

A decorative graphic is located in the bottom left corner of the page. It features a grid of squares in various shades of gray, with a prominent red square in the second row, first column.

H3C WLAN WIPS設定と検証



- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

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
- 禁止チャンネルの検出
- 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)

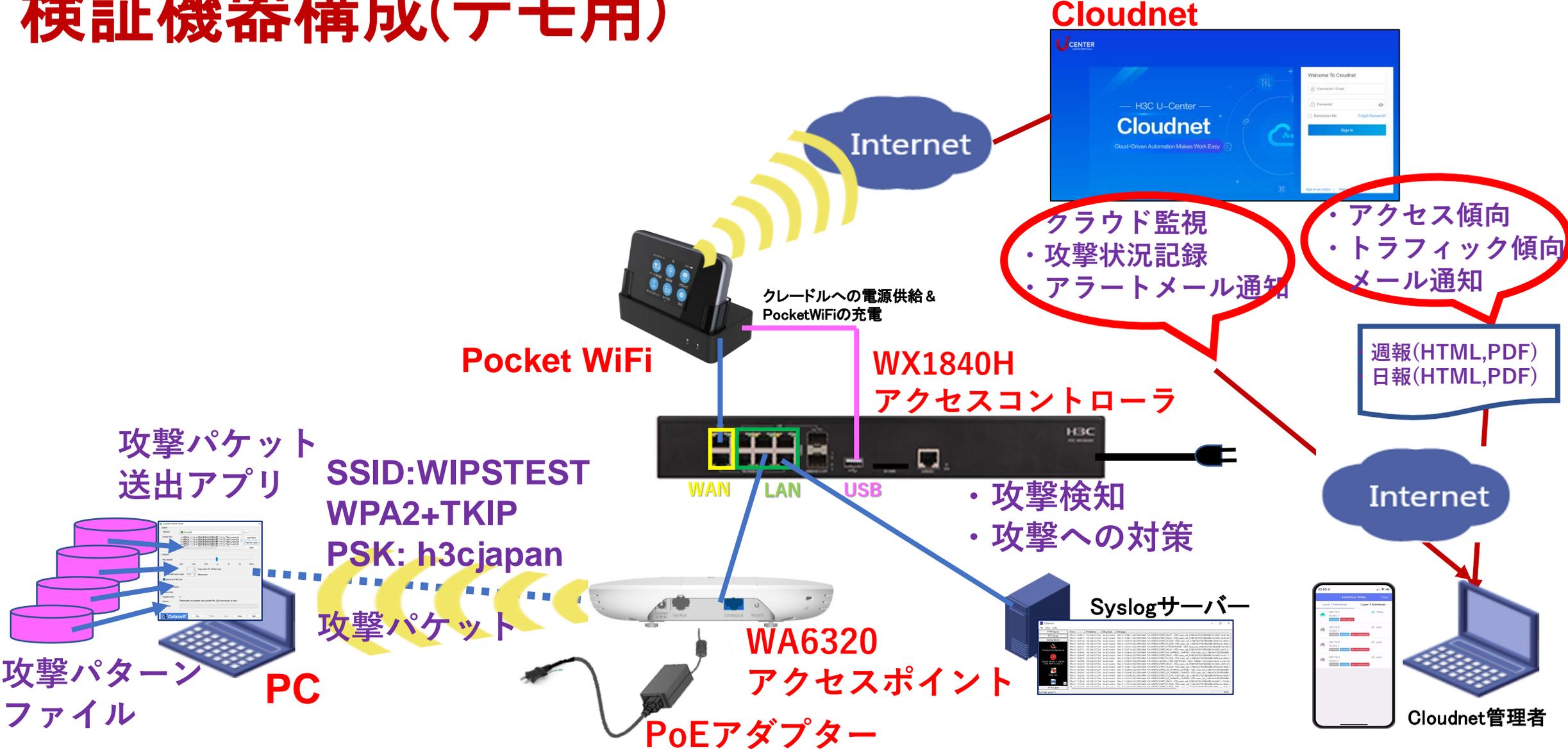
デバイスの分類(Classification)

- 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

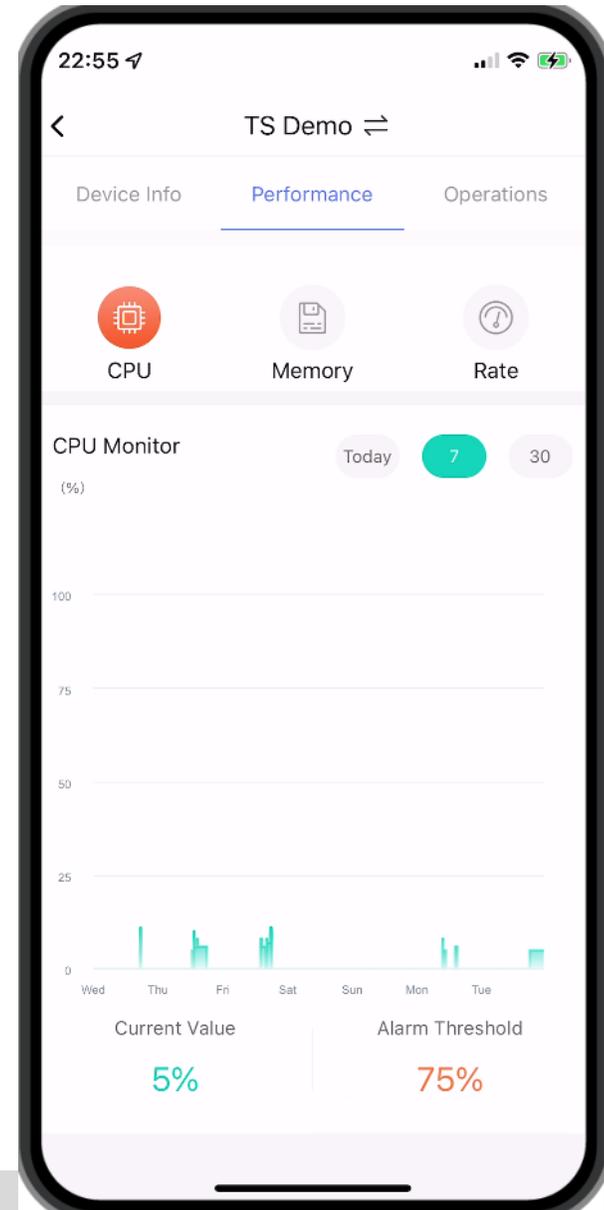
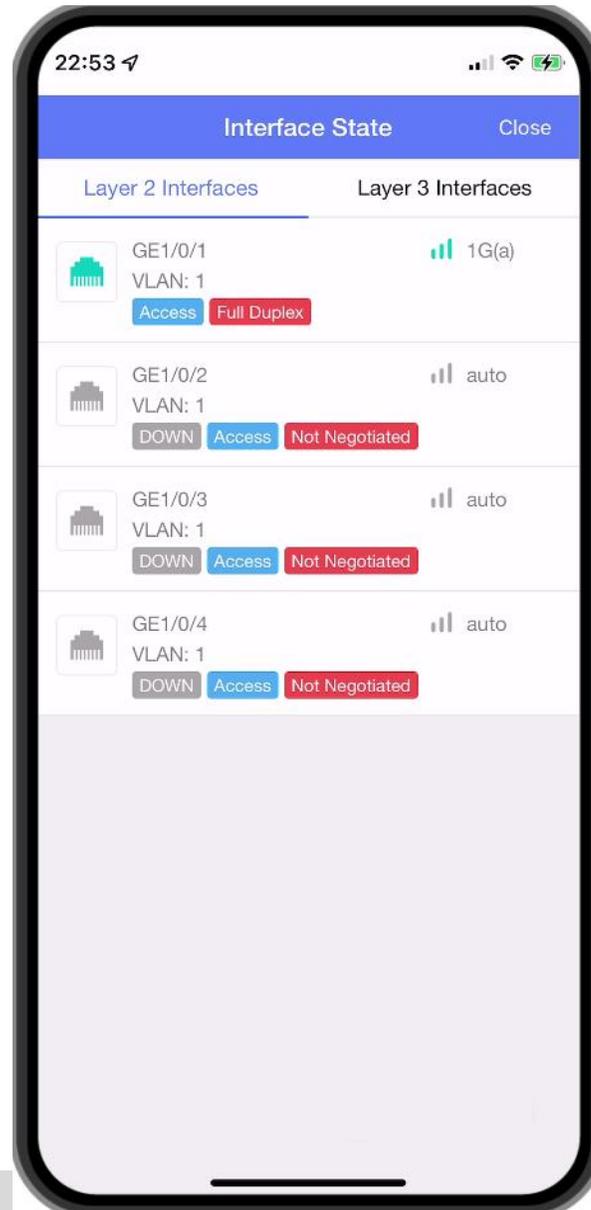
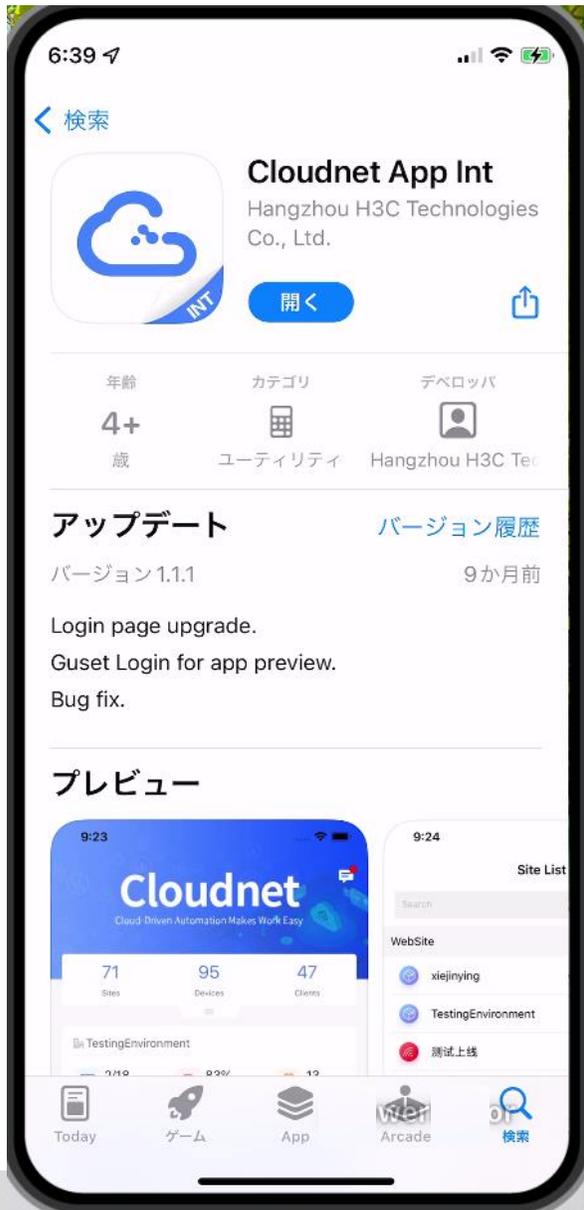


- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

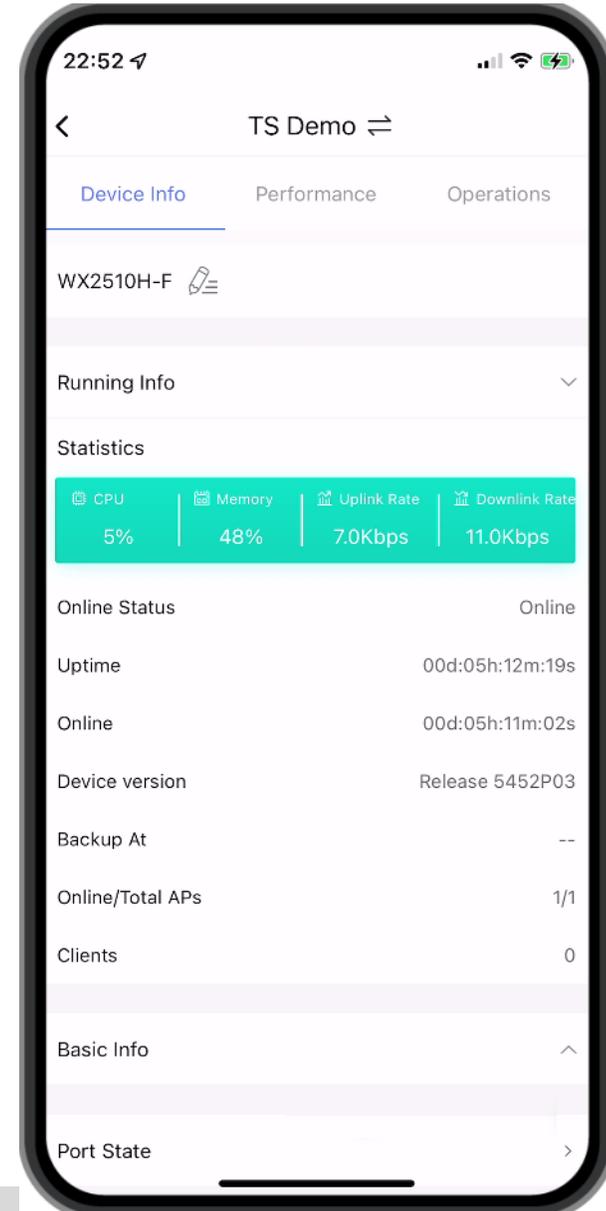
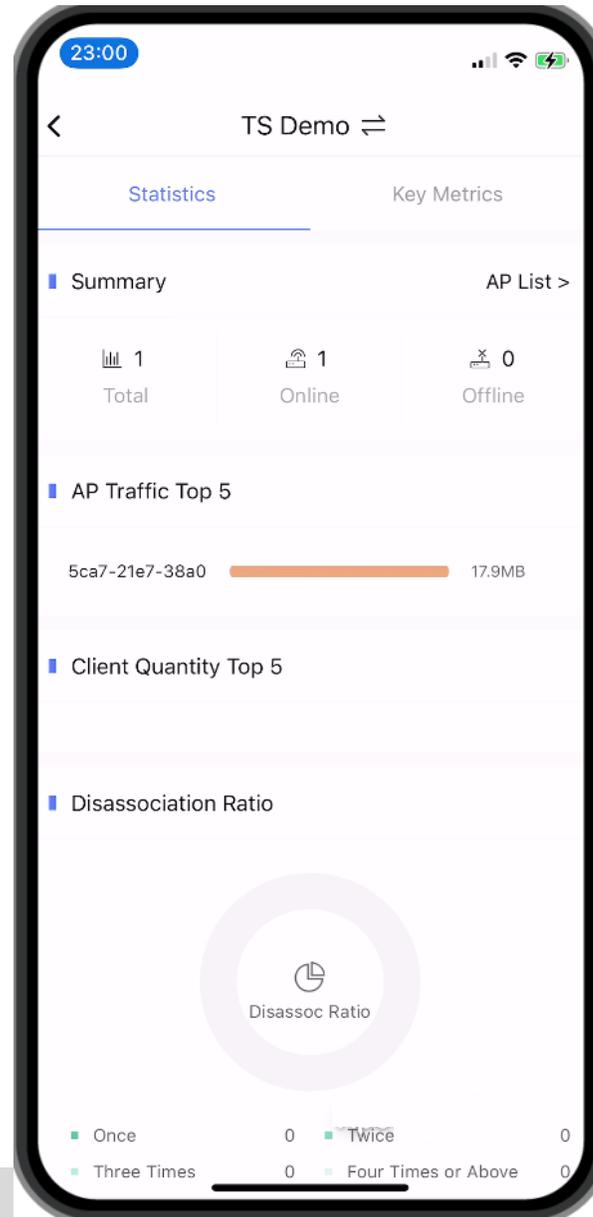
検証機器構成(デモ用)



Cloudnetアプリ(iOS)



Cloudnetアプリ(iOS)

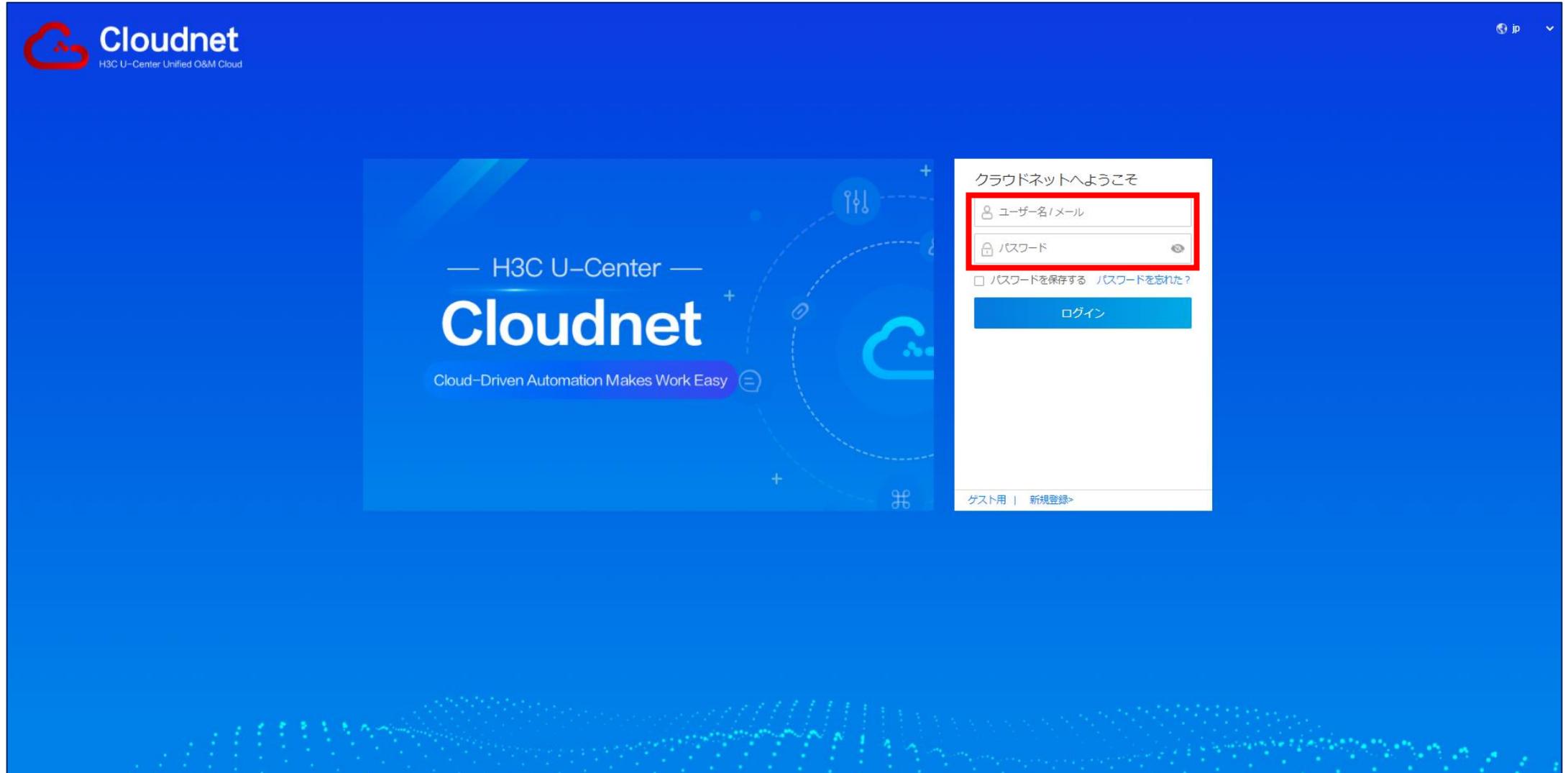




- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

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

① ネットワーク スマートO&M サービス

② 設定

③ AC

ワイヤレスセキュリティ

ワイヤレスセキュリティモニタリングの詳細については、スマートO&M>セキュリティ>にアクセスしてください。 [攻撃の検出 ページビュー](#)

攻撃の検出: オープン クローズ

SSIDスキャン 偽造MACの検出

Step1: 検出レベルを選択し、対策を確認します

検出レベル: 高 中 低 カスタマイズ

検知項目 反撃をサポートする

Malformed Packet Flood Attack

Step2: 検出APを選択 [?](#)

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

1 ネットワーク

スマートO&M サービス

② 設定

③ AC

ワイヤレスセキュリティ

ワイヤレスセキュリティモニタリングの詳細については、スマートO&M>セキュリティ>にアクセスしてください。 [攻撃の検出 ページビュー](#)

攻撃の検出: オープン クローズ

Step1: 検出レベルを選択し、対策を確認します

検出レベル: 高 中 低 カスタマイズ

検知項目			<input checked="" type="checkbox"/> 反撃をサポートする
<input checked="" type="checkbox"/> Malformed Packet	<input checked="" type="checkbox"/> Honeypot AP	<input checked="" type="checkbox"/> MITM Attack	
<input checked="" type="checkbox"/> Flood Attack	<input checked="" type="checkbox"/> Spoofing Attack	<input checked="" type="checkbox"/> Assoc/Reassoc DoS Attack	
<input checked="" type="checkbox"/> AP Flood Attack			

Step2: 検出APを選択

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

① ネットワーク

② 設定

③ AC

ワイヤレスセキュリティ

ワイヤレスセキュリティモニタリングの詳細については、スマートO&M>セキュリティ>にアクセスしてください。 [攻撃の検出 ページビュー](#)

攻撃の検出: オープン クローズ

Step1: 検出レベルを選択し、対策を確認します

検出レベル: 高 中 低 カスタマイズ

検知項目 反撃をサポートする

<input checked="" type="checkbox"/> Malformed Packet	<input checked="" type="checkbox"/> Weak IV	<input checked="" type="checkbox"/> Omerta Attack
<input checked="" type="checkbox"/> 802.11n 40MHz Disabled	<input checked="" type="checkbox"/> Power Save Attack	<input checked="" type="checkbox"/> Soft AP
<input checked="" type="checkbox"/> Windows Bridge	<input checked="" type="checkbox"/> Honeypot AP	<input checked="" type="checkbox"/> MITM Attack
<input checked="" type="checkbox"/> Flood Attack	<input checked="" type="checkbox"/> Spoofing Attack	<input checked="" type="checkbox"/> Broadcast Disassoc/Deauth
<input checked="" type="checkbox"/> AP Impersonation Attack	<input checked="" type="checkbox"/> HT-Greenfield AP	<input checked="" type="checkbox"/> Wireless Bridge
<input checked="" type="checkbox"/> Assoc/Reassoc DoS Attack	<input checked="" type="checkbox"/> AP Flood Attack	

Step2: 検出APを選択

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

① ネットワーク

② 設定

③ AC

ワイヤレスセキュリティ

ワイヤレスセキュリティモニタリングの詳細については、スマートO&M>セキュリティ>にアクセスしてください。 [攻撃の検出 ページビュー](#)

攻撃の検出: オープン クローズ

Step1: 検出レベルを選択し、対策を確認します

検出レベル: 高 中 低 カスタマイズ

検知項目	反撃項目
<input type="checkbox"/> Malformed Packet	<input type="checkbox"/> Malformed Packet
<input type="checkbox"/> Weak IV	<input type="checkbox"/> Weak IV
<input type="checkbox"/> Omerta Attack	<input type="checkbox"/> Omerta Attack
<input type="checkbox"/> 802.11n 40MHz Disabled	<input type="checkbox"/> 802.11n 40MHz Disabled
<input type="checkbox"/> Power Save Attack	<input type="checkbox"/> Power Save Attack
<input type="checkbox"/> Soft AP	<input type="checkbox"/> Soft AP
<input type="checkbox"/> Windows Bridge	<input type="checkbox"/> Windows Bridge
<input checked="" type="checkbox"/> Honeypot AP	<input checked="" type="checkbox"/> Honeypot AP
<input checked="" type="checkbox"/> MITM Attack ②	<input checked="" type="checkbox"/> MITM Attack
<input type="checkbox"/> Flood Attack	<input type="checkbox"/> Unencrypted Device
<input type="checkbox"/> Spoofing Attack	<input type="checkbox"/> Hotspot Attack
<input type="checkbox"/> Broadcast Disassoc/Deauth	
<input checked="" type="checkbox"/> AP Impersonation Attack	
<input type="checkbox"/> HT-Greenfield AP	
<input type="checkbox"/> Wireless Bridge	
<input type="checkbox"/> Assoc/Reassoc DoS Attack	
<input type="checkbox"/> AP Flood Attack	
<input type="checkbox"/> Unencrypt... 信頼できるデバイス	
<input type="checkbox"/> Hotspot At... ホットリスト	
<input type="checkbox"/> Prohibited... チャンネル	

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

Step2 : 検出APを選択 ②

SSIDスキャンのAP設定をコピーする

オプションのAP

AP名

<input type="checkbox"/>	AP名	AP状態
<input type="checkbox"/>	0c3a-fa4b-93a0	オンライン

選んだAP

AP名

<input type="checkbox"/>	AP名	AP状態
<input type="checkbox"/>	00dd-b6b1-4540	オンライン

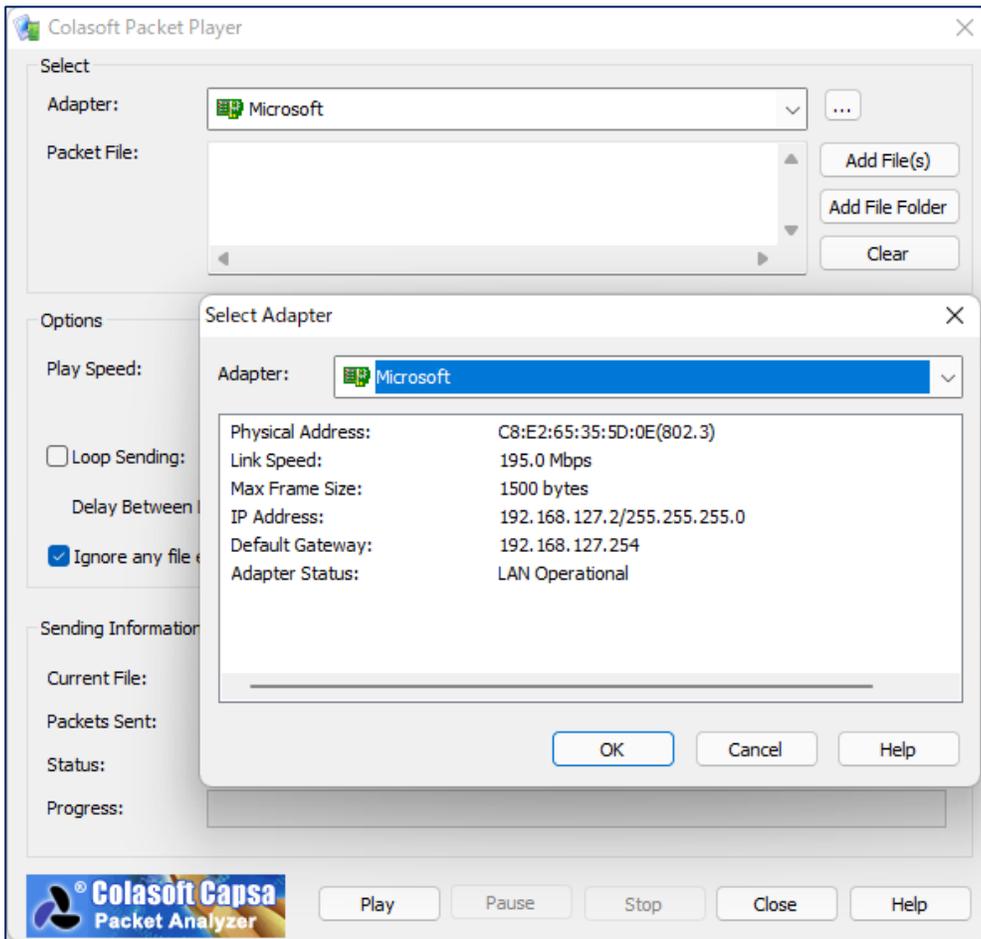
確定 キャンセル



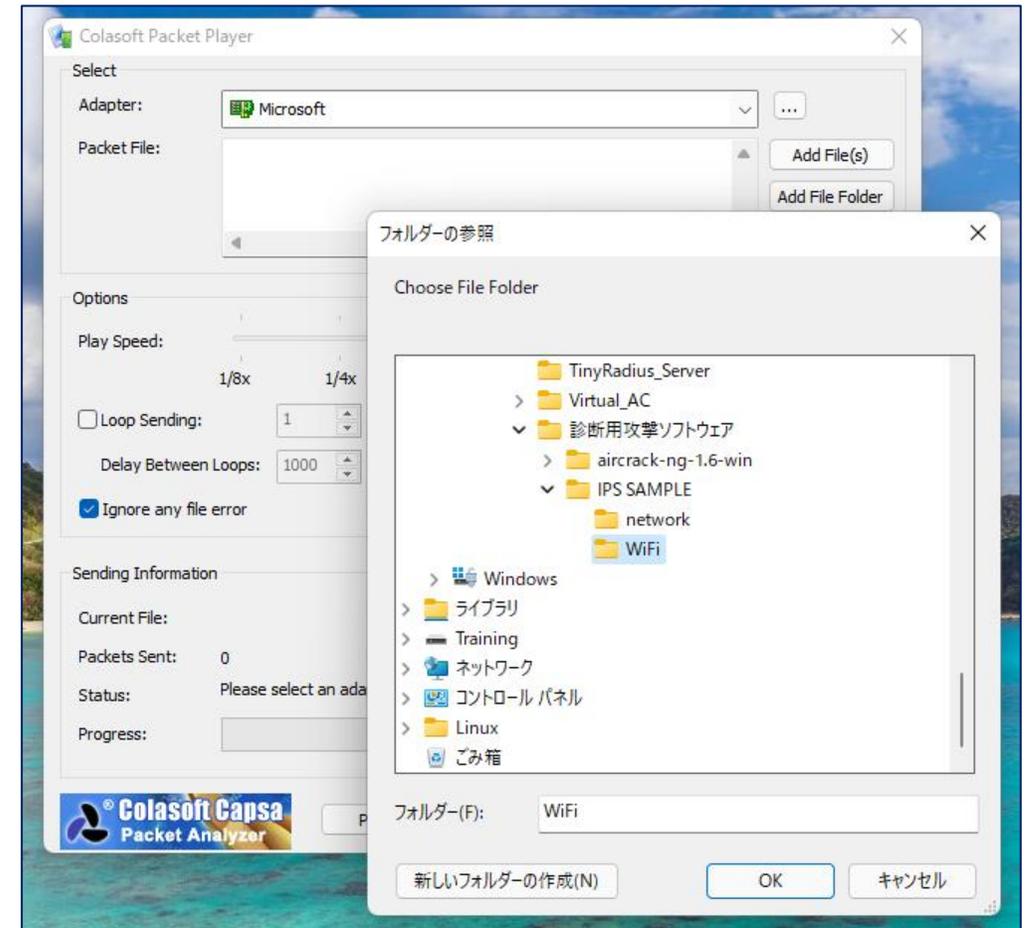
- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

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付

手順1: パケットを送出するWiFiのアダプターを選択する

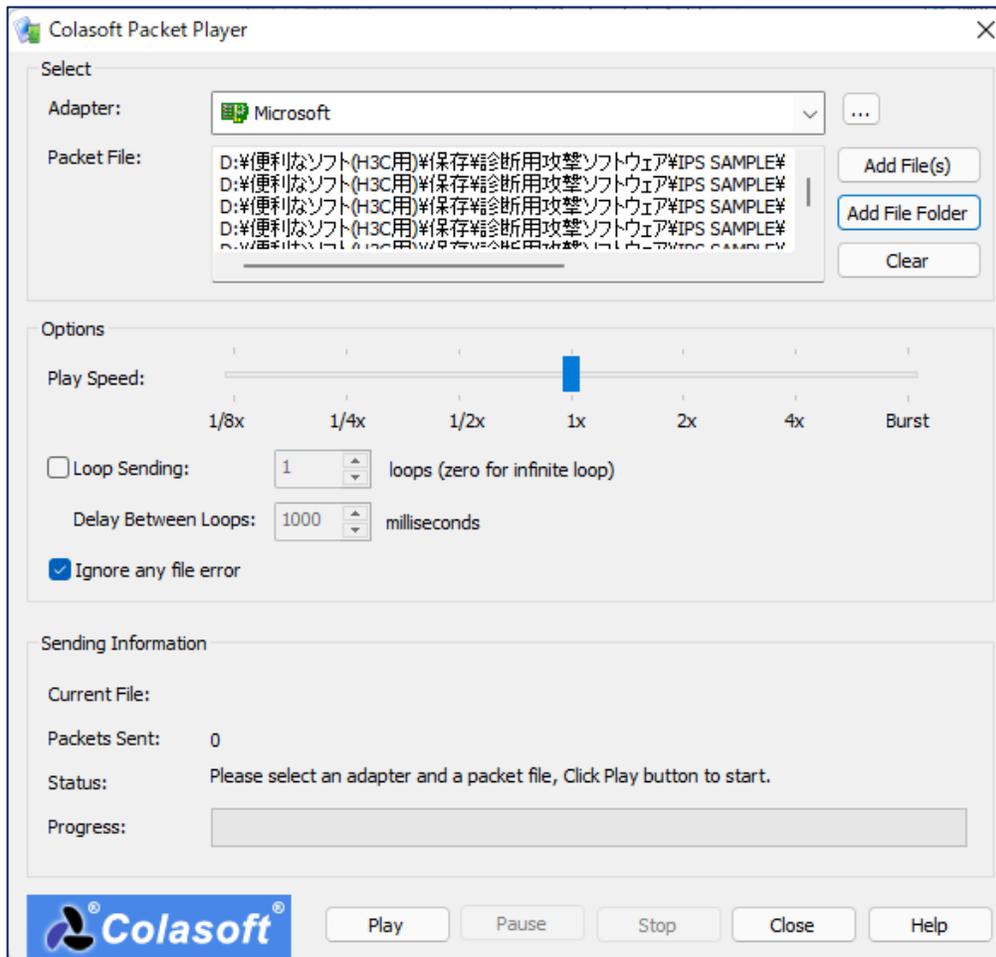


手順2: 送付する攻撃パターンのあるフォルダーを選択する



準備が揃ったら攻撃パッケージを送出する（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ボタンにより送出手を開始する



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



- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

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

The screenshot shows the H3C Cloudnet Smart O&M interface. The navigation menu on the left includes: ダッシュボード, 問題, クライアント, ネットワーク, 最適化, **セキュリティ** (Security), **攻撃検知** (Attack Detection), SSID検知, 偽MAC検知, Safeguard, VIP, and AI-Driven Tasks. The main content area is titled 'スマートO&M' and shows the following data:

- 攻撃検出: 5383回 (攻撃を累計して検出)
- ログ: 2164回 (昨天 攻撃を検出)
- 更新: 2246回 (累計レーダ対策)
- 912回 (昨天 レーダ対策)

The '攻撃総数: 2164個' section displays a horizontal bar chart for various attack types:

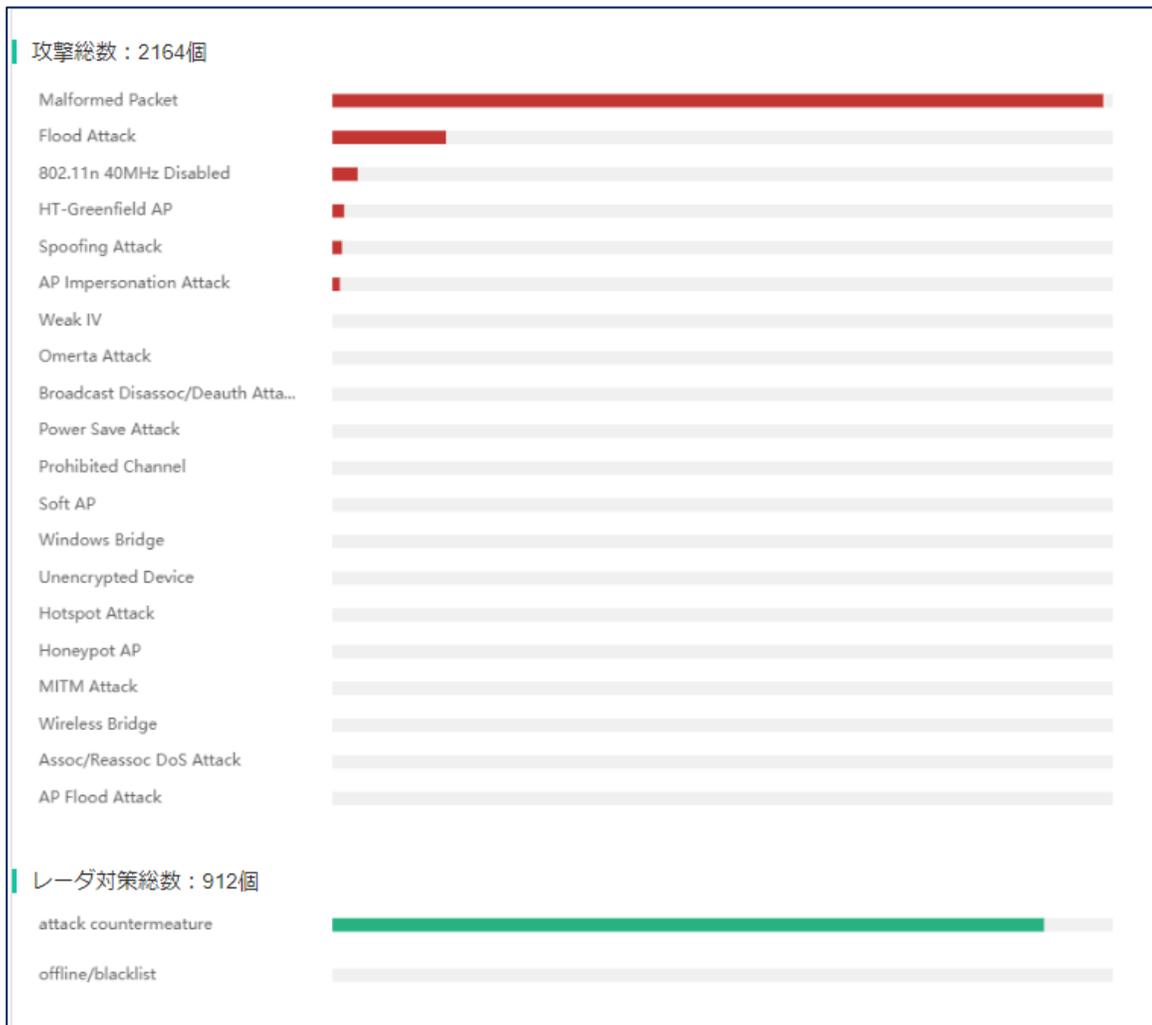
- Malformed Packet
- Flood Attack
- 802.11n 40MHz Disabled
- HT-Greenfield AP
- Spoofing Attack
- AP Impersonation Attack
- Weak IV
- Omerta Attack
- Broadcast Disassoc/Deauth Atta...
- Power Save Attack
- Prohibited Channel
- Soft AP
- Windows Bridge
- Unencrypted Device
- Hotspot Attack
- Honeypot AP
- MITM Attack
- Wireless Bridge
- Assoc/Reassoc DoS Attack
- AP Flood Attack

The 'レーダ対策総数: 912個' section shows a bar chart for 'attack countermeasure'.

The '攻撃を検出する図: 合計' line graph shows the total number of attacks detected over time from 03-30 01:05 to 03-31 00:00. The '検出 攻撃トレンド図: Malformed Packet' line graph shows the trend of Malformed Packet attacks over the same period.

Cloudnet上でのWIPSの状態を確認できる

・ 攻撃の種類別のグラフ

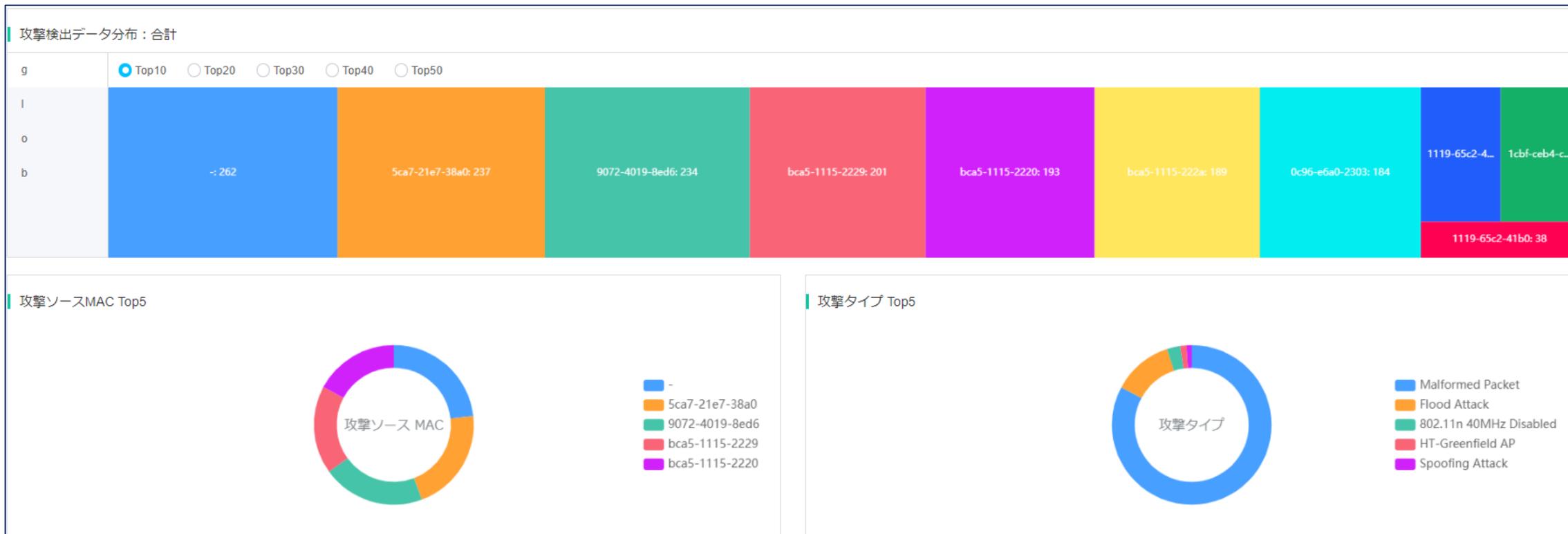


・ 攻撃の時系列トータル



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

①

②

③

SSID検知

無線セキュリティ設定情報はネットワーク>設定>AC>無線セキュリティ ページをご覧ください

SSIDスキャン

3092回
累計スキャンSSID

121回
ほぼ1時間 スキャンSSID

スキャン情報

番号	SSID	BSSID数	最近一回の検出時間	最初の検出時間	最近一回のBSSID	最近一回のレーダ対策されたか
1	.FREE_Wi-Fi_PASS PORT	1	2022-03-30 09:31:55	2022-03-30 09:26:20	9c2a-709d-1782	はい
2	0000softbank	1	2022-03-30 09:38:18	2022-03-30 09:27:25	9c2a-709d-1781	はい
3	603HWa-4AE830	1	2022-03-30 09:25:41	2022-03-30 09:25:41	1044-004a-e830	はい
4	802ZTa-17749D	1	2022-03-30 09:25:41	2022-03-30 09:25:41	9c63-ed17-749d	はい
5	901KC	1	2022-03-30 10:11:23	2022-03-30 10:06:13	2e83-6a94-2411	はい
6	A102ZTa-BE8DAF	1	2022-03-30 09:38:18	2022-03-30 09:37:07	c8ea-f8be-8daf	はい

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

The screenshot displays the H3C Cloudnet management interface. The top navigation bar includes 'ネットワーク', 'スマートO&M', and 'サービス'. The left sidebar contains various menu items, with 'セキュリティ' and '偽MAC検知' highlighted by red boxes and circled numbers 2 and 3 respectively. The main content area shows the '偽MAC検知' (Fake MAC Detection) section, which includes a notification about wireless security settings and two summary cards: '0回 フィッシングMACを累計検出' (0 times cumulative phishing MAC detected) and '0回 ほぼ1時間フィッシングMACを検出' (0 times phishing MAC detected in approximately 1 hour). Below these cards is a 'フィッシングログ' (Phishing Log) table with columns for '番号', '時間 衝突MAC', '衝突タイプ', 'メーカー', 'ブランド', 'IPv4アドレス', 'IPv6アドレス', 'ユーザ名', and '認証方式'. A 'データ' link is visible at the bottom right of the table.



- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

ACのGUI画面でWIPSで検知した状況を確認

- Network View > Monitoring > Wireless Security

The screenshot displays the H3C WX1840H management interface. The breadcrumb navigation is 'All Networks > Monitoring > Wireless Security > WIPS'. The sidebar on the left has 'Monitoring' (circled 1) and 'Wireless Security' (circled 2) highlighted. A red arrow labeled '更新' (Update) points to a refresh icon in the top right of the main content area.

Attack statistics

0.00%

40.24%

59.76%

Flood 55,145

CTS	10691
BlockAck	13864
Beacon	15694
Authentication	0
AssociationRequest	0

Others 0

ClientSpoofAP	0
AdhocSpoofAP	0
APSpooAdhoc	0
APSpooClient	0
APSpooAP	0

Malformed packet 37,129

MalformedAssocRequest	0
InvalidSourceAddress	52
AbnormalBSS&ESS	0
FATA-Jack	0
DuplicateIE	4

Device information

92% AP

8% Client

AP: 84

Client: 7

Uncate(client)

Ext(P)

Countermeasure Statistics

Att	36 (100%)
Manu	0 (0%)
Black	0 (0%)
Ass	0 (0%)
Class	0 (0%)

System View **Network View**

Access Points: 1 (green), 0 (grey), 0 (red)

Clients: 1

Event Logs: 0 (red), 3 (red), 70 (yellow), 19 (blue)

エラーログを確認する

- System > Event Logs

H3C WX1840H Save Roadmap admin

System > System > Event Logs > Event Logs

Event Logs

System Logs Statistics ?

Search

Time	Level	Description	Actions
2022-03-29 11:18:25	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=116; Prohibited channel detected.	...
2022-03-29 11:18:31	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=b2ca-09fe-0e75; Probe request flood detected.	...
2022-03-29 11:18:31	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=NULL; CTS flood detected.	...
2022-03-29 11:18:31	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=a46b-b6d1-7bd0; RTS flood detected.	...
2022-03-29 11:18:31	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-APName=00dd-b6b1-4540-SrcMAC=a46b-b6d1-7bd0; BlockAck flood detected.	...
2022-03-29 11:18:36	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=1; Prohibited channel detected.	...
2022-03-29 11:18:37	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=e82a-44d5-ee29; Error detected: redundant ie.	...
2022-03-29 11:18:41	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=56; Prohibited channel detected.	...
2022-03-29 11:18:46	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=132; Prohibited channel detected.	...
2022-03-29 11:18:56	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=140; Prohibited channel detected.	...
2022-03-29 11:19:01	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=144; Prohibited channel detected.	...
2022-03-29 11:19:06	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=1119-65c2-45a1; Error detected: invalid source addr.	...
2022-03-29 11:19:06	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=36; Prohibited channel detected.	...
2022-03-29 11:19:11	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=40; Prohibited channel detected.	...
2022-03-29 11:19:16	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=44; Prohibited channel detected.	...
2022-03-29 11:19:22	Notification	-VSD=oasis_vsd_219801A2YF821BE000B0-Channel=48; Prohibited channel detected.	...

System View Network View

Access Points 1 Clients 1 Event Logs 1 0 3 147 24

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.

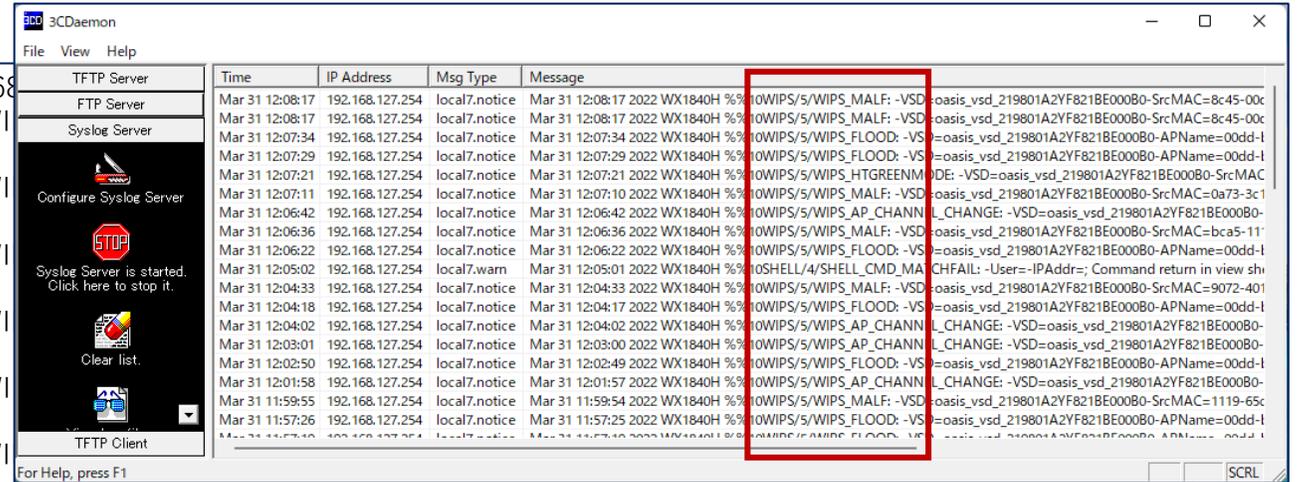
%Mar 29 12:40:40:872 2022 WX1840H **WIPS/5/WIPS_MALF**: -VSD=oasis_vsd_219801A2YF821BE000B0-SrcMAC=daa1-1985-3836; Error
detected: duplicated ie.

%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を設定しておくとも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: 192.168.127.254
Mar 29 12:47:28 192.168.127.254 Mar 29 12:47:27 2022 WX1840H %%10WIPS/5/WIPS_MALF: -VSD=ois_vsd_219801A2YF821BE000B0-APName=00dd-1-45b1; Channel change detected.
Mar 29 12:47:59 192.168.127.254 Mar 29 12:47:58 2022 WX1840H %%10WIPS/5/WIPS_MALF: -VSD=ois_vsd_219801A2YF821BE000B0-APName=00dd-1-45b1; Channel change detected.
Mar 29 12:51:18 192.168.127.254 Mar 29 12:51:17 2022 WX1840H %%10WIPS/5/WIPS_MALF: -VSD=ois_vsd_219801A2YF821BE000B0-APName=00dd-1-45b1; Error detected: invalid source addr.
Mar 29 12:51:26 192.168.127.254 Mar 29 12:51:25 2022 WX1840H %%10WIPS/5/WIPS_MALF: -VSD=ois_vsd_219801A2YF821BE000B0-APName=00dd-1-4540-SrcMAC=1019-65c2-4270; Beacon flood detected.
Mar 29 12:52:14 192.168.127.254 Mar 29 12:52:13 2022 WX1840H %%10WIPS/5/WIPS_MALF: -VSD=ois_vsd_219801A2YF821BE000B0-APName=00dd-1-4540-SrcMAC=a46b-b6d1-7bd0; Error detected: duplicated ie.
Mar 29 12:52:23 192.168.127.254 Mar 29 12:52:22 2022 WX1840H %%10WIPS/5/WIPS_MALF: -VSD=ois_vsd_219801A2YF821BE000B0-APName=00dd-1-4540-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=ois_vsd_219801A2YF821BE000B0-APName=00dd-1-38a0; Error detected: large duration.
Mar 29 12:52:42 192.168.127.254 Mar 29 12:52:41 2022 WX1840H %%10WIPS/5/WIPS_40MHZINTOLERANCE: -VSD=ois_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=ois_vsd_219801A2YF821BE000B0-APName=00dd-1-2220; 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=ois_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=ois_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=ois_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-death-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-req 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-death-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-req 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



- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

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
H3C Cloud Center Unified O&M Cloud

ネットワーク スマートO&M サービス

アカウント管理 | アカウントセキュリティ設定 | MSP管理

アカウント管理
ログアウト

①

基本情報

顔写真
アバターを変更する

アカウント名 H3C_salesdemo [パスワードを変更する](#) | [アカウントをキャンセルする](#)

メールアドレス **site_manager@h3c.com** [変更](#)

業務情報

* 業界タイプ Others Restaurant Shopping Government Enterprise [もっと見る](#)

* 企業名 H3C TS

* 企業LOGO
Cloudnet
H3C Cloud Center Unified O&M Cloud
ロゴは変更可能です
企業LOGOを修正する

連絡先

会社の住所

確定

② システム

- SMS Gateway
- サービススイッチ
- タグ
- サブアカウント
- オープンプラットフォーム
- アカウント**
- デバイスのバインド解除

③

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

The screenshot displays the H3C Cloudnet Smart O&M interface. The top navigation bar includes 'ネットワーク', 'スマートO&M', and 'サービス'. The breadcrumb path is 'ダッシュボード > ブランチ: PJ_DEMO > サイト: TS Demo > Device/Area: WX2510H-F'. The 'スマートO&M' menu item is highlighted with a red box and a circled '1'. The 'サマリー' (Summary) section is also highlighted with a red box and a circled '2'. The main content area shows 'ネットワーク健康度' (Network Health) with a gauge chart and '健康度スコア' (Health Score) with a line graph. Below these are statistics for '影響されたAPの統計' (Affected AP Statistics), '影響された端末の統計' (Affected Device Statistics), '問題分布統計' (Problem Distribution Statistics), and '問題トレンド' (Problem Trend). The '問題分布統計' section includes a donut chart and a table of problem types.

問題タイプ	割合
Assoc...	0%
Wirel...	0%
Auth	0%
Devic...	100%
IP	0%
Acces...	0%
Slow ...	0%
Roami...	0%
Wirel...	0%

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

The screenshot displays the H3C Cloudnet management interface. The left sidebar contains navigation items: ダッシュボード, 問題 (1), 問題分析, アラーム (2), クライアント, ネットワーク, 最適化, セキュリティ, Safeguard, VIP, and AI-Driven Tasks. The main content area is titled '警報購読' (3) and includes a '警報トレンド' (Alert Trend) line chart and a '警告レベル 警報タイプTOP5' (Warning Level Top 5 Alert Types) bar chart. The '警告レベル' chart shows 2 alerts at the 'Hint' level. Below the charts is a '警報詳細' (Alert Details) section with filters for alert level, status, type, area, and device.

警告レベル	致命的	緊急	重大	注意	ヒント
0	0	0	0	0	2

警告レベル	無制限	致命的	緊急	重大	注意	ヒント
警告解除状態	無制限	解除されました	未解除			
警告タイプ	無制限	警告タイプ名を入力してください				
警告エリア	無制限	エリア名を入力してください				
警告デバイス	無制限	デバイス名を入力してください				

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

修正警報策略

* 名: default strategy

説明: default strategy

エリア②: オープン クローズ

* 警報方式: **メール警報** ①

(説明: システムは毎日同じ場所に対して発生した警告を50通の警告メールに送ります; 全部の場所に対して発生した警告は全部の受信者に1000通の警告メールを送ります。特定の条件では制限値を超える可能性があります)

* 送り時間: 月曜日から金曜日まで 土曜日 日曜日

00:00 まで 23:59

* メンテナンスウィンドウ: クローズ

* Info sync ②: クローズ

* 警報アカウント:

オプション警報アカウント 4

アカウントを入力してスクリーニング 🔍

site_manager@h3c.com ②

警告アカウントが選択されました 0

アカウントを入力してスクリーニング 🔍

site_manager@h3c.com ③

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

The screenshot shows the Cloudnet interface with the 'Smart O&M' tab selected. The 'Alarm List' configuration is visible, showing a table of alarm types and their triggers. A red box highlights the 'Device state' section, which includes the following alarm types:

Alarm Category	Alarm Type	Alarm Severity	Alarm Triggers
Device state	<input checked="" type="checkbox"/> CPU Usage	Tip	Avg CPU usage within 10 min exceeds 85 % (75 to 100, 85 by default)
	<input checked="" type="checkbox"/> Memory Usage	Tip	Avg memory usage within 10 min exceeds 85 % (75 to 100, 85 by default)
	<input checked="" type="checkbox"/> AP bulk dropped	Tip	In the past 0 min one or more APs are disconnected,(0 to 120, 0 by default) ?
	<input checked="" type="checkbox"/> AP frequent dropped	Info	An AP dropped more than 5 times in 24 hours yesterday
	<input checked="" type="checkbox"/> Device offline	Info	Device offline from cloud platform for more than 10 minutes / 24 hours
	<input checked="" type="checkbox"/> Device frequently offline	Minor	Device offline from cloud platform more than 7 times within 10 minutes
	<input checked="" type="checkbox"/> AP batch online	Tip	In the past 0 min one or more APs are connected,(0 to 120, 0 by default)
	<input checked="" type="checkbox"/> Port UP/DOWN	Info	Device port status changed
	<input checked="" type="checkbox"/> Port PoE	Info	Port PoE function status changed
	<input checked="" type="checkbox"/> IP Address Conflict	Minor	IP address conflicts were detected on a switch interface
Device operation	<input type="checkbox"/> EoGRE Tunnel Interface Up/D own	Tip	EoGRE Tunnel Interface State Change
	<input type="checkbox"/> Device upgraded successfully	Tip	Device upgraded successfully
	<input type="checkbox"/> Device upgraded failed	Minor	Device upgraded failed
	<input type="checkbox"/> Device restart	Info	Device restart
	<input type="checkbox"/> Device unbinding	Info	Device unbound from the CLI

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

The screenshot shows the Cloudnet interface with the 'Alarms' section selected in the left sidebar. The main content area displays a table of alarms, with a red box highlighting the table and the 'Alarms' menu item. The table lists various alarms with their severity levels and descriptions.

Alarm Title	Severity	Description
High forwarding CPU utilization	Tip	The device's CPU usage is high because it forwards too many data packets
Broadcast multicast ratio is too high	Tip	Broadcast / multicast messages take up too much channel resources
Excessive wired port traffic	Tip	Excessive traffic on the physical interface
Device temperature alarm	Tip	Device temperature abnormality detected
RF does not start	Info	RF is off
High noise floor	Info	AP noise floor is too high
Message congestion	Info	Message congestion
Channel radar avoidance	Tip	The RF working channel has detected a radar and has evaded
Wired port receiving error packets continue to grow	Tip	Continuously receiving error packets on the physical interface of the AP
AP wired port is Down	Info	AP physical interface status is set to DOWN
Wired port negotiation rate is low	Tip	AP physical interface negotiation rate is low <input type="checkbox"/> Enable Periodic Sending (Once a Day)
Wired port receiving resources are insufficient	Tip	The AP physical interface peer sends packets too fast
Wired ports continue to send wrong packets	Tip	The physical interface of the AP continues to send out error messages
Wired ports negotiate half-duplex	Tip	AP physical interface duplex mode negotiation is half duplex
AP temperature alarm	Info	AP temperature abnormality detected
Insufficient sending resources	Info	Insufficient sending resources
Beacon frame sending failed	Info	Beacon frame sending failed
Beacon frame resource is insufficient	Info	Beacon frame resource is insufficient

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

The screenshot displays the Cloudnet interface, specifically the 'Smart O&M' section under 'Alarms'. The page title is 'Alarm List | Subscription'. The left sidebar contains navigation options: Dashboard, Issues, Issue Analysis, Alarms (highlighted), Clients, Network, Optimization, Security, Safeguard, VIP, and AI-Driven Tasks. The main content area shows a list of 15 alarms, each with a checkbox, a severity level dropdown, and a description. A red box highlights the entire list of alarms.

Alarm Name	Severity	Description
Beacon frame resource is insufficient	Info	Beacon frame resource is insufficient
Data message sending failed	Info	Data message sending failed
Insufficient message resources	Info	Insufficient message resources
WAN port uplink bandwidth alarm	Tip	Alarm uplink bandwidth within past 10 minutes on the WAN port: 50 M (Value range: 1-1000. Default: 50).
WAN port downlink bandwidth alarm	Tip	Alarm downlink bandwidth within past 10 minutes on the WAN port: 2 M (Value range: 1-1000. Default: 50)
Large deviation in flow ratio in and out direction	Tip	The proportion of the outgoing and incoming traffic of the device exceeds the preset threshold of the system
High 2.4GHz channel usage	Info	Channel usage of 2.4 GHz radios exceeds 60 % (Range: 20-100, Default: 60).
High 5GHz channel usage	Info	Channel usage of 5 GHz radios exceeds 60 % (Range: 20-100, Default: 60).
Too many clients on 2.4 GHz radios	Info	Number of clients on 2.4 GHz radios exceed 20 (Range: 10-200, Default: 20).
Too many clients on 5 GHz radios	Info	Number of clients on 5 GHz radios exceed 40 (Range: 10-200, Default: 40).
WAN port connectivity	Minor	WAN port connectivity check. Packet loss rate exceeded 10 % (10-100, 10 by default) in 10 minutes
Loop detected on switch port	Minor	Loop detected on switch port
Too much Tx broadcast or multicast traffic	Minor	Broadcast or multicast transmission rate exceeds 100 in the statistics collection period(40-500, 100 by default)
IRF split	Minor	IRF split
STP discarding detected on switch port	Minor	STP discarding detected on switch port

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

The screenshot shows the Cloudnet interface for configuring alarm notifications. The 'Alarms' section is active, and the 'Subscription' tab is selected. A list of alarm types is displayed, with the 'Fault Reports' checkbox checked. Below this, three specific alarm types are checked and highlighted with a red box:

Alarm Type	Severity	Description
<input checked="" type="checkbox"/> Add Fault Report	Tip	A new fault report was submitted and needs processing
<input checked="" type="checkbox"/> Fault Report State Change	Tip	The state of a fault report changed
<input checked="" type="checkbox"/> Doctor AP Test Notifications	Minor	One Doctor AP test notification sent

The 'OK' button is also highlighted with a red box.

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.



- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 **アクセストラフィックの週報、日報のメール送信**
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

装置のあるサイトを選択します

・Sites > Branch > Site

The screenshot displays the H3C Cloudnet management interface. On the left sidebar, the 'Sites' menu item is highlighted with a red box and a circled '1'. At the top, the breadcrumb navigation shows 'Branch: PJ_DEMO' and 'Site: TS Demo', with the 'Site: TS Demo' dropdown menu highlighted by a red box and a circled '2'. The main dashboard area shows various metrics and charts, including 'Online Device Ratio', 'Device Version', 'System Usage', 'Uptime', and 'Alarm Severity'. Below the dashboard, the 'Site Summary' section displays 'Cloudnet' logo, 'AC' (0 Online Devices, 1 Total Devices), and 'Client' (0 Online Clients). The 'Device Information' section includes a table with one device entry: WX2510H-F, AC, WX2510H-F-PWR, TS Demo, Release 5452P03. The 'Network Topology' section shows the last update time and options for auto refresh and discovery.

1

2

Branch: PJ_DEMO Site: TS Demo

Site Summary | Area Management | Time Zone

Online Device Ratio

Device Version System Usage

Alarm Severity Uptime

Online Device Ratio: 1 devices are offline.

Device Version: All devices in the site have been updated to the newest version.

Uptime: All devices are offline.

Alarms: No alarm today. The network is operating correctly.

System Usage: All devices are offline.

Alarm Severity

Critical: 0

Major: 0

Minor: 0

Info: 0

Tip: 0

Site Summary [+ Add Device](#)

Cloudnet

AC

0 1

Online Devices Total Devices

Device List

Client

0

Online Clients

Client List

Device Information

Refresh Delete Restart Upgrade CLI Helper File System Local Management Save Config

Enter device name [Advanced Search](#)

<input type="checkbox"/>	State	Device Name	Category	Model	Site	Device Version	+/-
<input type="checkbox"/>	●	WX2510H-F	AC	WX2510H-F-PWR	TS Demo	Release 5452P03	

Total entries: 1, current entries: 1 - 1. Page 1 of 1

Network Topology

Last Update: 2022-04-16 03:00 (Finished) [Refresh](#)

Auto Refresh OFF [Recalculate](#) [Discover Devices](#)

Show IP Address Show Interface Name [Expand All](#)

[Vertical](#) [Horizontal](#)

ServiceタブからReport Managementを選択します

Service > Report Management

The screenshot displays the H3C Cloudnet management interface. The top navigation bar includes 'Network', 'Smart O&M', and 'Service'. The 'Service' tab is highlighted with a red box and a circled '1'. A dropdown menu is open under 'Service', listing various management options. The 'Report Management' option is highlighted with a red box and a circled '2'. The main content area shows a 'Site Summary' section with a 'Device List' table. The table has the following data:

State	Device Name	Category	Model	Site	Device Version
●	WX2510H-F	AC	WX2510H-F-PWR	TS Demo	Release 5452P03

Below the table, there are controls for 'Auto Refresh' (set to OFF), 'Recalculate', and 'Discover Devices'. The interface also shows a 'Network Topology' section and a 'Cloudnet' status indicator at the bottom.

O&M Reportsの+ Addを選択します

The screenshot displays the H3C O&M Reports management interface. The top navigation bar includes the H3C logo and tabs for 'Network' and 'Smart O&M'. The left sidebar contains 'O&M Reports' (highlighted) and 'Users'. The main content area shows 'O&M Reports' with a header indicating 'Branch: PJ_DEMO' and 'Site: TS Demo'. Below the header, there are four buttons: 'Refresh', '+ Add' (highlighted with a red box), 'Bulk Delete', and 'Report Pushing Records'. A table with columns 'Report Name', 'Report Type', 'Site', and 'Pushing Interval' is shown below the buttons, but it is currently empty.

サイト,発行間隔、レポート形式を選択します

・Service > Report Management

H3C Network Smart O&M Service >

O&M Reports O&M Reports

Users

Return

Add Report Configuration ?

* Report Name: Daily Network Status Report

* Site Name: TS Demo

Report Type: Network O&M

Pushing Interval: Daily

Report Format: HTML

Receiver Accounts: HTML, PDF

Remarks: 1-255 chars

Save Cancel

review

レポートのサンプルが表示されます

- ・サイトの指定
- ・発行間隔
- ・レポート形式

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

The screenshot shows the H3C O&M Reports configuration interface. The main page is titled 'O&M Reports' and includes a sidebar with 'Users' and 'O&M Reports' sections. The main content area is titled 'Add Report Configuration' and contains several form fields:

- * Report Name: Daily Network Status Report
- * Site Name: TS Demo
- Report Type: Network O&M
- Pushing Interval: Daily
- Report Format: HTML

Below these fields is the 'Receiver Accounts' section, which includes a '+ Add Email' button (circled with a red '1') and a 'Remarks' text area. At the bottom of the main form are 'Save' and 'Cancel' buttons.

An 'Email Addresses' dialog box is open in the foreground. It features a 'Refresh' button and an 'Add Account' button (circled with a red '2' and highlighted with a red box). The dialog contains a table with the following data:

<input type="checkbox"/>	Account Name	Remarks	Q
<input type="checkbox"/>	koshiro		

At the bottom of the dialog, it shows 'Total entries: 1, current entries: 1 - 1. Page 1 of 1' and '10 Entries' per page. The dialog also has 'OK' and 'Cancel' buttons.

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

The screenshot displays the H3C O&M Reports interface. The main content area is titled 'Email Configuration' and includes a '+ Add' button, which is circled with a red '1'. Below this is a table with columns for 'Account Name' and 'Account'. An 'Add Configuration' dialog box is open, titled 'Add Configuration' and circled with a red '2'. The dialog contains the following fields:

- * Account Name: manager
- * Email Address: manager@h3c.com
- Remarks: site manager mail address

The 'OK' button in the dialog is circled with a red '3'.

登録したメールアドレスを選択します

The screenshot shows the H3C O&M Reports configuration interface. The main page is titled "O&M Reports" and includes a sidebar with "Users" and "O&M Reports" sections. The main content area is titled "Add Report Configuration" and contains several form fields:

- * Report Name: Daily Network Status Report
- * Site Name: TS Demo
- Report Type: Network O&M
- Pushing Interval: Daily
- Report Format: HTML
- Receiver Accounts: + Add Email
- Remarks: 1-255 chars

An "Email Addresses" dialog box is open, showing a table of accounts. The "koshiro" account is selected, and the "OK" button is highlighted. The dialog box also includes a "Refresh" button, an "Add Account" link, and pagination information.

<input checked="" type="checkbox"/>	Account Name	Remarks	Q
<input checked="" type="checkbox"/>	koshiro		

Total entries: 1 , current entries: 1 - 1. Page 1 of 1

10 Entries per page

OK Cancel

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

H3C Network Smart O&M Service

O&M Reports

Users

Return

Add Report Configuration ?

* Report Name: Daily Network Status Report

* Site Name: TS Demo

Report Type: Network O&M

Pushing Interval: Daily ?

Report Format: HTML Preview

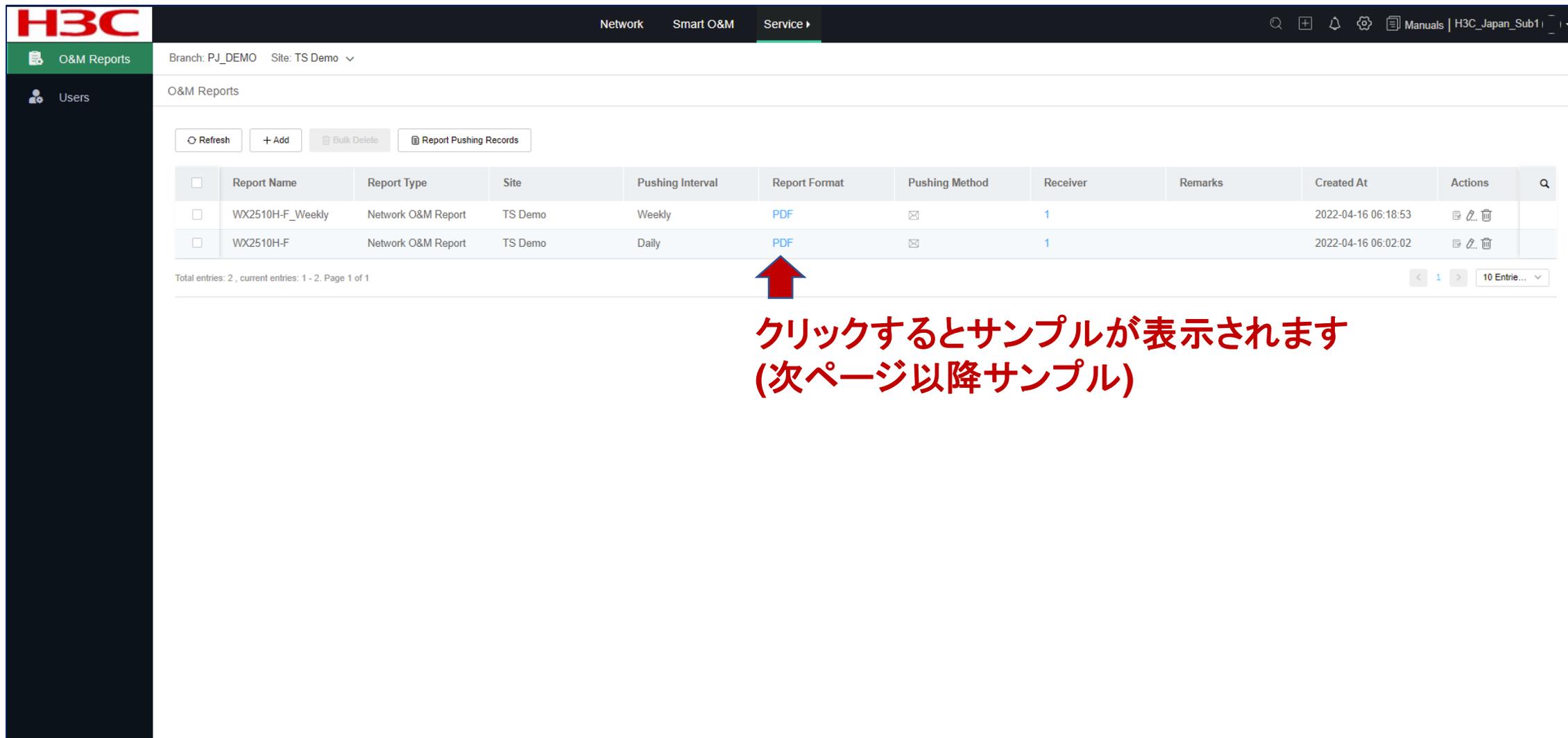
Receiver Accounts: + Add Email **koshiro@**

Remarks: 1-255 chars

2 Save Cancel

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



The screenshot displays the H3C O&M Reports management interface. The top navigation bar includes 'Network', 'Smart O&M', and 'Service'. The main content area shows a table of O&M Reports with the following columns: Report Name, Report Type, Site, Pushing Interval, Report Format, Pushing Method, Receiver, Remarks, Created At, and Actions. Two reports are listed: 'WX2510H-F_Weekly' (Weekly interval, PDF format) and 'WX2510H-F' (Daily interval, PDF format). A red arrow points to the 'PDF' link in the 'Report Format' column of the 'WX2510H-F' row.

<input type="checkbox"/>	Report Name	Report Type	Site	Pushing Interval	Report Format	Pushing Method	Receiver	Remarks	Created At	Actions
<input type="checkbox"/>	WX2510H-F_Weekly	Network O&M Report	TS Demo	Weekly	PDF	☒	1		2022-04-16 06:18:53	📄 🗑️
<input type="checkbox"/>	WX2510H-F	Network O&M Report	TS Demo	Daily	PDF	☒	1		2022-04-16 06:02:02	📄 🗑️

Total entries: 2 , current entries: 1 - 2. Page 1 of 1

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/CgAAHmJhARI5gAAS_rJvrMmw139.pdf](http://oasiscloudportal.h3c.com/group1/M00/00/6B/CgAAHmJhARI5gAAS_rJvrMmw139.pdf)

Daily Reportのサンプルです

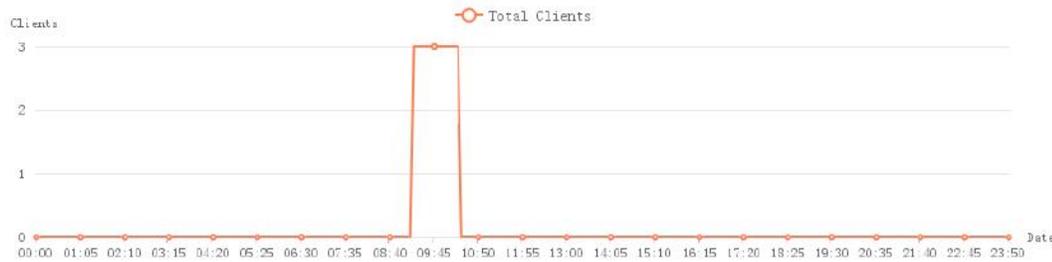
Daily Business Report

TS Demo
2022-04-21

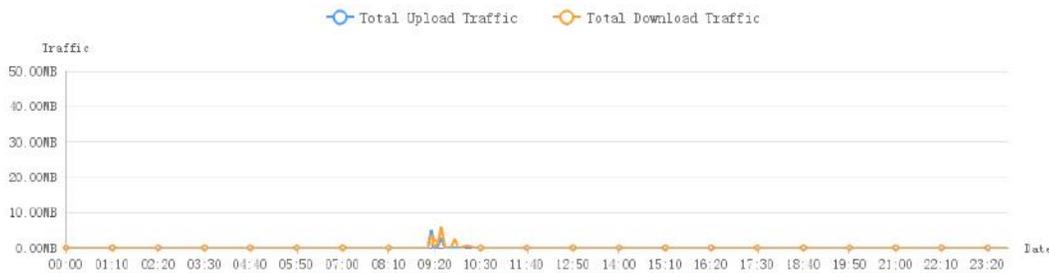
Access Clients Statistics



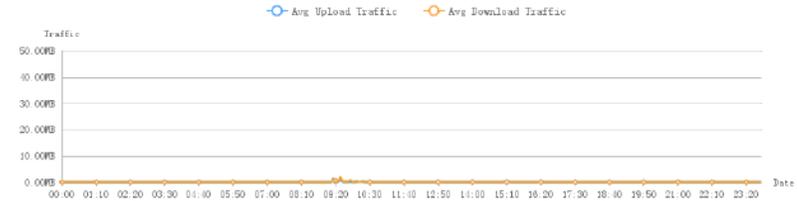
Access Client Trend



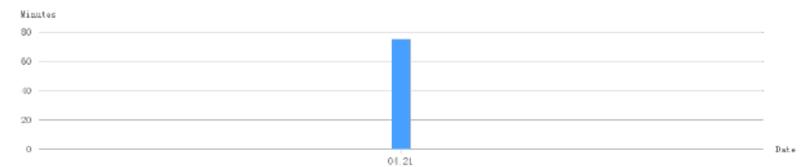
Access Client Total Traffic Trend



Access Client Avg Traffic Trend



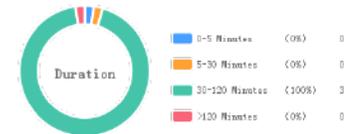
Average Online Duration Trend



Access Client Proportion



Online Duration Proportion



Number of Week Visits



By SSID



By Client Vendor





- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

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

Branch: H3C Site: H3C 神谷町オフィス Device/Area: All Devices Client: 31 | 5G 26 | 2.4G 5 | AP: 4 | AC: 1

Health Today Yesterday Last Seven Days Custom

AP Health

AP Quantity

Excellent Good Average

AP Radio Details Collected At: 09/17 10:35

Export Filter

AP Name	AC Name	AP Score	Deduction	Radio	Health	Online Clients	RSSI	Channel	Channel Usage
AP01	AC	100	-	1	Excellent	10	46db	60	3%
AP01	AC	100	-	2	Excellent	9	50db	100	2%
AP01	AC	100	-	3	Excellent	2	56db	11	18%
AP02	AC	100	-	1	Excellent	0	0db	36	0%
AP02	AC	100	-	2	Excellent	0	0db	100	6%
AP02	AC	100	-	3	Excellent	0	0db	1	16%
AP03	AC	100	-	1	Excellent	2	56db	36	1%

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) – 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

The screenshot displays the H3C Cloudnet Smart O&M interface. The 'Smart O&M' tab is selected in the top navigation bar. The left sidebar shows the 'Wireless' section highlighted. The main content area is titled 'Client Health' and features a bar chart showing client health status over time. A data table is overlaid on the chart, providing a summary of health metrics for 5GHz, 2.4GHz, and Total clients.

	Excellent	Good	Average	Idle	Total
5GHz	1	7	0	3	11
2.4GHz	0	2	1	0	3
Total	1	9	1	3	14

Below the chart, the 'Health Details' section shows a table of client information collected at 09/17 10:35. The table includes columns for MAC, VIP Level, Username, Auth Method, IPv4, IPv6, Security, RF Band, Client Score, Deduction, Health, and SSI.

MAC	VIP Level	Username	Auth Method	IPv4	IPv6	Security	RF Band	Client Score	Deduction	Health	SSI
8c45-00dd-bb8d	Non-VIP		Unauth	192.168.100.36	-	WPA2-Personal	2.4GHz	75	Packet Loss Rate:20, Retransmission Rate:5	Good	H3C
40a3-ccab-bc74	Non-VIP		Unauth	10.66.209.11	-	WPA2-Personal	5GHz	80	Packet Loss Rate:20	Good	H3C
9cfc-e89d-377b	Non-VIP		Unauth	192.168.100.35	-	WPA2-Personal	5GHz	80	Packet Loss Rate:20	Good	H3C
6263-a6ba-60ba	Non-VIP		Unauth	192.168.100.14	-	WPA2-Personal	5GHz	78	Packet Loss Rate:20, Retransmission Rate:2	Good	H3C
d4d2-52b3-8b98	Non-VIP		Unauth	192.168.100.29	-	WPA2-Personal	5GHz	80	Packet Loss Rate:20	Good	H3C
f4d1-08b8-c5d6	Non-VIP		Unauth	192.168.100.42	-	WPA2-Personal	5GHz	80	Packet Loss Rate:20	Good	H3C

Cloudnetの活用例 – Expert Mode表示

The screenshot displays the H3C Cloudnet Expert Mode interface. The top navigation bar includes 'Network', 'Smart O&M', and 'Service'. The left sidebar has 'Wireless' highlighted. The main content area is divided into several sections:

- Statistics:** Shows Uplink Rate (71.9Mbps), Downlink Rate (65.4Mbps), and Average RSSI (53db).
- Basic Client Info:** Lists details such as MAC (1098-c3e4-9da0), IP (192.168.100.37), Vendor (Samsung), and Device name (Canon).
- Connection Info:** Shows the current state as 'Online' with a score of 71. It details the Client (1098-c3e4-9da0), SSID (H3C-Guest), AP (AP01), and AC.
- Score Trend:** A line graph showing the score trend over time from 09/17 00:00:00 to 09/17 10:05:00.
- Client Logs:** A section on the right with a time range filter set to 2021-09-17.

Cloudnetの活用例 - Expert Mode表示

The screenshot displays the H3C Cloudnet Expert Mode interface. The top navigation bar includes 'Network', 'Smart O&M', and 'Service'. The left sidebar has 'Wireless' highlighted. The main content area is divided into several sections:

- Client Info:** Shows client details for 1098-c3e4-9da0, including AP (AP01) and AC (AC).
- Client Details:** A blue box containing technical specifications: MAC: 1098-c3e4-9da0, IPv4: 192.168.100.37, IPv6: -, Vendor: Samsung, RF Band: 2.4GHz, Protocol Type: 802.11gn, Username, Device Name: Canond28521, System Info: Canon MF741C/743C, Channel: 11, and Remarks.
- Health Report:** A table comparing current values to reference values for various metrics.
- Client Connection Info:** A series of line graphs showing Retransmission Rate, Uplink Traffic, Downlink Traffic, Uplink Packets, Downlink Packets, Channel Usage, RSSI, Uplink Rate, Downlink Rate, Latency, Packet Loss Rate, and Radio Load.
- Neighbor Client:** A section for monitoring neighboring clients.

Metric	Current Value	Reference Value
RSSI	53db	>30db
Channel Usage	18%	<40%
Uplink Rate	71.9Mbps	>43.3Mbps
Downlink Rate	65.4Mbps	>57.8Mbps
Uplink Traffic	352.3KB	-
Downlink Traffic	39.5KB	-
Latency	16.718ms	<15ms
Packet Loss Rate	47.76%	<1%
Retransmission Rate	22.14%	<5%
Association Duration	80ms	-
Authentication Duration	0ms	-

Cloudnetの活用例 – クライアントのRSSI等

Client Connection Info

Vendor: Samsung Client MAC: 1098-c3e4-9da0 Client IP: 192.168.100.37 AP Name: AP01 Channel: 11 Radio: 3

Packet Loss Rate:

Channel Usage:

Uplink and Downlink Packets:

Uplink ARP Packets:

Latency:

Uplink and Downlink Traffic:

Uplink ARP Rate:

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) – 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。

↓

RSSI:

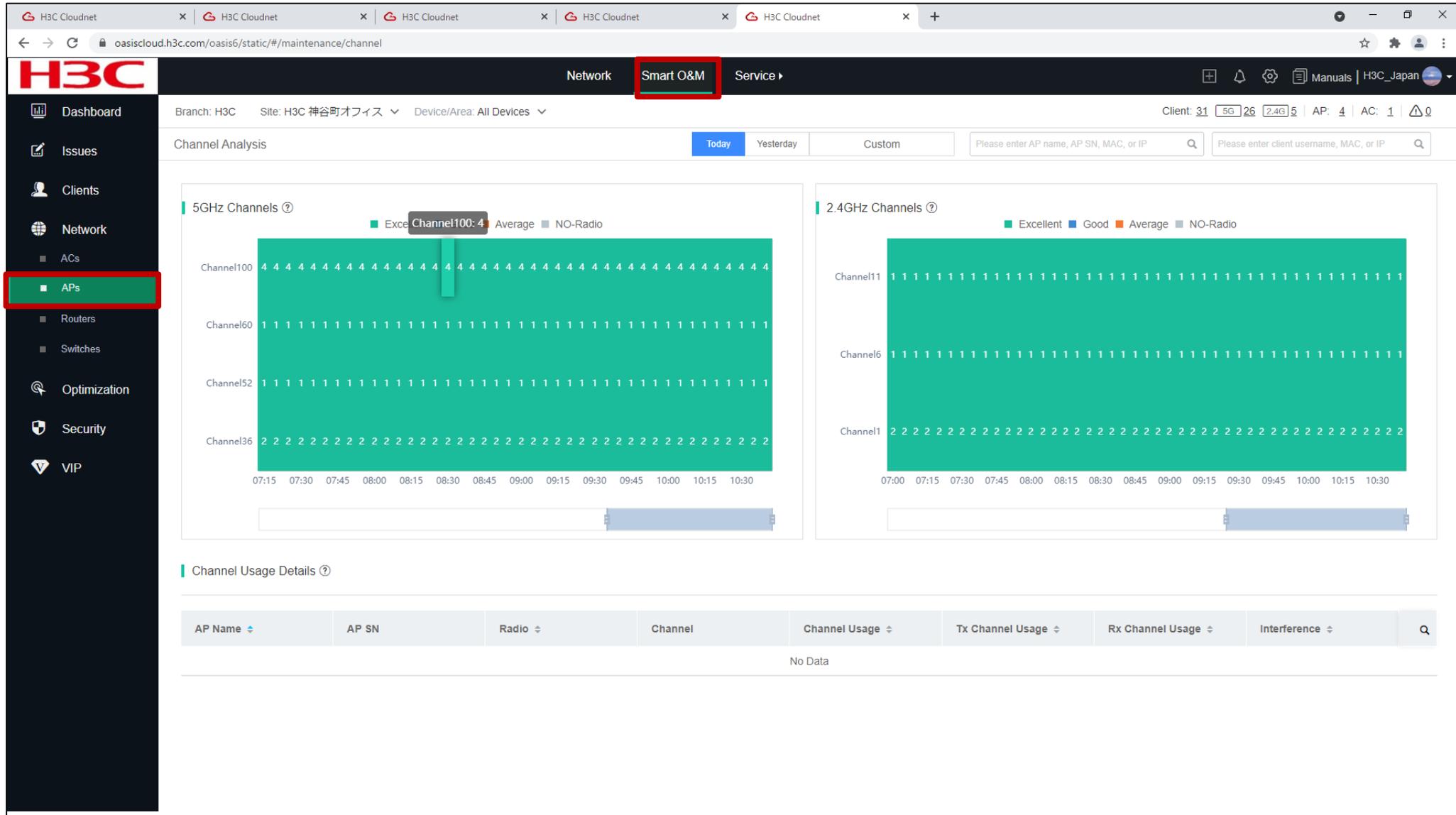
OK Cancel

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) – 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

The screenshot displays the H3C Cloudnet web interface. The browser address bar shows the URL `oasiscloud.h3c.com/oasis6/static/#/net/network/sitecollection/site`. The top navigation bar includes 'Network' (highlighted with a red box), 'Smart O&M', and 'Service'. The left sidebar menu has 'Sites' highlighted with a green box. The main content area shows a network topology map for 'Branch: H3C' and 'Site: H3C 神谷町オフィス'. The map includes a 'Cloudnet' node at the top, connected to an 'MSR830' router. Below the router are several 'Terminal' nodes and a switch node 'S5024PV3-EI-HP...'. At the bottom, there are nodes for 'AP03' (Type: AP), 'AC' (Type: AC), 'UISnode1' (Type: Other), and 'OM' (Type: Other). The interface also features controls for 'Auto Refresh' (OFF), 'Recalculate', 'Discover Devices', and options to 'Show IP Address' and 'Show Interface Name'. A legend on the left side of the map area includes icons for '+', '-', a list icon, and a camera icon. The map area also has 'Vertical' and 'Horizontal' view toggles and an 'Expand All' dropdown menu.



- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

```

#
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

```



- 01 WIPS機能概要
- 02 検証機器構成
- 03 CloudnetでWIPS検知機能を有効にする
- 04 攻撃ツールで攻撃をする
- 05 CloudnetでWIPS検知状況を表示する
- 06 ACのGUIでWIPS検知状況を表示する
- 07 Cloudnetで検知した攻撃を管理者にメールで伝える
- 08 アクセストラフィックの週報、日報のメール送信
- 09 参考: ACのCloudnetへの登録方法
- 10 参考: ACのコンフィグ例
- 11 参考: Anchor-ACでのWIPS検知機能の有効化

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

H3C WLAN Management Platform

WA6320-JP

Remember username

English ▾

Login

Internet Explorer 10, Firefox 30.0.0.5269, Chrome 35.0.1916.114, Safari 5.1, and their higher versions are supported.

ACのGUIのメニュー一覧

• Network view

Actions		
Dashboard		
Quick Start	>	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
Monitoring	>	
Wireless Configuration	>	
Network Security	>	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
System	>	
Tools	>	
Reporting	>	

System View

Network View

ACのGUIのメニュー一覧(続き)

• System view

Actions
Dashboard
Network Configuration >
Network Security >
System >
Tools >

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

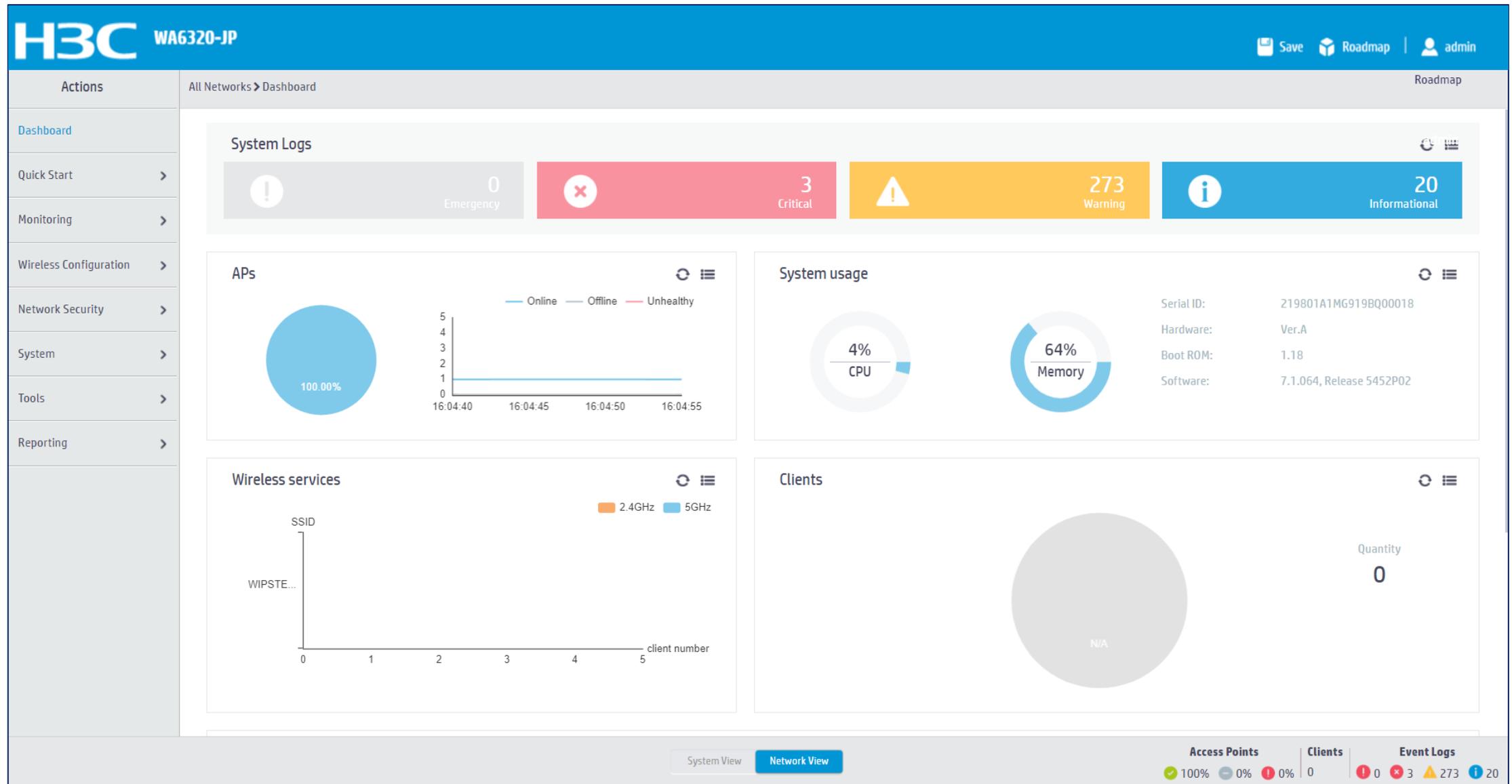
Tools

Debug

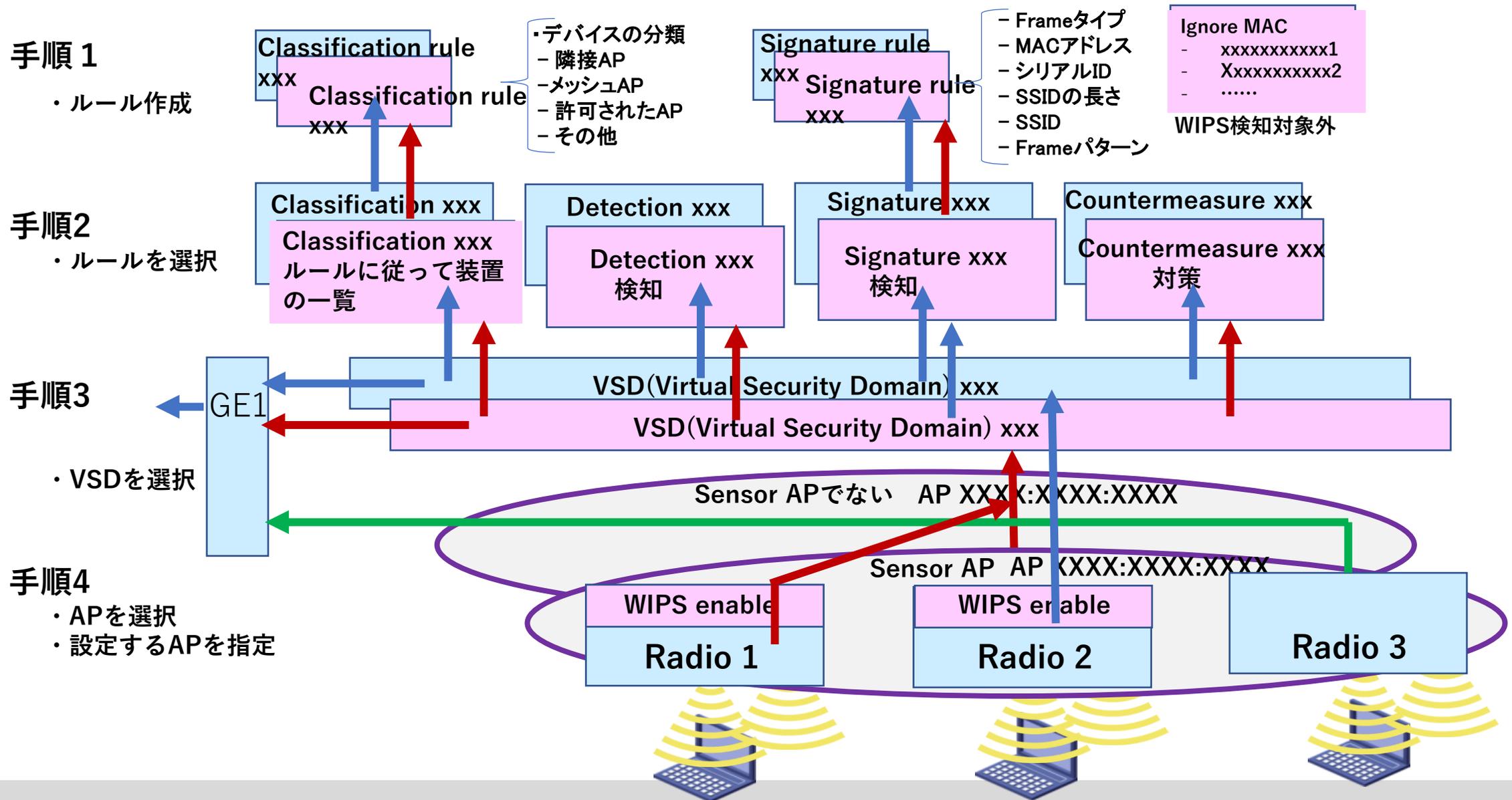
System View

Network View

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

The screenshot displays the H3C WA6320-JP GUI. The left sidebar contains a navigation menu with the following items: Actions, Dashboard, Quick Start, Monitoring, Wireless Configuration (highlighted with a red box and circled '1'), Wireless Networks, AP Management, Wireless QoS, Wireless Security (highlighted with a red box and circled '2'), WIPS (highlighted with a red box and circled '3'), Allowlist and denylist, Radio Management, Client Proximity Sensor, Applications, Network Security, System, and Tools. The main content area shows the breadcrumb path: All Networks > Wireless Configuration > Wireless Security > WIPS > Detection. The 'Detection' tab is highlighted with a red box and circled '4'. Below the breadcrumb, there are several tabs: WIPS Enable, VSD, Classification (circled '5'), Detection, Signature, Countermeasure, Classification rule, Signature rule, and Ignore MAC. The 'Detection' tab is active, showing a table with columns for Policy Name, Flood Attack Detection, Malformed Packet Detection, and Actions. The table is currently empty. At the bottom of the page, there are buttons for System View and Network View (highlighted with a red box), and a status bar showing Access Points (1 green, 0 blue, 0 red), Clients (1), and Event Logs (0 red, 3 blue, 58 yellow, 19 blue).

ACのGUIでAPでのWIPS検知ポリシーを設定する（続き）

1 Policy name * (1-63 chars)

Rate Limit Type	Interval(s)	Threshold	Quiet(s)
AP	60	256	1200
Client	60	512	1200

2 Flood attack detection

Device Type	Inactive Time(s)	Aging Time(s)
AP	300	600
Client	300	600

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。

Status	Type	Interval(s)	Threshold	Quiet(s)
<input type="checkbox"/>	Association request	60	50	600
<input type="checkbox"/>	Authentication	60	50	600
<input type="checkbox"/>	Beacon	60	50	600
<input type="checkbox"/>	Block ack	60	50	600
<input type="checkbox"/>	CTS	60	50	600
<input type="checkbox"/>	Deauthentication	60	50	600
<input type="checkbox"/>	Disassociation	60	50	600

System View Network View

Access Points: 1 0 0 0 Clients: 0 Event Logs: 0 5 7 7

ACのGUIでAPでのWIPS検知ポリシーを設定する（続き）

Actions

All Networks > Wireless Configuration > Wireless Security > WIPS > Detection > Add Policy

Save Roadmap admin

Dashboard Eapol success 60 50 600

Quick Start >

Monitoring >

Wireless Configuration >

Wireless Networks

AP Management

Wireless QoS

Wireless Security >

WIPS

Allowlist and denylist

Radio Management

Applications

Network Security >

System >

Tools >

Malformed packet detection

Status	Type	Quiet(s)
<input type="checkbox"/>	Duplicated IE	600
<input type="checkbox"/>	Fata jack	600
<input type="checkbox"/>	Illegal ibss ess	600
<input type="checkbox"/>	Invalid address combination	600
<input type="checkbox"/>	Invalid assoc req	600
<input type="checkbox"/>	Invalid auth	600
<input type="checkbox"/>	Invalid assoc req	600
<input type="checkbox"/>	Invalid disassoc code	600
<input type="checkbox"/>	Invalid HT IE	600
<input type="checkbox"/>	Invalid IE length	600
<input type="checkbox"/>	Invalid pkt length	600
<input type="checkbox"/>	Null probe resp	600
<input type="checkbox"/>	Overflow eapol key	600
<input type="checkbox"/>	Overflow ssid	600
<input type="checkbox"/>	Redundant IE	600

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。

System View Network View

Access Points Clients Event Logs

1 0 0 0 0 5 7 7

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。

Man-in-the-middle attack Quiet time: 600 seconds(5-604800,600 by default)

AP impersonation Quiet time: 600 seconds(5-604800,600 by default)

Honeypot AP Quiet time: 600 seconds(5-604800,600 by default) Similarity: 80 %(70-100,80 by default)

Apply 3

System View Network View

Access Points: 1 0 0 0 Clients: 0 0 0 0 Event Logs: 1 0 5 7 1 7

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

The screenshot displays the H3C WA6320-JP management interface. The breadcrumb navigation path is: All Networks > Wireless Configuration > Wireless Security > WIPS > Countermeasure. The interface includes a left sidebar with navigation options and a main content area with a table of countermeasures.

Navigation Path:

1. Wireless Configuration
2. Wireless Security
3. WIPS
4. Countermeasure
5. Add (+) button

Table Headers:

Policy Name	ClassifyTypeCount	Manual Countermeasures MAC	Select Sensors Status	Actions
-------------	-------------------	----------------------------	-----------------------	---------

Footer: Total 1 entries, 1 matched, 0 selected. Page 1 / 1.

System View / Network View: Network View is selected.

Access Points / Clients / Event Logs: Access Points: 1 (green), 0 (grey), 0 (red); Clients: 1 (red); Event Logs: 0 (red), 3 (grey), 54 (yellow), 8 (blue).

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

H3C WA6320-JP

Save Roadmap admin

Actions All Networks > Wireless Configuration > Wireless Security > WIPS > Countermeasure > Edit Policy

Dashboard

Quick Start >

Monitoring >

Wireless Configuration >

Network Security >

System >

Tools >

Reporting >

Policy name * **1** stop_attack (1-63 chars)

Categories

- External AP
- Misconfigured AP
- Potential-authorized AP
- Potential-external AP
- Potential-rogue AP
- Rogue AP
- Uncategorized AP
- Unauthorized client
- Misassociated client
- Uncategorized client
- 2** Attack
- Ad hoc

MAC address

MAC Address

HH-HH-HH-HH-HH-HH

Select sensor all **3**

4 Apply

System View Network View

Access Points Clients Event Logs

1 0 0 0 0 9 13 23

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

The screenshot displays the H3C WA6320-JP management interface. The breadcrumb navigation path is: All Networks > Wireless Configuration > Wireless Security > WIPS > VSD. The 'VSD' tab is highlighted with a red box and a circled '1'. Below the tabs, there is a search bar and a '+ Add' button highlighted with a red box and a circled '2'. The main content area is a table with columns: Name, Classification Policy, Detection Policy, Signature Policy, Countermeasure Policy, and Actions. The table is currently empty. At the bottom of the page, there is a status bar showing 'Total 7 entries, 1 matched, 0 selected. Page 1 / 1.' and a footer with 'System View' and 'Network View' buttons, along with statistics for Access Points (1 green, 1 grey, 1 red), Clients (1), and Event Logs (4 red, 10 grey, 362 yellow, 136 blue).

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

The screenshot displays the H3C WA6320-JP management interface. The top navigation bar includes 'Save', 'Roadmap', and 'admin' user information. The left sidebar shows the navigation menu with 'Wireless Security' expanded to 'WPS'. The main content area is titled 'All Networks > Wireless Configuration > Wireless Security > WPS > VSD > Edit Vsd'. The configuration fields are as follows:

- VSD name ***: Input field containing 'Sec_domain' (1-63 chars).
- Classification policy**: Dropdown menu showing 'Select...'.
- Detection policy**: Dropdown menu showing 'standard'.
- Signature policy**: Dropdown menu showing 'Select...'.
- Countermeasure policy**: Dropdown menu showing 'stop_attack'.

At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons. The bottom status bar shows 'System View' and 'Network View' tabs, along with statistics for Access Points (1 green, 1 grey, 1 red, 0 blue), Clients (1), and Event Logs (4 red, 10 grey, 362 yellow, 136 blue).

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

The screenshot shows the H3C WA6320-JP management interface. The breadcrumb path is "All Networks > Wireless Configuration > Wireless Security > WIPS > WIPS Enable". The "WIPS Enable" tab is highlighted with a red box. Below the breadcrumb, there are tabs for "VSD", "Classification", "Detection", "Signature", "Countermeasure", "Classification rule", "Signature rule", and "Ignore MAC". A search bar is present on the right. The main content area displays a table with the following data:

<input type="checkbox"/>	AP Name ▲	Status	Radios	VSD Name	Actions
<input type="checkbox"/>	5ca7-21e7-38a0	Online	5GHz(1),2.4GHz(2)	Sec_domain	<input type="checkbox"/>

The "Actions" column for the selected AP is highlighted with a red box. At the bottom of the page, there are navigation buttons for "System View" and "Network View", and a status bar showing "Access Points" (1 green, 1 grey, 1 red), "Clients" (1), and "Event Logs" (4 red, 10 grey, 362 yellow, 136 blue).

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

The screenshot displays the H3C WA6320-JP management interface. The main content area shows the configuration for WIPS (Wireless Intrusion Prevention System) on a specific AP (5ca7-21e7-38a0). A modal dialog titled "Enable WIPS" is open, allowing the user to configure the WIPS settings for this AP. The dialog includes the following fields:

- AP name:** 5ca7-21e7-38a0
- Radio list:** A dropdown menu showing "5GHz(1)" and "2.4GHz(2)" selected. The entire list is highlighted with a red box.
- VSD name:** Sec_domain (highlighted with a red box).
- Buttons:** "Apply" (highlighted with a red box) and "Cancel".

The background interface shows the "WIPS Enable" configuration page with various tabs like "WSD", "Classification", "Detection", etc. The left sidebar contains navigation options such as "Dashboard", "Monitoring", "Wireless Configuration", and "Wireless Security". The bottom status bar shows system metrics like "Access Points", "Clients", and "Event Logs".

SSIDを作成します

H3C WA6320-JP Save Roadmap | admin

Actions: All Networks > Quick Start > Add Services > Add Services

Dashboard: Add Services

Quick Start

Add AP

Add Services

Add User

Monitoring >

Wireless Configuration >

Network Security >

System >

Tools >

Reporting >

1 Basic settings

Wireless service name: WIPS (1-63 chars)

2 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

3

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

4 Apply and Configure Advanced Settings Apply

System View Network View

Access Points: 1 (green), 0 (grey), 0 (red)

Clients: 0

Event Logs: 0 (red), 5 (red), 12 (yellow), 14 (blue)

SSIDを載せる電波を選択します

H3C WA6320-JP

Save Roadmap admin

All Networks > Quick Start > Add Services > Add Services > Advanced Settings(wips2)

WLAN Authentication Authorization Intrusion Protection Key Management **Binding** Access Control

Bind to APs

Candidate

Search for

→

2 f010-903e-f7e0 (Radio3 2.4G)

Selected

Search for

←

f010-903e-f7e0 (Radio1 5G)

f010-903e-f7e0 (Radio2 5G)

3 Apply

System View Network View

Access Points Clients Event Logs

1 0 1 0 0 0 5 12 14

APが電波を出すようにします

The screenshot displays the H3C WA6320-JP management interface. The left sidebar contains a navigation menu with the following items: Actions, Dashboard, Quick Start, Monitoring, Wireless Configuration (highlighted with a red box and circled '1'), Wireless Networks, AP Management (highlighted with a red box and circled '2'), Wireless QoS, Wireless Security, Radio Management, Applications, Network Security, System, Tools, and Reporting. The main content area is titled 'All Networks > Wireless Configuration > AP Management > AP' and shows 'AP Groups' with a search bar and a table of AP entries. The table has columns: Name, Installation Date, Description, AP Group, Type, Model, Serial ID, MAC Address, Radios, Status, and Actions. One entry is visible: Name 'f010-903e-f7e0', Installation Date '2022-06-29', AP Group 'default-group', Type 'Manual AP (E...', Model 'WA6638', Serial ID '219801A24F8201...', MAC Address 'F0-10-90-3E-F7-E0', Radios '802.11ax(5GHz)(1...', Status 'Online', and Actions (highlighted with a red box and circled '3'). The bottom status bar shows 'Total 7 entries, 7 matched, 0 selected. Page 1 / 1.' and a summary of system metrics: Access Points (1 green, 0 grey, 0 red), Clients (0), and Event Logs (0 red, 5 yellow, 36 blue).

Name	Installation Date	Description	AP Group	Type	Model	Serial ID	MAC Address	Radios	Status	Actions
f010-903e-f7e0	2022-06-29		default-group	Manual AP (E...	WA6638	219801A24F8201...	F0-10-90-3E-F7-E0	802.11ax(5GHz)(1...	Online	[Edit] [Delete]

SSIDを載せる電波を選択して設定を保存(save)します

The screenshot displays the H3C WA6320-JP configuration interface for AP Management. The breadcrumb path is: All Networks > Wireless Configuration > AP Management > AP > Edit AP (f010-903e-f7e0). The interface is divided into several sections:

- Left Sidebar:** Contains navigation menus for Dashboard, Quick Start, Monitoring, Wireless Configuration (expanded), Wireless Networks, AP Management (selected), Wireless QoS, Wireless Security, Radio Management, Applications, Network Security, System, Tools, and Reporting.
- Form Fields:** Includes text boxes for Installation position (city/district/county), Installation position (street), Detail Installation position, AP description, and Remarks.
- Configuration Parameters:**
 - Region code: UNITED KINGDOM(GB)(Inhe... x v
 - LED mode: Normal(Inherit) x v
 - Map File: Select... v
 - AP connection priority: 4(Inherit) (0-7, Inherit by default)
 - CAPWAP tunnel keepalive: Echo interval 10(Inherit) seconds (0,5-255, Inherit by default)
 - Request retransmission: Interval 5(Inherit) seconds (3-8, Inherit by default); Retransmission attempts 3(Inherit) (2-5, Inherit by default)
 - Statistics report interval: 50(Inherit) seconds (0-240, Inherit by default)
 - AC Election: OFF (selected)
 - CAPWAP tunnel encryption: Inherit (Disabled) (selected)
 - Firmware upgrade: Inherit (Enabled) (selected)
 - Radio Selection (highlighted with a red box and '1'): 5GHz(1) radio ON, 5GHz(2) radio ON, 2.4GHz(3) radio ON.
- Buttons:** 'Apply' (highlighted with a red box and '2') and 'Cancel' buttons are located at the bottom left. A 'Save' button (highlighted with a red box and '3') is located in the top right corner.
- Bottom Bar:** Shows 'System View' and 'Network View' tabs, and a status bar with 'Access Points' (1 green, 0 red, 0 yellow), 'Clients' (0), and 'Event Logs' (1 red, 0 yellow, 36 blue, 22 grey).

ACのGUI画面でWIPSで検知した状況を確認

- Network View > Monitoring > Wireless Security

The screenshot displays the H3C WA6320-JP GUI. The sidebar on the left has 'Monitoring' (1) and 'Wireless Security' (2) highlighted. The main content area shows WIPS monitoring data. A red arrow labeled '更新' (Update) points to a refresh icon in the top right of the 'Attack statistics' section.

Attack statistics

0.00% (0.00%)

40.24% (40.24%)

59.76% (59.76%)

Flood

55,145

Attack Type	Count
CTS	10691
BlockAck	13864
Beacon	15694
Authentication	0
AssociationRequest	0

Malformed packet

37,129

Attack Type	Count
MalformedAssocRequest	0
InvalidSourceAddress	52
AbnormalBSS&ESS	0
FATA-Jack	0
DuplicateIE	4

Others

0

Attack Type	Count
ClientSpoofAP	0
AdhocSpoofAP	0
APSpoofAdhoc	0
APSpoofClient	0
APSpoofAP	0

Device information

92% AP

8% Client

AP: 84

Client: 7

Countermeasure Statistics

Category	Count	Percentage
Att	36	100%
Manu	0	0%
Black	0	0%
Ass	0	0%
Class	0	0%

System View | **Network View**

Access Points: 1 (green), 0 (grey), 0 (red) | Clients: 1 (red), 0 (red), 3 (red), 70 (yellow), 19 (blue)

H3C

The Leader in Digital Solutions

www.h3c.com