マルチメディア通信と分散処理　90－2
コンピュータセキュリティ　2－2
（1998．9．17）

マルチメディア通信環境における識閾下伝意の脅威と対策

村山 優子　岩手県立大学
岡本 栄司　北陸先端科学技術大学院大学
柴田 義孝　岩手県立大学

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，特に動画像の通信における新しい脅威のひとつとして識閾下伝意の問題を提起する．識閾下伝意については，心理学の分野では，長年その効果の是非が議論されていたが，10年程前から，様々な領域の研究や交流が進み，その効果が認められるようになった．現在，実験心理学の分野では，治療や教育目的のため，このような手法が使用されている．本予稿では，さらに，この識閾下伝意の問題が，本質的にコンピュータ・ウィルスの問題と同等であることを示し，画像情報におけるセキュリティの分野である情報隠蔽技術 (steganography) や「隠れ通信路」(covert channel) 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し，対策について考察する．

A Threat in Multimedia Communications; Subliminal Messages

Yuko Murayama, Iwate Prefectural University
Eiji Okamoto, Japan Advanced Institute of Science and Technology
Yoshitaka Shibata, Iwate Prefectural University

We present an old threat to the mass media but novel in computer networks — subliminal messages. Although the issue had been somewhat controversial in the past, it turns out that during the past decade the advocate of perception without awareness has been in the mainstream of the research community of psychology, and research on how it works is in progress. Computer networks have been traditionally utilised to carry text and binary data. Multimedia communication has brought about the use of them to transport images and sound as well. The current applications indicate that the networks are functioning as a new type of the mass media, so have they come across a new type of threat. We explore the problem and claim that it is identical to computer virus in the sense that the information in question includes more than what a receiver is aware of. We show how the problem of subminal messages fits in the area of steganography and covert channels, and present ideas on solutions.

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)[6] 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[9] 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 [14].
Bornstein[8] 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)[13] 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 [17][19]. 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 [21]. 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[4] 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

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.
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, 情報の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. さらに、本質的な問題は受信者が被害に気づかない点である。

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 [2] 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.

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 [18]. 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[12] という, 情報隠し (Information Hiding) 技術のひとつとみなせる[1].
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 [5]. これも, 可視的にしない場合 [7] は, 情報隠し技術のひとつとみなすことができる [3].
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. これらはすべて, 隠れ通信路 (Covert Channel)[1][15] 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 [10][1] 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.

6 対策

6.1 概要

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 [20] 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 [16] 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.

[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.

コンピュータウィルスの場合, 岡本 [20] 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.
従って, 識閾下効果は, その応用の善悪の判断は受信者自身あるいは受信者保護のための代理エージェントに任せられるべきではないだろうか. そのため, 技術的対策としては, その存在を検出することが, 第一であろう. 付加部分を取り除くかどうかは, 受信者の判断に委ねるべきであると思われる.

6.2 検出方法

インターネットでは, マルチメディア情報のうち, 画像と音声が識閾下効果の攻撃の対象となろう. 以下では画像, 特に動画を対象と考える. ある時間δt 内に情報受信者が見る画像情報量 S は, t 時における 1 フレームの画像情報量を $I(t)$ とした時, 次のようになる:

$$S = \sum_{t=t_0}^{t_0+\delta t} I(t)$$

問題は, これらが視覚的に識閾下となりうる時に, 検出することである.
画像の場合, 検出には, ビデオ情報をそのまま, 一コマずつヒトが目で見て検査する方法もあるが, 情報の海と化したインターネットでは量的に無理であろう. 従って何らかの自動化がのぞまれる.
一案としては, MPEG[11][22] などの圧縮技術を利用することが考えられる. MPEG-1, MPEG-2どちらも, 各画面を, I(Intra coded) ピクチャ, P(Predictive coded) ピクチャ, B(Bidirectionally predictive coded) ピクチャのいずれかとして符号化する. I ピクチャは他画面と独立して符号化され, P ピクチャは前方向予測符号化で, 過去の I か P ピクチャをもと

にして予測符号化される. Bピクチャは双方向予測符号化で, 時間的に前後に位置するIかPピクチャをもとにして予測符号化される. 従って, 連続した前後の画面との差分を表すのはBピクチャである.
既に圧縮されたものを, そのまま検出対象には, できない. 現在の圧縮プログラムでは, 圧縮に際し, ピクチャの種類を決定するのは, ヒトであり, 例えば, 全てIピクチャで圧縮されていたら, 画面の差分はとれない. 従って, 検出システムは, 対象となる動画像情報を一旦復号化しながら, 例えば, 識閾下となりうるδt時間分の画面情報をIBB...Bのピクチャ順に指定して再圧縮し, 結果のBピクチャのデータ量の変化で検出は可能であろう. 動画像での真の識閾下効果は, 例えば毎秒一コマのメッセージが30分くらいの間, 繰り返されなければ効果が期待されないともいわれるので, このような部分検出をくりかえし, 同じメッセージが何度も繰り返された場合を見つけなければならないだろう. しかし, 部分検出により, 受信者はた識閾下効果の可能性を知ることができる. 後は, その部分がどのようなメッセージであるかを確認できる機会を受信者にあたえるべきであろう. 従って, 受信者には次のようなサービスが必要となる.

- 部分検出により画像情報が識閾下に受信される可能性のある情報を含んでいるかどうかを知らせる.
- それらの付加情報がどのようなものかを知らせる.

7 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, 検出手法をさらに検討し, 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] 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.

[2] 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.

[3] 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.*

[4] 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.

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

[6] 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.

[7] 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.

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

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

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

[11] D. L. Gall. Mpeg: A video compression standard for multimedia applications. *Communications of the ACM*, Vol. 34, No. 4, pp. 47–58, 1991.

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

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

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

[15] 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.

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

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

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

[19] J. Weinberger. Validating and demystifying subliminal psychodynamic activation. *Perception Without Awareness: Cognitive, Clinical, and Social Perspectives*, pp. 170–188.

[20] 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.

[21] 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.

[22] 村上仁巳. データ圧縮総論: ビデオデータ圧縮. テレビジョン学会誌： 画像情報工学と放送技術, Vol. 49, No. 4, pp. 416–421, 1995.