OSHALiANG
Intellectual Property Law

サイバースクワッティングに悩まされる企業は規模の大小を問わない

はじめに

サイバースクワッティング（ドメイン占拠）は、今日の米国で顧客を相手に事業を営んでいる合法的な企業を悩ませている最大の問題のひとつである。サイバースクワッティングには多くの形態があるが、最終的な目的は常に同じである。すなわち、うっかり屋の消費者から金銭や貴重な個人情報を盗み取ることだ。サイバースクワッティングを行う者（ドメイン占拠者）は、性急な入力によるドメイン名のスペルの誤りを利用し、合法的な企業の商標やイメージカラーを使用することにより意図的に消費者に混同を生じさせることが多い。

サイバースクワッティングは合法的な企業に多大な損害を与える可能性がある。たとえば、自分たちがサイバースクワッティングの被害者だと消費者側が認識していないことがしばしばあり、時には合法的な企業にとって不利となる中傷的な流言飛語を（ソーシャルメディア、印刷媒体、e メールによる口コミなどを用いて）流し始めることもある。また、サイバースクワッティングの被害者が不満を公言しなくても、将来的に合法的な企業との取引を拒絶するようになるかもしれない。ドメイン占拠者たちが用いる戦術は日々進化している。1 つのサイトが削除されても、3 つ以上ものサイトが新たに出現することが多い。

ドメイン占拠者は、ドメイン登録者の身元を隠蔽するサービス（「ドメイン・プロキシ」サービスと呼ばれることもある）を利用する等の戦術を用いて自分の真の実体を隠すのに長けているため、責任者を見つけるのは往々にして困難であり、そのことが事態を更に錯綜させている。とはいえ、賢明な弁護士が適切なテコ入れを行えば、既存の知的財産権に基づくサイバースクワッティングの解決に利用しうる戦略はいくつか存在する。ドメイン占拠者たちが最もよく使う戦略をいくつか以下に概説する。[1]

1. e メールによるフィッシング（情報詐取）

e メールによるフィッシングは、詐欺師が合法的な企業になりすますために e メールアドレスを利用するという形を取る。一例を挙げれば、詐欺師がカモ予備軍に宛ててオファーレター（内定通知など特に選ばれた人に送られる通知）を送付し、個人情報の提供を求めるが、そのメールは詐欺師自身の金融ビジネスのアカウントにリンクされている、という形である。これらの e メールはアカウント認証を再設定するという口実で送付されることがある。あるいは、通信文の中で消費者金融などのサービスの申し出がなされることもある。

[1] 今回の記事で概説した例の一部は、厳密にはサイバースクワッティングとは見なされないが、各種の事例は話を簡潔にするために「サイバースクワッティング」と総称されている。

カモに財務情報を提供させた後で、詐欺師は被害者の金融関係のアカウントにアクセスするか、詐取した情報を用いて新規のアカウントを開設する。

2. タイポスクワッティング

タイポスクワッティングとは、企業の合法的なドメイン名に酷似したドメイン名（一般的なのは合法的なドメイン名のスペルを僅かに変えただけのドメイン名）をドメイン占拠者が登録する、という状況である。2 つのウェブサイトの類似性ゆえに、消費者は自分が非合法なウェブサイトに誘い込まれたことすら理解できない。多くの場合、タイポスクワッティングを行う者は、合法的な企業のサイトで提供されているサービスに類似したサービスを提供し、合法的な企業の商標やトレードドレスを使用し、時には元のサイトの文言をそのまま使用することさえある。悪漢が消費者の情報を手中にしたが最後、彼らはその情報を用いてクレジットカードを申し込む、消費者の金融口座にアクセスする等、詐取した情報をさまざまな違法な目的に利用することができる。時には、ドメイン占拠者がドメイン名の入力ミスを利用して占拠者自身が管理する別のウェブサイトにリクエストを転送する、という形でタイポスクワッティングが行われることもある。

3. ソフトウェアを利用し、侵害に相当しないドメインにサイバースクワッティング用のウェブページを開設する

ドメイン占拠者が消費者を欺くためのもうひとつの手段は、ウェブページへのリンクを作り出すソフトウェアを利用することである。このウェブページは、当該ページへのアクセスに用いられるリンクに応じて異なる動作を行う。この方法を使えば、ドメイン占拠者が侵害に相当しないドメイン名を登録・使用しながら、同時に合法的な企業の名称や商標の下で詐欺的なサービスを提供するサブページを利用することが可能になる。たとえば、ドメイン占拠者は、米国の三大貸金業者の名称を騙って消費者金融サービスを提供するいくつかの異なるウェブページにつながる複数のリンクを作り出すことができる。ただし、ルートドメインとなるのはドメイン登録者（占拠者）の合法的な事業である。このような状況は企業にとって厄介である。ドメイン登録者が当該ドメイン名について合法的な権利を持っている場合、「統一ドメイン名紛争処理方針」（Uniform Domain Name Dispute Resolution Policy；略称 UDRP）等の解決手段が利用できないであろうと思われるからだ。UDRP の手続に関する詳細な情報については以下の ICANN のウェブサイトを参照されたい：http://www.icann.org/resources/pages/policy-2012-02-25-en.

4. 紛らわしい類似ドメイン名で詐欺的サービスを提供する/競合他社のサイトへの転送

上記のような状況は合法的な企業にとって問題である。被害に遭った消費者から苦情が寄せられるま

で、合法的な企業の側が問題のサイトを知らないことが頻繁にあるからだ。ドメイン登録者（占拠者）が、合法的な企業の名称に商品やサービスを説明する言葉を添えたドメイン名を登録することはしばしばあるだろう。そのようなサイトは、消費者が使用した検索ワードに応じた検索結果の中に反映され、消費者の目に止まるかもしれない。消費者がそのサイトにたどり着いたが最後、ドメイン占拠者は以下のいずれかの手段を用いて収益を上げることができる：クリックスルー広告（バナー広告をクリックすると広告主のサイトに誘導される広告）、詐欺的サービスの提供、詐欺師自身が管理する別のサイトへの消費者の誘導。この種のサイバースクワッティングの別の形態は、ドメイン登録者（占拠者）が合法的な企業の名称ないし商標を使用しているが、説明的な言葉（.review、.loan、.shoe 等）を付け足した新規のジェネリックトップドメイン（gTLD）を使っている場合に発生する。

結論

残念ながら、警察にとってサイバースクワッティングは予防困難で時間のかかる取締対象だというのが事実である。本論に例示してきたように、多くの異なる戦術が使用されており、実行者の身元が露見するのを免れようと試みる中で、戦略は常に進化しつつある。ドメイン占拠者は多数のサイトを同時に運営していることがしばしばあり、特定の 1 つのサイトに大きな投資を振り向けることはない。その結果、企業は 1 つのサイトを削除させるためにリソースを消費しなければならないが、そんなことをしてもドメイン占拠者は次のサイトに移っていくだけなのである。この問題をいっそう悪化させるものとして、タイポスクワッティングの実行者がつけ込むスペルの入力ミスには何十万もの異なるパターンがあり、1,000 を超える数の gTLD があるという事情がある。それゆえ、防衛的なドメイン名登録が常に役立つわけではない。従って、ある会社のドメイン名の入力ミスとして普通に考えられるスペルを予防的に登録するという対策は、お勧めできないこともある。ドメイン占拠者たちが採用する戦術の恒常的な変幻性は、サイバースクワッティングが行われているサイトを特定し排除するプロセスを合理化するための新たな方策を、企業が持続的に模索しなければならないということを意味する。

ドメイン名保護および商標の専門家である同僚の Osha Liang は、以上に概説したような類のサイバースクワッティング行為により攻撃を受けたクライアントのために、費用対効果の高いやり方で多くの事案を解決している。サイバースクワッティング問題の解決にあたって支援を必要とされる場合には、ためらわず当事務所までご連絡頂きたい。