MBA 標準 0301 号

2004 年 6 月 30 日 標準化手続完了

MISAUTH プロトコル仕様書

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 0301 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「MISAUTH プロトコル仕様書」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

１．用語と概念

１．１ 移動端末

「MN」という略号で表す。
移動端末は自分の近くの基地局ルータを発見し接続を要求する。基地局ルータと接続された後、基地局ルータを介してインターネットと通信する。

１．２ 基地局ルータ

「BR」という略号で表す。
基地局ルータは固定的に設置され、固定的なインターネットへの接続を持っている。移動端末からのリクエストに応じて、移動端末とインターネットの間のルータとして動作する。

１．３ MISAUTH サーバ

「AS」という略号で表す。
MISAUTH サーバは固定的に設置され、基地局ルータからの認証要求を受け付ける。認証要求に基づきユーザの認証を行ない認証結果を基地局ルータに返答する。

１．４ 認証情報

アカウント識別子とパスワードの組。アカウント識別子は RFC2486 に定義された NAI のサブセットを使用する。RFC2486 で定義された NAI と異なる点は、

1. '@'による realm の指定が必須で有ること
2. username、realm に使用できる文字の種類に制限が有ること

の 2 点である。パスワードは構造を持たないバイト列である。双方とも、長さの上限は 253 バイトとする。

１．５ アカウント識別子

MIS ユーザ名と MIS ドメイン名を'@'で連結した文字列。MIS ユーザ名は英小文字、英大文字、数字、'-'、'_'からなる任意の文字列である。但し、先頭の文字は英大文字、英小文字である必要がある。MIS ドメイン名は英小文字、英大文字、数字、'-'からなる任意の文字列、もしくはそれらの文字列を'.'で連結した文字列である。MIS ドメイン名も先頭の文字は英大文字、英小文字である必要がある。

１．６ グループ

MIS ユーザ、BR はそれぞれ 0 以上の任意のグループに所属する事が可能である。グループは MIS ユーザの認証に使用される。あるグループに所属している MIS ユーザは自分が所属しているグループの BR しか使用することができない。AS では認証時にユーザの属するグループと BR の属するグループを検査する。グループ名の識別は 32bit の整数を使用する。

１．７ MIS ドメイン

MIS ユーザは必ず MIS ドメインに属している。MIS ユーザの属する MIS ドメイン情報は、BR より送信されるアカウント識別子に「MIS ユーザ名@MIS ドメイン名」の形式で含まれる。AS もそれぞれ MIS ドメインに属しており、BR から送信された MIS ユーザの認証要求に対して、MIS ユーザが属する MIS ドメインが自分が属する MIS ドメインと同じであれば認証を行うが、自分とは異なる MIS ドメインに属する MIS ユーザの場合は該当する MIS ドメインに属する AS、もしくはデフォルトで定義された AS に認証要求を転送する。この機能をプロキシ機能と呼ぶ。該当する MIS ドメインに属する AS、及びデフォルトで定義された AS が存在しない場合は認証失敗とする。

１．８ セキュリティ方式

MN と AS 間で使用される認証方式、セッション鍵の生成方式、データ秘匿方式の組を指す。

２．概要

MISAUTH プロトコルは、MIS システムにおいて認証サーバを利用するためのプロトコルであり、アプリケーション層のプロトコルとして動作する。MISAUTH プロトコルは、RADIUS プロトコルをベースに開発された。

AS は、BR に代わって MIS ユーザ名と MIS パスワードのペアの集合である認証情報を管理する。これにより、複数の基地局がアカウント情報を容易に共有することができる。又、プロキシ機能を利用する事により、分散管理されている MIS ユーザ情報に対して、容易にローミングサービスを提供する事が可能になる。

３．メッセージフォーマット

すべての MISAUTH プロトコルのメッセージは、MISAUTH プロトコルヘッダから始まる。MISAUTH プロトコルヘッダの次にくるものは、連続した 0 個以上のオブジェクトである。メッセージの種類は MISAUTH プロトコルヘッダによって識別される。現在は以下に示す 3 種類のメッセージが定義されている。

１． アクセス要求メッセージ
２． アクセス許可メッセージ
３． アクセス拒否メッセージ

それぞれのメッセージに含まれるオブジェクトについては後述する。

MISAUTH プロトコルのメッセージを BR と AS で通信する場合、及び AS 同士で通信する場合には UDP を用いる。認証要求を受け付ける AS 側のポート番号は通常 1812 を使用する。認証要求を送信する BR、もしくは AS 側のポート番号は任意である。MISAUTH プロトコルの１メッセージの最大長は 65535 バイトである。

図 1 メッセージフォーマット

３．１ MISAUTH プロトコルヘッダ

MISAUTH プロトコルヘッダは 20 バイトの大きさであり、以下の構造を持つ。

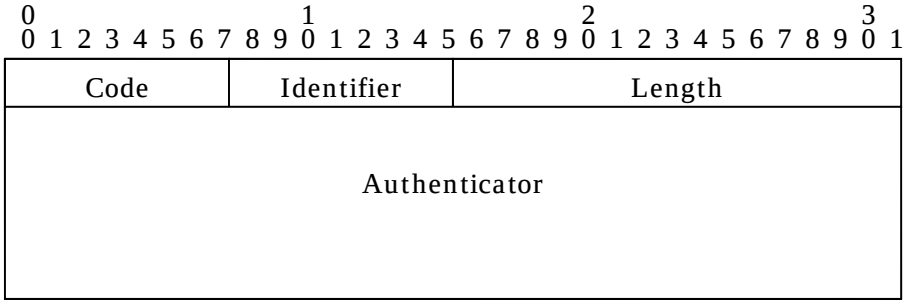

図 2 MISAUTH プロトコルヘッダ形式

Code フィールド（1 バイト）

この MISAUTH 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 ビットの符号なし整数である。

1　　アクセス要求
2　　アクセス許可
3　　アクセス拒否

Identifier フィールド（1 バイト）

アクセス要求メッセージとその返答のメッセージで同じ値をとり、その対応関係を表す。フィールドの長さは 1 バイトで、8 ビットの符号なし整数である。全てのメッセージは送信元 IP アドレス、UDP ポート番号、Identifier フィールドという 3 つの値の組によって、セッションが識別される。

Length フィールド（2 バイト）

この MISAUTH プロトコルヘッダから始まる、MISAUTH 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 MISAUTH メッセージの長さのほうが Length フィールドが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 MISAUTH メッセージの長さのほうが Length フィールドが示す長さよりも短い場合は、エラーであり、その MISAUTH メッセージは無視されなければならない。

Authenticator（16 バイト）

AS と BR 間、もしくは AS 間では、各 BR・AS ごとに固有の共有鍵を予め共有している。AS が BR、もしくは AS に応答メッセージを送信する場合、この共有鍵を使用して Authenticator に全て 0 をセットした状態のメッセージ全体に HMAC-MD5 を適用したハッシュ値を取得し、Autenticator に設定して BR、もしくは AS に送信する。応答メッセージを受信した BR、もしくは AS は同じ方法でハッシュ値を計算し、不正な応答メッセージでない事を確認する。このフィールドの長さは 16 バイトである。

３．２ MISAUTH プロトコルオブジェクト

MISAUTH プロトコル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。

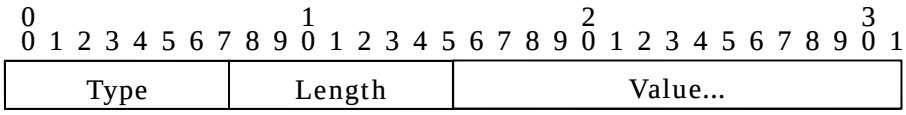

図 3 MISAUTH プロトコルオブジェクト形式

Type フィールド（1 バイト）

8 ビットの符号なし整数で、このオブジェクトの種類を示す。

1	NAI
4	基地局ルータ IPv4 アドレス
33	プロキシ要求
95	基地局ルータ IPv6 アドレス
200	認証用データ
201	認証用ハッシュ値
202	セッション鍵の種
203	セッション鍵
204	地理情報
205	セキュリティ方式
206	グループ種別

Length フィールド（1 バイト）

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。

Value フィールド（可変長：length – 2 バイト）

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。

４．オブジェクトフォーマット

４．１ NAI オブジェクト

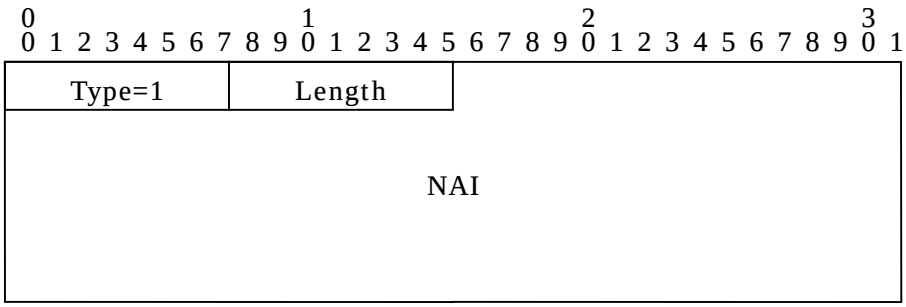

図 4 NAI オブジェクト

Type = 1

Length≧3

認証のためのユーザの識別子を示す。単純なバイト列として扱われる。長さは任意である。最後にヌル文字があった場合にも識別子の一部として扱われるため、オブジェクトの中にはターミネータとしてのヌル文字を含まないこと。

４．２ 基地局ルータ IPv4 アドレスオブジェクト

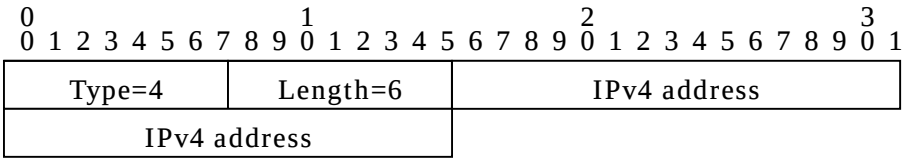

図 5 基地局ルータ IPv4 アドレスオブジェクト

Type = 4

Length=6

このオブジェクトが含まれる MISAUTH メッセージを送信した基地局ルータの IPv4 アドレスを示す。IPv4 形式のアドレスを設定する事ができる。Length の値が 6 でない場合はこのオブジェクトは無視される。

４．３ プロキシ要求オブジェクト

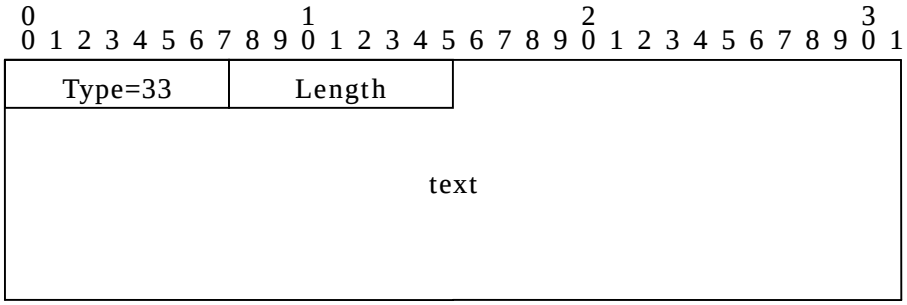

図 6 プロキシ要求オブジェクト

Type = 33

Lengtn≧2

AS がプロキシサーバとして動作する場合、このオブジェクトを必ず付加して他の AS に認証要求を転送し、このオブジェクトを付加して転送したメッセージが戻ってきた場合はこのオブジェクトを削除しなければならない。このオブジェクトに含めるデータはプロキシサーバとして動作する AS の任意である。従って、このオブジェクトを付加した AS 以外の AS は、このオブジェクトの値に依存した処理を行ってはならない。尚、プロキシサーバとして動作する AS を複数台経由する場合、本オブジェクトはメッセージ中に複数含まれる事ができる。

４．４ 基地局ルータ IPv6 アドレスオブジェクト

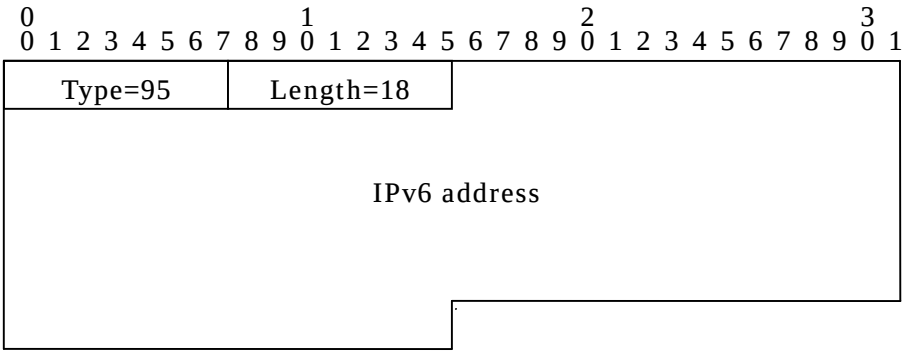

図 7 基地局 IPv6 アドレスオブジェクト

Type = 95

Length=18

このオブジェクトが含まれる MISAUTH メッセージを送信した基地局ルータの IPv6 表記のアドレスを示す。Length の値が 18 以外の場合はこのオブジェクトは無視される。BR が複数の prefix の IPv6 アドレスを持つ場合、本オブジェクトをメッセージ中に複数含めることができる。

４．５ 認証用データオブジェクト

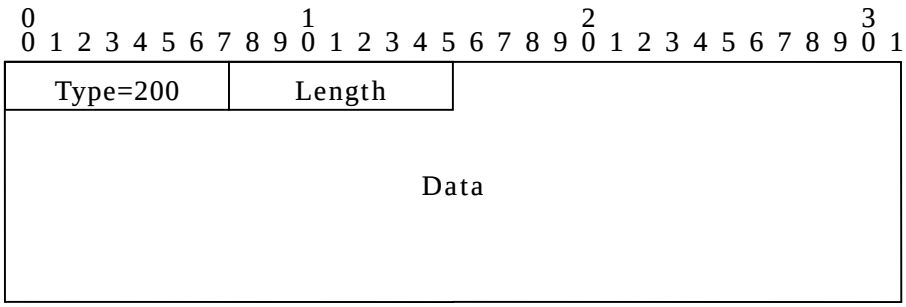

図 8 認証用データオブジェクト

type = 200

Length≧2

ユーザの認証に用いるデータを示す。長さは 253 バイト以下の任意の長さである。

４．６ 認証用ハッシュ値オブジェクト

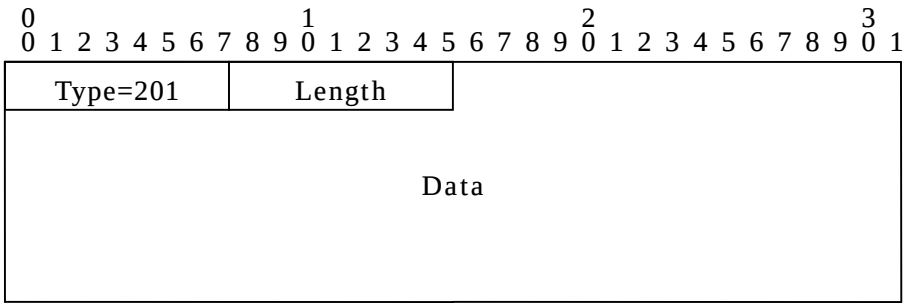

図 9 認証用ハッシュ値オブジェクト

type = 201

Length≧2

ユーザの認証に用いるハッシュの値を示す。長さは 253 バイト以下の任意の長さである。ハッシュ値の生成方法は後述のセキュリティ方式オブジェクトを使用して BR と AS の間で共有される。

４．７ セッション鍵の種オブジェクト

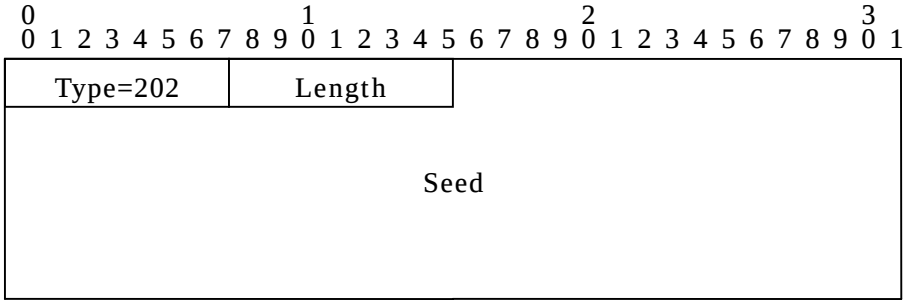

図 10 セッション鍵の種オブジェクト

type = 202

Lentgh≧2

認証が成功した場合に BR に送信されるセッション鍵を生成するための種を示す。長さは 253 バイト以下の任意の長さである。セッション鍵の生成方式は後述のセキュリティ方式オブジェクトを使用して MN と AS の間で共有される。

４．８ セッション鍵オブジェクト

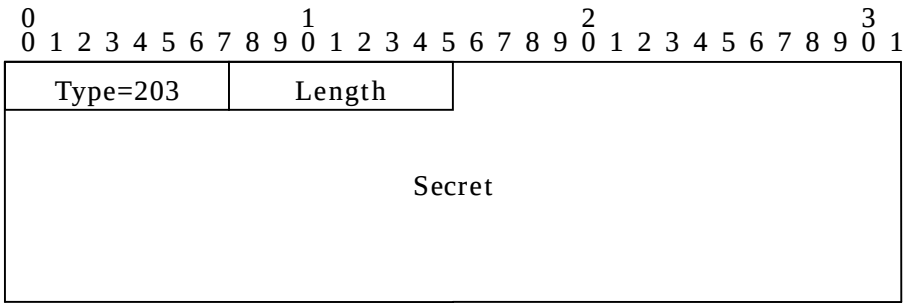

図 11 セッション鍵オブジェクト

type = 203

Length≧2

認証が成功した場合に BR に送信するセッション鍵を示す。長さは任意である。通常、セッション鍵は暗号化されている。セッション鍵の生成方式とセッション鍵の秘匿方式は、後述のセキュリティ方式オブジェクトを使用して BR と AS の間で共有される。

４．９ 地理情報オブジェクト

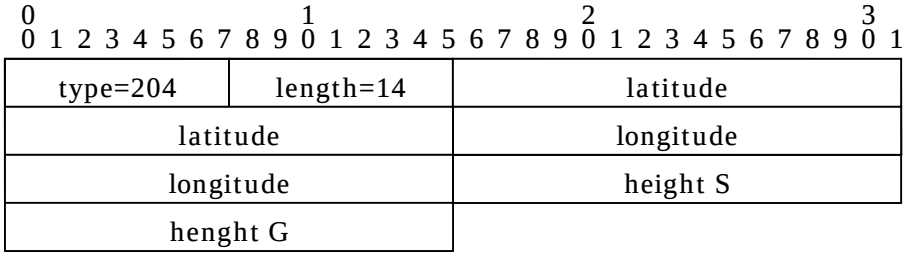

図 12 地理情報オブジェクト

type = 204

Length=14

Latitude　緯度。符号付 32 ビット整数。単位は 1/65536 度。

Longitude　経度。符号付 32 ビット整数。単位は 1/65536 度。

Height S　海抜。符号付 16 ビット整数。単位はメートル。

Height G　地上高。符号付 16 ビット正数。単位はメートル。

緯度・経度と高さの情報により地理的位置情報を示す。

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。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、正の値が海面、または地表より上を、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。Length は 14 で固定である。Length の値が 14 以外の場合はこのオブジェクトは無視される。

４．１０ セキュリティ方式オブジェクト

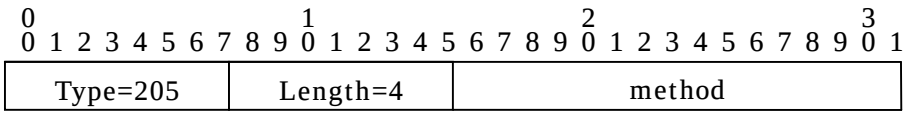

図 13 セキュリティ方式オブジェクト

type =205

length = 4

このオブジェクトが含まれる MISAUTH メッセージを送信した BR との間で使用される認証方式、セッション鍵の生成方式、データの秘匿化方式の組を示す。method は符号なしの 8 ビット整数であり、後述のセキュリティ方式を示す値を格納する。Length は 4 で固定である。Length の値が 4 以外の場合はこのオブジェクトは無視される。

４．１１ グループ種別オブジェクト

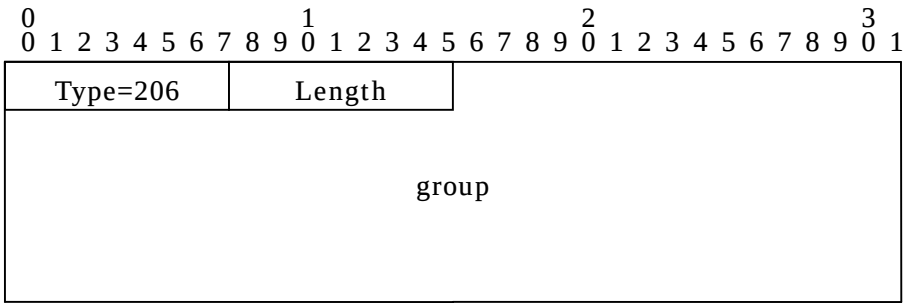

図 14 グループ種別オブジェクト

Type = 206

BR の所属グループを示す。所属グループは 32 ビットの整数で示される。BR が複数グループに属する場合は所属するグループの数だけ羅列できる。Length の値は(2+4n)である。Length の値が(2+4n)以外の場合、このオブジェクトは無視される。

５．メッセージフォーマット

５．１ アクセス要求メッセージ

アクセス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。

NAI オブジェクト
認証用データオブジェクト
認証用ハッシュ値オブジェクト
セッション鍵の種オブジェクト
セキュリティ方式オブジェクト
地理情報オブジェクト

アクセス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。

グループ種別オブジェクト
プロキシ要求オブジェクト
基地局ルータ IPv4 アドレスオブジェクト
基地局ルータ IPv6 アドレスオブジェクト

必要なオブジェクトが含まれていない場合は不正なメッセージとして接続を拒否する。不要なオブジェクトが含まれていた場合、それらは全て無視される。これらのうち、プロキシ要求オブジェクト、基地局ルータ IPv6 アドレスオブジェクトは複数含まれる事ができる。それ以外のオブジェクトが複数個含まれていた場合、最後のオブジェクトが有効となり、残りの重複するオブジェクトは無視される。

５．２ アクセス許可メッセージ

アクセス許可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。

セッション鍵オブジェクト
認証用ハッシュ値オブジェクト

アクセス許可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。

プロキシ要求オブジェクト

その他のオブジェクトが含まれていた場合、それらは全て無視される。

５．３ アクセス拒否メッセージ

アクセス拒否メッセージに必ず含まれるオブジェクトはない。
アクセス拒否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。

プロキシ要求オブジェクト

６．処理フロー

６．１ 正常に認証される場合の動作

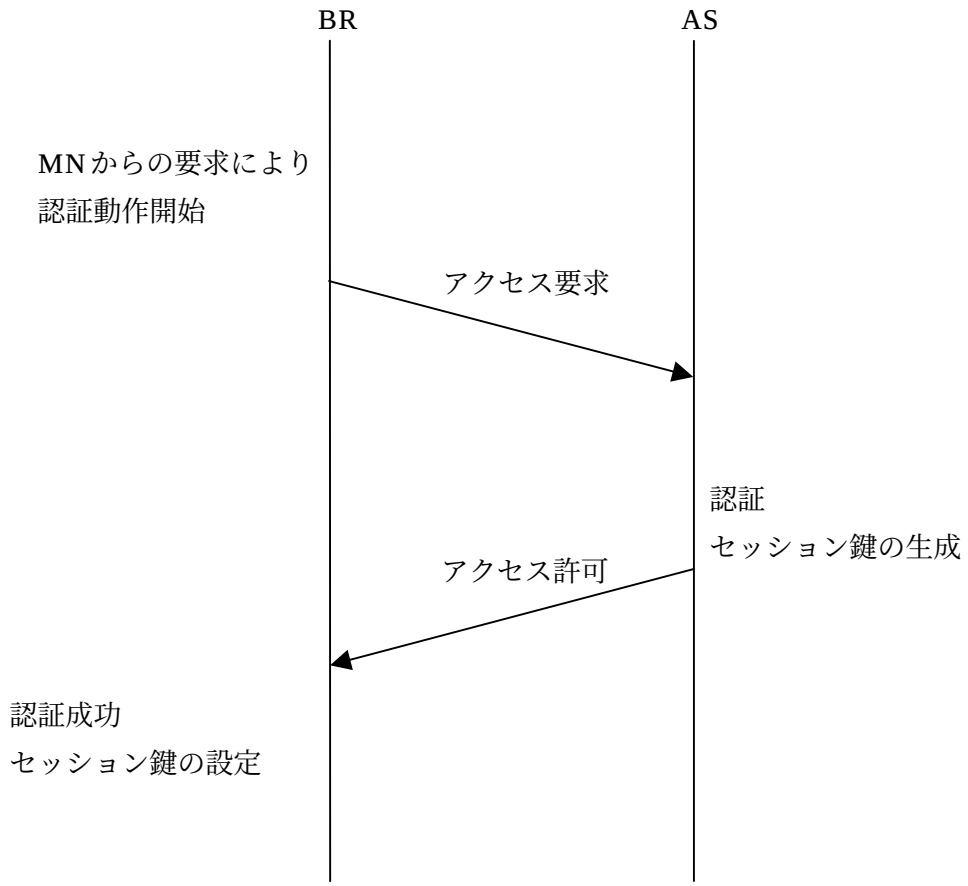

図 15 正常に認証される場合の処理フロー

BR から AS への認証要求が行われ、正常に認証される場合の処理フロー

１．MN からの認証要求開始

２．BR から AS へ認証要求

３．認証成功

４．セッション鍵の生成

５．AS から BR へのセッション鍵を含む認証成功メッセージの送信

６．認証成功

MIS ユーザの属するドメインが AS の属するドメインと等しい場合は AS が直接認証を行う。

６．２ 認証に失敗する場合の動作

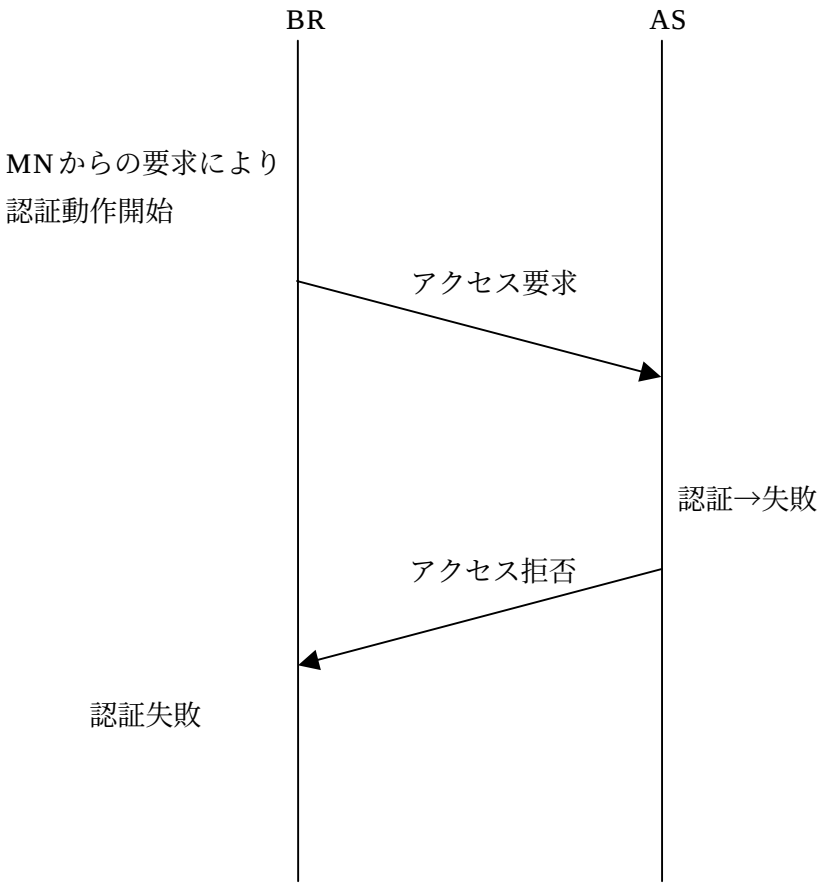

図 16 認証に失敗する場合の処理フロー

BR から AS への認証要求が行われ、認証が拒否される場合の処理フロー

１．MN からの認証要求開始
２．BR から AS へ認証要求
３．認証失敗
４．AS から BR への認証失敗メッセージ送信
５．認証失敗

MIS ユーザの属するドメインが AS の属するドメインと等しい場合は AS が直接認証を行う。

６．３ 何らかの原因により認証サーバからの応答が返らない場合の動作

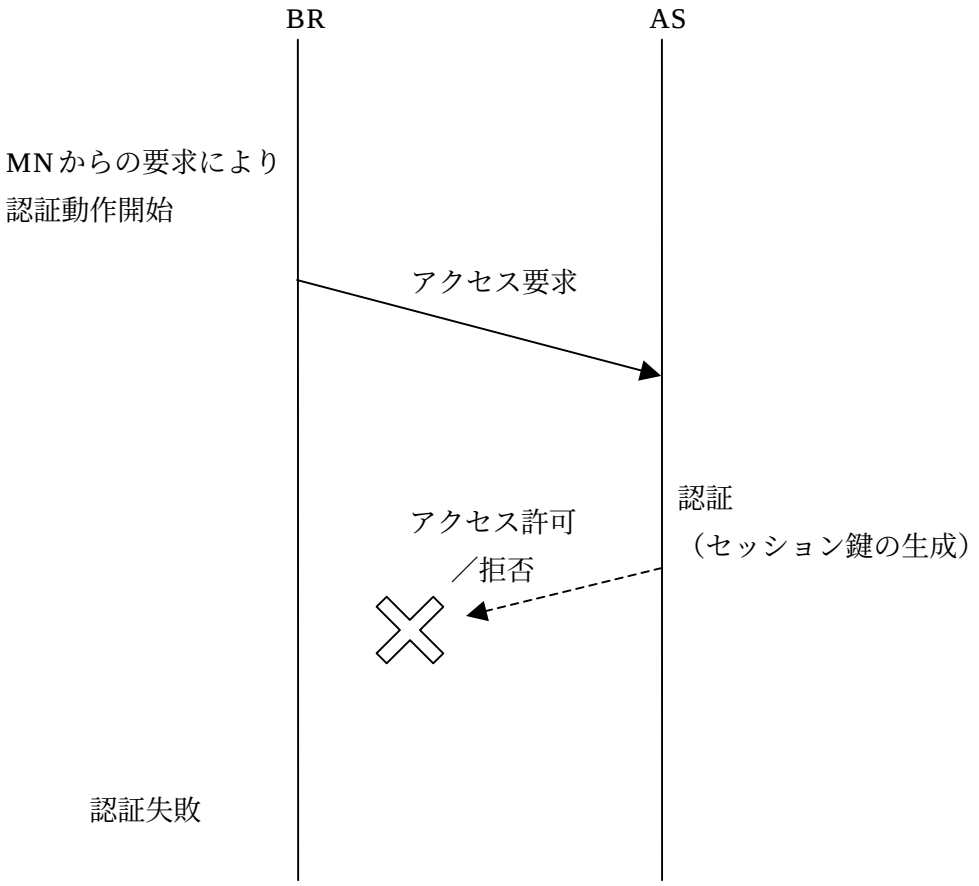

図 17 AS から応答が返らない場合の処理フロー

BR から AS への認証要求が行われるが、AS から応答がない場合の処理フロー

１．MN からの認証要求開始
２．BR から AS へ認証要求
３．認証成功/失敗
４．（認証成功の場合）セッション鍵の生成
５．AS から BR へのメッセージの送信

この場合認証要求は MN のタイムアウトにより失敗する。AS が何らかの理由により BR か

らの認証要求に応答できなかった場合、もしくはネットワークの理由等により応答が遅延した場合に発生する。

６．４ プロキシ機能により認証サーバ間で通信される場合の動作

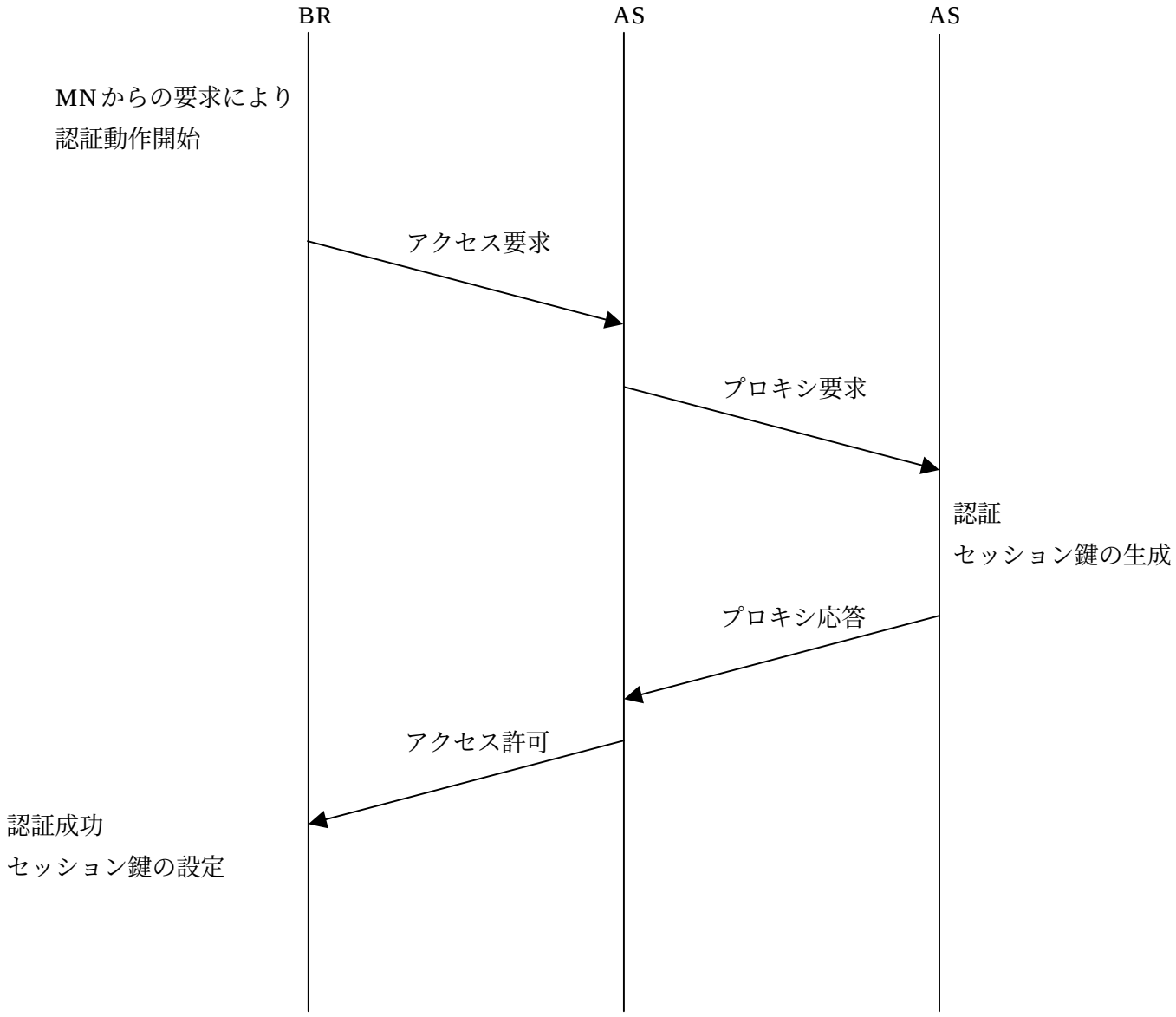

図 18 AS 間で通信される場合の処理フロー

BR から AS への認証要求が行われ、最初の AS がプロキシとして動作する場合の処理フロー。

１．MN からの認証要求開始

２．BR から AS へ認証要求
３．AS から他の AS へのプロキシ要求
４．認証成功
５．セッション鍵の生成
６．AS から AS へのセッション鍵を含むメッセージの送信
７．AS から BR へのセッション鍵を含むメッセージの送信
８．認証成功

MIS ユーザの属するドメインが AS の属するドメインと等しくない場合は AS が MIS ユーザの属するドメインに属する AS に対して認証要求を転送する。

７．認証サーバによる認証

AS は、BR から送られてきたアクセス要求メッセージの内容と、予め知っているユーザに関する情報を使って認証を行う。ユーザに関する情報には MIS ユーザ名、及び MIS パスワードがある。認証要求には認証用データと、セキュリティ方式オブジェクトにより共有される方式で計算された認証用データのハッシュ値が含まれている。AS では BR より送信された認証用データをセキュリティ方式オブジェクトで示された方式でハッシュ値を計算し、それが BR より送信された認証用データのハッシュ値と一致した場合、認証成功とする。セキュリティ方式オブジェクトで示される暗号化方式は１２節で述べる。

８．セッション鍵の作成

MN と AS は、同じ種、同じ秘密鍵、同じ方法を用いて、それぞれが独立にハッシュ値の計算を行う。秘密鍵は予め共有されている。種はアクセス要求メッセージのセッション鍵の種オブジェクトによって、方式はアクセス要求メッセージのセキュリティ方式オブジェクトによって、それぞれ BR から AS に渡される。

AS は認証に成功した後セッション鍵を計算し、セッション鍵オブジェクトにセッション鍵を入れたアクセス許可メッセージを送信する。認証サーバから送信するセッション鍵はセキュリティを確保するために通常は秘匿される。秘匿の方式は BR から送信されたセキュリティ方式オブジェクトにより共有される。セキュリティ方式オブジェクトで示される暗号化方式は１２節で述べる。

９．多重利用の防止

複数人が単一のアカウントを使用してログインし、不正にネットワーク資源を使用する事を、ここでは多重利用と呼ぶ。この多重利用による不正使用を防止するために、AS では以下の方法により多重利用を検出し認証を拒否する。

９．１ ブラックリスト

AS が多重利用だと判断したユーザ ID は AS が内部で保持しているブラックリストに登録する。一度ブラックリストに登録されたユーザは、以後 10 分の間認証を拒否する。ブラックリストの登録から 10 分以後の認証時に、そのユーザ ID はブラックリストより自動的に取り除かれる。

９．２ 検査方式

1. 前回の認証より 10 分以上経過している場合は、新規接続とみなし多重利用のチェック対象から除外する。
2. 移動距離が電波到達距離×２×マージン以内の場合、同一もしくは隣接する BR に接続変更したものとみなし多重利用のチェック対象から除外する。
3. 前回の認証より経過時間が 0 の場合は多重利用とみなし、接続を拒否する。同時にブラックリストに当該ユーザを登録する。
4. 移動速度が MN の制限速度×マージンを越えた場合は多重利用とみなし、接続を拒否する。同時にブラックリストに当該ユーザを登録する。

- 電波到達距離は現在は 200m と設定されている。
- マージンは現在は 2 と設定されている。
- MN の制限速度は現在は時速 60km と設定されている。
- 距離は以下の計算式により算出する

$$\text{距離} = 2 \times R \times \sqrt{\sin\left(\frac{la2 - la1}{2}\right)^2 + \cos(l2) \times \cos(l1) \times \sin\left(\frac{lo2 - lo1}{2}\right)^2}$$

R	地球の半径(6367000.0)		
la1	地点 1 の経度	la2	地点 2 の経度
lo1	地点 1 の緯度	lo2	地点 2 の緯度

９．３ 制限事項

1. 一人のユーザが複数の端末を使用する場合や、同一行動をとる複数のユーザが同一のユーザ ID を使用するなど、数百メートルの単位内で多重利用した場合、ハンドオーバしたのか多重利用なのか区別できないため、多重利用を検出できない。

2. 距離の算出は直線で近似しているので、長距離では誤差が生じる（但し、多重ログインの検出には十分使用できる）。

９．４ 今後の拡張

現在は固定値で保持している MN の制限速度を、MN の設置されている状況に合わせて MN ごとに設定可能とし、多重利用の検出の精度を向上させる必要がある。

１０．プロキシ機能

BR、もしくは他の AS からの認証要求を、他の AS に転送する機能を AS のプロキシ機能と呼ぶ。プロキシ機能を使用して認証要求を他の AS に転送する場合、 受信したメッセージの一番最後にプロキシ要求オブジェクトを必ず追加しなければならない。このオブジェクトに含める値はプロキシサーバとして動作する AS の実装に依存するので自由に使用して良いが、このオブジェクトを付加した AS 以外の AS はこのオブジェクトの値に依存した処理を行ってはならない。

他の AS に転送した認証要求の応答を受信した場合、必ず自分が追加したプロキシ要求オブジェクトを削除しなければならない。

プロキシ機能を使用して他の AS に認証要求メッセージを送信する場合、AS では特別な制御を行わず、一度の認証要求に対して一度だけ認証要求を送信する。

プロキシ先の AS から応答メッセージが受信できない場合、AS では BR、もしくは送信元の AS に対しての何らかの応答を含む処理を何も行わず、送信元のタイムアウト処理に全ての制御をまかせる。

受信したパケットに含まれるプロキシ要求オブジェクトの数があまりに多い場合、AS は認証要求を拒否しても良い。認証要求を拒否するプロキシ要求オブジェクトの数は AS の実装に依存する任意の数である。

プロキシ機能による通信のうち、アクセス許可メッセージにはセッション鍵が含まれているので、データを BR から送信されたセキュリティ方式オブジェクトにより共有される方法により秘匿する。セキュリティ方式オブジェクトで示される暗号化方式は 12 節で述べる。

- 認証要求を拒否するプロキシ要求オブジェクトの数は現在は 64 と設定されている。

１１．認証サーバの多重化

認証を確実に高速に処理するために AS を多重化する事が可能である。AS を多重化する場合、BR、及び AS は以下の動作を行うべきである。

１１．１ BR の動作

BR が AS に認証要求を送信する際に、複数の AS が指定されてる場合の動作を以下に示す。

１．指定されている全ての AS に対して、同時に認証要求を送信する。
２．応答が一番早い AS の認証結果を使用する。

１１．２ AS の動作

AS がプロキシサーバとして動作する際に、複数の AS が指定されている場合の動作を以下に示す。尚、自分以外の MIS ドメインに属する AS を複数指定する場合、優先順位を指定しなければならない。

１．プロキシ機能を使用して他の AS に認証要求を転送する際に、19～21（疑似乱数）回毎の認証要求はプロキシサーバとして指定された全ての AS に認証要求を転送する。
２．全ての AS に認証要求を転送しない場合、過去 5 分以内に認証要求を送信しているが、過去 5 分以内に応答を受信していない AS を除外した中で、最も優先順位の高い AS に認証要求を転送する。
３．2. に該当する AS が存在しない場合は、最終送信時刻が最も古い AS に対して認証要求を転送する。最終送信時刻が同じ場合は、優先順位が最も高い AS に認証要求を転送する。

１２．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。

HMAC-MD5/HMAC-MD5/HMAC-MD5	1

右側の数字はセキュリティ方式オブジェクトに含まれるセキュリティ方式の値である。
以下ではセキュリティ方式の詳細を説明する。

１２．１ HMAC-MD5/HMAC-MD5/HMAC-MD5 方式

認証に HMAC-MD5 を、セッション鍵生成に HMAC-MD5 を、データの秘匿に HMAC-MD5 と排他的論理和を使用する。

１２．１．１ 認証用ハッシュ値の生成方式

認証用のハッシュ値を計算するために、HMAC-MD5 を使用する。認証要求メッセージに含まれる認証データに対して、MN と AS で予め共有している MIS パスワードを鍵として HMAC-MD5 を適用し 16 バイトのバイト列を取得する。このバイト列が認証要求メッセージに含まれている認証データハッシュ値オブジェクトの値と一致した場合は認証が成功する。

１２．１．２ セッション鍵の生成方式

認証が成功した場合に MN と AS で共有するセッション鍵を計算するために、HMAC-MD5 を使用する。認証要求メッセージに含まれるセッション鍵の種に対して、MN と AS で予め共有している MIS パスワードを鍵として HMAC-MD5 を適用し 16 バイトのバイト列を取得する。これがセッション鍵となる。

１２．１．３ セッション鍵の秘匿方式

認証が成功した場合に AS から BR、もしくはプロキシ機能により AS 間で送信されるセッション鍵を秘匿するために HMAC-MD5 と排他的論理和を使用する。認証要求メッセージに含まれる認証用ハッシュ値に対して、BR と AS、もしくは AS 間で予め共有している秘密鍵を利用して MHAC-MD5 を適用し得られた 16 バイトのバイト列とセッション鍵の排他的論理和を計算し 16 バイトのバイト列を取得する。これが秘匿されれたセッション鍵となるのでセッション鍵オブジェクトに設定し BR に送信する。秘匿したセッション鍵を復号化するために、認証する AS は認証用ハッシュ値を必ず含めて応答メッセージを送信しなければならない。

１３．付録

１３．１ 図表番号

［完］