Pedi概説書

～ EDIメッセージ通信サービスの概要 ～

平成 6 年11月

財団法人　日本情報処理開発協会

産業情報化推進センター

KEIRIN 00 この資料は、競輪の補助金を受けて作成したものです。

はじめに

企業内・外において、各種データ端末やＯＡ端末を通信回線で結び、電子メールサービスを利用して個人間のメールをやり取りするユーザがかなり増えてきている。通常の郵便ではハガキや手紙を人や郵便車両が物理的に運んでいるが、電子メールサービスではコンピュータを介して利用者が送りたい情報を蓄積・転送し、利用者の要求条件（同報・優先度・通知要求など）に基づいてあて先に届けるのが特徴である。

電子メールサービスの利用形態には、上記のような人間と人間の間の個人間メール（以下、メールをメッセージと呼ぶ）をやり取りする形態と、人間と機械（コンピュータ）の間または機械と機械の間でコンピュータ処理が施されるメッセージ（商品伝票などを扱ったメッセージ）をやり取りする形態が考えられる。

ここで、１９８４年に勧告されたＭＨＳ(Message Handling Systems)は前者の人間と人間の間の形態を提供し、１９８８年に勧告されたＭＨＳをベースに提供される『Ｐｅｄｉ(EDI Messaging protocol：ＥＤＩメッセージ通信プロトコル）』はＥＤＩメッセージを扱う後者の、人間と機械（機械と機械）の間の形態を提供する。

コンピュータ処理が施されるメッセージの一つとして、ＥＤＩ（電子データ交換）メッセージがある。商取引を行う際に発生する各種帳票（注文書・納品書など）をペーパーベースで交換するのではなく、通信回線を介してコンピュータ間で直接データ交換を行うのがＥＤＩである。ＥＤＩは、ペーパレス化による事務処理の効率化、在庫管理の充実による流通コスト削減および労働時間の短縮などに役立てられている。

ＭＨＳは、当初、個人間メッセージに係わる電子メールサービスを提供する通信プロトコルとして、１９８４年にＩＴＵ－ＴＳ（旧ＣＣＩＴＴ）により勧告（８４年版ＭＨＳ）されたが、その後、ＯＳＩ参照モデルとの整合性を高めた改訂版が１９８８年に勧告（８８年版ＭＨＳ）され、個人間メッセージに加え汎用的なメッセージも取り扱えることが可能となった。８８年版ＭＨＳは、さらに、その後も機能の拡張・変更が行われ、１９９２年に最新の勧告（９２年版ＭＨＳ）がなされている。

ＩＴＵ－ＴＳの８８年版ＭＨＳと同等なＩＳＯの規格は、メッセージ指向型文書交換システム、すなわち、ＭＯＴＩＳ（Message-Oriented Text Interchange Systems)として知られている。また、Ｐｅｄｉは８８年版ＭＨＳ上でＥＤＩメッセージを扱えるよう拡張した通信プロトコルであり、１９９１年３月にＩＴＵ－ＴＳによりＸ．４３５／Ｆ．４３５として勧告されている。

ユーザはＰｅｄｉを利用することにより、1) 国連で承認されているＥＤＩデータ構文規則の「ＥＤＩＦＡＣＴ」に準拠したメッセージ・フォーマットなどを、国際的に規約が統一されている８８年版ＭＨＳ上で扱えるため、国際標準に準拠したＥＤＩ環境を容易に構築できる、2) 日本国内標準であるＥＤＩデータ構文規則の、「ＣＩＩ標準」に準拠したメッセージ・フォーマットもこの通信システムで送信可能であることから、国内標準への親和性もある、3) 個人間メッセージ用の通信システムとＥＤＩメッセージ用の通信システムを分けずに、通信システムを統合できる、などのメリットがある。

Ｐｅｄｉは、関係方面において非常に注目されており、当センターにおいて過去に実施した通信プロトコルに関するアンケートにおいて、その関心度が常に上位であることからも裏付けでき

る。

当センターでは、このように、各方面で関心の高いＰｅｄｉを特定テーマとして取り上げ、Ｐｅｄｉが、今後、業界標準として期待されるＭＨＳベースのＥＤＩ向け新通信手順として利用可能かどうかを調査研究するために、まず『Ｐｅｄｉ概説書』として取りまとめた。

本書の構成は、二章から成る本編と付録から構成されている。第１章では、Ｐｅｄｉの通信プロトコルを実現している、８８年版ＭＨＳについてその機能概要を説明して基本的理解を促し、その上でＰｅｄｉサービスの概要について説明する。

第２章では、Ｐｅｄｉサービスについてより深く理解して頂くために、提供される各種サービスについて項目ごとに説明する。

また、付録では、読者の皆様の関心が高いと考えられる「９２年版ＭＨＳの紹介」と「Ｈ手順とＰｅｄｉの比較」などを取り上げて説明する。

以上のような内容を持つ本書が、Ｐｅｄｉをご理解して頂くために活用して頂けることを念願する次第である。

なお、本書の執筆に当たり、「Ｐｅｄｉ概説書編集ＷＧ」、「新手順検討委員会」の委員各位および㈱情報処理相互運用技術協会（ＩＮＴＡＰ）のご協力に深く感謝申し上げる次第である。

財団法人　日本情報処理開発協会
産業情報化推進センター

Ｐｅｄｉ概説書編集ＷＧ委員名簿

区　分	所　属　等		氏　名
主　査	日本電信電話株式会社	サービス生産本部　ユーザシステム部 ﾊﾟｹｯﾄ通信ｼｽﾃﾑﾌﾟﾛｼﾞｪｸﾄｸﾞﾙｰﾌﾟ　主任技師	渡辺　　徹
委　員	九州日本電気ソフトウェア株式会社	基本ソフトウェア事業部 第１開発部　主任	草木　正美
	富士ゼロックス株式会社	ドキュメントシステム開発センター サービスコア開発部	四方田　正夫
	富士通株式会社	オープンソフトウェア事業部 第４開発部	鈴木　真二
	日本電気株式会社	基本ソフトウェア事業本部 基本ソフトウェア事業部　方式開発部	伊東　真理
ｵﾌﾞｻﾞｰﾊﾞ	(財)情報処理相互運用技術協会　[INTAP]	総務部 部長代理	小俣　光夫
	日本ｱｲ・ﾋﾞｰ・ｴﾑ・ｼｽﾃﾑｽﾞ・ｴﾝｼﾞﾆｱﾘﾝｸﾞ株式会社	プロジェクト推進部　第一ﾌﾟﾛｼﾞｪｸﾄ推進課 主任ｼｽﾃﾑｽﾞ・ｴﾝｼﾞﾆｱﾘﾝｸﾞ・ｽﾍﾟｼｬﾘｽﾄ	森　　玲子
事務局	(財)日本情報処理開発協会	産業情報化推進センター ユーザー環境課課長	藤田　雅範
	(財)日本情報処理開発協会	産業情報化推進センター ユーザー環境課　研究員	向山　洋二

目　　次

第 1 章

機　能　概　要

1．　機能概要

Ｐｅｄｉ（EDI Messaging protocol：ＥＤＩメッセージ通信プロトコル）は、１９８８年に勧告されたＭＨＳ（Message Handling Systems）をベースに、ＥＤＩデータを取り扱えるよう拡張した通信プロトコルである。よって、本章では、まずＰｅｄｉのベースになっている８８年版ＭＨＳについて説明し、次にＰｅｄｉの概要について説明する。

1．1　ＭＨＳの機能概要

1．1．1　電子メールシステムの概要

通常電子メールシステムは、文字列や文書や音声データなどをあて先に送り届ける蓄積交換型の通信システムである。利用者から発信されたメールは、電子メールシステムによってあて先のメールボックスに配信され保管されているので、受信者は自分の都合のよい時にメールボックスから取り出してメールを見ることができる。

電子メールシステムでは、以下のようなサービスが提供されている。

- 同報 …… 複数の相手に同時に発信する。
- 優先度 …… 配信の優先度を指定する。
- 通知 …… メールがあて先に届いたとき、またはエラーになったときに、そのことを発信者に通知する。また、受信者が処理したことを通知する。
- 往復メール …… 発信するメールに対して返事を要求する。
- 主題 …… メールに表題を付ける。
- 秘密度 …… 私信／親展／社外秘などを指定する。

また、以下の情報は電子メールシステムが自動的に情報を生成し、利用者に通知する。

- 発信者
- 発信時刻
- 配信時刻
- メールに対する識別子

本節では、ＩＳＯやＩＴＵ－ＴＳ（旧ＣＣＩＴＴ）によりＯＳＩ準拠の電子メールシステムとして規定されたＭＨＳについて説明する。なお、ＭＨＳではメールのことをメッセージと呼ぶ。

1．1．2　標準化活動

個々に存在する電子メールシステムを相互に接続し、統合的な利用を図るため、ＩＴＵ－ＴＳ（電気通信標準化センタ）とＩＳＯ（国際標準化機構）が相互のリエゾンを図りながら標準化活動を進めた。

ＩＴＵ－ＴＳでは、ＭＨＳ(Message Handling Systems)として検討を進め、１９８４年に発表

した勧告（レッドブック）と１９８８年の勧告（ブルーブック）の二つの基本標準がある。ＩＳＯでは、１９８８年にＤＩＳ(Draft International Standard)版ＭＯＴＩＳ(Message-Oriented Text Interchange Systems)を作成した。

１９８４年版ＭＨＳとＤＩＳ版ＭＯＴＩＳは機能が類似していたため、内容を調整した結果、１９８８年版ＭＨＳとＩＳ(International Standard)版ＭＯＴＩＳとは、一部の例外を除いて同一になった。ＩＴＵ－ＴＳとＩＳＯおよびそれを翻訳したＪＩＳの規格の一覧と対応関係を表1.1- 1に示す。

表1.1- 1　ＭＨＳの規格の一覧

内　　容	ＩＴＵ－ＴＳ	ＩＳＯ	ＪＩＳ
システムおよびサービス概説	Ｘ．４００	ＩＳＯ* 10021-1	ＪＩＳ　Ｘ5801
全体アーキテクチャ	Ｘ．４０２	ＩＳＯ　10021-2	ＪＩＳ　Ｘ5802
抽象サービス定義規約	Ｘ．４０７	ＩＳＯ　10021-3	ＪＩＳ　Ｘ5803
メッセージ転送システム：抽象サービス定義および手順	Ｘ．４１１	ＩＳＯ　10021-4	ＪＩＳ　Ｘ5804
メッセージ格納：抽象サービス定義	Ｘ．４１３	ＩＳＯ　10021-5	ＪＩＳ　Ｘ5805
プロトコル仕様	Ｘ．４１９	ＩＳＯ　10021-6	ＪＩＳ　Ｘ5806
個人間メッセージ通信システム	Ｘ．４２０	ＩＳＯ　10021-7	ＪＩＳ　Ｘ5807
ＥＤＩﾒｯｾｰｼﾞﾝｸﾞ･ｼｽﾃﾑ	Ｘ．４３５	－	－

（* ＩＳＯ／ＩＥＣ　10021:1990）

１９８４年版ＭＨＳに対する１９８８年版ＭＨＳの主な機能追加は以下の点である。

・メッセージ格納(MS)
・物理的配達との連携
・ディレクトリシステムとの連携
・安全保護の強化

通常、これらの標準に準拠した製品を開発するためには、基本標準に加えて、製品のサポート範囲を規定する実装規約化の作業が必要で、各国／地域を代表する機関で行われている。ＩＳＯでは各地域の実装規約のハーモナイズが行われており、国際実装規約（ＩＳＰ：International Standardized Profile）が作成されている。また、国内の実装規約の作成は㈶情報処理相互運用技術協会（ＩＮＴＡＰ）で行われており、第２版では以下のように体系化されている。

ＡＰ２１　　ＭＨＳ　個人間メッセージ通信
　ＡＰ２１１　ＵＡ　＋　ＭＴＡ　（Ｐ１とＰ２）
　ＡＰ２１２　ＭＴＳアクセス　（Ｐ３とＰ２）
　ＡＰ２１３　ＭＳアクセス　（Ｐ７とＰ２）

第２版では、ＭＴＳアクセスはプロフィル番号の割り当て(AP212) のみ行われ、具体的な規約は作成されていないが、次版ではそれが含まれた形でＩＳＰ準拠の規格が計画されている。

1. 1. 3　機能モデル

ＭＨＳでは電子メールシステム（メッセージ通信システム）の基本的な構造を図1.1- 1のようにモデル化している。

(1) 機能オブジェクト

① ＵＡ

利用者機能体（ＵＡ：User Agent）は、人間や応用プログラムに代わってメッセージの発信や受信を行う。

② ＭＴＡ

メッセージ転送機能体（ＭＴＡ：Message Transfer Agent）は、ＵＡから発信されたメッセージやほかのＭＴＡから転送されてきたメッセージを、ＵＡ／ＭＳに配信したりＭＴＡに転送したりする。

メッセージ転送システム（ＭＴＳ：Message Transfer System ）は、一つ以上のＭＴＡから構成され、メッセージの蓄積交換を行って、メッセージを目的のあて先まで配信する。

③ ＭＳ

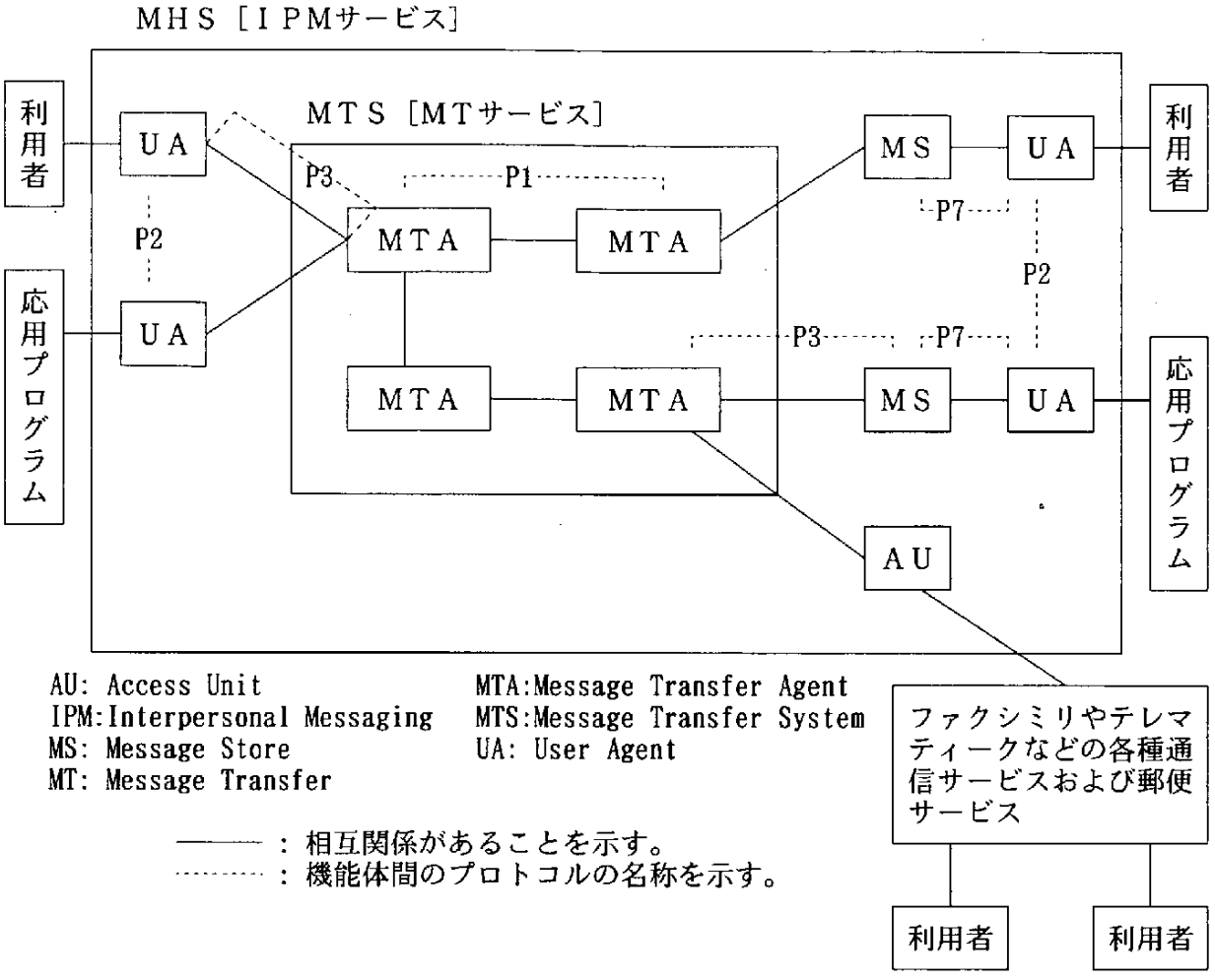
メッセージ格納（ＭＳ：Message Store ）は、メッセージの保管や検索する機能をＵＡに提供する。また、ＵＡからのメッセージの発信をＭＴＡに中継したり、メッセージが配信された時にＵＡにその旨を通知する（警報機能）。

④ ＡＵ

アクセス単位（ＡＵ：Access Unit ）は、ＭＨＳの世界のメッセージをその外の世界（例えば通常の郵便など）に配信するための機能体である。通常の郵便への配信に使用する物理的配達アクセス単位（ＰＤＡＵ：Physical Delivery Access Unit ）は、ＡＵの例の一つである（ＰＤＡＵについては「２．１１　物理的配達サービス」参照）。

(2) プロトコル

ＭＴＡ間のプロトコル（通信規約）をＰ１、ＵＡ間のプロトコルをＰ２、ＭＴＡとＵＡ／ＭＳとの間のプロトコルをＰ３、ＭＳとＵＡとの間のプロトコルをＰ７とそれぞれ呼んでいる（図1.1- 1）。



P1：MTA間でメッセージを転送するためのプロトコル(MTS転送プロトコル)。MTAでは、メッセージ内の封筒(P1プロトコル情報)を参照および更新しながら、メッセージ転送を行う。

P2：個人間メッセージのフォーマットを規定したプロトコル。

P3：UA/MSがMTAにメッセージを発信したり、MTAがUA/MSにメッセージを配信したりするためのプロトコル(MTSアクセスプロコトル)。

P7：UAがMSからメッセージを検索したり、UAがMSを介してメッセージを発信したりするためのプロトコル(MSアクセスプロトコル)。

図1.1-1　MHSの機能モデル

(3) 実現方法

ＵＡ／ＭＴＡ／ＭＳをどのように組み合わせてソフトウェア／ハードウェアで実現するかは、ＭＨＳでは特に規定されていない。同一の計算機内に異なる機能体（例えばＵＡとＭＴＡ）を実現してもよく、この場合、機能体間のインタフェースは任意である。図1.1- 2に例を示す。図1.1- 2において、ＵＡを使用するのは、利用者（人間）または応用プログラムである。利用者の場合は、キーボードやディスプレイ装置を使用して対話しながら、メールのデータを入力して発信したり、受信したメールを確認したりする。また、応用プログラムの場合、定型的な文書の一部を書き替えて自動的に発信したり、受信したメールを特定の場所に格納したり印刷したり内容のデータ処理を行ったりする。

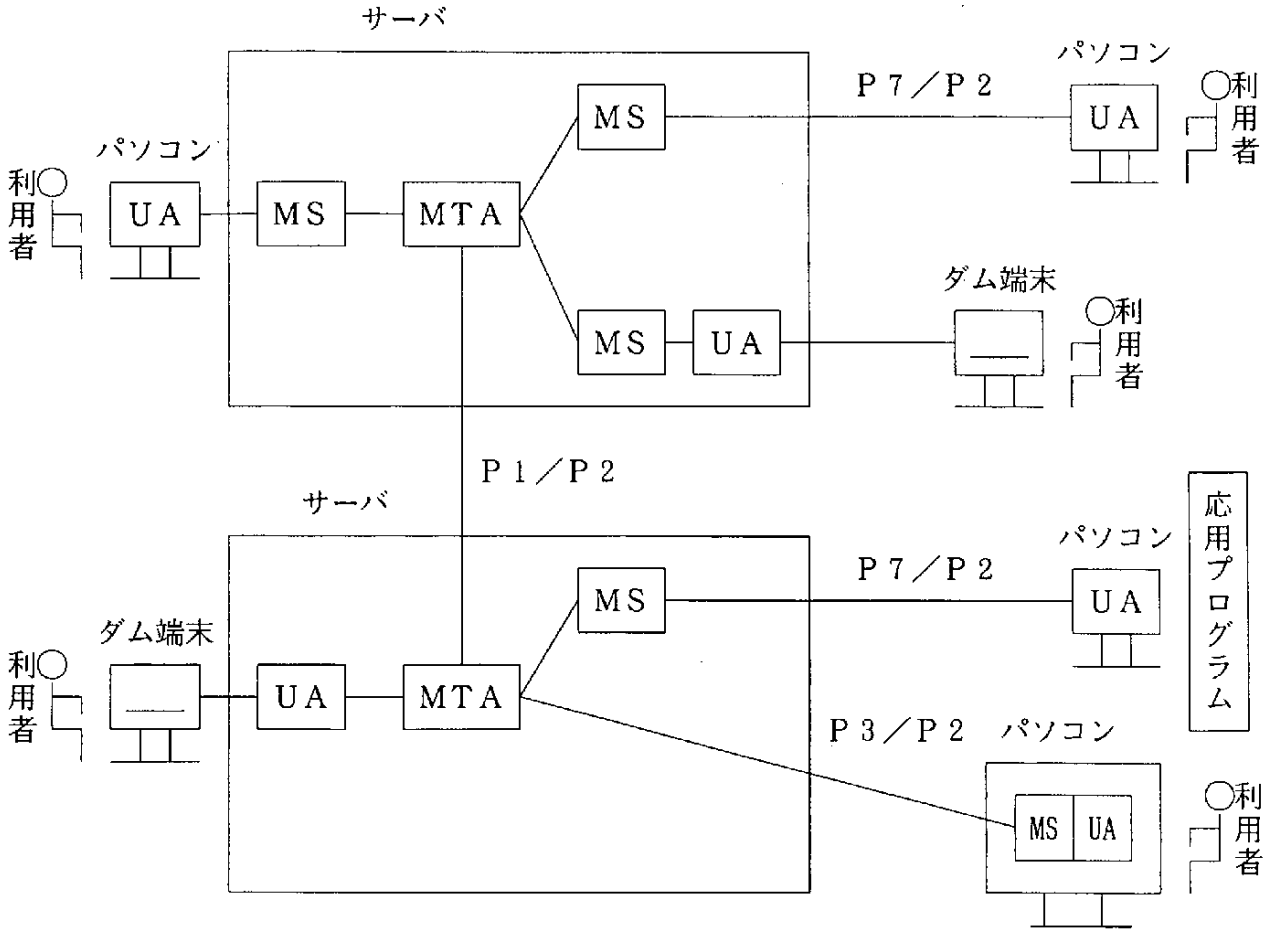


図1.1- 2 機能モデルと実現製品との対応例

1. 1. 4　管理領域

多数のＭＨＳネットワークが存在する場合、ユーザはそれらのＭＨＳネットワークの中で一意のネットワークアドレスを所有できることが望ましい。図1.1- 3に示すとおり、違うＭＨＳネットワークを利用しているユーザ同士がメッセージを交換することを考えれば、世界中で一意のネットワークアドレスの必要性が理解できる。

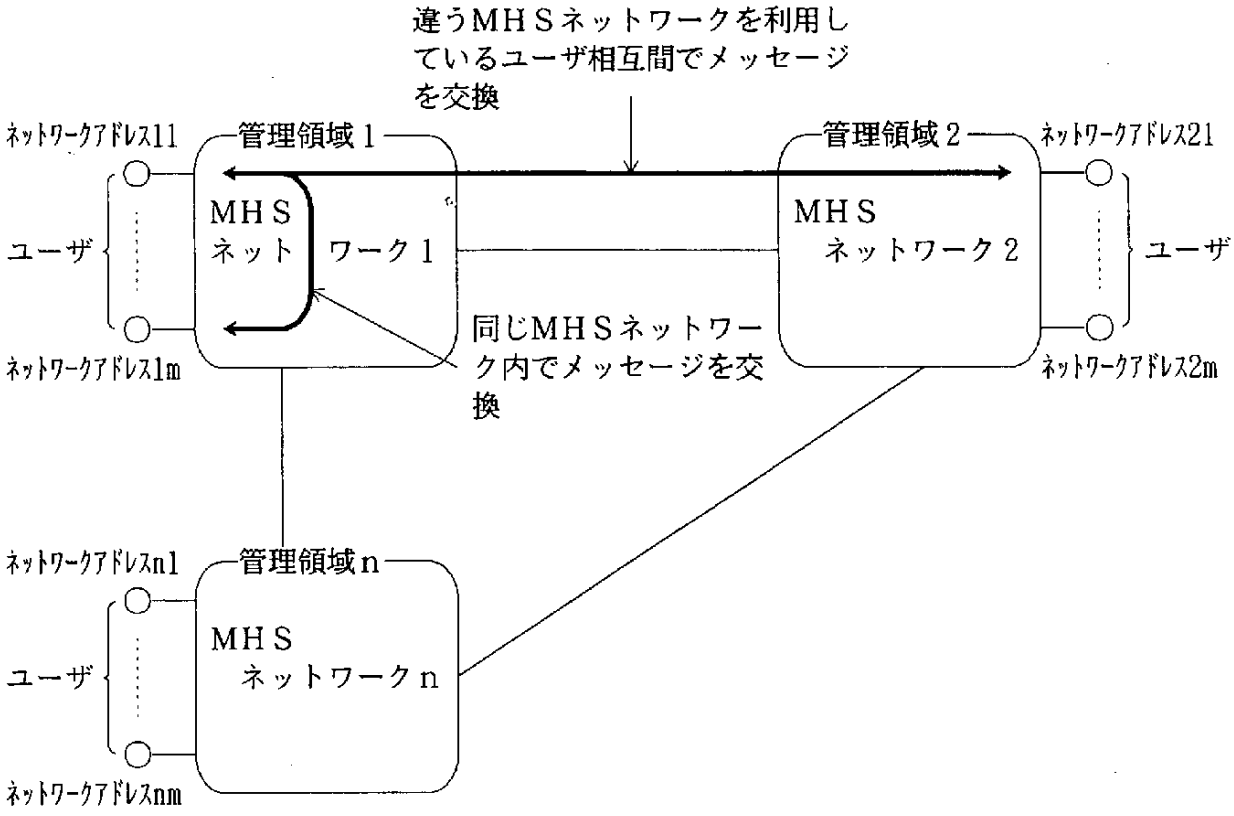


図1.1- 3　管理領域の概念

ユーザは、ＭＨＳサービスの提供を受ける場合、どのネットワークに加入するかを決定し、そこで、ネットワークアドレスを取得することとなる。上図を例に採ると、例えばＭＨＳネットワーク１を利用するならば、ＭＨＳネットワーク１の管理下にてアドレスが決定される。このアドレスが決定される領域を管理領域という。

管理領域は、そのネットワークを管理する管理者のレベルにより二つに大別できる。管理者が公衆サービスの提供を管理する主官庁の場合を主管機関管理領域(ADMD:ADministration Management Domain)、主官庁以外の組織の場合を私設管理領域(PRMD:PRivate Management Domain)と呼ぶ。日本では、ＮＴＴ等の電気通信事業者が提供する公衆ＭＨＳネットワークを識別するためにＡＤＭＤ名が使われる。ＡＤＭＤ名は、郵政省への登録が必要である。一方、ＡＤＭＤ以外の私設ＭＨＳネットワークを識別するためにＰＲＭＤ名が使われる。ＰＲＭＤ名は、ほかのＭＨＳネットワークへ接続を行う場合、郵政省へ登録することが望ましい。

図1.1- 3で示したＭＨＳネットワークはＭＨＳ機能モデル（ＭＴＡ，ＵＡ，ＭＳなど；図1.1- 1参照）により構成される。つまり、ＭＨＳネットワークを運用する場合（ＭＴＡ，ＵＡ，ＭＳを運用する場合）、ＭＴＡ，ＵＡ，ＭＳはそれを管理するどこかの管理領域に属することとなる。

管理領域には少なくとも一つのＭＴＡが必要で、ＵＡとＭＳは存在しなくてもよい。図1.1- 4にＭＨＳ機能体（ＭＴＡ，ＵＡ，ＭＳ）とＡＤＭＤ／ＰＲＭＤの関係を示す。この図で網かけ部分は一つのシステムを示し、その中に例えばＭＴＡとＵＡが含まれている場合は、一つのシステムにＭＴＡとＵＡが共存することを示す。

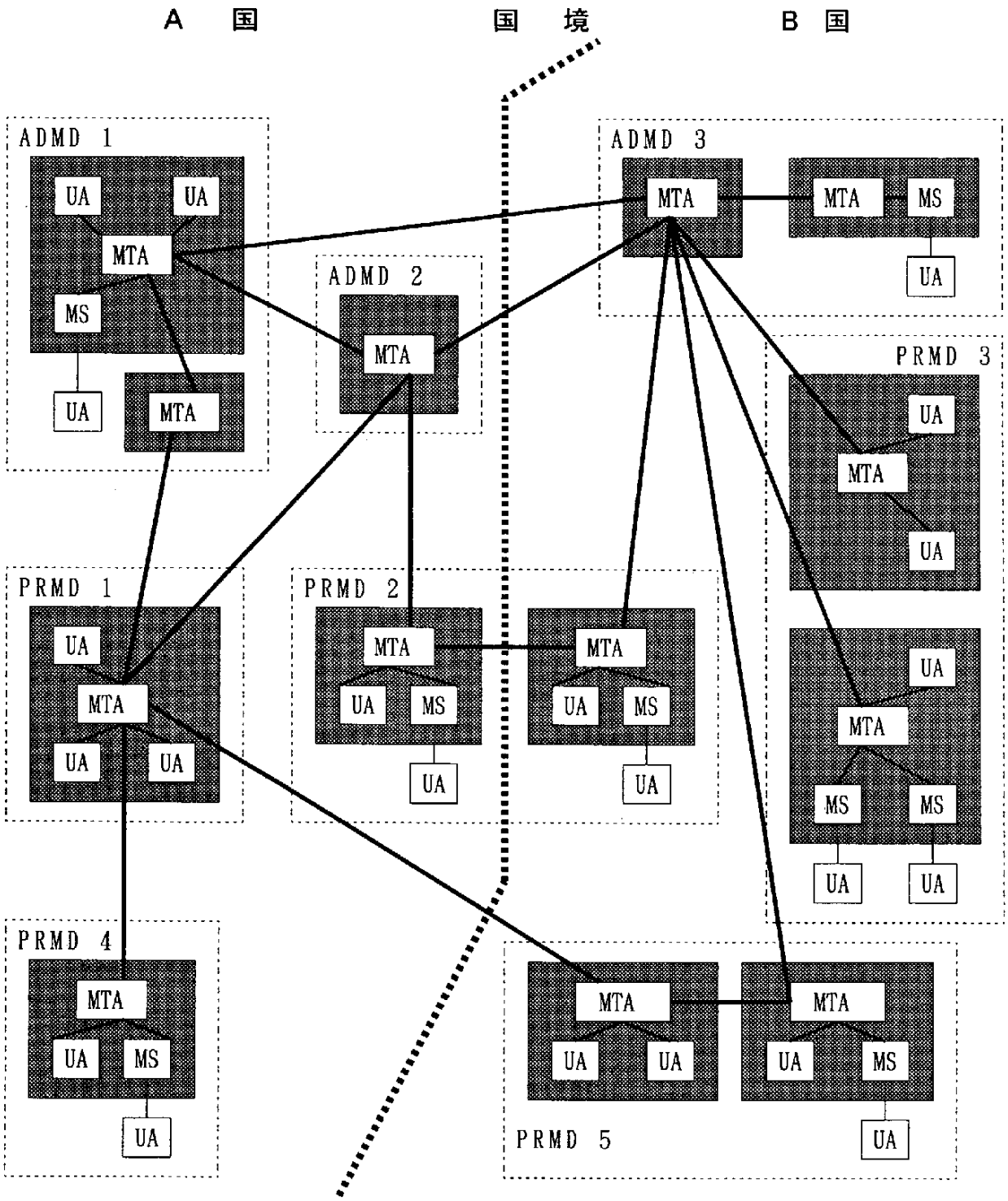


図1-1．4　主管機関管理領域（ＡＤＭＤ）と私設管理領域（ＰＲＭＤ）

1. 1. 5　アドレスと経路選択

ＭＨＳでは、利用者の識別をＯ／Ｒ名により行う。このＯ／Ｒ名は、さらに多くのパラメタから構成され、その中の要素により、利用者が所属するＭＨＳの管理領域などがわかるようになっている。また、１９８８年版ＭＨＳでは、ディレクトリ名も利用者の識別に使用可能となった。以下では、Ｏ／Ｒ名の構成、メッセージ配信時の経路選択の方法について述べる。

(1)　Ｏ／Ｒ(Originator/Recipient)名

Ｏ／Ｒ名は、Ｏ／Ｒアドレスと呼ぶＭＨＳが規定する形式とＩＴＵ－Ｔ勧告Ｘ．５００（ＩＳＯ／ＩＥＣ　９５９４）が規定するディレクトリ名から構成される。Ｏ／Ｒアドレスは、さらに幾つかのパラメタから構成される。表1.1- 2にＯ／Ｒ名の構成を示す。

表1.1- 2　Ｏ／Ｒ名の構成

パラメタ	概要
Ｏ／Ｒアドレス	ＭＨＳが規定する形式。標準属性と領域定義属性から成る。
標準属性リスト	ＭＨＳで共通に定義されるパラメタ。
国名	管理領域のある国名。
主管機関管理領域名	主管機関管理領域（ＡＤＭＤ）の名称。
私設領域名	私設管理領域（ＰＲＭＤ）の名称。
ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ	ITU-T勧告X.121/E.163/E.164が規定する数字列。
端末識別子	端末番号。
組織名	会社などの組織名称。
数字利用者識別子	管理領域内において数字で付与する一意な識別子。
個人名	個人の氏名。姓名などのパラメタを別々に指定する。
姓	氏名の姓。
名	氏名の名。
頭文字	氏名の頭文字。
世代名	世代名（２世、Ｊｒなど）。
部門名	組織等の部門名（複数指定可能。部課等の指定が可能）。
テレテックス個人名	漢字等で個人名を指定可能＊１。設定項目は、個人名に同じ。
テレテックス部門名	漢字等で部門名を指定可能＊１。設定項目は、部門名に同じ。
領域定義属性リスト	個々の管理領域が独自に定義する形式。
ディレクトリ名	Ｘ．５００が規定する形式。

注）＊１：この二つのパラメタ以外は、英数字しか使用することができない。

MHSでは、表1.1-2に示される全てのパラメタを使用する必要はなく、経路選択のために必要な国名、主管機関管理領域名（必要があれば、私設領域名）が設定必須であるほかは、管理領域ごとに使用するパラメタを決めることができる（「(3) 経路選択」参照）。しかし、全く使用方法が管理領域単位で異なる場合には、相互接続を行う際の相手システムのあて先を指定することができない等の問題が発生するため、１９８８年版勧告では、O／Rアドレスの個々の属性の組み合わせとして、四種類の形式を定めている（表1.1-3）。それぞれの形式では、指定が必須の属性と、任意に指定可能な属性に分けている。

参考：１９８４年版MHS勧告でもO／Rアドレスの属性の組み合わせを規定しているが、１９８８年版のものとは、名称などが異なる。また、１９８４年版のO／R名は、１９８８年版のO／Rアドレスに相当する。

表1.1-3 O／Rアドレスの形式

形式	使用目的	使用パラメタ（抜粋）
簡易記述 (mnemonic)	利用者にわかりやすい形式	組織名、部門名、個人名他
数字 (numeric)	数字のみしか入力できない端末用の形式	数字利用者識別子
郵便 (postal)	郵便で使用する要素を使用する形式（注１）	私書箱番号、街路アドレス他
端末 (terminal)	網番号等の端末に付与された番号を使用する形式	ネットワークアドレス他

注１）表1.1-2では、郵便用の属性を省略している。
注２）使用パラメタには、端末を除き、主管機関管理領域名と国名が設定必須である。

以下にO／Rアドレスの設定例を示す。

属性	設定例	説明
国名	ＪＰ	日本の国コード
主管機関管理領域名	ＪＩＰＤＥＣ	ＡＤＭＤ名を英字で設定
私設領域名	ＣＩＩ	ＰＲＭＤ名を英字で設定
Ｘ．１２１アドレス	（未設定）	
端末ＩＤ	（未設定）	
組織名	（未設定）	
ユニークＵＡ識別子	（未設定）	
個人名		
姓	ＳＡＮＧＹＯＵ	姓（産業）
名	ＴＡＲＯＨ	名（太郎）
頭文字	ＳＴ	
世代名	（未設定）	
部門	（未設定）	

図1.1-5 O／Rアドレスの設定例

(2) ディレクトリの使用

ディレクトリは、Ｘ．５００により規定される情報であり、MHSのO／Rアドレスのほか

に電話番号をはじめとする様々な情報を管理し、利用者へ情報提供することができる。

ディレクトリでは個々の情報に利用者が分かりやすい（親しみやすい）名前を付与し、情報の検索が容易に行えるようにしている。例えば、住所（の一部）と氏名を検索条件とし、ディレクトリに格納されている情報を取り出すことができるようになっている。

ＭＨＳのアドレスは、表1.1- 2に示したように複雑であり、これをディレクトリが管理することによって、あて先の利用者の指定を容易にすることができる（図1.1- 6）。具体的には、Ｏ／Ｒ名の中にディレクトリ名のみを指定してメッセージを発信することができる。（「(3) 経路選択」参照）。

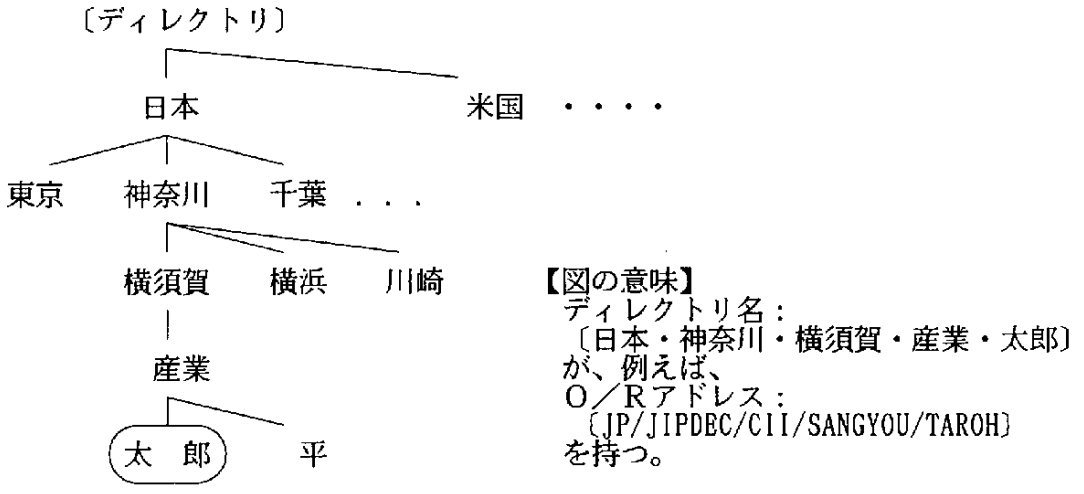


図1.1- 6 ディレクトリとＯ／Ｒアドレス

ディレクトリシステムとＭＨＳの関係およびディレクトリシステムの構成を図1.1- 7に示す。

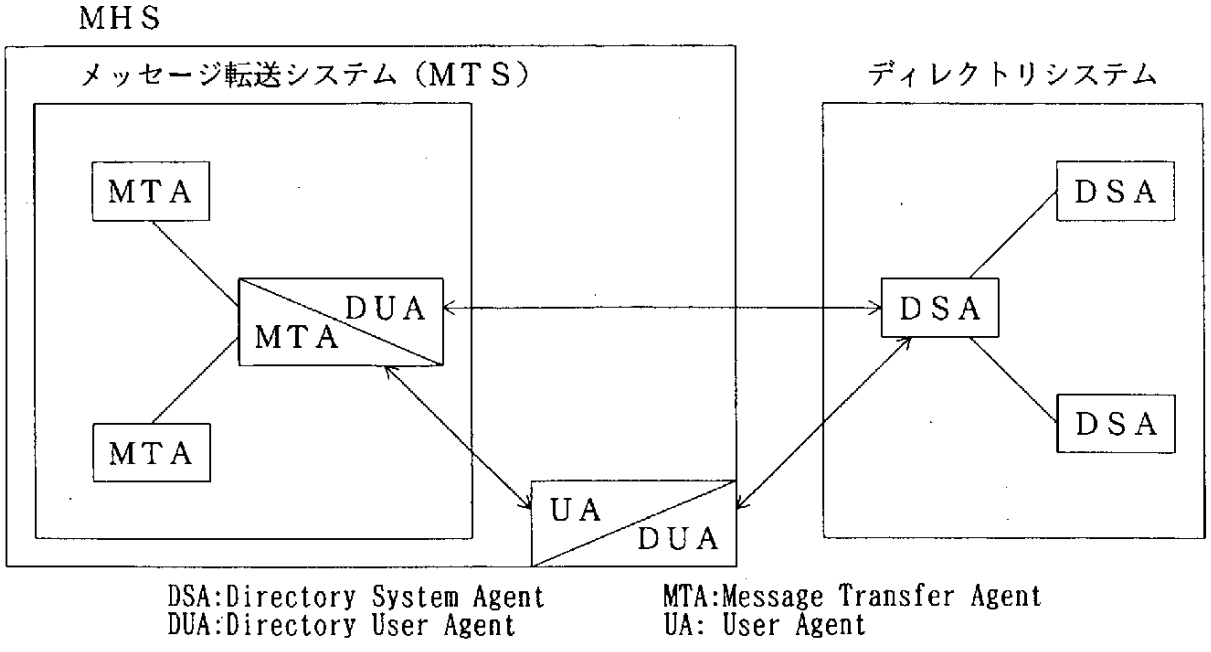


図1.1- 7 ＭＨＳとディレクトリシステムの連携モデル

図1.1- 7で、ＤＵＡは、ディレクトリシステムへアクセスする機能体で、ＭＨＳのＵＡに相当するものであり、ＤＳＡは、ディレクトリ情報を管理し、ほかのＤＳＡと協調して利用者（ＤＵＡ）へディレクトリ情報の提供を行う機能体である。

(3) 経路選択（あて先の指定と配信）

ＭＨＳでメッセージを配信する場合のあて先（受信者）には、受信者のＯ／Ｒ名を指定する。発信者は、発信ＵＡ／発信ＭＴＡへこのＯ／Ｒ名を渡す。受信者のＯ／Ｒ名にＯ／Ｒアドレスが含まれていれば、ＭＴＡはそれに従い配信する。Ｏ／Ｒアドレスがなく、ディレクトリ名のみが指定されている場合には、「(2) ディレクトリの使用」に示したようにＭＴＡがディレクトリシステムへ問い合わせ、Ｏ／Ｒアドレスへ変換した後、配信処理を行う。

参考：発信ＵＡが、ディレクトリシステムへアクセスして、ディレクトリ名からＯ／Ｒアドレスを取得し、ＭＴＡへは、Ｏ／Ｒアドレスのみを渡す方法もある（図1.1- 7参照）。

Ｏ／Ｒアドレスのうち、国名、主管機関管理領域名（および私設領域名）によりメッセージを配信する管理領域を決定することができる。これらのパラメタから、あて先がほかの管理領域にある場合には、当該管理領域内ではその他のＯ／Ｒアドレスのパラメタを参照する必要はなく、目的とする管理領域のＭＴＡへメッセージを転送する。一方、自分の管理領域内の利用者である場合には、その管理領域で規定されたＯ／Ｒアドレスの使用方法により受信者を決定し、配信処理を行う。これを経路選択と言う（経路選択の詳細は図1.1- 8を参照）。

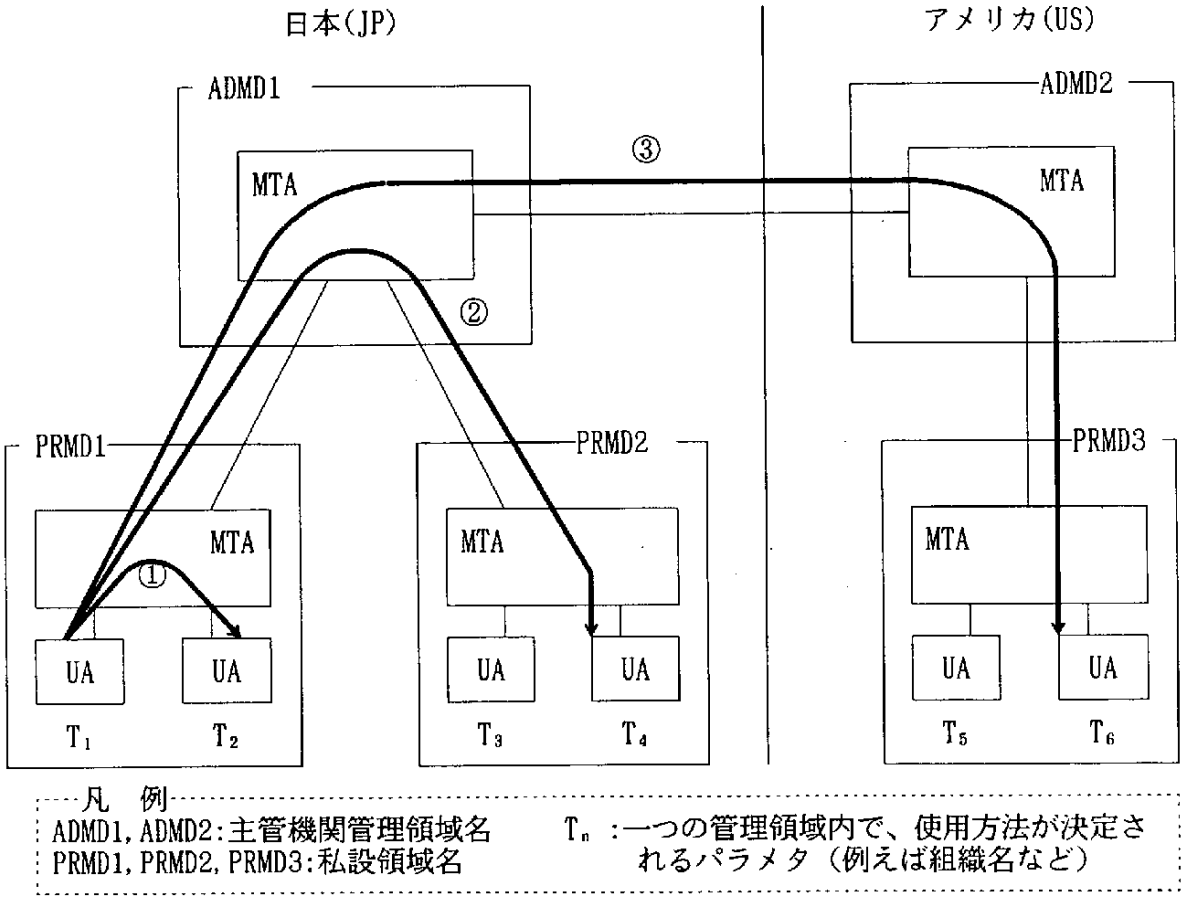


図1.1- 8　経路選択の概念図

図1.1- 8では、ＰＲＭＤ１の中の「T_1」パラメタを持つＵＡからメッセージ発信した場合、以下のパターンの経路選択が行われる。このとき、発信者(T_1)のＯ／Ｒ名は"JP/ADMD1/PRMD1/T_1"と表わされる。

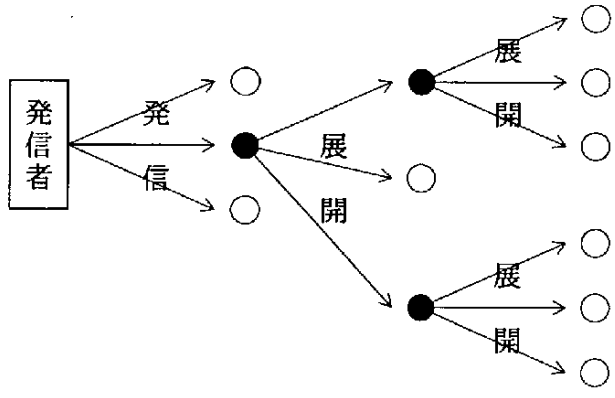
① 受信者O/R名=JP/ADMD1/PRMD1/T_2
自分の管理領域内のため"T_2"により経路選択。

② 受信者O/R名=JP/ADMD1/PRMD2/T_4
私設領域名が異なるため上位レベルであるADMD1に渡され、ADMD1内では、"PRMD2"により経路選択。

③ 受信者O/R名=US/ADMD2/PRMD3/T_6
国名が異なるため、アメリカにリンクを持つADMD1に渡され、アメリカ内で経路選択。

(4) 配布先表

配布先表は、グループ全体にメッセージを発信する場合、その構成員（メンバ）の一人一人の名前を指定する代わりに、グループ名を指定するだけでメンバ全員に発信できるようにするためのものである。発信ＵＡが指定する場合は、配布先表とＯ／Ｒ名に区別はない。配布先表は事前に利用者によりＭＴＡに登録され、ＭＴＡは指定されたあて先が配布先表であれば、配布先表のメンバに展開して配布を続ける。配布先表のメンバが更にまた配布先表でもよい。その場合ＭＴＡはその配布先表も展開する。この様子を図1.1- 9に図示する。



○：配布先表でないＯ／Ｒ名
●：配布先表

図1.1- 9　配布先表とその展開

1. 1. 6　サービスの概要

(1) メッセージ転送サービス（ＭＴサービス）

メッセージ転送サービスは、ＭＴＡによって提供されるサービス（図1.1- 1を参照）で、汎用的な、利用者（応用プログラムを含む）に依存しない、蓄積交換によるメッセージの転送サービスである。ＥＤＩメッセージを転送する場合にも本サービスを使用する。

ＭＴ(Message Transfer)サービスには、基本ＭＴサービスとＭＴ任意選択利用者ファシリティ（オプショナルサービス）がある。基本ＭＴサービスはどのシステムでも提供される機能で、ＭＴ任意選択利用者ファシリティは、必要に応じて選択できる機能である。それぞれの詳細を表1.1- 4、表1.1- 5に示す。

表1.1- 4　基本ＭＴサービス一覧

サービス要素	クラス
アクセス管理	ＬＭ
内容種別表示	Ｓ
変換済表示	Ｓ
配信時刻表示	Ｓ
メッセージ識別	Ｓ
配信不能通知	Ｓ
原符号化情報種別表示	Ｓ
発信時刻表示	Ｓ
利用者／ＵＡ能力の登録	ＬＭ

クラスは、INTAP実装規約の規定するサポートクラスを示す。記号の意味は以下のとおりである。本節以降の表も同様である。

Ｓ　：サポートする
Ｎ　：サポートしなくてもよい
ＬＭ：サポートの可否や方法は規定しない

表1.1- 5　ＭＴサービスの任意選択利用者ファシリティー一覧

サービス要素	クラス	サービス要素	クラス
代行受信者許可	Ｎ	メッセージ安全保護ラベル	Ｎ
代行受信者登録	ＬＭ	メッセージ順序完全性	Ｎ
内容機密性	Ｎ	同報	Ｓ
内容完全性	Ｎ	配信の否認不能	Ｎ
変換禁止	Ｓ	発生源の否認不能	Ｎ
情報損失を伴う変換禁止	Ｎ	発信の否認不能	Ｎ
遅延配信	Ｎ	発信者要求代行受信者	Ｎ
遅延配信取り消し	ＬＭ	配信不能通知の抑止	Ｎ
配信通知	Ｓ	打診	Ｎ
ディレクトリ名による受信者指定	Ｎ	打診発生源認証	Ｎ
他受信者名表示	Ｎ	配信証明	Ｎ
配布先表(ＤＬ)展開履歴表示	Ｎ	発信証明	Ｎ
配布先表(ＤＬ)展開禁止	Ｎ	あて先変更の発信者による禁止	Ｎ
明示変換	Ｎ	受信者指定あて先変更	ＬＭ
配信優先度の選択	Ｓ	報告発生源認証	Ｎ
配信保留	ＬＭ	要求配信方法	Ｎ
暗黙変換	ＬＭ	制限配信	ＬＭ
配信期限指定	Ｎ	内容の返送	Ｎ
メッセージ流れ機密性	Ｎ	安全保護付きアクセス管理	ＬＭ
メッセージ発生源認証	Ｎ	配布先表の使用	Ｎ

ＭＴＡは、ＵＡやＭＳからメッセージの発信を受け付ける。メッセージは封筒と内容から構成され、封筒にあて先や発信日時などが記載される。ＭＴＡは、メッセージを転送し、あて先のＵＡ／ＭＳに配信する。

ＭＨＳで取り扱う情報は、その性質からメッセージ、通知、打診の三種類の情報に分類できる。以下に通知、打診について説明する。通知には、配信通知と配信不能通知とがある。メッセージが正しくあて先のＵＡ／ＭＳに配信された場合、配信通知を発信ＵＡに送付するよう、メッセージの発信の際、発信ＵＡはＭＴＡに要求できる。また、メッセージがあて先に配信される前にエラーになった場合（あて先不明など）にも、その旨の通知（配信不能通知）がなされる（図1.1-10）。

あて先の確認や相手の格納領域の大きさの確認のために、試験的に発信することを打診と呼ぶ。打診の中にはメッセージの本文（内容）は含まれておらず、またそのデータ自身は相手に配信されないが、配信通知や配信不能通知は発信元に通知され、ユーザは送付したいメッセージを相手が受け取れるかどうかを知ることができる。

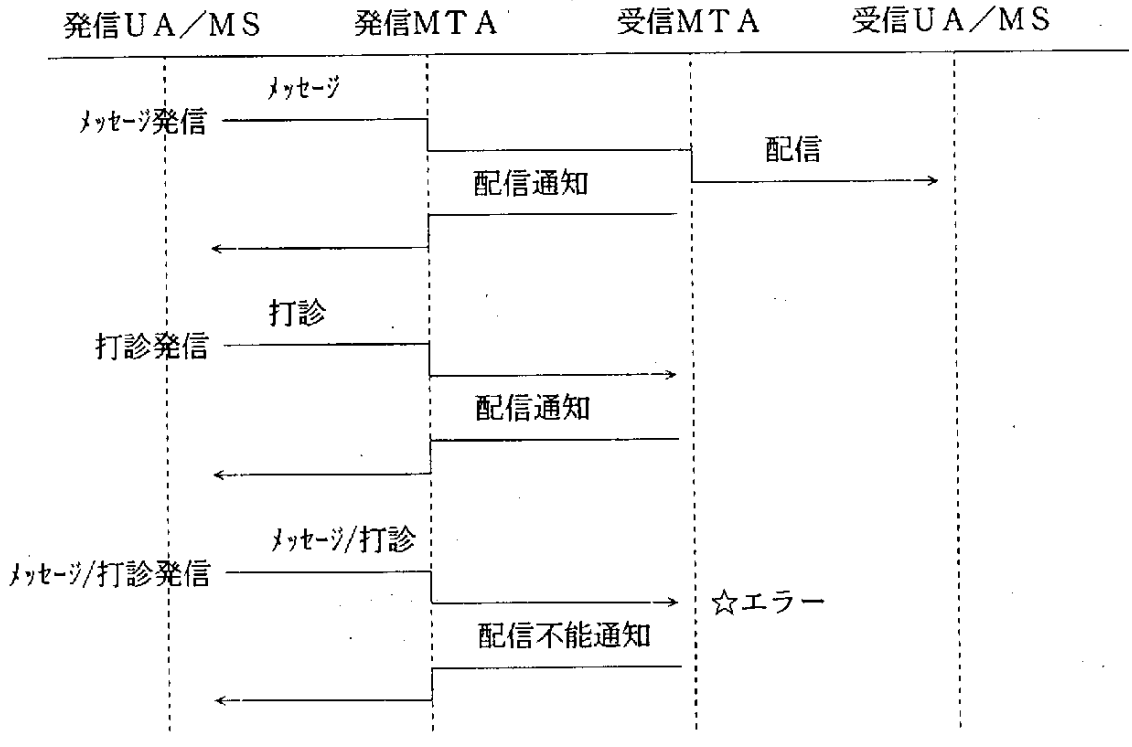


図1.1-10　ＭＴサービスにおけるメッセージ／打診と通知の流れ

(2) 個人間メッセージ通信サービス（ＩＰＭサービス）

個人間メッセージ通信サービスは、個人間でメッセージを交換するためのサービスである。

ＩＰＭ（Interpersonal Messaging)サービスは、メッセージを発信／受信するときにＭＴサービスを利用して実現される（図1.1- 1参照）。ＩＰＭサービスには、基本ＩＰＭサービスとＩＰＭ任意選択利用者ファシリティ（オプショナルサービス）がある。基本ＩＰＭサービスはどのシステムでも提供される機能で、任意選択利用者ファシリティは、必要に応じて提供される機能である。それぞれの詳細を表1.1- 6、表1.1- 7に示す。ＩＰＭサービスでは、ＭＴサービスに加えて、主題の表示、秘密度（私信や親展など）の表示、返信、回送などのサービスが提供される。

表1.1- 6　基本ＩＰＭサービス一覧

サービス要素	クラス	
	送信	受信
アクセス管理	ＬＭ	ＬＭ
内容種別表示	Ｓ	Ｓ
変換済表示	ＮＡ	Ｓ
配信時刻表示	ＮＡ	Ｓ
ＩＰメッセージ識別	Ｓ	Ｓ
メッセージ識別	Ｓ	Ｓ
配信不能通知	Ｓ	ＮＡ
原符号化情報種別表示	Ｓ	Ｓ
発信時刻表示	Ｓ	Ｓ
本体種別表示	Ｓ	Ｓ
利用者／ＵＡ能力の登録	ＮＡ	ＬＭ

クラスの記号の意味

Ｓ　：サポートする
Ｎ　：サポートしなくてもよい
ＬＭ：サポートの可否や方法は規定しない
ＮＡ：ありえない

個人間メッセージ（ＩＰメッセージ）をあて先のＵＡが取り出し後、受信者はメッセージを確かに受け取ったことを示す受信通知を発信者に送付できる。また、廃棄したり回送したりした場合は受信不能通知を発信することもできる（図1.1-11）。

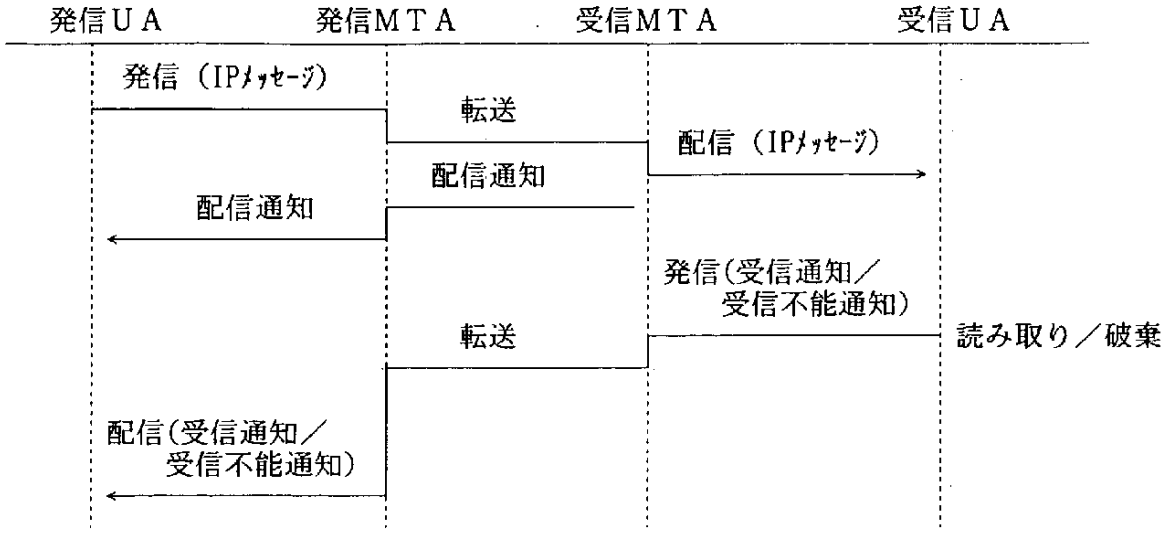


図1.1-11　ＩＰＭ／ＭＴサービスにおけるメッセージと通知

表1.1-7 ＩＰＭサービスの任意選択利用者ファシリティ一覧

サービス要素	クラス		サービス要素	クラス	
	送信	受信		送信	受信
付加物理表現	N	N	配信の否認不能	N	N
代行受信者許可	N	N	発生源の否認不能	N	N
承認者群表示	N	S	発信の否認不能	N	N
自動回送表示	N	S	差替えの表示	N	S
基本物理表現	N	N	通常郵便	N	N
秘密受信者表示	N	S	発信者表示	S	S
本体部暗号化表示	N	S	発信者要求代行受信者	N	NA
内容機密性	N	N	ＭＨＳによる物理的配信通知	N	N
内容完全性	N	N	物理的配達システム（ＰＤＳ）による物理的配信通知	N	N
変換禁止	S	S			
情報損失を伴う変換禁止	N	NA	物理的回送許可	N	N
局留め	N	N	物理的回送禁止	N	N
助言付き局留め	N	N	配信不能通知の抑止	N	NA
相互参照表示	N	S	正／写し受信者群表示	S	S
遅延配信	LM	NA	打診	N	NA
遅延配信取り消し	LM	NA	打診発生源認証	N	N
配信通知	S	NA	配信証明	N	N
ビューロファックスサービスによる配達	N	N	発信証明	N	N
			受信通知要求表示	N	N
ディレクトリ名による受信者指定	N	NA	あて先変更の発信者による禁止	N	NA
他受信者名表示	N	S	書留郵便	N	N
配布先表(ＤＬ)展開履歴表示	NA	N	親展書留郵便	N	N
配布先表(ＤＬ)展開禁止	N	N	返信要求表示	N	S
速達郵便サービス	N	N	返信ＩＰメッセージ表示	S	S
失効日時表示	N	S	報告発生源認証	N	N
明示変換	N	NA	回送先住所要求	N	N
回送ＩＰメッセージ表示	N	S	要求配信方法	N	NA
配信優先度の選択	S	S	内容の返送	N	NA
重要度表示	N	S	秘密度表示	N	S
本体部脱落表示	N	N	特殊配達	N	N
言語表示	N	N	主題表示	S	S
配信期限指定	N	NA	配達不能郵便の物理的返送	N	N
メッセージ流れ機密性	N	NA	配布先表の使用	N	N
メッセージ発生源認証	N	N	受信者指定あて先変更	NA	LM
メッセージ安全保護ラベル	N	N	制限配信	NA	LM
メッセージ順序完全性	N	N	安全保護付きアクセス管理	NA	LM
同報	S	NA	代行受信者登録	NA	LM
複式本体	N	S	配信保留	NA	LM
受信不能通知要求	N	S	暗黙変換	LM	LM

クラスの記号の意味

Ｓ：サポートする
Ｎ：サポートしなくてもよい
LM：サポートの可否や方法は規定しない
NA：ありえない

1. 1. 7　メッセージの構成

ＭＴサービスで転送されるメッセージは、封筒と内容から構成される。ＩＰＭサービスのデータ（ＩＰメッセージ）は、内容に入れられ、見出しと本体から構成される（図1.1-12）。

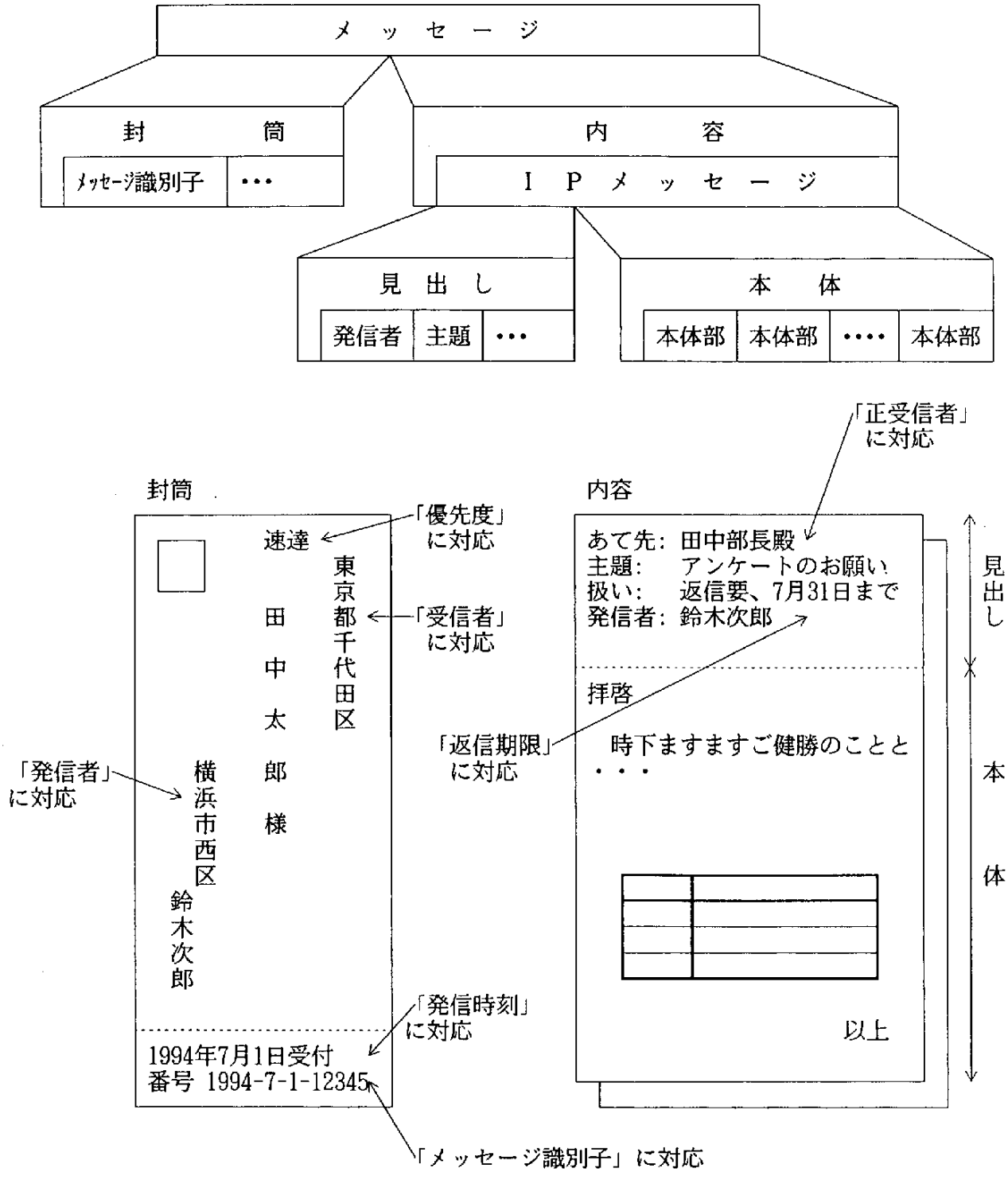


図1.1-12　メッセージの構造とイメージ図

(1) 封筒

封筒には、ＵＡが発信時にＭＴＡに指定した情報、および、ＭＴＡがＭＴサービスをＵＡ／ＭＳに提供するための制御情報が含まれている。以下にその中の主な情報について説明する。

・メッセージ識別子

ＭＴＳ内でメッセージを一意に識別するために、発信ＭＴＡが生成する。

・トレース情報

管理領域を通過するごとに、その管理領域名や到着日時などをＭＴＡが記録する。

・発信者

メッセージを発信した人のＯ／Ｒ名である。

・受信者

メッセージのあて先のＯ／Ｒ名である。

・優先度

メッセージの相対的な優先順位を発信者が、普通、不急、緊急という値で指定する。

・遅延配信時刻

この時刻以前にメッセージが配信されないことを指示するために、発信者が指定する。例えば、会社の人事異動の配布に利用できる。

・原符号化情報種別

本体の符号化種別（ＩＡ５、ＪＰ１など）を発信者が指定する。

・内容種別

内容の種別（１９８４年版ＭＨＳ、１９８８年版ＭＨＳ、Ｐｅｄｉなど）を指定する。

(2) 内容

① 見出し

見出しは、発信者が発信ＵＡに指定し、ＭＴＳを経由した後受信ＵＡから受信者に通知される情報である。以下にその中の主な情報について説明する。

・ＩＰメッセージ識別子

ＩＰメッセージを識別するための情報である。受信通知／受信不能通知を発信者が受け取った時、自分が以前に発信したＩＰメッセージと対応させるために使用する。

・発信者

ＩＰメッセージの発信者の情報が設定される。

・承認者

ＩＰメッセージの発信を承認した人の情報が設定される。これは、発信者と異なる場合のみ指定する。

・正／写し／秘密受信者

正／写し／秘密受信者の情報が設定される。

「正」と「写し」とは何かということは、基本標準では定義されていない。通常は、「正」には発信者がＩＰメッセージに対して何か行動を取ってほしい人を指定し、「写し」には参考までに発信した人を指定する。

秘密受信者とは、「ＩＰメッセージを送付したこと」を正受信者／写し受信者に知らせたくない人のことである。

・返信ＩＰメッセージ識別

ＩＰメッセージが返信である場合、対応する元のＩＰメッセージのＩＰメッセージ識別子が設定される。

・差替えＩＰメッセージ識別

過去に発信したＩＰメッセージを、本ＩＰメッセージで差し替える場合に、その対象を指定する。

・関連ＩＰメッセージ識別

本ＩＰメッセージと関連のあるＩＰメッセージを指定する。「関連」の意味は、利用者が自由に決めることができる。

・主題

ＩＰメッセージの目的や要約などを指定する。

・失効日時

本ＩＰメッセージが有効でなくなると考える日時を承認者が指定する。

・返信期限と返信先

返事が必要な場合に、その期限とあて先を指定する。返信先は、それが発信者でない場合のみ指定する。

・重要度

承認者の考える重要性を、高、普通、低で指定する。

・秘密度

承認者の考える秘密度を、私信、親展、社外秘で指定する。

② 本体

本体にはあて先の利用者に送ろうとする文書（本体部）を１つ以上入れる。本体部には以下の種別がある。

・ＩＡ５テキスト
・ＪＰ１テキスト（ＩＮＴＡＰが規定した形式）
・双方合意のデータ
・回送メッセージ

1. 1. 8　プロトコルの構成

図1.1-13にＭＨＳのプロトコル構成を示す。第７層は、ＭＨＳに関連する機能体を示し、その中に、機能体名、準拠するＩＳＯの規格、ＩＴＵ－Ｔ勧告、プロトコルの通称が記述されている。

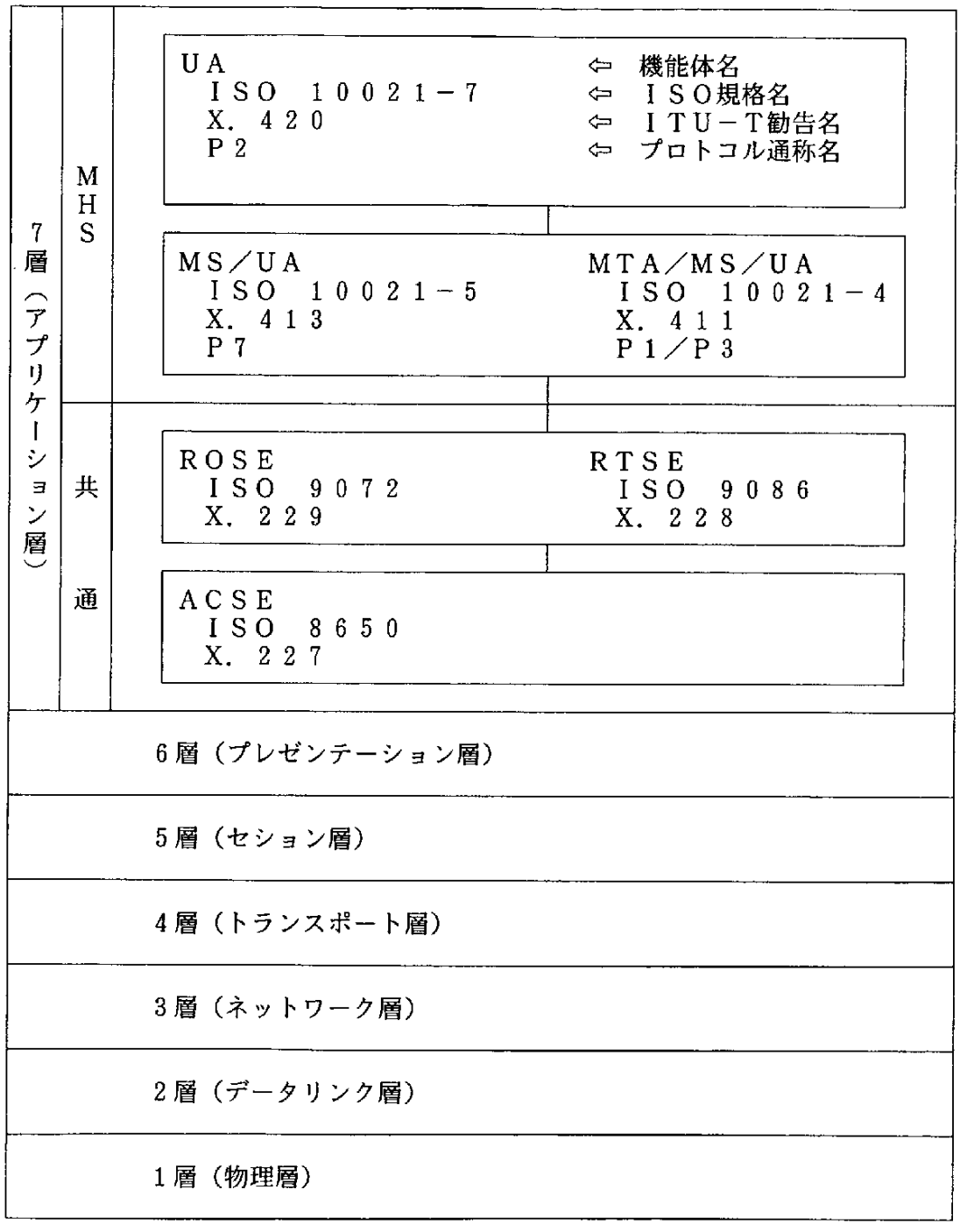


図1.1-13　プロトコル構成

1. 1. 9　安全保護サービス

(1)　安全保護の枠組み

ＭＨＳにおける安全保護上の脅威には、以下のように様々なものがある（図1.1-14）。

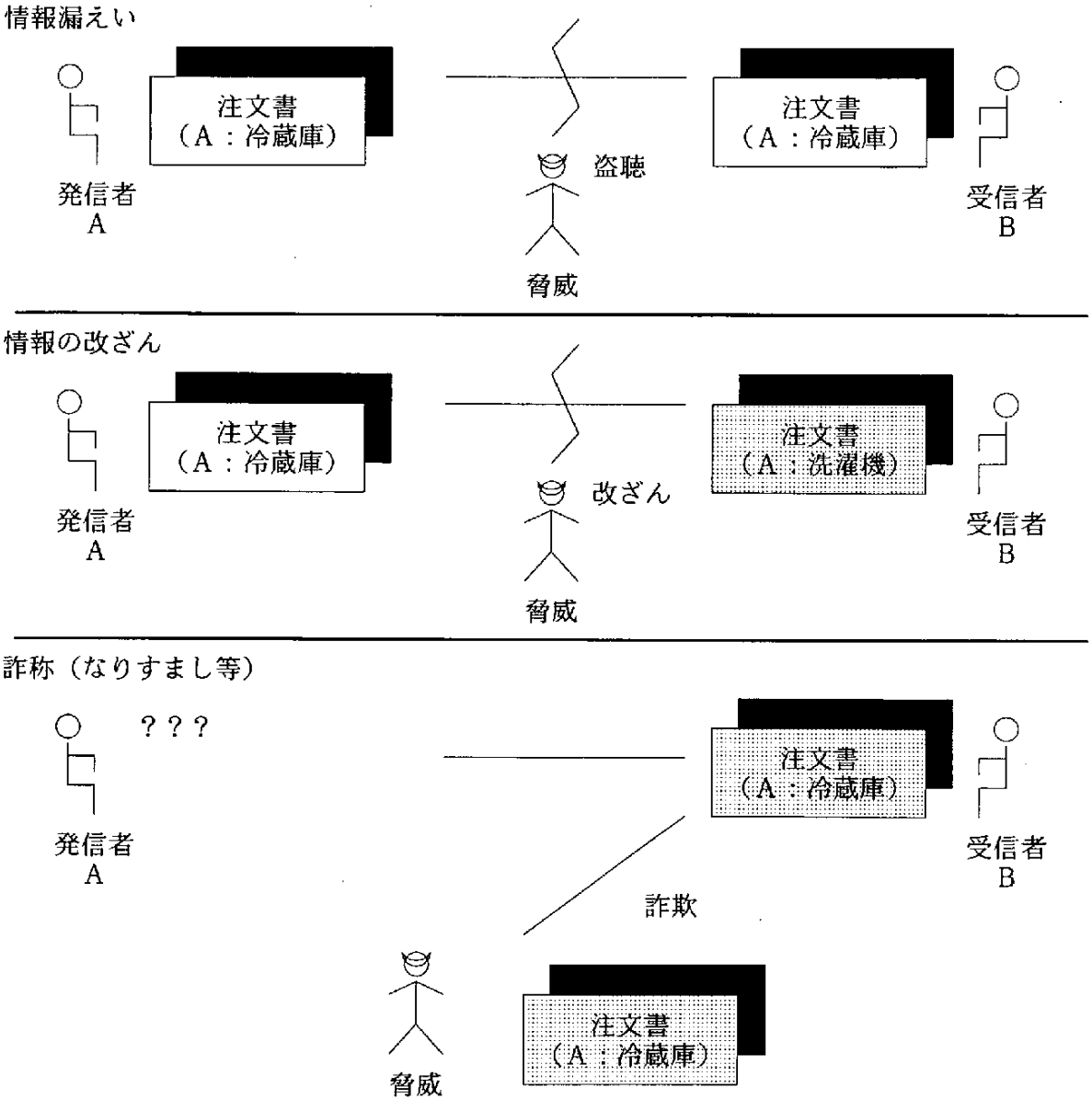


図1.1-14　安全保護における脅威の例

（ａ）情報漏えい

悪意の第三者により、配信途中のメッセージが盗み見られ、内容の機密性が失われる。

（ｂ）情報の改ざん

悪意の第三者により、中継ＭＴＡにおいて内容が改ざんされ、発信者の意図と異なるメッセージが受信者に届けられる。

（ｃ）詐称（なりすまし等）

悪意の第三者が、正当な発信者を装って、受信者にメッセージを送る。

このような安全保護上の脅威からシステムを防護するため、以下のように様々な技術が用いられる（図1.1-15）。

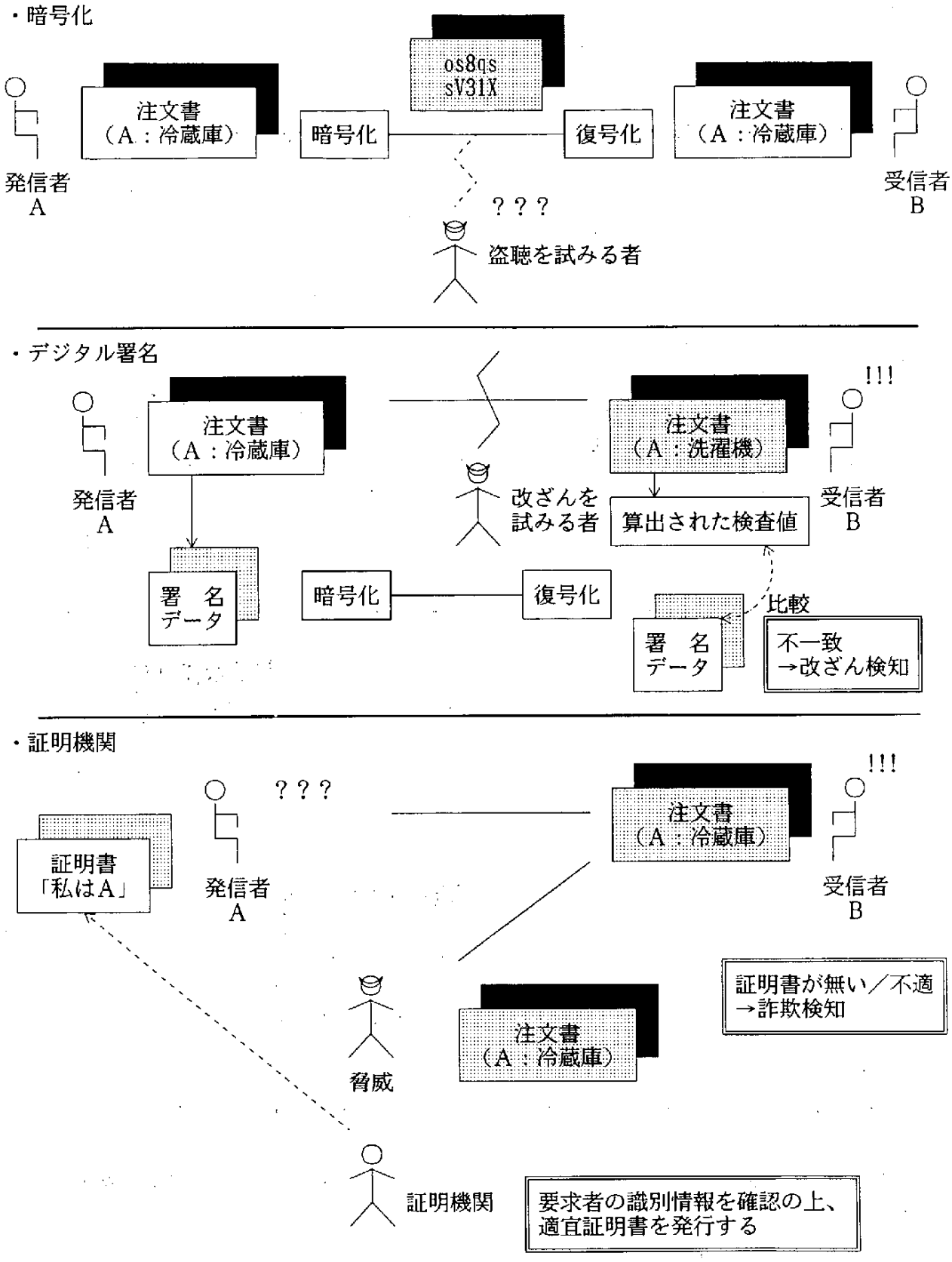


図1.1-15　安全保護に用いられる技術の例

（ａ）暗号化

内容を暗号化することで、たとえ配信途中のメッセージが悪意の第三者に盗み見られても、内容の機密性が保たれるようにする。

（ｂ）デジタル署名

メッセージ内容を暗号化したデータと同時に、暗号化されていないメッセージ内容から算出され、かつ、メッセージの配信中は機密性が保たれるような情報（デジタル署名、例えば、メッセージ内容のチェックサムを暗号化したものを署名データとして利用）を送り、受信者は、メッセージの受信の際、これらの情報の整合性をチェックする。これにより、たとえ配信途中のメッセージが悪意の第三者により改ざんされても、受信者は改ざんを検出できる。また、デジタル署名が発信者の秘密鍵（他人に見られないよう、秘密に管理された暗号鍵。詳細は「付録Ｄ．公開鍵暗号化方式」を参照。）により暗号化された場合、そのような署名情報を作成できるのは発信者以外にはいないため、発信者が後に(不当に)発信の事実を否認することはできない。

（ｃ）証明機関

発信者・受信者は、信頼できる機関(証明機関：注釈を参照)より、自分の身元を保証できる情報として資格証明を発行してもらい、個々に保管している。そして、通信の際に通信相手と資格証明を交換し、通信相手の識別を確実なものとする。これにより、たとえ悪意の第三者が正当なＭＨＳ利用者を装って他のＭＨＳ利用者にメッセージを送っても、受信者は、発信者(この場合悪意の第三者)の詐称(なりすまし等)を検出できる。

（注釈）

証明書……利用者の公開鍵（前述の秘密鍵に対し、誰もが見られるように公開された暗号鍵）を、ほかの幾つかの情報と共に、それを発行した証明機関の秘密鍵によって暗号化したもの。この「証明機関の秘密鍵により暗号化される」ことにより証明書はねつ造できないようになる。

証明機関…一人以上の利用者によって証明書の作成および割り当てを委託されている機関。証明機関は、利用者の鍵を作成することもできる。

上に挙げた脅威のほかにも、様々な脅威が存在している。ＭＨＳに限らず、ＯＳＩ環境における安全保護はデータ処理およびデータ通信の安全保護に限られており、ＯＳＩ環境における保護が効果を発揮するためには、ＯＳＩ以外の環境における安全保護と適切に連携する必要がある。例えば、ＯＳＩの枠組みによりシステム間のデータ通信を暗号化して安全に保護しても、(ＯＳＩの範囲外である)システムへの物理的なアクセスについて安全保護の規制がなければ、暗号化による安全保護は無意味なものになる。

ほかのＯＳＩ応用層と同様、ＭＨＳでもISO 7498-2[2](JIS X 5004 [3] 参照)を基に、メッセージ通信に対する安全保護サービスの枠組みと、それらのサービスの土台となる安全保護要素を規定している。

表1.1- 8は、ＭＨＳに現れうる安全保護上の脅威がどのような形で現れ、それらの脅威に対処するためＭＨＳの安全保護サービスをどのような組合せで利用するか、をまとめたものである。表1.1- 9はＭＨＳの安全保護サービス要素の能力の概要を示し、表1.1-10は、各々

のＭＨＳ構成要素が安全保護サービス要素の提供者と利用者のどちらになるか、を示している(ISO/IEC 10021-1,2[4-5]を参照)。

ＭＨＳの安全保護サービスはISO 7498-2に基づき、いくつかのクラスに分類される。ＭＨＳの安全保護サービスをサポートするために使用可能な安全保護要素は、メッセージ内の封筒に設定される安全保護関連引数と直接対応している。

(2) 認証の枠組み／暗号化技術／デジタル署名

事実上、すべての安全保護サービスは、通信を行っている相手方を確実に識別すること、すなわち認証に依存している。ＭＨＳにおける認証の枠組みは、他のＯＳＩ応用層と同様に、ISO 9594-8 [6](JIS X 5738 [7] 参照)において提供され、以下の二通りがある。

- 簡易認証……発信元が供給する名前とパスワードに依存し、受信者によってこれらの名前とパスワードが確認され、簡易的に認証される。
- 厳密認証……暗号化された通信相手の資格証明（相手の身元を保証できる情報：注釈を参照）により認証される。

なお、ISO 9594-8において、「簡易認証は不正なアクセスをある程度防ぐことができるが、安全なサービスの提供の基本として、厳密認証のみが使用されるべきである。」と勧告されている。

（注釈）

資格証明…身分証明が必要なときに提示するパスポートのようなものである。パスポートに国籍や個人名などの情報が写真や署名とともに示されるように、エンティティの識別情報を示すもの（パスポートでの国籍や個人名）とその識別情報の正当性を検査できるもの（パスポートでの写真や署名）とが対応できるようになっている。

一般に、認証に利用される暗号化システムは、以下の二つに大別される。

- 対称暗号化システム……秘密メッセージの発信元が情報を暗号化するために利用する鍵と、正当な受信者がメッセージを復号化するために使用する鍵が同一である。
- 非対称暗号化システム……秘密メッセージの発信元が情報を暗号化するために利用する鍵と、正当な受信者がメッセージを復号化するために使用する鍵が異なる。

いずれの暗号化システムにおいても、暗号化および復号化の際に利用される鍵をいかに管理し、いかに(正当な使用者に的確に)配送するか、が重要な課題となる。鍵管理の方法に関する指針としては、

- 要求される安全保護の水準に達する間隔で適切な鍵を生成する。
- 利用者への鍵の配送に当たり、適切なアクセス制御を行う。
- 利用者が安全な方法で鍵を利用できるようにする。もしくは、利用者へ安全に鍵を配送する。

が挙げられる。ISO 9594により規定されるディレクトリシステムは、認証機構の実現のために必要となる、暗号化および復号化鍵の管理/配送の枠組みを提供することができる。ただし、ディレクトリシステムにより管理／配送される情報は、暗号化鍵に限られず、汎用的な情報の

管理／配送に使用される。もちろん、鍵の配送／管理の枠組みとしてディレクトリ以外の機構を使用してもよい。

ＭＨＳにおいては、利用する暗号化システムを実現する暗号化アルゴリズムに自由度がある。しかし、ISO 9594-8において採用される厳密認証の手法は、非対称暗号化システムの一つである公開鍵暗号化システム(PKCS)の特性を利用している。この暗号化システムは、鍵の対の両方の鍵が暗号化に使用できる（つまり、公開鍵を用いて暗号化している場合は秘密鍵で復号でき、秘密鍵を用いて暗号化している場合は公開鍵で復号できる）という特性があり、この特性は情報源の証明に利用されるデジタル署名の基礎となっている。

デジタル署名機構は、発信元の認証及び発信元と転送されたデータ間の一義的な関係を証明することで、

- データの完全性……通信中のデータの完全性を保証
- 否認不能……任意の第三者により随時検証可能であり、データの完全性とその作成者の関係について、ねつ造が不可能なことを証明

を提供している。

デジタル署名については、「付録Ｃ．デジタル署名機構」を参照、PKCSについては「付録Ｄ．公開鍵暗号化方式」を参照されたい。

(3) ＭＨＳにおける安全保護方針

ＭＨＳにおける安全保護サービスは、ＭＨＳの範囲を越えた広範囲な安全保護方針（資産の危機や露見を許容範囲内に押さえるための対処の仕方を規定したもの）を実現可能とするものでなければならない。さらに、それぞれ異なる安全保護方針を持つ領域との相互協定（相互動作に関する取り決め）も必要である。

表1.1-8　ＭＨＳにおける安全保護への脅威と、脅威に対処する安全保護サービス

脅　　威	ＭＨＳの安全保護機能を提供するサービス要素
詐称 偽装およびＭＴＳの誤用	 メッセージ発生源認証 打診発生源認証 安全保護付きアクセス管理
不正な受信肯定 不正なメッセージの発信、主張 ＭＴＳ利用者に対するＭＴＡの偽装	配信証明 メッセージ発生源認証 発信証明 報告発生源認証 安全保護付きアクセス管理
他のＭＴＡに対するＭＴＡの偽装	報告発生源認証 安全保護付きアクセス管理
メッセージ順序 メッセージの再送 メッセージの最順序化 メッセージの先行受信 メッセージの遅延	 メッセージ順序完全性 メッセージ順序完全性
情報の改ざん メッセージの改ざん メッセージの破壊 経路選択およびその他の管理情報の変造	 コネクション完全性(*1) 内容完全性 メッセージ順序完全性
サービスの拒否 通信の拒否 ＭＴＡの故障 ＭＴＳメッセージ多量流入	
否認 発生源の否認 発信の否認 配信の否認	 発生源否認不能 発信否認不能 配信否認不能
情報の漏洩 機密性の喪失 匿名性の喪失 メッセージの悪用 トラヒック分析	 コネクション機密性(*2) 内容機密性 メッセージ流れ機密性 安全保護付きアクセス管理 メッセージ流れ機密性
その他の脅威 メッセージ安全保護ラベルを熟知しない発信者 安全保護環境を熟知しないＭＴＡまたはＭＴＳ利用者 誤った経路選択 異なった安全保護ラベル方式を使用するシステムよりの経路選択	 安全保護付きアクセス管理 メッセージ安全保護ラベル 安全保護付きアクセス管理 安全保護付きアクセス管理 メッセージ安全保護ラベル

*1　コネクション完全性とは、例えば応用層を例にとると、その下位層（プレゼンテーション層）のコネクションにおける全ての利用者データの完全性を図り、サービスデータ単位（ＳＤＵ）においてデータの改変、挿入、削除および再使用を検出する。（回復機能を備える場合もある。）

*2　コネクション機密性とは、例えば応用層を例にとると、その下位層（プレゼンテーション層）のコネクションにおける全利用者データの機密の保護を意味する。

*3　コネクション機密性、コネクション完全性は、応用層であるＭＨＳから提供されるのでなく、下位層から提供される。

表1.1-9　ＭＨＳの安全保護機能を提供するサービス要素の能力概要

ＭＨＳの安全保護機能を提供するサービス要素	能力の概要
メッセージ発生源認証	発信者またはメッセージが通過する任意のＭＴＡがメッセージの発信者の識別を認証できる。
報告発生源認証	発信者が配信通知または配信不能通知の報告元を認証できる。
打診発生源認証	打診の通過する任意のＭＴＡが打診の報告元を認証できる。
発信証明	メッセージの発信者が、最初に指定された受信者への配信のためにＭＴＡに送信されたことを確認できる。
配信証明	メッセージの発信者が、配信されたメッセージ、その内容および受信者の識別を認証できる。
安全保護付きアクセス管理	隣接するＭＨＳ構成要素間の認証と、安全保護環境の確立を行う。
内容機密性	メッセージの内容が、本来受信者以外の関係者に承認なしに公開されることを防ぐ。
メッセージ流れ機密性	メッセージの発信者がＭＨＳ内のメッセージの流れを隠せる。
内容完全性	受信者が、メッセージの内容が改ざんされていないことを確認できる。
メッセージ順序完全性	受信者が、メッセージの順序が保たれていることを確認できる。
発生源否認不能	メッセージの受信者に、メッセージおよびその内容の発生源を証明する。
発信否認不能	メッセージの発信者に、メッセージの送信済の証明を与える。
配信否認不能	メッセージの発信者に、メッセージの配信済の証明を与える。
メッセージ安全保護ラベル	重要度を示すことにより、メッセージを分類する能力を提供する。これにより、安全保護方針に従ったメッセージの扱いが強制的に決定される。

表1.1-10　ＭＨＳの安全保護機能を提供するサービス要素の提供者および利用者

ＭＨＳの安全保護機能を提供するサービス要素	発信MTS利用者	MTS	受信MTS利用者
メッセージ発生源認証	提供	利用	利用
報告発生源認証	利用	提供	－
打診発生源認証	提供	利用	－
配信証明	利用	－	提供
発信証明	利用	提供	－
安全保護付きアクセス管理	提供	利用	提供
内容機密性	提供	－	利用
メッセージ流れ機密性	提供	－	－
内容完全性	提供	－	利用
メッセージ順序完全性	提供	－	利用
発生源否認不能	提供	－	利用
発信否認不能	利用	提供	－
配信否認不能	利用	－	提供
メッセージ安全保護ラベル	提供	利用	利用

1. 2 ＥＤＩメッセージ通信サービスの概要

電子データ交換（ＥＤＩ:Electronic Data Interchange）とは、商取り引きをコンピュータネットワークを通して行うことである。これにより、迅速に、正確に、効率的に取り引きを行うことができる。

ＥＤＩの規約は、表1.2- 1に示すように四レベルに分けて考えることができる。ＥＤＩメッセージ通信サービス、いわゆるＰｅｄｉ（Ｆ．４３５／Ｘ．４３５）が規定するのは第１レベルで、本概説書ではそれについて説明する。

表1.2- 1　ＥＤＩの規定レベル

レベル	規約名称	内　　容
1	情報伝達	通信プロトコル，通知，回送など。
2	情報表現	ビジネスプロトコル，伝票フォーマット，商品コードなど。
3	業務運用	運用時間，故障時のルールなど。
4	取引基本	業務の種類や内容，決済方法など。

1. 2. 1　標準化の経緯

ＭＨＳによる電子データ交換（ＥＤＩ）の要求は、その通信の信頼性の高さ、任意の情報の転送機能などにより、１９８４年版ＭＨＳが勧告された時からあり、この１９８４年版ＭＨＳを元にしたＥＤＩの地域標準（注）が欧米で作成された。

注）欧州、米国（北米）などの地域的な標準化団体による、ローカルな標準。

ＭＨＳのような基本標準を基に、パラメタの使用方法を決めることで、様々なサービスで使用可能となる。

欧州と米国で作成された地域標準は、互いに異なる方法によるものであり、これらの間で相互に通信するために変換機能が必要であった。

さらに、ＥＤＩで交換する情報の構文規則についても、欧州はＵＮＴＤＩ[*1]、米国はＡＮＳＩ Ｘ．１２[*2]と異なっていた。しかし、構文規則としてＥＤＩＦＡＣＴ[*3]が１９８８年にＩＳＯ／ＩＥＣで規格化され（ＩＳＯ　９７３５）、また、ＭＨＳも１９８８年版勧告が作成されるなど、標準化が進展した。

このような背景のもとで、これらの国際標準を基にした世界的な標準としてのＥＤＩ通信規約の作成の要求が高まり、ＩＴＵ－ＴＳにおいて、勧告Ｆ．４３５およびＸ．４３５が１９９１年に作成された。ＩＳＯにおいては、この二つの勧告と同様のものが、１９９３年にＤＩＳ投票を終え、近々、ＩＳＯ規格として出版される予定である〔ＭＯＴＩＳ（ＩＳＯ／ＩＥＣ　１００２１：１９９０）の第８部および第９部として出版される〕。なお、この概説書の作成に当たっては、このＩＳＯ規格が未出版のため、前述の二つのＩＴＵ－Ｔ勧告を基にしたが、ＩＳＯ規格が出版された場合にも技術的な内容は変わらない。

実装規約の標準化活動として、ＩＳＯではＰｅｄｉのＩＳＰ（国際実装規約）についても作成

作業が行われている。国内においては、ＴＴＣがＪＴ－Ｘ４３５として勧告しており、ＩＮＴＡＰはＡＯＷ（アジア・オセアニア・ワークショップ）を通じてＩＳＰの作成に携わっている。

注）*1：United Nations Trade Data Interchange
*2：American National Standards Institute Committee X.12
*3：Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) - Application level syntax rules

1. 2. 2　追加規定

ＥＤＩメッセージ通信サービスは、個人間メッセージ通信（ＩＰＭ）サービスと同様、メッセージ転送（ＭＴ）サービスを使用して実現される。ＥＤＩメッセージ通信サービス（Ｐｅｄｉ）は、「１．１　ＭＨＳの機能概要」で説明した個人間メッセージ通信サービスと比較して以下の特徴的な機能を提供する。

① ＥＤＩメッセージの交換
ＩＰＭサービスは“Ｐ２”で規定するＩＰメッセージの交換を提供するのに対し、Ｐｅｄｉサービスは“Ｐ３５”で規定するＥＤＩメッセージの交換を行う。ＩＰメッセージやＥＤＩメッセージを運搬するメッセージ転送部分（Ｐ１、Ｐ３、Ｐ７）の違いはない。

② 内容種別と符号化情報種別
ＭＨＳメッセージの内容部分がＥＤＩメッセージであることを示すよう、封筒内の内容種別を指定する。また、符号化情報種別は、ＥＤＩメッセージの種類（ＥＤＩＦＡＣＴ－ＩＳＯ６４６、ＩＡ５テキストなど）を指定できる。

③ メッセージ回送と責任と通知
受信側がメッセージを回送する場合に、その責任の所在を明確にできる。そのために三種類のＥＤＩ通知（肯定、拒否、回送）が定義されている。

④ ＥＤＩＦＡＣＴ情報表示（インタチェンジ見出し）
本体部としてＥＤＩＦＡＣＴで定める交換データ（ＥＤＩＦＡＣＴインタチェンジ）を転送する場合が多いことを考慮して、ＥＤＩＦＡＣＴインタチェンジの情報の一部をＥＤＩメッセージ通信の見出しにも指定できる。

⑤ 安全保護
商取り引きに利用されるため、メッセージ／通知の証明や否認不能を指定できる。

⑥ 相互参照の拡張
ＥＤＩメッセージ同士が相互参照できるほか、本体部の間でも相互参照できる。例えば、発注伝票に対して受注伝票を送付する場合、対応する発注伝票のＥＤＩメッセージを識別する番号を相互参照に指定し対応を取ることができる。

1. 2. 3　ＥＤＩメッセージ通信サービスのモデルと特徴

ＥＤＩメッセージ通信サービスは、ＥＤＩメッセージ通信システム（ＥＤＩＭＳ:EDI Messaging System）によって提供され、ＥＤＩＭＳはＥＤＩ－ＵＡ、ＥＤＩ－ＭＳ、ＥＤＩ－ＡＵ、メッセージ転送システム（ＭＴＳ）から構成される。これらの関係を図1.2- 1に示す。ＥＤＩ－ＵＡ、ＥＤＩ－ＭＳ、ＥＤＩ－ＡＵの間で交換される情報を、ＥＤＩメッセージ／ＥＤＩ通知（後述）と呼ぶ。これらはメッセージ転送（ＭＴ）サービスのメッセージの内容として封筒と共にＭＴＡ内を転送される。

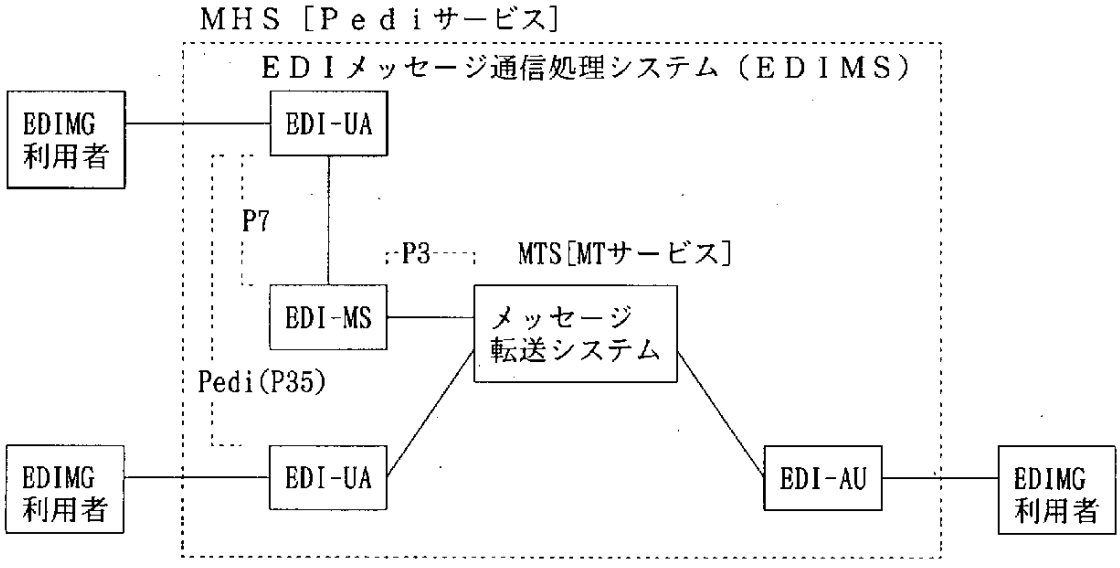


図1.2- 1　ＥＤＩメッセージ通信システム

(1)　ＥＤＩ－ＵＡ

ＥＤＩ－ＵＡは、ＥＤＩメッセージ通信システムの利用者に代わって、ＥＤＩメッセージを発信したり受信したりする。

(2)　ＥＤＩ－ＭＳ

ＥＤＩ－ＭＳは、ＥＤＩ－ＵＡから送られたＥＤＩメッセージを発信したり、ＭＴＡから配信されたメッセージを保管したり、ＵＡから検索を受け付けたりする。

(3)　メッセージ転送システム

メッセージ転送システム（ＭＴＳ）は、ＥＤＩ－ＵＡ、ＥＤＩ－ＭＳ、ＥＤＩ－ＡＵ間でＥＤＩメッセージとＥＤＩ通知を転送する。

(4)　ＥＤＩ－ＡＵ

ＥＤＩ－ＡＵは、ＥＤＩメッセージ通信のメッセージをその外の世界（例えば通常の郵便など）に配信するための機能体である。通常の郵便への配信に使用するＰＤＡＵ（Physical Delivery Access Unit ）は、ＡＵの例の一つである。

1. 2. 4　ＥＤＩメッセージ通信サービスの機能概要

(1)　ＥＤＩメッセージ通信サービスの基本

ＥＤＩ－ＵＡは、ＥＤＩメッセージを発信する。それを受信した側のＥＤＩ－ＵＡには、通常以下の三つの選択がある。そのいずれを選択したか発信ＥＤＩ－ＵＡに伝えるために、ＥＤＩ通知を発信する（図1.2- 2参照）。なお、通知を送信するかどうかは、発信ＥＤＩ－ＵＡが指定する。

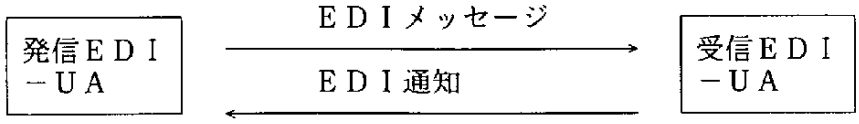


図1.2- 2　ＥＤＩメッセージとＥＤＩ通知

a）肯定

受信ＥＤＩ－ＵＡはＥＤＩメッセージを受諾し、それを発信ＥＤＩ－ＵＡに肯定通知（ＰＮ: Positive Notification ）で伝える。受信ＥＤＩ－ＵＡは、ＥＤＩメッセージに本体部を追加／削除して、さらに他のＥＤＩ－ＵＡに回送することもあり得る。

b）拒否

受信ＥＤＩ－ＵＡはＥＤＩメッセージを拒否し、それを発信ＥＤＩ－ＵＡに否定通知（ＮＮ: Negative Notification ）で伝える。

c）回送

本体を変更しないで、ほかのＥＤＩ－ＵＡにＥＤＩメッセージを回送する。一方、回送したことを元の発信ＥＤＩ－ＵＡに回送通知（ＦＮ: Forwarded Notification）で伝える。

(2)　ＥＤＩメッセージの責任と回送

ＥＤＩメッセージ通信サービスには責任という概念がある。この概念は、誰がＥＤＩメッセージの受け渡し（受信や回送）に責任を持つのか明確にしたものである。例えば、項番(1)の説明において、受信ＥＤＩ－ＵＡが、受信者（ＥＤＩＭＧ利用者）にＥＤＩメッセージを渡したりＥＤＩメッセージの本体部の変更（追加／削除）するためには、肯定通知を発信ＥＤＩ－ＵＡに送信し、受信ＥＤＩ－ＵＡはＥＤＩメッセージに関して責任を持たなければならない。なお、否定通知を送信すると、責任を拒否したことになる。さらに、回送通知を送信すると、受信側は責任を回避したことになり、回送先の処理に委ねられることになる。

(3)　安全保護サービス

ＥＤＩメッセージ通信サービスの安全保護サービス（以下の①～⑤）は、メッセージ転送サービス（表1.1- 5）で提供される安全保護サービスをＥＤＩメッセージとＥＤＩ通知に適用することにより実現されている。ＥＤＩメッセージ通信サービスにおける安全保護サービスの概念を図1.2- 3に示し、以下に各サービスの説明を簡単に記す。なお、各サービスの詳細については第２章（「２．９　安全保護サービス」）で説明する。

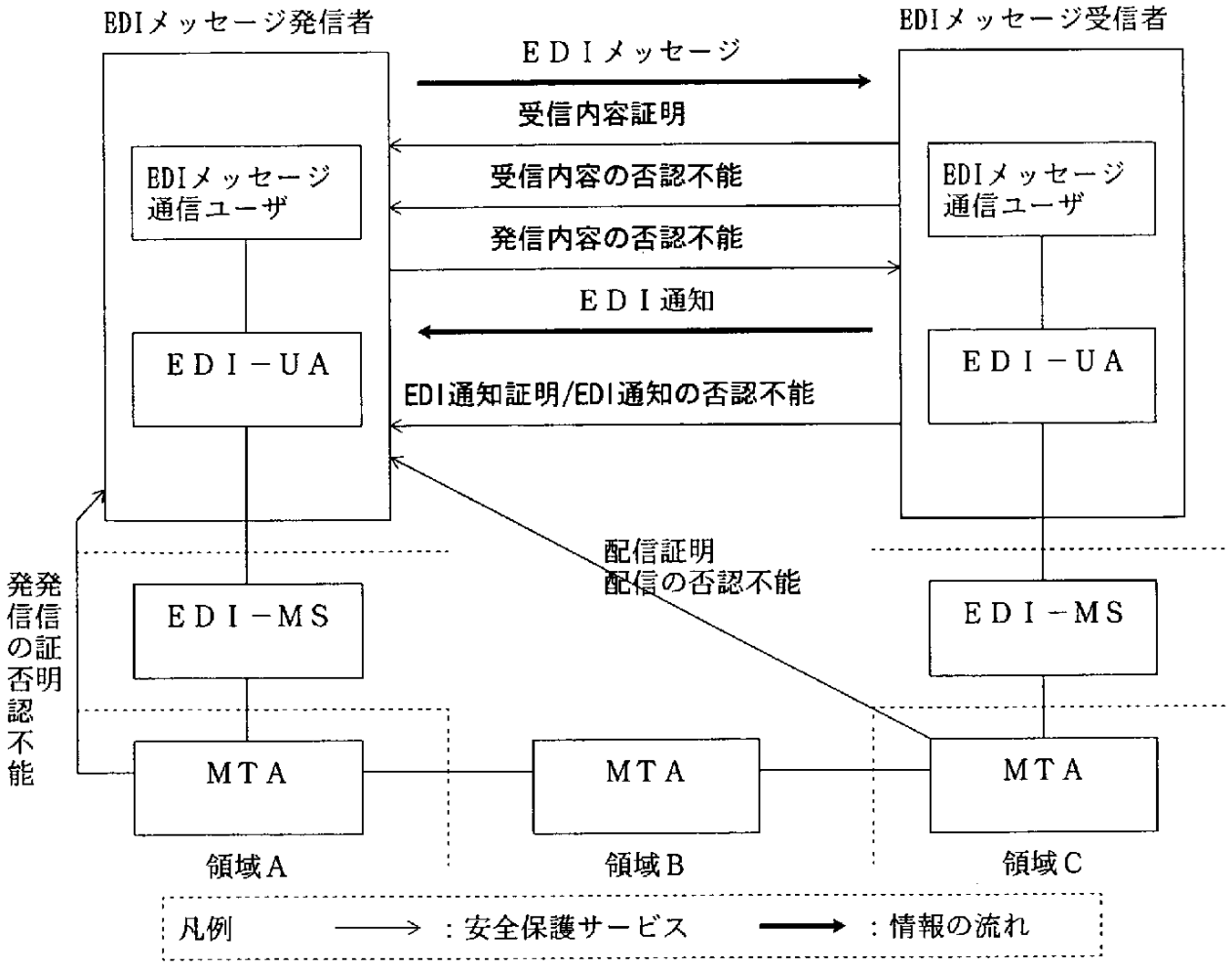


図1.2- 3　ＥＤＩ安全保護の概要

① 受信内容証明

受信内容証明は、ＥＤＩメッセージの受信者が発信者に、「受信した内容は、発信者が発信したものと同じである。」ということを保証するサービスである。

② 受信内容の否認不能

受信内容の否認不能は、受信内容証明に加えて、後で受信者が受信したことを否認しても、それに対して受信した証拠を提示できるサービスである。

③ ＥＤＩ通知証明

ＥＤＩ通知証明は、ＥＤＩメッセージの受信者が発信者に、「発信者が受信したＥＤＩ通知は、発信者が発信したＥＤＩメッセージを受信し作成したものである。」ということを保証するサービスである。

④ ＥＤＩ通知の否認不能

ＥＤＩ通知の否認不能は、ＥＤＩ通知証明に加えて、後でＥＤＩ通知の発信者（ＥＤＩメッセージの受信者）が発信したことを否認しても、それに対して発信した証拠を提示できるサービスである。

⑤ 発信内容の否認不能

発信内容の否認不能は、ＥＤＩメッセージの発信者が受信者に、「受信者が受信した内容は、発信したものと同じである。」ということを保証するサービスである。発信者の否認に対しても証拠を提示できる。

上記(1)～(3)を踏まえてＥＤＩサービスの一覧を表1.2- 2、表1.2- 3に示す。

表1.2- 2　基本ＥＤＩサービス一覧

サービス要素	クラス	
	送信	受信
アクセス管理	ＬＭ	ＬＭ
内容種別表示	Ｓ	Ｓ
変換済表示	Ｓ	Ｓ
配信時刻表示	Ｓ	Ｓ
ＥＤＩメッセージ識別	Ｓ	Ｓ
メッセージ識別	Ｓ	Ｓ
配信不能通知	Ｓ	ＮＡ
原符号化情報種別表示	Ｓ	Ｓ
発信時刻表示	Ｓ	Ｓ
本体種別表示	Ｓ	Ｓ
利用者／ＵＡ能力の登録	ＮＡ	ＬＭ

クラスは、TTC JT-X435の規定するサポートクラスを示す。本節の以降の表も同様である。記号の意味は以下のとおり。

Ｓ　：　サポートする
Ｎ　：　サポートしなくてもよい
ＬＭ：　サポートの可否や方法は規定しない
ＮＡ：　ありえない

表1.2-3　ＥＤＩサービスの任意選択利用者ファシリティー覧

サービス要素	クラス		サービス要素	クラス	
	送信	受信		送信	受信
代行受信者許可	N	N	ＥＤＩ通知の否認不能要求	N	N
応用安全保護要素	N	N	発生源の否認不能	N	N
文字集合	S	S	発信の否認不能	N	N
内容機密性	N	N	差替えの表示	N	S
内容完全性	N	N	発信者表示	S	S
変換禁止	S	S	発信者要求代行受信者	N	NA
情報損失を伴う変換禁止	N	N	配信不能通知の抑止	N	NA
相互参照情報	N	S	打診	N	NA
遅延配信	N	NA	打診発生源認証	N	NA
遅延配信取り消し	N	NA	受信内容証明	N	N
配信通知	S	NA	受信内容証明要求	N	N
ﾃｨﾚｸﾄﾘ名による受信者指定	N	NA	配信証明	N	N
他受信者名表示	N	S	ＥＤＩ通知証明	N	N
配布先表(ＤＬ)展開履歴表示	NA	N	ＥＤＩ通知証明要求	N	N
配布先表(ＤＬ)展開禁止	N	NA	発信証明	N	NA
ＥＤＩ回送	N	S	受信者表示	S	S
ＥＤＩメッセージ種別	S	S	あて先変更の発信者による禁止	N	NA
ＥＤＩ通知要求	S	S	関連メッセージ	N	S
ＥＤＩ標準表示	S	S	報告発生源認証	N	N
ＥＤＩＭ責任回送許可表示	S	S	要求配信方法	N	NA
ＥＤＩＮ受信者	N	S	内容の返送	N	NA
失効日時表示	N	S	サービス表示	N	N
明示変換	N	NA	格納メッセージ削除	NA	S
配信優先度の選択	S	S	格納メッセージ取出し	NA	S
本体部脱落表示	N	S	格納メッセージ一覧	NA	S
インタチェンジ見出し	S	S	格納メッセージ計数	NA	S
配信期限指定	N	NA	配付先表の使用	N	NA
メッセージ流れ機密性	N	NA	代行受信者登録	NA	LM
メッセージ発生源認証	N	N	配信保留	NA	LM
メッセージ安全保護ラベル	N	N	暗黙変換	NA	N
メッセージ順序完全性	N	N	ＭＳ登録	NA	N
同報	S	NA	受信者指定あて先変更	NA	LM
複式本体	N	S	制限配信	NA	LM
発信内容の否認不能	N	N	安全保護付きアクセス管理	N	N
受信内容の否認不能	N	N	格納ＥＤＩメッセージ自動回送	NA	N
受信内容の否認不能要求	N	N	格納メッセージ警報	NA	N
配信の否認不能	N	N	格納メッセージ自動回送	NA	N
ＥＤＩ通知の否認不能	N	N			

クラスの記号の意味

Ｓ　：　サポートする
Ｎ　：　サポートしなくてもよい
ＬＭ：　サポートの可否や方法は規定しない
ＮＡ：　ありえない

1. 2. 5　ＥＤＩメッセージの構成

ＥＤＩメッセージは、「１．１　ＭＨＳの機能概要」で説明したＩＰＭサービスと同様、見出しと本体で構成される。見出しには発信者や受信者などのフィールドが含まれ、本体は一つ以上の本体部から構成される。ＥＤＩＦＡＣＴで規定されたデータ列を転送する場合を例に採って、ＥＤＩメッセージの構成を図1.2- 4に示す。

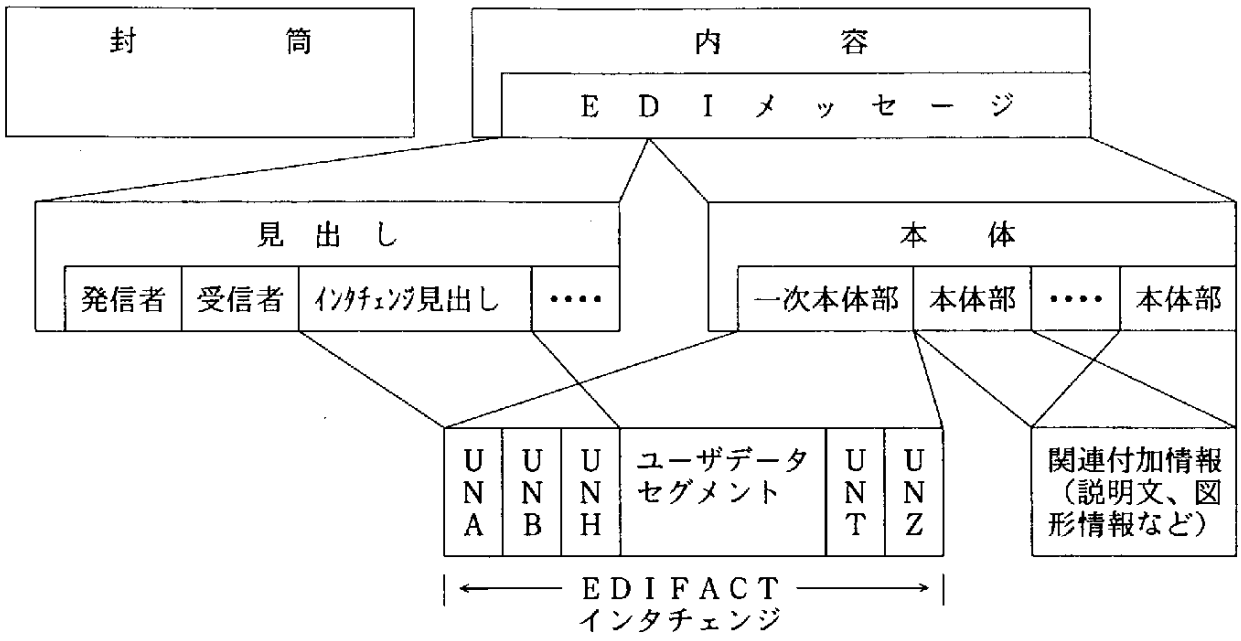


図1.2- 4　ＥＤＩメッセージの構造

(1)　封筒

①　内容種別

内容種別には、ＥＤＩメッセージ通信を示す「35」が設定される。

②　原符号化情報種別

内容がＥＤＩメッセージの場合、原符号化情報種別は、本体を構成する各本体部の種別が設定される。特に一次本体部の種別は「(2)③　ＥＤＩ本体部種別」と同じ値（ＥＤＩＦＡＣＴ－ＩＳＯ６４６、Ｘ．１２－ＩＳＯ６４６など）で、ＭＴＳがＵＡに配信するときに、ＵＡの処理能力と比較して配信するかエラーとするを決めるのに使用される。また、同封のデータ（一次本体部以外の本体部）がある場合にはその種別も設定される。

内容がＥＤＩ通知の場合、原符号化情報種別は省略される。

(2)　見出し

①　ＥＤＩメッセージ識別子

ＥＤＩメッセージを一意に識別するために指定する。相互参照などで使用する。

②　発信者表示／受信者表示

ＥＤＩメッセージの発信者と受信者のＯ／Ｒ名を指定する。受信者は複数指定できる。

③　ＥＤＩ本体部種別

本体に格納されている一次本体部の種別を示す。それには、ＥＤＩＦＡＣＴ、ＡＮＳＩ

X．１２、ＵＮＴＤＩで規定されたデータ列がある。また、「私的オクテット列」を指定することにより、ＣＩＩ標準で規定されたデータ列の転送も可能である。

④　ＥＤＩ通知要求

発信者は、肯定通知／否定通知／回送通知をそれぞれ受信者ごとに要求する。また、ＥＤＩ通知とＥＤＩメッセージ受信の安全保護についてもこのフィールドで指定する。

⑤　ＥＤＩ通知（ＥＤＩＮ）受信者

ＥＤＩ通知の返送先を指定する。このフィールドは、あて先、ＥＤＩメッセージ識別子、第一受信者から構成される。第一受信者には、回送が繰り返される状況において、最初にＥＤＩメッセージを受信した受信者のＯ／Ｒ名が設定される。

⑥　ＥＤＩメッセージ（ＥＤＩＭ）責任回送許可

発信者は、責任を回送できるかどうかを受信者ごとに指定する。

⑦　相互参照情報

相互参照情報は、他のＥＤＩメッセージや同一のＥＤＩメッセージの本体部との間で参照するためのものである。ＩＰメッセージを参照することも考慮されている。参照されたＥＤＩメッセージや本体部がどのような意味を持つかはＥＤＩ利用者（応用プログラム）が決めることができる。パラメタとしては、応用プログラムの固有の情報、ＥＤＩメッセージ識別子、本体部の番号（先頭から数えて何番目にあるか）が設定される。

⑧　インタチェンジ見出し

ＥＤＩＦＡＣＴで規邸されたデータ列であるＥＤＩＦＡＣＴインタチェンジ(EDIFACT Interchange)のフィールドの一部は、Ｘ．４３５の見出しにも含まれている。例えば以下のものがある。

・ＥＤＩメッセージ種別
・構文識別子
・インタチェンジ発信者／受信者
・処理優先度コード

同一の情報が重複して見出しにも本体部にも含まれているのは、情報を処理する主体が異なるためである。つまり、見出しは、ＥＤＩ－ＭＳやＥＤＩ－ＵＡで処理する（例えば検索）ことに使用され、本体は、ＥＤＩ－ＵＡの利用者や応用プログラムに使用される。

(3) 本体

本体は、一次本体部とそれを補足する付加本体部群とから構成される。一次本体部は必須の要素で、ＥＤＩＦＡＣＴ，Ｘ．１２，ＣＩＩ標準で規定されるデータ列が格納される。

〔参　考〕ＥＤＩＦＡＣＴ構文の概要

ＥＤＩＦＡＣＴは、ＩＳＯ９７３５として登録された国際ＥＤＩのための標準シンタックスルールである。ＥＤＩＦＡＣＴの規定によるデータ集合体は図1.2- 5に示すように階層構造を持っている。

ＥＤＩＦＡＣＴでは、発注伝票・納品書といった実際の帳票一件が１メッセージに相当する。メッセージヘッダ（ＵＮＨ）には、帳票の種類等の情報が入っている。あて先が同一である複数個のメッセージを集めたものを機能グループという（機能グループは省略されることもある）。機能グループヘッダ（ＵＮＧ）には、その機能グループの中の帳票の種類やアプリケーション上の送信者・受信者識別子（部門等を表すコードや名前）等が含まれる。一個以上の機能グループまたはメッセージを集めたものを交換（インタチェンジ）という。交換ヘッダ（ＵＮＢ）は、交換の送信者・受信者識別子等の情報を含む。送信者・受信者識別子は交換当事者間の合意によって定められるコードまたは名前である（詳細は「付録Ｆ．ＥＤＩＦＡＣＴ標準メッセージ構造」を参照）。

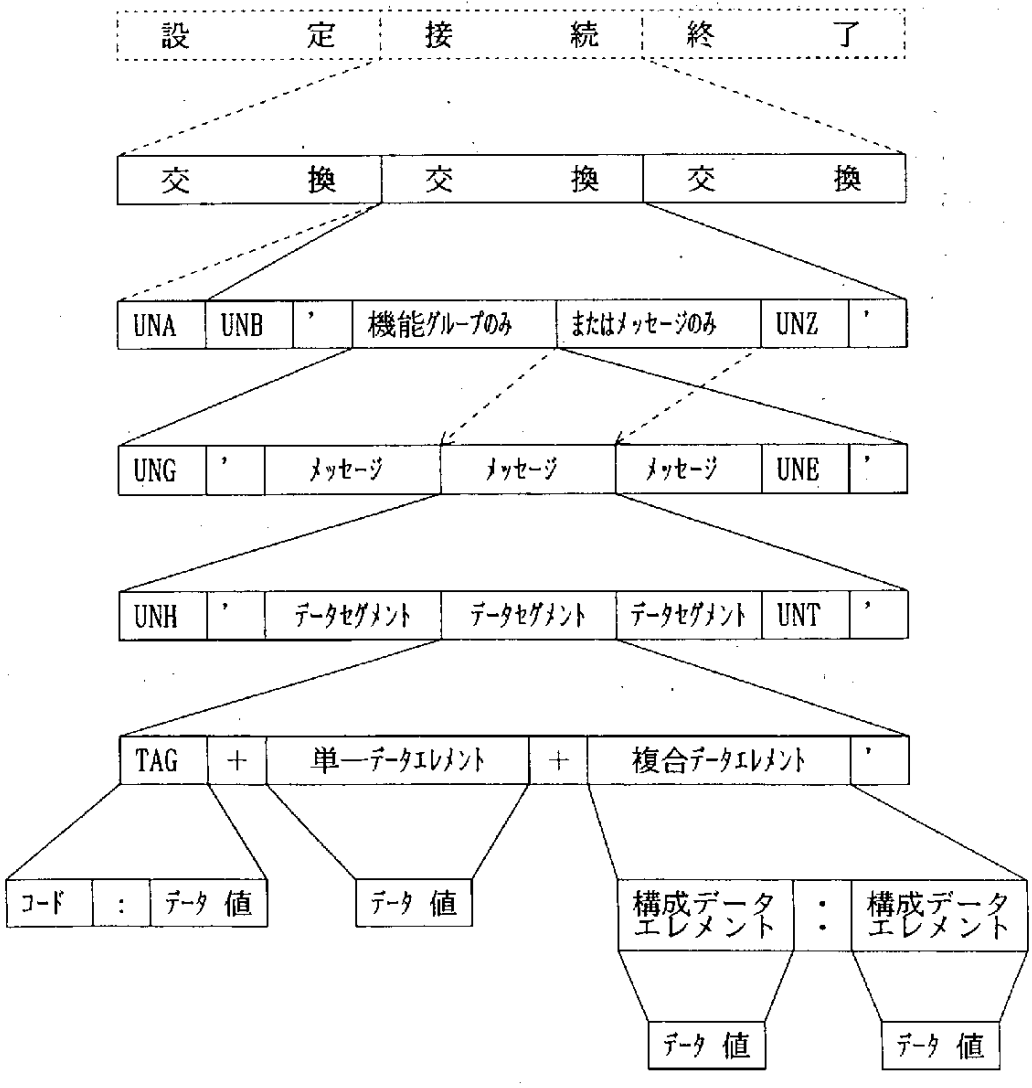


図1.2- 5　ＥＤＩＦＡＣＴによるデータ交換フォーマットの階層

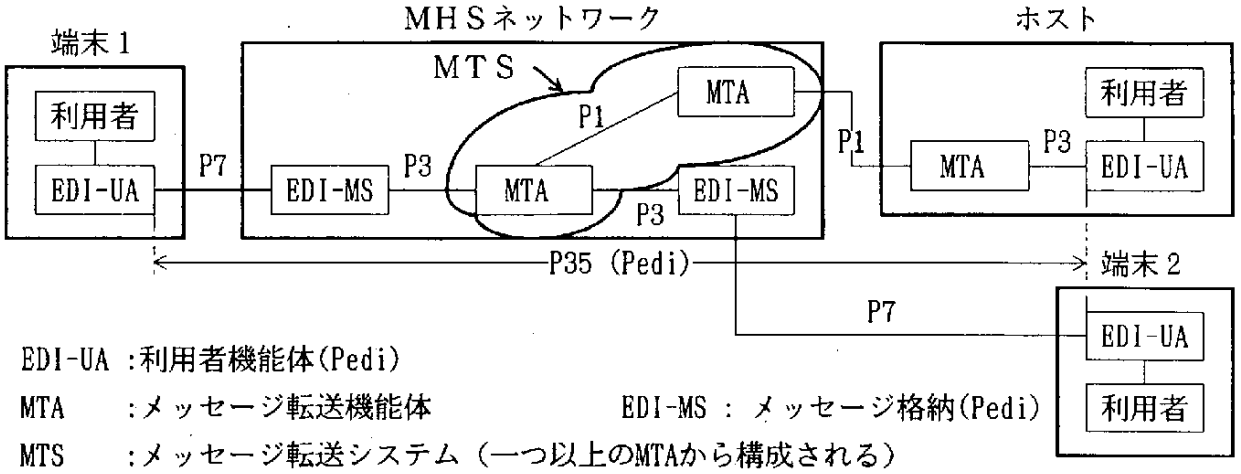
1. 2. 6　ネットワーク利用事例

表1.2- 4に示す四つの代表的なネットワーク利用事例を取り上げ、ネットワーク構成上の管理領域の考え方、ネットワーク構成とＭＨＳ機能モデル（ＭＴＡ，ＥＤＩ－ＭＳ，ＥＤＩ－ＵＡ等の機能体から構成されるモデル）との対応などについて説明する。ただし、ＭＨＳ機能モデルについては、説明を容易にするため、図1.2- 6に示すモデルを仮定する。

表1.2- 4　ネットワーク利用事例の分類

分類内容			項目
大分類		中分類	
ＶＡＮを利用する場合	Ｏ／Ｒ名をＶＡＮから付与	ＰＲＭＤが単一の場合	【例　1】
		ＰＲＭＤが複数の場合（ＶＡＮ間接続）	【例　2】
ＶＡＮを利用しない場合	Ｏ／Ｒ名を自ら設定	ＰＲＭＤが複数の場合	【例　3】
	Ｏ／Ｒ名を電気通信事業者から付与	ＡＤＭＤとＰＲＭＤが混在する場合	【例　4】

ＰＲＭＤ：私設管理領域，ＡＤＭＤ：主管機関管理領域
（詳細は「１．１．４　管理領域」を参照）



EDI-UA :利用者機能体(Pedi)
MTA　:メッセージ転送機能体　　EDI-MS : メッセージ格納(Pedi)
MTS　:メッセージ転送システム（一つ以上のMTAから構成される）
P1　:MTS転送プロトコル　　P3　: MTSアクセスプロトコル
P7　:MSアクセスプロトコル
P35　:ＥＤＩメッセージのフォーマットなどを規定したEDI-UA間のプロトコル

図1.2- 6　仮定したＭＨＳ機能モデル

図1.2- 6のモデルでは、端末１～端末２、端末１／端末２～ホストの間で、受発注伝票のようなＥＤＩメッセージの交換が行える。例えば、端末１～ホストにＥＤＩメッセージを送信する場合は以下のとおりとなる。

① 端末１は、ホスト（ＥＤＩ－ＵＡ）のあて先番号（Ｏ／Ｒ名）をメッセージの「封筒」部分に設定し、送信したいＥＤＩメッセージを「内容」部分に入れ込み、ＭＨＳネットワークへ発信する。〔→Ｐ３機能〕（メッセージ構成は図1.2- 7参照）

② ＭＨＳネットワークではあて先番号により経路選択を行い、目的となるホスト（ＭＴＡ）にメッセージを配信する。〔→Ｐ１機能〕

③ ホスト（ＭＴＡ）は端末１からのメッセージを受信し〔→Ｐ３機能〕、受信先のＥＤＩ－ＵＡに配信可能かどうかを封筒の中の制御情報（内容種別，原符号化情報種別，ｅｔｃ）などによりチェックし、問題がなければ配信通知を端末１に返送する共に、ＥＤＩ－ＵＡにメッセージを配信する。

④ ＥＤＩ－ＵＡは、配信されたメッセージを自分が受け取ってもよいかどうかを判断し、受け取る場合には端末１にＥＤＩ通知（肯定）を返送する。受け取ったＥＤＩメッセージは、利用者として位置付けられる応用プログラム（ＥＤＩアプリケーション）に渡され処理される。

メッセージ

封筒						内容
	発信者Ｏ／Ｒ名	受信者Ｏ／Ｒ名	原符号化情報種別	内容種別		ＥＤＩメッセージ または ＥＤＩ通知（肯定・拒否・回送）

注１）原符号化情報種別 …… 複式本体別の本体部種別の種類（ＥＤＩ本体部を示すＥＤＩＦＡＣＴ－ＩＳＯ６４６等、個人間メッセージの本体部種別等を示すＩＡ５テキスト、ｅｔｃ）が指定できる。
（詳細は「２．７．５　原符号化情報種別表示」を参照）

注２）内容種別 …… 内容の種別（Ｐｅｄｉ，Ｐ２－１９８４，Ｐ２－１９８８など）を指定する。ＥＤＩメッセージの場合は“３５”（Ｐｅｄｉ）が指定される。
（詳細は「２．７．２　内容種別表示」を参照）

図1.2- 7　メッセージの構成

逆に、ホスト～端末１にＥＤＩメッセージを送信する場合も、端末１がＥＤＩメッセージを受け取る動作を除いてほぼ同様となる。すなわち、端末１のように、ＥＤＩ－ＭＳ（Ｐｅｄｉ用メッセージ格納）を介してＭＴＳにアクセスする場合、ＥＤＩメッセージは一旦ＥＤＩ－ＭＳに蓄積され、直接、ＭＴＡからＥＤＩ－ＵＡにＥＤＩメッセージが届かないので、ＥＤＩ－ＵＡは、ＥＤＩ－ＭＳに蓄積されたＥＤＩメッセージの取り出しが必要となる。〔→Ｐ７機能〕

(1) ＶＡＮを利用し、ＰＲＭＤが単一の場合【例　１】

一つのＶＡＮ事業者により提供されるPediｻｰﾋﾞｽを複数企業が利用する形態について説明する。

図1.2- 8において、VANに接続する企業１または企業２の端末やホストは、VANから払い出されたﾈｯﾄﾜｰｸｱﾄﾞﾚｽ(O/R名)により、そのVANの中で相手を一意に識別できる。このﾈｯﾄﾜｰｸｱﾄﾞﾚｽを特定できる領域を管理領域と言い、図1.2- 8の場合の管理領域は、 VAN事業者という一つの私的な（公的な機関ではない）組織によりﾈｯﾄﾜｰｸｱﾄﾞﾚｽが特定されるので、私設管理領域（PRMD）と呼ばれる。

VANから加入端末へO/R名を付与する形態は、1)複数のﾊﾟﾗﾒﾀから構成されているO/R名(O/R 名については「1.1.5 ｱﾄﾞﾚｽと経路選択」を参照）についてVANからその全てのﾊﾟﾗﾒﾀを付与、2)VANからO/R名の中の特定なﾊﾟﾗﾒﾀ（PRMD名、組織名など）に対してﾕﾆｰｸな値を払い出し、VAN利用者側でその他のﾊﾟﾗﾒﾀ（部門名、個人名など）を自由に決定、等いろいろあるが、ここでは後者の方式を採った場合について説明する。図1.2- 8で示すようにVAN利用者のO/R名は、“VAN1から払い出された組織名「COMPANY1またはCOMPANY2」＋利用者が決定する部門名「KOUBAIまたはEIGYOUなど」”によりVANの中でﾕﾆｰｸなｱﾄﾞﾚｽとなっている。なお、ADMD名は本来ならば必須であるが、VAN1に閉じた接続を仮定しているため一つのｽﾍﾟｰｽを設定することとする。　図1.2- 8の例では、企業１の端末(PC:ﾊﾟｿｺﾝ,WS:ﾜｰｸｽﾃｰｼｮﾝ)～企業２のホストの間で、VAN1を経由してEDIﾒｯｾｰｼﾞの交換が行える。図1.2- 6と比較するとＭＨＳﾈｯﾄﾜｰｸの部分がVAN1に置き換わる形態となる。PCからホストにEDIﾒｯｾｰｼﾞを送信する場合を例に採ると、PCは受信者Ｏ／Ｒ名にﾎｽﾄのO/R名“国名「JP」＋ADMD名「１個のスペース」＋VAN1から払い出された組織名「COMPANY2」＋利用者が決定する部門名「CENTER」”を設定して ﾒｯｾｰｼﾞをVAN1へ発信し、VAN1では、指定された受信者O/R名により経路選択を行った後、目的となるホストにﾒｯｾｰｼﾞを配信する。これにより、ホストはPCからのEDIﾒｯｾｰｼﾞを受信できる。一つのVANの中で通信するのならば管理領域名（PRMD名＝「MDVAN1」）を意識せずにEDIﾒｯｾｰｼﾞ交換ができる。

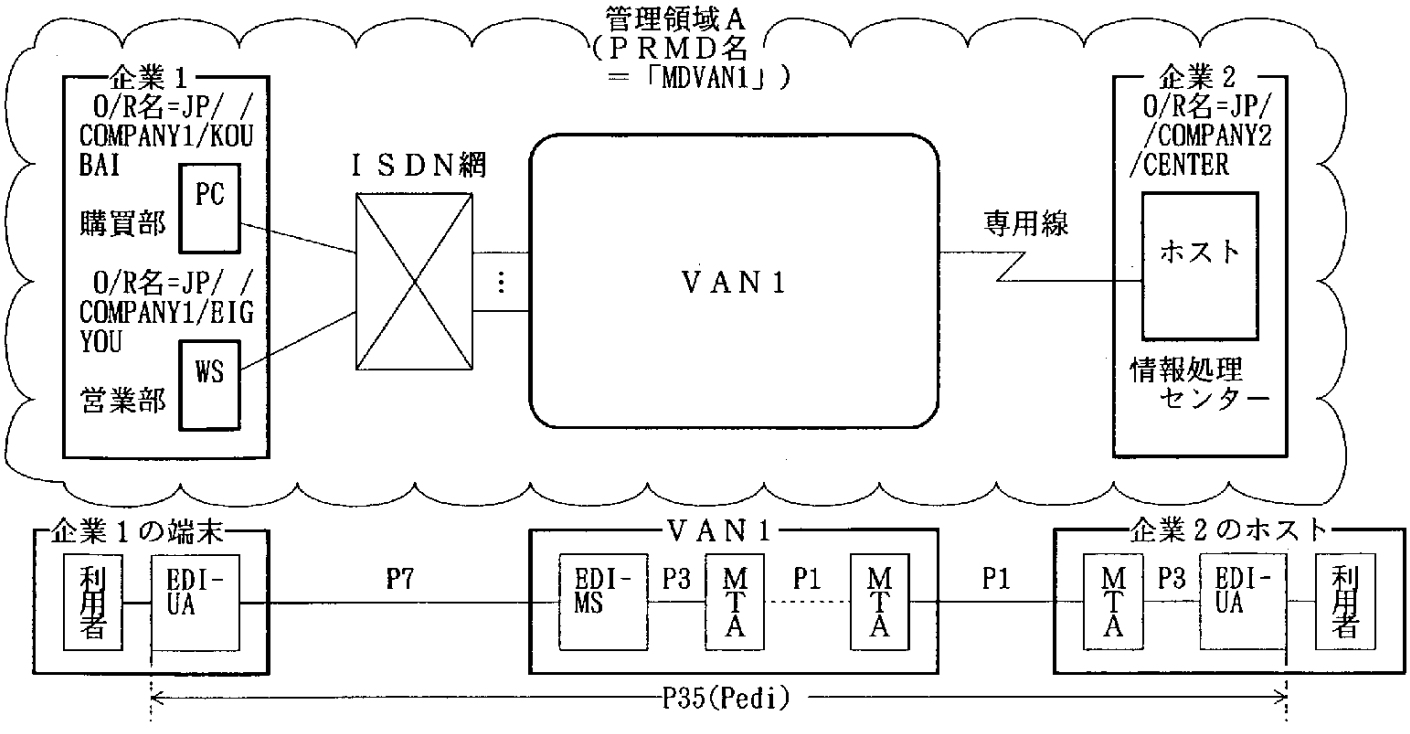


図1.2- 8　ネットワーク構成図とＭＨＳ機能モデル【例　１】

(2) ＶＡＮを利用し、ＰＲＭＤが複数の場合【例　２】

二つのＶＡＮ事業者の相互接続（ＶＡＮ間接続）により提供されるＰｅｄｉサービスを複数企業が利用する形態について説明する。

図1.2- 9において、企業１の端末または企業２のホストは、各々のＶＡＮから払い出されたネットワークアドレス（Ｏ／Ｒ名）により、そのＶＡＮの中で相手を一意に識別できる。【例　１】の場合と同様、ＶＡＮ１、ＶＡＮ２で各々の私設管理領域（ＰＲＭＤ）が設定され、例ではそのＰＲＭＤ名を「MDVAN1」、「MDVAN2」としている。

各々のＶＡＮの中のＯ／Ｒ名付与形態を【例　１】と同様とした場合、一つのＶＡＮに閉じて通信するのならばＰＲＭＤ名を意識せずにＥＤＩメッセージを交換できるが、ＶＡＮ間接続など複数のＶＡＮを経由する場合、相手のＶＡＮを示す経路選択情報としてＰＲＭＤ名を設定する必要がある。なお、ＡＤＭＤ名は本来ならば必須であるが、ＶＡＮ１とＶＡＮ２に閉じた接続を仮定しているため一つのスペースを設定することとする。

図1.2- 9の例では、企業１の端末（ＰＣ：パソコン，ＷＳ：ワークステーション）～企業２のホストの間で、ＶＡＮ１からＶＡＮ２を経由してＥＤＩメッセージの交換が行える。図1.2- 6と比較するとＭＨＳネットワークの部分が「ＶＡＮ１＋ＶＡＮ２」に置き換わる形態となる。ＰＣ（パソコン）からホストにＥＤＩメッセージを送信する場合を例に採ると、ＰＣは受信者Ｏ／Ｒ名に“国名「JP」＋ＡＤＭＤ名「１個のスペース」＋相手ＶＡＮ２のＰＲＭＤ名「MDVAN2」＋各々のＶＡＮで払い出される組織名「COMPANY2」＋利用者が決定する部門名「CENTER」”を設定してメッセージをＶＡＮ１へ発信し、各々のＶＡＮでは、指定された受信者Ｏ／Ｒ名により経路選択を行った後、目的となるホストにメッセージを配信する。これにより、ホストはＰＣからのＥＤＩメッセージを受信できる。

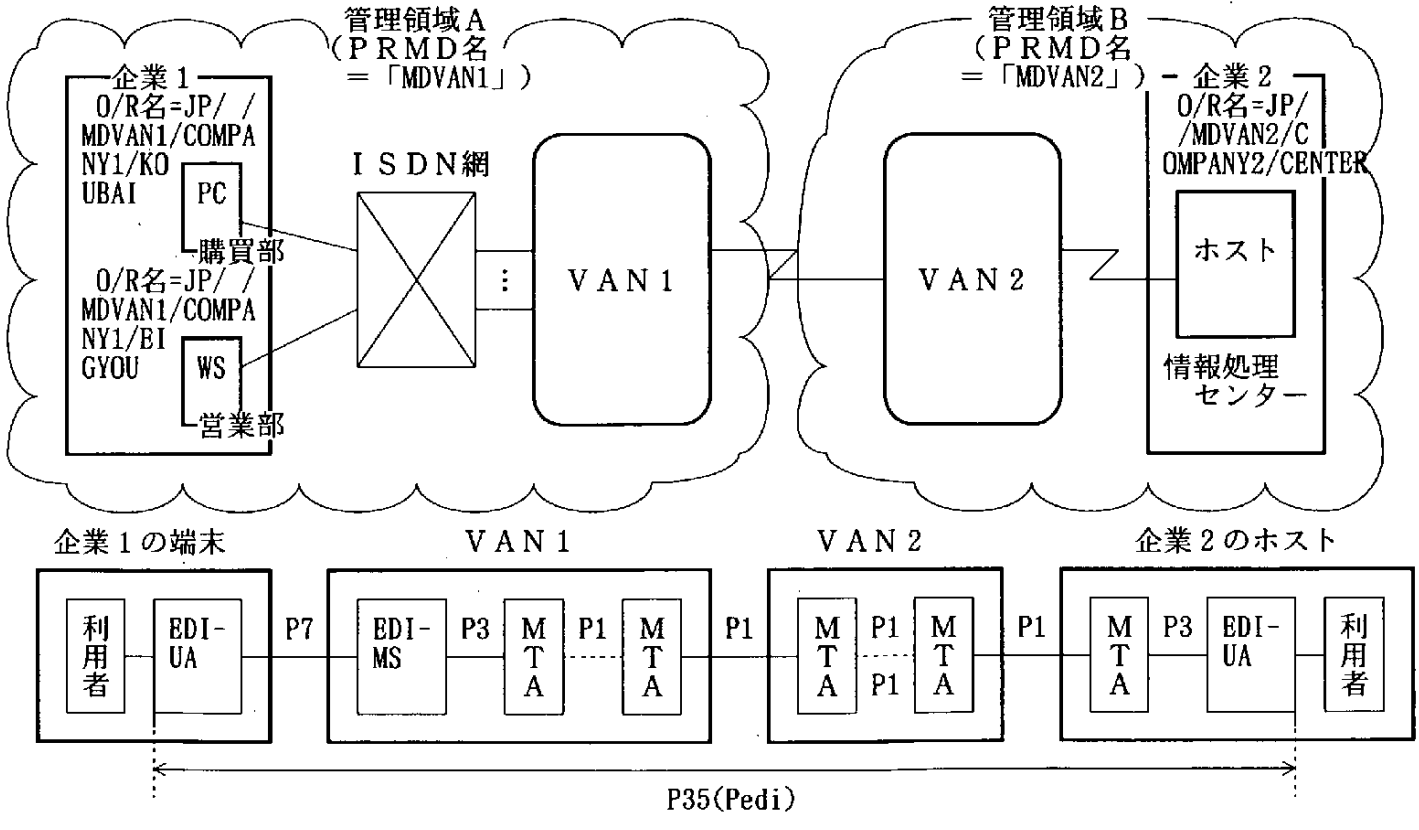


図1.2- 9　ネットワーク構成図とＭＨＳ機能モデル【例　２】

(3) ＶＡＮを利用せずに、ＰＲＭＤが複数の場合【例　3】

三つの企業が相互接続することにより提供される、Ｐｅｄｉサービスの形態について説明する。

図1.2-10において、企業１／企業２／企業３の端末は、企業１と企業２から払い出されたＯ／Ｒ名により、その管理領域の中で相手を一意に特定できる。企業１（企業３を含む）、企業２で各々の私設管理領域（ＰＲＭＤ）が設定され、例ではそのＰＲＭＤ名を「MDCOM1」，「MDCOM2」としている。ただし、企業３は経路選択を行うＭＴＡが存在しないため、その接続先である企業１の管理領域に組み込まれる。

【例　2】と同様、一つの企業（管理領域）内に閉じて通信するのならばＰＲＭＤ名を意識せずにＥＤＩメッセージを交換できるが、管理領域をまたがって複数企業間で通信を行う場合、相手の企業を示す経路選択情報としてＰＲＭＤ名を設定する必要がある。また、ＡＤＭＤ名は本来ならば設定必須であるが、企業１と企業２に閉じた接続を行うことを仮定しているため一つのスペースを設定することとする。

図1.2-10の例では、“企業１の端末（ＰＣ：パソコン，ＷＳ：ワークステーション）”または“企業３の端末（ＷＳ：ワークステーション）”～“企業２の端末”の間で、各々の企業のホストを経由してＥＤＩメッセージの交換が行える。図1.2-6と比較するとＭＨＳネットワークの部分が各企業のホストに置き換わる形態となる。企業３のＷＳから企業２のＷＳにＥＤＩメッセージを送信する場合を例に採ると、ＷＳは受信者Ｏ／Ｒ名に“国名「JP」＋ＡＤＭＤ名「１個のスペース」＋相手企業２のＰＲＭＤ名「MDCOM2」＋各企業にて決定する部門名「BIGYOU」”を設定してメッセージをホスト１へ発信し、各々のホストでは指定された受信者Ｏ／Ｒ名により経路選択を行った後、目的となる企業２のＷＳにメッセージを配信する。これにより、企業３からのＥＤＩメッセージを受信できる。

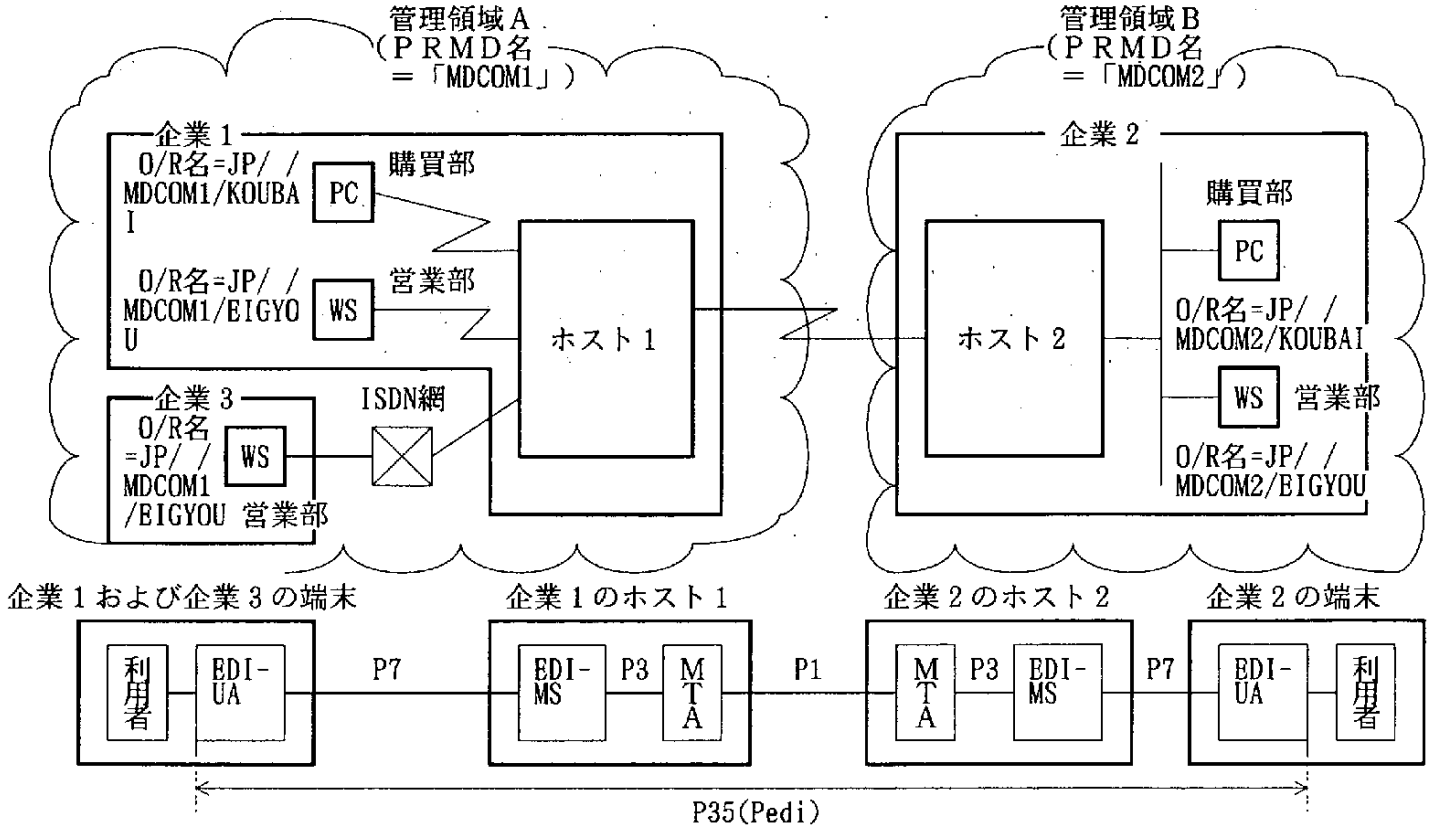


図1.2-10　ネットワーク構成図とＭＨＳ機能モデル【例　3】

⑷ ＶＡＮを利用せずに、ＡＤＭＤとＰＲＭＤが混在する場合【例　４】

電気通信事業者が提供するＰｅｄｉサービスを企業が利用する形態を説明をする。本節では電気通信事業者が提供するＰｅｄｉサービスを含めた電子メールサービスを公衆電子メール（ＭＨＳ）サービスと呼ぶこととする。図1.2-11の例では、自社内のＭＨＳネットワークを構築するとコスト面で割高になってしまうため、公衆電子メールサービス（例えば、NTT-PCｺﾐｭﾆｹｰｼｮﾝｽﾞが提供する「ＮＴＴメール」など）を利用し、全国的なネットワークを構築する形態を示している。

管理領域には、私設管理領域（ＰＲＭＤ）と主管機関管理領域（ＡＤＭＤ）の二つがあることを「１．１．４　管理領域」で述べた。以降、具体的な例を用いて、その違いを説明する。

【例　１】～【例　３】の場合では、ＶＡＮ業者のような私的な組織がネットワークアドレス（Ｏ／Ｒ名）を特定しているのに対し、図1.2-11に示す九州支社の端末が組み込まれる管理領域では、公的な機関により“認可（認定）”された電気通信事業者（例えばＮＴＴ）がネットワークアドレス（Ｏ／Ｒ名）を特定することとなる。このような管理領域を主管機関管理領域（ＡＤＭＤ）と呼ぶ。

企業がＡＤＭＤに接続する形態は、その企業が管理領域（ＰＲＭＤ）を持っているかどうかにより、以下のパターンが考えられる。（図1.2-12参照）

1)　ＰＲＭＤ接続型

公衆ＭＨＳサービスの運用するＡＤＭＤに対し、企業はそのＡＤＭＤ配下のＰＲＭＤとして接続する。【例　４】では東京本社の接続形態を指す。

2)　ＡＤＭＤ組み込み型

企業はＰＲＭＤを持っていないので、公衆ＭＨＳサービスの運用するＡＤＭＤに組み込まれる形で接続する。【例　４】では九州支社の接続形態を指す。

図1.2-11の例では、企業１の九州支社内端末～東京本社のホストの間で、公衆ＭＨＳネットワークを経由してＥＤＩメッセージの交換が行える。図1.2-6と比較するとＭＨＳネットワークの部分が「公衆ＭＨＳネットワーク」に置き換わる形態となる。企業１のＰＣ（パソコン）から本社ホストにＥＤＩメッセージを送信する場合を例に採ると、ＰＣは受信者Ｏ／Ｒ名に“国名「JP」＋ＡＤＭＤ名「PEMAIL」＋電気通信事業者が払い出した企業１のＰＲＭＤ名「MD COM1」＋企業で決定する部門名「HONSHACENTER」”を設定してメッセージを公衆ＭＨＳネットワークへ発信し、公衆ＭＨＳネットワークでは、指定された受信者Ｏ／Ｒ名により経路選択を行った後、目的となる本社ホストにメッセージを配信する。これにより、九州支社のＰＣからのＥＤＩメッセージを受信できる。

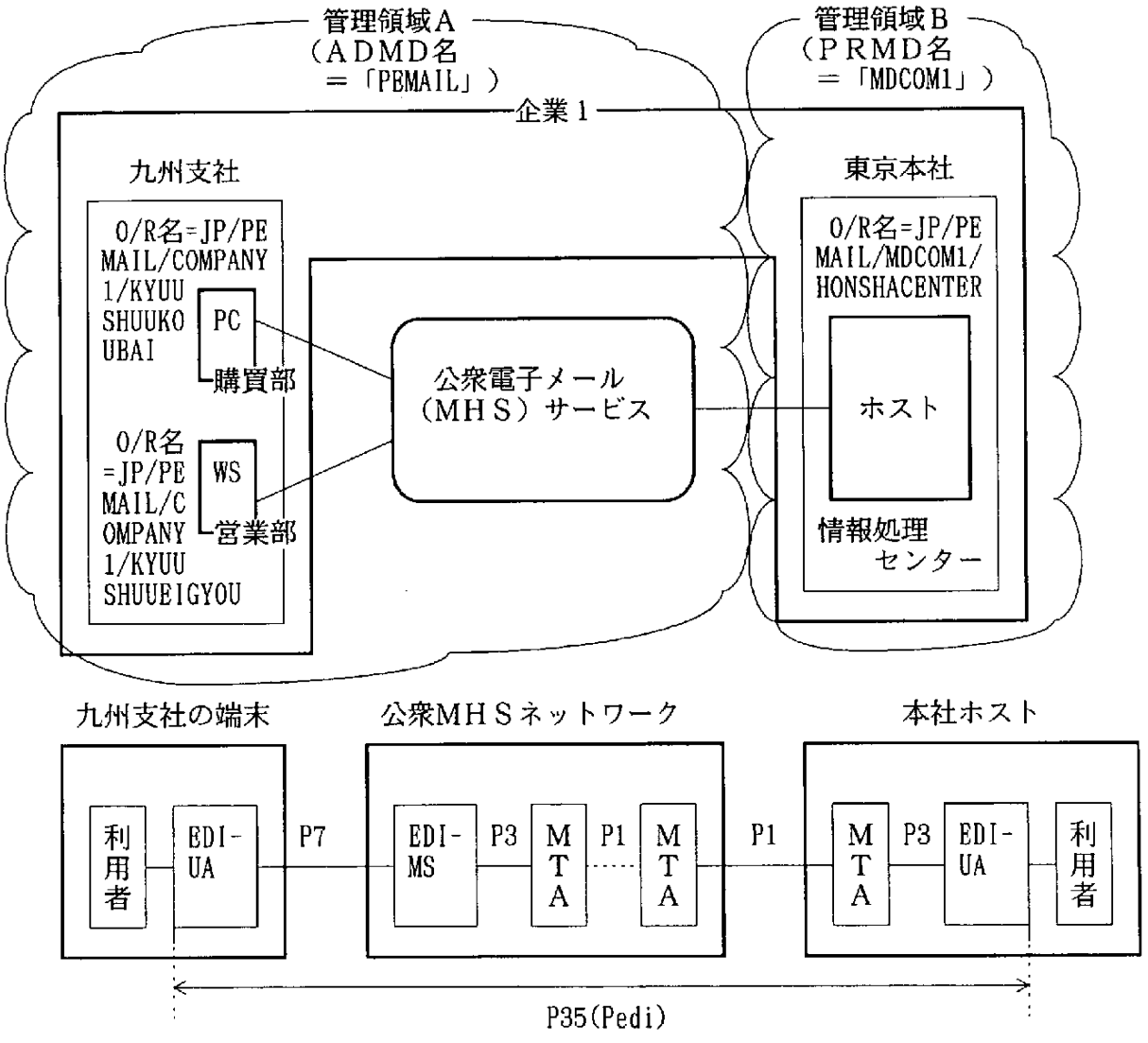


図1.2-11　ネットワーク構成図とMHS機能モデル【例　4】

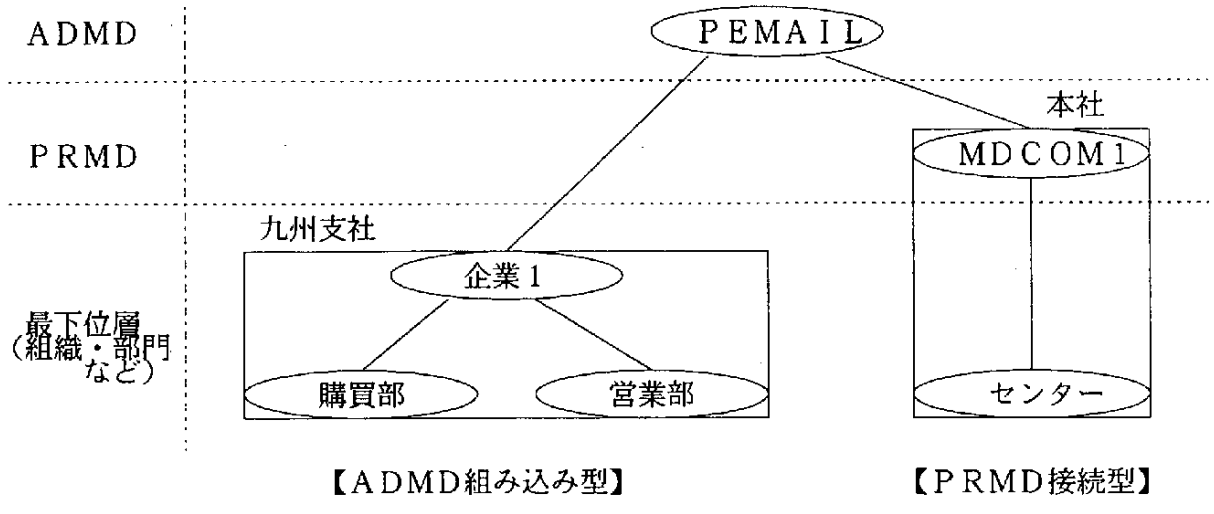


図1.2-12　ADMD接続形態

第 2 章

Ｐｅｄｉサービス概要

2. 1 概 要

第2章では、ＥＤＩメッセージ通信サービスで利用可能なサービスを紹介する。ＥＤＩメッセージ通信サービス（Ｐｅｄｉ）は、ＭＨＳ勧告が規定するメッセージ転送サービスおよびメッセージ格納サービスを利用し、さらにＥＤＩの実現に必要となる機能を追加するという方法で標準化されている。このため、Ｐｅｄｉを理解するためには、ＭＨＳのサービスに関する理解も必要である。本概説書では、このような主旨から、基本となるＭＨＳのサービスについても紹介し、その上でＰｅｄｉの追加規定を紹介することとした。

しかし、一方でＰｅｄｉを理解するためには、全体としてどのようなサービスが提供されるのか、ということも重要である。このため、本概説書では、ＭＨＳのサービスおよびＰｅｄｉの追加サービスを再整理し、類似した機能で分類し、サービスの説明をすることとした。

表2.1- 1は、この観点から整理したサービス分類を示す。本章の「２．２　基本サービス」以降では、この分類単位でサービスの詳細を説明している。なお、この分類は、ＭＨＳ勧告に規定されるものではなく、本概説書に限定して作成したものであることをお断りしておく。

表2.1- 1　サービス分類

分類	概要
基本サービス	ＥＤＩのサービス概要およびサービス全般の共通的事項
配信機能	メッセージの配送に関わる機能
配信通知機能	メッセージの配送の結果として報告される通知機能
変換サービス	メッセージ内容の符号化方式の変換機能
配布先表	配布先表に関する機能
情報表示機能	利用者へ通知される様々な情報に関する機能
あて先変更サービス	配送時に適用されるあて先の変更機能
安全保護サービス	メッセージ内容の保証などの安全保護に関わる機能
ディレクトリ利用サービス	ＭＨＳでディレクトリを利用する機能
物理的配達サービス	郵便などの物理的配達システムに関連する機能
メッセージ格納サービス	ＭＳ（メッセージ格納）の操作に関する機能

また、これらのサービスの整理と併せて、本概説書においてメッセージ内容／ＥＤＩメッセージの用語の使い分けを以下のとおり明確にした。メッセージ内容／ＥＤＩメッセージの関係を図2.1- 1に示す。メッセージ構成の詳細については第１章を参照されたい。

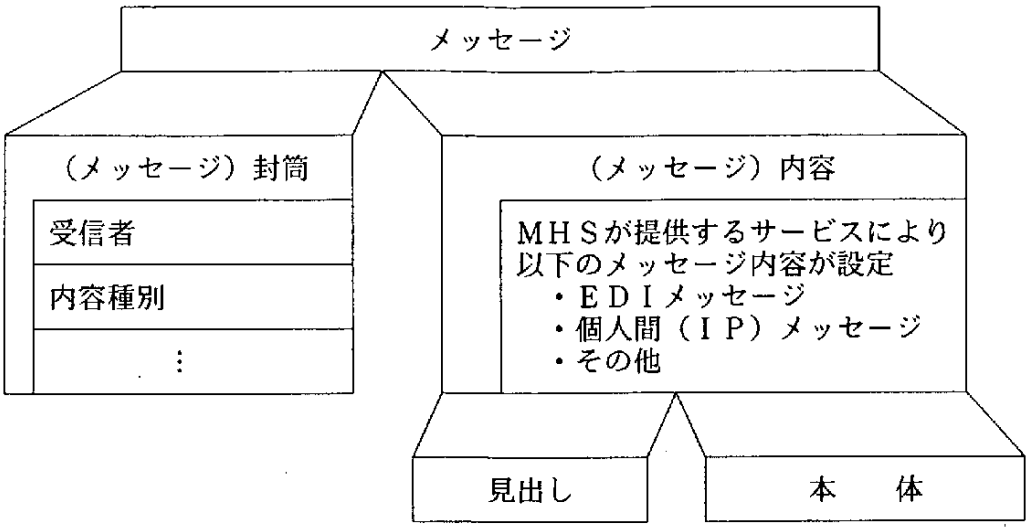


図2.1-1　メッセージ内容／ＥＤＩメッセージの関係

メッセージ内容は図2.1-1に示すとおりＭＨＳ上で提供される各サービスに依存した名前で表現される。例えば、ＰｅｄｉサービスではｅＤＩメッセージ、ＩＰＭサービスではＩＰメッセージのようになる。これらの違いを踏まえ、本概説書ではメッセージ内容／ＥＤＩメッセージの用語の使い分けを以下のとおり整理した。

① Ｐｅｄｉとして追加されたサービス（Ｐｅｄｉに特化したサービス）の場合
　メッセージ内容を「ＥＤＩメッセージ」と表現。

② ＭＨＳ全般のサービスの場合
　メッセージ内容にはＥＤＩメッセージ，ＩＰメッセージ等が設定されるため、これらを取りまとめて「メッセージ内容」または「内容」として表現。

③ ＥＤＩメッセージ，ＩＰメッセージ等と区別して用語を使用する場合
　メッセージ内容を「ＥＤＩメッセージ」または「ＩＰメッセージ」等と表現。

なお、本概説書で取り上げたＰｅｄｉに特化したサービスは以下のとおりである。

- 2.2.1　ＥＤＩメッセージ通信
- 2.2.2　ＥＤＩ通知と回送
- 2.7.8　ＥＤＩＦＡＣＴ情報表示
- 2.9.7　発信内容の否認不能
- 2.9.8　ＥＤＩ通知証明およびＥＤＩ通知の否認不能
- 2.9.13　受信内容証明および受信内容の否認不能

2. 2 基本サービス

2. 2. 1 ＥＤＩメッセージ通信

ＥＤＩメッセージ通信ユーザは、ＥＤＩメッセージの送信・受信を行う。ＥＤＩメッセージ通信ユーザにＥＤＩメッセージ通信サービスを提供するものをＥＤＩメッセージ通信システムという。ＥＤＩメッセージ通信システムは、ＥＤＩ－ＵＡ（以下ＵＡと呼ぶ）、ＥＤＩ－ＭＳ（以下ＭＳと呼ぶ）、ＭＴＡ等により構成される。ＥＤＩメッセージ通信システムとそれを利用するＥＤＩメッセージ通信ユーザを含めてＥＤＩメッセージ通信環境という。

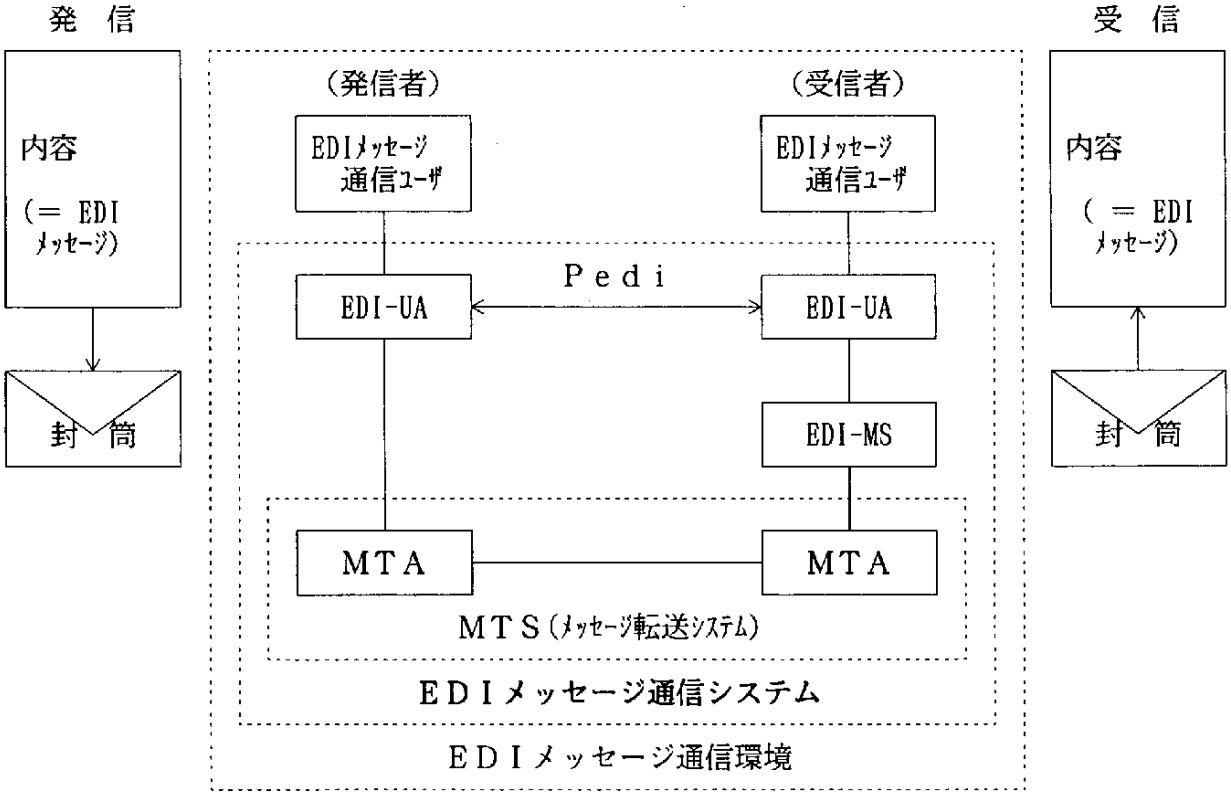


図2.2-１ ＥＤＩメッセージ通信

2. 2. 2　ＥＤＩ通知と回送

(1)　ＥＤＩ通知

ＥＤＩ－ＵＡ間（図中の発信ＵＡ、受信ＵＡを指す）の送達確認にはＥＤＩ通知（EDIN：EDI Notification）が用いられる。ＥＤＩ通知には、以下の三種類がある。

・肯定通知（PN: Positive Notification）

受信ＵＡが、ＥＤＩメッセージ責任を受け入れた場合に発信ＵＡへ返送する通知である。具体的には、ＥＤＩメッセージを受信者に渡した場合と、本体部を変更（追加・削除）して回送した場合である。回送については後述する。

・否定通知（NN: Negative Notification）

受信ＵＡがＥＤＩメッセージ責任の受け入れを拒否した場合、つまりＥＤＩメッセージを拒否したかまたはＥＤＩメッセージの回送を中止した場合に発信ＵＡへ返送する通知である。ＥＤＩメッセージの拒否とは、タイムアウト、ＥＤＩ交換に構文誤りがあった場合を指す。

・回送通知（FN: Forwarded Notification）

受信ＵＡがＥＤＩメッセージを変更せずに回送し、かつそれ以前にＰＮ、ＮＮが発信ＵＡへ返送されていない場合に返送する。

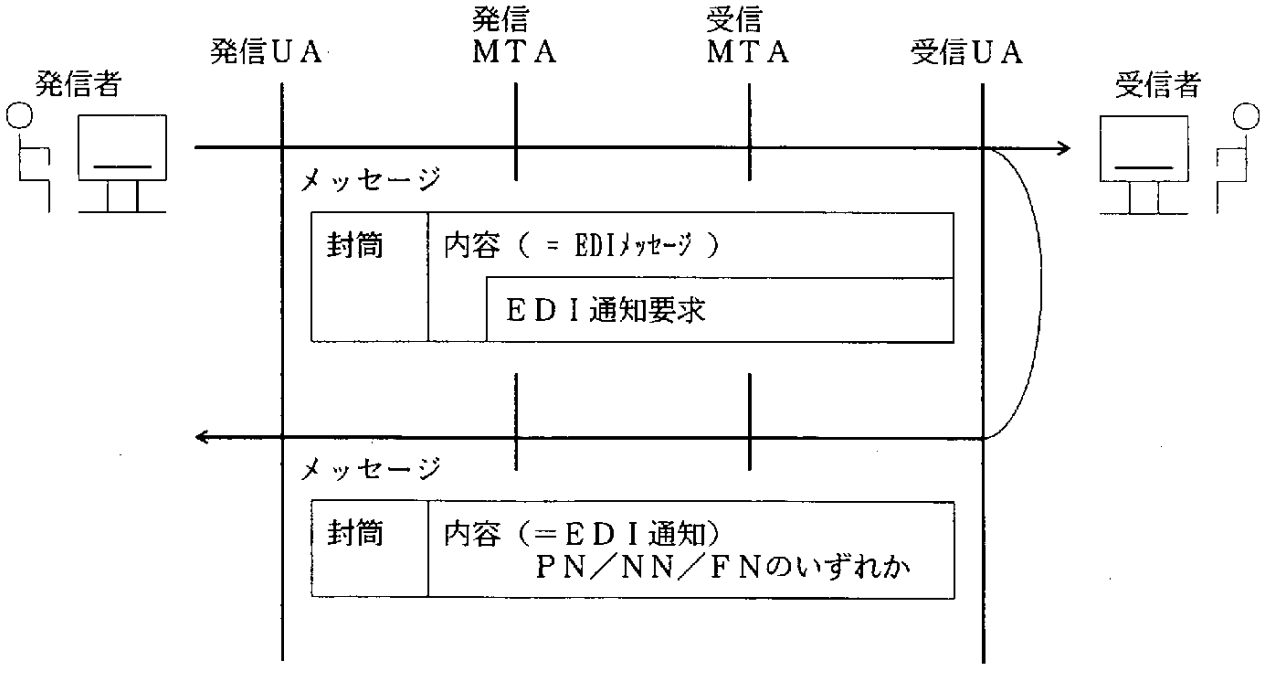


図2.2-2　ＥＤＩ通知

(2) ＥＤＩ回送とＥＤＩメッセージ責任

（ａ）ＥＤＩ回送

ＥＤＩ回送とは、第一受信者が受信したＥＤＩメッセージをほかの受信者に向けて転送することである（図2.2- 3(1)）。ＥＤＩ回送を行う場合のＥＤＩ通知については、以下の例で説明する。Ｐｅｄｉでは、ＥＤＩ回送やＥＤＩ通知のためにＥＤＩメッセージ責任という概念が新たに定義されている。

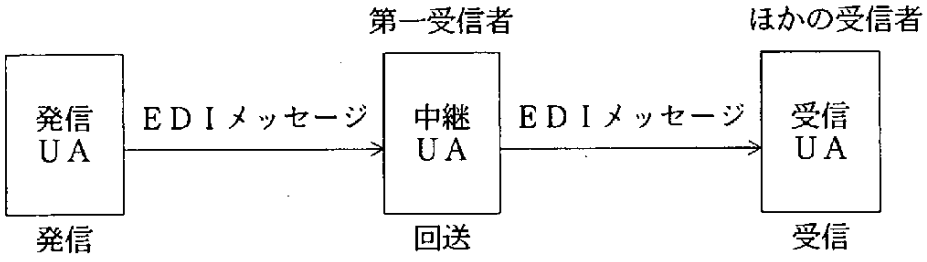


図2.2- 3(1) ＥＤＩ回送

（ｂ）ＥＤＩメッセージ責任（ＥＤＩＭ責任）

ＥＤＩメッセージ責任とは、誰がＥＤＩメッセージの受信や回送に責任を持つかを明確にするための概念である。ＥＤＩメッセージ責任を保持する利用者が、ＥＤＩメッセージを処理することができる。例えば、ＥＤＩメッセージの本体部の変更（追加・削除等）やＭＳからの取り出しを行うためには、ＵＡはＥＤＩメッセージ責任を受けいれていなければならない。

(3) ＥＤＩメッセージの転送形態

ＥＤＩメッセージの転送の形態としては、以下の3つのケースが考えられる。

・ケース１：回送のない場合
・ケース２：回送を行う（ＥＤＩメッセージ責任を回送する）場合
・ケース３：回送を行う（ＥＤＩメッセージ責任を回送しない）場合

ここでは、発信ＵＡ、中継ＵＡがＥＤＩ通知を要求したと仮定してそれぞれのケースについて説明する。

（ａ）ケース１：回送のない場合

発信者が受信者へ直接ＥＤＩメッセージを送るケースである。ＥＤＩメッセージは、発信ＵＡを通じて受信ＵＡへ発信される。受信ＵＡが発信ＵＡに返すＥＤＩ通知は、

・肯定通知（ＰＮ）
・否定通知（ＮＮ）

の２種類である。

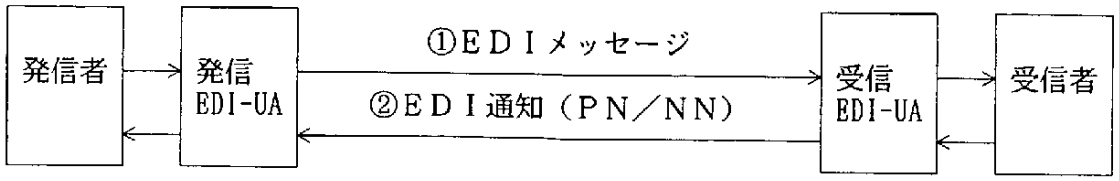


図2.2- 3(2)　ＥＤＩメッセージ転送形態（回送のない場合）

（ｂ）ケース２：回送を行う（ＥＤＩメッセージ責任を回送する）場合

中継ＵＡがＥＤＩメッセージを回送する際にＥＤＩメッセージ責任も回送する場合である。発信ＵＡから中継ＵＡへと送られたＥＤＩメッセージ（①）は、中継ＵＡの判断に基づいて受信ＵＡへ回送される（②）。その際、回送通知（ＦＮ）が中継ＵＡから発信ＵＡへ返される（③）。中継ＵＡはＥＤＩメッセージ責任を受け入れないので、中継ＵＡにおいてはＥＤＩメッセージの変更（追加・削除）は全く行われない。

・ＥＤＩメッセージの回送に成功した場合、受信ＵＡは発信ＵＡに肯定通知（ＰＮ）または否定通知（ＮＮ）を返す（④-1）。

・ＥＤＩメッセージの回送に失敗した場合、中継ＵＡは受信ＵＡへの回送のリトライが可能である。リトライをもう行わないと決定した場合には、否定通知（ＮＮ）が中継ＵＡから発信ＵＡへ送られる（④-2, ⑤）。ただし、否定通知（ＮＮ）を送るかどうかは中継ＵＡに選択権がある。

このケースでは、中継ＵＡとしてＶＡＮ事業者が考えられる。

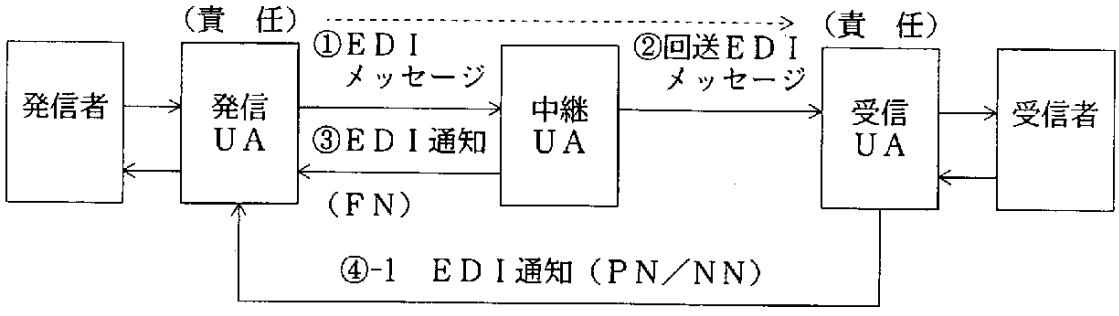


図2.2- 3(3)　ＥＤＩメッセージ転送形態（責任の回送に成功した場合）

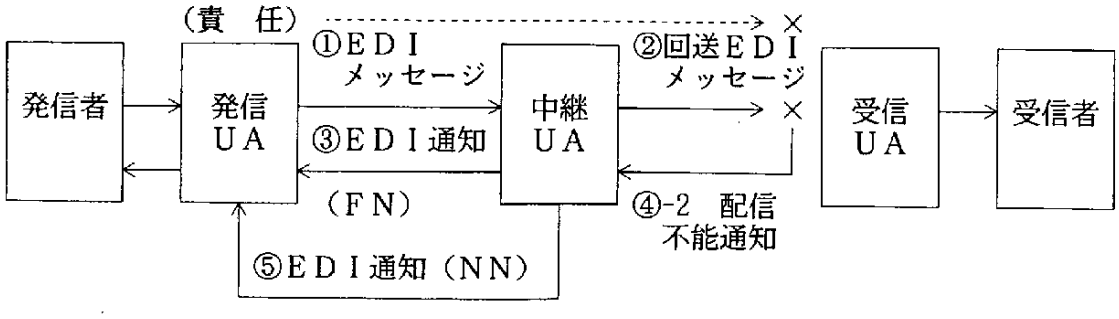


図2.2- 3(4)　ＥＤＩメッセージ転送形態（責任の回送に失敗した場合）

（ｃ）ケース３：回送を行う（ＥＤＩメッセージ責任を回送しない）場合

中継ＵＡがＥＤＩメッセージを回送する際にＥＤＩメッセージ責任を一度受け入れる場合である。中継ＵＡは、ＥＤＩメッセージを受信したとき、発信ＵＡに対し肯定通知（ＰＮ）を返す（②）。その後、中継ＵＡは受信ＵＡに回送ＥＤＩメッセージを送信する（③）。中継ＵＡはＥＤＩメッセージ責任を受け入れているので、ＥＤＩメッセージ回送にあたって、ＥＤＩメッセージの本体部を変更（追加・削除）することも可能である。このケースの場合、ケース２の時と異なり、受信ＵＡは発信ＵＡに対してではなく、中継ＵＡに対してＥＤＩ通知を返す（④）。このケースでは、組織のセンタを中継ＵＡとすることが考えられる。

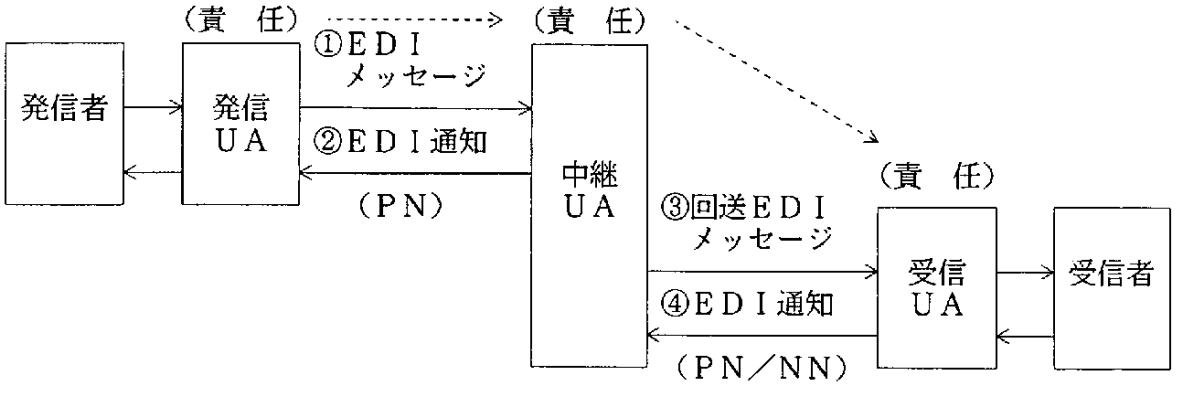


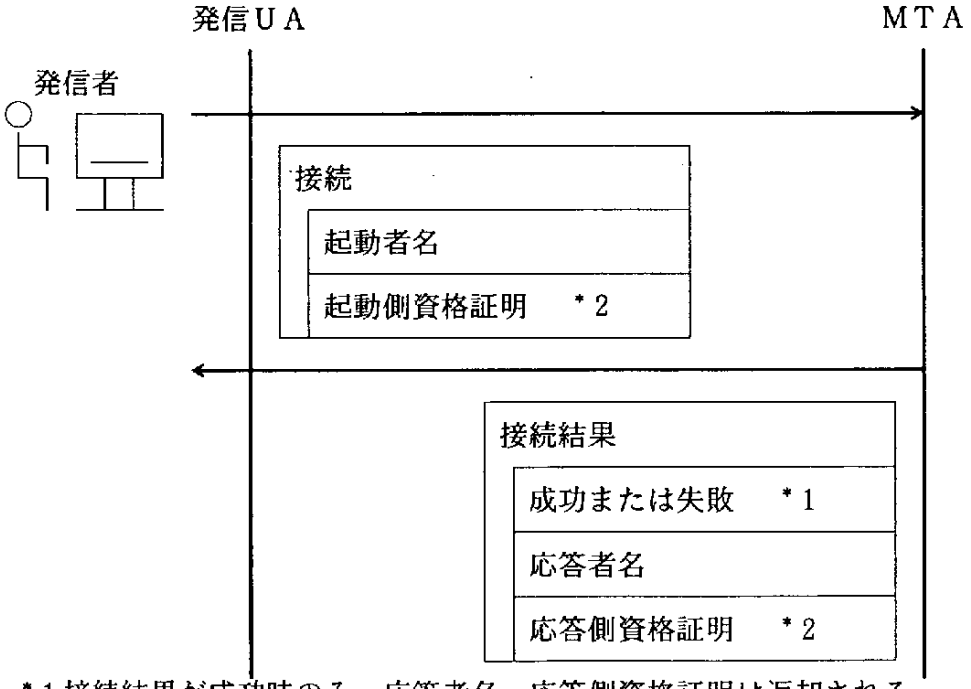
図2.2- 3(5)　ＥＤＩメッセージ転送形態（責任を回送しない場合）

2. 2. 3　アクセス管理

隣接する構成要素間（ＵＡ－ＭＴＡ，ＭＴＡ－ＭＴＡ，ＭＴＡ－ＭＳ，ＭＳ－ＵＡ）は、簡易認証による資格証明を交換して互いに相手を識別し、接続を試みる。このとき、応答側は、起動側資格証明により起動者側が自らを偽っていないことを確認した上で、起動者に（接続に引き続いて要求されるであろう）操作を要求する資格があるかどうかを判断し、接続の応答を行う。もし「起動者に操作を要求する資格がある」と応答側が判断した場合は、成功の旨の接続結果を起動者側に応答する。そうでない場合は、接続誤り、つまり失敗の旨の接続結果を起動者側に応答する。接続に失敗した場合（および操作終了後に接続を解放した後）は、改めて接続に成功するまで起動者側は操作を要求できない。

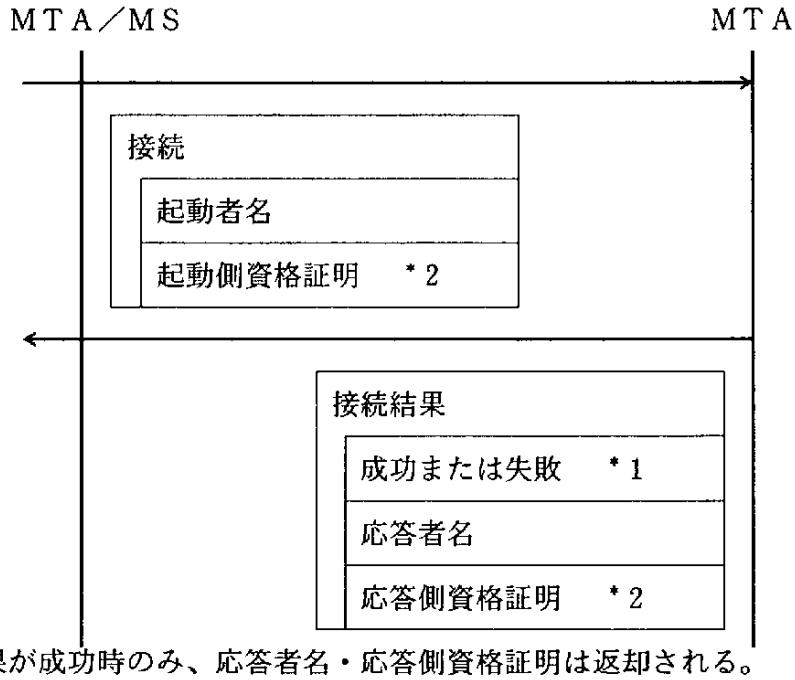
資格証明には、パスワードなどを用いた簡易認証に基づく起動側資格証明および応答側資格証明が用いられる。

なお、より安全なアクセス管理の方式は、暗号化技術を用いた厳密認証に基づく機密保護付きアクセス管理（「2.9.1」参照）によって提供される。

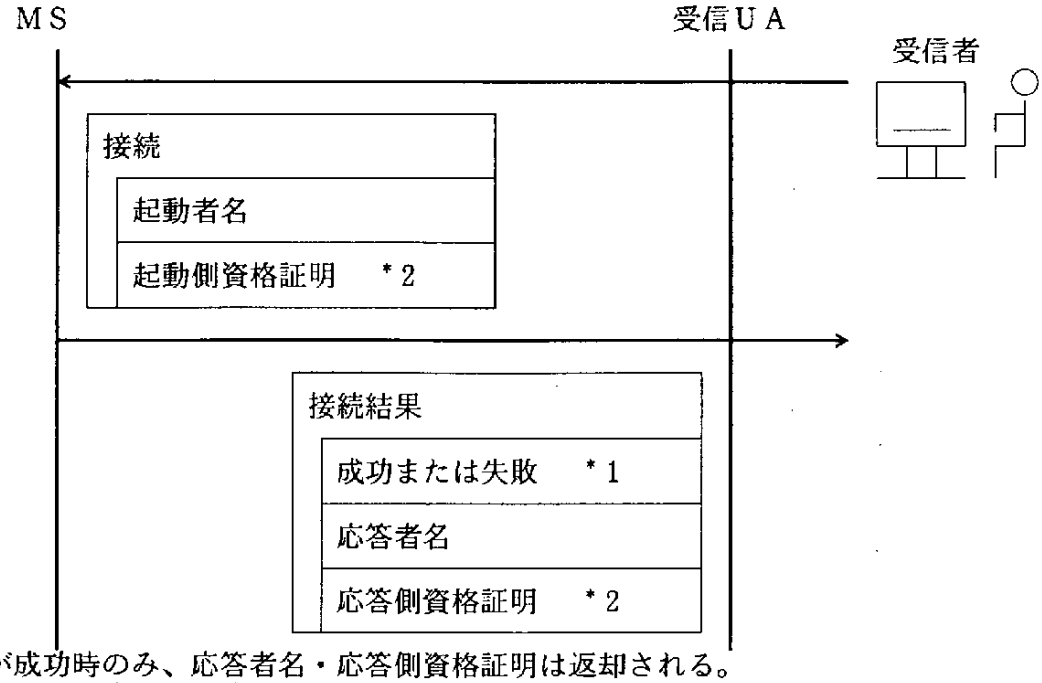


＊1 接続結果が成功時のみ、応答者名・応答側資格証明は返却される。
＊2 起動側資格証明・応答側資格証明はパスワード等を含んでおり、相手の識別情報を簡易に認証するのに使用される。

図2.2- 4(1)　アクセス管理



*1 接続結果が成功時のみ、応答者名・応答側資格証明は返却される。
*2 起動側資格証明・応答側資格証明はパスワード等を含んでおり、相手の識別情報を簡易に認証するのに使用される。



*1 接続結果が成功時のみ、応答者名・応答側資格証明は返却される。
*2 起動側資格証明・応答側資格証明はパスワード等を含んでおり、相手の識別情報を簡易に認証するのに使用される。

図2.2- 4(2)　アクセス管理（続き）

2. 2. 4　利用者／ＵＡ能力の登録

受信ＵＡは、受信ＭＴＡに対して、以下の能力を登録することができる。

1）配信可能内容種別

2）配信可能最大内容長

3）配信可能符号化情報種別

受信ＭＴＡは、登録された能力を超えたり、適合していないメッセージや打診の配信を防止し、配信不能通知を返す。

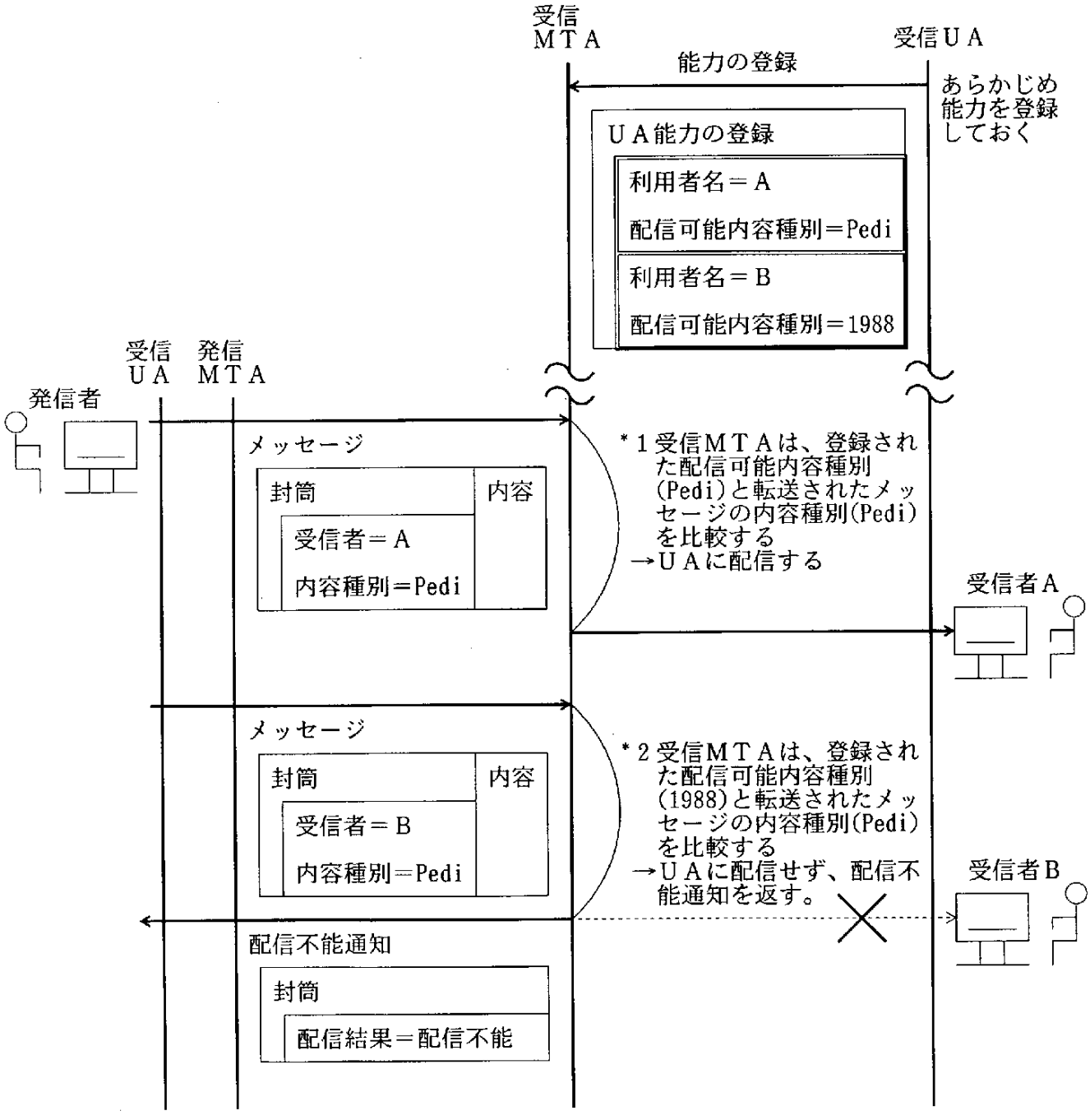


図2.2- 5　利用者／ＵＡ能力の登録

2. 3 配信機能

2. 3. 1 同報

発信ＵＡは、発信した一つのメッセージを複数の受信ＵＡへ配信することができる。（指定された全ての受信ＵＡに同時に配信することを意味していない。）

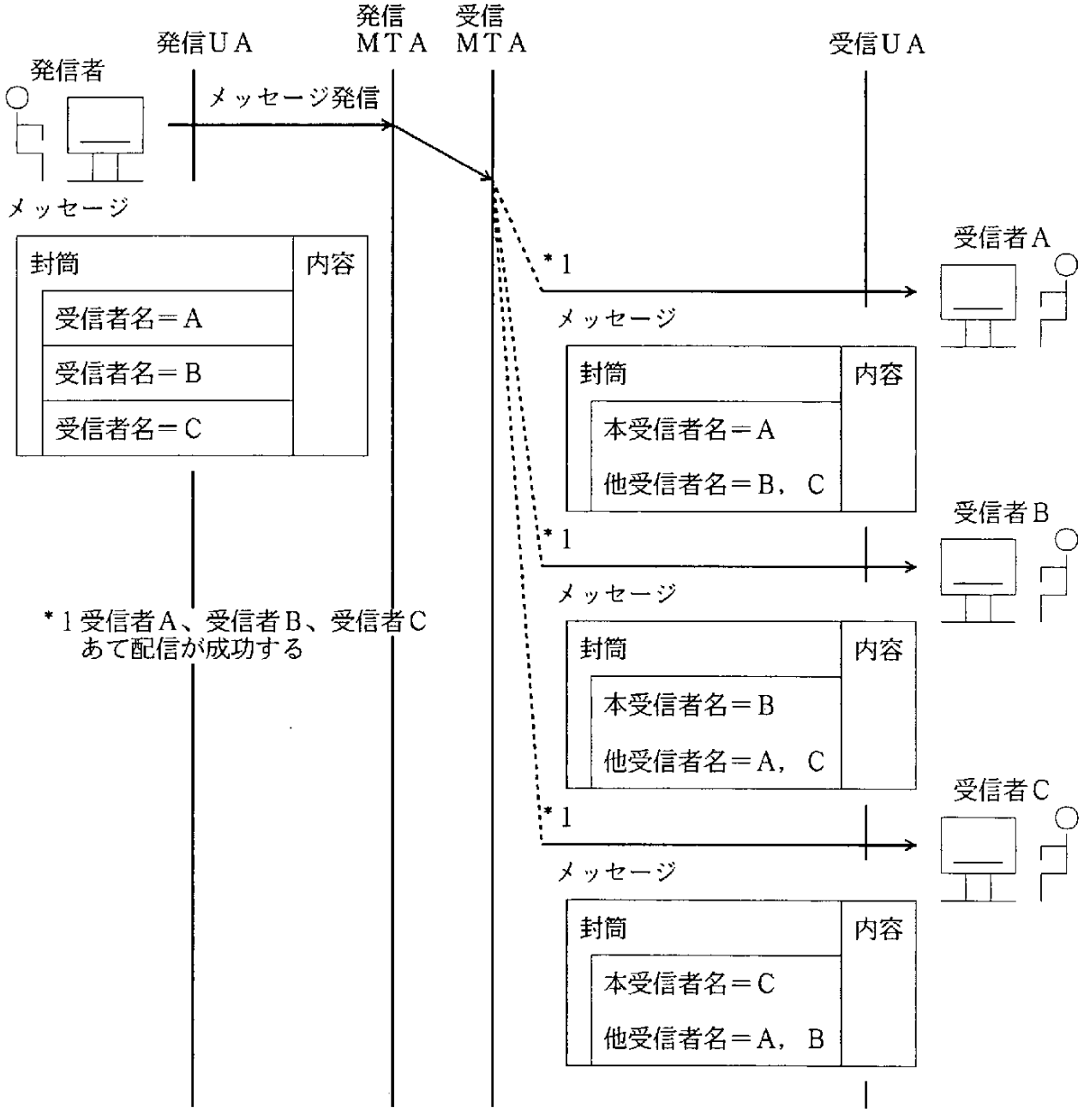


図2.3-1 同報

2. 3. 2　配信優先度選択

発信ＵＡは、通常のメッセージ配信に対する相対的な優先度として、“不急”または“緊急”のメッセージの発信を、各ＭＴＡに指示できる。なお、特に優先度が指定されない場合、相対的な優先度として、“普通”の優先度が仮定される。もちろん、明示的に“普通”の優先度を指定しても良い。

本指定の表示は、メッセージと共に受信者に送られる。

（注）優先度の値による具体的な処置は、ＭＨＳ実装システムが決定する。

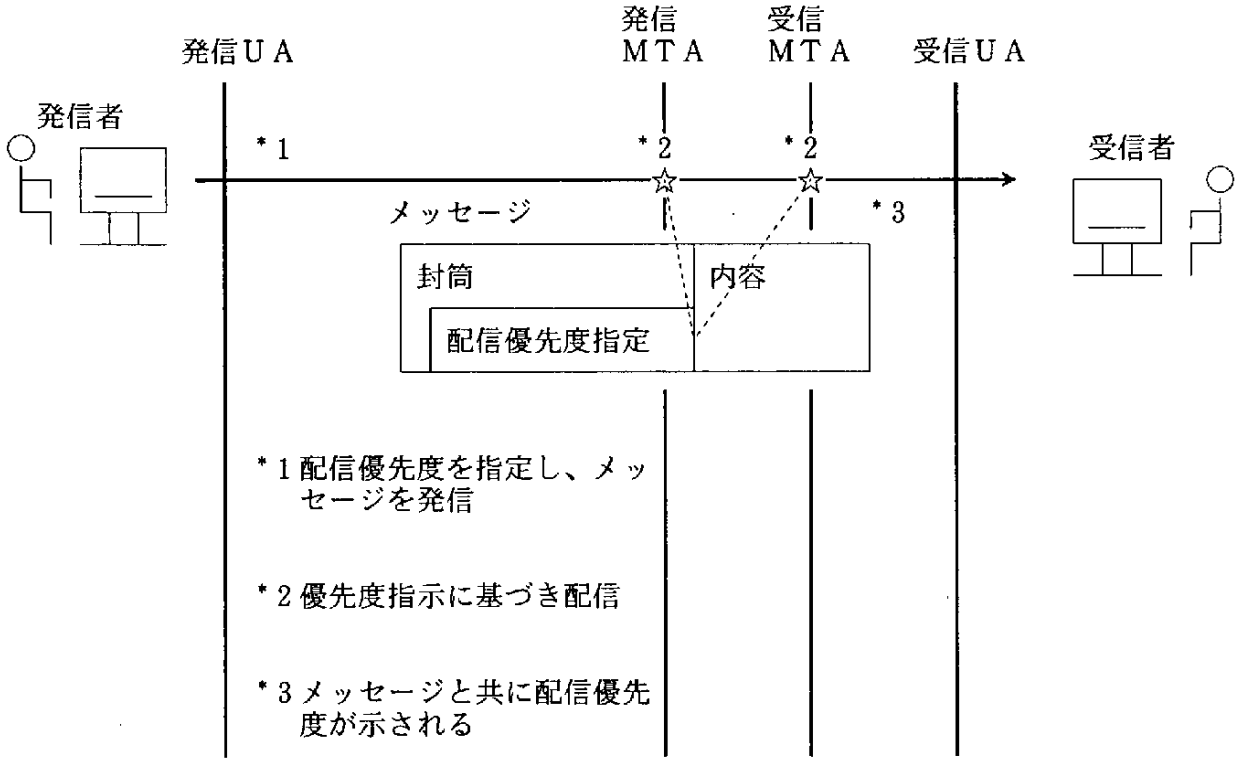


図2.3- 2　配信優先度

2. 3. 3　遅延配信・遅延配信取り消し

(1) 遅延配信

発信ＵＡは、指定した日時以前に発信メッセージを配信しないよう各ＭＴＡ（図の例では発信ＭＴＡ）に指示できる。この配信は、指定日時に達した後、できるだけ速やかに行われるが、指定日時の前に配信されることはない。遅延配信のために指定される日時の期限（例として、～か月先、等）は、発信者の属する管理領域によって決定される事項である。

例：発信者の属する管理領域が日本、受信者の属する管理領域がアメリカの場合
　　日本とアメリカの時差を補うために遅延配信は有効であるが、そのときに指定される配信時刻は発信側の日本において、アメリカとの時差を考慮し決定する事項である。

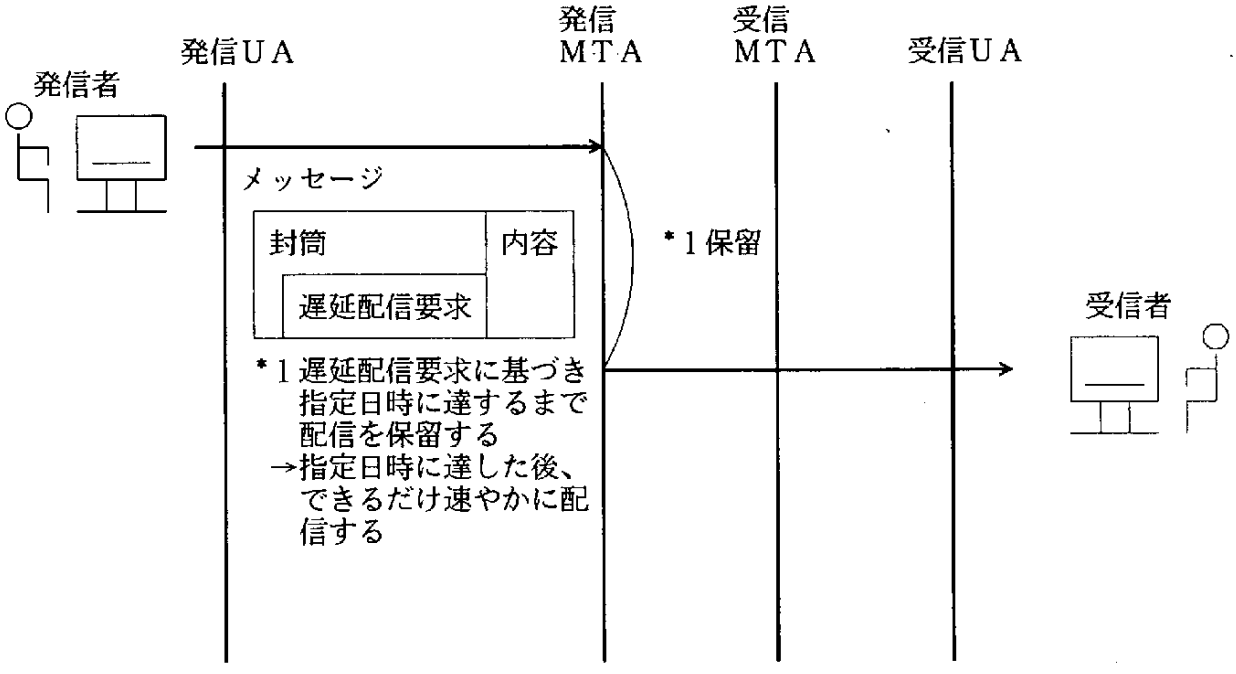


図2.3- 3　遅延配信

(2) 遅延配信取り消し

発信ＵＡは、以前に遅延配信を指定したメッセージの取り消しを各ＭＴＡ（図の例では発信ＭＴＡ）に指示できる。ただし、遅延配信取り消しの試みは常に成功するとは限らない。遅延配信取り消しが失敗する例としては、遅延配信時刻が過ぎてから取り消しを指示した場合等が考えられる。

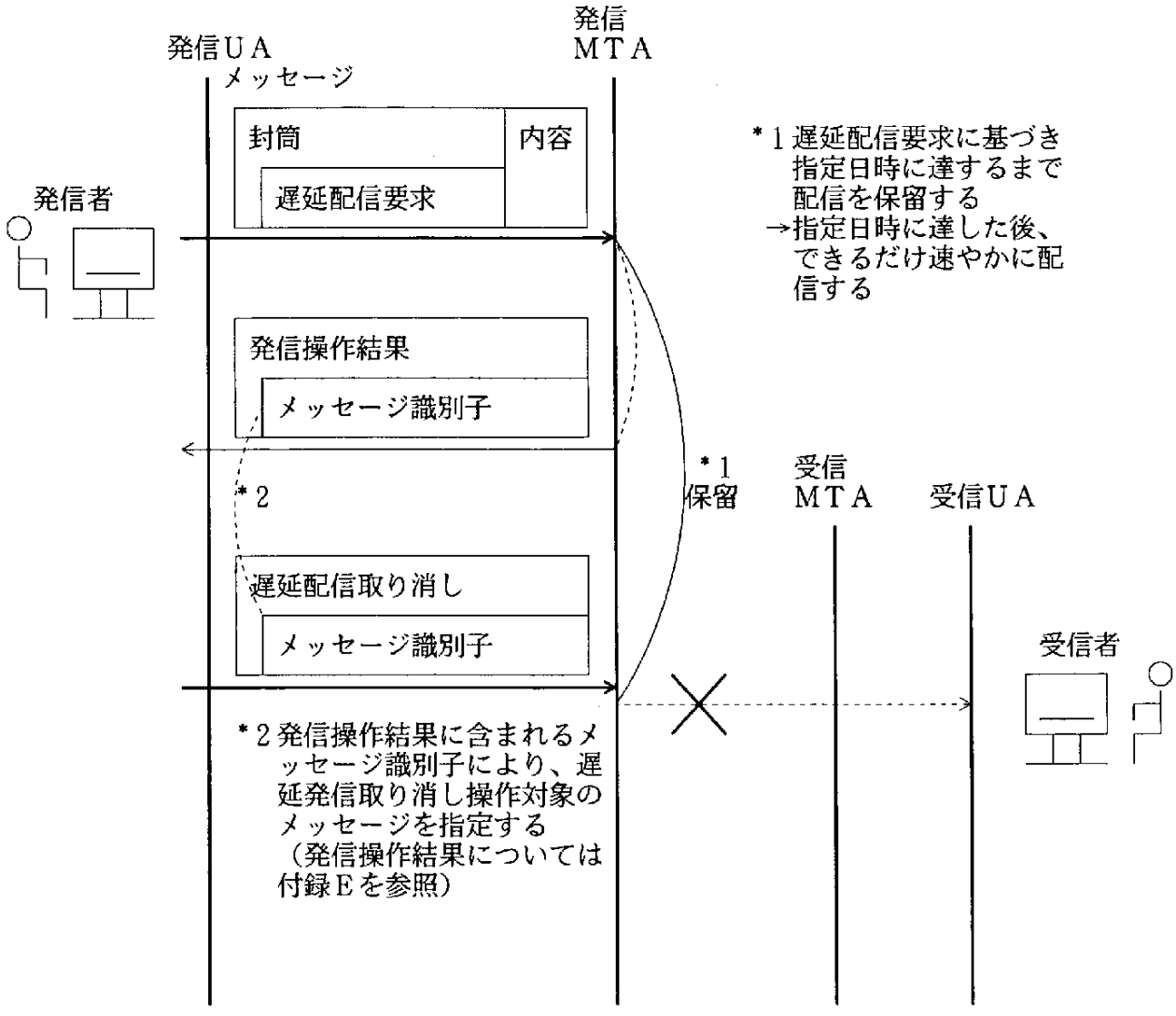


図2.3-4 遅延配信取り消し

2. 3. 4　配信保留

受信者は受信ＭＴＡに対して自分あてのメッセージ（通知も含む）を一時的に保留するよう要求することができる。

受信ＭＴＡは受信者から保留の解除を受けるまで最大保留時間内メッセージを保留する。保留の理由としては、符号化情報種別、内容種別、最大内容長、優先度等の値によって受信者（ＵＡ）が一時的に受信できない状態が想定される。最大保留時間は、ＭＨＳ実装システム側で運用を考慮した値を設定する。

受信ＭＴＡは、最大保留時間を過ぎてもメッセージを配信できない場合、発信者に配信不能通知を返却する。

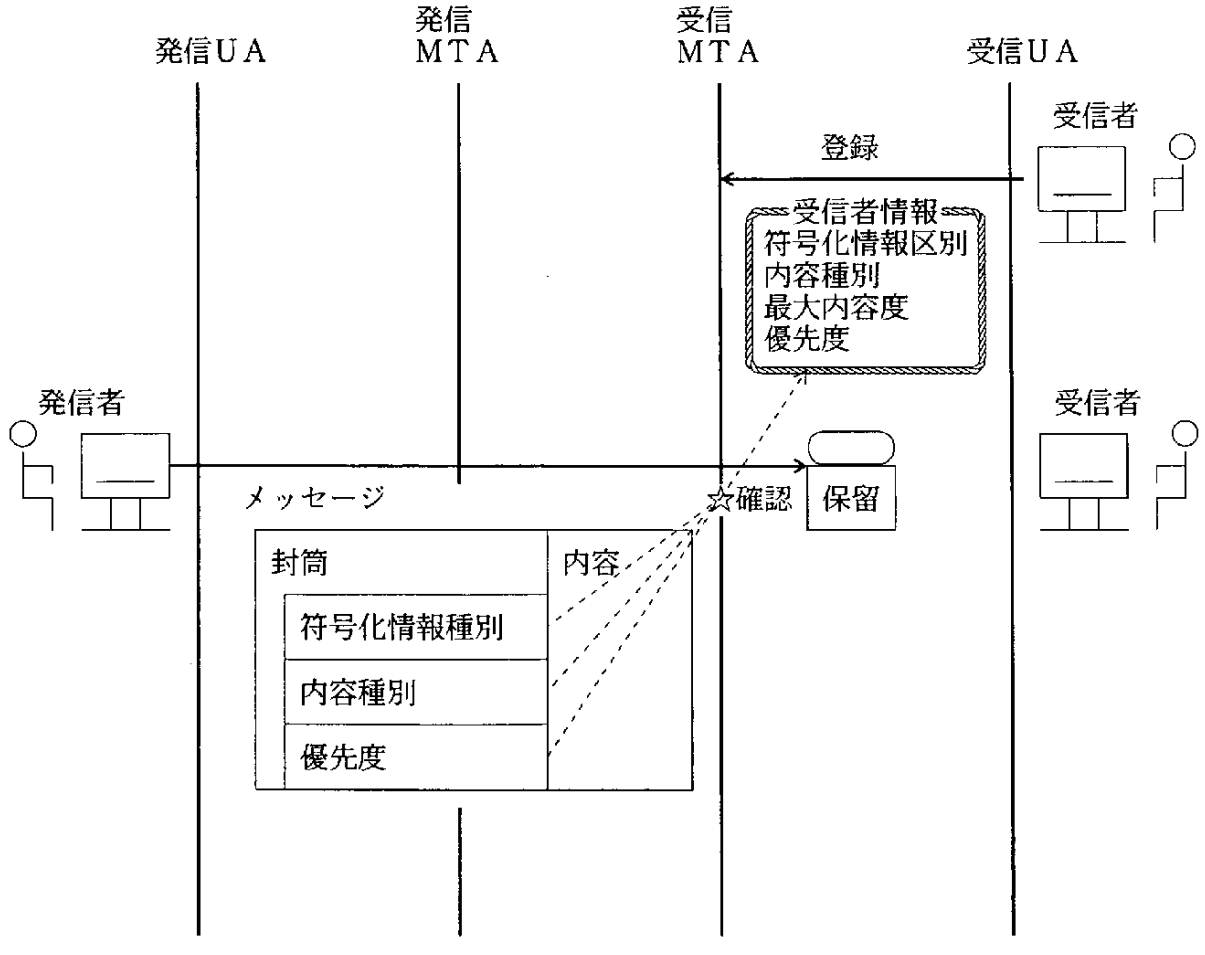


図2.3- 5　配信保留

2. 3. 5　打 診

発信者はメッセージを目的とする受信者に配信することが可能かどうかをＭＴＳに対して、打診することができる。

打診メッセージは通常のメッセージの封筒部分だけで構成され、打診要求を受けたＭＴＡは封筒に含まれる受信者および符号化情報種別、または内容長等から受信者へのメッセージの配信が可能かどうかを調べ、その結果を発信者に対して配信通知もしくは配信不能通知で返送する。

ここでいう「内容長」には、発信者が後に送信しようとするメッセージのサイズが設定される。

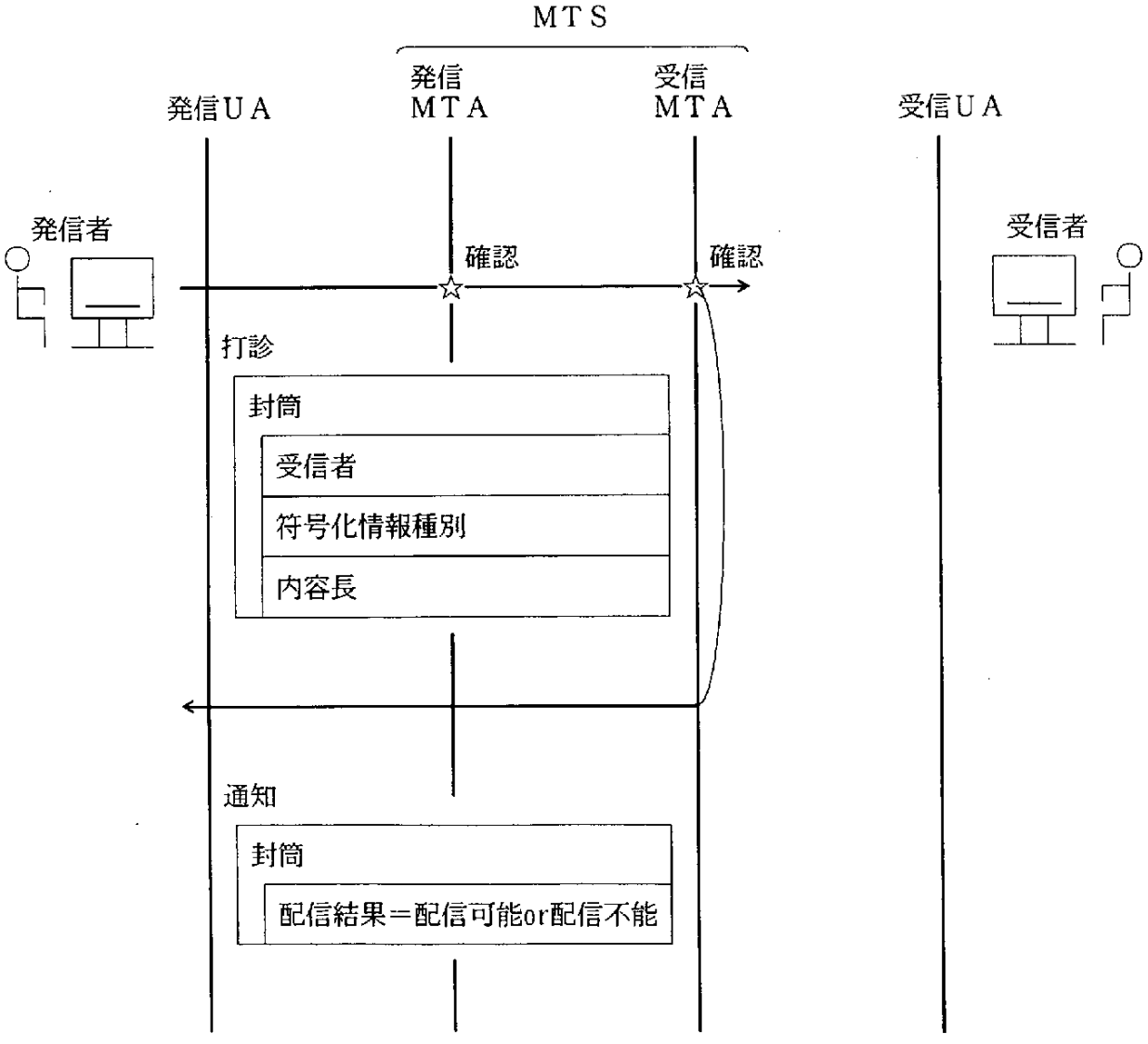


図2.3- 6　打診

2. 3. 6　要求配信方法

発信者は、メッセージの発信の際、受信者毎にメッセージの配信方法を要求することができる。

配信方法には「ＭＨＳ配信」「物理配達」「テレックス配信」「Ｇ３ファクシミリ配信」「Ｇ４ファクシミリ配信」「ＩＡ５端末配信」「ビデオテックス配信」「電話配信」「任意の配信」がある。以下に概要を示す。

- 「ＭＨＳ配信」……通常のＭＨＳユーザ（ＵＡ）への配信
- 「物理配達」……郵便サービスのような物理的配達システムを介した配信
- 「テレックス配信」……テレックス端末への配信
- 「Ｇ３ファクシミリ配信」…Ｇ３ファクシミリ端末への配信
- 「Ｇ４ファクシミリ配信」…Ｇ４ファクシミリ端末への配信
- 「ＩＡ５端末配信」……ＩＡ５テキスト端末への配信
- 「ビデオテックス配信」……ビデオテックス端末への配信
- 「電話配信」……電話への配信
- 「任意の配信」……上記いずれかの方法による配信

受信ＭＴＡは各受信者に指定された配信方法に従って、メッセージの配信を行う。配信に際しては必要に応じてメディア変換が行われる。受信ＭＴＡは、要求された配信方法で配信できない場合や、メディア変換に失敗した場合、発信ＵＡに配信不能通知を返す。

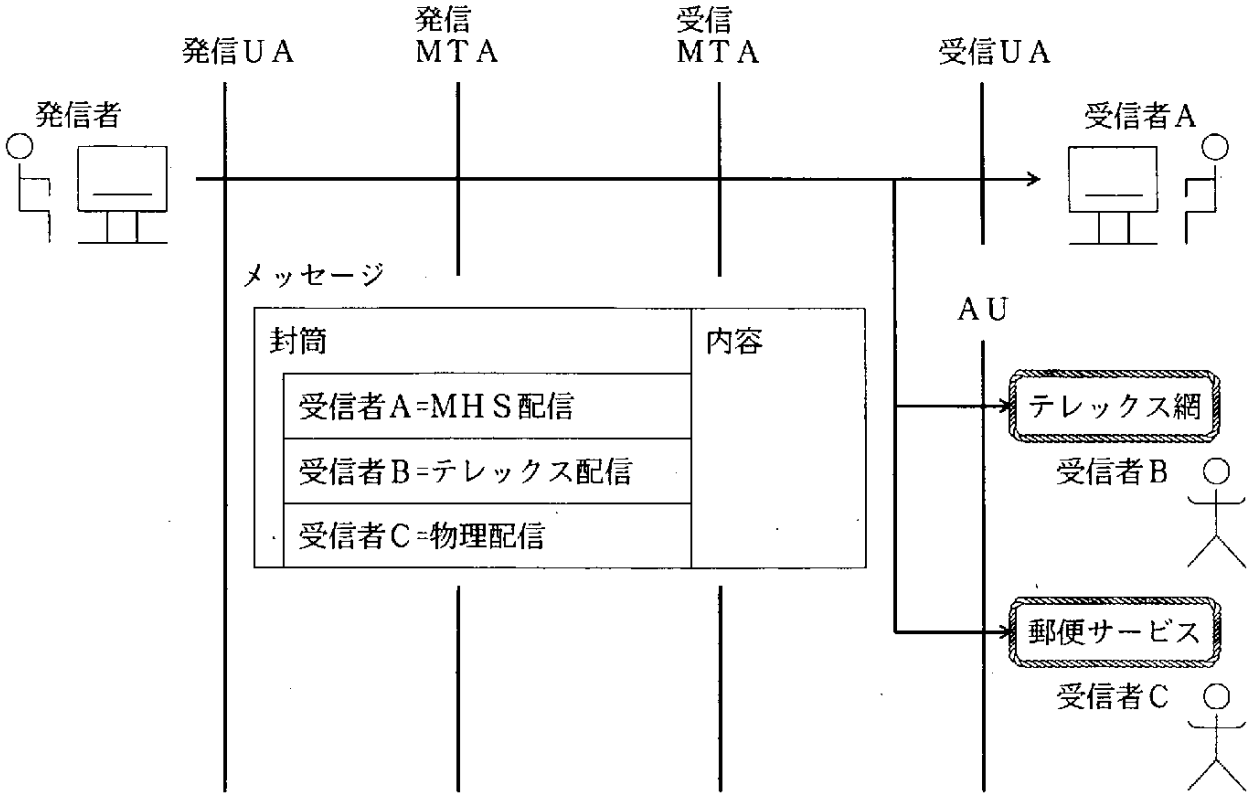


図2.3- 7　要求配信方法

2. 3. 7　制限配信

受信者は受信ＭＴＡに対して、ある特定の発信者からのメッセージの受信を制限するよう要求することができる。

要求の方法には以下の２つがある。

１）受信を制限する発信者を指定する。他の発信者からの受信は受け入れる。

２）受信を許可する発信者を指定する。他の発信者からの受信は受け入れない。

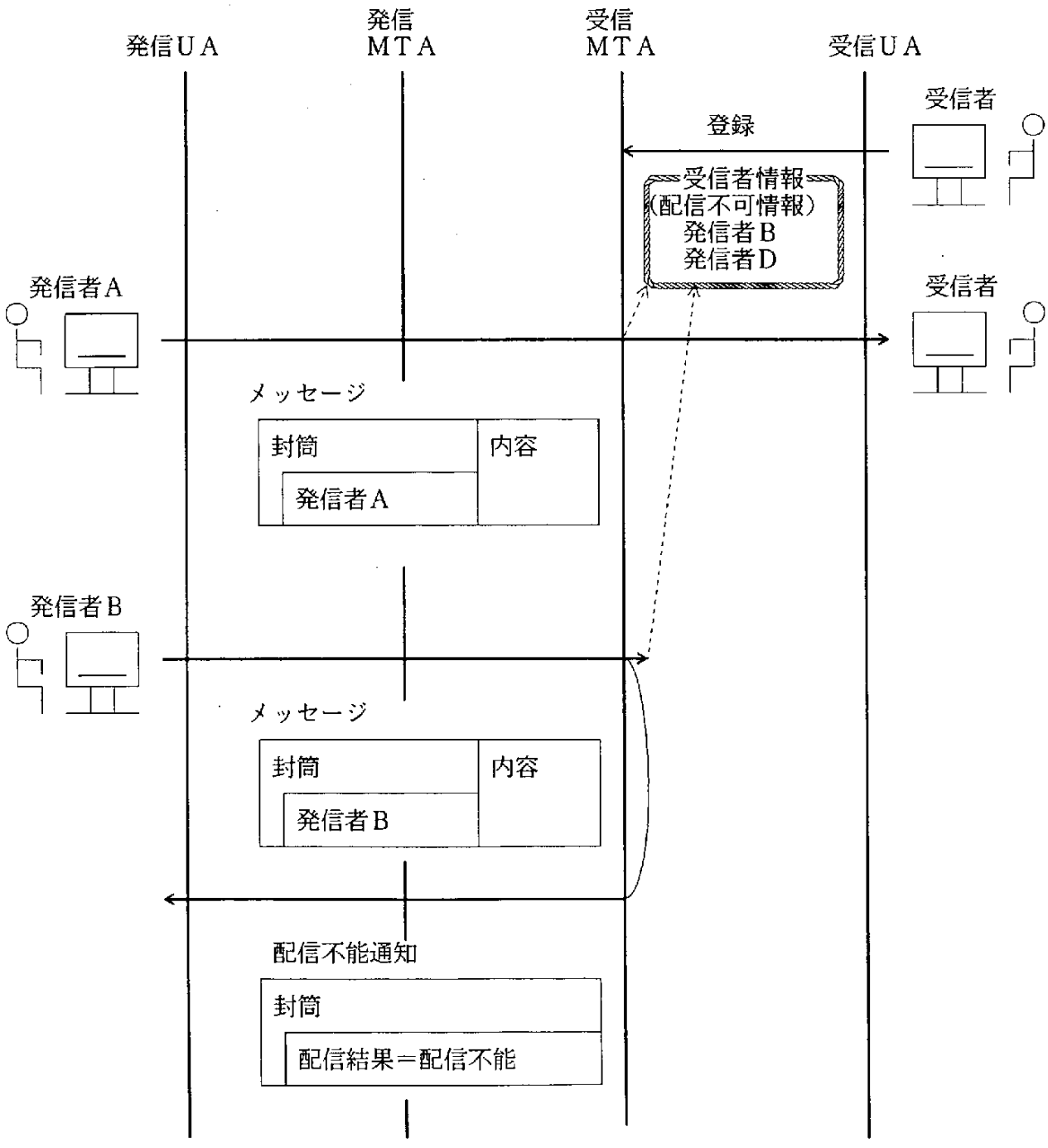


図2. 3- 8　制限配信

2. 3. 8　配信期限指定

発信ＵＡは、メッセージが配信されるべき日時期限を指定できる。

各ＭＴＡ（図の例では受信ＭＴＡ）は、配信期限までにメッセージを配信できない時に、配信不能通知を返送する。

（同報の場合には、全ての受信者に配信する前に配信期限が切れることもある。しかし、既に配信されているメッセージについては、無効とならない。）

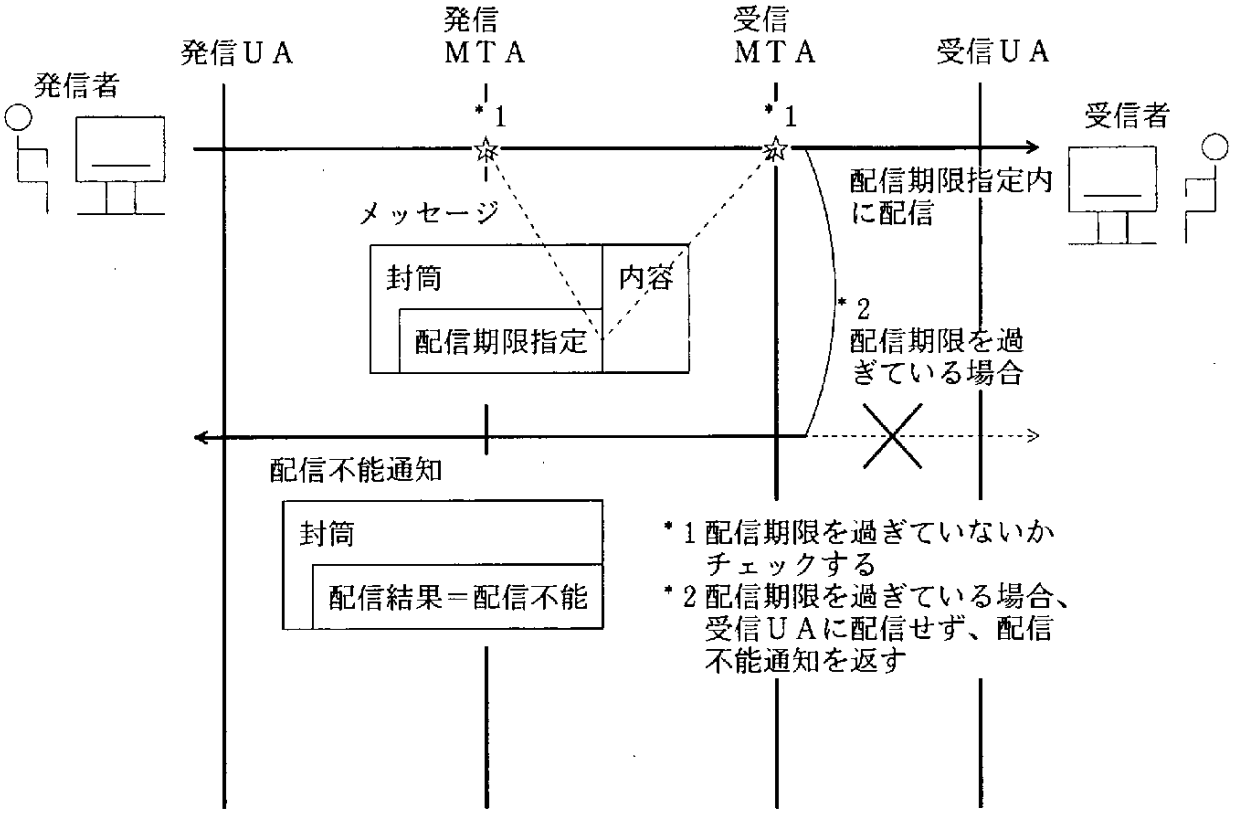


図2.3- 9　配信期限指定

2. 4 配信通知機能

2. 4. 1 配信通知

発信ＵＡは、発信メッセージが正常に受信ＵＡに配信された時に明示的な通知を返送するように要求できる。本通知は、報告対象発信識別子に示されるメッセージ識別子により配信通知と対応づけられる。

同報の場合には、発信ＵＡは本サービスを受信者ごとに要求することができる。

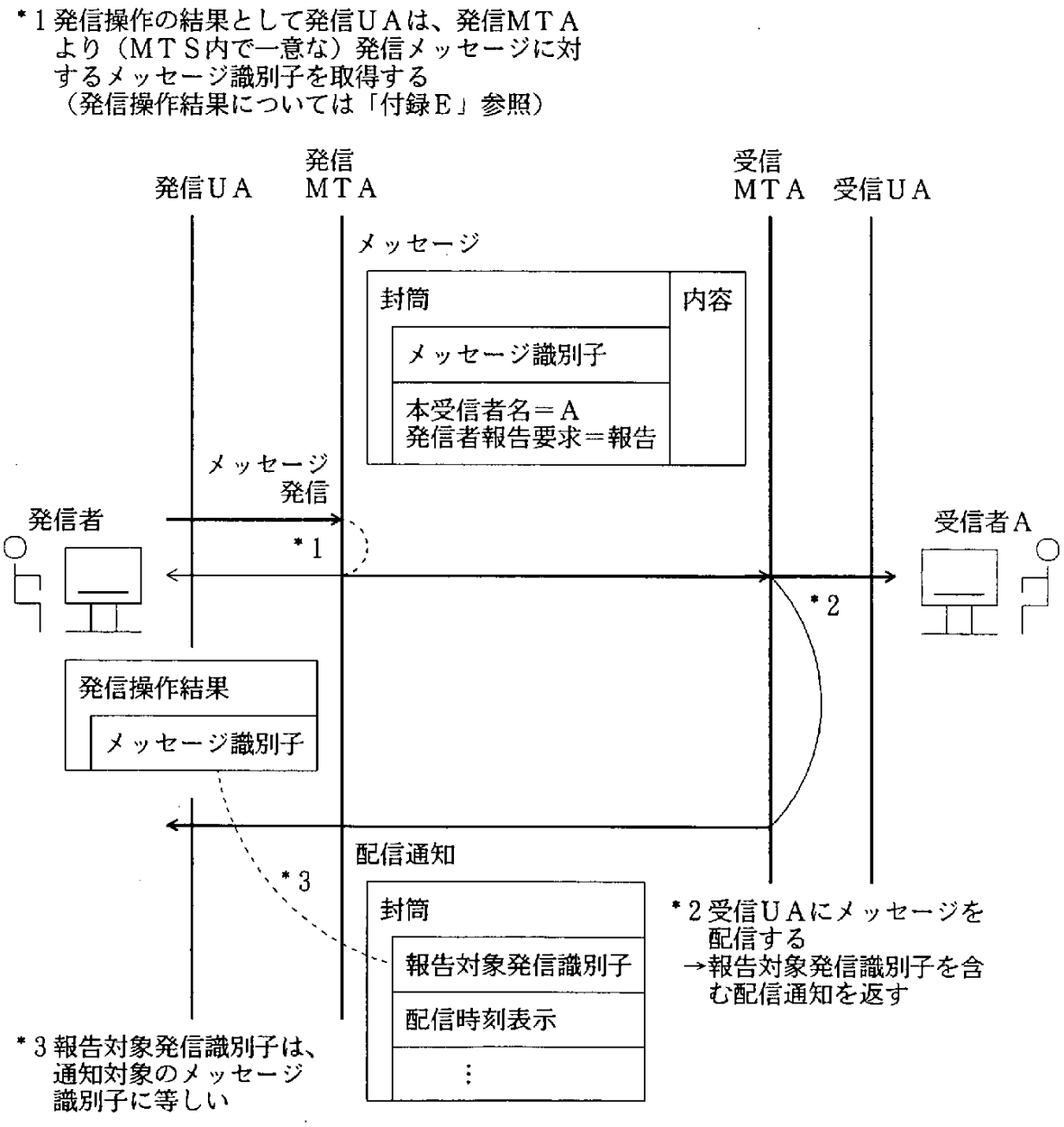


図2.4-1 配信通知

2. 4. 2　配信不能通知

発信したメッセージが目的の受信ＵＡに配信されなかった場合、ＭＴＡはその旨を発信ＵＡに通知する。メッセージが配信されなかった理由は通知の一部として含まれる（例として、“受信ＵＡを識別できない”、等がある。）。

同報の場合、配信不能通知は、当該メッセージが配信されなかった（いずれかの、または複数の）受信ＵＡ毎に行われるか、またはメッセージが配信できなかった全ての受信ＵＡに対して一括して行われる。

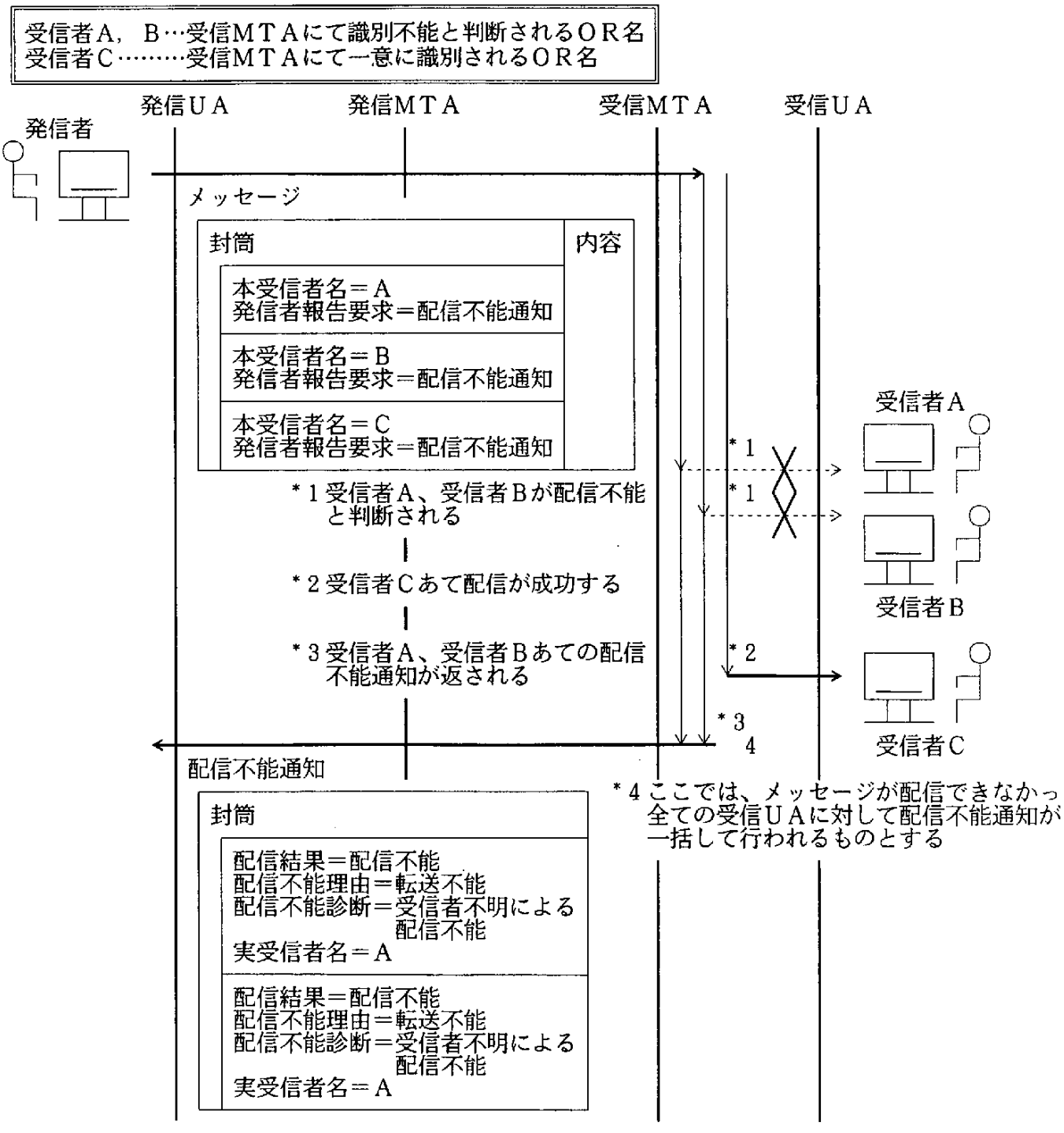


図2.4- 2　配信不能通知

2. 4. 3　配信不能通知の抑止

発信ＵＡは、発信したメッセージが配信不能と判断された場合でも、発信ＵＡに配信不能通知を返送しないことを要求できる。

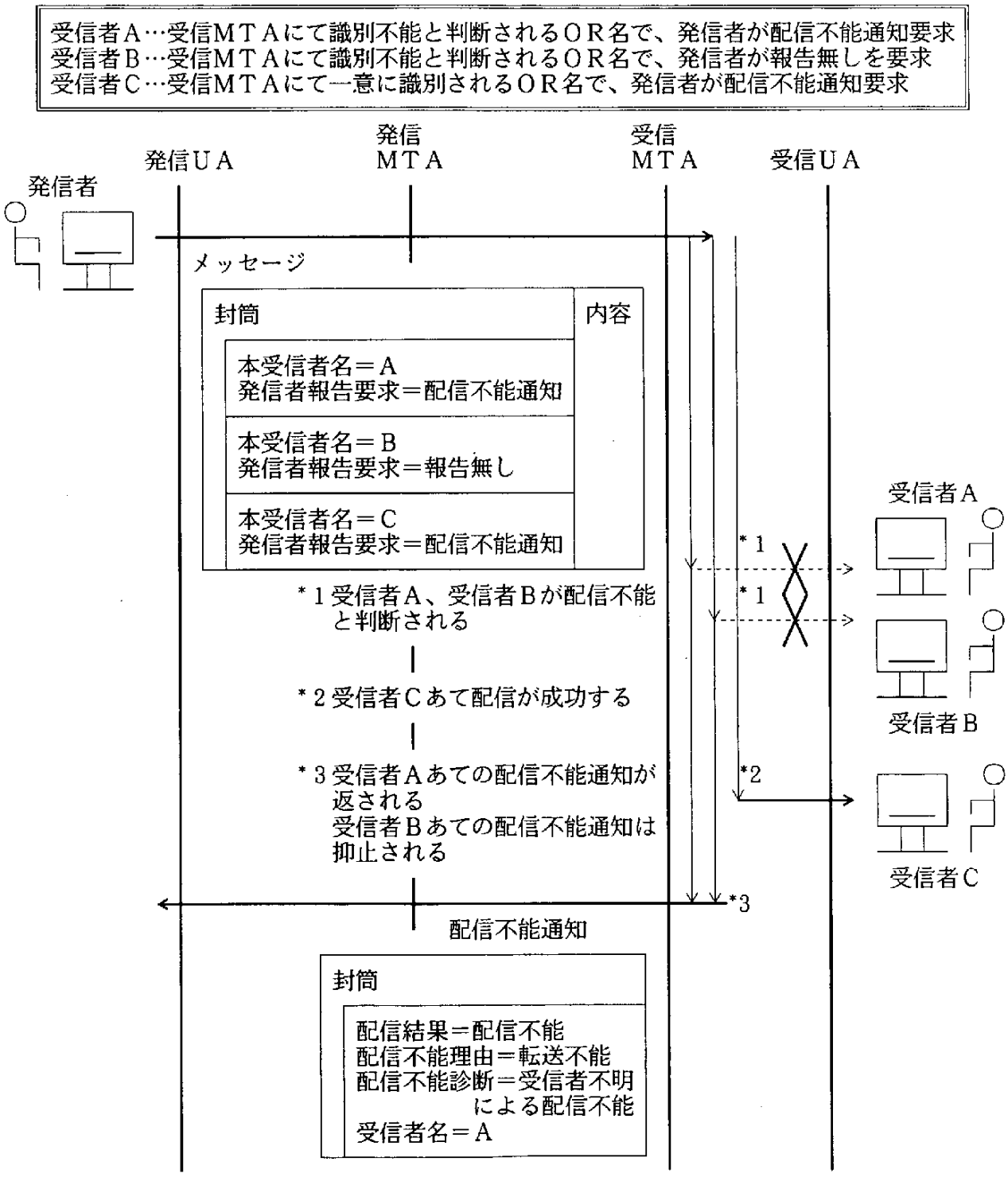


図2.4-３　配信不能通知の抑止

2. 4. 4　内容の返送

発信者は、本来受信者にメッセージが配信できない場合、送信した内容を配信不能通知と共に返送するようＭＴＡに要求することができる。

例えば、受信ＭＴＡにおいてメッセージが受信者に配信できない場合、発信者からこの指定がされていると、配信不能通知を内容と共に発信者に返却する。

ただしメッセージ転送中、内容に対し符号化情報種別の変換がされていた場合は、発信者が変換後の符号化情報種別を処理できない場合があるため、内容の返送はされない。

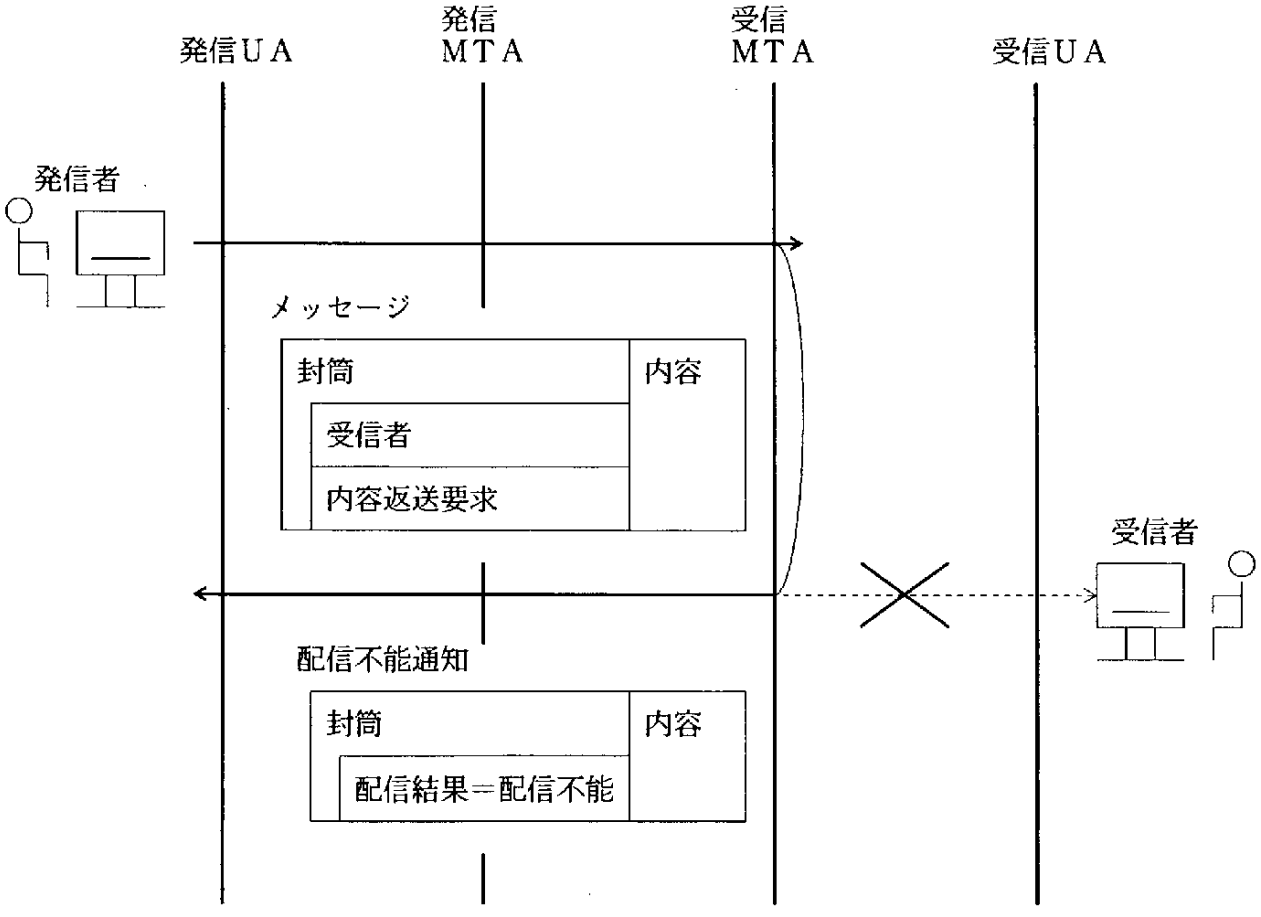


図2.4- 4　内容の返送

2. 5 変換サービス

2. 5. 1 明示変換

明示変換では、発信ＵＡが初めと終わりの符号化情報種別を共に指定することにより変換が行われる。

発信者は、受信者ごとにメッセージの符号化情報種別変換を要求することができる。

符号化情報種別変換には、ISO/IEC標準10021-4(メッセージ通信処理システム－第４部 メッセージ転送システム：抽象サービス定義および手続き）で規定されたものとして

- 「IA5テキストからテレテックスへの変換」
- 「テレテックスからテレックスへの変換」
- 「IA5テキストからG3ファクシミリへの変換」

等がある。

ＭＴＡは各受信者に指定された変換方式により符号化情報種別変換を行い、メッセージの配信を行う。

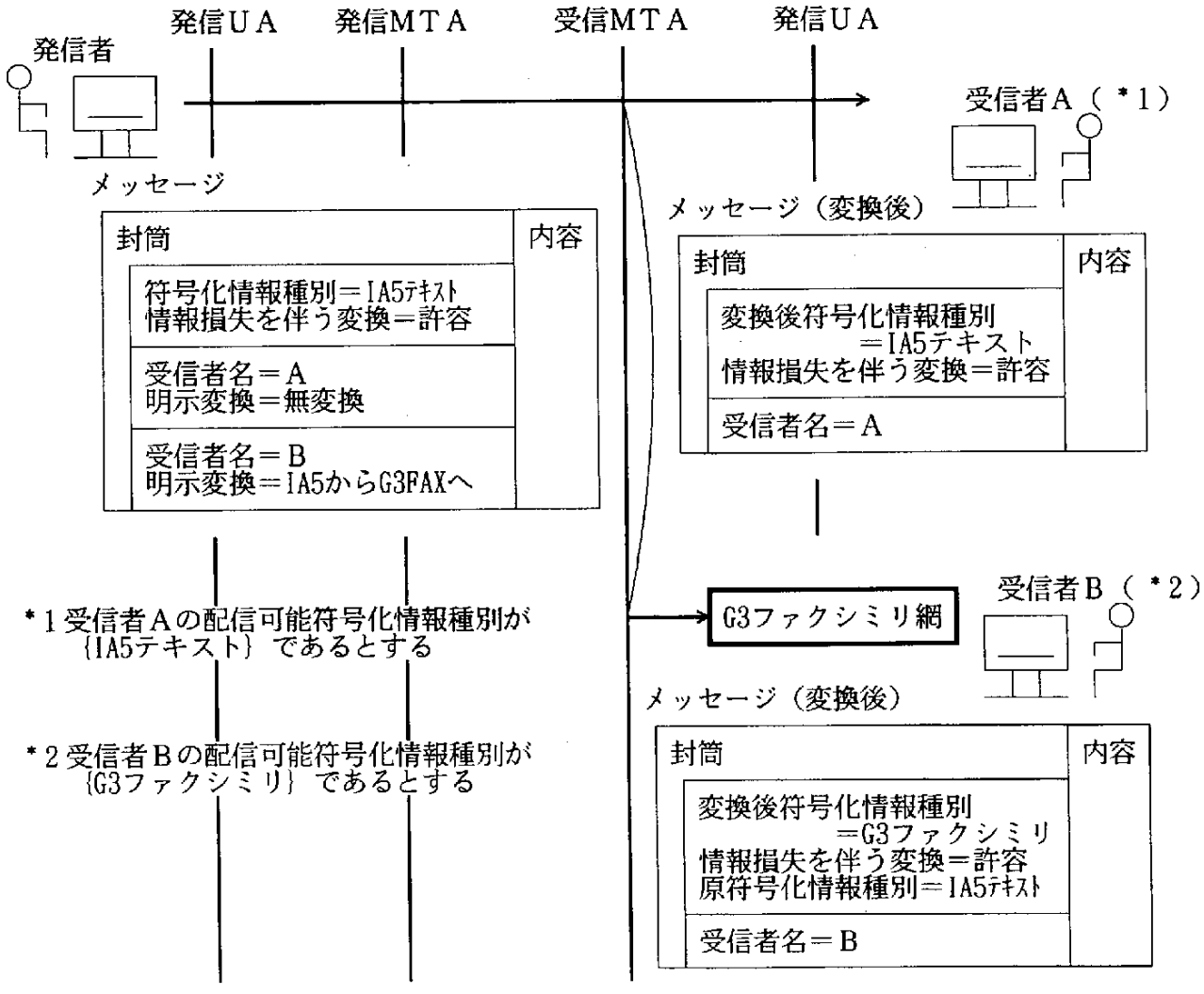


図2.5- 1 明示変換

2. 5. 2　暗黙変換

受信ＵＡは、受信ＵＡあてのメッセージを中継／受信するＭＴＡが、ある期間自動的に、メッセージの配信に先立って必要な全ての変換を行うことを指示できる。

メッセージを中継／受信するＭＴＡは、必要があれば符号化情報種別の変換を行い、その後にメッセージを配信する（ＭＴＡにおいて、受信ＵＡが取り扱える符号化情報種別への変換が複数の方法により実行できる場合は、最も適切な方法が採用される。）。

ただし、発信ＵＡは、メッセージ毎に暗黙変換を禁止することができる。発信ＵＡにより暗黙変換禁止が指定されたメッセージに対して、ＭＴＡが暗黙変換の必要を判断した場合は、配信不能通知が返送される。なお、発信ＵＡが暗黙変換を禁止していない場合、省略値として暗黙変換許容が仮定される。

ＭＴＡは受信ＵＡに、原符号化情報種別および変換後符号化情報種別を通知する。

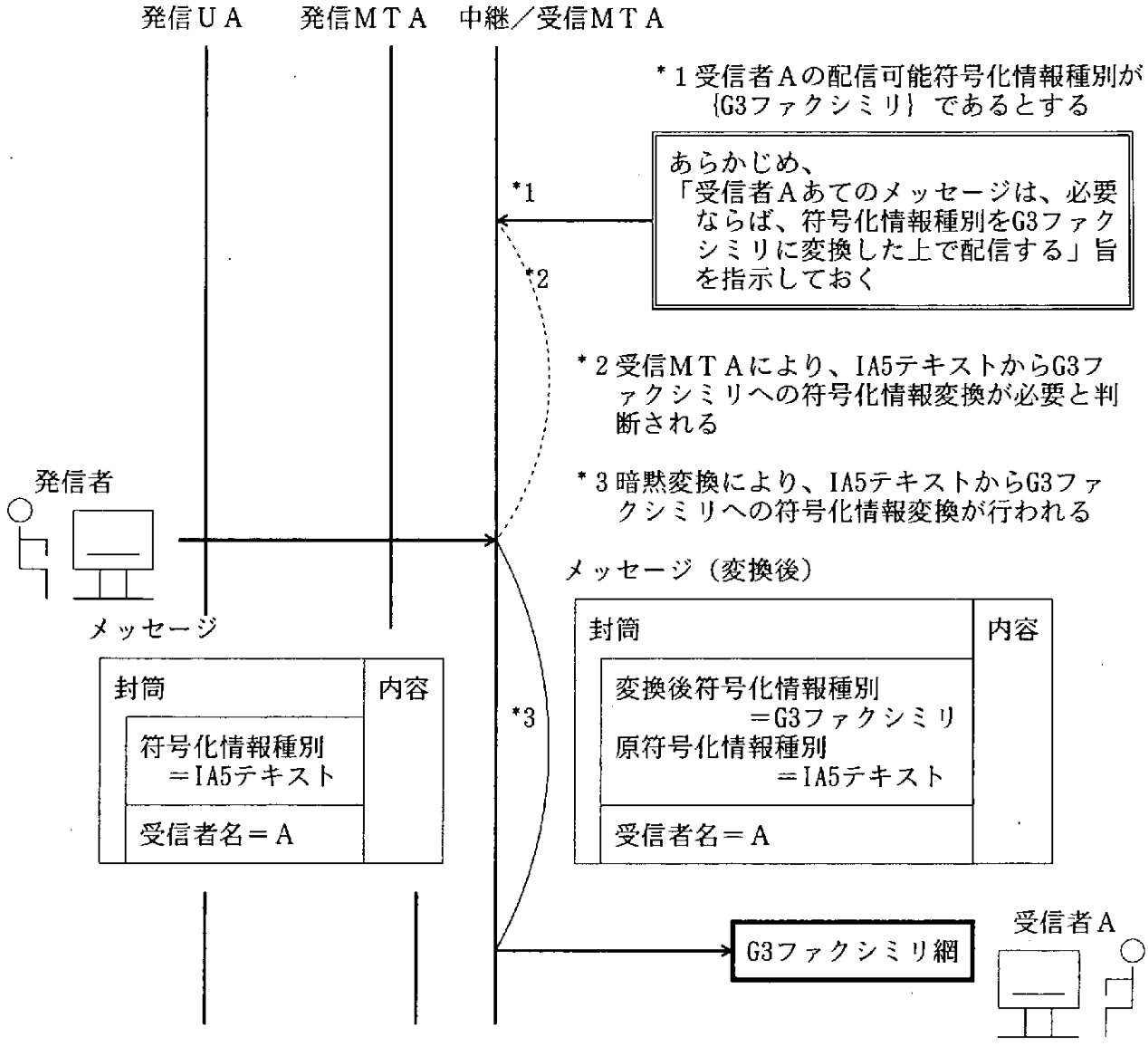


図2.5- 2　暗黙変換

2. 5. 3　変換禁止

発信者は、メッセージの発信に対し、発信するメッセージ毎に符号化情報種別の変換を禁止できる。符号化情報種別の変換禁止により、受信ＵＡへの配信が不能ならば配信不能通知が返送される。

（ＵＡからＭＴＡへの発信操作において、暗黙変換（「2.5.2 暗黙変換」参照）を明示的に禁止し明示変換を無変換と指定する、または、明示変換（「2.5.1 明示変換」参照）を指定しないことによりＭＴＡが省略値として無変換を仮定することにより、変換が禁止される。）

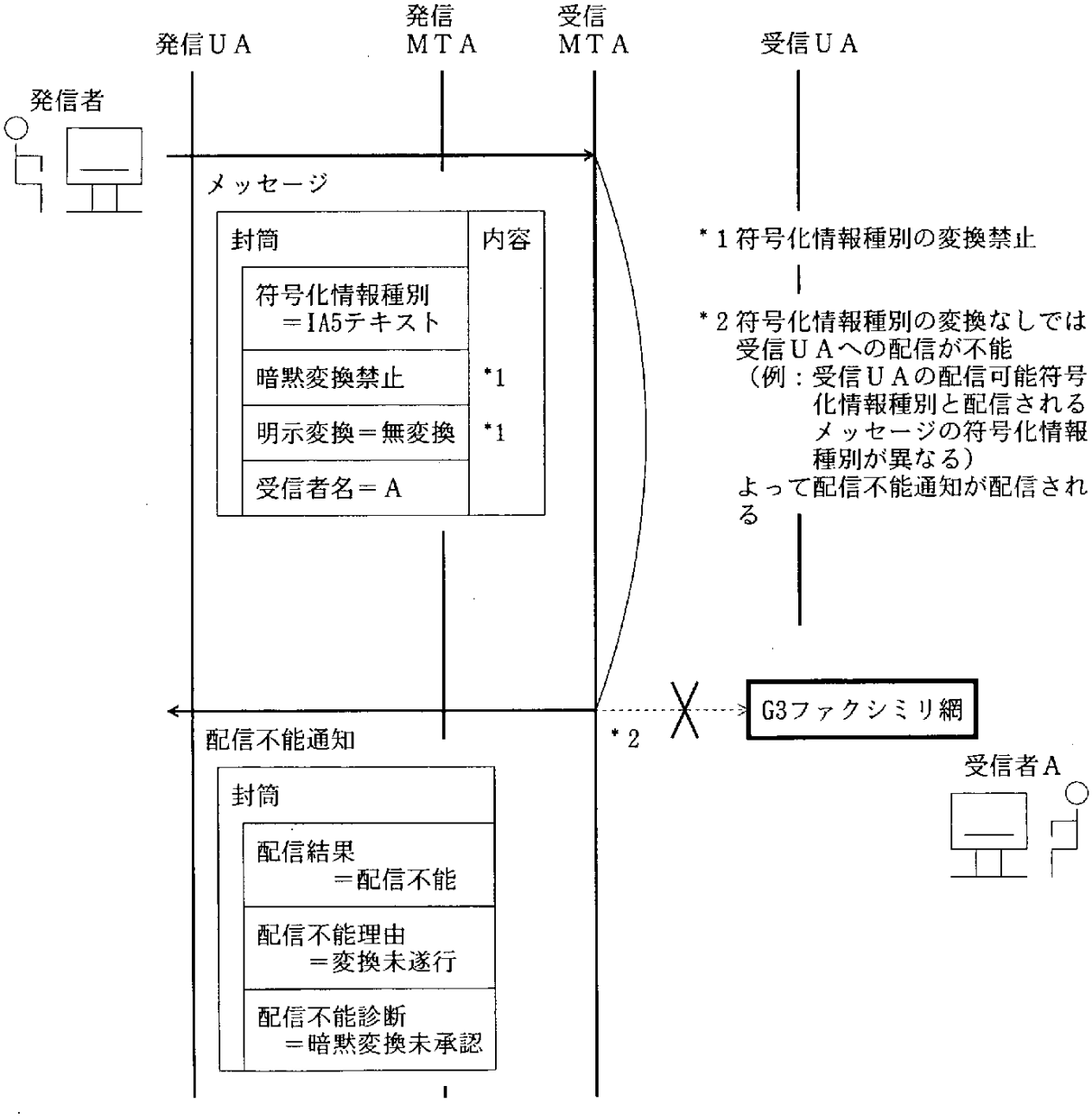


図2.5- 3　変換禁止

2. 5. 4　情報損失を伴う変換禁止

発信ＵＡは、特定の発信メッセージに対して符号化情報種別の変換が情報損失を伴う場合、変換を行ってはならないことを各ＭＴＡに指示できる。なお、発信ＵＡにより情報損失を伴う変換が明示的に禁止されない場合、省略値として情報損失を伴う符号化情報種別の変換が許容されると仮定される。なお、本サービスと変換禁止サービスの両方を指定した場合、後者が適用される。

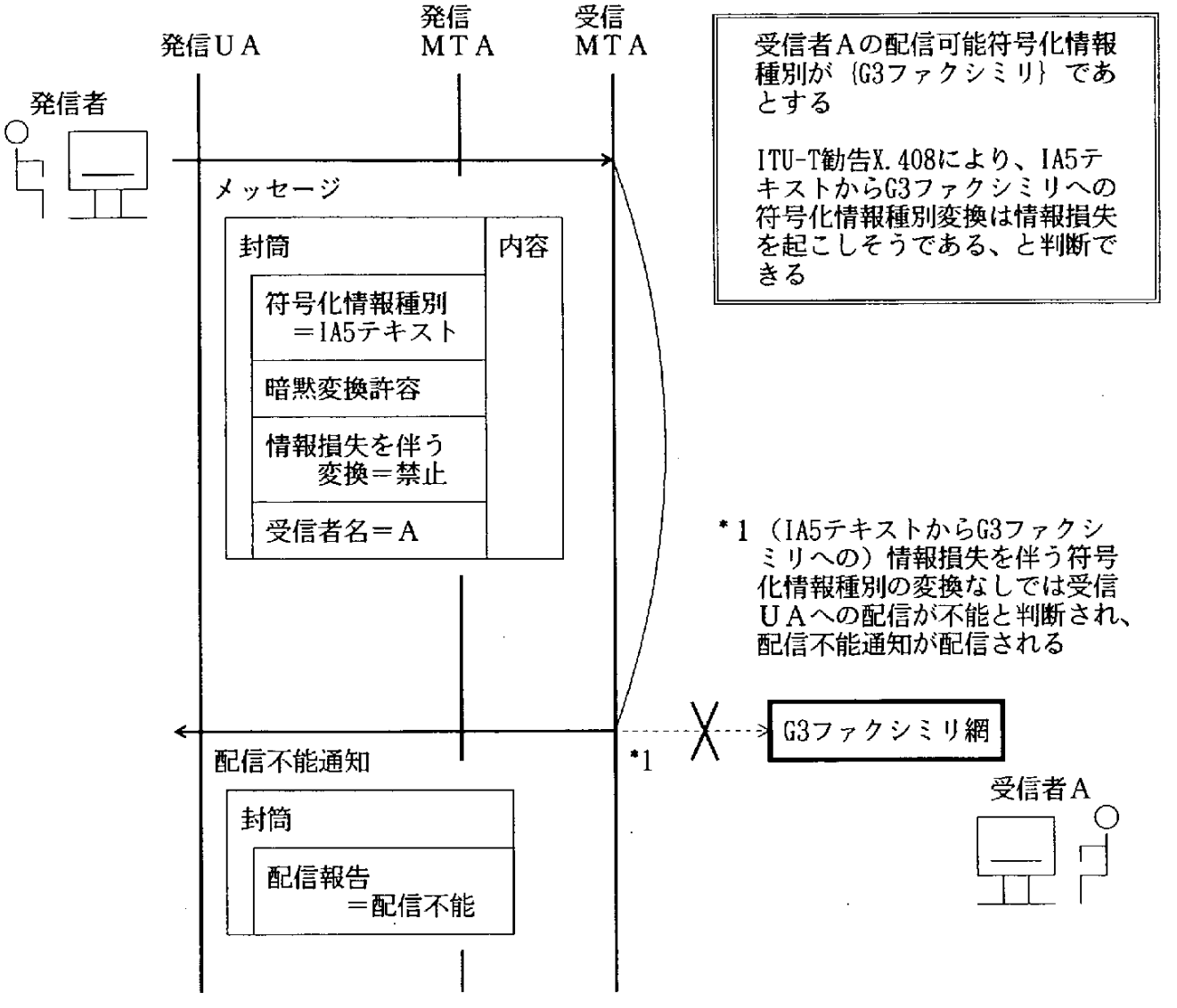


図2.5- 4　情報損失を伴う変換禁止

〈符号化情報種別の変換における情報損失とは〉

ＩＴＵ－Ｔ勧告X.408（メッセージ通信処理システム：符号化情報種別変換規則）において、ＭＨＳにおける一般的な変換が記述されている。そして、その中で

・情報損失なしに可能な符号化情報種別の変換

・可能であるが、情報損失を伴う符号化情報種別の変換

が定義されている。

符号化情報種別の変換における情報損失を定義するにあたり、

・形式面…メッセージの（例えば、紙の上に印字される、等の２次元的な）表現空間における、

Ｘ－方向（文字の大きさおよび文字数、等）および

Ｙ－方向（文字の大きさおよび行数、等）の寸法属性

・符号面…それぞれの符号化情報種別で使用される符号

が考察され、

・書式情報損失…それぞれの符号化情報種別の特性における、行長（文字数）およびページ長（行数）の定義の差異に伴う形式情報損失〈※1〉

・符号情報損失…それぞれの符号化情報種別の特性における、符号の定義の差異に伴う符号情報損失

が「符号化情報種別の変換における情報損失」として定義されている〈※2〉。

※1 書式変換における情報損失の判断は、表2.5- 1のとおり。

表2.5- 1　書式変換における情報損失

状　　況	判　　定
発信者の行長が、受信者の行長より短いか等しい	情報損失無し
発信者の行長が、受信者の行長より長い	情報損失
発信者のページ長が、受信者のページ長より短いか等しい	情報損失無し ただし、受信者のページには、発信者のページ毎に空白行を挿入しなければならない
発信者のページ長が、受信者のページ長より長い	もし、発信者のページが整数の受信者ページに変換されるのであれば、情報損失無し

※2 字体・文字の大きさや紙のタイプが変更された場合は、情報損失とは見なされない。
（詳細は、X.408を参照。）

2. 6 配布先表（ＤＬ）

配布先表を利用して、発信者が最終的な受信者を個別に指定することなく、配布先表（ＤＬ：Distribution List）として識別されるグループの名前によって一群の受信者にメッセージを送る機能が、ＭＴサービスを通じて利用者にオプショナルとして提供される。

配布先表の特性を以下に示す。

・ＤＬメンバ……当該ＤＬにあてられたメッセージを受け取る利用者、または、ほかに展開されるＤＬ。
・ＤＬ送信許可……当該ＤＬを使って、ＤＬメンバにメッセージを送ることを許されている利用者、または、ほかに展開されるＤＬ。
・ＤＬ展開点……ＤＬには、特定のＭＴＡで展開されるものがある。このような地点をＤＬ展開点と呼び、そのあて先はＯ／Ｒアドレスにより指定される。受信者としてＤＬが含まれるメッセージが発信されると、ＤＬ展開点のＯ／Ｒアドレスにより指定された（領域または）ＭＴＡに送られ、展開される。
・ＤＬ所有者……ＤＬの管理に責任を負う利用者。

第１章で示した図1.1- 9のように、ＤＬのメンバはほかのＤＬのメンバであってもよい。この場合、メッセージは親ＤＬの展開点から子ＤＬの展開点まで転送される。

あるＤＬが自分自身のメンバである場合、メッセージは同じＤＬに戻るため、無限に転送される可能性がある。これはＭＴＡによって検知され、再帰が抑止される。

配信通知および配信不能通知は、ＤＬ展開点で生成されることもあれば、受信者への配信時に生成されることもある。

ＤＬ展開によりＤＬメンバへ送られたメッセージに対する通知は、メッセージ送信元のＤＬに返送される。返送された当該通知はそのＤＬの所有者の設定した方針によって、ＤＬの所有者、またはメッセージの発信者、または双方に対して転送される。（図2.6- 1参照）

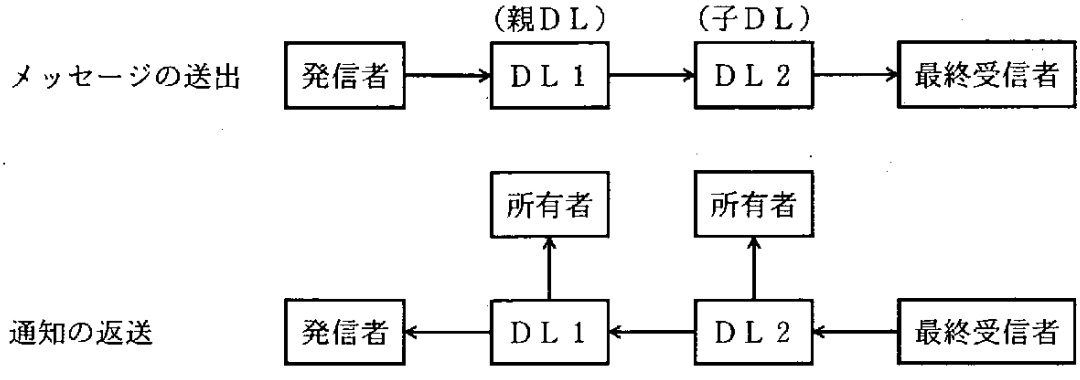


図2.6- 1　配布先表への通知

2. 6. 1　配布先表の使用

配布先表（ＤＬ）に対するメッセージの送信は、利用者に対するメッセージの送信と同様である。発信者はＤＬのＯ／Ｒ名にディレクトリ名、Ｏ／Ｒアドレス、またはその両方を含めても良い。発信者は使用されているＯ／Ｒ名がＤＬの名前であることを意識する必要はない。しかし、発信者は、ＤＬ展開禁止（「2.6.3 」参照）を使うことによって、知らないうちにＤＬに割当てられたメッセージがＭＴＡにより展開されることを禁止してもよい。

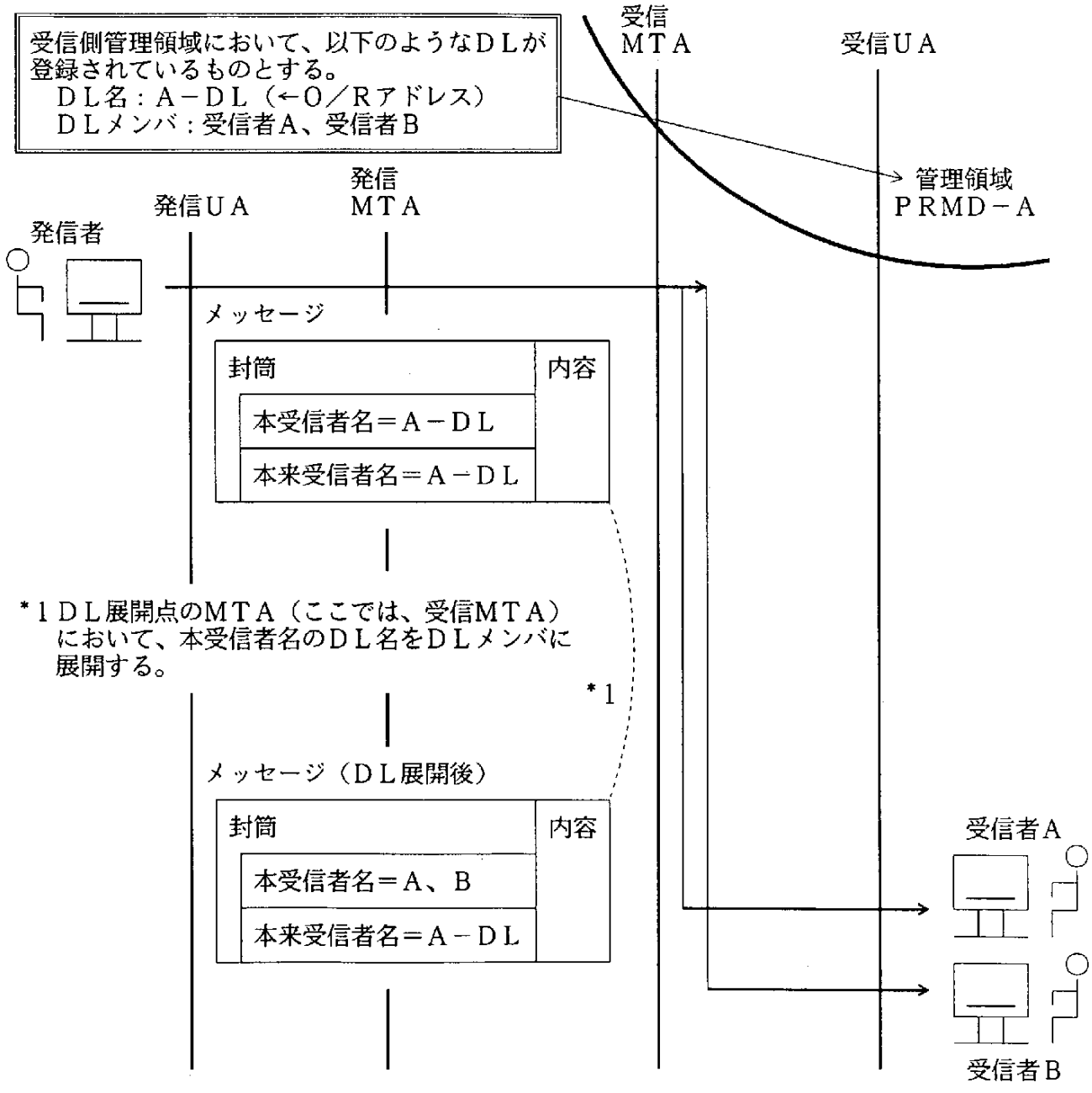


図2.6- 2　配布先表の使用

2. 6. 2　ＤＬ展開履歴表示

メッセージの配信において、受信者は、自分がＤＬメンバとしてメッセージを受け取ったこと、および、どのＤＬまたはその連鎖としてメッセージを受け取ったこと、の情報を得ることができる（本情報をどれだけ受信者に提供するかはローカルな問題である。）。

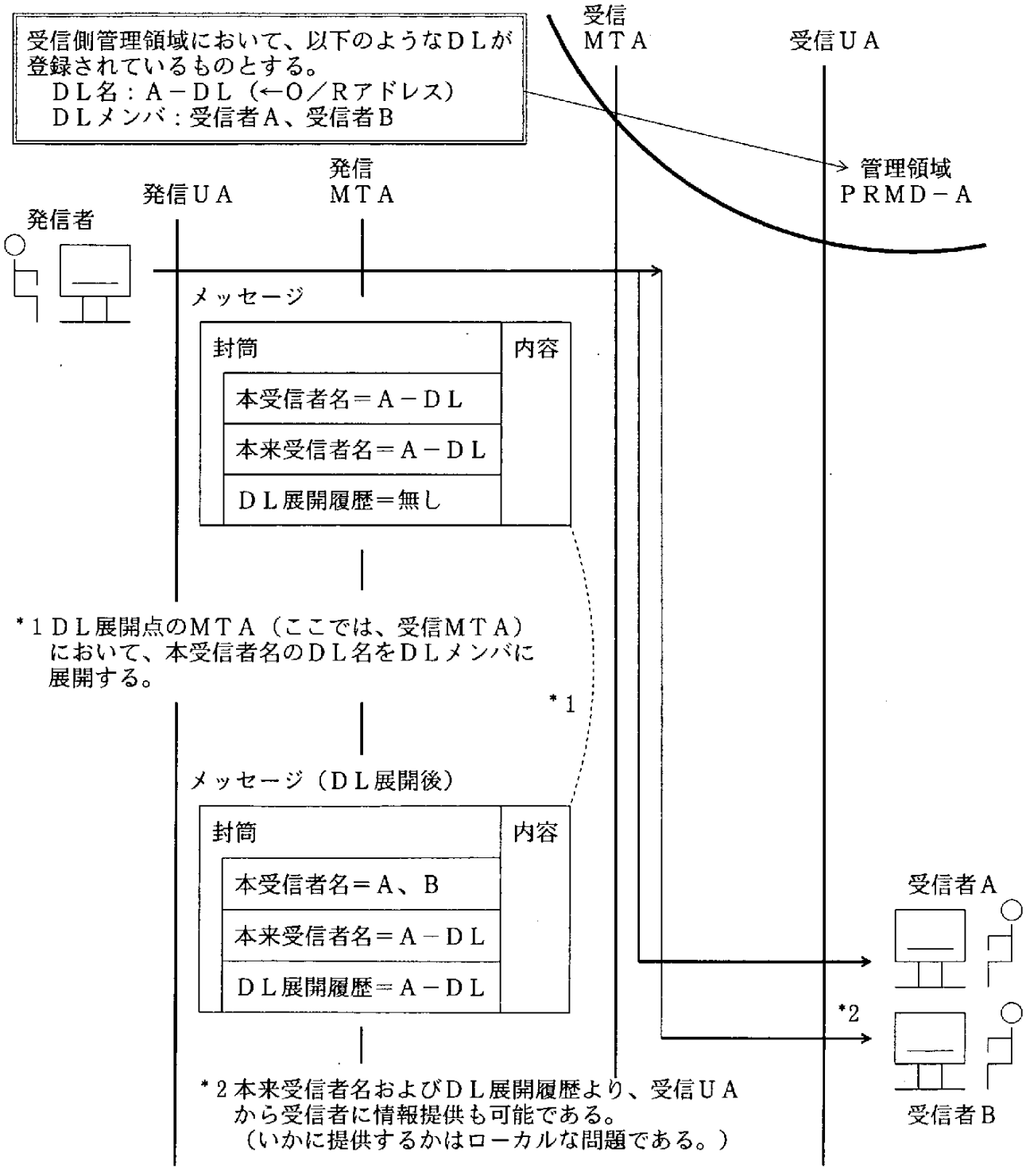


図2.6-３　ＤＬ展開履歴表示

2. 6. 3　ＤＬ展開禁止

メッセージの発信において、発信者は、ＤＬ展開禁止を指定することによって、知らないうちにＤＬに割当てられたメッセージがＭＴＡによって展開されることを禁止しても良い。なお、発信ＵＡからＭＴＡに対して発信される時にＤＬ展開禁止が指定されなければ、省略値としてＤＬ展開許容が仮定される。

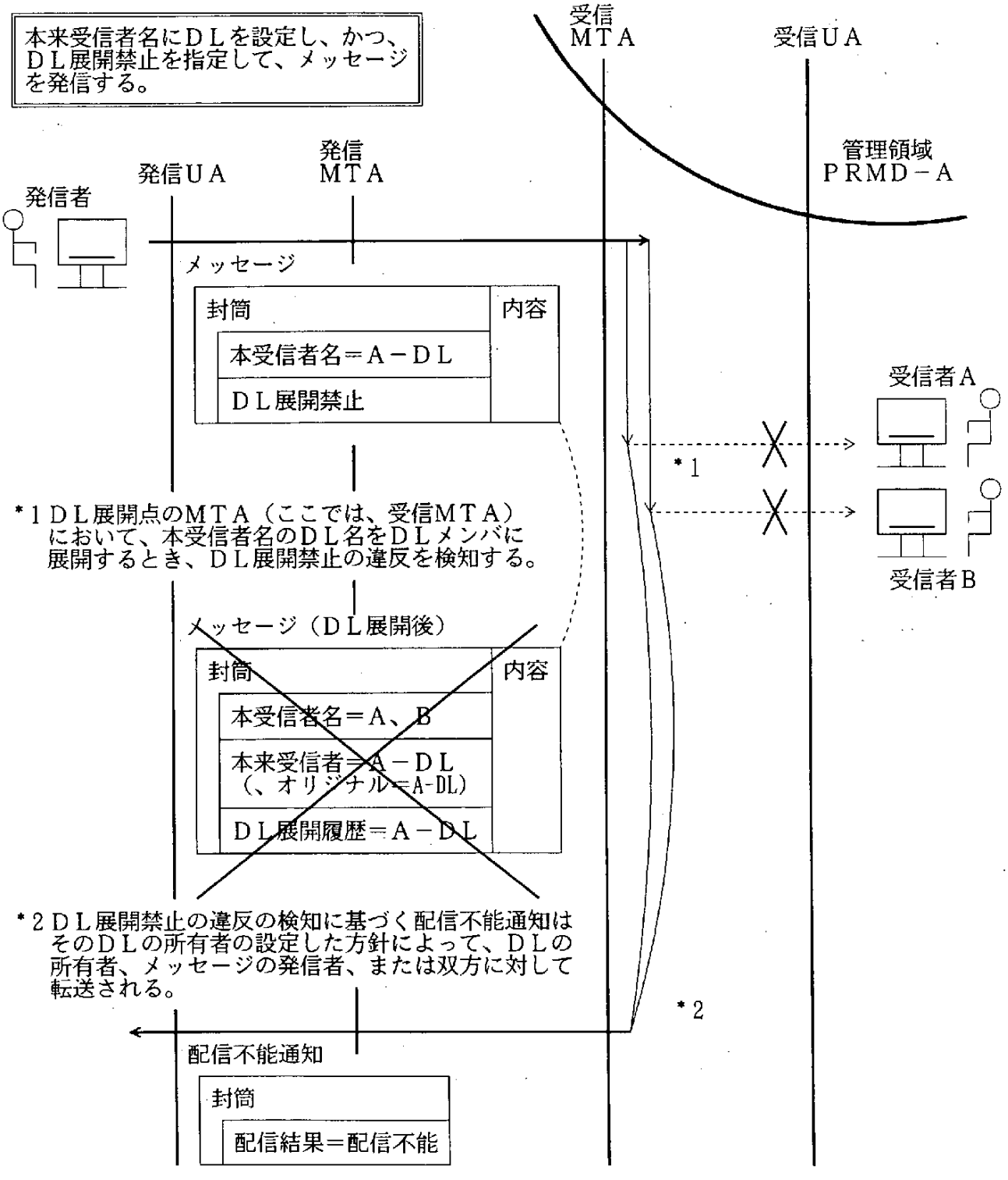


図2.6- 4　ＤＬ展開禁止

2. 7 情報表示機能

2. 7. 1 メッセージ識別

ＭＴＡは、ＵＡによって発信したメッセージや打診に対して、ＭＴＳにおいて一意な識別子を付与する。この識別子によって、ＵＡ、ＭＴＡ（、利用者）は発信したメッセージと配信通知等（「2.4.1」参照）の対応付けを行うことができる。

＊１発信操作の結果として発信ＵＡは、発信ＭＴＡより（ＭＴＳ内で一意な）発信メッセージに対するメッセージ識別子を取得する
（発信操作結果については「付録Ｅ」参照）

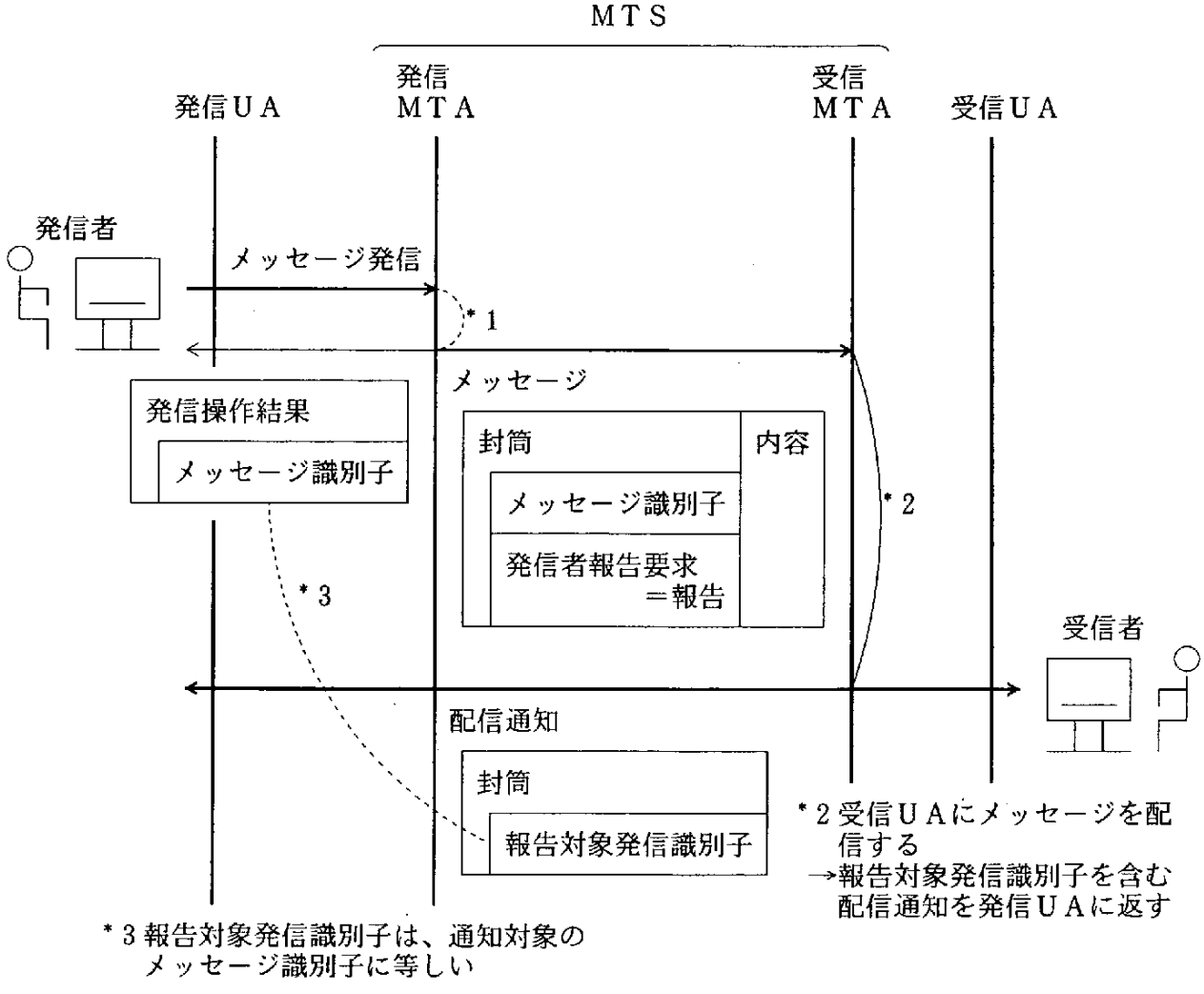


図2.7-1 メッセージ識別～配信通知における使用例

2. 7. 2　内容種別表示

発信ＵＡは、メッセージ発信時に、各発信メッセージの内容種別を付加して発信する。

1988年版ＭＨＳ標準を規定したＩＳＯ規格（ＩＳＯ／ＩＥＣ 10021：1991）で定義されている内容種別として、

・P2 1984

・P2 1988 (P22)

・内部封筒

等があり、X.435によってEDIのために拡張された内容種別として、

・Pedi (P35)

がある。

受信ＭＴＡは、受信ＵＡへの配信時にメッセージの内容種別を評価し、受信ＵＡへの配信が不能ならば配信不能通知を配信する。

＊1 受信者Ａの配信可能内容種別：P2-1984, P2-1988とし、内容種別：Pediは配信不能である、とする。

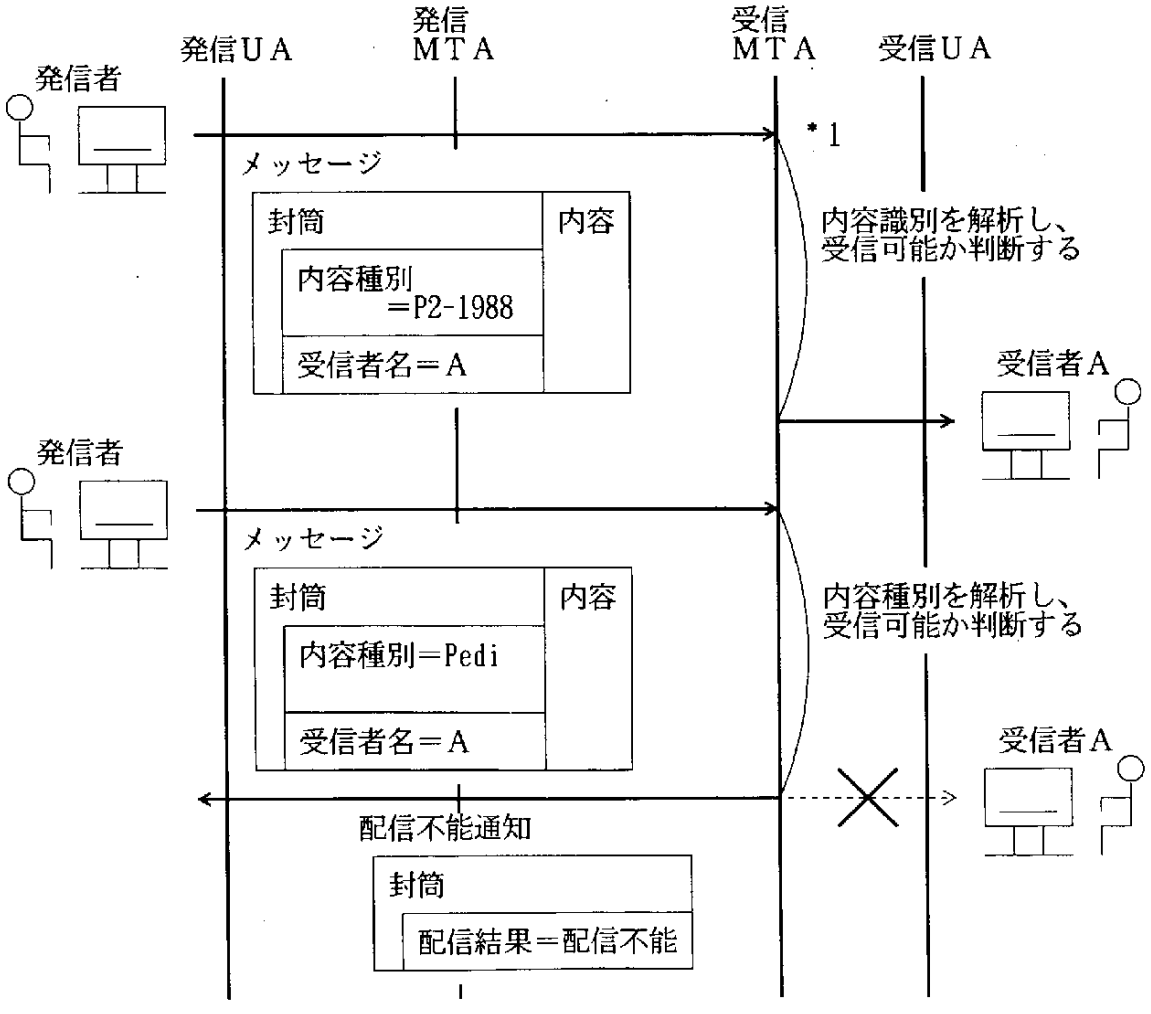


図2.7- 2　内容種別表示

（参考）　内部封筒：インナーエンベロープ

メッセージ流れ安全機密性（「2.9.4 」参照）で使用されるサービスに、二重封筒技法がある。この技法は、送りたいメッセージをさらに外側のメッセージの内容で包みこみ、メッセージを隠ぺいするものである。

この技法が使われる場合、メッセージの内容種別は内部封筒（インナーエンベロープ）という種別となる。これは、外側の封筒の受信者に送信されたメッセージ内容が、内側の封筒の受信者に送られるメッセージ（封筒および内容）であることを意味する。

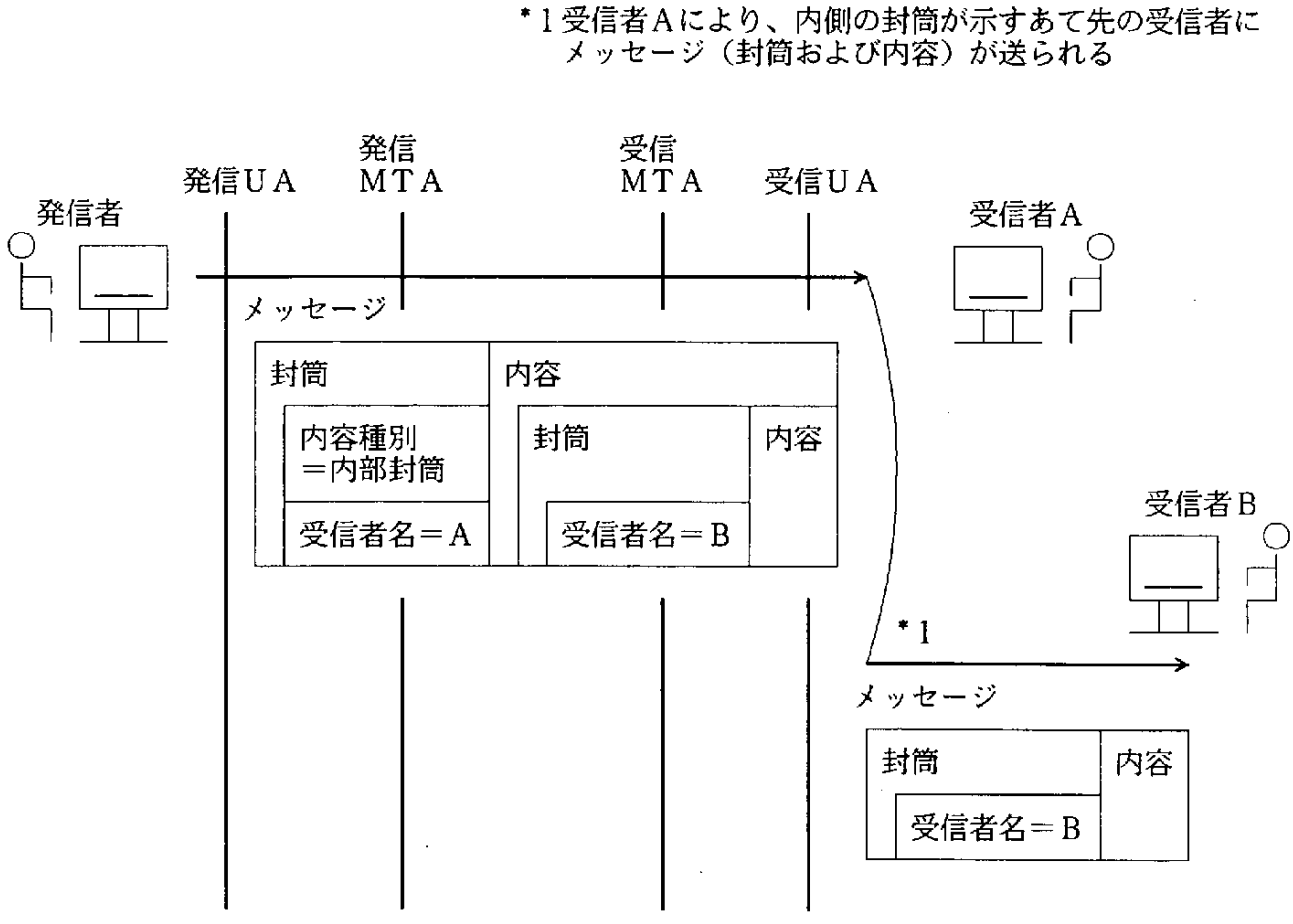


図2.7- 3　内部封筒：インナーエンベロープ

2. 7. 3　発信時刻表示

(1)　ＵＡが受信する場合

各ＭＴＡがこのサービスを提供しているならば、発信ＵＡおよび受信ＵＡは、発信ＵＡが発信ＭＴＡにメッセージを発信した日時を知ることができる。

＊１発信操作の結果として発信ＵＡは、発信ＭＴＡより発信したメッセージの発信時刻を取得する（発信操作結果については「付録Ｅ」参照）

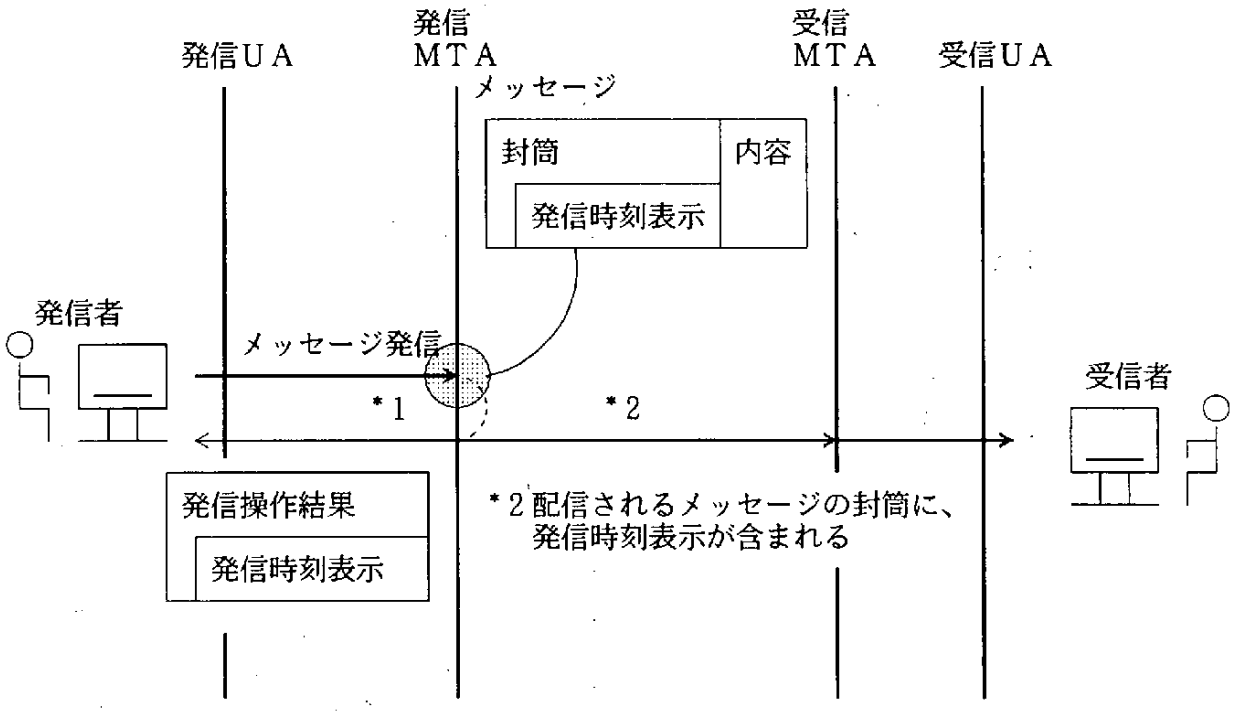


図2.7- 4　発信時刻表示～ＵＡが受信

(2) ＰＤＡＵ経由の場合

物理的配達アクセス単位（ＰＤＡＵ）がこのサービスを提供している場合には、ＰＤＡＵは物理メッセージに、発信ＵＡが発信ＭＴＡにメッセージを発信した日時を表示する。

＊１発信操作の結果として発信ＵＡは、発信ＭＴＡより発信したメッセージの発信時刻を取得する（発信操作結果については「付録Ｅ」参照）

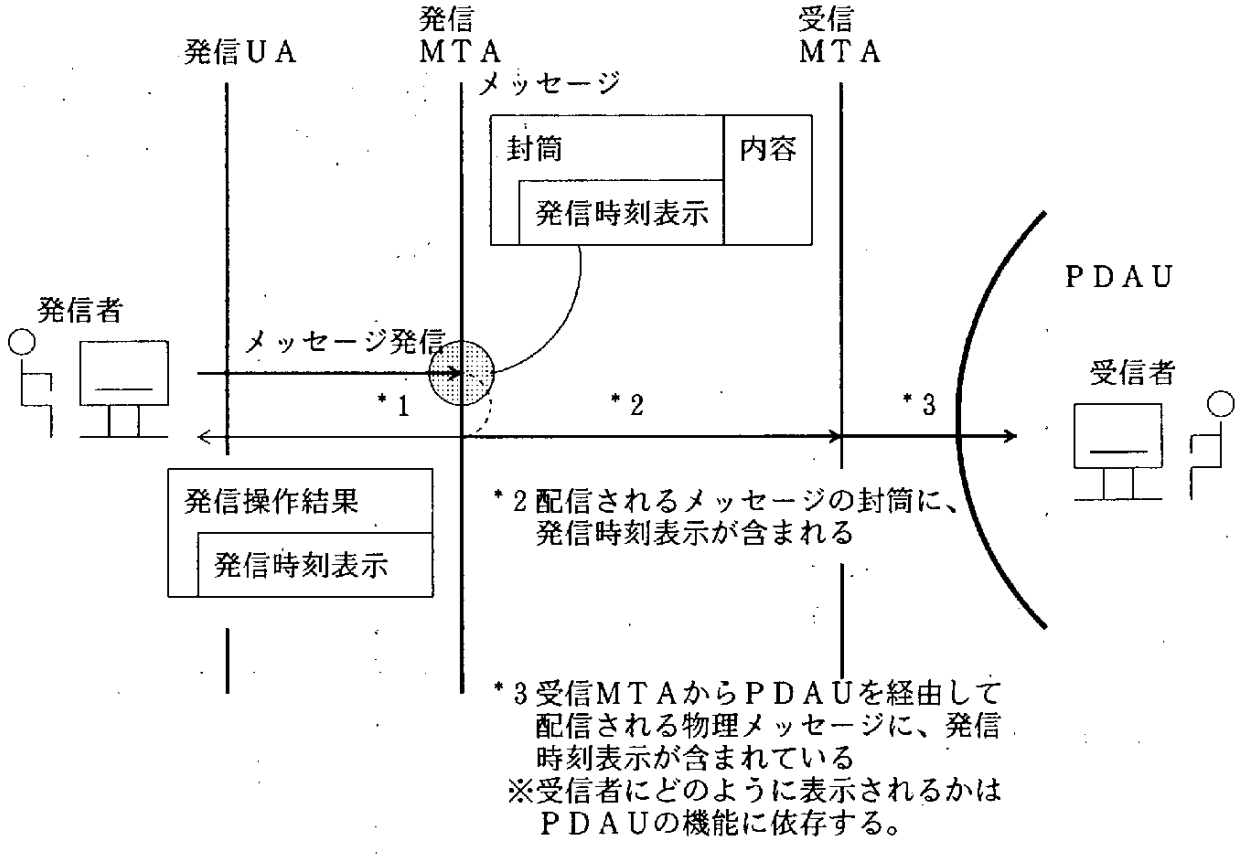


図2.7- 5　発信時刻表示～ＰＤＡＵ経由の受信

2. 7. 4　配信時刻表示

(1)　ＵＡが受信する場合

発信ＵＡは、発信操作時に配信通知（「2.4.1 」参照）を要求することにより、受信ＭＴＡ（またはＭＳ）から受信ＵＡにメッセージが配信された時刻を知ることができる。
受信ＵＡは、受信したメッセージの配信時刻表示からメッセージを配信された時刻を知ることができる。

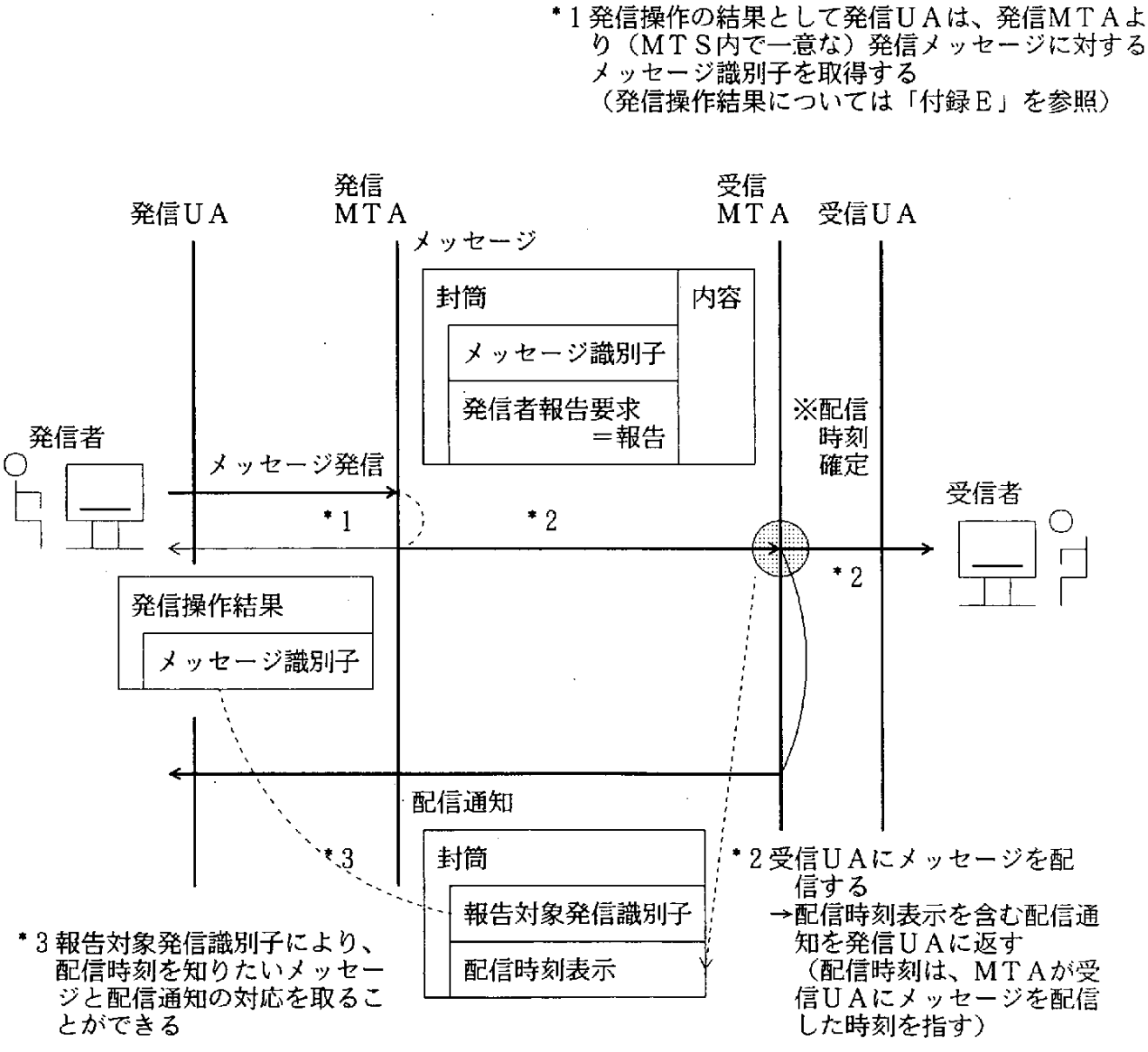


図2.7- 6　配信時刻表示～ＵＡが受信

(2) ＰＤＡＵ経由の場合

物理的配達アクセス単位（ＰＤＡＵ）がこのサービスを提供している場合には、ＰＤＡＵは、配信通知の配信時刻表示に、受信側のＭＴＡからメッセージが配信された時刻を表示する。

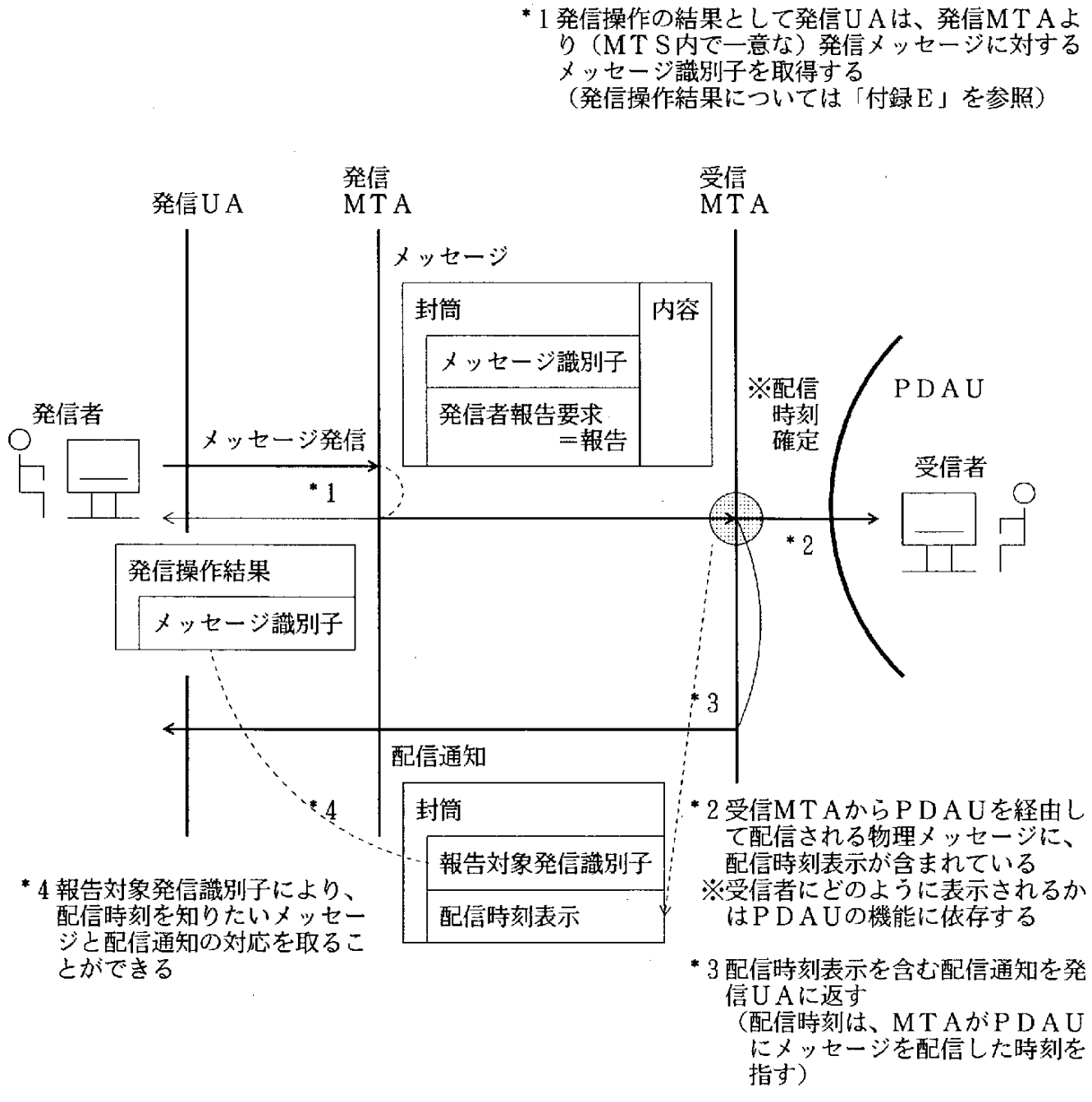


図2.7-7　配信時刻表示～ＰＤＡＵ経由の受信

2. 7. 5　原符号化情報種別表示

ＭＴＡは、さまざまなＵＡ能力を持つ利用者に対応するため、符号化情報種別（※1）で示される符号化方式によるメッセージを、別の符号化情報種別で配信できるような変換機構を提供することができる。このため、発信ＵＡは、メッセージ発信時に、このメッセージの符号化情報種別をＭＴＡへ通知する。

（発信ＭＴＡから中継ＭＴＡを経由して、）受信ＭＴＡから受信ＵＡへメッセージが配信されるまでの間に、様々な要因（※2）により、受信ＵＡに配信されるメッセージの本体の符号化情報種別がＭＴＡにより変換されている場合がある。その場合、ＭＴＡは、受信ＵＡに原符号化情報種別および変換後符号化情報種別を通知する。

※1 符号化情報種別……メッセージの内容を表現する符号化情報の種別を示す識別子。
例として、IA5テキスト、G3ファクシミリなどがある。

※2 様々な要因……以下の例が考えられる。

- 発信ＵＡが、受信ＵＡへメッセージを配信する時に、明示的な変換を指定した場合（「2.5.1 明示変換」参照）
- あらかじめ、受信ＵＡからＭＴＡに対し、受信ＵＡが受信可能な符号化情報種別と、ＭＴＡから受信ＵＡへのメッセージの配信の際必要な変換をＭＴＡが自動的に行うよう登録され、その登録に従って、受信ＵＡへのメッセージの配信の際ＭＴＡが自動的に符号化情報種別の変換を行った場合（「2.5.2 暗黙変換」参照）

2. 7. 6　変換済み表示

ＭＴＡが配信するメッセージの本体の符号化情報種別を変換した場合、受信ＵＡは、変換された旨を、原符号化情報種別と変換後符号化情報種別により、知ることができる。

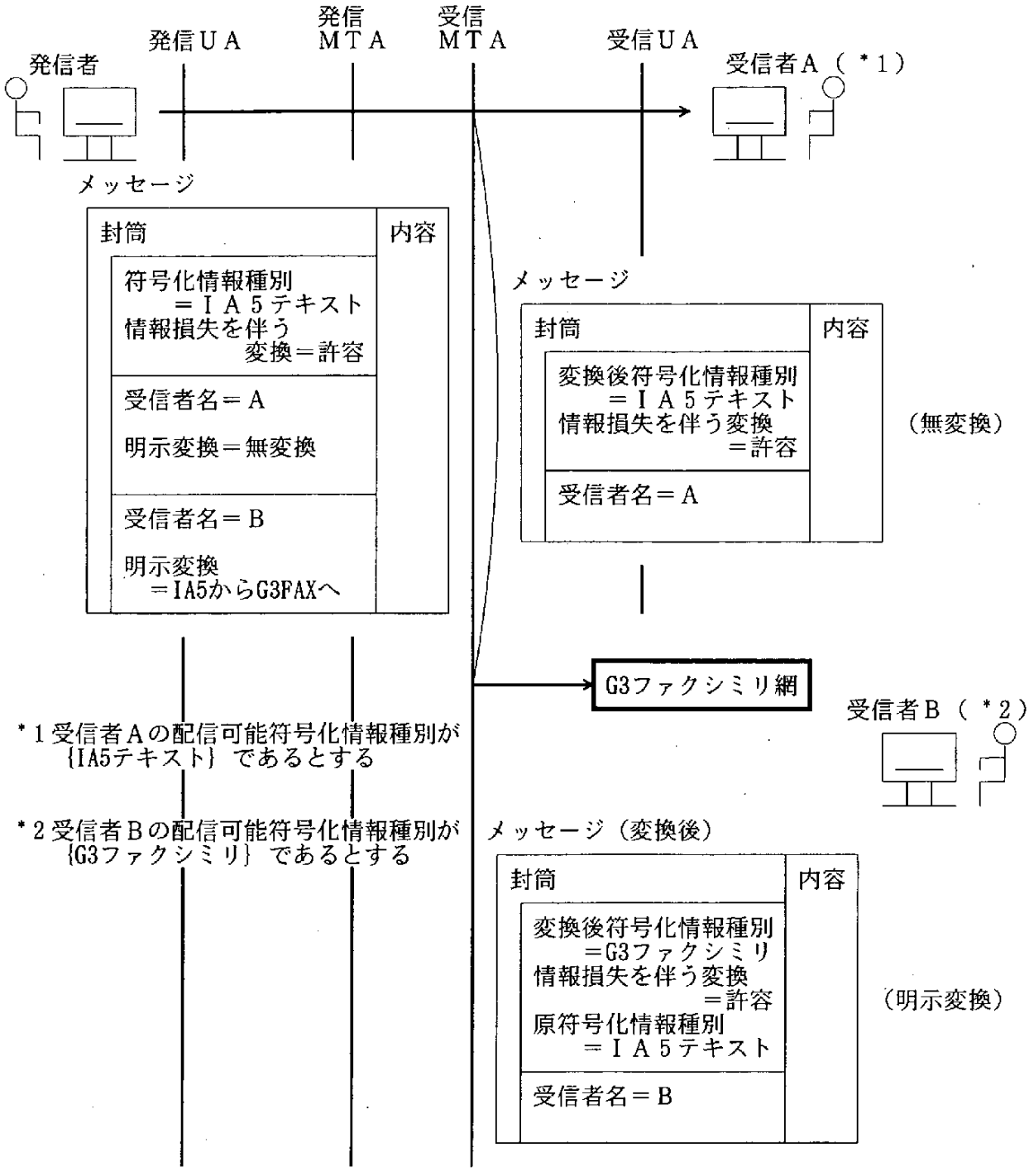


図2.7-8　変換済み表示

2. 7. 7　他受信者名表示

同報を処理する場合、発信ＵＡは、メッセージが配信される時に各受信ＵＡに対して、全てのほかの受信者のＯ／Ｒ名の公開をＭＴＡに指示できる。公開するＯ／Ｒ名は発信ＵＡにより提供される。なお、省略値は、受信者公開禁止が仮定される。

また、配布先表（ＤＬ）展開が行われた場合、発信者の指定したＤＬ名が展開されるが、ＤＬメンバ名は公開されない。

受信者Ａあて…受信者公開許諾を発信者が指定
受信者Ｂあて…受信者公開許諾を発信者が指定
受信者Ｃあて…受信者公開禁止を発信者が指定

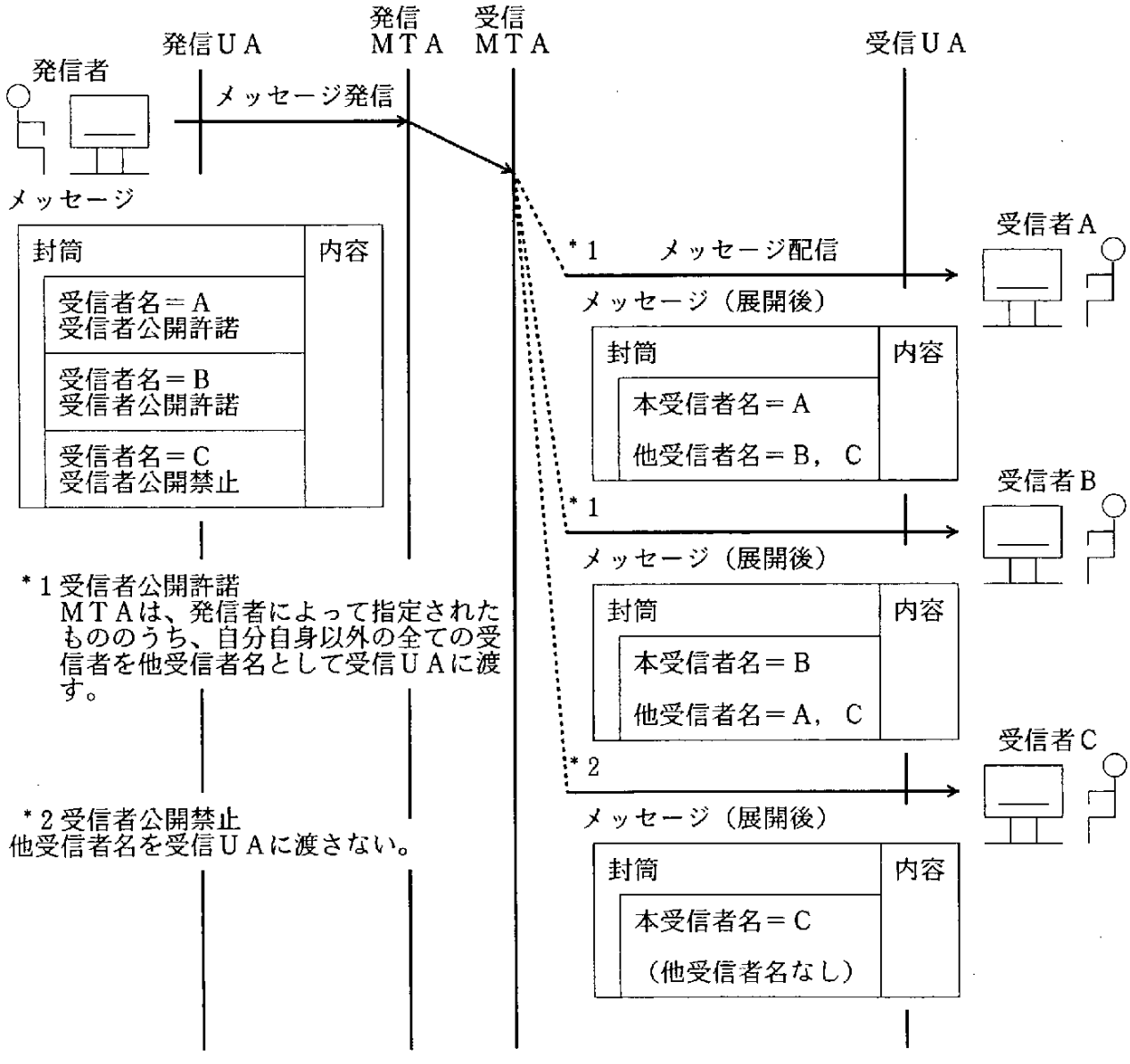


図2.7-9　他受信者名公開

2. 7. 8　ＥＤＩＦＡＣＴ情報表示

発信ＵＡは、ＥＤＩインタチェンジのデータ要素をＥＤＩメッセージの「見出し」の適切なフィールドにマッピングさせることができる。マッピングされる要素は、ＥＤＩメッセージ種別（例：送り状、発注書）やインタチェンジ送信者等であり、これらはＥＤＩメッセージの本体部にも含まれる情報である。これらの情報が見出しにも含まれていると、ＭＳの機能を用いて検索を行う際に有効である。

以下の図表ではＥＤＩインタチェンジの例としてＥＤＩＦＡＣＴインタチェンジを取り上げ、ＥＤＩＦＡＣＴインタチェンジがＥＤＩメッセージにマッピングされるイメージを示す。

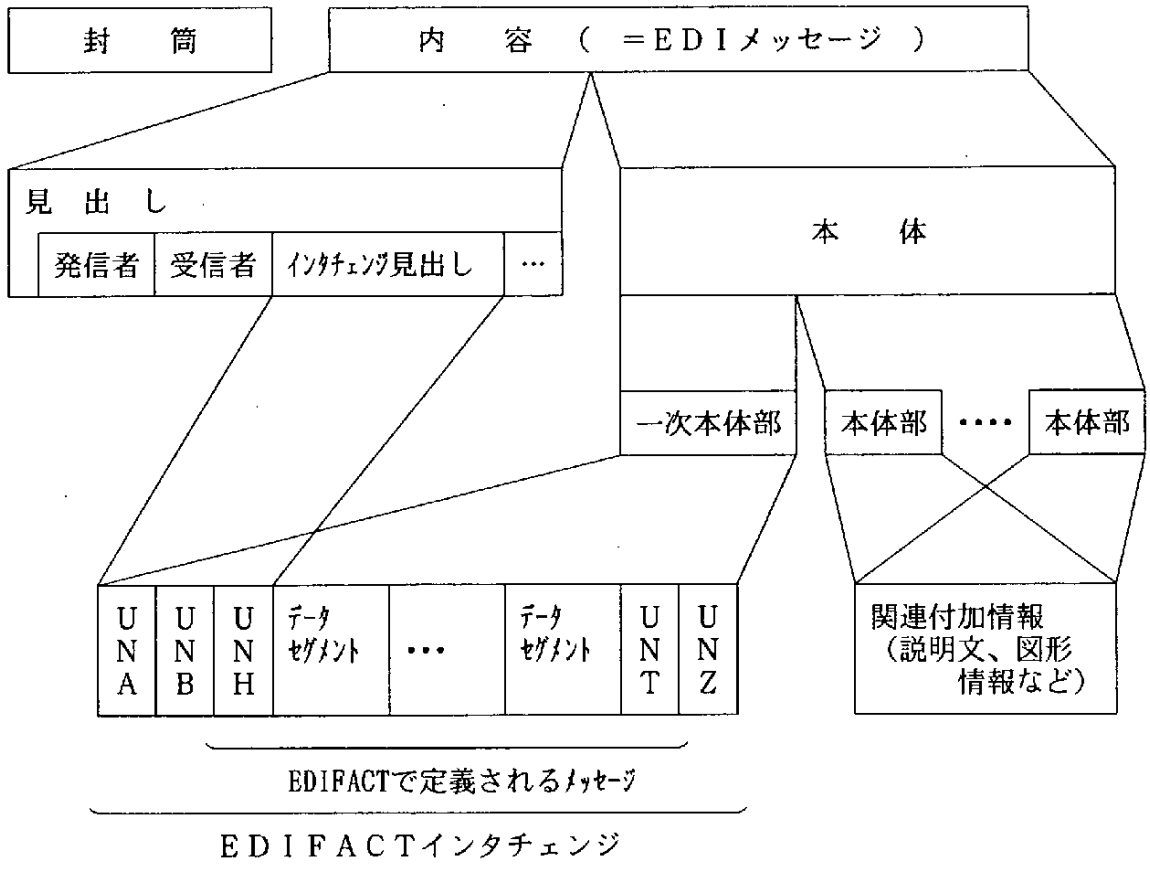


図2.7-10　ＥＤＩＦＡＣＴ情報表示イメージ

表2.7-1　ＥＤＩＦＡＣＴ情報表示項目

ｲﾝﾀﾁｪﾝｼﾞ見出しのフィールド名	概　　要	EDIFACT ｲﾝﾀﾁｪﾝｼﾞ
ＥＤＩ メッセージ種別	ＥＤＩインタチェンジに含まれるメッセージ（ＥＤＩＦＡＣＴにより定義される「メッセージ」であることに注意）の種別を提示する。 例：送り状、発注書	ＵＮＨ
サービス ストリング助言	ＥＤＩインタチェンジの中で用いられる特殊文字に関する規則を提示する。 例：データ要素分離子(+)、構成データ要素分離子(:)、 解放表示子(?)、セグメント終端子(')	ＵＮＡ
構文識別子	ＥＤＩインタチェンジの構文の識別子を提示する。ＥＤＩＦＡＣＴでは、構文識別子は管理機関、記述レベル、構文版番号から構成される。 例：管理機関(UNO=UN/ECE)、記述レベル(A)、構文版番号(2)	ＵＮＢ
インタチェンジ 送信者	ＥＤＩインタチェンジの送信者識別と識別コード修飾子を提示する。送信者識別（送信者のＩＤ：コードか名前が用いられる）は当事者間のインタチェンジ協定により取り決められる。	
インタチェンジ 受信者	ＥＤＩインタチェンジの受信者識別と識別コード修飾子を提示する。受信者識別（受信者のＩＤ：コードか名前が用いられる）は当事者間のインタチェンジ協定により取り決められる。	
処理優先度コード	処理の優先度を表すコードを提示する。コードは当事者間のインタチェンジ協定により取り決められる。	
準備日時	ＥＤＩインタチェンジの作成日時（年月日・時分）を提示する。これはＵＴＣ時刻で記述される。	
応用参照	ＥＤＩインタチェンジに含まれるメッセージが一種類の場合にメッセージ識別子を提示する。メッセージ識別子は、メッセージ種別、メッセージ版番号、メッセージリリース番号、管理機関などから構成される。	

2. 7. 9　本体種別表示

発信者は一つのメッセージの本体に複数の本体部分を含んだ形でメッセージを送信することができる。その際、発信者またはＭＴＡはメッセージ本体に含まれる各本体部分毎にその種別を付加して受信者に渡す。

本体種別としてＥＤＩ転送用に提供されている種別は次のものである。

・ＥＤＩ本体部分……ＥＤＩＦＡＣＴ、ＣＩＩフォーマット等に準拠したＥＤＩ交換データ

・回送ＥＤＩ本体部分…回送されたＥＤＩメッセージ

・外部定義本体部分……個人間メッセージ通信で使用される本体部分（ＩＡ５テキスト、音声、テレテックス等）

本体部分は明示的、または、暗黙的に発信者が発信した時の属性から変換されることがあり、その際、受信者には変換後の本体部分の属性が通知される。

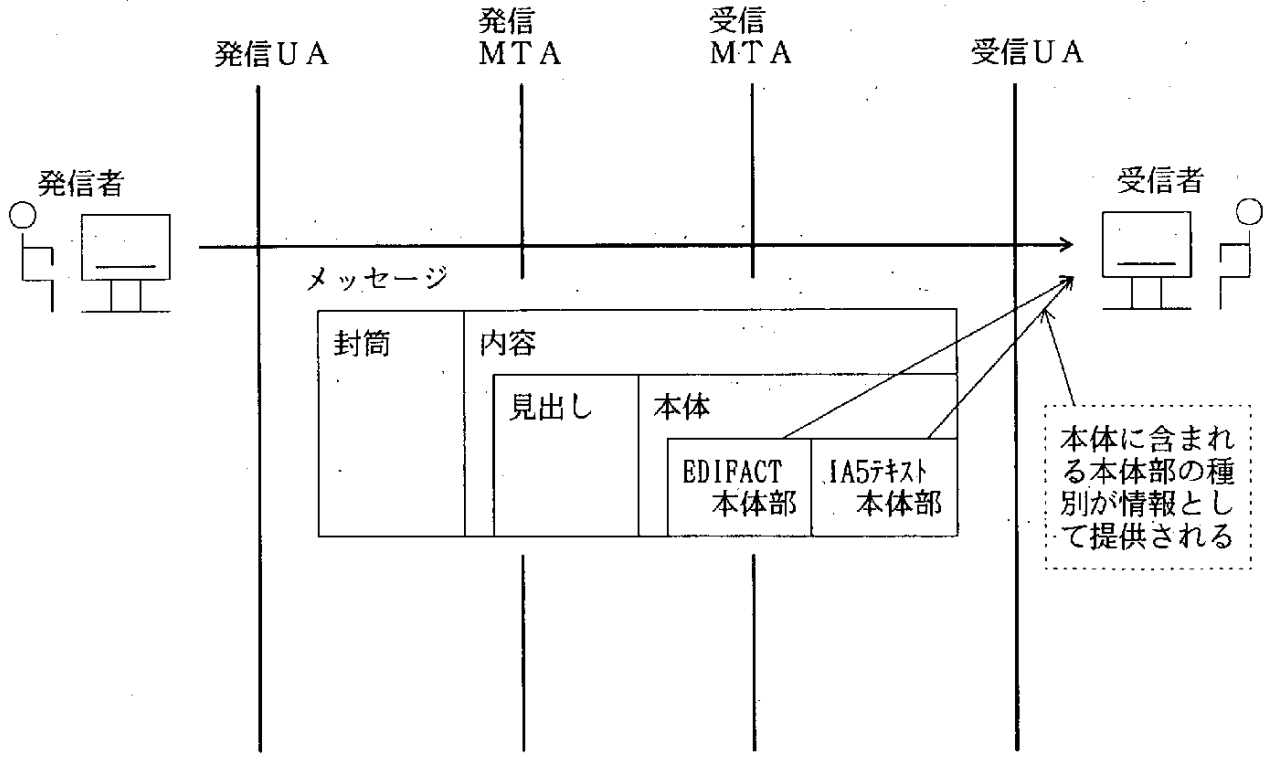


図2.7-11　本体種別表示

2. 7. 10　相互参照情報

(1) 概要

相互参照は、８４年版ＭＨＳから規定されているＩＰＭのサービスの一つをＥＤＩ用に拡張したものである。ＩＰＭでの利用は、ＩＰメッセージ間での関係を示すものであったが、Ｐｅｄｉでは、本体との相互関係を示すことができるように拡張された。例えば、発注伝票では、別に送受したメッセージに含まれる図表類や見積書を参照したり、同封するメッセージに添付した図表類を参照するような使い方ができるようになった。

(2) 参照情報

相互参照するための情報は、次に示す３つのパラメタの組み合わせによる。

① 応用相互参照　：応用プログラムが設定する任意の文字列（必須）
② メッセージ参照：ＥＤＩメッセージ識別子　（任意選択）
③ 本体部参照　　：ＥＤＩメッセージ内で一意な整数値　（必須）

応用相互参照は、ＥＤＩ利用者が任意に設定可能な情報である（勧告の規定範囲外）。メッセージ参照は、送信するＥＤＩメッセージの他の本体部を参照する際に必要なパラメタである（このパラメタが存在しないときは、同一メッセージ内であることを示す）。本体部参照は、参照するメッセージ内の何番目の本体部を参照するかを示すパラメタである。これらを組み合わせて、参照先を（世界的に）一意にすることが可能となる。

(3) 使用例

同一メッセージ内で相互参照情報を利用する例を以下に示す。図中の相互参照情報フィールドには、応用プログラム名の設定した“図表番号:12345”と、ＥＤＩメッセージの本体部の中に含まれる図表を格納した本体部の番号を示す“２”が設定されている。

もし、他のメッセージを参照する場合には、図の相互参照情報フィールドにメッセージ参照が追加されるだけである。

相互参照情報フィールドに設定可能な参照先は、複数設定可能である（最大数については、勧告上未規定である）。

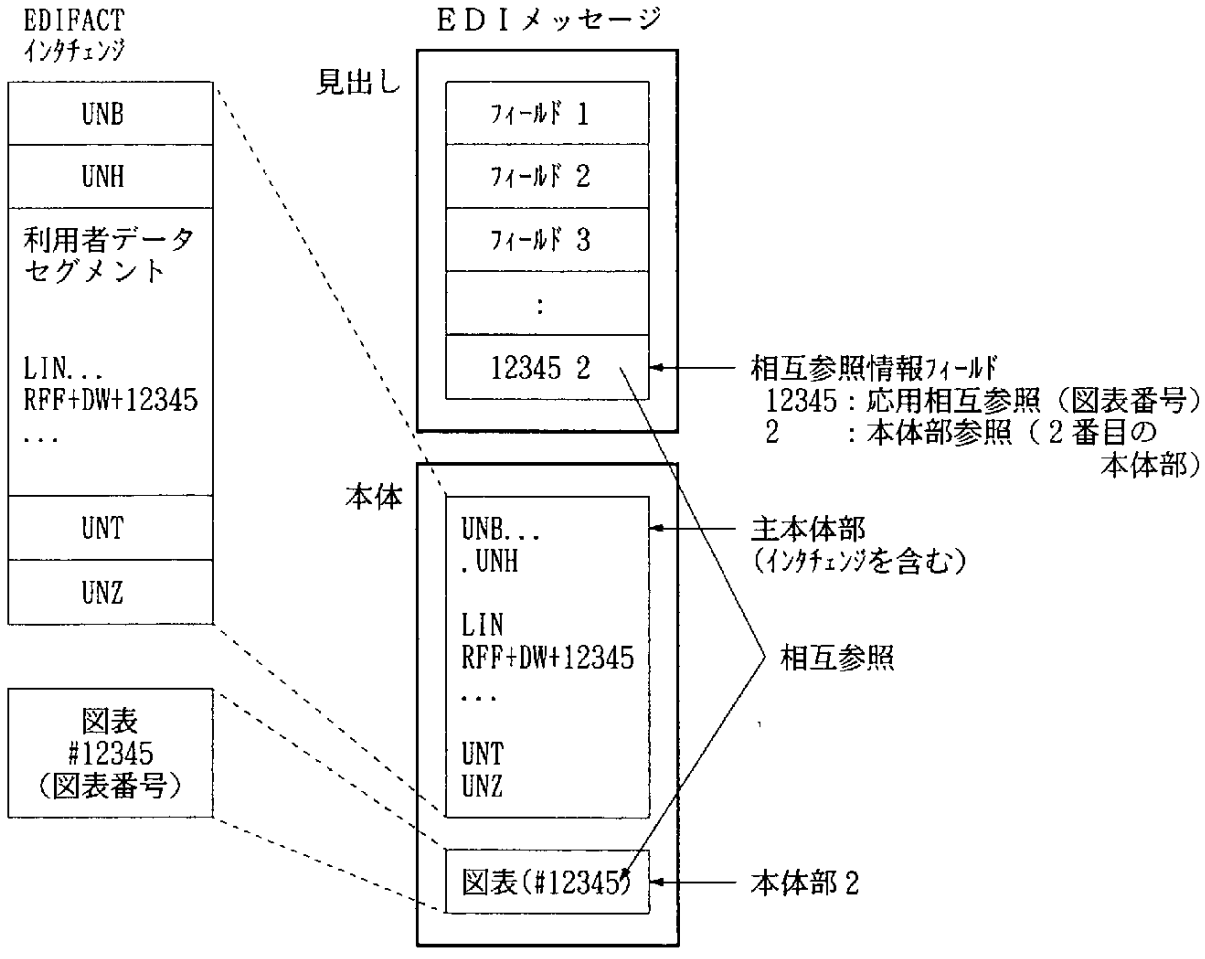


図2.2-12　相互参照情報の使用例

2. 8　あて先変更サービス

2. 8. 1　代行受信者許可

発信者はメッセージ発信時、本来受信者に配信が不可能な場合、代行受信者にメッセージ配信してもよいことを指示できる。代行受信者の決定方法には、

・発信者による代行受信者指定　　（「2.8.3 発信者要求代行受信者」参照）
・受信者による代行受信者指定　　（「2.8.4 受信者指定あて先変更」参照）
・受信ＵＡの属する管理領域において、あらかじめ登録された代行受信者を指定
（「2.8.2 代行受信者登録」参照）

がある。

このとき、発信者の要求により、代行受信者へメッセージが配信された旨を配信通知を使い発信者に通知することができる。

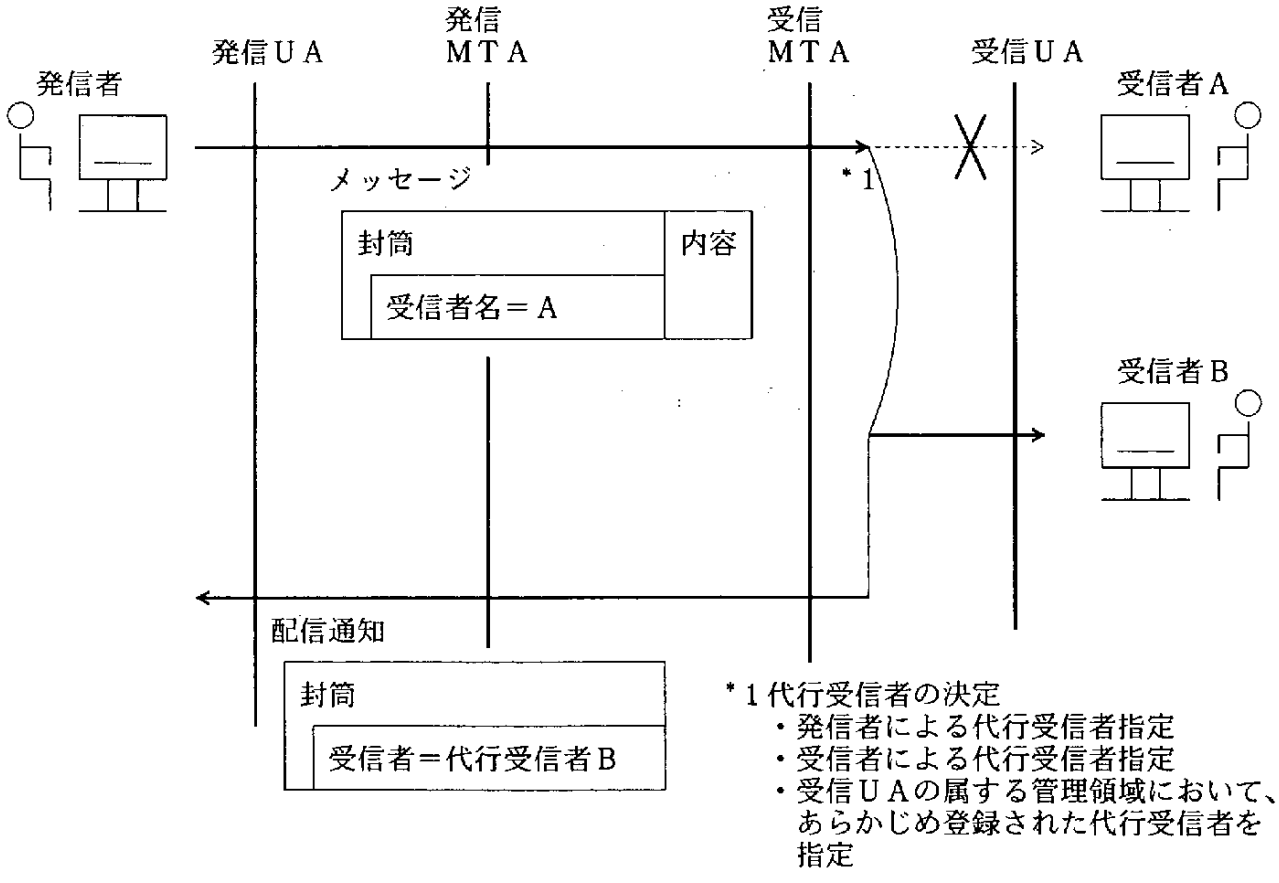


図2.8-1　代行受信者許可

2. 8. 2　代行受信者登録

代行受信者登録サービス要素を提供する管理領域は、利用者の名前と指定された受信者のO／Rアドレスが正確に一致しないメッセージを、代行受信者としての特定のＵＡに配信させることを許す。例として、国名、主官機関管理領域名および組織名は正確に一致するが、受信者の個人名がその組織においてＭＨＳに登録されている個人名に対応しないメッセージを受信できるＵＡを作ることができる。このようにして配信されたメッセージは、手作業で振り分けられることが想定される。

利用者の名前と指定された受信者のO／Rアドレスが正確に一致しないメッセージを受信側管理領域のＭＴＡが受け取ったならば、ＭＴＡは、代行受信者として登録されている受信ＵＡにメッセージを配信する。このとき、発信者が指定した受信者のO／R名が、本来受信者名として通知される。発信者が要求している場合は、このＵＡに配信されたことが配信通知により報告される。

なお、上記の場合でも、発信されるメッセージに代行受信者許可が設定されていない場合、代行受信はされず、配信不能通知が返される。

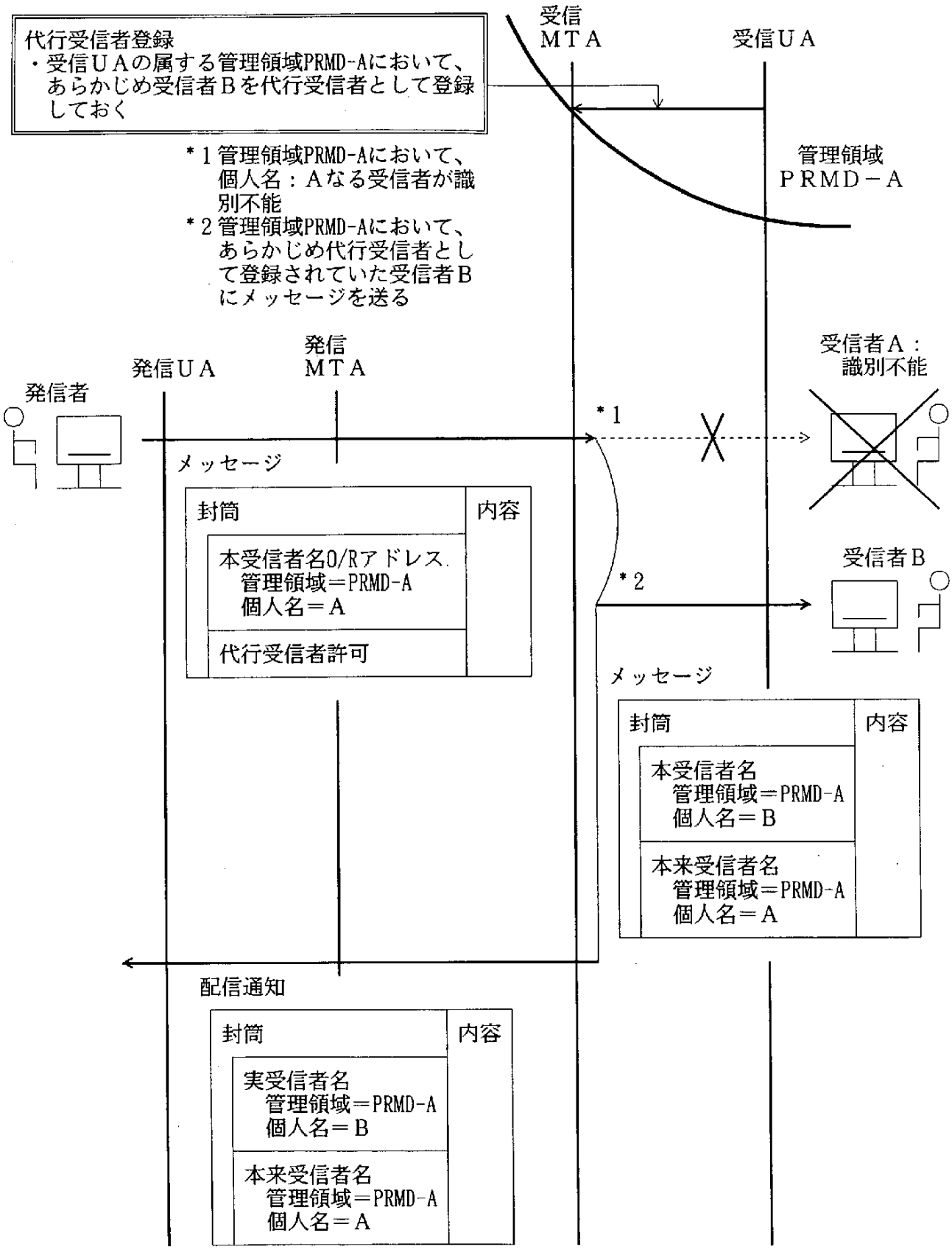


図2.8- 2　代行受信者登録

2. 8. 3　発信者要求代行受信者

発信者はメッセージ発信時、本来受信者に配信が不可能な場合、代わりに受信する受信者を指定することができる。

受信ＭＴＡは本来受信者へメッセージを配信できない場合、発信者からこの指定がされていれば指定先の受信者にメッセージを迂回して配信する。

代わりに受信した受信者は配信通知で発信者に通知される。

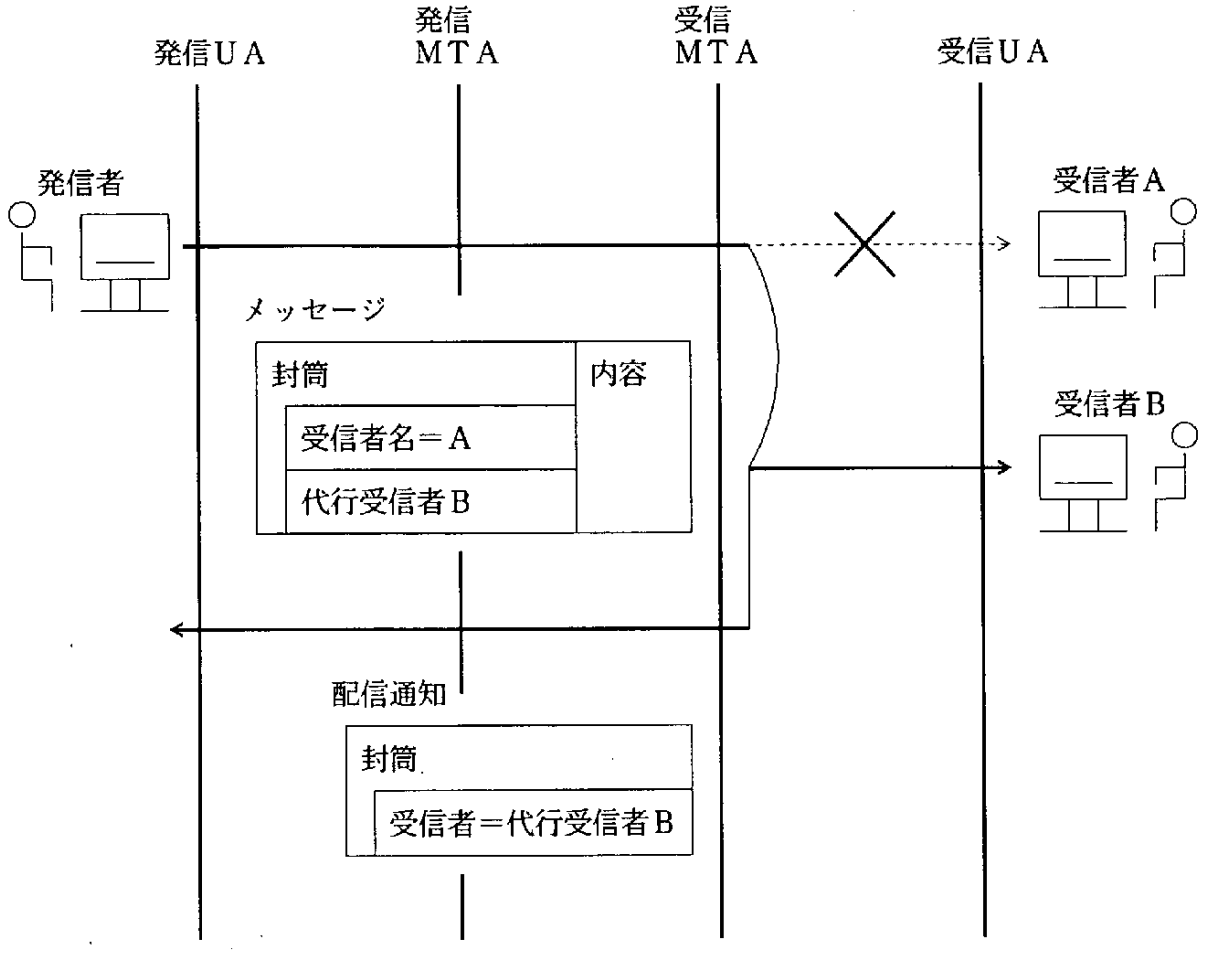


図2.8- 3　発信者要求代行受信者

2. 8. 4　受信者指定あて先変更

受信者はある特定の期間、例えば出張等によりメールを見ることができない場合、自分あてのメッセージを他の受信者に転送するよう、受信ＭＴＡに要求することができる。

受信ＭＴＡはメッセージ配信時、本来受信者による迂回の指示により、本来受信者への配信が行えない場合、迂回先の受信者にメッセージを転送する。

代わりに受信した受信者は配信通知で発信者に通知される。

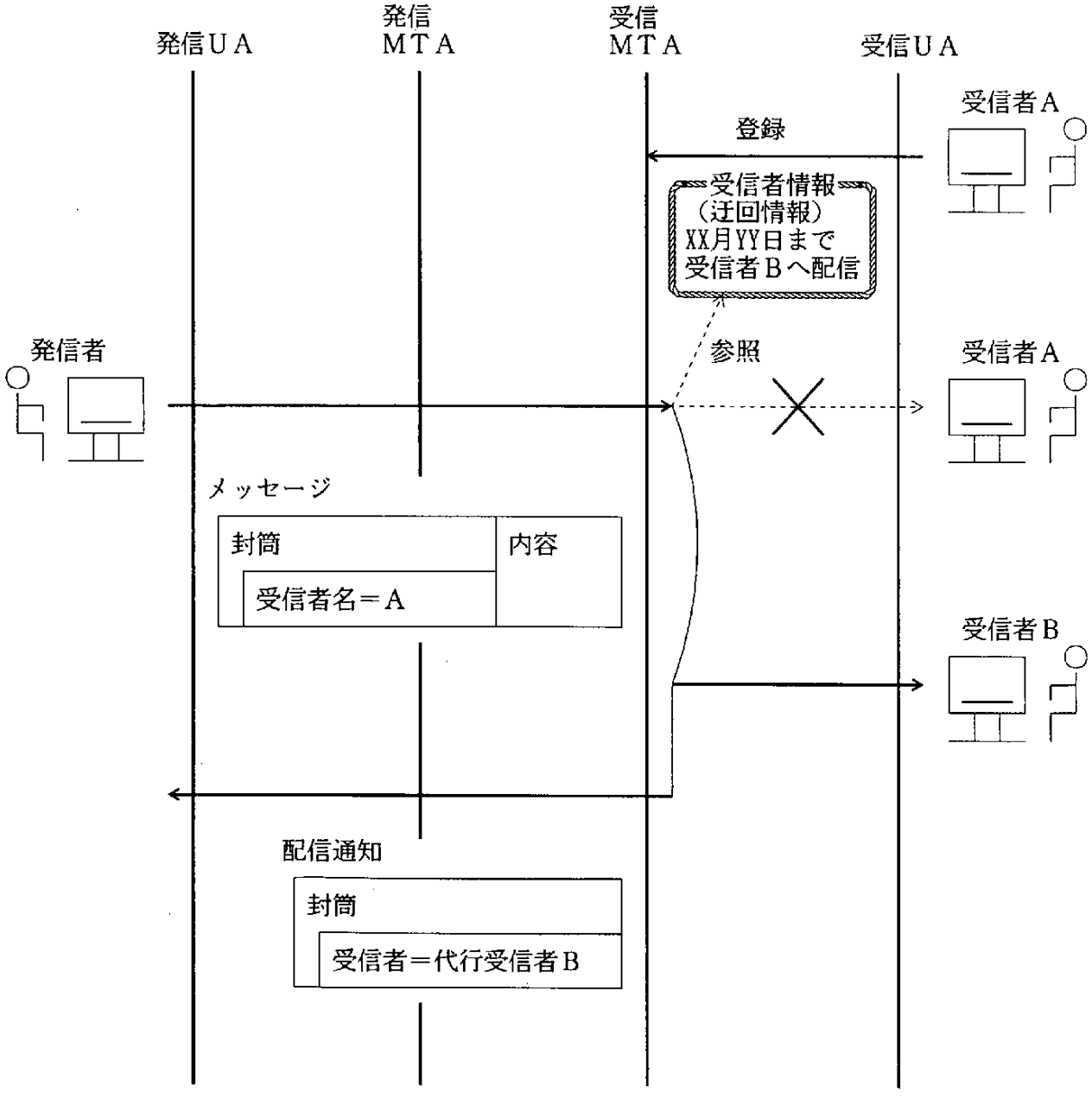


図2.8-4　受信者指定あて先変更

2. 8. 5　あて先変更の発信者による禁止

発信者は、受信者が指定した代行受信者に対してメッセージを迂回して配信してもよいかどうかを指定することができる。このサービスは「2.8.4 受信者指定あて先変更」サービスにより、受信者が指定したメッセージの迂回要求を、発信者が禁止するサービスである。

発信者が許可した場合、受信ＭＴＡはメッセージを本来受信者に配信できず、かつ、受信者によって代行受信者が登録されていればその受信者にメッセージを配信する。

発信者が禁止した場合、受信ＭＴＡは代行受信者への配信を行わず、配信不能通知を返却する。

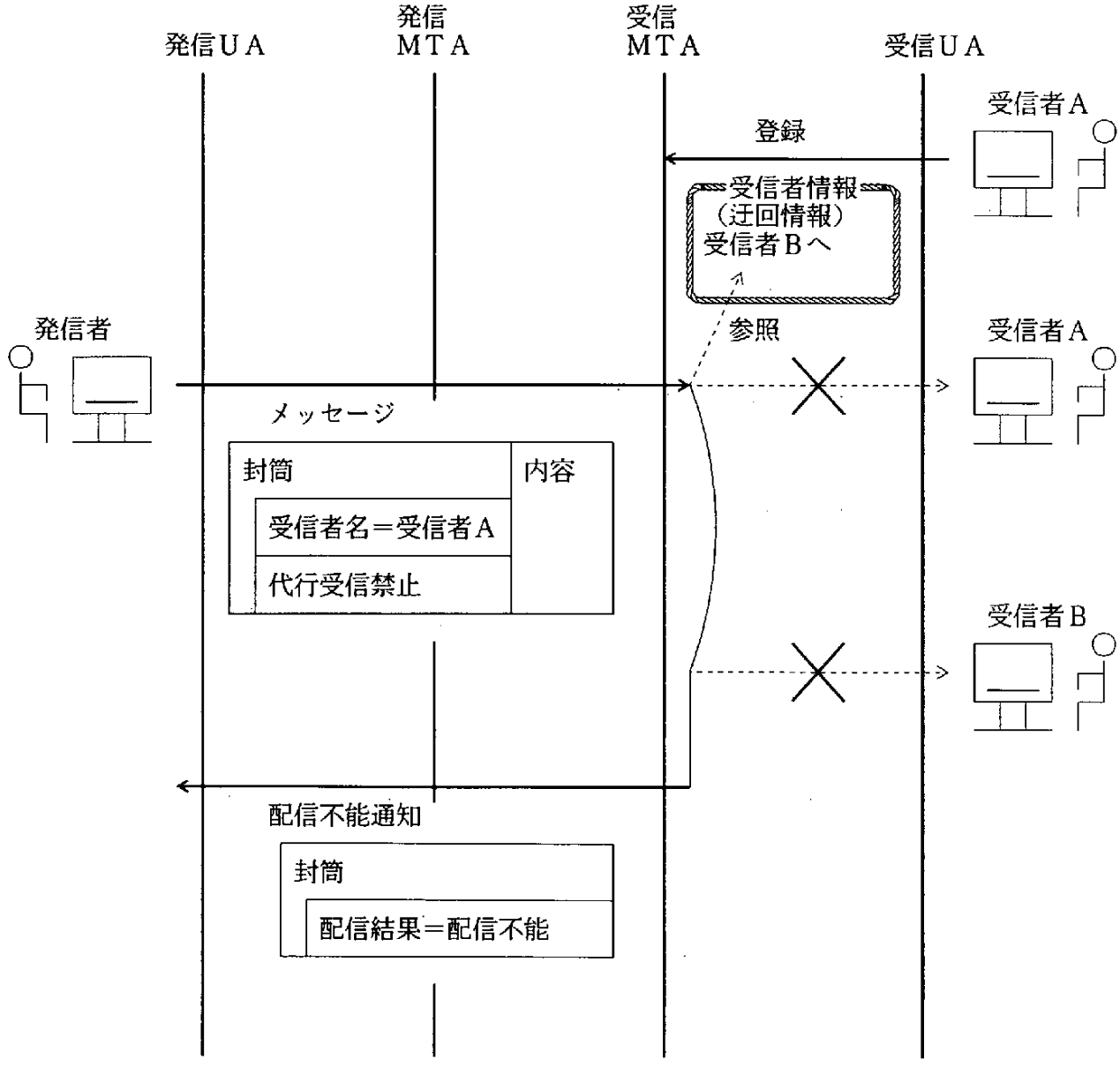


図2.8- 5　あて先変更の発信者による禁止

2. 9 安全保護サービス

2. 9. 1 安全保護付きアクセス管理

隣接する構成要素間（ＵＡ－ＭＴＡ，ＭＴＡ－ＭＴＡ，ＭＴＡ－ＭＳ，ＭＳ－ＵＡ）はお互いに厳密な資格証明の交換による接続を行うことにより、詐称のような脅威を防ぐことができる。

この操作はメッセージ転送や検索等の要求に先立って行われる。

資格証明には暗号化技術を使用した起動側資格証明および応答側資格証明が用いられ、発信者の情報とそれを証明する証明機関による証明情報によって認証を行う。

また接続の際、安全保護ラベルを交換することにより、その後のメッセージ通信における、機密保護方針（秘密度）を決定することができる（「2.9.9 安全保護ラベル」参照）。

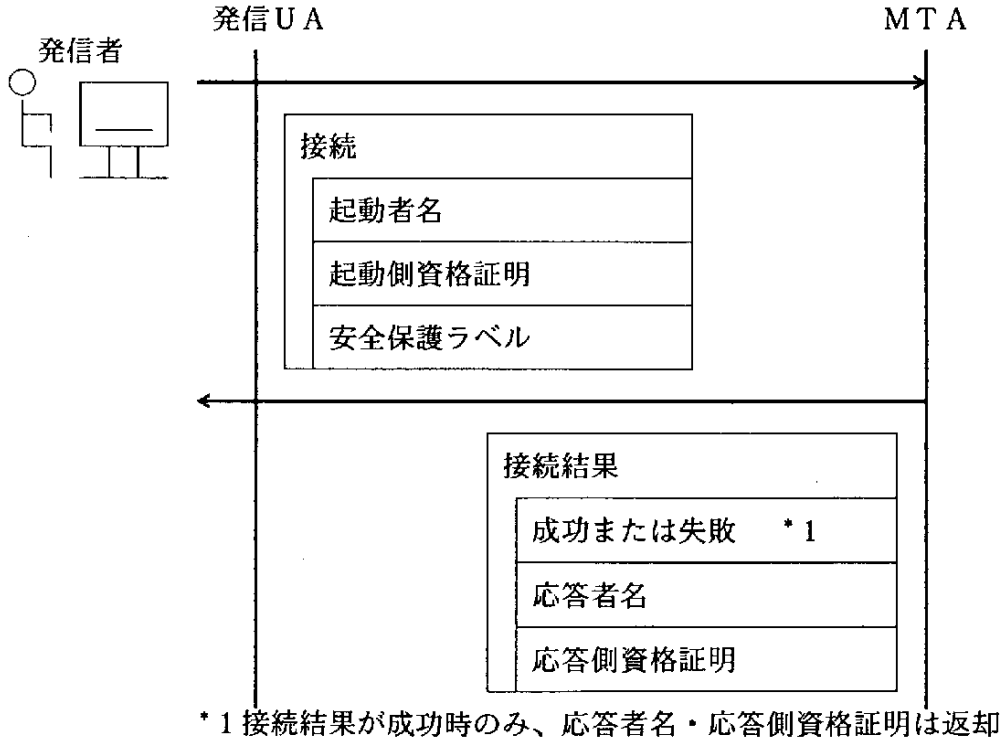
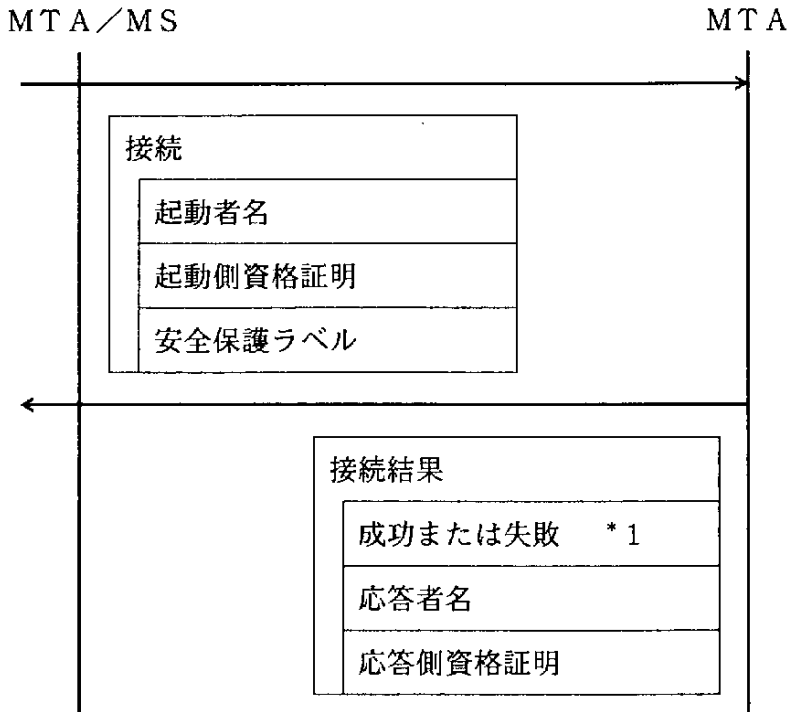
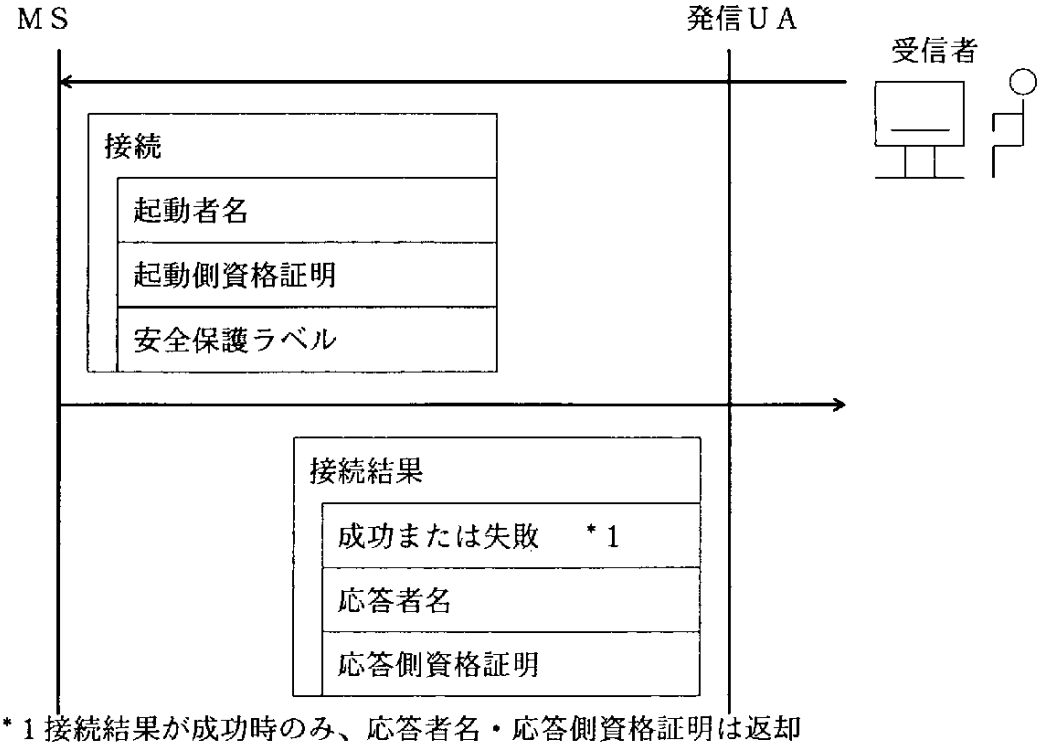


図2.9- 1(1) 安全保護付きアクセス管理



*1 接続結果が成功時のみ、応答者名・応答側資格証明は返却



*1 接続結果が成功時のみ、応答者名・応答側資格証明は返却

図2.9- 1(2)　安全保護付きアクセス管理（続き）

2. 9. 2　メッセージ安全保護ラベル

隣接する構成要素間（ＵＡ－ＭＴＡ，ＭＴＡ－ＭＴＡ，ＵＡ－ＭＳ，ＭＳ－ＭＴＡ）の接続において、安全保護ラベルの交換により、その後のメッセージ通信における安全保護方針が決定され、安全保護環境が確立される（「2.9.1 安全保護付きアクセス管理」参照)。

安全保護ラベルは、安全保護方針識別子、安全保護度などの安全保護属性を含んでおり、隣接する構成要素間で安全保護環境が確立された場合、その環境で取り扱われるメッセージや打診等が「どのような安全保護方針の下で」「どのような分類の秘密度により」取り扱われるか、を決定できる。表2.9- 1は、メッセージ安全保護ラベルに含まれる安全保護属性を示している。

表2.9- 2は、隣接するＭＨＳ構成要素間（ＵＡ－ＭＴＡ，ＭＴＡ－ＭＴＡ，等）で安全保護環境が確立している場合と確立していない場合について、相互動作を比較したものである。メッセージあるいは打診の発信者は、実施中の安全保護方針に従って、発信するメッセージあるいは打診にメッセージ安全保護ラベルを指定し、メッセージを発信・中継・受信するＭＴＡおよびＭＳに対し、安全保護方針に沿ったメッセージの扱いを強制することができる。

図2.9- 2に例として、受信ＭＴＡが、受信者に対し、メッセージの安全保護ラベルにより代行受信者指定サービスを提供する場合を述べる。

（注釈）

通知のメッセージ安全保護ラベルは、対象のメッセージ（あるいは打診）のメッセージ安全保護ラベルと同じでなくてはならない。

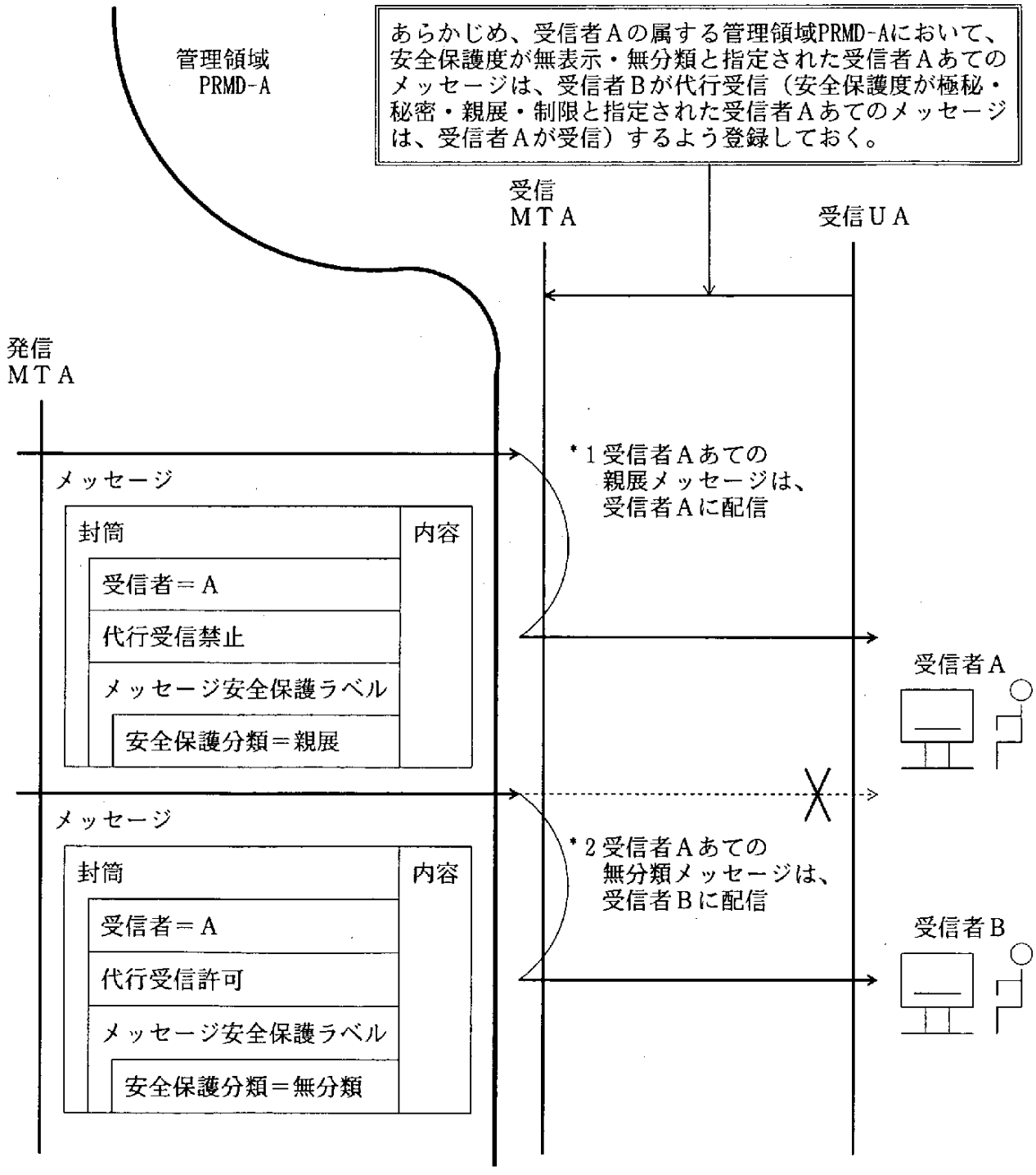


図2.9- 2　代行受信におけるメッセージ安全保護ラベルの利用

表2.9-1　メッセージ安全保護ラベルに含まれ得る安全保護属性

メッセージ安全保護ラベルに含まれ得る安全保護属性	備　　考
安全保護方針識別子	安全保護ラベルに関係した、実施中の（もしくは実施される）安全保護方針を識別する。
安全保護度	基本となる安全保護度は以下のとおり昇順の階層構造として定義される。 ・無表示（公開できる情報） ・無分類（非公開の情報） ・制限 ・親展 ・秘密 ・極秘 （秘密度大 ↓） これらの値の使用法は実施中の安全保護方針によって定義される。なお、規定範囲外の安全保護方針または相互協定によってこれらの分類への新たな定義を付加してもよい。
内密表示	印字可能文字から成る。印字可能文字の内容は、 ・実施中の安全保護方針によって定義されてもよい。 ・送信者によって値を決めることを許してもよい。 内密表示の例として、“信任”、“絶対信任”等がある。
安全保護分類群	安全保護分類群は、安全保護度および内密表示に関する制限の詳細を示す。安全保護度およびその値は、規定範囲外の安全保護方針または相互協定によって定義してもよい。

表2.9-2　メッセージ安全保護ラベルがＭＴＳ相互動作に与える影響

相互動作への影響	安全保護環境が確立されている	安全保護環境が確立されていない
発信者 →発信ＭＴＡ	発信者がメッセージ（あるいは打診）に割り当てるメッセージ安全保護ラベルは、確立されている安全保護環境により決定される。	発信者がメッセージ（あるいは打診）に割り当てるメッセージ安全保護ラベルは、送信者の意志により決定される。
ＭＴＡ→ＭＴＡ	ＭＴＡ間のメッセージ、打診、通知の転送はメッセージ、打診、通知のメッセージ安全保護ラベルと確立されている安全保護環境により決定される。	ＭＴＡ間のメッセージ、打診、通知の転送は送信者の意志により決定される。
受信ＭＴＡ →受信者	メッセージと通知の配信はメッセージと通知のメッセージ安全保護ラベルと、確立されている安全保護環境により決定される。メッセージあるいは通知のメッセージ安全保護ラベルが、登録済である受信者の利用者メッセージ安全保護ラベルによって許容されるが、確立されている安全保護環境では許容されない場合、受信ＭＴＡは配信を保留(hold-for-delivery）する。	メッセージと通知の配信は受信側ＭＴＡの任意である。

2. 9. 3　内容機密性

メッセージの発信者は、内容機密性サービスを使うことによってメッセージの内容が本来受信者以外の受信者に開示されることを防ぐ、つまり盗聴を防ぐことができる。内容機密性は非対称または対称の暗号化技術を使用する。メッセージの発信者は発信メッセージ中に、内容機密性アルゴリズム識別子（および内容機密性鍵）を付加して発信する。

① 内容機密性アルゴリズム識別子

メッセージの発信者が、メッセージを暗号化するのに使用するアルゴリズムを識別する。

対称暗号化アルゴリズムならば、内容機密性鍵（もしくは別の手段で送られる鍵）によりメッセージの発信者はメッセージの内容を暗号化している。よって、メッセージの受信者は、メッセージの内容の復号化に内容機密性鍵（もしくは別の手段で送られた鍵）を利用する。

非対称暗号化アルゴリズムならば、本来受信者の公開非対称暗号鍵によりメッセージの発信者はメッセージの内容を暗号化している。よって、メッセージの受信者は、メッセージの内容の復号化に受信者の秘密非対称暗号鍵を利用する。

なお、非対称暗号化アルゴリズムが使用される場合、実質的に同報はできない。

② 内容機密性鍵

メッセージの発信者がメッセージの内容を暗号化するため、また、メッセージの受信者がメッセージの内容を復号化するため、内容機密性アルゴリズム識別子と共に使われる対称暗号鍵である。この情報は、メッセージトークンと呼ばれる、発信メッセージの封筒の情報に含まれている。

内容機密性が対称暗号アルゴリズムにより実現され、内容機密性鍵が暗号化された内容と共に送られる場合、通常、その鍵は盗聴から防御する目的で暗号化される。　図2.9- 3では、ＤＥＳ(Data Encryption Standard)等の対称暗号化アルゴリズムによりメッセージの内容を暗号化することで内容機密性を保証した例を示す。

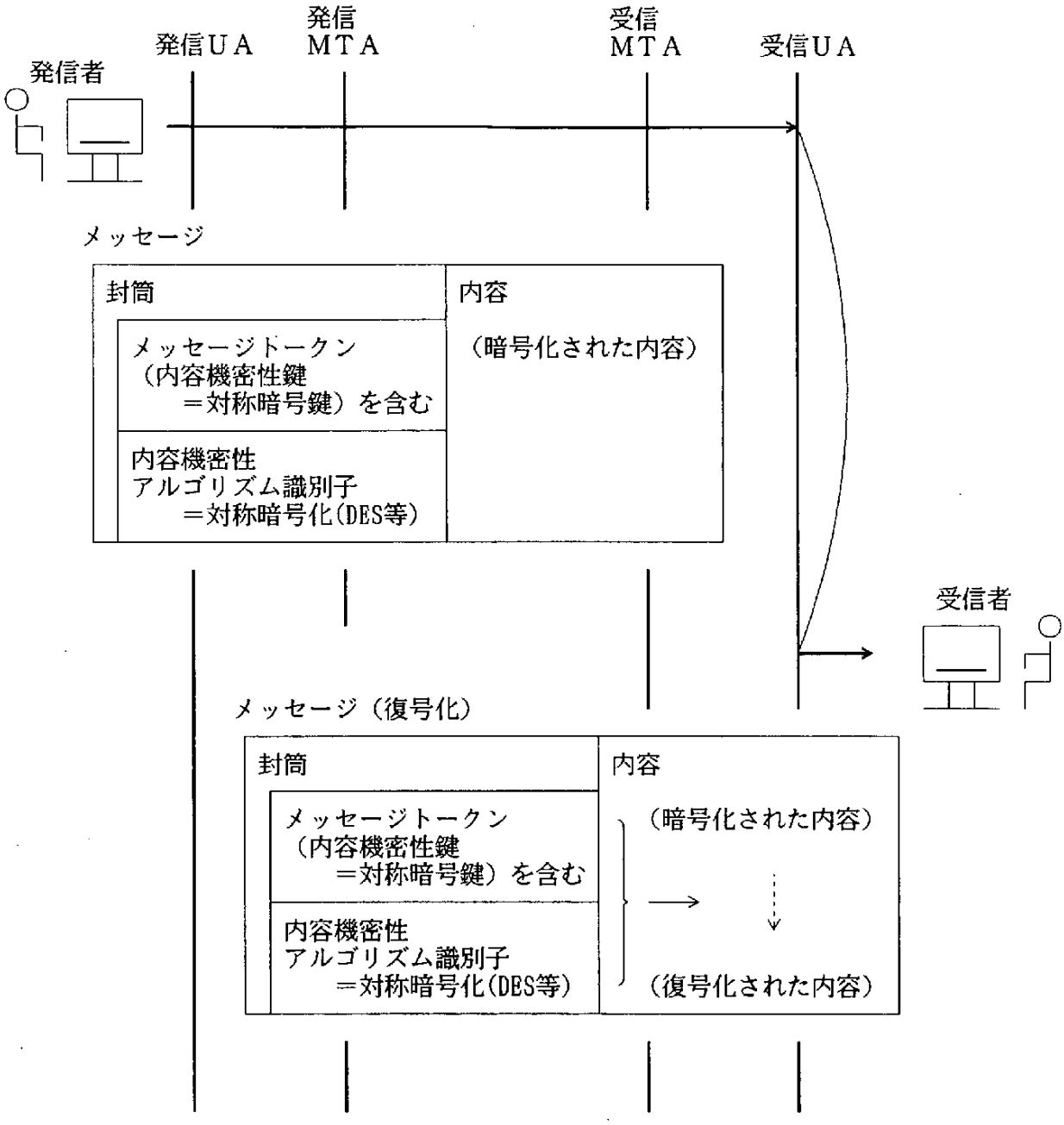


図2.9- 3　内容機密性～対称暗号化アルゴリズム使用の場合

2. 9. 4　メッセージ流れ機密性

メッセージの発信者は、第三者が不当にメッセージの流れを監視し、トラヒックの分析等を行う情報漏洩のような脅威を防ぐことができる。

現在提供されているサービスには二重封筒技法（「2.7.2 内容種別表示」参照）がある。

この技法は、送りたいメッセージをさらに外側のメッセージの内容で包むことでメッセージ中のアドレス情報を隠ぺいし（内容機密性サービスとの併用）、外側のメッセージを例えば、信頼できるＵＡ等に送信した後、そのＵＡから本来受信者に転送してもらう使用が想定されている。

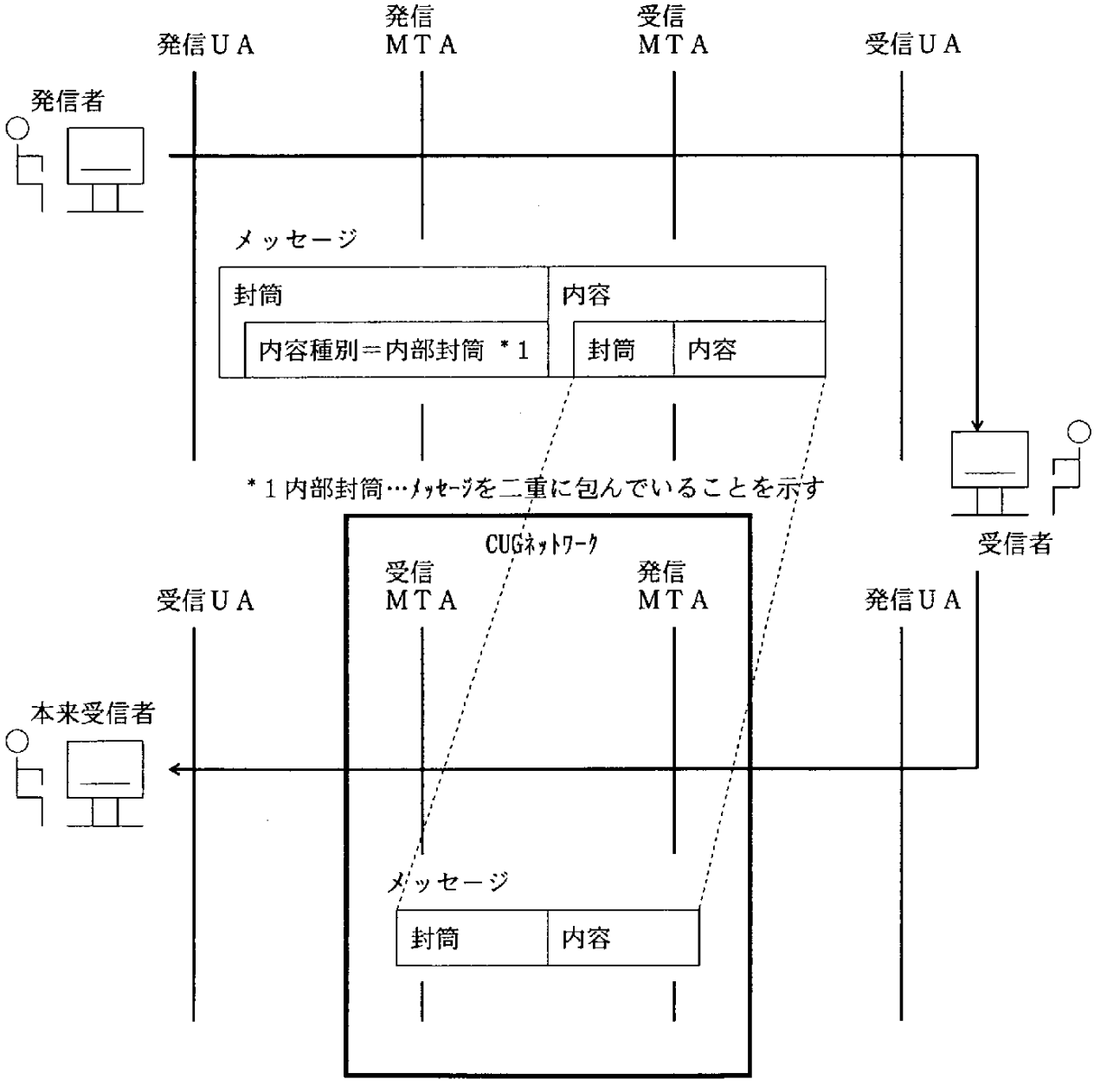


図2.9- 4　メッセージ流れ機密性

2. 9. 5　内容完全性

メッセージの発信者は、内容が変更されていないことを確認するための手段をメッセージの受信者に提供することができる。内容完全性は受信者ごとに適用可能であり、一方向性ハッシュ関数、対称暗号化アルゴリズム、非対称暗号化アルゴリズム等を使用する。

メッセージの発信者は、発信メッセージ中に、内容完全性検査（もしくは、内容完全性検査および内容完全性鍵）を付加して発信する。

① 内容完全性検査

メッセージの発信者が、メッセージを暗号化するのに使用するアルゴリズムを指定する。

内容完全性検査は、自らの構造中にアルゴリズム識別子（＝内容完全性アルゴリズム識別子）を含んでおり、この識別子により識別されるアルゴリズムを使用して計算される。

一方向性ハッシュ関数が使用される場合、メッセージの発信者は、暗号化されていないメッセージの内容を指定した一方向性ハッシュ関数によりハッシュ化することで、内容完全性検査値を算出している。メッセージ受信者は、配信されたメッセージの暗号化されていない内容を（メッセージ発信者と同様に）ハッシュ化し、それと内容完全性検査値が一致することにより、内容が完全であることを確認できる。

対称暗号化アルゴリズムが使用される場合、メッセージの発信者は、暗号化されていないメッセージの内容を対称暗号鍵である内容完全性鍵により暗号化することで、内容完全性検査値を算出している。よって、メッセージの受信者は、この内容完全性検査を対称暗号鍵である内容完全性鍵により復号化し、暗号化されていないメッセージの内容と一致させることで、内容が完全であることを確認できる。なお、内容完全性鍵の情報は、メッセージトークンと呼ばれる、発信メッセージの封筒の情報に含まれている。

非対称暗号化アルゴリズムが使用される場合、暗号化されていないメッセージの内容を目的の受信者の公開非対称暗号鍵により暗号化することで、内容完全性検査値を算出している。よって、メッセージの受信者は、内容完全性検査値を受信者の秘密非対称暗号鍵により復号化し、暗号化されていないメッセージの内容と一致させることで、内容が完全であることを確認できる。

② 内容完全性鍵

メッセージの発信者が、メッセージの内容を対称暗号鍵である内容完全性鍵により暗号化し内容完全性検査値を算出するために、またメッセージの受信者が、内容完全性検査値を対称暗号鍵である内容完全性鍵により復号化するために、内容完全性検査と共に使われる対称暗号鍵である。この情報は、メッセージトークンと呼ばれる、発信メッセージの封筒の情報に含まれている。

図2.9- 5の例では、ハッシュ関数を使用した場合を示している。ここでは、メッセージ内容の暗号化を行っていないので内容完全性鍵は入ってこない。

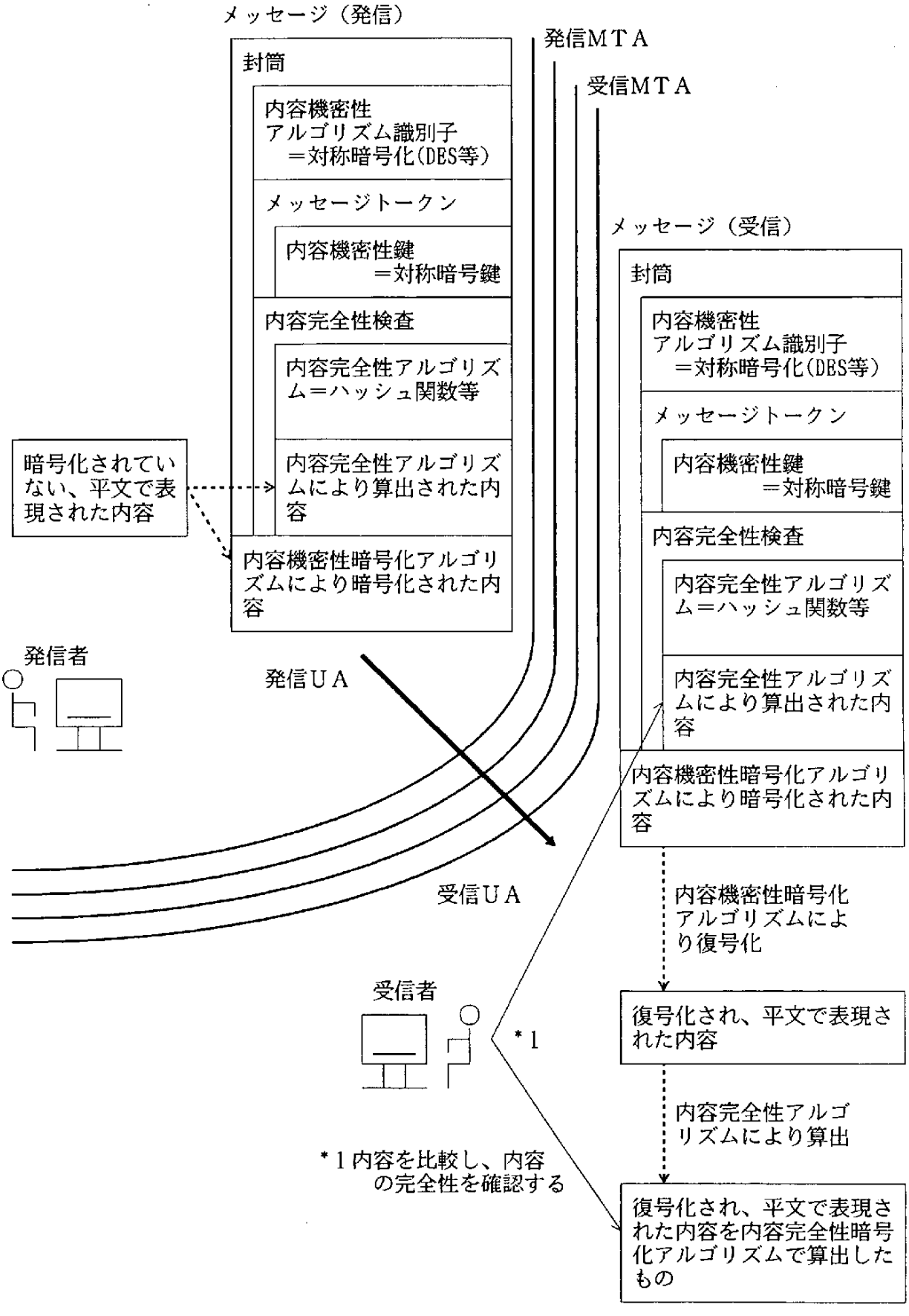


図2.9- 5　内容完全性～ハッシュ関数使用の場合

2. 9. 6　メッセージ順序完全性

メッセージの受信者は、発信者と受信者との間でメッセージの順序が保たれていることの確認により、第三者によるメッセージの破壊、再送、順序変更のような脅威を防ぐことができる。

メッセージの発信者は発信メッセージの情報としてメッセージトークンと呼ばれる情報に順序番号を付加して送信する。

受信者は受信したメッセージのメッセージ順序番号をチェックして、メッセージ順序性の検証を行う。

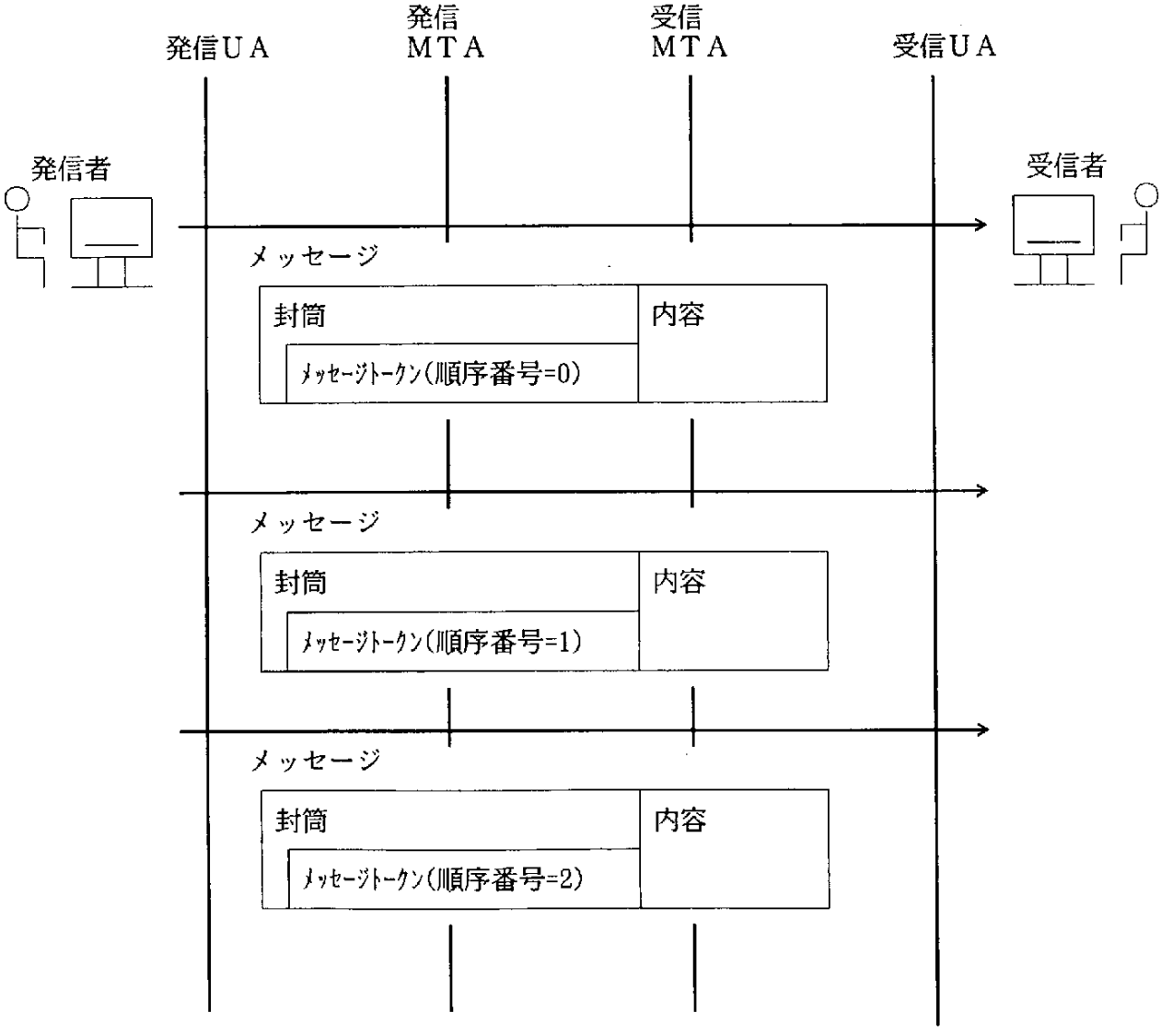


図2.9- 6　メッセージ順序完全性

2. 9. 7　メッセージ発生源認証および発生源／発信内容の否認不能

受信者またはメッセージを転送する各ＭＴＡはメッセージの発信元を認証することによって詐称のような脅威を防ぐことができる。

メッセージの発信者は発信メッセージ中に、「メッセージ発生源認証検査」と呼ばれるメッセージ内容等を発信者の秘密鍵で暗号化した情報、「発信者証明」と呼ばれる発信者の公開鍵を含む情報を付加して発信する（このサービスには非対称暗号化技術のみが適用）。

受信者またはＭＴＡは非対称暗号化技術を使用したこれらの情報を元に、発信者証明中の公開鍵によってメッセージ発生源認証検査を復号化し、メッセージの内容と照合することによって、発信元の認証を行う。

また発信者が秘密鍵によって暗号化したものを公開鍵によって復号化して照合（デジタル署名の利用）することにより、発信者による発信の否認を防ぐこともできる。

この時、メッセージ発生源認証検査に含まれる「内容」を復合化して発信メッセージの内容と照合することにより、発信メッセージの内容が改ざんされてないことと発信者が発信した内容を不正に否認することを防ぐことができる。

ただし内容機密性サービスが同時に提供される場合、暗号化された「内容」に対する署名は否認不能サービスの対象とならないことになっており、この場合はメッセージ発生源認証のみのサービスとなる。

メッセージ発生源認証は同時に内容の完全性も保証する。内容完全性サービスとの違いは、内容完全性サービスが受信者毎に提供するサービスであるのに対し、メッセージ発生源認証サービスはメッセージ毎に提供するサービスである。

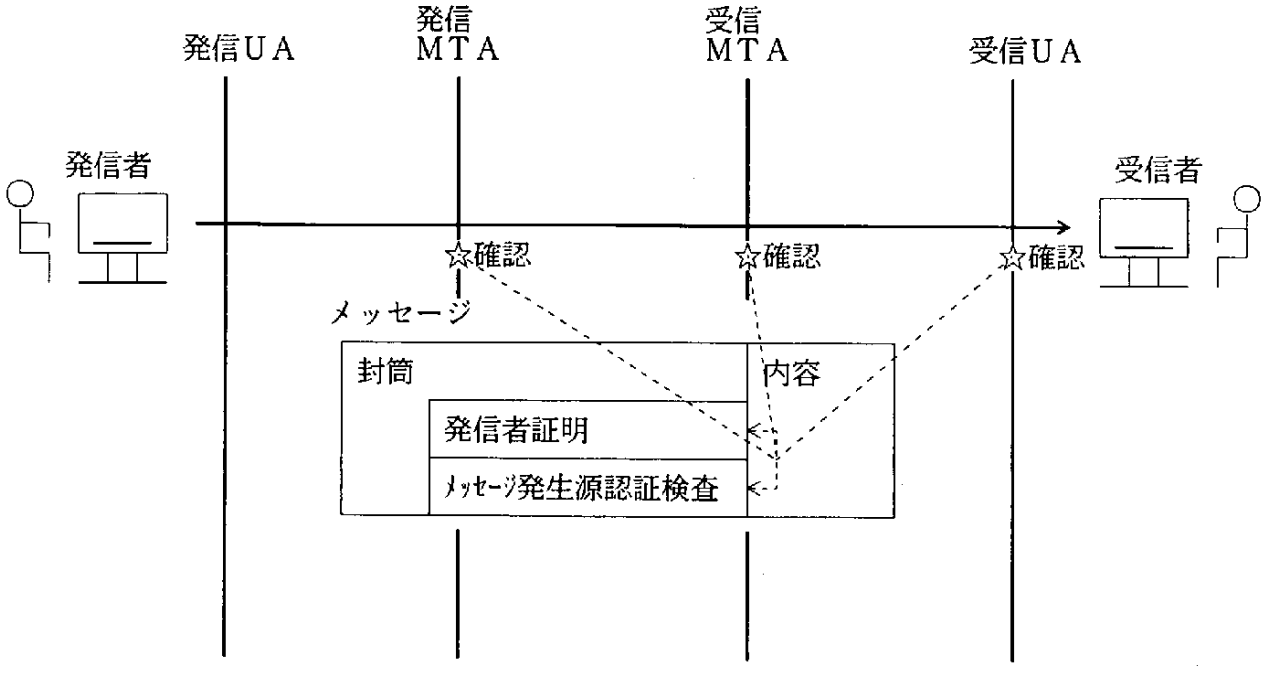


図2.9- 7　メッセージ発生源認証および発生源の否認不能

2. 9. 8　ＥＤＩ通知証明およびＥＤＩ通知の否認不能

発信者は、ＥＤＩメッセージ発信時に受信者に対するＥＤＩ通知要求の中で、「ＥＤＩ通知証明」または「ＥＤＩ通知否認不能」を要求することができる。このときＥＤＩメッセージ受信者は、ＥＤＩ通知受信者（ＥＤＩメッセージ発信者）に対してＥＤＩ通知の発信者が確かに自分であることを証明する。

［証明方法］

①　ＥＤＩ通知発信者（ＥＤＩメッセージ受信者）

ＥＤＩ通知の発信者は、ＥＤＩ通知中に以下の引数を付加して発信する。

・「メッセージ発生源認証検査」…メッセージ内容等を発信者の秘密鍵で暗号化した情報

・「発信者証明」…発信者の公開鍵を含む情報

②　ＥＤＩ通知受信者（ＥＤＩメッセージ発信者）またはＭＴＡ

ＥＤＩ通知の受信者またはＭＴＡは、非対称暗号化技術を使用したこれらの情報を元に、「発信者証明」中の公開鍵によって「メッセージ発生源認証検査」を復号化し、メッセージの内容（＝ＥＤＩ通知）と照合することによって、発信元の認証を行う。

備考：「ＥＤＩ通知証明」は「メッセージ発生源認証」安全保護サービス、「ＥＤＩ通知否認不能」は「発生源の否認不能」安全保護サービスにより提供される。

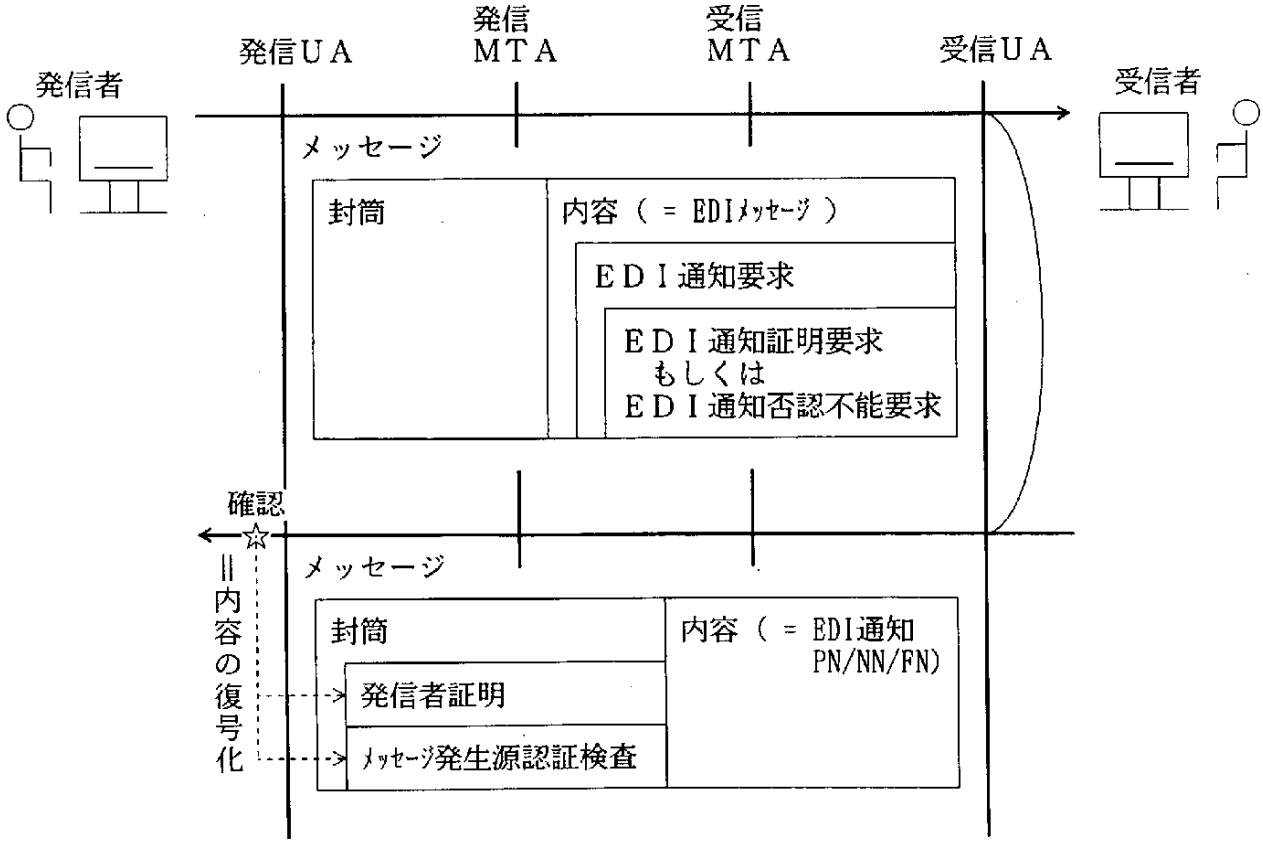


図2.9-８　ＥＤＩ通知証明およびＥＤＩ通知の否認不能

2. 9. 9　打診発生源認証

打診メッセージを転送する各ＭＴＡは打診メッセージの発信元を認証することによって、詐称のような脅威を防ぐことができる。

打診メッセージを発信するＭＴＡは打診メッセージ中に「打診発生源認証検査」と呼ばれるメッセージの内容識別子(*1)等を発信者の秘密鍵で暗号化した情報、「発信者証明」と呼ばれる発信者の公開鍵を含む情報を付加して発信する。

打診メッセージを中継転送する各ＭＴＡは暗号化技術を使用したこれらの情報を元に、発信者証明中の公開鍵によって打診発生源認証検査を復号化し、照合することによって打診元の認証を行う。

＊１内容識別子…発信者が内容を一意に識別するための識別子であり、発信したメッセージと返却された配信通知とを対応づけたりするために利用する。

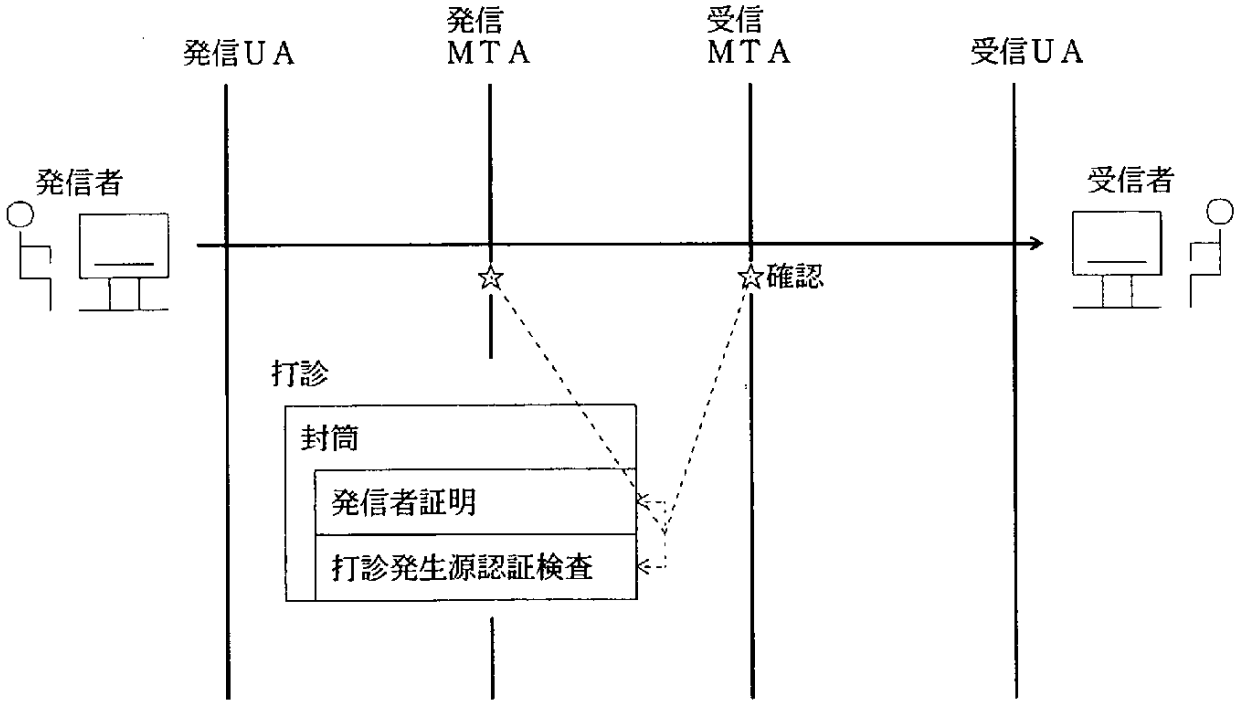


図2.9- 9　打診発生源認証

2. 9. 10　報告発生源認証

メッセージまたは打診の発信者は、配信通知または配信不能通知の報告元を認証することによって詐称のような脅威を防ぐことができる。

配信通知または配信不能通知を発信するＭＴＡは配信、配信不能通知中に「報告発生源認証検査」と呼ばれる受信者情報等を報告ＭＴＡ（図の例では受信ＭＴＡ）の秘密鍵で暗号化した情報、「報告ＭＴＡ証明」と呼ばれる報告ＭＴＡの公開鍵を含む情報を付加して発信する。

発信者は暗号化技術を使用したこれらの情報を元に、報告ＭＴＡ証明中の公開鍵によって、報告発生源認証検査を復号化し、照合することによって報告の発信元の認証を行う。

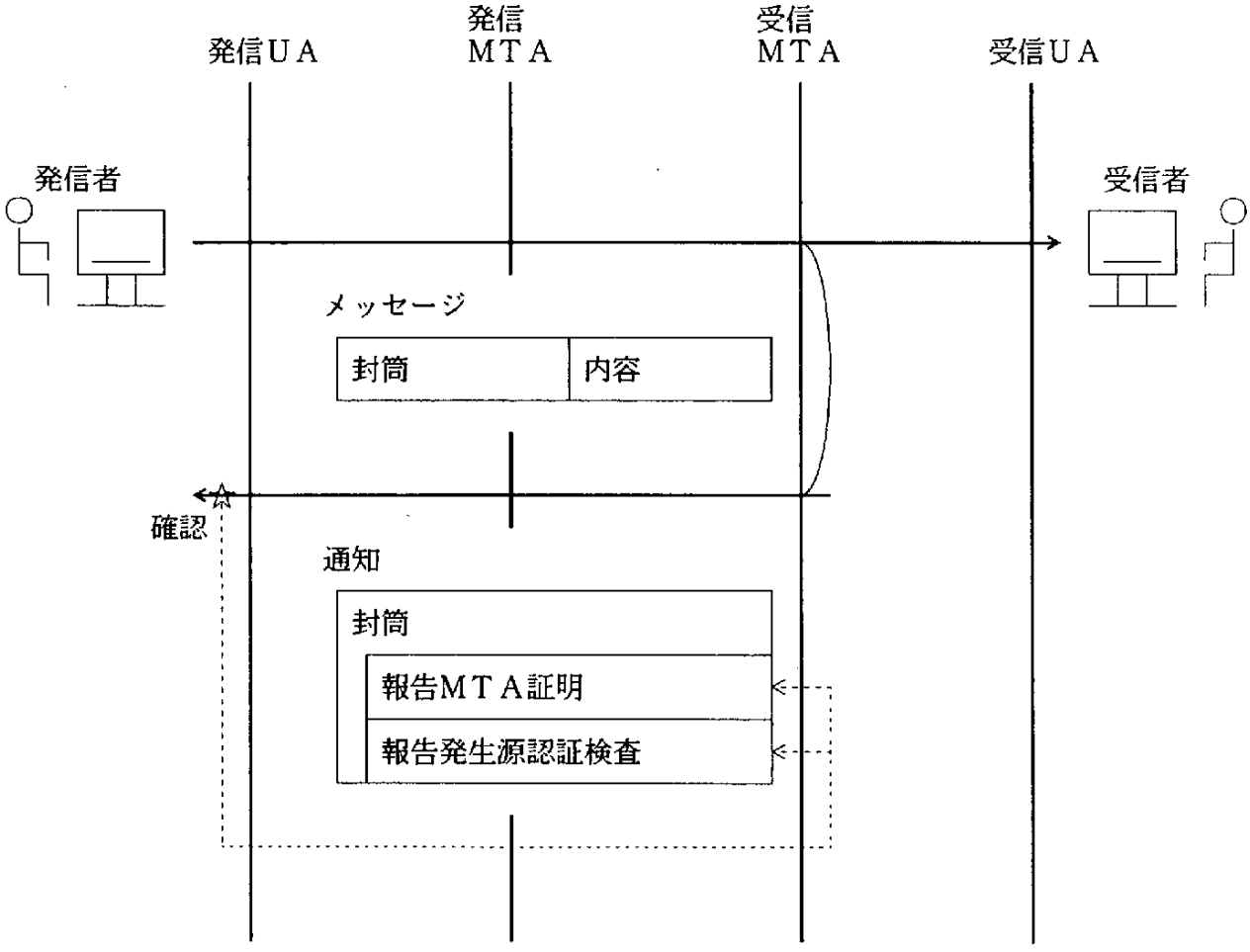


図2.9-10　報告発生源認証

2. 9. 11　発信証明および発信の否認不能

メッセージの発信者は、発信したメッセージが、自分が指定した受信者への配信のために発信ＭＴＡによって送信されたことを確認し、詐称のような脅威を防ぐことができる。

発信ＭＴＡは発信者から発信証明要求を指定されると発信操作結果中に「発信証明」と呼ばれる発信メッセージの引数等を発信ＭＴＡの秘密鍵で暗号化した情報、「発信ＭＴＡ証明」と呼ばれる発信ＭＴＡの公開鍵を含む情報を付加して返却する。

発信者は暗号化技術を使用したこれらの情報を元に、発信ＭＴＡ証明中の公開鍵によって、発信証明を復号化し、照合することによって、発信ＭＴＡの認証を行う。

また発信ＭＴＡが秘密鍵によって暗号化したものを公開鍵によって復号化して照合することにより、発信ＭＴＡによる発信の否認を防ぐこともできる。

発信証明の暗号化、復号化を対称鍵によって行うことも可能であるが、その場合発信証明のみ提供し，発信の否認不能は提供しない。またその時、発信ＭＴＡ証明は使用されない。

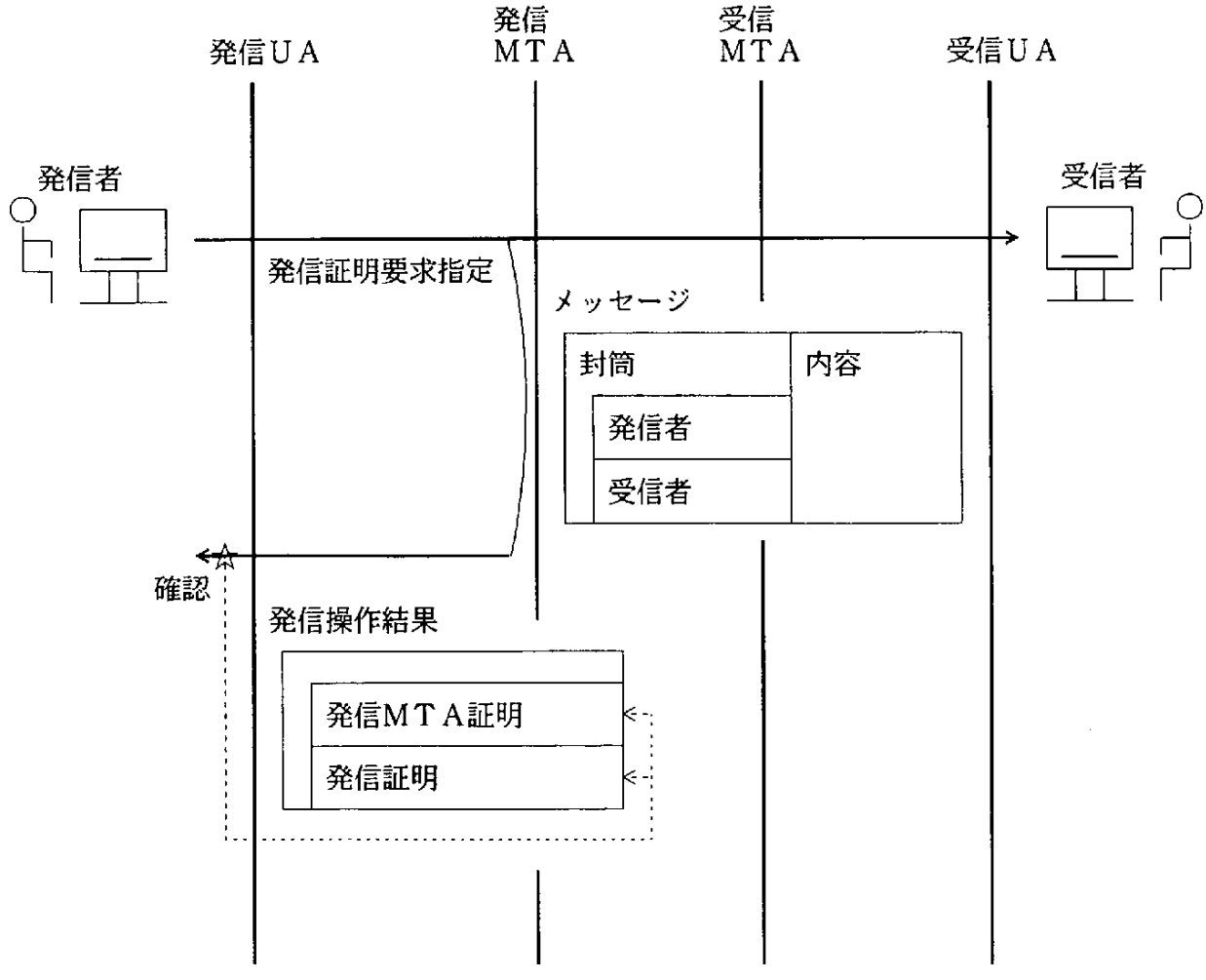


図2.9-11　発信証明および発信の否認不能

2. 9. 12　配信証明および配信の否認不能

メッセージの発信者は、メッセージが自分の指定した受信者に正しく配信されたことの確認により、詐称のような脅威を防ぐことができる。

受信ＭＴＡは発信者から配信証明要求が指定されていた場合、配信または配信不能通知中に「配信証明」と呼ばれる受信者情報等を受信者の秘密鍵で暗号化した情報、「受信者証明」と呼ばれる受信者の公開鍵を含む情報を付加して発信する。

発信者は暗号化技術を使用したこれらの情報を元に、受信者証明中の公開鍵によって、配信証明を復号化し、照合することによって、発信ＭＴＡの認証を行う。

また受信者の秘密鍵によって暗号化したものを公開鍵によって復号化して照合することにより、受信者による配信の否認を防ぐこともできる。

配信証明の暗号化、復号化を対称鍵によって行うことも可能であるが、その場合配信証明のみ提供し、配信の否認不能は提供しない。またその時、受信者証明は使用されない。

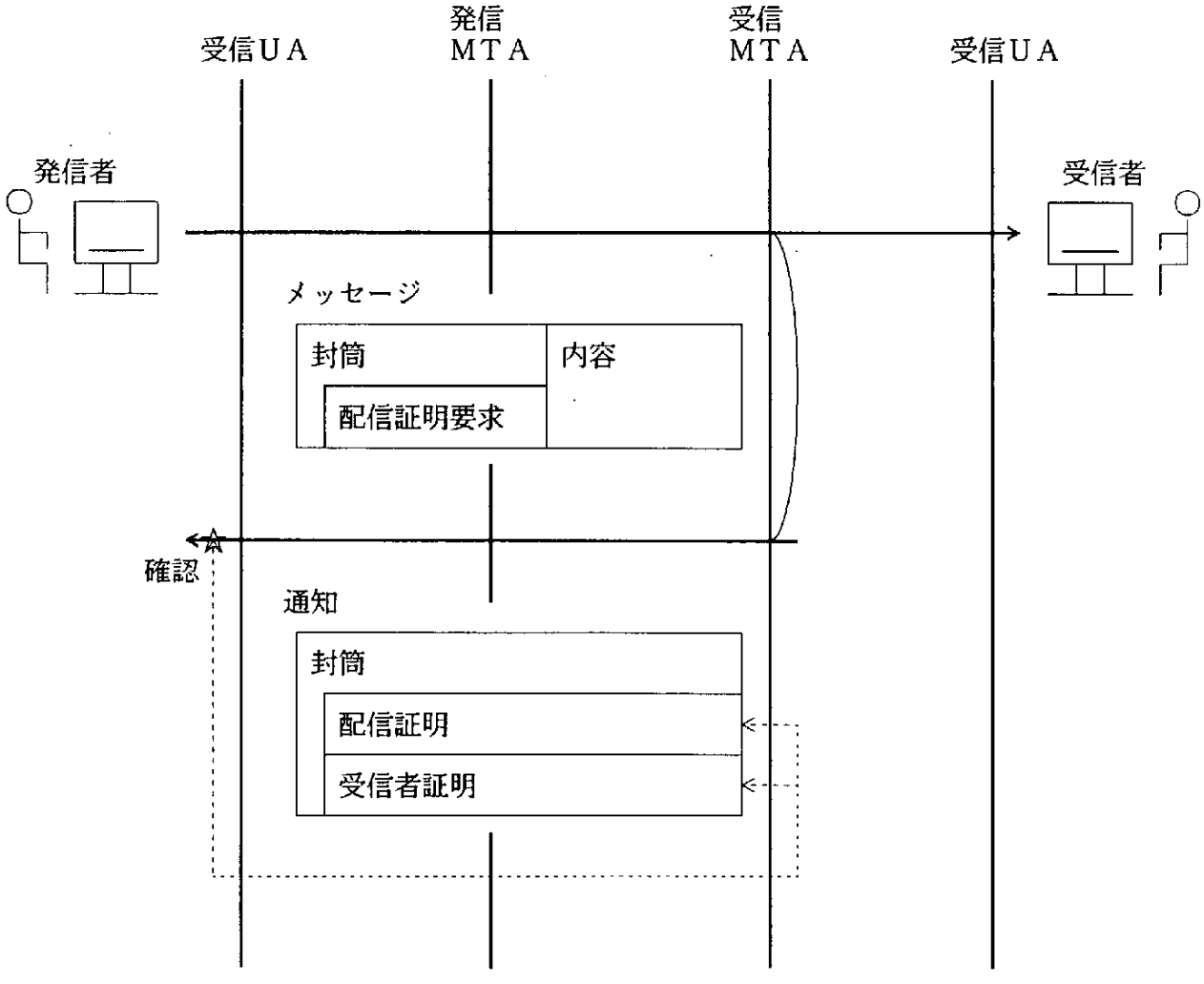


図2. 9-12　配信証明および配信の否認不能

2. 9. 13　受信内容証明および受信内容の否認不能

発信者は、ＥＤＩメッセージ発信時に受信者に対するＥＤＩ通知要求の中で、「受信内容証明」または「受信内容の否認不能」を要求することができる。このときＥＤＩメッセージ受信者は、自分の受信したＥＤＩメッセージの中身が改ざんされていないことをＥＤＩメッセージ発信者に対して証明する。以下に証明方法を示す。

・ＥＤＩメッセージ受信者（ＥＤＩ通知発信者）

当該メッセージに含まれる「内容完全性検査」を、ＥＤＩ通知（「原メッセージ内容完全性検査」）にコピーする。当該メッセージに「内容完全性検査」が含まれていない場合には、当該メッセージの「内容」を、ＥＤＩ通知（「原内容」）にコピーする。受信内容証明の場合には、当該メッセージに含まれる「メッセージ発生源認証検査」をＥＤＩ通知の中にコピーすることでも証明が可能である。

・ＥＤＩメッセージ発信者（ＥＤＩ通知受信者）

ＥＤＩ通知から得られる情報と自分が発信したＥＤＩメッセージの情報とを照合し一致することを確認する。

なお、「受信内容証明」と「受信内容否認不能」では用いる暗号化の技術が異なっており（「受信内容の否認不能」の方が確実な証明を提供する）、「受信内容の否認不能」サービスが用いられる場合、受信者は当該ＥＤＩメッセージを受信したことを後で不正に否認することはできない。「内容完全性検査（＊1）」については「2.9.5」を参照されたい。

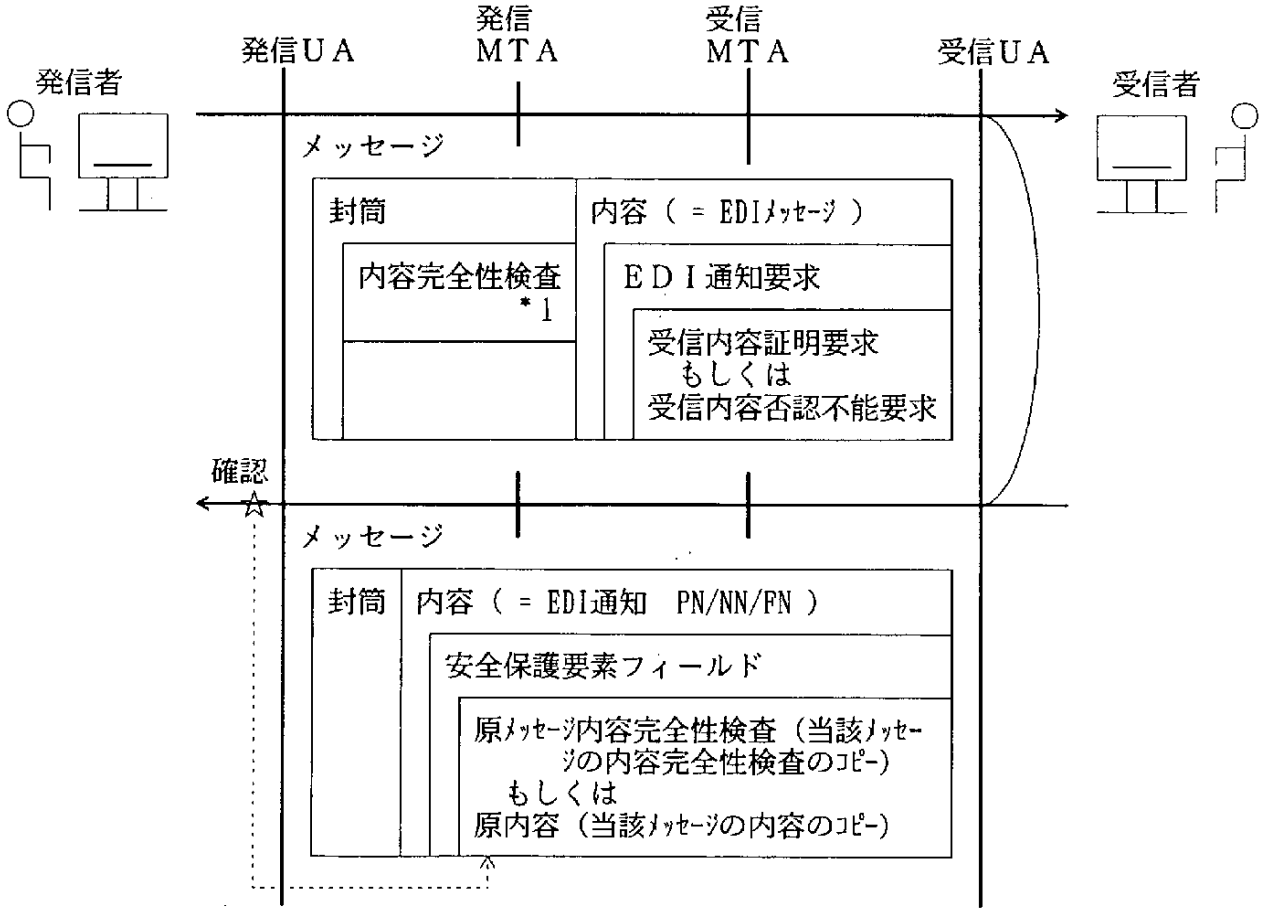


図2.9-13　受信内容証明　／　受信内容否認不能

2. 10 ディレクトリ利用サービス

2. 10. 1 ディレクトリ名による受信者の指定

あて先指定におけるディレクトリの使用には、ＭＴＡがディレクトリを使い指定された受信者の名前を解析する場合と、ＵＡが受信者の指定にディレクトリを使う場合（およびＵＡとＭＴＡの両方が受信者指定にディレクトリを使う場合）が考えられる。ただし、通常、ディレクトリ名からＯ／Ｒアドレスを得る処理は、発信ＭＴＡが行う。

(1) ＭＴＡがディレクトリを使い受信者の指定を名前解析する場合

ＭＴＡは、まずディレクトリに格納された情報を利用して認証を達成し、要求される情報へのアクセス権を得る。その後、受信者のＯ／Ｒアドレスを得るため、ＭＴＡはディレクトリに対して受信者のディレクトリ名を示し、ディレクトリから受信者のＯ／Ｒアドレスを得る。そして、ＵＡはＯ／Ｒアドレス（およびディレクトリ名）を、メッセージ封筒の受信者Ｏ／Ｒ名に指定し、発信を行う。

もし、配信に適切な形態のＯ／Ｒアドレスが見つからなかったり、ディレクトリから得られたＯ／Ｒアドレスが不正であったりした場合は、ＭＴＡよりエラーが返される。

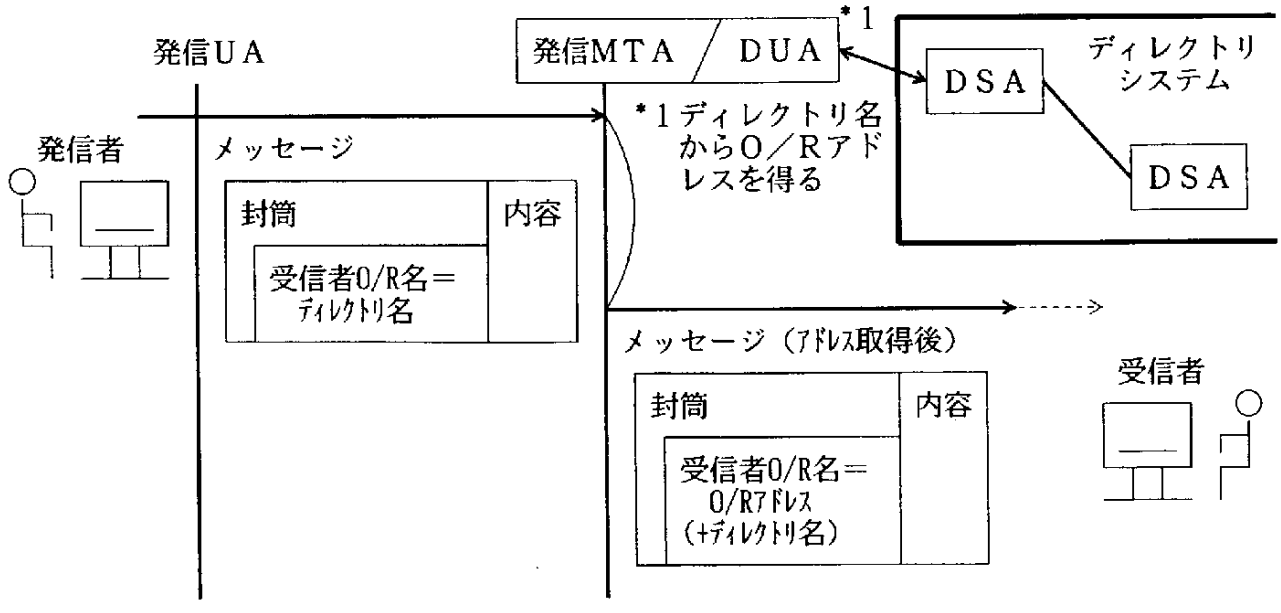


図2. 10-1 ＭＴＡがディレクトリを使い受信者の指定を名前解析

(2) ＵＡがディレクトリ名を使い受信者を指定する場合

ＵＡは、まずディレクトリに格納された情報を利用して認証を達成し、要求される情報へのアクセス権を得る。その後、ディレクトリに対して受信者のディレクトリ名を示し、ディレクトリから受信者のＯ／Ｒアドレスを得る。そして、ＵＡはＯ／Ｒアドレス（およびディレクトリ名）を、メッセージ封筒の受信者Ｏ／Ｒ名に指定し、発信を行う。

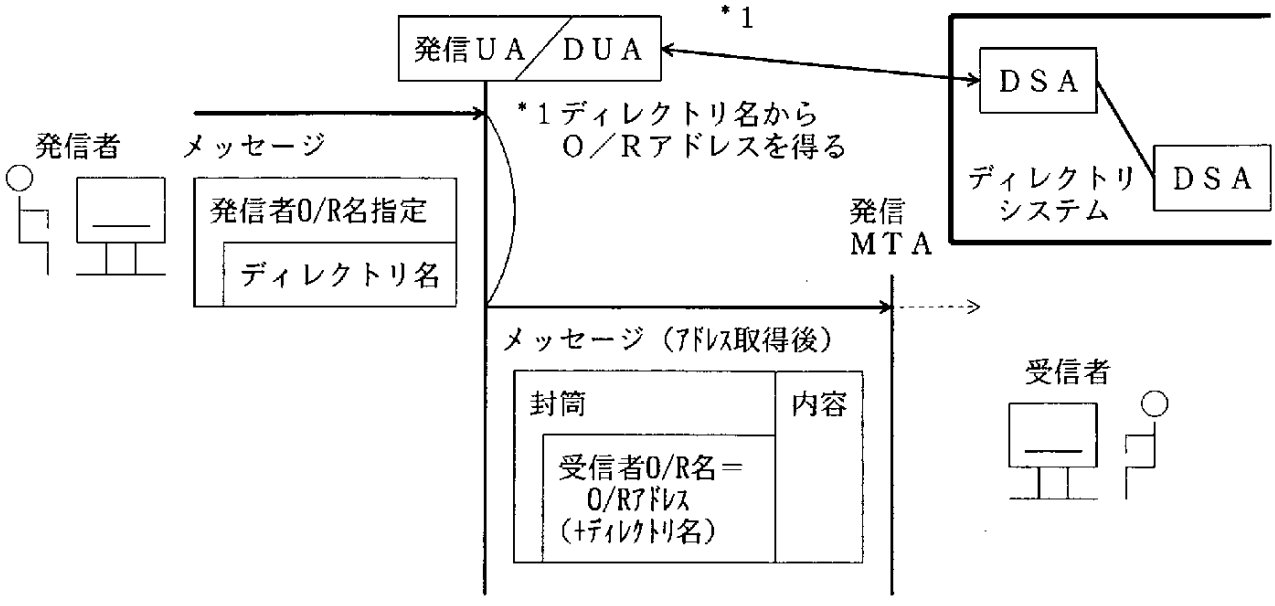


図2.10-2　ＵＡがディレクトリ名を使い受信者を指定

2. 11　物理的配達サービス

物理的配達サービスは、ＭＨＳと既存の郵便サービスのようなシステムとを相互に接続するためのサービスである。

ＭＨＳから他の物理サービス利用者へ発信されたメッセージは物理的配達システム（ＰＤＳ）へのアクセス部（ＰＤＡＵ）を経由して例えば郵便のような形で受信者へ配達される。また配達した結果は物理的配達システムからＭＨＳへ通知される。

物理的配達システムからＭＨＳへのメッセージの発信は規定されていない。

参考：なお物理的配達サービスはＩＮＴＡＰでは規定範囲外となっている。

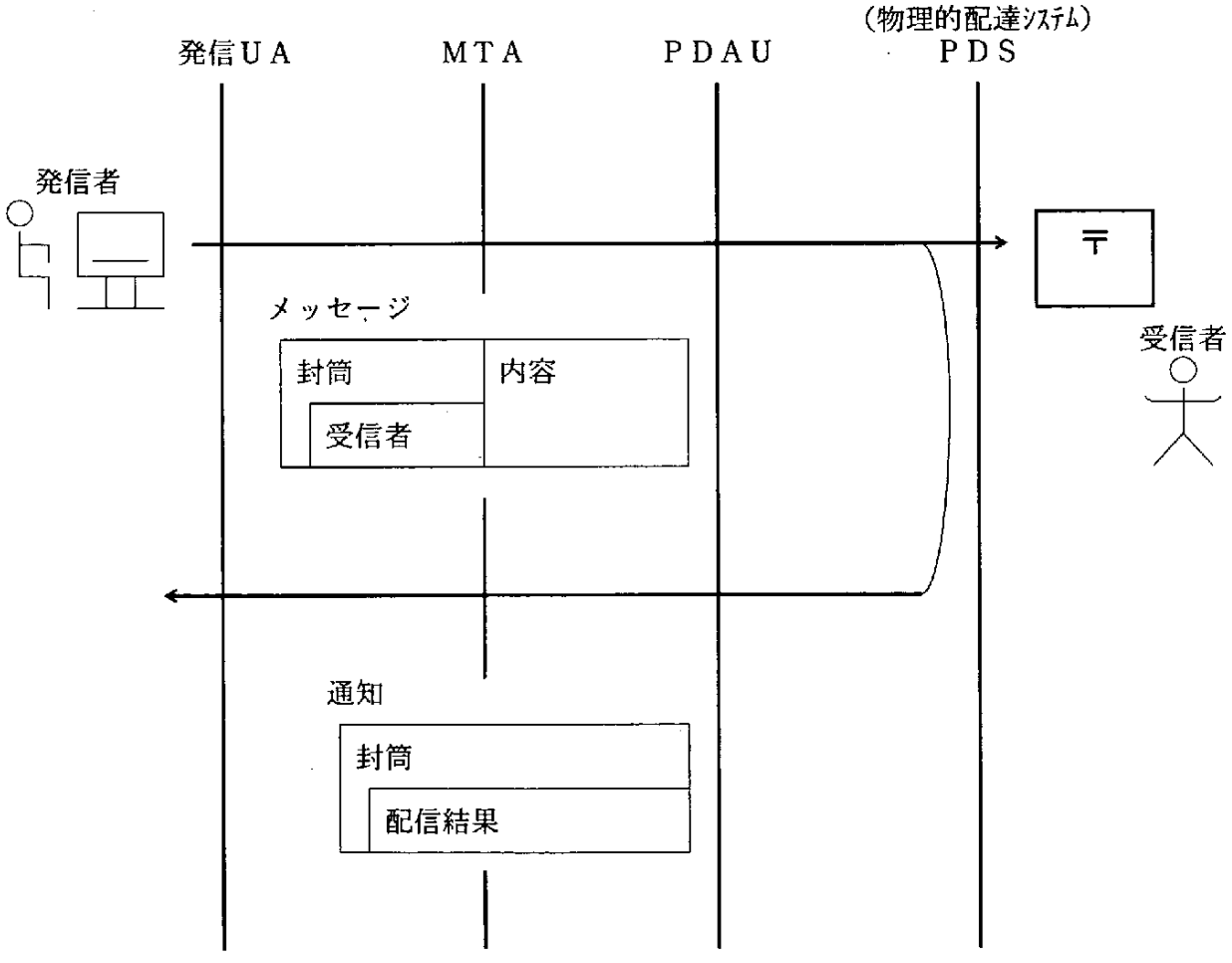


図2.11-１　物理的配達サービス

2. 12　メッセージ格納（MS）サービス

メッセージ格納（MS）は、MHSにおいてメールボックス機能を実現する。MSはMS利用者に一対一に対応しており、主に検索機能を利用者に提供する。

・届いたメッセージを蓄積し、検索機能を提供する。（「2.12.1」～「2.12.6」参照）

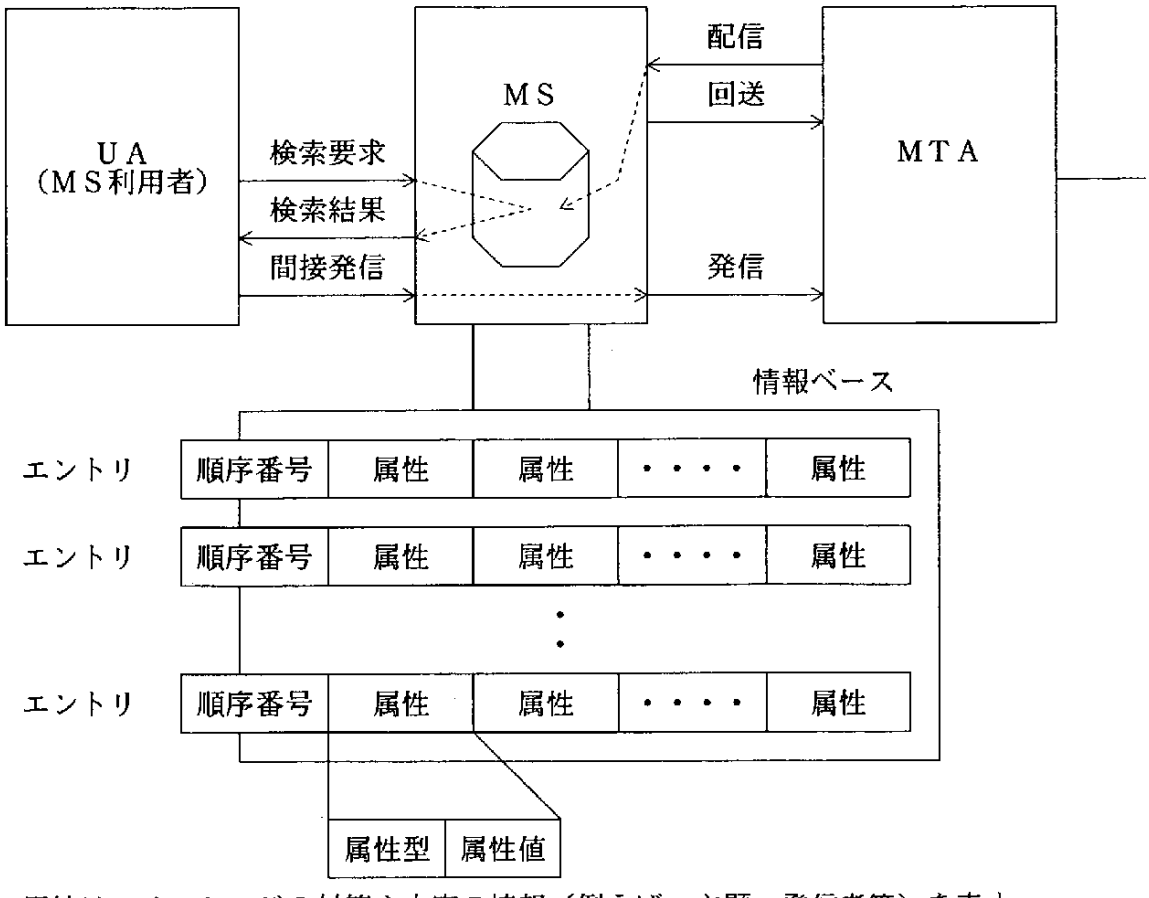
MSは、配信されたメッセージを“エントリ”として“情報ベース（＝メールボックス）”に蓄積する。MSはまた、利用者がエントリを検索するための機能を提供する。

・間接発信

MSは、MS利用者から発信されるメッセージや打診を透過的にMTAに発信する。MS利用者は、MSを意識することなくメッセージ発信、打診発信、遅延配信取り消し等を行うことができる。

・自動回送

MSは、MS利用者があらかじめ登録した条件に従って、自動回送を行う。（「2.12.7」参照）

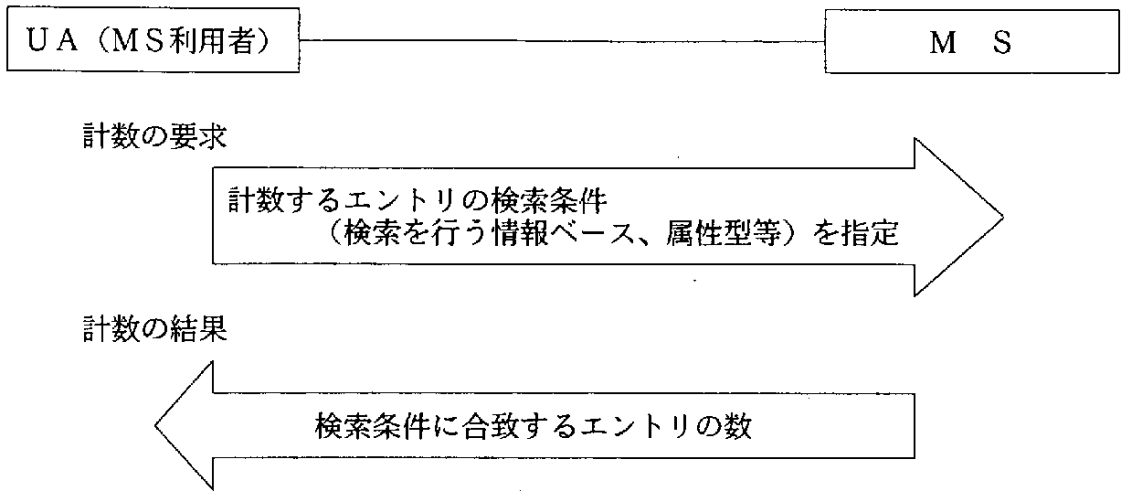


属性は、メッセージの封筒や内容の情報（例えば、主題、発信者等）を表す。
属性型は、それらの情報の種類を表し、属性値は実際の値を表す。
例：属性型　…　“配信優先度”
　　属性値　…　“緊急”、“普通”、“不急”
MS利用者は、検索条件として属性型を指定することができる。

図2.12-1　MSサービスの概念図

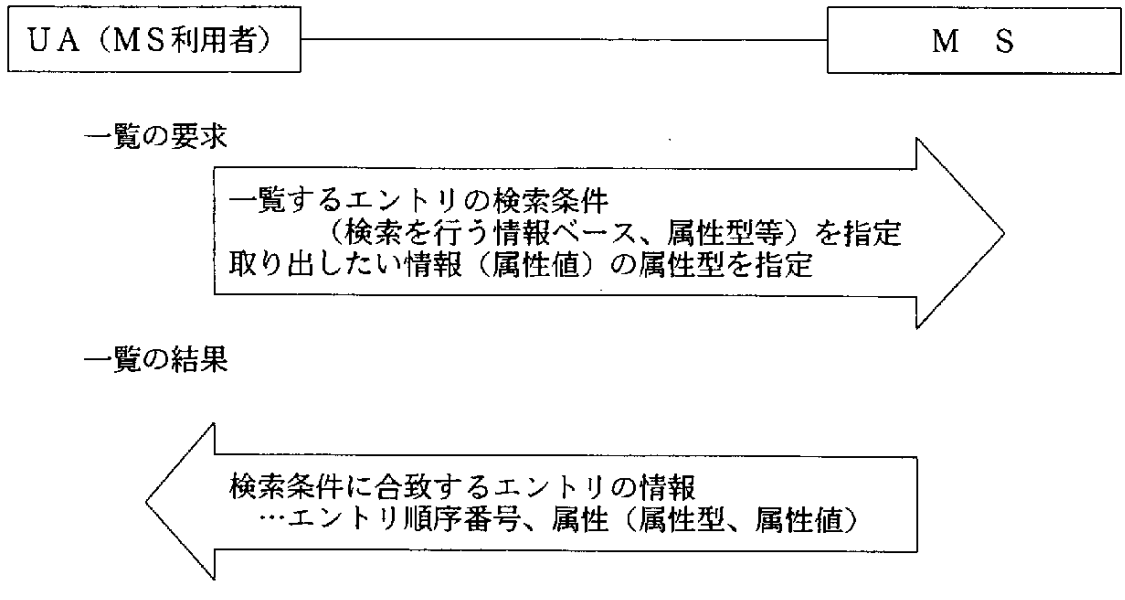
2. 12. 1　計 数

ＭＳ利用者は、計数機能を用いて、指定する検索条件に該当するエントリの数を知ることができる。



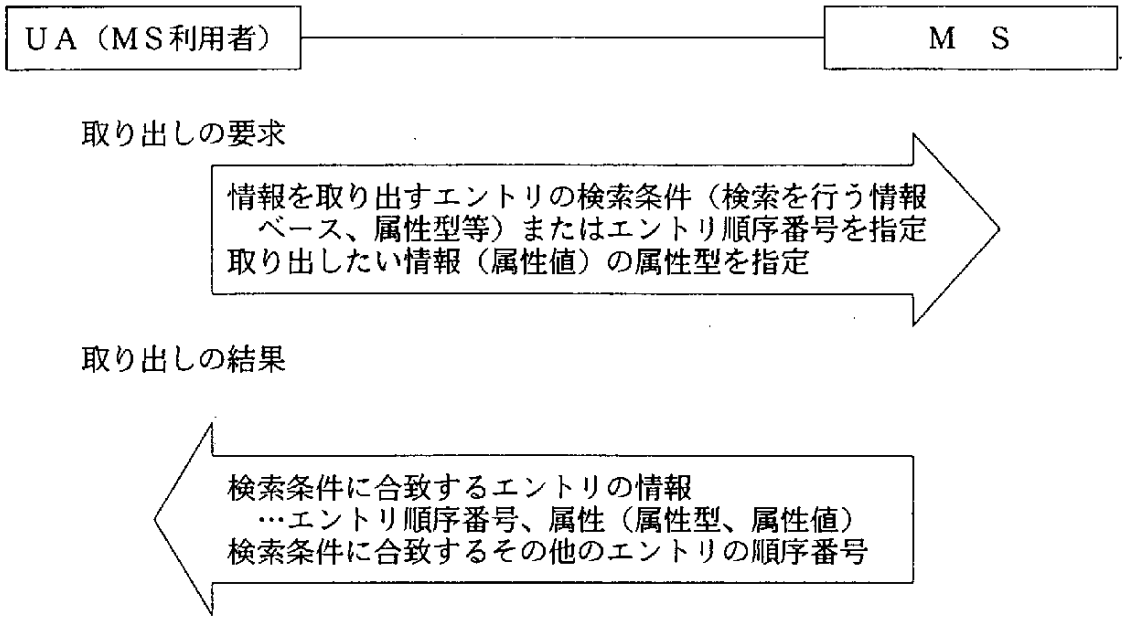
2. 12. 2　一 覧

ＭＳ利用者は、一覧機能を用いて、どのエントリが指定する検索条件に該当するかを知ることができる。さらに、該当するエントリについて必要な情報（主題、発信者名など）を取り出すことができる。ただし、一覧機能では、内容や封筒の全体を取り出すことはできない。（内容や封筒を取り出すには、後述の「取り出し」機能を利用する。）



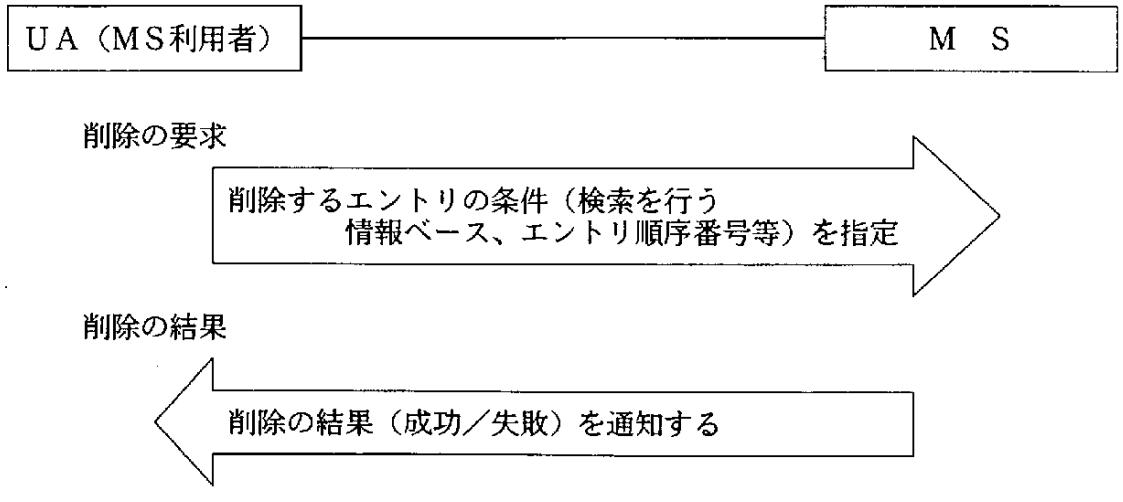
2. 12. 3　取り出し

ＭＳ利用者は、取り出し機能を用いて、指定する検索条件に該当するエントリ、またはエントリ順序番号を指定したエントリの情報を得ることができる。本機能によりＭＳ利用者が取り出すことのできる情報は、内容や封筒である。なお、一回の取り出し要求によって得られる情報は一つのエントリの情報に限られる。



2. 12. 4　削 除

ＭＳ利用者は、削除機能を用いて、指定する検索条件に該当するエントリを情報ベースから削除することができる。ただし削除できるエントリは、それ以前にメッセージの内容や封筒が取り出されている（取り出し）、もしくはそのエントリに対して一覧等の操作がなされているものに限られる。



2. 12. 5　MS登録

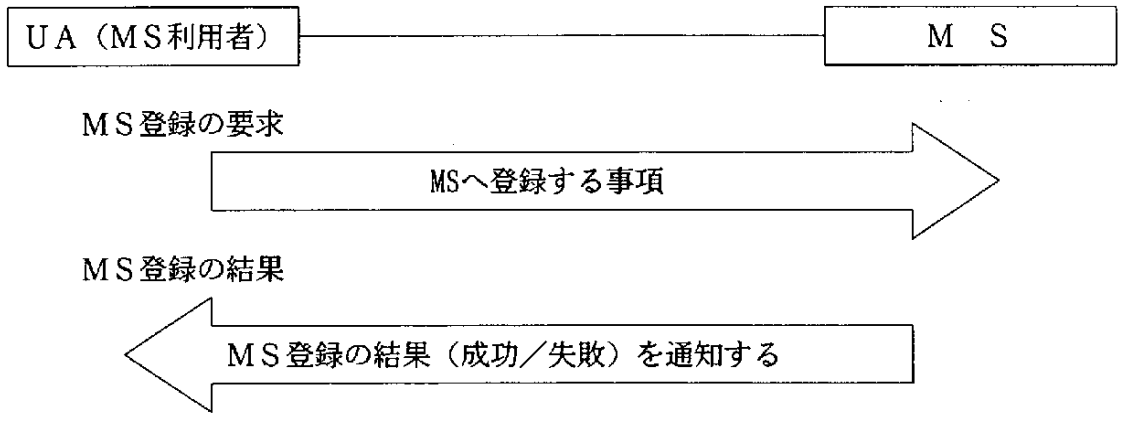
ＭＳ利用者はＭＳ登録を用いて、一覧・取り出しなどの操作における標準値を設定したり資格証明などを変更したりすることができる。具体的には以下の情報を設定できる。

・自動動作登録・登録解除
　警報や回送を行うエントリの条件の登録、変更、登録解除ができる。

・検索要求属性の既定値設定
　一覧や取り出しを行う際の検索要求属性の標準値を、ＭＳに登録することや変更することができる。

・資格証明変更
　パスワードなどの認証情報（ＭＳ利用者がＭＳへアクセスをするために必要なパラメタ）を変更することができる。

・利用者安全保護ラベル変更
　ＭＳ利用者の安全保護情報を変更することができる。



2. 12. 6　警 報

ＭＳ利用者は、警報機能により、ＭＳに新しいメッセージが到着したことを知ることができる。警報機能を利用するためには、ＭＳ利用者はＭＳ登録機能を用いて、警報を望むメッセージの条件をあらかじめＭＳに登録しておく必要がある。警報はＭＳ利用者がＭＳにアクセスしている間にのみ行われるものであり、これによってＭＳ利用者はデータの取り残しをなくすことができる。なお、警報機能を利用しない場合、ＭＳ利用者が新しいメッセージが到着していることを通知されるのは、次回のＭＳ利用開始時である。

2. 12. 7　自動回送

ＭＳは、ＭＳにあらかじめ設定されている条件に合致するメッセージがＭＳに到着した場合、そのメッセージを自動的に回送する。ＭＳが回送を行う条件は、ＭＳ利用者がＭＳ登録を用いて設定する。

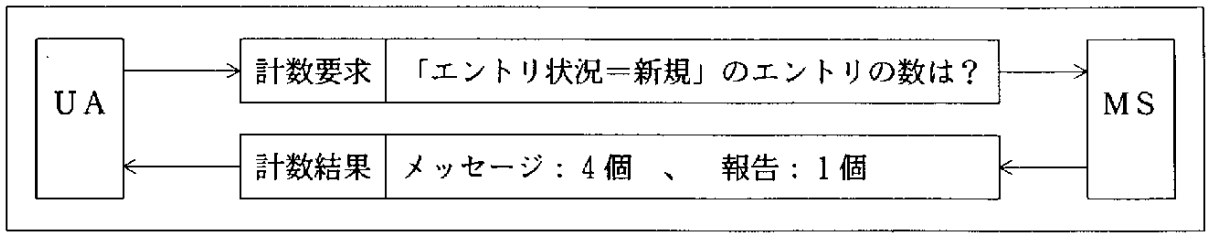
2. 12. 8　MS利用例

ここでは、以下のエントリを含む情報ベースを持つＭＳを仮定し、ＵＡからＭＳへの検索操作の例を挙げる。

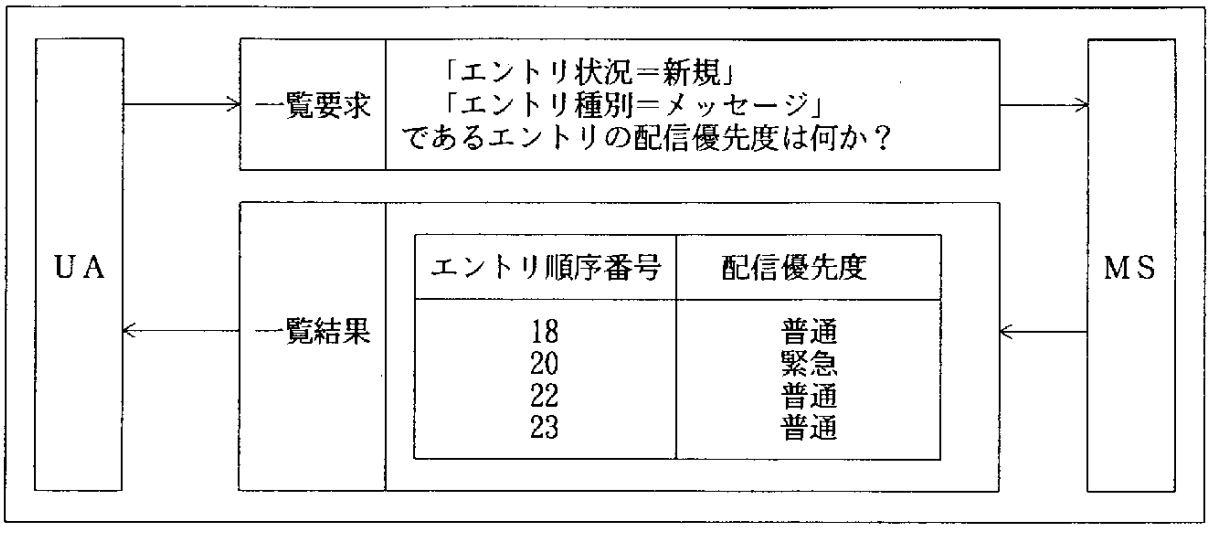
【情報ベース】

エントリ順序番号	エントリ種別	エントリ状況	配信優先度	発信者	本体部
3	メッセージ	一覧済み	緊急	A	EDIFACTデータ
5	メッセージ	一覧済み	不急	B	IA5テキストデータ
8	報告	一覧済み	－	A	－
10	メッセージ	一覧済み	普通	C	EDIFACTデータ
15	報告	新規	－	B	－
18	メッセージ	新規	普通	D	IA5テキストデータ
20	メッセージ	新規	緊急	A	EDIFACTデータ
22	メッセージ	新規	普通	E	EDIFACTデータ
23	メッセージ	新規	普通	F	IA5テキストデータ

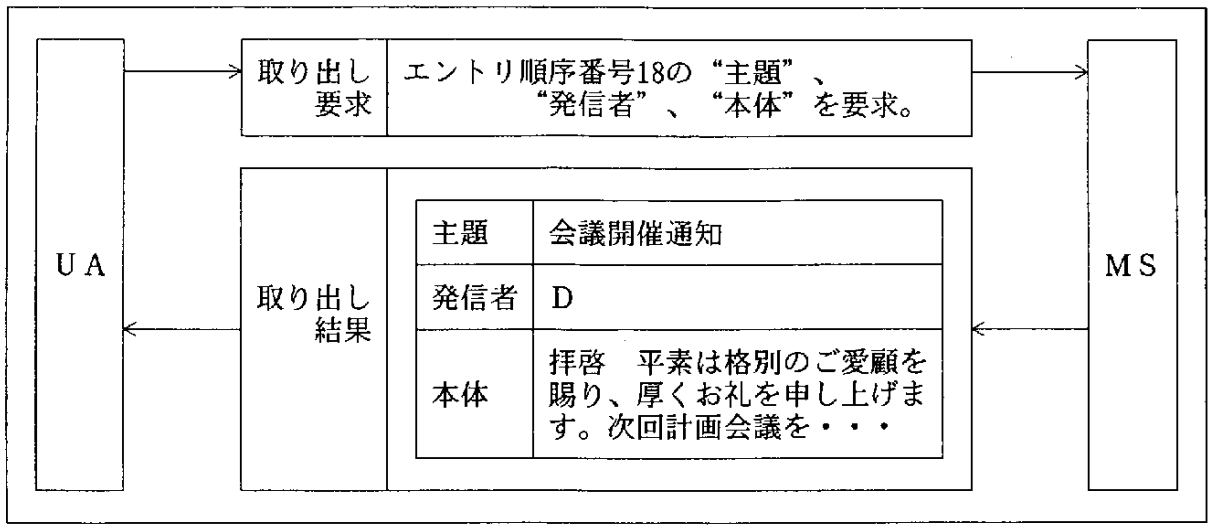
【計数】



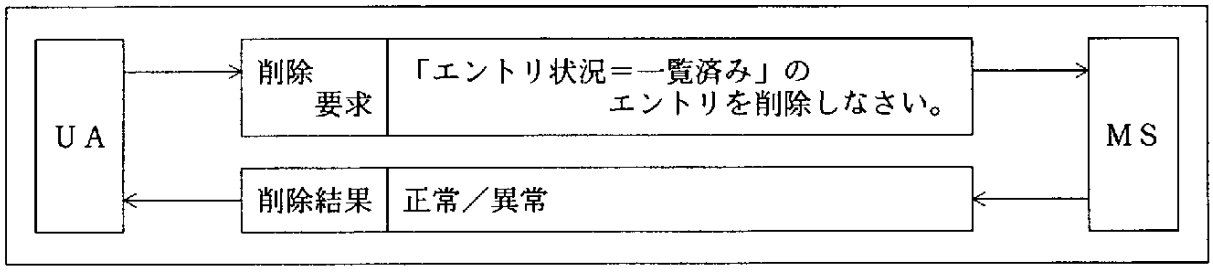
【一覧】



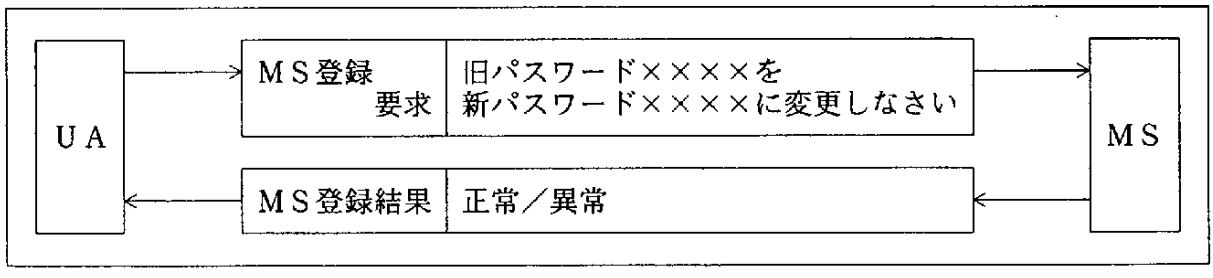
【取り出し】


UA
取り出し要求
エントリ順序番号18の“主題”、“発信者”、“本体”を要求。
MS
取り出し結果
主題
会議開催通知
発信者
D
本体
拝啓　平素は格別のご愛顧を賜り、厚くお礼を申し上げます。次回計画会議を・・・

【削除】


UA
削除要求
「エントリ状況＝一覧済み」のエントリを削除しなさい。
MS
削除結果
正常／異常

【MS登録】


UA
MS登録要求
旧パスワード××××を
新パスワード××××に変更しなさい
MS
MS登録結果
正常／異常

【参考文献】

(1) ITU-T Recommendation X.435(1991)、 Message handling: Electronic data interchange messaging system.

(2) ITU-T Recommendation F.435(1991)、 Message handling: Electronic data interchange messaging service.

(3) ISO 9735 Electronic Data Interchange For Administration , Commerce and Transport (EDIFACT) - Application level syntax rules(1988)

(4) 萩野、INTAP ジャーナルNO.20 、 EDI on MOTIS の解説(1992)

(5) 鈴木、INTAP ジャーナル、 MHS上のEDI について(1994)

(6) 黒田康嗣、菊地浩明「暗号メールFJPEMの公開実験」UNIX MAGAZINE 1994.5、p.118 - 123, アスキー、1994

(7) ISO 7498-2:1987, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

(8) JIS X5004:1991, 開放型システム間相互接続の基本参照モデルー安全保護体系

(9) ISO/IEC 10021-1:1990, Information technology - Open Systems Interconnection - Message-Oriented Text Interchange Systems(MOTIS) Part 1 : System and Overview

(10) ISO/IEC 10021-2:1990, Information technology - Open Systems Interconnection - Message-Oriented Text Interchange Systems(MOTIS) Part 2 : Overall architecture

(11) ISO/IEC 9594-8:1990, Information technology - Open Systems Interconnection - The Directory Part 8: Authentication framework

(12) JIS X5738:1993, 開放型システム間相互接続ーディレクトリー第8部 認証の枠組み

付 録

A. １９９２年版ＭＨＳの追加規定

B. H手順とＰｅｄｉの比較

C. デジタル署名機構

D. 公開鍵暗号化方式

E. メッセージの送受信

F. ＥＤＩＦＡＣＴ標準メッセージ構造

付録Ａ．　１９９２年版ＭＨＳの追加規定

Ｐｅｄｉの基となった１９８８年版ＭＨＳ勧告は、その後も機能拡張が行われ、１９９２年にＩＴＵ－Ｔ勧告として出版された。同様の機能拡張は、ＩＳＯ　１００２１に対しても適宜実施されていく。ここでは、１９９２年版ＭＨＳに追加された事項の中から、次の５点について紹介する。

① ファイル転送
② 音声メッセージ通信
③ メッセージごと通知種別
④ メッセージあて先変更
⑤ O/Rアドレスの視覚化

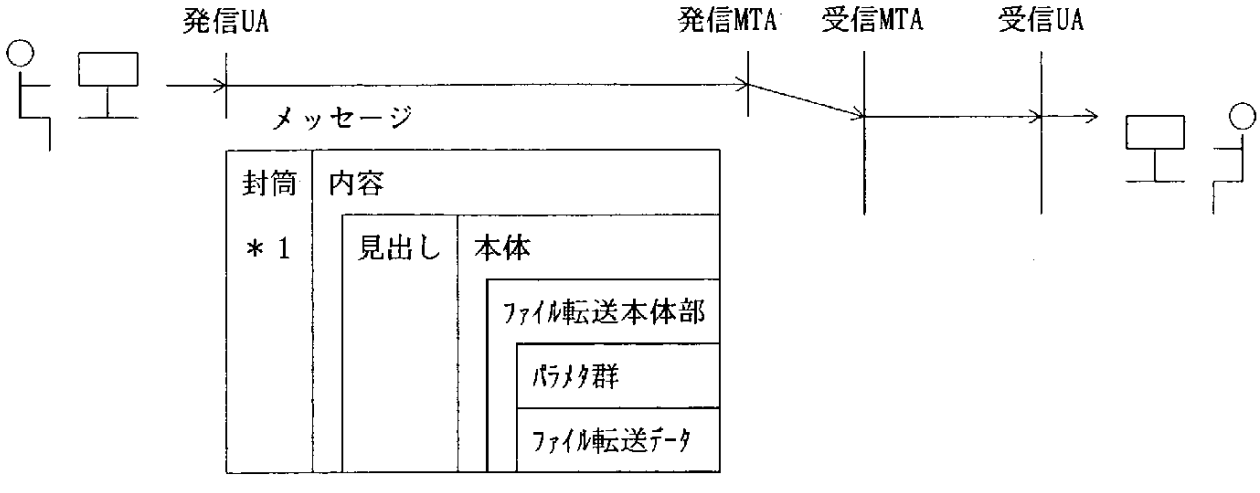
Ａ．１　ファイル転送機能

(1) 概要

ＭＨＳを利用してファイル転送を行うための規定が追加された。具体的には、X.420 に規定される本体部(Body part) の一種として、ファイル転送用の本体部種別が定義されたものである。

ファイル転送本体部種別は、ファイルの内容および属性を運ぶために用い、ISO 8571-2(FTAM)で定義されているファイルモデルに基づく引数（パラメタ）とデータ構造をもつ。ＭＨＳの規定では，FTAMで規定されている文書型のうち、次の３つの型を本体部種別として使用することができる。

① 非構造テキストファイル（FTAM-1）
② 非構造バイナリファイル（FTAM-3）
③ 連続バイナリファイル　（FTAM-4）



注）＊１：符号化情報種別は、オブジェクト識別子（id-eit-file-transfer）を指定する。

付図A.1-１　ＭＨＳを利用したファイル転送サービス

(2) ファイル転送本体部の構成

付表A.1- 1 ファイル転送本体部の要素

パラメタ	概要
ファイル転送パラメタ群 FileTransferParameters	転送するファイルに関する種々の属性。
関連格納済みファイル related-stored file	本体部のファイルと受信者が保持しているファイルとの関係を表す。格納済ファイルは、ファイル名または以前に送信されたＭＨＳメッセージへの参照のいずれかで識別される。
内容種別 contents-type	ファイル内容の抽象データ型と構造情報（ｵﾌﾞｼﾞｪｸﾄ識別子で指定する）。 省略時値は，FTAM-3（非構造ﾊﾞｲﾅﾘ）である。
環境 environment	このファイルを作成した環境（マシン、ＯＳ、アプリケーションなど）。
圧縮 compression	ファイルが圧縮モードで転送される場合の圧縮方式。
ファイル属性群 file-attributes	下記の任意選択のファイル属性を組み合わした値を設定する。 （但し、受信者の動作を保障するものではない。） （ファイル名、許可動作、格納域課金、生成日時、 最終変更日時、最終読出し日時、生成者識別、アクセス制御 法的資格、最終変更者識別、最終読出し者識別、 ファイルサイズ、上限ファイルサイズ、私用、拡張属性 注）上記属性は、FTAM(ISO 8571-2)と技術的に同等である。
拡張群 extensions	上記のパラメタ以外に新たなパラメタを定義するためのフィールド。
ファイル転送データ FileTransferData	転送する情報。

A．2 音声メッセージ通信

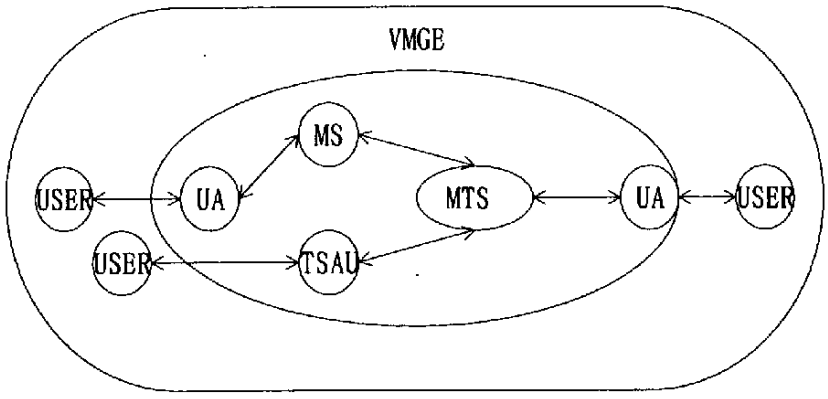
(1) 概要

ファイル転送と同様に、ＭＨＳを利用した音声メッセージの発信、転送、配信および受信を実現する規定が追加された。この音声メッセージ通信の標準化においては、ファイル転送の場合と異なり、音声メッセージを運ぶ本体部種別の規定のほかに、既存の音声メールシステムとのインタフェースの規定、利用者間での受信通知などのために、音声メッセージ通信システムとして一つの勧告が作成された（①X.420 に本体部種別の追加。②X.440 （音声メッセージ通信システム）の勧告化）。

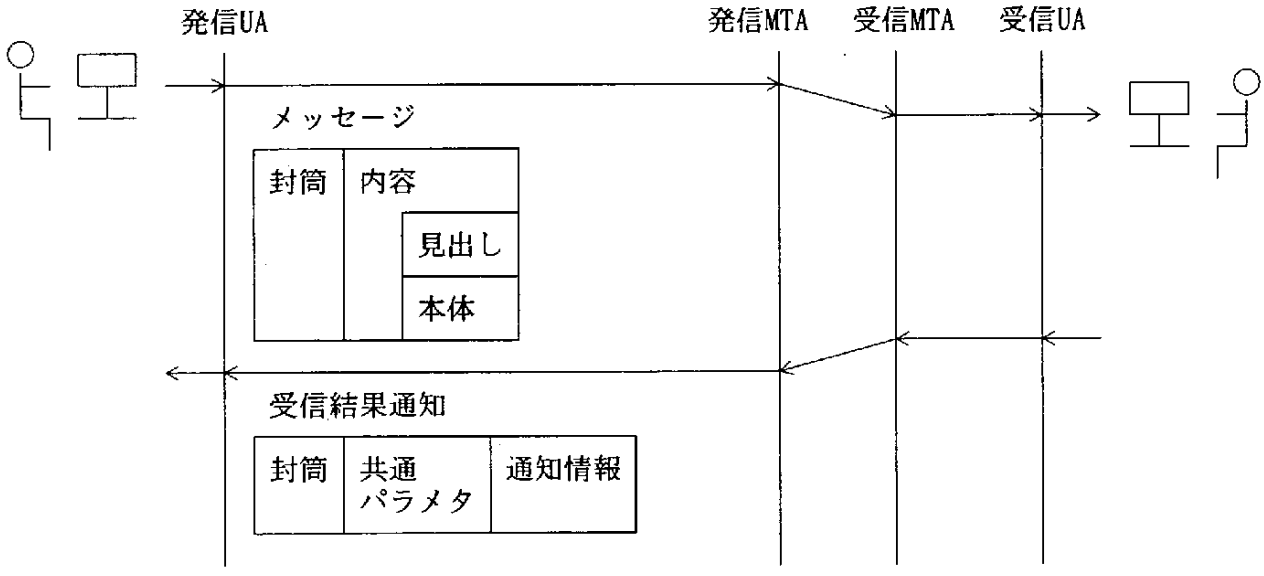
(2) 音声メッセージ通信システム

音声メッセージ通信システムは、Pediと同様の手法で、音声メッセージ通信環境(VMGE)を定義し、MHS 上で音声メッセージを交換するための規定を行ったものである（付図A.2- 1）。また、MHS を使用して転送する情報の形式として、音声メッセージおよび受信結果通知を規定し

ている。さらに、音声メッセージをサポートするMSの機能および属性定義を追加した。



付図A.2- 1　音声メッセージ通信環境



付図A.2- 2　音声メッセージの転送例

(3)　本体部種別の概要

音声メッセージ通信で使用する音声メッセージ（Voice Message:VM）は、勧告G.721(32K ADPCM)等に規定される符号化方式による音声情報、および音声に伴う図形や説明文等の関連情報とからなる（付表A.2- 1）。具体的には、音声情報を格納する主本体部（付表A.2- 1　※1の部分）と関連情報を格納する他本体部（付表A.2- 1　※2の部分）から構成される。

付表A.2-1　音声メッセージの構成

パラメタ	概要
見出し heading	IPM （個人間メッセージ）で定義されている見出しを一部追加・変更したもの（注１）
本体 body	音声メッセージ等を含める本体部
主本体部 primary-body-part （※１）	送信する音声メッセージを含める本体部。 （注２）
本体部 VBodyPart	音声メッセージ本体部。
音声パラメタ VoiceParameters	音声データに関する各種の情報。
voice-message-duration 音声メッセージ持続時間	再生時の所要時間（秒単位）。
voice-encoding-type 音声符号化種別	音声ﾃﾞｰﾀの音声符号化方式を示すオブジェクト識別子。
other-parameters 補足情報	補足情報（音声データの処理に必要な付加情報）。
extension-parameters 拡張パラメタ群	音声データの処理に必要な拡張情報。
VoiceData 音声データ	音声符号化種別の値によって示される方式でデジタル符号化された音声。
他本体部 additional-body-part（※２）	音声以外の付加的な情報を添付する場合に使用する。 （X．４２０で規定される本体部）

注１：例を以下に示す。
　　変更の例：標題⇨音声が格納可能な標題に変更
　　追加の例：音声符号化種別（音声データの符号化方式、32K ADPCM 等）
　　音声メッセージ作成日時
注２：主本体部の内容としては、ここに示した音声メッセージ本体部の他に回送音声メッセージも規定されている。これは、ＥＤＩ回送と同様に音声メッセージが回送された場合の形式であり、ここでは、説明を省略した。

A．3　メッセージごと通知種別

(1)　概要

メッセージ送信時の封筒（MessageSubmissionEnvelope ）に設定するパラメタの一つであるPerMessageIndicator （注釈を参照）に定義を追加したもので、送信するメッセージの内容が一般のメッセージではなく、特定の意味を持った“通知”であることを示すためのものである。

通知の種別（意味）は、取り扱うメッセージの内容に依存するものであり、勧告上は形式的に３種の値（通知１～通知３）を定義しているだけである。このパラメタを使用して、実際に運用する際には、実装ごとにこの値に意味を与える必要がある（サービス方針の決定）。

（注）PerMessageIndicator ：メッセージ単位にサービスを指定するパラメタであり（同報配信時に、あて先単位に要求するサービスではなく、全てのあて先に共通に適用される。）、他受信者名表示、暗黙変換禁止、代行受信者許可、内容返送要求が既に定義されており、９２年版勧告で上記の通知種別が追加された。

(2) ＭＴＡの動作

ＭＴＡでは、この通知の内容によって、サービス方針（管理領域が独自に規定する）に従い、通知種別が正しいかを検証することができる。この通知種別は、あて先として指定された受信者へは渡されず、このパラメタが設定されているメッセージを受信したＭＴＡで処理される。

なお、検証後の動作としては、次の３つの動作が規定されている。

a） 値は無視され、ＭＴＡの処理は成功とする

b） 通知種別は正しい値に設定されており、ＭＴＡの処理を終了する

c） 不正な引数として、配信不能通知を返送する処理を行う

Ａ．４　メッセージあて先変更機能

(1) 概要

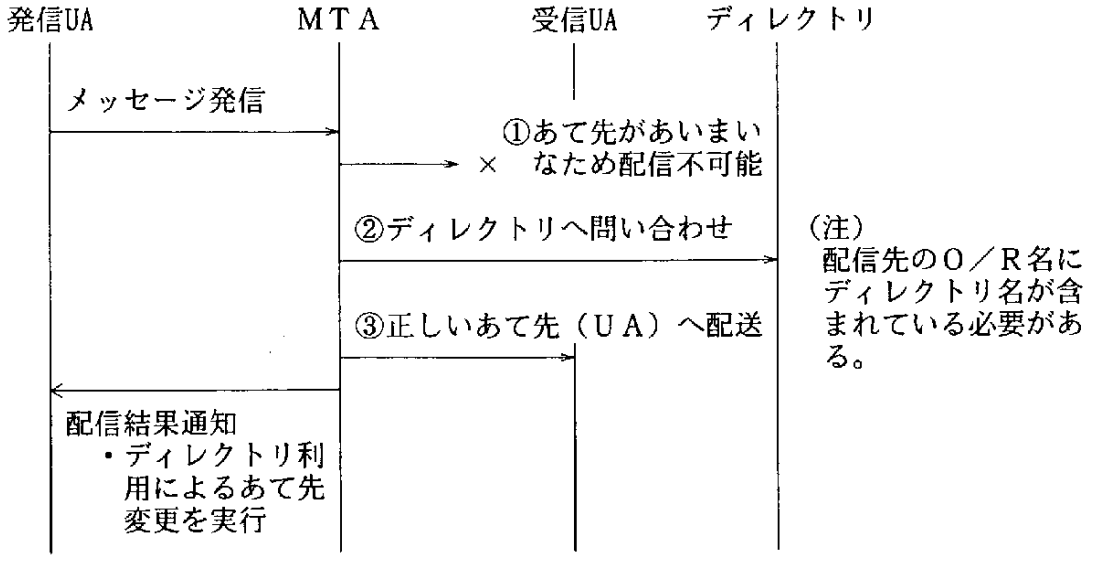
ＭＨＳでは、「２．８　あて先変更サービス」に示したようなあて先変更機能がある。８８年版ＭＨＳでは、あて先変更の方法として、①受信者の指示、②発信者の指示、③受信側管理領域（ＭＤ:Management Domain）の指示、による３種の方法があり、また、発信者へあて先変更の実施の有無を配信通知により知らされる機能が規定されている。これらのあて先変更の方法の他に、発信者が意図した受信者以外にメッセージが配信される条件として、８８年版ＭＨＳから追加されたディレクトリ機能を利用した方法がある。つまり、メッセージ発信の際に、目的の受信者が不明であり（Ｏ／Ｒアドレスの内容が正しくない場合）、かつ、Ｏ／Ｒ名にディレクトリ名が指定されている場合に、ディレクトリの検索機能を利用して正しいＯ／Ｒアドレスを得ることができる。このようにして得られたＯ／Ｒアドレスによって利用者へメッセージを配信することができる。このような機能もあて先変更の一種と見なし、９２年版ＭＨＳでは、配信通知のパラメタの中のあて先変更理由（あて先変更を実施した場合の理由を示すパラメタ）に下記のパラメタ値を追加した。

付表A.4-１　あて先変更理由のパラメタ値

パラメタ値	新規・既存
受信者割当て代行受信者　(0)	既存
発信者要求代行受信者　　(1)	既存
受信ＭＤ割当て代行受信者(2)	既存
受信者ディレクトリ変換代行受信者(3) (recipient-directory-substitute-alternate-recipient)	新規追加

(2) 通信シーケンス

ディレクトリによるあて先変更の通信例を以下に示す。



付図A.4-1 ディレクトリを利用したあて先変更機能

A．5 O／Rアドレスの視覚表現

(1) 概要

多くの属性からなるO／Rアドレス（「1．1．5 アドレスと経路選択」参照）を名刺などに示す場合に、各属性の名称を全て記述すると長すぎるため、その省略型のラベルを規定し、MHSのアドレスの表記方法を統一した。名刺以外の利用としては、電子メールシステムからMHSの利用者を指定する際の利用者インタフェースとして、ここで規定された名称を用いることで、どの電子メールシステムにおいても同一の形式であて先を表示することができる。

このラベルの形式には、(a)1文字で名称を表示し、言語の依存性を低減させる形式（ラベル付き形式）、および、(b)十分な表示部分がある場合の説明付き形式（自己説明付き形式）、の二つを用意した。

(2) 表現形式

（a）ラベル付き形式の例

- O／Rアドレスの個々の属性を示す英字1文字と値の組み合わせで表現する簡易な記述方法である。
- 英字1文字の後に“=”を付与し、その値を記述し、個々の属性を“;”で区切る方法と、英字1文字と値のみを記述する方法がある。

```
X.400: G=john; S=smith; O=a bank ltd; P=ab1; A=snomail; C=aq
```

または

```
G John
S Smith
O A Bank Ltd
P ABL
A Snomail
C AQ
```

省略文字の意味（1.1.5参照）：
G:Given Name（名）
S:SurName(姓)
O:OrgnizationName(組織名)
P:PRMD Name(私設領域名)
A:ADMD Name(主管機関管理領域名)
C:Country Name（国名）

（b）自己説明付き形式

・基本的に属性の名称を一般に理解できる程度に示し、値を記述する方法である。

Given name(G)	John
Surname(S)	Smith
Organisation(O)	A Bank Ltd
Org.Unit(OU1)	IT Dept
Org.Unit(OU2)	MSG Group
PRMD(P)	ABL
ADMD(A)	Snomail
Country(C)	AQ

付録Ｂ．　Ｈ手順とＰｅｄｉの比較

Ｈ手順とＰｅｄｉは同じＭＨＳを利用したＥＤＩ交換用手順（プロトコル）ではあるが、それぞれは開発経緯の違いから、機能面・運用面で次のような相違がある。

Ｈ手順は平成４年３月に流通システム開発センターによって制定された新ＪＣＡ手順であり、それまで電子メール用プロトコルとして利用していたＭＨＳの“Ｐ２”プロトコルフォーマットに、ＪＣＡ手順で規定した標準データ交換フォーマット（以下、ＪＣＡ標準データ交換フォーマットと呼ぶ）をマッピングすることで、ＭＨＳによるＥＤＩ転送を可能としたものである。米国でもＰｅｄｉが規定されるまでは“Ｐ０”方式といったＭＨＳメッセージの内容にＡＮＳＩ　Ｘ．１２交換データをのせてＥＤＩ転送を行っており、Ｈ手順はこれと似た方式を採ったものであり、言わばＥＤＩ交換の現実解的な方式である。

より早い普及を狙いとしているため、ＭＨＳは、現在、国内で多く普及している８４年版Ｐ１，Ｐ２プロトコルに８８年版Ｐ７プロトコルを加えた機能をベースにしている。また現行のＪＣＡ手順からの移行をスムーズにするために、交換データはＪＣＡ標準データ交換フォーマットをそのまま使用可能とし、また二重交換防止，サイクル管理といった運用機能もＪ手順と同様に規定している。

一方、ＰｅｄｉはこうしたＭＨＳのＥＤＩ交換での利用要求に答える形で規定された、言わば理想解的な方式であり、１９９１年のＩＴＵ－Ｔ加速勧告によって規定されたものである。そのためＭＨＳは全て８８年版がベースになっており、転送フォーマットもＥＤＩ転送用に新しく規定された。

交換データはＥＤＩ交換の標準フォーマットであるＥＤＩＦＡＣＴを前提にしているが、その他ＡＮＳＩ　Ｘ．１２やＵＮＴＤＩといった現在普及している交換データへの対応も考慮している。日本においては、ＣＩＩ標準フォーマット，ＪＣＡ標準データ交換フォーマット等を交換データとして採用することも可能である。

ＰｅｄｉはＥＤＩ交換用に規定された分、メッセージの見出しに交換データの一部を格納できたり、転送結果の通知（責任）や転送の方法（回送）に関して明確な規定がある。また、Ｏ／Ｒ名ではディレクトリによる受信者の指定も可能である。しかし、Ｈ手順で定められている運用機能（二重交換防止など）に関してまでは規定されていないが、これらの運用機能は、Ｈ手順と同様、ローカル機能として実現可能である。ただし、「８８年版ＭＨＳ（Ｐｅｄｉも含む）ではメールボックス内に格納されているメッセージを受信者側から削除する機能が必須となっている」が、「Ｈ手順ではＪＣＡでの運用面を考慮し、当該機能の利用を禁止している」という運用機能面での違いはある。

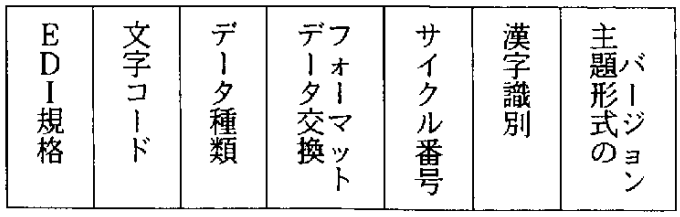
Ｈ手順とＰｅｄｉを比較した場合、ＭＨＳの機能レベルでは８８年版ＭＨＳを使用しているＰｅｄｉの方がセキュリティ面等でより優れているが、日本においてはまだ８８年版ＭＨＳの普及は余り進んでおらず、現時点では、８４年版ＭＨＳを使用するＨ手順の方が移行性・接続性の面では有利と考えられる。

以下に、Ｈ手順とＰｅｄｉについて、ＥＤＩ交換で要求される詳細な機能などの比較を行う。

付表B.1-1　H手順とＰｅｄｉの機能比較

機　能	H手順	Ｐｅｄｉ
データ送受信基本機能	ＭＨＳの基本機能を利用し、Ｐ１プロトコルを用いた同期型のファイル転送形態とＰ７プロトコルを用いた非同期型のクライアントーサーバ形態がある。	同　左
交換データ	ＪＣＡ手順用交換データを使用する。 主題の設定によりＪＣＡ手順以外の交換データを使用することが可能である。 （付図B.1-1，付表B.1-2参照） 交換データの送受信単位は１メッセージ＝１交換データである。 交換データを含むメッセージ中に他の付加情報（図形、文書等）を含めることはできない。	ＥＤＩＦＡＣＴメッセージのほかに、符号化情報種別（ＥＩＴ）の設定によりＡＮＳＩフォーマット等の使用が可能である。 交換データの送受信単位は１メッセージ＝１交換データである。 交換データを含むメッセージ中に他の付加情報（図形、文書等）を含めることができる。
文字コード	既定値としてＪＣＡフォーマットの文字コードであるＥＢＣＤＩＣが規定されているが、主題の文字コード、漢字識別パラメタを使用して利用者間で取り決めることにより、他の文字コード、漢字を使用することができる。	ＥＤＩＦＡＣＴやＡＮＣＩフォーマット毎にＴ６１コードやＩＳＯ６４６、ＥＢＣＤＩＣ等が規定されている。 将来的にＩＳＯ１０６４６コードが使用されるようになれば漢字の使用も可能である。
送受信データ長	ＩＮＴＡＰの規定するＭＨＳによるメッセージの最低保証値３２Ｋを規定している。	現在は、規定されていない。
マルチファイル転送(メッセージ単位)・パスワード認証・リカバリ転送	ＭＨＳの基本機能として実現されている。	同　左
ゼロ件データ転送、通知機能	規定はされてないが、運用上必要となる場合を考慮し、当事者間での調整が必要とした上で「メッセージ中の“主題”及び“本体”に、“発注なし”、“発注遅延”等を示すコードと付加情報をセットしてデータを送る」といったガイドラインを示している。	規定はされてないが、Ｈ手順と同様、ローカル機能として実現可能。
サイクル管理	メッセージ中の“主題”のサイクル番号フィールドを使用して管理するよう規定されている。 （主題の規定については付図B.1-1、付表B.1-2参照）	規定はされてないが、Ｈ手順と同様、ローカル機能として実現可能。
検索機能・転送状態問い合わせ	ＭＨＳ　Ｐ７プロトコルを使用した形態で基本機能として実現されている。	同　左
二重交換防止	Ｐ１プロトコル形態では主題中にサイクル番号を設定して管理するよう規定している。 Ｐ７プロトコル形態では検索時の条件指定や読みだしメッセージの即時削除による実現性を規定している。	規定はされてないが、Ｈ手順と同様、ローカル機能として実現可能。
処理履歴管理	送信データに関する情報（データ件数、データ識別子、送信相手、配信／受信結果等）、受信データに関する情報（受信件数、受信日時等）をロギング情報として採取するよう規定されている。	規定はされてないが、Ｈ手順と同様、ローカル機能として実現可能。
端末からのメッセージ削除	メールボックス内に格納されているメッセージに対する端末からの削除禁止。	削除可能。
複式本体	規定なし。	規定あり。
障害／再送処理	メッセージ単位の再送を行うよう、規定されている。	規定されていない。
送達確認	配信結果確認、受信結果通知の２種類の確認方法を規定している。 受信結果通知の方がより精度の高い確認が得られるがこの機能はオプションになっている。	配信結果確認に加えて、受信結果通知に相当するＥＤＩ通知メッセージによって確認を行う。
利用者名（Ｏ／Ｒ名）	Ｈ手順用Ｏ／Ｒアドレス形式を規定している（付表B.1-3参照）。	特に規定はなく、ＭＨＳで使用可能なＯ／Ｒ名形式を任意に使用する。
責任と回送	――	ＥＤＩメッセージの回送を考慮し、回送した場合の責任とＥＤＩ通知の対応を明確に規定している。
適用回線	専用線、ＩＮＳ－Ｐ、ＩＮＳ－Ｃ	規定されていない。
その他の運用規定	「端末－端末間のデータ交換禁止」、「端末からのメッセージ取り出しは１回のみ」等が規定。	――

（注）「データ転送強制中断」、「データ圧縮機能」、「転送許可時間指定」、「プライオリティ制御」などの機能は、Ｈ手順・Ｐｅｄｉ共に規定されていない。



付図B.1- 1　主題フォーマット

付表B.1- 2(1)　主題パラメタ詳細

パラメータ名	識別子	クラス（注1）	データ型	意味・値
EDI規格	EDI	M	ｵﾌﾞｼﾞｪｸﾄID（注3）	・使用するＥＤＩ規格を示す ・ＥＤＩ規格は、JIPDECへ申請／登録されたｵﾌﾞｼﾞｪｸﾄ識別子を指定する。 ・ＥＤＩ規格は、Ｈ手順対応ｼｽﾃﾑにおいて一意に設定される値であり、ｼｽﾃﾑ間で合意されるものである。 ・ＥＤＩ規格により、データ交換である事を認識する事ができ、一般電子メール（ﾃｷｽﾄ等）との区別を行うことが可能となる。 ・省略不可。（注2）
文字ｺｰﾄﾞ	CHAR	M	ｵﾌﾞｼﾞｪｸﾄID（注3）	・EDI規格で使用する文字ｺｰﾄﾞを示す。 ・Ｊ手順と同じデータ交換ﾌｫｰﾏｯﾄを使用する場合には、識別子(CHAR)から省略する事によりデフォルト値のEBCDICが暗に認識される。 ・他のデータ交換ﾌｫｰﾏｯﾄ（ＥＤＩｼﾝﾀｯｸｽﾙｰﾙ)では複数または任意の文字コードを許容しているものもあるため、EBCDIC以外でデータ交換を行う場合、その文字コードを指定しｴﾝﾄﾞｰｴﾝﾄﾞ間で認識を行う。 ・省略可。（注2）
ﾃﾞｰﾀ種類	TYP	M	数字4桁 0000～9999	・Ｈ手順における伝送ﾃﾞｰﾀの識別を示す。 ・ﾃﾞｰﾀの種類は、 0001　→　受発注情報 0011　→　請求情報 0012　→　支払情報 の三種類が現在JCAで規定されている。 ・0001～0020はＨ手順のﾘｻﾞｰﾌﾞ値である。 ・Ｊ手順と同じデータ換ﾌｫｰﾏｯﾄを使用する場合はＪ手順制御電文でのデータ種類に対応する。 ・省略不可。（注2）
ﾃﾞｰﾀ交換ﾌｫｰﾏｯﾄ	FMT	M	数字4桁 0000～9999	・データ交換ﾌｫｰﾏｯﾄ（ﾌｧｲﾙﾚｲｱｳﾄ)の番号を示す。 ・どのデータ交換ﾌｫｰﾏｯﾄ（ﾌｧｲﾙﾚｲｱｳﾄ)で送受信を行っているかを示し、Ｊ手順と同じデータ交換ﾌｫｰﾏｯﾄを使用する場合には0001を指定する。 ・0001～4999はＨ手順のﾘｻﾞｰﾌﾞ値である。 ・省略不可。（注2）

付表B.1- 2(2)　主題パラメタ詳細（続き）

パラメータ名	識別子	クラス	データ型	意味・値
ｻｲｸﾙ番号	CYN	M	数字12桁 YYMMDDhhmm99	・ｻｲｸﾙ日付を指定する場合は、ｱﾌﾟﾘｹｰｼｮﾝのデータ作成日付時分を西暦で指定する。（"YY"は下2桁） 送信実行時の日付時分は設定しない。 ・ｻｲｸﾙ順序は、O／Rｱﾄﾞﾚｽ、データ種類、データ交換ﾌｫｰﾏｯﾄ単位での伝送順番を示し、01から昇順で採番する。 ・ｻｲｸﾙ番号は、優先度（普通、不急、至急）制御があるため受信時は、昇順ﾁｪｯｸを行わない。 ・ｻｲｸﾙ番号の利用ﾊﾟﾀｰﾝ 採番単位：O／Rｱﾄﾞﾚｽ、データ種類、データ交交換ﾌｫｰﾏｯﾄ ①YYMMDDhhmm01～99 日付時分+連番でｻｲｸﾙ管理 ②000000000001～99 下2桁でｻｲｸﾙ管理(連番) ③000000000000 ｻｲｸﾙ管理なし ④YYMMDDhhmm00 日付時分でｻｲｸﾙ管理 ・省略不可。(注2)
漢字識別	KNJ	O	ｵﾌﾞｼﾞｪｸﾄID (注3)	・データ交換ﾌｫｰﾏｯﾄの中で、漢字を使用している場合のｺｰﾄﾞ種別を示す。 ・J手順と同じデータ交換ﾌｫｰﾏｯﾄを使用する場合には、識別子(KNJ) から省略して使用する。 ・運用上、ﾛｰｶﾙな漢字識別を使用する場合は、その漢字識別を設定し、エンドーエンド間で認識を行う。 ・省略可。(注2)
主題形式のﾊﾞｰｼﾞｮﾝ	VER	M	数字2桁 00～99	・主題形式のﾊﾞｰｼﾞｮﾝを示す。 ・本主題形式のﾊﾞｰｼﾞｮﾝは,01である。 ・省略不可。(注2)

注１）M：指定が必須。ﾃﾞﾌｫﾙﾄ値(文字ｺｰﾄﾞ)を使用する場合は、識別子から省略を行う。
　　O：指定は任意。使用しない場合は、識別子から省略を行う。
注２）省略可　：ﾊﾟﾗﾒﾀとして省略が可能なものを指す。
　　ｸﾗｽが"O"のものまたはｸﾗｽが"M"でﾃﾞﾌｫﾙﾄ値(文字ｺｰﾄﾞ)を使用できるもの。
　　省略不可：ﾊﾟﾗﾒﾀとして省略不可のものを指す。
　　ｸﾗｽが"M"のもの。
注３）桁数の表示されていないﾊﾟﾗﾒﾀに関しては、ｲﾝﾌﾟﾘﾒﾝﾄﾏﾀｰとする。

付表B.1-3　ORアドレスの付与方法

	センター側ホストコンピュータのORアドレス	端末側ホストコンピュータのORアドレス
国　名	“ＪＰ”	同　左
ＡＤＭＤ名	１コのスペース	同　左
ＰＲＭＤ名	センター側企業の名称 英字１６文字以内	収容されているホストの名称 ［センター側ホストコンピュータの名称 端末側ホストコンピュータの名称］ 英字１６文字以内
組織名	センタの電話番号　数字15桁	取引先の電話番号　数字15桁
個人名	リザーブ	同　左
部門名	リザーブ	同　左
領域定義属性	リザーブ	同　左

付録Ｃ．　デジタル署名機構

デジタル署名は、否認不能または認証のような安全保護サービスを提供している。

デジタル署名機構では、非対称暗号化アルゴリズムを使用する必要がある。それは、以下のことを必要とするからである。

・署名されたデータ単位は、秘密鍵の所有者以外は作成できない

・受信側は、署名されたデータ単位を作成できない

署名機構において最も重要な特色は、署名者の私的情報を使用しなければ署名が行えないことである。したがって、署名が確認されると、私的情報の唯一の所有者が署名を行ったことの証明を第三者（例えば、裁判所または調停機関）にいつでも示すことができる。

また、信頼できる第三者（調停者）が、扱われている情報の素性と完全性を立証することにより、以下の特性も提供される。

・発信元は、署名されたデータ単位の発信を否定できない

デジタル署名機構では、次の二段階の手順を定義する。

① データ単位に署名を行う。

この処理では、署名者の私的な（つまり、署名者にとって唯一のかつ秘密の）情報を使用し、上述の署名者の私的情報を秘密鍵として、データ単位の暗号化またはデータ単位の暗号検査値作成を行う。

② 署名されたデータ単位を確認する。

この処理では、公開された手順等を使用し、署名者の私的情報によって署名が行われたかどうかの判定を行う。しかし、そこから署名者の私的な情報を導きだすことはできない。

以下に、ＰＫＣＳ（Public Key Cryptosystem:公開鍵暗号システム）を使用したデジタル署名における発信側（署名者）および受信側の処理の例を示す。詳細は、ISO 7498-2およびISO 9594-8を参照されたい。

C. 1　ＰＫＣＳ（公開鍵暗号システム）を使用したデジタル署名の例

以下の例示においては、付表C.1- 1に示す記法および以下の用語や略語を用いる。

付表C.1- 1　記　　法

表記法	意　　味
Ｘｐ	利用者Ｘの公開鍵
Ｘｓ	利用者Ｘの秘密鍵
Ｘｐ[I]	利用者Ｘの公開鍵による情報Ｉの暗号化
Ｘｓ[I]	利用者Ｘの秘密鍵による情報Ｉの暗号化
Ｘ[I]	利用者Ｘによる情報Ｉの署名。暗号化した要約をＩに付加したもの
ｈ[I]	利用者Ｘの情報Ｉにハッシュ関数を適用

ハッシュ関数……大きな定義域から小さな値域に値を写像する関数。定義域上の値にこの関数が適用されたとき、結果が値域全体に均等に、かつ無作為に分散するものがよい。

一方向性関数……数学的関数ｆにおいて、計算は容易だが、値域内の一般的な値ｙに対してｆ（ｘ）＝ｙとなるような定義域内の値Ｘを見つけることが計算上困難なもの。幾つかの値ｙに関しては、値ｘを見つけるのが容易な場合もある。

ＣＡ……証明機関(Certification Authority)。情報の発信元、情報の完全性、情報の発信／受信時刻、等二つのエンティティ間で交換される情報を保証（保証が必要ならば）する。

ＰＫＣＳ……公開鍵暗号システム(Public Key Cryptosystem)。「付録Ｄ．公開鍵暗号化方式」を参照。

C. 1. 1　署名データの作成

情報(Info)の署名は、情報にその暗号化された要約を追加することによって行われる。要約は一方向性ハッシュ関数により生成され、暗号化は署名者の秘密鍵を使って生成される（付図C.1-1)。

Ｘ｛Info｝＝ Info, Xs[h(Info)]

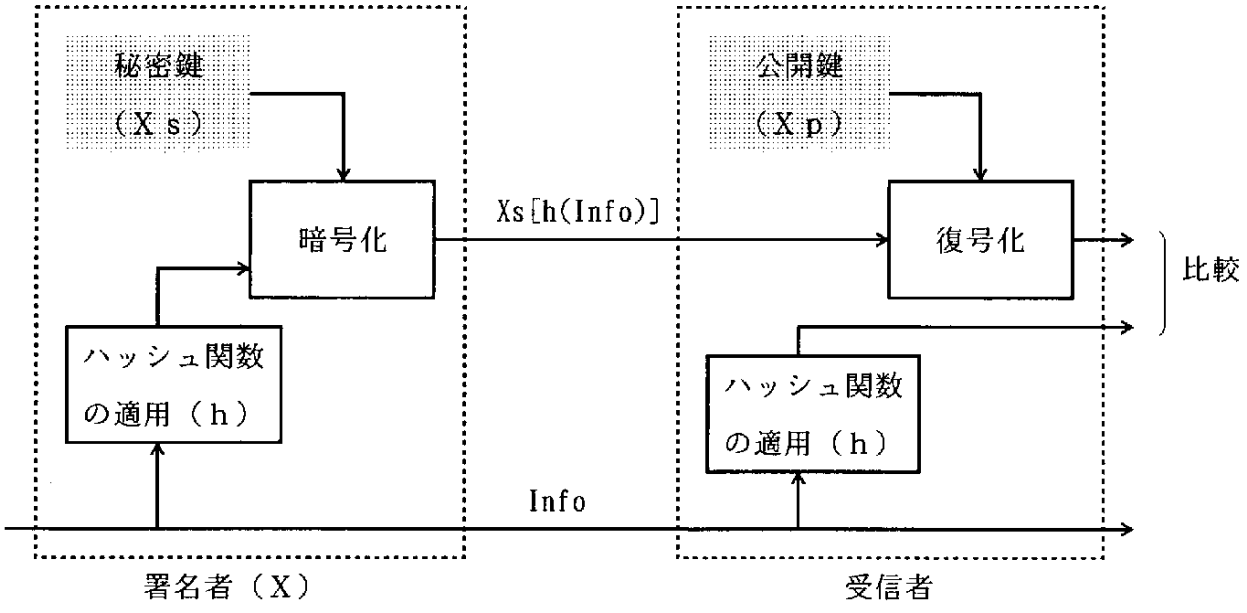
（備考）　秘密鍵を使った暗号化によって、署名のねつ造による詐称を防止できる。

C. 1. 2　署名データの確認

情報の受信者は、次の方法で署名を確認する。

① 情報に一方向性ハッシュ関数を適用する。

② この結果と、署名者の公開鍵を使って署名を復号することによって得た結果とを比較する。



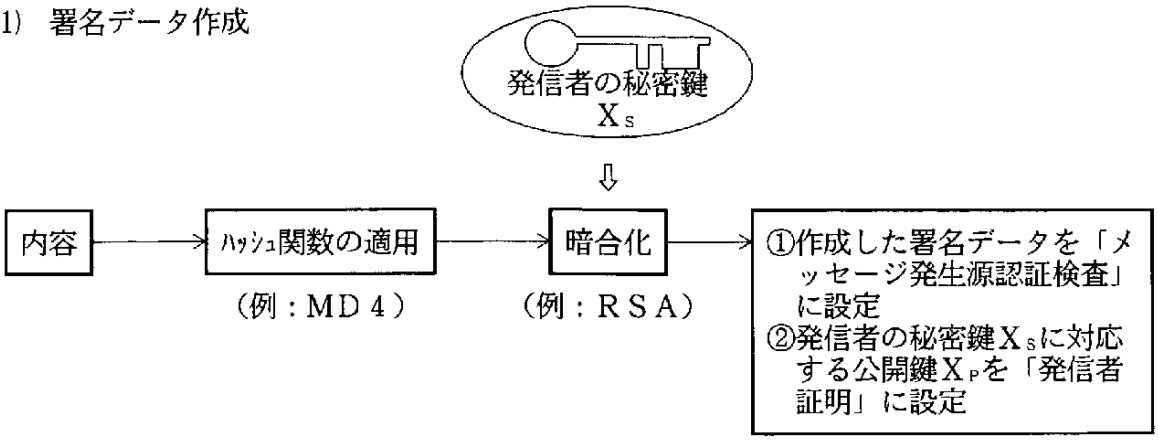
付図C. 1- 1　デジタル署名

C. 1. 3　署名データの利用例

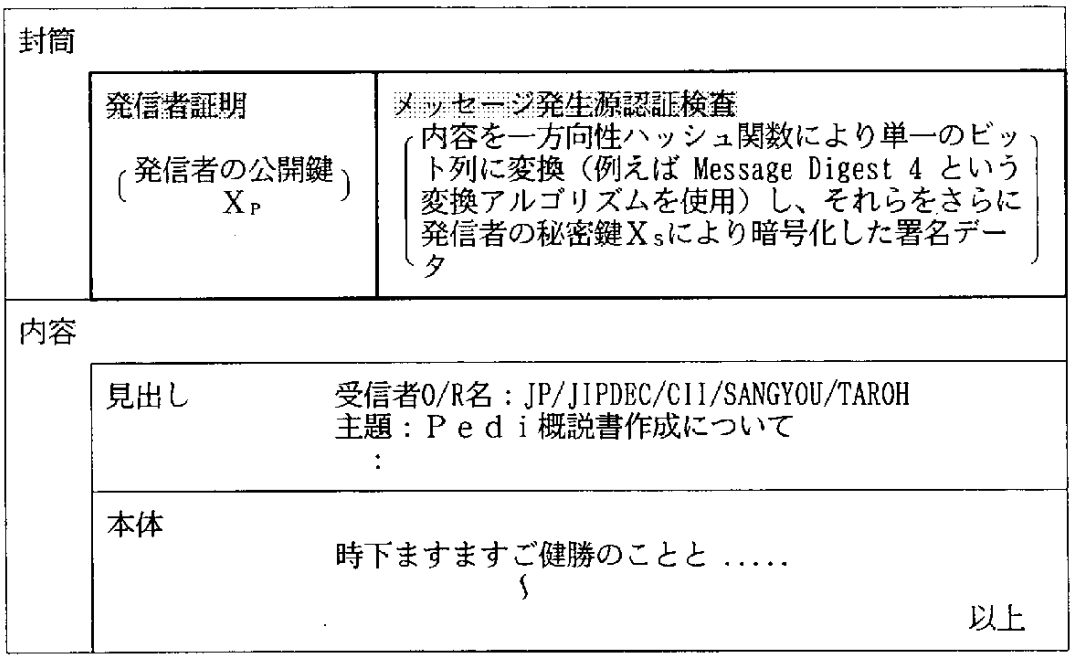
本書の第２章で説明したＰｅｄｉサービスにおいてもデジタル署名を利用したサービスがいくつかある。

その中で説明した「2.9.7 発生源の否認不能」サービスを例に挙げ、付図C. 1- 1にて示した署名データの作成と確認について説明する。

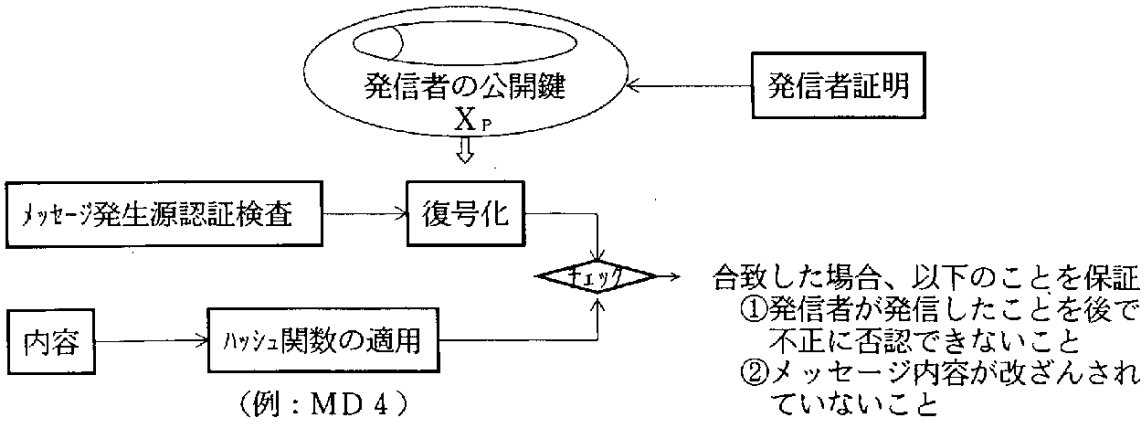
(1) 署名データ作成



メッセージ



(2) 署名データ確認



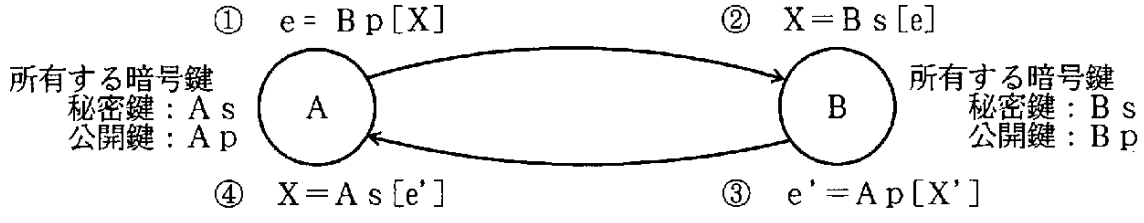
付録D.　公開鍵暗号化方式

データまたはトラフィックフロー情報の機密を保護する技術の一つに、暗号化技術がある。暗号化アルゴリズムは、非可逆の場合と可逆の場合がある。非可逆の場合、暗号化に対応する復号化の処理ができない。認証に利用される暗号化では可逆の暗号化アルゴリズムが使用される。可逆の暗号化アルゴリズムは、一般的に次の二つに分類される。

・対称暗号（すなわち秘密鍵暗号）
　暗号化鍵の情報には復号鍵に関する情報も含まれる。その逆も同様。
　つまり、秘密メッセージの発信元が情報を暗号化するために利用する鍵と、正当な受信者がメッセージを復号化するために使用する鍵が同一である。
・非対称暗号（すなわち公開鍵暗号）
　暗号化鍵の情報には復号鍵に関する情報は含まれない。その逆も同様。
　つまり、秘密メッセージの発信元が情報を暗号化するために利用する鍵と、正当な受信者がメッセージを復号化するために使用する鍵が異なる。

公開鍵暗号システム（ＰＫＣＳ:Public Key Cryptosystem）では、二つの鍵が対で使用され、一方が暗号化のために、他方が復号化のために使用される。そして、利用者ごとに個別の鍵対が関連づけられており、暗号化のための鍵は「公開鍵（Ｘｐ）」として開示されているが、復号化のための鍵は「秘密鍵（Ｘｓ）」として利用者毎に秘匿されている。任意の利用者は公知となっている公開鍵を使ってデータを暗号化できるが、公開鍵を使って暗号化されたデータを復号化できるのは、暗号化に使用された公開鍵に対応づけられる秘密鍵の利用者だけである。

ここで、Ｄ＝Xs[Xp[D]]との表記は「公開鍵を使って暗号化されたデータを秘密鍵を使って復号化したものが、元のデータに等しい」ことを示している。どの利用者も、情報をＸｐで暗号化することにより、秘密鍵Ｘｓの所有者だけに判るように通信できる。これを用いれば二人の利用者は、相互に相手の公開鍵を使ってデータを暗号化することによって、付図D.1- 1に示すように、秘密に通信できる。



付図D.1- 1　ＰＫＣＳを利用した秘密情報の交換

利用者Ａは公開鍵Ａｐと秘密鍵Ａｓとを持ち、利用者Ｂは別の鍵対ＢｐとＢｓを持つ。ＡとＢは相互に相手の公開鍵を知っているが、秘密鍵は知らない。そこでＡとＢは、次に示す手順によって相互に秘密情報を交換する。

① Aは、秘密情報XをBに送信したい。そこでAは、XをBの公開された暗号鍵を使って暗号化し、暗号化した情報をBに送る。これは、次のように表される。

$$e = Bp[X]$$

② Bは、秘密の復号鍵Bsを使ってeを復号化し情報Xを得る。Bは、Bsの唯一の所有者であり、この鍵が開示または送信されることはないので、ほかの利用者が情報Xを得ることは不可能である。Bsを所有しているか否かにより、Bは一意に決定されうる。復号の操作は、次のように表される。

$$X = Bs[e]、または、X = Bs[Bp[X]]$$

③ 同様にBは、秘密情報X'を、Aの公開された暗号鍵Apを用いて暗号化し、暗号化した情報をAに送ることができる。

$$e' = Ap[X']$$

④ Aは、秘密の復号鍵Asを使ってe'を復号化し情報X'を得る。

$$X' = As[e']、または、X' = As[Ap[X']]$$

この方法により、AとBは、秘密情報のXおよびX'を交換できる。この情報は、AとBの秘密鍵が漏洩しないかぎり、AとBとを除くいかなる利用者も知ることはできない。

このような交換は、利用者間の秘密情報の転送だけではなく、利用者の識別の検証にも利用できる。具体的には、AとBは、秘密の復号鍵（AsとBs）の所有によって識別される。Aは、BがAの情報Xの一部をBのメッセージX'の中で返すことにより、通信相手が秘密の復号鍵Bsを所有していると判断できることから、通信相手がBであることを検証できる。同様にしてBもAの識別を検証できる。

一部のＰＫＣＳでは、鍵の対の両方の鍵が暗号化に使用できる（つまり、交換可能：公開鍵を用いて暗号化している場合は秘密鍵で復号でき、秘密鍵を用いて暗号化している場合は公開鍵で復号できる）。この特性は情報源の証明に利用でき、デジタル署名の基礎となっている。ISO-9594の第8部では、付属書Bにおいて「この（交換可能な）特性を持つＰＫＣＳだけがこの規格の認証の枠組みの中で使用するのに適している」と述べており、そのようなアルゴリズムの一つとしてＲＳＡ（Rivest-Shamir-Adleman)公開鍵暗号システムがISO-9594の第8部／付属書Ｃにおいて説明されている。

付録Ｅ．　メッセージの送受信

ＭＨＳで扱うメッセージは、図1.1-13のプロトコル構成に示される様に、ＲＯＳＥまたはＲＴＳＥを使用し、更にこれらのプロトコルが下位層のプロトコルを使用してメッセージの交換を実現する。

ここでは、応用層におけるメッセージの転送方法の概要について示す。

E. 1　Ｐ３及びＰ７プロトコル

(1)　概要

ＵＡとＭＳ間のプロトコル（Ｐ７）及びＵＡとＭＴＡ或いはＭＳとＵＡ間のプロトコル（Ｐ３）では、一般にＲＯＳＥを使用する。但し、高信頼な転送機能が必要な場合には、ＲＴＳＥを加えて使用することができる（勧告Ｘ．４１９又はＩＳＯ　１００２１－６参照）。その選択は、通信を開始する際のアプリケーションコンテキストを折衝することで行う。ここでは、ＲＯＳＥのみを使用する例を示す。

ＲＯＳＥについては、Ｘ．２２９及びＸ．２１９を参照。

(2)　遠隔操作

遠隔操作（ROSE:Remote Operation Service Element)では、問い合わせ・応答型のアプリケーション（ＲＯＳＥ利用者）に対し、以下の共通的な機能（操作）を提供する。

(a) Invoke　（要求）

(b) ReturnResult　（結果）

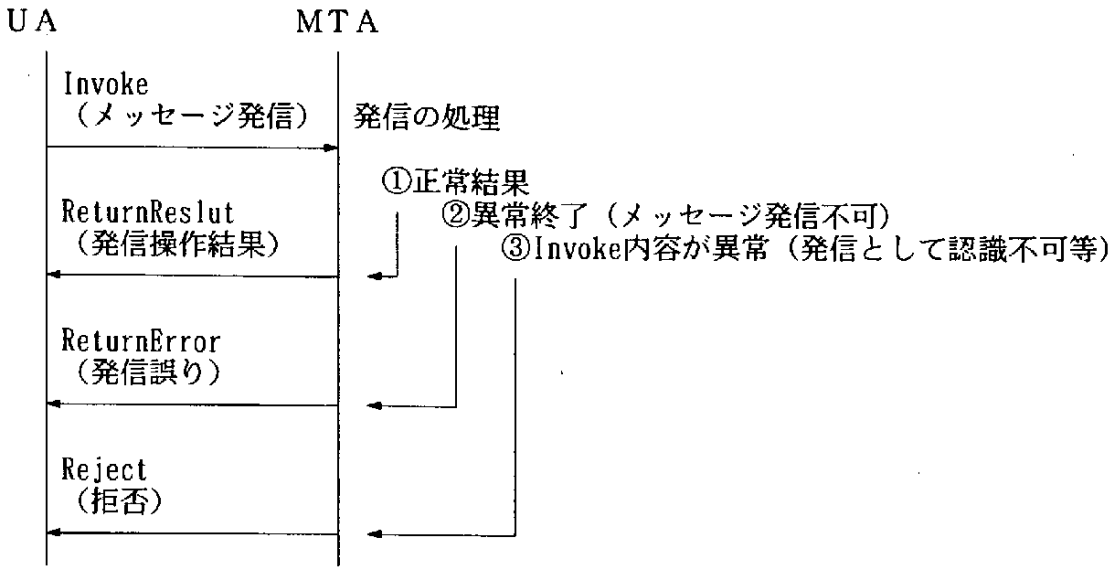
(c) ReturnError　（誤り）

(d) Reject　（拒否）

ＲＯＳＥ利用者（ここでは、ＵＡまたはＭＳ）は、ＭＳまたはＭＴＡに対して操作の要求（例えばメッセージ発信、一覧等）をInvokeを使用して行い、ＭＳまたはＭＴＡは、その結果をその他のROSEの機能を使って返す。

注）Ｐ３では、ＭＴＡからＭＳまたはＵＡへメッセージまたは通知を送信することがある。

ReturnResultは、Invokeにより要求された内容を正しく処理できた場合に結果を設定して送信する際に使用する。 ReturnErrorは、処理が正常にできなかった際に理由とともに誤りであることを通知するために使用する。Rejectはその他の操作(Invoke, ReturnResult, ReturnError）に対し、その形式誤り、システム上の理由等により操作の受け入れを拒否するために使用する。



付図E.1-1　ＲＯＳＥによる転送

メッセージ発信操作によるこの例では、ReturnResult（発信操作結果）に、メッセージ識別子、発信時刻などのパラメタが設定される。ＭＨＳではこれらのパラメタを利用し、さまざまなサービスを提供する。例えば、メッセージ識別子を利用したサービスに、配信通知、配信時刻表示などがある。これらのサービスでは、発信したメッセージに対する配信通知を１対１に対応させるために、ＭＴＳ内で一意な値となるメッセージ識別子を利用している。このようにして、情報の交換を行うことで、サービスの要求と実行が行われる。

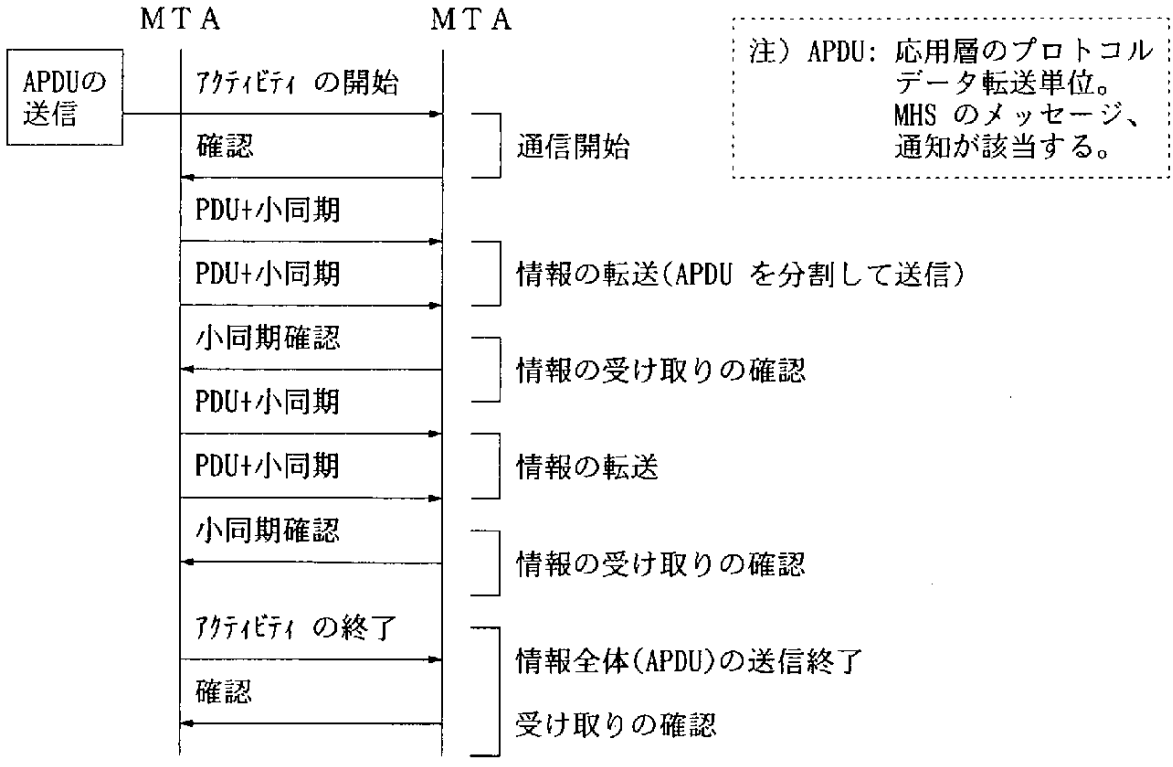
E. 2　Ｐ１プロトコル

(1)　概要

ＭＴＡ間のメッセージ転送では、ＲＴＳＥを必ず使用し、ＲＯＳＥは使用しない。ＲＴＳＥは、情報の紛失や重複して受信するといった障害なしに、情報の転送を行うための機能を提供する。ＲＴＳＥは、セション層のアクティビティや小同期等の機能要素をプレゼンテーション層を通して制御し、この機能を実現する。２章の例で、ＭＴＡ間の情報の転送には、このプロトコルを必ず使用する。

ＲＴＳＥについては、X. ２２８及びX. ２１８を参照。

(2) 通信の例



付図E.2-1 ＲＴＳＥによる転送

付録Ｆ．　ＥＤＩＦＡＣＴ標準メッセージ構造

Ｐｅｄｉ規約書では、ＥＤＩＦＡＣＴ（ＩＳＯ９３７５にて規定）シンタックスルールによるＥＤＩメッセージを転送するケースが多いことを想定し、いくつかのＰｅｄｉサービスでＥＤＩＦＡＣＴメッセージフォーマットを例に挙げ説明を行っている。本書でも同様の扱いとしているため、ＥＤＩＦＡＣＴ標準メッセージの文例と階層構造の具体例について説明し、本書の理解の手助けとなるよう付録の扱いで記述する。

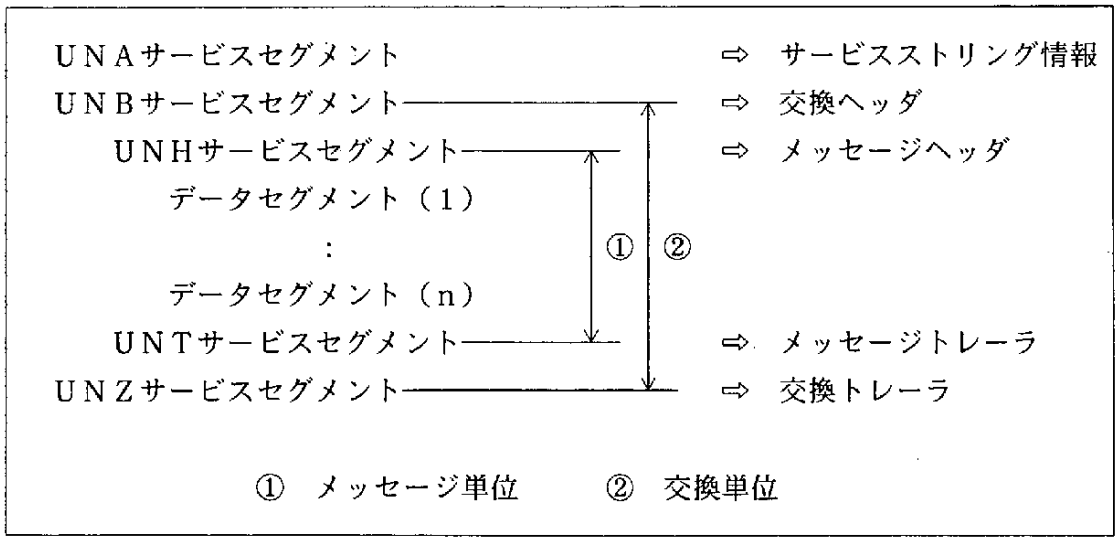
Ｆ．１　交換の構造

ＥＤＩＦＡＣＴシンタックスルールでは、一回の接続は一つ以上のＥＤＩＦＡＣＴインタチェンジ（交換）から成り、これらの「交換」はその始まりと終わりを示すサービスセグメントにより分離される。ＥＤＩＦＡＣＴシンタックスルールではこれらのサービスセグメントが規定されており、ユーザデータの交換を提供可能としている。

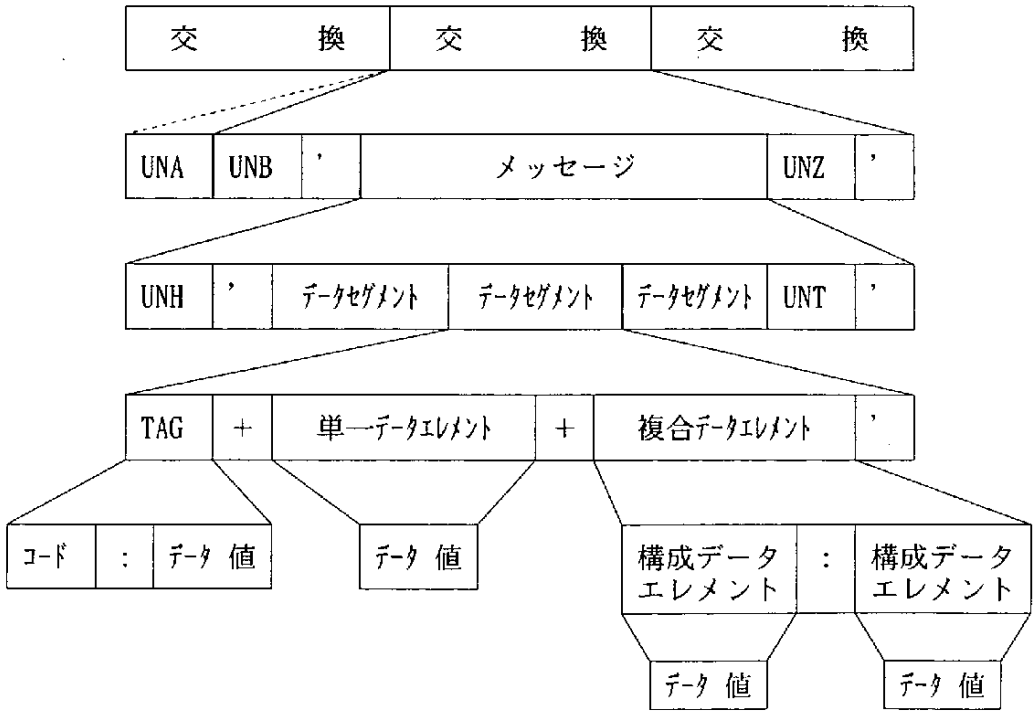
それぞれの「交換」は階層構造を持っていて、一つの「交換」は一個以上の機能グループまたはメッセージから構成される。機能グループは一つ以上の同一タイプのメッセージから構成され、機能グループ・ヘッダ・サービスセグメント（セグメントコードはＵＮＧ）で始まり機能グループ・トレーラ・サービスセグメント（セグメントコードはＵＮＥ）で終わる。機能グループを使用するかどうかは任意であり、省略されることもある。

メッセージは、メッセージ・ヘッダ・サービスセグメント（セグメントコードはＵＮＨ）で始まりメッセージ・トレーラ・サービスセグメント（セグメントコードはＵＮＴ）で終わる。これらのサービスセグメントの間には一つ以上のユーザデータセグメント（以下、データセグメントと呼称）が含まれる。

これらの様子を付図Ｆ.１- １，Ｆ.１- ２に示す。なお、付図では機能グループが省略された場合の階層構造を示している。



付図F.1- 1　交換の構成



付図F.1- 2　文例の階層構造

F. 2 ＥＤＩＦＡＣＴ標準メッセージ準拠の文例

(1) 文例

イギリスのＩＣＩ社からポルトガルのクウィミガル・ド・オポルト社へ化学薬品の納入に関して支払いを求めるインボイスメッセージの文例を以下に示す。なお、その時のインボイスは付図F.2- 1を参照されたい。

```
UNA:+.?'
UNB+UNOA:1+5012345678901:14+123456:91+871215:123619+REF01+PASSW+INVOIC+00001'
UNH+INV001+INVOIC:1'
BGM+380+75-064-H-227101+870421'
NAD+SU+5013456000145:14+ICI CHEMICALS AND POLYMERS+PO BOX 90:WILTON+MIDDLESBOROUGH
++T56 8JE+GB'
RFF+SS+EDS0633096'
RFF+PO+ABC-1234'
CTA+IC++512345:TL'
FII+RB+123-4567+:::WESTLAND BANK:FRANKFURT'
NAD+BY++ALPHONSO SCHMIDT AG:AVE INFANTI SANTO:LISBON 4:PORTUGAL'
RFF+CR+064-5787-1B
NAD+CN+++QUIMIGAL DE OPPORTO+AVE SANCHO 3+BARREIRO+++PT'
CUX+DEM:IN'
ALI+GB'
PAT+01+++05:03:1:60++++PAYMENT 60 DAYS FROM INVOICE DATE BY TELEGRAPHICS TRANSFER
TO:ACCOUNT NO 123-4566 QUOTE REF ABC-1234:WESTLAND BANK, FRANFURT'
PAI+70++30+03'
TDT+++10+++::BAILEY FREIGHT'
LOC+LC+::TEESIDE'
LOC+LD+::BARREIRO'
TOD+02++FRC:01+ITP:::BARREIRO++TAXES AND CLEARANCE UNPAID'
PAC+1++3:UN'
MEA+PD+04+KG:18440'
PCI++TEMP 20-25 DEG C:ALPHONSO SCHMIDT AG:064-5787-1B'
UNS+D'
LIN+++5013456000158:VN++12:18440:KG+2.85:NW:1:KG'
UNS+S'
TMA+52554'
FTX+CUS++WE HEREBY CERTIFY THAT THE GOODS MENTIONED IN THIS INVOICE ARE OF BRITISH
 ORIGIN'
VAL+IN+55735:DEM'
UNT+28+INV001'
UNZ+1+REF01'
```

(2) 解説

以下に主な各データエレメントの意味を示す。

Supplier Tlx no 512345 (コンタクト番号: テレックス) ICI Chemicals and Polymers (サプライヤ 名称) PO Box 90 Wilton Middlesborough England T56 8JE } (サプライヤ 住所)	Invoice date and No. 21-04-87 (インボイス日付) 75-064-H-227101 (インボイス 番号) Other reference EDS 0633096 (指定当事者番号)
Consignee Quimigal De Opporto (荷受人名称) Ave Sancho 3 Barreiro Portugal } (荷受人住所)	Buyer(other than consignee) Alphonso Schmidt AC (買主名称) Ave infanti Sento Lisbon 4 Portugal } (買主住所) Ref No 064-5787-1B (買い主参照番号)
	Country of origin of goods United Kingdom
Transport details Shipped from Teeside to Barreiro per Batley Freight Insured value DM 55735	Termsof delivery and payment Free delivcred Barreiro Taxes & clearance unpaid payment 60 days from date of invoice by telegraphics transfer to account no 123-4567 with Westland Bank, Frankfurt (振込口座番号) (振込先銀行) , D-6123 Quoti Ref ABC-1234 } 支払い条件基準

Shipping marks:Comtainer No.	No. and kind of packaes :Goods description (in full and/on in codes)	Gross weight. kg	Cuba. m3
Temp 20-25 DEC C Alphon 50 Schaidt AC 064-5787-1B	I demoutable ISO container	18,440	

Specification of commodities(in codes and/or in full)	Quantity	Unit price	Amount
5013456000158 - Pure dried vacuum salt	18,440 Kg	DM 2.850 Per Kg NET WT	DM 52554
We hereby Certify that the goods mentioned in this invoice are made of Britch orign.			

Packing	cluded above	Not inel. above
Freight		
Other costs(speclfy)		
Insurance		
Total invoice amount	DM 52554	

付図F. 2- 1 インボイス事例

```
UNA:+.?'
```

UNA(Service String Advice：サービスストリング情報）は、後に続く交換で区切符号や支持符号として使用するため指定される記号を定義する。付図F.1- 2のデータセグメント階層構造を参照。

- コロン(:）は、構成データエレメント分離符号として用いられる。復号データエレメント中の構成データエレメントを分離する。
- プラス記号(+）は、セグメントタグとデータエレメント分離符号として用いられる。
- フルストップ(.）は、小数表記に用いられる。
- 疑問符記(?）は、リリース符号として用いられ、ユーザデータ中で使用される特殊記号（「+」,「:」,「'」,「?」)の意味をリリースし、後に続く文字を通常の意味に戻す。
- アポストロフィ(' ）は、セグメント終了符号として用いられる。

```
UNB+UNOA:1+5012345678901:14+123456:91+871215:123619+REF01+PASSW+INVOIC+00001'
```

UNB(Interchange Header：交換ヘッダ）は、交換を開始し、識別し、特定する。

- UNB
  セグメントタグのコードを示す。
- UNOA:1
  セグメントタグ分離符号(+）に続き、シンタックス識別符号(Syntax indentifier)とシンタックスバージョン番号(Syntax version number）が設定される。
  文例では、管理機関が「ＵＮＯ＝ＵＮ／ＥＣＥ」、使用される文字セットがＵＮ／ＥＤＩＦＡＣＴシンタックスルールの水準Ａを示している。次の分離符号(:）の後の "1"は、シンタックスバージョン番号（Syn-tax version number）を示している。
- 5012345678901:14
  分離番号(+）の後に、送信者識別コード(Sender identification）と識別コード修飾子(Identifier code qualifier）が設定される。
  文例では、送信者識別コードの"5012345678901" が置かれ、更に分離符号(:）の後に、このコードが所属するコードセットを識別する修飾子"14"が続く。
- 123456:91
  分離番号(+）の後に、受信者識別コード(Recipient indentification)と識別コード修飾子(Identifier code qualifier）が設定される。
  文例では、受信者識別コードの"123456"が置かれ、更にデータエレメント分離符号(:）の後にこのコードが所属するコードセットを識別する修飾子"91"が続く。
- 871215:123619
  分離番号(+）の後に、交換の日時が設定される。
  文例では、メッセージ作成日付（"871215"は1987年12月15日を示す。）と時間("123619" は12時36分19秒を示す。）が表記されている。
- REF01
  この伝送のために、交換の送信者が割り当てたユニークな交換制御参照番号(Interchange controlreference)"REF01" が続く。

- PASSW
  受信者パスワード(Recipient reference password)の"PASSW" 設定されている。
- INVOIC
  アプリケーション参照符号の"INVOIC"が設定されている。このフィールドの一般的な利用方法は、メッセージタイプを表す識別子をこのフィールドに設定することにより、同一タイプの「交換」のみ選択するような操作が可能となる。
- 00001
  交換協定に明示されたコードを示す。交換を司る通信協定のタイプを指定する。

```
UNH+INV001+INVOIC:1'
```

UNH (Message header：メッセージヘッダー) は、メッセージを開始し、識別し、特定する。

- データエレメントとして、メッセージ参照番号 (INV001) とメッセージ識別子が設定される。メッセージ識別子は、「メッセージタイプ (INVOIC) 」とメッセージバージョン番号 ("1")を含む「メッセージ識別符号」から成る復号データエレメントである。

```
BGM　～　VAL
```

データセグメントの集合である。ここでは説明を省略する。

```
UNT+28+INV001'
```

UNT (Message trailer：メッセージトレーラー) は、メッセージを紹介し、メッセージの完全性を確認する。

- データエレメントとして、メッセージ参照番号とメッセージ内のセグメント数が設定される。
  文例では、このメッセージ (INV001) が２８個のデータセグメントから成ることを示している。

```
UNZ+1+REF01'
```

UNZ(Interchange trailer：交換トレーラー) は、交換を終了し、交換の完全性を確認する。

- データエレメントとして、メッセージ参照番号とメッセージ内のセグメント数が設定される。
  文例では、この交換(REF01)は１個のメッセージから成ることを示している。

【参考文献】

EDI入門　北澤　博著(SRC発行)

平成６年１１月発行

発行所　財団法人　日本情報処理開発協会
産業情報化推進センター
東京都港区芝公園３丁目５番８号
機械振興会館内
ＴＥＬ：（３４３２）９３８６

印刷所　株式会社　正文社

東京都文京区湯島３丁目４番１３号
ＴＥＬ：（３８３２）９５７１

Ｐｅｄｉ概説書 質問事項等ＦＡＸ送信用紙

年　月　日

宛　先	㈶日本情報処理開発協会　産業情報化推進センター　ユーザー環境課 〔ＦＡＸ〕：０３－３４３２－９３８９　〔ＴＥＬ〕：０３－３４３２－９３８６			
発信者	貴社名		ご所属	
	ご芳名		ご連絡先	電話:(　　)-　　- FAX :(　　)-　　-
	ご住所			
ご担当業務内容				
貴社内管理番号		当センター管理番号	Pedi-	
内容区分	1.質問　2.要望　3.意見　4.その他[　　]　＊該当番号を選択			
ご質問等の内容	別紙【有（　　枚を添付）・　無】			