Server Security Service

Summary

A problem is likely to occur in terms of security if the data is sent and received through web.
The Security Service recognizes and copes with various weaknesses concerning security that may occur when using service through web, obtaining the stability of service.
This service includes the **Authentication** that can be access only through user certification since users' information is managed at DB, and **Authorization** that can access the screen, page and methods by stratifying the user authority information.

Description

The service was implemented by expanding Spring Security of Spring Framework. The user authentication information and authority information are managed at DB and the session information can be contained by expanding the UserDetails interface of Spring Security.
Main functions for the Server Security are as follows:

1. Restriction on access to resources (url, method, etc.)
2. Checkup users' authentication
3. Request for recheck the authentication if not authenticated
4. Checkup hierarchical authority setting and user authority

Strength of Spring Security

- The Spring Security Service is the strong but flexible solution that provides authentication and authorization for enterprise application.
- Security is regulated through Servlet Filter and Java AOP and works based on the lifecycle of IoC of Spring.
- It provides main functions such as authentication, Web URL authorization, Method calling authorization, domain object based security processing and channel security (https force).
- It supports security control for various rich client/web service in addition to Layering issue resolution and web client by providing Service Layer and instance level security in addition to Web request.
- It supports various other frameworks, reusability, portability, code quality and reference (a diversity of areas such as government, bank, university and company).

Weakness of functions of the Spring Security

- User management function
- Role management function
- XML based (setting difficulty) authority check

General requirements for security-authentication, and the authority processing of the SI Project,

- RDB based authentication or common SSO association
- Usage of the session for easy and fast reference of user information
- Department, user and menu/screen/authority management – End users rather than developers want to work through the GUI based management function
- Requirement a massive amount of user/role data according to the project size, authority inheritance, authority reproduction, user management and department management of a hierarchy structure
- Introduction of Portal solution / X-internet – require flexible integration according to user management/menu-authority processing
- Requirements per project such as department/user/menu/screen/authority processing are similar but different so that there is a risk of duplicate development – common task nature with higher level of difficulties than ordinary tasks. Standardization, easy customizing, flexible expansion required

Expected Effects

- They can obtain flexible and strong framework with SI project utilization and strength of Server Security at the Server Security of e-government development framework.

Server Security

- Architecture
- Authentication
- Authorization

N. Reference

- Spring Framework-Spring Security
- Spring Framework-Spring Security Reference Documentation
- Spring Community forum