



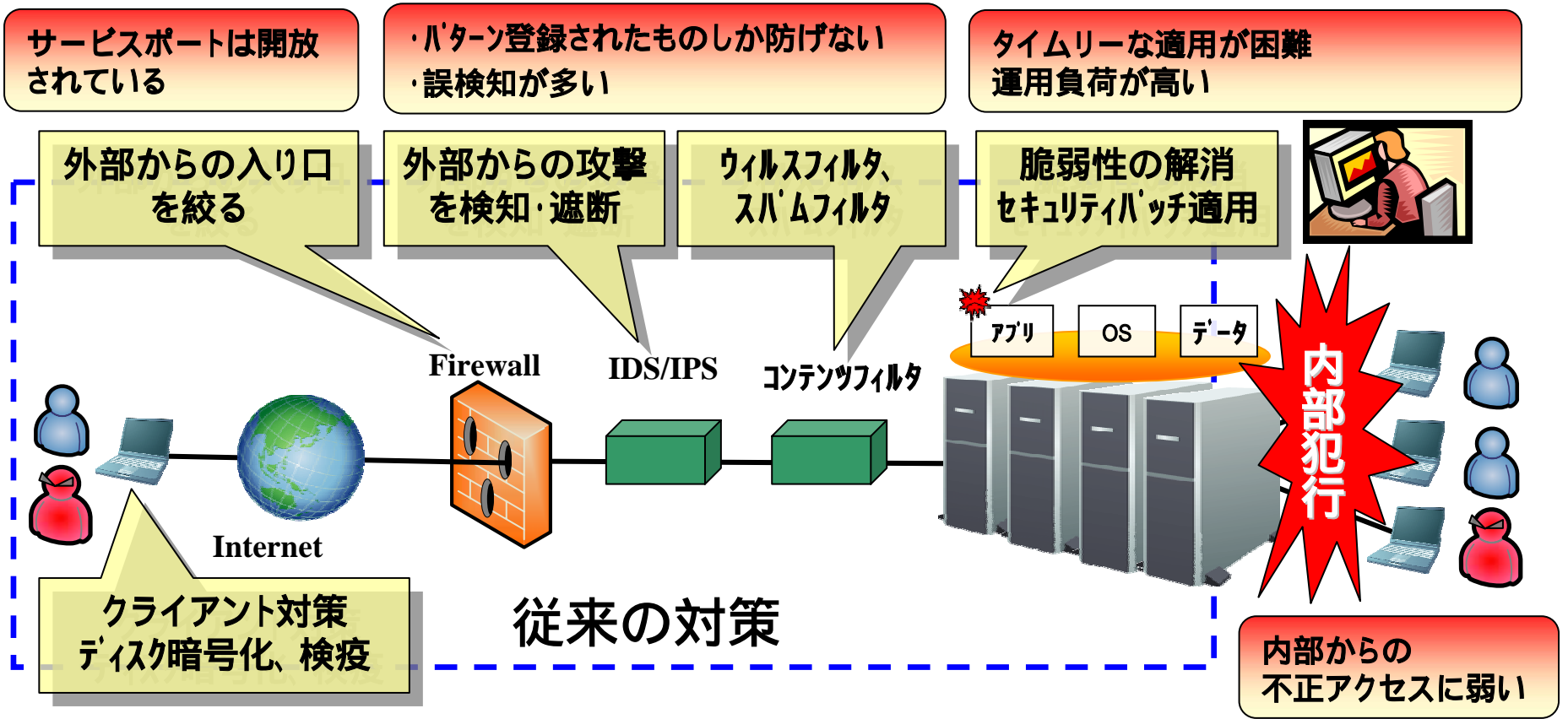
SHieldWARE

実運用フェーズに入ったセキュアOS



株式会社 富士通ソーシャルサイエンスラボラトリ
2006年6月15日

従来のセキュリティ対策の課題

1. 従来のセキュリティ対策は、**外部攻撃対策**に偏っている。
2. **未知の攻撃パターン**や、**内部からの攻撃**にはうまく対応できていない。
3. **パッチ適用**は有効だが、なかなかタイムリーに更新・運用できない。



従来のセキュリティ対策では対応困難な脅威

脅威	対応できない理由
<p>新しいパターンの攻撃 (ゼロディアタック)</p>	<p>新しいパターンのため、セキュリティベンダよりパターンやシグネチャの提供がされず、攻撃を検出できない</p>
<p>パッチが適用されるまでの攻撃</p>	<p>ベンダでのパッチ未提供、またはユーザ側での事前検証のため タイムリーにパッチ適用ができない</p>
 <p>管理者による不正アクセス</p>	<p>システム管理者が管理者権限を使い不正を行うため検知できない。 操作ログも改ざんされる。</p>
 <p>内部からの不正アクセス</p>	<p>内部ユーザが攻撃ツール等で脆弱性を利用しroot権限を奪う</p>

セキュアOSでは、データの存在するサーバ自体を要塞化し、機密データを守ることが可能です。

内部からの不正について

■ 運用現場は**性善説**が基本

■ 内部からの情報漏えいについての考え方

仮に、故意の不正行為は発生しないとしても、**「事故」**には対応する必要がある

運用の**アウトソーシング**という現実に対処する必要がある

- ・ 契約事業者(運用会社)
- ・ 契約社員、派遣社員
- ・ 離職者
- ・ メーカー、インテグレータ

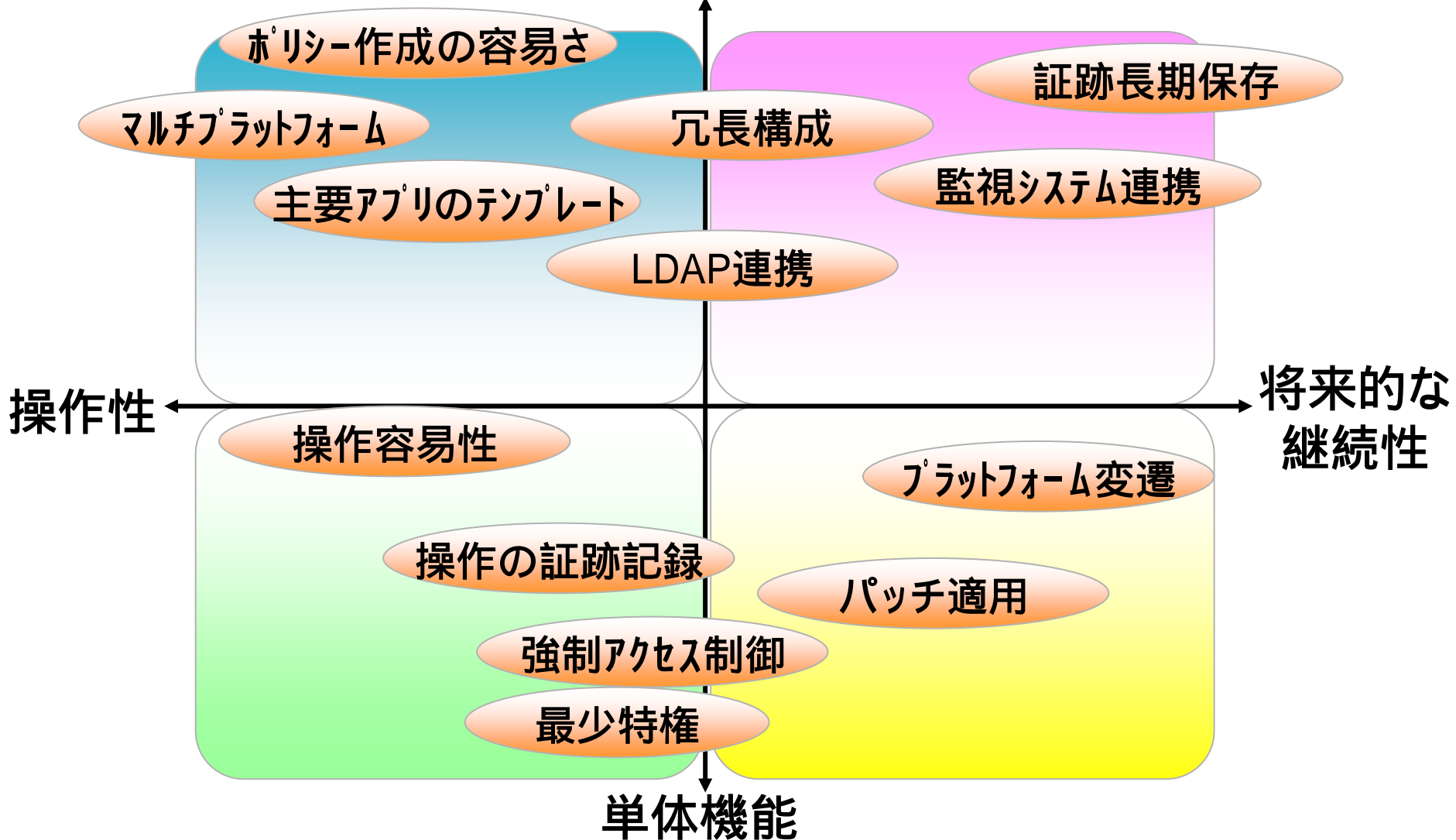
不正をしていないことを証明するためにも**監査証跡**は必要

■ **内部統制**というキーワードの中で対策を余儀なくされる。

セキュアOSは内部統制を高める重要技術となる

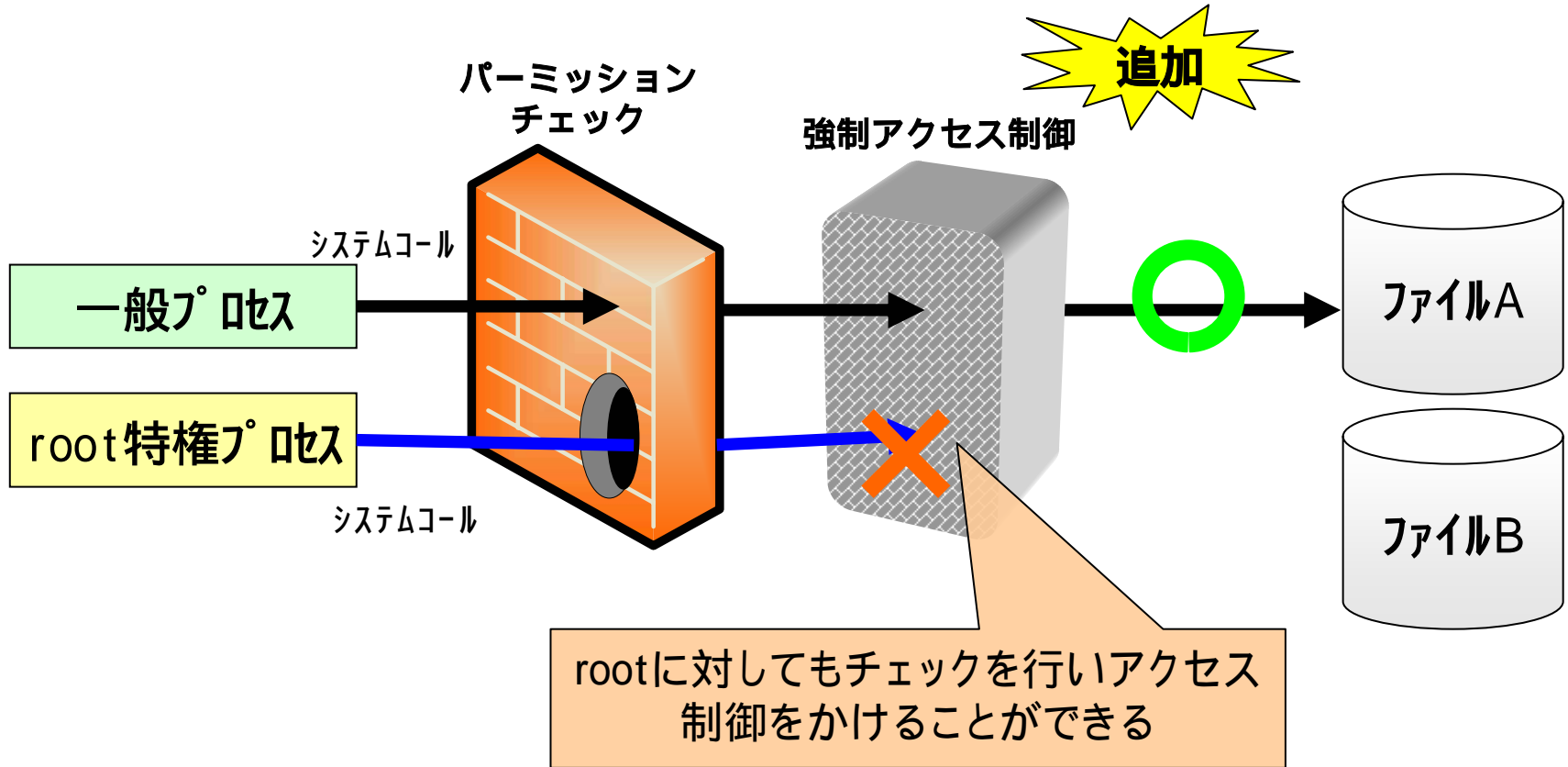
セキュアOS運用に向けた評価基準

システムとしての運用性



強制アクセス制御

セキュアOSによる強制アクセス制御

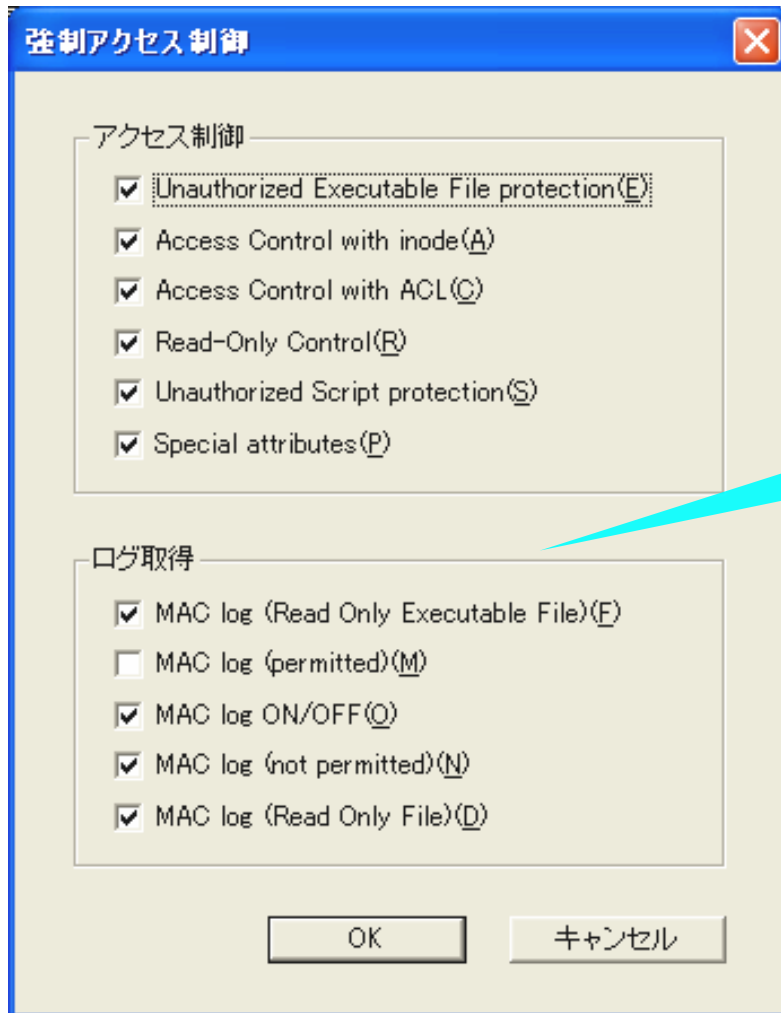


- ・あらゆるユーザに対して組織ポリシーを強制可能
- ・rootの特権範囲を制限

【強制アクセス制御】セキュリティオプションの設定

強制アクセス制御

操作容易性



- ・不正インストールされたファイルの実行禁止
- ・実行ファイルへの書込み禁止



- ・トロイの木馬や成りすましコマンドの起動防止
- ・システムの破壊を防止

以前より指摘されている汎用OSの問題点 = 特権ユーザの存在

UNIXならば root、Windowsならば administrator

- ❑ root特権を必要とするプロセスが多すぎる
rootを奪われる = ホストを支配される
- ❑ 管理者はみんなroot権限を使う
rootにならないとできないことが多い
- ❑ システム管理者はログの改ざんも可能
システム管理者による改ざんを検知・防御
する方法がない(ログを信用できない)

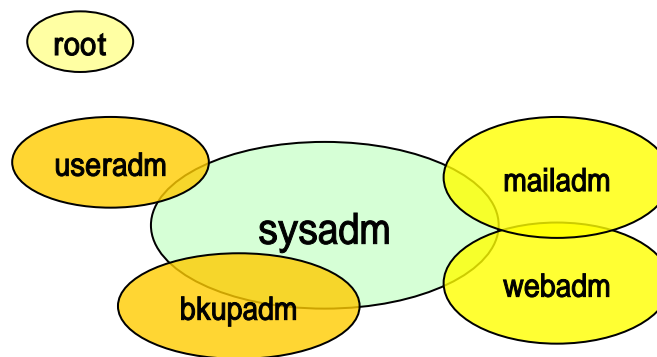
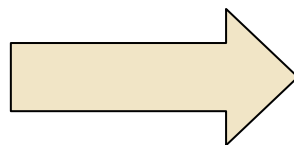
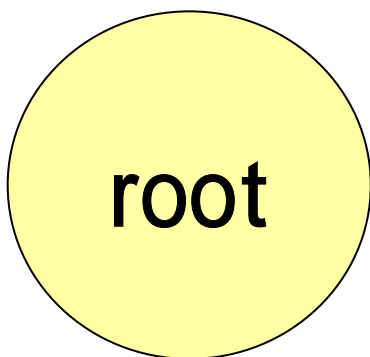


問題

誰にも必要以上の特権を与えない = 最少特権

作業目的ごとに利用するコマンドやファイルが異なる
それらを**ロール**として再定義

役割	利用するコマンド例	ロール
ユーザ管理者	useradd、passwd など	useradm
バックアップ運用者	dump、mount など	bkupadm
システム運用者(パッチ運用含む)	shutdown、mount、patch など	sysadm
一部のアプリ管理者 (Web管理者、メール管理者など)	アプリに依存する管理コマンド、 Log関連の操作コマンド など	webadm mailadm



一般のUNIXシステムではroot昇格後のログには元のユーザ（ログインユーザ）が残らないため不正の追跡は困難

コマンドの引数まで記録できるのはセキュアOSだけ

日付	プロセス	ファイル	メッセージ	PID	ログインユーザ	カレントユーザ	実
2006-06-06 17:08:55	bash		clear	2044	hosoda	root	
2006-06-06 16:41:23	bash		cat	1985	hosoda	root	
2006-06-06 16:41:22	bash		ls --color=tty -a	1984	hosoda	root	
2006-06-06 16:41:21	bash		pwconv	1983	hosoda	root	
2006-06-06 16:41:07	bash	/etc/shadow	vim /etc/shadow	1982	hosoda	root	
2006-06-06 16:41:02	bash	/etc/shadow	cat /etc/shadow	1981	hosoda	root	
2006-06-06 16:40:37	bash	/etc/passwd	vim /etc/passwd	1979	hosoda	root	
2006-06-06 16:40:34	bash		ls --color=tty	1978	hosoda	root	
2006-06-06 16:40:33	su		-bash	1936	hosoda	hosoda	

一般ユーザ: hosodaが、suコマンドを実行しrootに昇格

その後passwdファイル等を編集したことが記録に残る

内部統制・監査証跡のためのログ収集

操作の証跡記録

不正アクセスの記録～監視システムへの通知

いつ?	誰が?	何をした?	結果はどうなった?
2006-06-13 18:38:52	bash	exec /usr/bin/bash	root hosoda
2006-06-13 18:38:47	shutdown	reject This command is allowed to access the specific IP address	root hosoda
2006-06-13 18:38:47	vi	reject This command is allowed to access the specific IP address	root hosoda
2006-06-13 18:38:47	ls	reject This command is allowed to access the specific IP address	root hosoda
2006-06-13 18:38:47	cat	reject This command is allowed to access the specific IP address	root hosoda
2006-06-13 18:38:31	mail	exec /bin/mail -E	root hosoda
2006-06-13 18:38:31	cat	reject This command is allowed to access the specific IP address	root hosoda
2006-06-13 18:38:30	quota	exec /usr/sbin/quota	root hosoda
2006-06-13 18:29	su	exec cd /	hosoda hosoda
2006-06-13 18:29	sh	exec /sbin/sh	root hosoda
2006-06-13 18:29	su	exec /usr/bin/su -	hosoda hosoda
2006-06-13 18:29	vi	exec /usr/bin/vi kamac.txt	hosoda hosoda
2006-06-13 18:29	ls	exec /usr/bin/ls -l	hosoda hosoda
2006-06-13 18:29	ls	exec /usr/bin/ls -a	hosoda hosoda
2006-06-13 18:29	cat	exec /usr/bin/cat kamac.txt	hosoda hosoda
2006-06-13 18:29	mv	exec /usr/bin/mv kamac.sh kai	hosoda hosoda
2006-06-13 18:29	ls	exec /usr/bin/ls	hosoda hosoda

アクセスに対しセキュアOSが許可/拒否した記録

不正アクセス時に実行したコマンド

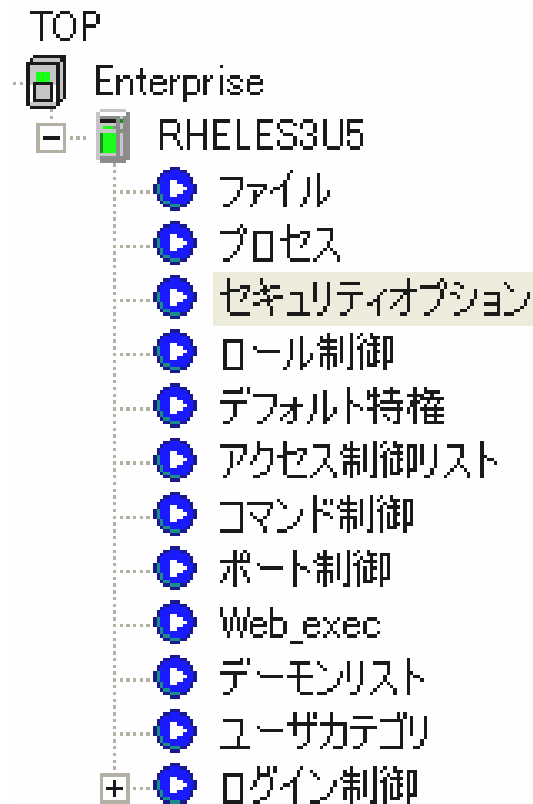
```
root#cat kamac.txt
bash: /usr/bin/cat: Permission denied
root#ls -a
bash: /usr/bin/ls: Permission denied
root#ls -l
bash: /usr/bin/ls: Permission denied
root#vi kamac.txt
bash: /usr/bin/vi: Permission denied
root#shutdown -h now
bash: /usr/sbin/shutdown: /sbin/sh: bad interpreter: Permission denied
root#
```

- 不正アクセスを検知・防御
- 対処記録(rejectなど)を残す
- セキュリティ監視システムとリアルタイムに連携し管理者に不正を通知

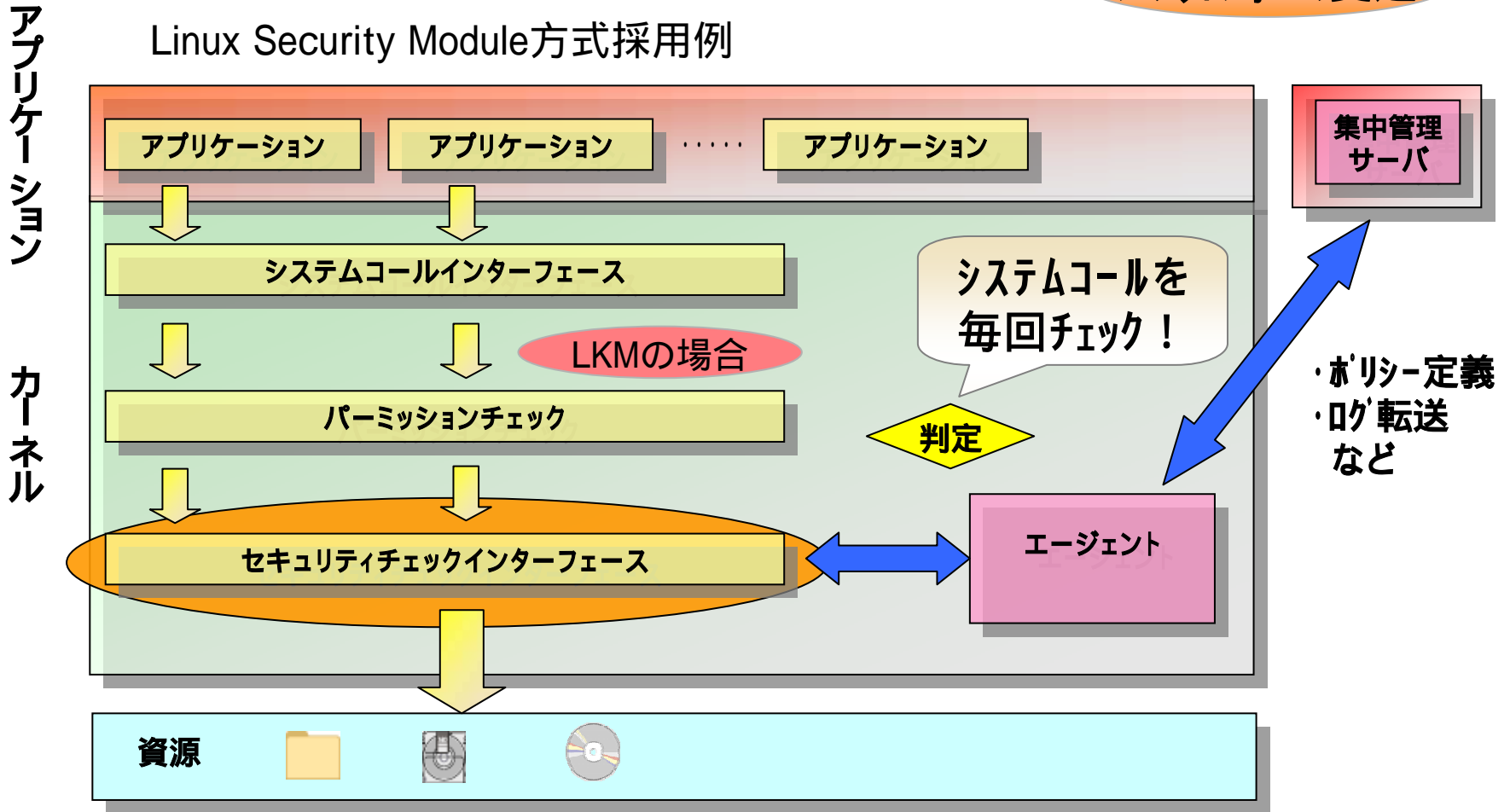
「セキュアOS = 難解」のイメージを直感的なGUIで簡略化

具体的にどう守るか？

- **ファイルシステム制御**
 - マルチレベルセキュリティ (MLS)
 - アクセス制御リスト (ACL)
 - マウント制御
- **ネットワークアクセスの制御**
 - IP、ポートベースセキュリティ
- **プロセス生成・実行の制御**
 - プロセスごとのアクセス制御
- **監査ログ**
 - ログ出力モード変更



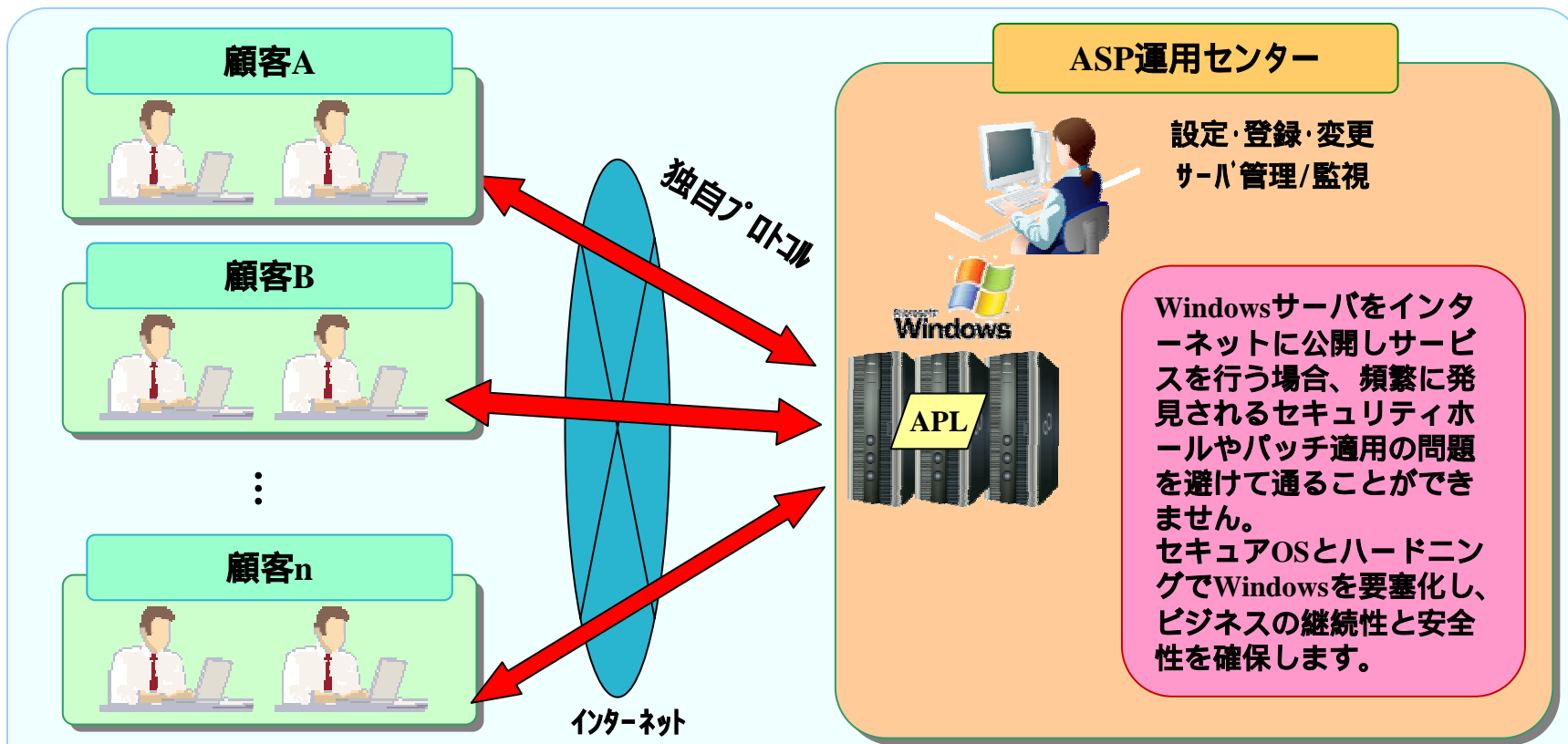
Linux Security Module方式採用例



- ・OSの仕様変更に伴い制御機構にも変更を反映
- ・Linux 2.4 2.6でLKM方式からLSM方式に変更(3ヶ月で対応)

導入事例

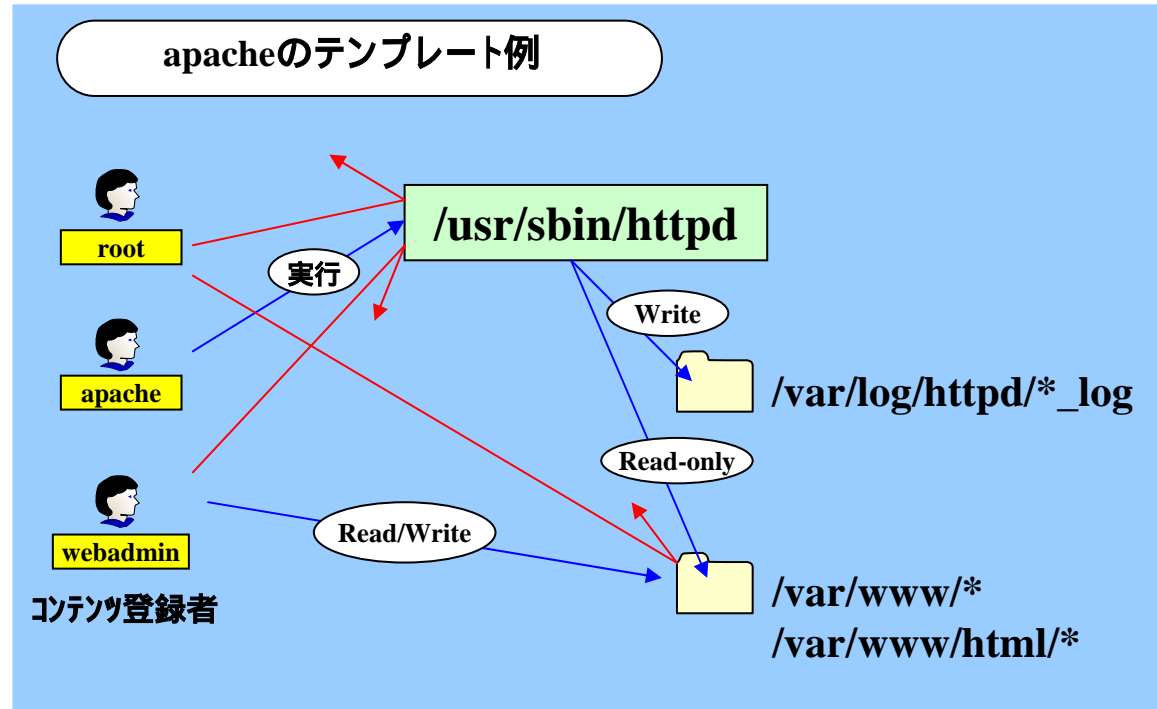
セキュアOSによりWindowsサーバを要塞化し クラウド型パッケージをインターネットで利用



MSPサービスにおいて、過去12ヶ月間に29種類のWindows Hotfix適用をスキップしても、セキュリティ上の問題なく運用できることを確認

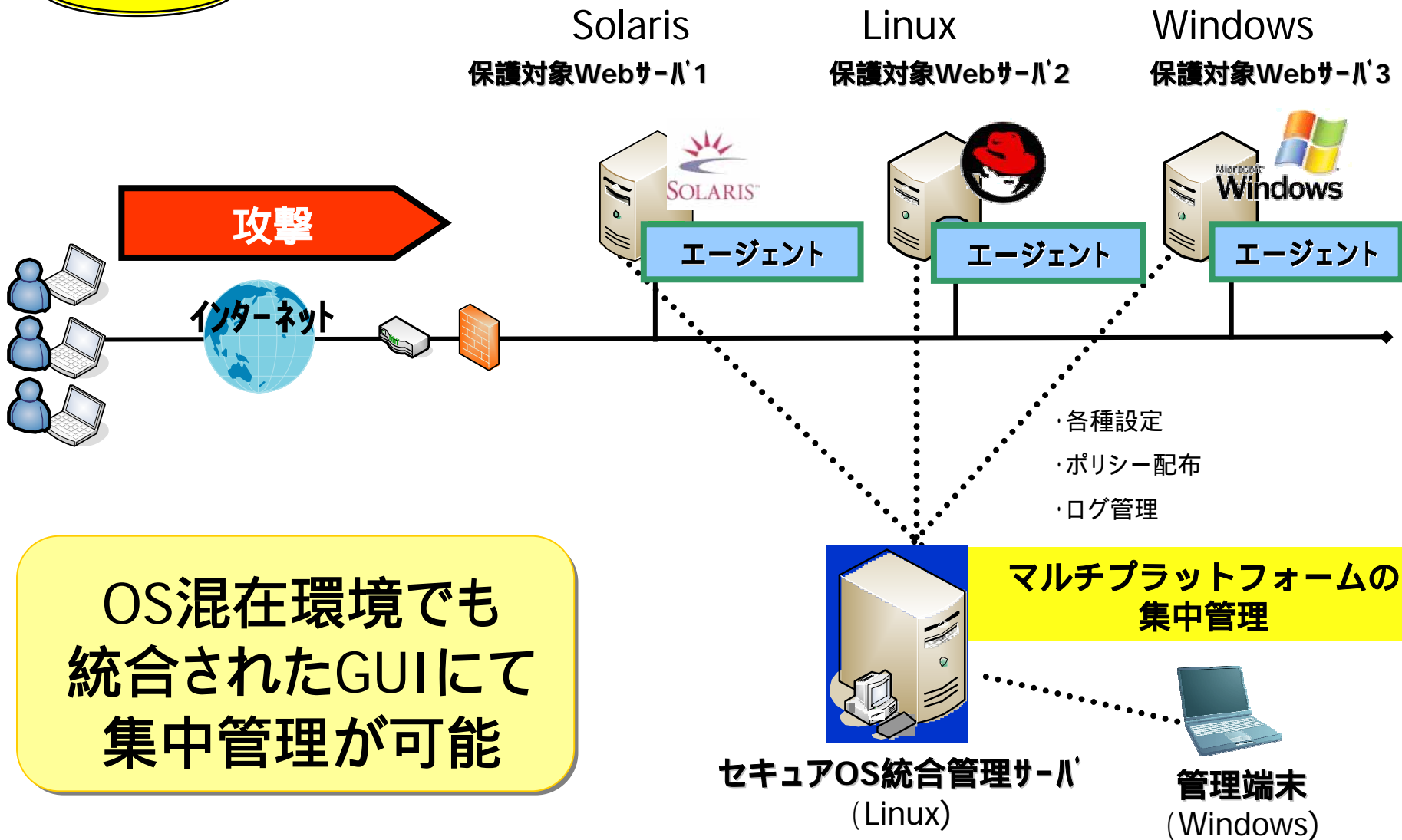
<テンプレート例>

- apache
- bind
- Sendmail
- LDAP
- syslog
- tomcat
- Interstage Web Application Server



DMZで利用される主要アプリケーションのセキュア化テンプレート提供により、複雑な設計不要で公開サーバを簡単にセキュア化可能です

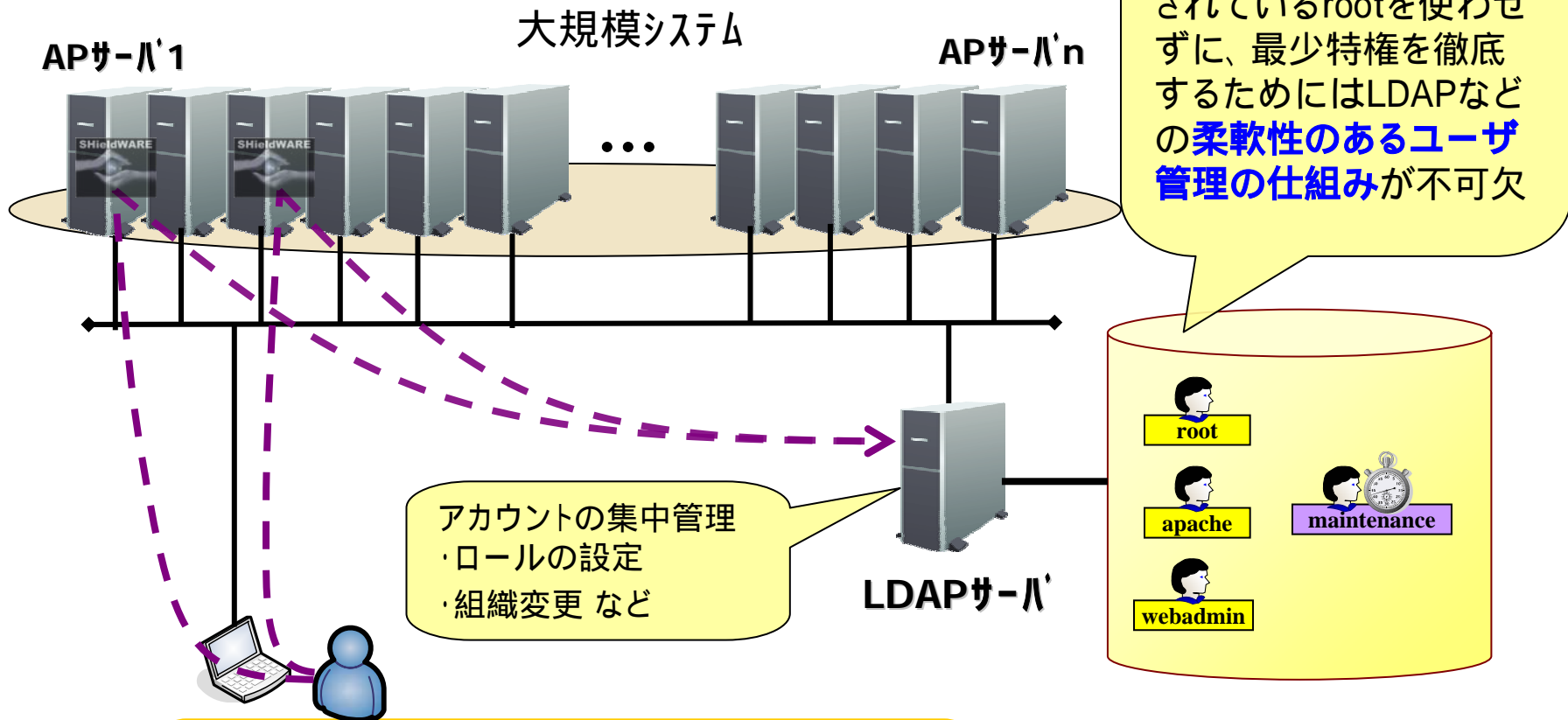
導入事例



大規模システムでのLDAP連携

LDAP連携

導入事例



LDAP連携により、LDAPに登録されたユーザーに対するアクセス制御を実現。

セキュリティ監視システムとの連携

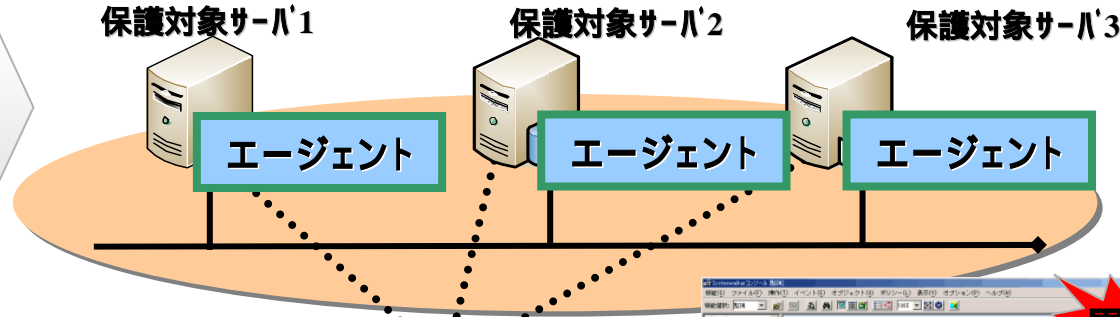
監視システム連携

導入事例

セキュリティ監視システムと連携することにより、各サーバのセキュリティ監査情報の集約が可能

セキュリティイベントの
集中管理

保護対象サーバ1 保護対象サーバ2 保護対象サーバ3



SIIfieldWARE WorkGroup Manager

現在のログ：取得時刻 2006-06-13 18:40:37 1393件中 1~50件を表示

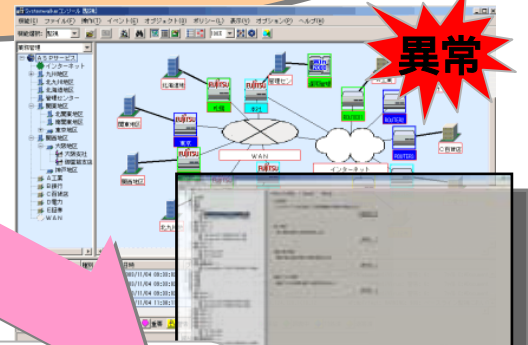
日付	プロセス	タイプ	メッセージ	カレントユーザ	ログインユーザ
2006-06-13 18:38:52	bash	exec	/usr/bin/bash	root	hosoda
2006-06-13 18:38:47	shutdown	reject	This command is allowed to access the specific IP address	root	hosoda
2006-06-13 18:38:44	vi	reject	This command is allowed to access the specific IP address	root	ho
2006-06-13 18:38:38	ls	reject	This command is allowed to access the specific IP address	root	ho
2006-06-13 18:38:35	cat	reject	This command is allowed to access the specific IP address	root	ho
2006-06-13 18:38:31	mail	exec	/bin/mail -E	root	ho
2006-06-13 18:38:31	cat	reject	This command is allowed to access the specific IP address	root	ho
2006-06-13 18:38:30	quota	exec	/usr/sbin/quota	root	ho
2006-06-13 18:38:29	su	exec	cd /	hosoda	ho
2006-06-13 18:38:29	sh	exec	/sbin/sh	root	ho
2006-06-13 18:38:26	su	exec	/usr/bin/su -	hosoda	ho
2006-06-13 18:38:16	vi	exec	/usr/bin/vi kamac.txt	hosoda	hosoda
2006-06-13 18:38:11	ls	exec	/usr/bin/ls -l	hosoda	hosoda
2006-06-13 18:38:10	ls	exec	/usr/bin/ls -a	hosoda	hosoda
2006-06-13 18:38:04	cat	exec	/usr/bin/cat kamac.txt	hosoda	hosoda
2006-06-13 18:37:57	mv	exec	/usr/bin/mv kamac.sh kamac.txt	hosoda	hosoda
2006-06-13 18:37:45	ls	exec	/usr/bin/ls	hosoda	hosoda



セキュアOS
統合管理サーバ

セキュリティ
イベント管理

運用管理サーバ

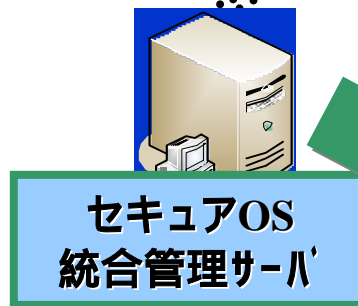
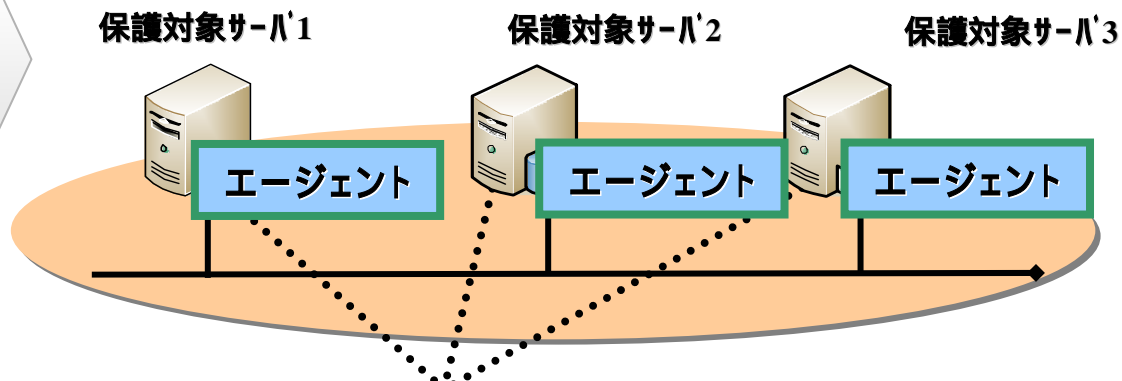


統合ログ管理システムとの連携により長期的な監査証跡保存を実現可能

導入事例

操作ログの 長期間保存

大容量ストレージ



ログ転送

運用管理サーバ



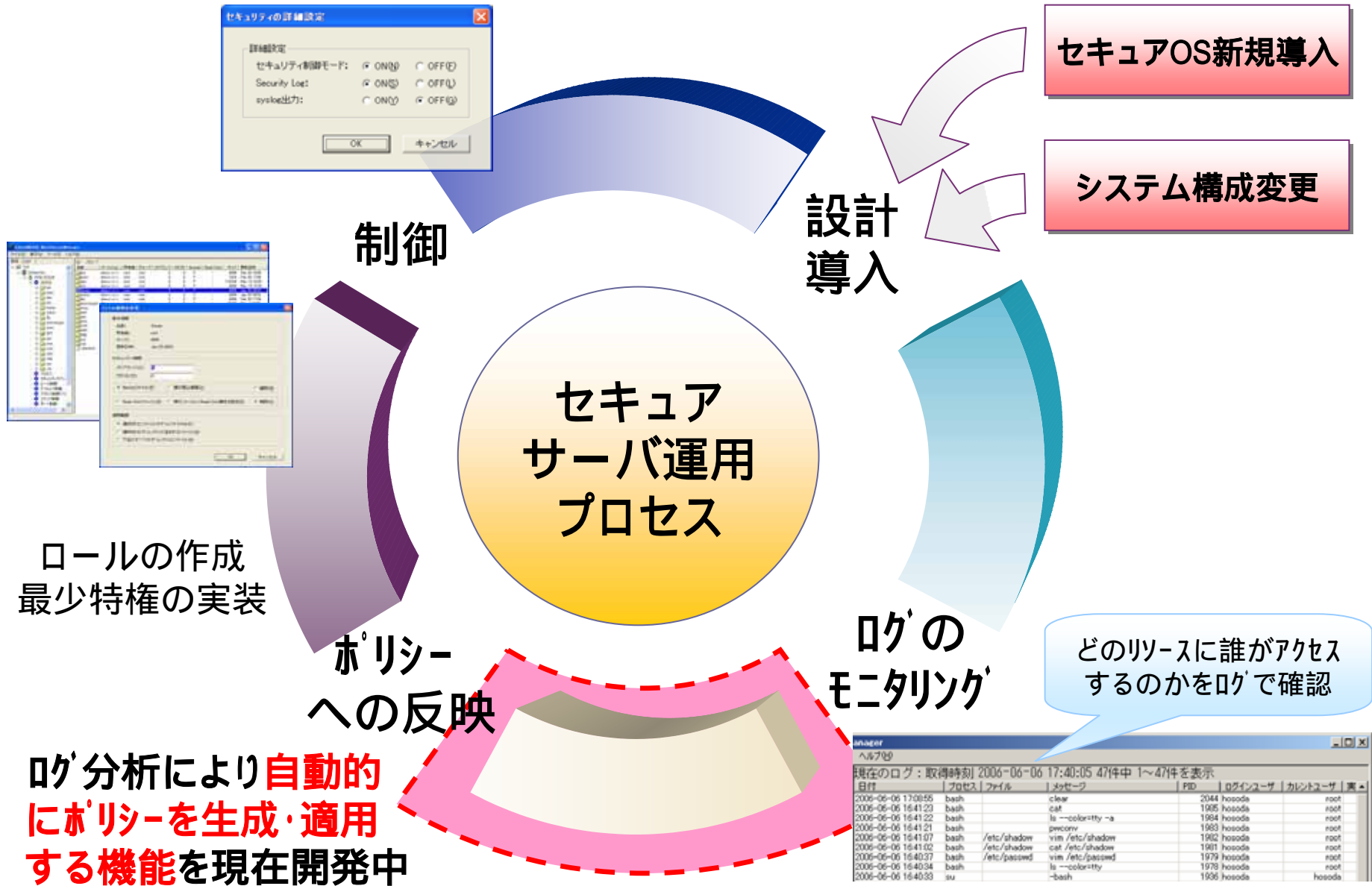
我々が目指したことと課題

- 既存セキュリティ対策で対応できなかった課題を解決
- 従来のトラステッドOS / セキュアOSの課題を解決
 - GUIでの設定(複数台をまとめて管理できる統合管理サーバを提供)
 - システムトータルでの運用に配慮
 - 機能を部分的に利用することも可能とした
 - マルチプラットフォーム対応
 - ベンダサポートの提供(ヘルプデスク、設計支援サービス、構築サービスなど)
 - 現実的な価格
- 運用管理システム連携
 - 任せるべき部分は専用の運用管理システムに任せる方針

■ 課題

- 初期ポリシー設計のためには、ある程度の知識が必要
 - ログ結果からポリシーを自動生成できる機能を現在開発中
- 集中管理サーバのクラスタ対応
 - お客様からの要望が多いため現在機能追加検討中

セキュアOS導入のPDCAサイクル



- セキュアOSの全ての機能を使う必要はない！
守るべき資産を明確にし、設計はできるだけシンプルにする
- 最少特権ルールに則ってユーザ権限を明確化する！
rootなしで運用できるようなロールを作成
 - rootアカウントを使わない / 使わせない
 - 例外措置的なロールの払い出しを想定しておく(例: 時限ユーザ払い出し)
 - 全てのシステムに標準定義されているrootを使わないならば、アカウントをシステム間で共有化する仕組みとしてLDAP連携は必須
- 導入時には運用現場からの反発を覚悟する！
 - 内部監査に対して運用現場は敏感に反応する
「操作の正当性証明」のためであることを理解してもらう
 - 現場オペレータにはrootなしの運用は想像困難
十分な運用教育が必要
- ログ管理システムとの連携を事前に計画する！
 - ログはホスト外に置くのが鉄則
 - ログの長期保存を計画する
 - セキュリティアラートのリアルタイム監視には運用管理システム連携が必須
- パッチ適用についてのルールを再度見直そう！
 - パッチ適用の必要性を明確にすることで、
一切適用しない / 定期保守日に一括適用 / 従来どおり随時適用
などの選択が可能

A large, stylized version of the FUJITSU logo, featuring the word "FUJITSU" in a red, serif font with a red infinity symbol above the letter "I".

THE POSSIBILITIES ARE INFINITE

製品紹介URL

<http://www.ssl.fujitsu.com/products/network/netproducts/shieldware/index.html>