Computer Security Symposium 2021
26 - 29 October 2021

接触確認フレームワークに対する陽性者特定攻撃の評価と対策

野本 一輝[1,a)]　秋山　満昭[2]　衛藤　将史[3]　猪俣　敦夫[5]　森　達哉[1,4]

概要：新型コロナウイルス感染症対策として，接触確認アプリが世界中で利用されている．接触確認アプリは，共通のフレームワークを用いて開発される．このフレームワークは，Bluetooth Low Energy (BLE) 通信と暗号技術を用いてプライバシーを保護した状態で新型コロナウイルス感染症の陽性者と接触した可能性を通知する．本研究の目的は，接触確認フレームワークに対する陽性者特定攻撃を評価する，すなわち，匿名化されているはずの BLE パケットに含まれる識別子と個人を効果的に結びつけることである．本研究では物理実験を用いて，BLE に含まれる識別子が，顔や衣服などの個人の特徴と結びつき，感染状態などのプライバシー情報が第三者によって推測される可能性があることを示した．本研究のシミュレーション実験では，数台の攻撃デバイスを利用する攻撃者が 1 時間あたり 5,000 人の歩行者を対象にしたときに，80% 以上の成功率で RPI と対象者の画像を正しく結びつけることができた．さらに本攻撃に対する対策手法を検討し，シミュレーションを用いて効果を定量的に評価した．

キーワード：接触確認アプリ, Exposure Notification, COVID-19, コンタクトトレーシング, プライバシー

Understanding the Risks of Re-identification Attack on the Contact Tracing Frameworks and its Countermeasures

Kazuki NOMOTO[1,a)]　Mitsuaki Akiyama[2]　Masashi Eto[3]　Atsuo Inomata[5]　Tatsuya MORI[1,4]

Abstract: As a countermeasure against COVID-19, digital contact tracing (DCT) applications are being used worldwide. DCT applications use a common framework. This framework uses Bluetooth Low Energy (BLE) communication and cryptography to notify the user of possible contact with a positive person of COVID-19 in a privacy-protected manner. The purpose of this paper is to evaluate positive person identification attacks on the DCT framework. That means to link individuals with identifiers contained in BLE packets that are supposed to be anonymized. Our physical experiments show that identifiers contained in BLE can be associated with personal characteristics and the privacy information like infection status can be assumed. In our simulation experiments, an attacker using several attack devices was able to link identifiers to images of the target with a success rate of over 80% when targeting 5,000 pedestrians per hour. We also used simulations to quantitatively evaluate countermeasure methods against this attack.

Keywords: contact tracing app, Exposure Notification, COVID-19, Privacy

1. はじめに

新型コロナウイルス感染症の感染拡大を阻止する技術として，スマートフォンを利用した接触確認 (Digital Contact Tracing, DCT) フレームワークが開発され，世界中で活用されている．DCT によって人々のプライバシーが侵さ

[1] 早稲田大学 / Waseda University
[2] 日本電信電話株式会社 / NTT
[3] 総務省 / Ministry of Internal Affairs and Communications
[4] 国立研究開発法人情報通信研究機構 / NICT
[5] 大阪大学 / Osaka University
[a)] nomoto@seclab.jp

れることはあってはならない．事実，陽性者や医療従事者に対する差別や偏見が社会問題となった [1]．DCT の代表的な実装は， Google と Apple が提供する Exposure Notification (GAEN) フレームワークである．GAEN は，接触判定をアプリ利用者のスマートフォン内で実施する分散システムである．2021 年現在， GAEN は世界を代表するモバイル OS である Android と iOS に搭載されている．

GAEN フレームワークでは，スマートフォンが Rolling Proximity Identifier (RPI) を BLE で近接の端末で広告する．広告された RPI は，誰でも収集可能であるが，RPI から個人を特定することはできない．しかしながら， GAEN フレームワークにおいては陽性者に紐付いた一時鍵の情報は公開される．また，その一時鍵から RPI を算出することができる．したがって， RPI を収集すると同時に，端末所有者の画像を撮影しておけば，あとから個人と感染状態が紐付けられるプライバシーリスクがある．

過去の研究でも，DCT フレームワークに対する陽性者特定攻撃の脅威が指摘されている [2], [3], [4]．しかし，科学的に再現可能な方法で評価されていない．これらの背景を元に，本研究は以下の Research Question に取り組む．

RQ1: **陽性者特定攻撃は実現可能か？**
RQ2: **攻撃はスケールするか？**
RQ3: **本攻撃に対する効果的な対策は何か？**

これらの Research Question を明らかにするために，DCT の代表的なフレームワークである GAEN を対象として広範囲なフィールド実験と大規模シミュレーションを行った．

本研究の貢献は以下の通りである[*1]．はじめに，スマートフォンを利用した広範囲なフィールド実験を通して，攻撃者が指向性アンテナを用いて陽性者特定攻撃を高い精度で実現できることを示した．比較的送信電力の弱いスマートフォンでも陽性者特定攻撃が成功することを示した．また，スマートフォンと攻撃デバイスの距離が遠いとき (7 [m] まで) でも攻撃が成功することを示した．次に，指向性アンテナの特性と歩行者の 3D モデルを用いたシミュレーション実験を行い，歩行者の流れや攻撃デバイスの数が攻撃の成功率に与える影響を評価した．その結果，1 時間あたり 5,000 人という大規模な歩行者の流れに対して，攻撃者はわずか数台の攻撃デバイスを配置するだけで，約 80% という高いリンク成功率を達成できることがわかった．

以上を総合すると，我々は DCT アプリをターゲットにした陽性者特定攻撃は実用的であると結論づける．本攻撃による脅威を抑制するために，複数の RPI を使って接触通知を行う新たなメカニズムや BLE フレームの広告周期を適切に調整する手法を提案する．これらの対策技術の有効性はシミュレーション評価によって明らかにする．

[*1] 著者らが ICSS 研究会 (2021 年 3 月) で発表した研究 [5] との差分 (追加項目) は以下の通り．(1) 攻撃デバイスにパラボラアンテナを導入して攻撃手法を変更，攻撃成功率を大幅改良 (2) スマートフォン複数機種を用いたフィールド実験により攻撃成否を評価 (3) アンテナの受信信号強度モデルおよび 3D モデリングを用いた現実世界に則したシミュレーションを構築，攻撃の実現可能性を評価 (4) シミュレーションを用い，対策効果を定量評価．

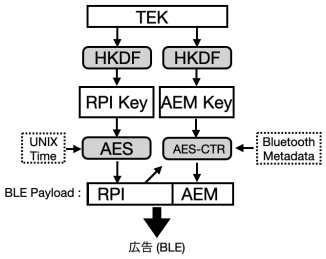


図 1 RPI の算出アルゴリズム [7]

2. GAEN フレームワーク

本章では，本研究で我々がターゲットとする GAEN フレームワークの概要を解説する．

GAEN フレームワークは，スマートフォン端末が，BLE を用い，一定期間で変更される匿名の識別子を交換する分散型の方式である [6]．GAEN フレームワークにおける，匿名識別子の生成スキームの概略を図 1 に示す．はじめに，各クライアント端末は，24 時間ごとにランダムに生成される TEK (Temporary Exposure Key) と呼ばれる鍵を生成する．TEK は 14 日間，デバイス内部に保存され，デバイスの持ち主が自身を保健当局の鍵管理サーバに陽性者登録しない限り，公開されることはない．クライアントデバイスは TEK と時刻から 15 分ごとに RPI を算出する．

新型コロナ陽性となったユーザは，アプリの機能を用いて，診断鍵を保健当局の鍵管理サーバにアップロードする．この診断鍵には，過去 14 日間の TEK および，該当する TEK が有効であった時間に相当するタイムスタンプのデータが含まれる．サーバは診断鍵をその国のクライアントに配信する．陽性者の診断鍵を受信したクライアントは，過去に受信した RPI と診断鍵のマッチングを行うことにより，濃厚接触の判断と通知を行う．

クライアントは， TEK ， RPI ， Bluetooth メタデータを元に， AEM (Associated Encrypted Metadata) と名付けられたデータを導出し，RPI および AEM を Payload に載せた BLE フレームを近隣に広告する [7]．クライアントは，200–270 [ms] の周期で BLE フレームを広告する [6]．クライアントは自らの RPI と AEM を広告するかたわらで，近隣クライアント端末が広告する BLE フレームを受信する．クライアントは，5 分に 4 秒の周期で BLE フレームを受信し，ペイロードを端末内部に保存する [8]．

3. 攻撃の全体像

本章では， GAEN フレームワークにおける陽性者特定

攻撃の概要を示す．はじめに，脅威モデルを説明する．次に，詳細な攻撃手法を説明する．

3.1 脅威モデル

陽性者特定攻撃を実行する攻撃者の目的は， GAEN フレームワークが動作するスマートフォン端末が BLE 信号を用いて広告する匿名識別子 (RPI) と，そのスマートフォン端末の所有者の写真を紐付けること，および GAEN フレームワークを使って自身を陽性者であると申告したユーザの RPI を特定することである．すなわち，攻撃者が陽性者の写真を自動的に収集することを狙いとする

攻撃者が使用する主な機器は， BLE 受信機とカメラである．攻撃者は，これらのデバイスを歩行者の多い道路に設置し，RPI と 歩行者の画像を継続的に収集する．攻撃者は，鍵管理サーバから収集した陽性者の診断鍵をダウンロードし， TEK ，日時情報，対応する RPI を算出する．これらのデータを解析することで，陽性者の診断鍵に対応する RPI を特定し，その画像を抽出することに成功する．

3.2 攻撃の流れ

陽性者特定攻撃の手順は，以下の 2 つのステップからなる．**Step 1**: RPI とターゲット画像の紐付け，および **Step 2**: RPI と陽性者の紐付け．攻撃者はこれら 2 つの紐付けを実現することにより，陽性者と紐付いた画像を自動的に収集することができる．以下に 2 つの紐付け手順を概説する．

Step 1: RPI とターゲット画像の紐付け： 攻撃者の目的は BLE 信号に含まれる RPI と 撮影された画像を正確に紐付けることである．対象者が攻撃機器に近づいた時刻をピンポイントで特定することを実現する鍵は，電波強度の情報を使うことである．理論的には，電波強度は距離の 2 乗に反比例して減衰する．したがって， RPI を含む BLE フレームを運ぶ電波の強度が最大となったタイミングが，その RPI を送信したスマートフォンの持ち主が最も攻撃デバイスに近づいた瞬間に一致するはずである．指向性が高いパラボラアンテナを使うことにより，そのような計測を高精度に実現することができる．攻撃者はそれぞれの RPI について，信号強度グラフの時系列データを生成する．信号強度の時系列データに対して，ピーク検出アルゴリズムを適用することにより，信号強度が最大となる時刻 $t_{\max}(i)$ を特定する．

攻撃者は特定された時刻 $t_{\max}(i)$ に撮影された画像を抽出し，物体検知アルゴリズムを適用することにより対象者の画像を切り出すことができる．本研究は，汎用的な物体検出アルゴリズムとして，You only look once (YOLO) を採用した [9].

Step 2: RPI と陽性者の紐付け： GAEN フレームワークでは，各国の保健当局が運用する鍵管理サーバにより，診断鍵が配布されている [10]．Testing Apps for Contact Tracing (TACT) project [11] による調査では，2021 年 7 月現在，カナダやイギリス，ドイツを含む少なくとも 25 ヶ国の国において 診断鍵 の入手が可能であることが確認されている．我々は上記の国に加えて，日本においても入手できることを確認している．これらの結果は攻撃者が陽性者に対応する診断鍵を容易に入手できることを意味する．

診断鍵をデコードすることで TEK や TEK が有効な日時に相当するタイムスタンプなどのメタデータを入手できる [12]．公開されるアルゴリズムを適用することで，有効な陽性者の RPI を導出できる [7]．導出した RPI と収集した RPI を比較することで，陽性者の RPI と対応する画像を特定できる．

表 1 攻撃デバイス

機材	モデル
コンピュータ	Apple Macbook Pro 2020 model (macOS 11.4)
BLE 受信機	Ubertooth One (firmware: 2020-12-R1) [13]
アンテナ	ANT-GRID-24dBi [14]
USB カメラ (× 2)	BUFFALO BSW505MBK

表 2 実験対象のスマートフォンのモデルと仕様 [15], [16], [17], [18], [19]

ベンダ	OS	モデル	BLE 送信電力 [dBm]	BLE アンテナゲイン [dBi]
Apple	iOS 14.6	iPhone 8	20	-0.44
Apple	iOS 14.6	iPhone XR	16	-4.9
LG	Android 10	G8X ThinQ	4.65	-5.03
Huawei	Android 9	P20 Lite	5.36	n/a
Motorola	Android 7.1.1	Nexus 6	6.57	-3.00

4. 実空間における攻撃の検証

本章の狙いは， **RQ1**: **陽性者特定攻撃は実現可能か？** を検証することである．特に，3.2 節で示した RPI と 対象者の画像を紐付ける (以下，リンクできる) ことに着目する．様々な条件で行われたフィールド実験により，陽性者特定攻撃の実現性を明らかにする．

4.1 実験デバイス

はじめに実験で用いた機器について示す．攻撃者が用いる機器は， PC ， BLE 受信機，アンテナ (メイン，サブ)， USB カメラ，および三脚である．実験に用いた機材一覧を表 1 に示す．BLE 受信機，アンテナとしてそれぞれ Ubertooth One , 指向性アンテナ (パラボラアンテナ) を用いた．USB カメラとして，視野角が 120 度 で解像度が 1,920×1,080 pixels の機器を採用した．実験では，対象者が利用するスマートフォンとして表 2 に示すデバイスを用いた．すべてのスマートフォンには， COCOA 1.2.4 がインストールされている．

実験のセットアップを図 2 に示す．図の左側は，セットアップの模式図を，右側は，実際に攻撃者が用いる機材のセットアップを設置した様子を撮影した写真を示す．セットアップでは，ターゲットとなる人物が 2 台 のカメラで撮影しているポイントを横切ることを想定する．アンテナと同じ位置にメインカメラを設置し，ターゲットの真正面から撮影できる位置にサブカメラを設置する．メインカメラ

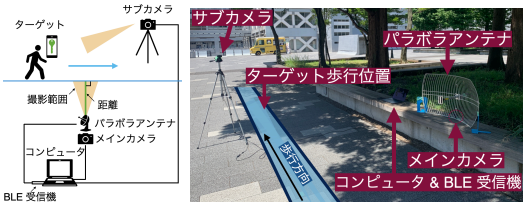


図 2 攻撃デバイスの設置図

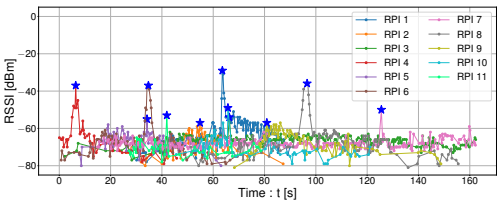


図 3 観測された RPI についての時間–信号強度グラフ．星印はそれぞれの RPI について信号強度最大となった時刻 $t_{\max}(i)$.

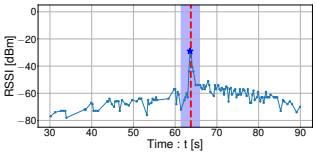


図 4 実験対象に一致する RPI (図 5) についての時間–信号強度グラフ．ターゲットとアンテナの距離は 2 [m] である．

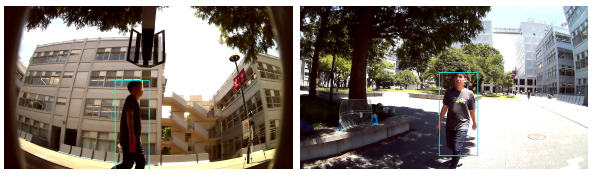


図 5 $t_{\max}(i) = 63.56$ [s] に一致する時刻に撮影された画像．YOLO v3 を用いて画像内の人物を検出した．薄緑色の長方形の枠で検出結果を示した．

は，RPI と人物の画像を精度良く紐付けることを目的とする．ただし，メインカメラでは人物の横顔しか撮影できないため，サブカメラを用いて人物の正面画像を収集する．

カメラおよびパラボラアンテナはいずれも コンピュータ に接続されている．コンピュータ は BLE 信号データと画像データを記録する．攻撃者はこれらのデータを用いて，陽性者特定攻撃を実現する．

4.2 RPI とターゲット画像の紐付け

3 章で示した RPI とターゲット画像の紐付け (step 1) が実現可能であることを，実験により検証する．図 2 に示すパラボラアンテナとカメラを用いることで，ターゲットがセットアップに最も近づいたタイミングを特定する．ターゲットのデバイスが生成した RPI を含む BLE フレームの信号強度が最も高くなったタイミングでターゲットがカメラの正面に到着し，その瞬間に撮影された画像に，対象者が写っていると仮定する．

実際には，電波の反射や散乱などの影響により，信号強度が最大となる時刻 $t_{\max}(i)$ と 対象者がカメラの前方を通過する時刻 $t_A(i)$ は ずれる可能性がある．そこで，信号強度が最大となる時刻と，ターゲットがカメラの正面を通過する時刻の差を計測する実験を行った．実験では，ターゲットはスマートフォンをポケットに入れて，攻撃デバイスの前方を通過する．ターゲットとアンテナおよびカメラの距離 2 [m] とした．また，試行回数は 45 回 とした．明らかな外れ値が 1 つ あったため，除外した．時刻差の平均値は 0.162 [s] ，標準偏差は 0.130 であった．すなわち，ターゲットの信号強度が最大となる時刻とカメラの正面を通過する時刻はきわめて近いこと，時刻に基づくリンクが実現的であることがわかる．分布は正規分布で近似できる．

図 3 は，受信したすべての RPI を含む BLE フレームの信号強度と，それぞれの信号強度が最大値をとる時刻 (星のシンボル) を示す．図において，11 個 のユニークな RPI が観測されていること，およびそれぞれの RPI に対応する BLE 信号強度が最大値をとる時刻を検出できていることがわかる．プライバシーを考慮し，データの収集において， RPI はハッシュ値として保存した．

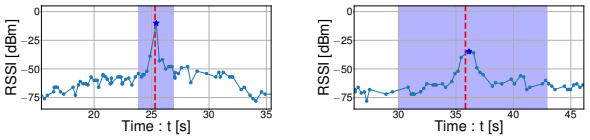
図 3 における RPI 1 に対応する時系列データを抽出したものを図 4 に示す．BLE 信号強度は，$t_{\max}(i) = 63.56$ [s] の時点で鋭いピークを持つ最大値をとることがわかる．図において，薄い紫色で示した領域は，ターゲットがカメラの画角にフレームインしてからフレームアウトするまでの時間を，赤い点線は，カメラの真正面に来た時間を示す．星のシンボルで示した時刻 $t_{\max}(i)$ に撮影した画像にターゲットが確実に含まれることがわかる．

図 5 は，図 4 で検出された時刻 $t_{\max}(i) = 63.56$ [s] に撮影した画像である．2 台 の USB カメラは連続で写真を撮影しているが，$t_{\max}(i)$ のタイミングと若干ずれるため，最も近いタイミングでキャプチャされた画像を採用する．対象者が正しく撮影され， YOLO v3 を用いて人物の画像を検出できたことがわかる．これらの実験結果は，ターゲットの RPI とその画像を結びつける陽性者特定攻撃が実現可能であることを明確に示している．

4.3 ターゲットと攻撃デバイスの距離

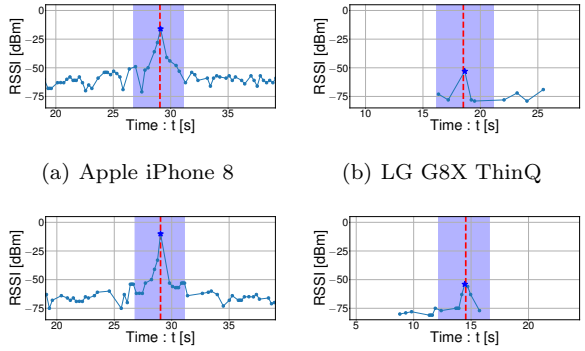
ターゲットのスマートフォンと，BLE 信号を計測するパラボラアンテナとの距離が離れたときにも攻撃が成功するかを検証する．一般的な歩道の幅は 7 [m] 以下である [20] ため，距離を 1 [m] から 7 [m] の範囲で変化させた．以下の実験では，ターゲットはスマートフォンをアンテナ側の手にもった状態で，攻撃デバイスの前方を歩行する．また，ターゲットのスマートフォンは iPhoneXR を採用した．

図 6 に，距離を 1 [m] および 7 [m] にしたときの， BLE フレームの信号強度の時間変化を示す．距離によらず，赤い点線で示した時刻 (ターゲットがカメラの真正面に来た



(a) 1 [m]　(b) 7 [m]

図 6　攻撃デバイスと歩行者の距離変動時の 時間–信号強度グラフ



(a) Apple iPhone 8　(b) LG G8X ThinQ

(c) Huawei P20 Lite　(d) Motorola/Google Nexus6

図 7　信号発信強度の異なる 4 台のスマートフォンにおける時間–信号強度グラフ (距離 2 [m])

時刻) と，星のシンボルで示した時刻 (電波強度が最大となった時刻) はきわめて近いことがわかる．つまり，BLE 信号強度が最大となる時刻で撮影した画像は，ターゲットを中央に撮影している．これらの結果は，一般的な歩道の幅である 1 [m] から 7 [m] の範囲において，陽性者特定攻撃が実現可能であることを示している．

4.4　スマートフォン機種の影響

スマートフォンの機種の違い，すなわち BLE 信号の送信電力強度，およびアンテナの利得が攻撃の成功率に与える影響を調査する．表 2 に示すように，スマートフォンの機種によって，BLE の送信電力とアンテナの利得は異なる．実験において，歩行者は，スマートフォンを手で持った状態で，攻撃デバイスの前方を通過する．歩行者が攻撃デバイスの前を通過する際の距離は 2 [m] に固定した．

図 7 に結果を示す．我々は，4 つのデバイスすべての場合において，攻撃が成功していること，すなわち，BLE の電波強度が最大となる時刻と，ターゲットがメインカメラの真正面に到着する時刻がほぼ一致していると判断する．また，図において，G8X ThinQ と Nexus6 に関しては，一部の信号しか観測されていないことがわかる．この結果は，2 つ の端末の電波送信強度が弱く，また送信アンテナの利得が十分に高くなかったため，ターゲットに近づくまでは信号が観測されなかった事実を反映している．そのようなデバイスに対しても，指向性が高いパラボラアンテナを活用することにより，ターゲットのデバイスから RPI データを取得することができる．

4.3 および 4.4 節に示す実験結果が示すように，RPI とターゲット画像の紐付けは，距離，デバイス種別によらず

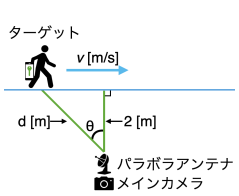


図 8　シミュレーションモデル

図 9　3D モデリングから生成された画像

表 3　シミュレーションで用いたパラメータ

	説明	値
G_t	対象スマートフォンの BLE アンテナゲイン	-4.9 [dBi]
G_r	パラボラアンテナのゲインの最大値	23 [dBi]
P_t	対象スマートフォンの BLE 送信電力	16 [dBm]
λ	BLE 信号の波長 (2.4 [GHz])	0.125 [m]
τ	BLE フレームの発信周期	0.270 [s]
$d_{\min}$	歩行者と攻撃デバイス間の距離の最小値	2 [m]

成立することがわかる．我々は，他の条件も実験したが，紙面の都合で割愛する．他の条件で実施した実験結果から得られる発見は同様であった．

5.　攻撃が大規模に行われたときの評価

本章の狙いは，**RQ2**: **攻撃はスケールするか？** を検証することである．物理空間における実験結果で得られた結果をもとに，シミュレーションを構築する．実験において，歩行者の人数，攻撃デバイスの台数に着目して，これらの要因が陽性者特定攻撃に与える影響を評価する．

5.1　シミュレーションモデル

本節ではシミュレーションモデルの概要を説明する．はじめに，シミュレーションの全体とプロセスを説明する．次に，シミュレーションの対象となる歩行者の振る舞いモデルを説明する．最後に，スマートフォンが発信する BLE 電波の伝搬モデルを説明する．

シミュレーションモデルの概要： 図 8 にシミュレーションモデルの構成要素を示す．ターゲットとなる人物には，それぞれ疑似 RPI としてランダムな数を付与する．この対象は，図の左から右の方向に向かって，速度 v [m/s] で等速直線運動する．v は後述するように，正規分布すると仮定する．対象の到着過程は，ポアソン過程に従うものとする．対象の軌跡は Panda3D を用いて，3D モデリング表現する [21] (図 9) ．このようなモデリングにより，カメラが撮影する画像を再現する．

図 8 において，θ はターゲットとパラボラアンテナの間の角度である．ターゲットごとに算出した電波強度の時間変化から，電波強度が最大になった時間を特定する．特定された時刻 $t_{\max}(i)$ に撮影された画像について解析し，3D モデリングを用いて再現する．画像において，θ が最小となったオブジェクト (人) に対して，受信した電波に対応する RPI を紐付ける．攻撃の成功率は，リンク結果を ground truth と比較することで算出する．シミュレーションにおいて利用した共通のパラメータは，表 3 に示す．

歩行者の振るまいモデリング: 前述したように，歩行者は

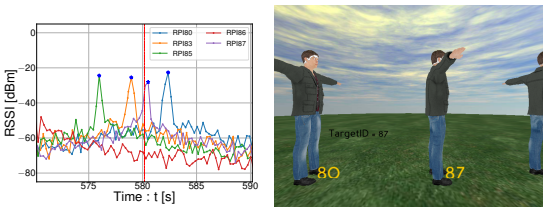


図 10 シミュレートされた時間–信号強度グラフ (左) と 一致する歩行者の 3D モデル (右)

ポアソン過程にしたがって，ランダム到着するものとする．本研究では，指数分布のパラメータ λ を $\lambda = n/3,600$ とした．ここで n は 1 時間 で到着する総人数であり，到着率は 1 秒 あたりの到着数である．個々の歩行者の歩行速度は，文献 [22] の実験結果に基づき，平均 1.30 [m/s], 標準偏差 0.22 の正規分布で与えた．

受信信号強度のモデリング: 攻撃者のパラボラアンテナが受信する BLE の電波信号強度は，フリスの伝達公式に基づいて算出する [23]．BLE 送信アンテナの絶対利得を G_t [dBi]，パラボラアンテナの絶対利得を G_r [dBi]，BLE の送信電力を P_t [dBm]，ターゲットとアンテナの距離を d [m]，電波波長を λ [m] とする．パラボラアンテナにおける受信電力 P_r [dBm] は， d と θ から以下の式で計算できる．

$$P_r(d,\theta) = 10\log_{10}\left(\frac{\lambda}{4\pi d}\right)^2 + G_t + G_r + P_t, \qquad (1)$$

$G_r(\theta)$ は，パラボラアンテナのゲインマップから求まる [24]．実空間では，都市雑音や歩行者の動き，伝搬損失などの減衰要因がある．本研究では，これらの要因を再現するために加法性白色ガウス雑音と損失補正を導入し，式 $P_r^* = P_r + \epsilon + \eta$ を用いる．経験的に加法性白色ガウス雑音を $\epsilon \sim \mathcal{N}(0, 3^2)$ ，損失補正値を $\eta = -12$ とした．図 10 にパラボラアンテナで受信した BLE 信号の強度 (左) と，RPI を含む BLE フレームに対応する歩行者の画像 (右) をシミュレーションした結果を示す．

5.2 1 時間あたりの歩行者の人数

はじめに，歩行者の到着率が陽性者特定攻撃の成功に与える影響を調べる．1 時間あたりの歩行人数 N を増加させたときに，攻撃の成功割合がどのように変化するかを，シミュレーション実験により評価する．N は 200 から 10,000 まで変化させた．結果を表 4 に示す．シミュレーションは同一条件で 3 回 行い，その平均値を結果として示した．リンクを行った際，ターゲットが何人の候補に絞り込めたかを m によって表現する．$m = 1$ は攻撃が完全に成功したこと，つまり 1 つ の RPI を 1 人 分の画像と紐付けることに成功したこと， $m = 2$ は，1 つの RPI を 2 人 分の画像のどちらかであると紐付けることに成功したこと，を意味する．なお，各行の合計は 100% にはならない．これは，誤ったリンクが行われたときをカウント対象にしていないことによる．表から，$N = 1,000$ のとき，陽性者特定攻撃は 81% の歩行者に対して完全に成立することがわかる．また，$N = 5,000$ のとき，完全に攻撃が成功する割合は 42% , 2 人 以下にまで候補を絞り込める割合は 60% である．一方，$N = 5,000$ の場合，歩行者間の平均距離は 1 [m] である．そのような場合にあっても，陽性者特定攻撃が成功することがわかった．今回のシミュレーション時間は 1200 秒とした．

表 4 1 時間あたりの歩行者人数 N と攻撃成功率

N	$m=1$	$m=2$	$m=3$	$m=4$	$m\geq 5$
200	96.637	1.212	0.000	0.000	0.000
400	93.216	2.917	0.000	0.000	0.000
600	90.585	4.203	0.169	0.000	0.000
800	82.252	7.424	0.256	0.000	0.000
1000	81.205	8.238	0.303	0.000	0.000
5000	41.889	18.243	2.283	0.201	0.020
10000	23.321	16.716	4.024	0.481	0.050

表 5 攻撃デバイス設置台数 L と 攻撃成功率

L	$m=1$	$m=2$	$m=3$	$m=4$	$m\geq 5$
1	41.415	17.938	2.725	0.156	0.020
2	61.048	15.729	5.325	1.078	0.140
4	83.256	5.476	3.524	1.828	0.709
6	93.491	1.938	1.304	0.994	0.615

5.3 攻撃デバイスの台数

攻撃デバイスの設置台数が攻撃に与える影響を評価する．攻撃デバイスは，歩行者が進む直線上に 100 [m] おきに等間隔に設置した．攻撃デバイスの台数 L を増加させたときの攻撃成功割合を調査した．結果を表 5 に示す． 1 時間あたりの歩行人数を $N = 5,000$ とした．攻撃デバイスの設置台数が増加するにつれ，攻撃成功割合が増加する．攻撃デバイスが 1 台 のとき，完璧な攻撃成功割合は 41% であったのに対し，攻撃デバイスの台数を $L \geq 4$ とすることで，完璧な攻撃成功割合を 80% 以上にすることが可能となる．このように，攻撃デバイスを増やすことにより，攻撃成功割合が高まることがわかった．

6. 対策

本章の狙いは， **RQ3**: **本攻撃に対する効果的な対策は何か？** を明らかにすることである．DCT フレームワークにおける陽性者特定攻撃に対する対策を議論し， DCT フレームワークの開発者や OS ベンダーなどのステークホルダーに対するいくつかの提言をする．

6.1 Interacted-RPI

フレームワーク開発者が対応すべき対策として，診断鍵と RPI のマッチングに複数の連続した RPI を使用する新しい方式を提案する．この方式では，攻撃者は少なくとも RPI の更新期間以上の期間，ターゲットの RPI を観測する必要がある．結果として，陽性者特定攻撃が困難になる．現在の GAEN の実装では， TEK と タイムスタンプ から一意に算出された RPI が BLE を用いて広告される．一方，提案する方式では，複数の連続した RPI によって算出される新しい識別子として，interacted-RPIs (I-

Algorithm 1: I-RPI の算出アルゴリズム

```
Data: RPI, PreviousIRPI, CurrentIRPI
initialization;
PreviousIRPI = random();
if RPI changes then
    CurrentIRPI = PreviousIRPI ⊕ RPI;
    Output CurrentIRPI;
    PreviousIRPI = CurrentIRPI ;
```

RPIs) を用いる．I-RPI ($currentIRPI$) は，現在時刻の計測値 (RPI) と 過去の I-RPI ($previousIRPI$) の排他的論理和 (XOR) によって算出される．I-RPI の算出アルゴリズムを Algorithm 1 に示す．RPI は 15 分 ごとに変動するため，攻撃者は平均して 7 分 30 秒 ，ターゲットの I-RPI を観測する必要がある．攻撃者は ターゲットの歩行経路上に約 586 [m] の距離を置いて攻撃デバイスを設置する必要がある．一般に，歩行者は多様な経路で歩行するため，本攻撃が難しくなる．近距離に陽性者と 15 分 以上近接する人が濃厚接触者として定義されるため，本対策を導入しても濃厚接触者は適切に陽性者の連続した I-RPI を受信し，濃厚接触を判定することができる [25].

受信デバイスは，1 日 1 回 ，受信した I-RPI と 陽性者の RPI を XOR した値 を比較する．I-RPI の導入によって受信機側に生じるオーバーヘッドを評価する．Android スマートフォン (G8X ThinQ) を用いてオーバーヘッドを計測した．1 タイムウインドウ (15 分) におけるオーバーヘッド は 1.71 [s] となることがわかった．このとき，1 日あたりの陽性者数が 10,000 人, 1 タイムウインドウ (15 分) あたりの近接する人の人数が 100 人 とした．したがって，オーバーヘッドは 15 分ごとに 2 秒 以下となり，十分に小さいことがわかる．

6.2 信号発信周期の調整

フレームワーク開発者と OS ベンダが対応すべき対策として，信号の送信間隔を長くすることで攻撃成功確率を低下させる手法を提案する．GAEN において， RPI は 200-270 [ms] の間隔で BLE フレーム を用いて広告される [6]．受信側の端末は，5 分 のスキャンウインドウごとに 4 秒間 BLE フレームを受信するスキャンを行う．濃厚接触判定を行うためには，受信デバイスはスキャンウインドウごとに少なくとも 1 つの RPI を含む BLE フレームを受信する必要がある．BLE フレーム が 200-270 [ms] という高周期で広告されるため，攻撃者は高い精度で信号強度グラフを描画し，ピーク検出を行うことができる．そのため，信号発信間隔を長くすることで信号強度グラフの解像度を低下させ，ピーク検出が困難となる．

攻撃成功割合 ： シミュレーションを行い，信号発信周期を調整する対策の有効性を検証した．信号発信間隔を 270 [ms] から 60 [s] まで変動させて，攻撃成功率を調べた．シミュレーションにおいて，1 時間あたりの歩行者人数 $N = 800$ 人とする．また攻撃者は 1 台 の攻撃デバイスを用いる．信号発信間隔を 15 [s] とすると，攻撃の成功率がおよそ 13% まで低下することがわかった．このとき，適切に RPI を受信できるようにするために，スキャンウインドウあたりのスキャン期間を 4 [s] から 15 [s] に変更する必要がある．

消費電力 ： 本対策がバッテリー消費電力に与える影響を評価する．p_t と p_r を BLE 信号の送信, 受信の 1 [ms] ごとの消費電力とする．P_{orig} と P_{new} を現在の GAEN フレームワークと提案する対策における消費電力とする．紙面の都合上詳細は割愛するが，一般に $p_t = p_r$ である [26] こと，および BLE 通信において，1 つのフレームを送信するのに必要な時間は 380 [us] であることなどを利用して，$P_{new}/P_{orig} = 3.39$ と計算できる． つまり，提案する対策を適用することで，消費電力は約 3.4 倍に増加する．ただし BLE の消費電力は非常に低いため [27], [28]，消費電力への影響は限定的であると考えられる

7. 研究倫理

本実験は，プライバシーに配慮した上で実験を行い，著者および事前に同意を得た知人のみを対象とした．本研究は，特定の条件下でプライバシーの脅威が顕在化することを実証したものであるが，いくつかの条件を満たす必要があるため，一般ユーザーのプライバシーが直ちに侵害されるような状況にはない．本研究が対象とした攻撃の脅威を軽減することを目的として，我々は 2021 年 2 月 11 日に調査結果と実行可能な対策を Google 社に報告した．この結果，同年 2 月 19 日に Google 社より「接触通知プログラムの観点から，この攻撃は対象外と考えている．これは，設計段階で考慮されたものである」との回答があった．同社の回答が示唆するように，本研究で対象とした攻撃は特定のアプリケーションの脆弱性に起因するものではなく，フレームワークの設計や BLE の設計上の問題に起因する．本研究成果を発表することで，多くの関係者に知見を共有し，議論が深まることが期待される．本研究が明らかにした攻撃成立条件や対策は，既存のフレームワークやプロトコルの設計を見直す際，および新たなフレームワークの開発時に活用でき，潜在的なプライバシーリスクの低減に貢献することが期待される．

8. 関連研究

GAEN フレームワークにおいて，陽性者の行動履歴を明らかにする攻撃手法は広く研究されている [29], [30], [31]. これらの研究のアイディアは，複数の BLE 受信機を設置，歩行者の RPI の収集を行い，陽性者の情報と比較することで，陽性者の行動履歴を追跡することである．しかし，これらの研究では写真や信号強度を用いて，特定の陽性者

を識別する手法について議論や検討がされていない．概念実証として，陽性者と画像を紐付ける攻撃が議論されている [2], [3], [4], [32]．本研究は，科学的に再現性のある方法で陽性者特定攻撃とその対策を評価した初めての研究である．

9. 結論

本研究は，DCT フレームワークにおける，RPI と人物の画像を紐付ける陽性者特定攻撃の実現可能性を評価した．この結果，陽性者特定攻撃の実現可能性が高いこと，および攻撃者は数台のデバイスを使うことで，毎時 5,000 人 の歩行者人流に対して 80% 以上の確率で攻撃が成功することを明らかにした．さらに，本攻撃の対策として，複数の RPI を用いる新たなメカニズムの導入や BLE フレームの広告周期を適切に調整する手法を提案し，有効性をシミュレーションによって明らかにした．

謝辞 本研究の一部は JSPS 科研費 19H04111 の助成を受けたものです．本研究の初期検討時に貴重な助言を頂いた佐古和恵氏に感謝します．

参考文献

[1] WHO UNICEF and IFRC. Social stigma associated with the coronavirus disease (COVID-19). https://www.unicef.org/documents/social-stigma-associated-coronavirus-disease-covid-19, Mar 2020.

[2] Tijmen Schep. CORONA DETECTIVE & CORONA MILDER. https://www.tijmenschep.com/corona-detective-corona-milder/, Dec 2020.

[3] Vincenzo Iovino. Immuni Detector & Paparazzi attack+camera. https://sites.google.com/site/vincenzoiovinoit/immuni, Jul 2020.

[4] Serge Vaudenay. Analysis of DP3T. Cryptology ePrint Archive, Report 2020/399, 2020. https://eprint.iacr.org/2020/399.

[5] 野本一輝ほか. Exposure Notification Framework がもたらすプライバシーリスクの評価と対策. Feb 2021.

[6] Apple and Google. Exposure Notification Bluetooth Specification. https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf, Apr 2020.

[7] Apple and Google. Exposure Notification Cryptography Specification. https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf, Apr 2020.

[8] Google. Exposure Notifications BLE attenuations. https://developers.google.com/android/exposure-notifications/ble-attenuation-overview, Nov 2020.

[9] Joseph Redmon, et al. You Only Look Once: Unified, Real-Time Object Detection, 2016.

[10] Stephen Farrell. October 2020 Survey of GAEN App Key Uploads. https://down.dsg.cs.tcd.ie/tact/survey10.pdf, Oct 2020.

[11] Doug Leith Stephen Farrell. Testing Apps for COVID-19 Tracing (TACT) - TEK Survey. https://down.dsg.cs.tcd.ie/tact/tek-counts/, Jul 2021.

[12] Google. google / exposure-notifications-server. https://github.com/google/exposure-notifications-server/blob/main/tools/export-analyzer/main.go, Feb 2021.

[13] Michael Ossmann. greatscottgadgets / ubertooth. https://github.com/greatscottgadgets/ubertooth/, Jul 2021.

[14] Premiertek. Outdoor 2.4GHz 24dBi Directional High-Gain N-Type Female Aluminum Die Cast Grid Parabolic Antenna Part#: ANT-GRID-24dBi. http://www.premiertek.net/products/networking/ANT-GRID-24dBi.html.

[15] UL Verification Services Inc. MPE report. https://bit.ly/3leUBq4, Sep 2017.

[16] UL Verification Services Inc. MPE report. https://bit.ly/3igifAQ, Sep 2018.

[17] Dt&C Co Ltd. Bluetooth LE Test Report. https://fccid.io/ZNFKA1935/Test-Report/Bluetooth-LE-Test-Report-4450952.pdf, Sep 2019.

[18] SGS-CSTC Standards Technical Services Co Ltd Shenzhen Branch. RF test report of LTE B26. https://bit.ly/3ff5VyS, May 2018.

[19] Sporton International INC. FCC RF Test Report. https://fccid.io/IHDT56QD2/Test-Report/Test-Report-BT-LE-2421227.pdf, Oct 2014.

[20] Meli Harvey. sidewalkwidths-nyc. https://github.com/meliharvey/sidewalkwidths-nyc, Mar 2021.

[21] Carnegie Mellon University. Panda3D — Open Source Framework for 3D Rendering & Games. https://www.panda3d.org/, Jul 2021.

[22] M Amanda and NYC Director. New York City Pedestrian Level of Service Study Phase I. 2006.

[23] H.T. Friis. A Note on a Simple Transmission Formula. *Proceedings of the IRE*, Vol. 34, No. 5, pp. 254–256, 1946.

[24] TP-LINK. TP-LINK 2.4GHz 24dBi Grid Parabolic Antenna TL-ANT2424B Data Sheet.

[25] Centers for Disease Control and Prevention. Appendices. https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/appendix.html, Jul 2021.

[26] Jia Liu, et al. Energy Analysis of Device Discovery for Bluetooth Low Energy. In *2013 IEEE 78th Vehicular Technology Conference (VTC Fall)*, pp. 1–5, 2013.

[27] Health Service Executive. Technology the COVID Tracker app uses - HSE.ie. https://www2.hse.ie/services/covid-tracker-app/why-use-the-covid-tracker-app.html, Jul 2020.

[28] Commonwealth of Pennsylvania. COVID Alert PA Frequently Asked Questions. https://www.health.pa.gov/topics/disease/coronavirus/Pages/COVID-Alert-FAQs.aspx, Jul 2021.

[29] Jianwei Huang, et al. On the Privacy and Integrity Risks of Contact-Tracing Applications, 2020.

[30] Lars Baumgärtner, et al. Mind the GAP: Security Privacy Risks of Contact Tracing Apps. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 458–467, 2020.

[31] O. Seiskari. BLE contact tracing sniffer PoC. https://github.com/oseiskar/corona-sniffer, Mar 2020.

[32] Yaron Gvili. Security Analysis of the COVID-19 Contact Tracing Specifications by Apple Inc. and Google Inc. Cryptology ePrint Archive, Report 2020/428, 2020. https://ia.cr/2020/428.