させ、商品代金をだましとったり、模倣品、海賊版その他購入しようとした品と全く別個の物を送りつけるサイトを指します。また、代金を振込ませる手口だけでなく、クレジットカード決済ができるかのように見せかけてカード情報を入力させるサイトも確認されています。このようなサイトも「なりすまし EC サイト」に含めて考えられます。

何も対策せずに放っておくと、

- 売上減少
- 信用失墜
- 被害者からのクレーム・問合せが殺到

という事態に陥ります。なりすまされた EC サイト運営者も被害者です。しかし貴店になりすました者が顧客や見込み客を騙すことで、知らず知らずのうちに貴店の信用が落ちてしまいます。積極的にサイト来訪者に注意を喚起し、対策を実施しましょう。

3. なりすまし EC サイトの特徴

典型的ななりすまし EC サイトの特徴として、下記のような事例が挙げられます。ただし、なりすまし EC サイトは、上記 2.に記載した通り多様化しており、これらの特徴に当てはまらないものも多く出てきています。

- 日本語が不自然
- 振込先が個人名（外国人の場合が多い）
- 支払い方法が銀行振込のみとなっている
- 問い合せ先のメールアドレスがフリーメールアドレス
- 「特定商取引に関する表示」が曖昧（店舗名・住所・電話番号・メール　の表示が欠けている）
- 価格が極端に安い
- フォームの崩れやリンク切れなど、Web サイトの作り方に粗雑な点が見られる
- 有名ブランド名＋激安　などの表示がある

4. 被害実態（アンケート結果）

なりすまし EC サイト対策協議会では、2014 年 10 月に協議会参加団体の協力を得てアンケートを実施し、EC サイト運営者 1208 社から回答を得ました。アンケートから得た被害実態は、下記のとおりです。

4.1. 被害実態

- 自社のサイトがなりすまされた経験があるか尋ねたところ、44.2%が「ある」と回答した。また、問合せ内容は「商品が届くケース」と「届かないケース」でそれぞれ何件だったか尋ねたところ、19%が「何も届かない」、2%が「届いたが偽造品だった」と回答した（残り 79%は無回答）。このことから、なりすまし EC サイトによる消費者被害の態様としては模倣品が送られてくる模倣品流通事例よりも、代金を支払ったのに物が送られて来ないという代金搾取詐欺事例の方が多いことがわかった。他方、EC サイト運営者の立場からみると、なりすまされたこと自体により知的財産権を侵害されている場合も少なくないことに留意すべきである。

- 自社のサイトがなりすまされて困ったことを尋ねたところ、29.7%が「被害を受けた自社サイト利用者/顧客からの問合せ対応」、24.4%が「自社サイ

ト利用者/顧客への被害」と回答した。直接的に金銭被害に遭うのは騙された顧客たちであるが、なりすまされたサイトにとっても、自らの落ち度ではないにもかかわらず信用失墜や被害者対応の対応コストという形で被害に遭っていると言える。

4.2. 対策状況

- 自社サイトの「なりすまし EC サイト」を発見するために何か対策をとっているか尋ねたところ、62.3%が「ない」と回答した。逆に対策を実施した EC サイト運営者にその具体策を尋ねたところ、21.8%が「警察への通報」、20.6%が「自社サイトでの注意喚起（URL 公表なし）」、16.7%が「相手方への警告」と回答した。加えて、その対策の結果を尋ねたところ、25.2%が「わからない」、8.9%が「効果はなかった」、7.9%が「多少効果があった」と回答した。もとより、特効薬的な端的な対策は存在しないが、一定の対策をすれば一定の効果が期待できるにもかかわらず、行動に移している事業者は半数にも満たない状況であることがわかった。

なりすまし EC サイト被害実態調査アンケートは、下記のページで確認できます。

被害実態調査結果 2014－なりすまし EC サイト対策協議会
http://www.saferinternet.or.jp/narisumashi/report/

5. 当事者たちの責任関係

消費者が、なりすまし EC サイトから商品を購入し、「商品が届かない」、「偽物が届いた」という事例が発生したとしても、その責任は EC 事業者が負うものではありません。むしろ、本来なら本物のサイトに来るはずだった消費者が、なりすましサイトへ行ってしまうことで、EC 事業者も金銭的な被害を受けているといえます。

しかしながら、被害に遭った消費者は、本物の EC サイトに対しても感情的に負のイメージを抱きがちですし、インターネットを利用した商取引自体を信用しなくなりがちです。また、企業にとっても、自社のなりすまし EC サイトで被害が発生した場合、顧客からの問い合わせに親身になって対応しないことで却って悪評が生じたり、顧客離れを起こしたりすることがないよう、注意が必要

です。

そのような事態を避け、消費者に安心して EC サイトを利用してもらい、市場を活性化するためにも、EC 事業者は、消費者に向けてなりすまし EC サイトの存在を知ってもらう活動を行ったり、自社サイトがなりすまされないような仕組みを導入したり、自社なりすまし EC サイトを発見する仕組みを構築したりする努力が必要です。

6. 対処法、予防法

自社 EC サイトがなりすまし被害に遭った際の対処法と、なりすまされないための予防法を知ることで、被害を最小限に防ぐことができます。

6.1. 対処法

対処法には、下記のような対応があります。

6.1.1. 問い合わせ対応

怪しいサイトを発見された方や実際に購入をしてしまった方から問い合わせが入る場合がありますので、それぞれの状況に即した対応を心がけましょう。なりすまし EC サイト対策協議会では、問い合わせ対応文を用意していますので、参考にしてください。

問い合わせ対応文－なりすまし EC サイト対策協議会
http://www.saferinternet.or.jp/wordpress/wp-content/uploads/template002.docx

6.1.2. 削除要請

ホスティングプロバイダーへは削除要請に際しては、模倣のされ方によって適用される法令が変わってきますので、顧問弁護士にご相談されることをお勧め致します。なりすまし EC サイト対策協議会では、削除依頼文を用意していますので、参考にしてください。

削除依頼文－なりすまし EC サイト対策協議会
http://www.saferinternet.or.jp/wordpress/wp-content/uploads/template003.docx

6.1.3. 都道府県警察サイバー犯罪相談窓口への連絡

自社 EC サイトのなりすまし EC サイトを発見した時は、速やかに警察に情報提供を行いましょう。警察による捜査等において、当該サイトがなりすまし EC サイトと確認できた場合は、銀行口座の停止やウイルス対策ソフト・フィルタリング製品への反映がなされる場合があり、一定程度、被害拡大を防止することができます。都道府県警察本部のサイバー犯罪相談窓口等一覧は、下記のとおりです。

都道府県警察本部のサイバー犯罪相談窓口等一覧 http://www.npa.go.jp/cyber/soudan.htm

6.2. 予防法

予防法には、下記のような対応があります。

6.2.1. 注意喚起

サイトの目立つところに注意喚起のお知らせを掲示しましょう。顧客が被害に遭わないように注意を促すとともに、貴店が対策に積極的なことを示し、安全に安心して買い物ができる環境整備に前向きな姿勢をアピールできます。

なりすまし EC サイト対策協議会では、サイト掲示用注意喚起文を用意していますので、参考にしてください。

サイト掲示用注意喚起文 – なりすまし EC サイト対策協議会 http://www.saferinternet.or.jp/wordpress/wp-content/uploads/template001.docx

6.2.2. 被害に遭っているかの確認

自身が運営する EC サイトがなりすましの被害に遭っているか、検索サイトやアラートサービスで確認を行いましょう。方法としては、下記の 4 つがあります。

- 自身が運営する EC サイトの店舗名を検索サイトで検索し、自身が運営する以外のドメインで EC サイトが存在するかをチェックする
- 自身が運営する EC サイトの店舗名やサービス名等を検索サイトのアラート

サービスに登録し、自身が運営する以外のドメインで EC サイトが存在するかをチェックする

- 自身が運営する EC サイトで掲載している画像を検索サイトで画像検索し、同じ画像を掲載している EC サイトが存在するかをチェックする
- 自身が運営する EC サイトに掲載している文章を検索サイトで検索し、文章を盗用した EC サイトが存在するかをチェックする

6.2.3. 商標権の取得等

基本的なことですが、商標権を取得してそれを自身のサイトに使用しておくことにより、商標を真似された場合には商標権侵害として侵害を証明しやすくすると共に、商標が真似されていない場合にはなりすまし EC サイトであることを識別しやすくすることができます。

また、サイトを真似された場合には、著作権を主張することもあるものの、著作権は必ずしも証明が容易ではないことから、著作権登録やスクリーンショットの保存等により、ある時点で既に存在又は使用していたことを主張しやすくすることができます。

6.2.4. 電子証明書（SSL サーバ証明書）

電子証明書には、「このウェブサイトは本物の○○社が運営しており、正しい URL は△△△である」ことを裏付けるものがあります。この証明書のことを「SSL サーバ証明書」と呼んでいます。SSL サーバ証明書を用いると、ウェブサイトが偽装されているものかを調べることができ、また消費者とウェブサイト間の通信を暗号化することができます。

SSL サーバ証明書にはいくつかレベルがあり、DV SSL サーバ証明書（ただし、ドメインの確認のみ）、OV SSL サーバ証明書、EV SSL サーバ証明書があります。

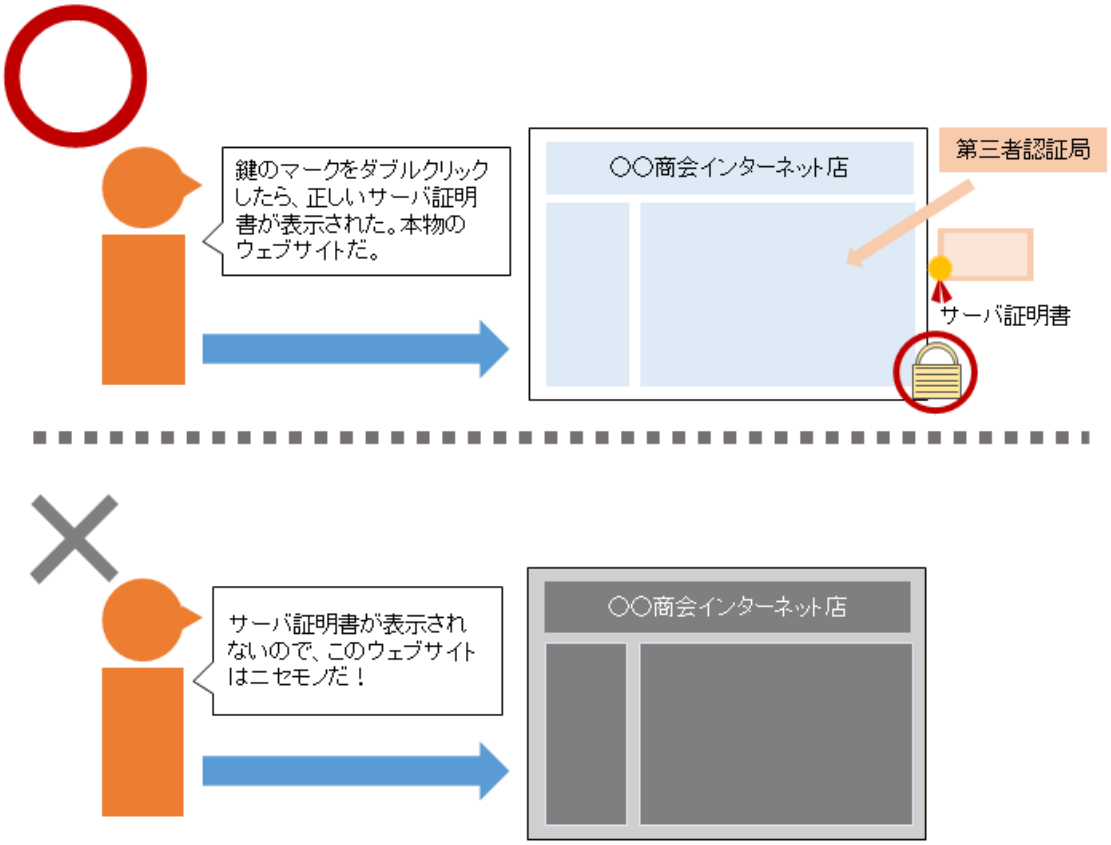
一番レベルの高い EV SSL サーバ証明書の例をご紹介します。ウェブサイトの URL に https でアクセスすると、ウェブブラウザのアドレスバーが緑色になり、カギのアイコンが表示されます。このアイコンをクリックすると SSL サーバ証明書が表示されます。

・InternetExplorer11 の合

・Mozilla Firefox Ver.36 の場合

・Google Chrome Ver.40 の場合

- 電子証明書の仕組み



電子証明書については、下記のサイトを参考にしてください。

シマンテック　技術者でなくても分かる 電子証明書と PKI 入門 http://www.symantec.com/ja/jp/page.jsp?id=pki-basics

GMO グローバルサイン SSL とは？ https://jp.globalsign.com/service/ssl/knowledge/

6.2.5. ウェブサイトや運営者情報の登録

そのほか、ウェブサイトや運営者情報を信頼された第三者機関に登録したり、サイトにマークを貼ったりするしくみもあります。このようなサービスについては、下記のサイトを参考にしてください。

公益社団法人日本通信販売協会　オンラインマーク制度 http://www.jadma.org/ost/

株式会社 TradeSafe　TradeSafe トラストマーク http://www.tradesafe.co.jp/

JIPDEC(一般財団法人日本情報経済社会推進協会)　ROBINS シール http://robins-cbr.jipdec.or.jp/usecase/robinsseal/

6.2.6. その他

6.2.1 から 6.2.4 までは、自社 EC サイトが本物であることを証明するための予防法を解説しました。EC サイト以外にも保護の必要があるものとして、電子メールや宣伝用 SNS アカウント等があります。

電子メール

インターネット上では、情報の送り手の顔が見えません。そのため、メールの送信者が、本当に本人のものなのか、第三者のものなのかを確認することは困難です。

その送信者を特定するための技術としては、主に S/MIME(エイスマイム)や DKIM（ディーキム）が使われています。

S/MIME では、電子メールに、電子証明書を利用した電子署名を付与し、送信者の特定をします。また、発信されたデータが改ざんされたものでないことも検知できますので、電子商取引を安心して行なうことができます。

S/MIME については、下記のサイトを参考にしてください。

シマンテック セキュアメール ID
http://www.symantec.com/ja/jp/secure-mail-id/

GMO グローバルサイン　S/MIME とは
https://jp.globalsign.com/service/clientcert/knowledge/smime/

JIPDEC(一般財団法人日本情報経済社会推進協会)　S/MIME とは
http://jcan.jipdec.or.jp/smime/

また、DKIM では、送信者のドメインを認証し、送信主体を特定します。DKIM については、下記のサイトを参考にしてください。

dkim.jp　dkim とは
http://www.dkim.jp/dkim-jp/about-dkim/

この DKIM を可視化して、安心してメールを開けるようにしたしくみもあります。

JIPDEC(一般財団法人日本情報経済社会推進協会)　安心マーク
http://robins-cbr.jipdec.or.jp/usecase/anshinmark/

宣伝用 SNS アカウント等の管理

宣伝のために利用している SNS アカウントやブログが不正アクセスされ、なりすまし EC サイトへの誘導リンクが投稿される事例があります。宣伝用アカウントの管理を徹底することをお勧め致します。

7. おわりに

本マニュアルは、「なりすまし EC サイト対策協議会」が実施したアンケート結果や検討会議の内容を元に作成したものです。

「なりすまし EC サイト」に起因する問題は、一定の落ち着きをみせているとの報告もありますが、犯罪者はこの後も少しずつ手口を移行させてくるものと思われますので、気を緩めることなく着実に、諸対策を講じていくことが大事です。

今後も、関係各団体・企業のウェブページや一般社団法人セーファーインターネット協会では、啓発情報を発表して参りますので、逐次ご参照いただければ幸いです。

以上

8. 関係関連団体・政府機関紹介

項目	関係関連団体・政府機関名	URL
E コマース	公益社団法人日本通信販売協会	http://www.jadma.org/
	一般社団法人日本流通自主管理協会	http://www.aacd.gr.jp/pc/
	楽天株式会社	http://corp.rakuten.co.jp/
セキュリティ	アルプス システム インテグレーション株式会社	http://www.alsi.co.jp/
	株式会社カスペルスキー	http://www.kaspersky.co.jp/
	キヤノン IT ソリューションズ株式会社	http://www.canon-its.co.jp/
	G DATA Software 株式会社	https://www.gdata.co.jp/
	株式会社シマンテック	http://www.symantec.com/ja/jp/
	株式会社セキュアブレイン	http://www.securebrain.co.jp/
	ソースネクスト株式会社	http://www.sourcenext.com/
	デジタルアーツ株式会社	http://www.daj.jp/
	トレンドマイクロ株式会社	http://www.trendmicro.co.jp/jp/
	BB ソフトサービス株式会社	http://www.bbss.co.jp/
	マカフィー株式会社	http://www.mcafee.com/jp/
	一般社団法人 JPCERT コーディネーションセンター	https://www.jpcert.or.jp/
	一般財団法人日本情報経済社会推進協会	http://www.jipdec.or.jp/
プロバイダ・IT	一般社団法人テレコムサービス協会	http://www.telesa.or.jp/
	一般社団法人電気通信事業者協会	http://www.tca.or.jp/
	一般社団法人日本インターネットプロバイダー協会	http://www.jaipa.or.jp/
	一般社団法人日本ケーブルテレビ連盟	http://www.catv-jcta.jp/
知的財産権	一般社団法人ユニオン・デ・ファブリカン	http://www.udf-jp.org/
金融・決済	一般社団法人全国銀行協会	http://www.zenginkyo.or.jp/
	一般社団法人日本クレジット協会	http://www.j-credit.or.jp/

オブザーバー	内閣官房 IT 総合戦略室	
	消費者庁 消費者政策課	
	警察庁 情報技術犯罪対策課	
	経済産業省 情報経済課	
	経済産業省 模倣品対策室	
	総務省 消費者行政課	
	内閣官房 情報セキュリティセンター	
	一般社団法人 EC ネットワーク	http://www.ecnetwork.jp/
	独立行政法人国民生活センター	http://www.kokusen.go.jp/