L-055

メール送信ワンタイムパスワードを用いた安全なログインシステムの開発
Development of secure login system using e-mail based one time password

梅田 知宏，平野　学
Tomohiro Umeda，Manabu Hirano

1. はじめに

近年オンラインバンキング等の普及により，一般消費者がインターネット上でパスワードを入力する機会が増えている．この結果，スパイウェアやネットワークの盗聴，データベースの流出などによってオンラインバンキング等の重要なパスワードが盗難される被害も増え始めている．そこで本研究では，携帯電話へのメール送信に基づくワンタイムパスワードを用いたログインシステムを提案する．

本研究で扱うワンタイムパスワードとは，認証に一度しか使用できない使い捨てのパスワードを用いることで，パスワードが盗まれてもそのパスワードで再度ログインすることを困難にする認証技術である．ワンタイムパスワードは，チャレンジという認証毎に毎回変化する値と，ユーザと認証サーバのみが知る秘密であるベースシークレットから生成される．ワンタイムパスワードを計算するパスワード生成器のことをトークンと呼び，その実現方法によってハードウェアトークンとソフトウェアトークンに分類される．また，チャレンジをトークンと認証サーバで同期させておく同期方式と，認証毎に認証サーバからチャレンジが送信される非同期方式に分類される．

2. マトリクス認証

マトリクス認証とは，セキュアプロバイダ（現パスロジ）によって開発された，非同期式のワンタイムパスワードの一つである．マトリクス認証では，2 次元の表の中に配置された文字や数字の位置情報をベースシークレットとして用いる．認証時には，毎回異なる数字や文字がランダムに碁盤目状に並ぶ表がチャレンジとして用意される．この中で，自分が指定したパターンの通りに並んでいる数字や文字を選んで入力していき，これをワンタイムパスワードとして使用する．

3. メール送信とマトリクス認証を組み合わせたログインシステムの設計と実装

本研究では，ワンタイムパスワードによるログインシステム，及びそのログインシステムの動作するウェブページを設計，開発し，動作確認を行う．ワンタイムパスワードの方式にはマトリクス認証を用いる．また，認証時に使用するマトリクス表はユーザの携帯電話に対してメールにより送信することを想定している．図 1 にシステムのシーケンス図を示す．本提案の特徴は既存のマトリックス認証に携帯電話でのメール送信を組み合わせていることである．利用者とメールアドレスの関連性が保証されていることにより、マトリクス表をサーバが指定したユーザに確実に送信させることができる．また，ワンタイムパスワードを入力する通信チャネルと別なチャネルでマトリクス表を送信

豊田工業高等専門学校 情報科学専攻

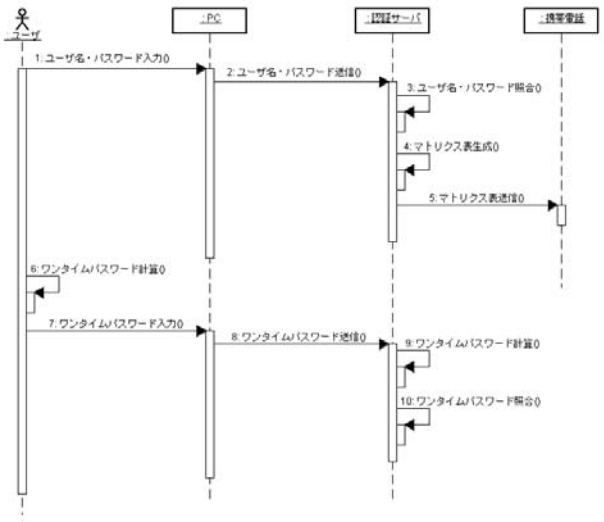

図 1．システムのシーケンス図

することにより，攻撃者にマトリクス表とワンタイムパスワードの情報を同時に盗聴されるのを防ぐことができるようになる．これはマトリクス表とワンタイムパスワードから位置情報を推測されるのを困難にするのに有効である．

4. 提案するログインシステムの実装

ログインシステム及びウェブページの開発には，データベースを用いたウェブアプリケーション開発のプロトタイピングが容易な Ruby on Rails を利用する．認証に用いるマトリクス表には，0～9 までの数字が各 5 回出現するものとし，縦 10×横 5 のものを利用するものとした．本研究では図 1 に示すシーケンス図を実現するマトリクス認証とメール送信によるログインシステム及びウェブページを開発し，動作確認を行った．

5. 考察

5.1　ワンタイムパスワードの考察

ワンタイムパスワードと固定パスワードとを比較し，ワンタイムパスワードのセキュリティ強度にどのような特徴が存在するのかを示す．そこで，パスワードに対して総当り攻撃を仕掛けた時に，

- パスワードを破るのに必要な試行回数の期待値 E(k)
- k 回試行を行うことでパスワードが破られる確率 P'k
- i 回の試行によって j 回連続で認証が成功する確率 P"

を求めた．結果を表 1，図 2 に示す．ここで，表中の n は使用できるパスワードの総数である．例えば，数字 8 桁のパスワードでは $n=10^8$ となる．

結果より，ワンタイムパスワードは固定パスワードと比べて倍の試行回数が必要なことが分かる．また，P'k については P'pwk≧P'otpk の関係が成り立ち，ワンタイムパスワードの方がパスワードが破られる確率が低いことが分かる．そして，P"に関しては P"pw≧P"otp の関係が成り立つことが分かる．よって，ワンタイムパスワードは連続した総当り攻撃に対して強いことが確認できた．

表 1．パスワードの強度

	固定パスワード	ワンタイムパスワード
$E(k)$	$\frac{n}{2}$	n
$P\prime_{\mathrm{k}}$	$\frac{k}{n}$	$\frac{n^k-(n-1)^k}{n^k}$
$P\prime\prime$	$\frac{i-j+1}{n}$	$\frac{n^{i-j+1}-(n-1)^{i-j+1}}{n^i}$

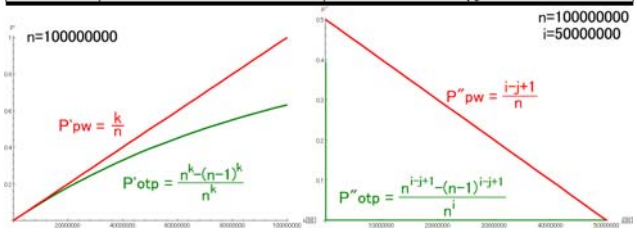

図 2．P’k 及び P”のグラフ

5.2　マトリクス認証の考察

提案システムでのマトリクス認証は，ワンタイムパスワードとマトリクス表から実質的なパスワードである位置情報を推測することで実現している．これは，実際に実用化されているマトリクス認証でも，位置情報をデータベースに記録していないためである．しかし，この方法では複数の位置情報から正しい位置情報を推測しており，正しいパスワード以外でも認証が成功してしまう．本節では，この実装方法によってどの程度セキュリティが低下するのかを考察する．

あるマトリクス表の特定の数字に対応する位置は，今回の実装では 1 つの数字に対して 5 つ存在する．その後，新しく生成したマトリクス表では前述の 5 つの位置には違う数字が割り当てられる．そこで，この時に割り当てられる数字の種類の期待値 Em を求める．その結果，Em≒4.23[種類]となることがわかった．

次に，正しいパスワード以外でも認証が成功してしまう確率 Pe を求める．その結果，Pe≒1/969 の確率で認証を成功してしまうことが分かった．使用できるパスワードの総数は 10^8 なので，1 度の試行でパスワードが破られる確率は本来のものより約 100000 倍に増加している．

提案システムの実装方法では，データベースの内容が流出してもパスワードが特定されないようにあえて位置情報ではなくワンタイムパスワードとマトリクス表だけをデータベースへ保存する方法を用いた．しかし，これにより正しくないパスワードでも認証が成功してしまうことが分かった．

そこで，マトリクス認証の実装方法について考察する．データベースへのパスワードの保存方法には以下の方法が考えられる．

1. ワンタイムパスワードマトリクス表を保存する
2. 位置情報を暗号化してから保存する
3. 位置情報をハッシュ暗号化してから保存する

これらの方法を比較・検討する．まず，提案システムの実装方法である方法 1 は，本節での考察どおり 1 度の試行でパスワードが破られる確率は増加しているが，データベースの内容が流出しても位置情報は特定できない利点を持つ．方法 2 は，1 度の試行でパスワードが破られる確率は本来と同じだが，データベースの内容が流出した際の安全性が暗号化アルゴリズムと暗号鍵の扱いに依存してしまう．それに対して，方法 3 は暗号鍵が存在しないため，データベースの内容が流出した際の安全性はハッシュ暗号化アルゴリズムのみに依存する．よって，データベースの内容が流出した際の安全性は方法 2 以上となる．また，1 度の試行でパスワードが破られる確率は本来と同じとなる．しかし，ワンタイムパスワードとマトリクス表から得られる位置情報の全組合せについてハッシュを計算する必要がある．

よって，基本的には方法 2 によって位置情報を保存する方法を選び，データベースや暗号鍵を適切に運用することが望ましいと考えられる．また，相対的にログイン頻度が少なくサーバの処理能力が高いシステムでは，方法 3 によって位置情報を保存する方法を選ぶのも有効だと考えられる．

5.3　メール使用の考察

提案システムでは既存のマトリクス認証と違い，マトリクス表をメールでユーザに送信している．これにより提案システムがどのように改善されたかを考察する．

メールを使用することによるデメリットは，ユーザの手間が増加することである．しかしメリットとして，セキュリティの強化が挙げられる．

まず，第三者がマトリクス表とワンタイムパスワードを同時に入手することが難しくなっている．携帯電話に送られるマトリクス表と PC 上で入力するワンタイムパスワードの同時入手は難しいためである．第 6.2 節で述べたように，マトリクス表とワンタイムパスワードの同時入手により位置情報の推測が可能になるため，マトリクス表とワンタイムパスワードの同時入手を防ぐことはセキュリティの強化に繋がる．

また，第三者がユーザに気付かれずにログインを試行することは難しくなっている．認証毎にマトリクス表がユーザに送信されることで，第三者がログインを試行したことがユーザ本人に通知されるためである．

6．まとめ

本研究では，安全なウェブページのログインシステムを実現するために，携帯電話のメールを用いたマトリクス認証によるワンタイムパスワードのログインシステムを設計，開発を行い，動作を確認した。そして，開発したシステムの安全性についての考察を行った。その結果，既存の固定パスワードに加えてマトリクス認証をメールと組み合わせることにより、安全性が向上することが確認できた。

参考文献

[1] Richard E.　Smith 著，稲村 雄 監訳，認証技術 パスワードから公開鍵まで