

# **AIR-SAP1602I-Q-K9 初期設定簡易マニュアル 802.11abgn Ver1.04a**

ファームウェア: ap1g2-k9w7-tar.152-2.JB 用  
対象機種: DT-5300、IT-300、DT-X7、DT-X8、IT-9000、V-T500、V-N500

## **カシオ計算機株式会社**

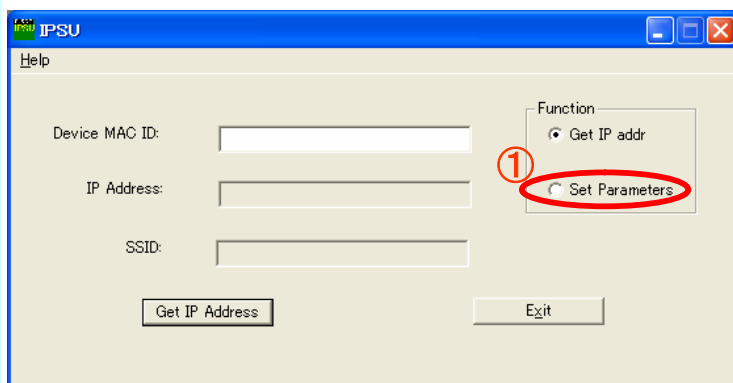
カシオ計算機で動作確認した場合の設定方法になります。  
動作保証をするものではありません。  
本マニュアルは1例として、WPA-PSKの設定を行っております。

2014/07/25 改訂

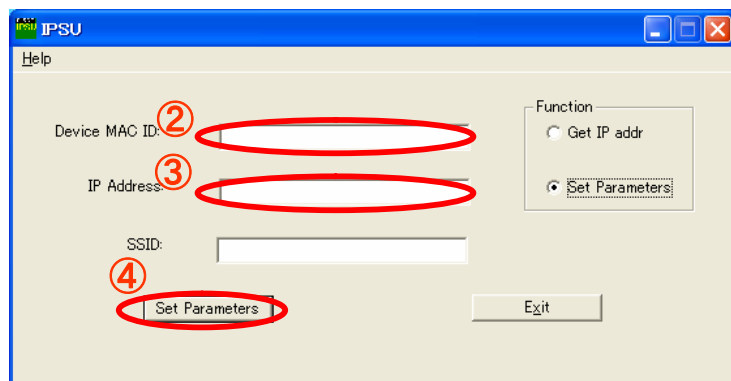
# 初期設定①「APとの接続」

Aironet-1602 (AIR-SAP1602-Q-K9) は、初期状態では IP アドレスが設定されていません。

最初に Cisco 社の WEB サイトより「IPSU」という設定ツールを入手して、AP の初期設定を行ってください。IPSU は Cisco.com にてユーザ登録いただき Download Software (Downloads Home) > Products > Wireless > Access Points > Cisco Aironet 340 Series > Cisco Aironet 340 Access Points > IP Setup Utility (IPSU)-1.01.013



- ①、IPSU を起動し、『Function』の『Set Parameters』を選択します。
  - ②、本体裏に記載されている MAC アドレスを入力します。
  - ③、運用する IP アドレスを入力します。
  - ④『Set Parameters』を選択します。
- ※SSID の設定は別途行います。



「Device does not answer for SET IP」のエラーメッセージが表示された場合は、MAC アドレスを入力し『Function』の『Get IP addr』を選択して、『Get IP Address』を選択して、IP が登録されているか確認してください。

この後、イントラネットに PC と AP を接続するか、接続している PC の IP アドレス、サブネットマスクを AP と同じセグメントに変更して、改めて PC のブラウザから AP に設定した IP アドレスを入力して他の項目を設定します。

繋がらない場合には、一度下記の手順で AP を初期化してみてください。

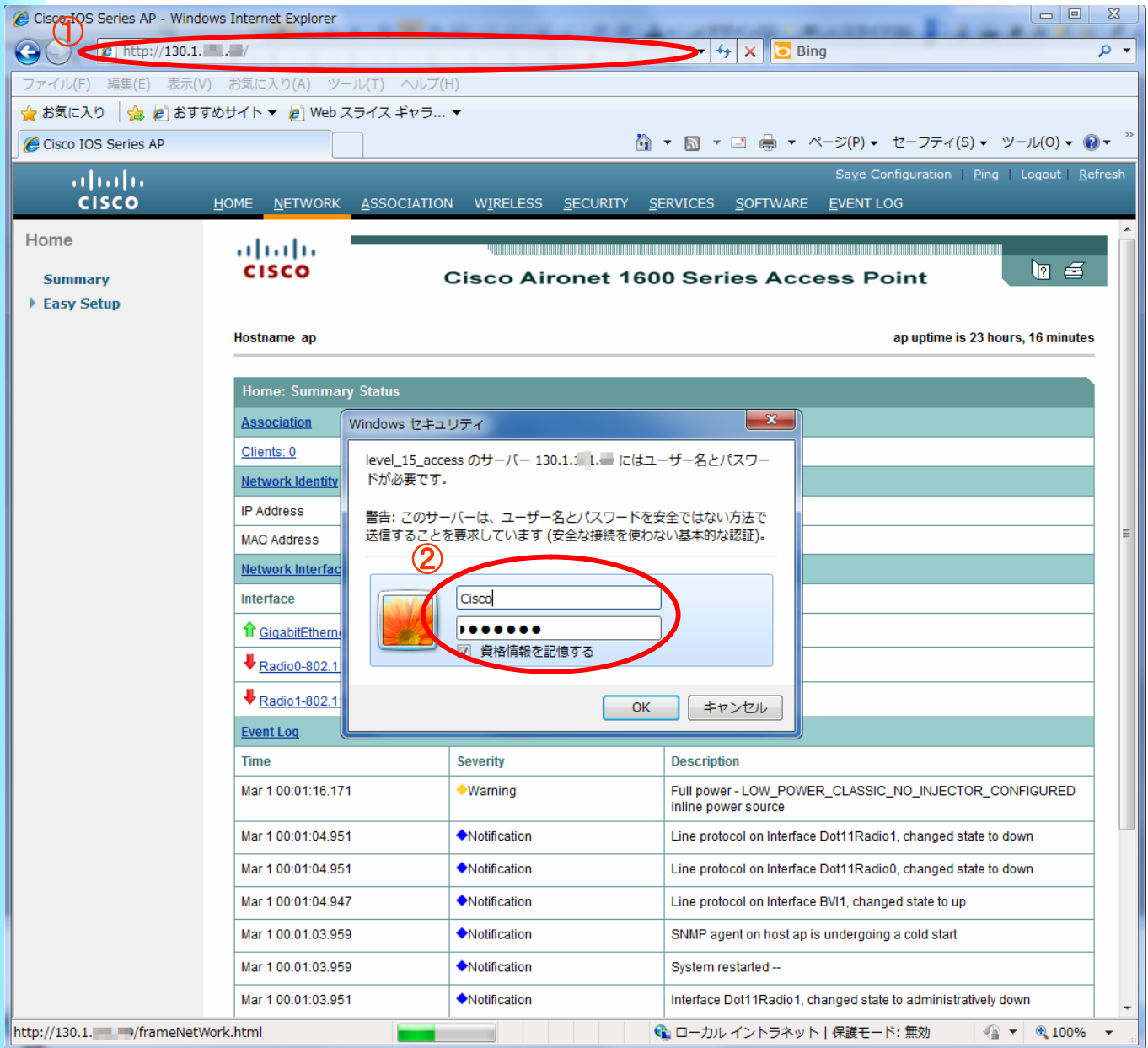
1. アクセスポイントの電源を切断します。
2. MODE ボタンを押しながら、アクセスポイントに電源を接続します。
3. そのまま MODE ボタンを 2～3 秒押し続け、ステータス LED がオレンジに変わったら MODE ボタンを離します。
4. 数分で、工場出荷状態で起動しますので、はじめから設定をやり直してください。

その他に注意事項として、

1. 設定する PC のファイアウォールを無効にして試してください。
2. 設定する PC の IP 設定を API に指定したい IP のセグメントと同じにして試してください。
3. AP と設定 PC の簡易環境として試してください。DHCP 環境の場合は IP が割り振られる可能性があります。

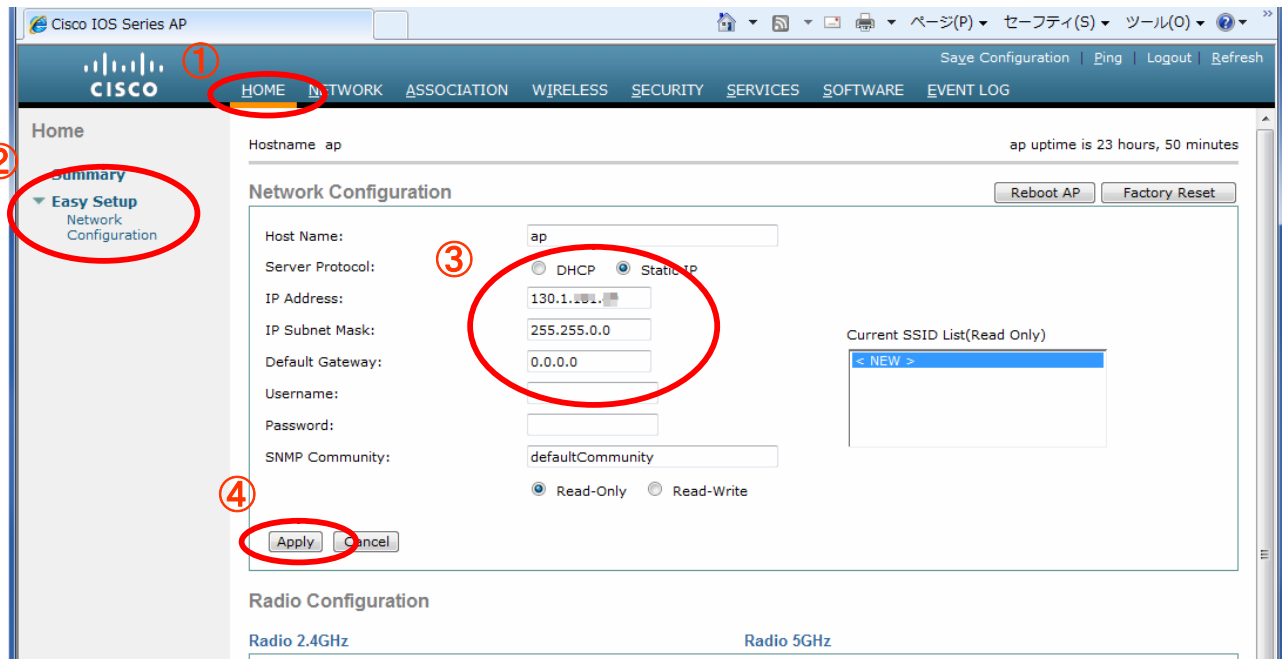
# 初期設定②「ブラウザによる設定」

- ①、APに設定したIPアドレスをブラウザのアドレスバーに入力します。
- ②、ユーザ名・パスワードを聞いてきますので、両方に『Cisco』を入力します。  
『OK』を選択します。



# 初期設定③「IPアドレス」

- ①、『HOME』を選択します。
- ②、『Easy Setup』『Network Configuration』をクリックします。
- ③、IPアドレスが、設定した値である事を確認し、必要に応じて『IP Subnet Mask』『Default Gateway』を設定します。
- ④、『Apply』をクリックします。



## ●ご注意

固定IP環境でWEB設定からのDefault Gatewayを有効にする場合は、IP ROUTING機能を無効にする必要があります。IP ROUTING設定を無効にするには、CLIにて指定する必要があります。誠にお手数ではございますが、TELNETなどにて以下の設定をお試しいただくようお願いいたします。

Telnetの場合は

[スタート]の[検索の開始]ボックスに「Telnet」と入力して、Enter キーを押します。

コマンド プロンプトで

Microsoft Telnet>open <AP IPアドレス>

と入力し、Enter キーを押します。

画面に従いAPのユーザ名・パスワード(初期値 ユーザ名: Cisco、パスワード: Cisco)を入力しAPに接続します。

画面上で以下の入力を行います。

```
ap>enable
```

Password: (APのパスワードを入力します。初期値はCisco)

```
ap#configure terminal
```

```
ap(config)#no ip routing
```

```
ap(config)#exit
```

```
ap#write memory
```

Building configuration...

[OK]

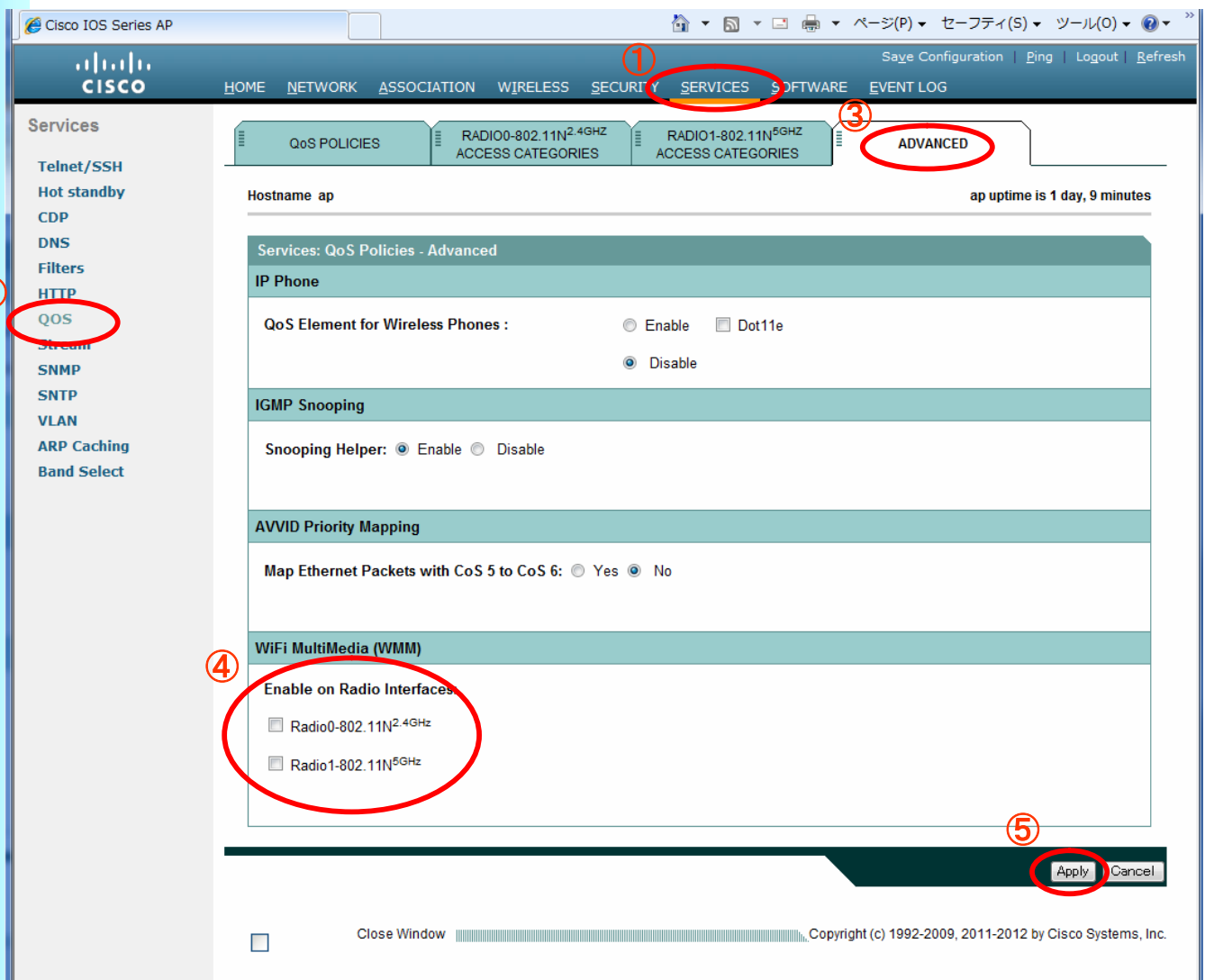
```
ap#exit
```

以上により、WEB設定からのDefault Gatewayが有効になります。

# 初期設定④「WMM」

WMM(WiFi Multi Media)を無効にします。

- ①、『SERVICES』を選択します。
- ②、『QoS』を選択します。
- ③、『ADVANCED』タブを選択します。
- ④、利用する無線規格の『Radio0-802.11N 2.4GHz』(802.11bg利用時)、  
『Radio1-802.11N5GHz』(802.11a利用時)のチェックを外します。
- ⑤、『Apply』をクリックします。



# セキュリティの設定⑤( WPA-PSK)「暗号方式」

- ①、『SECURITY』をクリックします。
- ②、『Encryption Manager』をクリックします。
- ③、利用する無線規格の『RADIO0-802.11N 2.4GHz』(802.11bg利用時)/『RADIO1-802.11N 5GHz』(802.11a利用時)を選択します。
- ④、『Cipher』で、暗号化の指定を行います。  
TKIPを使用する場合は、『TKIP』を選択します。  
AESを使用する場合は、『AES CCMP』を選択します。
- ⑤、『Apply-Radio0』(802.11bg利用時)、『Apply-Radio1』(802.11a利用時)又は『Apply-All』(両方の選択)をクリックします。

The screenshot shows the Cisco IOS Series AP configuration page for Security settings. The page is titled "Security" and has a navigation menu on the left with options: Admin Access, Encryption Manager, SSID Manager, Server Manager, AP Authentication, Intrusion Detection, Local RADIUS Server, and Advance Security. The main content area is titled "Security: Encryption Manager - Radio0-802.11N2.4GHz". It shows the "Encryption Modes" section with "None", "WEP Encryption", and "Cipher" options. The "Cipher" option is selected, and the "AES CCMP" mode is chosen. Below this is the "Encryption Keys" section with four keys, each having a "Transmit Key" radio button, an "Encryption Key (Hexadecimal)" input field, and a "Key Size" dropdown menu. The "Global Properties" section at the bottom has "Broadcast Key Rotation Interval" set to "Disable Rotation" and "WPA Group Key Update" options. The "Apply-Radio0", "Apply-All", and "Cancel" buttons are at the bottom right.

Encryption Key	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>		128 bit
Encryption Key 2:	<input checked="" type="radio"/>		128 bit
Encryption Key 3:	<input type="radio"/>		128 bit
Encryption Key 4:	<input type="radio"/>		128 bit

Global Properties	
Broadcast Key Rotation Interval:	<input checked="" type="radio"/> Disable Rotation <input type="radio"/> Enable Rotation with Interval: DISABLED (10-10000000 sec)
WPA Group Key Update:	<input type="checkbox"/> Enable Group Key Update On Membership Termination <input type="checkbox"/> Enable Group Key Update On Member's Capability Change

# セキュリティの設定⑥ (WPA-PSK) 「SSID」

- ①、『SECURITY』を選択します。
- ②、『SSID Manager』を選択します。
- ③、『SSID』を入力します。
- ④、『Interface』の利用する無線規格の『Radio0-802.11N 2.4GHz』(802.11bg利用時) / 『Radio1-802.11 5GHz』(802.11a利用時)にチェックを入れます。
- ⑤、『Client Authenticated Key Management』にて『Key Management』を『Mandatory』を選択します。
- ⑥、『Enable WPA』にチェックを入れ、『WPA/WPAv1』または『WPAv2』を選択します。
- ⑦、『WPA Pre-shared Key』を入力します。
- ⑧、『Apply』をクリックします。

Security: Global SSID Manager

SSID Properties

Current SSID List

SSID: CASIO

VLAN: < NONE > Define VLANs

Band-Select: Band Select

Interface: ☒ Radio0-802.11N 2.4GHz ☒ Radio1-802.11N 5GHz

Network ID: (0-4096)

Client Authenticated Key Management

Key Management: Mandatory

Enable WPA WPAv2

WPA Pre-shared Key: .....

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

Set SSID as Guest Mode

Set Data Beacon Rate (DTIM): DISABLED(1-100)

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N 2.4GHz

Set Beacon Mode: ☒ Single BSSID Set Single Guest Mode SSID: < NONE >

Radio1-802.11N 5GHz

Set Beacon Mode: ☒ Single BSSID Set Single Guest Mode SSID: < NONE >

Set Infrastructure SSID: < NONE > Force Infrastructure Devices to associate only to this SSID

Apply Cancel

Apply Cancel

こちらのボタンではありません

端末側でWPAを設定している場合はWPAまたはWPA1を端末でWPA2を設定している場合はWPAまたWPAv2を選択してください。

## 初期設定⑦-1「802.11bgn利用時の無線LAN電源のON」

※初期状態ではDisable(無効)となっており、無線LANが使用出来ません。

- ①、『NETWORK』を選択します。
- ②、『NETWORK INTERFACES』の『Radio0-802.11n 2GHz』を選択します。
- ③、『SETTINGS』タブをクリックします。
- ④、『Enable Radio』を『Enable』にします。
- ⑤、『DefaultRadio Channel』を環境に合せたチャンネルに設定します。
- ⑥、『Aironet Extensions』を『Disable』に設定します。
- ⑦、『Apply』を選択し、設定を反映させます。

The screenshot displays the Cisco Aironet configuration web interface. The top navigation bar includes links for HOME, NETWORK, ASSOCIATION, WIRELESS, SECURITY, SERVICES, SOFTWARE, and EVENT LOG. The left sidebar shows the NETWORK section with sub-items like NETWORK MAP, NETWORK INTERFACE, and NETWORK INTERFACE. The main content area shows the configuration for Radio0-802.11n 2GHz. The SETTINGS tab is selected, showing the following configuration:

- Operating Mode: Mixed (selected)
- Enable Radio: ☒ Enable (selected)
- Current Status (Software/Hardware): Disabled
- Role in Radio Network: Access Point (selected)
- DefaultRadio Channel: Channel 1 - 2412 MHz (selected)
- Least Congested Channel Search: (Use Only Selected Channels)
- Channel Width: 20 MHz
- Traffic Stream Metrics: ☐ Enable, ☒ Disable (selected)
- Aironet Extensions: ☐ Enable, ☒ Disable (selected)
- Ethernet Encapsulation Transform: RFC1042 (selected)
- Root Parent Timeout: 0 (0-65535 sec)
- Root Parent MAC 1 (optional): (HHHH.HHHH.HHHH)
- Root Parent MAC 2 (optional): (HHHH.HHHH.HHHH)
- Root Parent MAC 3 (optional): (HHHH.HHHH.HHHH)
- Root Parent MAC 4 (optional): (HHHH.HHHH.HHHH)

The bottom of the page shows the Apply and Cancel buttons, with the Apply button highlighted by a red circle and the number 7.



## 初期設定⑦-2「802.11an利用時の無線LAN電源のON」

※初期状態ではDisable(無効)となっており、無線LANが使用出来ません。

- ①、『NETWORK』を選択します。
- ②、『NETWORK INTERFACES』の『Radio0-802.11n 5GHz』を選択します。
- ③、『SETTINGS』タブをクリックします。
- ④、『Enable Radio』を『Enable』にします。
- ⑤、『DefaultRadio Channel』を環境に合せたチャンネルに設定します。
- ⑥、『Aironet Extensions』を『Disable』に設定します。
- ⑦、『Apply』を選択し、設定を反映させます。

The image displays two screenshots of the Cisco configuration interface, illustrating the steps to enable 802.11n 5GHz wireless LAN.

**Top Screenshot:**

- ① The **NETWORK** tab is selected in the top navigation bar.
- ② The **Radio0-802.11n 5GHz** interface is selected in the left sidebar under **NETWORK INTERFACE**.
- ③ The **SETTINGS** tab is selected for the **Radio1-802.11n 5GHz Settings** section.
- ④ The **Enable Radio** option is set to **Enable** (radio button selected).
- The **Operating Mode** is set to **Mixed**.
- The **Current Status (Software/Hardware)** is **Disabled**.
- The **Role in Radio Network** is set to **Access Point**.

**Bottom Screenshot:**

- ⑤ The **DefaultRadio Channel** is set to **Channel 36 - 5180 MHz** (selected in the dropdown menu).
- The **Least Congested Channel Search** (Use Only Selected Channels) is shown with a list of channels from 36 to 140.
- The **Channel Width** is set to **20 MHz**.
- ⑥ The **Aironet Extensions** option is set to **Disable** (radio button selected).
- ⑦ The **Apply** button is highlighted at the bottom right.

# 補足説明 「802.11bgチャンネル」について

## ■アクセスポイントが一つの場合

2.4GHz帯では、10mW以下の出力の電波は免許不要で利用可能な為、様々な機器で使用されており場合によっては思わぬ機器で電波干渉が発生する場合があります。(電子レンジ、セキュリティゲート、監視カメラやコードレス電話など)

802.11b/gで使用する2.4GHz帯の周波数を13のチャンネル(802.11bの場合は14)に分割しており、きめ細かく使用する事が可能です。

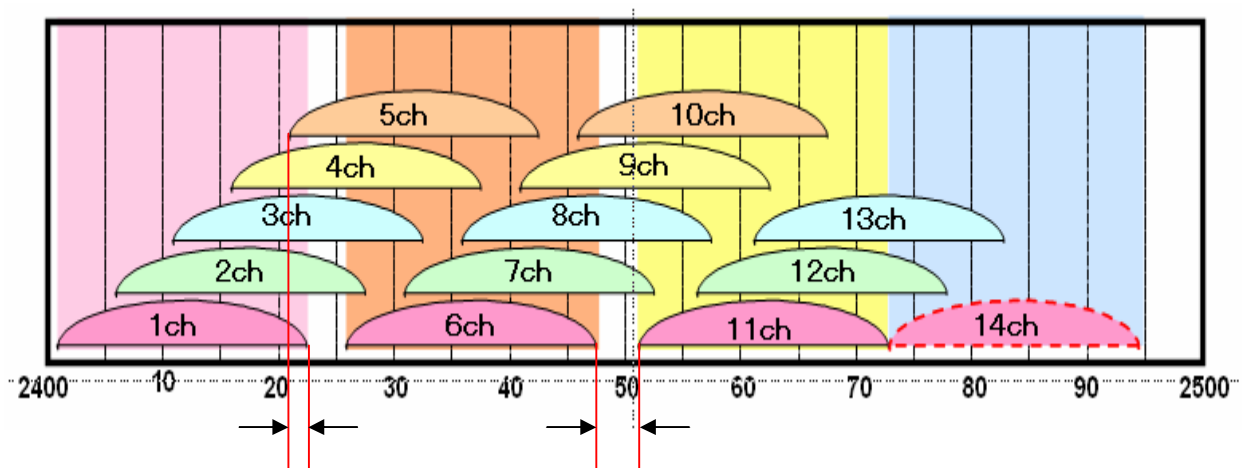
必ず事前に無線環境の調査・確認を行い、運用環境に合わせたチャンネル設定を行ってください。

## ■アクセスポイントが複数存在する場合

一つのチャンネルが使用する帯域は22MHzですが、隣り合うチャンネルの中心周波数の差は5MHzです。

隣り合ったチャンネルを同一の場所で使用すると、電波干渉が発生してしまいます。

そのため同一フロアに複数のアクセスポイントを設置する場合には隣り合うアクセスポイント同士で干渉が発生しないようにチャンネルを5ch(25MHz)以上離して設置する必要があります。



図のように、1chと5chの使用周波数帯域を見ると2MHzの重なりが発生します。逆に、6chと11chの使用周波数帯域を見ると、3MHzの空きがある事がわかります。

2.4GHz帯すべてを使用できる場合、1ch、6ch、11chと3チャンネルを同時に使用する事が可能です。

※802.11bの場合は、14chを利用できる機器がありますが、AIR-SAP1602I-Q-K9 については利用できません。

# 補足説明 「802.11a」について

## ■802.11a規格について

802.11aで利用できる周波数帯規格が複数存在します、機器においては対応していない規格があり注意が必要です。周波数規格はJ52・W52・W53・W56となります。先頭文字のJは国内(日本)規格・Wは国際規格を示し、2桁数字は中心周波数帯を示します、W52では国際規格・中心周波数5.2GHzとなります。DT-5300a規格対応モデルで利用できる規格はW52・W53・W56となります。

## ■DFS/TPCについて

W53・56は各種レーダーとの干渉を回避する義務があります。W53は気象レーダーとの干渉、W56は船舶・軍事用の各種レーダーとの干渉を避ける必要があります。アクセスポイントでこれらの電波を感知した場合には使用している周波数チャンネル・送信出力が自動的に変更します。無線設計者の意図しないチャンネルに変更される可能性があります。

●DFS:Dynamic Frequency Selection (動的電波周波数選択)

●TPC:Transmit Power Control (送信出力制御)

W53・56を使用する場合には、意図しないチャンネル変更や通信途絶等が起こる可能性があります。W52では上記の動作は必須になっていませんが、移動体衛星通信システムが利用している周波数のため屋外使用は電波法で禁止されています。

802.11a規格一覧表

規格	中心周波数	チャンネル番号	チャンネル数	DFS/TPC	アドホック	屋外利用	DT-5300	電波法改正年度
J52	5.2GHz	34・38・42・46	4	不要	可能	禁止	利用不可	2005年5月以前
W52	5.2GHz	36・40・44・48	4	不要	可能	禁止	利用可能	2005年5月以降
W53	5.3GHz	52・56・60・64	4	必須	禁止	禁止	利用可能	2007年～
W56	5.6GHz	100・104・108・112・ 116・120・124・128・ 132・136・140	11	必須	禁止	可能	利用可能	2007年～

## ■干渉について

802.11a規格の周波数帯は5GHzとなり、802.11b/g規格は2.4GHzとなりますのでa規格とb/g規格の干渉はありません。802.11a規格の同じチャンネル同士は干渉します。また、J52とW52では干渉する可能性があります。J52・W52は5.15GHz～5.25GHz、W53は5.25GHz～5.35GHz、W56は5.47GHz～5.725GHzの帯域。

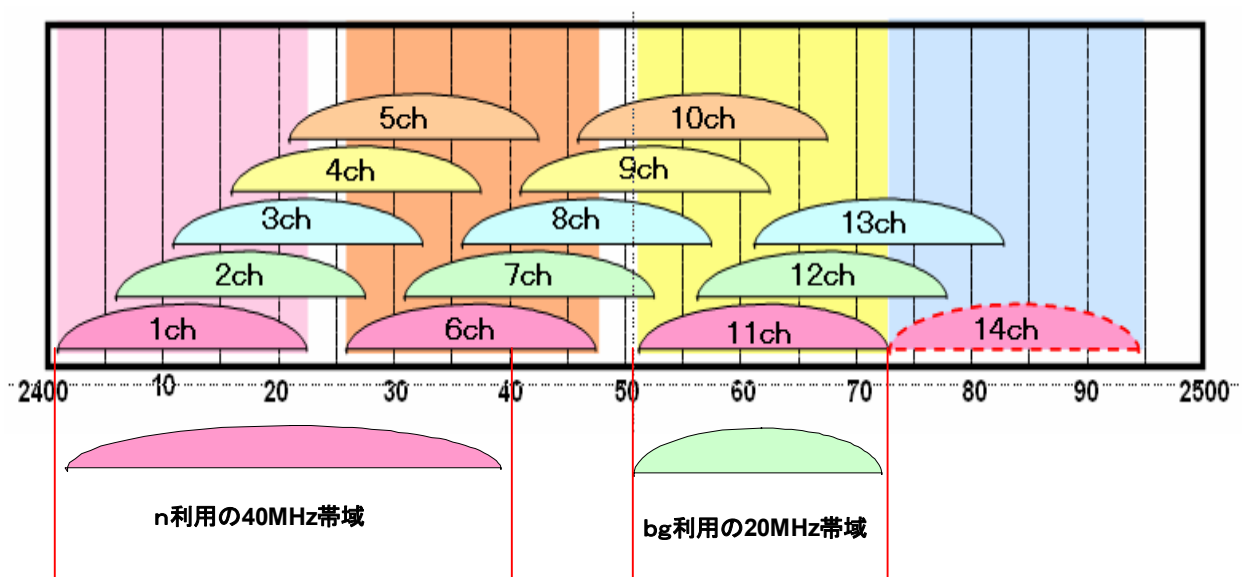
## ■DT-5300のabgの同時運用について

DT-5300のa対応機種ではabg全ての規格を利用可能とする設定ができます。またaからb/gへ、b/gからaにローミング可能ですが。しかしながらスキャン対象のチャンネルが増えるとローミング対象のサーチに時間がかかります。この為使用するチャンネルが絞り指定(11b/g:1・6・11、11aW52など)することをお勧めいたします。

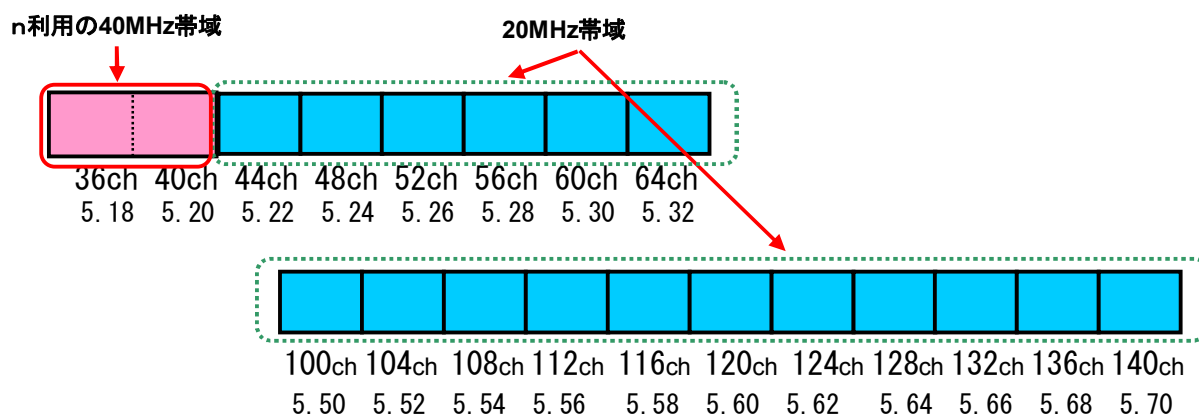
# 補足説明 「802.11nチャンネル」について

## ■n利用時の注意点

802.11nでは20MHz帯域で通信することが可能ですが、40MHz帯域を利用して通信を行うこともできます。(40MHz設定、チャンネルボンディング、デュアルチャンネル、ワイドチャンネルなどと呼ばれています。)2.4GHz帯で利用すると、40MHzの帯域を使用しますので、帯域が重ならないようにch設計を考慮しても、残り利用可能な20MHzのchは1つとなります。40MHzの指定方法によっては、他で利用するch帯域が重ならないように選択できない可能性もあります。このため2.4GHz帯域で802.11nの40MHzを利用する場合はch設計に注意が必要です。



同様に、5GHz帯で40MHzの帯域を利用した通信を行う場合にも、2ch分の帯域が必要になります。



# セキュリティの設定 固定WEP(付録)

※ご参考

【ASCIIコード一覧表】

上位 3ビット→ ↓ 下位 4ビット	0	1	2	3	4	5	6	7
0	NUL	DLE	SP	0	@	P	`	p
1	SOH	DC1	!	1	A	Q	a	q
2	STX	DC2	"	2	B	R	b	r
3	ETX	DC3	#	3	C	S	c	s
4	EOT	DC4	\$	4	D	T	d	t
5	ENQ	NAC	%	5	E	U	e	u
6	ACK	SYN	&	6	F	V	f	v
7	BEL	ETB	'	7	G	W	g	w
8	BS	CAN	(	8	H	X	h	x
9	HT	EM	)	9	I	Y	i	y
A	LF/NL	SUB	*	:	J	Z	j	z
B	VT	ESC	+	;	K	[	k	{
C	FF	FS	,	<	L	¥	l	
D	CR	GS	-	=	M	]	m	}
E	SO	RS	.	>	N	^	n	~
F	SI	US	/	?	O	_	o	DEL

※ご参考

WEP64bit ASCII: 5文字

16進数: 10文字

WEP128bit ASCII: 13文字

16進数: 26文字

例) WEP64bit ASCII「CaSio」を設定する場合

CaSio

436153696f

を入力します。

※ご参考

【キーインデックス対応表】

AP1131AG	DT-X7/X8/5200/5300/10/IT-300/900	DT-5100/870/950
Key 1	1	0
Key 2	2	1
Key 3	3	2
Key 4	4	3

# 制約事項・注意事項一覧

- ①、n規格を利用する場合は注意が必要です。古い端末では対応されていない場合が有ります、未対応のため通信障害が発生する可能性があります。
- ②、WPA/WPA2のミックスモードを利用する場合、セキュリティーが対応していない古い端末では接続できなくなる可能性があります。
- ③、APのLANケーブルが抜かれた・ネットワークに参加していない状態でAPの電源を入れ放置しないようにしてください。無線端末が接続して無線通信は行なえても有線通信が出来ず通信ができなくなる可能性があります。
- ④、DTIM初期値は大きな値を設定しないで下さい、初期値を短く設定してください。DTIMが長い場合、無通信状態から通信開始までのタイミングが遅くなる可能性があります。
- ⑤、Aironet Extention (CISCO社)は利用しないで下さい。シスコ社 独自の拡張となるため、対応されていない機種は通信障害が発生する可能性があります。
- ⑥、n規格の40MHz(倍速モード)利用についてはch干渉に注意が必要です。40MHzの帯域が広いいため他のchと干渉する可能性があります。
- ⑦、ファームウェアについてはカシオ評価のVerをご利用頂くよう推奨いたします。ファームが古いと不具合や改善箇所がある場合があります。また、新しい場合は新機能が含まれ対応していない端末との接続ができない場合があります。
- ⑧、AOSS,WPSの設定を行うと、古い端末では対応されていない場合が有り通信障害が発生する可能性があります。
- ⑨、DHCP、RADIUS機能を利用する場合はAP付属機能ではなくサーバのご利用をお勧めいたします。端末利用台数が多くなるとAPで処理しきれなくなる可能性があります。また、サーバの仕様・機能と異なり思わぬ障害が発生する可能性があります。
- ⑩、フィルター機能(MACアドレス、IPアドレス)を利用する場合は注意が必要です。フィルターを利用することで意図していない通信が阻害され思わぬ障害が発生する可能性があります。また、十分な管理(端末・AP)が必要となります。



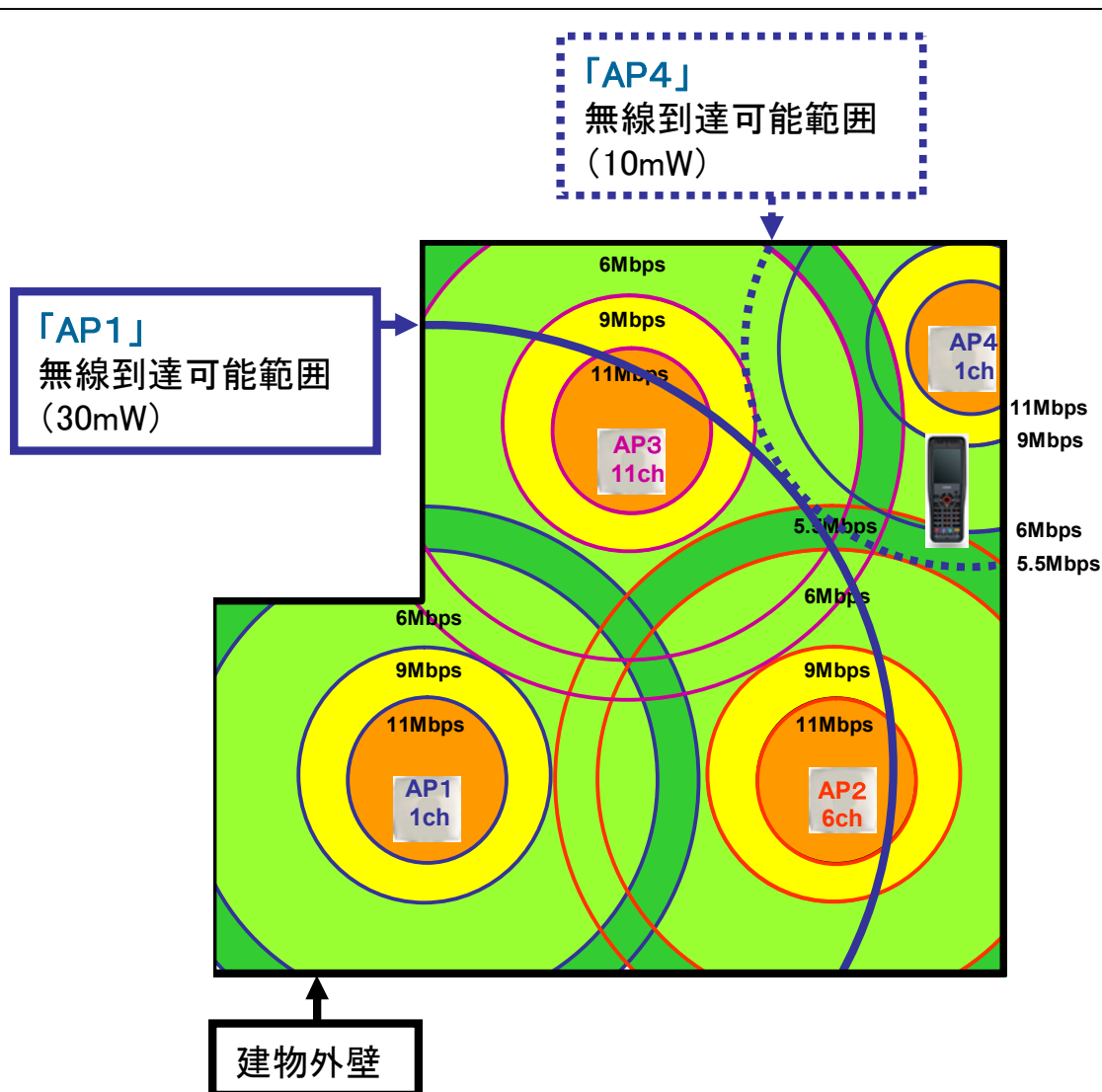
# 注意すべき運用・設定事項一覧

- ⑪、VOIP利用を行わない場合はQosの機能を無効とすることをお勧めいたします。特定通信が優先され端末通信が遅くなる可能性があります。
- ⑫、タイムアウト値(アプリケーションも含みます)は長くしないことをお勧めいたします。タイムアウトを長くすると次回リトライやエラーとなるまでの時間が長くなり結果、端末での待ち時間が長くなり運用に遅延が発生する可能性があります。
- ⑬、電波出力を自動出力とする場合は、意図しない電波環境となる可能性があります。
- ⑭、自動ch設定とする場合は、意図しないch環境となる可能性があります。
- ⑮、無線通信データレートの設定は初期値・全ての選択から不用意に制限しないことをお勧めします。低いレートの制限を行なうと通信できない場所が発生する可能性があります。
- ⑯、APの各種設定後は、HTをリセットしてからご使用下さい。リセットを行わないと、再接続・IP情報更新(IPアドレスの再取得)が出来なくなる場合があります。また、再設定後はHT⇒APに接続し、IP更新できるまで30～60秒かかる場合があります。
- ⑰、無線LANとIrDA(IO-BOX経由)での通信を同時に行うとIO-BOXの通信が中断されます。送信側のポートが干渉し合い、優先度の低い側が切断されたことによるもので仕様の為、制約とします。
- ⑱、まれに「CommunicationError」が発生する場合があります。カシオでのエージング中に「CommunicationError」が発生する場合がありますが、発生頻度も非常に低く、発生後もロックやファイルの破損等もなく通信を継続していることから、制約とします。
- ⑲、無線環境の構築には、「外部ノイズの影響」「最適なCH設計・設定」「業務として必要なスループットの見極め」「無線運用ポリシーの確立」「無線運用ポリシーに則った運用」などを考慮する必要があります。無線環境構築サービスを提供することも可能です、詳しくは、カシオ計算機の営業にお尋ね下さい。
- ⑳、HUBやルータなどの相性の問題も起き得る可能性もありますので、十分動作確認を行ってから設置してください。

## 【ご参考】無線セル設計に関して

### 【APの設定】

Ciscoのアクセスポイントは、出力を設定することによりセルを小さくすることが可能です。



右上の端末地点で「AP4」をデフォルトの出力「30mW」で設定すると、「AP1」の無線到達範囲と被ってしまうために、干渉してしまいます。APで無線の出力を設定することにより、建物全域をカバーする事が可能です。上記の設定は、干渉電波(ノイズ)があり無線チャンネルを3～4チャンネル設計できない場合に有効です。

※上記の設定は、理論上の動作になります。実際の環境では、反射などによるマルチパスにより、上記のように設計できない場合もあります。実地での検証を行ってください。

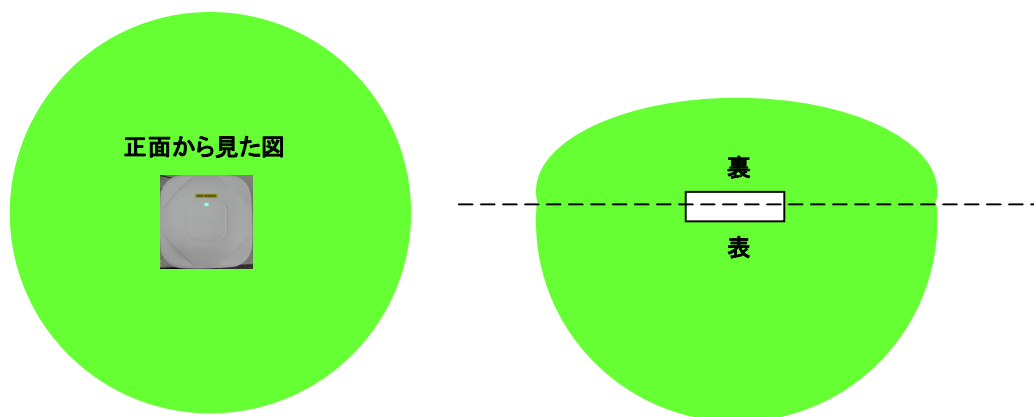


## 【ご参考】アンテナ特性と取り付け方法

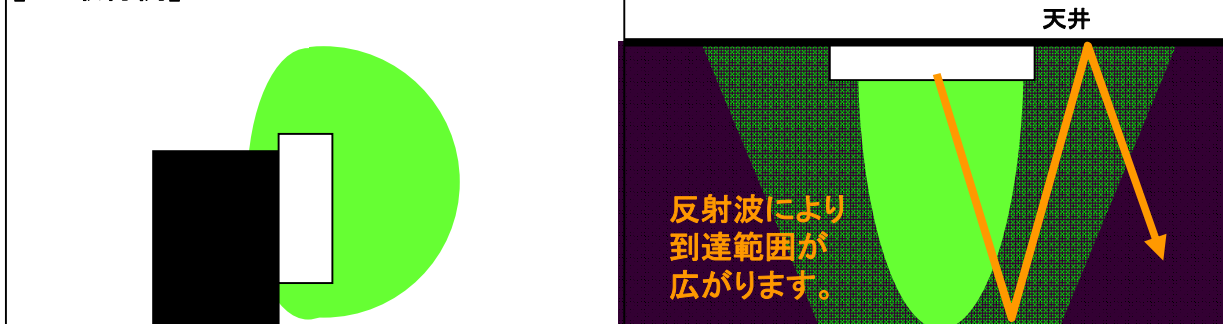
### 【AIR-SAP1602I アンテナ特性】

全方向アンテナが搭載されていますが、裏面方向は比較的感度が落ちる特性となっています。  
※下にアンテナ特性のイメージ図を示します。

正確には、Cisco社のWEBサイトに掲載されているアンテナリファレンスガイドをご覧ください。

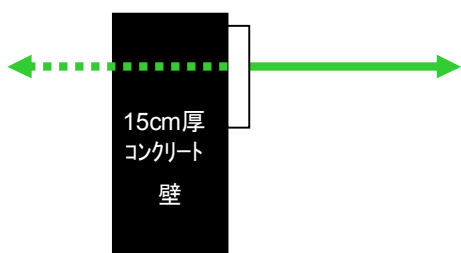


### 【AP取付例】



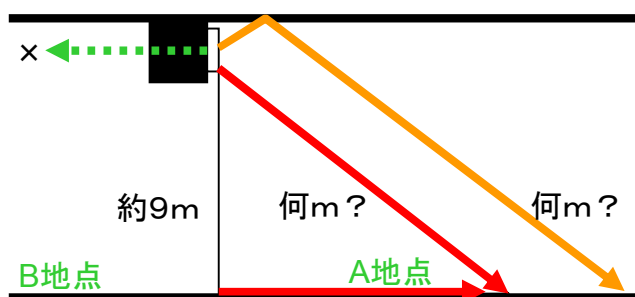
### 【注意を要する取り付け方法】

#### 『コンクリートに取り付けた場合』



形状、位置により変わりますが、15cm厚のコンクリート壁をはさむと11dB～19dBの減衰との測定例があるようです。  
(インターネット検索からの情報)  
この値は鉄筋量などコンクリート壁の構造により変動するため参考としてください。

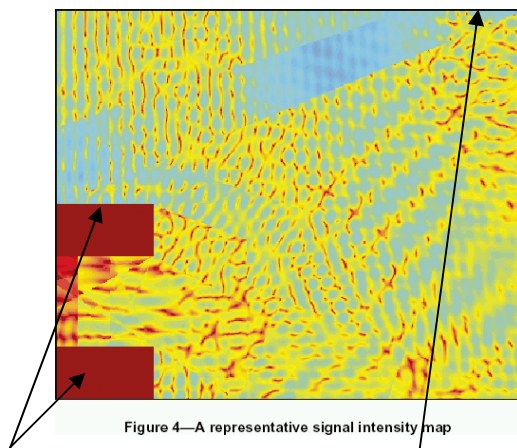
#### 『左記状態で高い天井に取り付けた場合』



- ①、通常、屋内での無線LAN運用距離は約30mとされています。
- ②、地上で使用する際には、ダイレクトパスではなくマルチパス(反射波)にて使用している場合が多いと考えられます。  
(より大きい範囲で輻輳を起こす可能性があります)
- ③、梁の片側に取り付けられたAPの電波は反対側には到達していないと考えられます。  
よって、A地点とB地点で同一APに接続している場合に電波強度・質は異なります。

## 【ご参考】技術資料～無線LANの環境は常に変化しています～

### 【無線LANの環境は常に変化しています】



鉄製の机

ドア

左図 (Figure4) は2.4GHzの電波がある室内において、反射波の影響を受けて、電波の強弱が発生している様子を視覚的に表したものです。この図は静的に捕らえた電波強度ですが、室内にある物体の移動により動的に変化します。

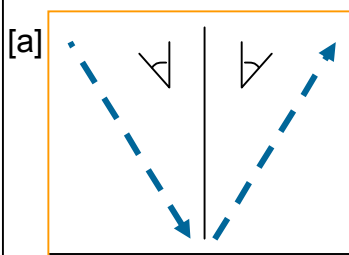
ANSI/IEEE Std 802.11, 1999 Editionによると、同じ位置にいても電波強度は動的に絶えず変化をしている、とあります。(青→黄→赤と弱くなります。)

(ANSI/IEEE Std 802.11, 1999 Editionより抜粋)

「2.4Ghz帯という特性上、10数センチ単位※1の波で電波の強い部分、弱い部分が交互にあるために、APIに近くても必ずしも近くのAPIにつながりっぱなしになるわけではなく遠くのAPIにつながる場合もあり、その為、交互にAPIにローミングする可能性がある」

※1: 約30万Km(電波長) ÷ 2.4Ghz = 約12.5cm

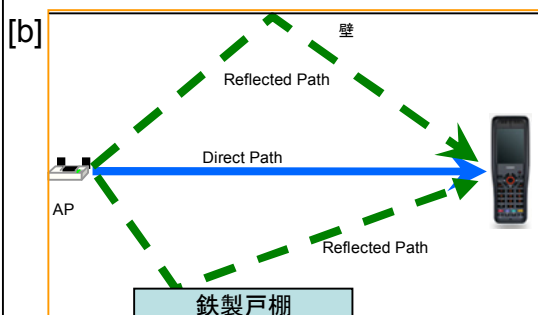
### 【反射波の補足】



#### 《1》Reflection

電波物体に当たると入射角と同じ角度で反射します。反射に関しては下記3つの物体で影響が異なります。

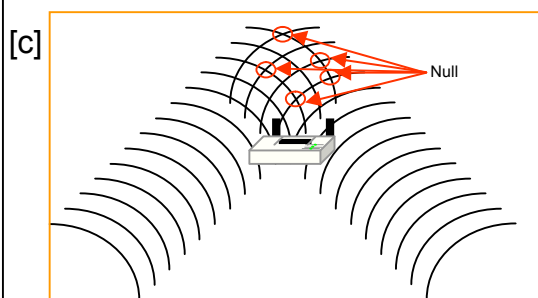
- ・コンクリート: 無線エネルギーが吸収・熱変換されるため反射した無線エネルギーは弱くなります。
- ・鉄板: ほぼ同等の無線エネルギーが反射します。
- ・水分: 無線エネルギーは吸収され、反射しません。



#### 《2》MULTIPATH

APからSTAに信号を送る場合、最初に届くのは「Direct Path」になります。その後、壁やパーティション等から反射した「Reflected Path」が届きます。その結果、STAは同じ信号を3度受けることになります。STA側で「Direct Path」と「Reflected Path」の判別がつかなければAP—STA間のデータデータ転送は化ける可能性もあります。

MULTIPATHにより悪影響を受ける場合も多いですが、MULTIPATHのお陰で、電波が届く場合もあります。



異なるAPからの反射波が横切るMulti Pathには[c]のような問題もあります。反射波同士が交わった「山」と「谷」では、お互いの信号を打ち消し合います。

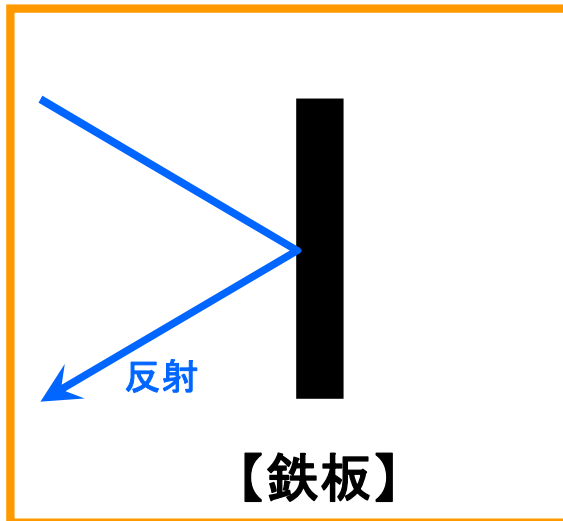
(「Nulls」や「Loss of Signal」になります。)

「Nulls」のポイントでは明確な障害物が無い場合でも無線の弱い所や隙間が存在する部屋の中の「Dead Spot」になります。

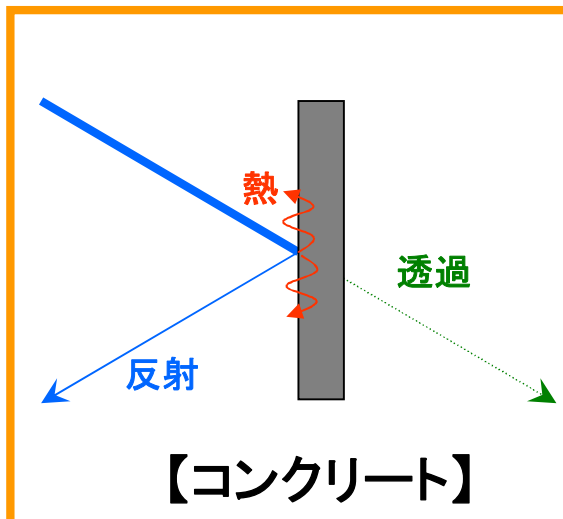
図C: 反射波同士が交わった「山」と「谷」の部分が「Nulls」になります。

## 【ご参考】技術資料～反射～

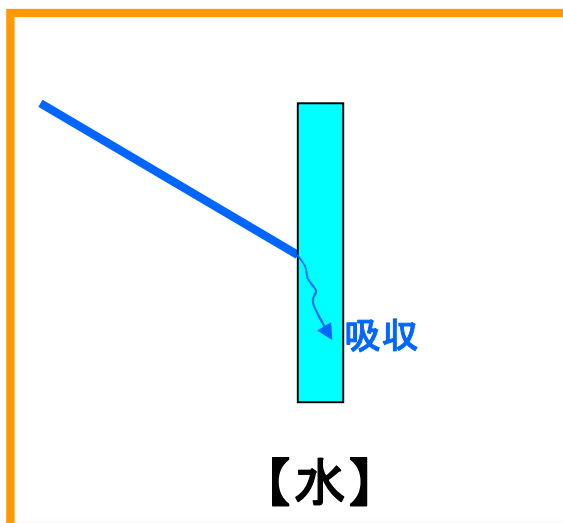
反射に関しては下記の3つの物体で影響が異なります。



【鉄板】  
ほぼ同等の無線エネルギーが  
反射します。



【コンクリート】  
無線エネルギーが吸収・透過・  
熱変換されるため反射した  
無線エネルギーは弱くなります。



【水分】  
無線エネルギーは吸収され、  
反射しません。  
人間の体は水分が非常に多い  
ために、動線によっては、  
影響を受けます。

## 【ご案内】無線LANサイトサーベイについて

---

無線LANを安定して運用するために、事前に運用環境の調査(サイトサーベイ)を行う事をお勧めします。

カシオ計算機では、無線LANの環境を構築する際にあたって、無線サイト調査サービス(サイトサーベイ)を行っています。

料金などに関しては、担当営業にご確認ください。