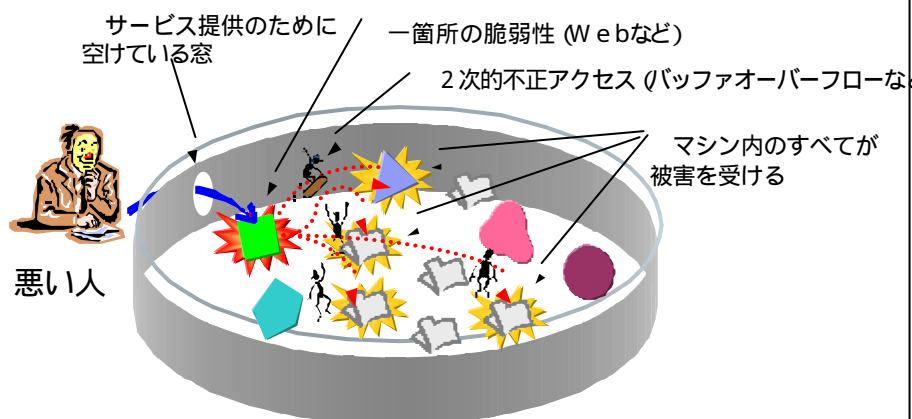


hp Compartment Guard for Linux の紹介

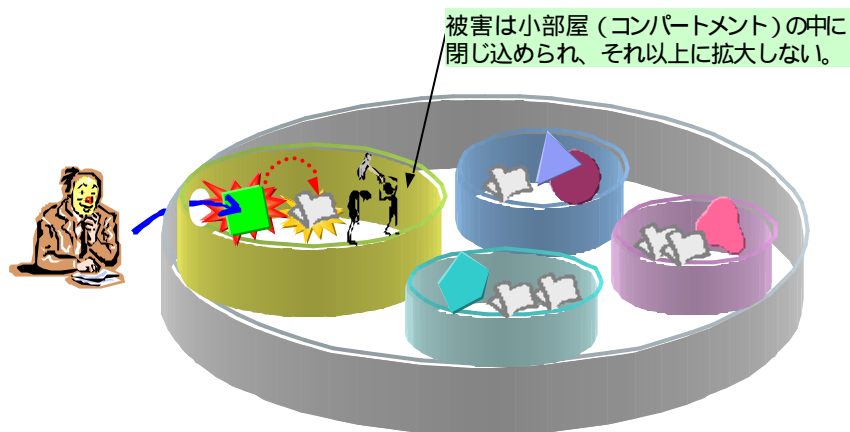
日本ヒューレット・パカード株式会社

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

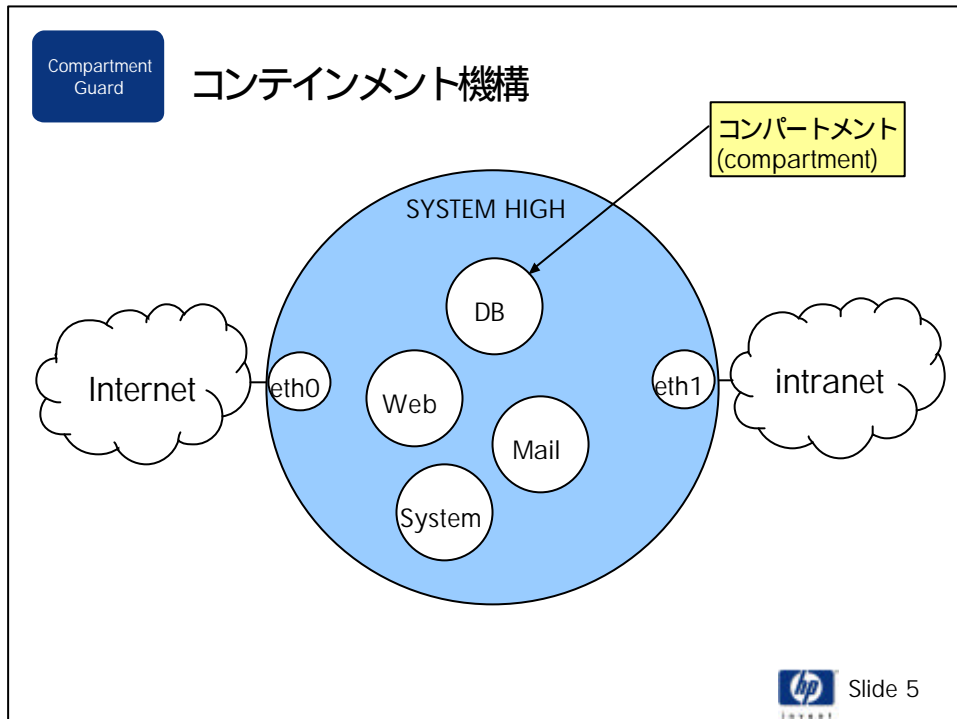


Compartment
Guard

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。



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 ガート機構

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。

hp Slide 6

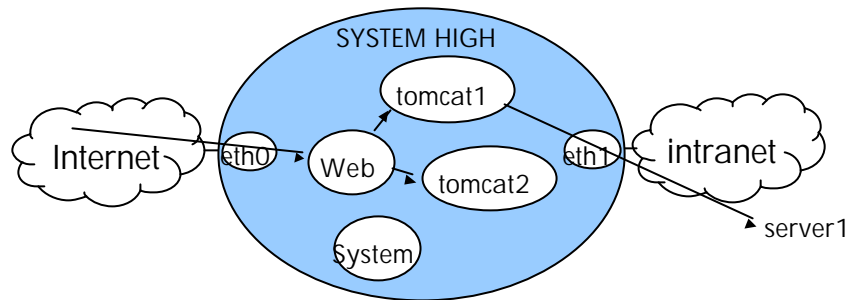
コミュニケーション ガート機構

```
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
```

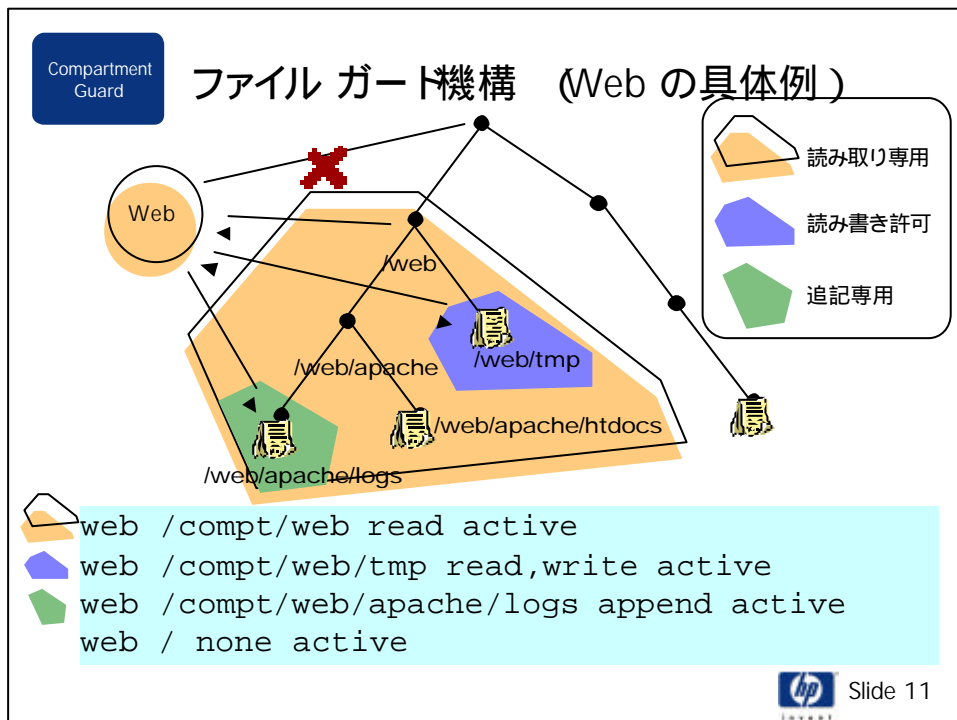
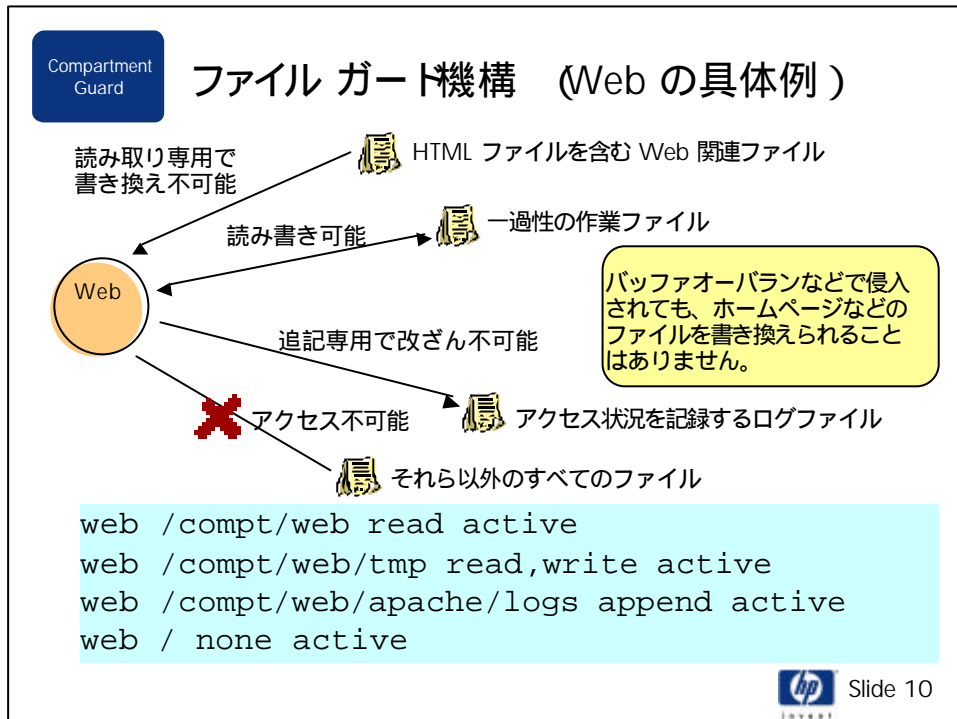
```
COMPARTMENT tomcat1 -> HOST server1 PORT 8080 METHOD tcp NETDEV lan_eth1
```



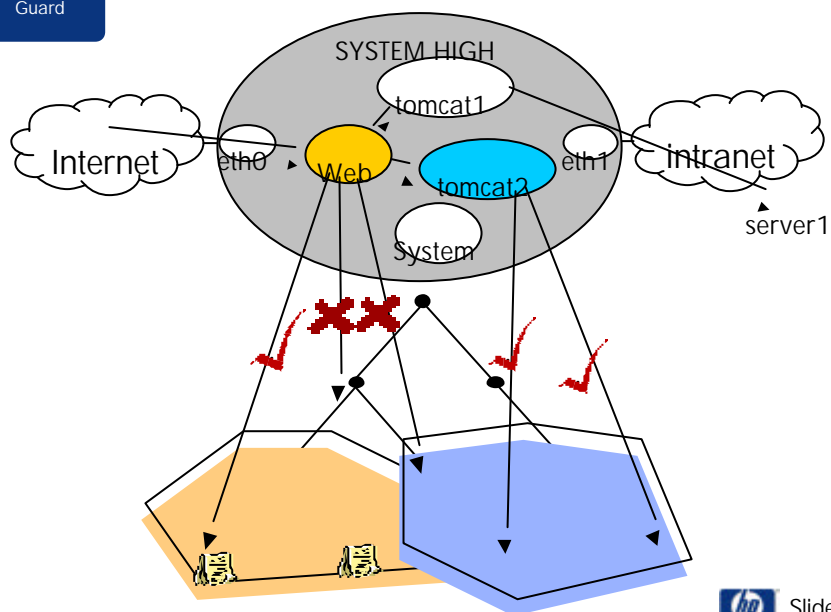
Compartment Guard for Linux による セキュリティ強化

ファイル ガート機構

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。

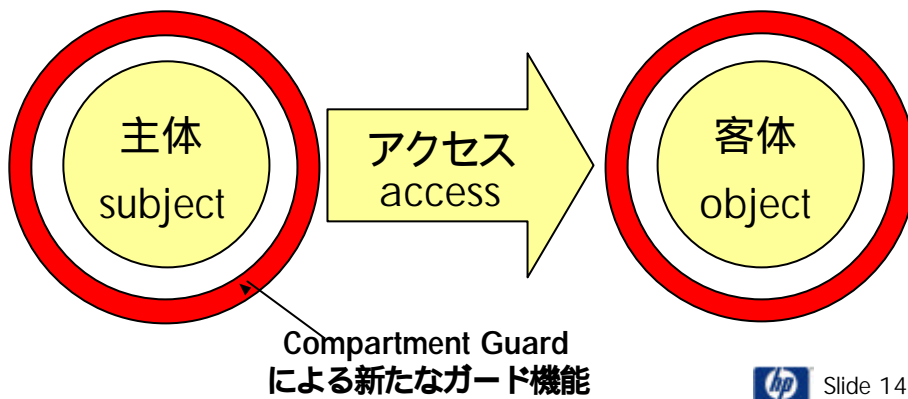


コミュニケーション ガード機能と
ファイル ガード機能を
柔軟に組み合わせることで、
あらゆるアプリケーションに
対応することができます。



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



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。

signal ガート機構

プロセスに対する signal 送信を無効化
することのできる機構です。
重要な監視デーモンなど、他のプロセス
を kill できなくすることができます。



モジュールロード・ガート機構

Linux kernel のロードを制限する
ことのできる機構です。



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。



pass through モード

コミュニケーションガート機構や
ファイルガート機構などのガート機構の
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。



privilege ガート機構

各種ガート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。



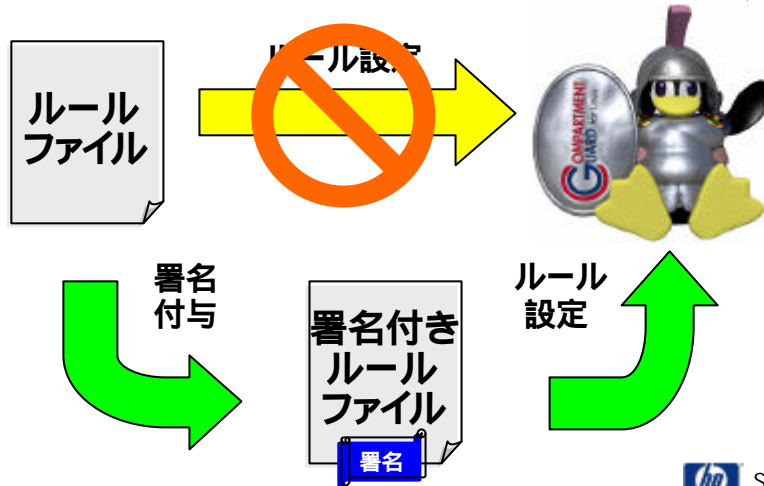
アプライアンス・プロテクション機構

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。



アプライアンス・プロテクション機構



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

Compartment
Guard

Compartment Guard for Linux の特長

安い 定価 15万円 / CPU

早い

簡単



Slide 24

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。



HP Service Guard/LX



Slide 25

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用します。



Compartment Guard for Linux の構成

サポートプラス

- ハードウェアオンサイト4時間対応 標準時間
- ソフトウェアサポート標準時間
- ソフトウェアアップデート

サポートプラス24

- ハードウェアオンサイト4時間対応 24x7
- ソフトウェアサポート24x7
- ソフトウェアアップデート

リアクティブサポート

プロアクティブ24 (P24) PSS、HASを強化

- アカウント管理
- ハードウェアオンサイト4時間対応 24x7
- ソフトウェアサポート24x7
- ソフトウェアアップデート

特長:
半年ごとにオンサイト・サポートをプランニング
毎月、稼働状況をチェック(電話)
ハードウェアオンサイト 4時間対応 24x7
ソフトウェアサポート 24x7

1年ごとにシステム稼働をチェック
Bレベルのテクニカル・サービス1回
四半期ごとにバッチの推奨
ハードウェア・イベントを通知

クリティカルサービス (CS) CSSとSCSを一本化

- アカウント管理
- 予防サービス
- 変更管理
- ハードウェアオンサイトプレミアム
- ソフトウェアサポート24x7
- ソフトウェアアップデート

特長:
四半期ごとにオンサイト・サポートをプランニング
部品在庫管理を拡張
迅速なエスカレーション管理
毎月、稼働状況をチェック(電話)
連絡を受けてから6時間以内にハードウェアを修理(99%向けに冗長構成を保証)
1日24時間、週7日間、環境の障害に対応/調整

プロアクティブサポート

Bレベルのテクニカル・サービス2回
リアルタイムで環境を監視
カスタマイズされたバッチ分析/管理を四半期ごとに実施
四半期ごとにファームウェアをアップデートし、マイクロコードをアップグレード
リモートで監視、分析、管理を実行



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 28

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。

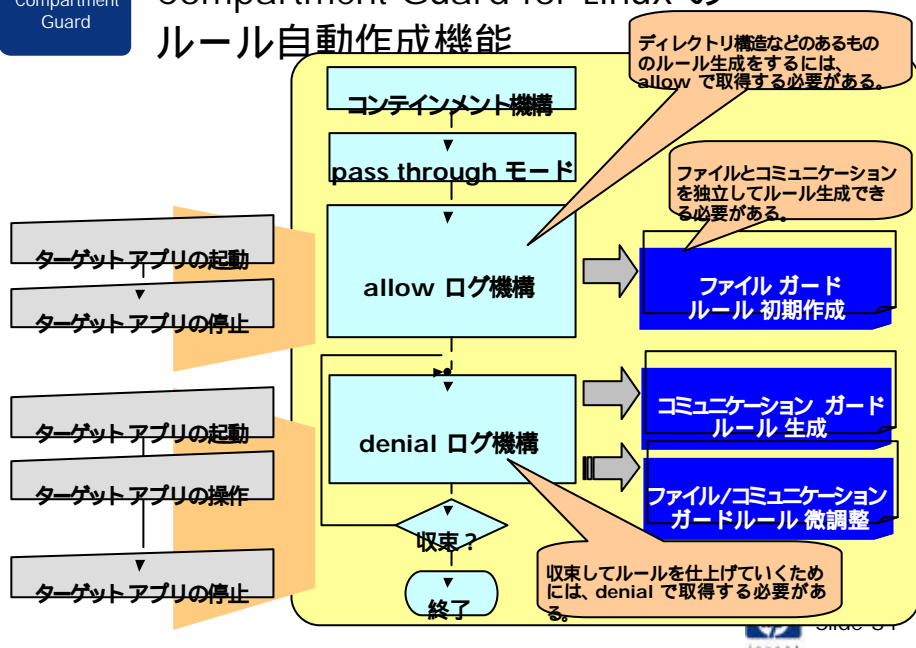


Slide 29

安い 定価 15万円 / CPU

早い 国産製品

簡単 単純なコンセプト





i n v e n t