security 101
技術編

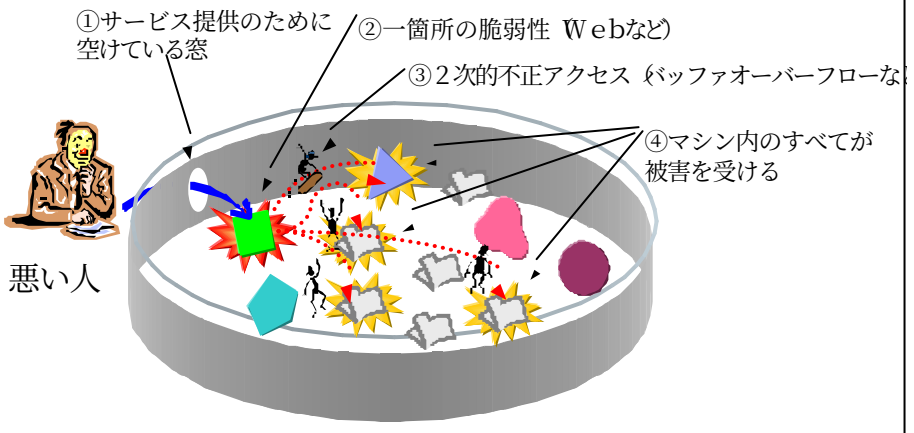
# hp Compartment Guard for Linux の紹介

日本ヒューレット・パッカード株式会社

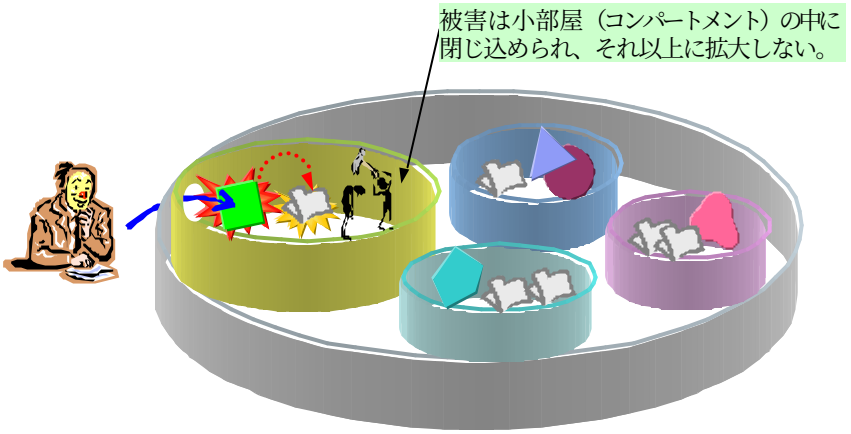
Slide 5

## OS自身がセキュリティ強化されていない場合

ひとたび、どこか（アプリケーションなど）の脆弱性に
つけこまれると、マシン全体が脅威にさらされてしまう。



## OS自身をセキュリティ強化している場合




Compartment Guard

## Compartment Guard for Linux による セキュリティ強化

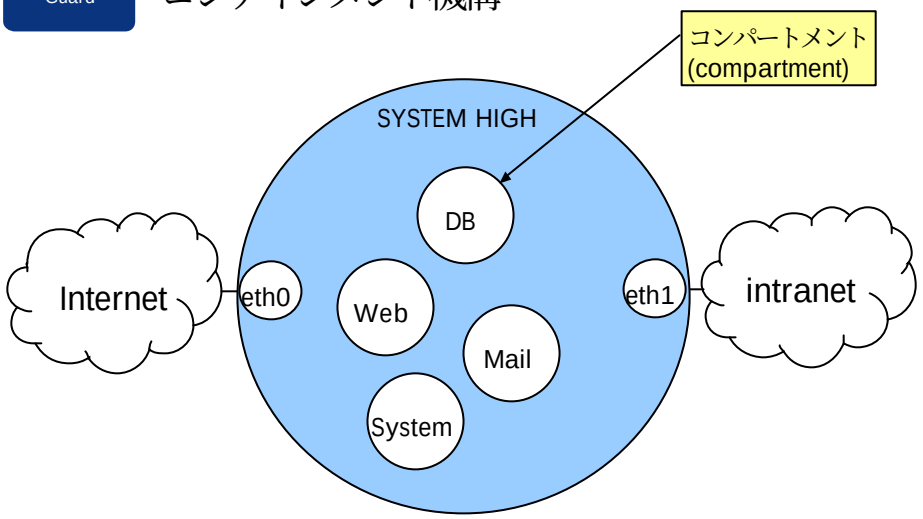
コンテインメント機構

すべてのプロセスをコンパートメントという区画に閉じ込める機構です。

Slide 10

Compartment Guard

## コンテインメント機構




Slide 11

Compartment Guard

## Compartment Guard for Linux による セキュリティ強化

コミュニケーション ガード機構

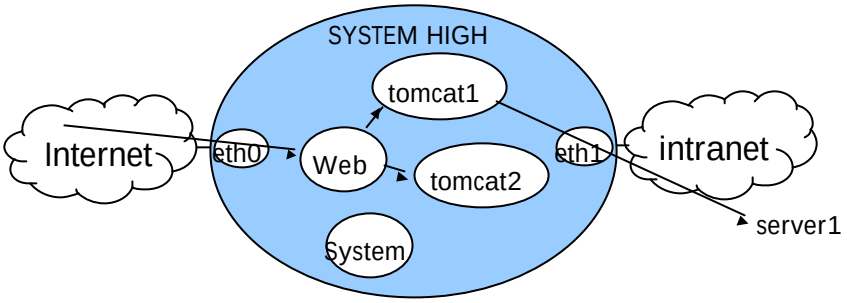
コンパートメント間、あるいは、
コンパートメントとネットワークの
通信を制限する機構です。

Slide 12

Compartment Guard

## コミュニケーション ガード機構

```
HOST * -> COMPARTMENT web PORT 80 METHOD tcp NETDEV lan_eth0
COMPARTMENT web -> COMPARTMENT tomcat1 PORT 8007 METHOD tcp NETDEV lan_lo
COMPARTMENT web -> COMPARTMENT tomcat2 PORT 8008 METHOD tcp NETDEV lan_lo
COMPARTMENT tomcat1 -> HOST server1 PORT 8080 METHOD tcp NETDEV lan_eth1
```




Slide 13

Compartment Guard

## Compartment Guard for Linux による セキュリティ強化

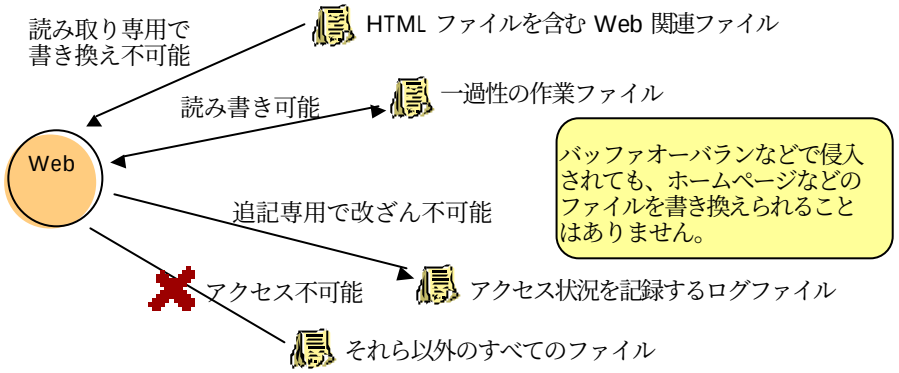
ファイル ガード機構

各コンパートメントから、ファイル システムに対するアクセスを 制限する機構です。

Slide 14

Compartment Guard

## ファイル ガード機構　(Web の具体例)

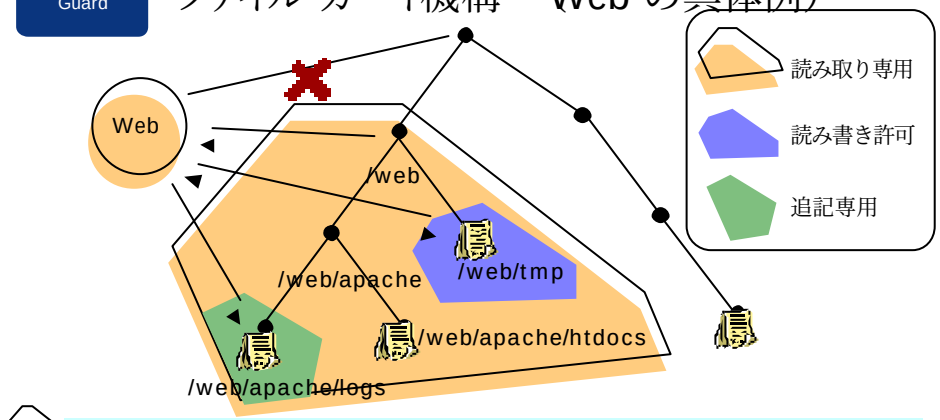



```
web /compt/web read active
web /compt/web/tmp read,write active
web /compt/web/apache/logs append active
web / none active
```

Slide 16

Compartment Guard

## ファイル ガード機構　(Web の具体例)




```
web /compt/web read active
web /compt/web/tmp read,write active
web /compt/web/apache/logs append active
web / none active
```

Slide 17

Compartment Guard

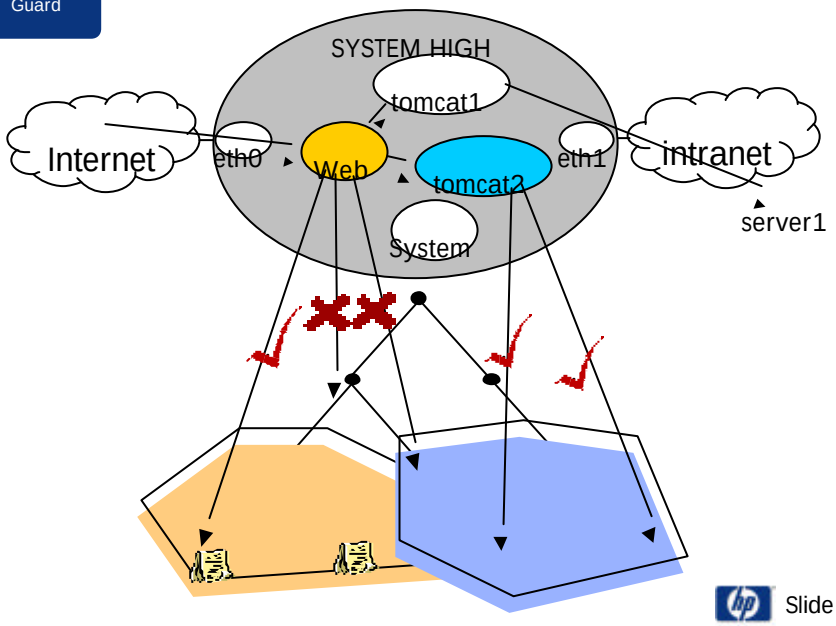
## Compartment Guard for Linux による セキュリティ強化

コミュニケーション ガード機能と
ファイル ガード機能を
柔軟に組み合わせることで、
あらゆるアプリケーションに
対応することができます。

Slide 18

Compartment Guard

## コミュニケーション ガードとファイル ガード

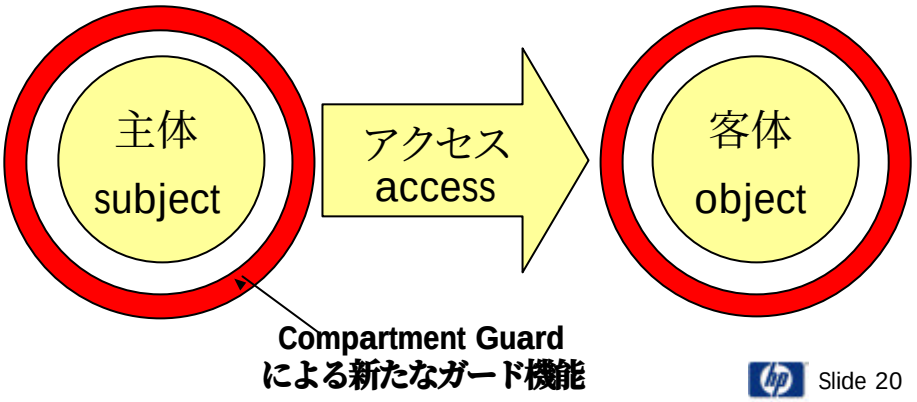



Slide 19

Compartment Guard

## 情報セキュリティ対策とは？

主体が客体にアクセスする上での
機密性、完全性、可用性を守ること




Slide 20

Compartment Guard

## Compartment Guard for Linux による セキュリティ強化

sticky ガード機構

プロセスの sticky ビットを無効化する
ことのできる機構です。

Slide 21

Compartment Guard

## Compartment Guard for Linux による セキュリティ強化

### モジュールロード・ガード機構

Linux kernel のロードを制限する ことのできる機構です。

Slide 22

Compartment Guard

## Compartment Guard for Linux による セキュリティ強化

### イベントログ機構

ルールの許可・不許可などのログを 記録する機構です。

### アラーム機構

特定のイベントに対して、自動的に アクションをする機構です。

Slide 23

Compartment Guard

Compartment Guard for Linux による
セキュリティ強化

## pass through モード

コミュニケーションガード機構や
ファイルガード機構などのガード機構の
アクセス制限を内部処理しながら、
アクセスの抑止だけを解除するモードです。

Slide 24

Compartment Guard

Compartment Guard for Linux による
セキュリティ強化

## privilege ガード機構

各種ガード機構の管理権限を以下のように守る機構です。

- 最少特権
- Trusted Chain

Linux 標準の CAPABILITY によって実現しています。

Slide 25

Compartment Guard

## Compartment Guard for Linux による セキュリティ強化

### アプライアンス・プロテクション機構

システム管理者がルール変更を
できないようにする機構です。

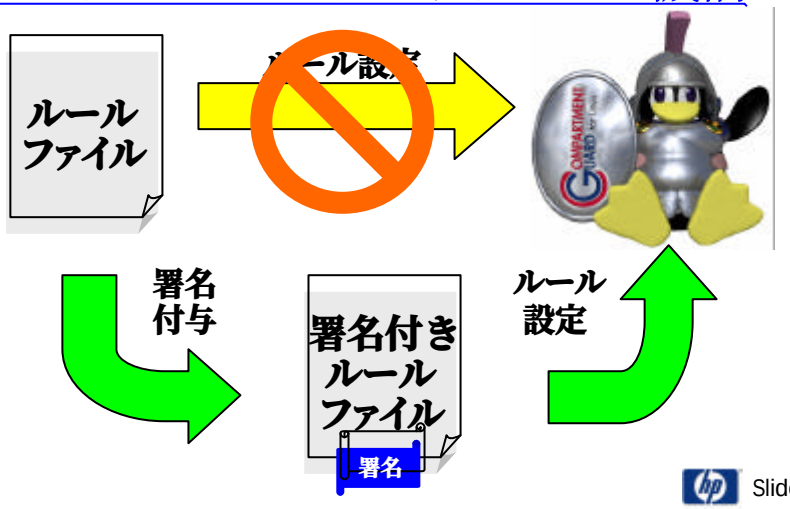
各お客様ごとに提供する専用ツールで
作成した署名付きルールファイルだけを
システムに適用できます。

Slide 26

Compartment Guard

## Compartment Guard for Linux による セキュリティ強化

### アプライアンス・プロテクション機構




Slide 27

Compartment Guard

## Compartment Guard for Linux による セキュリティ強化

アプライアンス・プロテクション機構

アプライアンス製品ベンダー様向け

アプリケーション・ソフトベンダー様向け

システム管理者様向け
操作制限端末の提供

Slide 28

Compartment Guard

## Compartment Guard for Linux の特長

安い　定価15万円／CPU

早い

簡単

Slide 29

Compartment Guard

## Compartment Guard for Linux の構成

DLKM (Dynamic Loadable Kernel Module)

RedHat AS ディストリビューションに
アドオンしてお使いいただく製品です。


Slide 30

Compartment Guard

## Compartment Guard for Linux の構成

standard boot モード

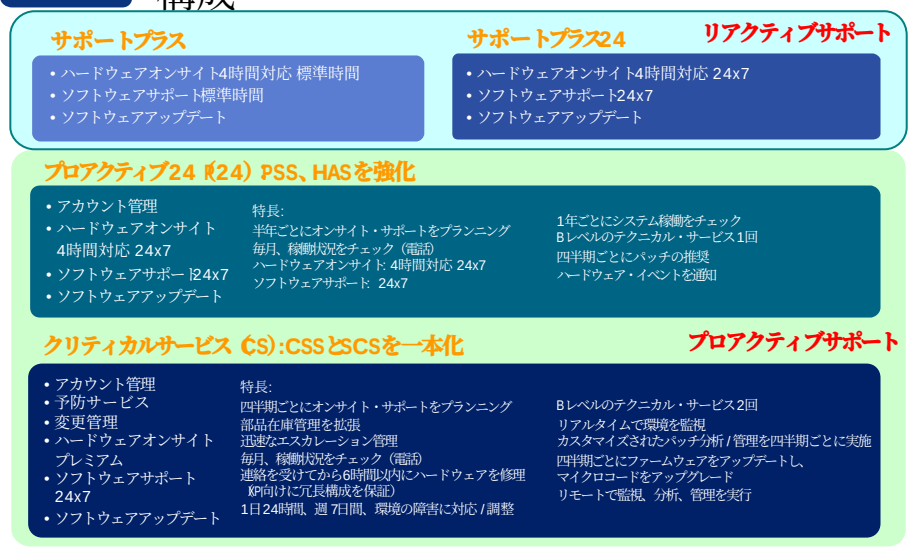
Compartment Guard for Linux の
モジュールをすべてインストールした
状態で、すべての機構を停止して
標準OSと同じ動作をさせるモードです。

障害時の切り分けに使います。

Slide 31

Compartment Guard

## Compartment Guard for Linux の構成




Slide 32

Compartment Guard

## Compartment Guard for Linux の特長

安い　定価 15万円／CPU

早い　国産製品

簡単

Slide 33

Compartment Guard

## Compartment Guard for Linux の リリース ポリシー

### バージョンアップ セーフ ポリシー

Compartment Guard for Linux の
バージョンアップをする場合に、現行
システムの設定情報をすべて継承
することを将来的に約束します。

Slide 34

Compartment Guard

## Compartment Guard for Linux の特長

安い　定価 15万円／CPU

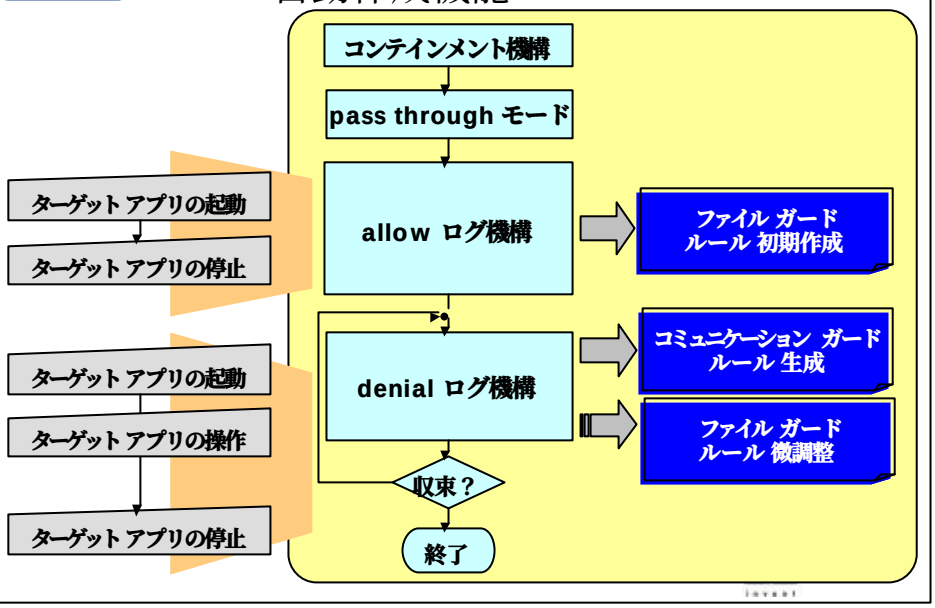
早い　国産製品

簡単　単純なコンセプト

Slide 35

Compartment Guard

## Compartment Guard for Linux の ルール自動作成機能




invent