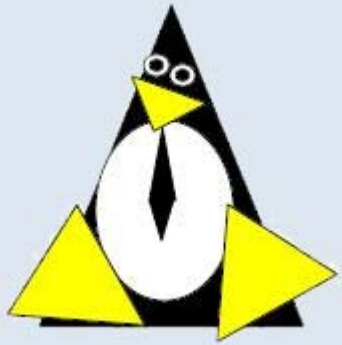
セキュアOSについて話しませんか？

NEC OSSプラットフォーム開発本部　　海外 浩平 <kaigai@ak.jp.nec.com>
NTTデータ 技術開発本部　　原田 季栄 <haradats@nttdata.co.jp>

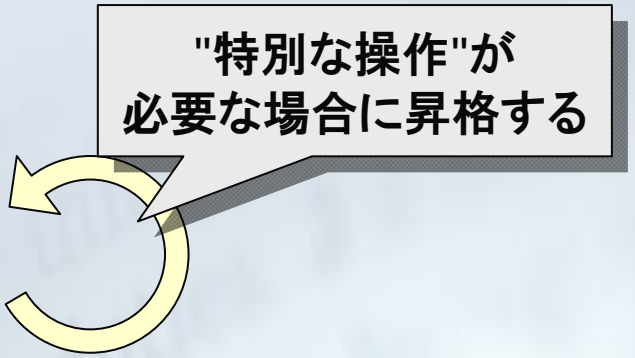
セキュアOSとは

- 定義
  - 万国共通の明確な定義はない :-)
  - 『最少特権』と『強制アクセス制御』の機能を持つ
    (セキュアOSと基盤ソフトウエアに関する研究会、'04)



最小特権

- 特権 (privilege)
  - 問答無用で "特別な操作" が許される
  - 特別な操作
    - ファイルに設定されたパーミッションを無視
    - ソケットをポート番号1024番未満にバインド
    - デバイスファイルを作成する
- 特権ユーザ
  - root　　：全ての特権を持っている
  - 非root　：全く特権を持っていない
- 最小特権 (Least privilege set)
  - 特定の利用者/プログラムに必要な特権だけを与える
    - POSIX Capability機能など



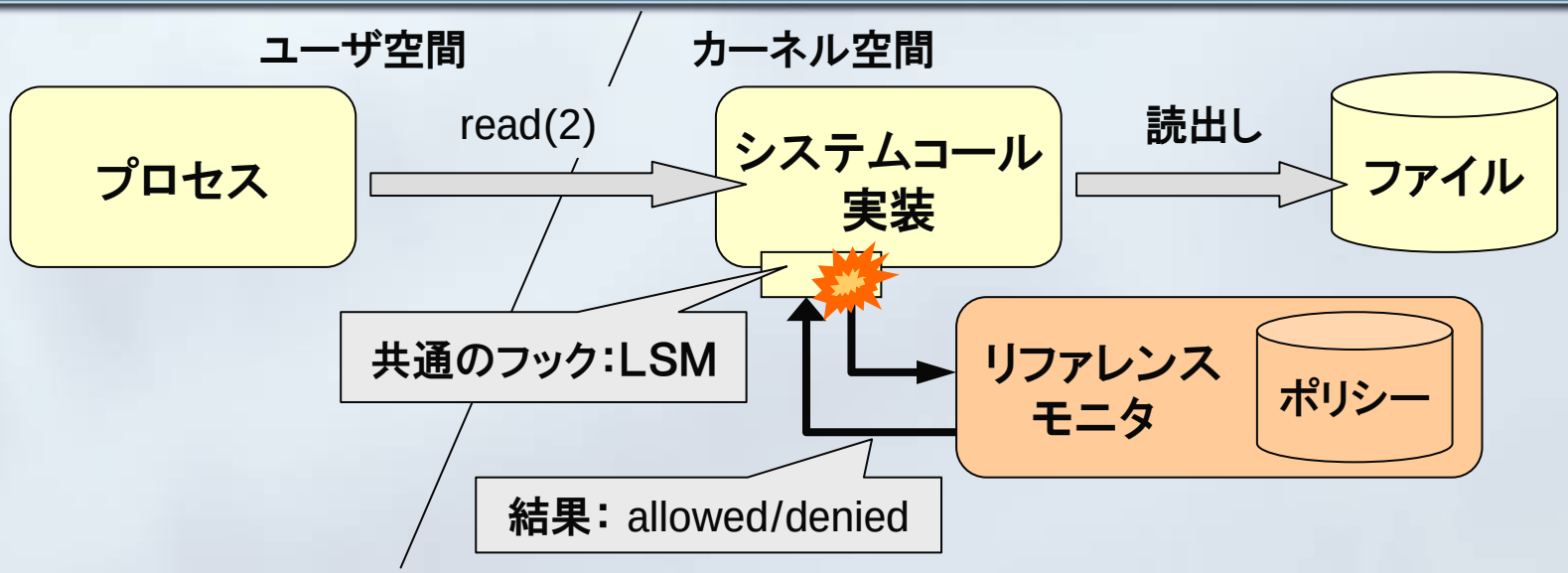
強制アクセス制御

- **任意アクセス制御** (DAC: Discretionary Access Control)
  - 伝統的な UNIX パーミッションの世界
  - ファイルの所有者が、"任意に"アクセス権を設定できる

```
% chmod 0644 myfile.txt
```

- **強制アクセス制御** (MAC: Mandatory Access Control)
  - セキュリティポリシーが、
    ファイルのアクセス権を"強制的"に設定する
    - ✓ファイルの所有者であっても、勝手に変更できない
  - 強制アクセス制御を無視する "特権" は無い
- **特典**
  - 勝手に公開範囲を変更されない
  - rootを奪取された場合の最後の砦

リファレンスモニタ



- OS資源にアクセスするには、システムコールが必須
  - ✓ システムコールの捕捉： LSMフレームワーク
- リファレンスモニタは、自身のポリシーに基づいて意思決定
  - ✓ 網羅性／一貫性の保証
- Linuxにおけるリファレンスモニタの実装
  - ✓ SELinux, TOMOYO Linux, Smack, AppArmor, LIDS, etc…

セキュアOSの利点

- Single Point of Failure の回避
  - 従来： root権限を奪われたら無条件降伏
    - ✓ システム中に一箇所でも権限昇格を許す穴が存在すればアウト
- アクセス制御における一貫性
  - 従来： サブシステム毎にバラバラのアクセス制御方式
    - ✓ ファイルシステム ⇒ rwx×{owner, group, others}
    - ✓ ネットワーク ⇒ ポート番号1024番未満 or Not?
    - ✓ データベース ⇒ GRANT / REVOKE
- 細粒度アクセス制御
  - 従来： 読み、書き、実行程度の粒度
    - ✓ 監査ログの改ざんを防ぎたい場合には？

セキュアOSの課題

- 標準セキュリティポリシーで未定義の動作
  - ポリシー学習モード(TOMOYO)、audit2allow (SELinux)
  - セキュリティポリシーの作成/編集
    - 難しい？情報が少ない？
    - プログラムが暗黙のうちに利用している権限
- アプリケーションの対応
  - セキュアOS環境での動作検証/保証なし
  - キラーアプリケーション不在
- 人間の心理
  - 「セキュリティなんて面倒なだけだよ～」

TOMOYO Linux最新動向

～詳細は、はてなダイアリーキーワードを参照ください～

最近(2008.4~)の主な活動

- **国際会議**
  - Embedded Linux Conference 2008, Ottawa Linux Symposium 2008 **でそれぞれ2回目の発表を行いました。**
    - “How to analyze your Linux’s behavior with TOMOYO Linux”(TOMOYO Linux**なら守るだけでなく解析もできるよ！）**
    - “Time to Glean: Mac For Linux”（LSM**メーリングリストの解析）**
  - Andrew Morton, James Morris**らを迎えて開催された**Linux Foundation Japan #8 SymposiumでTOMOYO Linux**のメインライン化の歩みについて発表を行いました。**
    - “Realities of Mainlining – Case of the TOMOYO Linux Project”
    - **資料および動画が公開されています。**
    - http://www.linux-foundation.jp/modules/tinyd5/index.php?id=9
  - **セキュリティの専門家、一般のユーザの方々に広く知っていただくために、**Black Hat 2008, linux.conf.au 2009**に提案中です。**

最近(2008.4~)の主な活動

- OSS活動
  - 2008.4 CELF Technical Jamboree (ELC参加報告)
  - 2008.5 TLUG (Tokyo Linux Users Group)
  - 2008.5 Linux World EXPO展示
  - 2008.8 OSC2008/名古屋
  - 2008.8 YLUGカーネル読書会(OLS参加報告)
  - 2008.8 CELF Technical Jamboree(OLS参加報告)
- 執筆
  - Software Design 4, 5月号「TOMOYO Linuxの歩き方」
  - Software Design 6月号「プロジェクト便り」
  - 2008.6 ThinkIT「チョコレートの国の侍」(連載全5回)

最近(2008.4~)の主な活動

- リリース
  - 2008.4 version 1.6
    - サーバでの利用のための機能強化
  - 2008.5 version 1.6.1
    - 環境依存のバグ等への対応
  - 2008.6 version 1.6.2
    - デスクトップでの利用のための機能強化
  - 2008.7 version 1.6.3
    - unionfsでの不具合の修正
  - 2008.9 version 1.6.4
    - 最新カーネルへの対応
- LiveCDリリース
  - Ubuntu
    - 適宜(随時)
    - Ubuntu本家より新しいです
  - CentOS
    - 2008.9提供開始
    - SELinuxと一緒に体験できます

最近(2008.4~)の主な活動

- その他の重要トピック
  - NPO日本ネットワークセキュリティ協会（というよりはJNSA）のWebサーバに導入しました。
    - 現在も稼働中です！（TOMOYO Linuxの公開している導入事例としては2件目）
    - http://www.jnsa.org/result/2007/tech/secos/
  - Mandrivaの最新カーネルに搭載されています。
    - http://tomoyo.sourceforge.jp/en/1.6.x/1st-step/mandriva2008.1/
  - 2chで2本目のスレが立ちました（だからどうした？）
  - TOMOYO Linuxを標準搭載しているTurbolinux 11 Serverの有償サポートをやっています。
    - ポリシーは公開しています。両方ともOSSなので利用するだけなら無料です。
    - http://www.turbolinux.co.jp/products/server/11s-tomoyolinux.html
  - 本格世界制覇進出に向けて、SourceForge.net, freshmeat.netにプロジェクトページを作成しました。

SELinux最新動向

～過去、現在、将来～拡大する適用領域

SELinuxの発展を振り返る

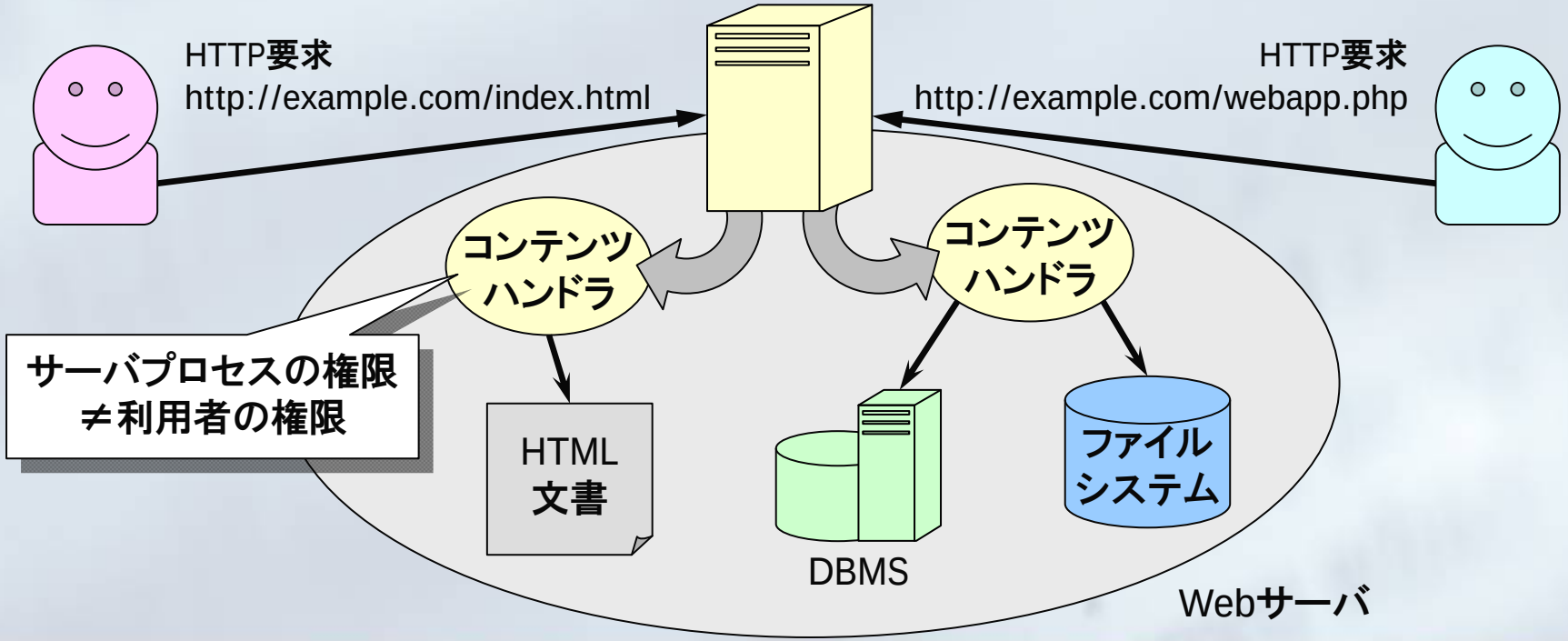
- ディストリビューション対応
  - RedHatEL, Fedora, Gentoo, Debian, Ubuntu, SuSE
- セキュリティポリシー
  - Reference Policy, Loadable Policy, SLIDE, Policy Druid
- システム管理
  - boolean, semanage/system-config-selinux, setroubleshoot
- ネットワーク
  - Labeled IPsec, CIPSO, Secmark, Labeled NFS
- 適応範囲の拡大
  - 組込みSELinux, SE-BSD, Solaris FMAC
  - X/SELinux, SE-PostgreSQL, XSM
- ISO/IEC15408認証

最新のトピック

- Kiosk PC
  - 公共施設で利用される共通の端末
  - SELinuxでゲスト利用者の権限を抑制、利用後の情報消去
- sVirt: SELinux - Virtualization Integration
  - KVMなどLinuxベース仮想化システムへの SELinux 適用
  - VM間の通信、Hyper Visorへの特権操作などを制御
- Per-Thread Individual Security Context
  - 一定の制約下でスレッド毎のセキュリティコンテキストを付加
  - Web ApplicationへのSELinux適用がターゲット
- SELinux User Guide
  - RedHat の Murray McAllister によるプロジェクト
  - 古くなったガイダンス文書/FAQを再編成

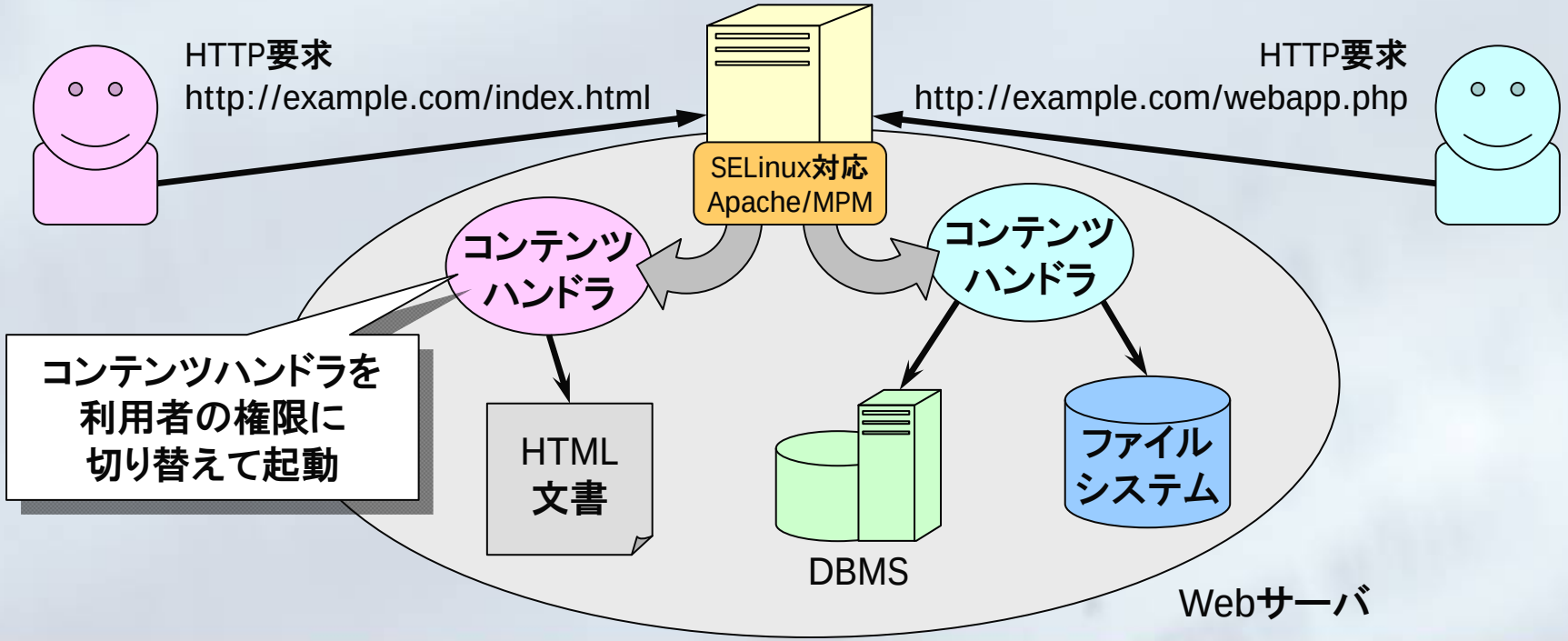
Web Application/SELinux連携

- 利用者が本質的に持っている権限
  ≠ ApacheがWeb Applicationを実行する際の権限
- 利用者に応じて、コンテンツハンドラの権限を切り替える
- 課題： マルチスレッド、KeepAlive
  - 解決策： Bounds Type、One time thread



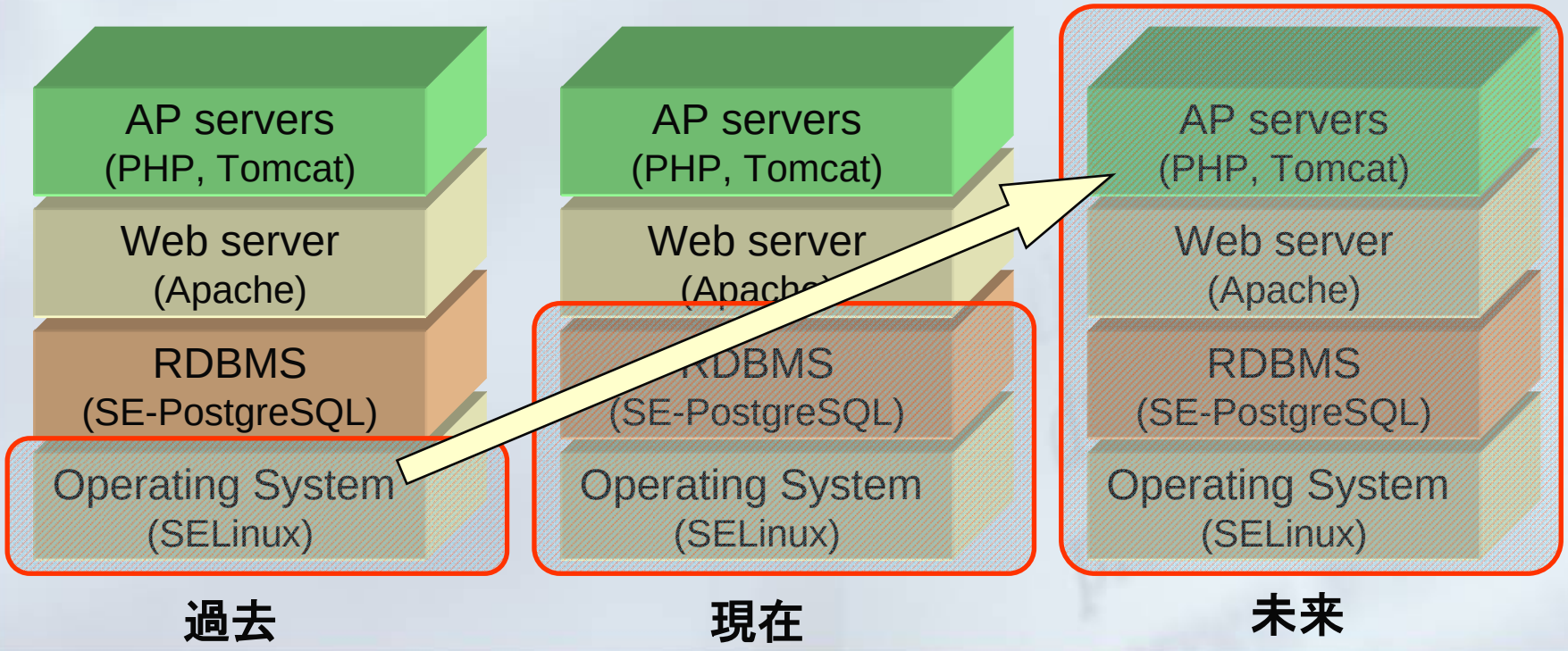
Web Application/SELinux連携

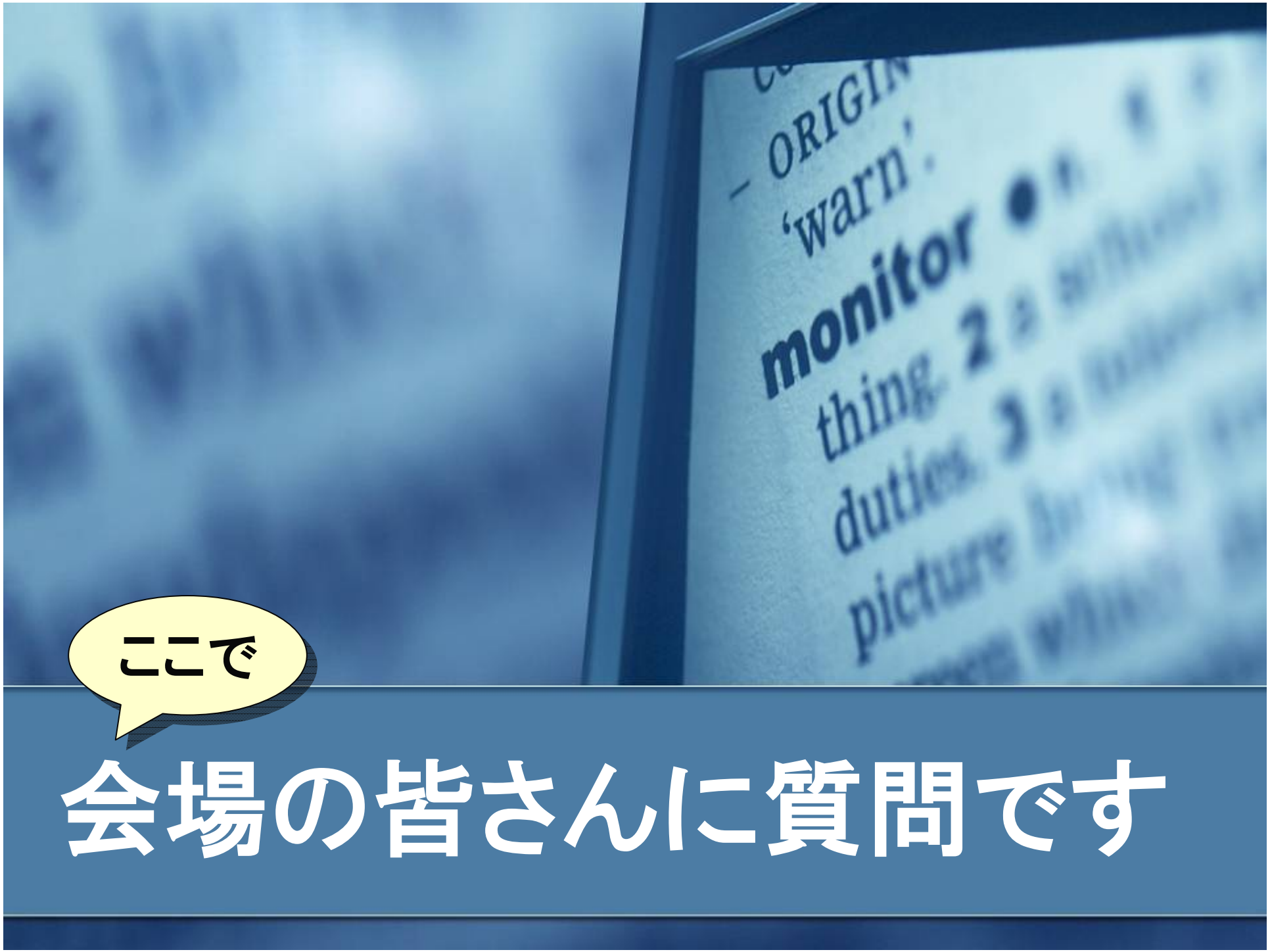
- 利用者が本質的に持っている権限
  ≠ ApacheがWeb Applicationを実行する際の権限
- 利用者に応じて、コンテンツハンドラの権限を切り替える
- 課題： マルチスレッド、KeepAlive
  - 解決策： Bounds Type、One time thread



LAPP/SELinuxと、将来の方向性

- SELinuxでソフトウェアスタック全体をカバー
  - アクセス制御の一貫性、網羅性を担保
- LAPP/SELinux
  - OS(SELinux) + DBMS(SE-PostgreSQL) + Web/AP (Apache/SELinux)





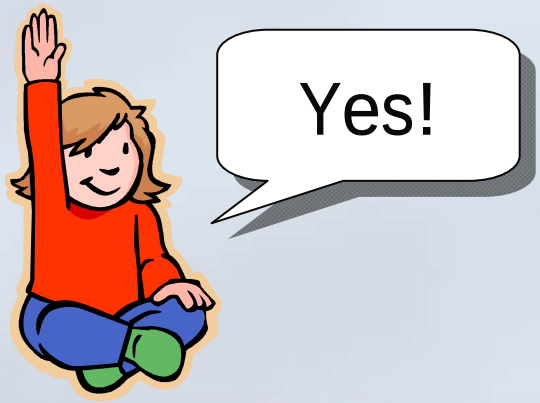
ここで

会場の皆さんに質問です

質問／挙手で回答してください

質問

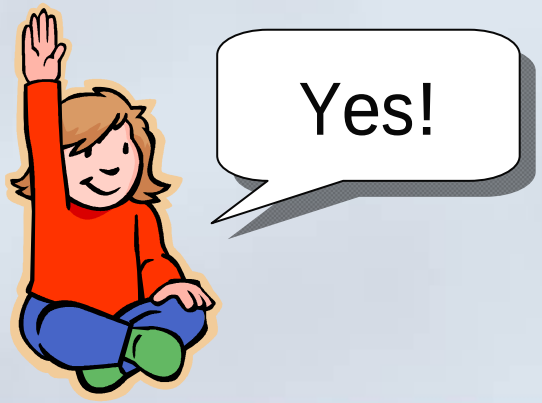
SELinux という名前を聞いた事がある



質問／挙手で回答してください

質問

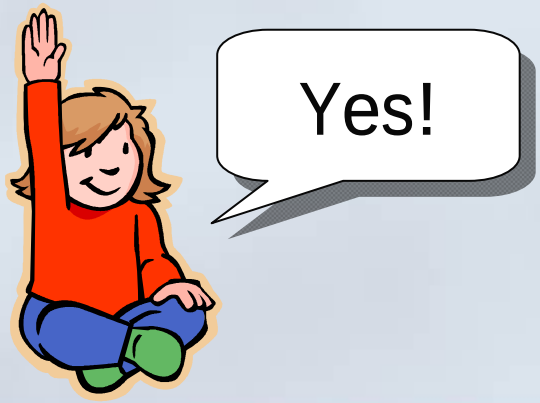
TOMOYO Linux **という名前を聞いた事がある**



質問／挙手で回答してください

質問

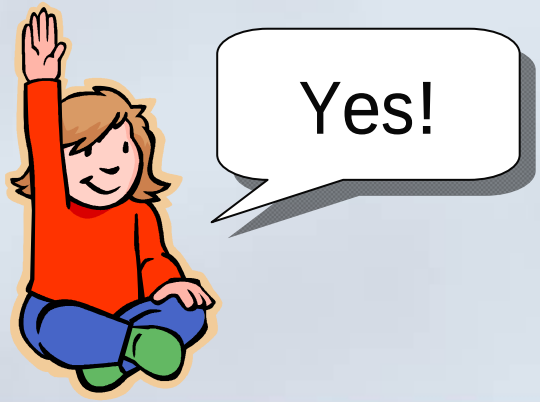
AppArmor という名前を
聞いた事がある



質問／挙手で回答してください

質問

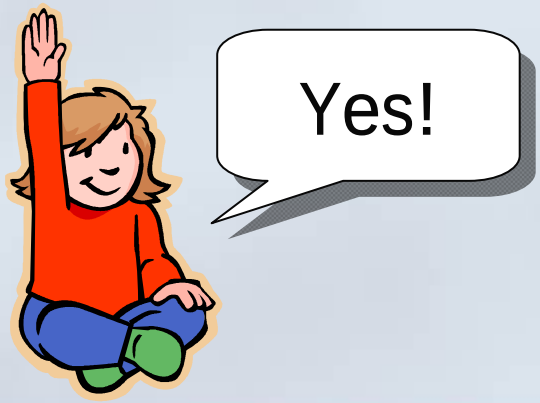
Smack という名前を聞いた事がある



質問／挙手で回答してください

質問

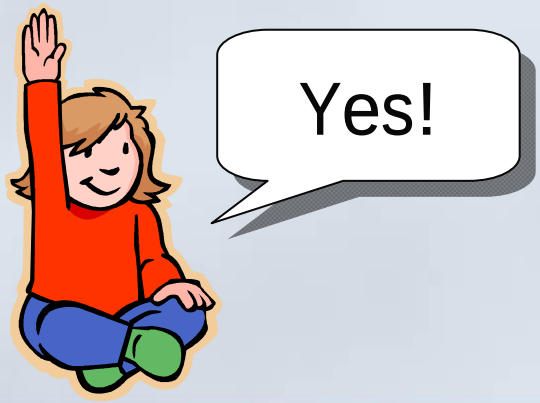
LIDS という名前を聞いた事がある



質問／挙手で回答してください

質問

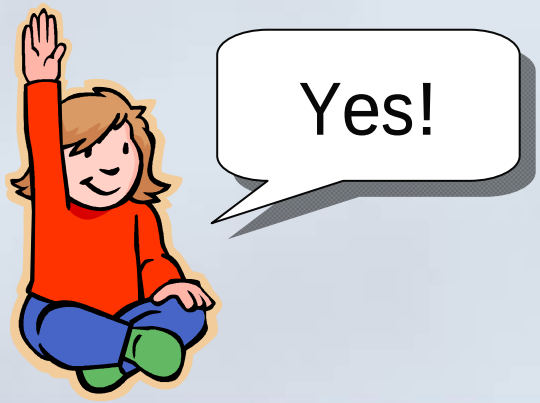
何かセキュアOSを使ったことがある



質問／挙手で回答してください

質問

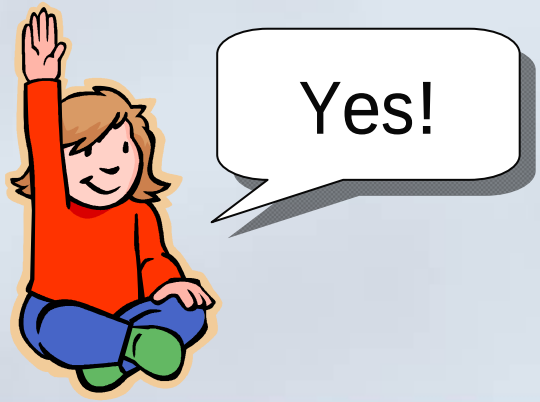
今も自分のマシンでは
セキュアOSが動作している



質問／挙手で回答してください

質問

何かセキュアOSを使ったことがある

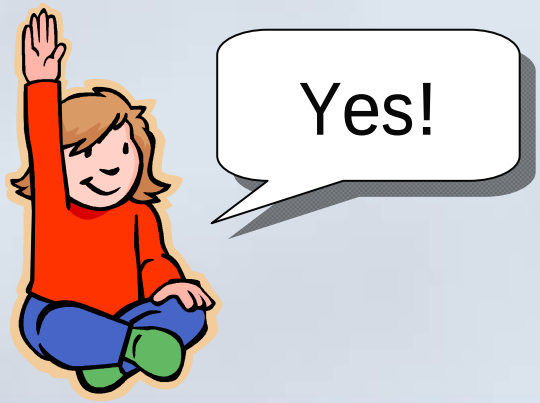


質問／挙手で回答してください

質問

俺にとってセキュアOSの印象は：

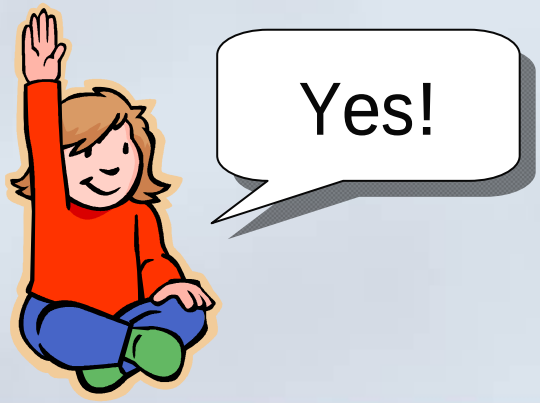
”難しい”



質問／挙手で回答してください

質問

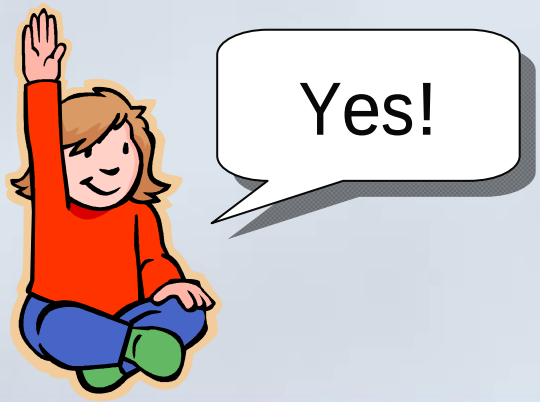
俺にとってセキュアOSの印象は：
”トラブルメーカー”



質問／挙手で回答してください

質問

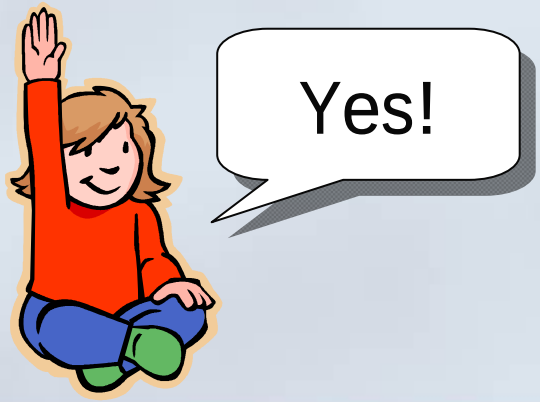
セキュアOSが原因(or 疑わしい)で、何かトラブルが発生した事がある



質問／挙手で回答してください

質問

俺にとってセキュアOSの印象は：
”怖い”

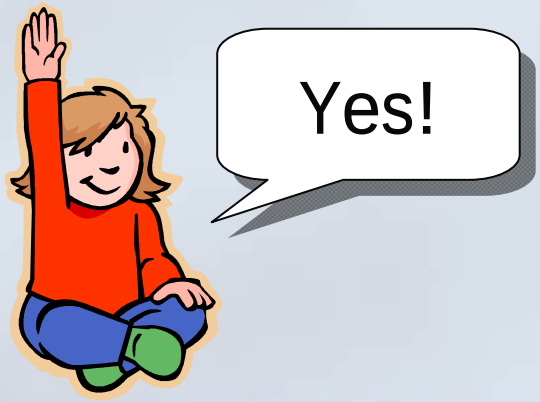


質問／挙手で回答してください

質問

俺にとってセキュアOSの印象は：

”頼りになる”

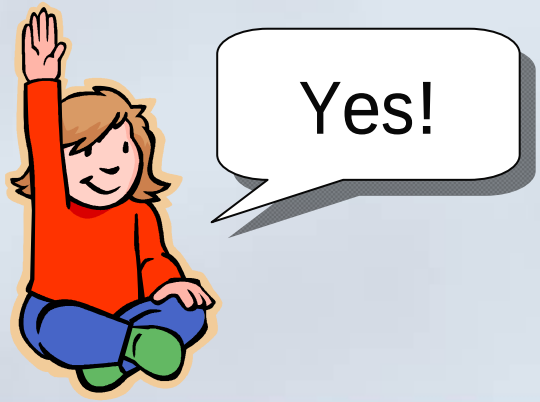


質問／挙手で回答してください

質問

俺にとってセキュアOSの印象は：

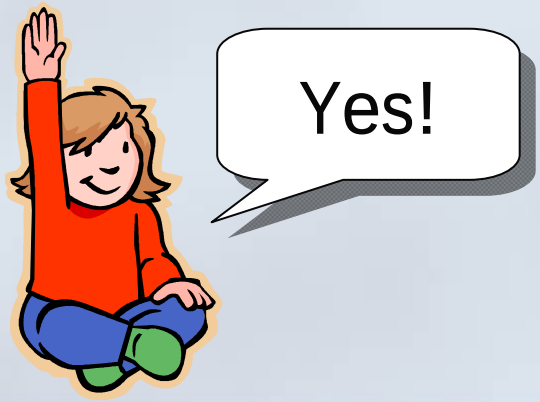
”その他”



質問／挙手で回答してください

質問

セキュアOSは必要だと思う



Open Discussion

テーマ

セキュアOSのメリット

Open Discussion

テーマ

セキュアOSの課題

Open Discussion

テーマ

青年の主張

- **日本セキュアOSユーザ会のご紹介**
  - SELinux, TOMOYO Linux, LIDS, AppArmor 等々...
    セキュアOS全般に関心のある開発者/利用者のグループ
  - **活動内容**
    - **ユーザ会MLの運営**

      users-ml@secureos.jp
      登録は http://lists.sourceforge.jp/mailman/listinfo/jsosug-users
    - **Webサイトの運営**

      http://www.secureos.jp/
    - **各種イベント/セミナー/勉強会**
    - **開発プロジェクト**
      - busyboxへのSELinuxコマンド移植PJ

TOMOYO Linux 1.6.x の素敵な機能

- 実行時の引数/環境変数のチェック
- 接続元IPアドレスに基づく権限分割

実行時の引数/環境変数のチェック

```
<kernel> /usr/sbin/httpd
allow_execute /bin/sh if exec.argc=3 exec.argv[1]=”-c”
                                    exec.argv[2]=”/usr/sbin/sendmail”
```

- この /usr/sbin/httpd は、以下の3つの条件を満たした場合のみ /bin/sh を実行できる。
  - 引数の数が3個
  - 第1引数が -c
  - 第2引数が /usr/sbin/sendmail
- この /bin/sh は「メール送信専用のシェル」であるため、Apache や CGI にセキュリティホールがあったとしても「自由に操作可能なシェル」が実行されることは無い。

実行時の引数/環境変数のチェック

```
<kernel> /usr/sbin/httpd
execute_handler /usr/bin/check-cgi-exec-param
```

- 標準入力や他の条件もチェックしたい場合、外部プログラムを利用できる。
  - プロセスが要求したプログラムの代わりに、ポリシーで指定されたプログラムが実行される
  - ポリシーで指定されたプログラムは、要求されたプログラムのパラメータ（引数/環境変数/標準入出力等）が適切な場合にのみ、要求されたプログラムを実行する
- 応用例
  - OSコマンドインジェクション対策
  - 通信内容のチェック（スパムフィルタ）

接続元IPアドレスに基づく権限分割

```
<kernel> /usr/sbin/sshd
allow_network TCP accept @LAN 1024-65535 ; set task.state[0]=1
allow_network TCP accept @WAN 1024-65535 ; set task.state[0]=0
allow_execute /bin/bash if task.state[0]=1
allow_execute /bin/rbash if task.state[0]=0
```

- この /usr/sbin/sshd は、@LAN に含まれるIPアドレスから接続してきた場合には /bin/bash の実行を、@WAN に含まれるIPアドレスから接続してきた場合には /bin/rbash の実行を許可する。
  - 他にも、sshログインしたユーザのUID/GIDなどに基づきアクセス許可の内容を制限することも可能。
- 応用例
  - 管理者用コマンドを実行できるクライアントの制限

ありがとうございました

商標

- TOMOYOは株式会社NTTデータの登録商標です。
- LinuxはLinus Torvalds氏の日本およびその他の国における登録商標または商標です。
- ターボリナックスおよびTurbolinuxは、ターボリナックス株式会社の商標または登録商標です。
- MandrivaはMandriva社の商標または登録商標です。
- その他、記載された会社名および製品名などは該当する各社の商標または登録商標です。