「措置入院」の診察のためのセキュアな精神保健指定医決定システムの開発（142306007）

Secure system of second appointment with mental health designated psychiatrist for involuntary admission.

研究代表者

平成 26 年度・27 年度研究代表者　杉浦伸一　　名古屋大学（現職：同志社女子大学）

Shin-ichi SUGIURA　　Nagaya　University

（Doshisha Women`s College of liberal arts）

平成 28 年度研究代表者　　郷間宏史　名古屋大学

Hiroshi Gohma　　Nagoya University

研究分担者

浅野美香†　MS ドリーム株式会社

Mika ASANO　MS Dream co. ltd.

研究期間　平成 26 年度～平成 28 年度

概要

精神科の措置入院患者の再診を担当する精神保健指定医の選択は守秘性が高く決定に苦慮する。この選択システムに携帯電話等の簡易なメール機能を使えるようにするために平文を符号化して暗号化することで、最小限の通信量で守秘文書を送信するシステムを開発した。さらに画像転送機能を加え、東海地区特有の手の外科テレトリアージや残存医療機能把握システムへの応用を検討した。

精神保健指定医決定システムへの導入とサイト上での仮想環境において、平文を Advanced Encryption Standard (AES)128 で暗号化した後、カギ情報を破壊して送信する転送アルゴリズムを開発し、VPN 等を用いずに情報交換する方法を構築した。この方法では、パスワードを付与する際に、カギ情報の一部のみを送信するため転送中の情報を傍受され翻訳されたとしても利用できない状況となった。受け取り側は、入手した 2 種類の暗号キーをブラウザーに送ることで平文に復元する方法とした結果、利用者は通信中に暗号化を意識することなく平文情報を暗号化して交換することが可能となった。

１．まえがき

精神障害の疑いのある者を強制的に入院させる「措置入院」、「医療保護入院」は、入院から 72 時間以内に二人目の精神保健指定医の受診が義務付けられている。行政担当者は、再受診を担当する医師を探す際に、これら守秘性が高い患者情報を、その都度電話で伝えたりメールで連絡したりして来た。これら措置入院患者の背景には犯罪が関っていることも多いため、精神保健指定医の少ない愛知県ではその対応に苦慮してきた。

本研究は、行政担当者が、守秘性の高い情報を VPN 等の特殊な情報網を用いずに簡易な通信方法で精神保健指定医を決定できるシステムを構築することである。また、災害等が発生した際に無線通信を用いたインターネット回線であっても守秘情報を交換できるプロトコールを開発することを目的とした。

２．研究開発内容及び成果

愛知県下では、かかりつけ医が精神疾患を疑う患者が発生した際に精神科医に相談したり、受診を依頼したりするシステムとして「こころの Dr ネット」が運用されている。今回、「このこころの Dr ネット」にサブドメインを作成し「措置入院」や「医療保護入院」患者が発生した際に利用可能なシステムを構築し、その情報伝達プロトコールを開発した。

精神保健指定医の検索システム

タイトル（名古屋市からの措置診察の依頼）、診察根拠通報、診察依頼日、依頼日あるいは依頼する曜日、診察場所、患者の身体情報および契機となった事案名を選択するだけで依頼文が自動的に完成するように設計した。また、送信先は選択式とし、候補者全員、特定のグループ、あるいは特定の医療機関のみに送信できるようにした。受け入れ施設の登録は、愛知県精神化病院協会が運営する「こころのDrネット」参加施設に依頼した。また、名古屋市の協力もあり、当初の30施設の計画であったが、結果として60施設の登録ができた。その結果、精神保健指定医が所属する県下の医療施設全てを網羅できた。

通信アルゴリズムの概要

守秘性が高い情報を、携帯電話等の簡易なメール機能を使えるようにするために文書を符号化して暗号化することで、最小限の通信量で守秘文書を送信するシステムを開発した。

今回、暗号化としてスタック型の2次元コードを元にQRコードなど、以下の暗号化を検討した。

1. ビットマップフォントによる暗号化の考察（スタック型二次元コードへの応用）
2. QR コードによる転送技術の検討
3. AES(CBC/128)暗号化を用いた更にセキュアな転送方法の検討

1. ビットマップによるコード化の検討

今回の研究では、送り先が携帯電話やiPadなどの場合があるため、送信するDot per inch（DPI）を事前に検討しなければならない。つまり、DPIは1インチあたりに何ドットの点を打てるかを表わす単位であり、96DPIでは、1インチ当たり96個の点を打てることを意味する。すなわち、画面上

の96ドットを1インチとして扱うことになる。ただし、1インチは物理的な長さではなく、ディスプレイ上のドット数によって変化する。

本研究では、記号による暗号化を実施するに当たり、空白のフォント欄にデータを投入するため、12 ポイントの文字として 16×16 ドットの枠内にドットを入力することで短縮文字をあらわすこととした。

2. QR コードによる転送技術の検討

ビットマップによるコード化はスタック型の 2 次元コードの基本形である。QR コードには切り出しシンボルと呼ばれる記号が 3 点に設けられており、これによって上下位置が決定できるため、読み取る方向にかかわらず正しく読み取りを行うことができるよう設計されている。従って、マトリックス型の QR コードも同様のプロトコールで読み取り可能なことがわかった。

3. AES(CBC/128)暗号化を用いた更にセキュアな転送方法の検討

図 1 にコントロール画面を添付した。

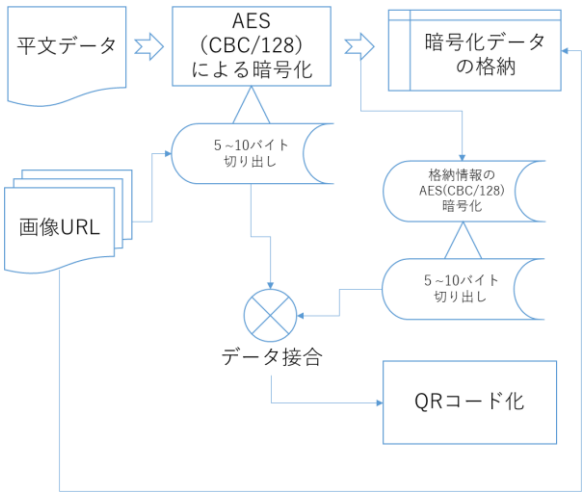

図 1　暗号化の概要

一般に、平文を AES(Advanced Encryption Standard)-128bit Cipher Block Chaining Mode モード（以降 AES（CBC/128）とする）で暗号化すると 16 バイト程度の文字列がバイナリ 64 バイトに拡大する。この結果を QR コード化するにあたり、短文の場合は問題ないが 200 文字程度であっても生成される QR コードが複雑になり読み取り性能が著しく悪化することが判明した。この問題を解決するために、新たなアルゴリズムとして、AES（CBC/128）暗号化後の文字列の先頭 5～10 バイトを QR コードに格納し、それ以降を web 上の通信で転送することにした。従って、QR コード内のデータと web 上のデータ双方を合わせたデータをローカルで複合するため、QR コードの複雑化を回避できた。この結果、長文であっても読み取り性能が安定した。

本研究の目的の骨子は、1.セキュアな平文転送及び 2.送受信の情報量を削減することであった。従って、大量の情報をメール送信には流さず、カギ情報だけを転送することで解決を図った。また、カギ情報であっても完全な情報を解読されれば情報へのアクセスが可能となることを考慮し、カギ情報の一部と、サイトアドレスの一部を分解し、QR コードとすることで更なる暗号化を行った。その結果、インターネット上で流れる情報をすべて入手し解読したとしても、記号の羅列であり解読不可能とした。

3．今後の研究開発成果の展開及び波及効果創出への取り組み

本研究で開発した通信方法は、同一サーバー内へのアクセスに用いるカギの一部を交換するだけであり、ネットワークに情報が流れない。その結果、通信量が制限される無線によるインターネット通信であっても大量の情報を交換できることになる。今回開発したシステムは、携帯電話などの平文通信という一般的な通信環境であっても守秘的に情報交換ができるため、今後多くの平文通信において応用可能と考えられた。

4．むすび

本研究は、従来の大量の文書を送信するという通信方法から閲覧するためのカギだけを交換する方法への抜本的な発想転換となっており、今後の通信技術の改革に寄与するものと考える。なお、本稿は、杉浦伸一の主導により本研究開発が行われたため、杉浦伸一及び MS ドリーム（株）の研究成果結果の内容を執筆した。

【誌上発表リスト】

[1]杉浦伸一、浅野美香、“複数疾患治療の構造化に挑む・ICT を利用した患者/医療者連携”臨床知識学会抄録集、東京大学伊藤国際学術研究センター（2017 年 1 月 28 日）

【申請特許リスト】

[1]杉浦伸一、浅野美香、インターネットを用いた平文暗号化のアルゴリズム、日本、準備中