

外国人被疑者取調べにおける通訳システムの機能の拡張

脇田和宏¹ 佐々木良一¹

概要: 近年, 来日する外国人が増加していく中, それに伴い我が国で発生する外国人犯罪件数も増加している. 外国人被疑者取調べにおいて通訳人を介し調書を作成しており, 通訳人を信頼できる第三者として通訳の正確性を保証している. 現在, 調書作成にかかる時間が問題となっており, 時間の短縮が求められる. そのため, 通訳人到着までの時間を有効に活用するため, 将来的に外国人被疑者取調べにおける通訳のシステム化を目指し通訳システムのプロトタイプの開発, 評価を行った. 基本的な機能を実装できたが, 音声認識精度の向上の必要性, 具体的な不正の洗い出しが不十分, 利用申請によるチェック機構の必要性に気づいた. 本研究においては, 運用, 前提条件の検討により具体的な不正の洗い出しを行い, 利用申請によるチェック機構の追加の提案, また改ざん検知におけるコスト効果のより良い手法の提案を行った. この結果, 利用申請機構を追加することにより, 具体的な不正への対応が取れていることを示した. また, 実験結果より, 改ざん検知における署名検証時間を短縮できることが明らかになった.

キーワード: セキュリティ, ブロックチェーン, ヒステリシス署名, IoT, デジタルフォレンジック, Google Cloud Platform, スマートコントラクト

Function Extension of Interpreter System for Interrogation of Foreign Suspects

KAZUHIRO WAKITA^{†1} RYOICHI SASAKI^{†1}

Abstract: Recently number of foreign crimes tends to increase because of increasing number of foreigners coming to Japan. When investigating foreign suspects, creating a record through an interpreter who guarantees interpretation accuracy as trusted third party. Now, it has become a challenge to shorten time it takes creating a record. Thus, we developed interpretation system for assisting to create a report, and evaluated the system. We noticed the improvements of the system, which the accuracy of voice recognition and insufficient enumeration of fraud, necessity of check mechanism so on. This article was described about Considerate enumeration of fraud by considering operation or assumptions, and additional proposal of check mechanism, and the improvement of the method of tamper detection. As a result, it was shown that the countermeasures against specific fraud were taken by adding the use application mechanism. Experimental results also show that signature verification time for falsification detection can be reduced.

Keywords: Security, blockchain, hysteresis signature, IoT, digital forensics, Google Cloud Platform, Smart Contract

1. はじめに

近年, 来日する外国人が増加していく中, 我が国で発生する外国人犯罪件数も増加している. このため, 外国人被疑者取調べにおいて通訳人の確保, 調書作成にかかる時間が問題となっている.

様々な業務がシステム化される中, 外国人被疑者取調べにおいて通訳人になる通訳システムはまだなく, 証拠保全における手法や通訳の正確性, 機器による誤差, 人による誤差等検討すべき課題が多くある現状である.

筆者らはこれまでに通訳システムのプロトタイプの開発と評価を行ってきた[1]が,

(問題 1) 具体的な不正の洗い出しが不十分

(問題 2) 利用申請によるチェック機構の必要性に気づいた.

本稿では, 具体的な不正について段階ごとに検討するとともに, 新たに利用申請機構を加えることで問題が解消され

たことを示した.

本稿では, 2 章で関連研究との比較を行い, 3 章において従来の研究について述べ, 4 章において, 本稿における拡張点である利用申請機構の追加や具体的な不正への検討を述べ, 従来手法との比較評価を行った. 5 章に本稿の各頂点の評価を行い, 6 章では, 今後の課題を述べる.

2. 関連研究

関連研究として, 一般的な取調べの可視化における技術課題, システム提案についてはこれまで文献[2]等で論じられてきた. また, 音声システムによる多言語支援を目的とし, 収録環境の限定や, 認識機能で用いるモデルを事前に学習させるなどの最適化を行い, 音声認識の認識率の低下及び結果として生じる翻訳間違いを防ぐ研究が行われている[3]. ブロックチェーンに関する研究は盛んに行われているものの, 取調べにおける発言の証跡に対する改ざん検知手法の性能評価は筆者らによる Google Scholar における調査では行われていなかった.

¹ 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120-8551
Chiyoda, Tokyo 101-0062, Japan

3. 従来の研究

3.1 通訳システム

3.1.1 取調べのシステム化

これまでに従来の取調べの手順から以下に示す部分のシステム化を行った（表 1 参照）。

表 1 取調べのシステム化

Table 1 Interrogation systematization

	従来の取調べ		通訳システム
①	被疑者逮捕	—	被疑者逮捕
②	通訳人到着 取調べ開始	システム化 →	通訳システムによる 取調べ開始
③	調書読み聞かせ	—	調書読み聞かせ
④	調書に署名	—	調書に署名

②の部分のみシステム化を行い、③調書の読み聞かせや④調書に署名は従来通り、通訳人が行うものとした。

また、通訳人においては信頼できる第三者としている。

3.1.2 システム概要

次に構築した通訳システムの概要を以下に示す（図 1 参照）。MicroSD カード上にシステムを構築し、音声認識及び音声翻訳には Google Cloud API[4][5]を用いてマイクによる入力情報から変換することとした。

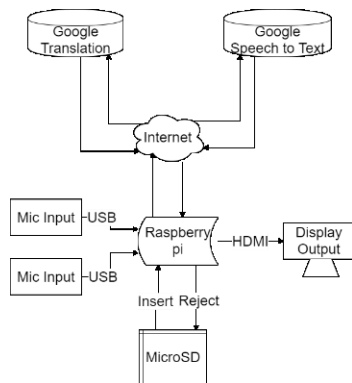


図 1 実験装置概要

Figure 1 Outline of experimental equipment

3.1.3 データフロー

次に通訳システムの流れにおいて、音声情報、音声認識テキスト、音声翻訳テキストと順に変換を加え、ディスプレイに表示することとした（図 2）。

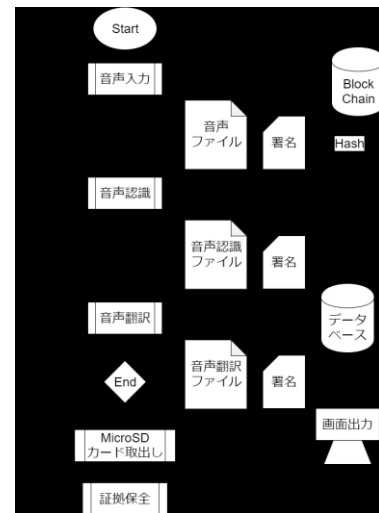


図 2 データフロー図

Figure 2 Data flow diagram for proposed method

3.1.4 改ざん検知

また、改ざんを検知するため、ブロックチェーン[6][7]とヒステリシス署名[8][9]を用いた以下のような仕組みを構築した（図 3 参照）。

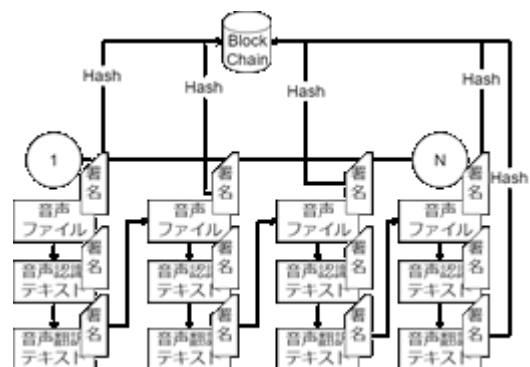


図 3 通訳システムの改ざん検知の仕組み

Figure 3 Interpretation system tampering detection mechanism

この際、検討した不正は以下のものであり、改ざん検知手法に対しての実験を行った（表 2 参照）。

改ざんシナリオ

- T1：ランダムに一つのファイルを改ざん
- T2：ファイルの一つ改ざんし、改ざんしたファイルの電子署名を生成する
- T3：最後のファイルを改ざんし、改ざんしたファイルの電子署名を生成する
- T4：すべて作り直す

表 2 改ざんシナリオに対しての実験結果

Table 2 Experimental results for falsification scenarios

	T1	T2	T3	T4
電子署名	○	×	×	×
ヒステリシス署名	○	○	△	×
ブロックチェーン	○	○	○	○

これまで検討した不正においてはファイルに対しての改ざんについてであり、より具体的な不正に対しての検討が不十分であった。

3.1.5 通訳システムの画面

以下に通訳システムの画面を示す (図 4 参照)。

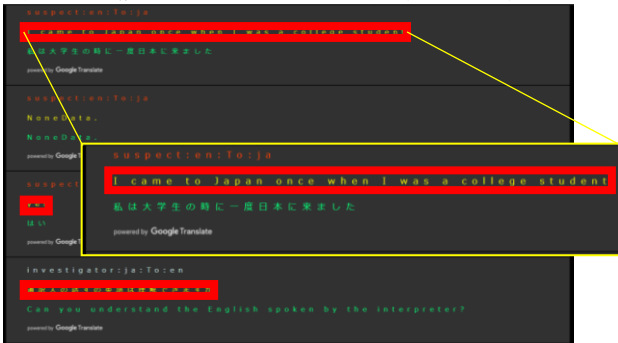


図 4 通訳システム画面
 Figure 4 Display of the interpreter system

4. 本稿における拡張点

これまでに具体的な不正の検討が不十分であったために対応できていなかった, (1) 通訳システムにあらかじめ不正な改ざんを施す, (2) 取調べの記録自体をなかったものとするなどといった不正に対応するため, 利用申請機構を追加するとともに, 通訳システムの運用, 前提条件を示し, さらに段階的に不正に対応できているかを検討する。

4.1 利用申請機構の追加

(問題 2) について利用申請機構を従来のシステムに組み込んだ概要を以下に示す (図 5 参照)。利用申請をすることにより, 通訳システムが利用できることとし, それまでは利用申請以外できないものとする。

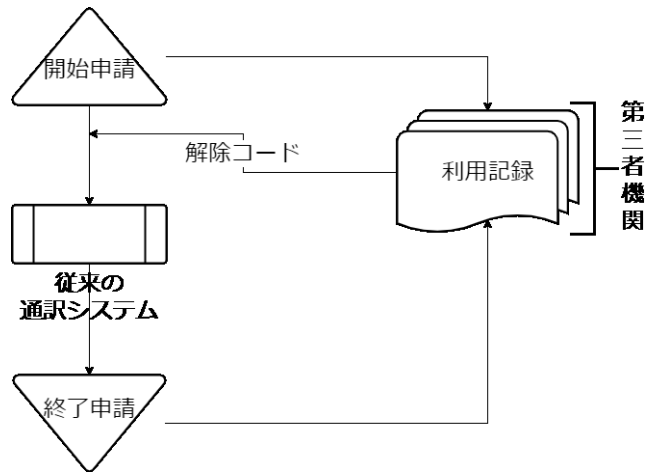


図 5 利用申請機能の概要
 Figure 5 Outline of function for request

利用申請情報を外部機関が保持することによって, 取調べの存在が残される。本稿の想定では, 第三者機関に代わりスマートコントラクトの利用を想定する[10]。

4.2 スマートコントラクト

スマートコントラクトとは, 仲介者を介在させることなく代金や商品の交換の契約を行うことができ, 購入者と販売者の間の交換契約内容をあらかじめブロックチェーンにプログラミングしておき, 定めた契約条件が満たされると自動的に取引が行われる仕組みである (図 6 参照)。



図 6 スマートコントラクトの概要
 Figure 6 Outline of smart contract

本稿においては, スマートコントラクトの仕組みを用いて購入者を捜査機関, 販売者を裁判所などの第三者機関として利用申請に対して解除コードを送るような仕組みを想定する (図 7 参照)。



図 7 システムに適用したスマートコントラクトの概要

Figure 7 Outline of smart contract for the system

4.3 運用の流れ

これまでに洗い出しが不十分であった具体的な不正を検討するにあたり, これまでに検討されていなかった通訳システムを利用した場合における運用の流れを示す (図 6 参

照).

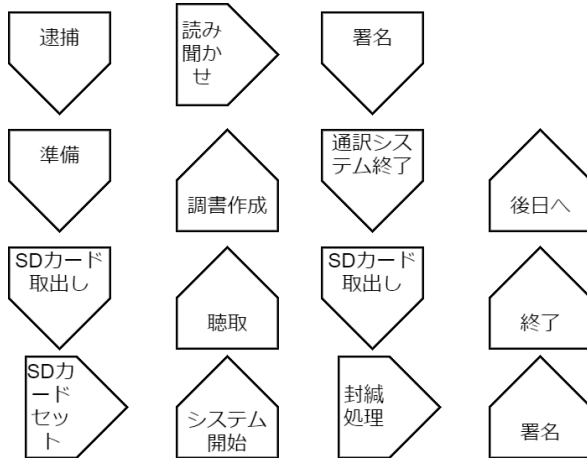


図 8 運用の流れ

Figure 8 Operation Flow

全体の流れとして

- ① 被疑者逮捕
- ② 取調べの準備
- ③ 封緘処理された MicroSD カードを取り出す
- ④ 通訳装置に MicroSD カードをセットする
- ⑤ システム開始時に第三者機関から解除コードを入手する
- ⑥ 取調べ
- ⑦ 通訳システムを利用して調書を作成
- ⑧ 通訳人は翻訳が正確であることを確認し、被疑者に読み聞かせを行う
- ⑨ 被疑者が同意すれば、調書に署名、通訳人、捜査官も署名
- ⑩ 通訳システムの終了申請を出す
- ⑪ MicroSD カードを取り出す
- ⑫ 調書と MicroSD カードを封緘処理する
- ⑬ 封緘処理した封筒に署名する
- ⑭ 取調べ終了
- ⑮ 後日

(被疑者による“事後の申し立て“を行った時とする) となると考える。

4.4 前提条件

(問題 2) を検討するため、以下の前提条件を考える (表 3 参照)。

表 3 前提条件

Table 3 Precondition

前提条件	内容
利用前の MicroSD カードは未開封とする	通訳システムを利用する前に不正なプログラムは動いていない
被疑者の同意をとった署名は有効である	被疑者は署名に対して嘘をつかない
通訳人の扱いは信頼できる第三者とする	通訳人は翻訳の正確さにのみ責任を持つものとする

利用申請による記録は正確に保管されるものとする	利用申請を記録する第三者機関は不正をしないものとする
取調べ終了後は調書と MicroSD カードは確実に封緘処理されるものとする	封緘処理した後の捨てた、紛失したと虚偽の申し立てをするといった不正はないものとする
通訳システム停止中に行われた不正は対象外とする	例えば別室に連れていき強引な説得後に通訳システムを利用する等の不正については通訳システムにおける対処を超える問題となるため対象外とする

4.5 不正の洗い出し

運用と前提条件を踏まえた上で考えられる不正について段階ごとに表にまとめた。

4.5.1 開始時点

表 4 システム開始時点における不正

Table 4 Improprity at system start

不正を行う人	通訳システム開始時点
被疑者	—
捜査官	—
通訳人	—

利用申請機構を追加したことで、申請による制限解除まで、開始時点、また開始時点より前においては、通訳システムを利用した取調べに関わる人に不正はできない。

4.5.2 システム利用中

表 5 システム利用中における不正

Table 5 Improprity during system use

不正を行う人	通訳システム利用中
被疑者	—
捜査官	(1) 途中で不適切に説得する
通訳人	—

(1) においては、MicroSD カードの中に保存されている通訳システムの情報から不正を発見することができる。

4.5.3 調書作成時点

表 6 調書作成時点における不正

Table 6 Improprity at the time of preparing the record

不正を行う人	調書作成時点
被疑者	—
捜査官	(2) 被疑者に対して無理やり署名させる
通訳人	(3) 嘘の読み聞かせをし、被疑者の同意を取る

(2) においては、被疑者に対して無理やり署名させようとしても、通訳人が信頼できる第三者としてその場にいるので防ぐことができる。

(3) においては、通訳人は信頼できる第三者としているため、対象外とする。

4.5.4 後日

表 7 終了後における不正

Table 7 Improprity after the end

不正を行う人	終了後
被疑者	(4) そんな供述はしていないと虚偽の申告 (5) 捜査官に誘導されたと虚偽の申告
捜査官	(6) 取り調べをなかったものにする虚偽の申告
通訳人	—

(4)においては、後日被疑者が取調べにおいて供述したことはないと虚偽の申告をした場合、署名された調書から嘘を見抜くことができる。

(5)においては、被疑者が捜査官に誘導されてしまったという申告をした場合、MicroSD カードに保存されている通訳システムの情報から、虚偽の申告であるか判断することができる。

(6)においては、捜査官が取調べ自体がなかったかのような都合の悪い事実を隠蔽しようとした場合、利用申請機構により、通訳システムを利用した際は記録が残るため、仮に提出されていなかった場合に気づくことができる。

(6)は、従来のやり方では対応できなかったものである。

4.6 従来の方式との比較評価

4.6.1 目的

本稿において、追加した利用申請機構を改ざん検知機能に組み込み、通訳システムの改ざん検知機能の署名検証コストを従来の手法と比較評価する。

4.6.2 手法

利用申請情報はタイムスタンプを持つ情報として、ヒステリシス署名に組み込むものとする。本稿の改ざん検知機能を図に示す(図9参照)。

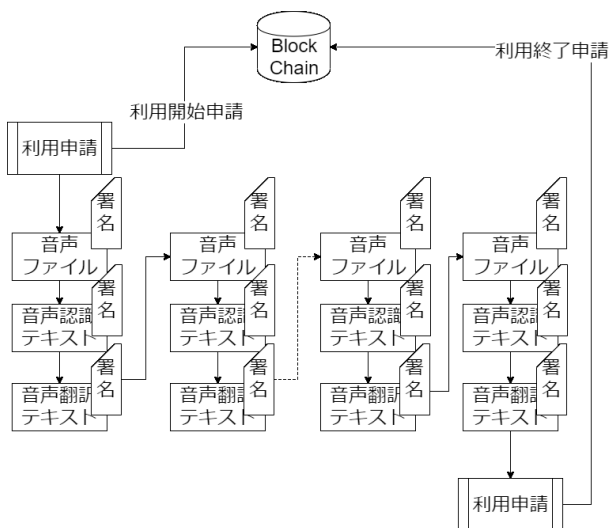


図9 利用申請情報を用いた改ざん検知方式

Figure 9 Falsification detection method using usage application information

4.6.3 比較検討

次に、従来の手法と本稿の手法を比較検討した(表8参照)。

表8 各手法の比較

Table 8 Merit and Demerit for Each Method

手法	メリット/デメリット
従来の手法	<ul style="list-style-type: none"> 全ての音声ファイルの署名情報のハッシュがブロックチェーンに紐づいている 検証に時間がかかる 第三者機関に情報を残さない

本稿の手法	<ul style="list-style-type: none"> 利用申請情報の検証が可能 検証にかかる時間が抑えられる(利用開始と利用終了のみ) 第三者機関に利用申請情報を残す
-------	--

本稿の手法は、従来の手法に比べ、第三者機関に利用申請情報を残し、また、ブロックチェーンに繋ぐ情報を利用開始申請及び利用終了申請の二つにすることができるため、署名検証にかかる時間を抑えることができる。

4.6.4 実験

全体でファイル数が30(発言数にすると10件分)のデータに対して、署名検証にかかる時間を従来の手法と比較した(図10参照)。

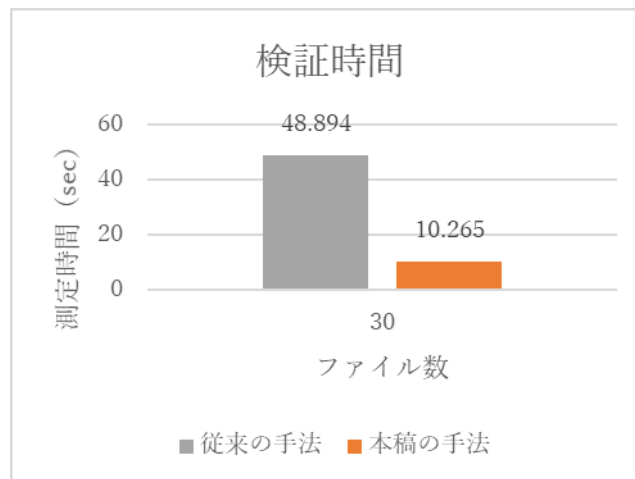


図10 検証時間

Figure 10 Computation time for Validation

本稿の手法は、従来の手法よりも署名検証にかかる時間を抑えることができることが実験によって明らかになった。

5. 評価

5.1 具体的な不正の検討

本稿において、前提条件を置いたうえで段階的に具体的な不正の検討を行った。また、通訳システムの利用を制限する仕組みを組み込むことで第三者機関に利用記録を残し、システムの濫用による不正を防ぐことができ、また、従来のやり方では対応できなかった取調べ自体の存在をなかったものにする不正にも対応できた。

5.2 改ざん検知機能

改ざん検知機能について、利用申請機構を組み込むことで不正に対応し、さらにブロックチェーンに繋ぐ数を減らすことにより署名検証時間のコストを下げる事ができた。

6. まとめ

本稿では、通訳システムの音声認識、音声翻訳機能の評価及び改ざん検知機能の改善を行った。今後は、利用申請の具体的なシステムの提案、翻訳精度が十分でない場合の訂正方法についてのさらなる調査、検討を行うとともに、本稿では対象外とした不正についての対応の検討を行って

いきたい。

参考文献

- [1] 脇田和宏, 佐々木良一, “外国人被疑者取調べにおける通訳システムのプロトタイプの開発と評価”, SCIS2020, 2020 Symposium on, Cryptography and Information Security, Kochi, Japan, Jan. 28 — 31
- [2] 高間 浩樹, 吉浦 裕, 越前 功, 佐々木 良一, “取調べの可視化における技術課題の明確化と対策提案”, 日本セキュリティ, マネジメント学会誌研究論文, 第 24 巻第 2 号, 10 pages, (2010 年 9 月).
- [3] 中口 孝雄, 大谷 雅之, 高崎 俊之, 石田 亨, “国際シンポジウムのための多言語支援システム”, 情報処理学会論文誌 Vol.58 No.1 197-204(Jan. 2017)
- [4] Google, <https://cloud.google.com/speech-to-text/docs?hl=ja>
- [5] Google, <https://cloud.google.com/translate/docs?hl=ja>
- [6] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system, ” 2008.
- [7] M.Araoz, What is Proof of existence?(2014). , <https://docs.prooffexistence.com/>
- [8] 松本 勉, 岩村 充, 佐々木 良一, 松木 武, “電子署名におけるアリバイ証明問題と経時証明問題—ヒステリシス署名とデジタル古文書の概念”, コンピュータサイエンス誌 bit, Vol.32, No.11, 共立出版 (2000)
- [9] 芦野 佑樹, 佐々木 良一, “セキュリティデバイスとヒステリシス署名を用いたデジタルフォレンジックシステムの提案と評価”, コンピュータセキュリティシンポジウム (CSS) 2006 論文集, 情報処理学会シンポジウムシリーズ, Vol. 2006, No. 11, pp. 363-368(2006).
- [10] 大上智也, 稲葉宏幸, “Ethereum のスマートコントラクトを用いた信頼性の高いカーシェアリングシステムの提案”, 研究報告電子化知的財産・社会基盤 (EIP), 2017-EIP-76, No. 7, pp. 1-4(2017).