7ZA-01

乱数とパスワードを組み合わせたユーザ認証方式の提案

渡邉 悠雅 †1　鈴木 秀和 †2　内藤 克浩 †3, 渡邊 晃 †2
†1 名城大学理工学部　†2 名城理工学研究科　†3 愛知大学情報科学部

1 はじめに

インターネットは我々の生活に欠かせないインフラの一つである. インターネットの普及と共に, 個人を認証することはより重要なものになった. 不正アクセスを防ぐためには, パスワードだけでは不十分で, 生体認証などの要素を加えた多要素認証システムが検討されている. しかし多要素認証は利用者の煩わしさやわかりにくさを伴いやすい. そこで, 本稿ではパスワードとユーザ端末で生成した乱数でハッシュ値を取り, これをパスワードとみなしてサーバに登録する要素認証方式を検討した. ユーザの利便性, 金銭的なコスト, サイバー攻撃に対する耐性といった観点より他認証方式と比較し, 有用であることを示した.

2 既存の多要素認証方式

認証技術はパスワードと組み合わせて活用することが多い. 以下に既存の組み合わせ対象となる技術とその概要を示す.

生体認証は本人の身体情報を用いた認証である. 指紋認証や顔認証など多くの種類があるが, カメラや指紋センサーなどの専用読み取り機が必要となる. また, 誤認証でユーザを認識しないことや他人を認証してしまうことがある.

IC カードによる認証は, 専用の読み取り機を使いカード内の秘密鍵を読み取ることで認証を行う. カード内の情報はハードウェアレベルとソフトウェアレベルの両方から守られており, 外部から秘密情報の参照を防ぐことができる. 専用読み取り機や IC カードに費用がかかるという課題がある.

OTP(One Time Password) による認証は, 一定時間のみ有効なパスワードを使用する認証方法である. Google Authenticator では, サーバとユーザが予め同じ鍵を共有し, 端末内の時刻カウンターをベースに定期的に 6 桁数字の OTP を生成し, 所定時間内に入力を要求する方式である/ セキュリティは固いが, 認証の手間の多いという課題がある.

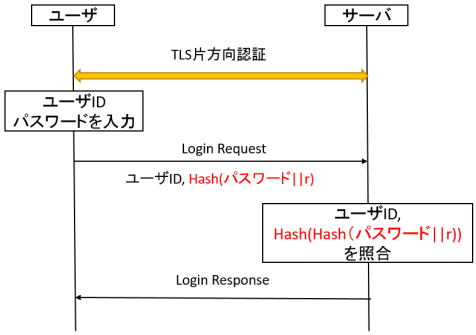

図 1　Login process of proposed method

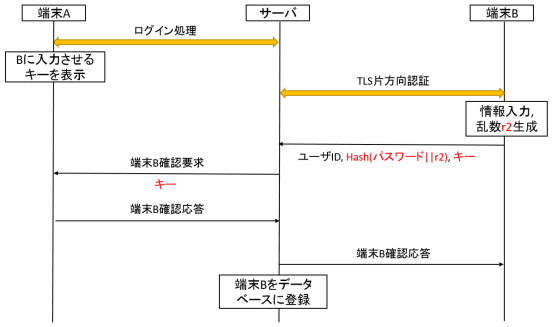

図 2　Login registration process of another terminal

3 提案方式

3.1 アカウントの生死絵と認証手順

本提案はユーザ端末で乱数を生成し, パスワードと乱数の組み合わせをサーバに登録する. 乱数がサーバに分からない点が特徴である.

(1) アカウント生成手順

アカウント作成は TLS でサーバを認証後, ユーザはアカウント情報としてメールアドレス, ユーザ ID, パスワード情報を入力する. ユーザ端末では十分に長い乱数 r を生成し, 不揮発メモリ内に保存するとともに, 乱数 r とパスワードでハッシュ値を求める. ユーザ端末はメールアドレスとユーザ ID, ハッシュ値をサーバに送信する. このハッシュ値をサーバに登録するパスワードとして扱

Proposal for User Authentication Method Combining Password and Random Number

Yuga Watanabe[†1], Hidekazu Suzuki[†2], Katsuhiro Naito[†3], Akira Watanabe
[†1] Faculty of Science and Technology, Meijo University
[†2] Graduate School of Science and Technology, Meijo University
[†3] Faculty of Information Science, Aichi Institute of Technology

表 1　Comparison of authentication methods

	セキュリティ			使い勝手			
	辞書攻撃	推測攻撃	リスト型攻撃	項目①	項目②	項目③	項目④
PW	×	×	×	○	○	○	○
PW+ 生体認証	△	○	×	×	○	○	×
PW+IC カード	△	○	○	×	○	○	×
PW+OTP	△	○	○	○	×	×	○
提案方式	○	○	○	○	○	○	○

わせる. 以降は登録メールアドレスが正規のものであると確認されたら, データベースにアカウント情報が登録される.

(2) 認証手順

Fig. 1 に提案方式における認証時のシーケンス図を示す. ログイン処理では,TLS によりサーバを認証後, ユーザはユーザ ID とパスワードを入力する. ユーザ端末はパスワードと保存されている乱数 r を組み合わせてハッシュ値を生成し, ユーザ ID と共にサーバに送信する. サーバはログイン情報をデータベースと照合し, ログイン情報が正規のものであると確認されれば, ユーザを認証する.

3.2　別端末からのログイン

提案方式では生成した乱数がユーザ端末内の不揮発メモリ内に保存されるため, このままでは別端末からのログインができない. そこで,1 アカウントに対し, 複数端末の登録を可能とするように拡張した. Fig. 2 は別端末からのアカウント生成方法を示したものである. 端末 A と新規端末 B を近くに持ってくる必要がある. 端末Aにて登録に必要なキーを発行する. 端末 B はアカウント登録時に, ユーザ ID とパスワード, 目視で確認したキーを入力する. パスワードは端末 A と同じものを利用できる. 端末 B では新たに乱数 r2 を生成し, 乱数 r2 とパスワードでハッシュ値を求める. サーバにはユーザ ID と生成したハッシュ値, キーを送信する. サーバはキーの一致確認処理を行い, キーが正しいと確認されると. 端末 B から送られたハッシュ値を同一ユーザのアカウントとしてデータベースに登録する. これによりユーザは同じパスワードで別端末からログインできるようになる.

4　評価

Table 1 は認証方式をセキュリティと使い勝手で比較したものである. 比較対象はパスワードのみ, パスワードにそれぞれ要素として生体認証,IC カード,OTP(One Time Password) を組み合わせた場合, 提案方式とした.

辞書攻撃は辞書に載っている単語をひたすら照合することでパスワードを解析する攻撃である. サーバサイドから台帳が漏洩した場合, パスワードだけでは解析される場合がある. 多要素認証であればログインされることは防げるので△とした. 提案方式は乱数が十分大きいので解析できない.

推測攻撃はターゲットが設定すると考えられる情報を予測してログインを試みる攻撃である。パスワードは好きな言葉や生年月日などを登録していると, 推測攻撃されてしまう.

リスト型攻撃は他のサービスなどから漏洩したアカウント情報を利用して, 不正アクセスを試みる攻撃である. 生体認証は漏洩した生体情報を使われる可能性があり, リスト型攻撃に耐性がない. 提案方式はサーバに登録されたハッシュ値が十分大きければ, 辞書攻撃安い即攻撃はできない. また, 認証にユーザ端末に保存されている乱数 r が必要となるためリスト型攻撃は不可能である. 使い勝手の評価項目は以下の項目で比較した.

① 導入費用または運用費用の安さ
② 使用方法の分かりやすさ
③ 使用時の手間や煩わしさ
④ 別端末からのログイン可否

パスワードのみは使い勝手の評価が良いが, セキュリティが弱い. 生体認証と IC カードは, 専用機器に費用が発生し, 読み取り機が無い端末ではログインできない. OTP は使用方法がわかりづらく, 制限時間内に情報入力を行う必要があるなど煩わしさが大きい. 提案方式はアカウント登録後の使い勝手がパスワードと同じである。セキュリティと使い勝手を兼ね備えた認証方式であるといえる.

5　まとめ

乱数とパスワードを組み合わせたユーザ認証方式を提案した. ユーザの利便性を損なうことが少なく, セキュリティを高めることができる認証技術である. 普段使用している端末以外でのログインがしにくいという課題は, キーを発行して登録処理をすることで解決する.

参考文献

[1] 鈴木 宏哉 , 山口 利恵 : 研究報告コンピュータセキュリティ（CSEC）,2016-CSEC-73(13),1-8 (2016-05-19)