

修士論文

電磁波を通じたスマートデバイスからの音情報漏えい に関する研究

仁科 泉美

2019 年 03 月 14 日

奈良先端科学技術大学院大学
情報科学研究科

本論文は奈良先端科学技術大学院大学情報科学研究科に
修士(工学) 授与の要件として提出した修士論文である。

仁科 泉美

審査委員：

林 優一 教授 (主指導教員)

藤川 和利 教授 (副指導教員)

安本 慶一 教授 (副指導教員)

藤本 大介 助教 (副指導教員)

電磁波を通じたスマートデバイスからの音情報漏えい に関する研究*

仁科 泉美

内容梗概

機器から放射される電磁波を計測・解析し、暗号化されていない機器の入出力情報を取得する脅威が指摘されている。これまで消費電力の大きく比較的放射の大きい視覚的な情報に対して漏えいが多く検討されてきたが、機器で処理される比較的消費電力の小さな聴覚情報も取得可能であることが報告されている。こうした情報漏えいを抑止するためには、漏えい源を明らかにすることが有用であるが、これまでに十分な検討は行われてない。

そこで、本研究では、聴覚情報の漏えいを引き起こす主要な回路の特定を行うことを目的とし、漏えいに寄与する回路が実装された部位を絞り込むために、音声再生時及び停止時に放射される電磁界強度を測定し、測定結果と測定位置をマッピングして分布図を作成する。そして、音声再生時及び停止時の分布図を比較することで、漏えいの主たる要因となる回路を特定する。また、実験結果に基づき、漏えいを引き起こす回路からの電磁波を通じた音情報漏えいを抑止するための対策手法についても議論する。

キーワード

電磁情報セキュリティ, スマートデバイス, 音情報, 電磁界計測

*奈良先端科学技術大学院大学 情報科学研究科 修士論文, 2019年03月14日.

Study on sound information leakage through EM radiation from smart devices*

Izumi Nishina

Abstract

It is possible to obtain unencrypted input/output information of devices, by measuring and analyzing electromagnetic (EM) emanation from devices that meet EM compatibility (EMC) standards. At present, most EM information leakage is visual information from comparatively strong EM radiation; however, sound information can also be obtain from comparatively weak EM radiation. To suppress sound information leakage through EM emanation, it is useful to identify the electrical components that leak sound information; however, there has not been enough discussion about this topic. In this research, I identify the main component that causes sound information leakage. I measure the EM field, including the sound information radiated from the components of devices, and create cartography relating to the intensity of the radiated EM field. Thus, I am able to identify the part causing information leakage. Finally, I verify the leakage source by extracting the component and measuring EM waves emanating from it. In this experiment, I measured the EM field against each part of sound playing components of a smartphone, and verified the leakage via the component.

Keywords:

EM information security, Smart devices, Sound information, EM field measurement

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 14, 2019.

目次

1. 序論	1
1.1 研究の背景	1
1.2 研究目的	4
1.3 本論文の構成	5
2. 電磁波を通じた音情報漏えい源の特定手法	6
2.1 音情報を有する漏えい周波数の探索	6
2.2 電磁波を通じた音情報漏えい源の推定	8
3. 電磁波を通じた音情報漏えい源の特定	10
3.1 実験環境	10
3.2 実験結果	11
3.2.1 音情報を含む漏えい周波数の探索	11
3.2.2 Cartography を用いた漏えい源の絞り込み	14
3.2.3 漏えい源となる素子の推定	15
3.2.4 素子単体での音情報漏えい検証	16
3.3 スマートデバイスからの電磁波による音情報漏えい抑止策の提案	19
4. 結論	21
謝辞	22
参考文献	23

図 目 次

1.1	機器からの漏えい信号を受信するシステム	3
2.1	機器動作時の放射電磁波のスペクトルの例	6
2.2	電磁波を通じた音情報取得のイメージ	7
2.3	提案する音情報の漏えい源探索手法の概念図	8
3.1	Cartography 作成の実験セットアップ	10
3.2	放射されるスペクトルの一部	12
3.3	漏えい周波数 (28MHz) での音情報のスペクトル	13
3.4	Cartography 作成結果の一部	14
3.5	負荷抵抗値の異なる端子	15
3.6	D 級アンプ単体からの音情報漏えいを検証する実験セットアップ .	17
3.7	漏えい信号の時間領域波形	18
3.8	漏えい信号に含まれる周波数成分	18

1. 序論

1.1 研究の背景

情報通信機器から非意図的に放射される電磁波が、他の機器へ電磁干渉を与えることが知られている。こうした機器の電磁干渉を抑制するため、日本の VCCI 規格やアメリカ合衆国の FCC 規格といった電磁環境適合性（EMC: Electromagnetic Compatibility）の規格が定められており、これらの規格を満たした機器が現在流通している。しかし、これらの EMC 規格は、機器からの放射電磁波による他の機器への電磁干渉を抑制することを目的とした規格であり、機器からの放射電磁波に重畳する情報の漏えいを抑制することを目的とした規格ではない。そのため、EMC 規格の規制値を満たした機器に対して、放射電磁波を用いた情報の取得が可能であることが指摘されている [1]。

機器からの放射電磁波を用いた情報漏えいは、ターゲットとなる機器の放射電磁波を受信し、得られた信号に統計処理や信号処理を施してターゲットの情報を再構築することにより放射電磁波に重畳した所望の情報を取得する。こうした情報漏えいは、ターゲットの機器に改変を加える必要のないパッシブな手法に分類され、攻撃の痕跡が残りにくい手法である。従来、ターゲット機器からの放射電磁波を受信するには高価かつ一般には入手困難な機材を使用する大掛かりなセットアップが必要であることから、外交や軍事といった一部の最重要分野に対する脅威であると考えられてきた。しかし、Wim van Eck らの実験により、安価な機材で短時間に CRT 端末からの情報取得及び解読が可能であることが示され [2]、最重要分野から一般的なセキュリティへと脅威の範囲が拡大した。近年では、計算機資源の高速化と記憶装置の大容量化によりソフトウェア無線や信号処理のリアルタイムな適用が可能となっており、より安価かつ小型なセットアップを用いた情報取得が可能となった [3]。これまで放射電磁波による情報漏えいの対象には、PC やモニタの画面情報 [4, 5]、プリンタの印字情報 [6, 7]、キーボードの入力キー情報 [3, 8]、暗号モジュール内の秘密鍵情報といった多岐に渡る機器が取り上げられてきた。また、可搬性を有するセットアップを用いた場合にもタブレット端末からの放射電磁波を用いた表示画面の再構築が可能であることが示さ

れた [9]。こうしたセットアップの軽量・小型化により、放射電磁波を用いた情報漏えいの脅威は、可搬性を有する個人所有レベルの機器まで拡大している。

機器に入出力される情報のうち、機器から人間が情報を受け取る最終的な経路では、暗号化されていない情報のやりとりが行われる。機器からの放射電磁波による情報漏えいの指摘が多い視覚情報では、機密情報を含んだ文書や Web サービスへのログインに用いられる ID・パスワードが入出力されることから、その盗聴リスクの検討が行われてきた。

一方で、通話による音声コミュニケーションを通じて機密情報や個人情報が機器に入出力されるが、こうした聴覚を通じて認識される情報、すなわち音情報についてはその漏えいは十分検討されてこなかった。この要因の一つとして、機器で再生される音情報は、機器に表示される画面のような視覚情報に比べて情報処理時の消費電力が小さいことが挙げられる。給電されない状態で利用する携帯電話やタブレットなどの可搬性を有する機器は消費電力を抑えるよう設計されており、そうした機器では音情報の処理時に発生する消費電力はより低いと考えられる。従って、音情報の処理時に機器から放射される電磁界の強度も小さく、音情報は周辺環境の電磁界に埋もれやすい情報であった。

しかし、近年の研究において、マイクロホン付きイヤホンケーブルが接続されたスマートデバイスを対象に、機器で再生した音情報の電磁波を介した漏えいの可能性が検討され、イヤホンケーブル近傍の放射電磁波を測定及び解析することにより重畳した音情報を取得可能であることが実験的に示された [10]。近傍界から音情報を取得可能であることから、ターゲットとなる機器の回路構成や攻撃側の受信システムにより音情報を伝搬する周波数（以降、漏えい周波数）における漏えい信号の強度が変化し、遠方まで伝搬する可能性がある。例えば、機器からの電磁波放射はディファレンシャルモード放射とコモンモード放射に分類される。ディファレンシャルモード放射は、通常の機器動作により生じる放射で、微小ループアンテナとしてモデル化される。一方、コモンモード放射は、回路の寄生要素により生じ、ダイポールまたはモノポールのアンテナとしてモデル化される。そのため、機器に構成されたアンテナ部に流れる電流値が等しい場合、コモンモード放射がより大きな電界強度を有することが知られている [11]。また、基板サイ

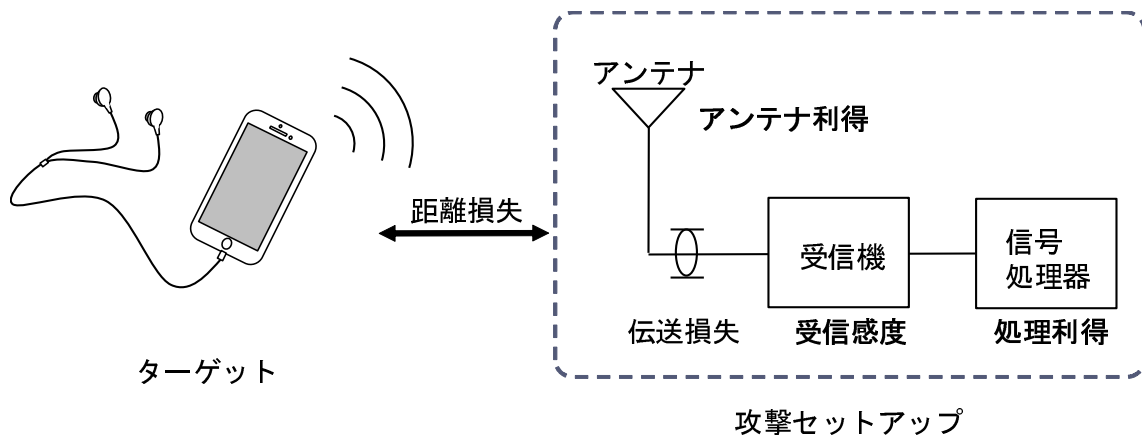


図 1.1 機器からの漏えい信号を受信するシステム

ズや機器に接続されるケーブルの長さといった機器の実装構造が漏えい信号の振幅値に影響を与えることが報告されており [12]、回路設計者や機器利用者が非意図的に情報漏えいしやすい環境を作り出す可能性がある。図 1.1 に示す攻撃者の受信システムにおいても、漏えい周波数付近で高利得なアンテナや広帯域な受信機の利用、信号処理による処理利得の改善により、音情報が取得可能な距離限界の延長が見込まれる [13]。対象とするスマートフォンやタブレットなどのスマートデバイスは、アプリケーションを介した音声コミュニケーションを通じて時間や場所を問わず複数人での通話が可能である。機器から放射される電磁波の観測により通話内容が漏えいした場合、プライバシー侵害や価値ある情報の流出につながる恐れがある。

機器から非意図的に引き起こされる放射は、Source-Path-Antenna モデルとして表される [14]。これは、データやクロックのような機器の動作に必要な信号 (Source) が、伝搬経路 (Path) を通じて非意図的に構成されるアンテナ (Antenna) へ伝搬されることにより機器外部へ放射されるというモデルである。このモデルより、機器からの電磁波を通じた情報漏えいを抑制するために、漏えい周波数において Source を生じる信号源 (以降、漏えい源) や伝搬経路といった要素の特定が行われてきた。これまで、フラットパネルディスプレイに表示した画面情報はディスプレイに接続されたフラットケーブル中のデジタル信号に含まれる

ことや [5,9]、暗号モジュール内の秘密鍵情報は論理ゲートを構成する CMOS 回路の動作により生じる過渡電流に含まれること [15] が示されており、漏えい源は対象とする情報の処理により異なることがわかる。つまり、電磁波を介した情報漏えいを抑止するには、対象となる情報ごとに漏えい源を特定する必要がある。一方で、既存研究では、スマートフォンで再生される音情報の漏えいに関して、漏えい周波数において音情報を再構築できるか否かを判断基準とした情報漏えいの有無を判断する評価が行われているが、その漏えい源に対する検討は十分なされていない。

1.2 研究目的

前節で述べた背景を踏まえ、本研究では、スマートデバイスからの電磁波を介した音情報の漏えい抑止に必要となる基礎知見を与えるため、音情報の漏えい源となる素子の特定を目的とする。一般的なスマートデバイスにおける音声再生に関連するデバイスの構成部品は、デジタル信号をアナログ信号へ変換する DAC、アナログ信号を増幅するオーディオアンプ、アナログ信号を音声に変換するイヤホンが考えられ [16–18]、これらの構成部品が漏えい源となっている可能性が高い。これらを対象に、基板レベルでの対策を施すべき箇所を特定する手法の一つである電磁界強度分布の作成を行う。音情報再生時のデバイス近傍における電磁界強度の分布図と非再生時の分布図を用いて電磁界強度の大きさを比較することにより、音情報の処理により電流の流れが大きく変化する位置が可視化される。このとき、上述の素子が実装された位置と放射電磁界強度の変化が大きい位置とを比較することにより、漏えい抑止策を施すべき素子を特定できる可能性がある。

そこで、本論文では、音情報の再生による放射電磁界強度の変化に着目し、スマートデバイスで再生した音情報の電磁的漏えいを引き起こす主要な回路を明らかにする。

1.3 本論文の構成

本論文の構成は以下の通りである。

第2章では、スマートデバイスからの電磁波を介した音情報漏えいを引き起こす漏えい源を特定する手法を提案する。音情報を機器外部へ伝搬する漏えい周波数において、音情報の処理による放射電磁界強度の分布を比較することで、漏えい源となる素子を検討する。

第3章では、第2章で提案した手法を用いて、音声再生に関連するデバイス部位が本体から分離したスマートフォンを対象に放射電磁界強度の分布図を作成し、再生した音情報が漏えいする要因となるデバイスの部位を特定する。特定した箇所に実装された素子と同様の素子のみを駆動させた場合にも音情報が漏えいすることを示す。

第4章では、本論文のまとめを行う。

2. 電磁波を通じた音情報漏えい源の特定手法

第2章では、漏えい周波数において、音情報の処理による放射電磁界強度の分布図を比較することで、機器で再生した音情報漏えいにおける漏えい源を絞り込む手法を提案する。提案手法では、まず、機器で再生した音情報を含む漏えい周波数を特定し、その漏えい周波数に着目して放射電磁界強度の分布図を作成する。続いて、強い放射が観測された範囲に含まれる素子に対して漏えい評価を行う。

2.1 音情報を有する漏えい周波数の探索

機器から放射される電磁波は、図 2.1 に示すように広帯域な周波数で生じているが、この全ての周波数に音情報が重畳しているのではなく、ある一部の周波数に音情報が重畳している。従って、音情報の漏えいに関する電磁界強度の変化を分布図として可視化するには、音情報が含まれる周波数に着目した測定を行う必要がある。

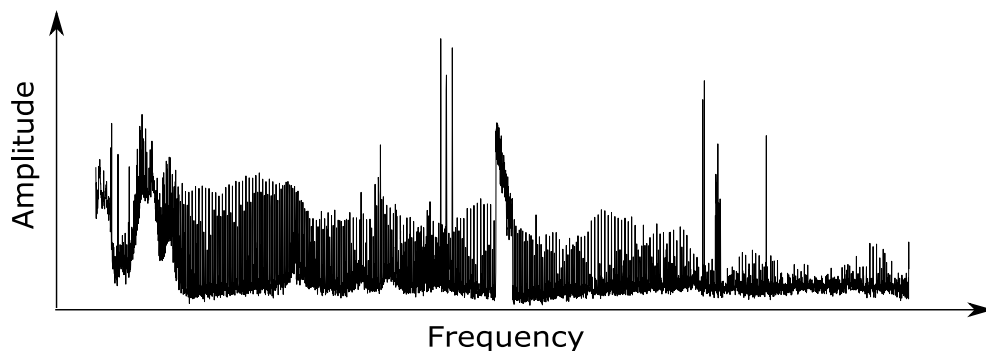


図 2.1 機器動作時の放射電磁波のスペクトルの例

機器で再生した音情報は AM 変調され機器外部へ放射される [10] ため、図 2.2 に示すように、観測する周波数帯のうち音情報を含む周波数に着目して AM 復調することにより機器で再生した音情報の再構築が可能となる。従って、観測周波数帯の範囲において一定の間隔で受信周波数を変化させながら AM 復調し、機器で再生した音と同様の音を人の耳で認識可能か否かを判断基準とした手法を用いて、漏えい周波数をくまなく探索していた [19]。また、スマートフォンからの

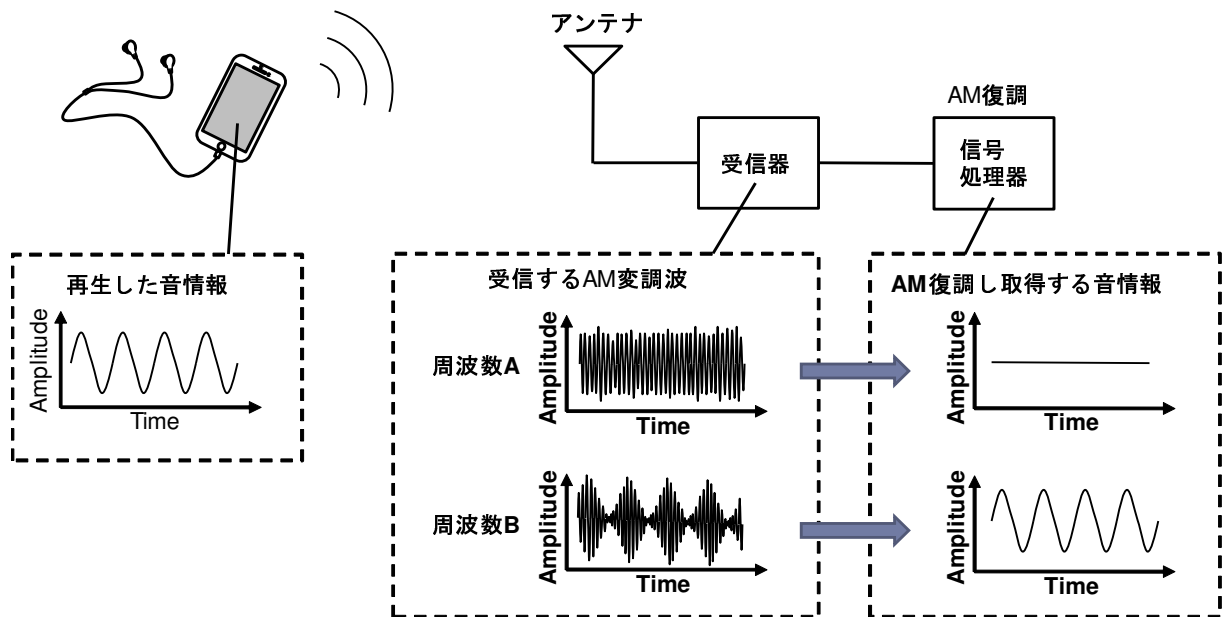


図 2.2 電磁波を通じた音情報取得のイメージ

放射電磁波から音情報漏えいの有無を評価した研究では、機器に挿入されたイヤホンケーブル近傍の放射電磁界強度を測定し、漏えい信号のスペクトルの振幅変化が大きい周波数の範囲を特定した後、その範囲に含まれる周波数に着目し AM 復調した信号を録音する。録音された信号から再生した信号と同一周期の信号が観測されることを判断基準として漏えい周波数を特定している [10]。音情報の再生によりスペクトルの振幅が大きく変化する周波数は、音情報処理により生じた変化が大きい周波数であると考えられるが、信号対雑音比 (SNR : signal-to-noise ratio) が低く所望の信号が背景雑音以下の信号レベルとなる場合があるため、漏えい周波数の特定は情報の再構築の可否により評価される。さらに、機器で再生する音情報が周期性を有する場合には、AM 復調した時間領域波形に所望の周期性や周波数成分が含まれるか否かを判断基準とした漏えい周波数の推定が可能である [20]。本研究では、機器に挿入されたイヤホンケーブル近傍の放射電磁界強度を測定し、漏えい信号のスペクトルの振幅変化が大きい周波数範囲を対象に AM 復調による信号の再構築が可能か否かを判断基準とした漏えい周波数の特定を行う。

2.2 電磁波を通じた音情報漏えい源の推定

特定した漏えい周波数において、強度分布を観測するために、放射電磁界強度の分布図である Cartography を作成する。回路の動作に伴い発生する電流変化が磁界を生み、磁界の変化が電界を発生させる。従って、機器上にサンプル点を設け、各サンプル点における放射の強さを測定し分布図にすることにより、所望する情報の処理により電磁界強度が変化する部位を可視化することができる [21, 22]。こうした Cartography の作成は、タブレット端末表面からの電磁波を介した描画情報や暗号デバイスからサイドチャネル情報の漏えい源の特定に用いられており [9, 23]、音情報の漏えい源探索においても有効な手法であると考えられる。具

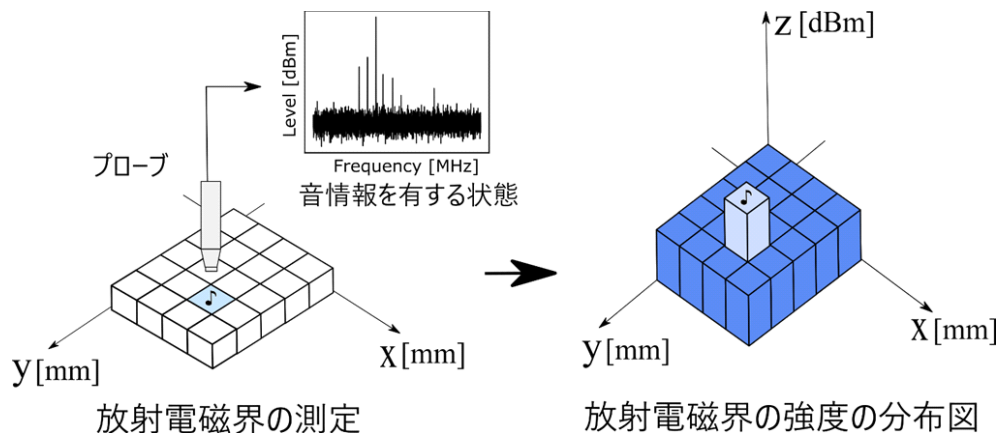


図 2.3 提案する音情報の漏えい源探索手法の概念図

体的には、図 2.3 に示すように評価対象となる領域に設けたサンプル点の近傍界を磁界プローブにより測定する。その後、プローブを水平方向及び垂直方向に走査し、各サンプル点とその測定結果をマッピングすることでスマートフォンから放射される電磁界強度を Cartography として可視化し、放射電磁界強度が大きい部位を確認する。本手法では、機器で音情報を再生していない状態と再生した状態の双方で分布図を作成する。双方の分布図を比較し、その値の差が大きくなる範囲では音情報の処理による変化が大きいと考えられ、該当する部位に漏えい源となる素子が含まれている可能性がある。そのため本手法では、放射強度の差が最大となる部位に主要な漏えい源となる素子が含まれるという考えに基づき、漏

えい源の範囲を絞り込む。

近年は素子の集積化が進んでいることから、複数の素子が1チップ化している状況が考えられる。本研究で対象とする素子では、DACとオーディオアンプの1チップ化が想定される[24,25]。電磁波を介した情報漏えいを抑止するには漏えい源となる素子の把握が求められるため、絞り込んだ範囲における更なる切り分けが必要となる場合がある。そこで、評価者はイヤホンから出力される信号の電圧値及びイヤホン部の負荷抵抗値の操作が可能である点に着目し、電氣的な負荷条件の変更による放射電磁界強度の変化を観測する。オームの法則から、回路に流れる電流の値は、電圧値が一定である場合には負荷抵抗の値により変化する。従って、デバイスで再生する情報の最大振幅値が一定のとき、イヤホンジャックへ接続する負荷抵抗値を変化させることにより、オーディオアンプに流れる電流を制御できる。つまり、負荷抵抗の値が小さい場合に放射電磁界強度が増大する場合には漏えい源はオーディオアンプであり、変化しない場合には漏えい源はDACであると考えられる。

以上により特定した素子が漏えい源であることを評価するため、特定した範囲に実装される電子素子を抽出し、素子単体を動作させた場合に信号の漏えいが発生するか検証する。

3. 電磁波を通じた音情報漏えい源の特定

第3章では、第2章で提案した手法を用いて、音声再生に関連するデバイス部位が本体から分離したスマートフォンを対象に放射電磁界強度の分布図を作成し、再生した音情報が漏えいする要因となるデバイスの部位を特定する。そして、特定した部位に実装された素子と同様の素子のみを駆動させた場合にも音情報が漏えいすることを示す。

3.1 実験環境

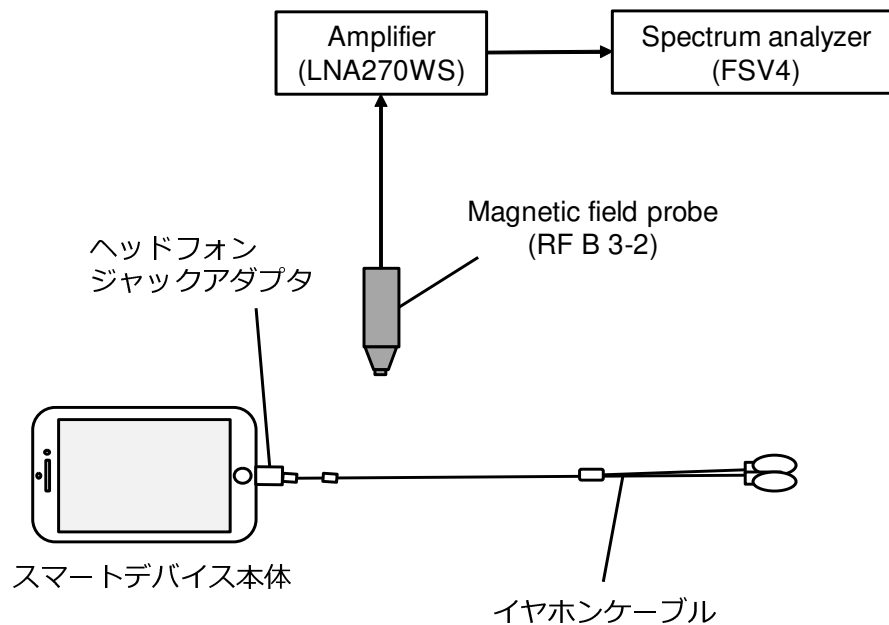


図 3.1 Cartography 作成の実験セットアップ

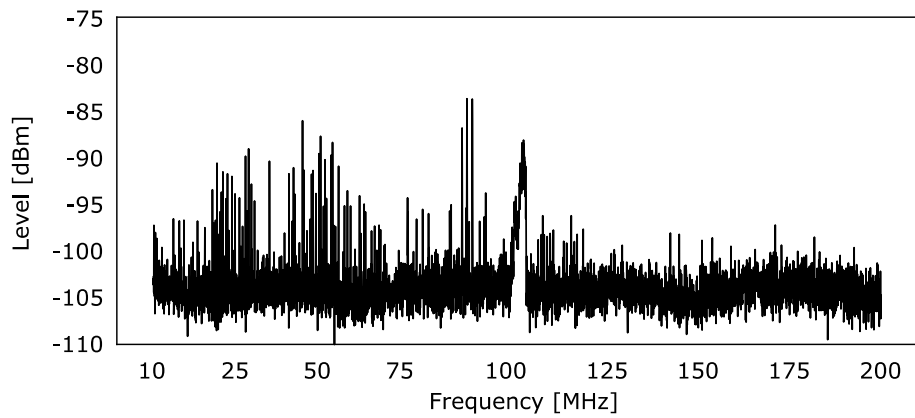
図3.1に本実験のセットアップを示す。一般に、スマートデバイスの音情報再生に関連するデバイス部位は DAC、オーディオアンプやイヤホンが考えられる。従来、基板レベルで放射電磁界の分布図を作成するには機器を開封した状態で近傍界を測定していたが、開封検知が実装された機器では通常の動作をしない恐れがある。そのため、本実験では計測を容易にするために DAC 及びオーディオアンプ

がスマートデバイス本体とイヤホンから分離しているスマートデバイス (iPhone7) を対象とする。対象としたスマートデバイスでは、DAC 及びオーディオアンプがヘッドフォンジャックアダプタに内蔵されている [26]。そこで、スマートデバイス本体、ヘッドフォンジャックアダプタ (機器接続時、約 74 mm) 及びマイクロホン付きイヤホンケーブル (機器接続時、約 1175 mm) の 3 つの領域に分けて評価を行う。実験では、各領域表面に磁界プローブ (LANGER RF-B 3-2) を当て、音情報を含む放射電磁界を近傍界として計測した。計測した放射電磁界のスペクトルは、信号増幅器 (COSMOWAVE LNA270WS) で増幅し、その出力を AM 復調機能付きスペクトルアナライザ (Rohde&Schwarz FSV) に接続し観測する。また、スマートデバイスで再生する音情報は 10 kHz の正弦波を用いた。

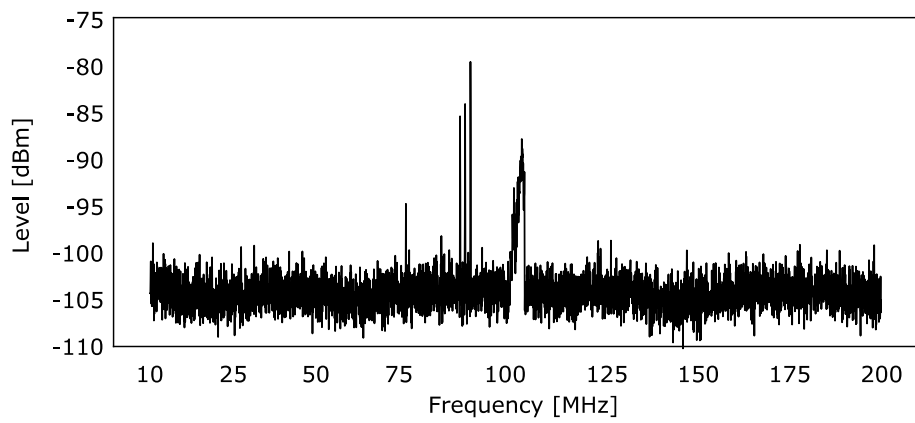
3.2 実験結果

3.2.1 音情報を含む漏えい周波数の探索

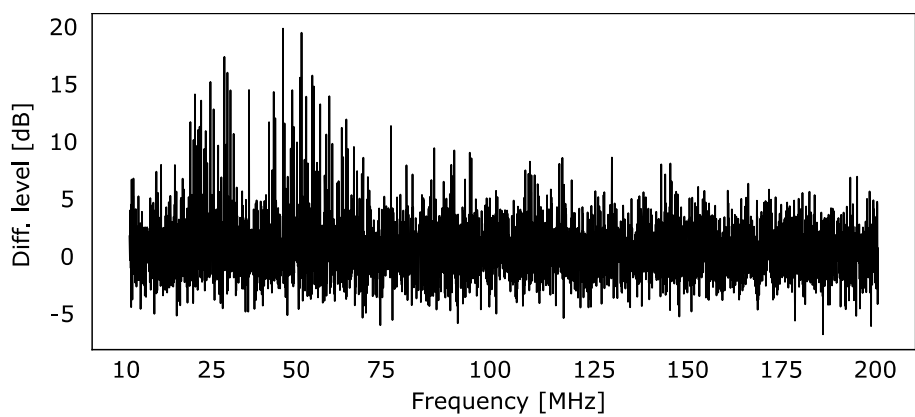
10 MHz から 1 GHz までの周波数帯に着目して音情報を再生した状態と再生していない状態の放射電磁界を測定し、音情報を有する周波数帯を探索した。その結果、音情報を再生した状態と再生しない状態でのスペクトルの振幅差が特に大きかったのは、10 MHz から 200 MHz までの範囲であった。観測されたスペクトルを図 3.2 に示す。図 3.2(a) は情報を再生した状態のスペクトルである。図 3.2(b) は情報を再生していない状態のスペクトルであり、背景雑音に相当する。図 3.2(a) と (b) の各周波数における振幅差を図 3.2(c) に示す。機器で信号を再生した場合に最大で 19 dB 程度振幅の増大が観測された。AM 復調により機器で再生した情報を認識できた 28MHz において、分解能帯域幅 20 Hz、スパン周波数 100 kHz としてスペクトルを観測した結果を図 3.3 に示す。図 3.3(a) は音情報を再生した状態で測定を行った結果であり、図 3.3(b) は音情報を再生していない状態での測定結果である。28.128 MHz から 28.228MHz の間では、音情報を再生した状態にのみ現れるスペクトルが複数存在する。これらのスペクトルは、再生した信号の周波数である 10 kHz と同様の周波数間隔をもつことから側帯波であると考えられる。つまり、これらの周波数帯は音情報を漏えいさせる周波数を含



(a) 音情報あり

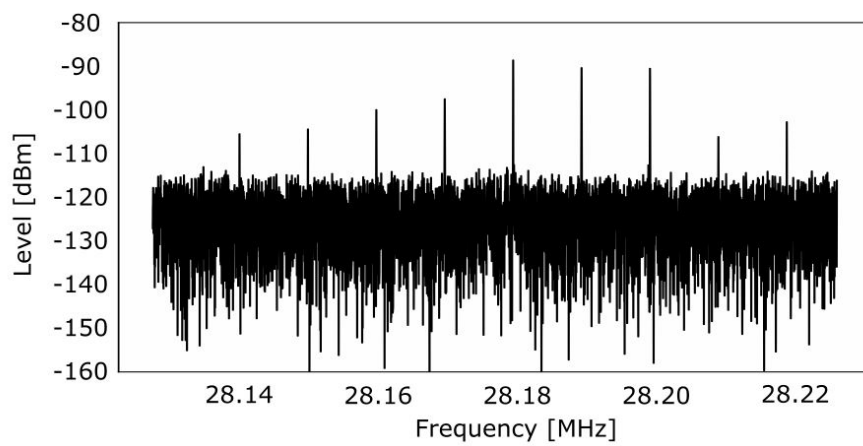


(b) 音情報なし

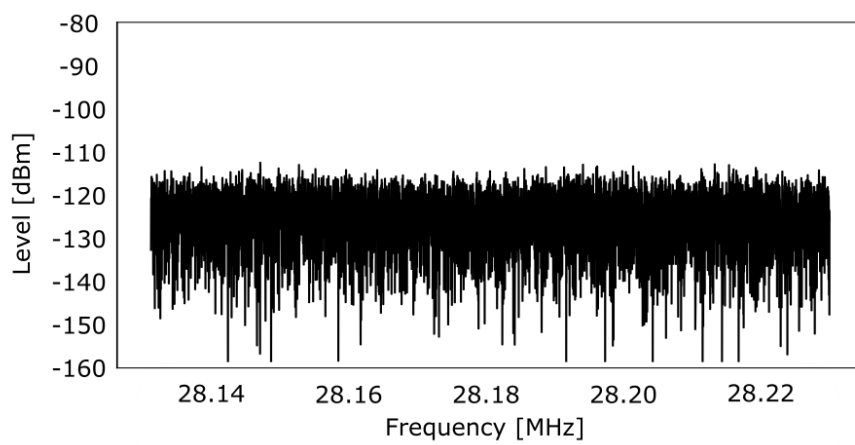


(c) スペクトルの振幅差

図 3.2 放射されるスペクトルの一部



(a) 音情報あり



(b) 音情報なし

図 3.3 漏えい周波数 (28MHz) での音情報のスペクトル

むと考えられる。そのため、図 3.3 に示す観測周波数帯において放射電磁界強度を計測し、Cartography を作成することで漏えい源の含まれる範囲を絞り込むことが可能であると考えられる。

3.2.2 Cartography を用いた漏えい源の絞り込み

続いて、先に示した観測周波数帯において、Cartography を作成する。放射電磁界の大きさは、スペクトルアナライザの Band Power 機能を利用し、観測周波数帯に現れる音情報に起因するスペクトルの電力を測定することにより観測する。

デバイス本体の画面表面においては、音情報に起因するスペクトルを観測することができなかった。マイクロホン付きイヤホンケーブルでは、イヤホンジャックから遠ざかるにつれ放射電磁界強度の減衰が観測され、最大振幅差は 3.98 dB であった。ヘッドフォンジャックアダプタでは図 3.4 に示す強度の分布がみられ、最大振幅差は図 3.4(a) に示す測定位置 11 において 8.92 dB であった。

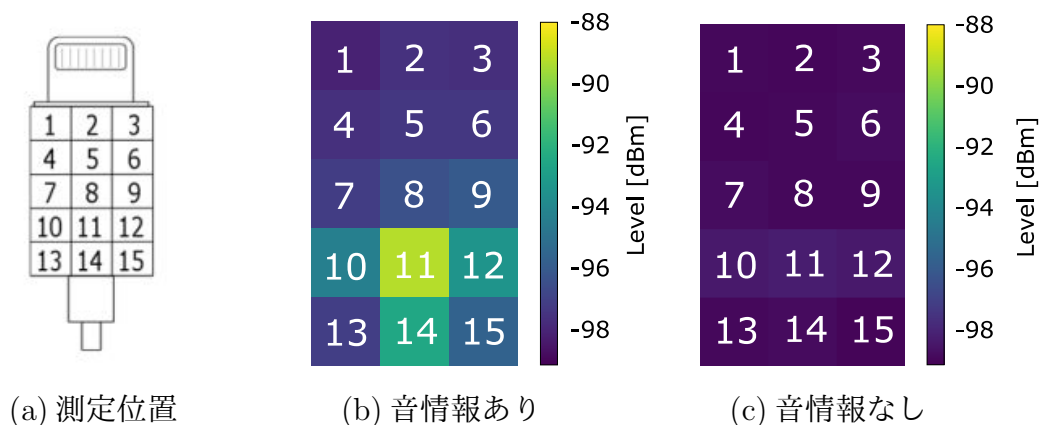


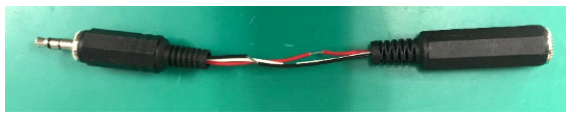
図 3.4 Cartography 作成結果の一部

以上の結果より、音情報の漏えい源は音情報の再生に起因した放射電磁界の強度が最も大きかった変換ヘッドフォンジャックアダプタ内部の IC である可能性が高いと考えられる。この IC には DAC とオーディオアンプが混載されているため、漏えい源となる素子を特定するためには Cartography により得られた電磁界分布による漏えい源となる素子の推定が必要となる。

3.2.3 漏えい源となる素子の推定

図 3.4(b) より、放射電磁界が大きい部位は音情報の入力部分よりも出力部分に近いことがわかる。音情報の再生は、デバイス本体から出力されたデジタル信号が DAC によりアナログ信号へ変換されたのちオーディオアンプで増幅され出力されることから、オーディオアンプが漏えい源であると予想される。

そこで、オーディオアンプの動作のみを変える実験を行うことで漏えい源を特定する。イヤホンから出力される音声の最大電圧振幅値が一定である場合、抵抗値の小さい端子をイヤホンジャックに接続した状態ではオーディオアンプはより大きな電流駆動力を必要とする。そのため、出力端子の抵抗値を変化させた場合、放射電磁波の強度が著しく変わる場合はオーディオアンプが漏えい源と特定できる。そこで上述の漏えい源特定のために、抵抗値の異なるオス型イヤホンジャック



(a) オープンな端子



(b) 15 Ω 抵抗付き端子

図 3.5 負荷抵抗値の異なる端子

クを 2 組用意し、オーディオアンプに流れる電流を変更した場合の放射電磁界を測定した。具体的には、負荷抵抗値の大きな端子として図 3.5(a) に示すオス型イヤホンジャックの各ピンとメス型イヤホンジャックの対応するピンをケーブルで接続し抵抗を設けていない端子（オープンな端子）を用意し、負荷抵抗値の小さな端子として図 3.5(b) に示すオス型イヤホンジャックの左チャンネルと接地及び右チャンネルと接地の双方に 15 Ω の抵抗をつけた端子（15 Ω 抵抗付き端子）を用意した。各端子をヘッドフォンジャックアダプタに挿入すると、デバイス本体の音声出力先はヘッドフォン出力を選択したことから、音情報はデバイス本体のスピーカではなくイヤホンジャックから出力されると考えられる。オーディオアンプに流れる電流がより大きい場合、オーディオアンプに起因する放射電磁界の大きさも増大することが予想される。先の実験により、音情報を再生した状態の電磁放射が最も大きい箇所である図 3.4(a) に示す測定位置 11 に磁界プローブを

当て測定した。

その結果を表 3.1 に示す。オープンな端子を接続した状態では音情報の処理によるスペクトルが観測されなかった一方、抵抗付き端子を接続した状態では音情報の処理によるスペクトルが観測された。負荷抵抗値の小さい端子を接続することにより、放射電磁界の大きさが増大していることがわかる。つまり、抵抗値の小さな端子を接続し電流値がより大きくなった場合、測定位置 11 における放射電磁界の大きさも増大することが明らかとなった。

表 3.1 測定位置 11 での放射電磁界の大きさ

場合	放射電磁界の強度 [dBm]		差 [dB]
	音情報あり	音情報なし	
オープンな端子	-97.20	-97.48	0.28
抵抗付き端子	-93.16	-97.22	4.06

以上のことから、音情報の漏えいを引き起こしている部位はオーディオアンプであると推察される。そのため、オーディオアンプより前段で行われる非圧縮の WAVE 形式や圧縮非可逆の MP3 形式といった音声再生のコーデックの違いが与える漏えい信号への影響は小さいと考えられる。

3.2.4 素子単体での音情報漏えい検証

続いて、オーディオアンプが音情報の漏えい源であることを確認するために、オーディオアンプ単体から放射される電磁波を解析することにより音情報の有無を確認した。スマートデバイスでは、電力効率を高めるため、オーディオアンプにはパルス幅変調（PWM: Pulse Width Modulation）を用いた D 級アンプが実装され、今回ターゲットとしたスマートデバイスにおいても D 級アンプが用いられていると考えられる [18, 26–28]。そこで、本実験では単体のオーディオアンプとして D 級アンプを選定する。本実験では、MAXIM 社の MAX9744 が実装された 20 W ステレオデジタルアンプボード PS-3246 を用いて PWM 信号の生成による電磁界を介した音情報の漏えいを検証する。

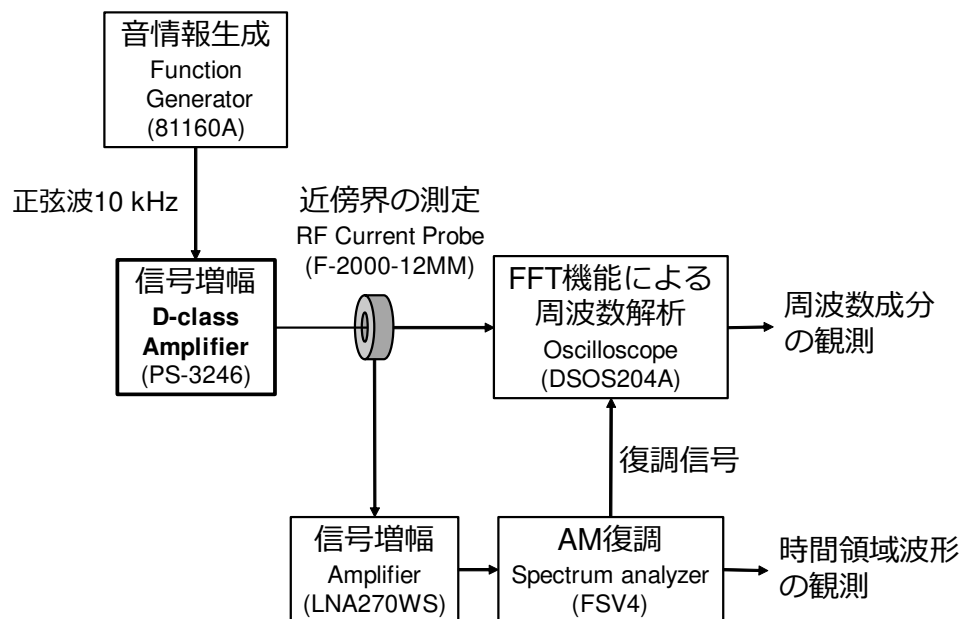


図 3.6 D 級アンプ単体からの音情報漏えいを検証する実験セットアップ

図 3.6 に本実験のセットアップを示す。本実験では、実デバイスで用いられる DAC の代用としてファンクションジェネレータ (KEYSIGHT 81160A) を使用し 10 kHz の正弦波を生成した。生成した正弦波を D 級アンプに入力し、D 級アンプからの出力である PWM 信号を後段に接続したオシロスコープ (KEYSIGHT DSOS204A) で確認する。また、D 級アンプからの放射電磁波を測定するために、D 級アンプの出力端子に接続されたケーブルの近傍界をクランプ型の電流プローブ (FISCHER RF Current Probe F-2000-12MM) で取得し、信号増幅器で増幅したのち、スペクトルアナライザに入力した。D 級アンプへ入力した信号が AM 変調され電磁波を介して漏えいすることを確認するため、スペクトルアナライザのゼロスパンモードで取得した時間領域波形に含まれる周波数成分を、後段に接続したオシロスコープの FFT 機能により観測した。

図 3.7 は D 級アンプへ信号を入力した状態と信号を入力していない状態におけるスペクトルの振幅差が大きい周波数に着目し、信号を入力した状態で測定した時間領域波形であり、周期性があることがわかる。信号を入力していない状態では、このような周期的な変化は観測されない。そのため、この時間領域波形で観

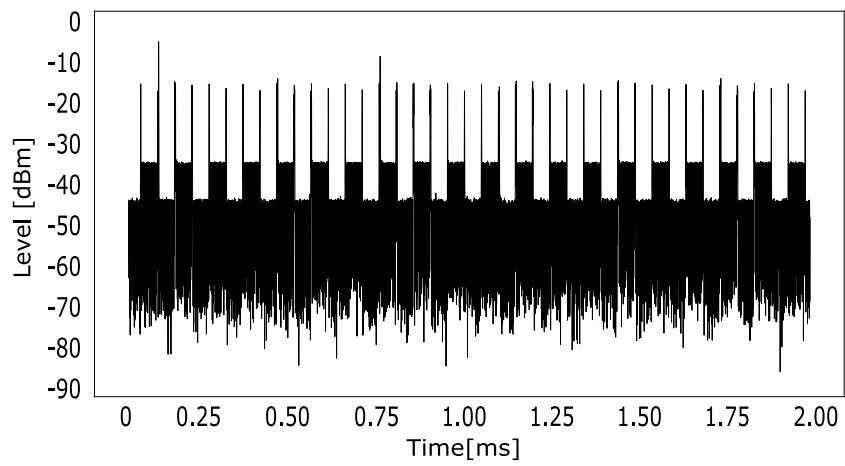


図 3.7 漏えい信号の時間領域波形

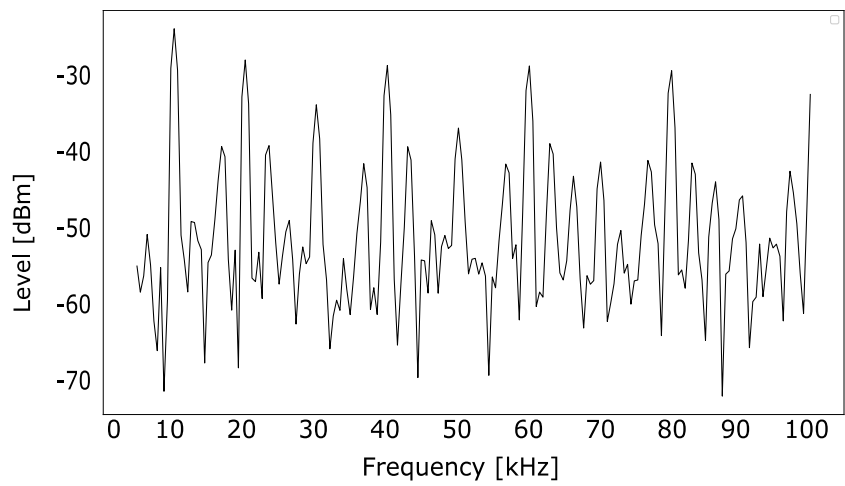


図 3.8 漏えい信号に含まれる周波数成分

測された周期変化は入力した信号に起因する変化であると推察される。この時間領域波形に含まれる周波数成分を図 3.8 に示す。D 級アンプの入力信号である 10 kHz と同じ周波数及びその高調波にピークが立っていることから、図 3.7 に示した時間領域波形は D 級アンプの入力信号を有すると考えられる。

以上より、D 級アンプ単体からも電磁波を介した音情報の漏えいが生じるため、スマートデバイスからの音情報の電磁波を介した漏えい源は D 級アンプが主たる要因であると考えられる。

3.3 スマートデバイスからの電磁波による音情報漏えい抑止策の提案

D 級アンプへの入力信号の増幅に用いられる PWM からは AM 成分が生成される [33] ことから D 級アンプが漏えい源であると推察される。前節の実験で用いたデバイスとは異なる Android 端末においても D 級アンプは実装されており [29–32]、iPhone7 以降に発売されたスマートフォンにおいても DAC 及びオーディオアンプがデバイス本体から分離したヘッドフォンジャックアダプタが用いられている。こうした機器においても、音情報が放射電磁波に重畳し機器外部へ漏えいする可能性がある。放射電磁波の電界強度は漏えい源の電力の大きさ及びアンテナとして作用する部位の放射能率で決まることから [13]、本節では漏えい源及びアンテナを構成すると考えられる部分に対する漏えい抑止策について検討する。

D 級アンプへの漏えい抑止策として、PWM のクロック生成方式に着目する。PWM のクロック生成が一定の周波数で生じる場合、音情報も同様に一定の搬送波で放射される。これは、攻撃者による音情報を含む周波数の特定と復調を容易にする。一方、PWM のクロック生成がスペクトル拡散方式で実施された場合、音情報を含む電磁波の放射がランダムに変化するとともに、出力信号スペクトルの拡散により特に高調波のスペクトルのエネルギーが低減される [34, 35]。音情報を含む電磁波の放射は一様でなくなるとともに、音情報を含む高調波のスペクトルの振幅値も低減することから、攻撃者による音情報を含む周波数の特定が難

化すると考えられる。

スマートフォンにイヤホンケーブルを挿入し音情報を入出力する状況下では、機器に挿入されたイヤホンケーブルが非意図的に構成されたアンテナとして振る舞うことが想定される。機器に接続されたケーブルからの放射はコモンモード放射を引き起こすことが多く、その場合にはダイポールまたはモノポールのアンテナとしてモデル化できる [11]。このとき、アンテナから距離 R の遠方界で測定した電界強度の大きさはケーブルの長さに比例するため、機器利用者が短いイヤホンケーブルを使用することで電界強度が減少すると考えられる。また、ケーブルをシールドすることにより、ケーブルと機器の筐体あるいはケーブルと機器周辺の導体との間に生じる寄生容量を抑え、コモンモード放射を抑制すると推察される。

D 級アンプで用いられるスペクトル拡散方式では、PWM のクロック生成が定格の周波数に対して最大 $\pm 10\%$ の範囲で変化する [34] ことから、攻撃者の受信システムの分解能帯域幅に対してスペクトル拡散方式の拡散率が十分でない場合が考えられるが、併せてアンテナとなりうる部位への漏えい抑止策を講じることでより音情報を含む電磁波の放射抑制が可能になると考える。

4. 結論

本論文では、スマートデバイスで再生した音情報が電磁波を介して機器外部へ漏えいする問題に対し、対策を講じるべき脅威の所存を把握するために必要となる音情報の漏えい源について検討を行った。

第2章では、電磁波を通じた音情報漏えい源を特定するために、音情報を機器外部へ伝搬する漏えい周波数において音情報の再生時・停止時の放射電磁界強度の分布図を比較することにより漏えい源となる素子の含まれる範囲を絞り込むと共に、電気的な負荷条件を変更した場合の放射電磁界強度の変化を観測することにより漏えい源を特定する手法を示した。

第3章では、第2章で提案した手法を用いて、音情報の再生に関連するデバイス部位が本体から分離したスマートフォンを対象に放射電磁界強度の分布図を作成し、再生した音情報が漏えいする要因となるデバイスの部位を特定した。そして、特定した部位に実装された素子と同様の素子のみを駆動させた場合にも音情報が漏えいすることを示した。また、その結果に基づき、漏えい源及び非意図的なアンテナを構成しうる部位に対する漏えい抑止策を示し、漏えいを抑制できる可能性を示唆した。

以上より、本論文では、スマートフォンで再生した情報が電磁波を介して機器外部へ漏えいする主要な要因となる素子がD級アンプであることを示した。漏えい源探索に用いた端末とは異なるスマートフォンにおいてもD級アンプは実装されており、こうしたデバイスにおいても再生した情報が放射電磁波に重畳し機器外部へ漏えいする可能性があるが、D級アンプやイヤホンケーブルに対策を施すことにより、電磁波を通じたスマートデバイスからの音情報漏えいの抑止が可能になると考えられる。

謝辞

末筆ながら、本研究を行うにあたり、ご支援下さった皆様に深く感謝の意を表します。

本学林優一教授には、日頃の研究活動において懇切丁寧なご指導とご教授を賜りました。ここに心より感謝申し上げます。

本学藤川和利教授及び安本慶一教授には、研究を進めるにあたり有益なご助言・ご討論を頂き、心より御礼申し上げます。

本学藤本大介助教には、本研学生活の中で適切なご助言と細部にわたるご支援をいただきました。厚く御礼申し上げます。

仙台高等専門学校衣川昌宏助教には、研究活動から論文の執筆に至るまで様々なご助言を頂き、感謝申し上げます。

最後に、日ごろの研学生活において様々な面でご協力いただきました、林研究室の皆様にこの場を借りて深く感謝申し上げます。

参考文献

- [1] M.G.Kuhn, "Security Limits for Compromising Emanations", Lecture Notes in Computer Science, CHES2005, vol. 3659, pp. 265-279, Aug 2005.
- [2] W. v. Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", Computers and Security, vol. 4, pp. 269-286, 1985.
- [3] S. P. Martin Vuagnoux, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards", 18th USENIX Security Symposium, pp. 1-18, 2009.
- [4] T. Hidema, "Information Leakage Via Electromagnetic Emanations and Evaluation of Tempest Countermeasures", ICISS 2007, Lecture Notes in Computer Science, vol.4812, pp.167-179, 2007.
- [5] M. G. Kuhn, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays", 4th Workshop on Privacy Enhancing Technologies, pp. 88-107, May.2004.
- [6] I. KUBIAK, "Laser printer as a source of sensitive emissions", Turkish Journal of Electrical Engineering and Computer Sciences, pp. 1354-1366, 2018.
- [7] T.Tosaka, K.Taira, Y.Yamanaka, A.Nishikata, M.Hattori, "Feasibility study for reconstruction of information from near field observations of magnetic field of laser printer", 2006 17th International Zurich Symposium on Electromagnetic Compatibility, pp. 630-633, 2016.
- [8] Hyo-Joon Choi, Ho Seong Lee, Dongjoo Sim, Jong-Gwan Yook, Kyuhong Sim, "Reconstruction of Leaked Signal from USB Keyboards", 2016 URSI Asia-Pacific Radio Science Conference (URSI AP-RASC), pp. 1281-1283, Aug.2016.

- [9] Yuichi Hayashi, Naofumi Homma, Mamoru Miura, Takafumi Aoki, Hideki Sone, "A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation", 21st ACM Conference on Computer and Communications Security(CCS), pp. 954-965, Nov.2014.
- [10] 林優一, "電磁波が引き起こすスマートデバイスからの音情報の漏えいに関する基礎検討", 電気学会研究会資料, EMC-14-5, pp. 17-20, Feb.2014.
- [11] H. W. Ott, "詳解EMC工学 実践ノイズ低減技法", 東京電機大学出版局, 2013.
- [12] Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, Jean-Luc Danger, "Analysis of Electromagnetic Information Leakage from Cryptographic Devices with Different Physical Structures", IEEE Trans. on Electromagnetic Compatibility, 2013.
- [13] 電気学会 電磁環境・情報セキュリティ技術調査専門委員会, 電磁波と情報セキュリティ対策技術, オーム社, 2012.
- [14] C.R.Paul, Introduction to Electromagnetic Compatibility (Wiley Series in Microwave and Optical Engineering), Wiley-Interscience, 2006.
- [15] Takeshi Sugaware, Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideki Sone, Akashi Satoh, "Mechanism behind Information Leakage in Electromagnetic Analysis of Cryptographic Modules", The 10th International Workshop on Information Security Applications(WISA2009), Lecture Notes in Computer Science, vol.5932, pp. 66-78, 2009.
- [16] ifixit, "Samsung Galaxy S9+の分解", <https://jp.ifixit.com/Guide/Samsung+Galaxy+S9%2B%E3%81%AE%E5%88%86%E8%A7%A3/104308>
- [17] ifixit, "Essential Phone の分解", <https://jp.ifixit.com/Guide/Essential+Phone%E3%81%AE%E5%88%86%E8%A7%A3/96764>
- [18] ifixit, "iPhone7 の分解", <https://jp.ifixit.com/Guide/iPhone+7+%E3%81%AE%E5%88%86%E8%A7%A3/67382>

- [19] Cihan Ulas, Serhat Sahin, Emir Memisoglu, Ulas Asik, Canturk Karadeniz, Blial Kilic, Ugur Sarac, "Development of Automatic TEMPEST Test and Analysis System", Scientific Cooperations International Workshops on Electrical and Computer Engineering Subfields, pp. 268-273, Aug.2014.
- [20] 林優一, 本間尚文, 鳥海陽平, 高谷和宏, 青木孝文,"電磁的畫面盜視における漏えいパラメタ高速推定法に関する検討",2016 年暗号と情報セキュリティシンポジウム, 2F2-2, pp. 1-5, Jan.2016.
- [21] 山口正洋,"プリント基板近傍の磁界計測",計測制御, vo.42, no.10, pp. 867-872, Oct.2003.
- [22] D. Baudry, A. Louis, B. Mazari,"Overview of emission and susceptibility investigation and modeling with near-field measurements",Proc. Gen. Assembly Int. URSI, 2008.
- [23] Sauvage, Laurent, Sylvain Guilley, Yves Mathieu,"Electromagnetic radiations of fpgas: High spatial resolution cartography and attack on a cryptographic module",ACM Transactions on Reconfigurable Technology and Systems (TRETs), vol.2, no.1, Article 4, Mar.2009.
- [24] E. TECHNOLOGY,"ES9218P", <http://www.esstech.com/index.php?cID=422>
- [25] 旭化成エレクトロニクス株式会社,"スマホでも DSD 音源を再生、ヘッドフォンアンプ内蔵 D/A コンバーターを開発", https://www.akm.com/akm/jp/aboutus/news/20180510AK4377_001/
- [26] ifixit, "Inside Apple 's New Audio Adapter", <https://ifixit.org/blog/8448/apple-audio-adapterteardown/>
- [27] chipwork, "Apple iPhone 6s Complementary Teardown Report with Additional Commentary"

- [28] chipworks, "Inside the iPhone 5s", <https://www.chipworks.com/aboutchipworks/overview/blog/nside-the-iphone-5s>
- [29] GADGET-MANUAL&SCHEMATICS, "Xiaomi Schematic & Diagrams", <https://www.gadget-manual.com/xiaomi/xiaomi-schematic-diagrams/>
- [30] T. Insights, "Huawei Mate 10 Teardown", <https://www.techinsights.com/about-techinsights/overview/blog/huawei-mate-10-teardown/>
- [31] Laptopmain, "Sony Xperia XZ Teardown", <https://www.laptopmain.com/sony-xperia-xz-teardown/>
- [32] ifixit, "LG G5 Teardown", <https://jp.ifixit.com/Teardown/LG+G5+Teardown/61205>
- [33] 高橋勲, 宮入庄太, "PWM インバータの出力波形とゲート制御信号との関係", 電気学会論文誌 B, 95B, 2 号, pp. 73-80, 1975.
- [34] Maxim Integrated, "アプリケーションノート 3977 D 級アンプ: 基本動作と開発動向", Mar.2007.
- [35] Maxim Integrated, "アプリケーションノート 3811 D 級アンプの電磁波妨害を最小限にするスペクトラム拡散変調モード", Jun.2013.

著者発表論文

1. 仁科泉美, 藤本大介, 衣川昌宏, 林優一, “スマートデバイスからの電磁情報漏えい源特定に関する基礎検討,” ハードウェアセキュリティ研究会, HWS2018-18, 2018.