4. 最近のセキュリティ技術とその応用

4-1 放 送

正会員 難 波 誠 一[†]

1. ま え が き

放送分野でのセキュリティ技術の中心となるスクランブル放送は、古くはCATV等で用いられていたが、衛星の登場で大規模なスクランブル放送が世界的に行われるようになった。我が国では放送衛星によるスクランブル放送が開始されてからほぼ2年が経ち、1992年からは通信衛星でもテレビや音声（多チャンネルPCM音声放送）のスクランブル放送が行われている。海外では主にヨーロッパで放送衛星や通信衛星を用いた放送が盛んに行われるようになり、これらでは種々のスクランブル技術が使われている。

スクランブル放送は、契約した受信機以外では視聴できないように信号をスクランブルする技術と、受信機でデスクランブルを行うための情報を安全に伝送し処理する技術とで実現される（これらを総称してコンディショナルアクセス（限定受信）技術と呼ぶ）。本稿では、これらの技術の最近の動向をまとめることとする。

2. スクランブル放送の動向

2.1. 我が国における動向

スクランブル放送には種々の目的があるが¹⁾、多くは有料放送を行うため、すなわち、放送を受信する人から直接かつ確実に料金を得るための技術手段として用いられる。我が国では表1に示したような種々の放送サービスの有料方式が電気通信技術審議会で審議され、順次答申、省令化されている。有料方式を実用化するには、安全性とコストの点からIC化が不可欠であるが、放送衛星のテレビ有料方式²⁾についてはCOATEC研究所で方式の細部を定め、IC化が行われ

た。このため、一般にCOATEC方式と呼ばれている。

通信衛星（CS）では、CATVのヘッドエンドに向けての番組配信や企業内通信等にスクランブルをかけたテレビ伝送が行われていたが、放送法が改正され、一般の受信者へ向けての放送サービスができるようになった。このCS放送はスクランブルが行えることが条件となっており、テレビ放送用の有料方式としては表1のように5種類（テレビ信号方式は3種類）が定められた³⁾。ただし、1992年から開始された放送では、BSと同じCOATEC方式と、通信用に使用されてきたいわゆるスカイポート方式の2種類が使用されている。

2.2 海外における動向

アメリカにおいては、従来からCATVが非常に発達しており、直接衛星放送は未発達である。このCATVのヘッドエンド向けの通信衛星の電波が直接受信されることへの対策としてスクランブルが行われているが、この方式にはビデオサイファ方式が多く用いられている。

一方、ヨーロッパでは、衛星放送、地上放送を含め多くのスクランブル放送が開発され、実施されている³⁾。海外の代表的な方式を表2に示す。

3. スクランブル放送のシステム構成

スクランブル放送のシステムは、信号をスクランブルするサブシステムと、デスクランブルを行うために必要な情報（我が国の方式では関連情報と呼ばれる）を処理するサブシステムとで構成される。CCIRにおける放送用の限定受信方式に関する勧告では、図1のような構成として一般的に表現されている⁴⁾。以下に各サブシステムに関する最近の動向について述べる。

4. 放送に使用される信号スクランブル技術

4.1 テレビジョン、ハイビジョン（映像）

テレビでは映像と音声がスクランブルされるが、片

[†] NHK放送技術研究所

“Recent Security Techniques and Their Application; Broadcasting” by Seichi Namba (NHK Science and Technical Research Laboratories, Tokyo)

表 1 我が国の放送用有料方式の概要

放送サービス	方 式	スクランブル方式	電通技審 答申	使用している放送事業者（有料放送開始）
テレビジョン	BS	[COATEC 方式] 映像：LR, LP, LR+LP 音声：PN 信号加算	1988.11	日本衛星放送 (JSB) (1991.4)
	CS	BS 準拠方式 [COATEC 方式]	1990.11	スペースシャワー(1992.10), ジャパンスポーツチャンネル(1992.10), 衛星映画演劇放送(1993.4 予定)
		〃 [M 方式]		(通信で使用)
		〃 [スカイポート方式]		日本ケーブルテレビジョン(CNN)(1992.5), ミュージックチャンネル(1992.12), スターチャンネル(1992.5)
		B-NTSC 方式 [ビデオサイファー]		(通信で使用)
		B-MAC 方式		(通信で使用)
ハイビジョン	BS	[COATEC 方式] 映像：LR, LP, LR+LP 音声：PN 信号加算	1990.6	なし
独立音声放送	BS	[COATEC 方式] PN 信号加算	1988.11	衛星デジタル音楽放送(SDAB)(1991.9)
多チャンネル PCM 音声放 送	CS	[COATEC 方式] PN 信号加算	1990.1	PCM ジパング(1992.12), ニッポンミュージックコンGRESS(1992.12), ミュージックパード(1993.6 予定), サテライトミュージック(1993.6 予定), PCM ジャパン(1993.6 予定), PCM セントラル(1992.12)
ファクシミリ 放送	地上 波	PN 信号加算+換字変換+スクランブル鍵による演算	1990.9	なし
衛星データ放 送	BS	審議中(PN 信号加算方式, 暗号方式)	審議中	

BS：放送衛星による放送, CS：通信衛星による放送, LR：ラインローテーション, LP：ラインパーミュテーション

図 1 限定受信システムの構成

表 2 海外の主なテレビジョン用限定受信方式

方式名	映像信号		音声信号		関連情報 伝送	セキュリティ モジュール	使用例
	信号方式	スクランブル方式	信号方式	スクランブル方式			
Eurocrypt	MAC/ パケット	LR	デジタル	PN信号加算	パケット	CPU内蔵IC カード	カナルプルス (TDF 衛星), フランステレコム (ケーブル) 等
VideoCrypt	PAL	LR	アナログ	なし	VBI, スマ ートカード	CPU内蔵IC カード	BskyB のスカイテレビジョン (アストラ衛星)
VideoCrypt S	PAL	LP	アナログ	スペクトル 反転	VBI, スマ ートカード	CPU内蔵IC カード	BBC Select (地上波)
VideoCypher	B-NTSC	極性反転	デジタル	PN信号加算	VBI	埋め込みモジ ュール	CATV 向け番組配信 (アメリカ通信衛星)
EuroCipher	D-MAC/ パケット	LR	デジタル	PN信号加算	パケット	VideoCipher に同じ	BskyB (マルコポーロ衛星)
Discret	SECAM 等	ラインシフト	アナログ	スペクトル 反転	VBI	埋め込みモジ ュール	カナルプルス(フランス)(地上)
Nagravision	SECAM 等	LP	アナログ	スペクトル 反転	VBI	CPU内蔵鍵型 モジュール	カナルプルス(スペイン)(地上)他 カナルプルス(フランス)(地上, 予定)
B-MAC	B-MAC	ライントラン スレーション	デジタル	PN信号加算 +多重位置	VBI	埋め込みモジ ュール	(通信衛星)

LR：ラインローテーション方式，LP：ラインパーミュテーション方式，VBI：垂直帰線期間多重

方のスクランブルで実用されている例もある。放送用のスクランブルでは、信号を完全に秘匿すると故障と区別しにくいこと、若干内容がわかる方が加入促進に効果があることなどから、内容が楽しめない程度であれば充分なことが多い。すなわち放送では、内容の秘匿性よりも品質が劣化しないことが重要である。

映像信号のスクランブルは、大きく同期信号部分の処理と有効映像信号部分の処理に分けて考えることができる。さらに、それぞれ振幅方向の処理と時間方向の処理が可能であり、これらを単独あるいは組合せて実用されている。このような観点で映像スクランブル方式をまとめてみると表 3 のようになる。

(1) 同期信号によるスクランブル

同期信号の振幅方向のスクランブル、すなわち同期信号の抑圧、あるいは振幅をランダムに変える方式は、主に CATV で用いられている。なお、同期抑圧は CS テレビ放送では、平均の変調度を上げ、小電力の衛星での伝送特性を改善する目的でも用いられる。

同期信号の時間位置をずらす方式には、表 2 の Discret や CS 放送用の一方式である B-MAC のライントランスレーション方式(走査線変移方式)がある。前者は、各走査線の同期信号の時間範囲内で同期信号の位置を前後させるもので、変化範囲も少なく、画像内容がかなりわかる方式である。一方、B-MAC の方式は、各走査線に時分割で送られる音声・データ信号の時間幅を変える方式であり、時間変動幅は数ライン

分累積されるので、画面内容は全くわからない状態になる。この方式は有効画面部分の伝送順序が保たれるので、伝送路の特性等による復元画質の劣化が少ない利点がある。

(2) 極性反転方式

映像信号の極性反転方式は、伝送路の振幅特性に非直線性があると正しいレベルに復元できず、走査線やフィールドごとに反転すると復元画面に雑音やフリッカを生じる。このため、ビデオサイファア方式等では、完全に極性を反転する方式が用いられている(ただし、安全性の点から他のスクランブル方式と併用される)。

(3) ラインローテーション方式

ラインローテーション方式(走査線内信号切替方式)は、各走査線の中にカットポイントを設け、その前後を入れ替えるもので、画面が水平方向に乱される方式である。走査線ごとにカットポイントの位置をランダムに変えることにより、高い秘匿性と安全性が得られる。この方式は処理に必要なラインメモリの量が少なく、コスト的にも有利であることから、表 2 のように種々の方式のテレビ信号に適用され、日本衛星放送(JSB)を初め、衛星放送用のスクランブル方式として広く実用されている。ただし、伝送路の特性により復元信号の接続点付近に劣化を生じやすいので、伝送される有効画面部分の前後に付加サンプルが設けられる²⁾。また、この方式はカットポイントの位置を制限

表 3 映像スクランブル方式の分類と適用例

		映像信号によるスクランブル			
		な し	明るさ方向	時 間 方 向	
				水平方向	垂直方向
			極性反転方式	ラインローテーション方式	ラインパーミュテーション方式
同期信号によるスクランブル	な し	スクランブルなし		電通技審方式, EBU MAC/パケット Eurocrypt, VideoCrypt	5 3 7 4 6 2 1 電通技審方式, CS スカイポート方式 Nagravision, VideoCrypt-S
	振 幅 方 向 同期抑圧	[CATV]	CS ビデオサイファー方式 (B-NTSC) [CATV]		CSM 方式
	時 間 方 向 ラインシフト等	CS B-MAC 方式, Discret			

することにより、画面の秘匿度を広い範囲で制御することができ（効果制御）、現在、JSB では内容がかなりわかる状態で運用されている。

我が国のハイビジョンの有料方式では、MUSE 伝送信号に対してラインローテーションが行われるが、これにはカットポイントを各走査線の中で一点設ける 1-CUT 方式と、輝度信号と色差信号のそれぞれに一点設ける 2-CUT 方式とがある⁵⁾。

(4) ラインパーミュテーション方式

ラインパーミュテーション方式（走査線転移方式）は、ラインシャフリング方式とも呼ばれ、走査線の順序をランダムに変えて送る方式であり、縦方向に画面が乱される方式である。ラインローテーション方式と異なり各走査線の中に切断点がないので、伝送路の特性に対して復元画質の劣化を生じにくい利点がある。この方式の秘匿度は、走査線を転移するためのラインメモリーの量を増すことにより上がる。

我が国の BS のテレビ放送やハイビジョン放送の有料方式におけるラインパーミュテーション方式では、非ブロック化方式（画面上にブロックを区切らずに転移を行う）を採用している。この方式は受信機に 64 ライン分（ハイビジョンでは 128 ライン）のメモリーを持ち、PN 信号で指定されたアドレスのラインメモリー

ーの内容を読み出すとともに、そのアドレスにそのとき受信される信号を書込む方法でデスクランブルを行う方式である²⁾。これは受信機側がメモリーが少なく処理が簡単となり、放送に適した方式である。

CS テレビ放送用のいわゆるスカイポート方式⁶⁾と M 方式⁷⁾にも、ラインパーミュテーション方式が用いられている。このうち、スカイポート方式では 1 フィールド 240 ライン分のメモリーで処理し、この走査線を入れ替えるパターンを常時送信する方式を用いている。

海外でも地上テレビ用にラインパーミュテーション方式が増えている。フランスのカナルプラス（地上）では、盗視聴の問題を生じた Discret 方式を順次ラインパーミュテーションによる Nagravision 方式に変更することになっている。また、イギリス BBC の Select（VTR 向けに夜間専門番組を放送するサービス）では、受信制御方式はスカイテレビジョンと同じ方式であるが、映像スクランブルには、BBC の全国放送網で伝送するときに伝送路特性の影響を受けにくいラインパーミュテーション方式を採用している⁸⁾。

4.2 音声信号

衛星放送やハイビジョンの音声はデジタル化されており、PN 信号を加算する方式で容易にスクランブル

ルが行える。我が国のBSやCSのテレビ放送、ハイビジョン放送の音声スクランブル方式は、いずれもPN信号加算方式である（ただし、アルゴリズムは方式により異なる。また、ハイビジョンではDPCM符号化された信号へ加算される）。

アナログ音声信号に対するスクランブルは、復元品質が劣化しやすく、安全性の高い方式を放送品質の音声に適用するのは困難である。放送用としては、スペクトルを反転する方式やRF変調信号に妨害波を重畳する（映像とともにスクランブルされる）方式などが用いられるが、表2のように、スペクトル反転方式が多い。

衛星放送の独立音声を用いる衛星デジタル音楽放送（SDAB）は、日本衛星放送（JSB）の電波の音声第3、第4チャンネルで行われるが、このスクランブルは連続するPN信号系列の第3、第4チャンネルの部分を加算して行われる。

CS音声放送（多チャンネルPCM音声放送）は、放送衛星のテレビ音声（2.048 Mb/s）を6チャンネル並列にした構成であり、スクランブル方式はテレビ音声と共通のCOATEC方式である。

4.3 データ信号

データ信号は、PN信号系列の加算によるストリーム暗号やブロック暗号でスクランブルが行える⁹⁾。

我が国では、地上テレビ放送の音声に多重するファクシミリ放送のスクランブル方式が定められ¹⁰⁾、衛星テレビやハイビジョンのデータチャンネルを利用するデータ放送のスクランブル方式が、電気通信技術審議会で審議中である。

5. スクランブル放送の受信制御技術

スクランブル放送を行うには、信号をスクランブルする技術以上に、その受信を制御する技術が重要である。この点に関する最近の話題を次に述べる。

5.1 セキュリティ処理と処理モジュール

関連情報を扱うサブシステムでは、秘匿化された信号を復元するための鍵の処理と、各人の契約内容に応じたデスクランブルの制御や課金方式の処理が行われるが、受信機において鍵情報を秘匿するとともに、契約に関する情報の改ざん（期間の延長など）を防ぐために、セキュリティ処理の部分が外部からアクセスできないことが重要である。我が国の衛星放送用のデコーダでは、この部分を専用のICとして内部に埋め込んでいる。しかし、専用ICの開発にはかなりのコストがかかり、また、これをデコーダの中に埋め込んでしまうと、不正に対処するときにはデコーダ全体を交換

することが必要となる。また、デコーダ自体に個別の鍵など秘密情報が含まれるので、放送局側で1台ごとに管理する必要があり、デコーダの自由な販売も行いにくい。このため最近、ヨーロッパを中心として、セキュリティ処理の部分を有料デコーダ本体から取り外し可能な形態とし、この部分のみを管理する方式が多く開発され、実用されている⁸⁾¹¹⁾¹²⁾。この場合、有料デコーダの本体には秘密の部分を含まないのので、契約更新時等にセキュリティモジュールを交換するだけで安全性を維持することができる。

この取り外し可能なセキュリティモジュールの形態としては、例えば、表2のVideoCrypt方式やEurocrypt方式ではCPU内蔵のICカード、NagravisionではICカードと同様な機能を持つ鍵の形をしたモジュールが用いられている。

スクランブル放送では、一般的に図1に示したような階層化した暗号方式を用いて、鍵の再生や契約内容の照合等のセキュリティ処理が行われ、我が国の方式も同様な構成である。

VideoCrypt方式では、セキュリティ処理を行うICカードを受信機がFiat-Shamir方式で認証し、認証されるとデスクランブル用の鍵が出力されるという独特の方式を実用化している。このICカードは契約者に定期的に郵送され、このカードの更新に合わせて認証アルゴリズムを変える安全性の高い方式である¹¹⁾。

5.2 課金方式の処理

有料放送の課金方式として、現在は、契約するとすべての番組が視聴できるフラットフィー方式が多い。しかし、多様化の時代には、必要な情報のみに支払う方法も望まれることから、視聴した量（番組数や時間数）に応じて料金を支払うペイパービュー方式の検討が進められている。ペイパービューを実現するには種々の方法があるが、受信機のみで処理を行うインパルスペイパービュー方式が多く検討されている。この方式には、あらかじめ支払った金額を受信機に蓄積し、視聴のたびに減額して、残金がなくなるまで視聴できるようにする前払い方式と、視聴した番組と料金の情報を放送局側に転送して課金を行う後払い方式とがある。前払い金の情報や視聴情報を放送局と受信機の間で伝送する手段として、電話線を用いる方法、ICカードを用いる方法等が検討されている¹³⁾。

6. む す び

放送における限定受信技術について、最近の動向をまとめたが、種々の方式が提案、実用化されており、今後も種々の放送に適用されると思われる。シス

テムの安全性とコストの問題は、放送の事業に密接に関わり、それぞれの事業方針により方式が採用されている。本文がそれらの全体的な流れを知る上で参考になれば幸いである。

(1992年10月16日受付)

【参 考 文 献】

- 1) 難波: “放送における情報セキュリティ技術”, 信学会, 情報セキュリティ研資, ISEC89-35 (Dec. 1989)
- 2) 難波: “放送における情報セキュリティ”, テレビ誌, **42**, 12, pp. 1291-1298 (Dec. 1988)
- 3) 秋山: “スクランブル方式”, テレビ誌, **46**, 1, pp. 31-39 (Jan. 1991)
- 4) 上野: “ヨーロッパの有料テレビ放送”, 放送研究と調査, pp. 20-25 (Dec. 1990)
- 5) CCIR Rec. 810, “Conditional-access Broadcasting Systems” (Sep. 1992)
- 6) 平成2年度電通技審答申諮問第16号
- 7) 多田ほか: “スカイポート方式スクランブル技術”, 放送技術, **4**, pp. 319-323 (Apr. 1990)
- 8) 根津ほか: “通信衛星テレビジョン信号スクランブル方式—M方式—の開発”, テレビ学技報, BCS'91-1 (Feb. 1991)
- 9) D. J. M. Kitson and C. K. P. Clarke: “BBC Select: A

terrestrial subscription television service”, International Broadcasting Convention, pp. 405-409 (July 1992)

- 9) 吉村ほか: “衛星データ放送における限定受信の一検討”, テレビ学技報, **14**, 44, pp. 37-42, BCS'90-38 (Aug. 1990)
- 10) 岡野: “電気通信技術審議会答申について (諮問第49号「ファクシミリ多重放送における有料方式に関する技術的条件」)”, 放送技術, **2**, pp. 160-164 (Feb. 1991)
- 11) P. Peyret, et al.: “Smart Cards Provide Very High Security and Flexibility in Subscribers Management”, IEEE Trans. on Consumer Electronics, **36**, 3, pp. 744-752 (Aug. 1990)
- 12) V. Lenoir: “Eurocrypt, a Successful Conditional Access System”, IEEE Trans. on Consumer Electronics, **37**, 3, pp. 432-436 (Aug. 1991)
- 13) ハイビジョン・ペーパービュー研究会最終報告書 (1991. 12)

なば せいいち

難波 誠一 昭和48年、東京大学大学院電気工学専攻博士課程修了。同年、NHKに入局。現在、同放送技術研究所デジタル放送方式研究部主任研究員。静止画放送、緊急警報放送等コード放送、限定受信方式、ISDBなど新放送方式、デジタル放送方式の研究に従事。工学博士。正会員。

4-2 Image Save and Carry (IS & C) における ファイル保護機構

谷内田 益 義†, 北 川 博 雄†

1. ま え が き

医療分野にもコンピュータの導入が盛んに行われている。簡単な医事会計システムから、各種検査の依頼や投薬の指示、検査結果の管理までカバーしたもので、様々なシステムが稼働している。これまでスピード、データ量の点で取扱いが難しかった画像についても、コンピュータとその周辺機器の発達にしたがって、様々な形でコンピュータの導入が図られている。

近年の医療画像の特徴は、コンピュータを組み込んだ撮影機器が導入され、画像のデジタル化が進んできている点である。コンピュータ技術の発達によって新たに開発されたDSA (X線造影撮影装置)、CT (X線断層撮影装置)、MRI (核磁気共鳴断層撮影装置) な

どがその典型である。またフィルムスキャナの開発によって、研究段階ながらフィルムに記録された画像をデジタル化し、評価する試みも広がっている。今のところ各撮影機器から発生した画像は、基本的にはフィルムで保管することが法律で義務づけられている。CTなどから発生するデジタル画像も、フィルムプリンタ等で一度フィルムに焼き付け、診断や保管が行われているのが実状である。しかしながら、今後は医用画像データのデジタル保管が認められる方向に進んでいくものと思われる。

法律上の問題とは関係なく、デジタル化した画像データの処理や、保存に関する研究が盛んに行われている。また、デジタル化した画像情報を臨床で用いるための計算機システムも研究開発されている。特に画像情報の有効利用を目標に、各撮影機器や画像表示端末、画像データの管理用コンピュータを病院内ネットワークで結び、デジタル化された画像情報を管理しようとする Picture Archiving and Communication System (PACS) と呼ばれるシステムも実験的に使用

† 株式会社リコー 中央研究所

“File Security Techniques on Image Save and Carry System” by Masuyoshi Yachida and Hiroo Kitagawa (Research and Development Center, Ricoh Company Ltd., Tokyo)