マルチメディア環境における セキュリティの脅威についての一考察*

村山 優子†
広島市立大学情報科学部‡

インターネットに代表される従来のコンピュータネットワークにおけるセキュリティの議論は，その構造の開放性 (openess) に起因する秘密性 (privacy) や，アドレス操作などによるネットワーク資源への不正なアクセスなどの脅威の対策が中心であった．80年代初頭のニューメデイアブームの後，光ファイバーなどの高速な媒体と圧縮技術の向上により，再び新しいメディアの時代として，マルチメディアのブームが到来している．インターネットにおいても，昨今のWWWのような情報システムや，遠隔会議などにより，このブームは着実に浸透している．こ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ネットワークでは，経験のない，新しい形の脅威が存在する．本論文では，そうしたマルチメディア通信の環境下で，今まで計算機ネットワークでは論じられていなかった識閾 (しきいき) 下効果による脅威について考察する．

1　まえがき

マルチメディアの旗印の下，放送，通信，計算機ネットワークの各分野の融合が様々な形で進んでいる [16]．こうした事態において，計算機ネットワークでは，今まで認識されずにいたセキュリティの脅威が存在する可能性がでてきた．本予稿では，そのような脅威のひとつである識閾下効果について考察する．

2　識閾下効果

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．仁科 [15] はサブリミナルを次のように定義している．

> 50%の確率で刺激の存在が知覚される強さ (liminal) より弱い (sub) 刺激水準のことで，ある人にははっきりと知覚されるが，ある人には全く存在に気付かれないという境界領域である．

こうした識閾下で受けとられた情報が人間の内部においてどのような影響を及ぼすかは1950年代以降様々な研究 [7][10][9] がおこなわれてきた．

識閾下効果は，以前，真偽のほどはともかく，米国での映画に挿入された識閾下伝意 (Subliminal message) による飲料の販売量の増加で話題となった．最近では，テレビ報道やアニメに挿入された画像で再び話題となったが，こうした動画における挿入以外にも使用されてきた．例えば，広告などの静止画に使用されている [6] ほか，自覚できない音声の挿入による識閾下伝意もある．例えば，山田 [12] によると，心拍音と同様な

*The First Thoughts on a Multimedia Security Threat
†Yuko Murayama
‡Faculty of Information Sciences, Hiroshima City University

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引き起こし，その負荷が論理的思考を司る大脳の左半球を飽和させ，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．

従って，この効果の応用は，マルチメディア環境において表現手段の一つと見て光ともなるが，知らされない情報受信として影ともなる [14].

3 識閾下伝意手法の規制

効果の有無はともかく，その可能性のある場合，放送分野では識閾下伝意手法は倫理的に問題があるとされる．我が国では，日本民間放送連盟が視覚による識閾下のメッセージを挿入しないよう自主規制を促し，米国でも連邦通信委員会が放送事業者に対し，免許人の義務に違反する旨の通達を出している．しかし，放送以外での広告や，音のメッセージでの応用については，他の表現手法と区別しにくいため，特別な規制はない．

いずれにしても，識閾下伝意が認識されていたマスメディアの世界では，情報提供者は，放送局や新聞社，出版社，広告代理店など，一般に責任の所在をあきらかにできる構造であった．しかし，インターネットに代表される計算機ネットワークが，マルチメディア環境を提供するようになると，事態はあきらかに変わってきた．

4 インターネットにおける識閾下効果の脅威

接続性重視のインターネット環境では，誰でも情報を提供でき，しかも，情報提供者は必ずしも情報源ではない．情報発信について，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インターネットでは，責任の所在の特定が難しい．インターネット上の情報の真偽は受信者が，判断しなければならない．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されない．検閲もない．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．

インターネットでは責任の所在が明らかでないことと，その地球規模にまで発展した現状を考え合わせると既存のマスメディアの環境に比べ識閾下手法の多発の可能性は大きい．また，ビデオ情報の他，比較的若年層が使用するとみられるアニメやゲームソフトに識閾下伝意が挿入された場合，社会的な脅威にもなりうるであろう．

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．これは，マスメディアの分野においても加入者分配網を提供するCATV事業者が同様の立場となる．しかし，CATVの場合，分配する情報源あるいは供給源を特定でき，責任の所在を明らかにできる．インターネットの場合，その情報がいつ誰により創られたかの特定が難しい．

5 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いささか異なる．識閾下効果の問題は，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．計算機や計算機ネットワークの分野では，これと同等な問題として，コンピュータウィルスやプログラムやサーバが期待されていること以外の動作を含むトロイの

木馬の脅威があげられる．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 [2] 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，α は付加された情報とする．

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

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

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* の問題については，やや表しにくい．

6 インターネットにおける対策についての考察

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 [11] 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 [8] 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．

コンピュータウィルスの場合，岡本 [11] 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．

対策には以下の 2 つのモデルが考えられる:

1. 検出機能を受信者あるいは代理エージェントに持たせる．

2. 検出を公証機関 (Certification Authority [3]) のような分散されたオーソリティ (あるインターネット地域で信頼されている機関) で行ない，情報 (X) に識閾下伝意が検出されたかどうかの情報 (r) を付加し，次のような証明書の形で発行する:

   $$\{X, r, T_S\}_{SK_S}$$

   すなわち，検証された情報とその結果がタイムスタンプがおされ，オーソリティの秘密鍵により暗号化される．

これら 2 つの方法は，併せて用いられるとよいであろう．検出機能のない受信者は，証明書つきの情報をもとめるか，なんらかの

サーバあるいは代理エージェントに検出サービスを依頼できる.

2の場合, 情報浄化 (information cleaning), すなわち, 付加された識閾下情報部分を取り除く機能をもつのもよい.

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[5][13] 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ろう.

- 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

本予稿では, 放送のようなマスメディア分野で長く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おいて新しい脅威として存在するという問題提起をした.

1960年代後半, 米国の ARPANET から始まった計算機ネットワーク環境は, 今やインターネットとして地球規模に発展した. 現在では, インターネットは単なる計算機ネットワークというより, 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, World-Wide-Web(WWW)[1] や Multicast Backbone(MBone)[4] 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.

このような状況で, 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. なかでも, 識閾下効果は, その応用の是非はともかく, 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ではないだろうか．本予稿では，そのためにも，識閾下効果の可能性のある情報の検出が第一に必要であることを説いた．

今後，検出手法をさらに研究し，検出システムおよび情報浄化機能の製作に取り組みたい．また，地域オーソリティ，或は，ある受信者グループのための代理エージェントなどのような分散された形の公証機関の研究も必要であろう．このようなオーソリティを利用するかしないかは，受信者が選択すればよい．オーソリティは要求された時にだけ，権威を表すという形で，真の分散処理体系が構築されるのだと思う．

References

[1] 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.

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

[3] CCITT and ISO. Recommendations x.500 series; the directory - x.509 (iso 9594-8) authentication framework;. International Standard X.509, March 1988.

[4] H. Eriksson. Mbone: The multicast backbone. *Communications of the ACM*, Vol. 37, No. 8, pp. 54–60, August 1994.

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

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

[7] R. S. Lazarus and R. A. McCleary. Automatic discrimination without awareness: A study of subception. *Psychological Review*, Vol. 58, pp. 113–122, 1951.

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

[9] M. Sagara, A. Tago, and Y. Shibuya. The influence of subliminal stimuli upon the impression of a line drawing of a face. *Japanese Psychological Research*, Vol. 4, No. 4, pp. 178–184, 1962.

[10] M. Sagara, S. Torii, and H. Katori. The influence of subliminal stimuli upon the judgement of distance. *Japanese Psychological Research*, Vol. 4, No. 2, pp. 58–64, 1962.

[11] 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.

[12] 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*, Vol. 7, pp. 313–328, 1992.

[13] 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.

[14] 白鳥 則郎. ポスト・モダン分散システム: Flexible computing. 情報処理学会誌, Vol. 36, No. 9, pp. 811–814, September 1995.

[15] 仁科 貞文. 『説得しない広告』の効果. 宣伝会議, Vol. 8, pp. 50–53, 1995.

[16] 日経ニューメディア別冊. 最前線レポート: 通信・放送融合へのシナリオ. 日経 BP 社, 1994. ISBN 4-8222-0877-X.