LIDS の新機能紹介

LIDS Development Team

面　和毅

目次

- LIDS とは何か
- LIDS の導入方法
- LIDS の諸機能
  - 基本的な機能
    - root に対するアクセス制限
  - lids-2.2.3 での新機能
    - syslogd の保護
    - TPE/TDE
    - NFMARK と iptables/iproute2 の連係
    - LIDS_EXEC

LIDS とは何か

LIDS とは何か

LIDS(Linux Intrusion Detection System)

- Linux 用のフリーのセキュア OS モジュール
  - Huagang Xie 氏作 (1999 年 10 月に公開)
- LIDS 1 系列 (2.4 カーネル)/LIDS 2 系列 (2.6 カーネル)
- Mandantory Access Control(MAC: 強制アクセス制御) と
  最小特権を提供
- inode ベースで ACL を管理 (利点と不利点)

メンテナ

LIDS-1: Yusuf Wilajati Purna

LIDS-2: Huagang XIE

Purna 氏からコメント

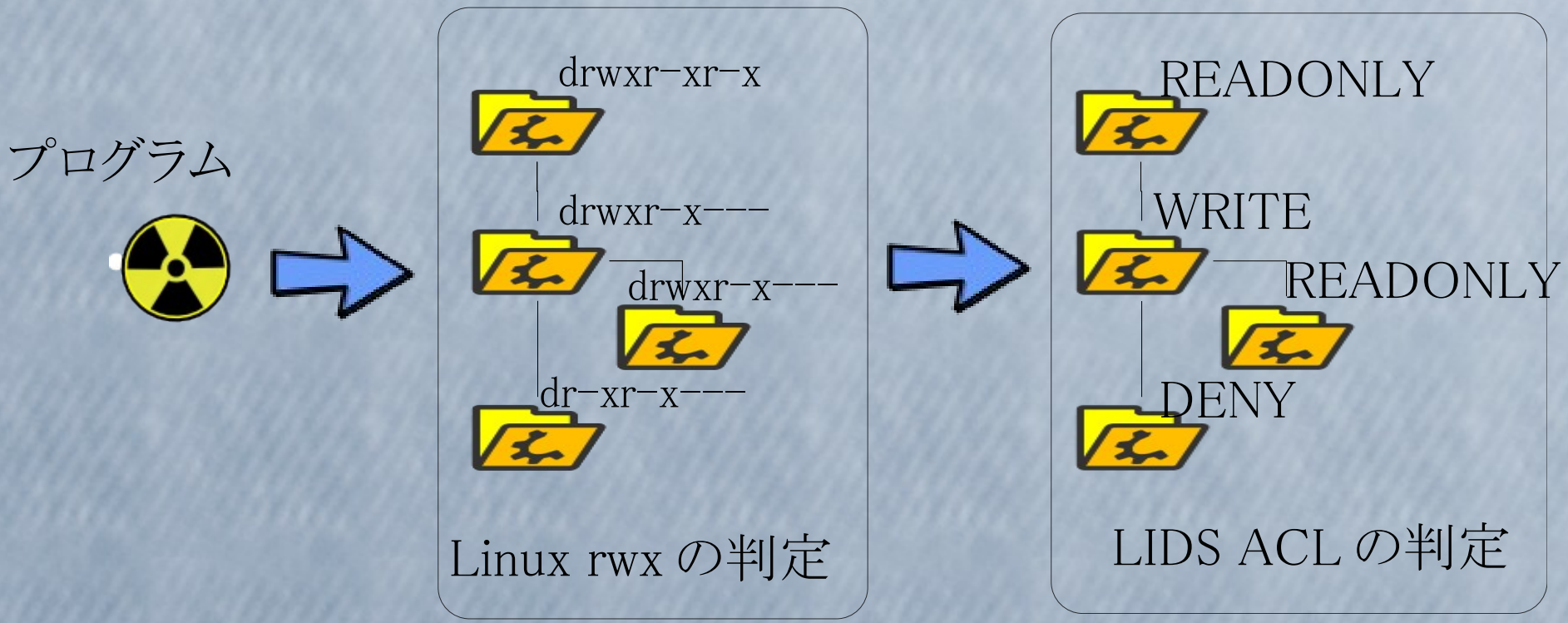
My comment to the CE makers is to encourage them to open their modified

source code to public as soon as possible.

Please say hello to Sony engineers, such as Tim Bird, Geoffrey, Machida-san, Wakamatsu-san, etc.

LIDS を導入すると

通常の Linux の権限がチェックされた後に、
もう一度 LIDS での権限がチェックされる



例えば


/var
READONLY
/root
WRITE
.bashrc
READONLY
/etc
DENY
LIDS ACL の判定

ACL の作り方

lidsconfコマンドで作成

- ファイルに対するデフォルトACL

lidsconf -A -o /var -j READONLY

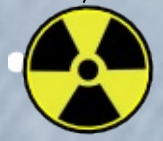
lidsconf -A -o /root -j WRITE

lidsconf -A -o /root/.bashrc -j READONLY

lidsconf -A -o /etc -j DENY

例えば

/sbin/hogehoge



読みたい!!

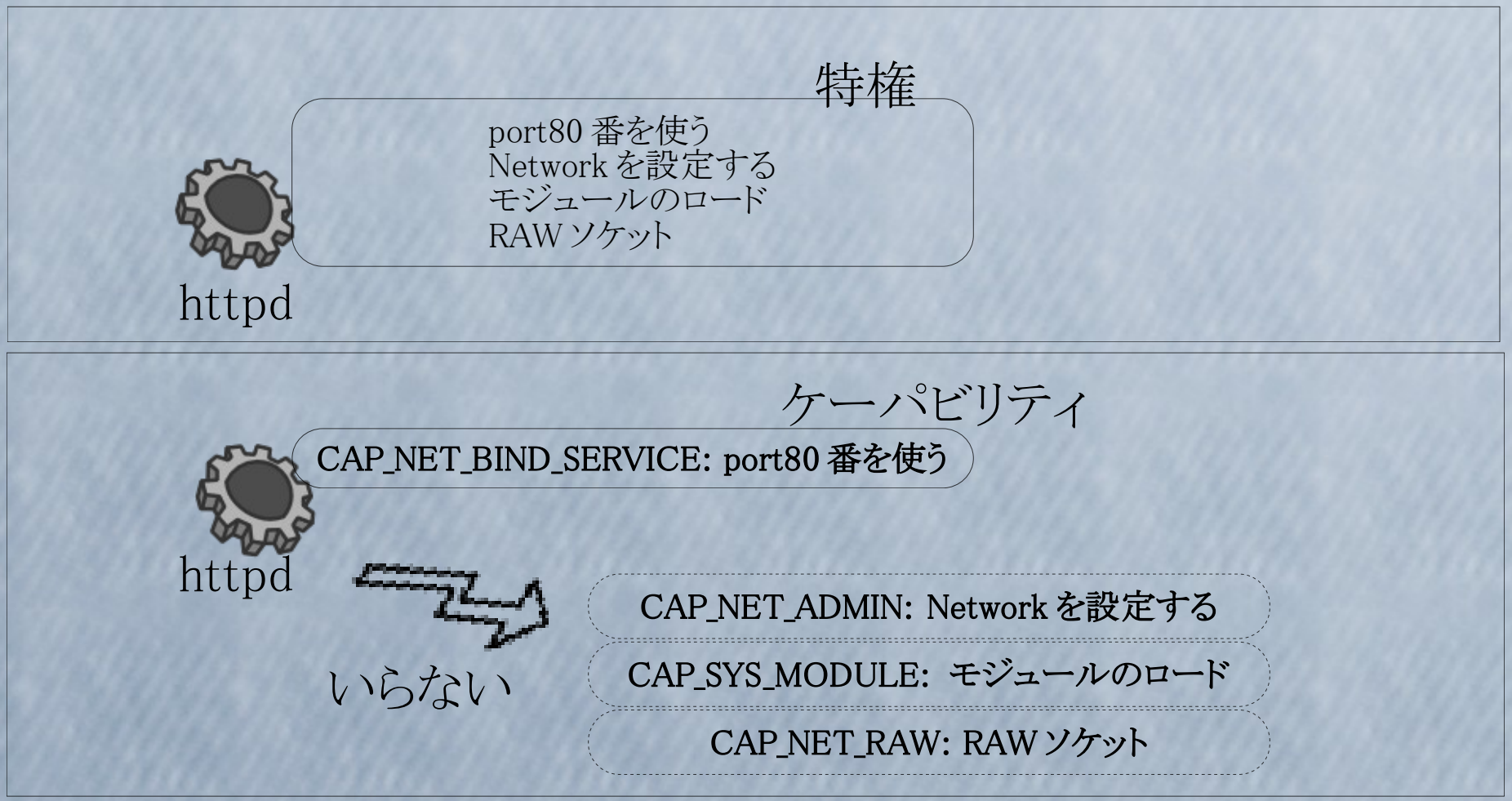
ACL の作り方

lidsconfコマンドで作成

- プログラムを指定した ACL

lidsconf -A -s /sbin/hogehoge -o /etc -j READONLY

ケーパビリティ



最小特権をケーパビリティ単位で実現している

ACLの作り方

lidsconfコマンドで作成

- ケーパビリティ

ケーパビリティバウンディングセットを作って、
その後、各プロセスに必要なケーパビリティを
加えていく

```
lidsconf -A -s /usr/sbin/httpd -o CAP_NET_BIND_SERVICE 80,443 -j GRANT
```

ACL の作り方

- ACL は BOOT/POSTBOOT/SHUTDOWN の3ステートに分けて記載が可能

起動時には /etc/mtab に書き込み出来る、など

柔軟な ACL を書ける

- ACL_DISCOVERY モード

SELinux の permissive みたいなもの。

このモードのログを参考に ACL を自動生成

する Perl スクリプトもある

LIDS の導入方法

LIDS の入手先

http://www.lids.org からダウンロード可能

2.6 カーネルは、lids-2.2.X-2.6.XX.tar.gz

2.4 カーネルは、lids-1.2.X-2.4.XX.tar.gz

それぞれ、下の2つが同梱されている

- カーネルにあてるパッチ

lids-2.2.X-2.6.XX.patch/lids-1.2.X-2.4.XX.patch

- LIDS の設定ツール

lidstools-XX(LIDS のバージョンに対応している lidstools を使う事)

LIDS のインストール方法

- パッチをあてて、カーネルを作り直す

（一番確実だが、面倒臭いという話も）

- RPM/Deb パッケージを使う

日本 SELinux ユーザ会 LIDS 支部では、

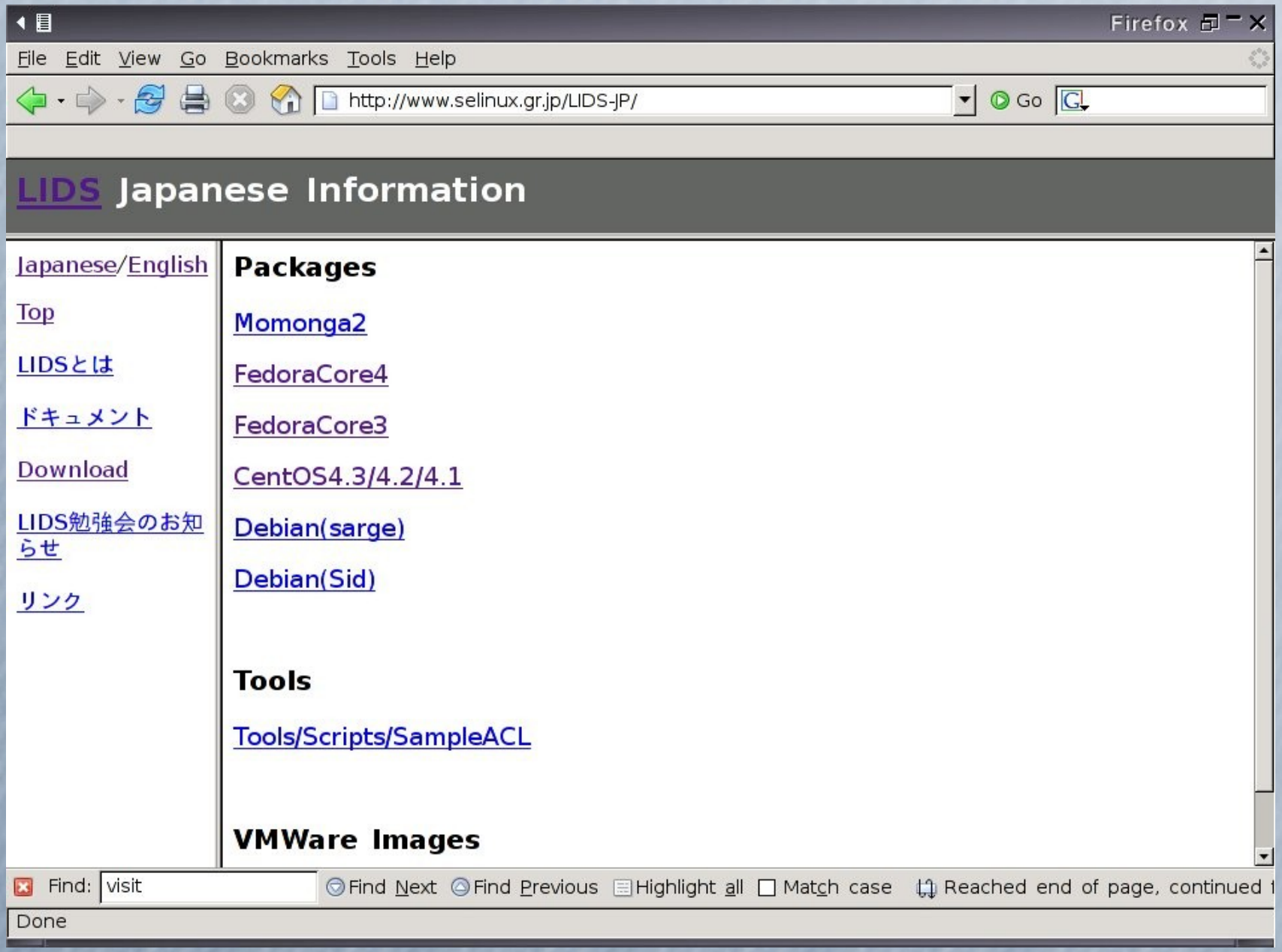
- FedoraCore3/4/5
- CentOS4
- Momonga
- Debian(sarge): vanilla kernel

を用意している

LIDS のインストール方法

- VMWare イメージのプレイマシンがあります
  - Debian(sarge) ベース
  - 基本的なパッケージしか入っていない
  - LIDS-1 系列 /LIDS-2 系列両方用意

LIDS パッケージ /VMWare イメージのダウンロード



lids-2.2.3 からの新機能

新機能 1

- Trusted Path Execution
-
- ACL で READONLY にされているファイルのみ
- 実行を許可
-

-> /home 以下を LIDS で書き込み可に
したとき個人宛てのメールに付いてきた
バイナリが不正に実行される事を抑制する

Trusted Path Execution とは

/bin/ls は READONLY で保護 -> 実行可能

/tmp は WRITE になっているので、

```
# cp -p /bin/ls /tmp/ls
```

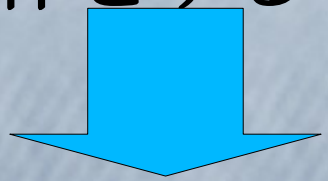
として、/tmp/ls を実行

-> TPE のエラーが出る。

新機能 3

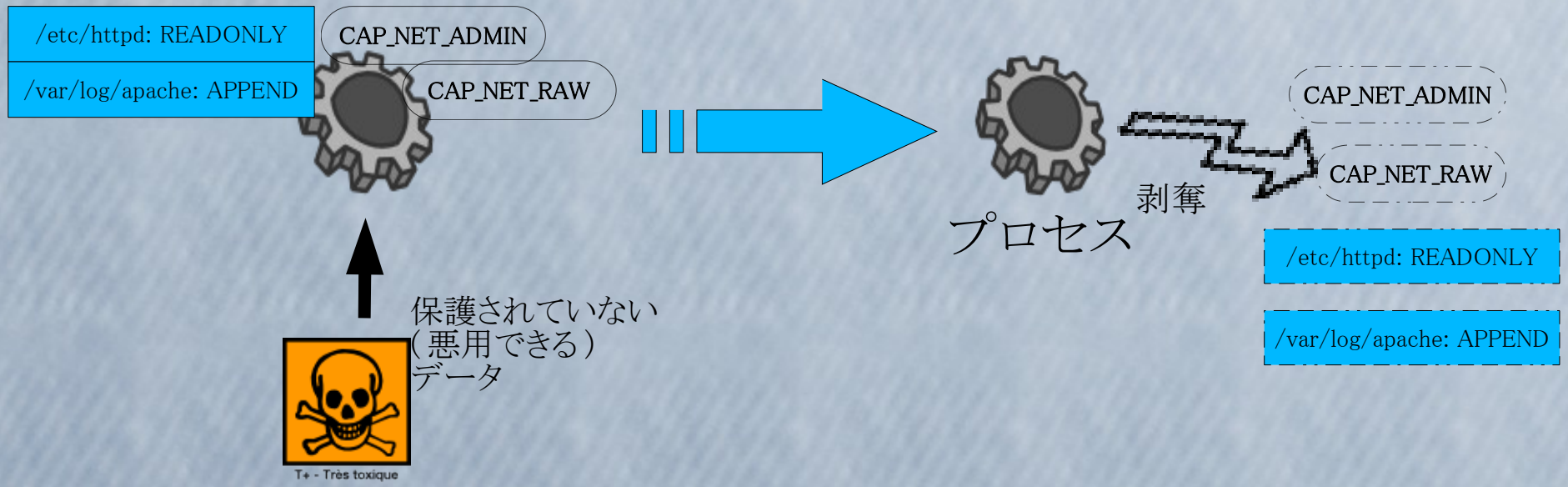
- Trusted Domain Enforcement
-

LIDS により保護されているバイナリでも、
不正な入力で異常動作をする可能性がある



- 保護されていない入力が与えられた場合
- ACL で与えられた権限が剥奪される！！

Trusted Domain Enforcement とは



例)
IP アドレスが列記されているファイルを指定されると、
そのファイルの IP アドレスに ping をうつ CGI スクリプト
(CAP_NET_RAW が与えられている)

1. /root/hosts は READONLY なので、ping が打てる
2. /var/tmp/hosts は WRITE なので、CAP_NET_RAW が剥奪される

新機能 3

NFMARK と iptables/iproute2 の連係

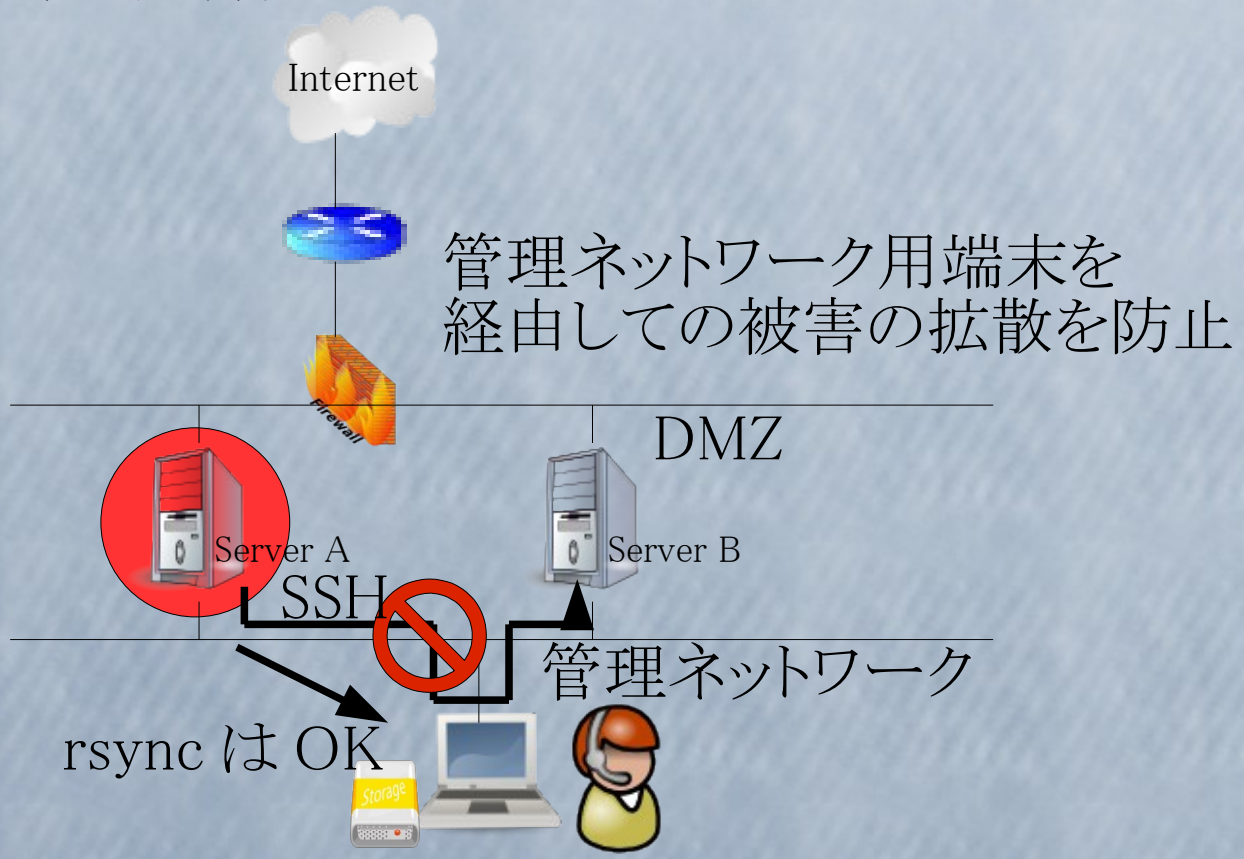
LIDS-2.2.3 では、NFMARK 機能をサポートしており、
特定のプロセスがソケットを生成した際に MARK フィールドに
MARK を付けることができる

-> iptables: mangle テーブルの「 MARK 」
iproute2: ip rule の「 fwmark 」

と連係させて、トラフィックを制御できる

新機能 3

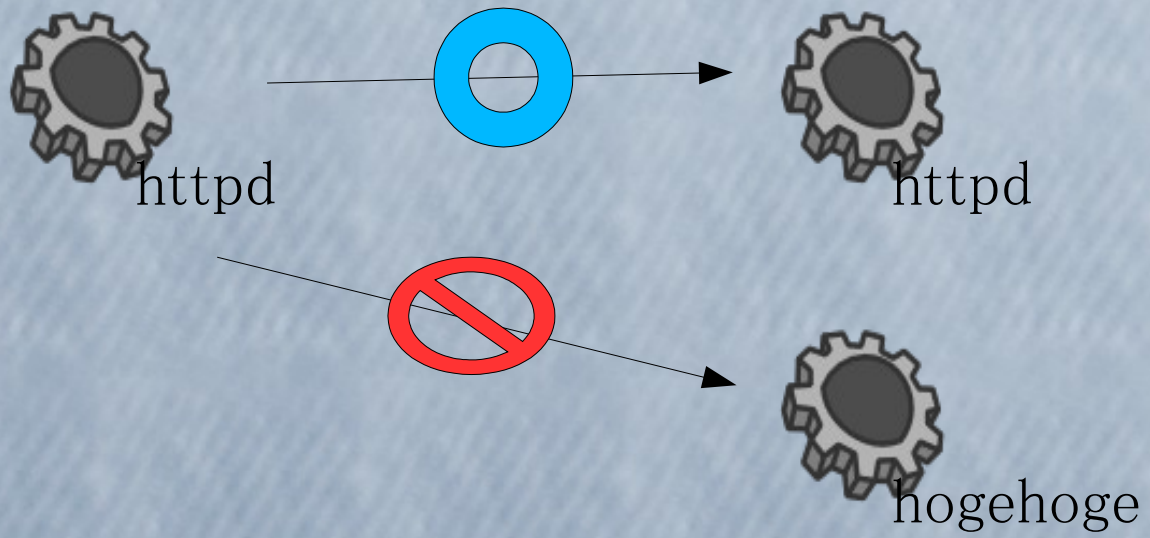
外部 (DMZ) に露出しているサーバを管理ネットワークからバックアップ／管理を行う際に、
万が一 DMZ に露出したサーバがクラックされたとしても、管理ネットワークを通して
その他のマシンに攻撃を展開していくことを防ぐ事が出来る



新機能 4

LIDS_EXEC

Lidsconf -A -s httpd -o LIDS_EXEC -j ENABLE



自分と同じプログラム（正確には同じ inode 番号）
の物しか、子供として起動できない

リリース予定

新バージョンリリース予定

2.2.3 は rc4 として 3 月上旬に出す予定

-> 2.2.3rc の最終版となる可能性が高い

その後、ドキュメントを整理して

LSM-ML 、LKM-ML に提出

（まあ、3月ぐらいを予定してボチボチと）

LIDS の情報

本家

http://www.lids.org

フォーラム

http://forum.lids.org

Wiki

http://wiki.artmis.com/index.php/Main_Page

ML

http://www.lids.org/maillist.html

LIDS の情報（日本語）

- 日本 SELinux ユーザ会 LIDS 支部

http://www.selinux.gr.jp/LIDS-JP/index.html

SoftwareDesign 2006 年 3 月号 -6 月号 (LIDS-JP 連載）

- @ IT 連載

http://www.atmarkit.co.jp/fsecurity/rensai/lids01/lids01.html

- Network World 6 月号 (LIDS TDE)
- ITPro SecureOS 連載

http://itpro.nikkeibp.co.jp/free/LIN/LIN_CONTENTS/20040706/2/

- 日経 Linux ムック

http://itpro.nikkeibp.co.jp/linux/extra/mook/mook10/index.shtml

- 日経 Linux 連載 (2005 年2月号 -9 月号）
- LinuxMagazine 2005 年 3 月号

御静聴ありがとうございました

LIDS-JP　面