狭帯域放送のためのアクセス制御方式

Conditional Access System Using Broadcasting for Narrow-band Mobile Broadcasting Systems

正会員 西本友成[†], 正会員 藤津 智[†], 正会員 砂崎俊二[†],
正会員 木村武史[†], 正会員 今泉浩幸[†], 正会員 藤田欣裕[†]
Yusei Nishimoto[†], Satoshi Fujitsu[†], Shunji Sunasaki[†],
Takeshi Kimura[†], Hiroyuki Imaizumi[†] and Yoshihiro Fujita[†]

Abstract A conditional access system (CAS) is essential for controlling digital content usage in narrow-band broadcasting such as terrestrial 1-segment broadcasting and digital audio broadcasting. We assume that 'broadcasting receivers' refers not only to mobile phones but also to mobile receivers that do not have two-way communication functions. This would include mobile receivers for use in motor vehicles and portable receivers used in combination with personal digital assistants (PDAs) and portable game stations. A CAS provides a way of restricting broadcasting reception and content playback services to subscribers. To distinguish between subscribers and non-subscribers, contract information needs to be distributed to each receiver, and this needs to be done by broadcasting to mobile receivers. Conventional CASs, i.e., those used for digital satellite broadcasting, broadcast contract information in this way. Doing this, however, requires a wide transmission band of about 300 kbps because contract information is transmitted to individual receivers. The current technology for distributing contract information on conventional CASs cannot therefore be applied to narrow-band broadcasting. In order to resolve this problem, we have developed a new CAS that is capable of transmitting contract information even in narrow-band broadcasting. We describe the scheme used to calculate the transmission rate of contract information. Furthermore, we have evaluated both the security and the implementation of the proposed CAS and determined that the proposed CAS can be applied to existing services.

キーワード：地上デジタル放送，地上デジタル音声放送，狭帯域放送，アクセス制御，契約情報

1. ま え が き

ワンセグやデジタルラジオなどの携帯受信機向けの狭帯域放送において，デジタルコンテンツの権利を保護し，その利用方法を制御するためには，アクセス制御方式であるCAS (Conditional Access System) が必須である¹⁾。

アクセス制御方式は，受信契約者のみに放送受信やコンテンツ再生を限定させる仕組みを提供する。受信契約者と非契約者を区別するために，受信機それぞれに契約情報を配信する必要がある。通信機能を有する携帯電話等では，個別の契約情報を通信により配信することが可能であるが，通信機能を持たないPDA (Personal Digital Assistants)，ゲーム機を利用したポータブル放送受信機や車載型放送受信機等においては，この契約情報を放送で配信する必要がある。

る。衛星デジタル放送では，ARIB STD-B25第1部の第1章から第4章で規定されるCAS-R方式（以下，現行CAS）^{2)~4)}を採用している。現行CASでは，放送により契約情報を配信している。しかし，放送で受信機個別の契約情報を送るために，300kbps程度の幅広い伝送帯域を必要とするため，現行CASによる契約情報の配信技術を狭帯域放送⁵⁾に適用できない。また，2.6GHz帯衛星デジタル音声放送^{2) 6)}では，契約情報の送出のために，256kbpsの専用チャンネルを設け契約情報の圧縮配信を行っている。ワンセグや地上デジタル音声放送⁷⁾等では専用チャンネルを設けることが難しく，この帯域でさえ確保することは困難であり，さらに狭い帯域で契約情報を配信する必要がある。そのため，狭い帯域においても契約情報を配信可能なアクセス制御方式を新たに開発する必要がある。

本稿では，まず狭帯域放送のためのアクセス制御方式の研究課題と要求条件を述べ，開発した狭帯域放送のためのアクセス制御方式を説明する。また，本方式の運用方法，安全性に関する検討結果および実装評価について報告する。

2006年11月7日受付，2007年1月23日再受付，2007年2月10日採録

[†] NHK放送技術研究所

(〒157-8510 世田谷区砧1-10-11, TEL 03-5494-3424)

[†] NHK Science and Technical Research Laboratories

(1-10-11, Kinuta, Setagaya-ku, Tokyo, 157-8510, Japan)

2. アクセス制御方式の課題と要求条件

通信機能を持たない放送受信機においてアクセス制御を実現するために、放送事業者は放送サービスの新規契約や契約解除を電話、郵便やインターネット等で受付け、放送により契約情報を受信機毎に効率的に配信する必要がある(図1)。この契約情報は、次の3種類に大別される。

- (1) 新規契約時の契約情報
- (2) 契約継続時の契約情報(サービス追加などの契約変更を含む)
- (3) 契約解約時の契約情報

放送では、上り回線がないため、契約情報の送出側で受信機における契約情報の受信状態を確認することができない。そのため、契約情報を受信させるために、同じ内容の契約情報を周期的に何度も送出する必要がある。現行CASでは、1ヶ月程度の短い有効期限をもった契約情報を利用し、契約中の契約者に対して、契約継続のための契約情報を周期的に送出する。契約解約者に対しては、契約情報を送出しないこととし、契約情報の有効期限の満了を持って解約となる。これにより、契約解約者に対して、放送の視聴を確実に停止することができる。しかし、契約を継続しているすべての契約者に対して、契約情報の有効期限が切れる前に、継続的に大量の契約情報を送出する必要がある。

短い周期で大量の契約情報を送出するためには、幅広い契約情報の伝送帯域を必要とする。しかし、300~400kbps程度の伝送帯域しか持たない狭帯域放送では、数kbpsから

数十kbps程度しか確保できない。そのため、契約情報の繰返し周期が長くなり、狭帯域放送の受信機に契約情報を確実に受信させることが困難になるという課題がある。

また、現行CASは、固定受信機を想定しており、契約情報を常時受信できる環境を前提として設計されている。そのため、1日5分程度の短時間の視聴形態や、不安定な受信環境である携帯受信機に適用できない。移動体向けの放送では、現行CASの想定よりさらに短い周期で契約情報を送出する必要がある、受信機が契約情報を受信する確率をできる限り高める必要がある。

今回、以下に示す要求条件を設定し、それを満足する狭帯域放送における携帯受信機のための契約情報の配信技術を備えるアクセス制御方式を開発した。

- (1) 狭帯域放送の伝送帯域を考慮して、契約情報を圧縮し、契約情報の送出レートを低くすること
- (2) 受信時間が短いモバイル利用環境においても、放送受信機に契約状態を反映できること

3. 狭帯域放送用のアクセス制御方式の設計

アクセス制御方式は、放送受信時に視聴制御する限定受信方式と、受信機に蓄積したコンテンツを再生時に視聴制御する限定再生方式に大別される。今回、これらの双方の方式について検討した。

3.1 限定受信方式の設計

図2に、現行CASの概要を示す。受信機毎に個別の情報である個別情報(EMM: Entitlement Management Message)

図1 契約情報の送出概要

Overview of contract information transmission systems.

図3 開発した狭帯域放送のための限定受信方式の概要

Developed conditional access system on narrow-band mobile broadcasting systems.

図2 現行の限定受信方式の概要

Overview of the current conditional access system.

と、受信機間に共通の情報である共通情報 (ECM: Entitlement Control Message) で構成される⁸⁾。契約情報を受信機毎に固有のマスタ鍵で暗号化して、受信機IDを宛先として付与し個別情報として配信する。各受信機では、受信機IDの一致する個別情報を受信したときに、マスタ鍵で復号し新規契約や契約継続の契約情報を取得する。

図3に、開発した狭帯域放送用アクセス制御方式の概要を示す。契約情報を共通情報として配信することで、複数の受信者向けの契約情報を一斉配信することができる。図4に、本方式で用いる共通情報であるECM-M (Entitlement Control Message for Mobile) と、個別情報であるEMM-M (Entitlement Management Message for Mobile) とEMMの構成を示す。本方式では、EMMで新規契約の契約情報のみを送出し、繰り返し送出する必要のある契約継続および契約解除の契約情報は、複数の受信機IDに向けた契約情報を束ねて共通情報としたECM-Mにより送出する。また、現行CASでは、ワーク鍵を受信機個別のマスタ鍵で暗号化し

てEMMで送出するが、本方式では、ワーク鍵を受信機共通に暗号化したEMM-Mとして送出する。

次に、本方式の詳細について述べる。複数の受信機をグループ化し、グループIDを割当てて、このグループIDと契約情報を配置したビット位置の情報から受信機側で受信機IDを生成できるようにし、受信機IDの送出を不要とすることで契約情報の送出レートを低減する。複数の受信機の契約情報を束ねたビット列化した契約情報列をECM-Mとして送出する。ビット列化した契約情報列は、契約状態を示す情報を含んでおり、契約中であれば1、未契約であれば0の値を持つ。さらに、ビット列化した契約情報列に対して、可逆圧縮を施し伝送効率を高めることができる。この契約情報列を複数まとめて、1セクションのECM-Mとして暗号化し生成する。受信機では、暗号化したすべての共通情報を復号し、受信機のグループIDと一致する時に、ビット列化された契約情報から自分宛の契約情報のみを取得する。現行CASでは、安全性向上のためにワーク鍵を更新する際に、受信機個別にワーク鍵を更新する必要があるため、数ヶ月程度の期間を要する。しかし、本方式では、受信機共通の暗号化を行うEMM-Mで送出するので、対象とする受信機のワーク鍵を同時に更新可能であり、ワーク鍵の更新の頻度を高めることで安全性を高めることができる。

さらに、複数の音声を提供し音声毎にアクセス制御する場合や番組のジャンル毎でアクセス制御する場合などには、一つの編成チャンネル内で、複数のサービスに対してアクセス制御できる必要がある。そのため、アクセス制御したいそれぞれのサービスに対して、サービスIDを割当てサービス毎に契約情報を送出する。受信機では、暗号化したすべての共通情報を復号し、自分宛の契約情報のみをサー

() 内の数値はバイト長を示す

(a) ECM-Mの構成

() 内の数値はバイト長を示す

(b) EMM-Mの構成

() 内の数値はバイト長を示す

(c) EMMの構成

図4 使用する共通情報と個別情報の構成

Structures of ECM-M, EMM-M and EMM on developed CAS.

表1 共通情報と個別情報の送出方法
Transmission method for ECM-M, EMM-M and EMM.

関連情報の種別	目的	個別/共通	必要帯域	送出方法
ECM-M	契約継続と契約解約の契約情報の送出	スクランブル鍵は共通 契約情報は個別 (受信機IDを付与した 受信機全部)	数kbps～ 数十kbps	周期的に 送出
EMM-M	ワーク鍵の更新	ワーク鍵は共通	若干	周期的に 送出
EMM	新規契約の契約情報の送出	契約情報は個別 (新規契約の受信機のみ)	数kbps	要求に応じて送出

ビス毎に取得する。また、システム鍵は、システムに固有の鍵であり、数種類のみを用意する。

表1に、本方式で用いる共通情報と個別情報の送出方法を示す。受信機毎の契約状態を受信機に反映するために、契約情報の有効期限を1年以上とし、契約継続のための契約情報を受信するための猶予期間を長くすることで、契約継続の契約情報を受信できる確率を高める。その一方で、契約解約のための契約情報を契約継続の場合と同様に周期送出することで、契約解約を実現する。契約解約の契約情報

報を受信する確率に基づいて、契約解約を実現することとし、最終的には契約情報の有効期限により確実に契約解除を執行する。また、新規契約のための契約情報は、即時に契約状態を受信機に反映するために、現行CASで用いるEMMにより送出する。新規契約時に、ユーザに受信機の電源を投入させ、電話等で視聴可能になったことをフィードバックさせる運用形態とすることで、新規契約の契約情報を確実に受信させる。よって、新規契約の契約情報を周期的に送出する必要はない。

図5に、各方式における受信契約者数と契約情報の繰返し周期の関係を示す。契約情報の送出レートを1.5kbpsとし、現行CASについては1TSパケットで伝送可能な契約情報の件数を6として⁶⁾、算出した。現行CASでは、契約者1千万件で繰返し周期が450時間を越えてしまうが、本技術では、2.5時間と大幅に短縮できる。現行CASでは、受信機IDを付与し受信機個別に契約情報を送出するので、未契約者の受信機に対して契約情報を送出する必要がある。しかし、本方式は、契約情報の高圧縮配信が期待できるが、すべての受信機IDに対して契約情報を配信するので、未契約者に対しても契約情報を配信する必要がある。そのため、現行

図5 受信契約者数と契約情報の繰返し周期の関係

Relation between the number of subscribers and the retransmission period of contract information.

CASとは異なり、受信機IDの発行総数が増加するほど契約情報の繰返し周期が長くなる欠点を持つ。この繰返し周期は、契約解約の契約情報を受信機に即時に反映するために、できる限り短くした方がよい。

そのため、予めこの受信機IDを受信機に割当ててではなく、新規契約時に放送でダイナミックに受信機IDを割当てて。受信機IDの割当て手段は、予め受信機毎に固定的に付与する受信機固定IDを宛先情報とし、EMMに受信機IDを記述し配信することで実現する。また、一度割当てた受信機IDを再利用するために、耐タンパーモジュール内に保持されている受信機IDを無効化し、ECM-Mを受け付けないロック機構を、耐タンパーモジュール内に予め実装しておく。例えば、編成チャンネル内のすべてのサービスを解約（有効期限切れを含む）した場合に、耐タンパーモジュール内の当該受信機IDを無効化しロック状態とする。再度、EMMにより受信機IDが付与された際に、ロック状態を解除する。これら受信機IDの付与やロック動作とロック解除動作は、編成チャンネル毎に独立に行う。これにより、受信機に割当てた受信機IDをダイナミックに変更でき、受信機IDを契約者のみに割当てることが可能になるので、受信機IDの総発行数は、当該放送サービスで想定する契約者数を考慮すればよい。

本方式により、契約継続と契約解約のための契約情報を効率的に送出することができるので、狭帯域放送においても、放送受信チャンネルのフラット/ティア課金を実現することができる。

3.2 限定再生方式の設計

図6に、限定再生方式において想定するストリームの構成例を示す。3.1節で述べた限定受信方式で使用するリアルタイム受信のためのコンテンツに加えて、DSM-CC (Digital Storage Media- Command and Control) データカプセル⁹⁾により蓄積再生用のコンテンツを伝送する。本稿では、このDSM-CCデータカプセルで伝送し、受信機

図6 限定再生方式で想定するストリームの構成例
Structure instance of streams on developed CAS for stored content.

表2 ACIの構成
Structure of access control information.

構成	備考
プロトコル番号	1Byte
事業者識別	2Byte
ワーク鍵識別	10Byte
各種データ領域	サービスID、コンテンツ鍵識別、コンテンツ鍵などを配置
事業者領域	各種の情報を配置

ACIは、データカプセルの1リソースとして伝送する

図7 開発した狭帯域放送のための限定再生方式の概要
Developed CAS for stored content on narrow-band mobile broadcasting systems.

に蓄積したコンテンツの再生時制御を目的とする。

開発した限定再生方式では、再生時制御をするコンテンツをコンテンツ鍵で暗号化し、それをDSM-CCデータカプセル化し、さらに、トランスポートストリーム上でスクランブル化し送出する。同時に、そのコンテンツのコンテンツ鍵と利用条件（有効期限や再生回数など）をACI (Access Control Information)²⁾と呼ばれるライセンス情報として送出する。ACI (表2) は、3.1節で述べたEMM-Mで配送するワーク鍵で暗号化する。受信機側では、トランスポートストリームをデスクランブルし、DSM-CCデータカプセルから暗号化コンテンツを取り出し蓄積する。

図7に、開発した限定再生方式のコンテンツ再生時の概要を示す。耐タンパーモジュールは、コンテンツ再生時にACIで指示するサービスIDの契約情報を確認し契約済みであれば、コンテンツ鍵を受信機に出力する。受信機は、そのコンテンツ鍵により暗号化コンテンツを復号し提示す

る。契約情報の送出方法に関しては、例えば、サービスID=1をリアルタイム受信する音声ストリーム、サービスID=2を蓄積再生コンテンツに割当て、二つのサービス分の契約情報をECM-Mで配送する。

本方式により、ECM-Mの契約情報でコンテンツの蓄積再生時の月極課金を可能にし、ACIでコンテンツ毎に利用を制御できる。例えば、歌謡曲のTOP10の楽曲コンテンツをDSM-CCデータカールセル伝送し、いつでも新しい楽曲コンテンツを再生できるダウンロードサービスを想定した場合、このサービスを月極課金で提供することができる。

4. 運用方法に関する検討

本方式により実施可能な運用方法を明らかにするため、契約情報の伝送手段であるECM-MとEMMの送出ビットレートについて検討した。ECM-Mで繰返し送出する契約情報の繰返し周期は、契約情報の送出レートと契約者数などから算出されるが、算出された周期において、契約情報が的確に更新されるかどうかを携帯受信機の電源ON時間を想定して見積もる必要がある。

4.1 ECM-Mの送出ビットレート

ECM-Mで送出される契約情報の繰返し周期Pは、式(1)と式(2)により算出される。

$$P = \frac{N_s \times N_{id}}{N_{ci}} \cdot \frac{1}{R_{TS}} \quad [s] \quad (1)$$

$$R_{TS} = \frac{R_{ECM-M}}{L_{TS}} \quad [pps] \quad (2)$$

ここで、 N_s はサービスの数、 N_{id} は受信機IDの総数、 N_{ci} は1TSパケットで伝送される契約情報件数の平均値である。また、 R_{TS} はTSパケットの送出レートであり、 R_{ECM-M} はECM-Mの送出レート(bps)、 L_{TS} はTSパケットサイズ(ビット)である。

図8に、受信機IDの発行数と契約情報の繰返し周期の関係を示す。実線は、契約情報列に対する可逆圧縮がない場合、破線は、契約情報列に可逆圧縮を行ったときの繰返し周期を示している。式(1)を用いて、 N_s を1とし、可逆圧縮なしの場合の N_{ci} を1,256件として算出した。また、可逆圧縮時は、ランレングス・ハフマン符号化を用い、受信契約率95%で算出し、 N_{ci} を2311件とした。

現行CASにおいて狭帯域放送での契約情報の配信は不可能とされてきたが、本技術では、次の条件下で契約情報の配信を可能にする。

厳しい条件として、契約情報の送出レートを15kbpsとし、繰返し周期を15分間とすると、受信機IDを1千万個程度まで発行できることがわかる。繰返し周期が15分間であれば、サイマル放送である現行のワンセグの視聴形態を想定し1日5分間程度の視聴^{10) 11)}が行われるとすると、契約情報の未受信は1ヶ月間の継続受信後に、100万件に対して5件程度の割合で発生すると算出される。

また、夜間中に放送番組を携帯受信機に備える蓄積装置

図8 受信機IDの発行数と契約情報の繰返し周期の関係
Relation between the number of receiver's ID and the retransmission period of contract information.

にダウンロードするような放送サービスを考えた場合、夜間に7時間程度は常時放送受信可能である。夜間の放送番組のダウンロード時間より、契約情報の繰返し周期が短ければ、ほぼ確実に契約情報を受信させることができる。この場合、契約情報の送出レートを15kbps、繰返し周期を7時間とすると、受信機IDを5億個程度まで発行できる。

本方式は、受信機IDを契約者のみに割当てることができるので、1,000万件以上の受信者を想定する大規模な放送サービスに充分適用できることがわかる。

4.2 EMMの送出ビットレート

新規契約時にユーザに受信機の電源を投入させ、電話等で視聴可能になったことをフィードバックさせる運用形態とすれば、EMMは、基本的に1回のみの送出で済む。現行CASと同じEMMを用いた場合、1TSパケットで6件の契約情報を配信できる⁶⁾。1TSパケットは1,504ビットなので、約1.5kbpsの送出レートで1秒に6件処理できる。よって、1日に51万8,400件と充分な新規契約数を処理できる。

5. 安全性に関する検討

本方式の安全性への影響について検討した。新規契約後に、サービス毎の契約情報を共通情報として送出するため、偽造した契約情報の注入によるサービス毎の不正視聴の恐れがある。このため、共通情報の暗号鍵であるワーク鍵を定期的に更新できる設計とした。また、正規の契約情報で上書きするために、契約継続と契約解約の契約情報を継続的に送出する設計とした。これにより、偽造したサービス毎の契約情報を注入された場合でも、放送受信すれば、契約情報の繰返し周期の時間内に正しい契約情報に修正される。なお、新規契約を現行CASと同じEMMにより行うので、不正な新規契約は、現行CASと同様に困難である。

また、契約情報とコンテンツの復号鍵であるスクランブル鍵を同封しており、すべての契約情報を耐タンパーモジュールで処理するので、契約解約の契約情報の不正な除去を防止できる。受信機への負荷を抑えながら、従来の方式と同等の安全性を保持している。

図9 試作したSIMカードと携帯放送受信機
Prototype mobile receiver with a SIM card.

6. 実装評価

本方式は、契約情報の高圧縮配信が期待できるが、ECM-Mを処理する過程において、耐タンパーモジュール内で自分宛以外の契約情報も含めて処理する必要がある。そのため、耐タンパーモジュールに負荷を与える恐れがある。そこで、低い演算処理能力を持つSIM (Subscriber Identity Module) カードで実装評価を行った。

図9に、試作したSIMカードと携帯放送受信機の概観写真を示す。本SIMカードは、JavaCard v2.2.1 OS, 16ビットCPU, 144kB EEPROMを備え、312.5kbps通信が可能である。共通鍵暗号アルゴリズムは、JavaCardv2.2.1で標準搭載するDES (Data Encryption Standard) を利用している。ECM-Mの処理は、契約情報の情報処理だけでなく、暗号化したコンテンツの復号鍵を復号する処理も含まれる。暗号化契約情報の送出レートが、約1.5kbps程度であれば、コンテンツの暗号復号処理に問題ない範囲で、SIMカード内でECM-Mを処理できることを確認できた。契約情報の送出レートを15kbpsとする場合、低速通信I/FのSIMカード実装では処理困難であるが、高速通信I/FのCA (Conditional Access) 専用LSI¹²⁾を用いれば充分処理可能であると考えられる。

7. むすび

狭帯域放送用のアクセス制御方式のための契約情報の配信技術を考案し、本技術を実用化した場合の運用スキームを明らかにした。また、開発したアクセス制御方式の安全性に関する検討と実装評価を行うことで、本方式を実サービスに適用できることを示した。

〔文 献〕

- 1) 山田ほか：“マルチメディア時代のコピープロテクション”，信学論誌，J87-A，6，pp.734-745 (2004)
- 2) 電波産業会：“デジタル放送におけるアクセス制御方式標準規格”，ARIB STD-B25 (2006)
- 3) 電波産業会：“BS/広帯域CSデジタル放送運用規定”，ARIB TR-B15 (2006)
- 4) 電波産業会：“地上デジタルテレビジョン放送運用規定”，ARIB TR-B14 (2006)

- 5) 伊藤泰宏：“地上デジタル放送技術”，信学誌，87，7，pp.583-588 (2004)
- 6) 秋山ほか：“有料モバイル音声放送における限定受信方式の設計”，情報処理学論誌，44，12，pp.3071-3080 (2003)
- 7) 近江克郎：“地上デジタル音声放送”，映情学誌，58，5，pp.613-617 (2004)
- 8) ISO/IEC: "Generic Coding of Moving Pictures and Associated Audio Systems", 13818-1
- 9) ISO/IEC: "Generic Coding of Moving Pictures and Associated Audio Information -Part 6: Extensions for DSM-CC", 13818-6
- 10) 矢野経済研究所：“2006視聴スタイル動向調査” (2006)
- 11) シードプランニング：“ワンセグ初期ユーザ調査 [2]” (2006.7)
- 12) 由良ほか：“モバイル衛星デジタル放送向け限定受信LSI”，東芝レビュー，56，7，pp.30-33 (2001)

西本 友成 1996年，熊本大学大学院工学研究科修士課程修了。同年，NHKに入局。熊本放送局を経て，1999年より，放送技術研究所に勤務。現在，蓄積型放送技術，放送コンテンツのアクセス制御技術の研究に従事。正会員。

藤津 智 1999年，東京工業大学大学院総合理工学研究科知能システム科学専攻修士課程修了。2004年，NHKに入局。放送技術研究所に勤務。現在，総合情報端末・セキュリティの研究に従事。正会員。

砂崎 俊二 1986年，熊本大学工学部電気工学科卒業。同年，NHKに入局。福岡放送局，放送技術局，技術局，NHKエンジニアリングサービス出向を経て，2005年より，放送技術研究所にてコンテンツセキュリティの研究に従事。正会員。

木村 武史 1980年，東京工業大学大学院修士課程修了。同年，NHKに入局。大阪放送局勤務を経て，1983年より，放送技術研究所に勤務。限定受信技術，デジタル放送多重・伝送技術，マルチメディア放送技術などの研究を行い，現在は，放送セキュリティ技術の研究に従事。正会員。

今泉 浩幸 1985年，東京工業大学大学院修士課程修了。同年，NHKに入局。福岡放送局を経て，1988年，放送技術研究所，2002年～2006年，NHKエンジニアリングサービス。通信ネットワーク利用放送技術，コンテンツ権利保護技術の研究に従事。現在，放送技術研究所 (システム) 主任研究員。正会員。

藤田 欣裕 1976年，東京大学工学部電気工学科卒業。同年，NHKに入局。大阪放送局を経て，1981年より，同放送技術研究所にて，固体撮像技術，高精細撮像システムの研究に従事。現在，同放送技術研究所 (システム) 部長。博士 (工学)。正会員。