認証回避型クラック・パッチ提供・利用の違法性

村　本　武　志

Ⅰ．問題の所在

ビジネス用プログラムのメーカーは、違法複製を防ぐために、さまざまな方策を講じる。アクセス・コントロールは、その一つであり、コンピュータ・システム上で、ユーザー（アクセス者）の属性に関する情報を事前に設定し、アクセス時にユーザー認証を行うことで、当該システムの利用を可能とする仕組である。これにより、インターネット上に流通する不正なコンテンツ利用手段、ゲームやビジネスプログラムなどのコンテンツ視聴・実行が制限される。

ライセンス認証システムは、アクセス・コントロールの一つであるかが問われる。これは、メーカーがユーザーに対し、シリアル・データ[1)]の入力後、インストール[2)]対象プログラムのソフトウェア、コンピュータ・ハードの情報の提供を求め、メーカーの既存ユーザー情報と照合することで、プログラムの違法複製を排除する仕組みである。この仕組みを回避・

無効化し、プログラムの実行を可能にするプログラム（クラック・パッチ、〝a crack〟）や、クラック情報（以下でクラック・プログラム、クラック情報を総称し「クラック・ツール」という。）の提供があとを絶たない。これらは、主にネットショップやネットオークションにより有償で提供され、コンテンツ事業者に深刻な被害をもたらしている。

従来、正規の記録媒体以外でゲームが制限されるアクセス・コントロール機能を回避し、ネット上にアップロードされた海賊版ゲームソフトを動作させる装置（「マジコン」等）の提供が問題とされてきた。これに対しては、不正競争防止法（以下「不競法」）の適用[3]がなされ、これに関する論考[4]も少なくない。ビジネス用プログラムについても、違法複製を助長するプログラムの提供が不競法の「技術的制限手段に対する不正競争」にあたるとする論考が散見され[5]、刑事事件化もなされつつある。[6,7] しかし、行政解釈は、ビジネス系プログラムを対象とするクラック・パッチ提供の不競法該当性には消極である。

本稿では、プログラムを実行するためにメーカーの認証を必要とするライセンス認証システム（以下「ライセンス認証システム」という。）の仕組みを概観し、これを無効化・回避するクラック・パッチの概要、これがライセンス認証システムを無効化・回避する仕組みと、提供行為の違法性につき不競法該当性を中心に検討する。

Ⅱ．ライセンス認証システム

1　概要

プログラムに付される「技術的保護・制限手段」は、無許可の違法複製を制限する「コピー・コントロール」と、プログラムの実行を制限する「アクセス・コントロール」に大別される[8]。

アクセス・コントロール[9]は、前掲のとおり、コンピュータ・システム

上で、ユーザー（アクセス者）の属性に関する情報を事前に設定し、アクセス時にユーザー認証を行うことで、当該システムの利用や実行を可能にする仕組である。これに対しコピー・コントロールは、コンテンツの無許可複製の防止手法である。コピープロテクトを無効にする技術の進歩は、この方法によるプログラムの違法複製防止を次第に困難にする。そこで、違法複製されたプログラムの利用を防止するために、使用機器の認証を必要とするアクセス・コントロールが用いられるようになってきた。

しかし、近年のアクセス・コントロール回避行為の横行や回避機器等の氾濫は、看過し得ない状況にある。これは、コンテンツ制作者への対価が確保されないという著作権者の利益が損なわれるだけでなく、コンテンツ提供事業者の公正な競争を阻害する。

ビジネス用プログラムでは、インターネットを介したメーカー認証を通じて、プログラム実行を可能化するライセンス認証システムの仕組みが取られるようになってきた。プログラム・メーカーの多くがこの仕組みを採用する。

前掲のとおり、この仕組みを回避・無効化するクラック・ツール提供の不競法上の「不正行為」該当性が問題とされるが、先決問題として、ライセンス認証システム自体が不競法上の「技術的制限手段」に当たるかが検討されなければならない。

2　プログラムのインストールと認証

ライセンス認証システムの仕組みは、メーカーによって多少の違いはあるが、概ね、次の手順によりプログラムの実行を可能にする。

まずユーザーは、プログラムをコンピュータにインストールするに際し、シリアルデータの入力が求められる。このデータは、メーカーが独自の法則により作成した数字や英文字で表示される識別記号である。一般のパッケージ製品では、パッケージ毎に付与される。同一シリアルデータを用い

て許諾された本数以上のプログラムを異なるコンピュータにインストールすると、メーカーはその後の認証を拒絶する。これにより、違法なプログラムの実行が物理的に制限されることになる。

ただ、ライセンスのタイプによっては、同一シリアルデータを入力しても、コンピュータ台数の制限なくインストールを可能とするものもある[10)]。

試用版は、製品評価のためにメーカーが無償で一般ユーザー提供する製品である。一定の使用制限期間が設けられるほか、プログラムを起動するたびに、コンピュータ画面上に、試用版であることや、起動日時点での残存使用期間が表示される。しかし、そのほかは、製品版であると試用版であると、その内容や機能は異ならない。

試用版をコンピュータにインストールする場合、シリアルデータの入力を求めるかどうかは、メーカーにより異なる。入力を必要とするメーカーは、試用版提供時に、試用版用のシリアルデータを提供する。これを入力せず、試用版の認証を受けない場合には、メーカーにより多少の違いはあるが、概ね次のような使用上の制限がなされる。インストール・プログラムの情報画面上に、認証が必要である旨の表示がなされるほか、インストール後の製品使用期間は、認証を経た場合よりも短く設定される。その間、プログラムを起動するたびにコンピュータ画面上でライセンス認証を求める警告がポップアップ画面等で表示される。定められた試用期間を経過すれば、その後は、作成したデータの閲覧のみが可能な状態となり、作成されたファイルの閲覧を除くほか、入力や編集作業等は一切できなくなる。

試用版から製品版への移行は、試用版上で製品を購入するか、別途、パッケージ版ないしオンライン版を購入することで可能となる。ユーザーが、製品版の取得により得られるシリアルデータを入力することで製品版として認証が得られる。これにより、使用期間や機能制限のないプログラムの実行が可能となる。製品版に移行する際に、新たに、製品版プログラ

ムのインストールは求められない。以後、プログラムの実行ごとに試用版であることや残存使用期間の表示はなされない。

3　ライセンス認証の仕組み

メーカーは一般に、プログラムをコンピュータにインストールしようとするユーザーに対し、シリアルデータの入力を求める。その後、ユーザー・コンピュータは、メーカーの認証サーバに、必要なデータ[11] を送付して認証を求める。ユーザー・コンピュータは、認証承認メッセージを受信しコンピュータに記録することで、プログラムの実行が可能となる。

シリアルデータの入力に始まるインストール作業の開始からプログラムの実行可能化に至るまでのプロセスは、インストール・プログラム中のサブプログラムである認証プログラムが自動的に処理し、ユーザーはプログラムが求めるとおりにボタン操作、入力を行えば足りる。

同一のシリアルデータを用いたインストール行為が、許諾された複製回数を超えた場合でも、それが同一コンピュータに対するものであれば、プログラムの実行は制限されない。しかし、異なるコンピュータへの複製回数を超えた場合には、メーカーは、ユーザーから認証申請を不適と判断する。これにより、プログラムの実行が制限される。

ユーザー・コンピュータがプログラムを実行できるのは、ユーザー側からの認証申請を受けたのちにメーカー認証サーバから送付されるメッセージ[12] をユーザー・コンピュータが検知することによる。

このようなユーザー・コンピュータ側での、一連のライセンス認証の作業は、インストール・プログラム中の認証に関わる認証プログラムにより処理される。同プログラムは、認証申請のためにインストール・プログラムのメーカー認証を得るに必要なデータを収集し、メーカー認証サーバによる照合データの作成と送信処理を行う。

Ⅲ. クラック・ツール

1 準則

ビジネス用プログラムのメーカーの多くは、ユーザーに製品の評価機会を与えるために、無償で試用版を提供する。前掲のとおり、試用版は、製品版とは異なり、使用期間を制限し、期間経過後は使用可能な機能を制限する。本稿では製品版の使用に制限を付する技術を、「技術的制限手段」というが、使用可能な期間が経過すれば、ユーザーは、プログラムの機能中の閲覧機能のみが使用できるなどがその例である。

経済産業省「電子商取引及び情報財取引等に関する準則」(2016 年 8 月)(以下「準則」)は、このような無償配布の試用版(準則では「制限版」と表現する。)に関し、それに施されるさまざまな技術的制限手段を無効化したり回避する行為あるいは当該制限を無効化したり回避するクラッキング制限を無効化したり回避する行為に用いる情報やプログラムであるクラック・パッチがプログラムの使用期間や機能を制限する技術が、不競法が定める「技術的制限手段」に該当するかについて検討するが、結論として、これについて消極的評価を行う。

2 クラック・ツールとその作用

(1) クラック・ツール

準則は、製品版(準則では「完全版」としている。)に比して何らかの制限がなされる試用版(一部機能が利用できない機能制限版、利用可能期間の制限がなされる体験版等)に対し、「上記制限のない完全版での使用を希望するユーザーに対して、制限解除の手段(体験版を完全版に変更するために必要なシリアルナンバー、体験版を完全版へ変更するパッチ等)を有償で提供するといった形態のビジネスが行われている。」旨の現状を指摘する。

準則は、メーカーにより提供される正規のシリアル・データや変更パッチ等によらず、試用版を製品版として使用できるようにするクラック・ツールの提供類型として、以下を挙げる。

①「制限解除に必要なシリアルデータを提供する場合」（シリアル・データ提供型）

②「制限解除に必要なシリアルデータを計算するキー・ジェネレーターを提供する場合」（キー・ジェネレーター提供型）

③「期間制限のある体験版に、疑似日時情報を与えることにより期間制限を解除する疑似情報発生プログラムを提供する場合」（疑似情報発生プログラム提供型）

④「制限版であることが記録されているレジストリ等のデータの改変情報を提供する場合」（設定データ変更型）

⑤「制限版か否かを判別する処理ルーチンを改変した疑似完全版を提供する場合」（疑似完全版提供型）

⑥「制限版か否かを判別する処理ルーチンを改変するクラック・パッチを提供する場合」（クラック・パッチ提供型）

⑦「制限版か否かを判別する処理ルーチンを改変するために必要なバイナリ変更情報を提供する場合」（バイナリ変更情報提供型）

(2)　各ツールの内容と作用

ア　不正シリアルデータ（①②）

(ア)不正シリアルデータ

シリアルデータは、製品版プログラムをコンピュータにインストールする際に入力が求められる識別データであり、製品版については、これが入力されなければ、そもそもプログラムのインストール作業が開始されない。

試用版をコンピュータにインストールするに際し、当該データの入力が求められるかどうかは、メーカーにより異なる。これは、製品認証のため

に当該データを用いるかどうかの違いである。この入力を不要とするメーカー製品は、製品のインストール後は、製品の起動の度に試用版である旨と残存使用期間を表示するに止まる。しかし、これを必要とする製品は、製品の起動の度に試用版シリアルデータの入力による認証を求める表示がなされる。製品認証を得ない限り、使用期間超過前に機能制限がなされる。

シリアルデータは、ユーザーがプログラムのライセンスを取得する場合に、製品ごとに、それぞれ別異の値で提供される。メーカーは、このようなシリアルデータの提供を、それが付された製品や、製品がインストールされたコンピュータと共にする場合以外は、認めない。しかし、準則が述べるとおり、ユーザーの取得チャネルは「権利者から有償で開示を受ける場合」以外に、「体験版の解析によりシリアルデータを自ら発見する場合、シリアルデータを提供している第三者のサイトから入手する場合等」などさまざまである。

「ユーザー情報から逐次シリアルデータを生成するソフトウェアの場合」については、「シリアルデータを生成するプログラム（以下「キー・ジェネレーター」という。）」がインターネット上で提供される。キー・ジェネレーターの入手方法として、体験版の解析により自ら作成する場合、第三者のサイトから入手する場合等がある。

上記①の「シリアルデータ」とは、不正に入手されたメーカーが製造した正規の製品版シリアルデータ、及び、②の「シリアルデータを計算するキー・ジェネレーター」により、メーカーの承認を得ず作出された製品版としての機能を持つシリアルデータの双方を含む。試用版シリアルデータは、メーカ―により無償で提供されることから、不正に入手したり、作出する必要はない。

準則はこれらシリアルデータを入手したユーザーは、「自己が有する制限版を起動する際に、当該シリアルデータを入力することにより、制限版を完全版として使用することが可能となる。」としている。

(イ)不正シリアルデータの機能

製品版のシリアルデータの機能は、大別して二つある。一つ目は、プログラムのコンピュータへのインストールを可能にする機能である。二つ目は、メーカーによる認証を取得させ、コンピュータにインストールされた製品を実行可能とする機能である。

前者については、当該シリアルデータが、メーカーが定めた法則に従って作出される限り、正規品であると偽造品であると、それを入力することでプログラムのコンピュータへのインストールを可能とする。

しかし、後者については、後掲のとおり、ライセンス認証システムの下では、許諾された台数を超えてプログラムをパソコンにインストールした場合、メーカーサーバは、認証を与えない。従って、たとえ正規のシリアルデータを不正に入手したところで、プログラムのインストール自体はできても、製品版としての使用はできない。メーカーによっては、プログラムを多数のコンピュータにインストールして用いることを許諾するライセンスを採用する。これは、多数のライセンス管理[13] を容易にするため、あるいはアプリケーション開発のために同一人が使用する場合の便宜[14]を図るためである。この場合、同一シリアルデータを用いたプログラムのインストール・コンピュータ台数は制限されない。不正なシリアルデータには、このような用途のものが多数利用される。

メーカー側は、さまざまな手法を用いて不正シリアルデータの使用に対し認証を与えないための対策を講じる。これにより、不正なシリアルデータを用いたとしても、ユーザーが、常にメーカ―からの認証を得られるわけではない。

イ　疑似情報発生プログラム提供型（③）

試用版は、製品をメーカーウェブサイトから無料でダウンロードすることができる。しかし、使用はインストール日から一定期間に限られ、それ

以降は、閲覧機能などわずかな機能の使用ができるに止まる。

上記③は、試用版の使用期限に関するデータを改変し、使用制限期間開始日を巻き戻すことで、試用版の使用期間制限を実質的に延長させるためのプログラム提供を指す。準則は、これを、「偽の日時データを正規の日時であるかのようにアプリケーション・ソフトウェアに付与することのできる疑似情報発生プログラム」としている。

ユーザーの入手方法に、「疑似情報発生プログラムを自ら作成する場合、疑似情報発生プログラムを提供している第三者のサイトから入手する場合」がある。これを用いることで、「使用期間に制限のある制限版に疑似情報発生プログラムを使用することによって使用期間の制限を解除することができ、期間経過後も使用することが可能となる。」。

準則（iii.72）は、この特色として、「他の態様と異なり、どのソフトウェアにも使用可能な汎用性の高い疑似情報発生プログラムを提供する行為であることが多く、このため、特定のソフトウェアを解析しているとはいえない場合が多い」とする。

このプログラムは、試用版の使用開始日を改変するにとどまる。改変日から定められた期間が経過すれば、再度の使用開始日の設定が必要となる。また、試用版使用中は、当該製品が試用版である旨の表示が消失するわけではない。

ウ　設定データ変更型（④）

準則によれば、設定データ変更型とは、プログラムのレジストリ[15]情報を試用版から製品版に変更することで、製品版の実行が可能とするものである。対象プログラムには何らの改変もなされない。これら情報は試用版の解析、ウェブサイトで入手が可能であるとされる。

エ　疑似完全版提供型（⑤）

準則は、「疑似完全版」について「制限版を解析し、制限版であるか否かを判定している処理ルーチンを無効化することにより、制限版を完全版と同等の機能を有する疑似完全版に改変し」たものをいうとし、その作成は、体験版の解析により行われるとする。これを入手したユーザーは、「当該疑似完全版をインストールするだけで、完全版と同等のソフトウェアを得ることが可能となる。」とされる。

しかし、「制限版であるか否かを判定している処理ルーチンを無効化」するメカニズムについては、準則は明らかにしていない。

オ　クラック・パッチ利用（⑥）

クラック・パッチとは、試用版を製品版に変更するためのデータを言い、一般には、試用版と製品版を比較することで得られる差分データで作成される。準則（iii. 73）は、これを「制限版であるか否かを判定している処理ルーチンの情報をもとに、制限版を制限のない形態に自動で変更する」プログラムとしている。ユーザーは、「このクラック・パッチを当てる（プログラムを実行する）ことにより、制限版を疑似完全版に改変し、完全版と同様に使用することが可能となる。」とする。

準則は、「この態様は、上記⑤疑似完全版提供型と異なり、疑似完全版を作成するのが、提供を受けたユーザーであるところに特色がある」とし、「クラック・パッチを実行するだけで行えることから、この場合も専門知識を有していないユーザーに対して行われるという特色がある。」としている。しかし準則は、クラック・パッチがどのような仕組みで「制限版であるか否かを判定している処理ルーチンの情報をもとに、制限版を制限のない形態に自動で変更する」のかについて説明はしていない。

カ　バイナリ変更情報提供型（⑦）

準則はこれを、「体験版を解析し、制限版であるか否かを判定している処理ルーチンに関するバイナリ情報（疑似完全版への変更情報を含む。）に改変する」ための情報で、「体験版の解析によりバイナリ変更情報を自ら発見する」ことにより得られるとする。「クラック・パッチ提供型」との違いは、提供される情報が「単なる解析情報にすぎず、クラック・パッチの実行という自動的に行われる改変ではなく、提供を受けたユーザーが、手動で変更することに特色があり、提供を受けたユーザーは、手動でプログラムを変更しなければならないことから、一定以上の知識を有するユーザーに限定されるという」点にあるとしている。

(3)　ライセンス認証システムの下での各クラック・ツールの意味

ア　不正シリアルデータの作用（①②）

準則は上記①は、「制限版における制限解除の条件が固定のシリアルデータの入力であるソフトウェアの場合」に関して問題となるとする。

前掲のとおり、ライセンス認証システム上、シリアルデータは、メーカーの認証を得るためのデータの一部を構成する。当該データの入力は、製品版プログラムのコンピュータへのインストール開始には必須であるが、その入力がなされれば自動的に当該プログラムの実行が可能となるというわけではない。前掲のとおり、インストールされたプログラムが実行可能となるためにはメーカー認証によりユーザー・コンピュータに送付・記録される認証承認メッセージが必要となる。製品版のシリアルデータを入力することで、製品版としての「認証」が得られ、使用期間や機能が制限されない製品使用が可能となる。製品版のシリアルデータを入力することのみで、試用版に付される「制限解除」がなされるわけではない。

すなわち、ライセンス認証システムを前提とする限り、不正シリアルデータは、「制限解除に必要な」ものというよりは、「制限のない製品版と

しての認証を得させるため」のものであるとの表現が正確である。

イ　擬似情報発生プログラム提供型（③）

擬似情報が必要となるのは、試用版プログラムがインストールされた場合に限られる。ライセンス認証システムの下では、この情報は、メーカーの製品認証に関わらない。また、ライセンス認証システムや、プログラム動作に関わる認証承認メッセージの作出に影響するものではない。試用版をダウンロードした場合でも、前掲①か②により取得した製品版の不正シリアルデータを入力し、メーカーサーバから製品版としての認証が得られればこのような擬似情報の必要はない。

ウ　設定データ変更型（④）

ライセンス認証システムの下では、試用版がインストールされた場合でも、その後に製品版のシリアルデータを入力し、メーカー認証サーバによる認証プロセスを経ることで、製品版の実行が可能となる。これは、認証承認メッセージがユーザー・コンピュータに記録される結果である。レジストリ情報が試用版のそれから製品版に改変されることのみで、製品版が実行可能化するわけではない。製品版の実行が可能となるためには、レジストリデータが制限版から製品版に変更されるだけではなく、認証承認メッセージがユーザー・コンピュータ内に記録されなければならない。

エ　疑似完全版提供型、クラック・パッチ利用型、バイナリ変更情報提供型

上記のとおりライセンス認証システムの下では、ユーザー・コンピュータで製品版を実行可能化するためには、認証承認メッセージがユーザー・パソコンに記録されなければならない。

準則は、クラック・パッチ利用型、バイナリ変更情報提供型のいずれに

ついても、プログラム処理ルーチンの変更をいうに止まる。しかし、ライセンス認証システムの下では、このような処理のみで試用版が製品版として使用が可能となることはない。また、ライセンス認証システムを前提とする限り、「当該疑似完全版をインストールすることで、完全版と同等のソフトウェアを得ることが可能となる」ことはない。この仕組みは、まさに、これに認証承認メッセージが記録され、それがインストールによりユーザーコンピュータに複製されることによる。

(3)　小括

ライセンス認証システムは、「製品がパソコンにインストールされることで生成される認証承認メッセージが、メーカーのライセンス認証サーバの処理で生成され、ユーザー・パソコンに送付されて記録されることでプログラムの動作が可能となる仕組み」を言う。大手ビジネス・プログラムメーカーのライセンス認証の基本的な仕組みは、概ね類似する。

これに対し、準則が挙げるクラック・ツールの仕組みや作用については、いずれもライセンス認証を意識し、その仕組みを前提とした説明がなされているわけではない。クラック・パッチ等での改変は、いずれもプログ処理ルーチンの変更をいうに止まり、それがライセンス認証システム中のどのようなファクターに影響するのかについての分析・検討はなされていない。

準則は、後掲のとおり、「試用版に施される技術的制限手段は、不競法上の規制対象に当たらないと結論づけるが、この判断は、ライセンス認証システムの存在を射程に入れたものではない。ライセンス認証システムは、試用版、製品版のいずれにも用いられる。そこで採用される技術的制限方法が、「特定の反応をする信号がプログラムとともに記録されていたり、プログラム自体が特定の変換を必要としたりするようなもの」か否かについては、準則の検討射程には入っていない。

以下では、まずクラック・ツールの提供や利用行為の一般的違法性を概観する。その上で、不競法が定める「技術的制限手段」について述べ、準則の挙げるクラック・ツール、とりわけクラック・パッチが、ライセンス認証システムの仕組みなり、それが作成するデータ等を、どのように改変するかを明らかにし、その提供行為が不競法上の不正競争に該当するかについて検討を進める。

3　クラック・ツールの提供・利用違法

準則は、上記クラック・ツールの提供や利用が、現行法で規制される根拠となり得るものとして、著作権法、不競法、不正アクセス禁止法、民法（不法行為法）を挙げる[16)]

以下では、著作権法及び不競法該当性についての準則の整理を概観する。

(1)　著作権法

提供される技術的保護手段の回避・無効化ツールにより、対象著作物の改変をもたらす場合、改変を伴わない場合がある。準則は、クラック・ツールとして挙げるもののうち、前掲の⑤から⑦までを前者、上記①から④までを後者に分類する。そして、前者の形態は、制限版に何らかの改変が施されることになることから著作権法上の権利侵害となるおそれがあるとする。

ア　ソフトウェアを改変する場合

(ア)著作者人格権侵害の成否

準則は、疑似完全版提供型のうち、提供者自らが制限版を疑似完全版に改変する場合、当該改変は著作者の意に反することは明らかであるとし、著作者人格権の一つである同一性保持権（20 条第 1 項）侵害の余地を認める。制限版を疑似完全版に改変することは、著作者が予定している機能

制限等を機能しなくするものにすぎず、バグを取り除くものでも、バージョン・アップを行うものでもないことになり、同一性保持権侵害に該当すると解釈されることになろう。

クラック・パッチ提供型、バイナリ変更情報提供型の場合、提供者は、自ら制限版を改変するわけではない。しかし、提供を受けたユーザーがクラック・パッチを使用したり、バイナリ変更情報をもとに試用版を疑似製品版に改変すれば、この改変は同一性保持権侵害を構成する。また、クラック・パッチの利用やバイナリ変更情報は上記同一性保持権侵害行為を容易にすることからユーザーの改変行為を惹起する行為に当たり、同一性保持権侵害惹起責任を負う余地があるとする。

（イ）著作権侵害について

準則はまず、疑似完全版提供型のうち、提供者自らが制限版を疑似完全版に改変する場合、翻案権（27 条）を侵害しないかが問題となるとする。このような行為は、いわばソフトウェア全体を制限版から完全版へ改変することから、創作性に変更がないとはいえないとして、翻案権侵害を構成する余地があるとする。また、疑似完全版を新たに複製する行為は、疑似完全版への改変行為が翻案権侵害を構成するか否かにかかわらず、著作権侵害を構成するとする。

次に準則は、疑似完全版への改変行為が翻案権侵害を構成するか否かにかかわらず、疑似完全版をサーバにアップロードする行為は、複製権（21 条）ないし原著作者の権利（28 条）を侵害するとする。また、当該サーバから第三者にダウンロードさせた場合には、更に公衆送信権（23 条 1 項）ないし原著作者の権利（28 条）を侵害する余地があるとする。

また、同一性保持権侵害の場合と同様に、クラック・パッチやバイナリ変更情報を提供することは、閲覧者による複製ないし翻案行為を惹起する行為となると考えられることから、およそ私的使用目的の複製ないし翻案行為があり得ない場合を除き、複製権侵害ないし翻案権侵害を惹起したこ

とに基づく責任を負う可能性があるとする。

イ　ソフトウェアを改変しない態様

他方で準則は、ソフトウェア＝プログラムに改変をもたらさないクラック・ツールについては、いずれも、著作権法上の問題は生じないとする。

まず疑似情報発生プログラムについてはあくまで虚偽の日時をソフトウェアに与えるにすぎず、当該ソフトウェアに特定の反応をする信号が記録されているわけではないとし、「技術的保護手段の回避を行うことをその機能とするプログラムの複製物」に当たらないとする。そしてレジストリ情報等の設定情報の変更については、これら情報等は単なるデータであって著作物とはいえず、著作権法上の問題は生じないとする。

ウ　ライセンス認証システムとの関係

ライセンス認証システムは、前掲のとおり、プログラムの実行可能化条件として、メーカーが送付する認証済メッセージの受信とユーザー・コンピュータへの記録を求める仕組みである。また、後掲のとおり、ライセンス認証システムに用いられるクラック・パッチは、ユーザー・コンピュータに送付され記録される認証済メッセージを、メーカー認証サーバを介さず自ら偽造し、ユーザー・コンピュータに記録させる機能を持つ。このような偽造された認証承認メッセージの作出と記録が、対象ソフトウェア＝プログラムの改変といえるかは疑問であり、準則の整理に従えば「ソフトウェアを改変しない態様」に当たり著作権侵害該当性は否定されそうである。しかしながら、この認証承認メッセージをプログラムの実行を可能化する信号と捉えれば、このメッセージを偽造してユーザーコンピュータに記録させるクラック・パッチの「技術的保護手段回避」プログラム性の有無と、その提供で利用行為の著作権法違反性が問題となる。

(2)　不競法による制限

不競法は、電磁的方法により、特定の反応をする信号をプログラムとともに記録媒体に記録等したり、特定の変換を必要とするように記録等することにより、プログラムの実行を制限する技術的制限手段を営業上用いる場合、これを無効化してプログラムの実行を可能化する装置・プログラムを譲渡等する行為を不正競争と扱う（2条1項10号・11号）。

準則は、「一般に、制限版における制限方法は、特定の反応をする信号がプログラムとともに記録されていたり、プログラム自体が特定の変換を必要としたりするようなものではなく、技術的制限手段に該当しない。したがって、当該行為は、いずれの態様においても、技術的制限手段に対する不正競争には該当しないと考えられる。」と結論づける。

ライセンス認証システムが採用される場合、そこで用いられる制限方法は、試用版であろうと製品版であろうと異ならない。前掲のとおり、準則が「制限版における制限方法」として説明する前提として、ライセンス認証システムが念頭に置かれてはいない。ライセンス認証システムが、不競法上の技術的制限手段に当たるか、クラック・ツールがその無効化プログラムに当たるかは、ライセンス認証システム全体の正確な理解を踏まえたものでなければならず、準則には更に検討が必要というべきである。

4　比較法[17)]

(1)　米国

米国は、デジタルミレニアム著作権法（Digital Milleniam Copyright Act of 1998）上で、保護対象の著作物へのアクセスを効果的にコントロールする技術的手段の回避につき規制する。回避手段の提供行為として、「技術、製品、サービス、装置、部品またはそれらの一部分を製造し、輸入し、公衆に提供し、供給し又はその他の取引」を挙げる。規制要件は、次のとおり。(a) 主として回避することを目的に設計され又は製造された

ものであること、(b) 回避する以外には、商業的に限られた目的又は用法しか有しないこと、及び、(c) 回避するために使用することを知っている者又はこれに協力する者によって提供されること。但し、政府の活動、リバース・エンジニアリング、暗号化研究、未成年者に関する例外、個人識別情報の保護、セキュリティ検査等については例外規定が設けられる。

また、同法は「何人も、本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避してはならない」として、ユーザーによる回避行為についても規制する。違反に対しては、民事賠償、差し止めのほか、刑事罰も課される。

不正なプロダクトキー等情報の販売については、Anti-Counterfeiting Amendments Act でも規制される。これは、パスワード[18]、シリアル・データ[19]、ライセンスキー[20] などの情報の提供を規制する。

なお、判例には自社製品以外の使用を禁止するために用いられていたアクセス・コントロールについては著作物の保護とは無関係であるとの理由から、自社製品以外の使用を排除する目的によるプリンタのインクカートリッジや門扉のリモコンのアクセス・コントロールは規制の対象とならないと判断したものがある。

(2)　EU

EU は、情報社会指令（Copyright Directire）[21] で、「関係する者が、その目的のためであることを知り、又は知るべき合理的な理由を有しながら行う、いずれかの効果のある技術的手段の回避に対し、適切な法的保護を与える」と定め、回避行為を規制する。

回避手段の提供態様は、「製造、輸入、頒布、販売、貸与、販売若しくは貸与のための宣伝、又は装置、製品若しくは部品の商業目的の所持である。提供対象の回避装置等に当たるためには、次の要件を満たすことが必要である。(a) いずれかの効果がある技術的手段の回避の目的で宣伝され、

広告され又は市場化されるもの、(b) いずれかの効果がある技術的手段を回避する以外に商業的に重要な目的又は用途をもたないもの、(c) 主としていずれかの効果がある技術的手段を回避を可能にするか、又は容易にする目的で設計され、制作され、調整され又は使用されるものであること。

同指令は、米国著作権法と同様、回避装置等の提供のみならず。ユーザーの回避行為も禁止する。

同指令に基づき、域内諸国は国内法の制定が求められる。たとえばドイツ、フランスは、同司令に即して、著作権法において製造行為や回避サービスの提供などの回避手段の提供行為、ユーザーによる回避行為を禁止する。ドイツでは、司法及び公共の安全、障害者、学校放送、授業及び研究のための公衆提供等について例外規定が置かれる。

IV. 制限手段の保護

1 概要

現行法上、プログラムの実行を制限する手段について定めるものに著作権法（「技術的保護手段」）と不競法（「技術的制限手段」）がある。

このような制限手段の回避・無効化「手段」に関し、著作権法は、ユーザーによる「回避手段の利用」と、「回避装置・プログラムの提供」を規制する。これに対し、不競法は、無効化手段の「提供」のみを不正競争として規制する。いずれもその違反には、一定の要件の下で刑事罰が科される。不競法の刑事罰規制は、2011 年の改正法で定められたが、この立法理由は次のように被害拡大への対処の必要と説明される。

1997 年の不競法改正時点では、必要最小限の規制にとどめる観点から、経済活動に対する過度の萎縮効果を回避するため刑事罰導入は消極とされた。しかし、回避機器等の提供者に資産がなかったり、その捕捉が困難であるなどの理由で損害賠償請求や差止請求での対応は実効性に欠けること、

民事訴訟は個別の問題への対応に止まり一般的な違法行為抑止の効果がないこと、組織的な販売事案について、民事措置だけでは立証するに足りる証拠を収集することが事実上困難であったり、川上である輸入元を押さえることができないことなどの不備が指摘されていた。

政府の知的財産戦略本部は、2010 年 5 月に「知的財産権推進計画 2010」を出し、アクセス・コントロール回避規制の強化を図るべきとした。また、「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」は、報告書「技術的制限手段に係る不競法の見直しの方向性について」（2011 年 2 月 21 日）で、回避装置などによる被害の拡大を抑止するための、規制対象となる装置などの範囲の拡大や回避装置などの提供行為に対する刑事罰導入が指摘されていた。

2　制限手段の回避規制

(1)　著作権法

著作権法は、複製権は著作権者が専有すると旨を定めるが（21 条）、私的使用、すなわち個人的に又は家庭内その他これに準ずる限られた範囲内においての使用のための複製は、適用除外とする（30 条）。しかし、著作物の複製が「技術的保護手段回避」の態様で行われる場合、複製者が当該事実の認識したことを要件として、当該複製行為を著作権法違反とする。違反行為には、刑事罰が科される（120 条）。

ここで技術的保護手段とは、電磁手的方法により、著作権等を侵害する行為の防止又は抑止をする手段であり、かつ、著作物等の利用に際し、これに用いられる機器が特定の反応をする信号を著作物等とともに記録媒体に記録し、若しくは送信する方式又は当該機器が特定の変換を必要とするよう著作物等に記録し、若しくは送信する方式によるものをいう。

規制対象となるのは制限手段の「回避」である。ここで回避とは、当該制限手段に付された「信号の除去若しくは改変」、または「特定の変換を

必要とするよう変換された著作物等の復元」(2 条 1 項 20 号）により、当該技術的保護手段によって防止される行為を可能とし、又は当該技術的保護手段によって抑止される行為の結果に障害を生じないようにする行為をいう。

ライセンス認証システムが「技術的保護手段」に当たるとすれば、クラック・ツール使用者による保護手段回避行為は、上記の「私的使用目的の複製」という著作権制限に当たらず、違法評価が与えられることになる。

著作権法は、前掲のとおり技術的保護手段の回避を行うことをその機能とする装置・プログラムの利用を規制するだけでなく、当該装置・プログラムの公衆への譲渡・貸与、公衆への譲渡・貸与目的での製造・輸・所持、公衆の使用に供し、又は当該プログラムを公衆送信行為、送信可能化行為を規制する（120 条の 2 第 1 号)。

(2)　不競法

これに対し、不競法は、「制限手段の効果を妨げる」（無効化）装置・プログラムの提供を違法とするに止まり、ユーザーによる回避・無効化行為そのものは不正競争とはしていない。ユーザーの回避・無効化プログラムの使用に対し罰則を科しておらず、これは著作権法の適用領域となる。

プログラムの技術的制限手段について不競法は、次のような定めを置く。電磁的方法によりプログラムの実行・記録を制限する手段であり、かつ、視聴等機器が特定の反応をする信号をプログラムとともに記録媒体に記録し、若しくは送信する方式又は視聴等機器が特定の変換を必要とするようプログラムを変換して記録媒体に記録・送信する方式によるもの（2 条 7 項）と定義する。著作権法が、制限手段を「著作権等を侵害する行為の防止又は抑止をする手段」とする限定を置くのに対し、不競法には、そのような限定はない。

次に、同法が規制対象とするのは、プログラムの実行・記録等をさせな

いために営業上用いている技術的制限手段により制限されているプログラムの実行・記録を、当該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を記録した記録媒体・機器の提供である。不競法は、被譲渡者を限定しない場合（2 条 10 号）のほか、「契約の相手方や契約により特定された者」以外の者に限定する場合（同条 11 号）の双方について定める。

規制の目的や規制の対象行為について違いはあるものの、プログラムの実行を制限する手段として、著作権法上の「技術的保護手段」と不競法上の「技術的制限手段」の内容に差異はない。従って、以下では不競法上の技術的制限手段を取り上げ、ライセンス認証システムとの関係について検討する。

3　不競法上の技術的制限手段

(1)　類型

不競法は、技術的制限手段として「(a) コンテンツに信号又は指令を付し、当該信号又は指令に機器を一定のルールで対応させる形態」と「(b) コンテンツ自体を暗号化する形態」の 2 つの類型を置く。

イ　技術的制限手段に当たるための要件は、次のとおり。
(ア) プログラムの実行又は記録を制限する手段であること、
(イ) 当該制限が電磁的方法によりなされること、
(ウ) 以下のいずれかの方式に当たること
(a) プログラムの実行又は記録のために用いられる視聴覚機器が特定の反応をする信号を
α　プログラムとともに記録媒体に記録するか（信号・記録型）、若しくは
β　送信する方式（信号・送信型）、又は

(b) 視聴等機器が特定の変換を必要とするようプログラムを

γ　変換して記録媒体に記録し（変換・記録型)、若しくは

Δ　送信する方式（変換・送信型）

(2)　技術的制限手段の要件

ア　プログラムの実行等制限手段であること

技術的制限手段は、プログラムの実行または記録を制限するための手段でなければならない。

(ア)プログラム

「プログラム」とは、不競法上「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されたもの」と定義される（2条第8項)。

一般にプログラムは、文書作成等を行なうことができるように組み合わされたコンピュータに対する指令への指令であり、ライセンス認証システムが採用するプログラムが、不競法にいう「プログラム」に当たることに問題はない。

(イ)技術的制限手段であること

技術的制限手段は、それが、プログラムの実行または記録を制限する手段に当たるものでなければならない。

ライセンス認証システムは、前掲のとおり、ユーザー・コンピュータでのプログラムが実行可能となるための条件として、コンピュータの記憶装置内に、認証対象のプログラムとともにプログラム認証を可とする認証承認メッセージの記録を求める。それがコンピュータに記録され、認証プログラムにより検知されなければ、ユーザー・コンピュータでのプログラムの実行はなされない。具体的には、プログラムの実行がコンピュータへのインストールされた後の一定期間に制限され、その経過後は、データ閲覧など限られた機能のみの使用ができるに過ぎなくなる。従って、ライセン

ス認証システムは、プログラムの実行を制限する手段に当たると解される。

イ　電磁的方法によること

電磁的方法とは、「電子的方法、磁気的方法その他の人の知覚によって認識することができない方法」（2 条第 7 項）をいう。

ライセンス認証システムは、プログラムの実行のために、認証承認メッセージの記憶装置への記録を必要とする。これは、人の知覚によって認識することができない方法である。従って、本件ライセンス認証上のプログラムの実行の制限は、「電磁的方法」によるものといえる。

ウ　制限方式

技術的性制限手段の方法には、前掲のとおり変換・記録型、変換・送信型、信号・記録型、信号送信型があるが、ライセンス認証システムは、以下のとおり、そのうちの信号・記録型に当たるものと解される。

(3) ライセンス認証システムの技術的制限手段の方式

ア　信号・記録型

これは、プログラムを実行するために用いられる機器が特定の反応をする信号を、プログラムとともに、記録媒体に記録する方式である。

不競法上で「信号」の定義はない。一般には、色・音・光・形・電波など、言語に代わる一定の符号を使って隔たった二地点間で意思を伝達すること、又はそれに用いる符号をいう。技術的制限手段としての信号といえるためには、一定の情報であって、それが、伝達されることによりプログラムを実行する機器が特定の反応をし、これによりプログラムの処理が可能となるもので足りる。東京地判平 21・2・27（マジコン事件）は、信号を「一定の情報と DS カードから DS 本体に伝達し、DS 本体側において一定の処理を起こさせるもの」と判示し、原告主張の符号が「データ」

であって「信号」ではないとの被告主張を退ける。データであっても、上記のような機能を果たす符号であれば「信号」にあたるとするものであろう。

イ　プログラムを実行する機器が「特定の反応をする信号」

メーカーのライセンス認証において、上記の「信号」に相当するのは、認証承認のメッセージと解される。コンピュータにインストールされたプログラムの制限のない実行が可能となるには、メーカーの認証が必要となる。認証とは認証承認メッセージという符号の生成と記録に外ならない。この符号がコンピュータに記録されることで認証が完了し、制限のないプログラムの実行が可能となる。従って、認証承認メッセージは、「信号」に当たると解される。

ウ　信号が「記録媒体」に記録されること

「記録媒体」とは、プログラムがインストールされるコンピュータ（ないしその記憶装置）を指す。

認証承認メッセージはプログラムのインストール後に、認証サーバ上で生成されてコンピュータに送信されるか（「自動生成・送信方式」）、ユーザーがメーカーから取得した情報を入力することでコンピュータ上に生成されて（「手動生成方式」）、記録装置たるコンピュータに記録される。

自動生成・送信方式での認証承認メッセージがコンピュータに記録されるプロセスは次のとおり。プログラムのインストール→プログラムによるリクエストコードの生成と認証サーバへの送信→認証サーバによる認証承認メッセージの生成→ユーザー・コンピュータへの認証承認メッセージの送信→受信したコンピュータへの認証承認メッセージの記録。

次に手動生成方式での認証承認メッセージは、認証サーバによる自動生成によらない。プログラムをインストールしたコンピュータをインター

ネットに接続したにもかかわらず認証に失敗したり、インターネットの接続環境にない状況下でインストールを行なう場合には、ユーザーはマニュアルに従い、メーカーからの認証承認メッセージの取得が必要となる。この場合、ユーザーは電話やファックスを通じて認証承認メッセージの生成に必要な情報を取得し、これをコンピュータに入力することで、認証承認メッセージがコンピュータ上で生成・記録され、認証が完了する。

エ　信号が「プログラムとともに」記録媒体に記録されること

認証承認メッセージは、プログラム中の認証プログラムにより、コンピュータに記録され、これにより製品版プログラムのインストールが完了する。厳密には、認証承認メッセージがコンピュータに記録される時期は、プログラムのインストールと同時ではない。しかし、法文上は、信号が「プログラムとともに」記録媒体に記録されることを求めるに過ぎず、記録時期がプログラムと同時であることまで求めていない。従って、認証承認メッセージの記録がプログラムの記録と同時でないことは、認証承認メッセージの信号・記録型該当性を損なうことはない。

Ⅴ．認証回避手段の提供規制

1　不競法

(1)　概要

不競法は、事業者の利益の保護と公正な競争秩序の維持という観点から、アクセス・コントロールの回避機器等の譲渡等を「不正競争」として規制する。コンテンツ提供事業者は著作者等の権利保護による文化の発展、視聴方法等をコントロール可能にすることで、制作者から信用を得てコンテンツを販売するところ、アクセス・コントロール回避機器の流通は、その信用を失わせ、当該コンテンツ提供事業者は他の事業者との関係で著しく

不利な立場になることを踏まえたものである。

不競法は、プログラムを実行させないために営業上用いる技術的制限手段の実行の効果を妨げるプログラムの記録媒体の提供を不正競争と扱い、差止（同法３条）、及び損害賠償（同法４条）の民事上での請求を認める。また、2011 年改正法は、不正利益を得る目的があるか、営業上、技術的制限手段を用いる者に対する加害目的を要件として、刑事罰規制を導入したことは、前掲のとおり（21 条２項４号）。技術的制限手段回避・無効化機器・プログラム提供規制で保護される主体はコンテンツ提供事業者であり、保護対象物には限定がない。

(2)　不正競争

不正競争に当たるのは、アクセス・コントロールを回避する機器・プログラムの譲渡、引渡し、譲渡等目的の展示、輸出、輸入、送信する行為である。技術開発への悪影響への配慮から、「製造」は対象とされず、また、規制すべき実態がないとして、「回避サービスの提供」は含まれていない。更に、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「のみ」を有する装置、プログラムが規制対象とされ、汎用性のある機器やプログラムは含まれない。

なお、回避行為自体は、それが民法上の不法行為、著作権法で違法評価がなされる余地があることは格別、不競法上は規制されない。個々の回避行為は互い独立して行われ、その被害も限定的であり、また個々の回避行為を捕捉することは困難であることなどが、その理由とされる。

(3) 無効化装置・プログラムの機能

改正前の不競法は、技術的制限手段に対する不正競争行為に関して規制対象となる装置の範囲を、「技術的制限手段を回避する機能のみを有する装置」としていた。しかし 2011 年改正法は、この「のみ要件」を外し、

これに代えて、「当該装置又は当該プログラムが当該機能以外の機能を併せて有する場合にあっては、影像の視聴等を当該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。」との限定を加えている。

2　認証回避型クラック・パッチの特性

(1)　認証のプロセス

前掲のとおり、プログラムがコンピュータ上で、何らの制限なく実行が可能となるためには、ユーザー・コンピュータ内に、認証承認メッセージが記録される必要がある。そのために通常は、プログラムをコンピュータにインストールする際に、同プログラムの一部である認証プログラムが求めるライセンス認証システムの処理プロセスを経る必要がある。すなわち、メーカー認証サーバによるユーザーからの認証申請データデータと既存ユーザー登録情報との照合作業が必要である。

(2)　クラック・パッチの作用

メーカー認証サーバがユーザー・コンピュータに向けて発行しない限り、同コンピュータ内に認証承認メッセージが記録されることはない。認証回避型クラック・パッチは、このプロセスをショートカットし、ユーザー・コンピュータ内に認証承認メッセージを偽造し、それをコンピュータに記録させることで信号＝認証承認メッセージを偽装する。

認証プログラムは、検知対象認証承認メッセージがメーカーの定める法則に従い作成されたものであれば、それを検知することで、インストールされたプログラムを自動的に実行可能化する。認証プログラムは、認証承認メッセージがクラック・パッチにより生成されたものでも、それがメーカー仕様の法則に従い作成されたものであれば、これをメーカー認証サーバにより送付された正規のものと認識し、プログラムの実行を可能化する。

3　不競法違反

①　不競法の定め

不競法は、プログラム実行の技術的制限手段を回避するプログラムの提供を、不正競争に当たるとして禁止する（第２条第１項第11号）。

> 「十一 他人が特定の者以外の者に……プログラムの実行……をさせないために営業上用いている技術的制限手により制限されている……プログラムの実行……を当該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……プログラムを記録した記録媒体若しくは記憶した機器を当該特定の者以外の者に譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該機能を有するプログラムを電気通信回線を通じて提供する行為」

②　目的要件

技術的制限手段に対する不正競争行為への罰則規定の適用要件として、行為者は「不正の利益を得る目的」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」を有することが必要とされる。

まず「不正の利益を得る目的」とは、必ずしも自分が利益を得る目的に限られず、第三者に不当な利益を得させる目的も含まれる。これは、公序良俗又は信義則に反する形での不当な利益を図る目的のことをいい、自ら不正の利益を得る目的のみならず、第三者に不当な利益を得させる目的も含まれる[22)]。

次に、「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」における「損害」とは、財産的損害、信用その他の有形・無形な損害を加える目的をいい、現実の損害が生じることは不要である[23)]。

(3) 認証回避型クラック・パッチ提供行為の「不正競争」該当性

ア　ライセンスシステムの営業上の技術的制限手段性

上記のとおり、ライセンス認証システムは、認証承認メッセージがプログラムとともにコンピュータに記録されなければ、プログラムを制限なく実行することができない仕組みを持つものであり、技術的制限手段に当たる。そして、メーカーは、このシステムを、プログラムに営業上、採用している。

イ　認証回避型クラック・パッチの不正競争性

認証回避型クラック・パッチは、上述のとおり、当該技術的制限手段の効果を妨げることによりプログラムの実行を可能とする機能を有する。

プログラムが適法なものでなければ、インストール先のユーザー側コンピュータが、認証プログラムの動作によりメーカーにライセンス認証を求めても、メーカーサーバは、プログラムの制限のない実行を可能にする認証承認メッセージをユーザー・コンピュータに向けて発行しない。ユーザー・コンピュータは、これを受信し、記録できない結果として製品版プログラムの完全なインストールができず、制限のないプログラムの実行ができない。

認証回避型クラック・パッチは、プログラムの機能の一つである認証手続きを行うサブプログラムである認証プログラムの動作を制約しつつ、メーカー認証サーバへの認証申請データの送信、同サーバによる認証承認メッセージのユーザー・コンピュータへの送信を省略させ、自ら認証承認メッセージを生成しユーザー・コンピュータに記録させることでプログラムの制限のない実行を可能化する。

以上から、認証回避型クラック・パッチは、「技術的制限手段を回避するプログラム」に当たるというべきである。

5　他の認証回避手段との差異

認証回避型クラック・パッチの使用により得られる状態は、外見上は、

シリアルデータを適法に取得してメーカーから認証を得た状態に等しい。試用版での試用期間が経過していない状態とは異なる。すなわち、認証回避型クラック・パッチの使用により製品版としてのライセンス認証が得られ、アプリケーションプログラムを起動しても画面上には試用版の表示や残存試用期間の表示も一切なされない。試用期間経過後もデータ入力や編集機能が支障なく可能となる。

認証回避型クラック・パッチの使用により試用版がインスールされたにも拘わらず製品版としての認証が得られ、制限のない使用が可能となる理由は、認証回避型クラック・パッチが、メーカー認証サーバを介さず（ショートカットし）、自ら認証承認メッセージを権限なく自ら生成（偽造）し、コンピュータに記録（偽装）することによる。

この点、有効なシリアルデータを不正に入手して認証申請を行うことでメーカー認証サーバから適法に生成された認証承認メッセージの送信を受ける類型（「信号不正取得型」）では、メーカー認証サーバによる正規品審査プロセスの省略はない。

この点で、認証回避型クラック・パッチ利用型は適法な認証承認メッセージが不正に取得され、コンピュータに記録されることによりプログラムが実行可能化される「信号不正取得型」とは明らかに異なる。

VI. おわりに

本稿では、プログラムの実行制限手段として、プログラムとともに認証承認メッセージのコンピュータへの記録を求めるライセンス認証システムの仕組みが、不競法上の信号記録型技術的制限手段に当たること、認証承認メッセージを偽造しコンピュータに偽装する認証回避型クラック・パッチの提供が、技術的制限手段であるライセンス認証システムを回避し、プログラムの実行を可能化する手段の提供として不正競争行為に当たること

について、それぞれ検討した。

不正競争に当たるとするためには、認証回避型クラック・パッチの提供が求められる。このようなクラック・パッチは、広く閲覧可能なネット上のウェアハウスやストレージに広く散在しており、これらツールのストレージ情報や、ツールを用いたクラック方法の情報提供が跡を絶たない。わが国の不競法は、これら情報の製造・提供行為については、不正競争として規制しておらず、著作権法上の適用も期待できない。

わが国の不競法は、技術的制限手段の回避について、装置及びプログラムの提供に限る。これは 2009 年当時の当該規律が必要最小限の規律とすることとの配慮に基づく[24,25]。これら見解は、「技術的制限手段の回避サービスの提供行為及び回避装置等の製造行為に対する規制については、現行の規制範囲において一定程度の対応が可能であるとの判断から、独立して規制の対象とはしない」とする。

しかし、認証回避型クラック・パッチのみならず、クラック方法を教示する情報、不正なシリアルデータが広くネット上で提供され、これらを利用したプログラムの違法複製被害は看過しえない状況にある。このような認証回避を目的とするクラック情報は、「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」わせるのみならず、「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」こと、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」[26]。

シリアルデータ等の不正提供に対しては、本年に至り、商標法違反で強制捜査がなされた[27]。しかし、シリアルデータが、クラック・パッチとと

もに提供されなければ、商標法の適用も期待できない。技術的制限手段回避サービスや情報の提供に対し、米国やEUにおけるような著作権法、あるいは不競法による規制を検討すべき時期に来ているのではないか。

以上

註

1) プログラムをコンピュータにインストールするに際し、入力が求められるデータ。呼称は、メーカーによって異なり、シリアルデータ、シリアルキー、プロダクトキーなどさまざまである。

2) プログラムをコンピュータに導入する作業をいう。プログラムやデータなどのファイルをコンピュータのハードディスクなどに複製（コピー）するとともに、当該プログラムを使用するために必要な設定作業を含む。インストーラとは、インストール作業を自動的に行うためのプログラムで、それを起動し、使用する機能の選択やインストール先のハードディスクなどを対話形式で指示することで、自動的にインストールが行われる（IT用語辞典e-word）。

3) 携帯用機器でのゲームカード利用に特定の信号受信を必要とする場合、それを無効化するプログラム格納機器の提供が不競法上の不正競争に当たるかが問題とされた事案で、当該プログラムが格納装置の輸入・販売等が不競法2条1項10号に当たるとし、同法3条1項、2項に基づき装置の輸入、販売の差止め等を認めたものに東京地判平成21・2・27［マジコン事件］がある。事案では、不競法上の「技術的制限手段」が検知→制限方式のものに限られるか，自主制作ソフト等の実行も制限する結果となる検知→可能方式のものを含むかが争われ、判決は、信号検知により視聴が制限される方式のみならず、信号が検知されることで視聴が可能となる方式も含むとした。

4) 角田政芳「インターネットで違法配信されている任天堂DS用ゲームソフトをダウンロードしてプレイできるようにしたマジコンを輸入してDSユーザーに販売する行為を不競法上のアクセス・コントロール無効化行為として差止めを認めた事例」発明106・12（2009）46、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（2010）279、廣瀬隆行「マジコン事件（実務家のための知的財産権判例 70 選 2009 年度版）」発明 107・9（2010）62、帖佐隆「マジコンをどう考えるか：マジコン事件東京地裁判決及び改正不競法との関連等も含めて」パテント 65・5（2012）39、金暁特「不競法 2 条 1 項 10 号技術的制限手段迂回装置提供行為の範囲について―マジコン事件を大罪に―」知的財産法政策学研究 44（2014）335 など。

5)　認証回避型クラック・パッチの提供に関する論考に、古川原明子「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―不競法および刑法の観点から」龍谷法学（2012）45-2，119、村本武志「プログラムの違法複製をめぐる著作権法、不競法と不法行為法の交錯」現代法学（2013）23=24、215 など。古川原は、ライセンス認証システムを「信号送信型」の技術的制限手段と捉える。この類型では、「信号」とともにプログラムが送信される必要があるところ、ここでの「プログラム」が何を指すのかは必ずしも判然としない。

6)　2014 年 9 月 29 日付け時事通信「不正プログラム販売容疑＝被害 500 件か、男逮捕―栃木県警」

7)　2014 年 9 月 11 日付け福井新聞「ブログでソフト使用解除ツール提供容疑で少年逮捕、MS オフィス被害」

8)　1999 年当時、技術的保護手段の対象であるコピー・コントロールとして、SCMS、CGMS、擬似シンクパルス方式が、アクセス・コントロールとして、DVD などに用いられている CSS が開発・利用されていたが、その後、これらの保護技術を組み合わせた技術が増加し、DVD において CSS と CGMS 等を重畳的に施したものや、DVD-Audio の保護技術である CPPM、DVD-Recorder の保護技術である CPRM、デジタルインターフェースの保護技術である DTCP 等が開発・利用されているとされる（文科省ウェブサイト「4　技術的保護手段の規定の見直し」http://www.mext.go.jp/b_menu/shingi/bunka/gijiroku/013/05072901/002-4.htm。

9)　アクセス・コントロールの方法の一つに、パスワード認証がある。これは、ユーザー ID とパスワードを定義し、これらの組み合わせが適合する場合にのみ、コンピュータ・システムにアクセスできる仕組みである。そのほ

か、IC カードによる ID カード、生体認証、電子署名、電子証明書などがある。ネットワークのアクセス・コントロールとしては、IP アドレス制限、URL フィルタリング、暗号通信、SSL 認証などの手段がある。

10) 例えば、マイクロソフト社では、許諾された本数に対応するコンピュータ（正確には CPU）への複製を認めるものに「ボリュームライセンス」と呼ばれる製品を販売する。製品開発用途での同一使用者であれば、同一シリアルでのインストールが許諾され、認証がなされるものもある。この場合のライセンス認証方式は、通常のパッケージ版とは異なる。

11) 認証許可のためにどのようなデータ送信が必要とするかは、メーカーにより異なる。名称も、マイクロソフト社は「インストール ID（あるいは confirmation ID)」、アドビシステムズ社、オートデスク社は「リクエストコード」）と呼ぶ。

12) 認証可とされる場合にユーザーパソコンに送信されるメッセージの呼称も各社で異なる。アドビシステムズ社では「レスポンスコード」、オートデスクインク社では「アクティベーションコード」、マイクロソフト社では「プロダクト ID」と呼ぶ。

13) ボリュームライセンス、サイトライセンスなどと呼ばれるが、メーカーによって呼称は異なる。

14) たとえばマイクロソフト社の MSDN 契約など。

15) Windows 95 以降の Windows 系 OS において、Windows の外観と動作を決定するすべての構成設定データが一覧表示されるデータベースである（マイクロソフト社)。

16) 前掲準則 iii. 74 参照。

17) 海外法制については、内閣官房知的財産戦略推進事務局「アクセス・コントロールの回避規制の在り方に関する主な論点」、同「これまでの議論を踏まえた論点整理について」（2010 年 3 月 16 日)、西村あさひ法律事務所「平成 21 年度経済産業省委託調査　コンテンツの技術的手段に係る各国法制度調査研究報告書」（2010 年 3 月）参照。

18) DMCA 違反を認めた判決に、I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Info. Systems, Inc., 307 F. Supp. 2d 521 (SD NY 2004)、R. C. Olmstead, Inc. v. CU Interface LLC, 657 F. Supp. 2d 878 (ND Ohio

2009), aff'd on other grounds, 606 F. 3D 262 (6th Cir. 2010)

19)　321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (ND Cal. 2004)、Microsoft Corp. v. EEE Business Inc., 555 F. Supp. 2d 1051 (ND Cal. 2008)、Microsoft Corp. v. Pronet Cyber Technologies, Inc., No. 1:08-cv-434 (ED VA Dec. 5, 2008).

20)　Actuate Corp. v. International Business Machines Corp., 2010 WL 1340519 (ND Cal. April 5, 2010)

21)　情報社会における著作権および関連権の一定の側面のハーモナイゼーションに関する欧州議会および EU 理事会の指令（2001/29/EC)。

22)　経済産業省知的財産政策室『逐条解説不正競争防止法 平成 23・24 年改正版』有斐閣（2012）183 は、営業秘密の不正取得に関する不競法 21 条 1 項 1 号の「図利加害目的」について、同旨を述べる。

23)　前掲逐条解説 183。

24)　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（2012)「技術的制限手段に係る不競法の見直しの方向性について（案)」平成 22 年 2 月、http://www.meti.go.jp/press/20110221003/20110221003-2.pdf

25)　日本知的財産協会デジタルコンテンツ委員会、http://www.jipa.or.jp/jyohou_hasin/teigen_iken/10/110121.pdf

26)　古川原・前掲 112―

27)　2014 年 6 月 17 日付け下野新聞