G-20

# NFC タグを用いたパスワード認証システムの検討

**Study of password authentication system using NFC tag**

○渡邉　裕樹[1], 泉　　隆[2]
*Yuki Watanabe[1], Takashi Izumi[2]

Abstract：Services such as the online banking has become widespread.　These services are needed highly secure authentication, such as the one-time password is used. However, there is a problem in terms of convenience.　In this study, we examined the password authentication system with highly safety and convenient using inexpensive NFC tag.

## １．まえがき

インターネットバンキングなどのサービスが普及してきている。このような中，平成 27 年度のネット上の不正アクセス認知件数は 2,051 件と前年度の 3,545 件に比べて減少しているものの，インターネットバンキングに係る不正送金事犯の被害額は約 30 億 7300 万円と過去最高を記録している[1]。これらのサービスでは安全性の高い認証が必要とされ，多くはワンタイムパスワードが使われている。しかし，利便性の点で，「手間が増える」「パスワードを覚えきれない」などの問題がある。これに対して，IC カードを用いた認証も考えられているがコストがかかるなどの問題がある。本研究では，安価な NFC タグ[2]を用いて，安全かつ利便性の高いパスワード認証システムについて検討した。

## ２．認証方式について

<2・1>　パスワード認証

あらかじめ本人が登録した固定文字列を毎回の認証で使う固定パスワードを用いる認証方式が一般的であり，簡単かつ容易なため広く普及している。パスワードの安全性を上げるために，複数の文字種を使う，文字列を長くすることが求められている。そうすると，利用者がパスワードを覚えるのが難しい。このパスワード方式では，パスワードクラックや盗聴されるなどの危険性もある。

<2・2>　ワンタイムパスワードを用いた認証

パスワード認証の安全性を高めるために，毎回異なる文字列を使い捨てるワンタイムパスワード（OTP）を用いた認証がある。固定パスワードより通信の盗聴等に強い。アプリケーションやトークンに表示されるパスワードをログイン毎に入力するものである。以下に方式の種類を示す。

（１）チャレンジアンドレスポンス方式

クライアントがサーバにアクセスすると，サーバはチャレンジと呼ばれるランダムな文字列をユーザに送信する。これに対しユーザ側では，チャレンジとパスワードを合成したレスポンスと呼ばれる文字列を作成してサーバに送信する。サーバ側も同じようにレスポンスを作成し，受信したレスポンスと照合することで認証するものである。

（２）トークン方式

ワンタイムパスワードを生成するトークンと呼ばれる機器やソフトウェアを利用して，あらかじめサーバ側と時刻やカウンタを同期した上で，ランダムな文字列からなるパスワードを生成するものである。生成したパスワードを入力した後，接続できる。

従来の銀行のオンラインバンキングなどでは，利用者に印刷した乱数表を配布しておき，これを利用してワンタイムパスワードを生成するものがあった。最近は，上記のワンタイムパスワードを生成するのに，ワンタイムパスワードアプリやワンタイムパスワードカード（電卓版）などのものが出ている[3]。これらの方式はいわゆるトークン方式と類似のものであるが，ワンタイムパスワードを携帯で受けたり，マトリクスから拾ってきたりしたものを再度入力する必要があり，手間がかかるといった問題がある。そこで，NFC タグを利用した，安価でかつ手間のかからない認証方式を提案する。

## ３．提案するパスワード認証方式

2 章のワンタイムパスワード生成方式の 2 つの方法を併用することを考える。(2) のトークン方式のトークンの代わりに安価な NFC タグを用いることを考える。そして，クライアントにスマートフォンを接続し，そのスマートフォンで NFC タグから乱数を読み取り，そのワンタイムパスワードを PC 経由で送信することによって，パスワードの手入力を省略しようとするものである。なお，パスワード生成のための乱数データは，NFC タグに格納するので，PC やスマートフォンとはトークンと同様に独立の関係にある。

提案システムの構成を図 1 に示す。また，パスワード認証の流れを図 2 に示す。

１：日大理工・学部・情報　２：日大理工・教員・情報

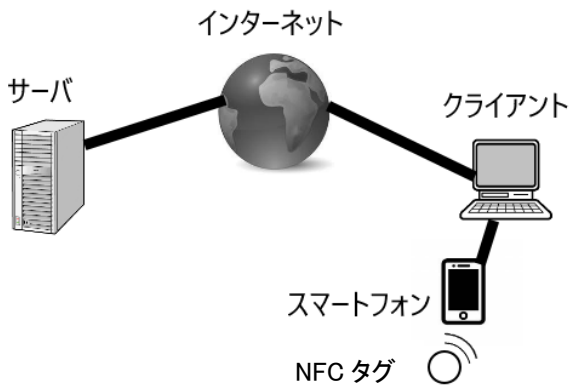


Fig.1. The configuration of the proposed system.

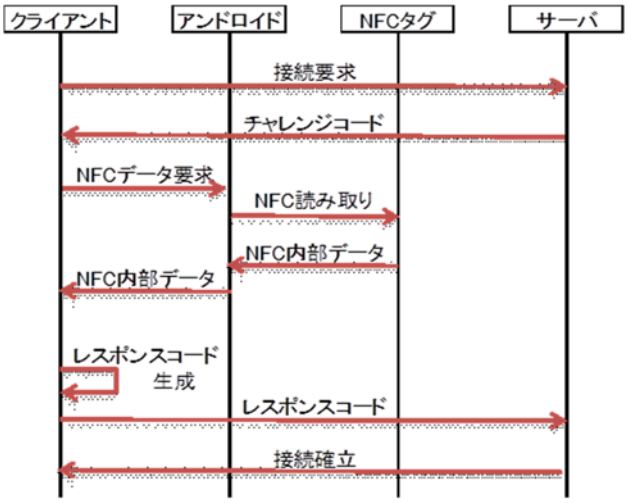


Fig.2. Flow of the proposed password authentication.

図 2 の流れでは，まずクライアントからサーバに接続要求を送信，サーバはそれに対してチャレンジコードを生成し返信する。次にクライアントは USB でつながれたスマートフォン端末を利用し NFC タグのデータを読み取る。それをもとにしてレスポンスコードを作成するサーバに送信する。サーバ側でもレスポンスコードを作成しクライアントから送信されたコードを照合し，合っていた場合は接続を確立する。その後，NFC タグの内容を更新する。この更新機能によって，トークンや電卓版カードと同等の安全性が得られると考える。

ここで NFC の内部に格納するデータは，データの容量を考慮しつつ，既存のワンタイムパスワードシステムに用いられていることが多い乱数表を考えている。

## ４．本研究に用いる乱数

研究で用いる言語は Java，乱数の生成には java.util の Random を用いる。この関数からは，4 バイトデータが出力されるが，NFC タグの記憶容量などを考えると 2 バイト程度までが適当なので，1 バイト又は 2 バイトデータを 1 桁として扱うことを考える。なお，手入力を考えていないので，1 桁として扱う数値の長さは考えなくてよい。

そこで，表 1 のスペックをもつ PC を用い，総当たり攻撃を想定した解読時間を計測した。実測をもとに算出した桁数に対する解読時間を表 2 に示す。表 2 の結果より，1 バイトでは，8 桁でも 100 秒で終了するのに対し，2 バイトでは 8 桁で 136.5 年となるので，2 バイトかつ 8 桁以上が適していると考えられる。

Table 1. PC specifications used in the experiment.

| | |
|---|---|
| OS | Windows10 64bit |
| CPU | Intel i7-3517U |
| メモリ | 4096MB |

Table 2. Decoding time for the number of digits. (Brute force attack)

| 桁数 | 1byte | 2byte |
|---|---|---|
| 1 | 10μs | 90μs |
| 2 | 100μs | 8.1ms |
| 3 | 1ms | 729ms |
| 4 | 10ms | 65.6s |
| 5 | 100ms | 98.4min |
| 6 | 1s | 147.6h |
| 7 | 10s | 553.5day |
| 8 | 100s | 136.5year |

## ５．まとめ

NFC タグを利用したパスワード認証システムを提案した。これによって，従来のパスワード認証方式に比べて，安価でかつパスワード認証の手間の少ないシステムの構築が期待できる。

今後は，スマートフォンアプリを作成し，模擬実験を行う。

## ６．参考文献

[1] 警察庁：「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」，http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf (2016-04)

[2] Sony Japan：「FeliCa | NFC について | NFC の定義」，http://www.sony.co.jp/Products/felica/NFC/ (2016-04)

[3] 三菱東京ＵＦＪ銀行：「ワンタイムパスワード」，http://direct.bk.mufg.jp/secure/otp/app.html(2016-09)