Tachyon:プライバシを考慮する電子タグ位置情報管理機構

岩井 将行[*] 高橋 元[*] 門田 昌哉[*] 中島 達夫[‡] 徳田 英幸[†*]

近年，RF タグとタグリーダの小型化と低価格化によって普及が可能になった．しかしユーザの望まない人や望まないアプリケーションに自らの位置情報が伝わってしまい，ユーザが不快な思いをする場面が発生し始めている．また，既存の位置情報システムが多く採用している中央集権的なデータベースは，管理者に対する信頼を前提としており，一括してユーザの情報が監視されている印象をユーザに与えてしまう問題点がある．著者らの開発した分散型位置管理機構：Tachyon は，ユーザの位置情報の伝播をユーザが望むプライバシの範囲で制限可能である．さらに Tachyon は，サーバーレスで動作し，ノード間の構成を容易に変更することが可能であり，拡張性のある位置情報管理システムといえる．

1. はじめに

近年，RFID のタグリーダの技術の発展と製品コストの低下している．RFID のタグの小型化の成功によって，RFID タグをユーザの携帯電話や財布などに貼り付けて持ち歩くことも可能になった．電池で駆動するアクティブ RF タグ，電池を持たないパッシブ RF タグ共に 5m〜10m の遠隔からでも読み取れるリーダが開発されている．そのため背景から RFID をユーザに携帯させユーザの位置情報の管理に利用する研究が注目されている．タグはユーザが能動的に指示をださなくても自動的に読み取ることが可能であるため位置情報管理システムには使い勝手がよい．

ユーザの位置情報管理システムは，オフィスのセキュリティシステムや会議運営，遊園地のアトラクションの混雑具合の把握，美術館の道案内にいたるまで様々な場面で応用が可能でありユビキタス環境のアプリケーションの代表とも言える．

しかしこういった RFID の現状の中において，2 つの弊害によって今後 RFID を使った位置情報管理システムの普及が鈍化することが予想できる．

プライバシが考慮されない位置情報管理への躊躇

ユーザの意図が反映されていなくても位置情報が取得できてしまう特性からユーザの「位置情報を公開したくない」場面や時間と相反して，公開されてしまう可能性がある．ユーザの不快が少しでも積み重なればユーザは自らの位置情報を公開するのを躊躇し，位置情報管理システムに参加することも拒むであろう．参加するユーザの数が少なければ，位置情報管理システムは意味をなさなくなり，位置情報管理システム全体の意義がなくなってしまう．

位置情報の集中管理されることへの弊害

位置情報を一つのサーバとデータベースで一括管理する方法は多くの研究で採用されている．しかしながら，常に自らの情報が一箇所に管理されてしまうことへの嫌悪感が発生する可能性がある．例えば会社で働いている人物がトイレや食事時間，休憩にいたるまで事細かにチェックされ，人事のデータとして利用されていたら当然不快に感じ，位置情報システムへの参加を躊躇するであろう．とくに見知らぬ管理者にデータベースで一括で管理されてしまうことを不安に思う人は多いのではないかと考えられる．

上記の問題点を解決するために，著者らは，プライバシを考慮する分散型位置管理機構 Tachyon を開発した．Tachyon は，まず第 1 の弊害を解決する手法として，ユーザの位置情報の伝播をユーザが望む範囲で制限する．ユーザに信頼して利用してもらうシステムであるためには，「望む相手に」「望む場所において」「望む時間帯だけ」公開可能であり公開した情報が信頼している人に使われていることを保証しなければならない．我々は XML でユーザのポリシを定義してポリシ同士をネゴシエーションさせることで解決した．例えば，ユーザ A のプライバシポリシとしてもつ信頼する相手のタグの中にユーザ B が存在しても，ユーザ B のプライバシポリシの XML にユーザ A を信頼する人物にいれていなければ，通信しない．このようにして，ユーザ望む位置情報の通知を実現した．

Tachyon は，第 2 の問題を解決するために P2P な完全分散システムを適応させることを考慮し，ユーザの位置情報は分散して管理される．既存の P2P 通信機構の多くが，スケーラビリティ，コンテンツ分散，コンテンツ検索の効率性などに重点を置いているが，通信の柔軟性と信頼性，システム管理の容易さが備わっていない． 位置情報を扱うシステムでは，ユーザが日常的な生活の場で頻繁に利用する場所が主であり，ノード数は，高々数十個程度で十分であるといえる．むしろ，ユーザの状況によって構築されるノードは頻繁に拡張させた可能性があるため，ユーザの認識できる範囲で容易に変更が行えることが必要である．例えば，会議を行うために急遽部屋を押さえた場合，一日だけその部屋に位置情報取得ノードを設置し，一日だけ分散位置情報管理システムに追加すればよいという分散位置情報管理システムの構築ができなければならない．これらの機構を備えたシステムは今まで存在していない．

2. Tachyon で保護されるプライバシの項目

Tachyon システムでは，ユーザ一人に対して，RF タグが一つと，Representation と呼ぶ分散オブジェクトを配置する．RF タグがリーダに読み取られた ID からユーザの場所を認識し，ユーザが存在している時間と場所を Representation が保持する．タグとユーザの関係は，図 1 の様に，各ユーザが固有のタグを持ち歩く．ノードは，RFID のリーダが接続され常にタグが検出範囲内に存在するかを

[*] 慶應義塾大学大学院 政策・メディア研究科
[†] 慶應義塾大学 環境情報学部
[‡] 早稲田大学大学院　理工学部コンピュータ・ネットワーク工学科
[*] Graduate School of Media and Governance, Keio University
[†] Faculty of Environmental Information, Keio University
[‡] Dept. of Information and Computer Science, Waseda University
[§] Tachyon(タキオンと発音) は情報処理振興協会平成 15 年度未踏ソフトウェア創造事業の中島 PM 成果の一つである．

認識している計算機である．この計算機上に分散オブジェクトである Reresentation が存在をさせる．

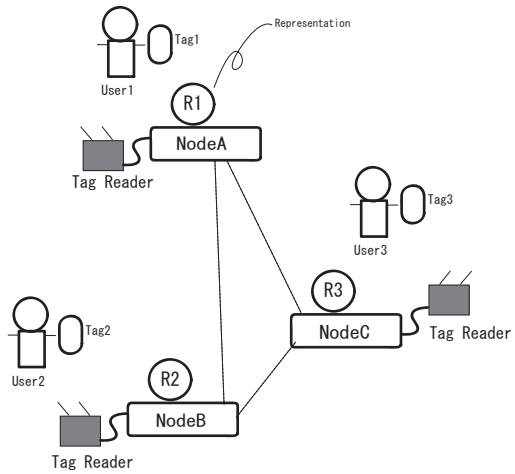

図 1 ノード，タグ，ユーザの関係

Representation は，それぞれのユーザのプライバシポリシも保持し他のユーザの Representation と交渉を行う．考慮するプライバシの項目には，位置情報を公開するユーザの視点を優先し以下ものを利用する．

- 位置情報を公開する相手/位置情報を伝達依頼を受け付ける相手
- 位置情報を公開する時間帯と曜日
- 位置情報を公開する場所
- 入退出後の情報更新の遅延

位置情報を公開する相手

位置情報を公開する相手とは，ユーザ A のポリシによって検索クエリーに反応する相手で INCOMMING COMPANIONS で規定する（図 2 参照）．INCOMMING COMPANIONS には自分へ位置情報の検索依頼を許可するユーザを記述する．INCOMMING COMPANIONS タグにないユーザからの検索依頼は受け付けず拒否する．OUTGOING COMPANIONS には自分から発生した位置情報クエリを閲覧できるユーザを示す．「あるユーザ A が検索を実行していること」が別のユーザ B から認識できたとする．ユーザ B からは，ユーザ A の具体的な位置情報は分からなくてもある程度ユーザ A が現在いる場所が推測できるため問題である．「ユーザ A が検索をかけていること」をユーザ B には認識させないようにするのが OUTGOING COMPANIONS の項目を設けた理由である．

位置情報を公開する時間帯と曜日

自分がいるということを他のユーザに「望む時間帯だけ」通知するために TIME SLOTS タグを用い曜日と時間を限定できる（図 3 参照）．これにより，休憩時間や非番曜日のプライバシを保護できる．

位置情報を公開する場所

PLACE タグは，「望む場所」とは各リーダがある部屋の文字列で記述する．この文字列は第 3 章で示すトポロジで一意であればどのような記述でも構わない．インターネットのスケールで運用する場合は，Frank らの Geocast 記述[1] 利用してもよい．

```
<INCOMMING_COMPANIONS>
  <INCLUDE>
    <COMPANION_GROUP>KMSF</COMPANION_GROUP>
    <COMPANION>userX@ht.sfc.keio.ac.jp</COMPANION>
    <COMPANION>userY@ht.sfc.keio.ac.jp</COMPANION>
  </INCLUDE>
  <EXCLUDE>
    <COMPANION>xxx@xxx.xxx</COMPANION>
  </EXCLUDE>
</INCOMMING_COMPANIONS>
<OUTGOING_COMPANIONS>
  <INCLUDE>
    <COMPANION_GROUP>ANY</COMPANION_GROUP>
    <COMPANION>ANY</COMPANION>
    </INCLUDE>
  <EXCLUDE>
  </EXCLUDE>
</OUTGOING_COMPANIONS>
```

図 2 INCOMMING COMPANIONS タグと OUTGOING COMPANIONS タグ

```
<TIME_SLOTS>
  <INCLUDE>
  <MONDAY>
    <TIME_SLOT beginning="11:30" end="12:30"/>
    <TIME_SLOT beginning="11:30" end="18:40"/>
  </MONDAY>
  </INCLUDE>
  <EXCLUDE>
    <TUESDAY>
      <TIME_SLOT beginning="12:30" end="14:40"/>
      <TIME_SLOT beginning="5:30" end="5:45"/>
    </TUESDAY>
  </EXCLUDE>
</TIME_SLOTS>
```

図 3 TIME SLOTS タグ

例えば Living Room，Kitchen Room，Bath Room，Entarance の 4 つのリーダがある場合がユーザが望むならば BathRoom のリーダに対しては自分の位置情報を報告しないということ可能である．図 4 に PLACE タグの記述を示す．

```
<PLACE>
  <include>ANY</include>
  <exclude>BathRoom</exclude>
</PLACE>
```

図 4 PLACE タグ

入退出後の情報更新の遅延

ユーザにとって必ずしも位置情報が正確であればよいということではない．位置情報をぼやかすことが必要である．Delay とは，ユーザの情報を曖昧にするパラメータである（図 5 参照）．ユーザは時に機敏に位置情報管理のシステムが反応してしまうことを嫌う場合がある．曖昧さを設定できることで，数分間席をはずしていることを逐次通知されることはない．APPEARANCE タグはユーザが現れてからその情報を他のノードに通知するまでの遅延秒数を表す．DISAPPEARANCE ユーザが立ち去ってからその情報を

他のノードに通知するまでのの遅延秒数を表す．

```
<DELAY>
  <APPEARANCE>600</APPEARANCE>
  <DISAPPEARANCE>600</DISAPPEARANCE>
</DELAY>
```

図 5　DELAY タグ

プライバシポリシ設定用の GUI

ユーザのプライバシポリシは，図 6 のような GUI でおこなう．他のユーザに閲覧されないため，この GUI を起動するためにはノードで認識したいるタグが唯一あったときだけ起動できる．

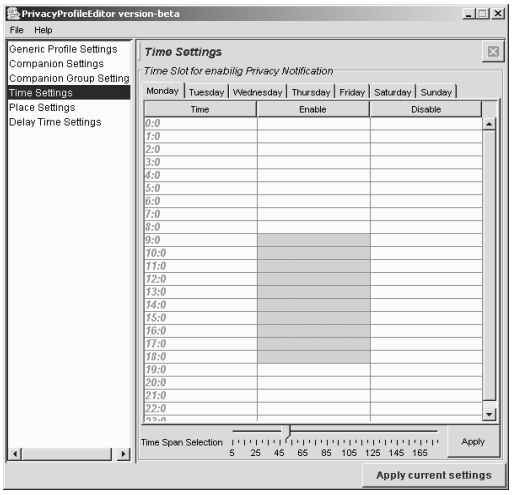

図 6　プライバシポリシ設定用の GUI

3. サーバレスシステム

ユーザの位置情報を一箇所のサーバでデータベースシステムを使って一括に管理している状況は監視されている懸念をユーザが払拭できない．

Tachyon では，サーバは設置せず分散するノード間でのオーバレイの P2P ネットワークトポロジを構成する．P2P ネットワークの基盤として Dragon[4),5)] を用いた．Dragon は，push，pull，callback，callbackpull などの様々な通信機構を実現しており，多様なトランザクション形態を必要とする分散位置管理システムに望ましい．まず Dragon によって構築されたノード間のオーバレイネットワークトポロジ上に，Representation をユーザごとに生成し放流する．サーバーレスのトポロジとなっているためどこから放流してもよい．各ノードは，ユーザの移動に伴いを検知するとトポロジ内部から Representation の発見と移送依頼を行う．Representation は，図 7 のように，この移送依頼に伴って自らの移送を行う．Representation はユーザの近傍のノードに配置される．

Tachyon は，サーバレスなトポロジのため，ノードが保持する Representation のリストを定期的に告知している実装である．図 8 のように，告知（Advatisement）を受け取りとプライバシネゴシエーションの様子を示す．

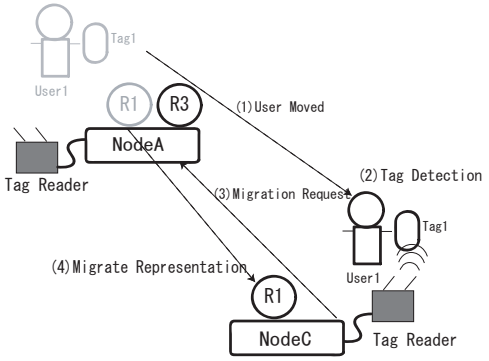

図 7　ユーザの移動に伴う Representation の移動

ユーザ 1 はユーザ 3 の存在を，告知（Advatisement）によって知ることができたとする．ただし，Advatisement には詳細なユーザの位置などの情報は含まれない．興味があるユーザ 1 は，ユーザ 3 の位置情報に興味があれば直接問い合わせを行い，前章のプライバシネゴシエーションをクリアすれば位置情報や詳細なデータを獲得できる．

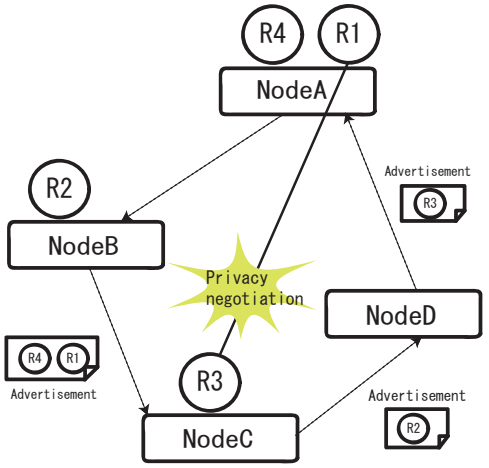

図 8　Representation の告知とプライバシネゴシエーション

4. Tachyon の運用

オーバレイネットワーク構築用のブラウザとして図 9 に示す uBlocks[6)] を用いた．ノードの増減が急遽あった場合でも簡単な操作でトポロジで変更できる．通常は円のようなグラフになるようにノード間を接続して利用する．より堅固なシステムにするためには完全グラフになるように接続する．

図 10 は慶応大学で開発したスマートファーニチャ[7)] に Tachyon の Node を設置している様子である．RF タグリーダには RFCODE 社のアクティブタグ spiderIII[11)] を利用し，小型 PC 上で Tachyon を動作させる．

5. 関 連 研 究

本章では関連研究と Tachyon の優位点を述べる．Marc Langheinrich らの行っている Privacy in Ubiquitous Systems[8)] のプロジェクトは，PrivacyDB という DB サーバを設置し，一度位置情報を登録すると，そのサーバの管理

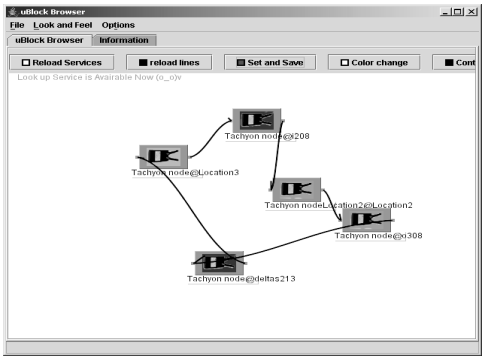

図 9 uBlocks ブラウザによるトポロジの構築の様子

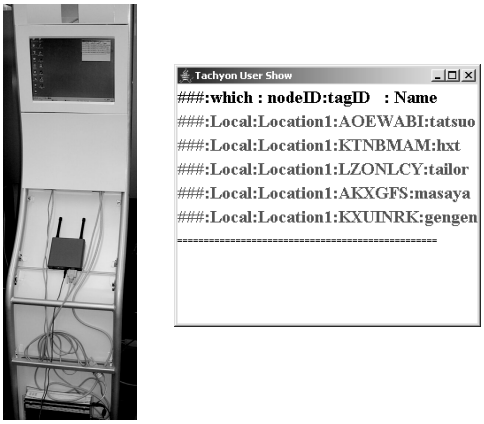

図 10 スマートファーニチャ内部に Tachyon の Node を設置している様子

者を全面的に信頼しなければならない C/S モデルである．Stephen A. Weis らの Cryptography and Information Security Group[12] では RFID の物理的なセキュリティとプライバシの保護機構が研究されているが分散システム全体として捉えた研究ではない．

Michael Beigl[10] らの仕事は近傍におけるサービスの共有のあり方を探るものであり，ユーザ間での位置情報を検索する機構は備えていない．

ピアツーピアを用いたシステムの代表例である Ion Stoica ら[2),3)] のシステムは，分散ハッシュテーブルを用いて peer が組まれるため小規模で信頼できるノード間での通信に限りたい場合には，不向きである．

Microsoft Windows Messenger[9] は，個人の情報を登録し，他のユーザに公開し，プライバシにかかわる情報の通知/非通知や ONLINE/OFFLINE の情報をユーザが自由に設定できる．しかし，ネットワークが同一なセグメントでの位置情報管理や，他のユビキタスアプリケーションとの連携を行うことはできない．またサーバの障害時には利用することはできない．

6. 終わりに

プライバシを考慮する分散型位置管理機構 Tachyon を開発した．Tachyon は，ユーザ自身によって自らの位置情報の望まない人や望まないアプリケーションへの伝達を防ぐプライバシを考慮した設定が行える．Tachyon によって位置情報システムを利用できる環境の提供が可能となる．また Tachyon は DB を持たず，完全に分散 P2P システムとして動作できるため，ノードの拡張に柔軟なシステム構築が行え　設営コストが低い点も利点である．今後は，スケーラビリティの評価を行い世界規模での運用に耐えうるシステムに発展させる．

参 考 文 献

1) Frank Durr. On a location model for fine-grained geocast. In *5th International Conference on Ubiquitous Computing, UbiComp2003*.
2) David Karger M. Frans Kaashoek Ion Stoica, Robert Morris and Hari Balakrishnan. Chord:A Scalable Peer-to-peer Lookup Service for Internet Applications. In *ACM SIGCOMM 2001*.
3) Shelley Zhaung ScottShenker IonStoica, DanielAdkins and Sonesh Surana. Internet Indirection Infrastructure. In *ACM SIGCOMM'02*.
4) Masayuki Iwai, Jin Nakazawa, and Hideyuki Tokuda. Dragon: Soft Real-Time Event Delivering Architecture for Networked Sensors and Appliances. In *The 7th International Conference on Real-Time Computing System and Applications*, pages 425–432, December 2000.
5) Masayuki Iwai, Jin Nakazawa, and Hideyuki Tokuda. Flexible Distributed Event-Driven Programming Framework for Networked Appliances and Sensors. In *The 3rd International Symposium on Distributed Objects and Applications Short Papers Proceedings*, pages 61–68, September 2001.
6) Masayuki Iwai, Jin Nakazawa, and Hideyuki Tokuda. uBlocks: Enabing Hand-made Distributed Application among Ubiquitous Embedded Devices. In *IEEE The First Workshop on Software Technologies for Future Embedded Systems*, May 2003.
7) M. Ito, A. Iwaya, M. Saito, K. Nakanishi, K. Matsumiya, J. Nakazawa, N. Nishio, K. Takashio, H. Tokuda. Smart furniture: Improvising ubiquitous hot-spot environment, May 2003. IEEE 3rd International Workshop on Smart Appliances and Wearable Computing.
8) Marc Langheinrich. Privacy awareness system for ubiquitous computing environments. In *4th International Conference on Ubiquitous Computing, UbiComp2002*.
9) Microsoft Corp. Microsoft windows messenger. http://messenger.msn.com/.
10) Philip Robinson and Michael Beigl, Trust Context Spaces. An infrastructure for pervasive security in context-aware environments. In *First International Conference on Security in Pervasive Computing*, 2003.
11) RF Code, Inc. Rfcode spider reader iii. http://www.rfcode.com.
12) S. A. Weis, S. Sarma, R. Rivest, D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *First International Conference on Security in Pervasive Computing*.