科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１７　日現在

機関番号：　１１４０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５９０５８３

研究課題名（和文）ロケーション管理技術と仮想化で実現するセキュアでユビキタスな院内情報システム基盤

研究課題名（英文）Secure and Ubiquitous Hospital Information System Infrastructure by Real-time Location System and Virtualization Technology

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）　　4,200,000円、（間接経費）　　1,260,000円

研究成果の概要（和文）：本研究課題では、PCの位置をリアルタイムに把握する手段として、ロケーションサーバとアクティブ型電子タグを採用し、その応用可能性を検討した。位置情報を利用し、１）診察室や研究室、院外等へモバイルPCを持ち運んだ際、各場所に応じたファイル・セキュリティを自動適用し、利用者が意識することなくデータ保全を行う仕組み、２）PCを診察室等へ持ち込んだ際には、持ち込んだPCと診察室の端末が自動的に互いを認証し、シームレスなデータ交換が可能となる機能を開発した。これらのシステムを医療場面での利用に合わせた最適化を行い、実用的な性能が得られることを評価した。

研究成果の概要（英文）：In this project, location server system and active type RFID tags were utilized to get the real-time position of mobile PC's. Using location information, 1) we developed the system which automatically applies the appropriate file access security policy according to each place when mobile PC is carried to the place with a different security policy such as, an examining room, a laboratory, or outside a hospital. 2) The function was also developed that the PC in an examining room and the mobile PC which was carried in the room authenticate each other by using the location information to enable seamless data exchange between them. And we also evaluated the optimal use in the medical scene of these systems.

研究分野：　医歯薬学

科研費の分科・細目：　境界医学・医療社会学

キーワード：　ロケーション管理　RFID　アクティブタグ　認証基盤　セキュリティ　ユビキタス技術

１．研究開始当初の背景

いわゆる診療記録の電子化により、診察室や病棟・研究室といった院内の複数箇所から、同一患者の診療記録の同時参照が可能となった。このメリットを最大限に享受するには、医療者がいつでもどこからでも必要な情報に素早くアクセスできる情報基盤が不可欠である。しかし、実際の医療機関において、全職員に自分専用のモバイルＰＣを病院情報システム端末として支給することは、費用の制約もあり、事実上不可能である。

他方、多くの医師は自分用のＰＣを所有し、資料整理・学術研究等に積極的に活用しているが、セキュリティ上の理由から病院情報システムとは異なるネットワークに接続されているのが一般的である。そのため、利用者は状況に応じて病院情報システムと各自のＰＣを意識的に使い分けることを強いられている。

この解決策として注目されているのが、ＯＳやアプリケーションソフトを物理的なコンピュータから切り離して利用する「仮想化技術」である。病院情報システムに応用し、医師が所有するＰＣと病院情報システムとを論理的に分離かつ連携することで、医師所有のＰＣで病院情報システム上の患者情報を安全に取り扱うことも可能となる。

これは極めて利便性が高いものであるが、利用者の勘違い等による情報漏洩のリスクが増大する危険性を内包している。このような危険性に対する従来の情報セキュリティ対策は、認証技術によるデータのアクセス制限と暗号化による保護が基本である。いずれも有用な対策ではあるが、利用者の利便性を損なうことに加え、不適切な利用や人的な操作ミスにより情報漏えいのリスクが逆に拡大するという脆弱性が存在する。

このような現状への解決策として、「適切な利用場面では必要な情報に容易にアクセスでき、不適切な場面ではアクセスが制限されデータも無効化される」という一連の動作を、利用者に意識させることなく制御するシステムの実現が期待されている。

２．研究の目的

本研究課題では、十分なセキュリティを担保しながら、院内のどこからでも必要な時に必要な情報にアクセスできる環境－すなわち病院情報システムの院内ユビキタス化の実現を最終的な目標とする。

この実現のため、無線ＬＡＮとアクティブ型電子タグによるロケーション管理技術と情報システムへのアクセス制御・データ保護技術を連携させることにより、①不適切な場所へＰＣを持ち出した際はアクセス制限と診療データの保全を自動で行う機構、②医師が通常持ち運ぶモバイルＰＣであっても、適切な場所からは安全に診療情報にアクセスできる情報基盤、の実現および医療場面に即した実証を目的とする。

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、開発および検証を行った。

(1) 全体の基盤として、ロケーションサーバに存在する各ＰＣ（デバイス）の位置情報をリアルタイムに抽出し、その情報をもとにＰＣのセキュリティ・ポリシーおよびアクセス権限を設定する実装方式を検証した。制御を施すポイントに着目し、セキュリティ面および実環境で運用した場合のレスポンス等の性能面から、最適な方式を検討した。

(2) 位置情報に基づくデータ保護機構として、ロケーションサーバの位置情報により、モバイルＰＣ内のファイルのアクセス権をリアルタイムに制御する機構を開発した。診察室から研究室へＰＣを持ち運ぶ場面を想定し、モバイルＰＣを診察室から持ち出した際に、診療データを含むファイルを自動でアクセス不可とし、研究室への到着により再度アクセス可能になる機能について開発し、実証した。

また、この機能を応用し、院外持出し禁止のデータを持ち出そうとした際に、ファイルの削除や復号不可能な状態にする等の情報保護技術への応用可能性を検討した。

(3) 位置情報に基づき各種アクセス権が自動設定される情報基盤として、医師が利用しているモバイルＰＣを病院情報システム端末のすぐ側に置くことで、モバイルＰＣと病院情報システム端末間で互いを自動的に認証する機能について開発し、実証した。この機能を応用し、自動認証されたＰＣ間で安全かつ利便性の高いデータ交換の機能を検証した。

４．研究成果

(1) ロケーション情報によるＰＣのセキュリティ・ポリシーおよびアクセス権限設定の実装方式の検証

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ているため、物流倉庫のような広い単一空間で有用なTDOA（電波到来時間差）方式やRSSI（受信電波強度）方式による位置検出では十分な精度が得られない。そのため、各ＰＣにWi-Fiアクティブタグを取り付け、位置検出したい箇所に励起装置（エキサイタ）を設置することで、数十㎝～数ｍのエリア検出を行うことを基本とした。図１にロケーションサーバによる位置検出の例を示す。

この位置情報を利用したアクセス制御の方式について、制御を施すポイントに着目し、①IEEE 802.1X 認証を用いた検疫ネットワーク機能によるネットワーク接続そのものの制御、②認証ゲートウェイでの認証により、セキュリティを担保したいサーバ等への通

信を許可/拒否してアクセス制御する方式、③アクセス先サーバでのアクセス権による制御、の３つを比較・検討した。

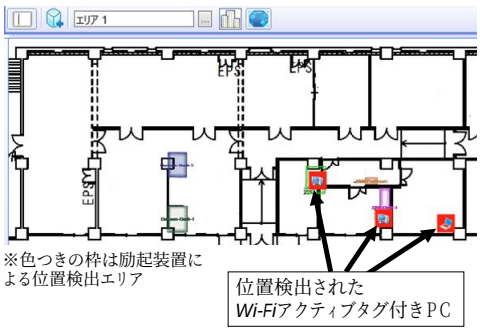

図1　ロケーションサーバによる位置検出結果

結果、非認証状態から認証状態への制御は、いずれの方式においても通常の権限付与と認証により容易に実現可能であるが、位置情報の変化に伴い認証解除する場合は、各方式による差異が明らかとなった。

③アクセス先サーバでの制御では、サーバ側の更新処理で即反映が可能であるが、①検疫ネットワーク、②認証ゲートウェイによる制御では、１回の認証の有効期間を短くし、再認証時に認証不可とする対応が必要な場合がある。しかし、１回の認証の有効期間を短くして頻繁に再認証する場合、認証処理の負荷がオーバヘッドとなるほか、連続した通信の安定性の阻害要因にもなり得る。

これを防ぐためには、クライアントＰＣから認証状態を随時照会して更新する等、サーバとクライアントが互いに呼応して動作する仕組みが不可欠であることが明らかとなった。そこで、クライアントＰＣと連携するサーバプログラムとして、①一定時間毎に各ＰＣの最新の位置情報を位置検出エンジンから抽出し管理するプログラム、②クライアント上のプログラムと連携し、各クライアントが必要とする制御情報を提供するプログラムの２つを開発した。

図２は今回開発した位置情報の抽出・管理プログラムの動作画面である。

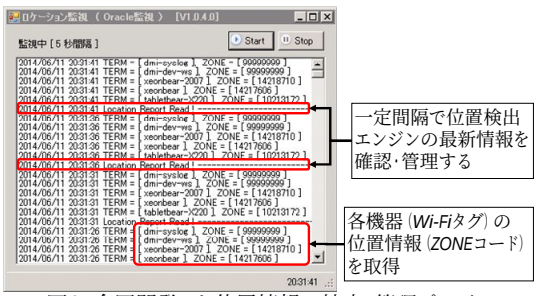

図2　今回開発した位置情報の抽出・管理プログラム

このプログラムは管理対象のＰＣとそれに紐付けられたWi-Fi アクティブタグの組み合わせをサーバ上のデータベースで管理している。加えて、各 Wi-Fi アクティブタグの位置情報を位置検出エンジンのデータベースから一定間隔で抽出し、一連の処理で必要なデータを提供するものである。

そして、図３は上記の位置情報を利用して、位置の変化や、同一エリアに存在する他のＰＣの情報、当該位置で適用すべきセキュリティ・ポリシー等を提供するサーバ側のプログラムである。各クライアントＰＣはサーバ上の本プログラムと常時通信し、連携して動作することで必要な制御を行う。

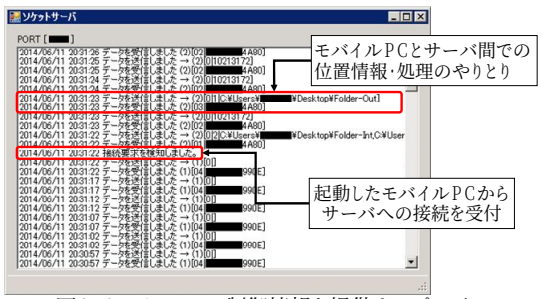

図3　クライアントに制御情報を提供するプログラム

(2) 位置情報に基づくデータ保護機構

上記の基盤を利用して、ロケーションサーバの位置情報により、モバイルＰＣ内のファイルのアクセス権をリアルタイムに制御するクライアント側のプログラムを開発した。図４は同プログラムの動作画面である。

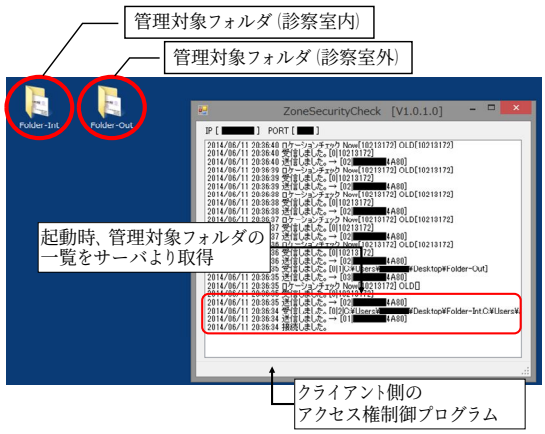

図4　位置情報によりファイル・アクセス権限を制御するクライアント側プログラムの動作例

ロケーションサーバには、管理するＰＣおよび各位置でアクセスを許可/拒否するフォルダのリストがあらかじめ登録されている。各ＰＣのクライアントプログラムは、起動時に、これらのフォルダ一覧をサーバから取得し、管理する。起動時の初期動作としてすべてのフォルダをアクセス不可とし、以降はロケーションサーバと常時通信し、同サーバからの指示に沿って動作する。

サーバでは当該ＰＣの位置を常に確認しており、位置の変化が検出された場合、新しい位置でアクセス許可されるフォルダをクライアントに通知する。クライアントは、新たにアクセス許可されるフォルダ、および、

移動に伴いアクセス不可となるフォルダについて、バックグラウンド処理でアクセス権を自動変更する（図５）。

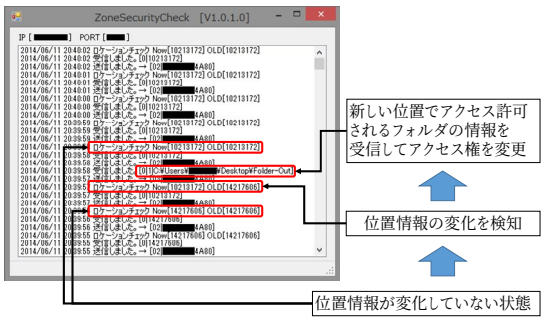

図5 位置情報の変化に伴う
ファイル･アクセス権制御の動作例

ここで、実際に診察室を模した環境で検証を行ったところ、２つの課題が明らかとなった。１つは「一時的にロケーションサーバと通信できない場合の考慮が必要となる」ことであり、もう１つは「ロケーションの境界にＰＣがある場合、頻繁にセキュリティの設定変更が発生し、安定した利用ができない」、というものであった。

前者は、検出不能の状態をひとつの「位置」として扱うことで容易に解決された（図２のZONE = [99999999]）。後者については、同一位置で複数回連続して検出された場合のみを位置の変化とする処理をサーバ側に追加することで、安定した動作が得られた。

この仕組みを、「モバイルＰＣを院内各所に持ち運んで使用する」場面に適用した際、利用者がストレスを感じない実用的な応答性が求められる。前述の位置情報の抽出・管理プログラム（図２）の更新間隔が長いと、システム上の位置情報と実際の機器の移動とに時差が生じる。その結果、利用者が位置変化の反映を待つこととなり、操作性が大きく損なわれる。そのため、更新間隔を短くする必要があるが、管理対象のＰＣ数が増えた場合、更新処理時間＞更新間隔となり、処理が追いつかなくなると、正常に機能しなくなることが危惧された。

そこで、本研究課題のユースケースである、「モバイルＰＣを持ち運んだ先で使用する」という点に着目し、位置変化のシステム反映の最適値を検証した。結果、今回のようなユースケースでは１秒以下という瞬時の応答性は不要であり、5 秒程度の時間を要しても、利便性に影響がないことが確認された。

これを踏まえ、かつ、本システムは位置情報の抽出・管理プログラムとクライアントとのやりとりを行うプログラムを独立させている特長を活かし、サーバ側の位置情報は 5 秒間隔と比較的長期間で更新し、クライアント側を１秒間隔という短期間で処理する最適化を行った。これにより、システムのボトルネックとなる位置情報更新処理の負荷を押さえ、かつ、デバイス数が増えても実用的に動作させることが可能となった。

(3) 位置情報に基づき各種アクセス権が自動設定される情報基盤

これまで述べた、位置検出基盤およびサーバとクライアントが連携して動作するプログラムを元に、隣接する端末が互いを自動的に認証し、安全かつ利便性の高いデータ交換を行う機能について開発し、実証した。

図６は、モバイルＰＣを診察室のデスクトップＰＣ付近に持ち込んだ場合の例である。

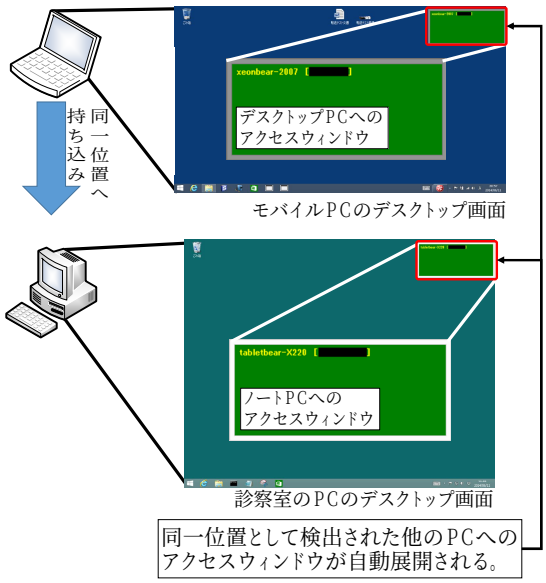

図6 複数の PC が同一位置に検出されたときの例

各ＰＣのクライアントプログラムはロケーションサーバ上の制御プログラムと連携し、自らの位置情報に加えて、自分と同一位置にある他のＰＣの情報を取得している。他のＰＣが存在する場合、それらのＰＣへアクセスするためのウィンドウ（アクセスウィンドウ）がお互いのデスクトップ画面に表示される。他のＰＣへの操作はこのアクセスウィンドウを経由して行う。本研究課題では、連携の基本的な機能として、アクセスウィドウを経由した画像やデータ等のファイル送受信を実装し、検証を行った。

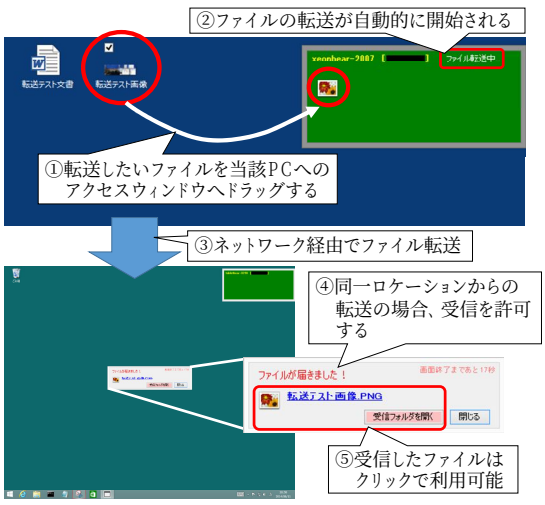

図7 アクセスウィンドウを利用したファイル転送の例

具体的な動作の流れを図7に示す。複数のＰＣの位置が同一と検出されると、各ＰＣに相手のＰＣへのアクセスウィンドウが表示される（３台が同一位置にある場合は、各ＰＣに他の２つのＰＣ用のアクセスウィンドウがそれぞれ表示される）。この状態で、送信元のＰＣで、①転送したいファイルをアクセスウィンドウにドラッグ＆ドロップすることで、②自動的にファイル転送が開始される。このファイル転送は、サーバを介さず、送信元・受信先間のソケット通信で直接行われる。受信先のＰＣでは、③ネットワークによるファイル送信の要求を受け、④ロケーションサーバから同一位置にあるとされたＰＣからの場合のみ、受信を許可し処理を継続する。⑤受信が完了すると、画面にメッセージが表示され、ファイル参照やファイルの使用が可能となる。

この機能を、診察室を想定した模擬環境で実証し、操作性を検証した。利用者がモバイルＰＣを持ち込んだ時にスムーズに同一位置と認識され、かつ、隣室のＰＣを同一位置と誤認識しない範囲として、励起装置の範囲を半径 50㎝ に最適化した。位置情報の更新間隔は、ファイルのアクセス件制御の場合と同様、サーバ側 5 秒間隔、クライアント側１秒間隔で、実用的な使用が可能となることが確認された。

(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

今回開発・実証した位置情報処理基盤と、同情報に基づくデータ保護機構およびアクセス制御基盤について、特に医療機関におけるユースケースとして、以下に挙げるような応用が期待される。

データ保護機能の応用例としては、大規模災害時に、病院の建物外に仮設した診療エリアで、病院情報システムや災害用診療バックアップシステムにより患者情報を扱う場面での活用が考えられる。今回のシステムを利用することで、患者情報が保存されたＰＣが手違いや万が一の盗難等で院外へと持ち出された際も、自動的にアクセス不可にすることが可能となり、診療情報のより安全な利用に資するものであるといえる。

また、アクセス制御基盤の応用例としては、リモートデスクトップ機能により、持ち運んだモバイル端末を診察室の病院情報システム端末の拡張画面として使用する、等が考えられる。今回のシステムは一般的なソケット通信の制御が基本原理であるため、他のサービスへの応用も容易に可能である。

また、全く別のユースケースとして、医療スタッフの所在確認に応用し、病院情報システムの利用者認証と連携させることにより、従来のＩＣカードや生体認証による本人認証の厳格化とは全く異なるアプローチによる不正アクセスの検出・防止システムへ発展させることも可能と考えられる。

これらのすべてに共通する点は、いずれも「一般利用者がそ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」ことである。すなわち、本研究で開発・検証された基盤を発展させ活用することにより、「利用者にとっての利便性の確保」と「情報システムとしての安全性の確立」という一般に相反する要件が同時に実現され、高度な情報化が進んだ医療現場において、医療従事者が医療の本質により専念し、質の高い医療を提供することを可能にするものであるといえる。

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　０　件）

〔学会発表〕（計　０　件）

〔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・大学院医学系研究科・助教
研究者番号：００３９６４３３

(2)研究分担者
近藤　克幸（KONDOH, Katsuyuki）
秋田大学・大学院医学系研究科・教授
研究者番号：３０２８２１８０