Confidential

JANOG44 LT
不正APでオフィスの業務が邪魔されたときの顛末

株式会社ポケモン
開発事業本部システム部
開発事業本部 開発プロデュース部
テクニカルディレクター インフラエンジニア
関 剛

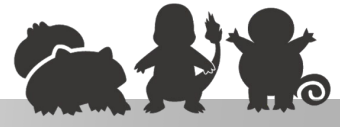
2019 年 07 月 26 日

All Rights Reserved, Copyright. The Pokémon Company

自己紹介

株式会社ポケモン
せき　たけし

社内IT担当

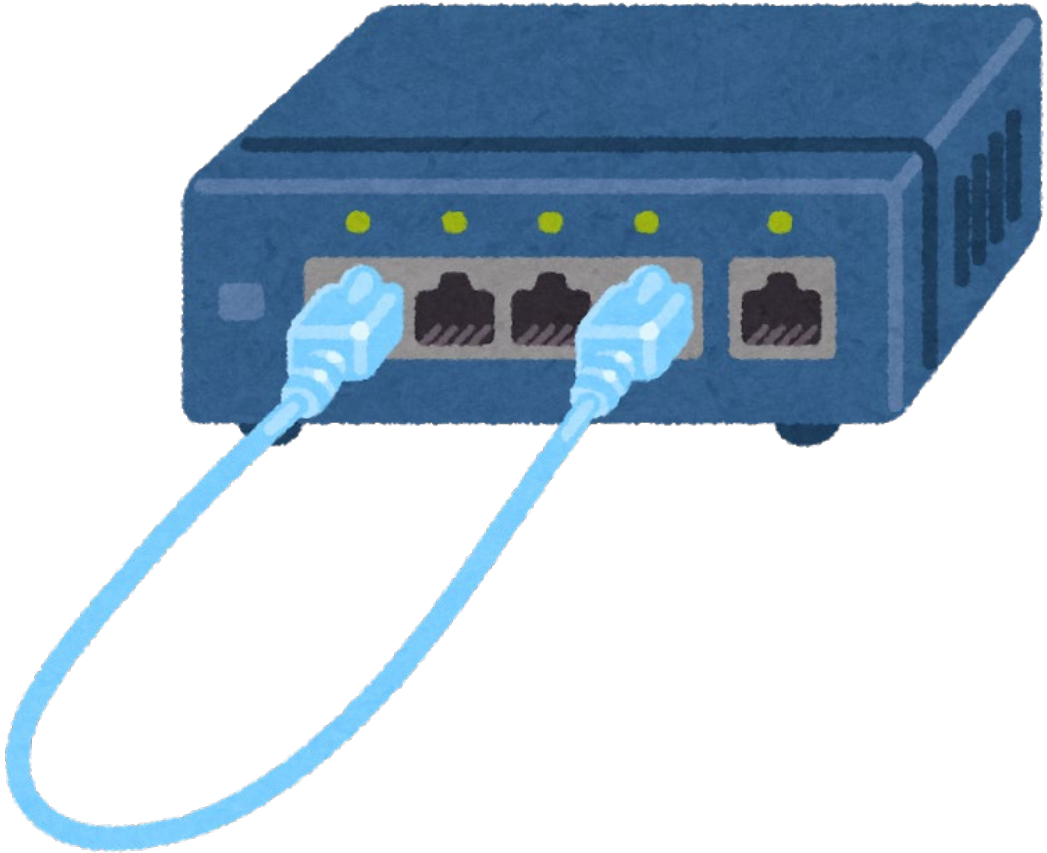


全然関係ないけど、
今週 ある登壇控室で

LAN-S4A
LAN/CAT5E
LAN/CAT5E

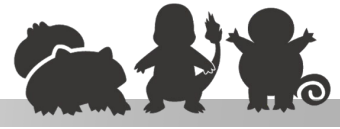
LAN-S4A
LAN/CAT5E
LAN/CAT5E

LAN-S4A
LAN/CAT5E
LAN/CAT5E



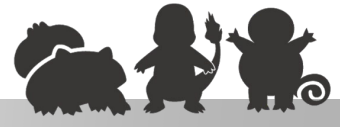
たぶん大丈夫
(知らない)

不正APでオフィスの業務が邪魔されたときの顛末(本題)



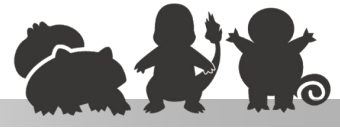
ある社員：
「Wi-Fi つながらない」

ぼく：
「そんなバカな」



ある社員：
「Wi-Fi つながらない」(真顔)

ぼく：
「調べます」(端末側だろ)



他の社員：
「Wi-Fi つながらない」(迫真)

ぼく：
「えっ、マジかよ」(設備?)

Cisco 5520 ワイヤレス コントローラ

Cisco Aironet 2800 シリーズ アクセス ポイント

そこそこお金かけた
システム入れている

ぼく：
「そんなバカな」(真顔)

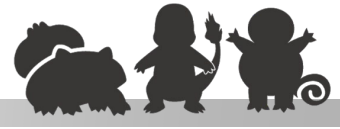
@tpc-tseki @tpc-yamashita （@helpdesk ）
連日おそれいります、昨日のPokemon[redacted]への接続不要ですが、本日も発生してしまっているようです。（30分ほど前から接続できません）
おそれいりますが、ご確認いただけますでしょうか。

88 replies Last reply 6 months ago

Last reply 6 months ago

(実は解決に半年かかった)

調査する

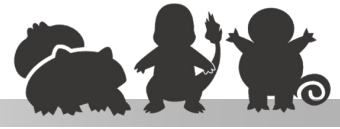


SSID: Pokemon[redacted]
プロトコル: 802.11ac
セキュリティの種類: WPA2-パーソナル
ネットワーク帯域: 5 GHz
ネットワーク チャネル: 100
IPv4 アドレス: 172.31.233.97
IPv4 DNS サーバー: 172.16.210.101
172.16.210.102
製造元: Intel Corporation
説明: Intel(R) Dual Band Wireless-AC 8260
ドライバーのバージョン: 20.60.0.7
物理アドレス (MAC): F8-94-C2-19-68-83

↑ちゃんとつながるとき

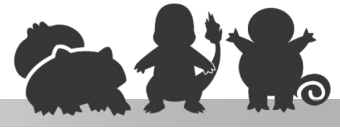
★確認★

- 当該 SSID は 5GHz のみ
- 当該 SSID は 11a/ac のみ
- IPアドレス172.31.0.0/16



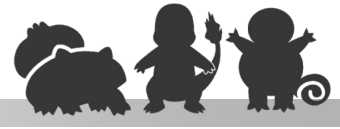
SSID: Pokemon[redacted]
プロトコル: 802.11ac
セキュリティの種類: WPA2-パーソナル
ネットワーク帯域: 5 GHz
ネットワーク チャネル: 100
IPv4 アドレス: 172.31.233.97
IPv4 DNS サーバー: 172.16.210.101
172.16.210.102
製造元: Intel Corporation
説明: Intel(R) Dual Band Wireless-AC 8260
ドライバーのバージョン: 20.60.0.7
物理アドレス (MAC): F8-94-C2-19-68-83

↑ちゃんとつながるとき



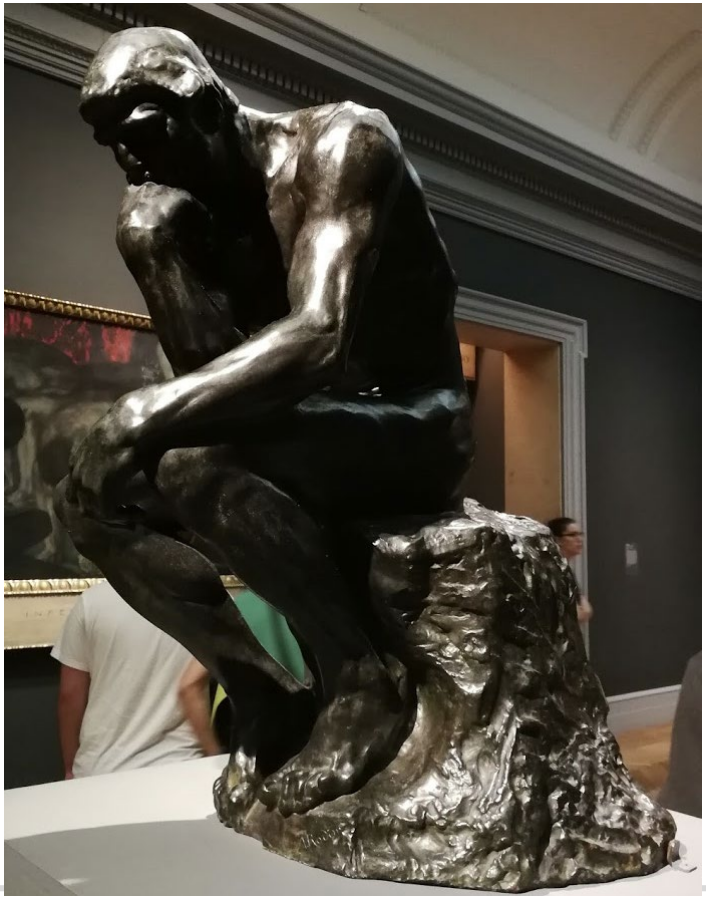
SSID: Pokemon[redacted]
プロトコル: 802.11n
セキュリティの種類: WPA2-パーソナル
ネットワーク帯域: 2.4 GHz
ネットワーク チャネル: 1
IPv4 アドレス: 192.168.137.19
IPv4 DNS サーバー: 192.168.137.1
製造元: Intel Corporation
説明: Intel(R) Dual Band Wireless-AC 8260
ドライバーのバージョン: 20.60.0.7
物理アドレス (MAC): F8-94-C2-19-68-83

↑ダメなとき

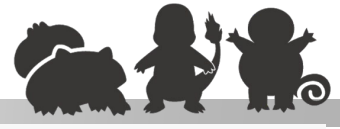


```
SSID:     Pokemon[redacted]
プロトコル:    802.11n
セキュリティの種類:     WPA2-パーソナル
ネットワーク帯域:    2.4 GHz
ネットワーク チャネル:     1
IPv4 アドレス:    192.168.137.19
IPv4 DNS サーバー:     192.168.137.1
製造元:     Intel Corporation
説明:     Intel(R) Dual Band Wireless-AC 8260
ドライバーのバージョン:     20.60.0.7
物理アドレス (MAC):     F8-94-C2-19-68-83
```

2.4Ghz? 11n? 192.168.137.19? なんだこれ?



★仮説★
誰かが野良 AP 立ててる



SEKI Takeshi / 関 剛 1:06 PM

@here

★★ モバイルルータ確認のお願い ★★

モバイルルータ および PC / スマホの **インターネット共有(テザリング)** OFF の確認のお願いです。

8F / 38F オフィス内はモバイルルータの使用・テザリングは禁止です

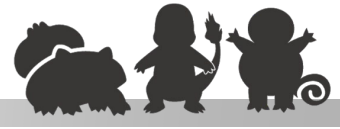
六本木拠点 8F / 38F においては今すぐ

- **モバイルルータの電源 OFF**
- **テザリングの OFF**

となっていることを確認してください。

優しく呼びかけた

★大きな謎★



当該 SSID の PSK を
一般社員は知らない

↓

SSID と PSK 一致しないと
野良 AP に繋がらないはず

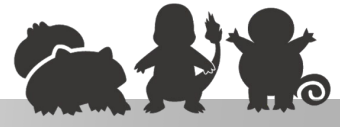
PSK が割れてる?

陰謀説?

Wi-Fiコントローラ・AP の
ファームウエアとか上げた

↓

改善なし
(逆にいろいろハマった)



ある社員：
「またWi-Fi つながらない」

Wi-Fi アナライザで見る

SEKI Takeshi / 関 剛 11:55 AM

8F に

WiFi_Explorer_-_Scanning.jpg

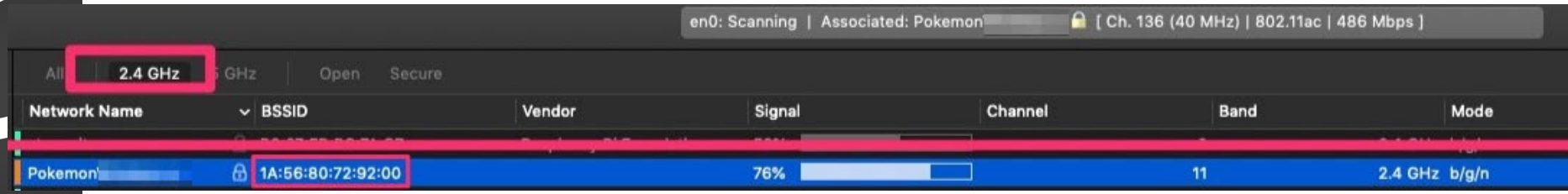
PokemonWireless-a を 2.4Gz で吹いてる AP(?) が一つあるぞ

「↓」矢印は関係ないです。

Pinned by you

当該 AP **1A:56:80:72:92:00**

やっぱり野良APがいる


en0: Scanning | Associated: Pokemon
[Ch. 136 (40 MHz) | 802.11ac | 486 Mbps]
All
2.4 GHz
5 GHz
Open
Secure
Network Name
BSSID
Vendor
Signal
Channel
Band
Mode
Pokemon
1A:56:80:72:92:00
76%
11
2.4 GHz
b/g/n

野良APのMACアドレスも
分かった

↓

すぐ解決できる!!

MAC Address Lookup

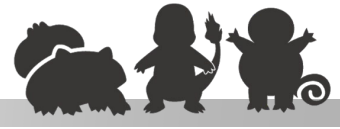
Enter any MAC address, OUI, or IAB below to lookup the manufacturer, location, and more

1A:56:80:72:92:00

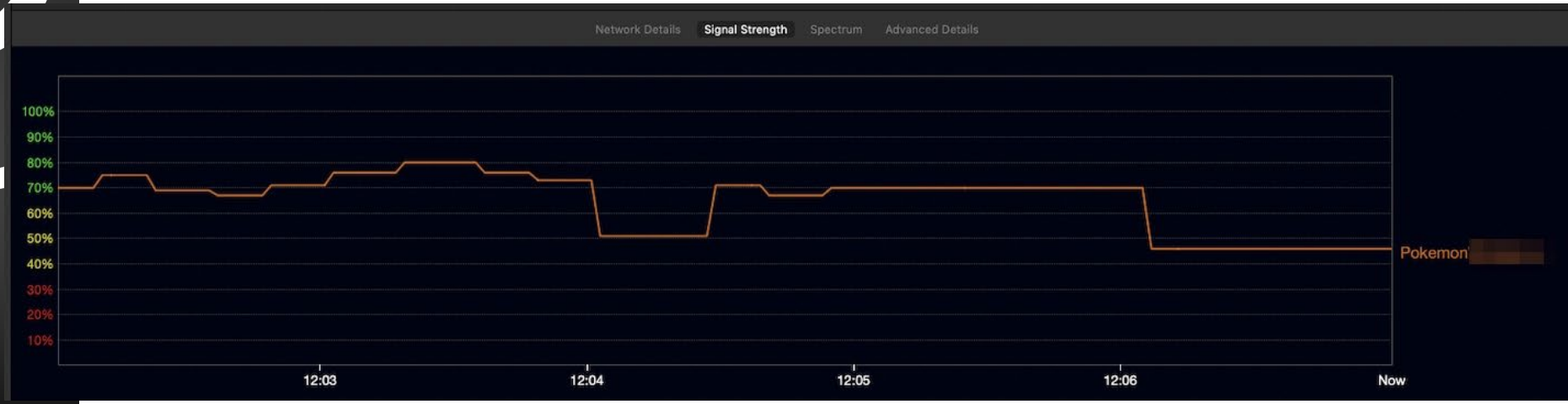
Where can I find my MAC Address?

MAC Address Details

Company	No Vendor Exists
Address Range	-
Type	IEEE



がーん。わからん。


Network Details
Signal Strength
Spectrum
Advanced Details
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
12:03
12:04
12:05
12:06
Now
Pokemon

アナライザ見ながら
オフィスを歩き回った

↓

だいたいのエリアは判明

野良 AP を監視

Cisco 5520 Wireless Controller

不正APの詳細

MACアドレス
1a:56:80:72:92:00

状態
アラート

タイプ	AP
有線ネットワーク上で不正	No
初回報告日時	Mon Jun 17 11:03:21 2019
最終報告日時	Mon Jun 17 12:30:03 2019
クラス	悪意のある
分類変更者	Manual
状態変更者	Manual
手動で封じ込め	No
更新クラス	悪意のある

この不正APに関連付けられているクライアント

MACアドレス	無線タイプ
28:16:a8:62:b3:71	802.11n2.4G

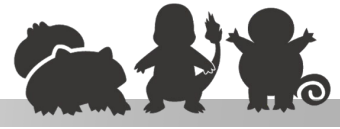
1 1 10 ページあたりの項目数

SEKI Takeshi / 関 剛 11:14 PM

あれ、

image.png

今(23:14)見たら不正 AP いない。



SEKI Takeshi / 関 剛 12:28 PM

image.png

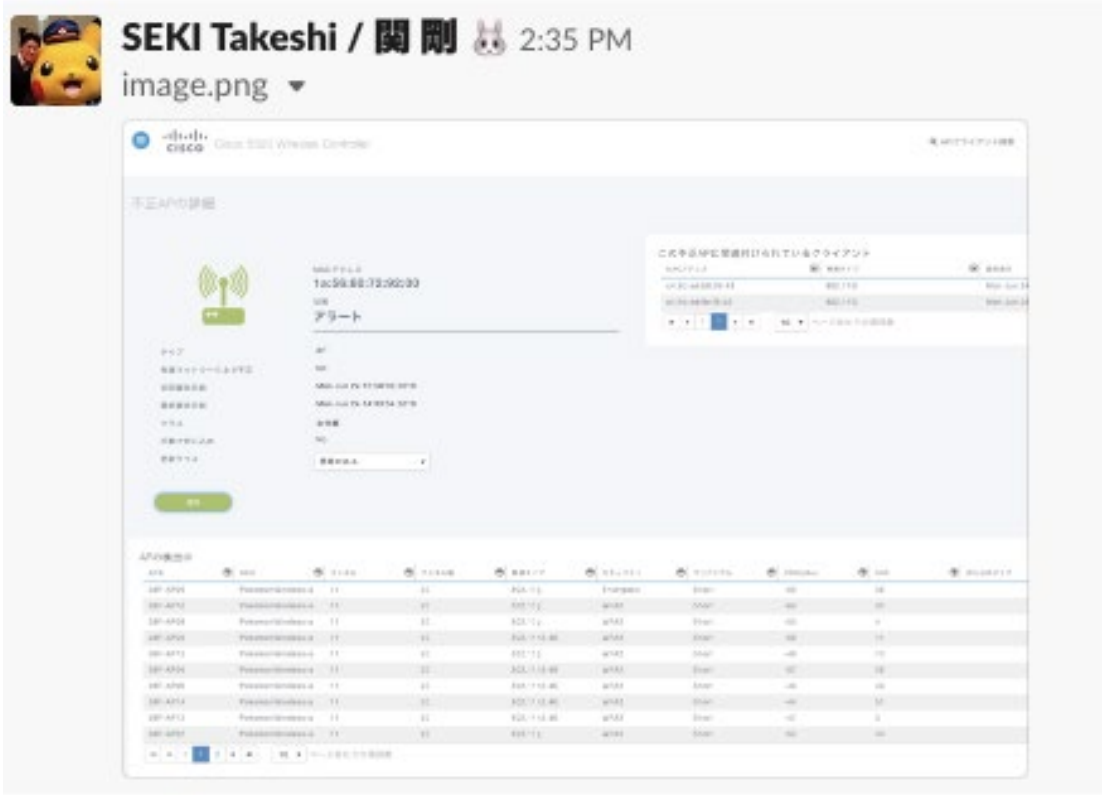
初回報告日時Tue Jun 18 10:59:42 2019
最終報告日時Tue Jun 18 12:28:20 2019

今日の 10:59 から再登場

野良APが出勤・退勤する
(たまにお昼も行くみたい)

2019/06/24
そしてついに…

事態は急展開する



38F にいるぞ

普段8Fオフィスの野良APが 38F オフィスに移動した!!

38Fを捜索すると…

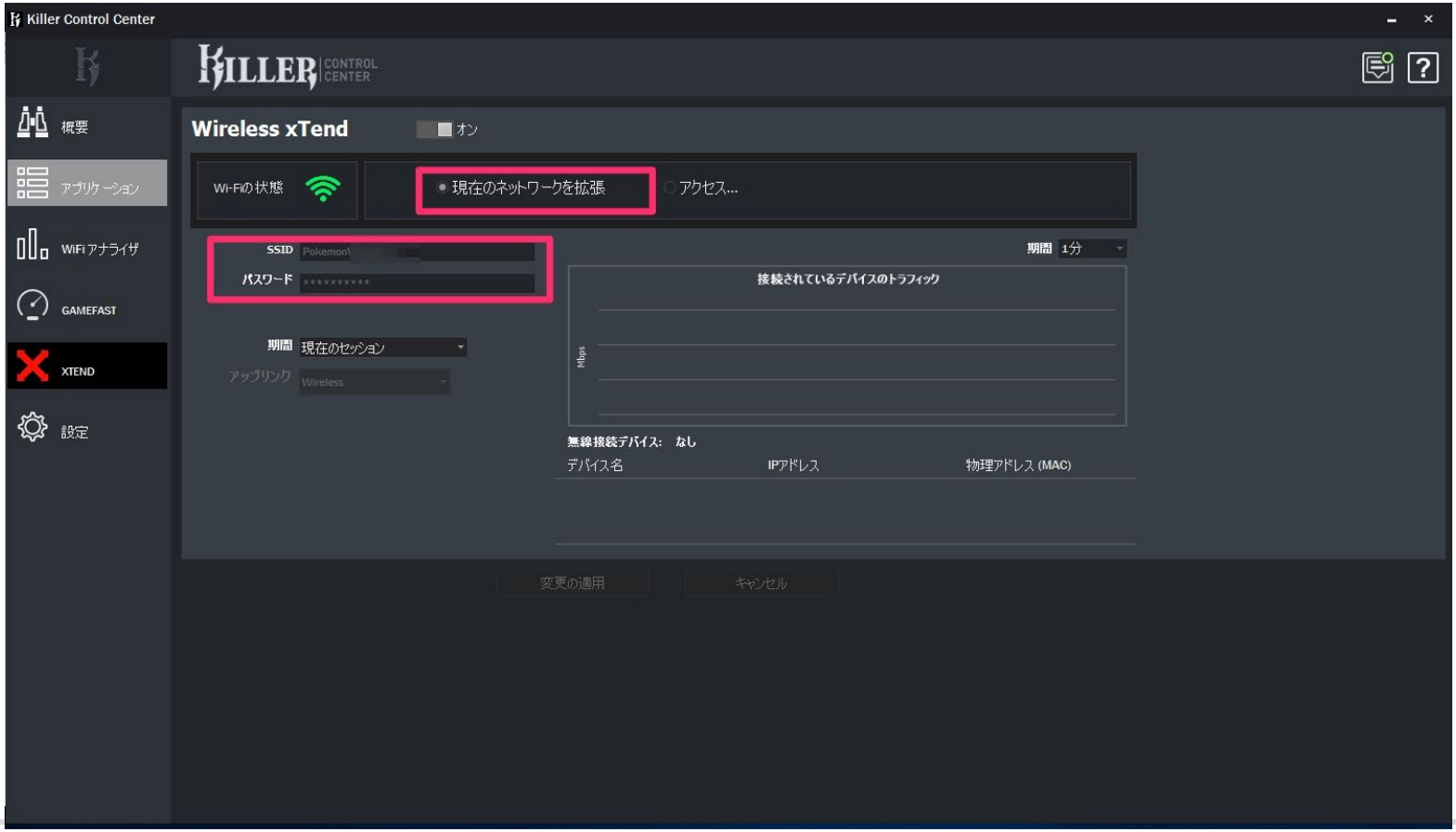
普段見かけないスタッフAと見慣れないPC が…

ALIENWARE™

あやしい

というか、こいつだ!

まさにエイリアン


Killer Control Center
KILLER CONTROL CENTER
概要
アプリケーション
WiFi アナライザ
GAMEFAST
XTEND
設定
Wireless xTend
オン
Wi-Fiの状態
現在のネットワークを拡張
アクセス...
SSID
Pokemon\
パスワード
****
期間
現在のセッション
アップリンク
Wireless
期間
1分
接続されているデバイスのトラフィック
Mbps
無線接続デバイス: なし
デバイス名
IPアドレス
物理アドレス (MAC)
変更の適用
キャンセル

Killer Control Center

勝手にネットワークを拡張してる!!

まさに殺し屋

KILLER NETWORKING

SUPERCHARGE YOUR COMPUTER WITH KILLER XTEND

Killer xTend adds powerful network capabilities to your computer by integrating a network switch and providing Wi-Fi extension features. Not only will Killer xTend keep your devices connected with a strong, powerful network connection, it will also prioritize the high priority traffic on your Killer enabled PC above the other home traffic that is being handled by Killer xTend.

https://www.killernetworking.com/technologies/killer-xtend/

なんとも言えない気持ち

Killer Wireless xTend

このアプリを
アンインストールして解決

めでたし。めでたし。