日本遠隔医療学会雑誌（2008.10）４巻２号:273～274.

携帯電話による安全性の高い利用者認証が可能な遠隔医療用通信インフラシステムの開発と評価

三上大季，林弘樹，守屋潔，山上浩志，吉田晃敏

研究論文

携帯電話による安全性の高い利用者認証が可能な遠隔医療用通信インフラシステムの開発と評価

三上大季[1)]、林弘樹[1)]、守屋潔[1)]、山上浩志[2)]、吉田晃敏[3)]
[1)] 旭川医科大学医工連携総研講座、[2)] 旭川医科大学病院経営企画部、[3)] 旭川医科大学

要旨
遠隔医療における通信インフラとして、低コストであるインターネットが多く利用されている。インターネットは公衆網であるため、通信内容の暗号化と共にサービスシステムへの不正なアクセスを防ぐための利用者認証が必須となる。最も一般的な利用者認証方式は ID/パスワードによる認証であるが、認証情報の漏洩による第三者の「なりすまし」が行われる危険性が高い。そこで本研究では、インターネットを基盤とした遠隔医療システムにおいて、本人が所有する携帯電話を利用者認証手続きに利用することで安全性を高め、且つ利用者認証と連動して通信端末間に安全な VPN 通信路を動的に確立できる通信インフラシステムを開発した。医療従事者に本システムを体験してもらいアンケート評価を行ったところ、92%の評価者が本システムの有効性を認めた。

キーワード：インターネット、セキュリティ、利用者認証、VPN、携帯電話

はじめに

過疎地・離島における都市部との医療格差を解消する手段として、IT 通信機器を利用した遠隔医療は実用化段階にある。遠隔医療に用いられる通信インフラとしては、現在コスト面での優位性からインターネットが多く採用されているが、公衆網であるインターネットを用いる場合、主に VPN によって実現されている通信の暗号化と共に、システムの正規利用者ではない者による不正アクセスを防ぐための厳格な利用者認証が不可欠である。

正規利用者の認証方法としては、ID/パスワードを用いた認証が最も一般的であるが、認証情報が漏洩した場合、本人以外の者が正規利用者として認証される「なりすまし」が行われる危険性が高い。そのため、バイオメトリクス認証、専用の物理デバイスを用いた認証等、記憶に依らない認証手法を採用または併用した利用者認証システムが増加しつつある。一方、現在普及している携帯電話には一意な固体識別番号が設定されており、使用者の特定に適している。また、携帯電話の高機能化により、Web アクセス機能、バイオメトリクス認証機能、非接触型 IC カード機能等、通話以外に応用可能な機能が搭載されている機種が近年多くなっている。

そこで本研究では、遠隔医療システムの端末から利用者認証を行う際に携帯電話を併用することで安全な認証を行い、また認証と連動して通信端末間に動的に VPN 構築を可能とする通信インフラシステムを開発し、その有効性、実用性の評価を行った。

システム概要

図 1 に本システムの概要を示す。本システムではインターネットを基盤にして、医療施設間通信（DtoD）、在宅医療における通信（DtoP）等、遠隔医療の様々な用途において安全な通信を行うことが可能である。本研究では評価用アプリケーションとして、利用者の権限に合わせて患者の診療歴を閲覧可能な医療情報 DB を構築した。システムの主な特長は次の 2 点である。

(1) 携帯電話による利用者認証

利用者認証にソフトバンク BB 社のオンライン認証サービス「SyncLock」[1)] を用いた。このサービスでは、同社が管理するシンクロ認証サーバに事前登録された利用者本人所有の携帯電話（他社の携帯電話にも対応）を本人認証キーとして用いる。認証後の通信管理、認証の仲介については、本研究で構築した認証管理サーバが行う。以下、図 1 におけるユーザの利用者認証の手順を示す。

① ユーザは PC から認証管理サーバにアクセスし、シンクロ認証サーバに事前登録した携帯電話 ID を入力する。
② 認証管理サーバはシンクロ認証サーバへ本人認証の証明要求を送信する。
③ シンクロ認証サーバからユーザの PC に認証用の数字を発行する。
④ ユーザは事前登録した携帯電話より、PC に表示された③の数字をシンクロ認証サーバに送信する。
⑤ シンクロ認証サーバで、事前登録された携帯電話情報、発行した認証用の数字、携帯電話から受信した数字を照合し、認証管理サーバに認証完了を通知する。

このサービスではインターネット網とモバイル網を用いた複合認証を行うため安全性が高く、認証時の通信データはワンタイム認証用の数字であることから盗聴による二次利用の恐れは無い。また、認証時に数字の入力に加えて、暗証番号、Ｑ＆Ａ、声紋、指紋のオプション認証も組み合わせることが可能なため、携帯電話を本人以外が操作しようとした場合にも安全性を保てる。

(2) 動的 VPN 構築

インターネット網の VPN 設定には、ファイアウォール機器を用いて固定的に複数拠点を LAN 接続する方法があるが、在宅医療等、不特定多数の患者と通信を行う場合には適していない。そのため本システムでは、通信制御用の中間サーバとなる認証管理サーバを介在させることで、異なる LAN にある端末でも必要なときに VPN 設定し、同一の仮想 Ethernet に接続可能な動的 VPN 構築システムを採用した。以下、図 1 における利用者認証後の VPN 構築の手順を示す。

⑥ 認証管理サーバは、医療情報 DB に認証ユーザのアクセス許可を通知する。
⑦ 認証管理サーバは、ユーザ PC と医療情報 DB 間に VPN を構築する。
⑧ ユーザ PC に医療情報 DB 閲覧画面が表示され、通信可能となる。

尚、利用者の離席等で PC の無通信時間が長時間継続した場合は、本人以外による端末操作の恐れがあるため、端末のスクリーンセーバ機能と連動して VPN を切断し、本人が再操作する場合には、携帯電話の Felica 機能を用いて簡易認証を行い、VPN を再設定する機能も備えた。

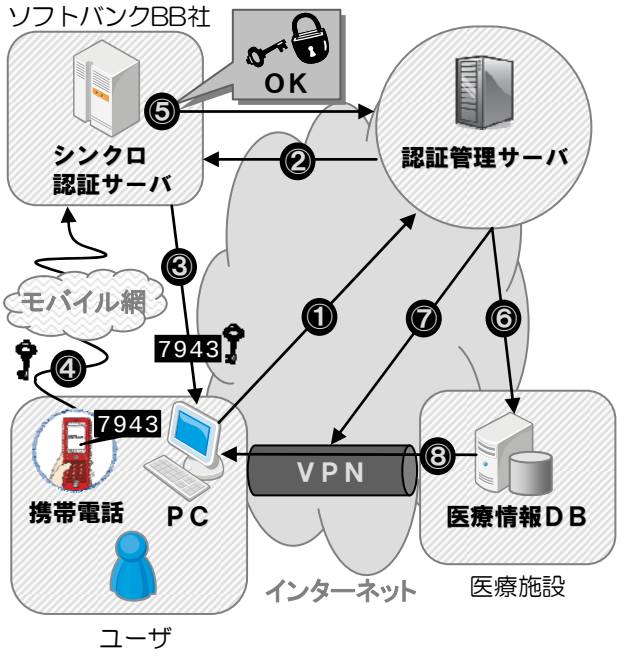

図１　システム概要

評価方法

旭川医科大学病院に勤務する 13 名の医療従事者に前述の①～⑦の手順の操作と Felica 機能による VPN 再接続機能を体験してもらい、本システムの有効性・実用性に関してアンケート形式の評価を行った。尚、全ての評価者は利用者認証において、同一種の評価用携帯電話を同一手順で操作した。

結果

図 2 に評価結果を示す。携帯電話を用いた認証操作に関して､携帯電話の認証数字入力操作については 76%､Felica 機能による VPN 再設定機能については 92%の評価者が操作が簡単であると回答した。また、ID/パスワードによる認証と比較して、76%の評価者が有効であるとし、本システム全体の評価としても、92%が有効であるとの評価を得た。

考察

本システムの特長である携帯電話を使用した認証、また動的 VPN 設定に関して、遠隔医療用途において概ね有効であることが確認された。数字四桁の番号入力による認証操作に関して、一部の評価者から煩わしいとの声もあったが、評価用携帯電話の操作に未習熟であることを理由とした評価者もいたことから、本人の所持する操作に慣れた携帯電話を使用した場合には、より容易に入力可能と考えられた。また、複数の評価者から「僻地や離島の患者は高齢者が多いため、在宅医療に用いる場合には簡単に利用できることが重要」とのコメントを得ており、特に高齢者向け携帯電話所持者にはより見やすい操作画面を提供する必要があると考える。

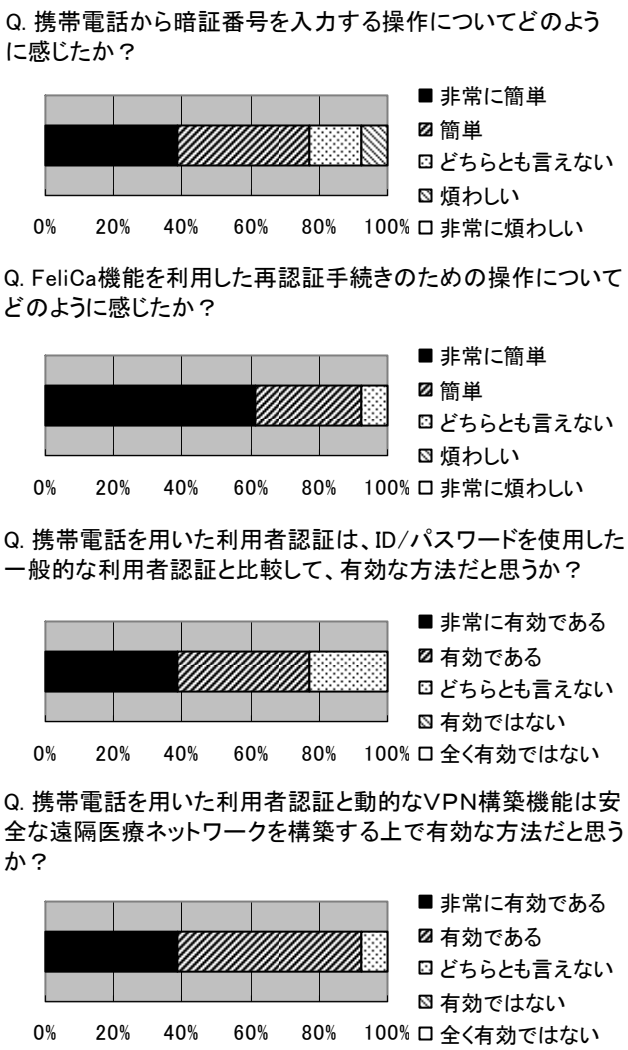

図２　アンケート評価結果

まとめ

インターネットを基盤として、携帯電話を用いた利用者認証、動的 VPN 構築が可能な遠隔医療用通信インフラシステムを開発した。医療従事者によるアンケート形式の評価により、遠隔医療用途として本システムの有効性を確認した。現状の本システムにおける VPN 設定時の通信帯域が 10Mbps 以下に制限されるため、今後は遠隔医療における通信品質の実用性評価を行う予定である。

参考文献

1)ソフトバンクBB株式会社. “SyncLock　シンクロック-新しい発想のオンライン認証システム 概要資料” . http://www.synclock.jp/04_download/image/SyncLock_doc20070920.pdf　2007.