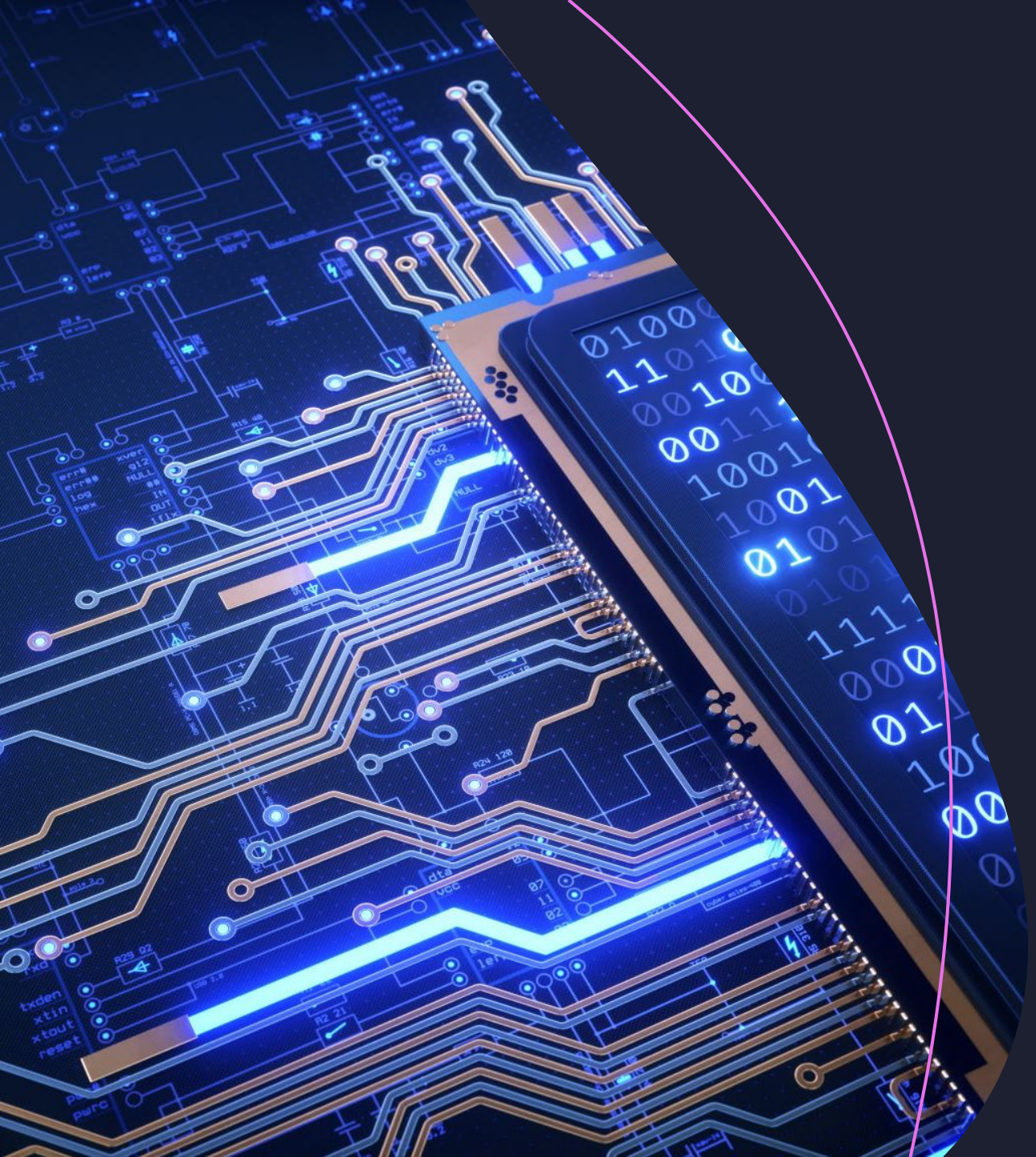


# 無線技術とサイバーセキュリティ

福知山公立大学 情報学部

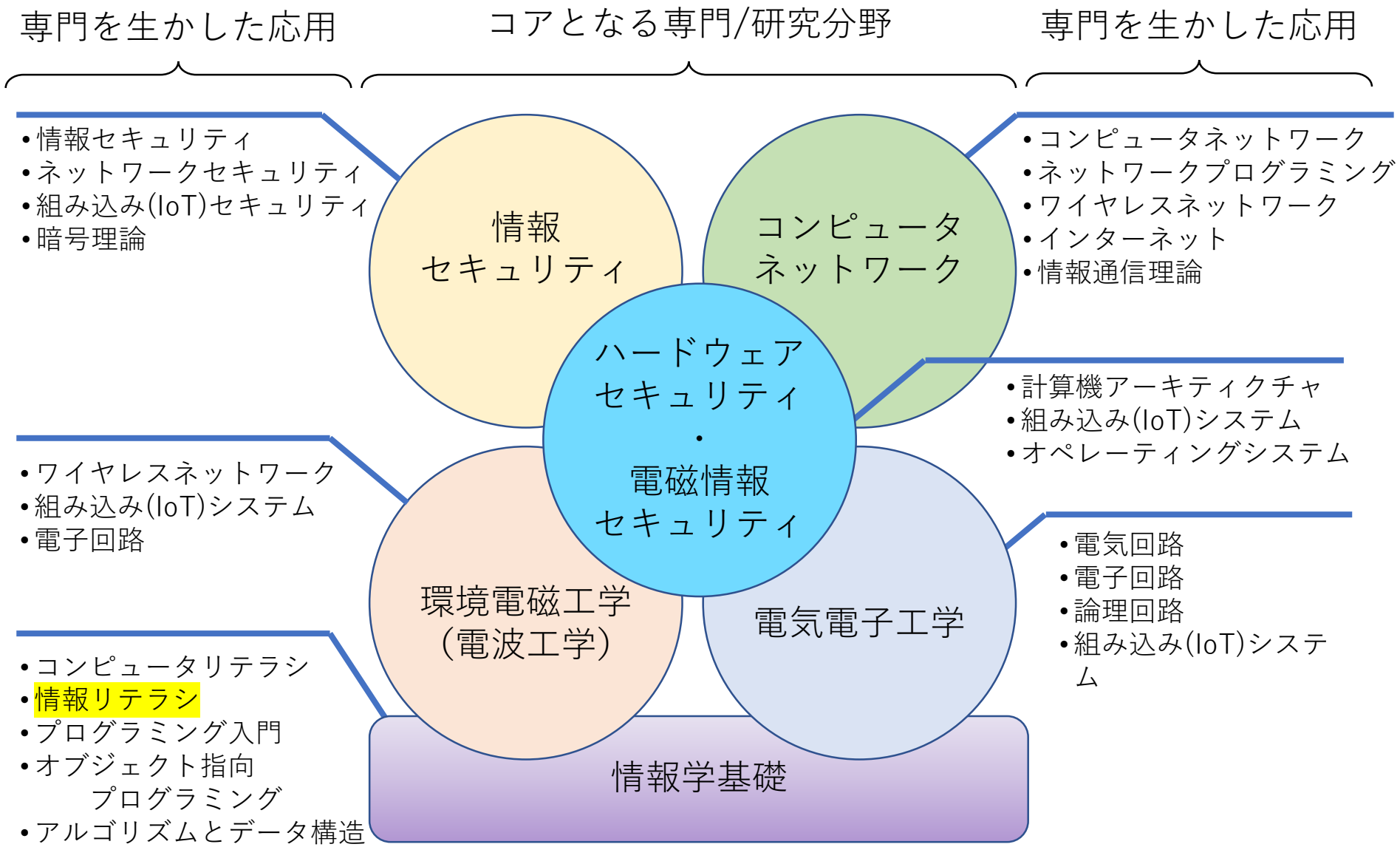
衣川 昌宏

# 自己紹介

衣川 昌宏（きぬがわ まさひろ）

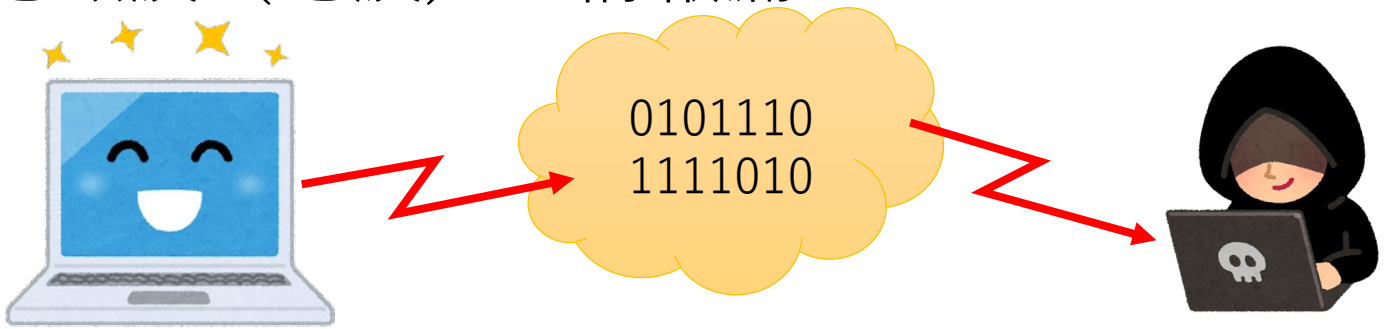
- 出身：兵庫県養父市（京都共栄学園バタビア卒）
- 学歴：会津大学→東北大学大学院→博士（情報科学）
- 職歴：情報ネットワーク関連で活躍
  - 零細企業勤務（3年間、会津若松市）
    - 企業ネットワーク構築、当時先端のVPNを安価・高安定で提供
  - （独）情報通信研究機構
    - 日本縦断高機能高速ネットワークJGN2plusのサービス開発
  - 教員職：仙台高等専門学校、会津大、東北学院大、東北文化学園大
    - 情報セキュリティ、情報ネットワーク、情報リテラシー、情報数学等を講義

# 専門


専門を生かした応用
コアとなる専門/研究分野
専門を生かした応用
•情報セキュリティ
•ネットワークセキュリティ
•組み込み(IoT)セキュリティ
•暗号理論
情報
セキュリティ
コンピュータ
ネットワーク
•コンピュータネットワーク
•ネットワークプログラミング
•ワイヤレスネットワーク
•インターネット
•情報通信理論
ハードウェア
セキュリティ
・
電磁情報
セキュリティ
•計算機アーキティクチャ
•組み込み(IoT)システム
•オペレーティングシステム
•ワイヤレスネットワーク
•組み込み(IoT)システム
•電子回路
環境電磁工学
(電波工学)
電気電子工学
•電気回路
•電子回路
•論理回路
•組み込み(IoT)システム
•コンピュータリテラシ
•情報リテラシ
•プログラミング入門
•オブジェクト指向
プログラミング
•アルゴリズムとデータ構造
情報学基礎

# 講演の概要

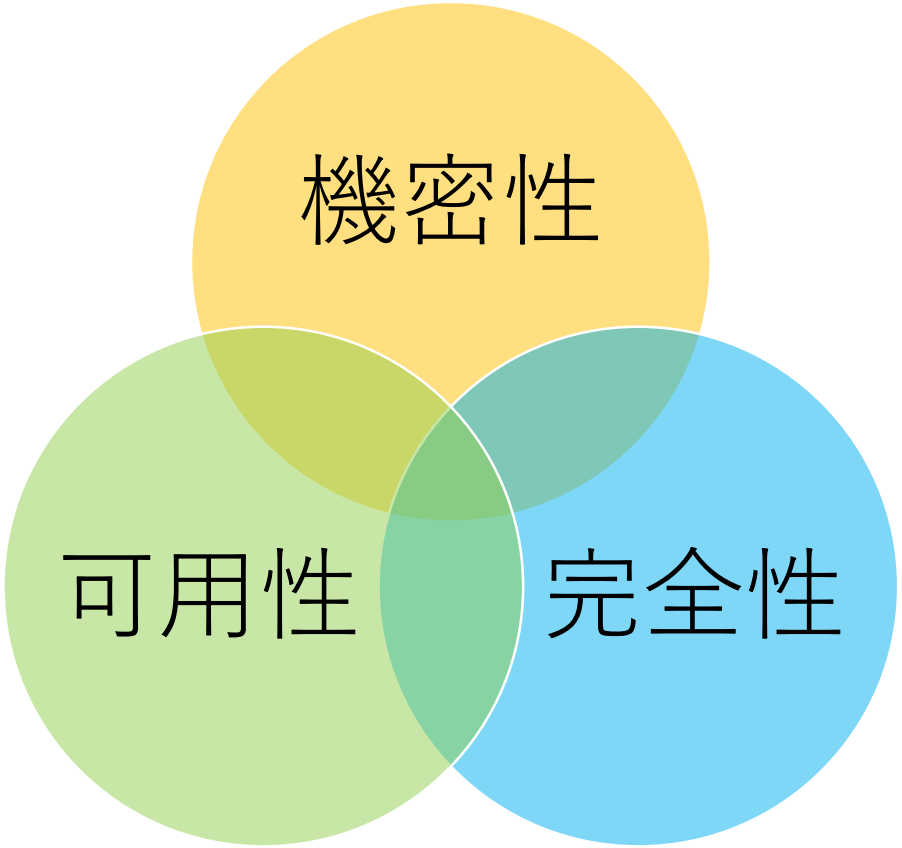
- 漏えい電磁波（電波）と情報漏えい




- 安全にワイヤレス機器を使うには




# 情報セキュリティの基本3要素




- 機密性
  - 許可されたものだけが、情報を閲覧変更可
  - 例：暗号化
- 完全性
  - 情報に無許可の改変が無いこと
  - 例：封印、ファイルのハッシュ値
- 可用性
  - 許可されたものが、いつでも利用可能である
  - 例：社会インフラ（電気・水道・通信など）

# 環境電磁工学

- 電波工学の一つ
  - 電子機器は動作時に非意図的に電波を放射してしまう（電圧・電流→電波）
  - その電波が、他の機器の動作を妨害することがある（電波→機器内部に干渉）

電波は出すけど
他の機器の妨害をしない、妨害を受けない

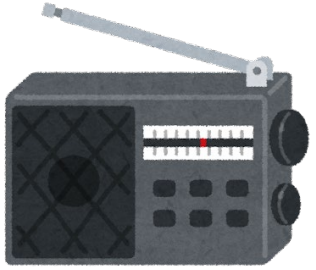
↓

電磁両立性


この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。
VCCI－A

電子機器の動作に伴う電磁放射

電波の感受性の高い機器に妨害を与える



ガリッ、ガリッ
ザー、ザー
ブーン、ブーン

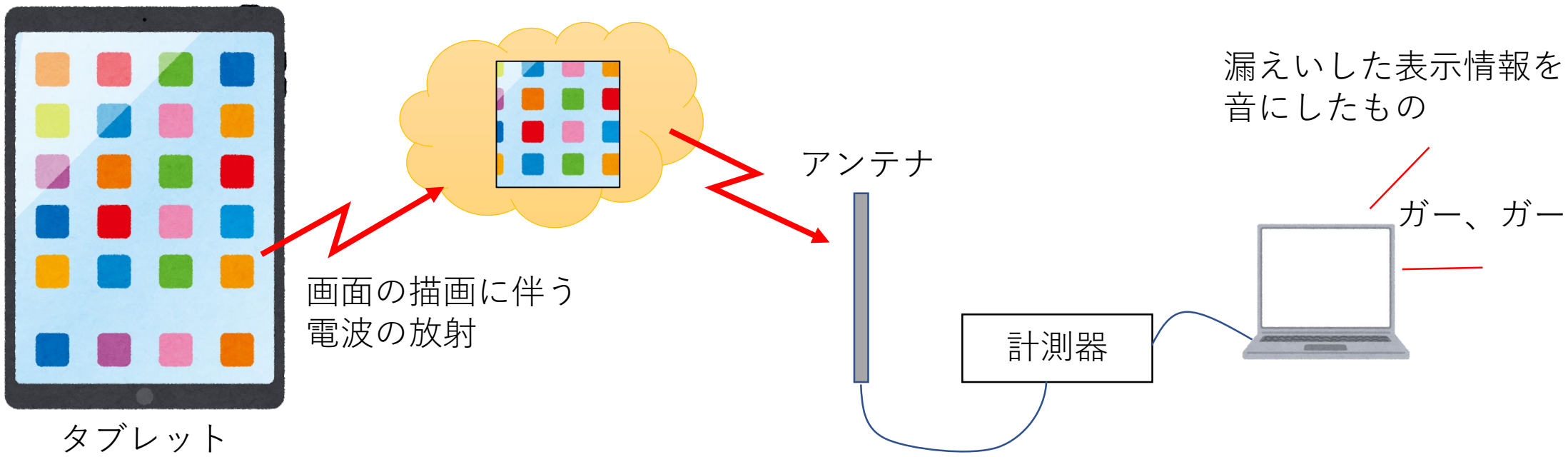
情報セキュリティでいうところの、
**可用性・完全性**の低下

# 環境電磁工学と情報セキュリティ（続）

- なぜ電波が放射されるのか
  - 情報通信機器が情報を処理する
    →情報処理に応じた電圧・電流の変化が機器の回路に生じる
    →電圧・電流の変化が電波を発生させる

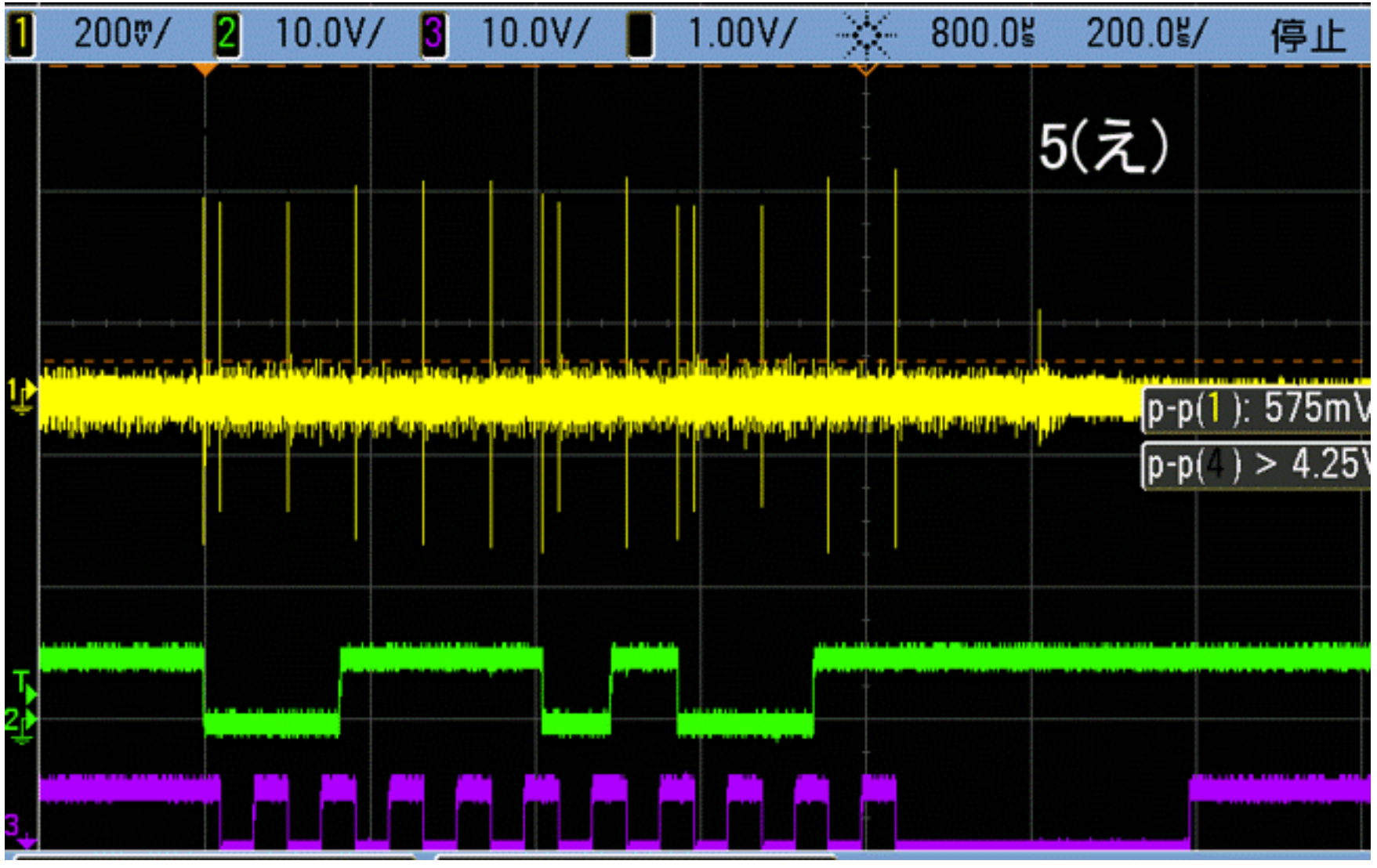
# デモンストレーション

- タブレットの画面描画時に発生する電磁波
  - 電波を観測する計測器を用いて、電波を音に変換し聞いて頂きます

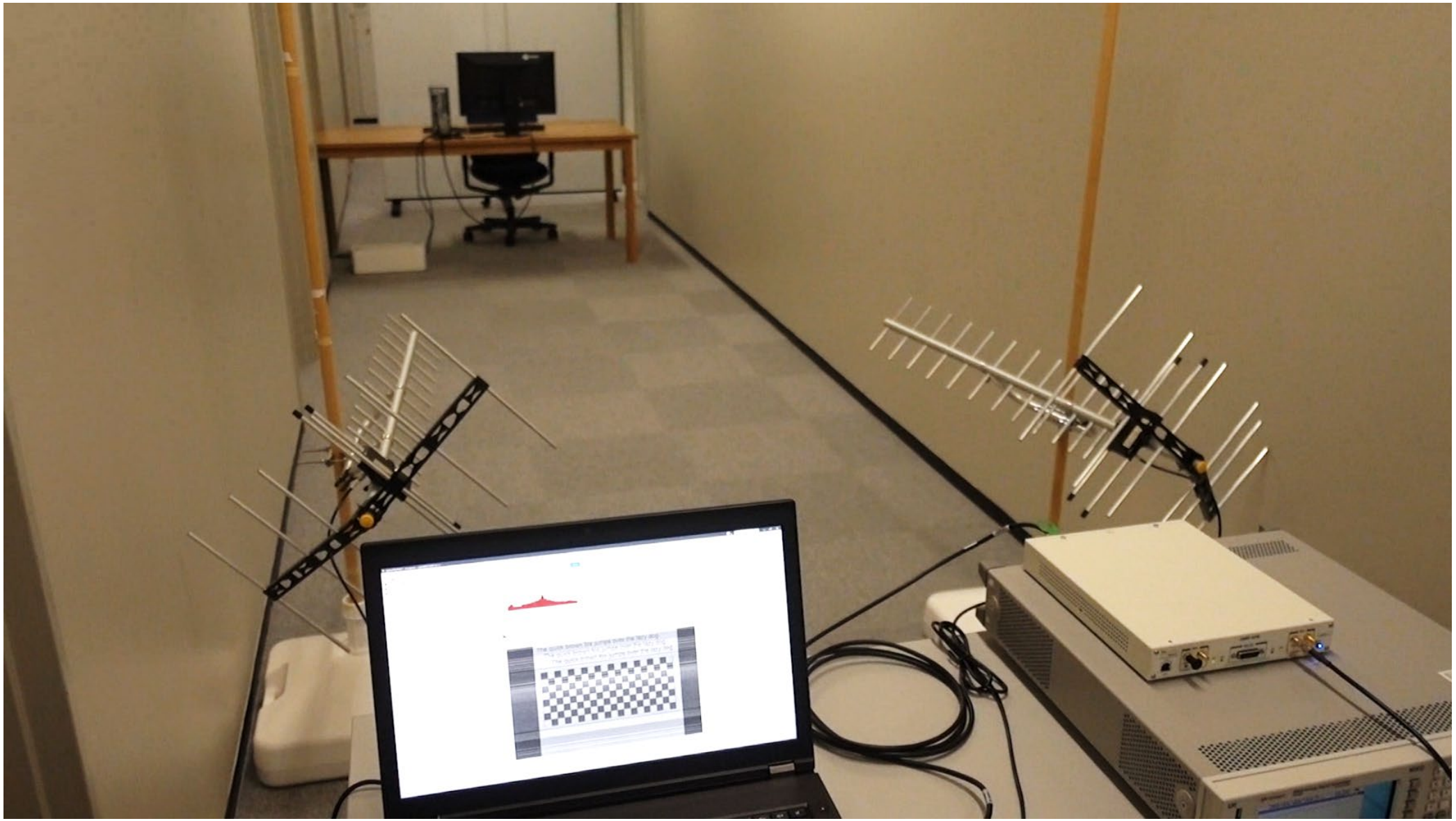


# 漏えい電磁波による情報漏えい

- キーボードの漏えい電磁波による情報漏えい



# 映像情報の復元例



# TEMPEST（テンペスト）

- 機器の動作に伴う電磁放射から、情報を盗聴する手法と対抗策
- 米国NSAとNATOのコードネーム
- 機密性の高い情報を扱う企業では、その対策が行われている

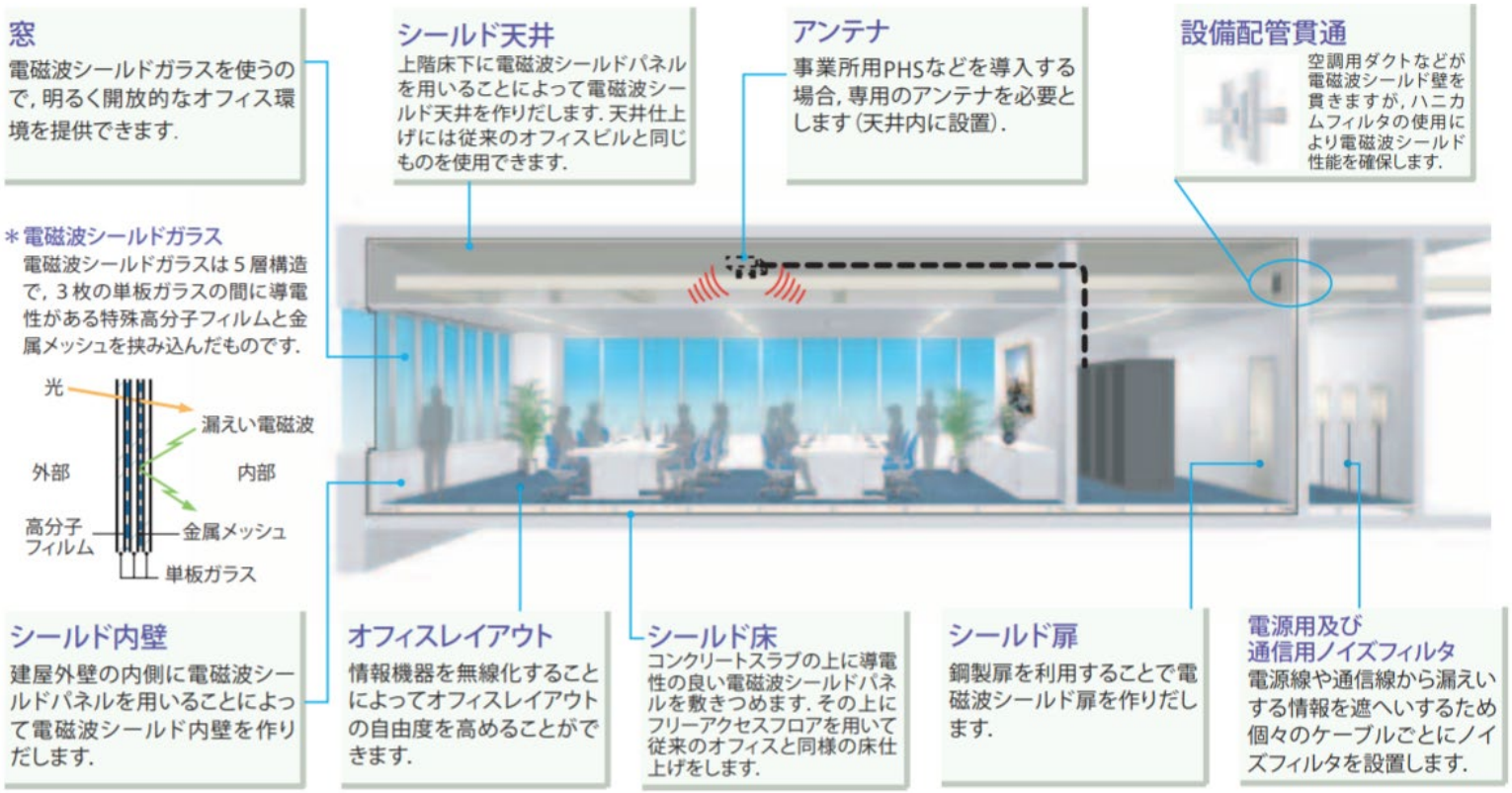



図５　情報セキュリティ対策を考慮したサイバービルの概念図

出典: https://www.jstage.jst.go.jp/article/bplus/2009/10/2009_10_10_28/_pdf/-char/ja

# IoTと電磁波

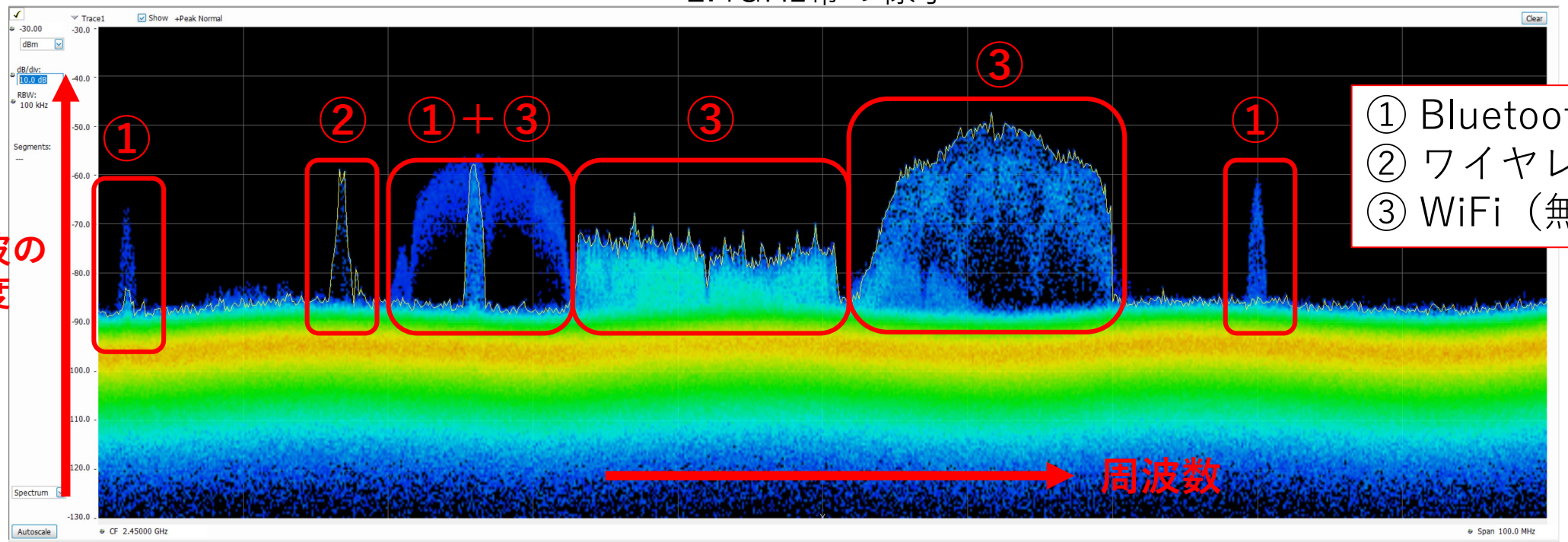
IoT機器とは、
- 機器同士が情報連携して協調動作
- 小型から大型機器まで
- スマートフォンやパソコンもその一部

IoT機器が用いる無線通信技術
- WiFi
- Bluetooth
- LPWA（Low Power, Wide Area（低電力広域））

# IoT無線のホームグラウンド 2.4 GHz 帯

- 2.4GHz帯はISM（産業・化学・医療）バンドの一つ
- 通信などに妨害を受けることを承知で使用する
- 電子レンジ、WiFi、Bluetooth、温熱治療器、マイク等など
- 使用する機器が多いので、電波のゴミだめとも呼ばれる（低可用性）

2.4GHz帯の様子



# 混雑度の低い5GHz帯

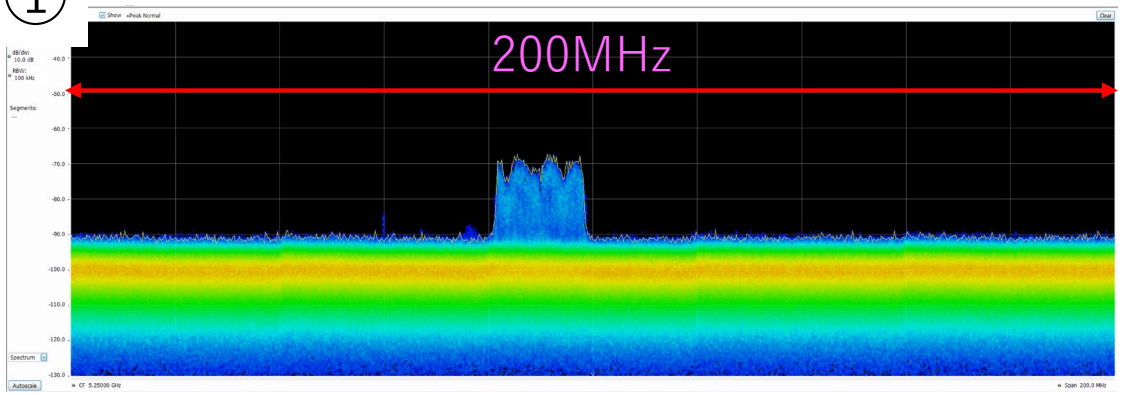
- WiFi（無線LAN）は2.4GHz帯以外に5GHz帯が利用できる
- 5GHz帯は、5.2GHz帯・5.3GHz帯・5.6GHz帯から構成される
- 気象・航空機レーダと周波数を共用しているため制限がある

| | チャネル | 帯域の名称 | DFS機能 | 屋外使用 |
|---|---|---|---|---|
| ① | 36, 40, 44, 48 | W52 | 不要 | 条件付き可※ |
| ① | 52, 56, 60, 64 | W53 | 必要 | 不可 |
| ② | 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144 | W56 | 必要 | 可 |

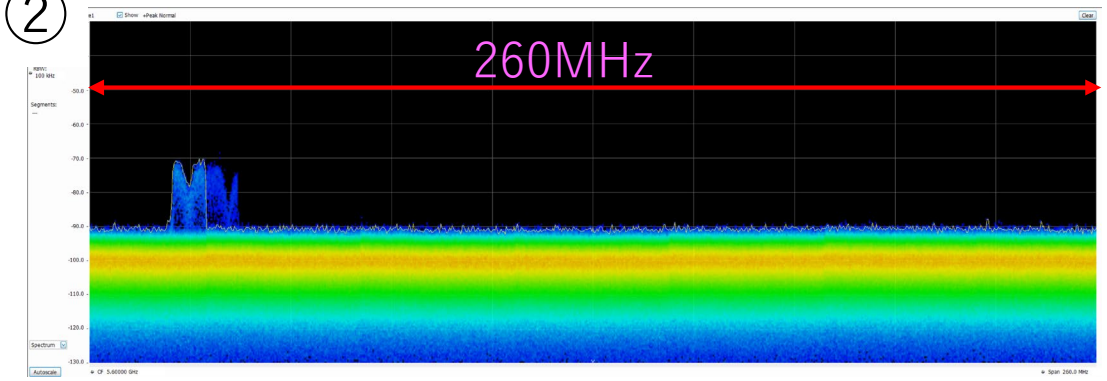
DFS機能とは、
周波数を共用しているレーダへの妨害を避けるため、レーダ波を検知すると電波の送信を停止し、他のチャネルへ移動する機能。

※専用の機器を用い、総務省総合通信局へ届出が必要

①




②



# 周波数帯と可用性

- 2.4GHz帯は混雑しており、混信して通信速度が低下しやすい
- 5GHz帯はチャネル数も多く、また電子レンジ等の大電力妨害波の発生もない。

WiFiアクセスポイント（AP）更新時の方針

- フロアごとに5GHz帯（802.11ac/ax）対応APを設置
  - 5GHz帯は壁（コンクリート等）を透過する際に、減衰が大きい。そのため、見通し範囲で使用するのが望ましい。
  - フロアが広い場合は複数台のAPを設置することが望ましい。ただし、チャネルの重複は厳禁。混信の元となる。

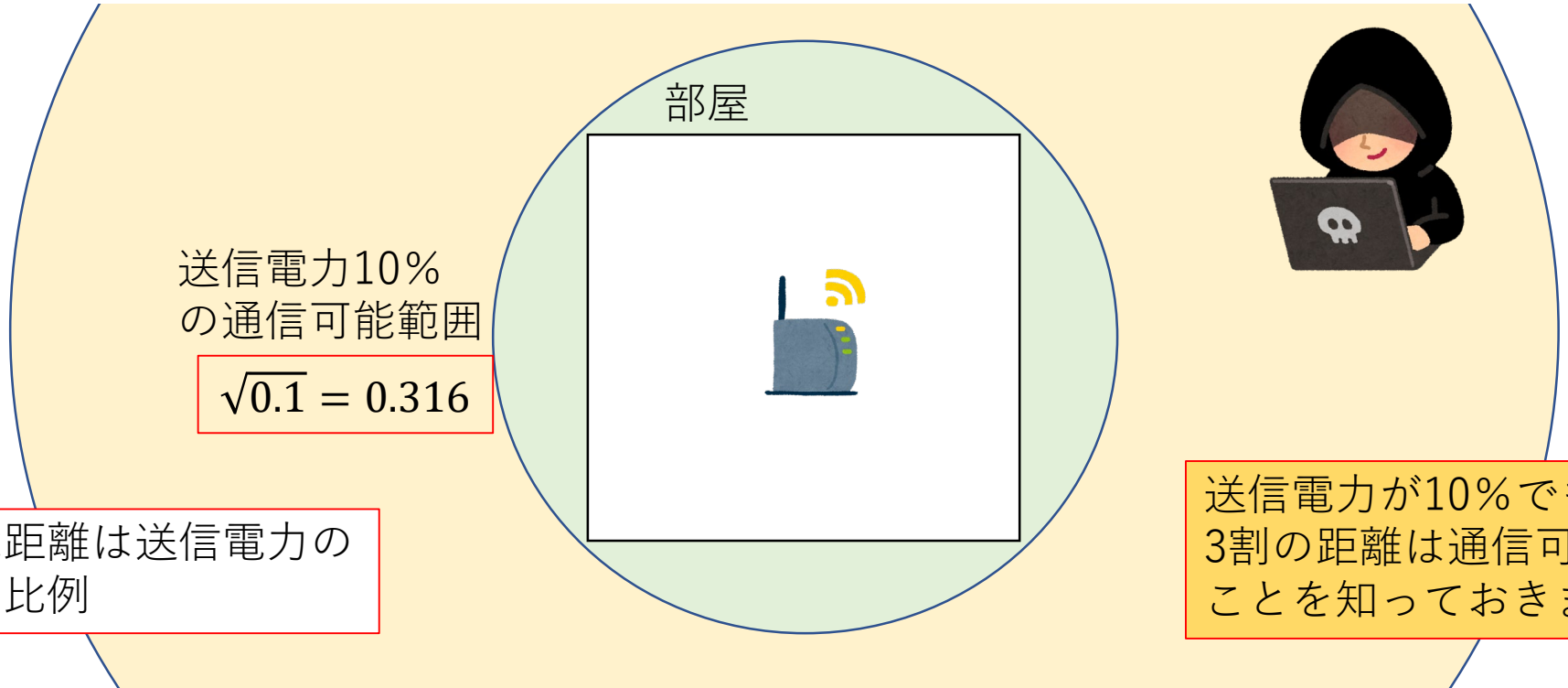
# WiFiの機密性と暗号処理

- WiFiの暗号処理は、
  - 攻撃手法が公知でもう使えない：WEP, WPA, 未アップデートWPA2
  - まだ安全に使える：アップデート済みWPA2, WPA3
- WiFiのAPもコンピュータで、ソフトウェアアップデートが必要
  - 情報セキュリティを低下させる脆弱性への対応パッチが、ベンダーから提供される。
  - APを設置して放置は禁止。社内LANへの侵入口となっているかもしれない。
  - しかし、APのソフトウェアアップデートは3〜5年で終わってしまう。
    - 技術革新が早く、製品寿命が短い
    - その割には、故障せず長年にわたって使用できてしまう。（脆弱性の温床）

WiFi APは生もの。メーカサポートの終了が消費期限。

# 電波の送信電力を考える

- APの設定項目には送信電力がある。
  - 製品出荷状態では100%と設定されている。
  - しかし、送信電力100%時の通信範囲（100m～）を考えると過剰
  - 攻撃者が屋外からアクセスすることを許すことにつながる。
  - 混信を招き、通信速度の低下も引き起こす可能性がある。



# ワイヤレスキーボードの機密性

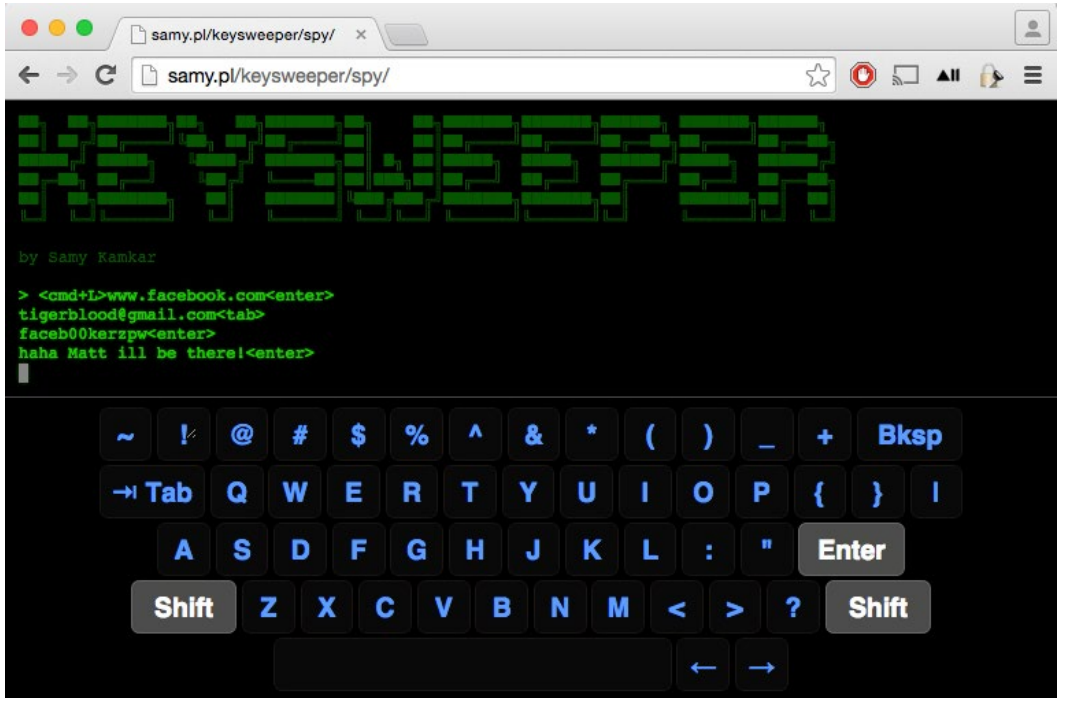
- ワイヤレスキーボードは入力キー情報を電波で送信している
- 暗号化されているか？

  →安価なワイヤレスキーボードはキー入力情報を暗号化していないことが多い。

キー入力情報を盗み見るための受信器兼中継器。

ネット上で設計図が公開されており、誰でも製作可能。

https://samy.pl/keysweeper/#key



# ワイヤレスキーボードは便利だけど危険

- キー入力情報は暗号化していても復元できる

1. キー入力のタイミング
2. キーボード内蔵のマイコンが暗号処理をする際の電磁放射

- 2は攻撃難易度が高いが、1は数万円の機材で攻撃が実行できる


[M-12353]　ＨａｃｋＲＦ　Ｏｎｅ　（ソフトウェア無線機）

**1台 ￥33,000**（税込）

出典：https://akizukidenshi.com/catalog/g/gM-12353/

# まとめ

- AI/BD/IoT時代を支えるのは無線通信
- 無線通信の情報セキュリティを高める必要がある
  - 機密性：情報窃盗防止や情報改ざんの防止
  - 完全性：通信の妨害を受けない・回避能力、情報改ざん防止
  - 可用性：常時利用可能な環境を維持する。周波数帯域確保や機器の保全。
- 安全性確保は電波の伝搬特性を応用することも有効
  - 不用意に強い電波を送信しない
- 無線通信には暗号化が必須
  - 無線機器の仕様書に、暗号方式が明記されているか確認