MBA 標準 0201 号

2004 年 4 月　公開

MIS プロトコル(MISP)仕様書　Ver. 1.02

MBA 標準は、モバイルブロードバンド協会プロトコル分科会が、同協会会員より提案された標準案を審議し、所定の内部手続を経て公開するものである。
この MBA 標準 0201 号は、モバイルブロードバンド協会正会員たるモバイルインターネットサービス株式会社より「MIS プロトコル(MISP)仕様書」として提案された標準案を審議し、所定の手続を経て公開に至ったものである。

モバイルブロードバンド協会

www.mbassoc.org

変　更　履　歴

2002/2/20 地理情報オブジェクトの長さを 12→14 に訂正した。
2002/5/31 上流回線種別オブジェクトの長さを６→８に訂正した。
2006/6/6 編集上の修正。表紙説明文中「標準草案」を「標準」に訂正した。

目次

1. はじめに

MIS プロトコル(MISP)は、基地局ルータと端末を接続するために設計された。

MISP は、IPv4 や IPv6 といったネットワーク層のプロトコルの下位層として動作する。MISP の上位層として同時に複数のプロトコルを扱うことも可能である。MISP の下位層としては、Ethernet、IEEE802.11b などのメディアを使うことができる。

MISP では、接続されたメディア上の基地局ルータを、端末が自ら発見できるような仕組みを備えている。端末は、メディアへ接続されると自動的に基地局ルータを認識し、基地局ルータと間の通信路を確立することができる。この際のセキュリティとして、ユーザ名とパスワードによる認証機能を備える。認証の際には、メディア上でパケットをモニタされても鍵が盗まれることがないように、暗号技術が使われている。さらに、基地局ルータと端末の間で鍵を交換し、通信の各パケットについて、認証および暗号化することができる。MISP による接続は、上位層からは Point-to-Point 接続にみえる。

これらの機能は、無線 LAN 環境を意識して設計されており、無線による公衆サービスに耐えうる安全性を備えている。

2. 用語と概念

2.1. アカウント

MISP を通じてネットワークを利用するための権利。

2.2. アカウント識別子

アカウントを識別するためのバイト列である。長さの上限は 253 バイトとする。

アカウント識別子は RFC2486 に定義された NAI (Network Access Identifier)として使用される。各アカウントは、相異なるアカウント識別子を持つ。

2.3. パスワード

アカウントの認証の際に使用するバイト列である。内部に構造は持たない。長さの上限は 253 バイトとする。

パスワードはアカウント毎の秘密情報である。

2.4. MN

移動端末を指す。「Mobile Node」の略である。

MN は、自由に移動する。各 MN には 1 つのアカウントを設定する。

2.5. BR

基地局ルータを指す。「Base Router」の略である。

BR は固定して設置され、持続的なインターネットへの接続を持っている。MN からの要求に応じて、MN とインターネットの間のルータとして動作する。その際、MN の持つアカウントの正当性を確認する機能を有する。

2.6. AS

認証サーバを指す。「Authentication Server」の略である。

BR の機能のうち、アカウントの正当性を確認する機能を代行することができる。1 つのアカウント識別子とパスワードの対応表を、複数の BR からの要求に対して使うことによって、アカウント識別子と対応するパスワードを集中管理することができる。

2.7. セッション

MN-BR 間で行われる一連の通信を指す。

ある MN-BR 間には、セッションは 1 つだけ存在することができる。セッションは互いに独立

である。つまり、あるセッションの動作は他のセッションには影響しない。

2.8. セッション鍵

セッション毎に作られる鍵である。MN と BR で共有される。1 つのセッションには、同時に、最大 2 つの鍵が存在し得る。セッション鍵は一定時間ごとに更新される。

2.9. 基地局グループ

BR の集合である。BR は、0 以上の基地局グループに属している。
1 つの基地局グループを表現するためには、識別子として 32bit の整数を使う。

2.10. セキュリティ方式

一つのセッション内で使われる、認証方式、鍵配送方式、データ暗号化方式の組を指す。

2.11. メッセージ

MISP のパケットを指す。

2.12. メディア

メッセージを実際に交換するために使う MN と BR の間に存在する仕組みを指す。

2.13. チャンネル

メッセージを実際に交換するために使う MN と BR の間に存在する通信路を指す。
1 つのメディアは、1 つ、または、複数のチャンネルを持つ。メディアの持つチャンネルの数は、メディアにより規定される。

3. MISP の構成

3.1. システム構成

MISP は、MN と BR の間で相互の認証などのために使用される。
BR の背後には MISAUTH サーバが控え MN と BR 間の認証を手助けする。

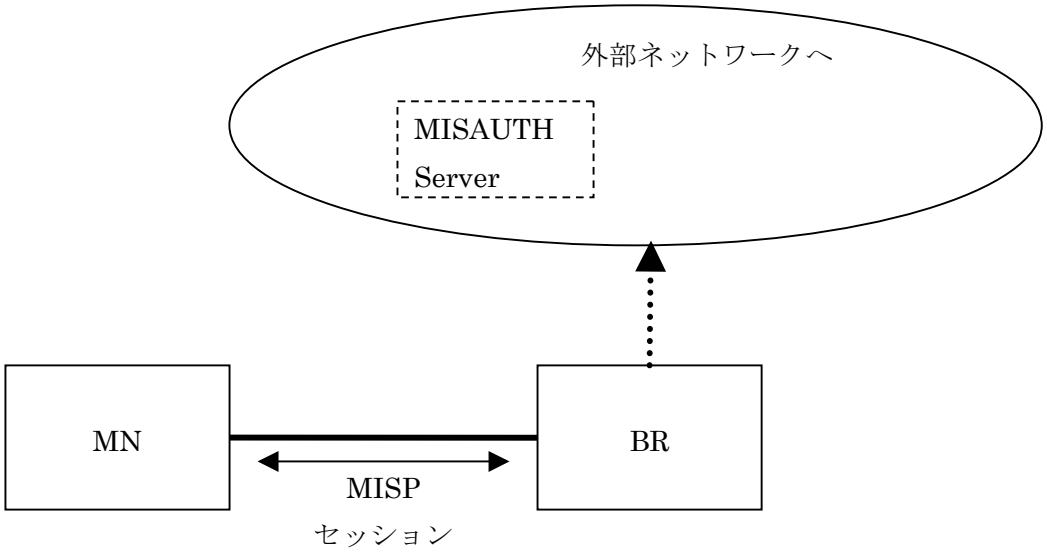

図 1　システム構成

1 台の BR に複数の MN を接続し MN と同じ数のセッションを維持することもできる。1 台の MN が複数の BR に接続し BR と同じ数のセッションを維持することもできる。どちらの場合にも、それぞれの MN と BR の間で使われる MISP のセッションは、すべて独立に動作する。
BR は、外部ネットワークへのリンクを持っていることが想定されており、その場合、MISP より上位層のプロトコルによって、パケットの転送が行われる。MISP 自体は、MN と BR の間でパケットを交換するだけであり、MN や BR に配送されたパケットをさらに転送する機能は持たない。

3.2. プロトコル階層

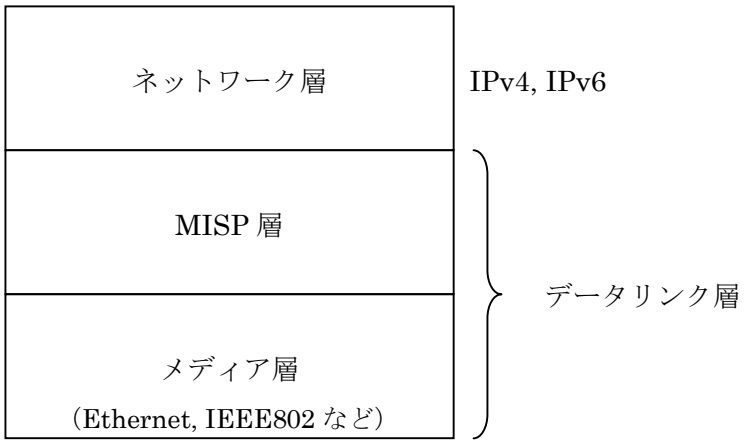

図 2　プロトコル階層

この仕様書では、プロトコル階層の中において、MISP 層のすぐ上に位置する層を「ネットワーク層」と呼び、すぐ下に位置する層を「メディア層」と呼ぶ。

以下では、上下の層に求められる条件について述べる。

3.2.1. ネットワーク層

MISP 層は、ネットワーク層に対してパケットの転送機能を提供する。

このとき、MISP 層は、パケットの正確な長さを保存しない。送信されたパケットよりも、受信されたパケットの長さが短くなることはないが、長くなることがある。その場合、元のパケットの情報は前に詰められ、後ろには不定長の 0 が付加されている。

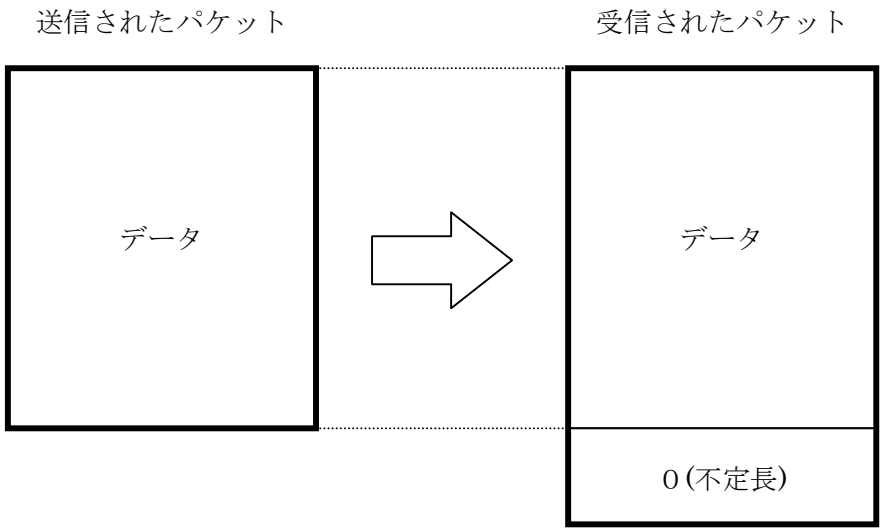

図 3　パケット長の変化

したがって、ネットワーク層で正確なパケット長が必要な場合には、ネットワーク層自身が長さを管理する必要がある。

3.2.2. メディア層

メディア層は「MAC アドレス」を持っていなければならない。

メディア層は、MISP 層から渡されたメッセージを、宛先として MISP 層に指定された MAC アドレスを持つ MN または BR に送信する。また、受信したパケットを、送り元の MAC アドレス情報と共に、MISP 層に伝達する。このとき、次の条件を満たす必要がある。

- メッセージは送り先に指定された MAC アドレスを持つ相手の MISP 層にだけ届く（自分の MAC アドレスでなければメディア層で破棄する）。
- ブロードキャストすることが指定されたメッセージは、可能な範囲で全ての相手の MISP 層に届く。
- 1 回送信したパケットが、2 回以上受信されても良い。
- 送信したパケットが受信されずに失われても良い。

MAC アドレスは、1 バイト以上 128 バイト以下の任意の長さのバイト列である。実際の長さはメディア層により定義される。

また、MAC アドレスは以下の条件を満たす必要がある。

- 互いに通信する MN と BR は異なる MAC アドレスを持つ。

- 1 つのメディア層を通して複数のコネクションが存在する場合、それらのコネクションに関与する全ての MN と BR は、相異なる MAC アドレスを持つ。

MN や BR はグローバルにユニークな MAC アドレスを使わなければならない。

3.3. 機能

MISP には次の機能がある。

- BR から MN への情報の広告
- BR による MN の認証
- MN による BR の認証
- MN と BR とのセッション鍵情報の交換
- ネットワーク層のための情報の交換
- パケットの認証と暗号化

以下で、それぞれ説明する。

3.3.1. BR から MN への情報の広告

BR はビーコンメッセージをブロードキャストして、信号の届く範囲にいる MN に対して、情報を広告する。MN はこのビーコンメッセージを受信して、近くの BR の情報を知る。

3.3.2. BR による MN の認証

BR は、アカウント識別子の入った認証要求メッセージを MN から受信し、そのアカウント識別子に対応するパスワードを使って、MN の正当性を確認する。

3.3.3. MN による BR の認証

MN は、認証成功メッセージを BR から受信し、その情報に基づいて、BR の正当性を確認する。

3.3.4. MN と BR とのセッション鍵情報の交換

MN と BR は、認証要求メッセージと認証成功メッセージの交換を通じて、セッション鍵についての情報を交換し、対となるセッション鍵情報を得る。

3.3.5. ネットワーク層のための情報の交換

MN と BR は、認証要求メッセージと認証成功メッセージの交換を通じて、ネットワーク層のための情報を交換する。

3.3.6. パケットの認証と暗号化

MN と BR は、ネットワーク層のパケットを交換する。その際に、セッション鍵情報に基づいた認証や暗号化の処理を行う。

3.4. セッション

MN-BR 間において、MISP によって結ばれた MN と BR の関係を「セッション」という。
セッションは、1 組の MN と BR につき、1 つだけ存在することができる。
セッションは、認証成功メッセージで始まる。
セッションの終わりは次のいずれかである。

- 有効なセッション鍵がなくなったとき。
- セッション終了メッセージが送信されたとき。
- MN-BR 間で物理的に通信できなくなったと認められたとき。

セッションは、(メディア層, MN の MAC アドレス, BR の MAC アドレス)の組で識別される。
セッションはチャンネルを持つ。
セッションは、1 つのセキュリティ方式を持つ。これが途中で変化することはない。
セッションは、2 つのセッション鍵を持つ。2 つのセッション鍵を区別して述べる場合には、それぞれ、「セッション鍵 A」、「セッション鍵 B」と呼ぶ。

4. メッセージフォーマット

4.1. メッセージの種類

メッセージには、大きく分けて次の 2 つの種類がある。

- データメッセージ
- コントロールメッセージ

データメッセージは、ネットワーク層のパケットを運ぶためのメッセージである。
コントロールメッセージには以下のものがある。

- ビーコン
- 認証要求
- 認証成功
- 認証失敗
- セッション終了

この章では、まず、メッセージを構成する要素として、MISP ヘッダとオブジェクトについて詳細なフォーマットを説明する。その後に、具体的なメッセージについて、それぞれ詳述する。
メッセージはネットワークバイトオーダー（ビッグエンディアン）に従う。

4.2. メッセージの構造

4.2.1. コントロールメッセージ

コントロールメッセージは、MISP ヘッダから始まる。MISP ヘッダの大きさは 4 バイトである。4 バイト未満の大きさのメッセージは存在しない。4 バイト未満の大きさのメッセージを受信した場合には、そのメッセージは破棄される。
メッセージの種類は MISP ヘッダの内容によって区別される。MISP ヘッダの後ろに続く部分には、「オブジェクト」が 0 個以上連続して格納される。オブジェクトとは、そのオブジェクトは、種類、長さ（バイト数）、値の組である。

4.2.2. データメッセージ

データメッセージは、MISP ヘッダから始まる。MISP ヘッダの大きさは 4 バイトである。4 バイト未満の大きさのメッセージは存在しない。4 バイト未満の大きさのメッセージを受信した場合には、そのメッセージは破棄される。
データメッセージの場合、MISP ヘッダに続く部分のフォーマットは、セッションで指定され

ているセキュリティ方式によって異なる。

4.3. MISP ヘッダ

MISP ヘッダは 4 バイトの大きさであり、以下の構造を持つ。

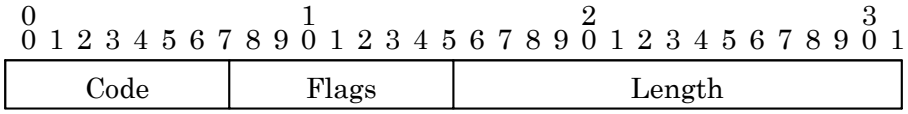

図 4　MISP ヘッダフォーマット

Code フィールド

このメッセージの種類を示す。フィールドの長さは 1 バイトで、8 ビットの整数である。メッセージの種類と Code フィールドの値の対応関係は以下の通りである。

0	データ
1	ビーコン
3	認証要求
4	認証成功
8	認証失敗
9	セッション終了

Code フィールドに、上の表にない値が入っている場合には、そのメッセージは無視されなければならない。

Flags フィールド

付加的な情報を示す。長さは 1 バイトで、8 つのビットからなる。各ビットの意味はメッセージの種類によって異なる。

Length フィールド

この MISP ヘッダから始まる、メッセージ全体の大きさをバイト単位で示す。フィールドの長さは 2 バイトであり、符号なし 16 ビット整数である。

実際のメッセージの長さのほうが Length フィールドの示す長さよりも長い場合には、末尾の余分な部分は無視される。
実際のメッセージの長さのほうが Length フィールドの示す長さよりも短い場合は、エラーであり、そのメッセージは無視されなければならない。

4.4. オブジェクト

MISP ヘッダに続く部分に出現する個々のオブジェクトは次のような形をとる。

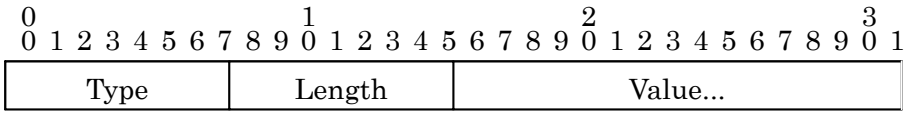

図 5　オブジェクトフォーマットの基本形

Type フィールド

オブジェクトの種類を示す。8 ビットの整数である。オブジェクトの種類と Type フィールドの対応関係は以下の通りである。

0	パディング
2	ビーコンタイムスタンプ
3	IPv4 ローカルアドレス
4	IPv4 リモートアドレス
5	ICV (Integrity Check Value)
6	NAI (Network Access Identifier; see RFC2486)
8	セッション鍵配送データ
9	地理情報
10	IPv4 利用可能アドレス残存数
11	IPv4 ソースアドレスフィルタ
13	エラー理由
14	基地局グループ
15	セッション鍵有効時間
16	シリアル番号
17	ビーコン間隔
18	セキュリティ方式

19　　上流回線種別
20　　チャネル
21　　ネットワーク層

Length フィールド

8 ビットの符号無し整数で、このオブジェクトの長さを示す。この長さには Type フィールドと Length フィールドも含む。よって最小値は 2 となる。フィールドの大きさは 1 バイトである。
Length フィールドの値が 2 未満のとき、または、Value フィールドの最後のバイトがメッセージの最後を越えてしまうほど大きいときは、そのオブジェクトを含むメッセージ全体を無効とし、無視しなければならない。
ただしパディングオブジェクトの場合(type=0)には、このフィールドは存在しない。

Value フィールド

オブジェクトのデータを示す。長さは可変であり、(Length-2)バイトである。
Length フィールドが 2 のときには、Value フィールドは存在しない。最大の長さは 253 バイトである。
ただしパディングオブジェクトの場合(type=0)には、このフィールドは存在しない。

以下では、各々のオブジェクトの固有のフォーマットについて述べる。なお、フォーマットの図では、4 バイト境界から始まっていないものもあるが、これは図の見易さを考慮したものであり、オブジェクトのアラインメントに制限はない。

4.4.1. パディングオブジェクト

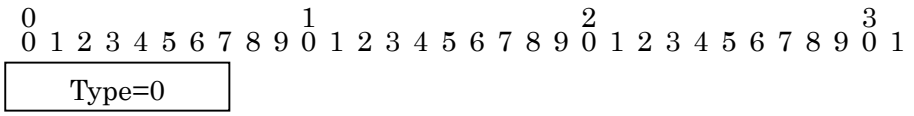

図 6　パディングオブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	0

パディングオブジェクトは、何の情報も運ばない。ただ単に無視される。メッセージ中において、何らかの理由でオブジェクト間に隙間ができた場合、そこには任意個数のパディングオブジェクトを詰めておくことができる。

パディングオブジェクトのフォーマットは、Length フィールドがないという点において特殊である。

4.4.2. ビーコンタイムスタンプオブジェクト

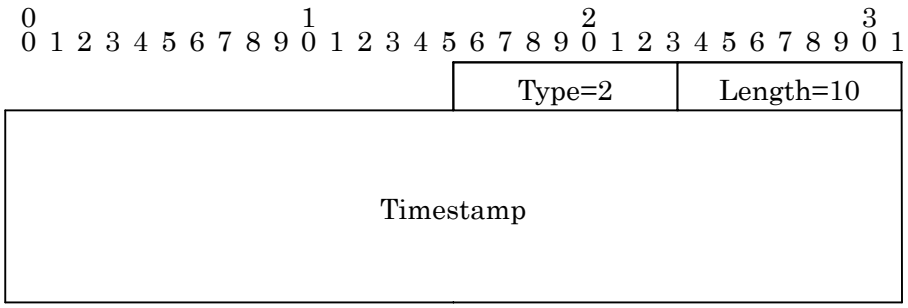

図 7　ビーコンタイムスタンプオブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	2
Length	10（固定値）。10 でない場合はこのオブジェクトは無視される。
Timestamp	8 バイトの符号無し整数。1970 年 1 月 1 日 0 時 0 分 0 秒 GMT からの時間をマイクロ秒単位で示す。

ビーコンタイムスタンプは、それが送信されたビーコンメッセージから始まる認証の識別子として使われる。

4.4.3. IPv4 ローカルアドレスオブジェクト

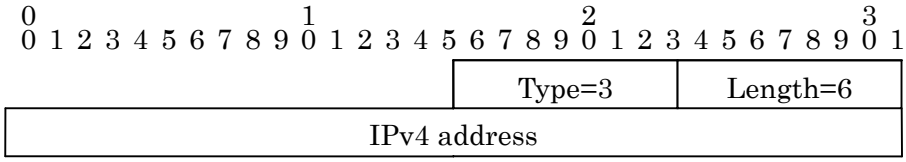

図 8　IPv4 ローカルアドレスオブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	3
Length	6（固定値）。6 でない場合はこのオブジェクトは無視される。
IPv4 address	IPv4 アドレス。4 バイト。

このオブジェクトが含まれる MISP メッセージを送信したホストの IPv4 アドレスを示す。

例えば、BR から MN に対して送信される認証成功メッセージにこのオブジェクトが含まれていた場合、このオブジェクトが示す IPv4 アドレスは BR の IPv4 アドレスである。

4.4.4. IPv4 リモートアドレスオブジェクト

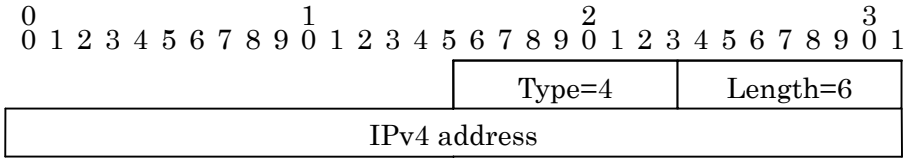

図 9　IPv4 リモートアドレスオブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	4
Length	6（固定値）。6 でない場合はこのオブジェクトは無視される。
IPv4 address	IPv4 アドレス。4 バイト。

このオブジェクトが含まれる MISP メッセージを受信するホストの IPv4 アドレスを示す。

例えば、BR から MN に対して送信される認証成功メッセージにこのオブジェクトが含まれていた場合、このオブジェクトが示す IPv4 アドレスは MN の IPv4 アドレスである。

4.4.5. ICV オブジェクト

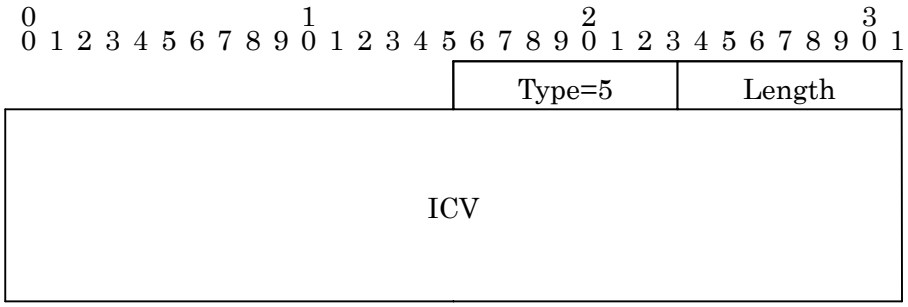

図 10　ICV オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	5
Length	このオブジェクトの長さ。Type, Length も含むバイト数。
ICV	(Length – 2)バイトのバイト列。

このメッセージ全体の正当性を確認するためのデータを示す。データの長さと意味は認証方式によって異なる。認証の方式に関する情報は、セキュリティ方式オブジェクトを使って、MN と BR の間で共有される。

4.4.6. NAI オブジェクト

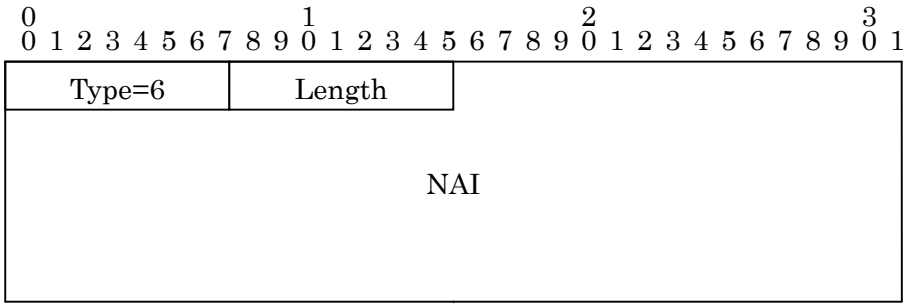

図 11　NAI オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	6
Length	このオブジェクトの長さ。Type, Length も含むバイト数。
NAI	アカウント識別子。(Length – 2)バイトのバイト列。

アカウント識別子を示す。MISP 上は、単純なバイト列として扱われる。ターミネータとしてのヌル文字を含まないこと。最後にヌル文字があった場合にも、アカウント識別子の一部として扱われる。

4.4.7. セッション鍵配送データオブジェクト

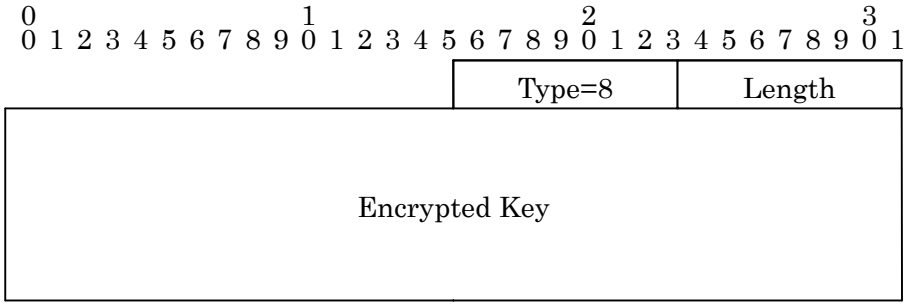

図 12　セッション鍵配送データオブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	8
Length	このオブジェクトの長さ。Type, Length も含むバイト数。
Encrypted Key	鍵の配送に使われるデータ。(Length – 2)バイトのバイト列。

MN と BR の間で鍵を配送するために使うデータである。通常、鍵が盗まれないように、暗号化がされている。データの長さと意味は認証方式によって異なる。利用する暗号の方式に関する情報は、セキュリティ方式オブジェクトを使って、MN と BR の間で共有される。

4.4.8. 地理情報オブジェクト

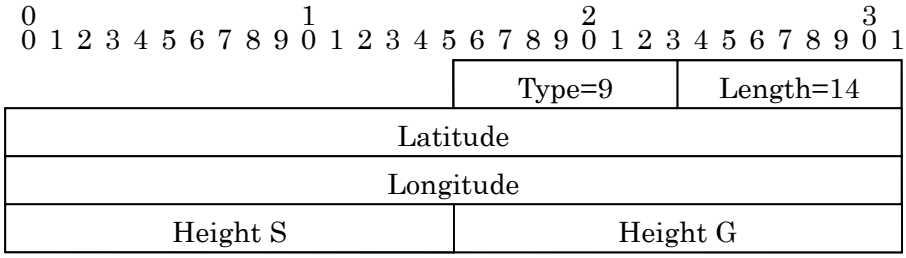

図 13　地理情報オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	9
Length	14（固定値）。14 でない場合はこのオブジェクトは無視される。
Latitude	緯度。符号付 32 ビット整数。
Longitude	経度。符号付 32 ビット整数。
Height S	海抜。符号付 16 ビット整数。
Height G	地上高。符号付 16 ビット整数。

BR のアンテナの地理的位置情報を、緯度・経度と高さの情報により示す。

緯度と経度はそれぞれ、符号付き 32 ビット整数である。単位は 1/65536 度である。符号は、北緯および東経を正とし、南緯、西経を負とする。ただし、0x80000000 は「情報なし」の意味とする。測地系としては WGS84 測地系を使う。（※リファレンスが必要）

海抜と地上高は、符号付の 16 ビット整数で表される。単位は「メートル」であり、正の値が高い場所を、負の値は海面または地表よりも下を示す。ただし、0x8000 は「情報なし」の意味とする。海抜の測地系としては WGS84 測地系を使う。

4.4.9. IPv4 利用可能アドレス残存数オブジェクト

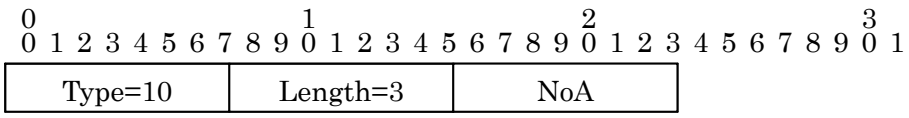

図 14　利用可能アドレス残存数オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	10
Length	3（固定値）。3 でない場合はこのオブジェクトは無視される。
NoA	利用可能な IPv4 アドレスの数。1 バイトの符号無し整数。

このオブジェクトを送信した BR において、MN に対して動的に割り当てるために用意している IPv4 アドレスのうち、未割り当てのアドレスの数を示す。この数は、逐次変化するため、この値が 1 以上のビーコンメッセージに対して認証要求メッセージを送った場合にも、IPv4 アドレスが不足する場合がある。

BR はこのオブジェクトを送信するときに、NoA の値を、本来の値よりも小さい値にして送信してもよい。

このオブジェクトが送信されていない場合、利用可能な IPv4 アドレスの数に関する情報は提供されていないとみなす。

4.4.10. IPv4 パケットフィルタオブジェクト

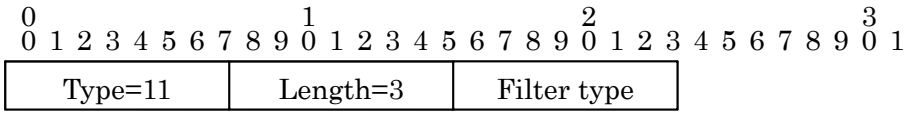

図 15　IPv4 パケットフィルターオブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	11
Length	3（固定値）。3 でない場合はこのオブジェクトは無視される。
Filter type	パケットフィルタのタイプ。下の表参照。

このオブジェクトを送信した BR を通過する IPv4 パケットは、パケットフィルタの影響を受ける可能性があることを示す。

Filter type に指定できる値は以下のものがある。

0	パケットフィルタの影響を受けることはない。すべての IPv4 パケットは正しく配送される。
1	パケットフィルタの影響を受ける可能性がある。具体的には、同じメッセージで送信される IPv4 リモートアドレスオブジェクトによって

指定された IPv4 アドレスを、IPv4 ヘッダのソースアドレスフィールドまたはデスティネーションアドレスフィールドに持っているパケットのみが、フィルタの通過を保証される。この場合、Mobile IPv4 を利用する場合には Reverse Path Tunnel を使う必要がある。

これ以外の値が Filter type に指定されていた場合、このオブジェクトは無視される。また、パケットフィルタオブジェクトが存在しなかった場合には、パケットフィルタの影響は受けないものとみなす。これは、パケットフィルタオブジェクトにおいて 0 が指定された場合と同等である。

4.4.11. エラー理由オブジェクト

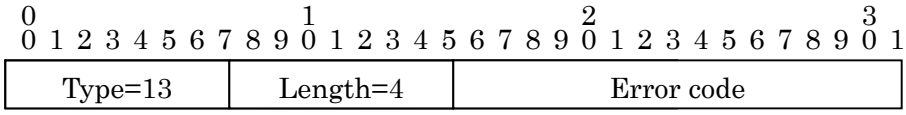

図 16　エラー理由オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	13
Length	4（固定値）。4 でない場合にはこのオブジェクトは無視される。
Error code	エラーが発生した理由を示す。16 ビットの整数。

エラーが発生したとき、そのエラーの内容を示す。Error code が 0-127 は一時的なエラー、128-255 は持続的なエラーを示す。

（後で消す＝一時的というのはリトライすぐにしても意味があるエラー）

1　認証サーバと通信できなかった。
128　認証操作を行って認証に失敗した。
129　IPv4 アドレスが不足しているため割り当てられなかった。
130　メッセージフォーマットがおかしい。

4.4.12. 基地局グループオブジェクト

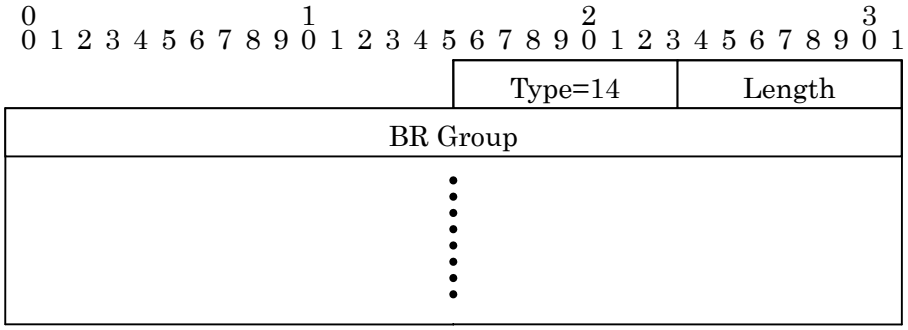

図 17　基地局グループオブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	14
Length	このオブジェクトの長さ。Type, Length も含むバイト数。2+4n（n は 0 以上 32 以下の整数）でなければならない。そうでない場合には、このオブジェクトは無視される。
BR Group	基地局グループを示す。基地局グループは 4 バイトの識別子であり、このオブジェクトは、1 つ以上の複数の基地局グループを含むことができる。

BR が属している基地局グループを示す。0 個以上 32 個以下の基地局グループを指定することができる。

基地局グループオブジェクトが存在しない場合には、その BR はどのグループにも属していないことを示す。Length フィールドの値が 2 の場合も同様である。

4.4.13. セッション鍵有効時間オブジェクト

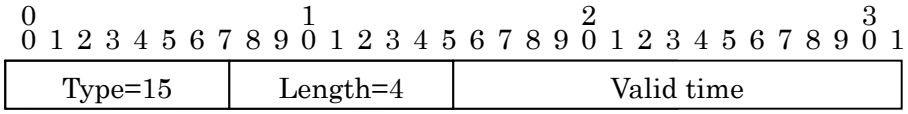

図 18　セッション鍵有効時間オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	15
Length	このオブジェクトの長さ。Type, Length も含むバイト数。
Valid time	16 ビットの符号なし整数。単位は秒。

セッション鍵の有効時間を示す。

4.4.14. シリアル番号オブジェクト

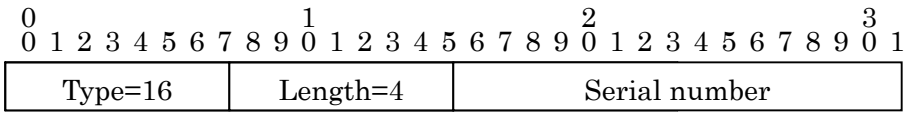

図 19　シリアル番号オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	16
Length	このオブジェクトの長さ。Type, Length も含むバイト数。
Serial number	16 ビットの符号なし整数。

連続する番号を Serial number フィールドに入れて送信する。番号は、このオブジェクトが送信される毎に 1 ずつ増える。0xffff の次は 0 に戻る。最初の番号は問わない。

受信側で観測した場合、パケットロスや重複により、必ずしも連続した番号が届くとは限らない。

BR は、シリアル番号オブジェクトをビーコンメッセージに載せて送信することができる。その場合、BR は、自分が送信する全てのビーコンメッセージにシリアル番号オブジェクトを入れなければならない。MN は、受信したビーコンメッセージのシリアル番号オブジェクトを調べることにより、ビーコンメッセージの消失を知ることができる。

4.4.15. ビーコン間隔オブジェクト

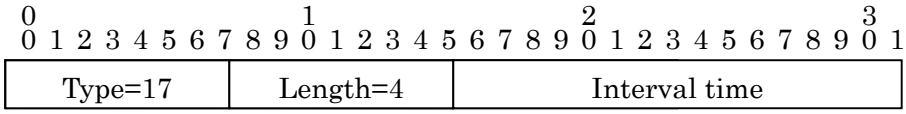

図 20　ビーコン間隔オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	17
Length	このオブジェクトの長さ。Type, Length も含むバイト数。
Interval time	16 ビットの符号なし整数。単位はミリ秒。

このオブジェクトを送信する BR が送信しているビーコンメッセージの時間間隔を示す。

4.4.16. セキュリティ方式オブジェクト

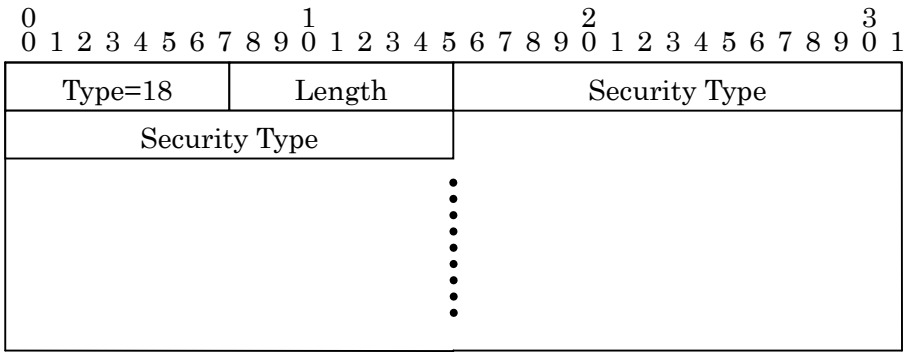

図 21　セキュリティ方式オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	18
Length	このオブジェクトの長さ。Type, Length も含むバイト数。2+2n（n は 1 以上 126 以下の整数）でなければならない。そうでない場合には、このオブジェクトは無視される。

Security Type　セキュリティ方式。1 つ以上のセキュリティ方式を列挙することができる。

セキュリティ方式を示す。

BR が送信するビーコンメッセージの場合には、その BR が受け入れることのできるセキュリティ方式を列挙する。1 個以上 126 個以下のセキュリティ方式を指定することができる。

MN が送信する認証要求メッセージの場合には、MN が選んだ、実際にこのセッションで使用するセキュリティ方式を 1 つだけ指定する。複数指定されていた場合、フォーマットエラーとなり認証は失敗する。

4.4.17. 上流回線種別オブジェクト

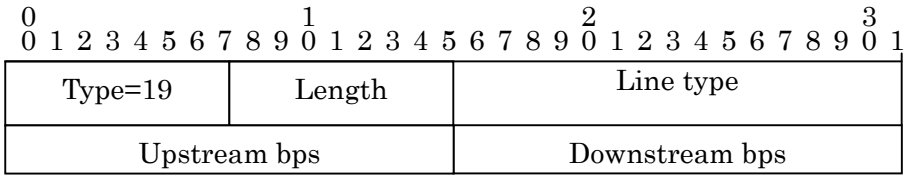

図 22　上流回線種別オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type　19

Length　このオブジェクトの長さ。8 でなければならない。8 以外の値だった場合には、このオブジェクトは無視される。

Line type　上流回線の種別。16 ビットの符号なし整数。

- 0　FTTH（光ファイバ）
- 1　xDSL
- 2　CATV

Upstream bps　上流回線の上りの速度。16 ビットの符号なし整数。

Downstream bps　上流回線の下りの速度。16 ビットの符号なし整数。

このオブジェクトを送信する BR が利用している上流回線の速度と種別を示す。

回線の速度は、16 ビットの符号無し整数で、単位は kbps とする。ただし、0xffff は、65.535Mbps 以上を示すものとする。また、「上り」とは BR から出て行く向きを指し、「下り」とは BR に入ってくる向きを指す。

4.4.18. チャンネルオブジェクト

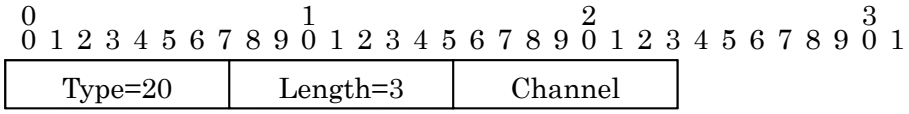

図 23　チャネルオブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	20
Length	このオブジェクトの長さ。3 でなければならない。3 以外の値だった場合には、このオブジェクトは無視される。
Channel	8 ビットの符号なし整数。

このオブジェクトを送信する BR が利用しているチャンネルを示す。チャンネルの表現はメディアにより異なる。

このオブジェクトが存在しない場合、そのメディアにはチャンネル切り替え機能がなく、チャンネルが 1 つしかないことを示す。

4.4.19. ネットワーク層オブジェクト

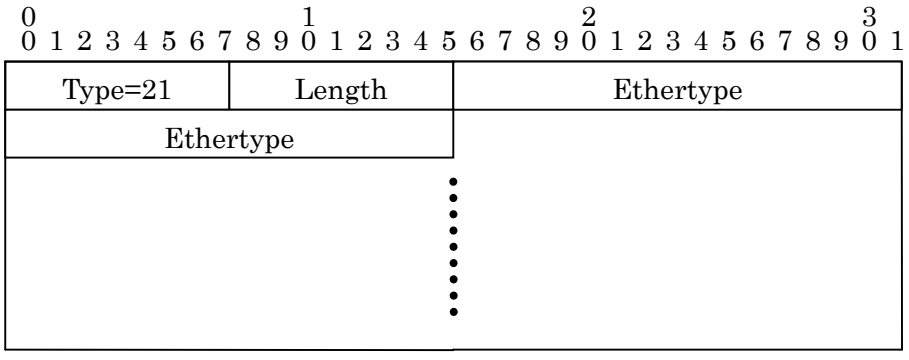

図 24　ネットワーク層オブジェクトフォーマット

各フィールドの内容は次の通りである。

Type	21
Length	このオブジェクトの長さ。Type, Length も含むバイト数。2+2n（n は 0 以上 16 以下の整数）でなければならない。そうでない場合には、このオブジェクトは無視される。
Ethertype	ネットワーク層の種類を示す（IPv4 の場合は 0x0800,、IPv6 の場合は 0x86dd）。

このオブジェクトが含まれていない場合には、ネットワーク層が 1 つも指定されていないものとして扱う。

BR がこのオブジェクトをビーコンメッセージに載せて送信した場合、その BR において、利用可能なネットワーク層を示す。

MN がこのオブジェクトを認証要求メッセージに載せて送信した場合、その MN がこのオブジェクトで指定されたネットワーク層の接続を要求していることを示す。MN は複数のネットワーク層を指定してよい。

BR がこのオブジェクトを認証成功メッセージに載せて送信した場合、そのセッションにおいて利用できるネットワーク層を示す。

4.5. メッセージ

4.5.1. データメッセージ

データメッセージは、ネットワーク層のパケットを運ぶために用いられる。データメッセージは、MN, BR の両方が、互いに送受信する。

- **フォーマット**

データメッセージのフォーマットは次の通りである。

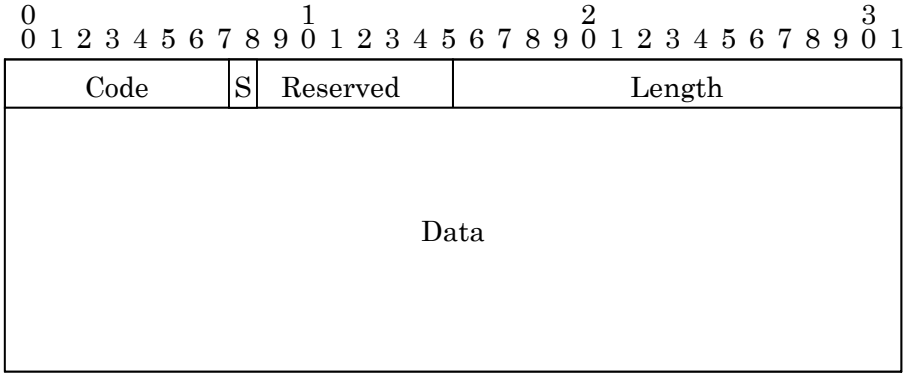

図 25　データメッセージフォーマット

各フィールドの内容は次の通りである。

Code	0（固定値）。
S	認証と暗号化に使うセッション鍵の指定。1 ビットであり、0 はセッション鍵 A を、1 はセッション鍵 B を示す。
Reserved	全ビット 0（固定値）。
Length	このデータメッセージ全体の長さをバイト単位で示す。16 ビットの符号なし整数である。
Data	セキュリティ方法に依存したフォーマット。長さは(Length-4)バイトである。

S ビットによって、このデータメッセージで使われるセッション鍵を示す。

Data フィールドのフォーマットは、セキュリティ方式によって決定される。各セキュリティ方式によって利用される Data フィールドのフォーマットについては、「セキュリティ方式」の章の各項目を参照すること。

4.5.2. ビーコンメッセージ

ビーコンメッセージは、BR が定期的に送信する。MN はビーコンメッセージを受信することにより、通信可能な BR を発見することができる。

- **フォーマット**

ビーコンメッセージのフォーマットは次の通りである。

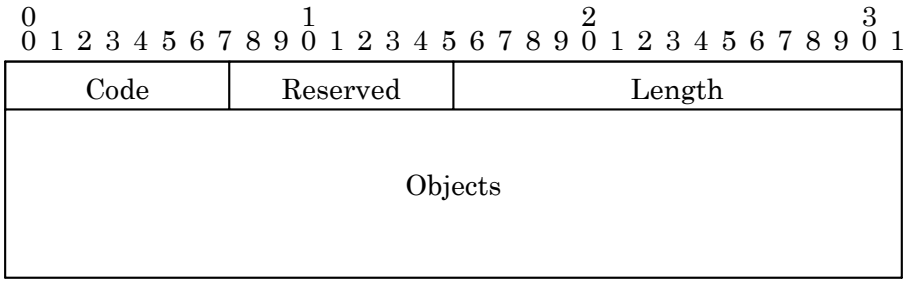

図 26　ビーコンメッセージフォーマット

各フィールドの内容は次の通りである。

Code	1（固定値）。

Reserved	全ビット 0（固定値）。
Length	このデータメッセージ全体の長さをバイト単位で示す。16 ビットの符号なし整数である。
Objects	オブジェクトを必要なだけ並べる。

ビーコンメッセージに必ず含まれるオブジェクトは次の通りである。

ビーコンタイムスタンプオブジェクト
基地局グループオブジェクト
シリアル番号オブジェクト
ビーコン間隔オブジェクト
セキュリティ方式オブジェクト
ネットワーク層オブジェクト

ビーコンメッセージに含むことのできるオブジェクトは次の通りである。

パディングオブジェクト
IPv4 利用可能アドレス残存数オブジェクト
IPv4 パケットフィルタオブジェクト
地理情報オブジェクト
上流回線種別オブジェクト
チャンネルオブジェクト

同種のオブジェクトが複数入っていた場合には、最初の 1 つだけが有効となり、残りの重複するオブジェクトは無視される。

上に挙げなかったオブジェクトが含まれていた場合、それらのオブジェクトは無視される。

- **送信**

ビーコンタイムスタンプの Timestamp フィールドの値は、同じ BR から送信されたビーコンメッセージでは、単調に増加しなければならない。つまり、同じ BR が送信したビーコンタイムスタンプオブジェクトを含むビーコンメッセージでは、後に送信されたメッセージに含まれる Timestamp フィールドの値のほうが、必ず大きい。

Timestamp フィールドの値は、UTC1970 年 1 月 1 日 0 時 0 分 0 秒からの経過時間をマイクロ秒単位で示した値を使う。

- **受信**

Reserved フィールドに入っている値は検査しない。

ビーコンタイムスタンプオブジェクトが含まれていなかった場合には、そのビーコンメッセージを破棄する。

4.5.3. 認証要求メッセージ

認証要求メッセージは、MN が BR に対して送信する。認証要求メッセージが送信されるのは、次の 2 つの場合である。

- 新しくセッションを開始しようとするとき。
- 既存のセッションのセッション鍵を更新しようとするとき。

➢ フォーマット

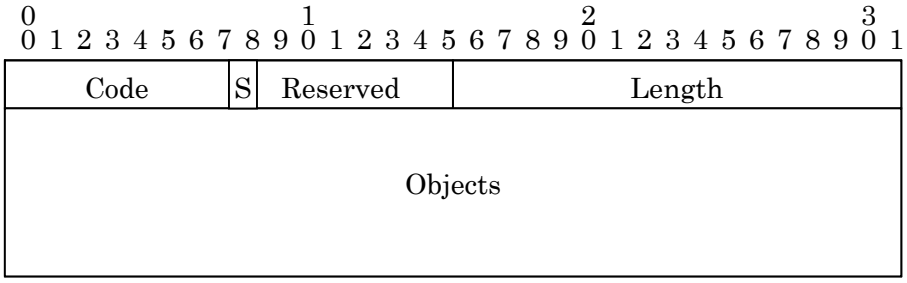

図 27　認証要求メッセージフォーマット

各フィールドの内容は次の通りである。

Code	3（固定値）。
S	配送するセッション鍵の指定。1 ビットであり、0 はセッション鍵 A を、1 はセッション鍵 B を示す。
Reserved	全ビット 0（固定値）。
Length	メッセージの長さ。
Objects	オブジェクトを必要なだけ並べる。

認証要求メッセージに必ず含まれるオブジェクトは次の通りである。

ビーコンタイムスタンプオブジェクト
セキュリティ方式オブジェクト
ICV オブジェクト
NAI オブジェクト
セッション鍵配送データオブジェクト
ネットワーク層オブジェクト

認証要求メッセージに含むことのできるオブジェクトは次の通りである。

パディングオブジェクト
IPv4 ローカルアドレスオブジェクト

同種のオブジェクトが複数入っていた場合には、最初の 1 つだけが有効となり、残りの重複するオブジェクトは無視される。
上に挙げなかったオブジェクトが含まれていた場合、それらのオブジェクトは無視される。

- **送信**

ビーコンタイムスタンプオブジェクトには、このメッセージを送るために受信したビーコンメッセージに入っていたビーコンタイムスタンプを入れる。
セキュリティ方式オブジェクトには、このメッセージで要求する認証とセッションで利用するセキュリティ方式を入れる。
セッションを開始する場合には、S ビットは常に 0 である。

- **受信**

Reserved フィールドに入っている値は検査しない。
必要なオブジェクトが欠けていた場合には、そのビーコンは破棄され、ビーコンは受信されなかったものとして扱われる。

4.5.4. 認証成功メッセージ

認証成功メッセージは、BR から MN に対して送信される。

- **フォーマット**

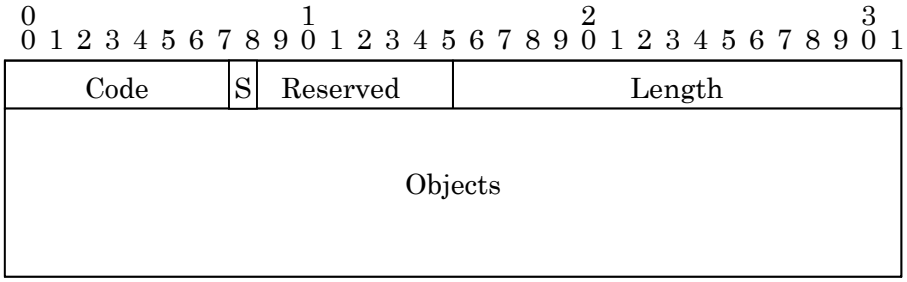

図 28　認証成功メッセージフォーマット

各フィールドの内容は次の通りである。

Code	4（固定値）。
S	配送され認証に使われるセッション鍵の指定。1 ビットであり、0 はセッション鍵 A を、1 はセッション鍵 B を示す。
Reserved	全ビット 0（固定値）。
Length	メッセージの長さ。
Objects	オブジェクトを必要なだけ並べる。

認証成功メッセージに必ず含まれるオブジェクトは次の通りである。

ビーコンタイムスタンプオブジェクト
セッション鍵有効時間オブジェクト
ICV オブジェクト
ネットワーク層オブジェクト

認証成功メッセージに含むことのできるオブジェクトは次の通りである。

パディングオブジェクト
IPv4 ローカルアドレスオブジェクト
IPv4 リモートアドレスオブジェクト

同種のオブジェクトが複数入っていた場合には、最初の 1 つだけが有効となり、残りの重複するオブジェクトは無視される。
上に挙げなかったオブジェクトが含まれていた場合、それらのオブジェクトは無視される。

- **送信**

ビーコンタイムスタンプオブジェクトには、このメッセージで扱っている認証を要求した認証要求メッセージに入っていたビーコンタイムスタンプを入れる。
セッション鍵有効時間オブジェクトには、このメッセージから開始されたセッション鍵の有効時間を入れる。

- **受信**

Reserved フィールドに入っている値は検査しない。
必要なオブジェクトが欠けていた場合には、その認証成功メッセージは破棄され、認証は持続的失敗となる。

4.5.5. 認証失敗メッセージ

認証失敗メッセージは、BR から MN に対して送信される。認証失敗メッセージは認証することができない。

➢ **フォーマット**

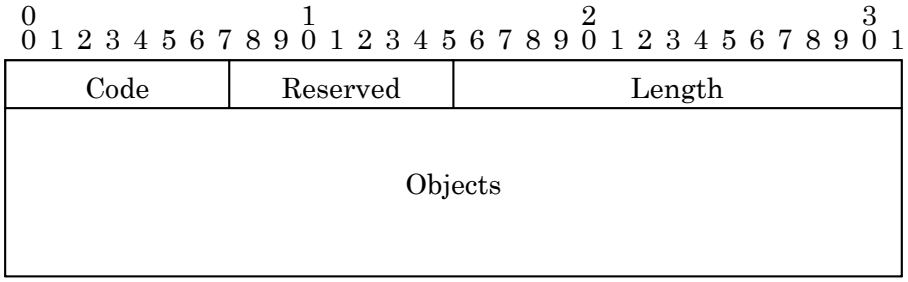

図 29　認証失敗メッセージフォーマット

各フィールドの内容は次の通りである。

Code	8（固定値）。
Reserved	全ビット 0（固定値）。
Length	メッセージの長さ。
Objects	オブジェクトを必要なだけ並べる。

認証失敗メッセージに必ず含まれるオブジェクトは次の通りである。

ビーコンタイムスタンプオブジェクト
エラー理由オブジェクト

認証失敗メッセージに含むことのできるオブジェクトは次の通りである。

パディングオブジェクト

同種のオブジェクトが複数入っていた場合には、最初の 1 つだけが有効となり、残りの重複するオブジェクトは無視される。
上に挙げなかったオブジェクトが含まれていた場合、それらのオブジェクトは無視される。

➢ **送信**

ビーコンタイムスタンプオブジェクトには、このメッセージで扱っている認証を要求した認証要求メッセージに入っていたビーコンタイムスタンプを入れる。

➢ **受信**

Reserved フィールドに入っている値は検査しない。
必要なオブジェクトが入っていなかった場合には、その認証失敗メッセージは破棄される。

4.5.6. セッション終了メッセージ

セッション終了メッセージは、MN、BR の両方が送信することができる。

- **フォーマット**

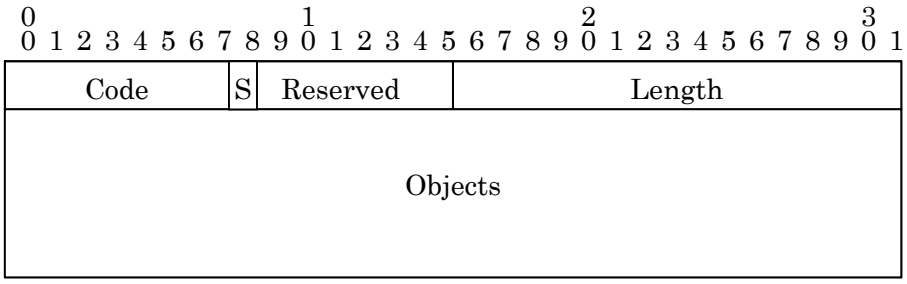

図 30　セッション終了メッセージフォーマット

各フィールドの内容は次の通りである。

b Code	9（固定値）。
S	認証に使うセッション鍵の指定。1 ビットであり、0 はセッション鍵 A を、1 はセッション鍵 B を示す。
Reserved	全ビット 0（固定値）。
Length	メッセージの長さ。
Objects	オブジェクトを必要なだけ並べる。

セッション終了メッセージに必ず含まれるオブジェクトは次の通りである。

ビーコンタイムスタンプオブジェクト
ICV オブジェクト

セッション終了メッセージに含むことのできるオブジェクトは次の通りである。

パディングオブジェクト
エラー理由オブジェクト

上に挙げたオブジェクトが複数入っていた場合には、最初の 1 つだけが有効となり、残りの重複するオブジェクトは無視される。
上に挙げなかったオブジェクトが含まれていた場合、それらのオブジェクトは無視される。

- **送信**

ビーコンタイムスタンプオブジェクトには、このメッセージで扱っているセッションを開始したビーコンに入っていたビーコンタイムスタンプを入れる。

- **受信**

Reserved フィールドに入っている値は検査しない。

ビーコンタイムスタンプオブジェクトが入っていなかった場合には、その認証失敗メッセージは破棄される。

5. 動作

5.1. 静的に設定される情報

5.1.1. MN に設定される情報

MN には、1 組のアカウント識別子とパスワードが設定されているものとする。

5.1.2. BR に設定される情報

BR は、アカウント識別子とパスワードの対応表を、あらかじめ持っているものとする。

または、AS を設置し BR と接続することによって、アカウント識別子とパスワードの対応表の管理を AS で一元化することもできる。AS と BR の間の通信方法については、MISP では規定しない。

5.2. MN による BR の発見・選択・監視

5.2.1. ビーコンメッセージの送信(BR)

BR は、MISP を使用するメディアのチャンネルにおいて、ビーコンメッセージを一定時間毎に送信する。BR は、実装可能な範囲でなるべく正確に、この時間を守ることを求められる。具体的なビーコンメッセージの送信間隔は、メディアによって異なる。具体的な値については、メディアの章を参照すること。

ビーコンメッセージは、MN と BR のセッションにかかわらず、常に送信される。

5.2.2. ビーコンメッセージの受信と監視(MN)

MN は、設定されたメディアすべてにおいてパケットの受信動作を行い、ビーコンメッセージを受信する。複数のチャンネルを持つメディアについては、設定されたすべてのチャンネルで受信動作を行う。

MN は、受信したビーコンメッセージの情報を使って、周囲に存在する BR の一覧表を作る。受信したビーコンメッセージから一覧表を作る方法はメディアによって異なる。詳しい方法は、メディアの章を参照すること。

5.2.3. BR の選択(MN)

ある基準に従って、その BR の一覧表の中から、使用する BR を選択し、セッションを開始しようとする。可能であれば、同時に複数個の BR に対してそれぞれセッションを持っても良い。

5.3. セッションの開始

5.3.1. ビーコンメッセージの受信(MN)

セッションを開始しようとする MN は、最初に以下の動作を行う。

1. セッションを開始しようとする相手の BR が送信したビーコンメッセージを受信し、1 つ選ぶ。
2. ビーコンメッセージに入っているセキュリティ方式オブジェクトを見てその BR で使用可能なセキュリティ方式を確認し、その中から、このセッションで使用するセキュリティ方式を 1 つ決定する。
3. セッション鍵を作る。
4. 認証要求メッセージを作成する。
5. 認証要求メッセージに対して認証の操作をする。実際の方法は、セキュリティ方式によって異なる。
6. 最初の認証要求メッセージを送信する。
7. 最初の認証要求メッセージを送信したときから 100ms, 300ms, 700ms, 1500ms 後の合計 4 回、認証要求メッセージを再送信する。このとき送信する認証要求メッセージは最初に送信した認証要求メッセージとまったく同じものとする。
   対象とする BR からの、対応するビーコンタイムスタンプオブジェクトを含む認証成功メッセージまたは認証失敗メッセージを受信した場合、または、最初の認証要求メッセージを送信したときから 3100ms 経過した場合には、この処理を中止し、次に進む。
8. 認証成功メッセージまたは認証失敗メッセージが受信できた場合には、そのメッセージの処理に移る。受信できなかった場合には、この BR とのセッションの開始処理は、失敗とする。

5.3.2. 認証要求メッセージの受信(BR)

当該の MN-BR 間にセッションが存在しない MN からの認証要求メッセージを受信した BR は、以下の動作を行う。

1. 受信した認証要求メッセージのビーコンタイムスタンプオブジェクトの値が、その時から 5 秒前の直前に送信したビーコンメッセージのビーコンタイムスタンプオブジェクトの値以上で、かつ、直前に送信したビーコンメッセージのビーコンタイムスタンプオブジェクトの値未満であるかどうか調べる。この範囲に入っていない場合、この認証要求メッセージを破棄して処理を終え、認証失敗メッセージを送信する。
2. 認証と鍵配送の操作を行う。具体的な動作はセキュリティ方式によって異なる。認証サーバと通信できない場合や認証に失敗した場合は、認証失敗メッセージを送信し、

処理を終える。

3. セッションが成立したとみなし、得られたセッション鍵を、セッション鍵 A として設定する。セッション鍵 B は無効とする。
4. 認証要求メッセージに載せて送られてきたネットワーク層のための情報があれば、該当するネットワーク層に渡す。また、ネットワーク層が認証成功メッセージに載せる情報があれば、それを受け取る。
5. 認証成功メッセージを作成する。
6. 認証要求メッセージに対して認証の操作をする。実際の方法は、セキュリティ方式によって異なる。
7. 認証成功メッセージを送信する。

5.3.3. 認証成功メッセージの受信(MN)

認証成功メッセージを受信した MN は、以下の動作を行う。

1. メッセージを認証する。具体的な動作はセキュリティ方式によって異なる。メッセージの認証に失敗したら、この認証成功メッセージを破棄して処理を終え、セッションの開始処理は持続的失敗となる。
2. セッションが成立したとみなし、得られたセッション鍵を、セッション鍵 A として設定する。このときに、セッション鍵有効時間オブジェクトに従って、セッション鍵の有効時間を設定する。セッション鍵 B は無効とする。
3. 認証成功メッセージに載せて送られてきたネットワーク層のための情報があれば、該当するネットワーク層に渡す。

5.3.4. 認証失敗メッセージの受信(MN)

MN は、認証失敗メッセージを受信すると、直ちに、セッションの開始処理が失敗したとみなす。

5.4. セッション鍵の更新

2 つのセッション鍵のうち、作成時刻が新しいものの残り有効時間が 10 秒以下になったとき、MN は他方のセッション鍵の更新処理を始める。

5.4.1. ビーコンメッセージの受信(MN)

セッション鍵を更新しようとする MN は、最初に以下の動作を行う。

1. セッションの相手の BR が送信したビーコンメッセージを受信し、1 つ選ぶ。

2. 新しいセッション鍵を作る。
3. 認証要求メッセージを作成する。
4. 認証要求メッセージに対して認証の操作をする。実際の方法は、セキュリティ方式によって異なる。
5. 最初の認証要求メッセージを送信する。
6. 最初の認証要求メッセージを送信したときから 100ms, 300ms, 700ms, 1500ms 後の合計 4 回、認証要求メッセージを再送信する。このとき送信する認証要求メッセージは最初に送信した認証要求メッセージとまったく同じものとする。
   BR からの、対応するビーコンタイムスタンプオブジェクトを含む認証成功メッセージまたは認証失敗メッセージを受信した場合、または、最初の認証要求メッセージを送信したときから 3100ms 経過した場合には、この処理を中止し、次に進む。
7. 認証成功メッセージまたは認証失敗メッセージが受信できた場合には、そのメッセージの処理に移る。受信できなかった場合には、このセッションの鍵の更新処理は、失敗とする。

5.4.2. 認証要求メッセージの受信(BR)

当該の MN-BR 間にセッションが既に存在する MN からの認証要求メッセージを受信した BR は、以下の動作を行う。認証要求が到着したときに古い鍵がまだ有効であれば認証が成功するまでその鍵は上書きされない。（ちょっと日本語あとでみなおす？）

1. 受信した認証要求メッセージのビーコンタイムスタンプオブジェクトの値が、その時から 5 秒前までに送信した何れかのビーコンメッセージのビーコンタイムスタンプオブジェクトの値と一致するかどうか調べる。一致しなければ、この認証要求メッセージを破棄して処理を終え、認証失敗メッセージを送信する。
2. 認証と鍵配送の操作を行う。具体的な動作はセキュリティ方式によって異なる。認証サーバと通信できない場合や認証に失敗した場合は、認証失敗メッセージを送信し、処理を終える。
3. 得られたセッション鍵を、認証要求メッセージで指定されたセッション鍵 A または B として設定する。
4. 認証成功メッセージを作成する。
5. 認証要求メッセージに対して認証の操作をする。実際の方法は、セキュリティ方式によって異なる。
6. 認証成功メッセージを送信する。

5.4.3. 認証成功メッセージの受信(MN)

認証成功メッセージを受信した MN は、以下の動作を行う。

1. メッセージを認証する。具体的な動作はセキュリティ方式によって異なる。メッセージの認証に失敗したら、この認証成功メッセージを破棄して処理を終え、セッションの開始処理は持続的失敗となる。
2. セッションが成立したとみなし、得られたセッション鍵を、S ビットに従いセッション鍵 A または B として設定する。このときに、セッション鍵有効時間オブジェクトに従って、セッション鍵の有効時間を設定する。
3. 認証成功メッセージに載せて送られてきたネットワーク層のための情報があれば、該当するネットワーク層に渡す。

5.4.4. 認証失敗メッセージの受信(MN)

MN は、認証失敗メッセージを受信すると、直ちに、セッション鍵の更新処理が失敗したとみなす。

5.5. データメッセージの交換

データメッセージは、MN、BR 共に、送受信できる。

5.5.1. データメッセージの送信

ネットワーク層から送信すべきパケットが渡されたとき、以下の動作を行う。

1. セッションが成立していない場合には、ネットワーク層にエラーを返し、このデータメッセージの送信処理を終える。
2. そのネットワーク層が、セッション上でサポートされているかどうか検査する。サポートしていなければ、ネットワーク層にエラーを返し、このデータメッセージの送信処理を終える。
3. そのセッション上の 2 つのセッション鍵のうち、有効で、かつ、設定された時刻がより新しいセッション鍵を選ぶ。データメッセージを作り、認証と暗号化の操作を行う。具体的な方法はセキュリティ方式によって異なる。
4. データメッセージを送信する。

5.5.2. データメッセージの受信

データメッセージを受信したときには、以下の動作を行う。

1. 受信したデータメッセージで指定されたセッション鍵が有効であることを確認する。そうでない場合には、このデータメッセージを破棄し、受信処理を終える。
2. 認証と暗号の復号処理を行う。具体的な方法はセキュリティ方式によって異なる。認

証に失敗した場合には、このデータメッセージを破棄し、受信処理を終える。
3. そのセッションでサポートしているネットワーク層かどうか検査する。サポートしていなければこのデータメッセージを破棄し、受信処理を終える。
4. ネットワーク層にパケットを渡す。

5.6. セッションの終了

5.6.1. 能動的なセッションの終了

MN と BR は、通信の必要がなくなった場合、セッション終了メッセージを送信して、能動的にセッションを終了する。

能動的にセッションを終了するときには、以下の動作を行う。

1. そのセッション上で、有効で、かつ、設定時刻がより新しいセッション鍵を選ぶ。使用可能なセッション鍵が 1 つもない場合には、セッションの情報を消去し、セッションを終了して、この処理を終わる。
2. セッション終了メッセージを作る。
3. セキュリティ方式により、セッション終了メッセージに対して、認証のために必要な操作を行う。
4. セッション終了メッセージを送信する。
5. セッションの情報を消去する。

5.6.2. セッション終了メッセージの受信

MN または BR が、セッション終了メッセージを受信したとき、以下の動作を行う。

1. 認証の操作を行う。具体的な方法はセキュリティ方式によって異なる。
2. セッションの情報を消去する。

5.6.3. BR の消滅

MN は BR の存在を監視している。通常はビーコンメッセージの受信によるが、この方法はメディアによって異なる。

BR の存在が確認できなくなった場合、その BR との間にあったセッションは直ちに終了したものとして扱う。

5.6.4. セッションの自然消滅

セッション鍵が A、B 共に無効になった場合セッションは自然消滅する。

6. セキュリティ方式

セキュリティ方式には次のものがある。左端の数字は、セキュリティ方式オブジェクトの Security Type フィールドで使う番号である。

1	Null
2	HMAC-MD5/HMAC-MD5/AES-CBC-128bit
3	HMAC-MD5/HMAC-MD5/HMAC-MD5-128bit

全ての BR と MN は、HMAC-MD5/HMAC-MD5/AES-CBC-128bit を実装しなければならないが、他の方式はオプションとする。

以下では、それぞれのセキュリティ方式について、順に説明する。

6.1. Null 方式

一切の認証・暗号化を行わない方式である。

6.1.1. セッション鍵

セッション鍵は形式上配送するが、認証には使用しない。セッション鍵の長さは 96bit(12byte)とする。

6.1.2. 認証要求メッセージ

- 送信(MN)

ICV オブジェクトには任意の長さの任意のバイト列を入れる。セッション鍵配送オブジェクトには、セッション鍵をそのまま入れる。

- 受信(BR)

受信した ICV オブジェクトは検査せず無視する。認証は、常に成功する。ICV オブジェクトが含まれていない場合にも、認証は成功する。

受信したセッション鍵配送オブジェクトから取り出したバイト列を、そのままセッション鍵とする。セッション鍵配送オブジェクトが含まれていない場合には、12 バイトの 0 をセッション鍵とする。

6.1.3. 認証成功メッセージ

- 送信(BR)

ICV オブジェクトには、セッション鍵を入れる。

➢ 受信(MN)

受信した ICV オブジェクトは検査せず無視する。認証は、常に成功する。ICV オブジェクトが含まれていない場合にも、認証は成功する。

6.1.4. 認証終了メッセージ

➢ 送信

ICV オブジェクトには、セッション鍵を入れる。

➢ 受信

受信した ICV オブジェクトは検査せず無視する。認証は、常に成功する。ICV オブジェクトが含まれていない場合にも、認証は成功する。

6.1.5. データメッセージ

➢ フォーマット

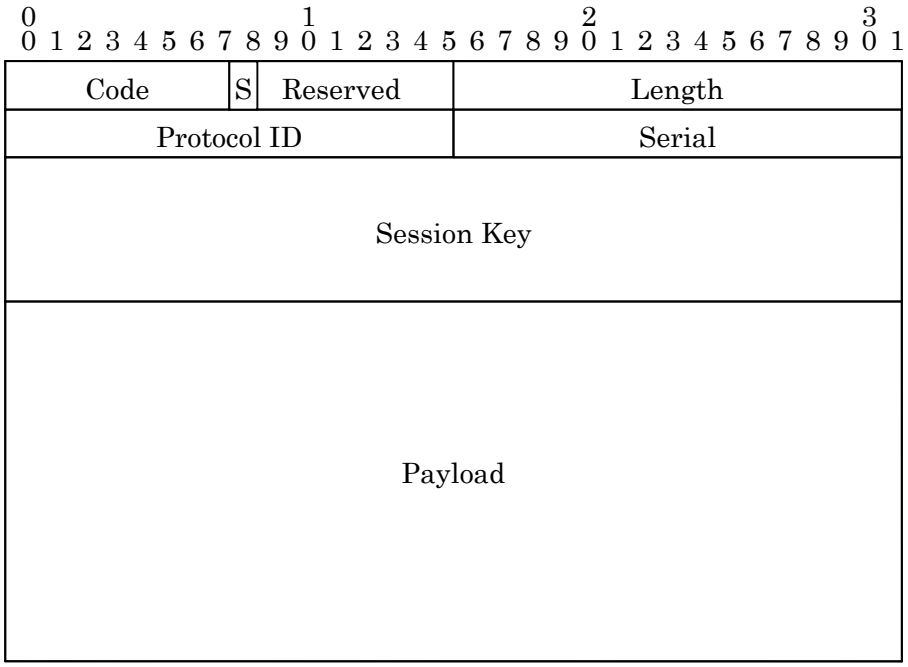

図 31　NULL 方式のメッセージフォーマット

各フィールドの内容は次の通りである。

Code	0（固定値）
S	認証に使うセッション鍵の指定。
Reserved	全ビット 0 に固定。
Length	このデータメッセージ全体の長さ。バイト単位。
Protocol ID	Payload の上位プロトコルの Protocol ID（2 バイト）。
Serial	シリアル番号。
Session Key	セッション鍵（12 バイト）
Payload	上位プロトコルのパケットデータ

- MTU

ネットワーク層に対する MTU は、メディア層の MTU から 20 バイト減じたものとする。

- 送信

Session Key フィールドにセッション鍵を入れる。Payload フィールドに入れる上位プロトコルのパケットデータは、平文である。

Serial にはシリアル番号を入れる。パケットを送信するたび 1 増える。初期値は何でも良い。シリアル番号は、MN と BR で別々に管理される。また、セッション毎に別々に管理される。

- 受信

Session Key フィールドに入っているデータは検査せずに無視する。認証は行わず、すべてのデータメッセージを受理する。

6.2. HMAC-MD5/HMAC-MD5/AES-CBC-128bit 方式

認証に MD5 と HMAC-MD5 を、セッション鍵配送に HMAC-MD5 を、データの秘匿に AES-CBC-128bit と MD5 を使う。

6.2.1. セッション鍵

セッション鍵の長さは 128bit(16byte)とする。

セッション鍵は、セッション毎に MN が作成した 16 バイトのセッション鍵の種に対してパスワードを鍵とした HMAC-MD5 を適用した結果の 16 バイトのバイト列とする。

セッション鍵の種を作成する方法は、以下の条件を満たす必要がある。

- 過去の情報から次のセッション鍵の種を予想することが難しい。
- 新たに作成したセッション鍵の種は、それ以前に使ったセッション鍵の種のいずれとも異なる。

この条件を満たすためには、例えば、ビーコンタイムスタンプ、MN の持つ現在時刻情報などを元に、適当に演算して作成することが考えられる。

6.2.2. 認証要求メッセージ

- **送信(MN)**

ICV オブジェクトには長さ 16 バイトのバイト列を入れる。バイト列は、次の方法によって求め、認証要求メッセージを作成する。

1. ICV オブジェクトを含む認証要求メッセージを作成し、ICV オブジェクト以外の要素をすべて適切に埋める。セッション鍵配送オブジェクトには、セッション鍵をそのまま入れず種を入れる。ICV オブジェクトの Value フィールドには、16 バイトの 0 を入れる。ここで作成された認証要求には、MISP ヘッダも含む。
2. 送信元 MAC アドレス、送信先 MAC アドレス、1.で作成した認証要求メッセージを繋げたバイト列を作る。
3. 2.で作成したバイト列に対して MD5 を適用し、16 バイトのバイト列を得る。
4. 3.で得られたバイト列に対して、パスワードを鍵とした HMAC-MD5 を適用し、16 バイトのバイト列を得る。
5. 4.で得られたバイト列を、1.で作成した認証要求メッセージの ICV オブジェクトの Value フィールドに上書きする。

- **受信(BR)**

受信した ICV オブジェクトは長さ 16 バイトのバイト列を含んでいる。長さが異なる場合には、認証失敗とする。ICV オブジェクトが含まれていない場合にも、認証は失敗とする。

ICV オブジェクトに含まれている 16 バイトのバイト列は、以下の方法により検査する。

1. 受信した認証要求メッセージの ICV オブジェクトの Value フィールドから 16 バイトのバイト列を取り出す。
2. 受信した認証要求メッセージの ICV オブジェクトの Value フィールドを 16 バイトの 0 に置き換えたバイト列を作る。このバイト列の長さは受信した認証要求メッセージの Length フィールドと同じ長さである。
3. 送信元 MAC アドレス、送信先 MAC アドレス、2.で作成したバイト列を繋げたバイト列を作る。
4. ３で作成したバイト列に対して MD5 を適用し、16 バイトのバイト列を得る。
5. 3.で得られたバイト列に対して、パスワードを鍵とした HMAC-MD5 を適用し、16 バイトのバイト列を得る。
6. 1.で得られたバイト列と 5.で得られたバイト列を比較し、一致していない場合には、認証失敗とする。

受信したセッション鍵配送オブジェクトは長さ 16 バイトのバイト列を含んでいる。長さが異なる場合には、認証失敗とする。セッション鍵配送オブジェクトが含まれていない場合にも、認証は失敗とする。セッション鍵配送オブジェクトに含まれていた 16 バイトのバイト列に対して、パ

スワードを鍵とした HMAC-MD5 を適用した結果の 16 バイトのバイト列を、セッション鍵とする。

以上のどの検査においても認証に失敗しなかった場合、認証に成功する。

6.2.3. 認証成功メッセージ

- 送信(BR)

ICV オブジェクトは、認証要求メッセージと、一点を除いて同じ方法で生成する。異なる一点は、HMAC-MD5 の鍵として、パスワードではなく、セッション鍵を使うことである。

- 受信(MN)

ICV オブジェクトは、認証要求メッセージと、一点を除いて同じ方法で検査する。異なる一点は、HMAC-MD5 の鍵として、パスワードではなく、セッション鍵を使うことである。

6.2.4. セッション終了メッセージ

- 送信

ICV オブジェクトは、セッション許可メッセージと同じ方法で生成する。

- 受信

ICV オブジェクトは、セッション許可メッセージと同じ方法で検査する。

6.2.5. データメッセージ

➢ フォーマット

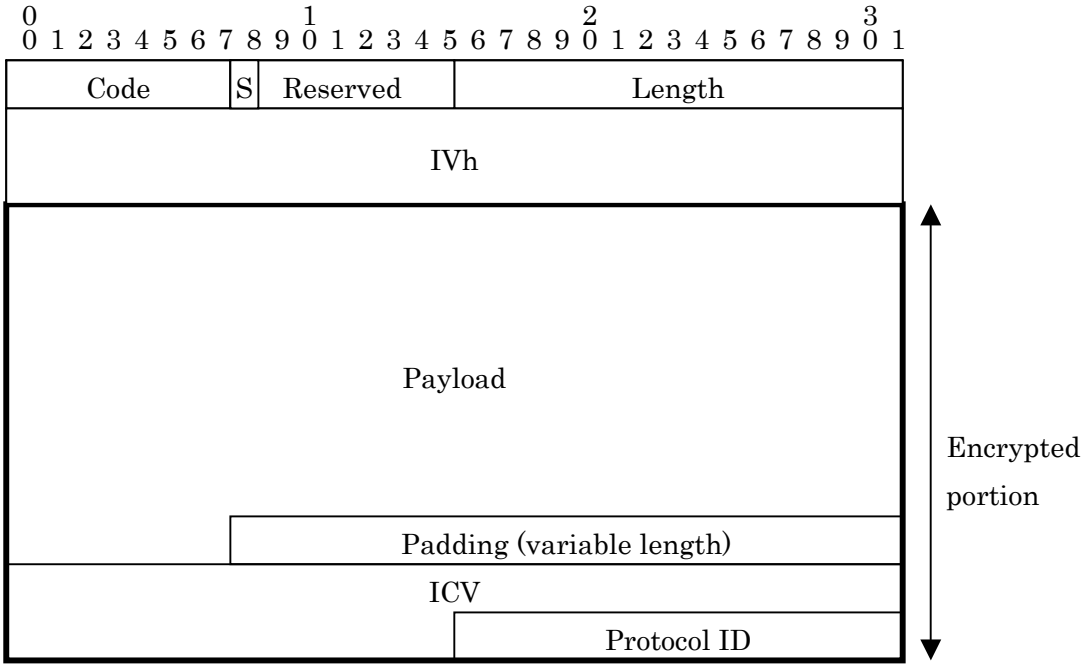

図 32　HMAC-MD5/HMAC-MD5/AES-CBC-128bit 方式のメッセージフォーマット

各フィールドの内容は次の通りである。

Code	0（固定値）
S	暗号化に使うセッション鍵の指定。
Reserved	全ビット 0 に固定。
Length	このデータメッセージ全体の長さ。バイト単位。12+16n(n は整数)でなければならない。そうでない場合には、このメッセージは無視される。
IVh	IV(Initialization Vector)の先頭 8 バイト
Payload	上位プロトコルのパケットデータ。任意のバイト数。
Padding	0 バイト以上 15 バイト以下の 0(Zero)。
ICV	6 バイトのバイト列。計算方法は後述。
Protocol ID	Payload の上位プロトコルの Protocol ID（2 バイト）

上の図の Encrypted portion は、鍵長 128 ビットの AES-CBC で暗号化されている。鍵として、

セッション鍵を使う。MISP ヘッダと IVh は暗号化されない。AES-CBC はブロック暗号であり、ブロックサイズが 16 バイトであるので、Encrypted portion のバイト数が 16 の倍数になるように Padding のバイト数を決定する。Padding の長さはどこにも保存しない。従って、復号時、元の Payload の正確なサイズはわからない。Payload の収められる上位のプロトコルは、パケット長を自ら管理する必要がある。

IVh は、セッション鍵が同じである限り、過去に使ったものと同じものが二度現れる確率が低くなるように擬似乱数を使って生成する。生成の方法としては、例えば、そのときの時刻、直前に使った IVh などを適当に演算する方法などが考えられる。CBC に用いる IV は、IVh を使って以下の方法で生成する。

1. IVh の各バイトを 1 ビット左ローテートする。このローテートはバイト毎に行われる。この結果、生成した 8 バイトのバイト列を IVl とする。
2. IVh を先頭 8 バイト、IVl を続く 8 バイトとする、16 バイトのバイト列を生成し、これを IV とする。

ICV は IVh の先頭 6 バイトとする。

- MTU

ネットワーク層に対する MTU は、メディア層の MTU から 20 バイト減じたものとする。

- 送信

以下の手順でデータメッセージを作成する。

1. 8 バイトの IVh を生成する。
2. フォーマットの項で述べた方法で、IVh から IV を生成する。
3. MISP ヘッダを生成する。
4. フォーマットの項で述べた方法で、ICV を生成する。
5. フォーマットに従って Encryption portion のバイト列を生成し、暗号化する。
6. MISP ヘッダと IVh を付け、データメッセージ全体を生成する。

- 受信

以下の手順で、受信したデータメッセージを検査する。

1. データメッセージ内の IVh を取出し、この IVh を使って IV を生成する。
2. Encrypt portion を復号する。
3. ICV を改めて計算し、Encrypt portion 内の ICV と比較する。一致していない場合には、このデータメッセージを破棄する。
4. Protocol ID に指定されたネットワーク層に Payload のデータを渡す。指定された Protocol ID をサポートしていない場合には、このデータメッセージを破棄する。

6.3. HMAC-MD5/HMAC-MD5/HMAC-MD5-128bit 方式

認証に MD5 と HMAC-MD5 を、セッション鍵配送に HMAC-MD5 を、データの認証に HMAC-MD5 を使う。

6.3.1. セッション鍵

セッション鍵の長さは 128bit(16byte)とする。

セッション鍵は、セッション毎に MN が作成した 16 バイトのセッション鍵の種に対してパスワードを鍵とした HMAC-MD5 を適用した結果の 16 バイトのバイト列とする。

セッション鍵の種を作成する方法は、以下の条件を満たす必要がある。

- 過去の情報から次のセッション鍵の種を予想することが難しい。
- 新たに作成したセッション鍵の種は、それ以前に使ったセッション鍵の種のいずれとも異なる。

この条件を満たすためには、例えば、ビーコンタイムスタンプ、MN の持つ現在時刻情報などを元に、適当に演算して作成することが考えられる。

6.3.2. 認証要求メッセージ

送受信共、HMAC-MD5/HMAC-MD5/AES-CBC-128bit 方式と同じ方式を用いる。

6.3.3. 認証成功メッセージ

送受信共、HMAC-MD5/HMAC-MD5/AES-CBC-128bit 方式と同じ方式を用いる。

6.3.4. セッション終了メッセージ

送受信共、HMAC-MD5/HMAC-MD5/AES-CBC-128bit 方式と同じ方式を用いる。

6.3.5. データメッセージ

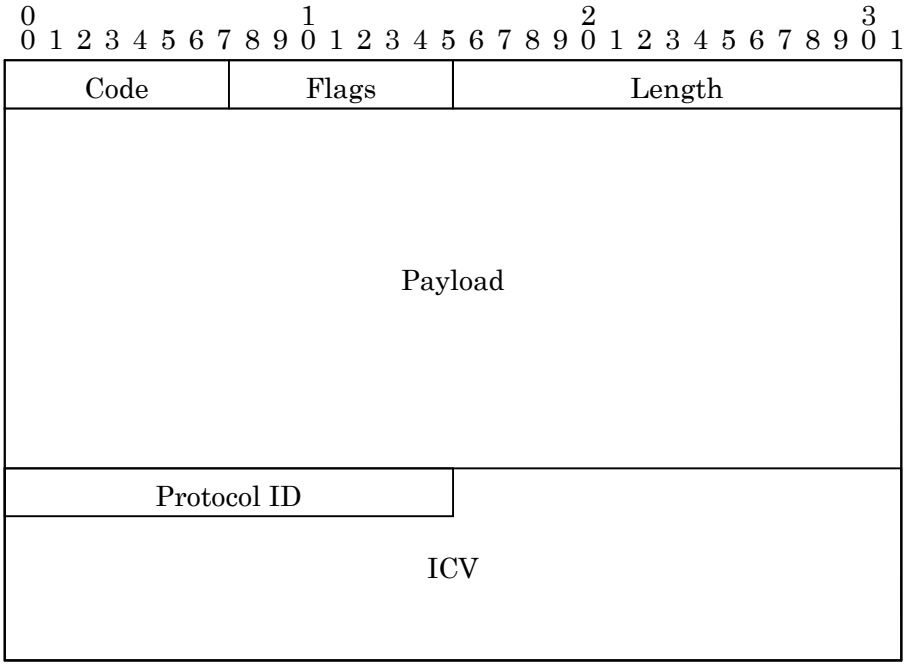

図 33　HMAC-MD5/HMAC-MD5/HMAC-MD5-128bit 方式のメッセージフォーマット

各フィールドの内容は次の通りである。

Code	データメッセージの場合は「0」
Flags	0 に固定。
Length	このデータメッセージ全体の長さ。バイト単位。
Payload	上位プロトコルのパケットデータ
Protocol ID	Payload の上位プロトコルの Protocol ID（2 バイト）
ICV	ICV（14 バイト）

上の図では、Payload の終わりが 32 ビット境界に一致しているように書かれているが、実際には、一致している必要はない。Payload フィールドと Protocol ID フィールドは、隙間なく隣り合っている。

ICV は次の方法で生成する。

1. 送信元 MAC アドレス、送信先 MAC アドレス、MISP ヘッダ（Code, Flags, Length フィールド）、Payload、Protocol ID フィールドをつなげたバイト列を作る。作られた

バイト列の長さは、

（送信元 MAC アドレスの長さ）＋（送信元 MAC アドレスの長さ）

＋（Length フィールドの値）－14

となる。

2. 1.で生成したバイト列に対して、セッション鍵を鍵とする HMAC-MD5 を適用する。その結果 16 バイトのバイト列を得る。
3. 2.で得られたバイト列の先頭 14 バイトを取り出し、ICV とする。

- MTU

ネットワーク層に対する MTU は、メディア層の MTU から 20 バイト減じたものとする。

- 送信

以下の手順でデータメッセージを作成する。

1. ICV フィールドを除いて、データメッセージの他の部分を生成する。
2. フォーマットの項で述べた方法で、ICV を生成する。
3. ICV フィールドを付加し、データメッセージ全体を生成する。

- 受信

以下の手順で、受信したデータメッセージを検査する。

1. データメッセージ内の ICV フィールドから ICV を取り出す。
2. フォーマットの項で述べた方法で、ICV を計算する。
3. 1.と 2.で求めたバイト列を比較する。一致していない場合には、このデータメッセージを破棄する。
4. Protocol ID に指定されたネットワーク層に Payload のデータを渡す。指定された Protocol ID をサポートしていない場合には、このデータメッセージを破棄する。

7. メディア

この章では、MISP によってサポートされている各メディアにおける個別の事柄について述べる。

7.1. Ethernet

7.1.1. MAC アドレス

6 バイトの Ethernet アドレスを、MAC アドレスとして使う。

7.1.2. フォーマット

MISP のメッセージを Ethernet 上で交換するときには、EtherType として 0x8893 を使い、Ethernet のペイロードに MISP ヘッダから始まる MISP メッセージ全体を格納する。

7.1.3. ビーコンメッセージ送信間隔

ビーコンメッセージは 1 秒毎に送信するものとする。

7.1.4. MN による BR の監視

MN は、ビーコンメッセージを受信すると、直ちにその BR を認識し、BR の一覧表に登録する。
MN は、最後にビーコンメッセージを受信してから 3.5 秒間経っても次のビーコンメッセージを受信できない BR について、存在しなくなったものとして扱い、BR の一覧表から削除する。

7.2. IEEE Std 802.11b

7.2.1. MAC アドレス

IEEE Std 802-1990 に規定された 48 ビットの「Universal LAN MAC address」を、MAC アドレスとして使う。

7.2.2. フォーマット

MISP のメッセージを IEEE802.11b のリンク上で交換する時には、RFC1042 で規定されたフォーマットに従ってカプセル化する。EtherType としては 0x8893 を使う。

7.2.3. ビーコンメッセージ送信間隔

ビーコンメッセージは 30 ミリ秒毎に送信するものとする。

7.2.4. MN の動作

受信装置が 1 台のＭＮの動作は以下を推奨する。

- ＭＮによるチャンネルのスキャン

MN は各チャンネルを 100 ミリ秒ずつ受信し、ビーコンを送信している BR の中から自己に必要なサービスを提供している BR の一覧表を信号強度の順に作成する。

- MN による BR の選択

MN は、一覧表の順に、成功するまで BR に認証要求メッセージを送出する。一覧表が尽きた場合はチャンネルのスキャンに戻る。

- MN による BR の監視

MN は以下の場合現在の BR は利用不可能になったとみなし、チャンネルのスキャンに戻る。

- ビーコンメッセージを 300 ミリ秒間 1 つも受信しなかった
- 過去 10 秒間ビーコンメッセージの 40%以上が受信できなくなった
- ビーコンメッセージとして受信した電波の信号強度が、30 秒間に渡って設定値を一度も上回らなかったとき。

8. ネットワーク層

この章では、MISP 層がサポートするネットワーク層の、それぞれに固有な事柄について述べる。

8.1. IPv4

8.1.1. プロトコル番号

0x0800 を使う。

8.1.2. IPv4 アドレス動的割当機能

- **機能**

MISP によって維持される Point-to-Point リンクの両端で使うべきアドレスを、BR が動的に決定し MN に対して通知することができる。

- **ビーコンメッセージ**

BR は、ビーコンメッセージに載せて IPv4 利用可能アドレス残存数オブジェクトを送信する。MN がこのオブジェクトを受信した場合、その内容が 0 だったならば、つまり、利用可能な IPv4 アドレスがない基地局に対しては、セッションを開始しようとしない。

- **認証要求メッセージ**

MN は、認証要求メッセージに IPv4 ローカルアドレスオブジェクトを入れて送信することによって、割り当ててほしい IPv4 アドレスを表明することができる。BR は、必ずしも要求通りの IPv4 アドレスを割り当てる必要はない。

- **認証成功メッセージ**

BR は、BR の IPv4 アドレスを IPv4 ローカルアドレスオブジェクトに、MN の使うべき IPv4 アドレスを IPv4 リモートアドレスオブジェクトに入れて、認証成功メッセージを送信する。

- **セッションの終了**

BR は、セッションが終了した場合、セッションに割り当てた IPv4 アドレスを解放する。

- **モバイル IP との連携**

MN は、セッションが成立した場合、セッションのアドレスが変化した場合、セッションが終了した場合、モバイル IP のモジュールに通知する。

8.1.3. パケットフィルタの存在を通知する機能

BR を通過していくパケットが、パケットフィルタの影響を受ける可能性があることを、MN に

通知することができる。

- IPv4 パケットフィルタオブジェクト

BR は、IPv4 パケットフィルタオブジェクトをビーコンメッセージに載せて、パケットフィルタに関する情報を MN に提供する。

現在は、IP ヘッダのソースアドレスによるフィルタに関する情報を提供することができる。このタイプのパケットフィルタがある場合、BR が認証成功メッセージの IPv4 リモートアドレスオブジェクトで指定した IPv4 アドレスをソースアドレスとして持つパケット以外は、正常に配送されない可能性がある。これはいくつかの IPv4 上のプロトコルに影響を及ぼす。例えば、この状況下で Mobile IPv4 を利用するためには、Reverse Tunnel 技術を使わなければならない。

9. 古いバージョンのプロトコルについて

9.1. EtherType

EtherType として 0xaaaa を使う。

9.2. ビーコン

BR は 30 ミリ秒毎にビーコンを送信する。

9.3. セキュリティ方式

セキュリティ方式のネゴシエーションは行われない。認証、鍵配送、データ通信は以下で説明するものを固定的に使用する。

新しいプロトコル上でこのバージョンのセキュリティ方式を選択したい場合には、セキュリティ方式のネゴシエーションにおいて、Security Type の番号として 1 を使う。ただし、これは、テストと過去との互換性のためだけに提供されるべきであり、実際の使用は推奨しない。

9.3.1. 認証方式

認証要求メッセージの ICV オブジェクトを使って認証を行う。

MN は、認証要求メッセージを送信するときに、認証要求メッセージ全体を入力として、パスワードを鍵とした HMAC-MD5 を計算する。この計算を行う認証要求メッセージには、ICV オブジェクト含まれているが、計算する際には、その Length フィールドは 18 であり、Value フィールドは 16 バイトの 0 で埋めておく。この HMAC-MD5 の計算結果の 16 バイトを、ICV オブジェクトの Value フィールドに入れ、認証要求メッセージを送信する。

認証要求メッセージを受信した BR は、同じ方法で ICV オブジェクトの Value フィールドの部分を計算する。つまり、ICV オブジェクトの Value フィールドにある 16 バイトの値を保存し、そこを 16 バイトの 0 で埋めた後、HMAC-MD5 を計算する。その結果と受信した ICV オブジェクトの Value フィールドに入っていた値を比較し、一致していれば、正当な認証要求メッセージであるとみなす。一致しない場合には、この認証要求メッセージは不当なものとして扱われる。

9.3.2. セッション鍵配送方式

セッション鍵は 16 バイトとし、MN と BR で同じバイト列を共有する。

セッション鍵は MN が乱数で生成する。BR にセッション鍵を配送するために、暗号化したセッション鍵を、認証要求メッセージのセッション鍵配送用データオブジェクトに入れて送信する。暗号化には、パスワードを鍵とする HMAC-MD5 の逆写像を使う。よって、復号化にはパスワードを鍵とする HMAC-MD5 を使う。

実際には、HMAC-MD5 の逆写像を計算することはできないので、MN は次の手順でセッショ

ン鍵を生成する。まず、乱数で 16 バイトのバイト列を生成し、それを暗号化されたセッション鍵とみなす。次に、その暗号化されたセッション鍵を HMAC-MD5 を使って復号化し、それをセッション鍵とする。

9.3.3. データ暗号方式

データの暗号化は行わない。パケット毎に認証のみを行う。認証には、HMAC-MD5 を使う。詳細については、この後のデータメッセージの章を参照のこと。

9.4. オブジェクト

以下に挙げる Type のオブジェクトのみを使用する。

2	タイムスタンプ
3	IPv4 ローカルアドレス
4	IPv4 リモートアドレス
5	ICV (Integrity Check Value)
6	NAI (Network Access Identifier; see RFC2486)
8	セッション鍵配送用データ

その他のオブジェクトは無視される。

9.5. メッセージ

9.5.1. データメッセージ

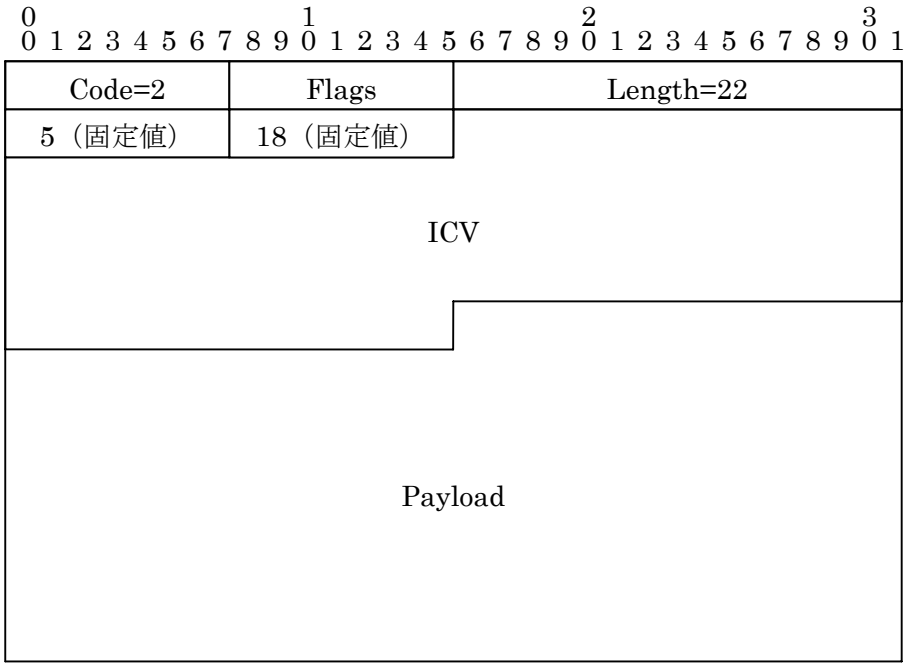

図 34　データメッセージフォーマット

各フィールドの内容は次の通りである。

Code	2
Flags	0（固定値）。どんな値が入っていても無視される。
Length	22（固定値）。その他の値が入っていた場合、動作は不定。
ICV	このメッセージ全体を入力とした、共有鍵を鍵とする HMAC-MD5 の計算結果。計算するときには、このフィールドは 16 バイトの 0 で埋めておくこと。
Payload	IPv4 パケットのデータ。

上位プロトコル層は、IPv4 のみをサポートする。新しいプロトコルのデータメッセージの Code フィールドが 0 であるのに対し、古いプロトコルでは 2 を使う。

9.5.2. 認証成功メッセージ

古いバージョンでは、ビーコンタイムスタンプオブジェクトとセッション鍵有効時間オブジェクトは送信されない。受信した場合は無視される。セッション鍵有効時間は 120sec で固定である。

9.5.3. 認証失敗メッセージ

古いバージョンでは、認証失敗メッセージは送信されない。受信した場合は無視される。

9.5.4. セッション終了メッセージ

古いバージョンでは、セッション終了メッセージは送信されない。受信した場合は無視される。

［完］