様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２０　日現在

機関番号：　１２５０１
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００１８１

研究課題名（和文）安全性と利便性を備えたOTP認証システム

研究課題名（英文）Secure OTP authentication system with user-friendliness

研究代表者
多田　充（Tada, Mitsuru）

千葉大学・統合情報センター・准教授

研究者番号：２０３０３３３１

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：現在運用されている多くのネットワーク上のシステムはユーザが設定したパスワードによる認証を採用しているものが多い。安全性向上のためOTP認証を採用するとしても，システムを稼働したまま修正し設定し直すのは困難である。そのため，所有物認証を行うセンターを導入し，既設のパスワード認証システムをOTP認証システムに拡張することを考えた。
まず，ユーザがログインする際，センターがサービスシステムの認証機能を起動させた後に従来のパスワード認証が可能となるような認証の強化策を示し，後に，パスワード認証を，システムへの改変を最小限に抑えつつ，所有物とパスワードの2要素によるOTP認証に拡張する方法を示した。

研究成果の概要（英文）：Among service systems running in a network, many ones adopt authentication with passwords determined by the users. Even to enable OTP authentication to enhance security, it is quite hard to modify and reset the system keeping running. Thereby we suppose to extend existing password authentication systems to OTP authentication systems by adding a center which does possession (WYH) authentication.
First, we have shown how to enhance password authentication, in which the center switches the authentication on and then usual password authentication is possible when a user tries to log-in. After that, we have shown how to construct OTP two-factor authentication with keeping modification to the original password authentication system to a minimum.

研究分野：　情報セキュリティ

キーワード：　ワンタイムパスワード　2要素認証

１．研究開始当初の背景

ネットワーク上のサービスシステムにおけるユーザ認証の手段として，最も普及している「ユーザ ID とパスワードによる認証」は，そのパスワード設定をユーザ自身に委ねている。しかも，適切なパスワード管理の煩わしさや困難さから，安易なパスワードを設定したり，複数のサービスシステムに対して同一のパスワードを設定したりしているユーザが少なくない。ユーザが使用するブラウザ等を乗っ取り，ユーザの入力内容や，システムからの通知内容を改ざんする MITB 攻撃を考慮しなければ，上記の問題を解決する方法として広く普及しているのは「ワンタイムパスワード(OTP)認証」である。確かに，安全性の側面において，OTP 認証は固定パスワードに比べ優位ではあるであるが，その最大の問題点は「ユーザの利便性」にある。OTP 認証として現在最も広く普及しているのは「ハードトークン」を用いた方法であるが，その安全な配付，ユーザによるトークンの紛失，コード漏洩による回収・再配布など，運用コストは決して低くない。さらに，ハードトークンによる方法の場合，その OTP 生成プログラム(生成ロジック)が漏洩すると，システム全体の安全性を脅かすものとなり，しかも，そのシステム全体を脅かす恐れのあるものを全ユーザに配付しなければならない。

２．研究の目的

本課題では，安全性だけではなく，利便性の上でも，従来の固定パスワード認証に替わりうる OTP 認証システム(プロトコル)の構築，実装・安全性解析・脅威分析を目指すものである。さらに，近年猛威を奮っている MITB についても，OTP 認証システムのアイデアを活かし，その問題を解決するプロトコルを構築・実装・安全性解析・脅威分析を行う。

３．研究の方法

我々の研究グループが論文発表している OTP 認証システムについて，ユーザの利便性を損なうことなく，実際の運用で起こりうる問題(携帯電話機器の機種変更，ユーザが記憶情報を忘れること)に対応できるシステムを構築するにあたり，特に，ユーザが所有する携帯機器に対する変更手続きや，紛失・盗難等からの救済処置が円滑にできるよう改良する。

さらに，MITB 対策に対しては，一般に 2 経路認証と呼ばれる方法を採用し，そのプロトコルを構築する。

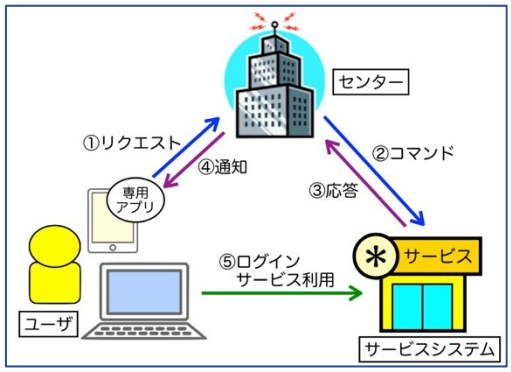
４．研究成果

まず，我々が研究対象としている 3 者間認証プロトコルは，ユーザ，(ユーザが利用する)サービスシステム，および，(一般的には，複数の)サービスシステムに接続するセンターを，その登場エンティティとして持つ。さらに，ユーザはサービスシステムを利用するための(PC などの)端末，および，センターにアクセスするための(スマートフォンなどの)携帯機器を使用する。プロトコル構築の際は，2 種類の機器を登場させるが，実際の利用の際は，携帯機器でサービスシステムを利用してもよい。

ユーザがサービスシステムを利用(ログイン)するとき，(1)ユーザはセンターに対してサービスシステム利用のリクエストを行う。(2)センターは利用対象となるサービスシステムに通知し，(3)センターはサービスシステムからの応答を得る。(4)センターはその応答をユーザの携帯機器に通知し，(5)ユーザはその通知に従い，サービスシステムを利用する。

我々のシステムでは，(1)の際に，ユーザに対して，(携帯機器の)所有物認証を含む 2 要素認証を実施する。最も簡単な方法は，パスワード等の記憶認証と合わせるものである。(5)の利用の際，サービスシステム独自で認証を実施してもよい。

以上をまとめると下図のようになる。



本課題を開始した平成 27 年度は，まず，パスワード認証を強化すべく，すでに設置されているパスワード認証を採用しているサービスシステムに，所有物認証に分類される「認証シャッター」を追加する方法を提案した。認証シャッターそのものは，平成 26(2014)年度，高田により提案されているが，本成果によるものは，ユーザおよびサービスシステムの他にシャッター制御センターを合わせた 3 者間認証になっており，シャッターを 開けるためには，ユーザはシャッター制御センターに対して記憶および所有物の 2 要素認証をパスする必要がある。そのため，

シャッターを開けてログインしたユーザ本人の確からしさ（認証レベル)を上げることができ，より安全にサービスシステムを運用できるようになる。本成果は「学術情報処理研究 第19巻」に採録された。また，ユーザの利便性を向上させるため，ユーザが所有物認証を行うための携帯端末の機種変更を円滑に行う方法について，情報処理学会第 72 回コンピュータセキュリティ(CSEC)研究会で発表した。

平成 28 年度は，既設のパスワード認証システムを 3 者間 OTP 認証システムに拡張する方法について，2 通りの可能性を考慮し，研究を行った。具体的には，ユーザが既に複数のサービスシステムに登録されている状態で，それらのサービスシステムをまとめるセンターを構築する場合，および，ユーザ情報を保有するセンターが，それに接続するサービスシステムに，ユーザを登録させる場合，である。これまで我々の研究グループが発表してきた基本的なアイデアにおいては，前者を想定していたが，大学等の組織においては，むしろ後者の方が起こりうると考え，後者の状況を前提とした OTP 認証システムを設計した。その研究成果は「学術情報処理研究 第20巻」に採録された。

平成 29 年度は，研究背景および研究目的にも述べている MITB 対策の実施を目指した。また，平成 27 年度に発表した「携帯端末の機種変更方法」(〔学会発表〕の文献 1)における問題点を指摘し，その改良方法を構築した。

MITB 対策は，ユーザがログイン認証を行った後，サービスシステムに何かしらのリクエストを送ったときに必要となるものである。基本的なアイデアについては平成 27 年に特許取得しているが，実際の構築については課題も多かったが，最終的には，その技術を用いて製品開発を目指せるようになった。

携帯機器の機種変更方法については，既発表では，機器固有情報で暗号化されているデータを，(携帯電話の契約者情報，利用 ID のような)ユーザ固有の情報を鍵として暗号化したものに変換し，別途設置される保管システムに預けるというものであったが，当年度は，秘密分散法を用いた鍵の構成法を行った。具体的には，データを暗号化する際に用いる鍵を，既発表のように機器固有情報のみ(または，それから導出される値)にするのではなく，機器固有情報(I)，ユーザ固有情報(C)から，暗号化から定まる値(Key)にし，それに伴いもう 1 つのパラメータ(K)を算出しておく。Key は，(I,C,K)のうち，2 つ分かれば導出することができるようにする。(つまり，(2,3)-閾値秘密分散法となる。)ユーザは K をセンターに預けておく。ユーザは，その携帯機器の中で I および C を入手できKey を算出できるので，データを復号することができるが，センターは，たとえ暗号化されたデータ(E)が漏洩しても，K しか知り得ないため，Key を算出することはできず，データを入手することができない。

携帯機器の変更の際は，ユーザは機器データのバックアップ(B)をとっておく。さらに，サービスシステムに対して予め定められた認証を行い，センターから K を送ってもらう。サービスシステムから K を受け取ったユーザは，C および K から Key を復元し，E を復号する。

K だけでなく B もセンターに預けることも可能であり，この場合は，ユーザがバックアップを取る必要がない。

なお，I および C は，ユーザが設定できる値ではなく，I および C から Key は一意的に決まる。そのため，一旦 Key が漏洩すると機種を変更するしかない。そのため，ユーザがパスワード(P)や，ランダムな値(R)を定め，それらも併せて Key を決定することも可能である。この場合，I,C,P,R から Key を決定，Key から求まる K を算出し，(I,C,P,R,K)のうち 4 つ分かれば Key を復元できるようにし，センターには R および K を預ける。ユーザは，機種変更の際，ユーザ固有情報の C,自身で設定したパスワード P，センターからサービスシステム経由で渡された(R,K)を用いて Key を復元し，E を復号する。なお，以上の手法に関しては，平成 30 年に特許出願を行っている。

我々が対象としている 3 者間認証システムにおいては，ユーザの携帯機器の変更が，最もユーザに煩わしさをもたらすものであると考えているため，その手続きを簡単にすることは，その実現に大きく貢献することになると思われる。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

1. 多田充:「ユーザ負担を考慮したワンタイムパスワード認証システム」，学術情報処理研究 (ISSN1343-2915)，no.20，pp.97-104，2016.
2. 多田充:「パスワード認証の強化策」，学術情報処理研究 (ISSN2188-9511)，no.19，pp.40-49，2015.

〔学会発表〕（計 2 件）

1. 糸井正幸，多田充:「ワンタイムパスワード認証システムの利便性について」，第 72 回情報処理学会コンピュータセキュリティ

(CSEC)研究会，2016 年 3 月 4 日，明治大学．

2． 多田充:「パスワード認証の強化策」，第 19 回学術情報処理研究集会，2015 年 9 月 28 日，豊橋技術科学大学．

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計 3 件）

1．
名称：機器内の情報を移行するシステム及び方法
発明者：多田充，糸井正幸
権利者：千葉大学，株式会社セフティーアングル
種類：特許権
番号：特願 2016-025767
出願年月日：平成 28 年 2 月 15 日
国内外の別： 国内

2．
名 称 ： Server system and method for controlling plural service systems
発明者：Mitsuru Tada，Masayuki Itoi
権利者：千葉大学，株式会社セフティーアングル
種類：特許権
番号：15/531003，PCT JP2015/82991
出願年月日：平成 27 年 11 月 25 日
国内外の別： 国外

3．
名称：複数のサービスシステムを制御するサーバシステム及び方法
発明者：多田充，糸井正幸
権利者：千葉大学，株式会社セフティーアングル
種類：特許権
番号：特願 2016-561901
出願年月日：平成 27 年 11 月 25 日
国内外の別： 国内

○取得状況（計 2 件）

1．
名称：サーバシステム及びリクエスト実行制御方法
発明者：多田充，糸井正幸
権利者：千葉大学，株式会社セフティーアングル
種類：特許権
番号：特許第 5770354 号
取得年月日：平成 27 年 7 月 3 日
国内外の別： 国内

2．
名称：複数のサービスシステムを制御するサーバシステム及び方法
発明者：多田充，糸井正幸
権利者：千葉大学，株式会社セフティーアングル
種類：特許権
番号：特許第 6199506 号
取得年月日：平成 29 年 9 月 1 日
国内外の別：国内

〔その他〕
ホームページ等
該当なし

６．研究組織
(1)研究代表者
多田 充（Mitsuru Tada）
千葉大学 統合情報センター 准教授
研究者番号：20303331

(2)研究分担者
(該当なし)

(3)連携研究者
(該当なし)

(4)研究協力者
糸井 正幸（Masayuki Itoi）
株式会社セフティーアングル 代表取締役