別紙 1

論文の内容の要旨

論文題目	二経路多要素による本人認証方式の研究
学位申請者	藤井治彦

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。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。提案方式は、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。

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。

そこで、まず、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。上で示した課題の内、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、たと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れなければ、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。

次に、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。上述の残された課題のうち、中間者攻撃に対する脆弱性は、たと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を可能として解決する。盗難に対する脆弱性は、たと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。

それを受けて最後に、SMSによって毎回変わるコールバック先を通知し、コールバック時、着信番号認証の後に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、上述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であるなどが挙げられる。

論文審査の結果の要旨

学位申請者氏名　藤井　治彦

審査委員主査　多田　好克

委員　大森　匡

委員　本多　弘樹

委員　森田　啓義

委員　古賀　久志

委員　鶴岡　行雄

第１章では、本研究の背景および研究の意義が論じられた。ネットバンク等に対するサイバー攻撃は近年増加しており、ワンタイム・パスワードなど従来の本人認証技術では解決できない攻撃が増加している。一方、携帯電話を利用して本人認証を行う二経路認証が普及してきている。これは従来技術の経済性・利便性を改善するが、依然、中間者攻撃など解決できない問題がある。本研究が従来と最も異なる点は、本人を特定する情報である認証識別子をインターネットとより安全な電話網を通して送信することにより、従来技術では実現困難であった、安全性・経済性・利便性を同時に満たせることについて示された。

第２章では、二経路認証技術の位置づけ、および課題について示された。二経路認証は、所有物認証技術に属し、従来の所有物認証の課題であった、トークンの初期配布コストが改善されるが、ソーシャル・エンジニアリングや中間者攻撃などに対する脆弱性や、携帯電話自体が盗まれたり、マルウェア感染した場合の脆弱性があることが示された。また関連研究、周辺技術、特許についても概観された。

第３章では、ワンコールでワンタイム電話番号を伝え、これにコールバックする方式と、そのプロトタイプの評価等について述べられた。音声のみで実現することにより、SMSやアプリに伴う課題を解決するが、ソーシャル・エンジニアリングによる転送設定の不正変更と、発信者番号偽造が同時になされると、なりすまされる脆弱性があることについて述べられた。また、プロトタイプの試作や評価実験など、実用化に向けての検討の概要についても言及している。

第４章では、発信者番号認証及び声紋認証による方式、および事業化システムの概要について述べられた。発信者番号偽造対策された国での利用を前提条件する代わりに、実用性の高い方式となった。中間者攻撃対策として、音声ガイダン

スで取引内容を確認させる手法をとっている。また携帯電話が盗まれても、声紋認証で防止できることについて示された。初期登録など運用面の方式についても論じられた。２件の事業化実績についても概要が述べられた。

第５章では、発信者番号認証を利用せず、SMSとワンタイム電話番号を利用して、本人認証する方式について論じられた。本方式は、さらに利用者の否認を防止するため宣誓の録音が可能となっている。生体認証は一般的に、生体情報をコピーして再利用されるリプレイアタックが課題となるが、宣誓文に毎回変わる内容をいれることによりこれを防御する。また、クライアント証明書を利用することにより利便性の向上がなされている。しかし、課題として、さらなる利便性の改善、通信コストの改善、電話会社がTTP（Trusted Third Party）でなければならない課題などが示された。

第６章では、結論として１章、２章、３章、４章、５章で得られた知見がまとめられた。ネットバンク等に対するサイバー攻撃は、従来技術での防御は困難であり、また他の二経路認証技術も安全性の課題があった。本研究方式により、フィッシング攻撃を初め、中間者攻撃、携帯電話盗難、リプレイ攻撃、ソーシャル・エンジニアリングなどが防御でき、さらに正当な利用者の否認まで防止できる。第４章で議論された方式では発信者番号を利用するため日本国内でしか利用できなかったが、第５章では世界対応可能な方式についての提案がなされた。

以上のような内容に鑑み、本論文は博士（工学）の学位請求論文として十分な価値を有すると判定した。