

特権ID管理SHieldWAREのご紹介

株式会社富士通ソーシャルサイエンスラボラトリ

- 「特権 ID」は、OSの最高権限を持つアカウント

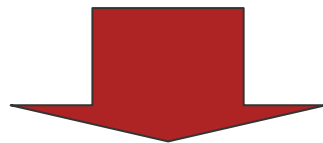
- 有名な特権ID:

UNIX系OS ⇒ root

Windows OS ⇒ Administrator

- 「特権 ID」を利用して行うサーバ管理業務が多い

「特権 ID」を利用しないと実施できないオペレーションが多い



万能な「特権 ID」の使いまわしが問題

システム管理者(特権ユーザー)による情報漏洩事件が近年、多発

■ 某証券会社:

約130万人分のデータが**システム管理者により**持ち出され、そのうち約5万人分のデータが、数十の名簿業者に流出

■ 某保険会社:

約13万件のクレジットカード情報が流出した可能性。**内部からの情報漏洩**が確定しても、正確な流出経路が不明。

■ 某通信系会社:

退職した管理者のIDをそのまま放置していたため、外部からのアクセスを許し、約450万件の個人情報漏洩

システム管理者(特権ユーザー)への確実な対策が求められている

特権IDの管理を求めるガイドライン

■ 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」

■ 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」

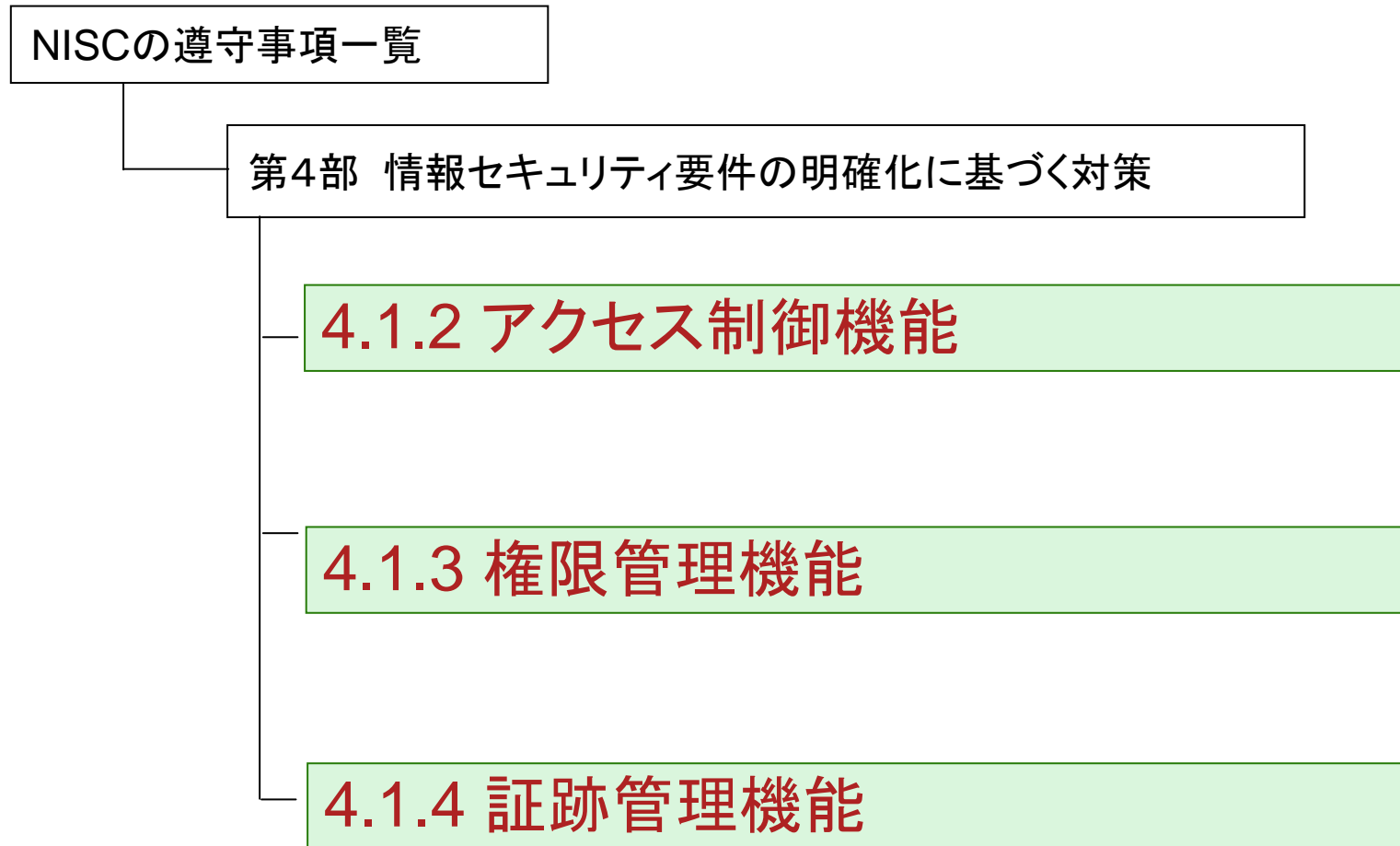
■ PCI SSC (PCIDSS) :

加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準

■ 金融商品取引法 (J-SOX)

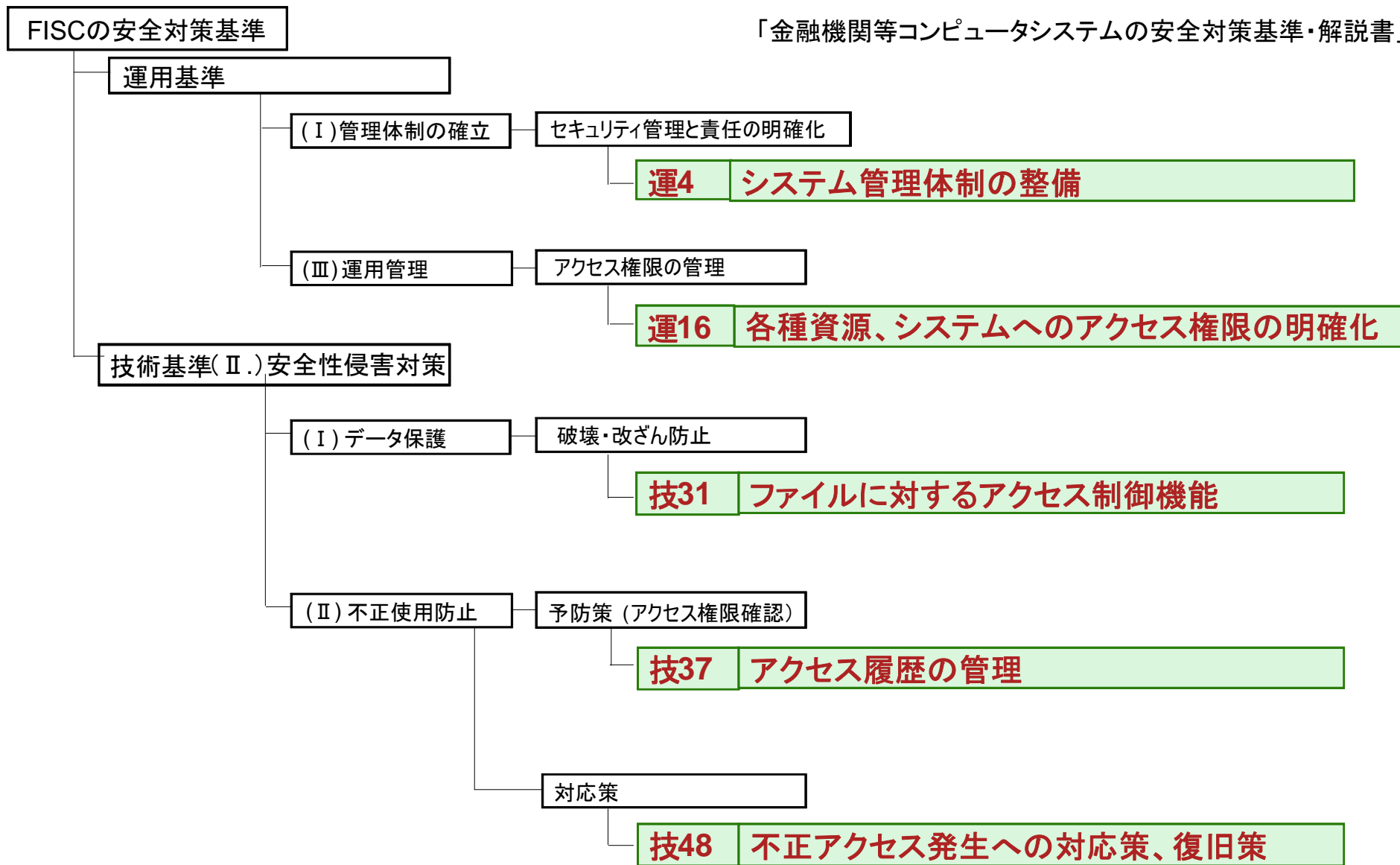
... 等々

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



FISCの「安全対策基準」

「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



「Payment Card Industry (PCI) データセキュリティ基準 バージョン1.2.1」より抜粋

要件7 : カード会員データへのアクセスを、業務上必要な範囲内に制限すること

7.1: システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。
アクセス制限には以下を含める必要がある。

7.1.1 特権ユーザー ID に関するアクセス権が、**職務の実行に必要な最小限の特権**に制限されていること。

7.1.2 特権の付与は、個人の職種と職能に基づくこと

要件10: ネットワークリソース及びカード会員データへのすべてのアクセスを追跡および監視する

10.1: システムコンポーネントへのすべてのアクセス (**特に、ルートなどの管理権限を使用して行われたアクセス**) を各ユーザーにリンクするプロセスを確立する。

10.3: イベントごとに、すべてのシステムコンポーネントについて少なくとも**以下の監査証跡エントリを記録する。**

10.5: 監査証跡は、**変更できないようにセキュリティで保護**されていること。

10.5.1 監査証跡の表示は、仕事関連のニーズを持つ人物のみに制限されていること。

10.5.2 監査証跡ファイルは**不正な変更から保護**されていること。

10.5.3 監査証跡ファイルは、変更が困難な**一元管理ログサーバ**または媒体に即座にバックアップされていること。

監査による不備改善指摘項目の約4割が「特権ID」関連

指摘例

- ① 特権IDを含めた操作ログ取得が実施されていない
- ② OS/DB/アプリを使用するユーザーIDのパスワード変更、もしくは利用制限の実施とログ取得がされていない
- ③ 特権IDを含めた操作ログのレビューが実施されていない



富士通総研先行ユーザー11社による不備指摘事項: **220件** / 553件

不備改善指摘への対策

では、指摘事項に対応するために何をすればいいのか

- ①特権IDの操作ログを取得すること
- ②特権IDのアクセス制限を行ない、ファイルやアプリへの厳格な利用制限を実装すること
- ③取得したログを定期的に確認すること

OK

SHieldWARE

OSのセキュリティを強化するためのモジュール

① 監査証跡

…OS機能では残らない詳細ログを記録

② 強制アクセス制御

…プログラムの起動やファイルの変更を強制的に制限

SHieldWAREを導入すると

⇒root権限(システム管理者)のアクセス制御が可能

⇒root権限が不正に利用されたとしても、被害を最小化

監査ログの例 ～特権ユーザー昇格後の追跡～

いつ

何に

何をした

誰がrootを使ったのか

日付	プロセス名	オブジェクト	メッセージ	ログインユーザー名	ユーザー名
2010-10-07 22:56:44.603	vi	/bin/vi	vi httpd.conf	sato	root
2010-10-07 22:56:36.697	ls	/bin/ls	ls --color=tty	sato	root
2010-10-07 22:56:24.624	vi	/bin/vi	vi /etc/hosts	suzuki	root
2010-10-07 22:56:04.572	crontab	/usr/bin/crontab	crontab -l	sato	root
2010-10-07 22:55:55.128	ls	/bin/ls	ls --color=tty -l	suzuki	root
2010-10-07 22:55:22.918	passwd	/usr/bin/passwd	passwd	sato	root
2010-10-07 22:55:09.349	tail	/usr/bin/tail	tail /var/log/messages	suzuki	root
2010-10-07 22:54:23.709	id	/usr/bin/id	id -u	sato	root
2010-10-07 22:54:23.704	id	/usr/bin/id	id -un	sato	root
2010-10-07 22:54:23.700	id	/usr/bin/id	id -gn	sato	root
2010-10-07 22:54:23.695	consoletype	/sbin/consoletype	/sbin/consoletype	sato	root
2010-10-07 22:54:23.689	id	/usr/bin/id	id -u	sato	root
2010-10-07 22:54:23.686	grep	/bin/grep	grep -q /usr/kerberos/sbin	sato	root
2010-10-07 22:54:23.683	grep	/bin/grep	grep -q /usr/kerberos/bin	sato	root

POINT



管理者権限(root)で行った操作は、一般のUNIXシステムでは管理者権限昇格後の履歴しか残りませんが、SHieldWAREでは、**管理者権限昇格前のユーザー名**も同時に記録します。



検索キー

- ✓ 期間
- ✓ ユーザー名
- ✓ プロセス名
- ✓ IPアドレス
- ✓ メッセージ文字列
- ✓ 対象ファイル名
- など

検索結果のCSVエクスポート
に対応

```
2006-06-06 16:41:21 bash
2006-06-06 16:41:07 bash /etc/shadow vim
2006-06-06 16:41:02 bash /etc/shadow cat
2006-06-06 16:40:37 bash /etc/passwd vim
2006-06-06 16:40:34 bash ls --color=tty
2006-06-06 16:40:33 su -bash
```

ログの検索条件

検索期間(P): 1970/01/01 9:00:00 から
2009/01/06 13:00:00 まで

ログ項目: IPアドレス 含まれる値: 10.36.129.285

AND

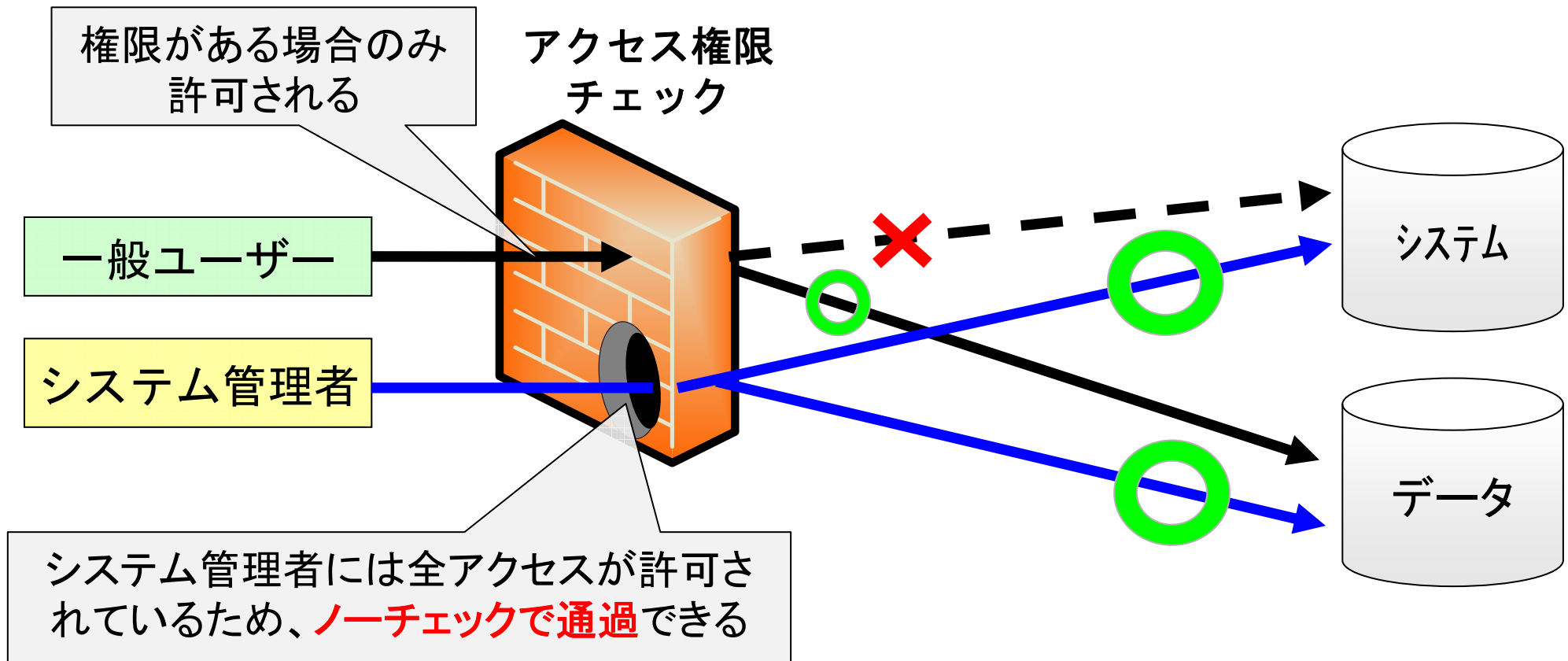
ログ項目: プロセス名 含まれる値:

AND

ログ項目: 検出ルール 含まれる値:

検索件数(N): 6

検索(S) 閉じる(C)



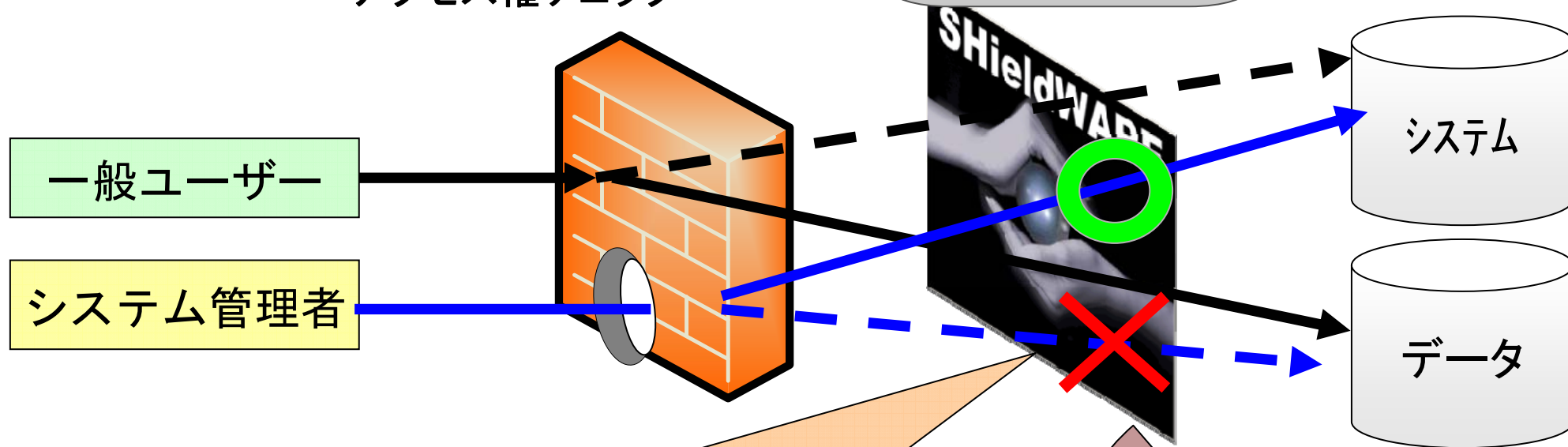
root権限の存在自体がセキュリティの抜け穴
一方で、管理者権限がないとできない作業も多い

SHieldWAREによる強制アクセス制御

POINT

OS標準
アクセス権チェック +

厳格なアクセス
制御モジュール

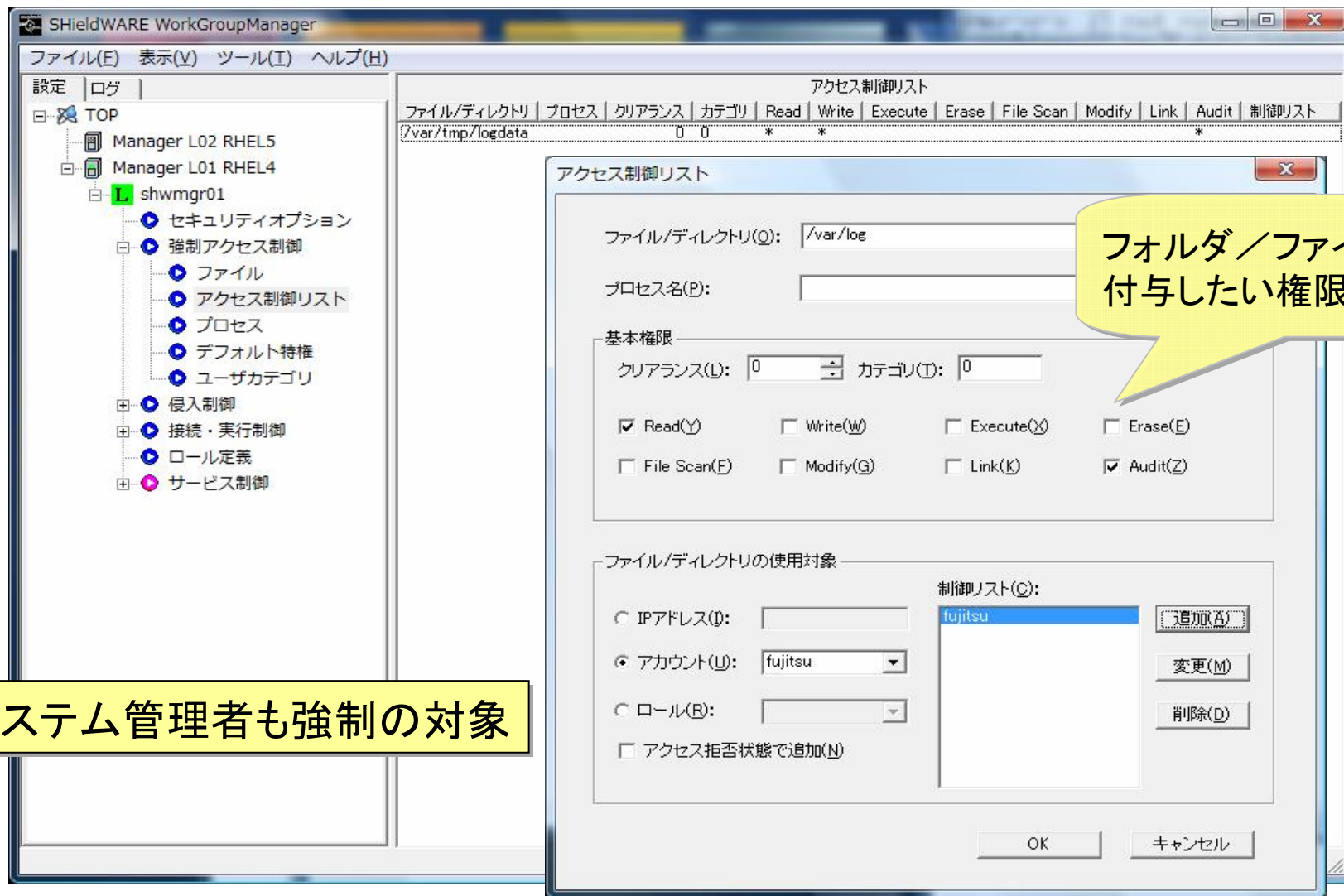


システム管理者に対しても
アクセス制御をかけることができる

セキュリティ違反ログ

[参考] 強制アクセス制御の設定GUI

プロセス、フォルダ、ファイル単位での強制的なアクセス制御が可能
 フォルダに対するアクセス制御設定の例

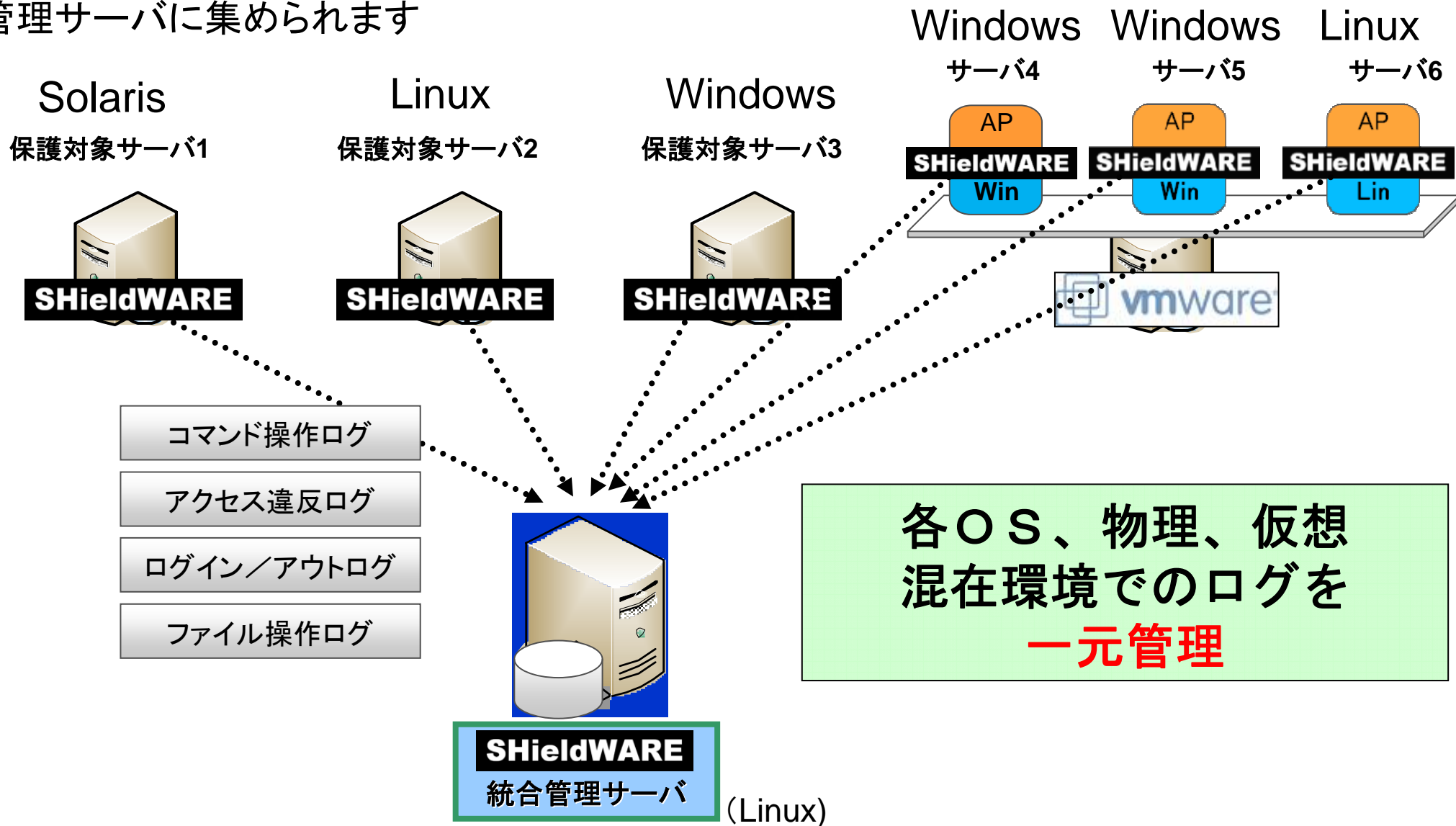


システム管理者も強制の対象

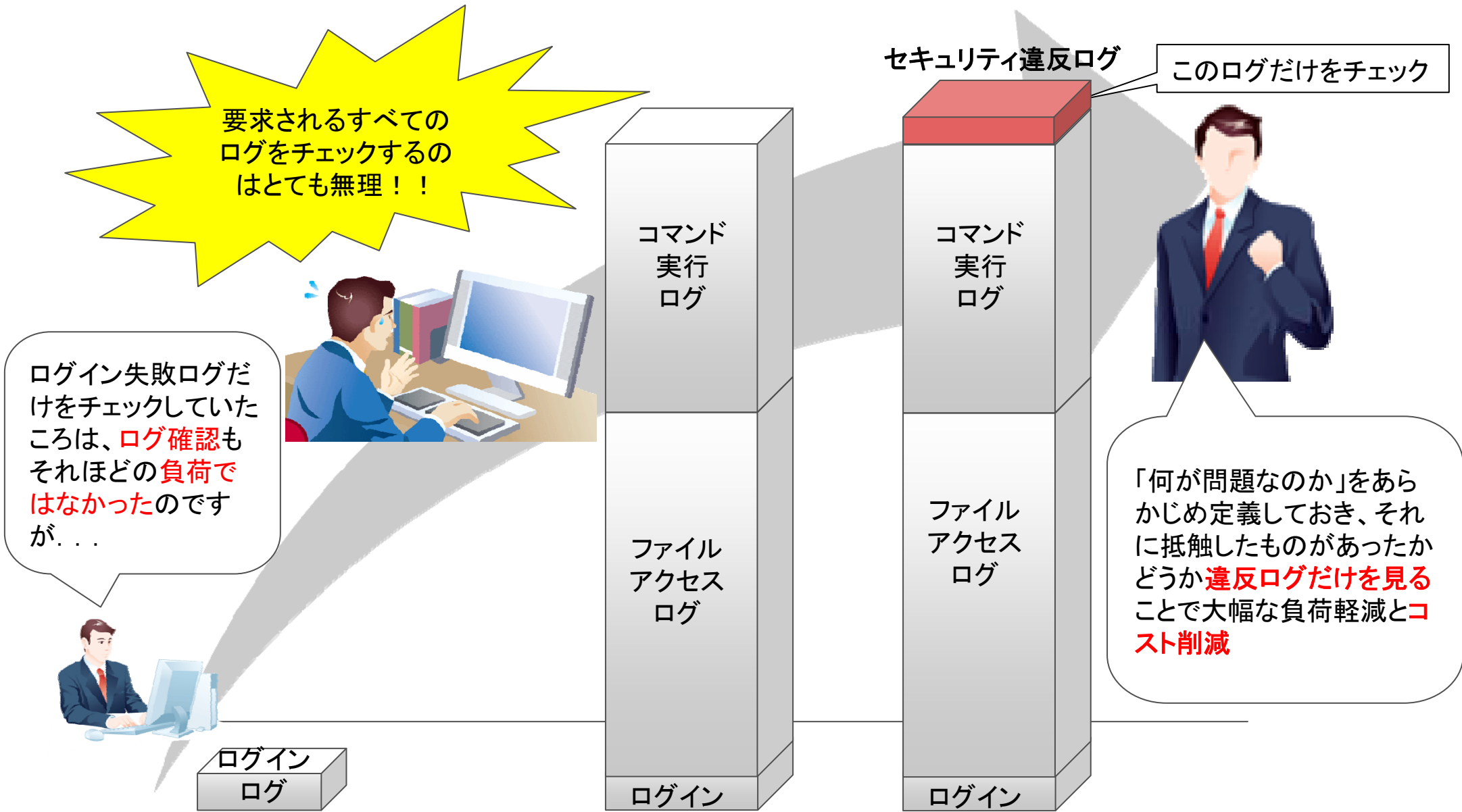
フォルダ／ファイルを選択、付与したい権限をチェック

ログの統合管理

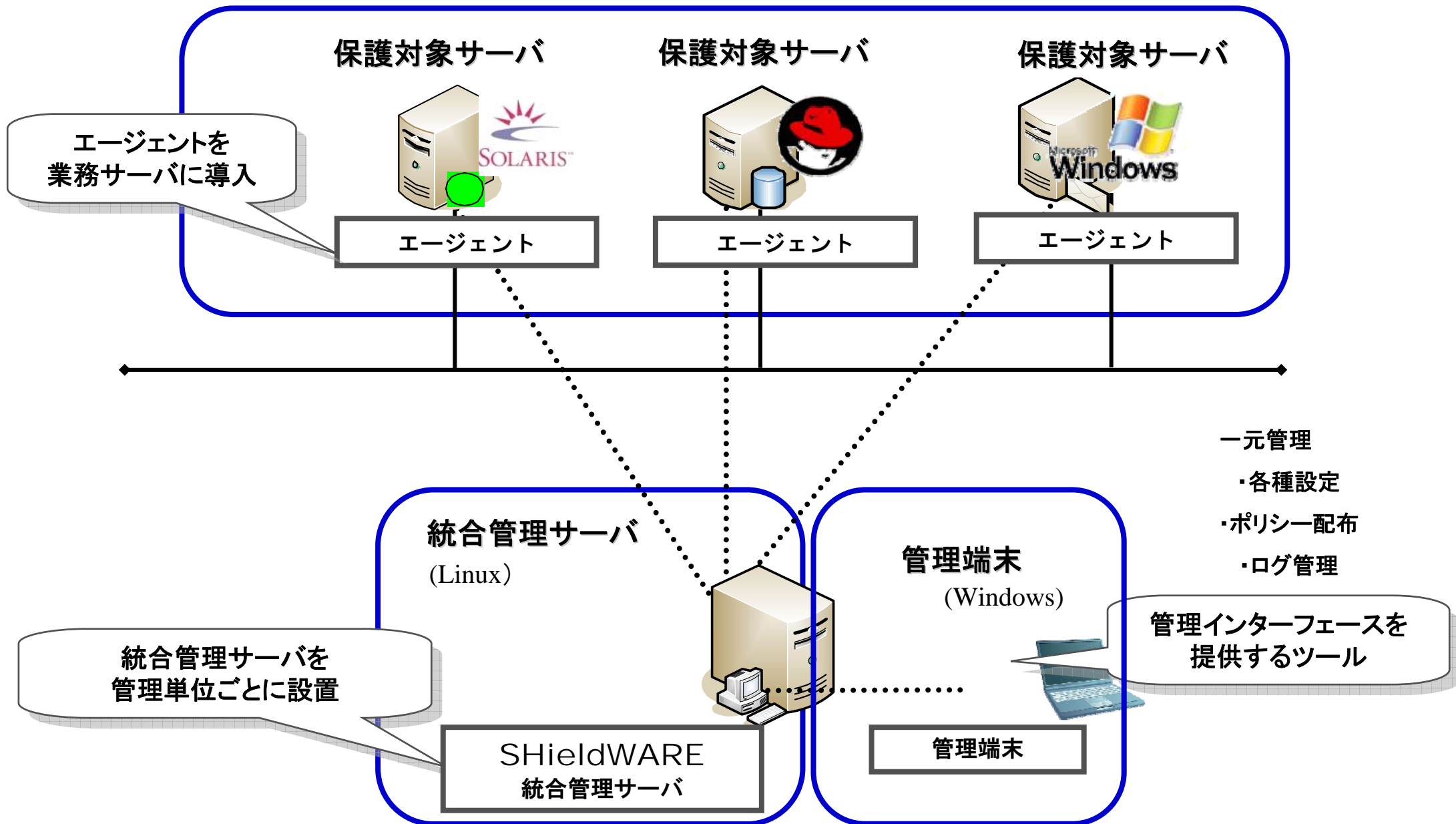
ログは各サーバ上に存在するのではなく、**リアルタイム**に管理サーバに集められます



不正アクセスログによりログレビューを効率化する



SHieldWARE のシステム構成



SHieldWARE V02L05 サポートOS

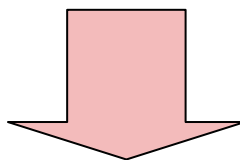
モジュール	サポートOS		
	名称	バージョン	
エージェント	Solaris™ Operating System	SPARC	8-10
	Red Hat Enterprise Linux	AS/ES v.4(x86, Intel64, Itanium)	4.0-4.8
		5(x86, Intel64, Itanium)	5.0-5.5
	Microsoft® Windows Server®	2003/2003 R2(x32, x64)	○
		2008(x32, x64)	○
		2008 R2(x64)	○
統合管理サーバ	Red Hat Enterprise Linux	AS/ES v.4(x86, Intel64)	4.0-4.8
		5(x86, Intel64)	5.0-5.5
管理クライアント	Microsoft® Windows®	2003/2003R2, 2008/2008R2, XP, Vista, 7	

仮想環境向けに価格改定

SHieldWARE V02L05 製品構成

		製品名称	標準価格	
エージェント	SHieldWARE V2 エージェント (1CPUサーバ用)(1-199)※	Solaris用	550,000円	
		Linux用	550,000円	
		Windows用	550,000円	
統合管理サーバ	SHieldWARE V2 統合管理サーバ	Linux専用	550,000円	
管理クライアント		Windows専用	(統合管理サーバに含む)	

※エージェントは対象機器に搭載されているCPUソケット数及び対象台数により1台当りのライセンス価格が異なります。詳細は弊社営業にまでお問合せください



仮想環境(ゲストOS)向けライセンス

クラウド環境にも適用可能

		製品名称	標準価格	
エージェント	SHieldWARE V2 エージェント (ゲストOS用)(1-2CPU用)	Linux専用	280,000円	
		Windows専用	280,000円	

※ホストOS(ペアレントOS)には対応していません。また、富士通ではHyper-V環境でのLinuxのサポートは行っておりません。

導入事例 A官庁様

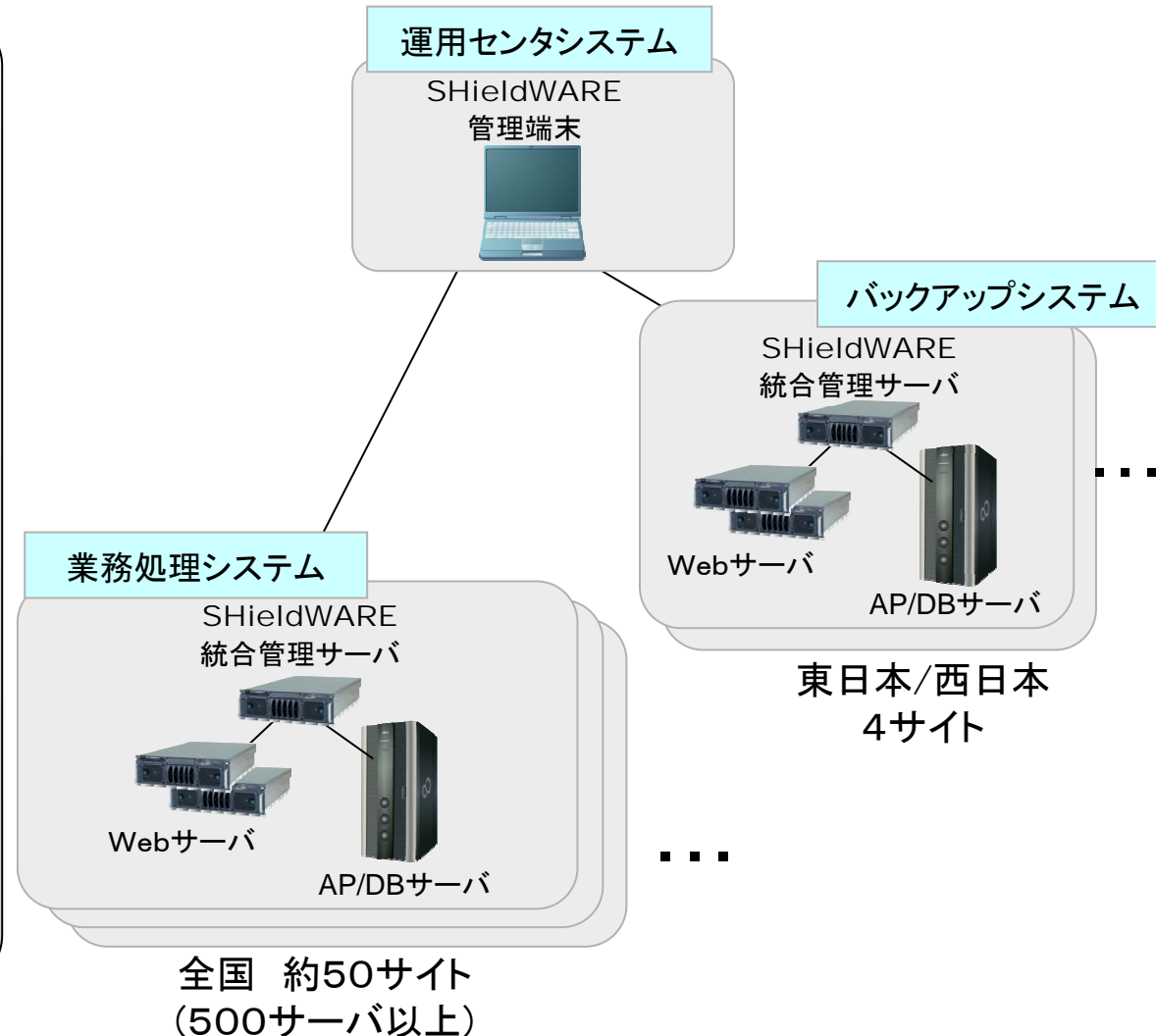
全国に配置されたSHieldWAREエージェントと統合管理サーバを、運用管理センターに設置されたSHieldWAREの管理GUIから集中管理・監視

顧客要件

- ・ログの改ざん防止
- ・特権ユーザー(root)の権限分離

SHieldWAREでの実現

- ・全サーバのsyslogを保護
- ・Webサーバでアプリケーションログを保護
- ・APサーバで業務プログラムログを保護
- ・運用管理者と一般ユーザーのアクセス権を制御



導入事例 B金融機関様

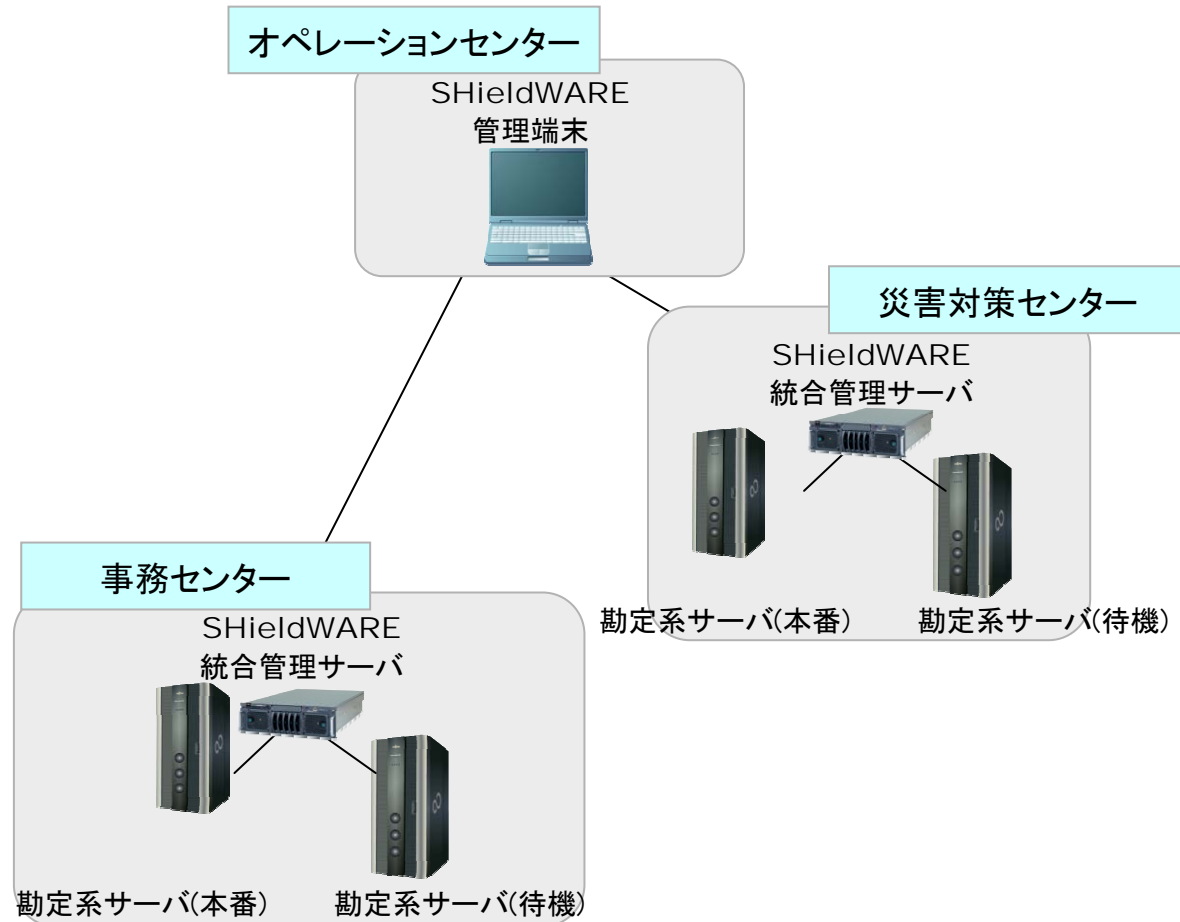
勘定系サーバにSHieldWAREエージェントを導入し、ベンダーを含むシステム管理者の操作記録を取得

顧客要件

- ・システム管理者の操作監査
- ・重要ファイルの改ざん防止

SHieldWAREでの実現

- ・全サーバのsyslogを保護
- ・システム管理者の操作をSHieldWAREのログとして取得
- ・ログを日次で印刷してレビューと承認を実施
- ・一部、システムファイルのアクセス制限



[参考]SHieldWAREの動作モード

以下の動作モードがあり、様々な場面で活用できます。


動作モード	セキュリティチェック	ログ取得	利用例
セキュリティモード	○	○	通常動作
テストモード	×	○	システムテスト時の 設定内容チェック
チェック停止	×	×	ハード障害時の ディザスタリカバリ時

株式会社 **富士通** ソーシャルサイエンスラボトリー
(富士通SSL)

<http://www.ssl.fujitsu.com>

E-mail : ssl-info@cs.jp.fujitsu.com

TEL : 044-739-1251



FUJITSU

shaping tomorrow with you