For Immediate Release

The Japan Email Anti-Abuse Group (JEAG) Drafts Recommendations on the Fight against Spam E-mail

TOKYO, February 23, 2006 – The Japan Email Anti-Abuse Group (JEAG), a working group founded by Japan's major Internet service providers (ISPs) and mobile telecommunication carriers to counter spam e-mail abuse, has drafted a list of recommendations for the reference of companies and mail server system administrators that are considering counter-spam measures. The recommendations include information on introducing effective technological countermeasures and working policies to eliminate spam.

Every year, large amounts of spam are sent to internet users without their consent, and the problem continues to become more critical. For example, more than 70% of the e-mail sent in the U.S. is spam. Spam not only consumes resources of corporate mail servers and system administrators, it is also a primary source of viruses and an instrument of fraud and other unethical practices. In Japan, the damage caused by spam continues to grow. While companies are working diligently to combat spam with a certain degree of success, spammer methods are becoming more devious and malicious. Therefore the potential damage and repercussions of spam on society are becoming an even greater cause of concern.

Amidst these circumstances, Japan's major ISPs and mobile telecommunication carriers founded JEAG in March 2005 as a working group to examine and implement technological measures to combat spam. Sub-working groups were formed to examine the three critical areas of:

- Eliminating Spam Sent to Mobile Phones
- Introducing Outbound Port 25 Blocking, and
- Implementing Sender Authentication Technology

While examining the challenges and countermeasures involved in starting the fight against spam, participating members have implemented their own effective measures to combat spam.

For the future reference of companies and mail server system administrators that are considering counter-spam measures, JEAG has drafted a list of recommendations based on a study on the challenges encountered while counter-spam measures are implemented. These recommendations have been approved by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry, who participated as observers. JEAG will work to widely propagate these recommendations and further educate e-mail server administrators about counter-spam measures. JEAG also hopes its counter-spam recommendations will be introduced rapidly not only by ISP hosting companies, but also by businesses and educational institutions.

JEAG will continue to contribute its expertise to greatly enhance Japan's messaging environment.

For more information on the recommendations and sub-working groups, please see the attached appendix.

Inquiries:
JEAG Office, E-mail: info@jeag.jp URL: http://www.jeag.jp (Japanese only)

Appendix

Wireless Sub-working Group Recommendations

The Wireless Sub-working Group examines ways to ensure the flow of wholesome e-mails to mobile phone addresses and enacts countermeasures to prevent spam from being sent to mobile phones.

To realize a flow of wholesome e-mails to mobile phones in this current era of high-speed internet connections, JEAG believes cooperation is necessary on both the outbound side and the inbound side. The sub-working group has thus compiled countermeasures used by ISPs and mobile telecommunication operators that have been proven effective in fighting spam.

The recommended countermeasures are close to being best practices and JEAG would like for companies considering counter-spam measures to use them as a reference when considering their own plan of action.

Outbound Port 25 Blocking Sub-working Group Recommendations

The Outbound Port 25 Blocking Sub-working Group examines ways of implementing Outbound Port 25 Blocking (OP25B), a technology that blocks and removes spam mail directly sent from the dynamic IP addresses of ISPs to mail servers at Outbound Port 25.

The Sub-working Group recommendations include proposals on the implementation process of OP25B and challenges and considerations related to its introduction, as well as proposals for the introduction of Submission Port[1] and SMTP Authorization (SMTP Auth)[2], which should be combined with OP25B implementation.

The number of providers implementing OP25B is increasing, and JEAG hopes to be able to contribute by stopping spam e-mail that originates from Japan as a first step.

Sender Authentication Sub-working Group Recommendations

The Sender Authentication Sub-working Group examines sender authentication technology[3], which is one technological method that makes it possible to determine outbound e-mails of false origin.

With the aim of introducing either SPF[4] as a common IP system or DKIM (DomainKeys)[5] as a common encryption system to pro-actively propagate sender authentication technology, the Sub-working Group's recommendations include proposals for settings and working policies for service.

JEAG expects that spam emails will decrease if more organizations implement sender authentication technology and employ filtering technology based on the results of this authorization technology.

---

[1] Submission Port: Item used when sending a mail (called 'Submission'), which JEAG recommends using as Port 587. Standardized by RFC2476.

[2] SMTP Auth: Technology that confirms a user's identity when a mail is sent and only allows mail to be sent when authorized. Standardized by RFC2554.

[3] Sender Authentication Technology: A technology that authorizes whether the server of outbound mail origin is appropriate when a user receives a mail.

[4] SPF: An IP address based sender authentication technology proposed by Meng Wong, a co-founder of Pobox.com in the U.S.
Specifically, permitted sent mail server information is obtained from "envelope"-like sender information (Envelope From), and authorized depending on whether the inbound mail comes from the correct outbound mail server or not.

[5] DKIM (DomainKeys): A sender authentication technology based on a combination of the electronic signature base technology called DomainKeys advocated by Yahoo! in the U.S. and Identified Internet Mail advocated by Cisco in the U.S.
Specifically, mail is signed on the outbound side when sent by using its own secret key. The inbound side obtains open keys from the DNS (Domain Name Service) server to verify signatures of mails that have been sent.

Reference

JEAG Secretariat Members

Internet Initiative Japan Inc.
KDDI Corporation
NTT DoCoMo, Inc.
Panasonic Network Services, Inc.
Plala Networks Inc.
Vodafone K.K.

JEAG Participating Members

@NetHome Co., Ltd.
DREAM TRAIN INTERNET INC.
FreeBit Co., Ltd.
Hewlett-Packard Japan, Ltd.
IBM Japan, Ltd.
IRI Communications, Inc.
Japan Internet Exchange Co., Ltd.
JAPAN TELECOM CO.,LTD.
JPCERT Coordination Center
KANSAI MULTIMEDIA SERVICE COMPANY
K-Opticom Corporation
NEC Corporation
NIFTY Corporation
Nihon Openwave Systems K.K.
NIPPON TELEGRAPH AND TELEPHONE EAST CORPORATION
NTT Communications Corporation
NTT-ME CORPORATION
NTTPC Communications, Inc.
Otsuka Corporation
Sendmail K.K.
Softbank BB Corporation
Sony Communication Network Corporation
TOSHIBA SOLUTIONS CORPORATION
WILLCOM, Inc.
Yahoo Japan Corporation

Observers

Ministry of Economy, Trade and Industry
Ministry of Internal Affairs and Communications
Nippon Information Communications Association

(Above organization names are listed in alphabetical order)

-ends-