2005 SELinux Symposium

Simplifying Policy Management with SELinux Policy Editor

Hitachi Software Engineering
The George Washington University
Yuichi Nakamura
ynakam@hitachisoft.jp

Contents

- Problems of policy
- SELinux Policy Editor
- Problem
- Summary

Problems of policy

Problems in configuring policy

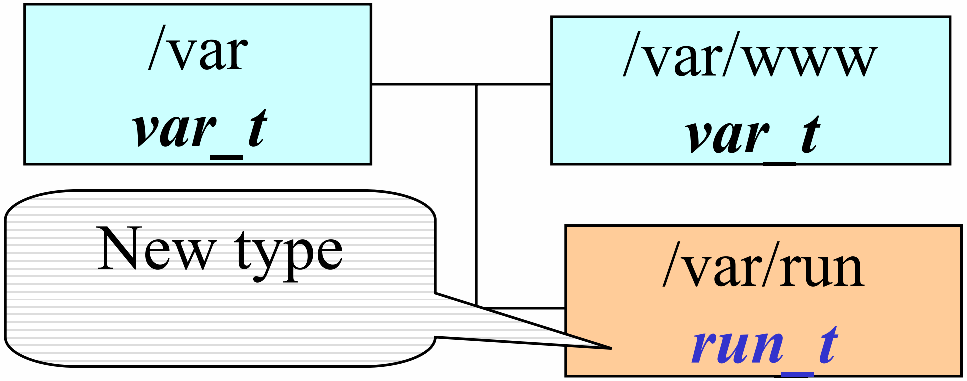
HitachiSoft

- Type label
- Too many configuration elements
- Text-based

Problem: Type label

- Not human friendly
- Can not remember type-file relationship
- Conflict situation

Example of conflict



/var
var_t

/var/www
var_t

New type

/var/run
run_t

・some_t can read under /var ：**allow** *some_t var_t* file:{*read*}

some_t can not newly labeled file
To add policy is necessary

Problems (cont)

- Too many configuration elements
  - Object class, access vector, macros
    - □ Object class about file:7
    - □ Access vector about file: more than 17
    - □ More than 100 macros..
  - "Attribute" makes things more complicated
  - RBAC is hard to understand
    - □ user A roles B;
    - □ role B types C;
      - Hard to understand why role B types C is necessary?
- Text based

SELinux is difficult for beginner

Existing tools

- setools by Tresys Technology
  - Features to analyze policy
  - Editing policy is text editor based
- polygen by MITRE
  - Generate policy from strace

Difficult for beginner

SELinux Policy Editor

Our approach

Problems

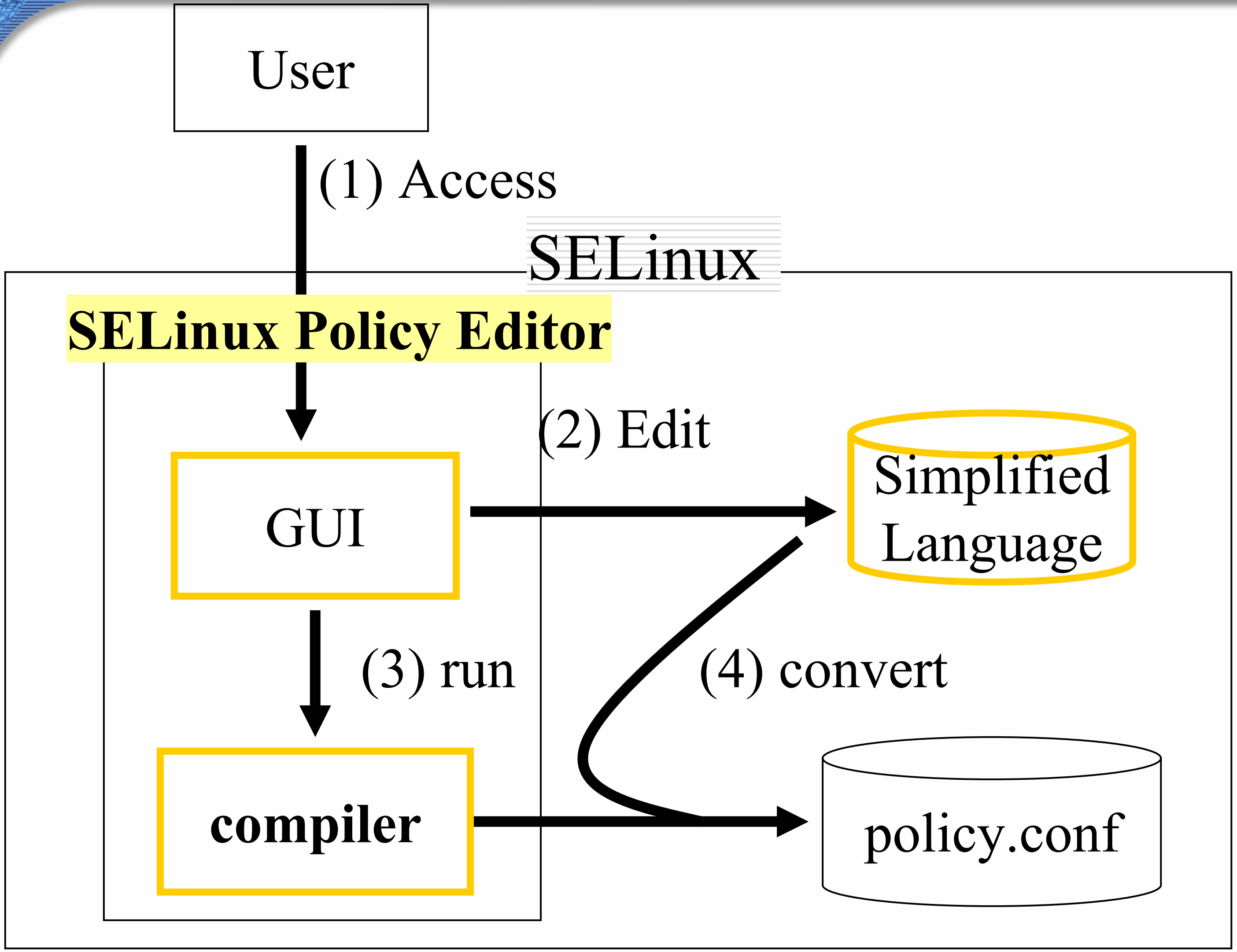
- Type label
- Many config elements
- Text-based

Our approach

- Simplified policy language
  - Hide type
  - Reduced elements
- GUI

Tool for SELinux beginner

Architecture



Simplified Language(1): Overview

- Main feature
  - Hide type
  - Integrated object class, access vector
  - “global” domain
  - Simplified RBAC
- Others
  - Domain transition support
  - File type trans support

Simplified Language (2)　Hide type

Example:

Allowing httpd_t to access under /etc/httpd and TCP 80

```
domain httpd_t;
allow /etc/httpd r;
allownet -tcp -port 80;
```

In normal SELinux policy language
we must label /etc/httpd and tcp 80

Simplified Language (3)
Integrating object class, access vector

Example

Original	Our language
7 file related object classes **file dir lnk_file chr_file blk_file sock_file fifo_file**	only “file”
4 access vectors **read getattr ioctl lock**	only “r(read)”

Object classes are integrated into following

-file, network, IPC, terminal,

special files(proc,tmpfs), admin

Simplified Language(4) “global” domain

- Domain: “global”
  - Inherited by all domains

    Example:

```
{  domain global;
deny /etc/shadow;  }
{ domain foo_t;
allow /etc  r;  }
```

-> foo_t can not read /etc/shadow, but can read others in /etc.

-> To access /etc/shadow describe “allow /etc/shadow r”

- Convenient to protect important resources

Simplified Language(5) Simplified RBAC

- Original RBAC
  - user A types B
  - role B types C
- Simplified RBAC
  - no “role B types C”
  - only “user A roles B”
  - Example: webmaster_r role

```
role webmaster_r;                    ….define webmaster_r role
user webmaster;                      ….webmaster can use this role
domain_trans login_t /bin/bash       ….login_t uses RBAC
allow /var/www r,w;                  ….webmaster_r can r/w /var/www
```

Simplified Language(6) Others

HitachiSoft

- Domain transition
  - Example: from initrc_t to httpd_t

    domain httpd_t;

    domain_trans initrc_t /usr/sbin/httpd;

- File type trans
  - We could not hide type here..

    domain httpd_t

    allow /etc exclusive etc_runtime_t;

    Equivalent to

    “file_type_auto_trans(httpd_t, etc_t, etc_runtime_t)”

Compiler

Main procedure

1. generate type label using resource name
2. Output SELinux config language
   - “allow” statement
   - relationship between resource and type

Compiler: Example

Simplified Language

```
domain one_t;        domain two_t;
allow /var r;        allow /var/www r;
```

Generate type

/var : var_t

/var/www : var_www_t

SELinux Policy

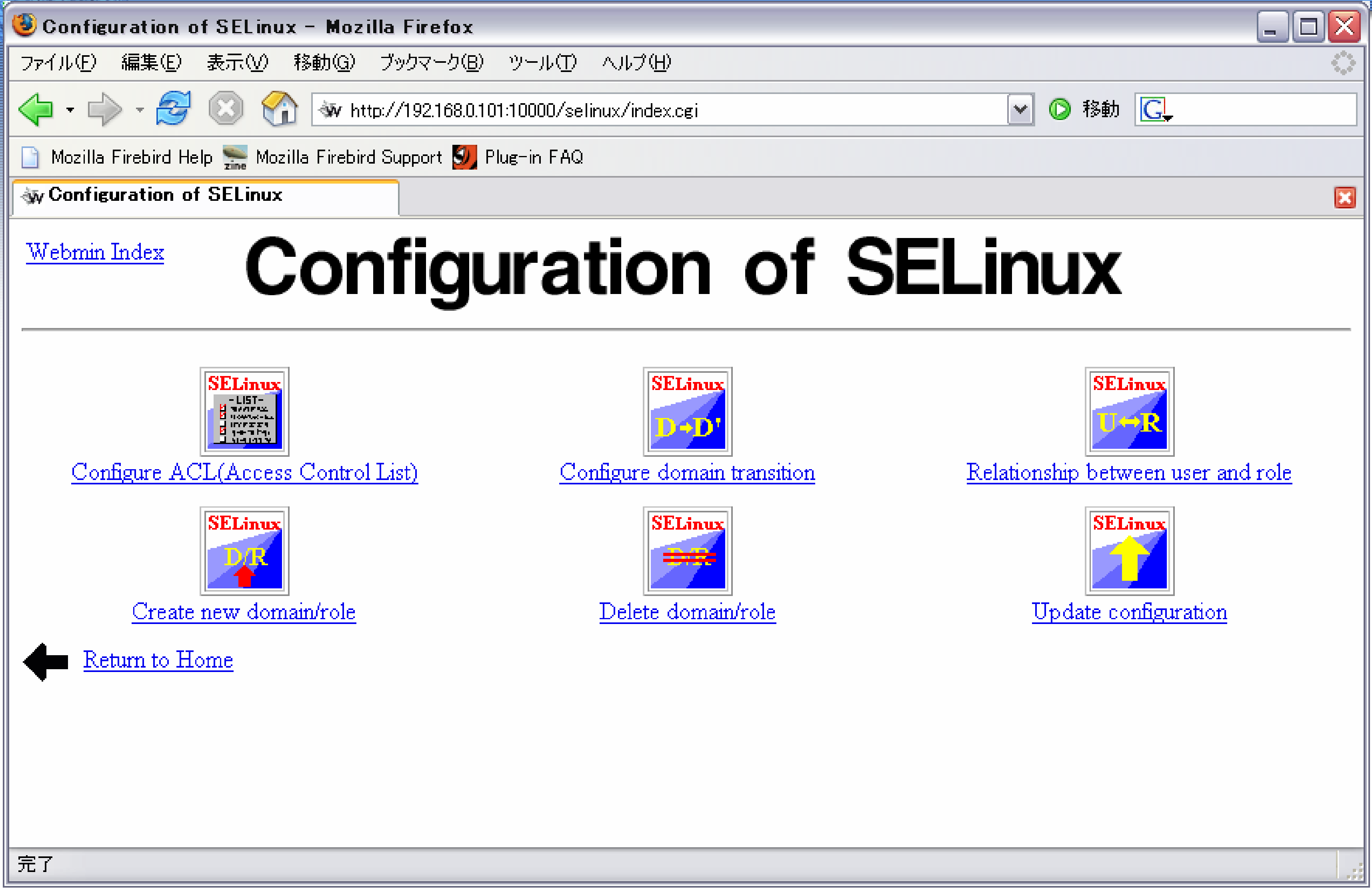
```
allow one_t var_t file:r_file_perms;
allow one_t var_www_t file:r_file_perms;
allow two_t var_www_t file:r_dir_perms;
…same "allow" for other 6 object classes
/var/(/.*) system_u:object_r:var_t
/var/www(/.*) system_u:object_r:var_www_t
```

"allow" statement for child directory

GUI

- Edit simplified language
- Implemented as Webmin module
  - □ http://www.webmin.com/
  - □ User can administrate system from web browser
- Features
  - □ Edit access control of file, network etc.
  - □ Domain trans
  - □ RBAC
  - □ Template

Main menu



Configuration of SELinux - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)
http://192.168.0.101:10000/selinux/index.cgi
移動
Mozilla Firebird Help
Mozilla Firebird Support
Plug-in FAQ
Configuration of SELinux
完了

Webmin Index

Configuration of SELinux

Configure ACL(Access Control List)

Configure domain transition

Relationship between user and role

Create new domain/role

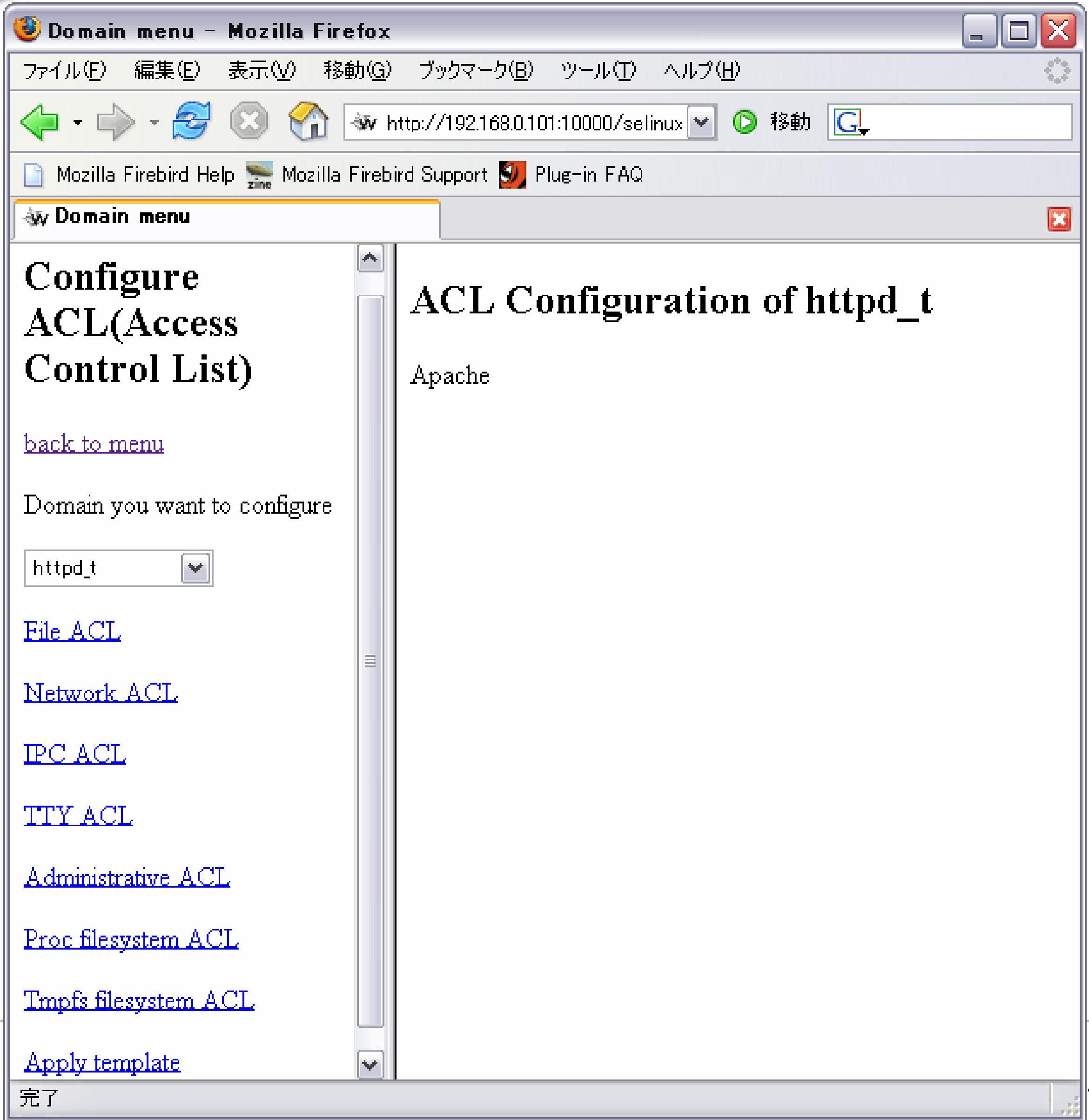
Delete domain/role

Update configuration

Return to Home

ACL menu

HitachiSoft



Domain menu – Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)
http://192.168.0.101:10000/selinux
移動
Mozilla Firebird Help
Mozilla Firebird Support
Plug-in FAQ
Domain menu
完了

Configure ACL(Access Control List)

back to menu

Domain you want to configure

httpd_t

File ACL

Network ACL

IPC ACL

TTY ACL

Administrative ACL

Proc filesystem ACL

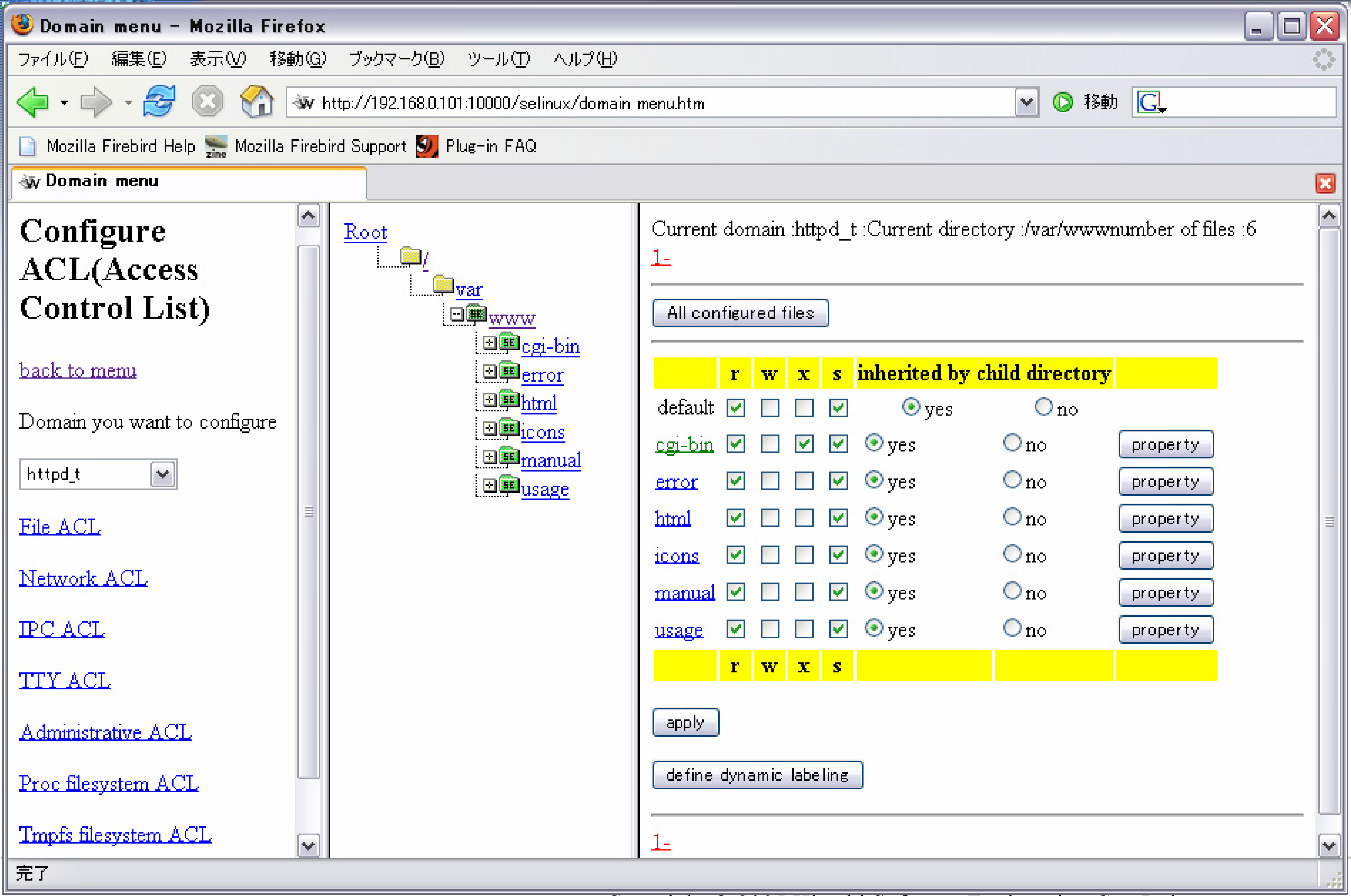
Tmpfs filesystem ACL

Apply template

ACL Configuration of httpd_t

Apache

File ACL


Domain menu - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)
移動
Mozilla Firebird Help
Mozilla Firebird Support
Plug-in FAQ
Domain menu
完了

http://192.168.0.101:10000/selinux/domain menu.htm

Configure ACL(Access Control List)

back to menu

Domain you want to configure

httpd_t

File ACL

Network ACL

IPC ACL

TTY ACL

Administrative ACL

Proc filesystem ACL

Tmpfs filesystem ACL

Root
/
var
www
cgi-bin
error
html
icons
manual
usage

Current domain :httpd_t :Current directory :/var/wwwnumber of files :6

1-

All configured files

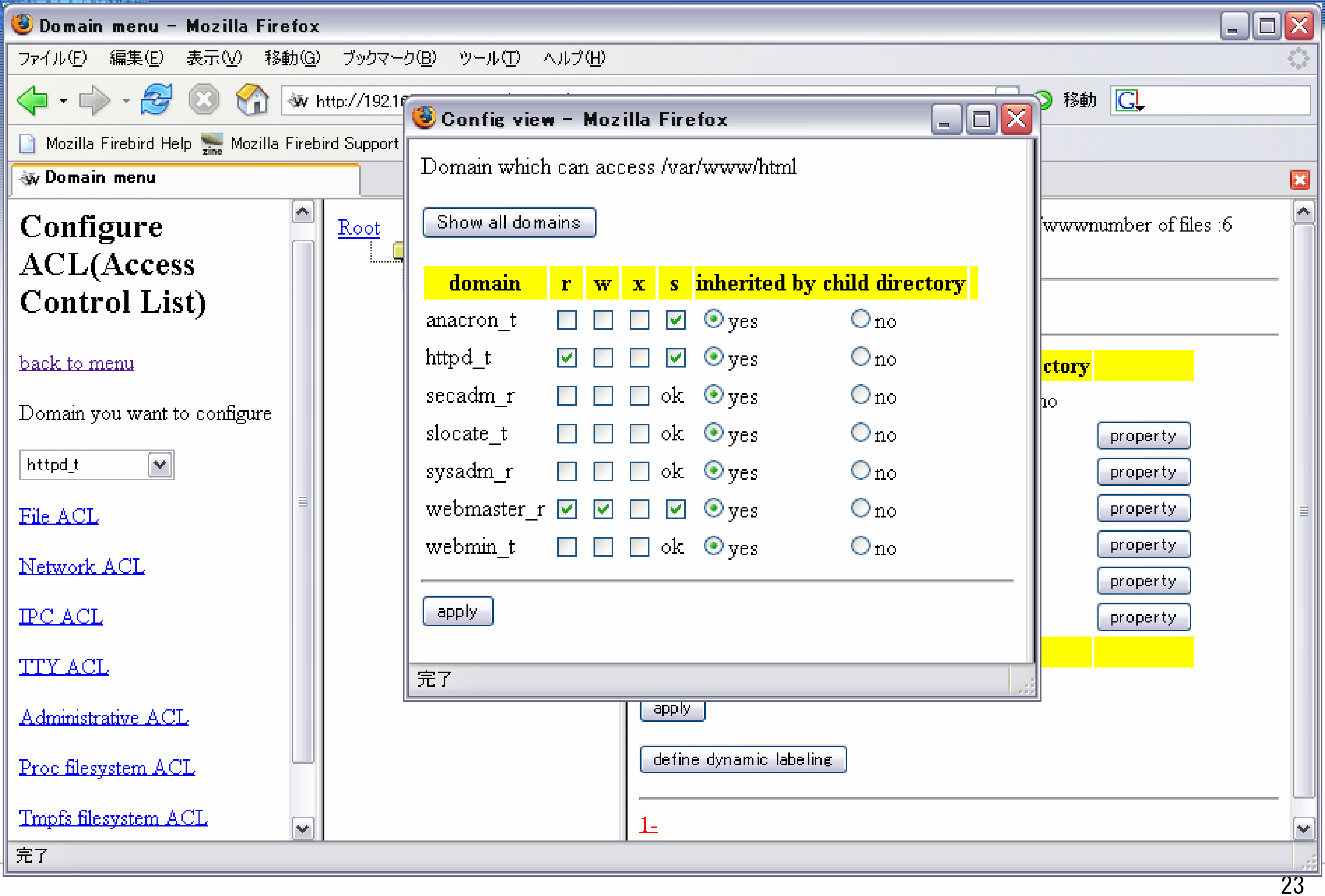
	r	w	x	s	inherited by child directory		
default	☑	□	□	☑	● yes	○ no	
cgi-bin	☑	□	☑	☑	● yes	○ no	property
error	☑	□	□	☑	● yes	○ no	property
html	☑	□	□	☑	● yes	○ no	property
icons	☑	□	□	☑	● yes	○ no	property
manual	☑	□	□	☑	● yes	○ no	property
usage	☑	□	□	☑	● yes	○ no	property
	r	w	x	s			

apply

define dynamic labeling

1-

File ACL property



Configure ACL(Access Control List)

back to menu

Domain you want to configure

httpd_t

File ACL

Network ACL

IPC ACL

TTY ACL

Administrative ACL

Proc filesystem ACL

Tmpfs filesystem ACL

Domain which can access /var/www/html

domain	r	w	x	s	inherited by child directory	
anacron_t	□	□	□	☑	● yes	○ no
httpd_t	☑	□	□	☑	● yes	○ no
secadm_r	□	□	□	ok	● yes	○ no
slocate_t	□	□	□	ok	● yes	○ no
sysadm_r	□	□	□	ok	● yes	○ no
webmaster_r	☑	☑	□	☑	● yes	○ no
webmin_t	□	□	□	ok	● yes	○ no

/wwwnumber of files :6

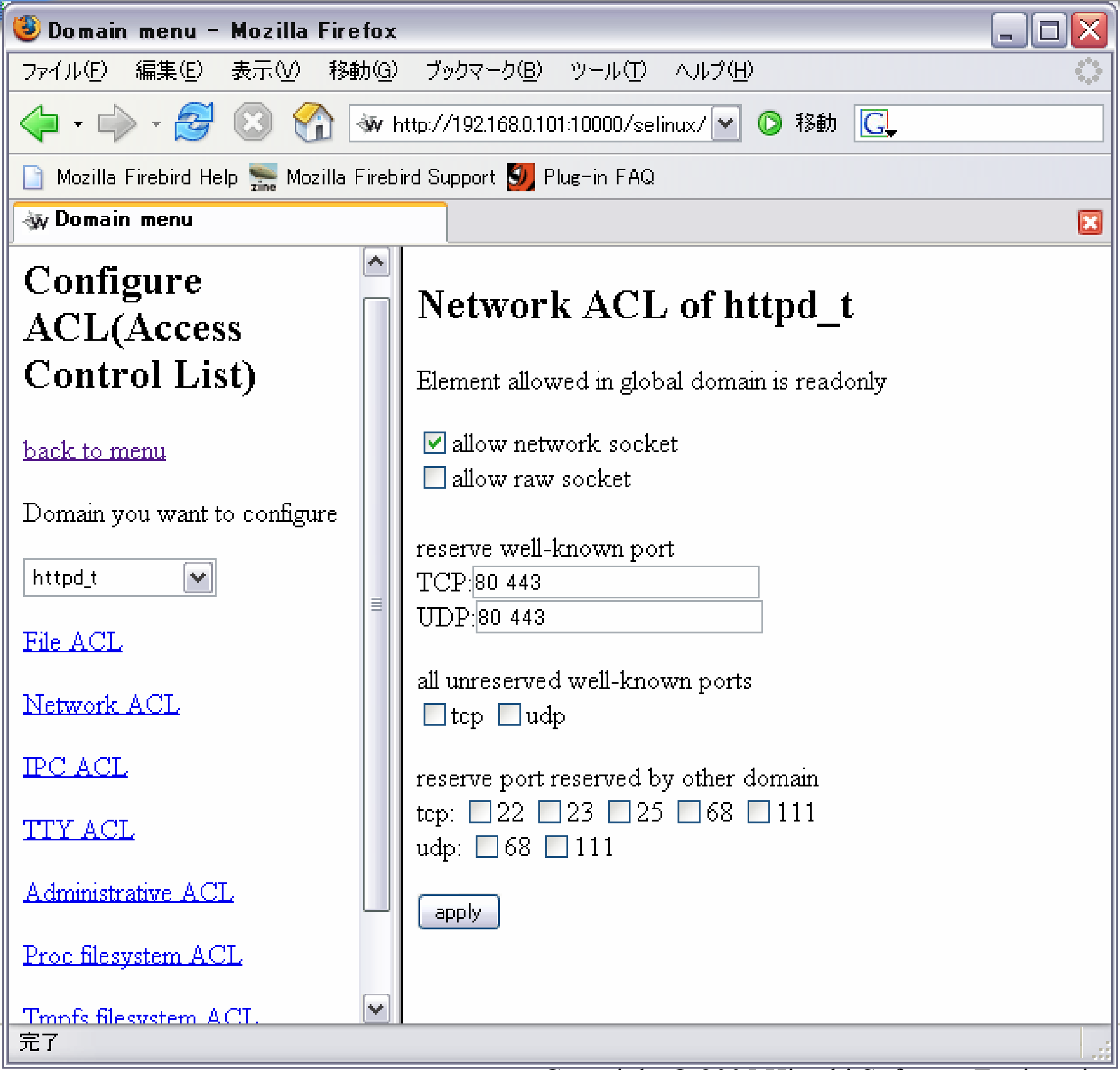
ctory

no

1-

Network

HitachiSoft


Domain menu - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)
http://192.168.0.101:10000/selinux/
移動
Mozilla Firebird Help
Mozilla Firebird Support
Plug-in FAQ
Domain menu
完了

Configure ACL(Access Control List)

back to menu

Domain you want to configure

httpd_t

File ACL

Network ACL

IPC ACL

TTY ACL

Administrative ACL

Proc filesystem ACL

Tmpfs filesystem ACL

Network ACL of httpd_t

Element allowed in global domain is readonly

☑ allow network socket
□ allow raw socket

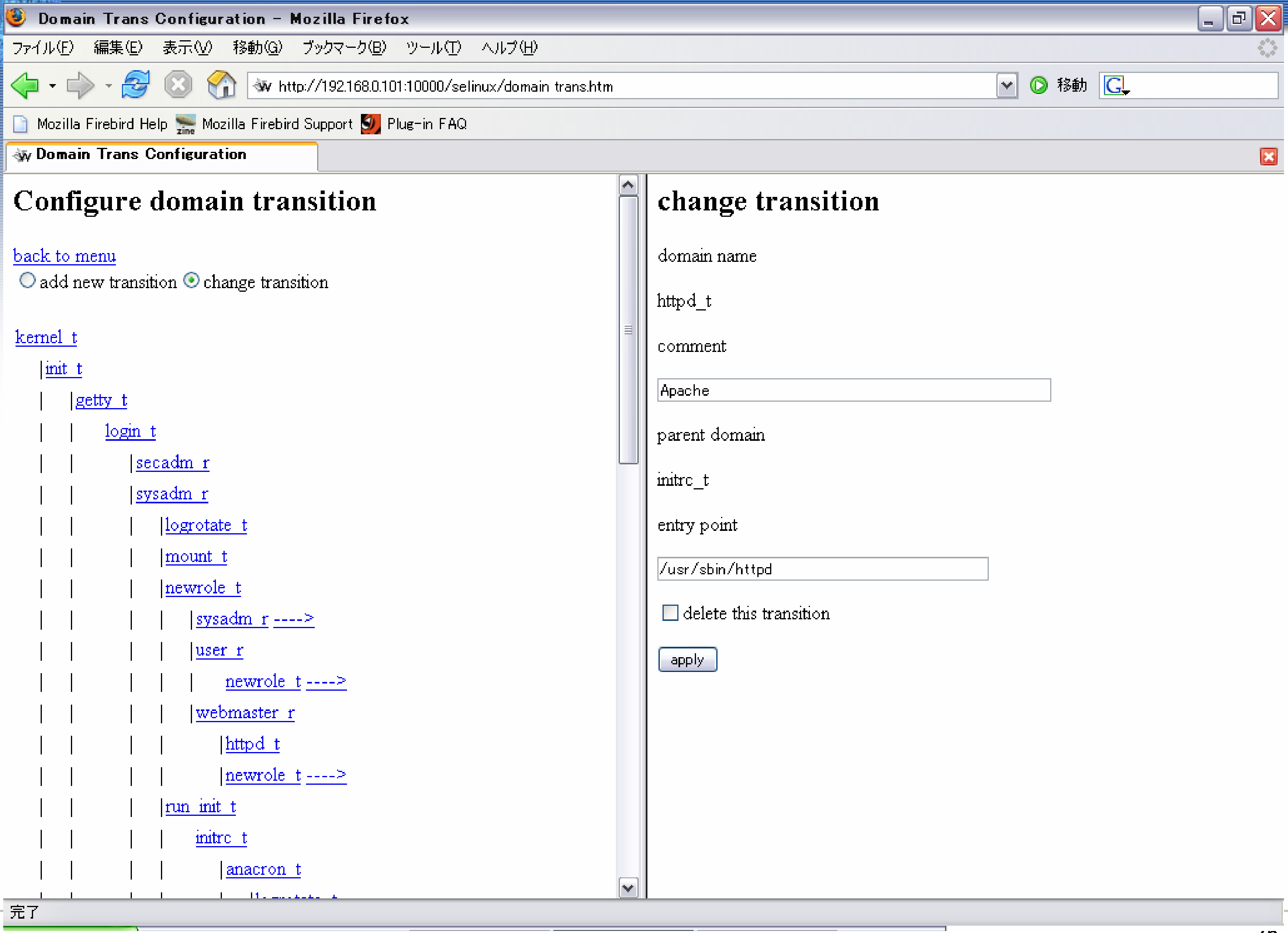
reserve well-known port
TCP: 80 443
UDP: 80 443

all unreserved well-known ports
□ tcp □ udp

reserve port reserved by other domain
tcp: □ 22 □ 23 □ 25 □ 68 □ 111
udp: □ 68 □ 111

apply

Domain trans


Domain Trans Configuration - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)
http://192.168.0.101:10000/selinux/domain trans.htm
移動
Mozilla Firebird Help
Mozilla Firebird Support
Plug-in FAQ
Domain Trans Configuration
完了

Configure domain transition

back to menu

○ add new transition ● change transition

```
kernel_t
   |init_t
   |   |getty_t
   |   |   login_t
   |   |       |secadm_r
   |   |       |sysadm_r
   |   |       |   |logrotate_t
   |   |       |   |mount_t
   |   |       |   |newrole_t
   |   |       |   |   |sysadm_r ---->
   |   |       |   |   |user_r
   |   |       |   |   |   newrole_t ---->
   |   |       |   |   |webmaster_r
   |   |       |   |       |httpd_t
   |   |       |   |       |newrole_t ---->
   |   |       |   |run_init_t
   |   |       |   |   initrc_t
   |   |       |   |       |anacron_t
```

change transition

domain name

httpd_t

comment

Apache

parent domain

initrc_t

entry point

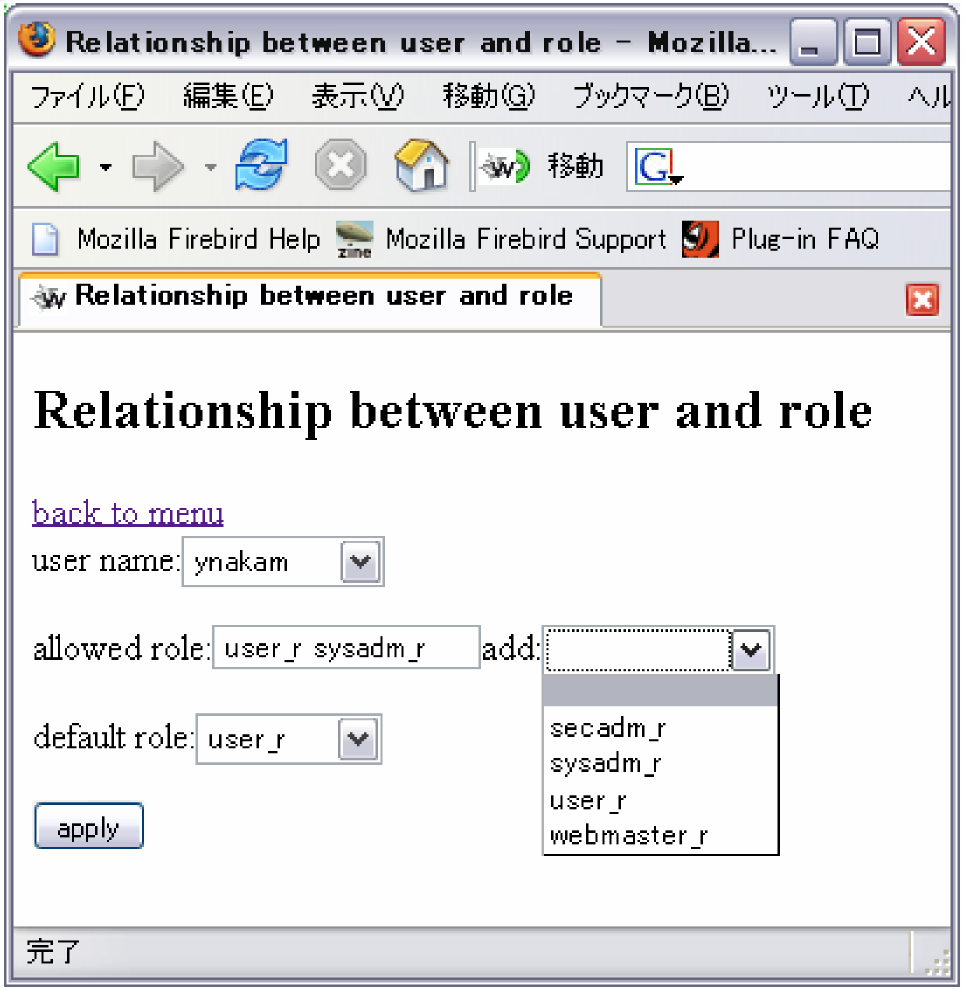
/usr/sbin/httpd

□ delete this transition

apply

RBAC

HitachiSoft


Relationship between user and role - Mozilla...
ファイル(F) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘル
移動
Mozilla Firebird Help
Mozilla Firebird Support
Plug-in FAQ
Relationship between user and role
完了

Relationship between user and role

back to menu

user name: ynakam

allowed role: user_r sysadm_r add:

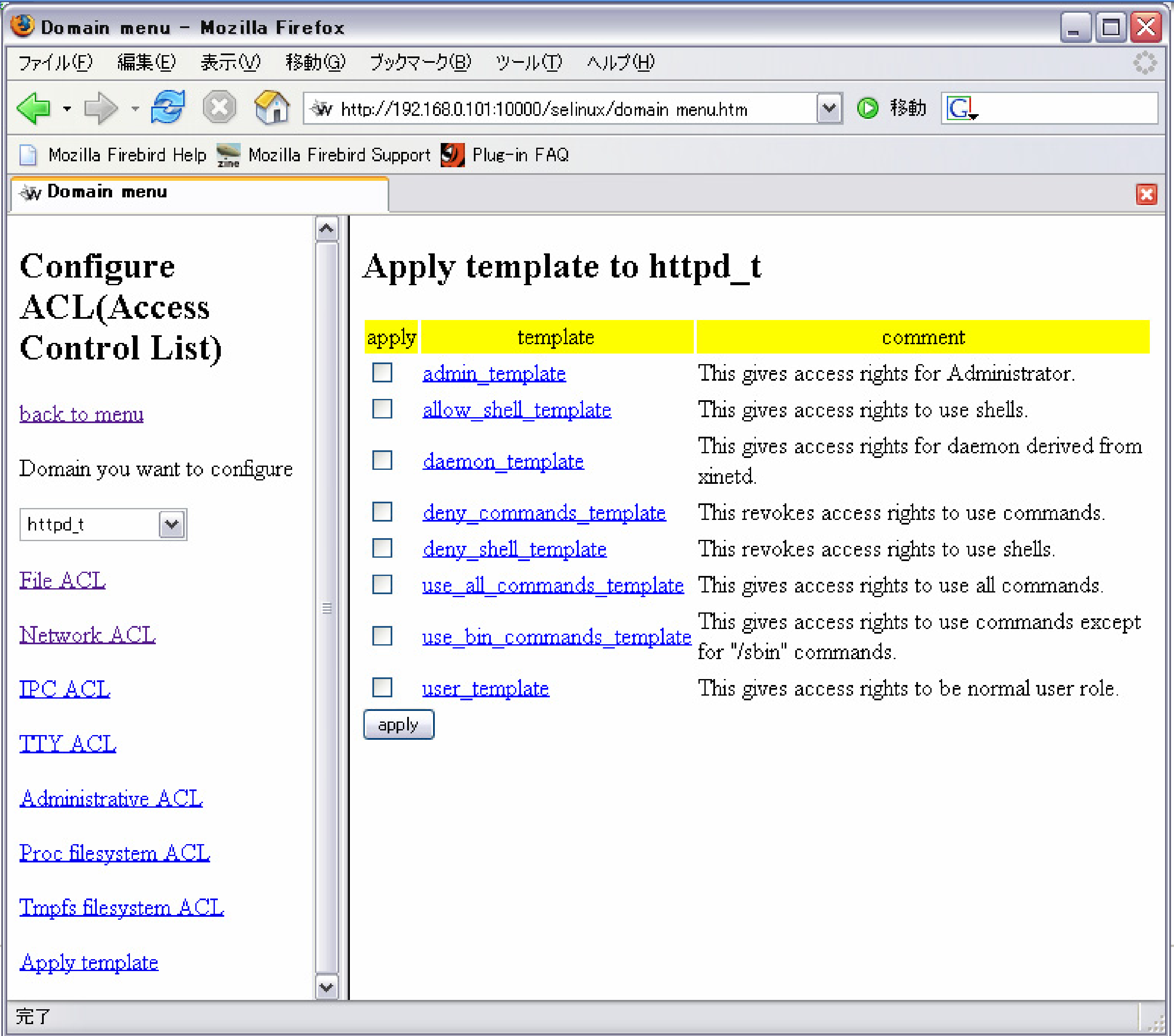
secadm_r
sysadm_r
user_r
webmaster_r

default role: user_r

apply

Template

HitachiSoft


Domain menu - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)
http://192.168.0.101:10000/selinux/domain menu.htm
移動
Mozilla Firebird Help
Mozilla Firebird Support
Plug-in FAQ
Domain menu
完了

Configure ACL(Access Control List)

back to menu

Domain you want to configure

httpd_t

File ACL

Network ACL

IPC ACL

TTY ACL

Administrative ACL

Proc filesystem ACL

Tmpfs filesystem ACL

Apply template

Apply template to httpd_t

apply	template	comment
□	admin_template	This gives access rights for Administrator.
□	allow_shell_template	This gives access rights to use shells.
□	daemon_template	This gives access rights for daemon derived from xinetd.
□	deny_commands_template	This revokes access rights to use commands.
□	deny_shell_template	This revokes access rights to use shells.
□	use_all_commands_template	This gives access rights to use all commands.
□	use_bin_commands_template	This gives access rights to use commands except for "/sbin" commands.
□	user_template	This gives access rights to be normal user role.

apply

History of SELinux Policy Editor

- Developed by Hitachi Software.
- First public release on 2003/1/31 by Hitachi Software
  - GPL
  - At http://www.selinux.hitachi-sk.co.jp/en
  - English and Japanese support
  - Only for 2.4 based SELinux

- Patch by Japan SELinux Users Group
  - Work on Fedora Core2
    - □ Mostly Mr. Takefumi Onabuta's contribution
  - patch to original version
- Future maintenance will be by SELinux Users group
  - In summer, we will have time
    - □ But stop development from now to May.

Problem of SELinux Policy Editor

- Reduced Security
  - Effect of integrating object classes, access vector
    - □ Example:File access vector
      - only s(getattr), r(read), w(write), c(create)
      - Does not support “append”
    - □ Syntax that supports detailed configuration is needed

- Can not use default policy
  - SELinux policy->Simplified policy is not supported
  - Policy packed with SELinux Policy Editor supports limited daemon
    - □ httpd, sshd
    - □ We have to prepare policy for other daemons

- Maintenance
  - Compiler must be modified to support new version of SELinux
    - □ Access vector, object class are changed

TO DO

- “audit2allow” feature
- Detailed config mode
- Converter SELinux policy -> Simplified language
  - will be difficult..
- Conditional Policy Extension support
- Improvement of usability

Downloading and installing

- You can download latest version
  - http://prdownloads.sourceforge.jp/selpe/13437/SELPE_jselugpatch.tgz
  - Extract and read “README”

Summary

HitachiSoft

- Complexity of SELinux policy
  - Type-label
  - Too many elements
  - Text-based

- SELinux Policy Editor
  - Resolve the complexity of SELinux by
    - □ Simplified language
    - □ GUI

Acknowledgements

- Mr. Takefumi Onabuta
  - Development of patch for FedoraCore2
- Dr. Jonathan Stanton, GWU
  - Advice for abstract

DIGITAL&GLOBAL

日立ソフト

HitachiSoft