Anti-Phishing
- .JP's Position -

October 31, 2007

ccNSO meeting

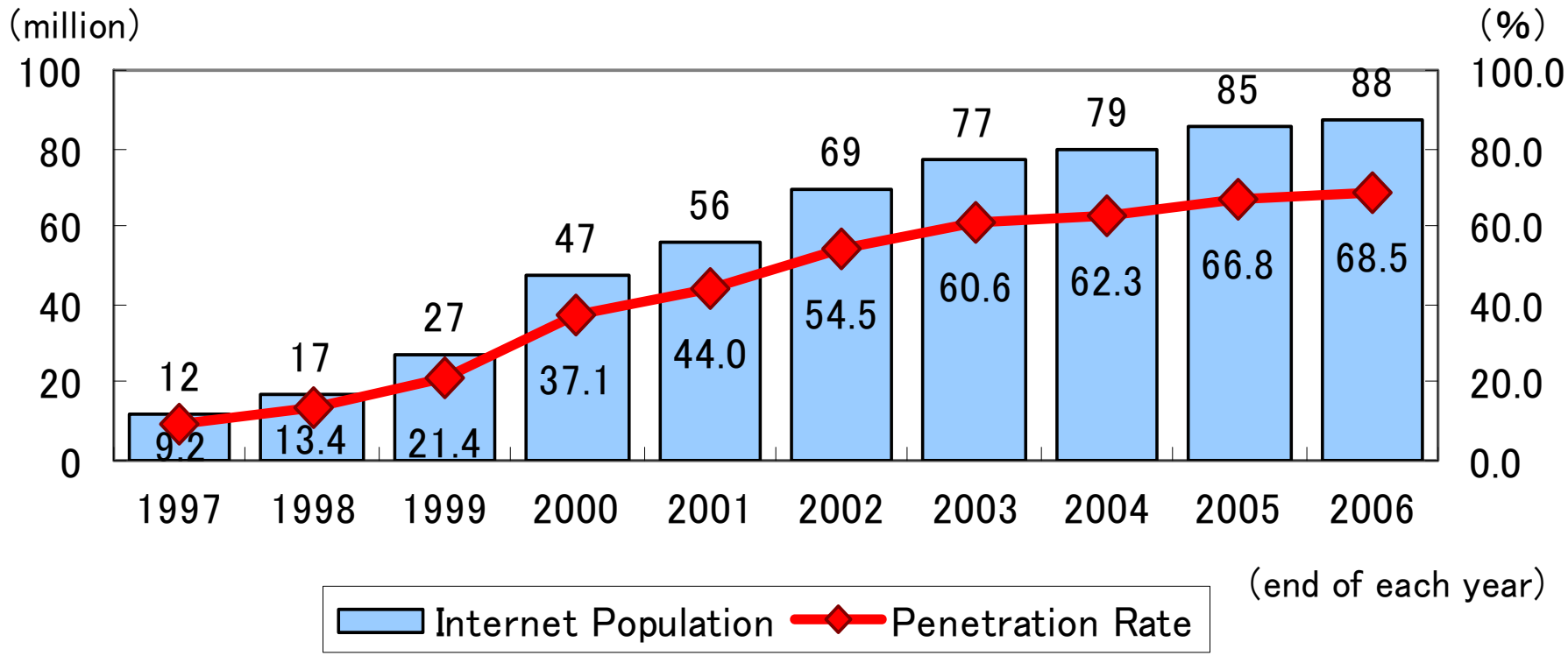
Hiro Hotta

Japan Registry Services, Co., Ltd. (JPRS)

http://jprs.jp/

http://日本レジストリサービス.jp/

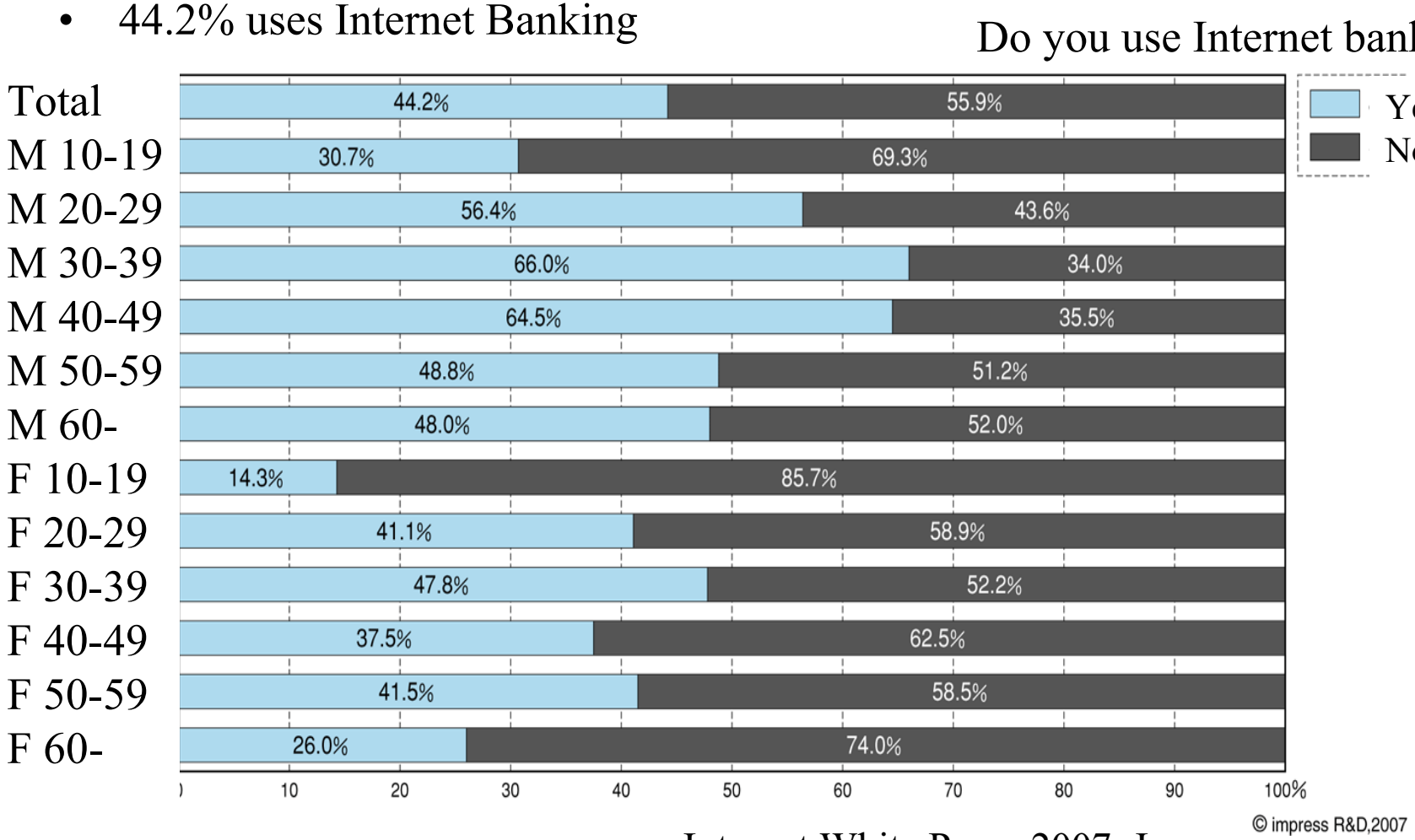
Internet Growth in Japan



Information Communication White Paper 2007, Japan

Usage of Internet Banking in Japan

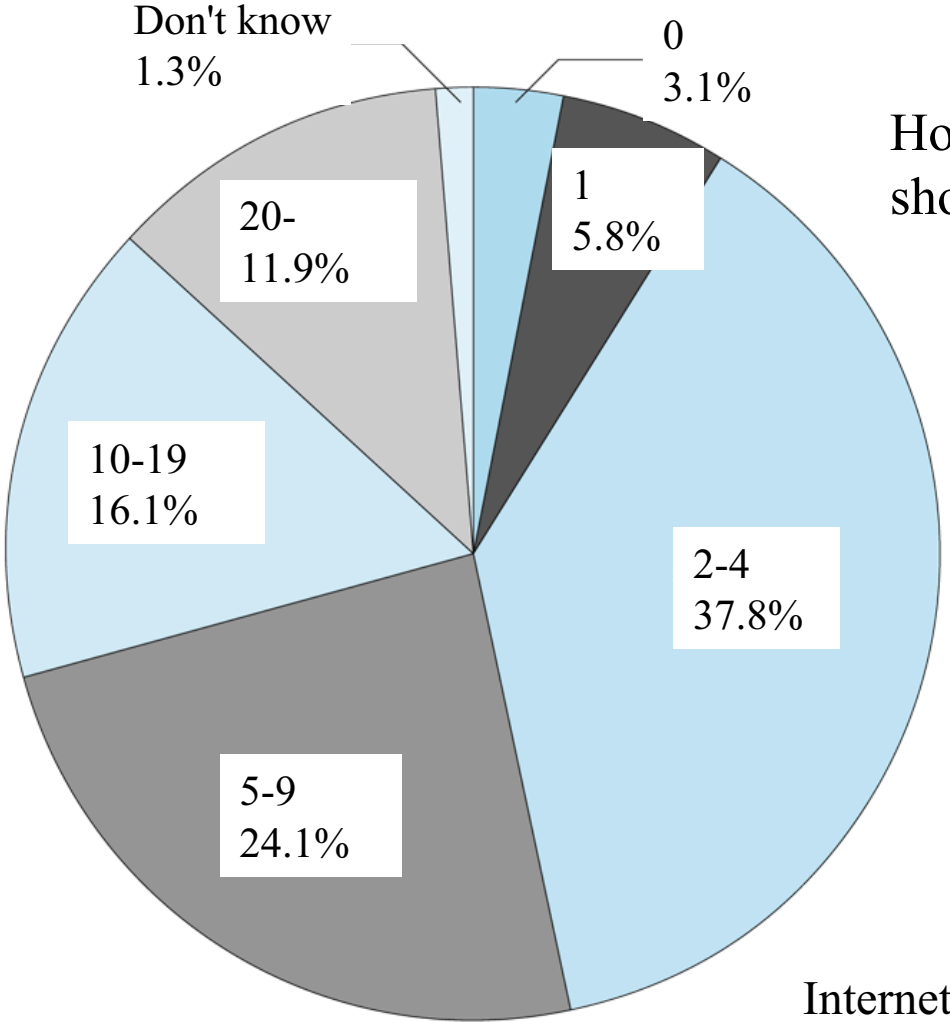
- 44.2% uses Internet Banking



Internet White Paper 2007, Japan

Usage of Online Shopping in Japan

- >95% of the respondents shop online at least once a year



How many times do you shop online for the last year?

Internet White Paper 2007, Japan

Trend : Unauthorized Access in Japan

- Number of arrestees for "Anti-Unauthorized Access Law" grows dramatically

		2000	2001	2002	2003	2004	2005	2006
unauthorized access	cases	62	66	102	143	142	271	698
	searches	30	35	51	58	65	94	84
	arrestees	34	51	68	76	88	113	130
helping unauthorized access	cases	5	1	3	2	0	6	5
	searches	4	1	2	2	0	6	3
	arrestees	5	1	3	2	0	6	5
total	cases	67	67	105	145	142	277	703
	searches	31 (3)	35 (1)	51 (2)	58 (2)	65	94 (6)	84 (3)
	arrestees	37 (2)	51 (1)	69 (2)	76 (2)	88	116 (3)	130 (5)

( ) shows the number of cases where both unauthorized access and helping unauthorized access happened

http://www.npa.go.jp/cyber/statics/h18/pdf35.pdf

Trend : Unauthorized Access in Japan (continued)

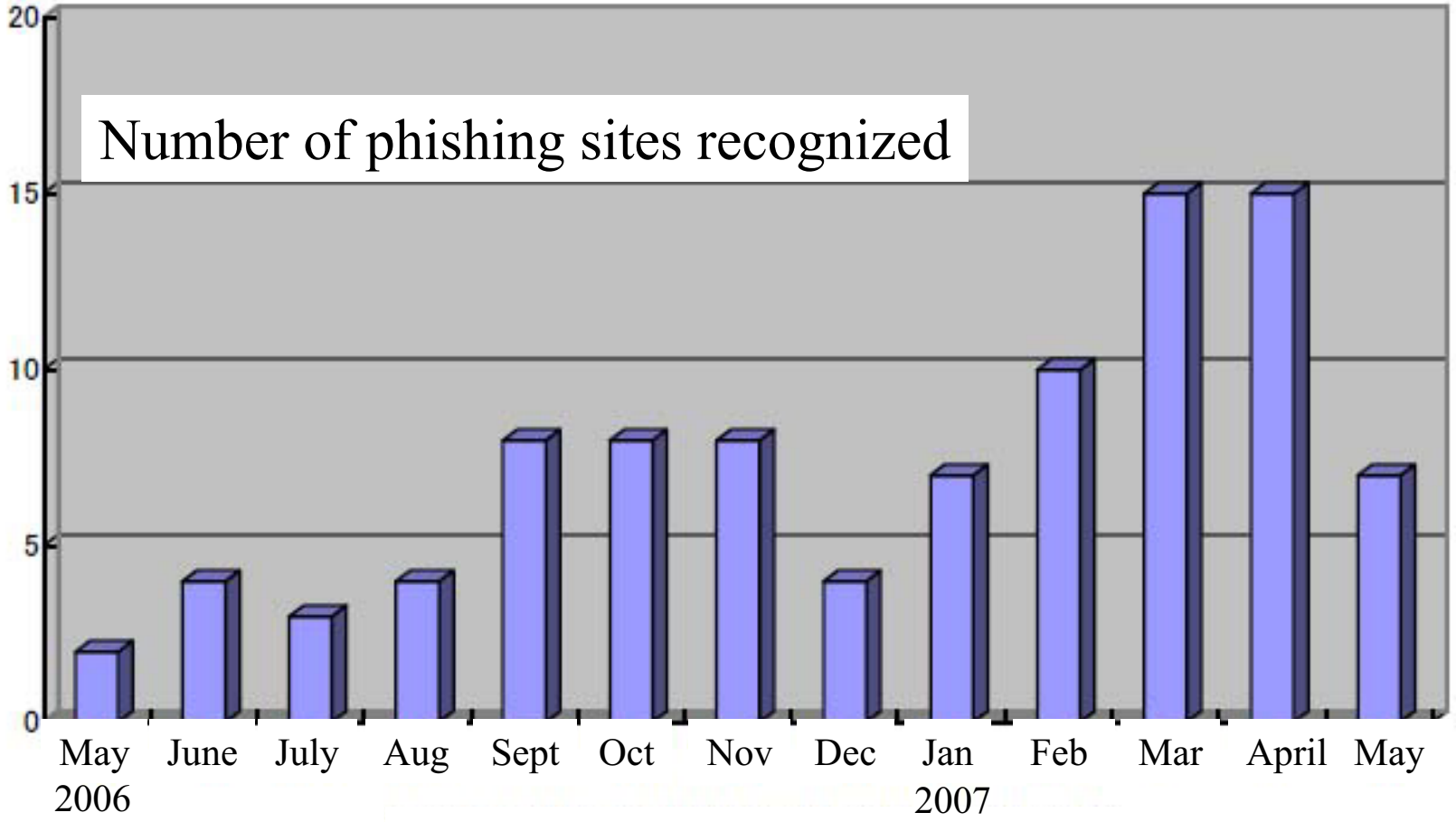
- Number of phishing grows steeply as a modus operandi

modus operandi		2005 cases	2006 cases
stealing identification (e.g. ID/password)		264	698
through	phising site	1	220
	spyware	33	197
	careless ID mgt. of users	95	178
	former employees	33	49
	peep	16	20
	leaked information through p2p	0	19
	purchasing from 3rd parties	69	12
	obtaining from fellows in crime	12	0
	others	5	3
attacking security holes		7	0

http://www.npa.go.jp/cyber/statics/h18/pdf35.pdf

Number of phishing sites recognized

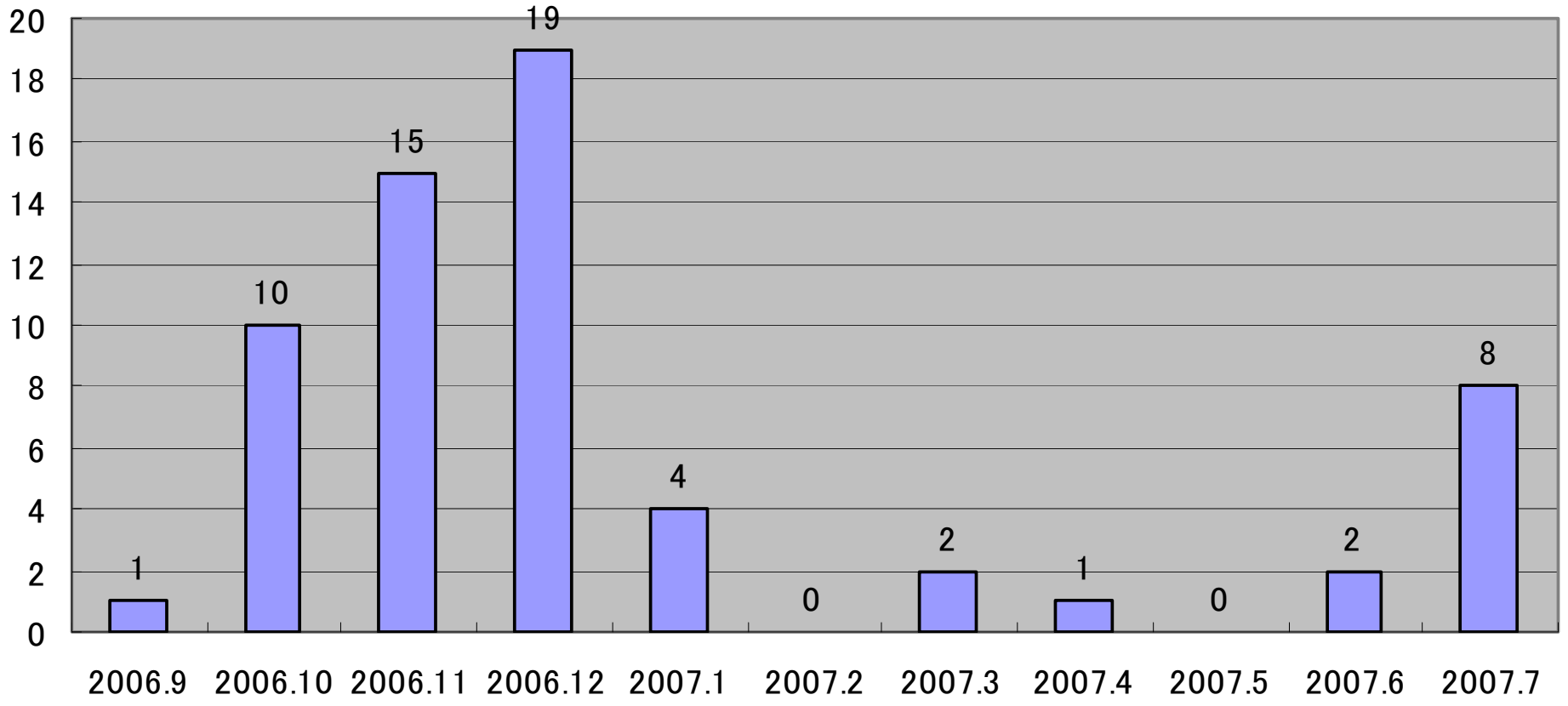
- The number of phishing site grows



https://www.antiphishing.jp/report/200706-case-077.pdf

Phishing-related reports JPRS received

- Number of phishing reports received by JPRS



Typical message of reports/requests about phishing

- From
  - Companies that provide security services
  - CERTs (Japan, abroad)
  - Banks (victims)

    :
- Message of the report/request
  - There is a website attempting to do phishing with a domain name "xxxxx.jp". It tries to hustle identification information of bank accounts. JPRS must inactivate the web-site immediately.
  - In order to communicate with the victims, give us the data input to the phishing site by the victims.

The bottomline of the registry's role

- Registry does accept the domain name application, verify the uniqueness of the domain name, and make the domain name usable on the internet.
- Registry does not get involved in the meaning of the domain name string or how to use the domain name.　This is because
  - Thorough assessment of the domain name meaning/usage would ruin the efficient introduction of the domain name in first-come first served basis.
  - It is almost impossible to decide the appropriateness of the meaning/usage of the domain name.
  - It is impossible to assess the appropriateness of the usage at the time the domain name is registered.

How JPRS behaves upon receipt of reports/requests about phishing

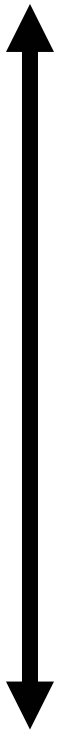
- JPRS receives reports/requests
  - JPRS checks the web site and stores the image of the web site
  - JPRS shares the situation with JPCERT/CC when appropriate
- JPRS tells the registrar of the domain name about the reports/situation and ask them to have the registrant take appropriate actions
  - registrars who are ISPs or web-hosting providers usually have contracts with their customers saying "inappropriate content will be taken down"
  - usually, when the registrar cannot reach the registrant, the registrar deletes the domain name (on ground of false registration info)
  - sometimes, the registrant changes the content of the web site (it is not known whether the site was an intentional phishing site or was hijacked)
- If the registrar does not respond, JPRS directly e-mails and mails about the reports/situation to the registrant of the domain name and ask them for appropriate actions
  - If not responded, JPRS may delete the domain name - no such case so far
- With above actions, all the phishing sites have been deleted so far
  - It is not known whether such deletion was the result of JPRS/registrar actions only

Limit of the anti-phishing action by registry

- Difficulties
  - Valid decision of the existence of bad faith is difficult
  - Bottomline of the registry's role is limited - non-involvement of meaning/usage of the domain name (DRP is the only exception)
  - Registrar should be the sole contact to registrants basically
  - Inactivating a domain name may result in inactivation of all the sub-domain names under the domain name (e.g., inactivation of ISP domain name should result in shutting down all the web sites under the ISP)
- Limited effect of the inactivation of the domain name
  - Cache data survives for several hours - even days
  - Typically, many domain names are used to refer to one phishing site

Options of registry actions

Soft



- Educate of users
- Ask the registrars to tell the registrant to solve the case appropriately
- Inactivate the domain name following the order from an authorized trusted party that deals with phishing cases
- Have the registrars to inactivate the domain name
- Inactivate the domain name by registry itself
- To have the phisher to be arrested by actively helping the public authority

hard

Advisory from JP Domain Name Advisory Committee

- May, 2007
  - JPRS explains the Advisory Committee about the phishing, and see if the advisory from the Committee is appropriate or not.
- August, 2007
  - JPRS formally asks for an advisory from the Advisory Committee about "how registry should act against phishing"
  - Advisory Committee discusses about this theme
- November, 2007
  - Advisory Committee drafts the outline of the advisory
  - Advisory Committee discusses about the outline
- February, 2008
  - Advisory Committee comes up with an advisory

Outline of the Draft Advisory

- Education of users, through cooperation with related organizations, such as CERT and ISP
- Current JPRS behavior is appropriate
  - To have the registrar to solve the case directly or indirectly
  - Current definition of the "registry role bottomline" is appropriate
- To be prepared for the emergent case
  - Discussion with related organizations about whether an authorized trusted party to decide inactivation of domain names should/can be set up is advised (in addition to slow law-enforcement process)
  - Preparation for a formal rule and process of emergent inactivation of domain names following the authorized trusted party's decision is advised