

FIT2011 ゾーンセミナー
C-10

WEEDS

TRUE TECHNOLOGY TO THE WORLD

**情報漏えい事件の「手口とその対策」
～手口から見える真のセキュリティ具体策～**

2011年10月20日(木)

営業本部

セールス&コンサルティング第1部 田口 孝貴

セールス&コンサルティング第3部 照山 祐一

環境変化対応型情報処理技術集団
ウィーズ・システムズ株式会社

■ Windows系

- ①USBメモリー持ち出し(レジストリーキー設定解除)
- ②セーフモードによる情報持ち出し
- ③Excelファイルパスワードロック解除

■ UNIX, Linux系

- ④OS標準ログの改ざん(wtmp、history)
- ⑤パスワード・クラック

■ データベース

- ⑥痕跡を残さないDBアクセス

■ プログラム変更

- ⑦不正な情報アクセスによる情報持ち出し & 改ざん

①

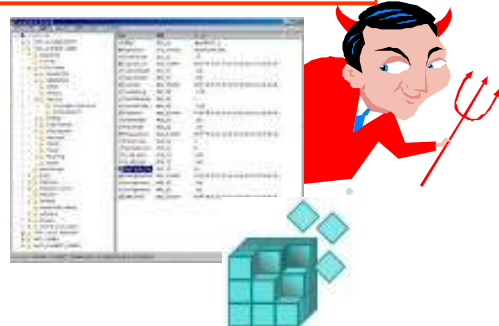
USBメモリー持ち出し
(レジストリーキー設定解除)

①USBメモリー持ち出し (レジストリーキー設定解除)

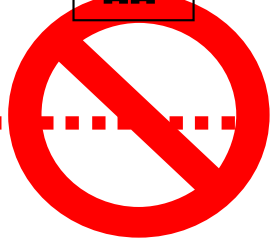
問題点



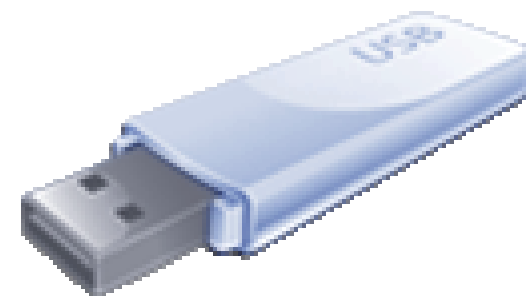
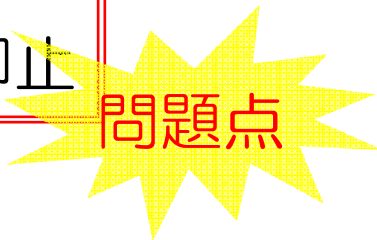
レジストリ
設定解除



操作抑止製品



レジストリー
キーによる抑止

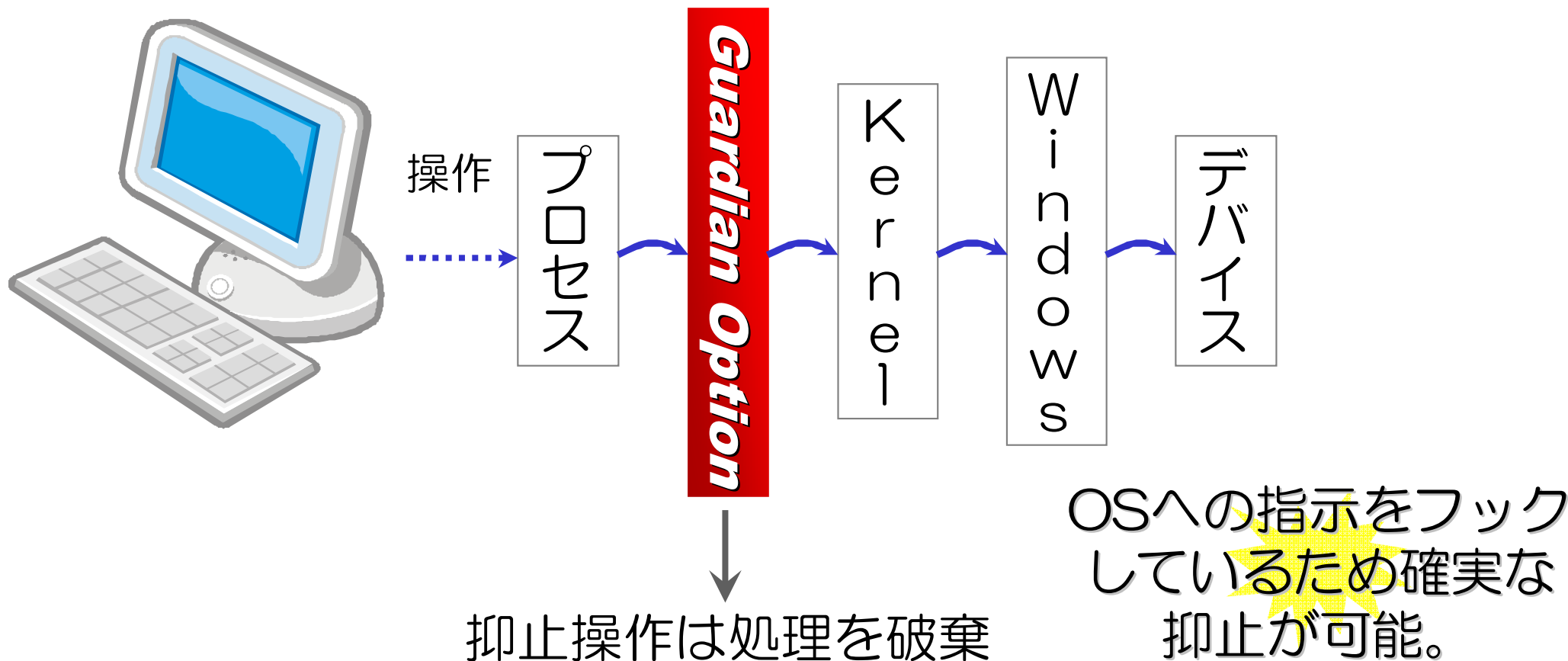


レジストリ設定の変更
で書込みは可能。

①USBメモリー持ち出し (レジストリーキー設定解除)

解決策

WEEDS Windows-SecureControl



②

セーフモードによる
情報持ち出し

②セーフモードによる情報持ち出し

問題点

通常ログイン



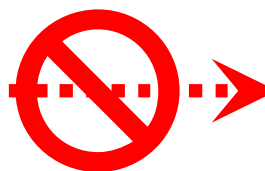
操作ログ取得製品

セーフモード
非対応

問題点

操作
ログ

セーフモード



操作
ログ

セーフモードでは
プロセスが立ち上がらない。



②セーフモードによる情報持ち出し

解決策

GUI操作



セーフモード

WEEDS Windows-SecureControl

セーフモード
に対応

操作
ログ

操作
ログ

③

Excelファイル パスワードロック解除

③Excelファイルパスワードロック解除

問題点

Excelのパスワードに
頼ったセキュリティ

問題点

サーバの
パスワード管理

不正ログイン

不正に解除
(総当たり攻撃でない)

③Excelファイルパスワードロック解除

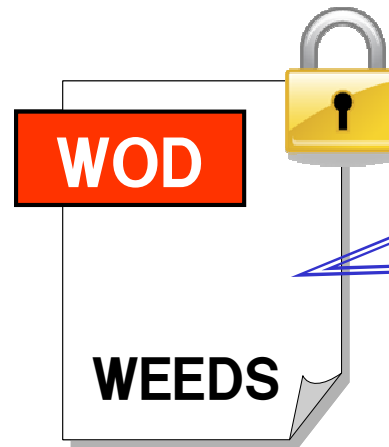
WEEDS

解決策

WEEDS Office-Doc



自動変換



日次で以下を実行

- ・暗号化
- ・パスワードロック
- ・有効期限設定

パスワードは製品が管理し、問合せ履歴が残る。

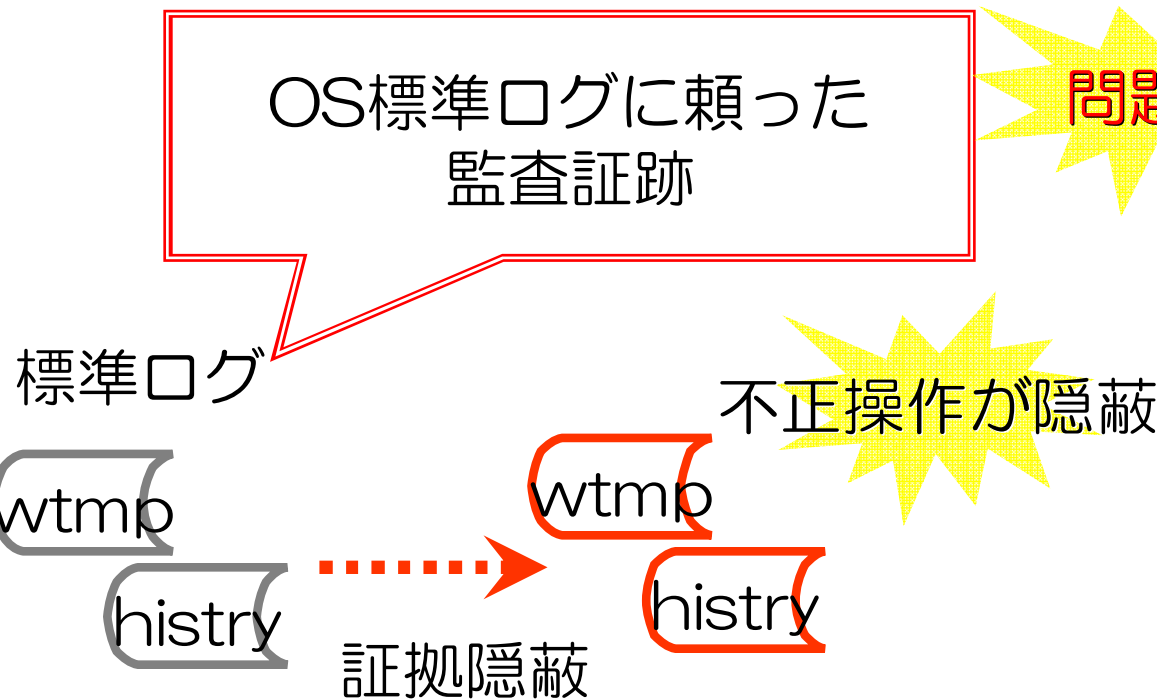
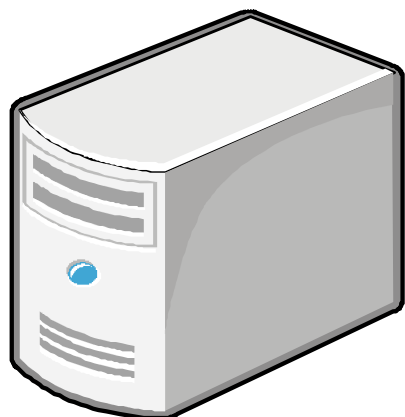
④

OS標準ログの改ざん (wtmp、history)

④OS標準ログの改ざん (wtmp、histry)

問題点

UNIX, Linuxサーバ



世に出回っている

改ざんツール



④OS標準ログの改ざん (wtmp、histry)

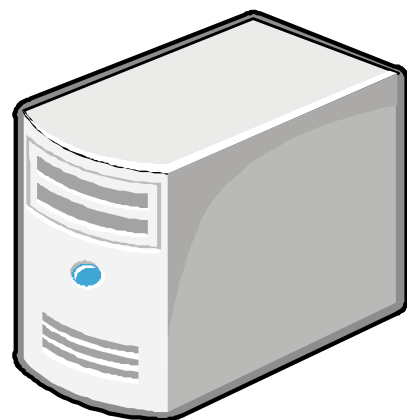
WEEDS

解決策

標準ログを使用せず、操作ログは瞬時に退避する。

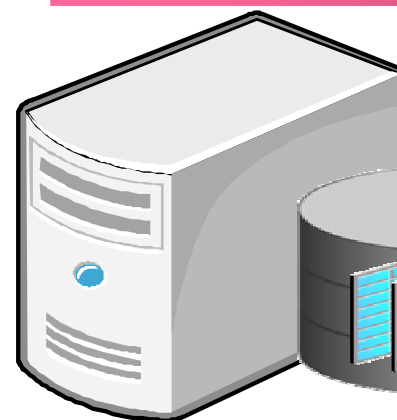
**WEEDS
UNIX-Trace**

**WEEDS Log-
Repository Manager**



操作
ログ

瞬時に転送



ログサーバ

発行コマンド数によって
ログ転送を指定。

⑤

パスワード・クラック

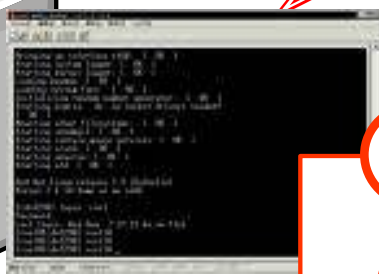
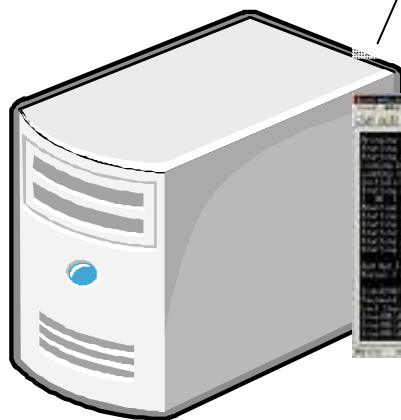
⑤パスワード・クラック

問題点

ログイン失敗(オンライン攻撃)を
チェックするだけではわからない

問題点

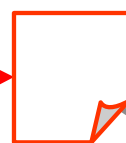
/etc/shadowファイル



持出し



解除



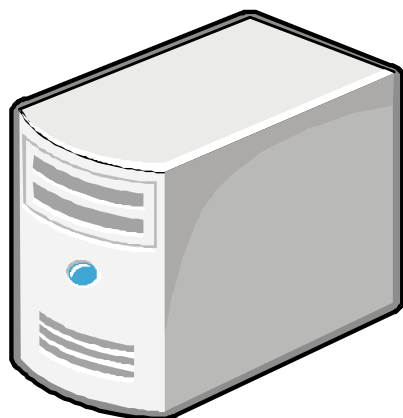
オフライン攻撃

世にパスワード
クラックツール
出回っている

⑤パスワード・クラック

解決策

**WEEDS
UNIX-Trace**

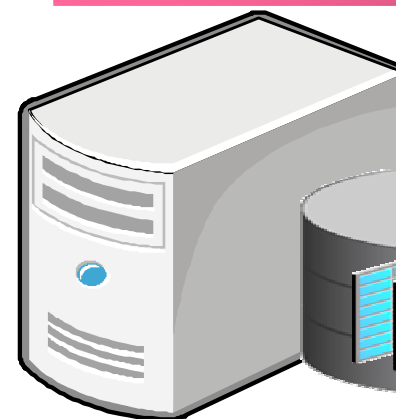


操作
ログ



すべての操作ログを取得
することはもはや必須。

**WEEDS Log-
Repository Manager**



ログサーバ



重要ファイル
アクセスレポート

⑥

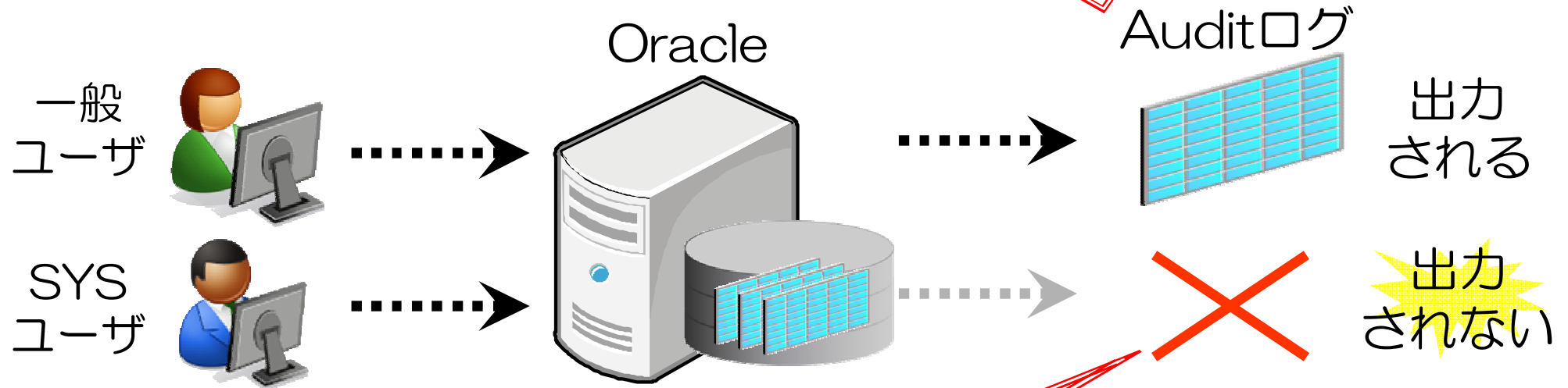
痕跡を残さないDBアクセス

⑥ 痕跡を残さないDBアクセス

問題点

Auditログに頼った
監査証跡の保持

問題点

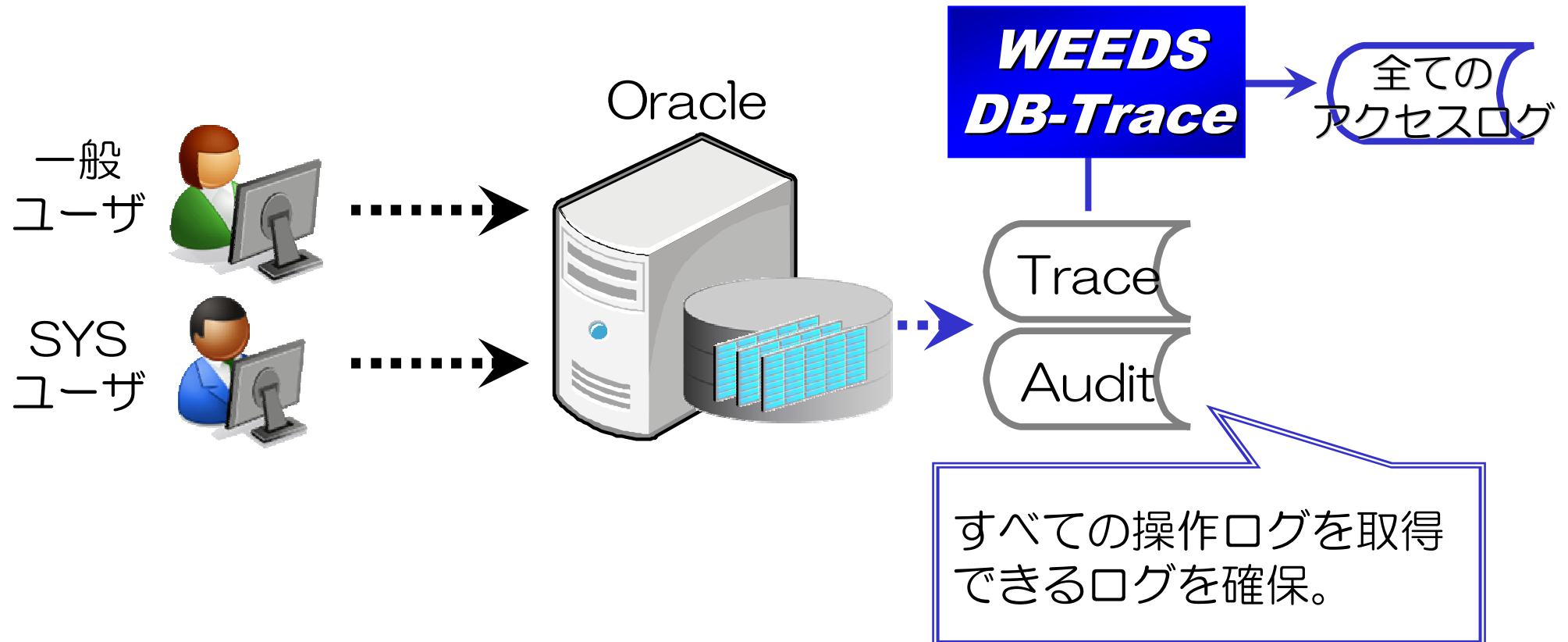


SYSユーザの操作は
Oracle Auditテーブルに
は残らない。

⑥ 痕跡を残さないDBアクセス

WEEDS

解決策



⑦

不正な情報アクセスによる
情報持ち出し&改ざん

⑦不正な情報アクセスによる情報持ち出し & 改ざん

問題点

個人の利権関わる情報への
操作ログを保持していない。

問題点

タイムカード

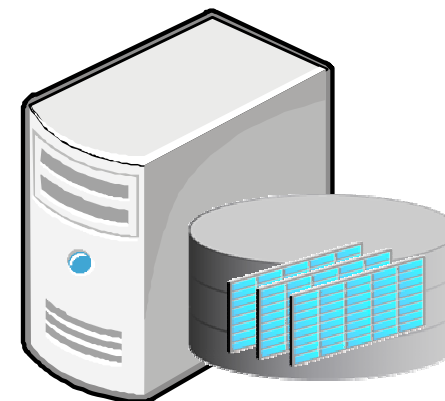


転送

勤怠情報
(CSV)

取込

給与システム



情報改ざん



⑦不正な情報アクセスによる情報持ち出し & 改ざん

解決策

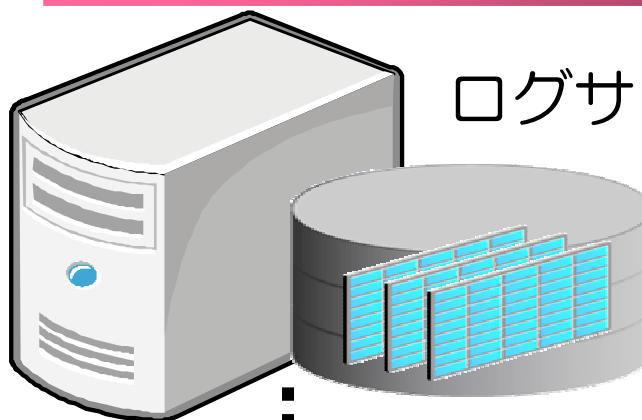
すべての操作ログを取得することはもはや必須。

**WEEDS
WinServer-Trace**

**WEEDS Log-
Repository Manager**

操作
ログ

ログサーバ



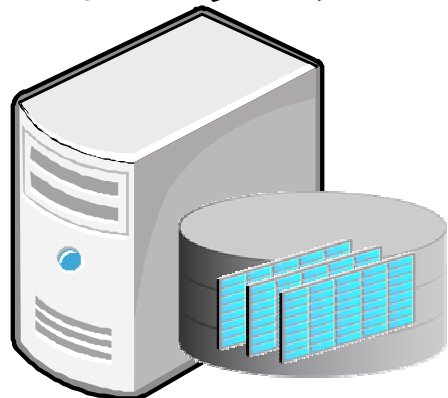
重要ファイル
アクセスレポート



⑦不正な情報アクセスによる情報持ち出し & 改ざん

問題点

個人情報格納
システム

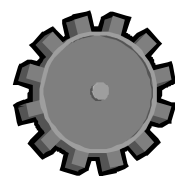


アプリケーションの追加・変更を検知していない。

問題点

不正プログラム

情報取得



個人情報

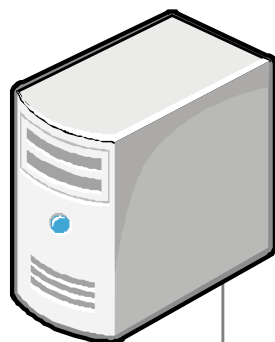
外部へ
持ち出し

不正プログラムの
配置

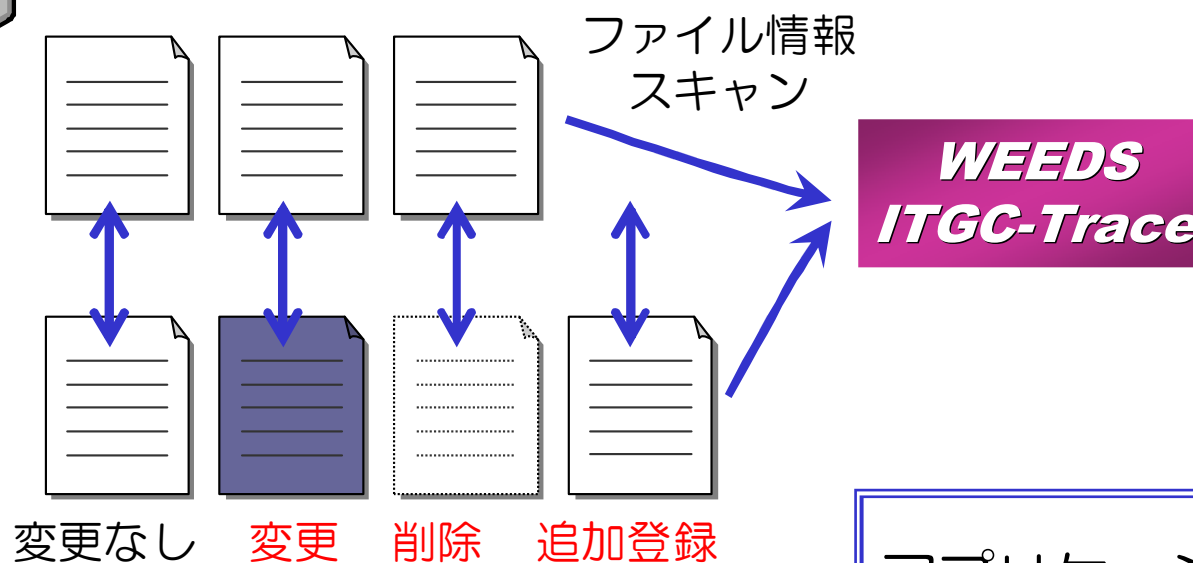


⑦不正な情報アクセスによる情報持ち出し & 改ざん

解決策



アプリケーションサーバ（お客様監査対象）



アプリケーションの変更
をモニタリング

お 知 ら せ

ニュース:みずほ情報総研様と共同開発

WEEDS



The screenshot shows the Mizuho Information & Research Institute website. At the top is the Mizuho logo. Below it is a navigation menu with links for Home, English, Site Map, Solution Introduction, Case Studies/Performance Introduction, Columns/Publications, Events/Seminars, About Mizuho Information & Research Institute, Company Information, CSR Initiatives/Activities, and News Release. The News Release link is highlighted. Below the navigation is a breadcrumb trail: Home > About Mizuho Information & Research Institute > News Release > 2011 News Release > Mizuho Information & Research Institute and Weeds Systems, Tracer for Salesforce joint development. The main heading reads: "年内にみずほ情報総研から販売開始予定" (Sales start planned within the year) and "みずほ情報総研とウイズ・システムズ、Tracer for Salesforceを共同開発" (Joint development of Tracer for Salesforce by Mizuho Information & Research Institute and Weeds Systems).

2011年10月14日
みずほ情報総研株式会社

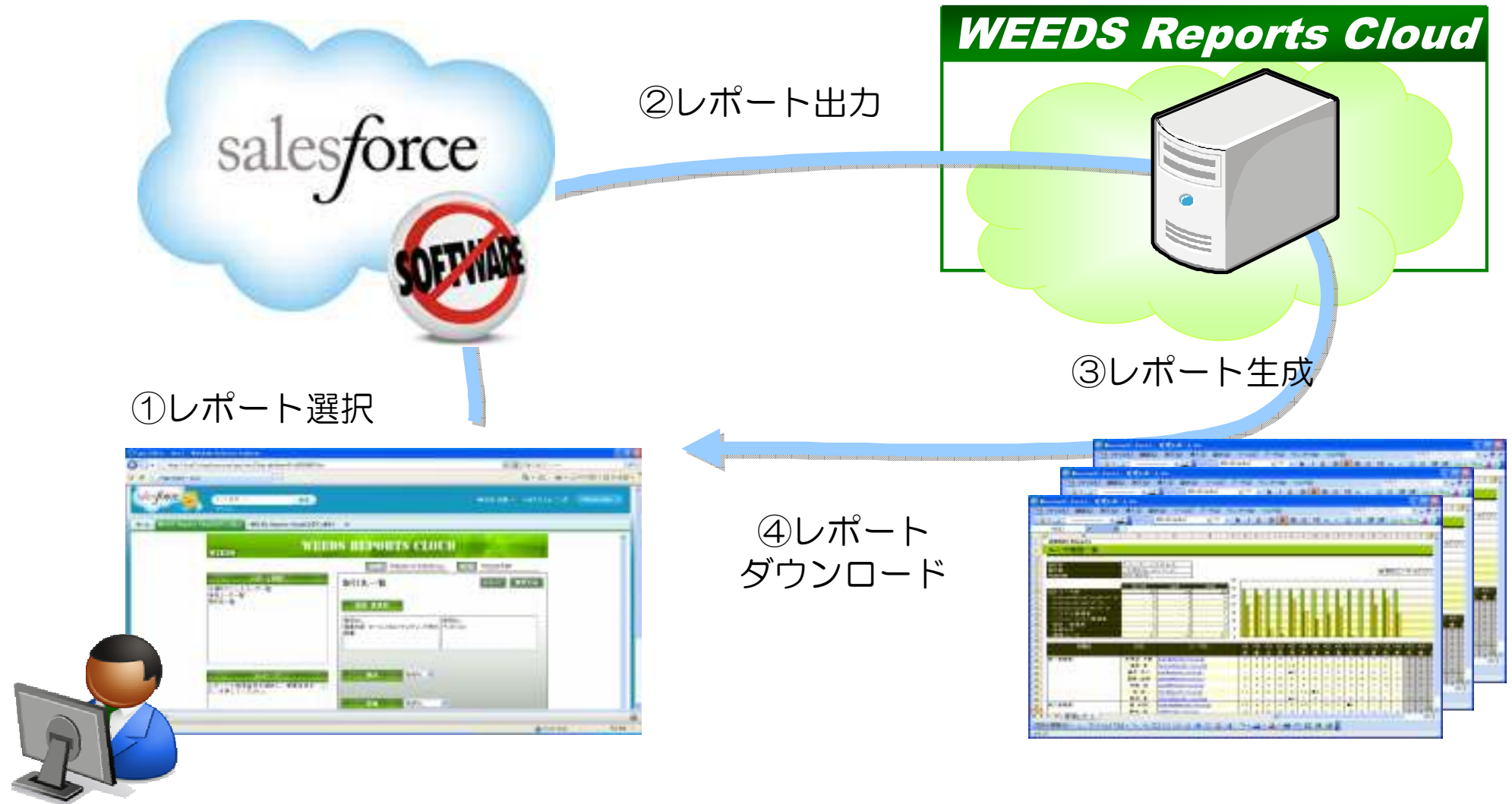
みずほ情報総研株式会社(本社:東京都千代田区、代表取締役社長:井上 直美)とウイズ・システムズ株式会社(本社:東京都豊島区 代表者:豊嶋 正裕)は、今般、『Tracer for Salesforce』を共同開発し、みずほ情報総研から年内の発売を予定しています。

みずほ情報総研は数多くの金融機関へのSalesforce(クラウド型 営業支援・顧客管理 CRMサービス)導入実績を誇っております。金融機関では金融庁監修の「金融分野における個人情報保護に関するガイドライン」において個人データへのアクセスの記録及び分析を実施することを求められております。そのため、個人データを取扱うSalesforceの操作ログ



ニュース：帳票生成クラウドサービス開始

WEEDS



ご清聴いただき、誠にありがとうございました。

ブース A-19にて
ご質問、ご相談お受けいたします。



人事部長

■ 開発・販売

ウィーズ・システムズ株式会社

〒171-0033

東京都豊島区高田1-36-10 アベックヒルズ目白

本社301号/開発センター302号/Show Room202号

TEL /FAX 03-5950-6350

URL : <http://www.weeds-japan.co.jp>

会社概要	会社名	ウイーズ・システムズ株式会社
	英文名	WEEDS SYSTEMS Inc.
	設立	2003年1月8日
	社員数	10名(2011年4月現在)
	決算期	12月

営業内容 ソフトウェア製品開発・販売、受託開発およびコンサルティング

製 品	WEEDS BI-Framework	WEEDS Trace Series
	WEEDS Reports	WEEDS DB-Trace
	WEEDS Data Collector	WEEDS UNIX-Trace
	WEEDS Web Library	WEEDS Windows-Secure Controll
	WEEDS Office Doc	WEEDS WinServer-Trace
	WEEDS Disk Crush	WEEDS ITGC-Trace
		WEEDS SAS-Trace
		WEEDS DynamicsCRM-Trace