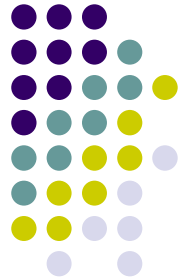
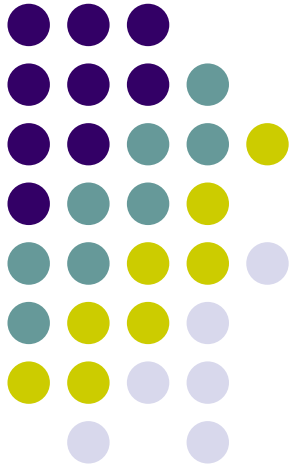
本資料について



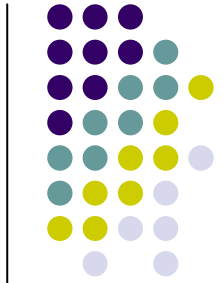
本資料は下記文献を基にして作成されたものです．文書の内容の正確さは保証できないため，正確な知識を求める方は原文を参照してください．

著者：モバイルブロードバンド協会
文献名:MISプロトコル(MISP)仕様書　Ver.1.02
発表日：2004年 4月 5日 公開

無線LANの問題とMISプロトコル（MISP）



渡邊研究室　　金本　綾子

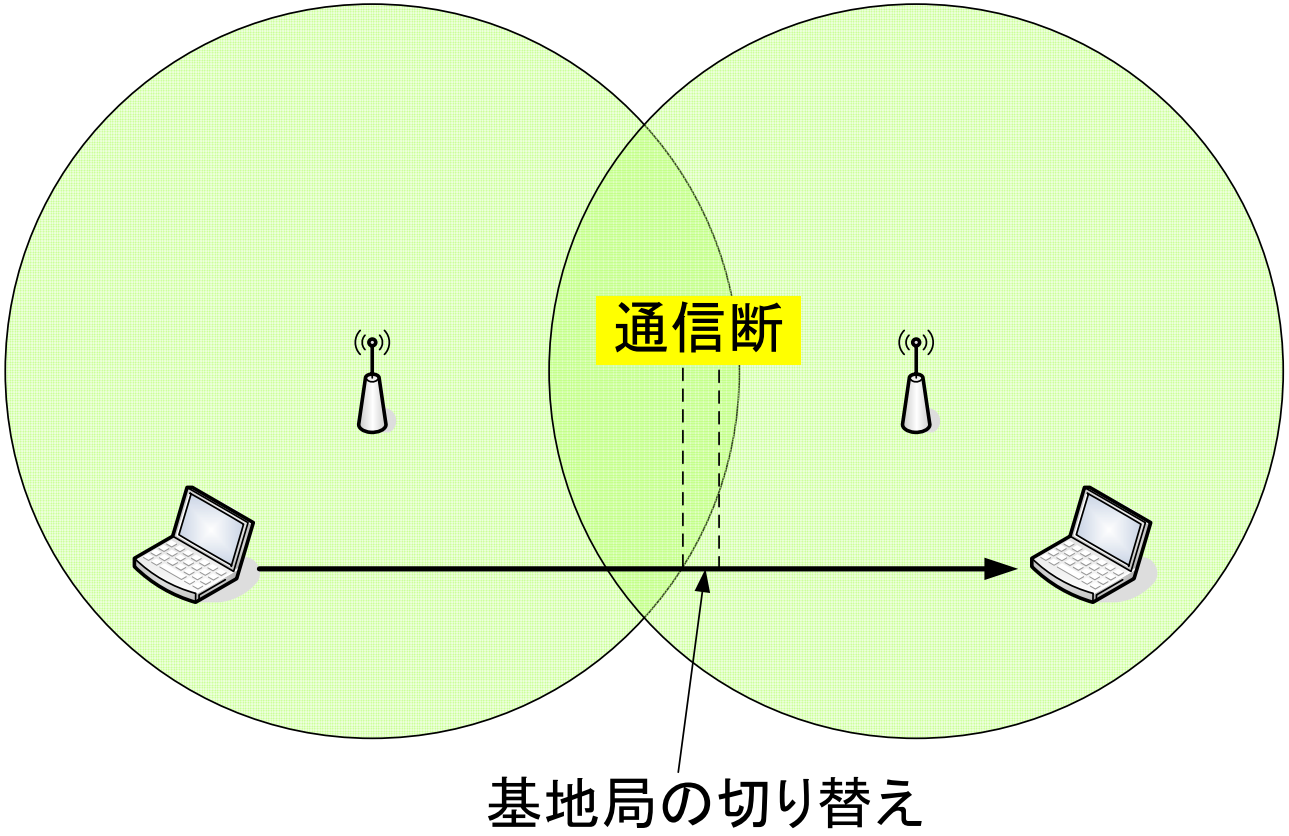


無線LANの問題と今後の課題

無線LANのハンドオーバーの実情

端末は基地局との通信が切れたら新たな基地局を探す

—秒～分単位の間通信が切断される



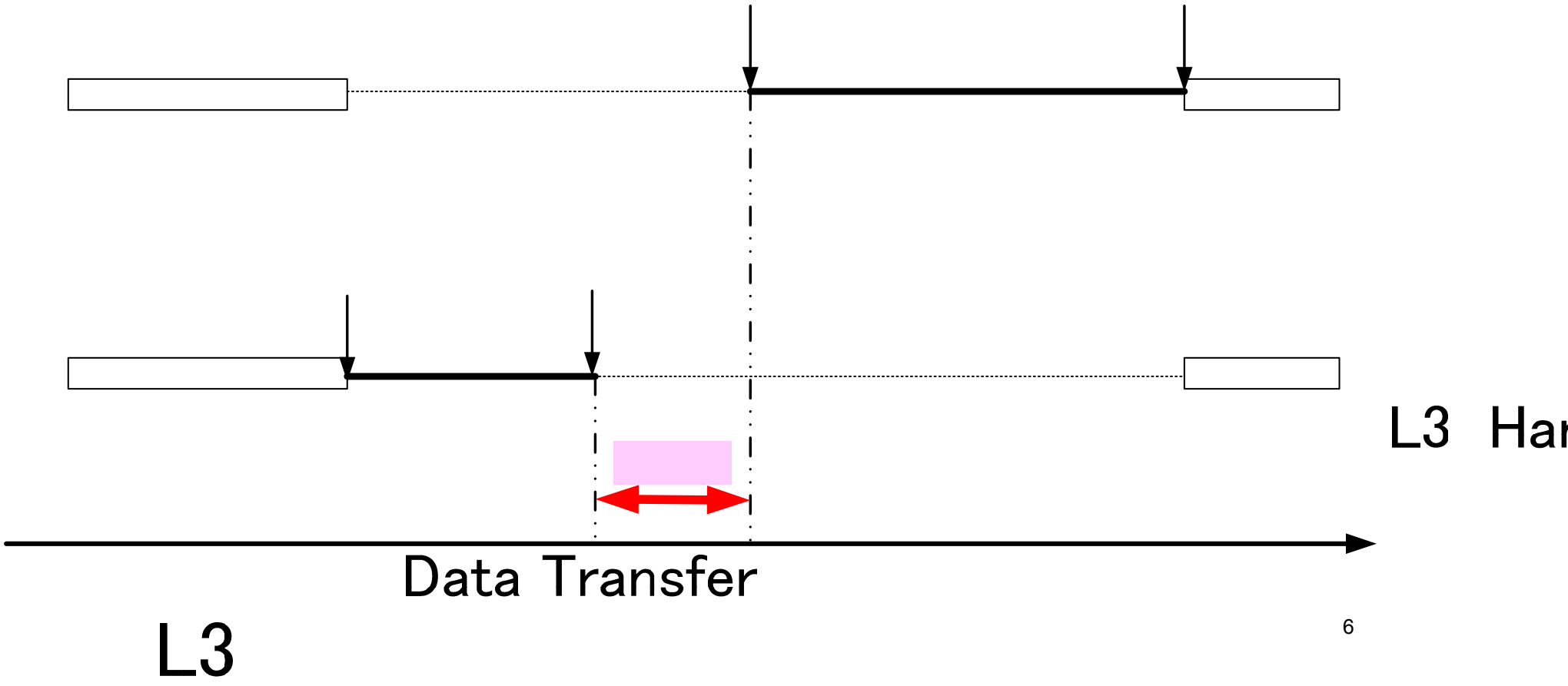
従来の無線LANの構造的問題

L2（データリンク）技術

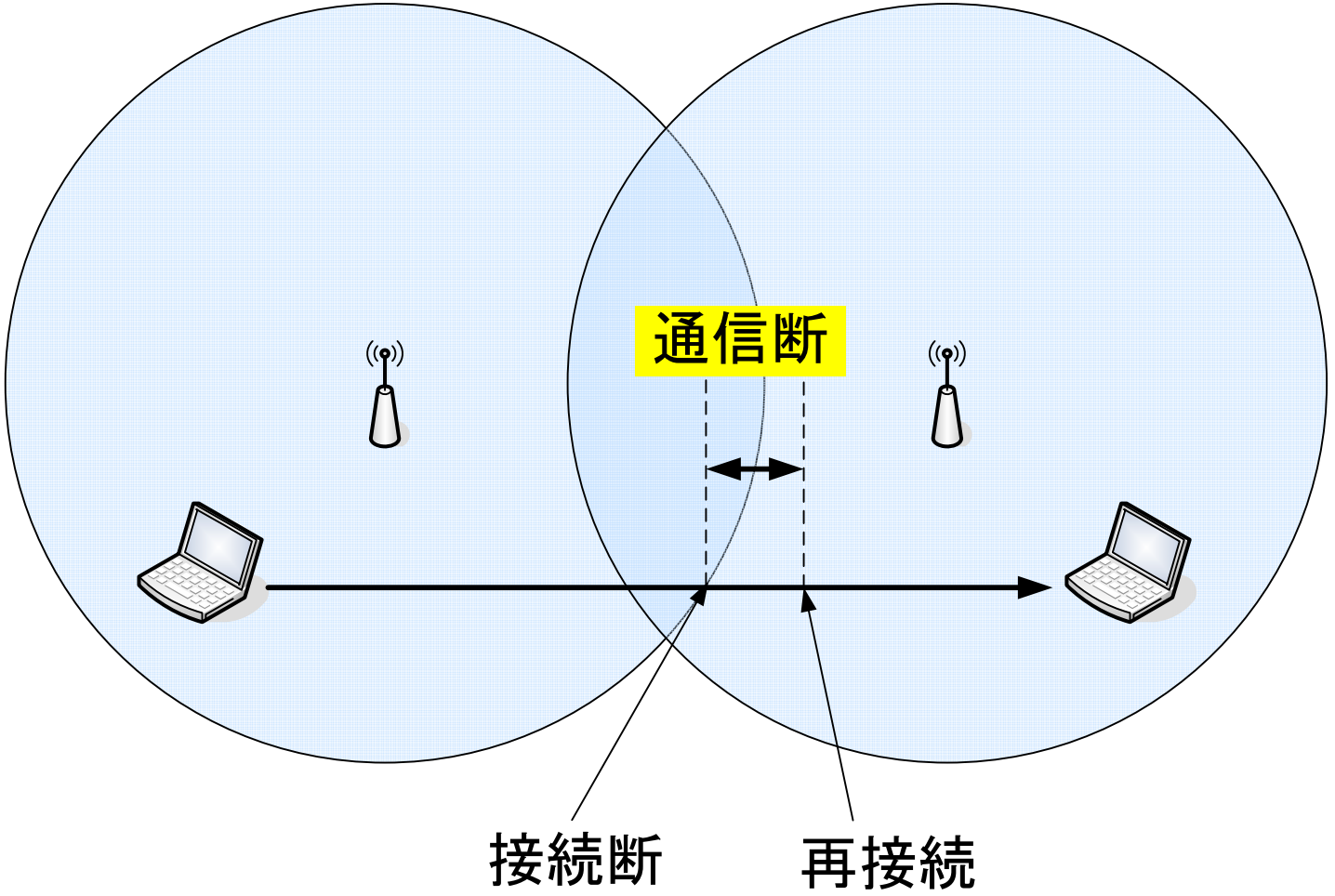
— L3（IP）との連携が悪い

広域（高速）移動体通信には適用できない

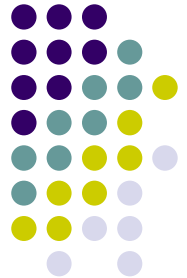
L2 and L3 ハンドオーバー



無線LANの再接続
（移動しながらの場合）

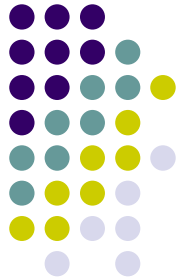


接続確立までの手間



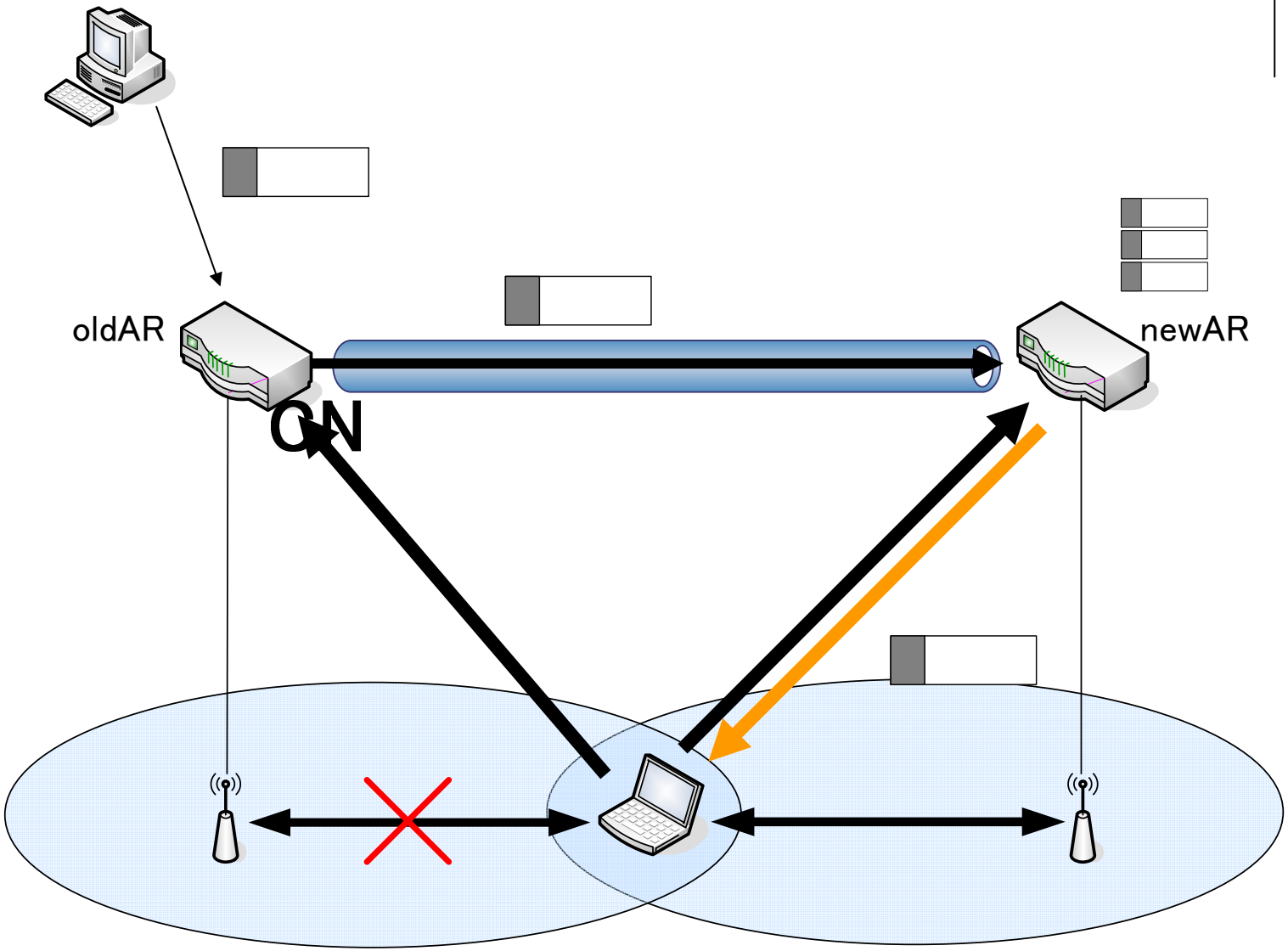
- 基地局の発見
- 自分の使える基地局であることの確認
  - —SSID？
- 適切な基地局の選定
  - —ビーコンの強度などにより

接続確立までの手間



- 基地局への接続要求
  - ―接続要求パケットの送出
- 接続パラメータの設定
  - ―セキュリティ等
- L2接続完了確認
- IPアドレスの割り当て

FMIPv6では



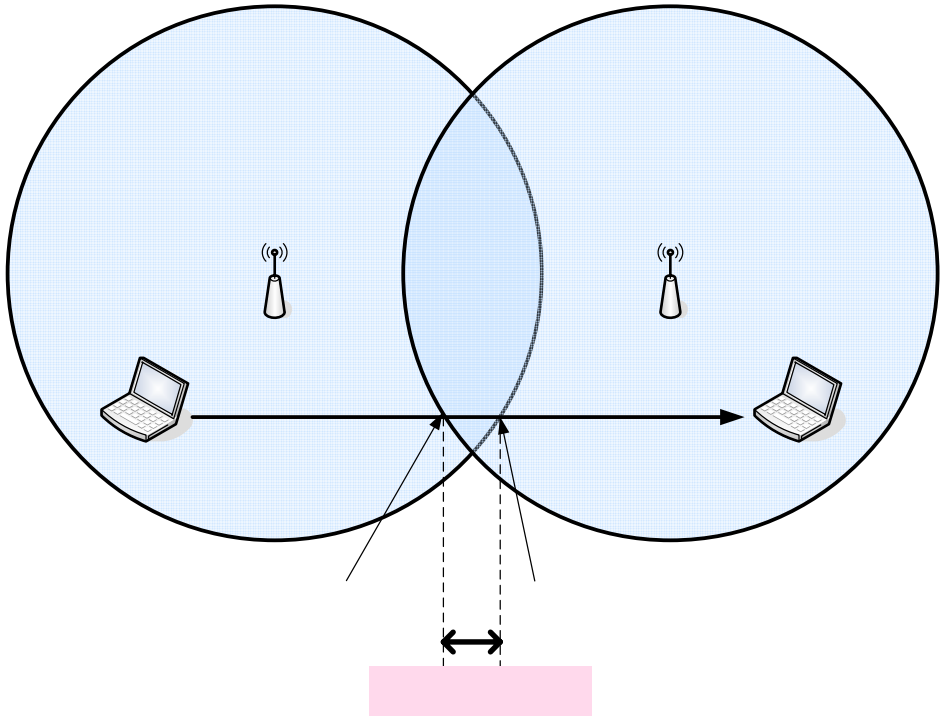
FMIPv6の問題点

- パケットの損失は抑えられるが、基地局間（デフォルトルータ間）の連携は非常に面倒
- 高速移動には対応できない
- 接続確立のために遅延が発生

無線LANとスムーズハンドオーバー

- 今の基地局と接続が切断する前に新たな基地局と接続しておく
  - — 同時に複数の基地局と接続できる必要

現状の規格ではL2では無理



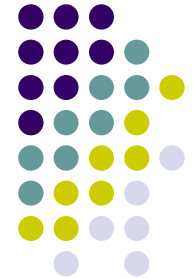
MISプロトコル

L2でハンドオーバーを実現

- 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が可能。
- 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可能。

MBAによる草案

MISプロトコルについてはじめに



MISプロトコルは、基地ルータと端末を接続するために設計された。

- 接続されたメディア上の基地ルータを自ら発見できる。
- メディアへ接続されると自動的に基地ルータを認識し、基地ルータとの間の通信路を確立することが可能。

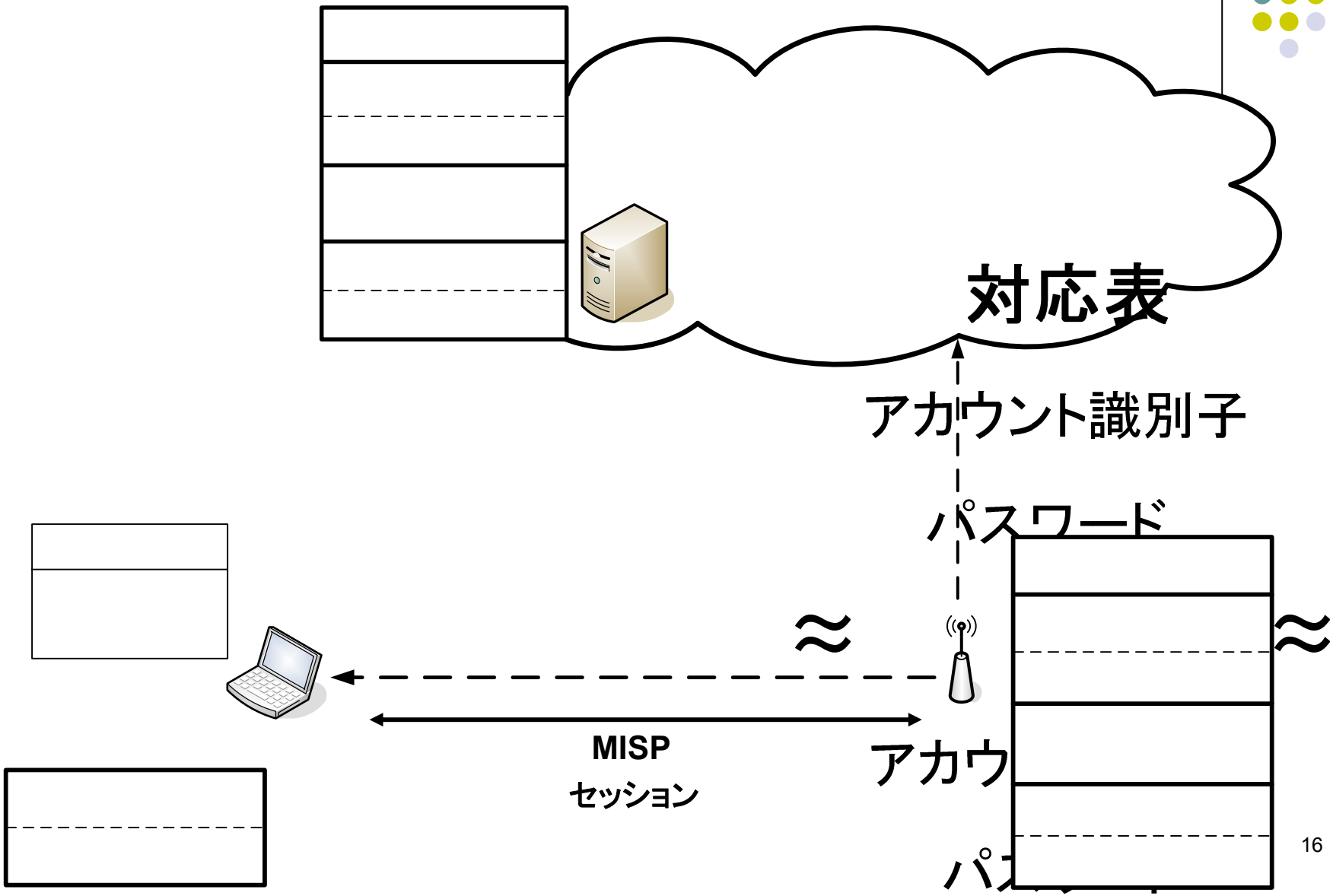
信頼度の高いセキュリティ

ーMNとBR間はユーザ名とパスワードによる認証。

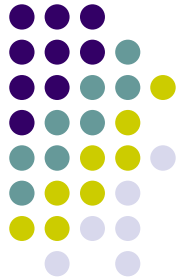
ー基地ルータと端末間で鍵を交換し、通信の各パケットについて、認証および暗号化。

⇒ これらの認証は高速に行われている

MISPの構成



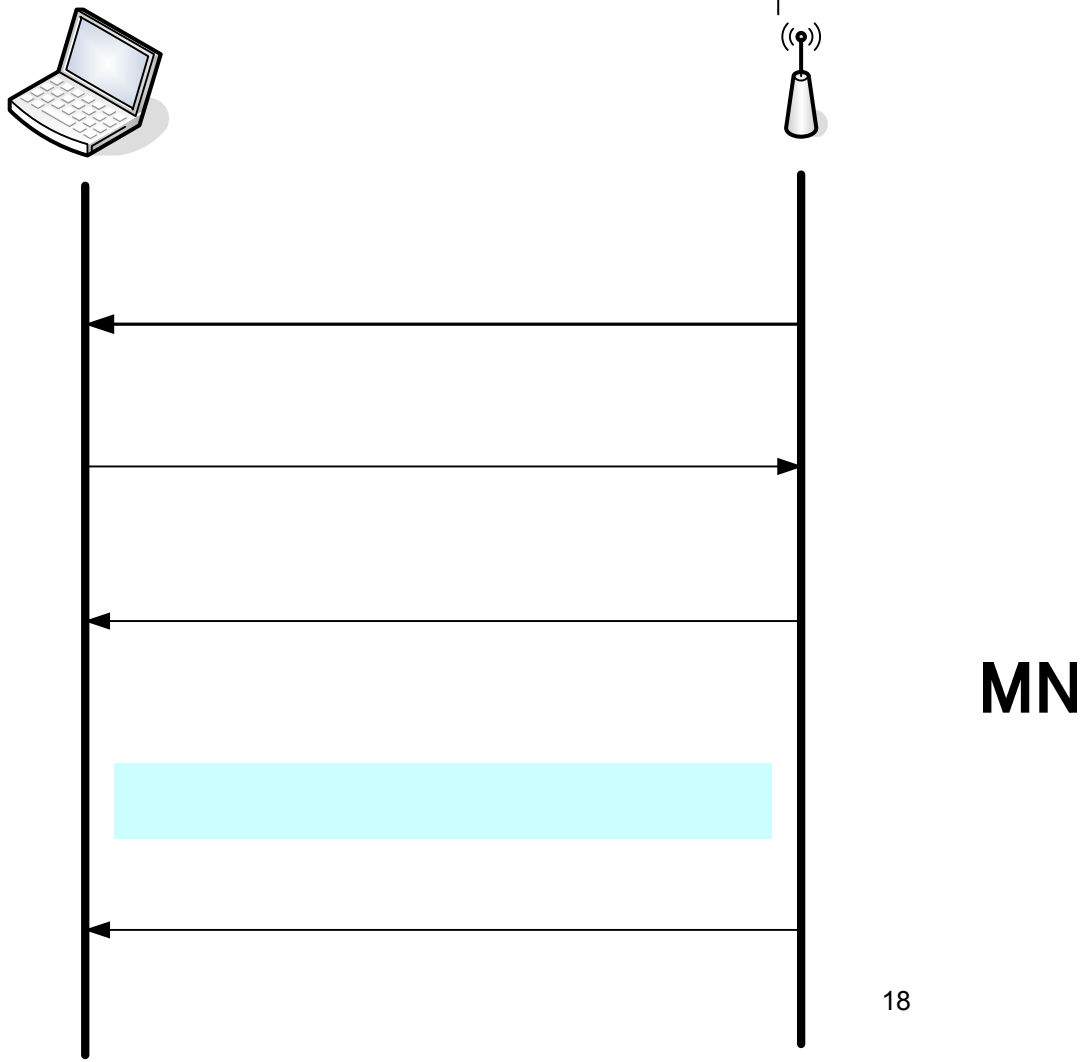
MISPの機能



- 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
- 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

セッションの開始

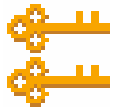
- ビーコンメッセージの受信（MN）
- 認証要求メッセージの受信（BR）
- 認証成功メッセージの受信（MN）
- 認証失敗メッセージの受信（MN）



ビーコンメッセージの受信（MN）

①セッションを開始しようとする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内のセキュリティ方式オブジェクトを見て、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を送信する。

認証要求メッセージの受信（BR）

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が規定値の範囲内であるか確認する。

②認証と鍵配送の操作を行う。

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。

④認証成功メッセージを作成する。

⑤認証成功メッセージに対して認証の操作をする。

⑥認証成功メッセージを送信する。

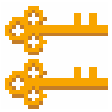
認証成功メッセージの受信（MN）

①メッセージを認証する。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する。

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、セッション鍵の有効時間を設定する。

認証失敗メッセージの受信（MN）

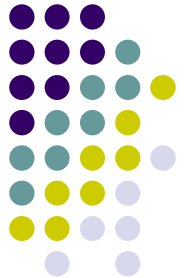
MNは、認証失敗メッセージを受信すると、直ちにセッションの開始処理が失敗したとみなす。



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を始める。

データメッセージの交換



- データメッセージの送信
- データメッセージの受信

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わたされた時以下の動作を行う

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。

③データメッセージを作り、セッション鍵により、認証と暗号化の操作を行う。

④データメッセージを送信する。

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。

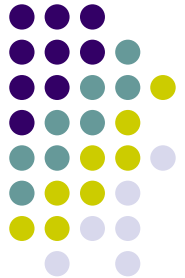
①受信したデータメッセージで指定されたセッション鍵が有効であることを確認する。そうでない場合には破棄し、受信処理を終える。

②認証と暗号の復号処理を行う。認証に失敗した場合は破棄し、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パケットを破棄。

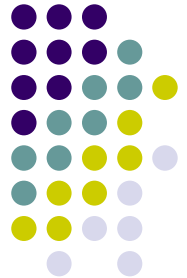
④ネットワーク層にパケットを渡す。

セッションの終了



- 能動的なセッションの終了
- セッション終了メッセージの受信
- BRの消滅
- セッションの自然消滅

能動的なセッションの終了



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。

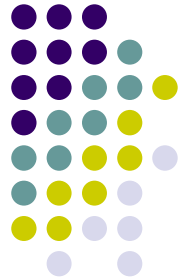
②セッション終了メッセージを作る。

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。

セッション終了メッセージの受信



MNまたはBRが、セッションの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。

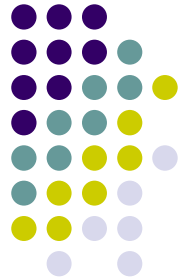
②セッションの情報を消去する。

BRの消滅

MNはBRの存在を監視している。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。

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。



おわり