A study on a practical measure against billing frauds

振り込め詐欺への現実的な対策についての検討

山本 匠[1,2], 加藤 岳久[1], 西垣正勝[1]

[1] 静岡大学創造科学技術大学院 〒432-8011 浜松市中区城北 3-5-1
[2] 日本学術振興会特別研究員(DC1)

あらまし 近年, 電話などを使って金銭の振り込みを要求する, 振り込め詐欺の被害が増加している. 現在までに様々な対策が検討されているものの, 確実な防止と利便性の両立に疑問が残っている. また, その多くは犯人と被害者との通話の中で機能するタイプの対策となっている. 会話が始まってしまうと, 犯人は巧妙な話術で被害者をおとしいれる. それゆえ, 犯人と被害者の通話そのものを阻止するか, または会話が始まる前に(被害者が受話器をとる時点で), 電話を掛けてきた相手の真贋を冷静かつ迅速に判断できる機能を被害者に提供する必要がある. 本稿では, 上記の要求を満たす現実的な方法を検討していく.

A study on a practical measure against billing frauds

Takumi Yamamoto[1,2] Takehisa Kato[1] and Masakatsu Nishigaki[1]

[1] Graduate School of Science and Technology, Shizuoka University,
3-5-1, Johoku, Naka, Hamamatsu, Japan

[2] Research Fellow of the Japan Society for the Promotion of Science (DC1)

Abstract Recently, the damage of a billing fraud in which a fraudster asks a victim to pay money into fraudster's bank account by using a telephone and so on, has been increased. So far, although several measures against the billing fraud have been proposed, their usability and detection accuracies are still insufficient. Moreover, most of the measures will only work during conversation between the victim and a fraudster. Once conversation starts, the fraudster can cheat the victim with cajoling words. Therefore the measure against billing frauds should have an ability to van the communication with the fraudster, or a function to allow victims to confirm the authenticity of the caller before the conversation starts. In this paper we study a measure to solve those problems in a practical manner.

1 はじめに

近年, 電話などを使って, 金銭の振り込みを要求する, 振り込め詐欺の被害が増加している[1]. 電話で「オレオレ」と身内になりすまし, 事故などで急に現金が必要になったと偽り, 特に高齢者からお金を騙し取る, 「オレオレ詐欺」が代表的な手口としてよく知られている.

警察や金融機関が顧客や市民に積極的に注意を促すなど, 官民一体となって対策に取り組んできたことで振り込め詐欺は減少傾向にあった. しかし最近になり, オレオレ詐欺の被害が増加傾向にあると言われている[2]. 平成 22 年 6 月末までの振り込め詐欺の被害額は, 約 35 億 8,929 万円(被害件数:3,235 件)にまで上っている. その内の約 7 割が, オレオレ詐欺の被害で[1], オレオレ詐欺の増加に歯止めをかけたいところである.

振り込め詐欺に対しては, 現在までのところ様々な対策が検討されているものの, 確実な防止と利便性の両立に疑問が残るというのが現状である[3-6]. 例えば, 犯人と被害者との通話の中で機能するタイプでは, 会話が始まってしまうと, 犯人の巧妙な話術で被害者がおとしいれられる危険性がある. それゆえ, 犯人と被害者の通話そのものを阻止するか, または, 会話が始まる前に(被害者が電話を受ける時点で)電話を掛けてきた相手の真贋を冷静かつ迅速に判断できる機能を被害者に提供する必要がある. 本稿では, 上記の要求を満たす現実的な方法を検討していく.

2 振り込め詐欺の手口と対策

本章では, 振り込め詐欺の代表的な手口[1]と既存対策について紹介する.

2.1　振り込め詐欺の手口

今日までに振り込め詐欺の手口は多様化し，かつ，巧妙化している．警視庁では，振り込め詐欺を大きく分けて，以下の 4 つに分類し対策を検討している．

●　オレオレ詐欺

電話を利用して息子，孫等を装い，会社でのトラブル，保証金や借金を装い，現金を預金口座に振り込ませる等の詐欺行為である．他に，警察官や弁護士等を名乗り，交通事故を装い，示談金と称して現金をだまし取る事例もある．

●　架空請求詐欺

不特定多数の人へ，有料サイトの利用料金や，架空訴訟の費用を請求する文書，メール等を送付する．そして，現金を振り込ませたり，送付させたりしてだまし取る詐欺である．

●　融資保証金詐欺

ダイレクトメール，FAX，電話等で融資を誘う．融資を申し込んだ人へ，保証金等を預金口座等に振り込ませる等，現金をだまし取る詐欺である．

●　還付金等詐欺

社会保険事務所の職員等を装った年金の還付金手続き，自治体の職員等を装った税金の還付手続きで，被害者をATMまで誘導する．そして，被害者自らにATMを操作させ，被害者の口座から現金を振り込ませる詐欺である．

2.2　対策

振り込め詐欺に対しては官民一体となった注意喚起の他に現在までのところ様々な対策が検討されている．

●　ATM 付近での携帯電話の使用の制限

ATM 付近で携帯電話の電波を検知したらATMユーザに警告を出す方式[3]や，妨害電波により携帯電話を使用不可能する方式[4]が検討されている．

しかし，犯人は ATM から離れた場所に被害者を移動させ振り込みの指示をすることで対策を無効化できる．また，通常の振込みでも携帯電話で相手と情報の確認をしながら，ATM を利用する場合もある．このため，携帯電話の利用制限はATM利用時の利便性を大きく損ねてしまう．

●　会話・通話内容から振り込み詐欺らしさを検知

日本電気(株)では，通話音声データを判定サーバに送信し，通話音声データと予め登録された詐欺師（犯人）の音声データを基に音声特徴を照合し，さらに音声データ中に含まれる口座番号（過去に振り込め詐欺に利用された口座番号）や振り込め詐欺特融のキーワードとの一致率から，ユーザに警告をする方式を提案している[5]．

また武田らは，人間行動の数理的モデルに基づく方式を提案している．この方式は，人間が行動する際に内在する「人間の状態」を理解し，人間が「過信」する状態を検出して，振り込め詐欺防止につなげる[6]．この方式では，既存方式の通話内容からのキーワードを検出することに加え，声の調子から被害者が異常な心理状態に置かれていることを警告し，通話内容を落ち着いて再考する機会を作る．

上述の会話・通話内容から振り込み詐欺らしさを検知する方式[5,6]では，検知漏れや誤検知等の検知精度が大きな課題となる．特に，電波の悪い場所や騒々しい場所など様々な環境で利用される携帯電話の通話内容から高い検知精度を実現できるかについては疑問が残る．また通常の振込みの場合，家族間であれば通話開始時に自分の名前を名乗らない（「オレ，オレ」と名乗る）人も少なくないため，詐欺特融のキーワードとの区別が困難となる．

以上から，振り込め詐欺対策の多くが確実な防止と利便性の両立に疑問が残っていることがわかる．また，犯人と被害者との通話の中で機能するタイプの方式が多く，犯人が被害者の心理を揺さぶることで対策が回避される可能性もある．それゆえ，犯人と被害者の通話そのものを阻止するか，または，通話が始まる前に（被害者が電話を受ける時点で）電話を掛けてきた相手の情報を冷静かつ迅速に分析・判断できる機能を被害者に提供する必要がある．以降では，上記の要求を満たす現実的な方法を検討していく．

本稿では，本研究の第一歩として，オレオレ詐欺，特に身内になりすますタイプの手口に焦点を当てて現実的な対策の検討を行う．

3　現実的な対策の検討

3.1　オレオレ詐欺対策への要求事項

本節では現実的なオレオレ詐欺対策に求められる要件についてまとめる．以下に著者らが考える要件を示す．

A) 利便性の低下を抑える
- (A-1) 対策の導入が通常の通話に影響を与えることを極力抑える．

B) 導入コストを抑える
- (B-1) 対策の導入時に，ユーザが新たに設定をする項目を極力少なくする．
- (B-2) 対策の導入にあたり，携帯電話通信事業者（以降　キャリアと呼ぶ）が管理するシステムや情報の増加を極力少なくする．

C) 身元不明の相手の情報を教える
- (C-1) 被害者が電話を掛けてきた相手を冷静に分析・判断するための情報や機会を与える．
- (C-2) ソーシャルエンジニアリングの隙となる，身元不明者との通話を極力阻止する．

要件 A は，新たな対策を導入することで，ATM や携帯電話の通常利用が阻害されないことを意味する．

要件 B は，新しい対策を導入することで，ユーザが新たに設定する項目があったり，キャリア等の第三者機関が管理する情報やシステムが増えたりしないことを意味する．

要件 C は，ユーザ（被害者）が身元不明の相手と通話する前に，可能な限り相手の情報を教え，ユーザが冷静になった上でその情報を分析・判断する機会を設けることである．また被害者が何の情報も無しに犯人と会話してしまうと，犯人の巧みな話術によって被害に遭う危険性が高まるため，犯人との通話そのものをできるだけ抑える．

3.2　想定システムと前提について

本研究で想定するシステムについて述べる．

●　想定システムの基本構成

想定システムは，通常の携帯電話の通信モデル（携帯電話，基地局，交換局）に加え，キャリアの管理下にコンシェルジュサーバを設置することを前提とする（図 1）．

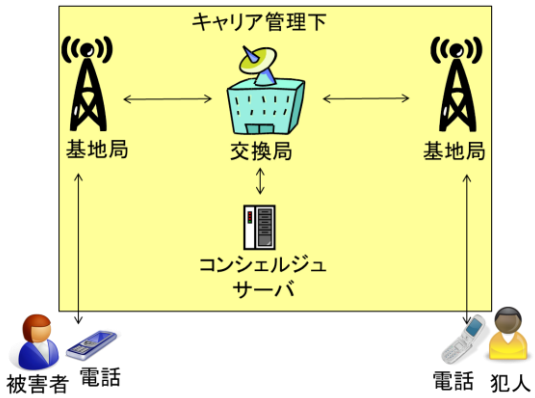

図 1　単純化した想定システムの概念図

コンシェルジュサーバは，ユーザ（被害者）に電話がつながる前に，電話を掛けてきた相手の身元確認を行い，その後，ユーザに通話の取り次ぎを行う電話交換手のような役割を持つ．なお，交換局がコンシェルジュサーバの機能を持ってもよい．

●　想定システムの基本プロトコル

本稿で想定する基本プロトコル（図 2）を説明する．なお本稿では，電話を受ける人のことを受信者，電話を掛けた人のことを発信者と呼ぶことにする．

Step 1. ユーザはあらかじめ自分の情報（今回は，家族氏名，生年月日，性別を例として説明する）をコンシェルジュサーバに登録しておく．

Step 2. 発信者は通話要求を行う．

Step 3. コンシェルジュサーバは発信者の要求を確認し，発信者に対し音声自動応答を行い，「発信者確認作業」を開始する．

Step 4. 発信者確認作業により得られた情報を元に，コンシェルジュサーバはユーザ（受信者）に通話の取り次ぎを行う．

Step 5. ユーザは与えられた情報を元に通話に応答するかを判断する

Step 6. コンシェルジュサーバはユーザからの判断に応じ，発信者に通話可能か否かを返答する．

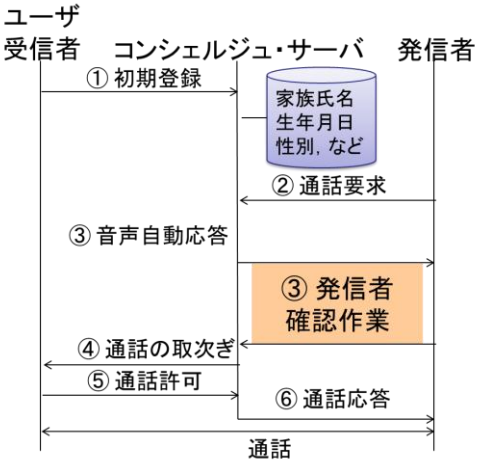

図 2　基本プロトコル

●　発信者確認作業

発信者確認作業では，コンシェルジュサーバがユーザ（受信者）に代わり発信者の身元を確認する．発信者確認の手順は以下の通りである．

Step 1. コンシェルジュサーバは発信者に対して身内かどうかを確認する．

Step 2. 発信者は電話の番号ボタンを使って質問に回答する．例えば「はい」が「1」，「いいえ」が「0」となる．

Step 3. 身内でなければ，身内以外の発信者からの電話であることをユーザに通知し，通話の取り次ぎを行う（Step. 9 に飛ぶ）．身内であるとの返答の場合は，コンシェルジュサーバは発信者に対して，性別を確認する．

Step 4. 発信者側は電話の番号ボタンを使って質問に回答する．例えば「男性」が「1」，「女性」が「0」となる．

Step 5. 続いてコンシェルジュサーバは発信者の生年月日（もしくはメールアドレス等）を確認する．

Step 6. 生年月日を確認された発信者は，電話の番号ボタンを使って生年月日を回答する．例えば「11 月 29 日」が誕生日の場合，「1129」と入力する．

Step 7. コンシェルジュサーバは入力された性別と生年月日に合致する身内が，あらかじめ登録されたデータベースの中に存在するかを確認する．

Step 8. データベースに含まれていた場合，例えば，「親族の方からお電話です．御子息の方の，性別，生年月日と一致していますので，おつなぎしますね」と，発信者の情報をユーザに通知する．一方，含まれていない場合，「親族を名乗る方からのお電話なのですが，登録されている親族の中で性別，生年月日が一致する人はいませんでした．電話を切ってもよろしいでしょうか？」と発信者の情報をユーザに伝える．

Step 9. ユーザは与えられた情報を元に通話に応答するか否かを電話の番号ボタンを使って答える．例えば「応答する」が「1」，「応答しない」が「0」となる．

Step 10. 「応答する」場合，コンシェルジュサーバはユーザと発信者の通話をつなげる．「応答しない」場合，コンシェルジュサーバは発信者に対し，「ただいま，おつなぎ出来ない状況です．ピーという発信音の後，30 秒以内のメッセージをお預かりします」と通知する．発信者はメッセージを残し，電話を切る．

コンシェルジュサーバが発信者に確認する質問や，問答の回数などはユーザの要望や環境によって適切に調整してやる必要がある．図 3 に発信者が身内の場合における確認作業の流れを示す．

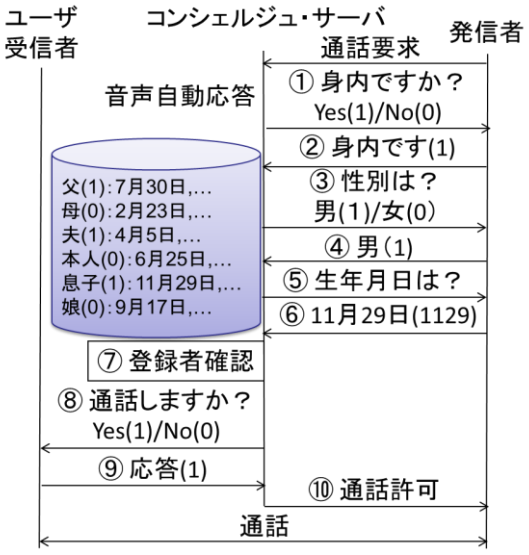

図 3 発信者確認作業のプロトコル
（受信者の息子を名乗る相手からの電話）

3.3 提案プロトコル

3.2 節の基本プロトコルでは，ユーザにかかってきた電話全てに対して，コンシェルジュサーバが身元の確認を行うため，3.1 節の要件 A（利便性の低下を抑える）を満たさない．また初期登録として，ユーザはあらかじめ自分の情報（家族氏名，生年月日，性別など）を登録しておく必要があり，3.1 節の要件 B（導入コストを抑える）を満たさない．そのため本節では上記の 2 点の改善を目的に，現実的な案を示す．

●要件 A への対応：アドレス帳バックアップサービスの利用

要件 A の問題（利便性の低下）については，携帯電話の機能であるアドレス帳を活用することが有効と考えられる．アドレス帳に登録されていない電話番号に対してのみコンシェルジュサーバを機能させることで，頻繁に電話のやり取りを行うであろう人との通話を妨げない．

ただし，アドレス帳はユーザ個々人の携帯電話の中にあるため，コンシェルジュサーバは自由にアドレス帳にアクセスすることが難しい．そのためアドレス帳そのものを利用するのではなく，キャリアが提供するアドレス帳バックアップサービス等[7]を活用する．アドレス帳バックアップサービスとコンシェルジュサーバはキャリアが管理しているものであり，キャリアの負担は少ない．

アドレス帳バックアップサービスを利用していないユーザに対しては，本サービス(振り込め詐欺対策）を受けるには事前にアドレス帳バックアップが必要であることを知らせ，バックアップを促せばよいと考えられる．

なお，ユーザが固定電話しか所有していないケースも考えられる．固定電話のみの世帯は徐々に少なくなっているものの，無視できないケースである．家族など，頻繁に掛かってくる電話番号を事前に登録してもらうことや，過去の通話履歴から頻繁に通話している電話番号をホワイトリストに登録するなどの対応が考えられる．

●要件 B への対応：既登録情報の活用

ユーザの初期登録の煩わしさを無くすためには，既に運用されているシステムから関連する情報を流用することが有効である．著者らは，キャリアが管理する携帯電話家族割引契約時の情報[8]や，近年その重要性が注目され始めている安否確認システム[9]の登録情報を活用することが有効ではないかと考える．

(a) 携帯電話の家族割引契約情報の利用

携帯電話購入時には自身の個人情報を登録する．また携帯電話の家族割引契約時には，新規契約者グループが家族なのか，または，新たにグループに追加される新規契約者が既契約グループの誰かと家族関係にあるか，既契約者の登録情報および新規契約者の身分証明書等を使った確認が一般的である[8]．すなわち家族割引契約時の登録情報（グループ情報）から，当該ユーザの身内が誰なのかを把握することが可能である．

(b) 安否確認システムの登録情報

安否確認システム[9]では，自分の情報（氏名，生年月日，学籍番号，社員番号，連絡先，住所，所属等）や，家族や知り合いの連絡先（緊急連絡先）をあらかじめ登録しておく．そして万が一の場合は，登録された緊急連絡先

等に自分の安否について通知する．安否確認システムは大学や企業の間では一般的になりつつある[9]．また，市民に安否確認情報の登録を積極的に呼びかけている地方自治体もある[10]．なお，提案方式ではキャリアが安否確認システムも運営していると仮定する．キャリア以外の企業が運営している安否確認システムとの連携も考えられるが，個人情報保護の観点からユーザにデータ共有の了承をとる必要がある．

(c) 運用形態

図 4 に提案システムの運用形態を示す．上述の家族割引契約情報および安否確認システム情報は，3.2 節の発信者確認作業における Step 4 および Step 6 にて入力された性別と生年月日の情報を検索するために利用される(図 5)．なお，ユーザならびにユーザの家族(身内)は，家族割引契約，および，安否確認システムへの登録を行っているものとする．

図 5 の例では，まず契約者 A の家族割引契約情報から家族情報(グループ情報)を取得する．家族情報から家族の連絡先がわかる．その連絡先をキーとし，既契約者である家族の個人情報を，キャリアが管理する契約者情報の DB(データベース)の中から検索することができる．

家族割引契約情報と同様に，当該ユーザの身内の連絡先をキーとして，安否確認システムの DB に登録されている身内の個人情報を検索することができる．

なお，本方式ではキャリアが安否確認システムのために取得した個人情報を別のサービス(振り込め詐欺対策)のために利用する．一般的にこのようなケースでは，各ユーザの同意が必要となる．そのため提案方式の運用開始時にはメール等で同意をとる対応が必要である．

キャリアにとってはコンシェルジュサーバ導入のコストがかかるが，3.2 節でも述べたように交換局にコンシェルジュサーバの機能を持たせることも可能だと考えられる．さらに，自動応答サービス自体は一般的に普及しているシステムであるため，提案方式の導入コストはそれほど大きくならないと考えられる．

●要件 C への対応:

提案プロトコルでは，ユーザ(受信者)と発信者が通話を開始する前に，コンシェルジュサーバが身内を名乗る相手に対し発信者確認(性別や生年月日等を尋ねる)を行う．そして，発信者が実際に身内の情報を知っているかどうかをユーザに通知した上で，通話に応じるか否かをユーザ本人に判断させている．そのため提案方式は，要件 C を満たしていると言える．

以上より，幾つかの仮定はあるが，提案方式は著者らが考える要求事項を満たしたオレオレ詐欺対策となっていると考えられる．

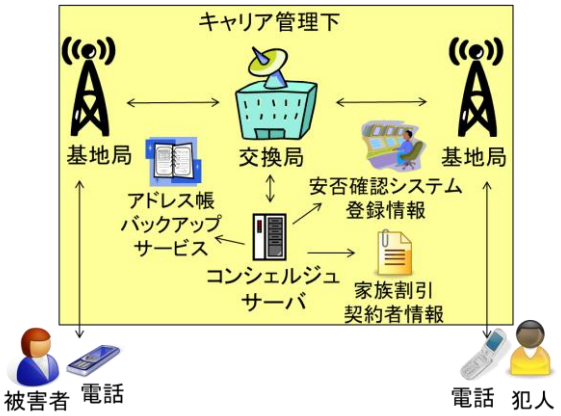

図 4 提案システムの運用形態

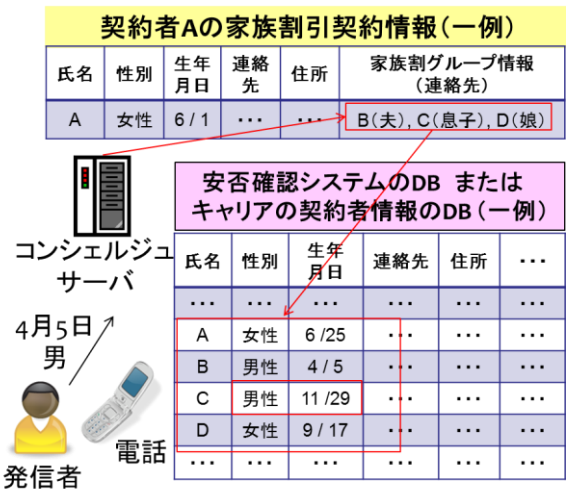

図 5 安否確認システムと携帯電話家族割引契約情報の活用形態

4 検討事項

4.1 提案方式に対する攻撃方法について

(ア) Brute-force 攻撃

本対策に対する Brute-force 攻撃とは，犯人が性別や生年月日に関する回答を変えながら何度も同じ受信者に対して電話をかけることである．本対策は，3.1 節の要件 A(利便性の低下を抑える)を満たすために，生年月日や性別といった簡素な確認を行う方式となっており，Brute-force 攻撃には比較的脆弱である．このため，ATM 等で導入されている「3 回連続で暗証番号の入力を間違えたらアカウントをロック」するといった運用を併用すべきであろう．すなわち，登録されている生年月日と性別の組を 3 回連続して誤った場合には，キャリアが当該発信端末からのそれ以降の発信を禁止する，もしくは，送信者を詐欺の被疑者として通報する．

(イ) Reverse-brute-force 攻撃

本対策に対する Reverse-brute-force 攻撃とは，犯人

が電話をかける相手についても変更しながら，性別や生年月日に関する回答を変えながら何度も電話をかけることである．本攻撃に対しては，1 つの端末から異なる複数の端末への発信および回答失敗が確認された場合，キャリアが当該発信端末からのそれ以降の発信を禁止する，もしくは，発信者を詐欺の被疑者として通報するという対策が有効であろう．ここで，このような対策が実行できる理由は，提案方式における機能モジュールをキャリア側で担っているからである．

4.2　個人情報について

提案方式では，安否確認システムの情報や携帯電話の家族割引契約者情報などを扱うため，個人情報への懸念が生じる．しかし，コンシェルジュサーバは個人情報（生年月日や性別等）の出力は行わず，発信者が入力した情報がユーザの身内の情報に含まれているか否かを判断するだけである．通話を拒否された場合に発信者が入力した情報（性別および生年月日）に合致する身内が存在しないというわずかな情報は漏れてしまうが，これらは個人を特定するに足る情報ではないため，大きな問題にはならないのではないかと考える．

4.3　オレオレ詐欺以外の振り込め詐欺

本研究では，振り込め詐欺における被害件数の割合から，身内になりすます詐欺（オレオレ詐欺）に焦点をあて対策の検討を試みた．しかし，提案方式の仕組みが一般的になれば，犯人は身内を名乗らず，別の誰か（警察や弁護士）を名乗り詐欺を働くだろう．また，架空請求詐欺，融資保証金詐欺，還付金等詐欺など，詐欺の手口も多様化している．提案方式でカバーしきれない部分に対しては，提案方式の拡張ならびに他の方式との組み合わせ等により，早急に現実的な解決策を考えていかなければならない．

5　おわりに

本稿では，近年社会問題になっている振り込め詐欺について，対策の検討を行った．特に，被害件数の多い「身内になりすますタイプの詐欺（オレオレ詐欺）」に焦点を当て検討を進めた．

本研究では犯人と被害者が通話を始める前に，被害者が身内を名乗る犯人の真贋を判断できる方式を提案した．提案方式は，ユーザとキャリアにとって「利便性の低下」ならびに「導入コスト」が極力抑えられるというメリットを有する．また，犯人がコンシェルジュサーバとのやりとりで，あきらめる可能性もある．

最後に，昨今高齢者の所在不明問題が社会問題となってきており，高齢者の生活を見守ることは社会的に求められ，ビジネスとしても成り立ってきている[11]．万が一の際には高齢の両親の安否を確認することができ，かつ，振り込め詐欺の脅威から両親を守ることができる「親孝行なサービス」として，提案方式は将来的に期待されていくと考える．

参考文献

[1] 警視庁，警察庁振り込め詐欺対策 HP，：http://www.npa.go.jp/safetylife/seianki31/1_hurikome.htm（2010 年 8 月確認）

[2] All About 専門家ニュース，振り込め詐欺被害が減少…一方でおれおれ詐欺が復活!?，http://allabout.co.jp/gm/gc/23490/（2010 年 8 月確認）

[3] CNET Japan，伊予銀行が携帯電波を感知する ATM 導入へ--振り込め詐欺対策として，http://japan.cnet.com/mobile/story/0,3800078151,20401724,00.htm（2010 年 8 月確認）

[4] Business Media 誠，ATM の近くで携帯が使えなくなる？――激増する還付金サギ，http://bizmakoto.jp/makoto/articles/0807/03/news040.html（2010 年 8 月確認）

[5] 振り込め詐欺防止システム，通話内容判定サーバ，振り込め詐欺防止方法およびプログラム，田丸伸一．公開番号：2008210085，2008 年

[6] ZDNet Japan，「今の電話，詐欺じゃない？」--富士通，名大との振り込め詐欺防止技術に関する共同研究で実証実験，http://japan.zdnet.com/news/sec/story/0,2000056194,20403547,00.htm（2010 年 8 月確認）

[7] au one アドレス帳，http://address.auone.jp/pre/（2010 年 8 月確認）

[8] ソフトバンクモバイル，ホワイト家族 24，http://mb.softbank.jp/mb/price_plan/3G/white_family/#service-contents（2010 年 8 月確認）

[9] 東北大学，安否確認システムの概要，http://www.bureau.tohoku.ac.jp/somu/saigaitaisaku/anpi-gaiyou.pdf（2010 年 8 月確認）

[10] 茨木市公式ウェブサイト，災害時の安否確認，http://www.city.ibaraki.osaka.jp/bousaikinkyu/anpi_s.html（2010 年 8 月確認）

[11] ASCII.jp，電気ポットでお年寄りの生活を見守る“みまもりほっとライン”が携帯電話と L モードに対応，象印，http://ascii.jp/elem/000/000/331/331446/（2010 年 8 月確認）