H3C WLAN WIPS設定と検証

検知する攻撃一覧

攻撃の検出(Detection)

- フラッドアタック検出
- 不正な形式のパケット検出
- スプーフィング攻撃の検出
- 弱いIV検出
- オメルタ攻撃検出
- ブロードキャストアソシエーション解除/認証解除攻撃の検出
- 40 MHz帯域幅モードがディセーブルになっているクライアントでの検出
- 省電力攻撃の検出
- 禁止チャネルの検出
- ソフトAP検出
- Windowsブリッジ検出
- 暗号化されていないデバイスの検出
- ホットスポット攻撃の検出
- AP偽装攻撃検出(社内と同じSSIDが近くに置かれていたらそのAPからのbcon送信間隔から外部とみなして管理者に通知)
- HT-グリーンフィールドAP検出
- ハニーポットAP検出
- MITM攻撃検出
- ワイヤレスブリッジ検出
- アソシエーション/再アソシエーションDoS攻撃の検出
- APフラッド攻撃検出
- デバイス侵入攻撃検出

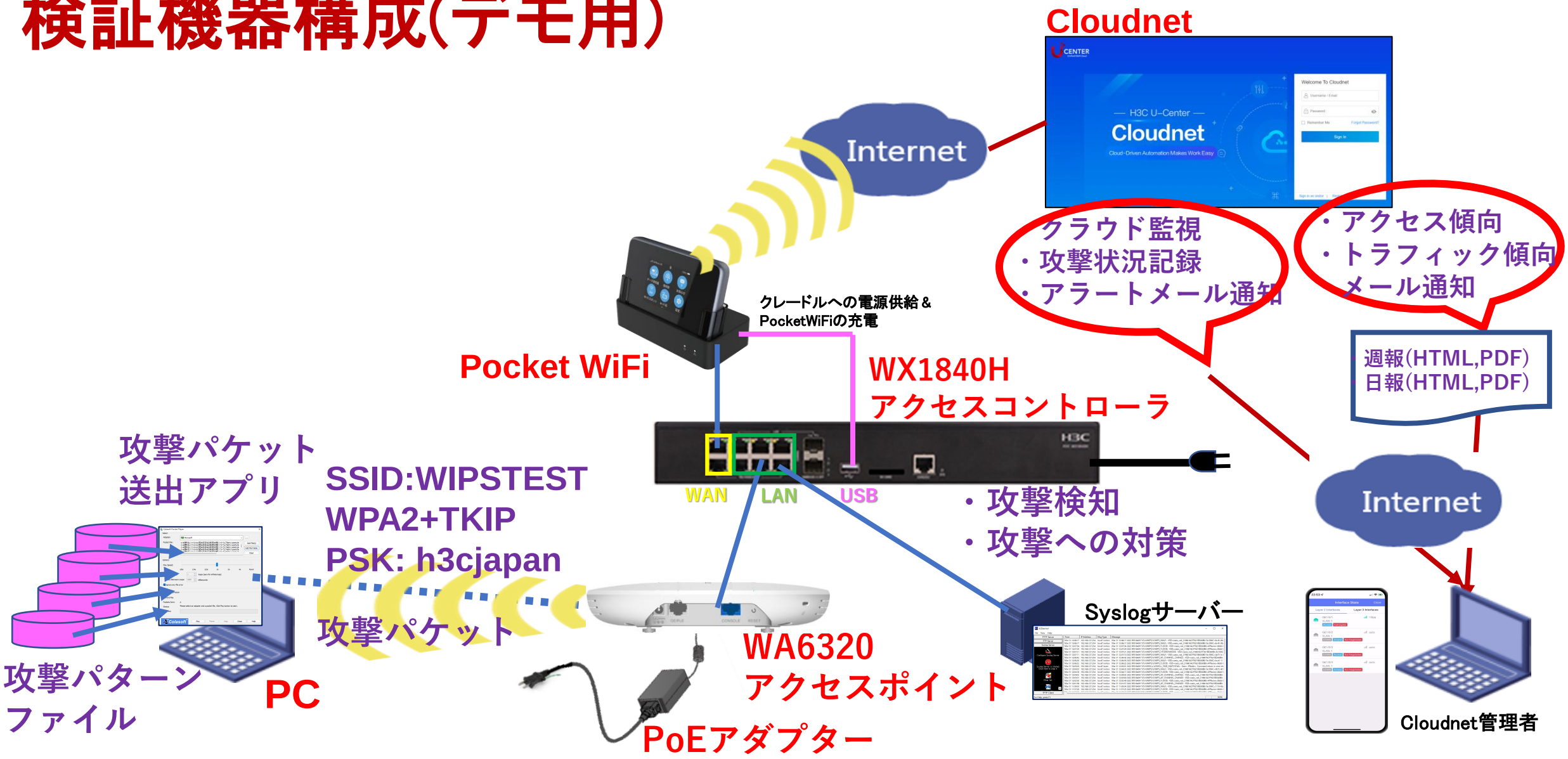
シグニチャベースの攻撃検出(Signature)

デバイスの分類(Classification)

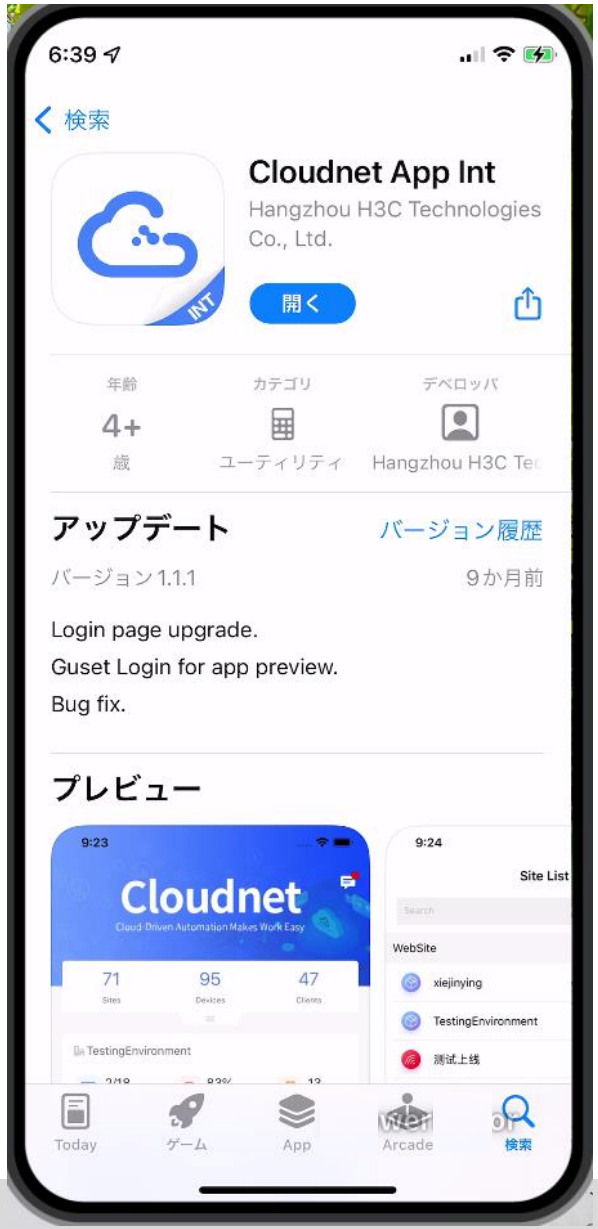
- AP分類
- クライアントの分類

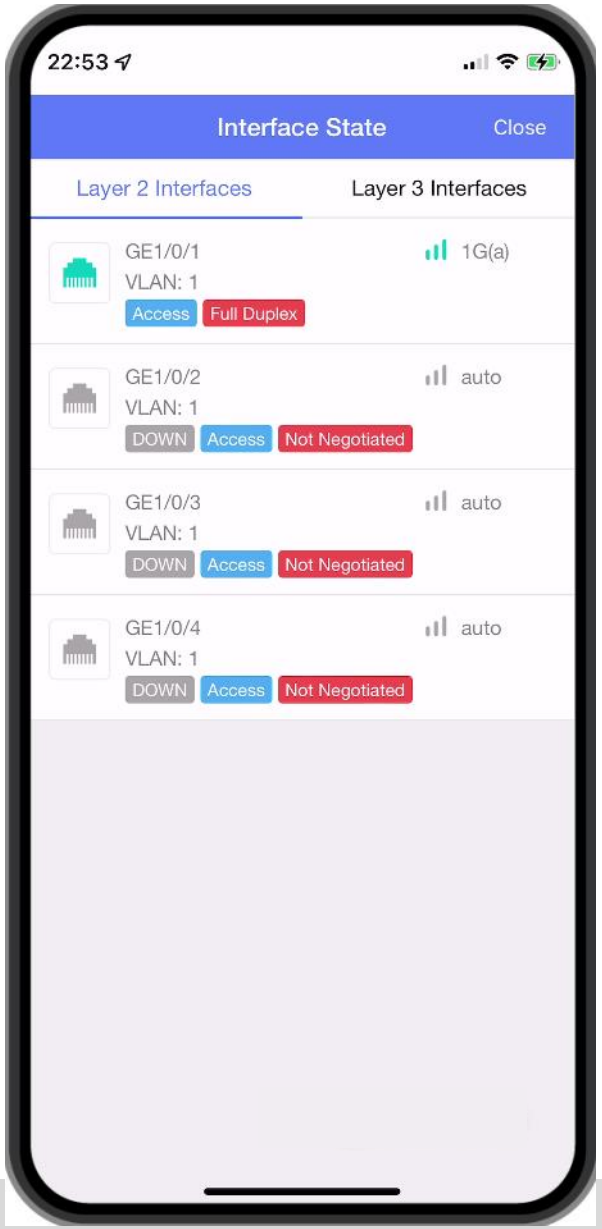
- 上記攻撃への対策(Countermeasure)
- 検知対象外のMACアドレス登録

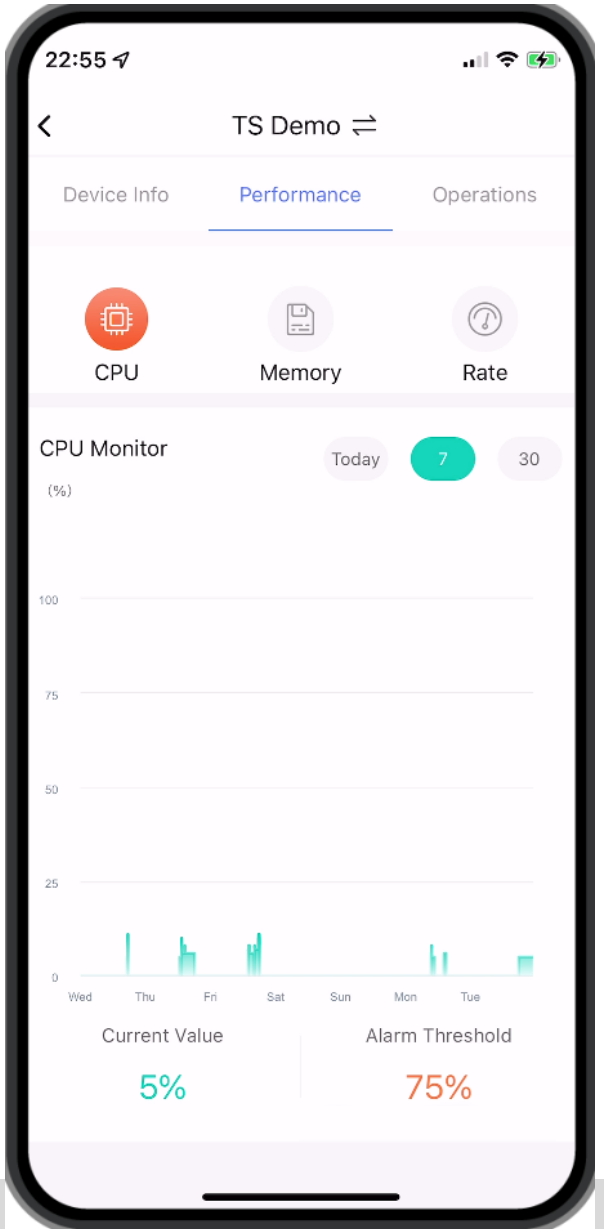
検証機器構成(デモ用)


Cloudnet
Internet
クラウド監視
・攻撃状況記録
・アラートメール通知
・アクセス傾向
・トラフィック傾向
メール通知
週報(HTML,PDF)
日報(HTML,PDF)
クレードルへの電源供給＆
PocketWiFiの充電
Pocket WiFi
WX1840H
アクセスコントローラ
WAN
LAN
USB
・攻撃検知
・攻撃への対策
攻撃パケット
送出アプリ
SSID:WIPSTEST
WPA2+TKIP
PSK: h3cjapan
攻撃パケット
Syslogサーバー
WA6320
アクセスポイント
攻撃パターン
ファイル
PC
PoEアダプター
Cloudnet管理者

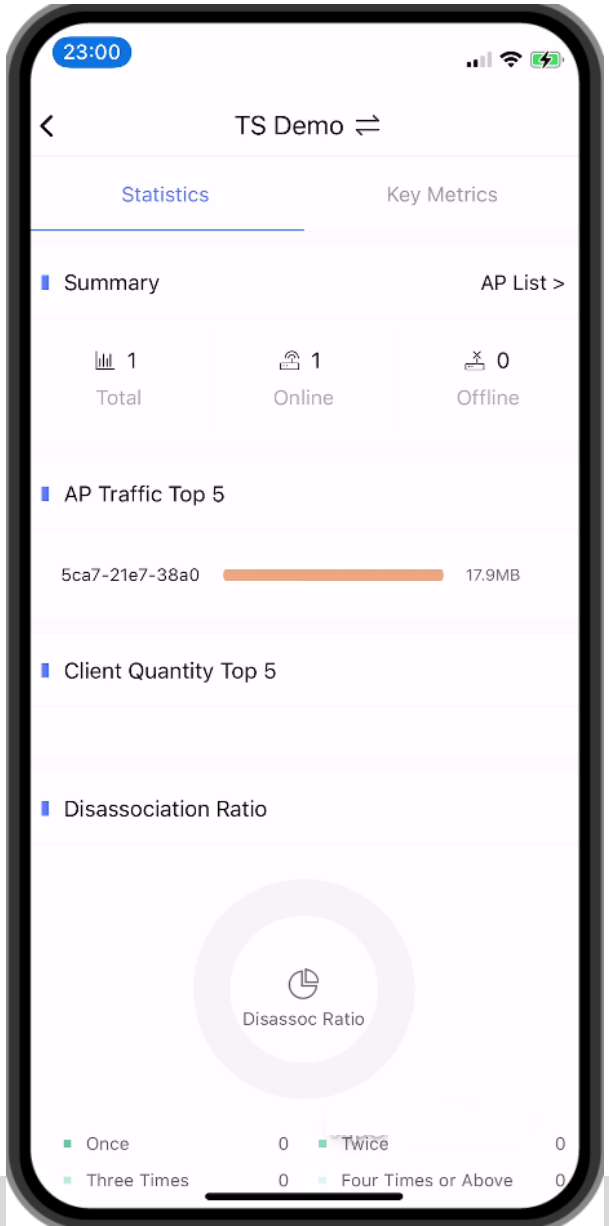
Cloudnetアプリ(IOS)

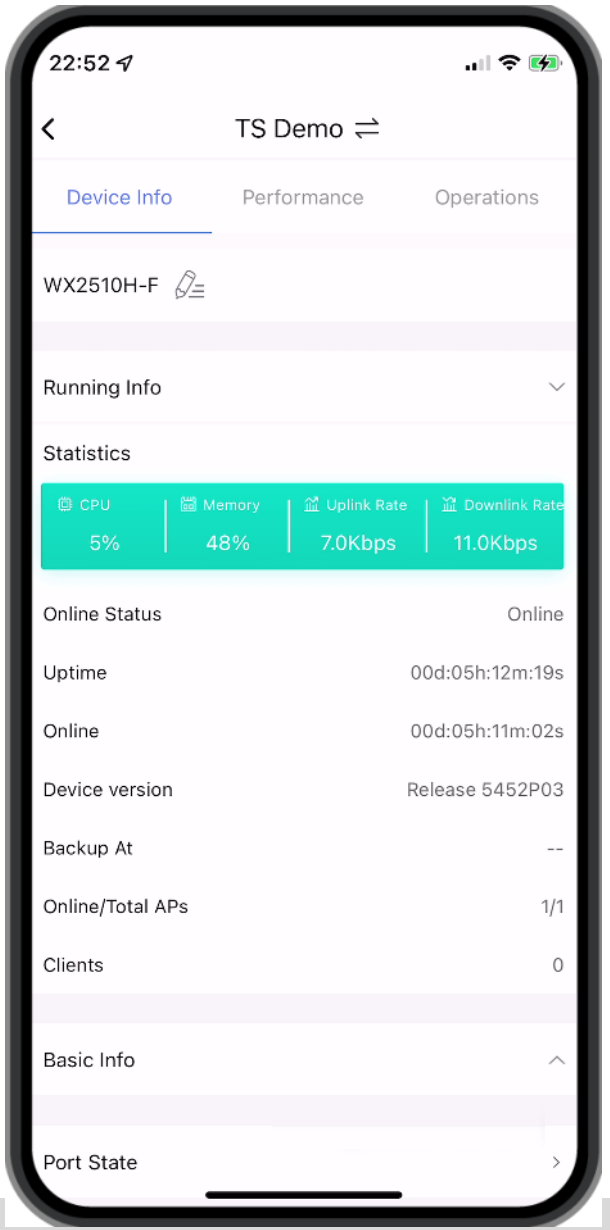






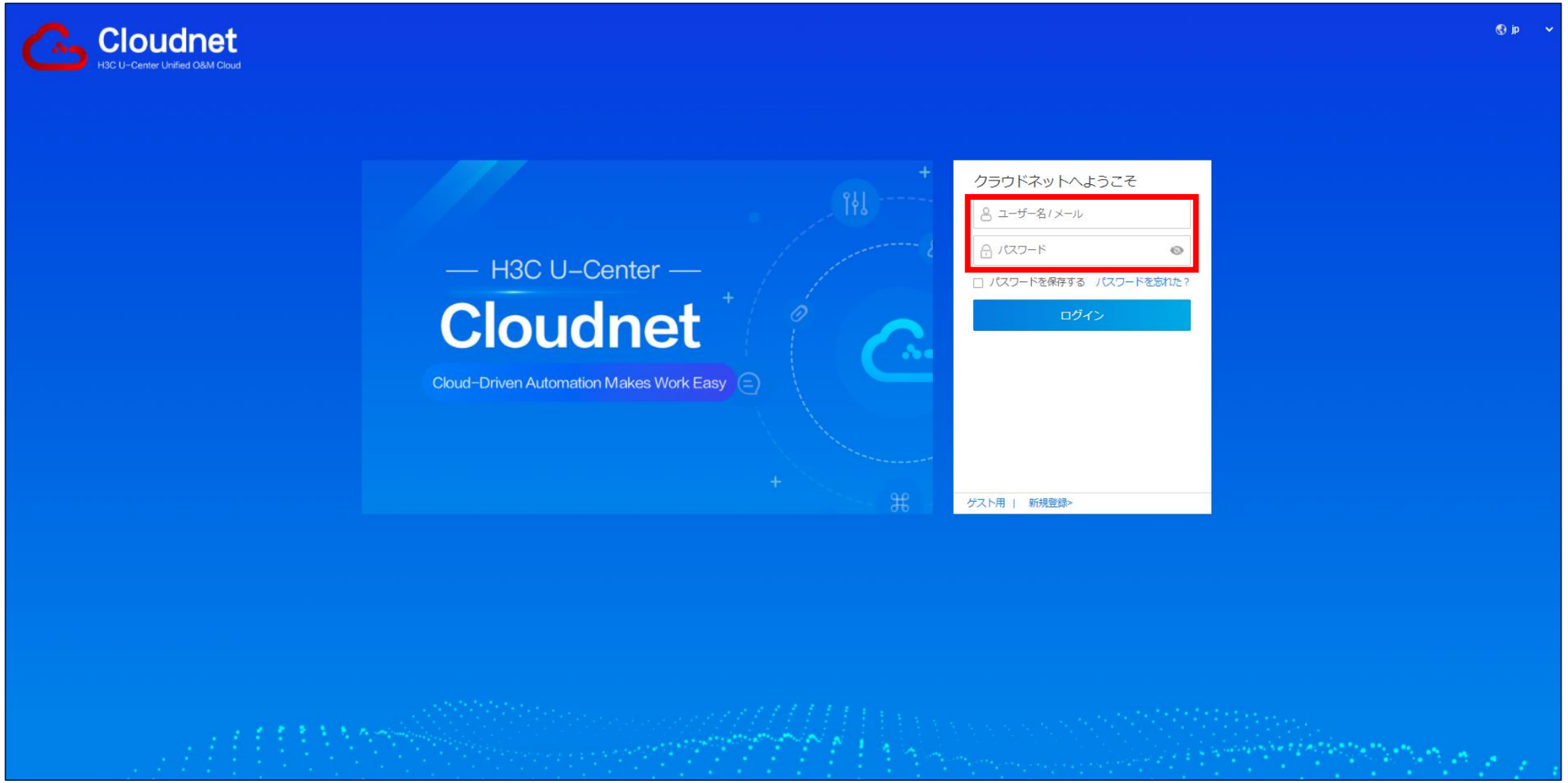
Cloudnetアプリ(IOS)





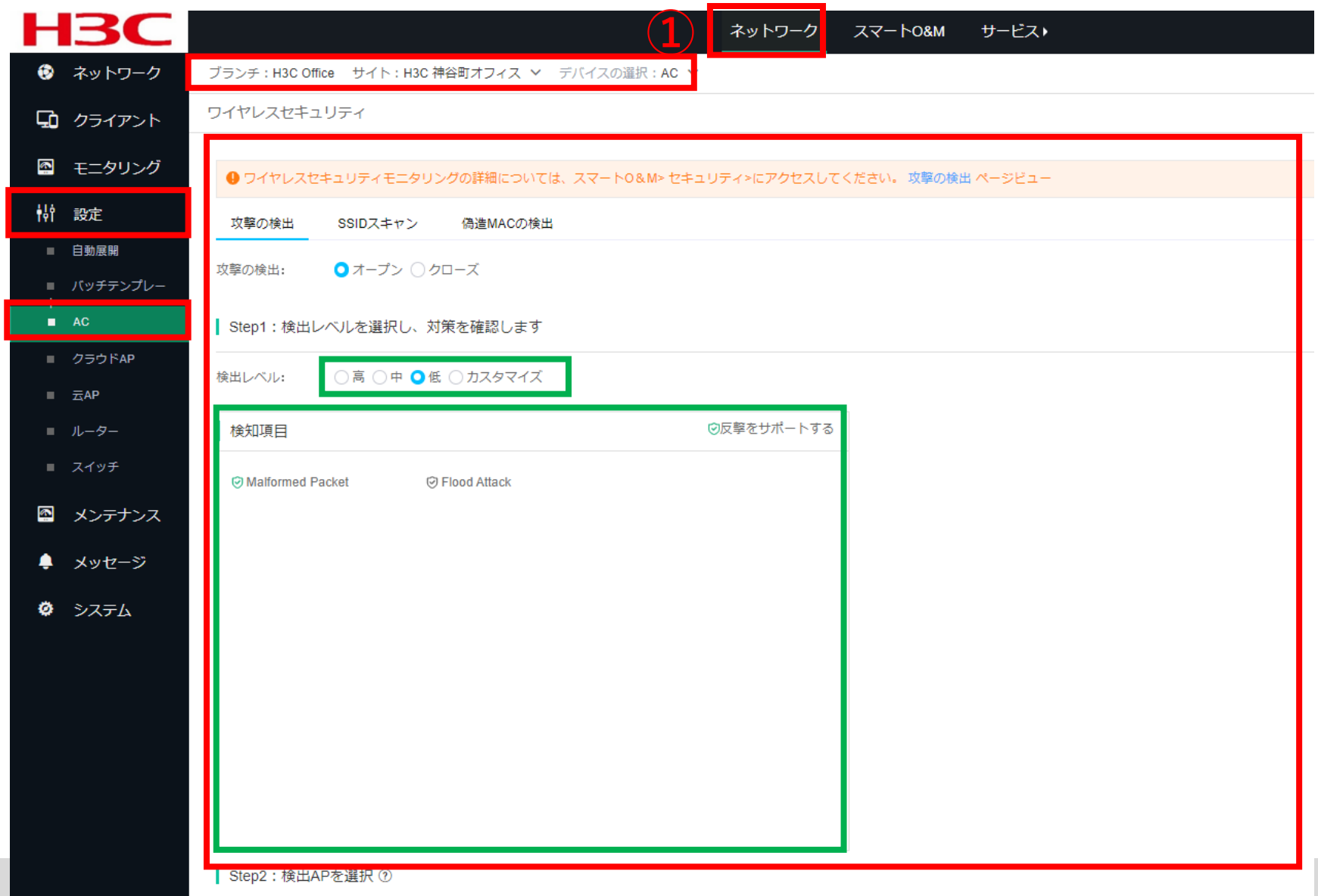
Cloudnetにログインする

- https://cloudnet.h3c.com/



CloudnetでACでのWIPS検知を有効にする(低レベルの場合)

- ネットワーク > 設定 > AC > ワイヤレスセキュリティ

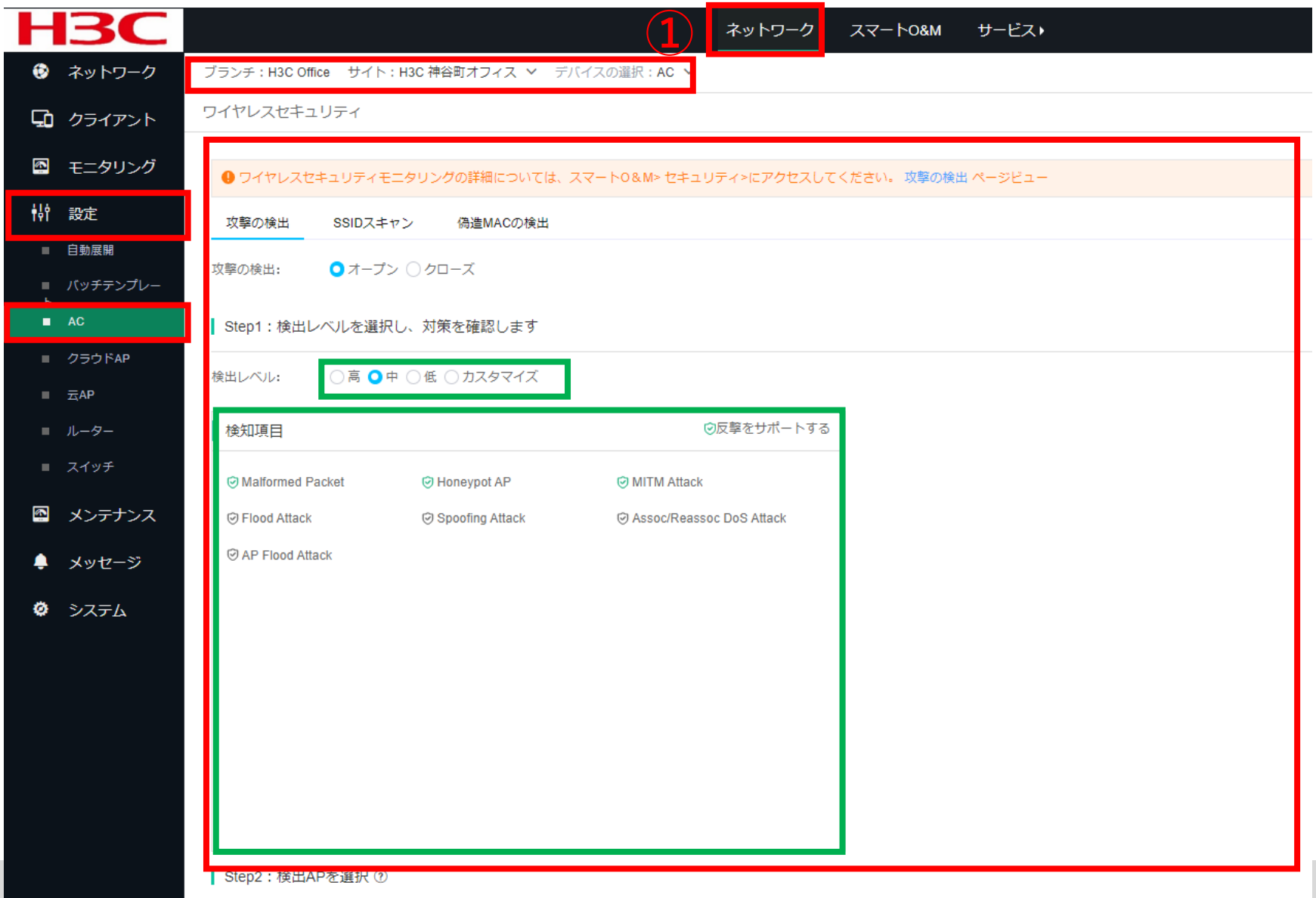


補足

・DoS, DDoSの一種であるMalformed Packet(不正なパケット)の攻撃を受けると、システムが停止させられる可能性がありますのでその攻撃に備えます。

CloudnetでACでのWIPS検知を有効にする(中レベルの場合)

- ネットワーク > 設定 > AC > ワイヤレスセキュリティ

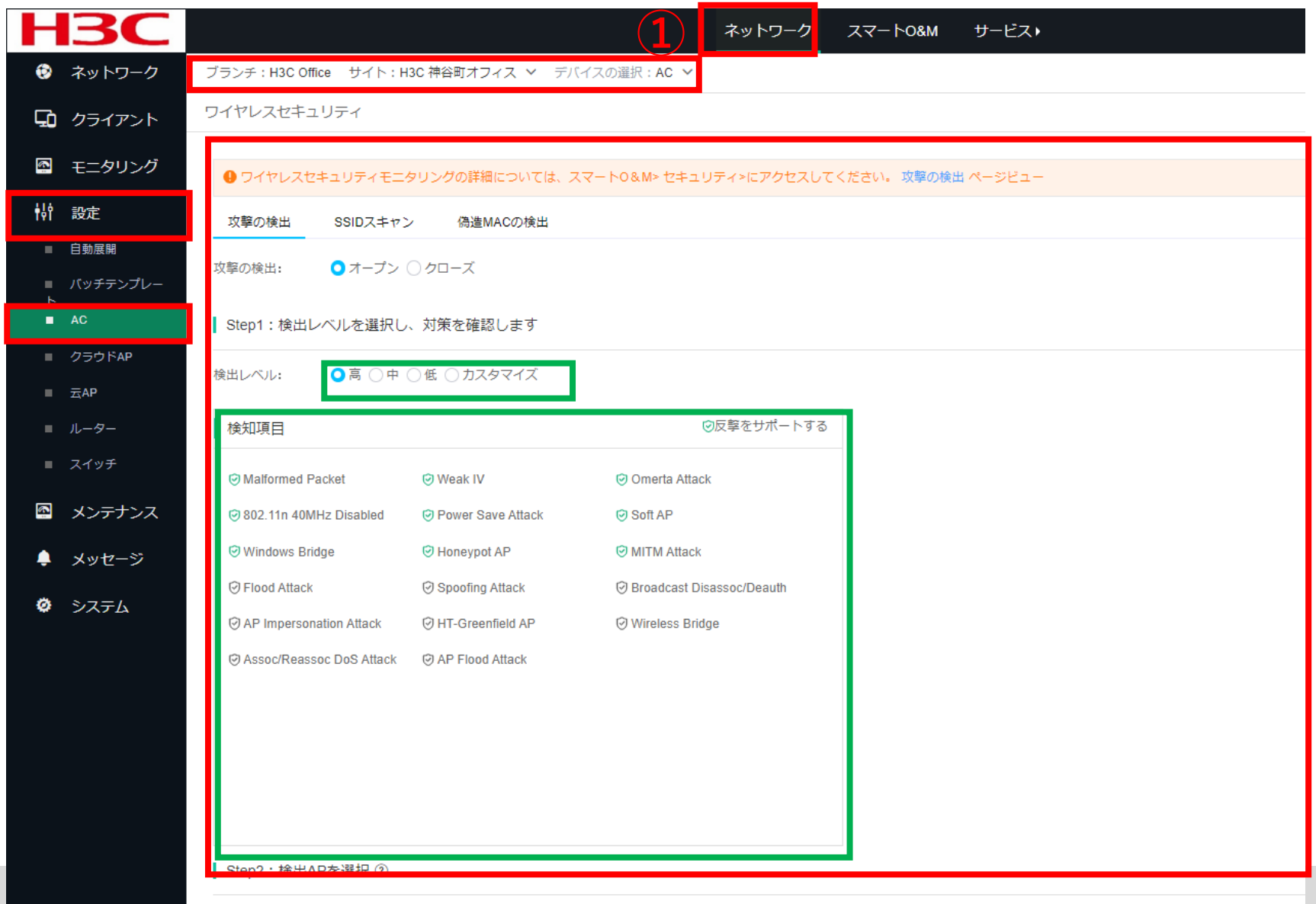


補足

中レベルでは Malformed Packetに加えて、Honeypot AP, MITM攻撃、フラッドやスプーフィングなど中程度の危険性のある攻撃に備えます。

CloudnetでACでのWIPS検知を有効にする(高レベルの場合)

- ネットワーク > 設定 > AC > ワイヤレスセキュリティ

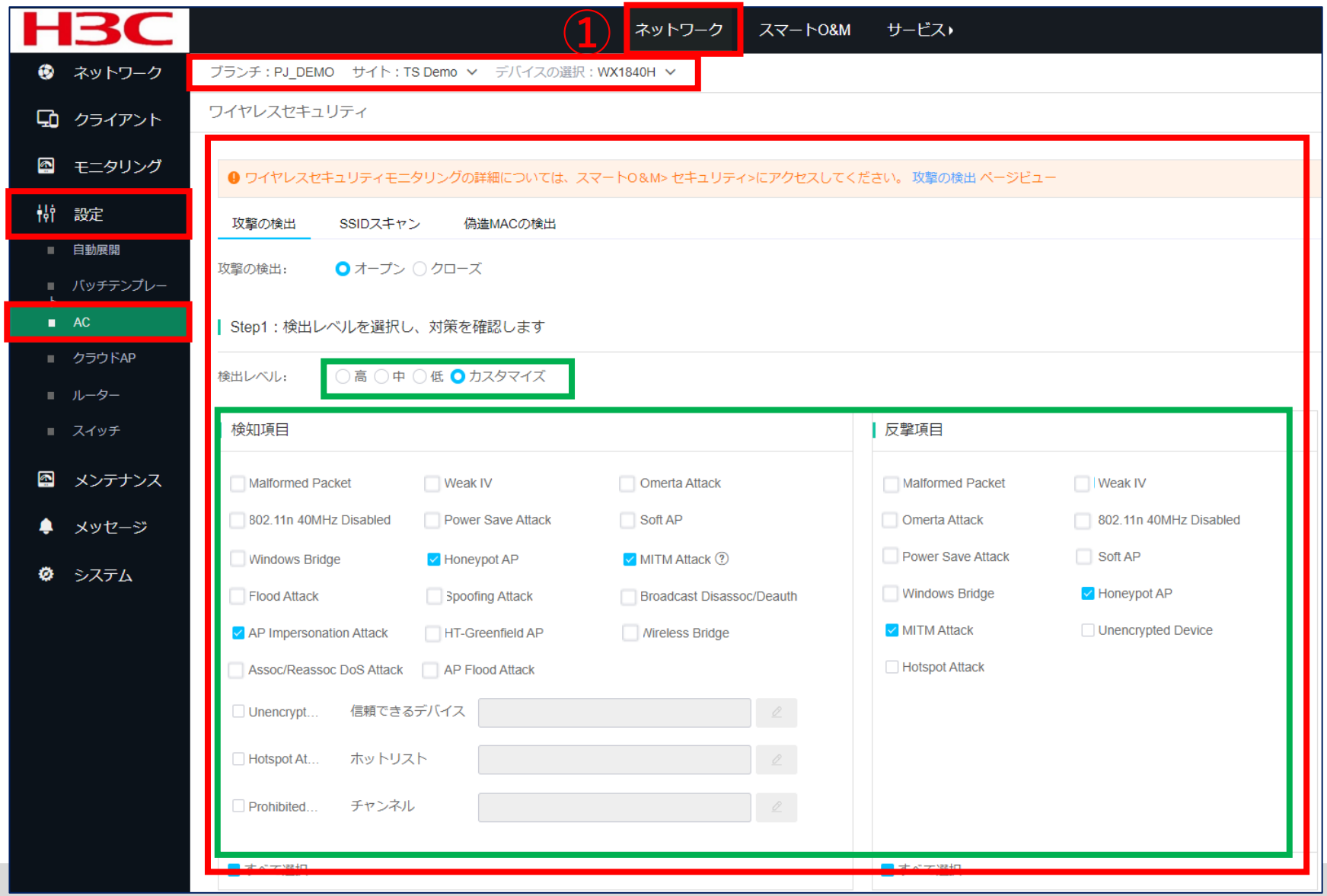


補足

高レベルでは通常ではあまり見られない高度な全ての攻撃に備えております。

CloudnetでACでのWIPS検知をすべて有効にするとCPU負荷過剰になります

- ネットワーク > 設定 > AC > ワイヤレスセキュリティ

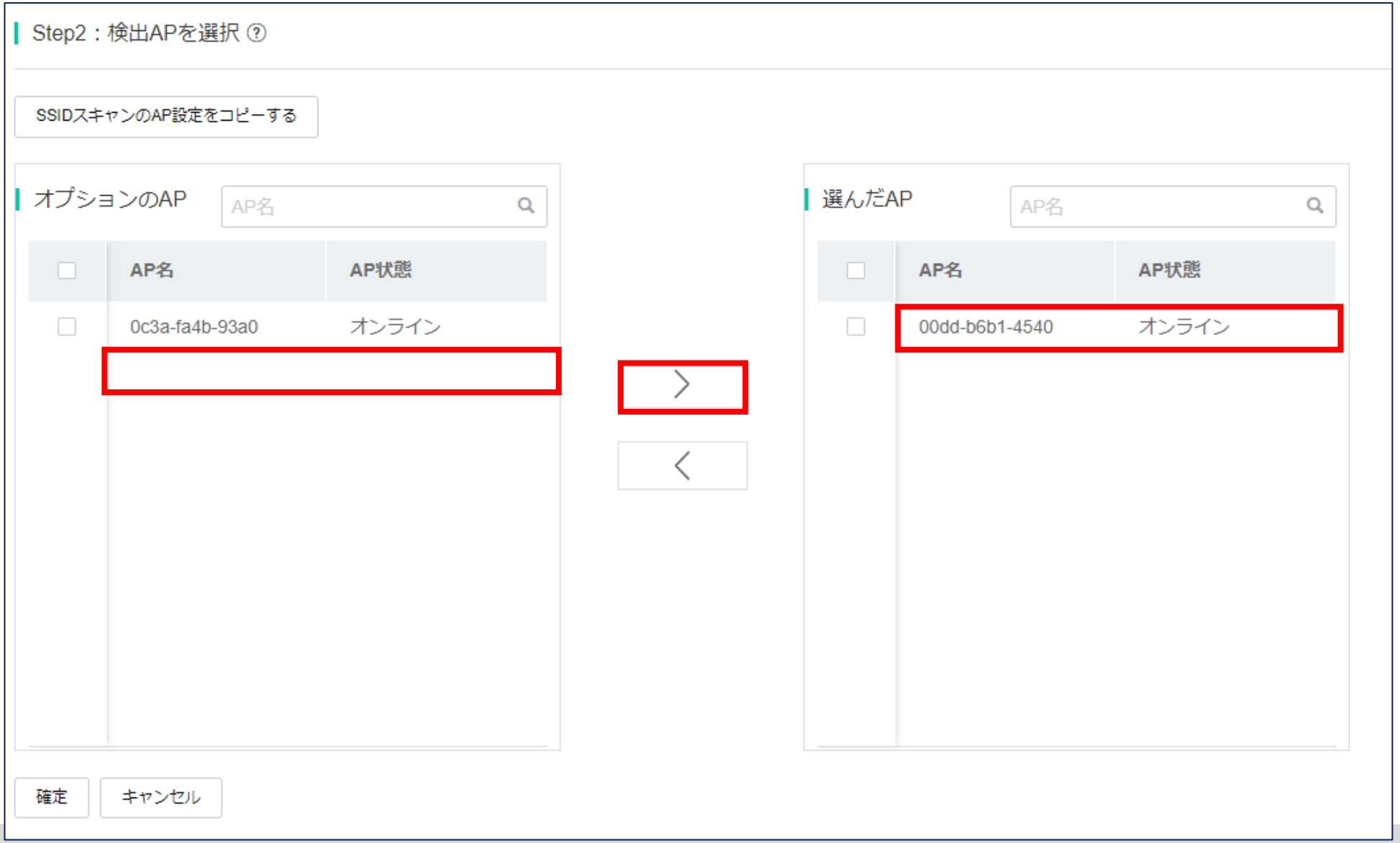


注意！！

全ての検知・対策を有効にするとCPUの負荷が過剰になり、システムの稼働に不具合が生じる可能性が有りますのでどれを有効にするかは検出レベル(高・中・低)で選択される項目を参考にしてください。

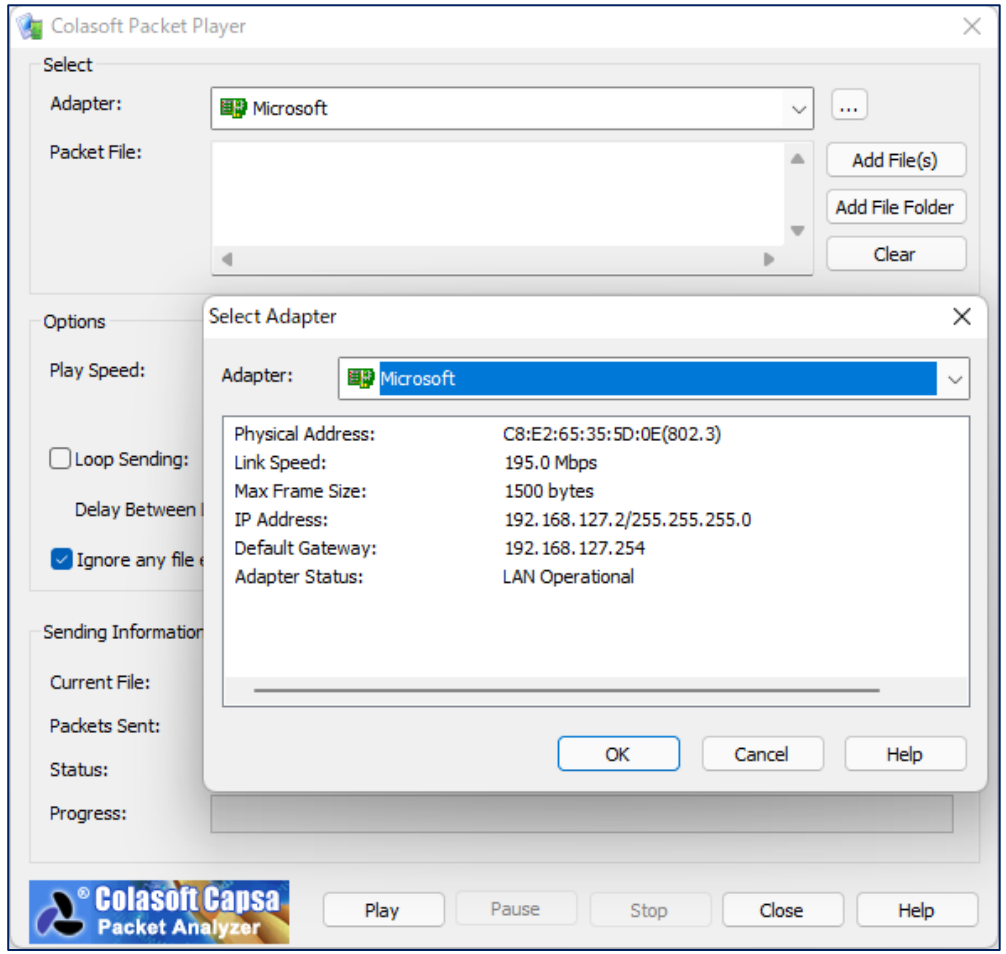
※このページのカスタマイズが推奨設定です。

WIPS検知を有効にするAP(Sensor)を選択する
選択基準としては外部から電波にアクセスされるAPを主なSensorとする

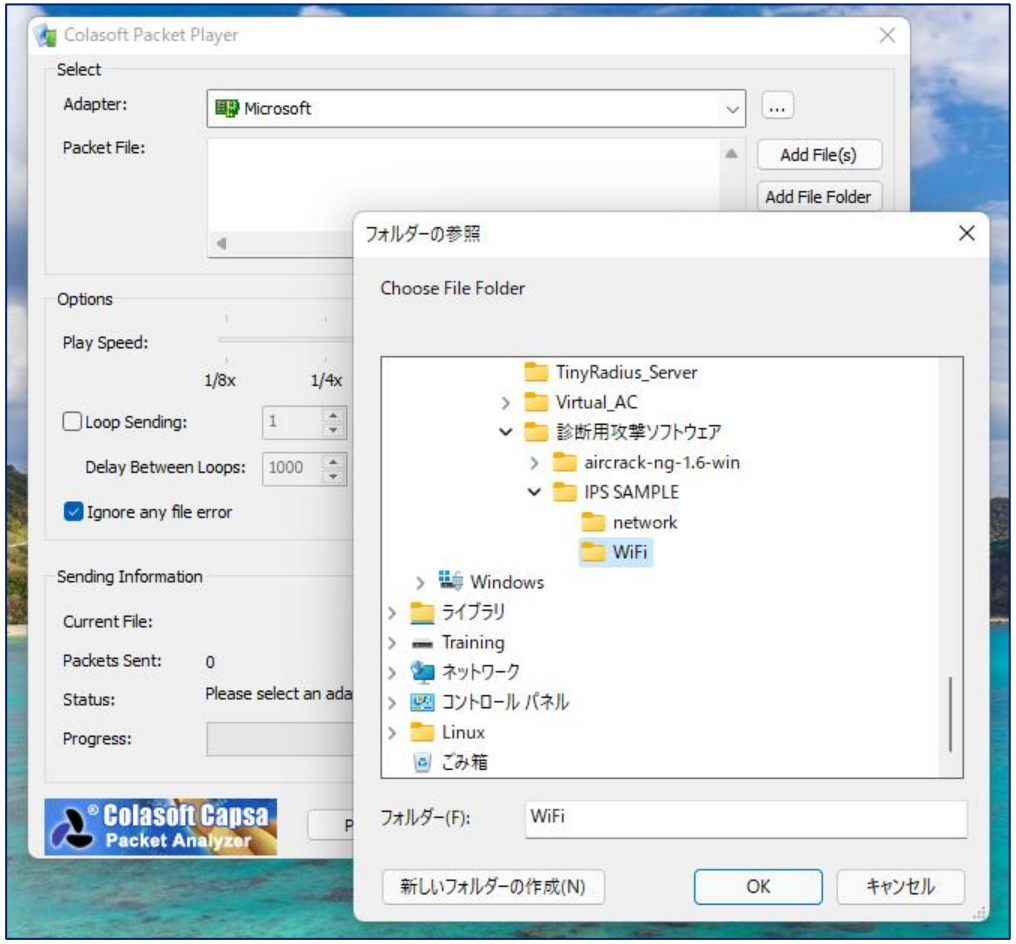


aircrack-ng-1.6-win(フリーのアプリケーション)で用意されたテスト用の攻撃パターンを読み込んで送出

手順1：パケットを送出するWiFiのアダプターを選択する

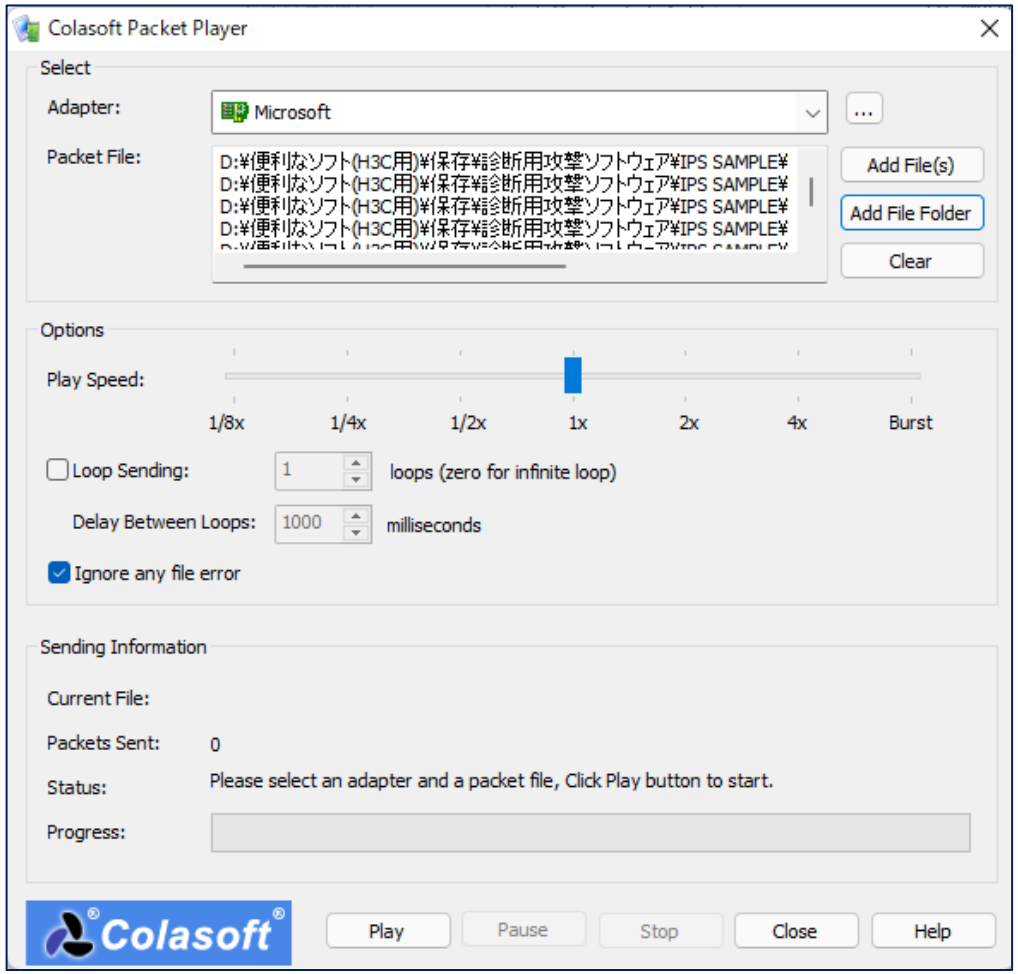


手順2：送出する攻撃パターンのあるフォルダーを選択する



準備が揃ったら攻撃パケットを送出する（回数や繰り返しの間隔など指定することができる）

手順３：Playボタンにより送出を開始する



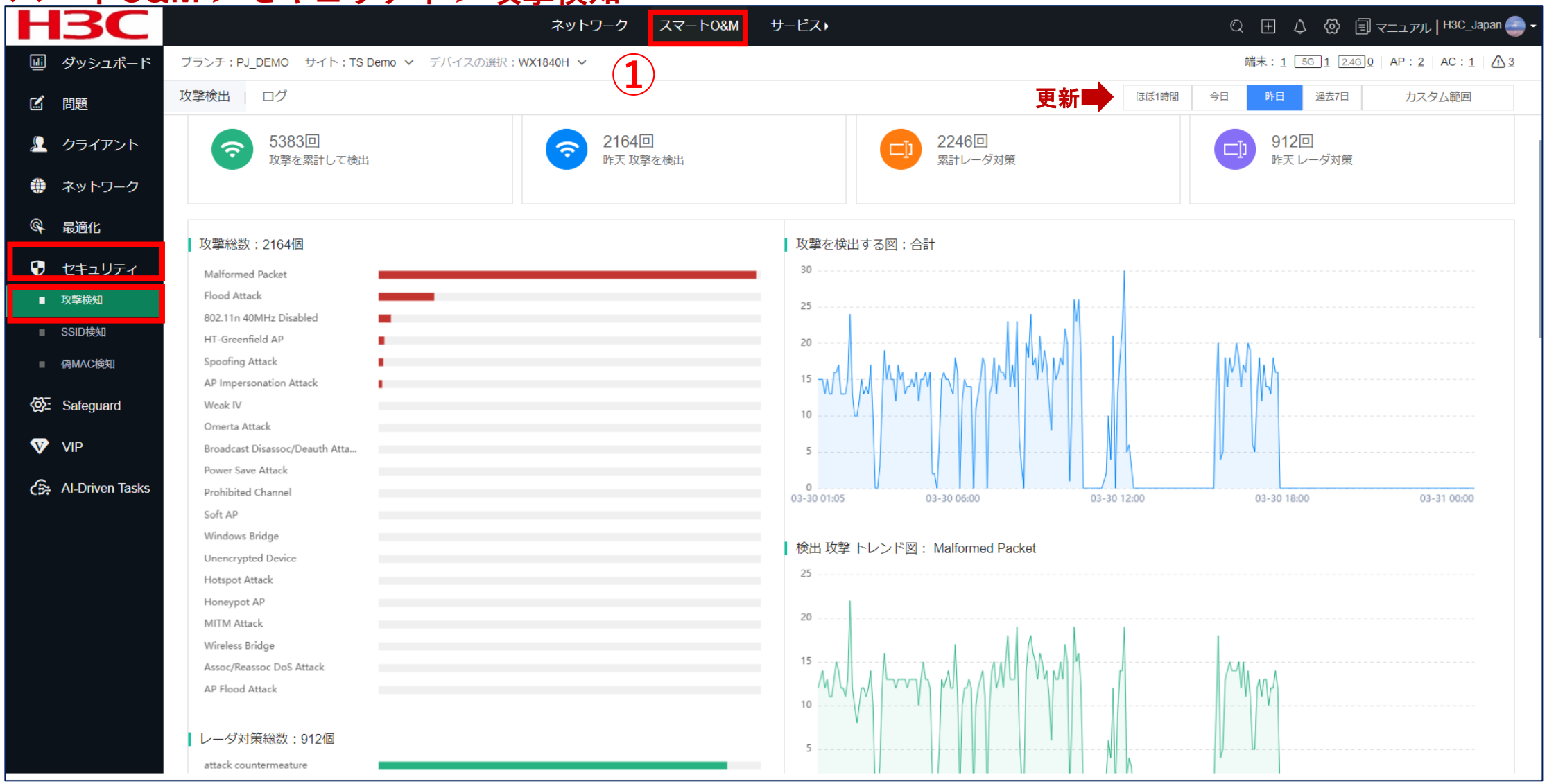
Syslogサーバーではこのデモでは**約10分で17個**程度のWIPSカテゴリーの攻撃が通知された

WX1840HのWIPS Monitor画面での検知数：

- Flood: **17,471**パケット
- Malformed Packet: **7,553**パケット

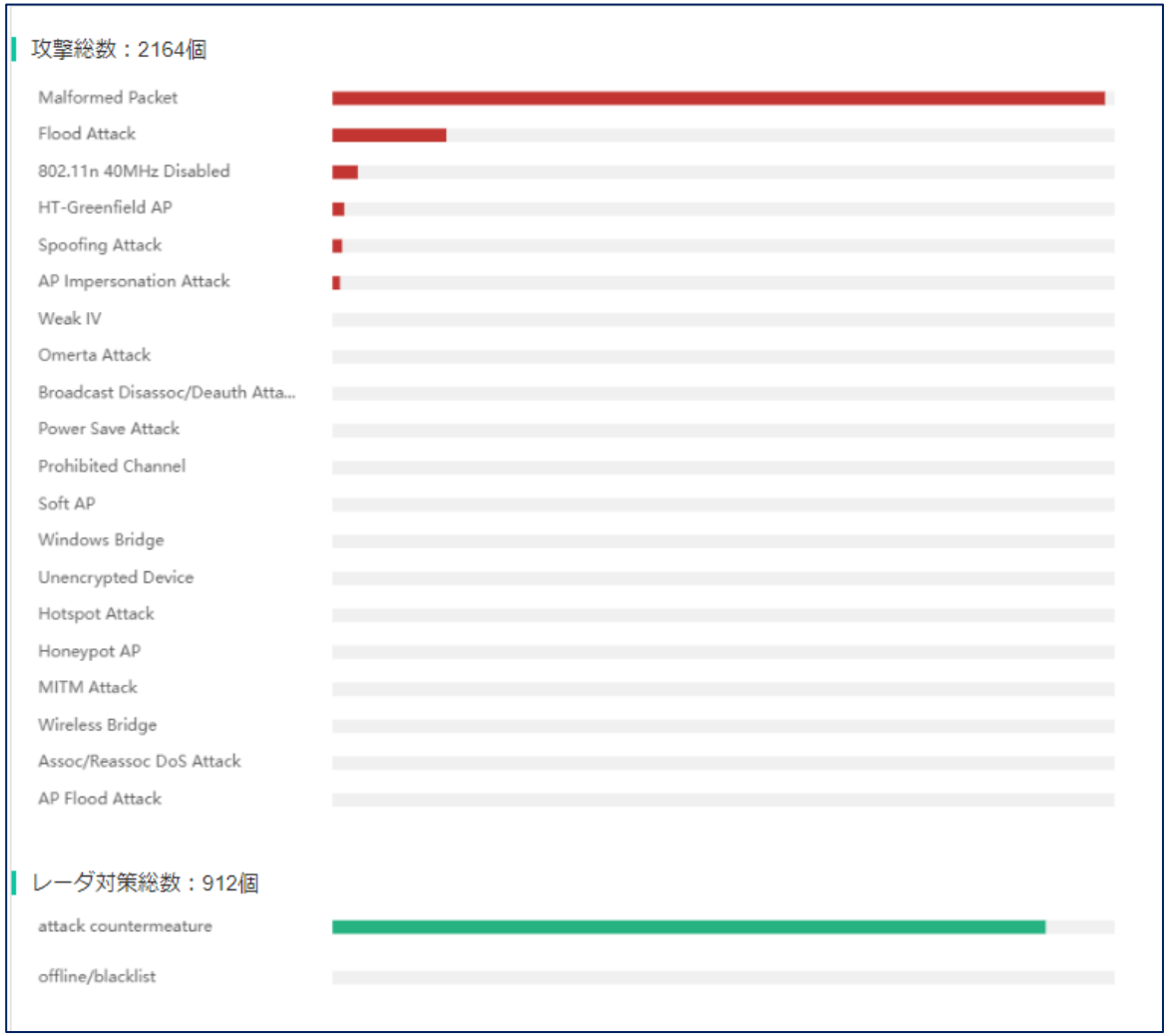
Cloudnet上でのWIPSの状態を確認できる

- スマートO&M > セキュリティ > 攻撃検知

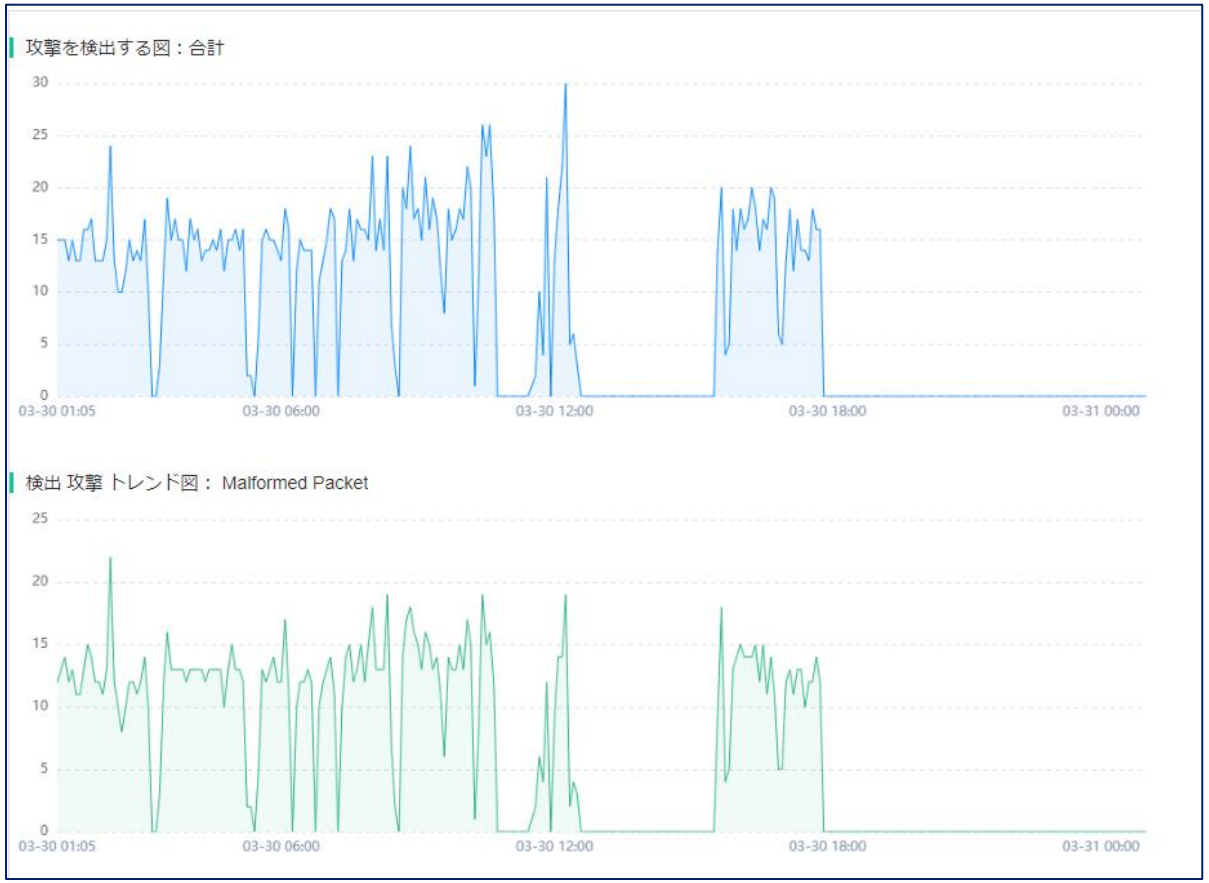


Cloudnet上でのWIPSの状態を確認できる

- 攻撃の種類別のグラフ

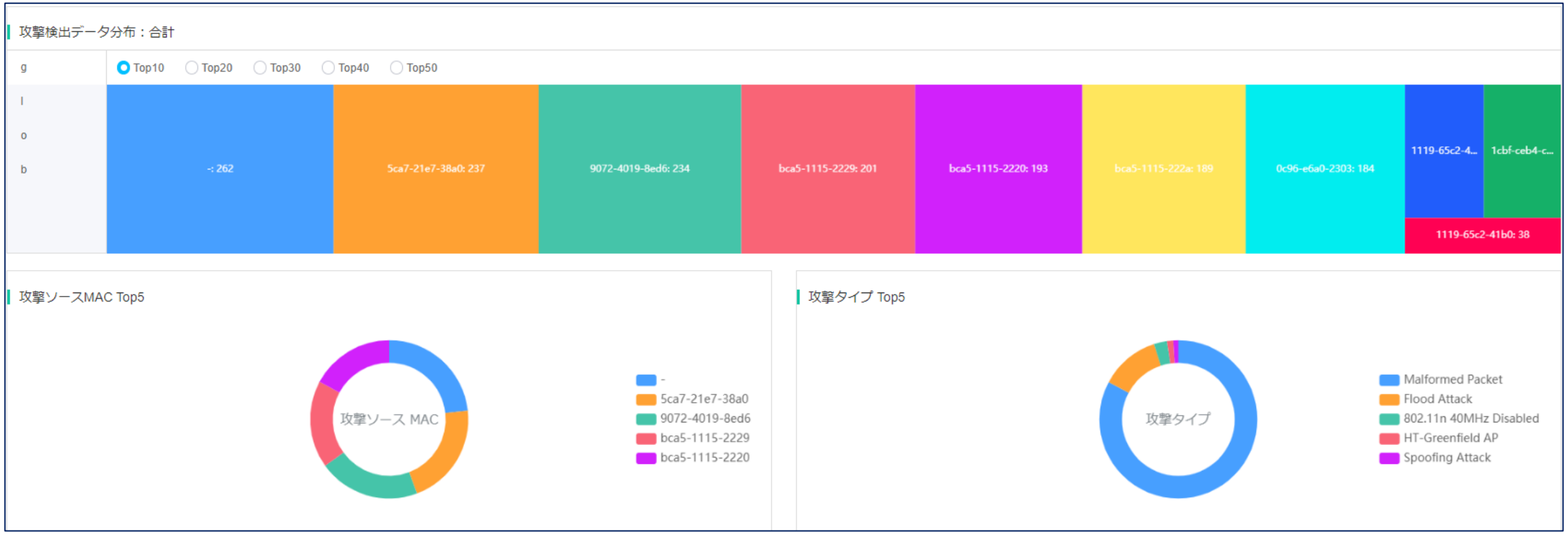


- 攻撃の時系列トータル



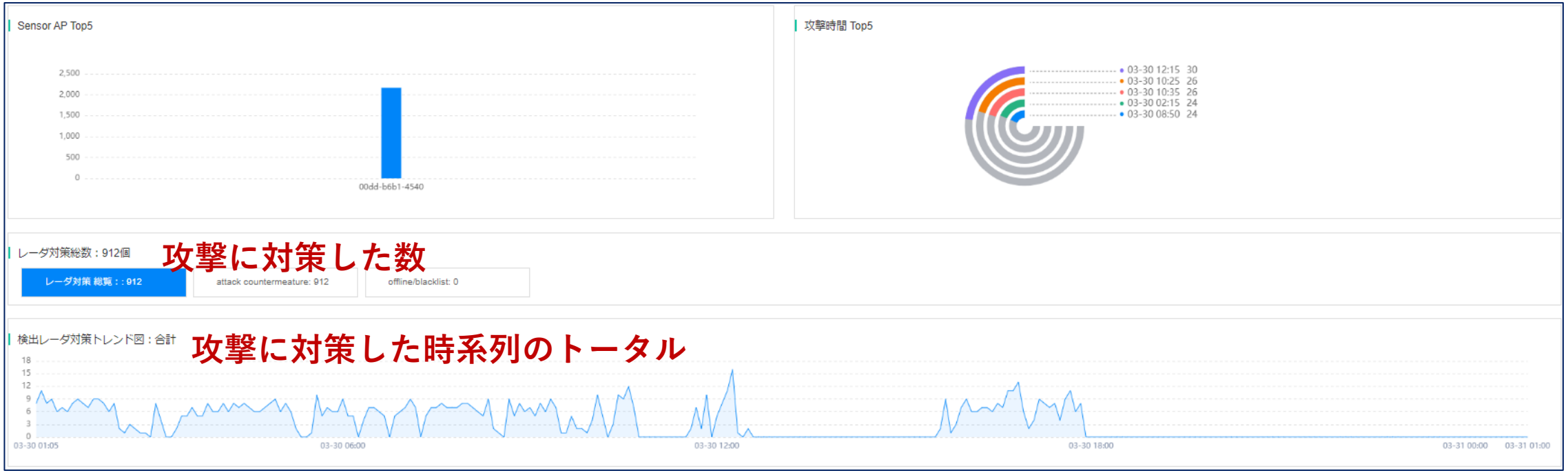
Cloudnet上でのWIPSの状態を確認できる

- 攻撃の多いMACのTop N(MACアドレスと攻撃回数)



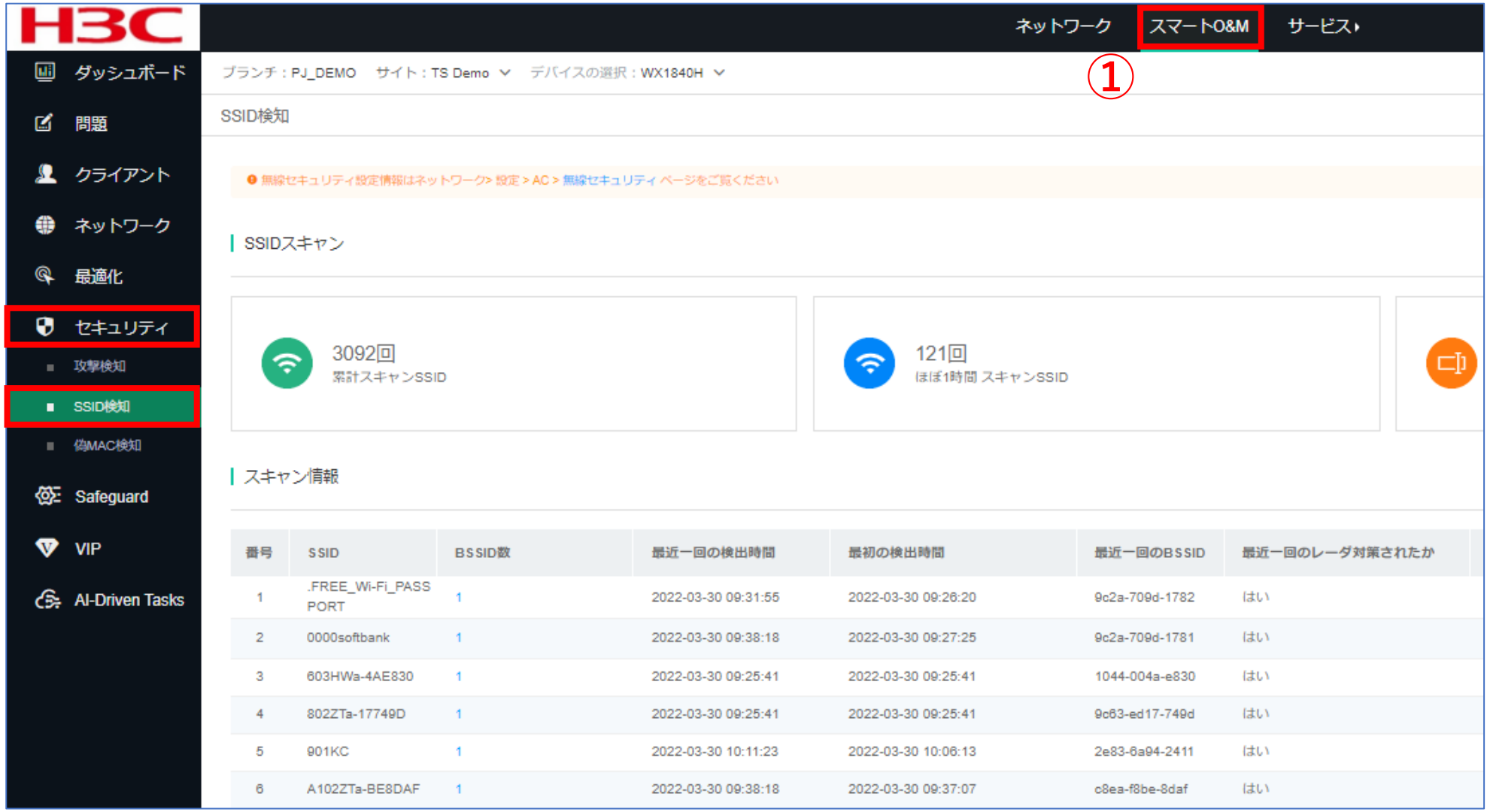
Cloudnet上でのWIPSの状態を確認できる

- AP毎のTop 5(MACアドレス)
- 攻撃時間ごとのTop 5



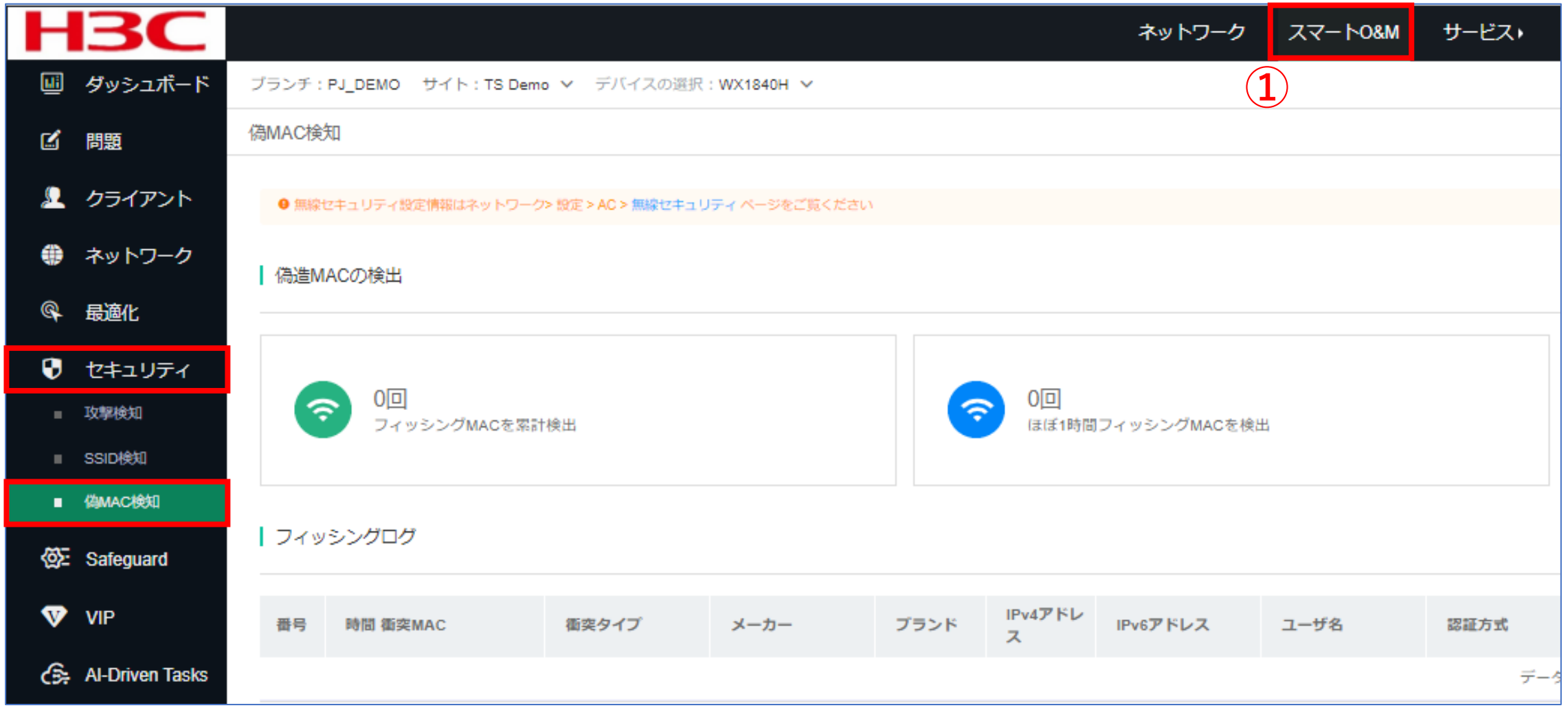
Cloudnet上でのWIPSの状態を確認できる

- スマートO&M > セキュリティ > SSID検知



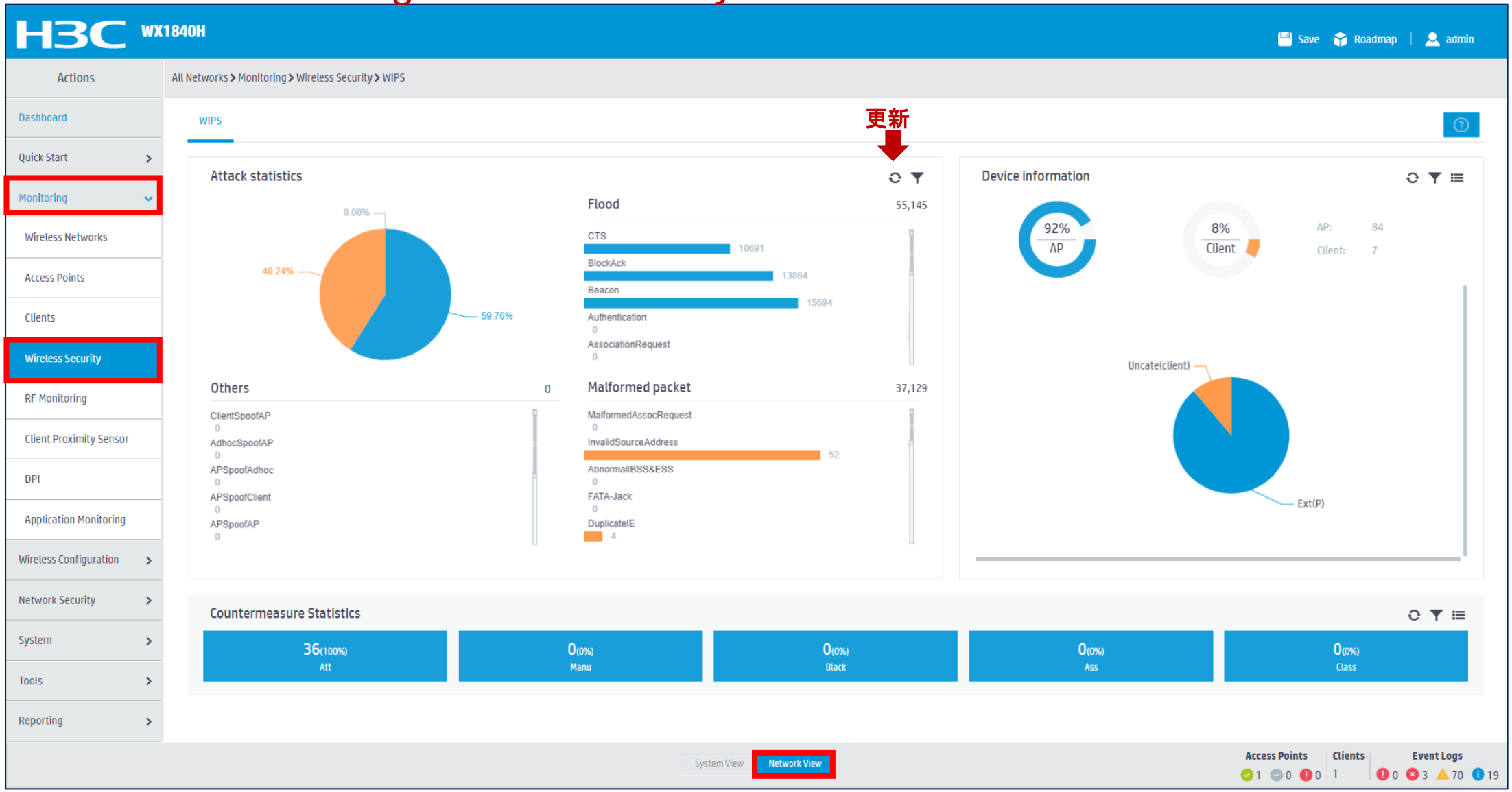
Cloudnet上でのWIPSの状態を確認できる

- スマートO&M > セキュリティ > 偽MAC検知



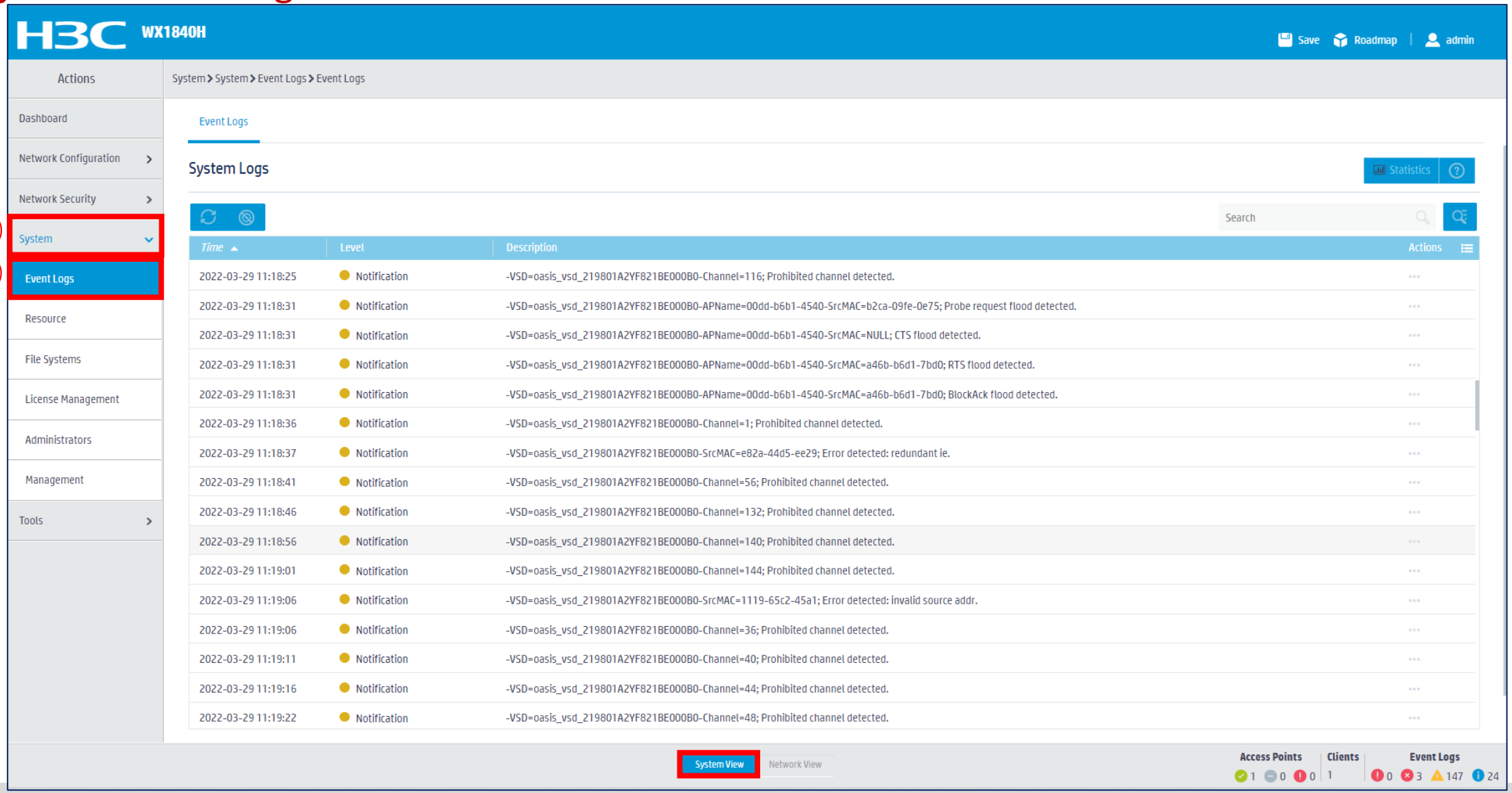
ACのGUI画面でWIPSで検知した状況を確認

- Network View > Monitoring > Wireless Security



エラーログを確認する

- System > Event Logs



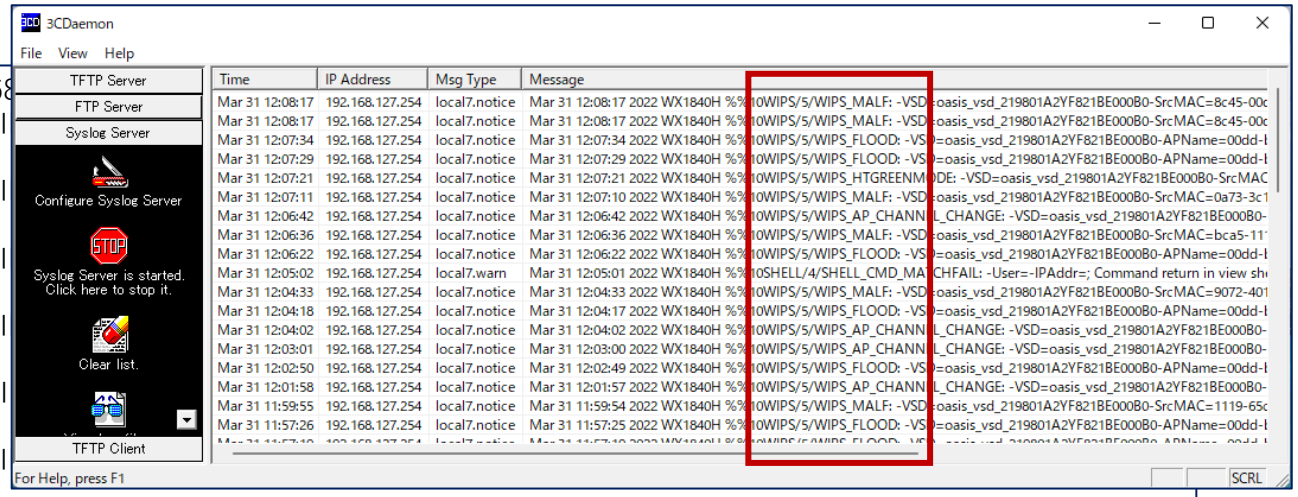
エラーログには攻撃とみなした理由が記述されている

Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=136	Prohibited channel detected.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=bca5	1115-2220; Error detected: invalid ie length.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=5ca7	21e7-38a0; Error detected: large duration.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00d	b6b1-4540-SrcMAC=1019-65c2-4271; Beacon flood detected.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00d	b6b1-4540-SrcMAC=1019-65c2-4270; BlockAck flood detected.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00d	b6b1-4540-SrcMAC=NULL; CTS flood detected.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00d	b6b1-4540-SrcMAC=a46b-b6d1-7bd0; RTS flood detected.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=e82a	44d5-ee29; Error detected: redundant ie.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00d	b6b1-4540-SrcMAC=9a0c-7fd9-2053; Probe request flood detected.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=1119	65c2-45b0; Error detected: invalid source addr.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=5a11	d486-9f61; Error detected: overflow eapol key.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=b0c7	45f9-61c1; HT-Greenfield AP detected.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=ae00	176f-7693; Error detected: duplicated ie.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=a46b	b6d1-7bd0; Error detected: large duration.
Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00d	b6b1-4540-SrcMAC=bca5-1115-2229; Beacon flood detected.

ACのログバッファーでも確認できる

[AC] **dis logbuffer reverse**
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 0
Current messages: 187
%Mar 29 12:42:39:373 2022 WX1840H **WIPS/5/WIPS_FLOOD**: -VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=f4a4-7543-779a; RTS flood detected.
%Mar 29 12:42:35:470 2022 WX1840H **WIPS/5/WIPS_MALF**: -VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=bca5-1115-2220; Error detected: invalid ie length.
%Mar 29 12:42:28:560 2022 WX1840H **WIPS/5/WIPS_MALF**: -VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=9072-4019-8ed6; Error detected: large duration.
%Mar 29 12:42:17:150 2022 WX1840H **WIPS/5/WIPS_FLOOD**: -VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=d4d2-52b3-8b98; BlockAck flood detected.
%Mar 29 12:41:43:650 2022 WX1840H **WIPS/5/WIPS_40MHZINTOLERANCE**: -VSD=oasis_vsd_219801A2YF821BE000B0-BSSID=1019-65c2-41b0-ClientMAC=12bc-d76b-fde3; 40MHz intolerance detected.
%Mar 29 12:41:24:577 2022 WX1840H **WIPS/5/WIPS_FLOOD**: -VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=1019-65c2-4291; Beacon flood detected.
%Mar 29 12:40:41:843 2022 WX1840H **WIPS/5/WIPS_MALF**: -VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=1119-65c2-45b0; Error detected: invalid source addr.
%Mar 29 12:40:40:872 2022 WX1840H **WIPS/5/WIPS_MALF**: -VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=daa1-1985-3836; Error detected: duplicated ie.
%Mar 29 12:40:13:198 2022 WX1840H **WIPS/5/WIPS_AP_CHANNEL_CHANGE**: -VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=1019-65c2-4272; Channel change detected.
%Mar 29 12:40:02:743 2022 WX1840H **WIPS/5/WIPS_MALF**: -VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=dec8-7571-6239; Error detected: overflow eapol key.

Syslogを設定しておくとログがリモートで保存できる



Mar 29 12:31:50 local Listening for Syslog messages on IP address: 192.168
Mar 29 12:47:28 192.168.127.254 Mar 29 12:47:27 2022 WX1840H %%10WI
SrcMAC=1019-65c2-4270; Channel change detected.
Mar 29 12:47:59 192.168.127.254 Mar 29 12:47:58 2022 WX1840H %%10WI
SrcMAC=1019-65c2-41b0; Channel change detected.
Mar 29 12:51:18 192.168.127.254 Mar 29 12:51:17 2022 WX1840H %%10WI
45b1; Error detected: invalid source addr.
Mar 29 12:51:26 192.168.127.254 Mar 29 12:51:25 2022 WX1840H %%10WI
4540-SrcMAC=1019-65c2-4270; Beacon flood detected.
Mar 29 12:52:14 192.168.127.254 Mar 29 12:52:13 2022 WX1840H %%10WI
Error detected: duplicated ie.
Mar 29 12:52:23 192.168.127.254 Mar 29 12:52:22 2022 WX1840H %%10WI
4540-SrcMAC=a46b-b6d1-7bd0; BlockAck flood detected.
Mar 29 12:52:42 192.168.127.254 Mar 29 12:52:41 2022 WX1840H %%10WIPS/5/WIPS_MALF: -VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=5ca7-21e7-38a0; Error detected: large duration.
Mar 29 12:52:42 192.168.127.254 Mar 29 12:52:41 2022 WX1840H %%10**WIPS/5/WIPS_40MHZINTOLERANCE**: -VSD=oasis_vsd_219801A2YF821BE000B0-BSSID=1019-65c2-45a0-ClientMAC=c6f2-12b3-d05a; 40MHz intolerance detected.
Mar 29 12:52:46 192.168.127.254 Mar 29 12:52:45 2022 WX1840H %%**10WIPS/5/WIPS_MALF**: -VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=bca5-1115-2220; Error detected: invalid ie length.
Mar 29 12:53:03 192.168.127.254 Mar 29 12:53:02 2022 WX1840H %%**10WIPS/5/WIPS_FLOOD**: -VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=1cbf-ceb4-c450; RTS flood detected.
Mar 29 12:53:07 192.168.127.254 Mar 29 12:53:06 2022 WX1840H %%**10WIPS/5/WIPS_FLOOD**: -VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=NULL; CTS flood detected.
Mar 29 12:53:30 192.168.127.254 Mar 29 12:53:29 2022 WX1840H %%**10WIPS/5/WIPS_FLOOD**: -VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=b060-888e-b3bd; Probe request flood detected.
Mar 29 12:55:01 192.168.0.50 Mar 28 12:55:22 2022 H3C %%10STAMGR/6/STAMGR_CLIENT_ONLINE: Client 56d3-1d7e-3934 went online from BSS 1019-65c2-3f00 vlan 1 with SSID H3C on AP fatap Radio ID 3. State changed to Run.

参考：エラーレベル

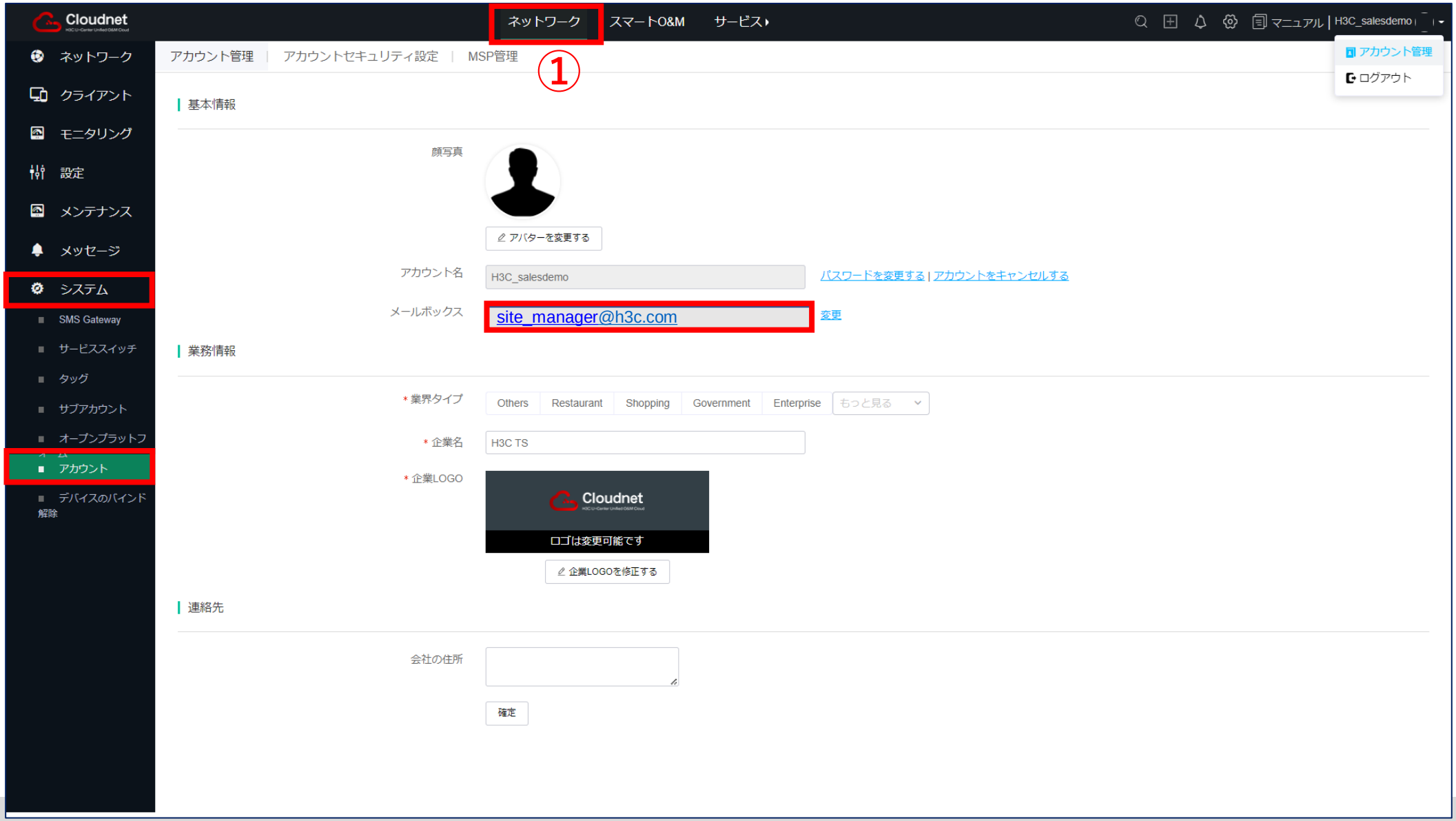
エラー名	状況説明	重大度レベル
emergency(緊急)	システムは使用できません	重大度= 0
alert(アラート)	推奨アクションはすぐに実行する必要があります	重大度= 1
critical(クリティカル)	危機的な状態	重大度= 2
error(エラー)	エラー状態	重大度= 3
warning(警告)	警告条件	重大度= 4
notification(通知)	正常だが重大な状態	重大度= 5
informational(情報)	情報メッセージ	重大度= 6
debugging(デバッグ)	デバッグレベルのメッセージ	重大度= 7

攻撃歴のコマンドでの確認

<AC>**display wips statistics receive**
Information from sensor 1
Information about attack statistics:
Detected association-request flood messages: 164
Detected authentication flood messages: 931
Detected beacon flood messages: 214550
Detected block-ack flood messages: 5400
Detected cts flood messages: 4559
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 4918
Detected reassociation-request flood messages: 0
Detected rts flood messages: 8120
Detected eapol-logoff flood messages: 0
Detected eap-failure flood messages: 0
Detected eap-success flood messages: 0
Detected duplicated-ie messages: 85
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 7
Detected invalid-address-combination messages: 1476
Detected invalid-assoc-req messages: 5
Detected invalid-auth messages: 40
Detected invalid-deauth-code messages: 35
Detected invalid-disassoc-code messages: 45
Detected invalid-ht-ie messages: 3
Detected invalid-ie-length messages: 24428
Detected invalid-pkt-length messages: 178
Detected large-duration messages: 1324
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 1
Detected overflow-ssid messages: 120
Detected redundant-ie messages: 675
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected signature rule messages: 0
Detected 40MHZ messages: 0
Detected power save messages: 0
Detected omerta messages: 0
Detected windows bridge messages: 0
Detected soft AP messages: 0
Detected broadcast disassoc messages: 0
Detected broadcast deauth messages: 0
Detected AP impersonate messages: 1
Detected HT greenfield messages: 23
Detected association table overflow messages: 0
Detected wireless bridge messages: 0
Detected AP flood messages: 0
Detected illegal channel 1 messages: 787
Detected illegal channel 2 messages: 19
Detected illegal channel 3 messages: 11
Detected illegal channel 4 messages: 11
Detected illegal channel 5 messages: 21
Detected illegal channel 6 messages: 12961
Information from sensor 3
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 183
Detected beacon flood messages: 47050
Detected block-ack flood messages: 16200
Detected cts flood messages: 6011
Detected deauthentication flood messages: 50
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 240
Detected probe-request flood messages: 19850
Detected reassociation-request flood messages: 66
Detected rts flood messages: 7245
Detected eapol-logoff flood messages: 0
Detected eap-failure flood messages: 0
Detected eap-success flood messages: 0
Detected duplicated-ie messages: 14
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 23
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 5811
Detected invalid-pkt-length messages: 3
Detected large-duration messages: 171
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 57
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 278
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 3

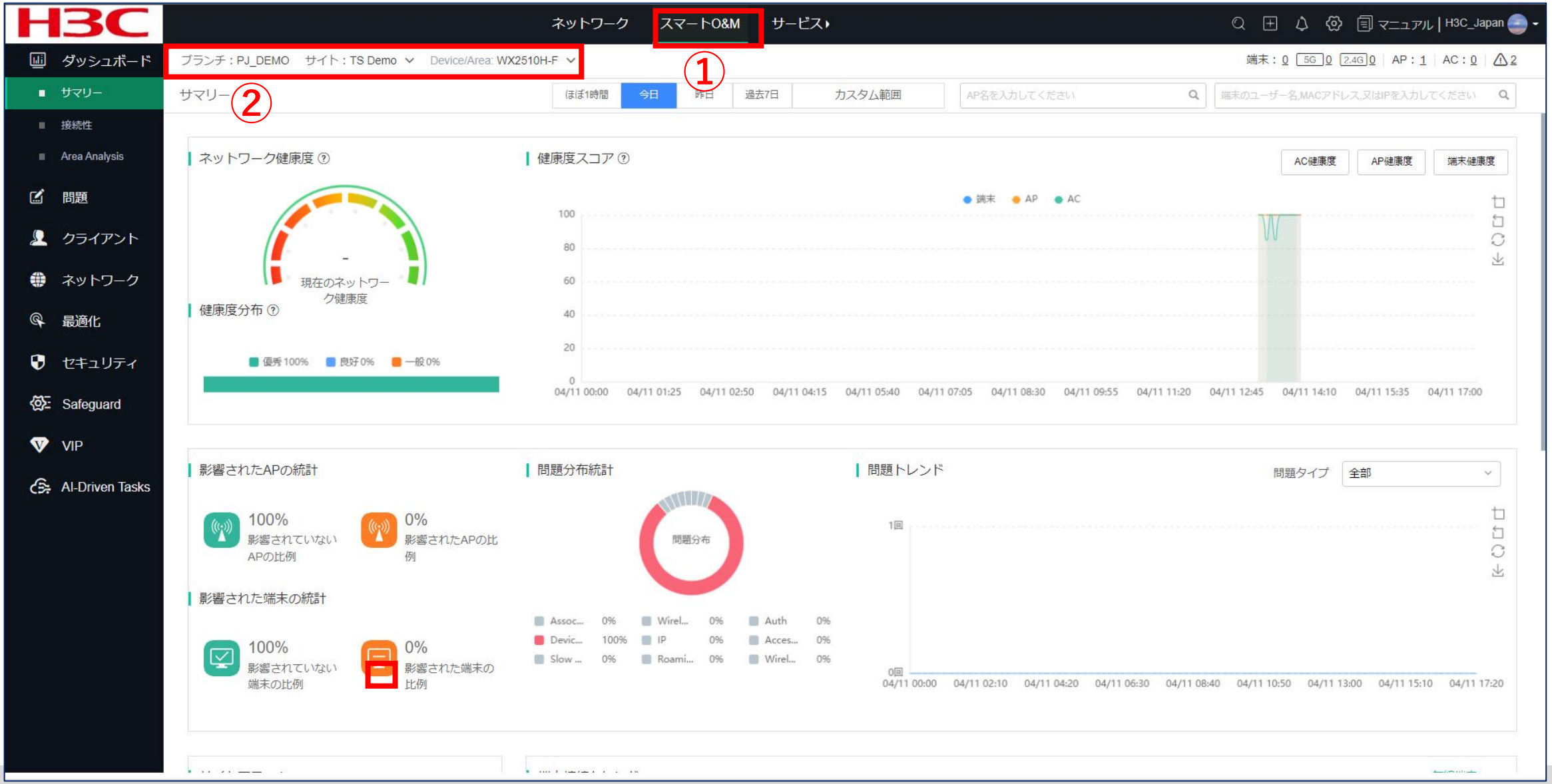
管理者のメールアドレスはアカウントに設定されています

- ネットワーク > システム > アカウント



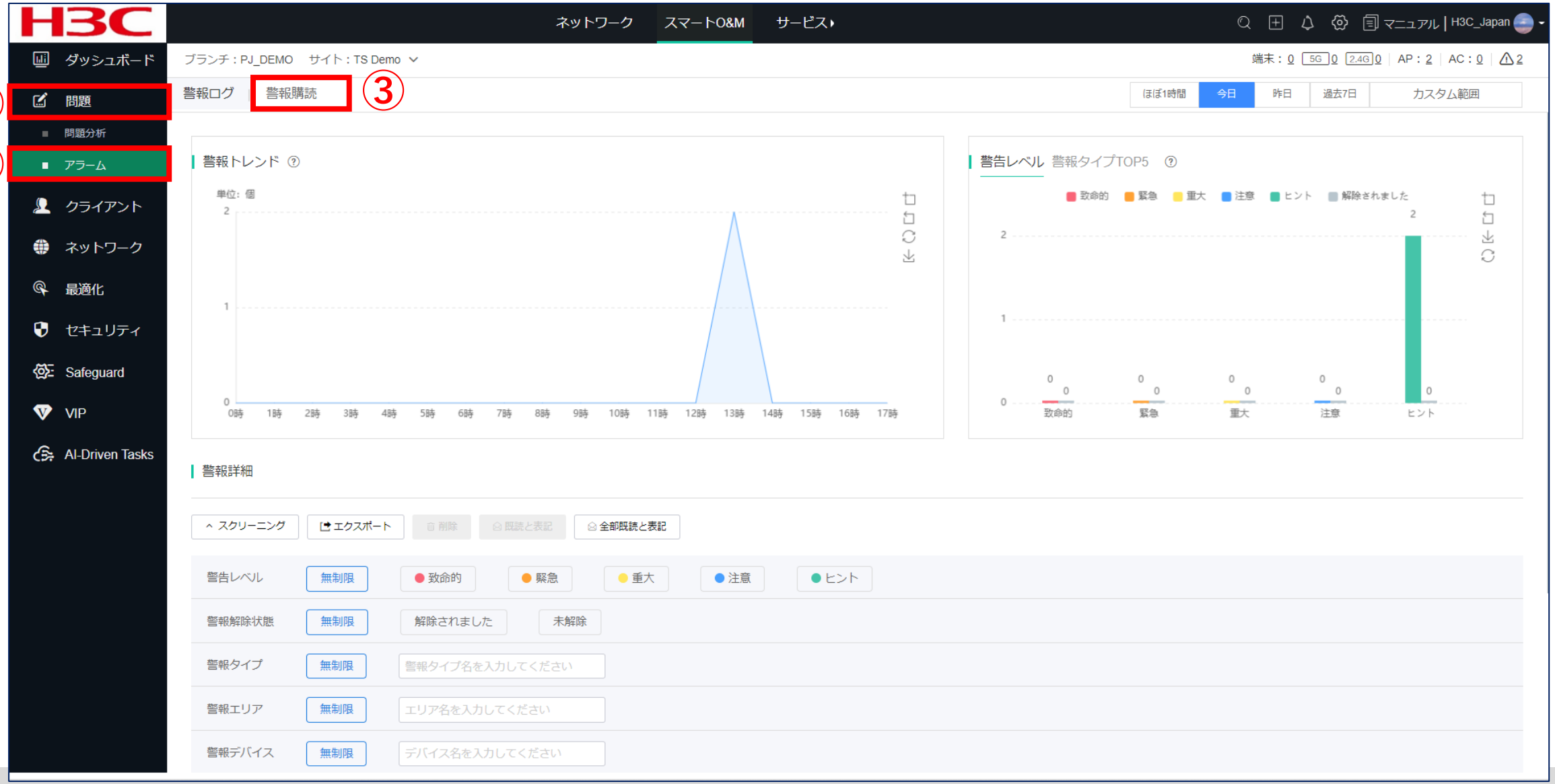
Cloudnet検知した攻撃を管理者にメールで伝える

- スマートO&M > ブランチ　> サイト > Device/Areaで対象の装置を選択



Cloudnet検知した攻撃を管理者にメールで伝える(続き)

- 問題 > アラーム > 警報購読



①

②

③

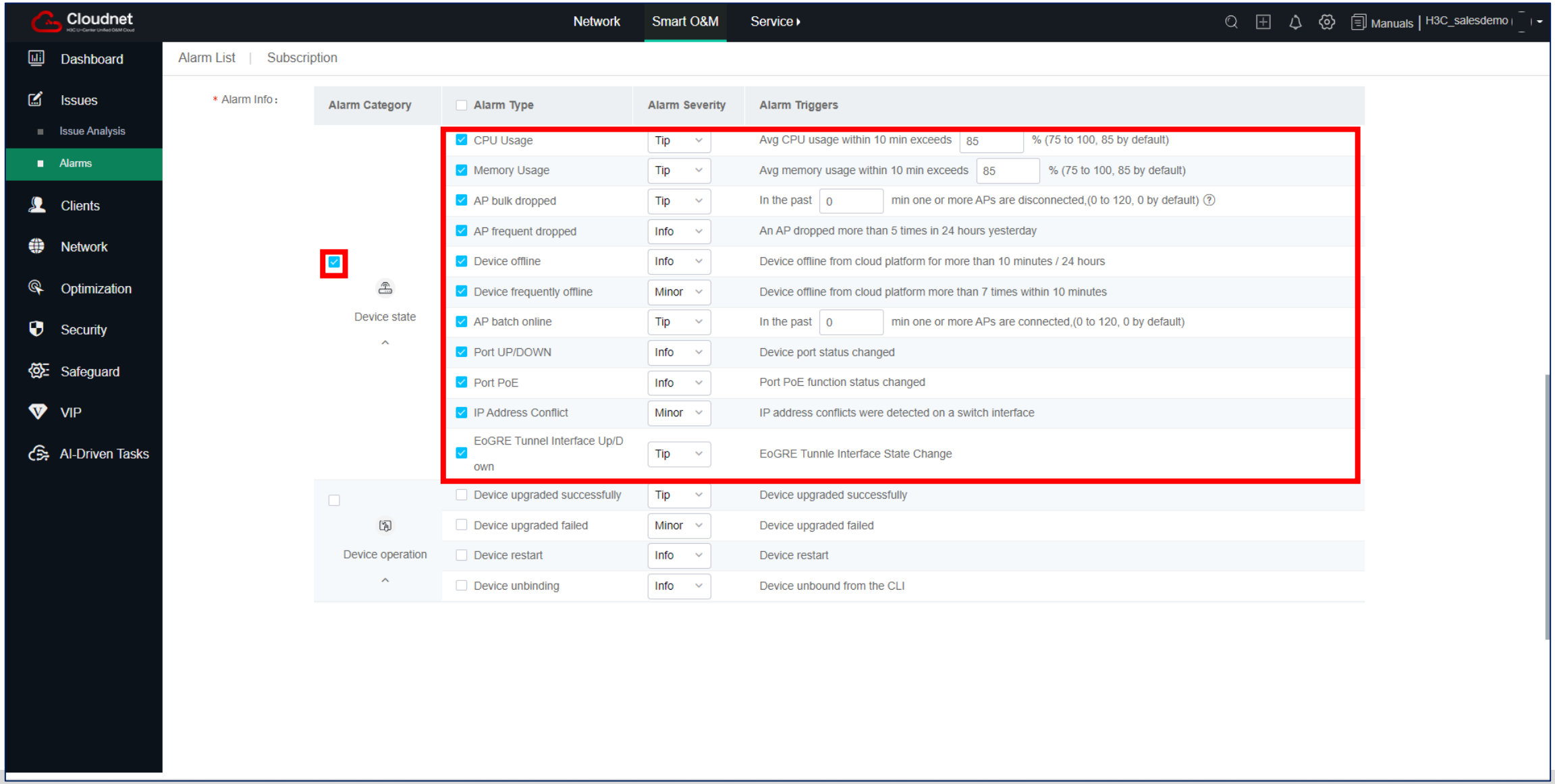
Cloudnet検知した攻撃を管理者にメールで伝える(続き)

- スマートO&M > 問題 > アラーム > 警報購読

アラームを検知した場合、「メール警報」を選択し、警報を送信するメールアドレスを選択します。
メールアドレスは管理者のアドレスとなります。

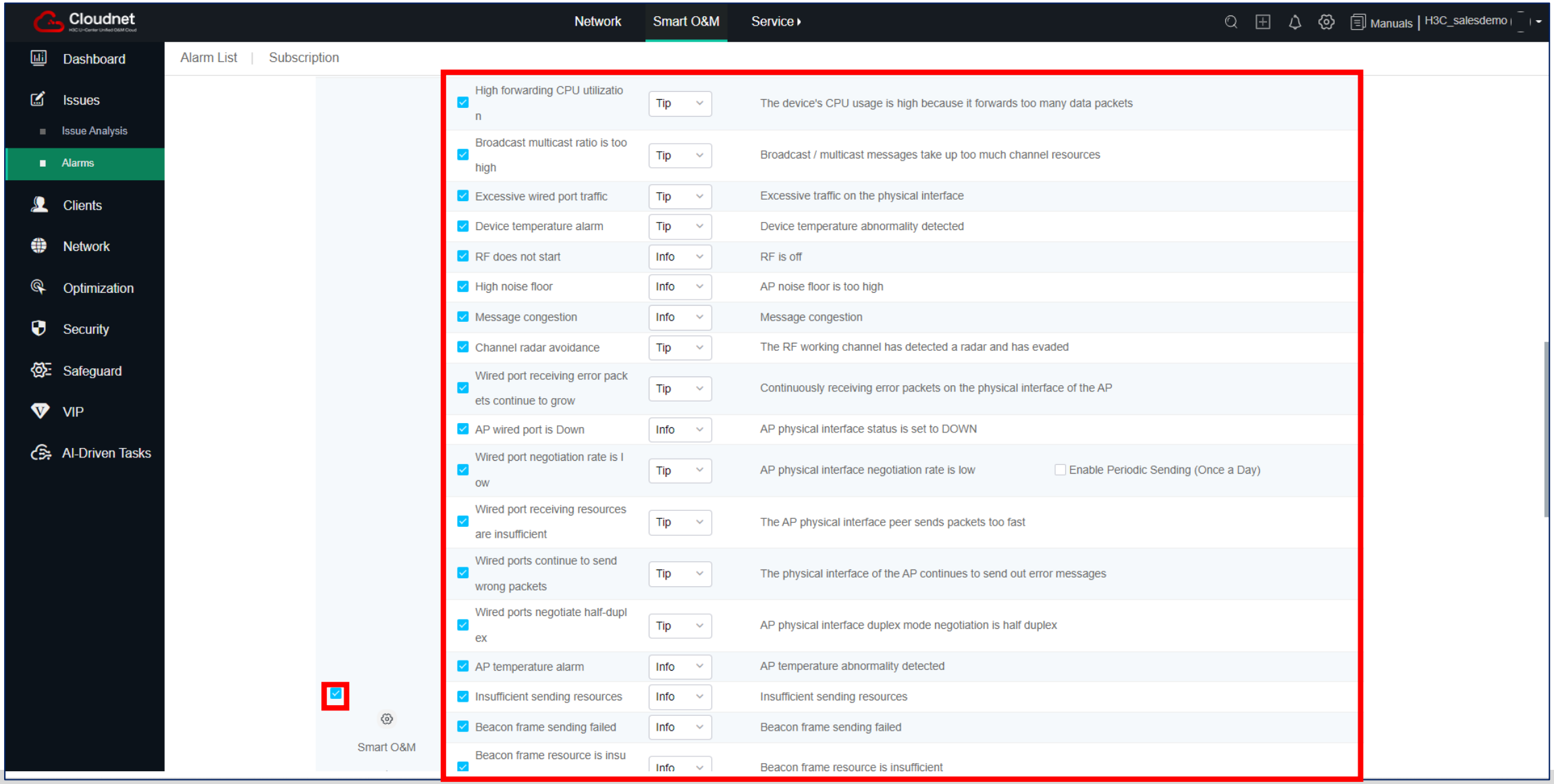
Cloudnet検知した攻撃を管理者にメールで伝える(続き)

- 警報分類 > Device stateとSmart O&Mからの警報を通知する



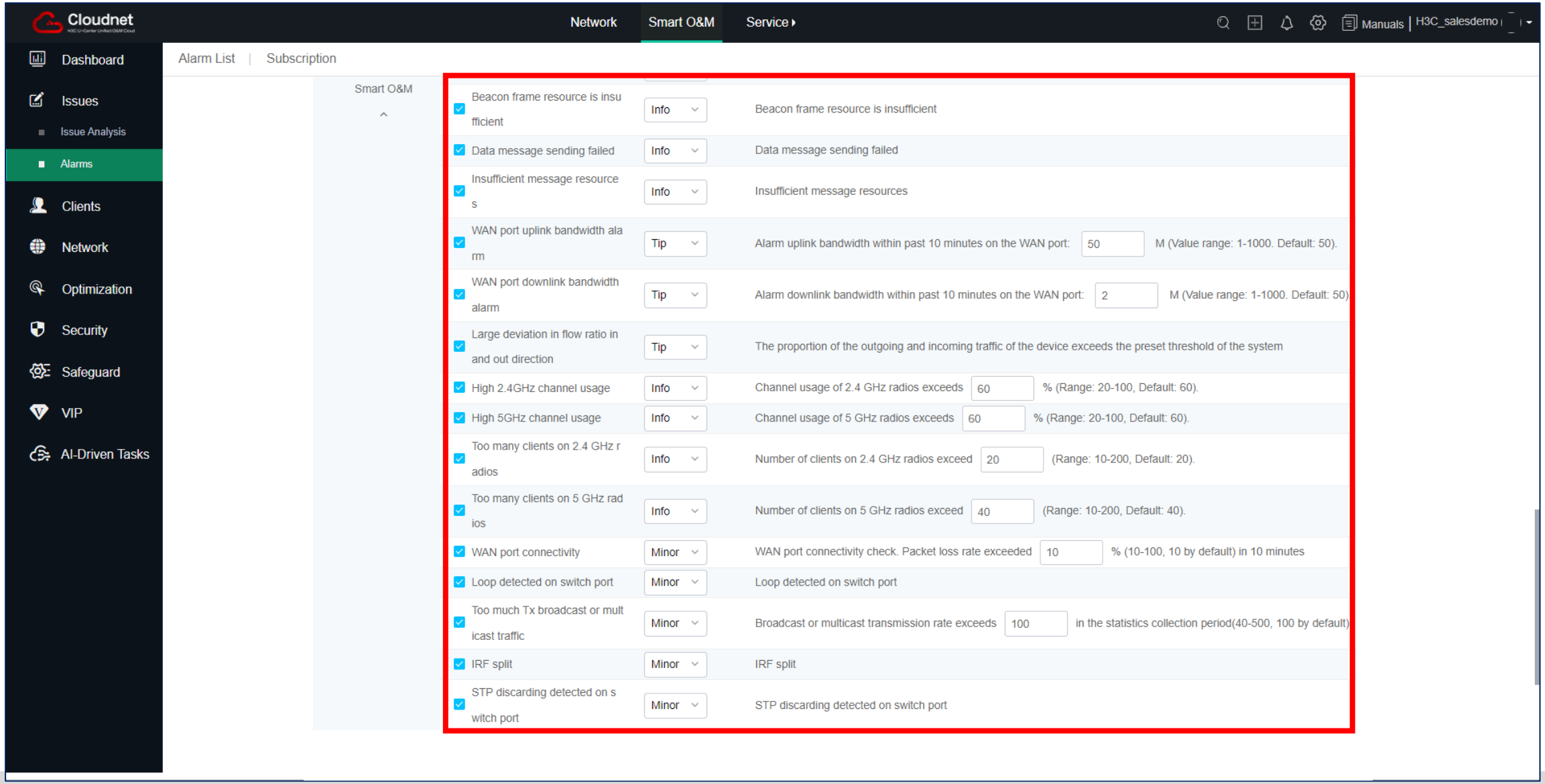
Cloudnet検知した攻撃を管理者にメールで伝える(続き)

- 警報分類 > Device stateとSmart O&Mからの警報を通知する



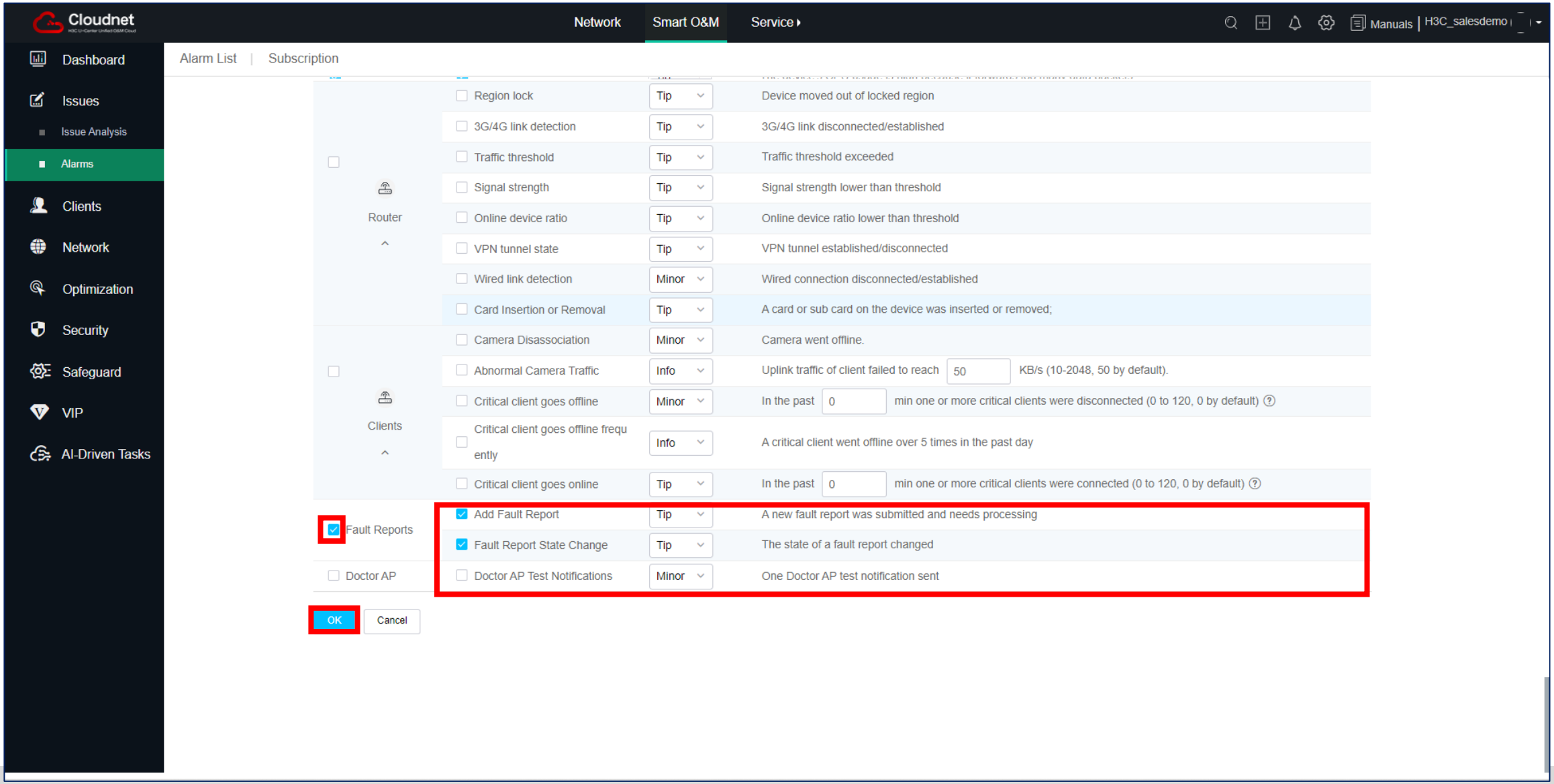
Cloudnet検知した攻撃を管理者にメールで伝える(続き)

- 警報分類 > Device stateとSmart O&Mからの警報を通知する



Cloudnet検知した攻撃を管理者にメールで伝える(続き)

- 警報分類 > Device stateとSmart O&Mからの警報を通知する



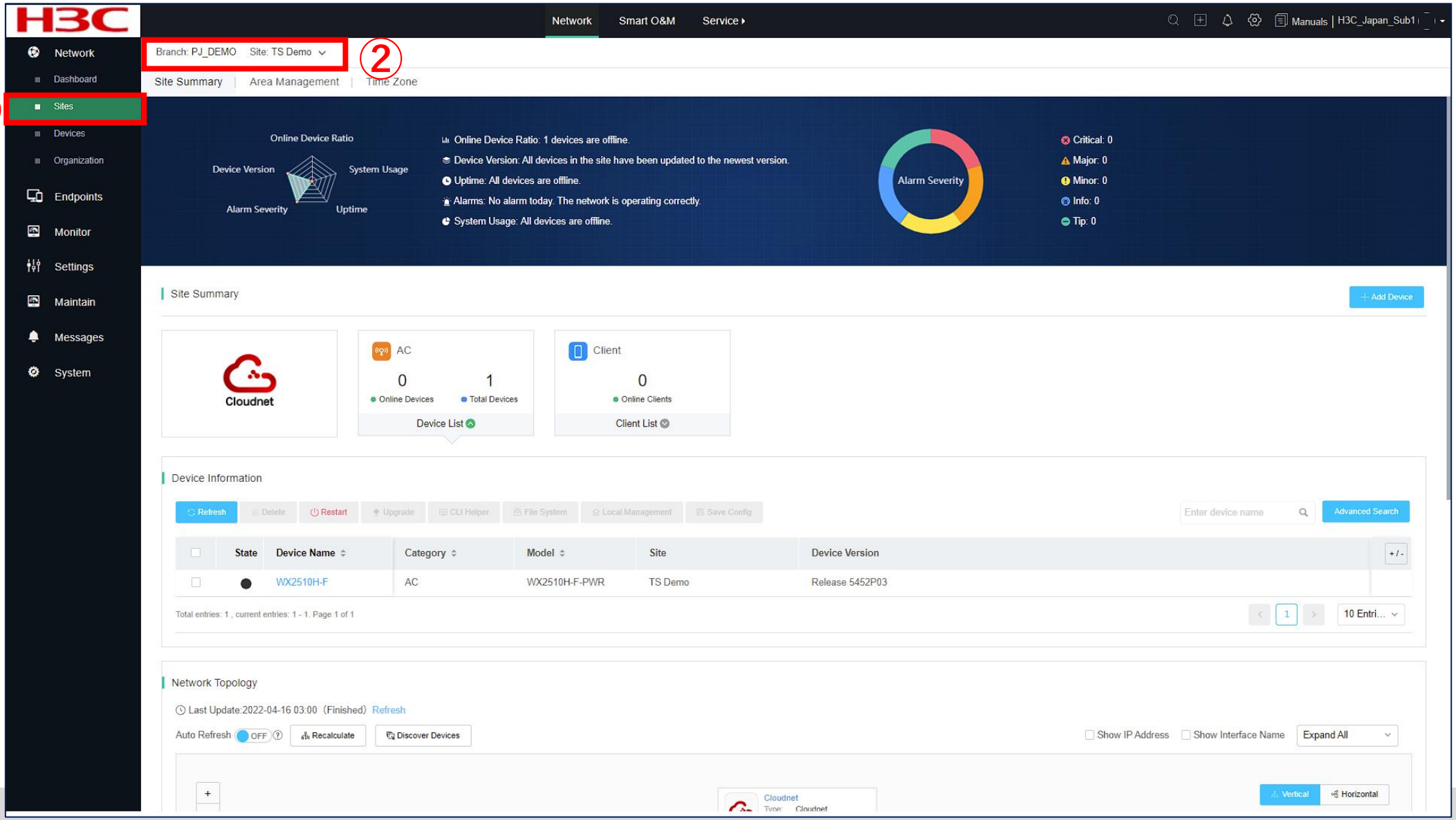
受信したアラートメールの例

From: <cloudnet@oasisinfo.h3c.com>
日付: 2022年4月12日(火) 10:46
件名: Cloud platform-Alarm
To: <site_manager@h3c.com>

Cloud platform-Alarm The device WX1840H_DEMO in the TS Demo site outgoing and incoming traffic ratio exceeds the system pre-made threshold, and there may be a large number of broadcast message replication.

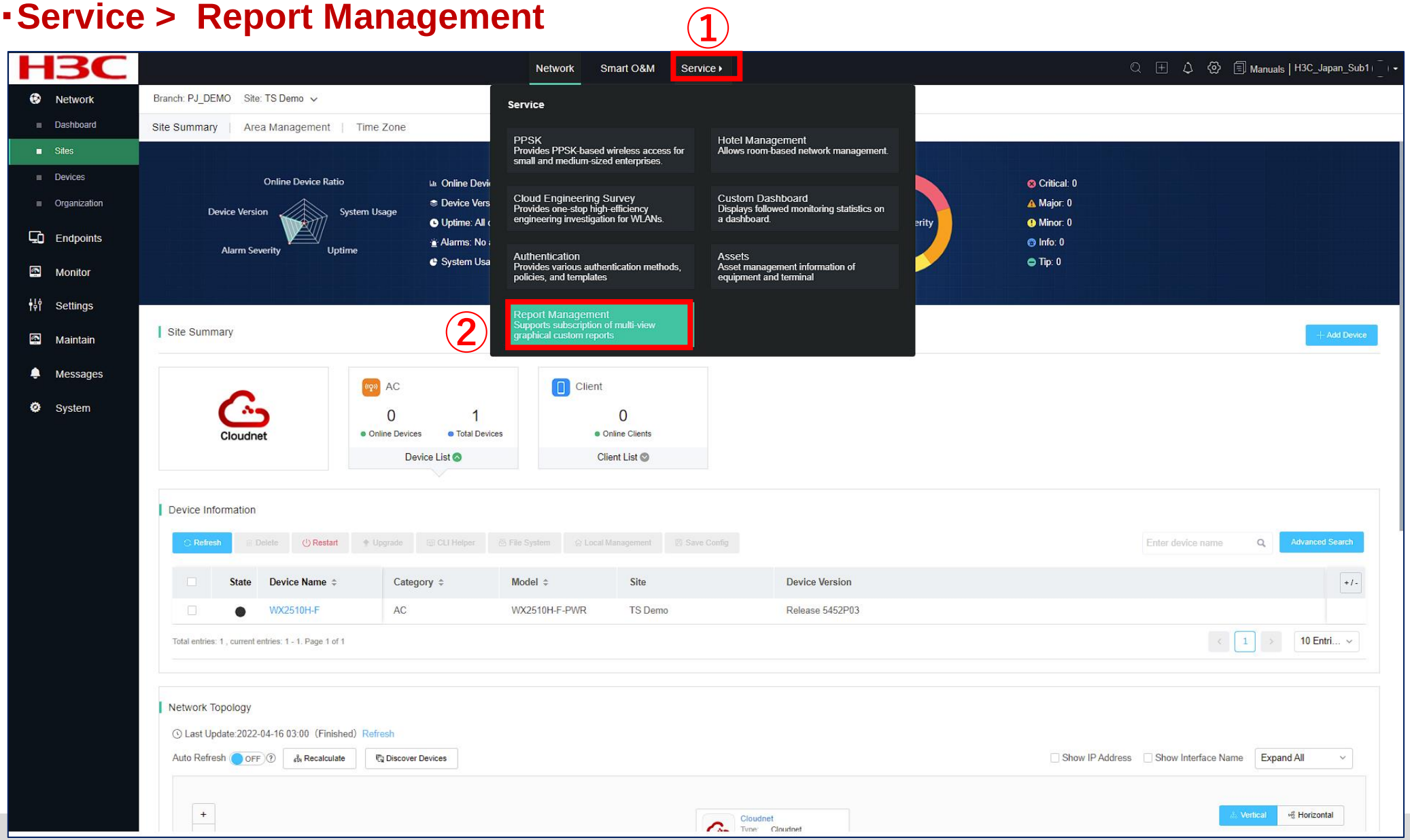
装置のあるサイトを選択します

- Sites > Branch >Site

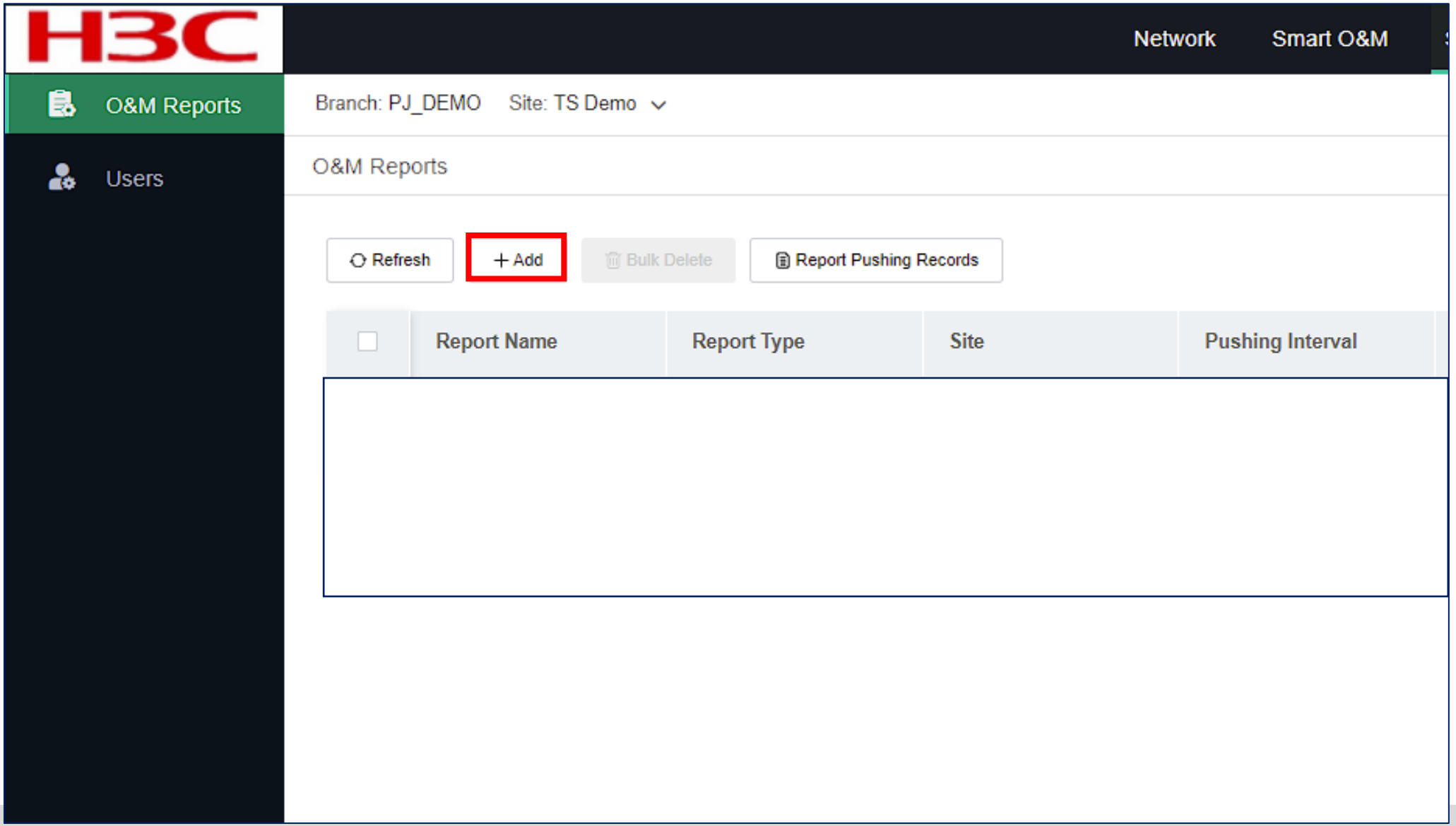


ServiceタブからReport Managementを選択します

・Service > Report Management

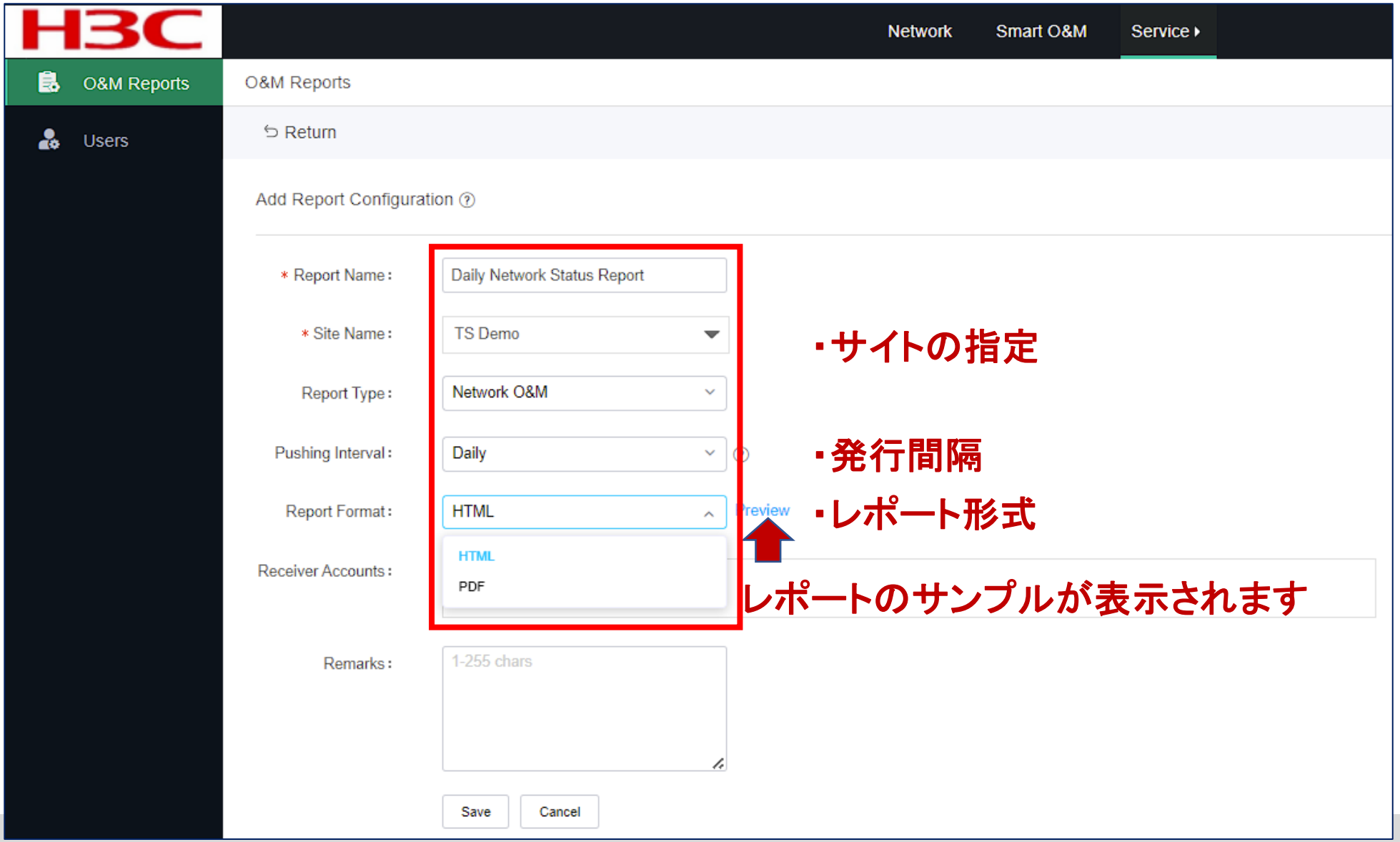


O&M Reportsの+ Addを選択します



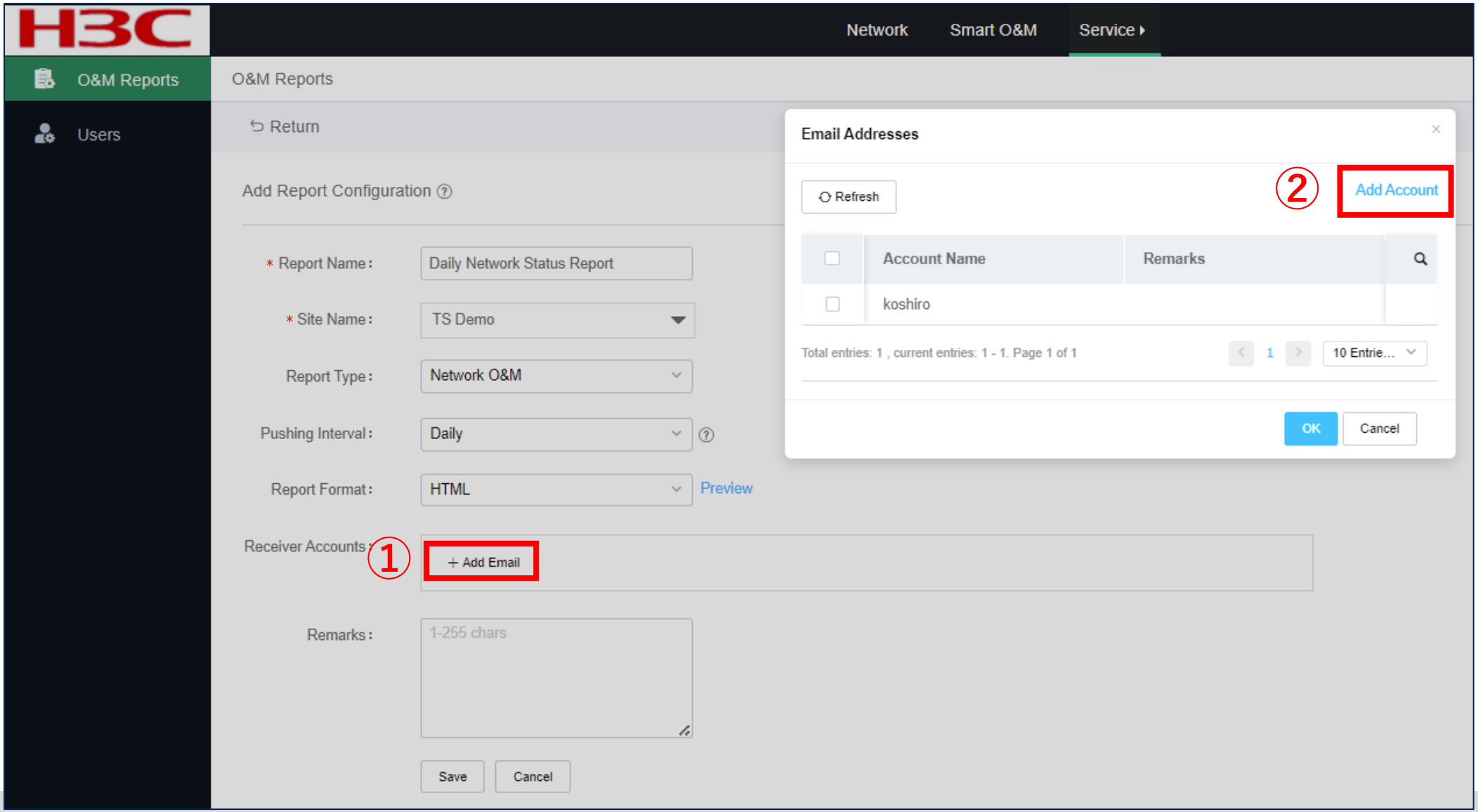
サイト,発行間隔、レポート形式を選択します

・Service > Report Management



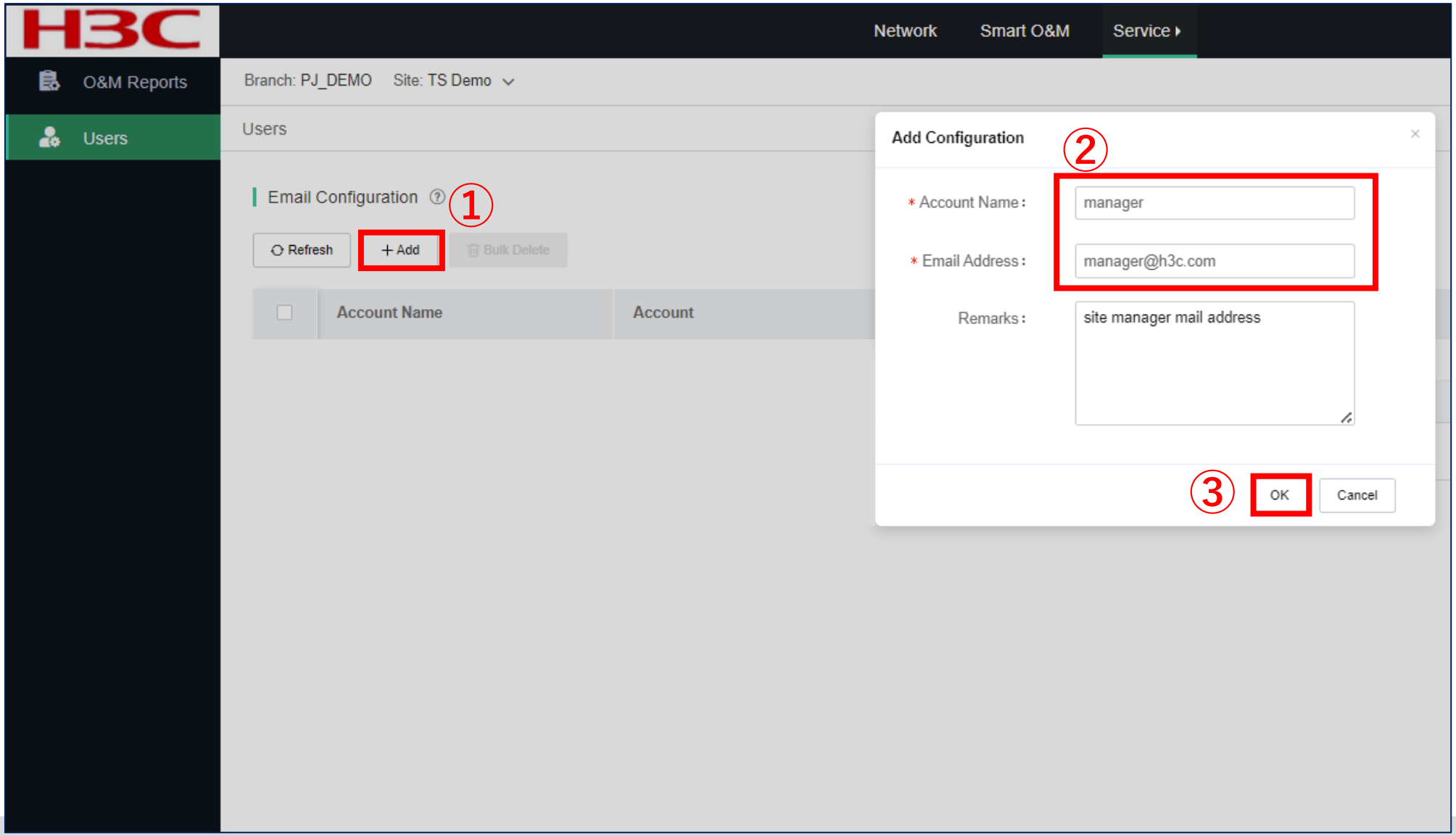
メールの送信先を指定します

・メールの送信先が登録されていない場合、Add Accountをクリックします

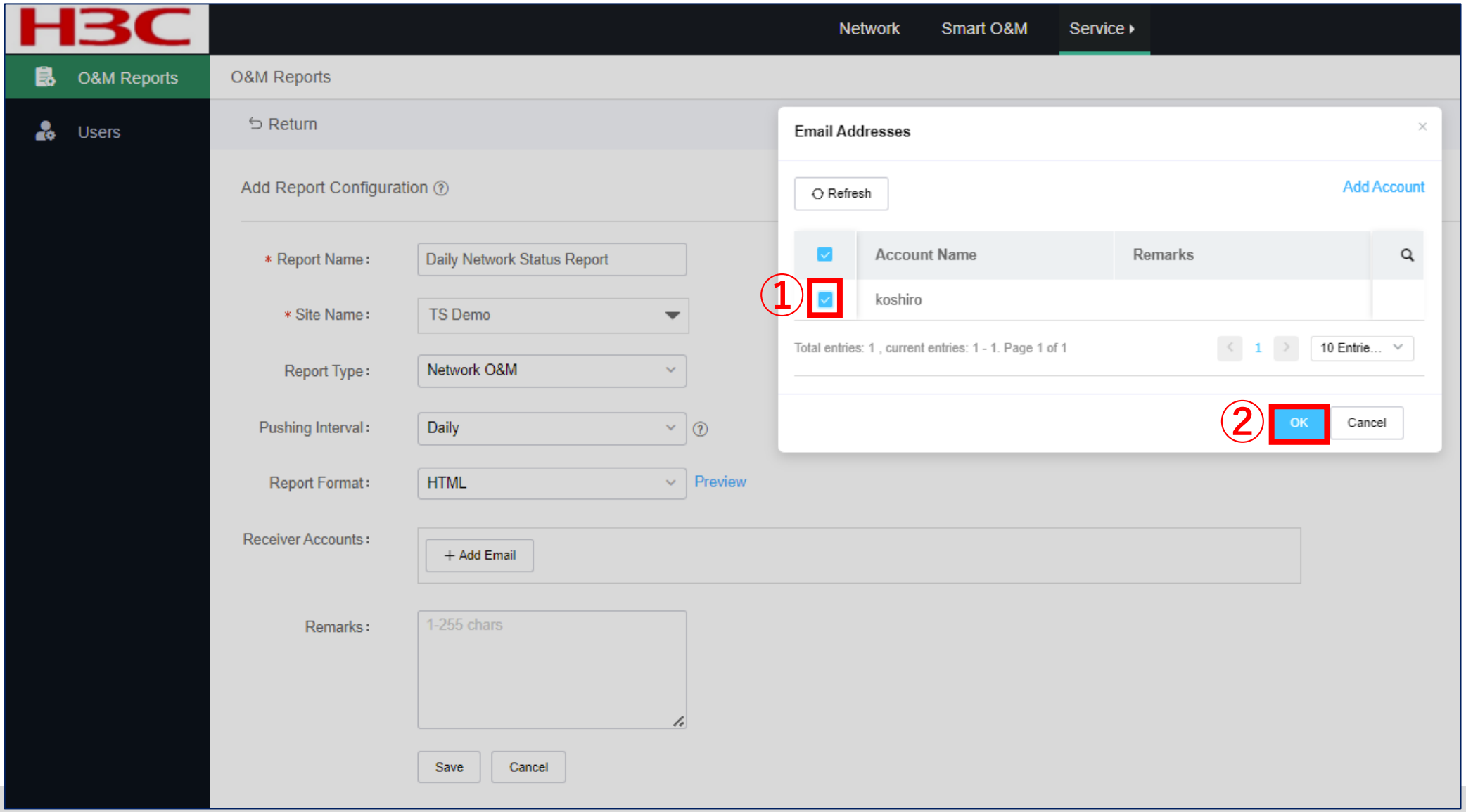


メールの送信先を登録します

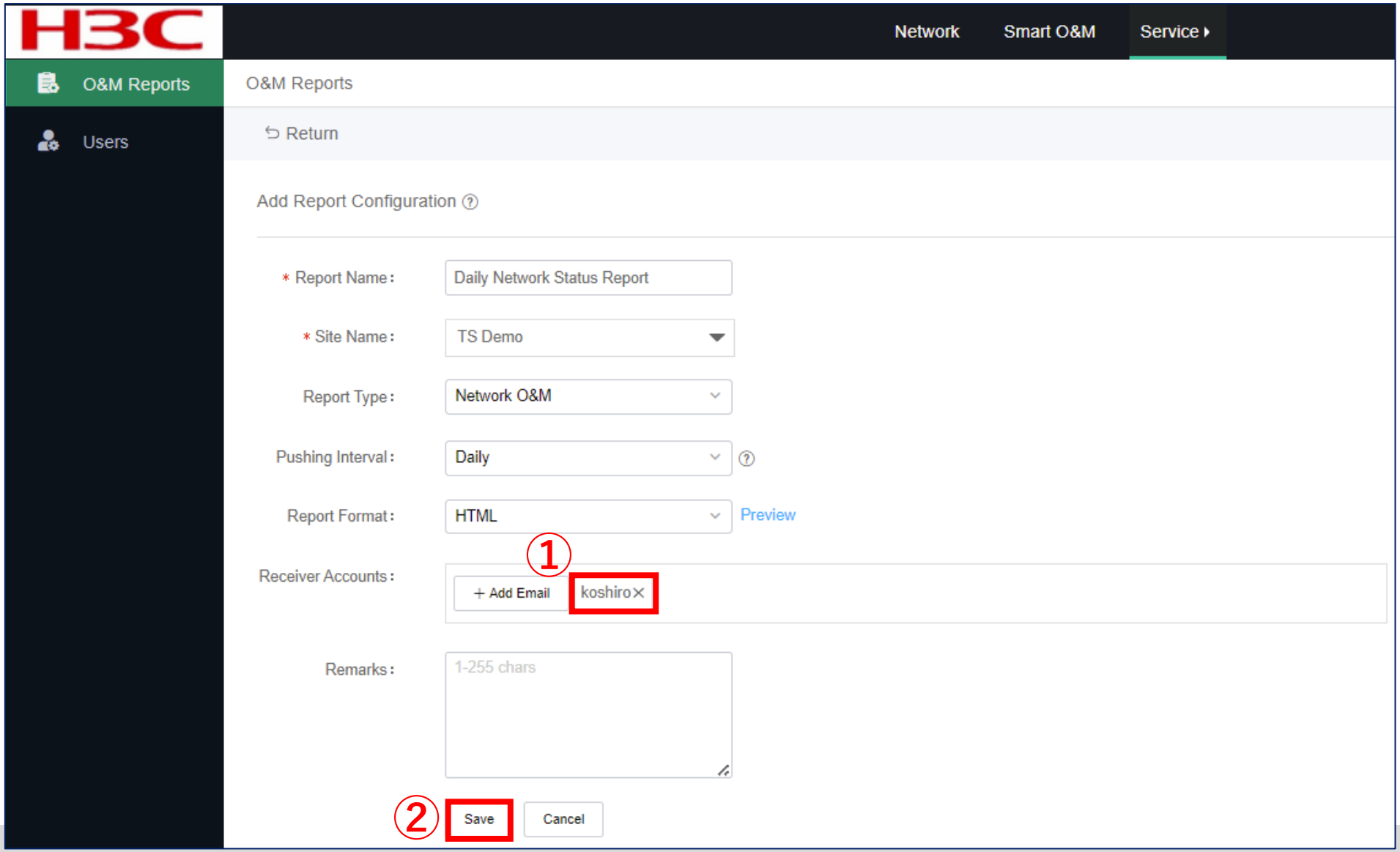
- +Addをクリック > Account Name, Email Addressを入力します



登録したメールアドレスを選択します

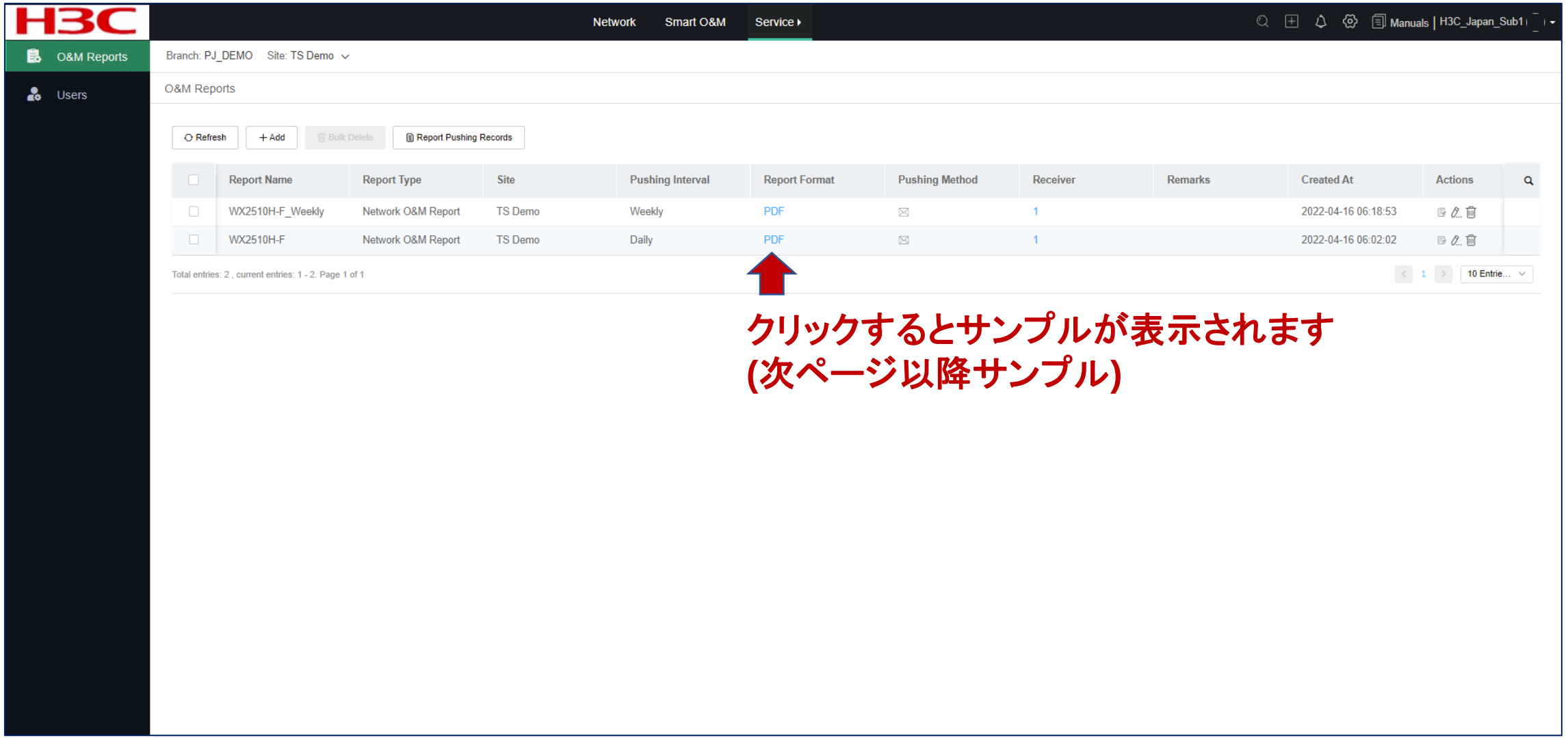


登録したメールアドレスが表示されたことを確認してsave



登録されました

- 以下の例ではDaily, Weeklyの両方のレポートを受け取るように設定したものです



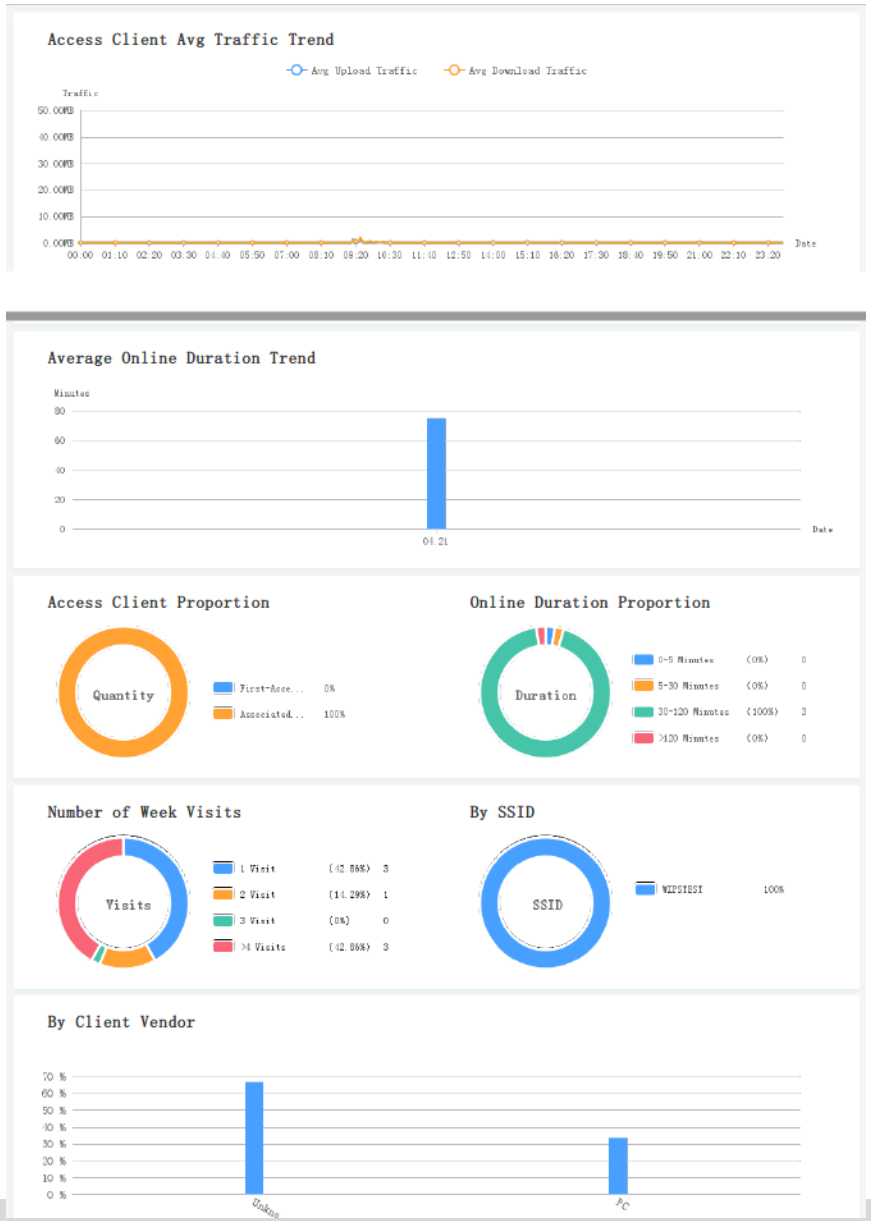
クリックするとサンプルが表示されます
(次ページ以降サンプル)

受信したReportメールの例

差出人: cloudnet@oasisinfo.h3c.com
日時: 2022年4月22日 7:01:22 JST
宛先: site_manager@h3c.com
件名: Cloudnet report

Click here for details :http://oasiscloudportal.h3c.com/group1/M00/00/6B/CgAAHmJhARl5gAAS_rJvrMmw139.pdf

Daily Reportのサンプルです



Cloudnet環境 -ACをCloudnetに登録

Cloudnet(旧名称：Oasis)はクラウドのH3C製品管理プラットフォームです。これは始めるのが簡単で、かつ機能は豊富です。

1.**装置がインターネットにアクセスできて**、DNSの名前解決ができること(固定IPでアクセスポイントを管理する場合はDNSの設定(例えば[H3C]dns server 8.8.8.8)などを忘れずに)

2.**firewallで以下のポートがオープン**であること

- ログイン、認証用ポート
  TCP 80
  TCP 443
- Cloudnet通信用ポート
  TCP 19443
- NTPサーバー用ポート
  UDP 123

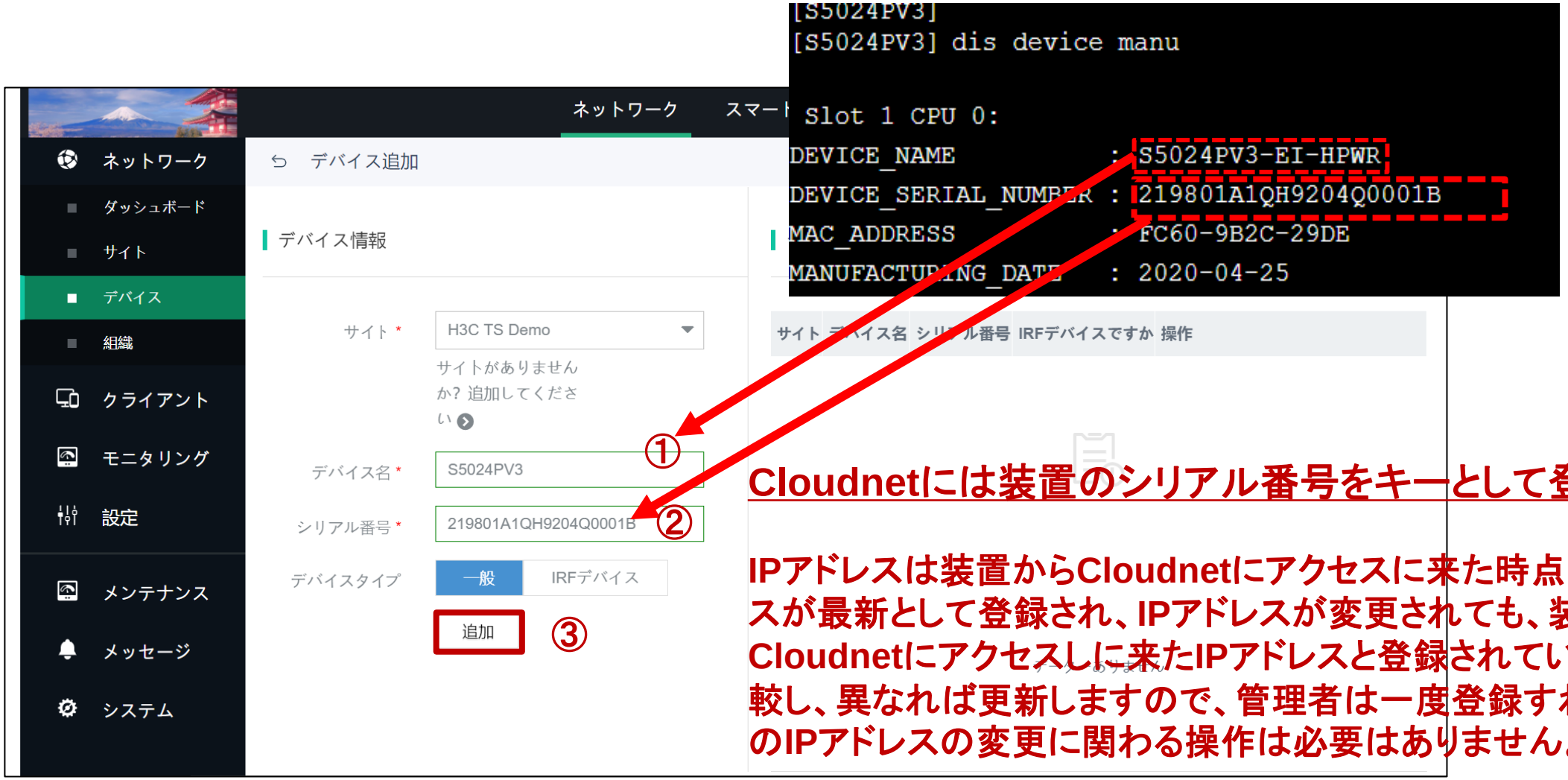
2.**装置のシリアル番号が分かっている**(<H3C>display device manuinfoコマンドで表示)

3.装置には予め以下のコマンドを投入してあること
[H3C]**cloud-management server domain oasiscloud.h3c.com**

4.Cloudnetにログインアカウントを作成し、ログインして装置を登録、管理を行います。

Cloudnet環境 –ACをCloudnetに登録

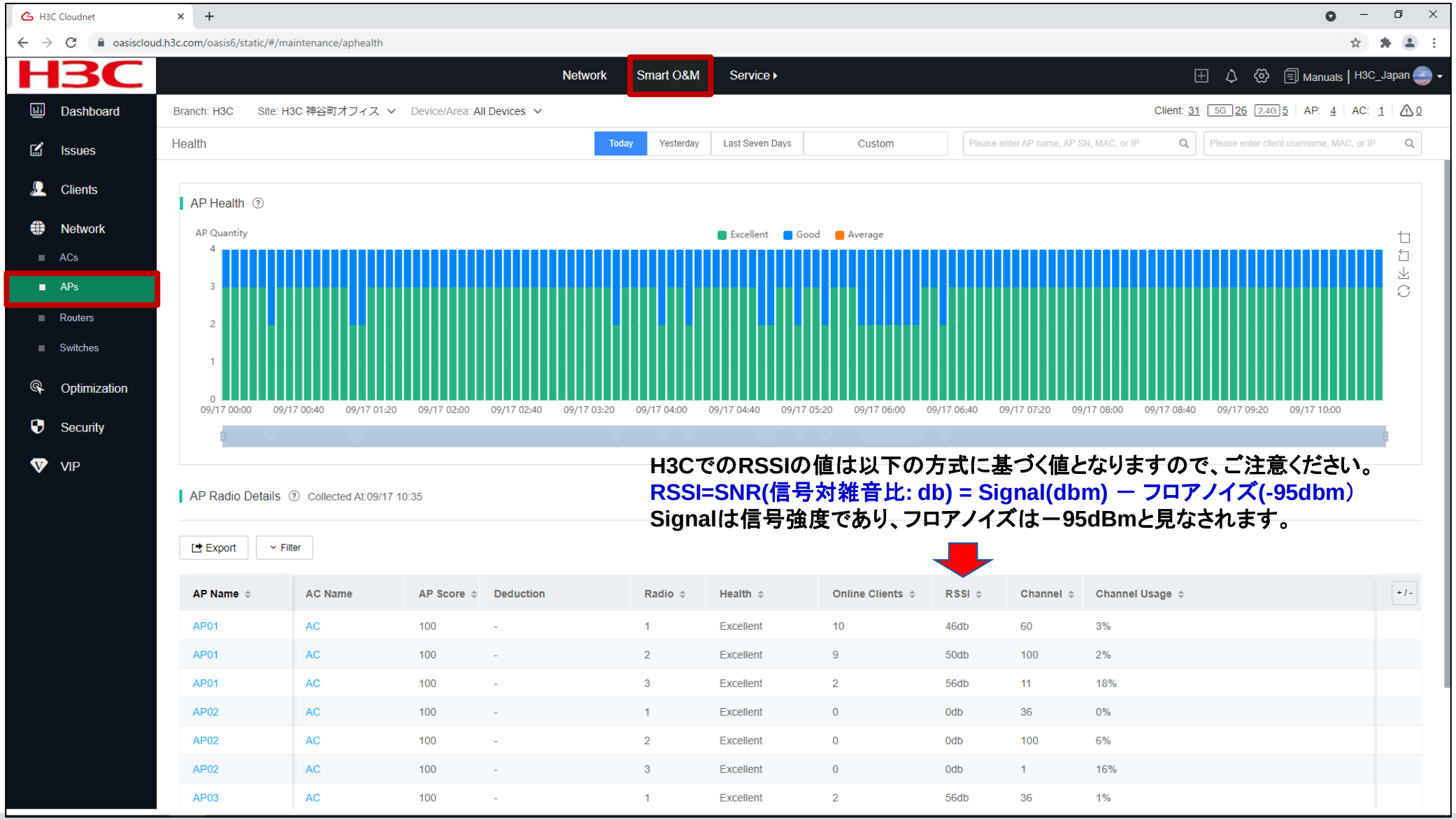
- ネットワーク > デバイス > デバイス追加



Cloudnetには装置のシリアル番号をキーとして登録します

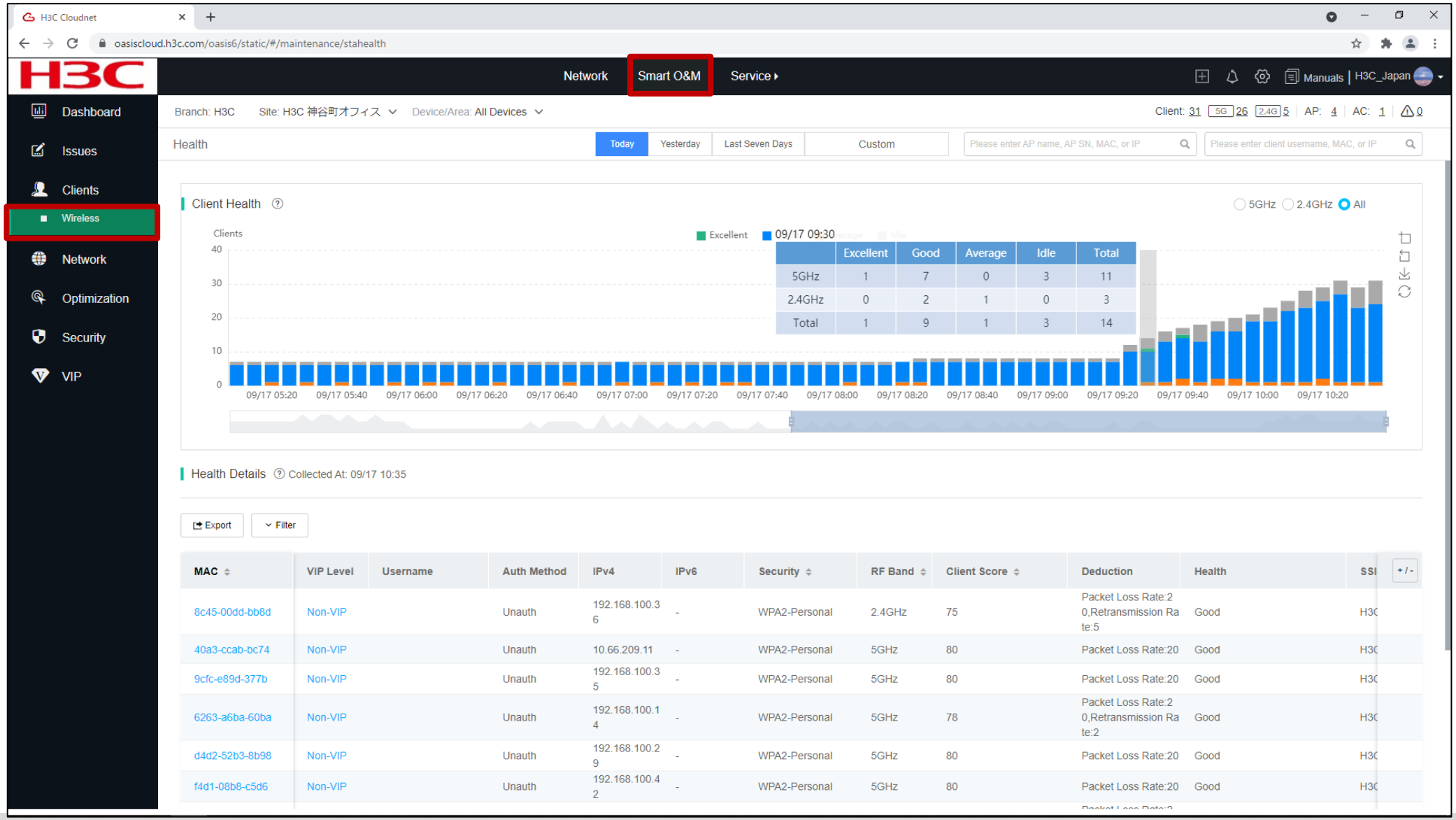
IPアドレスは装置からCloudnetにアクセスに来た時点のIPアドレスが最新として登録され、IPアドレスが変更されても、装置からCloudnetにアクセスしに来たIPアドレスと登録されているものを比較し、異なれば更新しますので、管理者は一度登録すれば、装置のIPアドレスの変更に関わる操作は必要はありません。

Cloudnetの活用例 – APの健康度チェック

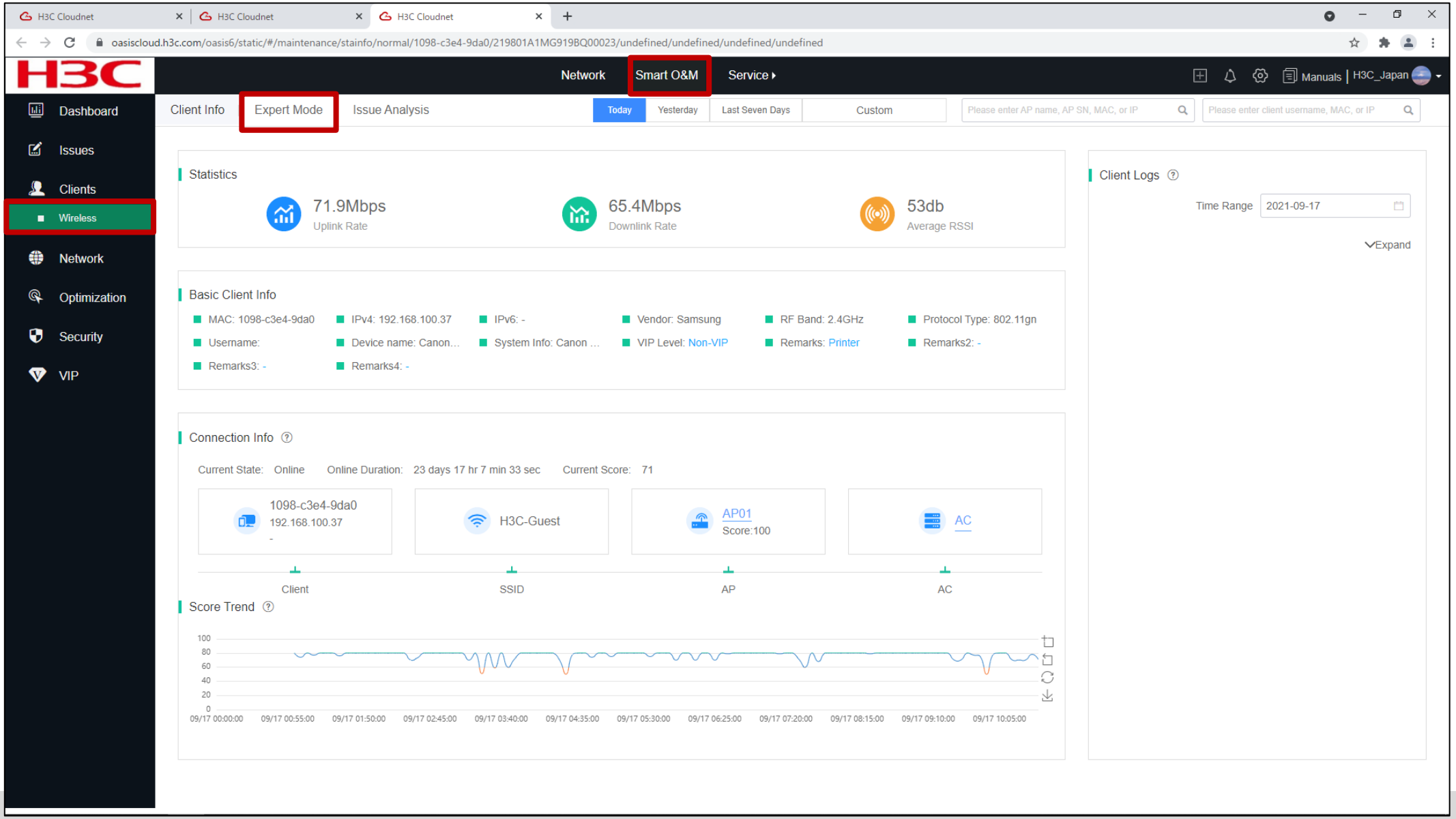


H3CでのRSSIの値は以下の方式に基づく値となりますので、ご注意ください。
RSSI=SNR(信号対雑音比: db) = Signal(dbm) ー フロアノイズ(-95dbm)
Signalは信号強度であり、フロアノイズは－95dBmと見なされます。

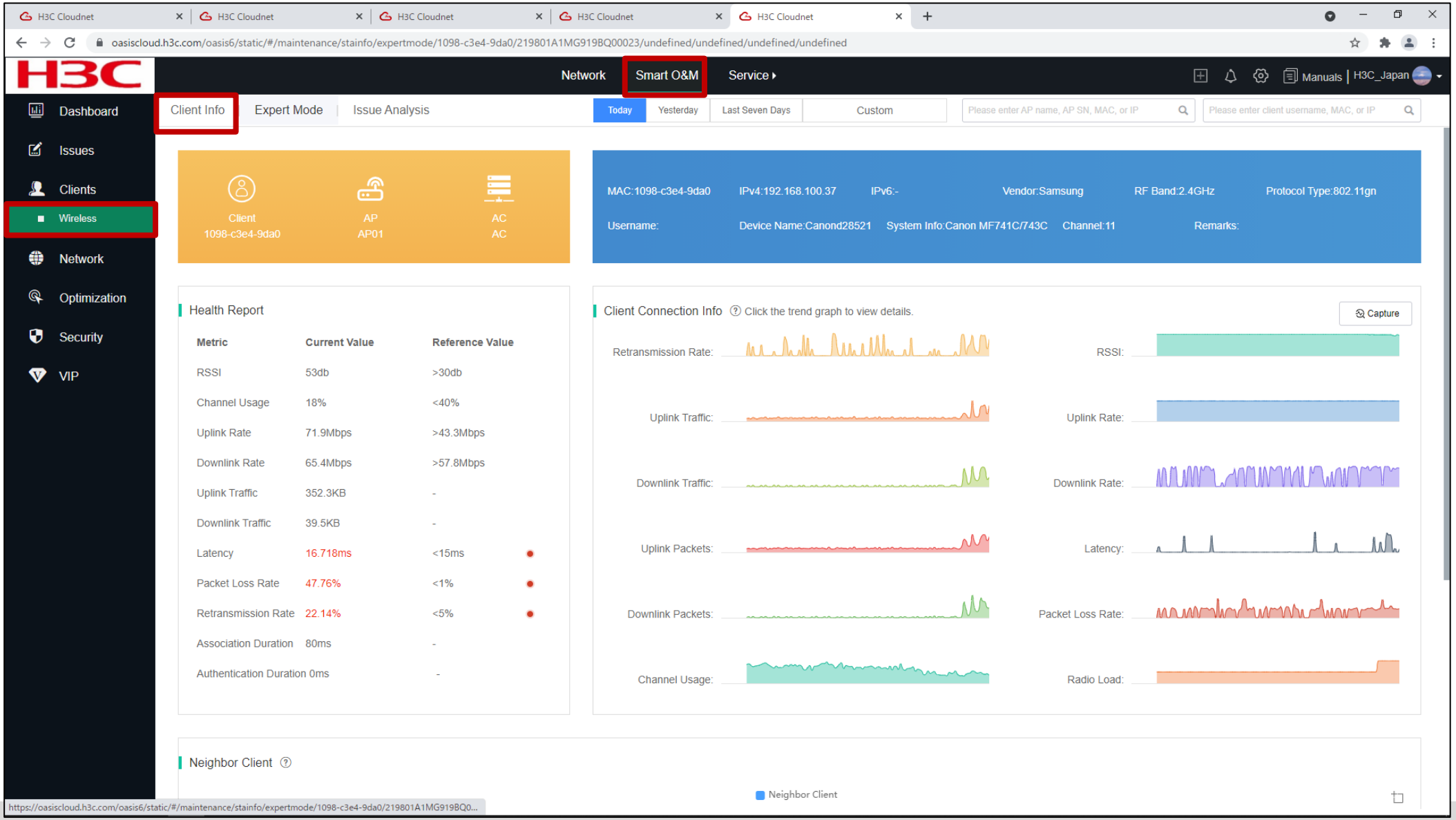
Cloudnetの活用例 – クライアント端末の健康度



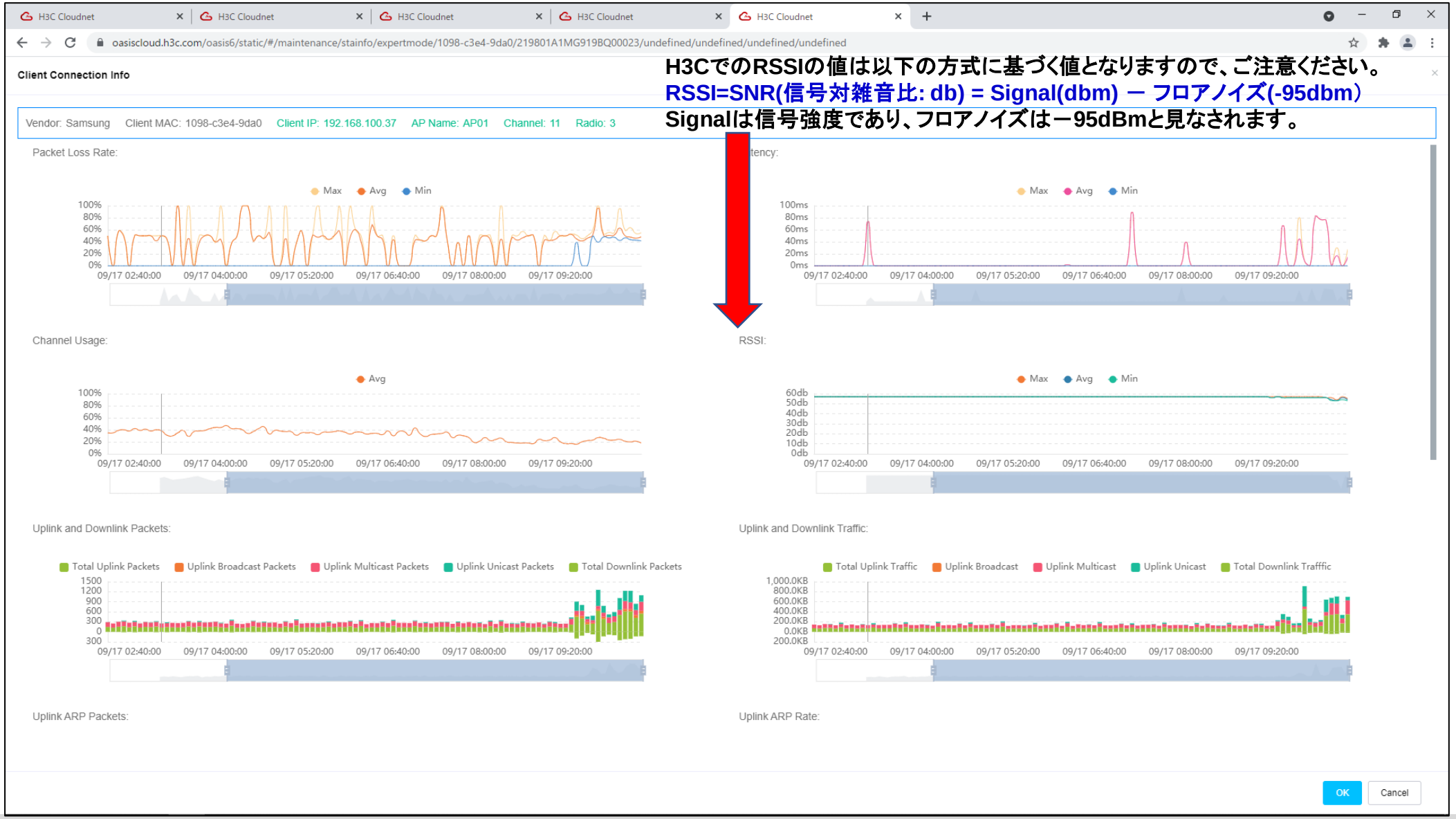
Cloudnetの活用例 – Expert Mode表示



Cloudnetの活用例 - Expert Mode表示



Cloudnetの活用例 – クライアントのRSSI等

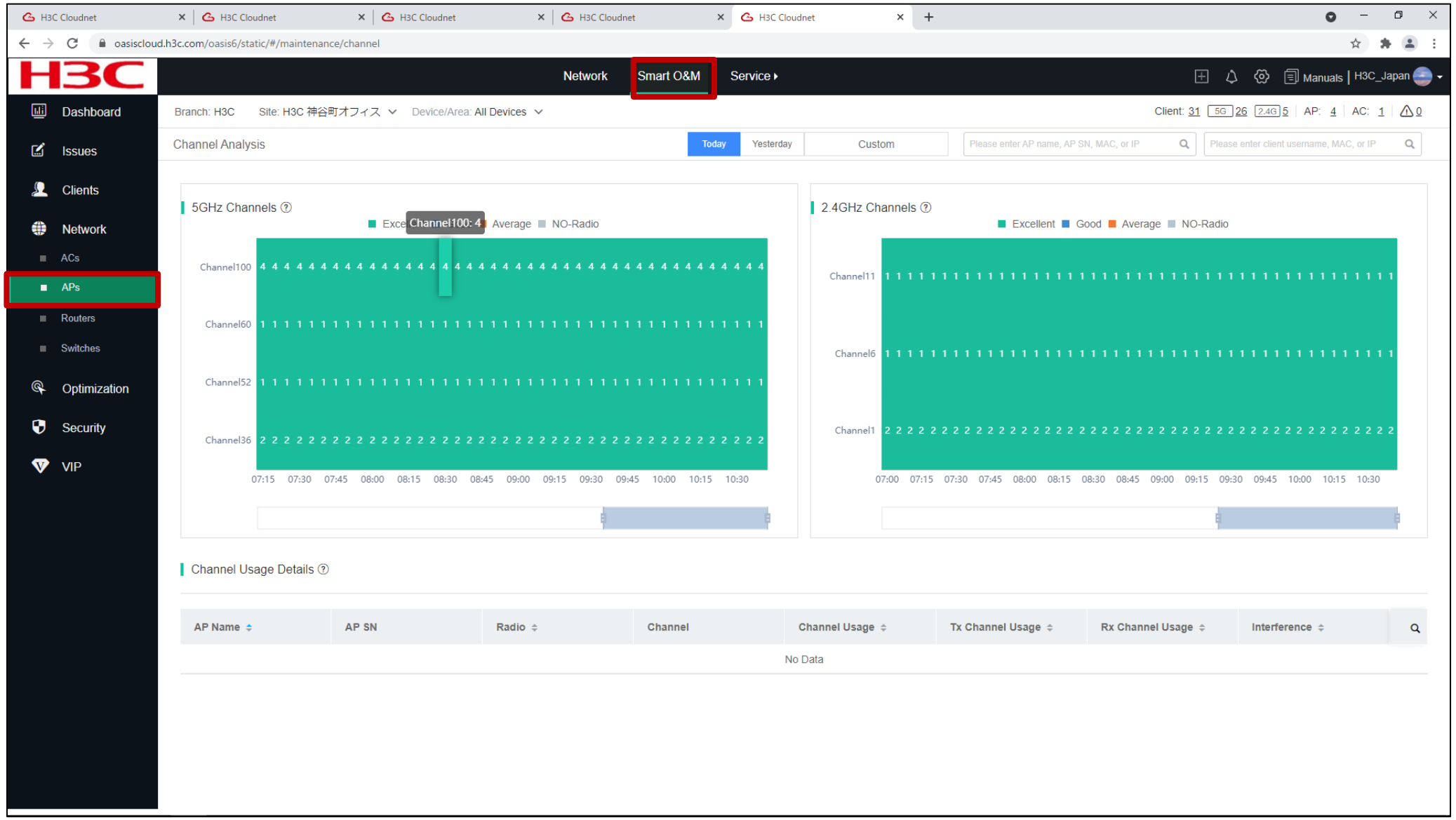


Cloudnetの活用例 – クライアントのRSSI等

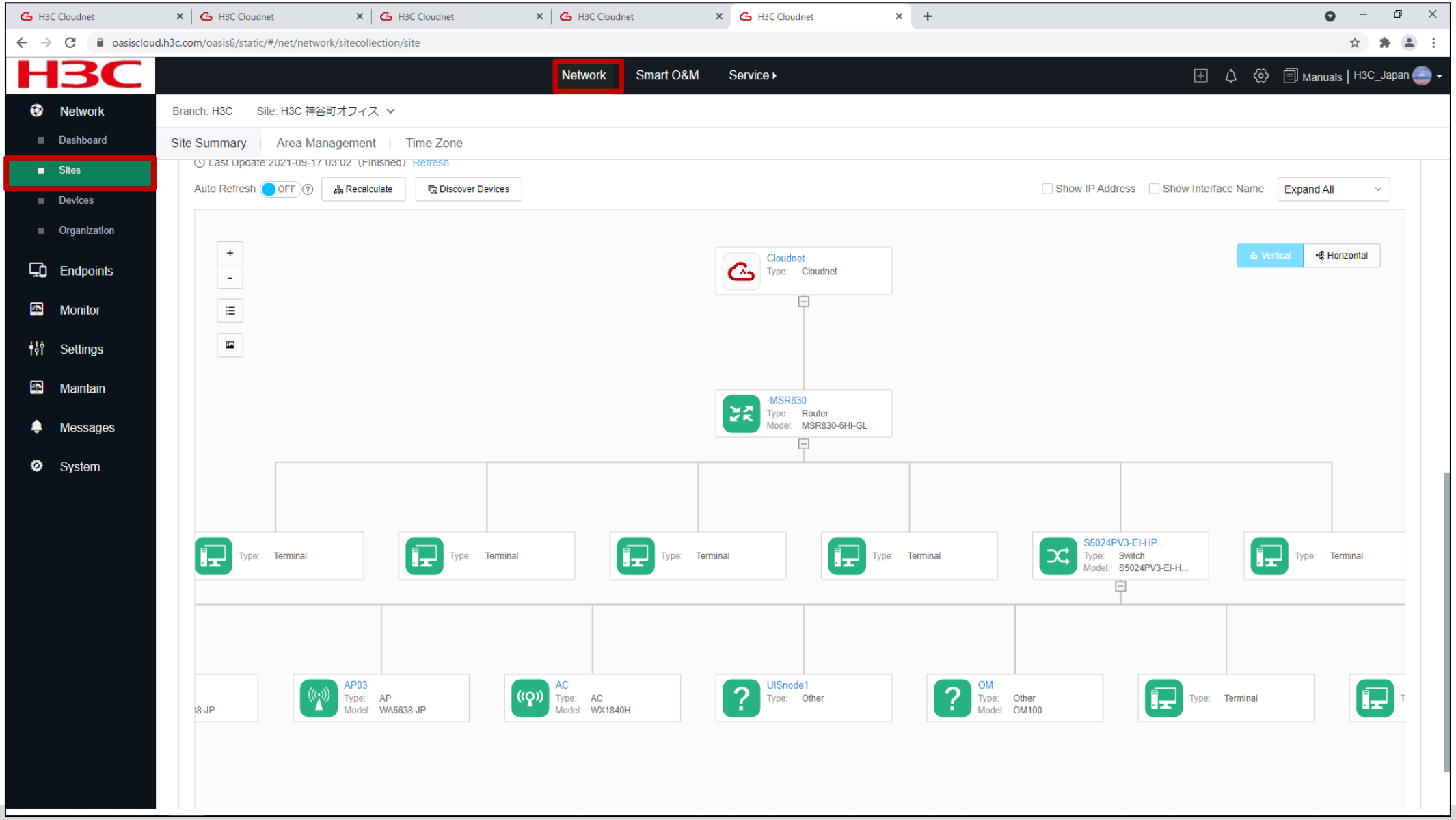
RSSI ＝SNR (信号対雑音比: db) = Signal(dbm) ー フロアノイズ(-95dbm）

RSSI(db)	dBM	評価
40以上	-55	非常に信頼性が高くリアルタイムの通信が可能な水準
25～40	-70～-55	信頼性が高くリアルタイムの通信の最低限の水準
15～25	-80～-70	遅いが信頼性の高い通信の最低限の水準
10～15	-85～-80	遅く信頼性の低い水準
10以下	-85	使用に耐えない

Cloudnetの活用例 – APのチャネル利用状況



Cloudnetの活用例 - トポロジーマップ



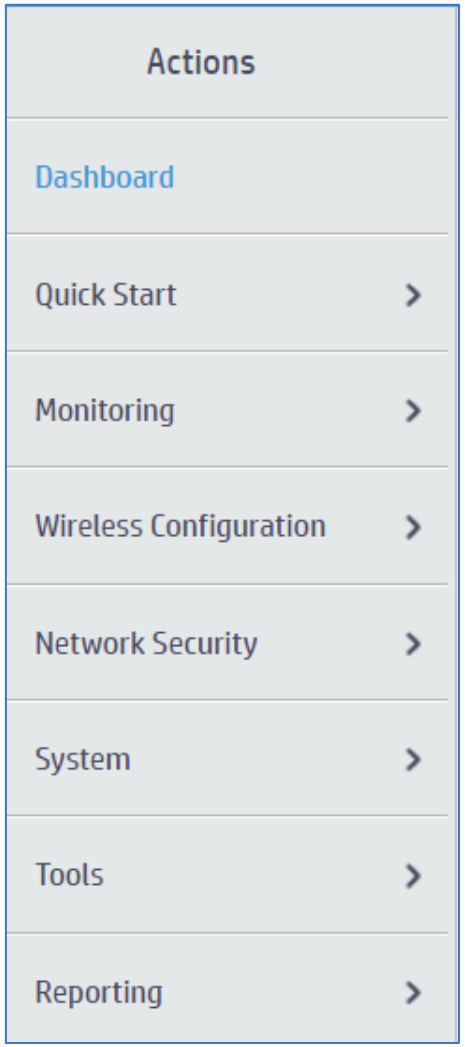
```
#
 version 7.1.064, Release 5452P02
#
 sysname WX1840H
#
 clock timezone JP add 09:00:00
 clock protocol ntp
#
wlan global-configuration
 region-code JP
#
 telnet server enable
#
 dhcp enable
#
 dns server 8.8.8.8
 dns server 114.114.114.114
#
 lldp global enable
#
 password-recovery enable
#
vlan 1
#
dhcp server ip-pool 1
 gateway-list 192.168.127.254
 network 192.168.127.0 mask 255.255.255.0
 dns-list 8.8.8.8
#
wlan service-template 1
 ssid WIPSTEST
 akm mode psk
 preshared-key pass-phrase simple h3cjapan
 cipher-suite ccmp
 cipher-suite tkip
 security-ie rsn
 security-ie wpa
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.127.254 255.255.255.0
#
interface GigabitEthernet1/0/7
 port link-mode route
 ip address dhcp-alloc
 nat outbound
#
interface GigabitEthernet1/0/8
 port link-mode route
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
interface GigabitEthernet1/0/2
 port link-mode bridge
#
interface GigabitEthernet1/0/3
 port link-mode bridge
#
interface GigabitEthernet1/0/4
 port link-mode bridge
#
interface GigabitEthernet1/0/5
 port link-mode bridge
#
interface GigabitEthernet1/0/6
 port link-mode bridge
#
 scheduler logfile size 16
#
line class console
 user-role network-admin
#
line class vty
 user-role network-operator
#
line con 0
 user-role network-admin
#
line vty 0 31
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
#
 undo info-center logfile enable
 info-center loghost 192.168.127.2
 info-center source WIPS loghost level
notification
 info-center source STAMGR loghost level
informational
#
 ssh server enable
#
 ntp-service enable
 ntp-service unicast-server ntp.nict.jp
#
domain system
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
```

```
#
local-user admin class manage
 password simple h3cjapan
 service-type ftp
 service-type ssh telnet terminal http https
 authorization-attribute user-role network-admin
#
 ftp server enable
#
 netconf soap http enable
#
 ip http enable
 ip https enable
#
 wlan auto-ap enable
 wlan auto-persistent enable
 wlan tcp mss 1360
#
wlan ap-group default-group
 vlan 1
#
wlan virtual-ap-group default-virtualapgroup
#
wlan ap 00dd-b6b1-4540 model WA6320-JP
 serial-id 219801A2YF821BE000B0
 vlan 1
 wips virtual-security-domain sec_domain
 radio 1
  radio enable
  service-template wipstest
  wips enable
 radio 2
  radio enable
  service-template wipstest
  wips enable
 gigabitethernet 1
#
wips
 #
 countermeasure policy stop_attack
  countermeasure attack honeypot-ap
  countermeasure attack man-in-the-middle
  select sensor all
 #
 detect policy standard
  ap-rate-limit threshold 256
  client-rate-limit threshold 512
  ap-impersonation
  honeypot-ap
  man-in-the-middle
#
virtual-security-domain sec_domain
 apply countermeasure policy stop_attack
 apply detect policy standard
#
 cloud-management server domain cloudnet.h3c.com
#
return
```

Anchor-ACのGUIにログインします http://192.168.0.50/
User: admin , Password: h3capadmin

ACのGUIのメニュー一覧

- **Network view**



Dashboard

Quick Start
- Add Wireless Service
- Add New User

Monitoring
- Wireless Network
- Clients
- Wireless Security
- Client Proximity Sensor
- Application Monitoring

Wireless Configuration
- Wireless Networks
- AP Management
- Wireless QoS
- Wireless Security
  - WIPS
  - Allowlist and denylist
- Radio Management
  - 802.11n/802.11ax settings ,transmission distance
- Applications
  - Mesh, Multicast

Network Security
- Packet Filter
- Traffic Policy
  - Qos Policies, Priority Mapping
- Access Control
  - 802.1x
- Authentication
  - RADIUS
- User Management
- Access Control
  - MAC Authentication
  - Port Security
  - Portal

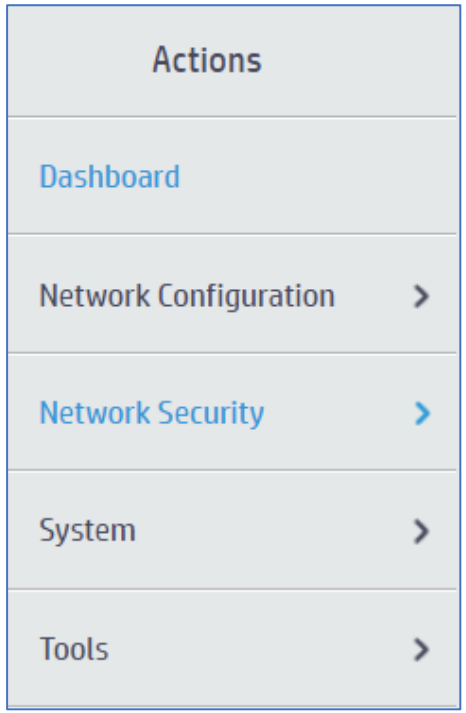
System
- Resource
  - ACL, Time Range
  - Cloud Platform

Tools
- Debug

Reporting
- Client Statistics
- Wireless Service Statistics

ACのGUIのメニュー一覧(続き)

- **System view**



Dashboard

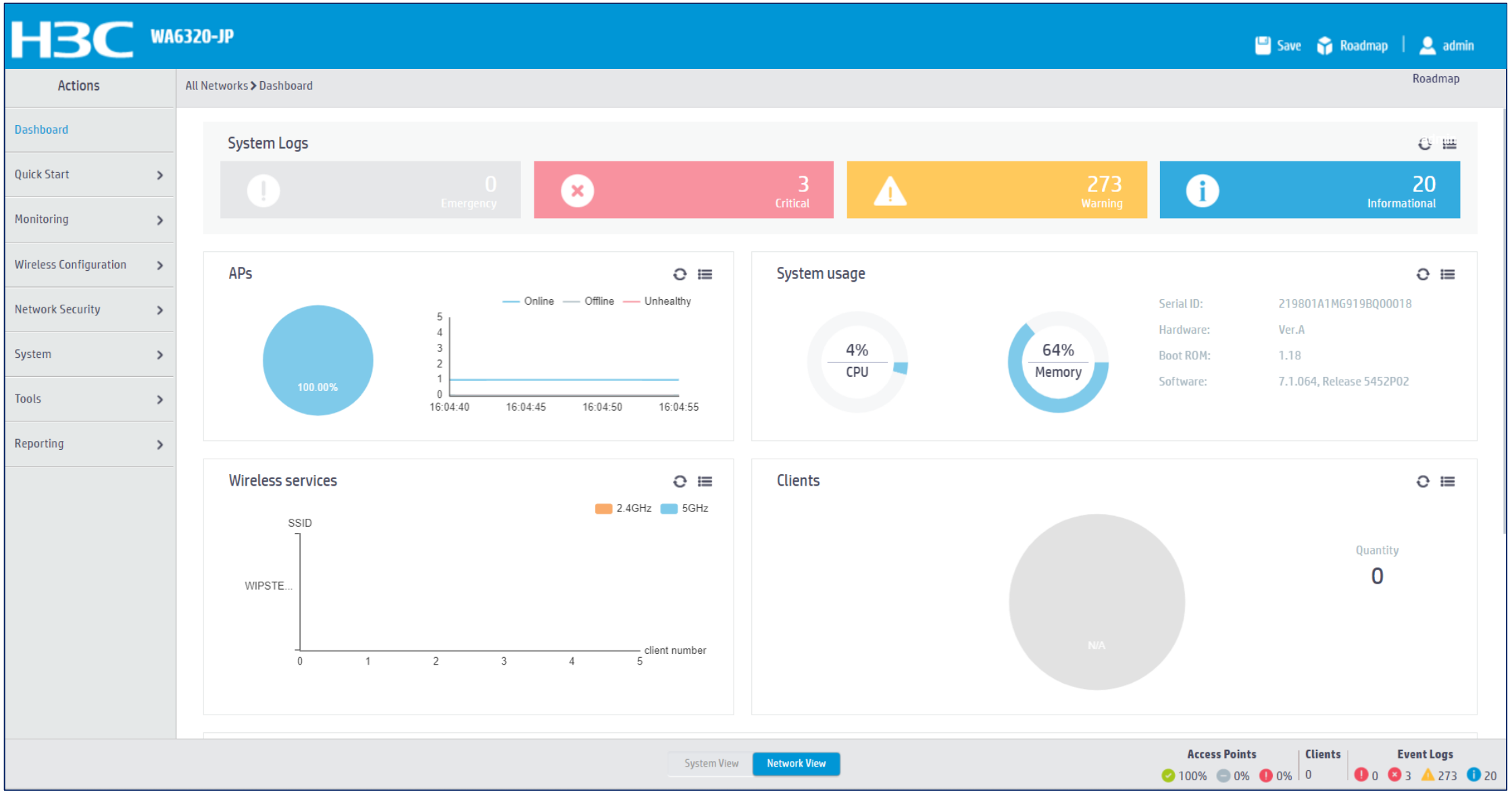
Network Configuration
- Network Interfaces
- VLAN
- Network Routing
  - Routing table
  - Static Routing
- Network Services
  - IP services
  - DHCP/DNS
  - Multicast
  - ARP
  - ND(Neighbor Discovery)
  - NAT

Network Security
- Packet Filter
- Traffic Policy
- Access Control
  - 802.1x
- Authentication
  - RADIUS
- User Management
  - Local users

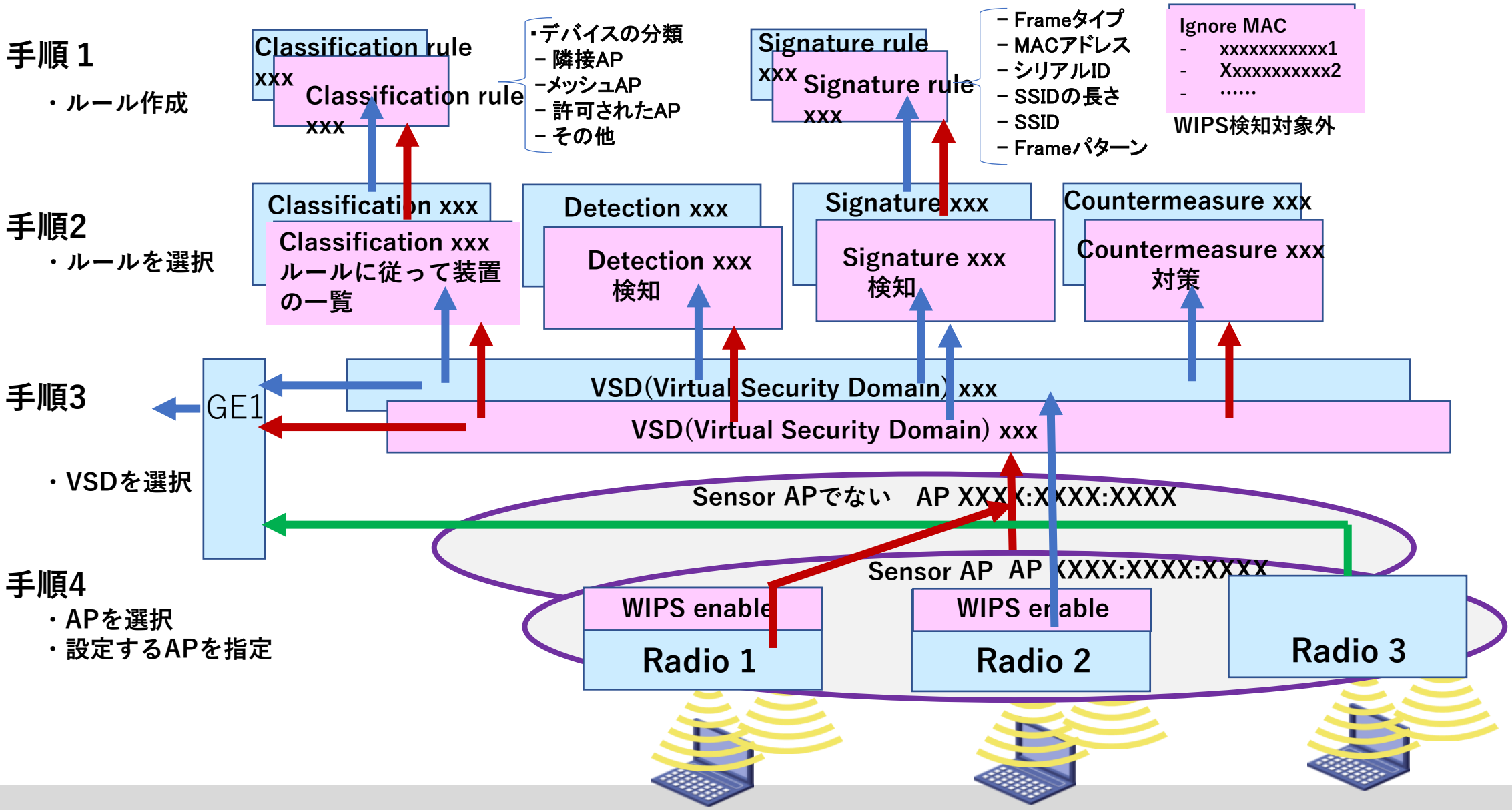
System
- Event Logs
- Resource
  - ACL
- Administrators
- Management
  - Configuration save, import
  - Upgrade
  - Reboot

Tools
- Debug

Dashboardが表示される

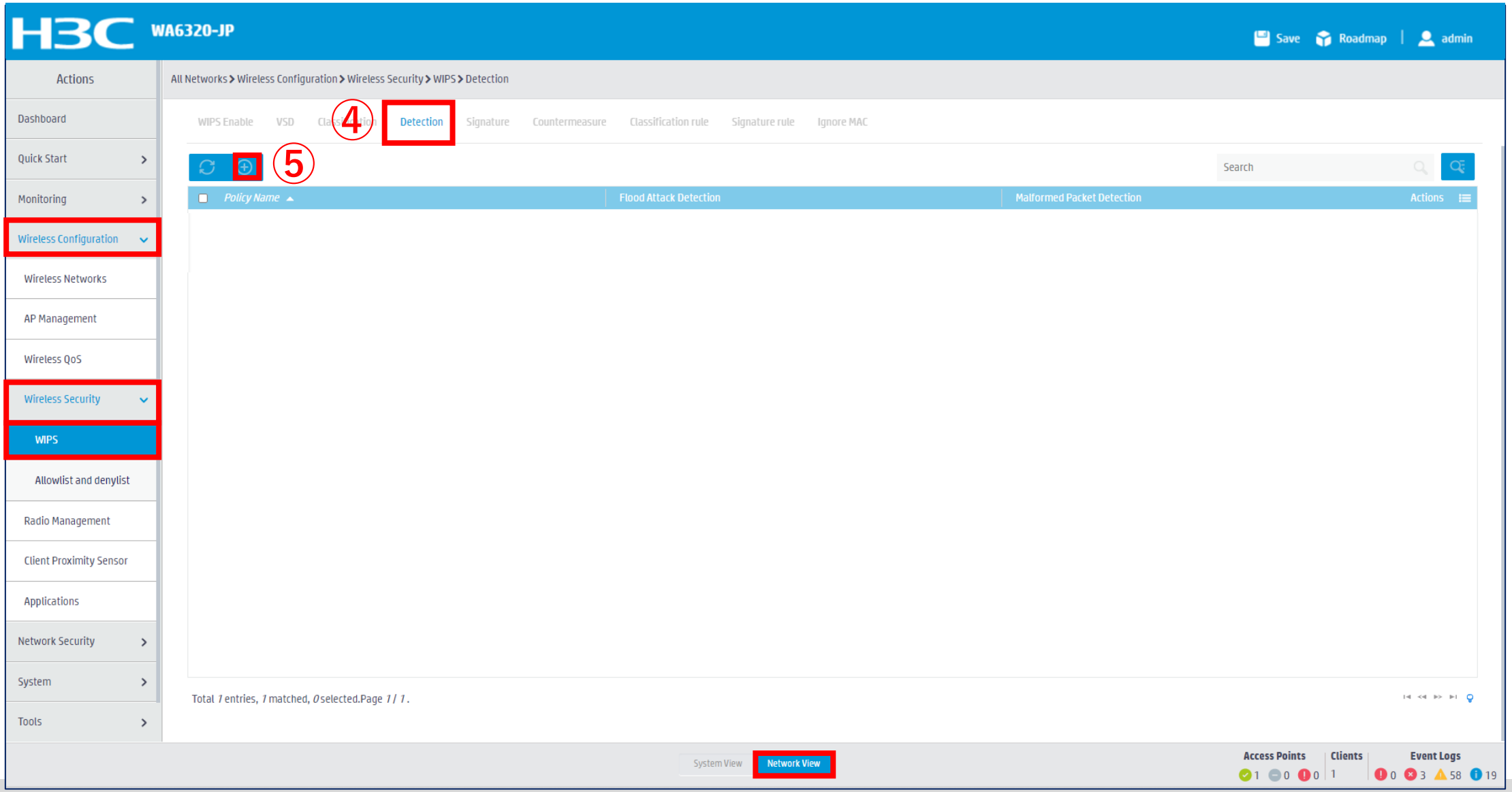


ACのGUIでAPでのWIPS検知ポリシーを設定する

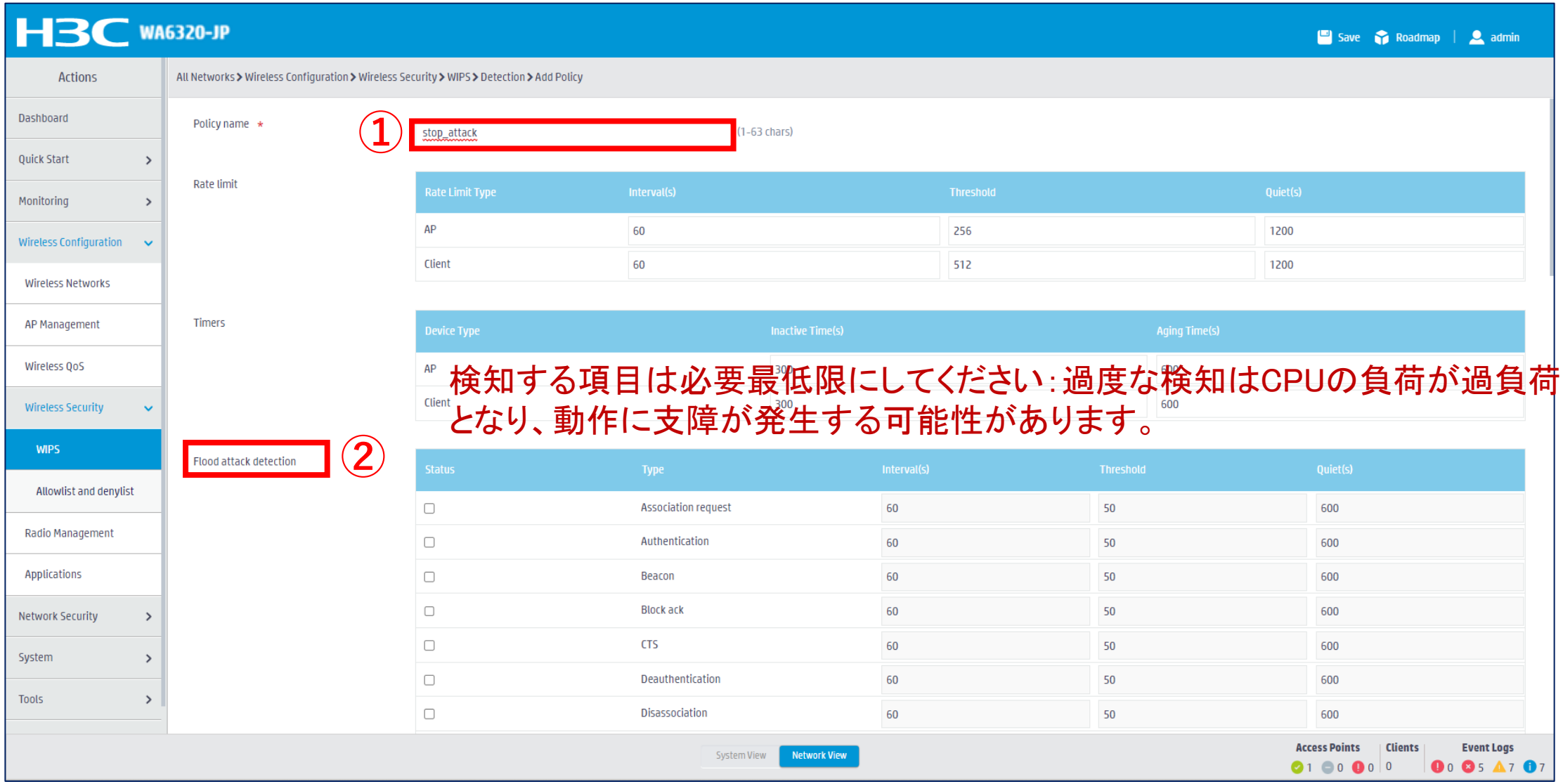


ACのGUIでAPでのWIPS検知ポリシーを設定する

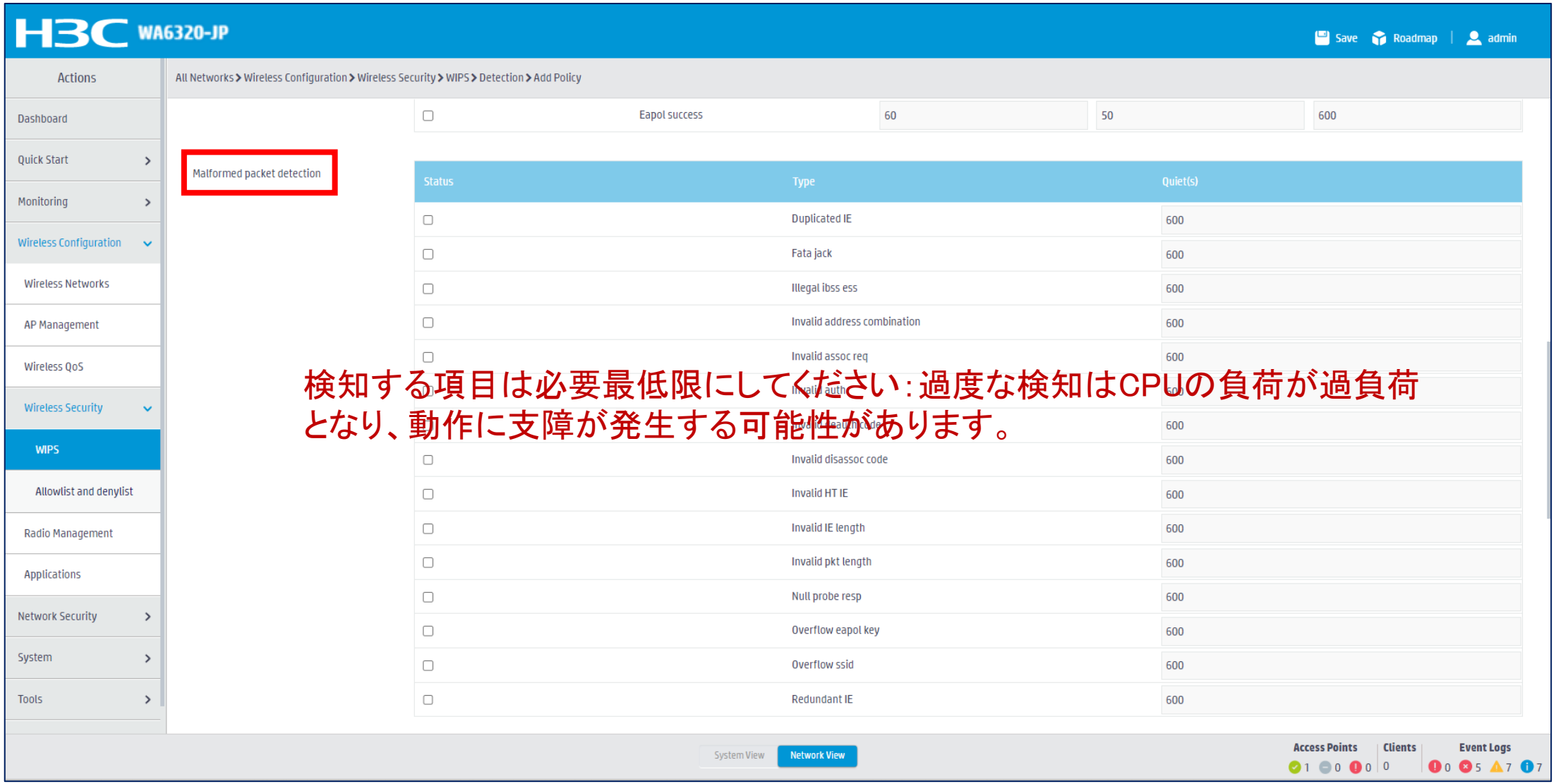
- Network view > Wireless Configuration > Wireless Security > WIPS > Detection



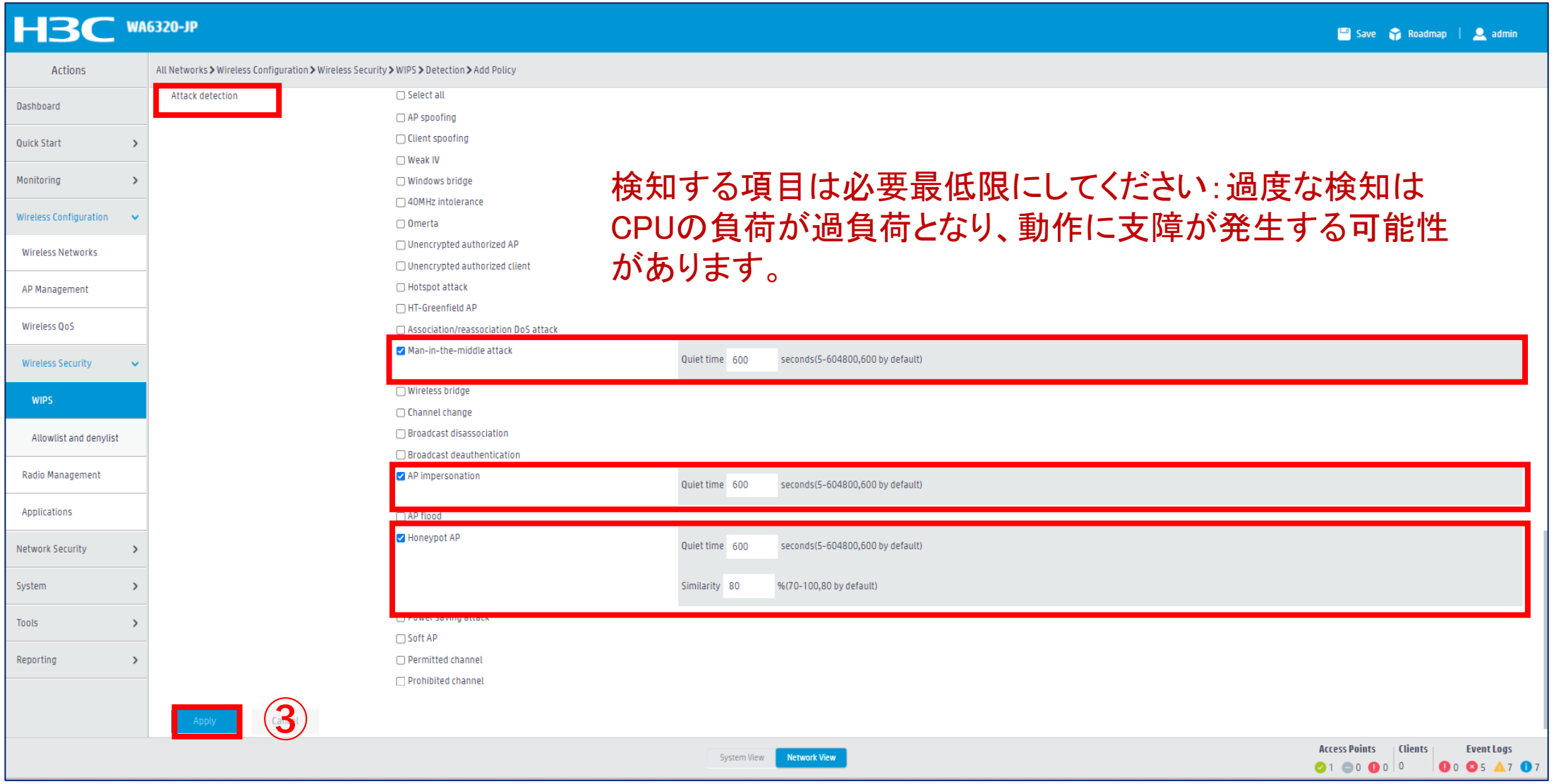
ACのGUIでAPでのWIPS検知ポリシーを設定する（続き）



ACのGUIでAPでのWIPS検知ポリシーを設定する（続き）



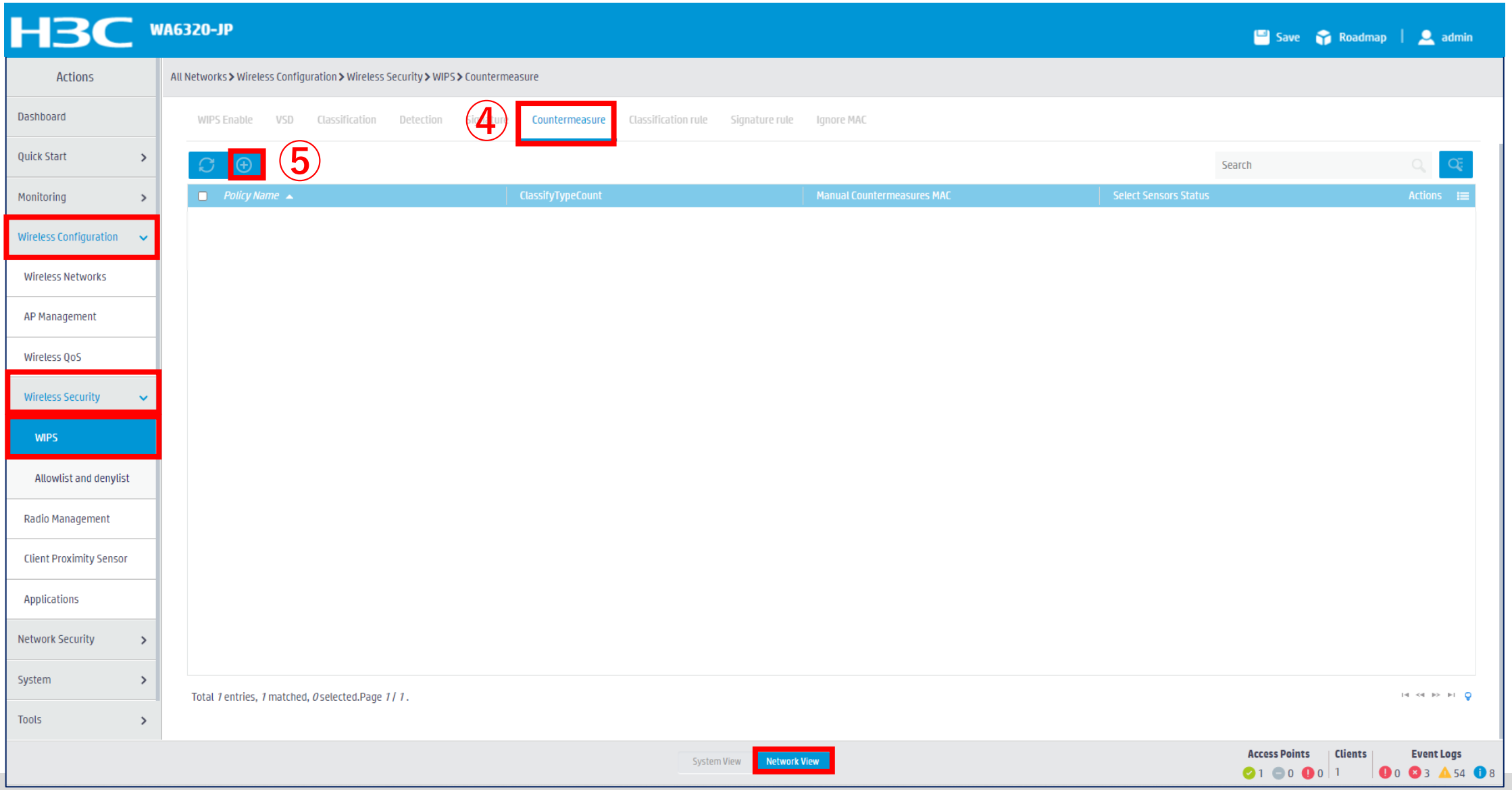
ACのGUIでAPでのWIPS検知ポリシーを設定する（続き）



検知する項目は必要最低限にしてください：過度な検知はCPUの負荷が過負荷となり、動作に支障が発生する可能性があります。

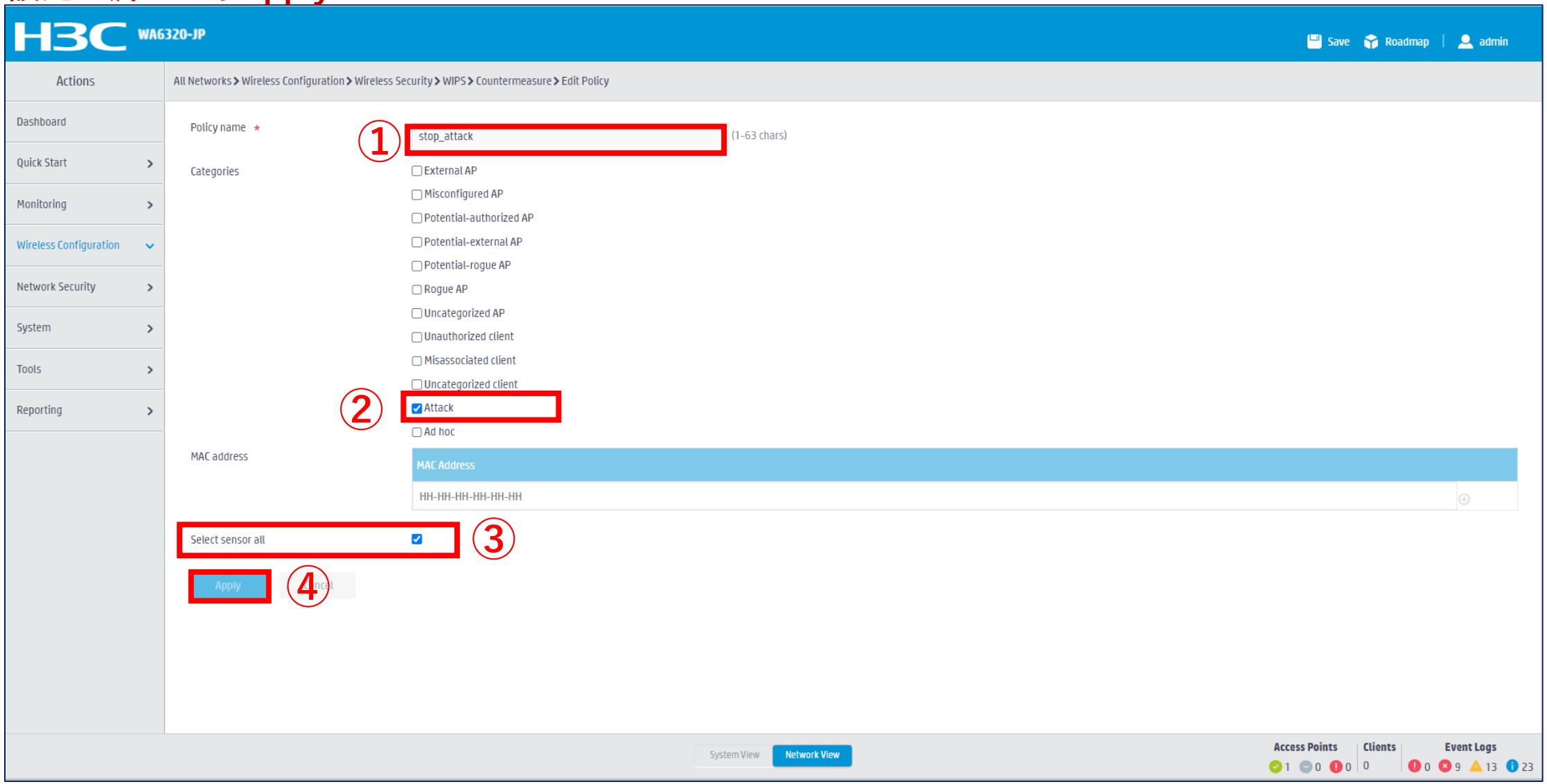
攻撃を検知したら対策するように設定する

- Wireless Configuration > Wireless Security > WIPS > countermeasure



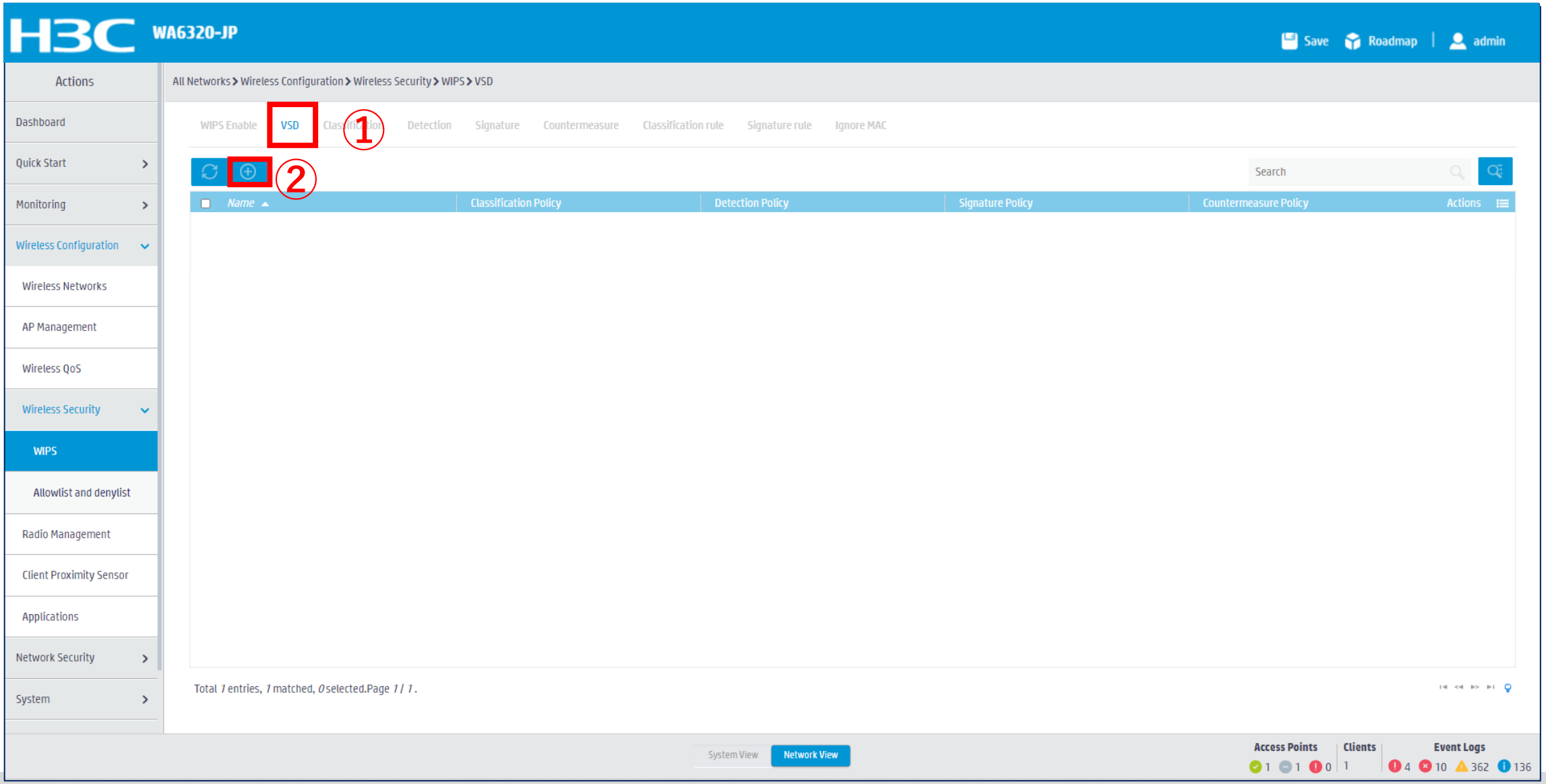
攻撃を検知したら対策するように設定する（続き）

- 設定が済んだらApply



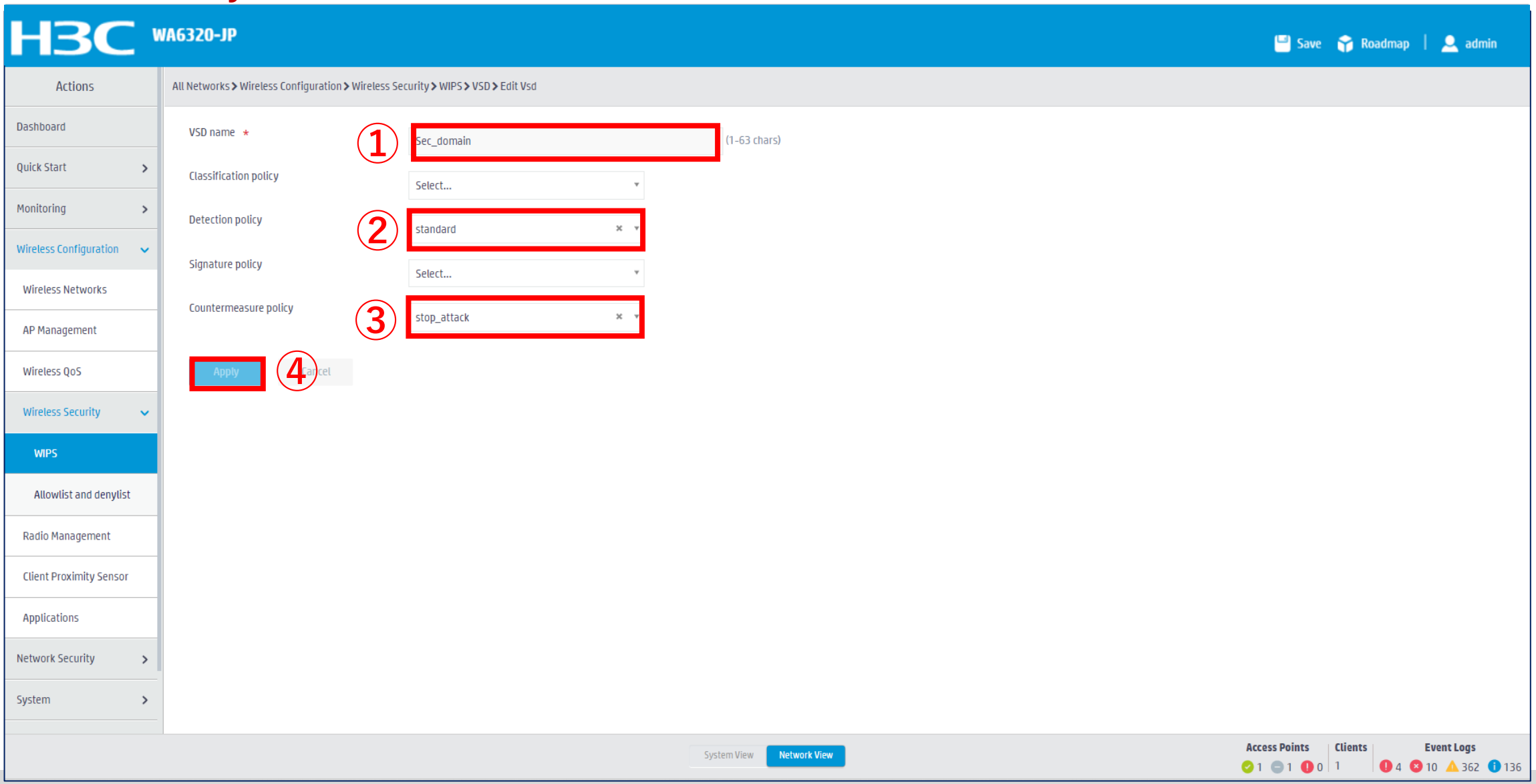
攻撃を検知したら対策するように設定する（続き）

- Virtual Security Domain(VSD)を定義する



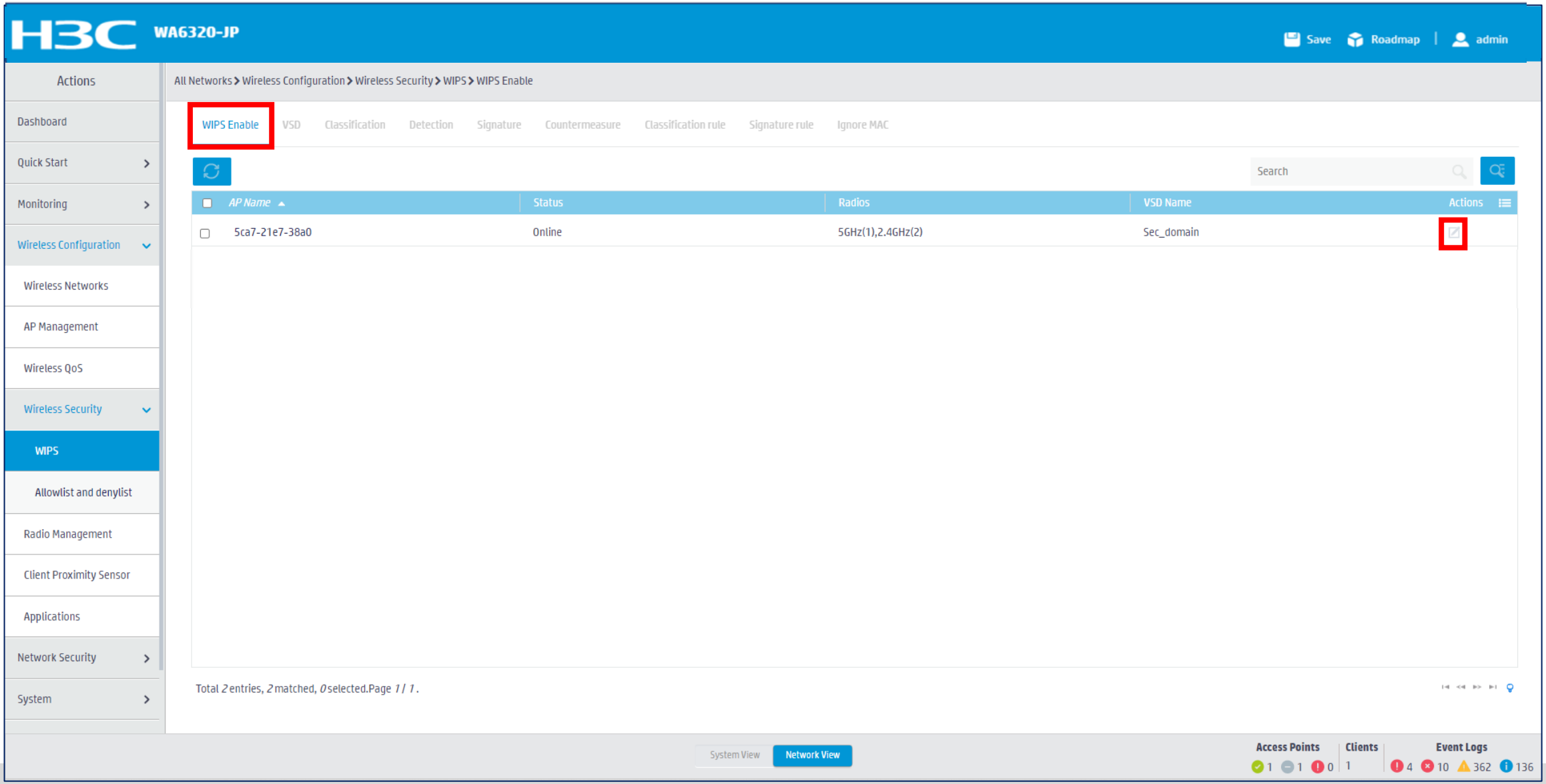
攻撃を検知したら対策するように設定する（続き）

- Virtual Security Domain(VSD)名とそこで適用するポリシーを選択する



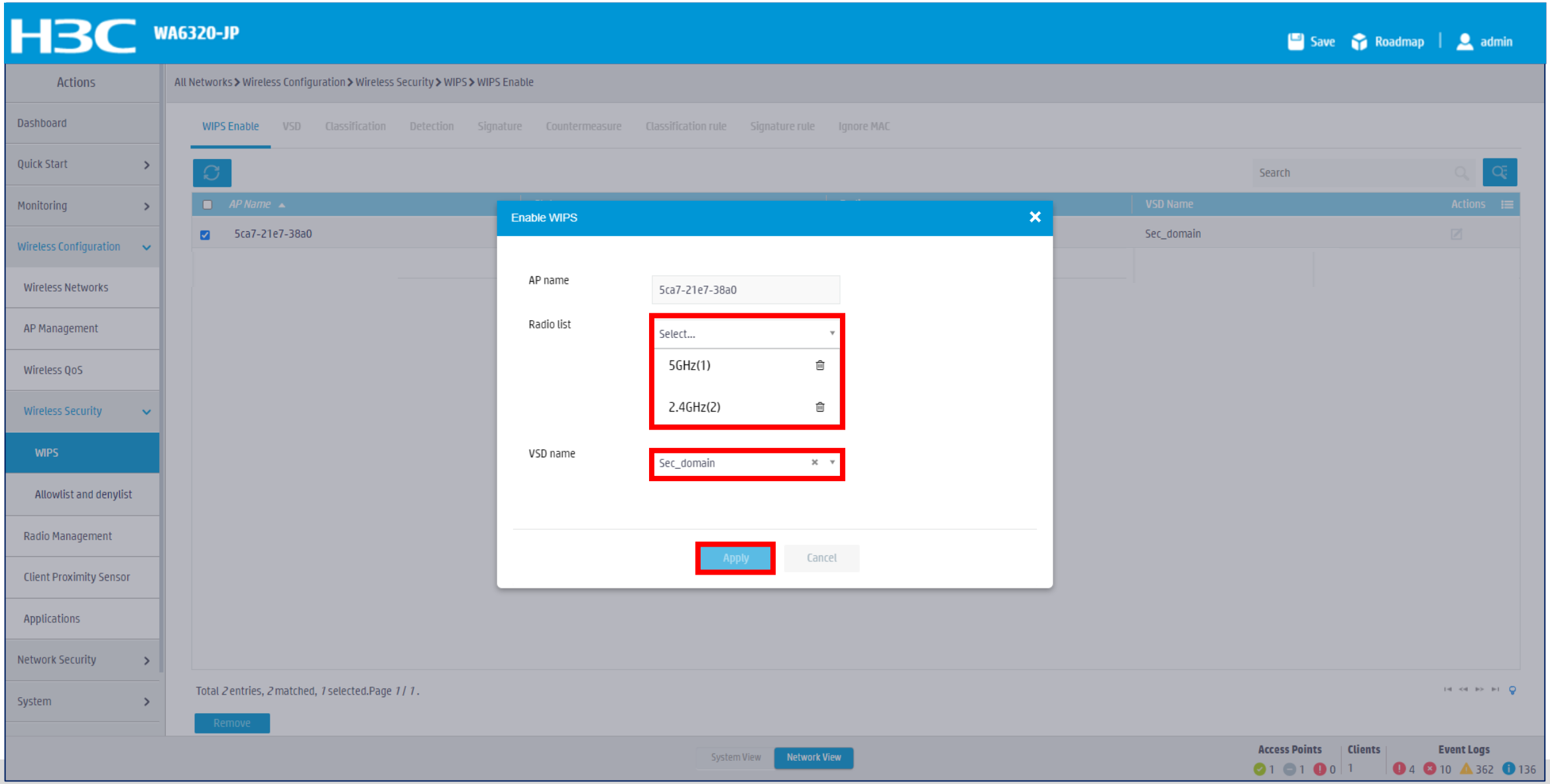
攻撃を検知したら対策するように設定する（続き）

- WIPSを有効にするAPを選択する

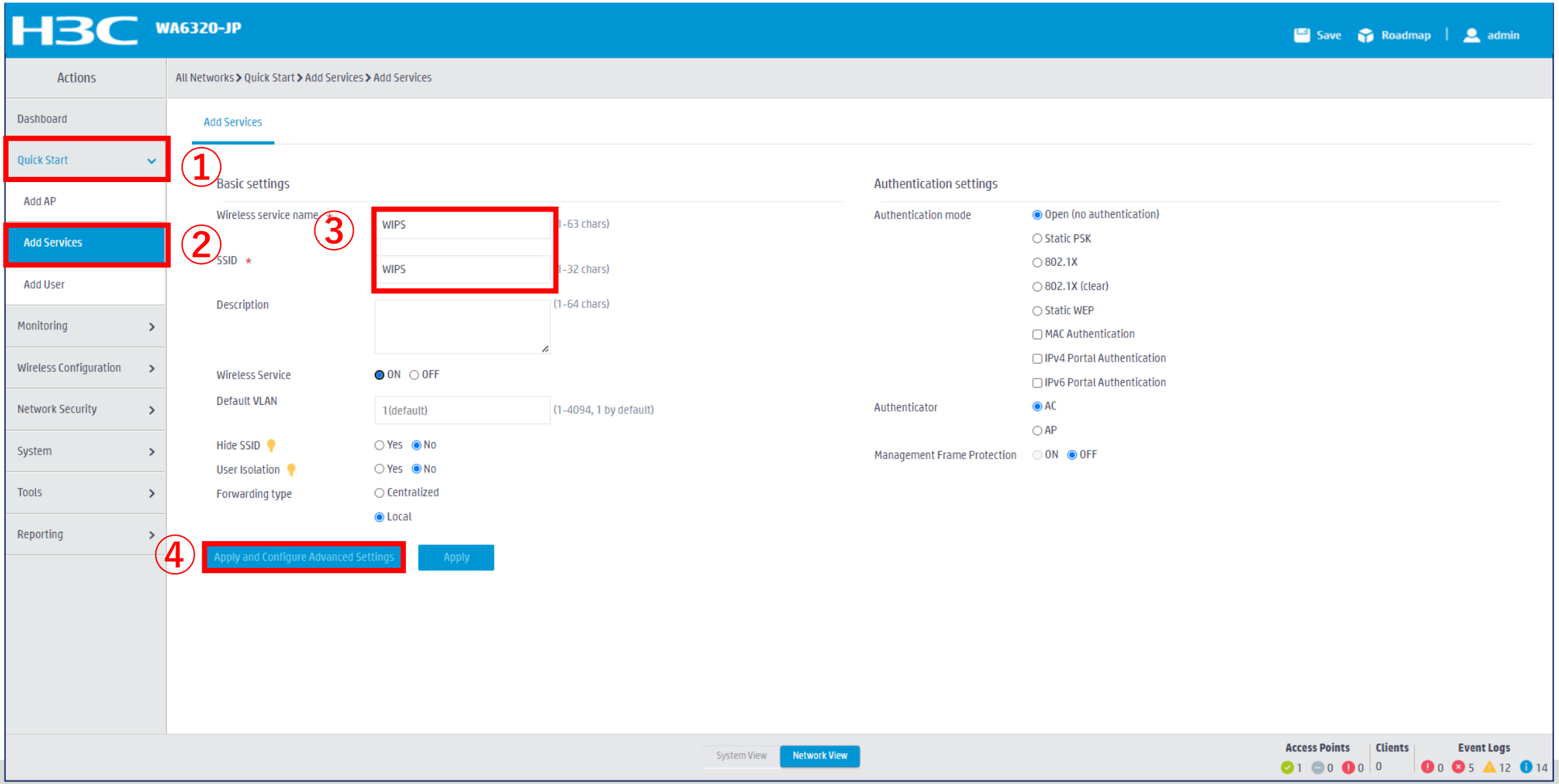


攻撃を検知したら対策するように設定する（続き）

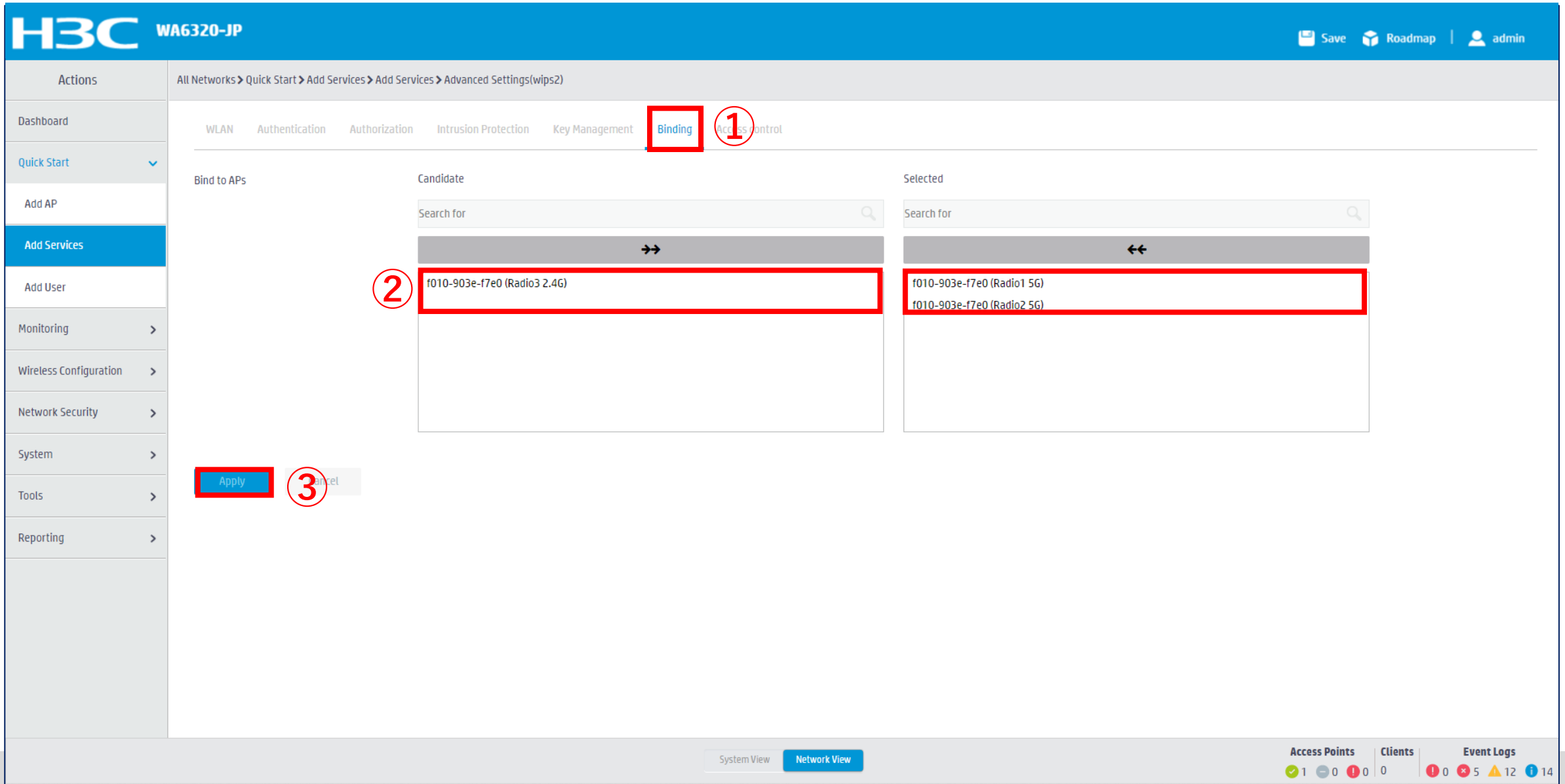
- WIPSを有効にするVSDとそれを適用する電波(radio)を指定する



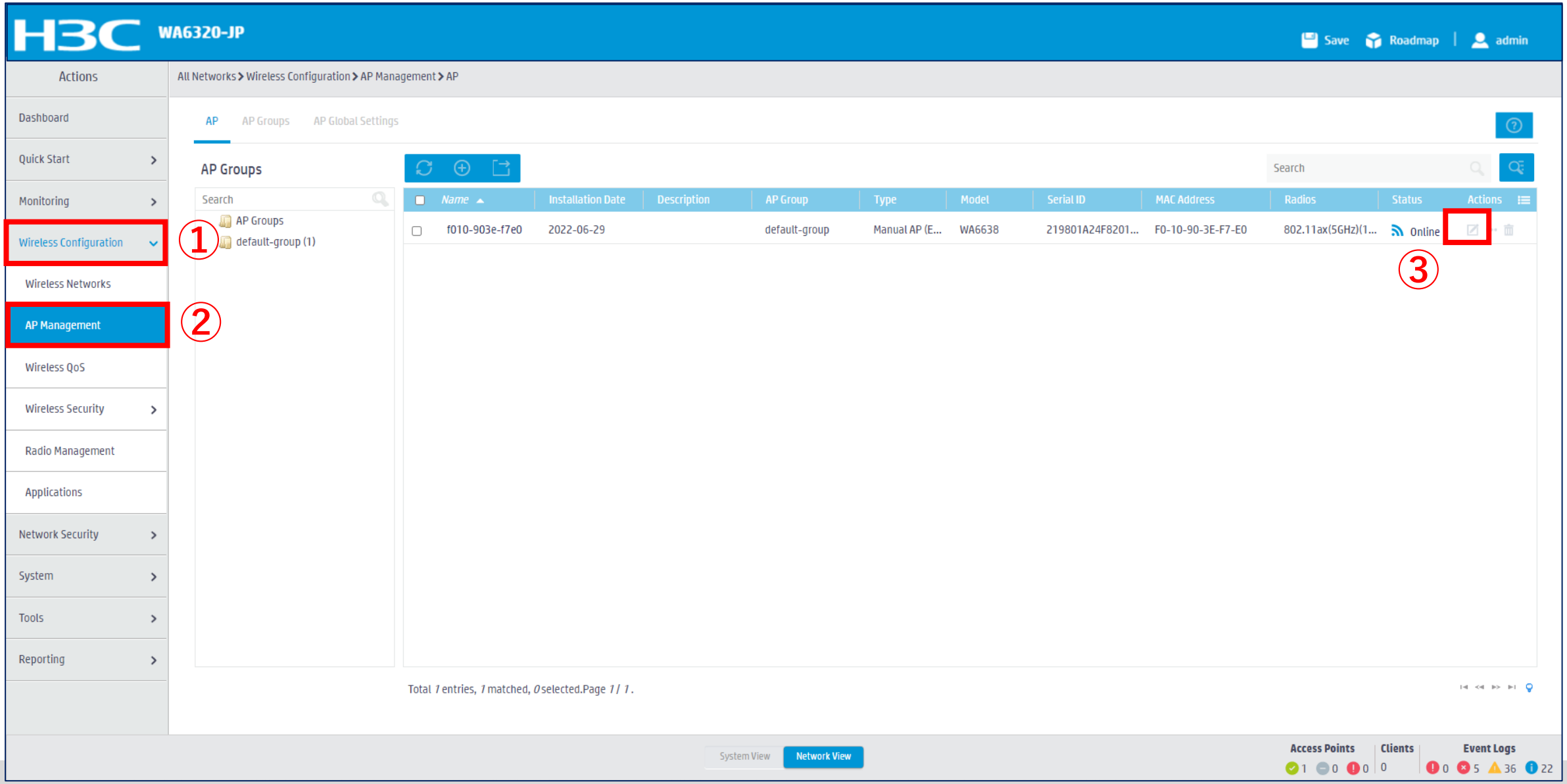
SSIDを作成します


H3C WA6320-JP
Save
Roadmap
admin
Actions
All Networks > Quick Start > Add Services > Add Services
Dashboard
Quick Start
Add AP
Add Services
Add User
Monitoring
Wireless Configuration
Network Security
System
Tools
Reporting
Add Services
①
②
③
④
Basic settings
Wireless service name *
WIPS
(1-63 chars)
SSID *
WIPS
(1-32 chars)
Description
(1-64 chars)
Wireless Service
ON OFF
Default VLAN
1(default)
(1-4094, 1 by default)
Hide SSID
Yes No
User Isolation
Yes No
Forwarding type
Centralized
Local
Apply and Configure Advanced Settings
Apply
Authentication settings
Authentication mode
Open (no authentication)
Static PSK
802.1X
802.1X (clear)
Static WEP
MAC Authentication
IPv4 Portal Authentication
IPv6 Portal Authentication
Authenticator
AC
AP
Management Frame Protection
ON OFF
System View
Network View
Access Points
Clients
Event Logs

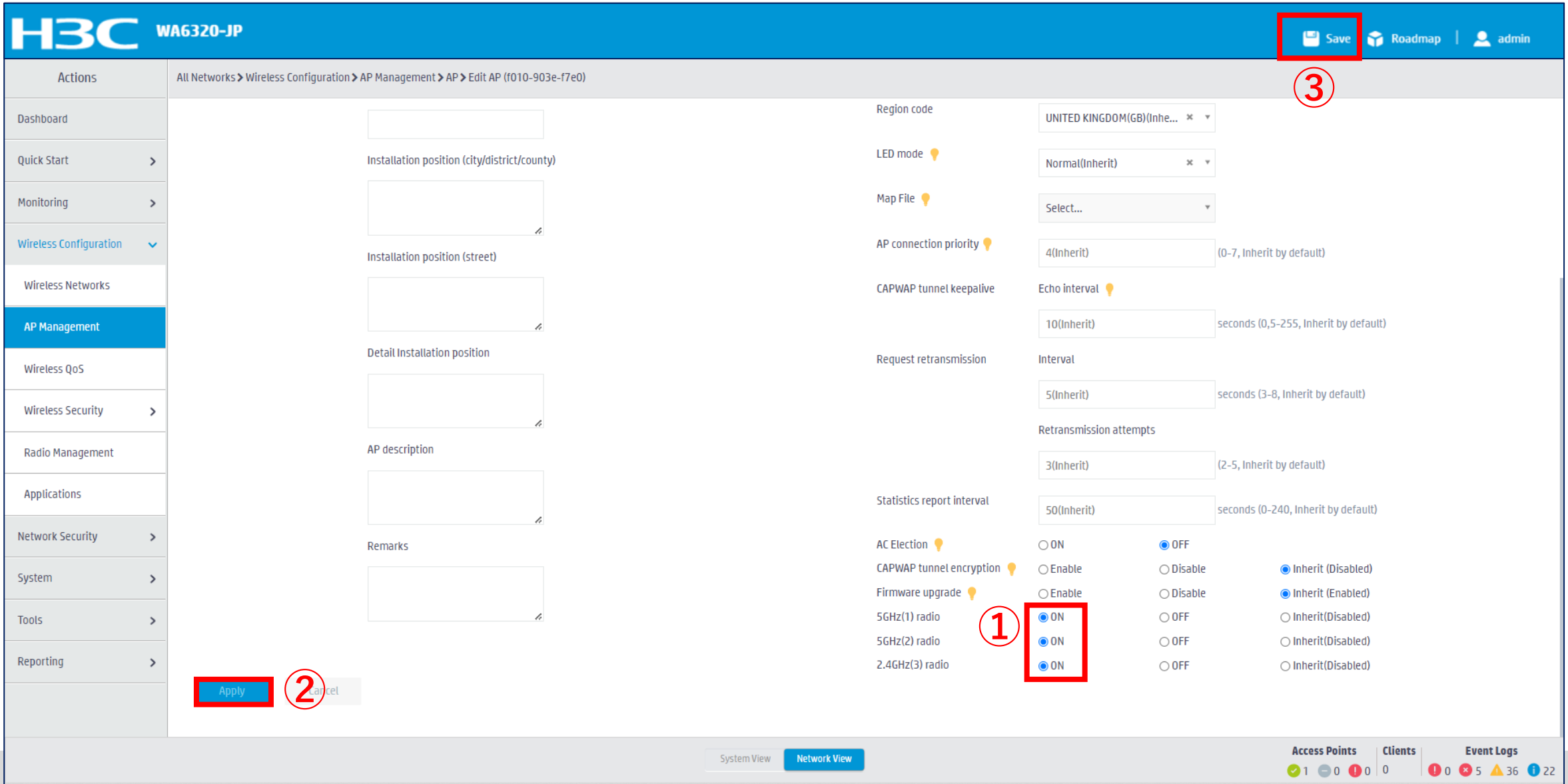
SSIDを載せる電波を選択します



APが電波を出すようにします

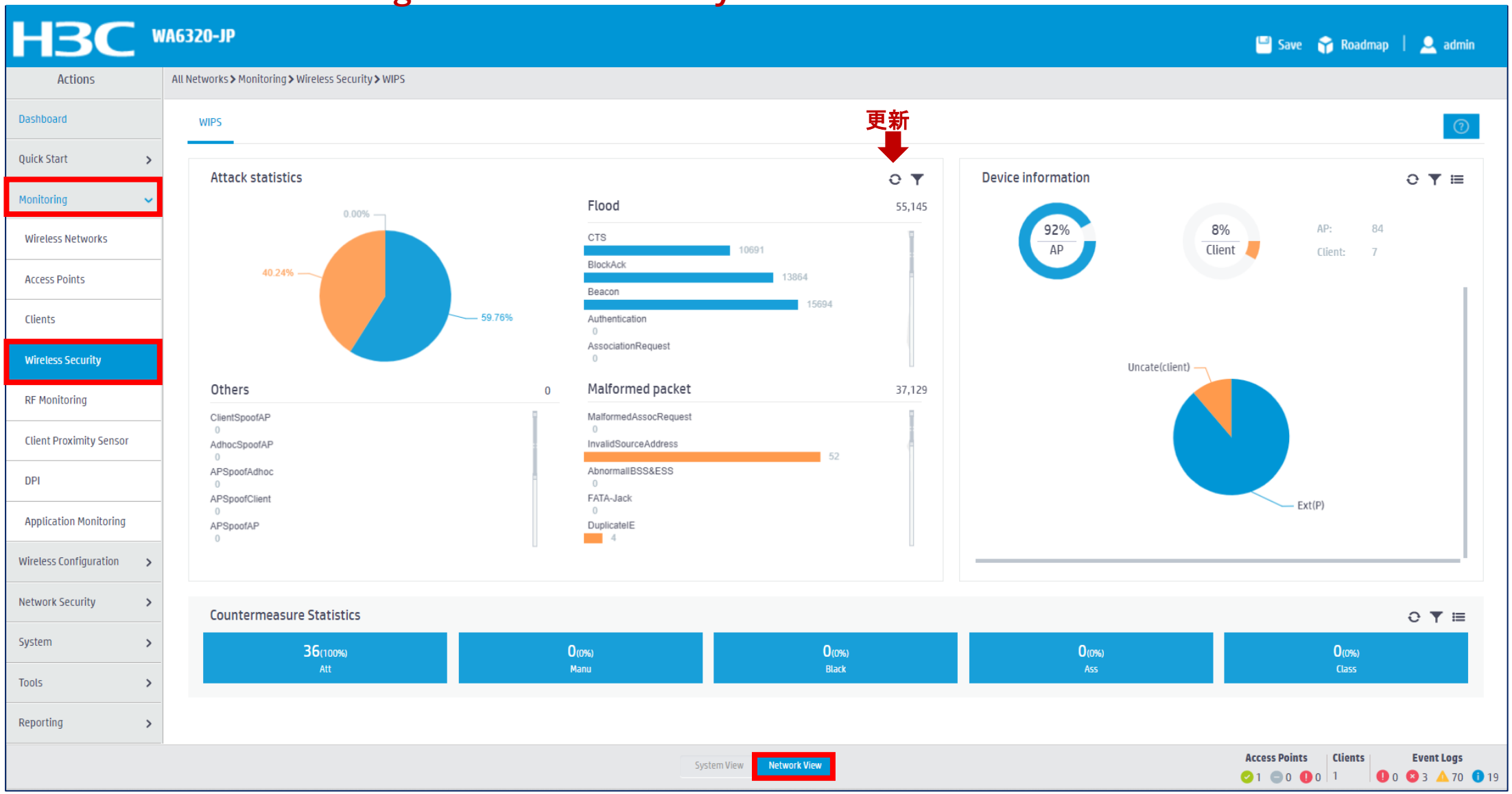


SSIDを載せる電波を選択して設定を保存(save)します



ACのGUI画面でWIPSで検知した状況を確認

- Network View > Monitoring > Wireless Security



The Leader in Digital Solutions

www.h3c.com