HITACHI
Inspire the Next

JP1で実現する内部統制のための エンドポイントセキュリティ

株式会社日立製作所 ソフトウェア事業部 ネットワーク管理ソフト設計部
加藤　恵理

2007年07月04日

Contents

1. 内部統制・・・何のためにやるのか？
2. 内部統制に関わるエンドポイントセキュリティ
3. JP1が目指すエンドポイントセキュリティとは
4. JP1で実現するエンドポイントセキュリティ
5. 内部統制のための次のステップ

1. 内部統制・・・何のためにやるのか？

1-1. 内部統制とは？

1-2. 内部統制の整備は IT抜きには成立しない

1-3. 「ITへの対応」を二つの側面から考える

1-1　内部統制とは？

内部統制とは、

経営者・従業員の不正・ミスによるリスクを無くすための
仕組み、および組織的活動

統制
（コントロール）

- 規則/手順の存在
- 規則通り業務/活動が行われていることに関する組織的なチェック等の活動

事前対策により、リスクを防ぐ

不正・ミス

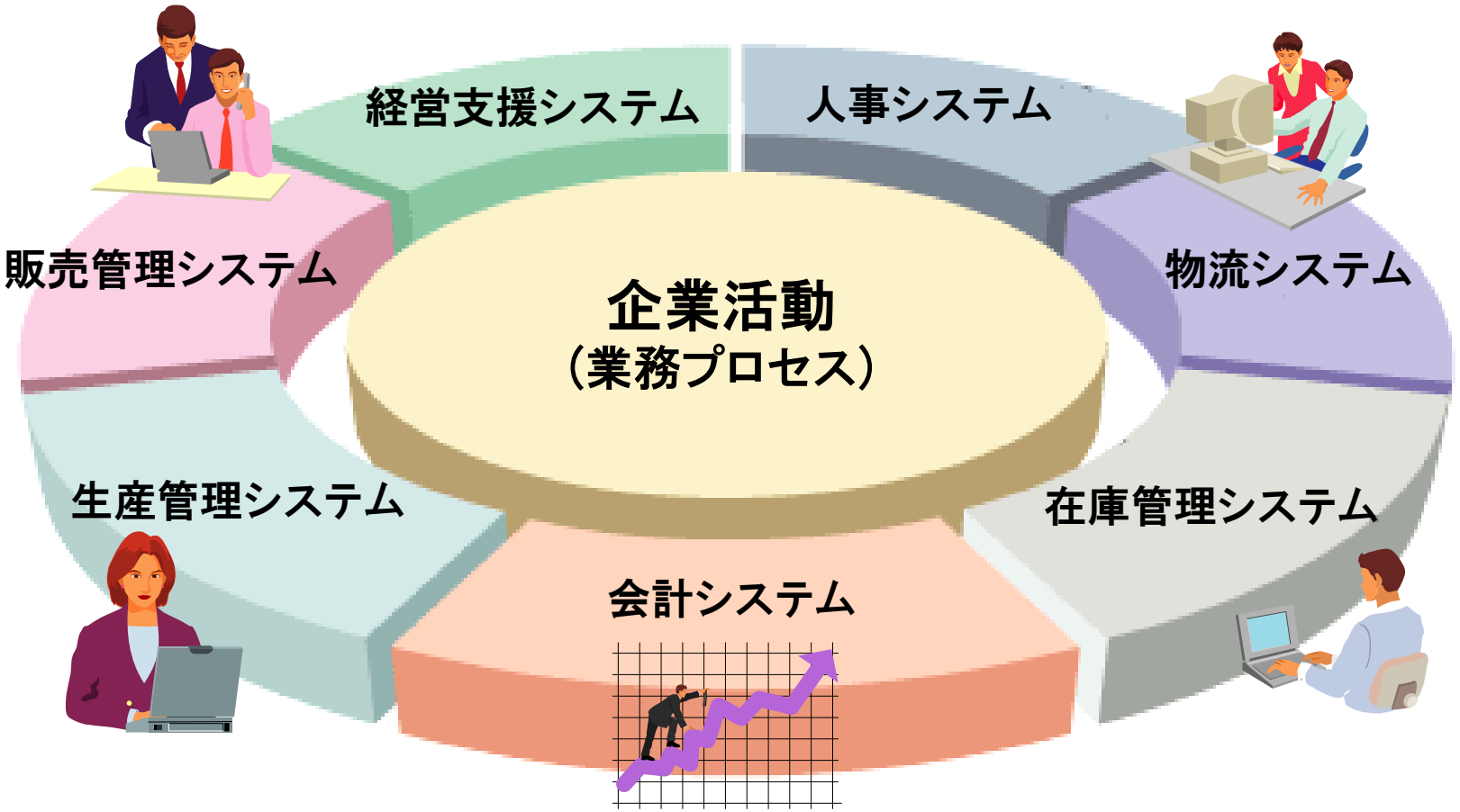
- ◆財務諸表の改ざん/不当表示
  ー費目の付け替え、期末の押し込み
- ◆オペレーションミス
- ◆犯罪（会社資産の個人使用）
- ◆ミス/不正の隠匿

リスク

- ◆資本市場からの信頼喪失
  → 株価暴落、上場廃止
- ◆顧客からの信頼喪失
  → 不買運動による業績低下
- ◆行政処分

1-2　内部統制の整備は IT抜きには成立しない

財務会計を始めとする企業の業務プロセスの多くは、
ITシステムによって処理されている。



1-3 「ITへの対応」を二つの側面から考える

ITによる統制

業務リスク削減のために
ITの機能↓を活用する

- 判断/処理のルール化
- 異常値の検知とアラーム
- 例外処理の禁止
- 証跡の取得
- 業務関連者の限定　等

ITを活用して、間違いや不正な処理が
起きない強固な業務の統制を実現する

業務リスクの把握

ITの統制

IT構築・運用の不備に
起因するリスク↓を削減する

- システム変更による不正処理
- プログラムのバグ等による
  異常処理
- 不正目的のデータ改竄
- システムダウン、データ消失等

IT自身を信頼できるものにするために
セキュリティや運用の面から統制すること

ITリスクの把握

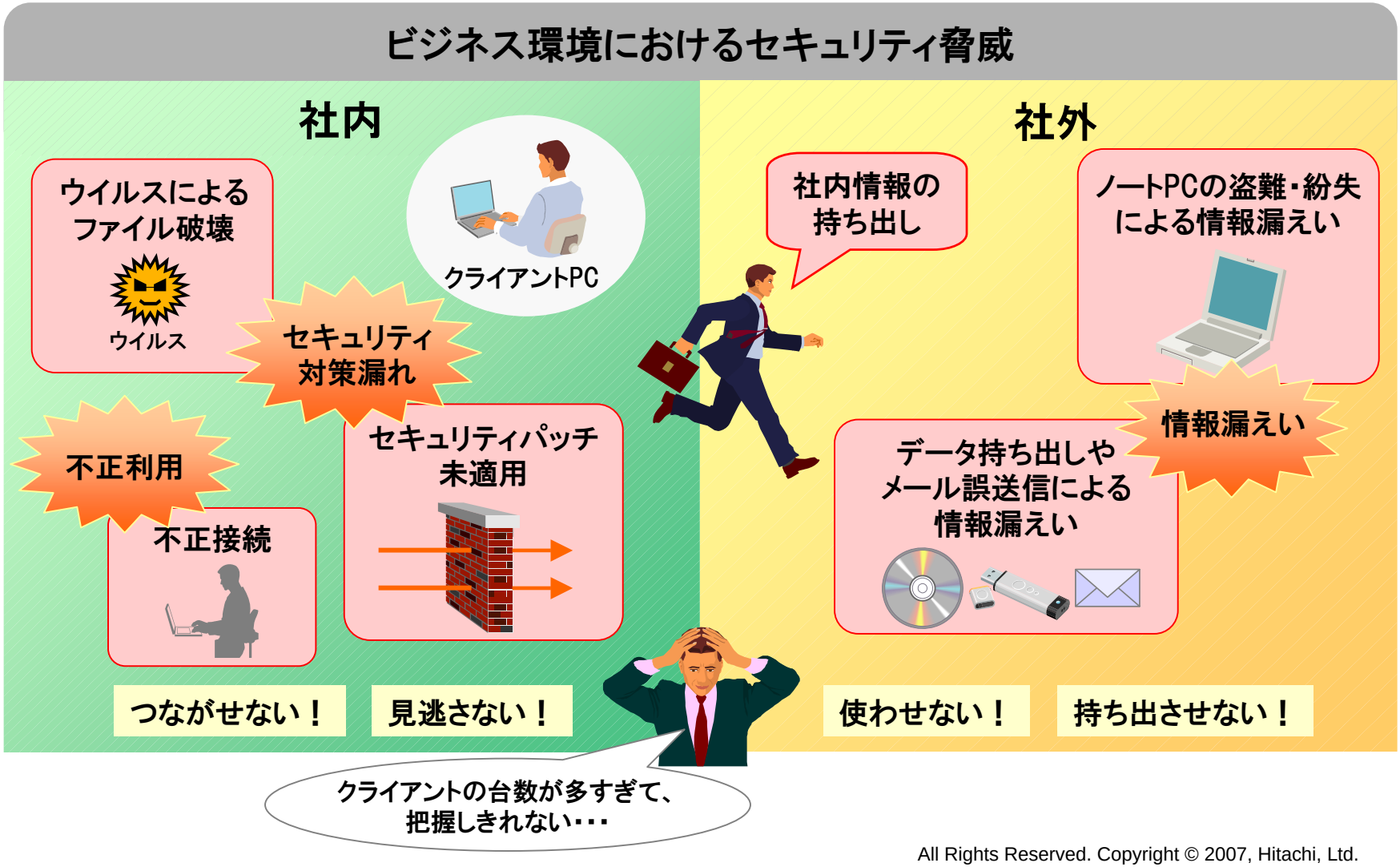
2. 内部統制に関わるエンドポイントセキュリティ

2-1. クライアントPCのセキュリティ脅威

2-2. クライアントPCの統制

2-1　クライアントPCのセキュリティ脅威

クライアントPCの誤った使い方が原因で発生している情報漏えい事件が、社会問題になっています。



2-2　クライアントPCの統制

- クライアントPCからの情報漏えいの主な原因は、以下の2つです。
  - ●従業員のセキュリティ対策に対する意識の低さ
  - ●社内でのクライアントセキュリティ対策漏れ

管理者主導によるクライアント統制

- 不正ソフトウェアを使わせない
- ウイルス対策 脆弱性対策
- 不正なPCの排除
- 社内情報を自宅に持ち帰らせない

漏れのないクライアントセキュリティ対策を実現するためには、
- ●従業員のモラル向上
- ●コンプライアンスに則ったクライアント管理　　が必要！

安全なビジネス環境の維持

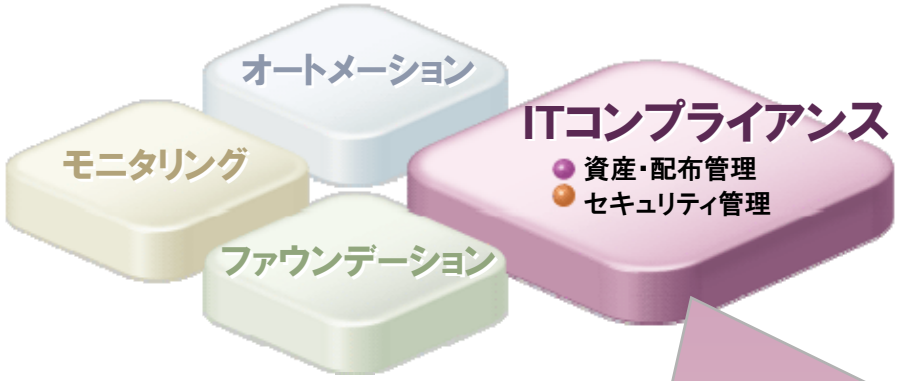
3. JP1が目指すエンドポイントセキュリティとは

3-1. JP1が目指すエンドポイントセキュリティとは

3-2. JP1によるエンドポイントセキュリティの実現

3-1　JP1が目指すエンドポイントセキュリティとは

ITコンプライアンスとは、
社内のIT資産を最適な状態に保ち、
お客様のビジネスを様々な脅威から守る手段です。



JP1の4つのコンセプトカテゴリ

ITコンプライアンス ー 大切な資産を守る

セキュリティポリシーや法令、規則に基づく内部統制を強化するために、
資産情報を集中管理し、速やかな対応策を実施。
ITコンプライアンスでは、次の4つの観点でセキュリティ対策を実施します。

つながせない　**使わせない**　**持ち出させない**　**見逃さない**

3-2　JP1によるエンドポイントセキュリティの実現

以下のJP1製品群で、ITコンプライアンスの実現を支援します。

該当章No	対策	概要	JP1該当製品
4-1	IT資産管理	IT資産の全般把握	JP1/NETM/AIM JP1/NETM/DM
4-2	ウィルス対策	ウィルス対策製品の管理	JP1/NETM/CSC JP1/NETM/DM
	脆弱性対策	ソフトウェア脆弱性対策の管理	
4-3	不正ソフトウェア対策	不正ソフトウェアの使用を防止	JP1/NETM/DM
4-4	不正PC排除	持ち込みPCなど、管理外PCの排除	JP1/NETM/NM
4-5	検疫システム	セキュリティ未対策PCの社内LAN接続を排除、検疫	JP1/NETM/CSC JP1/NETM/NM JP1/NETM/DM
4-6	情報漏えい対策	メディア、ノートPC等からの漏えい防止	JP1/秘文
4-7	操作・アクセスログ管理	不正な操作、アクセスを監視・記録	JP1/NETM/DM JP1/秘文

【凡例】
- JP1/NETM/AIM：JP1/NETM/Asset Information Manager
- JP1/NETM/CSC：JP1/NETM/Client Security Control
- JP1/NETM/NM：JP1/NETM/Network Monitor
- JP1/秘文：JP1/秘文 Advanced Edition

4. JP1で実現するエンドポイントセキュリティ

4-1. クライアントPCの状況が把握できていない
4-2. ユーザー任せのセキュリティ対策によるウイルス感染
4-3. 不正ソフトウェアの使用による損害
4-4. 持ち込みPCからのウイルス感染、情報漏えい
4-5. PCのセキュリティ管理に漏れが出てしまう
4-6. 外部媒体、ノートPCからの情報漏えい
4-7. PCの不正利用が把握できない

4-1 問題例（1）
クライアントPCの状況が把握できていない

- クライアントPCからのウイルス感染、情報漏えいが後を絶たない。
  セキュリティ対策を実施したいが、どの部署に何台クライアントPCがあるかも把握できていない。
- 各クライアントPCのセキュリティパッチやウイルス対策製品等のインストール状況がわからない。

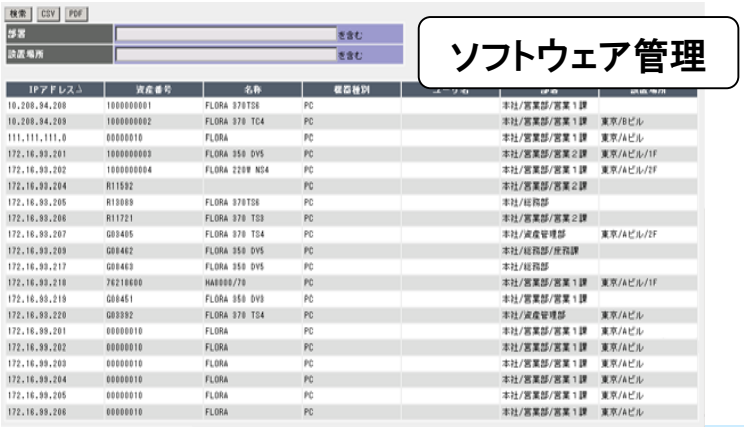
人海戦術でのクライアントPCの管理では限界がある

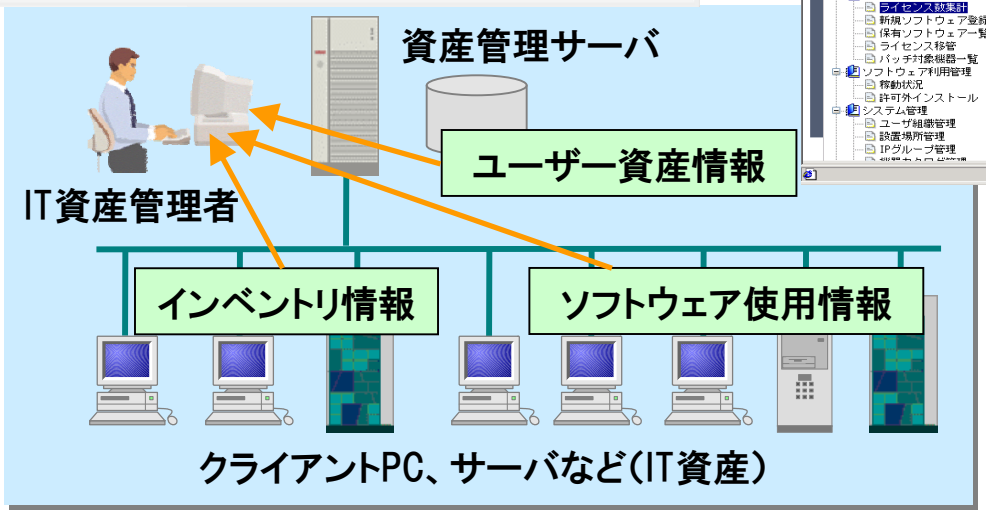
JP1なら、システム全体のクライアントPCを効率よく一元管理できます

4-1　IT資産管理

見逃さない

- インベントリ情報を定期的に収集することで、人手に頼らず、効率の良いIT資産管理を実現します。
- クライアントPCの台数やソフトウェアのインストール状況を一元管理できます。

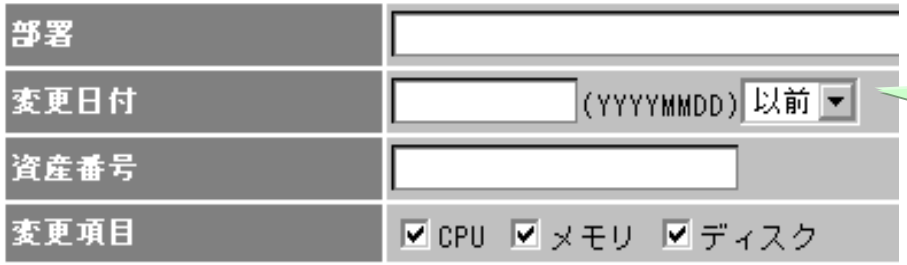




4-1　システムの変更管理

見逃さない

- 過去の変更履歴を確認できます。問題が発生した機器のハードウェアやソフトウェアの変更状況を確認でき、不正なシステム変更の防止を支援します。



変更日時、変更項目等の検索条件を指定して検索

検索

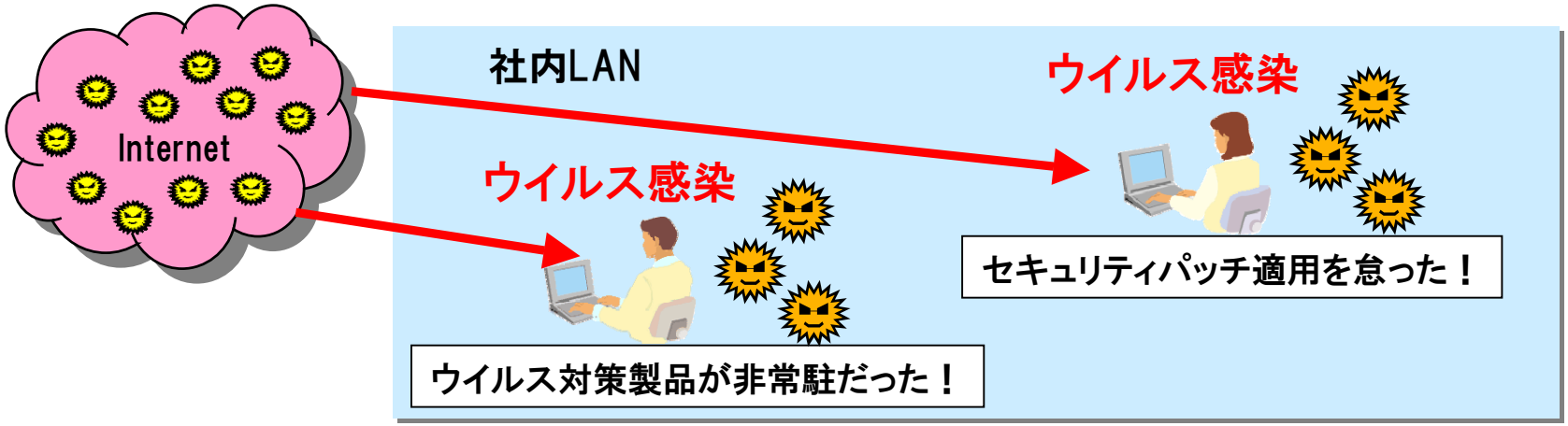
検索条件に合った機器の一覧を表示

変更日付△	変更前	変更後	資産番号	部署	ユーザ名
2004/01/18 02:57:41	CPUクロック数: CPU数: CPU: メモリサイズ: ディスク容量:	CPUクロック数:1000MHz CPU数:2 CPU:Intel Pentium III メモリサイズ:128MB ディスク容量:20GB	1000000001	本社/営業部/営業１課	営業太郎
2004/01/20 02:00:00	メモリサイズ:128MB ディスク容量:20GB	メモリサイズ:256MB ディスク容量:40GB	1000000001	本社/営業部/営業１課	営業太郎
2004/01/25 02:00:00	メモリサイズ:256MB ディスク容量:40GB	メモリサイズ:512MB ディスク容量:60GB	1000000001	本社/営業部/営業１課	営業太郎
2004/02/01 02:00:00	メモリサイズ:512MB ディスク容量:60GB	メモリサイズ:1024MB ディスク容量:80GB	1000000001	本社/営業部/営業１課	営業太郎
2004/02/10 02:00:00	ディスク容量:80GB	ディスク容量:100GB	1000000001	本社/営業部/営業１課	営業太郎
2004/02/18 02:57:42	CPUクロック数: CPU数: CPU: メモリサイズ: ディスク容量:	CPUクロック数:500MHz CPU数:1 CPU:Intel Pentium III メモリサイズ:512MB ディスク容量:40GB	1000000005	本社/資産管理部	資産太郎

問題例（2）

ユーザー任せのセキュリティ対策によるウイルス感染

- セキュリティパッチの適用は各ユーザーがバラバラに行っている。
  最新のセキュリティパッチを適用していないユーザーがいたため、
  ウイルスに感染してしまった。
- すべてのクライアントPCにウイルス対策製品がインストールされていたが、
  ウイルス対策製品を非常駐にしていたクライアントPCがあったため、
  ウイルスに感染してしまった。



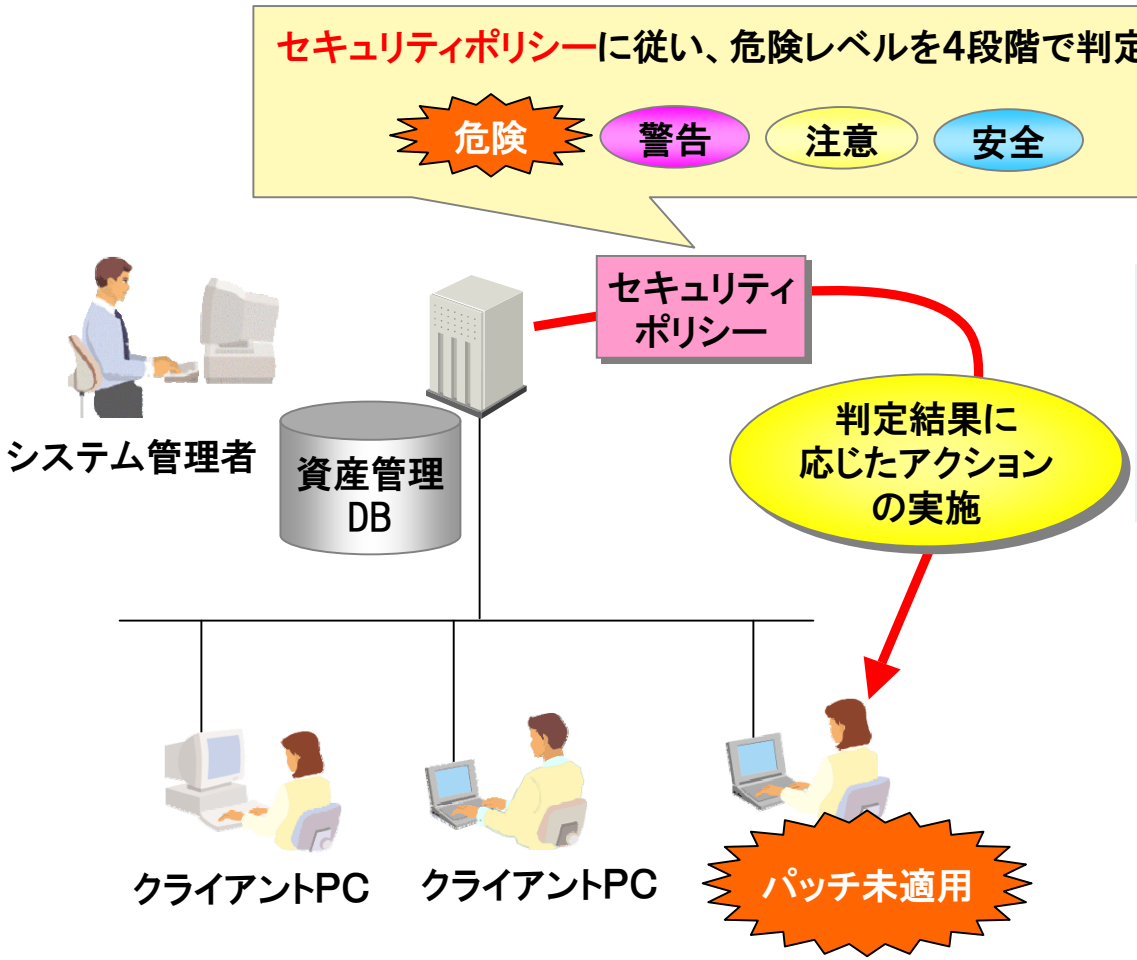
ウイルス感染は、ユーザー任せのセキュリティ対策が原因であることが大半

ITによる管理者主導のクライアントPCの統制が不可欠です

4-2　ウイルス対策・脆弱性対策

見逃さない

- クライアントPCの資産情報を一元管理し、セキュリティ対策状況を一元監視。
  ウイルス定義ファイルや、セキュリティパッチなどの適用が不十分なPCを検知し、
  セキュリティ上の脅威に対する予防策を講じることができます。



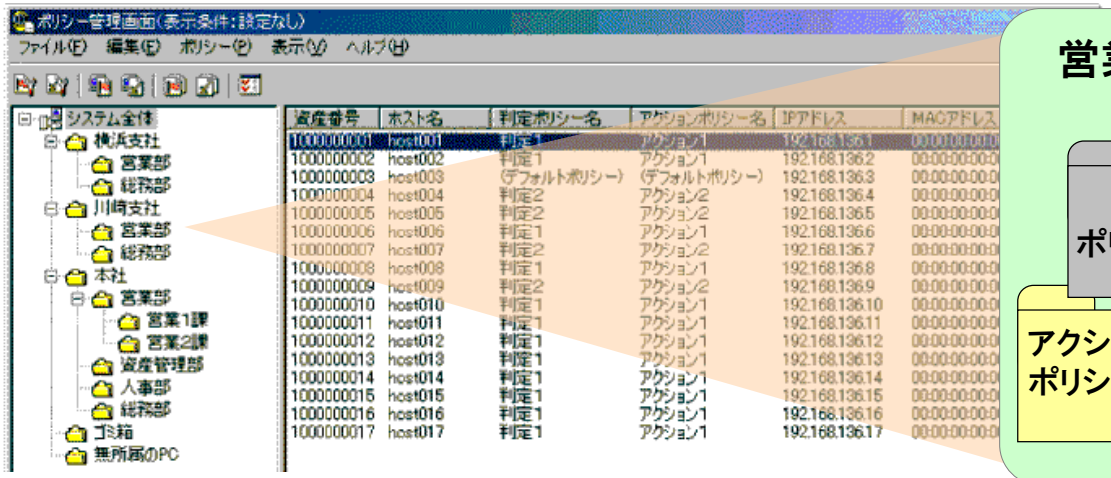
＜危険レベル判定情報＞
- Windows®更新プログラムの適用状況
- ウイルス対策製品の情報
- 不正ソフトウェアのインストール情報
- 必須ソフトウェアのインストール情報
- ユーザー定義情報

＜アクション設定情報＞
- 管理者への通知
- クライアントPC利用者への通知
- クライアントPCのネットワーク接続の制御
- ユーザー定義のアクション

4-2　柔軟なセキュリティ監査の実現

見逃さない

- 部署やPCごとにポリシーを割り当てることができます。
  部署ごとにセキュリティポリシーが異なる場合でも柔軟に対応することができます。
  また、セキュリティ対策状況を点数化して表示、レポートすることができます。



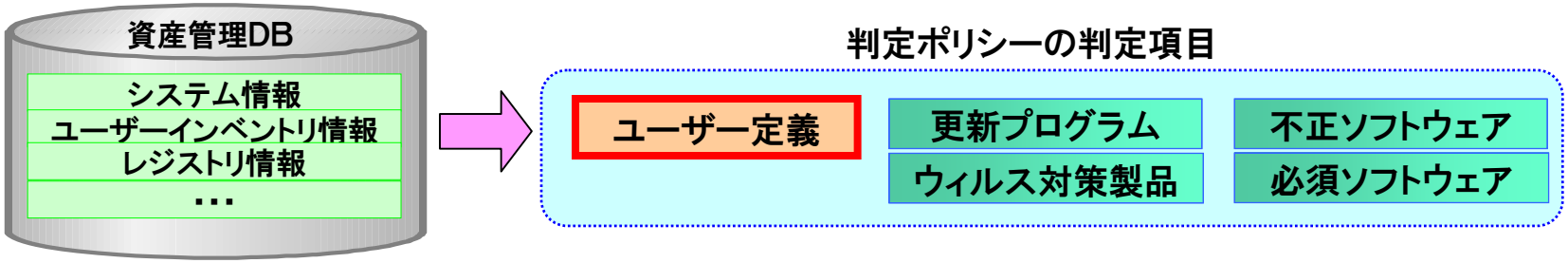
部署	最低点	平均点	台数
横浜支社/営業本部/第一営業部	3	61	32
横浜支社/営業本部/第二営業部	3	48	33
横浜支社/開発本部/第一開発部	6	55	31
横浜支社/開発本部/第三開発部	3	61	30
横浜支社/開発本部/第二開発部	3	51	45
川崎支社/人事本部/第一人事部	3	53	37
川崎支社/人事本部/第三人事部	6	49	28
川崎支社/人事本部/第四人事部	6	46	27
川崎支社/人事本部/第二人事部	6	58	44
川崎支社/品質保証本部/第一品質保証部	6	52	20
川崎支社/品質保証本部/第二品質保証部	4	50	84

セキュリティ対策状況を
部署ごとに点数化

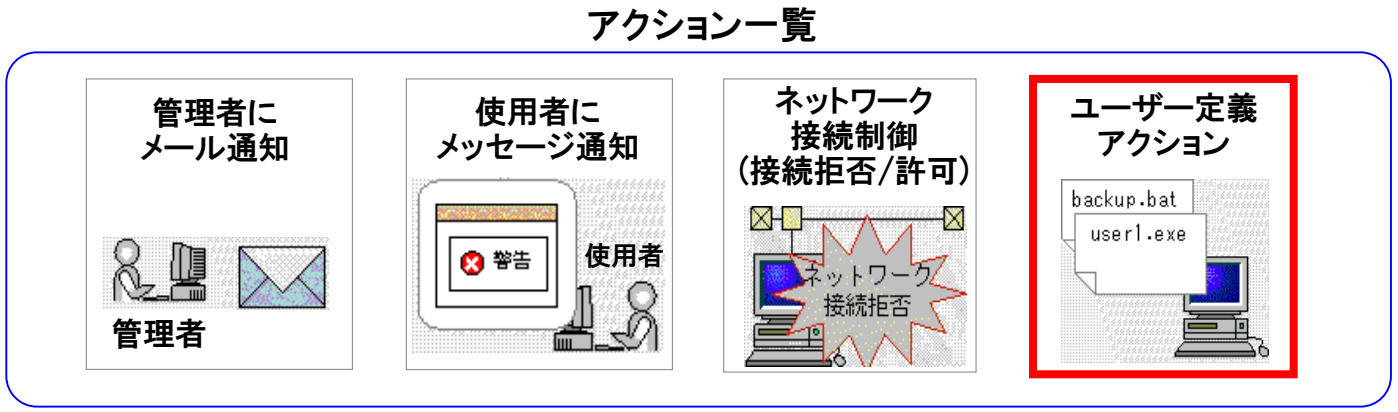
4-2　柔軟なセキュリティ監査ポリシーの設定

見逃さない

- ユーザーが定義した任意の情報を危険レベル判定の対象にできます。
  例えば、自動ログオンの有無などを危険レベルの判定項目とすることができ、
  柔軟なセキュリティ検査を行うことができます。



- 危険レベルの判定後に、任意のアクションを実行することができます。
  例えば、ユーザー独自のコマンドやバッチを実行することができます。

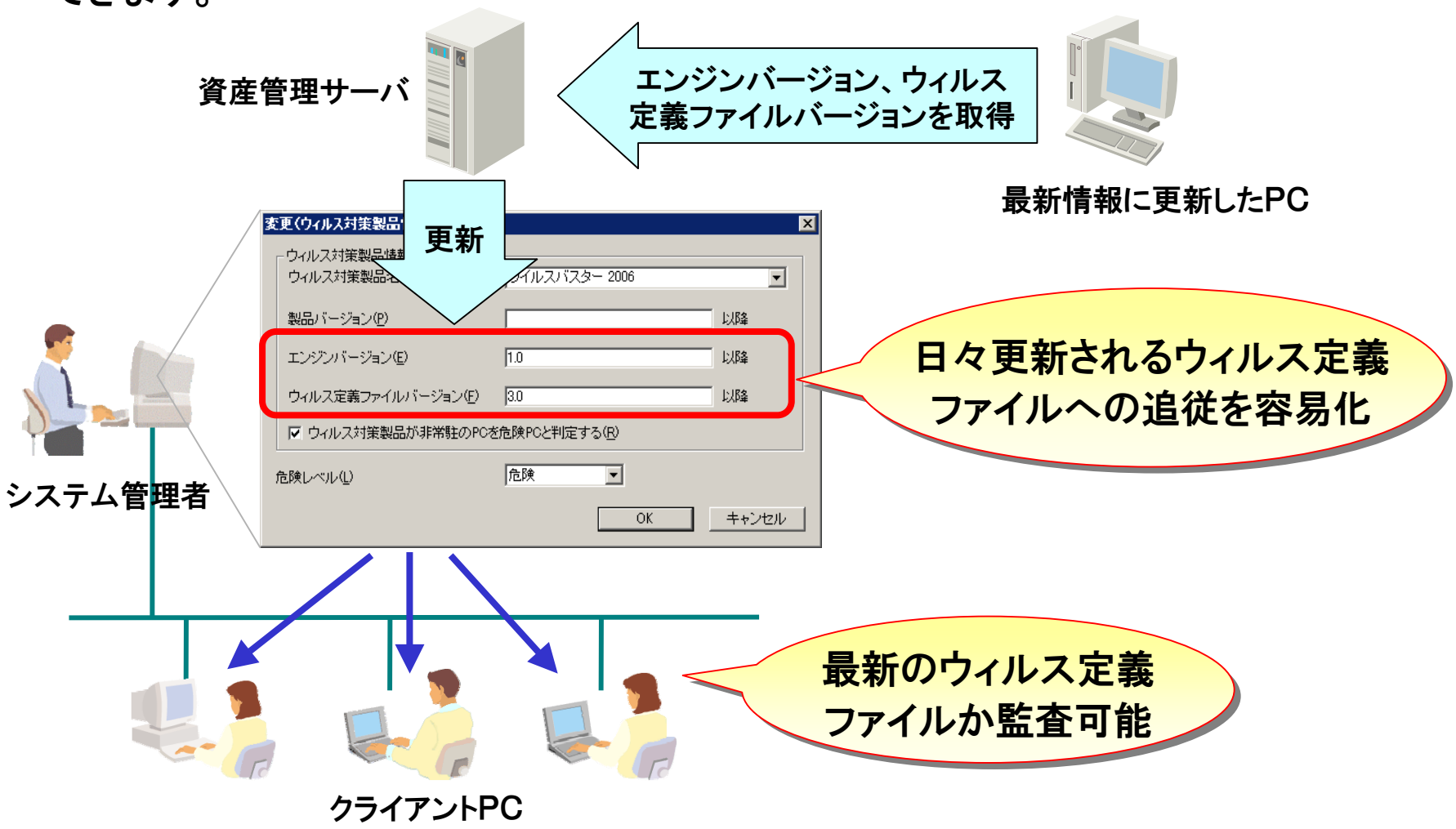


4-2　セキュリティ監査ポリシーのメンテナンスの容易化

JP1

見逃さない

- トレンドマイクロ社製ウィルス対策製品と連携し、ポリシーのエンジンバージョン、ウィルス定義ファイルバージョンを自動的に最新バージョンに更新することができます。



問題例（3）

不正ソフトウェアの使用による損害

- WinnyやShareのような管理用のサーバーを持たず、
  ピア・ツー・ピア方式で社外と通信できてしまうファイル交換ソフト経由で
  情報漏えいが発生してしまった。（情報漏えい）
- ライセンスが無いソフトウェアは使用させたくない。（ライセンス違反）
- 業務時間中にゲームソフトなど不必要なソフトを使用させたくない。（作業効率低下）

情報漏えい

ライセンス違反

作業効率の低下

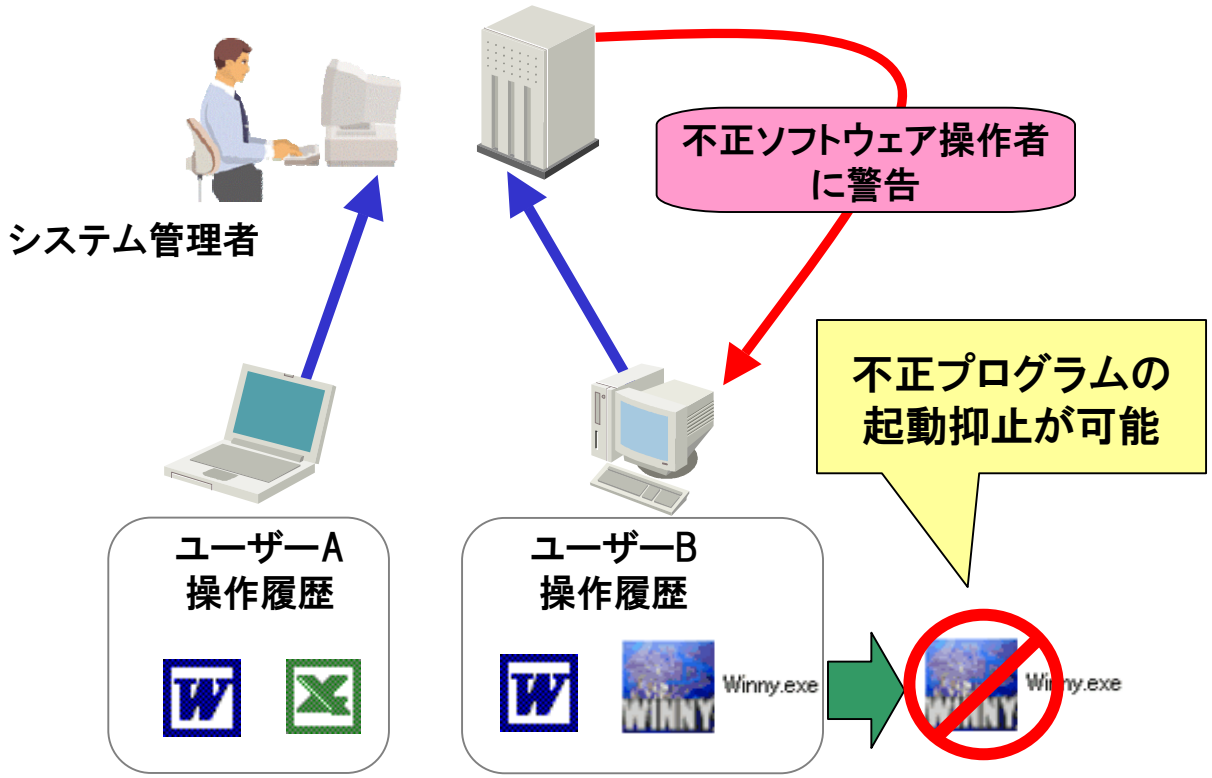
不必要なソフトウェアが使用されていることにより、
思わぬ損害や情報漏えいが発生する

クライアントPCの操作を監視することにより、ユーザーのモラル向上が図れます

4-3　不正ソフトウェアを使わせない

使わせない

- ユーザーが起動したプログラムの情報を取得し、起動を抑止できます。
  - ファイル交換ソフトやゲームなどの不正使用防止
  - 情報漏えい時の原因特定、追跡のためのトレース取得
    →問題のあるユーザーには警告を発することができます。



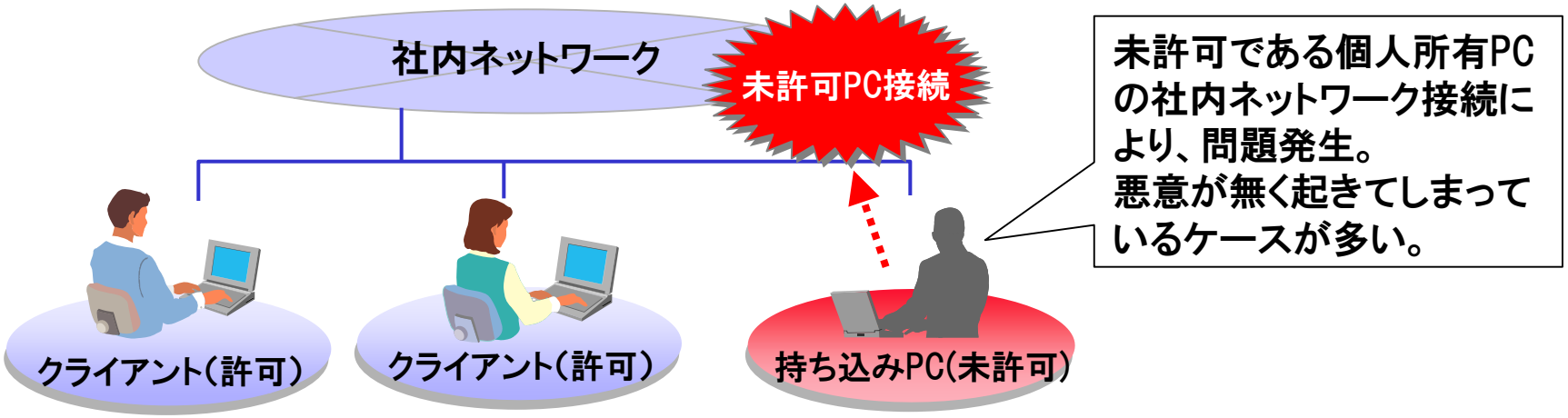
下記の条件で抑止の定義が可能
- ファイル名/ファイルバージョン
- ユーザーアカウント
- ユーザーグループ
- 時間

抑止プログラムの例
- 特定の通信ソフト
  フリーのメールクライアント、Winny、Share、SoftEtherなど
- ゲーム
- ライセンスのないソフトウェア

問題例（4）

持ち込みPCからのウイルス感染、情報漏えい

- 社内で使用を許可されていない個人所有のPCが社内ネットワークに接続され、ウイルスに感染してしまった。
- 社外から持ち込まれたPCから機密情報が持ち出されてしまった。
- クライアントPCの接続状態などは日々変化しているため、管理者がすべてを管理することが非常に難しくなっている。



悪意がなくても、不用意に未許可PCをネットワークに接続すると
ウィルス感染や情報漏えいが起こる

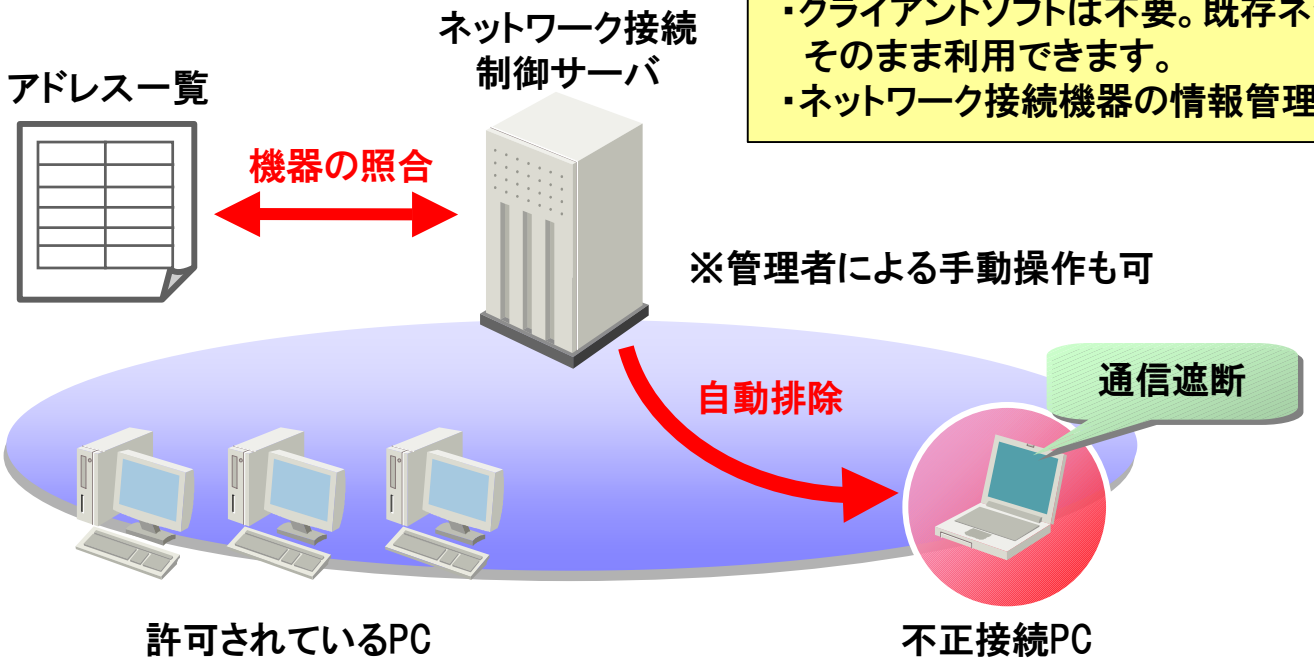
使用を許可されていないPCは、社内ネットワークへ接続させない仕組みが必要

4-4　不正PCは接続させない

つながせない

- ネットワーク接続制御サーバにより、あらかじめ許可されたPCだけを業務ネットワークへ接続させることが可能。

・不正に接続したPCの自動排除が可能です。
・クライアントソフトは不要。既存ネットワークをそのまま利用できます。
・ネットワーク接続機器の情報管理もできます。

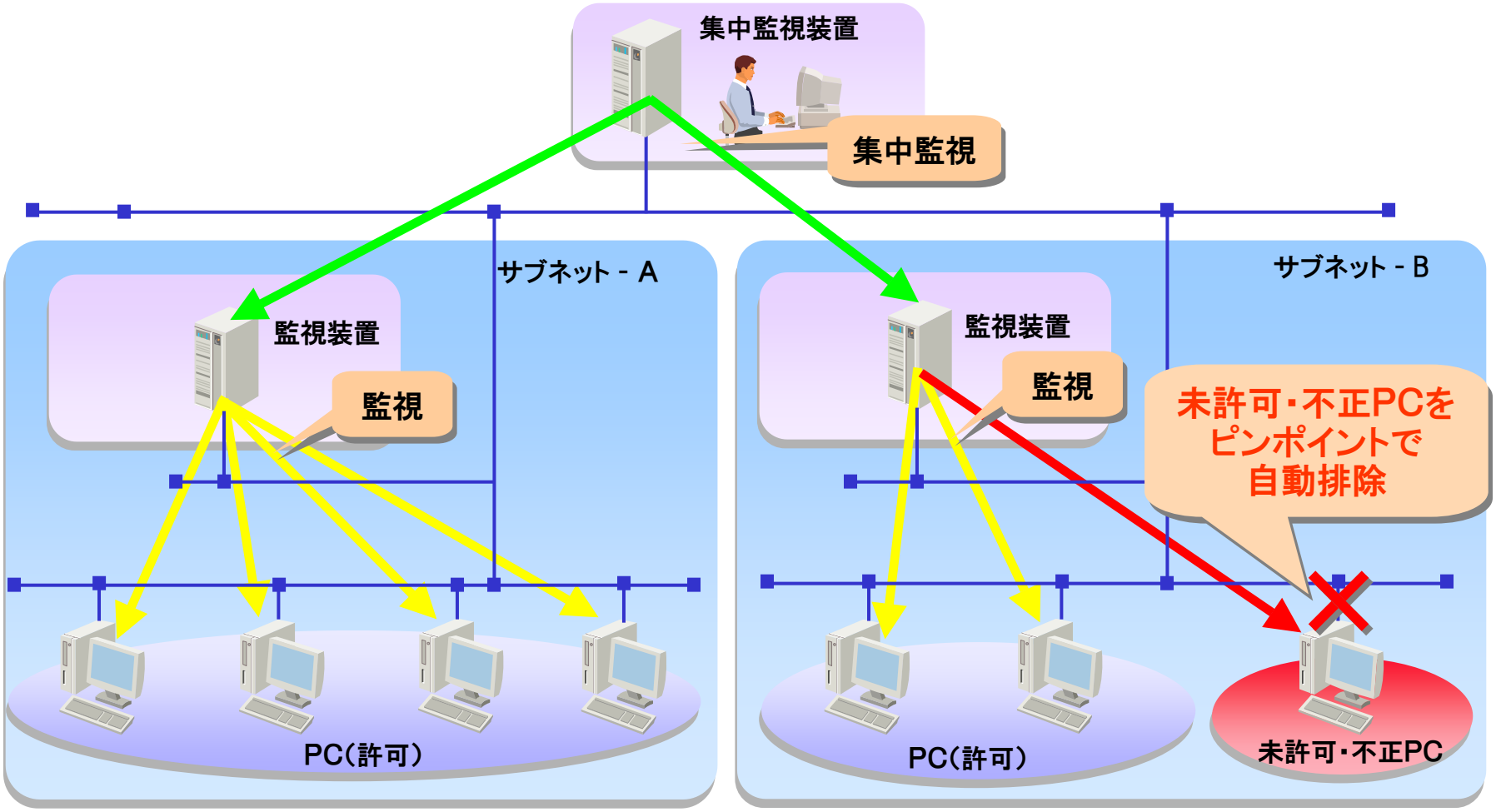


JP1資産管理サーバとの連携により、
セキュリティポリシーに応じた接続条件による管理が可能

4-4　不正PCの接続監視・強制排除

つながせない

- 不正PC、未許可PCをネットワークから排除することができます。



問題例（5）

PCのセキュリティ管理に漏れが出てしまう

- 社内PCにはウイルス対策製品を導入し、セキュリティ対策は実施しているが、それでもセキュリティ対策が不十分なPCが存在する。
- 情報漏えい防止対策製品を”インストール必須”と通達していたのに、インストールされていないPCがあった。このPCから機密情報の漏えいが発生した。
- セキュリティ対策が不十分なPCを発見しても、スピーディーに治療・回復まで行えていないため、社員の業務に支障を来たす場合がある。

●ユーザーに頼ったセキュリティ対策では対策漏れが発生しがちである
●セキュリティ対策が不十分なPCを発見しても、対策に時間がかかると手遅れになる危険がある

・セキュリティポリシーに反する場合は、社内ネットワークへの接続を制限する仕組みが必要

・セキュリティ対策が不十分なPCの発見・治療は、業務に支障なく、迅速に行なえる仕組みが必要

4-5　検疫システムで脆弱なPCをつながせない

つながせない

- セキュリティポリシーに基づいたクライアントPCの検疫システムを実現。
  ウィルス感染や情報漏えいにつながる脆弱なクライアントPCに対して、業務ネットワークに接続する前に、検査、隔離、治療を行い、エンドポイントで脆弱性を除去。

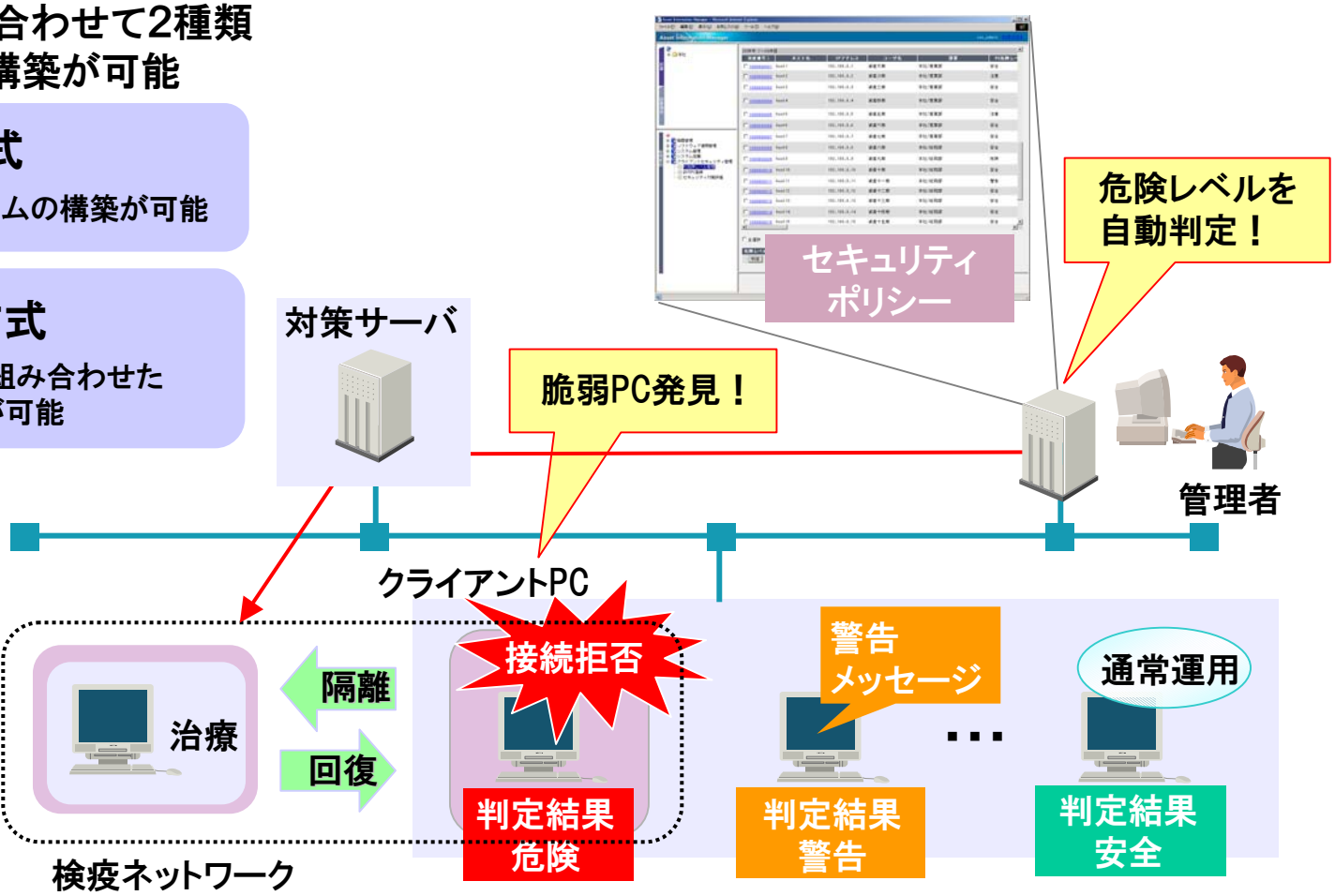
■ユーザー環境に合わせて2種類の検疫システム構築が可能

ソフトウェア方式

JP1だけで検疫システムの構築が可能

認証スイッチ方式

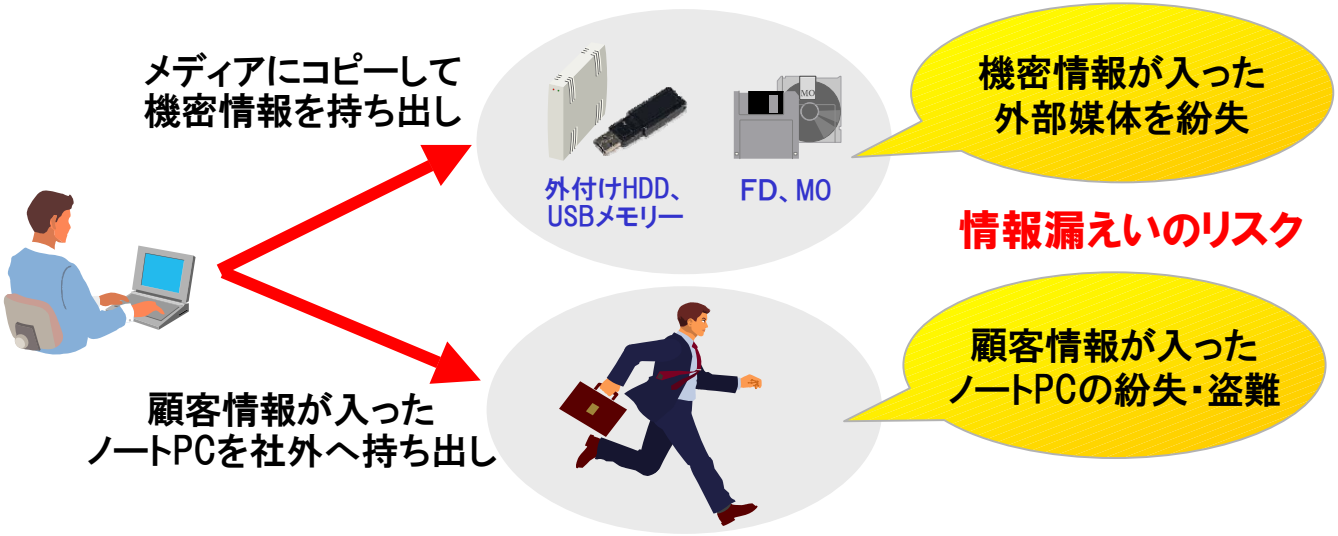
JP1と認証スイッチを組み合わせた検疫システムの構築が可能



問題例（6）

外部媒体、ノートPCからの情報漏えい

- 会社の機密情報をUSBメモリーに格納して持ち歩いていたところ、紛失してしまい機密情報が漏えいしてしまった。
- 顧客情報が入ったノートPCを社外に持ち出していたところ、ノートPCを置き忘れて紛失してしまい、顧客情報が漏えいしてしまった。



外部媒体やノートPCを社外に持ち出す場合の規則が無く、自由に持ち出されているため、情報漏えいが発生

情報を持ち出させない、持ち出しても漏えいさせない仕組みが必要

4-6　情報を持ち出させない、漏えいさせない

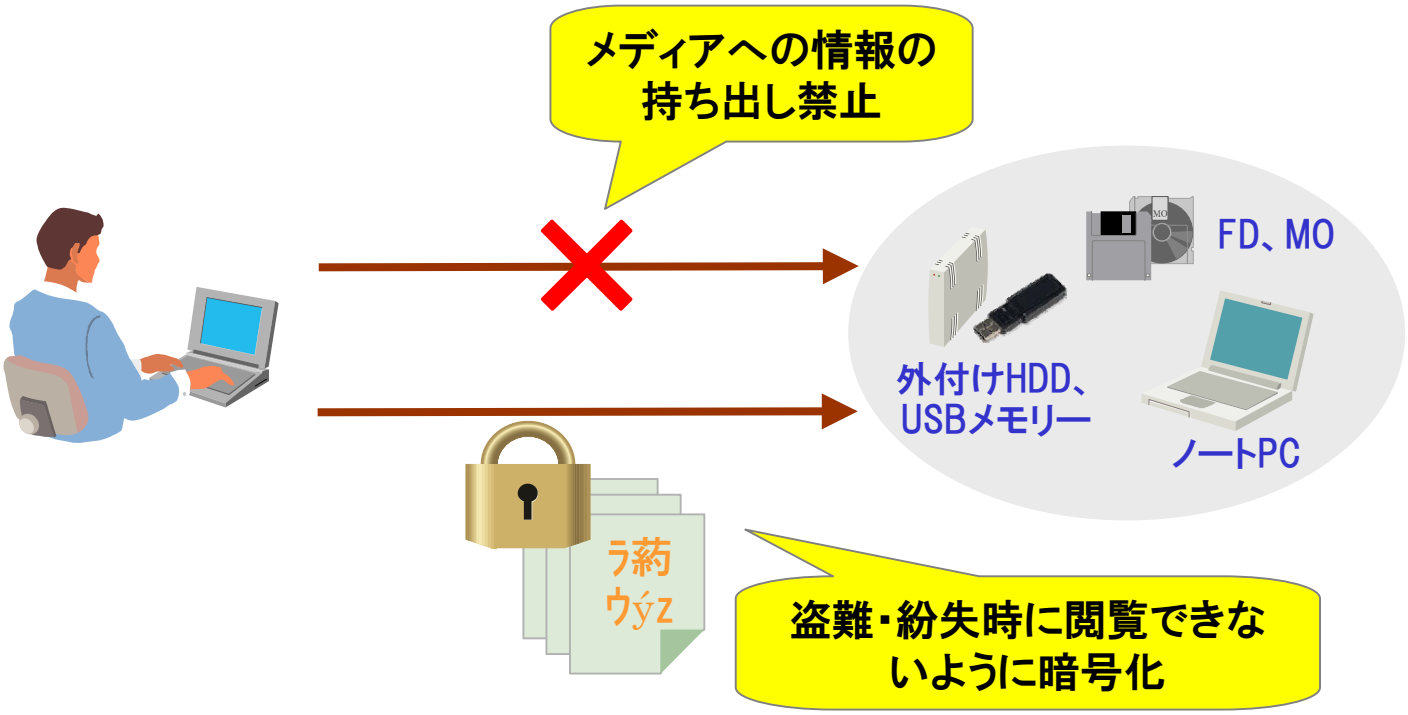
持ち出させない

持ち出し制御

リムーバブルメディア(USBメモリー、MD、FDなど)へのファイル無断書き出しを禁止し、
社外へのファイルの持ち出しのモラル向上ができます。

リムーバブルメディアやノートPCの暗号化

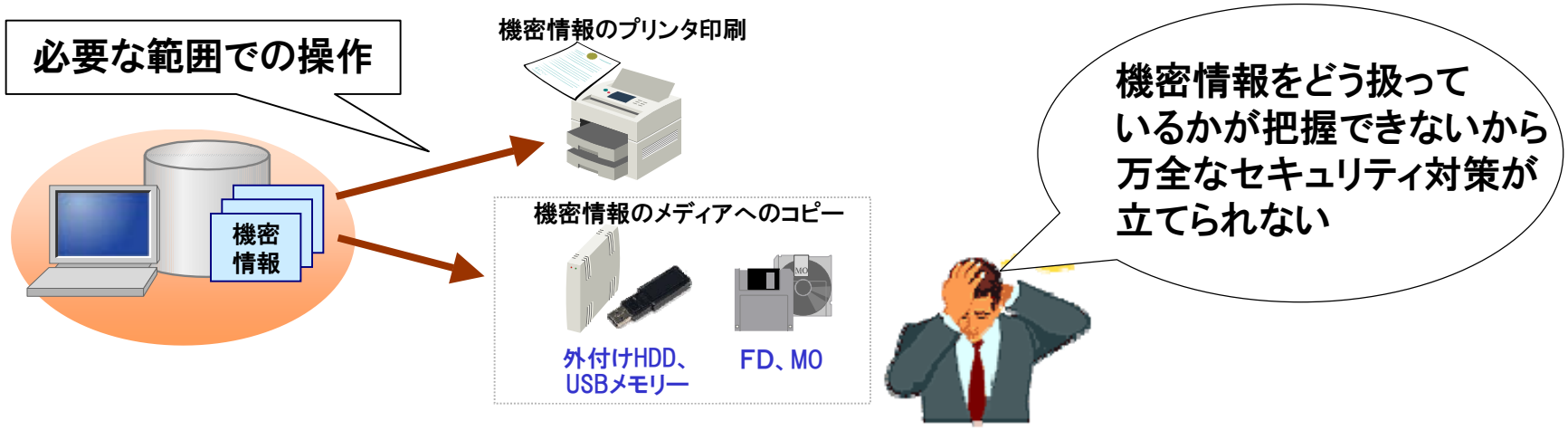
リムーバブルメディアにファイルを書き出す際に、自動的に暗号化できます。
また、ノートPCのドライブ暗号もできます。これにより盗難・紛失による漏えいを防止します。



問題例（7）

PCの不正利用が把握できない

- 取り扱い注意の機密情報は必要な範囲でユーザーが扱うことがあるが、コピーや印刷など、どのように扱われているかが把握できていないので、セキュリティ上不安である。
- また、いざ情報漏えいが発生してしまった場合、原因究明ができず、その後の対策が立てられない。



どうしてもユーザーが機密情報を扱わなければならない場合があるが
どのように扱われているかを把握できていないため、対策を立てられない

誰が、いつ、どのような操作を行ったか、ユーザー操作を把握することが必要

4-7　クライアントの活動履歴の採取

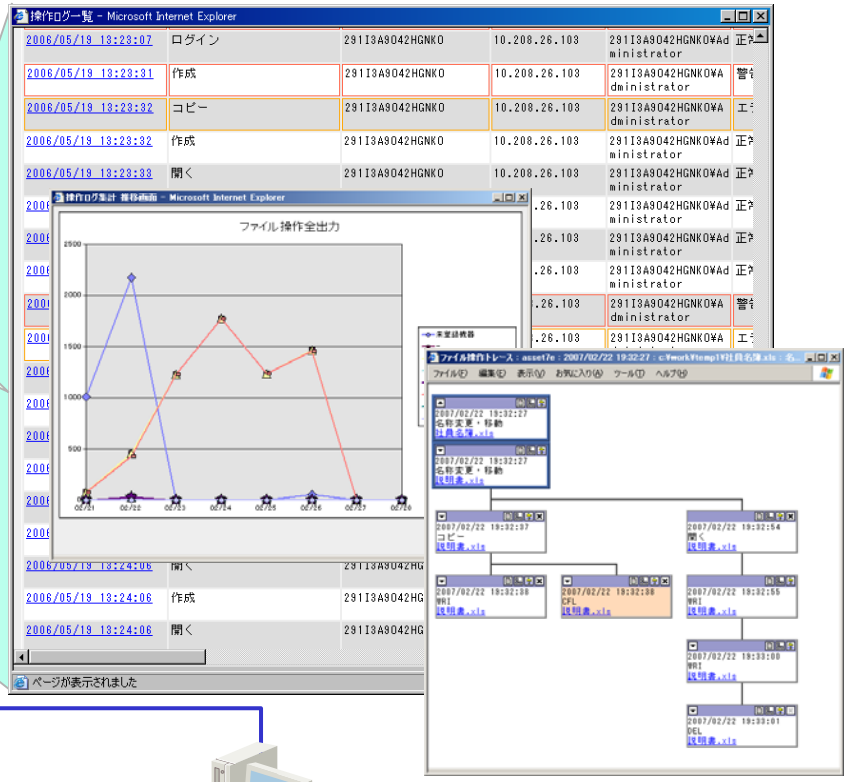
見逃さない

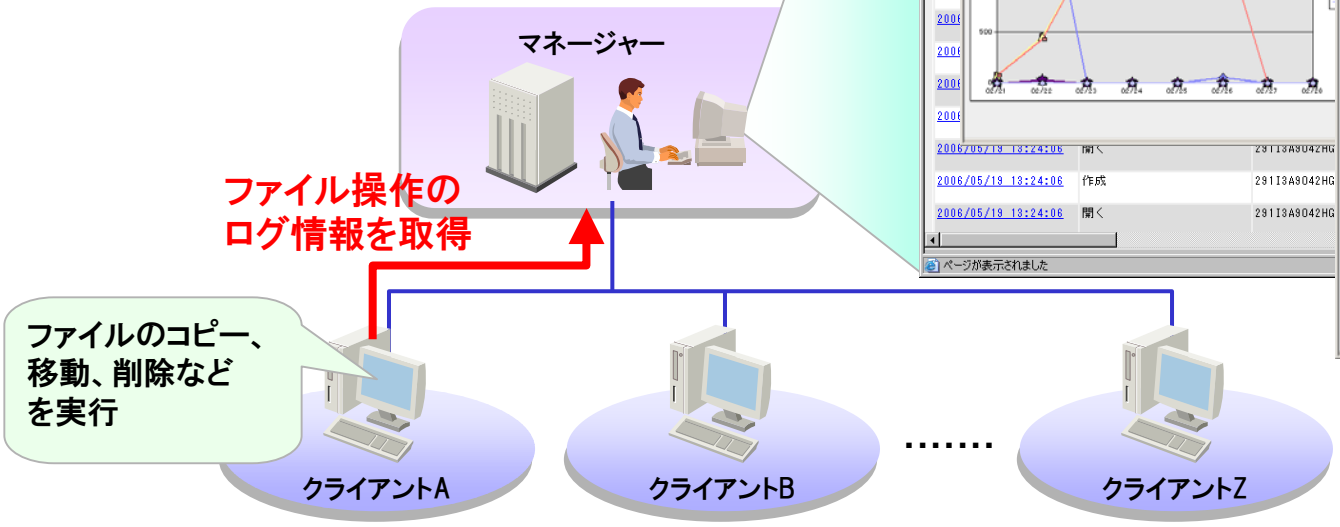
- クライアントPCにおける各種操作ログを統合的に監査。
  クライアント監査の支援や従業員のモラル向上が図れます。

操作ログの検索画面で、外部に持ち出したり、
印刷を実行したファイルの追跡に必要な情報を取得。

- 取得可能なログ
  - ・外部への持ち出し
  - ・ファイルのコピー
  - ・ファイルの移動、削除、印刷
  - ・アプリケーションの起動　等

ファイル名や、外部媒体へのコピーなどの操作でログ情報を絞り込み





5. 内部統制のための次のステップ

5-1. JP1を活用した主な統制ポイント

5-2. 活動履歴の採取（サーバ）

5-1　JP1を活用した主な統制ポイント

ミスや不正を起こりにくくするために・・・

業務の自動化

- 安定したサービスの提供
- 人の介在によるリスクの回避

安全なシステム環境を維持するために・・・

クライアントPCの統制

- 情報漏えいリスクの回避
- 安全なビジネスインフラの構築

業務要件の変更に追従するために・・・

作業プロセスの統制とシステムの変更管理

- 作業状況の監視
- 不正な変更の回避

システムの信頼性を保障するために・・・

システムの稼働監視

- 処理能力超過による異常動作の回避
- システム増強計画時のボトルネック把握

各プロセスの正当性を証明するために・・・

活動履歴の採取

- 業務システムの正当性を証明
- 各種作業の正当性を証明

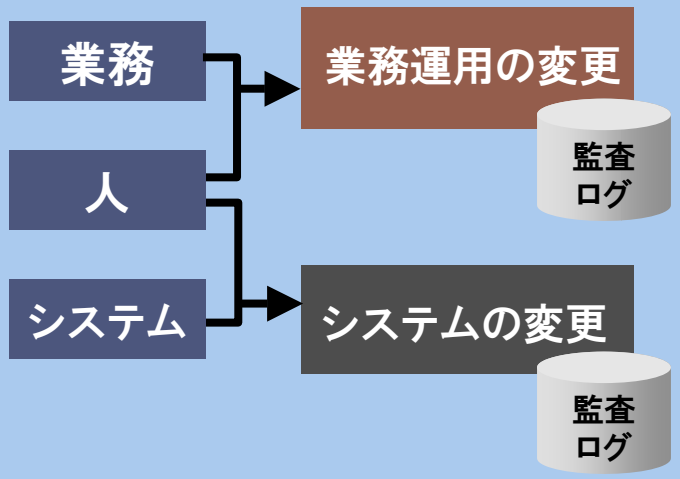
5-2　活動履歴の採取（サーバ）

- 業務運用の変更、サーバ上で動作するアプリケーションの更新、ユーザー情報の追加・変更といった、サーバ運用に関するログ情報を自動収集し一元管理します。また、検索機能などにより、監査時の運用を容易化します。

運用実績の記録

監査に必要な視点と
業務システムの運用実績の記録

（監査に必要な視点）　（運用実績の記録）



監査証跡管理の提供

収集

「見たい情報」を
「使いやすい形」で
収集

保管

収集した大量のログ
をバックアップして
長期保存

監査ログ

監査

「いつ」「誰が」
「どの権限で」
「どこから」「何をした」
という監査の実現

HITACHI
Inspire the Next

他社商品名、商標等の引用に関する表示

•Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
•Windowsは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
•その他記載されている会社名、製品名は各社の商標または登録商標です。

✧本製品を輸出される場合には、外国為替　及び外国貿易法並びに米国の
輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。
なお、ご不明な場合は、弊社担当営業に お問い合わせください。

●画面表示をはじめ、製品仕様は、改良のため変更することがあります。