Wi-Fi再入門〜見えない電波を知識で見抜く
Internet Week 2016

2016-12-01

株式会社DMM.comラボ / CONBU
Akira KUMAGAI

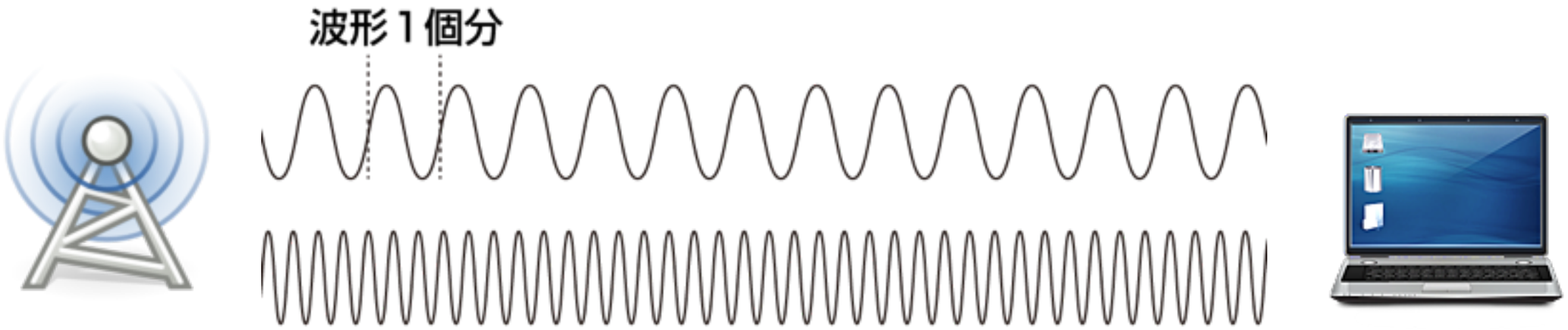
この資料の目的

- 電波とはどんなものか
- 無線独特の特性
- チャネル利用率と電波干渉
- 空間の分割
- 無線LANに使われている技術
- 公衆無線LAN

電波とはどんなものか?

電波ってなに

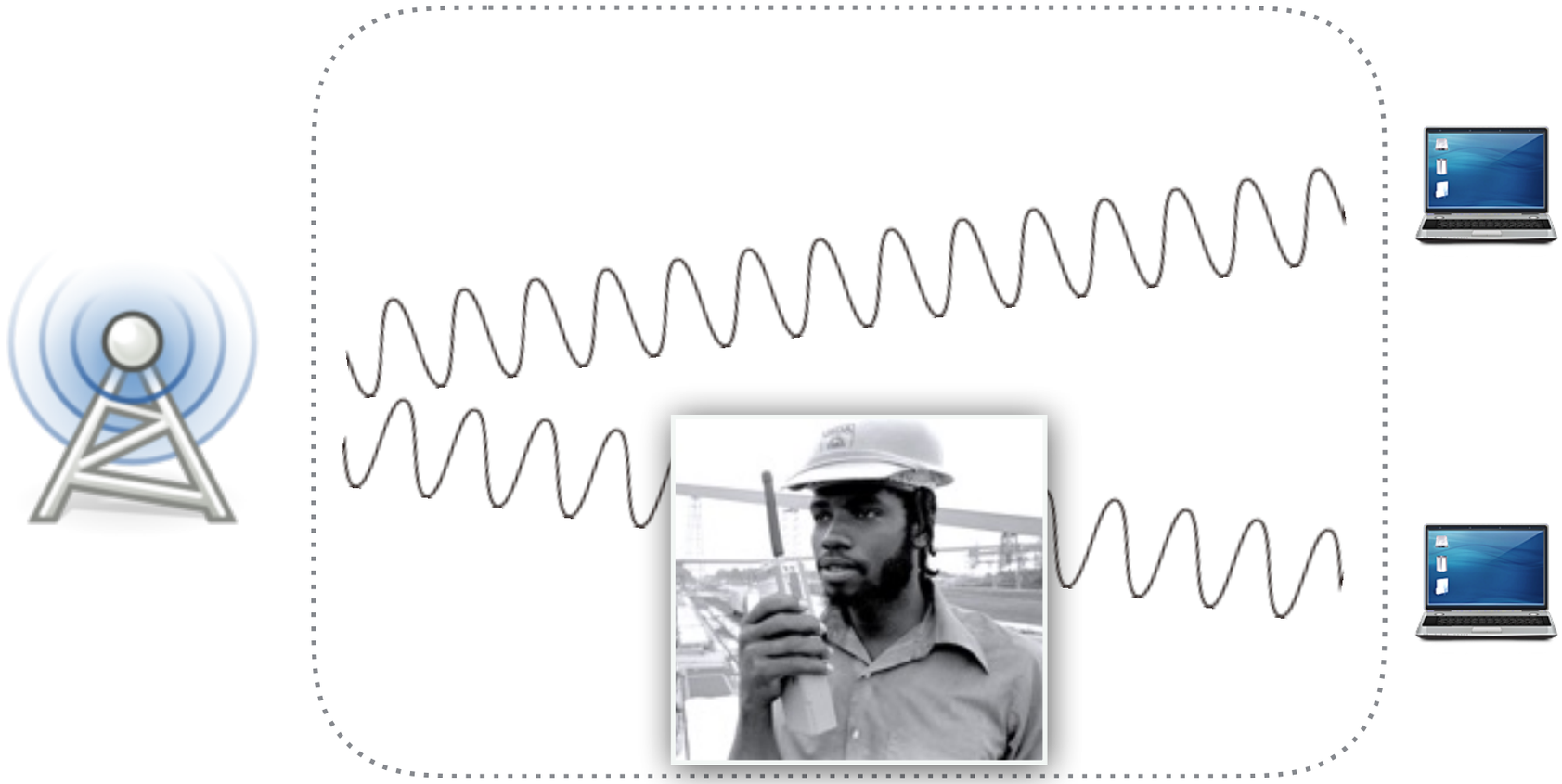
- 電磁波（光などの仲間です）
- 光とのちがいは周波数
  - 周波数(Hz)とは、波が1秒間あたりに繰り返される回数



１秒間に1,000,000,000回繰り返すと 1GHz

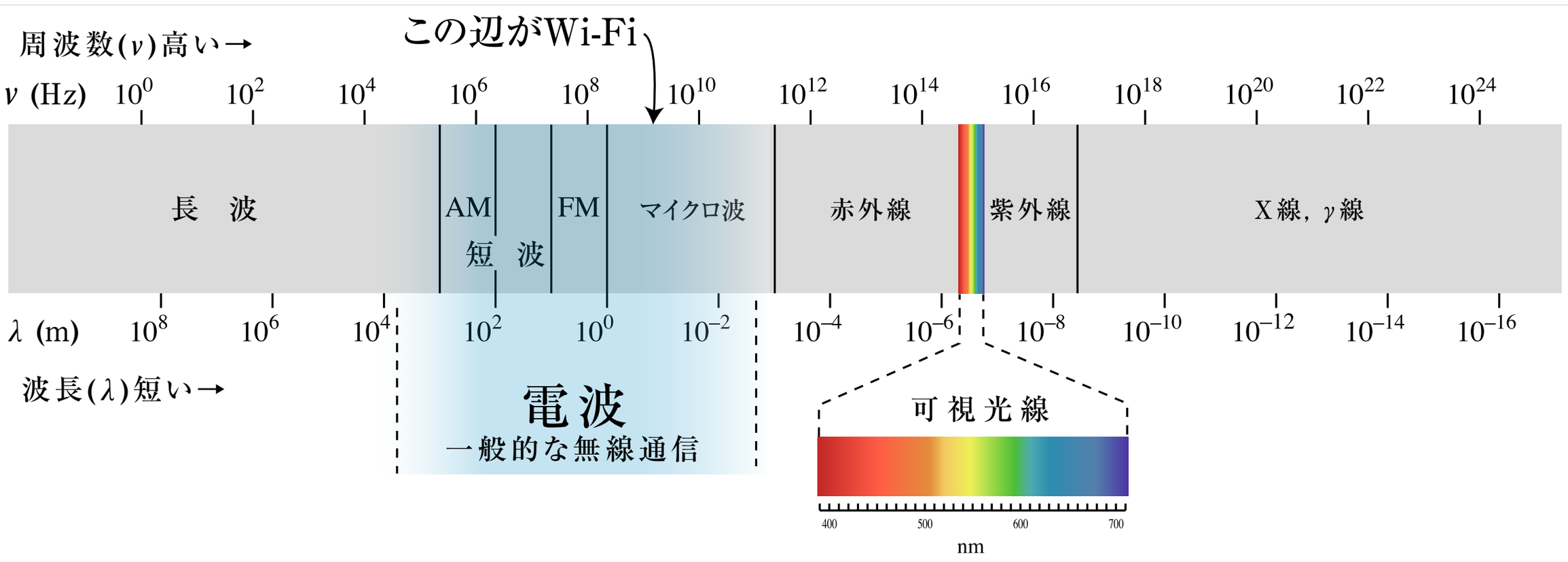
伝送媒体としての電波

- 空間を媒体とする共有メディア（空間だから共有せざるを得ない）
- 半二重通信「こちらは～です、どうぞ」が基本



伝送媒体(空間)

電波ってなに



電磁波と周波数

https://commons.wikimedia.org/wiki/File:EM_spectrum.svg

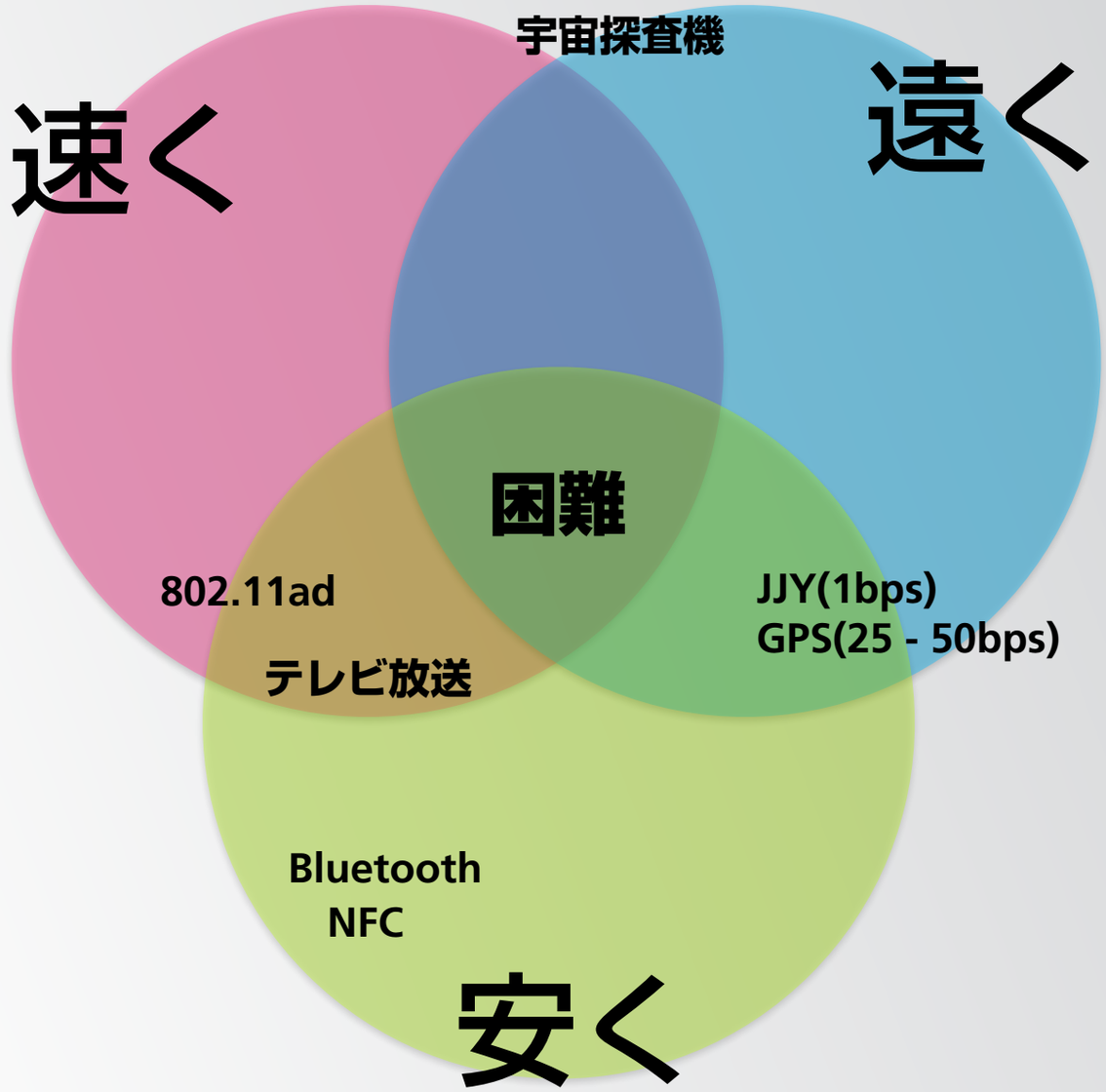
- 電波と呼ばれる範囲はけっこう広い
- 耳では聞こえない・音波は別のもの(音は空気の弾性波)

速く・安く・遠くまで

Photo CC BY cea+ https://www.flickr.com/photos/centralasian/4534292595/

“良い・安い・早い
これらのうちから 2つを選べます”

速く・安く・遠くまで



速く←→遠く　は両立できない

<u>シャノンの定理</u>
- 通信路容量の限界は**チャネル幅**と**信号品質**で決まる

<u>フリスの伝達式</u>
- 同じ周波数なら信号強度は距離自乗に反比例

安くなると
- みんなが使える小さな設備
- 自分と関係ない信号（ノイズ）が増える
  → 信号品質の低下

物理的に接触しなくても情報が取得できる

受信してみないとそれが何の情報なのか分からない（受信行為**自体**の法規制が不可能）

しかも安全に!?

安全性は後ほど触れるとして

まずは電波自体の特性

周波数(Hz)と性質

	低	周波数 →	高
波長	長い		短い
アンテナ	大きい		小さい
飛び方	障害物を貫通		障害物に反射/吸収
	導体、水分を貫通しない		
	いろいろある		光っぽい 直進性が高い
通信路容量	小容量		大容量
指向性	作りにくい		作りやすい
減衰	小		大

ワイファイはこのあたり

光として考える

アクセスポイントは電球

電波を光に見立てる

光として考える

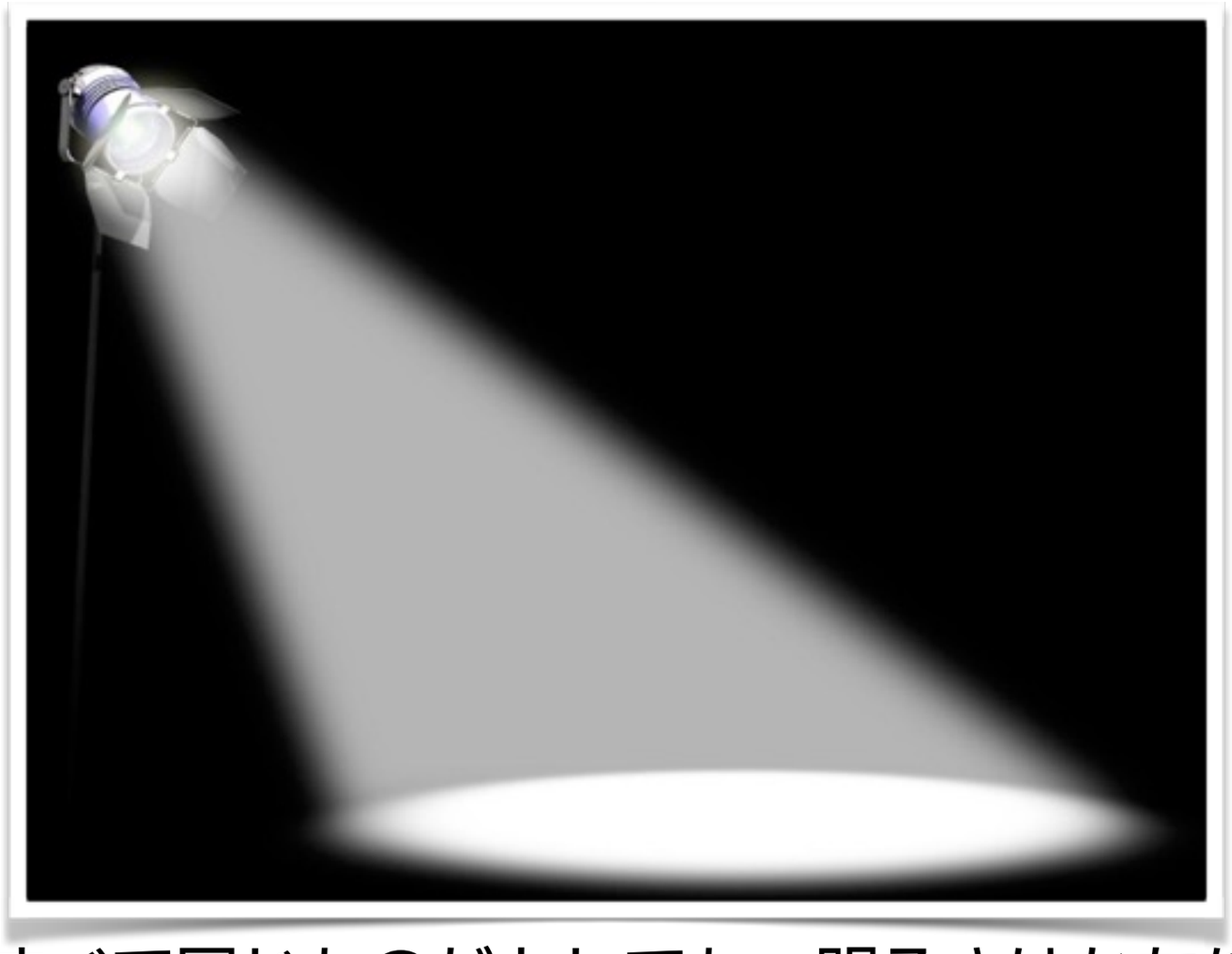
効率を考えると、カサがあったほうがいい

上方への光は無駄だし、よそに干渉する

光として考える

使いたいところが決まっていれば、
スポットでビームにするのが一番よい
強いし、干渉も防げる

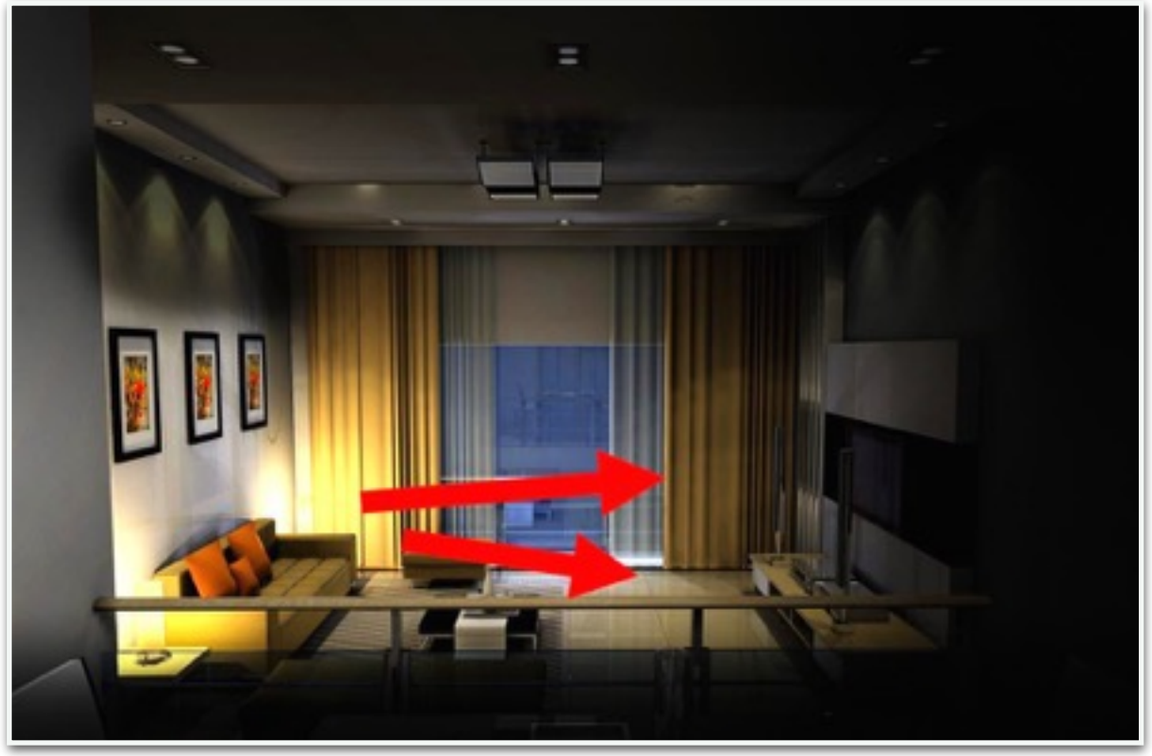
光として考える



- 電球はすべて同じものだとしても、明るさはかなり変わる
- カサやスポット器具自体に、電球の電力を高める効果はない。
  四方八方へ散らばっているエネルギーを狭い方向へまとめるだけ
- アンテナも、アンテナの指向性が電力を増幅することはない

光として考える

天井の照明



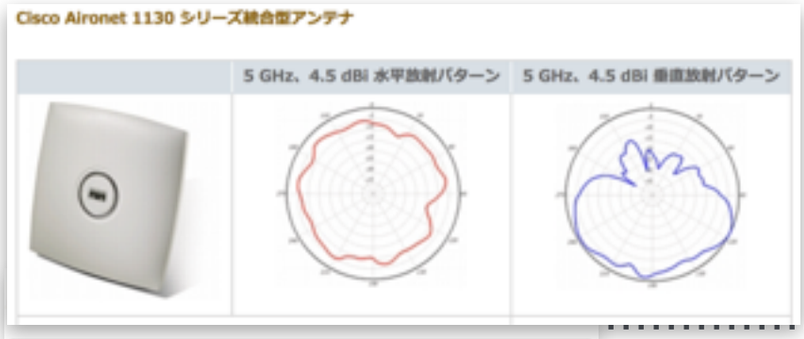
床置きの照明

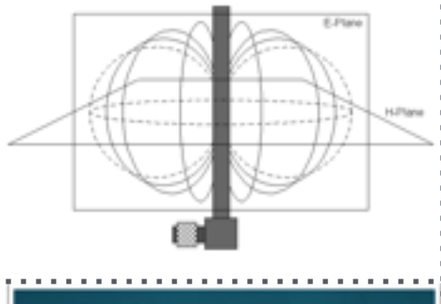
低いところに設置すると陰ができやすい

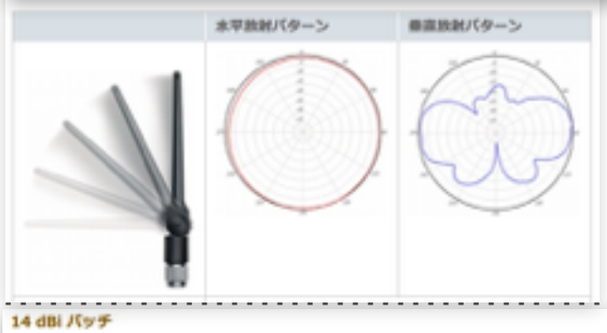
実際のアンテナの形状

完全無指向性のアンテナは作りにくい

機器内蔵アンテナは緩やかな指向性のものが多い

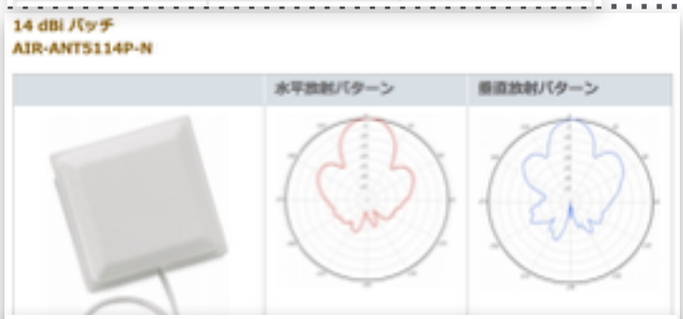




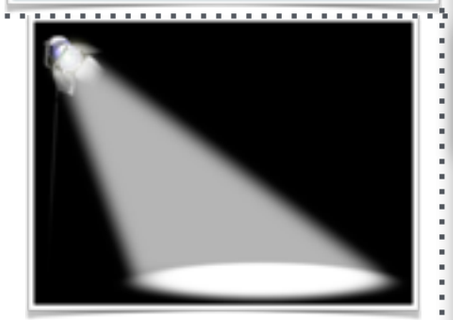


ダイポールアンテナ

似た照明器具はない



パッチアンテナ



八木アンテナ

パラボラアンテナ

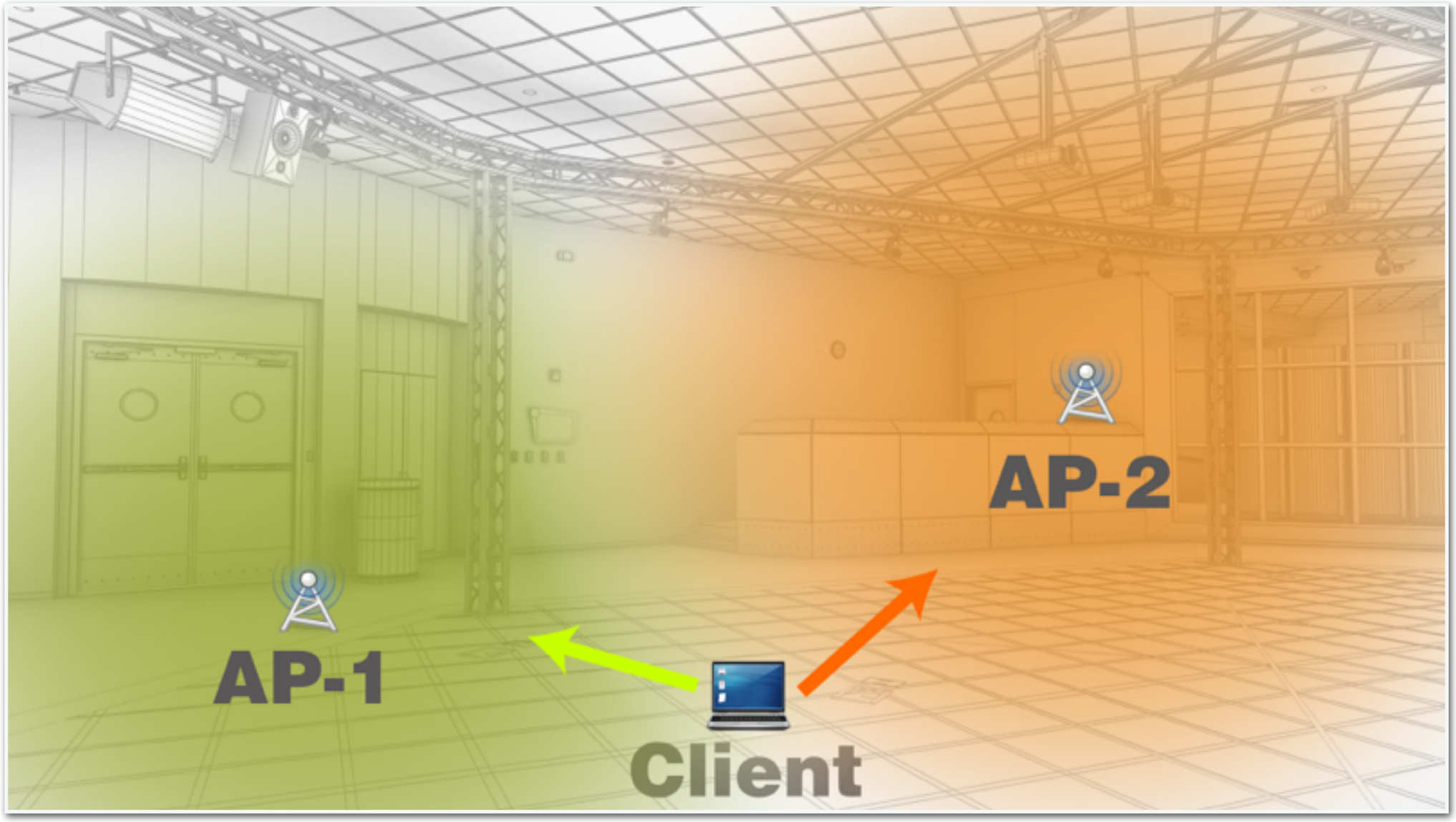
http://www.cisco.com/web/JP/product/hs/wireless/airoa/prodlit/product_data_sheet09186a008008883b.html

光として考える

天井から照らすと影ができにくいが、遠くまで届きすぎて、たくさん設置すると干渉する可能性がある

天井の照明器具は全部**同じ色**のため、それぞれの光を区別できず、混ざって干渉してしまう

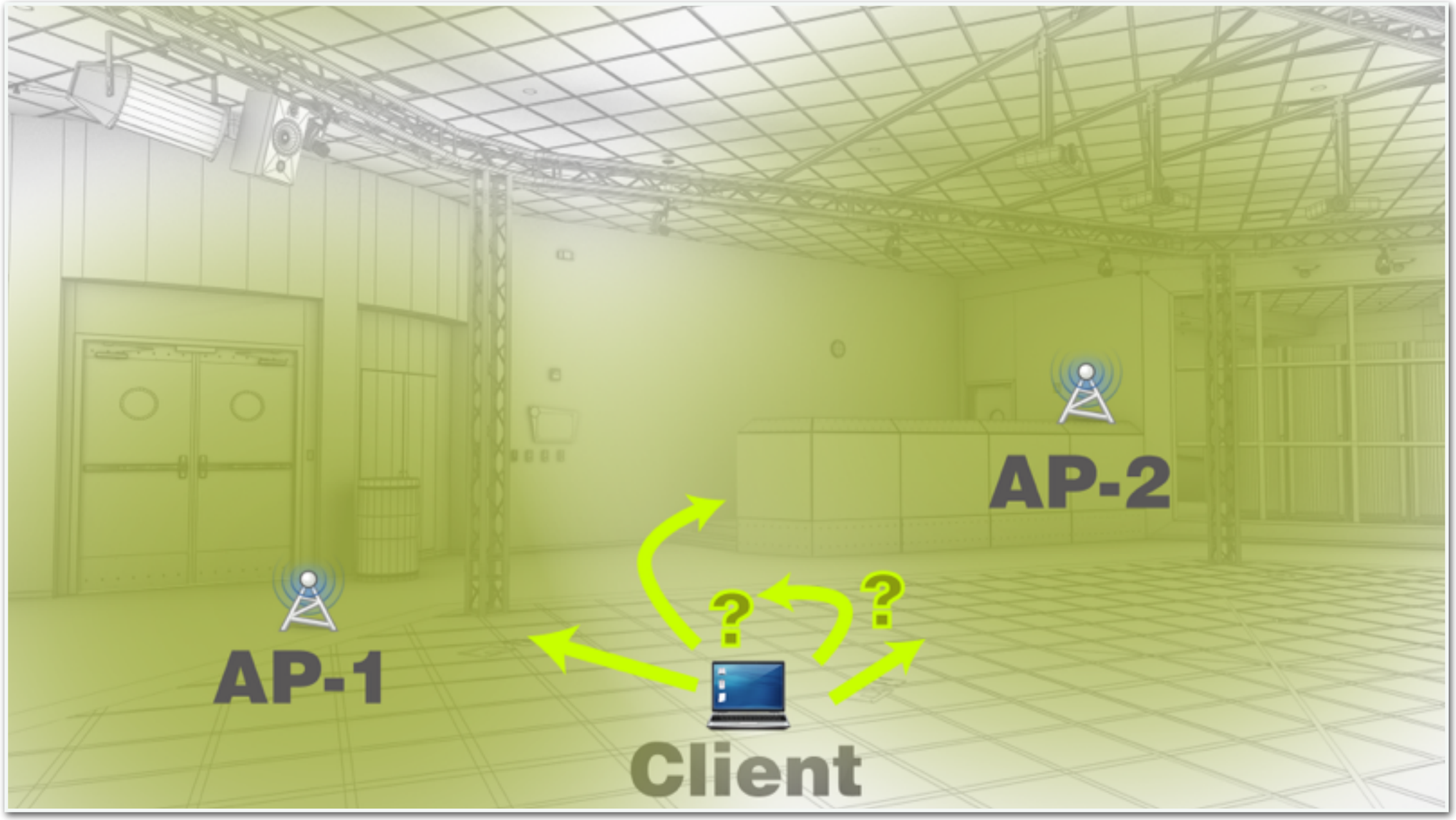
チャネルの違い



光の色（周波数）の違い

電波の場合でもチャネルの違いのようなもの

チャネルの違い



混ざった場合、空間が共有されてしまい、
大きなコリジョンドメインになってしまう（半二重ですよ!）

チャネルの違い

セル 2個

セル 1個

同じ色×同じ場所
（チャネル×電波到達範囲）

端末を収容できる空間の
最小単位“セル”となる

セルあたりの収容能力は
物理的に上限がある

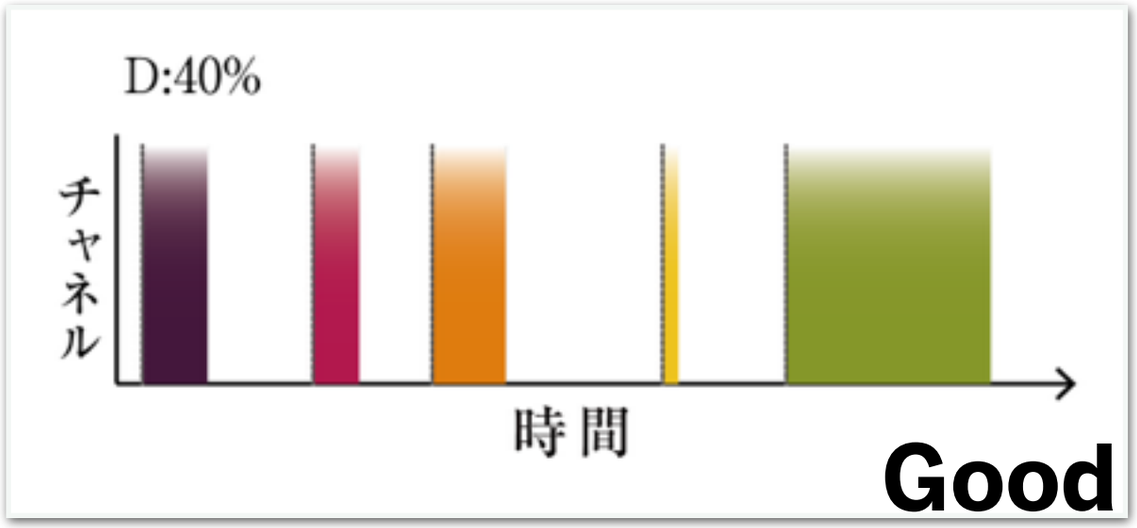
チャネルの違い

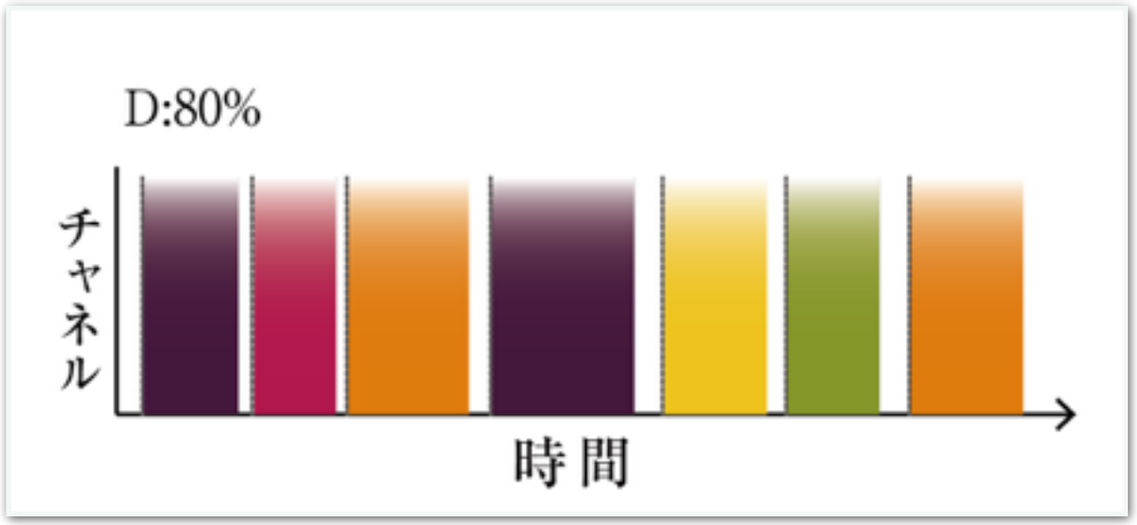
チャネルを共有している限り、近いところにAPを増設しても改善されない

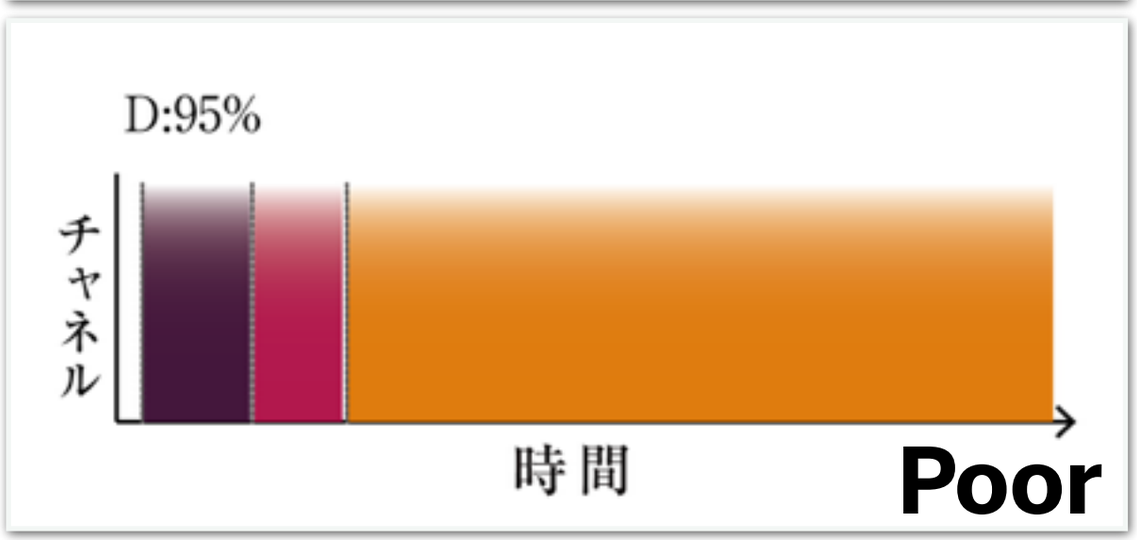
伝送媒体である空間そのものがボトルネックになっているため

高密度Wi-Fi環境では、これをいかに分割していくかがカギとなる

チャネル利用率







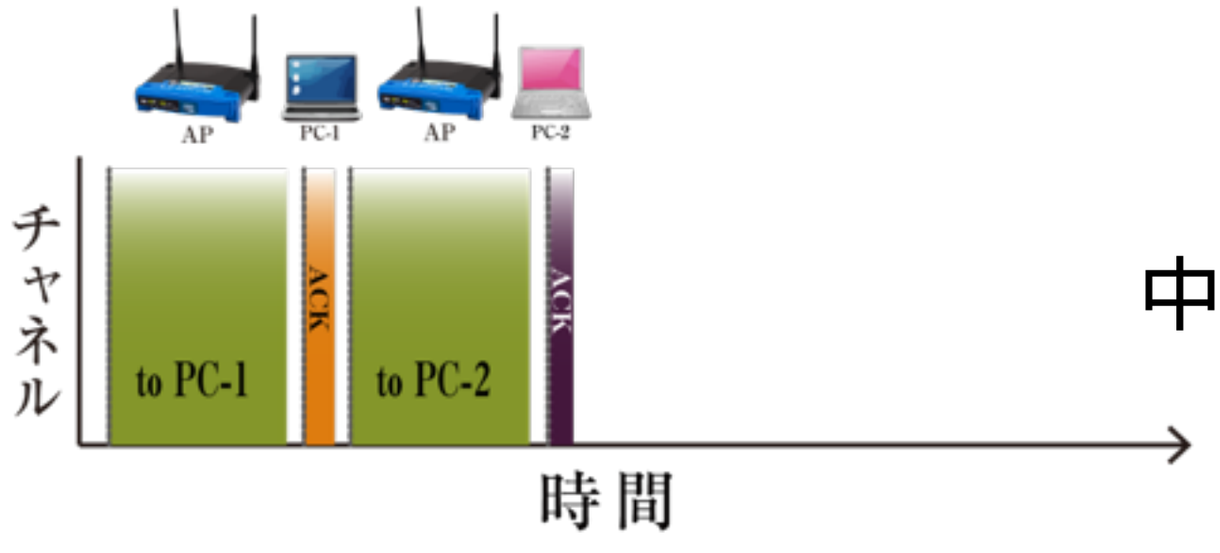
無線は、誰かが送信しているときは他の端末は送信できない

チャネル利用率が高まると衝突が発生しやすくなるので、低く保つのが理想

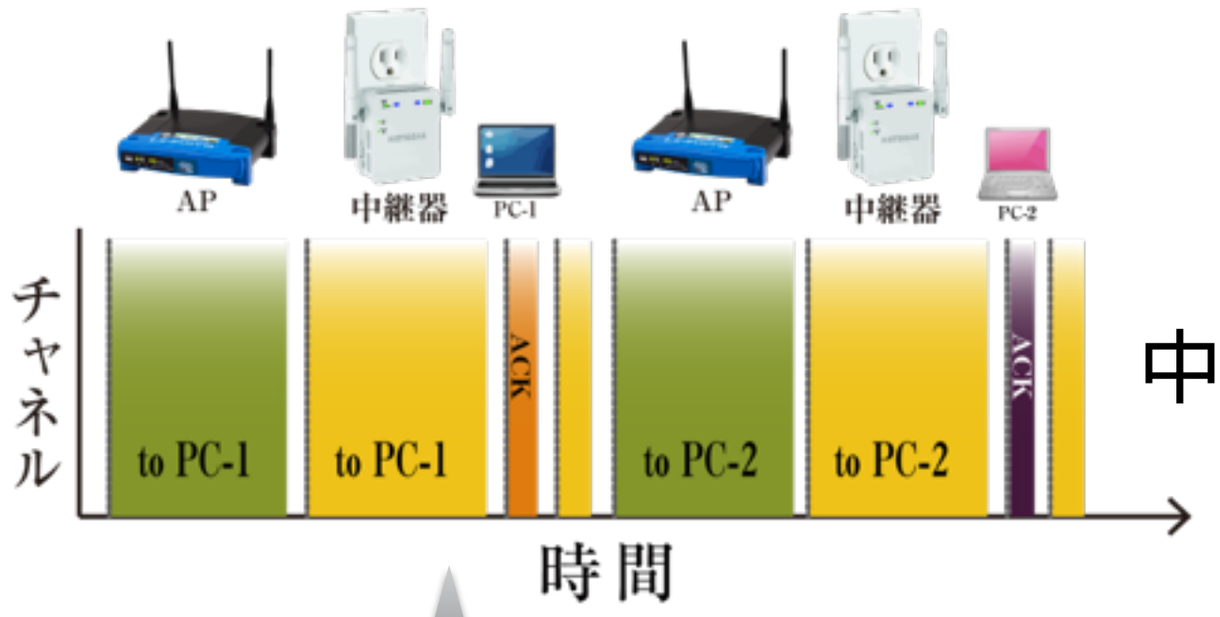
衝突が発生しやすくなるとチャネル利用率が更に高まり、ほかに誰も送信する隙間がなくなってしまい、破滅する

無線中継器の罠

色は電波の到達範囲



中継器なし

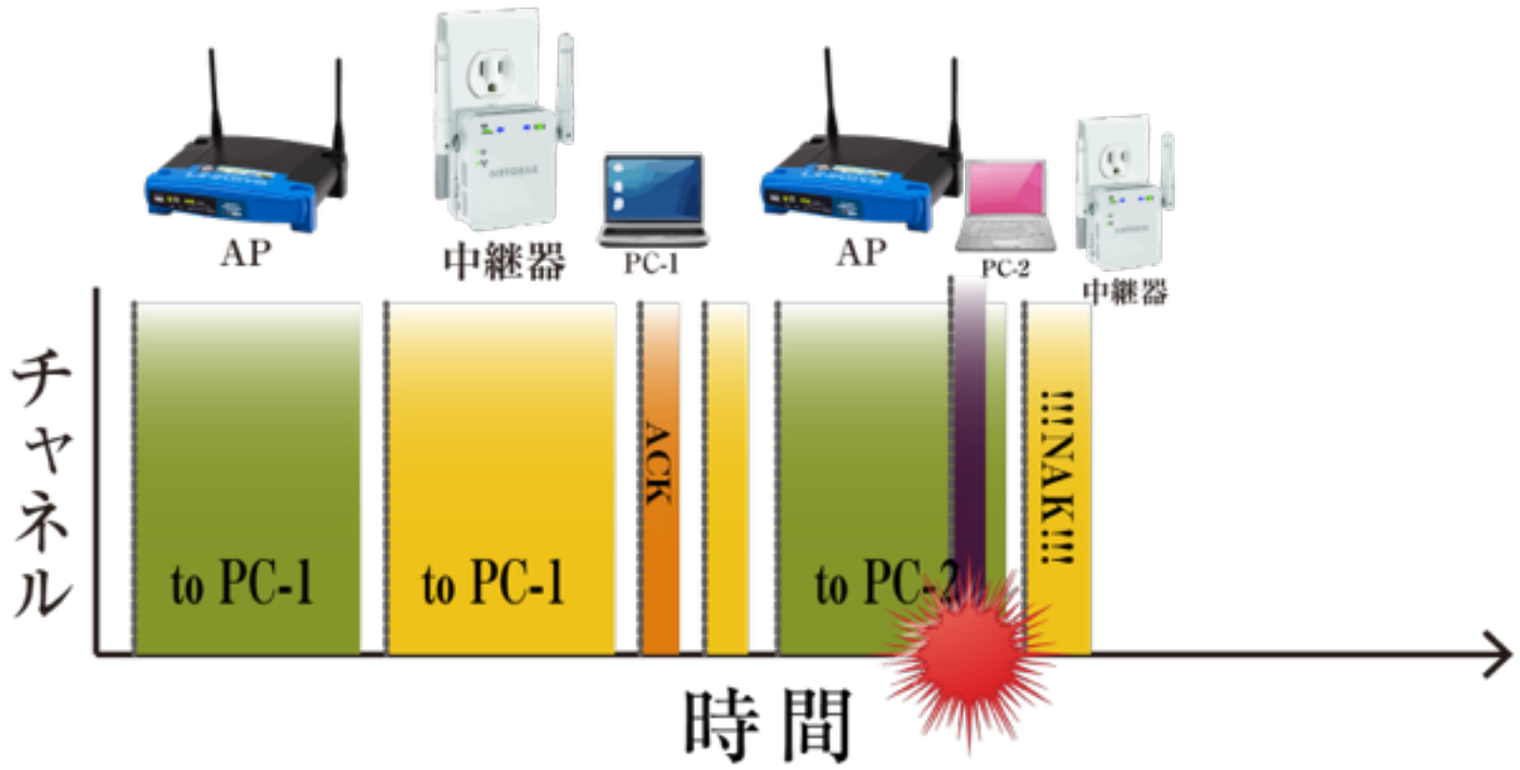


中継器あり

2倍以上の帯域(時間)を占有

無線中継器の罠（さらに・・）

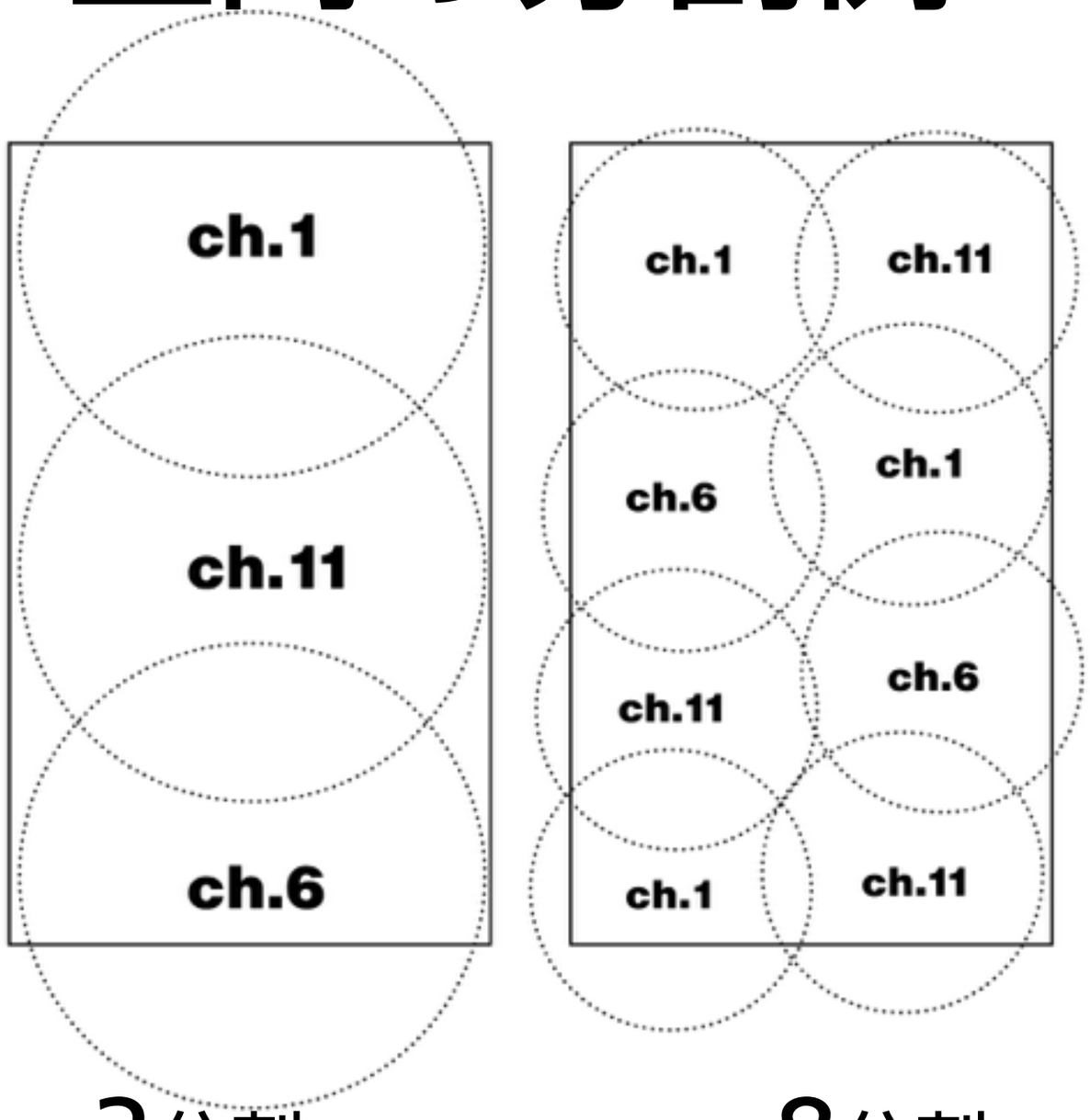
色は電波の到達範囲



APとPC-1は互いに電波が届かず、見えないため、同時に送信してフレームが壊れてしまうかもしれない

ユーザ数の少ない環境では有効な中継器も
混雑している環境に導入すると破滅することも

空間の分割例



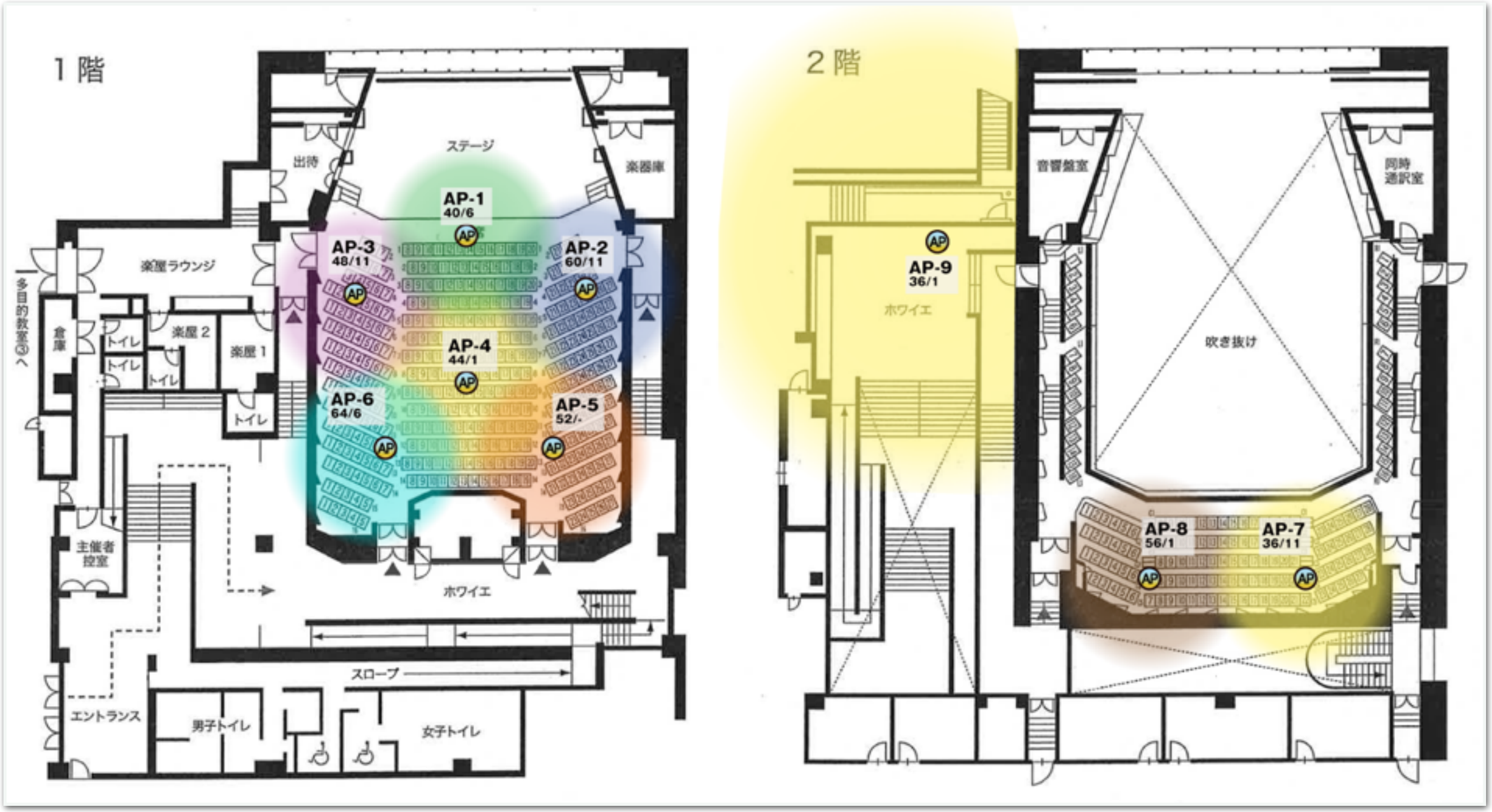
3分割
APあたり30端末
合計90端末

8分割
APあたり30端末
合計240端末

空間の分割例

	カバー範囲優先	収容端末数優先
何が制限になるか	電波の到達範囲	電波干渉
APの数	少ない	多い
アンテナの指向性	無指向性	指向性
電波の到達範囲	できるだけ広く	狭い範囲で止める
障害物	少ないほうがよい	多いほうがよい
周波数帯	低いほうがよい	高いほうがよい
ユースケース	家庭	オフィス、スタジアム等

APを設置してみる



電波の飛びすぎを防ぐ必要がある

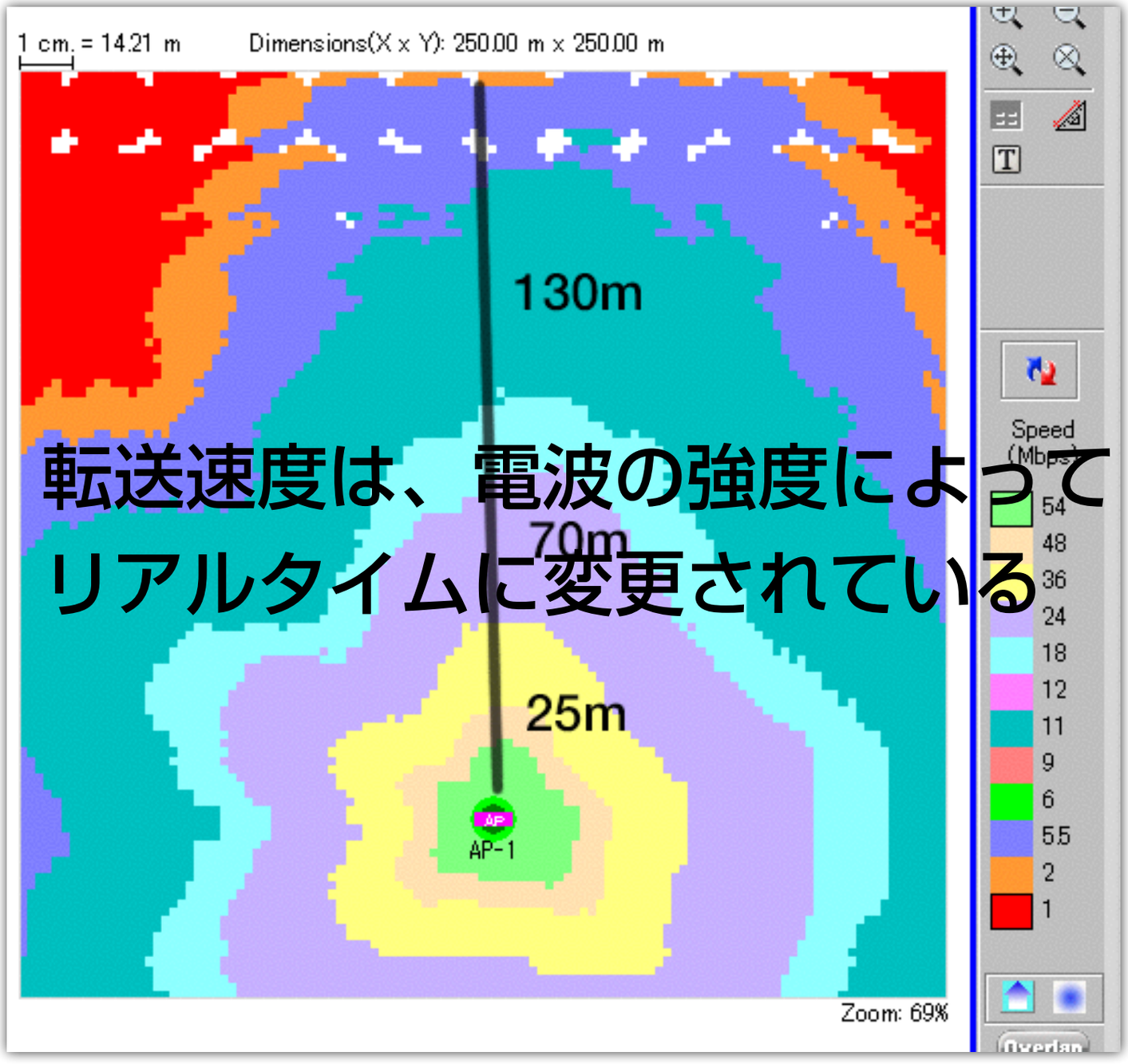
電波を遠くまで飛ばしすぎない

- 電波が必要以上に飛びすぎると、同じチャネルを使っている他のAPと相互に干渉が起きる

- 遠くまで飛んだとしても、AP一台あたりに収容できる端末数は限られているから、遠くまで飛ばしてもかえってパフォーマンスは悪化する

電波の強さとデータレート

電波の強さ(距離)と速度(bps)



だいたい自由空間を想定したシミュレーション

電波の強さと速度(bps)

macOS / OS X では option + Wi-Fi アイコン で現在接続中の速度を確認できます。リアルタイムに変化する様子がわかります

電波の強さと速度(bps)

- 電波の品質が低い場合（信号が弱い、ノイズが多い）、速度(bps)を自動的に下げるようになっている

- 電波の状況は、ほとんどの場合何らかのエラーがあり、無線LANはそれを前提に、がんばってエラー訂正をしながら動いている

- 伝送媒体が空間そのものであるため、品質の予測がしにくい

ノイズと速度(bps)

吾輩は猫である。名前はまだ無い。
どこで生れたかとんと見当がつかぬ。何でも薄暗いじめじめした所でニャーニャー泣いていた事だけは記憶している。吾輩はここで始めて人間というものを見た。しかもあとで聞くとそれは書生という人間中で一番獰悪な種族であったそうだ。この書生というのは時々我々を捕えて煮て食うという話である。しかしその当時は何という考もなかったから別段恐しいとも思わなかった。ただ彼の掌に載せられてスーと持ち上げられた時何だかフワフワした感じがあったばかりである。掌の上で少し落ちついて書生の顔を見たのがいわゆる人間というものの見始であろう。この時妙なものだと思った感じが今でも残っている。第一毛をもって装飾されべきはずの顔がつるつるしてまるで薬缶だ。その後猫にもたいぶ逢ったがこんな片輪には一度も出会わした事がない。のみならず顔の真中があまりに突起している。

吾輩は猫である。名前はまだ無い。
どこで生れたかとんと見当がつかぬ。何でも薄暗いじめじめした所でニャーニャー泣いていた事だけは記憶している。吾輩はここで始めて人間というものを見た。しかもあとで聞くとそれは書生という人間中で一番獰悪な種族であったそうだ。

ノイズ（他の通信）に埋もれたら遅いほうが有利

これが人間の飲む煙草というものである事はよっぽどの時分

ノイズと速度(bps)

ああ、その時です。背後の兵舎のほうから、誰やら金槌で釘を打つ音が、幽かに、トカトントンと聞えました。それを聞いたとたんに、眼から鱗が落ちるとはあんな時の感じを言うのでしょうか、悲壮も厳粛も一瞬のうちに消え、私は憑きものから離れたように、きょろりとなり、なんともどうにも白々しい気持で、夏の真昼の砂原を眺め見渡し、私には如何なる感慨も、何もつも有りませんでした。そうして私は、リュックサックにたくさんのものをつめ込んで、ぼんやり故郷に帰還しました。

あの、遠くから聞えて来た幽かな、金槌の音が、不思議なくらい綺麗に私からミリタリズムの幻影を剥ぎとってくれて、もう再び、あの恐ろしい厳粛らしい悪夢に酔わされるなんて事は絶対に無くなったようです。しかし、その小さい音は、私の脳髄の金的を射貫いてしまったものか、それ以後げんざいまで続いて、私は実に異様な、いまわしい癇癪持ちみたいな男になりました。と言っても決して、兇暴な発作などを起すというわけではありません。その反対です。何か物事に感激し、奮い立とうとすると、どこからとも無く、幽かに、トカトントンとあの金槌の音が聞えて来て、とたんに私はきょろりとなり、眼前の風景がたった今迄の美しさを失い、ただ純白のスクリンだけが残り、それをましまし眺めているような、何とも、はかない馬鹿らしい気持になるのです。

自分の通信は他者の通信にとってノイズとなる

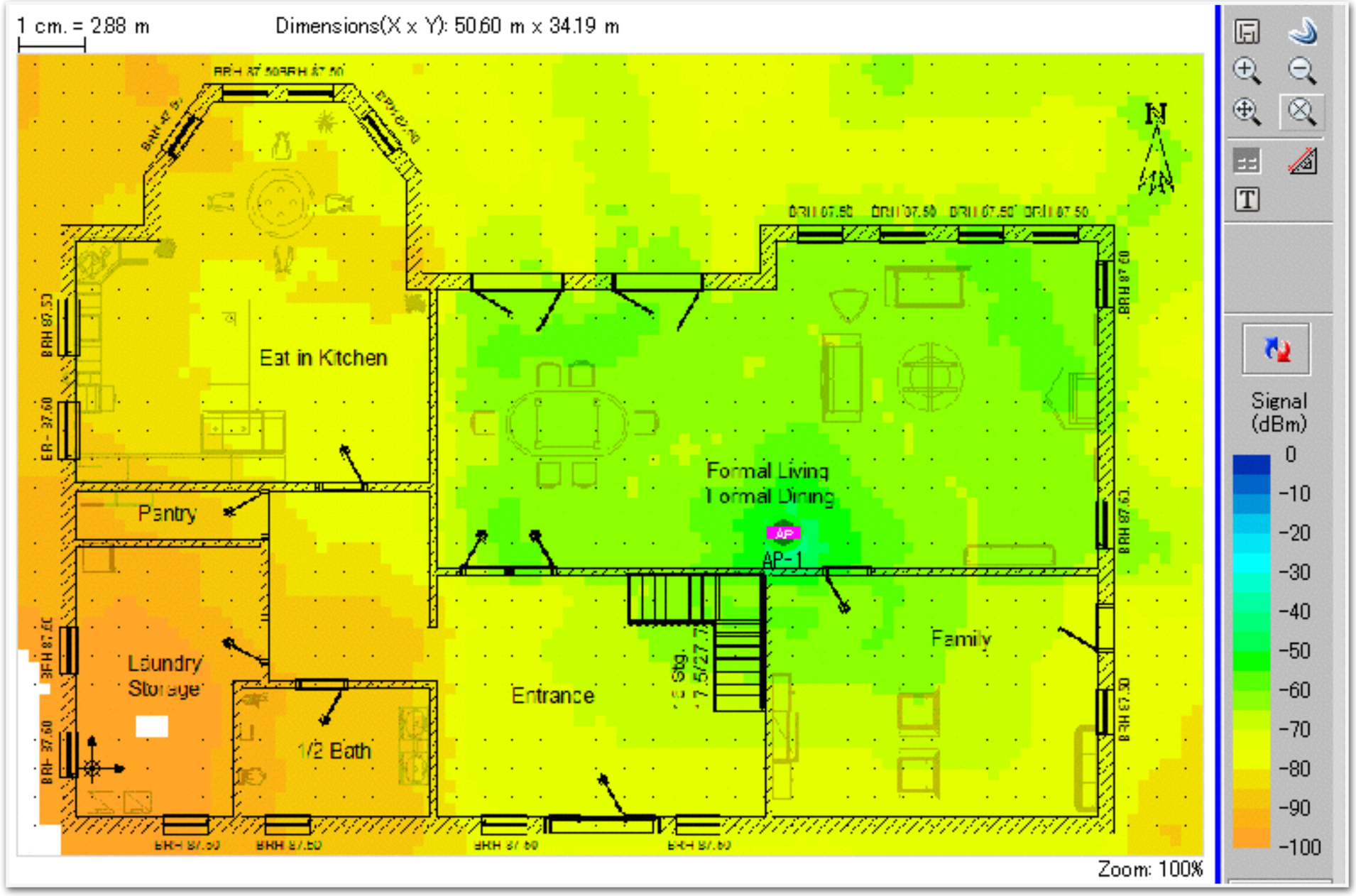
ノイズと速度(bps)

$$\text{信号の品質}(S/N) = \frac{\text{信号電力}}{\text{ノイズ電力}}$$

信号電力を高めるには
- 送信機をハイパワーなものにする
- 受信機の感度を高める
- アンテナの指向性を高めて無駄な方向に電波を送らない

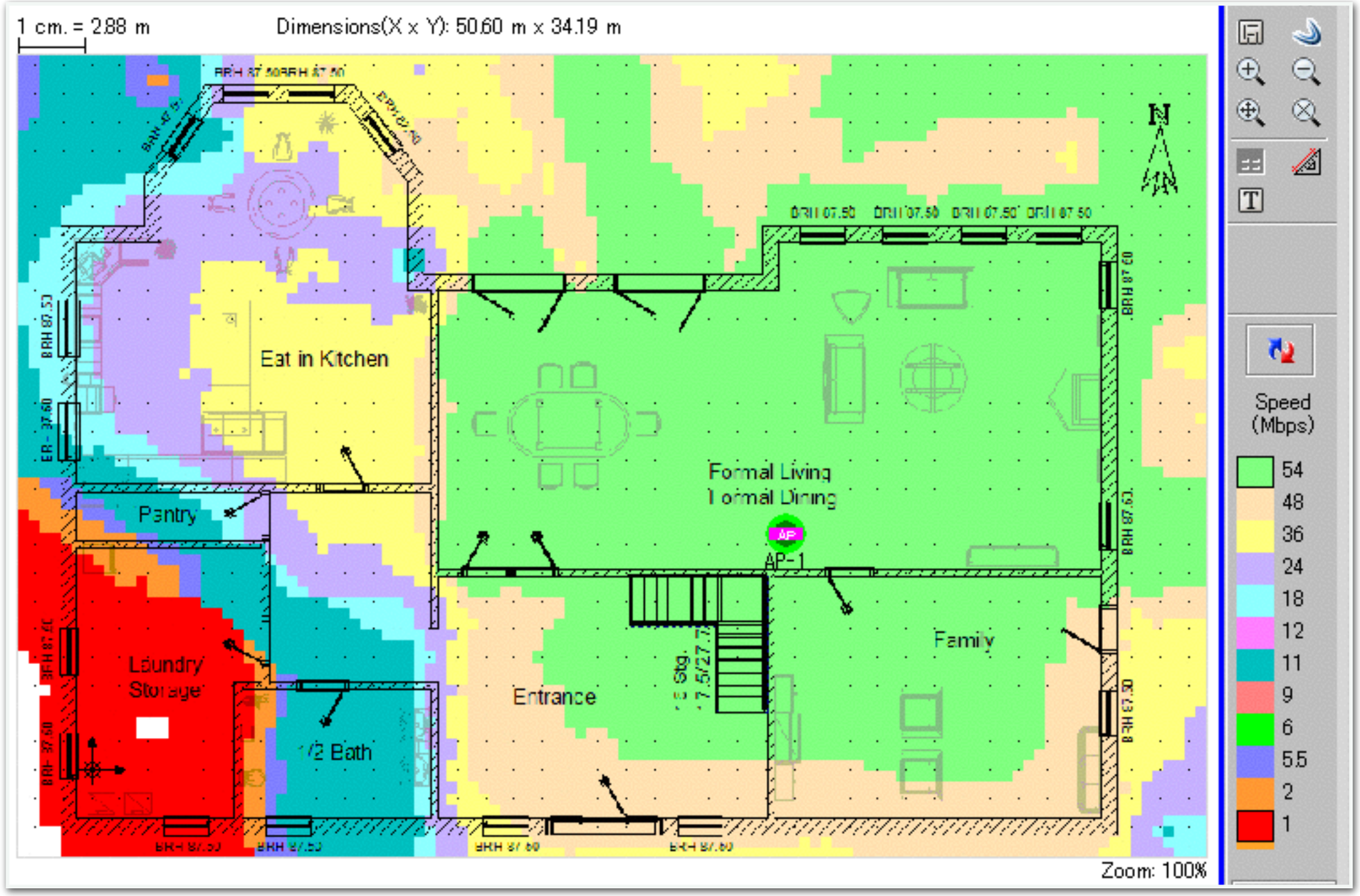
ノイズ電力を下げるには
- 無関係な他の無線局をローパワーにしてもらう
- アンテナの指向性を高めて無駄な方向のノイズを拾わない
- 受信機内部や自然界で発生するノイズを低減する

電波の強さと速度(bps)



通常は壁などがあるので、こういう電波強度になり、

電波の強さと速度(bps)



速度はこんな感じ、左下の部屋はちょっとつらい

まとめ

- 電波は半二重メディアで、空間を共有
- 光のような伝搬特性
- 同じ周波数の電波が混ざると干渉を起こす
- チャネル利用率を低く保つためにはセル設計が重要
- 電波の品質が悪いとデータレートが低下する

チャネル利用率

混雑とは？

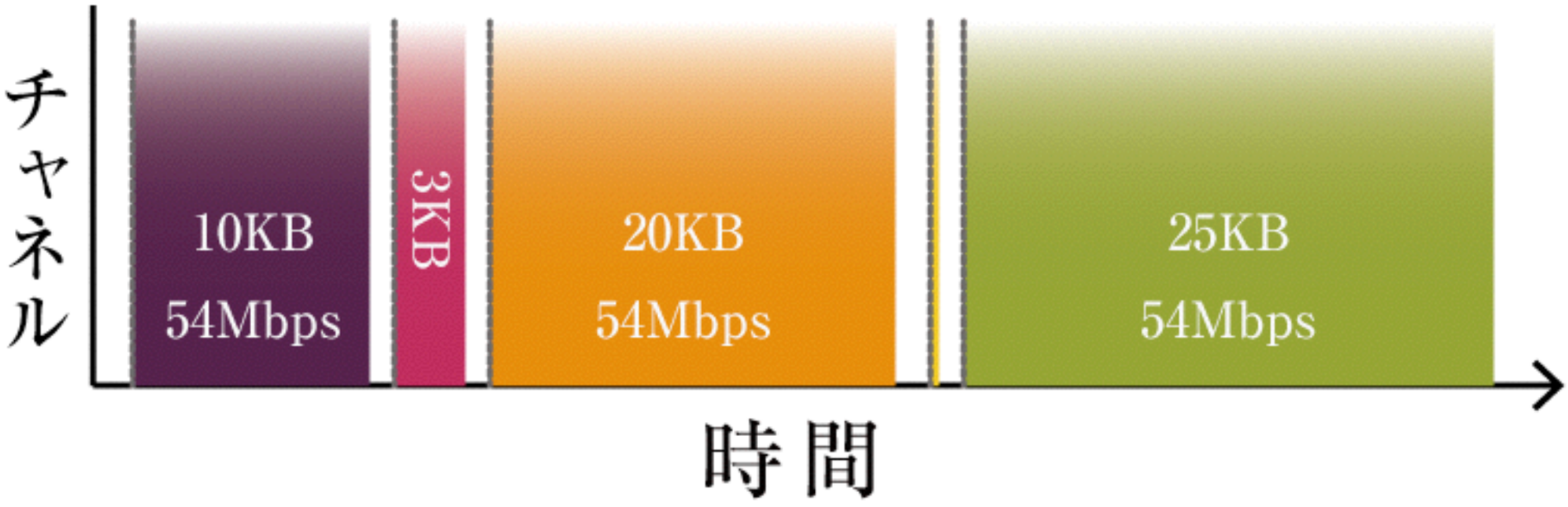
- 無線通信は時空間を占有して行なう
  スイッチングしない
- 同時に複数の端末が通信できてるように見えるけど
  その瞬間では、通信は必ず1:1 で行われていて
  ほかの端末は待機している

5台の端末がひとつのチャネルを時分割して共有

一台のアクセスポイントと複数の端末が
時間で区切って順番にデータを転送する

ある一瞬では APと端末はチャネルを占有している

実際には占有時間はトラフィックによってばらばら



占有時間、順番などもばらばら

通信内容がないこともある

ややこしいから、同じ10KBずつ流す仮定にしましょう

たとえば、

5台の端末に10KBずつ、計50KB転送することを考える

(全部54Mbpsで転送)

ところが、オレンジの端末が遠くに行ってしまい、

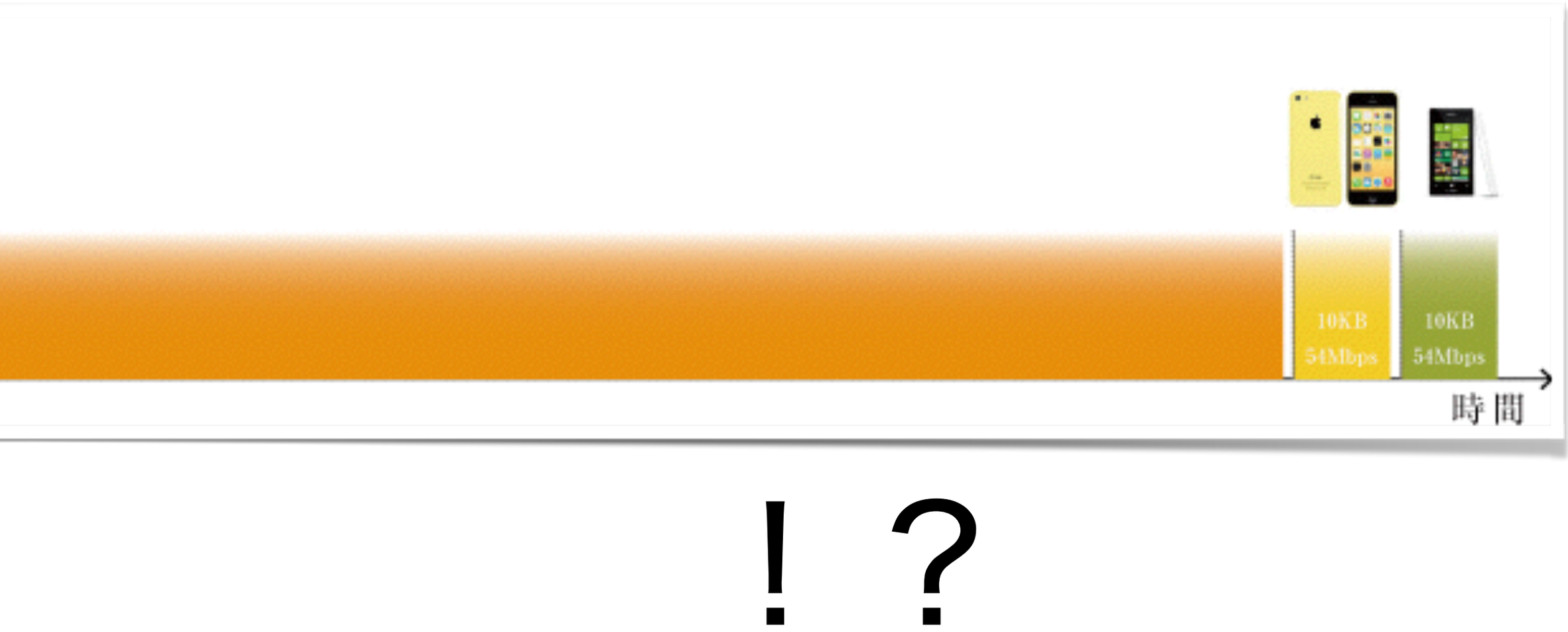
電波強度が下がり、転送速度が落ちました

チャネル

10KB	10KB	10KB
54Mbps	54Mbps	2Mbps

転送レート(bps)は電波強度によって変わる

オレンジの端末の転送速度が2Mbpsに下がった場合、

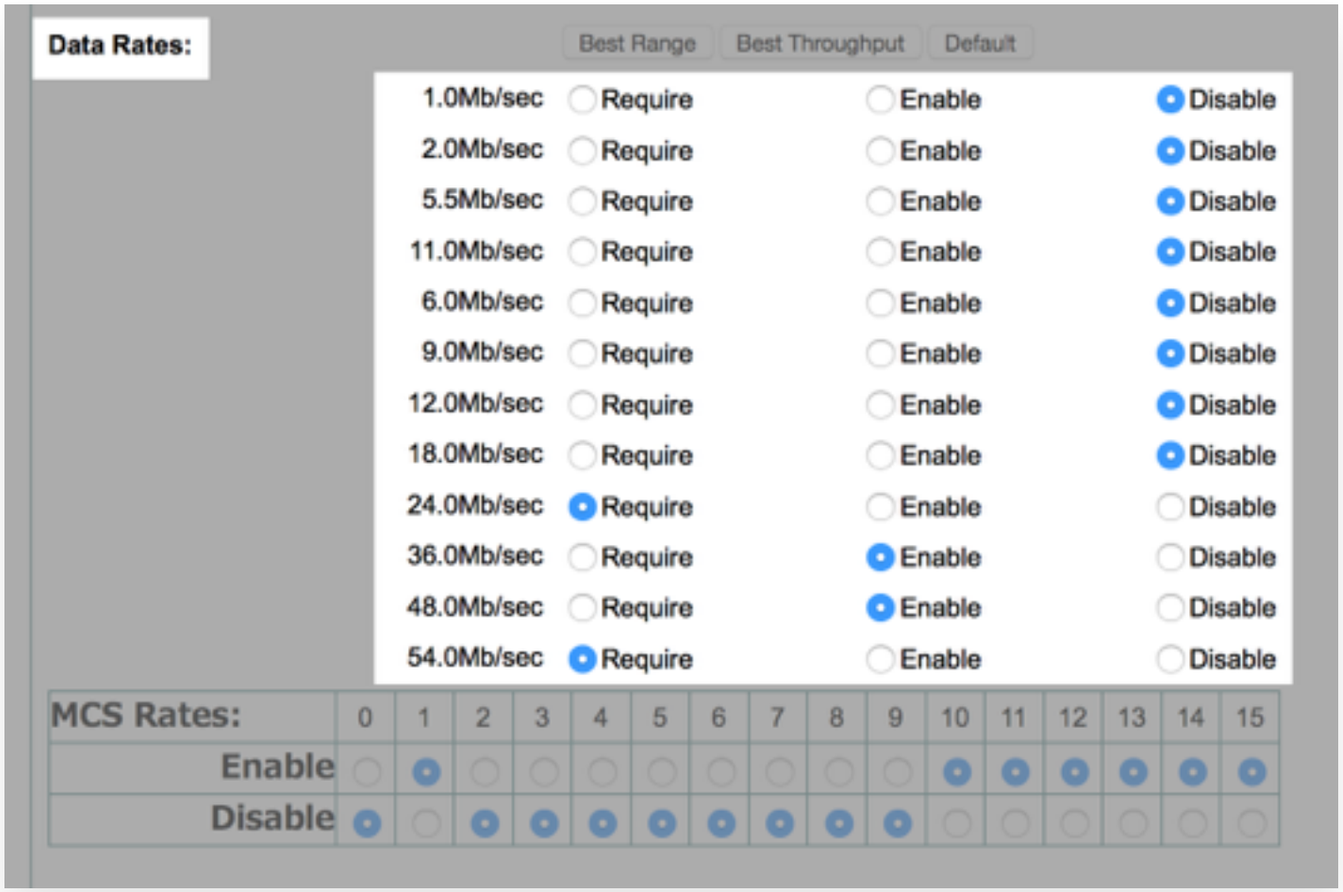

10KB
54Mbps
10KB
54Mbps
時間

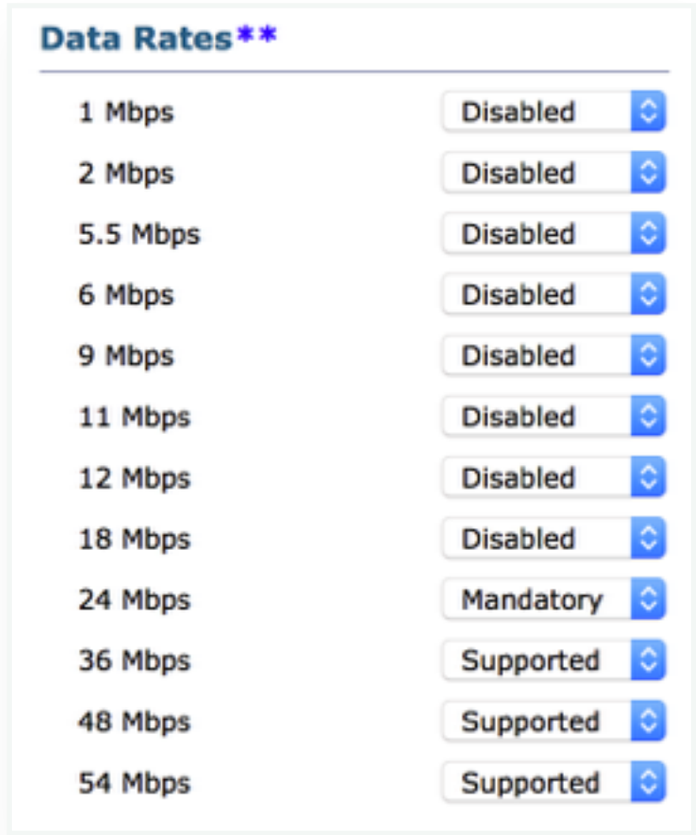
! ?

端末が一台遅いと全体が遅くなる

- 同じ50KBを転送するのに、遅い端末が一台いるだけで時間(エアタイム)が5倍くらい無駄になった
- 遅い端末の通信が終わるのを、みんな待っている
- 遅い端末の存在はリソースを食い潰す

電波を遠くまで飛ばしすぎない
遅いレートで通信させない





遅いレートをDisableにしてみましょう

遅いデータレートを制限すると

- 電波を遠くまで飛ばないようにできる
- 下のオレンジ色のようなことを起こりにくくできる

Airtime Fairness (ATF)

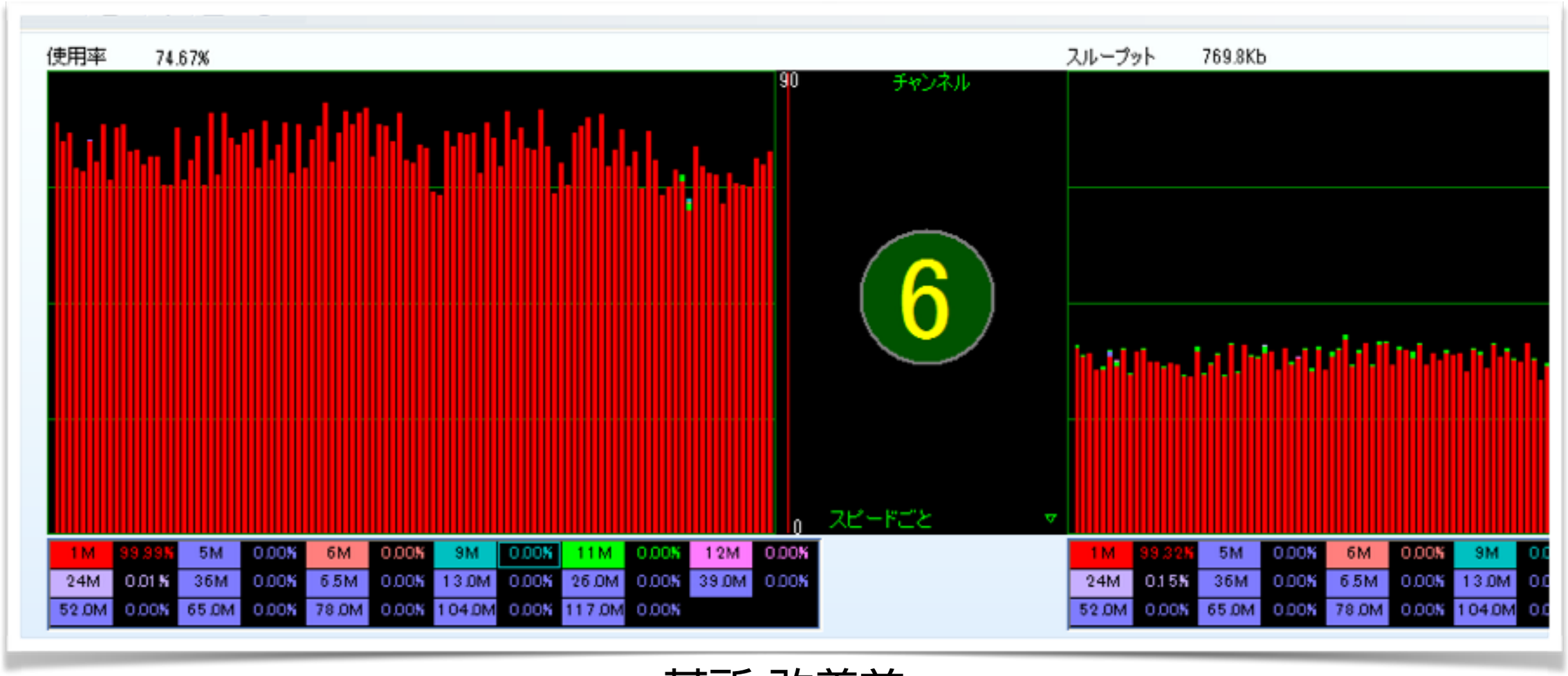
- 特定の遅い端末が全体の足を引っ張らないように、エアタイムをなるべく均等に割り当てる技術
- 最近のエンタープライズ向け製品に搭載

まとめ

- 遅いデータレートで接続している端末は、全体の足を引っ張る
- チャネル利用率が高くて不安定な場合、遅いデータレートを無効にすることで改善できる可能性がある
- ただし遅いデータレートを無効にすると電波の届く範囲は狭くなる

測定器で見てみる

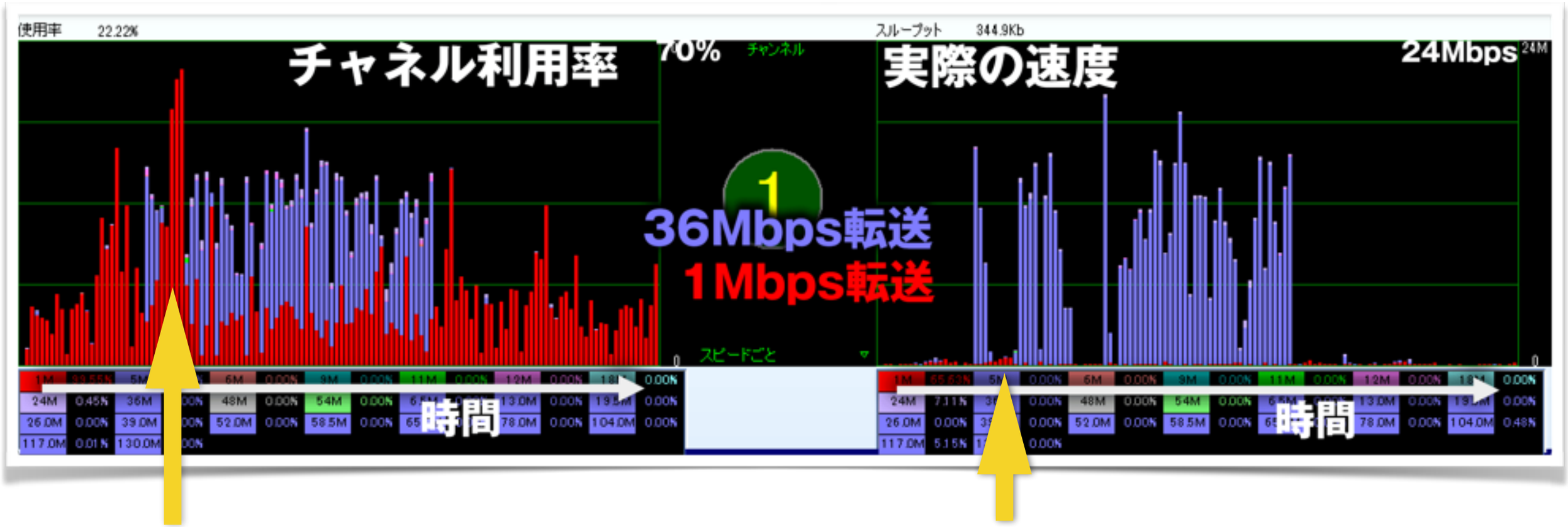
遅い端末がいる状態ってどんなの?



某所 改善前

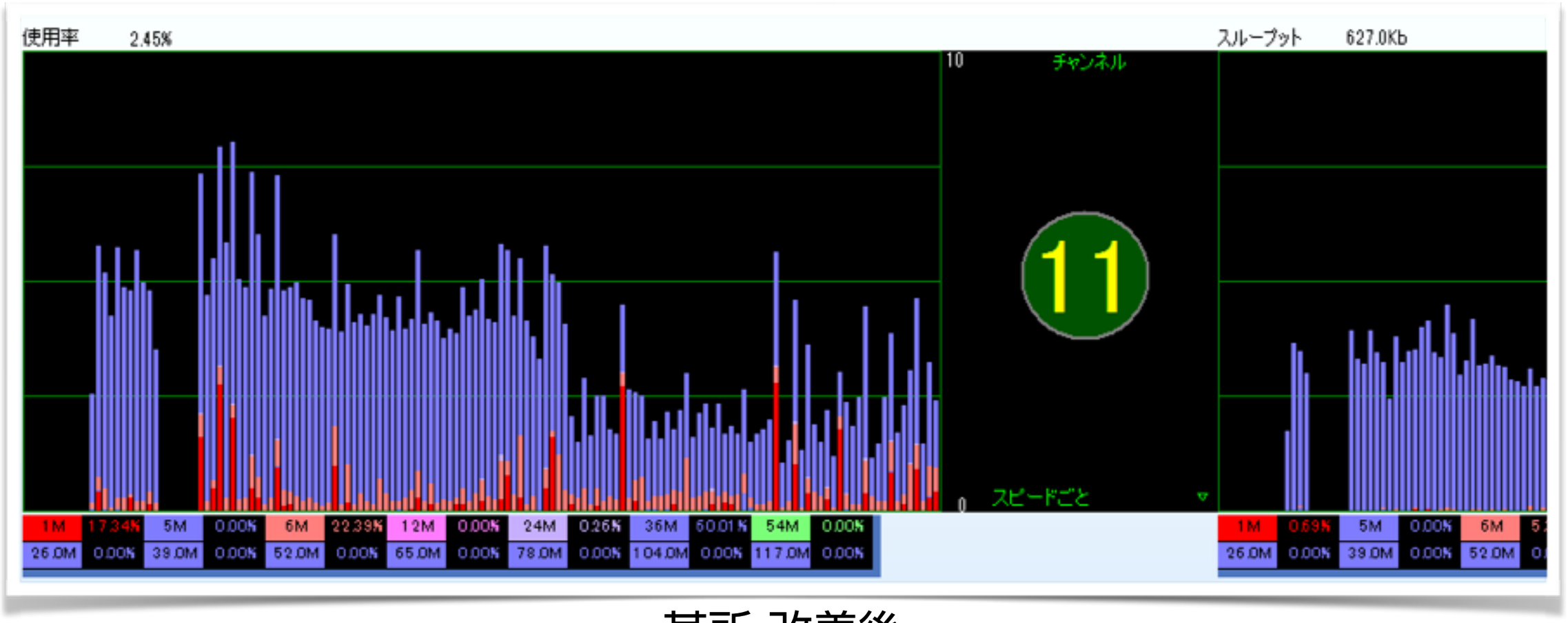
- チャネルの使用率 74.67%（高すぎる）
- それなのにスループットが769Kbしか出ていない

遅い端末ってどれくらい邪魔?



- 横軸は同じ時間
- 矢印のタイミングで、赤(1Mbps)はチャネル利用率をすごく上昇させているのに、スループットが全然出ていない

遅いデータレートを禁止するとどうなる?

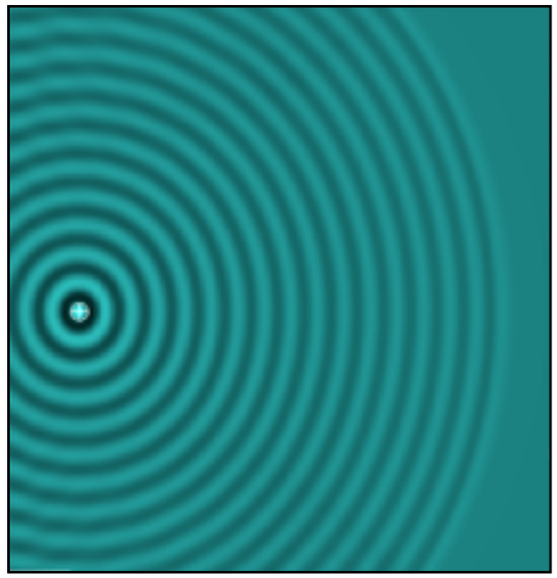


某所 改善後

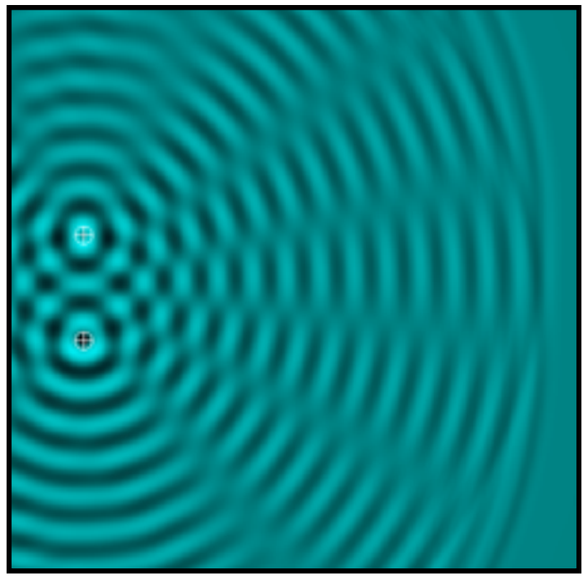
- 最低を36Mbpsに設定、それ未満を禁止
- チャネル使用率を約75%→2.5%まで改善

無線LANの技術

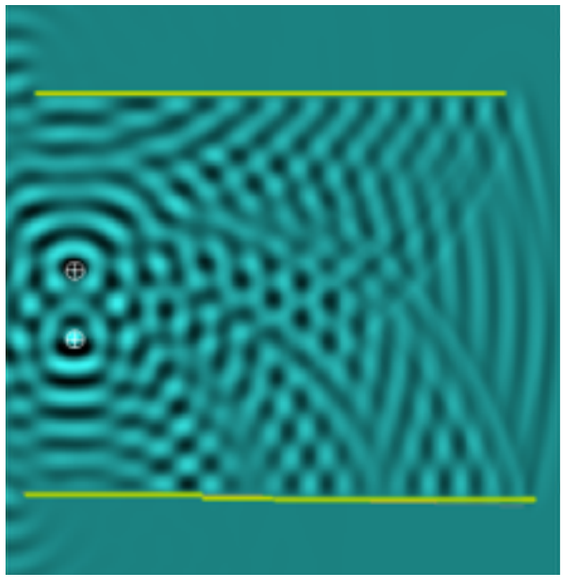
MIMO
電波を波紋としてイメージしてみる



送信アンテナ1つ



送信アンテナ2つ



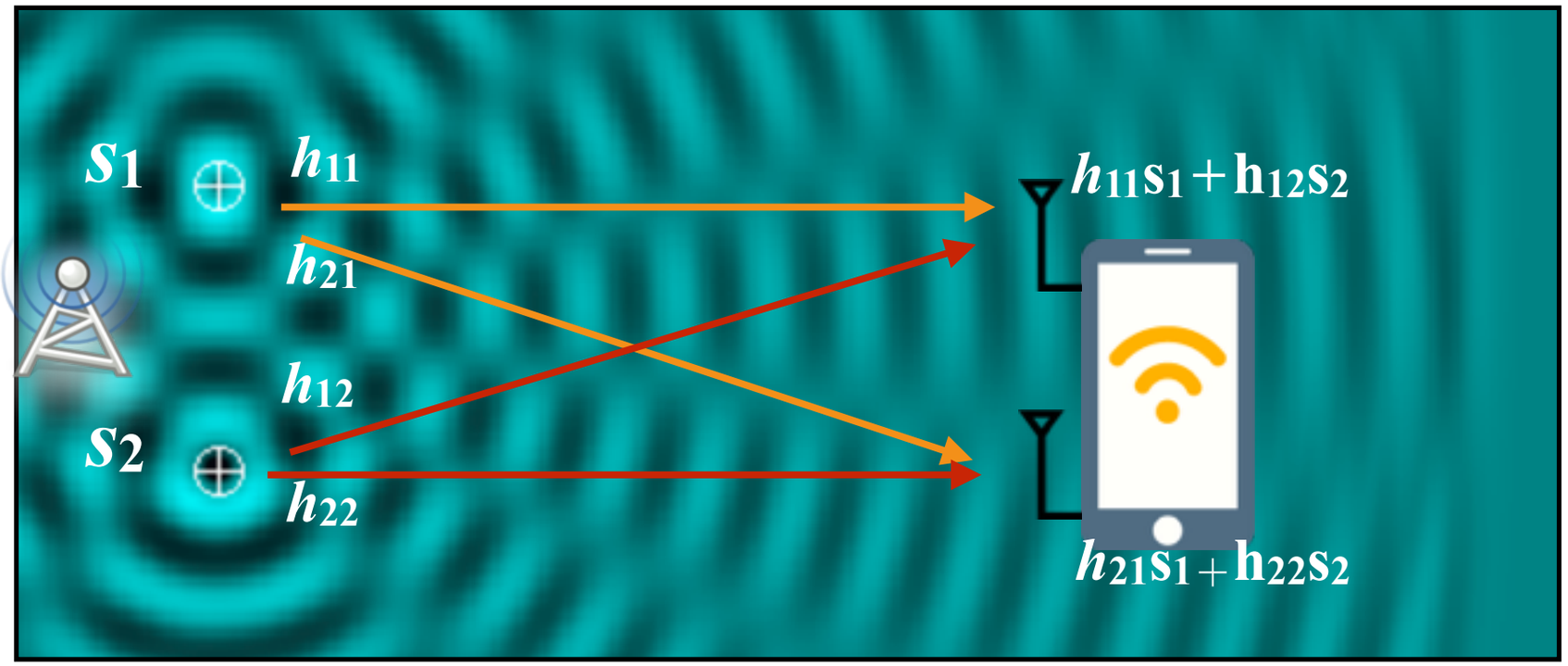
送信アンテナ2つ(壁あり)

ひとつのチャネルにて、複数のアンテナを使用して
複数のストリームを同時に送信するのがMIMO

でも同じチャネルで同時に通信できるのは1:1だったのでは…?
どうして同じチャネルで複数送信できるのか?

MIMO

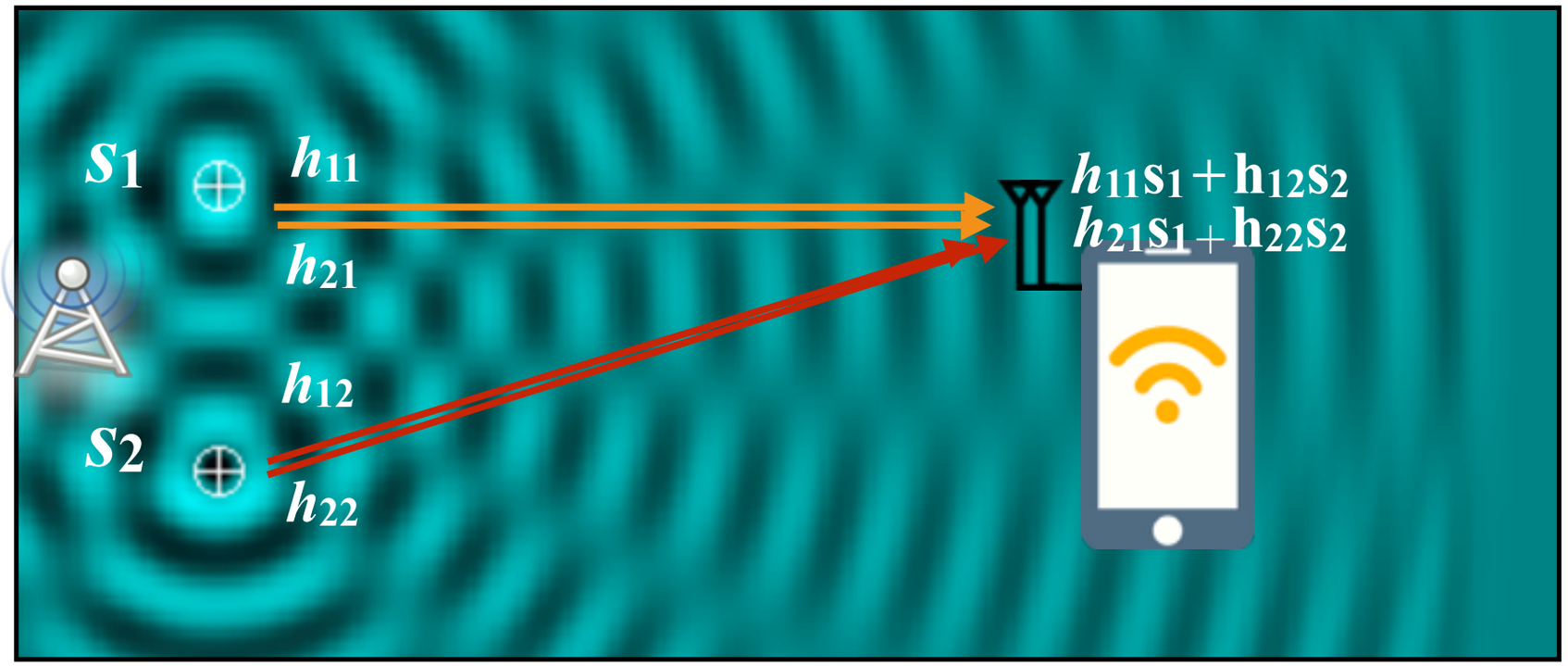
2つの信号(s_1, s_2)を同時に送受信したい



1.受信側のアンテナでは s_1, s_2 が混ざって受信される
2.伝送路が4つあり、その応答を調べておく
3.伝送路が既知なら s_1, s_2 に関する連立方程式を解ける
4.端末で s_1, s_2 が分離できる
5.帯域幅が2倍になった、めでたし

MIMO

もしアンテナが物理的に離れていなかったら？(伝送路の空間相関高)



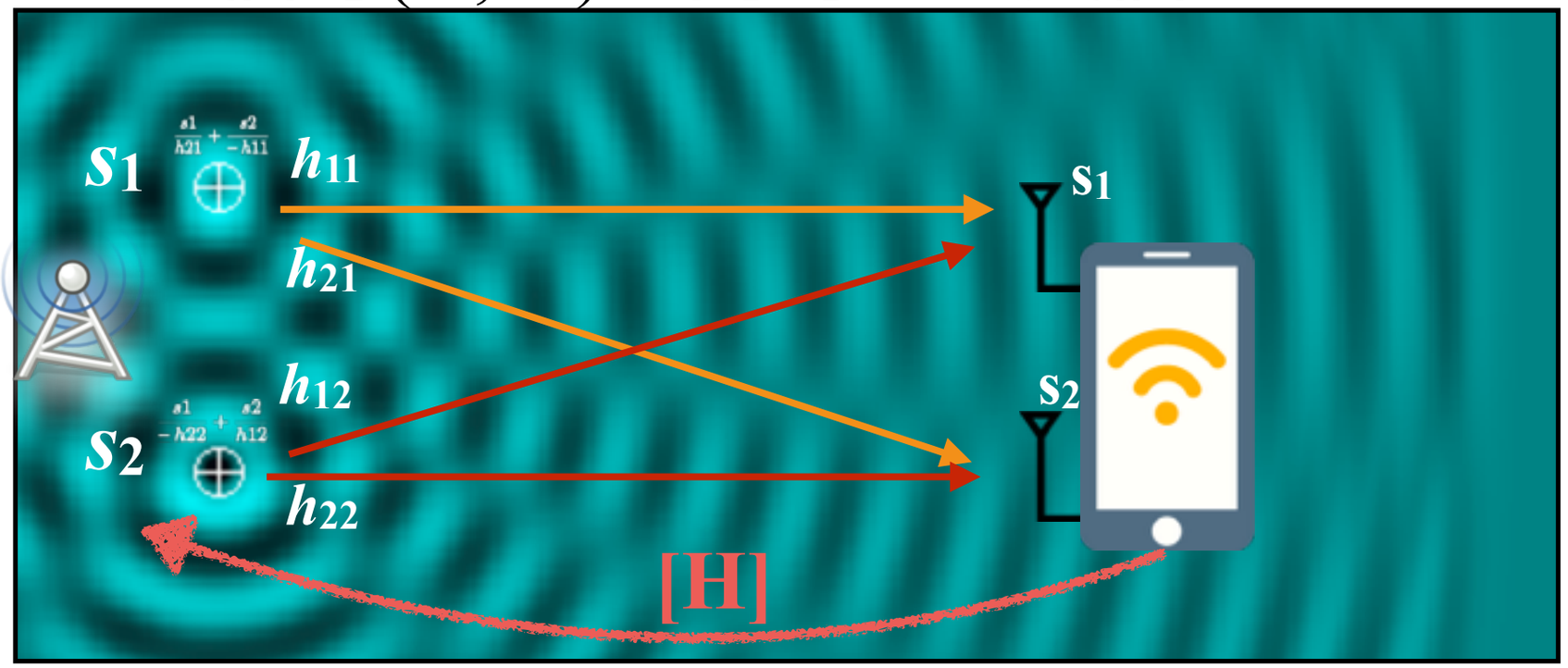
アンテナが近いと

- 相互に回り込みが発生して分離が難しくなり、特性が劣化する
  - 0.5λくらいは離したい
- でもアンテナを離すと端末の小型化が難しくなる
  - MIMOストリーム数(アンテナ数)を増やすとさらに小型化が難しい

そもそも分離の計算がけっこう大変なのですよね…それならば…?

MIMO

2つの信号(s_1, s_2)を同時に送受信したい その2



1.伝送路が4つあり、端末はその応答を調べてAPに送り返す

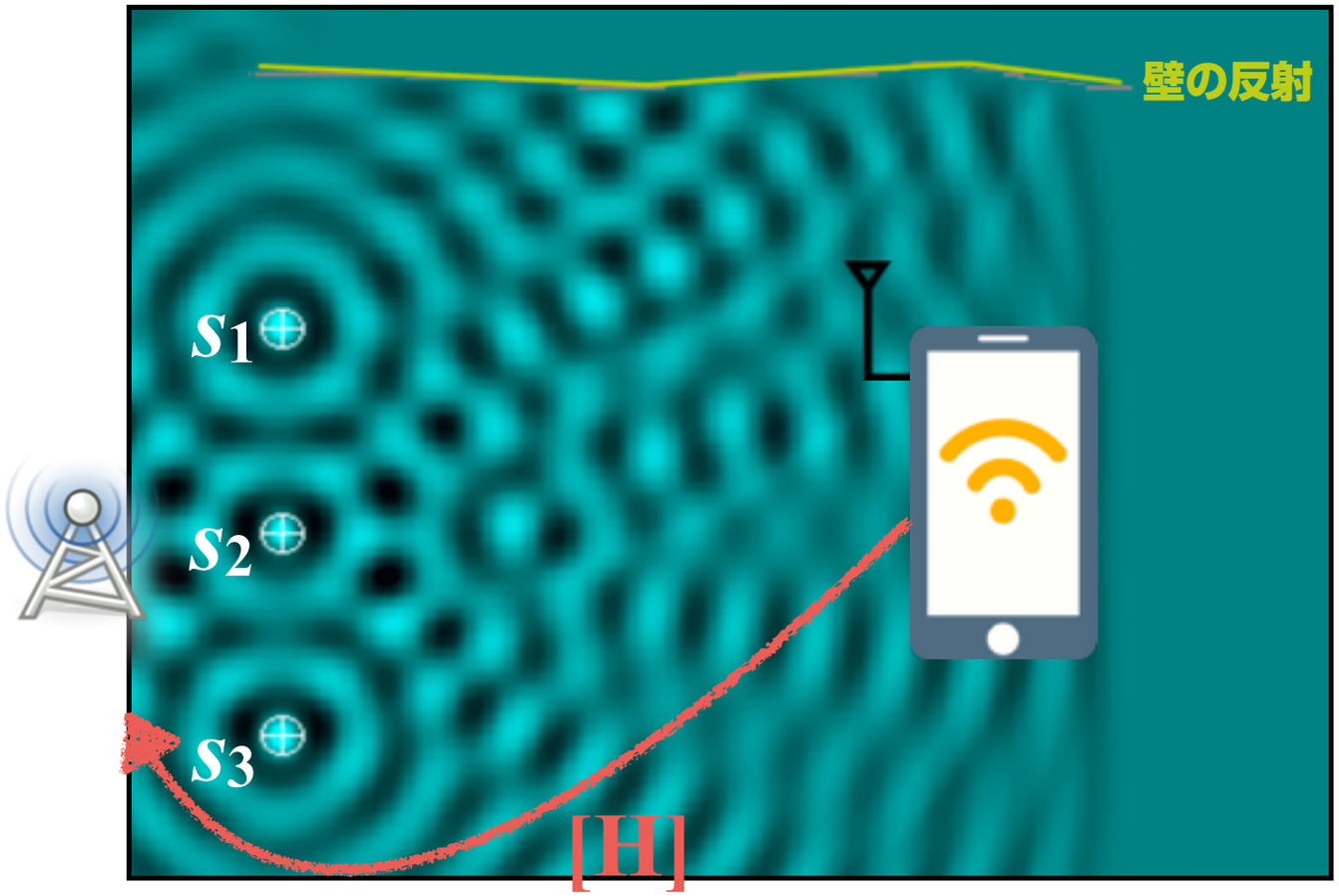
2.APは伝送路の応答がわかっているので、端末のそれぞれの受信アンテナで s_1, s_2 が分離ずみになるように*、データ送信前に事前加工してから送信する

3.端末側で分離の計算をしなくてよいので省電力化に有利

*端末のアンテナのうち、受信対象でないほうのアンテナで電力が最小(null)になるように加工する

ビーム フォーミング

干渉や反射の合成を味方につけて波が強くなるところを作る



1.伝送路が多数あり、端末はその応答を調べてAPに送り返す

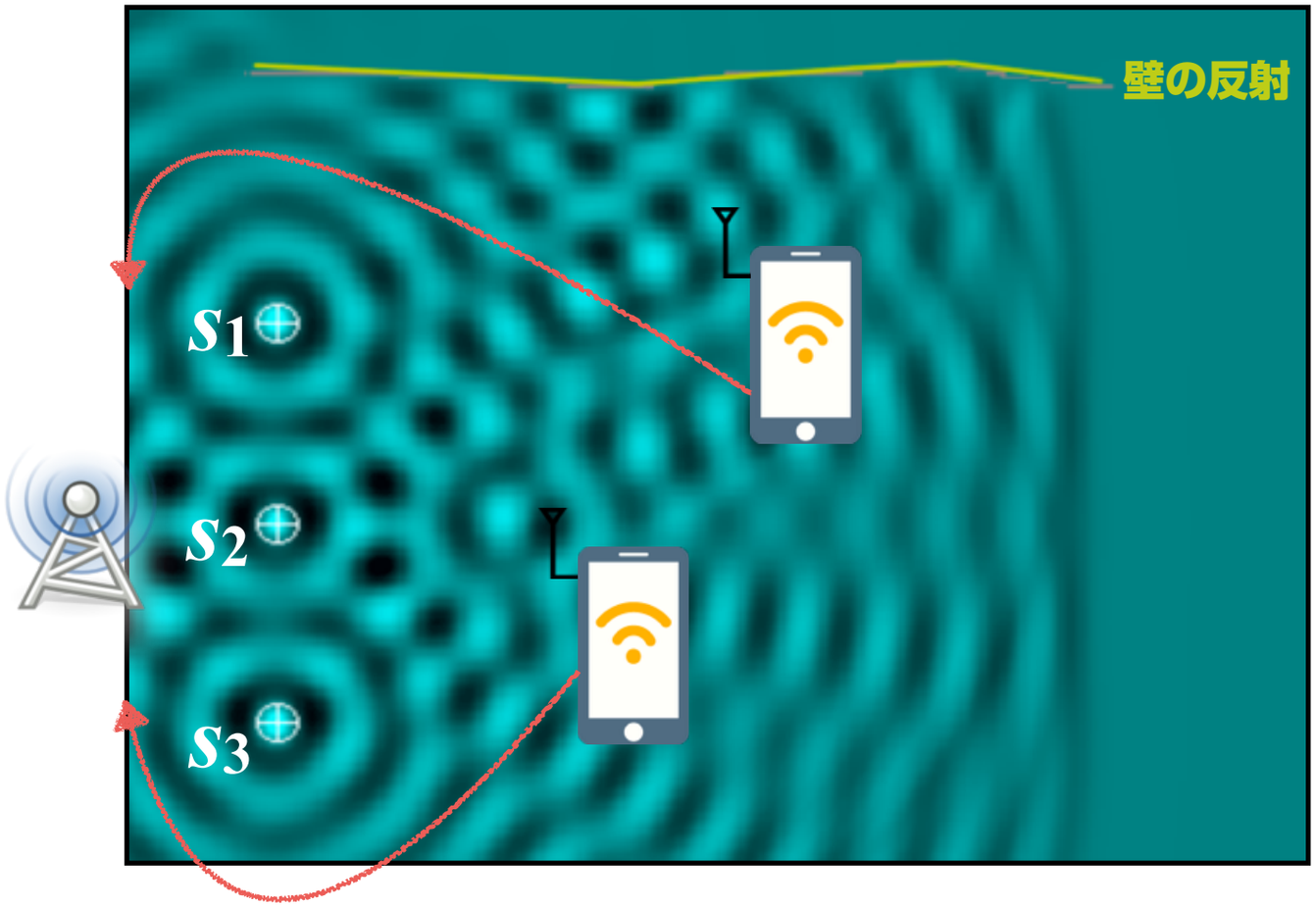
2.APは伝送路の応答がわかっているので、端末のそれぞれの受信アンテナで s が最大の電波強度になるように事前加工してから送信する*

干渉や壁の反射で波の濃淡をうまく作って、端末の存在する場所の波が強くなるようにする

*MIMOのように複数の送信機から同時送信するのではなく、アレイアンテナをアナログ的にスイッチングして指向性を作る方法もあります。

MU-MIMO

ビームフォーミングで空いた地点、空いたなら使ってしまう



1.複数いる端末はその応答を調べてAPに送り返す

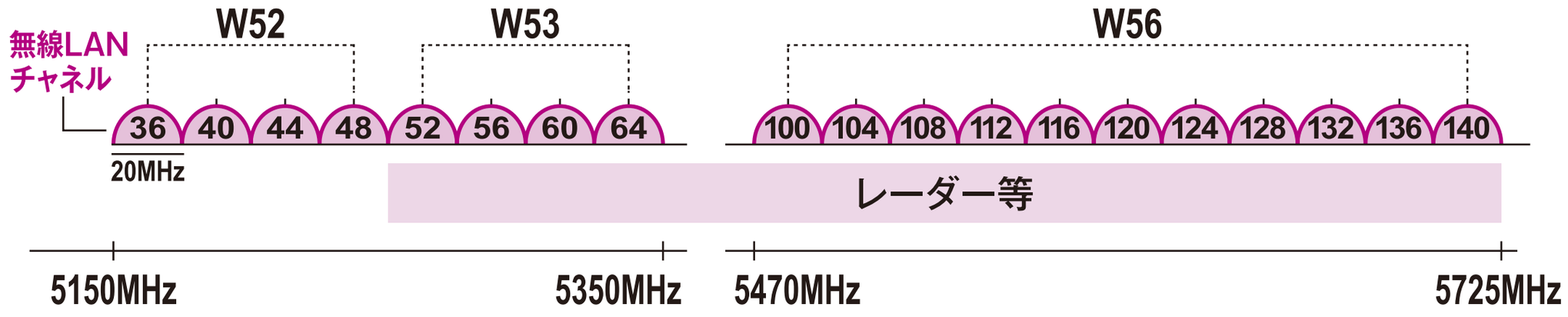
2.APはそれぞれのフレームが、宛先の端末で電波強度最大になり、
　宛先**でない**端末では**最小**になるように事前加工する

3.事前加工したフレームを同時に複数宛に送信する

4.端末はひとつずつACKを返す

DFS

レーダーの電波が存在したら送信してはいけない



- 5GHz帯には先客である気象レーダーがあるため、レーダーがいたら別のレーダーがいないチャネルに変更する義務がある
- レーダーがいないことを最低1分間は確認する義務があり、1分間以上何も送信できなくなるため、接続が途切れる原因となる
- 802.11a, 20MHz幅で使っていたときはチャネルに余裕があったが、チャネルボンディングによってバンド幅を広く使うようになり、DFSの影響を受けやすくなった
- 最近の製品ではレーダー波が検出されたらチャネル ボンディングをフォールバックして縮退しつつ停波は避けるようになっていたり、レーダー波を検出する前から他のチャネルをスキャンしておき、できるだけ停波しないでチャネルを変更する技術が用いられている

Captive Portal (capport)

Captive Portal とは

公衆無線LANなどに接続したときに出てくる画面

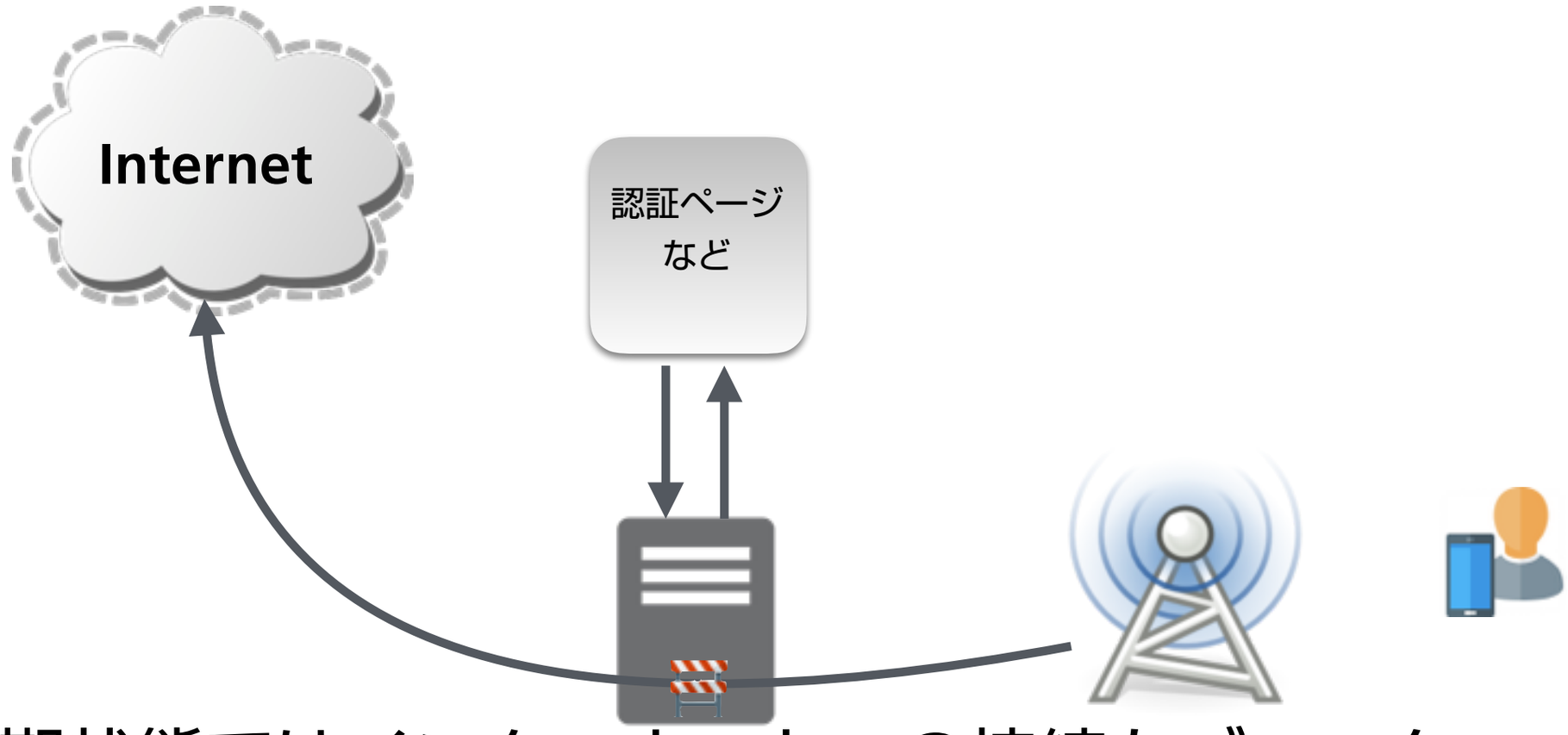
目的

- 認証
- 課金
- 情報表示

Webブラウザが使えれば端末を問わない

実装が比較的容易

Captive Portal の仕組み



1.初期状態ではインターネットへの接続をブロック

2.端末からのhttpリクエストを横取りして別の認証ページ
　などにリダイレクト

3.認証などが通れば接続を許可

Captive Portal の問題

- TLSエラー
  - httpsを横取りする
  - エラーが出ても続行する習慣がついてしまう
- ブラウザ以外の端末
  - スマートフォンのアプリなど、インターネット接続を要求するがhttpの横取りが不可能なもの
  - IoTデバイスなど表示や入力能力のない端末

Captive Portal Detection

- Webブラウザでなくても使えるよう、OS側でCaptive-Portal を扱う仕組み
- こんな画面が下からニョキッと出てくる→
- さまざまな実装のCaptive Portalがある
  - OSはどうやって検出する?
  - どうやって表示/入力する?
  - どうなったら接続成功??
    - 完全なdetectionが困難

Captive Portal Detection

- やっていることが man-in-the-middle attack だからそもそも無理がある
- Captive Portal の実装がばらばら
- 手順が明確になっていれば検出もちゃんとできる
- 手順が明確になっていればhttpを横取りなんて裏技みたいなことをしなくてもよくなる

公衆無線LANの利用者情報確認

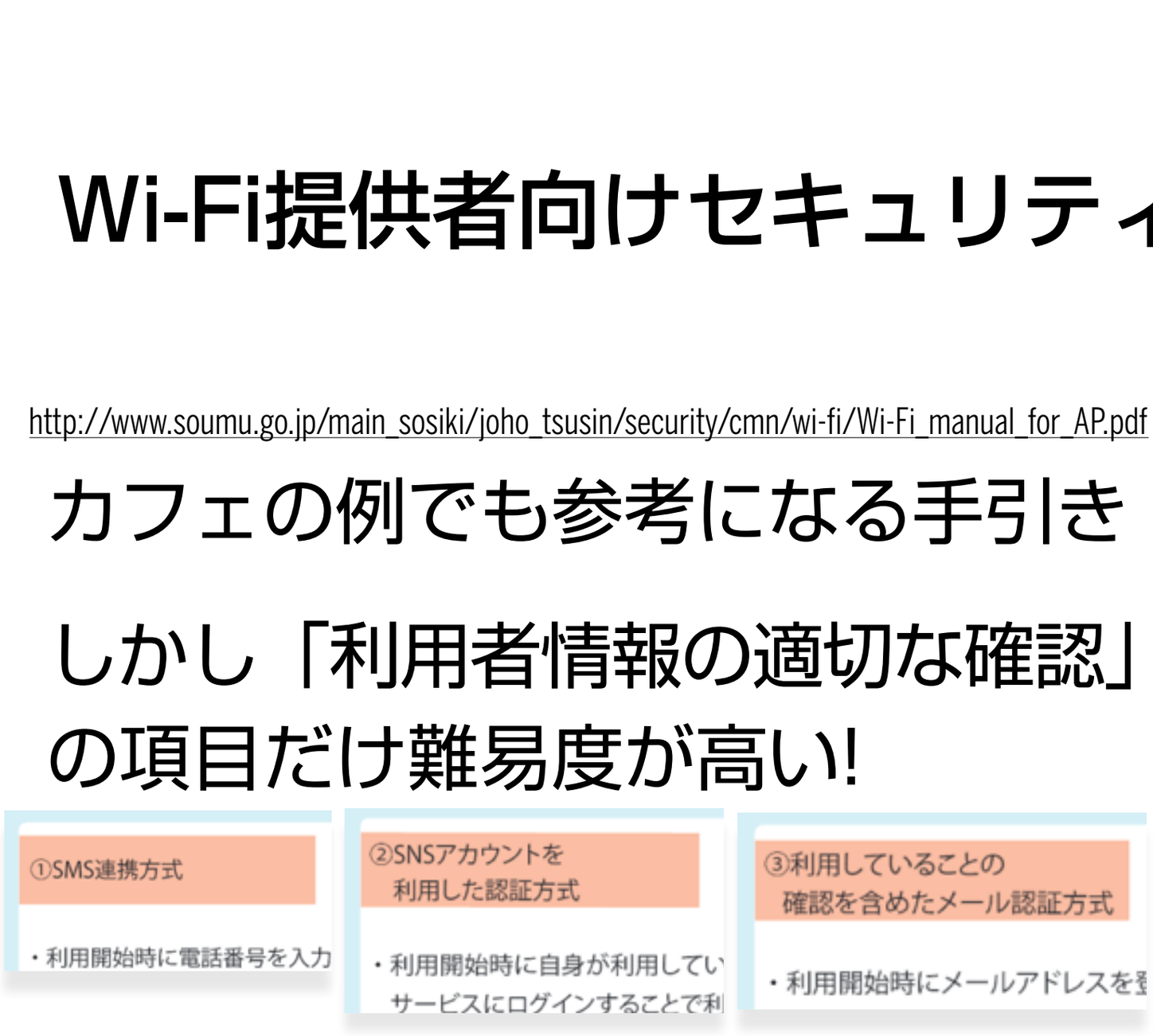
例えば、街のカフェ経営者がお客さんへサービスとしてインターネット接続を無料で提供したい場合、どうする?

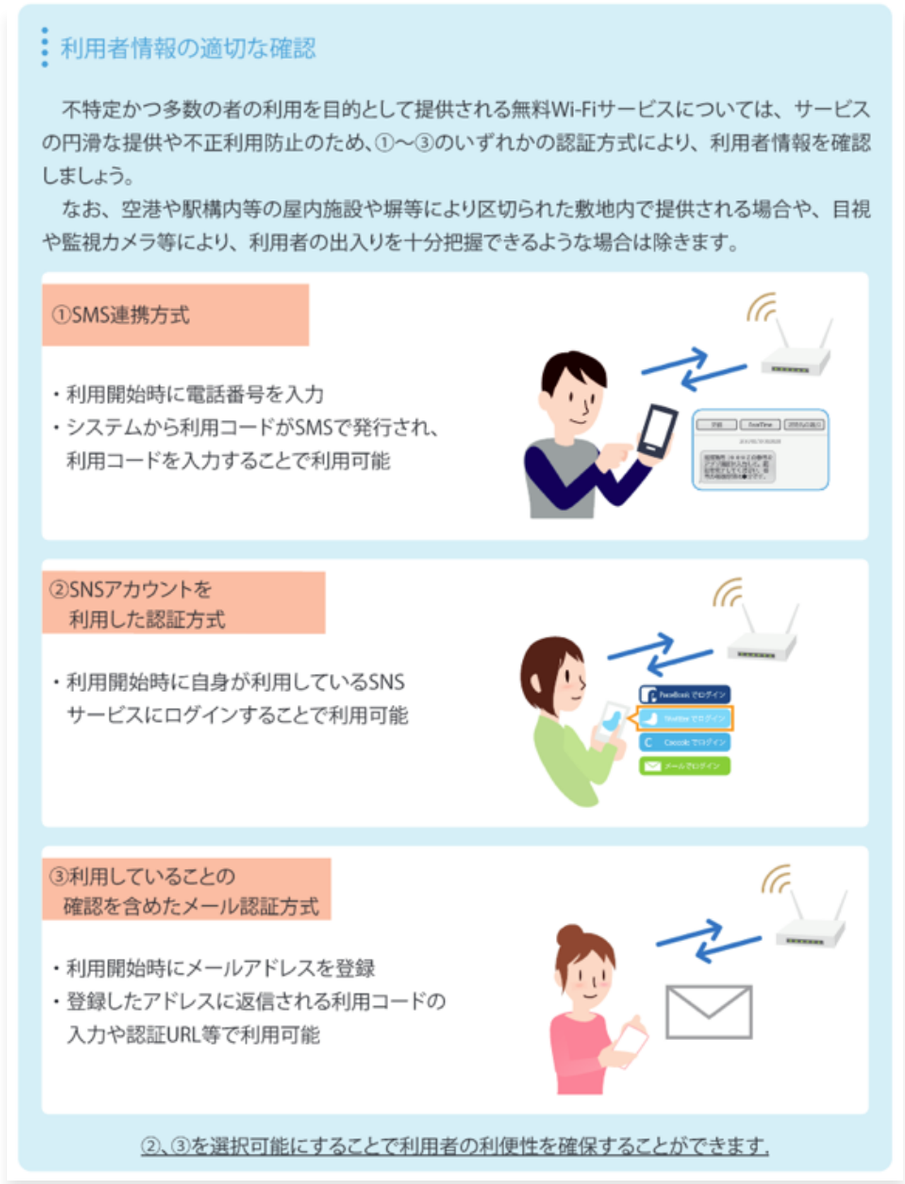
- 家電量販店で無線LANルータを買ってきて設置しPSKを教える?
  - この回線から悪さをする人がいたら?
    - 家庭用機器はログを残しにくい
    - 店外へ漏れた電波から接続しているかもしれない
- 公衆無線LANの導入
  - 無料は難しいかもしれない
  - 個人経営の店では難しいかもしれない

Wi-Fi提供者向けセキュリティ対策の手引き

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_AP.pdf

- カフェの例でも参考になる手引き
- しかし「利用者情報の適切な確認」の項目だけ難易度が高い!





- SMSはともかく、SNSアカウントやメールアドレスによる認証の実効性は??

Probe Request

無線LANの接続手順

1.端末がAPを探す

2.端末がAPの一覧を表示

3.ユーザがAPを選択

4.認証

5.接続完了

6.端末に接続を記憶

無線LANの接続手順

1.端末がAPを探す

2.端末がAPの一覧を表示

3.ユーザがAPを選択

4.認証

5.接続完了

6.端末に接続を記憶

無線LANの接続手順

1.端末がAPを探す

2.端末がAPの一覧を表示

3.ユーザがAPを選択

4.認証

5.接続完了

6.端末に接続を記憶

無線LANの接続手順

1.端末がAPを探す

- APから定期的に放送されるビーコン フレームを受信
  (受動的な検出)

  または

- 端末が Probe Request フレームを送信し APが応答した
  Probe Response を端末が受信
  (能動的な検出)

2.端末がAPの一覧を表示

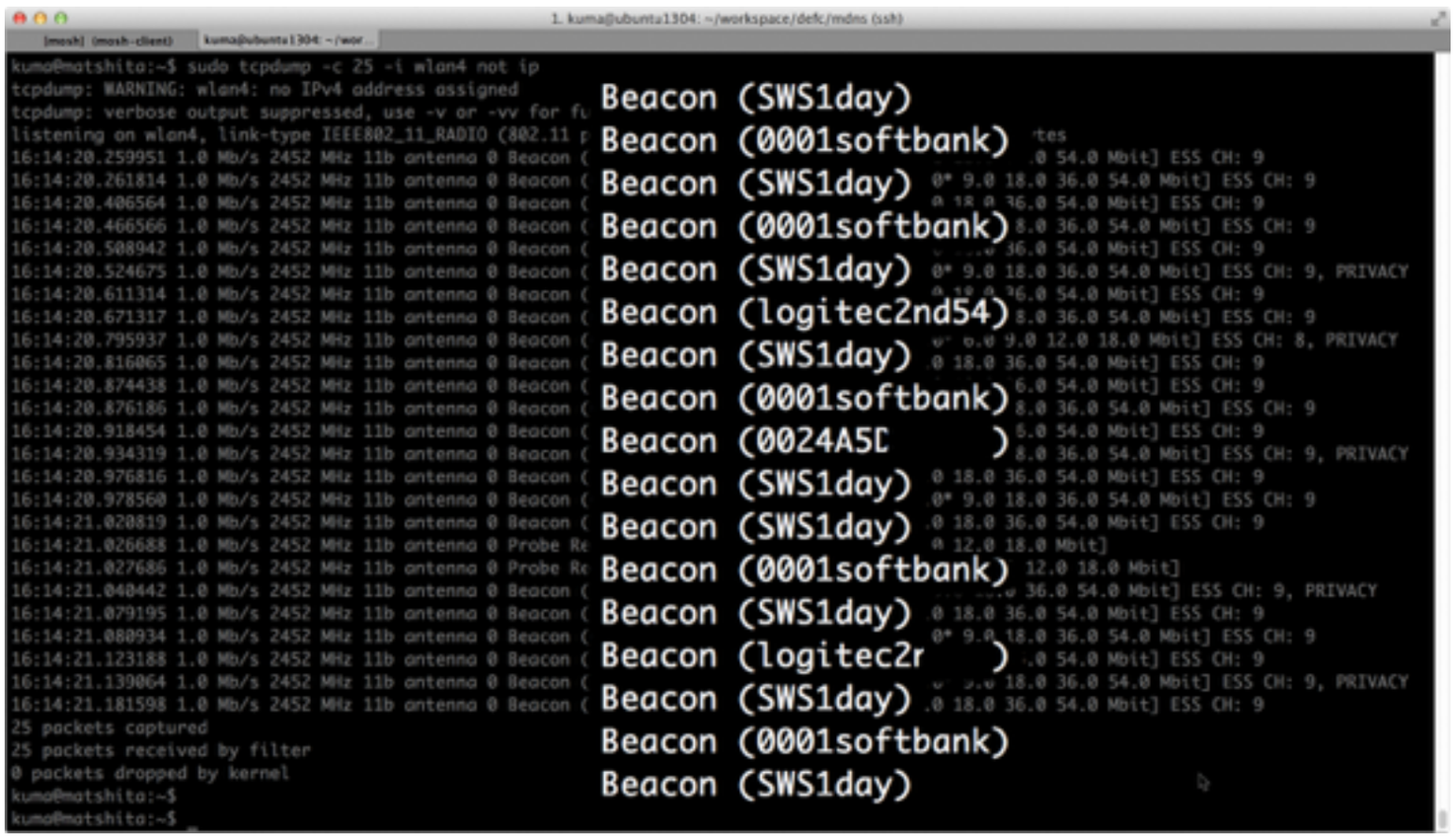
3.ユーザがAPを選択

4.認証

5.接続完了

6.端末に接続を記憶 (も可能)

受動的なAPの検出



APは通信相手がいないときも、
SSIDなどを定期的に放送している

(IEEE802.11 beacon frame)

能動的なAPの検出

AP 検出要求 (Probe Request)
「AP 誰かいますか」

AP 検出応答 (Probe Response)
「はい こちらは”MY_HOME_WIFI”」

端末はビーコンの受信を待たずに、積極的に検出要求を送信することもできる

能動的なAPの検出

AP 検出要求 (Probe Request)
「AP “**MY_HOME_WIFI**” いますか」

AP 検出応答 (Probe Response)
「はい」

端末はSSIDを**名指し**で積極的に検出要求を送信することもできる

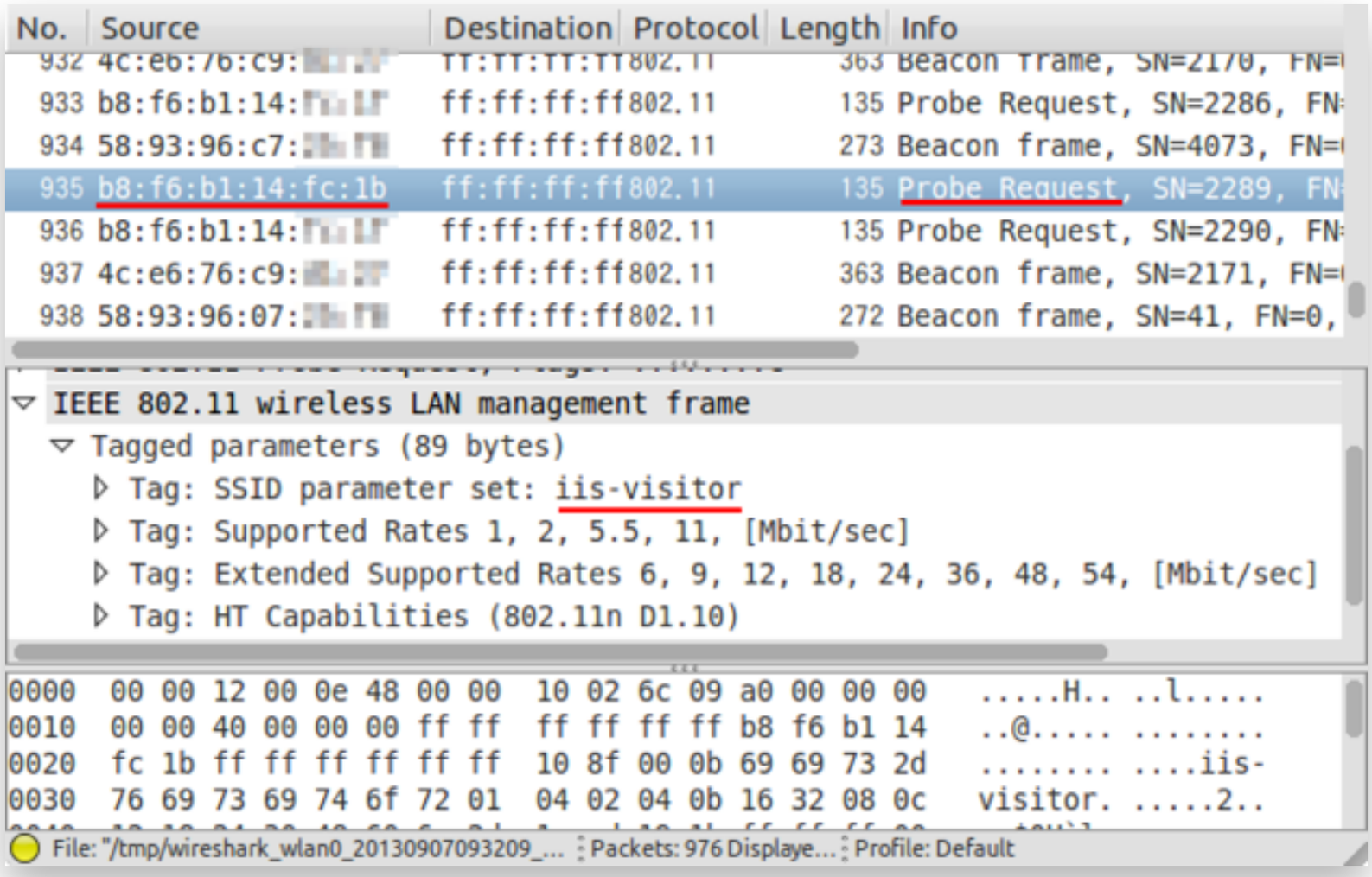
この方法でないと接続できないこともある
(SSIDをブロードキャストしていないなど)

問題点

端末は、自分の居場所がわからない

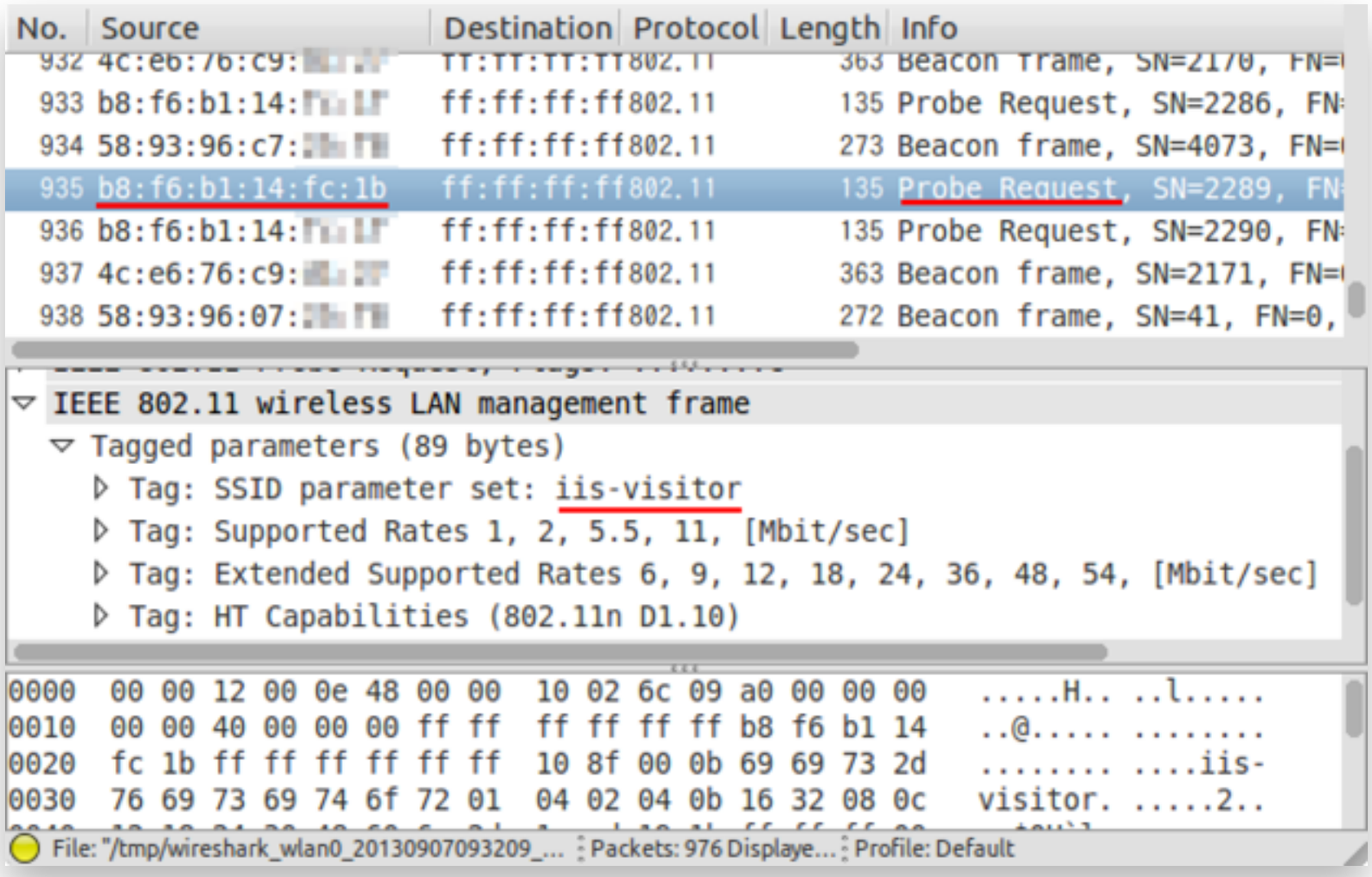
APがないはずの場所でもProbe Requestを送る

Probe Request に含まれる内容



- 端末の無線LANインタフェイスのMACアドレス
- 探しているSSID(ESSID)
  ≒接続を記憶させてあるSSID

Probe Request に含まれる内容



b8:f6:b1:14:...:... (Apple) の所有者は iis-visitor に接続したことがあるようです。

Probe Request に含まれる内容

Recently 802.11 probe request list

No.	firstseen	lastseen	seen	probe target	map	prober / OUI	flags	action
338	2013-06-19	2013-09-07 10:22:13	12547	uFi_FE		00:c6:10:5e:9 Apple, Inc.	w	-- Action --
148	2013-06-19	2013-09-07 10:22:13	12176	Ani a	map	00:c6:10:5e:9 Apple, Inc.	w	-- Action --
145	2013-06-19	2013-09-07 10:22:13	12852	aterm-c1	map	00:c6:10:5e:9 Apple, Inc.	w	-- Action --
36415	2013-08-20	2013-09-07 10:22:13	10001	HWD13_086361AC		00:c6:10:5e:9 Apple, Inc.	w	-- Action --
412	2013-06-19	2013-09-07 10:22:13	12775	0016014		00:c6:10:5e:9 Apple, Inc.	w	-- Action --
171	2013-06-19	2013-09-07 10:22:13	12799	logitec2nd48		00:c6:10:5e:9 Apple, Inc.		-- Action --
725	2013-06-20	2013-09-07 10:22:12	182	ppc1		10:bf:48:f5:0 ASUSTEK COMPUTER INC.		-- Action --
722	2013-06-20	2013-09-07 10:22:12	203	arms		10:bf:48:f5:0 ASUSTEK COMPUTER INC.		-- Action --
21946	2013-08-13	2013-09-07 10:22:10	7	BLW-5 M		7c:c5:37:d0:9 Apple, Inc.		-- Action --
21948	2013-08-13	2013-09-07 10:22:10	7	Hotel 1		7c:c5:37:d0:9 Apple, Inc.		-- Action --
21947	2013-08-13	2013-09-07 10:22:10	7	0808686		7c:c5:37:d0:9 Apple, Inc.		-- Action --
12163	2013-07-16	2013-09-07 10:21:21	1349	gtk	map	b8:f6:b1:14:f Apple, Inc. mbpw	w	-- Action --
1370	2013-06-21	2013-09-07 10:21:21	1564	geeksui_4F	map	b8:f6:b1:14:f Apple, Inc. mbpw	w	-- Action --
1369	2013-06-21	2013-09-07 10:21:21	1547	takano64		b8:f6:b1:14:f Apple, Inc. mbpw	w	-- Action --
1368	2013-06-21	2013-09-07 10:21:21	1559	caesi		b8:f6:b1:14:f Apple, Inc. mbpw	w	-- Action --
1367	2013-06-21	2013-09-07 10:21:21	1604	020F3A3C88		b8:f6:b1:14:f Apple, Inc. mbpw	w	-- Action --
1371	2013-06-21	2013-09-07 10:21:21	1577	PICNIC	map	b8:f6:b1:14:f Apple, Inc. mbpw	w	-- Action --
1365	2013-06-21	2013-09-07 10:21:21	1575	106F3F295	map	b8:f6:b1:14:f Apple, Inc. mbpw	a	-- Action --
1363	2013-06-21	2013-09-07 10:21:21	1592	sinap_guest	map	b8:f6:b1:14:f Apple, Inc. mbpw	w	-- Action --
1362	2013-06-21	2013-09-07 10:21:21	1624	shibuhouse_bf	map	b8:f6:b1:14:f Apple, Inc. mbpw	w	-- Action --
1361	2013-06-21	2013-09-07 10:21:21	1605	shibuhouse_highspeed		b8:f6:b1:14:f Apple, Inc. mbpw	w	-- Action --
12162	2013-07-16	2013-09-07 10:21:21	2256			b8:f6:b1:14:f Apple, Inc. mbpw		-- Action --
67332	2013-09-07	2013-09-07 10:20:37	18	ALICE_N		60:33:4b:f2:d Apple, Inc.		-- Action --
14826	2013-08-07	2013-09-07 10:20:29	2483	sc a		08:11:96:ae:l Intel Corporate	w	-- Action --
15991	2013-08-07	2013-09-07 10:20:26	26	BUFFALO		d8:d1:cb:de: Apple		-- Action --
18468	2013-08-09	2013-09-07 10:20:15	1472	o-net		e0:b9:a5:d0: Azurewave		-- Action --
56549	2013-08-31	2013-09-07 10:20:14	23	4CE676AD		70:56:81:48: Apple Inc		-- Action --
67387	2013-09-07	2013-09-07 10:20:00	4	GP02-F4559CC1		78:a3:e4:ca: Apple, Inc.		-- Action --
67386	2013-09-07	2013-09-07 10:19:44	1	D25HW-6416F0		90:84:0d:cd: Apple, Inc		-- Action --

- このように一度に複数のSSIDへProbe Requestを送信することがある
- MACアドレスとSSIDの組み合わせ単体ではあまり意味をなさなかったフレームが、名寄せの可能性をおびてくる
- この例では幾つものシェアオフィスに出入りしていること、特定の個人と交友関係にあることが推測できる

Probe Request に含まれる内容

- ESSID(いわゆるSSID)が含まれるが、BSSID(APのMACアドレス)は含まれない
  - よくあるSSIDなら識別できない
  - SSID内にBSSIDが含まれるものは完全にユニーク
- BSSIDからAPの位置情報を引けてしまう

  https://developers.google.com/maps/documentation/geolocation/

  * 一般的に公開されているAPIではBSSIDが2つ以上必要だが、プライベートAPIでは1つで引けるものもある
- たとえば **00005E0053FF_A** のようなSSIDは設置場所まで漏れる可能性が高い

APの位置が漏れる とは

N/A

特定の端末を追跡できる

Philz Coffee、WiFi利用の顧客分析をプライバシー問題により中止 (2014/05 TetchCrunch)

http://jp.techcrunch.com/2014/05/30/20140529philz-coffee-drops-euclid-analytics-over-privacy-concerns/

> “ 携帯電話やタブレットのWiFiをオンにした状態で、Philzに入るか店の前を通過すると、同カフェはEuclidの分析システム使ってそのデバイスを近隣の中で他のデバイスと区別することが可能だ。それがわかれば、店は他のデータと組み合わせて何らかの結果を導くことができる。例えば、店の近くや中にいた時間や、どこに立っていたかも。”

ゴミ箱ネットワークがスマホを追跡：ロンドン (2013/08 WIRED)

http://wired.jp/2013/08/12/recycling-bins-are-watching-you/

> “ 12カ所のポイントを通過した何十万人もの歩行者が、気がつかないうちに、自分のスマートフォンが持つ固有なMACアドレス(中略)を、Renew London社によって記録されていたのだ。”

問題点

- 長期にわたって追跡される(MACアドレスが固定)
- 端末の所有者と関係のある団体、住所などが漏れる
  - 同じ端末から要求のある*SSID1*と*SSID2*の関係性も推測できる
- オプトアウトが難しい
  - 端末からの電波を一方的に受信するだけで成立
- MACアドレスと所有者を紐づけられるとさらに問題が…

そこで、端末メーカーは対策をしてきました

Ephemeral MAC Address

Probe Request 時にはランダム化したMAC アドレスを使用する

iOS 8 strikes an unexpected blow against location tracking (2014/06 The Verge)

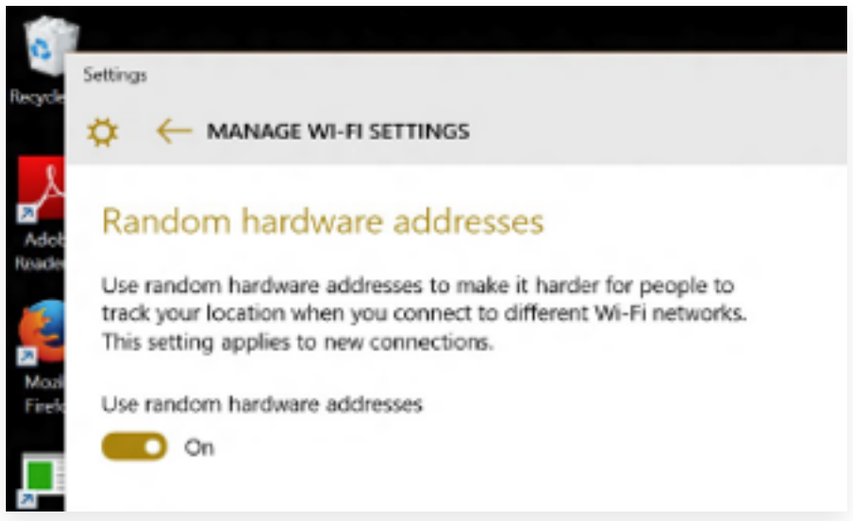
http://www.theverge.com/2014/6/9/5792970/ios-8-strikes-an-unexpected-blow-against-location-tracking/

> “ but a new iOS 8 feature is set to cause havoc for location trackers, and score a major win for privacy. (中略) When iOS 8 devices look for a connection, they randomize that address, effectively disguising any trace of the real device until it decides to connect to a network.”

iOS8.0ではこれが有効になる条件が厳しく、ほとんど意味がなかったが、9.0以降ではかなりランダム化されているように見える

Ephemeral MAC Address

Experience with MAC Address Randomization in Windows 10 (2015/07 IETF93)
https://www.ietf.org/proceedings/93/slides/slides-93-intarea-5.pdf



でも手元のPCで試したところサポートされていないようでした…

“ Only present if the hardware is recent and supports randomization.”

対処法

- 不要なAPの設定を端末から削除する
- APのSSIDはなるべくユニークでないものにする
  - 最低でもMACアドレスが含まれるものは避ける
- SSIDをステルスにしないほうがいいかも
  - 端末はステルスのAPに対しては積極的にProbe Requestを送るようだ

無線LANの特徴

免許不要で使える

- 安価で高速
- 買ってきてすぐ使える
- 不安定さを許容しなければならない
  - 誰もほかの無線局を排除できない
  - 故意の妨害は、**その行為自体**は違法ではない場合もある
- セキュリティ
  - 他人が何をしているかわからない
- 免許不要は良いことばかりじゃない
  - よそからの干渉など自己解決できない問題もある

もし免許が必要だったら?

- 安定した品質
- 国がリソース(電波)を管理してくれる
  - 混信はできる限り排除される
  - 免許なしに電波を出したら違法
  - 妨害したら電波法違反
  - なりすましや中間者攻撃なども(多分)電波法違反
- 用途が限られるかもしれない
- 無線LANみたいに爆発的に普及しない
  - 国内大手キャリア3社など

たとえば携帯端末では

- 通常、セルラーと無線LANの両方を装備している
- 品質差が徐々に縮まってきている
  - MulteFire, Wi-Fi Calling などセルラー側でも無線LAN帯域を積極的に使う動き
- ハイブリッドな無線ネットワークとして再構築されようとしている

__END__