# マルチメディア通信における動画による識閾下効果の問題定義*

村山 優子†
広島市立大学情報科学部‡

インターネットのような計算機網で, マルチメディア通信が実現される時, 従来のデータ, ソフトウェア, サービスプロセスなどのネットワーク資源への不正なアクセスの脅威などに加え, 画像や音声によるセキュリティの脅威が新たに存在するようになる. 本予稿では, 特に動画像における新しい脅威のひとつとしての識閾下効果の問題を考察し, 定義する. 画像情報におけるセキュリティの分野では, 現在, steganography とよばれる情報隠し技術がさかんに研究されている. これは, 画像情報の中にメッセージを気づかれないように挿入するなど情報の存在を隠す技術である. この他, 安全でない環境で, 他に気づかれずに情報を通信しあうための (Subliminal Channel) などを含めた covert channel と呼ばれる「隠れ通信路」などの概念において, 識閾下効果の問題が, どのような位置を占めるのかを明確にする.

## 1　まえがき

計算機網を代表するインターネットは, 80年代および90年代を通し, 爆発的な成長をとげてきたが, 90年代に入っての急激な伸びの主な要因は, その商業化に加え, 何といっても, その応用である Word-Wide Web (WWW)[8] の普及であろう. 80年代後半のインターネット研究者達の最大の関心事は, 果たして, どのような応用がインターネット基盤上に走ることを想定すれば良いかということであったが, WWW はまさに, その問いに対する解答である.

WWW は, もともと, データや文書など従来の計算機網で取り扱われてきたオブジェクトの共有を目指して作られたシステムであるが, 現在では, 画像や音声などを含むマルチメディアの情報システムとして機能している. 基盤のネットワークが高速になるにつれ, 映像情報も増えつつある. そのような環境下では, 今までの文字やソフトウェアなどのデータ転送を中心としていた網では, 経験のない, 新しい形の脅威が存在する.

本予稿では, そうしたマルチメディア通信の環境下における動画による識閾 (しきいき) 下効果の脅威を定義する.

興味深いことに, 心理学の分野において, 識閾 (しきいき) 下効果の有無は, 長年議論の対象であったが, ここ十年ほどの間に, この分野の研究は進み, 今では, 識閾下知覚 (Subliminal Perception) の存在は認識されている. 以下, 識閾下効果, インターネット上での脅威, そして識閾下効果攻撃と *belief* に沿って議論を進める.

## 2　識閾下知覚とその効果

識閾下とは, 英語の名称サブリミナル (Subliminal) で知られ, Sub(～の下) と Limen(識閾) から成る言葉である. 現在, 識閾について, 最も有名な定義は, Cheesman と Merikle[12] による主観的境界 (*subjective threshold*) といわれており, 以下のようである.

> *the detection level where subjects claim not to be able to discriminate perceptual information at better than chance level.*

被験者が偶然のレベル以上のところで, つまり自分の能力あるいは許容力の範囲を越えたところ

*The Problem Definition of a Threat from Subliminal Perception in Multimedia Communication

†Yuko Murayama
‡Faculty of Information Sciences, Hiroshima City University

では知覚した情報 (あるいはテストで察知することを求められている) を見分けられない検出基準である. すなわち, 偶然であれば情報を識別することはあるかもしれないけれども, そうでないときには必ず識別するとはかぎらないレベルのことをいう. 従って, 識閾下知覚とは, 上記のようなレベルで, ある刺激あるいは情報を被験者が識別してないが, 認知していることである.
彼らは, これに付随する客観的定義も以下のように与えている.

> *the level of detectability where perceptual information is actually discriminated at chance level.*

これは, 知覚された情報が, 偶然のレベルで, 実際に識別されることのできる検出基準という定義になるが, しかし, こうした客観性をだれに求めるのか, はっきりしない. 従って, 現在では, Subliminal Perception というよりも, 明らかに識別できる情報でも被験者自身が識別していないというものを含めた, Implicit Perception を主張する学者も多い [16].
Bornstein[10] によると, この分野の研究は, 以前のように識閾にこだわるモデル作りから, 現在のように, 信号検出 (signal detection) と情報処理 (information-processing) というアプローチに進んできているという.
心理学の分野では, 識閾下知覚や効果については, 長年, 議論の対象であった. 例えば, 20 年前, この分野の学者は, 小数派であった. しかし, 10 年前から, 研究が進み, 現在では, 主流派のひとつであるという. 医学系, 認知科学系, 社会学系の心理学者が, 情報交換をするようになり, 実験心理学の分野では, 識閾下知覚や効果の存在は認められるようになった. 現在は, それらのメカニズムの解明の研究がさかんにおこなわれている.
ただし, 実社会でこれらの効果が生まれるかどうかは, まだ, 議論の余地がある. なぜなら, 実生活の環境では, 様々な刺激が存在し, それらの複合作用がヒトに働くからである. 以前, 注目を集めた広告や宣伝目的の識閾下伝意 (Subliminal message)[15] は, 効果がないということがこの分野の研究者達の見解である.
他方, 心理学の実験などでは, 識閾下知覚に訴える手法が多く使われているという. 有名な例では, "MOMMY AND I ARE ONE" (MIO) というメッセージを挿入することで, 治療 (therapy) や教育環境では効果があるという [19][21]. これは, 大人に「小さい頃の母親」というやさしい保護者で栄養を与えてくれる存在と一体化したいという願いからだという. 本研究は動画環境だけにテーマを絞っているが, 同様なことが, 音声のメッセージについても存在する [23]. 心拍音と同様な音を, 耳に聞こえる限界より低いレベルで, メッセージの背景に加えると, メッセージの人間に与える影響力がより大きくなるといわれている. これは, 人に母親の胎内にいたときの安心できた状態の記憶を甦らせ, その負荷が論理的思考を司る大脳の左半球を満たし, メッセージの主張を無条件で受け入れやすい状態にするからであるという.
社会心理学者, Bargh[6] によると, 社会的な刺激のおよぼす影響の可能性を被験者が認識していると, 知覚した刺激や判断について偏見をもつようなことがなくなるという. 従って, 社会的な判断などにおける偏見, 特に人種や性についての偏見は, その判断について潜在的に影響するものが存在する可能性があることを認識していると, ヒトは影響されず, 認識していないと影響されるという.

## 3 インターネットにおける識閾下効果の脅威

前節のように, 現在では, 識閾下知覚や効果の影響が認識され, そのメカニズムが研究されつつある. その応用は今のところ実験室内であるが, 教育や治療にも使用されている. しかし, こうした応用に加え, 無差別対象へ偏見を与えるような悪用の可能性も考えられる. このようなことを直接意図したかどうかは不明だが, マスメディアでは, いくつかの使用例が報告されている. 例えば, ある教祖の写真をテレビ映像に挿入したり [1], また, 昨年公開されたある日本映画では, 97 分の映像の中に 38 カ所のサブリミナル的映像が使われていたという [2]. これらは 30 分の 1 秒のカットで, 映画の例では, 主人公がパラシュートで地上に降りる場面に, 女優の泣き顔が差し挟まれるなどしていた. 映画上映時には, あらかじめ観客にこのような映像部分が存在することを知らせていたが, その後, 衛星放送で放映される際に問題となり, サブリミナルの部分は取り除かれた.
現在までに報告されている応用例は, 単なる演出効果をねらったもので, 悪意が存在するとは言いがたい. しかし, いつ, そのような応用がされるかは, 予測できない.
テレビなどの伝統的なマスメディアの世界では, 各国で放送事業者の団体や政府機関を通して, 自主規制が促されている. それに対し, マルチメディア通信の基盤として機能しはじめたインターネット等の計算機網環境は, 誰でも平等に情

報を提供できる環境である．その特徴として，以下のようなことがあげられる．

- 情報提供者は必ずしも情報源ではない．
- 情報発信において，組織の階層構造が必ずしも反映されているとは限らない．
- 責任の所在の特定が難しい．

従って，インターネット上の情報の真偽の判断は受信者に任される．地球規模のインターネットは，自律システムの集合であり，統一的な法律では規制することは難しい．もちろん，検閲機構はない．従って，放送分野におけるような識閾下手法の規制は現在のところ不可能である．
また，インターネット上ではビデオ情報の他，アニメやゲームソフトに識閾下伝意が挿入される可能性もある．問題は，情報提供者が必ずしも識閾下伝意に気付いていないことにある．
インターネット上の映像は，WWW などの情報システムのユーザ・インターフェースを通じ，転送しながら見ることも可能であるが，現在のインターネットでは，網全体の速度が，発信元から宛先までの間のもっとも遅い部分網の速度となる．映像のユーザ・インターフェースの速度が，それに合わせて決まる場合，識閾下伝意のための画像部分が明確に視聴者に見えてしまうため，脅威とはならない．従って，網上の転送は，映像を実際に見ることとは独立に行なわれるという仮定を行なうか，あるいは，網が充分に高速であると仮定して，はじめて脅威となる．ATM 網など，網の高速化は進みつつあり，また，ビデオ・オン・デマンドの実用を目指すような計算機網環境では，このような仮定は必ずしも非現実的はない．

## 4 識閾下効果攻撃と *belief*

セキュリティには従来 2 種類の目的意識が存在した．秘密性と完全性の保持である．秘密性の保持とはある情報が発信者から受信者へ流れる時，それが，第三者へ漏洩しなようにすることであり，完全性の保持とは，情報が途中で改竄 (かいざん) されないようにすることである．
識閾下効果の脅威は，このようなセキュリティの枠組から考えると，完全性の問題といえる．しかし，それは，従来の完全性の定義とは異なり，実際に受信される情報が，『受信者が受信していると信じている情報』の他に，受信者が気づかない付加情報を含んでいることに起因している．情報が受信者にわたる前の第三者による改竄によるものかもしれないし，或は，もともと情報がそのようにつくられていた可能性もある．これは，従来のセキュリティ問題のひとつであるトロイの木馬問題 [4] と同等である．トロイの木馬問題とは，あるソフトウェアやサーバがそのユーザが期待する機能以外の動作を含むことであり，コンピュータウィルスもその一例である．これらはすべて，受信者側の受信した情報やオブジェクトについての *belief*(信じて疑わないこと) に基づく攻撃によるものである．
認証プロトコルの検証のための BAN ロジック [11] を用い，付加情報の発信者 ($A$) と受信者 ($B$) の情報あるいはオブジェクト ($X$) に対する *belief* をフォーマルに表すと次のようになる．ただし，$\alpha$ は付加された情報とする．

$$A \models (A \vdash (X + \alpha)), \text{ そして}$$
$$A \models (B \models (B \triangleleft X))$$

$$B \triangleleft (X + \alpha), \text{ しかし}$$
$$B \models (B \triangleleft X)$$

$A$ は自分が $X + \alpha$ を実際に発信したことを認識しており，$B$ が $X$ を受けとったと思い込むことを知っている．$B$ は自分が $X + \alpha$ を実際に受けとったのに，『$X$ を受けとった』と思い込んでいるのである．本来，BAN ロジックでは，

$$B \triangleleft (X + \alpha)$$

とした時，

$$B \models (B \triangleleft (X + \alpha))$$

の意味をもつので，今回のような *belief* 攻撃の問題については，表しにくい．

## 5 識閾下問題の位置付け

サブリミナル (Subliminal) という言葉は，セキュリティの分野では，G. Simmons が潜在通信路 (Subliminal Channel) について使用したものが最初である [20]．潜在通信路とは，例えば刑務所にいれられている者同士のように，直接通信が許されない 2 者が，第三者の検閲および転送の下，通信する場合，この第三者にその存在が知られないような通信路をこの二人の間に設けることである．これは Kahn により定義された古典的な Steganography[14] という，情報隠し (Information Hiding) 技術のひとつとみなせる[1]．

[1] 情報隠し技術は，暗号化技術とは異なる．前者は，情報の存在自体を気づかれないようにすることで，後者は情報内容を解読できないようにすることである．

現在, 画像の中に情報を埋め込む技術の研究が進みつつある. これは, 画像情報の中に何らかの形ですかし (watermark) を可視的あるいは一般には気付かれぬように挿入し, その画像情報の作者などを特定するために用いられるものである. これは, 悪用された場合に, 裁判などで, 知的所有権などを主張する目的のために使用するそうである [7]. これも, 可視的にしない場合 [9] は, 情報隠し技術のひとつとみなすことができる [5].

前節で述べたような トロイの木馬問題や本研究課題の識閾下効果問題は, 情報隠しの一例ととらえることもできるが, 情報受信者はその存在に気付かないという点で, 潜在通信路とは本質的に異なる.

しかし, これらはすべて, 隠れ通信路 (Covert Channel)[3][17] の一種とみなすことも可能である. 隠れ通信路とは, アクセス制御構造 [13][3] において, 異なるアクセスクラス間で, セキュリティ方針 (Security Policy) の一部であるアクセス制御方針 (Access Control Policy) に反するが, 実装では可能な情報の流れのことを意味する. しかし, 最近では, このアクセス制御構造やアクセスのクラスにこだわらず, 一般に認められていないにも関わらず, 実装上可能となる情報の流れをさす場合に使われる. この後者の広い定義から, *belief*(信じて疑わないこと) に基づく攻撃問題も, Steganography や潜在通信路も隠れ通信路のひとつと考えられる.

コンピュータウィルスには, 暗号化や認証の技術を応用したウィルス検知方式 [22] という情報提供者と情報自体の認証などの技術対策があり, トロイの木馬の脅威についてもサービスの認証 [18] などの対策がとられる. 識閾下伝意の場合, これらのような認証では解決できない. なぜなら, もとの情報自体が識閾下伝意を含んでいるかどうかが問題となるからである.

コンピュータウィルスの場合, 岡本 [22] によると, 社会的対策と技術的対策が併せて実施されなければならないとある. しかし, 地球規模のインターネットでは, その利用における規制について総意を取り付けることは不可能に近く, また, 中央管理されない構造であるため, 社会的対策は難しい. インターネットの中核となるインターネットのネットワーク層のサービスを提供するインターネット・サービス提供事業者 (ISP: Internet Service Provider) において, 情報レベルの対策を期待することも難しい. また, できたとしても, すべての ISP が行なうとは限らない. そうなると, インターネット全体の情報制御のレベルは, 最も弱い部分のレベルになってしまうので, 結局, 全体としての対策は難しい.

識閾下効果は, その応用の善悪の判断は受信者自身によって異なると思われる. しかし, 社会心理学者の Bargh の指摘するように, 識閾下伝意の存在や影響の可能性を知ることは, その心理的効果を起こすかどうかの重要な鍵となる. 従って, 受信者にとって, 最も必要なことは, その存在を知る手段を持つことであると思われる.

# 6 むすび

本稿では, 従来のマスメディアで古くから認識されてきた識閾下効果が, マルチメディア環境を提供するようになったインターネットに代表される計算機網において, 新しい脅威として存在するという問題を定義し, 考察した.

1960 年代後半, 米国の ARPANET から始まった計算機網環境は, 今やインターネットとして地球規模に発展してきた. 現在では, インターネットは単なる計算機網というより, マルチメディア情報システムとしてとらえることができる. 面白いことに, WWW などにみられるその応用は, 通信というよりは, より放送的で, マスメディアの様相を呈してきた. このような状況下では, マスメディアで使用される情報表現の手段が, インターネット上でも使用される可能性は否めない.

識閾下効果は, 心理学の分野では, 長年, 異端視されてきたが, ここ 10 年の間に, 様々な研究が進み, また, 医学系, 認知科学系, そして社会系のそれぞれの心理学者の交流が進んだこともあり, 主流の一派となった. 実験室レベルでは, この技術を使った手法が, 教育や治療のために使われている. 実社会での応用は, 今のところ未知数である. しかし, 放送業界などでの規制を見てもわかるように, 一般にこうした手法は, マスメディアの中では, 受信者に対し, 公正でないと理解されている. マスメデイア化の進むインターネットにおいて, これは重要な指針ではないだろうか.

社会心理学者によると, 識閾下伝意の存在や影響の可能性を知ることは, その心理的効果を起こすかどうかの重要な鍵となる. 受信者は少なくともその存在を確認できる手段を与えられるべきであろう. 計算機ネットワークの基盤上に作られるこれからの情報化社会では, 受信者の受信情報に対する *belief* を守る権利が保証されることも必要となろう.

今後, 検出手法を研究し, 検出システムおよび情報浄化機能などの製作に取り組みたい.

# References


[1] *The Mainichi Newspaper: Chugoku Region Version (in Japanese)*, pp. 27, June 1995.

[2] *The Asahi Newspaper (in Japanese)*, pp. 26, June 1995.

[3] M. D. Abrams, S. Jajodia, and H. J. Podell, editors. *Information Security: An Integrated Collection of Essays.* IEEE Computer Society Press, 1995. ISBN 0-8186-3662-9.

[4] J. P. Anderson. Computer security technology planning study. Report ESD-TR-73-51, Vols. I and II, HQ Electronic Systems Division, Hanscom AFB, MA, October 1972.

[5] R. Anderson. Redefining the limits of steganography. In *Proc. of Workshop of Information Hiding, Isaac Newton Institute, Univ. of Cambridge, 30 May - 1 June 1996.*

[6] J. A. Bargh. Does subliminality matter to social psychology? awareness of the stimulus versus awareness of its influence. *Perception Without Awareness: Cognitive, Clinical, and Social Perspectives*, pp. 236–255.

[7] H. Bergel. Protecting ownership rights through digital watermaking. *IEEE COMPUTER*, Vol. 29, No. 7, pp. 101–103, July 1996.

[8] T. Berners-Lee, R. Cailliau, A. Luotonen, H. F. Nielsen, and A. Secret. The world-wide web. *Communications of the ACM*, Vol. 37, No. 8, pp. 76–82, August 1994.

[9] F. M. Boland, J. J. K. O Ruanaidh, and C. Dautzenberg. Watermarking digital images for copyright protection. In *Conf. Proc.: Image Processing and Its Applications, 4-6 July 1995*, pp. 326–330. IEE.

[10] R. F. Bornstein and T. S. Pittman, editors. *Perception Without Awareness: Cognitive, Clinical, and Social Perspectives.* The Guildford Press, 1992.

[11] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. Technical Report 39, DEC Systems Research Center, February 1989.

[12] J. Cheesman and P. M. Merikle. Word recognition and consciousness. *Reading research: Advances in theory and practice*, Vol. 5, pp. 311–352, 1985.

[13] D. Denning. *Cryptography and Data Security.* Addison-Wesley Publishing Company, January 1983. ISBN0-201-10150-5.

[14] D. Kahn. *The Codebreakers.* Macmillan, 1967. ISBN 0025604600.

[15] W. B. Key. *Subliminal Seduction.* Prentice-Hall, 1973.

[16] J. F. Kihlstrom, T. M. Barnhardt, and D. J. Tataryn. Implicit perception. *Perception Without Awareness: Cognitive, Clinical, and Social Perspectives*, pp. 17–54.

[17] I. S. Moscowitz. Covert channels - here to stay? In *COMPASS '94: Proc. of the Nineth Annual Conference on Computer Assurance*, pp. 235–243, June 1994.

[18] J. M. Power and S. R. Wilbur. Authentication in a heterogeneous environment. *Computers & Security*, No. 6, pp. 41–48, 1987.

[19] L. H. Silverman and J. Weinberger. Mommy and i are one: Implications for psychotherapy. *American Psychologist*, Vol. 40, pp. 1296–1308, 1985.

[20] G. J. Simmons. The prisoners' problem and the subliminal channel. In *Advances in Cryptology: Proc. of Crypto 83*, pp. 51–67. Plenum Press, 1984.

[21] J. Weinberger. Validating and demystifying subliminal psychodynamic activation. *Perception Without*

*Awareness: Cognitive, Clinical, and Social Perspectives*, pp. 170–188.

[22] 岡本 栄司, 山田 忠直, 湯藤 典夫. 我が国におけるコンピュータウィルスの現状と対策. 情報処理学会誌, Vol. 33, No. 7, pp. 811–819, July 1992.

[23] 山田 尚勇. Vdt 使用の快適性に関する基礎研究に向けて. *Human Interface; News and Report*, Vol. 7, No. 2, pp. 313–328, May 1992.