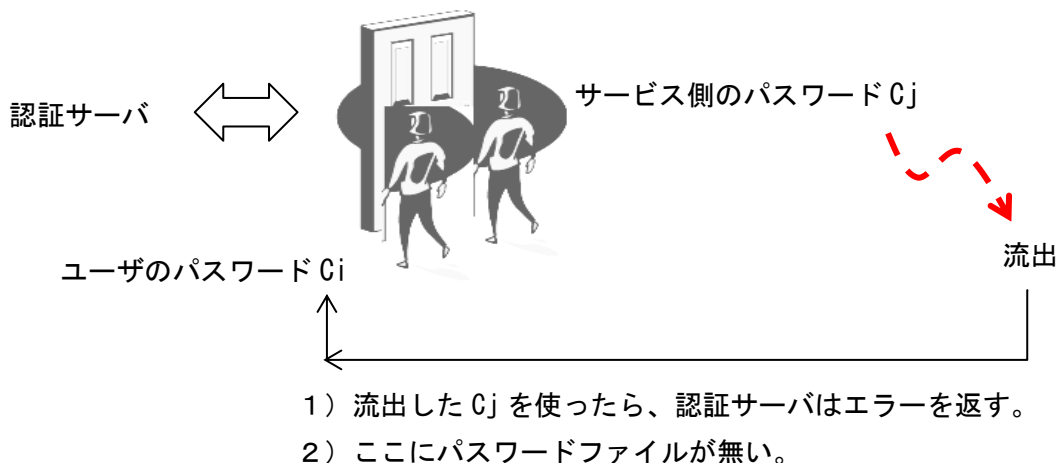


今後、パスワード入力は見かけなくなる！

【認証サーバセグメントにパスワードファイルは無いけど、認証サーバは認証の仕事をする】

二人の鍵（相異なる C_i と C_j : $C_i \neq C_j$ ）が揃わないとドアの鍵が作動しない、という扉システムが現実にあります。二つの鍵をパスワード C_i と C_j と読み替えて、この C_i と C_j が揃って扉に入ると、認証サーバが仕事をする、と考えてみましょう。これはパスワードファイルが無いという背景です；

図 1 ; $C_i \neq C_j$



もし、誰かがサービス側のパスワード C_j を盗み、この C_j 由来のパスワードを扉に入力するとどうなるでしょうか？認証サーバは $C_j=C_j$ を受け取ります。従来のパスワードは、 $C_j=C_j$ ならばそのユーザを認証します。しかし、本件の認証サーバは、 $C_j=C_j$ ならば、エラーを返します。

この $C_i \neq C_j$ という 2 つの確率変数を「二つで一つ™のパスワード」と名付けました。この $C_i \neq C_j$ は確率変数ですから、暗号（コード）です；記憶パスワードを「初期化」して与えます；初期化の後、その記憶パスワードはシステムから消去され、従って、個人の秘密は人の記憶の中だけに留まりますから、漏えいしない。（記憶パスワードのファイルは不要、記憶パスワードのバックアップ装置も不要）。

こういう情報技術を「鍵の知識分割と二重コントロール」と言います。この技術の情報基盤への実装は世界初です。もし、 $C_i \neq C_j$ が鍵の知識分割から生まれたものでないなら、その数理は最初から破たんしています。

【既存のログイン画面とのコラボレーション】

既存の、今お使いのログインの流れと「二つで一つのパスワード」はコラボレーションします。ATM を例に採って、その様子を図解します。まず、大掴みの流れを【対比表】に示します。

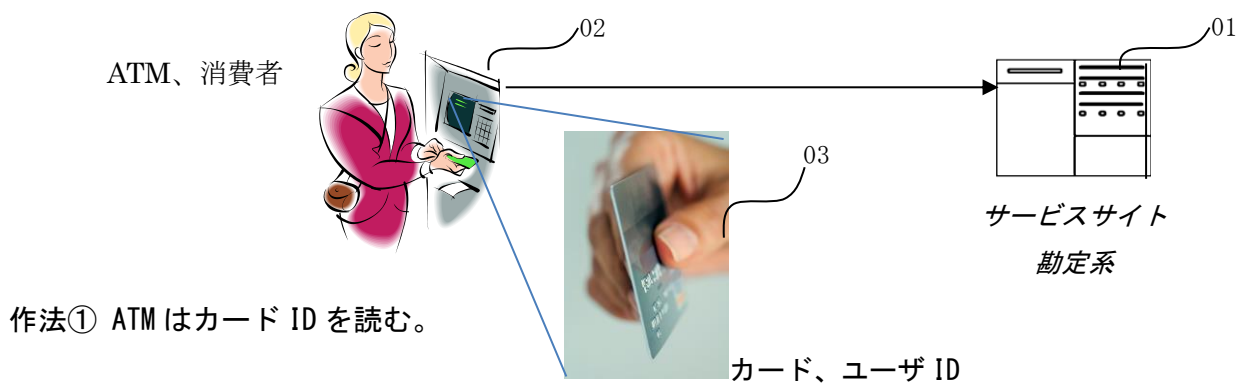
今後、パスワード入力は見かけなくなる！

【対比表】

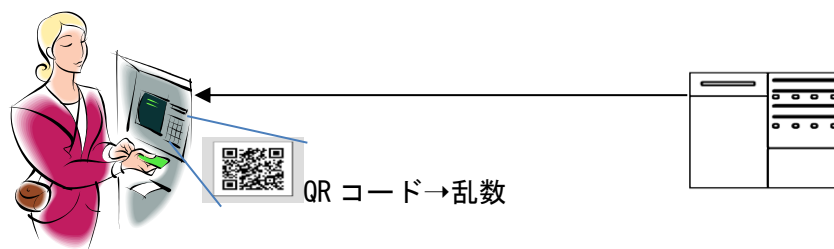
既存のログインの流れ	革新された部分	コラボレーションする
①カード ID の挿入		①カード ID の挿入
②画面が暗証番号の入力を促す ③暗証番号の入力	パスワード入力作法が無い	②画面が QR コードを表示する ③携帯端末が QR コードを読む
④金額の入力		④金額の入力

表 1； ログインの流れとコラボレーション

【ATM の場合】、通常の PC でも表面上は同様になる。

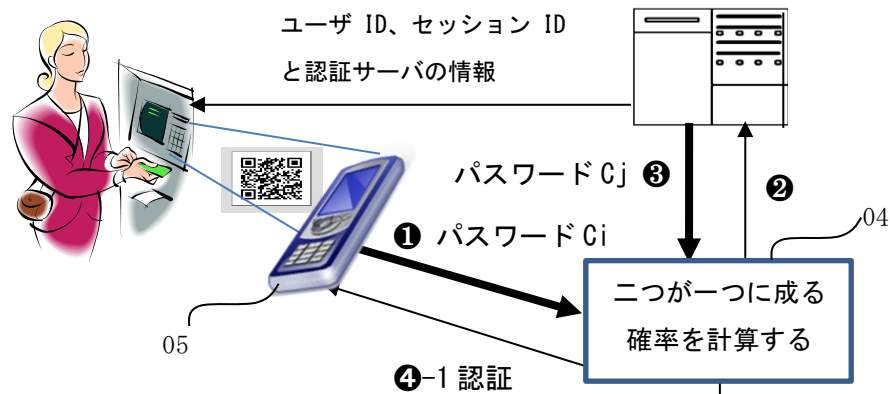


作法② 暗証番号の入力画面に代わって、QR コードを表示する。



今後、パスワード入力は見かけなくなる！

作法③ スマホに QR コードを読ませる。→入力操作が無い。



作法④ 金額をタッチインする画面



【考察】

夫が妻にカードを渡し、パスワード P を教れば、ATM は、通常通り、動作する。今回もカードとスマホを渡せば、ATM は、通常通り、動作する。この話は利便性を制限するか、しないか、は別の問題であることを意味する。では、何が変わったか？

- 1) 2 変数から構成されるパスワードが普及するにつれ、パスワード入力の姿を見かけなく成る。
→スキミングは困難、フィッシングも不可能。
- 2) アカウント・ハッキングを仕掛けられ、パスワードが不正に使用されても、それはエラーになる。→サイバー攻撃の脅威を減殺する。
- 3) 銀行行員がパスワード Cj のファイルを見ても、顧客に迷惑を掛けない。→自社構内を自社構内から守る。
- 4) 覚えやすいパスワード、「1 2 3 4」を何度使い回しても、何ら問題が起きない。流出したからと言って「1 2 3 4」の変更をお願いする必要も無い。→ISO の基準は過去遺物になる。
- 5) 記憶パスワードのバックアップ装置が不要になる。→情報基盤のリストラがビジネスに成る。

以上

2014 年 8 月 20 日