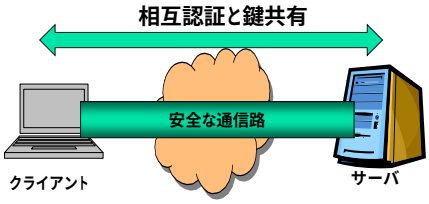
# パスワードを用いた認証鍵共有方式
## --フィッシング詐欺、所有物の盗難、サーバからの情報漏えいなどとどう闘うべきか --

(独) 産業技術総合研究所
情報セキュリティ研究センター
古原　和邦

## 相互認証と鍵共有

- ネット上で各種サービスを安全に提供したり、アクセスポイントや遠隔サーバに安全に接続する際に欠かせない技術






## 例

- ネットバンキング
- オンライントレード
- 遠隔サーバ･社内LANへのログイン
- ホットスポットやネットワークへの接続
- など

IT社会を支える重要な社会基盤の一つ



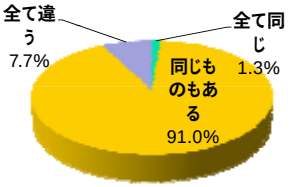
## パスワードを用いた方式の実運用上の問題点

- パスワードの入力場所を間違える (フィッシング詐欺)
- 同じパスワードを複数のサーバで利用
  - サーバ管理者の不正 (内部犯罪) やサーバからの情報漏えいに弱い
- (もしくは複数のパスワードを覚えなければならない)
  - 利便性の低下
- 所有物 (端末、携帯端末、トークン) を持たせた場合には紛失･盗難のおそれあり
  - (パスワードのオフライン全数探索が可能な場合あり)
- など

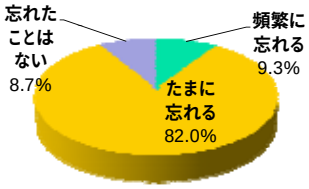


## ID,パスワードに関するアンケート結果

ID･パスワードは、同じ物を利用していますか？




登録した ID･パスワードを忘れることがありますか?




『ID･パスワードに埋もれる日々、90%以上が「忘れたことがある」』, インターネットコム株式会社, 株式会社インフォプラント,
http://japan.internet.com/research/20050909/1.html, 2005.09

## 対策の方向性

- 対策1：教育、啓発
- 対策2：注意を喚起するインターフェースの導入
  - 静的セキュリティ表示
  - 動的セキュリティ表示
- 対策3：新たな認証鍵共有方式の検討および導入

## 各対策の位置づけ

即座に対応可能

↕

長期的な計画が必要

周知徹底の難しさ（利用者次第）

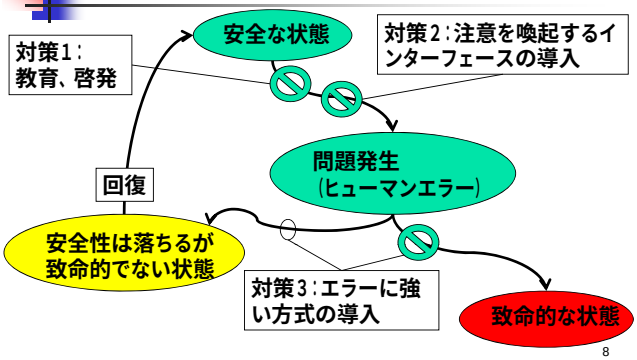
↕

技術によるセイフティーネット

- 対策1：教育、啓発
- 対策2：注意を喚起するインターフェースの導入
- 対策3：新たな認証鍵共有方式の検討および導入



## 各対策の位置づけ





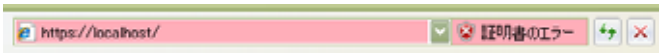

## 対策の方向性

- 対策1：教育、啓発
- 対策2：注意を喚起するインターフェースの導入
  - 静的セキュリティ表示
  - 動的セキュリティ表示
- 対策3：新たな認証鍵共有方式の検討および導入



## 静的セキュリティ表示の例：カラーアドレスバー、南京錠など

提示された証明書に問題がある場合：




提示された証明書に問題がない場合：


EV (Extended Validation) ガイドラインに準拠して発行された証明書(EV証明書)により検証された場合：



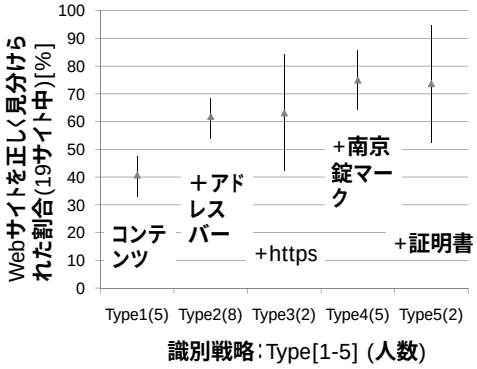

## 動的セキュリティ表示の例：ダイナミックセキュリティスキン

認証鍵共有にはPAKE (SRP)を利用

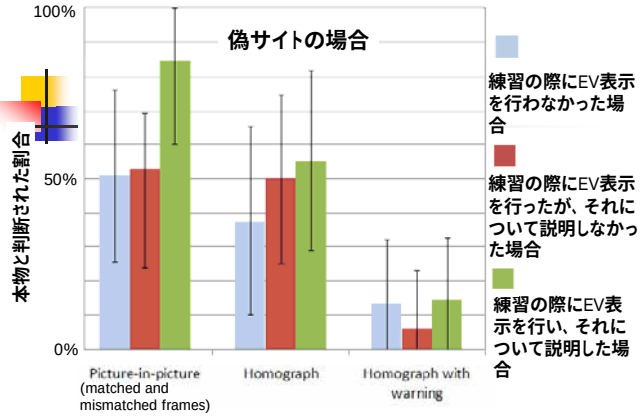

R. Dhamija and J.D. Tygar, “The Battle Against Phishing: Dynamic Security Skins,” Symposium On Usable Privacy and Security (SOUPS) 2005

## 

巧妙に作られたWebサイトには90%の被験者がだまされた




R. Dhamija, J. D. Tygar and Marti Hearst, “Why Phishing Works” Proc. of the Conference on Human Factors in Computing Systems (CHI2006), 2006.04




"An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks", C. Jackson, D. Simon, D. Tan and A. Barth, Usable Security (USEC'07), 2007.02

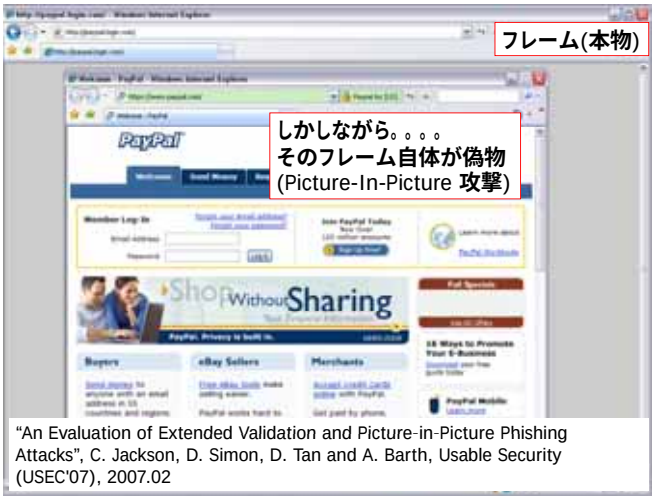


## Homograph (まぎらわしい名前)

- http://www.paylai.com/
- http://www.paypa1.com/
- http://www-bankofthewest.com/
- http://www.bankofthevvest.com/




"An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks", C. Jackson, D. Simon, D. Tan and A. Barth, Usable Security (USEC'07), 2007.02




"An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks", C. Jackson, D. Simon, D. Tan and A. Barth, Usable Security (USEC'07), 2007.02

## 教訓

- 教育や啓発は方法を間違えると逆効果
- 人間は間違えやすい生き物である (うっかりミスを0にするのは非常に困難)
- 入力情報のみに安全性を頼る認証方式の限界
  - 例) パスワード+OTP+マトリクス認証は入力箇所の詐称に弱い
- 長期的な視点で代替方式を検討する時期？



## パスワードを用いた認証鍵共有方式の比較(1/2)

○:耐性あり、X:耐性なし (短いパスワードが利用された場合)

| 方式 | 通信路の盗聴 | 並列オンライン攻撃 | 情報漏えい耐性 | | | 入力箇所間違い |
|---|---|---|---|---|---|---|
| | | | クライアント側から | サーバ側から | 時間差で両者から | |
| Classical PW-based (CHAP, IPsec PSK, LEAP, etc.) | X | X | ○ | X | X | X |
| PAKE | ○ | X | ○ | X | X | X |
| PKI (Server Auth.+PW) | ○ | X | ○ | X | X | X |
| PKI (Server Auth.+PW+OTP+Matrix) | ○ | ○ | ○ | X | X | X |
| PKI (Mutual Auth.) | ○ | ○ | X | ○ | X | ○ |
| LR-AKE | ○ | ○ | ○ | ○ | ○ | ○ |

## パスワードを用いた認証鍵共有方式の比較(2/2)

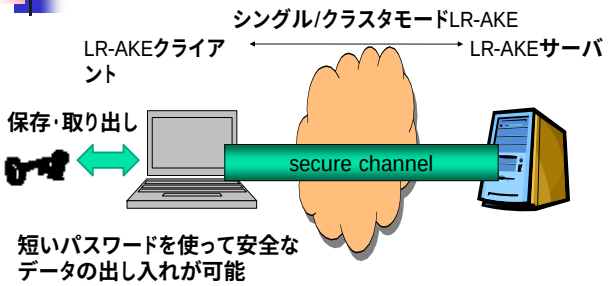
| | 方式 | 利用者の負担 パスワードの記憶 | 所有物 | 公開鍵の検証 |
|---|---|---|---|---|
| 1要素認証 | Classical password-based (CHAP, IPsec PSK, LEAP, etc.) | 複数 | 不要 | 不要 |
| 1要素認証 | PAKE | 複数 | 不要 | 不要 |
| 2要素認証 | PKI (server auth. + password auth.) | 複数 | 不要 | 必要 |
| 2要素認証 | LR-AKE | 一つ | 必要 | 不要 |
| 2要素認証 | PKI (server auth. +PW+OTP+Matrix) | 複数 | 必要 | 必要 |
| 2要素認証 | PKI (mutual auth.) | 一つ | 必要 | 必要 |

## 我々の提案(1/2)

- 入力情報を取られても致命的な状態に陥らない相互認証方式であって、かつ、記録情報の漏えいに強い相互認証鍵共有方式の検討
  - 例) LR-AKE (Leakage-Resilient Authenticated Key-Establishment)
  - 利用者が記憶すべき情報は短いパスワード一つでよくなる
  - 記録情報を持ち歩く必要があるが、可搬媒体(USB,SDメモリなど)の普及、低価格化によりその敷居は下がりつつある



## LR-AKEの応用例 (オンライン分散ストレージ)



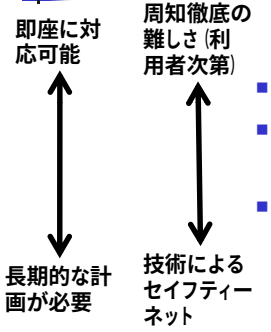

短いパスワードを使って安全なデータの出し入れが可能
(クライアント、サーバいずれの記録情報からも推測不可能)

## 我々の提案(2/2)

- WEBサイト毎のパスワードやクレジットカード番号などの入力は機械に任せる
  - 例) LR-AKEと連携して動作するWEBインターフェース (LR-LoginChecker)
  - 記録情報の漏えいに強い
  - サーバ側の変更は不要



## 今後の展望




- 対策1: 教育、啓発
- 対策2: 注意を喚起するインターフェースの導入
- 対策3: 新たな認証鍵共有方式の検討および導入