

6. インフォメーションハイディング の社会的側面

牧野京子 (株) 三菱総合研究所
makino@mri.co.jp

■インフォメーションハイディングの 歴史

本特集のここまでの記事では、画像、音声・音楽、ドキュメントといったデジタルコンテンツを対象としたさまざまなインフォメーションハイディングの技術的側面について述べてきた。本稿では少し視点を変えて、現実の社会生活においてインフォメーションハイディング技術がどのような場面で利用されてきたか、また社会生活の変化に伴いどのように変化してきたかといった点に注目し、インフォメーションハイディング技術の社会的側面といったものについて考えてみたいと思う。

現実の社会生活においてインフォメーションハイディング技術は、秘密のメッセージを第三者に気付かれないように相手に届けるということを目的に、メッセージを目に見えないインクで書いたり、秘密の場所にメッセージを書き込んだりという方法が古代ギリシャの時代から利用されてきた。前者について私たちに最も身近な方法としては「あぶりだし（炙り出し）」が挙げられる。後者については、ギリシャの歴史家 Herodotus によるペルシャ戦争の記述に示されている方法が歴史に残る最も古い方法として有名である。その方法は、信頼のおける奴隷の頭髪を剃ってその頭皮に秘密メッセージを入れ墨し、頭髪が生え揃ってから奴隷を使者として目的地に向かわせ、到着した時に頭髪を再び剃って、秘密メッセージを届けるといった方法である。

古代ペルシャ戦争の時代から近年に至るまで、インフォメーションハイディング技術は軍事や外交における機密情報の伝達手段として国家権力により独占的に利用されてきた。一般市民の社会生活におけるコミュニケーション手段として必要とされる状況は少なく、またその利

用環境の入手も困難なものであった。ところが、1980年代に入り金融業界における暗号の利用が開始され、またインターネットが普及するとともに、ネットワークを通じて伝達される情報に対するセキュリティ確保の必要性から、暗号技術、インフォメーションハイディング技術の利用が社会生活に密接にかかわりを持つようになり始めた。さらには、音楽、画像、映像などのデジタルコンテンツの利用技術、ハードウェアの進歩は、デジタルコンテンツの複製、交換といった操作を個人レベルの環境で容易に実現可能にした。これに伴い、デジタルコンテンツの著作権にかかわる問題が社会問題化し、1990年代後半になると著作権侵害抑止の有効な手段の1つとしてインフォメーションハイディング技術は関心を集めた。このような背景のもと、インフォメーションハイディング技術は、軍や外交での利用という限られた分野だけでなく、広く社会生活全般にかかわる利用技術として研究開発が進められるとともに、新たなビジネスの創出が期待される技術分野として注目を集め始めている。

■さまざまな局面での利用

ここでは、さまざまな分野におけるインフォメーションハイディング技術の利用場面をトピック的にとりあげることにより、インフォメーションハイディング技術が社会生活において重要な役割を担っていることを明らかにする。

◇軍事、外交

軍事や外交といった国防の観点において、機密情報の安全な伝達は至上命令である。これを実現するための手段としては、暗号化による機密情報の保護とインフォメ

ーションハイディング技術を利用した機密情報の秘匿といった2つの手段が存在するが、軍事、外交の分野においては、前者の方が重要視されていた時代が長く続いてきた。

また、この分野においては先に示したペルシャ戦争の時代から、第2次世界対戦、東西冷戦時代の諜報活動全盛時代までさまざまな技術の開発が行われている。その詳細については一般に明らかにされていないが、近年米国で開発されたものに「ステゴ・コミュニケーション・システム (Stego Communication System)」がある。1997年から2年間かけてU.S.Army 研究所 (ARL) と産業界、大学との共同研究により開発されたシステムであり、戦場での情報伝達のほか、送信された画像の改ざんチェックシステムとしても応用可能とされている。

最近最も「ステガノグラフィ」という言葉に注目を集めたトピックとしては、Osama bin Laden とアルカイダの間の情報伝達に「ステガノグラフィ」が利用されているという推測報道がある。eBay や Amazon といった一般の Web 上に掲載されている画像や音楽ファイルに秘密メッセージを埋め込んで、情報伝達に利用するというものである。これについては、ミシガン大学の研究者が、同サイトの200万枚にもおよぶ映像を調査した結果、ステガノグラフィの痕跡は発見されなかった。しかしながら、ステガノグラフィ技術に対する米国政府の危機感依然として強いものがあり、軍を中心にステゴ解析の研究が進められているが、その進捗状況については明らかにされていない。

◇言論 / 表現の自由の確保

インフォメーションハイディング技術は、権力による言論や表現の自由を管理しようとする政策に対抗する手段として利用される場面も多い。

暗号技術の利用が社会生活に浸透し、一般市民の利用が拡大すると、国家による暗号のコントロールを可能とする法律が施行され始めた。米国の鍵預託 (key escrow) イニシアティブや英国の RIP (Regulation of Investigatory Powers) 法がこれにあたる。前者は、暗号鍵のコピーを政府機関に預けることを義務付けることにより法執行機関や、国家諜報機関に便宜を与える法律¹⁾である。後者は市民が持っている暗号鍵でも警察が提出を要求する権限が認められ、これを拒否すると最大2年の刑が科せられるといった法律である。この RIP 法に対し、フリーソフト運動の提唱者である Richard Stallman は反対の意を表明するとともに、暗号鍵もしくは暗号化されたファイルを所持しているということで違法と判断されるような法律の対抗手段として、物理的なファイルの存在自体を隠すことが可能であるステガノグラフィ技術の個人での利用の必要性を強調している。

◇プライバシー保護

個人の情報が価値を有し、それを売買するビジネスが成り立つ社会においては、一般市民がプライバシーを自分自身で保護することが可能な仕組みを持っていることが、セキュリティの観点から重要である。

ネットワークの利用者にとって、電子メールは非常に重要な個人情報であるが、これを第三者の侵害から守る手段、プライバシー保護の手段として最も広く普及しているものに、Phil Zimmermann によって開発された電子メールの暗号ツールである PGP (Pretty Good Privacy) がある。しかしながら、メールの内容が暗号化されていても、メールの送受信時のトラフィック情報の解析や認証により、利用者を特定することは可能であり、暗号技術だけではプライバシー保護には限界がある。また、利用した暗号の強度によっては、暗号が解読されるといった危険性もないとはいえない。これらを補うための技術として、インフォメーションハイディング技術はプライバシー保護にとっても重要な技術である。

また、プライバシー保護の一部として、匿名性の確保も重要な課題である。電子投票、オンラインショッピング、Web 情報閲覧、企業における内部告発や密告、警察への通報、現政権への対抗勢力の活動など、社会生活において匿名性の確保が必要とされる場面は多数存在する。中でもネットワークを利用した電子投票についての匿名性の確保と改ざんの防止は重要である。日本においても投票時間の短縮や経費節減、投票率の向上が期待されて電子投票システムの導入が進みつつあるが、投票する有権者が本人であることが確認できた上で、投票内容を秘密にする、投票内容と有権者を結び付ける情報を残さないといった要求をどのように実現するかが課題であり、インフォメーションハイディング技術の応用が期待される分野である。

◇著作権保護

電子媒体が登場する以前においては、著作物をコピーする際に必要となる経費や時間、コピーすることにより発生する品質の劣化というものがあり、著作物の不正コピー、不正使用といった行為の抑止力となってきた。電子媒体が登場して経費や時間、品質の劣化といった問題が解消してからも、ファイルそのものの容量の大きさが不正コピーの抑止力となっていた。しかし昨今の MP3 に代表されるファイル圧縮技術の進展により、個人レベルの利用環境においても容易にファイルの入手、交換が可能な状況となってきた。これに伴い、著作権侵害に対するこれまでの抑止力は効力を失い、新たな抑止力、著作権管理のメカニズムが求められはじめていく。

	カバーデータの位置付け	エンベッドデータの内容	利用目的
ロバスト・ウォーターマーキング	カバーデータ自体が意味を持つ	著作権情報	著作権管理 著作権侵害抑止
フラジャイル・ウォーターマーキング	カバーデータ自体が意味を持つ	著作権情報	不正利用検知 改ざん検知
フィンガープリンティング	カバーデータ自体が意味を持つ	識別情報	配布（流通）経路追跡 不正利用抑止
ステガノグラフィ	カバーデータ自体は意味を持たない	秘匿情報自体	情報の存在自体の秘匿

表-1 インフォメーションハイディング技術の種類と特徴

■ビジネスへの展開

◇インフォメーションハイディング技術の用途

ここまで述べてきたようにインフォメーションハイディング技術は、一般市民の社会生活の基盤を支える技術として、さまざまな用途で利用されはじめており、その用途によりウォーターマーキング、フィンガープリンティング、ステガノグラフィの3種類の方法がある。ウォーターマーキングは、データに著作権情報を埋め込んでその不正利用を防止する技術で、編集操作や改ざん攻撃に対する耐性を持つロバスト・ウォーターマーキングと、耐性を持たない、編集操作や改ざん攻撃により簡単に無効化されてしまうフラジャイル・ウォーターマーキングの2種類の方法がある。前者はコンテンツに埋め込まれた著作権情報を保護することにより、著作権管理や不正コピーなどの著作権侵害の抑止を利用目的とし、後者は埋め込まれた著作権情報が編集操作や改ざん攻撃により無効化されることにより、不正利用や改ざんを検知することを目的とする。フィンガープリンティングはコンテンツに埋め込まれた識別情報により、配布（流通）経路の追跡を可能とする技術であり、ステガノグラフィは、秘匿したい情報そのものをコンテンツに埋め込むことにより、情報の存在自体を秘匿することを目的とする技術である。

また、インフォメーションハイディング技術の用途を考える時に重要なのが、カバーデータの位置付けの違いである。ウォーターマーキングおよびフィンガープリンティングはカバーデータ自体が意味を持つのに対し、ステガノグラフィは意味を持つのは埋め込まれた秘匿情報のみであり、カバーデータ自体は意味を持たない。以上4つの方法の特徴を表-1にまとめる。

ビジネスモデルを考える場合、用途のほかに先に示し

たような軍事／外交、言論／表現の自由の確保、プライバシー保護、著作権保護といった利用分野といった視点が必要となる。さらに、音楽、画像（静止画）、映像（動画）、ドキュメントといったカバーデータの対象となるメディアの種類も影響する。音楽、画像、映像を対象としたインフォメーションハイディング技術については、すでに研究開発段階から実用段階に入った技術といえる。ドキュメントを対象としたインフォメーションハイディング技術については、研究開発の段階ではあるが、書籍の著作権保護など実用化への期待は大きい。

◇ビジネスモデルの社会的背景

昨今では、インフォメーションハイディング技術のビジネスモデルとして、デジタルコンテンツの著作権の保護／管理、不正利用の抑止にウォーターマーキング技術を利用した著作権管理のビジネスモデルが、急速に注目を集め始めている。この背景には、ADSL等のブロードバンド・インターネットの普及、MP3を代表とするファイル圧縮技術の普及に伴い、デジタルコンテンツ配信ビジネスが本格化する反面、デジタルコンテンツの著作権侵害の問題が深刻化しているという状況がある。

「デジタルコンテンツ白書2002」（財団法人デジタルコンテンツ協会）によると、インターネットを始めとするネットワーク上でダウンロードまたはストリーミングの形態で流通する音楽および映像コンテンツの2001年の国内市場規模は、それぞれ348億円（前年比102.5%）、10億円（前年比146%）となっている。現段階では、本格的な市場形成までには至っていないが、ネットワークを利用した配信方法による新たなユーザの獲得に対する業界からの期待は大きい。また、コンテンツの作成者にとっても、この新たな配信方法は、中間媒体を介することなくコンテンツをユーザに直接提供する手段

として注目を集めている。しかしながら、この配信方法は、提供されるコンテンツの完全な複製が可能であり、購入後の操作について制限がないため、不正コピーや配布といった著作権侵害にかかわる問題が解決すべき課題となっている。現在実際に発生している著作権侵害の件数や被害の額について正確な数値を把握することは困難であるが、オークションサイトで出品されているソフトの90%が不正コピーによる海賊版であるとさえいわれている。また、ベリマトリックス・ジャパンの調査結果によると、2001年6月から12月までの6カ月間に違法音楽コンテンツを掲載しているサイトは30以上、被害の総額は73億円にのぼるといふ。

また、こういったデジタルコンテンツの著作権侵害の問題について広く世に知らしめるという意味で象徴的だったのが、米ナップスター社の訴訟問題である。ナップスター社は、自社のサーバを介してMP3の音楽ファイルを自由に交換することを可能にするサービスを無料で提供した。このサービスを利用すると著作権者に無断で不特定多数のユーザ間で音楽ファイルの交換が無料で行える。この点が問題となり、ナップスター社はデジタルコンテンツの著作権者側から著作権侵害にあたるとして起訴され、2001年2月にはこのサービスが著作権侵害にあたるとの判決が下されている。また、これとは別に第三者のサーバを介することなく、ファイルの交換を可能にしたヌーテラ (Gnutella)、モーフィアス (Morpheus)、カザー (KaZaA) といったファイル交換用のソフトも続々と登場している。これらのソフトについては、第三者のサーバを介していないため、利用者間の私的なファイル交換とみなすことが可能であり、著作権侵害にはならないとの判断もあり、今後大きな問題となる可能性がある。日本においても同様の問題は発生しており、1998年の8月から、日本音楽著作権協会 (JASRAC) や日本レコード協会など6団体が、著作権を有する音楽ファイルを無断で配信しているウェブサイトに対し、警告を行っている。

◇インフォメーションハイディング技術のビジネスモデル

こういった社会的背景により、著作権保護の問題が社会問題として広く一般市民に認識されるようになるとともに、著作権侵害の防止に対応したデジタルコンテンツ流通を可能にする新しいビジネスモデルが求められ始めている。

その1つとして特に注目を集めているのが、著作権管理 (DRM: Digital Rights Management) 技術である。DRM技術とは、デジタルコンテンツ自身にウォーターマーキングを利用して著作権情報を埋め込むことにより、デジタルコンテンツのセキュアな配信と、配

信されたコンテンツの不正利用の制御を実現する技術である。この技術は、デジタルコンテンツの暗号化を行う暗号化ツール、復号化および有効期限や利用制限 (保存、閲覧、編集、印刷等) に基づく制御を実現する専用のビューア、正規ユーザに配信されるライセンスを管理する仕組みから構成されており、デジタルコンテンツ配信における改ざん防止や著作権保護だけでなく、機密文書の漏洩防止にも適用が可能である。

2001年以降、複数のベンダがデジタルコンテンツの配信と著作権管理、利用制御の機能を実現する製品および著作権保護を含むデジタルコンテンツ配信サービスの提供が開始され始めている。

さらに著作権侵害防止の新たなビジネスとして、ウォーターマーキングと検索エンジンを利用して、インターネット上を自動的に巡回してデジタルコンテンツの著作権侵害を検出し、著作権所有者もしくはコンテンツの正規ユーザにメールなどで通知するサービスがある。コンテンツに著作権情報が埋め込まれていれば、そのコンテンツが著作権者の許可なく不正利用していると判断することが可能である。ここから先の不正利用者の特定や利用の停止、損害賠償の請求などは法律にゆだねられることとなるが、コンテンツに埋め込まれた著作権情報は、その際の証拠としての意味も大きい。しかしながら、インターネット上に公開された大量のデジタルコンテンツの中から、特定のウォーターマーキングが施されたコンテンツを追跡し、著作権者に支払うべき著作権使用料を回収するためには、膨大な時間とコストが必要となる。この点に注目し登場したのがこのサービスである。

以上2つの事例は、ロバスト・ウォーターマーキングであるが、フラジャイル・ウォーターマーキングを利用したビジネスモデルとしては、社内の機密文書や契約書、病院のカルテなど、特定の関係者以外の第三者への情報漏洩や改ざんが大きな損害をもたらすようなコンテンツに対し、ロバスト・ウォーターマーキングを利用して情報を埋め込み、情報の漏洩や改ざんを早期に検知する仕組みが考えられる。

また、フィンガープリンティングについては、配布されたコンテンツの不正利用が発覚した際に、埋め込まれた識別情報を抽出することにより流出元の特特定を可能にするという利用のほか、識別情報をバーコードの代替として利用するなど物流事業における製品管理の効率化を図るといった利用も今後の展開として考えられる。

◇ビジネスへの応用に必要とされる要件

ウォーターマーキングやフィンガープリンティングは、デジタルコンテンツの不正コピーや不正配布といった著作権侵害行為の抑止策として利用される。確かに

対象メディア	実施団体	概要
音楽 (SMF : Standard MIDI File)	(社) 音楽電子 事業協会 (AMEI)	SMF用の電子透かし埋め込みソフトウェア「MIDI Sign」とデータの権利管理情報を規定する「ISMC (International Standard MIDI Code) 規格」の運用を2001年12月号より開始。ISMC規格によりSMFにユニークなID番号 (ISMC番号) を付与し、そのID番号をMIDI Signによって電子透かしとして埋め込む方式。
音楽	日本音楽著作権 協会 (JASRAC)	2000年より音楽の著作権管理のための電子透かし技術の評価プロジェクトを開始。「利用可能な技術標準」の策定とその水準を満たす能力を有する技術 (企業) を選定。音楽電子透かし技術評価の国際的なガイドライン策定。
映像 (DVD)	CPTWG* ¹ VMW Group* ²	1997年より公募による標準化方式の選定作業開始。Galaxy技術とMillennium技術の統合化を目指し、現在もなお選定作業継続中。

*1 : Copy Protection Technical Working Group

*2 : Video Watermarking Group

表-2 標準化や評価基準の確立を目指す動き

抑止効果はあり、コンテンツの配信元にとっては、ウォーターマーキングは著作権侵害に対する損害賠償請求時の重要な証拠となり得るし、フィンガープリンティングはコンテンツの不正コピーや不正利用行為の犯人追跡に必要な情報を提供するため、保険としての意味合いを含め利用している場合もある。

しかしながら、ビジネスへの応用という観点で考えた場合重要となってくるのが、ウォーターマーキングやフィンガープリンティングを埋め込むコンテンツの商品的価値 (売上) とそれにかかるコスト (時間および費用) との経済的バランスの問題である。当然のことであるが、ビジネスにおいて前者が後者よりも大きいことが絶対条件となる。つまり、ビジネスへの応用に必要とされるの要件としては、これらに費やすコストと時間は保護するコンテンツの価格を超えてはならないのであり、費用対効果を考えた利用が重要である。

また、こういったインフォメーションハイディング技術を利用したビジネスが社会生活の中で浸透していくためには、技術に対する高い信頼性が求められる。これを実現するためには、インフォメーションハイディング技術を評価するための国際的な評価基準の確立や技術の標準化が不可欠である。インフォメーションハイディング技術の個別の技法については、一般に公開されることが少ないのが現状であるが、音楽、映像を対象としたウォーターマーキングを中心に標準化やその評価基準の確立を目指す動き (表-2 参照) も出始めている。

しかしながら、これらの活動はまだまだ始まったばかりであり、今後も技術開発と連携した活動が不可欠である。

■今後の展望

インフォメーションハイディング技術は、これを利用して情報を隠し伝える人間の立場やそれを取り巻く社会情勢の変化により、同じ技術が大きな効果や良い結果をもたらす可能性を持つ反面、多大な危険性をも併せ持つ可能性がある。たとえば、デジタルコンテンツにウォーターマーキングすることにより著作権保護の手段として有効に利用される反面、不正コピーしたデジタルコンテンツを他の媒体に埋め込んで隠す手段として利用することもできるのである。

インフォメーションハイディング技術は、常に情報を隠そうとする側とそれを破ろうとする側とのせめぎあいの状況である。インフォメーションハイディング技術が、強固な安全性を提供する成熟した技術として一般市民の生活に定着していくためには、新たな技術の開発とそれを破る技術 (ステゴ解析技術)、両者の継続的な研究開発の努力が重要である。

また、技術面だけでなく、標準化やその評価基準の確立といった面からの取り組みも、今後のインフォメーションハイディング技術を利用したビジネスの発展のために不可欠な要素である。

参考文献

- 1) Ross Anderson 著, トップスタジオ 訳: 情報セキュリティ技術大全, 日経 BP 社 (2002).
- 2) Scott Moskowitz 著, 坂本 仁 訳: 電子透かし, 小学館 (1999).
- 3) Cyber Law Japan : <http://www.law.co.jp>
- 4) DZNet : <http://www.dznet.co.jp>
- 5) デジタルコンテンツ白書 2002, (財) デジタルコンテンツ協会 (2002). (平成 15 年 2 月 10 日受付)

