TOPICS

法的リスクマネジメント講座 第91回

中小企業を狙い撃ちにするサイバー攻撃にどう備えたらよいか

～EC（電子商取引）サイト防衛編～

長谷川俊明法律事務所
弁護士
長谷川 俊明

はじめに

中小企業を狙い撃ちにし、減少する気配のないサイバー攻撃に対し、中小企業が低コストでできる防御策を連載形式で探ってきました。今回は、「EC（電子商取引）サイト防衛編」として、同サイトにおける顧客個人情報の漏洩をどう防いだらよいかに焦点を絞って検討します。

背景　中小企業によるECサイト活用増大

ECサイトを活用して事業の拡大をめざす中小企業が増えています。背景には、EC市場が個人事業主も手軽に参入でき、大きな資金を要しない点があります。

反面、ＥＣサイトがサイバー攻撃の標的にされ、顧客の個人情報を大量に流出させてしまうケースが多く発生しています。ＥＣサイトには、適切なセキュリティ対策が欠かせないとされるゆえんです。

対策の前提　弱みを知りましょう

ECサイトのセキュリティ対策の前提としては、ECサイトがどこに弱みをかかえるかを知るべきです。

ECは、エレクトロニック・コマース（Electronic Commerce）の略で「電子商取引」のことですから、ECサイトは、インターネット上に電子商取引を行うための情報を蓄積しているコンピューターシステムを指します。

ECサイトの開設は、それほど時間やコストをかけることなく簡単にできる場合がほとんどです。EC事業には、B to B（事業者間）とC to C（個人間）の取引があり、Bは個人事業主を含みます。

中小や個人の小売業でもECサイトの開設によって、容易に市場における“売主”になれるのが特色です。この場合、“買主”は、一般消費者であることが、多く想定されます。インターネットを介して広く世界にも開かれるのがECサイトの“強み”ですが、逆にこれが最大のリスク要因になるのです。

組織的な手口を分析しましょう

警察庁は、今年3月15日までに国内事件の捜査を通じて明らかになった、外国のフィッシンググループによる組織的な手口の分析結果を公表しました。なかには、次のような手口があり、ECサイト防衛上の重大な脅威になっています。

グループは匿名性の高いSNSなどでメンバーを募集し、役割分担をして連絡を取り合い、実行役が偽サイトを設置して誘導された個人から、クレジットカードの情報などを盗み出していたといいます。

さらに警戒すべきこととして、盗んだ情報はサイバー犯罪者らが集う掲示板サイトで売買され、タバコなどの商品の不正購入にも使われていたそうです。

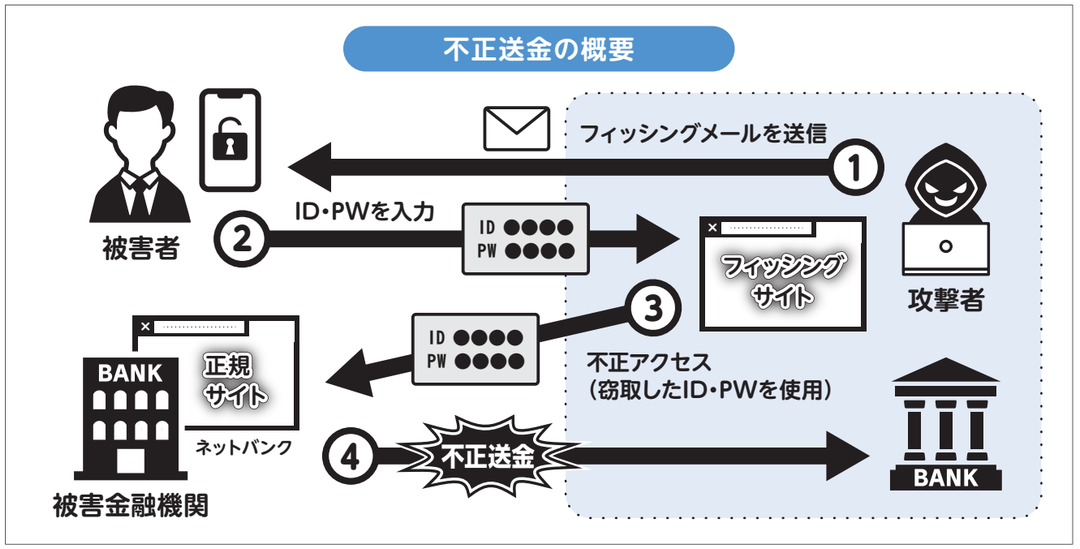
サイバーセキュリティ大手企業によれば、犯罪者の間では精巧な偽サイトを簡単につくれるツールキットが数千円から数万円で売買され、フィッシング攻撃を容易にしているといいますから余計に怖くなります。

顧客個人データの大量ネット流出をなぜ防止すべきなのか、その影響を考えましょう

代表的なECサイトは、ショッピングモールに出店して小売店が開くものです。一般消費者を買主とする売買の代金決済が少なからずクレジットカードによって行われています。

そのため、ECサイトは上記のようなフィッシンググループの格好の攻撃ターゲットになってしまうのです。犯罪者グループの狙いは、クレジットカードに含まれる顧客の個人情報です。攻撃が“成功”した暁には、大量の個人データがネット流出し、世界中に拡散してもおかしくありません。

その結果、流出した個人情報の保有者本人に直接的被害が生じるかもしれません。ECサイトを開設した小売業者は、サイトからの個人データの流出を防止すべきリスク管理体制構築に不備があったとして、顧客から、集団的訴訟を提起されるかもしれません。



出典：サイバー空間をめぐる脅威の情勢等｜警察庁Webサイト（npa.go.jp）

ＥＣサイト開設者にとって致命的なダメージになりうるのが、レピュテーションリスク※であり、デジタル社会でビジネスを行ううえで最も基本的なのは、デジタルデータの適切な管理です。これが行われずデータ流出の有効な防止策もほとんど講じていないとの評判が立つだけで、ＥＣ市場のプレーヤー“失格”の烙印を押されたも同然なのです。顧客・取引先は離れていってしまいます。

（※）自社に関するネガティブな評判や噂が社会的に拡散されブランド価値や企業価値の信用低下を招くリスク

ポイントは、データ流出をどう防止したらよいかです フィッシング対策が急務です

顧客の個人データなどを盗み出されないようにするには、犯人グループの常とう手口をよく研究する必要があります。ECサイト攻撃の場合、とくに目立つのがフィッシングによる盗取なので、これに遭わないようにするのが最善の防衛策です。具体的には、怪しげなサイトに近づかないことです。“本物”のサイト運営者による警告が出ていないかどうかにも日頃から注意が必要です。

フィッシングを使った手口の特徴は、ECのための偽サイトをつくり、そこに集まった潜在的顧客による閲覧者情報などを“一網打尽” に取得しようとする点にあります。

ショッピングサイトなどで売買契約にまで至った場合であれば、代金決済に使うクレジットカード情報が盗み出されてしまいます。上の図は、同情報が不正送金に使われる場合の流れを示しています。

ちなみに、フィッシングの文字通りの意味は、「魚釣り」です。偽の餌をまくなどして誘い込んだ魚を一本釣りする、あるいは網で一挙に捕獲するのは、典型的なフィッシングのやり口です。

偽のECサイトに集まる閲覧情報は魚にたとえられています。乱暴な話ですが、犯罪行為ですから仕方ありません。

おわりに

フィッシングの直接被害を受ける多くは、偽の網にとらわれてしまう個人消費者です。被害防止に最も必要なのは、偽ECサイトに、閲覧をしたりして近づかないことです。ただ、フィッシングの手口も、日々高度化していますから、消費者に負担を押しつけるのは、酷というものです。

ECサイトを開設している企業サイドで、次のような、組織としての防止策を講じるべきです。

第一に、自社のサイトが改ざんされたりしていないか日常的監視を怠らず、改ざんや偽サイトに気づいたら、直ちに警察に届け出ることです。

第二に、ECサイトの改ざんや偽サイトの発生を、消費者にいち早く警告する一方で、 本家の自社サイトは公的な認証※を得て信頼できることを広くアピールすることです。

企業は、サイバー攻撃の被害者として行動しているだけでは足りないのです。

（※）公的な認証とは、例えばデジタル庁の行っている公的認証サービスがあります。（下記URL参考）

参考URL

・公的個人認証サービス(JPKI)｜デジタル庁
https://www.digital.go.jp/policies/mynumber/private-business/jpki-introduction/#guidance1
・サイバーセキュリティサーベイ2023 - KPMGジャパン
https://kpmg.com/jp/ja/home/insights/2024/02/cyber-security-survey2023.html
・サイバー空間をめぐる脅威の情勢等｜警察庁Webサイト
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html