L-054

携帯電話を利用した取引同期型ワンタイムパスワードトークン
Transaction-Synchronized One-Time Password Token Using Cellular Phone

石田 夏樹† **佐々木 伸也**† **堤 俊之**†
Natsuki Ishida Shinya Sasaki Toshiyuki Tsutsumi

1．はじめに

インターネットバンキング等のオンラインサービスの普及に伴い，オンラインサービス利用者が PC に入力する本人確認情報が盗まれて悪用されるフィッシング詐欺被害が多発している．フィッシング詐欺対策としてオンラインサービス事業者は，本人確認情報を従来の固定パスワードから，認証毎に毎回異なるワンタイムパスワード（以下，OTP と略す）に強化しつつある[1].

しかし，現在多く利用されている時刻同期型 OTP は，PC とサーバの間で通信内容を改ざんする中間者攻撃に対して脆弱である．取引同期型 OTP は，サーバ側で OTP と取引内容の組み合わせを認証することで中間者攻撃を防止する．本稿では，携帯電話を利用した取引同期型 OTP トークンの実現方式を提案する．

2．時刻同期型 OTP

2.1 時刻同期型 OTP の特徴

時刻同期型 OTP は，一定時間毎に変化するパスワードである．利用者は時刻同期型 OTP トークンを持ち，トークンに表示された乱数を OTP として認証に使用する．

図 1 に，時刻同期型 OTP トークンの動作を示す．時刻同期型 OTP トークンは，サーバと同じ時刻を刻むタイマーを搭載し，一定時間毎に現在時刻を暗号化することで乱数を生成する．

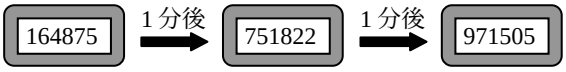

図 1: 時刻同期型 OTP トークンの動作

2.2 時刻同期型 OTP トークンによる取引認証処理

インターネットバンキングで銀行振込取引を行う場合を例に，図 2 に，時刻同期型 OTP トークンを使用した取引認証処理の手順を示す．ただし，トークンとサーバは，利用者毎に異なる秘密鍵を共有しているものとする．以下に，処理内容を説明する．

（1）PC がサーバに取引内容を送信する．
（2）サーバが PC に取引確認画面を送信し，PC が取引確認画面を表示する．
（3）トークンが現在時刻を暗号化して OTP を生成する．
（4）トークンが OTP を表示する．
（5）利用者が PC に OTP を入力する．
（6）PC がサーバに取引内容と OTP の組を送信する．
（7）サーバが現在時刻を暗号化して OTP を生成する．
（8）サーバが(6)で受信した OTP と，(7)で生成した OTP を比較して認証し，一致する場合は，認証成功として取引内容を執行する．

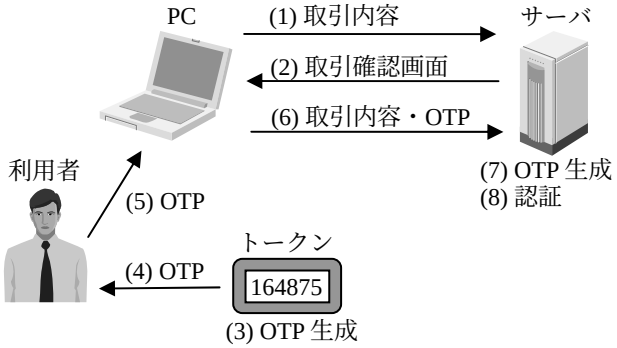

図 2: 時刻同期型 OTP トークンを使用した取引認証処理

2.3 中間者攻撃に対する脆弱性

時刻同期型 OTP には，利用者が要求した取引内容以外の認証に OTP が流用できるという脆弱性がある．この脆弱性を利用すると，中間者攻撃による不正な取引の執行が可能になる．

図 3 に，時刻同期型 OTP の利用者を狙った中間者攻撃の手口[2]を示す．(1)攻撃者は，利用者が PC に入力した取引内容と OTP の組を入手する．入手の手口には，利用者の PC にスパイウェアを仕掛ける，又は利用者を攻撃者が用意した偽のサーバにアクセスさせるといった手口がある．(2)次に，攻撃者は取引内容を改ざんし，改ざんした取引内容と OTP の組をサーバに送信する．

時刻同期型 OTP の場合，以上の(1)(2)が OTP の有効時間内に実行されると，認証が成功し，サーバでは攻撃者により改ざんされた取引内容が執行されてしまう．

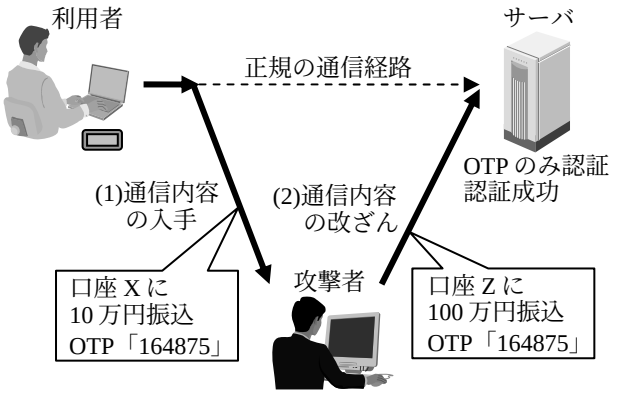

図 3: 時刻同期型 OTP の利用者を狙った中間者攻撃の手口

3．取引同期型 OTP

本章では，中間者攻撃に対して安全である取引同期型 OTP について説明する．

†日立ソフトウェアエンジニアリング（株）

3.1 取引同期型 OTP の特徴

取引同期型 OTP は，取引毎に変化し，特定の取引内容の認証に限り有効なパスワードである．利用者は，取引同期型 OTP トークンを持ち，トークンに表示された OTP を認証に使用する．

図 4 に，インターネットバンキングで銀行振込取引を行う場合を例とした，取引同期型 OTP トークンの動作を示す．取引同期型 OTP トークンは，サーバから，取引内容とその取引内容の認証に限り有効な OTP の組を取得する．

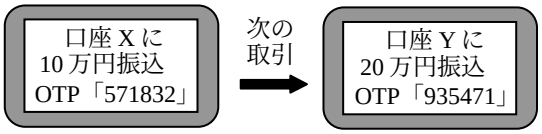

図 4: 取引同期型 OTP トークンの動作

3.2 携帯電話を利用した取引同期型 OTP トークンによる取引認証処理

利用者の所有する携帯電話を利用した取引同期型 OTP トークンの実現方式を提案する[3].

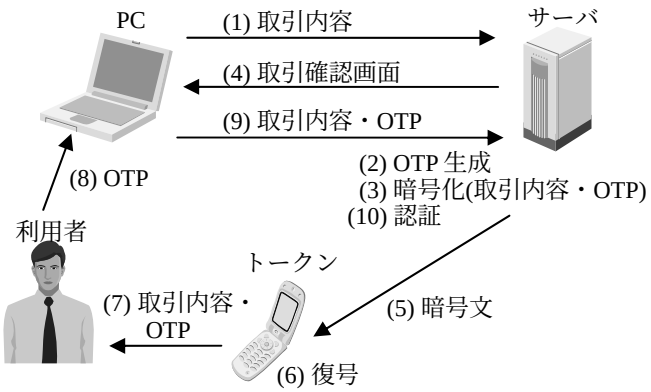

図 5: 取引同期型 OTP トークンを使用した取引認証処理

図 5 に，取引同期型 OTP トークンを使用した取引認証処理の手順を示す．ただし，トークンとサーバは，利用者毎に異なる秘密鍵を共有しているものとする．以下に，処理内容を説明する．

（1）PC がサーバに取引内容を送信する．
（2）サーバがランダムに OTP を生成し，(1)で受信した取引内容と OTP の組を記憶する．
（3）サーバが取引内容と OTP の組を暗号化する．
（4）サーバが PC に取引確認画面を送信し，PC が取引確認画面を表示する．
（5）トークンがサーバから暗号文をダウンロードする．
（6）トークンが暗号文を復号する．
（7）トークンが取引内容と OTP の組を表示する．
（8）利用者が取引内容を確認し，PC に OTP を入力する．
（9）PC がサーバに取引内容と OTP の組を送信する．
（10）サーバが，(9)で受信した取引内容と OTP の組と，(2)で記憶した取引内容と OTP の組を比較して認証し，一致する場合は，認証成功として取引内容を執行する．

3.3 中間者攻撃に対する耐性

図 6 に，取引同期型 OTP の中間者攻撃に対する耐性を示す．取引同期型 OTP の場合，利用者はトークンの表示を確認することで，認証前にサーバで執行される取引内容を確認することができる．これにより利用者は，OTP を取得するまでの手順（3.2 節の (1)〜(7)）で，PC とサーバの間で中間者攻撃を受けていないことを確認できる．

また，時刻同期型 OTP では，サーバで OTP のみで認証が行われるのに対し，取引同期型 OTP では，取引内容と OTP の組で認証が行われる．このため，たとえ中間者攻撃により，改ざんされた取引内容と OTP の組がサーバに送信されたとしても，サーバでは取引内容が不一致となるため認証に失敗し，改ざんされた取引内容が執行されることはない．

すなわち，取引同期型 OTP は，トークンに表示された取引内容の認証にのみ有効な OTP である．よって，たとえ攻撃者が OTP を入手したとしても，攻撃者は，OTP をトークンに表示された取引内容以外の認証に流用することはできない．

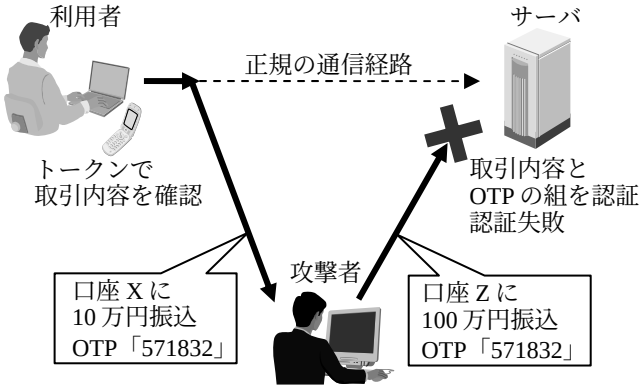

図 6: 取引同期型 OTP の中間者攻撃に対する耐性

4．おわりに

本稿では，携帯電話を利用した取引同期型 OTP トークンの実現方式を提案した．取引同期型 OTP は，トークンに表示された取引内容の認証に限り有効な OTP であり，従来の時刻同期型 OTP よりも高い安全性を実現する．

ただし，本稿が提案する取引同期型 OTP トークンは操作性に課題がある．時刻同期型 OTP トークンでは，OTP の取得の際にトークンの操作が不要であるのに対し，取引同期型 OTP トークンでは，サーバから暗号文を取得する際にトークンの操作が必要である．今後は，暗号文の取得方法を改良し，操作性の改善を図る．

参考文献

[1] 中山 靖司：日銀レビュー インターネットバンキングの安全性を巡る現状と課題：http://www.boj.or.jp/type/ronbun/rev/data/rev06j14.pdf
[2] IT Pro：ワンタイムパスワードでは防げない中間者フィッシングが出現：http://itpro.nikkeibp.co.jp/article/USNEWS/20060713/243303/
[3] 日立ソフトウェアエンジニアリング株式会社：取引連動型ワンタイムパスワード認証 ケータイ OTP：http://hitachisoft.jp/Products/K-OTP/