5. 暗号強度評価技術

松 井 充[†]

1. ま え が き

かつて暗号技術が軍事目的を中心として用いられていた時代には、暗号機器の内部構造は最も機密性の高い情報として、特定の資格者以外に詳細が明らかにされることはなかった。また暗号機器自体にも、その内部を第三者に容易に解析されることのないよう、構造上のさまざまな工夫がこらされていた。

しかしデジタル時代の到来によって、暗号技術はプライバシー保護の観点から注目され、その技術内容や安全性に関する議論も公の場で活発に行われるようになっていった。この流れを決定付けたのは、1977年に米国で標準化された商用標準暗号 DES (Data Encryption Standard) である¹⁾。

この暗号方式は、政府によってその仕様が完全に公開された点が画期的であった。当時、標準暗号制定の任にあたった米国商務省標準局は、暗号機器の互換性を実現するため、暗号アルゴリズムは公開とし、したがって通信の安全性は、送信者と受信者が秘密に共有する鍵のみによって実現することを目指したのであった。

オープンネットワークで利用可能な暗号は、不特定多数によって共有されるため、DESのようにたとえ暗号アルゴリズムが公開されても、鍵の秘匿性によって通信の安全性が保たなければならない。このような暗号方式は、近年の急激な通信網の広がりとともにますます必要とされている。

ところで、このことを暗号強度の立場からみると、強い暗号とは、第三者がそのアルゴリズムを知っていると仮定しても、通信路から得られた情報をもとに鍵を推定する（これを暗号解読者の暗号に対する攻撃と

呼ぶ）のに必要な情報量または計算量が充分大きいものでなければならない。この意味で暗号強度評価技術と暗号解読技術とは表裏をなしている。

1990年代に入って、DESをはじめとするブロック暗号と呼ばれるタイプの暗号化方式に対する新しい解読法がいくつか発見され、大きな話題となっている。これにともなう、これらの解読法に対する暗号強度指標や、この指標に基づいた安全な次世代暗号の設計指針が現在盛んに研究されている。

そこで本稿では、まず暗号解読に対する一般的な考え方を解説し、続いてブロック暗号に対する新しい解読法を概観するとともに、各解読法に対応する暗号強度指標がいかに構築されるかを、最新の結果を交えながら述べてみたい。

2. 暗号攻撃の分類

先に述べたように、暗号攻撃とは、解読者が暗号アルゴリズムを知っているとの条件で鍵を推定する試みである。その理論化のための前提条件として次の2つの(自然な)仮定をおくのが普通である。

- ・ 解読者は暗号文を自由に入手できる。
- ・ 暗号文は一定の鍵で暗号化されている。

以下、これらの条件は満たされていると仮定する。さて、暗号解読者は暗号文だけではなく、平文に関する何らかの情報も知っている想定するのが現実的である。そこでこの平文情報の種類によって、暗号攻撃を次のように分類する。

2.1 暗号文単独攻撃

これは、解読者は平文に関する何らかの統計的情報を持っているが、具体的な平文は知らないという条件での解読である。例えば日本語や英語などの自然言語は、統計的に偏りが大きい情報として知られている。したがって平文が自然言語であれば、解読者がその言語に関する統計情報を持っていることは、暗号解読の有力な手がかりになることがある。

ところで、平文が全くランダムな情報ならば、ある

[†] 三菱電機株式会社 情報技術総合研究所 情報セキュリティシステム開発センター

“How to Evaluate Strength of Block Ciphers” by Mitsuru Matsui (Information Technology R&D Center, Information Security System Development Center, Mitsubishi Electric Corporation, Kamakura)

図 1 バーナム暗号

いは、解読者が平文に関する情報を何も持っていないならば、暗号文単独攻撃はそもそも不可能であることに注意しよう。すなわちこの場合、暗号文を任意の鍵で復号した情報が正しい平文の候補であるということ以上は何もいえないからである。

この事実にもとづいた、暗号文単独攻撃に対して「絶対安全な」暗号が存在する。これは、平文と同じ長さの完全な乱数列をあらかじめ送信者と受信者で共有しておき、これを鍵として、与えられた平文と排他的論理和したものを暗号文とする方式である（図1）。この暗号はバーナム暗号と呼ばれ、暗号文単独攻撃の条件下では情報量的に解読することが不可能な暗号である。

バーナム暗号は、軍事・外交目的では現在も用いられているといわれるが、これを広域ネットワーク上で不特定多数が用いる暗号として利用するのは、次のような理由から困難である。

- ・平文と同じ長さの鍵をあらかじめ送信者と受信者が安全な通信路を用いて共有できると仮定するのは現実的でない。
- ・任意の長さの「完全な」乱数列を生成するのは困難である。

現実的な暗号とは、ある固定された長さの鍵を一度共有すれば、この鍵で大量のデータを暗号化しても安全性が（現実的な意味で）損なわれない方式である。したがって、ネットワークで用いられる暗号方式の強度評価を行う場合には、解読者は鍵の長さよりも充分長い暗号文、およびそれに対応する平文に関する情報を得ることができると仮定しなければならない。

2.2 既知平文攻撃

既知平文攻撃とは、解読者は与えられた暗号文と、対応する平文のペアを自由に入手できるとの条件で鍵を求める解読条件である。通信路から平文を得られるという条件は、例えば暗号アルゴリズムを認証通信に用いた時には、普通に起こりうることである。

図2は、秘密鍵暗号を用いた基本的な認証方法である。ここで確認者と証明者は、あらかじめ同じ暗号アルゴリズムと同じ鍵を共有しているとする。認証の目的は、証明者が確認者に対して、この鍵を直接送信す

図 2 秘密鍵暗号を用いた認証

ることなく、鍵を知っているという事実だけを相手に納得させることである。

認証のプロセスは以下の通りである。まず確認者は証明者に対して使い捨ての（擬似）乱数 R を送付する。これに対して証明者はこの乱数を平文として、自分の持っている鍵 K で暗号化し、その結果得られた C を確認者に送り返す。確認者は自分でこの乱数を暗号化することができるので、これが証明者から送り返されてきたものと一致するかどうかで証明者の正当性を確認できる。

ここで、確認者が使い捨ての乱数を用いる点は重要である。同じ乱数を2度使うと、前回の通信を盗聴していた第三者は、そのときの C を送り返すことにより、証明者になりすますことができるからである。

しかしながらこの認証方式の場合、第三者は通信路から平文 R と暗号文 C のペアを同時に得ることができる。したがって、通信の盗聴を続けていれば、 R が毎回変化するというまさにその理由で、平文と暗号文とペアをたくさん手に入れることができ、既知平文攻撃の環境が成立するのである。

またこれ以外にも、平文の一部が定型文書であるために、その内容が広く知られているということは充分あり得ることであり、このことから既知平文攻撃という環境はきわめて現実的な解読条件といえることができる。

2.3 選択平文攻撃

これは既知平文攻撃という条件の上に、さらに解読者が平文の内容を自由に指定できるという条件を持たせたものである。これに対し既知平文攻撃では、平文と暗号文のペアは与えられたものであり、解読者はその内容に干渉できないというのが前提であった。

したがって、選択平文攻撃は解読者にとってきわめて有利な条件といえるが、これも実際の通信では起こり得ることである。例えば、図2の認証通信において、確認者になりすました（そのようなことができるとして）第三者が、自分で自由に生成した R を乱数の代わりに証明者に送った場合、にせの確認者は正しい証明者から、対応する暗号文を自由に手に入れることができ、選択平文攻撃の環境が成立するのである。

表 1 解読者からみた暗号解読のための条件

	平文の入手	平文の生成
暗号文単独攻撃	×	×
既知平文攻撃	○	×
選択平文攻撃	○	○

表 1 は、本節で述べた暗号攻撃のための 3 つの環境を、解読者が得られる(あるいは操作できる)平文に関する条件の点から分類した。

3. 暗号解読法と暗号強度指標

暗号解読の効率をあらわすパラメータとは、すなわち暗号強度を示すパラメータであり、この意味で暗号解読と暗号強度評価はいわば表裏の関係にある。そこで本節では、秘密鍵暗号、特にブロック暗号を対象に、現在有力とされる 3 つの代表的暗号解読法を紹介しながら、その暗号強度指標をあわせて解説する。

3.1 全数探索法

(1) 全数探索法の概要

全数探索法とは、可能性のあるあらゆる鍵をひとつひとつ総当たりでチェックする方法であり、「総当たり法」あるいは「しらみつぶし解読」とも呼ばれている。具体的には、与えられた平文を各鍵候補で暗号化し、これが与えられた暗号文と一致するかどうかで正しい鍵を判別するものである。

したがって、これは基本的には既知平文攻撃であり、しかも平文と暗号文の組は 1 つしか必要でない。ただし、暗号文の数が多い場合には、暗号文単独攻撃にも用いることができる。この場合には、各鍵で復号した結果得られた情報の偏りが、あらかじめ解読者の知っている平文の偏りと一致するかどうかで正しい鍵を(確率的に)判別するのである。

このように、全数探索法は、解読者が取得すべき情報量が少ないという点と、解読者は暗号アルゴリズムの詳細を知らずとも、暗号装置さえあればこの解読が実行できる点で、きわめて現実的な解読法である。

例えば、最近の研究によれば、DES は 100 万ドル(人件費を除く)の超並列専用解読装置を作成すれば、全数探索法で数時間の計算で解読が可能と試算されている²⁾。この解読装置の実装には、電力消費や平均故障時間の見積もりなど、さらに考慮されなければならない点も多いが、全数探索法の効果的な実現法として大きな注目を集めている。

(2) 全数探索法に関する暗号強度指標

全数探索法に対する暗号強度は、単純に鍵の長さで

評価することができる。DES は 56 ビットの鍵が標準仕様であるが、上で述べたように、この長さは現在の技術水準から考えて、もはや安全とはいえないとされている。

また、いくつかの暗号で利用されている 64 ビットの鍵でも暗号学的には不十分とされることが多い³⁾。さらに今後 10~20 年の予想される技術進歩を考慮すると、これから設計される暗号は 100 ビット程度以上の鍵の長さが必要というのが研究者の一般的な見方である。

3.2 差分解読法

(1) 差分解読法の概要

差分解読法は、1990 年にイスラエルの暗号研究者 Biham と Shamir によって発表された選択平文攻撃である⁴⁾。これは、暗号アルゴリズムの内部構造を解析することによって実現する解読法であり、その原理は「平文の変化に対する暗号文の変化を統計的にとらえる」ものである。

より具体的には、解読者はあらかじめ平文 P の変化量 $\Delta P (\neq 0)$ と、暗号文 C の変化量 ΔC をそれぞれ固定し、次にランダムに与えた(数多くの)平文 P に対して次の確率を調べるのである。

$$DP(\Delta P \rightarrow \Delta C) \stackrel{\text{def}}{=} \text{Prob}_P\{F(P \oplus \Delta P) \oplus F(P) = \Delta C\} \quad (1)$$

ここで、 F は暗号化関数を表すものとする。この式の意味は、入力平文を ΔP だけ変化させたときに暗号文が ΔC だけ変化する確率である。もし F が理想的にランダムであるならば、どんな $\Delta P (\neq 0)$ や ΔC に対しても $DP(\Delta P \rightarrow \Delta C)$ は充分小さな値にならないなければならない。

しかしながら、アルゴリズムによってはこの値が大きくなるような ΔP と ΔC の組が見つかっており、このことが手がかりとなって、それまで解読不可能であったいくつかの暗号が解読されたのである。一般に差分解読法の成功に必要な平文と暗号文のペアの数は $DP(\Delta P \rightarrow \Delta C)$ の逆数に比例することが知られている。

DES に対する全数探索法よりも高速な解読法は、差分解読法によって初めて与えられた⁵⁾(ただし大量の選択平文と対応する暗号文の組が必要なため実際の通信路でこの解読条件が成立することは考えにくい)。なお、差分解読法は非常に多くの選択平文が与えられたという条件では、既知平文攻撃にも適用できることが知られているが、これも現実的ではないとされている。

(2) 差分解読法に関する暗号強度指標

このことを暗号強度の点からみてみると、暗号アルゴリズムの差分解読法に対する強度指標は次の値で与えられることが知られる。

$$DP_{max} \stackrel{\text{def}}{=} \max_{\Delta P \neq 0, \Delta C} DP(\Delta P \rightarrow \Delta C) \quad (2)$$

ところが一般に、与えられた暗号アルゴリズムに対して、この DP_{max} の値を正確に求めるのは、膨大な計算が必要のため大変難しいとされている。このため、実用となっているほとんどの暗号アルゴリズムで、この値は知られていない。

そこで、これを求めるかわりに暗号アルゴリズム $C = F(P)$ を、より小さい部分関数 $F_1, F_2, F_3, \dots$ を用いて $C = F_n(\dots(F_2(F_1(P))))$ という形に分解し、 $DP(\Delta P \rightarrow \Delta C)$ や DP_{max} の代わりに次の値を差分解読法に関する強度指標とするのが一般的である。

$$DP'(\Delta P_1 \rightarrow \Delta P_2 \rightarrow \dots \Delta P_{n+1}) \stackrel{\text{def}}{=} \prod_{i=1}^n \text{Prob}_{P_i} \{F_i(P_i \oplus \Delta P_i) \oplus F_i(P_i) = \Delta P_{i+1}\} \quad (3)$$

$$DP'_{max} \stackrel{\text{def}}{=} \max DP'(\Delta P_1 \rightarrow \Delta P_2 \rightarrow \dots \Delta P_{n+1}) \quad (4)$$

ここで、 P_i は平文 P を、 $P_{i+1} (1 \leq i \leq n-1)$ は $F_i(P_i)$ を、 P_{n+1} は暗号文 C を表すものとする。また上記最大値は、 $\Delta P_i \neq 0$ を満足するすべての $\Delta P_1, \Delta P_2, \dots, \Delta P_{n+1}$ をわたるものとする (図3)。

Biham と Shamir が DES に対して初めて差分解読法を与えた時も、正確には $DP'(\Delta P_1 \rightarrow \Delta P_2 \rightarrow \dots \Delta P_{n+1})$ の値が大きくなるような ΔP_i の具体例を与えたのであった。

一般に DP'_{max} の具体的な値を求めることも、計算量的に容易ではないが、最近、筆者によってこの値の

図3 n段ブロック暗号アルゴリズム

効率的な計算法が与えられ、例えば DES についてはこの値が確定し、Biham と Shamir によって与えられた値が、真の DP'_{max} であることが証明された⁶⁾。これに対し、 DP'_{max} の正確な値が知られていないブロック暗号も数多く、重要な研究テーマとなっている。

3.3 線形解読法

(1) 線形解読法の概要

これに対し線形解読法は、1993 年、筆者によって与えられた解読法で、原理的に既知平文攻撃法であるという特徴を持っている⁷⁾。これも差分解読法と同じく、暗号アルゴリズムの内部構造を解析することによって実現する解読法であり、その原理は「平文と暗号文のビット相関関係を統計的にとらえる」ものである。

より具体的には、解読者はあらかじめ平文 P のマスク値 IP と暗号文 C のマスク値 $IC (\neq 0)$ をそれぞれ固定し、次にランダムに与えた (数多くの) 平文 P に対して次の確率を調べるのである。

$$LP(IC \rightarrow IP) \stackrel{\text{def}}{=} |2 \text{Prob}_P \{P \bullet IP = (C \bullet IC)\} - 1|^2 \quad (5)$$

ここで $\bullet$ は、ビットごとの論理和をとった値のパリティ (0 または 1) を示している。この式の意味は、入力平文のうち IP で指定されたビットのパリティが、暗号文のうち IC で指定されたビットのパリティと一致する確率の、 $1/2$ からの偏り (の自乗) というのである。

もし暗号化関数 F が理想的にランダムであるならば、どんな IP や $IC (\neq 0)$ に対しても $LP(IC \rightarrow IP)$ は小さな値にならなければならない。

しかしながら、アルゴリズムによってはこの値が大きくなるような IP と IC の組が見つかっており、このことを手掛かりに、それまで解読不可能とされてきたいくつかの暗号が解読されたのである。一般に、線形解読法の成功に必要な平文と暗号文のペアの数は $LP(IC \rightarrow IP)$ の逆数に比例することが知られている。

例えば、DES に対する初めての計算機による解読実験は線形解読法によって与えられた⁸⁾ (ただし、大量の既知平文と対応する暗号文の組が必要であり、実際の通信路でこのような解読条件が成立することは現状では考えにくい)。なお、線形解読法は暗号文単独攻撃にも利用できることが知られている。

(2) 線形解読法に関する暗号強度指標

このことを暗号強度の点から見てみると、暗号アル

ゴリズムの線形解読法に対する強度指標は次の値で与えられることが知られる。

$$LP_{max} \stackrel{\text{def}}{=} \max_{\Gamma C \neq 0, \Gamma P} LP(\Gamma C \rightarrow \Gamma P) \quad (6)$$

ところが一般に、与えられた暗号アルゴリズムに対して、この LP_{max} の値を正確に求めるのは、膨大な計算が必要なため大変難しいとされている。このため、実用となっているほとんどの暗号アルゴリズムで、この値はいまだに知られていない。

そこで、これを求めるかわりに暗号アルゴリズム $C=F(P)$ を、より小さい部分関数 $F_1, F_2, F_3, \dots$ を用いて $C=F_n(\dots(F_2(F_1(P))))$ という形に分解し、 $LP(\Gamma C \rightarrow \Gamma P)$ や LP_{max} の代わりに次の値を強度指標とするのが一般的である。

$$LP'(\Gamma P_{n+1} \rightarrow \Gamma P_n \rightarrow \Gamma P_1) \stackrel{\text{def}}{=} \prod_{i=1}^n |2 \text{Prob}\{(P_i \bullet \Gamma P_i) = (P_{i+1} \bullet \Gamma P_{i+1})\} - 1|^2 \quad (7)$$

$$LP'_{max} \stackrel{\text{def}}{=} \max LP'(\Gamma P_{n+1} \rightarrow \Gamma P_n \rightarrow \dots \Gamma P_1) \quad (8)$$

ここで、 P_i は平文 P を、 $P_{i+1} (1 \leq i \leq n-1)$ は $F_i(P_i)$ を、 P_{n+1} は暗号文 C を表すものとする。また上記最大値は、 $\Gamma P_{n+1} \neq 0$ を満足するすべての $\Gamma P_1, \Gamma P_2, \dots, \Gamma P_{n+1}$ をわたるものとする。

筆者が DES に対して初めて差分解読法を与えた時も、正確には $LP'(\Gamma P_{n+1} \rightarrow \Gamma P_n \rightarrow \dots \Gamma P_1)$ の値が大きくなるような ΓP_i の例を与えたのであった。

一般に、 LP'_{max} の具体的な値を求めることも、 DP'_{max} 同様、計算量的に容易ではないが、文献⁶⁾によってこの値の効率的な計算法が与えられ、例えば、DES についてはこの値が確定した。これに対し、 LP'_{max} の正確な値がまだ知られていないブロック暗号も多く、これは重要な研究テーマとなっている。

4. 暗号強度評価の例

ここでは、前節で述べた差分解読法に関する強度指標 DP'_{max} および線形解読法に関する強度指標 LP'_{max} を用いた暗号強度の実例を示す。

図4および図5は、DES について DP'_{max} および LP'_{max} の値を示したものである。ここで横軸はアルゴリズムの段数を表している。すなわち DES の標準仕様は 16 段であるが（前節の $F_1, F_2, \dots$ をそれぞれ 1 段と考えている）、この段数を減少させた “reduced DES” に対しても DP'_{max} および LP'_{max} の値をプロットしものである。縦軸はこの確率を 2 を底とする対数で表示している。

図4 差分解読法に基づく DES の暗号強度

図5 線形解読法に基づく DES の暗号強度

この表から、DES 暗号のデータのランダム化の傾向を読み取ることができる。さらにこのグラフに、他のアルゴリズムの DP'_{max} や LP'_{max} の値を重ねることによって暗号強度の相対的な比較ができるのである。

5. む す び

ブロック暗号の暗号解読技術や強度評価技術は、暗号学のなかでも急速に発展している分野である。DES にかわる新しい標準となるべき暗号方式が望まれるなか、新しい特徴を持ったブロック暗号の提案も盛んであり、暗号強度評価技術は、これらの性能評価のための重要な手段を与えている。

暗号の性能は強度だけではなく、その実用性のためには大きさや速度も評価されなければならない。今後これらを全体的にとらえる「暗号総合性能指標」の確立が重要な課題となるであろう。

(1992年2月28日受付)

〔参 考 文 献〕

- 1) National Bureau of Standard, "Data Encryption Standard", Federal Information Processing Standards, No. 46, U. S. Department of Commerce (1987)
- 2) M. J. Wiener: "Efficient DES Key Search", Presented at the Rump Session of CRYPTO '93 (1993)
- 3) B. Schneier: "Applied Cryptography", John Wiley & Sons Inc. (1994)
- 4) E. Biham, A. Shamir: "Differential Cryptanalysis of DES-like Cryptosystems", Proceedings of CRYPTO '90—Advances in Cryptology, Lecture Notes in Computer Science, Vol. 537, Springer Verlag (1990)
- 5) E. Biham, A. Shamir: "Differential Cryptanalysis of the full 16-round DES", Proceedings of CRYPTO '92—Advances in Cryptology, Lecture Notes in Computer Science, Vol. 740, Springer Verlag (1992)
- 6) M. Matsui: "On Correlation Between the Order of S-boxes and the Strength of DES", Proceedings of Euro-

crypt '94—Advances in Cryptology, Lecture Notes in Computer Science, Springer Verlag (to appear)

- 7) M. Matsui: "Linear Cryptanalysis Method for DES", Proceedings of Eurocrypt '94—Advances in Cryptology, Lecture Notes in Computer Science, Vol. 765, Springer Verlag (1993)
- 8) M. Matsui: "The First Experimental Cryptanalysis of the Data Encryption Standard", Proceedings of CRYPTO '94—Advances in Cryptology, Lecture Notes in Computer Science, Vol. 839, Springer Verlag (1994)

まつい みつひろ
松井 充 昭和55年、京都大学理学部卒業。昭和57年、同大学院修士課程数学専攻修了。同年、三菱電機(株)入社。以来、符号理論、暗号理論の研究開発に従事。

1996年1月号「学会誌第50巻第1号を迎えて」記念特集/「デジタルテレビ放送」小特集予定目次

【ふ お か す】	東京理科大 宇都宮敏男
【記 念 特 集】	学会誌発展の経緯をたどる編集長 元木紀雄
【小 特 集】	1. デジタル放送サービスのイメージ.....郵政省 安成知文
	2. デジタル放送の技術と動向東 芝 仁尾浩一, 通信総研 都竹愛一郎, NHK 松村 肇, NHK 河合直樹, 東 芝 平川秀治
	3. 欧州における技術動向.....フジテレビ 上瀬千春
	4. アメリカの動向NHK 久保田啓一
	5. 日本のCSデジタル放送実験と事業計画日立 中川一二夫, フジテレビ 上瀬千春, 上瀬千春, ISAT 橋本和彦
【講 座】	(複雑性への挑戦開講にあたって)編集理事 中嶋正之
	複雑性への挑戦 (第1回): 複雑性の科学東工大 北原和夫
【てれび・さろん】	国際交流ノート (第21回): 私の国際交流ノート(18) —— 国際? 日本と外国 ——カーネギーメロン大 金出武雄
【論 文】	VTRにおけるデジタルFM信号処理方式の検討三菱電機 畠中恵司・白崎義之・藤原直久・渡部美代一・川辺貞信
	領域分割による動画像のカット点検出法.....北 大 水野 哲・長谷山美紀・北島秀夫
	DC型PDPの寿命特性に関する研究——ネオンオレンジタイプ——岡谷電機 渡辺 聡・中島文男, 電機大 金田輝男
	アルカリ土類金属—希土類元素複合酸化物粉末のAC-PDP印刷保護膜への適用沖電気 小岩一郎・金原隆雄・見田充郎
	高速Hough変換と実時間形状計測を応用した矩形物体の検査久留米高専 中島勝行・大淵 豊, 阪 大 井上勝敬
	帯域削減スペクトル拡散方式による周波数帯域の有効利用.....豊田工大 杉浦彰彦・稲津 稔
	ホログラフィック光学素子を用いたリアルタイム3次元ディスプレイ大阪市立大 阪本邦夫・高橋秀也・志水英二, イメージ情報科学研究所 上田裕昭
【これすばんでんす】	画像符号化装置の一評価法に関する検討.....東工大 西方敦博・坂口千明・中山 実・清水康敏
	デジタルHDTVシステムの高効率圧縮符号化およびブロック歪みの改善天津大 李 桂苓・赵 康・元木紀雄
【研 究 速 報】	ポインティング知覚における指差し情報と視線情報による正答率ATR 宮里 勉・岸野文郎
【会 議 レ ポ ー ト】	第32回民放技術報告会東京放送 宮澤俊二
	第40回MMM'95国際会議NHK 宮下英一
	SMPTE会議報告NHK 中須英輔
	Workshop on HDTV (台湾)NHK 加井謙二郎
	世界無線通信会議WRC-95報告東京放送 荒井清実