

経済産業省からの提言「情報セキュリティガバナンス導入ガイドンス」
～ 具体的な情報セキュリティ対策の推進とは～

2009年9月4日(金)

営業部 田口 孝貴

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

経済産業省「情報セキュリティガバナンス導入ガイドンス」
で書かれていることの紹介

しかし本ガイドンスには、

セキュリティガバナンス（統治）の、

- 必要性
- 怠った場合のリスク
- 責任範囲
- 評価

といった概要しか書かれていない。

そのため本セミナーでは、

「情報セキュリティガバナンス導入ガイドンス」で定められている「情報セキュリティ」の定義より、

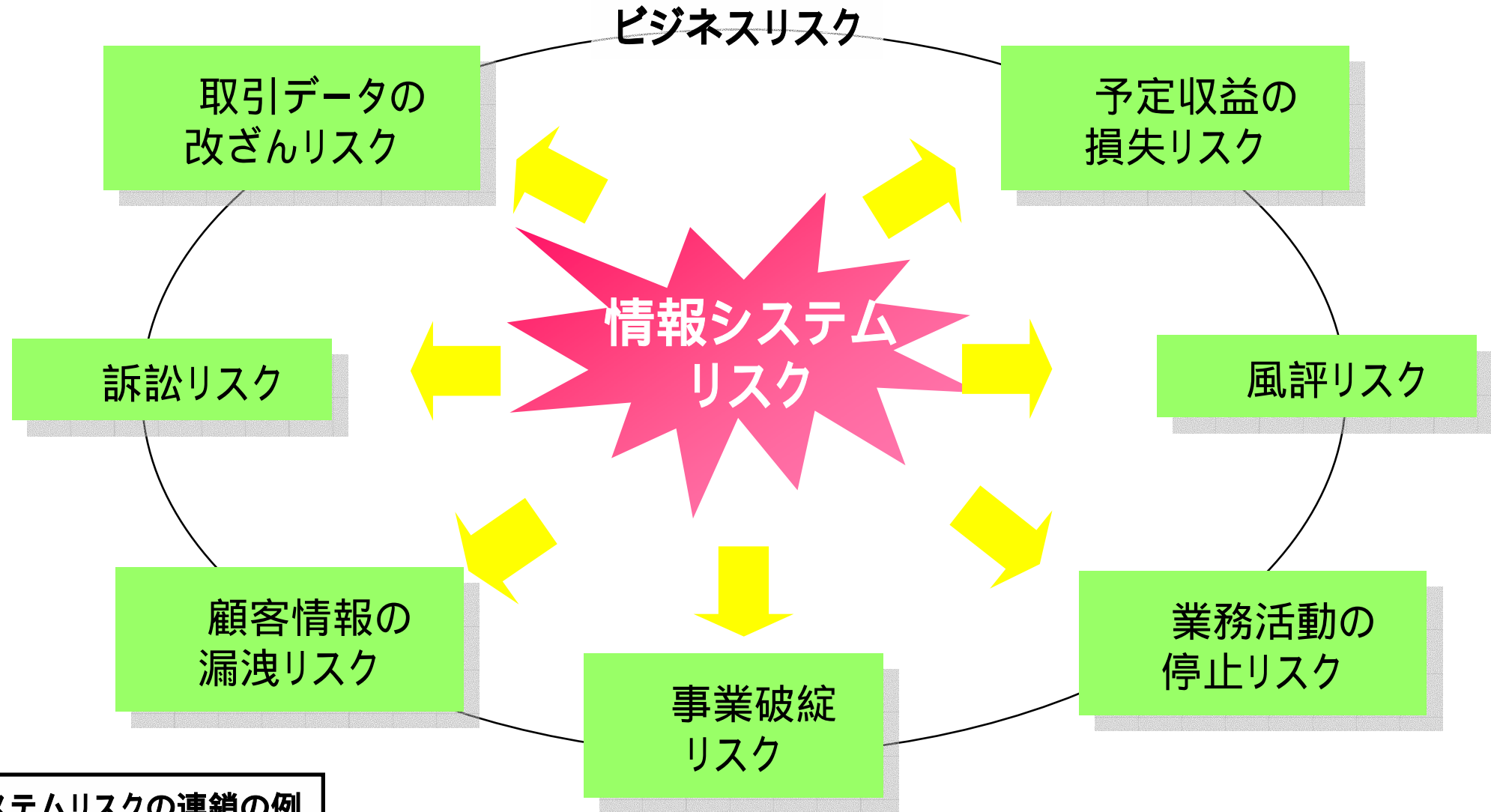
- 具体的な対策例
- 企業におけるセキュリティ対策の実態
- あるべきセキュリティ対策

をご紹介します。

会社概要	会社名	ウイズ・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	15名(2009年8月現在) 平均年齢30歳
	決算期	12月

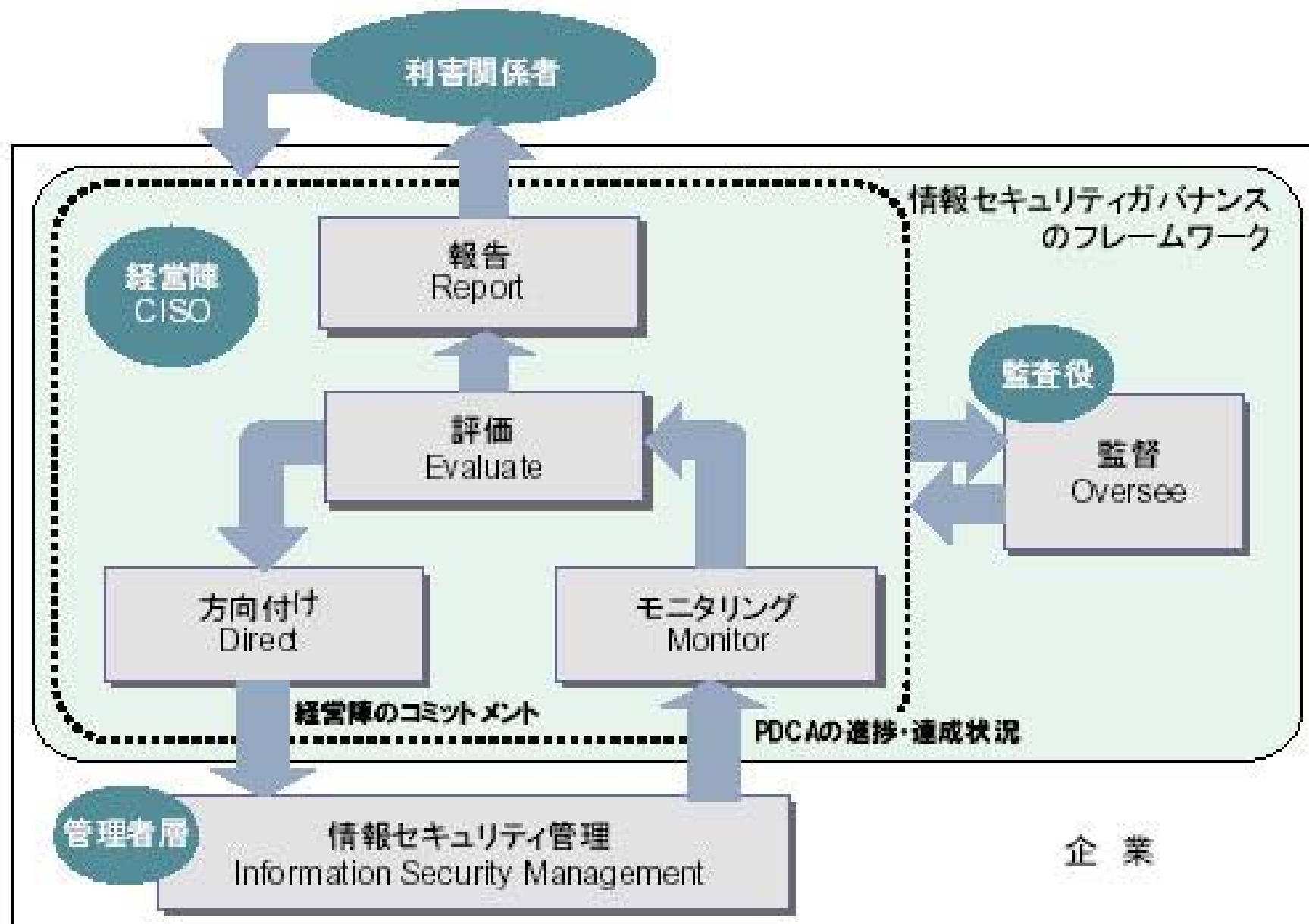
営業内容 ソフトウェア製品開発・販売、受託開発およびコンサルティング

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

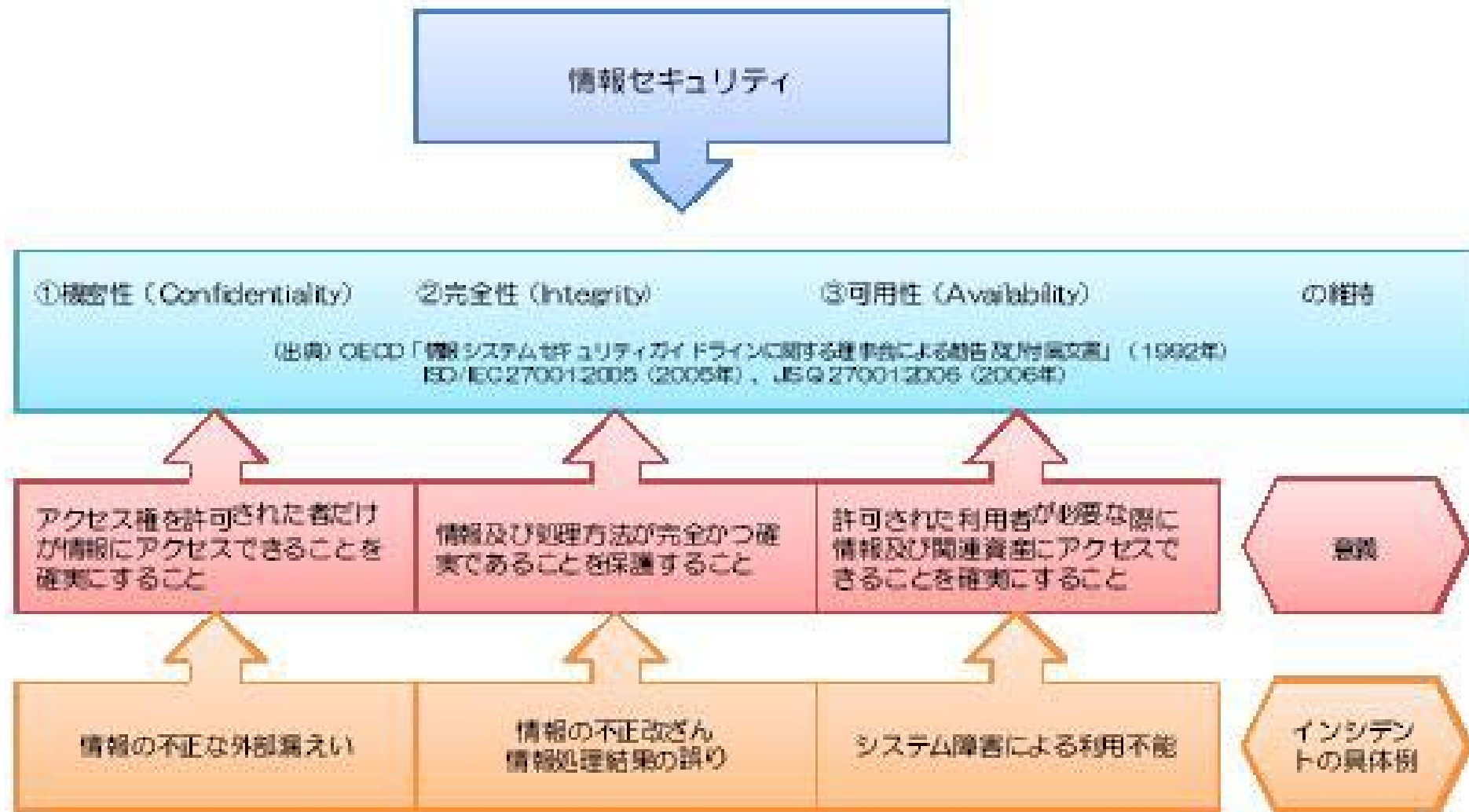


情報システムリスクの連鎖の例

FISC: 金融機関等のシステム監査指針第3版より抜粋

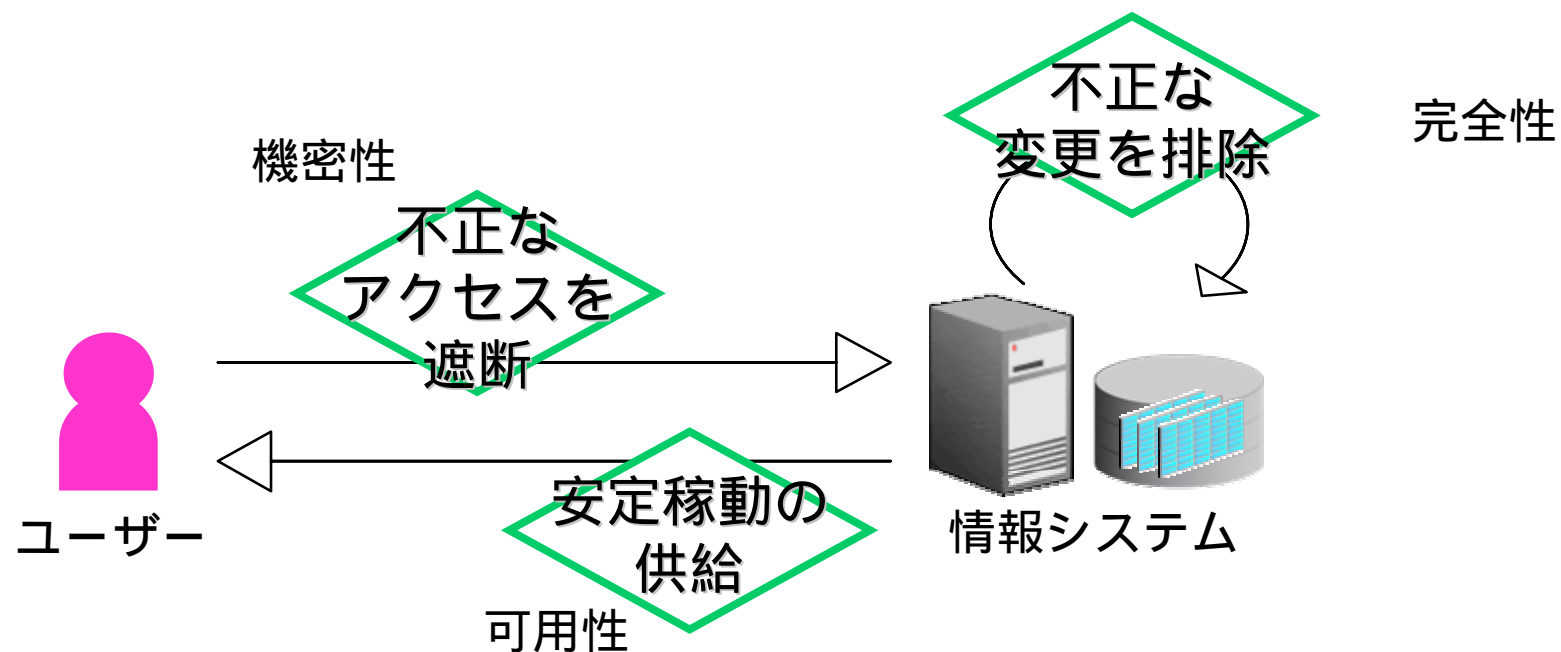


経済産業省「情報セキュリティガバナンス導入ガイダンス」より抜粋



経済産業省「情報セキュリティガバナンス導入ガイダンス」より抜粋

機密性、 完全性、 可用性（CIA）を維持すること。



システム障害による利用不能や情報の不正改ざん、
情報漏えい等を防止するために重要な機能を担うもの。

定義

アクセス権を許可された者だけが情報にアクセスできることを確実にすること。

対策例

IDやパスワードにより、不必要に誰でも情報へアクセスできないようにする。



問題点

「許可された者のアクセスは不正がない」
ことが前提の対策。

アクセスを許可された者の不正アクセス事件が
絶えない昨今では、この対策では不十分。

定義

アクセス権を許可された者だけが情報にアクセスできることを確実にすること。



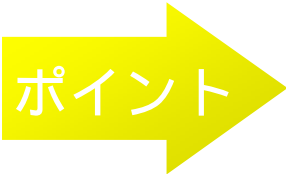
アクセス
コントロール

+

許可された者のアクセスに、不正がないことを確認すること。



アクセス
監査



「アクセスコントロール」と「アクセス監査」の両方が同時に機能して初めて機密性が保たれる。

定義

情報及び処理方法が完全かつ確実である
ことを保護すること

どう
やって？

問題点

運用やメンテナンスで、アクセスは必ずある。
アクセスがあっても不正か否かは判断不可能。

データやアプリケーションに不正な
変更がないよう保護することは非現実的。

定義

情報及び処理方法が完全かつ確実である
ことを保護すること

対策

情報システムに不正な改ざんが
ないか、事後チェックする。

アクセス
監査

ポイント

不正か否かは事前にはわからない。
だから、事後にモニタリングが必須となる。

定義

許可された利用者が必要な際に情報及び関連資産にアクセスできることを確実にすること

インシデントの例

・ システム障害による利用不能

例) 人的ミスによるシステム障害

- 操作ミス
- 不正アタック など

強化し過ぎると業務遂行に負担に

対策

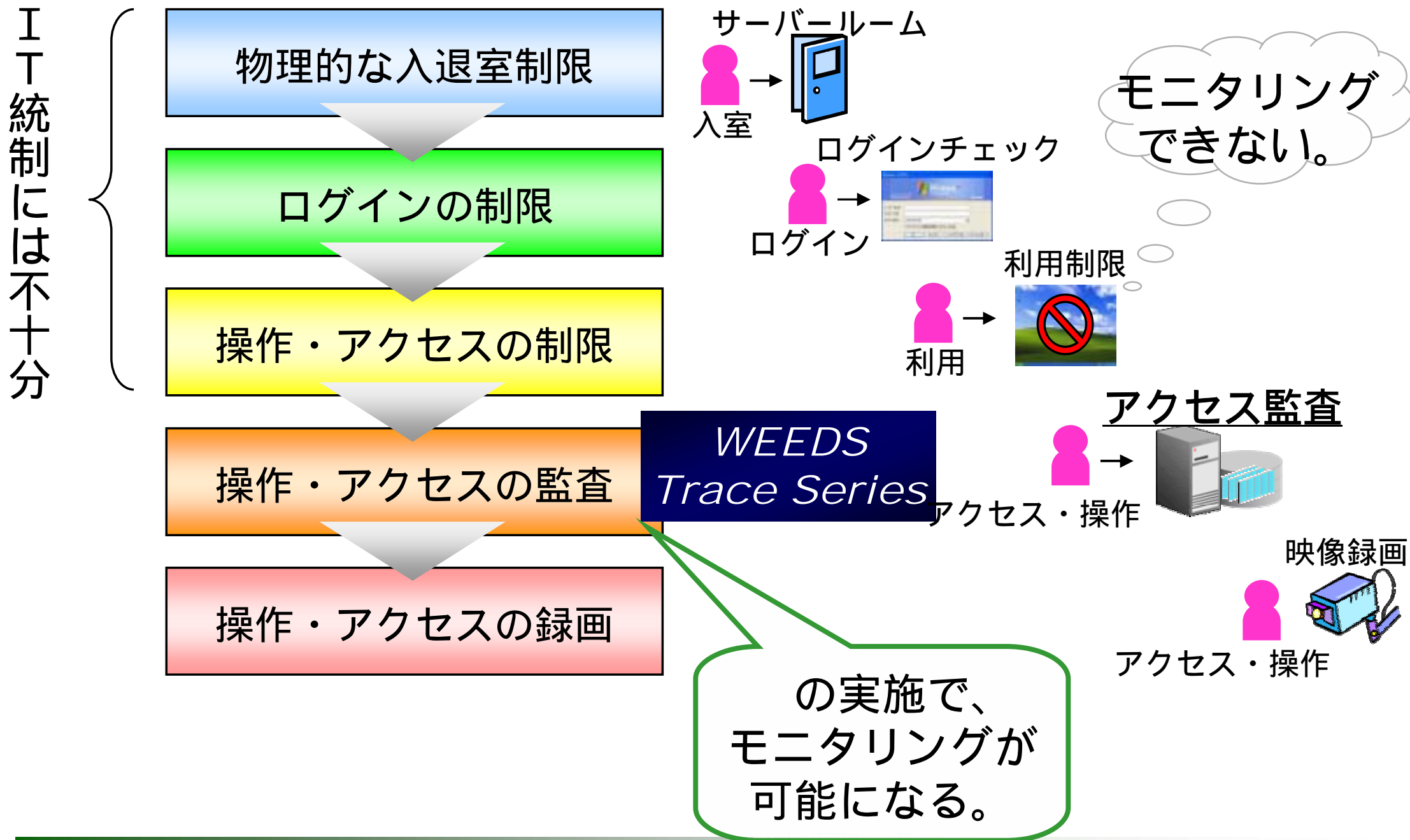
アクセス
コントロール

アクセス
監査

<

予防的
統制

発見的
統制



- ・ 多くの企業が、 ~ までのアクセスコントロールは実施している。
- ・ 昨今の情報漏えい事故は、許可された者の不正アクセスが原因。

アクセスコントロールでは防げない！

- ・ アクセス監査を実施しなければ、情報漏えい事故を防ぐことはできない。

アクセス監査の実施は、もはや必要不可欠に。

過去の情報漏えい事件を振り返ると、

最近の情報漏えい事件

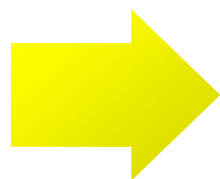
2009年7月	アリコジャパン	最大11万件	内部犯罪
2009年4月	三菱UFJ証券	148万件	内部犯罪

過去の大きい情報漏えい事件

2007年3月	大日本印刷	863万名	内部犯罪
2007年3月	UFJニコス	119万件	内部犯罪
2007年3月	アメリカンホーム 保険	150万件	内部犯罪
2006年12月	日産自動車	最大537万名	内部犯罪
2006年6月	KDDI	399万名	内部犯罪

漏えいの原因 73%が「内部から」、21%が「外部から」

1. 全てのアクセスをモニタリングできる環境の構築
 - ✓ 情報システムへの全てのアクセスログを収集。
 - ✓ モニタリングできる形でアクセスログを収集することがポイント。（見てもわからない、情報不足、のログは収集しても意味がない）
2. モニタリング実施の社内告知
 - ✓ 不正抑止、操作ミス防止効果が見込める。
3. モニタリングの実施
 - ✓ 収集したログを的確な形、タイミングでレポートニングする。
4. 業務の改善
 - ✓ レポートから不用意なアクセス経路を是正する。



WEEDS Trace Series

で容易に実現可能。

アクセスログの暗号化

アクセスログから情報漏えいする危険性がある。

誰でもアクセスログを参照できる環境は、金庫に鍵をかけないのと同じ

自動暗号化、ワンタイムパスワードなど、基本は自動化すること

ログの暗号化は必須事項！

ログから情報漏えいしたら本末転倒です。

・ 監査したいアクセスに絞って監査する。

情報漏えい対策 : 個人情報への“参照”

不正改ざん対策 : データへの“追加、更新、削除”

ただログを収集してもダメ。
意味のある形でログを収集して、
かつレポートिंगすることが重要！

アクセスログを収集するには、

WEEDS

・ 個人情報情報が格納されている場所は、

データベース

WEEDS DB-Trace

ファイルサーバー

WEEDS Office Doc

・ 不正な操作を発見するには、

サーバーの操作ログを収集

WEEDS Windows-Trace

・ OS (WindowsやLinux、UNIX)

WEEDS UNIX-Trace

・ プログラムの不正変更も重要な監査

プログラムがいつ変わったかを収集

WEEDS ITGCTrace

アクセスログ監査への具体的な対処方法

WEEDS

Windows



2000
XP
2003Svr
Vista
2008Svr

操作記録取得

WEEDS Windows-Trace

プログラム登録 / 変更記録取得

UNIX、Linux

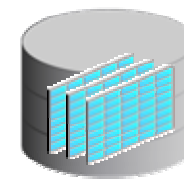


AIX
Solaris
HP-UX
Redhat
MIRACLE

操作記録取得

WEEDS UNIX-Trace

データベース



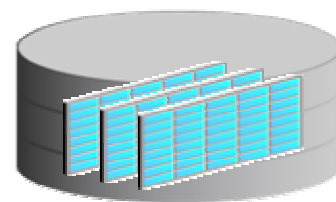
Oracle
SQL Server
DB2
Teradata

DBアクセス取得

WEEDS DB-Trace

WEEDS ITGC-Trace

ログリポジトリサーバー



アクセスログ

WEEDS LOG Repository Manager

- データベースアクセス（SQL）を全て漏れなく収集することは必須。
- SQLを単に保持していても監査はできない。
- SQLを分析して、
 - どの情報（テーブル）の、
 - どの項目（フィールド）に、
 - どんな条件（Where句）で、
 - どんなアクセス（アクション）をしたか
- 膨大なアクセスログを1件1件監査することは非現実的。
- 監査したい情報へのアクセスを抽出して監査することが重要。（月間集計など）

WEEDS DB-Traceの監査レポート



Microsoft Excel - DBT月次レポート.xls

ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) ツール(T) データ(D) ウィンドウ(W) ヘルプ(H) 質問を入力してください

校閲結果の返信(C)... 校閲結果の差し込み終了(N)... Arial Black 14 B I U

A1 WEEDS DB-Trace

WEEDS DB-Trace															
月間アクセス集計：アプリ、端末ユーザー、テーブル別															
監査対象月	2008/07														
監査対象DB	ora92														
アクセス種別	追加数+更新数+削除数														
アプリ	端末ユーザー	テーブル	1日	2日	3日	4日	5日	6日	7日	8日	9日	10日	11日	12日	
			火	水	木	金	土	日	月	火	水	木	金	土	
NotAppList	oracle	LBAD\$USER	0	0	0	2	0	0	0	0	0	0	0	0	0
		SDO_GEOM_METADATA_TABLE	0	0	0	5	0	0	0	0	0	0	0	0	0
osqledit.exe	ryamazaki	PLAN_TABLE	0	0	0	1	0	0	0	0	0	0	0	0	0
		WEEDS_ORACLE_ACTION	0	0	0	160	0	0	0	0	0	0	0	0	0
	shizu	顧客マスタ	0	0	0	0	0	0	0	15	0	0	0	0	0
		支店担当者マスタ	0	0	0	0	0	0	0	29	0	0	0	0	0
		商品マスタ	0	0	0	0	0	0	0	50	0	0	0	0	0
		担当者マスタ	0	0	0	0	0	0	0	51	0	0	0	0	0
		売上データ	0	0	0	0	0	0	0	140	0	0	0	0	0
sqlplus.exe	Administrator	WEEDS_AUDIT_ACCESS	0	0	0	13	0	0	0	0	0	0	0	0	
		WEEDS_LOGIN_RELATION	0	0	0	3	0	0	0	0	0	0	0	0	
		WEEDS_LOGIN_SESSION	0	0	0	0	0	0	0	0	0	0	0	0	
		WEEDS_SQL_COMMENT	0	0	0	0	0	0	0	0	0	0	0	0	
		WEEDS_SQL_DESCRIBE	0	0	0	0	0	0	0	0	0	0	0	0	
		WEEDS_SQL_INFO	0	0	0	0	0	0	0	0	0	0	0	0	
WEEDS_SQL_RAW	0	0	0	0	0	0	0	0	0	0	0	0			

アクセスしたアプリケーション、ユーザー、テーブル毎にアクセス統計を監査する。

図形の調整(R) オートシェイプ(U) コマンド NUM

WEEDS DB-Traceの監査レポート



Microsoft Excel - DBT月次レポート.xls

ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) ツール(T) データ(D) ウィンドウ(W) ヘルプ(H) 質問を入力してください

75%

A1 WEEDS DB-Trace

WEEDS DB-Trace 出力日: 2008/07/29

監視テーブル設定一覧

監視対象期間	2007/07/29 ~ 2008/07/29	監視実行	daily_dbt
監視日	2008/07/29	監視ID	daily_dbt_20080729122622
監視時刻	12:26:22		

監査対象DB	監視テーブル	監視フィールド	監視内容	登録部門	登録者	登録ユーザーID	登録日
POSERVER03	V\$PARAMETER	pga_aggregate_size	Where句の条件内容 設定	運用管理部	メンテナンスユーザー	WEEDS	2008/05/19
	KANRI_ユーザー	ユーザーID	監視テーブル及びフィールド設定	開発部	豊嶋正裕	mtoyoshi	2008/05/19
	KANRI_ユーザー	ユーザー名	監視テーブル及びフィールド設定	開発部	豊嶋正裕	mtoyoshi	2008/05/19
	WEEDS_AUDIT_ACCESS	NoField	監視テーブル設定	開発部	豊嶋正裕	mtoyoshi	2008/05/19
	KANRI_ユーザー	undefined	監視テーブル及びフィールド設定	運用管理部	メンテナンスユーザー	WEEDS	2008/05/29
	WEEDS_AUDIT_ACCESS	psserver	Where句の条件内容 設定	運用管理部	メンテナンスユーザー	WEEDS	2008/05/29
	KANRI_ユーザー	NoField	監視テーブル設定	運用管理部	メンテナンスユーザー	WEEDS	2008/05/30
ora92	SYSHARSETS	NoField	監視テーブル設定	開発部	志津公史	tshizu	2008/07/04
	V\$PARAMETER	VALUE	監視テーブル及びフィールド設定	運用管理部	メンテナンスユーザー	WEEDS	2008/05/19
	顧客マスク	NoField	監視テーブル設定	開発部	志津公史	tshizu	2008/06/19
	ALL_ARGUMENTS	teruteru	Where句の条件内容 設定	開発部	志津公史	tshizu	2008/06/19
	商品マスク	NoField	監視テーブル設定	営業部	星光史	mhoshi	2008/06/22
	WEEDS_1755	NoField	監視テーブル設定	営業部	星光史	mhoshi	2008/06/22
	WEEDS_SQL_INFO	NoField	監視テーブル設定	開発部	山崎玲那	ryamazaki	2008/07/04
	NLS_DATABASE_PARAMETERS	NoField	監視テーブル設定	開発部	山崎玲那	ryamazaki	2008/07/04
	WEEDS_LOGIN_RELATION	NoField	監視テーブル設定	開発部	志津公史	tshizu	2008/07/04
	WEEDS_AUDIT_ACCESS	NoField	監視テーブル設定	開発部	志津公史	tshizu	2008/07/04

図形の調整(R) オートシェイプ(U) コマンド

監視すべきテーブル、フィールドの登録状況レポート。
登録しておくことで、監視テーブル、フィールドへのアクセスが発生した場合に瞬時に把握できる。

日次監査

時間外のDBアクセス
監査対象データへのアクセス
DB直接アクセス利用
大量データアクセス
SQL実行失敗
高負荷DBアクセス
利用申請一覧
利用申請コマンド一覧
利用申請/作業実績コマンド
一覧
未申請利用一覧
未申請コマンド一覧

利用分析

データベースアクセス一覧 -ユーザー単位-
データベースアクセス一覧 ログイン単位-
データベースアクセス一覧 アクセス単位-
アクセス統計:ユーザー別、アプリ別、月間、年間

月次監査

監視コマンド設定状況
月間利用状況概要
月間アクセス分布
年間監査項目状況一覧
月間監査項目状況一覧
月間コマンド利用状況

- DBへのアクセスログこそが、企業活動の実態を浮かび上がらせます。

不正アクセス

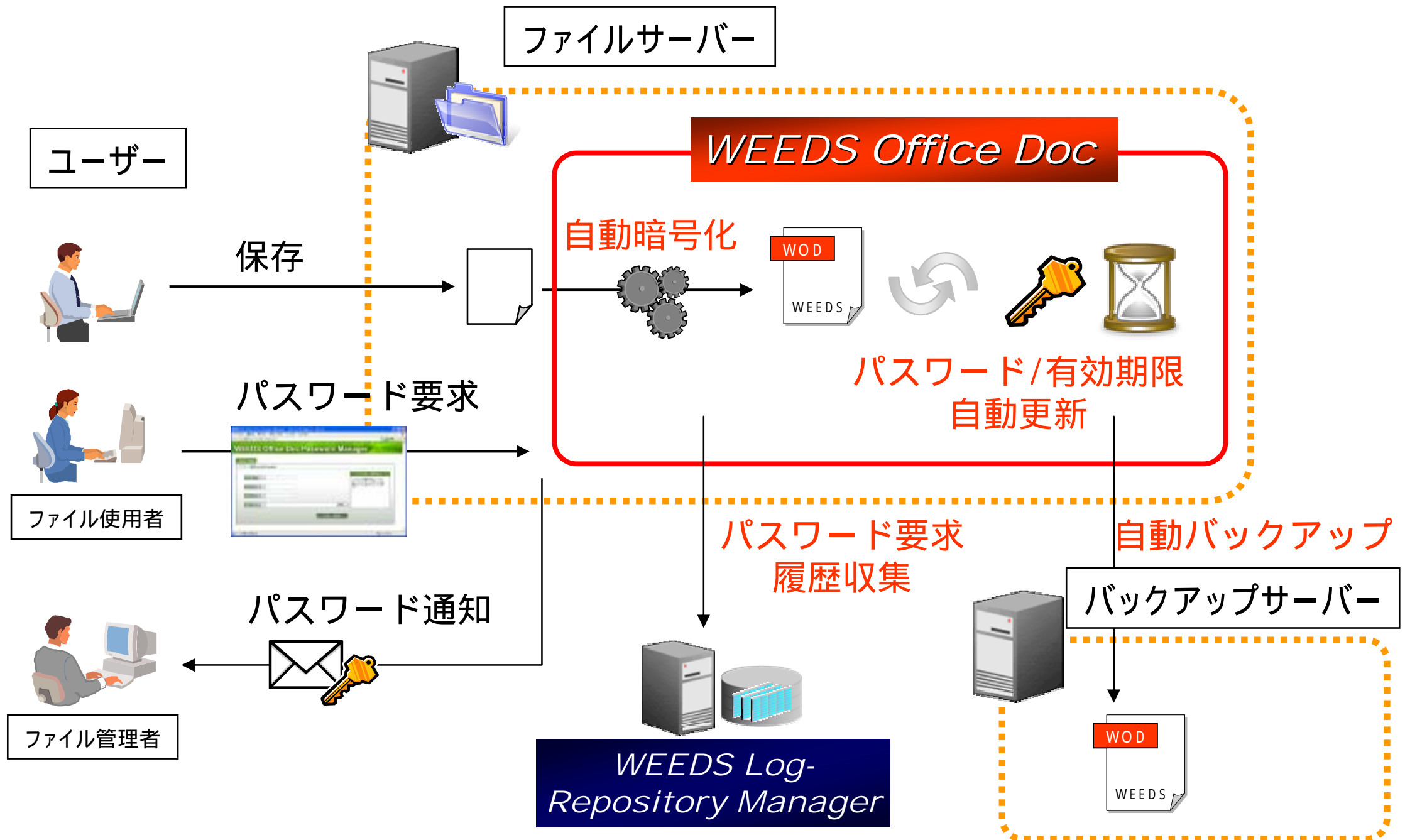
- IT関係者（システム部、ITベンダー）が不正をしていない証拠はあるか？
- 情報漏えい、会計帳簿の不正改竄など、内部犯罪の殆どがIT関係者。
- 不正ができないではなく、不正をしていないことを証明すること。

TCO的な分析

- 利用していない情報は削除することが賢明

- ・ 全てのファイルを自動暗号化
ファイルサーバーにファイルを配置するだけで自動的に暗号化
- ・ 暗号解除パスワードはワンタイムパスワード（最低1日1回変更）
パスワードが流出しても1日で無効になる
- ・ パスワードは管理者を通じて取得
パスワードはファイル使用者へ直接知らせるのではなく、ファイル管理者を経由させる
- ・ ファイルの有効期限（最低1日間）を設け、万一流出しても利用不可能に
暗号化ファイルが流出しても1日で無効になる

ファイルサーバーのセキュリティ対策



- ✓ アクセス監査なしに、セキュリティ対策終わりはない。
- ✓ ログは嘘をつきません。
アクセスログが企業活動の実態を浮かび上がらせる。
- ✓ “不正できない”環境はあり得ない。
“不正していない”ことを照明する。
- ✓ セキュリティの基本は暗号化。
 - ✓ 暗号化、ワンタイムパスワードなどを自動化することでセキュリティレベルを強化できる。

PCIDSSとは

クレジットカード業界で策定された、カード加盟店を中心としたカード会員データを取り扱う事業者が守らなければならないセキュリティ対策基準



PCIDSSの良い点

(例) ISMSでは、

あくまでも「自己責任を前提に、セキュリティを向上させるために、組織をあげて継続的にリスクマネジメントを行うこと」をコミットするもの。

それに対してPCIDSSでは、

サーバやネットワーク機器をはじめとした「現場」におけるセキュリティ対策が多く、具体的な対策が記載

「客観的にも十分なセキュリティが確保されている」という具体的な実装レベルでの要求を明らかに

PCIDSSを参考にセキュリティレベルを向上

「カード情報」「個人情報」に置き換えれば、全ての企業でPCIDSSを参考にセキュリティレベルを向上できる。

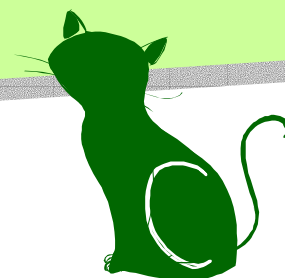
WEEDS Trace SeriesのPCIDSS対応

PCIDSSの12からなる要件のうち、要件10に適応。
(その他の要件内のうち対応しているものもあり)

WEEDS

TRUE TECHNOLOGY TO THE WORLD

WEEDS Trace Seriesで
低コストで意味のあるセキュリティ対策を
実現して下さい。



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 アペックヒルズ目白

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>