2024年度
ISSスクエアシンポジウム
研究成果報告

2025/02/28

システム分科会

目次

- 取り組み内容について
  - システム分科会のテーマ（概要）
  - 活動報告
  - 背景
  - 目標
- 実証経過報告
  - ハードウェア・ソフトウェア開発
  - WiFiアクセスポイントの情報収集
  - 収集データの分析・可視化
    - ヒートマップで脆弱性WiFiアクセスポイント可視化
    - グラフ表示による集計情報の可視化
- 考察・まとめ
  - 考察
  - まとめ

システム分科会のテーマ（概要）

- **概要**

“The Information Security of things”をキーワードに、一般家庭の機器に組み込まれる小さいITシステムから、社会インフラの中に組み込まれる大規模ITシステムまでを俯瞰し、それを支えるセキュリティシステム技術の現状と課題について、研究を行っている。

- **メンバーリスト（院生9名、指導教員2名）**

RL　:情セ大　大久保 隆夫、須崎 有康

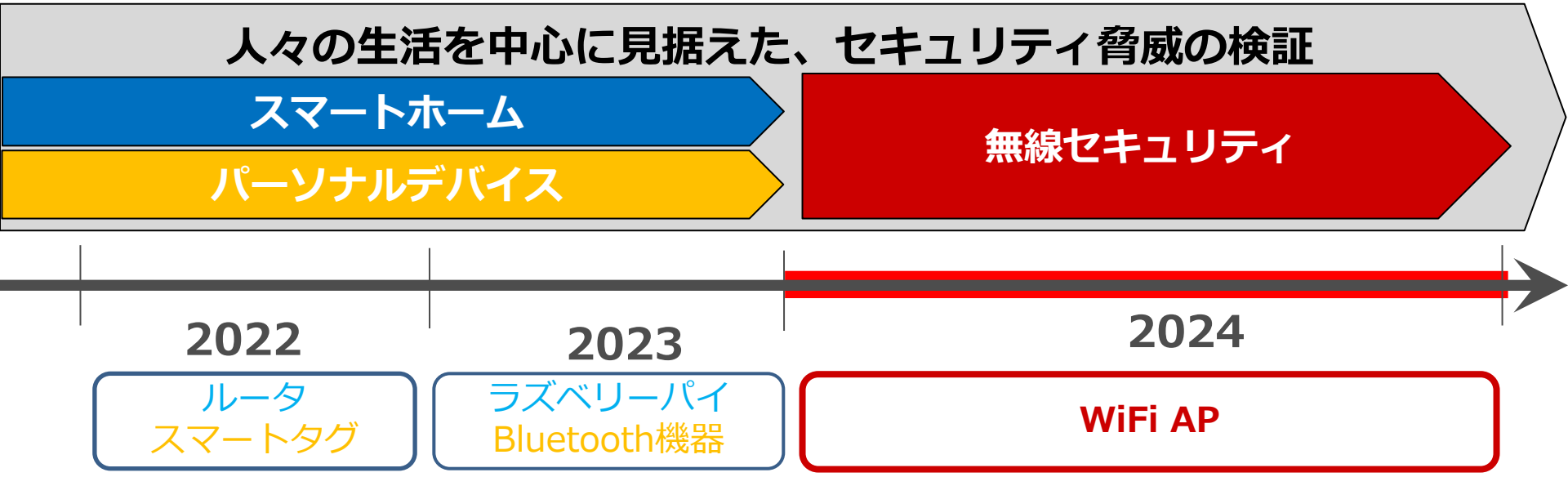
幹事

情セ大 M1：吉村 隼哉, 佐藤 龍

メンバー

中央大 M1：-
中央大 M2：浅田 勇飛, 今枝 俊輔
情セ大 M2：松坂 惇平, 江 鴻浩
情セ大 M1：松浦 栄亮, 水上 昌大, 吉村 隼哉, 佐藤 龍, 小川 森護

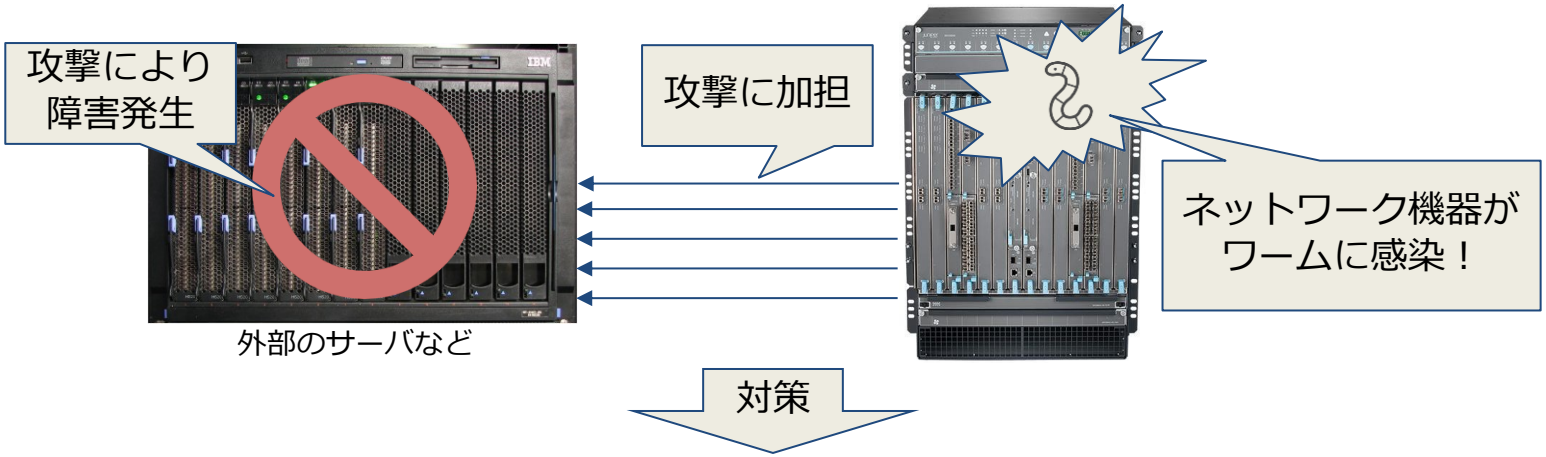
活動報告（これまでの取り組み）



活動	活動内容
第1回	幹事と実行委員の決定、昨年度テーマの紹介、残タスクの共有、M2メンバの役割決定、環境セットアップ、次回のテーマ検討
第2回	今年度のテーマを選定し、Wi-Fi脆弱性マッピングをテーマに進めることを決定
第3回	ハードウェアや開発言語を検討し、スマートスピーカーの遠隔開発セットアップを実施
第4回	10月入学の小川さんへの活動内容説明、Raspberry Piおよび周辺機器の動作確認、今後の進め方について検討
第5回	不足物品の調達、Raspberry Piの組み立て、開発環境の整備
第6回	追加部品取り付け後の状態確認、分析プログラムの開発準備、タスク抽出と割当、リポジトリ作成とアクセス確認、データ収集
第7回	成果のまとめ、発表資料作成に向けた相談

背景

ネットワーク機器がマルウェアに感染する事例が増加し，買い換えが奨励されている
→ 古い無線AP(=暗号規格)を可視化できれば実態把握や注意喚起に有効ではないか



脆弱なネットワーク機器を減らすため
アップデートや買い替えを奨励

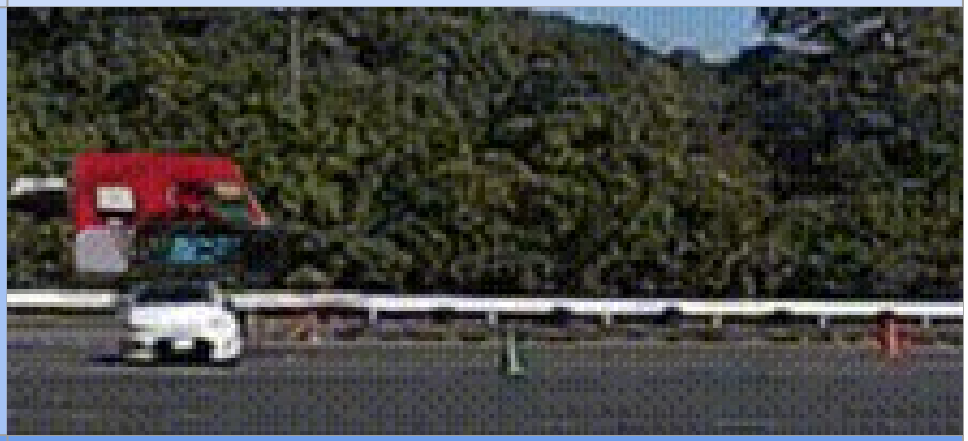
実際どれだけ古いデバイスが使われているのか？
WarDrivingの手法で可視化してみよう！

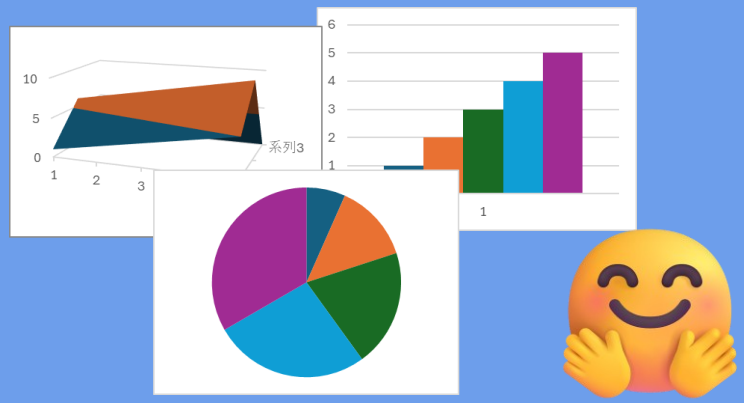
https://commons.wikimedia.org/wiki/Category:Juniper_Networks#/media/File:Juniper_Networks_SRX5800_service_gateway_and_security_appliance.jpg
https://commons.wikimedia.org/wiki/File:IBM_Bladecenter_E_(front).jpg

目標

①周囲のWiFiデバイスを
スキャンするため
ハード・ソフトを構築

②デバイスを車に乗せ，
横浜周辺のWiFiアクセス
ポイントの情報を収集





③収集した情報を元に
ヒートマップや統計情報を
作成し分析を実施

①ハードウェア開発

- **参考Webページを元にハードウェアの構築を開始**

Raspberry PI Wardriving setup

how to setup a Raspberry PI 4 or 3b to collect Wifi information. This is commonly called Wardriving (Wikipedia)

【参考Webページ】
https://www.designer2k2.at/de/mods/elektronik/156-raspberry-pi-wardriving-setup

①ハードウェア開発

- **必要物品のリストアップと調達**

品目	国内販売URL	価格
Raspberry Pi 4	https://akizukidenshi.com/catalog/g/g116834/	¥10,800
RTC hat	https://www.switch-science.com/products/5334	¥803
OLED hat	https://www.digikey.jp/ja/products/detail/adafruit-industri	¥3,528
GPS Module (serial, not usb)	https://www.amazon.co.jp/-/en/dp/B0BV2KTV5N/	¥2,299
WIFI USB Sticks, suitable for monitoring mode	https://www.amazon.co.jp/dp/B0C8SVZ9Q1/	¥5,400
SD card for the operating system, like the Samsung Pro Endurance	https://www.amazon.co.jp/dp/B08CXF3VH9/	¥1,680
USB Stick for actual logfile	https://www.amazon.co.jp/dp/B08PTR59PS	¥680
Bluetooth dongle (optional)	https://www.amazon.co.jp/dp/B09FJYCXDK	¥1,200
モバイルバッテリ	https://www.amazon.co.jp/dp/B09RJ4HKFB	¥5,240
Type-C ケーブル	https://www.amazon.co.jp/Anker-PowerLine-USB-C-Ma	¥990
ラズパイケース	https://www.amazon.co.jp/dp/B07WCKLFLP	¥1,039
GPIO分岐端子	https://www.amazon.co.jp/dp/B08CXZC3RC	¥1,099
電池	https://www.amazon.co.jp/dp/B01ASR2RT6	¥840
	計	¥33,659

①ハードウェア開発

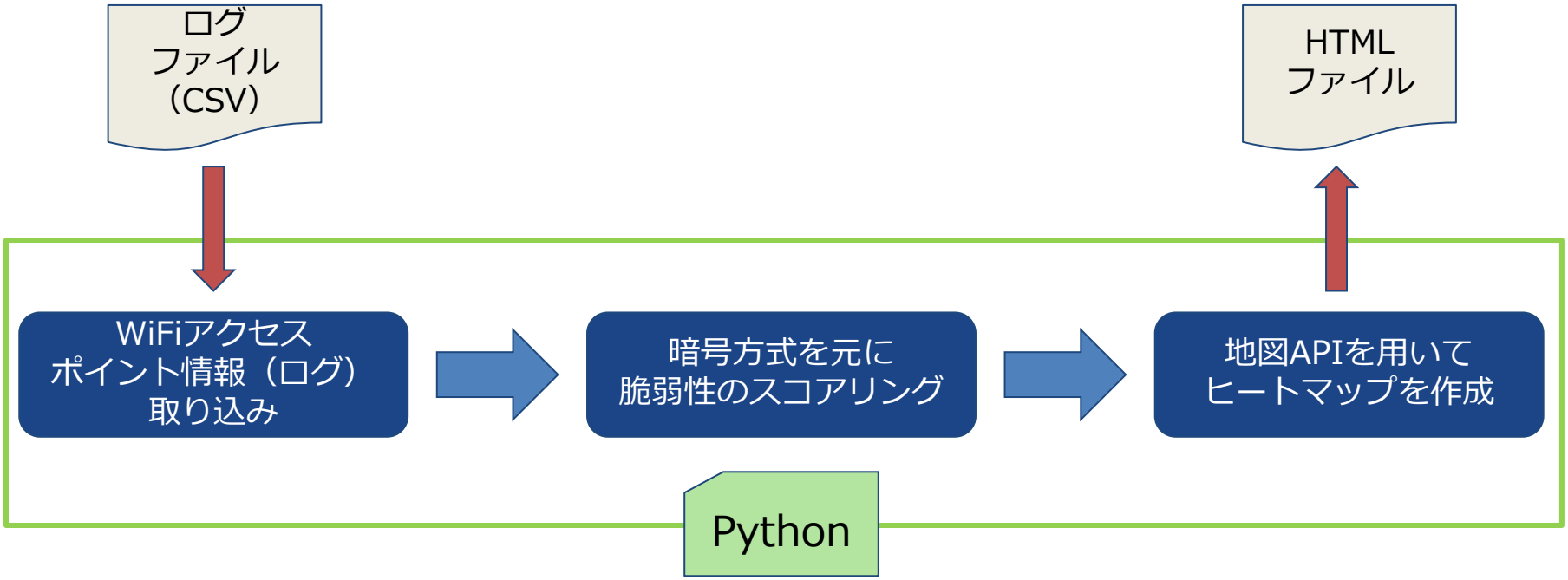
- **組み立て作業の様子**

完成！！

②ソフトウェア開発

- **ヒートマップ作成システムの概要**

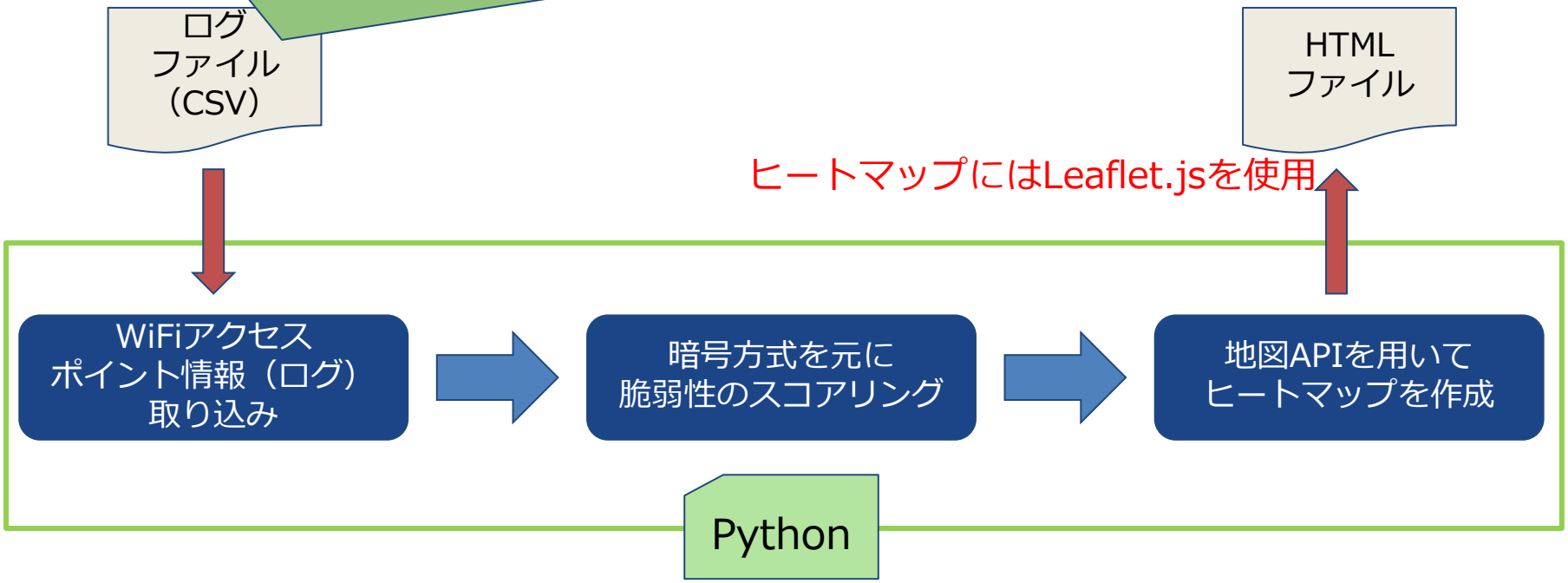
ヒートマップにはLeaflet.jsを使用



②ソフトウェア開発

ヒートマップ作成システムの概要

MAC	SSID	AuthMode	FirstSeen	Channel	RSSI	Current Latitude	Current Longitude	Altitude Meters	Accuracy Meters	Type



②ソフトウェア開発

● 脆弱性のスコアリング

Scaled times (0 to 1 range) after PowerTransformer and MinMaxScaler:

暗号方式	解読時間	脆弱性スコア
CCMP	**10の25乗年**程度	0.000
TKIP+CCMP	10の12乗年程度	0.005
TKIP	7分程度	0.867
WEP	数十秒程度	0.923
No encryption	ほぼ０秒	1.000

【参考】

[1]https://internet.watch.impress.co.jp/cda/news/2008/10/14/21162.html
[2]https://news.mynavi.jp/techplus/article/20100824-wpatkip/
[3]https://xtech.nikkei.com/it/article/COLUMN/20090526/330680/#:~:text=%E4%BE%8B%E3%81%88%E3%81%B0%EF%BC%8C%E7%B1%B3%E5%9B%BD%E6%94%BF%E5%BA%9C%E3%81%8C%E8%A6%8F%E6%A0%BC,%E3%81%AB%E9%95%B7%E3%81%84%E5%B9%B4%E6%9C%88%E3%81%A7%E3%81%99%E3%80%82

②WiFiアクセスポイントの情報収集

- **横浜、みなとみらいエリアで計測**


CPU: 6% メモリ: 12% 温度: 43.3
検出 8515
メモリ使用量: 346MB
2025年01月11日 20:03:20

③収集データの分析・可視化

- **ヒートマップで脆弱性WiFiアクセスポイント可視化**

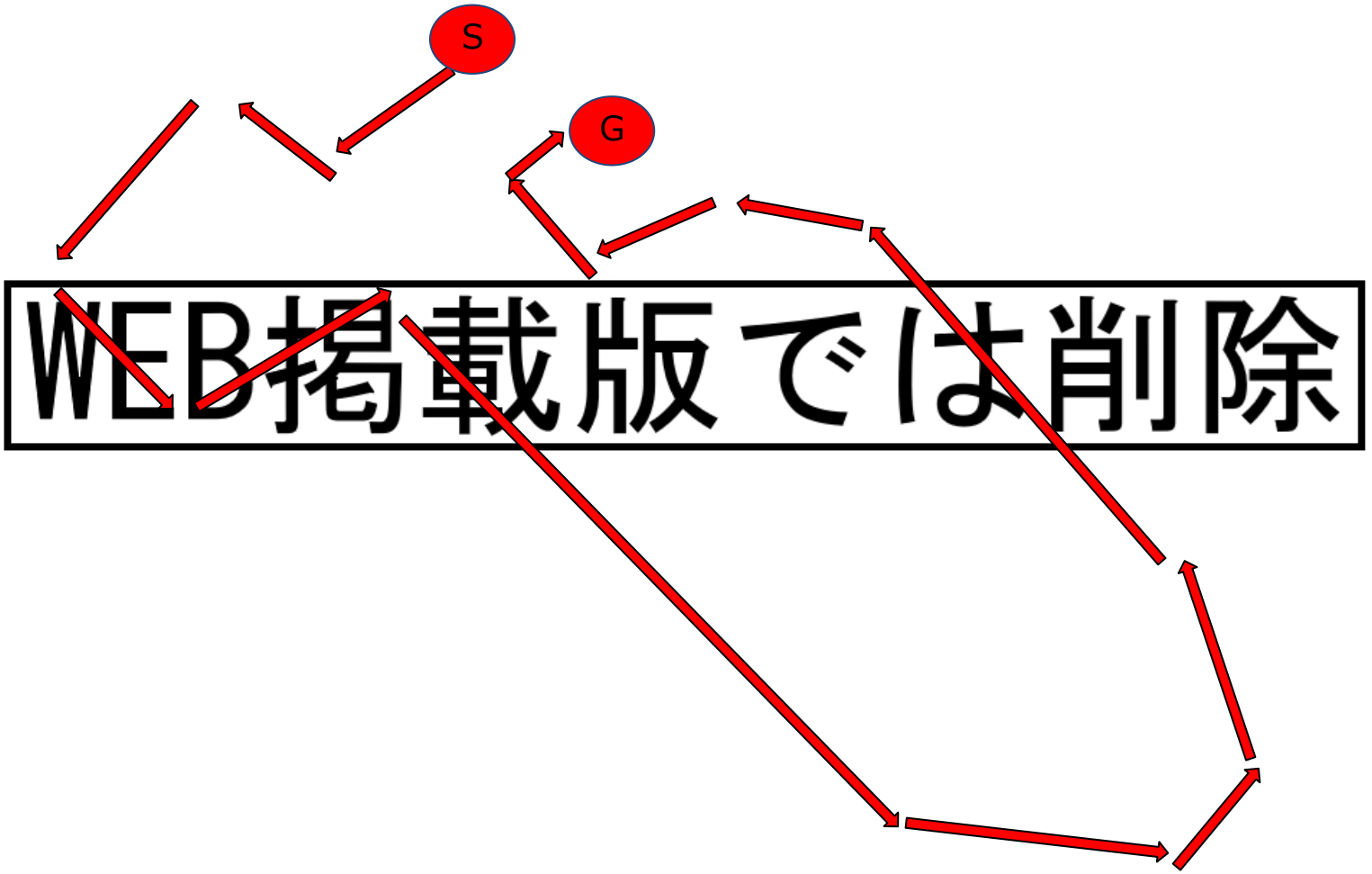
濃くなる程、脆弱性のある
アクセスポイントが多い

WEB掲載版では削除

③収集データの分析・可視化

- **ヒートマップで脆弱性WiFiアクセスポイント可視化**

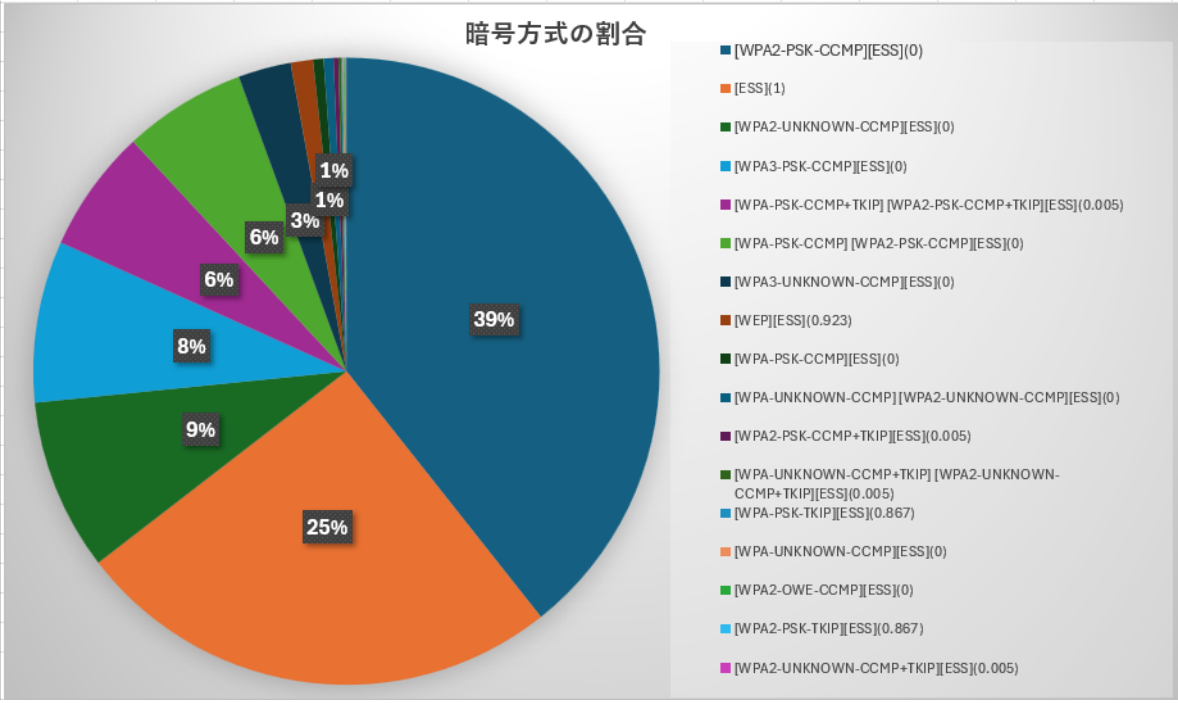
濃くなる程、脆弱性のある
アクセスポイントが多い



③収集データの分析・可視化

- **グラフ表示による集計情報の可視化**
  - **暗号方式の割合**

暗号方式（スコア）	件数
[WPA2-PSK-CCMP][ESS](0)	8543
[ESS](1)	5478
[WPA2-UNKNOWN-CCMP][ESS](0)	1922
[WPA3-PSK-CCMP][ESS](0)	1811
[WPA-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP][ESS](0.005)	1379
[WPA-PSK-CCMP] [WPA2-PSK-CCMP][ESS](0)	1376
[WPA3-UNKNOWN-CCMP][ESS](0)	593
[WEP][ESS](0.923)	249
[WPA-PSK-CCMP][ESS](0)	117
[WPA-UNKNOWN-CCMP] [WPA2-UNKNOWN-CCMP][ESS](0)	110
[WPA2-PSK-CCMP+TKIP][ESS](0.005)	55
[WPA-UNKNOWN-CCMP+TKIP] [WPA2-UNKNOWN-CCMP+TKIP][ESS](0.	31
[WPA-PSK-TKIP][ESS](0.867)	17
[WPA-UNKNOWN-CCMP][ESS](0)	12
[WPA2-OWE-CCMP][ESS](0)	10
[WPA2-PSK-TKIP][ESS](0.867)	7
[WPA2-UNKNOWN-CCMP+TKIP][ESS](0.005)	4
[WPA3-PSK-CCMP+TKIP][ESS](0.005)	2
[WPA-PSK-TKIP] [WPA2-PSK-TKIP][ESS](0.867)	2
[WPA-UNKNOWN-TKIP][ESS](0.867)	2
[WPA-PSK-CCMP+TKIP][ESS](0.005)	1
合計	21721

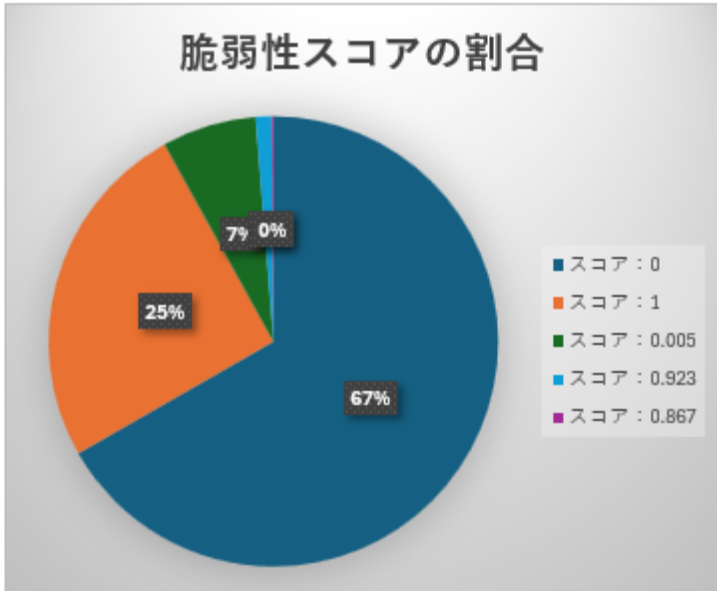


③収集データの分析・可視化

- **グラフ表示による集計情報の可視化**
  - **脆弱性スコアの割合**

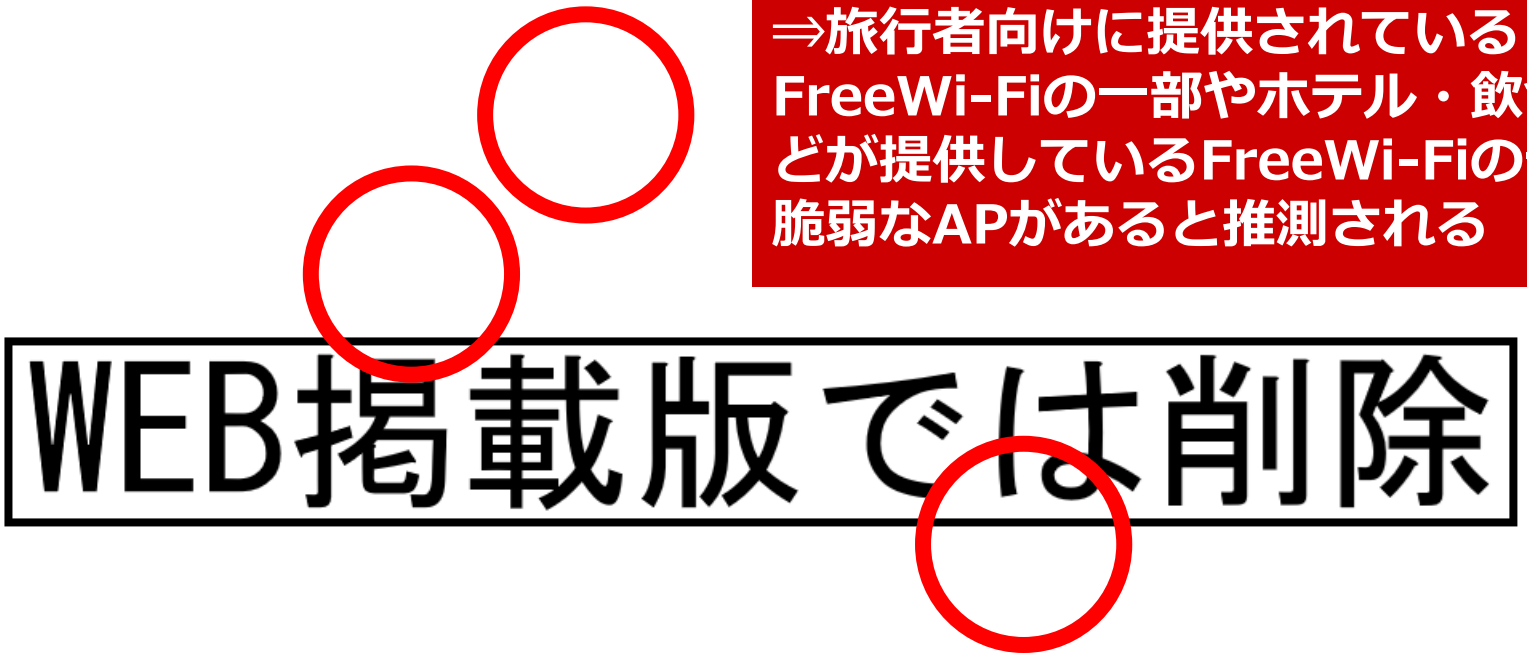
スコア：０～１　　**※0に近いほど堅牢**
1に近いほど脆弱

スコア	件数
スコア：0	14494
スコア：1	5478
スコア：0.005	1472
スコア：0.923	249
スコア：0.867	28
合計	21721



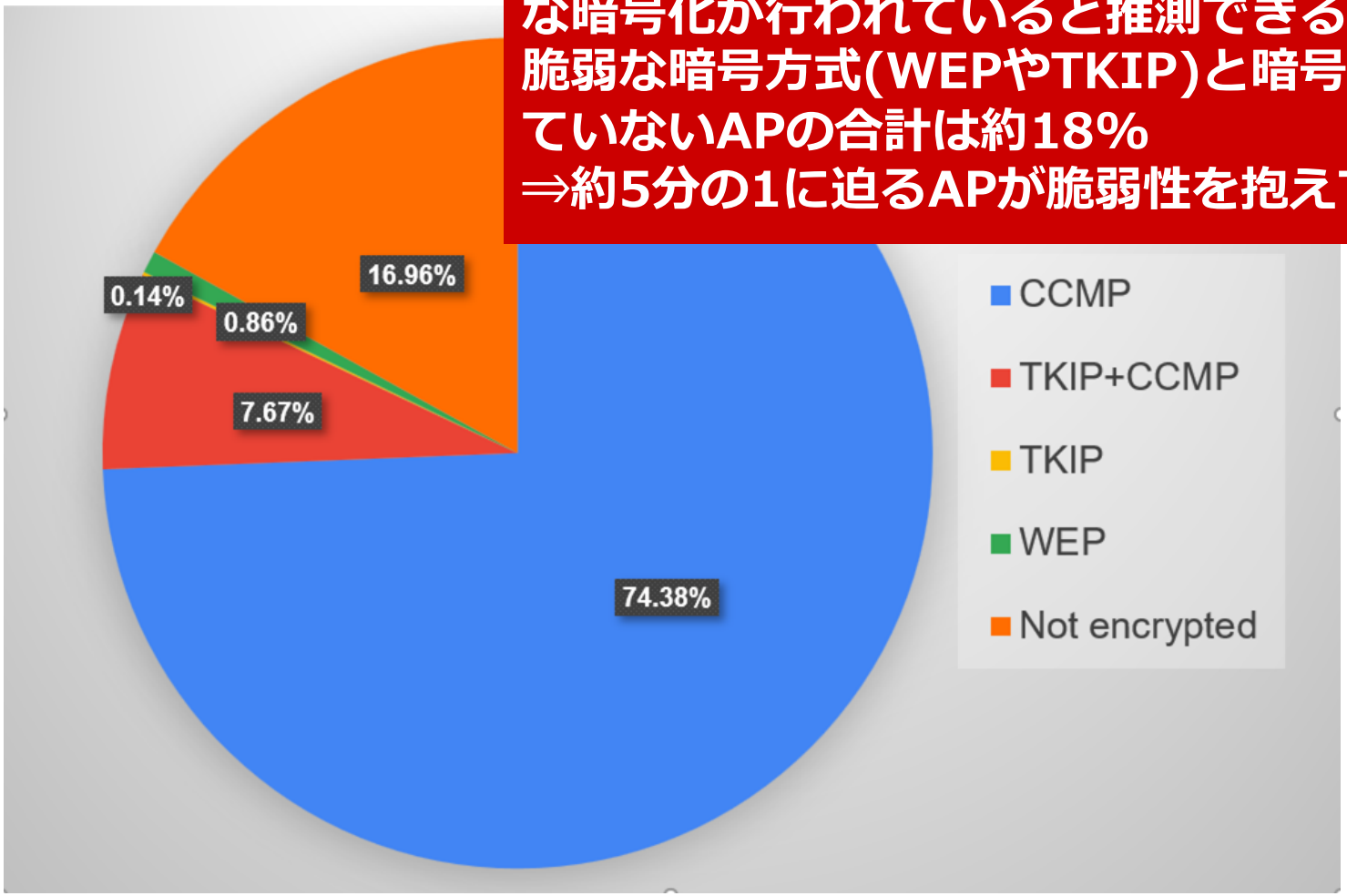
考察

高脆弱性APの密集地点(赤丸部分)は
駅前や大通りなど人口が多い場所
⇒旅行者向けに提供されている
FreeWi-Fiの一部やホテル・飲食店な
どが提供しているFreeWi-Fiの一部に
脆弱なAPがあると推測される



考察

最も多い暗号化方式は「CCMP」
⇒大半の場所で利用されているWi-Fiは堅牢な暗号化が行われていると推測できる
脆弱な暗号方式(WEPやTKIP)と暗号化されていないAPの合計は約18%
⇒約5分の1に迫るAPが脆弱性を抱えている



まとめ

背景

古いネットワーク機器がマルウェアに感染する事例が増加し，買い換えが奨励されている
⇒古い無線AP(=暗号規格)を可視化できれば、実態把握や注意喚起に有効ではないか？
実際どれだけの古いデバイスが使われているのかについてWarDrivingの手法で可視化を行った

目標

①周囲のWiFiデバイスをスキャンするためハード・ソフトを構築 **達成！**

②デバイスを車に乗せ，横浜周辺のWiFiアクセスポイントの情報を収集 **達成！**

③収集した情報を元にヒートマップや統計情報を作成し分析を実施 **達成！**

活動結果

■目標①②③を達成しマッピングと分析に成功
■利用されている暗号化方式はCCMPが最も多く大部分は新しい機器へ更改されていると推定
■公衆無線LANはOpenで利用される傾向が強いことが判明
■WEP，TKIP，Openを利用している脆弱なAPの合計は約18%にも及ぶ
■WEPについては10年以上前※1に設置された機種の可能が高い

※1 2014年ニンテンドーWiFiコネクションサービス終了以降，初期状態でWEP有効の機器がほとんど出荷されていないと仮定

ヒートマップ