スマートフォンを利用した二要素認証による Web認証の強化について

中村素典 / 国立情報学研究所

平成24年7月4日
学術情報基盤オープンフォーラム

認証とは

- 認証の目的
  - サービスやリソースに**アクセスする権限を持つ**ことの証明
- 認証の手段
  - 権限を持っていることを証明するための**秘密情報の提示**
    - クレデンシャル（パスワード、公開鍵署名：トークンやICカード、等）
- 秘密情報に求められる特性
  - 容易に**推測**できないこと
  - 容易に**複製（なりすまし）**できないこと
  - 容易に**漏洩**しないこと
  - 利便性を大きく損なわないこと

  など

パスワードの問題点

- 推測されやすい
  - 長い文字列は覚えにくい→短くなる
    - 生年月日や電話番号など、容易に知りうる情報であることも
    - more than 10 percent of passwords used in Gillard's department could be easily broken in an hour by hackers using "brute force"

      http://www.zimbio.com/Prime+Minister+Julia+Gillard/articles/FlLSmfAsG2v/Australian+Prime+Minister+computer+hacked
  - アカウントごとに異なると覚えられない→同一パスワード
    - 75 Percent of Individuals Use Same Password for SNS and Email

      http://www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email
- 漏洩しやすい
  - 覚えられない文字列はメモされ、他人の目につきやすい
  - 安易に他人に教えることが可能
  - 通信路が安全であるかの確認が重要(HTTPS、サーバ証明書)
  - フィッシング被害を受けやすい
- 共有パスワード(共用アカウント)の問題
  - 守るべき秘密であることの意識が薄くなりやすい、更新を怠りがち、安易な伝達

認証統合、そしてシングルサインオン

- 認証統合
  - 組織の中でサービス毎に個別に管理されていたパスワード(とID)を一元管理
    - パスワードのより厳密な管理が期待(徹底)できる
      - 初期パスワードのまま放置されることがない
- シングルサインオン(「認証」と「認可」の分離)
  - セキュリティレベルの統一
    - HTTPS、サーバ証明書の確認すべき点が集約される
  - パスワードの入力先の一元化
    - フィッシングの難易度を上げやすい
- しかし、万一パスワードが漏洩した際の影響は大きくなる

パスワードの限界

- 推測攻撃（計算性能）の向上
- スパイウェアによる不正入手
- フィッシングに対する脆弱性
  - 似通ったドメイン名を用いた偽サイト
    - サーバ証明書の警告は出ない
    - IdPへのリダイレクトも含めて偽装されると気がつきにくい
      - ユーザ毎に異なる画像を出したりするのは効果的だけど。
  - 相互認証をしたいが、Webページにパスワード入力する限り無意味
- ソーシャルエンジニアリングに対する脆弱性
- 人間の入力ミス
  - 大学によっては、2種類（学内用、学外用）のパスワードを使い分け
    - 結局、可能性を減らしているだけに過ぎない
    - 学外サービスに、誤って学内用パスワードを入力してしまうかも

「認証」「認可」分離のメリット

- クレデンシャルの一元管理
- セキュリティレベルの統一
- クレデンシャルの入力先の統一
  - 高度な認証技術の導入が容易

- 共有パスワードなしに、グループアクセスが実現

高度な認証に対する需要:
NISTのLoA 技術要件 (NIST SP 800-63)

- レベル1
  - ユーザの同一性を保証(身元識別は不要)、認証の有効期限なし
  - チャレンジ-レスポンス可(辞書攻撃に弱い)
- レベル2
  - 単一要素認証、身元識別あり、失効処理の保証
  - オンライン推測攻撃を防止すること(パスワード/TLS可)
  - 認証サーバでの平文パスワード保持の禁止
- レベル3
  - 複数要素認証、ソフト暗号化トークン使用可
  - なりすまし攻撃、中間者攻撃を防止すること
- レベル4
  - 実用上最大限の保証、ハード暗号化トークンを使用
  - 認証後の暗号化処理も認証プロセスに結びつく鍵を使用

翻訳版:http://www.ipa.go.jp/security/publications/nist/documents/SP800-63-J.pdf

認証強化のメリット

- クレデンシャル流出の可能性低減
  - 推測によるもの
  - クラッキング（サーバへの侵入）によるもの
  - フィッシングによるもの
  - ユーザの不注意によるもの
- クレデンシャル流出時の対応コストの低減
- 確実な本人認証を必要とするサービスへの対応

認証方式のいろいろ

- マトリックス認証
  - マトリックス自体が秘密、位置情報が秘密
- ワンタイム（使い捨て）パスワード
- 生体認証（指紋、静脈、…）
- 電子証明書

5	0	G	T	V
A	3	E	2	R
8	D	K	P	U
Z	4	J	M	9
Q	F	L	X	7

容易に導入できる要件

- 発行（登録）、配布コストが低い
- ユーザ操作が簡単
- 新たな持ち物が増えない（特殊デバイス不要、紛失しにくい）
- 特殊なソフトウェアが不要
- 利用場所を選ばない
  - 汎用、多用途なものが望ましい
    - 複数ドメインでも共有可能であればなお良い

2要素認証による安全性向上

- 2つの要素（モノと記憶など）が揃って初めて認証が成立
  - ICカード＋PIN
  - ICカード＋生体認証
  - セキュリティトークン＋PIN

などなど

http://rsa.com/company/news/releases/images/SID800&SID7002.jpg

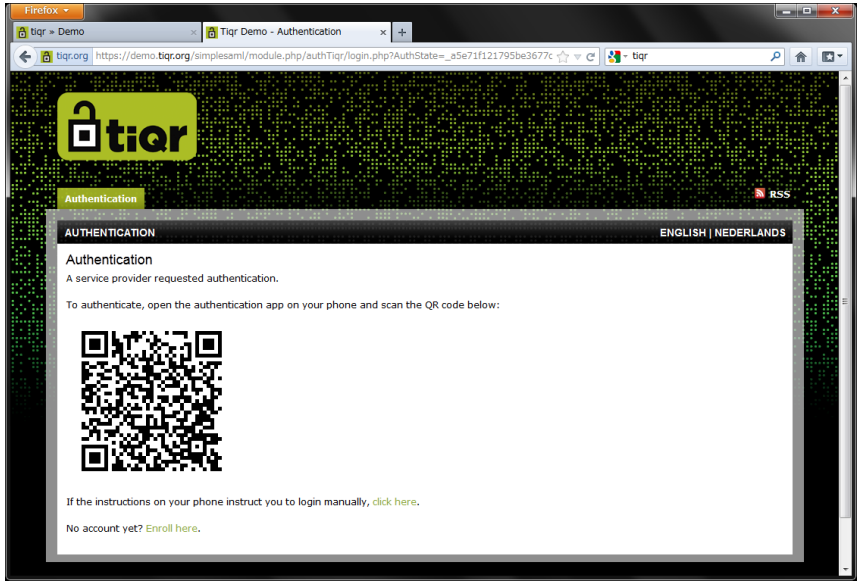
http://www.nikkei.co.jp/topic5/2004newpro/yusyut.html

http://japan.rsa.com/node.aspx?id=1313

- より優れた利便性を追求しSURFnetで開発された方式
  - 2010年より開発開始
  - Open Standardに準拠
  - スマートフォンのアプリとして実装（iPhone, Android対応）
  - QRコードを用いてユーザのログイン操作を軽減
  - https://tiqr.org/

Available on the App Store

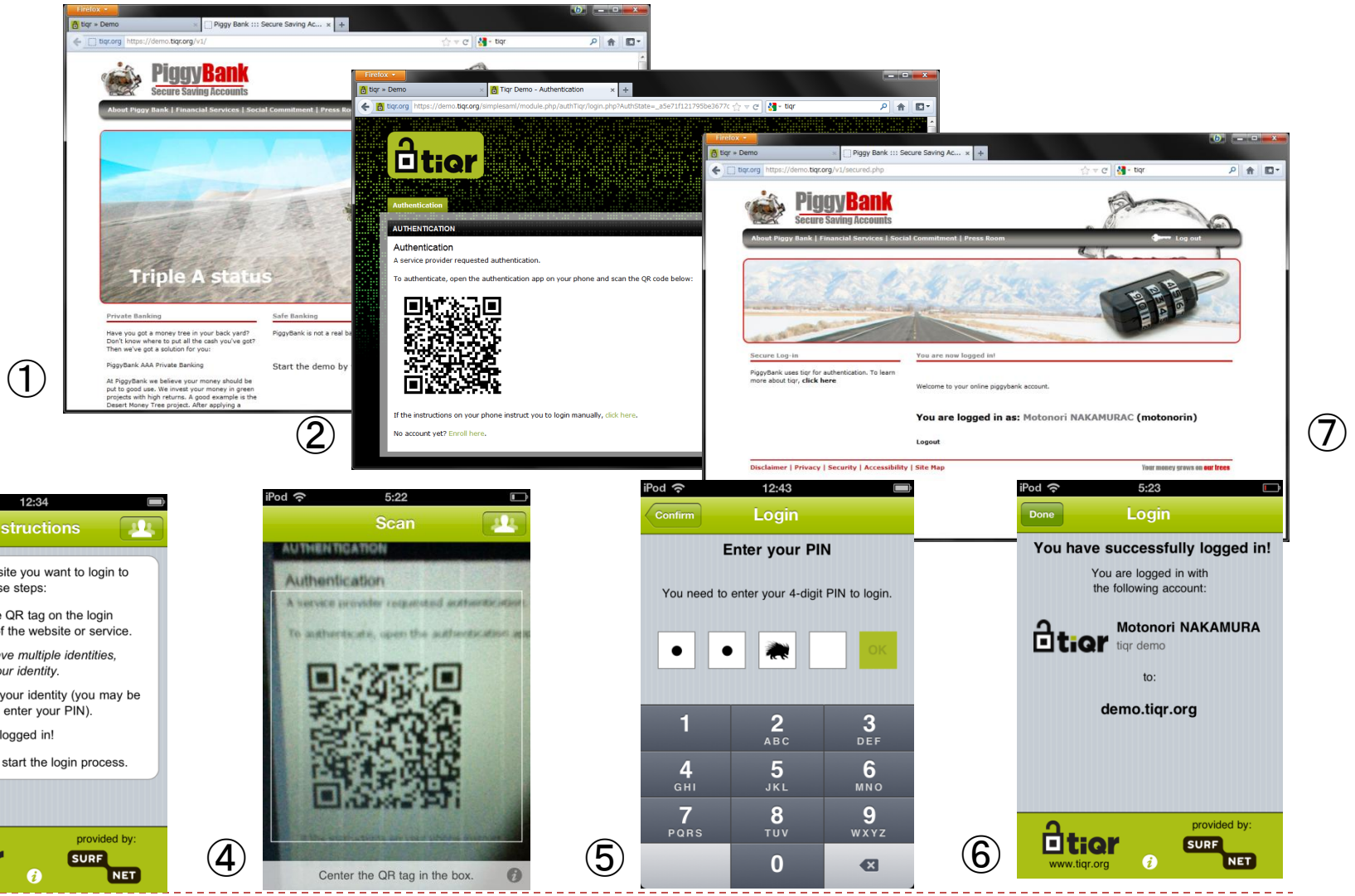
Download for Android



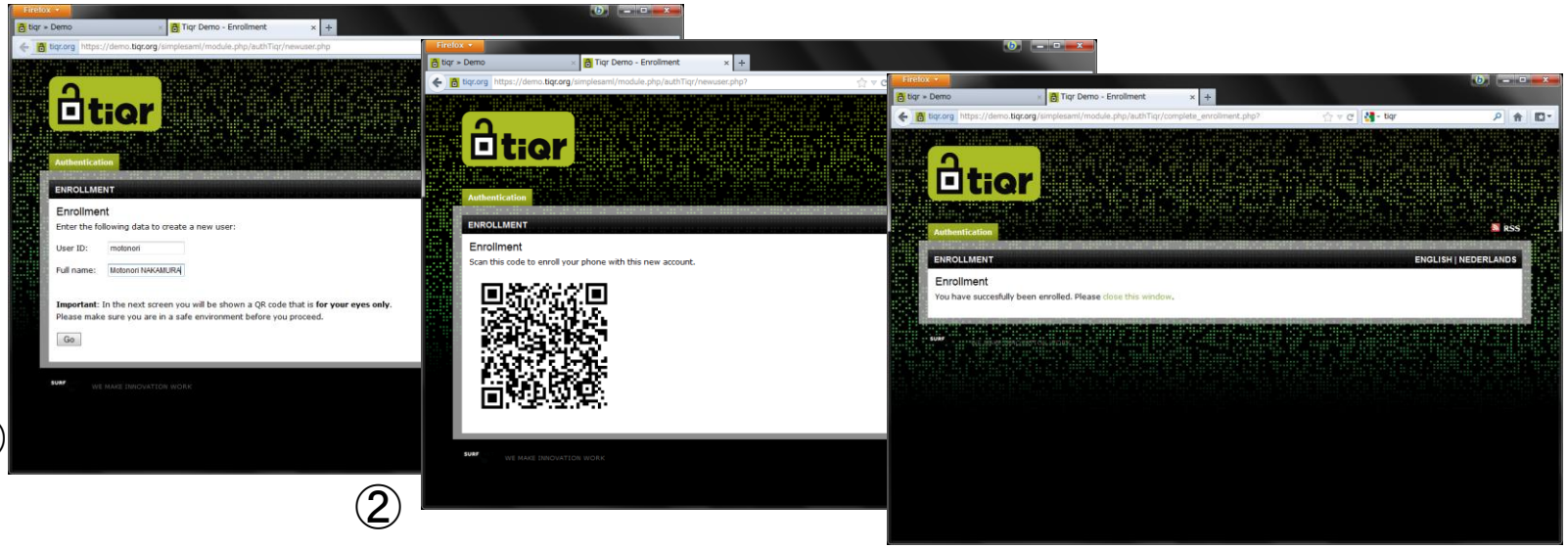
動作の概要

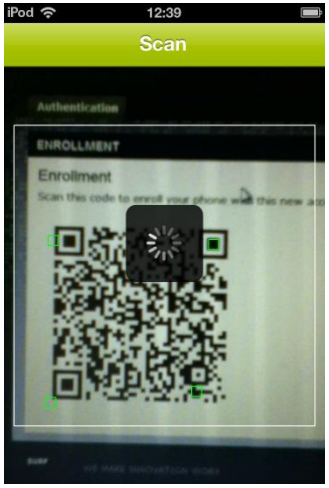
※スマホがネットワークに接続できない場合は、レスポンスを手入力することも可能

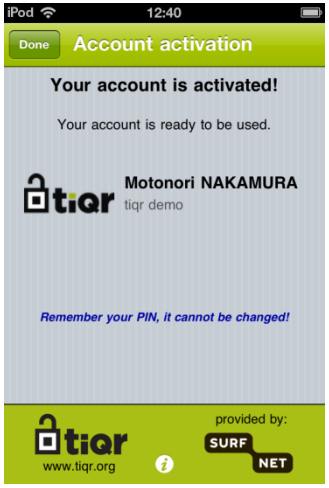
認証の手順（デモサイト）

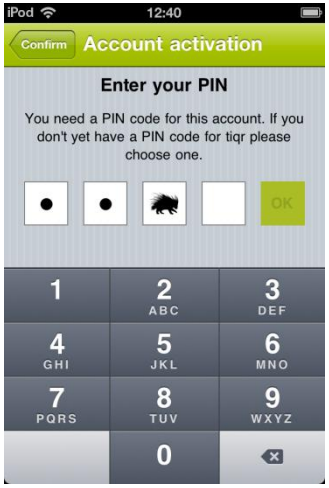

①
PiggyBank
Secure Saving Accounts
Triple A status
②
tiqr
Authentication
AUTHENTICATION
Authentication
A service provider requested authentication.
To authenticate, open the authentication app on your phone and scan the QR code below:
If the instructions on your phone instruct you to login manually, click here.
No account yet? Enroll here.
⑦
PiggyBank
Secure Saving Accounts
You are logged in as: Motonori NAKAMURAC (motonorin)
Logout
③
iPod 12:34
Scan
Instructions
Go to the website you want to login to and follow these steps:
Scan the QR tag on the login screen of the website or service.
If you have multiple identities, select your identity.
Confirm your identity (you may be asked to enter your PIN).
You are logged in!
Press Scan to start the login process.
tiqr
www.tiqr.org
provided by:
SURF NET
④
iPod 5:22
Scan
Center the QR tag in the box.
⑤
iPod 12:43
Confirm
Login
Enter your PIN
You need to enter your 4-digit PIN to login.
OK
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
⑥
iPod 5:23
Done
Login
You have successfully logged in!
You are logged in with the following account:
Motonori NAKAMURA
tiqr demo
to:
demo.tiqr.org
tiqr
www.tiqr.org
provided by:
SURF NET

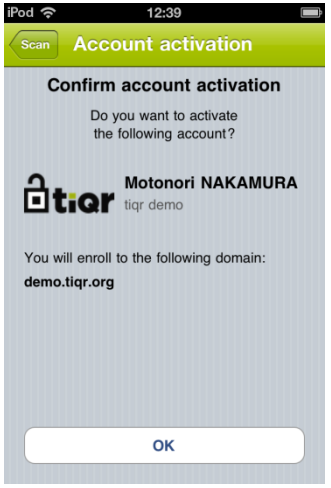
登録の手順（デモサイト）


①
②
⑦
tiqr
Authentication
ENROLLMENT
Enrollment
Enter the following data to create a new user:
User ID:
motonori
Full name:
Motonori NAKAMURA
Important: In the next screen you will be shown a QR code that is for your eyes only.
Please make sure you are in a safe environment before you proceed.
Go
Enrollment
Scan this code to enroll your phone with this new account.
ENGLISH | NEDERLANDS
Enrollment
You have succesfully been enrolled. Please close this window.


③
iPod 12:39
Scan
Authentication
ENROLLMENT
Enrollment


④
iPod 12:40
Done
Account activation
Your account is activated!
Your account is ready to be used.
Motonori NAKAMURA
tiqr demo
Remember your PIN, it cannot be changed!
tiqr
www.tiqr.org
provided by:
SURFNET


⑤
iPod 12:40
Confirm
Account activation
Enter your PIN
You need a PIN code for this account. If you don't yet have a PIN code for tiqr please choose one.
OK
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0


⑥
iPod 12:39
Scan
Account activation
Confirm account activation
Do you want to activate the following account?
Motonori NAKAMURA
tiqr demo
You will enroll to the following domain:
demo.tiqr.org
OK

実際に利用するには

- 初期登録の手順の検討が必要
  - 本人確認を行った上での登録
- 日本語への対応も必要
- tiqrは今のところSimpleSAMLphpのみに対応
  - Shibbolethには未対応…

2(多)要素認証の活用(併用)に向けて

- SP毎に、IdPに要求するLoAが異なるサービスの展開
  - 一つのSPの中でも、利用サービスによって異なる場合も
  - SPからの要求に応じた認証の例：
    - SP Aの利用のためにLoA 1で認証した後、SP Bをアクセスすると、再度LoA 2以上での認証が求められる等（レベルアップ）
    - ICカードを抜き取ると、LoA 3を求めるSPのサービスから自動的にログアウト（レベルダウン）
- 高度な認証処理への柔軟な対応のためには
  - 様々な認証方式の任意の組み合わせに対応可能な認証エンジンの実現が望まれる