TTC 標準
TTC STANDARD

JT-H234
オーディオビジュアルサービスのための暗号鍵管理および認証システム

Encryption Key Management and Authentication System for Audiovisual Services

第1版

1994年11月24日制定

社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

＜参考＞

１．国際勧告等との関連

本標準はテレビ電話・テレビ会議などのオーディオビジュアルサービスにおける暗号鍵管理および認証方法を規定しており、加速勧告化手続きによる郵便投票により、1994 年 11 月に承認された ITU-T 勧告 H.234 に準拠している。

２．上記国際勧告等に対する追加項目等

2.1　オプション選択項目

なし。

2.2　ナショナルマター項目

なし。

2.3　その他

（1）本標準は上記 ITU-T 勧告に対し、先行している項目はない。

（2）本標準は上記 ITU-T 勧告に対し、削除した項目はない。

（3）本標準は上記 ITU-T 勧告に対し、追加した項目はない。

３．改版の履歴

版　数	制　定　日	改　版　内　容
第1版	1994年11月24日	制　　定

４．工業所有権

本標準に関わる「工業所有権の実施の権利に係る確認書」の提出状況は、ＴＴＣホームページでご覧になれます。

５．その他

（1）参照している勧告、標準等

ＴＴＣ標準　　：ＪＴ－Ｈ２２１，ＪＴ－Ｈ２３０，ＪＴ－Ｈ２３３，
ＪＴ－Ｈ２４２

ＩＴＵ－Ｔ勧告　：Ｘ．５０９，Ｘ．２０９，Ｔ．１２０

ＩＳＯ規格　　：ＩＳＯ８７３２

目　　次

０．要約

本標準では、暗号鍵管理の 3 つの方法が述べられている。すなわち、ISO8732、ディフィーヘルマン、RSA である。これらは JT-H221 フレーム構成を用いてディジタル的に伝送されるオーディオビジュアル信号の暗号化に適応できる。ここで定義された管理メッセージは JT-H221 の暗号化制御信号（ECS）チャネル内で伝送され、これらの構成と使用方法は JT-H233 に定義されている。

１．本標準の規定範囲

セキュリティシステムは 2 つの部分から成り立っている。1 つは機密保持メカニズムすなわちデータに対する暗号化処理であり、もう 1 つは鍵管理サブシステムである。

本標準は TTC 標準 JT-H221、JT-H230、JT-H242 に準拠した狭帯域オーディオビジュアルサービスでの使用に適したセキュリティシステムに関する認証と鍵管理方法を記述している。機密保持に関する仕様は本標準と独立しており、別の標準である JT-H233 に含まれている。

セキュリティは、秘密の鍵を用いることで確保される。鍵はセキュリティシステムの機密保持部分で用いられ、送信データを暗号化し、復号する方法を制御する。もし、第三者が使用されている鍵を知ってしまうと、セキュリティシステムはもはや安全とは言えない。

従って、ユーザによる鍵の管理は、どんなセキュリティシステムにとっても重要である。本標準では、3 種の実用的な鍵管理方法を記述しており、いずれかが使用される。自動鍵管理が使用不可能である場合は、手動鍵管理のような本標準に規定されていない代替手法が使用可能である。

最初の方法は ISO8732 として知られている。この方法は、鍵の機密保持の品質を高く保つことが物理的に可能であるシステムにおいて手動設定された鍵を基にしたものであり、鍵の自動配送は、手動で配送された鍵のもとで暗号化される。これらの自動鍵配送を暗号化するためのアルゴリズムは、通常、通信それ自身を暗号化する方法と同じである。自動配送された鍵のセキュリティは手動配送された鍵のセキュリティに依存している。

自動配送された鍵は、1 セッションの間のみ、あるいは一定期間（例えば、1 か月）内の複数セッションにわたって使用される。ISO8732 では、2 つの端末間において、自動的に情報を交換するプロトコルのみならず、手動鍵配送の機密保持のための物理的なプロトコルも含んでいる。

ここでは、2 つの異なった環境が規定されている。一つはポイント・ポイント（2 階層）の環境であり、2 つの端末が一つの共通鍵を共有し合うものである。もう一つは 3 階層の環境であり、通信を行いたい 2 端末は共通鍵を共有せず、それぞれが第三者装置との共通鍵を使うものである。2 つの環境間を識別することが必要であるが、第三者とのインタフェースは本標準の規定外である。

2．3．2 節に規定されているセッション鍵配送は、ISO8732 の方法により自動配送された鍵がセッション鍵として使用されるのに十分な機密強度を保持している点において、機能的には ISO8732 のコピーと言える。しかしながら、本標準の方式に従うと、これらの鍵は、2．3．2 節で記述される＜鍵＞（鍵暗号化鍵）として使われる。

2 番目の方法は、システム上で自動的に鍵を生成し配送する（この鍵配送自体も暗号化される）拡張ディフィーヘルマン方式として知られる簡単で安全な手法である。鍵が配送されるまではユーザの操作を必要としないが、同じチェックシーケンスが互いの端末で利用できることを音声で確認することが望ましい。本手法は例えば、衛星チャネルで伝送されるオーディオビジュアル信号を局外者が盗聴することを防ぐのに適している。局外者がシステムに進入するためには、暗号化が実行される前に双方の通信を完全に横取りし、両者に自分が正当な通信相手であるような振りをして鍵配送を行うことが必要である。なお、本機能は認証機能をそなえていない。

3 番目の方法は、もっと複雑になるが極めて高いセキュリティを提供し、またオーディオビジュアルサービスのエンティティ（端末、MCU など）の認証機能も提供する。この RSA 手法は勧告 X．509 で提案されている公開鍵手法によく似ており、RSA アルゴリズムを使用している。本手法では、相互接続性を必要とする全てのエンティティが利用できる認証機関の確立が必要である。なお、認証は実際上オフラインで行われ、その機関の安全性を信頼する。この認証メカニズムにより会議に参加している各グループは、お互いを確実に確認することができる。また、ポイント・ポイント通信と同じく多地点間通信でも動作可能である。

以上の方法は、誤りのないクリアチャネルを必要とする。ただし、アクセス管理や認証機関の安全性や否認不可はこれらの方法によっても提供されない点に注意すべきである。

4 番目の方法として、手動鍵配送を本標準で参考として記載する。

手動鍵配送は JT－H234 のメッセージ配送なしに、ユーザが直接鍵暗号化鍵を端末に入力するものとして定義する。同じ鍵が両方の端末に入力される。鍵の長さは暗号化アルゴリズムに依存している。鍵のビット順序は最上位ビット（MSB）は最初に入力され、最下位ビット（LSB）は最後に入力される。実際に端末へ鍵を入力する手法は端末に依存し、本標準の範囲を超えている。

以下に入力手法の例を示す。

・入力のために電話のキーパッドを使用する。(MSB)00111010 . . . 01110100(LSB)

・コンピュータからダウンロードする。

・16 進のキャラクタとして入力するためにキーボードを使用する。(MSB)3A . . . 74(LSB)

手動入力は通信を始める前に、あるいは通信中に行われる。後者の場合、利用者は会議中に暗号化を求めることを決定し、端末に備えられたインタフェースを用いて鍵を入力する。そして端末のユーザインタフェースを通して暗号化を開始する。ユーザ・インタフェースを通して暗号化が要求されると、BAS コードの暗号化オンの送信、ECS チャネルの使用、暗号化アルゴリズムの選択、鍵管理の手動モードが同意され、そしてセッション鍵が交換される。

暗号化システムが秘密を確保していると見なすには、全ての会議出席者は他の会議出席者にせよ MCU や変換装置にせよ、誰がまたは何が暗号化されていないデータにアクセスできるか知っている必要がある。このため、エンティティが互いに認証できるように会議開始前に初期設定の時間が必要である。こうして、暗号化されていないデータにアクセスするすべてのエンティティは、会議が始まる前に他のすべてのエンティティに、確実に確認される。認証システムはネットワーク提供者に例えば、MCU を使った通信での課金情報のような情報も提供する。

もし、暗号化されていないデータが MCU（いわゆる信頼できる MCU）に存在し得る場合には、その装置は認証システムの一部であるべきである。ネットワーク内に信頼できる MCU があるということはユーザにも知らされるべきである。

以下、2 章ではこれらの手法に共通な点を取り上げ、3、4、5 章ではそれぞれ ISO8732、ディフィーヘルマン、RSA 方式を取り扱う。

定義

AVSE：オーディオビジュアルサービスのエンティティ（端末、MCU 等）

＜鍵＞：鍵暗号化鍵

２．メッセージシステムと鍵配送

2.1　メッセージチャネル

以下に述べるシステムは、回線の両端末間で順々に伝達される、多くの定義されたメッセージで構成されている。この伝達のために必要な誤りの無いチャネルは標準 JT-H233 のセッション交換（SE）ブロックの項に記述されている。

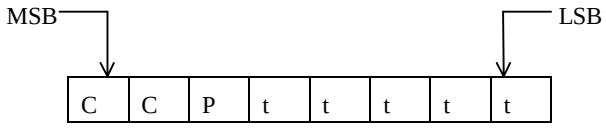
2.2　メッセージフォーマット

鍵配送や認証のために暗号化システムで使用するメッセージは、ITU-T 勧告 X．209 に記載の ILC（識別子、長さ、内容）形式にフォーマット化される。長さは長短いずれかの形式で符号化される。X．209 に記述の不定長形式は使用しない。

本標準で使用する X．209 の定義の一部について以下に簡単に説明する。

2.2.1　識別子

識別子は次のような構造を持った 1 オクテットである。



2 ビットの CC はタグクラスであり、識別子のタイプを定義する。この勧告で定義する識別子は 10（文脈依存）である。

基本形式／構文形式ビット（P）は、内容が基本形式であるか内部にさらにデータ要素を持つかを示すものである。

5 ビットのタグ（ttttt）は一意的に識別子を（そのクラスに応じて）規定する。

従って本標準の識別子は全て 10P $t_1t_2t_3t_4t_5$ のオクテット形式を持つ。

2.2.2　長さ

長さ（L）とは、内容をオクテット単位の長さで規定するものであり、それ自身が可変長である。

短形式とは 1 オクテット長であり、L が 128 未満の場合に長形式に代わって優先的に使用される。ビット 8 の値は 0 であり、ビット 7 から 1 には符号なしの 2 進数として L を符号化したものが入る。この場合、MSB と LSB はそれぞれビット 7 とビット 1 である。

長形式とは 2 から 127 オクテット長のものであり、L が 128 以上で、かつ 2 の 1008 乗未満の場合に使用される。第 1 オクテットのビット 8 の値は 1 である。この第 1 オクテットのビット 7 から 1 には符号なしの 2 進数で、長形式のオクテット長から 1 を引いた数を符号化したものが入る。この場合、MSB と LSB はそれぞれビット 7 とビット 1 である。 L 自体は符号なしの 2 進数として符号化され、MSB と LSB はそれぞれ第 2 オクテットのビット 8 と最終オクテットのビット 1 である。この 2 進数の符号化はできるだけ少ないオクテットを用い、8 ビットの値が全て 0 のオクテットが先行しないようにする。

2.2.3 ビット列

基本形式におけるビット列は、8 ビット毎にオクテットにまとめられたビットと、これに先行し、内容の最終オクテットの未使用ビットの数（0 から 7 まで）を符号なしの 2 進数として符号化した 1 オクテットで構成される。MSB、LSB はそれぞれビット 8 とビット 1 である。

2.3 セキュリティシステムの開始

システム開始のために、以下詳述する P0、P1、P2 の 3 つのメッセージを使用する。セキュリティシステムは、回線の任意の一方の端末からタイプ（P0）のメッセージを送出することにより起動される。メッセージ（P0）は送信者が処理できる鍵管理手法（ISO8732、ディフィーヘルマン、RSA の内可能なもの全て）を示すビット列を含む。このメッセージの受信者は使用する鍵管理手法を決め、その結果に応じてタイプ（P0）またはタイプ（P1）のメッセージで応答する。

もし両端末が同時にメッセージ（P0）を送出しても、交換されたビット列の比較により鍵管理手法の選定を行うことができる。

－両端末が同じ手法をサポートしている場合は、その手法を使用する。複数の手法をサポートしている場合の優先順位は、ISO8732、ディフィーヘルマン、RSA／X．509、そして最後に手動として本標準で参照される未定のオプション、の順である。

－両端末に共通の手法が無い場合、その回線は暗号化できない。

2.3.1 開始メッセージ

メッセージ名	セキュリティシステム要求（P0）
メッセージ識別子	$10Pt_1t_2t_3t_4t_5$ = 10000000
意味	本メッセージの送信者は暗号化システムの使用を要求する。 本メッセージは暗号化を開始するために用いられるほかに、相手端末からのメッセージ（P0）への応答にも用いられる
内容	以下に示す基本形式のオクテット これに含まれるビット列はどの鍵管理手法が使用可能かを示す。（MSB）0000XDRM（LSB） ・X は ISO8732 がサポートされるとき 1、そうでないとき 0 がセットされる。 ・D はディフィーヘルマン方式がサポートされるとき 1、サポートされないとき 0 がセットされる。 ・R は RSA がサポートされるとき 1、サポートされないとき 0 がセットされる。 ・M は手動鍵登録のような規定されていない鍵管理システムがあるとき 1，そうでないとき 0 がセットされる。
X．209の“抽象構文記法（ASN．1）”	Request Encryption System ::= [0] IMPLICIT OCTET STRING
	本メッセージの内容は常に1オクテット長である。

メッセージ名	暗号化不能（P1）
メッセージ識別子	$10Pt_1t_2t_3t_4t_5$ = 10000001
意味	メッセージ（P0）への応答として送信される。 本メッセージの送信者は暗号化システムを使用しない。
内容	本メッセージは内容を持たない。

メッセージ名	暗号化システム開始失敗（P2）
メッセージ識別子	10 $Pt_1t_2t_3t_4t_5$ = 10000010
意味	本メッセージの送信者は暗号化システムの開始を失敗した。この失敗は鍵配送の失敗によることがあり得るが、セキュリティの性格上、失敗の原因はメッセージ内に記述されない。
内容	本メッセージは内容を持たない。

2.3.2　セッション鍵の配送

情報の暗号化に用いられるセッション鍵は、セッション鍵配送によって得られる。セッション鍵を含むメッセージは、ここで述べるようにフォーマット化され、認証または、＜鍵＞配送プロトコルによって得られた鍵暗号化鍵（本標準では＜鍵＞と略す）を用いて暗号化される。これらの 2 つのタイプの鍵の違いに、留意しなければならない。すなわちセッション鍵は JT-H221 のフレーム構成をとるオーディオビジュアル信号の暗号化／復号に使用され、一方ここで言う＜鍵＞はセッション鍵の配送における暗号化と復号のみに使用されるものである。

暗号化メカニズムは、Ｎビット長の鍵を用いる。共通な＜鍵＞が通信の当事者間で確立され、これもＮビット長である。RSA の場合、さらに＜鍵＞を導き出すための認証≪鍵≫がある。

共通な＜鍵＞は、この節（図 1／JT-H234）で述べる様に、4 個のＮビットのセッション鍵を暗号化することに用いられる。暗号化の方法は、オーディオビジュアル信号の暗号化のために選ばれたと同一でなければならず、これは JT-H233 の中で定義している、P9 メッセージの伝送により示される。

セッション鍵配送メッセージは、8 ビットのメッセージ識別子と、誤り訂正を有する初期化ベクトルと、4N ビットの乱数からなる。回線の両端末が互いにこのような値を送信し、それによってそれぞれ 4 個 1 組のセッション鍵を得る。各セッション鍵はＮビット長であり、Ｎの値は使用される暗号化アルゴリズムに依存する。（例えば B-crypt の場合、N＝56）

伝送され受信された乱数は、次の様に 4 つのＮビットブロックとして処理される。

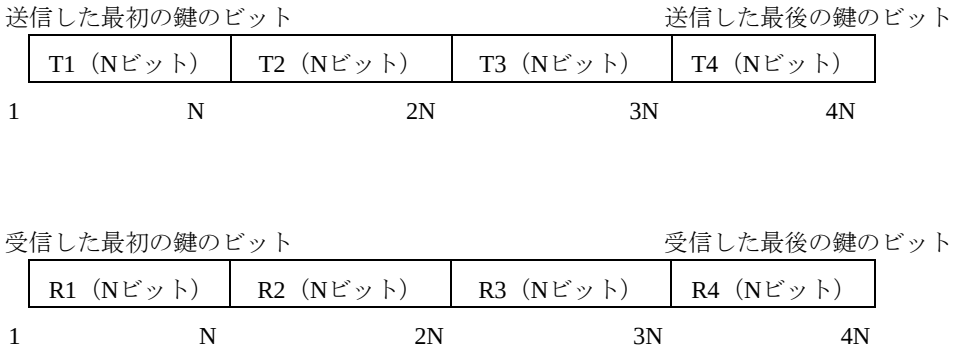


図 1／JT-H234　セッション鍵配送のビット順序

4 つのセッション鍵はそれぞれ送信したブロックと受信したブロックをビット順序を保ちながら 1 ビット毎に排他的 OR をとることによって求められる。すなわちセッション鍵の最上位ビット（暗号化装置に設定される鍵データの最初のバイトまたはワードの最上位ビット）は送受信したブロックの第 1 ビット同士の排他的 OR をとることによって得られる。図 1／JT-H234 のビット順序を用いて 4 つのセッション鍵が以下のように求められる。

送信回線暗号化鍵 1　　：ブロック T1 とブロック R3 の排他的 OR

送信回線暗号化鍵 2　　：ブロック T2 とブロック R4 の排他的 OR

受信回線暗号化鍵 1　　：ブロック T3 とブロック R1 の排他的 OR

受信回線暗号化鍵 2　　：ブロック T4 とブロック R2 の排他的 OR

暗号化鍵 1 は JT-H221 の付属資料 A（3）で暗号化オンに記述されるように JT-H221 のフレーム化された信号の内容の暗号に使用される。付表 A-1／JT-H221、あるいは付表 A-2／JT-H221 における BAS コマンドの下で MLP がオンのとき、同じ鍵 1 か代わりの鍵 2 のどちらか使用して、MLP チャネルは、T．120 シリーズ標準に規定される様に暗号化される。

選択された暗号化アルゴリズムによってはセッション鍵に対しパリティを必要とするかも知れないが、これはそのアルゴリズム内に閉じた問題であり、伝送の形態にまで影響することはない。

チェックは 4Nビット全体に対してのみ行われる。もし排他的 OR をとって得られた 4Nビットの結果が全て 0（すなわち 4 個のNビットのセッション鍵が全て 0）であれば、セッション鍵は暗号化装置に設定されずセキュリティシステムは起動されない。

セッション鍵配送メッセージ（P6）

本メッセージはメッセージ識別子、デフォルトの誤り訂正ビットを含む 96 ビットの初期化ベクトル、4Nビットの乱数からなる。

メッセージ名	セッション鍵情報（P6）
メッセージ識別子	$10Pt_1t_2t_3t_4t_5$ = 10100110
意味	本メッセージの送信者はセッション鍵情報を配送している。
内容	セッション鍵データの暗号化に用いられる（暗号化されていない）初期化ベクトルと、暗号化され上述のようにフォーマット化されたセッション鍵情報を含む構文形式
X．209の 抽象構文表記法	Session Key Information ::= [6] IMPLICIT SEQUENCE { initialization-vector[0]IMPLICIT BIT STRING, session-key-information[1]IMPLICIT BIT STRING}

３．ＩＳＯ８７３２鍵管理

3.1　まえがき

参考文献 1 の標準は、認証と暗号化に対する暗号化鍵の保護と配送に関して一定の方法を与える。この標準は、次のようなものを含む手動と自動の両方での鍵情報の管理を定義する。

・認められていない開示、修正、置換を防ぐために鍵情報の有効期間の管理
・暗号化の設備や装置の間で相互に実行可能とするための鍵情報の配送
・鍵情報の生成、配送、保管、登録、使用、破棄を含む全ての段階の間で鍵情報の完全さを保証すること
・鍵管理処理の失敗発生、あるいは鍵情報の安全性が競われるときの回復

自動的に配送される鍵の暗号化に使われるアルゴリズムは、通信それ自身の暗号化に使用されるものと通常は同じであり、メッセージ P8 の交換により取り決められる。DES 以外のアルゴリズムが使用されたときは、鍵管理システムは厳密に言えば参考文献 1 に一致せず、この一点においてのみ規格からはずれている。

3.2　鍵管理構成

通信する両者に対する要求一覧は参考文献 1 に示されている。ここでは 2 階層構成と 3 階層構成がある。これらはいずれも鍵配送に使用される。

3.3　鍵管理環境

鍵配送には、ポイント・ポイント、鍵配送センタ（CKD）、鍵転送センタ（CKT）の 3 つの環境が存在する。これらの環境の詳細は参考文献 1 に示されている。

ポイント・ポイントは 2 階層の環境であり、2 つの端末は共通鍵を共有する。共通鍵は、ISO8732 に概説されるように、安全なプロトコルと物理的な保護を用いて手動で配送されていると仮定する。ISO8732 に記述される自動鍵配送は、共通＜鍵＞が一方の端末で生成されて、安全な方法でもう一方の端末に渡すことを保証する。そして、これは 2. 3. 2 節に記述されるセッション鍵の生成に用いる鍵である。

鍵配送センタ（CKD）と鍵転送センタ（CKT）との間の相違は、この標準においては問題ではない。互いの第三者、あるいはセンタ（CKD か CKT）が存在する場合、各端末が共有する鍵は 2 倍の長さで規定される。端末の 1 つを端末 A と呼ぶと、これとセンタとのインタフェースはまたこの標準の仕様外である。しかし、センタとの交換の終了時点において端末 A はクリアな＜鍵＞だけでなく、端末 B の 2 倍の長さの鍵（アルゴリズム仕様に関して ISO8732 を参照）の下で暗号化された＜鍵＞も保有する。ECS 経由で SE ブロックを通してこれを端末 B に送り、そこでクリアな＜鍵＞に変換されてセッション交換プロトコルを始めることができる。

3.4 暗号化サービスメッセージの配送

ISO8732 は、メッセージ配送にテキストを使用する。送出するメッセージの順序やメッセージの送出される状況は参考文献 1 に示される。次のメッセージ（P11）は、ISO8732 の暗号化サービスメッセージ（CSM）を送るための仕組みを与える。各々のバイトは、1 つのテキストキャラクタを表わす。

ビット順序は、MSB が先に送出されるものとする。

メッセージ名	暗号化サービスメッセージ（P11）
メッセージ識別子	10 $Pt_1t_2t_3t_4t_5$ = 10101011
意味	本メッセージの送信者は1つの単独の暗号化サービスメッセージを送出している。
内容	テキストの基本形式ビット列
X．209の ASN．1の表記	Cryptographic Service Message ::= [11] IMPLICIT Visible String

端末ユーザインタフェースは、ISO8732 プロトコルに陰に規定されている。適当な鍵や他の識別子を、名称により識別するためのプロトコルを与えるものと仮定されている。例えば私設網において、2 階層の環境の各々の通信ペアはシステムの暗号ユニットに埋め込まれた共有鍵と称するものを持っている。そして呼を張るための仕組みが自動的に暗号化サブシステム共有鍵と呼ばれる専用鍵を認識する。

ISO8732 は誤り条件や誤り応答のためのサービスメッセージを規定している。ISO8732 をサポートする 2 つの端末が実際に互いに 3 つの環境のうちの 1 つに適合しないその場限りのやり方で通信を試行するなら、（共通的に知られている識別子、鍵の名称、カウンタ、センタなどを含む）プロトコルは破綻し、試みた暗号化セッションは端末のオペレータへの通知と共に終端されるであろう。暗号化を要求する呼を完結するため、2 つの端末のユーザは別の鍵管理配送の仕組みへ移行するか、または、（おそらくは互いの第三者やセンタを使うことで）3 つの環境のうちの 1 つに設定するであろう。

3.5 ISO8732 メッセージ配送の例

一般的なメッセージ配送の流れを示した図 2／JT-H234 を例に考えてみる。送るべき最初のメッセージは RSI（サービス要求）である。ISO8732 の 13．4 節は CSM［暗号化サービスメッセージ］のメッセージフォーマットを記述している。その形式は、

CSM（MCL／．．．）

で、ここで全てのキャラクタは ASCII 表示、括弧はメッセージの最初と最後を示す。また先頭のスラッシュ［またはソリダス］（／）はフィールド内容からフィールドタグを分けるために用いられる。

この場合、MCL フィールドの内容は RSI であり実際の送出テキストは次の様になる。

CSM（MCL／RSI．．．）

RSI メッセージに対するフィールドの順序は ISO8732 の表 3 に示されている。その順序は MCL RCV ORG SVR　EDC（オプション）である。この例では、オプションの EDC は省かれている。

表 2 は、各々のフィールドをより詳しく決定する。かくして送出メッセージは次の様になる。

CSM（MCL／RSI‾RCV／A‾ORG／B‾SVR／KK．KD．IV）

－	フィールドセパレータとして使う空白部	KD	2 つのセッション鍵の要求
A	受信者	IV	IV の要求
B	送出者	MCL	メッセージクラス
.	サブフィールドのセパレータ	RCV	受信者
SVR	サービス要求	ORG	創設者
KK	＜鍵＞の要求		

ISO8732 の 14．7 節には RSI メッセージが詳しく記述されている。

第二番目のメッセージは、KSM［鍵サービスメッセージ］、第三番目は RSM［応答サービスメッセージ］、第四番目は DSM［サービス切断メッセージ］で第五番目は再び RSM となる。

ユーザ A またはユーザ B は、切断（DSM）手順を始める。本図はユーザ A から始めた場合を示している。

図 2／JT-H234　ポイント・ポイント環境（通常のメッセージの流れ）

４．拡張ディフィーヘルマン方式の＜鍵＞配送

4.1　まえがき

＜鍵＞配送は、ディフィーヘルマン方式を基にしているが、オーディオビジュアル回線の特性を活用して、積極的な盗聴に対して保護手段を与えるために拡張されている。
＜鍵＞配送の結果、秘密の値が共有され、回線の検証とセッション鍵の配送の両方にその値が使われる。
動作は次の様になる。［付録の参考文献 1 を参照］

（1）＜鍵＞配送プロトコルは、ここに述べる方法に従ってデータを交換する。
（2）（1）で得られたデータは、回線の暗号化で使うセッション鍵の配送に使われる。
（3）（1）で得られたデータは、回線の検証に使われる。

4.2　基本プロトコル

これは、最初のデータ交換と、それに続く双方向の中間結果の交換から成る。共有する秘密の値は、この中間結果から得られる。

4.2.1　＜鍵＞配送の方式

使われる方式は、基本ディフィーヘルマン方式を二重にしたものである。結果として生じる＜鍵＞が一方の端末で選ばれた素数と原始根だけに依存しないように、二重の配送が使われる。

2 人のユーザ（AVSE）である、A と B を考える。
なお、ここでは添え字を見やすくするためにべき乗表現に記号（ ^ ）を用いる。

A が B に送る。：素数 p_A
　　原始根 a_A
　　値 $c_1 = \{a_A \hat{} a_1 \bmod p_A\}$
　　ここで、a_1 は A だけが知っている乱数。

B が A に送る。：素数 p_B
　　原始根 a_B
　　値 $c_2 = \{a_B \hat{} b_1 \bmod p_B\}$
　　ここで、b_1 は B だけが知っている乱数。

A が B に送る。：値 $c_3 = \{a_B \hat{} a_2 \bmod p_B\}$
　　ここで、a_2 は A だけが知っている乱数。

B が A に送る。：値 $c_4 = \{a_A \hat{} b_2 \bmod p_A\}$
　　ここで、b_2 は B だけが知っている乱数。

ここでユーザ A と B は、それぞれ一対の結果 r_1，r_2 を計算する。

ユーザ A の結果：$r_1 = c_1 \hat{} a_1 \bmod p_A$

$r_2 = c_2 \hat{} a_2 \bmod p_B$

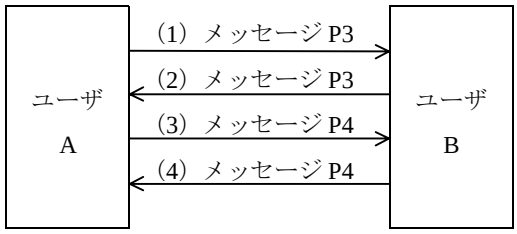
ユーザ B の結果：$r_1 = c_4 \hat{} b_2 \bmod p_A$

$r_2 = c_3 \hat{} b_1 \bmod p_B$

ユーザ A と B の双方の結果 r_1，r_2 は、いずれも $r_1 = a_A \hat{} (a_1 \cdot b_2) \bmod p_A$ と $r_2 = a_B \hat{} (a_2 \cdot b_1) \bmod p_B$ となり、同一の値が共有される。最終結果 R_{12} は r_1 と r_2 をビット毎に排他的 OR を取って得られる。r_1 と r_2 が同じ長さではない場合には排他的 OR の演算は以下のようになる。ここで、L とは、短い方の長さを示している。

｛（r_1 の下位の L ビット）ExOR（r_2 の下位の L ビット）｝

二重ディフィーヘルマン方式の＜鍵＞配送の図解を以下に示す。



(1) p_A, a_A, $(a_A \hat{} a_1 \mod p_A)$ （メッセージ（P_3）で送る）

(2) p_B, a_B, $(a_B \hat{} b_1 \mod p_B)$ （メッセージ（P_3）で送る）

(3) $(a_B \hat{} a_2 \mod p_B)$ （メッセージ（P_4）で送る）

(4) $(a_A \hat{} b_2 \mod p_A)$ （メッセージ（P_4）で送る）

図 3／JT-H234　二重ディフィーヘルマン方式の＜鍵＞配送

4.2.2 ＜鍵＞の導出

上述のようにして、ユーザ A と B はそれぞれ $r_1=a_A\hat{}\ (a_1\cdot b_2) \bmod p_A$ と $r_2=a_B\hat{}\ (a_2\cdot b_1) \bmod p_B$ を生成する。そしてこれらの値をビット毎に排他的 OR を取ることにより最終結果 R_{12} を得る。ユーザ A、B は両者共に最終結果 R_{12} の値を確認して、もしすべてのビットが 0 であれば“暗号化システム開始失敗”メッセージ（P2）を相手ユーザへ送る。

回線の両側の端末に、K ビットの最終結果 R_{12} が得られ、これから検証符号と、セッション鍵の暗号化に使われる＜鍵＞が導出される。機密保持にNビット、検証符号に M ビットを使う時、下位の M ビットが検証符号、次のNビットが＜鍵＞を構成する。これを図 4／JT-H234 に示す。M の値は 64 ビットである。N の値は＜鍵＞の長さであり、使用する暗号化アルゴリズムにより定まる。

K は（M＋N）ビットより長くなければならない。64 ビット暗号化アルゴリズムで 64 ビット検証符号の時、K は 128 ビットより大きくなければならない。実際の場面では、K はこれよりかなり長いであろう。

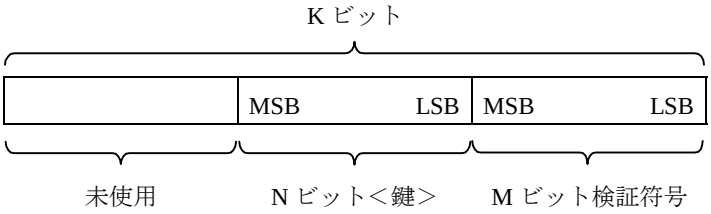


図 4／JT-H234　＜鍵＞配送の結果

4.3 ディフィーヘルマン方式のメッセージ

本節は、セキュリティシステムの開始やディフィーヘルマン方式の＜鍵＞配送に必要なメッセージの内容について記述する。

4.3.1 ＜鍵＞配送情報

メッセージ名	＜鍵＞配送情報（P3）
メッセージ識別子	10 $Pt_1t_2t_3t_4t_5$ = 10100011
意味	本メッセージの送信者は二重ディフィーヘルマン方式の＜鍵＞配送の一部分として、＜鍵＞配送情報を送信する。
内容	下記の原始根、素数と中間結果の基本形式から構成される構文形式 注：原始根（primitive root）は、このメッセージ内容の説明に使用される基本形式（primitive）と関係ない。
ASN．1の表記法	Key Exchange Information ::= [3] IMPLICIT SEQUENCE { primitive root [0] IMPLICT BIT STRING, prime [1] IMPLICT BIT STRING, intermediate-result [2] IMPLICT BIT STRING } 原始根（primitive root）の内容は基本形式ビット列である。 素数（prime）の内容は基本形式ビット列である。 中間結果（intermediate result）の内容は基本形式ビット列でありディフィーヘルマン方式の＜鍵＞配送の中間結果の一つを含んでいる

4.3.2 中間＜鍵＞配送情報

メッセージ名	中間＜鍵＞配送情報（P4）
メッセージ識別子	10$Pt_1t_2t_3t_4t_5$ = 10000100
意味	本メッセージの送信者は二重ディフィーヘルマン方式の＜鍵＞ 配送の一部分として、＜鍵＞配送情報を送信する。
内容	中間結果を含む基本形式ビット列
ASN．1の表記法	Intermediate Key Exchange Information ::= [4] IMPLICIT BIT STRING
	中間結果のビット列はディフィーヘルマン方式の中間結果の一つを含んでいる。 メッセージ（P3）及び（P4）が二重ディフィーヘルマン方式の＜鍵＞配送を構成するが、これにより最終の＜鍵＞が回線の両端末で決定される。

4.3.3 ＭＣＵからの検証符号情報

メッセージ名	MCUからの検証符号情報（P5）
メッセージ識別子	$10Pt_1t_2t_3t_4t_5$ = 10100101
意味	ＭＣＵはディフィーヘルマン方式の＜鍵＞配送から得られた検証符号情報を送信する。
内容	回線識別子と検証符号の構文形式
ASN．1の表記法	Link check code information ::= [5] IMPLICIT SEQUENCE { link-identifier [0] IMPLICIT BIT STRING, check-code [1] IMPLICIT BIT STRING }

ＭＣＵはディフィーヘルマン方式の＜鍵＞配送を完了した回線それぞれにメッセージ（P5）を送信する。

注：回線識別子（link identifier）は検証符号（check code）がＭＣＵからのどの回線に関連するかを識別するのに使用される。MCU の構成の知識が、この識別子の解釈に必要である。（以下の 4．4 節も参照）

4.4 回線検証用の拡張

4．2 節で、64 ビットの検証符号が得られた。これは、16 桁の 16 進数字の全部または一部として端末により提示されねばならない。ここでは、図 5／JT-H234 に示すビット順序を使用し図 4／JT-H234 の用語の定義に従う。

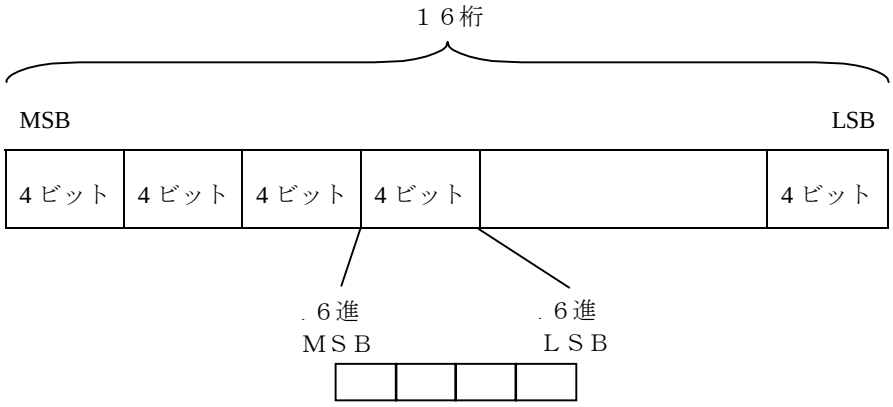


図 5／JT-H234　回線検証用ビット順序
（検証符号の各 4 ビットが 1 つの 16 進数字を形成し、ユーザに示される。）

この値は左端の桁を MSB（検証符号の終了）として、それぞれのユーザに示される。全ての桁を伝える必要はなく、左端 4 桁でおそらくは十分である。この場合回線の問題を見逃す確率がわずか 2^{16} 分の 1 である。

示された値は、一方のユーザから他のユーザへ、オーディオビジュアルチャネルを通じて口頭で伝えられる。相手のユーザはその値と自分の端末に表示された値が一致しているかどうか確認する。

｛口頭による検証は音声が実際に暗号化される前に可能である。更に、4．3．3 節に示す多地点接続状態での、この過程および代案の過程のタイミングは同じとすべきである。｝

５．RSA に基づいた動作

5.1　まえがき

5.1.1　概要

この節では、ポイント・ポイントおよび多地点接続の両者を含むオーディオビジュアルサービスのための、RSA に基づいた認証システムについて述べる。

ここで述べている認証の手段と機能は ITU-T 勧告 X．509 に基づいている。この勧告では、一つあるいはそれ以上の認証機関の層を使って認証が確立される。認証機関（CA）はオフラインで認証子をエンティティや他の CA に発行する。この認証子を使ってエンティティや CA は自分自身を他のエンティティや CA に対して認証する。オーディオビジュアルサービスの場合、エンティティはユーザ端末と信頼された MCU の両方である。

ここで述べる認証の枠組みは 2 層の CA を使っている。最下層では例えば国や会社というようなネットワークド領域は、それぞれ自分の CA を持っている。認証された領域間のオーディオビジュアルサービスを可能にするには、これらの CA は自分たちを認証するために、より高い層にある共通の CA を持つことになる。この共通の CA はユーザに対して共通の信用手段になる。これが可能でない場合、5．5 節に簡単に述べる様に、他の案が存在するが、もっと複雑になる。

ネットワーク領域層での CA は認証子における識別名を複製しないということを信用されるべきである。認証そのものは信用されない環境でも確立されなければならない。さらに、いったんエンティティが認証されると（呼が終了するまで）信用される。

5.1.2　用語説明

CA	認証機関
CCA	地域認証機関
GCA	総括認証機関
h[＊]	関数 h を[＊]に適用した結果。
X＜＜Y＞＞	X によって生成された Y の認証
Xp	エンティティ X の公開 RSA 鍵
Xs	エンティティ X の秘密 RSA 鍵
Xp[＊]	Xp による[＊]の暗号化／復号。RSA の場合はべき乗演算。
Xs[＊]	Xs による[＊]の暗号化／復号。RSA の場合はべき乗演算。

5.2　システムの設定

ここで規定しているシステムは 3 層の階層からなる。最下層はオーディオビジュアルサービスのユーザである。各ユーザは、他ユーザと通信中には中間層にある CA の内ただ一つと関係がある。中間層にある CA はユーザのグループ（通常同じ地域やネットワークドメインのユーザ）に対する認証機関としてはたらく。これらの CA は、CCA（地域認証機関）と呼ばれ、関連のあるユーザに認証子を発行する。最上層には GCA（総括認証機関）と呼ばれる単一の CA がある。GCA は全ての CCA に対して認証子を発行する。階層を図 6／JT-H234 に示す。

認証のシステムでは RSA アルゴリズムを使う。これは暗号化と復号の鍵が異なる、いわゆる公開鍵アルゴリズムである。鍵のうち一方が秘密であるのに対してもう一方の鍵は公開することができる。これらの鍵はそれぞれ秘密鍵と公開鍵と呼ばれる。

認証にはハッシュ関数 h[＊]を使う。この関数は圧縮機能を持っており任意の長さの文列を決められた長さの文字列に写像する。この決められた長さは使っている RSA 係数の長さを越えてはならない。この関数 h[＊]は認証機関によって規定されるべきものであり、この勧告では規定しない。一般に利用できるハッシュ関数の例を付録 1 の参考文献に記す。

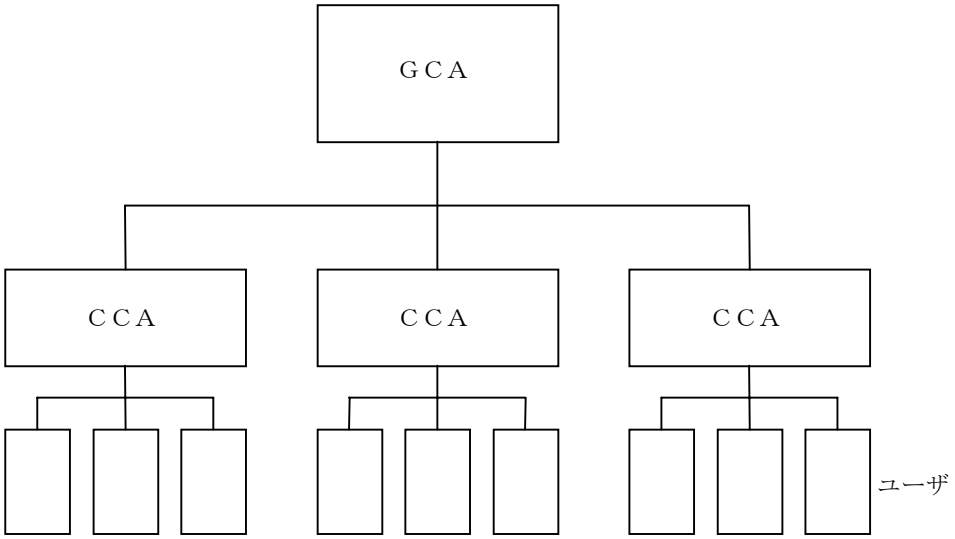


図 6／JT－H234　認証機関の階層

5.3　認証鍵の生成と配送

ＲＳＡアルゴリズムにおいて認証鍵は秘密鍵と公開鍵の組からなる。各ＣＡと各ユーザは各々の認証ペアを持っている。

GCA は秘密鍵 GCAs と公開鍵 GCAp とから構成される自身の認証鍵を生成する。

それぞれの CCA は秘密鍵 CCAs と公開鍵 CCAp とから構成される自身の認証鍵を生成する。CCA は CCAp を GCA に使えるようにして GCA がこの鍵を確認する。

秘密鍵 Us と公開鍵 Up とで構成されるユーザ U の認証鍵は CCA によって生成される。Up と Us とはユーザが使用できる。CCA は Up を認証する。

GCA の認証鍵の生成と CCA の認証鍵の生成と配送は国際的な同意があるべきである。

注：認証機関とユーザとの間の物理的インターフェースはこの勧告の範囲外である。

5.4 認証

GCA は認証子を計算して公開鍵 CCAp を確認する。認証子とは次の情報からなるもので GCA＜＜CCA＞＞と書く：

GCA＜＜CCA＞＞：GCA, CCA, CCAp, T1, GCAs, [h(GCA, CCA, CCAp, T1)]

ここで　GCA　＝　GCA の ID
　　CCA　＝　CCA の ID
　　CCAp　＝　CCA の公開鍵
　　T1　＝　認証子の効力の開始と終了の日付
　　GCAs[＊]　＝　鍵 GCAs を使って＊を暗号化したもの

注：ここで示しているシステムにおいては GCA の ID は一意に決定されるが、X．509 に適合するように含めている。

CCA は認証子を計算してユーザ X の公開鍵 Xp を確認する。認証子とは次の情報からなるもので CCA＜＜X＞＞と書く。

CCA＜＜X＞＞：CCA, X, Xp, T2, CCAs, [h(CCA, X, Xp, T2)]

ここで　CCA　＝　CCA の ID
　　X　＝　X の ID
　　Xp　＝　X の公開鍵
　　T2　＝　認証子の効力の開始と終了の日付
　　CCAs[＊]　＝　鍵 CCAs を使って＊を暗号化したもの

GCAp、GCA＜＜CCA＞＞及び CCA＜＜X＞＞は Xs と一緒に存在しエンティティ X により使えるようになる。例えばスマートカードやハードウエアモジュールに組み込んだ形で実現される。また X は GCAp のハードコピーを持つべきである。こうすると GCAp が正しいかどうか疑わしい場合の参照に利用できる。

認証子の検証：GCA＜＜CCA＞＞は GCAp を使って h（GCA, CCA, CCAp, T1）を計算しこれと GCAp［GCAs［h（GCA、CCA、CCAp、T1）］］とを比較し等しいことを確認することで検証できる。CCA＜＜X＞＞は CCAp を使って h（CCA、X、Xp、T2）を計算し、これと CCAp［CCAs［h（CCA、X、Xp、T2）］］とを比較し等しいことを確認することで検証できる。

5. 4 節で述べた構造を図 7／JT-H234 に要約する。ここではユーザを X と Y とし、認証機関を各々CA1 と CA2 としている。

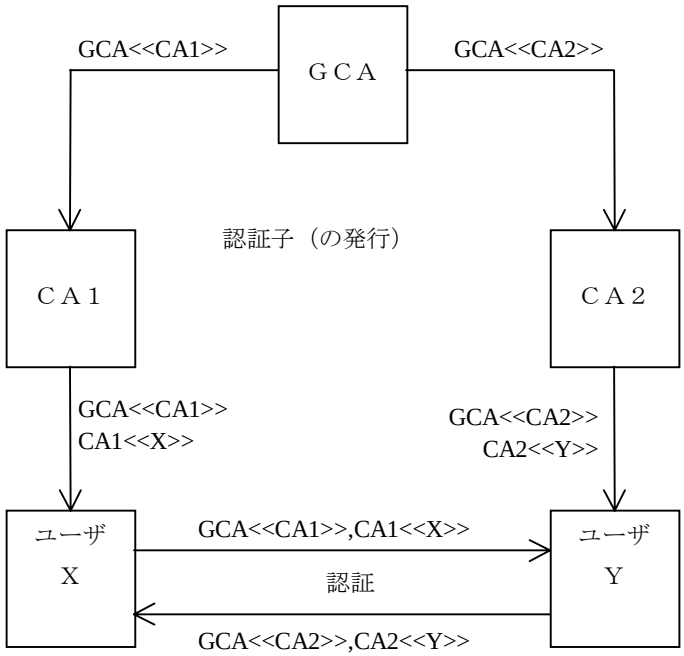


図 7／JT-H234　認証手続きの概略

5.5　GCA を使わない別の認証方法

もし 2 つのネットワークのオペレータ／会社が彼らのユーザを互いに認証する場合、認証機関 CA1 と CA2 は認証子 CA1＜＜CA2＞＞と CA2＜＜CA1＞＞とを交換することにより、互いを確認しなければならない。このシステムは運用の上では複雑なものである、というのはユーザ X と Y は CA1＜＜CA2＞＞または CA2＜＜CA1＞＞を得るために外部のディレクトリに入らなければならず、前もって認証機関の ID を交換しなければならないからである。これは図 8／JT-H234 に詳しく述べてある。

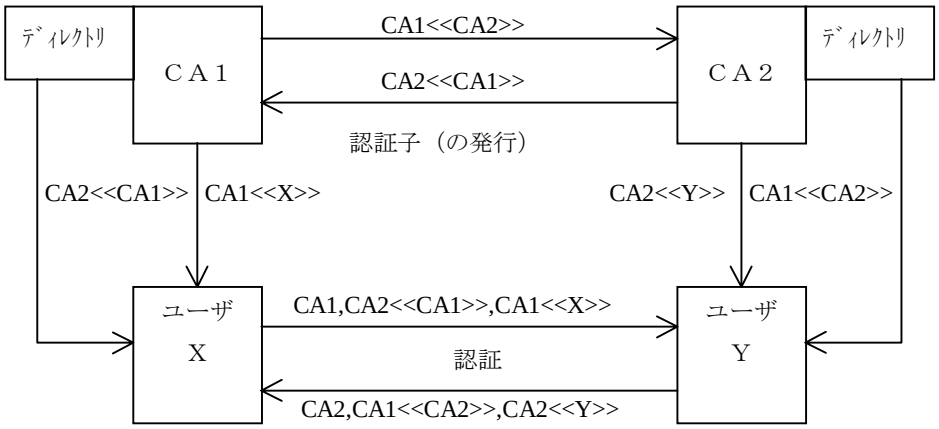


図 8／JT-H234　高位の認証機関が無い場合の認証

5.6 エンティティの認証

以下に認証の手順を詳しく述べる。これは可能なすべての接続、すなわち MCU－MCU、端末－MCU、MCU－端末、端末－端末に適用される。

呼の確立時における 2 つのエンティティ間の認証の手順は 4 つのメッセージを伴う：

RSA. P1－認証開始
RSA. P2－認証応答
RSA. P3－認証完了
RSA. P4－認証失敗

RSA. P1 と RSA. P3 は X で示される発呼側エンティティにより送られ、RSA. P2 は Y で示される着呼側エンティティにより送られる。X と Y の CCAs はそれぞれ CX と CY で示される。

RSA. P1 の内容は、GCA＜＜CX＞＞, CX＜＜X＞＞, RX, Y, Xs［h（RX, Y）］である。ここで RX は X により生成された乱数である。

Y は、（1） RSA・P1 から X p を受け取り、GCAp を有した認証子を信用できるものとしてこれを使って X p を確認。
（2） メッセージが正しいことを確認。すなわち h（RX, Y）を計算し、これと Xp［Xs［h（RX, Y）］］とを比較して等しいことを確認する。
（3） 認証子の満了日を確認。
（4） X が正しいことを確認。

RSA. P2 の内容は、GCA＜＜CY＞＞,CY＜＜Y＞＞, RY, X, RX, Xp［KY］, Ys［h（RY,X,RX,KY）］である。ここで RY は乱数、KY は鍵データ（2. 3. 2 節を参照）で、ともに Y により生成される。

X は、（1） RSA・P2 から Yp を受け取り、GCAp を有した認証子を信用できるものとしてこれを使って Yp を確認。
（2） Xp［KY］を復号し、KY を得る。
（3） メッセージが正しいことを確認。すなわち h（RY、X、RX、KY）を計算し、これと Yp［Ys［h（RY、X、RX、KY）］］とを比較して等しいことを確認。
（4） 認証子の満了日を確認。
（5） RX が RSA. P1 で送ったものと同じであることを確認。
（6） Y が正しいことを確認。

RSA. P3 の内容は、RY、Y、Yp［KX］、Xs［h（RY、Y、KX）］である。
ここで KX は X により生成された鍵データである。

Y は、（1） Yp［KX］を復号し、KX を得る。
（2） メッセージが正しいことを確認。すなわち h（RY、Y、KX）を計算し、これと Xp［Xs［h（RY、Y、KX）］］とを比較して等しいことを確認。
（3） RY が RSA. P2 で送ったものと同じであることを確認。
（4） X が正しいことを確認。

もし RSA．P1、RSA．P2 または RSA．P3 のいずれかの検証が失敗した場合、メッセージ RSA．P4（認証失敗）を送ることで呼の確立は中断される。RSA．P4 は RSA．P1、RSA．P2、RSA．P3 のいずれかの後に X と Y のどちらからも送ることができる。メッセージ RSA．P4（認証失敗）を送ると呼の確立の手続きが打ち切られる。

注：特別な公開パラメータを選ぶことにより RSA の計算速度を上げることが可能である。

注：この構造は、KX が RSA．P1 ではなく RSA．P3 で送られる点で本来の X.509 とは異なっている。こうすると X はディレクトリから Yp を得る必要がないという利点がある。X と Y の双方にとって GCAp は唯一の信頼できるものである。この鍵が信用され、エンティティの秘密情報が盗まれないと信用されている限り、X と Y はディレクトリにアクセスする必要はない。同様に RSA．P3 においては安全のために Y の ID が付加され、RSA．P2 と RSA．P3 においては署名はそれぞれ暗号化されていない鍵データ KY と KX 上に存在する。

5.6.1　RSA．P1 メッセージの同時伝送

もしエンティティ X がエンティティ Y へ認証開始メッセージ RSA．P1（X→Y）：GCA＜＜CX＞＞、CX＜＜X＞＞、RX、Y、Xs［h（RX、Y）］を送り、さらに Y が RSA．P2（X→Y）を受信する前に X へ認証開始メッセージ RSA．P1（Y→X）：GCA＜＜CY＞＞、CY＜＜Y＞＞、RY、X、Ys［h（RY、X）］を送った場合、X と Y は RX と RY を比較することでこの事態を解決することができる。

RX＞RY なら、メッセージ RSA．P1（Y→X）は無視され、Y はメッセージ RSA．P2 で応答する。

RY＞RX なら、メッセージ RSA．P1（X→Y）は無視され、X はメッセージ RSA．P2 で応答する。

RX＝RY なら、両方のメッセージ RSA．P1 は無視され、認証手順はメッセージ RSA．P4（認証失敗）を送って終了する。

5.7　セッション鍵の暗号化のための鍵の生成

メッセージ RSA．P2 と RSA．P3 で送られる鍵データ KY と KX は共通＜鍵＞K を確立するために使用される。そして K は§2．3．2 に記述されているようにセッション鍵配送メッセージを暗号化するために使用される。（これらのメッセージから 4 個 1 組のセッション鍵が得られるが）K の長さが N だとすると、K は KX の第 64 ビットから第（64＋N－1）ビットまでと KY の第 64 ビットから第（64＋N－1）ビットまでの剰余 2 の加算によって求められる（第 0 ビットは KX と KY の LSB を示す）。KX の第 64 ビットと KY の第 64 ビットから K の第 0 ビットが生成される。N の値は＜鍵＞の長さであり、使用される暗号化アルゴリズムによって決定される。

KX と KY の未使用ビット（第 0 ビットから第 63 ビットまでと第（64＋N）ビットとそれ以上のビット）はランダムな情報が詰められる。KX と KY からの共通鍵 K の生成を図 9／JT-H234 に示す。

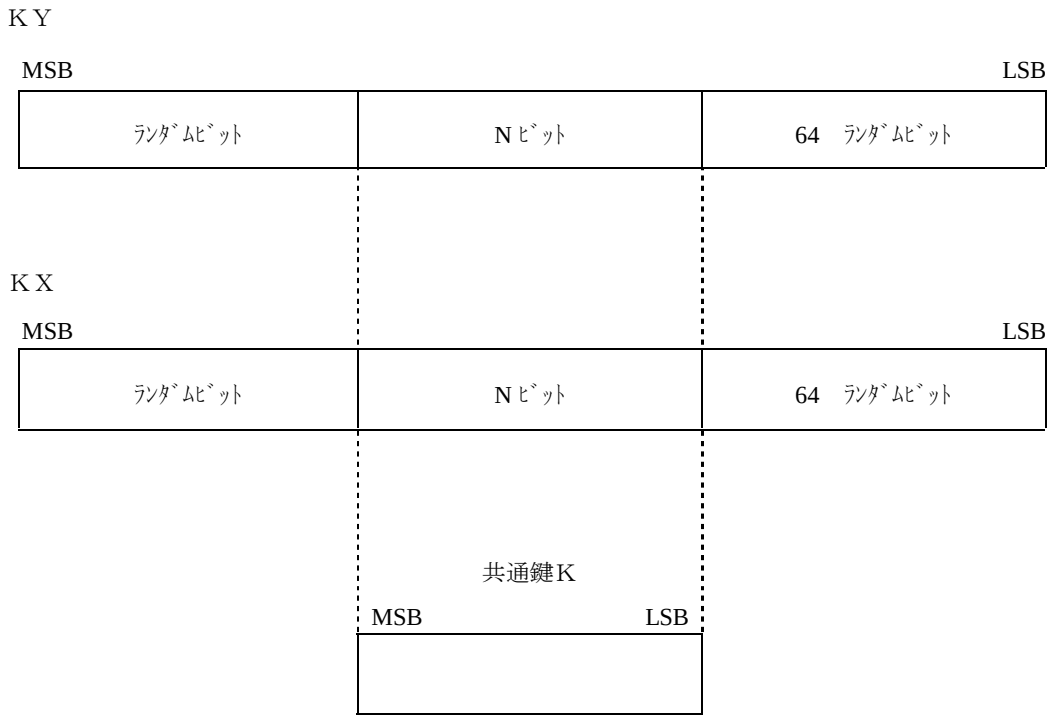


図 9／JT-H234　共通＜鍵＞の生成

（共通鍵 K は KX と KY の N ビットのブロックの剰余 2 の加算により生成。）

5.8 RSA メッセージ

この節では 5．6 節で記述した RSA に基づいた認証方法に必要なメッセージの内容について詳述する。この記述は ITU-T 勧告 X．209 に基づいている。この節で使われているいくつかの X．209 の定義は 2．1 節に簡単に述べてある。

5.8.1 認証開始

メッセージ名	認証開始（RSA.　P1）
メッセージ識別子	$10Pt_1t_2t_3t_4t_5$ = 10100111
意味	意図した受信者と認証手続きを始めたいときにこのメッセージを送信し、手続きを始めるのに必要な情報を送る。
内容	2つの構文形式である認証子GCA＜＜CX＞＞および3つの基本形式である乱数RX、IDナンバーY、ハッシュ関数で圧縮された暗号化情報Xs［h（RX，Y）］からなる構文形式。
ASN．1の表記法	RSA．P1 ::=［7］IMPLICIT SEQUENCE｛ GCA-certificate-for-CCA［0］IMPLICIT GCA-Certificate, CCA-certificate-for-entity［1］IMPLICIT CCA-Certificate, calling-entity-random-number［2］IMPLICIT BIT STRING, called-entity-identity［3］IMPLICIT BIT STRING, hashed-information-in-calling-secret-key［3］IMPLICIT BIT STRING}

発呼側エンティティの乱数（Calling-Entity-Random-Number）、着呼側エンティティの ID（Called-Entity-Identity）、発呼側秘密鍵中のハッシュ関数で圧縮された暗号化情報（Hashed-Information-In-Calling-Secret-Key）の内容はいずれも基本形式ビット列である。

GCA-Certificate-For-CCA の内容：GCA の ID、CCA の ID、公開鍵 CCAp、有効期間 T1、ハッシュ関数で圧縮された暗号化情報 CCAs［h（GCA，CCA，CCAp，T1）］の 5 つの基本形式からなる構文形式。

ASN．1 表記法では、

```
GCA-certificate ::= SEQUENCE {GCA-identity［0］IMPLICIT BIT STRING,
                    CCA-identity［1］IMPLICIT BIT STRING,
                    CCA-public-key［2］IMPLICIT BIT STRING,
                    certificate-valid-date-range［3］IMPLICIT BIT STRING,
                    hashed-information-in-GCA-secret-key［4］IMPLICIT BIT STRING}
```

GCA の ID（GCA-Identity）、CCA の ID（CCA-Identity）、CCA の公開鍵（CCA-Public-Key）、確認された有効期限（Certificate-Valid-Date-Range）、GCA の秘密鍵中のハッシュ関数で圧縮された暗号化情報（Hashed-Information-In-GCA-Secret-Key）はいずれも基本形式ビットである。

CCA-Certificate-For-Entity の内容：送信データは CCA の ID、エンティティ X の ID、公開鍵 Xp、有効期間 T2、ハッシュ関数で圧縮された暗号化情報 CCAs［h（CCA，X，Xp，T2）］の 5 つの基本形式からなる構文形式。

ANS．1 の表記法では、

CCA-Certificate ::= IMPLICIT SEQUENCE {CCA-Identity［0］IMPLICIT BIT STRING,
entity-identity［1］IMPLICIT BIT STRING,
entity-public-key［2］IMPLICIT BIT STRING,
certificate-valid-date-range［3］IMPLICIT BIT STRING,
hashed-information-in-CCA-secret-key［4］IMPLICIT BIT STRING}

CCA の ID（CCA-Identity）、エンティティの ID（Entity-Identity）、エンティティの公開鍵（Entity-Public-Key）、確認された有効期限（Certificate-Valid-Date-Range）CCA の秘密鍵中のハッシュ関数で圧縮された暗号化情報（Hashed-Information-In-CCA-Secret-Key）はいずれも基本形式ビット列である。

5.8.2 認証応答

メッセージ名	認証応答（RSA.　P2）
メッセージ識別子	$10Pt_1t_2t_3t_4t_5$ =10101000
意味	ﾒｯｾｰｼﾞの送り手が認証開始に反応して認証手続きに必要な情報を送る。
内容	2つの構文形式である認証子GCA＜＜CY＞＞，CY＜＜Y＞＞と、5つの基本形式であるRY，XのID，乱数RX，鍵情報Xp［KY］，ハッシュ関数で圧縮された暗号化情報Ys［h（，X，RX，KY）］からなる構文形式。
ASN．1の表記法	RSA．P2 ::=［8］IMPLICT SEQVENCE { GCA-certificate-for-CCA［0］IMPLICIT GCA-Certificate, CCA-certificate-for-entity［1］IMPLICIT CCA-Certificate, called-entity-random-number［2］IMPLICIT BIT STRING, calling-entity-identity［3］IMPLICIT BIT STRING, Calling-Entity-Random-Number［4］IMPLICIT BIT STRING, key-information-in-calling-public-key［5］IMPLICIT BIT STRING, hashed-information-in-called-secret-key［6］IMPLICIT BIT STRING}

着呼側エンティティの乱数（Called-Entity-Random-Number）、発呼側エンティティの ID（Calling-Entity-Identity）、発呼側エンティティの乱数（Calling-Entity-Random-Number）、発呼側公開鍵中の鍵情報（Key-Information-In-Calling-Public-Key）、着呼側秘密鍵中のハッシュ関数で圧縮された暗号化情報（Hashed-Information-In-Called-Secret-Key）はいずれも基本形式ビット列である。

GCA-Certificate-For-CCA と CCA-Certificate-For-Entity は 5．8．1 節での表記法と同様である。

5.8.3 認証完了

メッセージ名	認証完了（RSA.　P3）
メッセージ識別子	$10Pt_1t_2t_3t_4t_5$ =10101001
意味	認証手続きの起動者であるメッセージの送り手が認証手続きを完了するため情報を送信する。
内容	乱数RY，YのID，暗号化された鍵情報Yp［KX］，ハッシュ関数で圧縮された暗号情報Xs［h（RY，Y，KX）］の4つの基本形式からなる構文形式。
ASN．1の表記法	RSA．P3 ::=［9］IMPLICIT SEQUENCE { called-entity-random-number［0］IMPLICIT BIT STRING, called-entity-identity［1］IMPLICIT BIT STRING, key-information-in-called-public-key［2］IMPLICIT BIT STRING, hashed-information-in-calling-secret-key［3］IMPLICIT BIT STRING}

着呼側エンティティの乱数（Called-Entity-Random-Number）、着呼側エンティティの ID（Called-Entity-Identity）、着呼側公開鍵中の鍵情報（Key-Information-In-Called-Public-ey）、発呼側秘密鍵中のハッシュ関数で圧縮された暗号化情報（Hashed-Information-In-Calling-Secret-Key）はいずれも基本形式ビット列である。

5.8.4 認証失敗

メッセージ名	認証失敗（RSA.　P4）
メッセージ識別子	$10Pt_1t_2t_3t_4t_5$ =10101010
意味	認証手続き中に何かを誤ったり認証手続きを終結することを伝えるときこのメッセージを送信する。このメッセージの送信または受信にあたり呼接続終了を起動する。
内容：	本メッセージは内容のオクテットを含まない。

６．MCU 動作

信頼できる MCU の場合（MCU への入力信号は全て復号されるため MCU は安全な場所に設置しなければならない。）、各端末と MCU 間の通信は、ポイント・ポイントの回線に対する本勧告に記載の様に暗号化が行われる。明らかに、この方法はアナログ電話回線による会議への電話接続には適用しない。この様な復号を用いない MCU の動作については本勧告では規定しない。

7．参照標準

(1) ISO 規格：ISO 8732　：“Banking-Key management”

(2) ITU-T 勧告：X．209　：“Specification of basic encoding rules for Abstract Syntax Notation One（ASN．1）”．

(3) TTC 標準：JT-H233　：“オーディオビジュアル・サービスのための機密保持システム”．

(4) TTC 標準：JT-H221　：“オーディオビジュアル・サービスにおける 64kbit/s から 1920kbit/s チャネルのフレーム構成”．

(5) TTC 標準：JT-H230　：“オーディオビジュアル・サービスのためのフレーム同期の制御信号と通知信号”．

(6) TTC 標準：JT-H242　：“1920kbit/s までのディジタルチャネルを利用したオーディオビジュアル端末間の通信を設定する方式”．

(7) ITU-T 勧告：X．509　：“The directory-authentication framework”．

付録１

（JT-234 に対する）

参考文献

1. Diffie W and Hellman M :“New Directions in cryptography”, IEEE TransactionsIT-22,6(Nov.1976), pp. 644--654.

2. Rivest R.L, Shamir A. and Adleman L.:“A Method of Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, 21, 2（February1978）, pp. 120-126.

3. “The MD4 Message Digest Algorithm” : RSA Data Security Inc. , Redwood City, California 94065.

付録２

（JT-H234 に対する）

セキュリティシステム用語集（1／2）

authentication	：	認証
Audiovisual Service Entity(AVSE)	：	ｵｰﾃﾞｨｵﾋﾞｼﾞｭｱﾙｻｰﾋﾞｽのエンティティ
certificate	：	認証子
certification	：	認証
certification authority	：	認証機関
common key	：	共通鍵
constructor	：	構文形式
content	：	内容
context specific	：	文脈依存
cryptographic key	：	暗号化鍵
Cryptographic Service Message(CSM)	：	暗号化サービスメッセージ
decryption	：	復号（化）
Diffie-Hellman	：	ディフィーヘルマン
disconnected service message(DSM)	：	サービス切断メッセージ
encryption	：	暗号（化）
entity	：	エンティティ
identifier	：	識別子
indefinite	：	不定長形式
key distribution	：	鍵配送
key-encrypting key	：	鍵暗号化鍵
key exchange	：	鍵配送
Key Distribution Center(CKD)	：	鍵配送センタ
Key Translation Center(CKT)	：	鍵転送センタ
key service message(KSM)	：	鍵サービスメッセージ
keying material	：	鍵の素材
link	：	回線

セキュリティシステム用語集（2／2）

primitive	：	基本形式
primitive root	：	原始根
privacy system	：	セキュリティシステム
public key	：	公開鍵
REK	：	REK
response service message（RSM）	：	サービスメッセージ応答
Request Service（RSI）	：	サービス要求
RSA	：	RSA
secret key	：	秘密鍵
security agency	：	認証機関
session exchange（SE）	：	セッション交換
session key exchange	：	セッション鍵配送
shared key	：	共有鍵

ＴＴＣ標準作成協力者　（平城 6 年 11 月 30 日現在）

（ＪＴ－Ｈ２３４　第 1 版）

第五部門委員会

部門委員長	高橋　　修	富士通(株)	
副部門委員長	斎藤　慧一	沖電気工業(株)	
副部門委員長	藤本　　功	三菱電機(株)	
委　員	工藤　　暁	キヤノン(株)	（平城 6 年 8 月工藤　暁氏の後任）
〃	早崎　博之	三洋電機(株)	
〃	福崎　和廣	シャープ(株)	
〃	吹抜　洋司	(株)東芝	
〃	鈴木　俊郎	(株)日立製作所	
〃	吉田　　功	東京電力(株)	
〃	西谷　隆夫	日本電気(株)	（5-1 専門委員長）
〃	林　　伸二	日本電信電話(株)	（5-1 副専門委員長）
〃	後藤　道代	松下電器産業(株)	（5-1 副専門委員長）
〃	小寺　　博	日本電信電話(株)	（5-2 専門委員長）
〃	和田　正裕	国際電信電話(株)	（5-2 専門委員長、兼 AVS 特別専門委員長）
〃	大久保　栄	日本電信電話(株)	（AVS 副専門委員長）

第五部門委員会第二専門委員会

専門委員長	小寺　　博	NTT　(株)
副専門委員長	和田　正裕	KDD　(株)
委　員	山中　　治	宇宙通信(株)
〃	内藤　　章	KDD　(株)
〃	岡本　俊郎	東京通信ﾈｯﾄﾜｰｸ(株)
〃	長谷　雅彦	NTT　(株)
〃	江角　　斉	岩崎通信機(株)
〃	本玉　靖和	沖電気工業(株)
〃	森川　重則	カシオ計算器(株)
〃	杉山　　明	キヤノン(株)
〃	西村　利浩	九州松下電器(株)
〃	柿井　栄治	京セラ　(株)
〃	山田　　浩	三星電子ｼﾞｬﾊﾟﾝ(株)
〃	中島　　洋	三洋電機(株)
〃	福崎　和廣	シャープ(株)
〃	平井　秀幸	住友電気工業(株)
〃	矢島　明彦	ｾｲｺｰｴﾌﾟｿﾝ(株)
〃	栗原　　章	ソニー　(株)
〃	小関　吉則	(株)田村電機製作所
〃	南　　重信	(株)東芝
〃	古閑　敏夫	日本電気(株)
〃	岡野　一美	日本無線(株)
〃	後藤　　浩	(株)日立製作所
〃	吉田　雄治	富士通　(株)
〃	前之園敏雄	富士電機(株)
〃	尾形　茂之	松下通信工業(株)
〃	高橋　俊也	松下電器産業(株)
〃	岡　　進	三菱電機(株)
〃	池田　　勇	(株)明電舎
〃	金子　　誠	ヤマハ　(株)
〃	谷川　俊昭	(株)リコー
〃	大谷　暢宏	ﾛｯｸｳｪﾙ ｲﾝﾀｰﾅｼｮﾅﾙ ｼﾞｬﾊﾟﾝ(株)
〃	勝野　進一	長野日本無線(株)
〃	清水　英夫	東京電力(株)

検討グループ（SWG-2）

ﾘｰﾀﾞ	古閑　敏夫	日本電気(株)
	岡本　俊郎	東京通信ﾈｯﾄﾜｰｸ(株)
特	近藤　正宏	沖電気工業(株)
	山田　　浩	三星電子ｼﾞｬﾊﾟﾝ(株)
特	岡田　浩行	シャープ(株)
特	寺岡　心光	(株)東芝
特	北山　浩一	(株)日立製作所
特	臼井　敏彰	富士通(株)
特	斎藤　和正	松下通信工業(株)
特	秋田　康貴	三菱電機(株)
	清水　英夫	東京電力(株)

特：特別専門委員

TTC事務局　田母神昌彦（第５技術部）