暗号技術を位置づける社会的枠組みについての考察

山根信二[†] 村山優子[†]

1990 年代の暗号技術規制論は，キーエスクローシステムを中心とする枠組みで論じられた．だが当時の議論はもはや有効ではない．今後の暗号技術の進路策定について議論する際には，1990 年代の議論とは異なる枠組みが必要である．現在，議論のための枠組みの形成が急がれている新たな暗号技術問題として，暗号解析をめぐる係争があげられる．暗号技術の開発評価において暗号解析は重要な役割を担ってきたが，暗号解析の公表やその再配布については議論が分かれている．日本では，1999 年から著作権の「技術的保護手段」の回避を行うプログラムを公表しようとする者は処罰されることになった．本論文では，この法制による暗号解析への影響を，2000 年にアメリカで起こった DVD プロテクト破り訴訟を参考にしながら検証する．コピープロテクトに対する暗号解析の公表を法的に規制することは，コンピュータ専門家がかかえる技術的および法的リスクを増大させる．また，その影響はコピープロテクト技術のみにとどまらず，暗号技術の開発評価全般に及ぶ可能性がある．このような問題に対処するためには，暗号解析を含む暗号技術開発の進路策定を決める枠組みを刷新することが必要である．最後に，今後の専門家に要求される新たな役割についても検討を行う．

An Analysis of Social Framework for Cryptography Technology

Shinji Yamane[†] and Yuko Murayama[†]

The regulation of cryptography in 1990s had been formed under the “framework of key escrow system,” such as the limitation of the key-length or the lawful access field. While the 1990s’ framework is not effective anymore, a new framework of regulation is evolving worldwide. After 1999, the copyright act in Japan prohibits “the circumvention of a technological copyright protection measure.” This act can make some work including the reverse engineering and cryptoanalysis illegal. The same problem has examined in the U.S. on the DeCSS DVD decoder lawsuit in 2000. The outlawing of the circumvention of the copyright protection technology is not limited only the cryptanalysis, and will effect to the further social problem. The new role of computer professionals are required to deal with this new kind of risks. Finally this paper examines the computer professional’s activities for the comming alternative framework as well.

1. はじめに

暗号化された機密情報の解読法を公表しても，その行為自体が処罰されることはこれまでになかった．日本で国内では個人の暗号利用は制限されず，暗号および復号プログラムも自由に配布されてきた．しかし，こうしたことがらは自明のことではない．著作権法改正によって，暗号解読プログラムの公表が規制対象に含まれかねない状況が発生している．

本論文では，これまで暗号技術の位置づけを規定してきた枠組み（framework）を整理するとともに，暗号技術開発の中でも特に暗号解析において近年発生した問題を解決するための枠組みについて検討する．

† 岩手県立大学ソフトウェア情報学部
Faculty of Software and Information Science, Iwate Prefectural University

2. 1990 年代の暗号政策の枠組み

現在の動向に触れるまえに，まず従来の枠組みを概観する．1990 年代後半における暗号規制論は，もっぱらキーエスクローシステム☆（法執行機関が暗号化された情報に合法的にアクセスできる社会制度）を中心に論じられた．アメリカでクリッパーチップからキーエスクローセンターの国際協調構想にいたるまで形を変えながら議論され続けた[21] キーエスクロー提言は，日本でもまた活発に議論されてきた．たとえば 1997

☆ キーエスクローシステムは，鍵寄託，鍵供託，鍵回復（キーリカバリー）制度とも呼ばれている[23]．この語が幅広く用いられるにつれて，法執行機関が暗号化された情報に合法的にアクセスするという当初の制度だけでなく，組織内の鍵バックアップ一般をも指すようになった．本論文ではそうした一般的な意味ではなく，提案当初の法執行機関を前提にした運用形態を指して「キーエスクローシステム」という呼称で統一する．

年に郵政省審議会の「ネットワークを通じた認証業務の在り方に関する調査研究会報告書」[14]が，アメリカではキーエスクローの導入が決定され国際的にも採用が呼かけられていると報告しており，同年の警察庁外郭団体による報告書[8]もキーエスクローが国際社会において「きわめて高い関心を持って議論されている」ことを報告している．そして翌1998年，警察庁の情報セキュリティビジョン策定委員会の報告書[9]では，暗号化された情報へのアクセスの必要性やキーエスクローセンターおよび公証機関の業務について検討を行い，日本国内で利用できるキーエスクローセンターを制限する方策の検討についても言及している．

この動きは審議会レベルにとどまらない．1998年の警察白書[11]あるいは政府の高度情報通信社会推進本部の基本方針[12]でも，暗号技術の「不正利用」対策として，法的環境整備の検討を行うことが明記されている．これらの動向は，法執行機関がいかに暗号技術をコントロールするかが1990年代の国家的論点だったことを示している．

だが，こうした1998年までの審議はその後方針を転換する．個々のキーエスクロー技術自体は研究が進められ実用化も進んでいるが，ナショナルセキュリティのために暗号鍵の長さを制限したり暗号鍵を管理する体制としてのキーエスクローシステムは省庁の審議では扱われなくなる．その結果，1999年にはキーエスクローシステムは「もう死んでしまった過去の話」[28]だとする見方も出ている．暗号技術の開発が進む一方で，政府の暗号についての基本方針が1年後には顧みられなくなるというこの方針転換は，暗号技術の社会的位置づけが不変不動のものではないことを示している．たとえば，暗号技術はある枠組みでは武器として位置づけられ，別の枠組みでは電子認証の基盤として位置づけられる．枠組みによって暗号技術の位置づけはまったく異なり，さらにその枠組みがいつ再び転換するのかも定かではない．キーエスクローシステムの国家的議論を成立させていた枠組みが機能しなくなった今日，今後の暗号技術のあり方について進路策定を決めるためには，新たな枠組みについて考えることが不可欠である．

3. 暗号解析と著作権保護技術

キーエスクローシステムの後，暗号技術はそれまでとは異なる枠組みによって社会的に位置づけられている．その一例として，公開議論による暗号評価の進展をあげることもできる．AESのような公募方式による暗号の採用を可能にする枠組みは，かつてクリッパーチップの採用が唱えられていた1990年代の枠組みとは明らかに異なるものである．

この状況に対して，本論文では新たな枠組みにおいて暗号技術の開発にどのような係争が起こり解決が必要とされるのかを検討する．そのために，以下では暗号技術の新たな法規制として暗号解析の位置づけに注目する．この係争は，1990年代末のコピープロテクト破り規制において問題化したものである．

1996年のWIPO著作権条約において，「著作権保護技術の迂回（回避）」への対応が義務づけられた．それまでも無断コピーは処罰されてきたが，この新たな規制は無断コピーを行う前段階のプロテクト外しも対象に含めるものである．たとえば，著作権保護に暗号化技術を使った場合，その技術を破ったりリバースエンジニアリングにかけたりすることは迂回行為に該当する．さらに迂回を行うプログラムの配布についても検討対象となる．WIPO条約は加盟国に対して，著作権保護技術の迂回に対する「適切な」法的保護および効果的な法的救済措置を講じるように義務づけている[18]．その「適切な措置」を具体的に実施する際に，各国のセキュリティ技術の位置づけが問われることになる．

国際条約に端を発するこの新たな動向は，国内のみならず国際的同時性において見る必要がある．そこで本論文では，以下でアメリカと日本の動向をとりあげる．まず，アメリカでの動向について．これは1995年のNII著作権保護法案からWIPO著作権条約インプリメント法案を経て，最終的に1998年のデジタルミレニアム著作権法として制定され，現在に至っている．そして日本での動向について．これは1998年の文部省および通産省の審議会を経て，1999年の第145回国会における著作権法改正に至っている．そして，この枠組みの中でコンピュータ専門家がどのような役割を果たすのかを論じる．

3.1 アメリカでの動向

3.1.1 著作権法案についての議論

アメリカでの議論においてはACMが中心的な役割を果たしてきた．1990年代後半の *Communications of the ACM* では，知的財産権の専門家パメラ・サミュエルソン（後にACM U.S. Public Policy Committeeメンバー）の批判[17]をはじめとして，たびたびWIPO関連の法案についての批判がなされており，それら一連の批判は後に冊子にまとめられてもいる[19]．特にコンピュータ専門家の間で議論を呼んだのは，セキュリティ開発における評価用プログラムの発表のみならず，コンパチビリティを実現するためのリバースエン

ジニアリング全般が非合法になりかねないという点である．

またACM周辺では，論説だけでなく関連する専門家集団との共同声明も行われた．たとえば，ACMをはじめとする数理・計算機・通信の各分野の学会（AAAS, AAAI, AMS, ASA, ACM, CRA, SIAM, IEEE）の会長が米議会司法委員会に共同声明を提出している[6]．また，ACMのUS Public Policy Committeeの議長でもあるパデュー大学コンピュータサイエンス学部教授のスパフォードがまとめたセキュリティ専門家の署名運動[26]がある．

これらのコンピュータ専門家の批判を受けて成立したのが1998年のデジタルミレニアム著作権法（DMCA）である．この法律のセクション1201では「技術的保護措置を迂回する（circumvent a technological protection measure）」ことを禁じている．この規制対象となる行為とは，著作権者から権限を得ることなしに，「スクランブル化された著作物を逆スクランブル（descramble）し，暗号化された著作物を解読（decrypt）し，その他の方法で技術的保護措置を回避し（avoid），バイパスを作り，削除し（remove），無効化し（deactivate），または，駄目にする（impair）」という広い範囲に及ぶものである[1]．

この条文に対して，議会を通過するまでにいくつかの例外行為が盛り込まれた．たとえば非営利の図書館・アーカイブ・教育機関は，規制対象から除外されている．これは，特定のプラットホームでしかアクセスできないような著作権保護手段によって，アーカイブの目的である公共性が損われないための措置である．また，研究教育目的のための暗号解析も合法とされている．当初の法案には存在しなかったこれらの例外条項は，上述した専門家集団による批判をとりいれた成果だといえる．

3.1.2 DVD事件の技術的問題点

本項では，DMCA法案施行後の係争として，DMCAに基づいて暗号解読プログラムの配布禁止を求めた事例をとりあげる．

問題になったのは，1999年末にインターネット上で配布されたDeCSSプログラムである．これはDVDムービーのデジタルコピーを防止するために暗号化および認証を行うためのコンテンツ・スクランブリング・システム（CSS）を破るためのプログラムである．まず最初にWindows上でのDVD再生ソフトをリバースエンジニアリングしたアセンブラのコードがネット上に投稿され，その後C言語に書き直されたうえで，DVDビデオファイルを再生したりハードディスク上に保存したりするツールに組み込まれて配布されている[15]．

アマチュアによって暗号解読されたことが社会的関心を集め，1999年11月に報道された直後から，DVDのプロテクト破りの技術的問題についてはジャーナリズムによってさまざまな指摘が行われている．まずDVDが暗号解読された原因として，設計者・再生ソフトメーカに問題があったのではないかという指摘がなされた．具体的には，DeCSS開発者の談話を通じて，商用Windows用DVD再生ソフトの中に暗号鍵を保護していなかった製品があったために暗号鍵を取り出すことが容易だったこと，そしてそのCSSの暗号鍵が40ビットの長さしか持っていないために暗号鍵の推測も容易だったという指摘[16]がなされている．また，実際には40ビットよりもさらに少ない範囲で暗号鍵を推測できるという暗号解析[27]も，早い段階から報道されていた[13]．

さらにSchneier[20]はそうした実装およびCSSアルゴリズム固有の脆弱性を認めつつも，現在の汎用PC上でのソフトウェアタンパではコピープロテクトのリバースエンジニアリングを止めることはできないと指摘し，より優れたアルゴリズムと実装によってもPC上でのDVD破りは時間の問題だったはずだと論じている．アルゴリズムや製品に固有の問題だけでなく，汎用PC上でのコピープロテクトソフトウェアに共通する脆弱性についてのこの指摘は，今後CSS以外のコピープロテクト技術を検討する際にも重要である．

3.1.3 DVD訴訟の社会的位置づけ

このDeCSSをめぐって起こったのが，機器メーカを中心としたDVDコピー管理協会（DVDCCA）がカリフォルニアで起こした訴訟と，映画会社のロビイスト団体である米国映画協会（MPAA）がニューヨークで起こした訴訟である☆．これらの訴訟で告訴されたのは世界各地の人物で，その中には1999年にDeCSSを作成配布したプログラマ，CSSの暗号解析[27]をオンラインで公表したプログラマ，さらにそのソースコードの再配布を行った（あるいはサイトにリンクを

☆ DVDCCAとMPAAとの主張には企業秘密盗用と著作権法違反のどちらに力点をおくかで微妙な相違があるが，新しく施行されたDMCAに違反するものだという主張は両者に共通している．以下，アメリカでの訴訟の裁判資料は，被告の弁護を行うElectronic Frontier Foundation（http://www.eff.org/pub/Intellectual_property-/Video/DVDCCA_case/），Harvard Law SchoolのBerkman Center for Internet & Society（http://eon.law.harvard.edu/openlaw/dvd/）のオンライン情報を参照した．

張った）人々から構成されている☆.

この裁判をめぐる議論はいまだに明確な枠組みが定められているとはいえない．たとえば DeCSS にリンクしているだけの被告は複製行為を行ってはおらず，著作権を侵害していない，という被告側の当初の主張は DMCA においては問題にならない．なぜなら DMCA は著作権法ではあるが，従来のように無断コピー行為を処罰するのではなく，その前段階と見なされるセキュリティ技術破り（とツールの配布）を処罰するものだからである．この点で，DMCA は従来の著作権法よりもむしろ無権限アクセス処罰法に近い．

また，CSS アルゴリズムの暗号解析[27] をオンラインで公表した人物も被告に含まれていることは注目に値する．これは論文から DeCSS のソースコードにリンクを張っていたためだと考えられるが，これは CSS の内部動作を評価するために必要な手続きだったと考えられる．DMCA 成立時の論点の 1 つとして，暗号化の研究開発は例外条項になっているのにコンピュータセキュリティの研究開発は含まれていないという批判があった[24]．しかしこの CSS 破りをめぐる訴訟では，そもそも暗号解析の研究論文すら例外とは見なされない可能性を示している．このように，法案施行後の法廷では，法案審議中のコンピュータ専門家による批判が十分に考慮されていない．

3.1.4 「ハッカー」という問題設定

法案成立時のコンピュータ専門家による議論が十分に生かされていない法廷の状況は，原告側の主張を強く反映したものである．たとえば DeCSS プログラムの配布やリンクによって告訴された者は在野のホビイストばかりであり，なかには十代の学生も含まれている．それとは対照的に，リンクを張っているアカデミックの暗号学者は告訴されていない．さらに MPAA による訴訟では，過去にネットワーク攻撃侵入ツールを配布してきたアンダーグラウンド雑誌の編集者が被告代表としてあげられている．こうした被告の顔ぶれのために，裁判官や多くの報道は被告を過激な思想を持つ「ハッカー」としてとらえており，学会でひろく共有されてきた問題意識との接点を見逃しがちである．

著作権法を拡張する際に「無法者のハッカー集団☆☆」というラベルが用いられるという事態はこれ以前にも起こっている．知的財産権研究者の Halbert は，1980 年代の報道において，ホビイストにすぎなかったハッカーのイメージがテロリストと混同されるようになった過程を検証している[7]．Halbert によれば，ハッカーのイメージが社会的脅威へと変形されたのは知的財産権や政府の機密についての権益を促進するためにほかならない．2000 年の DeCSS をめぐる訴訟とその報道における「過激な思想を実践するハッカー」という図式もまた同様の枠組みに従っているといえるが，暗号技術開発において重要な役割を占める暗号解析にまで範囲がひろがっているという事態はこれまでになかったものである．

この係争は最高裁まで続き，それまでにさらなる議論が進められることが予想されるが，一審の判断は原告の訴えを支持している．すなわち 2000 年 8 月 17 日の連邦地方裁判所の判断では，被告は過激な運動の信奉者とされ，原告の訴えを支持して暗号解読プログラムの配布やリンクを禁じる命令が出されている[32]．しかし，実際に被告を支援する側に注目すれば，3.1.1 項でとりあげた DMCA 法案についての議論を行った専門家が数多く存在しており，その裾野はいわゆる「運動の信奉者」にとどまらないことが明らかになる．たとえば訴訟反対集会にはサミュエルソンも参加しており[10]，DMCA 法案審議中に署名運動を行ったスパフォードは著作権侵害行為および侵害行為に対して激しい批判[25] を行ってきたセキュリティ専門家である☆☆☆．過激派集団としての「ハッカー」というラベル貼りはこうしたコンピュータ専門家の裾野のひろがりを単純化している．

3.2 日本での動向

次に日本での動向を検討する．日本でのコピープロテクト技術の迂回（回避）への対策は，文部省・文化庁の著作権審議会，そして通産省の産業構造審議会によって検討が始められた．

1998 年に答申された著作権審議会ワーキング・グループの報告書[30] では，権利侵害行為を事前に防止するために，権利侵害行為の前段階である迂回行為自体を規制すること，そして回避プログラムを提供する行為を営利非営利を問わず規制対象とすることが提案されている．そしてこの報告書と相前後する 1998 年後半に，通産省でもプロテクト破りをどう位置づけるかが検討されていた．それは産業構造審議会の分科会

☆ 特に DVDCCA による裁判においては，被告の全貌を把握することは困難である．告訴状[4] によれば，DeCSS の配布行為を行っていた 21 人の個人と 72 のサイトのほかに 1 番から 500 番までの氏名不詳の人物（“Does 1–500”）が告訴されている．

☆☆ 元来ハッカーは技術的に評価されてきた人々であり，セキュリティ破りや無断コピーを行う者を指す呼称ではない．現在でも RFC2828[23] はハッカーという呼称を正統的な意味において用いるように推奨している．

☆☆☆ スパフォードのハッカーに対する批判の不当な点については，江口[2),3)] を参照．

による報告書案[29]としてオンライン公開され，パブリックコメントの募集も行われている．その案では，以下のように規制に対する例外事項が盛り込まれていた．「試験，研究開発（特にリバースエンジニアリング）のための管理技術の無効化その他，公益性の観点や生じ得る経済的被害との比重衡量の観点から，管理技術の無効化が是認される場合が存在すると考えられる．これらの是認される目的のみに管理技術の無効化機器等を用いる者に当該機器などを提供する行為については，規制の対象としない扱いが可能となる方向で検討する」．

これらの知的財産権保護についての 2 つの議論は，翌年 1999 年の国会でそれぞれ別々に審議されることになる．

3.2.1 不正競争防止法

通産省からの不正競争防止法の改正案[5]は，1999 年 4 月 16 日に第 145 回国会において成立した．その不正競争防止法第二条において，「不正競争」に新しい概念が導入されている．それは，営業上の「技術的制限手段」，すなわち「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制限する手段」の効果を妨げるための専用装置やプログラムに対して，譲渡や配布を制限しようとする考え方である．ただし，この装置もしくはプログラムが技術的制限手段の試験または研究のために用いられる場合は，対象には含まれないとされる．

この例外条項は，リバースエンジニアリングや暗号解析の社会的位置づけに対して一定の理解を示している．これに対して，日本の著作権法はどのように変わったのかを次に検討する．

3.2.2 著 作 権 法

1999 年の著作権法の改訂は 6 月 15 日に第 145 回国会において成立し，同月 23 日に平成 11 年法律第 77 号として公布され，10 月に施行された．WIPO 条約の実施にかかわる部分は以下の部分である．

第百二十条の二 次の各号のいずれかに該当する者は，一年以下の懲役又は百万円以下の罰金に処する．

一 技術的保護手段の回避を行うことを専らその機能とする装置（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含む）若しくは技術的保護手段の回避を行うことを専らその機能とするプログラムの複製物を公衆に譲渡し，若しくは貸与し，公衆への譲渡若しくは貸与の目的をもって製造し，輸入し，若しくは所持し，若しくは公衆の使用に供し，又は当該プログラムを公衆送信し，若しくは送信可能化した者．三 営利を目的として，第百十三条第三項の規定により著作者人格権，著作権又は著作隣接権を侵害する行為とみなされる行為を行った者[31]

DMCA と同様に，無断コピーや著作権侵害の行為の有無とは関係なく，迂回に用いられる装置やプログラムを配布しようとする行為事態を処罰するという考え方が示されている．ただし，DMCA は研究教育目的といった公正な使用を対象外として扱っていたが，日本の著作権法にはそういった例外規定がないことが大きく異なる．

4. 考 察

現在の枠組みでは．もはや暗号技術は武器として扱われることはない．しかしこれまでに見てきたように，現在の枠組みにおいては，とりわけ暗号解析の位置づけについて新たな係争が起こっている．以下では，今後考えられる影響と，その影響に対してどのような方策が必要とされるかを考察する．

4.1 リスク分析

4.1.1 技術的リスク

暗号技術の開発評価において，暗号解析は重要な役割を担っている．特に近年では AES，Nessie，CRYPTREC などに見られるように，暗号解析を公開の場で議論することが暗号技術の開発評価における主流であるともいえる．この動向に対して，著作権保護技術の迂回についての社会的位置づけは不整合を起こしている．

特に，現在の汎用 PC において保護技術の迂回を防止することが技術的に困難であることを考えた場合，迂回を規制または防止できるという前提に立ったシステムは技術的リスクをともなっているといえる．したがって，現状では迂回を処罰するのではなく，迂回されることを前提とした技術開発（たとえば透かし技術をはじめとする追跡技術や配布抑止技術）に基づく防止策を推進することがより有効であると考えられる．

4.1.2 法的リスク

日本国内で暗号解析のソースコードを公表した場合，研究目的であれば不正競争防止法が規制する「技術的制限手段の効果を妨げる」プログラムには該当しない．だが，もしその暗号方式が著作権保護に使われていた場合は考慮を必要とする．

アメリカでの地裁の判断を考慮すれば，次のような法的リスクが考えられる．暗号解析を行う研究者がその結果を公表した場合に，もしもその暗号が著作権保護に用いられ，かつ公表されたソースコードをリンクした解読ツールを発表した場合，研究者は著作権侵害

の訴訟を招くリスクをかかえることになる．そこで法的環境整備によって評価用ソースコードおよび教育活動や公的アーカイブ活動を処罰対象外とすることが考えられるが，公正な利用に対する例外条項を設けたDMCA おいても，暗号解析をオンライン公開したした者が告訴されたことに注意する必要がある．これは，たとえ研究発表であっても，それが回避プログラムとリンクしている場合には「ハッカー集団」というラベル貼りによって暗号解析の公開が不法行為として見なされうる可能性を示している．特に日本の著作権法においては，DMCA に追加された例外条項がそもそも存在しない点にも注意する必要がある．

さらに，この法規制が及ぶ範囲が今後さらにひろがることも考えられる．DVD 訴訟において問題となっているのは，暗号技術開発の中でもコピープロテクトの暗号解析という一分野にすぎない．しかし，これが暗号解析全般そして暗号技術開発，さらにはセキュリティ技術開発に及ぶ可能性も否定できない．すなわち，将来において DVD のような記憶媒体だけではなく，通信データを著作物として主張された場合，情報通信にかかわる広範な暗号解析やリバースエンジニアリングが著作権法上のリスクをかかえることになる．これは暗号技術の開発評価全般に対して深刻な影響を与える可能性がある．

4.2 将来の枠組みに向けて

以上のリスクをふまえて，これまでの議論の枠組みに不足していた論点について考察し，今後取り組むべき問題について論じる．日本では著作権法案のリスクについて現在にいたるまでまったく議論されてこなかった．これには以下の理由が考えられる．

まず，暗号政策についての議論が 1990 年代のキーエスクローの枠組みでしか問題化されなかったことがあげられる．たとえば同じ第 145 回国会では，通信傍受法や住民基本台帳法をめぐってナショナルセキュリティとプライバシーとのトレードオフがさかんに論じられた[22]．だが，その対立図式では著作権法を問題化することができない．新しい著作権法の問題点を明らかにするには，暗号解析を位置づける枠組みを刷新することが必要である．

次に，審議が専門化細分化していたことがあげられる．日本の場合，不正競争防止法は研究開発目的の暗号解析を例外扱いとしているが，著作権法には例外条項がない．これは法律によって暗号解析の位置づけが異なるために起こった不整合だといえる．このような不整合を招かないためには，法律上のカテゴリを横断するような枠組みの上で個々の法案を検討することが望ましい．

以上の点をふまえて，暗号解析をはじめとする暗号技術の重要性を考慮したとき，ナショナルセキュリティや著作権中心主義による拙速な立法論を相対化するために，暗号技術についての新たな議論の枠組みを確立することが要請されている．そのためには，技術的な分析に基づいて暗号技術の社会的位置づけを明確にする必要があると考えられる．

暗号技術開発の中でも，特に暗号解析の位置づけは長大な問題をはらんでおり，正当な位置づけのためにコンピュータ専門家や学会が果たすべき役割は大きい．この取組みについてはいまだ十分な蓄積がなく，コンピュータ専門家がどのような役割を果たすべきかというモデルについては議論の余地がある．最後に，そうしたセキュリティ技術の進路策定を決める枠組みを提示する役割を率先して担ってきたアメリカの ACM，特に U.S. Public Policy Committee を中心とした活動についての評価を試みる．

3.1.1 項で示したように，ACM が試みた技術的分析の提供や学会を越えた連携によるポリシーメーカへの働きかけは議会での立法において一定の成果をおさめたといえる．暗号技術を社会的に位置づける枠組みを相対化し刷新する作業はコンピュータ専門家集団に負うところが大きく，これからは各国の専門家集団が同様の役割を果たすことが期待される．

しかし 3.1.3 項で検討したように，アメリカでの DMCA 施行を受けて起きた DeCSS 訴訟では，DMCA が及ぼす広範な影響を明確化することは必ずしも成功していない．訴訟においては，保護技術を迂回するプログラムの開発配布は，過激な「ハッカー」集団が起こした侵害事件として位置づけられている．すなわち，暗号解析はもっぱら著作権中心主義における侵害行為として位置づけられ，暗号技術の研究教育や開発評価における重要な要素としては位置づけられなかった．これまでの訴訟では，この位置づけを刷新するための作業が不足していたということができる．これは，脆弱性の暴露に対して無法者のラベルを貼って処罰を行うのではなく，むしろ暴露を前提としたうえでなお安全な社会体制作りを推進する必要がある．すでに公開の議論による暗号評価は主流の位置を占めているが，今後は法曹界や業界団体を含む社会的な認識を形成することが要求される．

5. ま と め

暗号技術を社会的に位置づける枠組みは，不変不動のものではない．いずれの枠組みが適切なのかという

問題は，その枠組みの歴史的な相対化を抜きにしては語ることができない．本論文では，1990 年代の枠組みとそれ以後に形成された著作権中心主義の枠組みとを整理するとともに，著作権保護技術および暗号技術の開発評価全般に及ぶ影響を検討し，技術的なリスクの分析の必要性について論じた．

コンピュータ専門家が果たすべき役割の諸形態についてはいまだ十分な蓄積がないが，アメリカと日本の事例から今後検討すべき課題について示した．

参 考 文 献

1) Digital Millennium Copyright Act: United States Code, Title 17, Sec.1201 (HR-2281) (1998).
2) Eguchi, S.: The Unauthorized Access Issue in Japan, *The First International Workshop for Foundations of Information Ethics* (*FINE99*), Kyoto (1999). http://www.fine.bun.kyoto-u.ac.jp/~eguchi/fine99-eguchi.html
3) 江口 聡：クラッキングと「ハッカー倫理」，電子情報通信学会技術研究報告，FACE97-22 (1998).
4) Electronic Frontier Foundation: DVD CCA Complaint in DVD CCA v. McLaughlin, Bunner, et al. (Legal Complaint sent to defendants by email) (1999). http://www.eff.org/IP/Video/DVDCCA_case/19991228-complaint.html, Also published at http://cryptome.org/dvd-v-500.htm
5) 不正競争防止法：平成 11 年 4 月 23 日法律第 33 号による改正 (1999).
6) Greenwood, M.R.C., Waltz, D.L., Jaffe, A., Moore, D.S., Simons, B., Lazowska, E., Guckenheimer, J. and Reinert, J.R.: Letter on the Impact of HR 2281 from Presidents of Eight Major Scientific Societies (Sept. 14. 1998). http://www.acm.org/usacm/copyright/presidents-letter-998.html
7) Halbert, D.J.: Hackers: The Construction of Deviance in the Information Age, *Intellectual Property in the Information Age: The Politics of Expanding Ownership Rights*, Chap.5, pp.101–120, Quorum Books (1999). Originally appeared in *Information Society*, Vol.13, No.4, pp.361–374 (1997).
8) 情報セキュリティ調査研究委員会：情報セキュリティ調査研究報告書，日本実務出版 (1997).
9) 情報セキュリティビジョン策定委員会：情報セキュリティビジョン策定委員会報告書：安全なネットワーク社会の実現を目指して，警察庁 (1998). http://www.npa.go.jp/hightech/secv_repo/.
10) Kang, Y.P.: Just Like Old Times in Berkeley, *Wired News* (July 11, 2000). http://www.wired.com/news/culture/0,1284,37501,00.html
11) 警察庁：平成 10 年警察白書：ハイテク犯罪の現状と警察の取組み (1998).
12) 高度情報通信社会推進本部：高度情報通信社会推進に向けた基本方針，Chap.II-7 (1998). http://www.kantei.go.jp/jp/it/981110kihon.html
13) McCullagh, D.: Blame US Regs for DVD Hack, *Wired News* (Nov. 11, 1999). http://www.wired.com/news/technology/0,1282,32487,00.html
14) ネットワークを通じた認証業務の在り方に関する調査研究会：ネットワークを通じた認証業務の在り方に関する調査研究会報告書，Chap.10，郵政省 (1997). http://www.mpt.go.jp/policyreports/japanese/group/internet/index-net-n.html
15) Patrizio, A.: DVD Piracy: It Can Be Done, *Wired News* (Nov. 1, 1999). http://www.wired.com/news/technology/0,1282,32249,00.html
16) Patrizio, A.: Why the DVD Hack Was a Cinch, *Wired News* (Nov. 2, 1999). http://www.wired.com/news/technology/0,1282,32263,00.html
17) Samuelson, P.: Regulation of technologies to protect copyrighted works, *Comm. ACM*, Vol.39, No.7, pp.17–24 (1996).
18) Samuelson, P.: The Future of the Information Society and the Role of Copyright in It, 情報化社会の未来と著作権の役割，IIP 研究論集 3, pp.1–53，信山社 (1998).
19) Samuelson, P., Neumann, P., et al.: *Intellectual Property in the Age of Universal Access*, Association for Computing Machinery (1999).
20) Schneier, B.: DVD encryption break is a good thing, *ZDNet News* (Nov. 12, 1999). http://www.zdnet.com/zdnn/stories/comment/0,5859,2395497,00.html
21) Schneier, B. and Banisar, D. (Eds.): *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*, John Wiley & Sons (1997).
22)「世界」編集部（編）：ストップ! 自自公暴走：日本の民主主義の再生のために,「世界」別冊 No.668, 岩波書店 (1999).
23) Shirey, R.W.: Internet Security Glossary, Request For Comments, RFC 2828 (Also FYI 36) (Status: Informational) (2000).
24) Simons, B.: Outlawing Technology, *Comm.*

☆ 参考文献中の URL は 2001 年 6 月 10 日時点のものである．

ACM, Vol.41, No.10 (1998). Also reprinted in *Intellectual Property in the Age of Universal Access*[19].
25) Spafford, E.H.: Are Computer Break-ins Ethical?, *Computers, Ethics & Social Values*, Johnson, D.G. and Nissenbaum, H. (Eds.), 1st edition, pp.125–135, Prentice-Hall (1995). Originally appeared in *J. Syst. Softw.* Vol.17, pp.41–47 (1992).
26) Spafford, E.H., et al.: WIPO Letter from the InfoSec Community (1998). http://www.cerias.purdue.edu/homes/spaf/WIPO/
27) Stevenson, F.A.: Cryptanalysis of Contents Scrambling System, Online Document (1999). http://crypto.gq.nu/ (removed in 2000). There are several mirror sites, i.e., http://www.lemuria.org/DeCSS/crypto.gq.nu.
28) 鈴木裕信：時代遅れな「キーエスクロー」，*Internet Magazine*, No.56, pp.330–331 (1999).
29) 通商産業省：産業構造審議会（知的財産政策部会デジタルコンテンツ分科会，情報産業部会基本問題小委員会デジタルコンテンツ分科会）合同会議報告書案「デジタルコンテンツのコピー管理技術及びアクセス管理技術の回避に関する法的基盤の在り方について」(1998). http://www.meti.go.jp/feedback/data/ideji30j.html
30) 著作権審議会：著作権審議会マルチメディア小委員会ワーキング・グループ（技術的保護・管理関係）報告書，Chap.2，文部省 (1998). http://www.monbu.go.jp/singi/chosaku/00000224/
31) 著作権法，平成 11 年 6 月 23 日法律第 77 号による改正 (1999).
32) United States District Court, Southern District of New York: MPAA v. Corley (Universal City Studios, Inc., et al. v. Reimerdes, et al.), 111 F.Supp.2d 294. Judge Lewis A. Caplan's decision on August 17 (2000). http://www.eff.org/pub/Intellectual_property/Video/MPAA_DVD_cases/20000817_ny_opinion.pdf, http://eon.law.harvard.edu/openlaw/DVD/NY/opinion.pdf.

(平成 12 年 12 月 12 日受付)
(平成 13 年 6 月 19 日採録)

山根 信二（正会員）

昭和 44 年生．国際基督教大学教養学部卒業．CSK に勤務．平成 8 年東北大学大学院情報科学研究科人間社会情報科学専攻博士前期課程修了．平成 12 年東北大学大学院情報科学研究科人間社会情報科学専攻博士後期課程中退．修士（情報科学）．平成 12 年から岩手県立大学ソフトウェア情報学部コミュニケーション学研究室助手．コンピュータのリスクおよびネットワークセキュリティの研究に従事．CPSR，ACM，IEEE 各会員．

村山 優子（正会員）

津田塾大学学芸学部数学科卒業．三菱銀行および横河ヒューレット・パッカード社に勤務．昭和 59 年 University College London 大学院理学部計算機科学科修士課程修了．平成 2 年同大学院博士課程修了．Ph.D.（ロンドン大学）．慶應義塾大学環境情報学部非常勤講師を経て，平成 6 年 4 月より広島市立大学情報科学部情報工学科講師，平成 10 年 4 月より岩手県立大学ソフトウェア情報学部助教授．現在に至る．インターネット，ネットワークセキュリティの研究に従事．IEEE，ACM，電子情報通信学会，映像情報メディア学会，日本 OR 学会，情報知識学会各会員．