



WCSを用いた WLANの集中管理



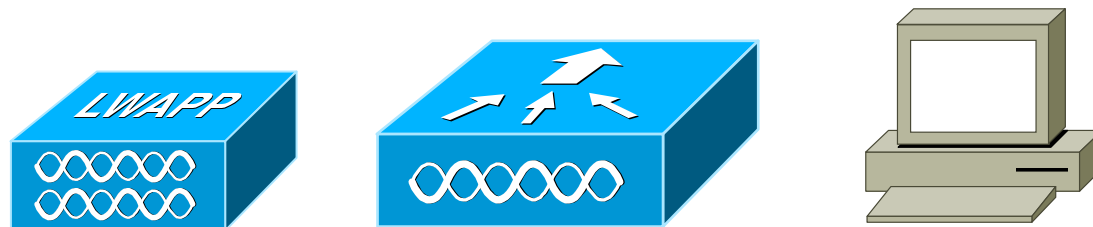
シスコシステムズ合同会社
ソリューションズ システムズ エンジニアリング
システムズ エンジニア
Richard Li

背景

- 今日、ビジネス要求に柔軟に対応するため、無線LANを導入する企業は増加傾向にあります。
- 無線LANは従来の接続手段から、ゲストアクセスやVoice over WLANなどのサービスを支えるプラットフォームに進化しています。
- 無線LANの導入効果を最大限に発揮するには、PPDIOOのオペレーションと最適化が重要であり、効率的に効果的に無線LANをマネジメントする必要があります。



集中型アーキテクチャのコンポーネント



■ AP

CAPWAP・アクセスポイントは、全てのユニファイド・ワイヤレス・アーキテクチャで使用され、クライアントの無線アクセスを提供するとともに、WLCへトンネルします

■ WLC

シスコ・ユニファイド無線LANコントローラは、無線クライアントのトラフィックを集約し、無線ネットワークを制御します

■ WCS

シスコ無線コントロールシステムは、集中管理、無線プランニングおよび可視化ツール、およびロケーション・サービスを提供します

WLAN運用・管理のタスク

TASKS?

1. 日常状況の把握
クライアントデバイス・ネットワーク資源の利用効率・WLANシステムのパフォーマンス・セキュリティなど、WLANの状況を定期的に情報収集
2. インシデントの把握
ネットワーク機器がダウンしたか・不正デバイスが発見されたか・WLANシステムが攻撃されたか、などのインシデントをリアルタイムに把握
3. インシデントの対応
WLAN機器がダウンした場合、再起動したり、交換したりする、不正AP・クライアントが検知された場合、位置を把握し、排除する、etc.

どんな日常状況を把握すべきか

WHAT DO YOU NEED TO KNOW?

- どんなデバイスがWLANに接続しているか？
- どのくらいのトラフィックが流れているか？
- WLANデバイスへの負荷がどのくらいあるか？
- 無線環境はクリアなのか？
- 過去にWLANが攻撃されていたか？
- 過去に社内に不正AP・不正クライアントが存在したか？
- VoWLANの場合、QoSがちゃんと守られているか？
- Etc.

- Client**
 - Busiest Clients
 - Client Count
 - Client Sessions
 - Client Summary
 - Client Traffic Stream Metrics
 - Throughput
 - Unique Clients
 - v5 Client Statistics
- Compliance
- Device
- Guest
- Mesh
- Network Summary
- Performance
- Security

Report Launch Pad

Reports > Report Launch Pad

Client	
Busiest Clients	New
Client Count	New
Client Sessions	New
Client Summary	New
Client Traffic Stream Metrics	New
Throughput	New
Unique Clients	New
v5 Client Statistics	New
Compliance	
Configuration Audit	New
PCI	New
Device	
AP Profile Status	New
AP Summary	New
Busiest APs	New
Utilization	New

Mesh	
Alternate Parent	New
Link Stats	New
Nodes	New
Packet Stats	New
Stranded APs	New
Worst Node Hops	New
Network Summary	
802.11n Summary	New
Executive Summary	New
Performance	
802.11 Counters	New
Coverage Hole	New
Network Utilization	New
Traffic Stream Metrics	New
Tx Power and Channel	New
Graph	New
Table	New
Voice Statistics	New

8種類、合計46項目のレポートを提供できます。

日常状況の把握 クライアント サマリ

Client Summary : New
Reports > Report Launch Pad > Client > Client Summary > Client Summary Report Details

Save Save and Run Run Now Cancel

Settings

Report Title: Client Summary

Reporting Period: Last 7 Days

From: [] : []

To: [] : []

Schedule

Scheduling: Enable

Export Format: CSV

Destination: File C:\ftproot\reports\ClientSummary\<ReportTitleName> <yyyymmdd> <HHMMSS>

Email: wcs-alerts@cisoo.com

Start Date/Time: 10/08/2009 03 : 45

Current Server Time: 10/08/2009 03:41:57 GMT

Recurrence: No Recurrence Hourly Daily Weekly

Customize Report

Click here to customize report content based on your preference. Customize

オンデマンドでレポートを生成することもできるが、スケジュールに従って、毎日や毎週の頻度でレポートを作成され、保存されたり、メールで送られたりすることもできます。

日常状況の把握 クライアント サマリ

The screenshot shows the Cisco Wireless Control System interface. At the top, there's a navigation bar with 'Monitor', 'Reports', 'Configure', 'Services', 'Administration', 'Tools', and 'Help'. The main content area is titled 'Client Summary : New' and shows the 'Client Summary Report Details' configuration page. The 'Settings' section includes 'Report Title' (Client Summary) and 'Reporting Period' (Last 7 Days). The 'Schedule' section includes 'Scheduling' (Enable checkbox), 'Export Format' (CSV), and 'Destination' (File path). A 'Create Custom Report' dialog box is open, showing 'Custom Report Name' (Client Summary) and a list of 'Available data fields' and 'Data fields to include'. The 'Customize' button in the dialog is highlighted with a red box.

レポートに含まれる
内容もカスタマイズ
できます。

クライアント サマリ レポート

Client Summary

Wireless Control System

Generated: Thu Oct 08 03:43:14 GMT 2009

Reporting Period: Last 7 days

Client Summary

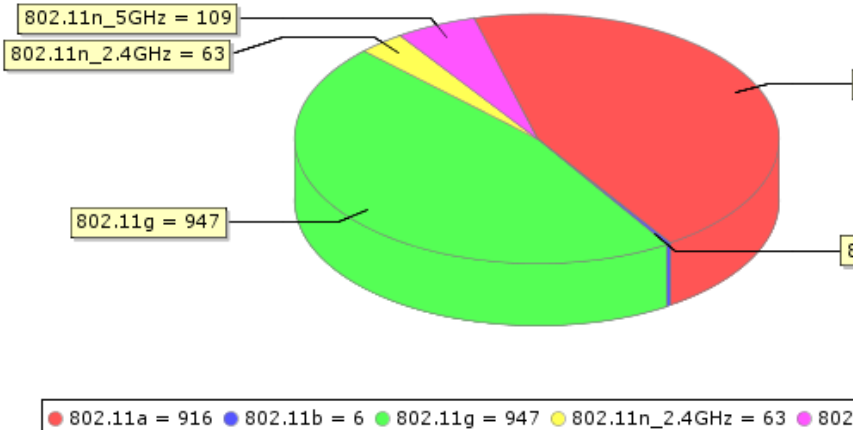
Number of Sessions	Number of Users	Number of Unique Users	Number of New Users	Number of Unique APs	Number of Users per AP	Total Session Time (Minutes)	Average Session Time (Minutes)	Average Session Time per User (Minutes)	Total Traffic (MB)	Average Traffic per Session (KB)	Average Traffic per User (KB)	Total Throughput (Mbps)	Average Throughput per Session (KB)
16042	1368	1155	3	55	24.87	856754.19	53.41	626.28	1216997.68	75863.21	889618.18	2373.70	147.97

Client Summary by Protocol

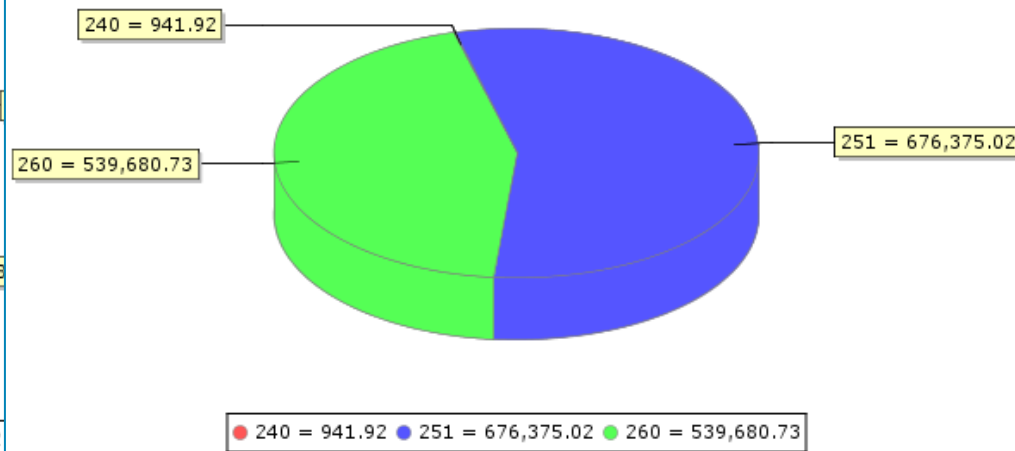
Protocol	Number of Sessions	Number of Users	Session Time (Minutes)	Traffic (MB)	% of Sessions	% of Users	% of Session Time
802.11a	6586	916	541993.26	399510.24	41.05	44.88	63.26
802.11b	45	6	2687.67	471.13	0.28	0.29	0.31
802.11g	8614	947	261807.67	788350.21	53.70	46.40	30.56
802.11n_2.4GHz	225	63	10960.65	8284.73	1.40	3.09	1.28
802.11n_5GHz	572	109	39304.93	20381.36	3.57	5.34	4.59

レポートに豊富な情報が提供されているので、管理者の判断・運用に非常に役に立ちます。

Users by Protocol

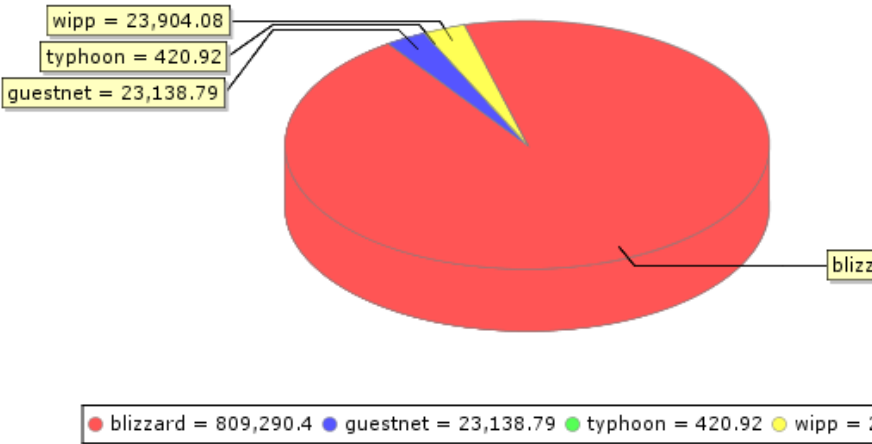


Traffic by VLAN

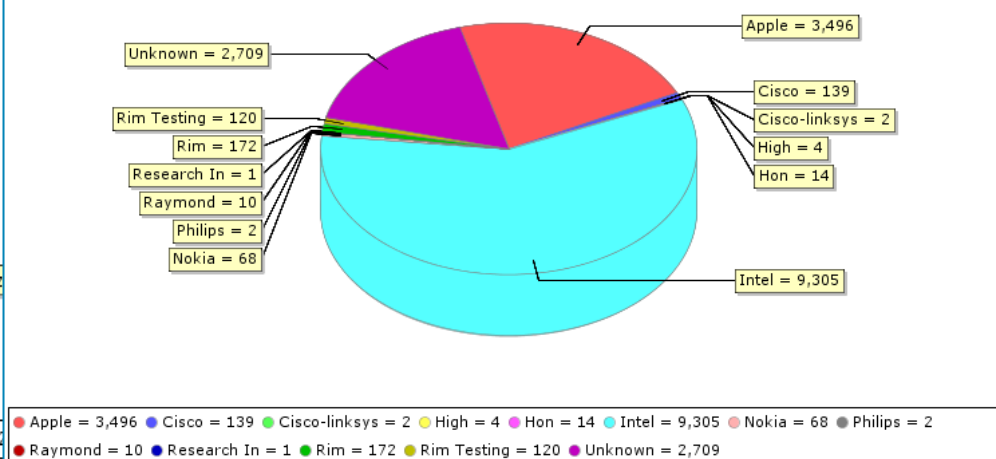


グラフィカル サマリ

Time by SSID



Sessions by Vendor



Traffic Stream Metrics

Traffic Stream Metrics : Traffic Stream Metric Graph

Reports > [Report Launch Pad](#) > Performance > [Traffic Stream Metrics](#) > Traffic Stream Metrics Report Details

Settings

Report Title: Traffic Stream Metric Graph

Report By:

Report Criteria:

Protocol: 802.11a/n 802.11b/g/n

Reporting Period: Last
 From :
To :

Schedule

Scheduling: Enable

Export Format:

Destination: File
 Email

Start Date/Time: :

Current Server Time: 10/15/2009 07:15:30 GMT

Recurrence: No Recurrence Hourly Daily Weekly

Customize Report

[Click here to customize report content based on your preference.](#)

Voice over WLANの普及によって、Voiceアプリケーションから見たWLANシステムのパフォーマンスも把握する必要があります。

Traffic Stream Metric Graph

Wireless Control System

Generated: Thu Oct 15 07:15:27 GMT 2009

Report By: AP By Controller

Protocol: all

Reporting Period: Last 7 days

遅延、パケットロスなどの視点でWLANのパフォーマンスを評価します。

Traffic Stream Metrics

Time	Client MAC	AP Name	Radio Type	Avg Queuing Delay (Downlink)	Avg Queuing Delay (Uplink)	QoS	% Packet with more than 20 < 40 ms delay (Downlink)	% Packet with more than 20 < 40 ms delay (Uplink)	% Packet with more than 40 ms delay (Downlink)	% Packet with more than 40 ms delay (Uplink)
10/14/09 10:24 PM	00:1b:d4:54:61:e1	sjc14-12b-ap1	802.11b/g/n	33.00	0.00	Normal	16.70	0.00	37.24	0.00
10/14/09 10:24 PM	00:1b:d4:54:61:e1	sjc14-12b-ap4	802.11b/g/n	20.00	0.00	Normal	32.45	0.00	9.11	0.00
10/14/09 10:26 PM	00:1b:d4:54:61:e1	sjc14-12b-ap4	802.11b/g/n	16.00	0.00	Normal	31.44	0.00	3.49	0.00
10/14/09 9:52 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	30.00	0.00	Normal	23.04	0.00	50.69	0.00
10/14/09 9:53 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	2.00	0.00	Normal	25.20	0.00	40.44	0.00
10/14/09 9:55 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	26.00	0.00	Normal	18.28	0.00	58.42	0.00
10/14/09 9:57 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	29.00	0.00	Normal	23.06	0.00	52.27	0.00
10/14/09 9:58 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	10.00	0.00	Normal	23.72	0.00	52.77	0.00
10/14/09 10:00 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	58.00	0.00	Normal	26.97	0.00	37.70	0.00
10/14/09 10:03 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	22.00	0.00	Normal	21.51	0.00	57.51	0.00
10/14/09 10:04 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	10.00	0.00	Normal	24.66	0.00	47.94	0.00
10/14/09 10:07 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	27.00	0.00	Normal	29.03	0.00	19.45	0.00
10/14/09 10:09 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	26.00	0.00	Normal	31.27	0.00	17.54	0.00
10/14/09 10:10 PM	00:1b:d4:54:61:e1	sjc14-22b-ap3	802.11b/g/n	30.00	0.00	Normal	28.84	0.00	25.36	0.00

WLANでどんなインシデントがあるか

WHAT DO YOU NEED TO PREPARE?

- APがダウンした
- APのラジオインタフェースがダウンした
- WLCがダウンした
- MSEがダウンした
- 不正AP・不正クライアントが検知された
- WLANが攻撃を受けた
- Etc.

アラームをメールで通知する

Email Notification
Monitor > [Alarms](#) > **Email Notification**

i Email notifications will be sent on the occurrence of alarms belonging to checked categories and selected severity levels.

Enable	Alarm Category	Severity Levels	To
<input checked="" type="checkbox"/>	Access Points	▲	admin@cisco.com
<input checked="" type="checkbox"/>	Controllers	▲	admin@cisco.com
<input checked="" type="checkbox"/>	Coverage Hole	▲	admin@cisco.com
<input checked="" type="checkbox"/>	Location Notifications	▲	admin@cisco.com
<input checked="" type="checkbox"/>	Mobility Services	▲	admin@cisco.com
<input checked="" type="checkbox"/>	Mesh Links	▲	admin@cisco.com
<input checked="" type="checkbox"/>	Rogue AP	▲	admin@cisco.com
<input checked="" type="checkbox"/>	Security	▲	admin@cisco.com
<input checked="" type="checkbox"/>	WCS	▲	admin@cisco.com
<input checked="" type="checkbox"/>	Interference	▲	admin@cisco.com
<input checked="" type="checkbox"/>	Adhoc Rogue	▲	admin@cisco.com

WCSには11種類計150項目のアラームが用意されています。それらのアラームがヒットする場合、指定のメールアドレスに通知メールを飛ばすことができます。WLANに発生しうるインシデントに備えて、迅速な対応を可能にします。

アラームメールのイメージ

The screenshot shows the Outlook Express interface. The main window displays a list of emails in the inbox. The selected email is from WCS-60@192.168.100.12 with the subject 'WCS Alarm: Rogue AP, severity Minor' received on 2009/05/13 10:01. The email body contains the following text:

送信者 : WCS-60@192.168.100.12 宛先 : wcs-admin@cisco.com
件名 : WCS Alarm: Rogue AP, severity Minor

WCS has detected one or more alarms of category Rogue AP and severity Minor in Virtual Domain root for the following items:

- Rogue AP '00:1a:a2:fd:2e:20' with SSID 'blizzard' and channel number '1' is detected by AP 'LAP5' Radio type '802.11b' with RSSI '-79' and SNR '10'. RogueAP contained.
- Rogue AP '00:1a:a2:fd:58:9e' with SSID "" and channel number '44' is detected by AP 'LAP2' Radio type '802.11a' with RSSI '-70' and SNR '27'. RogueAP contained.
- Rogue AP '00:1a:a2:fd:a3:9f' with SSID 'blizzard' and channel number '44' is detected by AP 'LAP1' Radio type '802.11a' with RSSI '-88' and SNR '8'. RogueAP contained.
- Rogue AP '00:1a:e3:74:27:ed' with SSID "" and channel number '36' is detected by AP 'LAP5' Radio type '802.11a' with RSSI '-73' and SNR '21'. RogueAP contained.
- Rogue AP '00:1a:e3:74:2e:bd' with SSID "" and channel number '40' is detected by AP 'LAP2' Radio type '802.11a' with RSSI '-56' and SNR '41'. RogueAP contained.
- Rogue AP '00:1b:2b:68:97:70' with SSID 'cbcakas' and channel number '1' is detected by AP 'LAP5' Radio type '802.11b' with RSSI '-69' and SNR '28'. RogueAP contained.
- Rogue AP '00:1f:ca:50:96:5e' with SSID 'IndoorMesh' and channel number '44' is detected by AP 'LAP6' Radio type '802.11a' with RSSI '-64' and SNR '31'. RogueAP contained.

E-mail will be suppressed up to 30 minutes for these alarms.

Alarms (Edit View)

Monitor > Alarms

 Entries 1 - 50 of 4797
 ⏪ 1 2 3 4 5 6 7 8 9 10

<input type="checkbox"/>	Severity	Failure Source	Owner	Date/Time ▾	Message	Acknowledged
<input type="checkbox"/>	●	Controller SJC 14 LWAPP2/171.71.128.78		10/8/09 5:24:24 AM	User authentication from Controller '171.71.128.78' failed for User...	No
<input type="checkbox"/>	▲	AP 00:22:64:99:72:e6		10/8/09 5:24:24 AM	Failed to authorize AP '00:22:64:99:72:e6' with certificate type 'U...	No
<input type="checkbox"/>	●	Controller SJC 14 LWAPP1/171.71.128.75		10/8/09 5:23:54 AM	User authentication from Controller '171.71.128.75' failed for User...	No
<input type="checkbox"/>	▲	AP 00:22:64:99:72:e6		10/8/09 5:23:54 AM	Failed to authorize AP '00:22:64:99:72:e6' with certificate type 'U...	No
<input type="checkbox"/>	▲	Controller SJC 14 LWAPP2/171.71.128.78		10/8/09 5:23:47 AM	IDS 'NULL probe resp 1' Signature attack cleared on AP 'sjc14-31b-a...	No
<input type="checkbox"/>	●	Rogue AP 00:19:a9:0c:98:ac		10/8/09 5:23:26 AM	Rogue AP '00:19:a9:0c:98:ac' is removed; it was detected as Rogue A...	No
<input type="checkbox"/>	▲	Controller SJC 14 LWAPP2/171.71.128.78		10/8/09 5:20:47 AM	IDS 'NULL probe resp 1' Signature attack detected on AP 'sjc14-42b-...	No
<input type="checkbox"/>	●	Rogue AP 00:17:df:aa:01:9c		10/8/09 5:18:09 AM	Rogue AP '00:17:df:aa:01:9c' with SSID " and channel number '48' i...	No
<input type="checkbox"/>	▲	Controller SJC 14 LWAPP1/171.71.128.75		10/8/09 5:17:24 AM	IDS 'NULL probe resp 1' Signature attack detected on AP 'sjc14-12b-...	No
<input type="checkbox"/>	●	Rogue AP 00:25:45:35:f9:61		10/8/09 5:16:34 AM	Rogue AP '00:25:45:35:f9:61' with SSID " and channel number '48' i...	No
<input type="checkbox"/>	●	Rogue AP 00:25:45:35:32:6a		10/8/09 5:16:23 AM	Rogue AP '00:25:45:35:32:6a' with SSID " and channel number '48' i...	No
<input type="checkbox"/>	▲	Controller SJC 14 LWAPP1/171.71.128.75		10/8/09 5:16:34 AM	IDS 'NULL probe resp 1' Signature attack detected on AP 'sjc14-12b-...	No
<input type="checkbox"/>	▲	Controller SJC 14 LWAPP2/171.71.128.78		10/8/09 5:16:34 AM	User 'admin' with IP Address '10.33.112.10' has made too many unsuc...	No
<input type="checkbox"/>	▲	Controller SJC 14 LWAPP1/171.71.128.75		10/8/09 5:16:23 AM	User 'admin' with IP Address '10.33.112.10' has made too many unsuc...	No
<input type="checkbox"/>	●	Rogue AP 00:22:90:93:18:00		10/8/09 5:15:16 AM	Rogue AP '00:22:90:93:18:00' with SSID 'alpha' and channel number '...	No
<input type="checkbox"/>	●	Rogue AP 00:23:eb:ad:8c:0f		10/8/09 5:15:04 AM	Rogue AP '00:23:eb:ad:8c:0f' with SSID 'alpha' and channel number '...	No
<input type="checkbox"/>	●	Rogue AP 00:26:0b:4a:dd:b0		10/8/09 5:15:02 AM	Rogue AP '00:26:0b:4a:dd:b0' with SSID 'WLAN400' and channel number...	No
<input type="checkbox"/>	●	Rogue AP 00:22:90:93:18:03		10/8/09 5:15:02 AM	Rogue AP '00:22:90:93:18:03' with SSID " and channel number '1' is...	No
<input type="checkbox"/>	●	Rogue AP 00:22:55:59:37:bf		10/8/09 5:14:46 AM	Rogue AP '00:22:55:59:37:bf' with SSID " and channel number '...	No

アラームの中から該当する不正APを選択します。

Alarm Details : Rogue AP - Cisco:0c:98:ac

 Monitor > [Alarms](#) > Alarm Details

General	
Rogue MAC Address	00:19:a9:0c:98:ac
Vendor	Cisco
Rogue Type	AP
On Network	Controller: No , Switch Port Trace: Not traced
Owner	
Acknowledged	No
Classification Type	Unclassified
State	Alert
SSID	alpha_voice
Channel Number	48
Containment Level	Unassigned
Radio Type	a
Strongest AP RSSI	-47
No. of Rogue Clients	0
First Seen Time	1/17/09 9:11 AM
Last Seen Time	10/8/09 5:43 AM
Generated By	Controller
Severity	● Minor
Previous Severity	
Event Details	
Switch Port Trace Status	

Switch Port Tracing Details (last trace)

Switch ports were not traced for this rogue AP.

Click [here](#) for more details...

Rogue Clients

Client MAC Address

No rogue clients found

Message

Rogue AP '00:19:a9:0c:98:ac' with detected by AP 'sjc14-22b-ap3' Radio type '802.11a' with RSSI '-72' and SNR '28'.

Annotations New Annotation

Date/Time	Posted By	Message
0		

Location Notifications

Absence 0

- Select a command --

 - Select a command --
 - Assign to me
 - Unassign
 - Delete
 - Clear
 - Acknowledge
 - Unacknowledge
 -
 - Trace Switch Port
 -
 - Event History
 -
 - Detecting APs
 - Map (High Resolution)**
 - Rogue Clients
 -
 - Set State to 'Unclassified - Alert'
 - Set State to 'Malicious - Alert'
 - Set State to 'Friendly - Internal'
 - Set State to 'Friendly - External'

不正APの詳細情報が表示されます。SSIDやチャンネル、検知された時間などが表示されます。これらの情報に基づいて対応します。この例では、マップ上で不正APの位置を表示させます。

Maps Tree View

- Maps (Root Area)
 - Cisco San Jose - Site 5
 - BLD 14
 - 1st floor
 - 2nd floor
 - 3rd floor
 - 4th floor

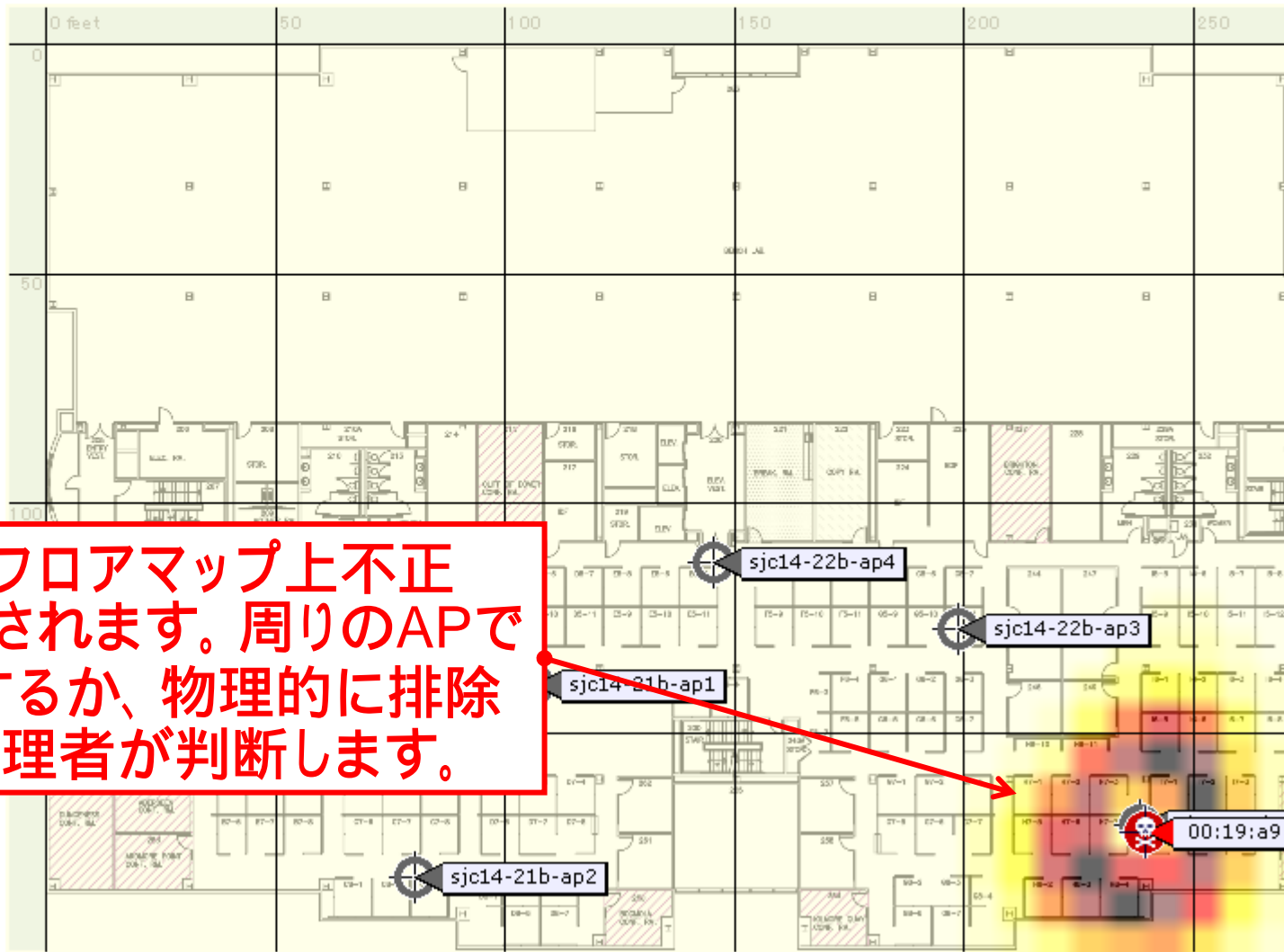
Floor View

Monitor > Maps > Cisco San Jose - Site 5 > BLD 14 > 2nd floor

-- Select a command --

Data may be delayed up to 15 minutes or more depending on background polling interval

+ - 100% Grid Color
+ - + - + -



オフィスのフロアマップ上不正 APが表示されます。周りのAPで封じ込みするか、物理的に排除するか、管理者が判断します。

まとめ

- シスコWCSがWLANに関する豊富な情報を提供し、IT管理者の運用管理をサポートします。企業WLANの導入効果を最大限にすることができます。
- ここで紹介したのは、WCS多くの機能の僅か一部に過ぎません。他にも様々なWLAN管理上に役に立つ機能が多くあります。
- 下記のURLでトライアルライセンスを入手できますので、ぜひ一度ご自分でWCSを試してください。

<https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=214>

TRY IT PLEASE

