様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１６　日現在

機関番号：　１１４０１
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０３２４

研究課題名（和文）ロケーション情報で支援する医療現場に最適化したユーザ認証支援機能

研究課題名（英文）User Authentication Assist System Optimized for Medical Situations Supported by the Location Information

研究代表者

大佐賀　敦（Ohsaga, Atsushi）

秋田大学・医学（系）研究科（研究院）・助教

研究者番号：００３９６４３３

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：本研究課題では、病院という建物自体が認証の基盤となり、正当な利用者本人がその場にいるという事実により情報システムの利用者認証が完了する機能を実現すべく、院内無線LANインフラを利用し、無線LANアクセスポイント(AP)への接続情報で認証に必要十分な位置情報が得られることを確認した。また、上下階や隣の建物のAPへ接続による誤検出への解決策として、実際の人の移動ではあり得ない移動をノイズとして除去することで位置推定精度の向上を試み、利用者の位置情報を実用的な精度で捉える機能を構築し、同機能の有効性について実証できた。

研究成果の概要（英文）：In this research project, to realize the user authentication of the information system by the fact that a rightful user is in the right place using the hospital building itself as the basis for authentication, we confirmed that the connection information to the Wireless LAN access point (AP) provides sufficient location information for authentication. In addition, as a solution to false positives by connecting to the AP of the upper or lower floor or of the next buildings, we tried to improve the position estimation accuracy by removing the movement which was not possible by the movement of the actual person as noise, and constructed the function to capture user's location information with practical accuracy, and demonstrated the effectiveness of the function.

研究分野：　医療情報学

キーワード：　ロケーション情報　RFID　ユビキタス技術　セキュリティ　認証　無線LAN

１．研究開始当初の背景

いわゆる「電子カルテ」に代表される病院情報システムでは、利用者認証機能が患者個人情報を守る最終的な砦となっている。しかし、広く普及しているID・パスワードには、「容易に他者に利用され得る」という短所が存在し、長期間にわたり安全性を確保する手段としてはすでに限界となっている。そのため、ＩＣカード等の物理認証や、指紋・静脈・顔等の生体認証といった、より強力な認証手段を組み合わせる「２要素認証」の導入進められているが、実際の医療現場では、物理認証や生体認証が最適な認証手段となっていないのが現状である。

頻繁に端末を離れて診察・処置を行う医療者にとって、移動の都度、ＩＣカードを抜き差しするのは極めて煩雑であるほか、生体認証でも、酒精綿を頻用するスタッフ等での指紋読み取り精度の低下や、マスクや帽子を着用した状況での顔認識率の低下といった限界が存在する。そのため、診療場面では、セキュリティ強化対策が原因で緊急時の診察に支障が出た事例も生じており、情報システムを活用し、安全な医療を提供するためには、この課題の解決が急務である。

その解決策として着目されるのが、利用者に極力負担を強いない自動認証技術の応用である。「医療者という正当な利用者が院内という適切な場所で利用している」ことを、「本人が現にそこに居るという事実で確認する」システムの実現より、利用者の負担を軽減し、かつ確実なセキュリティ基盤が現実のものとなる。

この自動認識の応用例として、数十ｃｍ程度の距離から離れて読み取りできる職員証を身につけ、端末に近づくだけで利用者認証を行うものがあり、企業など一定の条件下では実用化されている。しかし、この仕組みをそのまま医療場面で利用する場合、数多くの端末とスタッフが密集する診療現場で利用者と端末を１：１で自動認証することは事実上不可能であり、根本的な方式の見直しと医療機関での利用に向けたシステム最適化が不可欠である。

このような現状において、患者・社会が電子化された診療情報を安心して医療機関に託すことができ、かつ、医療者が電子化された診療情報を十分に活用するためには、「正当な利用者は必要な診療情報に速やかにアクセスでき、かつ、不適切な状況では利用が制限される」という動作を、利用者に過度な操作負担を強いることなく完了できる認証システムが不可欠であり、患者急変時の診療記録参照など、日々の診療を行っている医療現場からも、その実現が切望されている。

２．研究の目的

本研究では、病院という建物自体が認証基盤の一部となり、「正当な利用者本人がその場所に居るという事実」により認証される、ユビキタス化した利用者認証機能の実現を最終的な目的とする。

その一環として、本研究課題ではロケーション管理システムが持つ位置情報と情報システムの利用者認証を動的に連携させることにより、（１）必要な時のみ利用者の位置情報を検索し、認証に必要十分なデータを提供する位置情報処理基盤の構築、および、（２）前述の位置情報処理基盤と連携し、利用者のアクセス場所と本人の所在情報を照合することで、利用者認証を強化する認証基盤の実現、の２点の実証を目的とする。

３．研究の方法

上記の目的の達成のため、以下の３つについて、開発・検証を行った。

(1) 病院を想定した単一階の模擬環境を想定し、利用者の位置検出基盤について検証した。位置検出の方式として、①Wi-Fi アクティブタグの検出に特化したロケーションレシーバによるエリア検出、②病院内に広く整備されている無線LANインフラを利用した位置検出、の２つのモデルにより検討した。

(2) 無線LANアクセスポイントを用いた位置検出基盤を、実際の医療機関での利用に即して複数階への拡張を行い、上下階や別の建物など、本来の人の移動と一致しない無線 LAN アクセスポイントへのローミングを判断するアルゴリズムの実装と検証を行った。

(3)無線 LAN インフラを用いた位置検出基盤を利用して、位置情報に基づく認証機能の構築を行い、病院環境での動作を検証した。患者情報を有するノート PC を想定し、セキュリティレベルの低い場所へ同 PC を持ち出した際に自動的に認証が解除され、暗号化したデータを自動的に復号・使用不能とする仕組みを構築し、検証した。

４．研究成果

(1) 無線LANインフラを用いた場合の位置情報の粒度の検証

無線LANインフラは、チャネル干渉を防ぐため、安定利用が可能な限りできるだけ粗に配置することが大原則となっている。そのため、位置検出デバイスをできるだけ密に設置して精度を上げるエリア検出とは全く逆の設置方針となることから、無線LANインフラを位置検出に用いる場合、自ずと位置精度に限界が存在する。そこで、研究代表者らの施設を例に、通信に最適化された無線LANアクセスポイント(AP)から得られる位置情報を、実際の機器配置により検証した。図１は、病棟における AP の配置と電波強度の例を示したものである。

① 入院病棟では、職員が常駐するスタッフステーションが最も大きな単一空間のため、独立したAPの設置が可能であること

が確認できた。これによりスタッフステーションと病室等の他の場所とを識別することが可能であった。

② 外来診察室では、業務スペースとしての大きな単一空間は無いが、診療科毎に固まって存在するため、概ね、診療科単位での位置の推定が可能であった。

③ 中央診療部門・事務スペースでは、部門の特性により部屋の構成が大きく異なっていた。しかし、業務を行う場所はそれぞれ固定されているため、診察室同様、AP のカバーエリアを元に、当該部署での所在を確認可能であった。

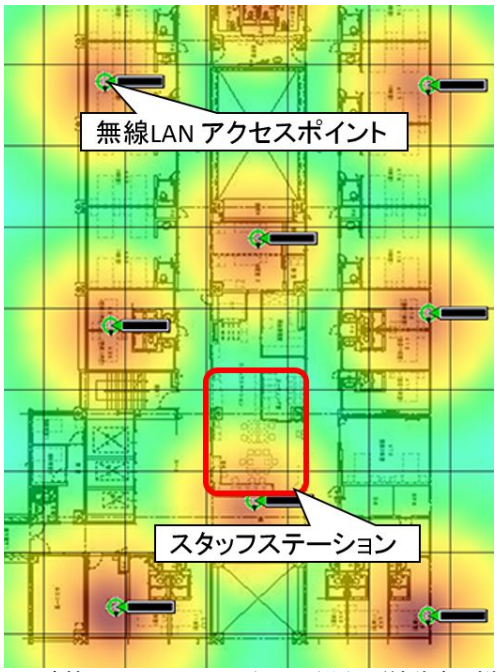

図 1 病棟におけるアクセスポイント配置と電波強度の例

このように、位置検出基盤として既存の無線 LAN インフラを使用する場合は、基本的に部署の粒度とし、入院病棟では、スタッフステーションと各病室群へと粒度を上げることで、利用者が特定部署で業務を行っていることの確認に利用でき、第三者による不正アクセスの検出に有用なパラメータが得られることが示唆された。

(2) 複数階における位置検出精度の向上

院内無線 LAN の AP への接続情報から当該機器の所持者の位置を推定する場合、上下階や別の建物等の AP への接続が位置誤検出の原因となる。そこで、上記の位置検出基盤を複数階へ拡張した際であっても、このような誤検出を防ぐためのアルゴリズムの開発と検証を行った。具体的には、集中コントローラ型無線 LAN アクセスポイントの接続・切断情報が SNMP プロトコルにより位置情報基盤に送信・集約され、接続 AP の粒度での位置検出を行い、結果を図示するアプリケーションを開発した。(図 2)。これにより、各機器の AP 間のローミングの様相の時系列を視覚的に把握でき、上下階等、人の移動と乖離する場面の実態の把握が可能となった。

図 2 無線 LAN アクセスポイントへの接続情報を用いた位置検出アプリケーション

この結果を元に、位置検出基盤に「人の移動としての認識が適切なローミング先」の情報を設定し、一連の接続・切断情報を時系列で判断するアルゴリズムを実装した。図 3(A)は、階段があり、実際の移動に伴い起こり得るローミングの例であり機器の位置が正しく更新されている。一方、図 3(B)は、当該箇所に階段・エレベータ等がない場所で上階のアクセスポイントへローミングした例である。これは、実際の人の移動が不可能なものであるため、検出機器の情報に×が表示され、ノイズとして処理されている。

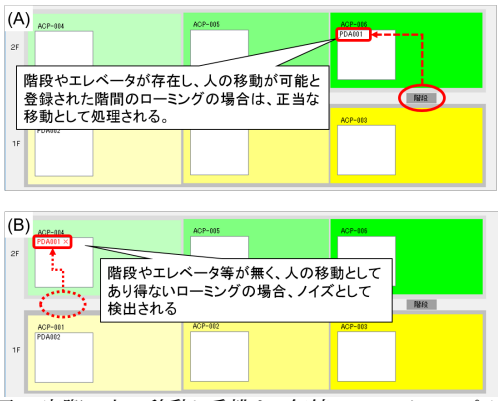

図 3 実際の人の移動と乖離する無線 LAN アクセスポイントローミングを位置情報のノイズとして処理した例

このように、上記のアルゴリズムにより、無線 LAN AP への接続情報をもとに、エレベータや階段等、実際にあり得る移動に伴うフロア間のローミングは移動として正しく認識し、それ以外の上下階・隣の建物へのローミングをノイズとして除去することが可能となった。

(3) 位置情報に基づく認証機能の病院環境におけるユースケースでの動作検証

前述の位置検出機能の応用事例として、業務用 PC をセキュリティレベルの低い場所へ持ち出した際に自動的に認証が解除され、暗

号化したデータを自動的に復号・使用不能とする仕組みを構築し、検証した。

当該 PC 内のアプリケーションおよびデータファイルを使用不能にする方法としては、①対象ファイルを直接破壊する方法、②対象ファイルをあらかじめ暗号化し、復号不可能にする方法、の２つが考えられた。前者はデータ抹消ソフトウェアと同様の仕組みにより確実にファイルを破壊することが可能であるが、ファイルサイズが大きくなると処理に時間を要するという課題が存在する。

そこで、ファイルサイズに関係なくデータを素早く使用不能にする方法として、対象となるファイルをあらかじめ電子証明書で暗号化しておき、復号のための証明書を破壊することで、実質的に使用不能にする方式での実装を行った。具体的には、今回、検証対象とする OS を Microsoft Windows 7 および 10 とし、同 OS が標準で有する EFS (Encrypting File System)機能を利用し、PC の証明書ストア中の当該電子証明書を破壊し、EFS により保護されたファイルの読み取りを不可能にする方式とした。

この証明書破壊のトリガーとして、本研究課題で開発・検証した位置情報基盤を利用し、一連の制御を行う常駐アプリケーションを開発した。図 4 は同アプリケーション画面である。このツールは対象の PC に常駐し、院内無線ＬＡＮに接続できる時は、無線ＬＡＮシステムの集中コントローラから得られるアクセスポイントの接続情報を時系列処理することで現在位置を把握し、管理対象外になった時には、証明書ストア中の利用者証明書の破棄を行うものである。

また、同アプルケーションは、災害時等、院内無線ＬＡＮインフラが使用できない時の手段として、位置識別専用の独立した Wi-Fi アクセスポイントへの接続による、ピンポイントの位置情報による制御も可能とした。

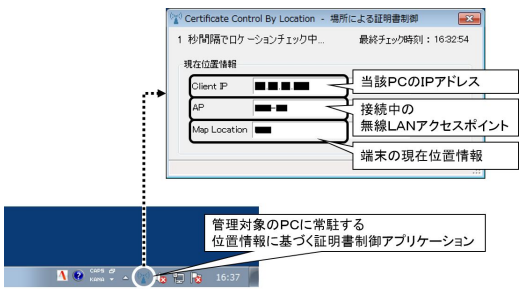

図 4 管理対象の PC に常駐し実行される位置情報による証明書制御アプリケーションの画面

このアプリケーションを用いて、研究代表者らの院内無線 LAN 環境を用い、端末移動場面での検証・評価を行った。院内無線 LAN システムへの接続情報を元に端末自身の位置を判断し、設定した利用場所外へ持ち出された際、常駐アプリケーションにより証明書が破棄され EFS により暗号化したファイルへのアクセスを不能とできた。

しかし、動作の詳細を検証したところ、利用者ログイン中に証明書が破棄された場合、当該セッション中はアクセスが可能なままで、一度ログアウトすることでアクセス不能となった。そこで、利用可能な範囲外へ移動したことを検出したタイミングで強制ログアウトする機能を追加した。これにより、ログイン状態のまま PC を持ち出した場合でも、持ち出しが検出されたタイミングで自動的にログアウトされ、ファイルへのアクセスを不能にでき、一連の機能を実証できた。

(4) 本研究課題で開発・検証したシステムの応用可能性および意義

これまで、屋内において、無線技術により位置を直接検出する方式としては、複数の無線 LAN アクセスポイントを用いて信号強度の測位を行う RSSI (Received Signal Strength Indication)方式と、主に専用の受信機を複数用いて、電波の到達時間差を利用する TDOA (Time Difference Of Arrival)方式があり、いずれも物流倉庫のような広い単一空間では有効な位置検出が可能であった。しかし、実際の医療機関は壁やパーティションで仕切られた細かな空間が密集した構造となっているため、これらの方式では個々の診察室や端末位置を必要十分な精度で検出する事は極めて困難で、実用化の大きな障壁となっていた。

この課題に対しては、BLE(Bluetooth Low Energy)ビーコンによるエリア検出や、Bluetooth の電波による三角側位を行う仕組みが開発されており、Bluetooth の電波が微弱であることと相まって、ビーコンを密に配置することで位置精度の改善が実現している。また、IMES (Indoor MEssaging System)等、位置を精密に推定する技術は日々進歩しており、今後、高精度な位置情報が容易に得られることは想像に難くない。しかし、以上述べたいずれの方法も、それ専用の設備投資が必要であるため、医療機関が容易に導入するには、大きなコスト的障壁が存在する。

加えて、位置情報は本質的に極めて機微な情報であり、慎重な取り扱いが求められるべきものである。本研究課題のユースケースで取り上げた医療者の位置情報は、業務中の情報とはいえ、本当にそこまでの位置情報を常時把握する必要があるかという点については、個人としての尊厳としてのプライバシー確保の点からも、常に慎重な配慮が必要と考えられる。

このような懸念点も存在する一方で、位置情報の活用は IoT 機器の普及とともに急速に進むと考えられる。これに対し本研究課題では、従来の「高精度かつ連続的な位置把握」という発想を逆転させ、「所在が確認できる程度の荒い位置情報」を「認証に必要なときのみ位置情報を利用する」というアプローチにより、その解決を試みた。

敢えて荒い位置情報しか取得できないシ

ステムとし、必要な場面のみ位置情報を利用することで、「情報システムに常に現在位置を把握されている」というプライバシー侵害への抵抗感も軽減可能であるといえる。また、位置情報の精度を割り切ることで、高価な位置検出専用の機器の導入も不要となり、一般的な無線ＬＡＮインフラが活用可能となり、最小の設備投資での導入が可能となる。

厚生労働省「医療情報システムの安全管理に関するガイドライン」第５版では、その公開から約 10 年後を目処に、医療情報システムにおける利用者認証において 2 要素認証を必須にするとしている。各医療機関においてもその対応が求められるものであるが、本報告書の冒頭「研究開始当初の背景」で述べた通り、医療機関においては、2 つめの要素としての IC カード認証や生体認証は最適なものとは言い難い。この課題に対しても、本研究課題で検証した位置情報を用いて、「利用者本人の所在」を 2 つ目の要素とすることでの解決が可能である。

これら今回実現した機構で最も重要な点は、一般の利用者はこの基盤を特段意識する必要もなく、また特殊な操作も必要としない点である。本研究課題で開発・検証した情報基盤の医療場面への応用により、医療従事者がユビキタス環境の恩恵を最大限に享受可能となり、高度に情報化が進んだ医療現場において医療の本質により専念し、質の高い医療を提供することが可能になることが期待される。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　１　件）

① 大佐賀 敦、 近藤 克幸、Wi-Fi アクティブタグによるリアルタイム位置情報を利用した端末認証・制御機能　―無線スレート端末と病院情報システム端末間ファイル交換システムへの応用―、医療情報学、査読有、Vol.34(Suppl.)、2014 年、694-697

〔学会発表〕（計　２　件）

① 大佐賀 敦、 近藤 克幸、リアルタイム位置情報を用いたファイル保護機能のオフライン患者ＩＤ検索ツールへの応用、平成 28 年度大学病院情報マネジメント部門連絡会議、2017 年 1 月 26 日、琵琶湖ホテル（滋賀県・大津市）

② 大佐賀 敦、 近藤 克幸、Wi-Fi アクティブタグによるリアルタイム位置情報を利用した端末認証・制御機能　―無線スレート端末と病院情報システム端末間ファイル交換システムへの応用―、第 34 回医療情報学連合大会（第 15 回 日本医療情報学会学術大会）、2014 年 11 月 8 日、幕張メッセ国際会議場（千葉県・千葉市）

〔図書〕（計　０　件）

〔産業財産権〕
○出願状況（計　０　件）
○取得状況（計　０　件）

〔その他〕
ホームページ等

６．研究組織

(1)研究代表者
大佐賀　敦（OHSAGA, Atsushi）
秋田大学・医学（系）研究科（研究院）・助教
研究者番号：００３９６４３３

(2)研究分担者
近藤　克幸（KONDOH, Katsuyuki）
秋田大学・その他部局等・理事
研究者番号：３０２８２１８０