ハードウェアに潜む電磁波セキュリティの脅威とその対策

Electromagnetic Information Security Threats
to Hardware and Their Countermeasures

林 優一 Yu-ichi HAYASHI

アブストラクト 情報セキュリティ確保に関する重要性が日々増大する中、上位レイヤにおけるセキュリティ確保と同様、物理層におけるセキュリティ確保の重要性も高まっている。近年の計測器の高精度化・低価格化、計算機の高速度化と記憶装置の大容量化に伴い、従来では技術的に困難だった高度な攻撃の脅威が増大しており、こうした脅威は軍事・外交分野のみならず民生品へと拡大している。本稿では、物理層におけるセキュリティの中でも、攻撃の痕跡が残りにくい、その脅威の検出が困難とされる電磁波を通じたセキュリティ（電磁情報セキュリティ）の問題に焦点を当て、民生用機器にも拡大している電磁波を通じた情報漏えいの脅威について解説するとともに、情報漏えいのメカニズム、そして、メカニズムに基づく上位レイヤのプロトコルやアプリケーションに依存しない情報機器全般に適用可能な漏えい情報の計測を困難化する対策手法を紹介する。

キーワード 電磁情報セキュリティ、サイドチャネル攻撃、物理セキュリティ、環境電磁工学

Abstract With the rising importance of information security, the necessity of implementing better security measures in physical as well as upper layers is becoming increasingly apparent. Given the development of high-accuracy, low-cost measurement devices, high-performance computers, and large storage devices, the threat of advanced attacks at the physical level has expanded from the military and government sectors to the commercial sector. In this paper, we introduce the problem of information security degradation through electromagnetic (EM)-based compromising of security measures in the physical layer (i.e., EM information security). Owing to the invisibility of EM radiation, such attacks can lead to serious threats. Moreover, we explain the mechanisms of EM information leakage and introduce countermeasures that make it difficult for information to leak. In particular, this study is focused on the countermeasures applicable to conventional information devices that do not depend on upper-layer protocols and applications.

Key words EM information security, Side-channel attacks, Hardware security, Electromagnetic compatibility

1. はじめに

電磁放射により情報漏えいが引き起こされる問題は、コードネーム TEMPEST⁽¹⁾として1950年代後半から主に米国を中心に軍事・外交分野において検討されてきた。そうした経緯から、電磁放射を用いた情報のモニタリングは高価かつ入手困難な機器を用いた政府レベルでのみ実現可能な攻撃であると広く信じられ、一般的な製品への脅威としてはみなされてこなかった。

これに対し、近年では、計測器の高精度化・低価格化、計

算機の高速度化と記憶装置の大容量化に伴って、電磁波を安価に長期間計測し、その計測データに統計処理等の加工を施すことが容易になったことから、こうした脅威は軍事分野から民生品へと拡大している。

具体的には、デスクトップ及びノートブックパーソナルコンピュータ（PC: Personal Computer）等のモニタ画面情報^{(2),(3)}、タブレットやスマートフォンの画面情報及び打鍵情報⁽⁴⁾、PC内部におけるCentral Processing Unit（CPU）の演算情報⁽⁵⁾、プリンタの印字情報⁽⁶⁾、キーボードの入力キー情報⁽⁷⁾、暗号処理を行うデバイス内の秘密鍵情報^{(8),(9)}の電磁波を通じた漏えいに関する脅威が報告されている。

電磁波を通じた情報漏えいの対策に関してはこれまでは図1に示すように、漏えい電磁波が攻撃者に到達するまでに、漏えい電磁波の強度を徐々に減衰させ、背景雑音以下にすることにより、攻撃者にターゲットとなる情報を含む漏えい電磁波の計測を困難化するゾーニングという対策手法がとられてきた。しかし、計測器の高精度化・低価格化、計算機の高

林 優一 正員 奈良先端科学技術大学院大学・先端科学技術研究科
E-mail yu-ichi@is.naist.jp
Yu-ichi HAYASHI, Member (Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma-shi 630-0192, Japan).
電子情報通信学会 基礎・境界サイエンス
Fundamentals Review Vol.13 No.1 pp.28-37 2019年7月
©電子情報通信学会 2019

図1 ゾーニングによる情報漏えい対策

図2 安価・小形なセットアップを用いて専門知識を有しない攻撃者により実行される攻撃

速化と記憶装置の大容量化に加えて、こうした装置が小形化、低消費電力化されたことにより、攻撃者は攻撃セットアップを持ち運びすることが可能となっている。そのため、図2に示すように、大掛かりな攻撃セットアップを設置することが困難だと想定されていたエリアまで攻撃者が侵入可能となったことから、図1に示したゾーニングによる対策のうち、壁や建物など空間における減衰に着目した対策は従来ほど効果を見込むことは難しくなっている。こうした背景により、今後は機器自身によるより強固な対策が求められると考えられる。

従来の攻撃対象として、上記に列挙した機器それぞれにおいて、内部で処理される情報や処理プロセスに着目した機器自身による対策手法が提案されているが、新たなデバイスが攻撃の対象となった場合、こうした対策手法を他の機器に拡張して適用することは難しい。

こうした状況を踏まえ、本稿では、民生用機器にも拡大している電磁波を通じた情報漏えいの脅威について解説するとともに、情報漏えいのメカニズム、そして、上位レイヤのプロトコルやアプリケーションに依存しない情報機器全般に適用可能な漏えい情報の計測を困難化する対策手法を解説し、電磁情報セキュリティ確保の一助となることを目的とする。

2. 電磁波を通じた機器からの情報漏えいの脅威

情報漏えいのメカニズムや対策手法を述べる前に、本章では電磁波を通じた情報漏えいの脅威について具体例を取り上げながら説明する。

攻撃セットアップの高精度化・軽量化・低消費電力化・低価格化などが進み、電磁波を通じた情報漏えいの脅威は軍事・外交分野から一般的な製品へと拡大している。本章ではこうしたセットアップを用いた攻撃の実行の可能性について検討する。また、本章では多くの民生用機器に対して攻撃が実行されることを想定し、攻撃者については「専門知識を有しない攻撃者」を想定する。

2.1 専門知識を有しない攻撃者による情報取得の可能性

漏えい電磁波を通じた情報の取得は大きく分けて「計測」と「解析」の二つのフェーズから成る。そして、これまでこうした情報取得に関しては、高度な専門知識を有する攻撃者が想定されてきた。この要因の1つとして、上述した二つのフェーズのうち、「計測」に関しては(1)攻撃者ごとに「計測」に用いる機器が異なり、また、その操作法が大幅に異なることや、(2)同一機種を用いた場合にも「計測」を行う際に用いるパラメータが大きく異なるため、電磁波を通じた情報取得を行う際に実行される「計測」には一定以上の知識や経験を有していることが条件であると考えられていたことが理由として挙げられる。

一方、ソフトウェアを用いて計測器間の差異を吸収するとともに、ネットワークで共有された計測パラメータをローカル環境でロードすることで、攻撃に必要な「計測」が完了すれば、従来攻撃の実行が困難と考えられてきた専門知識を有しない攻撃者によっても攻撃が実行される可能性がある。

そこで、次節では専門知識を有することなく「計測」を実施するために必要となるステップを完了できる可能性について検討する。

2.1.1 ソフトウェアを用いた計測環境の共通化

機器から放射される漏えい電磁波の計測は時間領域若しくは周波数領域で行われるが、これらの計測には帯域幅、サンプリング速度、トリガ、周波数帯、観測スパンなど、計測に関わる各種パラメータを適切に設定する必要があり、これらの値を適切に設定するためには専門的な知識が必要となる。また、計測器ごとにこれらの値を設定するための手続きやインタフェースが大きく異なっているため、操作を共通化することは難しいと考えられてきた。

これに対し、こうした計測器の操作を共通化するための Application Programming Interface (API) や Software Development Toolkit (SDK) の開発が進められており、こうしたラ

イブランチ群を上位のアプリケーションから利用することで、機種間の差異を吸収でき、複数の機器を制御可能なソフトウェアを開発することが可能となる。

例えば、ソフトウェア無線（SDR：Software Defined Radio）を計測器として用い、GNU RadioなどのSDKを用いることで、下層の計測器の違いを意識することなく、ソフトウェア側から計測パラメータを設定することができるとともに、計測で使用する変調方式を含む信号処理・信号の送受信などに関してもソフトウェアから制御可能となるため、攻撃に必要なハードウェア構成を自由に組み替え可能となる。そのため、上述したようなソフトウェアの差異を吸収するプログラムを事前にインストールした上で、攻撃プログラムをネットワークからダウンロードし、実行することでハードウェアへの攻撃に必要な計測が可能となる。

2.1.2 ブルートフォース的探索による漏えいパラメータ抽出

続いて本項では、機器制御に加えて「計測」を行うために必要となる諸パラメータ共有の可能性について述べる。これらのパラメータについては、計測後に行う解析と合わせて推定することが一般的であるが、前節で述べた手法を用いて計測環境を共通化し、多人数の専門知識を有しない攻撃者がバザール方式のハードウェアハッキングにより、ブルートフォース的に諸パラメータを抽出し、それらをネットで公開・共有することで、攻撃者自身が直接推定することなしにパラメータを利用することが可能となる。

例えば、スマートフォンなどのポータブルタッチスクリーンデバイスから放射される電磁波を計測して攻撃を行う場合、同一プロダクトが世界的に流通していることが多いため、攻撃に必要な諸パラメータが推定され、公開・共有された場合、同様の端末に対し、広い範囲で攻撃が実施される可能性がある。

2.2 安価なセットアップを用いた攻撃の具体例

本節では、専門知識を有しない攻撃者が2.1.1、2.1.2で述べた手順に従い、攻撃の実行が可能であることをタブレット端末への攻撃例を通じて示す。

図3に攻撃セットアップの概観を示す。本例では計測器として受信波をデジタルデータとして計測可能なSDRを用いている。図3に示すSDRはスーパーヘテロダイン受信方式となっており、受信電波を周波数変換して一定周波数の中間周波とし、中間周波増幅器で十分な増幅度と選択度をとった後に検波を行う。検波後の信号はデジタル信号に変換され、イーサネットを通じてIPパケットとして信号処理を行うPCに転送する。計測器と信号処理を行うPCはIPベースのネットワークで接続されているため、信号処理に計算リソースが必要になった場合には遠隔にある計算リソースを利用することも可能である。

受信部のアンテナは室内で地上波デジタル放送を受信する際に利用する市販の小形UHFアンテナを用いている。ま

図3 可搬性を有するセットアップ

図4 USBタイプの小形SDR

図5 可搬性を有するセットアップを用いて復元された表示画面

た、より安価な構成としては図4のようなUSBタイプのSDR チューナ受信機を用いることも可能性である。

続いて図5に図3を用い、タブレット端末に表示された画面とタブレット端末から放射された電磁波を用いて表示画面を復元した結果を示す。攻撃者は図3のセットアップを準備し、ネットワークからダウンロードしたという想定で準備した攻撃プログラムをPC上で実行する。このプログラムにより、攻撃に必要なパラメータが計測器に自動的に設定されるため、計測に必要な諸パラメータを把握する必要はない。また、本例では計測プログラムと解析プログラムが同一のプログラムとして構成されているため、プログラム実行後は「計測」＋「解析」の結果を直ちに取得することができる。

本セットアップの受信感度では、図1に示すようなターゲットとなる機器から十分離れた位置からの攻撃は困難であるが、図6に示すように攻撃対象との距離を数m以内に縮めることで、ターゲットとなる端末に表示されている情報を取得可能となる。

本章では、民生品へと拡大する電磁波を通じた情報漏えい

図6 ターゲット近傍におけるポータブルなセットアップを用いた攻撃

の脅威について、専門知識を有しない攻撃者が安価なセットアップを用いて実行する攻撃を想定し、その実現可能性について検討を行った。本章で示した攻撃セットアップはオンラインストアなどで容易に購入できる機器から構成されており、こうしたセットアップを用いた攻撃が現実実施される可能性は十分にある。

次章以降ではこうした攻撃を抑止するために、電磁波を通じた情報漏えいが発生するメカニズムと漏えいに基づく攻撃への対策について検討を行う。

3. 電磁波を通じた情報漏えいメカニズム

電磁波を通じた情報漏えいは、主として電子機器が処理するデータに応じて、機器内部で生成・伝送される電氣的な信号の時間変化に起因して発生する電磁放射によって引き起こされる。一般的に、情報通信機器から生じる電磁放射は、電磁両立性（EMC: Electromagnetic Compatibility）の観点から、そのレベルが規制されている。しかし、電磁波を通じた情報漏えいは、データに応じて時間的に変化する放射電磁波に起因することから、電磁波の強度が規格規制値以下の微弱な信号であっても引き起こされる可能性がある。

図7は電磁波を通じて情報が漏えいする様子を模式的に示している。漏えい源となる集積回路（IC: Integrated Circuit）がデータに応じて処理を行う際、情報を含む信号はその時間変化に対応した周波数成分を持つ。そして、そのうちアンテナとして振る舞う部位まで電磁結合を通じて伝搬した周波数成分、更に、アンテナの周波数特性にマッチした周波数成分が空間へ放出される。以降では上述したメカニズムによって機器外部に情報が漏えいする流れについて述べる。

3.1 電磁信号で表現されるターゲット信号

図7のターゲット信号は、漏えい対象となる情報を表す電磁信号を指す（本稿では、以後、電流、電圧、電磁波の時間的な振幅変動により表現される信号を総称して「電磁信号」と呼ぶ）。暗号モジュールを対象とした場合、暗号処理に応じて発生するサイドチャネル情報を表す電磁信号、ディスプ

図7 電磁波を通じた情報漏えいのメカニズム

図8 暗号モジュールから漏えいするサイドチャネル情報（時間領域）

図9 暗号モジュールから漏えいするサイドチャネル情報（周波数領域）

レイを対象とした場合はディスプレイを描画するために生成・伝送される電磁信号が対象となる。また、上述以外のターゲットに関しても同様である。

図8にターゲット信号の一例として代表的な共通鍵暗号の一つである Advanced Encryption Standard (AES)⁽¹⁰⁾ の処理実行時にその内部処理に応じて暗号モジュール外部に漏えいする電磁信号（暗号モジュールを対象にした場合はこの信号を「サイドチャネル情報」と呼ぶ）の時間領域波形を示す。攻撃者にとっては本情報を計測することができれば、秘密鍵を解読できる可能性があり、暗号モジュールを対象とした攻撃（サイドチャネル攻撃⁽¹¹⁾）ではここに挙げる電磁信号がターゲット信号となる。続いて、図8に示したターゲット信号を

周波数領域で示した結果を図9に示す。情報を取得する場合には、図9に示す周波数の変動を全て計測できることが望ましいが、ターゲット信号に含まれる周波数のうち特定の周波数成分が漏えいした場合でも、漏えいした周波数における振幅強度の時間変動が図8に示したターゲット信号の振幅の時間変動に対応する場合がある。このことから、攻撃者は自身が用意できる計測セットアップに合わせて、ターゲット信号が含む周波数を計測することで情報の取得が可能となる。

一方で、全ての周波数が機器外部に漏えいするわけではなく、外部に漏えいするまでに経る「カップリングパス」や「放射を引き起こすアンテナ構造」の持つ周波数特性によってフィルタされるため、こうしたフィルタを通過し、機器外部にまで到達した周波数を計測することで、ターゲット情報の取得が可能となる。

3.2 設計者の意図しない経路を伝搬して機器内に拡散されるターゲット信号

ターゲットとなる信号は機器設計者が意図して配置した線路や素子を伝搬して、機器の所望の機能を実現するが、設計者が意図しない経路にも伝搬する可能性がある。

図10(a)は隣り合う線路間に電界による結合が生じ、この結合を通じて本来は信号が本来伝送されるべき線路以外にもリークする様子を示している。こうした電界を通じた信号のリークは、結合した二つの線路間にキャパシタが生じたとみなすことができる。(以後、こうした結合を容量性のカップリングが生じたと呼ぶ。) また、図10(b)に示すように磁界による結合も同様に信号の漏れを近接する線路に引き起こす。磁界による結合は近接する線路をターゲットとなる信号

により生ずるが取り囲むことにより発生する。磁界を通じた信号の漏れは、結合した二つの線路間にインダクタが発生したとみなすことができる。(以後、こうした結合を誘導性のカップリングが生じたと呼ぶ。)

また、前記の例では図10に示したようにプリント基板上での結合を例に挙げ説明したが、電磁界を通じたカップリングはICチップなどの中でも発生することが知られており、これらに対しても同様の考え方を当てはめることができる⁽¹²⁾。

先述した寄生容量、寄生インダクタンスは周波数特性を持つことから、これらが周波数フィルタ的に振る舞い、**3.1**で図9に示したターゲット信号の周波数スペクトルの中から透過しやすい周波数が隣接する線路に漏れさせる。こうした漏れを繰り返しながら、**3.3**で説明する「意図しないアンテナ構造」に到達することで、機器外部に情報の漏えいが発生する。

3.3 非意図的なアンテナ構造からの情報の流出

3.2で概説したようにターゲットとなる信号は容量性・誘導性のカップリングを繰り返しながら本来ターゲット信号が伝搬する範囲を越えて、周辺の線路などに伝搬する。このとき、伝搬する信号は寄生キャパシタンス・寄生インダクタンスの持つ周波数特性に従って、オリジナルの信号から特定の周波数がフィルタされた状態で伝搬する。更に、漏えい信号が持つ周波数スペクトルのうち、漏えいした先の線路長などに共振する周波数は、その線路構造をアンテナとして機器の周囲に放射される。アンテナとして振る舞う部位は本来アンテナとして設計されたわけではなく、設計者の意図に反してアンテナと振る舞ってしまう部位(以後「非意図的なアンテナ構造」と呼ぶ)によって放射が発生する。

例えば、非意図的なアンテナ構造にはきょう体に接続された線路や基板ときょう体それを接続する線路、マザーボードとドーターボードそれを接続する線路などがある。そして、これらの物理長に共振する周波数がターゲット信号からカップリングを繰り返し、非意図的なアンテナ構造まで伝搬することで機器外部への放射が発生し、機器外部に情報が漏えいする。

ここで、図8に示したターゲット信号が異なるアンテナ構造に伝搬した際、周囲に放射される電磁界について検討する。図11にサイズが $200 \times 125 \text{ mm}^2$ のPCB基板とその基板に電源線を模擬した線路を50 cm、150 cmとして接続した場合、機器外部へ漏えいする信号の時間領域波形及び周波数領域波形を示す。機器内部で生成されたターゲットとなる信号のスペクトルは図8、図9に示すとおりであるが、ターゲットとなる信号源から非意図的な構造に到達するまでに**3.2**で示したカップリング時の周波数特性、非意図的なアンテナ構造の周波数特性が漏えいするターゲット信号の周波数特性を変化させている。例として、サイズが $200 \times 125 \text{ mm}^2$ のPCB基板と50 cm、150 cmがターゲット信号の周波数スペ

図10 カップリングを通じた信号の誘導

図 11 異なる物理構造を通じて漏えいするターゲット信号

図 12 非意図的なアンテナ構造の周波数特性

クトルに与える影響を図 12 に示す。

基板のサイズが同じ場合でも接続される線路長が変化すると非意図的なアンテナ構造の持つ周波数特性が変化し、この特性がカップリング時に変化した周波数特性を更に変化させることにより、機器外部に放射される漏えい信号の周波数特性が大きく変化して計測されることが分かる。

上記の例では基板サイズは一定とし、線路の長さを変化させたが、基板のサイズを変化させた場合もターゲット信号が機器外部に放出されるまでに受ける周波数特性の変化は基板のサイズによって大きく変化する。

4. 電磁波を通じた情報漏えい対策技術

本章では **3.** で述べた漏えいのメカニズムに基づき、漏えいを抑止するための対策について述べる。情報漏えい抑止についてはターゲット情報に特化した対策手法も数多く検討されているが、ここでは上位のプロトコルやアルゴリズムによらない対策法を紹介する。

4.1 ターゲット信号への対策

ターゲットとなる信号は上位レイヤにおけるプロトコルやアルゴリズムに依存して決定されるため、対策を施す際、信号を伝送する周波数を機器外部に漏れにくい周波数へ変更する対策や放射を弱めるために信号の強度自体を抑制する対策を適用することは難しい。そのため機器外部への信号の漏えいを抑止するためには後述する **4.2**, **4.3** で示す対策が有効であると考えられる。

一方、攻撃の中には機器の外部に漏えいする電磁波を計測し、情報を取得するもの以外に、IC パッケージなどを開封し、ターゲット信号を侵襲／非侵襲にプロービングする攻撃なども存在し、こうした攻撃に関しては機器外部への漏えいを抑止した場合においても情報を取得されるおそれがある。そこで本節ではこうしたターゲット信号に対して直接プロービングを行う攻撃に対する対策例を紹介する。

これまででも述べたように、電磁波を用いて情報を取得する攻撃は、「情報を計測するフェーズ」と「計測した情報を解析するフェーズ」に分けることができ、攻撃はこの順序に従って実行される。上述したターゲット信号を侵襲／非侵襲にプロービングする攻撃は「情報を計測するフェーズ」に相当し、このフェーズを抑止することで、後段で行われる「計測した情報を解析するフェーズ」の実行を阻止することが可能となり攻撃を無効化できる可能性がある。

「情報を計測するフェーズ」ではプローブを用い、ターゲット信号の時間変化に対応して変化する電磁界を計測する。電磁界の計測は、電界若しくは磁界をプローブにより検出することで行われるが、プローブが周囲の電磁界を侵襲せずに計測を行うことは物理法則上回避が極めて困難である。すなわち、ターゲット信号から生じた電磁界をプローブにより計測されているか否かを検知できれば、計測の困難性を限りなく高めることが可能になる。

プローブによる計測は一般的に対象となる電磁界を計測する際、図 13 に示すようにプローブと計測対象となる信号の周囲に電磁界の結合は発生する。これは **3.2** で述べた容量性、誘導性のカップリングが生ずるのと同じ現象である。こうして発生した寄生素子は機器の等価回路を変化させる。そのため、こうした等価回路の変化を検知可能な機構をターゲット信号の近傍に配置することにより「情報を計測するフェーズ」を抑止することができると考えられる。

ここで、上述した計測に伴う機器の等価回路を検出する具

図 13 プローブの接近により発生する電磁界結合

図 14 プローブの接近により変化する電磁界結合に応じて変化する発信器の周波数

体的な手法について示す。本例では暗号モジュールが動作する際、内部の暗号処理に応じて発生するサイドチャネル情報をターゲット信号とし、攻撃者が暗号モジュール内部をプロービングすることでその信号を計測する攻撃を対象とする。先述したようにこうした攻撃はプロービングによる寄生素子成分による等価回路の変化を捉えられれば検出可能となる。

攻撃検知の一例として、暗号モジュール内部に LC 発信器を実装し、その発信周波数の変化から攻撃を検知する手法が挙げられる⁽¹³⁾。このような検知手法ではプローブが近づくと暗号モジュール内部の LC 発信器自身、若しくはその周囲の回路と寄生結合が発生し、LC 発信器の発信周波数を決める L または C の値が寄生キャパシタンス、若しくは寄生インダクタンスによって変化し、発信周波数が図 14 に示すように攻撃によって変化する。この変化を捉えることでターゲット情報を計測するためにプローブが近づいてきていることが検出可能となる。

また、別の検知手法として基板上に定常的に分布する雑音の振幅変化を時間若しくは周波数領域で計測することで攻撃を検知する方法が挙げられる。図 13 はプローブ接近時に生ずる寄生結合を示しており、先述したようにこれはシステム内部の等価回路を変化させるが、別の見方をすると結合を通じてシステム側の電磁界がプローブ側に伝搬していると考えられる。そのため、ターゲット信号付近に定常的に分布する電磁界の強度変化を計測することで攻撃を検知でき

図 15 暗号モジュールから漏えいしたサイドチャネル情報

る可能性がある。

4.2 ターゲット信号の機器内拡散を抑止する手法

3.2 で述べたようにターゲットとなる高周波信号は電磁界を通じたカップリングにより、設計者の意図しない部位へ伝搬する。そして、この伝搬を繰り返しながら最終的には非意図的なアンテナ構造に到達し、機器外部へ放射される。そのため、機器外部への漏えいを抑止するための手法として意図しない部位に伝搬する高周波信号を特定の位置に閉じ込めるデカップリングが有効な対策手法として働く。本節ではデカップリングを用いた対策の具体例として、実装が容易で安価な素子であるキャパシタを用いた対策手法について説明する。

本例では、前節と同様に暗号モジュールから漏えいするサイドチャネル情報をターゲット信号とする。図 15 に暗号モジュールから漏えいしたサイドチャネル情報の分布を示す。この分布はサイドチャネル解析によって得られた基板上の相関値の分布を表したものとなっている。解析対象とした周波数帯は 0~500 MHz であり、相関値が高いほど、秘密鍵の解読が容易であることを表している。漏えいしたサイドチャネル情報は基板上のカップリングを通じて伝搬を繰り返し、暗号モジュールを実装した基板上に拡散している様子が分かる。図 15 に示す基板の下部には電源線が接続されており、その部位までサイドチャネル情報が伝搬した場合、電源線を非意図的なアンテナとし、機器外部に放射が発生する可能性がある。こうした漏えいに対し、本例ではターゲット信号がカップリングを通じて暗号モジュールの外部及び基板に拡散することを抑止するため、デカップリングコンデンサを用いてサイドチャネル情報を特定の範囲内に閉じ込める手法を紹介する。

デカップリングを行うために用いるコンデンサはターゲットとなる信号を閉じ込めたいエリアの周辺に実装を行う。その際、ターゲットの信号特性、IC の実装場所、周囲の線路の配線パターンなどに応じて、キャパシタの周波数特性、容量、実装する位置、個数などを決定する。なお、通常の機器設計においてデカップリングコンデンサを IC 周囲に実装することは機器動作を保証するために一般的であるが、これら

の実装は情報漏えいを防ぐためのものではない。本節では一般の機器設計で実装されるデカップリングコンデンサに加えて、情報漏えい抑制の観点からデカップリングコンデンサを追加し、情報漏えいを抑止する手法を示す。

図 16 に暗号モジュールが実装された IC の背面にデカップリングコンデンサを実装し、信号を特定のエリアに閉じ込めて基板への拡散を抑止した例を示す。図 17 は図 16 の対策を施した後の基板上的サイドチャネル情報の分布を示している。図 15 において基板に拡散していたターゲット信号は、図 17 において、IC 外部に伝搬していないことが確認でき、デカップリングコンデンサを通じてターゲット情報を特定のエリアに閉じ込めることに成功していることが分かる。

上述の例ではキャパシタの周波数特性及び容量を用いてターゲット信号を特性の領域に閉じ込める例を示したが、図のように線路間のカップリングによって信号が拡散する場合はカップリングの生じている線路の上に磁性材料の粉末が練り込まれた電磁波吸収シートなどを適用することで、カップリングを抑制し、ターゲット信号の拡散を抑止することも可能である。こうした電波吸収シートはデカップリングキャパシタに比べ、数百 MHz から数 GHz の広い帯域の信号のカップリングを遮断できる特性を持ち合わせており、漏えいを抑制したい信号の周波数成分が広帯域な場合、有効に働く。ただし、線路の上に設置するため、信号が伝搬する伝送路の特性に影響を与える可能性があることから、伝送線路のインピーダンスに与える影響を考慮した上で適用する必要がある。

また、図 17 の下部には基板に電源供給をするために接続された電源線があり、こうした線路にターゲット信号が伝搬

図 16 裏面へのデカップリングコンデンサの実装

図 17 デカップリングコンデンサの実装により抑制されたターゲット信号の基板への拡散

すると機器外部への放射が発生する。こうした基板から線路へのカップリングを抑止するために電源線などの機器に接続される線路上にフェライトコアを実装し、基板と線路を高周波的に分離することで接続線路を意図しないアンテナとした放射を抑制する対策も有効な手法である。

4.3 非意図的なアンテナ構造からの電磁放射の抑制

最後にターゲット信号を機器外部に漏えいさせるアンテナ構造への対策について説明する。前章でも述べたが、ここで言うアンテナ構造とは、Wi-Fi や Bluetooth などの通信に用いられる電磁波を機器外部に放射する「設計者が意図して設計したアンテナ」とは異なり、設計者がアンテナとして設計を行っていないにもかかわらず、意図せずしてアンテナとして動作してしまう部位を指す。

こうした非意図的なアンテナからの放射は図 7 に示した様にターゲット信号がカップリングを繰り返し、基板や機器に接続された伝搬し、伝搬した信号が伝搬した先の物理構造が共振し得る周波数を含んでいた場合、その構造がアンテナとして振る舞い機器外部への放射が発生する。

こうした潜在的にアンテナとして振る舞う部位への対策としては、機器設計時にそれが見つかった場合は、線路長などの物理的なサイズを変更し共振が発生しないような構造に変更するなどの対策や、4.2 で述べたようなターゲット信号が非意図的なアンテナ構造に伝搬することを抑止するような対策を適用することが有効である。一方で、機器が製造された後に非意図的なアンテナ構造が明らかになった場合は、施せる処置は設計段階で行える措置とは異なる。こうした場合、機器製造後にも後付けで適用できる対策手法が求められる。本節の後半ではこうした機器製造後に施す対策について具体的な例を挙げながら説明を行う。

図 18(a) に図 5 で示した機器外部に情報を漏えいさせている周波数のタブレット表面の強度分布を図示する。この漏えいでは描画信号の伝送を行う線路から周囲とのカップリングを通じて情報が漏えいし、ディスプレイの縁の金属導体をアンテナとして放射が発生している。一方、タブレット背面は金属で隙間なく覆われているため機器外部への放射はほとんど観測されていない(図 18(b))。そこで、本例はタブレット表面からの非意図的なアンテナを通じた電磁放射を抑制手法として「画面に対する電磁シールドの適用」について紹介を行う。

一般に電磁シールドは導体制の障壁で二つの場所を仕切って、二つの場所の間を電磁界が伝搬することを制限する電磁放射抑制手法である。シールド効果を上げるためには障壁を隙間なく導体で構成することが望ましいが、ディスプレイ表面にシールドを施す場合、その可読性を損なわないように対策を行う必要がある。そこで、メッシュ状の導体により構成されるシールド材を用い、画面の視認性を低下させずに周囲への電磁放射を抑止する手法を示す。

本例では、具体的なシールド素材として、透明なフィルム

(a) タブレット表面に分布する漏えい電磁界

(b) タブレット裏面に分布する漏えい電磁界

図 18 タブレット表・裏面に分布する電磁界

図 19 シールド素材を用いた対策手法の適用

に導体をメッシュ状に散布した透明導電膜を用いる (図 19 上)。また、タブレット端末で用いられるタッチスクリーンは一般に静電容量式となっている場合が多く、シールド材で画面を覆った場合タッチスクリーンからの入力ができなくなる可能性がある。そこで本稿では、画面とシールド材の間に図 19 下に示す光学的な情報漏えいを抑止可能な偏光フィルタを挿入し、タッチスクリーンとシールド材の距離を離すことで、画面との結合を低下させ、入力に影響が生じないように

(a) 対策手法の適用前 (b) 対策手法の適用後

図 20 対策手法の適用によって抑制される情報漏えい

にシールドを適用している。また、フィルタを挿入しても結合度の変化が十分得られない場合には、シールド材を構成するメッシュの荒さを変化させることで画面との結合度を弱めることが可能となる。本対策により視覚的にも電磁波的にも盗視を抑止する効果が得られる。

図 20 はタブレットにシールドを適用する前と後の 50 cm における画面盗視の結果である。シールド前では画面上のキーボードをはっきりと識別することができるが、シールド適用後は、漏えい電磁波が 50 cm の位置に到達する前に背景雑音以下のレベルに減衰しており、キーボードを識別することは困難であることが分かる。このように、漏えい周波数を大幅に減衰させるシールド材を適切に選択することで、視覚的・電磁的盗視への対策を行うことが可能となる。

上述の例は非意図的なアンテナ構造を覆う形でシールド構造を適用し、電磁波の放射を抑制したが、機器に接続された通信線や電源線などのフェライトコアが実装可能な構造においては、フェライトコアを実装することにより、前章で述べたようにカップリングを抑制する効果があるほか、共振することを抑制し、情報を含む電磁放射を低減できる可能性がある。

5. まとめ

本稿では、漏えい電磁波によるセキュリティ低下の脅威に焦点を当て、漏えい電磁波を通じた情報の取得において実行される「計測」と「解析」の二つのフェーズのうち主に「計測」について着目し、上位レイヤのプロトコルやアプリケーションに依存しない漏えい情報の計測の困難化を実現するために、攻撃が実施される可能性の検討、電磁波を通じた情報漏えいを「漏えい源」、「漏えいが周囲へ拡散するカップリングパス」、「機器外部へ放出されるアンテナ構造」の三つに分類し、漏えいが発生するメカニズムについて解説した。また、上述したメカニズムに基づき漏えい電磁波の「計測」を困難化する対策法についても解説した。

本稿では漏えい電磁波に対する脅威への対策手法として、計測を困難化する手法に着目したが、上位レイヤにおける対策手法も有効であることも多々ある。そのため、機器の設計者は、システム全体及び利用形態を俯瞰し、電磁波を通じた情報漏えいの危険性がどの程度あるのかを検討し、必要に応じて適切な対策を施すことが重要になる。理論的には情報が漏えいし得る対策であっても、機器が使用される状況、想定される攻撃者に対し、十分有効に働く場合もあり得る。ま

た、利用者側でも、そうした対策がきちんと取られている製品であるかどうかを意識していくことが今後重要になると考えられる。

謝辞 本稿の執筆にあたり、有益な議論や御指摘を頂きました、東北大学・電気通信研究所の本間尚文教授及び共同研究者の皆様に深く感謝致します。

文 献

- (1) R. Anderson, "Emission Security", in Security engineering, Chapter17, John Wiley & Sons, 2008.
- (2) M.G. Kuhn, "Compromising emanations of LCD TV sets," IEEE International Symposium on Electromagnetic Compatibility, pp. 931-936, Long Beach, USA, Aug. 2011.
- (3) H. Sekiguchi and S. Seto, "Estimation of receivable distance for radiated disturbance containing information signal from information technology equipment," IEEE International Symposium on Electromagnetic Compatibility, pp. 942-945, Long Beach, USA, August, 2011.
- (4) Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. 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'14), pp. 954-965, Scottsdale, USA, Nov. 2014.
- (5) Zajic and M. Prvulovic, "Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," IEEE Trans. Electromagn. Compat., vol. 56, no. 4, pp. 885-892, March 2014.
- (6) T. Tosaka, K. Taira, Y. Yamanaka, A. Nishikata, and M. Hattori, "Feasibility study for reconstruction of information from near field observations of the magnetic field of laser printer," 17th International Zurich Symposium on Electromagnetic Compatibility, 2006. EMC-Zurich 2006, pp. 630-633, Singapore, Feb. 2006.
- (7) M. Vuagnoux and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," IEEE International Symposium on Electromagnetic Compatibility, pp. 121-126, Fort Lauderdale, USA, July 2010.
- (8) D. Agrawal, B. Archambeault, R. Rao, and P. Rohatgi, "The EM

Sidechannel (s)," CHES 2002, Lect. Notes Comput. Sci., pp. 29-45, San Francisco, USA, Aug. 2002.

- (9) G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming channels : When electromagnetic side channels meet radio transceivers," Proc 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 163-177, 2018.
- (10) National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES), FIPS PUB. 197. [Online]," Nov. 2001, Available : <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- (11) S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks-Revealing the Secrets of Smart Cards, New York, Springer-Verlag, 2007.
- (12) M. Yamaguchi, S. Tanaka, Y. Endo, S. Muroga, and M. Nagata, "On-chip integrated magnetic thin-film solution to countermeasure digital noise on RF IC," Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC), pp. 536-539, 2015.
- (13) N. Homma, Y. Hayashi, N. Miura, D. Fujimoto, D. Tanaka, M. Nagata, and T. Aoki, "EM attack is non-invasive? -design methodology and validity verification of EM attack sensor," Cryptographic Hardware and Embedded Systems-CHES 2014, Lect. Notes Comput. Sci., Vol. 8731, pp. 1-16, Springer-Verlag, Sept. 2014.

(ISEC 研究会提案, 2019 年 3 月 31 日受付,
2019 年 5 月 5 日再受付)

林 優一 (正員)

2009 東北大学大学院情報科学研究科博士課程了, 奈良先端大先端科学技術研究科教授。情報セキュリティ, 環境電磁工学の研究に従事。IEEE EMC Society 電磁情報漏えいに関する分科委員会委員長 (第 5 技術委員会) IEEE, 電気学会, IACR, 情報処理学会各会員。博士 (情報科学)。暗号と情報セキュリティシンポジウムイノベーション論文賞 (2013, 2014, 2016), IACR CHES Best Paper Award (2014), RIEC Award (2014), IEEE EMC Best Symposium Paper Award (2013) 各受賞。