

# 日本におけるフィッシングと関連事件

## *Phishing & related issues in Japan*



情報セキュリティ大学院大学  
INSTITUTE of INFORMATION SECURITY

フィッシング対策協議会  
技術・制度検討WG主査  
情報セキュリティ大学院大学  
内田 勝也

Council of Anti-Phishing in Japan  
Chair of A.P. Technology & System Study WG  
Institute of Information Security  
Katuya Uchida, Professor, Ph.D.



CeCOS II 東京  
TOKYO May 26 & 27, 2008



## 本日の内容

1. Phishingの分類: Taxonomy of Phishing in Japan
2. 携帯電話でのワンクリック詐欺: About Click fraud via Cellphone
3. 振り込め詐欺: Furikome-Sagi (Money Transfer Fraud)
4. Phishing報告件数: No. of Phishing reported, APWG vs Japan
5. 日米コンピュータ犯罪とセキュリティ調査:  
Computer Crime & Security Survey  
~Dollar Amount Losses by Type USA vs Japan~
6. 日本のコンピュータ犯罪の特徴: Computer crime in Japan
7. 振り込め詐欺等の統計: Furikome-sagi (Money Transfer Fraud)
8. 今後を考える: About the future



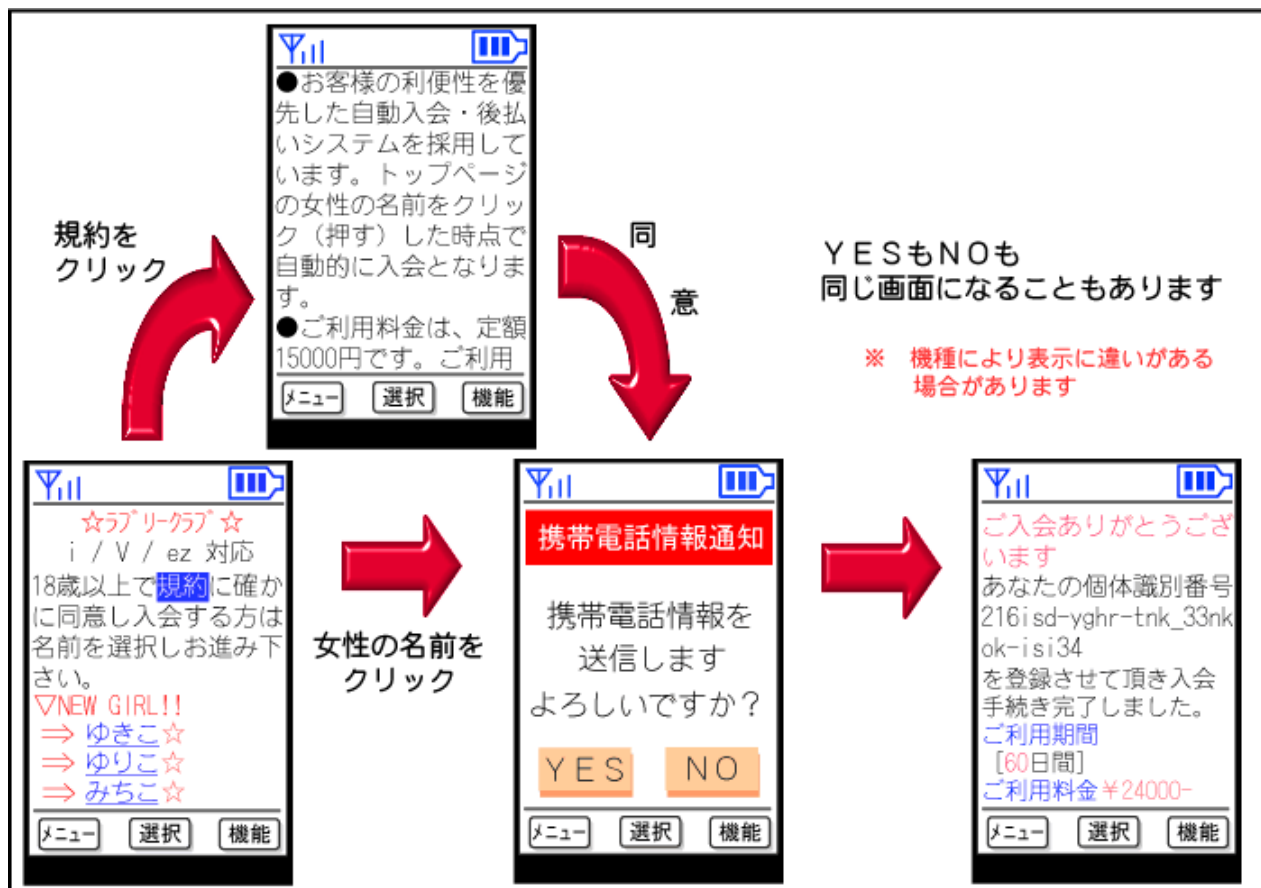
# Phishingの分類 Taxonomy of Phishing in Japan

- ソーシャルエンジニアリング: Social Engineering
  - 広義のフィッシング: Comprehensive Phishing
    - ◆ ネットワーク経由: via Network
      - 電子メール利用: Mail
        - ウェブサイト利用: Web site
          - 狭義のフィッシング: Narrow Phishing
          - ワンクリック: Click fraud
            - 携帯電話利用: via Celler Phone
            - ウェブ利用: via Web site
          - フリーダイヤルへの誘導: To Toll free dial
        - トロイの木馬: Trojan Horse (Malicious Software)
          - Targeted Trojan (Spear Trojan)
          - Random Trojan (Non Targeted)
            - Key Logger/Spyware – ID Theft
    - ◆ 物理的方法: via Physical
      - 電話利用: Voice Phishing (Vishing)
        - 振り込め詐欺: Furikome-Sagi (Money Transfer Fraud)
        - ID盗難: ID Theft

Social engineering is to get important information by using people's psychological weakness.



# 携帯電話でのワンクリック詐欺 About Click fraud via Cellphone



- 携帯電話でインターネットに接続し、色々なサイトを見ているうちに、突然アダルト（出会い系）サイトにつながり、料金請求の表示がされる
- Suddenly connects with a malicious site while hooking up to the Internet with the cellular phone, and the charge claim is displayed.

<http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku35.htm>



## 振り込め詐欺 Furikome-Sagi (Money Transfer Fraud)

- ソーシャルエンジニアリングの一種と考えることができる  
A kind of social engineering
- 家族の一員(夫、子供、孫等)になりすまして、電話で送金を強いる  
Criminal masquerades as family's member, and tells a victim to transfer money by telephone.
- 日本における特殊なPhishingであると考えられる  
One of the special case of phishing in Japan
- この背景として、日本では  
Financial system in Japan;
  - ◆ 普通預金の口座開設は、1円から可能で口座維持費用は不要  
The savings account can open from one yen and the account maintenance fee is free.
  - ◆ ATMは、預金の預入／払出だけでなく、送金もできる  
Money transfer is available by ATM as well as deposit and withdrawal.
  - ◆ 従来は、ATMを使って現金の振込も自由にできた(現在は、現金10万円以上はATMではできない)  
Money transfer of cash was freely available by ATM. (Currently, money transfer of 100000 yen or more cash cannot be done by ATM.)

### 参考

振り込め詐欺事例(音声): [Case1: Furikome-Sagi \(Voice in Japanese\)](#)

[http://www.keishicho.metro.tokyo.jp/seian/koreisagi/hurikome\\_onsei/hurikomesagi.htm](http://www.keishicho.metro.tokyo.jp/seian/koreisagi/hurikome_onsei/hurikomesagi.htm)

ソーシャルエンジニアリング例: [Case2: Social Engineering](#)

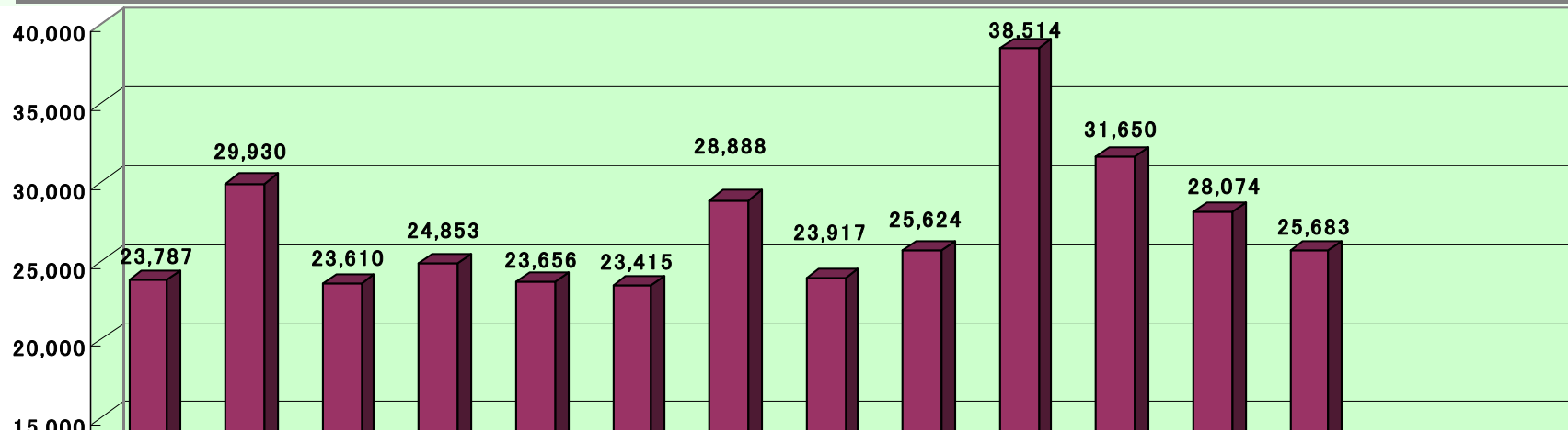
Nov. 1995, "Meet the Enemy" by Ray Caplan at Computer Security Institute(CSI) Annual Conference



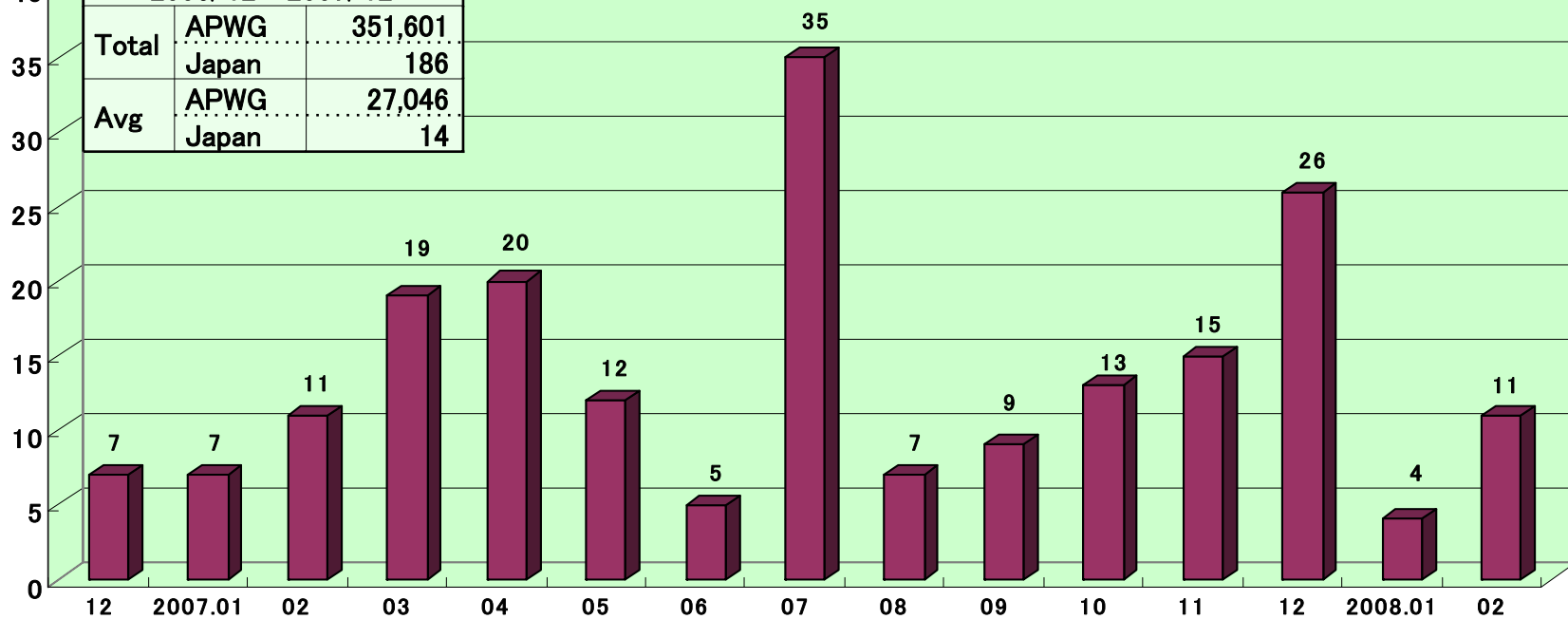
CeCOS II 東京  
TOKYO May 26 & 27, 2008



# Phishing報告件数 (No. of Phishing reported) APWG vs Japan



2006/12~2007/12		
Total	APWG	351,601
	Japan	186
Avg	APWG	27,046
	Japan	14



# Computer Crime & Security Survey Dollar Amount Losses by Type USA vs Japan

CSI : Computer Security Institute (<http://www.gocsi.com/>) Japan : Uchida (<http://www.uchidak.com/Eng/>)

Respondents: CSI: 2006=313, 2005=639 Japan: 2007=246, 2006=216		CSI			Japan		
		2006		2005	2007		2006
ウイルス感染	Virus	15,691,460	1	42,787,767	2,916,042	1	5,029,847
ノートPC盗難	Laptop Theft	6,642,660	3	4,107,300	636,707	2	3,769,338
通信詐欺	Telecom Fraud	1,262,410	8	242,000	509,960	3	20,000
情報資産の盗難	Theft of proprietary Info	6,034,000	4	30,933,000	229,260	4	230,382
内部者のアクセス乱用	Insider Net Abuse	1,849,810	7	6,856,450	224,178	5	579,987
不正アクセス	Unauthorized Access	10,617,000	2	31,233,100	222,637	6	213,200
DoS攻撃	Denial of Service	2,922,000	5	7,310,725	140,202	7	258,132
ボットネットに悪用された	Bots within the organ.	923,700	9	-	108,860	8	-
金融詐欺	Financial Fraud	2,556,900	6	2,565,000	100,160	9	50,000
システム侵入	System Penetration	758,000	10	841,400	35,260	10	64,310
ウェブの改ざん	Web site defacement	162,500	16	115,000	27,552	11	38,585
ファイル破壊/改ざん	Sabotage	260,000	15	340,600	20,160	12	12,200
パスワード盗聴	Password sniffing	161,210	17	-	17,460	13	-
Phishingに悪用された	Phishing, as a sender	647,510	11	-	5,010	14	-
無線LANの無許可利用	Abuse of wireless net	469,010	12	544,700	1,160	15	11,300
DNSサーバが悪用された	Exploit of DNS Server	90,100	18	-	360	16	-
IMの誤使用	Instant Msg misuse	291,510	13	-	160	17	-
公開ウェブアプリ誤使用	Misuse of public Web App	269,500	14	2,227,500	-		12,100
その他	Other	885,000			113,800		1,231,160
<b>総額</b>	<b>Total Losses</b>	<b>52,494,290</b>		<b>130,104,542</b>	<b>5,308,928</b>		<b>11,520,541</b>
<b>平均</b>	<b>Average of Losses/Resp</b>	<b>167,713</b>		<b>203,606</b>	<b>21,581</b>		<b>53,335</b>



総額で約10倍、回答社平均で約8倍  
Total Losses: 10 times, Average Losses: 8 times

## 日本のコンピュータ犯罪の特徴 Computer crime in Japan

- コンピュータ犯罪自体が少ない  
Computer crime is fewer than USA
- 英語のPhishingには多くの人が感心を示さない(?)  
Many people are not interested in English Phishing





## 事例：電子メール⇒電話 Case3: Email ⇒ Toll Free (English)

From: "AF Financial" <affinance@size.com>  
To: <undisclosed-recipients>  
Sent: Tuesday, May 13, 2008 9:12 PM  
Subject: Telephone banking

We recently reviewed your account, and we suspect an unauthorized ATM based transaction. Therefore as a preventive measure we will temporary limit your access to sensitive features. To ensure that your account is not compromised please call our **security center toll free at: +1 - 877 - 285 - 9764** and verify your identity to prevent deactivation.

If this is not completed by May 15, 2008, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes.

We thank you for your cooperation in this manner.

AF Financial Group, Customer Service.

If you do not have an account with us, please ignore this message as it has reached your email address by mistake. We are sorry for any inconvenience this may caused.

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.

Copyright (c) 2008 AF Financial Group. All Rights Reserved.

多くの日本人は、この様なメールが来ても、対応しない  
Recently, I received this mail, however, I did nothing.

# 事例：電子メール⇒電話 Case3: Email ⇒ Toll Free



[Home](#) | [News](#) | [Privacy](#) | [Alerts](#) | [Help](#) | [Contact Us](#)

**Online Banking:**  
[Login](#) | [Register](#) | [Help](#)

PERSONAL SERVICES

BUSINESS SERVICES

ONLINE BANKING

FINANCIAL TOOLS

ABOUT AF FINANCIAL

CONTACT US

**Quick Links:**

Personal Services

Business Services



**URGENT NOTICE:** An email has been sent out saying it is from AF Financial Group with "Unusual purchase pattern" in the subject line. This email suggests that you call a toll free number to verify your debit card number, expiration date, and personal identification number (PIN). **THIS EMAIL IS A SCAM AND HAS NOT BEEN SENT BY AF BANK.** Please delete this email and do not call the phone number listed. If you have given out your debit card information please contact AF Bank Customer Support ASAP; 800-723-4718 or 336-246-4344.



**BANKING:**  
Checking, Savings, CDs, Compare All Accounts, Consumer Loans, Mortgages

**INSURANCE:**  
Auto Insurance, Homeowners Insurance, Health Insurance, Life Insurance, Bonds, Report a Claim, Samaritan's Purse Travel Protection, Request a Quote

INVESTMENTS



**BANKING:**  
Checking, Compare All Accounts, Commercial Loans

**BUSINESS INSURANCE:**  
Commercial Insurance, Group Health Insurance, Bonds, Report a Claim, Samaritan's Purse Travel Protection, Request a Quote

INVESTMENTS



**Free Credit Report**  
[Click Here](#)

Copyright © 2008 AF Financial Group. All Rights Reserved.

AF Financial Group and its affiliated banks are each a member FDIC and an Equal Housing Lender.



## 事例：電子メール⇒偽ウェブ Case4: Pure Phishing in English

件名: Bank of America Alert: Your account has been blocked.

差出人: onlinebanking@bankofamerica.com

2008/05/21 10:37



### Online Banking Alert

Need additional  
up to the minute  
account  
information?  
[Sign In >>](#)

### Your Online Banking is Blocked

Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on [sign in to Online Banking](#) to continue to the verification process and ensure your account security. It is all about your security. Thank you. and visit the customer service section.

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#)   
© 2007 Bank of America Corporation. All rights reserved



多くの日本人は、この様なメールが来ても、対応しない  
Recently, I received this mail, however, I did nothing.



## 日本のコンピュータ犯罪の特徴 Computer crime in Japan

- コンピュータ犯罪自体が少ない  
Computer crime is fewer than USA
- 英語のPhishingには多くの人感心を示さない(?)  
Many people are not interested in English Phishing
- 犯罪者にとって、Phishing より、「費用対効果」(?)のある犯罪がある  
There are crimes with “Cost-Effectiveness” from Phishing for criminals
- ただ、Phishing (含 ID Theft等)は、今後次第に増加していくと思われる  
Phishing (inc. ID Theft) will increase gradually in the future in Japan



## 振り込め詐欺 Furikome-sagi (Money Transfer Fraud)

Year(Jan.-Dec.)	2004	2005	2006	2007
No. of Items	25,667	21,612	19,020	17,930
Amount 10K¥	2,837,866	2,515,187	2,549,330	2,514,242
(Avr. 10K¥)	(111)	(117)	(134)	(140)
(Amount K\$)	(283,787)	(251,519)	(254,933)	(251,424)

Upper: No. of Items  
 Middle: Amount 10K¥  
 Lower: Avr.Amount 10K¥

## Crimes related Japanes Banks

Fiscal year (Apr. - Mar.)	2003	2004	2005	2006	2007
偽造キャッシュカード Forged Cash Card	106 33,072 (312)	468 106,236 (227)	913 <b>97,691</b> (107)	633 57,603 (91)	550 31,900 (58)
盗難キャッシュカード Stolen Cash Card		459 50,031 (109)	6,114 <b>427,980</b> (70)	6,863 308,835 (45)	3812 144,856 (38)
盗難通帳 Stolen Passbook	670 194,300 (290)	305 40870 (134)	280 <b>103,880</b> (371)	253 26,818 (106)	170 29,070 171
インターネットバンキング Internet banking		1 0 (0)	49 10,486 (214)	100 10,900 (109)	191 <b>16,426</b> (86)

注)預金者保護法: 2005年8月成立、2006年2月施行

Note) The Depositor Protection Act : Enact Aug. 2005, Enforcement Feb. 2006

[http://www.npa.go.jp/safetylife/seianki31/1\\_hurikome.htm](http://www.npa.go.jp/safetylife/seianki31/1_hurikome.htm)

<http://www.fsa.go.jp/news/19/ginkou/20080416-1.html>



**CeCOS II 東京**  
 TOKYO May 26 & 27, 2008



## 今後を考える About the Future

- 犯罪のROI (Return On Investment) を考える必要がある。犯罪者にとって、効率的な犯罪が多くなるのは当然であろう。このため、Phishing の増加傾向は変わらないが、急激に増加しないであろう
- また、英語等、日本語以外の Phishing が報告される可能性は少ない。
- Phishing 対応は、技術だけでなく、犯罪者、被害者等の心理面からの研究が重要になるであろう。

### 参考

Robert B. Cialdini, “INFLUENCE – Science and Practice”

6つの人間の脆弱性: Six weapons of influence

- 返報性: Reciprocation
- コミットメントと一貫性: Commitment and Consistency
- 社会的証明: Social Proof
- 好意: Liking
- 権威: Authority
- 希少性: Scarcity





*Questions?*

*Comments!*

*Rebuttals...*

***Thank you !***



情報セキュリティ大学院大学  
INSTITUTE of INFORMATION SECURITY

*Katsuya Uchida (uchida@iisec.ac.jp)*



**CeCOS II 東京**

TOKYO May 26 & 27, 2008

