NEWS RELEASE

NTT

October 18, 2005

Trial of a next-generation DDoS defense system for Internet site protection carried out in the U.S.A.

- A field trial carried out in the U.S.A. to verify the effectiveness of the Moving Firewall technology, which is to be released for practical uses by the end of this fiscal year -

Nippon Telegraph and Telephone Corporation (hereafter referred to as NTT: headquartered in Chiyoda-ku, Tokyo, Japan; President and CEO: Norio Wada) has conducted, in the U.S.A., a field trial of a defense system that collaborates with ISPs(*1) to protects data centers and Internet sites owned by enterprises from DDoS(*2) attacks. This system uses Moving Firewall(*3), an anti-DDoS technology being developed by NTT Information Sharing Platform Laboratories, to provide automatic protection from DDoS attacks through coordinated action of the entire network.

For defense against DDoS attacks to be effective, it is important for targeted corporate s or data centers (hereafter referred to as the user) to collaborate with the ISP networks. This trial verifies the effectiveness of Moving Firewall, which enables the user to autonomously take defensive measures in collaboration with the ISP network, in a commercial network.

The trial was carried out using a data centers and networks in the United States, a country where DDoS attacks occur frequently, with cooperation of Verio (http://www.verio.com/), a U.S. subsidiary of NTT Communications. Verio has abundant experience and know-how about anti-DDoS measures.

<Background to the trial and results>

As convenient network-based services, such as online shops and Internet banks, are becoming widely used, crimes that threaten the safety and security of the Internet are being committed frequently.

In particular, the number of cases of damage inflicted by DDoS attacks is rising every year. A DDoS attacker sends a large number of malicious packets to a network or a server to overwhelm it and render it unable to provide its normal service. For example, in 2004, a certain website in the U.S. became inaccessible due to a DDoS attack launched by the MyDoom worm, which then reached epidemic proportions.

The most common security measure taken today is the firewall, but this does not offer good defense against DDoS attacks. Being frequently subjected to DDoS attacks, the United States is likely to see a rapid expansion of its market for anti-DDoS products. Although the existing products fulfill some limited functions, such as the detection of attacks and the provision of some defense against them, they do not incorporate collaboration between the user and the ISP. This has resulted in complicated operation

of these products. DDoS attackers and their targets are rarely confined to a single network under the same ISP or in the same country. Today a DDoS attack usually involves multiple ISPs and countries. As these attacks multiply and become daily incidents, demands are expected to increase for automatic or labor-saving defense operations, and for coordinated defense measures involving multiple providers.

Even before DDoS attacks became a serious social problem, NTT had developed a prototype of Moving Firewall, which provides network-wide defense against such attacks, and verified its effectiveness. In this U.S. trial, a prototype of Moving Firewall was installed in a data center and an ISP's network. During the trial, the DDoS defense system successfully dealt with an attack that was launched from several machines and could have potentially affected thousands of hosting users. The trial also confirms that Moving Firewall can effectively mitigate damage to the user.

Usually, data centers and enterprises have their own security policy, based on which they take security measures using security systems, such as firewalls and intrusion detection systems. Therefore, it is important that defense against DDoS attacks can be ultimately controlled at the discretion of the user. In this trial, an interface was provided at the portal site through which the ISP proposed possible defense measures and the user selected and implemented these measures.

<Outline of the trial>
The trial was carried out as follows:
(1) Application and verification
The DDoS defense system based on Moving Firewall technology was used in Verio's regular anti-DDoS operation, and practical feasibility was verified.
(2) Location
The trial involved a data center and a backbone network in the U.S. (a total of three systems were installed).
(3) Period
From April to July 2005.

<Technical points>
To achieve good coordination between the user, who detects a DDoS attack, and the defensive action taken at a position closer to the source of the attack within the ISP network, it is necessary for the user and the ISP (or multiple ISPs) to interact with each other to carry out a series of actions, such as sharing information about the attack, making requests for defensive action, approving, validating, and notifying the defensive action, executing it, and sending feedback of the result.

This system supports the aforementioned series of anti-DDoS actions across multiple ISPs and other entities by enabling multiple attack detectors and defensive devices constituting the defense system to operate in a coordinated manner. In particular, this system differs from other technologies on the market in that it allows collaboration between attack detectors at the user site and the defensive devices of the ISP. This feature is expected to effectively relieve congestion of the access link between the user and the ISP.

<Future plans>
This U.S. trial has proved both the effectiveness of the next-generation DDoS defense system proposed by NTT and the importance of coordinated actions by multiple providers to ensure network security. NTT will continue to improve the interface specifications and extend its know-how about collaboration between providers and between devices, developed and nurtured in the course of the development of Moving

Firewall technology, and seek to achieve widespread use of the technology through actual provision of a service by operating companies.

Since the same kind of threat is also increasing in Japan, we have refined the technology to achieve cost reduction of some of the functions verified in the U.S. trial (the attack detection function, in particular), and began an evaluation test in the NTT Group's commercial network and data centers this summer. We plan to release the technology for practical uses by the end of this fiscal year.

We will continue our R&D into this technology so that it can provide precise and rapid defense against abnormal traffic and attacks on servers by integrating a broader range of security technologies, such as those for combating viruses and worms and for monitoring Web server loads.

<Glossary>

*1 ISP (Internet Service Provider)
An ISP provides the service of connecting the computers of its business or residential customers to the Internet through telephone lines, ADSL lines, leased lines for data communications, etc.

*2 DDoS (Distributed Denial of Service) attack
A DDoS attack uses viruses or other means to take over servers, and uses these servers as staging platforms to send a large number of packets to a target server (such as that of an online shop, Internet bank, etc.) with the intention of rendering the server congested and unable to provider its normal service.

*3 Moving Firewall
A Moving Firewall is a system that prevents DDoS packets from invading the network by automatically detecting a malicious communication, tracing it to the source of the attack, and rejecting packets from that source, thereby protecting the communication of normal users and keeping the entire network safe and secure.

- [Appendix] Field trial of DDoS countermeasure operation using Moving Firewall

[For inquiries, contact]

Takeshi Tachi
Producer, R&D Strategy Department
Nippon Telegraph and Telephone Corporation
Phone: +81-3-5205-5390
E-mail: security-p@ml.hco.ntt.co.jp