TTC 標準
TTC STANDARD

JT-H233
オーデイオビジュアルサービスのための機密保持システム

〔Confidentiality System for Audiovisual Services〕

第2版

1995年11月28日制定

社団法人
情報通信技術委員会

THE 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機密保持方式を規定しており、加速勧告手続きによる郵便投票により、1995 年 7 月に承認されたＩＴＵ－Ｔ勧告H.233 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 ナショナルマター決定項目

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	1993年　４月２７日	制　定
第２版	1995年１１月２８日	ＩＴＵ－Ｔ勧告の変更に伴う追加・変更

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、標準など

ＴＴＣ標準　　：ＪＴ－H221、ＪＴ－H230、ＪＴ－H242、ＪＴ－H234

ＣＣＩＴＴ標準：X.208

ＩＳＯ規格　　：ＩＳＯ／ＩＥＣ 9979

目　　次

１．範　囲

セキュリティシステムは２つの部分からなる。１つは機密保持方法すなわちデータの暗号化処理であり、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 およびＪＴ－H242 に準拠した、狭帯域オーディオビジュアル（ＡＶ）サービスに使用するセキュリティシステムの機密保持について記述する。

暗号化アルゴリズムはこのようなセキュリティシステムに必要であるが、本標準では暗号化アルゴリズムの仕様は含まない。つまり、セキュリティシステムは２つ以上の特定のアルゴリズムに対応する。

この機密保持システムは、端末間または端末と多地点制御装置(ＭＣＵ)間のポイント・ポイント通信に適用できる。ＭＣＵで復号しない多地点会議動作へ拡張するかもしれないが、これは今後の検討課題である。

２．参照標準

［１］ＴＴＣ標準ＪＴ－H221：

オーディオビジュアル・テレサービスにおける 64kbit/s から 1920kbit/s チャネルのフレーム構成

［２］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の通信を設定する方式

［３］ＴＴＣ標準ＪＴ－H230：

オーディオビジュアルシステムのためのフレーム同期の制御信号と通知信号

［４］ＩＴU-T勧告X.208：

Abstract　Syntax　Notation　1

３．略　語

H221	：H.221 フレーム化/フレーム構造	［１］参照
ＦＡＳ	：ＦＡＳ（フレーム同期信号）	［１］参照
ＢＡＳ	：ＢＡＳ（ビットレート割当信号）	［１］参照
ＥＣＳ	：ＥＣＳ（暗号化制御信号）	［１］参照
ＭＬＰ	：マルチレイヤプロトコル論理チャネル	［１］参照
ＣＲＣ４	：4 ビット巡回形冗長性検出	［１］参照
ＭＳＢ	：ＭＳＢ（最下位ビット）	
ＬＳＢ	：ＬＳＢ（最下位ビット）	
ＭＣＵ	：多地点会議制御ユニット	
ＳＥ	：ＳＥ（セッション交換）	
ＩＶ	：ＩＶ（初期化ベクトル）	
ＳＶ	：ＳＶ（開始変数）	
ＩＬＣ	：ＩＬＣ（識別子、長さ、内容）	
ＡＩＭ	：オーディオに関するＣ＆Ｉ符号	［３］参照
ＡＩＡ	：オーディオに関するＣ＆Ｉ符号	［３］参照
ＶＩＳ	：ビデオに関するＣ＆Ｉ符号	［３］参照

４．システムの特性

4.1　機密保持

(1) 機密保持はシステムにより提供される他のセキュリティーサービスとは独立している。鍵はＴＴＣ標準ＪＴ－H234 に記述されているような方法で与えられたり、人手により入力されたりする。

(2) 機密保持は伝送速度ｐ×64kbit/s のＴＴＣ標準ＪＴ－H221 にしたがってフレーム化されたＡＶ信号に適用される。ここでｐは１～３０までの任意の値をとる。ＪＴ－H221 についてはフレーム構造自身は暗号化されない。

(3) 機密保持は、音声・ビデオ・データなどあらゆるユーザ情報の伝送に適用され、これらは同じ鍵を使って暗号化される（ＴＴＣ標準ＪＴ－H221 付属資料Ａによれば、ＭＬＰデータもこれに含まれるが現在検討課題になっている）。

(4) 機密保持システムは、使われている暗号化アルゴリズムとは無関係であり、現在いくつかのアルゴリズムが規定されている。更に他のアルゴリズムも追加可能である。

(5) 機密保持メカニズムはポイント・ポイント通信で可能であり、またＭＣＵにおいて復号が認められている。いわゆる信頼できるＭＣＵを用いる多地点間通信にも使える。

4.2　アルゴリズム仕様

アルゴリズム仕様は本標準には含まれていない。ここでは広い範囲の機密保持アルゴリズムを取り扱う。

アルゴリズム仕様については、どこでも入手できるものでなければならず（5.2 節参照）、以下の項目を含む必要がある。

・初期化ベクトル（ＩＶ）とセッション鍵のビット長

・初期化ベクトルによる開始変数の生成

５．機密保持メカニズム

5.1　動作説明

図 5-1/ＪＴ－H233 は回線暗号装置のブロック図を表す。暗号化器と復号器から構成されている。暗号化器は、入力されたユーザデータを暗号化する。復号器は暗号化されたデータを復号化し元のユーザデータを得る。

暗号化器と復号器の間には２つの通信路（チャネル）がある。１つは暗号化されたユーザデータの伝送に使われる。もう１つは暗号化制御信号（ＥＣＳ）用の暗号化されないチャネルであり、暗号化器から復号器へ制御情報を伝えるために使用される。これら２つのチャネルは物理的に切り離されているように見えるが、実際には１つのデータ列として多重化される。

ストリーム暗号化技術が使用される（5.2 節参照）。

鍵は他の方法で与えられ、要求に応じて機密保持メカニズムに対して提示される。鍵はデータと同期して暗号化器と復号器で用いられる。鍵設定の同期化を示すフラグは制御チャネルを介して送られる（図 5-2／ＪＴ－H233 中のＬ参照）。

データ暗号化は暗号化器から制御される。暗号化オン／オフフラグがデータの暗号化の開始を通知するため、制御チャネルを介して伝送される。復号器はこのフラグに応動し、要求に応じてデータを復号する。

5.1.1　ＪＴ－Ｈ２２１フレームにおける制御と通知

端末に機密保持システムを具備していることを相手端末に通知するために、ＢＡＳコード‘暗号化能力’を伝送しなくてはならない。接続されている両端末からこの能力が伝送された場合、暗号化オンＢＡＳコマンドを用いる事により、暗号化制御信号（ＥＣＳ）チャネルを両方向に開くことができる。暗号化オフコマンドを用いてＥＣＳチャネルを閉じることができるが、この場合、先にＥＣＳチャネル内で暗号化オフフラグを伝送しなくてはならない。仮に、暗号化オフフラグを受ける前に、暗号化オフＢＡＳコマンドを受信した場合、ユーザに対して、第三者の侵入もしくは、機密保持システムに不具合が生じた可能性があることを示す警告が必要となる。

ＪＴ－H221 フレーム構造をとる信号が一方向のみ使用される場合、ＥＣＳチャネルは上記の手続きを用いないで開けられるかもしれない。受信側が選ばれたアルゴリズムその他を復号できるかどうか確認する方法は、本標準の範囲外である。

5.1.2　メッセージフォーマット

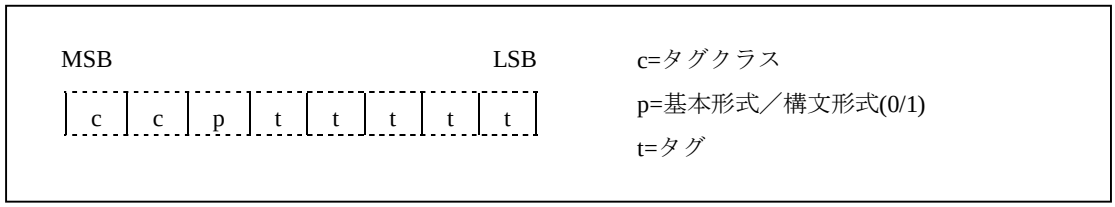
鍵配送や認証に暗号化システムで使用するメッセージは、ＩＴＵ－Ｔ勧告Ｘ．208（［1］参照）記載のＩＬＣ（識別子、長さ、内容）形式でフォーマット化される。ＩＬＣは Identifier（識別子）、Length（長さ）、Content（内容）の頭文字をつらねたものである。

長さは長短いずれかの形式で符号化される。Ｘ．208 記載の不定長形式は使用しない。

本標準で使用するＸ．208 の定義の一部について以下に簡単に説明する。

5.1.2.1　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。



タグクラスは、識別子のタイプを規定するものであり、この標準で定義する識別子では、10（文脈依存）あるいは 11 となる。

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、本標準の識別子はすべて 10Ｐｔ$_1$ｔ$_2$ｔ$_3$ｔ$_4$ｔ$_5$あるいは 11Ｐｔ$_1$ｔ$_2$ｔ$_3$ｔ$_4$ｔ$_5$のオクテット形式を持つ。

5.1.2.2　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、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を符号化する。この場合、ＭＳＢ，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する。この場合、ＭＳＢ，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，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。

5.1.2.3　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数（０から７まで）を符号なしの２進数ビットで示す１オクテットで構成される。これらのＭＳＢ，ＬＳＢは、それぞれビット８とビット１となる。

5.1.3　暗号化されないＥＣＳチャネル

機密保持システムでは、暗号化器と復号器との間で暗号化されない制御チャネルが必要である。回線暗号システム１つにつき、制御チャネルは１つだけ必要である。音声、ビデオ、および存在可能ないかなるデータの暗号化にも、同一の制御チャネルが使用される。

ＥＣＳチャネルはＪＴ－H221 のマルチフレームに同期した、128 ビットのブロックから構成される（図５－２／ＪＴ－H233）。従ってブロックの最初のビットはマルチフレームの第０フレームにおける第 17 オクテットの第８ビットである。ブロックにはセッション交換（ＳＥ）と初期化ベクトル（ＩＶ）の２種類がある。ＩＶブロックに含まれる情報は、次のマルチフレームの開始から有効となり、新しいＩＶが伝送されるまで有効である。ＥＣＳチャネルにはＩＶブロックまたはＳＥブロックのいずれかが必ず含まれる。いくつかのアルゴリズム定義によれば、同一のＩＶを繰り返し使用してよいことが言及されている。繰り返し使用するかしないかの選択は、エラーからのより早い回復と、付加的な機密保持との間のトレードオフに基づくだろう。

ブロックは以下の構成をとる。

(1) ヘッダ（12 ビット）構成

－ビット０：型の選択　　０　＝ＳＥ（セッション交換）
　　１　＝ＩＶ（初期化ベクトル）

－ビット１，２：マルチブロック構成時のブロックの識別
　　００＝単一ブロック、他に付随するブロックはない
　　０１＝複数ブロック連続時の最初のブロック
　　１０＝連続時の中間ブロック
　　１１＝連続時の最終ブロック

－ビット３：ＩＶブロックの場合　暗号化オン／オフ（Ａ）
　　１＝オン
　　０＝オフ

－ビット４，５：ＩＶブロックの場合　ＩＶの長さ（ＣＣ）
　　００＝64 ビット＋誤り訂正 32 ビット
　　０１，１０，１１＝予約済み

－ビット６：ＩＶブロックの場合　鍵設定の同期化（Ｌ）の為に予約

－残りのビット：予備（Ｓ）“０”に設定

－ビット８～１１：ビット０～７用の誤り訂正パリティビット

(2) ＳＥブロック：９×（情報８ビット＋誤り訂正４ビット）の構造をとる
　　108 ビット

ＩＶブロック：誤り訂正（32 ビット）付きの初期化ベクトルまたはその一部（64 ビット）

(3) ＳＥブロック：８ビットの予備

ＩＶブロック：20 ビットの予備－受信情報に従って動作するシステムに対し、一定間隔を提供しているが、将来の拡張にも使用可能である。

5.1.3.1　セッション交換ブロック

ＳＥブロックでは、８＋４ビットのヘッダに続く 116 ビットは９×（８＋４）＋８の構造をしており、最後の８ビットは未使用である。９ワードは、それぞれ情報の８ビットと誤り訂正の４ビットからなる。受信側で、情報ビット（ヘッダに示されるなら２ブロック以上）は、１つのストリームに形成される。それには、認証と鍵管理に関するメッセージや以下に定義するアルゴリズム能力やコマンドに関するメッセージＰ８，Ｐ９が含まれる。

ＳＥブロックの未使用ワードの全 12 ビットは“０”とすること。

アルゴリズム能力（Ｐ８）

メッセージ名　　：復号アルゴリズム能力情報（Ｐ８）

メッセージ識別子　：11Ｐｔ$_1$ｔ$_2$ｔ$_3$ｔ$_4$ｔ$_5$＝11000000

内　　容　　：［３～255 の数］［それに続くバイト］

第一バイトはそれに続くバイトの数を表す。以下に示すメディア識別子、アルゴリズム識別子、パラメータ識別子の３バイトを１組にし、有効は復号アルゴリズムを示す。例えば、端末がＤＥＳとＦＥＡＬの復号能力を有する時は、以下のＰ８メッセージを送信する。

｛［11000000］［00000110］［00000000］［00000010］
［00000000］［00000000］［00000001］［00000000］｝

アルゴリズムコマンド（Ｐ９）

メッセージ名　　：使用アルゴリズム情報（Ｐ９）

メッセージ識別子　：11Ｐｔ$_1$ｔ$_2$ｔ$_3$ｔ$_4$ｔ$_5$＝11000001

意　　味　　：暗号化オンビットが続いてＩＶヘッダでセットされる場合はこのメッセージで設定されたアルゴリズムが使用される。

内　　容　　：暗号方式バイト（アルゴリズム能力メッセージＰ８と同じ値）

メディア識別子

オーディオビジュアル信号のどの要素が暗号化されるのかを１バイトで示す。このバイトの各ビットは次の対応となる。

第１ビット（LSB）：音声　０＝暗号化適用　１＝暗号化未適用
第２ビット　　：ビデオ　０＝暗号化適用　１＝暗号化未適用
第３ビット　　：ＬＳＤ　０＝暗号化適用　１＝暗号化未適用
第４ビット　　：ＨＳＤ　０＝暗号化適用　１＝暗号化未適用
第５ビット　　：ＭＬＰ用に予約　“０”とすること
第６ビット　　：Ｈ－ＭＬＰ用に予約　“０”とすること
第７ビット　　：将来の使用のために予約“０”とすること
第８ビット(MSB)　：将来の使用のために予約“０”とすること

［00000000］は、多重化された信号（ＦＡＳ，ＢＡＳおよびＥＣＳは除く）が暗号化されていることを示す。その他の場合の手続きについては検討中である。

アルゴリズム識別子

アルゴリズムの識別のために、１バイトを用いる。アルゴリズムの定義は、暗号用乱数が現在の鍵とＩＶ値からどのようにして得られるか、その生成法に関する完全な仕様を含む。現在、いくつかのアルゴリズムが認められており、以下のコードが識別に使用される。

ＭＳＢ　　ＬＳＢ	
00000000	未使用、将来のために予約
00000001	ＦＥＡＬ（付属資料ＡのＡ１参照）、ＩＳＯ／ＩＥＣ 9979 アルゴリズム登録 No. 0010
00000010	ＤＥＳ（付属資料ＡのＡ２参照）、モード1、ＩＳＯ／ＩＥＣ 9979 アルゴリズム登録 No. 0004
00000011	ＤＥＳ（付属資料ＡのＡ２参照）、モード２に予約
00000100	ＤＥＳ（付属資料ＡのＡ２参照）、モード３に予約
00000101	Ｂ－ＣＲＹＰＴ、ＩＳＯ／ＩＥＣ　9979 アルゴリズム登録 No. 0001
00000110	ＩＤＥＡ、ＩＳＯ／ＩＥＣ　9979 アルゴリズム登録 No. 0002
00000111	ＢＡＲＡＳ（ＥＴＳＩ）に予約
その他の値	未使用、将来使用のために予約

パラメータ識別子

5.2 節で定義される暗号化アルゴリズムのパラメータを識別するのに、1 バイトを用いる。デフォルト値は［00000000］で、アルゴリズムがパラメータ値を必要としない場合にも使用される。動作パラメータに関しては、付属資料Ａを参照すること。

装置で認められたアルゴリズムのうち、少なくとも１つの復号機能を備えるべきである。もし２つ以上のアルゴリズムを備えている場合、伝送される情報の暗号化のために必要とするアルゴリズムの選択はシステムオペレータに託される。

他のメッセージ

Ｐ１	メッセージ名	：暗号化不能
	メッセージ識別子	：10Ｐ$t_1t_2t_3t_4t_5$＝10000001
	意　味	：この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のオクテットを含まない
Ｐ２	メッセージ名	：暗号化システム開始失敗
	メッセージ識別子	：１０Ｐｔ１ｔ２ｔ３ｔ４ｔ５＝10000010
	意　味	：この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事があり得るが、セキュリティ上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のオクテットを含まない

Ｐ１またはＰ２を送信する必要性が出た場合や、これらのメッセージのいずれかを受信した場合は、ユーザに対して、なんらかの通知を行わねばならない。通知の内容およびその後の動作については、設計者に任される。

5.1.3.2　初期化ベクトル

ＩＶのデフォルト長は 64 ビットで、誤り訂正ビットも含めると 96 ビットとなる。もっと長いＩＶも２つ以上のブロックを使えば伝送可能である。ＭＳＢ（最初のＩＶブロックのビット 12）から伝送する。

5.1.3.3　制御チャネル情報の誤り保護

制御チャネルを通して伝送される情報の誤りは保護されるべきである。［12，８］ハミング符号は、このために用いられる。誤り訂正行列を図５－３／ＪＴ－H233 に示す。

同じ方法をヘッダ、セッション交換、初期化ベクトルに適用する。いずれの場合も８ビット毎の１バイトに４ビットの誤り訂正ビットを付加する。

ＩＶは８ビットに分割されて各バイトの次に４ビットのパリティが付加され、デフォルトの場合、パリティを加えた全体の長さは 96 ビットとなる。

5.2　送信暗号化方法

本節では、音声、ビデオおよび関連するデータの暗号化について扱う。暗号化は、ＪＴ－H221 マルチフレーム同期が確立している場合にだけ実行される。

暗号化システムは、データ速度によらず同じ機能を実行する。全てもしくはその一部のユーザデータが暗号化される。暗号化システムは、様々な形態をしたユーザ情報への容量の割当て情報を必要としない。なぜならば、多重化後にデータを暗号化し、分離前にデータを復号するからである。その二つの送信方向は、独立している。いずれかが、もしくは両方が暗号化されてもよいし、それぞれに異なったアルゴリズムを適用してもよい。

暗号化の時間的順序は、送信のそれに従い、ビット毎にシリアルに処理する。データはＣＲＣ４の計算を実行する前に暗号化しなくてはならない。従ってＣＲＣ４計算は暗号化データに対して実行され、どんな関連するネットワークにも有効なＣＲＣ４コードが与えられることを保証する。ストリーム暗号化法では、暗号用乱数は、現在の鍵と初期化ベクトルより両方の端末で生成される。暗号化器では、暗号化されるデータが暗号用乱数との剰余２の加算により暗号化される。復号器では、もとのユーザ情報を復元するため、暗号化されたビット列に対して同じ暗号用乱数を用いて剰余２の加算がなされる。

初期化ベクトル（ＩＶ）は暗号化器において、ランダムに発生され、ＥＣＳを介して復号器に伝送される。初期化ベクトルは、暗号化または復号されるデータと同期して使われる。これにより暗号化器と復号器は周期的に再同期する。

注）選択されたアルゴリズムによっては、暗号化器と復号器へのＩＶビットの設定順序に注意を払う必要がある。

同期がはずれるとデータは新しい初期化ベクトルを受信するまで誤ったままである。初期化ベクトルの伝送間隔は、再同期までに許容されるデータ損失量により決定される。

暗号化システムによって、チャネル内の各ビットは下記３項のいずれかの方法で扱われる（付録１参照）。

a)　暗号用乱数を生成して、適用する場合：
　　ユーザ情報（音声、ビデオ、データ）

b)　暗号用乱数を生成するが、適用しない場合：
　　第１チャネルと付加チャネルのＦＡＳ、ＢＡＳ（ＴＴＣ標準ＪＴ－H221 参照）とＥＣＳ。暗号用乱数は、引き続き使うために記憶したり遅らせたりすることなく捨てられ、引き続く情報を暗号化するのには使われない。

c) 暗号用乱数を生成しない場合：

伝送路への端末出力が、関連するＢＡＳコマンドで定義された伝送レート以外のチャネルを含むならば（例えば、一次群のＴＳ０やＴＳ16 とか、ポイント・ポイントで送信されることのない他のチャネル）、これらのビットのために暗号用乱数が生成されることはない。

ＴＴＣ標準ＪＴ－H221 付属資料Ｂに述べられている 56kbit/s 伝送に対しては、暗号用乱数が８個のサブチャネルに対して生成されるが、最初の７ビットだけを使用し、７ビット（septet）の信号と剰余２の加算をする。制限付き 128kbit/s やより高ビットレートの伝送でも暗号用乱数は生成されるが、各タイムスロットでスタッフされた第８ビットには適用しない。

5.3 システム使用手順

相手端末の能力セットから“暗号化能力”（ＴＴＣ標準ＪＴ－H221 参照）を受信して、端末が暗号化を開始しようとする場合、まず、ＥＣＳチャネルを開いてメッセージＰ８を送信する。相手はメッセージＰ８を受信して、適合する暗号化アルゴリズム、モードが自端末にあるかを調べ、もしなければメッセージＰ１を返信する。もし適合するものがあれば使用したい暗号化アルゴリズム、モードを決めてメッセージＰ９を返信する。それから、ＩＶブロックの送信を開始する。Ｐ２は失敗回復手順に使用されるかもしれない（今後の検討課題）。

6. マルチレイヤプロトコルの暗号化

今後の検討課題である。

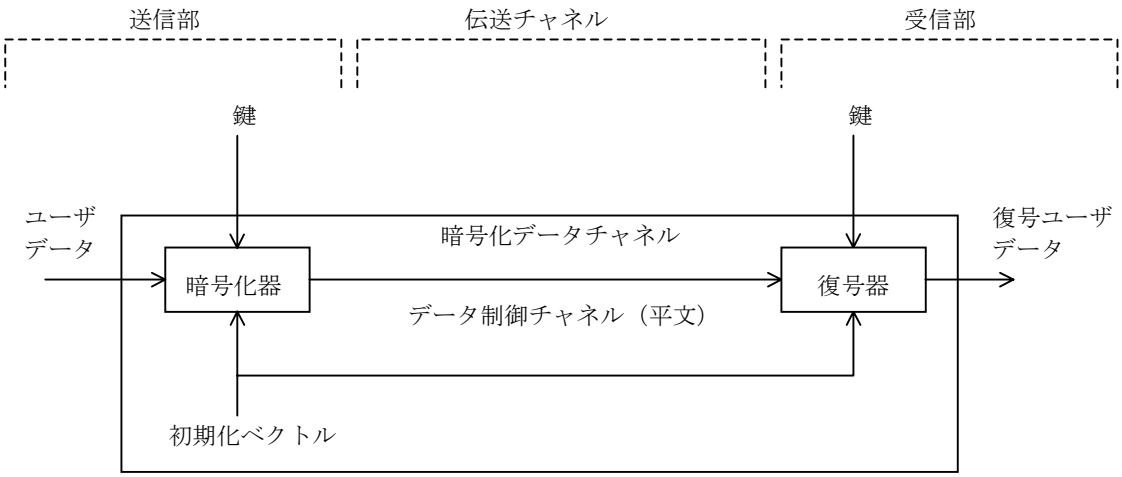


図５－１／ＪＴ－H233　回線暗号装置のブロック図

	ビット番号														
	0	1	2	3	4	5	6	7	8	9	10	11	12-119	120-127	
ＳＥ型	0	n	n	s	s	s	s	s	e	e	e	e	メッセージ	予　備	
	0	1	2	3	4	5	6	7	8	9	10	11	12-107	108-127	
ＩＶ型	1	n	n	A	C	C	L	s	e	e	e	e	メッセージ	予　備	

図５－２／ＪＴ－H233　制御チャネルブロック

生成行列　G

$$\begin{pmatrix} 100000001110 \\ 010000000111 \\ 001000001010 \\ 000100000101 \\ 000010001011 \\ 000001001100 \\ 000000100110 \\ 000000010011 \end{pmatrix}$$

パリティ検査行列　H

$$\begin{pmatrix} 1110 \\ 0111 \\ 1010 \\ 0101 \\ 1011 \\ 1100 \\ 0110 \\ 0011 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{pmatrix}$$

図５－３／ＪＴ－H233　誤り訂正行列

付属資料Ａ（規格）

（ＪＴ－H233 に対する）

暗号化方法の動作パラメータ

A.1　ＦＥＡＬ

暗号用乱数は、現在の鍵と初期化ベクトルの値から、両方の端末で生成される。ＩＳＯ8372 で定義されるＯＦＢ（出力フィードバック：Output Feedback）モードでのＦＥＡＬ－８（鍵が 64 ビットの８段ＦＥＡＬ）を使用する。ＦＥＡＬアルゴリズムの詳細は、参考文献［Ａ１］を参照すること。暗号化器ではこの乱数と暗号化されるデータとの剰余２の加算がされ、復号器では暗号化されたデータと暗号化器と同じ暗号用乱数とが剰余２の加算をされ、元のユーザ情報を復元する。付図Ａ－１／ＪＴ－H233 参照。

開始変数（ＳＶ）は、初期化ベクトル（ＩＶ）に等しい。初期化ベクトルはすべてのマルチフレームの最初にセットされる。

暗号化アルゴリズムに従って出力される 64 ビットのうち、ＭＳＢ側の最初の８ビットを使用し、オーディオビジュアル信号の８ビットと剰余２の加算をする。暗号化ブロックの第１ビットは信号ブロックの第１ビットと剰余２の加算をされ、結果はチャネルを通して、第一番目に伝送される。暗号化ブロックの第２ビットは、信号ブロックの第２ビットと剰余２の加算をされ、結果はチャネルを通して、その次に伝送され、以下同様に続く。８ビットすべてが伝送されると、次の暗号用乱数が生成され暗号化に使用される。

A.2　ＤＥＳ

ＤＥＳのアルゴリズムおよびデータ列への暗号用乱数の適用方法が、参考文献［Ａ２］に記述されている。

ＤＥＳモード１は、ＯＦＢ－８およびＯＦＢ－６４と呼ばれる２つの方法のうち１つを使用する。その開始変数（ＳＶ）は、初期化ベクトル（ＩＶ）に等しい。

パラメータ識別子は、以下の通り設定する。

フィールド値		ＯＦＢモード	ビット数
ＭＳＢ	ＬＳＢ		
0000	0000	ＯＦＢ－８	8
0000	0001	ＯＦＢ－64	16

上記以外の全ての値は、今後の検討課題のために予約されている。

ＤＥＳモード２およびＤＥＳモード３は、今後の検討課題である。

A.3　ＩＤＥＡ

ブロック暗号化アルゴリズムのＩＤＥＡは、64 ビットの入力および出力ブロックを用いて動作する。そして、ＩＤＥＡは、128 ビットの暗号鍵で制御される。ＩＤＥＡは、参考文献［Ａ３］で定義されている。ＩＳＯ8372 によれば、暗号用乱数を生成する動作モードは、Output Feedback　ＯＦＢ－８である。その開始変数（ＳＶ）は、初期化ベクトル（ＩＶ）に等しい。

データ列への暗号用乱数の適用方法は、ＩＳＯ8372 で定義されているＯＦＢと本質的に同じである。

８個のデータビット列を暗号化するために使用される８個の暗号用乱数ビット列は、参考文献［Ａ３］の図１に図示されている 64 ビットの出力ブロックのもっとも左のビット列である。

本動作モードでは、パラメータ識別子（5.1.3.1 節参照）は、［00000000］に設定する。

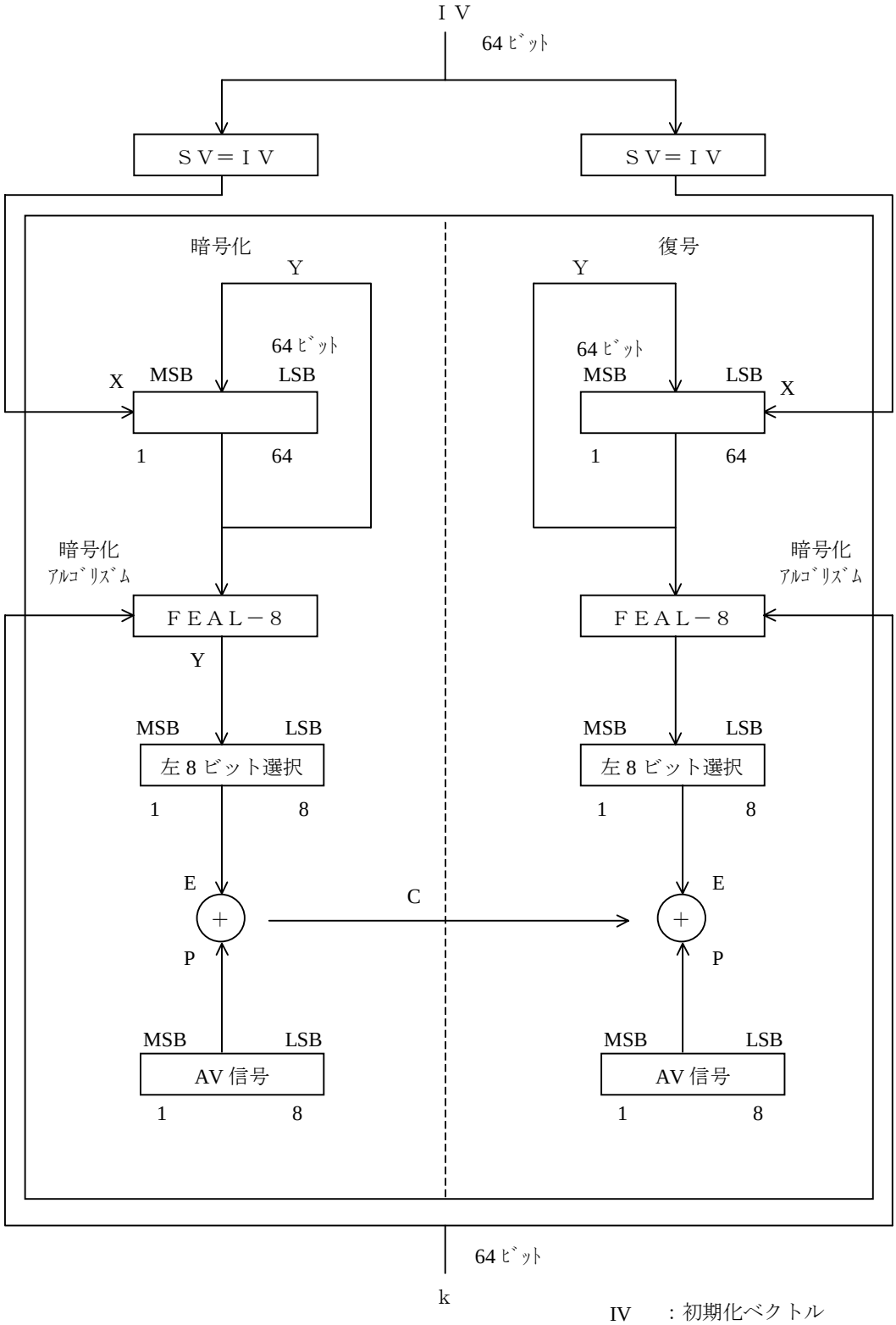
ＩＳＯ8372 で記述されている Cipher Block Chaining モードや Cipher Feedback モードのようなその他の動作モードは、今後の検討課題である。

参考文献

［Ａ１］ＩＳＯ／ＩＥＣ　9979　　登録 No.0010（ＦＥＡＬ）

［Ａ２］ＩＳＯ／ＩＥＣ　9979　　登録 No.0004（Data Encryption Standard）

［Ａ３］ＩＳＯ／ＩＥＣ　9979　　登録 No.0002（ＩＤＥＡ）



IV　：初期化ベクトル
K　：鍵
SV　：開始変数

付図Ａ－１／ＪＴ－H233　　ＦＥＡＬでのＯＦＢ（出力フイードバック：Output Feedback）モード動作

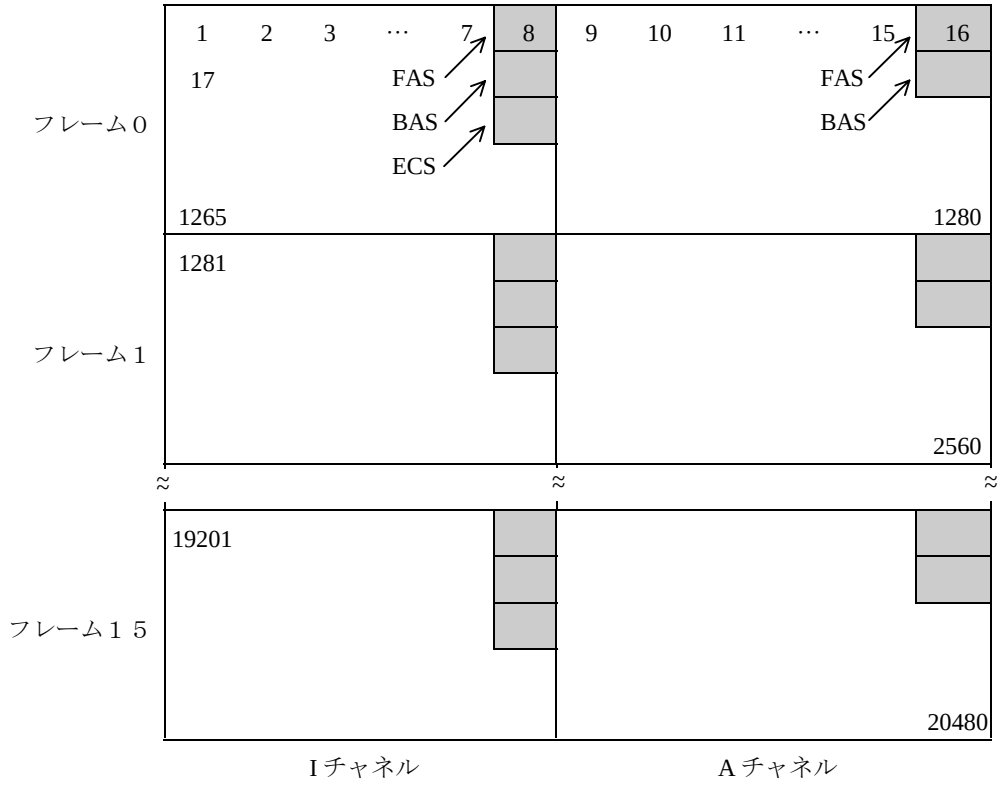
付録１

（ＪＴ－H233 に対する）

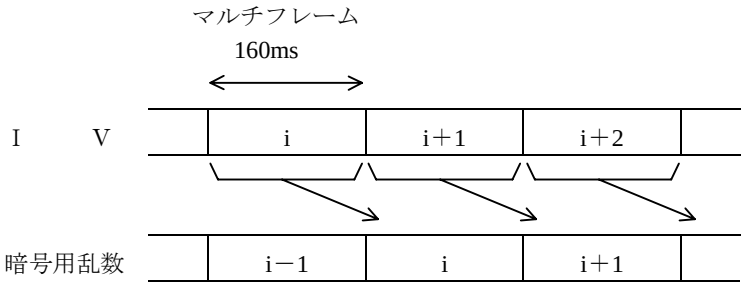
２×Ｂチャネルの暗号化と復号（本付録は、本標準の必須要素ではない）

この付録は、本標準の暗号化、復号がどのように行われるかを図に示すものである。

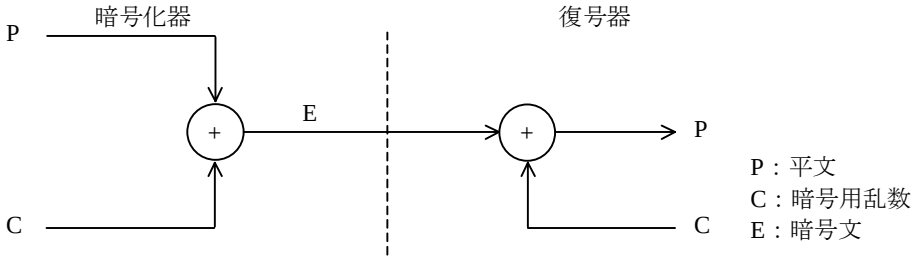
－暗号用乱数は全てのビットに対して生成される。
－暗号用乱数は斜線部を除くビットに対して加算される。



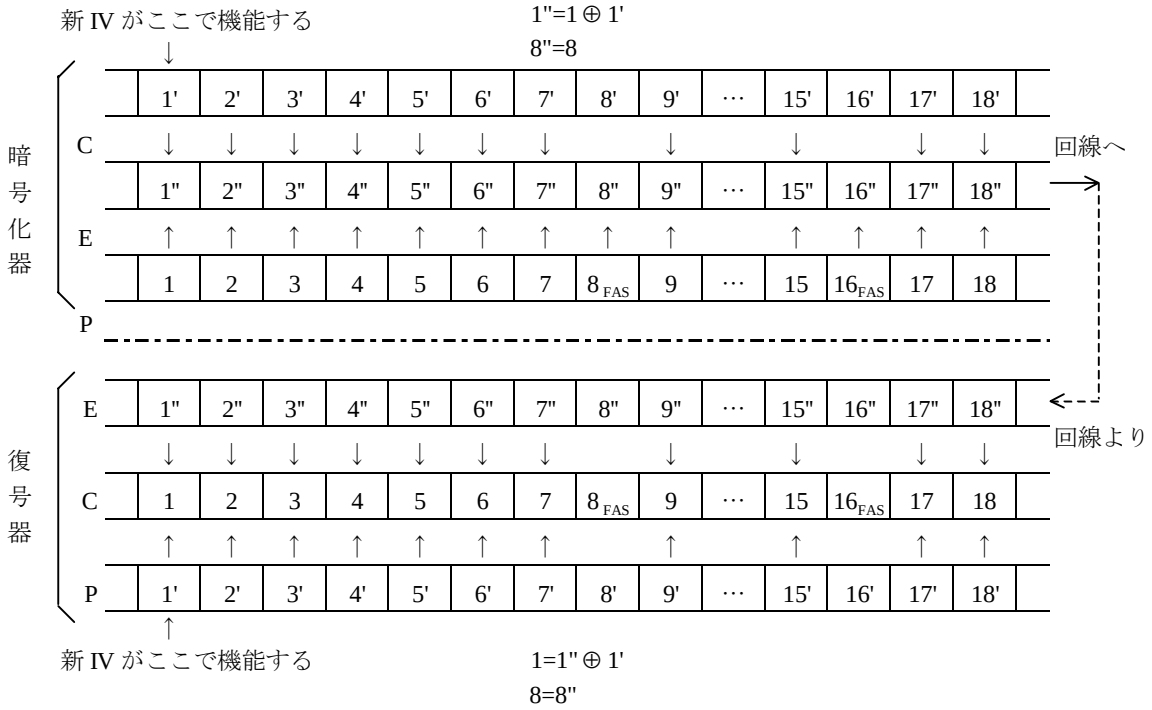
付図１－１／ＪＴ－H233　２×Ｂチャネルのマルチフレームにおけるビットの番号付けと非暗号化ビット



付図１－２／ＪＴ－H233　新しいＩＶからの暗号用乱数の生成



付図１－３／ＪＴ－H233　加算ストリーム暗号



付図１－４／ＪＴ－H233　ビット単位の暗号化と復号

付録２

（ＪＴ－H233 に対する）

オーディオビジュアルセキュリティ通信手順（本付録は、ＪＴ－H233 の必須要素ではない）

オーディオビジュアル通信会議でセキュリティが必要とされる場合、そのオーディオビジュアル通信は、ＴＴＣ標準ＪＴ－H233、ＪＴ－H234 および他のＴＴＣ標準ＪＴ－Ｈシリーズによって成し遂げられる。通信手順の必要な構成要素は、いくつかのＴＴＣ標準で定義されているので、本付録では、これらのＴＴＣ標準を参照しながら手順の一例を規定する。

オーディオビジュアル通信において、セキュリティを開始するためには、２つの場合が考えられる。

(1) 呼が確立し、その通信の中で参加者が暗号化を行うことを決定する場合。

(2) 機密保持メカニズムが完全に操作できるまでオーディオビジュアル通信が起こらないように、外的な手段によって呼設定がされる前に、暗号化を行うことの決定を理解する場合。

以下の表Ａ.１とＡ.２は、セキュリティに焦点を合わせる点において、それぞれ上記二つの場合に該当する。これらの手順は、鍵配送で使用される拡張ディフィーヘルマン方式に時系列的に記述されている。

セキュリティ通信を起動させる場合、オーディオビジュアル信号を実際に暗号化するときのタイミングに特有の注意を払うべきである。特別な方法が標準化されているわけではないが、端末設計では、安全な通信が開始される前に数秒またはそれ以上に対処するための適切な対処方法を組み入れるべきである。

一つの方法として、暗号化された信号が有効になるまで暗号化通信を可能にする（上記（１））ことかもしれないし、別の方法としては、暗号化された信号が有効になるまで全てオーディオビジュアル信号全体を無視する（上記（２））ことかもしれない。どちらの方法でも、暗号化状態がユーザに対して、電気信号または他の手段によって表示されるべきである。

表 A.1　呼設定の後にセキュリティを起動する場合

時間番号	手　　順	メッセージ	使用チャネル	参照及び注釈
1	呼設定	BC/LLC/HLC	D チャネル	JT-Q939
2	音声パス；音声をミュートした場合の AIM の送信；着信音声がミュートされている場合のユーザへの表示；ミュートされている場合の暗号化されていない通常の発信音声の表示	AIM	BAS	JT-H230
3	ECS 能力交換（注 1）	Encrypt-cap	BAS	JT-H242
4	ECS チャネルのオープン（注 1）	Encrypt-on	BAS	JT-H242
5	利用可能な暗号化アルゴリズムの識別	P8	H.233	
6	共通の鍵管理システムの識別	P0	ECS(SE)	JT-H234
7	鍵管理方式の認識後、暗号化アルゴリズムの選択	－	(ﾛｰｶﾙ)	
8	セッション鍵の交換とオーディオビジュアル通信の両方のために選ばれたアルゴリズムの送信	P9		JT-H233 (注 2)
9	素数、原始根と中間結果の交換	P3,P4	ECS(SE)	JT-H234
10	鍵暗号化鍵、r1、r2 及び R12 の計算	－	(ﾛｰｶﾙ)	JT-H234
11	64 ビットの検証符号を 16 桁の 16 進数字での表示	(ﾛｰｶﾙ)	(ﾛｰｶﾙ)	JT-H234
12	口頭による検証（ポイント・ポイント）または、MCU（多地点間通信）からの検証符号情報による 64 ビットの検証符号化；音声がミュートされている場合、口頭による検証は、暗号化が起動される後まで延期することがきる。	16 桁 16 進数	ﾒｲﾝ(ﾎﾟｲﾝﾄ･ﾎﾟｲﾝﾄ)または ECS(多地点間通信)	JT-H234
13	初期化ベクトルと 4N ビットの暗号化乱数の転送	P6	ECS(SE)	JT-H234
14	暗号化オンと初期化ベクトル	ECS 内の A と IV	ECS(IV)	JT-H233
15	暗号化された出力信号のユーザへの表示；検証が自動的でない場合のミュートの解除は、口頭による検証が必要であり、まだ口頭による検証が終了していない場合である。	16 桁 16 進数 AIA	(ﾛｰｶﾙ) BAS ﾒｲﾝﾁｬﾈﾙ	JT-H230 JT-H234
16	暗号化されたオーディオビジュアル通信	ｵｰﾃﾞｨｵ､ﾋﾞﾃﾞｵ その他	ﾒｲﾝﾁｬﾈﾙ	
17	通常でないオーディオ信号、ビデオ信号	AIM,VIS	BAS	JT-H230
18	暗号化オフ	ECS 内の A	ECS(IV)	JT-H233
19	ECS チャネルのクローズ（注 4）	Encript-off	BAS	JT-H242
20	呼切断	－	D ﾁｬﾈﾙ	JT-Q939

注１：　ＪＴ－H242 で定義されているモード初期化手順と共通モード確立手順の一部

注２：　暗号化アルゴリズムと本標準の付属資料Ａで記述されているモードは、セッション鍵交換とオーデイオビジュアル通信の二つで共通的に使われる。

注３：　４Ｎビットの乱数は、手順 10 で決定される鍵暗号化鍵を用いて手順８で決定される暗号化アルゴリズムとこの手順で獲得される初期化ベクトルによって暗号化される。

注４：　ＪＴ－H242 で定義されている通信終了フェーズ手順の一部

表 A.2　呼設定の後にセキュリティの起動を決めた場合

時間番号	手　　順	メッセージ	使用チャネル	参照及び注釈
0	2当事者間でのセキュリティの使用の決定		外的手段	（注0）
1	呼設定	BC/LLC/HLC	Dチャネル	JT-Q939
2	通常でないオーディオ信号、ビデオ信号; 通常でないオーディオ信号または、ビデオ信号を受信した場合、ユーザにその旨を示す。	AIM、VIS	BAS	JT-H230
3	ECS能力交換（注1）	Encrypt-cap	BAS	JT-H242
4	ECSチャネルのオープン（注1）	Encrypt-on	BAS	JT-H242
5	利用可能な暗号化アルゴリズムの識別	P8	ECS(SE)	JT-H233
6	共通の鍵管理システムの識別	P0	ECS(SE)	JT-H234
7	鍵管理方式の認識後、暗号化アルゴリズムの選択	－	(ﾛｰｶﾙ)	
8	セッション鍵の交換とオーディオビジュアル通信の両方のために選ばれたアルゴリズムの送信	P9		JT-H233 (注2)
9	素数、原始根と中間結果の交換	P3,P4	ECS(SE)	JT-H234
10	鍵暗号化鍵、r1、r2及びR12の計算	－	(ﾛｰｶﾙ)	JT-H234
11	64ビットの検証符号を16桁の16進数字での表示	(ﾛｰｶﾙ)	(ﾛｰｶﾙ)	JT-H234
12	MCUからの64ビットの検証符号情報(多地点時)	16桁16進数	ECS	JT-H234
13	初期化ベクトルと4Nビットの暗号化乱数の転送	P6	ECS(SE)	JT-H234 （注３）
14	暗号化オンと初期化ベクトル	ECS内のAとIV	ECS(IV)	JT-H233
15	暗号化された出力信号のユーザへの表示;通常のオーディオ、ビデオによる64ビットの検証符号の口頭による提示（ポイント･ポイント時）	AIA,VIA 16桁16進数	(ﾛｰｶﾙ) BAS ﾒｲﾝﾁｬﾈﾙ	JT-H230
16	暗号化されたオーディオビジュアル通信	ｵｰﾃﾞｨｵ、ﾋﾞﾃﾞｵ その他	ﾒｲﾝﾁｬﾈﾙ	
17	通常でないオーディオ信号、ビデオ信号	AIM、VIS	BAS	JT-H230
18	暗号化オフ	ECS内のA	ECS(IV)	JT-H233
19	ECSチャネルのクローズ(注4)	Encript-off	BAS	JT-H242
20	呼切断	－	Dﾁｬﾈﾙ	JT-Q939

注０：　標準化の範囲外

注１：　ＪＴ－H242 で定義されているモード初期化手順と共通モード確立手順の一部

注２：　暗号化アルゴリズムと本標準の付属資料Ａで記述されているモードは、セッション鍵交換とオーディオビジュアル通信の二つで共通的に使われる。

注３：　４Ｎビットの乱数は、手順 10 で決定される鍵暗号化鍵を用いて手順８で決定される暗号化アルゴリズムとこの手順で獲得される初期化ベクトルによって暗号化される。

注４：　ＪＴ－H242 で定義されている通信終了フェーズ手順の一部

付録３

（ＪＴ－H233 に対する）

セキュリティシステム用語集

additive stream cipher	加算ストリーム暗号
authentication	認証
cipher stream	暗号用乱数
confidentiality	機密保持
constructor	構文形式
content	内容
context specific	文脈依存
decipher	復号する
decipherment	復号
decrypt	復号する
decryption	復号
decryptor	復号器
encipher	暗号化する
encipherement	暗号化
encrypt	暗号化する
encryption	暗号（化）
Encryption capability	暗号化能力
Encryption Control Signal（ECS）	暗号化制御信号
encryptor	暗号化器
identifier	識別子
initialisation vector（IV）	初期化ベクトル
key distribution	鍵配送
key-loading synchronisation	鍵設定の同期化
key management	鍵管理
link encryptor	回線暗号装置
link encryption system	回線暗号システム
plain text	平文
primitive	基本形式
privacy system	セキュリティ　システム
session exchange（SE）	セッション交換
session key	セッション鍵
starting variable（SV）	開始変数

ＴＴＣ標準（平成７年１２月現在）

（ＪＴ－Ｈ２３３　　第２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	矢後　嘉信	沖電気工業(株)	
副部門委員長	藤本　　功	三菱電機(株)	
委　員	大谷　正寿	キヤノン(株)	
〃	細川　義夫	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）
〃	則松　武志	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 副専門委員長 兼　AVS 特別専門委員長）
〃	大久保　栄	(株)ｸﾞﾗﾌｨｯｸｽ･ｺﾐｭﾆｹｰｼｮﾝ･ﾗﾎﾞﾗﾄﾘｰｽﾞ	（AVS 副専門委員長）
〃	大西　廣一	日本電信電話(株)	（VOD 専門委員長）

第二専門委員会（ＪＴ－Ｈ２３３）

専門委員長	小寺　　博	日本電信電話(株)
副専門委員長	和田　正裕	国際電信電話(株)
委　員	南園　健一	宇宙通信(株)
〃	内藤　　章	国際電信電話(株)
〃	岡本　俊郎	東京通信ネットワーク(株)
〃	長谷　雅彦	日本電信電話(株)
〃	江口　忠博	大阪メディアポート（株）
〃	杣　　宗政	岩崎通信機(株)
〃	本玉　靖和	沖電気工業(株)
〃	森川　重則	カシオ計算機（株）
〃	前川　義人	キヤノン(株)
〃	西村　利浩	九州松下電器(株)
〃	柿井　栄治	京セラ（株）
〃	小山田　応一	国際電気(株)
〃	中島　　洋	三洋電機(株)
〃	牧山　健志	シャープ(株)
〃	川西　康之	住友電気工業(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
〃	桐山　　隆	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)
〃	梅崎　一也	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)
〃	大盛	雄司	東京電力(株)

（ＪＴ－Ｈ２３３）

（ＳＷＧ４　検討グループ）

特	緒方	成好	日本電信電話(株)
特	近藤	正宏	沖電気工業(株)
特	萩生田	忠	キヤノン(株)
特	小林	光寿	京セラ(株)
	小山田	応一	国際電気(株)
特	辰巳	正弘	シャープ(株)
特	藤尾	博寿	ソニー(株)
特	遠藤	幸男	日本電気(株)
◎特	北山	浩一	(株)日立製作所
	後藤	浩	(株)日立製作所
特	梅崎	靖	富士通(株)
特	大野	寛之	松下通信工業(株)
特	馬場	昌之	三菱電機(株)
特	長尾	政司	(株)リコー
	勝野	進一	長野日本無線(株)

◎：作業リーダ　　特：特別専門委員

ＴＴＣ事務局　　佃井　彰彦　　（第５技術部）