

仮想OS対応

特権ユーザーのサーバ操作ログ取得と管理

SHieldWARE



サーバに鉄兜を着せる

金融機関、官公庁で1500サーバ以上のご採用いただいております！

富士通株式会社

SHieldWARE が必要だったお客様

1 サーバ操作ログ記録が必要

・パソコン操作ログはとったが、個人データ等が入った**重要なサーバ**の操作ログはとっていない。

2 サーバの外部アタック防衛が必要

・外部アタックで特権ユーザー権限(root, Administrator)がのっつられ、**重要データ**が盗まれるのを防ぎたい。

3 特権ユーザー権限の分割が必要

・特権ユーザー(root, Administrator)のアクセス権限を**細分化**したい。

1 サーバ操作ログ記録

I can SHieldWARE もとのユーザーを簡単に追跡

特権ユーザー権限 (root, administrator) で行った操作は、全て、特権ユーザー権限昇格後の操作履歴で残ってしまいが、SHieldWARE のログを見れば、特権ユーザー権限昇格前のユーザーを特定できます。

いつ	何に	何をした	誰が			
日付	プロセス名	オブジェクト	メッセージ	ログインユーザ名	ユーザ名	メッセ
2010-10-27 11:49:29.093	clear	/usr/bin/clear	clear	fujitsu	root	exec
2010-10-27 11:49:21.575	vi	/bin/vi	vi /etc/passwd	fujitsu	root	exec
2010-10-27 11:49:04.888	consoletype	/sbin/consoletype	/sbin/consoletype	fujitsu	root	exec
2010-10-27 11:49:04.877	id	/usr/bin/id	/usr/bin/id -u	fujitsu	root	exec
2010-10-27 11:49:04.874	grep	/bin/grep	/bin/grep -q /usr/kerberos/sbin	fujitsu	root	exec
2010-10-27 11:49:04.871	grep	/bin/grep	/bin/grep -q /usr/kerberos/bin	fujitsu	root	exec
2010-10-27 11:49:04.866	egrep	/bin/grep	egrep -qi ^COLOR*none /etc/DIR_COLORS.xterm	fujitsu	root	exec
2010-10-27 11:49:04.862	dircolors	/usr/bin/dircolors	dircolors --sh /etc/DIR_COLORS.xterm	fujitsu	root	exec
2010-10-27 11:49:04.856	hostname	/bin/hostname	/bin/hostname	fujitsu	root	exec
2010-10-27 11:49:04.851	id	/usr/bin/id	id -un	fujitsu	root	exec
2010-10-27 11:49:04.847	egrep	/bin/grep	/bin/egrep -q C\ /usr/local/sbin(\$!)	fujitsu	root	exec
2010-10-27 11:49:04.843	egrep	/bin/grep	/bin/egrep -q C\ /usr/sbin(\$!)	fujitsu	root	exec
2010-10-27 11:49:04.839	egrep	/bin/grep	/bin/egrep -q C\ /sbin(\$!)	fujitsu	root	exec
2010-10-27 11:49:04.833	bash	/bin/bash	-bash	fujitsu	root	exec
2010-10-27 11:49:04.808	su	su	su -succeeded	root	root	login
2010-10-27 11:49:02.446	su	/bin/su	su -	fujitsu	fujitsu	exec
2010-10-27 11:49:00.330	id	/usr/bin/id	id -un	fujitsu	fujitsu	exec

ここで、fujitsuからrootに昇格したことがログからわかります。

SHieldWAREのログは特権ユーザーからもアクセスできない特別なエリアに格納されます。

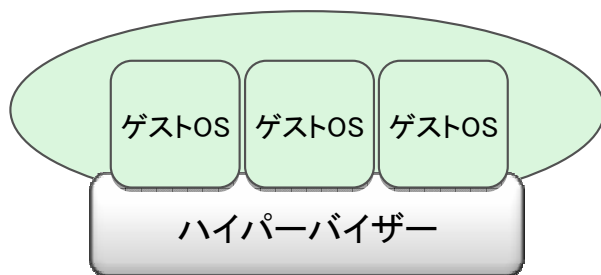
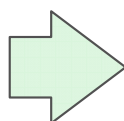
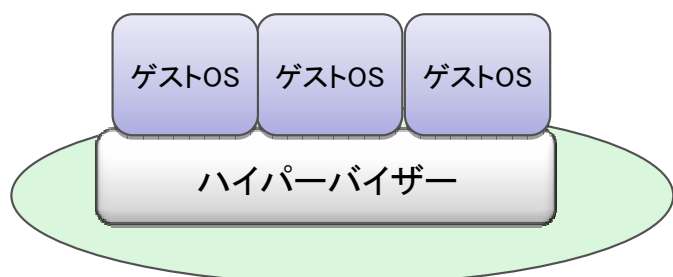
I can SHieldWARE 仮想環境でもしっかり証跡

VMwareの管理ツールでは、VMware管理操作以外の証跡は取れません。

SHieldWARE を導入すれば、ゲストOSの操作証跡を確実に管理できます。

VMwareの運用管理
ゲストOSのサーバ操作ログは
取れない

SHieldWARE導入後の
運用

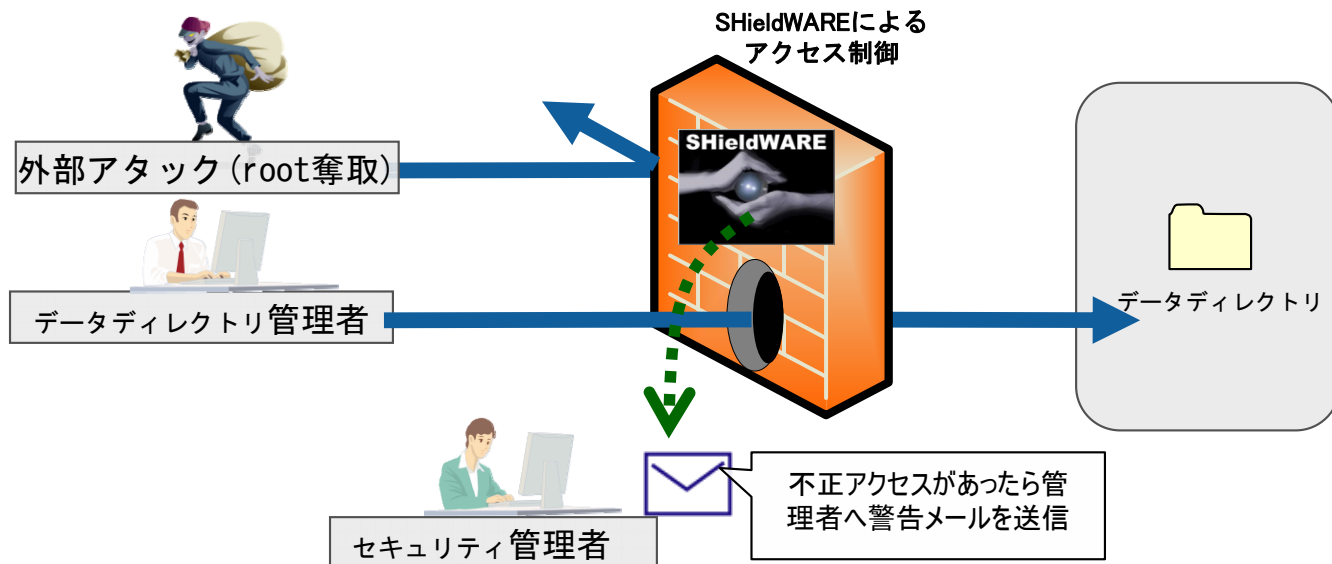


2 外部アタック防御

I can SHieldWARE

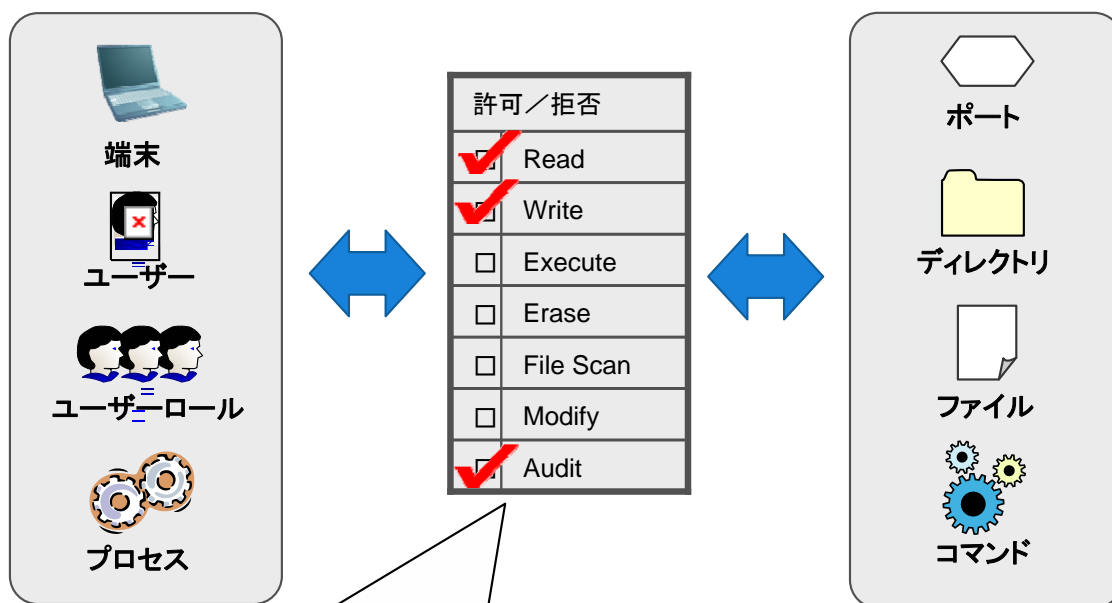
外部アタックを防御

OSのアクセス権限でチェックができない特権ユーザー権限も、SHieldWAREのアクセス制御を使って、重要なデータを守ることができます。



アクセス制御の実現は SHieldWARE のGUIで簡単に設定ができます。

正しいアクセスパターンを定義することで、それ以外のアクセス（外部アタック等）を拒否します。



サーバ内のリソースに対してアクセス可能なユーザーやプロセス、端末等を割り当てていきます。

3 特権ユーザー権限の分割

I can

SHieldWARE

特権ユーザー権限を分割

お客様の現状課題



特権ユーザーを
持っている人は？

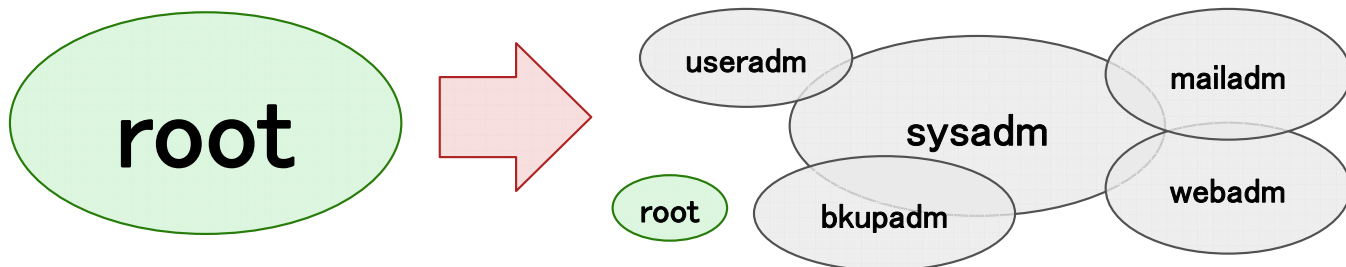


特権ユーザー権限持ってる人・・・え！こんなに！？

必要以上の権限をあたえているということは、**重要サーバ**への不正アクセスやセキュリティ事故を誘発することになります。

SHieldWARE

で、特権ユーザー権限をこんな風に分割しましょう

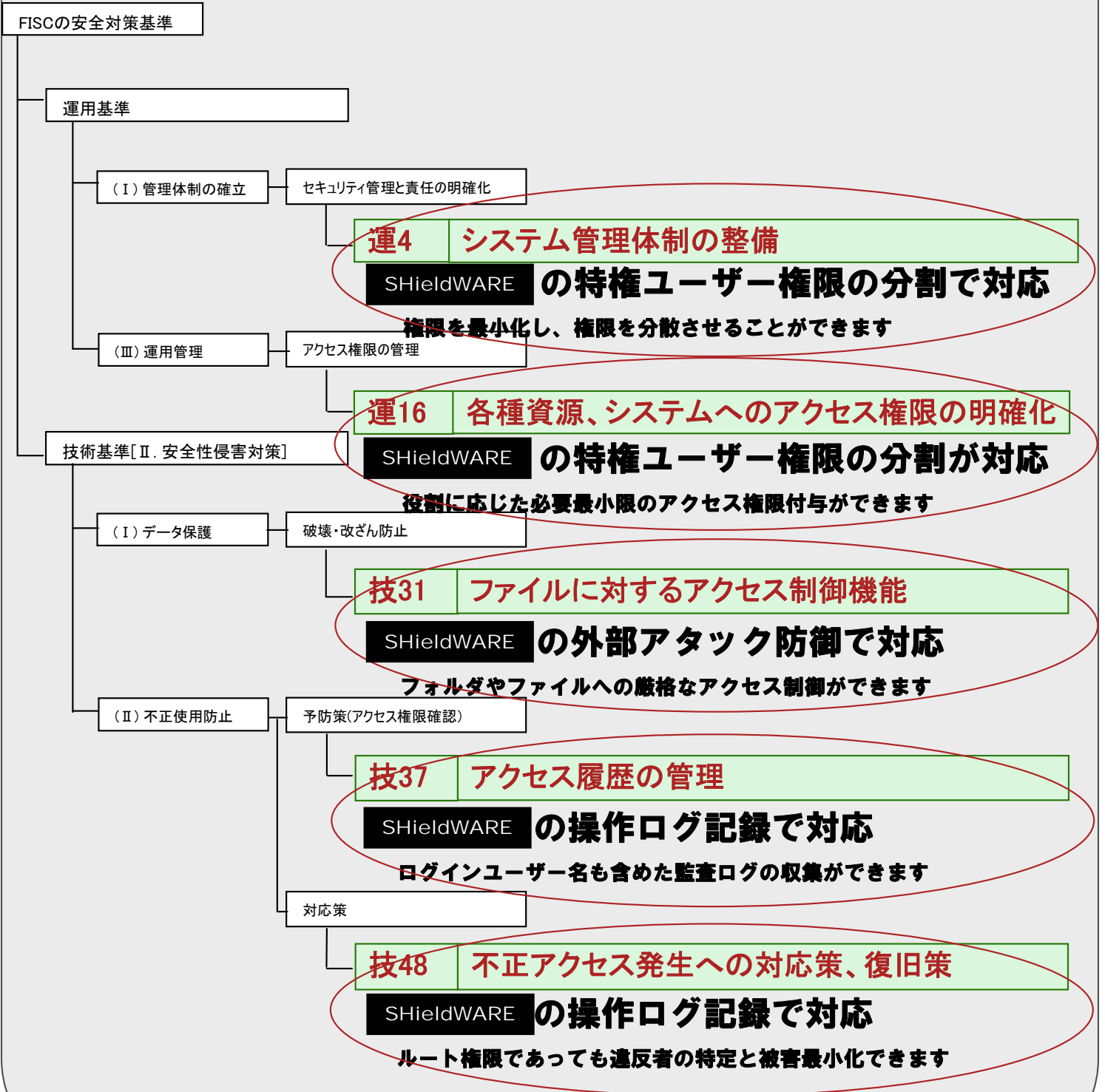


役割	利用するコマンド例	ロール
アカウント管理者	useradd、passwd など	useradm
バックアップ運用者	dump、mount など	bkupadm
システム運用者(パッチ運用含む)	shutdown、mount、patch など	sysadm
一部のアプリ管理者 (Web管理者、メール管理者など)	アプリに依存する管理コマンド、 Log関連の操作コマンド など	webadm mailadm

必要とされるガイドライン

金融情報システムセンター(FISC)

「金融機関等コンピュータシステムの安全対策基準・解説書」



「金融機関等コンピュータシステムの安全対策基準・解説書」より抜粋

必要とされるガイドライン

内閣官房情報セキュリティセンター(NISC)

「政府機関の情報セキュリティ対策のための統一基準」

NISCの遵守事項一覧

第2.1部 情報セキュリティ要件の明確化に基づく対策

2.1.1.2 アクセス制御機能

SHieldWARE の外部アタック防御で対応
フォルダやファイルへの厳格なアクセス制御ができます

2.1.1.3 権限管理機能

SHieldWARE の特権ユーザー権限の分割で対応
役割に応じた必要最小限のアクセス権限付与ができます

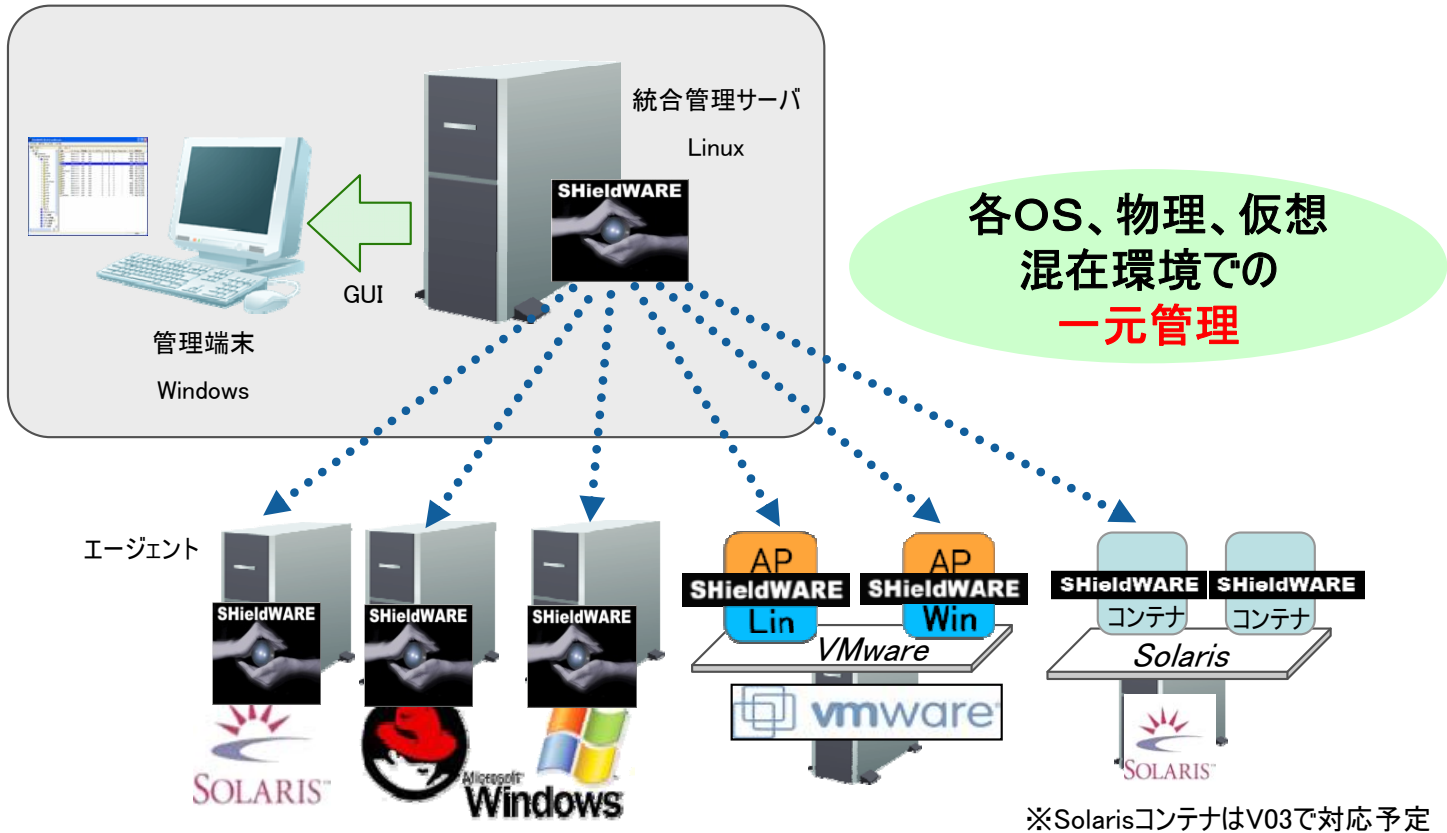
2.1.1.4 証跡管理機能

SHieldWARE の操作ログ記録で対応
ログインユーザー名も含めた監査ログの収集ができます
ルート権限であっても違反者の特定と被害最小化できます

内閣官房「政府機関の情報セキュリティ対策のための統一基準」の遵守事項一覧表より抜粋

システム構成例

統合管理サーバで守りたいサーバのセキュリティポリシーを一元管理します



価格

価格は標準価格

統合管理サーバライセンス	¥550,000
--------------	----------

エージェントライセンス (1 CPU)	¥550,000
---------------------	----------

エージェントライセンス (2 CPU)	¥950,000
---------------------	----------

エージェントライセンス (仮想OS用)	¥280,000
---------------------	----------

※SHieldWAREを管理するためには、統合管理サーバが必須です。統合管理サーバは専用のLinux機で動作させてください

※エージェントライセンスのCPU数とはソケット数のことです

SHieldWARE に決めた理由

Good!!

1. 安心な構築、保守

- ・富士通の製品で、**開発元から直接支援を受けられるため、構築、保守が安心。**



富士通Systemwalker認定製品

※**試供版**で動作確認もできます。ご希望の方はお問い合わせください
「類似製品の多くは、輸入製品が多く、サポートが不安」

Good!!

2. 高速なアクセス制御処理

- ・SHieldWARE の性能劣化は**2～3%程度**。

類似製品の性能劣化は2%～10%程度です。

※他社製品はアプリレイヤ、OSレイヤ間で処理が走りますが、

SHieldWARE はOSレイヤのみでアクセス制御処理を実現。

Good!!

3. 明瞭会計、低価格

- ・ライセンス体系は**単純明瞭**なCPU数課金。

※コア課金、ティア課金の排除

「類似製品は、サーバモデルによって価格が変わりライセンス管理が複雑」

しかも**安かった。**

導入のきっかけ

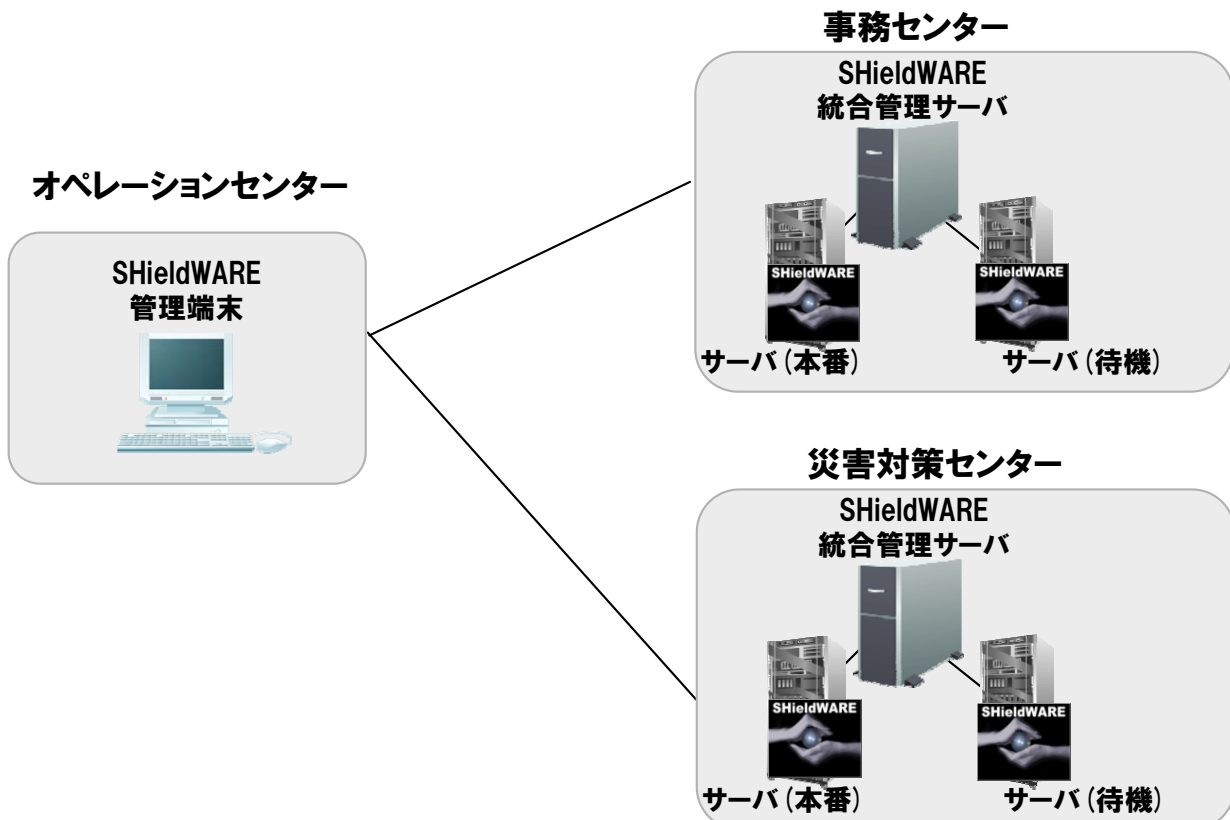
- ・監査人から操作ログ未取得の指摘あり。
- ・個人情報、機密情報等の重要データの流出、改ざんを防止して、お客様被害を防ぎたい。
- ・金融機関でデファクトスタンダードな製品を導入したい。

SHieldWARE で実現

個人情報、機密情報を有するサーバにSHieldWAREエージェントを導入し、外部委託先を含むシステム管理者の操作記録を取得

- ・システム管理者の操作ログをSHieldWAREで取得
- ・ログを日次で印刷してシステム監査を実施
- ・特権ユーザー(root)、一般ユーザーから全サーバのsyslogを保護
- ・特権ユーザー(root)、一般ユーザーから一部、システムファイルのアクセスを制限

2拠点間導入の事例



ログ点検の目的

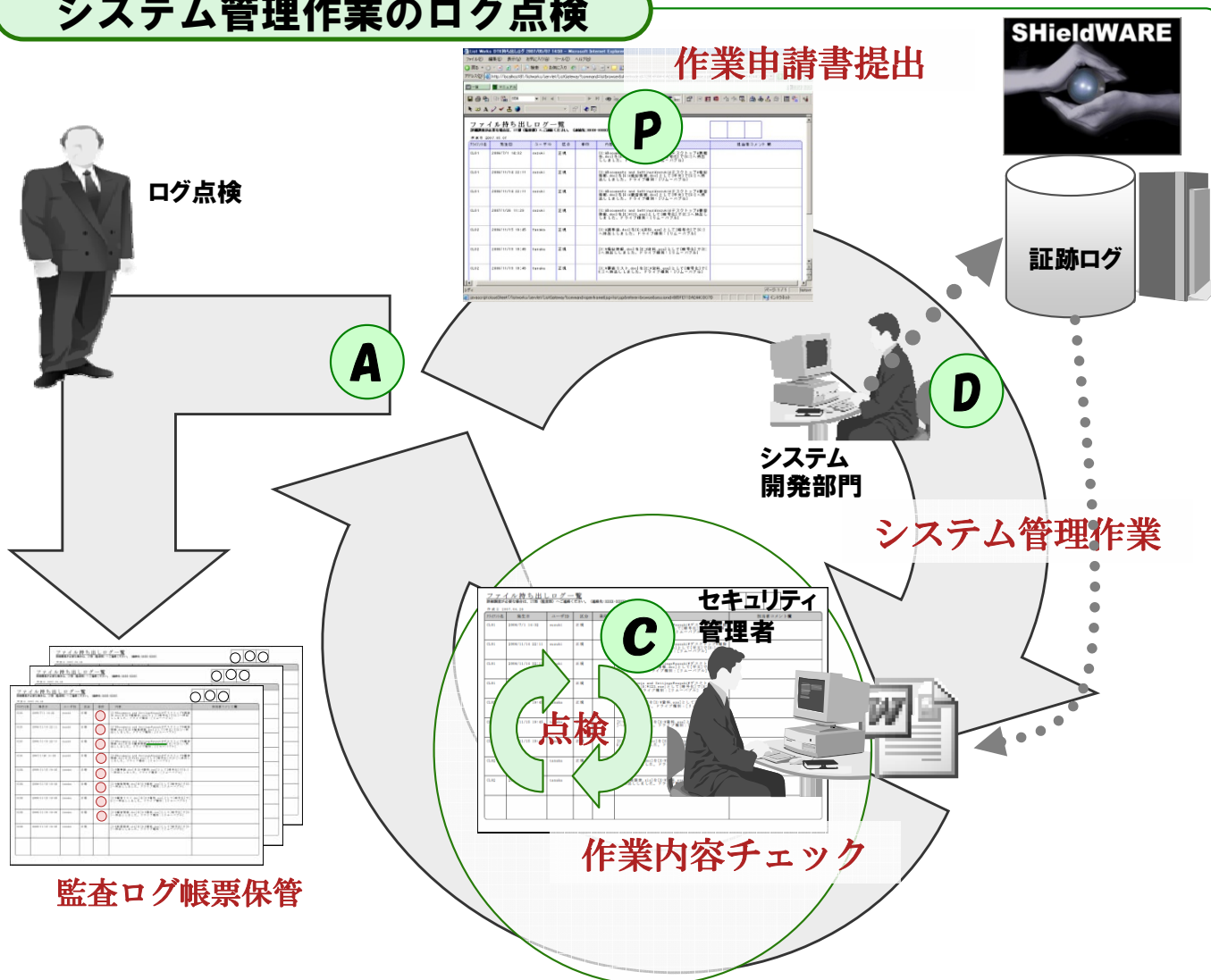
特権ユーザーの正当性を証明するための統制強化を実施したい。

- ・システム管理作業の掌握
- ・システムログの改ざん防止

金融機関での運用

- P** 事前に、システム管理作業の作業内容を申請
- D** 作業を実施し、作業内容のコマンドをSHieldWAREで記録
- C** 運用部門で、作業内容が申請通りであることをチェック
- A** 作業内容に問題が無ければ監査ログ帳票に検印し保管

システム管理作業のログ点検



サポートプラットフォーム

モジュール	サポートOS	
エージェント	Solaris	Solaris TM 8 Operating System Solaris TM 9 Operating System Solaris TM 10 Operating System
	Linux	Red Hat [®] Enterprise Linux [®] AS v.4/ES v.4(for x86, for Intel64, for Itanium) Red Hat [®] Enterprise Linux [®] 5(for x86, for Intel64, for Intel Itanium)
	Windows	Microsoft [®] Windows [®] 2000 Server Microsoft [®] Windows Server [®] 2003/2003 R2(x86, x64) Microsoft [®] Windows Server [®] 2008(x86, x64)
統合管理サーバ	Linux	Red Hat [®] Enterprise Linux [®] AS v.4/ES v.4(for x86, for Intel64) Red Hat [®] Enterprise Linux [®] 5(for x86, for Intel64)
管理端末	Microsoft [®] Windows [®]	

統合管理サーバ

推奨スペック	Redhat Linuxが動作可能なIntel Platform、 CPU: Intel Xeon 2.4GHz以上、メモリ:4GB以上
必要動作条件	/usrパーティション:最小100 MB以上

管理端末

推奨スペック	Windows XPが動作するPC
必要動作条件	CPU: Intel Pentium III 500MHz以上、メモリ128MB以上

SHieldWAREに関するお問合せは

富士通株式会社

サービスビジネス本部 安心安全ビジネス推進室

〒144-8588 東京都大田区新蒲田1-17-25 富士通ソリューションスクエア

<http://segroup.fujitsu.com/secure/>

製品・サービスについてのお問合せは

<http://segroup.fujitsu.com/secure/contact>

カタログに記載の会社名、商品名は各社の商標または登録商標です。