二経路多要素による本人認証方式の研究

藤井　治彦

電気通信大学大学院情報システム学研究科

博士(工学)の学位申請論文

2014 年 3 月

二経路多要素による本人認証方式の研究

博士論文審査委員会

主査　多田　好克　教授
委員　大森　匡　教授
委員　本多　弘樹　教授
委員　森田　啓義　教授
委員　鶴岡　行雄　教授
委員　古賀　久志　准教授

ABSTRACT

This research describes two-path multifactor user authentication method and outline of the commercialized system. With the spoofing of internet banking is increasing, the need for secure user authentication is increasing as well. Initially a combination of knowledge authentication and possession authentication such as one-time passwords has been recommended. However, there are problems in security and operational aspect such as initial cost of the distribution token. Two-path authentication methods using mobile phones as token, e.g., Google 2-Step, can be used to solve the operational cost problems. However, they cannot be used to prevent some security problems.

We propose three methods for solving the above-mentioned problems.

(1) One call and call back method

This method provides possession factor authentication by calling back to the one-time phone number sent by one call from the authentication server. This method can be used for any cell phone and solves the problems of other two-path authentication method like social-engineering-attack. In addition, I made a prototype of it and did the evaluation.

(2) Caller ID and voiceprint method

This method uses caller ID authentication limiting the usage in Japan. The operator send the server's phone number by mail. Once the user calls the server, it checks the Caller ID, sends the guidance of content of the transaction and checks the user's voiceprint which is registered before. This method solves token theft, man-in-the-middle-attack and so on. This method is commercialized and its outline is mentioned in the paper.

(3) SMS and voiceprint challenge-response method

This method sends oath text and one-time phone number by SMS. This method can be used in a country where the caller ID can be forged. It prevents replay attack by changing the oath text each time, and it also prevents denial by legitimate user by recording his/her oath reading.

和文概要

本論文では、インターネット上の本人認証技術の課題と解決案について提案および事業化システムの概要について議論する。近年、電話網など別の経路を通して識別符号を送信する二経路認証方式が普及してきているが、ソーシャル・エンジニアリングや盗難、マルウェア、中間者攻撃等に対する脆弱性の課題や利用者の否認などの課題があった。

提案方式では、(1)ワンコールにより毎回変わる電話番号を伝え、それにコールバックをする方式、(2)日本国内などに限定し発信者番号認証や音声ガイダンス確認、声紋判定による方式、および(3)SMS で毎回変わる電話番号を伝え、宣誓録音や声紋チャレンジレスポンスによる方式を提案し、前記課題が解決できることを示す。

目次

図目次

表目次

第1章　序章

1.1　研究の背景

インターネットバンキングへの不正アクセス事件が増加している。例えば平成 23 年度 3 月末から 11 月までの不正送金総額は 56 金融機関で 3 億円に上っている[1]。当初、米国 FFEIC*により、パスワード認証とワンタイム・パスワードや乱数表など所有物認証を組み合わせた二要素認証が推奨され[2]、日本国内においても多くの金融機関が採用した。しかし、トークンの配布コストなど経済性の課題や[3]、毎回変わる数列の入力など利便性の課題があった。また、近年、中間者攻撃に対する脆弱性も指摘されている[4]。

これらの背景には、インターネットや暗号理論の根本的な課題が関係する。インターネットはオープンなネットワークなので、盗聴やなりすましを完全に防御するのが困難である。また暗号理論では、パスワードやトークン等、識別符号(鍵)初期共有問題を、ビジネスモデルや利用者の利便性を満たしながら解決するという議論が少ない(図 1-1)。

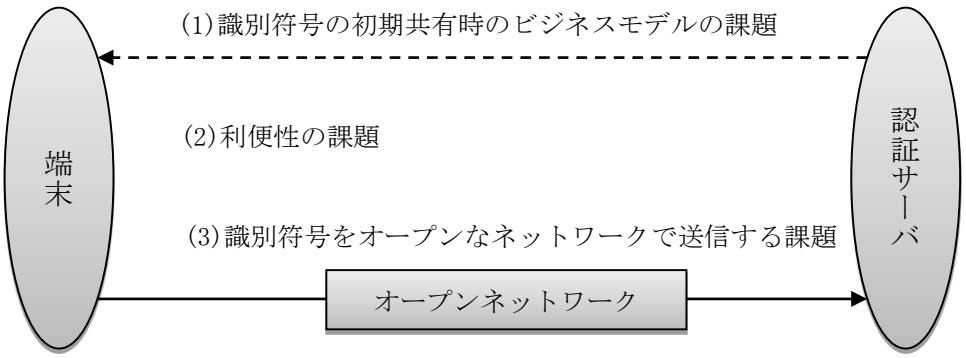


図 1-1　従来の本人認証方式の課題

*本論文の略語一覧を附表に示す。

1.2　研究の目的

本研究の目的は、安全性、経済性、利便性を兼ね備えた本人認証方式を提案することにある。本研究では、携帯電話の音声通話及び SMS の活用を提案する。本方式では、PC など利用者端末からネットワークサービス提供者側へ識別符号の伝達を必要としない。予め登録した携帯電話を利用して電話網を介してネットワークサービス提供者側に、発信者番号や SMS、声紋など送達することにより、利用者端末への本人認証を実現する方式を提案する。本方式のメリットは、すでに普及している携帯電話機をトークンとして利用でき運用面の課題を解決しながら、フィッシング攻撃や、中間者攻撃、盗難などの攻撃を防御できる点にある(図 1-2)。

なお、提案方式については、NTT セキュアプラットフォーム研究所にてプロトタイプ試作を行い、NTT ソフトウェア株式会社及び NTT コミュニケーションズにて製品化を行った。本論文では、これらの概要についても議論する。

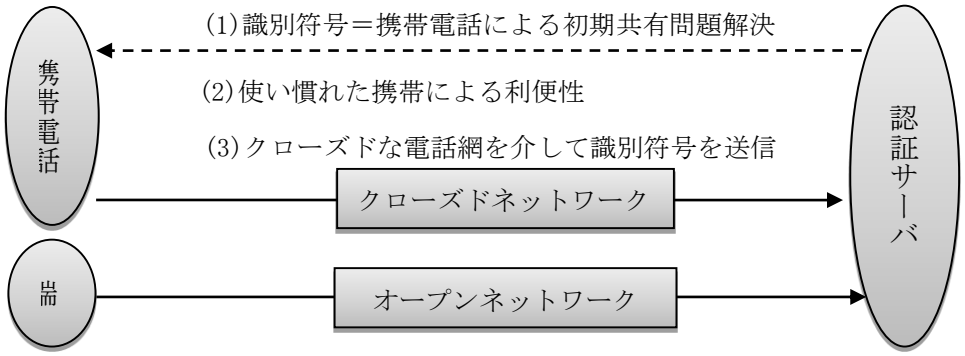


図 1-2　提案方式の原理

1.3　本論文の構成

本論文では、第２章において本人認証方式の分類と課題、及び評価方法について言及する。第３章にて類似方式のソーシャル・エンジニアリングに対する脆弱性を解決するワンコール・コールバックによる本人認証方式の提案お行い、プロトタイプの評価実験と考察について述べる。第 4 章では中間者攻撃対策等を可能とした発信者番号・音声ガイダンス・声紋認証による本人認証方式の提案を行い、システムの評価実験及び考察について述べる。第 4 章の方式は日本など発信者番号偽造対策された国でしか利用できない課題があるが、第 5 章では、これを解決し世界共通的に利用でき、リプレイ攻撃対策などを可能とした SMS・宣誓録音・声紋チャレンジレスポンスによる本人認証方式について提案と考察を行う。最後に第６章で本論文をまとめる。

第2章　本人認証方式

2.1　はじめに

本研究の対象は、一般利用者の端末上でネットワークサービスを受けるための本人認証方式である(Human to Machine)。本章では、従来の本人認証方式の分類と課題、及び評価方法について述べる。

2.2　本人認証方式の分類

本人確認技術は、本人を識別する情報の種類(識別符号)と、それを送信する経路によって分類できる。

2.2.1　識別符号の種類による分類

識別符号の種類による分類は、本人の記憶による認証、本人の所有物による認証、本人の生体情報による認証に分類可能である(表 2-1)[5]。

(1) 記憶認証

パスワード、PIN、第二パスワード、母親の旧姓などが例としてあげられる。導入は容易であるが、フィッシング攻撃などに脆弱であり、またサイトごとにパスワードを覚えたり、定期的にパスワードを変更する利便性の課題や、パスワードをサイトごとに使いまわすことにより、一つのサイトで情報漏えいが起こると、他のサイトにも影響が及ぶ課題などがある。

(2) 所有物

ワンタイム・パスワード、乱数表、IC カードなどが例として挙げられる。安全性はパスワードより向上するが、トークンの配布コストや、IC カードの場合の読取り装置を利用者端末に設置するなど、利便性と経済性の課題が存在する。

(3) 生体認証

虹彩や顔、指紋、静脈、声紋などで本人を認証する方式である。所有物認証のようにトークンを持ち歩く必要はないが、利用者端末に読み取り装置を設置する経済性と利便性の課題が存在する。

表 2-1　識別符号の種類による分類と課題

分類	長所	短所
記憶認証	導入が容易 広範囲に普及している	安全性が低い サイト毎に覚えなければならない 定期的に変更しなければいけない 大量情報漏えいするリスク
所有物認証	安全性が高い	トークンが必要 IC カードの場合、読取り装置が必要 トークンを持ち歩く必要がある トークンを盗まれるとなりすまされる
生体認証	安全性が高い トークン不要 トークンの盗難がない	読取り装置が必要 初期登録の運用面での難しさ 生体情報を盗まれると取り替えができない 誤認証、誤排除

2.2.2　識別符号を送信する経路による分類

近年のサイバー攻撃は、インターネットや、暗号理論の本質的な弱点を突く攻撃が多い。例えば、インターネットは、オープンなネットワークであるがゆえ、中間者攻撃が仕掛けられやすく、識別符号の盗聴・不正利用などを根本的に解決するのは困難である。また暗号理論では、遠隔地の不特定多数に、パスワードや秘密鍵を共有させるかについて、ビジネスモデルを満たした上での議論が少ない。

これに対し、利用者の本人確認を、電話網など比較的安全な網を介して行い、サービス提供はインターネットを用いて行う方式を二経路認証という(この点、両者を電話網のみで行う、ダイヤルアップとは異なる)。本方式は安全性を簡潔に改善できるメリットと、従来の本人認証方式で課題であった、識別符号の初期共有問題を解決する。電話会社は、携帯電話本人確認法[44]に基づいて、厳格な本人確認の後、トークンたる電話端末を利用者に手渡し、この費用は電話会社と利用者間で負担するため、セキュリティシステム側は、負担不要という点が特徴である。

二経路認証は、利用するチャネルで、さらに分類可能であり、音声通話を用いる方式、SMS を用いる方式、アプリを用いる方式に分類可能である。さらに音声通話はサーバから利用者携帯電話に電話をかけるコールバック方式と、利用者携帯電話からサーバにかける発信者番号方式に分類可能である(表 2-2)。

表 2-2　識別符号の送信経路による分類

分類			説明
一経路認証*			インターネットのみで完結
二経路認証	音声通話	発信型	認証サーバから電話機に発信
		着信型	電話機から認証サーバに発信
	SMS		認証サーバから SMS を送信
	アプリ		ブラウザフォンの JAVA アプリなどでワンタイム・パスワードを発生

*本研究では、従来のインターネットのみの本人認証方式を、一経路認証と呼ぶ。

二経路認証の課題

実用化されている二経路認証には、以下に示す安全性の課題がある。

(1) ソーシャル・エンジニアリングに対する脆弱性

ソーシャル・エンジニアリングとは、人間の心理的な隙やミスにつけこんで、秘密情報を盗むなどして、なりすます攻撃方法である。二経路認証の音声通話(発信型)方式は、ソーシャル・エンジニアリングに対する脆弱性がある[6]。攻撃者が、利用者の住所・氏名・生年月日・電話番号などを、何らかの方法で盗み出し、電話会社のオペーレーターを騙したり、もしくは転送設定の PIN を盗むなどし、サーバからの通話を攻撃者の携帯電話に転送させ、なりすませる脆弱性がある。

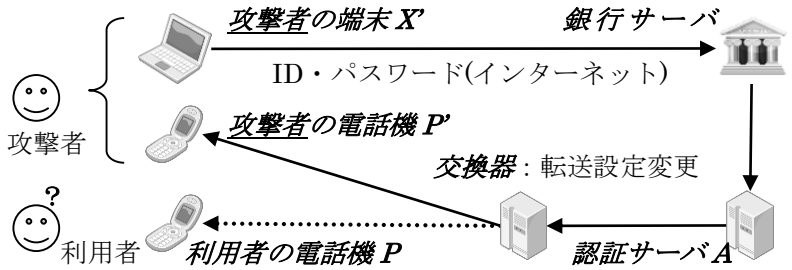


図 2-1　音声通話(発信型)方式のソーシャル・エンジニアリングに対する脆弱性

(2) 認証アプリの脆弱性

携帯電話の個体識別を送信する方式は、個体識別情報を HTTP リクエストのヘッダ情報にて送信されているに過ぎず、容易に書き換えられる課題がある[7, 8]。また認証アプリをどうやって安全にインストールするかについても課題がある。ID パスワードを用いて認証アプリにログインする方式は、この ID パスワードが盗まれると認証アプリに不正ログインできるので所有物認証の意味を成さない。

(3) SMS 遅延問題

SMS 方式は、ワンタイム・パスワードが記載された SMS が遅延する課題があった。

(4) ワンタイム・パスワードの利便性と安全性のトレードオフの課題

SMS や音声通話(発信型)方式の課題として、攻撃者がワンタイム・パスワードを受信していなくても、推測して入力できる課題がある。実用化されている方式は、利便性の

ためワンタイム・パスワードを数桁にしており、ブルートフォースアタックによる脆弱性がある。

(5) マルウェアに対する脆弱性

二経路認証特有の課題として、マルウェアにより音声通話や SMS、アプリの操作が乗っ取られるとなりすまされる課題がある。

(6) 中間者攻撃に対する脆弱性

中間者攻撃とは、例えばネットバンクの場合、攻撃者が利用者とネットバンクの間に入り、ワンタイム・パスワードなどは、そのままにし、送金先と送金額を変えてしまう攻撃方法である。攻撃者は、送金結果画面も書き換えてしまうため、利用者は攻撃を検知することができない課題がある。

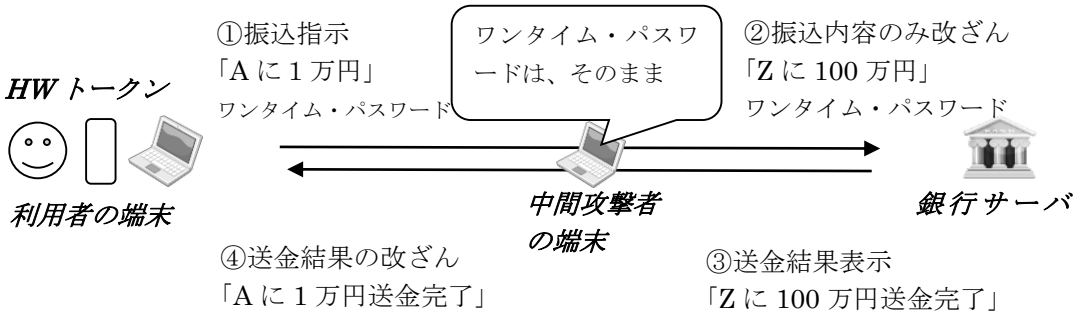


図 2-2　中間者攻撃に対する脆弱性

(7) 盗難に対する脆弱性

携帯電話や専用トークンとパスワードがセットで盗まれるとなりすまされる課題がある。

(8) PC とスマートフォンで共通方式が利用できない課題

PC とスマートフォンで異なる方式だと、運用面や利便性面上の課題が発生するため、両方に対応できる方式が望ましい。例えば、音声通話(発信型)方式の場合、スマートフォン用のサイトの認証に適用すると、スマートフォンのブラウザ利用中に電話がかかってくるため、画面遷移やセッション管理があやふやになる課題がある。

(9) 生体認証と組み合わせ時のリプレイ攻撃に対する脆弱性

携帯電話には指紋読み取り装置や、カメラがついているため生体認証を利用できる特性がる。しかし生体認証には、生体情報をコピーし不正利用されるリプレイ攻撃の課題がある。

2.3 本人認証方式の評価方法 (UDS 評価方法)

Bonneau らは、本人認証方式の評価方法を、Usability(安全性), Deployability(普及性*), Security(安全性)の 3 つのフレームワークに分類し、25 の詳細な評価項目を策定し、代表的な 35 の本人認証技術を評価した[3, 9, 附表](以降、UDS 評価方法)。近年、この評価方法を採用する研究が増えており[15, 13]、本研究でも、この評価項目に沿って評価を行う。なお、Bonneau らは、評価軸の追加及び修正提案を認めており、本研究でも提案方式の効果を明瞭にするため、評価軸の追加及び修正を行う。以下、Bonneau らの評価軸、及び本研究で追加する評価軸の概略を示す。

2.3.1 利便性(Usability)

(1) 記憶不要性 (Memorywise-Effortless)

一切、記憶しなければならない情報がないこと。一つだけ覚えていれば、あらゆる認証に利用できる場合は、準記憶不要性としている。

(2) 利用者スケーラビリティ (Scalable-for-Users)

大量のアカウントを持ったとしても、利用者が記憶しなければならないものを増えないこと。

(3) 所持物不要性 (Nothing-to-Carry)

利用者が認証専用ハードウェアや乱数表を持ち歩かなくて良いこと。携帯電話を認証ハードウェアとして利用する場合は、準所有物不要性としている。

* Deploy は「展開、配置」という意味であるが、本研究では普及という意味で利用する。

(4) 物理的操作不要性 (Physically-Effortless)

タイピングや画面のスワイプなど物理的操作が不要なこと。ただし発声など利用者の負担にならないものは準物理操作不要性としている。

(5) 操作方法の覚えやすさ (Easy-to-Learn)

操作方法を全く知らない人でも、難なく覚えられるたり、思い出せたりすること。

(6) 操作効率 (Efficient-to-Use)

毎回の認証や初期登録処理が、常識的な範囲の時間内に終わること。

(7) 認証エラーの低さ (Infrequent-Errors)

正当な利用者が、毎回、確実にログインできること。

(8) 復旧容易性 (Easy-Recovery-from-Loss)

トークンの紛失や、パスワードの失念時、例えばバックアップツールなどにより、簡便かつ遅滞なく確実に復旧できること。もし再度、申込み用紙が必要な場合は、この手続の容易性を判定する。

2.3.2 普及性(Deployability)

(1) アクセス性 (Accessible)

パスワード認証を利用できる利用者なら、例え障害や肉体的コンディションによらず利用できること。

(2) 利用者数変動費 (Negligible-Cost-per-User)

利用者及び認証サーバ側に発生する、トークンなど利用者数に応じたコストが無いこと。

(3) サーバ互換性 (Server-Compatible)

認証サーバ側の、既存のパスワード認証機構を改造不要で利用できること。

(4) ブラウザ互換性　(Browser-Compatible)

プラグインなどない標準ブラウザで利用できること。2012 年現在では、HTML5 や JavaScript 等を利用しても、これに含まれる。ただし Flash 等、標準ではないが非常に一般的なプラグインを利用する場合は、準ブラウザ互換性とする。

(5) 成熟度　(Mature)

その本人認証技術が、研究段階を終え実用化されているかどうか。

(6) 知的所有権の解放　(Non-Proprietary)

誰もが利用目的にかかわらず、ロイヤリティーの支払いなく利用できること。

(7) 携帯電話互換性　(Cellphone-or-Carrie Compatible：新規)

ニ経路認証の中には、Bluetooth を用いて PC と通信する方式など、一般的な携帯電話で利用できない方式がある。また、第 4 章で議論する方式は、発信者番号偽装対策が前提条件であり、これを区別するために新評価軸を設定する。

2.3.3　安全性(Security)

(1) 物理的観察耐性　(Resilient-to-Physical-Observation)

ショルダー・サーフィン*や、キーロガー†などにより、攻撃者に数度観察されても、なりすませないこと。

(2) 標的型なりすまし耐性　(Resilient-to-Targeted-Impersonation)

知人などが、生年月日など被害者の個人情報を全て不正利用したとしても、なりすませないこと。

(3) 制限下推測耐性　(Resilient-to-Throttled-Guessing)

サーバや耐タンパチップ等によって、リクエストの連続送信が制限された状況での推測攻撃を一定以上の安全性を担保できること。目安として、1 日 1 アカウントあたり 10 回、推測攻撃が行われたとして、1 年間に全アカウントの最大 1%しか、なりすませないこと。

---

*他人のキーボードやディスプレーを盗み見て、パスワードなどの個人情報を入手すること。
†キーボードからの入力を関しして記録するスパイウェアのこと。

(4) 無制限下推測耐性 (Resilient-to-Unthrottled-Guessing)

上記制限なく可能な限りの計算資源を利用し、ブルートフォース攻撃*等を仕掛けたとしても、一定以上の安全性を担保できること。目安として、2^{40}~2^{60}回の推測攻撃を行ったとしても、全アカウントの1%未満しか、なりすませないこと。

(5) 内部観察耐性 (Resilient-to-Internal-Observation)

マルウェア感染などにより、盗聴が10~20回程度行われても、リプレイ攻撃†ができないこと。例えTLSを用いたとしても盗聴可能とし、またPCや携帯電話など、ソフトウェアのアップデートが行われるものは、マルウェアに感染しているという前提をとる。ただし、二経路認証の場合、PCと携帯電話の、両方が同時にマルウェア感染しないと、なりすませない場合は、準内部観察耐性を有するとする。

(6) 情報漏えい耐性 (Resilient-to-Leaks-from-Other-Verifiers)

認証サーバの管理者などが情報を漏えいするなどして、他のサーバに不正ログインできないこと。

(7) フィッシング攻撃耐性 (Resilient-to-Phishing)

攻撃者が、正規のサイトになりすましパスワードなどを盗み、後でこれを利用して不正ログインできないこと。但し中間者攻撃のように、被害者と認証サーバの両方に同時にコネクションを張り、なりすますような高度なものは含まない。

(8) 盗難耐性 (Resilient-to-Theft：修正)

Bonneau らは、トークンが物理的に盗まれても、別途パスワード認証が行われていれば、なりすましを防げることとしている。パスワード認証をセットでつけることは、どの本人認証方法でも可能であり、またパスワード認証の脆弱性を考慮すると、この判断基準はあまり意味が無い。本研究では、従来の盗難耐性の基準を、準盗難耐性に格下げをし、新しい盗難耐性の基準は、パスワードとセットで盗まれたとしても、なりすましを防げることとする。

---

*暗号解読手法の一つ。考えられる全ての鍵もしくはパスワードを試すやり方。
†パスワードや暗号鍵を盗聴し、そのまま再利用して、なりすますこと。

(9) TTP 不要性　(No-Trusted-Third-Party*)

信頼出来る第三者機関(Trusted Third Party)に頼らないこと。

(10) 意思確認の確実性　(Requiring-Explicit-Consent：修正)

Bonneau らは、正当なユーザが気付かないでログイン等できないこととしており、例えばワンタイム・パスワードの送信がなされたことを持って、本人の意思確認ができるとしている。しかし中間者攻撃を想定すると、何に対する本人認証かは証明がつかない。また正当なユーザが、マルウェアに乗っ取られたと被害を詐称して、コマンドの取消や無効を主張された場合、証明する方法が無かった。電子行政や、高額商品の取引、電子投票を想定すると、この観点の評価は重要である。本研究では、従来の意思確認の基準を、準意思確認に格下げを行い、新しい意思確認の基準は、上記のような否認や中間者攻撃が行われたとしても、厳格な意思確認ができることとする。

(11) 同定不可能性　(Unlinkable)

複数の認証サーバ管理者が結託しても、同一の利用者が利用しているかどうか判明つかないこと。

(12) 中間者攻撃耐性　(Resident-to-Man-in-the-Middle-Attack：新規)

Bonneau らの示した代表的技術では、中間者攻撃に対する防衛ができるものがほとんどないため、本評価軸は追加されなかったとある[9,pp24]。しかし、今日、中間者攻撃対策ができなければネットバンクなどの不正送金は防止できない。よって本研究では、この評価軸を追加する。関連研究等

本節では関連研究及び関連製品・特許について述べる。

2.3.4　関連研究

二経路認証

携帯電話をトークンとして利用する二経路認証は、近年多く提案されている。Google などの 2Step 認証の中間者攻撃やソーシャル・エンジニアリング、盗難などに対する脆弱性の改善方法が提案されたが、日本など発信者番号の偽造対策された国でしか利用で

*信頼できる第三者機関のこと。

きない課題があった[5, 10, 11, 12, 33]。二次元バーコードを利用者端末に表示させる方式は、カメラを利用する方式は不利便性があった[13, 14]。利用者端末と携帯電話間で Bluetooth もしくは Wi-Fi を利用して通信する方式は、携帯電話の機種や利用者端末の機種の限定や、初期設定時の安全性と利便性の担保に課題があった[15, 16, 17, 18]。

三要素認証

トークンの盗難問題に対しては、生体認証を組み合わせ、三要素認証とするのが理想的であるが、特殊なハードが必要であり、運用面の課題があった[19, 20]。また生体認証特有の問題として、指紋など生体情報を不正コピーして利用される、リプレイ攻撃の課題があった。

2.3.5 関連製品及び特許

以下に、二経路認証に関連する製品及び特許を記す。

表 2-3 関連製品及び特許

分類		製品名	特許番号
音声	サーバ→携帯	KDDI WEB コミュニケーションズ Twilio [21] Google 2Step [22] サードネットワークス社 Secure Call [23] NTT コミュニケーションズ V ポータル [24]	
		Phone Factor [25]	米国 8365258
		Strike Force [26]	米国 7870599 B2
	携帯→サーバ	(第 4 章方式) NTT ソフト CallPassport [33] NTT コミュニケーションズ VoiceID [32]	日本 3497799 日本 4750765 日本 4422194
SMS		NTT データジェトロニクス認証マスターfor VPN[27] NTT メディアクロス空電プッシュ[28]	
アプリ		Softbank テレコム Synclock[29]	

2.4　本章のまとめ

本章では、本人認証方式の分類と課題点、及び評価方法について論じた。本人認証方式は、記憶認証、所有物認証、生体認証に分類でき、特に所有物認証のうち、識別符号を別の経路から送信するものを二経路認証という。これは、乱数表など、従来の所有物認証の配布コストなどを解決するが、ソーシャル・エンジニアリング、マルウェア、中間者攻撃、盗難などに対する脆弱性、認証アプリの脆弱性、SMS 遅延問題、ワンタイム・パスワードの利便性と安全性を両立できない課題、PC とスマートフォンで同一の認証方式が利用できない課題があった。また Bonneau らによる本人認証方式の評価方法についての研究も進んでおり、本研究では、これを追加修正する評価方法を採用する。

第3章　ワンコール・コールバックによる本人認証方式

3.1　はじめに

本章では、サーバからワンコールを用いて、利用者携帯電話の着信履歴にコールバック先を残し、これにコールバックすることにより本人認証を行う方式の提案、評価、及びプロトタイプによるフィージビリティの評価実験の結果を示す。

本章の方式により、2.2.2　で示した二経路認証の課題のうち、ソーシャル・エンジニアリングに対する脆弱性については、例え攻撃者に転送されても、発信者番号偽造しない限り、なりすませない。認証アプリの脆弱性及び SMS 遅延問題については、音声通話のみで実現することにより解決する。またワンタイム・パスワードを用いないことにより、安全性と利便性のトレードオフ問題も発生しない。

3.2　提案方式

本節では、前述した問題を解決する手段として、あらゆる携帯電話で利用可能なワンコール・コールバック本人認証方式を提案する。

3.2.1　目標と設計方針

本章の研究の目的は、2.2.2　で示した二経路認証の課題のうち、ソーシャル・エンジニアリングに対する脆弱性、認証アプリの脆弱性、SMS 遅延問題、ワンタイム・パスワードの安全性と利便性のトレードオフ問題を解決することにあり、次のような設計方式とする。

(1) 転送設定変更でなりすませないこと

コールバック方式のように転送設定の変更のみで、なりすませないこと。ソーシャル・エンジニアリングに対する安全性が担保できることが望ましい。

(2) 発信者番号のみに依存しないこと

本方式は、発信者番号のみに依存しないことにより、世界的に展開できることを目標とした。

(3) 音声通話のみで実現すること

認証アプリのインストール時の問題や、SMS の遅延問題を解決するため、本方式では音声通話のみで実現できることを目指す。

(4) 安全性と利便性の両立

ワンタイム・パスワードのように利便性と安全性がトレードオフの関係にならないことが望ましい。

(5) その他の利便性、普及性、利便性において、従来方式と同等もしくはそれ以上であること

安全性のみ高くなり、普及性、利便性が低いようでは、実用に適さない。

3.2.2　実現手法

前述した設計方針に従う方式として、ワンコール・コールバックによる本人認証方式を提案する。これは、認証サーバが、利用者端末から本人認証要求を受け付け、予め登録された携帯電話の番号に、ワンコールする。このとき認証サーバは、自己に割り振られた十分に多い数の電話番号のうち、ランダムに一つ選び、その番号を発信者番号としてワンコールを行う。利用者の携帯電話には、サーバからの着信履歴が残り、それに 30 秒など規定時間以内にコールバックを行う。サーバは、正しいサーバの電話番号に(着信番号)、正しい携帯電話の電話番号(発信者番号)のチェックを行い音声通話開始後、利用者端末に表示した 4 桁程度の数列のプッシュ入力を求め、正しいと本人認証完了として、利用者端末にログイン許可を与えるものである。

例えパスワードが盗まれても、その携帯電話を盗まない限りなりすませない。また例え発信者番号が偽造可能であっても、正しい電話にしかワンコールが来ないので、なりすませない。また音声通話しか利用しないので全ての携帯電話で対応可能であり、読み取り装置なども不要であり、また操作も非常にシンプルである。

3.2.3　システムの構成と役割

提案システムの構成と役割について述べる。

(1) 認証サーバ

インターネットもしくは VPN を介して接続され、利用者携帯電話とは電話網を介して接続されている。予め十分な数の電話番号が割り振られており、そのうち一つを選んで発信する機能をもち、着信があると、どの電話番号から(発信者番号)どの番号へ(着信番号)の通話かを判定する機能、及び通話時のプッシュボタン(DTMF*)入力判定機能等がある。

(2) サービス提供サーバ

ネットバンクなど、利用者端末にサービスを提供するプロバイダ。Web アプリケーションサーバが代表例となる。本研究では音声通話を扱う認証サーバと、ネットバンクなどサービス提供サーバを分離することにより、個々のサービス提供サーバが電話線を扱わないで済むように設計をした。

(3) 利用者端末

PC やスマートパッドなど任意の端末。インターネット接続機能を持ち、一般的な WEB ブラウザがインストールされている。

(4) 利用者携帯電話

一般的な携帯電話。音声通話機能、通話履歴表示機能、発信者番号通知機能、DTMF 送信機能などを持つ。これらの機能があれば、固定電話、ビジネスフォン、フィチャーフォン、スマートフォン、PHS などであってもよい。

*プッシュ方式の電話機などで、ボタンを押すたびに発信される音。プッシュ音、トーン信号と呼ばれることもある。

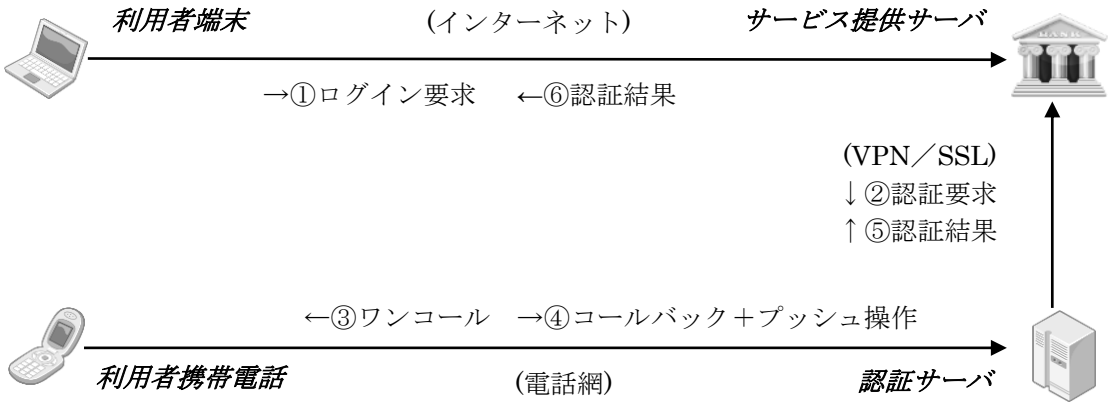


図 3-1　システム構成と役割

3.2.4　初期設定

利用者は　、サービス提供サーバに ID、パスワード、電話番号の登録を行う。

3.2.5　認証手順

認証手順の例と具体的処理は次の通りである。

① 利用者の認証が必要な処理の要求。この時、利用者端末の画面には 4 桁程度のセッション番号が表示される。

② サービス提供サーバから、認証サーバに対しての認証リクエスト送信。認証リクエストには、利用者の電話番号、セッション番号、タイムアウト時間などが含まれる。

③ 認証サーバが利用者携帯電話にワンコールし着信履歴を残す。

④ 利用者が利用者携帯電話を操作しコールバック。セッション番号をプッシュボタンで入力する。

⑤ 認証サーバからサービス提供サーバに対して認証結果通知。

⑥ 認証サーバから利用者端末へ結果送信。

図 3-2　着信履歴の様子

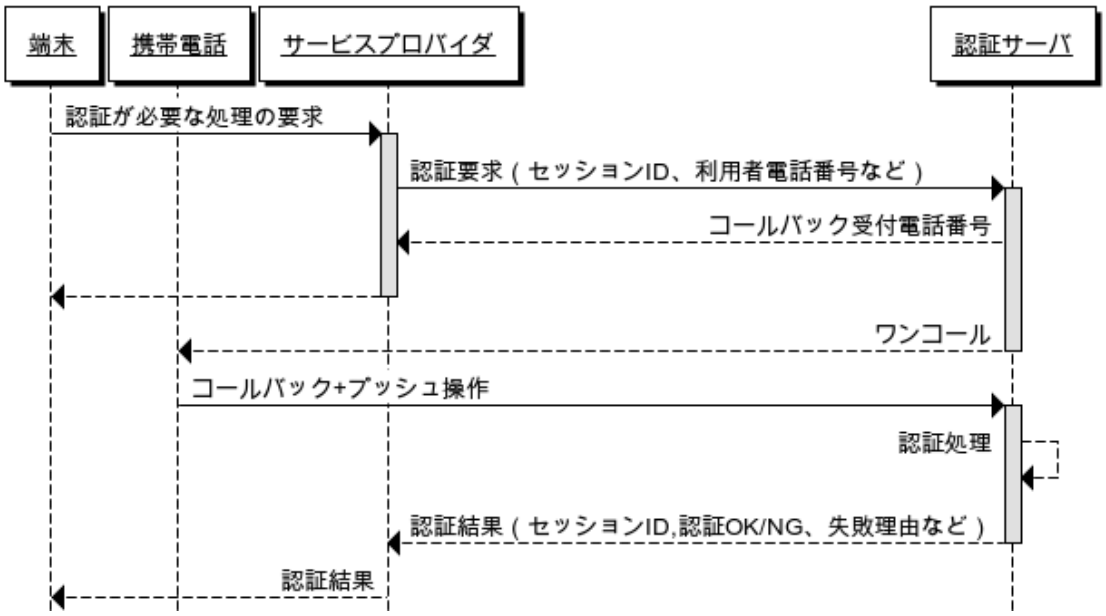

端末
携帯電話
サービスプロバイダ
認証サーバ
認証が必要な処理の要求
認証要求（セッションID、利用者電話番号など）
コールバック受付電話番号
ワンコール
コールバック+プッシュ操作
認証処理
認証結果（セッションID,認証OK/NG、失敗理由など）
認証結果

図 3-3　シーケンス図

3.3　プロトタイプの試作と評価

3.3.1　　目的

ワンコールの実現方法や冗長化方式、性能評価など提案方式のフィージビリティ検証のためプロトタイプの試作と評価実験を行った。

3.3.2　　概要

(1) システム構成の概要

図 3-4 にプロトタイプのシステム構成を示す。安定性を向上させるため冗長構成とした。また電話回線を両サーバで共有することにより、サーバ及び電話回線数を自由に設定できるようにした。コールバックの割り振りはラウンドロビンとしたため、片方のサーバが発したワンコールに対するコールバックが、もう片方のサーバにくる可能性があるため、共有 DB でセッションを管理し、これに対応できるようにした。Asterisk(IVR*)、Linux(OS)、PostgreSQL(DB)など OSS†により実装コストを抑えた。

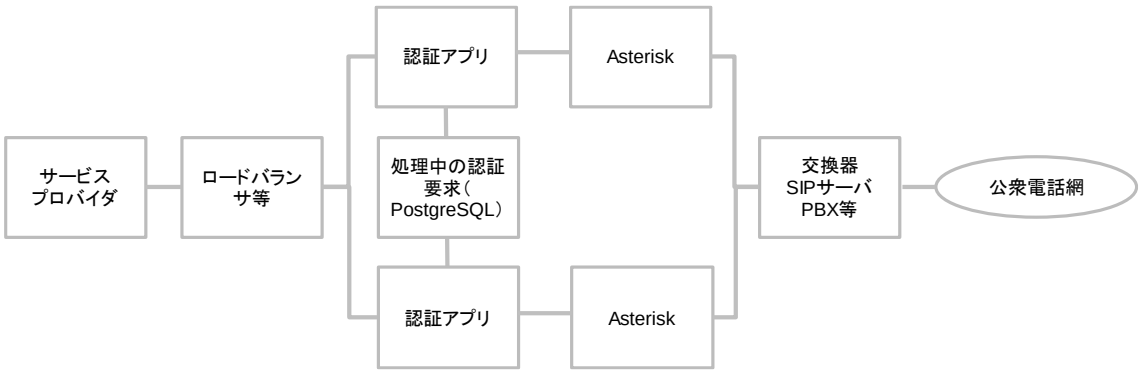


図 3-4　システムの構成と概要

*音声通話の自動応答を行うコンピュータシステム。
†ソースコードを、インターネットなどを通じて無償で公開し、誰でもそのソフトウェアの改良、再配布が行えるソフトウェア。

(2) アーキテクチャの概要

図 3-5 にアーキテクチャの概要を示す。上段のモジュールはワンコールを行い、下段のモジュールはコールバックを受ける。図 3-4 の上段と下段の物理サーバは、上下モジュールの両方の役割を行う。図 3-5 上段モジュールは、サービス・プロバイダより認証要求を受け、認証要求ストアに、要求 ID、利用者電話番号、コールバック先などを記録した後、Asterisk に対して、ワンコールを指示する。利用者の携帯電話には、毎回変わるコールバック先電話番号からの着信履歴が残り、これにコールバックを行うと、下段モジュールが着信応答を行う。認証要求ストアを参照し、着信番号、発信者番号の組み合わせが正しいかなどの判定を行い、サービス・プロバイダに認証結果を返す。

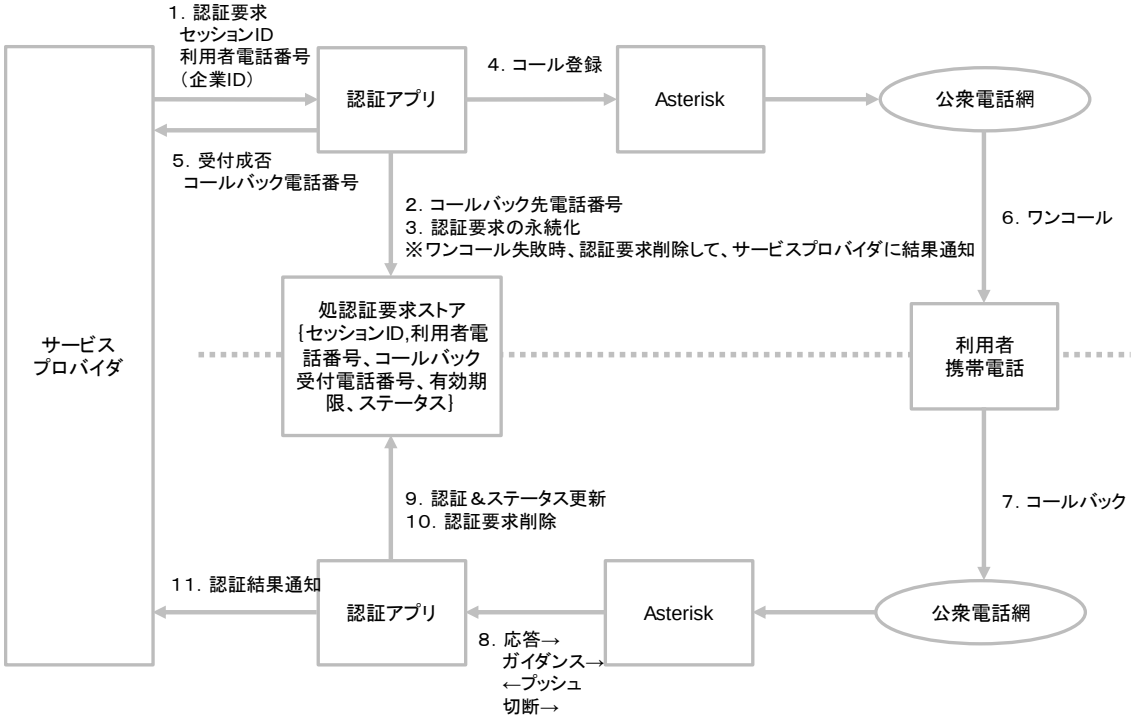


図 3-5　アーキテクチャの概要

(3) ワンコール実現方法

図 3-6 にワンコールの実現方法のシーケンスを示す。Asterisk に対してコール要求を行い、Asterisk から SIP*の Ringing イベントを検知したら、切断することにより、ワンコールの実現を行った。コールタスクはセッション ID、利用者携帯電話番号、発信者電話番号(コールバック先。本例ではフリーダイヤルを複数充てた)を受け付けると、Asterisk に対してコール要求を行う。Asterisk は架電を開始し公衆網から呼び出し音を検知すると、コールタスクに対して Ringing イベントを返す。コールタスクは、これを検知すると切断信号を送信し、架電操作を終了させることにより、ワンコールを実現する。

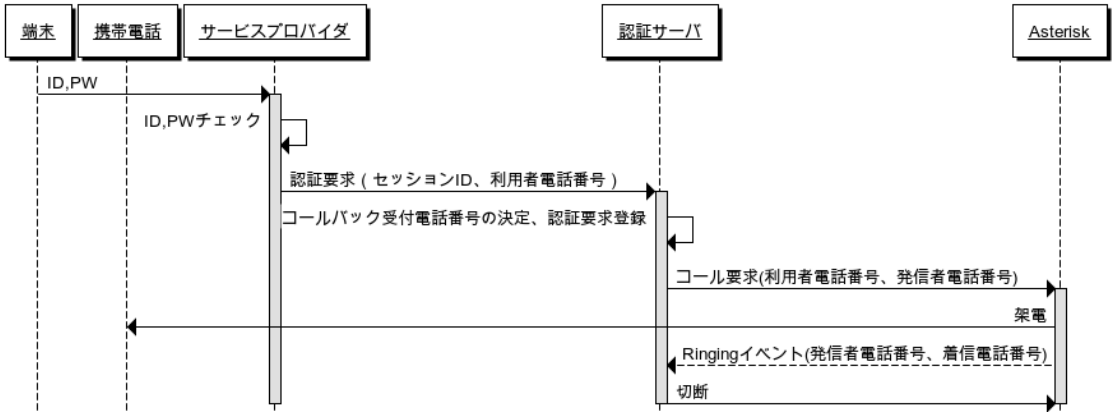


図 3-6　ワンコール実現方法

* VoIP を応用したインターネット電話などで用いられる、通話制御プロトコルの一つ。

3.3.3　性能評価実験

(1) 目的

本検証は、プロトタイプ版アプリケーションに負荷を掛けた際のシステムの挙動を確認することにより、システム全体の限界性能を見極める事を目的として実施した。そのため、一般的な Web システムでの負荷検証とは異なり、スループットには着目せず、システムのリソースの使用率を中心に計測を実施した。また、本検証では利用者によるサービス・プロバイダへの WEB アクセスは模擬せず、サービス・プロバイダから認証サーバへのリクエストを同時に行うことにより負荷試験を実施した

(2) システム構成

本検証の論理構成を図 3-7 に示す。

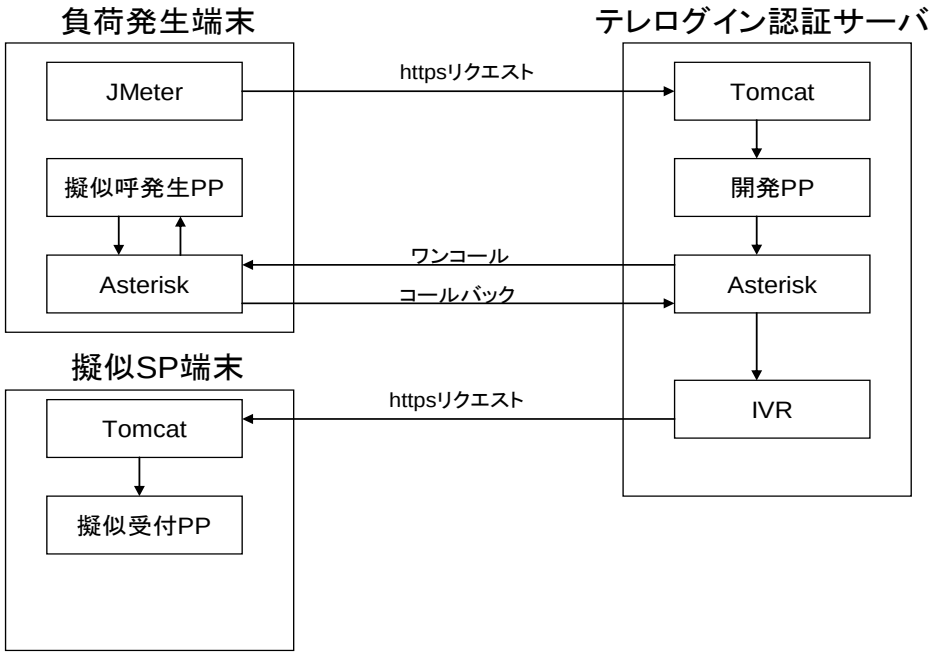


図 3-7　システム構成

表 3-1　ハードウェア諸元表

マシン	機種名	CPU	メモリ
認証サーバ	HP Proliant DL360 G5	Intel Xeon X5355 2.66G	4.0GB
擬似 SP 端末	HP Proliant DL360 G5	Intel Xeon X5355 2.66G	4.0GB
負荷発生端末	HP Proliant DL360 G5	Intel Xeon X5355 2.66G	4.0GB

表 3-2　ソフトウェア諸元表

マシン	OS	使用ソフトウェア
認証サーバ	RedHat Enterprise Linux　ES4	Tomcat5.5.23 認証サーバ PP 群 PostgreSQL8.1 Asterisk1.2.18 Fastagi-Server
擬似 SP 端末	RedHat Enterprise Linux　ES4	Tomcat5.5.23 擬似受付 PP
負荷発生端末	RedHat Enterprise Linux　ES4	JMeter2.2 Asterisk1.2.18 擬似呼発生 PP

(3) 試験ツール

- **WEB 負荷ツール(JMeter*)**

サービス・プロバイダから認証サーバへの HTTPS リクエストをエミュレートする。

- **仮想利用者端末**

本検証では、認証サーバからのワンコールを仮想的に受付ける端末を Asterisk 用いてエミュレートした。

- **擬似呼発生モジュール**

認証サーバから仮想利用者端末へのワンコールを検知して、認証サーバへのコールバックをエミュレートする。

- **擬似 SP 端末**

認証サーバからの HTTPS リクエストを受付けるサービス・プロバイダサーバを、Tomcat†と検証用モジュールを用いてエミュレートした。

- **リソース監視ツール sar‡**

サーバのリソース使用率を取得するために、sar を使用する。情報収集は試験パターンの実行前に開始し、実行完了後に終了する。

(4) 試験仕様

性能検証の基本的な仕様を下表に示す。

表 3-3　性能検証基本仕様

項目	値
負荷継続時間(試験時間)	20 分
負荷量	同時 3、6、9、12 接続
コールバック受付通知方法	ワンコール
利用者携帯電話番号	JMeter にて生成
コールバック受付電話番号	20 個
DTMF(数列)	擬似呼発生モジュールにて生成(固定数列)

負荷量

1 時間あたり 10000 アクセス

10000(アクセス)÷3600(秒)　=　2.78/s

1 秒間のアクセス数は 3 とする。

---

* Apache ソフトウェア財団にて開発されている、クライアント・サーバシステムのパフォーマンス測定および負荷テストを行う Java アプリケーション。

†Java Servlet や Java Server Pages (JSP) を実行するためのサーブレットコンテナ(サーブレットエンジン)。

‡CPU やネットワーク、メモリ、ディスクなどのシステム情報を確認・出力できるコマンド。

(5) 擬似呼発生モジュール仕様

擬似呼発生モジュールはワンコールの度に、Asterisk によって起動される。コールバックまでの待機時間は、5～35 秒とし重み付けに従って待機して、コールバックを実施する。コールバック後、認証サーバからのアナウンスを聞く時間は、1～35 秒とし重み付けに従って待機し、プッシュボタン操作(DTMF 送信)を行う。なお、送信する数列は固定値となるため、認証の結果としては失敗するが、失敗を判定するのはサービス・プロバイダとなるため、認証サーバが行う処理には影響しない。

表 3-4　ワンコール後の待機時間

ワンコール着信後の待機時間						
待機時間	5 秒	10 秒	15 秒	20 秒	25 秒	35 秒*
割合	80%	10%	3%	3%	3%	1%

表 3-5　アナウンス待機時間

アナウンス待機時間						
待機時間	1 秒	5 秒	10 秒	15 秒	25 秒	35 秒†
割合	10%	50%	30%	5%	4%	1%

※試験環境ではネットワーク遅延が発生しないため、待機時間は実際のコールバックの動作を行う時よりも時間を多めに見積もっている。

*認証サーバでは 30 秒間コールバックがない認証要求を削除するため、35 秒後のコールバックは失敗する。

†認証サーバではコールバック後、30 秒経っても 4 桁の数列が入力されない際は、タイムアウトして接続を切断する。

(6) 試験実施手順

試験の実施手順を以下に示す。

① 負荷発生端末、認証サーバの CPU、メモリ等の各種リソースを安定状態に保つ。

② 認証サーバにて sar によるリソース監視を開始する。

③ 負荷発生端末から HTTPS 負荷スレッドを 3 として、JMeter を起動する。スレッドの起動は 1 秒以内に完了させる。負荷発生時間は 20 分とする。

④ 測定時間経過後、sar によるリソース監視を停止、測定結果を退避する。

⑤ 認証サーバを再起動する。

HTTPS 負荷スレッドを 3 スレッド増加して、①～⑥を繰り返す。スレッドの最大数は 12 までとする。

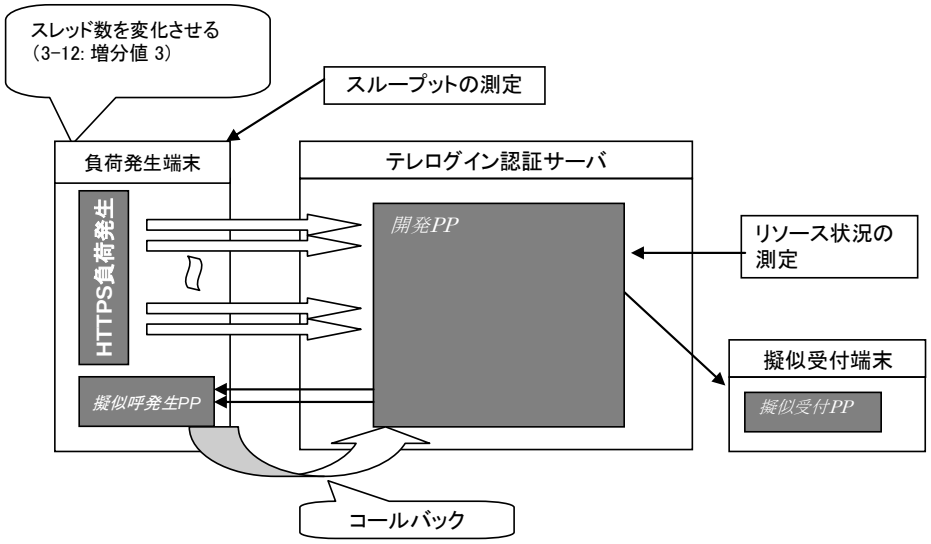


図 3-8　性能検証概念図

(7) CPU 使用率

CPU 使用率を図 3-9 に示す。

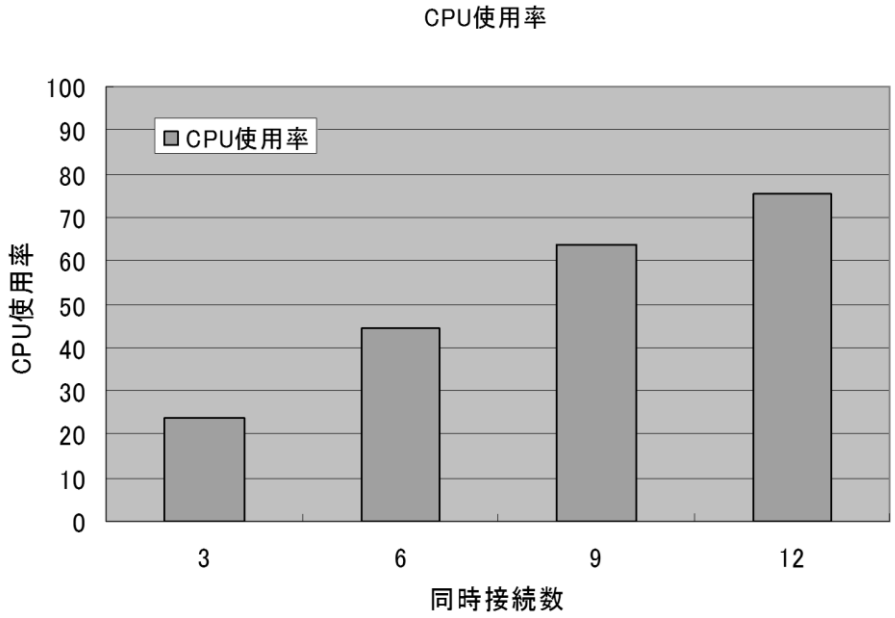


図 3-9　CPU 使用率

(8) 結論

同時 3 接続の負荷は、1 時間あたり 1 万人のユーザが接続することを想定した際の値*である。CPU 使用率は 23%であり、同時 3 接続では十分リソースに余裕があることが伺える。同時 6、9、12 接続と負荷を増やすごとに CPU 使用率も単調増加を続けているため、適切に負荷が掛かっていると言える。

同時 12 接続(4 万ユーザ/時間)においても CPU 使用率は限界値を示していないが、コールバックに失敗する事象が発生した。この現象として IVR と DB の接続数が増加し、IVR 側の設定によるタイムアウトが原因と推定される。

(9) 負荷への耐性について

運用要件にもよるが、本検証環境で実運用を行うのであれば、サービスプロバイダサイトへのアクセスが 1 時間あたり 20000 アクセス程度(認証サーバへの同時接続 6)であれば適用可能であると考える。

それ以上のアクセスがあるサイトでは、アプリケーションサーバと IVR サーバを別々のサーバで運用することを検討する必要がある。

*10000(人)÷3600(秒)＝2.78

3.3.4　輻輳と電話回線数

本方式は通常の WEB システムと異なり、電話回線を用いるため、輻輳を考慮する必要がある。電話回線を利用するのは、図 3-10 のフェーズ１のワンコール部分と、フェーズ３コールバック部分である。

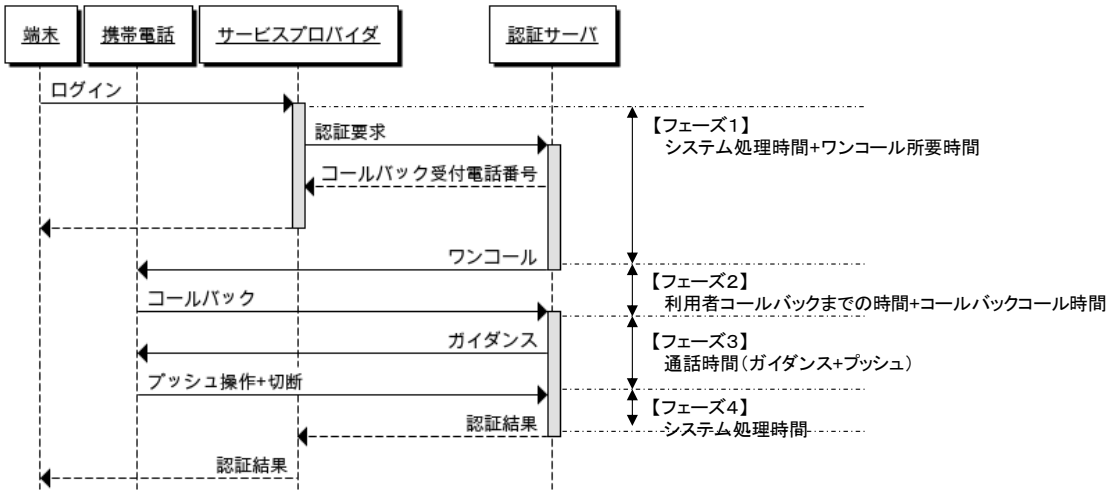


図 3-10　処理シーケンスと処理時間

(1) ワンコール

ワンコールについては、回線を占有する時間が短いため、必要な回線数に影響をほとんど与えないと考えてよい。

(2) コールバック

コールバックは、回線数に影響を与えるため、通話時間に含まれるガイダンスの時間について考慮する必要がある。単位時間当たりのコールバック数を C [件/秒]、1 コールバックの通話時間を t_3 [秒]とすると、必要な回線数は単純に計算すると、通話時間に比例し $C \times t_3$ となる。なお、正確にはアーラン B 式を用いた見積りを行うべきである。

3.4　考察

本節では、設計方針に対する達成度の考察と、第二章で定義した UDS 評価を行った後、新たな課題の抽出を行う。

3.4.1　設計方針に対する達成度

本節では設計方針に対する達成度について考察を行う。

(1) 転送設定変更でなりすませないこと

攻撃者が ID 盗難及び転送設定変更を行い、ワンコールを攻撃者の携帯電話にかけさせたとしても、コールバック時、サーバに通知されるのは、攻撃者の発信者番号なので、なりすましは防御できる。

(2) 発信者番号のみに依存しないこと

コールバック先は利用者の携帯電話にしか通知されないので、攻撃者が例え発信者番号偽造可能であったとしても、正しいコールバック先に電話することができないので、なりすましを防御できる。

(3) 音声通話のみで実現すること

ワンコール、コールバックともに音声通話のみで実現し、SMS 遅延問題は発生しない。また、認証アプリのインストールが不要なので、携帯電話の紛失、盗難、機種変更により、携帯電話端末が変わったとしても操作が不要である。

(4) 安全性と利便性の両立

本方式ではセッション番号は、短くても安全性に影響をさほど与えない。攻撃者にセッション番号を推測されたとしても、それを正当な携帯電話からプッシュされる必要があるからである。これに対し、SMS 方式などのワンタイム・パスワードは十分に長い必要がある。ワンタイム・パスワードは SMS で送信されるだけなので、利用者の電話操作不要である。よって攻撃者が推測さえできれば、あとは攻撃者の PC に入力するだけなので、ワンタイム・パスワードの推測は十分に長い必要があり、利便性と両立ができない課題がある。

(5) その他の利便性、普及性、利便性において、従来方式と同等もしくはそれ以上であること

後述の UDS 評価で考察を行う。

3.4.2 UDS 評価

本節では、第 2 章で示し UDS 評価方法にて評価を行う。

利便性(Usability)

(1) 記憶不要性 (Memorywise-Effortless)

本方式は一切記憶認証を排除しているため、攻撃者が利用者端末に正当な利用者の ID を入力し、利用者の携帯電話にワンコールを発生させることを防げない。しかし、利用者が騙されてコールバックを行なっても、攻撃者の画面に表示されているセッション番号を知ることができないので、不正アクセスは防がれる。よってパスワード認証を不要とできるので、本評価項目を満たすと言える。

(2) 利用者スケーラビリティ (Scalable-for-Users)

本方式はパスワード認証が不要であるので、本評価項目を満たすといえる。

(3) 所持物不要性 (Nothing-to-Carry)

本方式は携帯電話のみ持ち歩けばよいので、準所有物不要性を満たすと言える。

(4) 物理的操作不要性 (Physically-Effortless)

本方式はコールバックする部分は提携作業であるが、セッション番号をプッシュする必要がある。よって本評価項目は部分的に満たすと言える。

(5) 操作方法の覚えやすさ (Easy-to-Learn)

本方式は着信履歴にコールバックし、利用者端末に表示されたワンタイム・パスワードをプッシュするだけなので、操作が簡単といえる。よって本評価項目を満たすと言える。

(6) 操作効率 (Efficient-to-Use)

本方式では、遅延の可能性がある SMS を用いず、リアルタイム性の保証された音声通話により、改善はされたものの、多少の操作時間が発生するので、本評価項目は部分的に満たすと言える。

(7) 認証エラーの低さ (Infrequent-Errors)

本評価項目はセッション番号の入力失敗や、生体認証の読み取りエラーのように、利用者の正当なログインが失敗する可能性についてである。本方式はセッション番号の入力があるため、本評価項目を部分的に満たすと言える。

(8) 復旧容易性 (Easy-Recovery-from-Loss)

本方式の場合、携帯電話に認証アプリのインストールなどが不要なため、携帯電話を無くしたとしても、携帯電話ショップに行けば復活できる。ただし携帯電話ショップに行く手間はあるので、本評価項目を部分的に満たすと言える。

普及性(Deployability)

(1) アクセス性 (Accessible)

盲目の方であっても、音声通話を利用でき、また、盲目の方は利用者端末に音声読上げソフトを導入していることを考慮すると、本評価項目は部分的に満たすといえる。

(2) 利用者数変動費 (Negligible-Cost-per-User)

本方式はトークンや読み取り装置の配布コストは無いものの、通話料金が発生する。よって、本評価項目は満たさないと言える。ただし、プッシュ操作を廃止し、ワンコール及びコールバックを共に不完了呼*にした場合、通話料金はゼロとなるが、利用する電話会社が、これを許容する必要がある。コールバック先を着信課金番号†とし、通話料金のボリュームディスカウントを適用し、全体のコストを押さえる方法もある。この方法のメリットは利用者側を無料にすることができ、SMS 方式のように利用者が通信費を負担しなければならないのに比べ、事業優位性が確保できる。

*着信応答前に通話を終了させるもの。
†通話料金を着信者が全て負担する電話番号。

(3) サーバ互換性　(Server-Compatible)

本方式は改造が必要なので、本評価項目を満たさない。

(4) ブラウザ互換性　(Browser-Compatible)

本方式は、利用者端末側に一切、追加ハードウェアやソフトウェアを必要としない。よって本評価項目を満たすと言える。

(5) 成熟度　(Mature)

本方式は研究段階にあるものの、性能試験などを行なっているので、部分的に満たすとした。

(6) 知的所有権の解放　(Non-Proprietary)

本方式は日本電信電話株式会社が保有する特許に基づく方式なので、本評価項目を満たさない。

(7) 携帯電話互換性　(Cellphone-or-Carrie Compatible：新規)

本方式は音声通話しか利用しておらず、また、発信者番号偽造対策が必須条件ではない。よって本評価項目を満たすといえる。

安全性(Security)

(1) 物理的観察耐性　(Resilient-to-Physical-Observation)

本方式の場合、ID 及びセッション番号を盗み見ることが可能であるが、セッション番号は毎回代わるので、それを別のセッションで再利用することはできない。よって本評価項目を満たすと言える。

(2) 標的型なりすまし耐性　(Resilient-to-Targeted-Impersonation)

攻撃者が電話会社オペーレーターを騙すに十分な個人情報(住所、氏名)を伝え、転送設定を不正変更できても、なりすますには、発信者番号偽装を同時に行わなければならない。両方を同時に行うのは、単発で行うより困難である。よって、本論文では、本評価項目を部分的に満たすとした。

(3) 制限下推測耐性　(Resilient-to-Throttled-Guessing)

本方式は、携帯電話を持っていないと利用できないので、連続してトライアンドエラーをすることができない。よって本評価項目を満たす。

(4) 無制限下推測耐性　(Resilient-to-Unthrottled-Guessing)

本方式はブルートフォースが不可能なので本評価項目を満たすと言える。

(5) 内部観察耐性　(Resilient-to-Internal-Observation)

本方式では、例えコールバック先やワンタイム・パスワードを盗んだとしても、発信者番号をなりすまして送信を同時にしないと、成りすませない。しかしマルウェアが音声通話をのっとると、なりしましが可能である。よって、本評価項目を部分的に満たす。

(6) 情報漏えい耐性　(Resilient-to-Leaks-from-Other-Verifiers)

本方式では例え、電話番号が盗まれたとしても、単純にそれを利用することができない。よって本評価項目を満たすと言える。

(7) フィッシング攻撃耐性　(Resilient-to-Phishing)

本方式では、利用者が騙されてフィッシングサイトに誘導され、ID を盗まれたとしても、攻撃者は、利用者の携帯電話を盗まない限り、なりすますことができない。よって本評価項目を満たす。

(8) 盗難耐性　(Resilient-to-Theft：修正)

携帯電話が盗まれると、なりすますことができる。よって本評価項目は満たさない。

(9) TTP 不要性　(No-Trusted-Third-Party)

本方式は携帯電話会社が TTP である必要があるので本評価項目を満たさない。

(10) 意思確認の確実性　(Requiring-Explicit-Consent：修正)

本方式は不意の本人認証は防御できるものの、利用者の否認や中間者攻撃時の厳格な意思確認までは防げない。よって本評価項目を部分的に満たす。

(11) 同定不可能性　(Unlinkable)

安全性よりはプライバシー保護の観点の評価項目である、本方式は、電話番号で利用者を特定できるので、本評価項目を満たさない。

(12) 中間者攻撃耐性　(Resident-to-Man-in-the-Middle-Attack：新規)

本方式は提案方式では、従来方式同様、中間者攻撃は防げない。ネットバンクを例にとって説明を行うと、利用者が利用者端末から送金額、送金先等を送信する。攻撃者はこれを受け取り、サービス提供サーバ(ネットバンク)に、送金額、送金先を変更して送信を行う。サービス提供サーバから認証要求を受けた認証サーバは、利用者携帯電話にワンコールを行う。利用者は利用者端末のセッションと信じてしまい、コールバックを行い、認証サーバはサービス提供サーバに対して、認証成功を返し、攻撃者の口座に資金移動が行われる。この取引結果を記した結果画面も攻撃者が書き換えるので利用者は攻撃に気がつくことはない。このように中間者攻撃に対する脆弱性が存在する。

表 3-6　UDS 評価

Scheme	利便性(Usability)								普及性(Deployability)								安全性(Security)											
	記憶不要性 (Memorywise-Effortless)	利用者スケーラビリティ (Scalable-for-Users)	所持物不要性 (Nothing-to-Carry)	物理的操作不要性 (Physically-Effortless)	操作方法の覚えやすさ (Easy-to-Learn)	操作効率 (Efficient-to-Use)	認証エラーの低さ (Infrequent-Errors)	復旧容易性 (Easy-Recovery-from-Loss)	アクセス性 (Accessible)	利用者数変動費 (Negligible-Cost-per-User)	サーバ互換性 (Server-Compatible)	ブラウザ互換性 (Browser-Compatible)	成熟度 (Mature)	知的所有権の解放 (Non-Proprietary)	**携帯電話互換性 (Cellphone-or-Carrie Compatible：新規)**		物理的観察耐性 (Resilient-to-Physical-Observation)	標的型なりすまし耐性 (Resilient-to-Targeted-Impersonation)	制限下推測耐性 (Resilient-to-Throttled-Guessing)	無制限下推測耐性 (Resilient-to-Unthrottled-Guessing)	内部観察耐性 (Resilient-to-Internal-Observation)	情報漏えい耐性 (Resilient-to-Leaks-from-Other-Verifiers)	フィッシング攻撃耐性 (Resilient-to-Phishing)	**盗難耐性 (Resilient-to-Theft：修正)**	TTP 不要性 (No-Trusted-Third-Party)	**意思確認の確実性 (Requiring-Explicit-Consent：修正)**	同定不可能性 (Unlinkable)	**中間者攻撃耐性 (Resident-to-Man-in-the-Middle-Attack：新規)**
本章方式	●	●	△	△	●	△	△	△	△			●	△		●		●	△	●	●	△	●	●			△		
OTP over SMS	●	●	△		●		△	△	△			●	●	●	△		●	●	●	●	△	●	●		‡	△	*	
Google 2-Step			△		●	△	△	△	△			●	●		●		△	†	●	●		●	●		‡	△		

※　●は評価項目を満たす。△は部分的に満たすことを示す。空欄は満たさないことを示す。
※　灰色太字は、追加修正事項。

*Bonneau らは本評価項目を満たすとしているが、電話番号により同定可能なので、本評価項目を満たないと修正した。

† Google 2-Step は音声通話モードを評価した。転送設定変更によりなりすませるため、本評価項目を満たさない。

‡Bonneau らは本評価項目を満たすとしているが、電話会社が TTP である必要があるので、本評価項目を満たさないと修正した。

3.4.3　課題

本節では、本方式に残された課題について議論する。

(1) 転送と発信者番号同時攻撃に対する脆弱性

発信者番号偽装と転送設定変更を同時に行うと、なりすませる課題がある。

(2) マルウェアに対する脆弱性

携帯電話がマルウェアに感染し、遠隔地の攻撃者の指示で、ワンコールを受けコールバックを行い、プッシュ操作を行った場合、なりすましを防げない課題がある。

(3) 中間者攻撃に対する脆弱性

3.4.2　でも述べたように、利用者端末の画面が中間者攻撃により書き換えられた場合、何に対する本人認証か判別がつかなくなる課題がある。

(4) 盗難に対する脆弱性

本方式は、従来の所有物認証同様、携帯電話及び携帯電話のロックコードが盗まれた場合、なりすませる脆弱性が存在する。

(5) ワンコールの約款上の課題

ワンコールを技術的に実現する方法は確立できたが、これは不完了呼となり、電話会社の承諾なしには実現できない課題がある。

(6) 新規・再登録時の実現方法の課題

本方式ではアプリのインストールの課題は解決できた。しかし、電話番号を如何に安全かつ安価で便利に登録するかについては未検討である。これに関しては第 4 章にて検討を行う。

(7) PC とスマートフォンで共通方式が利用できない課題

本方式をスマートフォン上のサイトに適用すると、ブラウザ表示中にワンコールがかかってき、その後、コールバックする必要があり、画面遷移が確定的にならない課題がある。

3.5　本章のまとめ

本章では、ワンコール及びコールバックによる認証方式により、他の二経路認証で課題であったソーシャル・エンジニアリングによる脆弱性、認証アプリの課題、SMS 遅延問題や、ワンタイム・パスワードの安全性と利便性が両立しない課題を解決した。またそのプロトタイプの実装とフィージビリティの評価実験、及び、安全性、利便性、経済性について考察した。

残された課題として、転送と発信者番号偽装が同時に行われた場合なりすませる脆弱性、マルウェア感染、中間者攻撃、携帯電話盗難による脆弱性、また不完了呼の利用や新規・再登録など商用上の課題、PC とスマートフォンで共通の方式が利用できない等がある。

第4章　発信者番号・声紋認証による本人認証

4.1　はじめに

本章では、前章での残された課題のうち、転送と発信者番号同時攻撃に対する脆弱性、中間者攻撃に対する脆弱性、盗難に対する脆弱性、ワンコールの約款上の課題、新規・再登録時の実現方法の課題を解決する方式の提案を行う。

日本等、発信者番号偽造対策がなされている国に限定したサービス提供をする代わりにワンコールを廃止しシンプルなものとした。また音声通話上で取引内容のガイダンスを流すことにより中間者攻撃を防止し、声紋認証を組み合わせることで盗難対策も可能とした。初期登録方法など実用面に即した提案も行う。なお方式は SI 製品及び ASP サービスとして 2 件事業化されており[30, 31, 32]、その概要についても記述する。

4.2　提案方式

本節では、前述した課題を解決する手段として、発信者番号及び声紋認証を利用した本人認証方式を提案する。

4.2.1　目標と設計方針

本章での研究の目的は、前章の課題解決及び、実用化のための検討にあり、次のような設計方針を置く。また、この章の後半では、ネットバンクでの実際の適用例について述べる。

(1) 発信者番号偽造対策を前提とすること

日本国限定にする代わりに発信者番号を安全として扱う。これにより前章方式で課題であった、転送設定と同時に発信者番号偽造による、なりすましを防御する。

(2) 携帯電話が盗難されてもなりすませないこと

パスワードもしくはPIN、ロックコードと合わせて携帯電話が盗まれても、なりすませないこと。

(3) 中間者攻撃が防御されること

(4) ワンコールを用いないこと

実用化に向け、不完了呼など電話会社の特別な承諾が必要な技術を排除する。

(5) 新規・再発行の安全安価便利な実現

実用化に向け、電話番号の登録方法の提案も行う。

(6) ネットバンク利用者全てを防御できること

ネットバンクの利用者のハードウェア環境は千差万別であり、これら全てに即応できなければならない

4.2.2　実現方式

本研究では、前章で提案した方式の改善として、発信者番号及び声紋認証による本人認証方式を提案する。これは、認証サーバが、利用者端末から本人認証要求を受け付け、認証サーバはこれに対応した発信者番号からの通話の着信を指定時間待つ。正しい発信者番号からの着信があると、音声ガイダンスで認証内容(ネットバンクの場合は送金内容)を音声ガイダンスで伝えた後、利用者に発声を促し声紋認証の後、本人認証を完了するものである。

例え中間者攻撃がなされても音声ガイダンスで検知及び認証操作の中断ができ、携帯電話(及びロックコード)が盗まれても声紋認証により成りすますことはできない。

また、利用者の ID 及び電話番号の新規／再登録の手法として、ネットなどで住所氏名を入力し、本人限定郵便を用い、免許証など原本を郵便配達員に提示の上、登録完了用パスワードを受取、それを利用者に入力することにより完了する。これにより、コストを抑えた上で、厳格な利用者登録が可能となる。

4.2.3　システム構成と役割

図 4-1 に提案システムの構成を示す。本例では、わかりやすさのため、ネットバンクを例に用いて説明を行う。

(1) 認証サーバ

インターネットもしくは VPN を介して接続され、利用者携帯電話とは電話網を介して接続されている。IVR 機能を持ち、音声認識機能、声紋認識機能などを持つ。

(2) ネットバンクサーバ(サービス提供サーバ)

前章と同等の一般的な WEB サーバ。ネットバンクサービスを提供し、利用者の ID、電話番号、残高情報などを持つ。

(3) 利用者端末

前章と同様であり、PC やスマートパッドなど任意の端末。インターネット接続機能を持ち、一般的な WEB ブラウザがインストールされている。

(4) 利用者携帯電話

前章の条件に加え、日本国内の電気通信事業者の電話端末であり 050、090、080、03 など電気通信番号(電話番号)が付与されていることを条件とする。Skype など電気通信事業者法に定める電気通信サービス以外のソフトフォンは対象外とする。なお本稿執筆時では日本国内において Skype からは発信者番号通知サービスは利用できない*。

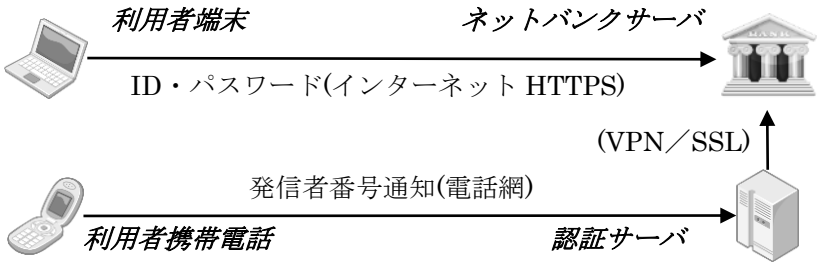


図 4-1　基本原理

* Skype：http://www.skype.com/intl/ja/features/allfeatures/caller-identification/

4.2.4　初期登録／電話番号変更

本節では初期登録及び電話番号変更の手続きについて述べる。

(1) 電話番号郵送

通常の商習慣と同様に、住民票のコピーなど本人確認書類及び、届出印が押印された口座開設申込書に、利用者携帯電話の電話番号を記入して郵送する。ただし登録可能な電話番号は国内の電話番号(0 から始まる番号)のみとする。

(2) 本人限定受取郵便の受取

ID・パスワード・認証サーバの電話番号が、本人限定受取*で郵送され。利用者はこれを受け取ると、認証サーバの電話番号を、利用者携帯電話のアドレス帳などに保存する。

(3) 声紋登録

初回、認証サーバの電話番号にかけると声紋登録モードとなり、音声ガイダンスで、登録するキーワードの発音を求められ、声紋登録が完了する。

*日本郵政株式会社　本人限定受取：http://www.post.japanpost.jp/service/fuka_service/honnin/

4.2.5　認証手順

(1) 第一認証

第一認証とは残高照会など簡易なコマンドのことである。多くのネットバンクは、多要素認証の不利便性緩和のため、残高照会などはパスワード認証レベルにとどめている。

(2) 送金内容の送信

利用者端末からネットバンクサーバに、送金先、送金内容を送信する。この段階では、まだ送金は実行されない。

(3) 認証要求

ネットバンクサーバは、ランダムに生成したセッション番号を発行し、認証サーバに、以下の内容を送信する。

- ✧ *送金先、送金額*
- ✧ *利用者携帯電話の電話番号*
- ✧ *セッション番号*

(4) 第二認証要求画面

ネットバンクサーバは、利用者端末に、以下の内画面を表示し、第二認証を要求する。

- ➢ *「60 秒以内に、認証サーバに電話してください」*

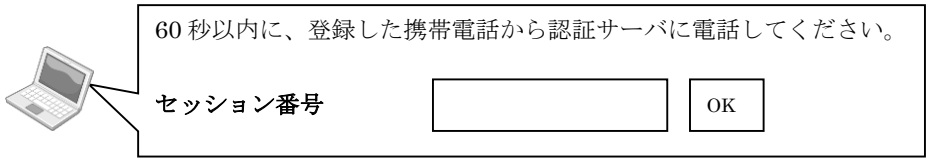


図 4-2　電話認証要求画

(5) 発信者番号認証

利用者は登録時に得たから認証サーバの電話番号へ発呼する。認証サーバは発信者番号を検知して着信応答する。

(6) 音声ガイダンス確認及び声紋判定

認証サーバは、音声ガイダンスで送金内容の確認を促す。もし異常がある場合は通話を終了することにより、送金処理は中止される。利用者は異常がないならばキーワードを発生する。

- *「こちらはB銀行です。YYY銀行に1万円送金の認証要求がきております。送金するなら、登録したキーワードを発話してください」*

(7) セッション番号通知

認証サーバは声紋判定を行い、正しければ音声ガイダンスでセッション番号を通知する。

(8) 認証結果通知

認証サーバはネットバンクサーバに対して、認証 OK／NG／タイムアウトを返す。

(9) 資金移動及び結果画面表示

ネットバンクサーバはセッション番号が正しいならば資金移動処理の後、利用者端末に対して送金結果画面を表示する。

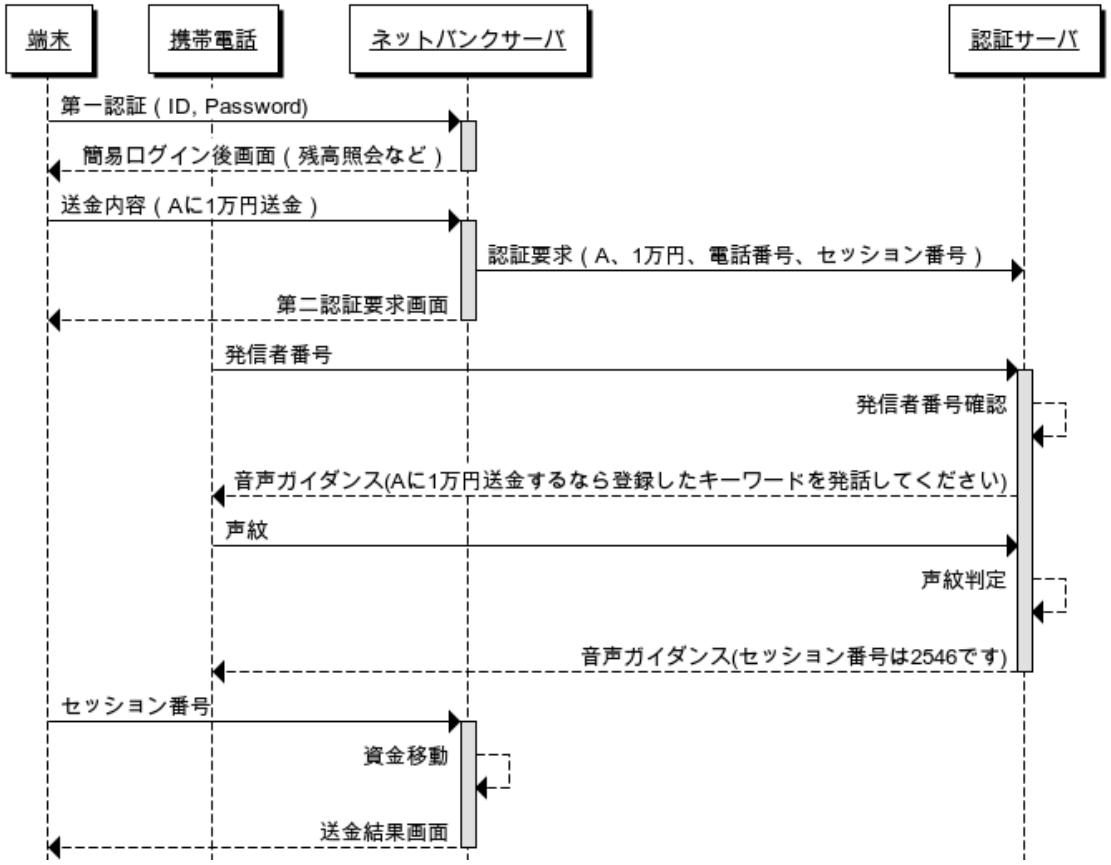

端末
携帯電話
ネットバンクサーバ
認証サーバ
第一認証 (ID, Password)
簡易ログイン後画面 (残高照会など)
送金内容 (Aに1万円送金)
認証要求 (A、1万円、電話番号、セッション番号)
第二認証要求画面
発信者番号
発信者番号確認
音声ガイダンス(Aに1万円送金するなら登録したキーワードを発話してください)
声紋
声紋判定
音声ガイダンス(セッション番号は2546です)
セッション番号
資金移動
送金結果画面

図 **4-3**　シーケンス図

4.3　事業化システムの概要

提案方式は SI 製品及び ASP サービスとして事業化された。本節では事業化システムの概要について述べる。図 4-4 にサービスイメージを記す。

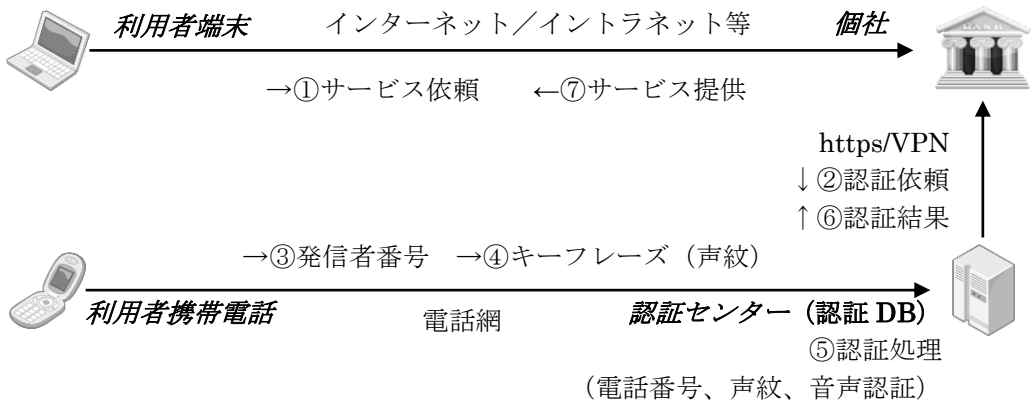


図 4-4　サービスイメージ

4.3.1　システム要件の概要

本システムでは、可用性を担保するために、各コンポーネントにサーバを分離し、回線及び機器の構成を N＋1 構成*とした。以下にシステム要件を実現する為のシステム構成の概要を示す(図 4-6)。

(1) 回線サーバ

エンドユーザからの電話を着信し、発信者番号認証、音声認識認証、声紋認証をそれぞれ組み合わせた認証を行う。認証が終了した後、認証(音声認識認証、声紋認証)の結果を認証サーバへ通知する。

本サーバは、電話回線(本例の場合、NTT 東日本 INS1500†)を直収できる CTI‡ボードを内蔵する。電話回線、回線サーバ、認証サーバで、ワンセットとし、電話回線増強の際は、これらをセットで増やすだけでよいようにした。

(2) 認証サーバ

認証 DB からの認証要求を受け付け、発信者番号認証、及び認証結果の返却を行う。

認証 DB からの認証要求と回線サーバからの認証の結果から発信者番号認証を行う。

認証が終了した後、アクセス履歴の記録、及び認証 DB へ認証結果の返却を行う。

回線サーバと一対一の関係にある。回線サーバと認証サーバを切り分けた理由は、CTI ボードや音声・声紋認証は、市中製品を利用するため、Windows である必要があり、認証サーバは開発費を押さえるため Linux で作成したためである。

(3) アクセス管理サーバ

認証要求の進行状況を管理する。

認証要求の進行状況は認証サーバによって記録、更新される。

複数の認証 DB サーバ、認証サーバでのセッションの管理を行うため、本機能を別個のサーバに切り分けた。

---

*動作に必要なサーバ数に加えて 1 台余分に用意しておくことにより、故障によるシステム停止を防止する手法。

†NTT の ISDN サービスの商品名。B チャネル(64kbps)23 本と D チャネル(64kbps)1 本からなる。

‡電話や FAX をコンピュータシステムに統合する技術。

(4) 認証 DB サーバ

利用者からの認証依頼の受け付け、及び認証結果の返却を行う。

認証要求が ID(パスワード)で行われた場合、ID(パスワード)から電話番号への変換を行い、認証サーバへ認証要求を行う。

認証サーバから認証結果が返却された後、レポートの記録及び認証結果の返却を行う

認証依頼を受け付けるため、安定性が必要なため、この機能を別個のサーバに切り分けた。

(5) 管理サーバ

認証センターへの認証要求の履歴を保持しているアクセス管理サーバに対して検索・集計を行う。

認証処理には直接関与せず、運用上必要なサーバであるため、この機能を別個のサーバに切り分けた。

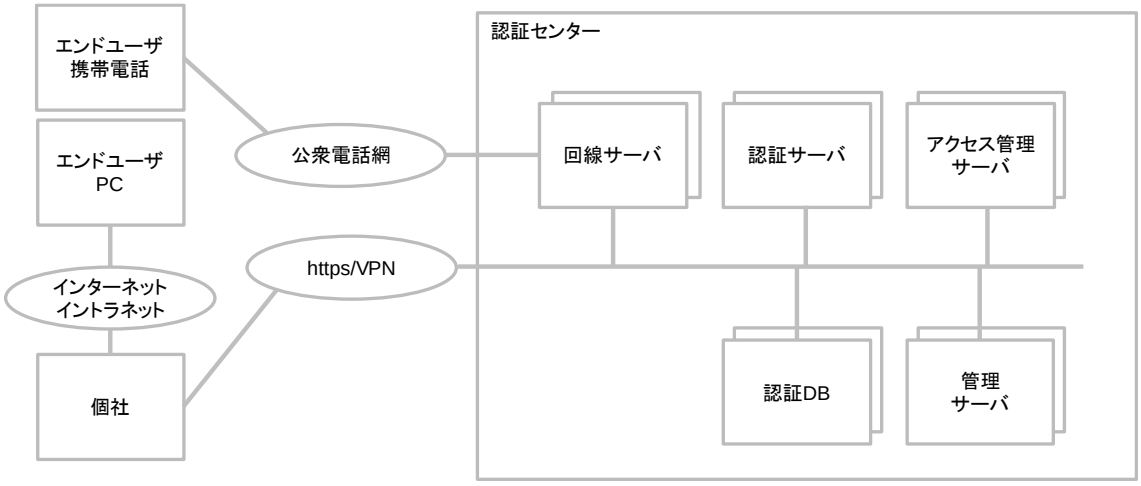


図 4-5　ASP センターのシステム構成

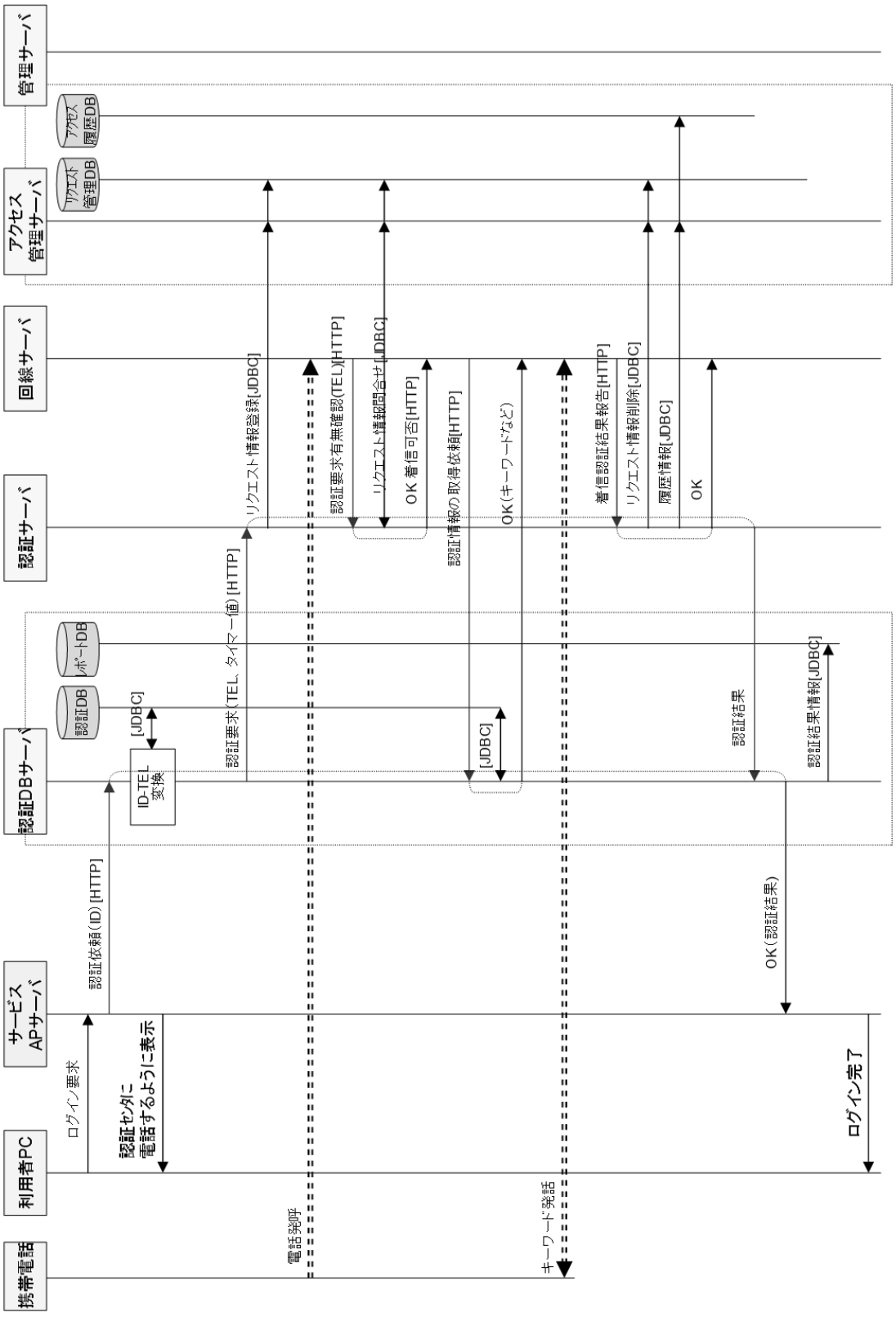


図 4-6　ASP センターのシーケンス

4.3.2　回線数の算定例

認証センターのキャパシティは、下表の前提条件とした。

要求条件	
認証要求数	10 万回／月

その他の前提条件	
各個社の 1 か月の平均営業日数	20 日
1 日の中での最繁時集中率(1 時間当たり)	20%
1 通話内の発話回数と通話時間	発話回数：1 回(確率 60%)　10 秒(キーフレーズは 1 種類) 発話回数：2 回(確率 30%)　20 秒(キーフレーズは 1 種類) 発話回数：3 回(確率 10%)　30 秒(キーフレーズは 1 種類) 1 通話あたりの平均通話時間　15 秒 通話開始までの時間　5 秒
声紋認証利用率	100%
呼損率	0.1% (認証を行うために架電したが、話中になる確率)
その他	個社毎の認証要求数のばらつきがない 最繁時内は認証要求数のばらつきがない

上記前提条件から、アーラン B 式で算出した結果、下表の回線が必要である。

項目	数量	備考
呼量	5.6 アーラン	20［秒］×(10［万回］／ 20［日］)× 20% ／ 3600［秒］
必要回線数	15 回線	INS1500(23 回線)利用のため余裕度は 1.5 倍

4.3.3　実現機能

本人認証技術は、既存アプリケーションとの接続部分の作りこみが重要である。本システムでは代表的なアプリケーションを想定し以下の機能を備えた。

(6) Web におけるベーシック認証

個社の Web サイトで使用している Apache のベーシック認証モジュールを置き換える。置き換えるベーシック認証モジュールは、Apache2.0 のベーシック認証モジュールを改造したもので、通常のベーシック認証が成功した場合に認証依頼を行い、Apache2.0 のベーシック認証モジュールの仕様で認証結果を返却する。

(7)　Windows ログオンにおける認証

個社内で管理される LAN 接続 PC へのログオン処理に GINA *を拡張した認証要求処理(以降、拡張 GINA)を組み込む。通常の Windows ログオンに加えて電話認証を行うことでセキュリティを強化する事が出来る。

(8) VPN 接続における電話認証

Radius 認証に電話認証要求処理を組み込む。通常の Radius 認証に加えて電話認証を行うことでセキュリティを強化する事が出来る[33]。

(9) シンクライアント利用における電話認証

シンクライアント上のソフトウェアを起動した際の本人認証時に電話認証要求処理を組み込む。通常のシンクライアントでの認証に比べ、セキュリティを強化する事が出来る。シンクライアント製品(本例では CITRIX†)との実現例を図 4-7 に示す。

*Windows NT/2000/XP のログオン処理を行うモジュール。
†Citrix:www.citrix.com

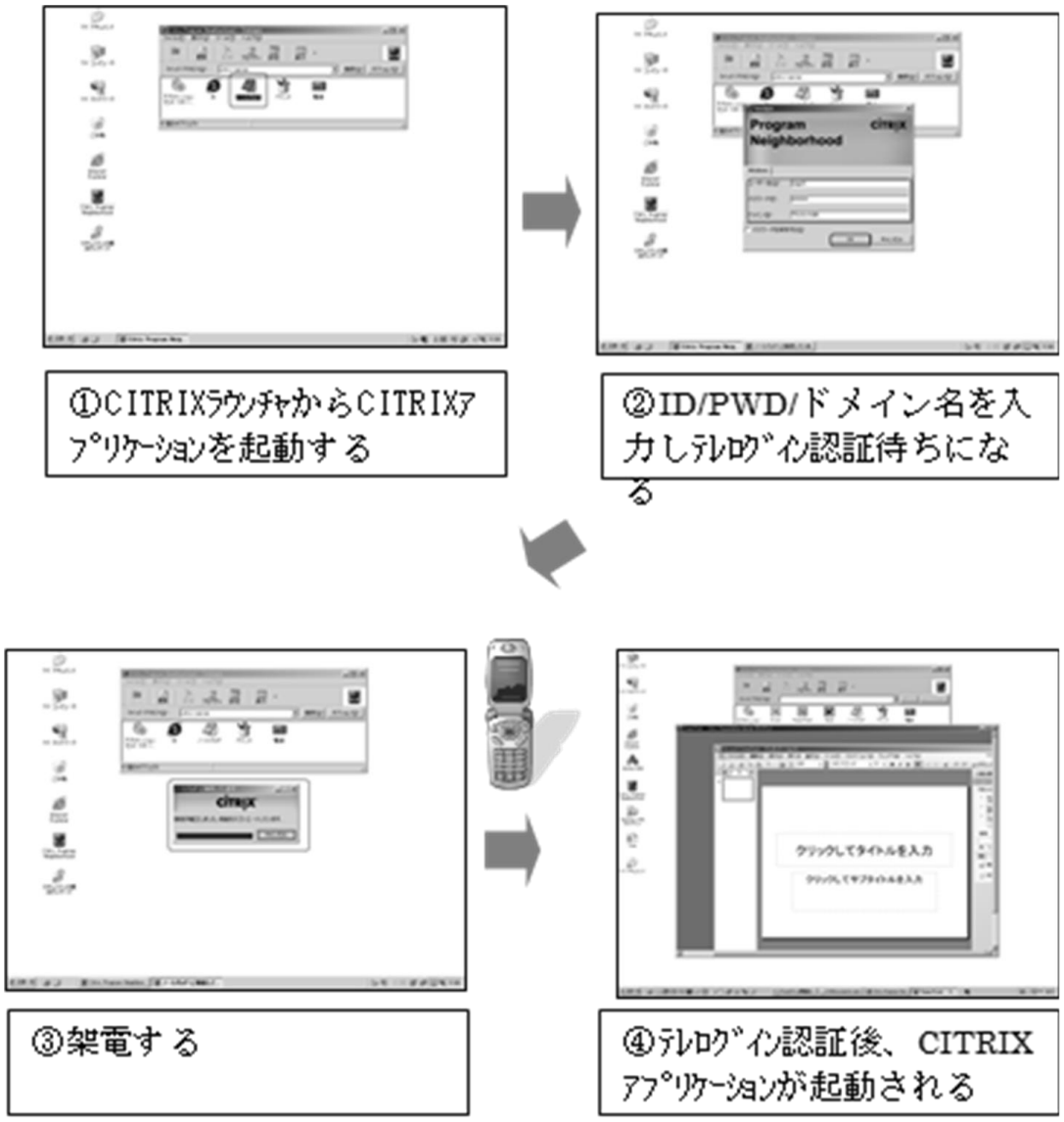


図 4-7　シンクライアントでの実現例

4.4　考察

本章で提案した方式に関して、設計方針に対する達成度、UDS 評価及び残された課題の抽出を行う。

4.4.1　設計方針に対する達成度

(1) 発信者番号偽造対策の安全性

本方式は、発信者番号偽造対策を前提条件とした。発信者番号の安全性については、電話網の構成要素を交換機網、交換機と電話端末をつなぐアクセス網、電話端末の 3 つに分けて考察する。

交換器網は物理的に保護もしくは暗号化されている閉域網であり、発信者番号の偽造は困難である。次に、アクセス網と電話端末の安全性については、サービス毎に異なる。3G 携帯電話については、アクセス網は AKA[34]で暗号化されている。AKA は今日まで脆弱性が見つかっておらず、その安全性は評価されている[35]。電話端末について、AKA の鍵を格納する SIM チップは耐タンパー性があり、不正読み取りは困難である。固定電話(加入電話や光 IP 電話)の場合、電話端末を識別するのでなく、アクセス回線毎に、発信者番号が割られているので、異なる回線からの成りすましはできない。当該回線のワイヤータップは電線や屋内配線へのアクセスを必要とするため物理的に困難である。また、光 IP 電話の場合は、電話端末を SIM 挿入可能としたり[36]、AKA を用いる[37]などして 3G 携帯電話と同等の安全性を実現することが可能である。よって、発信者番号を偽造することはできない。

また、日本国内においては総務省令[38]及び TCA ガイドライン[39,40]によって、各電話会社が対策の実施を公表している[41,42]。海外では発信者番号をユーザや電話会社が書き換えられる国が存在するため、本技術は世界共通で利用することはできない。ただし、その国で発信者番号を書き換え、国際通話を用いて、日本国内のサーバに不正ログインしようとした場合、発信者番号は”0”以外から始まる番号となり[43]、成りすましを判別することができる。よって日本国内においては、発信者番号は偽造困難であると言え、なりすましは困難であるといえる。

(2) 盗難に対する安全性

攻撃者が利用者の携帯電話と、ID とパスワードを盗んだとする。攻撃者は発信者番号認証まで進むことはできるが、声紋認証を突破することができない。よって本方式では盗難によるなりすましを防止することができる。

(3) 中間者攻撃に対する安全性

攻撃者が、送金内容をセッション・ハイジャックし、送金先と送金額を書き換え、ネットバンクに送信したとする。利用者は音声ガイダンスで改ざんを検知でき、電話を切ることにより、送金を中止できる。よって本方式では中間者攻撃を阻止することができる。

ただし、電話網も同時に中間者攻撃にあった場合は、なりすましが可能となる。しかし、上記(1)で述べたように、電話網はクローズドであり、現状のインターネットに比べて十分に安全であり、中間者攻撃は困難と言える。

次に、攻撃者が、攻撃者の電話番号を PC に表示させ、偽造ガイダンスを流す中間者攻撃も考えられる。初期登録でサーバの電話番号が伝えられているが、騙されて電話をかけてしまう利用者は確率的に発生する。この場合、例え、利用者の声紋を盗られたとしても、攻撃者は携帯電話の発信者番号を、なりすまして認証サーバに電話することができないので、なりすましは防がれる。

なお第 5 章方式は、宣誓内容により、中間者攻撃を検知・防御することができる。

(4) ワンコールを用いずに実現

前章方式のように、不完了呼を用いないことにより約款上の課題を解決した。

(5) 新規・再発行時の安全安価簡便な実現

例え本人書類や印影を偽造して申し込んだとしても、郵便局員に免許証など原本を提示しなければならないので、なりすましは防止できる。また郵便局員から手渡しで ID, パスワードなどを渡されるので、ポストから盗まれるといった心配もない。また日本では、携帯電話不正利用防止法[44]により、携帯電話販売時、厳格な本人確認が義務付けられており、なりすましての購入は困難と言える。

(6) ネットバンク利用者全てを防御できること

本方式では、生体認証として、声紋認証を採用した。この理由として、声紋認証以外は、特殊な読取り装置が必要で、一部の携帯電話しか対応していないためである。顔認証の場合、カメラのみであるが、ネットバンクの法人ユーザを考慮した場合、固定電話からも利用できる必要があり、声紋を採用した。また、第 5 章でも述べるが、声紋認証には、他の生体認証に対して、リプレイアタックを防御できる特性や、初期登録の運用面の簡便さなどの特性があることも採用条件の一つである。

4.4.2 UDS 評価

Security、Deployability、Usability の観点から考察を加える。第 3 章方式と異なる項目を中心に記述する。

利便性(Usability)

(1) 記憶不要性 (Memorywise-Effortless)

本方式では、音声ガイダンスや発生などの操作があるため、利便性向上のため、第一認証はパスワードを採用した。よって、本評価項目は満たさない。

(2) 利用者スケーラビリティ (Scalable-for-Users)

サイト毎にパスワードを記憶しなければならないので、本評価項目は満たさない。

(3) 認証エラーの低さ (Infrequent-Errors)

声紋認証があるため、必ず認証失敗が発生する。よって本評価項目は満たさない。

普及性(Deployability)

(1) アクセス性 (Accessible)

本方式は、音声ガイダンスを聞き取り、声紋を発生する必要がある。よって、本評価項目を満たさない。

(2) 成熟度 (Mature)

本システムは、SI 製品及び ASP 製品として事業化され、総務省実証実験[31]などに採用せれている。よって本評価項目は満たす。

(3) 携帯電話互換性　(Cellphone-or-Carrie Compatible：新規)

本方式は、発信者番号偽造対策された国／電話会社でしか利用できない。よって、本評価項目は満たさない。

安全性(Security)

(1) 標的型なりすまし耐性　(Resilient-to-Targeted-Impersonation)

発信者番号は日本国内では厳格に安全性が規定されており、転送設定のように、電話会社オペーレーターを騙すことにより、なりすませることはない。よって本評価項目を満たす。

(2) 内部観察耐性　(Resilient-to-Internal-Observation)

携帯電話がマルウェアに感染し、電話操作を乗っ取りキーワードを不正録音すると、攻撃者が後でなりすますことができる。よって部分的に満たすといえる。

(3) 盗難耐性　(Resilient-to-Theft：修正)

前節で述べたとおり、携帯電話が盗難されても、声紋認証で防御することができる。

(4) 意思確認の確実性　(Requiring-Explicit-Consent：修正)

本方式は、音声ガイダンスで取引内容を流しているが、利用者の否認までは防げない。よって部分的に満たすとした。

(5) 中間者攻撃耐性　(Resident-to-Man-in-the-Middle-Attack：新規)

本方式は、例え送金先、送金額、及び送金結果画面が改ざんされたとしても、音声ガイダンスで検知でき、送金を中止することができる。よって本評価項目を満たす。

表 4-1　UDS 評価

Scheme	利便性(Usability)								普及性(Deployability)								安全性(Security)															
	記憶不要性 (Memorywise-Effortless)	利用者スケーラビリティ (Scalable-for-Users)	所持物不要性 (Nothing-to-Carry)	物理的操作不要性 (Physically-Effortless)	操作方法の覚えやすさ (Easy-to-Learn)	操作効率 (Efficient-to-Use)	認証エラーの低さ (Infrequent-Errors)	復旧容易性 (Easy-Recovery-from-Loss)	アクセス性 (Accessible)	利用者数変動費 (Negligible-Cost-per-User)	サーバ互換性 (Server-Compatible)	ブラウザ互換性 (Browser-Compatible)	成熟度 (Mature)	知的所有権の解放 (Non-Proprietary)	**携帯電話互換性 (Cellphone-or-Carrie Compatible：新規)**		物理的観察耐性 (Resilient-to-Physical-Observation)	標的型なりすまし耐性 (Resilient-to-Targeted-Impersonation)	制限下推測耐性 (Resilient-to-Throttled-Guessing)	無制限下推測耐性 (Resilient-to-Unthrottled-Guessing)	内部観察耐性 (Resilient-to-Internal-Observation)	情報漏えい耐性 (Resilient-to-Leaks-from-Other-Verifiers)	フィッシング攻撃耐性 (Resilient-to-Phishing)	**盗難耐性 (Resilient-to-Theft：修正)**	TTP 不要性 (No-Trusted-Third-Party)	**意思確認の確実性 (Requiring-Explicit-Consent：修正)**	同定不可能性 (Unlinkable)	**中間者攻撃耐性 (Resident-to-Man-in-the-Middle-Attack：新規)**
本章方式			△	△	●	△		△				●	●				●	●	●	●	△	●	●	●			△		●			
第 3 章方式	●	●	△	△	●	△	△	△	△			●	△		●		●	△	●	●	△	●	●	●			△					
Voice	●	●	●	△	●	△			△	△		△	△				●		△							●	△					
OTP over SMS	●	●	△		●		△	△	△			●	●	●	△		●	●	●	●	△	●	●	●		‡‡	△	*				
Google 2-Step			△		●	△	△	△	△			●	●		●		△	†	●	●		●	●	●		‡	△					

※　●は評価項目を満たす。△は部分的に満たすことを示す。空欄は満たさないことを示す。
灰色太字は、追加修正事項。

*Bonneau らは本評価項目を満たすとしているが、電話番号により同定可能なので、本評価項目を満たないと修正した。

† Google 2-Ste は音声通話モードを評価した。転送設定変更によりなりすませるため、本評価項目を満たさない。

‡Bonneau らは本評価項目を満たすとしているが、電話会社が TTP である必要があるので、本評価項目を満たさないと修正した。

4.4.3　課題

本節では、本方式の残された課題について述べる。

(1) パスワードやセッション番号の入力の手間

本方式では、電話操作が多くなった分、利便性確保のため、第一認証にパスワードを導入した。

(2) 世界的に利用できない課題

本方式では、発信者番号偽造対策がなされている国でないと利用できない課題がある。

(3) リプレイ攻撃に対する脆弱性

携帯電話に感染したマルウェアや、利用者の近くにいる人が、利用者のキーワードの発生を録音し、これを再利用した、なりすましを防ぐことはできないという課題がある。

(4) 利用者の否認防止ができない課題

音声ガイダンスを流したからといって、利用者の否認を防止することができない課題があった。

(5) PC とスマートフォンで共通方式が利用できない課題

スマートフォン上のサイトに本方式を適用した場合、ブラウザから音声通話への画面遷移は確定的に行えるが、音声通話終了後、ブラウザ画面への画面遷移が確定的に行えない課題が存在する。

4.5　本章のまとめ

本章では、発信者番号認証及び声紋認証による本人認証方式により、第 3 章方式で課題であった、転送設定と発信者番号偽装の同時攻撃を防御でき、盗難によるなりすましも防御できるようになった。また実用化システムの概要を述べた。本方式は、不完了呼を用いないことによる約款上の課題も解決した。ただし、発信者番号偽造対策がなされた、日本国内でしか利用できない課題や、声紋のリプレイ攻撃の課題、否認の課題、パスワード入力などの残課題がある。次章では、これらの課題を解決する方法について提案を行う。

第5章　SMS・声紋チャレンジレスポンスによる本人認証方式

5.1　はじめに

本章では、4.4.3　で示した課題である、パスワードやセッション番号の入力の手間、世界的に利用できない課題、リプレイ攻撃に対する脆弱性、利用者の否認防止ができない課題、PC とスマートフォンで共通方式が利用できない課題を解決する方式を提案する。

本章の提案方式では一般的な携帯電話を認証デバイスとして利用し、SMS でコールバック先電話番号を送信し所有確認を行い、利用者に音声通話で操作内容を宣誓させ、これの声紋判定及び録音を行う。宣誓を証拠として残すことにより、利用者の否認を防止でき、宣誓内容は毎回異なることからリプレイ攻撃を防止できる。また発信者番号認証を用いないことから世界的に利用できる。ただし SMS 遅延問題はあるが、初回のみクライアント証明書をダウンロードし、毎回の認証はこれを用いて認証し、送金や電子申請など重要な認証のみ、上記認証をすることにより、SMS 遅延問題や、利便性の課題を緩和する。

本章では、理論の提案と考察を行う。

5.2　提案方式

本節では、前述した問題を解決する手段として、SMS 及び声紋チャレンジレスポンスによる本人認証方式を提案する。

5.2.1　目標と設計方針

本章での研究の目的は、前章の課題解決及び、実用化のための検討にあり、次のような設計方針を置く。

(1) パスワードなど入力の不要化

毎回の煩雑な処理を不要とすること。

(2) 世界共通的に利用できること

発信者番号認証など、特定の国／電話会社でしか利用できない技術を用いず、世界共通的に利用できること。

(3) 声紋のリプレイ攻撃を防止できること

攻撃者がマルウェアなどを利用して、利用者の声を録音して再利用し、不正ログイン出来ないこと。

(4) 利用者の否認防止ができること

利用者が「間違ってクリックした」、「(中間者攻撃などに)騙されてクリックした」、「画面表示が壊れていた」などと主張し、否認をすること。

(5) PC とスマートフォンで共通に利用できること

5.2.2　実現方式

本研究では、前章で提案した方式の解決方式として、SMS・声紋チャレンジレスポンスによる本人認証方式を提案する。これは、一般的な携帯電話を認証デバイスとして利用し、予め登録された利用者の SMS に、毎回変わる認証サーバの電話番号(ワンタイム電話番号)と、毎回かわる URL(ワンタイム URL)、及び操作内容を記したテキストを送信する。利用者は、60 秒など指定時間内に、ワンタイム電話番号にコールバックすると、音声ガイダンスにより、操作内容を読み上げ宣誓することを求められ、録音及び声紋判定される。利用者は音声通話修了後、SMS のワンタイム URL をクリックすると、クライアント証明証がインストールされる。二回目以降の毎回のログインは、このクライアント証明書を用いて行われる。ただし送金や電子申請など重要な認証は、再度、上記 SMS 送信から宣誓録音、声紋判定までが行われ、厳格な認証が行われる。

本方式により、初回及び重要認証時のみ SMS を利用することにより SMS 遅延問題や利便性の問題が緩和される。発信者番号認証を利用しないことにより、世界的に利用できる。宣誓を録音することにより、利用者の否認を防止でき、宣誓内容は毎回異なることからリプレイ攻撃を防止した上での声紋認証も可能となる。SMS 及びワンタイム URL を用いることにより、スマートフォン上のサイトの認証に利用しても、確定的に画面遷移が可能となるので、スマートフォン上の認証方式としても利用可能となる。

5.2.3　システム構成と役割

図 5-1 に提案システムの構成を示す。本例でも、分かりやすさのため、ネットバンクを例に用いて説明を行う。

(1) 認証サーバ

前章と同じくインターネットもしくは VPN を介して接続され、利用者携帯電話とは電話網を介して接続されている。IVR 機能を持ち、音声認識機能、声紋認識機能など持ち、さらに本方式では新たに SMS 送信機能を持つ。

(2) ネットバンクサーバ(サービス提供サーバ)

前章と同等の一般的な WEB サーバ。ネットバンクサービスを提供し、利用者の ID、電話番号、残高情報などを持つ。

(3) 利用者端末

前章と同じく PC もしくはスマートフォンであり、インターネット接続機能を持ち、一般的な WEB ブラウザがインストールされている。ただし、スマートフォン内のサイトの認証に利用する場合は、下記、利用者携帯電話と利用者端末は同一となる。

(4) 利用者携帯電話

日本国内など限定せず、世界的に一般に利用されている携帯電話端末とする。SMS の送信機能、音声通話機能を持つ。ただし、Skype などパスワード認証でログインできるものは含まない。

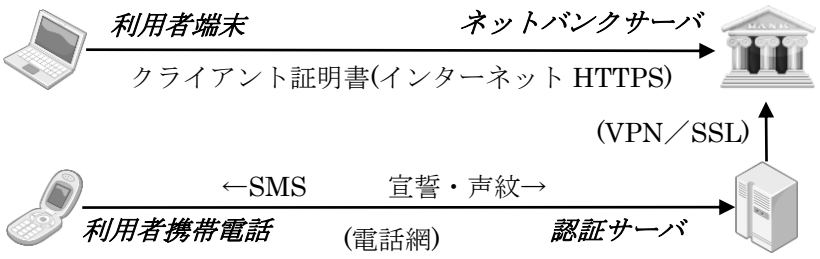


図 5-1　基本原理

5.2.4　電話番号の新規登録／変更及びスマートフォンへのクライアント証明書配布

本節では声紋、電話番号の登録方法及び利用者端末がスマートフォンなどの場合のクライアント証明書インストール方法について述べる。

(1) 電話番号郵送

利用者は、申込書に電話番号などを記入し、自筆署名もしくは捺印の上、本人確認書類のコピーともに、ネットバンクに郵送する。ただし本人確認書類は、電話番号変更時には不要である。

(2) SMS 送信

サーバは、利用者携帯電話に対して、SMS を用いて、ワンタイム電話番号、ワンタイム URL、宣誓内容を送信する。宣誓文には、日付など毎回変わる文字列があり、また声紋登録の精度を向上すべく、他の単語の復唱も追加的に求めても良い。

- *本文例：*

  “こちらは B-Bank です。

  1)60 秒以内に 050-1111-1111 に電話し宣誓文を読み上げてください。

  2)宣誓文『私、Alice は、B-Bank に声紋を登録します。今日の日附は…』

  3)上記操作後、次の URL よりクライアント証明書をダウンロードしてください.　https://b-bank.com/9fasd8abgrgat8erae5“

(3) コールバック

利用者はワンタイム電話番号をクリックし電話をかける。サーバは指定時間以内であることを確認し着信応答する。

(4) 宣誓／声紋登録

利用者は、音声通話開始後、宣誓文を読み上げる。サーバは正しく読み上げられたこと、音声認識で確認し、宣誓録音データの保存、及び声紋データの抽出を行う。

(5) 認証完了／クライアント証明書インストール

利用者がワンタイム URL をクリックすると、クライアント証明書がインストールされる。

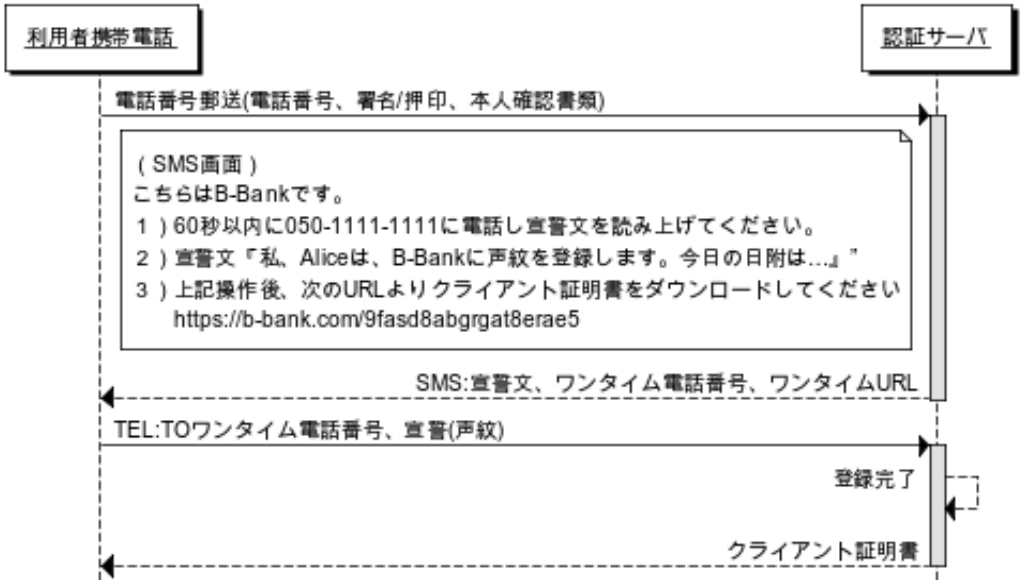


図 5-2　電話番号新規登録／変更及びスマートフォンへのクライアント証明書配布

5.2.5　PC へのクライアント証明書配布

本節では、前節で登録した情報を元に、利用者端末が PC の場合のクライアント証明書インストール方法について述べる。

(1) 利用者端末に電話番号の入力

利用者は、利用者端末のクライアント証明書発行画面で、電話番号を入力する。この時、PC の IP アドレスを送信してもよい。

(2) 利用者携帯電話に SMS 送信

新規登録時と同様の SMS を送信する。ただし宣誓文は PC にクライアント証明書をインストールする旨の文に変わり、利用者携帯電話側にダウンロード操作不要であるため、ワンタイム URL は省略される。

- *本文例*

  “こちらは B-Bank です。

  1)60 秒以内に 050-1111-1111 に電話し宣誓文を読み上げてください。

  2)宣誓文『私、Alice は、IP アドレス X.X.X.X の PC にクライアント証明書をインストールします。今日の日附は…』”

(3) コールバック

(4) 宣誓録音／声紋認証

利用者は、音声通話開始後、宣誓文を読み上げる。サーバは、音声認識で正しく読み上げられたか確認後、録音データを保存し、新規登録で登録された声紋データと照合する。

(5) 認証完了／クライアント証明書インストール

利用者端末画面が画面遷移し、証明書がインストールされる。

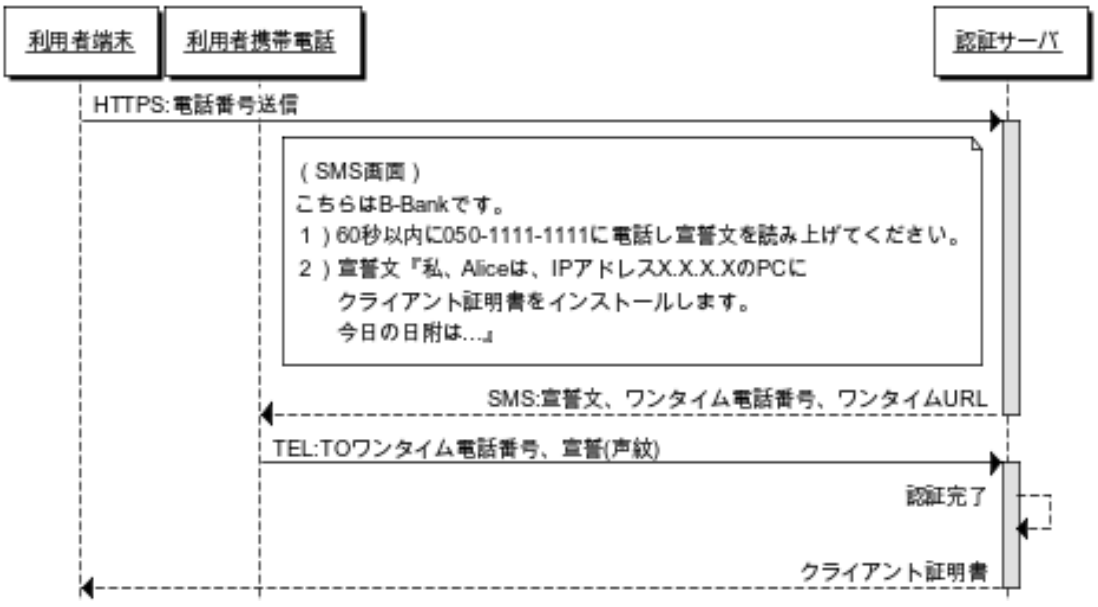


図 5-3　利用者端末へのクライアント証明書配布

5.2.6　簡易認証(第一認証)

残高照会など毎回の簡易な認証(第一認証)は、クライアント証明書を用いて行い、利用者の操作は不要となる。

5.2.7　重要認証(第二認証)

本節では、送金や電子申請など、需要な認証時の操作について述べる。今回は、スマートフォン上のサイトでの重要認証時の操作について述べる。

(1) クライアント証明書による第一認証

利用者は、利用者端末からクライアント証明書を用いて、第一認証をする。

(2) 送金内容の送信

利用者は、利用者端末からネットバンクサーバに、送金内容を送信する。この段階では、まだ送金は実行されない。

(3) 認証要求

ネットバンクサーバは、認証サーバに、送金額、送金先などを送信し、認証要求を行う。

(4) SMS 送信

新規登録と同様に、サーバは、利用者携帯電話に対して、SMS を用いて、ワンタイム電話番号、ワンタイム URL、宣誓文を送信する。

- *本文例：*

  “こちらは B-Bank です。

  1)60 秒以内に 050-1111-9758 に電話し宣誓文を読み上げてください。

  2)宣誓文『私、Alice は、口座番号 YYY に ZZZ 円送金します。

  今日の日附は…』

  3)上記操作後、次の URL よりネットバンク画面に戻ってください(任意)

  https://b-bank.com/9fasd8abgrgat8erae5“

(5) コールバック

(6) 宣誓／声紋認証

(7) 認証完了／送金実行

ワンタイム URL をクリックすると、ネットバンクの画面に戻り、その後の処理(例えば振込先の登録など)が可能となる。

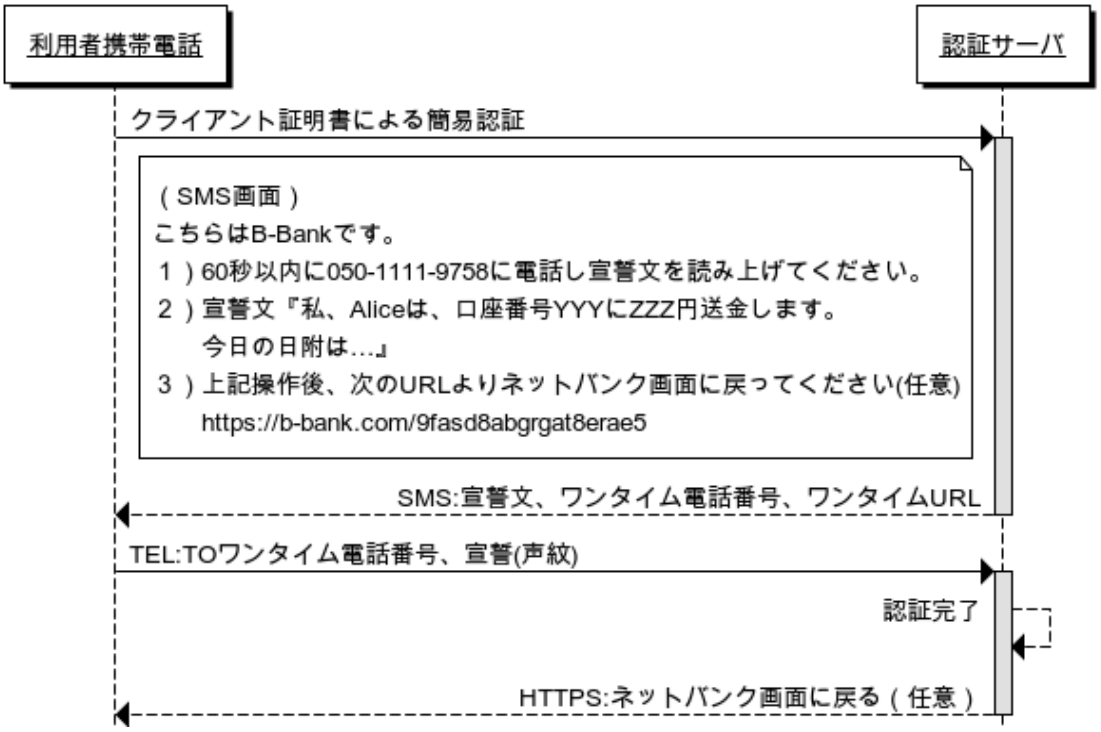


図 5-4　スマートフォンでの重要認証

5.3　考察

本章で提案した方式に関して、設計方針に対する達成度、UDS 評価及び残された課題の抽出を行う。

5.3.1　設計方針に対する達成度

(1) パスワードなど入力の不要化

毎回の煩雑な処理を不要とすること。

(2) 世界共通的に利用できること

本方式は発信者を認証に利用せず、SMS 及び音声通話及び 3G コネクションを用いることにより、世界共通的に利用できるようにした。SMS は最も普及しているモバイルサービスであり[45]、またその仕様は標準化団体により規定されている[46]。前章 4.4.1　(1)で示したように、電話網のうち交換器網は物理的保護もしくは暗号化されている閉域網であり、アクセス網は AKA により暗号化されている。AKA の鍵を格納する、携帯電話端末の SIM チップは耐タンパー性を有しており、不正読み取りは困難である。また 3G コネクションは、ブロック暗号 KASUMI[47]に基づいた f8,f9[48]アルゴリズムにより盗聴／改ざんが防止されている。

(3) 声紋のリプレイ攻撃を防止できること

攻撃者が、マルウェアなどを利用して、利用者の宣誓を不正録音したとしても、宣誓内容は毎回変わり、また日付なども含まれるので、後で不正利用することはできない。

(4) 利用者の否認防止

利用者本人の声で宣誓が録音されるので、後で否認を防止できる。なお、同等の手法は多くのテレフォンショッピングなどで、オペーレーターと客との会話録音でも用いられトラブル防止のための実績のある手法である。

(5) パスワードなど入力の不要化

クライアント証明書を用いることによりパスワードなど入力操作を減少させた。また宣誓を用いることにより、セッション番号の入力なども不要化できた。

(6) PC とスマートフォンで共通に利用できること

音声通話終了後、再度、SMS 画面を開き、ワンタイム URL をクリックすることで、課題であった、音声通話終了後の画面遷移の不確定さを解決した。よって本方式はスマートフォン用サイトにも安定して適用することができる。

5.3.2 UDS 評価

Security、Deployability、Usability の観点から考察を加える。本節では、第 4 章方式と異なる項目を中心に記述する。

利便性(Usability)

(1) 記憶不要性 (Memorywise-Effortless)

クライアント証明書によりパスワードが一切不要なため、本評価項目を満たす。

(2) 利用者スケーラビリティ (Scalable-for-Users)

パスワードのように、利用者自信がサイトごとに記憶する情報がないので、本評価項目を満たす。

(3) 物理的操作不要性 (Physically-Effortless)

本方式は宣誓の発話のみであり、パスワードやセッション番号の入力は一切不要である。よって本評価項目を満たす。

普及性(Deployability)

(1) 成熟度 (Mature)

本方式は原理の提案のみであるため、本評価項目を満たさない。

(2) 携帯電話互換性 (Cellphone-or-Carrie Compatible：新規)

本方式は世界的中の携帯電話で利用できる。よって本評価項目を満たす。なお、生体認証に、声紋認証以外を用いた場合、本評価項目を満たすことはできない。

安全性(Security)

(1) 物理的観察耐性 (Resilient-to-Physical-Observation)

攻撃者に SMS を盗み見られたとしても、声紋を真似して送信することができない。よって本評価項目を満たす

(2) 内部観察耐性 (Resilient-to-Internal-Observation)

攻撃者がマルウェアなどを用いて SMS や音声通話を盗聴したとしても、毎回宣誓文はことなるので、なりすませない。よって本評価項目を満たす。

(3) 意思確認の確実性 (Requiring-Explicit-Consent：修正)

前節で説明したように、利用者による否認まで防げる厳格な意思確認を実現できる。

表 5-1　**UDS 評価**

Scheme	利便性(Usability)								普及性(Deployability)								安全性(Security)											
	記憶不要性 (Memorywise-Effortless)	利用者スケーラビリティ (Scalable-for-Users)	所持物不要性 (Nothing-to-Carry)	物理的操作不要性 (Physically-Effortless)	操作方法の覚えやすさ (Easy-to-Learn)	操作効率 (Efficient-to-Use)	認証エラーの低さ (Infrequent-Errors)	復旧容易性 (Easy-Recovery-from-Loss)	アクセス性 (Accessible)	利用者数変動費 (Negligible-Cost-per-User)	サーバ互換性 (Server-Compatible)	ブラウザ互換性 (Browser-Compatible)	成熟度 (Mature)	知的所有権の解放 (Non-Proprietary)	**携帯電話互換性 (Cellphone-or-Carrie Compatible：新規)**	物理的観察耐性 (Resilient-to-Physical-Observation)	標的型なりすまし耐性 (Resilient-to-Targeted-Impersonation)	制限下推測耐性 (Resilient-to-Throttled-Guessing)	無制限下推測耐性 (Resilient-to-Unthrottled-Guessing)	内部観察耐性 (Resilient-to-Internal-Observation)	情報漏えい耐性 (Resilient-to-Leaks-from-Other-Verifiers)	フィッシング攻撃耐性 (Resilient-to-Phishing)	**盗難耐性 (Resilient-to-Theft：修正)**	TTP 不要性 (No-Trusted-Third-Party)	**意思確認の確実性 (Requiring-Explicit-Consent：修正)**	同定不可能性 (Unlinkable)	**中間者攻撃耐性 (Resident-to-Man-in-the-Middle-Attack：新規)**
本章方式	●	●	△	●	●	△		△				●			●	●	●	●	●	●	●	●		●			●
第 4 章方式			△	△	●	△		△				●	●			●	●	●	●	△	●	●			△		
第 3 章方式	●	●	△	△	●	△	△	△	△			●	△		●	●	△	●	●	△	●	●			△		
Voice	●	●	●	△	●	△			△	△		△	△			●		△						●	△		
OTP over SMS	●	●	△		●		△	△	△			●	●	●	△	●	●	●	●	△	●	●		‡‡	△	*	
Google 2-Step			△		●	△	△	△	△			●	●		●	△	†	●	●		●	●		‡	△		

※　●は評価項目を満たす。△は部分的に満たすことを示す。空欄は満たさないことを示す。
灰色太字は、追加修正事項。

*Bonneau らは本評価項目を満たすとしているが、電話番号により同定可能なので、本評価項目を満たないと修正した。

† Google 2-Ste は音声通話モードを評価した。転送設定変更によりなりすませるため、本評価項目を満たさない。

‡Bonneau らは本評価項目を満たすとしているが、電話会社が TTP である必要があるので、本評価項目を満たさないと修正した。

5.3.3　課題

本節では、残された課題について述べる。

(1) 操作効率の改善

本方式は重要認証の度に宣誓文を読み上げる手間や、声紋認識エラーの手間が発生する課題がある。

(2) 通信コストの課題

クライアント証明書の利用で改善はされたものの、重要認証の度に、SMS や音声通話に通信コストが発生する課題がある。

(3) 電話会社依存の課題

本方式は SMS や音声通話などを利用するため、電話会社が TTP である必要がある課題がある。

5.4　本章のまとめ

本章では、SMS 及び声紋認証による本人認証方式により、第 4 章で課題であった、パスワードやセッション番号の入力の手間、世界的に利用できない課題、リプレイ攻撃に対する脆弱性、利用者の否認防止ができない課題、PC とスマートフォンで共通方式が利用できない課題を解決する方式を提案及び考察を行った。ただし残された課題として、操作効率の改善、通信コストの課題、電話会社依存の課題などがある。

第6章　結論

本論文では、二経路多要素による本人認証技術に関する研究結果及び事業化例の概要を論じた。近年、ネットバンクなどインターネット上でのサービス利用時、別途、電話網など別の経路から識別符号を送信することにより本人認証を行う技術が普及してきているが、本論文では、既存技術の脆弱性の指摘と改善技術の提案を行った。

ワンコール、ワンタイム電話番号による着信番号認証、通知発信者番号認証、音声通話上での宣誓録音、声紋判定などを組み合わせ、従来の二経路認証技術の安全性、普及性、利便性の課題を改善した。

以下では、本論文で述べた研究内容について述べる。

第 2 章　本人認証方式

本人認証技術は、記憶認証、所有物認証、生体認証の 3 つに分類できる。近年、従来の所有物認証の初期配布コストなどを改善する技術として二経路認証が普及してきている。二経路認証は利用するチャネルにより音声通話方式、SMS 方式、アプリ方式に分類できる。

しかし、音声通話の転送設定を変更するなどソーシャル・エンジニアリングに対する脆弱性、安全な認証アプリを如何に実現するかという課題、ワンタイム・パスワードの安全性と利便性のトレードオフの課題、携帯電話のマルウェア感染の課題、中間者攻撃に対する脆弱性、携帯電話盗難の脆弱性、PC 内サイトと携帯電話内サイトで共通の認証方式を利用できない課題、生体認証と組み合わせた場合リプレイ攻撃の課題などがあった。

第 3 章　ワンコール・コールバックによる本人認証方式

第 3 章では、認証サーバが利用者携帯電話にワンコールし、毎回変わる認証サーバの電話番号を着信履歴に残し、利用者はこれにコールバックし発信者番号を通知することにより本人認証を行う方式を提案した。前章で示した課題のうち、SMS 遅延問題、認証アプリの課題は、音声通話のみを用いることにより解決し、ソーシャル・エンジニアリングの課題は、例え転送設定が変更されたとしても、発信者番号のなりすましが同時

に行わなければ、なりすませないことにより解決した。またワンタイム・パスワードを用いないことにより、利便性と安全性のトレードオフ問題も解決した。

方式の提案と同時に、プロトタイプ・システムの試作及び評価実験を行った。プロトタイプ・システムは、ワンコールの確実な実現方法、冗長化など可用性の実現方法の検証、回数などスケーラビリティの検討及び測定などを行った。

残された課題としては、転送設定と発信者番号偽装が同時に行われた場合なりすませる脆弱性、マルウェア、中間者攻撃、盗難に対する脆弱性、ワンコールの約款上の課題、新規・再登録の実現方法、PC とスマートフォンで共通の方式が利用できない課題などが判明した。

第 4 章　発信者番号・声紋認証による本人認証

第 4 章では、日本国内など発信者番号の偽装対策が施された国や電話会社での利用を前提条件とし、発信者番号及び声紋認証による本人認証方式の提案を行った。新規・再登録時、利用者は本人限定受取郵便を利用して、認証サーバの固定された電話番号を通知さる。毎回のログインは、利用者端末に ID・パスワードを入力後、指定時間以内に、登録した携帯電話から認証サーバに発信し、発信者番号通知を利用して認証を行う。音声通話確立後、取引内容を音声ガイダンスで確認し、予め登録したキーワードを発生し、声紋認証の後、本人認証を完了する。

前章の残された課題のうち、中間者攻撃に対する脆弱性は、例え取引内容がインターネット上の途中の経路で書き換えられたとしても、音声ガイダンスによって、それを検知し取引操作を中断することが可能とすることにより解決する。盗難に対する脆弱性は、例え盗難が行われても声紋認証で防御できることにより解決する。転送設定と発信者番号偽造が同時に行われた場合の脆弱性も、発信者番号偽造対策された国や電話会社に限定することにより問題を解決する。またワンコールを用いないことにより約款上の課題も解決する。新規・再登録の方法も、本人限定郵便を利用するなどして具体的に提案を行った。

本方式は、SI 製品、ASP 製品として実用化されており、事業化システムの概要についても示した。可用性を高めるため機能ごとにサーバを切り分け、回線数の実際的な算出も行った。アプリケーションとして、Web ベーシック認証、Windows ログオン、VPN、シンクライアントの認証に対応できるようにした。

残された課題としては、パスワードなどの入力の手間、世界的に利用できない課題、リプレイ攻撃に対する脆弱性、利用者の否認に対する脆弱性、PC とスマートフォンで共通の方式が利用できない課題が判明した。

第 5 章　SMS・声紋チャレンジレスポンスによる本人認証方式

第 5 章では、SMS により毎回変わるコールバック先を通知し、コールバック時、着信番号認証の後、音声ガイダンスによる取引内容の確認、及び宣誓の録音とこの声紋判定による本人認証方式の提案を行った。毎回の簡易な認証はクライアント証明書を用い、送金など重要な認証のみ上記操作をする。

本方式により、前章の残された課題のうち、パスワード入力の手間はクライアント証明書の導入により解決した。発信者番号認証を用いず SMS、音声通話、3G コネクションのみ利用することにより世界的に利用できる。宣誓録音により利用者の否認を防御でき、宣誓は毎回変わることからリプレイ攻撃を防御できる。また SMS の利用により、スマートフォン上のサイトの認証に利用しても、確定的に画面遷移ができることから、PC とスマートフォンで共通の認証方式として利用できる。

今後の課題として、操作効率の改善、通信コストの課題、電話会社が TTP であるなど課題がある。

参考文献

1 警察庁, インターネットバンキングに係る不正アクセス禁止法違反等事件の発生状況について, 2011.

2 Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment, 2006.

3 J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," IEEE Symposium on Security and Privacy (SP), 2012.

4 B. Schneier, “Two-Factor Authentication: Too Little, Too Late,” COMMUNICATIONS OF THE ACM, Vol. 48, No. 4, pp. 27–27, 2005.

5 情報処理振興事業協会セキュリティセンター:本人認証技術の現状に関する調査報告書(オンライン), 入手先 http://www.ipa.go.jp/security/fy14/reports/authentication/ (参照 2013-10-1).

6 IT media, 中間者攻撃で取引内容を改ざん、オンラインバンキングを狙う(オンライン), 入手先 http://www.itmedia.co.jp/enterprise/articles/0912/16/news020.html(参照 2012-06-06)

7 ソフトバンクテレコム株式会社, Synclock(オンライン),入手先 http://www.synclock.jp/08_personal/faq.html(参照 2012-06-06).

8 独立行政法人情報処理推進機構,情報セキュリティ白書 2012,pp.44-45, 独立行政法人情報処理推進機構, 2012.

9 J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," Technical reports published by the University of Cambridge Computer Laboratory ISSN 1476-2986, 2012.

10 藤井治彦, 鶴岡行雄, 多田好克, “電話網の発信者番号通知を利用した本人認証方式”,情報処理学会論文誌, Vol.54, No.2, pp.992-1001, 2013.

11 H. Fujii, and H. Takei, N. Miyake, and E. Kuwana, Japan Patent 3497799, 2001.

12 H. Fujii, N. Shigematsu, H. Kurokawa, and T. Nakagawa, “Telelogin: a two-factor two-path authentication Technique Using Caller ID,” NTT Technical review, Vol. 6, No. 8, pp. 1-6, 2008.

13 田中充, 勅使河原可海, “携帯電話の 2 次元コード読み取り機能を活用した個人認証方式”, 情報処理学会論文誌, Vol.49, No.7, pp.2425-2439, 2008.

14 D. McCartney, D. Barrera, J. Clark, S. Chiasson, and P. C. van Oorschot, "Tapas: design, implementation, and usability evaluation of a password manager." Proceedings of the 28th Annual Computer Security Applications Conference. ACM, 2012.

15 A. Czeskis, M. Dietz, T. Kohno, D. Wallach, D. Balfanz, "Strengthening User Authentication through Opportunistic Cryptographic Identity Assertions." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, pp. 404-414, 2012.

16 H. Sun, Y. Chen, and Y. Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attack," IEEE Transactions on Information Forensics and Security, vol. 7.2, pp. 651-663, 2012.

17 B. Parno, C. kuo, and A. Perrinng, "Phoolproof phishing prevention," Financial Cryptography and Data Security, pp. 1-19, 2006.

18 S. Suoranta, A. Andrade, and T. Aura, "Strong Authentication with Mobile Phone," Information Security, pp. 70-85, 2012.

19 L. O’Gorman, “Comparing passwords, tokens, and biometrics for user authentication,” Proc. IEEE, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

20 X. Huang, Y Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: preserving security and privacy in distributed systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22.8, pp. 1390-1397, 2011.

21 株式会社 KDDI ウェブコミュニケーションズ, Twilio(オンライン), 入手先 http://twilio.kddi-web.com/ (参照 2013-11-18).

22 Google Inc., 2 段階認証プロセス (オンライン), 入手先 http://www.google.com/landing/2step/#tab=how-it-protects (参照 2013-10-01).

23 サードネットワークス株式会社, Secure Call(オンライン), 入手先 http://www.thirdnetworks.co.jp/sc/03ser02.html(参照 2012-5-24).

24 NTT コミュニケーションズ株式会社, V ポータルダイレクト個人認証ダイヤル(オンライン). 入手先 http://www.ntt.com/v-portaldirect/data/scene_attestation.html (参照 2012-5-24).

25 サイバネットシステム株式会社, Phone Factor(オンライン), 入手先 http://www.cybernet.co.jp/phonefactor/(参照 2012-5-24).

26 Strike Force Inc., Strike Force Commences Patent Litigation against Out-of-Band Authentication Infringers Starting With Phone Factor (a subsidiary of Microsoft), Fiserv & First Midwest Bancorp (オンライン), 入手先 http://www.strikeforcetech.com/pdf/SFOR-OOB-Patent-Litigation-032713.pdf (参照日 2013-11-18).

27 NTT データジェトロニクス株式会社,認証マスター for VPN (オンライン), 入手先 http://www.nttdata-getronics.co.jp/solution/sds/remoteaccess/ninshomaster.html (参照 2012-5-24)

28 株式会社 NTT メディアクロス,空電プッシュ(オンライン), 入手先 http://www.nttmc.co.jp/karadenpush/(参照 2012-5-24).

29 ソフトバンクテレコム株式会社, Synclock(オンライン),入手先 http://www.synclock.jp/08_personal/faq.html/(参照 2012-5-22).

30 NTT ソフトウェア株式会社, CallPassport(オンライン), 入手先 http://www.ntts.co.jp/products/callpassport(参照 2012-5-23).

31 総務省,ブロードバンド・オープンモデルによる地域課題解決支援システムの検証のうち、小・中学校教員の事務軽減支援の実証実験に係る請負, 2011.

32 NTT コミュニケーションズ,電話に向かって話すだけの簡単便利な本人認証～端末認証、音声認識、声紋認証などの技術を組み合わせた VoiceID 技術～(オンライン), 入手先 http://www.ntt.com/ict/library/future/sec_solution.html(参照 2013-04-03).

33 NTT ソフトウェア株式会社, CallPassport/VPN(オンライン). 入手先 http://www.ntts.co.jp/products/callpassport/vpn.html(参照 2013-04-04).

34 European Telecommunications Standards Institute: ETSI TS 133 102 V10.0.0 Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture (3GPP TS 33.102 version 10.0.0 Release 10), 2011.

35 A. Bais, W. T. Penzhorn, and P. Palensky, “Evaluation of UMTS security architecture and services,” IEEE International Conference on Industrial Informatics, pp. 570-575, 2006.

36 江川尚志, 山本浩司, 川口銀河, “NGN におけるネットワーク品質規定とセキュリティ技術”, 電子情報通信学会誌, Vol.89, No.12, pp.1059-1061, 2006.

37 力武健次, 衛藤将史, 鈴木未央, 井上大介, “NGN/IPv6 セキュリティ試験システムの設計と評価”, 電子情報通信学会技術研究報告, IA2009-18, ICSS2009-26, pp.97-102, 2009.

38 事業用電気通信設備規則(平成二三年六月二九日総務省令第七三号)第三十五条の二の三, 第三十五条の七, 第三十五条の十五, 第三十五条の二十二, 第三十六条の八

39 社団法人電気通信事業者協会, 発信者番号偽装表示対策ガイドラインの策定について, 2011.

40 社団法人電気通信事業者協会,異なる電気通信番号の送信の防止に係る省令の取り扱い方針(平成 20 年 4 月 21 日総務省公表)の運用に係るガイドライン第 1 版, 2011.

41 東日本電信電話株式会社,発信者番号表示の偽装防止対策について(オンライン). 入手先 http://www.ntt-east.co.jp/info/detail/sender.html(参照 2012-06-01).

42 株式会社 NTT ドコモ,発信者電話番号表示の偽装防止対策を実施(オンライン). 入手先 http://www.nttdocomo.co.jp/info/news_release/page/20050218.html(参照 2012-06-01).

43 東日本電信電話株式会社,発信者番号を偽装した振り込め詐欺等への注意喚起について(オンライン). 入手先 http://www.ntt-east.co.jp/release/detail/20101119_01.html (参照 2012-5-22).

44 携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律第三条.

45 I. T. Report, ITU Internet Rep. 2006: Digital Life (オンライン), 入手先 http://www.itu.int/ (参照日 2013-04-05).

46 TS 23.040: Technical Realization Short Message Service (SMS) 3GPP(オンライン), 入手先.http://www.3gpp.org/(参照日 2013-04-05).

47 TS 35.202: Specification 3GPP Confidentiality Integrity Algorithms Document 2: KASUMI Specification 3GPP (オンライン), 入手先 http://www.3gpp.org/(参照日 2013-04-05).

48 TS 35.201: Specification 3GPP Confidentiality Integrity Algorithms Document 1: f8 and f9 Specification 3GPP. (オンライン), 入手先 http://www.3gpp.org/ (参照日 2013-04-05).

附表

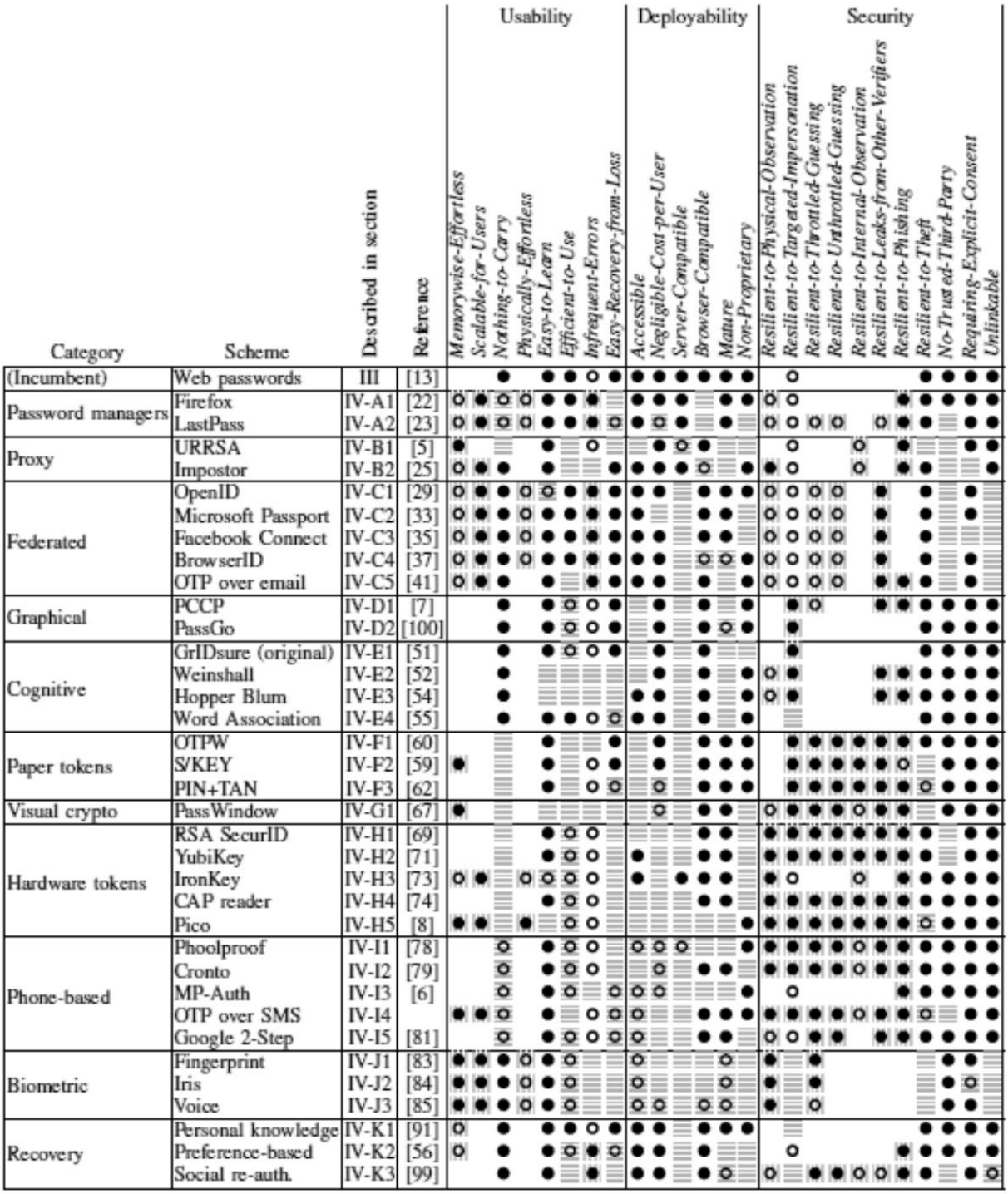
略語一覧

略語	正式名称
FFEIC	Federal Financial Institutions Examination Council;
SMS	Short Message Service
PC	Personal Computer
PIN	Personal Identification Number
IC カード	Integrated Circuit Card
ID	Identification (Data)
HTTP(S)	Hyper Text Transfer Protocol (over Secure socket layer)
HTML	Hyper Text Markup Language
TLS	Transport Layer Protocol
VPN	Virtual Private Network
DTMF	Dual-Tone Multi-Frequency
PHS	Personal Handy phone System
DB	Date Base
IVR	Interactive Voice Response
OSS	Open Source Software
IF	Inter Face
AMI	Asterisk Managed Interface
VM	Virtual Machine
SIP	Session Initiation Protocol
VoIP	Voice over Internet Protocol
AP	Application
PP	Prototype Program
SP	Service Provider
SQL	Structure Query Language
Sar	System Admin Reporter
TTP	Trusted Third Party

SI	System Integration
ASP	Application Service Provider
CTI	Computer Telephony Integration
TL	Telelogin(本システムの開発用の名称)
JDBC	Java Data Base Connectivity
バーチャル IP	Virtual Internet Protocol (Address)
LAN	Local Area Network
GINA	Graphical Identification and Authentication
Radius	Remote Authentication Dial In User Service
AKA	Authentication and Key Agreement
SIM	Subscriber Identity Module
3G	3rd Generation
TCA	Telecommunications Carriers Association
URL	Uniform Resource Locator

Bonneau らによる UDS 評価

以下に、Bonneau らによる本人認証技術の評価結果を示す[3, 9]。



Category	Scheme	Described in section	Reference	Usability: *Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	Deployability: *Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	Security: *Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A1	[22]	○	●	○	○	●	●	●		●	●	●		●	●	○	○					●	●	●	●	●
	LastPass	IV-A2	[23]	○	●	○	○	●	●	●	○	●	○	●		●		○	○	○	○		○	●	●		●	●
Proxy	URRSA	IV-B1	[5]	●				●		○			●	○	●				○			○		●			●	●
	Impostor	IV-B2	[25]	○	●	●		●			●	●	●	●	○		●	●	○			○		●	●			●
Federated	OpenID	IV-C1	[29]	○	●	●	○	○	●	●	●	●	●		●	●	●	○	○	○	○		●		●		●	
	Microsoft Passport	IV-C2	[33]	○	●	●	○	●	●	●	●	●	●		●	●		○	○	○	○		●		●		●	
	Facebook Connect	IV-C3	[35]	○	●	●	○	●	●	●	●	●	●		●	●		○	○	○	○		●		●			
	BrowserID	IV-C4	[37]	○	●	●	●	○	●	●	●	●	●		○	○	●	○	○	○	○		●		●			
	OTP over email	IV-C5	[41]	○	●	●		●		●	●	●	●		●		●	○	○	○	○		●	●	●		●	
Graphical	PCCP	IV-D1	[7]			●		●	○	○	●		●		●		●		●	○			●	●	●	●	●	●
	PassGo	IV-D2	[100]			●		●	○	○	●		●		●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E1	[51]			●		●	○	○	●		●		●				●						●	●	●	●
	Weinshall	IV-E2	[52]			●							●		●		●	○	●				●	●	●	●	●	●
	Hopper Blum	IV-E3	[54]			●						●	●		●		●	○	●				●	●	●	●	●	●
	Word Association	IV-E4	[55]			●		●	●	○	○	●	●		●										●	●	●	●
Paper tokens	OTPW	IV-F1	[60]					●					●		●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY	IV-F2	[59]	●				●		○	●		●		●	●	●		●	●	●	●	●	○		●	●	●
	PIN+TAN	IV-F3	[62]					●		○	○		○		●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow	IV-G1	[67]	●									○		●	●		○	●	●	●	○	●	●		●	●	●
Hardware tokens	RSA SecurID	IV-H1	[69]					●	○	○					●	●		●	●	●	●	●	●	●		●	●	●
	YubiKey	IV-H2	[71]					●	○	○		●			●	●		●	●	●	●	●	●	●		●	●	●
	IronKey	IV-H3	[73]	○	●		○	○	○	○		●		●	●	●		●	○			○		●	●	●	●	●
	CAP reader	IV-H4	[74]					●	○	○					●	●		●	●	●	●	●	●	●	●	●	●	●
	Pico	IV-H5	[8]	●	●		●		○	○							●	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-I1	[78]				○	●	○	○		○	○	○			●	●	●	●	●	○	●	●	●	●	●	●
	Cronto	IV-I2	[79]				○	●	○	○			○		●	●		●	●	●	●	○	●	●	●	●	●	●
	MP-Auth	IV-I3	[6]				○	●	○		○	○	○				●		○					●	●	●	●	●
	OTP over SMS	IV-I4		●	●		○	●		○	○	○			●	●	●	●	●	●	●	○	●	●	○		●	●
	Google 2-Step	IV-I5	[81]				○	●	○	○	○	○			●	●		○	○	●	●		●	●	●	●	●	●
Biometric	Fingerprint	IV-J1	[83]	●	●	●	○	●	○			○					○	●			●						●	
	Iris	IV-J2	[84]	●	●	●	○	●	○			○					○	●			●						●	○
	Voice	IV-J3	[85]	●	●	●	○	●	○			○	○			○	○	●			○						●	
Recovery	Personal knowledge	IV-K1	[91]	○		●		●	●	○	●	●	●		●	●	●								●	●	●	●
	Preference-based	IV-K2	[56]	○		●		●	○	●	○	●	●		●				○					●	●	●	●	●
	Social re-auth.	IV-K3	[99]			●		●		●		●	●		●	○		○		●	●	○	○	●	●		●	○

●= offers the benefit; ○= almost offers the benefit; *no circle* = does not offer the benefit.
|||= better than passwords; ≡= worse than passwords; *no background pattern* = no change.
We group related schemes into categories. For space reasons, the peer-reviewed paper [1] describes at most one scheme per category, but this tech report discusses them all.

関連論文の印刷公表の方法及び時期

論文誌

藤井治彦，鶴岡行雄，多田好克. "電話網の発信者番号通知を利用した本人認証方式"，情報処理学会論文誌 54.2 (2013): 992-1001.(主に本論文の第３章及び４章に関連)

査読付き国際会議

Haruhiko Fujii, and Yukio Tsuruoka, "Three-factor user authentication method using biometrics challenge response", Financial Cryptography and Data Security (2013). (主に本論文の第５章に関連)

Haruhiko Fujii, and Yukio Tsuruoka, “SV-2FA: Two-Factor User Authentication with SMS and Voiceprint Challenge Response”, International Conference for Internet Technology and Secured Transactions (2013). (主に本論文の第５章に関連)

参考論文等の印刷公表の方法及び時期

参考論文等

題目「携帯電話を用いた匿名購入システム」

印刷公表の方法及び時期

平成 14 年 FIT(情報科学技術フォーラム) 一般講演論文集

題目「電話網の発信者番号通知を利用した本人認証方式」

印刷公表の方法及び時期

平成 24 年 Programming Tools and Techniques 第 387 回

題目「携帯電話を用いた匿名購入システム」

印刷公表の方法及び時期

平成 14 年 FIT(情報科学技術フォーラム) 一般講演論文集

題目「テレログイン方式の概要」

印刷公表の方法及び時期

平成 18 年 (財)金融情報システムセンター,地域金融機関 IT 研究会報告書

題目「携帯電話を用いた認証方式―個体識別情報送信機能を用いた試み」

印刷公表の方法及び時期

平成 14 年 Cyber Security Management

題目「Telelogin: a Two-factor Two-path Authentication Technique Using Caller ID」

印刷公表の方法及び時期

平成 20 年 NTT Technical Review, Vol.6, No.8

関連特許

藤井治彦,中川哲也,”ユーザ認証方法、ユーザ認証システム、ユーザ認証装置及びユーザ認証プログラム”,中華人民共和国特許第 752764 号,2007. (主に本論文の第 3 章に関連)

藤井治彦,中川哲也,畑恵介,重松直子,”カード利用処理システム、カード利用処理装置、カード利用処理方法及びカード利用処理プログラム”, 特許第 4634422 号,2009. (主に本論文の第 3 章に関連)

藤井治彦,中川哲也, “ユーザ認証方法、ユーザ認証システム、ユーザ認証装置及びユーザ認証プログラム”, 特許第 4813273 号,2008. (主に本論文の第 3 章に関連)

藤井治彦,中川哲也, “ユーザ認証方法、ユーザ認証システム、ユーザ認証装置及びユーザ認証プログラム”, 特許第 4813272 号,2008. (主に本論文の第 3 章に関連)

藤井治彦,三宅延久,武井英明,桑名栄二, “ユーザ認証方式”,特許第 3497799 号,2001. (主に本論文の第 4 章に関連)

藤井治彦,中川哲也,畑恵介,重松直子,”認証処理システム、認証装置、認証処理方法及び認証処理プログラム”, 特許第 4750765 号,2009. (主に本論文の第 4 章に関連)

藤井治彦,中川哲也, 畑恵介, "電話番号によるブラウザフォン認証方式、電話番号によるブラウザフォン認証システム、ブラウザフォン認証サーバ、電話番号によるブラウザフォン認証プログラム、サービス提供方法、サービス提供システム、サービス提供サーバ及びサービス提供プログラム”, 特許第 4422194 号,2007. (主に本論文の第 4 章に関連)

藤井治彦,池田紀務,新井克也,花木三良,”ブラウザフォンのメールによるユーザ認証方法、ユーザ認証サーバ、認証サーバのユーザ認証方法、及び認証サーバのユーザ認証プログラム並びにそのプログラムを記録した記録媒体”, 特許第 3820477 号,2004. (主に本論文の第 5 章に関連)

藤井治彦,塩野入理,”インターネットアクセス機能を持つ携帯装置を用いたユーザ認証システム及びそのユーザ認証装置”，特許第 3704318 号,2003.（主に本論文の第 5 章に関連）

藤井治彦,塩野入理,“ブラウザフォンのメールによるユーザ認証方法、ユーザ認証サーバ、認証サーバのユーザ認証方法、及び認証サーバのユーザ認証プログラム、そのプログラムを記録した記録媒体”．特許第 3670613 号,2003.（主に本論文の第 5 章に関連）

謝辞

本研究の過程において、終始懇切なる御指導と御鞭撻を賜り、本論文をまとめるに際して、親身な御助言と力強い励ましを頂いた、多田好克教授に、心より感謝を申し上げます。鶴岡行雄教授、小宮常康准教授、荒堀喜貴助教におかれましては、学会原稿作成時や発表時等、多くの有益な御助言を頂き、深謝申し上げます。

多田研究室と小宮研究室のメンバは、社会人学生である私の立場をご理解、ご協力いただき、御礼申し上げます。

本論文の審査過程において、数々の御助言と御指導を賜りました、大森匡教授、本多弘樹教授、森田啓義教授、古賀久志准教授に深謝申し上げます。

この挑戦に賛同し、協力していただいた NTT セキュアプラットフォーム研究所の上司の皆様である高橋克己様、冨士仁様、三好潤様、清水敏之様、NTT アイキューブ桑名栄二様､本論文の製品化にご尽力くださった NTT コミュニケーションズ中川哲也様、及び NTT ソフトウェア、NTT データ先端の方々に謹んで感謝の意を表します。

最後に、陰ながら応援してくれた淡路島の家族に感謝いたします。