Study of Web service systems and information security countermeasure system

Keizo Saisho saisho.keizo@kagawa-u.ac.jp



We are developing a distributed Web system consisting of a Web server and cache servers on the cloud acting as a proxy for it, a mechanism for keeping the responsiveness of interactive application by limiting the number of simultaneous sessions to the Web server, and an information security measure system that can take appropriate measures against vulnerable hosts. The number of cache servers on the distributed web system scales with traffic.

Below, simultaneous session limitation mechanism and information security measure system are introduced.

## 1. Simultaneous Session Limitation Mechanism for Web Server

The simultaneous session limitation mechanism aims to keep responsiveness to users by limiting the number

of sessions to the Web server and blocking accesses except from permitted (authorized) users. Figure 1 shows the overview of the mechanism. The IPF server (firewall) blocks access from unspecific IP address, and the UI server (user identification server) prohibits access from users who have the same IP address but are not authorized from Auth server, such as access via a broadband router or proxy server.



## 2. Information Security Measure System

Fig.1 Overview of simultaneous session limitation mechanism

Figure 2 shows the overview of the information security measure system. The vulnerability information gathering part gathers vulnerability information and C&C server information from vulnerability information sites, etc., and the IT asset management part collects device information within the organization such as importance of retained information, installed software information. The Influence estimation part estimates necessary measures based on these information, and instructs the network control part, notifies administrators

and users of the application of security patches, and so on. The network control part isolates target devices from the network or connects to the quarantine network according to the instruction. This research is being developed in collaboration with the Kida laboratory.



Fig.2 Overview of information security countermeasure system