



特定非営利活動法人(内閣府 NPO 法人)

日本オープンソース推進機構

Japan Open Source Advocacy Organization

2005 SELinux Symposium

SELinux business and community in Japan

Yuichi Nakamura

(ynakam@selinux.gr.jp)

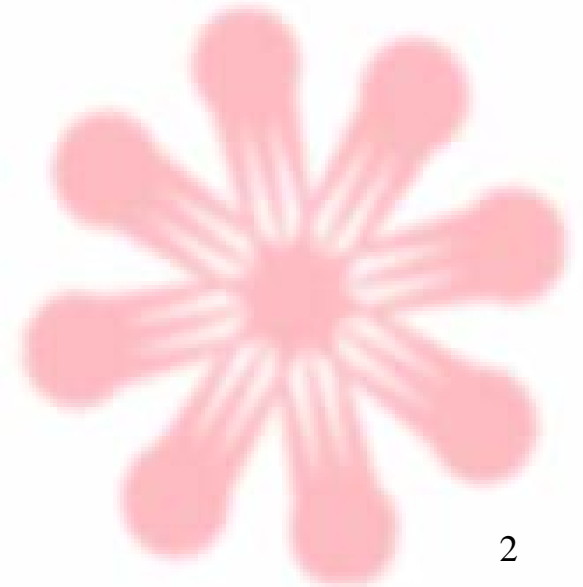
Japan Open Source Advocacy Organization





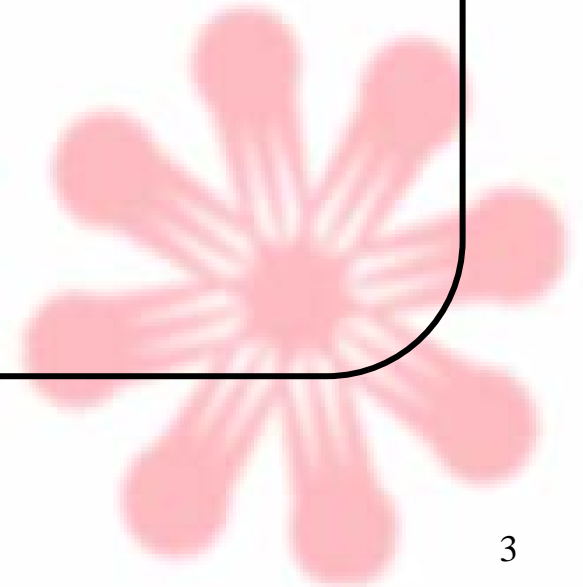
Contents

- * 1. Introduction
- * 2. Promotion
- * 3. Business
- * 4. R&D
- * 5. Problems





1. Introduction





Activities in Japan

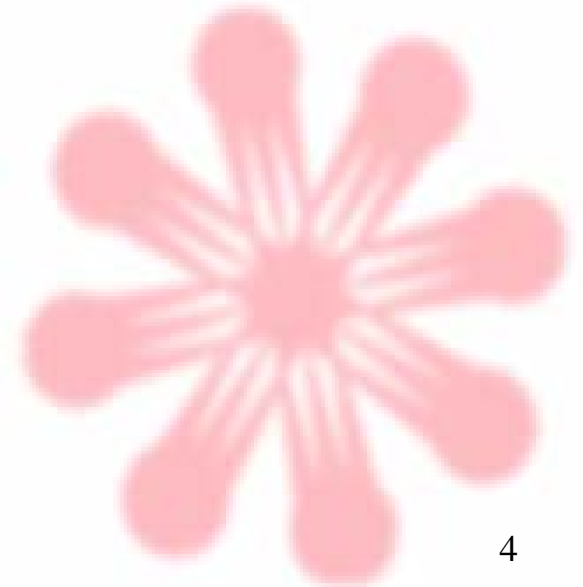
* Promotion

- * companies, communities , government are promoting
 - * Before kernel2.6
 - * Promotion is successful
 - * Many people are interested in SELinux in Japan

* Business

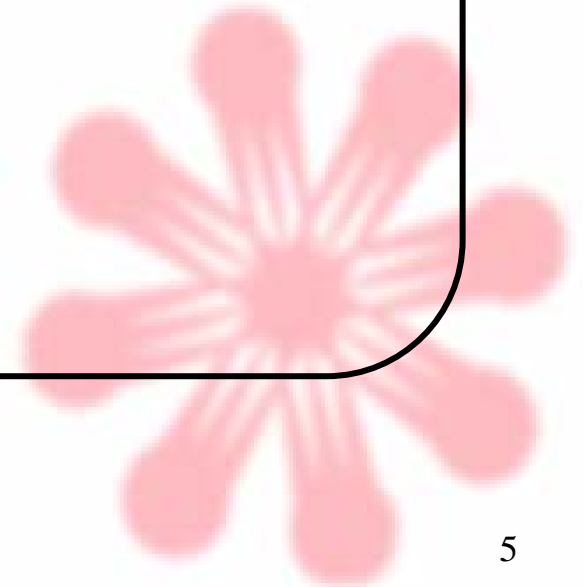
- * System construction
- * Product
- * Education

* R&D





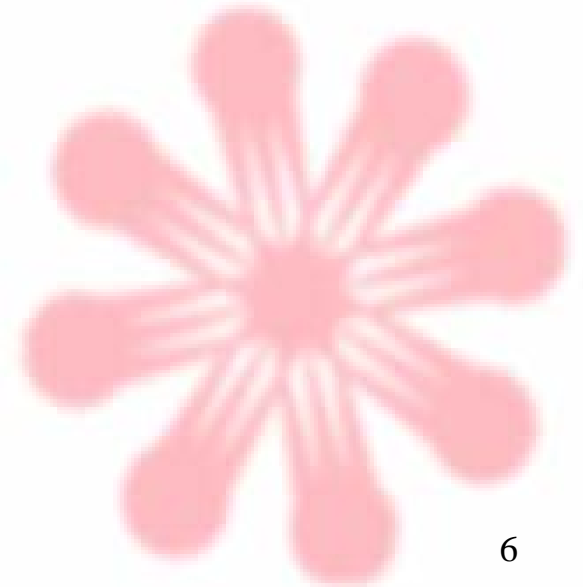
2. Promotion





Promotion of SELinux

- * With secure operating system
- * Publishing company
- * Government
- * Community





Promotion of SELinux with secure operating system(1)

- * SELinux is promoted with commercial secure operating system
- * Many commercial secure OS are used.
 - * Pitbull (Argus System, USA)
 - * Hizard (Secubrain, South Korea)
 - * Secuve TOS (Secuve, South Korea)
 - * Compartment Guard (HP Japan)
- * SELinux is good “entry point” to secure OS for business scene
 - * Free, many documents, included in Linux distributions..

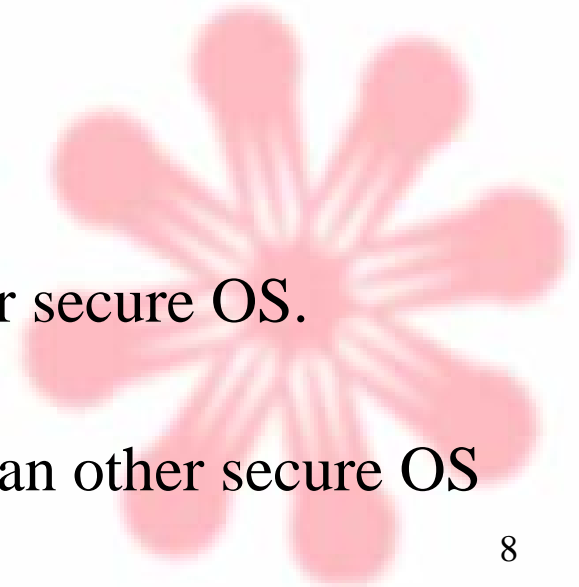




Promotion of SELinux with secure operating system(2)

- * SELinux is promoted cooperating with other secure OS.
 - * Develop market of secure OS together.
 - * Cooperate in conference, exhibitions, write article together, discussion
 - * Example: “Secure OS Conference” 2004/4,12
 - * More than 200 people

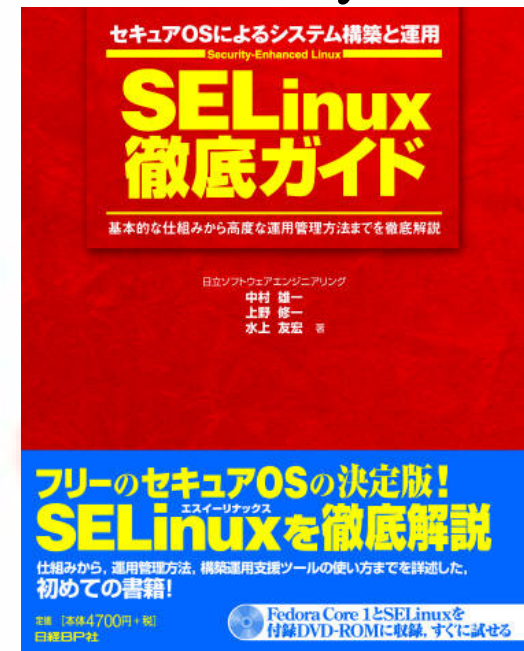
- * As a result
 - * SELinux is more well known.
 - * Side-effect
 - * SELinux is often compared with other secure OS.
 - * Many people think :
SELinux is much more difficult than other secure OS





Promotion with publishing company(1)

- * Publish companies are interested in SELinux
 - * Since kernel 2.4 SELinux.
- * Articles in magazines
 - * more than 15 articles in 2004, 6 articles in 2003, many others in web magazines.
- * First(?) SELinux book(2004/3)
 - * <http://www.amazon.co.jp/exec/obidos/ASIN/4822221113>
- * Exhibition
 - * net&com 2004
 - * Linux World Japan





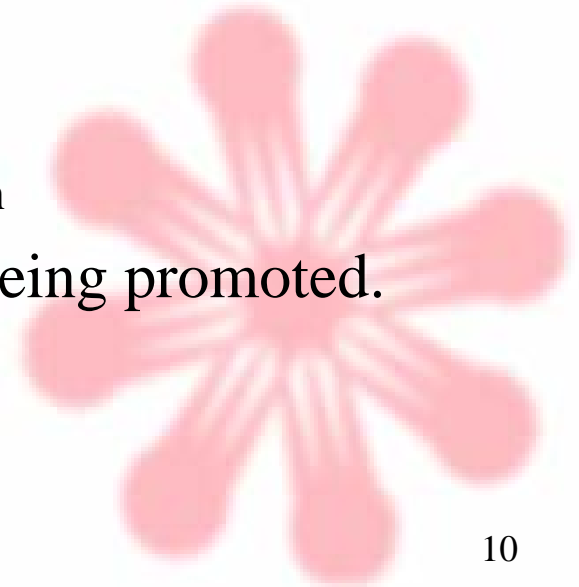
Promotion with publishing company(2)

* As a result

- * Many people know SELinux
- * Many Japanese documentation

* Side-effect

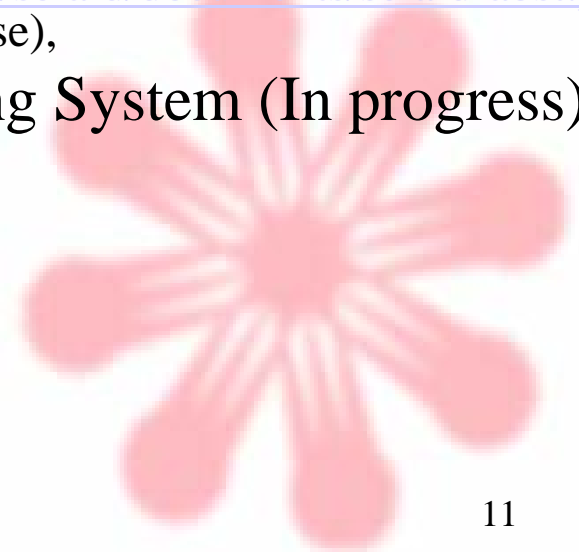
- * They think SELinux is difficult.
 - * No targeted policy in 2003
 - * Some concepts are difficult
 - * RBAC, security context , domain transision
- * As a entry-point to SELinux: LIDS is being promoted.
- * LIDS(<http://www.lids.org/>)
 - * Easy MAC system.
 - * No type label





Government

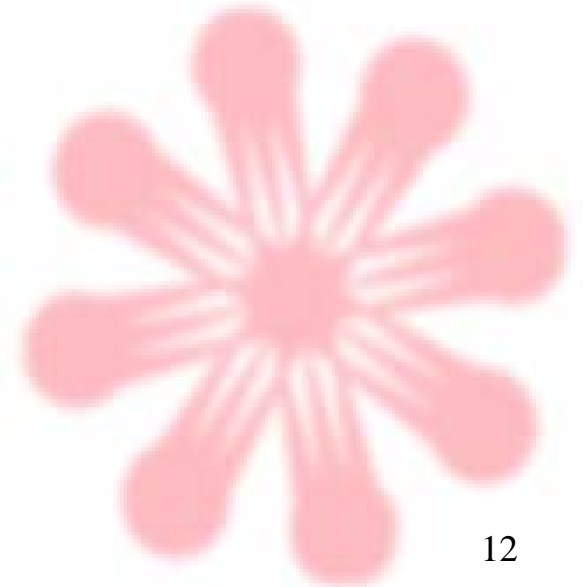
- * Ministry of Internal Affairs and Communications
 - * Research committee of Secure OS
- * IPA (Information Technology Promotion Agency)
 - * 2001-2002: Research of OS security and SELinux
 - * http://www.ipa.go.jp/security/fy13/report/secure_os/secure_os.html(Japanese)
 - * 2003: Development for SELinux tool(SELinux/Aid)
 - * <http://www.ipa.go.jp/security/fy15/development/selaid/documents/selaid-abst.pdf>
(Abstract only is English most of this is Japanese),
 - * 2004: Research about Secure Operating System (In progress)
- * Other ministries
 - * Closed committee about Secure OS





Promotion by Community

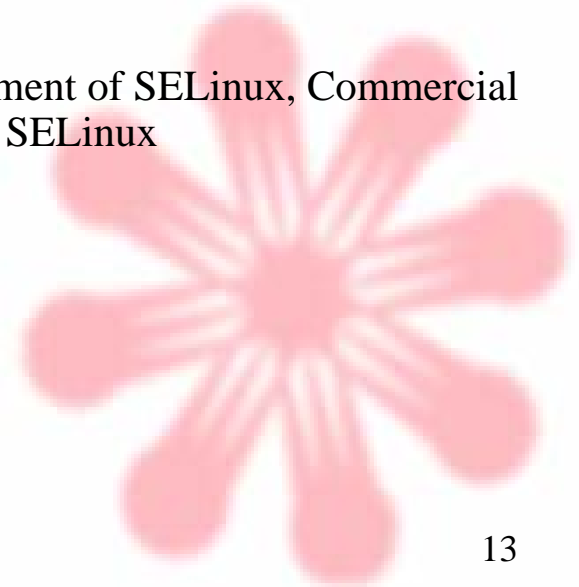
- * Japan SELinux Users group
- * JOSAO
- * Other Groups





Japan SELinux Users Group

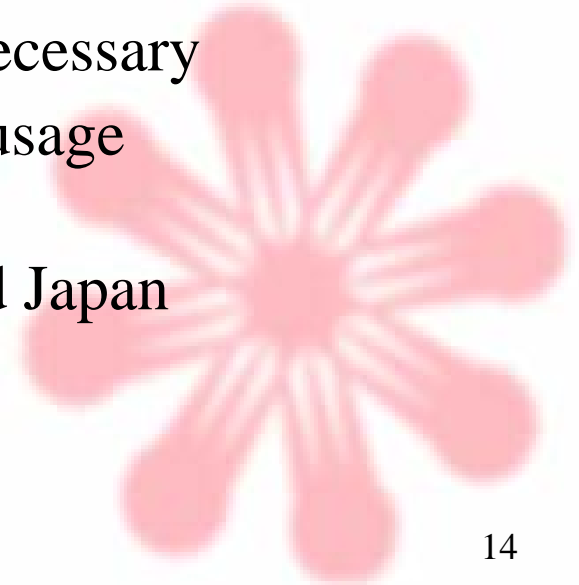
- * Provide place to communicate for engineer
 - * Homepage: <http://www.selinux.gr.jp/>
 - * Mailing List
 - * About 750 people , 1-2 mails per day
 - * Event for discussion
 - * Workshop 2004/7/16
 - * SELinux BOF 2004/11/30
 - * 5 presentations
 - * Trend of SELinux, Performance improvement of SELinux, Commercial secure OS vs SELinux , Tutorial, Usage of SELinux
- * Place for development
 - * 2.4 install package (now stopping..)
 - * Maintenance of SELinux Policy Editor
- * Documentation
- * Never involved in business.





JOSAO SELinux committee

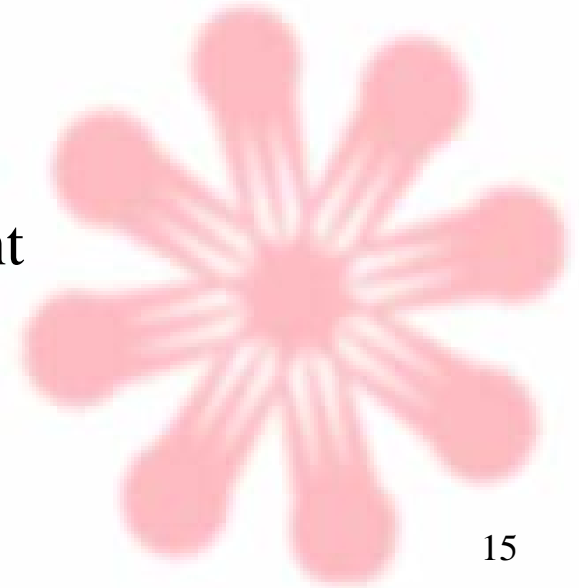
- * Japan Open Source Advocacy Organization(JOSAO)
 - * <http://www.josao.jp/>
- * Members from various companies
 - * Software company, Data center, Linux Distributor
- * Promote business usage of SELinux
 - * For more promotion, “case study” is necessary
 - * Trying to find case study of business usage
 - * SELinux trial campaign (In progress)
 - * SELinux hacking demo in LinuxWorld Japan





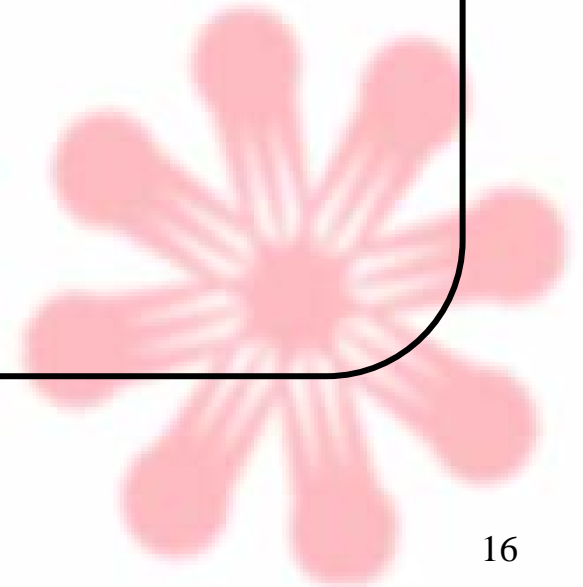
Other communities

- * Linux consortium(<http://www.linuxcons.gr.jp/>)
 - * Comparison of secure OS
- * Secure OS research group
 - * In the information network law association
 - * <http://in-law.jp/index-eng.htm>
 - * Discussion of secure OS
- * Secure OS research group
 - * In Japan Society of Security Management
 - * <http://www.jssm.net/>
 - * Developing criteria of secure OS





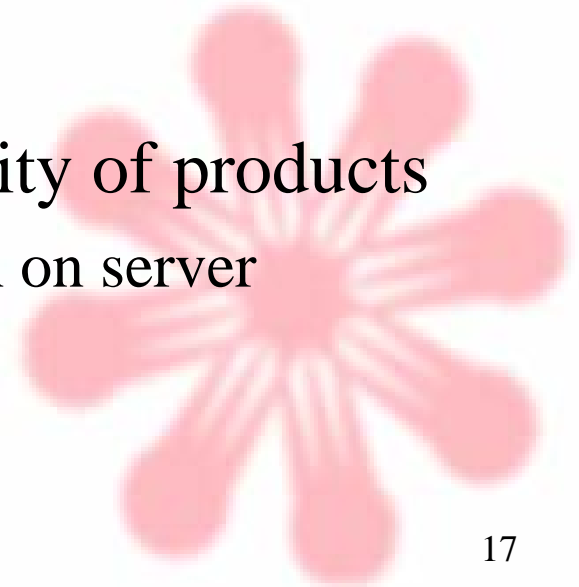
3. Business





Business

- * System construction & support using SELinux
 - * It will be main, currently not so big but some examples.
 - * In combination with other products
- * Education, publishing
- * Product using SELinux
 - * SELinux is used to enhance security of products
 - * Example: Distribution, single-sign on server
 - * Tools
 - * Available tools are free however.

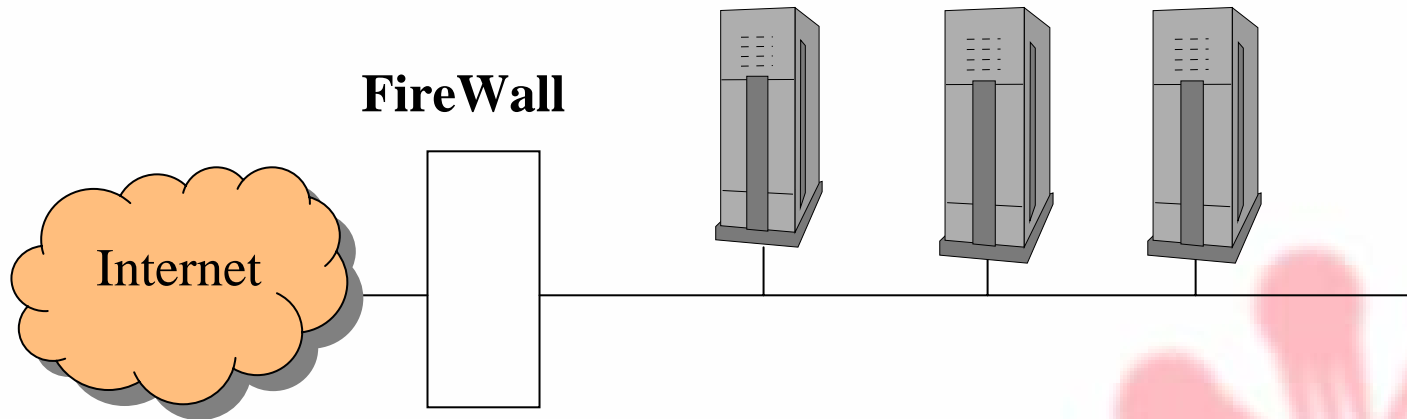




System Construction: Advantage of SELinux for customer(1)

* Typical system for DMZ without SELinux

WWW Mail DNS



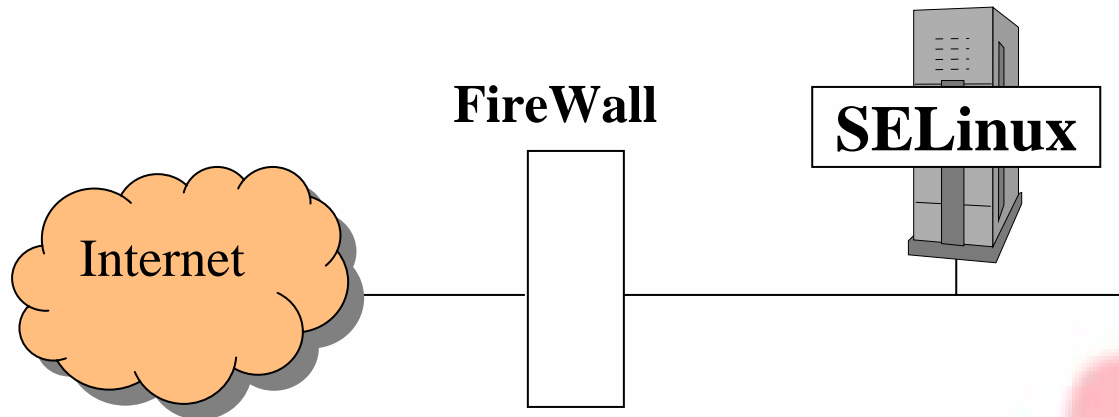
- One application for one machine
- Must apply security patch immediately



System Construction: Advantage of SELinux for customer(2)

* DMZ system using SELinux : Simple System

WWW+Mail+DNS



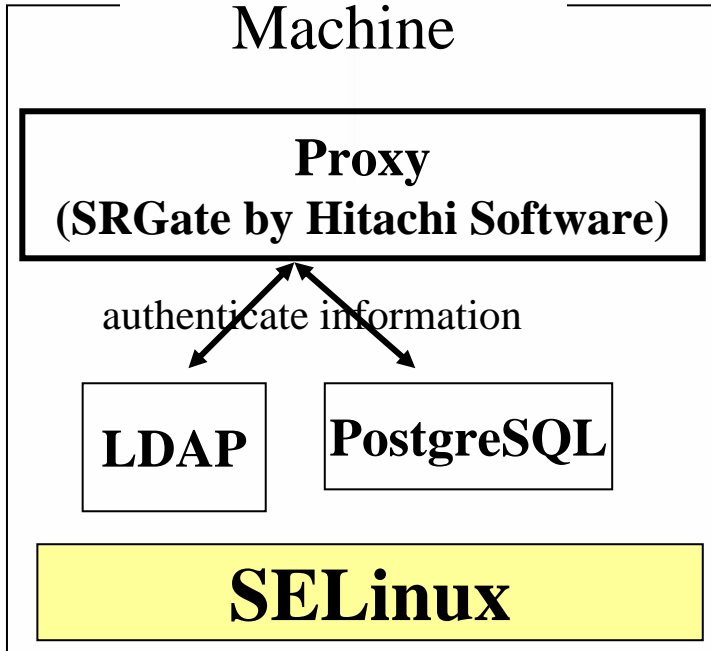
- Multiple applications in one machine
- Need not apply patch immediately
 - time to evaluate patch

SELinux can reduce costs of machine and maintenance



System construction: Customer Example

Single Sign on Machine



- * Single-sign on system
 - * Developed by Hitachi Software
 - * Sold as “SRGate” with SELinux
- * Customer: a manufacture company
- * SELinux based on SUSE Linux 9
- * Customer chose SELinux because:
 - * 1) Within one machine three applications
 - * Proxy, LDAP, PostgreSQL
 - * 2) Security level is enhanced



Education

* Motivation

- * Few engineers can construct SELinux system

* SELinux Training course by Japan Trusted System(www.jts1.co.jp)

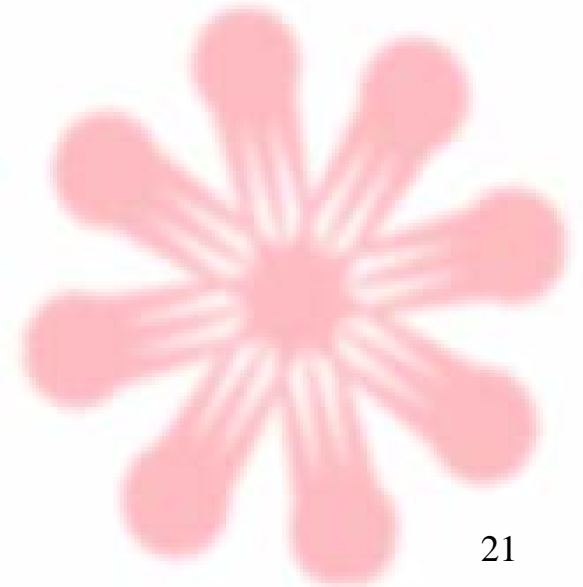
- * 1day, 2day courses
- * 7 companies are selling
- * Total about 170 students

* Students

- * Marketing dept, R&D dept, Education Dept etc.
- * Some of them become teacher in their company
 - * SELinux spread from teacher!

* Future:

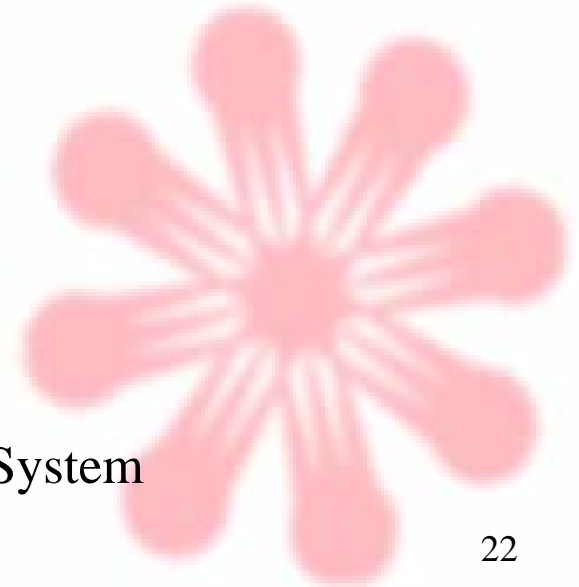
- * Qualifying examination with Turbo Linux





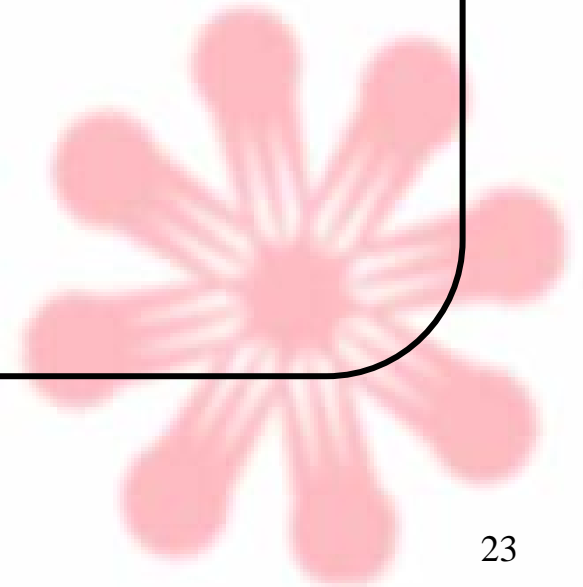
Product example: Turbo Linux

- * Turbo Linux <http://www.turbolinux.com/>
 - * Japanese Distributor
 - * Main market is Japan ,China
 - * Server: No2 in Japan, No1 in China
- * Turbo Linux 10 Server
 - * Latest server distribution (2004/11)
 - * SELinux support
 - * based on strict policy
 - * Not general use
 - * Apache, BIND, postfix.. etc are supported
 - * SELinux/Aid
 - * tool developed by Hitachi Software
 - * Education
 - * SELinux training course with Japan Trusted System
 - * SELinux qualifying examination(2005/5)





4. R&D





R&D

* NEC

- * Performance improvement

* NTT Data

- * Dynamic state change extension

* Japan Research Institute

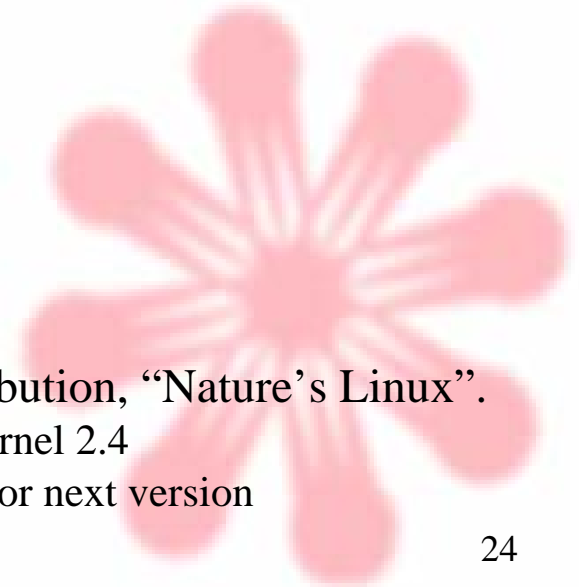
- * LBSM

* Hitachi Software

- * Tools: SELinux Policy Editor, SELinux/Aid
- * Available on <http://www.selinux.hitachi-sk.co.jp/>

* IPTelecom

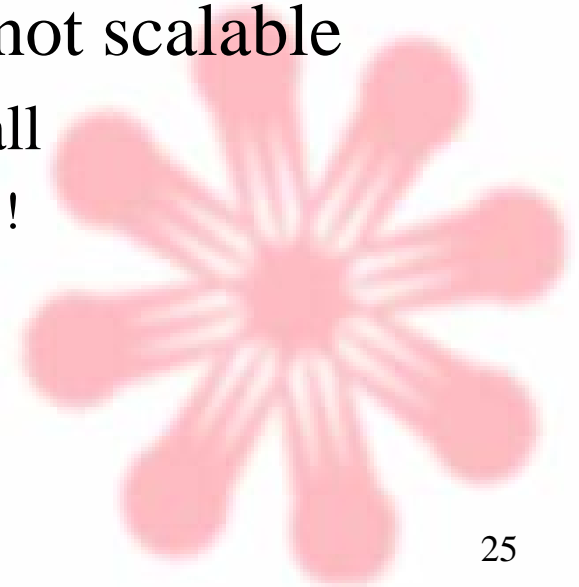
- * Develop and maintain original security-enhanced distribution, “Nature’s Linux”.
- * running with some part of code in grsecurity based-on kernel 2.4
- * currently developing with SELinux based-on kernel 2.6 for next version





Performance improvement

- * By NEC
- * Included in mainline kernel
- * Improved scalability of SELinux
 - * Rewrite AVC by using RCU
 - * Before using RCU: SELinux was not scalable
 - * Example : performance of write() call
 - * 2CPU:58%, 4CPU:10 %, 32CPU:0.1%!
 - * After RCU: SELinux is scalable
 - * performance of write()call
 - * almost the same up to 32 CPU!





Kernel based IDS

- * Developed by NTT Data(<http://www.nttdata.co.jp/en/>)
 - * For detail: Adaptive Access Policy for the Linux Kernel, Horie et.al., The 2005 International Symposium on Applications and the Internet
 - * <http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=30170&page=1>
- * Extension of SELinux Policy
 - * 1) Register “Trigger” access by policy extension
 - * 2) Change policy state dynamically when trigger comes
 - * Like cond policy extension

* Example:

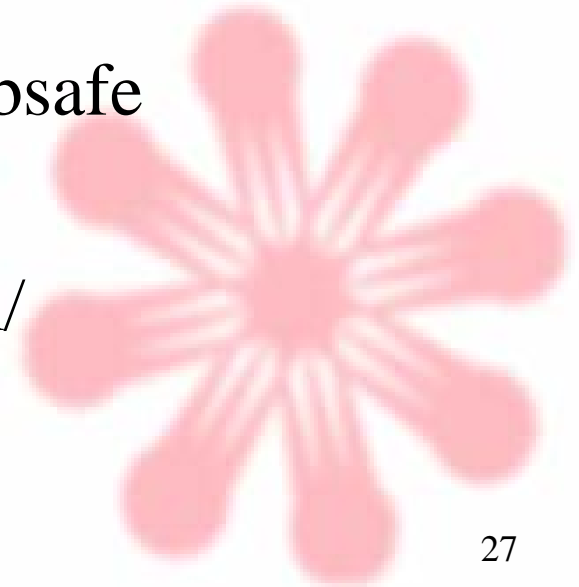
```
strict ftpd_t shell_exec_t:file { execute } ; ... Watch execute access of /bin/sh  
allow ftpd_t user_home_t:file rw_create_file_perms 1; State 1: ftpd can upload file  
allow ftpd_t user_home_t: file r_file_perms 3 ; State 3: ftpd can not upload file
```

When shell exec is detected,
policy changes from state 1(ftp can upload) to state 3(ftp can not upload)



Linux Basic Security Modules(LBSM)

- * Developed by Japan Research Institute
(<http://www.jri.co.jp/english/>)
- * Log gathering function
 - * Works on SELinux
- * MAC by LOMAC model
- * Prevention of Buffer Overflow by libsafe
- * Available at
 - * <http://sourceforge.jp/projects/lbsm/>

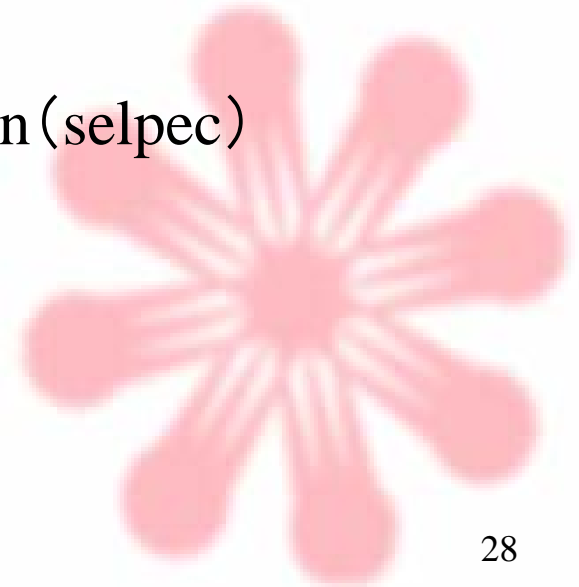




SELinux/Aid

- * Available under GPL
 - * <http://www.selinux.hitachi-sk.co.jp/tool/selaid/selaid-top.html>
- * Developed by Hitachi Software
 - * sponsored by IPA(Information technology Promotion Agency, Japan)
- * Included in Turbo Linux 10 Server
- * English is supported

- * Composed of 3 tools
 - * SELinux Policy Editing and Configuration (selpec)
 - * Policy view/edit tool
 - * X, Web browser, console interface
 - * SELinux LOG analyzer(sellog)
 - * SELinux log analyze tool
 - * SELinux CHecKer(selchk)
 - * policy, file context check tool





Screenshot of selpec(1)

Security Policy Operation - Edit Policy Configurations - Access Control List - File

Application: **apache** Comment: Apache - Web server

Source Domain: **httpd_t** Comment: The httpd_t is a domain for apache core process.

File ACL (General) | File ACL (Others) | File Descriptor

Path: /var/www/html

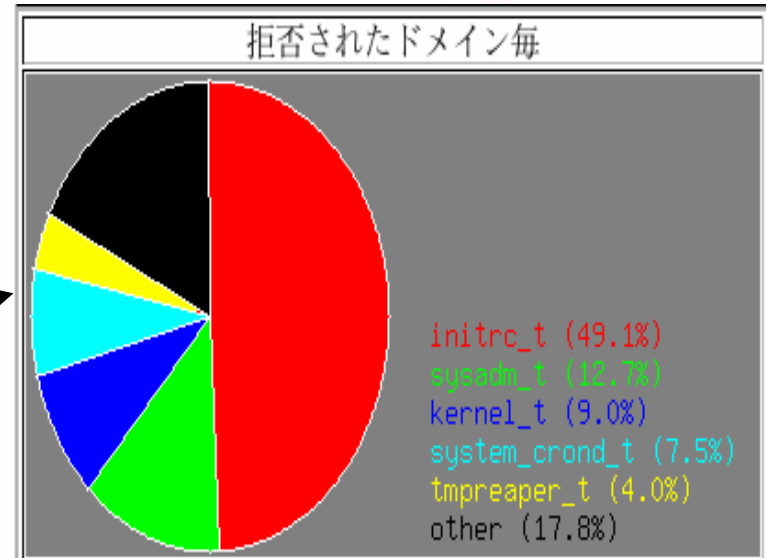
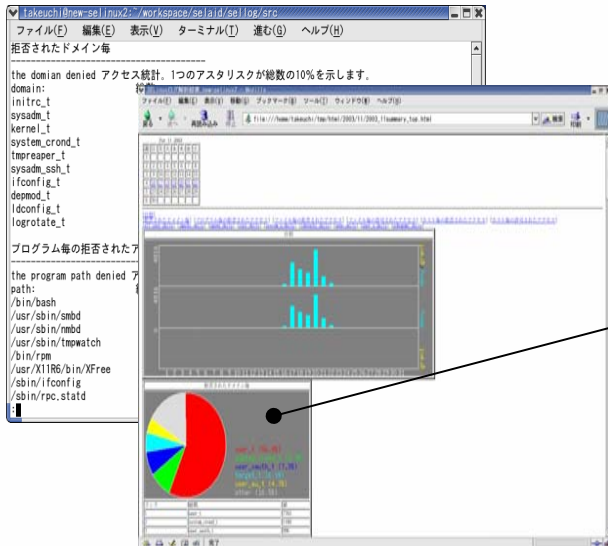
Persistently Labeled Files:						
Name	Type Name	Class N...	READ	WRITE	EXECUTE	SEARCH
.	httpd_sys_content_t	dir	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
mrtg	httpd_sys_content_t	dir	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
usage	httpd_sys_content_t	dir	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

To allow permission only check



Sellog

- sellog
 - Analyze SELinux audit log
 - Show statistics
 - Search suspicious log





sellog screenshot

WARNING_REMOTE_ATTACK

リモートアタックによりshellが立ちあげが拒否された痕跡がある。ただし、被害の痕跡は見当たらない。

close

Result - Mozilla

ファイル(E) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ウィンドウ(W) ヘルプ(H)

再読み込み 停止 file:///home/ynakam/logtool/result/audit 検索 印刷

Red Hat Network Support Shop Products Training

の利用期間:7月7日19時41分0秒-8月3日7時10分59秒

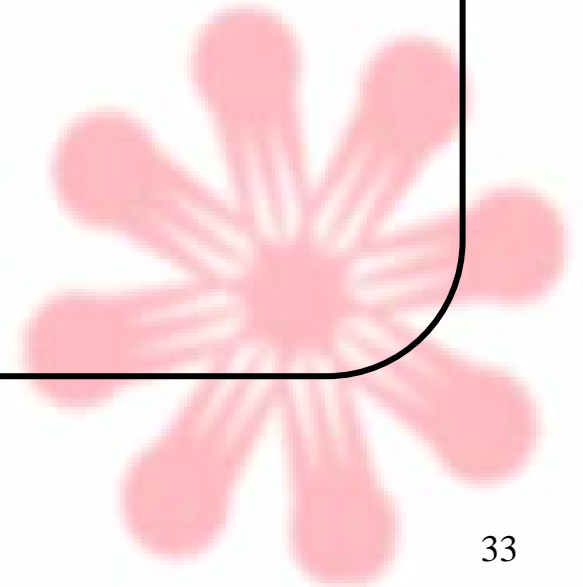
	08/02 01:15:09	SYSTEM_OTHER	for user ueno Aug 2 01:15:09 TEST log for samba attack
<u>WARNING GENERAL</u> <u>WARNING_REMOTE_ATTACK</u>	08/02 01:15:10	<u>DENY SHELL</u>	Aug 2 01:15:10 192 kernel: avc: denied { execute } for pid=32440 exe=/usr/sbin/smbd path=/bin/bash dev=08:02 ino=162980 scontext=system_u:system_r:smbd_t tcontext=system_u:object_r:shell_exec_t tclass=file
	08/02 01:45:20	SYSTEM_OTHER	Aug 2 01:45:20 www sshd(pam_unix)[17093]: session opened for user ueno by (uid=500)
	08/02 01:48:04	SYSTEM_OTHER	Aug 2 01:48:04 www 8月 2 01:48:04 httpd: httpd停止 succeeded
	08/02 01:48:28	SYSTEM_OTHER	Aug 2 01:48:28 www 8月 2 01:48:28 httpd: httpd起動 failed

Explanation of Log

**Search suspicious log
by pattern match**



5. Problems





Problems

- * Many think SELinux is difficult
 - * Side effect of early promotion
- * R&D
 - * After development, few maintenance
 - * Budget
 - * Promotion is only within Japan
 - * Japanese culture?
 - * language, paper works
- * Need more case study, solutions
 - * Solutions understandable to customers





New law enforcement

- * We have to focus on Security in 2005.
 - * The new law, “Personal Information Protection Act” will be enforced from April 1st.
 - * Network service vendors, software vendors, system integrators and any vendors work for services treating private information, have to build for strong defensive system and order to take a measures to cope with this new law.
 - * For usual unix security system and open source system have been cracked ...
so new security systems based on LSM attract end user’s attention now.
 - * We’ve not still had enough experience and skills for security system like SELinux ...now trying to research and make good case studies.
 - * It’s going to be huge market about Security services in Japan for these reasons.
 - * We’d like to ask foreign security specialists to take notice of our security market in this year.



Acknowledgements

- * Dr. Jonathan Stanton@ The George Washington University
 - * Advice and review of Abstract and bio
- * Mr. Hideaki Saisho@ Hitachi Software
 - * Information about SRGate
- * Mr Hiroyuki Kojima@JOSAO
 - * Discussion about business usage, information about Nature's Linux
- * Mr. Kohei Kaigai @ NEC
 - * Information about his work on performance improvement
- * Mr. Naoki Yoshida @ Turbo Linux
 - * Information about Turbo Linux 10 Server
- * Mr. Takashi Horie@ NTT DATA
 - * Information about Kernel based IDS
- * Mr. Takefumi Onabuta @ Japan Research Institute
 - * Information about promotion of government and LBSM
- * Mr. Yuya Taguchi @ Japan Trusted System
 - * Information about education of SELinux
- * And, SELinux Developers!

