

修士論文

漏えい電磁情報の取得性高精度化のための 計測雑音低減に関する研究

川上 莉穂

奈良先端科学技術大学院大学

先端科学技術研究科

情報理工学プログラム

主指導教員: 林 優一 教授

情報セキュリティ工学研究室（情報科学領域）

令和2年3月13日提出

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

川上 莉穂

審査委員：

林 優一	教授	（主指導教員, 情報科学領域）
岡田 実	教授	（副指導教員, 情報科学領域）
安本 慶一	教授	（副指導教員, 情報科学領域）
藤本 大介	助教	（副指導教員, 情報科学領域）

漏えい電磁情報の取得性高精度化のための 計測雑音低減に関する研究*

川上 莉穂

内容梗概

電磁照射により情報を含む漏えい電磁波の強度を制御し、機器から意図的な情報漏えいを引き起こす脅威がある。本脅威では情報漏えいの過程で、計測雑音レベルも増加する。漏えい電磁波を通じた情報の取得性は計測雑音レベルより変化するため、その強度を考慮した議論が求められる。

本論文では、電磁照射により生じた漏えい情報評価の精度向上のために、(1) 照射電磁波の自己干渉波による計測雑音レベルの増加、(2) 電磁照射により生ずる漏えい電磁波が含むターゲットとなる信号以外による計測雑音レベルの増加に着目する。実験では、計測雑音レベルが増加した環境下においても自己干渉波抑制信号による雑音の抑制とターゲット信号と他信号の分離により、雑音を低減することで、漏えい電磁波と計測雑音の強度の信号雑音比 (SNR) が改善することを実証した。さらに、高精度化した評価手法を適用することで脅威の対象が拡大する可能性を示した。

キーワード

電磁情報セキュリティ, 電磁的情報漏えい, 意図的電磁妨害, 信号雑音比

* 奈良先端科学技術大学院大学 先端科学技術研究科 修士論文, 令和 2 年 3 月 13 日.

Accurate Electromagnetic Information Leakage Measurement Method by the Background Noise Reduction*

Riho Kawakami

Abstract

There is a threat that controls the intensity of leakage electromagnetic (EM) wave containing information by applying an intentional EM irradiation and causes intentional information leakage from electrical devices. In this kind of threat, when information leakage is induced, the level of background noise which is EM wave not including information also increases. Since the acquisition of information through leaked EM waves is affected by the background noise level, consideration of the measured background noise when measuring the leaked EM wave is needed. In this thesis, a study on the accuracy improvement method of the leakage information evaluation caused by EM irradiation is proposed by reduction of noise. In this study, as background noise, I focused on (1) the increase in the background noise level due to the self-interference wave of the irradiated EM wave, and (2) the increase in the background noise level due to other than the target signal contained in the leakage EM wave generated by the EM irradiation. In the experiment, in an environment where the background noise level was increased, it was validated that the background noise was reduced by suppressing the attenuation in a self-interference wave and separating the target information signal from other signals which were noise. Then, it was demonstrated that the signal-to-noise ratio (SNR) of the intensity of the leaked EM wave and the background noise was improved. Furthermore, the possibility

* Master's Thesis, Graduate School of Science and Technology, Nara Institute of Science and Technology, March 13, 2020.

of expanding the threat target by using a highly accurate evaluation method was shown.

Keywords:

electromagnetic information security, electromagnetic information leakage, information electromagnetic interference, signal-to-noise ratio

目次

図目次		vi
第 1 章	序論	1
1.1	電磁波を介した電磁的情報漏えいの脅威	1
1.2	漏えい電磁波の放射強度の制御による電磁的情報漏えいの評価と 問題点	2
1.3	本研究の目的	5
1.4	本論文の構成	6
第 2 章	電磁照射による意図的な情報漏えい誘発時に生ずる計測雑音の低 減手法	8
2.1	電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の 抑制手法	8
2.1.1	自己干渉波の問題	8
2.1.2	信号復元の困難性を決定する要因	9
2.1.3	自己干渉波の抑制手法	12
2.2	複数の情報を含んだ漏えい電磁波からのターゲット信号取得手法 .	13
2.2.1	情報混合の問題	14
2.2.2	漏えい電磁波の周波数特徴の違いを利用したフィルタリン グ手法	15
2.2.3	回路構造の差異により変化する漏えい電磁波の強度	17
2.3	まとめ	17
第 3 章	電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の 抑制に関する検討	19
3.1	自己干渉波抑制の実験環境	19
3.2	搬送波の自己干渉抑制効果の実証	21
3.2.1	提案手法による自己干渉波抑制の評価	21
3.2.2	機器からの漏えい電磁波のスペクトル比較	22

3.3	漏えい電磁波の振幅復調結果の比較	24
3.4	自己干渉波抑制によるターゲット信号取得に関する考察	25
3.5	まとめ	26
第 4 章	複数の信号を含む漏えい電磁波からのターゲット信号の取得に関する検討	27
4.1	データ信号とクロック信号が含まれる漏えい電磁波からのターゲット信号の取得	27
4.1.1	データ信号とクロック信号が含まれる漏えい電磁波を取得する実験環境	27
4.1.2	フィルタリングによるターゲット信号の取得	29
4.1.3	移動平均によるクロック信号フィルタリングの考察	30
4.2	複数のデータ信号が含まれる漏えい電磁波からのターゲット信号の取得	31
4.2.1	複数の信号が含まれる漏えい電磁波を取得する実験環境	31
4.2.2	ターゲット信号が取得可能となった照射周波数	34
4.2.3	漏えい電磁波の放射強度の差異についての考察	36
4.3	まとめ	37
第 5 章	結論	38
	謝辞	40
	参考文献	41
	発表リスト	44

図目次

1.1	電磁的情報漏えいの脅威	1
1.2	電磁照射による脅威対象機器の増加	2
1.3	漏えい電磁波の誘発手法	3
1.4	計測雑音増大の要因	4
1.5	電磁的情報漏えいと SNR の関係	5
1.6	本論文の構成	7
2.1	電磁照射を用いた情報漏えいの誘発における自己干渉波の問題	9
2.2	変調度の説明	10
2.3	漏えい電磁波のスペクトル	11
2.4	提案手法における自己干渉波抑制の原理	13
2.5	電磁照射を用いた情報漏えいの誘発における情報混合の問題	14
2.6	内部信号によって変化する漏えい電磁波のスペクトル	15
2.7	提案手法によるクロック成分のフィルタリング	16
2.8	回路構造の差異により変化する漏えい強度	18
3.1	自己干渉抑制評価のための実験環境	20
3.2	自己干渉抑制評価のための評価信号	21
3.3	漏えい電磁波のスペクトル	22
3.4	ターゲット信号を含んだ漏えい電磁波のスペクトル	23
3.5	漏えい電磁波の振幅復調結果	25
4.1	データ信号とクロック信号が含まれる漏えい電磁波を取得する実験環境	28
4.2	SDA ラインと SCL ラインの伝送信号	29
4.3	複数の情報を含む漏えい電磁波	30
4.4	複数の信号を含む漏えい電磁波を取得する実験環境	32
4.5	マイコン間の伝送信号	33

4.6	データ信号を取得した照射周波数	34
4.7	照射周波数 400 [MHz] の漏えい電磁波	35
4.8	照射周波数 1250 [MHz] の漏えい電磁波	36

第 1 章 序論

1.1 電磁波を介した電磁的情報漏えいの脅威

電磁環境両立性（EMC: Electromagnetic Compatibility）の分野では、機器の動作時に生じる不要な放射電磁波が他の機器に干渉し、機器動作を妨害することや誤動作を引き起こすことが問題（EMI: Electromagnetic Interference）となっている。これまで不要電磁放射に関して、EMC の規格により他機器への干渉を防ぐことを目的とした抑制手法が検討されている [1][2][3]。しかし、EMC 規格以下の電磁放射においても、不要放射電磁波を通じて情報通信機器の内部情報が漏えい（電磁的情報漏えい）する問題が報告されており [4][5][6]、EMC とセキュリティの両分野にまたがった課題となっている。

電磁波を通じた情報漏えいは、機器から生じる非意図的な放射電磁波（漏えい電磁波）を受信・解析することにより機器内部の情報が外部へ漏えいする脅威である [7]。これまでに電磁波を介した情報漏えいの脅威対象は、PC（Personal Computer）等の情報端末のモニタ画面情報 [8][9][10]、プリンタの印字情報 [11][12]、キーボードの打鍵情報 [13][14] など多岐にわたって報告されている（図 1.1）。

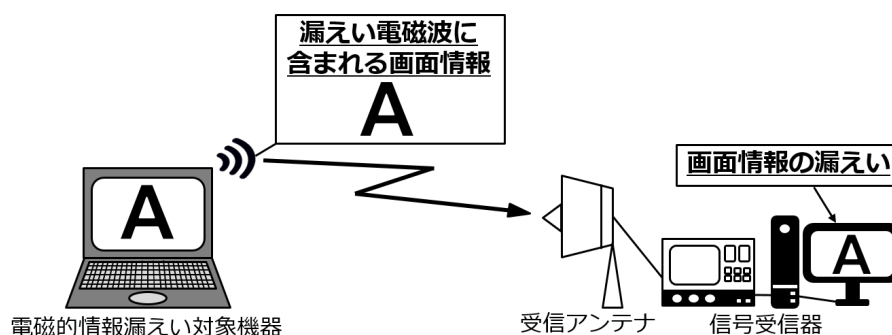


図 1.1 電磁的情報漏えいの脅威

機器のセキュリティを低下させる原因となる機器情報を含む電磁波の漏えいのメカニズムは環境電磁工学において Source-Path-Antenna モデルと呼ばれる 3 つの

要素の積で表現されることが知られている [15][16]。Source は機器の駆動源の出力となる機器内部信号であり、Path は Source と後述する Antenna を結合させる伝搬経路である。そして、機器設計者の意図しない回路配線が Antenna として振舞い機器外部へ信号を含んだ電磁波が放射される。回路配線の Antenna としての放射効率は回路構造に応じて異なるため、機器毎にその漏えい強度は異なる。

そのため、電磁的情報漏えいの脅威対象機器は、上述した機序に従い放射された漏えい電磁波が背景雑音に埋もれることなく攻撃者まで伝搬する機器に限られていた。これに対し、本論文では、近年検討されている機器からの漏えい強度を攻撃者が制御できる新たな脅威 [17] に着目する（図 1.2）。

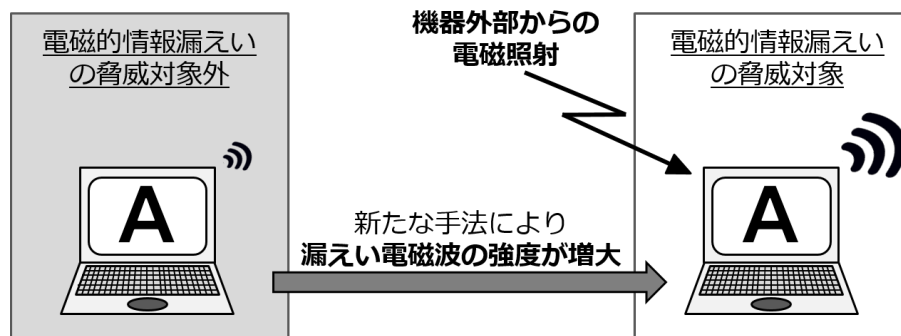


図 1.2 電磁照射による脅威対象機器の増加

漏えい強度を制御する手法では、漏えい電磁波の放射強度が弱いため、従来脅威の対象とされていなかった機器も対象になることから、新たな情報漏えいに対する評価手法が求められる。

1.2 漏えい電磁波の放射強度の制御による電磁的情報漏えいの評価と問題点

漏えい強度を攻撃者が制御できる新たな脅威は、機器に対して電磁波を照射し、漏えい電磁波の放射強度を制御可能とすることが報告されている [18][19]。そのプロセスを以下で具体的に述べる。

特定周波数の電磁波を機器外部より照射し、搬送波となる照射電磁波を機器内部へ伝搬させる（図 1.3：①）。この時の照射電磁波の周波数は、主に評価対象としている信号が伝送している伝送線路長に依存していると考えられており、照射電磁波の伝搬効率の良い周波数を選択している [20]。そして、機器内部の入出力回路に伝搬した搬送波は、回路内部の潜在的に情報漏えいを誘発する構造（MOSFET）を変調素子として動作させる。MOSFET は一般的に集積回路（IC: Integrated Circuit）の入出力回路に使用されており、MOSFET の Gate にターゲット信号となる機器内部信号が入力され、ターゲット信号の振幅値に応じて Drain-Source 間の抵抗値が変化する。そして、機器外部から注入された搬送波が Drain-Source 間の抵抗値の変化により振幅変調され、ターゲット信号を表現する振幅変調信号が生成される（図 1.3：②）。この振幅変調信号が漏えい電磁波として機器外部に放射する（図 1.3：③）。そして、この漏えい電磁波を振幅復調にて復元することで、内部情報を取得する（図 1.3：④）。この手法より、これまで電磁的情報漏えいの脅威対象外であった機器が脅威となることが示されている。

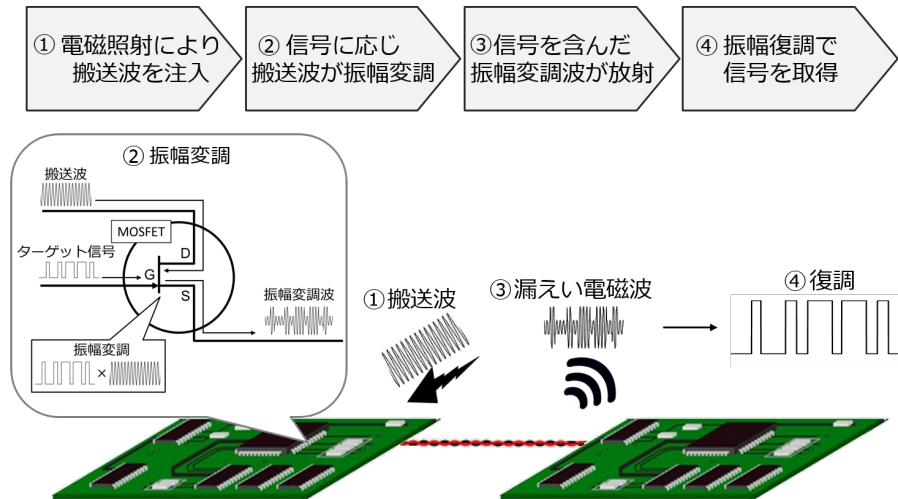


図 1.3 漏えい電磁波の誘発手法

一方、電磁照射により情報漏えいを誘発させる手法は漏えい電磁波の取得精度を低下させてしまう恐れがある。本論文では、取得精度を低下させる要因を以下の2つとする。

- (1) 漏えいを制御するために照射する電磁波による自己干渉波
- (2) 電磁照射より漏えいするターゲット以外の信号が含まれる漏えい電磁波

さらに、(1)を自己干渉ノイズ、(2)を他信号干渉ノイズとし、これら2つを併せて計測雑音と定義する(図1.4)。

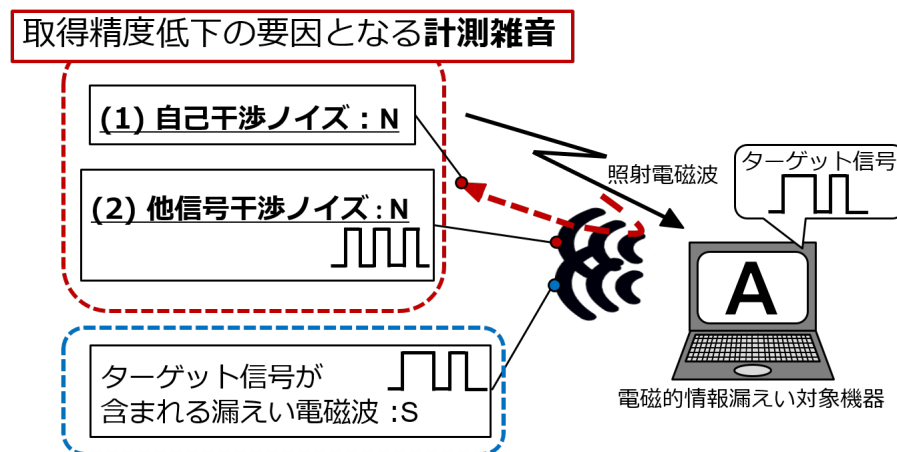


図 1.4 計測雑音増大の要因

従来手法では、漏えい電磁波のみならず計測雑音の強度も増大する恐れがあるため、本研究では、ターゲット信号を含む漏えい電磁波と計測雑音の信号雑音比 (SNR: Signal to Noise Ratio) を用い、漏えいを評価する。そこで、図 1.5 に漏えい電磁波と計測雑音の関係を示す。図 1.3 では、信号成分を増大させることに (図 1.5 : ①) に主眼をおいていた。その一方で、漏えい誘発時に照射される電磁波が計測雑音を増大させる (図 1.5 : ②) 可能性がある。そのため、漏えい電磁波が、電磁照射により増大した計測雑音に埋もれてしまい、機器内部情報を表すターゲット信号の取得が困難となる可能性がある。これにより、本来漏えいが増大している機器に対しても漏えい情報が取得できないため脅威の対象外と判断され、電磁的情報漏

えいに対する対策が施されない。しかし、増大した計測雑音の強度を抑制することが可能となれば、脅威範囲外とされていた機器も脅威の範囲内となる恐れがある。そのため、漏えい電磁波の強度のみに着目している従来手法では電磁的情報漏えいの評価が不十分となり、新たな評価手法が求められる。

そこで、本論文では、情報漏えいを誘発させる手法において、誘発過程で計測雑音を増大させる要因となる電磁波を抑制する（図 1.5：③）手法について検討する。

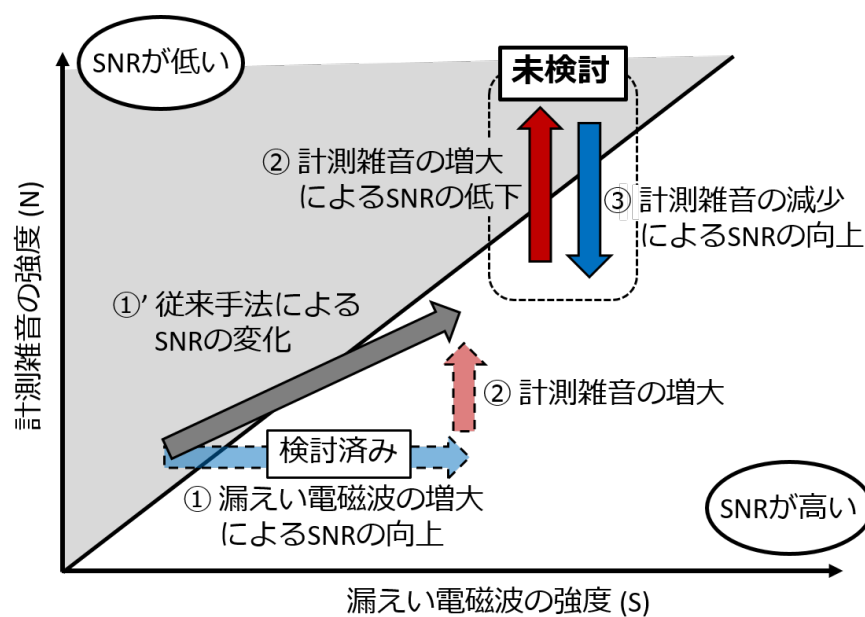


図 1.5 電磁的情報漏えいと SNR の関係

1.3 本研究の目的

電磁的情報漏えいを強制的に誘発させる手法は、基礎的な検討として漏えい源が単一である機器に対して電磁波を照射し漏えいの強度を増大させていた [17]。そして、評価者は漏えい電磁波の強度にのみ着目し、漏えいの有無を判断していた。しかし、計測雑音を考慮した場合、SNR が低下し、計測環境によっては評価結果に差異が生ずる可能性がある。

そこで本論文では、強制的に情報漏えいを誘発させる手法の適用時に生ずる計測雑音の増大抑制による漏えい精度評価向上を目的とし、電磁的情報漏えいの評価環境の構築によって評価する。

具体的には対象機器に対して電磁的情報漏えいが誘発されているのか否かの評価を困難化する SNR 低下の問題を (1) 電磁照射による情報漏えい誘発時に生ずる自己干渉波の重畳 と (2) 電磁照射による複数の漏えい電磁波の混合 の 2 つに分類する。そして、(1) の環境における実験では、自己干渉波抑制の有意性を示すために照射電磁波による自己干渉波が漏えい電磁波と共に受信され SNR が低下する環境を構築する。また、これまでの評価対象機器は単一の漏えい源であったため、(2) の実験では複数の漏えい源が存在する機器を用いて、複数の漏えい電磁波が放射される評価環境を構築する。そして、構築した実験系を用いて、(1) (2) の環境下における、ターゲット信号を含む漏えい電磁波以外の電磁波による計測雑音を低減する手法を提案し、SNR が改善されることを実証する。そして、電磁照射によりターゲット信号を含む漏えい電磁波以外の信号強度が増大する環境下においても高精度な評価が可能であることを示す。

1.4 本論文の構成

本論文の構成は以下の通りである (図 1.6)。

第 2 章では、強制的な情報漏えいを誘発する評価手法では、計測雑音の増加により SNR が低下する可能性があるため、計測雑音の低減手法を提案する。そして、計測雑音の強度が強く SNR が低い場合においても、提案手法により電磁的情報漏えいの評価が高精度に行える可能性について論ずる。

第 3 章では、電磁照射による自己干渉波が、漏えい電磁波と共に受信器に入射され、計測雑音が増大し SNR が低下する環境下におけるセキュリティ評価のため、(1) 電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の抑制手法を実証する。そして、自己干渉ノイズが存在する環境下においても、SNR を向上させ、機器内部信号が取得可能である事を示す。

第 4 章では、実際の機器を模擬し、複数の信号が伝送されている機器からターゲット信号とそれ以外の信号が放射されることにより、SNR が低下する環境下に

おけるセキュリティを評価する。そのため、(2) 複数の信号を含む漏えい電磁波からターゲット信号の取得手法を実証する。そして、他信号干渉ノイズが生じ、複数の情報が混合された電磁波を受信した場合においても、信号処理を施すことにより機器内部信号が取得可能であることを示す。

第5章では、本論文の結論を述べる。

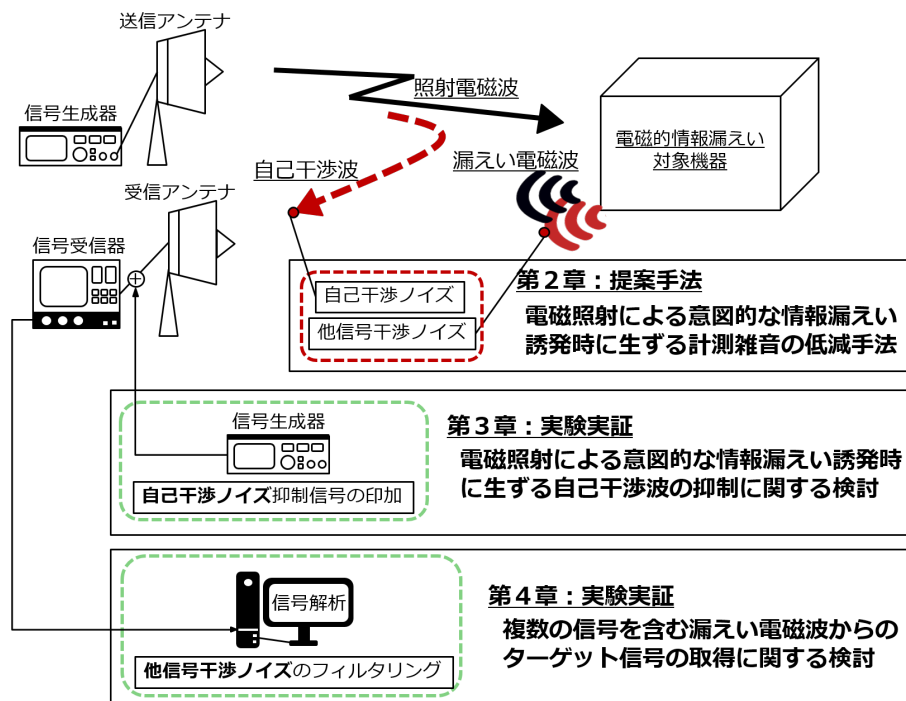


図 1.6 本論文の構成

第 2 章 電磁照射による意図的な情報漏えい誘発時に生ずる計測雑音の低減手法

本章では、文献 [17] の手法による SNR 低下の問題を（１）電磁照射による情報漏えい誘発時に生ずる自己干渉波の重畳 と（２）電磁照射による複数の漏えい電磁波の混合 の２つに分類し、それぞれの環境下における計測雑音の低減手法を提案する。

2.1 電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の抑制手法

本節では、（１）照射電磁波の自己干渉波が計測雑音となり、SNR の低下により受信信号が劣化し、漏えい電磁波の取得精度が低下する環境を想定する。そこで、SNR 向上のため、自己干渉波の抑制手法を提案する。

2.1.1 自己干渉波の問題

漏えい電磁波を誘発する従来手法では、機器に向けて電磁照射（図 2.1 : ①）し、照射電磁波を搬送波として MOSFET へと伝搬させ、ターゲット信号を表す振幅変調波を生成する（図 2.1 : ②）。そして、振幅変調波が機器外部に放射（図 2.1 : ③）されることで、強制的な電磁的情報漏えいを誘発させる。

しかし、上述の手法では、機器に向けて照射する電磁波が、評価対象だけではなく受信アンテナに入射（図 2.1 : ④）される。そのため、照射電磁波を受信アンテナで受けてしまうことは不可避であり、本来取得したい漏えい電磁波の振幅変調信号成分に照射電磁波が重畳する。そして、重畳した信号は波形自体の振幅を増大させるため、受信器により振幅復調をする際には大振幅の信号と小振幅の振幅変調信号を同時に観測する必要がある。しかし、振幅値が増大した波形から、ターゲット信号を表現するわずかな振幅値を読み取ることが容易ではなく、ターゲット信号の復元が困難となる。

以下では、電磁照射による自己干渉波の影響により、漏えい電磁波から信号復元

の困難性を決定する要因について論じ、提案手法を説明する。

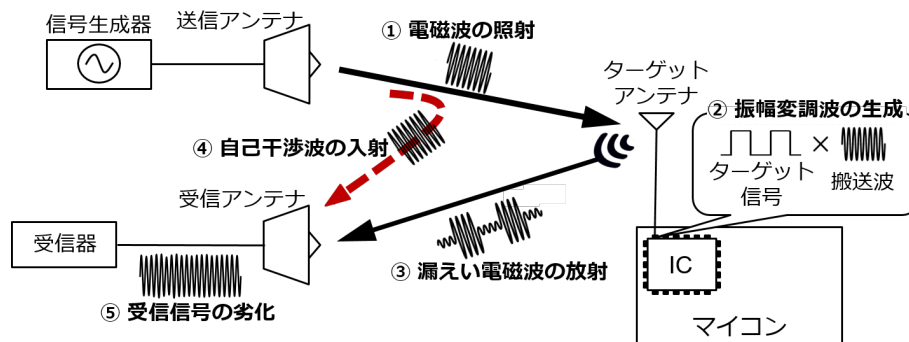


図 2.1 電磁照射を用いた情報漏えいの誘発における自己干渉波の問題

2.1.2 信号復元の困難性を決定する要因

理想的な振幅変調信号は、搬送波を $A_c \cos(\omega_c t)$ 、ターゲット信号を $A_t \cos(\omega_t t)$ とすると以下の式 (2.1.1) で表すことができる [21]。

$$\begin{aligned} AM &= (A_c + A_t \cos \omega_t t) \cos \omega_c t \\ &= A_c \cos \omega_c t + \frac{m}{2} A_c \{ \cos(\omega_c + \omega_t)t + \cos(\omega_c - \omega_t)t \} \end{aligned} \quad (2.1.1)$$

$$m = \frac{A_t}{A_c} \quad (2.1.2)$$

ここで、 A_c 、 A_t は各信号の振幅、 ω_c 、 ω_t は角速度、 t は時間、式 (2.1.2) で表される m は変調度である。変調度とは、搬送波がターゲット信号をどれだけ含んでいるか表す指標となる。そして、実際に受信される波形の変調度 m に依存して、振幅復調の困難性が決まる。搬送波はターゲット信号に応じて変調され、振幅変調

波の変調度は、搬送波の振幅値 A_c とターゲット信号の振幅値 A_t によって定まる。
 (図 2.2) そして、搬送波の振幅値とターゲット信号の振幅値が近い ($m=1$) ほど、
 変調度が高くターゲット信号の復元が容易となり、無変調である $m=0$ では、ター
 ゲット信号の取得が不可能となる。

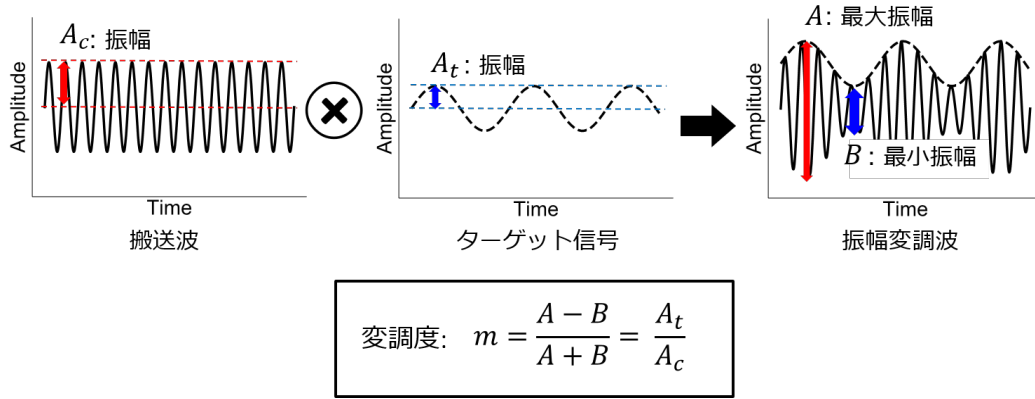


図 2.2 変調度の説明

実際の受信信号は、式 (2.1.1) に搬送波の位相から位相が θ ずれた自己干渉波 $A'_c \cos(\omega_c t + \theta)$ が加算されるため、以下の式 (2.1.3) で表すことができる。

$$\begin{aligned}
 AM' &= A_c \cos \omega_c t + \frac{m}{2} A_c \{ \cos(\omega_c + \omega_t)t + \cos(\omega_c - \omega_t)t \} + A'_c \cos(\omega_c t + \theta) \\
 &= A_c \cos \omega_c t + \frac{m}{2} A_c \{ \cos(\omega_c + \omega_t)t + \cos(\omega_c - \omega_t)t \} \\
 &\quad + A'_c \cos \omega_c t \cos \theta - A'_c \sin \omega_c t \sin \theta \\
 &= (A_c + A'_c \cos \theta) \cos \omega_c t \\
 &\quad + \frac{m'}{2} (A_c + A'_c \cos \theta) \{ \cos(\omega_c + \omega_t)t + \cos(\omega_c - \omega_t)t \} \\
 &\quad - A'_c \sin \theta \sin \omega_c t
 \end{aligned} \tag{2.1.3}$$

$$m' = \frac{A_t}{A_c + A'_c \cos \theta} \tag{2.1.4}$$

式 (2.1.3) の第 1、2 項より変調度が変化していること、第 3 項より雑音が生じ信号

が歪むことがわかる。式(2.1.4)は自己干渉波の影響により、低下した変調度を示している。これらの自己干渉波の影響により、ターゲット信号の取得が困難化する。

ここで、説明の簡単化のため、変調度が高い漏えい電磁波と変調度が低い漏えい電磁波の時間領域波形と周波数領域波形を図示する(図2.3)。周波数領域に着目すると、変調度が高い波形では搬送波の強度に対する側帯波の強度の比率が高い。一方、自己干渉波が存在する環境である変調度が低い波形では、搬送波の強度に対する側帯波の強度の比率が低いことが分かる。このことから、搬送波と側帯波の強度スペクトル比を調整することで変調度が改善され、変調度を高めることによりターゲット信号の取得可能となる。

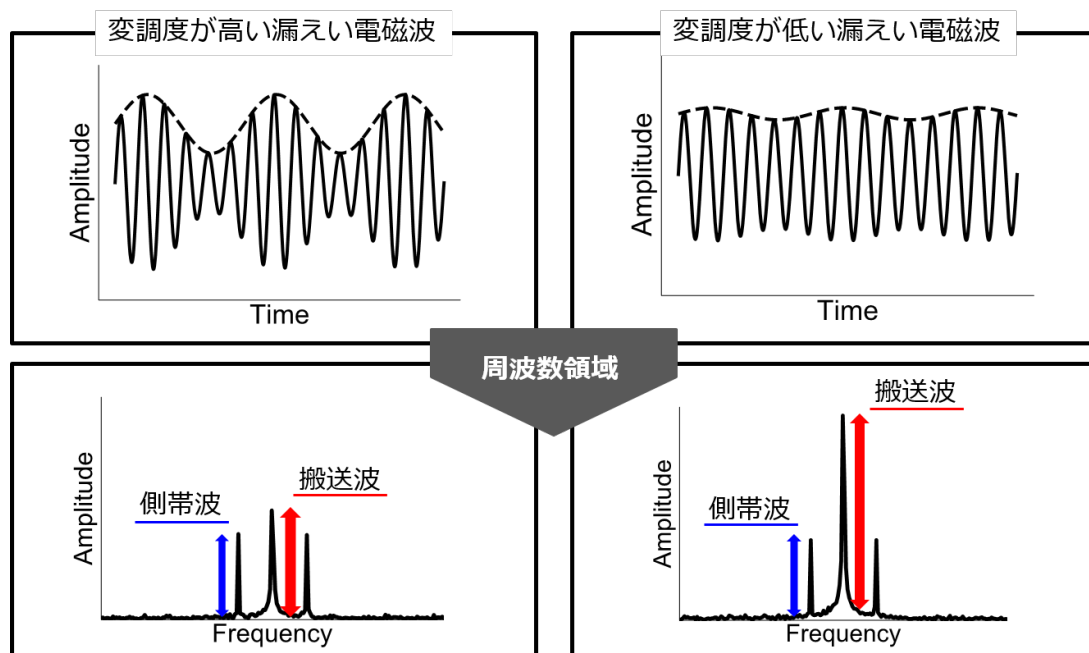


図 2.3 漏えい電磁波のスペクトル

次に、変調度を高めるため、搬送波の強度を減少させる手法を述べる。受信される信号は漏えい電磁波と電磁照射による自己干渉波が含まれる。そのため、自己干渉波となる搬送波と逆位相・同振幅の波形を受信信号に加えることで、自己干渉波を抑制できる可能性がある。よって、自己干渉波の抑制により、搬送波の強度に対

する側帯波の強度の比率が高くなるため、変調度が高まると考えられる。

次に、変調度を高めるために、式 (2.1.3) に加算する信号を以下に示す。式 (2.1.5) は自己干渉波の逆位相と搬送波の逆位相をもつ信号の和であり、自己干渉波抑制信号である。

$$cc = A'_c \cos(\omega_c t + \theta + \pi) + A_{cc} \cos(\omega_c t + \pi) \quad (2.1.5)$$

ここで A_{cc} は搬送波を打ち消し受信信号の変調度を向上させる度合いを決定するパラメタである。これにより得られる信号は以下の式で表すことができる。

$$AM_{cc} = (A_c - A_{cc}) \cos \omega_c t + \frac{m_{cc}}{2} (A_c - A_{cc}) \{ \cos(\omega_c + \omega_t)t + \cos(\omega_c - \omega_t)t \} \quad (2.1.6)$$

$$m_{cc} = \frac{A_t}{A_c - A_{cc}} \quad (2.1.7)$$

式 (2.1.6) と式 (2.1.7) から自己干渉波の影響が抑制されていること、変調度が向上していることがわかる。これにより自己干渉波抑制前に比べてターゲット信号の取得が容易となる。ただし、 A_{cc} の設定次第では、可変調や復元信号の反転などを引き起こす場合もあるため、注意が必要である。

2.1.3 自己干渉波の抑制手法

次に、前節で述べた変調度が低下する要因を踏まえ、振幅変調成分を含まない搬送波による自己干渉波の影響を抑制し、振幅変調信号を高精度に取得するため、受信器の前段において自己干渉波を打ち消す提案手法について論ずる。

機器から放射された変調波を受信する際には、自己干渉波が重畳する（図 2.4：①）。そこで、変調波に自己干渉波が重畳した受信波を受信器へと入力する前の段階で、自己干渉波の逆位相をもつ信号を足し合わせることで、自己干渉波を抑制す

る。ここで、自己干渉波を抑制するためには逆位相の波を自己干渉波に同期して生成する必要があるため、自己干渉波の位相と振幅情報をプロファイリングする（図 2.4：②）。このとき、単に受信信号に抑制信号を加えた場合、アンテナから抑制信号が放射し測定環境に影響を与えるため、方向性結合器などの一方向性の線路を用いる必要がある（図 2.4：③）。そして、自己干渉波の逆位相・同振幅の抑制信号を加えることにより、自己干渉波が抑制された信号を受信器に入力でき、変調度の高い振幅変調波が受信可能である（図 2.4：④）。このように、提案手法では、逆位相の信号の足し合わせと方向性結合器を組み合わせることで測定環境に影響を与えず自己干渉波の抑制を実現する。

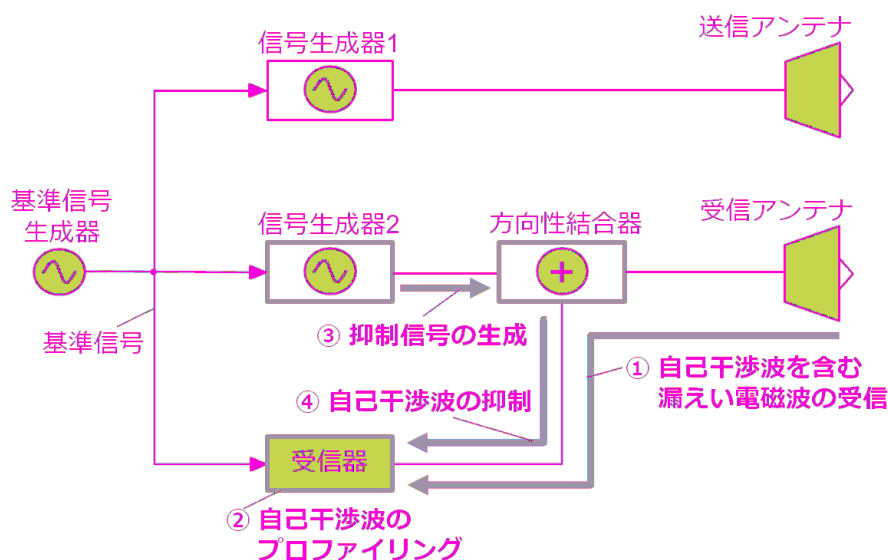


図 2.4 提案手法における自己干渉波抑制の原理

2.2 複数の情報を含んだ漏えい電磁波からのターゲット信号取得手法

本節では、(2) 電磁照射によって、ターゲット信号以外の情報を含む電磁波が誘発され、この漏えい電磁波が計測雑音となり SNR が低下し、ターゲット信号を含

む漏えい電磁波の取得精度が低下する環境を想定する。そこで、他信号干渉ノイズを除去することによる、ターゲット信号の取得手法を提案する。

2.2.1 情報混合の問題

情報漏えいを誘発させる手法（図 2.5：①）における、照射電磁波の周波数は、評価対象としている信号が伝送している伝送線路長に依存していると考えられており、照射電磁波の伝達効率の良い周波数を選択している。そのため、電磁照射に対して同程度の感度をもつ配線パターンが回路内に存在する場合、複数の配線から漏えいされた信号が混合し（図 2.5：②）、複数の情報を含む漏えい電磁波が受信される（図 2.5：③）。従って、他信号干渉ノイズによって SNR が低下することで、ターゲット信号の取得が困難となる。そこで、本節では、同程度の長さの配線を用いた近距離通信においても、伝送される信号の周波数が異なる場合には、ターゲット信号以外の信号をフィルタリングすることにより、SNR を向上させる手法を提案する。

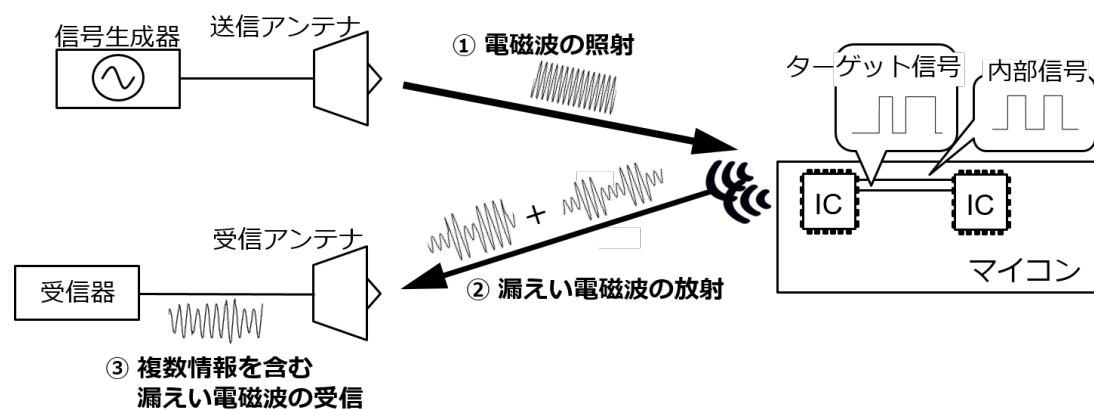


図 2.5 電磁照射を用いた情報漏えいの誘発における情報混合の問題

2.2.2 漏えい電磁波の周波数特徴の違いを利用したフィルタリング手法

一般的な信号伝送方式として多く用いられるクロック信号とターゲット信号（データ信号）が隣接して伝送される系を考える。同程度の線路長の場合、電磁照射への感度が近くとも、振幅変調された信号は周波数成分が異なる。クロック信号は単一の基本周波数とその高調波成分をもつため、固定された周波数スペクトルしか存在しないうえに、データ通信の転送レートなどから容易に周波数が予想できる。一方で、データ信号は、伝送されるデータによって、周波数スペクトルが異なるため、周波数成分が時間変動する（図 2.6）。以上の特徴を利用し、ノイズ成分となるクロック信号のみをフィルタリングすることが可能となる。

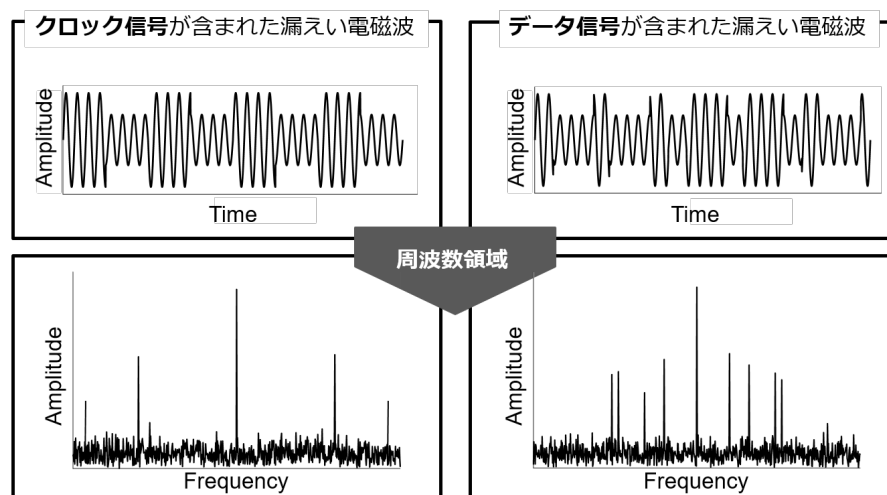


図 2.6 内部信号によって変化する漏えい電磁波のスペクトル

次に、複数の情報が含まれる漏えい電磁波に対するフィルタリング手法について説明する。情報が混合した漏えい電磁波の周波数領域を図 2.7 に示す。この波形からデータ信号のみを取得するためには、クロック成分のみをフィルタリングする必要がある。しかし、クロック周波数は既知であるが、漏えい電磁波に含まれる振幅値や位相は未知であるため、情報が混合した漏えい電磁波からクロック信号を単に差し引くだけでは、クロック成分の除去ができない。また、一般的なローパスフィルタでは、クロック信号の近傍帯の周波数成分も減衰させてしまう恐れがある。そのため、データ信号の周波数成分は減衰させず、クロック成分のスペクトルが存在する一定の間隔で、フィルタリングする周波数特性のフィルタが必要となる。移動平均によるフィルタは図 2.7 のような周波数特性であるため、クロック信号である高調波成分が等間隔にある信号の除去に適している。よって、データ信号に影響を与えることなく、クロック成分を選択的に除去することで、データ信号の取得が可能となる。また、フィルタリングのパラメタは漏えい電磁波のサンプリング周波数と除去したいクロック信号の周波数により算出する。

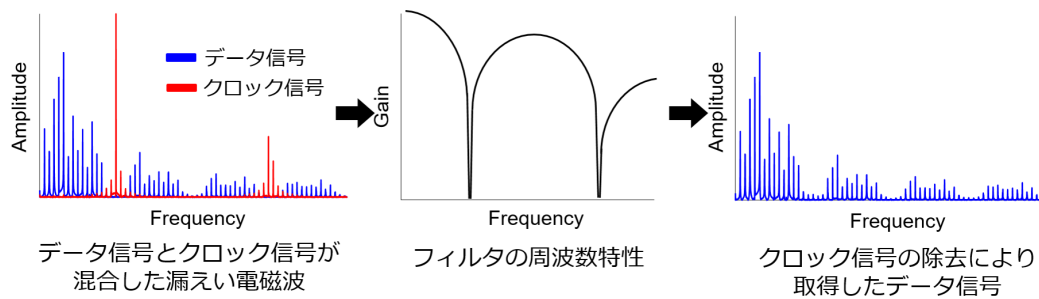


図 2.7 提案手法によるクロック成分のフィルタリング

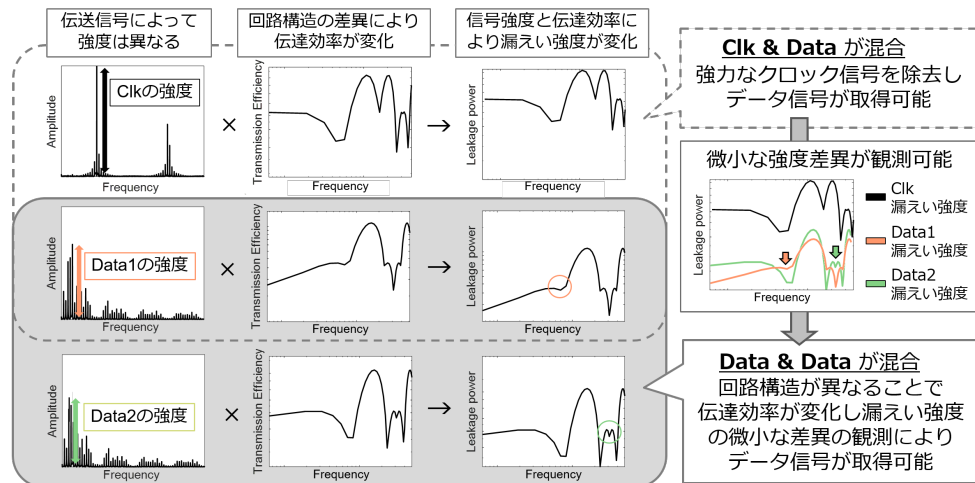
2.2.3 回路構造の差異により変化する漏えい電磁波の強度

照射電磁波の受信感度が近い場合であっても、漏えい電磁波の放射強度は異なると考えられる。これは、Source-Path-Antenna モデルに基づく、内部信号のスペクトル強度 (Source)、回路構造の差異により照射電磁波の伝達効率 (Path-Antenna) が異なるためである。クロック信号は単一の周波数成分をもつため、スペクトル強度が強いことにより、漏えい電磁波の強度が強くなる。そこで、前述の手法によりクロック信号を除去することにより、データ信号が含まれる漏えい電磁波の強度の微小な差異の観測が可能となる。回路構造により漏えい強度が変化するイメージ図を図 2.8 に示す。そして、放射強度が強い、伝達効率の良い照射周波数を選択することで、所望するデータ信号が取得可能となる。

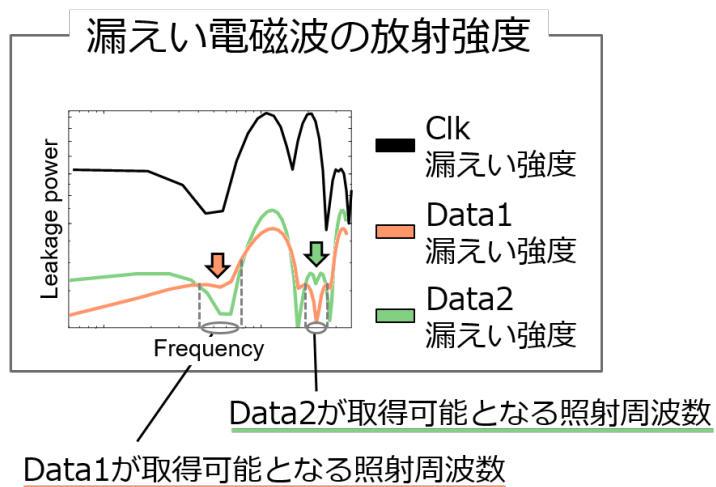
2.3 まとめ

本章では、電磁照射により計測雑音が増加することで、漏えい電磁波の取得精度が低下し、ターゲット信号となる機器内部信号が取得困難となる可能性について指摘した。そこで、(1) 照射電磁波の自己干渉波により SNR が低下する環境、(2) 電磁照射により複数の漏えい電磁波が誘発され、SNR が低下する環境を想定した。(1) の環境下において、自己干渉波を抑制し、ターゲット信号の取得制度を決定する変調度を向上させる手法を提案した。(2) の環境下において、ノイズ成分となる信号を除去し、効率の良い照射周波数を選択することによって、ターゲット信号が取得可能となる手法を提案した。

内部信号のスペクトル強度×照射電磁波の伝達効率→漏えい電磁波の強度



(a) 漏えい電磁強度の差異



(b) 照射電磁波の選択

図 2.8 回路構造の差異により変化する漏えい強度

第 3 章 電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の抑制に関する検討

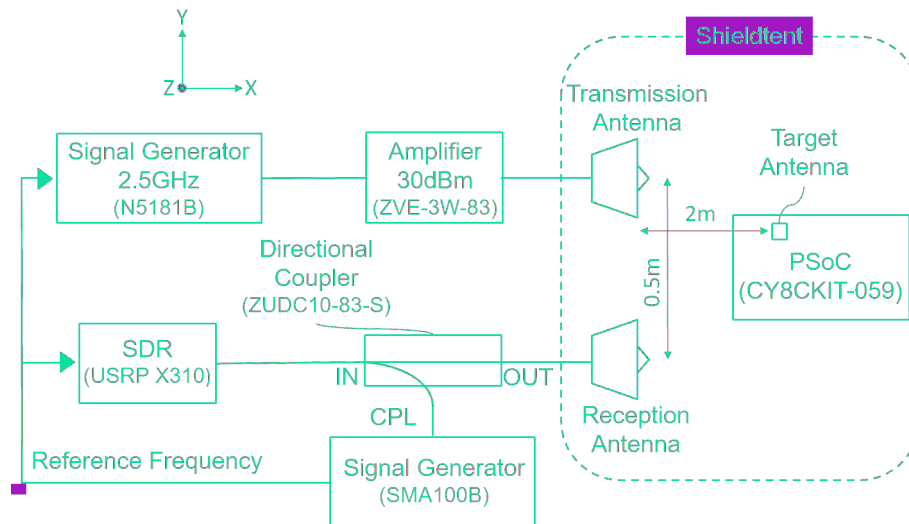
本章では、従来手法では考慮されてこなかった、計測雑音が増大し、SNR が低下する環境下における、強制的な情報漏えいの評価について論ずるため、(1) 電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の抑制について検討する。そこで、漏えい電磁波と共に照射電磁波が受信器にて受信される環境を構築し、2.1 節で提案した手法を用いて、受信された照射電磁波のみを除去することで、自己干渉波を抑制し SNR の向上を実証する。

3.1 自己干渉波抑制の実験環境

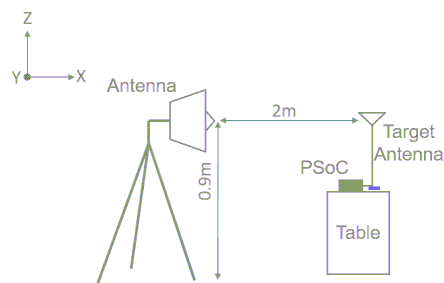
本実験では、自己干渉波を抑制することにより、ターゲット信号が取得可能であることを確証する。そこで、図 3.1 に実験環境と使用機器、設定したパラメタ、図 3.2 にターゲット信号を示す。また、自己干渉抑制の効果のみを議論するため、対象機器であるマイクロコントローラー（マイコン）に注入する電磁波の周波数に感度の良いアンテナ（ターゲットアンテナ）を接続し、照射電磁波の注入効率および、実験の再現性を高めた。さらに、評価対象機器と自己干渉波以外の信号を除去するため、シールドテント（Graphtec TM-3-2-2.5-1）内で実験した。

まず、このマイコン（Cypress CY8CKIT-059）に設置したターゲットアンテナ（Ettus-Research VERT2450）に対して、シグナルジェネレータ（Keysight N5181B）で生成した搬送波を増幅器（Mini-Circuits ZVE-3W-83）により増幅したのち、送信アンテナを用いて照射した。搬送波はターゲットアンテナを介して、マイコン内へ伝搬し、マイコンの入出力回路において振幅変調され所望するターゲット情報を含んだ状態でターゲットアンテナより放射される。この搬送波を受信アンテナにより受信し、自己干渉波を抑制するために、シグナルジェネレータ（Rohde & Schwarz SMA100B）により前章で述べた自己干渉波を打ち消す信号を生成し、方向性結合器を通して受信信号に足し合わせ、受信器となるソフトウェア無線送受信機（SDR: Software Defined Radio）へ入力した。方向性結合器は、自己干渉波を打ち消す信号が受信アンテナへと戻ることを抑制するために使用した。

この時、シグナルジェネレータ（SMA100B）の参照周波数信号を SDR とシグナルジェネレータ（N5181B）に入力することで各測定器の同期をとり、高精度な位相調整を可能とした。



(a) 実験環境の全体図



(b) シールドテント内の実験環境

図 3.1 自己干渉抑制評価のための実験環境

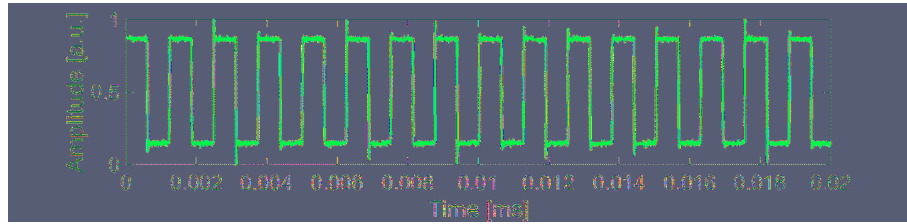


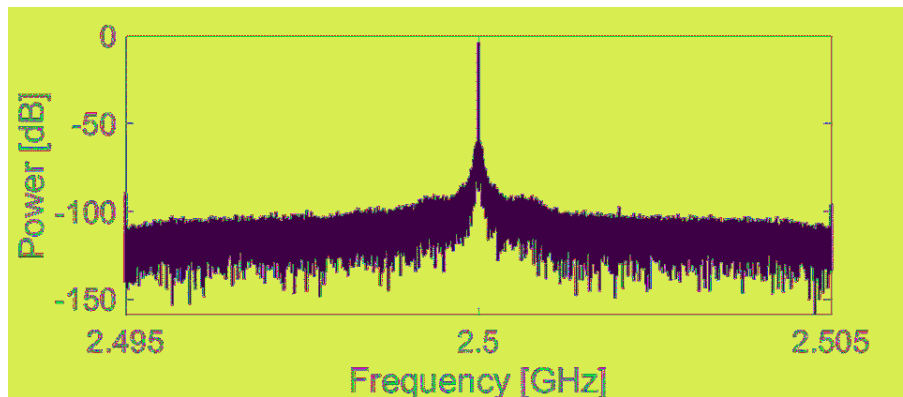
図 3.2 自己干渉抑制評価のための評価信号

3.2 搬送波の自己干渉抑制効果の実証

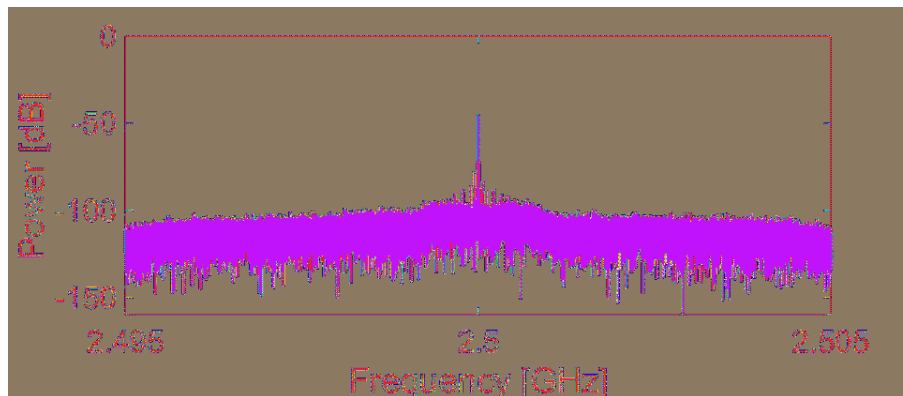
本節では、自己干渉波と逆位相の信号を足し合わせた自己干渉抑制信号による、自己干渉波の抑制により、ターゲット信号を含む振幅変調信号の強度が高まることを実験結果にて確認する。さらに、搬送波の強度が低下し側帯波の強度が向上することにより、変調度が向上することを示す。

3.2.1 提案手法による自己干渉波抑制の評価

まず初めに、自己干渉抑制の有効性を示すため、評価対象マイコンから信号が出力されていない状況で実験した。送信アンテナから正弦波をターゲットアンテナへ照射し、受信アンテナにて受信された信号のスペクトルを図 3.3 に示す。図 3.3(a) は自己干渉波を含む信号が受信された際の信号のスペクトルである。図 3.3(b) は電磁照射を行い、搬送波が受信アンテナへ到達した後、自己干渉波抑制を適用した信号のスペクトルである。両図を比較すると、自己干渉抑制により、搬送波の周波数成分が 40 dB 減少し、自己干渉波の抑制に成功していることが確認できた。



(a) 自己干渉波を含む漏えい電磁波のスペクトル



(b) 自己干渉波を抑制した漏えい電磁波のスペクトル

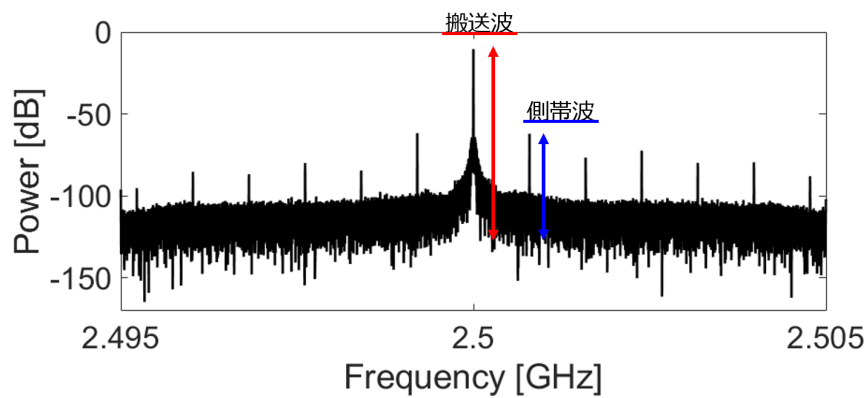
図 3.3 漏えい電磁波のスペクトル

3.2.2 機器からの漏えい電磁波のスペクトル比較

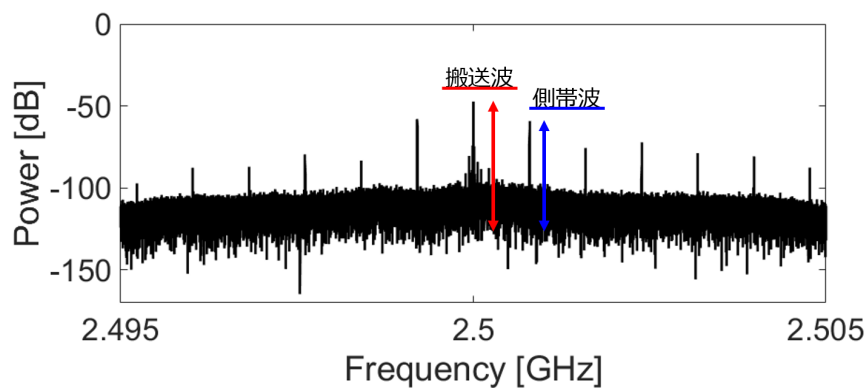
次に、評価対象マイコンにおいて、周波数 0.80 [MHz] の方形波を、ターゲット情報を表す電気信号（図 3.2）として駆動させた場合について実験した。従来手法と同様の計測をし、信号を受信した場合に観測された漏えい電磁波のスペクトルを図 3.4(a) に、提案手法により自己干渉波抑制を行い、信号を受信した場合に観測された漏えい電磁波のスペクトルを図 3.4(b) にそれぞれ示す。

図 3.4 では搬送波の周波数 (2.5 [GHz]) から 0.80 [MHz]、1.6 [MHz]、2.4 [MHz]、3.2 [MHz]、4.0 [MHz] 離れた周波数成分にピークが観測された。このことから、受

信信号にはターゲット信号 (0.80 [MHz]) の情報が含まれていることが推定される。さらに、両図を比較した場合、受信信号に自己干渉波抑制を適用した (図 3.4(b)) 際、搬送波の強度に対するターゲット信号成分を示す第 1 側帯波の強度の比率 (変調度) が向上していることが確認できた。



(a) 従来手法により得られた漏えい電磁波のスペクトル



(b) 提案手法により得られた漏えい電磁波のスペクトル

図 3.4 ターゲット信号を含んだ漏えい電磁波のスペクトル

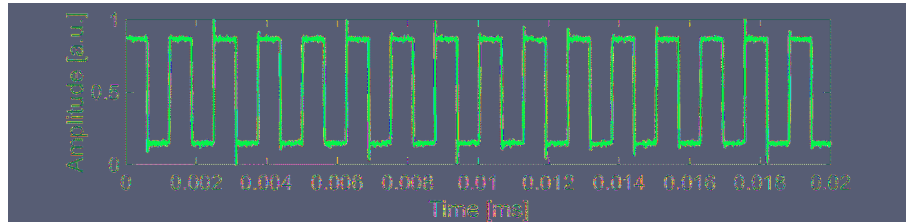
そこで、変調度を算出した結果を表 3.1 にて示す。算出した結果、変調度が向上していることが確認できた。よって、提案手法により、自己干渉ノイズとなる搬送波の影響が低減され、結果として SNR が向上したターゲット信号が取得できる可能性がある。

表 3.1 自己干渉波抑制による変調度の比較

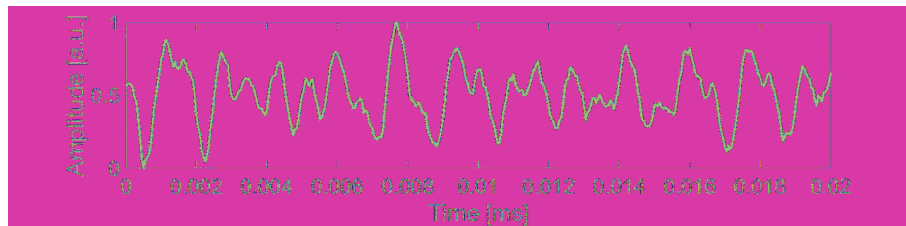
	搬送波の強度 [dB]	側帯波の強度 [dB]	変調度
自己干渉波を含んだ 漏えい電磁波	-8.0	-61	0.0022
自己干渉波を抑制した 漏えい電磁波	-47	-58	0.29

3.3 漏えい電磁波の振幅復調結果の比較

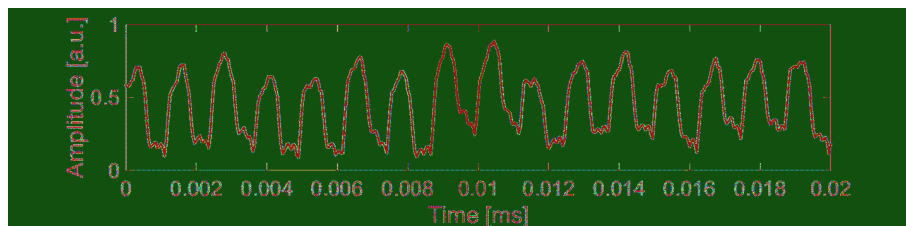
本節では、漏えい電磁波を振幅復調し、ターゲット信号を復元した結果を示す。提案手法を適用した場合と、しない場合におけるターゲット信号の取得について比較した。ターゲット信号となる方形波と漏えい電磁波を振幅復調結果の時間領域波形を図 3.5 に示す。マイコンから出力するターゲット信号は図 3.5(a) であり、観測された信号を、振幅復調し、観測した波形を時間領域にて図 3.5(b) 図 3.5(c) に示す。図 3.5(b) は従来手法で観測された信号であり、図 3.5(c) は提案手法により自己干渉波を抑制し、観測された信号となっている。周波数 0.80 [MHz] の基本波をもつターゲット信号と同様の時間変化をしている信号が観測され、ターゲット信号が漏えい電磁波を通じて機器外部で取得できることが示された。一方、提案手法を適用しない状態で振幅復調により、得られた信号である図 3.5(b) では、自己干渉波の影響を受け、信号が歪み、ターゲット信号から情報が欠落して観測されていることが確認できた。このことから、自己干渉波を抑制することにより、ターゲット信号に忠実な波形が取得できることを実証した。



(a) ターゲット信号



(b) 従来手法により取得した漏えい信号



(c) 提案手法により取得した漏えい信号

図 3.5 漏えい電磁波の振幅復調結果

3.4 自己干渉波抑制によるターゲット信号取得に関する考察

自己干渉波抑制により、送受信アンテナ間の位置関係の制限が緩和されと考えられる。よって、電磁的情報漏えいの評価が容易となるほか、装置の小型化が可能となることが推定できる。また、漏えい電磁波受信器のダイナミックレンジを増大させることが可能となる。そのため、放射強度が微小であり従来観測困難であった漏えい電磁波の観測が容易となり、より高精度な評価が可能であると考えられる。

3.5 まとめ

本章では、自己干渉波と漏えい電磁波が受信される環境を構築し、実際に自己干渉波を抑制させることで計測雑音を低減し、SNR の向上によって、漏えい電磁波からターゲット信号を取得できることを示した。具体的には、搬送波の逆位相となる自己干渉波抑制信号を、漏えい電磁波の観測時に、方向性結合器を用いることで測定環境に影響を与えず足し合わせた。そして、自己干渉波の抑制を図ることで、ターゲット信号の情報を含む側帯波の強度を増大させ、SNR の改善を試みた。その結果、ターゲット信号に、より忠実な波形を復元できることを明らかにした。

第 4 章 複数の信号を含む漏えい電磁波からのターゲット信号の取得に関する検討

本章では、第 3 章に引き続き、従来強制的に情報漏えいを誘発させる手法では考慮されてこなかった、計測雑音の増大により SNR が低下する問題について論ずるため、(2) 複数の信号を含む漏えい電磁波からターゲット信号の取得について検討する。まず、信号伝送線路長が等しく、漏えい源が複数存在する評価系を構築し、複数の漏えい電磁波を強制的に誘発させる。そして、複数の情報を含む漏えい電磁波に対し、2.2 節で提案した信号処理を施すことによりノイズ成分を除去し、ターゲット信号の取得を実証する。

4.1 データ信号とクロック信号が含まれる漏えい電磁波からのターゲット信号の取得

本節では、データ信号とクロック信号が含まれている漏えい電磁波に対し、各信号の周波数成分の違いに着目し、信号処理により他信号干渉ノイズとなるクロック成分が除去可能であることを確認する。その後、ターゲット信号となるデータ信号が取得可能であることを示す。

4.1.1 データ信号とクロック信号が含まれる漏えい電磁波を取得する実験環境

本実験は、複数の情報が含まれる漏えい電磁波に対しクロック信号をフィルタリングすることにより、ターゲット信号が取得可能であることを議論する。そこで、図 4.1 に、実験環境と使用した機器、図 4.2 にターゲットとなるデータ信号とクロック信号を示す。実験環境は、評価対象となるマイコン 2 台 (Cypress CY8C5888LTI-LP097) と通信線路、照射電磁波を生成するシグナルジェネレータ (Rohde & Schwarz SMA100B) と生成した信号を通信線路へ注入するインジェクションプローブ (FCC F-140)、漏えい信号を受信する電流プローブ (FCC F-2000) と受信器となるスペクトラムアナライザ (Rohde & Schwarz FSV4) とオシロスコープ (Keysight DSOX3054T) で構成した。マイコン間をフラットケーブルに

て接続し、通信方法として近距離通信に用いられる I2C 通信を模擬した [22]。そして、IC 間を制御するシンプルな 2 線式双方向バスであるシリアル・データライン (SDA) とシリアル・クロックライン (SCL) の線路長を 30 [cm] とした。照射周波数は伝送線路長のおよそ 1/2 波長となる周波数 500 [MHz] を使用した。信号は、SDA ラインで 0.1 [Mbps] のデータ信号 (図 4.2(a))、SCL ラインでは 0.1 [MHz] のクロック信号 (図 4.2(b)) をそれぞれマイコン A から B へ伝送した。また、インジェクションプローブによりアンテナによる遠方からの電磁照射、及び、電流プローブにより漏えい電磁波を遠方から受信するアンテナを模擬し、照射電磁波の注入効率、及び、漏えい電磁波の測定の再現性を高めた。

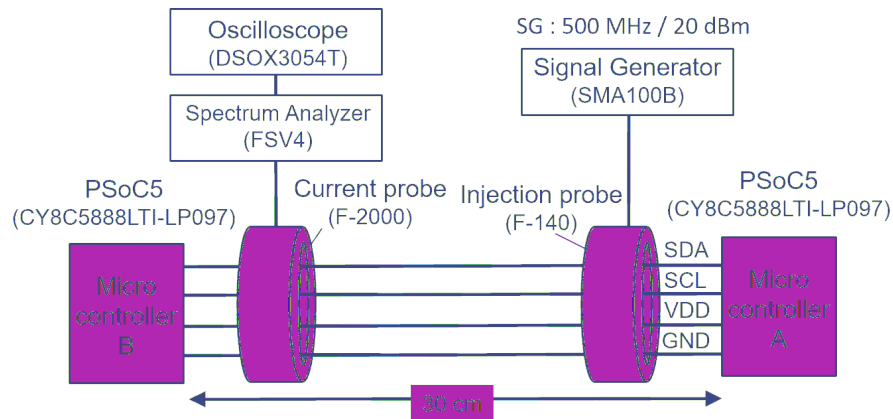
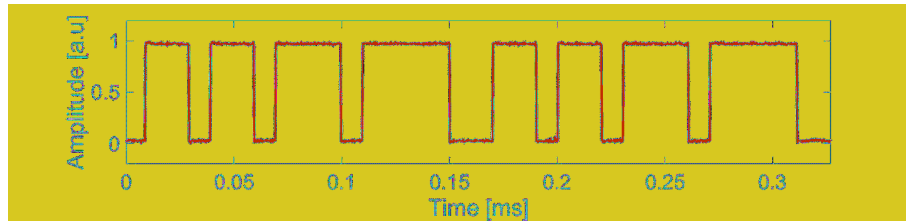
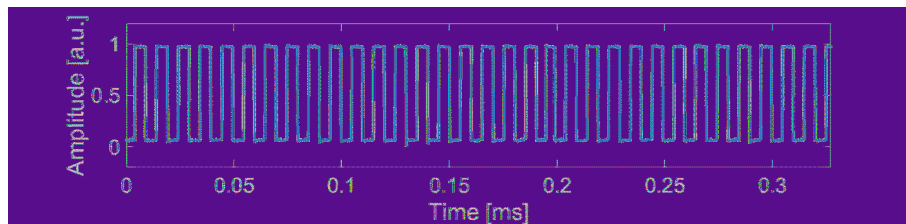


図 4.1 データ信号とクロック信号が含まれる漏えい電磁波を取得する実験環境



(a) SDA ラインに伝送されるデータ信号

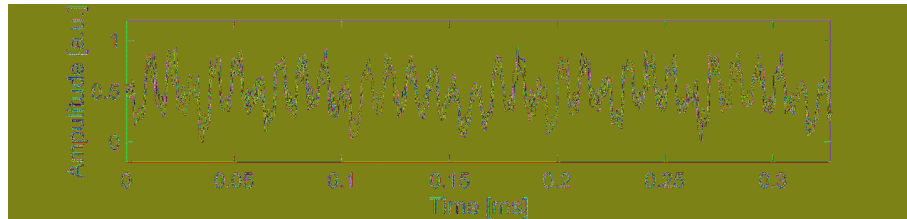


(b) SCL ラインに伝送されるクロック信号

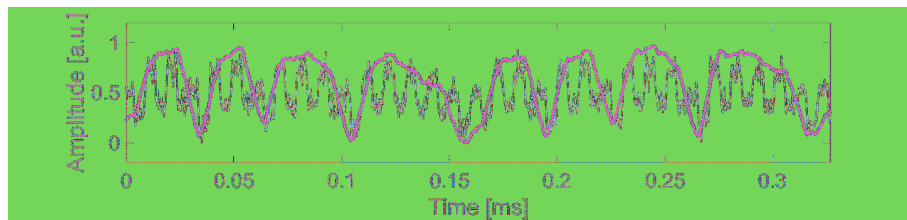
図 4.2 SDA ラインと SCL ラインの伝送信号

4.1.2 フィルタリングによるターゲット信号の取得

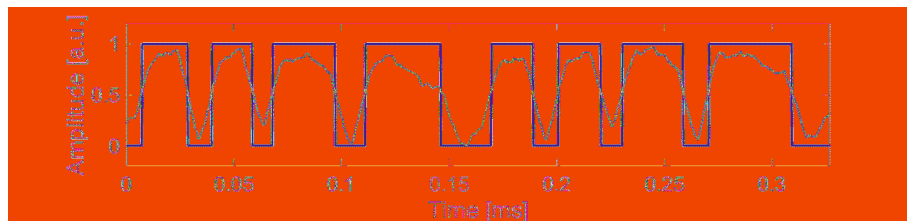
電磁波を注入することで強制的に漏えい電磁波を誘発させ、電流プローブにて観測された信号を図 4.3(a) に示す。この信号に対し、変調波に含まれる周波数成分の違いを利用することで、クロック信号の基本波成分を除去するフィルタリング処理を行った。フィルタリングした信号を図 4.3(b) に示す。フィルタリングする際に、クロック信号の周波数と漏えい電磁波受信時のサンプリング周波数を利用し、クロック信号の 1 周期間隔で移動平均による信号処理を施した。本実験では、漏えい電磁波のサンプリング周波数 4 [MHz] と除去したいクロック信号 0.1 [MHz] からフィルタの長さを 40 とし、クロック信号の 1 周期となる 10 [μ s] 間隔で他信号干渉ノイズを除去した。さらに、図 4.3(b) を二値化した結果を図 4.3(c) に示す。ターゲットとなる信号 図 4.2(a) と図 4.3(c) を比較すると、ターゲット信号に忠実な信号であることが確認できた。この結果より、データ転送レートから既知であるクロック周波数の情報を用いることで、クロック信号が除去でき、データ信号が取得可能であることを示した。



(a) 観測された漏えい電磁波



(b) 信号処理によりクロック信号を除去した信号



(c) 二値化信号

図 4.3 複数の情報を含む漏えい電磁波

4.1.3 移動平均によるクロック信号フィルタリングの考察

移動平均によるクロック信号のフィルタリングは、クロック信号の周波数と漏えい電磁波のサンプリング周波数が既知であることが条件であり、選択的にクロック信号を除去している。また、ジッタのような理想的な周波数からズレがある場合においても、フィルタには遷移域が存在することから、クロック周波数を抑制することが可能になると考えられ、データ信号が取得できる可能性がある。一方で、スペクトル拡散のように本来の帯域幅を上回る広い帯域幅にてクロック信号が使用された場合、移動平均によるフィルタリングではデータ信号の取得が困難であると考えられる。よって、クロック信号の周波数を一定値に固定しないことにより、電磁的

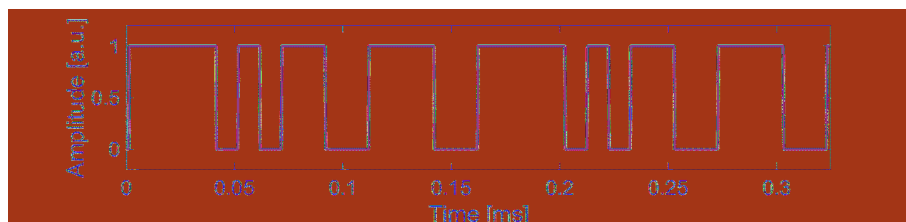
情報漏えいの対策ができる可能性がある。

4.2 複数のデータ信号が含まれる漏えい電磁波からのターゲット信号の取得

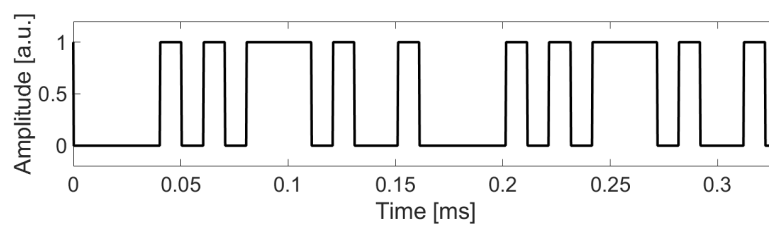
本節では、複数のデータ信号とクロック信号が含まれている系に着目し、MOS-FET へ伝達効率の良い照射周波数を選択することで、データ信号が取得可能であることを確認する。さらに、信号が混合している漏えい電磁波に対し信号処理を施し、伝送されているデータ信号に忠実な信号が取得できたことを示す。

4.2.1 複数の信号が含まれる漏えい電磁波を取得する実験環境

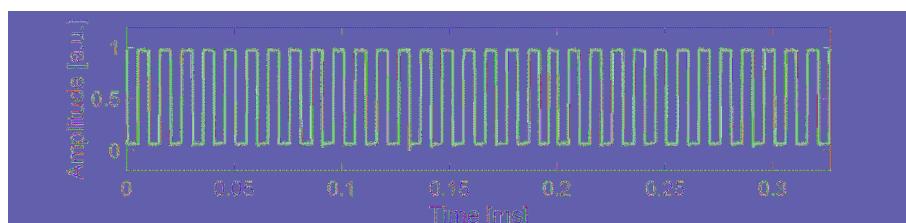
本実験では、複数の漏えい電磁波が誘発される場合において、回路構造や照射電磁波の伝達効率が異なることから、漏えい電磁波の放射強度が違うことに着目した。そして、効率の良い照射周波数を選択することで、取得可能となるデータ信号が異なることを確認するため、漏えい源が複数存在する環境を構築した。ここで、一般的な信号伝送方式として多く用いられる I2C 通信を模擬し、クロック信号とデータ信号が隣接して複数伝送される（本実験では 4 信号が伝送されている）、機器を評価対象とした。図 4.4 に、実験環境と使用した機器、設定したパラメタ、ターゲットとなるデータ信号 (0.1 [Mbps]) を図 4.5(a) 図 4.5(b) に、クロック信号 (0.1 [MHz]) を図 4.5(c) 示す。各信号は、マイコン (Cypress CY8C5888LTI-LP097) A から B へ伝送されており、伝送線路長は 8 [cm] とした。また、シグナルジェネレータ (Rohde & Schwarz SMA100B) によりアンテナによる遠方からの電磁照射、及び、SDR により漏えい電磁波を遠方から受信するアンテナを模擬し、照射電磁波の注入効率、及び、漏えい電磁波の測定の再現性を高めた。



(a) データ信号 1



(b) データ信号 2



(c) クロック信号

図 4.5 マイコン間の伝送信号

4.2.2 ターゲット信号が取得可能となった照射周波数

照射周波数を変化させ、漏えい電磁波を観測し、特定のデータ信号が取得可能となった照射周波数を図 4.6 に示す。縦軸は取得率、横軸は照射周波数を示している。取得率は、データ信号 1 パターン (16 bit) である 0.16 [ms] が含まれる漏えい信号を 3.0 [ms] 観測し、算出した結果である。この結果より、回路構造の差異により照射電磁波の伝達効率が異なり、周波数に応じて、取得信号が異なることを確認した。

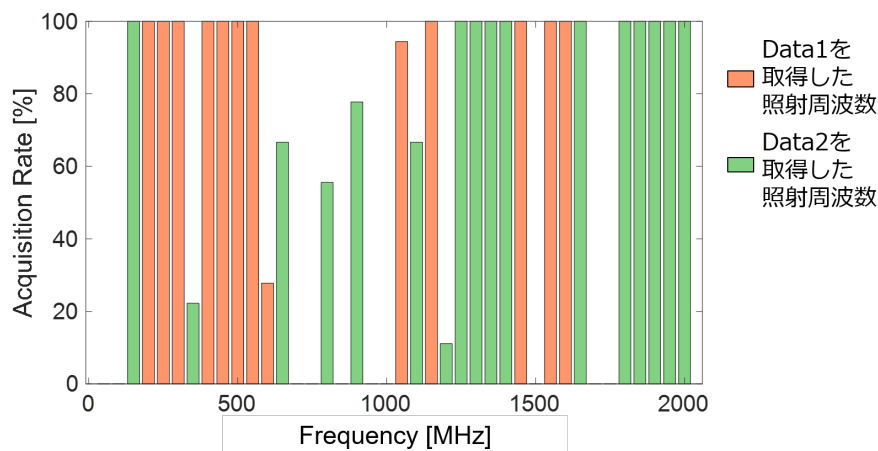
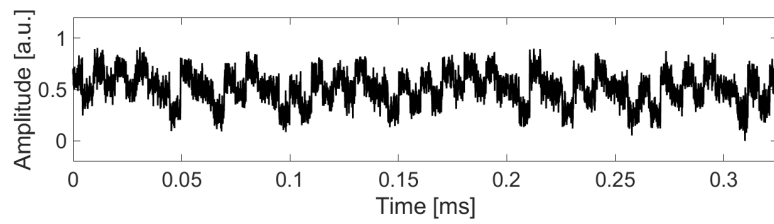
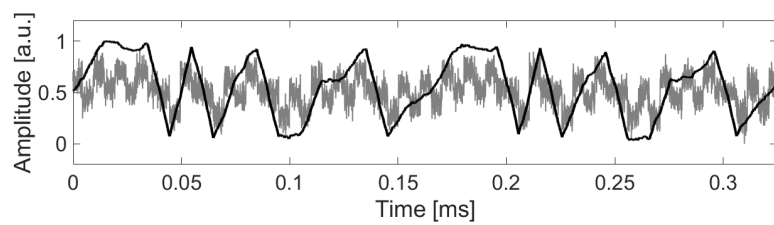


図 4.6 データ信号を取得した照射周波数

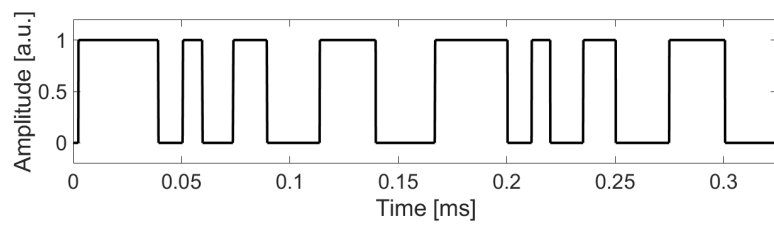
一例として、照射周波数 400 [MHz] (図 4.7)、1250 [MHz] (図 4.8) のときに取得した信号を示す。図 4.7(a) 図 4.8(a) は情報が混合した漏えい信号、図 4.7(b) 図 4.8(b) は 2.2 節で提案した信号処理によりクロック信号を除去し正規化した信号、図 4.7(c) 図 4.8(c) は二値化による処理を施した信号である。図 4.5(a) のデータ信号 1 と図 4.7(c) の漏えい電磁波から取得した信号 (照射周波数 400 [MHz]) また、図 4.5(b) のデータ信号 2 と図 4.8(c) の漏えい電磁波から取得した信号 (照射周波数 1250 [MHz]) をそれぞれ比較すると、ターゲット信号に忠実な信号であることが確認できた。



(a) 漏えい電磁波

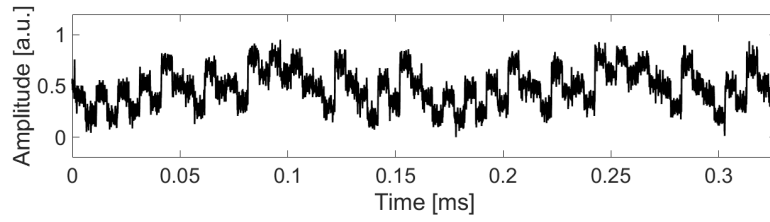


(b) 信号処理によりクロック信号を除去した信号

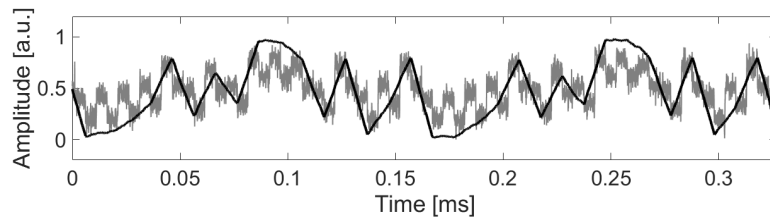


(c) 二値化信号

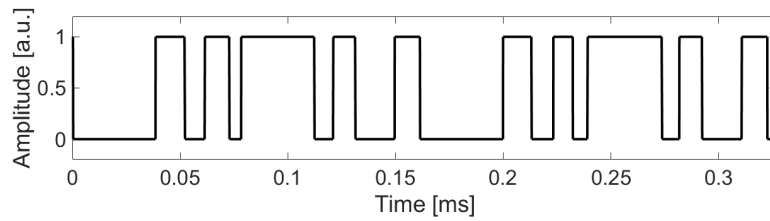
図 4.7 照射周波数 400 [MHz] の漏えい電磁波



(a) 漏えい電磁波



(b) 信号処理によりクロック信号を除去した信号



(c) 二値化信号

図 4.8 照射周波数 1250 [MHz] の漏えい電磁波

4.2.3 漏えい電磁波の放射強度の差異についての考察

図 4.6 の結果より、データ信号 1 が取得可能となった照射周波数は 200 [MHz] ~ 1600 [MHz]、データ信号 2 が取得可能となった照射周波数は 150 [MHz] ~ 2000 [MHz] の間であり、放射強度の差異により取得可能となるデータ信号が異なることが確認できた。各データ信号が伝送されている線路長に差異がないことから、IC 内部の構造や、電磁放射メカニズムの Source-Path-Antenna モデルにおける、Path と呼ばれる設計者の意図しない電気的かつ磁氣的結合が照射周波数に応じて異なり、放射強度に差異が生じると推察できる。また、本実験による複数の情報を含む漏えい電磁波からのデータ信号の取得は、放射強度に差異が生じることが条件であ

る。そのため、複数の漏えい電磁波の放射を同強度にすることで、電磁的情報漏えいの対策ができる可能性がある。

4.3 まとめ

本章では、実際の機器を模擬し、複数の信号が伝送されている系において、複数の漏えい電磁波が放射される環境を構築した。実際に他信号干渉ノイズとなるクロック信号をフィルタリングすることで、SNR を向上させ、複数の情報を含む漏えい電磁波からターゲット信号を取得できることを示した。具体的には周波数成分のスペクトルの違いに着目し、クロック信号を除去することで、SNR の向上を試みた。また、回路構造や照射電磁波の伝達効率の違いにより、漏えい電磁波の放射強度が変化することから、伝達効率の良い照射周波数を選択することで、ターゲット信号が取得可能となることを示した。その結果、漏えい電磁波が放射される環境下である、複数の伝送線路を有する機器から所望するターゲット信号が取得可能であることを示した。

第 5 章 結論

本論文では、電磁照射により機器から生じる非意図的な漏えい電磁波の強度を制御し、電磁的情報漏えいを強制的に誘発させる脅威に着目した。そこで、漏えい電磁波の SNR を低下させる要因である (1) 漏えいを制御するために照射する電磁波による自己干渉波と (2) 電磁照射より漏えいするターゲット以外の信号が含まれる漏えい電磁波を計測雑音と定義した。そして、この計測雑音を低減し、漏えい評価の精度向上を目的とした。

第 2 章では、SNR が低下するそれぞれの環境下において、計測雑音を低減する手法を提案した。具体的には、(1) 電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波が、計測雑音を増大させる環境下において、自己干渉ノイズの減少を目的とし、変調度を指標とした自己干渉波抑制手法を提案した。また、(2) 電磁照射により、ターゲット信号を含む漏えい電磁波と、ターゲット信号以外の情報を含む漏えい電磁波が誘発される環境下において、他信号干渉ノイズの減少を目的とし、漏えい電磁波の周波数や強度を指標とした他信号干渉ノイズをフィルタリングする手法を提案した。

第 3 章では、(1) 自己干渉ノイズが生じる環境を構築し、ノイズ低減の実験を行った。そして、自己干渉波抑制の実験において、自己干渉抑制信号を生成し自己干渉波の抑制を行い、漏えい電磁波の変調度が向上したことから自己干渉波抑制手法の有意性を示した。さらに、自己干渉波を抑制したことによりターゲット信号に忠実な波形が復元可能となったことを確認した。

第 4 章では、(2) 他信号干渉ノイズが生じる環境を構築し、ノイズ低減の実験を行った。複数の信号を含む漏えい電磁波からのターゲット信号取得の実験において、漏えい電磁波の周波数特徴に着目したフィルタリングを行い、他信号干渉ノイズを除去し、データ信号とクロック信号が混合している漏えい電磁波からデータ信号が取得可能であることを実証した。また、異なるデータ信号が混合している漏えい電磁波から特定のデータ信号が取得可能であることを示した。

以上の議論において、本論文では、強制的な情報漏えいの誘発手法により SNR が低下する環境下であっても、計測雑音の低減によって SNR を向上させることで、ターゲット信号が取得可能であることを示した。従来手法では、漏えい電磁波の

強度にのみに着目しており、情報漏えいが誘発されたか否かの評価のみが議論されていた。しかし、本論文で提案した手法により、計測雑音を低減させ SNR を向上させることが可能であることが示された。そのため、電磁的情報漏えいを強制的に誘発させる脅威の評価においては、背景雑音の強度変化も考慮すべきであると考えられる。

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。

主指導教員の林優一教授には、日頃の研究活動において丁寧かつ熱心な御指導、御鞭撻を賜りました。ここに心より感謝申し上げます。

副指導教員の岡田実教授及び安本慶一教授には、本論文の執筆にあたり有益な御助言・御討論を頂き、心より御礼申し上げます。

本研究室の藤本大介助教には、研究方針の策定や、研究活動においての丁寧かつ熱心な御指導、御助言を頂き、学会参加においても多大なご支援を頂きました。厚く御礼申し上げます。

本研究室の Youngwoo Kim 助教には、英文執筆を始めとする研究活動において様々な御支援、御助言を頂き、感謝申し上げます。

仙台高等専門学校の衣川昌宏助教には、実験の御指導から論文の執筆に至るまで様々な御助言を頂き、感謝申し上げます。

また、本研究室秘書の石谷由美様には諸手続きを始めとする様々な場面でお世話になりました。心より感謝申し上げます。

最後に、日ごろの研究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] Electromagnetic Compatibility (EMC) - Part 6-3: Generic Standards - Emission Standard for Residential, Commercial and Light-Industrial Environments, IEC Standard IEC 61000-6-3, 2006.
- [2] EMC requirements for telecommunication equipment - Product family Recommendation, ITU Standard ITU-T K.48, 2006.
- [3] International Telecommunication Union-Telecommunication Standardization Sector(ITU-T), “K.115: Mitigation methods against electromagnetic security threats, ” 2015.
- [4] Markus Guenther Kuhn and Ross. J. Anderson, “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations,” in International Workshop on Information Hiding, vol. 1525, Berlin, Heidelberg: Springer, pp. 124–142, 1998.
- [5] Wim van Eck, “Electromagnetic Radiation from Video DisplayUnits: An Eavesdropping Risk?,” Computers & Security, Vol.4, pp. 269–286, 1985.
- [6] Markus Guenther Kuhn, “Security Limits for Compromising Emanations,” Lecture Notes in Computer Science, CHES2005, vol. 3659, pp. 265–279, Aug 2005.
- [7] International Telecommunication Union-Telecommunication Standardization Sector(ITU-T), “K.84: Test methods and guide against information leaks through unintentional electromagnetic emissions, ” 2011.
- [8] Markus Guenther Kuhn, “Compromising emanations: eaves-dropping risks of computer displays,” University of Cambridge computer Laboratory, Technical Report, UCAM-CL-TR-577, 2003.
- [9] 林優一, 本間尚文, 三浦衛, 青木孝文, 曾根秀昭, “タブレット端末に対する電磁波を介した情報漏えいの脅威,” 2014 年暗号と情報セキュリティシンポジウム, 2A3-4, 2014-1-22.
- [10] Hidenori Sekiguchi and Shinji Seto, “Study on Maximum Receivable Distance for Radiated Emission of Information Technology Equipment Caus-

- ing Information Leakage,” IEEE Transactions on electromagnetic compatibility, vol. 55, no. 3, June 2013.
- [11] Toshihide Tosaka, Kunihiro Taira, Yukio Yamanaka, Atsuhiko Nishikata and Mitsuo 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.
 - [12] Cihan Ulas, Ulaş Aşık and Cantürk Karadeniz, “Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines,” Computers & Security Volume 58, pp. 250-267, May 2016.
 - [13] Martin Vuagnoux and Sylvain Pasini, “An improved technique to discover compromising electromagnetic emanations,” IEEE Symp. Electromagn. Compat., pp.121-126, Fort Lauderdale, FL, USA, July 2010.
 - [14] Martin Vuagnoux and Sylvain Pasini, “Compromising electromagnetic emanations of wired and wireless keyboards,” SSYM’09: Proceedings of the 18th conference on USENIX security symposium, pp. 1–16, August 2009.
 - [15] Yoshiki Kayano and Hiroshi Inoue, “Prediction of EM Radiation from a PCB Driven by a Connected Feed Cable,” IEICE TRANSACTIONS on Communications, vol.E92-B, No.6, pp.1920-1928, 2009.
 - [16] Yu-ichi Hayashi, Kouhei Ohmura, Takkaki Mizuki and Hideki Sone, “Influence of PCB and attached line of hardware on electromagnetic (EM) information leakage,” Electrical Engineering in Japan, Volume 182, Issue 4, 2012.
 - [17] 裕マーティン, 衣川昌宏, 藤本大介, 林優一, “意図的な電磁波注入による情報漏えいの制御に関する基礎検討,” 電子情報通信学会基礎・境界ソサイエティ/NOLTA ソサイエティ大会, pp.185, A-20-6, 2018.
 - [18] Masahiro Kinugawa and Yuichi Hayashi, “A Study on Feasibility of Electromagnetic Information Leakage Caused Forcibly by Low-Power IEMI,” Joint International Symposium on Electromagnetic Compatibility and

Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo, 2019.

- [19] 鍛冶秀伍, 藤本大介, 衣川昌宏, 林優一, “電子機器への連続波注入による強制的な電磁情報漏えいの誘発に関する基礎検討,” 電子情報通信学会 暗号と情報セキュリティシンポジウム, SCIS2020, 3E3-3, 2020.
- [20] 鍛冶秀伍, 衣川昌宏, 藤本大介, 林優一, “電磁的情報漏えいを誘発する照射周波数推定法に関する基礎検討,” 電子情報通信学会 ハードウェアセキュリティ研究会, vol.119, no.143, pp.235-238, 2019.
- [21] Newkirk, David and Karlquist, Rick, “Mixers, modulators and demodulators” . In D. G. Reed (ed.), The ARRL Hand-book for Radio Communications (81st ed.), pp. 15.1–15.36, Newington: ARRL. ISBN 0-87259-196-4, 2004.
- [22] NXP Semiconductors, “UM10204 I2C バス仕様およびユーザーマニュアル,” <https://www.nxp.com/docs/ja/user-guide/UM10204.pdf>, 2012.

発表リスト

- [1] 川上莉穂, 鍛冶秀伍, 衣川昌宏, 藤本大介, 林優一, “電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の抑制に関する基礎検討,” ハードウェアセキュリティ研究会, vol. 119, no. 2, HWS2019-6, pp. 31-35, 2019.4.12.
- [2] 川上莉穂, 藤本大介, 林優一, “複数の信号を含む漏えい電磁波からのターゲット信号の抽出に関する検討,” 電子情報通信学会ソサイエティ大会, A-20-5, 2019.9.12.
- [3] 川上莉穂, 藤本大介, 林優一, “電磁照射により意図的に生じた漏えい電磁情報の計測法に関する研究,” ハードウェアセキュリティ夏のワークショップ, 2019.9.26.
- [4] 川上莉穂, 鍛冶秀伍, 衣川昌宏, 藤本大介, 林優一, “複数のデータ伝送路を有する IC から強制的に引き起こされる電磁的情報漏えいに関する検討,” ハードウェアセキュリティフォーラム 2019, 2019.12.6.