K06 立松

・FON ってなに?

FON は世界最大の WiFi コミュニティです。誰もが「世界中どこからでもインターネット に無料で接続したい!」という望みを持っているはずです。そのようなメンバーが助け合 って WiFi を広めて行こう!ということをコンセプトに私たちは活動しています。 参加は簡単!FON 取り扱い店で La Fonera を購入して接続してスタートするだけ! (公式サイトより)

という FON。ルータの安さも影響してか、近年、世界的に大流行です。

FON のルータ「ラ・フォネラ」のファームウェアは OpenWRT という Linux ベースの OS です。人気とともに、ハックする情報もネットに出回ってきました。それらを参考に して、とりあえず、「ラ・フォネラ」に SSH で入るログインしていじくる方法をご紹介し ましょう。

まずは「ラ・フォネラ」を買わないとどうにもなりません。大須とかで売ってますので、 買ってきましょう。筆者は、大須のツクモで 1000 円で入手しました。wk t k しながら お家に帰ったら、さっそくいじってみましょう。

2.繋げてみる

FON の電源を入れ、FON の無線に繋げます。キーは、本体裏に記載してあるはずです。

次に、http://192.168.10.1/にアクセスしましょう。 FONの設定画面が現れるでしょう。

ファームウェアのバージョンを確認します。 もし、バージョンが 0.7.1r2 以降だと、ダウングレー ドが必要になります。やりかたは次のとおりにやって ください:

1.LAN ケーブルを抜く。

2.裏のリセットボタンを1分間押し続ける。

3.電源を切って再起動。

4.FON の設定画面にアクセスして、バージョンが 0.7.1r1 になっていることを確認してください。



これがラ・フォネラだ。

11911		
ファームウェア バージョン:	0.7.1 c1	
MIE イノダーネット技術	The second s	
F WIFI INTN'L 7.	PET FARM 1	
ゲートウェイアドレス:	THE FARLE D	
DNSサーバー:	211.134.41.129	
WIFi的定		
パブリックSSID:	FORLASHSHIM	
プライベートSSID:	MyPlace	
暗号化:	minut	1
IPTFLA:	101.168.10.1	

まずは Web 管理画面へ。

3.ハックする

さて、いよいよハックします。HTML ファイルを、2 つ用意しましょう。

<html><body>
<form method="post" action="http://192.168.10.1/cgi-bin/webif/connection.s
h " enctype="multipart/form-data">
<input name="username" value="\$(/usr/sbin/iptables -1 INPUT 1 -p tcp --dpo
rt 22 -j ACCEPT)" size="68" >
<input type="submit" name="submit" value="Submit" onClick="{this.form.wifi
mode.value='";' + this.form.wifimode.value +';"'}" />
</form></body></html>

これを、1.html として保存します。 次に、

<html><body> <form method="post" action="http://192.168.10.1/cgi-bin/webif/connec tion.sh " enctype="multipart/form-data"> <input name="username" value="\$(/etc/init.d/dropbear)" size="68" > <input type="submit" name="submit" value="Submit" onClick="{this.fo rm.wifimode.value='";' + this.form.wifimode.value +';"'}" /> </form></body></html>

これを、2.html として保存しましょう。

まず、最初に 1.html を開いて、submit をクリックします。Web 管理画面が開いて、 「設定を保存しました」っぽいメッセージが表示されれば成功です。2.html も同じ要領で やってしまいましょう。(もし、このときにパスワード等を要求されたら、両方とも admin を入力すればおk。)

2つとも成功したら、いよいよログインします。 TeraTerm や Poderosa などのターミナルソフトで、

- **192.168.10.1** に、**ID**: root、**PASS**: admin で入りましょう。 右のような画面になったら成功です。
 - 次回からも SSH でアクセスできるように設定をしましょう。
 - /etc/init.d/下にある dropbear の名前を、S50 dropbear に 変更します。

	-	1000		
3 1 192.168.10.1				
usySox v1.1.3 (2006.11.21-19:49+0	000) Built-in s	shell (ash	
inter 'help' for	a list of built-in	a commands.		
!!				
! -				
	Wernion 0.2.1 res	. 1)		
Tozera Firmware	(Version 0.7.1 re			
Fonera Firmware * Based on Ope	n (Version 0.7.1 re	7 1)		
Fonera Firmware * * Based on Ope * Fowered by F	e (Version 0.7.1 re enWrt - http://open YON - http://www.fo	vi)		
Fonera Firmware Based on Ope Powered by F	nWrt - http://open NWrt - http://www.for	/ 1)		
Fonera Firmware Based on Ope Powered by P cost8OpenWrt:-#	<pre>(Version 0.7.1 ret mWrt - http://open/ CON = http://www.for 11</pre>	v 1)		
Fonera Firmware Based on Ope Fowered by F cost8OpenWrt:-# ash: 11: not fo	<pre>(Version 0.7.1 ret enWrt - http://open CON = http://www.for 11 pund</pre>	v 1)		
Fonera Firmware * Based on Ope * Powered by F cost8OpenWrt:-# ash: 11: not fc cost8OpenWrt:-#	<pre>v (Version 0.7.1 ret mWrt - http://open NON - http://www.for 11 11 12 13 13</pre>	v 1)		
Forera Firmware * Based on Ope * Powered by P ************************************	<pre>(Version 0.7.1 ret mWrt - http://open YGW - http://www.fo 11 jund js hostapd.conf</pre>	resolv.com		
<pre>"" Fonera Firmware " Based on Ope " Fowered by F cot8OpenWrt:-# ash: 11: not fo cot8OpenWrt:-# bop.leases</pre>	<pre>v (Verpion 0.7.1 ret nWrt - http://open f0W - http://www.for und is hostapd.conf astwork.confin</pre>	resolv.cond		
<pre></pre>	<pre>(Version 0.7.1 re- nWRt - http://oww.for - http://www.for und is hostapd.conf is aetwork-config cd /</pre>	resolv.conf		
<pre></pre>	<pre>t (Version 0.7.1 ref nWrt - http://open 10 11 bund 12 bostapd.conf network-config cd / 13</pre>	resolv.cond		
<pre> Topera firmware Based on Opp Powered by f Towered by f toot80penBrt1-# ont80penBrt1-# ont1g.tar hrp.leases cot80penBrt1-# cot80penBrt1/# </pre>	<pre>t (Version 0.7.1 ret mWrt - http://open f0W = http://www.foi 11 12 bostapd.conf network-config cd / 12</pre>	resolv.cond		
Tourca firmware * Based on Ope * Powered by f ooot8OpenWrt:-# asb: l: not fo oot8OpenWrt:-# oot8OpenWrt:-# oot8OpenWrt:-# oot8OpenWrt:-#	<pre>t (Version 0.7.1 ret neWert - http://opens CW - http://www.for 11 11 12 13 16 ostapd.conf network-config cd / 13</pre>	resolv.com		

・次に、/etc/firewall.user を vi で開いて、22 番ポートをいじ くっている箇所(「iptables ほにゃらら 22」っていうところ)が二箇所あるので、コメ ントアウトを外しておきましょう。

これで完成です。あとは、ラ・フォネラを好きなように調教するだけです。 物足りないという人は、http://fon-wiki.maniado.com/ FON まとめ Wiki を見ましょう。

ステキな FON ライフを堪能してください。では、ごきげんよう!