博 士（医 学） 加 藤 五十六

学 位 論 文 題 名

電子カルテセキュリティ管理強化目的での自由文入力キーストロークダイナミクスによる個人認証

学位論文内容の要旨

〖背景と目的〗キーストロークダイナミクスとは「電子筆跡」とも言えるバイオメトリクス認証の一種であり，誰が入力しているのかを通常のキーボード操作中にキー操作のタイミング情報に基づいて推定あるいは認証する技術である．動的なキー操作の個人差を分析して入力者を同定する試みは1970 年代に始まるが，ほとんどの研究はあらかじめ決められた文章や単語を入力する場合（固定文入力）の分析に焦点が当てられていた．日本語の自由文入力分析については過去の研究報告は少ない．自由文キーストロークダイナミクス分析を応用して電子カルテへの［なりすまし入力］を検出する機構が実用化可能であることを示すために，バッチモードで動作する識別エンジンとデータ収集システムを構築して精度を検証した．

〖対象と方法〗まず病院外で８名（年齢 28～61）のボランティアの同意を得て個人所有のパーソナルコンピュータ（ＰＣ）にデータを採取するプログラムをセットして日常作業の中でサンプルを収集した．次に北海道大学病院で医師と看護師 35 名の同意を得てシステム端末に採取プログラムをセットし，病院業務中での入力からデータを採取した．データは３連続キーストローク（トリプレット）を単位として計測，蓄積，分析した．サンプル採取，識別，および結果の視覚化はすべてＣ＋＋によって記述した自作プログラムで行った．識別エンジンは本人データを学習した後で識別対象データと学習データの類似性を示す数値を算出し，それをあらかじめ決めた「カットオフ値」と比較し，カットオフ値を越えれば「対象データは学習データと同じ人物から由来している」と判定する．ボランティア由来のデータを用いて学習データの量と識別精度の関係を検証するヒストグラムを作成した．１回に判定するデータのサイズと識別精度の関係はボランティアデータからＲＯＣ曲線をプロットして確認した．病院で採取した実データからもボランティアグループと同一条件でＲＯＣ曲線を作成し，両者を比較した．

〖結果〗病棟でのデータ採取では医師は長文の日本語入力することなくログアウトする事も多く（９０％以上），採取効率（採取データ量／日数）は低かった．病院端末と同等の能力のＰＣにおいて，認証識別エンジンが学習に要する時間は典型値で約１秒，判定に要する時間は 40 ミリ秒以下であった．学習量と識別精度の関係では学習トリプレット数が多いほど良好な分離を得た．ヒストグラム上では他人挑戦の曲線は右端まで低く伸び，左側では本人認証の曲線は

0になった．1回の判定に用いるデータ量と精度の関係では判定に用いるデータ量が増えるにつれてＲＯＣ曲線は左上に移動し，より高い判別能を示した．本人認証の結果値ヒストグラムには個人差があり，左側にすその広がる人の存在を確認できた．病院採取データとボランティアデータを比較したＲＯＣ曲線では，全ての領域で病院採取データがより高い精度を示し，学習 7000 トリプレット，1回判定数 150 で，他人受け入れ率 5%，本人拒否率 0.3%を達成した．

【考察】旧来の使用開始時に行う「門番型」認証では高い「他人発見率」が要求され，一方ではある程度の「本人拒否率」も許容されている．しかし持続的な監視を計画するならば特異度が高い（本人拒否率が低い）ことが重要であり，ＲＯＣ曲線では左端の部分に注目する必要がある．

ボランティアデータにおける本人認証と他人認証の評価値ヒストグラムの左側では本人認証の曲線は0になっているが，これは認証エンジンの特徴として特異度を極めて高い値にするカットオフ値の設定が可能である事を示しており，高い特異度を要求する持続監視目的に適している事を示唆する．本人認証の個人別結果値ヒストグラムのすそが左側に広がっている人は，いわゆる「羊と山羊問題」の山羊に相当し，特異度が高く（本人拒否率が低く）なるようにカットオフ値を設定しようとすると精度の足を引っ張る存在である．判定に要する時間，学習に必要な時間はいずれも受け入れ可能な値であった．

病院採取データとボランティア由来のデータの結果の比較では，構成メンバの属性がボランティアグループでは年齢，性別，職種等様々であるのに対し病院では一様だった．採取条件は病院では端末の能力差，キーボードの個体差や経年変化の差等の採取条件の不安定性があり，いずれも病院採取データから得られる結果を相対的に劣化させるバイアス要因と予測した．それにもかかわらず病院採取データからの結果の方が精度において大幅に上回った．したがって今回の場合については，いずれも決定的な障害にはならず，ボランティアの側になんらかの精度を悪化させた要因も存在していた可能性が高い．その原因として疑わしいのは入力コンテキストの多様性である．病院採取データの入力はほとんどが看護記録の記載で入力コンテキストとしては一様であったが，ボランティアは日本語入力以外にプログラミング，ファイルのメンテナンスなどの多様な作業を同一人物が行い，入力コンテキストに多様性があった．今回開発した認識エンジンは入力コンテキストの多様性についてはロバストではなかったとするとこの結果の差は説明可能になる．

同一仕様のキーボードを使う必要があるとか，初期の学習データとして大量の入力が必要である等のキーストロークダイナミクスの一般的な普及を妨げている問題のいくつかは病院情報システムでは容易に解決可能である．

Windows はリアルタイムＯＳではなく，本手法における時刻測定の分解能は 16ms であったが，より高い精度での時刻測定が可能になれば識別精度が向上する可能性は高い．

【結語】持続監視目的でのキーストロークダイナミクスは，未完成の技術ではあるが，実際の現場で試しても良いレベルの性能を有していることが判った．電子カルテのセキュリティ管理は，病院ではキーストロークダイナミクスの欠点をカバーしやすい事もあって試験現場の候補になりうる．自作した認証識別エンジンと採取プログラムからは，ボランティアのデータと病院で採取した実データの両方で見込みのある結果が得られた．病院採取

データの認証精度が上回った理由は入力コンテキストの多様性の差であった可能性がある．現時点での到達精度は，リアルタイムの警報に直結するには不十分であるがレトロスペクティブな分析や監査には応用可能な程度であり，さらなる精度向上の努力が必要である．

学位論文審査の要旨

主　査　　教　授　　櫻　井　恒太郎
副　査　　教　授　　前　沢　政　次
副　査　　教　授　　玉　城　英　彦

学位論文題名

電子カルテセキュリティ管理強化目的での自由文入力キーストロークダイナミクスによる個人認証

キーストロークダイナミクスとは「電子筆跡」とも言えるバイオメトリクス認証の一種であり、入力者をキー操作のタイミング情報に基づいて認証する技術である。自由文キーストロークダイナミクスを応用して電子カルテへの「なりすまし入力」を検出する機構の実用性を示すため、バッチモードで動作する認証エンジンとデータ収集システムを作成し、精度を検証した。　対象はボランティア８名と現役の医師および看護師３５名であり、同意を得て業務中の入力データを採取した。データは３連続キーストローク（トリプレット）を単位として分析した。認証エンジンは本人データを学習後、対象データと本人データの類似性を示す数値を算出して「カットオフ値」と比較判定した。まずボランティアのデータを用いてヒストグラムとＲＯＣ曲線をプロットして精度を確認し、病院で採取した職員のデータもボランティアグループと同一条件でＲＯＣ曲線を作成して両者を比較した。

判定に要する時間は１回 40 ミリ秒以下であった．学習トリプレット数（2000,3000,,7000)が多いほど判別は良好となった。１回の判定データ量（50～200 トリプレット)が増えるにつれてＲＯＣ曲線は左上に移動し、より高い判別能を示した。病院採取データとボランティアデータを比較したＲＯＣ曲線では全ての領域で病院採取データがより高い精度を示し，学習 7000 トリプレット，１回判定量 150 の場合、他人受入れ率 5%，本人拒否率 0.3%であった。

持続監視目的では特異度が高い（本人拒否率が低い）ことが特に重要でありＲＯＣ曲線の左端に注目する必要がある．ボランティアデータのヒストグラムでは本人の分布が 0 となる判別値の領域があり、感度を犠牲にすれば特異度を極めて高い値にすることが可能である。病院採取データとボランティアデータの比較では精度において前者が大幅に上回った。この原因としては入力コンテキストの差が考えられる。すなわち病院採取データはほとんどが看護記録の記載で入力コンテキスト一様であるのに対し、ボランティアの入力はメール作成、プログラミング，ファイルメンテなど多様であった．本方法の実用化に必要なキーボード仕様の統一や大量の学習データ取得などの条件は、病院においては解決可能である。

結論として、自由文キーストロークダイナミクスは、自作した認証エンジンとデータ収

集システムにより、現場で試用可能な性能を有していることが証明され、病院の環境は実用に適している。現時点での性能はリアルタイムでの警報にはまだ不足しているがレトロスペクティブな分析には応用可能である.

以上の発表に対し、副査の前沢教授より、学習用データの採取に要する時間、および実用化の問題点についての質問があった。申請者は、学習はボランティアでは４日から２ヶ月を要したこと、問題点としては精度が不足しているが改善の方法は見つかっていること、電子カルテのソフト面の改良が有効であると回答した。続いて副査の玉城教授より、セキュリティ保持手段としての価値、拒否する従業員への対応、サンプル数やボランティアの構成の計画性についての質問があった。申請者はこの方法は多様な監視システムのひとつであり補助的であること、本人を守る意味もあることを理解してもらうべきだが拒否も止むをえないこと、 設定は計画的ではなく、比較する８人として均質な職員を選択したと回答した。聴衆の大学院生より、複数の記載者たとえば指導医と研修医が協力して文書を作成する場合に対応できるかとの質問があった。申請者は各々が別のＩＤを使う限り問題はなく、同一ＩＤを複数で共有すことを検出することがこのシステムの標的である、と回答した。最後に主査の櫻井より、検証するのに必要なトリプレット数、２人が混在している場合の認証、薬物の影響についての質問があった。申請者は、必要数は５０～７０であること、境界不明で混在している場合は個別認証はできないこと、アルコールなどの影響があると別人と判断されること、と回答した。

この論文は、電子カルテ入力における実用的な個人認証を独創的な方法と自作によるプログラムで実証し、特許申請にまで進んだことが高く評価され、今後の発展が期待される。

審査員一同は、これらの成果を高く評価し、申請者が博士（医学）の学位を受けるのに充分な資格を有するものと判定した。