

Internet Topics: The Blocking of Child Pornography by ISPs in Japan

The blocking of child pornography by ISPs is designed to prevent the circulation of such content by shutting down access to servers that distribute illegal child pornography. From April 2011 a number of ISPs and other organizations in Japan began implementing blocking. Here we explain the circumstances of these activities, examine current implementation methods, and look at some of the issues faced.

■ Background

The Internet is a useful tool that is part of the daily routine of many people, but it has also been used to circulate illegal content since its earliest days. In fact, in a number of countries the development of Internet-related laws stems from efforts to combat child pornography. The international Convention on Cybercrime*1 that was adopted in November 2001 included measures for dealing with crimes involving child pornography, treating this in the same category as acts directly related to computers such as unauthorized access.

As a result of changing Internet usage and crimes against children, discussions took place in Japan at the General Security Countermeasures Conference*2 in 2008, with a number of precedents in foreign countries examined to have ISPs, content distributors, search engine companies, and content filtering companies prevent general users from accessing child pornography. The resulting report*3 detailed technical methods for ISPs and other organizations to block child pornography in addition to points to consider when implementing these methods. The report also proposed the establishment of a council that promotes these activities*4 and an association that is responsible for the listing of child pornography locations.

■ Implementation and Evaluation

In light of these proposals, communication industries evaluated the legal aspects of blocking the circulation of child pornography on the Internet, examined blocking technology, and had discussion on establishment of an association for managing an address list as well as guidelines for how this list should be handled within Safer Internet of JAPAN*5 Working Group for Anti-Child-Pornography*6. From a legal perspective, discussions focused on the issue of over blocking where normal communications are also blocked as a side effect, including methods to counter this. From a technical perspective, participants evaluated issues such as the side effects of DNS blocking on normal DNS operation, with a focus on compatibility with the existing operation of DNS and related technology such as DNSSEC.

■ Blocking Implementation and Issues

After considering these issues, the ICSA (Internet Content Safety Association)*7 was established in March 2011 to create and manage a list of addresses containing child pornography, and a system for blocking child pornography in Japan based on the address list provided by this association was constructed. However, this blocking of content is not a comprehensive countermeasure, serving only as a temporary step that allows law enforcement agencies to conduct countermeasures in a smooth manner*8. Participating ISPs and other organizations began the actual blocking based on this list of addresses from April of this year. IJ also started to block through a number of services in April.

Currently most providers have adopted DNS blocking, which is less costly to implement. However, this method is expected to have an impact on the ability to provide DNS services, and some have pointed out that it is incompatible with the DNSSEC technology used to prevent the spoofing of DNS query replies. Furthermore, blocking methods using DNS can only block part of the address list, and it is deemed that evaluation of methods for blocking on a per-image basis will be necessary going forward*9. For this reason, we will need to continue evaluating migration to a method of blocking that is more precise and effective, taking overall cost, equipment configuration, and operation into consideration.

■ Summary

Child pornography countermeasures must be implemented to protect the human rights of the children involved. By participating in these activities IJ will continue to strive towards creating an Internet where no illegal content is circulated.

Author:

Mamoru Saito

Manager of the Office of Emergency Response and Clearinghouse for Security Information, IJ Service Division

Supervisors/Contributors:

Takamichi Miyoshi Managing Director, IJ

Koji Yamamoto Vice Manager, Application Service Department, IJ Service Division

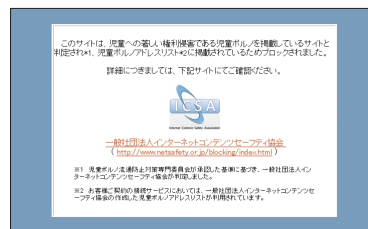


Figure 1: Warning Message When Blocked Using the ICSA Address List

*1 Convention on Cybercrime (<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>).

*2 A conference led by the National Police Agency. In the past it has dealt with issues such as countermeasures for illegal or harmful material on the Internet and copyright infringement using file sharing software (<http://www.npa.go.jp/cyber/csmeeting/index.html>) (in Japanese).

*3 2008 General Security Countermeasures Conference Report "The Issue of Child Pornography Circulated on the Internet and Countermeasures" (<http://www.npa.go.jp/cyber/csmeeting/h20/pdf/pdf20.pdf>) (in Japanese).

*4 The Council for Promotion of Measures Preventing the Circulation of Child Pornography (temporary name) later became the Expert Committee on Measures Preventing the Circulation of Child Pornography (<http://www.netsafety.or.jp/blocking/007.html>) (in Japanese).

*5 Safer Internet of JAPAN (<http://good-net.jp/about.html>) (in Japanese).

*6 "Final Report of the Working Group for Anti-Child-Pornography" (http://good-net.jp/press_jipo_20110428.html) (in Japanese).

*7 Internet Content Safety Association (<http://www.netsafety.or.jp/about/index.html>) (in Japanese).

*8 Refer to the ICSA explanation of this scheme. "Regarding Work Towards the Creation of an Address List" (<http://www.netsafety.or.jp/blocking/index.html>) (in Japanese).

*9 "Guidelines for Using DNS Blocking to Counter Child Pornography" (<http://good-net.jp/ustr/imgbox/pdf/20110427091336.pdf>) (in Japanese).