uVALUE

徹底解説！
進化したJP1のITコンプライアンス

～セキュリティ管理、資産・配布管理の新機能を中心に～

2007.6.6

HITACHI
Inspire the Next

株式会社 日立製作所 ソフトウェア事業部
JP1販売推進センタ
伊庭　健一

Contents

本日のBトラックセションの紹介

【B-1】徹底解説！
進化したJP1のモニタリング
～統合管理、アベイラビリティ
管理の新機能を中心に～

【B-3】徹底解説！
進化したJP1のオートメーション
～ジョブ管理の新機能を中心に～

【B-2】徹底解説！
進化したJP1のITコンプライアンス
～セキュリティ管理、資産・配布
管理の新機能を中心に～

uVALUE

1
JP1のITコンプライアンスとは

HITACHI
Inspire the Next

1-1 JP1のITコンプライアンスとは

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します。

JP1のITコンプライアンスは、企業内システム環境の的確な把握と、不正アクセスやウィルス感染といった脅威やリスクからの保護を実現します。
企業や組織で定められた統制基準を満たし、「正しく運用させるための仕組み」をPDCAサイクルに沿って支援します。さらに、「正しく運用されていること」を証明するために必要な証跡記録を収集。
企業の内部統制の根幹となる運用基盤を整備することで、ビジネスの健全性・信頼性が高まります。

ITコンプライアンスを支える管理製品

- **資産・配布管理**
  IT資産の把握、セキュリティ脆弱性対策状況の把握、IT資産の利用実態やライセンスの管理、ソフトウェアの一括配布、および各種操作ログの管理を実現。
  また、セキュリティに問題があるクライアントPCの検査・隔離・治療・回復といった検疫システムを構築できます。
  クライアントPCや業務サーバの操作記録（証跡記録）の取得により、ITによる内部統制の強化を支援します。

- **セキュリティ管理**
  組織内での情報の共有化を推進しつつ、メディア・印刷による機密情報の不正な持ち出しを防ぎます。
  また、モバイルPC上のデータやリムーバブルメディア内の情報を暗号化することで、万一紛失や盗難に遭った場合にも第三者による解読を防げます。

uVALUE

2
本日ご紹介するITコンプライアンス製品一覧

HITACHI
Inspire the Next

2 本日ご紹介するITコンプライアンス製品一覧

JP1管理分野	製品名	概要
資産・配布管理	JP1/NETM/AIM	IT資産のライフサイクルをトータルで管理
	JP1/NETM/DM	クライアントやサーバの ハードウェア・ソフトウェア資産を一元管理
	JP1/NETM/CSC	クライアントの資産をセキュリティの観点から PDCAサイクルで管理
	JP!/NETM/NM	情報システム内への不正接続を排除し、 システムのセキュリティを維持
セキュリティ管理	JP1/秘文	ディスクやメディアの暗号化、持ち出し制御 による情報漏えい対策

【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

uVALUE

3
進化したITコンプライアンスの新機能紹介

HITACHI
Inspire the Next

3 進化したITコンプライアンスの新機能紹介

資産・配布管理(JP1/NETM)

章No.	新機能概要
3-1	効率の良いOSのパッチ配布運用を実現したい。
3-2	クライアントPCの操作ログを活用した追跡や評価を容易に行いたい。
3-3	ソフトウェアの稼働情報を活用し、部署別に適切なライセンス管理をしたい。
3-4	部署別セキュリティ対策状況を簡単に把握したい。
3-5	不正PCの排除とその状況を管理したい。

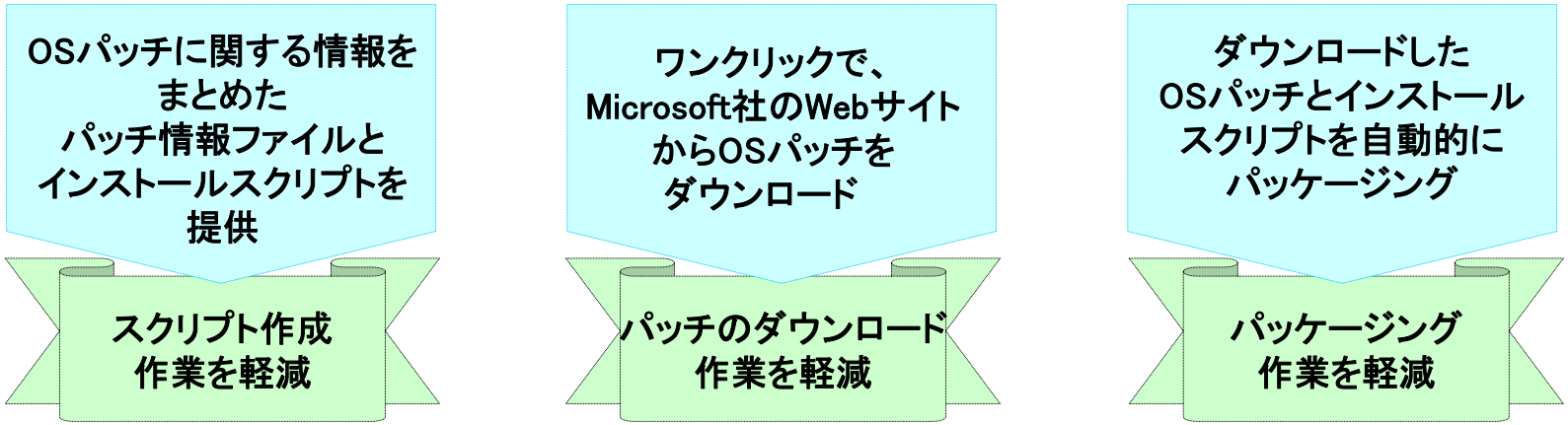
セキュリティ管理(JP1/秘文)

章No.	新機能概要
3-6	社外でデータの編集を安全に行いたい。

効率の良いOSのパッチ配布運用を実現したい

効果 OSパッチ適用作業が大幅に簡易化されるため、システム管理者の負担を軽減できます。

●OSパッチの自動パッケージング機能をサポートします。
従来はシステム管理者が、Microsoft社のWebサイトを定期的に確認、パッチをダウンロードしてスクリプトを作成し、パッケージングを行う必要がありました。

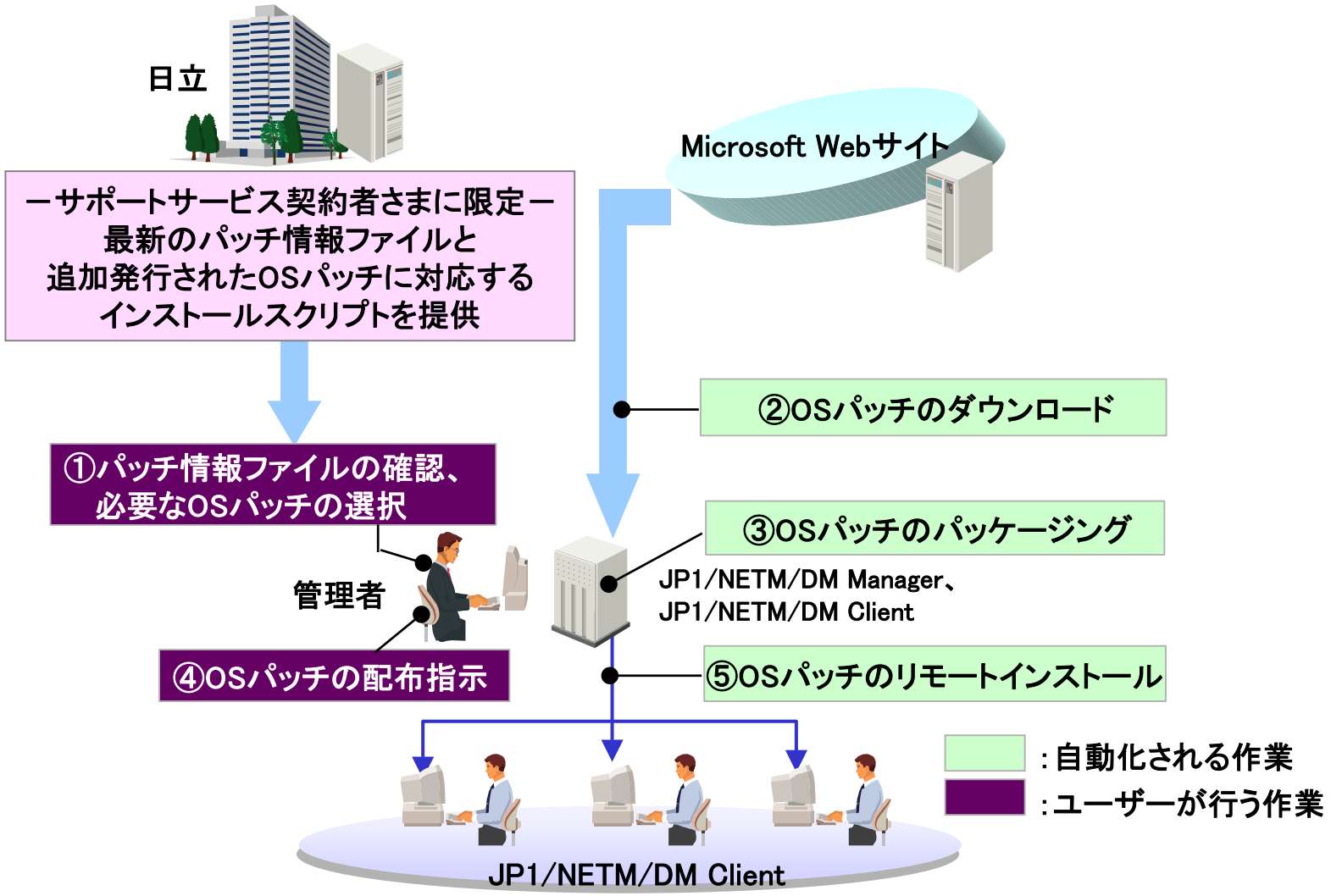


提供する情報
・2006年1月以降に発行のOSパッチに関する情報をまとめたパッチ情報ファイルとスクリプトを提供します。

JP1/NETM/DM 08-10では、
2006年1月から2007年2月に発行されたOSパッチのパッチ情報ファイルとスクリプトを製品に同梱します。
※2007年3月以降に発行されるOSパッチのパッチ情報ファイルとスクリプトは、
サポートサービス契約者さまに限定しての提供となります。

効率の良いOSのパッチ配布運用を実現したい

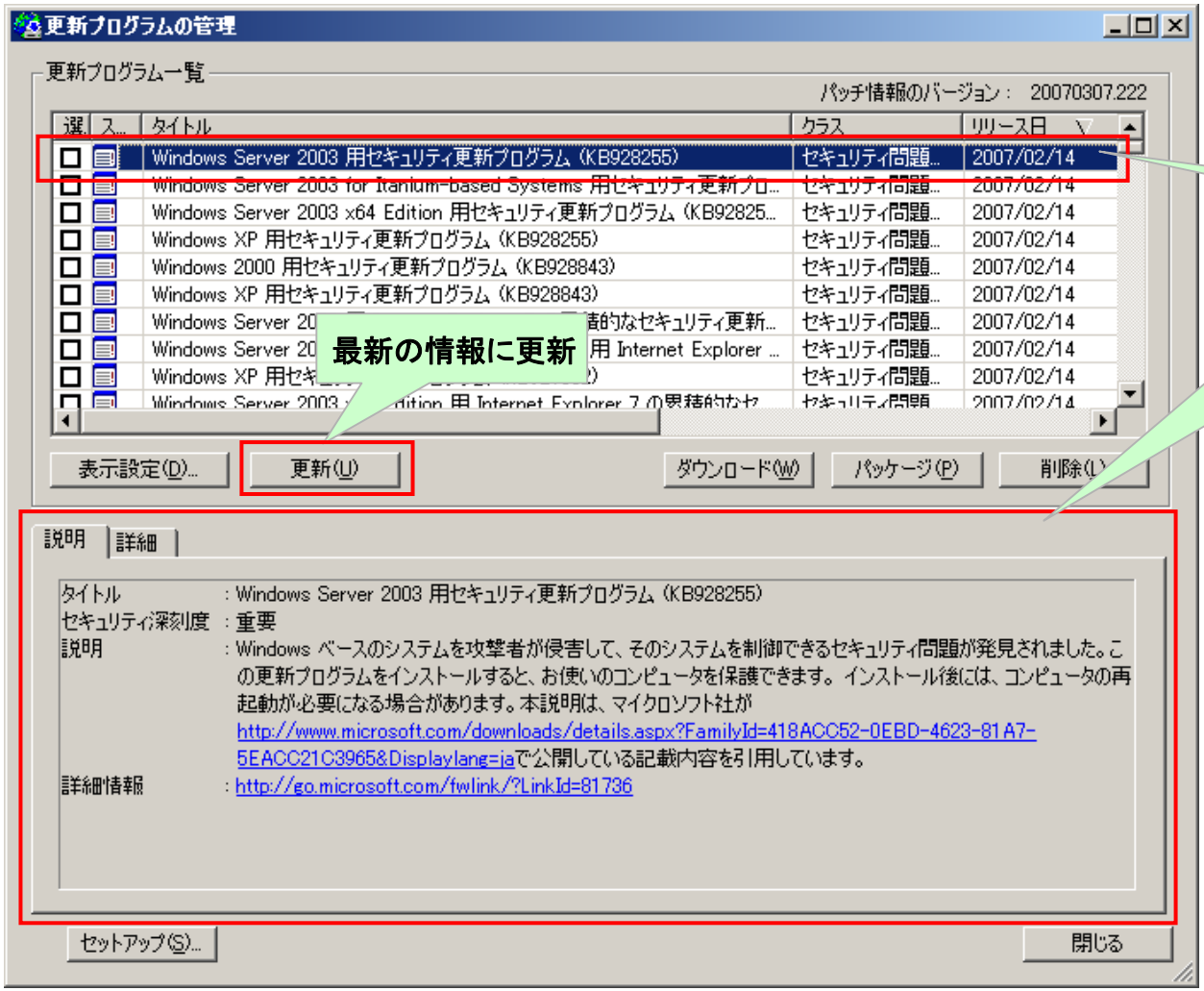
●OSパッチ配布の運用イメージを下図に示します。



効率の良いOSのパッチ配布運用を実現したい

●OSパッチの配布を下記の手順で実行します。

① リモートインストールマネージャのメニュー[オプション]から「更新プログラムの管理」を起動します。



② [更新]ボタンをクリックして、
最新の情報に更新します。

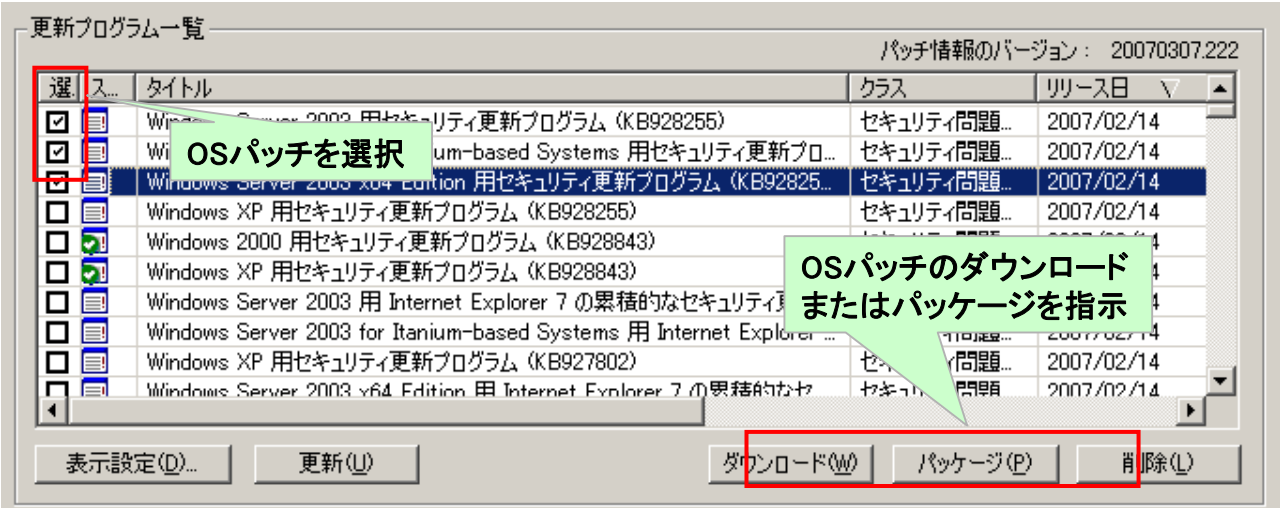
一覧でフォーカスしたOSパッチの
「説明」と「詳細」を表示します。

＜説明タブ＞
・タイトル
・セキュリティ深刻度
・説明
・詳細情報
（Microsoft社Webサイトへのリンク）

＜詳細タブ＞
・クラス
・製品
・リリース日
・サポート技術情報
・セキュリティ番号
・更新プログラムID
・言語
・更新プログラムのダウンロードURL

効率の良いOSのパッチ配布運用を実現したい

③ 一覧から、必要なOSパッチを選択し、[ダウンロード]または[パッケージ]ボタンをクリックします。



＜ステータスアイコン＞

- OSパッチを ダウンロードしていない
- OSパッチを ダウンロード、または パッケージ済

＜表示設定ボタン＞
画面上に表示する項目の「表示」あるいは「非表示」設定 、製品とクラスについてのフィルタリング設定ができます。

＜更新ボタン＞
（サポートサービス契約者さまの場合）「更新プログラム一覧」を最新の情報に更新できます。

＜ダウンロードボタン＞
「更新プログラム一覧」で選択したOSパッチをMicrosoft社Webサイトからダウンロードします。

＜パッケージボタン＞
「更新プログラム一覧」で選択したOSパッチをMicrosoft社Webサイトからダウンロードし、パッケージングします。

＜削除ボタン＞
「更新プログラム一覧」で選択して取得したダウンロード済みのOSパッチの実行ファイルを削除します。

④ リモートインストールマネージャから、配布先とパッケージを指定して、配布指示を実行します。

効率の良いOSのパッチ配布運用を実現したい

●下記のパッチのダウンロードをサポートします。(2007年3月時点)

#	サポート対象のパッチ	対応バージョン
1	Windows Vista	
2	Windows Server 2003	
3	Windows XP	
4	Windows 2000	Service Pack 2以降
5	Microsoft .NET Framework	1.0, 1.1, 2.0
6	Internet Explorer	6.0, 7.0
7	Outlook Express	5.5, 6.0
8	Windows Media Player	7.1, 9.0, 10.0
9	Microsoft Data Access Components	2.5, 2.7, 2.8

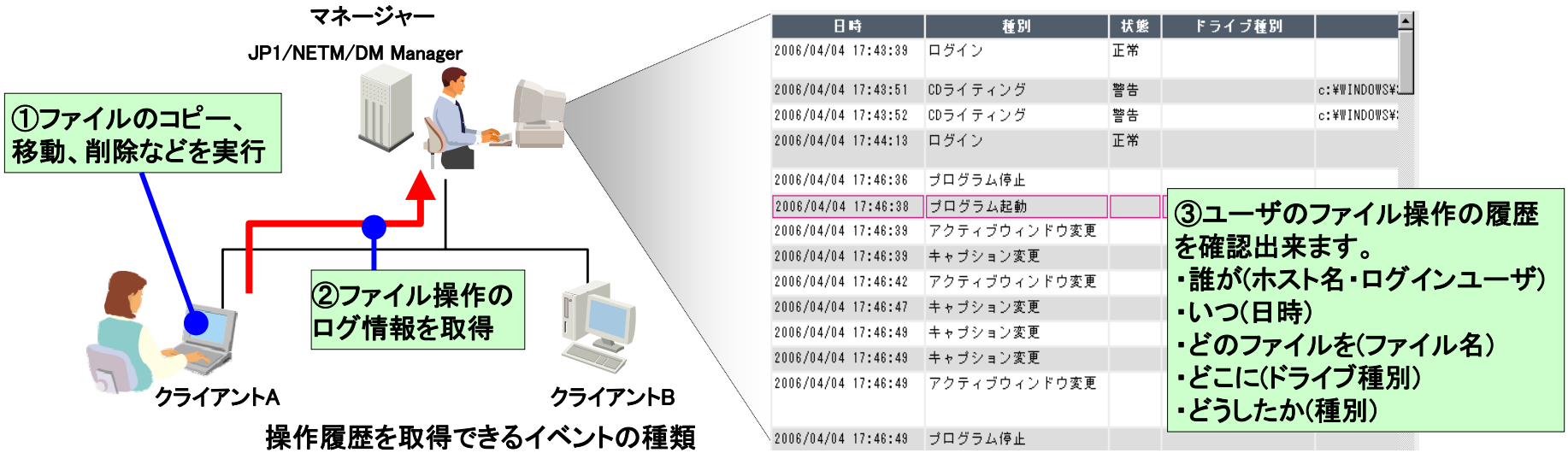
注意事項

・上記プログラムに対応したパッチのうち、JP1/NETM/DMで取得できる種別(クラス)は次の4種類です。
　＊重要な更新
　＊セキュリティ問題の修正プログラム
　＊Service Pack (ただしWindowsに関するService Packは取得できません)
　＊修正プログラム集
・JP1/NETM/DM Clientがサポートしているパッチがサポート対象です。
　Microsoft Office、Microsoft SQL Server、Microsoft Exchange Server 、Microsoft Internet Information Serverなどのパッチは含みません。
・パッチカタログファイルに登録されているパッチ(MSのWebサイトよりダウンロード可能なもの)のみサポートします。

クライアントPCの操作ログを活用した追跡や評価を容易に行いたい

効果 操作ログを取得、集計、追跡調査することで、情報の扱われ方が把握でき、定期監査や運用改善に利用できます。

●取得可能な操作履歴にファイル操作が加わりました。
エクスプローラ上でのファイル操作の履歴情報を、検索・表示できます。



操作履歴を取得できるイベントの種類

イベント	説明
プロセスの起動	プログラムの起動時のイベント
プロセスの停止	プログラムの停止時のイベント
キャプションの変更	ウィンドウタイトルの変更時のイベント
アクティブウィンドウの変更※1	アクティブウィンドウの切り替え時のイベント
マシンの起動/停止	PCの起動または停止時のイベント
ログオン/ログオフ	ログオンまたはログオフ時のイベント
ファイル操作	**Windowsのエクスプローラ上のファイル操作のイベント(※2)**

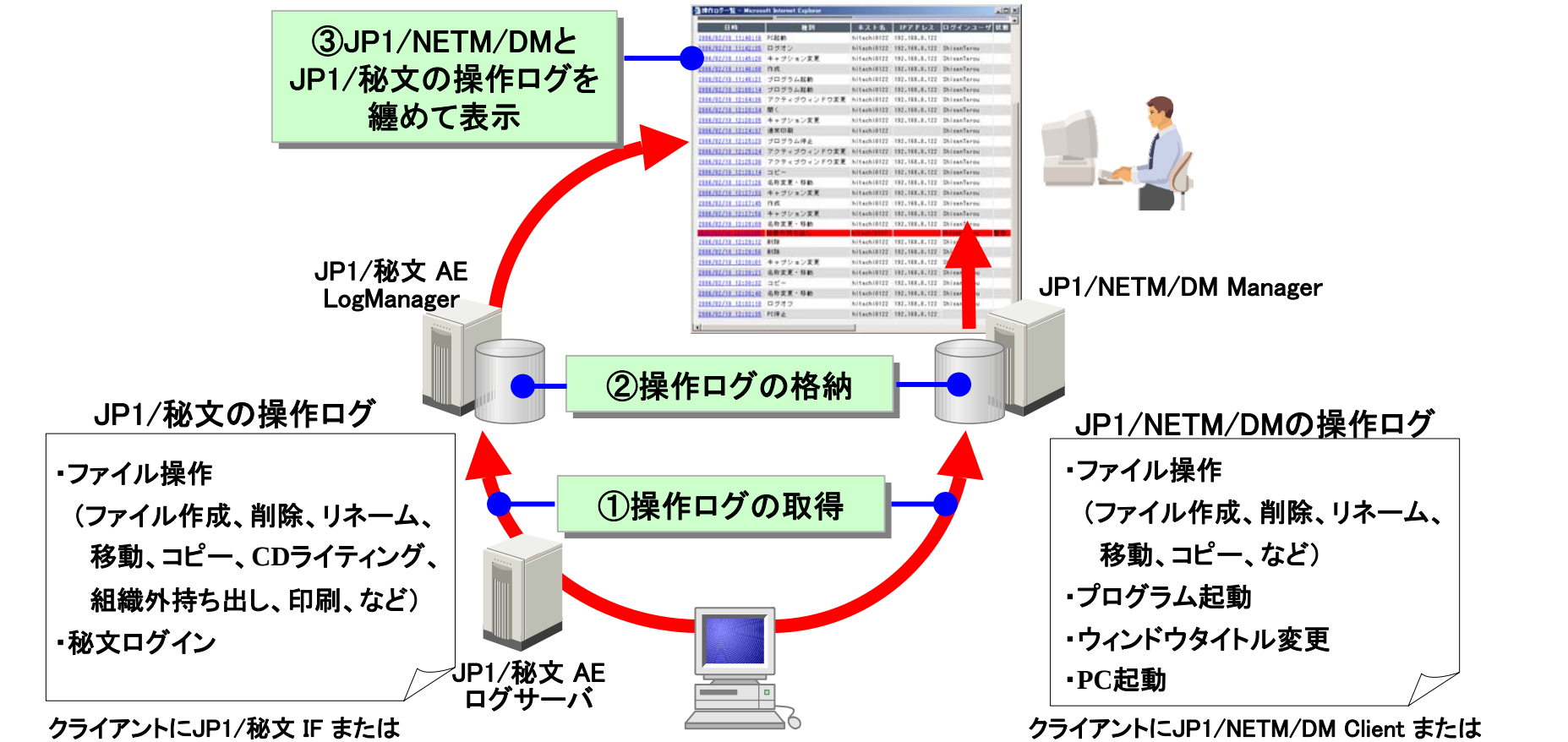
今回追加

注※1 :JavaやVisual Basicで作成されたソフトウェアは，アクティブウィンドウの変更イベントを取得できません。

注※2 :カスタマイズされたコモンダイアログでは，操作履歴を取得できない場合があります。

クライアントPCの操作ログを活用した追跡や評価を容易に行いたい

●JP1/NETM/DMで取得した操作ログとJP1/秘文で取得した操作ログを、検索・表示できます。
特定の操作のログに絞り込むことも、複数の操作のログをマージして表示することもできます。



クライアントにJP1/秘文 IF または
JP1/秘文 IF＋IC または JP1/秘文 IF＋IS
または JP1/秘文 IF＋IC＋ISが必要です

クライアントにJP1/NETM/DM Client または
JP1/NETM/DM Client – Base＋
JP1/NETM/DM Client – Operation Log Featureが必要です

クライアントPCの操作ログを活用した追跡や評価を容易に行いたい

●取得可能な情報は下記の通りです。

項目名	JP1/NETM/DM	JP1/秘文 LogManager
作　成	ファイル作成 フォルダ作成	作成（アクセス対象が「プリンタ」を除く） フォルダ作成
開　く	ファイルオープン	オープン 書き込み
削　除	ファイル削除 フォルダ削除	削除 フォルダ削除
コピー	ファイルコピー フォルダコピー	コピー フォルダコピー
名前変更・移動	ファイル移動 フォルダ移動 ファイル名称変更 フォルダ名称変更	名称変更・移動
CDライティング	ー	ライティングソフト
組織外持ち出し	ー	組織外持ち出し
平文持ち出し	ー	平文持ち出し
機密ファイル作成	ー	機密ファイル作成
通常印刷	ー	通常印刷
透かし印刷	ー	すかし印刷

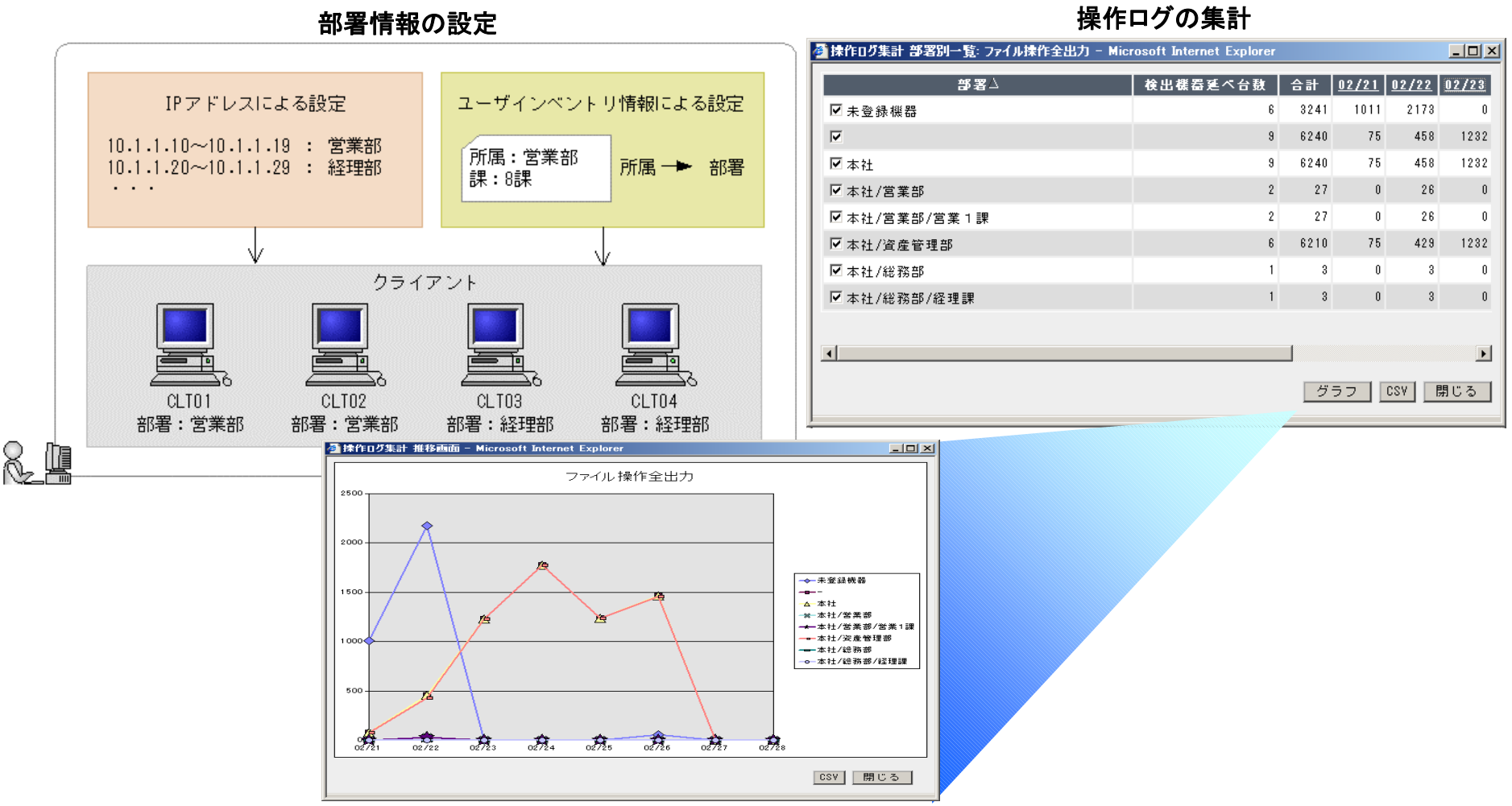
3-2 クライアントPCの操作ログを活用した追跡や評価を容易に行いたい

資産・配布管理 Win

JP1/NETM/DM

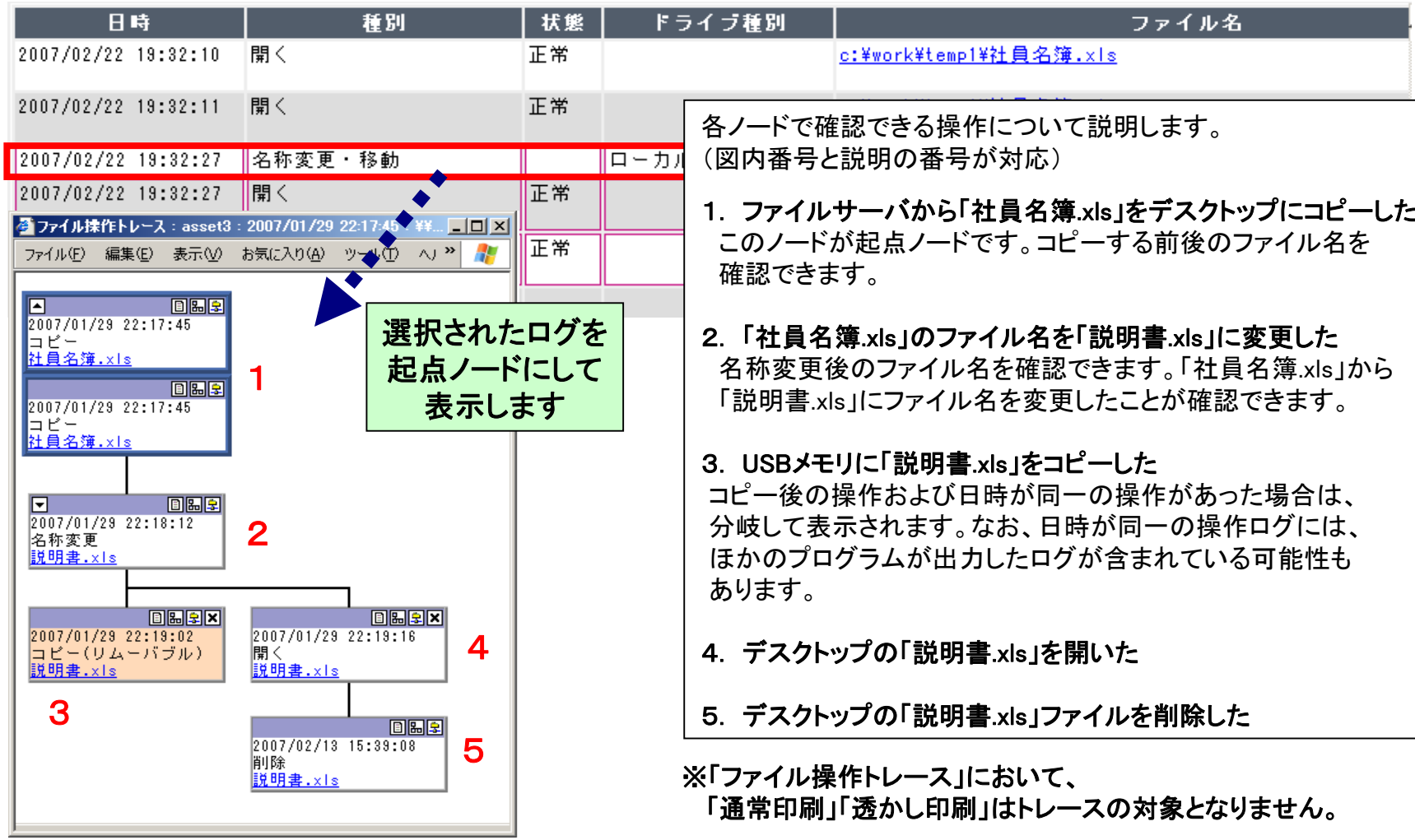
NEW 08-10

●操作ログを集計することで、特定の操作が1日当たりどのくらい行われたか、操作ログの検出結果の推移などを確認できます。例えば、リムーバブルディスクへのコピー操作を集計することで、頻繁に外部へ情報を持ち出しているクライアントを調査できます。



クライアントPCの操作ログを活用した追跡や評価を容易に行いたい

●ある特定ファイルの操作ログから、そのファイルの操作経路を追跡できるようにしました。
これにより、誰がどこに機密情報ファイルを移動させたかなどを把握することができ、情報漏えい時のファイル流出経路の調査や、重要ファイルに対する操作形跡の視覚的な確認に活用できます。



各ノードで確認できる操作について説明します。
（図内番号と説明の番号が対応）

1. **ファイルサーバから「社員名簿.xls」をデスクトップにコピーした**
   このノードが起点ノードです。コピーする前後のファイル名を確認できます。

2. **「社員名簿.xls」のファイル名を「説明書.xls」に変更した**
   名称変更後のファイル名を確認できます。「社員名簿.xls」から「説明書.xls」にファイル名を変更したことが確認できます。

3. **USBメモリに「説明書.xls」をコピーした**
   コピー後の操作および日時が同一の操作があった場合は、分岐して表示されます。なお、日時が同一の操作ログには、ほかのプログラムが出力したログが含まれている可能性もあります。

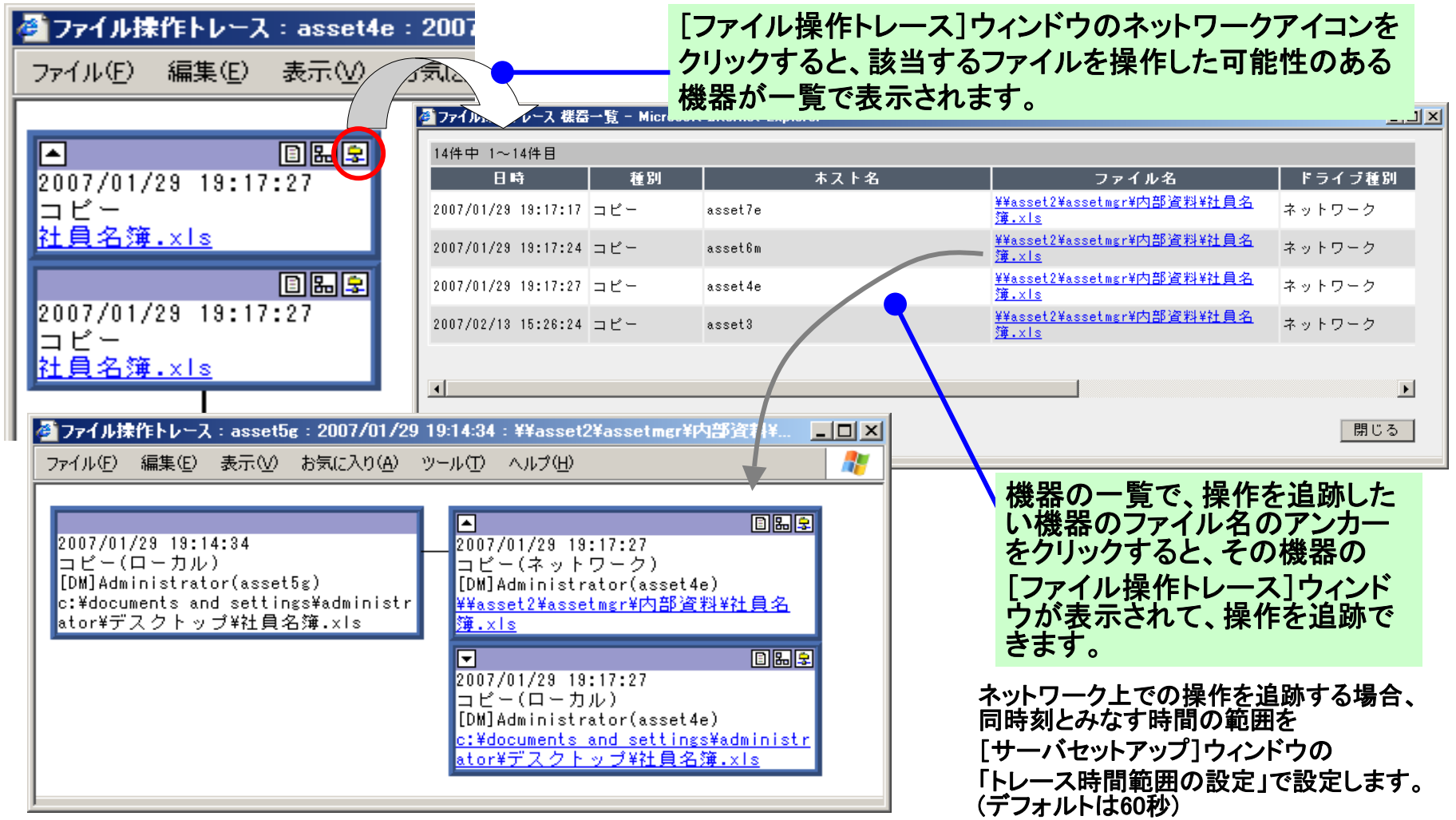
4. **デスクトップの「説明書.xls」を開いた**

5. **デスクトップの「説明書.xls」ファイルを削除した**

※「ファイル操作トレース」において、
「通常印刷」「透かし印刷」はトレースの対象となりません。

クライアントPCの操作ログを活用した追跡や評価を容易に行いたい

●[ファイル操作トレース]ウィンドウのネットワークアイコンを利用すると、ネットワーク上の別の機器からの操作を追跡できます。この為、ネットワークを利用したファイル持ち出しも監視できます。



[ファイル操作トレース]ウィンドウのネットワークアイコンをクリックすると、該当するファイルを操作した可能性のある機器が一覧で表示されます。

機器の一覧で、操作を追跡したい機器のファイル名のアンカーをクリックすると、その機器の[ファイル操作トレース]ウィンドウが表示されて、操作を追跡できます。

ネットワーク上での操作を追跡する場合、同時刻とみなす時間の範囲を[サーバセットアップ]ウィンドウの「トレース時間範囲の設定」で設定します。(デフォルトは60秒)

3-3 ソフトウェアの稼働情報を活用し、部署別に適切なライセンス管理をしたい

資産・配布管理 | Win

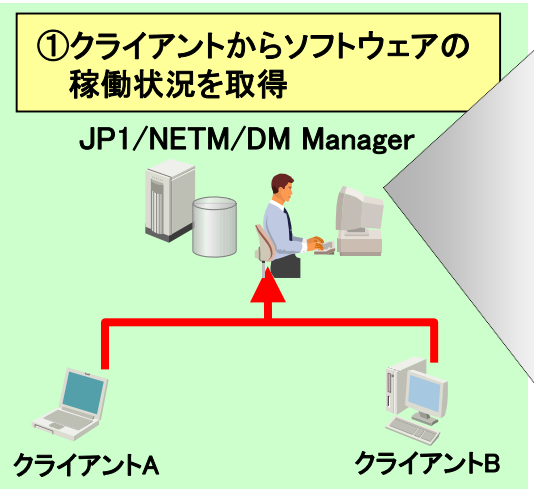
JP1/NETM/DM

NEW 08-10

効果 ライセンス管理を適切に行うことで、ライセンス違反の防止や、遊休ライセンスの把握ができ、効果的な投資を実現できます。

●ソフトウェアの稼働状況(稼働時間、利用台数、月ごとの利用率など)を参照できるようになりました。

①クライアントからソフトウェアの稼働状況を取得



検索 CSV

検索開始月	2007/03
ソフトウェア名	を含む
バージョン	
ホスト名	全一致
IPアドレス	完全一致

②各ソフトウェアの稼働時間、稼働台数、利用している機器の稼働時間を表示

ソフトウェア名	ソフトウェア稼働時間	PC稼働時間	稼働台数
SoftA,ver1	15	36	6
SoftB,ver1	2	4	1
SoftC,ver01	1	11	1

ソフトウェア稼働状況 資産一覧:softA - Microsoft Internet Explorer

稼働率 表示 CSV

ホスト名	IPアドレス	2007/01	2007/02
HostA	192.168.0.1	50%	37.5%
HostB	192.168.0.2	37.5%	77.5%
HostC	192.168.0.3	37.5%	50%
HostD	192.168.0.4	40.9%	50.9%
HostE	192.168.0.5	50%	30%
HostF	192.168.0.6	50%	70%

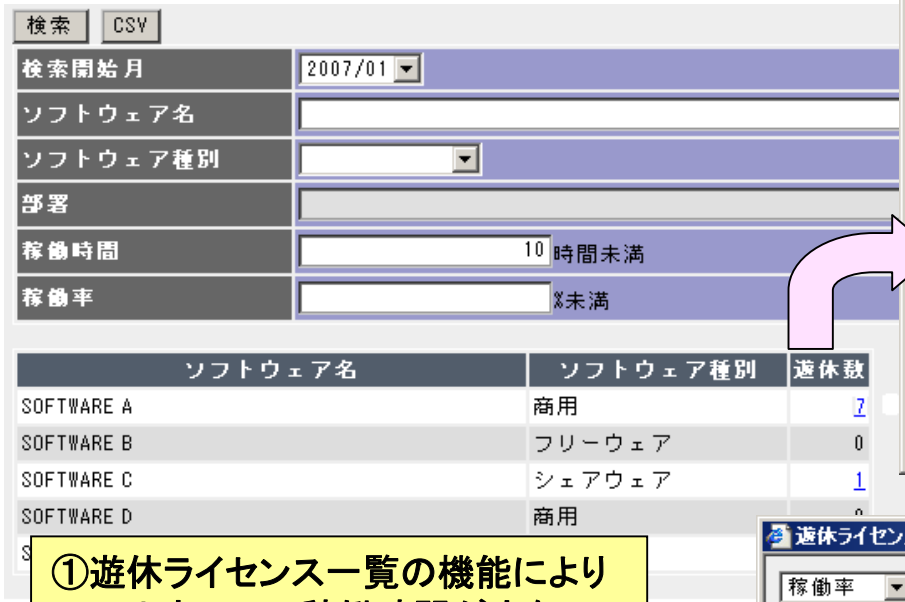
閉じる

③各ソフトウェアを利用している機器の一覧と、月ごとの利用状況を表示

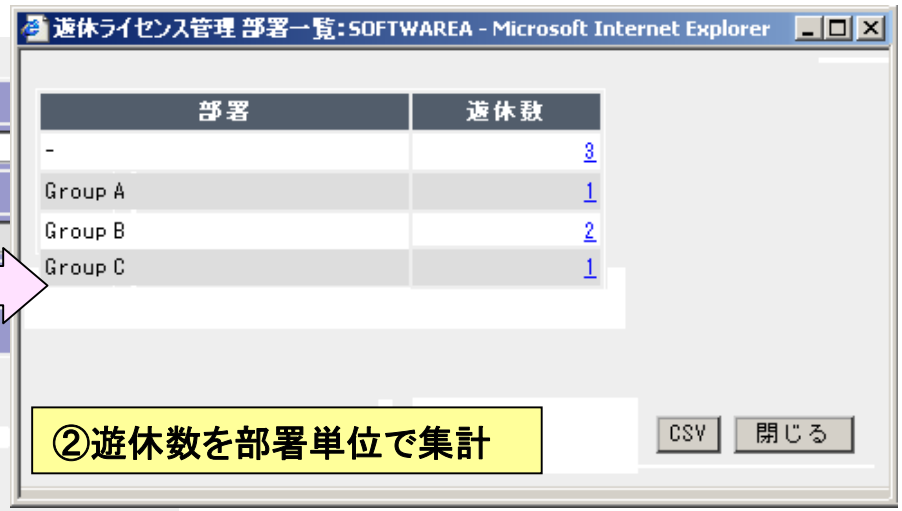
3-3 ソフトウェアの稼働情報を活用し、部署別に適切なライセンス管理をしたい

資産・配布管理 Win
JP1/NETM/AIM
NEW 08-10

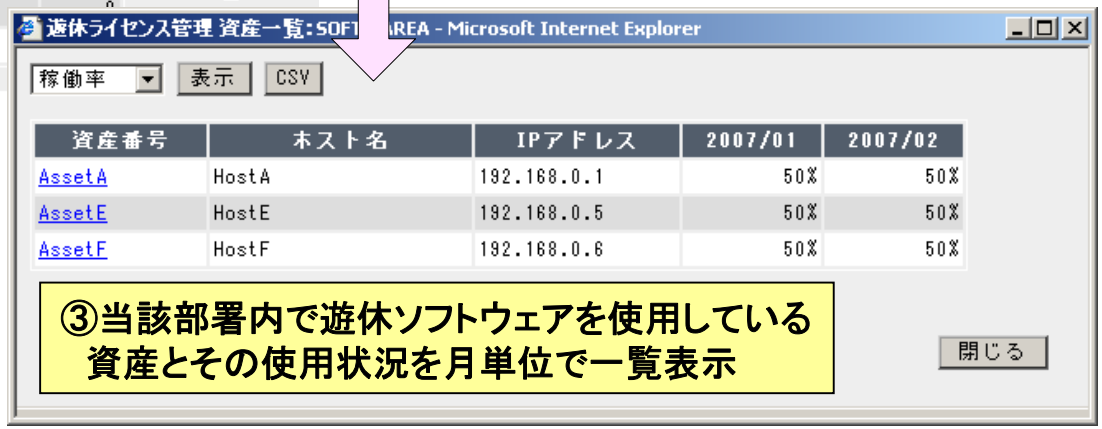
●JP1/NETM/DMで管理しているソフトウェアの稼働状況をもとに、JP1/NETM/AIMにて、使用頻度の低いソフトウェアを検出できるようになりました。ライセンスを割り当てていても使用していないソフトウェアを検出して、他の申請者に割り当てたり、契約更新やバージョンアップ版購入数の見直しを行うなど、ライセンス利用の最適化を図ることができます。



①遊休ライセンス一覧の機能により
ソフトウエアの稼働時間が少ない
機器数を集計



②遊休数を部署単位で集計



③当該部署内で遊休ソフトウェアを使用している
資産とその使用状況を月単位で一覧表示

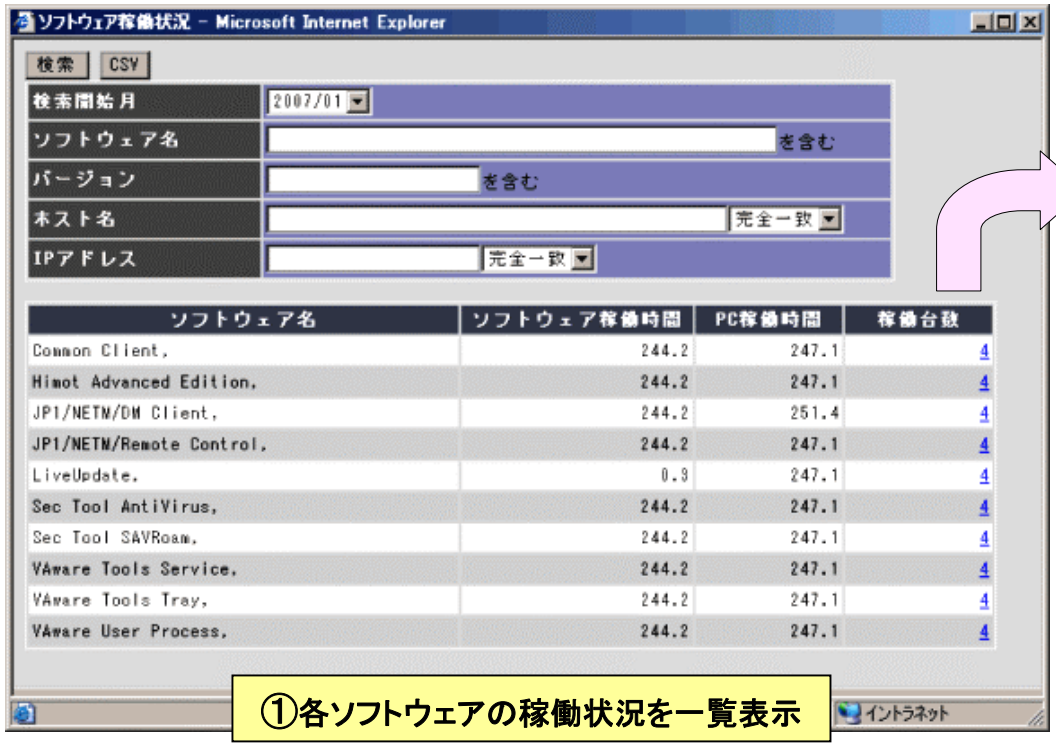
3-3 ソフトウェアの稼働情報を活用し、部署別に適切なライセンス管理をしたい

資産・配布管理 | Win

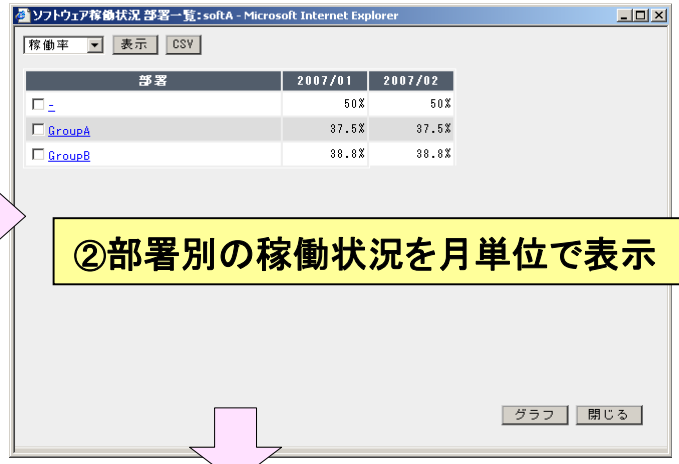
JP1/NETM/AIM

NEW 08-10

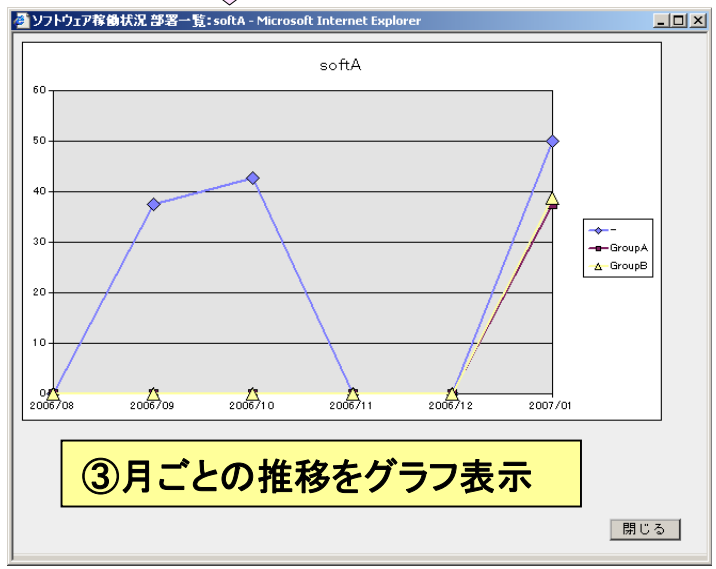
●JP1/NETM/DMで管理しているソフトウェアの稼働状況をもとに、JP1/NETM/AIMにおいて、部署単位での稼働状況（稼働率）と、その推移を把握することができます。



①各ソフトウェアの稼働状況を一覧表示



②部署別の稼働状況を月単位で表示



③月ごとの推移をグラフ表示

部署別セキュリティ対策状況を簡単に把握したい

効果　クライアントの資産をセキュリティの観点から状況把握ができ、効果的なセキュリティ改善策を講じることができます。

概　要

●クライアントの危険レベルを管理

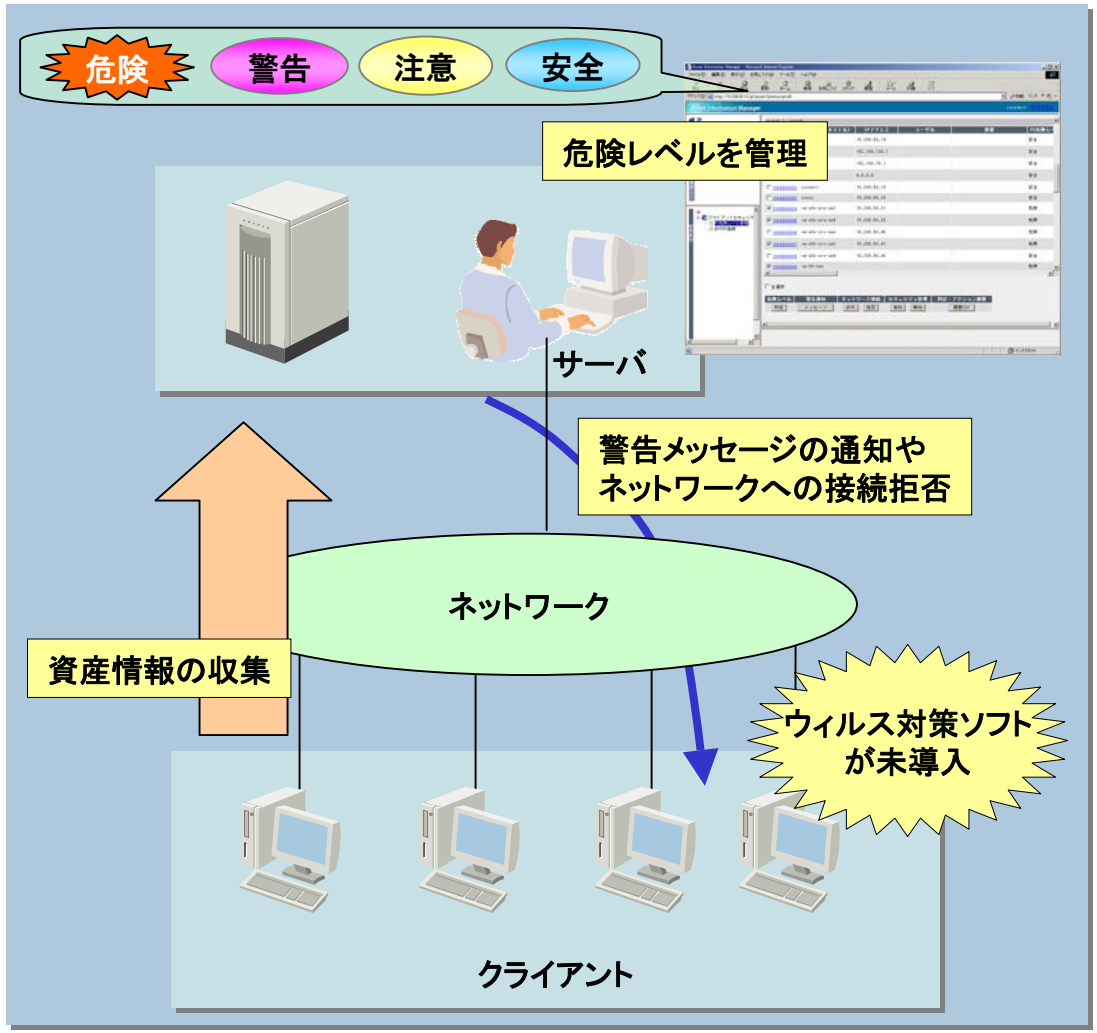
クライアントのセキュリティ対策の状況に応じた危険レベルをセキュリティポリシーで判定できます。管理者が設定したセキュリティポリシーに基づき、クライアントの危険レベル（「危険」「警告」「注意」「安全」）が自動的に判定され、Webブラウザの画面で管理することができます

●危険レベルに応じたアクションを実行

セキュリティ対策が不十分なクライアントを検知すると、クライアントの利用者に対して警告メッセージを通知したり、ネットワーク制御製品と連携してネットワークへの接続を拒否したり、管理者に対してメール通知するといったアクションを実施できます。

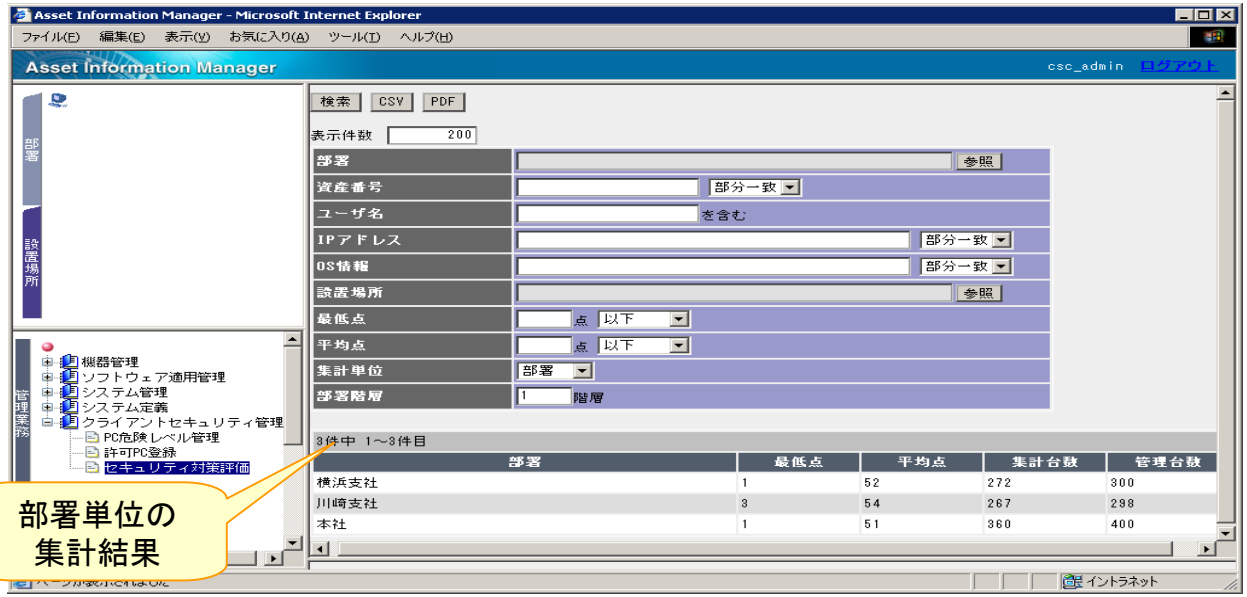
●JP1製品と連携

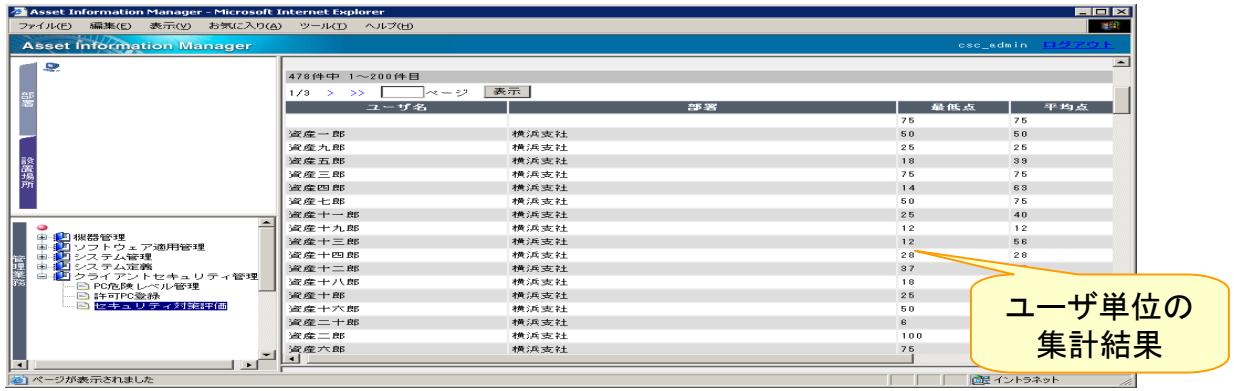
JP1/ 秘文がインストールされているかどうかを管理できます。また、JP1イベントをJP1/IMに通知し、JP1/IMの統合コンソールでセキュリティ対策が不十分なクライアントを検知できます。



部署別セキュリティ対策状況を簡単に把握したい

●危険レベルを点数で評価し、検索条件に一致したクライアントの評価点を表示します。
部署単位及びユーザ単位に表示することが可能です。





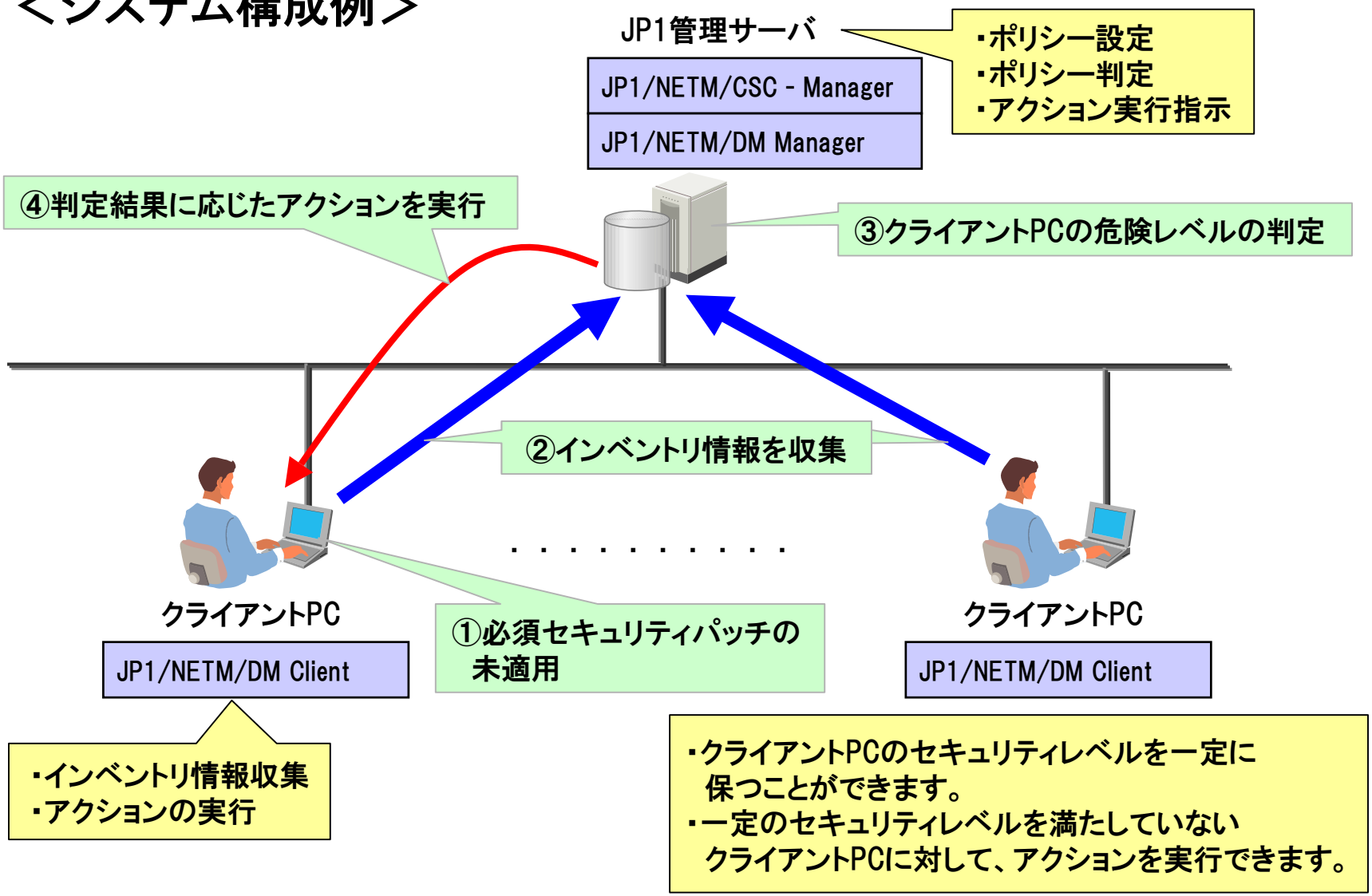
1. 検索
主な検索条件：
・集計単位（部署，ユーザ）
・部署
・OS情報
・最低点
・平均点
条件を組み合わせて対象のクライアントを表示させることができます。

2. 表示項目
・最低点
・平均点
・集計台数
・管理台数
・部署
・ユーザ名

評価点 = 100（点）
× （更新プログラムの係数）
× （ウィルス対策製品の係数）
× （不正ソフトウェアの係数）
× （必須ソフトウェアの係数）
× （ユーザ定義の係数）
【危険レベル係数】
安全 ： 1
注意 ： 0.75
警告 ： 0.5
危険 ： 0.25

部署別セキュリティ対策状況を簡単に把握したい

＜システム構成例＞



不正PCの排除とその状況を管理したい

効果　許可していないPCに対して、社内ネットワーク接続を排除することで、未許可PCからのウイルスの蔓延や情報漏えいを防止できます。

概　要

●不正に接続したPCの自動排除

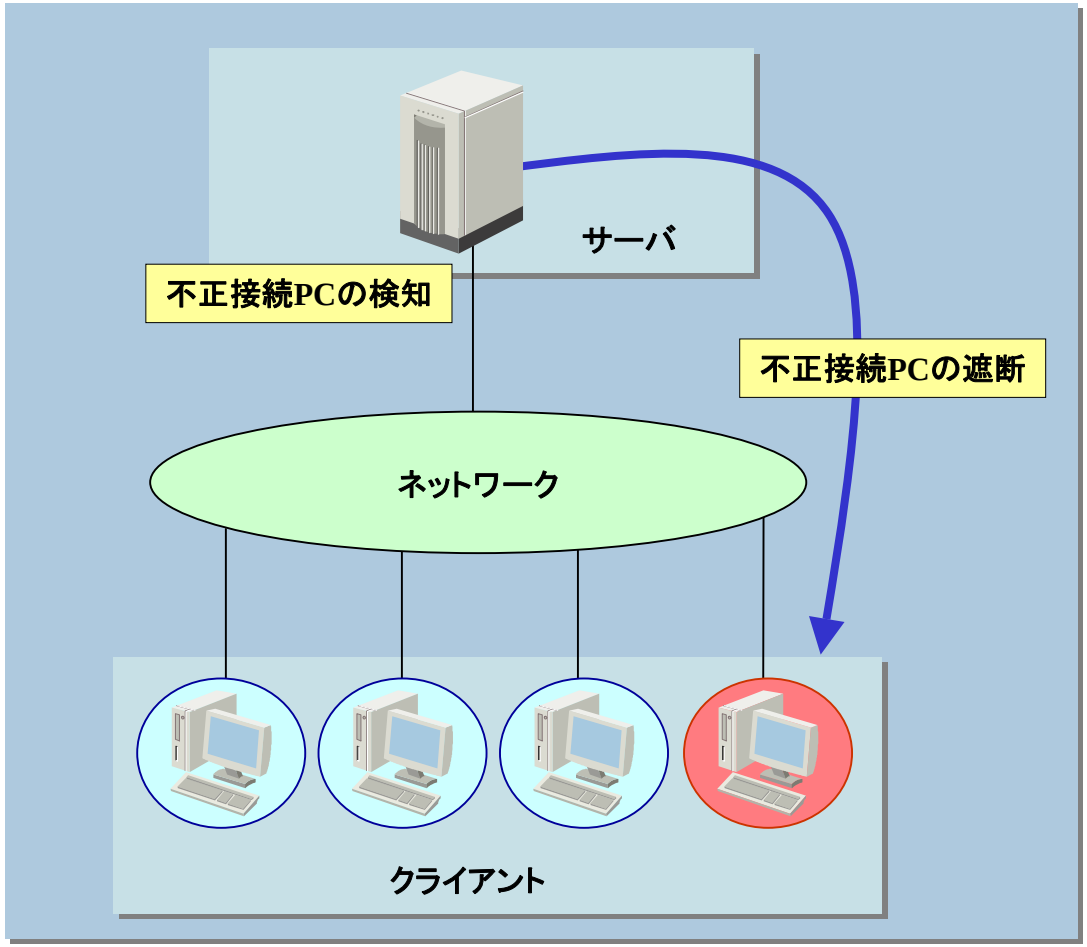
・不正接続PCの検出と対策（排除）を自動で行います。
・不正接続PCのみを、ピンポイントで即座に排除します。
・監視モードと排除モードがあります。
・MACアドレス/IPアドレス/IPアドレス範囲/MACベンダによる監視が行えます。

●他製品との組合せ、検疫システムの構築が可能

・検疫ネットワーク支援機能を利用して検疫システムを実現できます。
・JP1/NETMとの自動連携による検疫システムを構築できます。

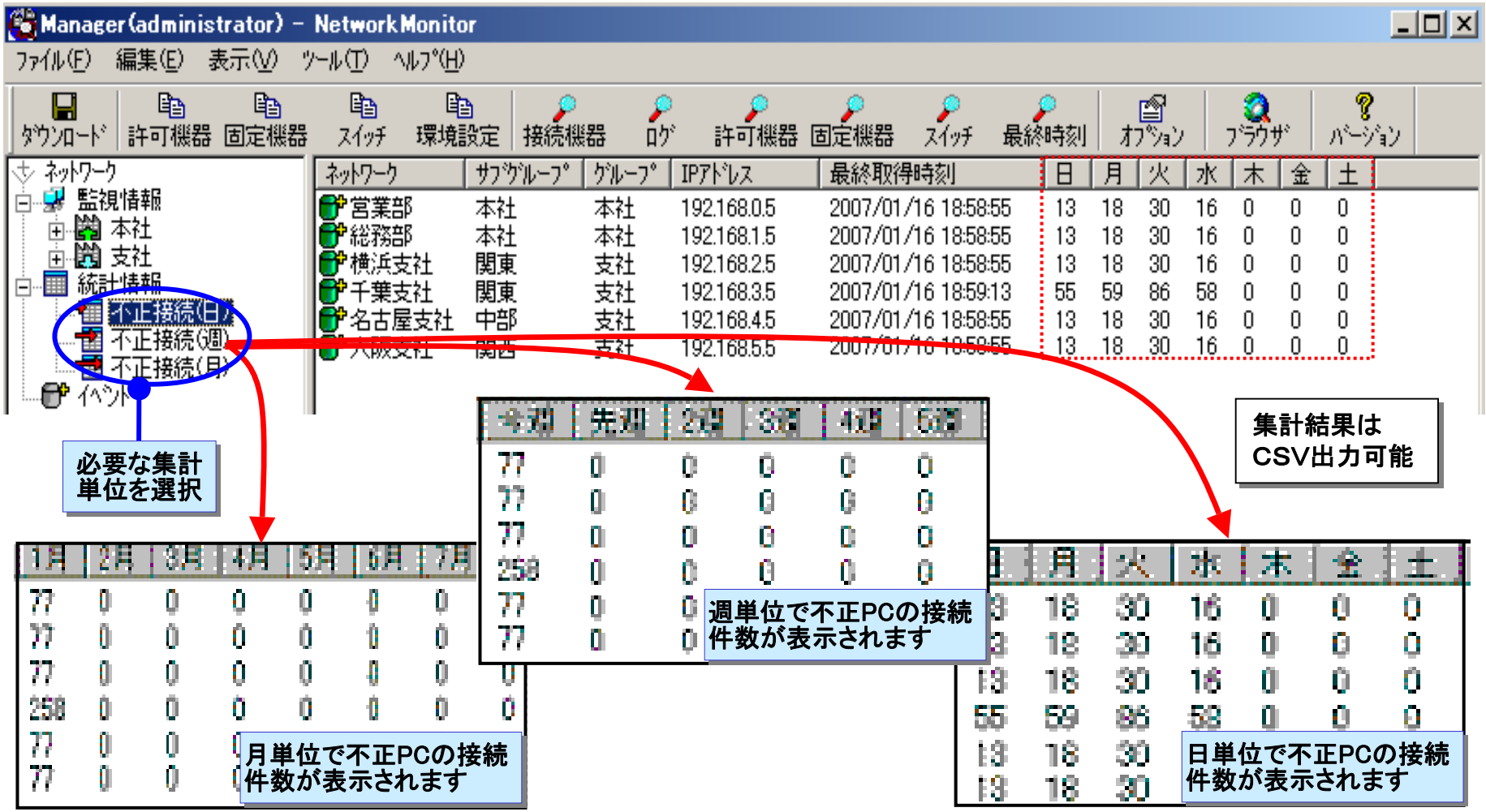
●既存ネットワークをそのまま利用可能

・クライアントソフトは不要です。
・アドレス環境（固定IP，DHCP）、有線（HUB、SW）、無線を問わず導入できます。
・クライアントソフト無しでPCの使用状況などが把握できます。



不正PCの排除とその状況を管理したい

● 不正PCの接続件数や機器の稼動状況を日、週、月単位で集計することができます。
これにより、管理者はPCの接続状況や稼動状況を統計的に把握することができます。

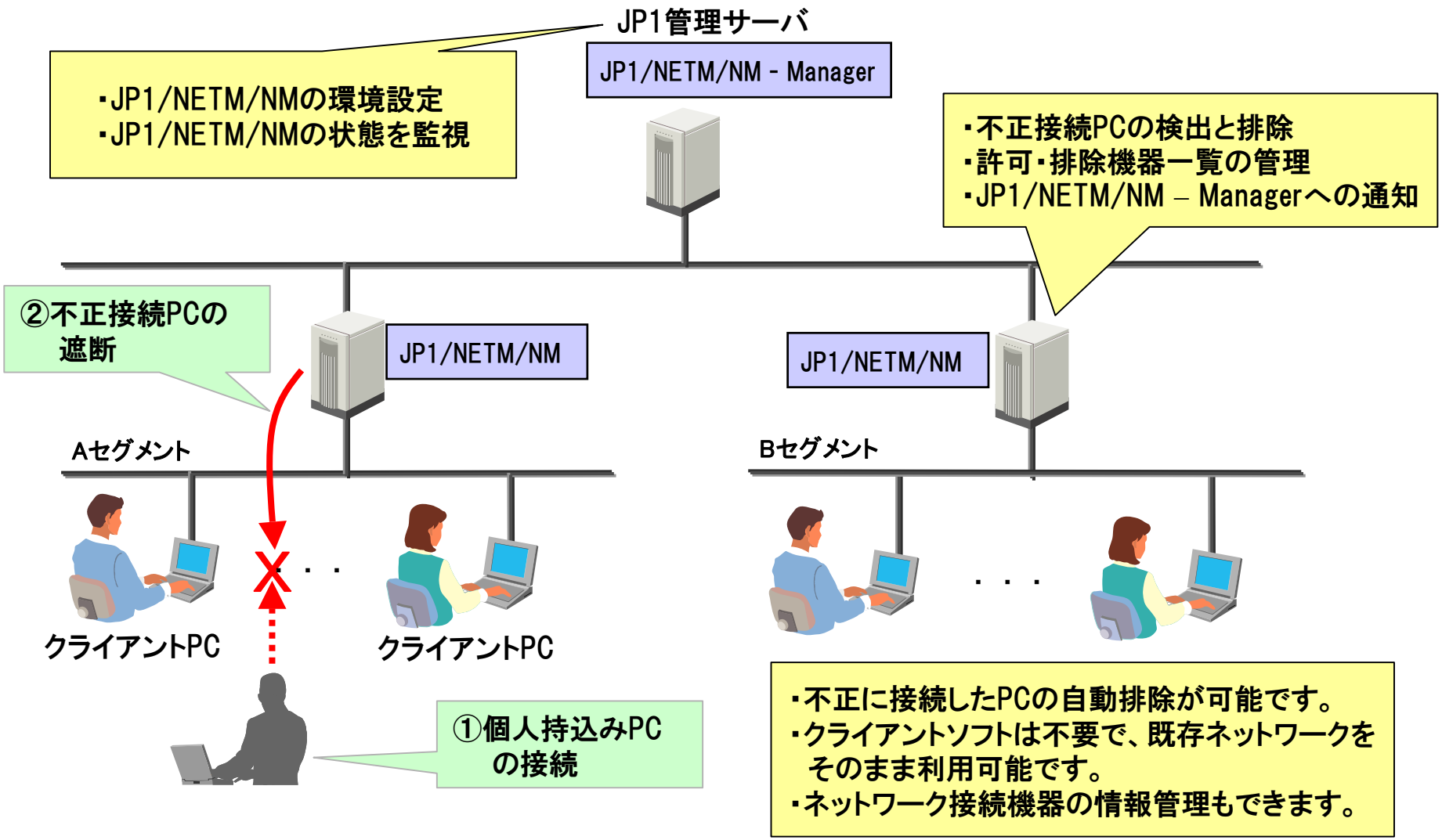


日、週、月ごとに不正PCの接続件数を表示します。不正PCの台数ではありません。
週は日曜～土曜を一週間とします。

結果は印刷可能です。

不正PCの排除とその状況を管理したい

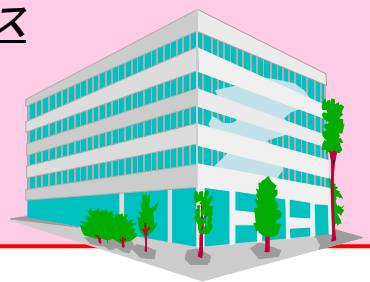
＜システム構成例＞

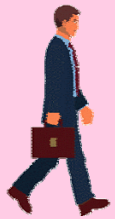


社外でデータの編集を安全に行いたい

効果 JP1/秘文 CGPの専用USBメモリを使うことで、社外でのデータの安全な編集と不用意なデータ流出の防止を両立できます。

オフィス



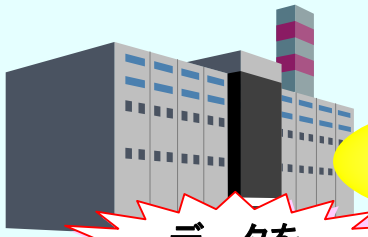


会社の情報をやむを得ず外出先に持ち出す

編集 OK！

ローカル保存 OK！

社外 （業務委託先etc）



データを残さない

外出先（委託先など）でも安心して業務データの編集が行えます

USBメモリ内での編集・保存のみ可能

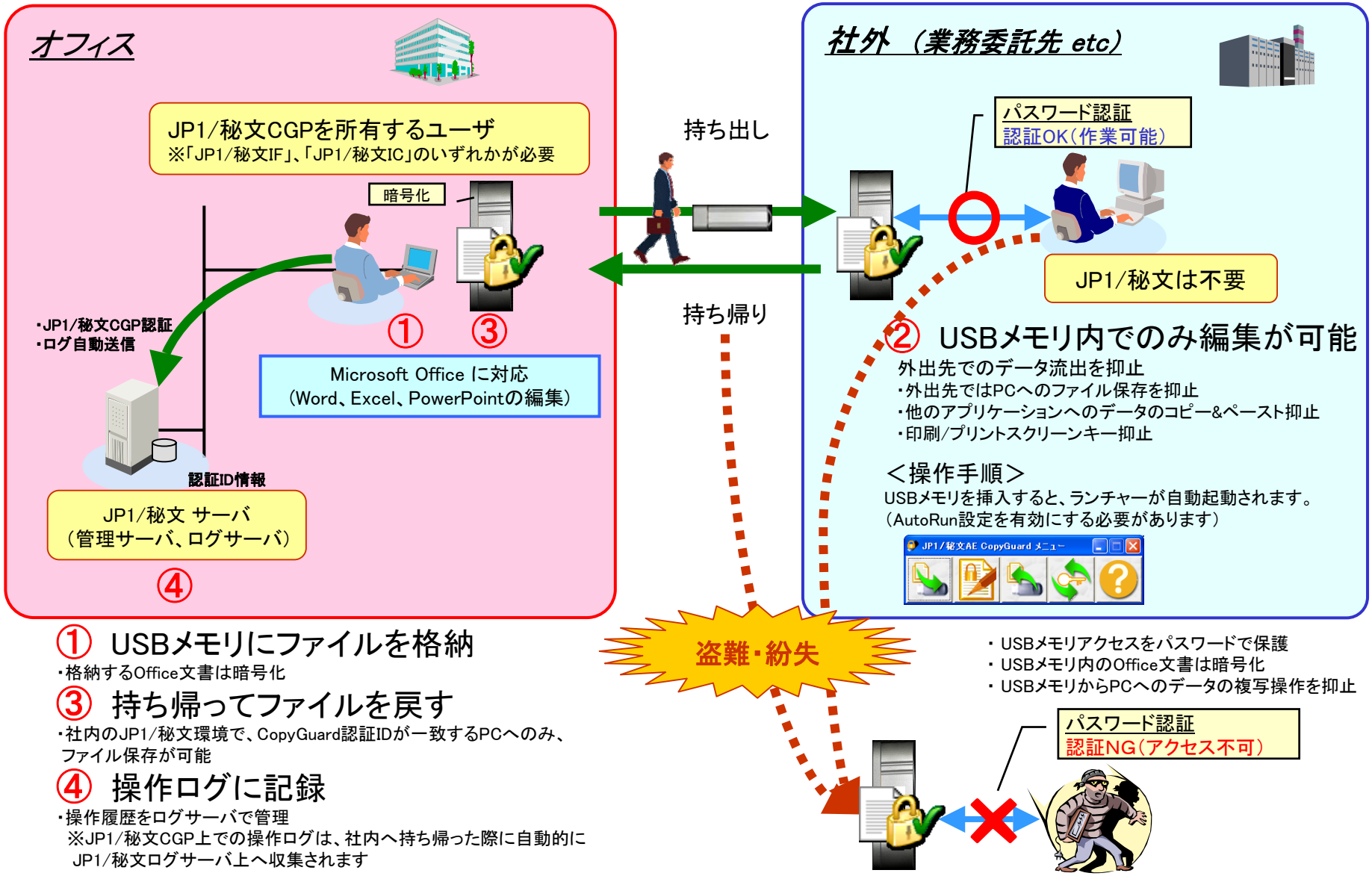
編集 OK！

ローカル保存 NG！

ローカルファイルへデータ貼付NG！
プリントスクリーンキーNG！
印刷NG！

【凡例】JP1/秘文 CGP：JP1/秘文 Advanced Edition CopyGuard Professional

社外でデータの編集を安全に行いたい



① USBメモリにファイルを格納

・格納するOffice文書は暗号化

③ 持ち帰ってファイルを戻す

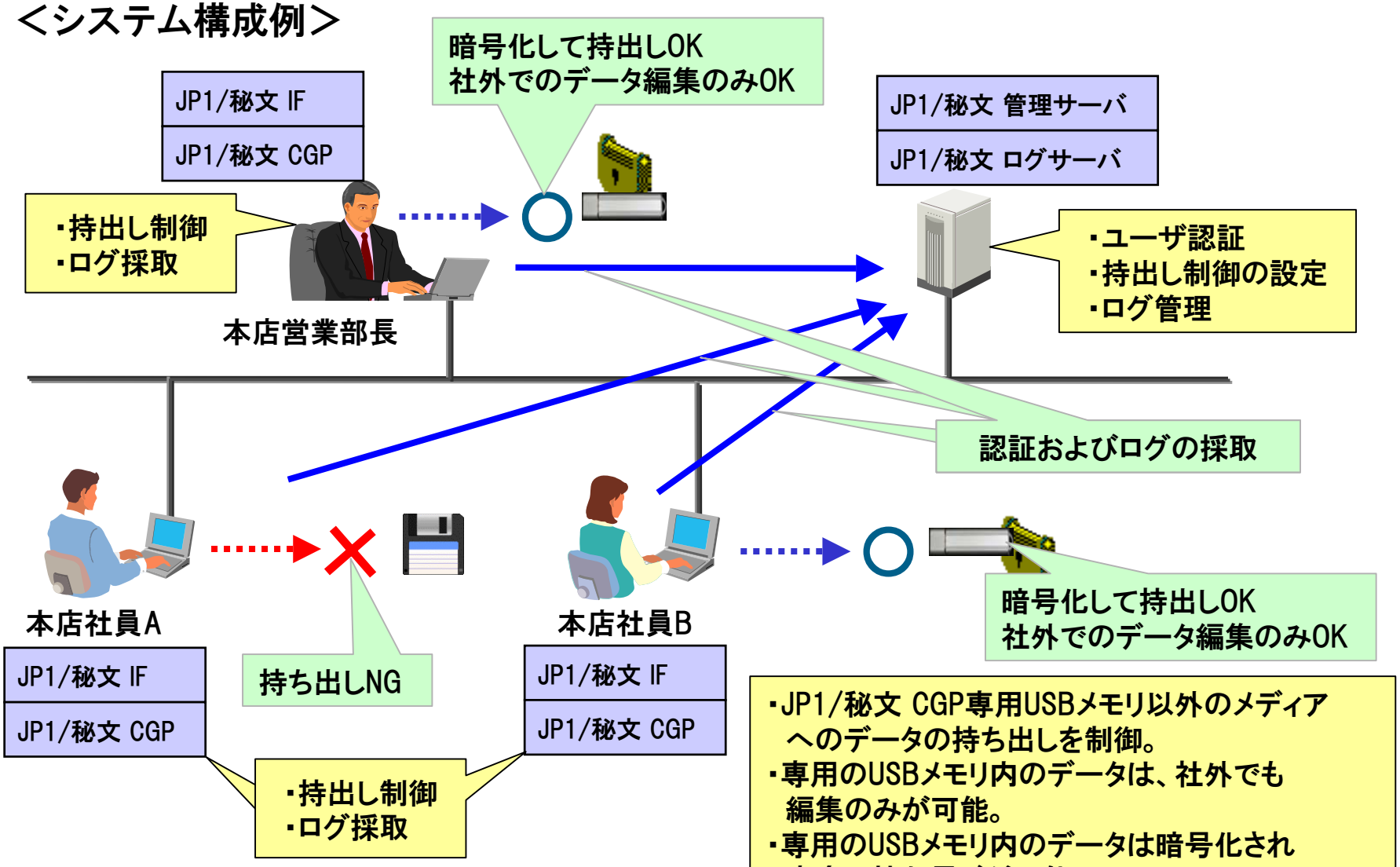
・社内のJP1/秘文環境で、CopyGuard認証IDが一致するPCへのみ、ファイル保存が可能

④ 操作ログに記録

・操作履歴をログサーバで管理
※JP1/秘文CGP上での操作ログは、社内へ持ち帰った際に自動的にJP1/秘文ログサーバ上へ収集されます

社外でデータの編集を安全に行いたい

＜システム構成例＞

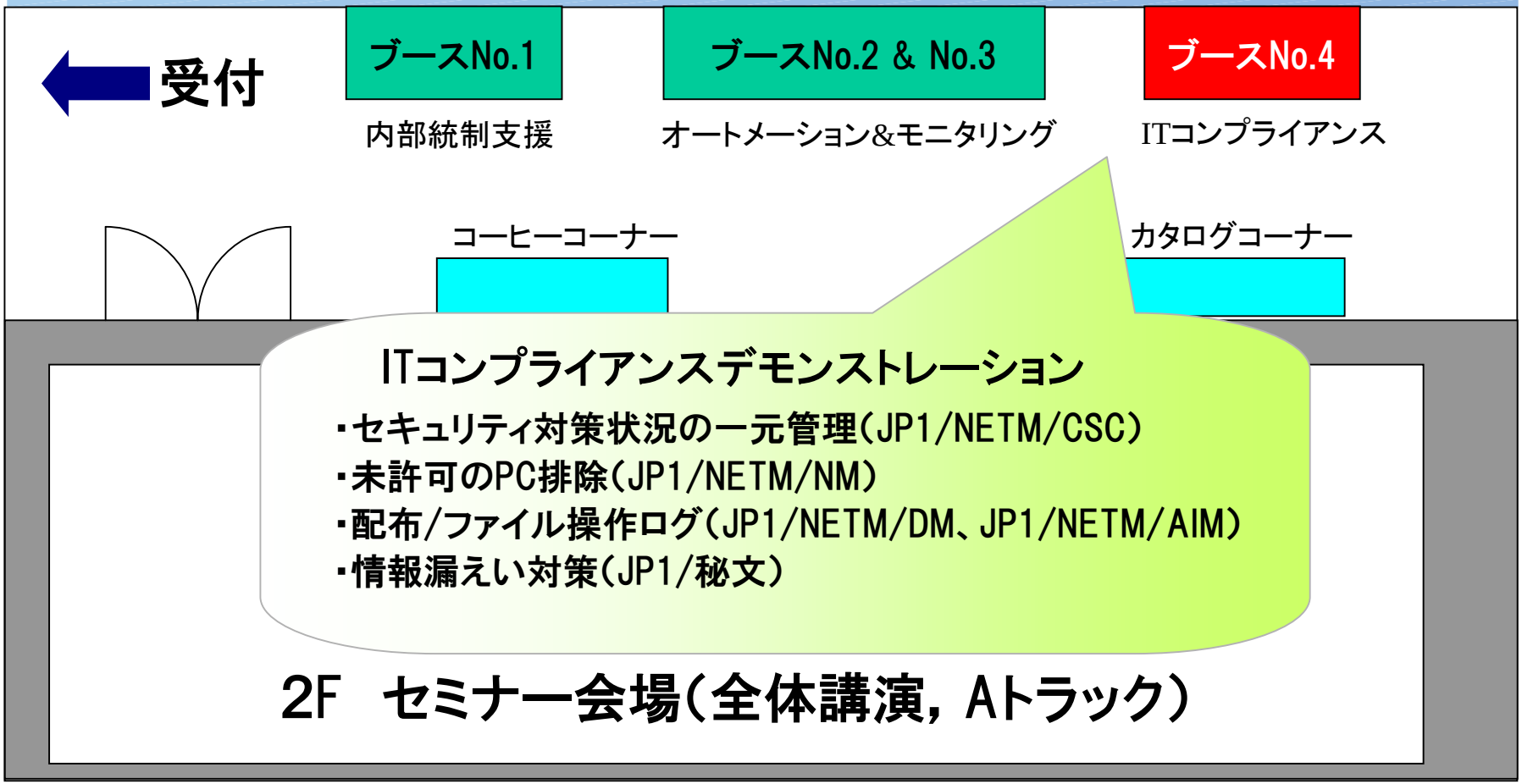


・JP1/秘文 CGP専用USBメモリ以外のメディアへのデータの持ち出しを制御。
・専用のUSBメモリ内のデータは、社外でも編集のみが可能。
・専用のUSBメモリ内のデータは暗号化され安全に持ち運びが可能。

4
デモブースのご紹介

4 デモブースの紹介

本日ご紹介したITコンプライアンスのデモンストレーションを展示コーナーにてご覧いただけます



付録　その他強化ポイント

JP1/NETM/DMのその他強化ポイント(1)

08-10

●JP1/Baseと連携することで、JP1/Baseのユーザ管理機能で管理するJP1ユーザを
JP1/NETM/DMのユーザとして使用できます。JP1ユーザは、ユーザごとに権限を設定できます。
管理者ごとに権限を設定したJP1ユーザを作成することで、特定の管理者だけが設定を
変更できるようにしたり、管理者の業務を分担したりできます。
今回、ユーザ管理機能をサポートするのは、マネージャ、中継マネージャ、パッケージャです。

ユーザ管理機能

ユーザ認証

JP1/Baseのユーザ認証機能を利用し、ログイン画面から入力されたJP1ユーザIDとパスワードでユーザ認証を行います。

ユーザ権限による操作抑止

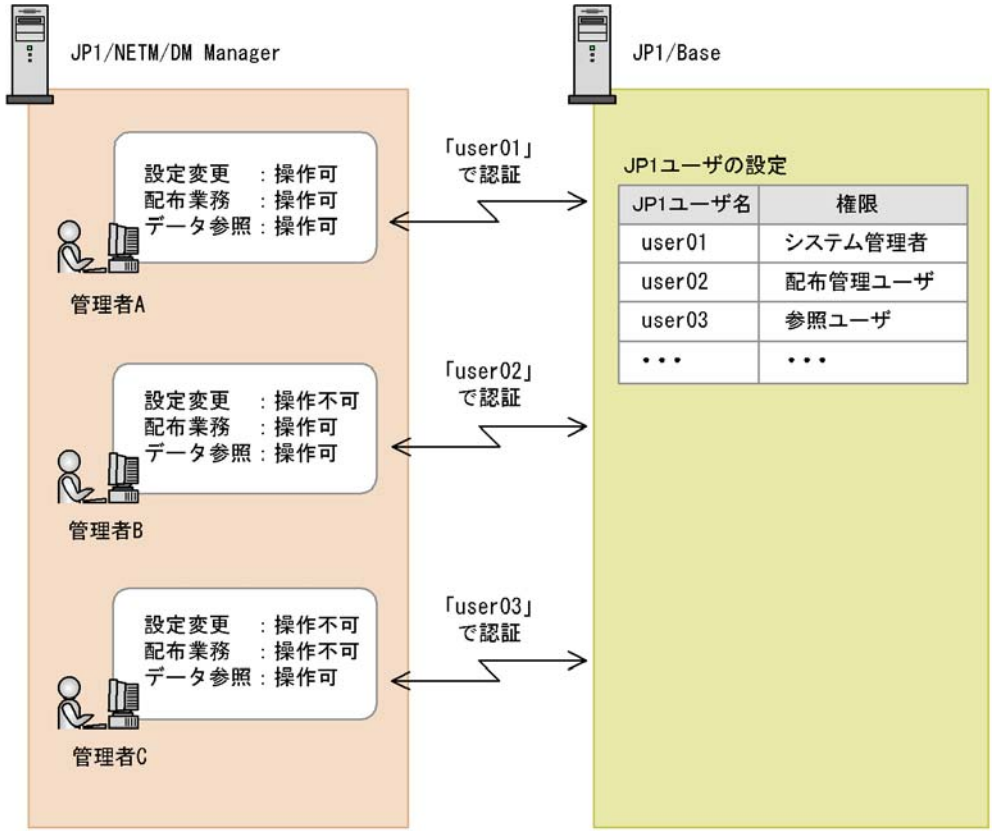
JP1/BaseのJP1権限レベルとJP1/NETM/DM固有の実行権限定義(ユーザごと)を照らし合わせて、操作権限のない機能については、非活性化や非表示などの制限を施し、権限のないユーザが操作できないようにします。

**ユーザ権限による
コマンド起動抑止**

コマンドを起動時に、ユーザ権限を確認し、権限のないユーザであった場合は、コマンドの起動を抑止します。

ユーザごとの状態保存

画面の表示状態や印刷時の設定などの状態をログインユーザごとに保存します。



ユーザ管理機能を使用するかどうかは、JP1/NETM/DM Managerのインストール時に選択します。

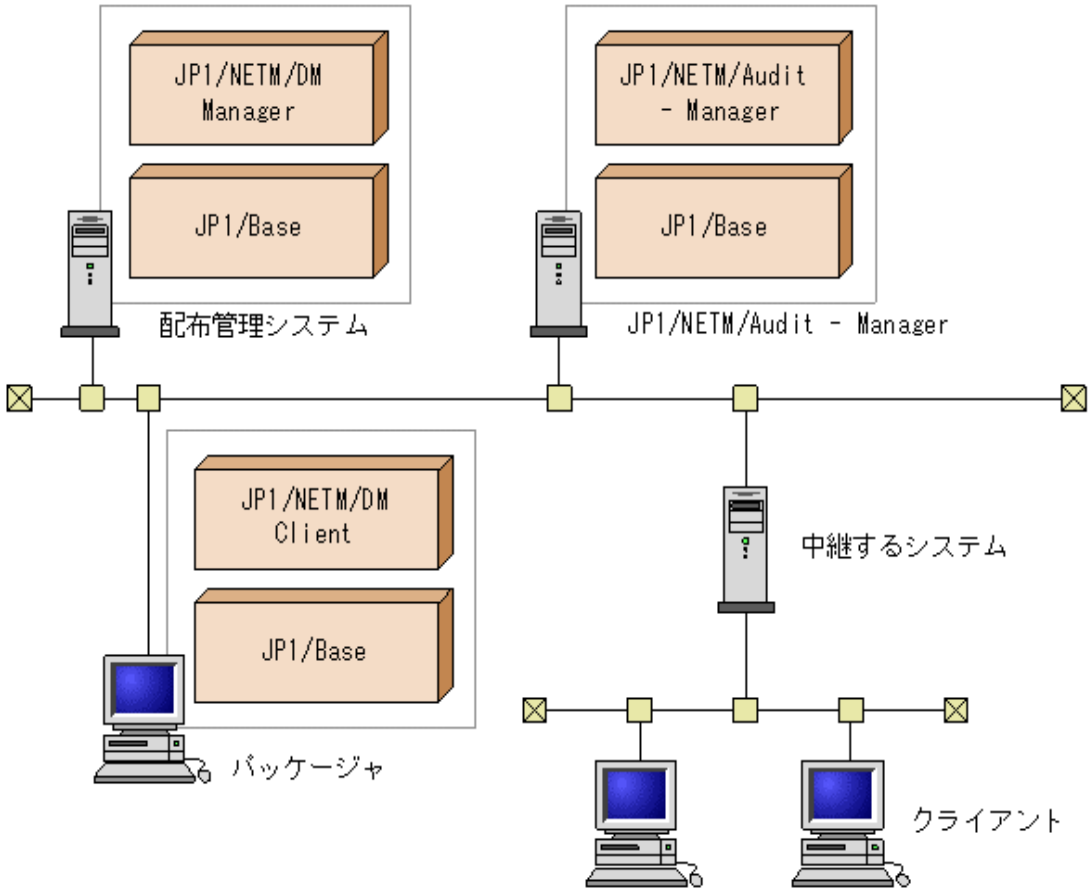
JP1/NETM/DMのその他強化ポイント(2)

●JP1/NETM/DMサーバサービス、GUI、コマンドの起動や停止、ログイン認証、GUIにおける操作(配布するパッケージの作成や配布ジョブの実行など)の、事象発生時に監査ログ(「いつ」「どこで」「誰が」「どのような権限で」「何に対して」「どうした」の証跡記録)を出力します。

08-10

JP1/NETM/DMで出力した監査ログは、JP1/Baseで収集してJP1/NETM/Audit - Managerで管理・参照できます。

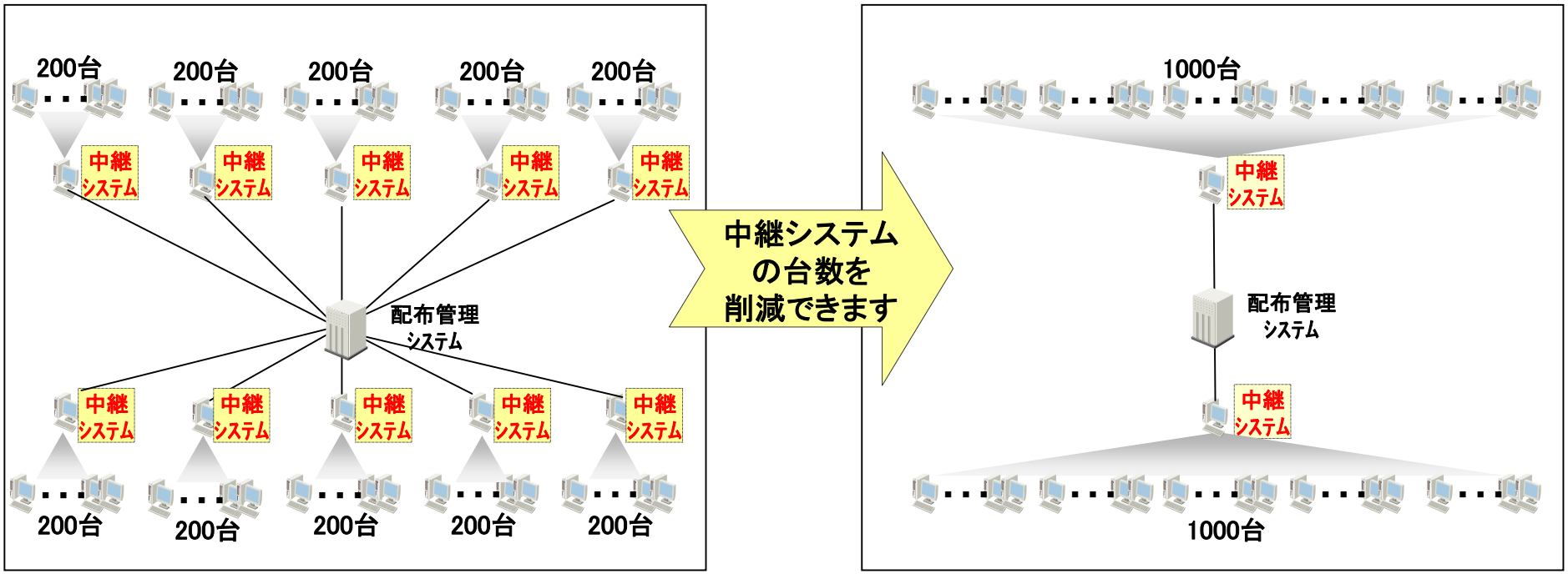
※JP1/NETM/Audit - Manager、およびJP1/Baseがない環境でも、ユーザが指定したフォルダ内のログファイルに監査ログを出力します。



JP1/NETM/Audit – Manager、およびJP1/Baseは、08-10以降が必要です。

JP1/NETM/DMのその他強化ポイント(3)

●中継システムの処理方法を見直し、クライアントが同時に接続できる台数の上限を拡大しました。 08-10
Windows：従来の推奨台数の上限を200台から、1000台(*1)に拡大しました。
(*1)中継システムでリモートインストールマネージャ(GUI)を使用しない場合に限ります。
UNIX：従来の接続数の設定値の上限を256台から、9999台に拡大しました。



JP1/NETM/DMのその他強化ポイント(4)

●新OS Windows Vistaに対応し、管理できる環境を増やします。 Win 08-10

Windows Vistaに対応した製品は従来の製品と形名が異なります。
なお、次に示す機能は、Windows Vista版JP1/NETM/DM Clientの場合は使用できません。

・中継システム機能
・暗号化されたパッケージのリモートインストール
・Visual Testで作成したレコーダファイルのリモートインストール
・ソフトウェアの稼働監視(OSのバージョンが64ビットの場合)
・ファイル操作履歴の取得
・秘文連携機能

●他社ソフトウェア配布サポート Unix Linux 08-00

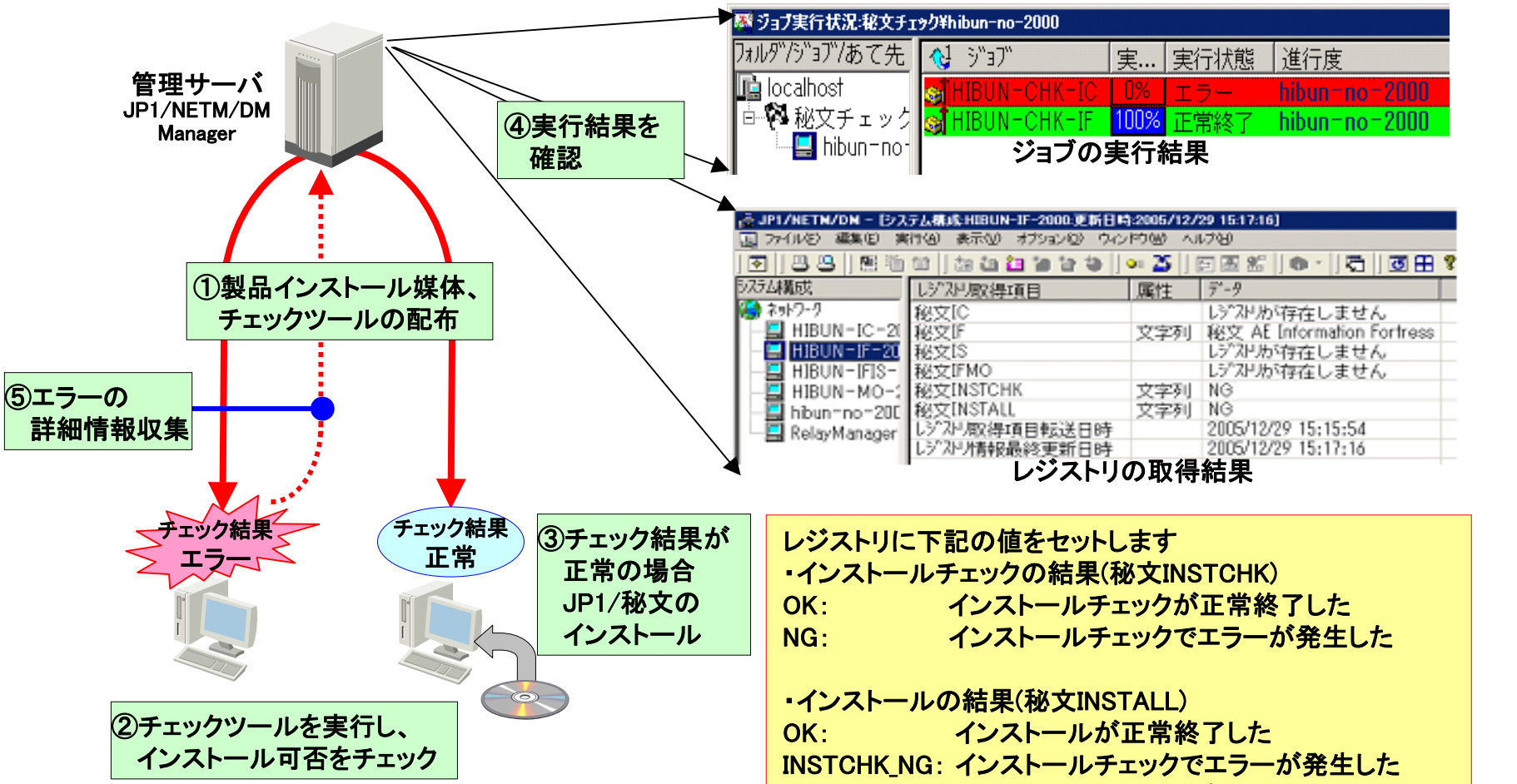
UNIXのOS標準インストーラに対応したソフトウェアを配布できるようにしました。
以下のインストールコマンドを提供している他社ソフトウェアを配布できます。

OS	HP-UX	Solaris	AIX	Linux
インストールコマンド	swinstall	pkgadd	geninstall	rpm

JP1/NETM/DMのその他強化ポイント(5)

08-00

●JP1/秘文がインストールできる環境かどうかをリモートでチェックできます。
空きディスク容量は充分か、Windowsの暗号化ファイルシステム(EFS)を使用していないか、など
JP1/秘文をインストールするために必要な条件を満たしているかをチェックできます。
インストール条件を満たしている場合、JP1/秘文をリモートでインストールすることができます。

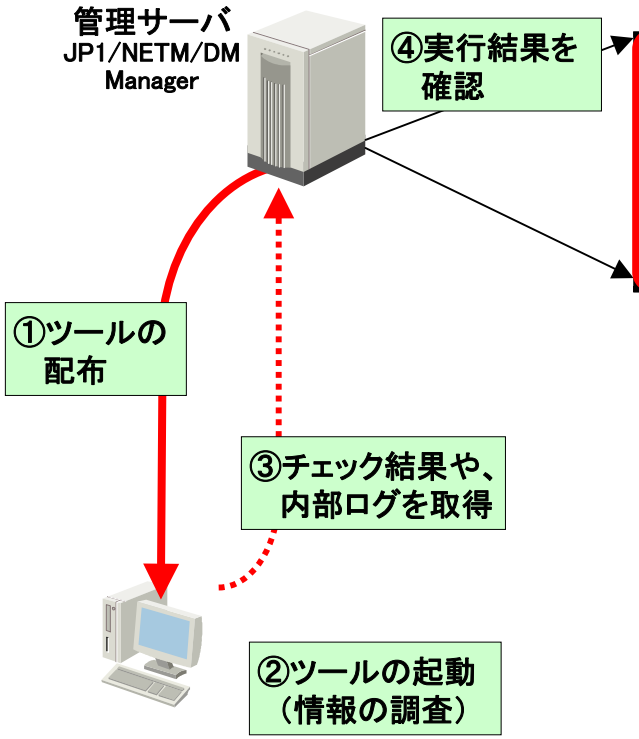


レジストリに下記の値をセットします
・インストールチェックの結果(秘文INSTCHK)
OK: インストールチェックが正常終了した
NG: インストールチェックでエラーが発生した

・インストールの結果(秘文INSTALL)
OK: インストールが正常終了した
INSTCHK_NG: インストールチェックでエラーが発生した
NG: インストールでエラーが発生した

JP1/NETM/DMのその他強化ポイント(6)

●数種類あるJP1/秘文製品の内、どの製品がインストールされているか把握することができます。 08-00
また、指定したJP1/秘文製品がインストールされていない PCをリストアップすることもできます。
JP1/秘文で不具合が生じた場合に、JP1/秘文の内部ログをリモートで取得できます。
また、リモート操作機能(*1)を利用して、対策や復旧をリモートから支援することもできます。
(*1)リモート操作機能をインストールしている場合のみ可能です



秘文IC		レジストリが存在しません
秘文IF	文字列	秘文IF JP1/秘文 AE Information Fortress 0751/A
秘文IS	文字列	秘文IS JP1/秘文 AE Information Share 0751/A
秘文IFMO		レジストリが存在しません

下記のJP1/秘文の詳細バージョンをレジストリ情報として取得出来ます
JP1/秘文 AE Information Cypher
JP1/秘文 AE Information Fortress
JP1/秘文 AE Information Fortress Mail Option
JP1/秘文 AE Information Share

JP1/NETM/CSCのその他強化ポイント(1)

●従来よりサポートしていたInternet Explorerに加え、Windows Media PlayerやOfficeなどのパッチを指定して判定できるようになりました。これにより、その製品がインストールされている資産のみを判定対象とし、判定の際の誤検知を防止します。 08-10

●ポリシー自動更新機能を拡張しました。 08-10
従来のトレンドマイクロ社のウィルス対策製品に加え、シマンテック社およびマカフィー社のウィルス対策製品についても、ポリシー自動更新機能の対象としました。

McAfee社　製品名	バージョン
McAfee VirusScan ASaP	2.8
McAfee Managed VirusScan	3.0
McAfee Managed VirusScan plus AntiSpyware	3.5
McAfee Managed Total Protection	4.0
McAfee VirusScan Enterprise	7.1 8.0i 8.5i

Symantec社　製品名	バージョン
Norton AntiVirus	2004 2004 Professional 2005 2006 2007
Symantec AntiVirus Corporate Edition	9.0 10.0 10.1
Symantec Client Security	2.0 3.0 3.1

●不正ソフトウェアの検索方法を改善しました。 08-10
従来はソフトウェア名は「部分一致」のみでしたが、「完全一致」「部分一致」「前方一致」「後方一致」から選択できるようにしました。

●判定対象のOSを追加しました。 08-10
Windows Vistaを判定対象OSとして追加しました。

JP1/NETM/CSCのその他強化ポイント(2)

●対応するウィルス対策製品を追加しました。 08-10
JP1/NETM/DM 08-10でサポートするウィルス対策製品の情報をデフォルトの判定ポリシーに追加しました。

●JP1/NETM/DM Clientで収集したインベントリ情報を使用した判定が可能 となります。 08-00
例えばレジストリ情報を参照し、自動ログオンの有無などを判定項目とすることが可能です。

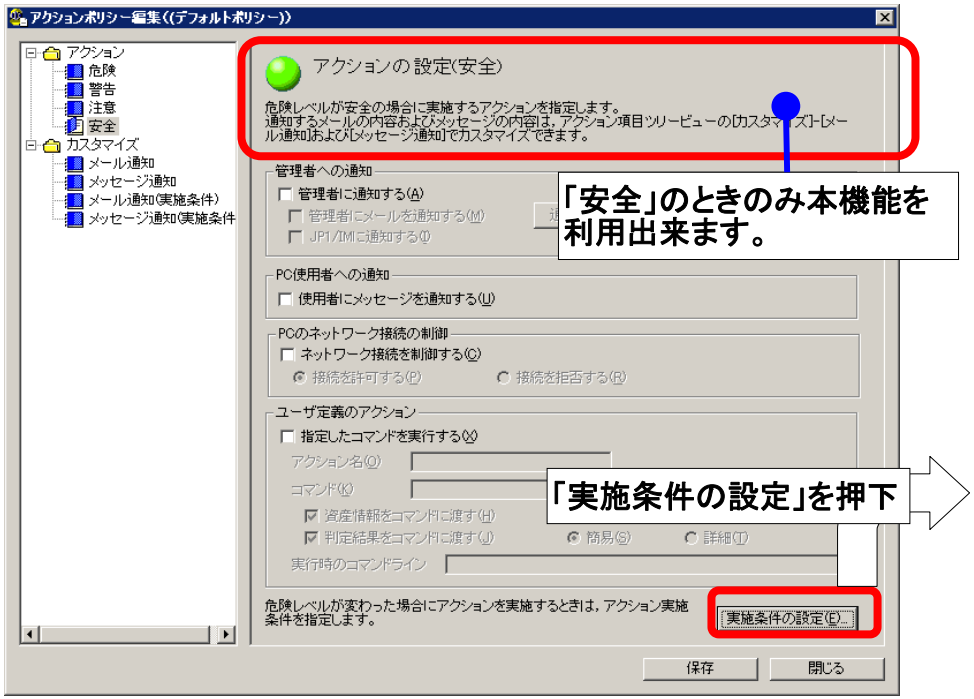
●危険レベル判定後のアクションにユーザが指定した実行ファイル(bat、exe)を 08-00
実行することが可能です。本機能により、ユーザ独自のアクション(他のシステムとの連携等)を行うことが可能となります。

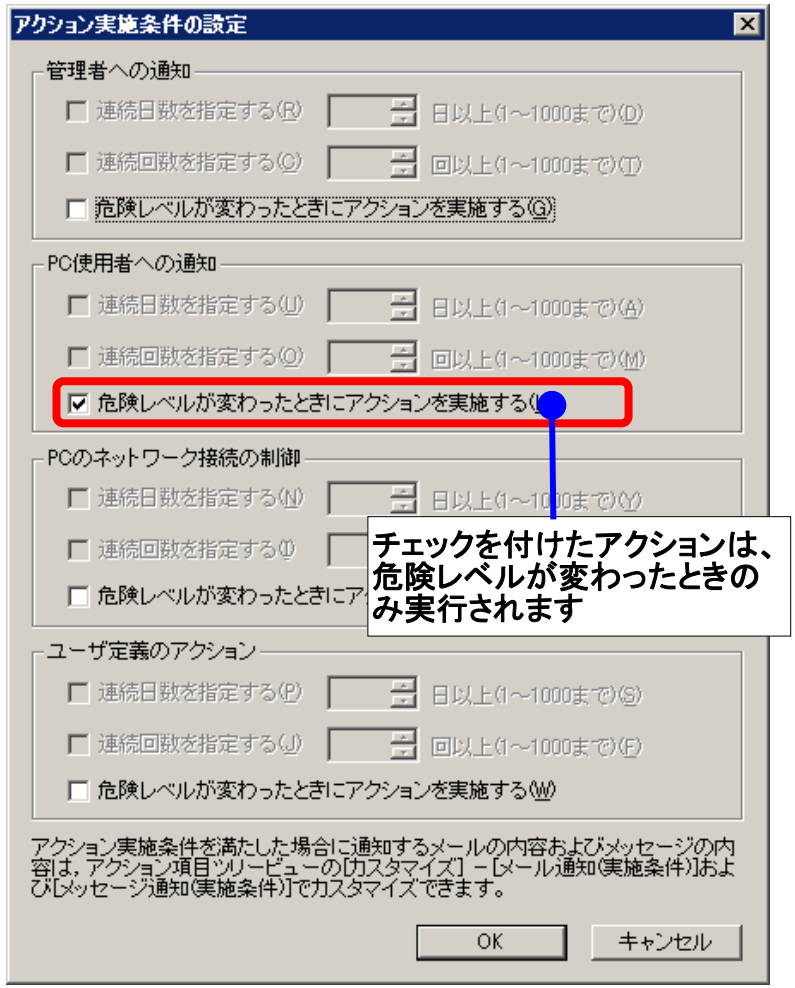
●ネットワーク制御コマンドをサポートしました。これによりネットワークへの接続許可または 08-00
接続拒否を行うことができます。
本機能を利用する事で、例えばウィルス対策製品などの外部システムと連携し、
ウィルス感染したPCをネットワークから切り離すことが可能となります。

JP1/NETM/CSCのその他強化ポイント(3)

08-00

●危険レベルが変更(「注意」「警告」「危険」⇒「安全」)のときのみアクションを実行するように設定することが可能です。
本機能を利用する事で常に安全なクライアントPCに対し、メッセージ通知等の余計なアクションを行わなくなり、サーバへの負荷が低減します。



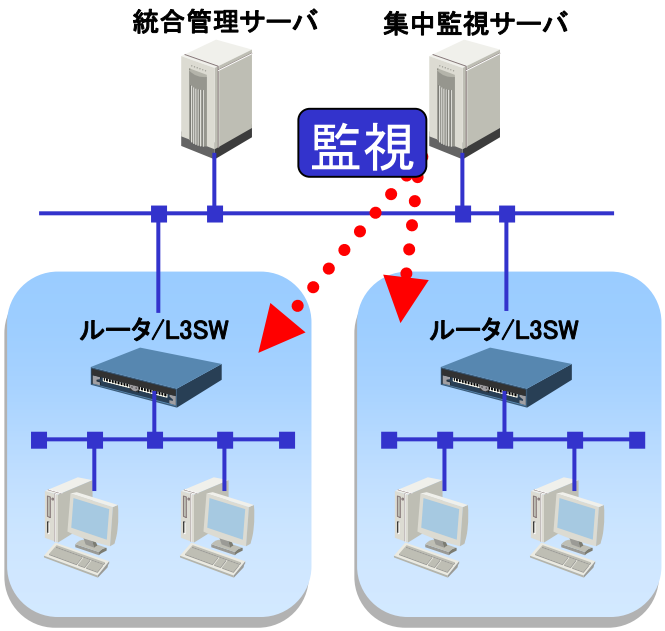


	1回目の判定	判定に対するアクション	2回目の判定	判定に対するアクション
危険レベル変更あり	警告	「警告」に対するアクション実施	安全	「安全」に対するアクション実施
危険レベル変更なし	安全	「安全」に対するアクション実施	安全	アクション実施しない

JP1/NETM/NMのその他強化ポイント(1)

08-10

●複数のセグメントを1台のサーバで集中監視することが可能です。(排除は行えません。)
これにより、不正PCの監視のみ行いたいセグメントに対しては監視サーバ(JP1/NETM/NM)を導入する必要がなくなり、導入が容易となります。強制排除が必要なセグメントのみ監視サーバを順次配置していくことで、導入コストを低減することができます。



集中監視機能はJP1/NETM/NM – Managerのコンポーネントの一つですが、別サーバへのインストールが可能です。集中監視機能をインストールするためのモジュールは、JP1/NETM/NM – Managerに同梱されています。

JP1/NETM/NMとの機能差異

集中監視機能ではJP1/NETM/NMで使用できる以下の機能が使用できません。

- 不正PC排除機能
- 検疫支援機能
- JP1/NETM/DM連携による許可機器一覧の配布機能

前提環境

<OS>
Windows XP Professional
Windows Server 2003, Standard Edition (R2含む)
Windows Server 2003, Enterprise Edition (R2含む)
<ソフトウェア>
Internet Explorer 6.0以降
IIS 5.xまたはIIS 6.0

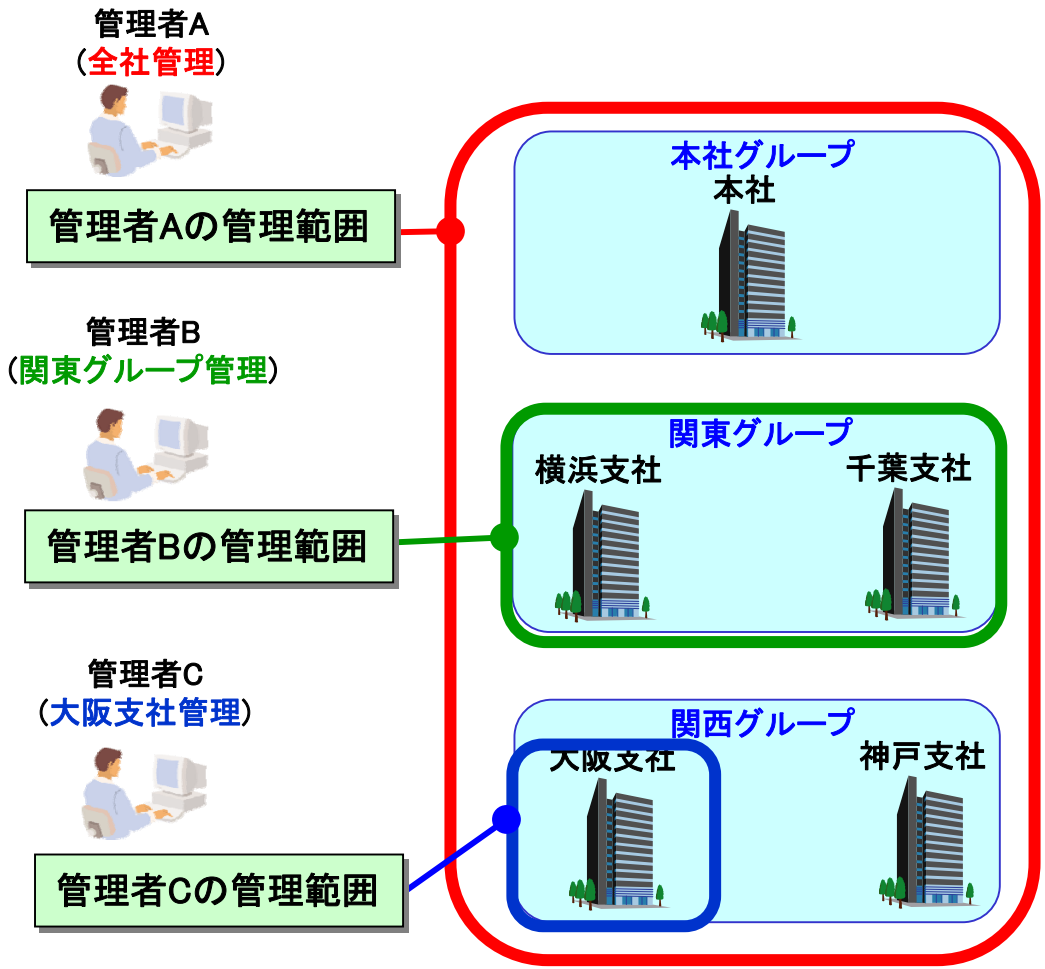
注意事項

- 1台の集中監視サーバは100ネットワーク、3000クライアントを監視対象の目安としてください。
- ネットワーク監視の範囲はICMPのPingが届く範囲となります。

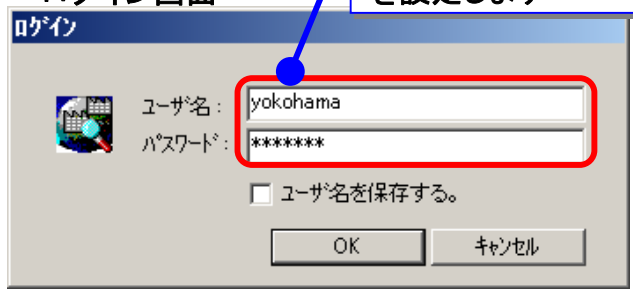
JP1/NETM/NMのその他強化ポイント(2)

08-10

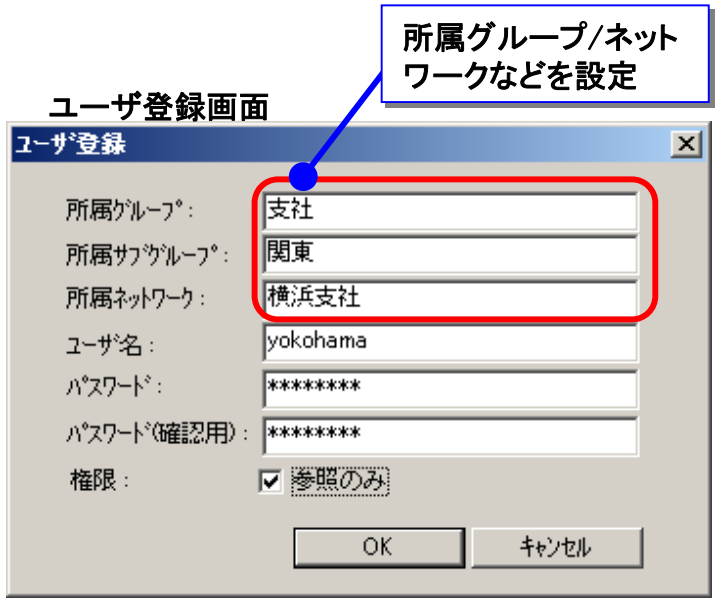
●ログインユーザごとに操作できる範囲を限定することができます。
また、参照のみのユーザを作成することが可能です。
これにより、管理者が複数いる場合でも責任分担して運用することが可能となります。



ログイン画面



ユーザ登録画面



JP1/NETM/NMのその他強化ポイント(3)

●JP1/NETM/NMで検知したイベントをJP1イベントとしてJP1/IMに通知できるようになりました。
これにより、管理者は他の製品とともにJP1/IM統合コンソールでイベントを集中監視できるようになります。また、イベントをメール通知できるようになりました。 08-10

●ネットワークの登録および機器一覧の登録をCSVファイルだけでなく、GUIから登録できるようにしました。 08-10

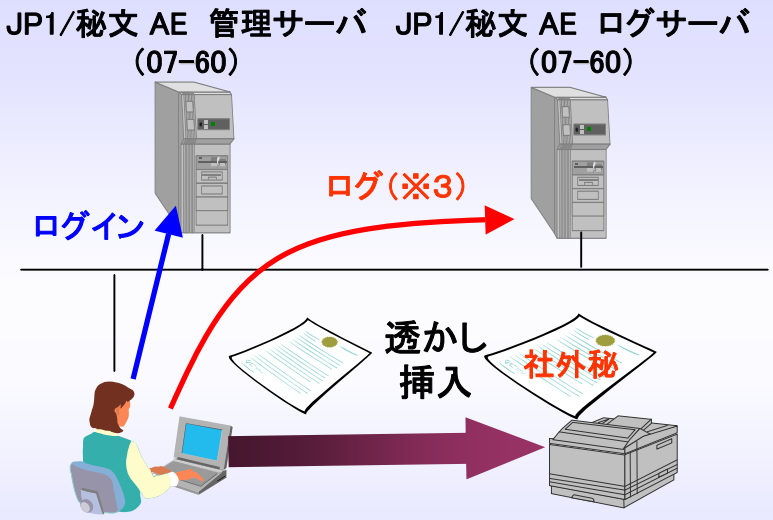
●コンピュータ名の変更を検出できるようにしました。
PCのコンピュータ名が変更された際に、ログおよびトラップを出力することができます。 08-10

●対象外機器を排除できるようにしました。
監視対象外のネットワークに属するPCをネットワークから排除することができます。 08-10

JP1/秘文のその他強化ポイント(1)

●秘文ユーザ透かし印刷(JP1/秘文WP) 07-70
従来は透かし定義情報の設定項目の文字構成に秘文ユーザ(JP1/秘文管理サーバにログインしているJP1/秘文IF ユーザ名)が設定できませんでしたが、今回のエンハンスで設定できるようにしました。これにより、JP1/秘文 IF ログインユーザも透かし印刷できるようになります。

●JP1/秘文 AE IFと連携し、印刷物に透かし情報(※1)を埋め込みます。(JP1/秘文WP) 07-60
業務上印刷を禁止できない場合でも、透かし情報を挿入することで、印刷物からの情報漏えいへの注意喚起や、印刷物の放置防止効果が見込めます。



設定可能な透かし情報(※2)	
日時	YYYY-MM-DD hh:mm:ss
ユーザID	Windowsにログインしているユーザー-ID
ユーザ名	ActiveDirectoryに登録されている姓名
PC名	印刷を実行したPCのNetBios名
IPアドレス	印刷を実行したPCのIPアドレス
固定文字列	「社外秘」など任意の文字列

※1:透かし情報とは、文書の背景に重ね合わせて印刷する、あらかじめ定義しておいた文字列などの情報のことです。
※2:サイズ、位置、パターン等は任意に設定できます。
※3:透かし情報を挿入して印刷した場合、ログにWATERMARK ADDEDと出力されます。

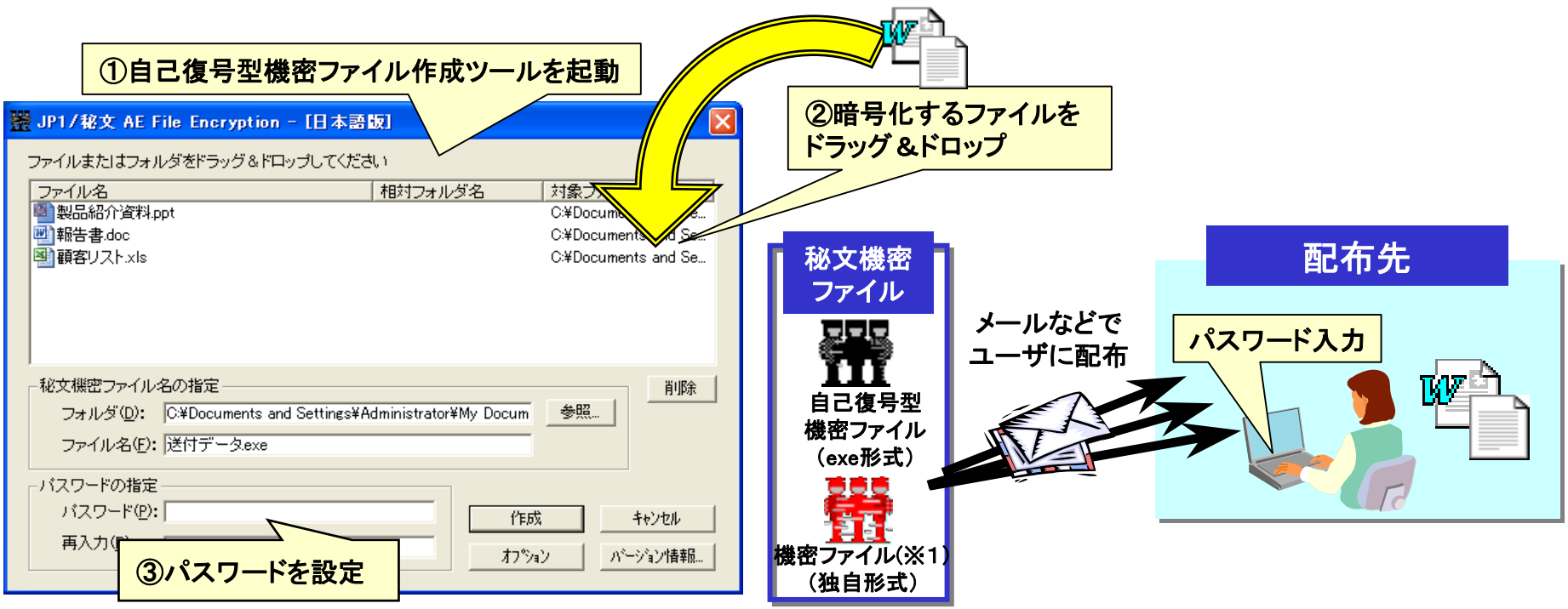
JP1/秘文のその他強化ポイント(2)

●Citrix Presentation Serverやターミナルサービスでの使用サポート（JP1/秘文FE）
クライアントOSだけでなく、Windows Server 2003上で動作する、Citrix Presentation Serverやターミナルサービスでも JP1/秘文FEを利用できます。

07-52

●ファイルを自己復号形式の暗号ファイルにする機能を提供します。（JP1/秘文FE）
メール添付ファイルなど配布データの暗号化に最適です。暗号化されたファイルは、JP1/秘文の無い環境でもパスワードの入力で復号化できます。

07-52

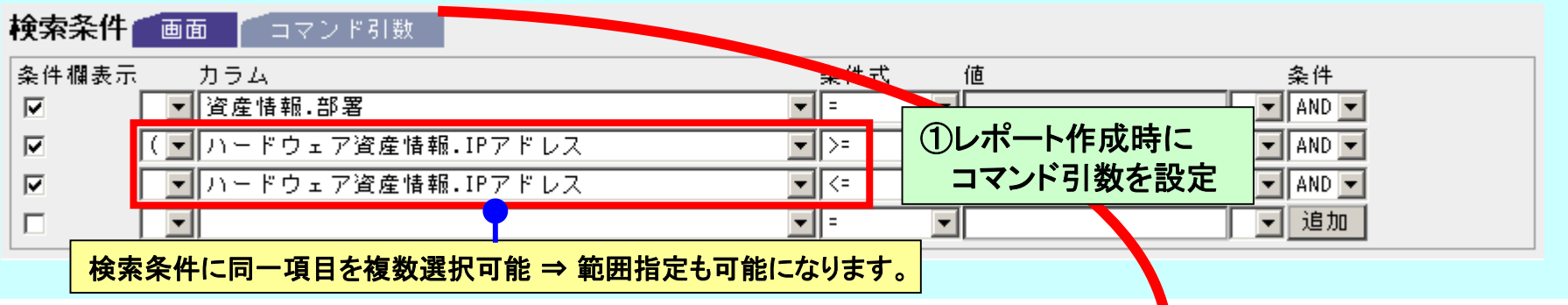


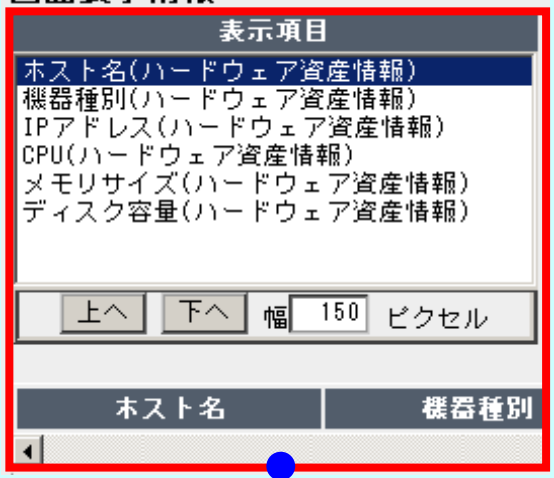
※1：機密ファイルは復号プログラムを含みません。機密ファイルを復号する端末にも、JP1/秘文 AE FE およびJP1/秘文 07-52以降が必要になります。その他環境へ秘文機密ファイルを送付する場合は、自己復号型機密ファイルを使用してください。

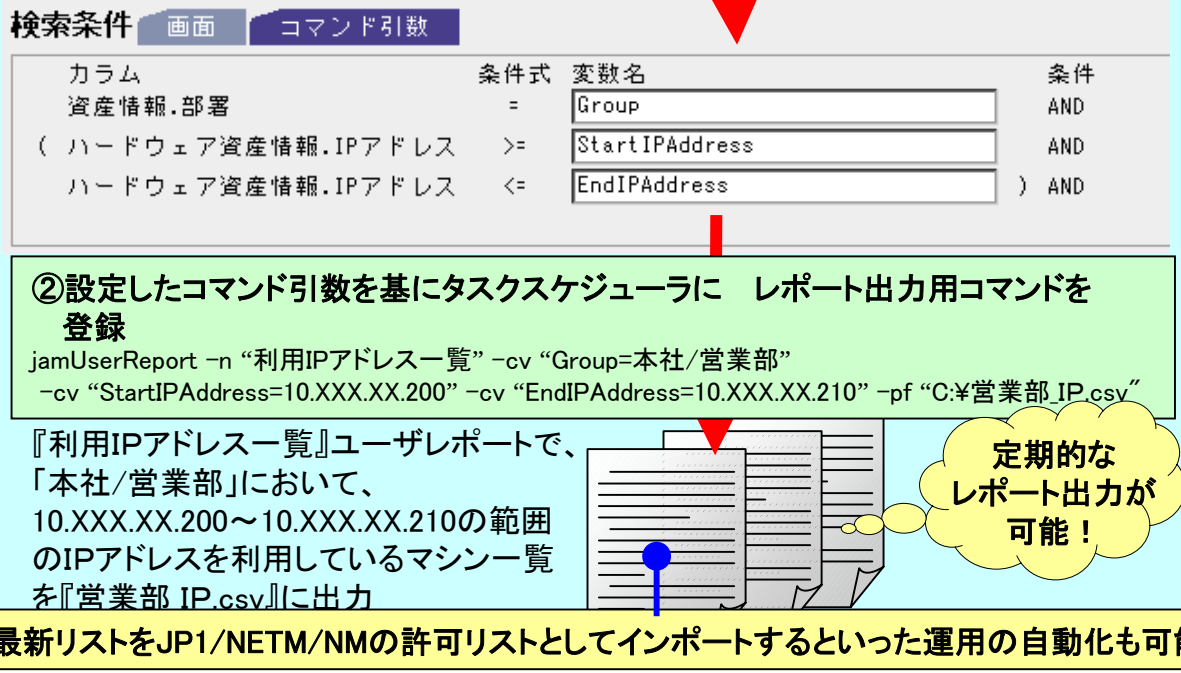
JP1/NETM/AIMのその他強化ポイント(1)

●ユーザレポート機能において、同一項目条件の複数指定と検索結果項目の表示幅の変更ができるようになりました。さらに、指定した条件による検索結果を定期的に出力するためのCSV出力コマンドをサポートしました。これにより、より柔軟で効率的なレポート作成が可能となります。

08-10







JP1/NETM/AIMのその他強化ポイント(2)

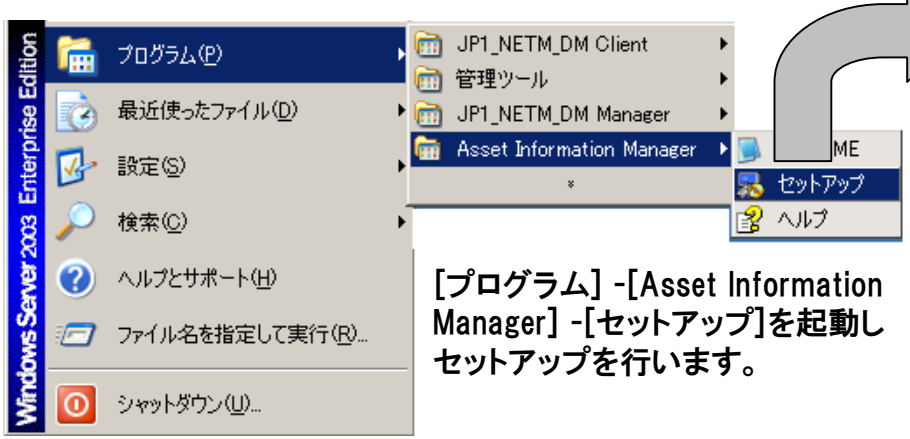
●これまでコマンドを起動して行わなければならなかった設定を「セットアップ」ダイアログから行えるようにしました。JP1/NETM/AIMの初期導入およびメンテナンスが容易に行えるようになります。 08-02

セットアップから使える機能一覧

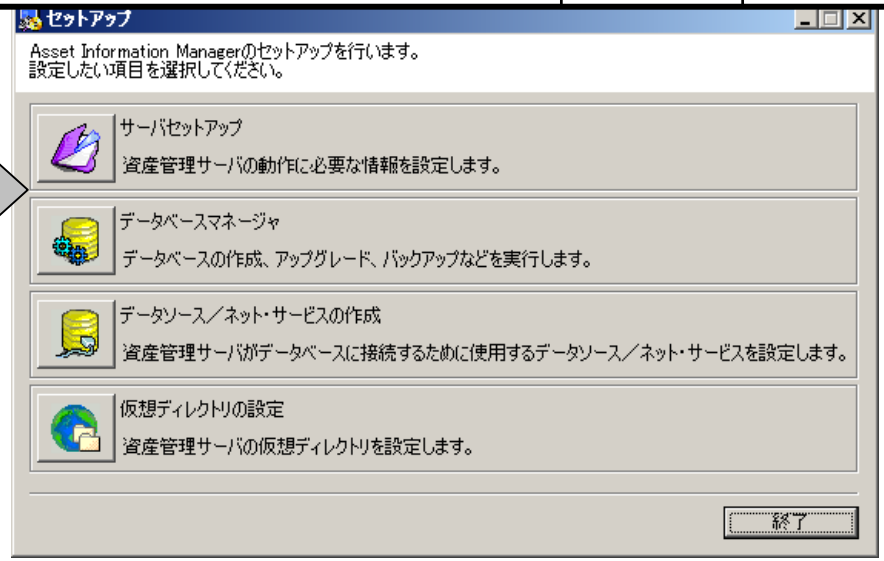
新規手順は新規に環境構築を行う場合に行う順番
更新手順はリビジョンアップ、バージョンアップを行う順番

メニュー	機能概要	新規手順	更新手順
仮想ディレクトリの設定	JP1/NETM/AIMで使用する仮想ディレクトリの設定を行う	1	
サーバセットアップ	JP1/NETM/AIMの動作に必要な設定を行う	2	
データベースマネージャ	JP1/NETM/AIMで使用するデータベースの作成、アップグレード、バックアップ、リストアなどを行う	3	1
データソース／ネット・サービスの作成	JP1/NETM/AIMがデータベースに接続するために必要なODBCの設定を行う	(4)	

手順(4)は他製品連携を行う場合に必要な手順です。



[プログラム] -[Asset Information Manager] -[セットアップ]を起動しセットアップを行います。



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
■AIXは、米国における米国International Business Machines Corp.の登録商標です。
■HP-UXは、米国Hewlett-Packard Companyのオペレーティングシステムの名称です。
■Linuxは、Linus Torvaldsの米国およびその他の国における登録商標あるいは商標です。
■Microsoft Internet Explorerは、米国Microsoft Corp.の商品名称です。
■Microsoft Officeは、米国Microsoft Corp.の商品名称です。
■Microsoft SQL Serverは、米国Microsoft Corp.の商品名称です。
■McAfeeは、米国法人Network Associates,Inc. またはその関係会社の米国またはその他の国における商標です。
■ORACLEは、米国Oracle Corporation の登録商標です。
■Symantec AntiVirus Scan Engineは、Symantec Corporation の商標です。
■Solarisは、米国及びその他の国におけるSun Microsystems,Inc.の商標又は登録商標です。
■UNIXは、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。
■ウイルスバスターは、トレンドマイクロ株式会社 の登録商標です。
■秘文は、日立ソフトウェアエンジニアリング(株)の登録商標です。
■Citrix Presentation Serverは、米国あるいはその他の国におけるCitrix System,Incの登録商標です。

その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

HITACHI
Inspire the Next

✧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。