Computer Security Symposium 2017
23 - 25 October 2017

静電容量方式タッチパネルに対する敵対的な干渉の脅威

丸山 誠太[1,a)]　若林 哲宇[1,b)]　森 達哉[1,c)]

概要：静電容量方式のタッチパネルに能動的に干渉を行い，ユーザの意図しないタッチイベントを引き起こす攻撃手法を提案する．提案する攻撃手法は二つ存在する．第一の手法は，攻撃回路からタッチパネルに対して特定周波数の交流電流が印加されるように外部から電界を加えることでタッチイベントを引き起こす．第二の手法は，攻撃回路とタッチパネル間の静電容量を任意に変化させることでタッチイベントを引き起こす．それぞれの手法を実装し，複数台のスマートフォンを利用して評価を行った結果，本攻撃が実用的であることが明らかになった．また本攻撃と NFC を利用した攻撃手法を組み合わせることで，攻撃者による端末制御の奪取へと至る，新たな攻撃が可能になることを示す．さらに，本攻撃への有効な対抗手段について論じる．

キーワード：Touchscreen，False touch，NFC，Android，Trojan of Things

A Novel Class of Attacks against Capacitive Touchscreens

Seita Maruyama[1,a)]　Satohiro Wakabayashi[1,b)]　Tatsuya Mori[1,c)]

Abstract: We present two novel attacks against capacitive touchscreens, which are common in devices such as smartphones and tablet computers. The first attack, named *Touch Flood Attack*, scatters touch events, alternating the selection of buttons on a screen. The second attack, named *Electrical Touch Attack*, generates arbitrary touch events with the relay circuit. This paper describes the attacks as well as the experimental results that clarify the conditions for successful attacks. We also present countermeasures against our attacks.

1. はじめに

タッチパネルは携帯端末やパソコン，現金自動預け払い機など様々なデバイスに組み込まれ，日常的に利用されている．タッチを検出するための方式として，抵抗膜方式や超音波方式，静電容量方式など，複数の方式が実用化されており，それぞれの特徴に応じて使い分けられている．これらの検出方式のなかでも，静電容量方式のタッチパネルは，Apple 社の iPhone で採用されて以降，多くのスマートフォンに採用されている．

本論文は，静電容量方式のタッチスクリーンに対する攻撃手法を提案する．提案する攻撃手法は二種類存在する．一つ目の手法を *Touch Flood Attack*，二つ目の手法を *Electrical Touch Attack* と呼ぶことにする．Touch Flood Attack は，真のタッチ位置周辺に大量のタッチイベントを発生させ，実際にユーザがタッチしたボタンとは別のボタンがタッチされたとソフトウェアに誤認識させることを狙いとする．この手法ではスマートフォンの背面から攻撃することを想定している．一方 Electrical Touch Attack は，テーブルや机の天板に埋め込まれた攻撃回路が，回路に近接したタッチパネルの任意の位置にタッチイベントを発生させることで攻撃を行う．この手法では，攻撃回路がタッチパネル（タッチスクリーンの前面）に近接していることを前提とする．これらの攻撃手法と NFC を利用した攻撃手法を組み合わせることで，Android 端末の制御奪取へと至る攻撃が可能となる．この攻撃は，予め細工が施された机の上に，被害者が Android 端末をアンロックした状態で前面あるいは背面を下にして置くことによって発動する．

[1] 早稲田大学
Waseda University
[a)] maruyama@nsl.cs.waseda.ac.jp
[b)] wakabayashi@goto.info.waseda.ac.jp
[c)] mori@nsl.cs.waseda.ac.jp

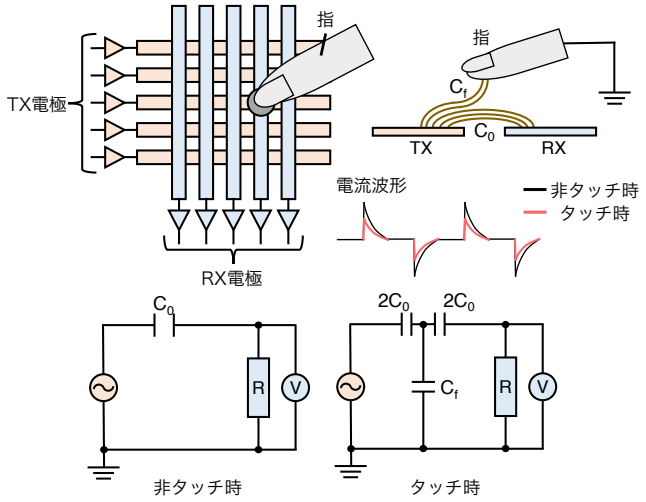

図 1 相互容量方式タッチパネルの原理図 [1,2]

本研究の貢献は以下のとおりである．

- 静電容量方式タッチパネルに対する能動的な攻撃手法，Touch Flood Attack（3 章）と Electrical Touch Attack（4 章）の提案及び実装を行った．
- 偽のタッチイベントである false touch が発生する条件を実験により突き止めた（3.2 節）．
- 真のタッチにより false touch の発生パターンが変化することを発見し，その原理を説明する仮説を提示した（3.3 節）．
- 市販の Android 端末 7 台（6 社）を用いた攻撃実現可能性の検証と攻撃成功条件の調査を行った（3.4 節）．
- タッチパネルに対する攻撃手法と NFC を利用した攻撃手法を組み合わせ，スマートフォン端末の制御奪取へと至る攻撃シナリオを考案した（5 章）．
- タッチパネルに対する攻撃の実現性を評価し，攻撃の対抗手段を提案した（6 章）．

2. 投影型静電容量タッチパネル

本章では投影型静電容量方式の検出方式のうち，マルチタッチを正確に検出できる相互容量方式について説明する．相互容量方式は，現在ほとんどのスマートフォンのタッチパネルに採用されている方式である [2]．**図 1** に示すように，相互容量方式のタッチパネルは，送信（TX）電極と，受信（RX）電極からなる．TX 電極と RX 電極は，それぞれの交点で容量結合している（図 1 中の C_0）．タッチパネルは TX 電極に交流電流を順次印加し，それをそれぞれの RX 電極で監視している．ある TX 電極と RX 電極の交点を指でタッチした時，指は容量 C_0 の間に割り込んで結合し（図 1 中の C_f），RX 電極に流れる電流が減少する（図 1 では便宜上 C_0 が等分割されている）[2]．それぞれの TX 電極と RX 電極の交点で，この電流減少を検知することでタッチパネルはタッチ位置を検出する．

静電容量方式タッチパネルは，スマートフォンの充電器やディスプレイが発するノイズで誤作動を起こすことが知られている [3]．この誤作動は以下のように分類される．

(1) *false touch*: ある座標について，実際にはタッチされていないのにタッチされていると認識する．
(2) *no-touch*: ある座標について，実際にはタッチされているのにタッチされていないと認識する．
(3) *jitter*: 実際にタッチされている座標の周辺座標がタッチされていると認識する．

タッチパネルメーカはこれらの誤作動について対抗手段を講じてきた．しかし，攻撃者により意図的に強力なノイズが印加された場合はどうであろうか．この着想をもとに，タッチパネルにノイズを印加し false touch（もしくは jitter）を生じさせる攻撃を考案した[*1]．この攻撃こそが Touch Flood Attack（3 章）である．

3. Touch Flood Attack

3.1 攻撃の概要

我々はスマートフォンの背面に設置した電極板に正弦波を印加することで，タッチパネルに false touch が生じることを確認した．この現象の原理は以下のように説明できる．スマートフォンの背面に設置された電極板がタッチパネルと静電容量結合する．電極板に交流電流が印加されると，電流の一部が RX 電極に流れこみ，RX 電極における電圧測定値が変化する．この測定値の変化により false touch が発生する．Touch Flood Attack はこの原理を利用し，真のタッチ位置周辺に false touch を大量発生させる．3.2 節，3.3 節では，この false touch が発生する条件や，発生パターンを調査した実験について述べる．

スマートフォンに確認ダイアログが表示されている最中に，Touch Flood Attack が実施されたとする．そして，この確認ダイアログの “NO” ボタンをユーザがタッチしたとする．すると，“NO” ボタンをタッチしたにもかかわらず，“YES” のボタンがタッチされたとスマートフォンが一定の確率で誤認識する．この誤認識率を市販のスマートフォンを用いて調査した結果について 3.4 節で述べる．

3.2 false touch が生じる条件の調査

外来ノイズにより false touch が引き起こされる条件を調べるため，我々は複数の実験を行った．実験には静電容量センサから直接，測定値を取得できるタッチパネルを用いた．本節では実験のセットアップと以下の 2 つの実験の詳細を述べる．最初の実験では，印加するノイズの電圧を変えつつ，周波数を掃引を行った．その結果，ノイズの電圧を大きくするとタッチパネルへの影響が大きくなること，特定の周波数のノイズがタッチパネルに大きな影響を与えることを発見した．次の実験では，この固有周波数をもつ

[*1] 本論文では false touch と jitter を区別せず false touch と呼ぶ

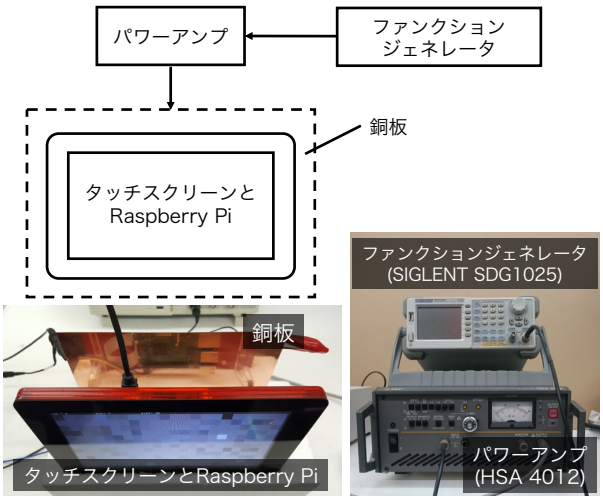

図 2　実験セットアップ

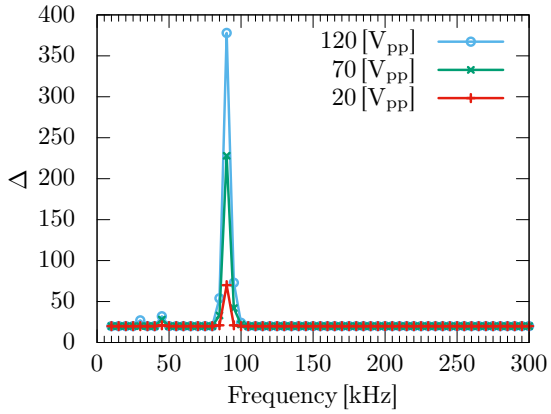

図 3　ノイズの周波数と電圧がタッチパネルに与える影響

ノイズを印加した際に生じる false touch の空間的なパターンについて調査した．これらの実験を行う中で，ノイズ印加中にユーザがタッチパネルに触れた場合，false touch の発生条件や発生パターンが変化する現象を発見した．この現象については 3.3 節で詳細に述べる．

実験セットアップ：実験セットアップを**図 2** に示す．本実験では，相互容量方式のタッチパネルとして Raspberry Pi 7-inch Touchscreen Display を使用した．このタッチパネルには静電容量センサの測定値を，そのまま外部に提供する動作モードがある．タッチパネルと静電容量結合させる電極板として銅板を使用した．この銅板はタッチスクリーンの背面側に，タッチパネルから 7 cm 離して平行に配置した．銅板に印加するノイズは，ファンクションジェネレータにより生成した正弦波をアンプリファイアにより昇圧することで生成した．このセットアップからも分かるように，Touch Flood Attack はタッチスクリーンの背面側から，すなわちスマートフォンの背面側から攻撃を行うことを想定している．

ノイズの周波数と電圧がタッチパネルに与える影響： 我々は異なる周波数と電圧を持つノイズを生成し，それらのノイズがタッチパネルに与える影響を調査した．ノイズがタッチパネルに与える影響を定量的に調査するには，影響の大きさを測るメトリックが必要となる．実験に使用したタッチパネルは 264 個の静電容量センサ（TX 電極 22 本 × RX 電極 12 本）を持つ．そのため測定ごとに 264 次元の時系列データを得ることができる．この測定値からノイズがタッチパネルに与える影響 Δ を以下のように定義する．

$$\delta_i = x_i - \bar{x_i}$$

$$\Delta = \max_i(\delta_i) - \min_i(\delta_i)$$

x_i $(i \in \{1, \ldots, 264\})$ は各センサの測定値を表し，$\bar{x_i}$ $(i \in \{1, \ldots, 264\})$ はノイズが印加されていない時の測定値を平均化した値を表す．x_i は測定の度に変化する変数である一方，$\bar{x_i}$ はノイズが印加されていない時の平均測定値を基に決定した定数である．我々はこのメトリック Δ を計算し記録するソフトウェアを開発した．このソフトウェアは毎秒 7 回，タッチパネルからセンサの測定値を取得し，Δ の表示と記録を行う．ノイズ非印加時には，タッチパネルに触れているものが何もない時，Δ は約 20 の値をとり，タッチパネルに指が触れている時，Δ は 250 以上の値をとる．そのため，ある電圧と周波数を持つノイズを印加した際に Δ の値が 250 を上回った場合，そのノイズは false touch を発生させると考えられる．

我々は銅板に印加するノイズの電圧と周波数を変えながら，Δ を計測した．ノイズの電圧は 3 パターン（20 Vpp，70 Vpp，120 Vpp）で，周波数は 5 kHz から 300 kHz の間で掃引した．**図 3** は本実験の結果を示している．我々はまず，90 kHz 付近に Δ の明確なピークがあることを発見した．この結果は特定の周波数のノイズがタッチパネルに影響を与えることを示している．この周波数は 3.4 節で明らかになるように，タッチパネルごとに固有のものである．また図 3 からは，ノイズの電圧を高くするとタッチパネルに与える影響が大きくなることが分かる．2 章で説明した通り，タッチパネルは RX 電極に流れる電流の減少によりタッチを検出する．そのため TX 電流を打ち消すことができる電圧と周波数，位相のノイズが，RX 電極に流れたときに false touch が発生するものと推測される．

false touch が生じた座標の可視化：我々は複数の周波数と電圧のノイズについて，ノイズにより発生する false touch の座標を個々に記録し，その分布を調べた．我々が本実験のために開発したソフトウェアは 30 秒の間，毎秒 2 回タッチパネルからタッチ座標を取得し，記録する．タッチパネルに何も触れていない状態で実験を行ったため，記録された座標はすべて false touch の座標である．使用したタッチパネルは 800×480 の解像度を持ち，10 点マルチタッチをサポートしている．そのため，サンプリングごとに最大 10 箇所のタッチ座標が報告される．銅板に印加したノイズは，電圧が 3 パターン（20 Vpp，70 Vpp，120 Vpp）と周

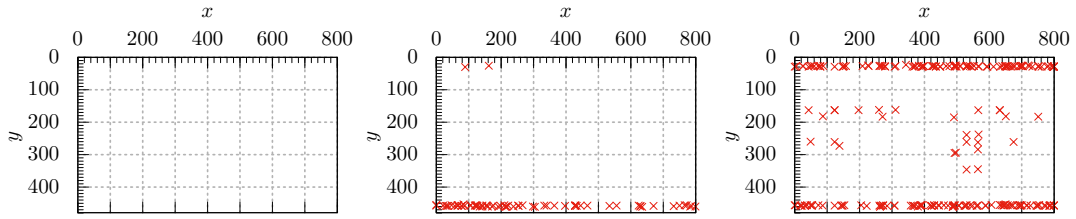

図 4　90 kHz ノイズ印加時に生じた false touch の分布．**左図：**20 Vpp，**中央図：**70 Vpp，**右図：**120 Vpp

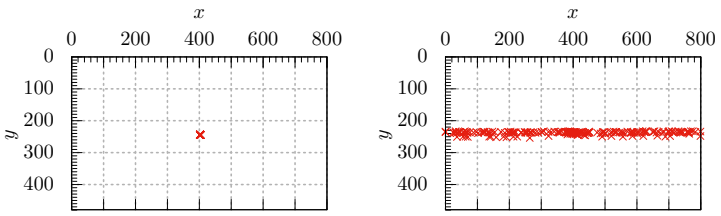

図 5　指でタッチパネル中央を触っている時のタッチイベント分布．
左図：ノイズ非印加時，**右図：**ノイズ印加時

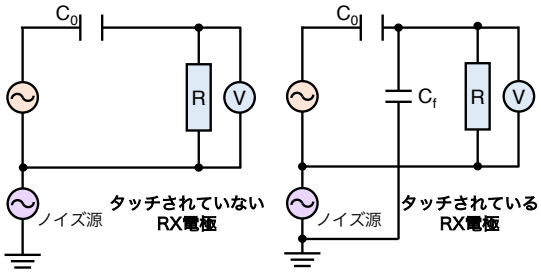

図 6　ノイズ印加時のタッチパネル動作原理図

波数が 2 パターン（60 kHz，　90 kHz）の 6 パターンである．60 kHz のノイズは，前実験（図 3）で Δ を上昇させなかった周波数の代表として，90 kHz のノイズは Δ を上昇させた周波数の代表として選択した．

実験の結果，予想通り 60 kHz のノイズは false touch を発生させなかった．そのため以降では 90 kHz のノイズを印加した際に生じる false touch の分布について述べる．**図 4** に 90 kHz のノイズを印加した際に生じた false touch の分布を示す．図 4 より 20 Vpp のノイズ印加時には，タッチパネルに false touch が発生しないことがわかる．また 70 Vpp，120 Vpp のノイズ印加時の false touch の分布から，高い電圧のノイズはより広範囲に false touch を生じさせることが分かる．しかしこれらの false touch の分布は，タッチパネルの上端と下端の直線上に集中している．このように偏った分布では，攻撃者が狙っている座標に false touch が発生する確率は低いと考えられる．

3.3　真のタッチによる false touch 発生パターンの変化

今までの実験では，タッチパネルに触れているものが何もない状況で false touch のパターンを調べてきた．しかし我々は，指でタッチパネルに触れた状態でノイズを印加すると，false touch の発生パターンが変化することを発見した．**図 5** は，指でタッチパネルの中央に触れている状況下で，20 Vpp，90 kHz のノイズを印加した際の false touch の発生パターンを示している．まず，指でタッチパネルに触れていなかったときと比べ，false touch を発生させるのに必要なノイズ電圧が低下していることが分かる．この 20 Vpp, 90 KHz のノイズは，タッチパネルに触れているものが何もない状況（図 4 の左図）では false touch を生じさせなかった．また図 5 より，false touch が真のタッチ座標を含む水平線上に集中して生じていること分かる．

何故真のタッチにより，低い電圧のノイズでも false touch が生じるようになるのか．何故図 4 の false touch 発生分布が，図 5 に示した分布へと変化するのか．そして何故，垂直線上でなく水平線上に false touch が集中するのか．これらの疑問に答える仮説を提示する．ノイズ印加時のタッチパネル動作原理図を**図 6** に示す．図 1 に示した原理図と異なり，駆動電圧源とアースの間にノイズ源がある．このノイズ源は，タッチパネルと静電容量カップリングした銅板に印加された交流電流によるものである．指でタッチパネルに触れていないとき，ノイズ源は RX 電極での電圧測定に影響を及ぼさない[*2]．なぜなら，図 6 左図に示すとおり，ノイズ源はタッチパネル回路全体の対地電圧を変化させるだけだからである（コモンモードノイズ）．一方で指でタッチパネルに触れているとき，ノイズ源は指で触れられている RX 電極での電圧測定に影響をおよぼす．なぜなら，図 6 右図に示すとおり，ノイズ源が人体の静電容量を通して RX 電極に接続され，ノーマルモードノイズが発生するためである．実験に使用したタッチパネルの RX 電極線が，図 5 の false touch が集中して発生している直線と平行に配置されているという事実は，この仮説を支持する．

この直線状の false touch 発生パターンは攻撃者にとって望ましいものである．なぜならばディスプレイ上に表示されるボタンは通常，一直線上に整列された状態で同時に表示されるからである．このようなボタンのペアとして，“YES ／ NO”，“OK ／ CANCEL”，“接続／キャンセル”

[*2] 指でタッチパネルに触れていないときでも一部のノイズはノーマルモードノイズに変換されるためタッチパネルに影響を及ぼす．ノイズ電圧が高ければ，一部のノイズだけでも十分高い電圧となるため図 4 では 20 Vpp のノイズでは false touch が発生せず，70 Vpp 以上のノイズでは false touch が発生したと考えられる．

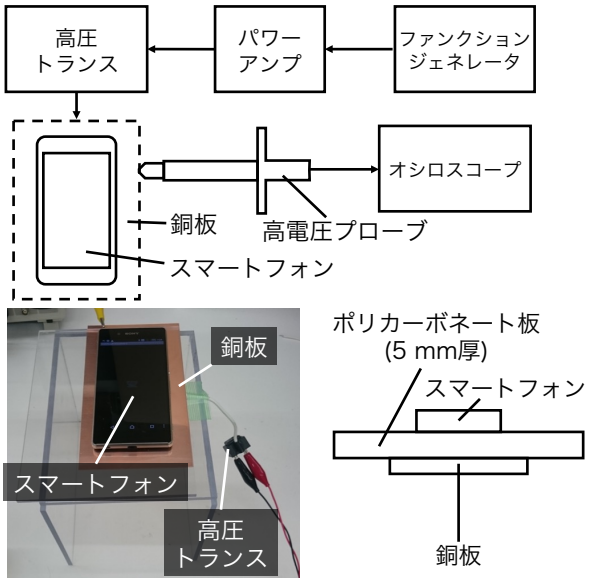

図 7　スマートフォンへの Touch Flood Attack の実験セットアップ

ボタンなどが挙げられる．真のタッチ座標を含む直線上に一様分布に従って false touch が大量に発生すると仮定すれば，ユーザが “NO” のボタンをタッチしたにもかかわらず，“YES” のボタンがタッチされたと認識される誤作動が 50%の確率で発生すると期待できる[*3]．Touch Flood Attack はこの誤作動の発生を狙いとした攻撃である．

3.4　市販のスマートフォンを用いた攻撃実現可能性の調査

本節では市販のスマートフォンを用いて，Touch Flood Attack の成功条件を評価した実験について述べる．実験の対象として，**表 1** に示す 7 機種の Android 端末を使用した．実験のセットアップを**図 7** に示す．ターゲットのスマートフォンと正弦波ノイズが印加される銅板は，5 mm 厚のポリカーボネートで絶縁されている．このセットアップでは図 2 に示したセットアップと異なり，アンプの出力をさらに高圧トランスを用いて昇圧している．これは，我々が使用したアンプの出力電圧の限界である 150 Vpp を越える電圧のノイズを生成するためである．高圧トランスは市販のプラズマボールから取り出したものを使用した[*4]．

我々はそれぞれのスマートフォンにタッチイベントを可視化するアプリをインストールした．次いで指でタッチパネルに触れながら，銅板に印加する正弦波の周波数と電圧を変化させた．そして目視により false touch が生じているか確認し，false touch を生じさせる周波数と電圧のペアを探した．また false touch が生じた機種に対しては，以下に述べる 2 つの追加調査を行った．

false touch 出現パターンの調査：false touch は一直線上に集中して出現する（図 5 右図）．この直線が水平線（horizontal）であるか垂直線（vertical）であるかを，画面の向きを縦向きに設定した場合を基準に調査した．

攻撃成功率の測定：我々は以下の試行を繰り返し，Touch Flood Attack の成功率を測定した[*5]．まず NFC タグを介して，Android 端末に Bluetooth ペアリングリクエストを送信する．端末にはペアリングの可否を問う確認ダイアログが表示される[*6]．この際 Android 端末は図 7 に示したように配置され，Touch Flood Attack の影響下にある．次いで指で，このダイアログ上の “NO” ボタンをタップする．Android が “NO” ボタンがタップされたと認識した場合を攻撃失敗，“YES” ボタンがタップされたと認識した場合を攻撃成功とする．なお 5 回タップの後，“YES”，“NO” どちらのボタンもタップされていないと認識された場合は攻撃失敗とみなす．なお，あらかじめ Android の画面の向きは，false touch の出現パターンが horizontal であれば縦向きに，vertical であれば横向きに設定した．

表 1 に調査結果を示す．我々は 7 機種中，5 機種に対して false touch を生じさせるノイズの電圧・周波数を特定した．その 5 機種のうち 3 機種について，約 50%の確率で攻撃が成功した．false touch が生じるものの攻撃が成功しない 2 機種は，以下のように false touch の出現分布が偏っていた．Nexus 9 はタッチパネル上の特定領域にのみ false touch が出現した．AQUOS ZETA SH-04F は真のタッチ座標がタッチパネルの右半分／左半分の領域であれば，左半分／右半分の領域に false touch が生じた．これらの結果から機種ごとに false touch の出現パターンが異なることが分かった．また false touch が生じなかった 2 機種についても，ノイズ印加時に以下のような不具合が生じた．Galaxy S 6 edge は，真のタッチ位置への追従が遅くなった．ARROWS NX F-05F はタッチを認識しなくなった．

3.5　攻撃実施への課題

Touch Flood Attack を実施するには，表 1 に示したようなパラメータの調査に加え，以下に列挙する前提条件が満たされる必要がある．5 章で述べる攻撃シナリオでは，これらの前提条件を満たすことができる．

C-1　Android 端末がアンロックされた状態で攻撃回路上に置かれていること

C-2　以下の端末情報が取得できること

- 機種（ex. Nexus 7, Galaxy S4, Xperia XZ, etc.）
- 画面の向きの設定（ex. 縦向き， 横向き）

C-3　端末が画面を上にした状態で置かれていること

C-4　攻撃対象のボタンが画面上に表示されていること

4.　Electrical Touch Attack

4.1　攻撃の概要

本章では，我々が Electrical Touch Attack と呼ぶ攻撃手

[*3] false touch が発生する直線上に，画面遷移を引き起こすような GUI 部品が “YES”，“NO” ボタン以外存在しない場合を仮定
[*4] 攻撃回路は高圧トランスと発振回路だけで安価に製作できる．
[*5] 成功率測定の様子を撮影した動画を Ref. [4] で閲覧できる．
[*6] この確認ダイアログを使用した理由は 5 章で明らかになる．

表 1　市販のスマートフォンを用いた Touch Flood Attack 実現可能性の調査結果

機種	製造者	false touch 発生	周波数 [kHz]	電圧 [Vpp]	攻撃成功率	false touch 発生方向
Nexus 7	ASUS	✓	128.2	40.0	18/30	vertical
ARROWS NX F-05F	FUJITSU		—	—	—	—
Nexus 9	HTC	✓	280.9	490.0	0/10	horizontal
Galaxy S6 edge	SAMSUNG		—	—	—	—
Galaxy S4	SAMSUNG	✓	384.5	70.4	13/30	horizontal
AQUOS ZETA SH-04F	SHARP	✓	202.0	700.0	0/10	horizontal
Xperia Z4	SONY	✓	218.0	340.0	20/30	horizontal

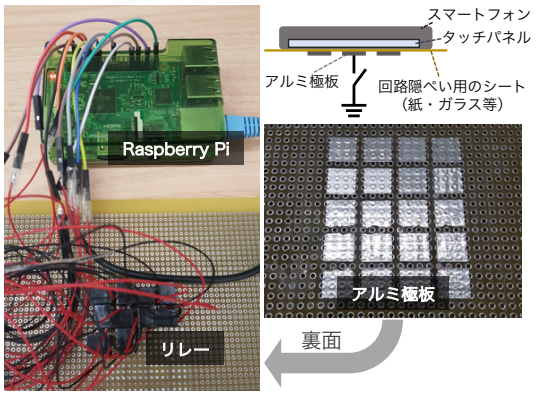

図 8　Electrical Touch 攻撃回路

法について説明する．この手法は，テーブルや机の天板に埋め込まれた攻撃回路が，近接したタッチパネルの任意の位置にタッチイベントを生じさせる．なおこの手法は，攻撃回路がタッチパネル（タッチスクリーンの前面）に近接していることを前提とする．我々が製作した，アルミ極板とリレーからなる攻撃回路を**図 8** に示す．この攻撃回路は以下のように動作する．アルミ極板がタッチパネルに近接し，静電容量結合する[*7]．この時，回路上のアルミ極板はリレーにより絶縁されている．次にアルミ極板のうちの一つをリレーによりグラウンドに接続する．グラウンドに接続された極板には，TX 電流の一部が流れるようになる．これはタッチパネルに指で触れた時，TX 電流の一部が指に流れることと同じである．グラウンドに接続する極板をリレーにより選択することで，攻撃者は任意の座標にタッチイベントを発生させることができるようになる．

攻撃回路（図 8）のアルミ極板は，一辺が 0.8 cm の正方形で，それぞれ 0.2 cm 離して配置されている．これらの極板のうち，ある一枚のアルミ極板をグラウンドに接続すると，その極板の中央の位置にタッチイベントが生じる．一方で，縦横に隣接するアルミ極板を二枚同時にグラウンドに接続すると，それらのアルミ極板の間の位置にタッチイベントが生じる．そのためこの回路は 0.5 cm 間隔で任意の座標にタッチイベントを発生させることができる[*8]．

[*7] 静電容量結合のため，攻撃回路を被害者から隠すためにアルミ極板の上に薄い紙などを被せても動作する．
[*8] この攻撃回路によってタッチイベントが発生する様子を撮影した動画を Ref. [4] で閲覧できる．

4.2　攻撃実施への課題

Electrical Touch Attack を実施するためには，前提条件 **C-1**，**C-2**，**C-4**（3.5 節）に加え，以下に列挙する前提条件を満たす必要がある．5 章で述べる攻撃シナリオでは，これらの前提条件も満たすことができる．

C-3'　端末が画面を下にした状態で置かれていること
C-5　攻撃回路に対する端末の相対位置が取得できること
C-6　攻撃対象のボタンの座標が分かること

5.　NFC を利用した攻撃シナリオ

本章では，Touch Flood Attack（3 章）や Electrical tocuh（4 章）によるタッチパネルへの攻撃手法がもたらす新たな脅威を，具体的な攻撃シナリオにより明らかにする．本章で提案する攻撃シナリオは，NFC 機能を持つ Android 端末を対象とした攻撃である Trojan of Things [5] と，タッチパネルへの攻撃手法を組み合わせたものである．5.1 節では，Trojan of Things について概要を述べる．Trojan of Things の詳細については Ref. [5] を参照されたい．5.2 節では，Trojan of Things とタッチパネルへの攻撃手法を組み合わせた新たな攻撃シナリオを提示する．

5.1　Trojan of Things

Android 端末を NFC タグにかざすと，**表 2** に示すように NFC タグに記録されているデータに応じて端末が様々な動作をする．Trojan of Things は，悪性 NFC タグを私達の身の回りのモノ—貨幣，洋服，机など—に埋め込むことで実装され，埋め込まれた悪性 NFC タグが偶発的に端末に読み込まれ，実行されることを狙いとする．

5.2 節で提示する攻撃シナリオでは，Ref. [5] で提案された **"複数の悪性レコードを使用した攻撃"** を利用する．この攻撃では，NFC タグエミュレータを利用することで，表 2 に示したような機能を次々と Android 端末に実行させることができる．これらの機能は，即時実行されるものと確認ダイアログを通してユーザの承認を求めるものの 2 種類に分類できる（表 2）．即時実行される機能を利用することで，3.5 節や 4.2 節で述べたタッチパネル攻撃手法実施への課題が解決される．また承認を必要とする機能については，タッチパネルへの攻撃手法により承認を突破することで利用できるようになる．このように Trojan of Things

表 2 NFC タグから利用できる Android OS の機能

動作	ユーザの承認
指定した URL をブラウザで開く	不要
指定したアプリを起動する	不要
指定した Google Play ストアページを表示する	不要
指定した内容でメールを送信する	必要
指定した Wi-Fi AP に接続する	必要
指定した Bluetooth デバイスとペアリングする	必要

```
1: アンロック状態のスマートフォンが置かれるのを待つ （C-1）
2: スマートフォンの端末情報を取得する （C-2）
3: if 端末が画面を上にして置かれている （C-3） then
4:     攻撃対象のボタンを表示させる（C-4）
5:     Touch Flood Attack を実施する
6: else（C-3'）
7:     攻撃回路に対する端末の相対位置を取得する（C-5）
8:     攻撃対象のボタンを表示させる（C-4），（C-6）
9:     Electrical Touch Attack を実施する
10: end if
```

図 9 攻撃シナリオの擬似コード

とタッチパネルへの攻撃手法を組み合わせることで，端末の制御奪取へと至る新たな攻撃が可能となる．

5.2 攻撃シナリオ

本節で提示する攻撃シナリオは NFC 機能が有効になっている Android 端末をターゲットとする．このシナリオでは攻撃者が事前に，タッチパネル攻撃回路，NFC カードエミュレータ，制御用のシングルボードコンピュータからなる攻撃デバイス（以下 “ToT Device” と呼ぶ）を，机の天板に埋め込むことを想定する．タッチパネルへの攻撃実施の前提条件（3.5 節，4.2 節）を満たしていれば，以下の手順で端末制御を奪取できる．ToT Device は NFC を介し Bluetooth ペアリング確認ダイアログをターゲット端末に表示させる．Touch Flood Attack もしくは Electrical Touch Attack により，確認ダイアログの “はい” ボタンをタップする．これによりターゲット端末は ToT Device がエミュレートしている Bluetooth マウスとペアリングする．攻撃者は NFC を介し，任意の悪性アプリのストアページを端末に表示させ，ペアリングした Bluetooth マウスを使ってアプリのインストールに同意する．

タッチパネルへの攻撃手法を実施するまでの ToT Device の動作を擬似コードで**図 9** に示す．ToT Device の各動作により，3.5 節もしくは 4.2 節に述べた攻撃実施の前提条件が満たされる（図 9 括弧内参照）．以降では，これらの前提条件がどのように満たされるのか順次詳細に説明する．

（C-1） Android 端末がアンロックされた状態で攻撃回路上に置かれていること： スマートフォンの NFC 通信可能距離はおよそ 5 cm 以下である [5]．ToT Device はターゲット端末が発する NFC 搬送波を検知することで，**C-1** が満たされていることを確認できる．

（C-2） 端末の機種，画面の向きの設定が取得できること： ToT Device は NFC を介して，攻撃者が用意したウェブページを端末に開かせることができる．このウェブページにより以下の情報を取得し，ToT Device に通知できる．

- 機種（ユーザエージェントから取得 [6]）
- 画面の向きの設定（Screen Orientation API から取得）
- Android のバージョン（ユーザエージェントから取得）
- 言語設定（Accept-Language HTTP header から取得）

なお，Android のバージョンと言語設定は **C-6** を満たすために取得した

（C-3 ／ C-3'） 端末が画面を上／下にした状態で置かれていること： C-1 と **C-2** により満たされる．**C-2** が満たされていれば，端末の機種がわかる．NFC 通信可能領域が端末の裏面／表面にしかない機種であれば，**C-1** より端末が画面を上／下にした状態で置かれていることがわかる．NFC 通信可能領域が端末の両面にある機種の場合は以下のようにして端末の置かれた状態を判別する．Electrical Touch Attack 攻撃回路により，端末にタッチイベントを発生させようと試みる．ToT Device は NFC を介して開かせたウェブページを使い，タッチイベント発生の有無を確認する．タッチイベントが発生した場合，端末は画面を下にした状態で置かれている．発生しなかった場合，端末は画面を上にした状態で置かれている．

（C-4） 攻撃対象のボタンが画面上に表示されていること： 本攻撃シナリオで攻撃対象となるのは，Bluetooth ペアリング確認ダイアログと Google Play ストアページ上のボタンである．ToT Device は NFC を介して，これらのボタンを端末に表示させることができる．

（C-5） 攻撃回路に対する端末の相対位置が取得できること： C-3' により満たされる．Electrical Touch 攻撃回路（図 8）により，端末のどこか二箇所にタッチイベントを発生させようと試みる．ToT Device は NFC を介して開かせたウェブページを利用し，発生したタッチイベントの座標を取得できる．二箇所のタッチイベントの座標と，タッチイベントを引き起こした攻撃回路上の極板の位置から，攻撃回路に対する端末の相対位置が取得できる．

（C-6） 攻撃対象のボタンの座標が分かること： C-2，**C-4** により満たされる．攻撃対象となるボタンは，Bluetooth ペアリング確認ダイアログや，Google Play ストアページ上のボタンである．ボタンの表示位置は機種や画面の向き設定，OS のバージョン，言語設定により異なるが，これらの情報は **C-2** 情報取得時にウェブページから取得できる．

6. 議論

6.1 脅威の評価

Touch Flood Attack は過半数のスマートフォンに false touch を生じさせることに成功した（3.4 節）．false touch

の生じた 5 機種中 3 機種の false touch 発生パターンは攻撃者にとって望ましいものであった．また Elecrical Touch Attack（4 章）は原理上，全ての静電容量方式のタッチパネルに対し有効である．5 章ではこれらの攻撃手法を利用した NFC 搭載 Android 端末の制御奪取へと至る攻撃シナリオ示した．この攻撃シナリオの脅威を評価するため，我々は Android ユーザ 300 人を対象にインターネット調査を行った．この調査により以下の 3 点が明らかになった．

(1) Android 端末の約 71%が NFC 機能を搭載している．
(2) NFC 機能搭載端末ユーザの 40%が常に NFC を有効にしている（分からないと回答したユーザを除く）．
(3) Android ユーザの約 39%がテーブル・机に着席している際に，ロックを解除した状態でスマートフォンをテーブル・机の上に置く

これら 3 点のうち，(1) NFC 機能搭載率と (2) NFC 機能有効設定率は今後増加していくと考えられる [5]．(3) より，5 章で述べた攻撃シナリオは，NFC 機能搭載端末ユーザの約 4 割に対し脅威となることが分かった．このことから本論文で提案した 2 つの攻撃手法及び攻撃シナリオは，静電容量方式のタッチパネルを搭載したデバイスに対する現実的な脅威であると結論付けられる．

6.2 対抗手段

本節では静電容量タッチパネルに対する干渉攻撃への対抗手段について論じる．Touch Flood Attack や Electrical Touch Attack は静電容量方式のタッチパネルを対象にした攻撃である．つまり，他のタッチ検出方式であれば攻撃の影響を受けない．そのため静電容量方式の利点を活かしつつ，攻撃の影響を受けないようにするには，静電容量方式を他のタッチ検出方式（抵抗膜方式等）と組み合わせれば良い．他の検出方式でタッチが検出されないにもかかわらず，静電容量方式でタッチが検出されれば，干渉攻撃を受けていると判断し，一時的に静電容量方式によるタッチ検出を無効にすることで攻撃に対処できる．検出方式を組み合わせたタッチスクリーンを採用しているデバイスとして，Samsung 社の Galaxy Note が挙げられる [2]．このデバイスは，指による操作と専用ペンによる細かい操作を両立させるため，静電容量方式と電磁誘導方式を組み合わせたタッチスクリーンが採用されている．

また Touch Flood Attack に関しては，特徴的な false touch の出現パターンを識別することで，対処することができる．タッチパネルの通常使用において図 5 右図のような，多数のタッチイベントが直線状に発生することは考えづらい．そのためタッチイベントの出現パターンから，干渉攻撃を受けていると判断することができる．

Android 端末へのタッチパネルへの干渉攻撃の脅威は，NFC 機能の実装を改善することで軽減される．5.2 節で提案した攻撃を可能にしたのは NFC 機能により漏えいしたデバイスの各種情報である．この情報漏えいは NFC によるブラウザの起動の際，ユーザの承認を求めるように Android OS の動作を変更することで防ぐことができる．

7. 関連研究

これまで複数のタッチパネルへの攻撃手法が考案されてきた．Aviv ら [7] は，タッチパネルに残された皮脂汚れから，スマートフォンのパスワードを推測することが可能であることを報告した．Maggi ら [8] は監視カメラの映像から，林ら [9] はスクリーンから漏洩する電磁波から，タッチスクリーンキーボードの入力内容を不正に入手する攻撃が現実的であると示した．上述の通りタッチスクリーンから受動的に情報を盗み出す攻撃手法は複数提案されている．一方で我々の知る限り，タッチスクリーンへの能動的な干渉による攻撃手法を提案したのは，本研究が初めてである．

8. まとめ

本研究はタッチスクリーンへ電磁干渉しスマートフォンを攻撃する新たな攻撃手法を提案し，実験により攻撃手法のメカニズムや発生条件を明らかにした．さらにこの攻撃手法と NFC を利用した攻撃手法と組み合わせた，端末制御の奪取へと至る攻撃シナリオを提示し，その脅威を評価した．加えて，これらの攻撃に対する複数の対抗策を示した．

参考文献

[1] Hattori, R.: touch panel, http://www.astec.kyushu-u.ac.jp/hat-lab/FPD/TouchPanel.pdf (2016).
[2] 越石健司：タッチパネル = Touchscreen : 技術開発・市場・アプリケーションの動向，オーム社 (2012).
[3] Klein, H. W.: Noise Immunity of Touchscreen Devices, http://www.cypress.com/file/120641/download (2013).
[4] Maruyama, S.: TouchFlood, http://nsl.cs.waseda.ac.jp/touchflood/.
[5] 丸山誠太， 星野遼， 森達哉：Trojan of Things: モノに埋め込まれた悪性 NFC タグがもたらす脅威の評価，コンピュータセキュリティシンポジウム 2016 論文集, Vol. 2016, No. 2, pp. 458–465 (2016).
[6] WhichBrowser: WhichBrowser/Parser-PHP: Browser sniffing gone too far — A useragent parser library for PHP, https://github.com/WhichBrowser/Parser-PHP.
[7] Aviv, A. J., Gibson, K. L., Mossop, E., Blaze, M. and Smith, J. M.: Smudge Attacks on Smartphone Touch Screens., *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT 2010)*, pp. 1–7 (2010).
[8] Maggi, F., Gasparini, S. and Boracchi, G.: A fast eavesdropping attack against touchscreens, *Information Assurance and Security (IAS), 2011 7th International Conference on*, IEEE, pp. 320–325 (2011).
[9] Hayashi, Y., Homma, N., Miura, M., Aoki, T. and Sone, H.: A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, ACM, pp. 954–965 (online), DOI: 10.1145/2660267.2660292 (2014).