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

会員システムは個人を認証するための技術であり, インターネットの普及と共にその必要性は増した. 不正アクセスを防ぐためにアカウント情報の保護が重要であるが、セキュリティの強化は利用者の煩わしさやわかりにくさを伴いやすい. 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, パスワードとしてサーバに登録する認証方法を検討した. 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た

2　既存の認証方式

パスワード認証方式はユーザ ID とパスワードの情報よりユーザを識別する認証方法である. ユーザはメールアドレス等で予めアカウント作成を行う必要があるが, 認証専用機器の用意をする必要がない. パスワードは辞書にある言葉や, 生年月日などの分かりやすい数字であると解析されてしまう可能性が高い. パスワードを使いまわしていると, 他の認証サービスで漏洩したパスワードで不正アクセスされることがある.

ユーザの身体情報を利用する生体認証は, 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. 誤認証でユーザを認識しないことや似ている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いでいる.

OTP(One Time Password) は一定時間のみ有効なパスワードを生成する認証技術であり, 本稿では二段階認証アプリによりパスワードを生成する方式を想定する.

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

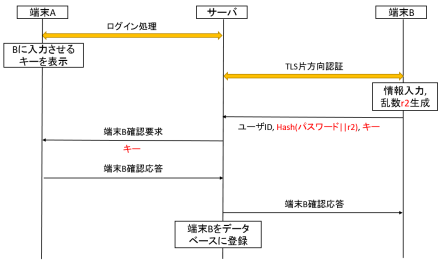

図 1　Login process of proposed method

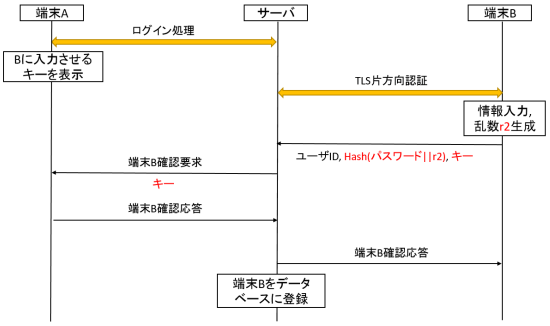

図 2　Login registration process of another terminal

サーバとユーザが保持する同じ鍵と時刻カウンターを組み合わせたハッシュ値を, 認証の鍵としている.

3　提案方式

3.1　概要

提案方式では一般的なパスワード認証方式と同様に, メールを使ったアカウント作成を行う. ユーザはメールアドレス, ユーザ ID, パスワードのアカウント情報を入力完了する直後, ユーザ端末内では十分に長い乱数を生成する. その後, 生成した乱数とパスワードを一方向性ハッシュ関数にかけ, ハッシュ値を求める. なお, 乱数生成とハッシュ値計算の作業はプログラムが自動的に行う. ユーザ端末はメールアドレスとユーザ ID, 生成した乱数とパスワードを組み合わせて生成した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次第, データベースにアカウント登録される.

表 1　Feature comparison of authentication

	辞書攻撃	ショルダーハッキング	リスト型攻撃	項目①	項目②	項目③	項目④
パスワード	×	×	×	○	○	○	○
生体認証	○	○	×	×	○	○	×
IC カード	○	○	○	×	○	○	×
OTP	○	○	○	○	×	×	○
提案方式	○	○	○	○	○	○	○

Fig. 1 に提案方式における認証時のシーケンス図を示す. ログイン処理ではユーザはユーザ ID とパスワードを入力し, ユーザ端末はパスワードと保存されている乱数を組み合わせてハッシュ値を生成する. サーバにはログイン情報として, ユーザ ID と生成したハッシュ値を送信する. サーバがログイン情報をデータベースとの照合し, ログイン情報が正規のものであると確認されれば, ユーザにログイン応答が返される.

3.2　他端末でのログイン

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ている. それゆえ, アカウント取得を行った端末以外でのログインが困難になる. この課題を解決する手段として、乱数を保持するユーザ端末 (以下端末 A とする) とログインしたいデバイス (以下端末 B とする) を紐づける方法を検討した. Fig. 2 はキーによる他端末の登録を示したものである.

3.3　利点

端末内で生成した乱数は端末側のみ保持しており, 通信経路に直接流れることがないため攻撃者に盗まれにくい. しかし, 攻撃者は不正アクセスするために, パスワードだけでなく乱数を所持する必要がある. そのため, 攻撃者は他の Web サービス等で使いまわしたパスワードを使用していてもログインすることができない.

また, サーバ側のデータベースが盗難された場合に, 他の Web サービスにパスワードが流用されることがない. サーバ側には, 乱数とユーザのパスワードを組み合わせたハッシュ値をパスワードとして台帳に記録している. ハッシュ値は常に固定サイズの予測不可能な文字列であり, パスワードと組み合わせる乱数はそれ自体に言葉の意味を持たない文字列である. ハッシュ値から乱数やパスワードを逆算することは不可能であり, 攻撃者は乱数や元のパスワードを知ることはできない. 辞書攻撃や推測攻撃による耐性が非常に高いといえる.

提案方式では乱数の生成, ハッシュ値の算出はプログラムが自動的に行う. そのため, 他デバイス登録処理時以外は一般的なパスワード認証と変わらない使い勝手になる. ユーザが新たに覚えることが少なく, 使用時の煩わしさが少ない.

4　評価

Table 1 に認証方式の比較表を示す [1]. 比較対象は主要である認証方式のパスワード, 生体認証,IC カード,OTP(One Time Password) である.

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. 本稿ではサーバサイドの台帳から辞書攻撃される場合も想定してる. ショルダーハッキングは, 入力している情報を攻撃者が背後から観察し盗み出す攻撃である. リスト型攻撃は他のサービスなどから流出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. 特徴の評価項目は以下のとおりである.

① 導入費用または運用費用の少なさ
② 使用方法の分かりやすさ
③ 使用時の手間や煩わしさの少なさ
④ 普段使っている端末以外からのログインできるか

提案方式以外にも,IC カードと OTP は辞書攻撃, ショルダーハッキング, リスト型攻撃に対して耐性を持っている. しかし,IC カードは読み取り機やカードに対する費用が発生してしまう. OTP はユーザに使用方法の分かりにくさと煩わしさを与えてしまう. 提案方式はセキュリティの高さを持ちつつ, 費用の少なさと使いやすさを兼ね備えた認証方式といえる.

5　まとめ

パスワードとユーザ端末内で生成した乱数でハッシュ値を取り, そのハッシュ値をパスワードとしてサーバに登録させる. 乱数はユーザ端末内のみ保持しており, 通信系路上に乱数と元のパスワードが直に送信されることはない. 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, 普段利用している端末でキーを生成し, キーを利用してログインしたい新たな端末を登録して解決する.

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)