Executive Summary

While the government's economic remedies are now finally underway, the International Monetary Fund (IMF) is projecting a 6.2% decrease in real growth for the Japanese economy during fiscal 2009. Clearly, the recession will continue for the foreseeable future. According to a survey conducted by the Japan Users Association of Information Systems, 55% of companies asked forecasted lower IT investment for 2009 as compared to 2008. The survey indicated an average decrease of 10%; 2009 is shaping up to be a very difficult year for the IT industry.

According to an IDC study, the scope of the so-called cloud computing market (SaaS/PaaS/IaaS) grew at a 19.2% clip during fiscal 2008 compared to the prior year. Some estimations have this level of growth continuing through 2009 and beyond. All indications are that the global economic crisis has convinced companies to opt for IT services that are provided over the Internet on an as-needed basis. This contrasts with historic practices of developing proprietary systems, investing in capital equipment, and managing systems in-house. The shift to a pay-per-use format is an obvious effort to control overall costs, while optimizing the corporate IT environment.

This type of IT services model has been championed more than once in the past; however, we can identify several reasons as to why the practical implementation of this model is a real possibility today. First, we can point to the advancement in broadband Internet and stable network services, available at more reasonable prices than ever. Second, we have seen great strides in computer system virtualization and Web services technologies. Third, the current economic recession is serving as an added impetus for the shift toward a per-use service model.

As these trends continue apace, ensuring safety on the Internet becomes an even more important issue in terms of corporate business continuity. In this sense as well, it is vital to identify and understand the incidents and vulnerabilities that exist under the surface of the Internet cloud. Corporate IT managers need this information to be able to fairly evaluate cloud services provider service levels, and to create policies ensuring the safe use of such services.

This whitepaper summarizes technical information related to potential incidents and vulnerabilities that threaten the stable operations of the Internet as a whole, possibly preventing our client firms from using the Internet in safety and confidence.

This whitepaper consists of information from a survey report conducted over the13 weeks between January 1 and March 31, 2009. Here, we offer commentary on the survey results, looking at historical statistical data focused on SQL injection attacks (a threat to Web services), alerts related to ID and password management (indispensable for using services over the Internet), and "scareware," a recent and growing cause of damages.

During the period in question, the ratio of spam observed averaged 81.5% of all emails—remaining an extremely high percentage. We will explain in this whitepaper that thorough deployment of appropriate control mechanisms on the part of the sender is an effective action for reducing spam. We will present data to support our conclusions.

IIJ will continue to respond to all manner of incidents and vulnerabilities, actively disseminating information in order to support the further development of the Internet into a safe and stable part of the social infrastructure, particularly as the Internet becomes an even more critical component of the infrastructure underlying corporate activities.

Author
Toshiya Asaba
Executive vice president. Member of the WIDE Project. Mr. Asaba joined IIJ in its inaugural year of 1992, becoming involved in backbone construction, route control, and interconnectivity with domestic and foreign ISPs. Asaba was named IIJ director in 1999, and as executive vice president in charge of technical development in 2004. Mr. Asaba founded the IIJ Innovation Institute Inc. in June 2008, and he serves concurrently as president and CEO of that organization.