漏えいに強いパスワード認証とその応用

―― 短いパスワードを許容しながら情報漏えい耐性を実現 ――

古原 和邦*、辛 星漢

パスワードはネットワーク上のユーザーを確認し、そのユーザーとの間に暗号化通信路を作成する遠隔ユーザー認証や、ファイルの暗号化等の用途で広く利用されている。しかし、パスワードには、それが盗まれ悪用されるセキュリティ上の問題や、長いパスワードを複数覚えられない利便性の問題があり、それらの改善が求められている。この研究の目的は、これらの問題を解決する新たな方式を考案、実用化し、社会に提供することにある。この論文において、この目的を達成するために取り組んだ研究の戦略と道筋について紹介する。

キーワード：認証、鍵管理、パスワード、フィッシング詐欺、クラウド

Secure password authentication schemes and their applications

– How to achieve security with short passwords –

Kazukuni KOBARA* and SeongHan SHIN

Passwords are widely used for encrypting files, authenticating remote users on a communication network, and establishing encrypted channels for authenticated users. However, the possibility of passwords being stolen or abused raises security problems, and having to remember a number of lengthy passwords is often inconvenient. The purpose of this research is to develop new schemes to resolve these problems and make them generally available to society. In this paper, we introduce our research strategies and scenario to achieve this purpose.

Keywords：Authentication, key management, password, phishing, cloud

1　はじめに

1.1　背景

パスワードはネットワーク上のユーザーを確認し、そのユーザーとの間に暗号化通信路を作成する遠隔ユーザー認証や、ファイルの暗号化等の用途で広く利用されている。しかし、パスワードには、それが盗まれ悪用されるセキュリティ上の問題や、長いパスワードを複数覚えられない利便性の問題があり、それらの改善が求められている。

一方、個人を特定する方法としては、パスワード以外に、生体情報や所有物等を利用する方法も存在する。しかし、生体認証には、人工物を使った成りすましや識別能力の低さ、人工物を検出するために特別な装置を必要とするなどの問題点[1]があり、それらを改善するための研究が現在も進められている。所有物認証は、盗まれたり拾われたりした場合の悪用を防止するために、パスワード等と組み合わせる必要があり、必ずしもパスワードの代替とはなっていない。ファイルの暗号化方式にもパスワードの代わりに暗号鍵を使う方式が存在するが、その復号鍵を保護するためにパスワードが必要となる。以上のように、パスワード以外の情報を使う方式も存在してはいるが、現在のところパスワードを完全に置き換えるには至っていない。そこでこの研究では、パスワードを扱う方式自体を改良することにより、パスワードの抱える問題の解決を目指す。

パスワードのセキュリティ上の問題に関しては、警察庁が公表した統計データ[2]を図1に示しておく。ここで、「パスワードの設定・管理の甘さ」とは、推測され易いパスワードが利用されていたために、全数探索等によりパスワードが求まったことを意味し、「元従業員や知人等」とはサーバーの管理者等、被害者のパスワードを知り得る立場にあった者の犯行を意味する。前者については1.2節でもう少し詳しく解説する。後者については、最近では関係者でなくともサーバーからの漏えい情報を使うことによりパスワードを

産業技術総合研究所　セキュアシステム研究部門　〒305-8568 つくば市梅園1-1-1 中央第2
Research Institute for Secure Systems (RISEC), AIST　Tsukuba Central 2, 1-1-1 Umezono, Tsukuba 305-8568, Japan　＊E-mail: kobara_conf-ml@aist.go.jp

Original manuscript received October 24, 2013, Revisions received January 14, 2014, Accepted April 3, 2014

表1　パスワードを用いた遠隔ユーザー認証方式の比較

	認証方式	パスワード全数探索への耐性				フィッシング詐欺への耐性	パスワードの数
		盗聴や成りすましに対して	記録情報が漏洩した場合				
			クライアント側から	サーバ側から	時間差で両方から		
1要素認証	パスワードのみを使う従来のプロトコル	×	○	×	×	×	複数
1要素認証	PAKE	△	○	×	×	○	複数
2要素認証	PKI サーバ認証 +PW	△	○	×	×	×	複数
2要素認証	PKI サーバ認証 +PW+OTP	○	○	×	×	×	複数
2要素認証	PKI（相互認証）	○	×	○	×	△	一つ
2要素認証	LR-AKE（本研究）	○	○	○	○	○	一つ

知り得る立場になり得ることが問題となっており、この問題点について 1.3 節で解説する。「聞き出した又はのぞき見た」、「パスワードの設定・管理の甘さ」などへの対策としては、利用者への注意喚起に加えて、パスワード以外の情報も併用する 2 要素認証を導入することが推奨されている。しかし、2 要素認証が広まった場合には、クライアント端末の紛失・盗難への耐性も重要となるため、この問題点について 1.4 節で解説する。そして、最後に 1.5 節でフィッシング詐欺の問題について解説する。

また、パスワードを用いた遠隔ユーザー認証方式の比較を表 1 にまとめておく。表中の一番左の列は方式を表しており、大きくパスワードのみを用いる 1 要素認証と、パスワードと記録情報を用いる 2 要素認証に分けることができる。なお、これらの方式は単にユーザーを認証するだけでなく、ユーザーとの間に暗号化通信路を設立する機能も持ち合わせていることに注意する。各方式の概要について簡単に説明すると、「PKI（Public-Key Infrastructure）サーバー認証 +PW」、「PKI サーバー認証 +PW + OTP」は、サーバーに公開鍵秘密鍵対を持たせ、その公開鍵を用いてクライアント端末とサーバーとの間で暗号化通信路を設立し、その暗号化通信路を使いユーザーの PW（Password）や OTP（One-Time Password）をサーバーに渡す方式である。サーバーの公開鍵をユーザーが管理すべき認証情報と考えれば 2 要素認証となり、ユーザーが管理しなくてよい情報と考えれば 1 要素認証となる。多くの場合、後者で運用されており、これがフィッシング詐欺を受け入れる技術的要因の一つとなっている。この問題点については 1.5 節において解説する。パスワードのみを使う 1 要素認証は、「パスワードのみを使う従来のプロトコル」と「PAKE（Password Authenticated Key Exchange）」に分類できる。前者には、通信路の盗聴や成りすましに弱いという問題点があったが、これを解決したのが PAKE である。ただし、これらの方式はユーザーを認証するためにパスワードあるいはそのハッシュ値（パスワードを加工した値）をサーバーに置かなければならず、その漏えいに弱いという問題がある。さらに、ユーザーが同じパスワードを複数のサーバーで使い回していた場合、あるサーバーの問題により漏えいしたパスワードが、他の落ち度のないサーバーやサービスへのログインに利用できてしまう。この問題を防ぐには、ユーザーにサービス毎に異なるパスワードを設定してもらう必要があり、表 1 の最後の列に示すようにユーザーは複数のパスワードを覚えなければならない。

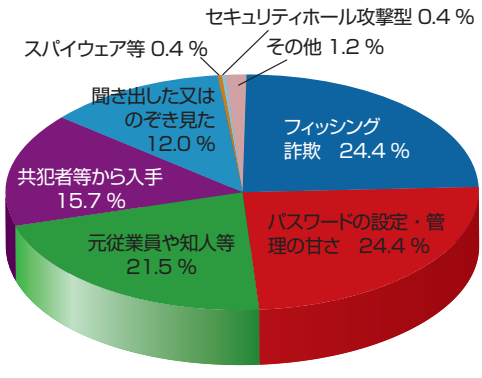

図1　パスワード入手の手口

サーバーからの漏えいに強い方式としては、PKI 相互認証がある。この方式はサーバーとユーザーの両方に公開鍵秘密鍵対を持たせ、サーバーにはユーザーの公開鍵（あるいはその関連情報）が置かれる。そのため、サーバーから情報が漏えいしたとしても成りすましに必要となる秘密鍵を得ることができない。しかし、この方法はクライアント側に秘密鍵を置くため、クライアント側からの情報漏えいに弱くなる。この問題については 1.4 節で解説する。LR-AKE（Leakage-Resilient Authenticated Key Establishment）はこの研究により考案し実用化を行った方式であり、利用

者は一つの短いパスワードを利用しつつ、盗聴、成りすまし、サーバーとクライアントのいずれからもの記録情報の漏えい、フィッシング詐欺等への耐性を持つ。

以下の節では上述の各問題点と表 1 の 2 列目以降について説明する。

1.2　パスワードの全数探索に対する脆弱性

パスワードの全数探索への耐性を高める最も基本的な方法は、ランダムに選択した非常に長いパスワードを利用することにある。しかし、この方法は利便性を大幅に低下させるため実用的でない。そこで、人間が負担なく覚えられる範囲内の短いパスワードを利用しながら、全数探索への耐性を高めることを考える。これは、一見矛盾した問題のように見えるが、パスワードの全数探索が、オフライン全数探索、並列オンライン全数探索、直列オンライン全数探索に分類でき、これらの能力に差があることを理解できれば解も見えてくる。

ここで、オフライン全数探索とは通信の盗聴等により得たデータを使い、サーバーに接続することなくパスワードを試す方法である。例えば通信路に乱数 c と r=h（c,pw）により計算された r が流れ、関数 h（）が公開でパスワード pw のみが秘密である場合、それらを盗聴した攻撃者は、パスワードの候補 pw' を使って r'=h（c,pw'）を計算し、r=r' が成立するかを確認することにより、pw' が正しいパスワードであるか否かを検証できる。試せるパスワードの数は計算能力の向上に比例して年々大きくなり、サーバーの設定により制限されることはないため、非常に強力な攻撃方法となる。

オフライン全数探索に対して十分な安全性を確保できる鍵の長さとして米国国立標準技術研究所（NIST: National Institute of Standards and Technology）は 2010 年までは 80 ビット以上、2011 年から 2030 年までは 112 ビット以上、2031 年以降は 128 ビット以上の利用を推奨している [3]。これらは、ランダムに選択された英数大小文字のパスワードの長さに換算するとそれぞれ 14 桁、19 桁、22 桁に相当する。実際、これらの見積もりを踏まえ、ファイル暗号化ソフト等では 20 桁以上のパスワードの使用を推奨している [4]。一方、人間が負担なく記憶できるパスワードの長さは 7 ± 2 桁程度 [5] と言われており、もはやオフライン全数探索には耐えられない長さとなっている。

これに対して、並列オンライン全数探索と直列オンライン全数探索では、サーバーと認証プロトコルを実行し、入力したパスワードが受け入れられるか否かを検証する方法である。一つのアカウントに対して一つ一つパスワードを試す方法が直列オンライン全数探索であり、それを複数のアカウントに対して並列で行うのが並列オンライン全数探索である。これらはいずれもサーバーに接続しなければパスワードを試せないため、サーバー側で一定時間内に試せるパスワードの数を制限することにより、計算量能力の向上とは無関係にパスワード全数探索リスクを抑えることができる。

つまり、パスワードを扱う方式に対してどのタイプの全数探索を適用できるかにより、安全に使えるパスワードの長さが変わってくる。表 1 のパスワード全数探索への耐性の列は、オフライン全数探索が適用可能な場合を×、並列オンライン全数探索が適用可能な場合を△、いずれも適用不可な場合を○としている。記録情報が漏えいした場合については 1.3 節と 1.4 節で説明するが、漏えいが起きていない場合においても、「パスワードのみを使う従来のプロトコル」の場合、通信路を盗聴するだけでオフライン全数探索を適用可能であり、「PAKE」、「PKI サーバー認証 + PW」の場合、誰でもパスワードを試せるため、複数のアカウントに対して並列にオンライン全数探索を掛けることができる。「PKI サーバー認証 + PW + OTP」、「PKI 相互認証」、「LR-AKE」の場合、クライアント側のパスワード以外の認証情報を入手できなければパスワードの正しさをオンラインで確認できないため、オンライン全数探索すら適用できない。

1.3　サーバー側からの情報漏えいに対する脆弱性

通常、サーバーは専門の管理者により厳重に管理され、情報漏えいは起こり難いと考えられていた。しかし、ここ数年だけを見てもサーバーからの情報漏えい事件は度々起こっており、起らないと仮定する方が難しくなってきている。ここ 2、3 年に起きた代表的なサーバー側からの情報漏えい事件を表 2[6]-[13] に示しておく。

サーバー側からの情報漏えいは一度で大量の情報が漏れ、非常に多くのユーザーに悪影響を与えるという問題がある。日本ネットワークセキュリティ協会が算出した 2012 年上半期の一人あたり平均想定損害賠償額は 5 万 7710 円 [14] となっている。

情報漏えいがサーバー側で起きた場合のパスワード認証方式への影響であるが、表 1 において「PKI サーバー認証 +PW」および「PKI サーバー認証 +PW+OTP」と分類している方式では、サーバーにユーザーのパスワードそのもの、もしくはそのハッシュ値（パスワードを加工した値）が保存してある。そのため、それらの値が漏えいすれば、オフライン全数探索を適用することによりパスワードの特定が可能となる。さらに、その特定されたパスワードが他のサービスにも使い回されていた場合、漏えいを起こしていないサービスにも悪影響が出ることとなる。

なお、「PKI サーバー認証 +PW+OTP」と分類している方式ではワンタイムパスワードを生成するための情報もサーバー側に保持されており、この情報が漏えいすればユーザー

表2　サーバーからの情報漏えい事件の例

情報漏えい事件	内容
アドビシステムズの情報漏えい [6]	不正アクセスにより約 290 万件の顧客情報が流出した可能性があると発表された（2013 年 10 月）。
OCN の情報漏えい [7]	不正アクセスにより OCN のアカウント情報約 400 万件が外部に流出した可能性があると発表された（2013 年 7 月）。
ヤフーの情報漏えい [8]	不正アクセスにより約 148 万件の利用者 ID およびパスワード再設定用の「秘密の情報」などが流出した可能性が高いと発表された（2013 年 5 月）。
米 Yahoo! の情報漏えい [9]	サイバー攻撃により約 40 万件のユーザーのログイン認証情報が外部に流出した（2012 年 7 月）。
米シティグループの情報漏えい [10]	不正アクセスにより約 21 万件のクレジットカードの顧客情報が流出し（2011 年 6 月）、その流出カード情報の不正利用による被害総額が 2 億円を超えた [11]。
ソニー PSN の情報漏えい [12]	ソニーの PSN(PlayStation Network、利用者 7,700 万人) および Qriocity への不正侵入により大規模な個人情報流出が起きた（2011 年 4 月）。この事件によりソニーは英国で約 3,500 万円の罰金支払い命令を受けた [13]。

が打ち込むべき OTP も求まる。

1.4　クライアント側からの情報漏えいに対する脆弱性

図 2 に端末や記録媒体等の紛失・置き忘れおよび盗難により発生した情報漏えい事件の件数をまとめておく。この図は、日本ネットワークセキュリティ協会の「情報セキュリティインシデントに関する調査報告書」[15] に掲載されている 2005 年から 2011 年までの統計データから作成している。

2007 年くらいまでは漏えい件数は順調に減少しているが、これはそれ以前に多発した情報漏えい事件に対処するため会社や組織等において PC や可搬媒体の持ち出し制限が進んだことによるものと思われる。しかし、2007 年以降はその効果も鈍化し、年間 300 件以下への削減が難しくなっている。これらの数値はあくまで報道により明らかとなった大規模事件によるもののみであるが、報道されなかった小規模の事件を含めるとその数はさらに増えると思われる。その上、今後はスマホやタブレット PC 等の小型かつ高機能端末を持ち歩く機会も増え、それに比例して端末の紛失・置き忘れおよび盗難件数も増加すると予想される。

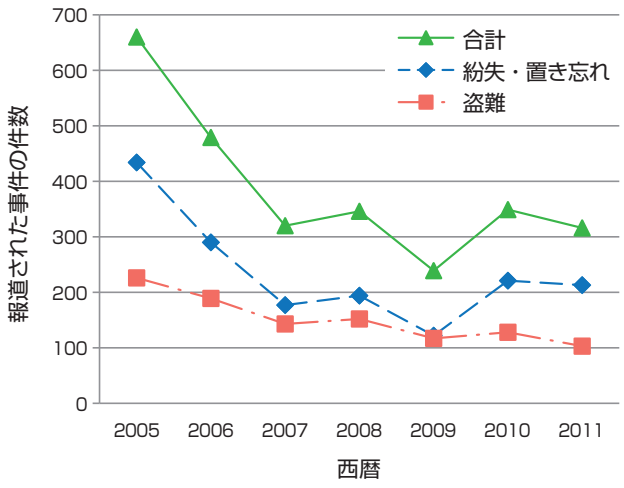

図2　クライアント側からの情報漏えい件数

クライアント端末には、認証方法によりパスワードで暗号化された暗号鍵、端末に記憶させたパスワード等、遠隔ユーザー認証に必要な情報が記録されており、これらが漏えいするとユーザーへの成りすましやユーザーのパスワードの特定が可能となる。表 1 において「PKI 相互認証」と分類している方式では、クライアント端末にユーザー認証用の鍵が保存され、通常、その鍵はパスワードで暗号化されている。そのため、攻撃者がこの端末を入手できれば、このパスワードと鍵をオフライン全数探索により求めることが可能となる。

1.5　フィッシング詐欺への脆弱性

表 1 において「PKI サーバー認証 +PW」および「PKI サーバー認証 +PW+OTP」と分類している方式では、ユーザーとサーバーとの間に暗号化通信路が設立され、その後、ユーザーの打ち込んだパスワードやワンタイムパスワード等がその暗号化通信路を通ってサーバーに伝えられる。サーバー側では元のパスワードやワンタイムパスワードが復号され、正しい値と比較されることによりユーザー認証が行われる。通信路は暗号化されているため、盗聴されたとしてもそこを流れたパスワードやワンタイムパスワードを得ることはできない。しかし、攻撃者は例えば「あなた銀行口座の暗証番号が漏えいしています。以下のホームページから早急にパスワードの変更を行ってください。」などと記載したスパムメールを送り付けるなどさまざまな方法でユーザーを攻撃者の用意した偽サーバーに導き、ユーザーのパスワード等の情報を盗もうとする。「PKI 相互認証」と分類している方式では、ユーザーのパスワードがサーバーに伝えられることはないが、認証後に打ち込んだ情報（例えば、クレジットカード番号や個人情報等）は盗られてしまう。

これら PKI を使った方式には、偽サーバーに繋がった際にユーザーに警告を出す仕組みがあるが、悪意のないサーバーが警告の出る公開鍵証明書を利用していたり、偽サーバーに誘導され出された警告をユーザーが無視したり、漏えいした秘密鍵が悪用され警告すら出ない偽サーバーがあったりして有効に機能していない。これに対して、PAKE および LR-AKE では、パスワードがサーバー側に伝えられることもなければ、正規のサーバーでエラーが出ることもな

い。認証プロトコル中でサーバーの認証も行われるため、偽サーバーへの接続は強制的に拒絶される。

2　問題解決のための研究シナリオ

この研究のシナリオを図 3 に示す。目標は、図中左のパスワードの問題を解決する新方式を考案・実用化し社会に提供することにある。研究シナリオの特徴としては、問題の解決可能性や、問題解決のための暗号学上の基礎理論面での改良を十分に行った後に、実用化研究に進む点にある。これは、新方式実用化後にその土台となる暗号技術に致命的な解読方法が見つかった場合、パッチ適用等の軽微な修正では問題を解決できず、根本原理の修正や方式の切り替えなどに多大なコストと時間が掛かるためである。実際、無線 LAN[16]、自動車の電子鍵 [17]、IC カード [18]、携帯電話 [19] 等の暗号の解読方法が、それらの実用化後に見つかり大きな社会問題になった例がいくつも存在する。

以下の各節においてこの研究シナリオの各段階について解説する。

2.1　問題の解決可能性に関する理論研究

ある社会問題が科学技術を以て解決可能か否かを早い段階で明白にすることは、そのテーマに研究リソースをつぎ込むべきかの判断を助け、リソースの最適配分に繋がるという意味で非常に重要である。幸い暗号技術に関連する問題は、要求されている項目が解決可能か否かを論理的に明白にし易く、本段階の研究に取り組み易いという特徴がある。

この研究においては、前節 1.2 から 1.5 までの問題が暗号技術をもって解決可能であるか否かを理論的に判断することになり、それらが解決不可能な問題であれば、何故それが不可能であるかを理論的に明らかにし、逆に、解決できる可能性があるのであればその実現例を示すことなる。解決可能なのか不可能なのかを明確にできなかった場合には、未解決問題として学会等に問題提起し他の研究者の協力を仰ぐことになる。

2.2　理論面での改良に関する研究

問題解決が理論的に不可能でない場合には、具体的な解決案が提示されることとなるが、初期の解決案は往々にしてその計算量や安全性等に改良の余地が残る。そのため、しばらくは、解決案の理論面での改良が行われる。なお、この改良は提案者達により行われることもあれば、他の研究グループにより行われることもある。また、情報セキュリティ分野においてこれらの改良は、防御面だけでなく攻撃面に対しても行われ、この攻撃面での改良も非常に重要な役割を演じている。なぜなら、新たな方式が社会に出た後で攻撃方法が改良されるのと、防御者側が事前に新たな攻撃を予測しておくことでは、後者の方が格段に修正コストと社会への影響度が小さくなるからである。

2.3　実用化に向けた研究

攻撃方法が見つからず、かつ、理論面での改良が進んだ方式は、実用化に一歩近づくことになる。実用化に向けた研究としては、

●実用化の際に必要となる追加機能に関する研究
●実装方法に関する研究
●他のアプリとの連携方法に関する研究

等がある。一つ目は、提案方式をより使い易くしたり、より多くの用途で利用できるようにしたりするための研究であり、二つ目は、それらをどのように実装すべきかに関する研究である。3 つ目は、実装方式を如何にして外部アプリと連携させるかに関する研究である。この研究において実際に取り組んだ研究の詳細と結果については次章で紹介する。

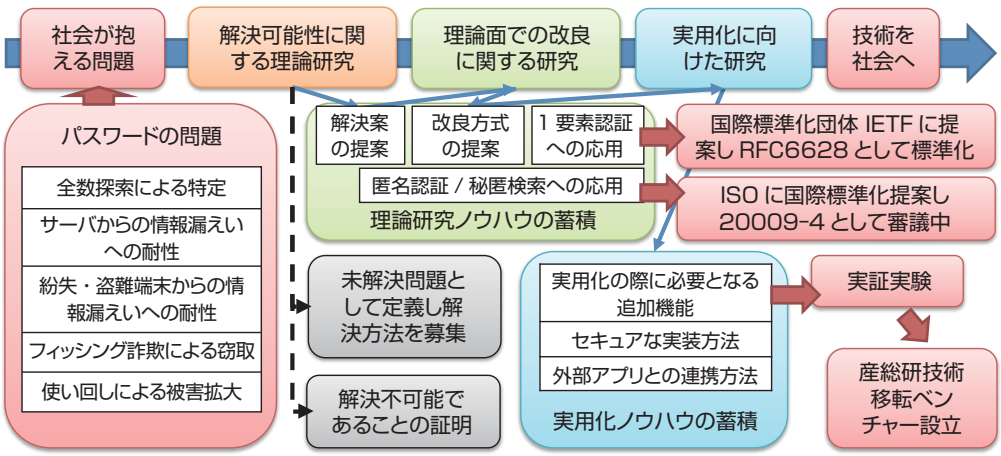

図 3　この研究におけるシナリオ

3　研究シナリオの検証と結果

本章では、前述のシナリオに沿って研究目標を実現するために選択した研究内容とその選択理由、ならびにそれらの結果について説明する。

3.1　問題の解決可能性に関する理論研究結果

この段階の研究により前述の問題が解決可能な場合に、その解決策に求められる制約条件が明らかとなった。その代表的な制約条件を以下で紹介する。

●［制約条件1：］ユーザーが短いパスワードを一つだけ使う1要素認証においてサーバー側から記録情報が全て漏えいすることを想定した場合、暗号技術をどのように組み合わせたとしてもそのユーザーのパスワードをオフライン全数探索から保護することは不可能である。

この条件により、短いパスワードを一つだけ使う1要素認証では前節1.2から1.4までの問題を全て解決することはできないことが分かる。そのため、研究対象を、パスワード以外の情報をクライアント側で保持する2要素認証に限定することにした。しかし、認証方式を2要素にしただけでは、問題の解決には繋がらない。実際、既存の2要素認証方式として現在広く利用されている「PKIサーバー認証 +PW+OTP」方式はサーバーからの情報漏えいに弱く、また、別の2要素認証方式である「PKI相互認証」方式はクライアントからの記録情報の漏えいに弱い。短いパスワードとクライアント端末に記録される認証情報と暗号技術をいかに組み合わせれば、問題が解決できるかについては、今まで学会においても産業界においても提案や実例がなく、学術的にもチャレンジングな課題となっていた。

一方、2要素認証方式の限界として以下の条件も導くことができる。

●［制約条件2：］一つの短いパスワードと記録情報を使う2要素認証においてサーバー側とクライアント側から同時に記録情報が漏れることを想定した場合、暗号技術をどのように組み合わせたとしてもそのユーザーパスワードをオフライン全数探索から保護することは不可能である。

ここで、「同時に記録情報が漏れる」とは1回の同じ認証において使われるサーバー側の記録情報とクライアント側の記録情報の両方が漏れることである。しかし、このことは、例えばn回目の認証で使われるサーバー側の記録情報とn+1回目の認証で使われるクライアント側の認証情報が同一の認証で使われない場合においては、問題を解決できる余地を残している。したがって、本制約条件により実現可能性が否定されていない最も高いレベルのセキュリティは、サーバー側とクライアント側の両方から記録情報が漏れたとしても、漏えいが同時に発生したのでなければ、ユーザーのパスワードをオフライン全数探索から保護できるというものである。ちなみに、並列オンラインパスワード全数探索は、クライアント側に記録される認証情報の候補数が十分多い場合に限っては、2要素認証に対しては無力である。なぜなら、2要素認証では各ユーザーのクライアント側に記録されている認証情報を大量に入手できなければ、並列でオンラインパスワード全数探索を適用できないからである。

我々は、情報漏えいへの耐性に関して実現可能性が否定されていない最も高いレベルのセキュリティを満たす構成が存在するか否かについて焦点を絞って研究を行い、実際にこれを満たす具体的な構成例を世界に先駆けて提案できた。技術構成上の要点としては、まず、クライアント側にはサーバー毎に独立に選択された秘密情報を置き、各サーバーにはユーザーを認証するための情報としてクライアント側に置かれた秘密情報とそのユーザーが覚える一つのパスワードを組み合わせ加工することにより得られたデータを置いた。これにより、そのサーバーに置かれたデータからパスワードが特定されることを困難にした。また、認証終了後にそれらクライアントとサーバーに記録されている情報を自動更新することで、クライアントとサーバー両方から異なるタイミングで漏えいが起きたとしてもパスワードを特定できないようにした。さらに、それらの情報と通信路を流れたデータが組み合わされたとしてもパスワードの候補を絞ることが数学的に難しくなるように暗号プロトコルを構成した。

我々は、その方式を漏えいに耐性のある認証付き鍵共有方式という意味でLR-AKE（Leakage-Resilient Authenticated Key-Establishment）と名付けた[20]。

3.2　理論面での改良に関する研究結果

この段階の研究において、我々はLR-AKEの計算量削減、より巧妙な攻撃への耐性確保、それらを破ることの困難さの数学的な証明に取り組んだ。また、得られた知見を応用することにより、既存方式の改良にも成功した。

計算量に関しては、最初に提案した方式[20]ではクライアント側に重い暗号処理（具体的には、1024 bit以上の多倍長の乗算720回程度）を必要としており、当時の携帯端末等の非力なクライアント端末上での実行は容易ではなかった。そこで、多倍長の乗算を3回にまで削減可能な方式を提案し、また、その方式を破ることが数学的に困難であることを証明した[21]。

より巧妙な攻撃への耐性に関しては、攻撃者がクライアント側に記録されている認証情報を書き換えられたとしても利用者のパスワードや分散保存しているデータを取り出せない方式を提案し、それらを破ることが数学的に困難であることを証明した[22]。クライアント側に記録される認証情

報は持ち運びを考慮して可搬媒体に記録される場合もあるが、この攻撃は、それらが盗まれ書き換えられた後に元に戻された場合等を想定したものである。

また、本段階の研究により蓄積された暗号プロトコル構成方法の知見を応用することにより、PAKE、匿名パスワード認証方式（Anonymous PAKE）、秘匿検索方式の改良にも成功した。ただし、これらのプロトコルは秘密情報として1要素しか利用しないため、サーバーからの漏えい情報を使ったオフライン全数探索への耐性は確保されないが、通信路の盗聴と成りすまし（秘匿検索においては検索語の特定）への耐性を最も少ない計算量で達成し、また、それらを破ることが数学的に困難であることの証明にも成功している[23]-[25]。ここで、匿名パスワード認証プロトコルとは、サーバーに対してユーザー個人を特定させることなく、そのユーザーが特定のグループに属していることのみを示す認証方式であり、以下のような用途への応用が可能である。

●組織メンバーからの匿名での内部告発
●会員への匿名カウンセリングサービス（医療/いじめ/悩み等の相談）
●特定の属性を有しているメンバーのコミュニティの形成（女性限定等）
●利用目的を限定した匿名通信路

また、パスワードの代わりに検索語を利用することにより検索語をサーバーに秘匿しながら検索を行ったり、お互いの条件を秘匿しながらマッチングを行ったりする際の効率のよいコアエンジンとしても利用できる。文献[25]の方式は、その後、ISO（International Organization for Standardization）にも提案し20009-4（Anonymous entity authentication - Part 4: Mechanisms based on weak secrets）として標準化に向けた審議が進んでいる[26]。文献[23]の方式については、汎用的なインターネットプロトコル（IKEv2: Internet Key Exchange version 2）へ適用するための仕様を国際標準化団体（IETF: Internet Engineering Task Force）に提案し、国際規格RFC 6628として承認・発行された[27]。実装版のLR-AKEシステムにおいても、文献[23][24]の方式はユーザーに使い捨てパスワードを発行し、ネットワーク経由でユーザーにクライアント側の認証情報を配布する際のプロトコルとして利用しており、ユーザー登録時の利便性を高めることに貢献している。

3.3　実用化に向けた研究結果

本節では、2.3節で紹介した研究の具体的な内容と結果について説明する。

3.3.1　実用化の際に必要となる追加機能に関する研究結果

LR-AKEでは、利便性とセキュリティを両立するため、利用者が短いパスワードを選択したとしても高いレベルのセキュリティを保てる工夫が施してある。具体的には、攻撃者が通信路を流れたデータとサーバーあるいはクライアントに記録されているデータを入手したとしても、パスワードのオフライン全数探索と並列オンライン全数探索を適用できないようにプロトコルが設計されており、また、攻撃者がクライアント端末から漏えいした認証情報を入手し、パスワードを一つずつサーバーに対して逐次試せる状態になったとしても、正規の利用者が認証を受けると、認証用記録情報は自動更新され、それ以降、攻撃者の入手した漏えい認証情報は使えなくなる。

攻撃者は記録情報が更新されるまでの間はパスワードを試せるが、これに対しては、認証が数回失敗した時点でそのアカウントをロックすることが可能である。しかし、単純な方法では、クライアント側の記録情報を入手していない低レベルの攻撃者が故意に認証を失敗し正規ユーザーのアカウントをロックさせたり、大量の認証リクエストによりサーバーに負荷を掛けたりして、正当な認証処理を妨害する恐れがある。そこで、このような低レベルの攻撃者が接続してきた場合には、サーバーに負荷を掛けることなくその認証処理を中断させ、また、認証が失敗した際に、記録情報を知らずに成りすましが試みているのか、漏えいした記録情報が使われ別の端末からパスワードが試されているのか、正当なユーザーがパスワードを打ち間違えたのかを切り分けられる仕組み[28]を考案し実装した。これにより、記録情報を入手していない攻撃者による正規アカウントの不正ロックと認証サーバーへのサービス妨害を防止しつつ、漏えい情報を使った攻撃の検知が可能となった。

さらに、全てのパスワード認証方式がLR-AKEに代われば、ユーザーは複数の独立したサービスを利用する場合においても記憶すべきパスワードを一つにすることができる。しかし、過渡期においては、利用者はLR-AKE用のパスワードに加えて、他のサービスで利用されているパスワードも複数覚えるか、どこかに保存しなければならない。そこで、情報漏えいに強いというLR-AKEの性質を応用して、他の方式で使われているパスワードや暗号鍵等の重要情報を、LR-AKEのサーバー、クライアント、LR-AKE用のパスワードに分散保存し、LR-AKE認証をパスしなければ元の情報を復元できない機能[29]を検討し実装した。LR-AKEに分散保存された情報は、LR-AKE用のパスワードと同様、サーバー、クライアントいずれに記録されている情報からも復元することはできず、また、LR-AKE認証が行われる度に自動更新される。

しかし、この分散保存機能を加えたことにより、新たな

課題が生じることとなった。前述のとおり我々の提案方式は漏えいには強いが、サーバー、クライアントいずれかのデータが利用できなくなると保存したデータを取り出せなくなる。また、LR-AKE では、漏えいに強くするためサーバーおよびクライアントに記録されている情報をユーザーが認証される度に更新している。そのため、サーバーの故障やクライアント端末の紛失等で、バックアップデータを使って一方のノードを前の状態に戻したとしても LR-AKE に分散保存したデータは取り出せない。そこで、複数の LR-AKE 対応サーバーと複数のクライアントを使うことにより、漏えい耐性を維持しながらノードクラッシュ後のデータの取り出しを可能にし、また、一つの LR-AKE クライアント端末から保存したデータを、他の LR-AKE クライアント端末から取り出せるようにした。また、ユーザーがうっかりしきい値回以上パスワードを間違えアカウントをロックさせた場合に、そのユーザーの有効な LR-AKE アカウントから、そのロックされたアカウントを解除する仕組みも実装した。我々は、LR-AKE のこのような冗長構成をクラスタモード [30] と名付け、これまでのクライアント端末とサーバーを 1 台ずつ使う構成をシングルモードと分類することにした。

クラスタモードを応用すれば、個人で自分用のデータを LR-AKE に分散保存する以外に、グループを形成して、サーバーに情報を漏らすことなくそのグループ内だけで同じ情報を共有することができる [31]。そのため、例えば、社内の計算機管理者達が、サーバーや端末の管理パスワードを共有しておくなど、重要情報の管理をグループ間でセキュアに行える。また、その際、各ユーザーが記憶すべきパスワードは、各メンバー個人の短いパスワードに設定でき、そのパスワードはグループの他のメンバーやサーバー管理者に知られることはない。

3.3.2　実装方法に関する研究結果

LR-AKE は、基本的に高いセキュリティが求められる用途で利用されるため、方式としての高いセキュリティレベルの確保に加えて、実装時のセキュリティ対策にも配慮した。これらの作業はセキュアに実装するためのベストプラクティスを適用することが主で、新規性が求められる学術論文や特許等の成果に繋がるものではなかったが、本作業で得られた知識は、その後取り組むこととなった重要インフラや制御システムのサイバーセキュリティ対策の研究を進める上で大いに役立つこととなった。

また、実装してみることにより見えてきた仕様上の曖昧さも明らかとなった。前述のとおり LR-AKE には、流出した認証用のデータを自動的に無効化するため、ユーザー認証後に記録データを更新する機能や、認証の失敗原因が正規ユーザーによるパスワードのタイプミスなのか、それとも、クライアント側に記録している情報が漏えいし、それを用いてパスワードが試されたのかを切り分ける仕組みを備えている。これらはいずれもプロトコルが正常に終了した場合を想定していたため、通信が途中で途切れた場合については曖昧さが残っていた。そこで、プロトコルのどの時点において通信が途切れたとしても、必ず通信を再開でき、かつ、上述の機能やセキュリティレベルが損なわれないようにするための検討を行い、仕様の詳細に反映させ実装を行った。

3.3.3　他のアプリとの連携方法に関する研究結果

実装の精度が高まってくると、各種アプリケーションとの連携方法が課題となった。一つの方法は、各種アプリケーションの一部として LR-AKE が組み込まれることであるが、この方法は初期の修正に加えて、アップデートの度に修正が生じ工数の大きさが問題となる。その上、責任分解点が曖昧となるため、アプリケーション開発者側の理解も得難い。そこで、アプリケーション側から LR-AKE の機能を呼び出すためのインターフェース API（Application Programming Interface）を定義し、LR-AKE をアップデートしたとしてもインターフェースは変更しないか、古いインターフェースを残し、新たなインターフェースを追加することにより、LR-AKE 側の更新に伴う連携アプリ側の修正を生じさせないようにした。さらに、アプリケーション側のプログラムに修正を加えることなく連携を取る仕組みについても検討を行い実装を行った。具体的には、LR-AKE 認証後に LR-AKE のクライアント側とサーバー側でワンタイムパスワードを生成し、サーバー側ではアプリケーション側が備えるパスワード登録手続きを使って、そのワンタイムパスワードをそのアプリケーションで使われる利用者のパスワードとして登録し、クライアント側からその使い捨てパスワードを使ってそのアプリケーションが提供するパスワード認証手続きを使って認証を受ける。また、その際、サーバーに関する情報を LR-AKE サーバーと LR-AKE クライアント間に張られた安全な通信路を介してクライアントに伝えることによりサーバー認証も行う。これにより、ユーザーとしては LR-AKE 認証を受けるだけで、LR-AKE と連携している各種サービスを受けられるようになり、かつ、連携先アプリケーションのソースコードの変更は不要となる。

実際、この仕組みは AIST での実証実験でも利用した。本実証実験では、外部ネットワーク上の認証されたユーザーを内部ネットワークに接続する VPN（Virtual Private Network）と LR-AKE を連携させ、LR-AKE 認証を受けることにより AIST 内ネットワークの一部に接続できるようにした。当然ながら、VPN ソフトウェアは他社の製品であるため、その中身を変更することはできない。そこで、前述のメカニズムを使い VPN のソースコードを変更すること

なく連携を可能とした。実証実験は、2010 年 3 月 13 日から当該システムを駆動させ動作に問題無いことを確認し、同年 7 月 27 日からは、問題発生時に即座に対応できるよう当時の情報セキュリティ研究センターと先端情報計算センターの方々に参加をお願いし、通常の VPN 接続の代わりに利用して頂いた。駆動面で問題がないことが確認されたため、2011 年度からはより多くの方にも参加してもらうべく準備を進めていたが、3 月 11 日につくば地区も震災に見舞われ、LR-AKE サーバーを含む産総研つくばのサーバー群は当面停止されることとなった。幸い、実証実験での LR-AKE は前述のクラスタモードで運用しており、セカンダリサーバーを AIST の中国センターに設置していたため、つくばの LR-AKE サーバーを停止し VPN と連携を中止させた後も、LR-AKE に分散保存していたデータを取り出す機能は提供し続けることができた。

4　おわりに

サーバーとクライアントのいずれから記録情報が漏えいしたとしても、ユーザーのパスワードに対する全数探索を困難にする暗号構造に関する基礎理論研究とその実用化研究について紹介した。実用化した技術については、その後、産総研技術移転ベンチャー企業を設立し、ユーザー認証や鍵管理を必要とするソフトウェアから LR-AKE の機能を呼び出すための商用版ソフトウェア開発キット（SDK: Software Development Kit）と商用版サーバー、技術サポートを提供した。さらに、一部の機能は IETF（Internet Engineering Task Force）へ提案し RFC6628 として国際標準化された。

現在の状況は、技術が社会に提供されイノベーター（イノベーション普及学等 [32] で言うところの革新的な採用者）にようやく採用され始めた段階にある。2013 年 4 月には、りそな・日刊工業新聞中小企業優秀新技術・新製品賞の奨励賞と産学官連携特別賞を受賞し、産業界の一部においても知られる機会を作ることができた。

しかし、過去、公開鍵暗号系の技術が社会に普及するまでに 20 ～ 30 年程度を要していることを考慮すると、LR-AKE においても普及には同等の年月を要すると思われる。そのため、LR-AKE がアーリーアダプター（新しいものに敏感な利用者層）やアーリーマジョリティ（平均より早く新しいものを取り入れる利用者層）に広まり、技術が急激に広まり始めると言われている普及率 16 % 程度のクリティカルマスを超えるまでは、地道に実績を積み重ね、知名度を向上させる活動に取り組むことになると思われる。

また、この論文が研究成果を実用化し、社会に提供する際の参考になれば幸いである。

参考文献

[1] 鈴木 雅貴, 宇根 正志: 生体認証システムの脆弱性の分析と生体検知技術の研究動向, *金融研究*, 28 (3), 69-106 (2009).

[2] 警察庁: 平成23年中の不正アクセス行為の発生状況等の公表について, http://www.npa.go.jp/cyber/statics/h23/pdf040.pdf, (2012).

[3] E. Barker, W. Barker, W. Burr. W. Polk and M. Smid: Recommendation for key management - Part 1: General (revision 3), *NIST Special Publication*, 800-57, (2012).

[4] TrueCrypt Foundation: TrueCrypt Beginner's Tutorial Part 2, http://www.truecrypt.org/docs/tutorial2 , 2013年8月閲覧

[5] G. A. Miller: The magical number seven, plus or minus two: Some limits on our capacity for processing information, *Psychological Review*, 63 (2), 81-97 (1956).

[6] http://headlines.yahoo.co.jp/hl?a=20131004-00000005-rbb-sci, 2013年10月閲覧

[7] http://www.ntt.com/release/monthNEWS/detail/20130724.html, 2013年10月閲覧

[8] http://itpro.nikkeibp.co.jp/article/NEWS/20130523/479201/, 2013年10月閲覧

[9] http://jp.reuters.com/article/technologyNews/idJPTJE86B02120120712, 2013年10月閲覧

[10] http://www.bloomberg.co.jp/news/123-LMJIFD1A1I4H01.html, 2013年10月閲覧

[11] http://www.zaikei.co.jp/article/20110627/74852.html, 2013年10月閲覧

[12] http://www.nikkei.com/article/DGXZZO27529030X20C11A4000000/, 2013年10月閲覧

[13] http://japanese.engadget.com/2013/01/24/psn-3500/, 2013年10月閲覧

[14] 日本ネットワークセキュリティ協会: 2012年 情報セキュリティインシデントに関する調査報告書【上半期 速報版】, http://www.jnsa.org/result/incident/2012.html (2013).

[15] 日本ネットワークセキュリティ協会: 情報セキュリティインシデントに関する調査報告書, http://www.jnsa.org/result/2013.html (2009-2012).

[16] 産業技術総合研究所: 無線LANのセキュリティに係わる脆弱性の報告に関する解説, https://www.rcis.aist.go.jp/TR/TN2009-01/wpa-compromise-summary.html , (2009).

[17] K. Zetter: Researchers crack KeeLoq code for car keys, *WIRED*, http://www.wired.com/threatlevel/2007/08/researchers-cra/, (2007).

[18] E. Phillips: Mifare crypto1 RFID completely broken, http://hackaday.com/2008/01/01/24c3-mifare-crypto1-rfid-completely-broken/, (2008).

[19] H. Horesh: Technion team cracks GSM cellular phone encryption, http://www.cs.technion.ac.il/~barkan/GSM-Media/HaaretzInternetEnglish.pdf, (2003).

[20] SH. Shin, K. Kobara and H. Imai: Leakage-resilient authenticated key establishment protocols, *ASIACRYPT 2003*, LNCS 2894, 155-172 (2003).

[21] SH. Shin, K. Kobara and H. Imai: An efficient and leakage-resilient RSA-based authenticated key exchange protocol with tight security reduction, *IEICE Transactions*, E90-A (2), 474-490 (2007).

[22] SH. Shin, K. Kobara and H. Imai: An RSA-based leakage-resilient authenticated key exchange protocol secure against replacement attacks, and its extensions, *IEICE Transactions*, E93-A (6), 1086-1101 (2010).

[23] SH. Shin, K. Kobara and H. Imai: Secure PAKE/LR-AKE protocols against key-compromise impersonation attacks, *第31回情報理論とその応用シンポジウム*, 965-970 (2008).

[24] SH. Shin, K. Kobara and H. Imai: RSA-based password-authenticated key exchange, revisited, *IEICE Transactions*, E91-D (5), 1424-1438 (2008).

[25] SH. Shin, K. Kobara and H. Imai: Anonymous password-authenticated key exchange: New construction and its extensions, *IEICE Transactions*, E93-A (1), 102-115 (2010).
[26] ISO: Anonymous entity authentication -- Part 4: Mechanisms based on weak secrets, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64288 2013年10月閲覧
[27] SH. Shin and K. Kobara: Efficient augmented password-only authentication and key exchange for IKEv2, *IETF, RFC 6628*, 1-20 (2012).
[28] Y. Onda, SH. Shin, K. Kobara and H. Imai: How to distinguish on-line dictionary attacks and password mis-typing in two-factor authentication, *ISITA2010*, 571-576 (2010).
[29] 辛 星漢, 古原 和邦, 今井 秀樹: 情報漏洩に堅牢な認証・データ管理システムの概要(シングルモード), *コンピュータセキュリティシンポジウム 2007*, 2007 (10), 673-678 (2007).
[30] 辛 星漢, 古原 和邦, 今井 秀樹: 情報漏洩に堅牢な認証・データ管理システムの概要(クラスタモード), *第30回情報理論とその応用シンポジウム*, 790-795 (2007).
[31] 辛 星漢, 古原 和邦, 今井 秀樹: グループ間でのファイル共有を柔軟かつ安全に行うための新方式検討, *コンピュータセキュリティシンポジウム 2011*, 2011 (3), 803-808 (2011).
[32] E.M. Rogers: *Diffusion of Innovations, 5th* Edition, Free Press, New York (2003).

執筆者略歴

古原 和邦（こばら かずくに）

1994年山口大学大学院博士前期課程修了。同年東京大学生産技術研究所入所。2000年東京大学生産技術研究所助手。2003年博士号（工学）取得。2006年（独）産業技術総合研究所入所。情報セキュリティ研究センターセキュリティ基盤技術研究チーム長として、セキュリティ技術の基礎理論とその実用化研究に取り組む。同年7月同所主幹研究員。2012年からはセキュアシステム研究部門の制御システムセキュリティグループ長として制御システムや重要インフラ向けのセキュリティ技術の研究に取り組む。この論文では、主に研究シナリオや実用化の記述を担当。

辛 星漢（しん しぇんはん）

2005年東京大学博士号（情報理工学）取得。2006年（独）産業技術総合研究所入所。情報セキュリティ研究センターセキュリティ基盤技術研究チームで、認証技術や暗号プロトコルの基礎理論とその応用研究に取り組む。2012年からはセキュアシステム研究部門セキュアサービス研究グループで、インタネットサービスのセキュリティ技術の研究や国際標準化に取り組む。この論文では、主に理論研究内容の記述を担当。

査読者との議論

議論1　論文タイトルと梗概をより明確かつ構成的に

コメント（松井 俊浩：産業技術総合研究所セキュアシステム研究部門）

タイトルにある、次世代～技術というのは、提案書でよく見かけますが、何とははっきりと示せない改良によって、ぼんやりと今よりよくなることを示唆するだけに思われます。梗概に、「ここで次世代とは～重要情報を取り出せず～短いパスワードですませられることである」とあるとおり、次世代の中身が示せるなら、そのような述語を充てるべきです。ご提案のタイトルは、今後も続くすべてのより新しい認証、鍵管理の論文のタイトルになりえる、あいまいな、したがって読者の注意が定まらない導入になってしまっています。また、Synthesiologyという、技術の構成方法を専門によらずに議論する技術論文誌としては、一つの技術の紹介ではなく、Synthesisや方法論の根源にアプローチしているというニュアンスも欲しい。すなわち、なぜこのような基盤技術が必要で、それによって社会や産業がどのように変わるのかをイメージできるようなタイトルです。

回答（古原 和邦）

題目の「次世代認証」を具体的な「漏えいに強いパスワード認証」に変更し、後半の「鍵管理基盤」、「LR-AKE」を、「その応用」に短縮しました。

議論2　社会や産業の問題の分析と必要な技術開発

コメント（松井 俊浩）

論文は、いきなりユーザー認証方式の比較から始まっていて、社会のどういう問題を解決しようとして行っている技術開発なのかが示されていません。現在、パスワードが、どういう状況におかれていて、なぜ漏えいするのか、漏えいすると何が起こるのか、どうして保護が難しいのかなどをなるべく論文の始まり部分で述べることで、問題の定義研究の意義がはっきりします。1.2節以下に順次それらが示されていきますが、順番が逆です。

回答（古原 和邦）

1章冒頭の記述をパスワードの状況を説明する内容に変更し、パスワードの使われ方や漏えい原因等について説明し、1.2-1.5節で保護の難しさを説明する構成に変更致しました。

議論3　Synthesiology論文としての特徴

コメント（松井 俊浩）

論文を読み通して、この論文の特徴は、現場のフィードバックで改良するのではなく、事前にあらゆる問題を想定して対策を施しておくこと、リスクアセスメントをかけながら研究開発を行う手法にあるのだと感じました。セキュリティのように安全あるいは信用に関わる技術では、中途半端な技術を世に出して信を問うという、よくある手法が不適当なのです。そのためには、事前にあらゆる問題を抽出し、検討し、対策を講ずることが必要です。その点を強調して、系統的に記述されると良いと思います。

回答（古原 和邦）

ご指摘の通り2章の冒頭で、この研究シナリオの特徴、すなわち、「方式の根底をなす暗号技術について事前にセキュリティ面における十分な検討と改良を行った上で、実用化研究に移ることの重要性」を記述しました。

議論4　1要素PAKE

コメント（松井 俊浩）

3.1では、1要素認証ではどうしてもパスワード漏えいを防げないので、2要素認証に限定して研究を進めると書かれていますが、3.2の中盤では、1要素のPAKEを改良して、十分な安全性を得たように書かれています。2要素は不要なのかとの混乱を招きますので、整理してください。その後にも検索語を秘匿した検索とか国際標準化への発展が書かれていますが、本題からはずれるのであれば、これらの記述は混乱を招かないよう削除してください。

回答（辛 星漢、古原 和邦）

2要素認証が不要との誤解を受けないよう、PAKEと匿名パスワード認証については盗聴と成り済ましのみへの耐性、秘匿検索については、ネットワーク上からの攻撃に対して検索語が保護されるのみで、サーバ側からの漏えいに耐性を有している訳ではないことを3.2の第4段落に追加いたしました。

また、この部分は、理論面での改良研究により蓄積された技術的知見が、さまざまな応用先に広がった例を示しておりますので、その説明を 3.2 節の第一段落の最後と、上記と同じ箇所に追加しました。

議論5　オフライン全数探索および並列オンライン全数探索の説明

コメント（坂上 勝彦：産業技術総合研究所情報基盤部）

提案手法は、オフライン全数探索および並列オンライン全数探索がいずれも適用不可である強固な手法だと理解しました。しかし、他分野の読者は、遠隔ユーザ認証方式の実例を身近な例でしか知らないため、オフライン全数検索、並列 / 直列オンライン全数検索が具体的にどういうものであるかが、本文中の短い記述だけでは把握できないと考えられます。提案手法の優位性を示す重要なポイントですので、分かりやすい説明を加筆するとよいと思います。

回答（古原 和邦）

1.2 節において、オフライン全数検索、並列 / 直列オンライン全数検索の説明を追加しました。

議論6　なぜ4つの問題点に帰着されるのかの説明

コメント（坂上 勝彦）

既存のパスワード認証方式の各問題点として節 1.2 ～ 1.5 の 4 つが挙げられており、2 章の冒頭ではこの研究の目標がこの問題点を抜本的に解決するものであると述べられています。しかし、なぜこの 4 つの問題点に帰着されるのかが、非専門家には理解できません。分かりやすい説明の加筆をお願いします。

回答（古原 和邦）

1.1 節にパスワード入手の手口に関する統計データを追加し、それらと 1.2 ～ 1.5 節の 4 つの問題の関係の説明を追加しました。