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

丸山 誠太[1,a)]　星野 遼[1,b)]　森 達哉[1,c)]

概要：NFC タグと呼ばれる小型機器にスマートフォンをかざすだけで，スマートフォンの様々な機能を利用できる．NFC の通信可能距離の短さゆえ，ユーザの意思に反してスマートフォンが NFC タグが近接してしまう危険性はこれまで十分に論じられてこなかった．しかし，NFC タグが私達の身の回りのモノに埋め込まれていた場合はどうであろうか．本論文では Trojan of Things という新たな脅威を定義し，その具体例として，貨幣型トロイ，ウェアラブルトロイ，家具型トロイなる新しい概念の攻撃が実現可能であることを示す．さらに，NFC が提供するユーザビリティを損なう事なく攻撃を防ぐ手段を提案する．

キーワード：NFC, Android, Trojan of Things

Trojan of Things: Understanding the threats of malicious NFC tags embedded in the things

Abstract: NFC tag is a small chip that enables short-range wireless communication with mobile devices. By just holding up a smartphone against a pre-programmed NFC tag, it can launch many functionalities of smartphone such as opening an URL with web browser, configuring Wi-Fi network, etc. Due to the limitation of short-range wireless communication of NFC technology, not much security threats and their countermeasures have been discussed so far. However, what will happen if maliciously programmed NFC tags are embedded into things around our lives? Given the background, this work proposes a new proof-of-concept attack called “Trojan of Things”. As concrete examples of the Trojan of Things, we implement three different types of attacks: “currency trojan”, “wearable trojan”, and “furniture trojan”. We demonstrate that these attacks are feasible in the real world. We also evaluate the conditions of the successful attacks with respect to the distance between a targeted mobile device and an NFC trojan using 18 different models of smartphones developed by 11 different manufactures. We also present effective countermeasures against the threats of the Trojan of Things without sacrificing the high usability of NFC tags.

Keywords: NFC, Android, Trojan of Things

1. はじめに

NFC (Near Field Communication) は通信可能距離が 10 cm 程度の近距離無線通信技術である．スマートフォンの NFC 搭載率は年々増加傾向にあり，2018 年に出荷されるすべてのスマートフォンの 2/3 が NFC を搭載すると予想されている [1]．NFC は事前の認証処理を経ることなく，NFC 対応機器同士を近づけるだけでデータの交換を実現する．NFC が提供する高いユーザビリティはスマートフォンと現実世界のモノをシームレスにつなぐ役割を果たす．例えば，IC チップとアンテナを搭載した NFC タグとよばれる小型の紙片のような機器にデータを記録しておけば，そのタグにスマートフォンをかざす動作だけでタグからデータを取り出し，任意のアプリケーションを起動したり，ネットワークの接続設定をしたりすることができる．NFC タグの用途は様々であり，例えばタグを内蔵したスマートポスターが広告や情報配信サービスを行うメディアとして利用されている [2]．

スマートフォン向け OS である Android はバージョン

[1] 早稲田大学
Waseda University
[a)] maruyama@nsl.cs.waseda.ac.jp
[b)] hoshino095@nsl.cs.waseda.ac.jp
[c)] mori@nsl.cs.waseda.ac.jp

2.3 から NFC をサポートしている．Android 端末を NFC タグにかざすと，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．動作の例を以下に挙げる．

- 指定した URL をブラウザで開く
- 指定したアプリを起動する
- 指定した宛先，件名，本文のメールを送信する
- 指定した Wi-Fi ネットワークに接続する
- 指定した Bluetooth 機器とのペアリングを行う
- NFC 対応アプリにインテントを送信する

これらの機能を利用し，端末に悪意のある動作をさせることを意図したデータが記録された NFC タグを，本論文では悪性 NFC タグと呼称する．

スマートフォンと NFC タグをつけたモノがもたらす高い利便性の一方で，悪性 NFC タグがフィッシング攻撃やマルウェア感染に悪用されるリスクが報告されている [3–6]．冒頭で述べたように NFC による通信は 10 cm 以下の近距離に限られる．そのため，ユーザが意図しないうちに NFC タグを勝手に読み込んでしまう状況は考えにくいと思われてきた．既存の報告で懸念されている脅威モデルは，NFC を利用した既存設備に悪性 NFC タグが設置されたり，悪性 NFC タグを内蔵したスマートポスターが掲示されたりするケースである．このような脅威に対する対策として，セキュリティリスクの啓発を行う組織である Wall of Sheep [5] は，第三者が作成した NFC タグを信用せず，用心することを提言している．

しかしながら，ユーザの用心だけで悪性 NFC タグの読み込みを防ぐことは可能だろうか．例えば悪性 NFC タグが家具や貨幣，衣服といった**用心すべき対象として想定することがない身近なモノ**に埋め込まれていた場合はどうだろうか．ユーザはそのようなモノに NFC タグが埋め込まれているとは想像しない．したがって，ユーザは意図せずスマートフォンを悪性 NFC タグに近づけてしまうリスクがある．

以上の議論を元に，我々は次の問題提起をする．それは，**スマートフォンとモノがシームレスに繋がるようになったことで，現実世界のあらゆるモノをマルウェアのように動作させることが可能になったのではないか？**という Research Question である．この Research Question に答えるため，本研究は *Trojan of Things* と名付ける Proof of Concept を提示し，その実現可能性と対策方法を論じる．Trojan of Things とは，「一見何の変哲もないモノだが，ユーザの意図しない形でスマートフォン等の電子機器と通信を行い，マルウェアのような動作をするモノ」である．本研究では貨幣や衣服，家具をモノの例としてとりあげ，それぞれ貨幣型トロイ（*Currency Trojan*），ウェアラブルトロイ（*Wearable Trojan*），家具型トロイ（*Furniture Trojan*）なる新しい概念の攻撃が実現可能であることを示す．

本研究の貢献は以下のとおりである．

- 様々な悪性動作をするように NFC タグをプログラムし，実世界で動作する Trojan of Things として貨幣型トロイ，ウェアラブルトロイ，家具型トロイの 3 つの PoC 実装を作成した．
- 悪性 NFC タグを用いた攻撃の成功率を高めるために，ユーザの判断をミスリードする手法を考案し，NFC タグに実装した．
- 市場で入手可能な異なる機種の Android 端末 18 台（11 社）を用いて，Trojan of Things による攻撃の実現可能性の検証と攻撃成功条件の評価を行った．
- Trojan of Things への対策として，モノとの接続時に表示されるメッセージの変更や，コンテキストアウェアなモノとの通信方法を提案した．これらの手法では，NFC が提供する高いユーザビリティを損なう事なく，Trojan of Things による攻撃を防ぐことができる．

本研究が対象とする悪性 NFC タグによる攻撃が成立する条件および制約については 9.1 節で議論する．

本論文の構成は以下のとおりである．2 章では，関連研究を紹介し，それらと本研究の差異について述べる．3 章では，悪性 NFC タグによる Trojan of Things の実装の概要を説明し，実装の詳細は 4 章，5 章，6 章，7 章で述べる．8 章では，悪性 NFC タグで実装した Trojan of Things がもたらす脅威の評価を行う．9 章では，悪性 NFC タグによる Trojan of Things の制限事項と，Trojan of Things がもたらす新たな脅威への対抗手段について論じる．最後の 10 章で本研究のまとめをする．

2. 関連研究

本章では，NFC タグを用いたスマートフォンへの攻撃に関する研究を示す．Miller [3] は，攻撃者がスマートフォンに十分近づくことができるという想定のもと，悪性 NFC タグを用いてスマートフォンに任意のウェブページを表示し，Browser Exploit を成立させる攻撃を報告した．Mulliner [4] は，Nokia 6131 を対象に，NFC タグを読み込んだ際に表示されるダイアログのサイズが固定であることを利用し，攻撃者が改行コードを用いて表示されるメッセージを自由に設定できることを報告した．さらに Mulliner は NFC Worm という PoC を提示した．NFC Worm に感染した端末はスマートポスターのデータを書き換え，そのポスターを読み込んだ他の端末が NFC Worm をダウンロードするように仕向ける．Wall of Sheep [5] は，DEFCON の会場でスマートポスターと NFC タグを貼り付けたボタンを用いた実験を行った．タグの読み込みにより特典を受けられると周知したところ，約 50 人の参加者が NFC タグを読みとった．また Wall of Sheep は，悪性 NFC タグを用いて Android 端末にマルウェアを感染させるデモを会場で披露し，信頼できない NFC タグを読み込む際には用心

するよう呼びかけた．Gold ら [6] は，スマートポスターを利用し偽の SNS サイトにログインさせるフィッシング攻撃や，NFC の P2P モードを利用して悪性ファイルをユーザに無断で端末に保存する攻撃を考案した．

上述の研究では，攻撃者がスマートフォンに十分近づけることを前提としているか，ポスターの文章や既存の設備を利用しユーザを誘導することで，ユーザの意思で悪性 NFC タグを読みこませる．一方，本研究で提示する悪性 NFC タグによる Trojan of Things は，身の回りのモノに悪性 NFC タグを埋め込むことで，悪性 NFC タグが偶発的に読み込まれることを狙いとする．ユーザがいくら注意しても，身の回りのモノに埋め込まれた悪性 NFC タグにスマートフォンを近づけないようにすることは困難であり，Trojan of Things による脅威は既存研究のものとは異なる新たな脅威であるといえる．

3. 攻撃の概要

本章では，悪性 NFC タグによる Trojan of Things の実装の概要について説明する．悪性 NFC タグを攻撃ベクトルとして Trojan of Things を実装するためには，悪性 NFC タグについて理解する必要がある．4 章では，悪性 NFC タグにより引き起こされる悪性動作について説明する．5 章では，複数の悪性タグを用いた高度な攻撃を実現するために，NFC のカードエミュレーションモードを利用し，複数のタグを連続でスマートフォンに読み込ませる手法について述べる．Android OS は端末の設定変更を伴う特定の NFC タグを読み込んだ際，確認ダイアログを通してユーザに承認を求める．6 章では，この確認ダイアログによる OS とユーザの対話を妨害することで，悪性 NFC タグによる攻撃を強化する手法について述べる．4 章，5 章，6 章において作成した悪性 NFC タグを身の回りのモノに埋め込むことで，Trojan of Things を実装することができる．NFC による通信は NFC タグとスマートフォンが近接しなければ開始されないため，悪性 NFC タグの埋め込み先は，スマートフォンと近接する機会の多いモノが妥当である．7 章では悪性 NFC タグの埋め込み先のモノについて検討し，埋め込み先として通貨や衣服，家具を選んだ．また，それらのモノに実装した Trojan of Things がスマートフォンに対して実際に動作するか確認する．Trojan of Things の実装に使用した機器を**表 1** に示す．表 1 の非接触 IC カードリーダ/ライタを使用したプログラムの実装には，オープンソースのライブラリである nfcpy [7] を利用した．5 章，6 章，7 章で述べる内容は既存研究にはない，我々の新たな取り組みである．

4. 悪性 NFC タグを用いた攻撃ベクトル

本章では NFC タグによるウェブページの表示，アクセスポイントへの接続，Bluetooth 機器とのペアリングを例に挙げ，これらの動作を悪用できることを説明する．なお，Android 端末が NFC タグを読み込んだ際の動作は，NFC タグに格納された “NDEF (NFC Data Exchange Format) レコード” の内容により決定される．

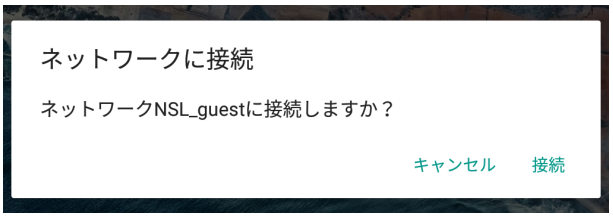

図 1 SSID:“NSL_guest” のアクセスポイントに接続する際の確認ダイアログ（Nexus 7）

4.1 悪性ウェブページの表示

スマートフォンに指定した URL をブラウザで開かせる NDEF レコードを，本論文では URI レコードと呼ぶ．URI レコードにより，Android OS はユーザに確認することなく，ブラウザを起動して指定されたウェブページを表示する．本研究で提示する攻撃においては，URI レコードをスマートフォンの各種情報の取得に用いる．取得した情報は，複数の悪性レコードを使用した攻撃（5 章）において，後続のレコードによる攻撃に利用できる．例えば，OS のバージョンや端末の機種情報，ブラウザの言語設定は，6.1 節で述べる手法において，適切な文字列の選択に利用できる．また，端末の画面サイズを取得することで，各アプリの UI の位置を知ることができる．これは 4.3 節で述べるマウスのペアリングが成功した場合，画面を見ないでスマートフォンを操作するために必要な情報である．加えて，HTML5 API を通じて，加速度センサー，照度センサー，近接センサーなどの値を取得することで，悪性タグが読み込まれた際の状況を推定できる．推定した状況に応じて，次にスマートフォンに読み込ませる悪性タグを選択することで，攻撃成功率の上昇が期待できる．

4.2 悪性アクセスポイントへの接続

指定した Wi-Fi ネットワークにスマートフォンを接続させる NDEF レコードを，本論文では WiFiConfig レコードと呼ぶ．スマートフォンがこのレコードにより，攻撃者の用意した無線 LAN アクセスポイントに接続させられ，中間者攻撃を受ける危険性がある．WiFiConfig レコードにより Wi-Fi ネットワークに接続する際には，確認ダイアログ（**図 1** 参照）が表示される．6.1 節では，この確認ダイアログに表示されるメッセージを変造することで，ユーザの判断を妨害する手法について述べる．

4.3 悪性 Bluetooth 機器とのペアリング

指定した Bluetooth 機器とスマートフォンをペアリング

表 1 使用機器

使用機器	製品名	メーカー	備考
NFC タグ	MM-NFCT2 NFC タグ	SANWA SUPPLY	丸型・直径 38mm
非接触 IC カードリーダ/ライタ	RC-S380	SONY	—
Nexus 7	Nexus 7 (2013)	ASUS	Android 6.0.1
Xperia Z3	Xperia Z3	Sony Mobile Communications	Android 5.0.2

させる NDEF レコードを，本論文では BTSSP レコードと呼ぶ．我々は NFC Forum が発行した仕様書 [8] をもとに，BTSSP レコードを nfcpy 上に実装した．BTSSP レコードを利用をして，攻撃者の Bluetooth マウスをターゲットのスマートフォンとペアリングさせることで，ターゲットのスマートフォンを攻撃者が遠隔操作できる．4.2 節同様，ペアリング前に確認ダイアログが表示される．

5. 複数の悪性レコードを使用した攻撃

本章では，NFC のカードエミュレーションモードを利用して，複数の悪性レコードを使用した攻撃を実現する手法について説明する．なおこの手法は，家具型トロイ（7.3 節）のように装置を埋め込むスペースが確保できるものを想定している．4 章で説明したレコードを動作させるには，NDEF レコードを NFC タグの先頭に書き込む必要がある．そのため，一つの NFC タグでは一つのレコードで実現できる動作しか実行させることができない．カードエミュレーションモードを利用すると，NFC デバイスを NFC タグのように振る舞わせることができる．このモードに対応した NFC デバイスは容易に入手でき，RC-S380 (表 1) はその一つである．我々は，複数の悪性レコードを使用した攻撃を，NFC デバイスでエミュレートするタグを動的に切り替えることで実現した．エミュレートしている NFC タグが読み取られたことを確認したら，別のタグのエミュレーションを開始するように，NFC デバイスをプログラムすることでタグを動的に切り替えることができる．

6. 判断のミスリードによる攻撃強化

WiFiConfig レコードや BTSSP レコードによる攻撃では，OS が設定変更前に確認ダイアログを表示し，ユーザの承認を求める．この確認ダイアログによる OS とユーザの対話を妨害し，ユーザの判断をミスリードすることで攻撃が成功しやすくなると考えられる．そのような手法として，本章では確認ダイアログのメッセージを変造する手法と，確認ダイアログの視認を困難にする手法を提案する．

6.1 確認メッセージの変造

WiFiConfig レコードにより表示される確認ダイアログを題材に，ダイアログのメッセージを変造することで，ユーザをミスリードする手法について説明する．WiFiConfig レコードにより表示される確認ダイアログのメッセージは，

```
...
<string name="prompt_connect_to_network"
    msgid="8511683573657516114">
"ネットワーク<xliff:g
    id="NETWORK_SSID">%1$s</xliff:g>に接続しますか？"
</string>
...
```

図 2 android/platform/packages/apps/Nfc/res/values-ja/strings.xml [11]（抜粋）

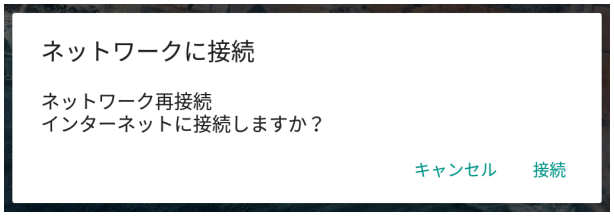

図 3 SSID:“再接続 \n インターネット” のアクセスポイントに接続する際の確認ダイアログ（Nexus 7）

図 2 に示すように定義されている．ただし，図 2 中の文字列 `<xliff:g id="NETWORK_SSID">%1$s</xliff:g>` は，レコード中に設定された SSID の値で置換される．無線 LAN の識別子である SSID は，長さが 0~32 オクテット列と定義されており [9]，各オクテットの値は任意に設定できる．そのため ASCII 印字可能文字だけでなく，日本語や改行コードを SSID に含めることができる．SSID を “再接続 \n インターネット” と指定したレコードを，Nexus 7（表 1）で読み込んだ際に表示される確認ダイアログを**図 3** に示す．この SSID の狙いは，ユーザに図 3 の確認メッセージを，本来の意味である「Wi-Fi ネットワークに接続するかの確認」ではなく，「インターネットに再接続するかの確認」と解釈させ，悪性ネットワークに接続させることである．我々は hostapd [10] を使用して，上述の SSID を持つアクセスポイントを構築した．そして確認ダイアログ（図 3）の “接続” ボタンをタップすると，構築したアクセスポイントにスマートフォンが接続されることを確認した．

ただし，スマートフォンメーカーによる Android OS の改変により，表示されるメッセージの定義が図 2 と異なる端末が存在する．例として Xperia Z3（表 1）で表示される確認ダイアログを**図 4** に示す．メーカーによるメッセージ改変の実態については 8 章で詳細に述べる．メッセージの定義の差異に対応するには，まず 4.1 節で述べた方法で機種を特定し，次に 5 章で述べる手法を用いて，機種に合わせた WifiConfig レコードを読み込ませればよい．

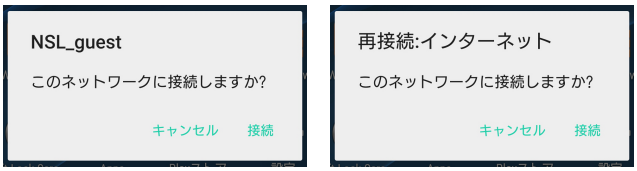

図 4 SSID:“NSL_guest”（左）と SSID:“再接続:インターネット”（右）のアクセスポイントに接続する際の確認ダイアログ（Xperia Z3）

図 5 図 4 (左) に Screen Filter を適用した図

6.2 インストール済みのアプリを利用する

Android Application レコードは，すでに Android 端末上にインストールされているアプリを起動する NDEF レコードである．このレコードを利用して，半透明な黒いウィンドウを最前面に表示する “Screen Filter” [12] というアプリを起動すれば，確認ダイアログの視認を困難にすることができる．Screen Filter は，Google Play ストアで 500 万回以上ダウンロードされているアプリであり，本手法では，端末に Screen Filter がインストールされていることを前提としている．

本手法は，5 章で説明した複数の悪性レコードを使用した攻撃により実現される．Android Application レコードを用いて Screen Filter を起動させてから，WiFiConfig レコードや BTSSP レコードを端末に読み込ませると，確認ダイアログが表示された時には画面が暗くなっているため，ユーザは確認ダイアログを視認しにくくなる（**図 5**）．そのため確認ダイアログが表示されていることや，その内容にユーザが気づかず，確認ボタンをタップしてしまうことが期待できる．

7. 悪性 NFC タグの埋め込み先

偶発的に悪性 NFC タグをスマートフォンに読み込ませるためには，スマートフォンに近接する機会の多いモノに悪性 NFC タグを埋め込むのが妥当である．本章ではスマートフォンに近接する機会が多いモノとして，紙幣，衣服，家具を例として Trojan of Things の概念実証を行う．

7.1 貨幣型トロイ

貨幣型トロイは，紙幣や硬貨などの現金通貨を Trojan of Things にしたものである．現金通貨は支払いの手段として用いられることで，人から人へと物理的に流通していく．その通貨に悪性 NFC タグを埋め込むことで，多くの攻撃機会を得ることが狙いである．財布とスマートフォンを共にズボンのポケットに入れて持ち運ぶ人は少なくないであろうから，スマートフォンと悪性 NFC タグが近接する機会も少なくないと考えられる．

図 6 貨幣型トロイ

図 7 ウェアラブルトロイ

紙幣を模した玩具を加工し，NFC タグを埋め込んだものを**図 6** に示す．NFC タグは図 6 の丸枠で囲まれた部分に貼付されている．この紙幣を財布にしまい，財布をズボンのポケットにいれた．続けてスクリーンロックを解除したスマートフォンを同じポケットに入れたところ，スマートフォンが NFC タグを読み込むことを確認した．

7.2 ウェアラブルトロイ

ウェアラブルトロイは，衣服を Trojan of Things にしたものである．衣料品店に陳列されている衣類や，屋外に干された洗濯物，席に掛けられた上着など，様々な衣類が対象であり，標的型攻撃も可能である．胸ポケットやズボンのポケットなどスマートフォンに近接する可能性が高い部分に悪性 NFC タグを埋め込むことで，スマートフォンが悪性 NFC タグに近接する機会が多くなると考えられる．実際にズボンのポケットに NFC タグを貼付し（**図 7** 丸枠内），そのポケットにスマートフォンをしまったところ，スマートフォンが NFC タグを読み込むことを確認した．

7.3 家具型トロイ

家具型トロイは，家具に悪性 NFC タグを埋め込むことで Trojan of Things としたものである．家具型トロイは，貨幣型トロイやウェアラブルトロイと異なり，攻撃が発生する場所を攻撃者が特定できる．そのため攻撃者は，付近に悪性アクセスポイントや Bluetooth 機器を設置しておくことができ，4.2 節や 4.3 節で述べた悪性 NFC タグを活用しやすい．また，悪性 NFC タグを目立たないように埋め込むことが容易であり，NFC タグを並べて埋め込むことで，広い範囲でスマートフォンにタグを読み込ませることができる．具体的な家具型トロイの実装として，天板の裏に悪性 NFC タグを貼り付けた机（机型トロイ）を挙げることができる．8 章では机の天板の裏に悪性 NFC タグが貼り付けられていることを想定して，NFC タグの最大通信可能距離の測定を行う．

8. モノに埋め込まれた悪性 NFC タグがもたらす脅威の評価

本章では，市場で入手可能な異なる機種の Android 端末 18 台（11 社）を対象に，NFC 最大通信可能距離，工場出荷

時の NFC 設定，および NDEF レコードにより表示される確認ダイアログについて調査した結果を示し，調査結果より Trojan of Things の脅威の評価を行う．調査結果を**表 2** に示す．NDEF レコードにより表示される確認ダイアログの表示内容については，**表 3**，**表 4** に示す．表 3 では WiFiConfig レコードに設定した SSID を “<SSID>” で，表 4 では BTSSP レコードに設定した機器の名称を “<name>” でそれぞれ示した．WiFiConfig レコードは Android 5.0 以降よりサポートされている．そのため，Android のバージョンが 5.0 未満の端末では WiFiConfig レコードにより表示されるメッセージは存在しない（表 2）．

最大通信可能距離は，机型トロイを想定して，NFC タグ（表 1）を木板（ウォールナット材）の裏面に貼付し，表面に設置したスマートフォンから読み取る実験を行った．本実験では木板の厚みを 5 mm 間隔で変更した．表 2 より，測定に使用した Android 端末の NFC 最大通信可能距離は平均で 3.4 cm，最低で 2.0 cm である事が分かる．財布や衣服，机の天板の厚みを考慮すると，これらのモノに埋め込まれた悪性 NFC タグが，Android 端末の NFC 通信可能距離まで近づくことは十分起こりうる．また，過半数の Android 端末が工場出荷状態において NFC のリーダ/ライタモードが有効に設定されており，悪性 NFC タグによる攻撃が可能な状態となっていた．さらに，確認ダイアログのメッセージは，“Ascend P7” を除いて，NFC タグにより確認ダイアログが表示されたのだとユーザが判断できるような内容ではなかった．特に，WiFiConfig レコードにより表示される確認ダイアログで，6.1 節の手法に対抗できるものは存在しなかった．以上より，悪性 NFC タグで実装した Trojan of Things の脅威がきわめて現実的であると結論づけることができる．

9. 議論

本章では，悪性 NFC タグによる Trojan of Things の制限事項について議論する．また悪性タグによる Trojan of Things がもたらす新たな脅威に，ユーザビリティを損なうことなく対抗する手段について論じる．

9.1 制限事項

端末による制約

端末による制約事項を 2 点挙げる．第一に，本研究で実装した Trojan of Things は，NFC を搭載した Android 端末に対してのみ有効である．NFC を搭載する Android 端末の出荷台数が 2018 年には 8 億 4000 万台あまりに達すると予測されており [1]，Trojan of Things は多くの端末に対して脅威となる．一方で，iPhone 6 などの iOS 端末は本論文執筆時点で NFC のリーダ/ライタモードをサポートしておらず，NFC タグにより機能を呼び出すことはできない．第二に，Android が NDEF レコードに応じた機能を呼び出すのは，NFC 機能が設定で有効になっており，端末のスクリーンロックが解除されているときに限られる．表 2 で示したように，工場出荷時に NFC 機能が有効になっている機種は多い．また，新しい機種であるほど NFC 機能が有効に設定されている傾向が見られることは強調しておきたい．こうした制約のなか，悪性 NFC タグをどのようなモノに埋め込むのが効果的であるのか，どの程度の人が NFC 機能を有効としているのかを明らかにするためには，さらなる研究・調査が必要であり今後の課題としたい．

モノによる制約

悪性 NFC タグによる攻撃の機会を多く得るには，タグが埋め込まれていることを気づかれることなく，モノが使用される必要がある．特に貨幣型トロイを実装するためには実際に流通している通貨に悪性 NFC タグを埋め込む必要があるが，手触りや厚みが変化することは避けられず，通貨使用者が加工に気づきやすいと考えられる．このように加工したことが気づかれやすいモノに，悪性 NFC タグを埋め込むことは合理的でない．しかし，通貨の加工に気づいても，その加工が悪意のあるものであると判断するとは限らない．例えば，アメリカでは紙幣にシールを貼ることが許されており [13]，実際にサンタクロース等のシールが貼付されたドル紙幣が販売されている [14]．通貨へのシール貼付が許されており，それが一般に認知されている場合，貨幣型トロイが長期間流通してしまう懸念がある．

9.2 対抗手段

本節では悪性 NFC タグによる Trojan of Things がもたらす新たな脅威に対する対抗手段について論じる．NFC の強みは，「端末をかざす」という簡単な意思表示により通信を開始できるユーザビリティの高さにある．その一方で，ユーザの意思に反して端末に NFC 機器が近接してしまう危険性については，これまで十分に論じられてこなかった．この危険性を緩和するための簡便な方法として，NFC タグにより指定された動作をする前に確認ダイアログを通してユーザの意思を確認するというものが考えられる．しかし，この方法では「端末をかざす」という動作と「確認ダイアログのボタンをタップする」という動作をユーザに強いることとなり，NFC が持つユーザビリティの高さが十分に発揮されなくなってしまう．そこで我々は，コンテキストに応じたユーザの意思確認を提案する．この手法は，スマートフォンに搭載された各センサーの値よりコンテキストを推測し，ユーザの追加の意思表示が必要なときに限り，確認ダイアログを表示するものである．例えば，静電容量センサーや加速度センサー，ジャイロセンサーの値を使用すれば，ユーザがスマートフォンを手に持って，NFC 機器にかざしたのかを判断できる．また，照度センサーの値から，端末がポケットの中などにしまわれていないことを確認できる．これらのセンサーの値から推測されるコンテキ

表 2 機種ごとに測定した NFC 最大通信可能距離とレコードにより表示されるメッセージ

Brand Name	Manufacture	Android Version	Maximum Reading Distance [cm]	NFC R/W Activated in Factory State	Message Type (Wi-Fi, Japanese)	Message Type (Wi-Fi, English (US))	Message Type (Bluetooth, Japanese)	Message Type (Bluetooth, English (US))
Nexus 5X	LG	6.0	4.5	✓	WI-JA-1	WI-EN-1	BT-JA-1	BT-EN-1
AQUOS ZETA	SHARP	5.1.1	3.5	✓	WI-JA-1	WI-EN-1	BT-JA-1	BT-EN-1
SAMURAI KIWAMI	FREETEL	5.1	3.0		WI-JA-1	WI-EN-1	BT-JA-1	BT-EN-1
TORQUE G02	KYOCERA	5.1	3.5	✓	WI-JA-1	WI-EN-1	BT-JA-1	BT-EN-1
ARROWS NX	FUJITSU	5.0.2	4.0		WI-JA-1	WI-EN-1	BT-JA-1	BT-EN-1
AQUOS SERIE	SHARP	5.0.2	3.0	✓	WI-JA-1	WI-EN-1	BT-JA-1	BT-EN-1
TORQUE G01	KYOCERA	4.4.2	3.5	✓	—	—	BT-JA-1	BT-EN-1
ONETOUCH IDOL 2 S	ALCATEL	4.3	3.0		—	—	BT-JA-1	BT-EN-1
ELUGA P	PANASONIC	4.2.2	2.0		—	—	BT-JA-1	BT-EN-1
INFOBAR A02	HTC	4.1.1	2.5		—	—	BT-JA-1	BT-EN-1
Ascend P7	HUAWEI	4.4.2	3.5	✓	—	—	BT-JA-5	BT-EN-5
isai vivid	LG	5.1	5.0	✓	WI-JA-2	WI-EN-2	BT-JA-2	BT-EN-2
DM-01G	LG	5.0.2	5.0		WI-JA-2	WI-EN-2	BT-JA-2	BT-EN-2
Galaxy S7 edge	SAMSUNG	6.0.1	3.0	✓	WI-JA-1	WI-EN-1	BT-JA-4	BT-EN-4
GALAXY S4	SAMSUNG	5.0.1	3.0		WI-JA-1	WI-EN-1	BT-JA-4	BT-EN-4
Xperia Z5	SONY	6.0	3.0	✓	WI-JA-3	WI-EN-1	BT-JA-3	BT-EN-3
Xperia Z3	SONY	5.0.2	3.0	✓	WI-JA-4	WI-EN-3	BT-JA-3	BT-EN-3
Xperia Z2	SONY	5.0.2	2.5		WI-JA-4	WI-EN-3	BT-JA-3	BT-EN-3

表 3 WiFiConfig レコードにより表示される確認ダイアログのメッセージ

Type	Title	Message	Positive Button	Negative Button
WI-JA-1	ネットワークに接続	ネットワーク<SSID>に接続しますか？	接続	キャンセル
WI-JA-2	接続	<SSID>に接続しますか？	はい	いいえ
WI-JA-3	ネットワークに接続	ネットワーク [<SSID>] に接続しますか?	接続	キャンセル
WI-JA-4	<SSID>	このネットワークに接続にしますか?	接続	キャンセル
WI-EN-1	Connect to network	Connect to network <SSID>?	CONNECT	CANCEL
WI-EN-2	Connect	Connect to <SSID>?	YES	NO
WI-EN-3	<SSID>	Connct to this network?	CONNECT	CANCEL

表 4 BTSSP レコードにより表示される確認ダイアログのメッセージ

Type	Title	Message	Positive Button	Negative Button
BT-JA-1	—	Bluetooth デバイスをペアに設定してもよろしいですか?	はい	いいえ
BT-JA-2	—	Bluetooth ペアリング要求を受信しました。ペアリングしますか？	はい	いいえ
BT-JA-3	—	ペアリングしますか?[<name>]	はい	いいえ
BT-JA-4	—	Bluetooth デバイスをペアリングしますか？	はい	いいえ
BT-JA-5	NFC ペアリング要求	Bluetooth デバイス とペアリングしますか？	ペア設定する	キャンセル
BT-EN-1	—	Are you sure you want to pair the Bluetooth device ?	YES	NO
BT-EN-2	—	Bluetooth pairing requested. Pair?	YES	NO
BT-EN-3	—	Pair with [<name>]?	YES	NO
BT-EN-4	—	Pair the Bluetooth device ?	YES	NO
BT-EN-5	NFC pairing request	Pair with the Bluetooth device ?	Pair	Cancel

```
...
<string name="prompt_connect_to_network"
    msgid="8511683573657516114">
"NFC タグから Wi-Fi 設定データを受信しました。\n
    以下の SSID の Wi-Fi ネットワークに接続しますか？\n
    SSID:[<xliff:g id="NETWORK_SSID">%1$s</xliff:g>]"
</string>
...
```

図 8 改良した Nfc/res/values-ja/strings.xml

ストから，ユーザの意思で端末が NFC 機器にかざされたと判断できない場合に限り，ユーザの意思を確認するために確認ダイアログを表示する．この手法であれば，ユーザビリティを損なうことなく，端末が意図せず NFC 機器に近接してしまうリスクを低くすることができる．

加えて，表示される確認ダイアログのメッセージにも改良が必要である．ここまで述べてきたように，Android OS は NFC タグにより Wi-Fi ネットワークに接続する場合や，Bluetooth 機器とペアリングする場合には，確認ダイアログを表示している．しかし，現在定義されている確認ダイアログのメッセージ（図 2）では，偶発的に端末が悪性 NFC タグに近接してしまった場合，確認ダイアログが表示された理由をユーザが理解することは困難である．それゆえに，6.1 節で述べたようなメッセージの変造により，ユーザが確認ダイアログが表示された理由を誤って解釈してしまう危険性がある．したがって，図 2 の定義を改め，**図 8** に示すような定義を採用すべきである．この改良されたメッセージにより，「スマートフォンが NFC タグを読み込んだから，確認ダイアログが表示されたのだ」と明確にユーザに通知することができる．

9.3 倫理

本論文は悪性 NFC タグをモノに埋め込むことで Android 端末を攻撃する手法を示した．悪性 NFC タグを用いた攻撃の脅威は，すでに公知の事実である [3–6]．本論文の狙いは，悪性 NFC タグが身の回りのモノに埋め込まれる潜在的な脅威に警鐘を鳴らすことにある．NFC を搭載したスマートフォンの普及が進んでいることや，ユーザが注意してもスマートフォンを悪性 NFC タグから遠ざけておくことは容易ではないことから，開発者が Trojan of Things がもたらす脅威を認識し，早急に対抗手段を講じる必要があると考えている．

10. まとめ

本研究は Trojan of Things と称する新たな脅威の PoC を提案した．Trojan of Things の具体例として貨幣，衣服，家具に悪性 NFC タグを埋め込んだトロイを実装し，攻撃の実現可能性および攻撃成立条件を評価した．攻撃成立条件の評価では現在市販されている 18 機種の Android 端末を利用し，攻撃が現実的であることを明らかにした．これらの結果は「現実世界のあらゆるモノをマルウェアのように動作させることは可能」であることを支持する．また，本研究では悪性 NFC タグを用いて実装した Trojan of Things への対抗策として，コンテキストによって確認ダイアログを表示する方法，および適切なダイアログの構成例を示した．これら対抗技術の実装と評価，および実世界に設置された Trojan of Things に対する人間の行動分析は今後の課題である．

参考文献

[1] IHS Inc.: NFC-Enabled Cellphone Shipments to Soar Fourfold in Next Five Years, http://press.ihs.com/press-release/design-supply-chain/nfc-enabled-cellphone-shipments-soar-fourfold-next-five-years.

[2] Mobile, G.: NFC and Marketing, http://www.jcdecauxna.com/sites/default/files/assets/innovate/documents/studies/nfc_by_gauge_mobile.pdf.

[3] Miller, C.: Don’t stand so close to me: an analysis of the NFC attack surface, *Briefing at BlackHat USA. Las Vegas, NV, USA* (2012).

[4] Mulliner, C.: Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones., *ARES*, pp. 695–700 (2009).

[5] Wall of Sheep: NFC Security Awareness Project, http://www.wallofsheep.com/pages/nfc-security-awareness-project.

[6] Gold, K., Shetty, S. and Rogers, T.: A testbed for modeling and detecting attacks on NFC enabled mobile devices, *Military Communications Conference, MILCOM 2015-2015 IEEE*, IEEE, pp. 635–640 (2015).

[7] Tiedemann, S.: nfcpy/nfcpy: A Python module to read/write NFC tags or communicate with another NFC device., https://github.com/nfcpy/nfcpy.

[8] NFC Forum: Bluetooth Secure Simple Pairing Using NFC, http://members.nfc-forum.org/apps/group_public/download.php/18688/NFCForum-AD-BTSSP_1_1.pdf.

[9] IEEE Standard: IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *IEEE Std 802.11-2012* (2012).

[10] Malinen, J.: hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator, https://w1.fi/hostapd/.

[11] Google Git: res/values-ja/strings.xml, https://android.googlesource.com/platform/packages/apps/Nfc/+/423b56d3c540ec39d8803ac46213018fa04367a6/res/values-ja/strings.xml#46.

[12] haxor industry: Screen Filter - Android Apps on Google Play, https://play.google.com/store/apps/details?id=com.haxor.

[13] BUREAU OF ENGRAVING AND PRINTING: Currency NOTES, https://www.moneyfactory.gov/images/Currency_notes_508.pdf.

[14] Ltd. First Editions, Inc.: Santa Dollars, http://santadollars.com/.