マルチメディア情報処理特集

放送型データ配信サービスのためのマルチキャスト技術

マルチキャストは，第3世代以降の広帯域移動通信網の普及とマルチメディア系アプリケーションの需要増加に伴う放送型データ配信サービスの基盤技術として注目されている．

筆者らは「高信頼マルチキャスト」，「マルチキャストセキュリティ」，「マルチキャストセッション管理」に関連するプロトコル技術を開発した．

上野 英俊（うえの ひでとし）　鈴木 偉元（すずき ひではる）
田中 希世子（たなか きよこ）　石川 憲洋（いしかわ のりひろ）

New Technology Reports

1. まえがき

近年，移動通信網における放送型通信の技術として再びマルチキャストが注目されている．マルチキャストは，すべてのクライアント（データ受信者）に対してデータを同報配信するブロードキャストとは異なり，受信を希望する複数のクライアントにデータを同報配信する技術である．ネットワーク内で単一のアドレスを指定して特定の相手にデータを送信するユニキャストと比べて，マルチキャストは，ネットワーク利用効率の良いデータ伝送技術であり（図1），利用可能な無線資源に限りのある移動通信網において特に効果的である．

インターネットに代表されるIP（Internet Protocol）ネットワーク上でマルチキャストを実現するIPマルチキャストは，以前から研究が行われており，受信者のグループ管理，IPマルチキャストの経路制御，アプリケーションプロトコルなどの技術分野が存在する（図2）．IPマルチキャストを用いたアプリケーションの例として，TV放送のようなストリーム型データ配信アプリケーションと，電子新聞やJava[*1]プログラムなどを配信するファイル型データ配信アプリケーションが存在する．また，小規模なグループ型通信を実現した例としてマルチメディア会議システムなどが存在する．近年になって，ADSL（Asymmetric Digital Subscriber

＊1　Java：米Sun Microsystems社が提唱しているネットワークに特化したオブジェクト指向型開発環境である．

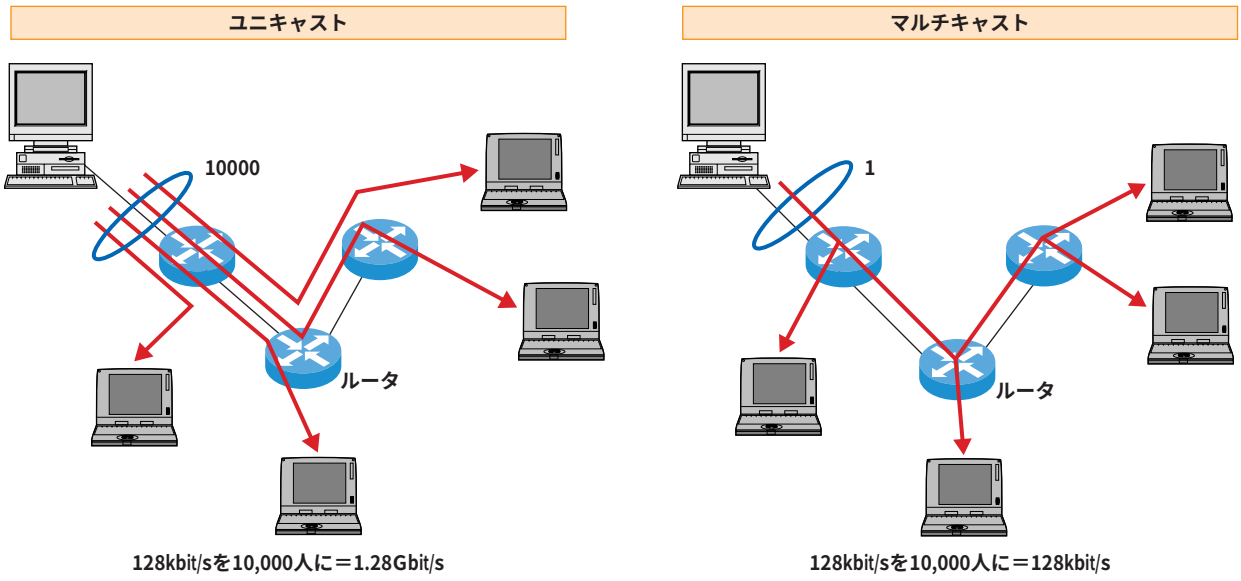
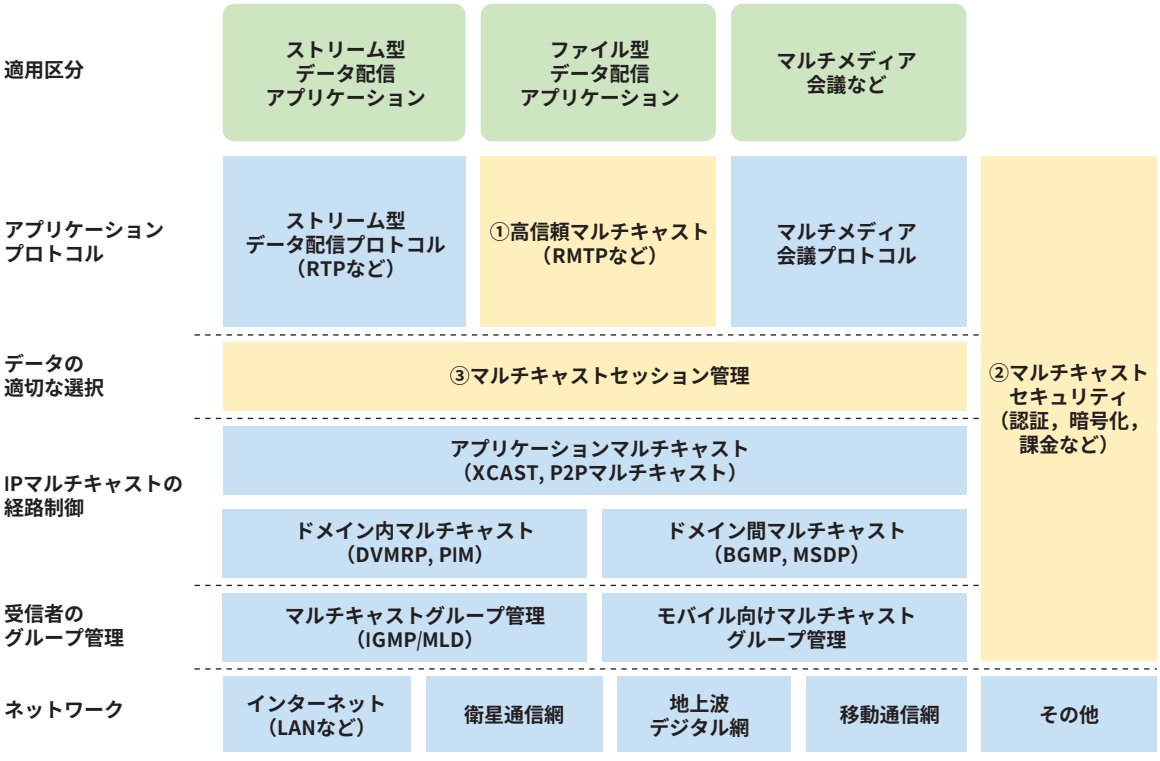


図1　マルチキャストによるネットワーク利用効率の向上（例）



BGMP：Border Gateway Multicast Protocol
DVMRP：Distance Vector Multicast Routing Protocol
LAN：Local Area Network
MLD：Multicast Listener Discovery
MSDP：Multicast Source Discovery Protocol
P2P：Peer-to-Peer
PIM：Protocol Independent Multicast
RTP：Real-time Transport Protocol
XCAST：eXplicit multiCAST

図2　マルチキャストの技術分野

Line）上の動画像配信アプリケーションなど，IPマルチキャストを用いた商用サービスが開始されている．また，3GPP（3rd Generation Partnership Project）では，移動通信網における各種データ配信の実現を目指したMBMS（Multimedia Broadcast Multicast Service）に関する国際標準化が進められている[1]．しかしながら，マルチキャストを用いたサービスは依然，普及には至っておらず，ビジネスモデルの欠如や技術課題について多く指摘されている．

本稿では，図2に示した技術分野の中から要素技術として以下の3項目に焦点を絞り，最新技術動向と著者らの取

り組み内容について説明する．

①高信頼マルチキャスト

IPマルチキャストは，トランスポート層としてUDP（User Datagram Protocol）を用いるため，データの欠落を回復できないという問題がある．ファイル型データ配信アプリケーションを実現するには，元データを完全に復元することが不可欠であるため，何らかの方法で欠落したデータを回復する必要がある．IPマルチキャストにおいてもユニキャストと同様に再送によるデータの回復が可能であるが，複数のクライアントを対象とする場合，データ回復を必要とするすべてのクライアントにとって有効な冗長データを生成するデータ符号化技術が存在する．また，誤り率変動量の大きな無線網において，データの欠落がないことを保証するためには再送が必要であるため，再送によるトラヒック増加をできる限り最小化するような効果的な再送とデータ符号化技術の組合せ方式が有効である．

②マルチキャストセキュリティ

IPマルチキャストは，クライアント数が増大した際のスケーラビリティを考慮して設計されているため，サーバ（データ送信者）において明示的にグループに参加しているクライアントを特定しない匿名モデルを採用している．この匿名モデルでは，広告によるビジネスモデル構築に必要不可欠なデータを受信したクライアント数（視聴率）の測定やユーザへの課金の実現が不可能であり，IPマルチキャストが普及しない要因になっている．以上のことから，クライアントにおけるデータ受信履歴の収集やユーザ課金実現のためのクライアント認証が必要である．また，受信権限を持たないクライアントによるデータ受信を防止するためのマルチキャスト用暗号化技術が重要である．

③マルチキャストセッション管理

IPマルチキャストでは，クライアントが受信を所望するグループ（マルチキャストアドレス）を選択し，当該グループへの加入手続きを実行することでデータ受信を開始する．これに対し，サーバがクライアントの受信を所望するグループを適応的に指示する方式が検討されている．このサーバ主導の方式によれば，更新されたデータをいち早くクライアントに提供可能となり，例えばニュース速報などの実時間性の高いプッシュ型のデータ配信サービスの実現が可能となる．また，ユーザにおけるグループの選択という負担を軽減するという利点もあり，入力手段や表示機能に制限のある携帯電話などを利用するユーザにとって利便性を向上することができる．

以下では，上述した技術分野について各項目に分けて詳細を説明する．

2. データ欠落を回復する高信頼マルチキャスト

高信頼マルチキャスト（RM：Reliable Multicast）は，IPに対するTCP（Transmission Control Protocol）のような信頼性（データ欠落の検出，通知，再送，順序保証など）を備えたマルチキャスト技術である．これまでに数多くのRM技術が提案され[2]，基本的な信頼性保証機能だけでなく，フロー制御，輻輳制御，前方誤り訂正（FEC：Forward Error Correction），モバイルインターネットへの適用など，より高度な機能拡張について検討が進められてきた．また，IETF（Internet Engineering Task Force）において標準化活動が進められるなど，RMの普及に向けて活動が本格化している[2]．

2.1 高信頼マルチキャストトランスポートプロトコル

RM技術の中で最も重要なものは，高信頼マルチキャストトランスポートプロトコルである．RMTP（Reliable Multicast Transport Protocol）[3]は，NTTと日本IBM㈱が共同で開発した高信頼マルチキャストトランスポートプロトコルであり，TCPと同等レベルの信頼性で，データの誤りが無く複数のクライアントに対して同報配信できるプロトコルである．RMTPの主要機能には，サーバとクライアント間のコネクションの確立，開放などのコネクション管理，IPマルチキャストを利用したデータ配信，データがサーバから送信された順番でクライアントに配信されることを保証する順序制御，送信パケットに付与された順序番号を利用した欠落パケットの再送制御，クライアントの受信状況に応じたサーバの送信レート制御，サーバにクライアントからの応答が集中しないようにクライアントからの応答送信タイミングを調整するバックオフ制御がある．

RMTPのシーケンス例を図3に示す．RMTPによるデータ配信は，コネクション設定フェーズ，データ配信および再送フェーズ，個別再送フェーズから構成される．コネクション設定フェーズでは，サーバはクライアントに対してデータ送信の開始を通知する．通知を受けたクライアントは，コネクション設定の確認をサーバに応答する．データ配信および再送フェーズでは，サーバはデータを複数のパケットに分割して，IPマルチキャストを利用して配信する．最後のパケットを受信したクライアントは，受信状況に応じて，肯定応答（ACK：ACKnowledgement）または

図3　RMTPの通信シーケンス例

否定応答（NACK：Negative ACKnowledgement）をサーバに送信する．サーバはACKを送信したクライアントとのコネクションを解放し，NACKを送信したクライアントに対しては，NACKで指定された再送を要求するパケット番号に基づいてデータ再送を行う．サーバはすべてのクライアントからACKを受信するまで，このプロセスを繰り返す．何らかの理由でクライアントがIPマルチキャストによるデータ配信を受信できない場合，一定時間内にクライアントからACKを受信できない場合に，サーバはクライアントをIPマルチキャストによるデータ配信から切り離すことも可能である．この切り離されたクライアントに対してデータ配信を継続する場合，ユニキャストによる個別再送を行うことができる．

2.2 無線ネットワークにおける誤り回復技術

無線ネットワークは有線ネットワークに比べて一般に誤り率が高く，遅延の変動幅が大きいといった特性があるため，誤り耐性の向上は，モバイル端末に対するマルチキャスト配信における重要な課題の1つである．特にファイル型データの配信では，データの欠落のない高信頼なデータ伝送が必要である．

代表的な誤り回復技術には，誤り部分を再送して回復する自動再送要求（ARQ：Automatic Repeat reQuest）と，サーバから符号化による冗長データを付加し，受信側で誤りを訂正するFEC，およびデータのコピーを繰り返し送信する連送がある．これらの誤り回復技術は組み合わせることができ，特にARQとFECは誤り回復特性にそれぞれの特徴があるために組み合わせると効果が大きいことが知られている．例えば，FECによって回復可能限界までのデータ損失を回復し，一部の回復限界を超えた損失をARQによって回復するなどの方法がある．著者らは，無線ネットワークに適した誤り回復方式を確立するために，既存の誤り回復技術の通信性能（送信時間，送信パケット数）を理論解析によってモデル化するとともに，無線LAN（WLAN：Wireless Local Area Network）と10数台のノートPCを用いた実験によって解析モデルの妥当性を検証した．数値例を用いた解析結果から，具体的なARQとFECの組合せ構成を導くことができた[4]．また，FECの符号化パラメータ（符号長：n，情報ブロック数：k）は通信網の特性やアプリケーションの要求条件に合わせて決定する必要があるが，ARQとFECのように相反する特徴をもつ両者を組み合わせる場合には符号化パラメータを一意に決定することは難しい．そこで著者らは，送信完了までに要する送信時間と送信パケット数である通信コストを用いた評価関数を定義し，この評価関数から算出される値を最小にするような符号化パラメータ値を導く方法を確立した[4]．符号化パラメータの導出方法を確立することによって，従来ではフィールド実験や運用データを用いた評価検証を必要としていたシステム設計を，シミュレーションにより容易に実現できる．また，異種無線網を利用した端末が混在する場合には，適切なパラメータ値に調整する必要があり，このパラメータ調整に利用できるメリットがある．なお，一般的には送信時

間を最小にする値とパケット数を最小にする値とは独立に存在する．どちらをどれだけ優先するのかという設計ポリシーに関する合理的な決定方法が課題として残る．例えば，実時間性の高いアプリケーションでは送信時間を最小にすることを優先し，移動通信におけるファイル配信のようにデータ数に基づく従量課金の場合には送信パケット数を最小とすることを優先することになる．著者らが開発した評価関数を用いたパラメータ設計方法は，通信コストを送信時間と送信パケット数の両面からバランスよく最小にできる値を導出できる．

3. 暗号化とクライアント認証を実現するマルチキャストセキュリティ

IETFでは，非権利者のデータ受信を防止するためのマルチキャスト向けのデータ暗号化技術に関して，早くからその必要性を認識していた．そこでIETFでは，マルチキャスト用の暗号化と必要な鍵管理を行うためのグループ鍵管理アーキテクチャを規定した（図4）．グループ鍵管理アーキテクチャは，グループメンバーで共有するトラヒック暗号化鍵（TEK：Traffic Encryption Key），および鍵暗号化鍵（KEK：Key Encryption Key）を規定しており，これらの鍵をクライアント個別鍵（CIK：Client Individual Key）を用いてグループメンバーに提供することで，マルチキャスト配信データの暗号化を可能としている．KEKは，グループメンバーの加入／離脱に応じて更新することが想定されるため，グループメンバー間で同期しながらKEKを更新する方法が研究テーマの1つとなっている．このほかにもIETFでは，IPsec（Internet Protocol security）を拡張し，TEKを用いてマルチキャスト配信データ暗号化を実現するためのデータ暗号化プロトコルを規定している．

IETFのグループ管理アーキテクチャは，鍵配布によって交わされる情報を基にアカウンティング（課金やユーザのアクセス情報の収集）を実現することが可能である．しかし，グループへの加入／離脱と同期して，正確にアカウンティングを実現することができないという問題があった．さらに，IPマルチキャストの匿名モデルでは，任意のクライアントがデータ受信を要求できるため，手当たり次第にグループに加入するマルチキャストのサービス拒否攻撃（DoS：Denial of Service）の問題が存在していた．マルチキャストDoSは，マルチキャスト配信経路を不必要に構築することが可能であるため，ネットワーク全体に影響を及ぼす深刻な問題となる．

著者らは，以上のような問題点に着目し，IETFのグループ鍵管理アーキテクチャと各種プロトコルを拡張したクライアント認証＆グループ鍵配信プロトコル（AKDP：receiver Authentication and group Key Delivery Protocol）を提案した．この提案プロトコルでは，グループ鍵の配信とともに，クライアントのグループへの加入，離脱に同期したクライアント認証を行うことが可能であるため，正確なアカウンティングを実現することができる．また，クライアントの認証を実行することにより，権限を持つクライアントのみのグループへの加入を許可するため，結果としてマルチキャストのDoSへの対処が可能となる．AKDPは，マルチキャスト用のグループ管理プロトコル（IGMP：Internet Group Management Protocol）をベースに，クライアント認証とグループ鍵配信機能を追加したプロトコルであり，クライアント，AKDPを実装したルータ（AKDPルータ），およびクライアントの認証情報やKEKを保持する鍵管理サーバが連携して動作する（図5）．そのため，AKDPの提案に際しては，処理時間によるサービス性の低

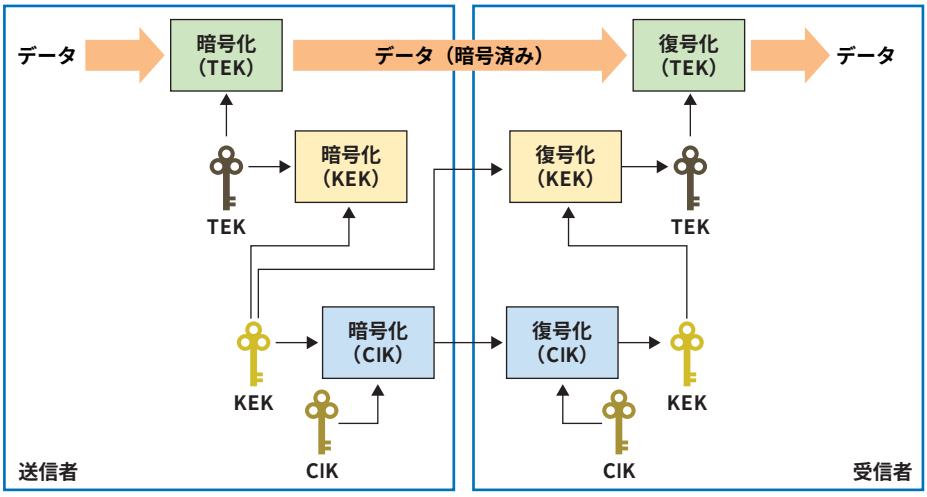


図4　グループ鍵管理アーキテクチャ

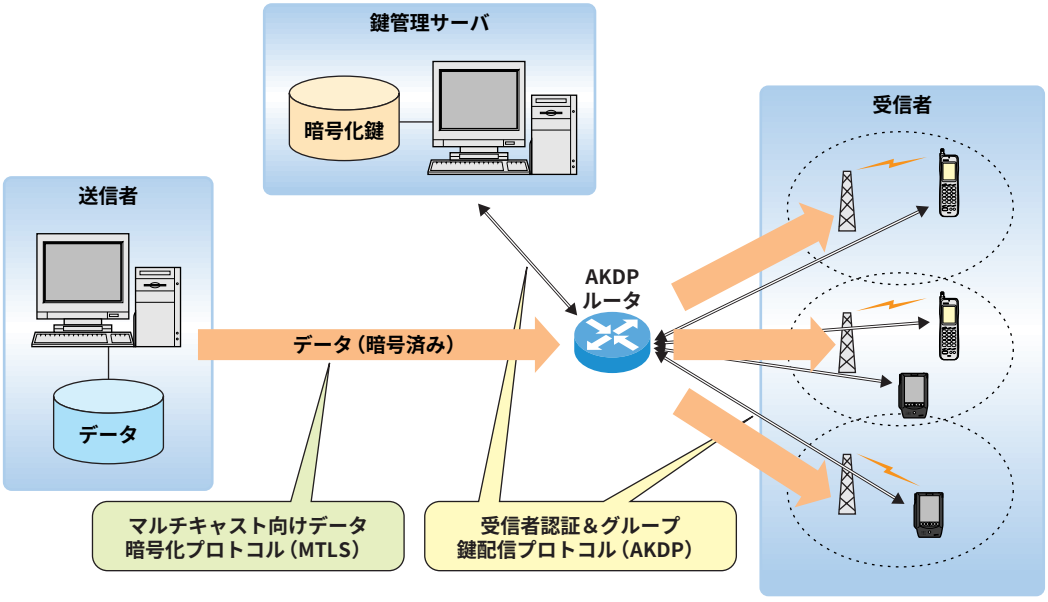


図5　マルチキャストセキュリティアーキテクチャとプロトコル

下や，クライアント数が増加した場合のスケーラビリティの問題について検証することが重要であった．筆者らは，プロトタイプソフトウェアによりAKDPの一連のクライアント認証，およびグループ鍵の配信処理が数百ミリ秒で完了することを検証し，さらに一般的に考えうるクライアント数のAKDPルータへの同時アクセス（1ms間に256台のアクセス）に関しても問題が無いことを確認した[5]．

また著者らは，データ暗号化プロトコルについても任意のアプリケーションで利用可能なトランスポート層のマルチキャスト向けデータ暗号化プロトコルであるMTLS（Multicast Transport Layer Security）を新たに提案し，実証検証用プロトタイプシステムの試作と性能評価によりその実現性を立証した[6]．MTLSは，IPマルチキャストで用いられるトランスポート層であるUDP上の暗号化プロトコルを規定しており，任意のUDPアプリケーションに適用でき，かつ移動通信向けの軽量なプロトコルを規定していることが特徴である．プロトタイプシステムにおけるMTLSの性能評価では，3.839Mbit/sの最大スループットが得られ，3G携帯電話網やIEEE802.11bのWLAN上で提供する映像配信サービスを対象とした場合に，MTLSは十分実用に耐えうる事を確認した．

上記のとおり，IPマルチキャストでは，ユニキャストで用いられるセキュリティ技術をそのまま適用できないため，IPマルチキャストを対象とした技術検討が多数行われてきた．本稿で述べられなかった例として，受信データの再配布を防止するためのマルチキャスト用電子透かしや，悪意のあるユーザがデータを送信するのを防止するサーバアクセス制御，正しいサーバからデータを送信していることを検証するための送信元認証などの研究も行われている．IPマルチキャストを用いて放送型データ配信サービスを実現する上では，守るべきデータのコストやコンテンツプロバイダの要求条件および制約条件を考慮して，総合的な見地から必要なセキュリティ技術を選択し，適用することが重要である．

4. ユーザに最適なデータを提供するマルチキャストセッション管理

IPマルチキャストにおいて，クライアントは受信を所望するグループ（マルチキャストアドレス）を選択し，当該グループへの加入手続きを実行することでデータ受信を開始する．そのため，クライアントは配信データに関するメタ情報（セッション情報）をあらかじめ入手し，受信を所望するグループを選択する必要がある．しかし，携帯電話や携帯情報端末（PDA：Personal Digital Assistant）のように，入力，表示機能に制限のあるモバイル端末を用いる場合には，膨大なセッション情報から適切なグループを選択することはユーザにとって負担となる．特に，位置情報などのモバイル端末の特徴を活かしたサービスと連携する場合には，ユーザを取り巻く環境がめまぐるしく変化し，その都度受信を希望するデータも頻繁に変化することが想定されるため，適切なグループを選択するためのユーザへの負担はさらに顕著になる．著者らはこのような課題に着目し，グループの選択処理を他の装置で代行して行うための仕組みを提案した[7]．

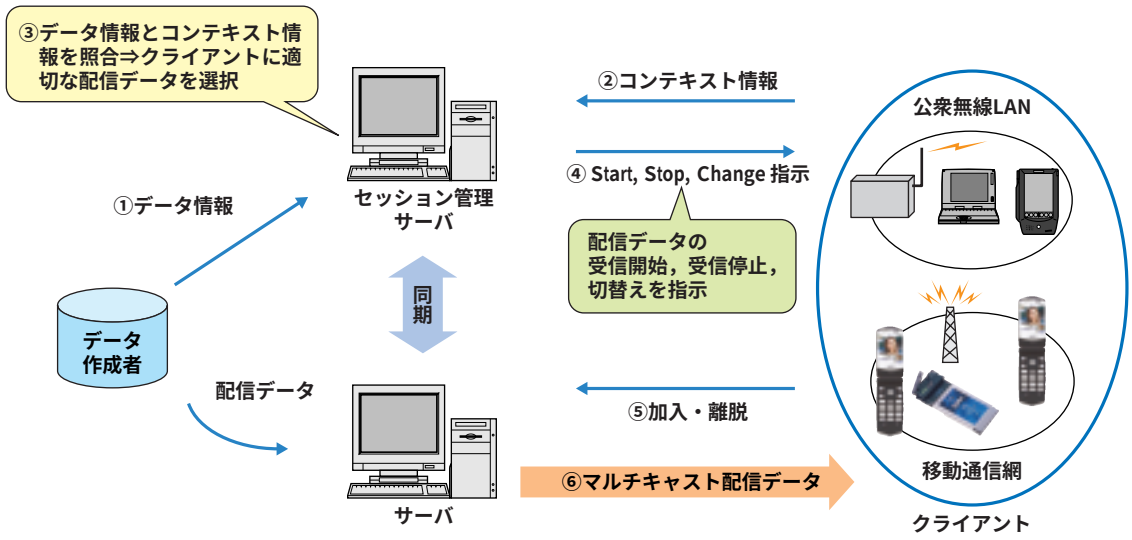


図6　マルチキャストセッション管理の制御の流れ

この提案方式では，配信データおよびセッション情報を保持するネットワーク側でグループの選択処理を行う．そのために著者らは，セッション管理サーバを新たに定義した（図6）．セッション管理サーバは，①コンテンツプロバイダなどのデータ作成者から配信データ情報（データの名称や概要などのセッション情報と配信時刻などの配信条件を含む）を収集し，②さらにクライアントやネットワーク装置などからコンテキスト情報*2（趣味嗜好などのユーザに関する情報，温度や天気など周囲環境に関する情報を含む）を収集する．その後，セッション管理サーバは，③収集したデータ情報とコンテキスト情報を照合し，クライアントに対して適切な配信データを選択する．その後，セッション管理サーバは，④当該データを配信するグループの受信開始（Start），グループの受信停止（Stop），新旧グループの切替え（Change）のいずれかをクライアントに対して指示する．当該指示を受信したクライアントは，⑤通常のIPマルチキャストの動作に従い，グループの受信開始，受信停止，切替えを自動的に実行することによって，⑥変更後のマルチキャストアドレスで配信されるデータの受信が可能となる．以上のように，提案方式は⑤，⑥ではIPマルチキャストの動作をそのまま踏襲し，それ以外①～④の機能を新たに提供することを特徴としている．

このようなサーバ主導のグループ切替えを利用したアプリケーションの一例として，ユーザの位置情報とユーザ趣味に応じたデータ切替えのアプリケーションがある．このアプリケーションでは，ユーザのコンテキスト情報として，RFID（Radio Frequency IDentification）タグや全地球測位システム（GPS：Global Positioning System）を利用することによって得られる位置情報と，ユーザによりあらかじめ登録された趣味情報を利用することの双方によって，ユーザが移動しながらその地域に密着した配信データを自動的に切り替えながら受信することができる．

この提案方式では，利用するコンテキスト情報の内容や，データの配信条件を自在に管理することで，新しいデータ配信サービスへの応用が期待できる．特に広告配信を伴うデータ配信サービスの場合には，その配信ターゲットを絞り込むことが重要であるため，本提案方式のようにクライアントが受信するデータを適切に選択する技術が必要である．

5. あとがき

マルチキャストに関する近年の研究開発と国際標準化によって，商用サービスの実現に向けた技術的課題が解決されつつある．放送型データ配信サービスを支える関連事業社間のビジネスモデル構築や，著作権などの法律に関わる政策的な課題も数多く残されてはいるが，マルチキャストが新たな通信メディアを創出する基盤技術となることを期待したい．

文　献

[1] 3GPP:“Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description,” 3GPP TS 23.246, 2004.
[2] 木下真吾：“リライアブルマルチキャスト技術の最新動向，”信学論文誌，Vol.J85-B，No.11，2002.
[3] 山内長承，ほか：“高信頼同報バルク転送機構，”情処論文誌，Vol.39，No.6，1998.
[4] 鈴木偉元，ほか：“無線LANでのマルチキャスト誤り回復方式の

＊2　コンテキスト情報（context information）：エンティティの状況を特徴付けるために使用可能なあらゆる情報．エンティティはユーザとアプリケーションの相互作用に関連すると見なされる人，場所，またはオブジェクトで，ユーザとアプリケーション自体も含む．

比較評価，”DICOMO2003，Vol.2003，No.9，2003.
[5] 上野英俊，ほか：“マルチキャスト通信のためのアクセス制御＆グループ鍵配信プロトコル，”第二回情報科学技術フォーラム，2003.
[6] 上野英俊，ほか：“マルチキャスト通信のためのトランスポート層データ暗号化プロトコルの提案と実装，”電子情報通信学会 技術研究報告，Vol.103，No.122，2003
[7] 田中希世子，ほか：“コンテキスト情報を用いたマルチキャスト配信アーキテクチャの提案，”DICOMO2003，Vol.2003，No.9，2003.

用 語 一 覧

3GPP：3rd Generation Partnership Project
ACK：ACKnowledgement（肯定応答）
ADSL：Asymmetric Digital Subscriber Line
AKDP：receiver Authentication and group Key Delivery Protocol（クライアント認証＆グループ鍵配信プロトコル）
ARQ：Automatic Repeat reQuest（自動再送要求）
BGMP：Border Gateway Multicast Protocol
CIK：Client Individual Key（クライアント個別鍵）
DoS：Denial of Service（サービス拒否攻撃）
DVMRP：Distance Vector Multicast Routing Protocol
FEC：Forward Error Correction（前方誤り訂正）
GPS：Global Positioning System（全地球測位システム）
IETF：Internet Engineering Task Force
IGMP：Internet Group Management Protocol（グループ管理プロトコル）
IP：Internet Protocol
IPsec：Internet Protocol security
KEK：Key Encryption Key（鍵暗号化鍵）
LAN：Local Area Network
MBMS：Multimedia Broadcast Multicast Service
MLD：Multicast Listener Discovery
MSDP：Multicast Source Discovery Protocol
MTLS：Multicast Transport Layer Security
NACK：Negative ACKnowledgement（否定応答）
P2P：Peer-to-Peer
PDA：Personal Digital Assistant（携帯情報端末）
PIM：Protocol Independent Multicast
RFID：Radio Frequency IDentification
RM：Reliable Multicast（高信頼マルチキャスト）
RMTP：Reliable Multicast Transport Protocol
RTP：Real-time Transport Protocol
TCP：Transmission Control Protocol
TEK：Traffic Encryption Key（トラヒック暗号化鍵）
UDP：User Datagram Protocol
WLAN：Wireless Local Area Network（無線LAN）
XCAST：eXplicit multiCAST