# Study of information security countermeasure system and Web service systems

Keizo Saisho

saisho.keizo@kagawa-u.ac.jp

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

Below, information security measure system and distributed Web system are explained.

## 1. Information Security Measure System

Figure 1 shows the overview of an 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.
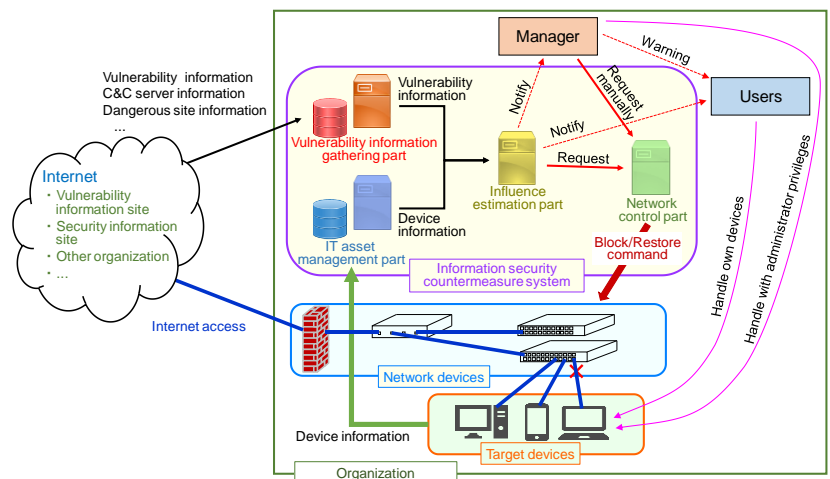

Fig.1 Overview of information security measure system

## 2. Distributed Web system

Figure 2 shows the overview of a distributed Web system. In a distributed Web system, when the number of access to the Web server increases and the Web server alone cannot process them, the cache server on the cloud is booted and the accesses are distributed (shown by magenta arrow) to the booted cache server (inside the magenta rectangle). If the number of accesses continues to increase, an additional cache server is booted and accesses are distributed (shown by red arrow) to the booted cache server (inside the red rectangles). When the number of accesses decreases, the cache server to be stopped is selected, the access to the cache server is stopped, and then the selected cache server is stopped. In this way, it is possible to build a cost-effective distributed Web system by starting and stopping according to the load of the server(s). We are developing and evaluating the load monitoring function, cache server management function, and access distribution function required for distributed Web systems.
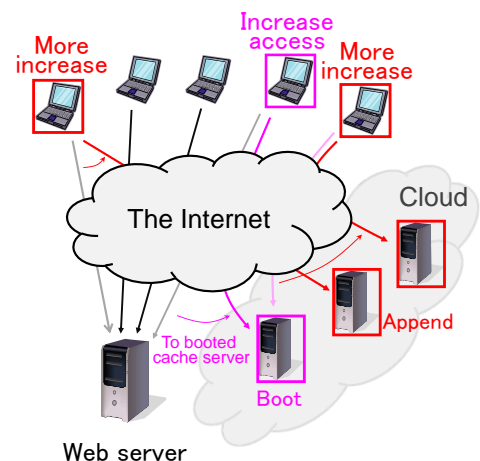

Fig.2 Overview of distributed Web system