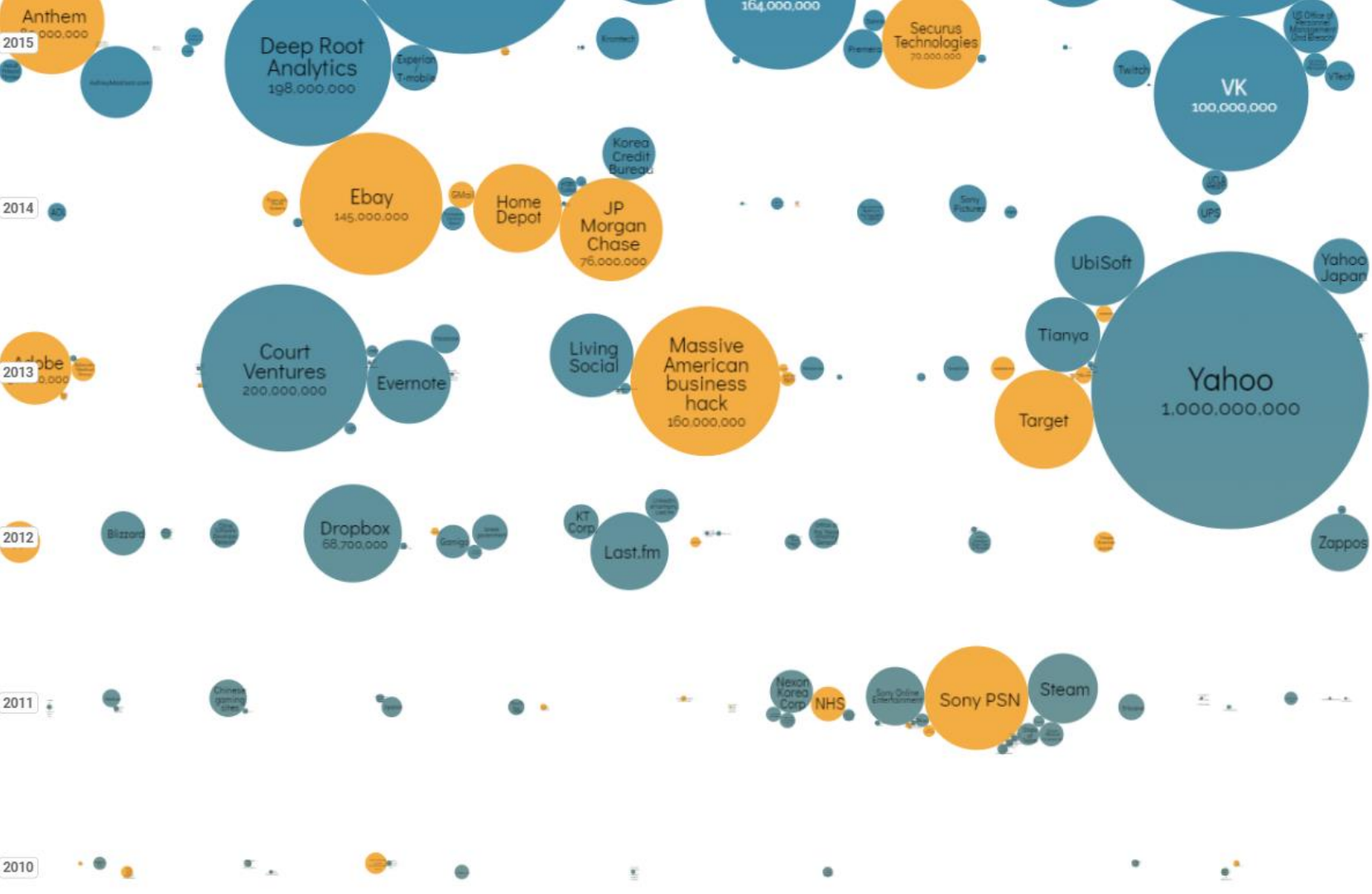
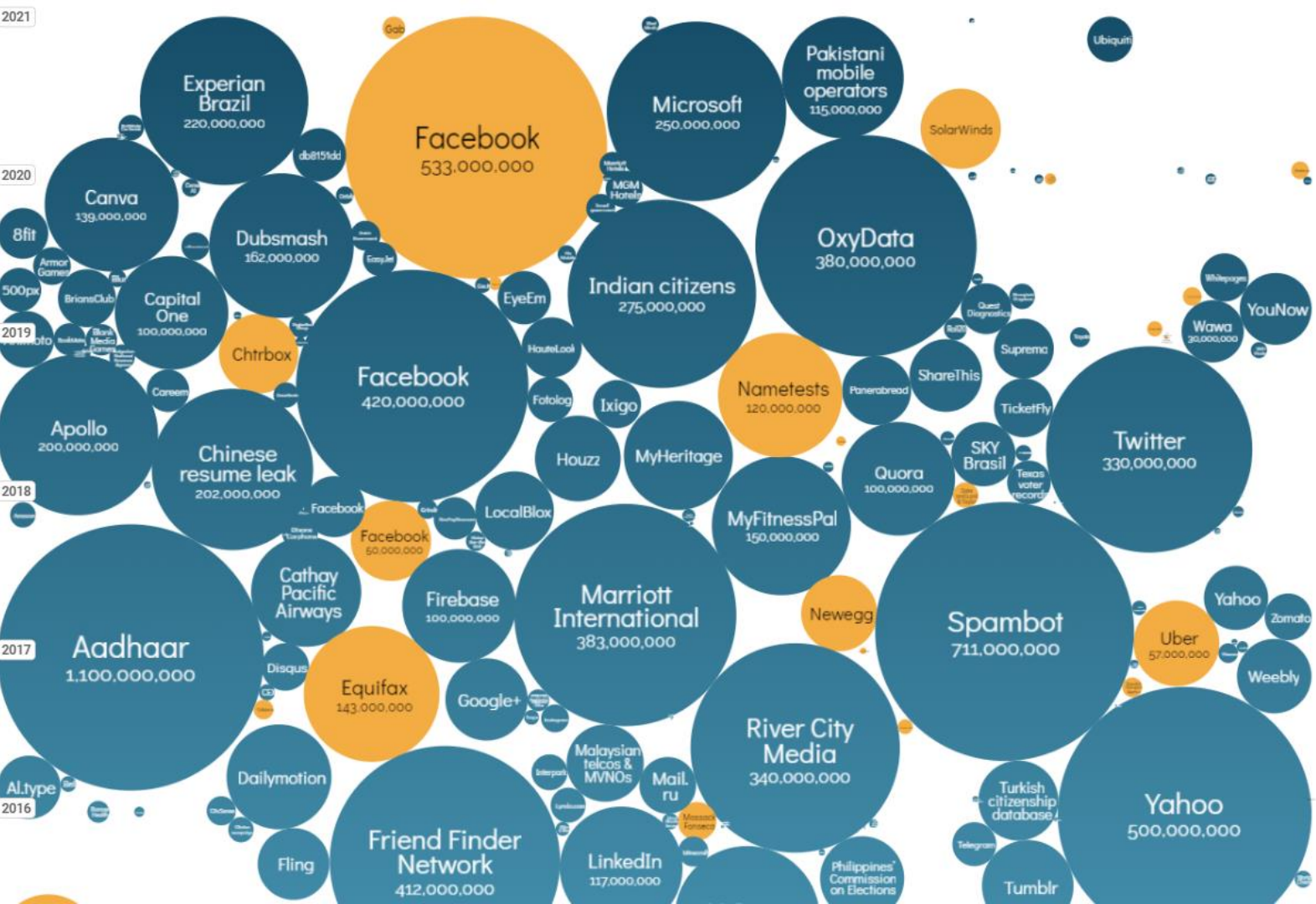
ネットワークセキュリティ監査の簡素化にも
有効な手法をご提案

NetAlly
Channel Account Manager
Japan & S.Korea

杵鞭 俊之


2015
2014
2013
2012
2011
2010
Anthem
Deep Root Analytics
198,000,000
Experian
T-mobile
164,000,000
Securus Technologies
70,000,000
Twitch
VK
100,000,000
Ebay
145,000,000
Home Depot
Korea Credit Bureau
JP Morgan Chase
76,000,000
UPS
UbiSoft
Yahoo Japan
Court Ventures
200,000,000
Evernote
Living Social
Massive American business hack
160,000,000
Tianya
Target
Yahoo
1,000,000,000
Dropbox
68,700,000
KT Corp
Last.fm
Zappos
Nexon Korea Corp
NHS
Sony PSN
Steam


2021
2020
2019
2018
2017
2016
Experian Brazil 220,000,000
Facebook 533,000,000
Microsoft 250,000,000
Pakistani mobile operators 115,000,000
Ubiquiti
SolarWinds
Canva 139,000,000
Dubsmash 162,000,000
OxyData 380,000,000
8fit
Capital One 100,000,000
Indian citizens 275,000,000
EyeEm
Chtrbox
Facebook 420,000,000
HauteLook
Fotolog
Ixigo
Nametests 120,000,000
Panerabread
ShareThis
Suprema
TicketFly
Wawa 30,000,000
YouNow
Apollo 200,000,000
Chinese resume leak 202,000,000
Houzz
MyHeritage
Quora 100,000,000
SKY Brasil
Twitter 330,000,000
Facebook 50,000,000
LocalBlox
MyFitnessPal 150,000,000
Cathay Pacific Airways
Firebase 100,000,000
Marriott International 383,000,000
Newegg
Spambot 711,000,000
Yahoo
Zomato
Uber 57,000,000
Weebly
Aadhaar 1,100,000,000
Disqus
Equifax 143,000,000
Google+
River City Media 340,000,000
Dailymotion
Malaysian telcos & MVNOs
Mail.ru
Turkish citizenship database
Yahoo 500,000,000
Friend Finder Network 412,000,000
LinkedIn 117,000,000
Fling
Philippines' Commission on Elections
Tumblr

Novelty

A Casino Gets Hacked Through a Fish-Tank Thermometer

Secure your laptop. Secure your smart phone. Secure your tablet. And, before I forget, sec...

Entrepren... • 1 day ago

"The attackers used that (a fish-tank thermometer) to get a foothold in the network," she recounted. "They then found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud."

"The industrial sector is facing a new set of challenges when it comes to securing a converged IT-OT environment," Tim Erlin, vice president of product management and strategy at security firm Tripwire, told Security Info Watch. "In the past, cybersecurity was focused on IT assets like servers and workstations, but the increased connectivity of systems requires that industrial security professionals expand their understanding of what's in their environment. You can't protect what you don't know."

So how do we, as business owners, address this problem? The only tactic is just to stay ahead of it. Which is why it's important to bring in an IT expert regularly to do a complete assessment of our network security. But we need to make sure that such an assessment includes evaluating any and every connected device. That means our building heating controls, smart speakers, smoke detectors, alarm systems, overhead lighting and even the coffee machine in the break room.

Oh, and don't forget the fish tank.

Source: https://www.entrepreneur.com/article/368943

プロビジョニング

Capital One suffers massive data breach due to misconfigured firewall

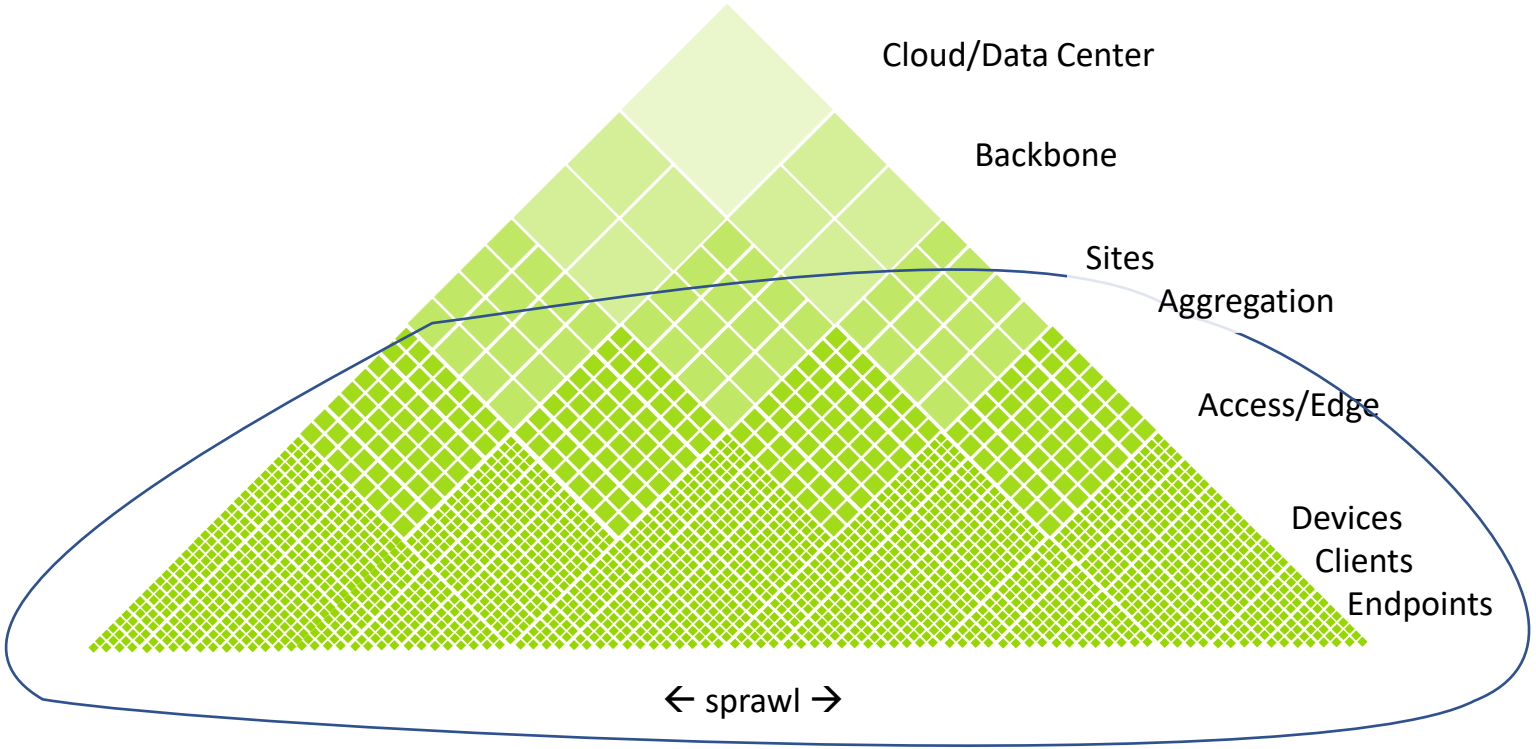
By: The Associated Press July 30, 2019

A security breach at Capital One Financial, one of the nation's largest issuers of credit cards, compromised the personal information of about 106 million people, and in some cases the hacker obtained Social Security and bank account numbers.

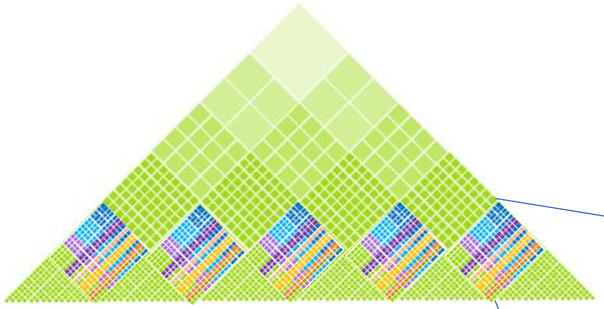
Security Landscape

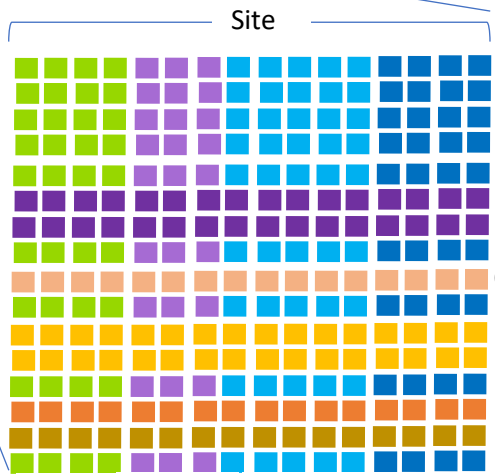
- Portable
- 2x RJ-45
- 1x Fiber/SFP+
- 2x Wi-Fi Radios
  - ✓ 4x4 Promiscuous
  - ✓ 1x1 Connectivity
- BT/BLE Radio
- Connectivity Validation
- Advanced Analysis
  - ✓ Network Discovery
  - ✓ Wi-Fi Analysis
  - ✓ Path Analysis
  - ✓ Capture
- Layer 1 to Layer 7
  - ✓ L1:TDR/BERT/PoE
  - ✓ L7:EURT
- Remote operation
- Collaborative

Site Infrastructure, Access and Devices



より複雑化





Segmentations

- ❑ Department
- ❑ User
- ❑ Overlay (VoIP, Surveillance, …
- ❑ Legacy

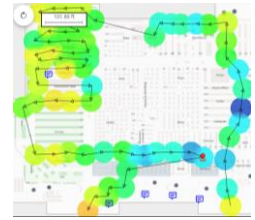
Use Models

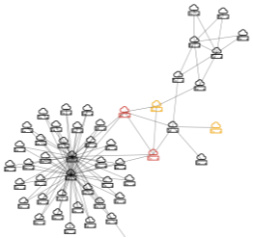
Handheld

有線環境 アセスメント
- 情報コンセント(PoE, VLANs, Subnets)
- アクセスプロビジョニング検証
- 通信到達
- ディスカバリと問題
- 端末エミュレーション (MAC spoofing)

RF アセスメント
- AirMapper サーベイ
- AP/Client 位置
- BLE サーベイ

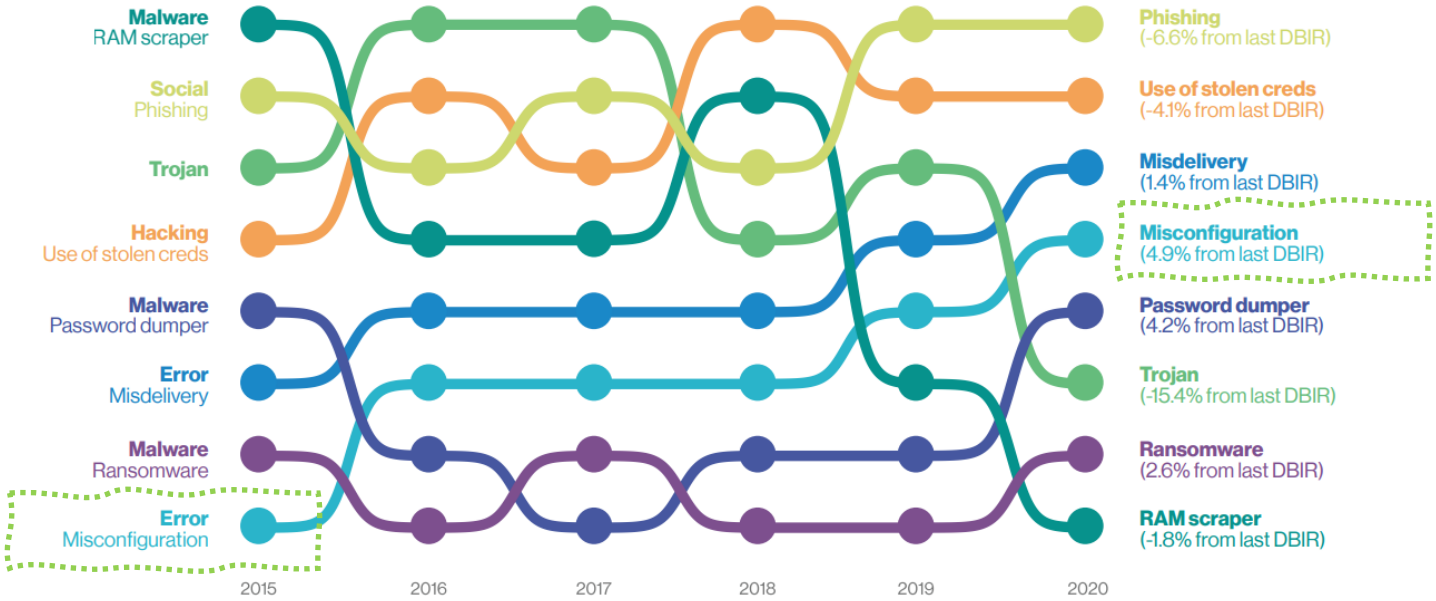
Drop-in
- リモート対応
- 手軽なモニタリング
- Discovery/Wi-Fi Snapshots



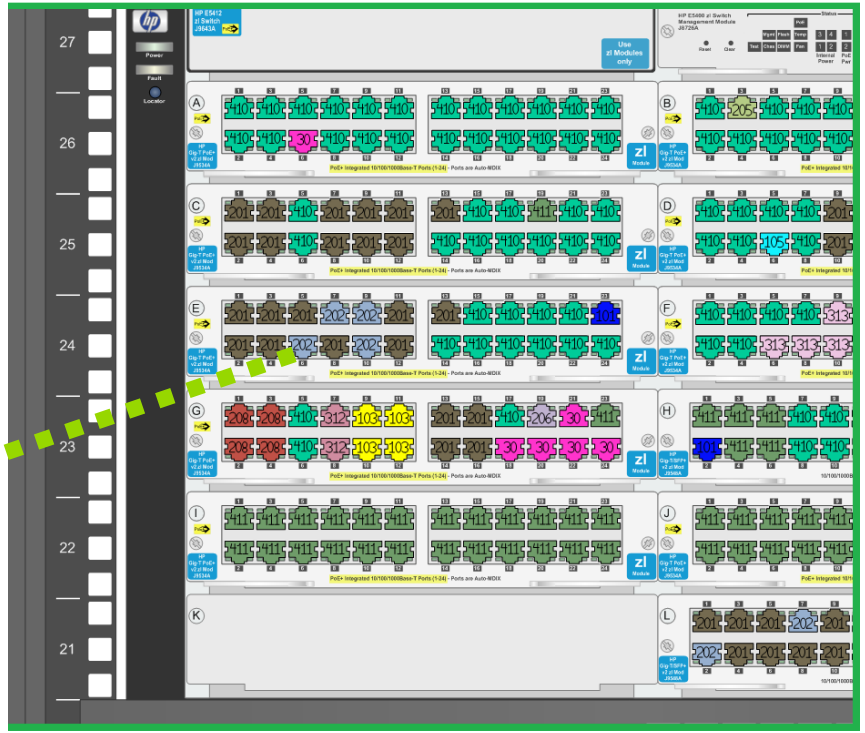


解析
- Network デバイス
- Networkの変更
- Wi-Fi / RF セキュリティ
- レポート

Provisioning

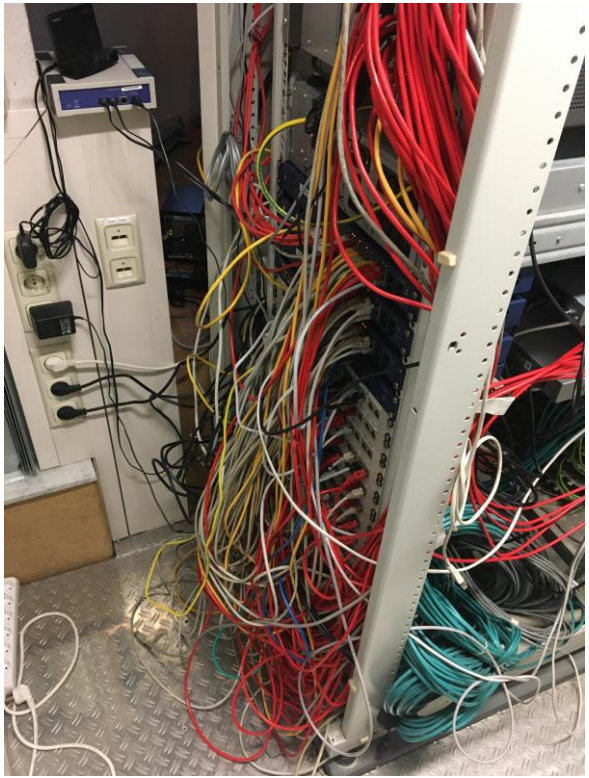


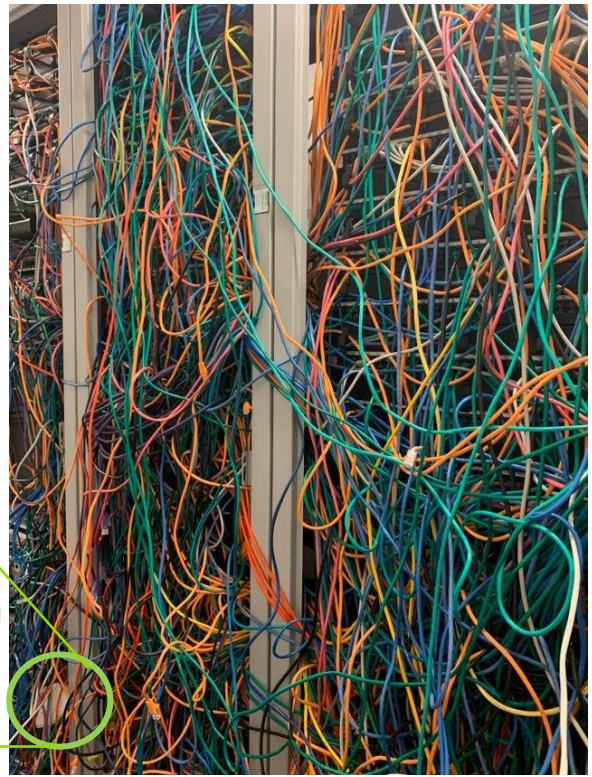
Source: Verizon 2020 Data Breach Investigations Report (DBIR)



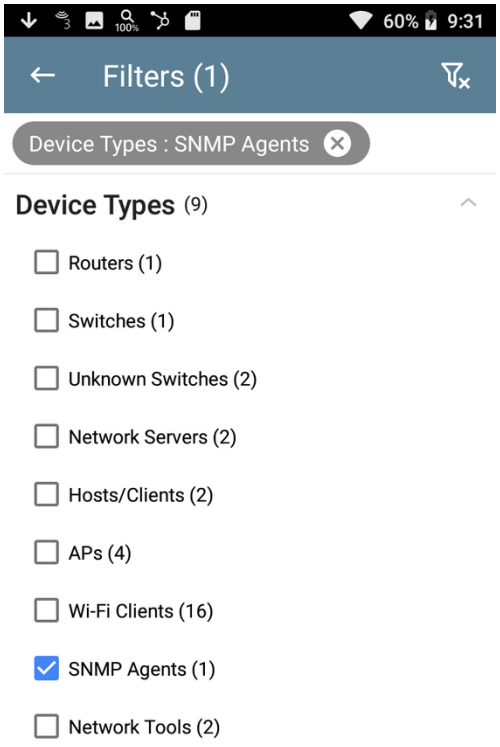
- ❑ Cable/patch panel/switch confusion
- ❑ Default passwords and community strings, simple passwords
- ❑ Out of box plug and play enabled
- ❑ Dashboard/CLI disparity, saving provision changes
- ❑ DHCP pools/inter-VLAN routing/radius/NTP/
- ❑ Segmentation: VLAN assignment
- ❑ Quality of Service
- ❑ Power distribution
- ❑ Legacy devices

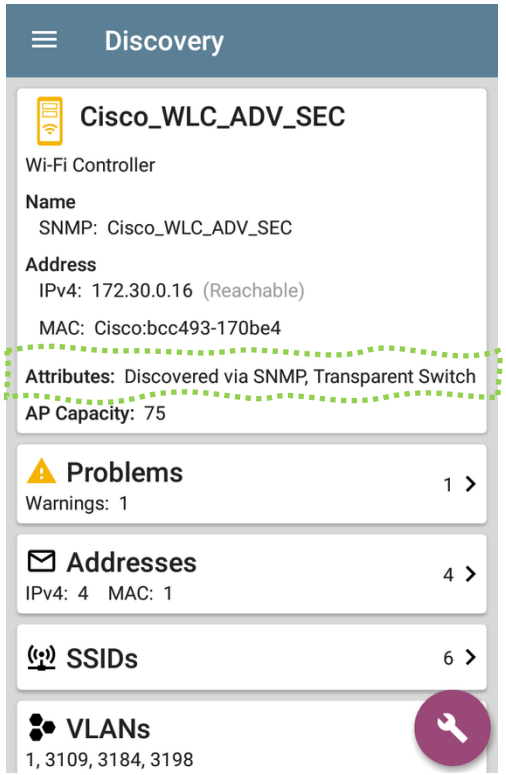
reddit.com/r/cablefail





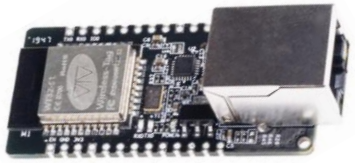
Provisioning: Defaults



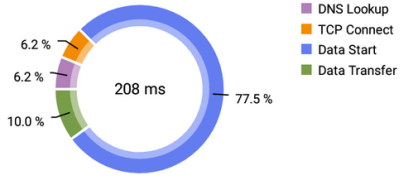


プロビジョニング検証

AutoTest



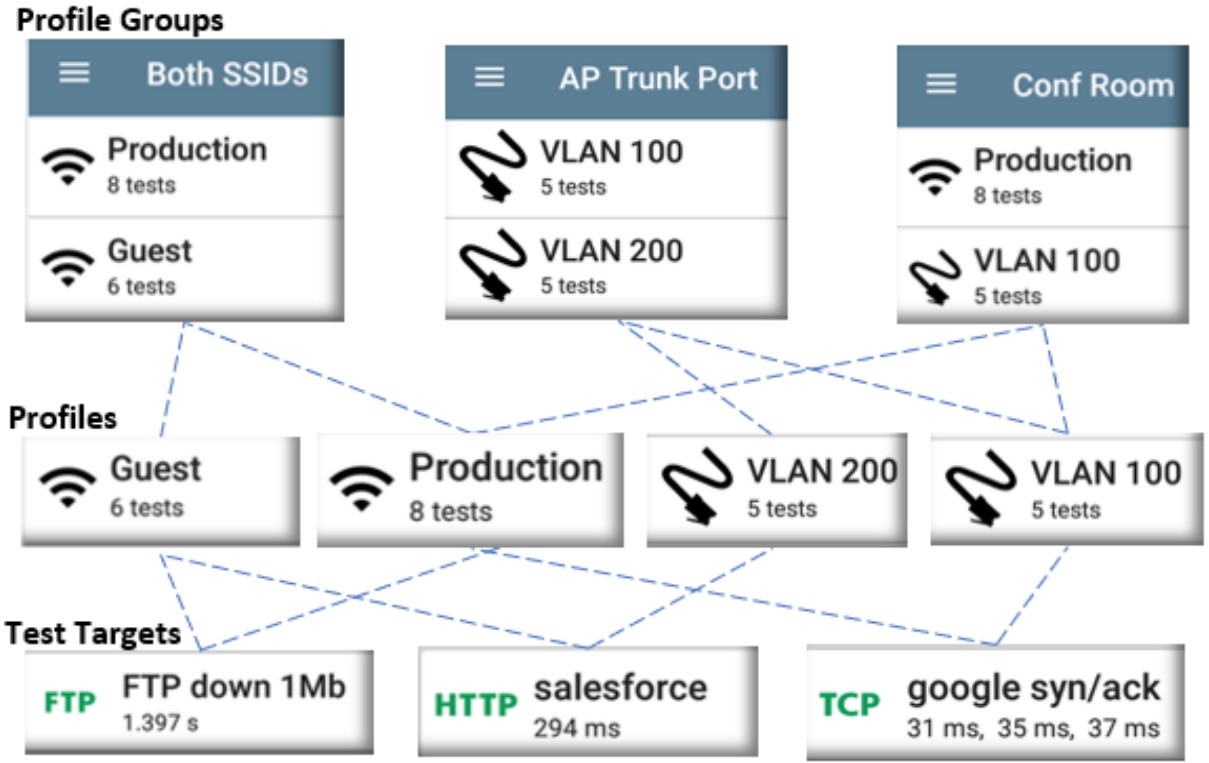
End User Response Time



Result Codes

Response contains excluded text (8)
OK (HTTP 200)

プロビジョニング検証: AutoTest



DHCP 2nd Offer 検知

DHCP 192.168.0.75
343 ms

Device Name: 192.168.0.1

IPv4 Address: 192.168.0.1
MAC Address: Actntc:207600-b04db0

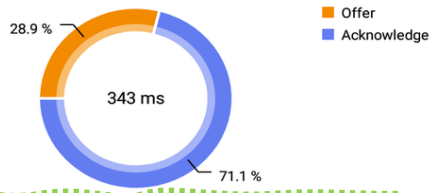
Results

Offered: 192.168.0.75
Accepted: 192.168.0.75
Subnet Mask: 255.255.255.0
Subnet: 192.168.0.0/24
Lease Time: 1 day 0 seconds
Expires: 8/14 12:02 PM

Relay Agent: --

Metric	Result
Offer	99 ms
Acknowledge	243 ms
Total Time	343 ms
Threshold	60 s

End User Response Time



Offer 2 Server Name: 202-148.compute-1

IP Address: 10.0.0.1
MAC Address: Ntgear:e4f4c6-14b009

IPv6 Addresses
fe80::3e8c:f8ff:feff:14ea (link local)

Result Codes
Second DHCP offer received (10)

セグメンテーション

U.S. House of Representatives
Committee on Oversight and Government Reform

The Equifax Data Breach

Majority Staff Report
115th Congress

December 2018

セキュリティに関する懸念

アプリケーションサーバとその他ネットワークがセグメンテーション（分離）されていない。

Security Concern 1. *There is no segmentation between the Sun application servers and the rest of the [Equifax] network. An attacker that gains control of the application server from the internet can pivot to any other device, database, or server within the [Equifax] network, globally.*[468]

Proper network segmentation "lays the groundwork for controls which protect against lateral movement on the network by malicious software and actors, preventing a potential infection or compromise from spreading across the network."[469] If an attacker breaches the network perimeter of an organization with a flat, unsegmented network, they can move laterally throughout the network and gain access to critical systems or valuable data.[470]

正しくセグメンテーションすることにより、リスクを大幅に軽減する事が可能となる。

Why modern enterprises need network segmentation

As businesses become more digital and connected, and cyber attacks become more sophisticated and destructive, it is becoming increasingly clear that enterprises need a new approach to security.

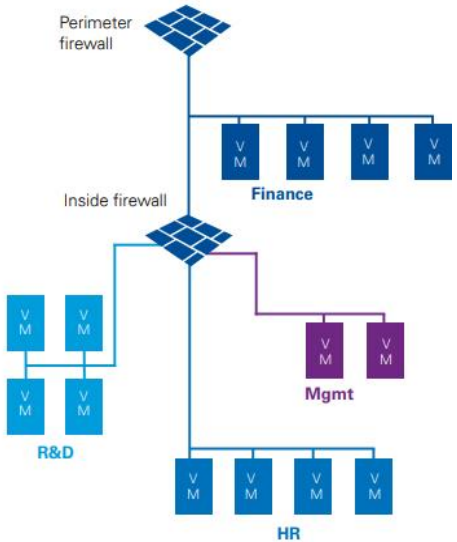
Enter network segmentation.
Network segmentation is one of the most powerful but underutilized security steps and a cornerstone of a successful information security program. It directly addresses the realities of today's threat landscape—that you cannot prevent a cyber breach, but you can isolate one.

Network segmentation focuses on separating parts of the network from one another with barriers or controls. In some cases, the segmentation occurs by function—for example, the finance system is segmented from the HR system. In other cases, the segmentation occurs by data classification—for example, sensitive or regulated data, such as personally identifiable information (PII), is isolated from the rest of the network.

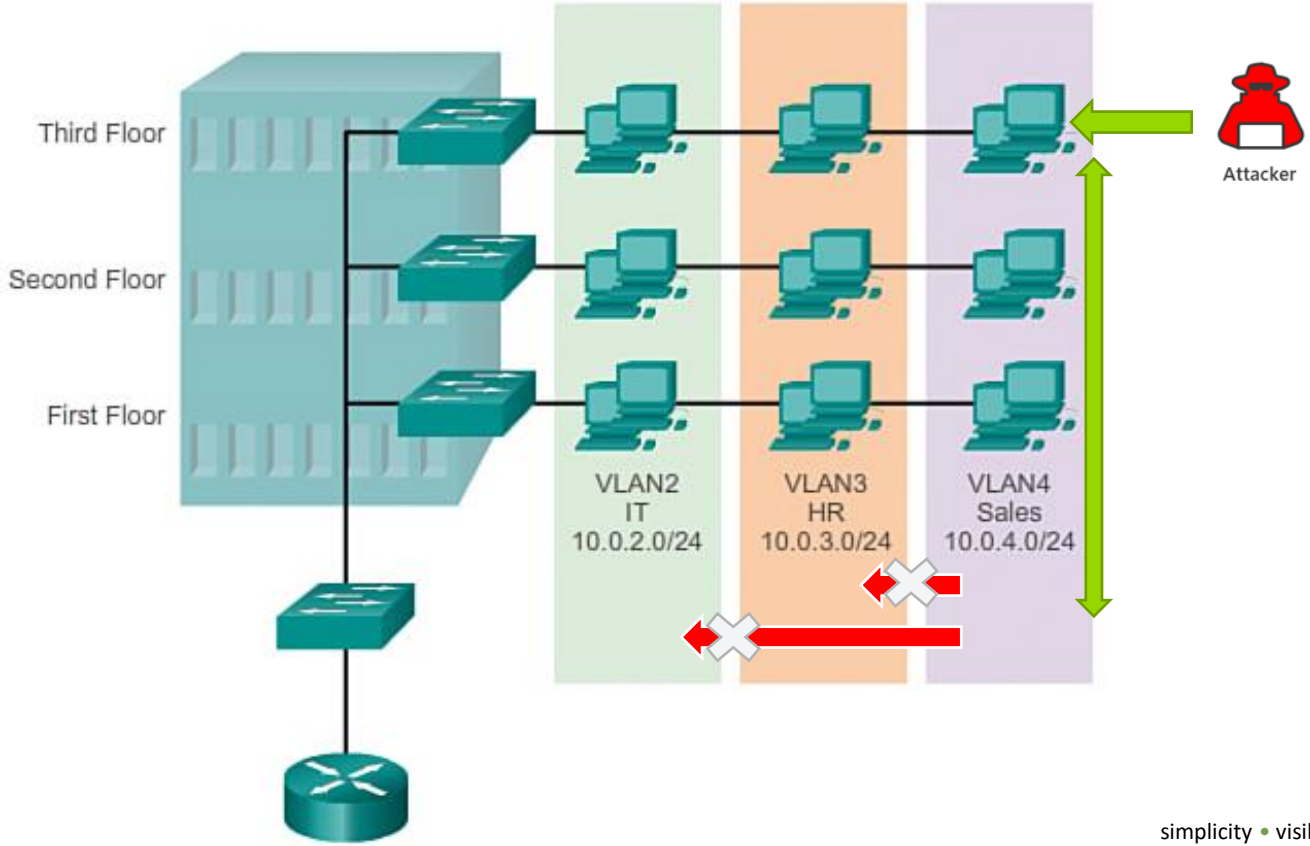
By implementing network segmentation, modern enterprises can help address today's major cyber security challenges far better than with flat networks.

Proper network segmentation lays the groundwork for controls which protect against lateral movement on the network by malicious software and actors, preventing a potential infection or compromise from spreading across the network. It also allows for additional control points across the network, which significantly increases visibility and control over traffic on the network.

Since the vast majority of breaches are thought to occur toward the network periphery, it is clear that proper network segmentation should be the starting point for protecting modern enterprises. In fact, one of the most infamous corporate data breaches to date—the blamed on improper network segmentation. According to *Computerworld*, hackers broke into the retailer's network using login credentials stolen from a third-party contractor. They then leveraged that access to move through the network, eventually accessing the company's point-of-sale systems (POS), which handled sensitive consumer payment card data[2].

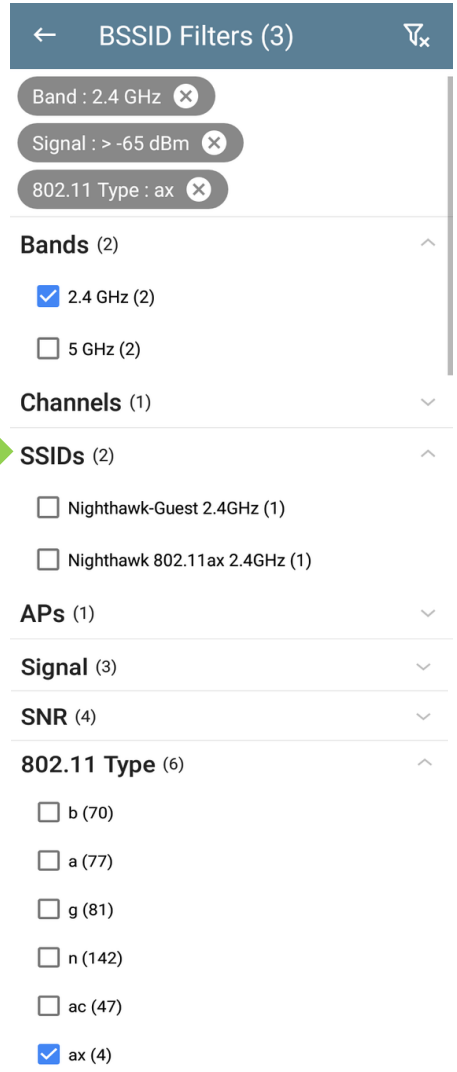


VLAN セグメンテーション



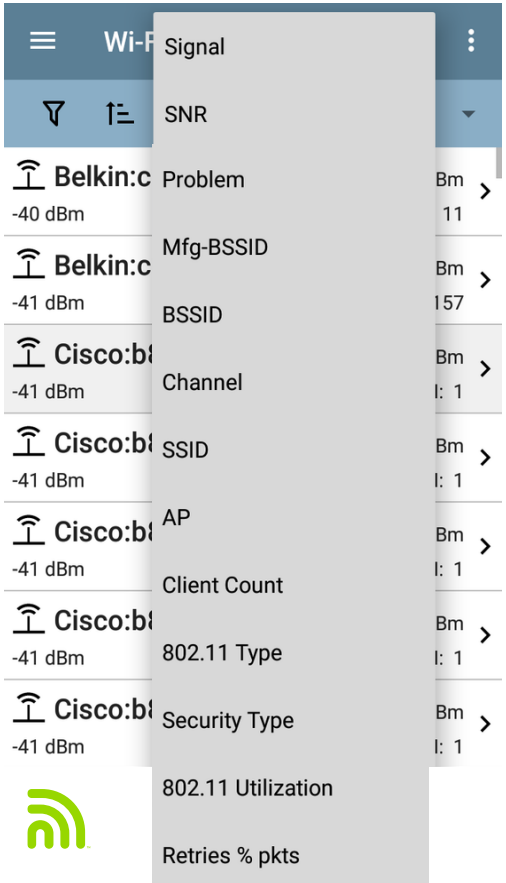
Wired セグメンテーション

Filters

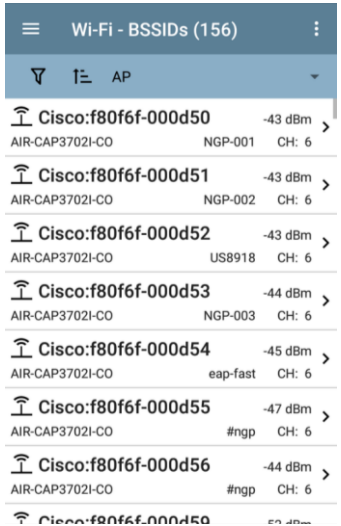

BSSID Filters (3)
Band : 2.4 GHz
Signal : > -65 dBm
802.11 Type : ax
Bands (2)
2.4 GHz (2)
5 GHz (2)
Channels (1)
SSIDs (82)
SSIDs (2)
Nighthawk-Guest 2.4GHz (1)
Nighthawk 802.11ax 2.4GHz (1)
APs (1)
Signal (3)
SNR (4)
802.11 Type (6)
b (70)
a (77)
g (81)
n (142)
ac (47)
ax (4)


Device Types : Routers
Device Types : Switches
Device Types : Network Servers
Device Types : Wi-Fi Controllers
Device Types : SNMP Agents
IPv4 Subnet : 10.0.0.0/8
Band : 2.4 GHz
Client : Connected
SNR : > 30 dB
Security : WPA2-E
SSID : DEN TTS
Channel : 36
NetBIOS Domain : MSHOME
Authorization : Flagged
Basic Rate : 1 Mbps

Sorting


Signal
SNR
Problem
Mfg-BSSID
BSSID
Channel
SSID
AP
Client Count
802.11 Type
Security Type
802.11 Utilization
Retries % pkts


Wi-Fi - BSSIDs (156)
SSID
Cisco:f80f6f-000d55 -43 dBm #ngp #ngp CH: 6
Cisco:f80f6f-000d56 -44 dBm #ngp #ngp CH: 6
Cisco:f80f6f-000d59 -52 dBm #ngp #ngp CH: 149
Cisco:f80f6f-000d5a -55 dBm #ngp #ngp CH: 149
26181a-792ea6 -52 dBm CH: 161
16180a-792ea6 -51 dBm 4ÛLguests 4ÛLguests CH: 5
16181a-792ea6 -52 dBm 4ÛLguests 4ÛLguests CH: 161

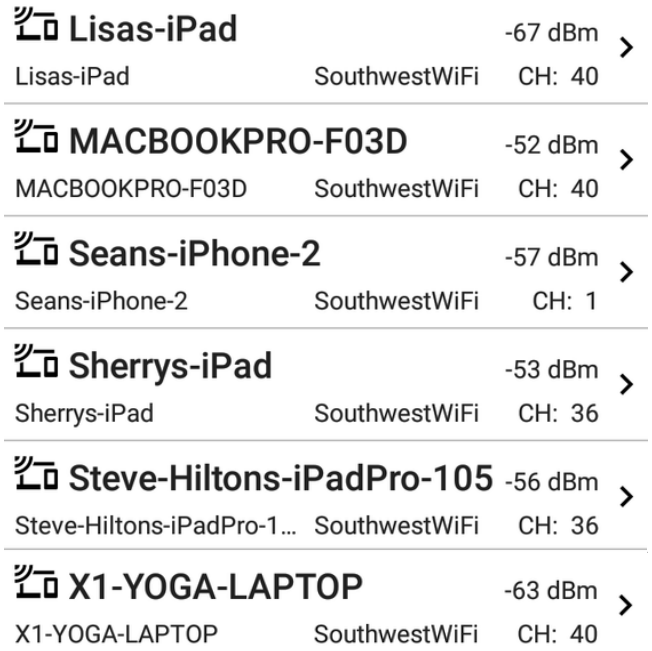

Wi-Fi - BSSIDs (156)
AP
Cisco:f80f6f-000d50 -43 dBm AIR-CAP3702I-CO NGP-001 CH: 6
Cisco:f80f6f-000d51 -43 dBm AIR-CAP3702I-CO NGP-002 CH: 6
Cisco:f80f6f-000d52 -43 dBm AIR-CAP3702I-CO US8918 CH: 6
Cisco:f80f6f-000d53 -44 dBm AIR-CAP3702I-CO NGP-003 CH: 6
Cisco:f80f6f-000d54 -45 dBm AIR-CAP3702I-CO eap-fast CH: 6
Cisco:f80f6f-000d55 -47 dBm AIR-CAP3702I-CO #ngp CH: 6
Cisco:f80f6f-000d56 -44 dBm AIR-CAP3702I-CO #ngp CH: 6

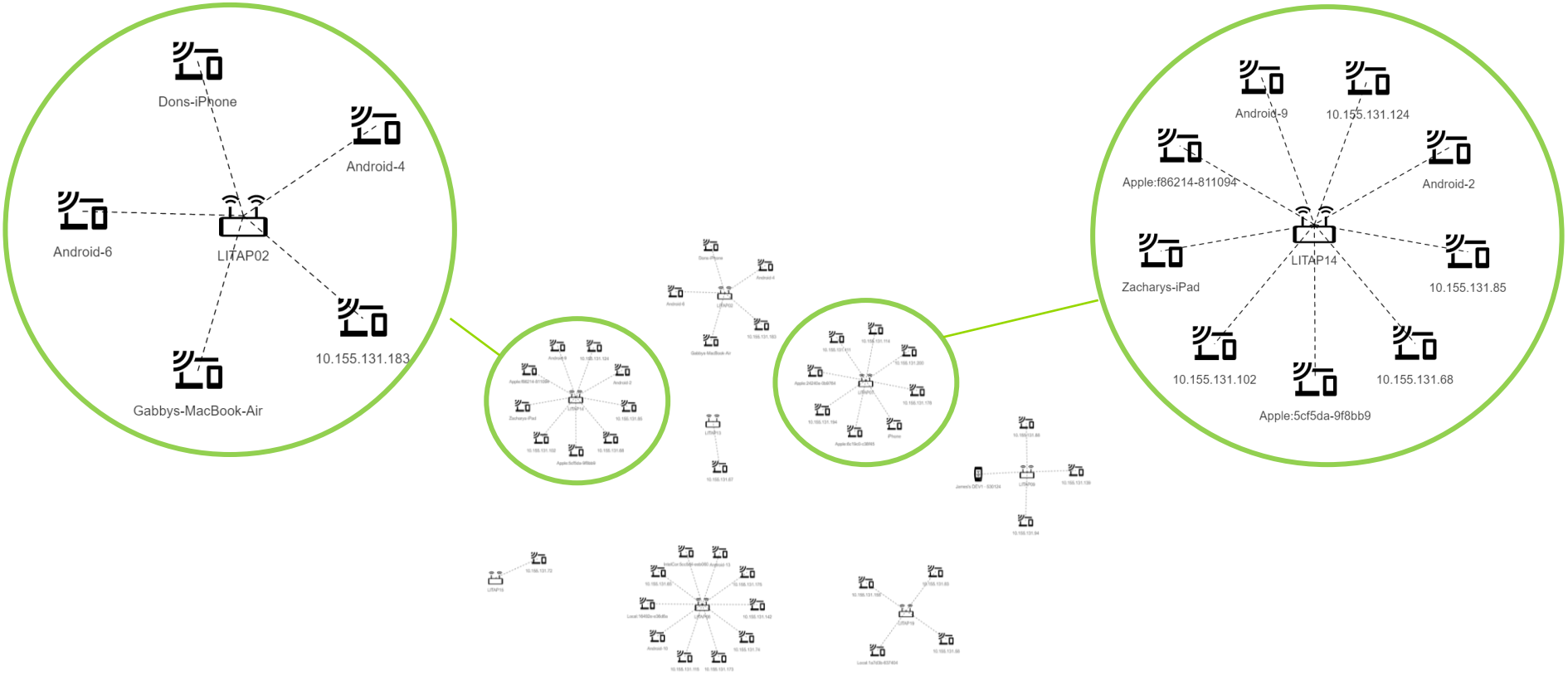

Wi-Fi - BSSIDs (156)
Retries % pkts
Cisco:0c2724-8f0b3e -65 dBm 14% NSVisitor CH: 48
Cisco:b83861-84aaf9 -60 dBm 10% Lobo CH: 36
Cisco:f80f6f-000d53 -44 dBm 8% NGP-003 CH: 6
16181a-792ea6 -52 dBm 5% 4ÛLguests CH: 161
HPE:9c8cd8-8c2fb0 -56 dBm 1% cosj-aruba-iap CH: 52
Aerohv:348584-064b64 -58 dBm 0% HNT 802.11ax CH: 44
Aerohv:c8675e-019964 -77 dBm 0% EZWIFI CH: 157


Wi-Fi - BSSIDs (156)
Security Type
HPE:34fcb9-2e1f32 -74 dBm Open ame-003 CH: 36
Cisco:b83861-84aaf8 -62 dBm Open COS Cisco Captive Portal CH: 36
Cisco:b83861-84aaf7 -- Open COS Cisco Captive Portal CH: 1
f29fc2-af28ab -- Open Ubiquity Captive Portal CH: 6
f29fc2-af28aa -67 dBm Open Ubiquity Captive Portal CH: 40
6eb0ce-bbc7ea -45 dBm Open Home-Guest-2.4G CH: 11
6eb0ce-bbc7e9 -53 dBm Open Home-Guest-5G CH: 48

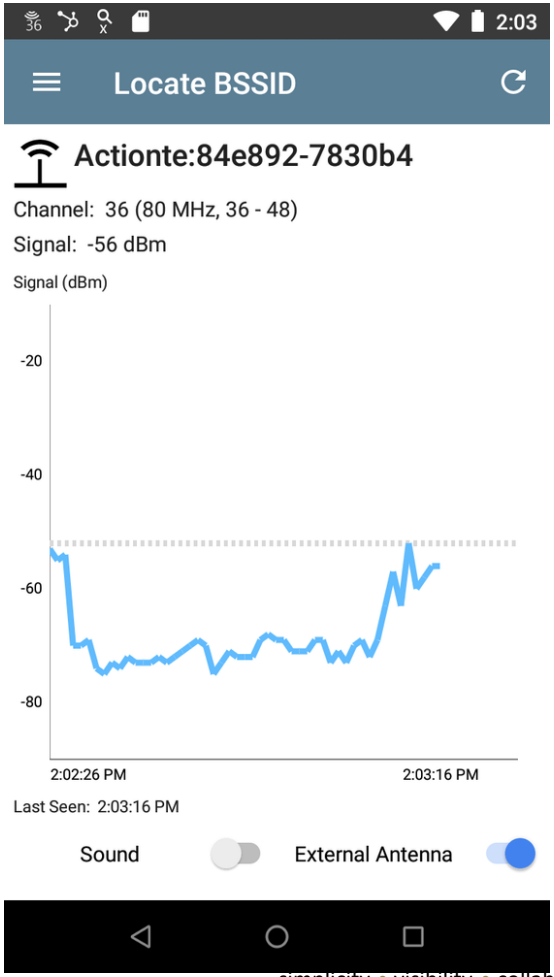
Wi-Fi セグメンテーション

Wi-Fi セグメンテーション



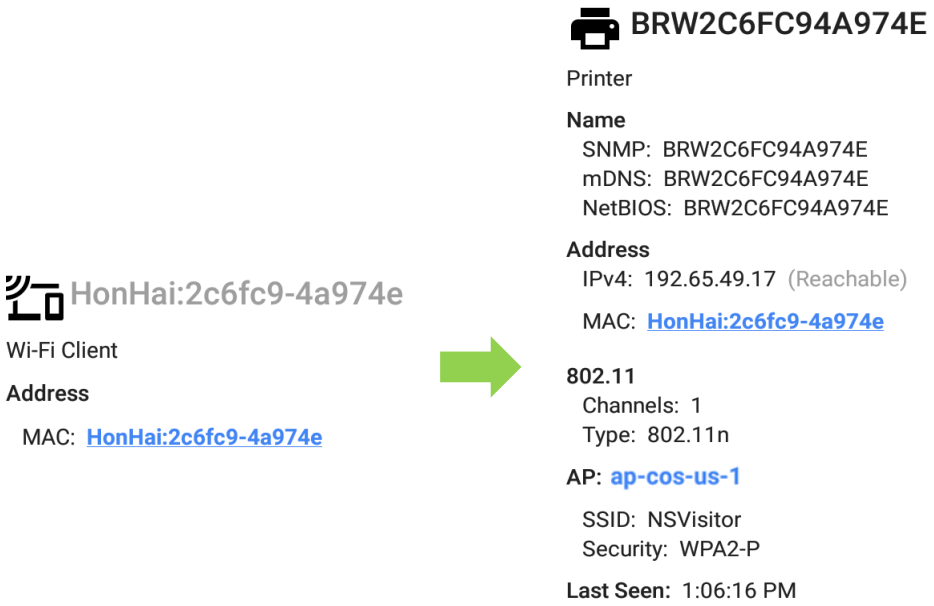

Dons-iPhone
Android-4
Android-6
LITAP02
10.155.131.183
Gabbys-MacBook-Air
Android-9
10.155.131.124
Apple:f86214-811094
Android-2
Zacharys-iPad
LITAP14
10.155.131.85
10.155.131.102
10.155.131.68
Apple:5cf5da-9f8bb9

無許可Wi-Fiの検出



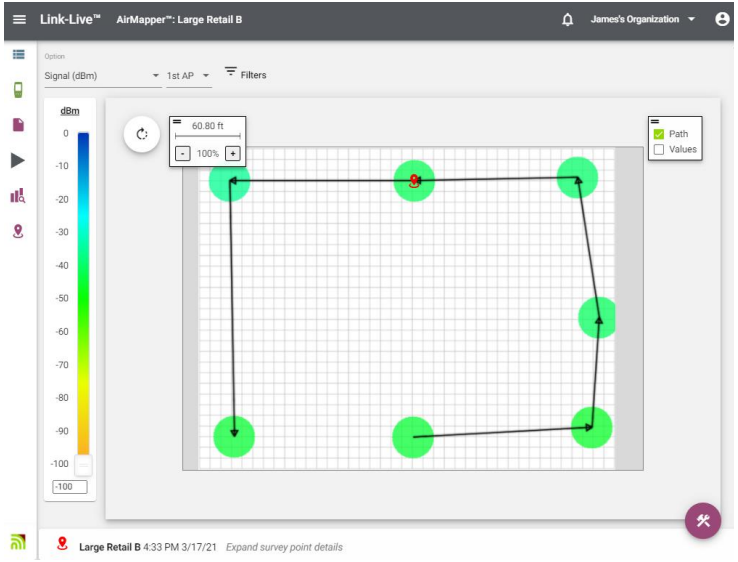
Wi-Fi 解析

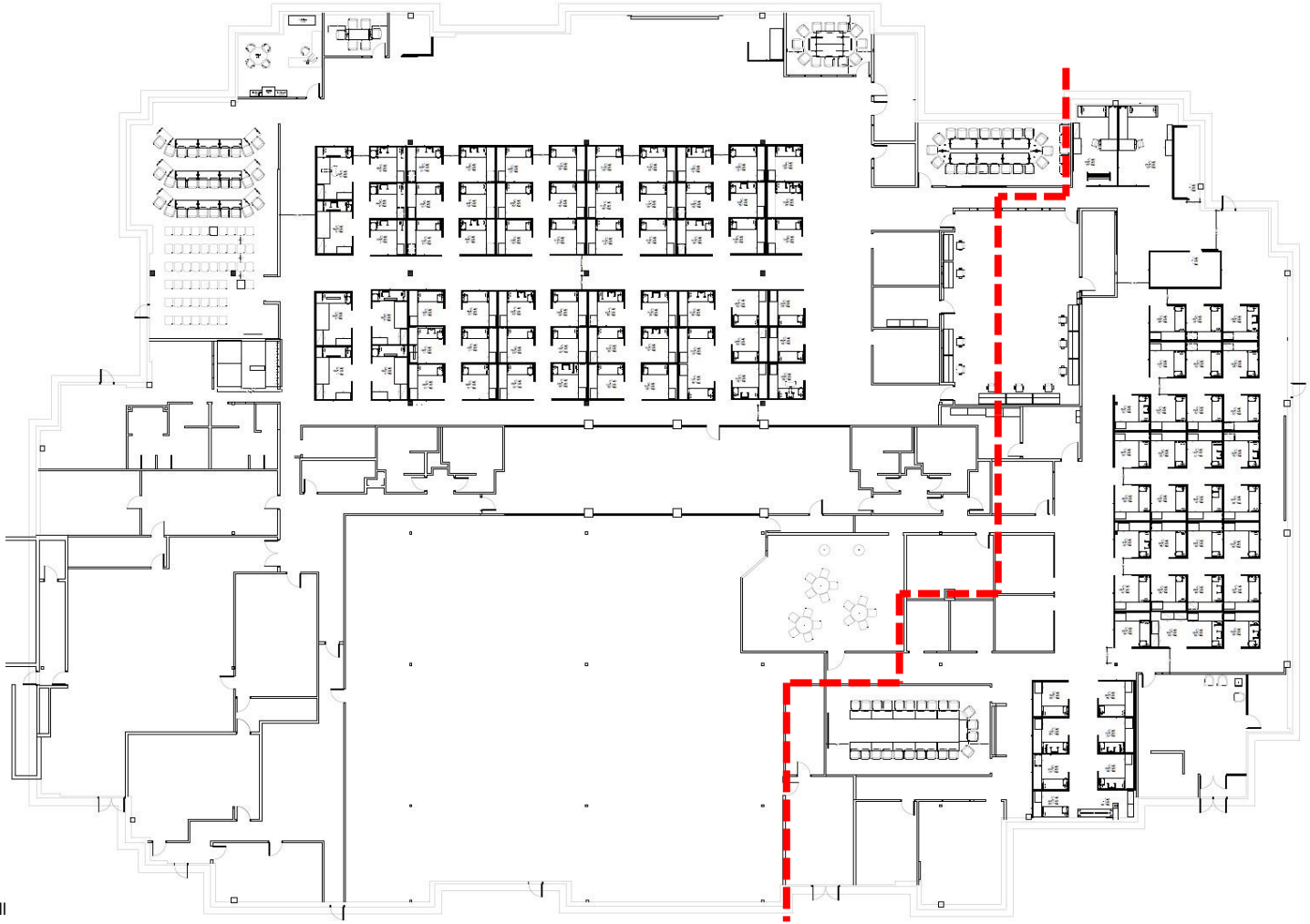
Breaking the Layer 2 Ceiling



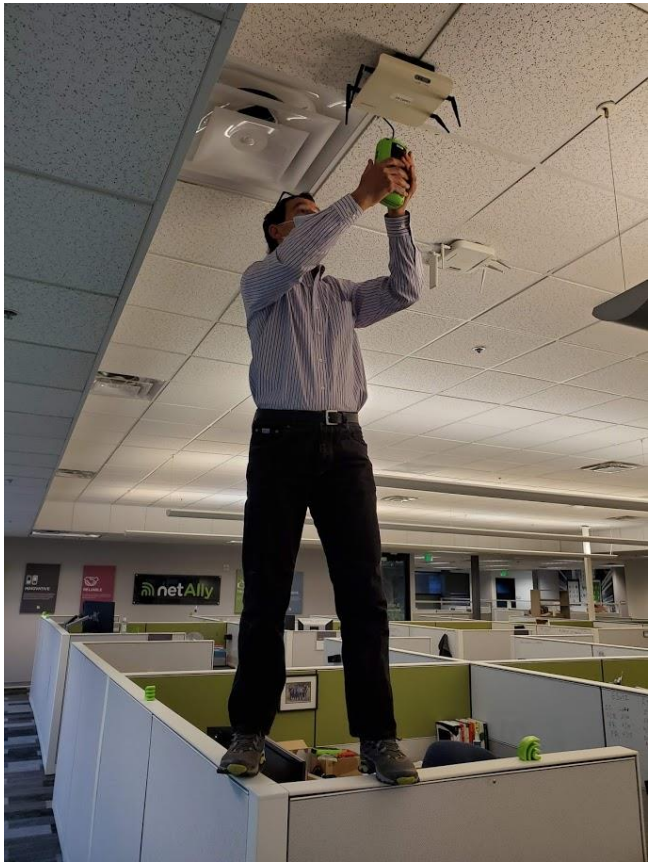
Wi-Fi Demo

迅速で簡単なサーベイ

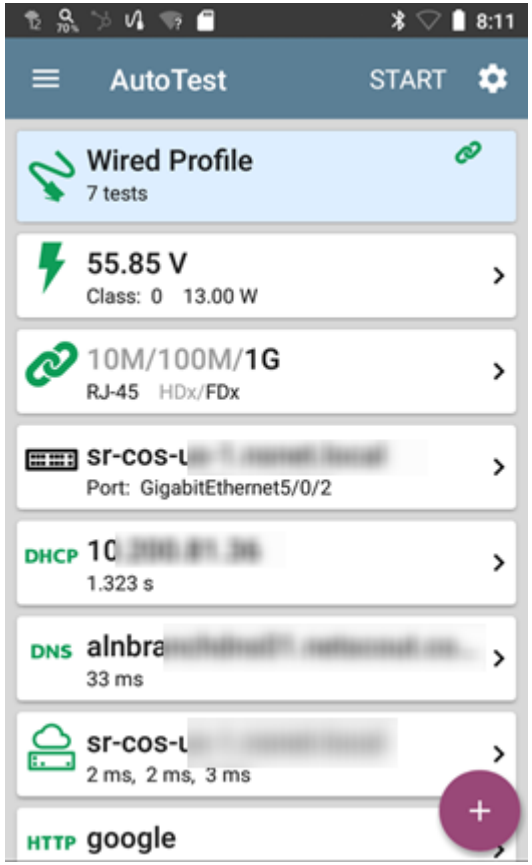




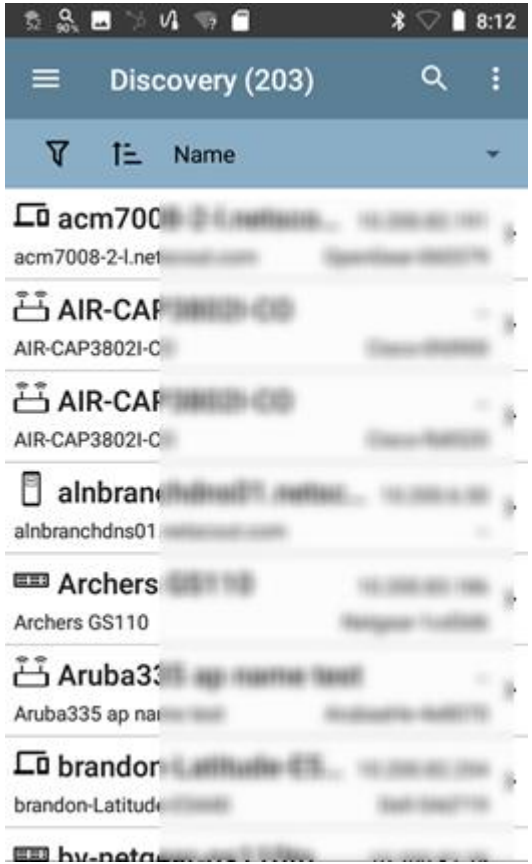

AIRMAGNET
Cos01-02
POWER



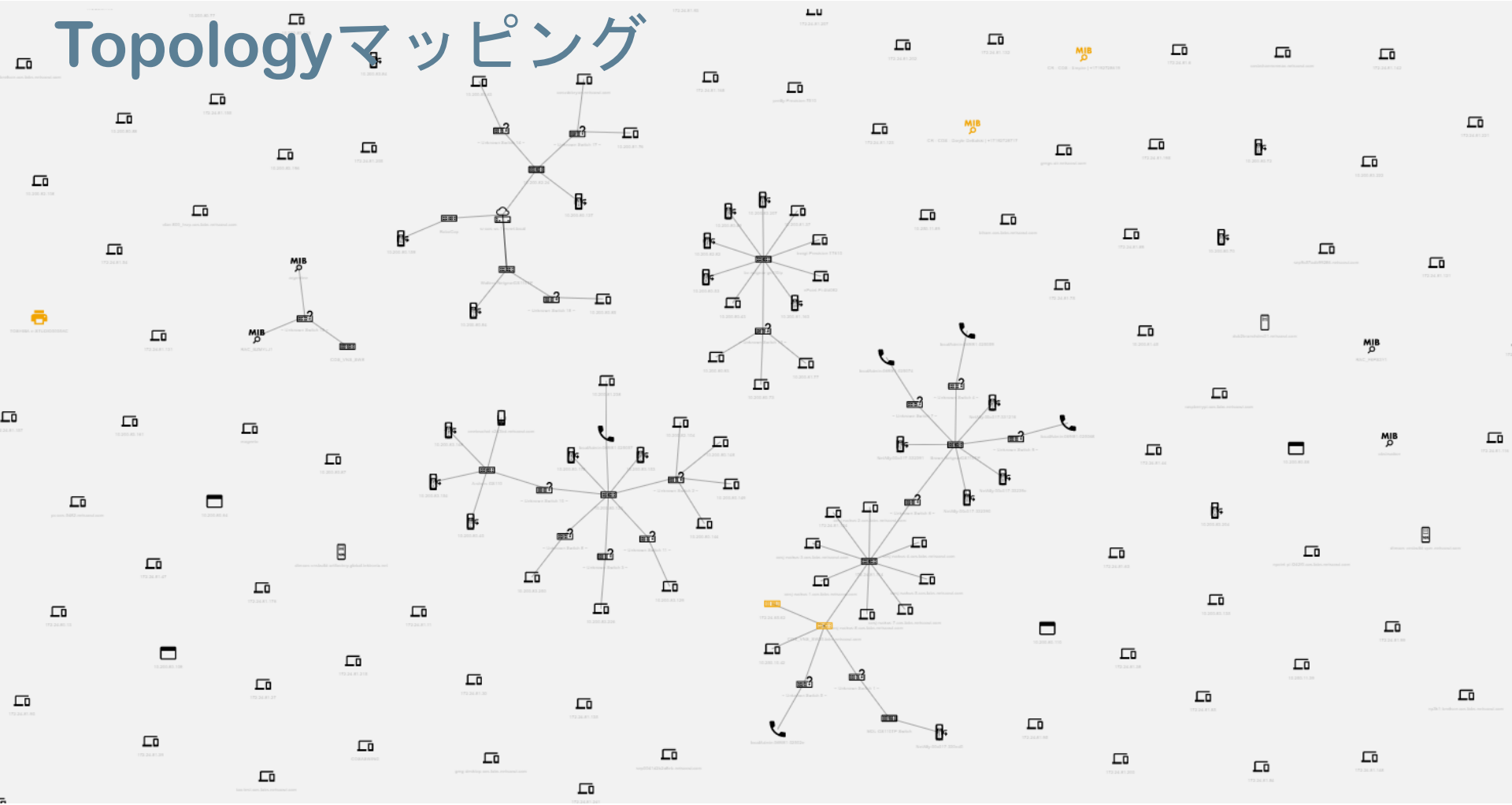
10



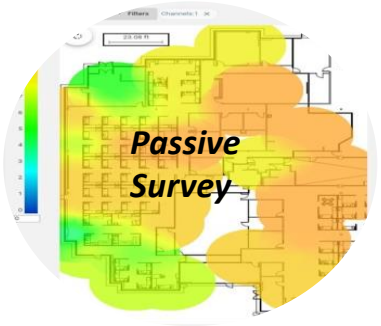
60



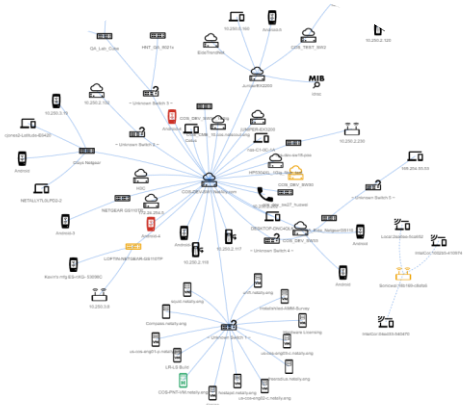
Topologyマッピング



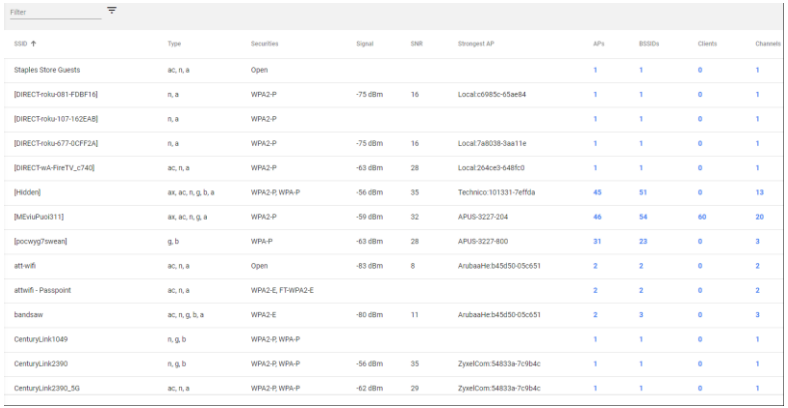
シングルウォークで多くの情報を



Topology

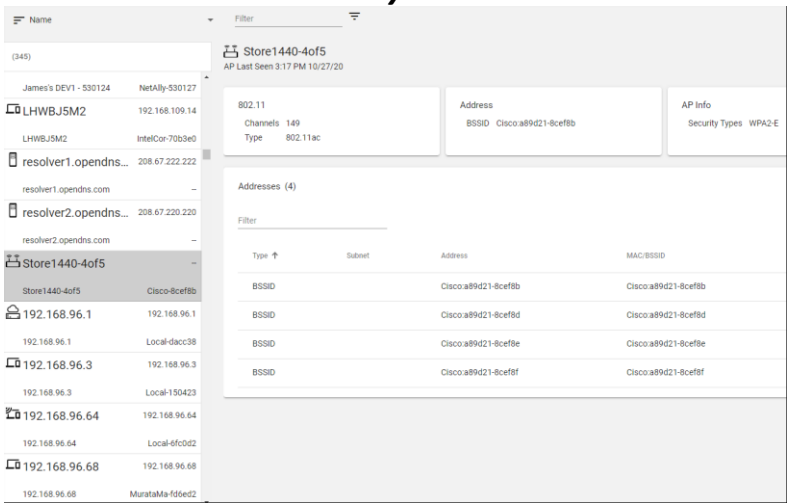


Aggregated Wi-Fi Analysis



SSID	Type	Securities	Signal	SNR	Strongest AP	APs	BSSIDs	Clients	Channels
Staples Store Guests	ac, n, a	Open				1	1	0	1
[DIRECT-roku-081-FDBF16]	n, a	WPA2-P	-75 dBm	16	Local:c6985c-65ae84	1	1	0	1
[DIRECT-roku-107-162EA8]	n, a	WPA2-P				1	1	0	1
[DIRECT-roku-677-0CFF2A]	n, a	WPA2-P	-75 dBm	16	Local:7a8038-3aa11e	1	1	0	1
[DIRECT-wA-FireTV_c740]	ac, n, a	WPA2-P	-63 dBm	28	Local:264ce3-648fc0	1	1	0	1
[Hidden]	ax, ac, n, g, b, a	WPA2-P, WPA-P	-56 dBm	35	Technico:101331-7effda	45	51	0	13
[MEviuPuxi311]	ax, ac, n, g, a	WPA2-P	-59 dBm	32	APUS-3227-204	46	54	60	20
[pocwyg7swean]	g, b	WPA-P	-63 dBm	28	APUS-3227-800	31	23	0	3
att-wifi	ac, n, a	Open	-83 dBm	8	ArubaaHe:b45d50-05c651	2	2	0	2
attwifi - Passpoint	ac, n, a	WPA2-E, FT-WPA2-E				2	2	0	2
bandsaw	ac, n, g, b, a	WPA2-E	-80 dBm	11	ArubaaHe:b45d50-05c651	2	3	0	3
CenturyLink1049	n, g, b	WPA2-P, WPA-P				1	1	0	1
CenturyLink2390	n, g, b	WPA2-P, WPA-P	-56 dBm	35	ZyxelCom:54833a-7c9b4c	1	1	0	1
CenturyLink2390_5G	ac, n, a	WPA2-P, WPA-P	-62 dBm	29	ZyxelCom:54833a-7c9b4c	1	1	0	1

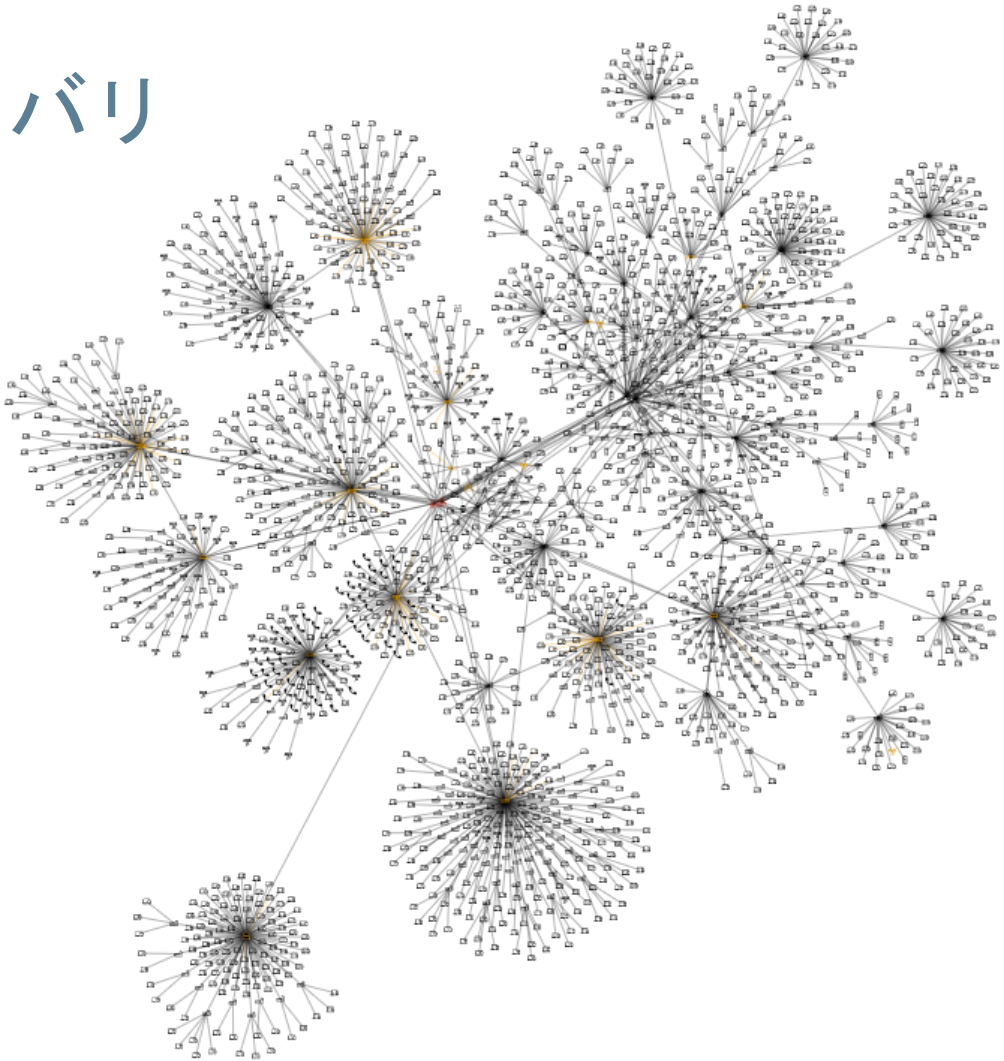
Network Element Analysis



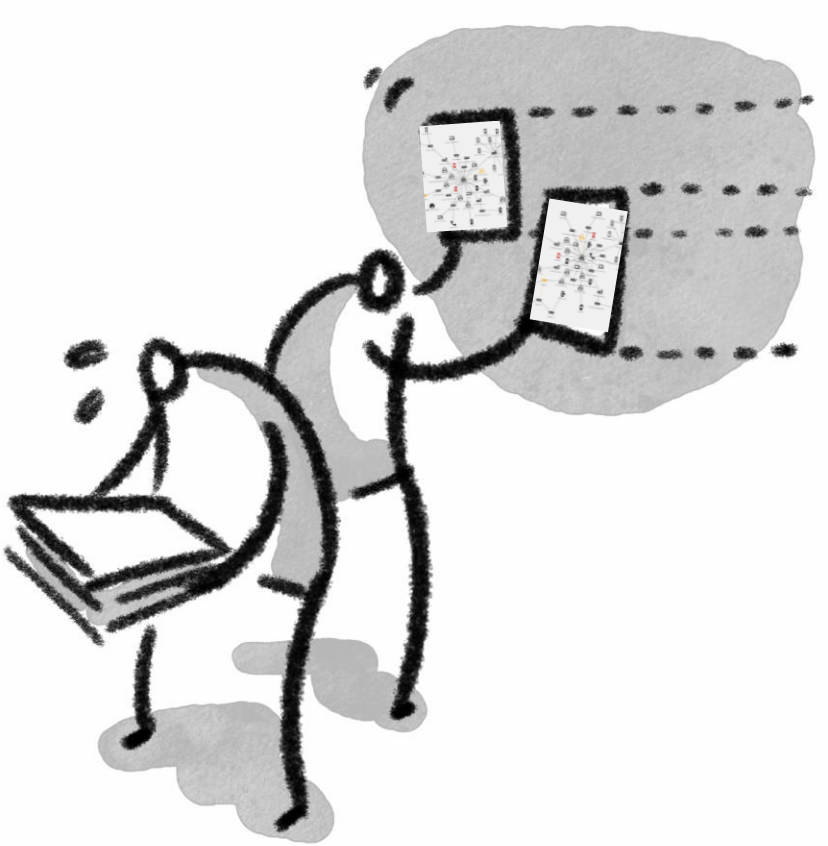
V1.5

異なるディスカバリ

ディスカバリ



ディスカバリの差分



Thank you

E-mail： netally@keisokuki-land.co.jp
infoj@netally.com

東洋計測器株式会社
計測器ランド

http://www.keisokuki-land.co.jp/support/netally/