ネットワーク時代の知的所有権入門

あなたは注意していますか?

ネットワーク知的所有権研究会
●
弁護士　宮下佳之
Yoshiyuki Miyashita
●
弁護士　寺本振透
Teramoto Shinto
http://www.st.rim.or.jp/~terra/

第36回

不正アクセスの法的分析とサイバービジネスにおける対処法について

●●● 1. ログイン名とパスワードによる本人の同一性確認システムの問題点

最近、有料でコンテンツを提供しているウェブサイトもずいぶん増えてきました。あらかじめオフラインで会員登録手続きをした正規の会員に対してログイン名とパスワードを発行し、このログイン名とパスワードによって、本人の同一性を確認する例が多いようです[❶]。

また、社内のLANに社外からリモートアクセスができるように、ダイアルアップ接続の設定をする企業もずいぶん多くなってきました[❷]。この場合も、ログイン名とパスワードによって、LAN上のリソースへのアクセス権が認められた者か否かを識別することにしている場合がほとんどです。

ネットワークの外の世界では[❸]、会員しか入場できない施設の入り口には、門番がいて、身分証明書や会員証の写真と目の前の人物の顔とを照合して、入場が認められた者かどうかを確認する方法などが用いられます。しかしネットワークの世界では、アクセスしようとしている人物の顔を（通常は）確認できないので、正規の会員しか知らない（はずの）ログイン名とパスワードを入力させることによって、本人の同一性を確認することにしているわけです[❹]。

このログイン名とパスワードによる本人の同一性確認システムは、「これらの情報を知っているユーザーは、本人しかいないだろう」という前提の下で成り立っているものでありますが、読者の皆さんもご承知のとおり、ログイン名やパスワードは、漏出したり解析されたりする危険がつきまとっており、きちんと管理していないと相当危うい面もあります[❺]。

何らかの方法で、正規の会員のログイン名とパスワードを入手して、正規の会員になりすまして、有料のコンテンツをただで入手したり、正規の会員向けの有料サービスの提供を受けたりする例も後を絶たないようです。また、本人になりすまして、本人の名誉を毀損するような発言をしたりするケースも頻発しています[❻]。

コンテンツの利用料は、多くはクレジットカードや銀行振込によって、決済する仕組みになっているので、本人の同一性をきちんと確認できるシステムは、大変重要です。正規の会員以外の者が正規の会員になりすまして、コンテンツを入手すれば、正規の会員の口座から利用料が引き落とされることになり、会員が被害を被ることになりますし、「アクセスしたのは俺じゃないから、利用料は払わない」と言われて、利用料を回収できなければ、コンテンツ提供者が被害を被ることになります。また、社内LANに外部の者にアクセスされれば、社内の機密事項が漏洩したり個人のプライバシーが侵害されたりすることになりますから、大問題になりかねません。

●●● 2. 不正アクセスに適用される法律の概要

1.刑事責任に関する法律

第三者の住居等に「正当な理由がないのに」「侵入」すると、住居侵入罪[❼]という罪を犯したことになります。この住居侵入罪で問題とする「侵入」とは「（住居の平穏を害する態様で）立ち入ること」と解されており、物理的に人間が住居等に立ち入ることを想定したものです。したがって、ネットワークへの「侵入」は、住居侵入罪を構成するものではありません。また、「他人の財物を窃取した者」は、窃盗の罪[❽]に問われることになりますが、「窃取」とは「占有者の意思に反して、その占有を

インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

侵害し、目的物を自己又は第三者の占有に移すこと」と解されており、物理的な物の所持[9]を問題としています。そのため、ネットワークに不正にアクセスして一定のデータを入手することが「窃盗」に該当すると考えるのは、相当難しそうです。

もっとも、ネットワークに不正にアクセスして、コンピュータや記録データを「損壊」することなどにより、コンピュータに「使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者」は、電子計算機損壊等業務妨害罪[10]という罪を犯したことになります。また、コンピュータに「虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法な利益を得、又は他人にこれを得させた者」は、電子計算機使用詐欺罪という罪を犯したことになり、刑事責任を問われることになります。さらに、不正にダウンロードしたものが著作物であれば、著作権侵害の罪が問題とされる余地があります[11]。

しかし、ネットワークに不正にアクセスすること自体に関しては、犯罪は成立しないという見解が一般的であるため、「不正アクセス禁止法制の整備」についての検討が必要であると言われております[12]。

2.民事責任に関する法律

不正アクセス自体については、今のところ犯罪が成立しないと言っても、損害が発生すれば、被害者から損害賠償の責任を問われることになるし[13]、ネットワークへの不正アクセスは、他人の所有物（つまり、一定のコンテンツ等が記録された媒体を含む、コンピュータ）上の所有権を侵害し、または侵害するおそれのある行為であるので、差し止め請求[14]の対象にもなると考えられます。

●●●3.不正アクセスに対する対応策

最近、不正アクセスによる被害がかなり増加しているようです。今後ネットワークの普及に伴って不正アクセスによる被害は、より一層増大することが予想されます。すでに申し上げたとおり、日本では不正アクセスに関する法律が十分整備されているとは言えない状況であるので、ネットワーク管理者およびネットワークに参加するユーザー自身が、セキュリティーの重要性についての自覚を持って自ら対策を講じていく必要がありそうです。

では、次に、寺本氏に別の観点から不正アクセスに関する問題についてお話しいただきましょう。

---

[1] BitCashのように、プリペイド方式の場合には、匿名のまま有料コンテンツをダウンロードできますが、その場合でもBitCashカードの裏面に印字されたカード情報によって、利用権限のある者であるか否かが識別されることになります。なお、BitCashの仕組みをより詳しく知りたい方は、http://www.bitcach.co.jpを参照して下さい。

[2] 確かに、社外から社内のLANのリソースにアクセスできれば便利ですが、不正アクセスのリスクを考えると、ダイアルアップ接続の設定をすることにも躊躇を感じます。私の所属する事務所でも、専用線を引いてサーバーを立ち上げたものの、いまだにリモートアクセスができるように設定していません。気にしすぎかもしれませんが、万一のことを考えると、不正アクセスのリスクを過小評価するのも危険であると思います。

[3] もちろん、人物の顔写真で本人の同一性を確認する手法も完全ではありません。整形手術の技術もかなり進んでいるようだし、世の中には、自分にそっくりの人物もいるかもしれませんよね（それに、“Mission Impossible”のトム・クルーズみたいなスパイも、もしかしたら、いるかもしれない！）。とは言え、顔写真による本人の同一性確認システムは、相当程度信頼でき、かつさほど費用もかからない方式であるものと思われます。

[4] 最近は、指紋等のような個人の身体的特徴によって、本人の同一性を識別するシステムも実用化されつつありますが、今のところ、多くのシステムは、ログイン名とパスワードに頼っているのが実情です。

[5] ユーザー側の管理がずさんである例としては、「ログイン名とパスワードを忘れないようにメモして、机の近くに張り付けていた」、「ログイン名をそのままパスワードにした」、「そもそもパスワードの設定をしていなかった」等が挙げられます。

[6] たとえば、朝日新聞の1997年11月27日朝刊によると、ある女性会員になりすまして、「失楽園して」等と書き込みをした者が、名誉毀損の容疑で逮捕された事件も起きているようです。

[7] 刑法第130条。刑罰は、「3年以下の懲役又は10万円以下の罰金」です。

[8] 刑法第235条。刑罰は、「10年以下の懲役」です。

[9] 刑法第245条には、「電気は、財物とみなす」との規定があるので、「電気」については、窃盗の罪が問題となり得ます。そこで、「自然力の利用によるエネルギー」に関しては、この規定を手がかりに、窃盗の罪を問題とすることが考えられますが、記録媒体という物理的なものではなく、電子的データ自体に関して、窃盗の罪で言う「窃取」があり得ると考えるのは、困難です。

[10] 刑法第234条の2。刑罰は、「5年以下の懲役又は100万円以下の罰金」です。

[11] 著作権法第119条。刑罰は、「3年以下の懲役又は100万以下の罰金」です。

[12] 1995年7月21日付の「セキュリティ・プライバシー問題検討委員会報告書」や1997年6月9日付の「情報通信ネットワークの安全・信頼性に関する研究会報告書」等において、その趣旨の提言がなされています。なお、上記「情報通信ネットワークの安全・信頼性に関する研究会報告書」によると、米国、英国、フランス、ドイツ、カナダにおいては、すでに、不正アクセスを禁止する法律が制定されているようです。

[13] 民法第709条には、「故意又は過失に因りて他人の権利を侵害したる者は之に因りて生じたる損害を賠償する責に任ず」と規定されています。この規定で言う「権利」の侵害は、「必ずしも厳密な法律上の具体的権利の侵害であることを要せず、法的保護に値する利益の侵害をもって足りるというべきである」（東京高裁平成3年12月17日判決）と解されていますから、コンテンツを不正に取得された場合にも、この規定に基づいて損害賠償ができるものと思われます。

[14] 不正競争防止法によると、「不正の手段による営業秘密を取得する行為」により、「営業上の利益を侵害され、又は侵害されるおそれがある者」は、「侵害の停止又は予防を請求することができる」ものとされていますが、ネットワークへの不正アクセスは、他人の物理的なものを勝手に使用する行為を伴うものであるので、所有権侵害に基づく差し止め請求も可能であると考えられます。

©1994-2007 Impress R&D

1. “ニセ夜間金庫”問題

“ニセ夜間金庫”事件を覚えておいででしょうか？ 本物の夜間金庫の前に“故障中ですのでアチラの臨時金庫をお使いください”という表示を出しておいて、ベニヤ板で巧みに作ったニセモノの夜間金庫に、銀行の顧客が現金を投入するのを待って、後でごっそり現金を持ち出そうという犯行の試みでした。現実には、銀行の顧客があまりにうまくだまされて、どんどんニセ夜間金庫に現金袋を投入したため、その重みでベニヤ板がゆがんで現金袋が表に顔を出してしまったために、犯人の目的は達成されなかったと記憶しています。私がまだ子供のころの事件でした。古い事件ですし、犯行の目標にされた金融機関の名誉のため、あえて詳しい情報は、ここには書きません。

さて、インターネット上のB to C（企業対消費者）の商売を議論するときには、正当な消費者のふりをして企業に害を及ぼすような不正アクセスを防止する方法について、よく議論されます。しかしながら、正当な商店のふりをして消費者からお金をまきあげる“不正なアクセス勧誘”については、それほど議論されていないようにも見えます。それもそのはずで、さまざまな委員会や業界団体の議論の場に出てくる企業は、もともと、自分が“不正なアクセス勧誘”をするつもりはありませんから、自分に対して不正アクセスがなされることを防止すれば足りるように、一応は見えるからです。

しかしながら、一般の消費者の立場からすれば、“自分は別に不正アクセスをしようとは思っていないから、企業が不正アクセスを防止するのは御随意にといったところです。だが、自分が正当な商店にアクセスしているつもりが、実は、ニセ商店にアクセスしていたという事故を回避するためには、どうすればよいのだろうか？”ということが大きな関心事となります。

本当は、正当に商売をしようと思っている企業の側としても、“不正なアクセス勧誘”を防止する仕組みについて、もっと関心を持たなければならないはずです。それは、次のような状況を心配する必要があるからです。仮に、インターネット上に“ニセ商店”が横行し、消費者がだまされて“金は払ったが商品が来ない”という事件が続出したとしましょう。消費者は、仮に正当な商店にアクセスしているときも、“これは本物だろうか？”という疑いを払拭することはできないでしょう。その結果、ネット上のB to Cの取引が萎縮し、結局、正当な商売を行おうとする企業にとってもはなはだ不都合なことになります。

2. さまざまな防御策

さて、“ニセ夜間金庫”的な犯罪のえじきにならないためには、どのような防御策を講じればよいのでしょうか？ おそらくは、以下に列挙するものを含めたいくつもの対策を組み合わせていくことになるのでしょう。

1.認証システムの活用

業界の現在の議論の中では、いわゆる認証システムは、ネット上の商店にアクセスして買い物をしようと試みる人がその本人に間違いないかどうかを、商店や決済を処理する金融機関が確認できるようにするために利用されようとしているようです。しかしながら、それだけではなく、逆に、消費者が、今アクセスしている商店が本物であるかどうかを確認できるようにするためにも利用されるべきでしょう。

ただし、消費者側からすると、仮に“そのネット上の商店が本物である”と確認できたとしても、それで安心できるわけではありません。依然として、次のような疑問が残ります。

その“本物”とはいったい誰なんだ？いちいち登記簿謄本をとって確認するわけにはいくまい。

その“本物”は、本当に信頼できる商店なのか？ たとえば、対面の取引で何度もヤマト運輸やFedExに荷物の配送を頼んできた人ならば、ネット上にあるヤマト運輸やFedExらしく見えるサイトが本当にヤマト運輸やFedExに間違いないと確認できれば、あとは、そんなに心配する必要はなくなります。あるいは、長年多くのSONY製品を愛用してきた人ならば、ネット上にあるSONYらしく見えるサイトが本当にSONYのものに間違いないと確認できれば、ほぼ安心して買い物ができます。ですが、多くの場合、ネット上で初めて知った企業と初めて取引をすることになります。したがって、それが本物であると確認できたとしても、消費者は安心できないのです。

さらに、ネット上で電子決済手段を用いて支払いを済ませてしまったものの、商品がいつになっても届かないという事態を防ぐためには、どうすればよいのでしょうか？

2.Payment upon Delivery

これは、商品の引き渡しがあったことを確認し、初めて代金の決済を行うという考え方です。

たとえば、ネット上で、電子決済手段で支払いができるようにして、コンピュータプログラムを販売している商店があるとします。もし、先に支払いをすませないとプログラムのダウンロードができないとするとどうなるでしょうか？ 仮にそれが正当な商

インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

Illust:MACOTT

店であったとしても、ダウンロード中に消費者のコンピュータがハングしたとすると、消費者は損失を被ります。ニセ商店ならば、消費者のコンピュータのハングか回線の切断を装って、うまく金だけをせしめるように仕組むでしょう。困ったことには、多くの消費者が利用している汎用システムには十分な程度にまでは信頼性がないため、いつコンピュータがハングしてもおかしくはありません。したがって、ニセ商店が、それを装うこともおそろしく容易なこととなります。当然、コンピュータのハングに対して、システム供給者は、責任を負うつもりはないでしょう。それが“仕様”なのですから。

このような状況に対して、正当な商店と消費者とは互いの知恵と協同によって対処しなければなりません。正当な商店は、なるべくPayment upon Deliveryのポリシーを採用すべきです。たとえば、プログラムの販売であれば、プログラムのファイルが完全に消費者側のシステムにダウンロードされたことを条件として、消費者側のシステムから商店に向けて電子決済手段による支払いが実行されるような仕組みを採用するということです。また、消費者も、そのようなポリシーを採用している商店を選んで取引をするようにつとめ、ニセ商店が横行する機会を減らすように誘導していくべきでしょう。

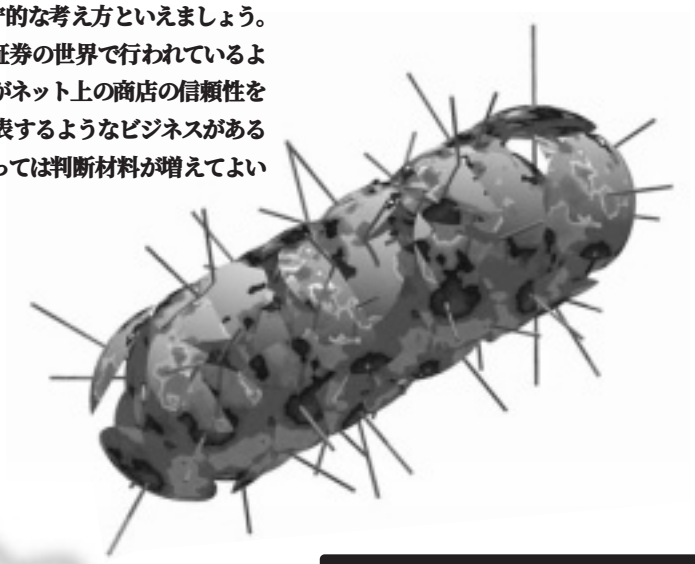
ネット上で商品の引き渡しを完結できない商品（パソコン、書籍など）の場合には、“商店”と“信頼できる宅配業者”と“電子決済手段の提供者”との三者が提携し、かつ宅配業者が消費者に商品を届けたという確認データを電子決済手段の提供者に送ることにより、初めて商店向けの決済が行われるような仕組みを採用することが望まれます。この文脈においては、商店がどのような宅配業者を採用しているかを表示する一方、信頼できる宅配業者を採用している商店を消費者が選択して取引することも重要です。

3.メンバーシップ制、格付け

もっとも、すべての商品またはサービスについて、Payment upon Deliveryのポリシーを採用できるとは限りません。先にお金を受け取らないと商品を作るのが困難な場合もあるからです。

このような場合、消費者としては、ある程度信頼できる電子決済手段の提供者のメンバーになっている商店との取引を選択することによって、電子決済手段の提供者のチェックシステムに依存することも考えられます。この文脈においては、流通自由な電子マネーを使っていきなり買い物をするのはなかなか問題があり、クローズドな電子決済手段での買い物を選択するようにしておくことも保守的な考え方といえましょう。

あるいは、証券の世界で行われているように、第三者がネット上の商店の信頼性を格付けして公表するようなビジネスがあると消費者にとっては判断材料が増えてよいのでしょうね。



e-mail ip-law@impress.co.jp

皆様からのご質問、ご意見は、こちらのメールアドレスで受け付けております。お待ちしております。

©1994-2007 Impress R&D

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp

Copyright © 1994-2007 Impress R&D, an Impress Group company. All rights reserved.