

意図しないBLE接続を防ぐ デジタルサイネージ・スマートフォン連携システムの構築

中島 博敬^{1,a)} 鈴木 茂哉¹ 徳永 徹郎² 田中 清² 宮崎 泰彦² 丸山 剛一² 中村 修³

概要：デジタルサイネージとスマートフォンが連携したシステムにおいて、BLE ビーコンを用いてスマートフォンとデジタルサイネージを安全に関連付ける方式について提案する。既存のデジタルサイネージとスマートフォンの連携では二次元バーコード等が用いられているが、Bluetooth Low Energy のブロードキャスト通信 (BLE ビーコン) を用いても連携できる。一方、BLE ビーコンでは電波を用いる為、真正なビーコンに成りすました不正ビーコンにより悪意のある情報を配信することが可能であり、物理空間上に存在するデジタルサイネージと、デジタルサイネージから広告されるビーコンの関連付けが課題であった。提案手法では、BLE ビーコンから発信された URL を用いてスマートフォンがデジタルサイネージに接続した際、スマートフォンがデジタルサイネージに正しく接続されているか識別子を用いた検証により信頼関係の構築を可能とする。この手法により、同じ空間上に複数台のデジタルサイネージが存在するような環境下においてもユーザはスマートフォンが接続されたデジタルサイネージを識別可能である。提案手法の有用性を検証するため実装を行い、スマートフォンが接続されたデジタルサイネージを検証できるか、および複数台環境下において識別できるかの2点で定性評価を実施し、提案手法が有用である評価を得た。

1. はじめに

一般的に、デジタルサイネージは情報を不特定多数のユーザに対して配信することを目的として設置される。デジタルサイネージでは、表示するコンテンツを柔軟に変更することができるため、タッチパネルと組み合わせることでインタラクションによりユーザが求める情報の提供が可能となる [1] が、インタラクション中はデジタルサイネージのスクリーンをユーザが占有してしまうという問題が指摘されてきた [2]。

ここで、多くのユーザが所持する、スマートフォンと連携することでニーズに合ったより詳細な情報をユーザに提供できる。

デジタルサイネージとスマートフォンの連携では、二次元バーコードや、デジタルサイネージに表示された URL をユーザが手入力する手法などが従来用いられている [3] が、Bluetooth Low Energy (BLE) のブロードキャスト通信 (BLE ビーコン) を用いた連携が考え得る。

BLE ビーコンは電波を用いる為、真正なビーコンに成りすました不正ビーコンにより悪意のある情報を配信するこ

とが可能である。そのため、BLE ビーコンと物理空間に存在するデジタルサイネージの関連付けなしには、情報空間に存在するデジタルサイネージから送信された情報を信頼することができず、結果としてデジタルサイネージとコンテンツ間の信頼関係を構築できない。

そこで、本研究では、BLE ビーコンを用いて情報空間に存在するデジタルサイネージと、物理空間上に存在するデジタルサイネージを識別する手法について検討を行い、実際にシステムを構築し有用性について評価を行った。

本論文の構成は以下の通りである。2章ではデジタルサイネージとスマートフォンの連携手法として二次元バーコードと Bluetooth Low Energy ブロードキャスト通信について整理する。3章では本研究の提案手法である、意図しない BLE 接続を防ぐデジタルサイネージ・スマートフォン連携システムの提案についてその目的と提案手法について述べる。4章ではデジタルサイネージ・スマートフォンへの本提案手法の実装手法の検討と実装について述べる。5章では本提案手法と従来の BLE ビーコンによるスマートフォンへの URL 広告手法について定性評価を実施し、結果について述べる。最後に6章で、まとめと今後の課題について述べる。

¹ 慶應義塾大学大学院 政策・メディア研究科

² 日本電信電話株式会社 NTT サービスエボリューション研究所

³ 慶應義塾大学 環境情報学部

a) hiro@awa.sfc.keio.ac.jp

2. デジタルサイネージとスマートフォン連携手法

デジタルサイネージとスマートフォンの連携について様々な手法が提案されているが、ここではデジタルサイネージとスマートフォン間で通信を確立する操作をペアリングと定義し、主なペアリング手法について整理する。

2.1 二次元バーコード

デジタルサイネージは、スクリーンを用いて情報を伝達することから、画面上にペアリングに必要な情報を表示させることでペアリングを行う事が可能である。最も簡易な手法は、画面に情報を表示し、ユーザのスマートフォン上に入力させるという手法である。

また、情報の入力を簡便にする手法としては、バーコードを利用する手法も考えられ、二次元バーコードを表示し、それをスマートフォンで読み取ることで、ペアリングを行うという手法 [4] も提案されている。

2.2 Bluetooth Low Energy ブロードキャスト通信

デジタルサイネージとスマートフォンを連携する手法として電波の利用が考えられ、スマートフォンに一般的に搭載されている Bluetooth を用いた手法が考えられる。

Bluetooth Low Energy は Bluetooth 規格の一つであり、GATT(Generic Attribute Profile) というプロファイルを利用することで、近傍に存在する不特定多数の端末に情報をブロードキャストすることが可能である。

Bluetooth Low Energy のブロードキャスト通信を行う方式として Apple により提案された iBeacon[5] と Google により提案された EddyStone[6] が広く利用されている。

2.2.1 iBeacon

iBeacon は Apple により提案された Bluetooth Low Energy によるビーコン規格である。iBeacon ではビーコンはあらかじめ定義された UUID に加え Major, Minor それぞれ 16 ビットの情報を発信することができる。

2.2.2 EddyStone

EddyStone は Google により提案された Bluetooth Low Energy によるビーコン規格である。EddyStone は下記に示す 3 つの動作モードが存在する。

- EddyStone-UID

EddyStone-UID は iBeacon とほぼ同等の UUID, Major, Minor 情報の発信が可能である。

- EddyStone-URL

EddyStone-URL は最大 17 バイトの URL を送信することが可能である。

- EddyStone-TLM

EddyStone-TLM はビーコンのバッテリー電圧や気温などのテレメトリ情報の発信が可能である。

3. 意図しない BLE 接続を防ぐデジタルサイネージ・スマートフォン連携システムの提案

3.1 研究の目的

情報伝達において、発信者・受信者間の信頼関係の構築が大きな問題であることは広く知られている。デジタルサイネージシステムにおいても同様であり、発信者・受信者間の信頼関係を構築する手法として、発信者が配信したコンテンツが正しく配信されているかを報告するシステム [7] などが提案されている。

一方、デジタルサイネージとスマートフォンの連携システムでは、スマートフォンに表示される情報は物理空間ではなく情報空間に存在する。そのため、1 章で述べたとおり、物理空間上で構築されたデジタルサイネージとユーザ間の信頼関係を、情報空間上にも展開しなければ、ユーザはスマートフォン上に表示される情報を信頼することができない。一度、デジタルサイネージとスマートフォン間の信頼関係が構築されてしまえば、ユーザはスマートフォン上に表示されるデジタルサイネージの情報を信頼できるようになる。

このデジタルサイネージとスマートフォン間の信頼関係の構築作業は通信路を確保するペアリングに加え、ユーザによるスマートフォンが意図したデジタルサイネージに接続されているかを検証するプロセスが必要である。本研究ではこのプロセスを通信相手の検証と定義する。

ここでは 2 章で整理したペアリング手法について、物理空間上に存在するデジタルサイネージと、情報空間上に存在するスマートフォン間で信頼関係を安全かつ簡単に構築するという観点から議論を行う。

二次元バーコードを利用した場合、ユーザはデジタルサイネージに表示された情報をスマートフォンで読み取るため、ユーザは確実に意図したデジタルサイネージとスマートフォンをペアリングでき、通信相手の検証なしに信頼関係の構築が可能であるため、信頼性は非常に高い手法である。一方、ユーザはスマートフォンをデジタルサイネージにかざして情報の読み取りを行う必要があり、第三者によりユーザが、デジタルサイネージとスマートフォンを連携したことを観察できてしまうというプライバシー上の問題がある。また列車内や美術館などの空間ではカメラの利用が制限されるため利用できないという問題がある。

一方 BLE ビーコンでは、二次元バーコードのようにスマートフォンのカメラでデジタルサイネージに表示された情報を読み取る必要はなく、二次元バーコードで発生するプライバシーや空間固有の問題を回避することができる。しかし、BLE ビーコンは電波を用いることから、通信相手の検証は二次元バーコードのように視覚的に確認することができないため、信頼性が低い手法である。すなわち、BLE ビーコンは下記の問題を抱えている。

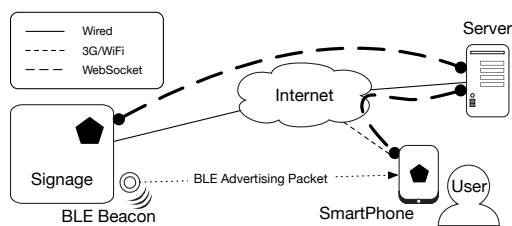


図 1 システム概要

- 受信したビーコンが真正なビーコンであるかを検証できない。
- 同じ空間内にデジタルサイネージが複数設置されているような状況で、ユーザは受信したビーコンがどのデジタルサイネージから送信されたビーコンであるか識別できない。

デジタルサイネージを複数ユーザで同時に利用する手法 [2] では、ユーザのスマートフォンとデジタルサイネージ上に図形や色彩情報が異なるポインタを表示することにより、複数ユーザによる同時利用が可能となる手法が提案されている。複数ユーザが同時に利用する場合でも、デジタルサイネージとスマートフォンの連携は欠かすことができず、ペアリングや通信相手の検証は重要である。

上記の問題を考慮し、本研究では BLE ビーコンを用いて安全かつ簡単にデジタルサイネージとスマートフォン間でペアリングを行った後、通信相手を検証する手法を提案する。またその際、近傍に複数台のデジタルサイネージが存在する場合でも動作するアーキテクチャを目指す。

3.2 提案手法

本研究では、デジタルサイネージから発信された BLE ビーコン情報を受信したスマートフォンが、デジタルサイネージに接続した際、デジタルサイネージ・スマートフォン双方に同一の識別子を表示することで、ユーザが接続されたデジタルサイネージの識別が可能となるシステムを提案する。

図 1 に提案手法の概要を示す。

まず、BLE ビーコンは情報を一方向にのみ発信可能であり、BLE ブロードキャスト通信だけではスマートフォンは受信したビーコンが真正なデジタルサイネージから発信されたビーコンであるか検証することができない。

一般に、ある通信路が信頼できないと仮定した場合、その通信路の通信を検証するには代替通信路を用いて検証する。デジタルサイネージとスマートフォンの通信相手の検証において代替通信路としてインターネットが利用できる。デジタルサイネージとスマートフォンは WiFi や携帯電話網に接続されており、PKI [8] や DNSSEC [9] などインターネットで安全な通信を支援する技術を用いることで、安全な接続を確立できる。

2.2 節で整理したように、BLE ビーコンは主に 2 つの方

式が存在する。本提案手法で選択する BLE ビーコンについては 4 章にて議論する。

まず、スマートフォン側クライアントアプリケーションは BLE ビーコンに含まれる情報からサーバに接続を行う。前述の通りサーバとスマートフォン間は PKI や DNSSEC により安全な接続が確立でき、信頼関係を構築することができる。

サーバは、デジタルサイネージとも安全に接続されており、デジタルサイネージ・スマートフォン双方共に複数台からの接続を受け入れ、デジタルサイネージ・スマートフォンの通信を中継する。この際、サーバはスマートフォンが受信した BLE ビーコンに含まれたデジタルサイネージ情報に基づき、通信を中継するデジタルサイネージを決定する。この際、ビーコンに含まれた情報が不正な情報である場合、サーバはスマートフォンからのリクエストを中継すべきサイネージが存在しないことを検知できるため、不正なビーコンの排除が可能である。

一般的に、BLE ビーコンは 10m~50m 程度の範囲にビーコンを伝搬させることが可能である。そのため、ビーコンが届く範囲に複数台のデジタルサイネージが設置されているような状況では、ユーザが意図しないデジタルサイネージに接続する可能性が存在する。

そこで、サーバを経由してスマートフォンからの接続要求を受け取ったデジタルサイネージは、ユーザが視覚的に識別可能な図形を用いた識別子を発行し、サーバを経由してスマートフォンに送信する。同時に、デジタルサイネージはスマートフォンに送信した識別子をディスプレイ上に表示させ、ユーザにスマートフォンが接続したことを通知する。

ユーザは、スマートフォンに表示されたデジタルサイネージから受信した識別子と、デジタルサイネージ上に表示された識別子を照合することで、意図したデジタルサイネージに接続されているかを検証できる。

スマートフォンが接続されたデジタルサイネージが真正であることを確認した後は、ユーザは、識別子をデジタルサイネージ上で移動させることが可能となる。そこで、ユーザがデジタルサイネージ上に表示された情報をスマートフォンで選択することで、デジタルサイネージから詳細な情報が送信されユーザは詳細な情報を閲覧できる。

4. 実装

本提案手法の有用性を確認するため、デジタルサイネージとスマートフォンの連携システムを構築した。

4.1 BLE ブロードキャスト通信方式の検討

BLE ブロードキャスト通信の方式として EddyStone-URL 方式を採用した。理由を下に述べる。

- iBeacon は UUID と Major, Minor ID を利用してビー

コンを識別するが、デジタルサイネージのように運用者が多岐にわたるシステムにおいて Major, Minor ID を管理することが難しい。

- EddyStone-URL 方式は Web ブラウザに組み込みが予定されており、ブラウザから直接ビーコンに含まれる URL に接続が可能である。

デジタルサイネージは、システム内に組み込まれた EddyStone BLE ビーコンを利用し、予め定義された一意な URL を広告する。

4.2 クライアント実装

スマートフォンクライアントは JavaScript により実装を行った。本研究では Web アプリケーションとして実装を行い、専用のアプリケーション無しに動作することを目指したが、Web ブラウザによる EddyStone のサポートが Google Chrome for Android の一部バージョンに限定される [10] ことから、JavaScript アプリケーションをスマートフォンネイティブアプリケーションに変換する Apache Cordova[11] を利用し、スタンドアロンアプリケーションを作成した。

4.3 デジタルサイネージ・サーバ実装

デジタルサイネージとして、Google Chrome を動作させたコンピュータを用いた。デジタルサイネージには 3.2 節で述べたとおり、EddyStone-URL ビーコンを組み込み、一意の URL を広告した。

一意の URL は、サーバをホスト名に持ちデジタルサイネージの ID をパスに持つ URL とし、スマートフォンクライアントは受信したビーコンに含まれる上記 URL に接続する。

デジタルサイネージとスマートフォン間の通信は WebSocket を利用し、サーバにより中継される。スマートフォンクライアントはビーコンに含まれる URL に接続する機能のみが実装されているため、WebSocket 通信に必要な機能的な JavaScript コードはサーバより取得し実行する。

4.4 識別子

物理・情報空間の関連付けのため、本提案システムではデジタルサイネージ・スマートフォン双方に識別子を表示する。実装では、識別子として事前に用意した図形画像を用いた。

5. 評価

評価においては、本提案手法とデジタルサイネージに特定の URL を広告する EddyStone-URL ビーコンを備え付けた 2 つの環境を用意し、下記の項目について定性的に評価を実施した。

- スマートフォンで受信したビーコンが真正なビーコン

であると確認できるか。

- 同じ空間内にデジタルサイネージが複数設置されている環境下で、ユーザは受信したビーコンがどのデジタルサイネージから送信されたビーコンであるか識別できるか。

表 1 は評価結果を示す。

表 1 提案手法と既存手法の比較

	提案手法	BLE ビーコンのみ
デジタルサイネージの真正性検証	○	×
複数台環境における識別	○	×

デジタルサイネージに EddyStone-URL ビーコンのみを実装した場合、ユーザはスマートフォンが接続した URL がデジタルサイネージが広告した URL か検証できない。また、複数台サイネージが存在する環境下では接続されたデジタルサイネージを識別できない。

対して、本提案手法では、ユーザはスマートフォンを利用してデジタルサイネージから発信されたビーコンに含まれる URL に接続した際、接続先のデジタルサイネージとスマートフォン双方に識別子である図形が表示され、図形の一致により、接続されたデジタルサイネージが真正であるか確認できた。また複数台のデジタルサイネージが存在する環境においても、表示される図形を確認することにより、どのデジタルサイネージに接続されているか確認することができた。

6. まとめ

本提案手法により、真正なデジタルサイネージの場合、デジタルサイネージ・スマートフォン双方に一意な図形が表示され、ユーザが接続されたデジタルサイネージが情報空間上で真正であり、物理空間上に存在することが検証できた。

一方、ユーザの検証無しに BLE ビーコンから送信された情報だけでは真正か不正かを識別することができず、不正な BLE ビーコンから発信された不正な URL にユーザが誘導される恐れがある。

今後、真正なビーコン情報を情報空間で事前に共有する等の手法を用いることで、BLE ビーコンの真正性検証が可能となり、より安全なスマートフォン・デジタルサイネージ連携が実現できると考えられる。

参考文献

- [1] 中村伊知哉：デジタルサイネージの動向、情報管理、Vol. 55, No. 12, pp. 891-898 (オンライン), DOI: 10.1241/johokanri.55.891 (2013).
- [2] 宮田章裕, 瀬古俊一, 青木良輔, 橋本遼, 石田達郎, 伊勢崎隆司, 渡辺昌洋, 井原雅行：デジタルサイネージとモバイル端末を連携させた複数人同時閲覧のための情報

- 提示システム, 情報処理学会論文誌, Vol. 56, No. 1, pp. 106–117 (2015).
- [3] Lee, J., Lee, J., Jung, H., Moon, S. and Yoon, K.: Smart digital signage using smartphone, *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, pp. 978–981 (2013).
 - [4] 徳永徹郎, 宮崎泰彦, 井元麻衣子, 中茂睦裕, 市井亮美, 加藤晃市: M-030 Web アプリケーションへのマルチデバイス連携フレームワークの適用と評価 (M 分野: ユビキタス・モバイルコンピューティング, 一般論文), 情報科学技術フォーラム講演論文集, Vol. 12, No. 4, pp. 389–392 (2013).
 - [5] Apple Inc.: iBeacon for Developers, (online), available from <https://developer.apple.com/ibeacon/> (accessed 2016-05-01).
 - [6] Google Inc.: Beacons — Google Developers, (online), available from <https://developers.google.com/beacons/> (accessed 2016-05-01).
 - [7] 坂田浩二, 井上博之, 前田香織: コンテンツ表示のディペンダビリティを向上させたデジタルサイネージ監視システムの開発, 情報処理学会論文誌, Vol. 53, No. 3, pp. 987–996 (2012).
 - [8] Cooper, D., Santesson, S., Farrell, S., yen, S. B., Housley, R. and Polk, T.: RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, *Internet RFCs* (2008).
 - [9] Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S.: RFC 4033: DNS Security Introduction and Requirements, *Internet RFCs* (2005).
 - [10] Mohan, A.: The Physical Web expands to Chrome for Android, Google Inc. (online), available from <http://goo.gl/jsbNys> (accessed 2016-05-01).
 - [11] The Apache Software Foundation: Apache Cordova, (online), available from <https://cordova.apache.org> (accessed 2016-05-01).