

論 説

インターネットを介した認証回避手段の 有償供与行為の可罰性

—不正競争防止法および刑法の観点から—

古川原 明 子

1. はじめに¹

音楽や映画のデジタル化や情報通信技術の著しい進展を背景に、デジタルコンテンツの提供事業が展開され、そこでは著作物の保護の手段としてアクセスコントロール等の技術が活用されてきた。しかし、アクセスコントロール等の新しい技術が開発されれば、それらを回避するための装置やプログラムが開発されるというイタチごっこの状況が生じ、そのような回避装置やプログラムが氾濫することでコンテンツ事業者には甚大な被害が発生している。こうした回避行為を規制し、コンテンツ提供者や業界の利益を保護するために、著作権法や不正競争防止法など関連する分野で法整備が進められてきた²。そこでは、当事者間の差止請求、損害賠償請求等の民事的請求を基本としつつ、侵害の程度が著しく、当事者間の民事的請求にのみ委ねられることに限界があるような行為に対しては刑罰を導入することで、しかるべき利益のより効果的な保護が目指されている。

1 本稿の執筆にあたっては、東京経済大学現代法学部教授・村本武志弁護士に検討の機会とともに、多くの貴重な資料とご意見を頂いた。また、明治学院大学法科大学院長・京藤哲久教授には、業務妨害罪について有益なご指摘を頂いた。その他、不競法の改正から、インターネットや認証回避の仕組みまで、それぞれの専門家にご教示いただく機会を得た。

2 2012年6月15日には、著作権者の許諾なしに音楽や動画を違法ダウンロードする行為に罰則を科す規定やリッピングを違法化する規定を盛り込んだ著作権法改正案が衆議院で可決された。

本稿では、インターネットを通じて、ソフトウェアの認証を回避する手段を有償で供与する行為を取り上げ、当該行為を不正競争防止法および刑法により処罰することの可能性を検討する³。

2. 認証回避手段の概要

本稿は、デジタルコンテンツのうち、ソフトウェア（コンピュータプログラム）を対象とし、その実行の際に求められる認証を回避する手段を、インターネットを通じて供与する行為の可罰性を検討するものであるが、その仕組みの概要を以下に述べ、このような限定された形態に検討の対象を絞ることの趣旨を説明しておきたい。

（ア）ソフトウェアと認証システム

認証とは、アクティベーションとも呼ばれ、「商用ソフトウェアについて、インターネットなどを通じてライセンス認証を行い、使用可能な状態にする仕組み⁴」である。

コンテンツ事業の急成長の中で、コンテンツ事業者は、不正コピーや不正アクセスを防止する技術を用いて、コンテンツに対価が支払わなければコピーを作成できない、あるいは視聴等ができないように、コピー管理技術やアクセス管理技術を施すようになっており、そのために資金と労力を投入している。このようなコピー管理技術やアクセス管理技術の一つが、本稿で対象とする認証システムである。しかし、これらの管理技術の無効化機能を有する装置やプログラムを用いて、管理技術を無効化する行

3 後述のように、認証はコピーコントロールのための技術であると同時にアクセスコントロールのための技術でもあると解されるが、本稿ではそのうちアクセスコントロール機能に着目するため、コピーコントロールと一体化していないアクセスコントロール機能自体を保護の対象としない著作権法については、検討の対象から外した。

4 大辞林（第五版）。

為や、これらの無効化装置等を提供する行為が行われるようになった。このような事態に対処するため、各コンテンツ事業者は、管理技術の高度化に努めてきているが、既存の無効化装置等に耐えうる管理技術を開発しても、ほどなくこの新しい管理技術に対する無効化装置等が発生することになる⁵。

ソフトウェアメーカーにとって、正当な対価を支払わない不正なソフトウェアの使用はおよそ許容しがたい行為である。それは、ソフトウェアの使用に対する対価徴収の確保を妨げ、ソフトウェアメーカーに逸失利益を被らせるにとどまらない。タダ同然でソフトウェアを無制限に使用する不正ユーザーが存在することが広く知られ、かつそれが放置される事態が続くならば、認証システムはその有効性を失うことになり、決して安くはない、むしろ高額といえるソフトウェアを購入した正規ユーザーらが「正しい者は損をする」との不公平感を持つことで、節度を失ったユーザーらによるモラルハザードを招きかねない。さらには、ソフトウェアや管理技術開発者の開発意欲を削ぐことも危惧されるのである。そこで、ソフトウェアメーカーは、多様な管理技術を開発してきたが、一つ一つのソフトウェアに異なる識別番号を付すという方法が従来は一般的であった。しかし、識別番号を付すのみでは、ソフトウェアの不正コピーを十分に防止することはできない。また、一つのライセンスに対して使用できるコンピュータの台数を制限するソフトウェアにおいては、正規品を一度手に入れた以降の複数コンピュータでの使用をいかに防ぐかが重要となるが、これに対処することもできない。特に、一つのライセンスの複数台での使い回しが企業内で組織的に行われた場合には、ソフトウェアメーカーには大きな損害が予想されるが⁶、その実態を把握すること自体が非常に困難であるという

5 経済産業省知的財産政策室編著『逐条解説不正競争防止法（平成21年改正版）』（有斐閣、2010）71-72頁。

6 企業の不正コピーに対して日本国内で初めて訴訟提起があったのは1999年で

限界があった。

そこで新たな管理技術として開発されたのが認証を用いたシステムである。これは、ソフトウェアを使用するコンピュータにインストールして初回に起動する際に、ユーザーに対して一定の手続きを要求するものである。一般に、ユーザーはソフトウェアを購入もしくは体験版として入手する。しかし、そのソフトウェアには、認証を受けなければインストールが完了しない、もしくは一定期間を過ぎると起動できなくなる、あるいは機能が大幅に制限されるといったプロテクトが施されている。そこで、ユーザーは、ソフトウェアの初回の起動に先立って、ソフトウェアメーカーによる認証を受けて、このプロテクトを解除しなくてはならない。この認証の手続きは、ソフトウェアの初回の起動の手順に組み込まれ、ほぼ自動的に開始するいわば強制的な手続きである。ところで、ソフトウェアメーカーの有する認証サーバーには、これまでに当該ソフトウェアを正規入手したユーザーの情報が蓄積・保管されている。その情報とは、ソフトウェアごとに異なる識別番号と、ユーザーのコンピュータの独自の値を持つデータ（ハードウェア情報やMacアドレスなど）により構成された固有情報を対応させて、一定の値としたものであり、認証サーバーにはこの組み合わせが登録・保管されている。新規ユーザーはソフトウェアを初めて起動する際に、当該ソフトウェアの識別番号と、自己のコンピュータの固有情報を認証サーバーに伝え（主にインターネットを通じての送信による）、認証サーバーはこれと登録済みの値との照会を行い、すでに登録した値との重複を確認する。ソフトウェアの識別番号とコンピュータの固有情報の組み合わせが、これまでに登録した値と一部重複するなど、使用規約に反

ある。これは会社ぐるみの不正コピーに対して米MS社など日米のソフト・メーカー7社が東京都内の会社に対して訴訟を起こしたものであり、情報システム部門がマスタ・ソフトを一括管理したうえでCD-RやMOなどに不正コピーして支社や事業所に貸し出すという、大規模で組織的な行為が行われていたと原告らは主張した。日経バイト（2000年1月号）、22頁。

する組み合わせでなければ、ユーザーのコンピュータに、その組み合わせでのみ機能するプロテクトの解除信号を送り、ユーザーはこれを用いることによってソフトウェアを起動できるようになる。他方、識別番号とコンピュータの固有情報との組み合わせに使用規約に反するような不合理な点があれば、使用不可信号をユーザーのコンピュータに送り、ソフトウェアの起動を不可能とする。このような認証システムによって、ソフトウェアメーカーは、ソフトウェアとコンピュータが特定の組み合わせでのみ起動することを確保し、不正コピーや複数台のコンピュータによる一つのソフトウェアの使い回しを防いでいるのである。

インターネットを通じてのソフトウェアの配布という形態は今後増加し続け、いずれ主流となることが予想される。ソフトウェアがCD-ROMやDVD-ROMといった形態をとって販売されるのではなく、インターネットからのダウンロードを可能にすることにより配布される場合には、潜在的顧客によるアクセスが容易になり、販売の機会と効率性が高まる一方で、複数台のコンピュータでの使用は容易となり、不正使用の危険性もまた飛躍的に高まる。デジタルコンテンツには、映像や音楽、データベースと様々なものがあるが、このうちアプリケーションソフトといったソフトウェアは個人による使用のみならず、法人単位での使用が予定されており、不正使用による損害は甚大なものとなる。したがって、認証を無効化する装置やプログラムが流通することは大きな問題であり、コンテンツ事業者は早期の対応を望んできた。そうした無効化の手段の一つとして、ソフトウェアにおける認証を回避することでその効果を無効化する行為に対して、法律による規制、特に刑事罰による規制がどこまで可能なかを検討することは、喫緊の課題と言える。

(イ) 認証回避手段

以上のような認証システムを無効化する手段の供与として、本稿ではインターネットを介した認証回避手段の供与を取り上げる。

ソフトウェアの認証を回避する手段としては、いくつかのパターンが挙げられるが、(1) ユーザーのコンピュータのhostsファイル⁷を改変されたものと置き換える、(2) 正規に配布されたものではないが、起動を可能とするような識別番号を入力する、(3) ソフトウェアのプログラムの一部を改変されたものと置き換える、という手段が、数年前から問題となっている。(1)により、当該コンピュータはソフトウェアメーカーの認証サーバーへのアクセスが不可能となる。(2)により、擬似的に完全版としてソフトウェアを起動することが可能となる。(3)により、認証サーバーによるソフトウェアの使用可・不可の判別が不可能となる。これらの手段の一部もしくは全てをとった結果、ソフトウェアの無制限な使用が可能となり、ソフトウェアメーカーにとって深刻な事態が生じる。しかし、コンピュータのファイルを書き換える手段や、ソフトウェアのプログラムを書き換える手段が、認証を回避する「装置・プログラム」と言えるかは慎重に検討せねばならない。さらに、ファイルやプログラムの書き換えのタイミングが認証サーバーにアクセスする前なのか後なのかによって、可罰行為となるか否かが変わりうるため、適用する規定の構成要件ごとに行為態様を整理した上での検討が必要となる。

(ウ) 供与の態様

こうした認証回避手段の供与が、インターネットを通じて行われた場合には、被害の拡大・防止という観点からは問題が一層大きくなる。その場合、不特定多数の人間が場所と時を選ばずに認証回避手段を入手すること

7 インターネットではサーバーやコンピュータ等にアクセスする際、場所を特定するために数字で構成されたIPアドレスを使用している。URLはそれを分かりやすく文字列に置き換えたものである。このIPアドレスとURLの情報を管理しているサーバーがDNS (Domain Name Server) であるが、同じ情報をローカルコンピュータ (自己が使用するコンピュータ) 上のhostsファイルにも置くことができる。DNSとhostsファイルの情報が異なる場合、後者が優先されるため、hostsファイルにあるIPアドレスにアクセスすることになる。

が可能となり、不正な認証回避手段の存在をこれまでに知らなかった人々にその存在を広く知らしめる機会が増大する。また、匿名性を保持して認証回避手段を供与することが可能になるために、ソフトウェアメーカーは供与者を特定することが甚だしく困難であり、民事的請求を行うことができない。

さらに、インターネットを介した場合は、供与の流れを不透明にすることが容易となる。例えばインターネットオークションを利用した認証回避手段の有償供与にあたって、出品者は落札者へ回避手段を直接供与するのではなく、まずは回避手段の説明書に該当する電子メールを送付する場合がある。書き換えるべきコンピュータファイルのテキストデータや複数の非正規の識別番号など、ソフトウェアの特定のプログラムと置き換えるべきプログラム以外がこのメールに記載され、プログラムについては、それを入手することができるインターネットサイトのURLのみがメールにて示される。そこで、落札者は、ソフトウェアの書き換えに必要なプログラムを、指定されたインターネットサイトからダウンロードすることにより入手するのである。

このような実態を踏まえて、以下では、まずソフトウェアの認証回避手段の有償供与が不正競争防止法の罰則の対象となるかを検討し、次に、当該行為に対して刑法上の主に偽計業務妨害罪が成立するかを検討する。

3. 改正不正競争防止法

2011年5月に成立した「不正競争防止法の一部を改正する法律」は、同年9月13日に「不正競争防止法の一部を改正する法律の施行期日を定める政令」が閣議決定されたことをうけ、同年12月1日より施行された⁸。これ

8 経済産業省知的財産政策室編『不正競争防止法 2011』（2011）。また、改正法の解説として、「特集・不正競争防止法の改正」ジュリ1432（2011）4頁以下の中

まで度重なる改正を行ってきた同法の、2011年改正のポイントは二つある。一つは、営業秘密侵害罪に係る刑事訴訟手続きの特例（営業秘密の内容の言い換え、期日外での尋問等）を設けた点、もう一つは、技術的制限手段に係る規律の強化を図った点である。本稿で対象とする認証回避手段の供与行為は、後者との関係で問題となる。具体的には、ソフトウェアの認証というシステムが不正競争防止法（以下、不競法とする）2条1項11号および2条7項の「技術的制限手段」の要件を満たし、その上で、インターネットを通じての認証回避手段の供与行為が「不正競争」にあたり、これを有償で供与した場合に21条2項4号の構成要件を満たすのかが問題である。なお、不競法は認証回避を行う個別のユーザー（以下、不正ユーザー）については、処罰の対象から除外している。

（ア）不競法2条1項11号

①「他人が特定の者以外の者に影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録をさせないために営業上用いている技術的制限手段」

ソフトウェアが、不競法2条8項の「プログラム」に該当することは、問題がない。

では、ソフトウェアの起動に際して行われる認証は、2条7項の「技術的制限手段」にあたるだろうか。本稿で対象とするソフトウェアは、認証を経なければ起動が不可能となるようにプロテクトがかけられており、ソフトウェアメーカーは認証によって、ソフトウェアの使用が可能か不可能かの情報を、当該ソフトウェアを起動するコンピュータに対してインターネットを介して送信している。すなわち、ソフトウェアメーカーは、ソフトウェアの起動に制約を課す管理を措置しているのであり、その手段として、電磁的方法により視聴等機器が定められたルールに従って反応する信

原裕彦「不正競争防止法の一部を改正する法律の概要」、奥邨弘司「不正競争防止法改正の意義と課題—技術的制限手段の保護について」を参考にした。

号を送信する方式をとっている⁹。このシステムは、2条7項が定める「電磁的方法」により「プログラムの実行」を「制限する手段」であり、コンピュータという「視聴等機器」が「特定の反応をする信号」を「送信する方式」であるから、「技術的制限手段」にあたる¹⁰。

不競法は、技術的制限手段の例として、コンテンツに信号を付してコピーを制限するコピーコントロール技術（SCMS、CGMSなど）と、コンテンツを暗号化して、契約者以外に視聴を制限するアクセスコントロール技術（スクランブル放送など）を挙げている¹¹。本稿で対象とする認証は、正規の識別番号を要求し、これを確認することで不正コピーを防止すると共に、さらにソフトウェアと起動するコンピュータとが使用規約に沿った組み合わせであることを要求し、これを確認することで、正規のライセンス保持者以外による使用を防止している。

したがって、この認証は、正規のソフトウェアを購入し、正規の識別番号を取得した上で、特定のコンピュータにインストールした者という「特定の者」に限って当該ソフトウェアの起動を許可するための手段である。すなわち、そうした「特定の者以外の者」にソフトウェアというプログラムを起動させないための手段である。

この認証は、ソフトウェアの適正かつ公平な販売と切り離すことのできないものであり、ソフトウェアメーカーがその営業上の利益¹²を確保するために必要不可欠のシステムであるから、認証が「営業上用いられてい

9 前掲・注5、逐条解説41頁。

10 経済産業省「不正競争防止法の概要（平成23年度版）」の参考資料「不正競争防止法第2条第1項第10号・第11号及び第7項の構造について（技術的制限手段関係）」参照。（<http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/fukyofoukouzou.pdf>）（2012/06/15アクセス）。

11 経済産業省「不正競争防止法の概要（平成23年度版）」（<http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/h23hontai.pdf>）（2012/06/15アクセス）。

12 この利益には、コンテンツのみならずそれを提供するサービスの信用といった無形の利益が含まれるものと考えられる。前掲・注5、逐条解説74頁。

る」手段であることに問題はない。

したがって、本稿で対象とする認証は、不競法2条1項11号が規定する「他人が特定の者以外の者に影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録をさせないために営業上用いている技術的制限手段」にあたる。

②「技術的制限手段の効果を妨げることにより可能とする機能を有するプログラム」

では、インターネットを通じてこのような認証を回避する手段を供与することは、「不正競争」と言えるだろうか。不競法2条1項11号は、制限されているプログラム（ここではソフトウェアを指す）の実行を、技術的制限手段の効果を妨げることにより可能とする機能を有するものが「装置もしくはプログラム」であることを要求しており、たとえばコピーガード回避機能を持つソフトウェアが念頭に置かれていたものと思われる。

では、本稿で対象とする認証回避手段は「プログラム」であると言えるだろうか。既存のhostsファイルと置き換えるデータと識別番号のみでは、「電子計算機に対する指令であって、一の結果を得ることができるように組み合わせられたもの」（不競法2条8項）という定義を満たすことはないと考えられる。一方、ソフトウェアのプログラムの一部を改変されたものと置き換える場合には、そのプログラムの一部がサブプログラムとして機能しているなど、やはりプログラムであると言える限りにおいては、2条8項の定義を満たしうる。

もっとも、ソフトウェアのプログラムに置き換えるプログラムを含んだ一組のセットとして、hostsファイルの置き換えデータや識別番号が供与されている場合には、全体として「プログラム」と捉える余地はあるだろう¹³。しかし、その場合には、ソフトウェアのプログラムの置き換えのみで

13 装置については「当該装置の部品一式であって容易に組み立てることができるもの」を規制対象とするとの文言があり、プログラムについては「当該プログ

「技術的制限手段の効果を妨げる」ことが可能であるかが確認されねばならない。認証を回避するために、hostsファイルの置き換え、識別番号の入力、ソフトウェアのプログラムの置き換えのいずれが必要不可欠の手段なのか、逆に行わなくても回避が可能なもの（回避効果を補完するために行われるにすぎないものなど）があるのかといった技術的な点は、ソフトウェアとコンピュータのOSの種類に応じて変わりうる。

③「電気通信回線を通じて提供する行為」

次に、インターネットを通じての認証回避手段の供与が、「電気通信回線を通じての提供」にあたるかを検討する。認証の回避を可能とするプログラムが、電子メールに添付して送信される場合や、供与者のHPから直接にダウンロードできる場合であれば、この要件は当然に満たされる。しかし、上述したように、認証の回避を可能とするプログラムをダウンロードできるインターネットサイトのURLを示す行為を、「プログラムを電気通信回線を通じて提供する」行為と言えるのかは難しい問題である。多くの場合、プログラムがアップロードされているインターネットサイトは、無料オンラインストレージと呼ばれるもので、その利用にあたってユーザー登録は不要である。したがって、インターネットサイトにプログラムをアップロードした者（以下、行為者Aとする）と、このインターネットサイトのURLを教えた者（以下、行為者Bとする）が、同一人物であるかを確認することは、ソフトウェアメーカーには不可能である。もちろん、認証回避手段となるプログラムの開発者¹⁴が行為者AやBと同一人物である

ラムが他のプログラムと組み合わせられたものを含む」との文言がある（いわゆる「組込規定」）。しかしhostsファイルの置き換えデータや識別番号はプログラムではないこと、ソフトウェアの置き換えプログラムが必要不可欠の回避手段ではない可能性があることがやはり問題となる。

- 14 装置等の製造行為は、不競法の規制対象とはなっていないため、プログラムの開発行為自体も同様に規制の対象ではないと考えられる。ただし、提供行為の共犯もしくは共同正犯とするなど、既存の法令によって一定程度の対応は可能である。日本弁護士連合会「産業構造審議会知的財産政策部会・技術的制限手段に係

必要はないし、開発者が個々の不正ユーザーにプログラムを直接送信等する必要もない。また、行為者Aと行為者Bが同一人物である必要もない。

しかし、行為者Aと行為者Bが全くの無関係である場合には、行為者Bの行為をプログラムの「提供」と呼ぶことはできない。行為者Bの行為は、「このURLにアクセスすれば回避プログラムをダウンロードできる」という情報を伝えているにすぎない。そのような行為は、雑誌や個人のブログ等で認証回避の手順を紹介したり、認証回避手段の入手先について情報を与えたりする行為と同じである。そのような情報提供を不正競争として規制することは、2011年（平成23年）改正によっても想定されていなかった。不競法見直しの議論では、「回避のためのノウハウなどの情報提供について、改造サービスの提供行為として捕捉することができないことから、回避サービス自体を規律すべきとの指摘もあるものの、平成11年改正当時の検討において、情報提供一般に対する規制につながることであり相当に慎重な検討が必要であるとの理由から、規制の対象としていない」とした上で、「現時点での結論を急ぐ必要はない」として、平成11年改正の姿勢を維持するとの方向性が示されていたのである¹⁵。

もっとも、こうした情報提供に対して、行為者Bを行為者Aの帮助犯とする余地はある。また、雑誌の場合には問題となる記事が雑誌全体に占める割合は少なく、他方、オークションで認証回避手段を販売する行為者Bにとって、URL教示は不可欠の情報提供である点に違いはある。しかし、どれほど重要な（ソフトウェアメーカーにとって致命的な）情報であっても、情報は装置やプログラム自体ではない。およそソフトウェアメーカーに損害をもたらすような情報提供の全てを不正競争とすることは、表現の自由との関係からも問題である。現段階では規制が相当ではない行為、例

る規制の在り方に関する小委員会「技術的制限手段に係る不正競争防止法の見直しの方向性について（案）」に関する意見書」（2011）5頁参照。

15 前掲・注7、小委員会報告書14頁。

例えば雑誌やブログ等でファイルやプログラムの書き換え方法を紹介する行為や、単に認証回避手段の入手先を教示する行為との区別を明確にすることが求められる。

不競法は2011年の改正で、技術的制限手段の効果を妨げる機能を有する回避装置につき、旧法では回避機能「のみ」を有するものに限定していたところを、このいわゆる「のみ」要件を削除することで、回避機能とその他の機能を併せて有するものにまで規制の対象を広げた。旧法が「のみ」要件を付したのは、規制を必要最小限にすることで、映像や音の視聴等装置の提供事業者の開発努力を減退させるなど、過度の抑制効果が生じないように配慮したためである¹⁶。しかし、技術的制限手段回避措置に係る規定を導入した1999年（平成11年）の改正当時には存在しなかった態様の回避装置等の流通が相当数認められ、コンテンツ事業者の被害を一層深刻なものとしている現状と、「のみ」要件の解釈如何によっては適切な規制が困難となることに鑑み、見直しの結果、「のみ」要件は削除された。「のみ」要件に関する議論はもっぱら装置を念頭に行われたようであるが、回避機能以外の機能を有するプログラムも「映像の視聴等を技術的制限手段の効果を妨げることにより可能とする用途に供するために行うものに限る」という制限を付した上で、規制の対象に含まれる¹⁷。しかしこれは、プログラム自体の定義であり、提供の態様を定義する議論ではない。

問題となるケースの大半では、行為者Aと行為者Bは同一人物であるか、意思を通じた関係にあるものと考えられているようだ。例えばインターネットオークションを利用したあるケースでは、行為者Bにあたる者は、

16 前掲・注7、小委員会報告書2頁、4頁以下参照。

17 この要件は装置の客観的な機能面に着目して判断されるべきとされ、見直しにおいても「故意」又は「図利加害目的」を導入することに対しては消極的に考えられていたが（前掲・注7、小委員会報告書6-7頁）、効果無効化という目的としてこれを理解した場合、譲渡者の主観を一切考慮せずに装置等の中核的機能の性質を客観的な機能からのみ判断することは困難ではないかと思われる。

認証回避プログラムがアップロードされているインターネットサイトのURLを教示するにあたって、プログラムのアップロードは一週間程度の短期間であることを同時に落札者に伝えており、実際にそのプログラムは一定期間をすぎると削除されている。こうしたアップロードと削除のタイミングに照らせば（かつそれが多数回繰り返されているとすれば）、行為者Aと行為者Bが同一人物か、少なくとも意思を通じた関係にあると推測することができるだろう。しかし、この点を強制的な捜査権限を有しない個人や企業が確認することは不可能であり、認証回避手段の供与者らがこの点をいわば抜け穴として利用している実態があるものと思われる。

冒頭に述べたように、不競法は旧法においては、差止請求権、損害賠償請求権等の民事的請求の対象にとどめていた技術的制限手段回避装置等の譲渡等の行為に対して、改正により刑事罰を導入した。民事的な救済に関してはいわゆるマジコン事件判決が確定しているが、これは当該事件の当事者に対してのみ拘束力を有し、類似行為を行う者に対しては何らの拘束力を持たない。そのため、判決後も同様の機器を販売する者が絶えない。また、露店でのゲリラ的な販売やネットショップの開設、オークションでの出品の場合には、匿名性が高く、ソフトウェアメーカーらが販売者を特定することは極めて困難であり、民事訴訟を開始することさえできないケースが多い。そうした民事訴訟による問題解決の限界に鑑みて、捜査機関による捜査を含めた刑事上の措置に問題の解決が期待されたことが、刑事罰導入の主たる目的であった¹⁸。そこで、本稿で対象としたインターネットを介した認証回避手段の供与行為が不競法2条1項の「不正競争」にあたり、それが有償で行われている場合に、不競法21条2項4号の構成要件に該当し、処罰の対象となる可能性が高いのであれば、「提供」の実態解

18 産業構造審議会知的財産政策部会技術的制限手段に係る規制の在り方に関する小委員会「技術的制限手段に係る不正競争防止法の見直しの方向性について（案）」（平成22年12月）17頁以下、および、前掲・注7、小委員会報告書18頁。

明は被害者ではなく、捜査機関が強制力をもって行いうる。しかし、ソフトウェアメーカーは多大な労力と時間を費やして捜査機関をその気にさせるための情報を収集せねばならず、しかもその間の被害を黙認せざるを得ない。本稿で対象とした行為は必ずしも特異な形態ではなく、むしろ頻発し、増加する傾向にあるため、「提供」の解釈は大きなポイントとなる。

(イ) 不競法21条2項4号

技術的制限手段回避装置等の供与行為が21条2項4号の罰則の対象となるには、「不正な利益を得る目的」又は「営業上技術的制限手段を用いている者に損害を加える目的」が必要である。認証回避手段の供与が有償で行われている場合は、行為者は供与によって対価を得ているのであるから、21条2項4号に定める「不正の利益を得る目的」があることに問題はなく、当該行為が2条1項11号の「不正競争」にあたるのであれば、刑事罰の対象となる。

(ウ) 従来問題となったケースとの比較

■マジコン事件¹⁹

携帯型ゲーム機を製造、販売する原告及び同ゲーム機用のゲームソフトを格納したゲーム・カードを製造、販売する原告らが、被告らに対し、いわゆるマジコンと呼ばれる機器の輸入、販売等が旧不正競争防止法2条1項10号に違反すると主張して、同法3条1項及び2項に基づき、同装置の輸入、販売等の差止め及び在庫品の廃棄を求めた事案であるが、本稿との関係では、技術的制限手段の定義が重要である。

原告らは、原告仕組みは不競法2条7項の「技術的制限手段」に該当すると主張したのに対し、被告らは、「技術的制限手段」は検知→制限方式のものに限られ、自主制作ソフト等の実行も制限する結果となる検知→可能

19 東京地判平成21年2月27日<LEX/DB25440477>。判例評釈として蘆立順美「技術的制限手段の意義と専用品該当性判断」速報判例解説（法学セミナー増刊）6号279頁以下がある。

方式のものを含まないと主張した。これは、2条7号が「特定の反応をする信号」とのみ規定し、反応の方式を明示していないためである。このような双方の主張に対し、東京地裁は2条1項10号の立法趣旨に照らして、いかなる「技術的制限手段」が念頭に置かれていたのかを検討した上で、検討の段階で具体例として挙げられていたMODチップが検知→可能方式であること点にも触れて、検知→制限方式のものだけでなく、検知→可能方式のものも含むと判示した。

本稿で対象とした認証は、ソフトウェアが正規の識別番号を有することと、ソフトウェアとそれを起動させるコンピュータの固有情報の組み合わせが使用規約に反しないものであることを確認した上で、ソフトウェアの起動を可能とする信号を送信するのであるから、本事案における原告仕組みと同様に、検知→可能方式を基本とする。さらに、その逆の場合にはソフトウェアの起動を不可能とする信号を送るため、検知→制限方式も用いている。

次に、本事案における被告装置と本稿で対象とした認証回避手段を比較する。前者を用いた場合、技術的制限手段は非正規品を正規品として検知してしまい、いわば機械を欺くといった形で視聴機器たるゲーム機を誤作動させることになる。他方、後者を用いた場合には、視聴機器たるコンピュータを認証サーバーにアクセスさせないことにより、認証がそもそも不可能になる。また、前者においては技術的制限手段を阻害する機能を有した装置が譲渡・展示等されるのに対して、後者においては、回避手段が電気通信回線を通じて複数の段階を踏んで供与されるのであり、プログラムの定義や提供の要件の充足が容易ではないことは、上記3（ア）②③で述べた通りである。装置という有体物の譲渡と、プログラムの電気通信回線を通じた提供の違いを踏まえた時に、電気通信技術の更なる拡大と、デジタルコンテンツの普及が今後一層見込まれる現状においては、実態を勘案した上での対応が必要となる。

■Winny事件²⁰

本稿で対象とした回避手段供与行為が、不競法21条2項4号の罰則の対象となるかについて、2条1項11号の「提供」を満たさない可能性があることを、3（ア）③で指摘した。認証回避プログラムを電気通信回線を通じて直接に送信するのではなく、そのプログラムがアップロードされたインターネットサイトのURLを教示する場合にも「提供」であると認めるためには、プログラムをアップロードした者と、URLを教示した者が同一人物もしくは意思を通じた関係になければならないことをそこでは挙げた。しかし、これは教示者が不競法21条2項4号の正犯（共同正犯を含む）たりえるかを検討した場合の議論であり、プログラムをアップロードした者と無関係な者がURLを教示した場合に、回避手段提供行為を片面的に幫助したとして、教示者を幫助犯とする余地はある。前提として、プログラムをアップロードした者に図利加害目的があることが必要だが、その上で、教示行為が幫助と認められるためにはいくつかの点を確認しなければならない。そこで参考となるのがWinny事件である。これは、適法用途にも著作権侵害用途にも利用できるファイル共有ソフトをインターネットを通じて不特定多数の者に公開、提供した者が、正犯者がこれを利用して著作物の公衆送信権を侵害することを幫助したとして、著作権法違反幫助に問われた事案である。ただし、不競法では、個々の不正なユーザーは処罰の対象からは外されているため、不競法違反の正犯は回避手段提供者（すなわちプログラムをアップロードした者²¹）となる点がWinny事件とは異なる点に、注意が必要である。

Winny事件で最高裁は、「単に他人の著作権侵害に利用される一般的可能性があり、それを提供者において認識、認容しつつ当該ソフトの公開、提供をし、それを用いて著作権侵害が行われたというだけで、直ちに著作

20 最決平成23・12・19判時2141号135頁。

21 プログラムの開発行為が規制の対象でないことは、3（イ）で触れた。

権侵害の幫助行為に当たると解すべきではない」として、「かかるソフトの提供行為について、幫助犯が成立するためには、一般的可能性を超える具体的な侵害利用状況が必要であり、また、そのことを提供者においても認識、認容していることを要する」と述べた。その上で、「当該ソフトを利用して現に行われようとしている具体的な著作権侵害を認識、認容しながら、その公開、提供を行い、実際に当該著作権侵害が行われた場合や、当該ソフトの性質、その客観的利用状況、提供方法などに照らし、同ソフトを入手する者のうち例外的とはいえない範囲の者が同ソフトを著作権侵害に利用する蓋然性が高いと認められる場合で、提供者もそのことを認識、認容しながら同ソフトの公開、提供を行い、実際にそれを用いて著作権侵害（正犯行為）が行われたときに限り、当該ソフトの公開、提供行為がそれらの著作権侵害の幫助行為に当たると解する」と述べている。

図利加害目的を有してアップロードされた認証回避プログラムがどこで入手できるのかを、それを求める者に対して教示し、いくつかのデータを供与することと併せて対価を得る者がいた場合（オークションでセット出品するなど）、認証が回避される具体的ソフトウェアをこの者が認識することは当然可能であり、また、回避の認容を超えて推奨しているときとさえることができる。この者が、回避がほぼ確実に試みられることを認識、認容していることは明らかであろう。

したがって、認証回避手段の入手方法を教示した者は、不競法21条2項4号の従犯となる可能性はある。

（エ）不競法による対応の限界

インターネットを通じて認証回避手段を有償供与する行為が、不競法21条2項4号により処罰されるかをここまで検討し、行為者が正犯もしくは従犯となる可能性を述べたが、そこにいたる解釈にはいくつか困難な点があることも指摘した。すなわち、①認証回避手段が電磁的方法であるからといって、これをただちに「プログラム」として捉えることができるか、②

電気通信回路を通じて不正ユーザーに回避手段を入手させることを「提供」と捉えることができるかが、回避手段供与行為を不競法2条1項11号の「不正競争」と評価できるか否かを左右する。

このような限定的な解釈が、コンテンツ業界の要望に即しているとは思われない。本稿で対象とした認証回避手段は、決して専門的な知識を有した一部の者だけが知りうるものではなく、認証システムを組み込んだソフトウェアが有名であればあるほど、認証回避手段の存在が知れ渡ることになる。認証によりコンテンツを保護しようとする仕組み自体は今後増えていくであろうし、それに呼応して認証回避手段も開発されるだろう。しかし規制の必要性は、不競法の解釈を拡大することによって解消されるべき問題ではない。不競法がその基本原則として示すように、広範で曖昧な規制は本来保護すべきコンテンツ業界の技術開発をかえって萎縮させかねず、規制は必要最小限にとどめられなければならない。そこで、不競法の規制対象から漏れる行為に、既存の法令で対応する可能性についての関心はなお残るものと予想される。また、不競法21条7項は、1項および2項に該当して刑罰が適用される行為であっても、刑法その他の罰則を妨げないことを規定しており、認証回避手段供与行為の処罰が不競法により可能だとしても、さらに刑法上の犯罪の成否を確認する必要がある。そこで、本稿で対象とした認証回避手段の供与行為との関係で問題になると思われる刑法上の業務妨害罪等の成否について検討する。

4. 業務妨害罪

本稿で対象とする行為（以下、認証回避行為）が業務妨害罪との関係で問題となるのは、①hostsファイルの置き換え、②非正規の識別番号の入力、③ソフトウェアのプログラムの置き換えの一部又は全部によって、ソフトウェアメーカーの認証サーバーによる認証を不可能とする点である。

このような行為が業務妨害罪のうち、偽計業務妨害罪もしくは電子計算機損壊等業務妨害罪にあたる可能性はあるだろうか。業務妨害罪が成立する場合、行為の主体は個々の不正ユーザーであり、供与行為者は幫助犯となる（ただし、供与行為者を正犯とする余地があることについて後述する）。

（ア）偽計業務妨害罪

①「偽計」

偽計業務妨害罪における偽計は、詐欺罪における欺罔とは異なり、人に対する働きかけの要素を不要とするのが、判例および裁判例のこれまで一貫した傾向である。

機器や装置への働きかけの結果、その誤作動が問題となった事例としては、電力量計に細工をして使用料より少ない電力量を指示させた事例²²、パチンコ遊技機にとりつけられた電子計算機部分を不正に交換し、人為的に「大当たり」を発生させるなどした行為について刑法234条の2の電子計算機損壊等業務妨害罪にあたるとした第一審判決を破棄し、控訴審において追加された予備的訴因の偽計業務妨害罪の成立を認めた事例²³がある。

一方、機器や装置への働きかけの結果、その作動不能が問題となったケースとしては、タクシーの配電盤回転子を密かに取り外した事例²⁴、有線放送会社が、同業者の進出を阻止するため、同業者が放送送信に利用している電線を密かに切断して、顧客への放送を不能にした事例²⁵があるが、いずれも偽計にあたるとされている。さらに、最高裁も、「応答信号の送出を阻害する機能を有するマジックホンと称する電気機器を加入電話回線に取り付け使用」したという人への働きかけを含まない行為が、端的

22 福岡地判昭和61・3・3判タ595号95頁。

23 福岡高判平成12・9・21判時1731号131頁。電子計算機損壊等業務妨害罪が成立しない理由として、パチンコ遊技機にとりつけられた電子計算機部分が234条の2にいう「業務に使用する電子計算機」と認められないことを述べた。

24 大阪高判昭和32・9・27労刑集7輯75頁。

25 大阪高判昭和49・2・14刑月6巻2号118頁。

に「課金装置の作動を不能にした行為」にあたるとして、偽計性を認めている²⁶。

認証回避行為は、これらの事案と同様に、人を欺罔し、あるいは人の錯誤又は不知を利用する場面はなく、ソフトウェアメーカーのサーバーが行方客体となる。

しかし、いくつかの点で違いがある。第一に、偽計が認められた事例では、機器や装置に目に見える工作が加えられている点が挙げられる。具体的には、電力量計への細工（内部の電線の切断）、ロムの取り付け、配電盤回転子の取り外し、電線の切断、電気機器の取り付けである。一方、認証回避行為は、電磁的記録の書き換えや置き換えといった、人の知覚によつては認識できない方法で行われる。

第二に、認証回避行為は、認証サーバーとの関係では作動不能のパターンにあたるが、認証サーバーによる認証は、ソフトウェアの不正なコピーや使用を防止することが目的であり、ソフトウェアメーカーの中核的な業務とは必ずしもいえない点である。これは、スーパーにおいて万引きが多発するために、警備員を雇って巡回させる行為に類似する。確かに万引きを防止することによりスーパーが損失を被る機会は減少するが、そのスーパーにとって万引きの防止が営業の本質的な部分を構成しているとは思われない。これまで偽計が認められた事例では、偽計がなければ正常に作動した機械により行われていた業務は、課金や放送といった、被害者にとって中核的な業務であった。

したがって、認証回避行為が偽計であると認めることは、目に見える工作ではない電磁的記録の書き換えと、中核的な業務を担わない機械の作動不能を含む点で、偽計概念を拡大することになる。後者の点は「業務」との関連で項をあらため、さらに検討する。

26 最決昭和59・4・27刑集38巻6号2584頁。刑法判例百選Ⅱ（第四版）48頁〔山口〕。

ところで、認証回避行為を、①hostsファイルの置き換え、②非正規の識別番号の入力、③ソフトウェアのプログラムの置き換えの全てを含む一連の行為として捉えた場合には、認証回避行為は認証サーバーの作動不能を引き起こす行為であるが、特定の状況下における部分的な行為を取り上げた場合には別の構成も可能である。認証回避を目論んでいる者が、認証を要するソフトウェアをソフトウェアメーカーのHPからダウンロードすることにより入手する場合を考えてみよう²⁷。ここで働きが問題となるのは認証サーバーではなく、ダウンロードサーバーであり、両者は別個独立して存在することが多い。このいわば将来の不正ユーザーは、まず自己のコンピュータのhostsファイルを書き換えて認証サーバーへのアクセスを不可能としてから²⁸、ソフトウェアメーカーのダウンロードサイトにアクセスする。しかし、この時点ではダウンロードサーバーは、書き換えられたhostsファイルを有するコンピュータからのアクセスであることを判別することができない。そのために、その後の認証が不可能となるようなコンピュータに対して、ソフトウェアのダウンロードを開始してしまうのである。

このように構成した場合は、認証回避行為を認証サーバーの作動不能を招く一連の行為として捉えた先の構成による問題点の一つは解消される。すなわち、ソフトウェアメーカーにとって、ソフトウェアの配布はそれなくしては営業が成立しないまさに中核的な業務であり、対価を徴収するタイミングとも合致する。したがって、これを担うダウンロードサーバーの誤作動を招く行為が業務妨害となることは明らかであろう。ただし、認証が不可能であるコンピュータであると知っていたらダウンロードを許可し

27 製品版を購入せずに、無料の体験版や試用版を入手して、これを不正に製品版として起動させ（その際に非正規の識別番号を使用する）、そのことが認証サーバーに感知されなければ、無償でソフトウェアの機能を利用することができる。

28 自己のコンピュータのファイルを変更すること自体は何ら違法行為とはならない可能性が高い。

なかったはずのソフトウェアを、それを感知することが技術的に不可能であった（この“不備”はソフトウェアメーカー側の問題であり、ユーザーの行為によるものではない）ためにダウンロードしてしまうことを、コンピュータに本来期待された動作²⁹とは異なる動作を生じさせたという意味での誤作動と言えるのかについては、更に検討が必要である。

②「業務を妨害」

判例および裁判例は業務妨害罪を危険犯として捉えており³⁰、現金自動預払機利用客のカードの暗証番号等を盗撮するためのビデオカメラを設置した現金自動預払機の隣にある現金自動預払機を、一般の利用客を装い相当時間にわたって占拠し続けた事例で、被告人らの行為は「偽計を用いて銀行が同現金自動預払機を客の利用に供して入出金や振込等をさせる業務を妨害するもの」であるとして、実際に外形的混乱・支障が生じたことではなく、その危険性を理由に偽計業務妨害罪の成立を認めた³¹。また、マジックホンについて、たとえ同機器を取り付けた者がただ1回通話を試みただけでこれを取り外した等の事情があったとしても、業務妨害罪の成立は妨げられないとした事例³²があり、やはり実際の外形的混乱・支障ではなく、業務が妨害される危険性を重視したといえる。こうした見解をとる場合には、認証回避行為についても、個別の不正使用という外形的妨害よりも、業務が妨害される危険性がいかに継続して発生したかが重要となる。

これに対し、偽計概念の拡張に伴い、業務妨害概念が、業務妨害罪が成立する要件としての重要性を高めてきたことに鑑み、業務妨害罪を侵害犯と解する見解も学説上は有力である。そのような見解は、実際に業務が妨

29 電子計算機にとって「正しい」「誤り」という表現は不正確であり、このような動作を「判断の誤り」と呼ぶことが適当かは検討すべきである。

30 大判昭和11・5・7刑集15巻573頁。

31 最決平成19・7・2刑集61巻5号379頁。

32 最決昭和61・6・24刑集40巻4号292頁。

害され、業務遂行に支障が生じたこと、すなわち業務の外形的妨害を求め³³、マジックホンに関する上述の最高裁昭和59年決定が「課金装置の作動を不能にした行為」を捉えることで、業務の外形的妨害を認めたものと解する³⁴。また、「単に個別的な業務における判断の誤りを生ぜしめたにすぎない場合は除外される」として、替え玉受験やカンニングは業務妨害ではないとする見解もある³⁵。偽計概念の拡張により不明確となった処罰範囲を限定しうるのは業務概念であるから、これを徒に広く解釈することは妥当ではなく、業務妨害罪は侵害犯として解されるべきであろう。

「偽計」の検討で示したように、認証回避行為を業務妨害として捉える場合には、二つの構成が考えられる。一つは認証サーバーの作動不能であり、もう一つはダウンロードサーバーの誤作動である。

認証サーバーの作動不能を対象とした場合、そこで妨害されるもしくは妨害の危険が生じる業務とは、ソフトウェアが不正にコピーされたものではないことや、使用規約に反する使用でないことの確認と、不正であると判断したならば、ソフトウェアの起動や使用を不可能とする信号の送信である³⁶。

まず、認証回避を行う個々の不正ユーザーが、この確認と送信という業務を妨害していると解することができるかを検討しよう。不正ユーザーが認証回避を行うことにより、認証サーバーはこのユーザーの存在自体を感知せず、認証の機会を有しない。すると、表現は不適切かもしれないが、認証サーバーは「やるべき仕事をやらずに済んだ」ことになり、業務遂行に混乱や支障をきたしたとはいえない³⁷。

33 米澤慶治編『刑法等一部改正法の解説』98頁。

34 前掲・注27、山口48頁。

35 西田典之『刑法各論』〔第5版〕（成文堂、2010）128頁。

36 不競法で検知→可能方式と呼ばれる機能。

37 極端に考えれば、本来当該ユーザーの認証に割いていたはずの時間を他のことに使えたのであるから、業務遂行をスムーズにしたとさえ言える。

例えば、改札を密かに乗り越えるなどして、切符を持たずに全席指定の電車に乗り込んだXを考えてみよう。やがて車掌が、乗越し乗車や不正乗車に対応するために、乗客一人一人の切符を確認にやって来る。すなわち検札（車内改札）である。Xは検札をやり過ごすために、車両間に設置されたトイレに隠れた。このトイレに隠れる行為は、鉄道会社に対する偽計業務妨害にあたるだろうか。Xの無断乗車は改札を通っていないために二項詐欺³⁸とはならず、刑法上は不可罰の利益窃盗である（ただし、鉄道営業法29条違反にはなる）。Xが自己の利益窃盗が露見しないよう検札を逃れることが、同じ被害者に新たな法益侵害をもたらすものとして別途に業務妨害罪にあたるとすることは、利益窃盗を不可罰とする法の趣旨に反するもので不合理ある。

これは、認証がソフトウェアメーカーにとって中核的な業務であるか否かという、前述の問題にも関連する。無賃乗車Xのケースに例えるならば、認証は改札ではなく検札にすぎないのである。

次に、ダウンロードサーバーの誤作動として認証回避行為を検討してみよう。不正ユーザーによる個々のダウンロードは、個別のダウンロードにおける判断の誤りにすぎないため、業務妨害からは除外すべきである³⁹。また、認証が不可能なコンピュータであると分かっているならば、ソフトウェアメーカーは、ソフトウェアのダウンロードを許可しないはずであり、それにも関わらず、そのようなコンピュータであることを秘してソフトウェア

38 乗車駅および降車駅付近の短区間の乗車券を所持し、乗車駅改札係員に乗車駅付近の区間の乗車券を呈示して鉄道職員をして降車駅まで輸送の役務を提供させたいいわゆる「キセル乗車」の行為について詐欺利得罪の成立を認めた事例として、大阪高判昭和44・8・7判時572号96頁がある。また、入場券による入場を手段とする無賃乗車においては、改札係員あるいは列車乗務員の財産的処分行為がないので詐欺利得罪は成立しないとした事例として、広島高判昭和51・12・6判時851号241頁がある。

39 ダウンロードの途中で認証を挟み、認証を経なければダウンロードが完成しないという仕組みであったならば、これとは異なる結論を導きえたものと思われる。

を入手している点に注目したならば、業務妨害罪ではなく、まずは電子計算機使用詐欺罪（刑法246条の2）の成否が検討されるべきであるため、この点は後に検討する。

③ 認証回避手段を供与する行為

業務妨害罪に関しては、不正ユーザーを直接の行為者としてここまでの検討を進めてきた。そして、業務妨害罪の成立には、業務遂行に外形的な混乱や支障が生じたという結果が必要であると解し、さらに偽計概念や業務概念を限定的に解した場合、個々の不正ユーザーの行為が偽計業務妨害罪の構成要件に該当すると考えることは困難であるとの結論に達した。

では、判例のように、業務妨害罪を危険犯と解した上で業務概念を拡張した場合に、結論は異なるであろうか。認証の目的はソフトウェアの不正なコピーや使用を防止することである。実態に即して考えれば、対価徴収の確保のために不正行為防止の対策をとることは、コンテンツ業界にとっては、コンテンツの販売と一体のものとして考えられるほどに必要不可欠で、継続的になされる活動である。認証を当然に予定し、それを使用規約にも盛り込んだ上でソフトウェアを販売するメーカーは、ソフトウェアが不正使用されないことを確保し、公平かつ適正な販売をするという業務を、その営業活動として行っているとも言える。

そこで、認証とは、ソフトウェアメーカーの公平かつ適正な販売をするという業務の一貫であると考えたならば、不正なダウンロードが行われる手段と機会を広範かつ継続的に供与する回避手段供与者がいた場合、この供与者こそが当該業務を現に妨害し、また、妨害する危険のある行為を、自ら行ってきた正犯であると評価する可能性が生じる。

すなわち、ソフトウェアメーカーの、公平かつ適正な販売という業務を、認証回避手段供与者は、不正ユーザーを生み出すことで現に妨害している。また、本来は非常に高額なソフトウェアを無料かつ無制限で使用することを可能とするような認証回避手段の供与が、著しく低額な料金

で、しかもインターネットオークション等の不特定多数の者が目にする場において行われ、かつ継続されている場合には、将来にわたって大量の不正ユーザーを生み出す危険性がある。認証回避手段を取得した者は、高い確率でソフトウェアの不正使用を行うと思われるという点で因果関係も認められるであろうから、認証回避手段の供与者が生ぜしめた業務妨害の危険性は具体的かつ高いものであり、その危険性が継続していると考えられる。

なお、たとえ正犯性が認められなくとも、少なくとも幫助犯にはあたりうる。業務妨害罪の成否にあたって業務の外形的妨害を重視する見解によれば、個別のユーザーの認証回避行為が業務妨害にあたるかにつき問題が生じることは上述の通りであるが、判例・通説の立場に従えば、ダウンロードサーバーによる判別を不可能にした点、すなわち「個別的な業務における判断の誤りを生ぜしめた」場面を捉えて業務妨害を認めることも十分にありうる⁴⁰。その場合には、マジックホンに関する上述の最高裁昭和59年決定と同様に、不正ユーザーを偽計業務妨害罪の正犯とし、個別的な妨害を行った正犯の行為を容易にしたことを捉えて、認証回避手段の供与者を幫助犯とすることになるであろう。

④ソフトウェアの不正使用と業務妨害

しかし、判例および裁判例の解釈は妥当ではない。

ある業務が事業主にとって中核的か否かの判断を捨象したならば、およそ事業にとって不要な業務は存在しないのであるから、ある単独の業務を妨げることは、事業に何らかの影響を及ぼすことになる。「単に個別的な業務における判断の誤りを生ぜしめたにすぎない場合」を広く業務妨害に含めるという理解は、個別の業務と事業全体の関連性を意識することで生

40 まさに判断を誤らせたことをもって業務妨害を認めたとも解しうるものとして、電気料金計算徴収業務妨害罪の成立を認めた判決（福岡地判昭和61・3・3、同昭和61・3・24判タ595号95頁）がある。前掲・注27、山口49頁。

じたものと思われ、有機的・組織的で複雑な企業活動の有り様を反映している点は評価しうる。ところが、これを業務妨害罪の成否にそのまま持ち込んだ場合には、処罰範囲の不当な拡大を招く危険がある。

この点は、保護法益の解釈とも関係する。不競法2条1項11号は、守られるべき利益に「単に経済的・金銭的な意味での利益だけでなく、コンテンツ及びそのコンテンツを提供するサービスへの「信用」といった無形の利益を含めた事業上の利益を確保することを目的」としている⁴¹。こうした包括的利益を業務妨害罪の保護法益に含めることで、認証という個別の事業の位置づけは高いものとなる。また、業務の継続性が容易に認められることとなる。

しかし、業務妨害罪は、市民や企業の財産的利益を保護するために、財産危険犯として、あるいは、財産犯の補充的作用を果たしてきたという歴史をもつ。また、治安や通信のような公益性の高い社会制度の機能を維持するという社会的利益の保護のために利用されてきたということも踏まえると、業務妨害罪はいわば「融通のきく犯罪類型」であるといえる⁴²。しかし、罪刑法定主義の原則に反する運用は許されるものではなく、業務妨害罪は限定的に解釈されなければならない。そのためには、業務妨害罪の法益や構成要件を明確にするとともに、これを侵害犯として解することがやはり必要であると思われる。しかし、判例および裁判例は、侵害結果を不要とした上で、偽計概念や業務概念を拡大することで、業務妨害罪の処罰範囲の不明瞭さをさらに増幅させてきた⁴³。

たとえば、前掲のパチンコ遊技機にとりつけられた電子計算機部分を不正に交換した事例では、設定を超えた高確率でパチンコ台に大当たりを発

41 前掲・注5、逐条解説80頁。

42 京藤哲久「業務妨害罪」芝原邦爾ほか編『刑法理論の現代的展開 各論』（日本評論社、1996）117頁以下、120-121頁。

43 前掲・注42、京藤121頁。

生させること自体を業務妨害とせず、「ロムやフラットハーネスの取り替えにより、これらのパチンコ遊技台を営業の用に供することが相当期間不可能になり、それにより各パチンコ店の営業が一部妨げられたこと」をもって業務妨害罪の成立が認められた。さらに、犯罪の虚偽予告をして警察職員を出動させた行為について、「妨害された警察の公務（業務）は、強制力を付与された権力的なものを含めて、その全体が、本罪による保護の対象になると解する」として業務を全体的に捉えることで業務概念を拡大した上で、「虚偽通報さえなければ遂行されたはずの本来の警察の公務（業務）が妨害される（遂行が困難ならしめられる）」とし、業務妨害罪の成立が認められている⁴⁴。捜査機関等に虚偽の通報をした事例としては、他に、海上保安部に虚偽の犯罪事実を通報し、巡視船艇又は航空機等の出動を指示させ、各種指令、連絡等を行わせ、職員を出動せしめて搜索等を行わせた行為に対し、「通報さえ存しなければ遂行されたはずの本来の行政事務、パトロール業務、出動待機業務等の業務の遂行を困難ならしめ」として偽計業務妨害罪が認められたものがある⁴⁵。

業務妨害罪のこのような解釈に対しては、処罰範囲の不当な拡大であるとして批判が向けられている。他者の意図的行為により本来行うべき仕事が増えたことを「妨害」というのであれば、企業組織などにおいて、同僚の意図的懈怠により相対的に自らの仕事が増えた者は、その同僚を業務妨害罪で訴えうるとの批判⁴⁶は重要である。不正使用を防止するための認証を回避する行為が業務妨害であると評価した場合には、同様の批判が当てはまるだろう。

44 東京高判平成21・3・12高刑集62巻1号21頁。

45 横浜地判平成14・9・5判タ1140号280頁。

46 野澤充「犯罪の虚偽予告がなければ遂行されたはずの警察の公務」成瀬幸典ほか編『判例ブラクティス刑法Ⅱ 各論』（信山社、2012）132頁。また、生田勝義「警察への虚構犯罪通報は偽計業務妨害か？」立命館法学337号（2011）1201頁参照。

また、個別のユーザーの認証回避行為を業務妨害とすることは、不可罰の利益窃盗にすぎないソフトウェアの不正使用を、業務の自由が侵害されたことを理由に容易に処罰することになる。このような処罰を許せば、企業にとって望ましくない行為を直接処罰する規定がない場合に、業務妨害罪として処罰することが可能となりかねない。それが不合理であることは、企業に損害を与える財産犯に対して、同時に業務妨害罪が成立しないこととのバランスからしても⁴⁷⁾、明らかであろう。

(イ) 電子計算機損壊等業務妨害罪（刑法234条の2）、電子計算機使用詐欺罪（刑法246条の2）

認証回避行為は、電子計算機損壊等業務妨害罪にあたるか。

コンピュータは電子計算機であるが、自己のコンピュータは「人の業務に使用する電子計算機」ではない。また、虚偽の情報若しくは不正な指令を与えられた電子計算機（不正ユーザーのコンピュータ）と、それによって使用目的に沿うべき動作ができない、又は使用目的に反する動作をさせられる電子計算機（認証サーバーもしくはダウンロードサーバー）は同一、もしくはネットワーク化されるなどして同じシステムとして作動していなくてはならないため、「人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え」「電子計算機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」という構成要件を満たさない。また、ソフトウェア自体は電子計算機とはいえない。

そこで、認証回避行為が「虚偽の情報若しくは不当な指令を与え」にあたらない場合に、なお「その他の方法」に含まれるかが問題となるが、この方法が動作阻害を直接に惹起することが必要である。しかし、認証

47 財産犯と業務妨害罪は排他的関係にはなく、たとえば窃盗罪が成立する場合には、業務妨害罪が背後に隠れているにすぎないのではないかという疑問がありうるとの指摘がある。山口厚『刑法各論』（有斐閣、2003）166頁・注11）。

サーバーの作動不能を結果とした場合には⁴⁸、不正ユーザーのコンピュータが認証サーバーにアクセスすることがない点で直接性の要件を満たさない⁴⁹。他方、ダウンロードサーバーの誤作動を結果とした場合には、サーバーにアクセスするという接触はあるが、認証が不可能なコンピュータであるかを判断する機能をサーバーが有しているわけではないため、単にそれを明らかにしない不作為を「虚偽の情報若しくは不正な指令を与え」と言うことはできない。したがって、認証回避行為は電子計算機損壊等業務妨害罪にはあたらない。

同様の理由により、認証サーバーとの関係では、認証回避行為は、電子計算機使用詐欺罪の「人の事務処理に使用する電子計算機に虚偽の情報若しくは不正の指令を与えて」という構成要件に該当しない。他方、ダウンロードサーバーにアクセスし、本来は高額な対価を払わなければ使用が不可能である機能を、対価を払わずに使用するつもりであることを秘して、無償もしくは低額でソフトウェアをダウンロードする場合には、ソフトウェアの使用というサービスを客体として「財産上不法の利益を得た」という結果は満たし、オンライン決済の金額が本来支払うべき金額と異なるという点で「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」と言えるが、ダウンロードするコンピュータが今後の認証を受けることが出来るか否かをユーザーがダウンロードサーバーに送信する手順は組み込まれていないのであるから⁵⁰、「虚偽の情報若しくは不正の指令を与えて」

48 電子計算機損壊等業務妨害罪は、動作阻害という結果が発生しなければ成立しない。山口厚『刑法〔第2版〕』（有斐閣、2011）276頁。

49 ホームページ内の天気予報画像とわいせつ画像の置き換えに電子計算機損壊等業務妨害罪が認められた事例では、被告人はサーバーコンピュータに直接アクセスすることにより、そのハードディスク内に記憶・蔵置されていたデータの削除と、新たなデータの記憶・蔵置を行っていた。大阪地判平成9・10・3判タ980号285頁。

50 たとえばダウンロード開始の時点で、「あなたのコンピュータはhostsファイルを書き換える等により、弊社の認証を回避する可能性のある状態になっていま

という要件を満たさないものとする。したがって、認証回避行為は電子計算機使用詐欺罪にはあたらない。

5. おわりに

ソフトウェアの認証回避手段の供与行為に対しては、刑罰を含む実効的な規制が必要とされてきたが、インターネットを介する点や、コンピュータのファイルやソフトウェアのプログラムの書き換えといった、一つ一つの行為は刑罰の対象とならない行為の組み合わせによって回避が行われる点で、現行法の枠内ではいまだ限界事例にとどまらざるをえない。認証回避行為によってソフトウェアメーカーに甚大な被害が数年に渡って生じている実態は看過できるものではないが⁵¹⁾、一方で認証回避行為を処罰した場合に、処罰範囲が無限定となり、ソフトウェア業界を不必要に萎縮させることや、日常的なトラブルに過ぎない行為が業務妨害罪として処罰されることも問題である。

本稿で見てきたように、インターネットを介した認証回避手段の有償供与に検討の対象を限定した場合であっても、多様な形態に対し、それぞれの行為のどこをどう切り取るかによって規制の対象となるか否かが左右される。そこで、認証回避手段供与行為の規制を検討する際には、行為態様を細かく分析することが前提として必要である。改正後に不競法21条2項4号が適用されたものとして、ゲーム機の改造代行とマジコンの販売があ

せんか」のチェックボックスが表れ、これに「いいえ」という答えを送信した場合にのみダウンロードが完了するような手順はない。使用規約に対する同意・不同意のチェックは、規約を全て読まずに「同意」を選択できる場合がほとんどであるため、実際上このような機能を果たしていない。

- 51) 複製が可能で、使用しても減ることのないという特製を有するデジタルコンテンツについて、その特製に反するような使用回数・複製回数制限を課すことが、コンテンツ業界の成長にとって不可欠であるのか、また顧客のニーズに答えているのかを考える必要はあるだろう。

る。この二件はいずれも装置が対象である。また、デジタル放送を視聴するためにテレビ等に挿入する「B-CASカード」について、有料放送を無料で見られるように不正にデータを書き換えたカードを、インターネットオークションを介して販売した者が逮捕された。データの書き換えに関する情報を公開した者も捜査の対象とされ、購入者については電磁的記録不正作出・同供用罪での立件が検討されているとのことである⁵²。また、カードのデータを自宅パソコンで改変し、自宅の衛星放送受信チューナー内蔵レコーダーに挿入した者が、電磁的記録不正作出および同供用罪で逮捕されている。一方、データを改変し、改変プログラムを自宅からファイル供用ソフトを使って不特定多数に提供した者が、不競法違反で逮捕されている⁵³。

本稿に関係すると思われるものとしては、DVD複製防止のコピーガードを解除するソフト（いわゆるリッピングソフト）を書籍の付録として販売した会社の取締役および社員が逮捕された事件がある⁵⁴。さらに、インターネットオークションを通じ、ソフトウェア体験版を複製したDVD-Rを販売したことに対して、著作権法違反（海賊版頒布）での逮捕者が出ている。海賊版と併せて不正なインストール方法を記載した「不正マニュアル」をセットで販売したとのことである⁵⁵。本稿で対象としたケースとの違いは、提供の細かな態様にすぎず、今後は、インターネットを介したプログラム単体や、プログラムではないが認証回避に不可欠の非正規な識別番号の供与行為がどこまで処罰されるのかが注目される。それによって現行法がデジタルコンテンツを保護する射程と限界が明らかになり、次の改正

52 毎日新聞2012年6月19日。

53 毎日新聞2012年6月20日。被疑者は一時自己のホームページで改変方法を公開していたとのことであるが、この行為が起訴の対象となるかは不明である。

54 朝日新聞2012年7月17日。

55 コンピュータソフトウェア著作権協会2012年7月23日発表。http://www2.accsjp.or.jp/criminal/201224_1/1192.php（2012/08/15アクセス）。

を視野にいれて、さらなる検討が進むことが期待される。