■JP1 Version 8のカタログ一覧

詳細は各製品のカタログをご参照ください。

JP1は、日立グループの「環境情報表示制度」に基づき環境配慮を評価し、スーパー環境適合製品として登録した製品です。本製品をご利用いただくことで、導入前に比べCO2を約50%削減できます(弊社モデルケースの場合)。詳しい環境情報は、当社のホームページで、ご覧いただけます。
http://greenweb.hitachi.co.jp/

●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。
●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うえ、必要な手続きをお取りください。
なお、ご不明な場合は、弊社営業担当員にお問い合わせください。

製品に関する詳細・お問い合わせは下記へ

■ 製品情報サイト
http://www.hitachi.co.jp/jp1/

■ インターネットでのお問い合わせは
http://www.hitachi.co.jp/soft/ask/

■ 電話でのお問い合わせは**HMCC**(日立オープンミドルウェア 問い合わせセンター)へ
0120-55-0504 利用時間 9:00～12:00、13:00～17:00 (土・日・祝日・弊社休日を除く)

株式会社 日立製作所 情報・通信グループ ソフトウェア事業部

CA-553U | 2008.3
Printed in Japan(H)

統合システム運用管理 JP1 Version 8
資産・配布管理/セキュリティ管理

JTCompliance V8.5

HITACHI
Inspire the Next

JP1 Version 8

uVALUE with Harmonious Computing

JP1 Version 8 ITCompliance

資産・配布管理/セキュリティ管理

IT環境を統制し、ビジネスの透明性を確保する。

違法行為やミス・不正・エラーから企業を確実に守るために、企業内部の統制を強化することが求められています。そのためには、企業情報システムを統制することが不可欠であり、各種法令や規則に基づいた資産情報の的確な管理や速やかな対応策が必要です。

JP1のITコンプライアンスは、資産情報を一元管理することで、企業情報システムを構成するコンピュータシステムの健全かつ有効な環境を提供し続けます。さらに、脆弱なクライアントPCの強制排除や情報漏えい対策など、さまざまなセキュリティリスクへの予防対策を講じることができます。

企業リスクを回避し、ビジネスの透明性を確保するIT環境統制 ――

すべてはお客さまの継続的な発展のために。

内部統制強化に向けたさまざまなニーズに多彩な機能で応えます。

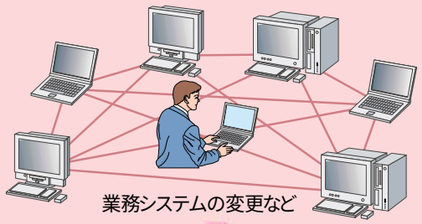
Service Quality Management

大切なIT資産を「守る」――
それが、JP1のITコンプライアンス。

**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。**

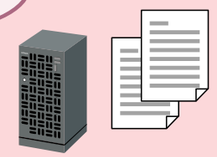
JP1のITコンプライアンスは、企業内システム環境の的確な把握と、不正アクセスやウイルス感染といった脅威やリスクからの保護を実現します。企業や組織で定められた統制基準を満たし、「正しく運用させるための仕組み」をPDCAサイクルに沿って支援。さらに、「正しく運用されていること」を証明するために必要な証跡記録を収集。
企業の内部統制の根幹となる運用基盤を整備することで、ビジネスの健全性・信頼性が高まります。

正しく運用されていることの証明

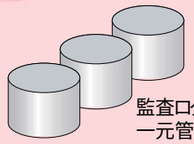


証跡記録の収集

「いつ」「誰が」
「どのような権限で」
「どこから」「何をした」



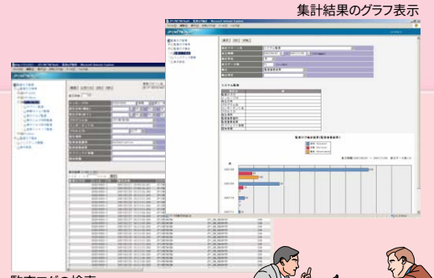
蓄積



監査ログの
一元管理

長期保存

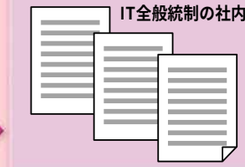
集計結果のグラフ表示



監査ログの検索

監査目的に応じて抽出

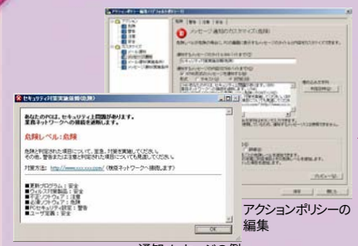
正しく運用させるための仕組み



Plan

●IT全般統制の社内基準設定

セキュリティの脅威やリスクを洗い出し防御対策を決定（各種ポリシーの設定）
- 配布条件の設定
- セキュリティポリシーの設定
- 持ち出し制御条件の設定
- 稼働監視ポリシーの設定　など



アクションポリシーの編集

通知メッセージの例

各種資産情報の参照

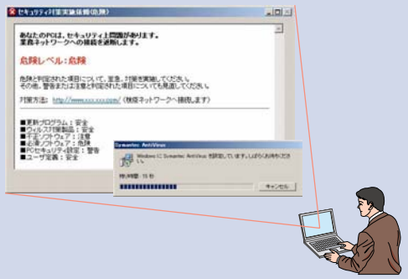
インベントリ情報

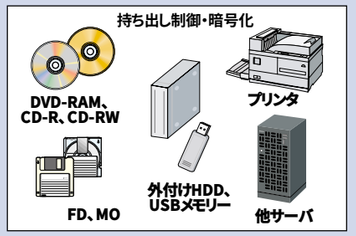
ウイルス対策製品情報

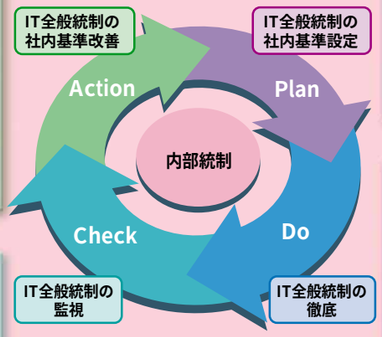
Do

●IT全般統制の徹底

さまざまな脅威やリスクに対する防御対策を実施
- 脆弱なPCへのパッチ/ソフトウェア配布
- 不正接続PCの検出/排除
- 媒体や印刷物の持ち出し制御
- セキュリティ対策が不十分なPCの接続拒否
- 未許可ソフトウェアの起動抑止
- システム変更情報や障害情報の取得　など







Action

●IT全般統制の社内基準改善

セキュリティ対策状況やIT資産の利用状況から各種ポリシーを改善
- セキュリティポリシーの見直し
- 利用制限ポリシーの見直し
- 購入ライセンスの適正化　など

ライセンス数の見直し

パスワード判定の定義

判定ポリシーの編集

Check

●IT全般統制の監視

健全なシステム環境が維持されているかを監視
- セキュリティレベルの把握（点数評価）
- 各ソフトウェアの稼働状況を把握
- ファイル操作の追跡
- 操作ログの集計　など

セキュリティレベルの点数評価

操作ログ一覧

ファイル操作の追跡

ITコンプライアンスを支える管理製品

■ 資産・配布管理

ハードウェアやソフトウェアなどのIT資産を一元管理。さらに、検疫システムの構築、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。

■システムの現状把握と是正手段の提供により、IT統制の徹底を図る　ソフトウェア配布・資産管理

「JP1/NETM/DM」

クライアントPCのハードウェア情報、ソフトウェア情報や、PCの利用状況などは、IT資産管理だけではなく、セキュリティ対策を講じる上でも必要不可欠な情報です。ソフトウェア配布・資産管理は、クライアントPCの情報をサーバ側で一元管理し、セキュリティレベルの向上につながる施策も実現できます。

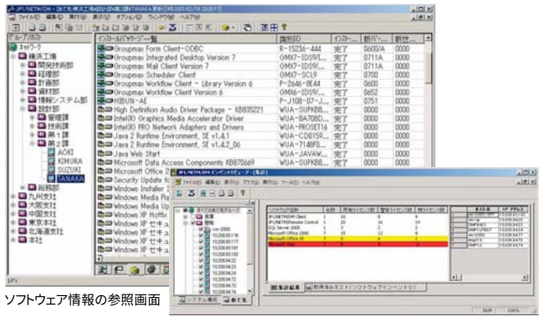
IT資産の現状を把握し、セキュリティ対策を徹底したい。

●クライアントPCの各種情報（インベントリ情報）を把握

クライアントPCのハードウェア使用状況やインストールされているソフトウェアの種類などを「インベントリ情報」として取得し、一元管理できます。ソフトウェアの新規インストールやパッチの適用などによりインベントリ情報が更新されると、一元管理された情報に更新内容が自動的に反映されます。なお、ネットワークに接続されていないPCであっても、媒体を利用して管理できます。

＜取得できるインベントリ情報＞＊

・ハードウェア情報（ハードディスク空き容量、実装メモリー容量など）
・ソフトウェア情報



ソフトウェア情報の参照画面

ライセンス情報集計画面

・セキュリティ関連情報

セキュリティレベルの維持・向上を図るために欠かせない、次のような情報です。

＜取得できる情報＞
・詳細バージョン（Windows®/UNIX、Microsoft® Internet Explorer、Microsoft® Office）
・パッチの適用/未適用情報
・ウイルス対策製品（エンジンや定義ファイルのバージョン、常駐/非常駐）
・パスワード（脆弱性、更新からの経過日数など）
・スクリーンセーバー（設定有無、パスワードの有無など）
・Windows® の設定（自動ログオンの設定有無、自動更新の有効/無効など）
・意図しない設定/不適切な設定の有無（共有フォルダ、Guestアカウントなど）

・ユーザー固有情報

必要に応じて、ユーザーが任意に設定できる情報です。Microsoft社のActive Directoryで管理している情報を取り込むこともできます。

＜登録例＞
・PC利用者の氏名　・所属　・電話番号　・社員番号　・メールアドレス　など

＊ **これらのインベントリ情報は、「クライアントセキュリティ管理」の判定ポリシーとして利用できます。**

●インベントリ情報の集計

ハードウェア情報、ソフトウェア情報、セキュリティ関連情報、ユーザー固有情報を組み合わせてレポーティング（集計・印刷）できます。

●クライアントPCの探索

ネットワークに存在するクライアントPCを探索し、[JP1/NETM/DM]がインストールされていないPCを検出できます。

●管理対象クライアントPCの自動メンテナンス

[JP1/NETM/DM]をインストールしておけば、新規に追加されたクライアントPCであっても、管理対象端末として自動的に登録されます。また、一定期間にネットワーク接続がなく、存在を確認できなかった端末は管理対象から自動的に除外できます。「管理対象から除外された端末」は、セキュリティ対策が長期間実施できていない状態にあるので、これらを安易に業務システムに接続させないなどの運用を行うことで、システムの健全性を確保できます。さらに、[クライアントセキュリティ管理:JP1/NETM/Client Security Control]と連携すれば、このような運用を自動化できます。

●ソフトウェア起動／印刷操作／外部メディア操作の抑止

企業内で使用禁止としている通信ソフトウェアやゲームなどのインストール状況をチェックし、起動を抑止できます。同様に、印刷や外部メディアの操作も抑止できます。また、これらの操作を抑止した場合「抑止履歴」をサーバ側に通知、そのクライアントPCをコンソールで確認・特定できます。また、ソフトウェアについては業務で利用するアプリケーションなどを許可ソフトウェアとして設定することで、設定されていないソフトウェアの動作を制限できます。これにより、未知のソフトウェアなどの起動も抑止できます。

●ユーザー操作履歴の管理

ユーザーのPC利用状況や操作状況を把握でき、監視の事実を告知したり、禁止操作について利用者に警告することで、不正な操作や行動を抑止できます。情報漏えいなどの問題が発生した場合には、原因を特定するために、ユーザーPCの操作履歴を利用できます。

操作履歴の設定画面

＜管理できる操作履歴＞
・プロセスの起動
・プロセスの停止
・キャプションの変更
・アクティブウィンドウの変更
・マシンの起動/停止
・ログオン/ログオフ
・ファイル操作
・印刷操作
・外部メディア接続／切断
・Webアクセス

●ソフトウェア稼働状況の管理

ソフトウェアの稼働時間、利用台数、機器ごとの利用率を把握できます。

クライアントＰＣでの各種操作を記録/追跡したい。

●各種操作ログの取得

[JP1/NETM/DM]や[情報漏えい防止:JP1/秘文]から、ユーザー操作に関する、次のようなログを取得できます。

＜ファイル操作ログ＞
ファイルの作成／オープン／削除／コピー／名前変更／移動の操作をログに取得できます。さらに、[情報漏えい防止:JP1/秘文]からは、CDライティング、組織外持ち出し、平文持ち出し、機密ファイル作成、透かし印刷などの操作をログに取得できます。

＜印刷ログ＞
クライアントPCで実行された印刷の操作をログに取得できます。印刷が抑止されている状況では、印刷しようとして抑止された場合や、抑止を解除して印刷が実行された場合も、履歴をサーバ側に通知、そのような操作を行ったクライアントPCをコンソールで確認、特定できます。

＜外部メディア操作ログ＞
クライアントPCへの外部メディア接続／切断状況をログに取得できます。

＜Webアクセスログ＞
Microsoft® Internet ExplorerでのWebアクセスをログに取得できます。

含まれる情報はログの種類によって異なりますが、主に次のような情報で構成されています。

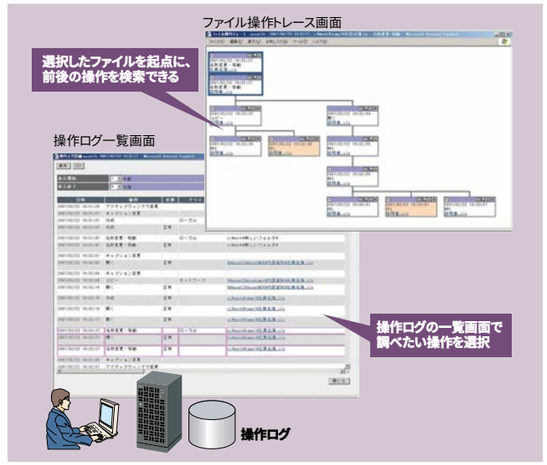
＜ログの構成要素例＞
・ユーザー名　・ファイル名　・時刻
・パス（フルパス名、ネットワークパス名）
・ドライブ種別（ローカルディスク、ネットワークドライブ、リムーバブルメディアなど）
・ドキュメント名　・使用プリンタ名　・抑止結果
・接続／切断ドライブ名
・Webアクセス先のタイトル　・URL

●操作ログの検索

取得したログは、ユーザー名、ファイル名、時刻、パスなど、ログに含まれる各種情報をキーにして検索できます。また、代表的な検索・集計パターンはテンプレートとして提供しています。テンプレートはそのまま利用するほかに、カスタマイズも可能です。

●ファイル操作の追跡

指定したファイルについて、「どこからコピー/移動したか」「どこへコピー/移動したか」をGUIで追跡できます。万一の情報漏えいの際に原因となった操作を突き止めたり、定期的な監視をすることで不正操作の抑止効果を狙えます。



●ファイル操作ログの集計

指定した条件で、操作ログをPC単位や部署単位に集計できます。不正コピーや不正ソフトウェア起動など、チェックしたい操作の発生数について、その推移を把握できます。

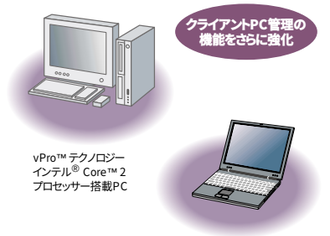
ＪＰ１におけるインテル® vPro™ テクノロジー対応（ＡＭＴ連携）

セキュアな環境の実現と、企業コストのさらなる削減を支援する技術「インテル® vPro™テクノロジー」。その技術の1つに、電源やOSの状態に依存しないで使用できる管理機能をハードウェア側から提供する「AMT（Active Management Technology）」があります。JP1は、業界でもいち早く、この「AMT」と連携しました。この技術を搭載したPCを用いた場合、JP1のAMT連携機能により、JP1「ITコンプライアンス」カテゴリの製品をさらに幅広く、効果的に使用できるようになります。

＜例＞
・JP1/NETM/DM未導入のマシンを検出する際、電源OFF中のPCも対象にできる
・電源OFFや休止状態のPCに対してもセキュリティパッチなどを配布できる
・認証スイッチ不要/ネットワーク遮断ソフトも不要で、検疫システムを構築できる
・マネージャーからクライアントPCに対して、BIOS情報の設定や診断プログラムの実行をリモート操作可能（SOL/IDE-R対応）。

JP1のAMT連携機能は、企業のITコンプライアンスへの対応をいっそう強力に支援します。
また、TCO削減もさらに加速。JP1、およびvPro™テクノロジー搭載PCの導入をぜひご検討ください。

SOL:Serial Over LAN　IDE-R:Integrated Device Electronics Redirect　TCO:Total Cost of Ownership



ソフトウェアを効率的かつ適正に配布運用したい。

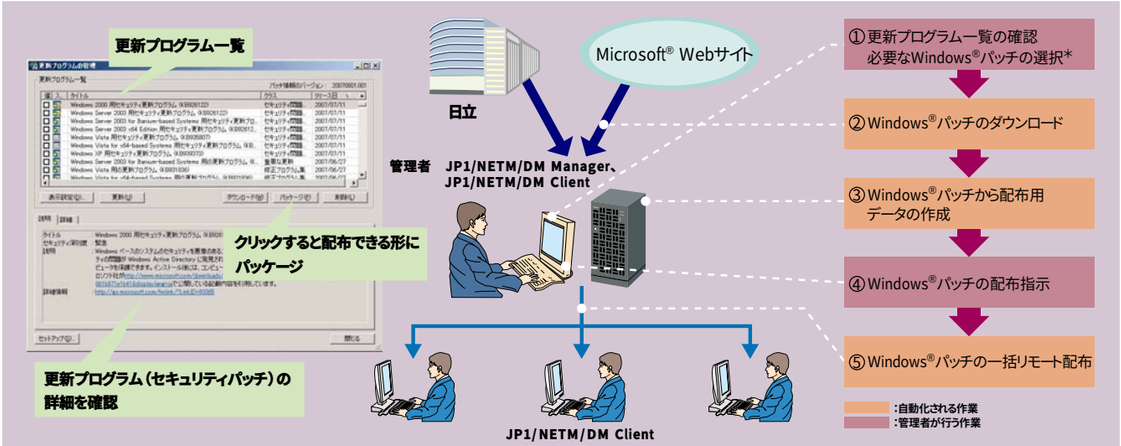
●パッチ配布の省力化を支援

Microsoft®社から提供されるセキュリティパッチやService Packなど、更新プログラムの一覧と、これらを適用するために必要なスクリプトを提供します。ボタン1つで、スクリプトとWindows®パッチを配布可能な形にパッケージできるので、配布したいときにすばやく対応できます。また、WSUSと連携することで、Microsoft® Officeなどのパッチも配布できます。

WSUS:Microsoft® Windows Server® Update Services

●ソフトウェアの配布・インストールの自動化

センターサーバからクライアントPCへのソフトウェアの配布・インストールを自動化できます。また、配布状況をサーバからビジュアルに確認できます。配布の際の運用方法には「PUSH型」と「PULL型」があります。



*更新プログラム一覧の最新情報を入手するには、日立ミドルウェアサポートサービスVの契約が必要です。

●計画的な配布運用を支援する日時指定スケジュール

ネットワーク上に分散するクライアントPCのソフトウェアを、一斉に切り替えることができます。また、実行日時を指定することで配布インストールを自動化できます。

●対話式インストーラを提供しているソフトウェアの配布

インストーラに自動応答するスクリプトファイルにより、対話式インストーラを提供している他社ソフトウェアやユーザープログラムをリモートインストールできます。また、Windows® インストーラに対応したソフトウェアは、スクリプトのテンプレートを利用してサイレントインストールが行えます。

●配布先グループの自動メンテナンス

新たに追加されたクライアントPCや移設されたクライアントPCを自動的に検知し、あらかじめ作成しておいたグルーピング条件（ポリシー）に従った配布先グループに自動的に振り分けることができます。ユーザーインベントリ項目を利用したグルーピング条件を設定することで、組織体制に合わせて階層化した、配布先グループを自動作成できます。これにより、組織体制との不整合がなくなるとともに、メンテナンス作業の省力化を図れます。

●信頼性の高いインストール支援

インストール条件指定によるクライアントPCの事前チェックや、インストール失敗時の自動リカバリーなどで、高信頼な運用を実現します。

各クライアントPCに対し、ソフトウェアのインストール条件（ハードディスクの空き容量、実メモリー容量など）を設定することで、ソフトウェアの配布可否を事前にチェックできます。また、インストール済みのソフトウェアのバージョンを条件に、ソフトウェア配布要否もチェックできます。

●各業務に適した運用支援

運用手順はユーザー自身で作成できます。例えば、クライアントPCの電源ON/OFFと組み合わせた配布運用も可能です。また、プログラム/データのインストール前後や、エラー発生時は、任意のプログラムを起動できます。これにより、さまざまな業務に適した運用が可能となります。

●ネットワークへの負荷を最小限に抑える多彩な配布方法

・大量データは分割した上で、インターバルを取りながら配布可能
・データ転送中であっても、マネージャーから中断や再開を制御可能
・緊急パッケージは、他データの転送を中断しても優先的に配布可能
・マルチキャスト転送による、LAN内の送信量や配布時間の削減

●ファイル収集

クライアントPCやサーバのファイルを一括収集して利用できます。ファイルを収集する直前/直後に任意のプログラムを起動できるため、ファイル収集前にデータを加工したり、収集後にデータを削除したりと、ユーザー業務に沿った運用を行えます。

遠隔地での障害発生や問い合わせに迅速に対応したい。

障害発生時には遠隔地であっても、迅速な対応が求められます。JP1の［JP1/NETM/DM］では、クライアントPCやサーバを遠隔操作できます。これにより、障害対応が迅速化するだけではなく、出張費の削減も図れます。

●画面共有とリモート操作機能

クライアントPCやサーバをマネージャー端末から遠隔操作できます。ディスプレイの切り替え操作なしで同時に複数のクライアントPCやサーバを監視できます。また、以下のような特殊操作も可能です。
・リモートログオン　・リモートシャットダウン/リブート
・ファイル転送　・クリップボード転送

●リモート操作内容の漏えい防止

遠隔地からリモート操作を行う場合に、接続先PCの画面を非表示（黒い画面）にできます。もし、画面非表示中にリモート操作が終了したり、画面非表示が強制解除された場合は、自動的に接続先PCをロックします。

●認証情報による接続元の制限

接続元を制限し、特定のPCや管理者にだけ接続を許可することで、リモート操作をより安全にお使いいただけます。
接続元は、次のような条件で制限できます。
・接続元PCのホスト名やIPアドレス
・接続元ユーザーのユーザー名とパスワード　など

●リモート操作の高速化

ビットマップの減色、転送データの圧縮、壁紙の表示/抑止、ローカルフォントの使用、ビットマップキャッシュによる描画などの機能を提供。低速な回線環境でもスムーズにリモート操作できます。

●画面の記録と再生

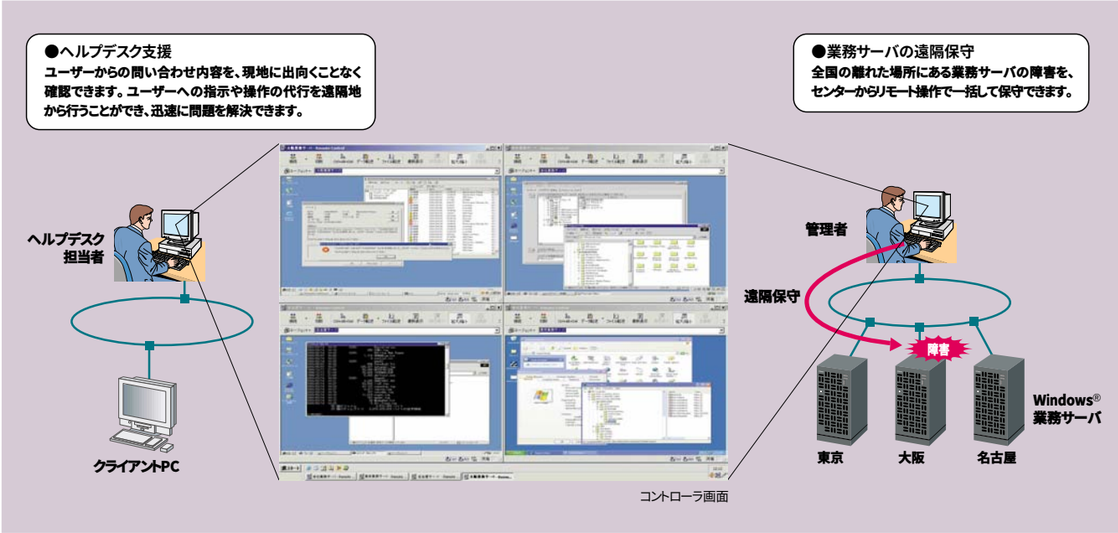
リモート操作時の操作内容をビジュアルな動画で記録できます。記録した操作内容は、配布して再生可能。例えば、操作手順を示すガイドや、監査証跡として利用できます。

●チャット機能

電話とマシンが離れていても、チャットを利用することにより画面上で対話しながら作業できます。一度に複数のPCと会話をしたり、特定のPCのみにメッセージを送ったりすることができます。

●質問者からのリモート操作の接続要求

ヘルプデスク対応で質問者側からリモート接続を依頼できます。また、複数のマネージャーに同時に接続を要求することも可能です。



※［リモート操作：JP1/NETM/Remote Control］でも同機能を提供しています。

クライアントPCへのインストールを自動化したい。

●スタートアップキットによるインストール

スタートアップキットで設定情報を事前に定義しておくことで、1台ごとに対話形式でインストールすることなく［JP1/NETM/DM Client］の初期導入を自動化できます。これにより、ユーザーの操作を最小限に抑えられます。

クライアントPCのセキュリティ対策状況を一元管理する　クライアントセキュリティ管理

「JP1/NETM/Client Security Control」

クライアントPCのセキュリティ対策状況を一元管理し、システム全体のセキュリティレベルを維持。
セキュリティ対策が不十分なクライアントPCを検知した場合、セキュリティポリシーに従って
最適なアクションを実施できます。

システム全体のセキュリティレベルを効率的に維持したい。

●セキュリティポリシーの設定（Plan）

組織のセキュリティ方針に基づき、部署ごとに、判定、アクションという2段階のセキュリティポリシーを設定できます。また、セキュリティ監査項目を自由に設定できるため、ユーザーの運用に合わせた柔軟なセキュリティ監査を実現できます。

＜判定ポリシー＞

セキュリティ監査項目の判定条件と危険レベルの設定

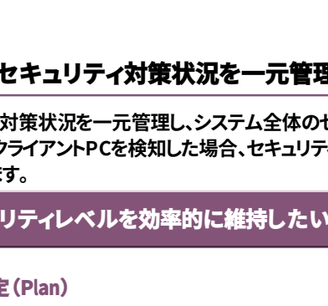
＜アクションポリシー＞

危険レベルに応じてクライアントPCに実施するアクションの設定

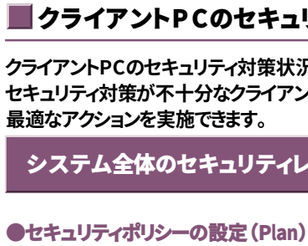
＜セキュリティ監査項目例＞

- パスワードの脆弱性
- Windows®自動ログオン機能の設定有効（なりすまし防止）
- 時刻合わせプログラムの非稼働（ログ監査時の時刻同期）
- Windows®更新プログラムの未適用
- ウイルス定義ファイルの未更新
- ウイルス対策製品の非常駐
- 不正ソフトウェアのインストール
- 必要なソフトウェアの未インストール　など

評価一覧画面



アクションポリシー編集画面



●危険レベルの判定（Do）

セキュリティ監査項目ごとに設定した危険レベルにより、各クライアントPCの危険性を判定します。また、危険レベルの判定は特定の事象を契機に自動実行できます。

＜危険レベルの判定契機＞

- クライアントPCによるインベントリ情報の更新時（自動実行）
- スケジューラによる定期実行時（自動実行）
- 管理者がクライアントPCに危険レベルの判定を指示した時（手動実行）

●危険レベルに応じたアクションの実施（Do）

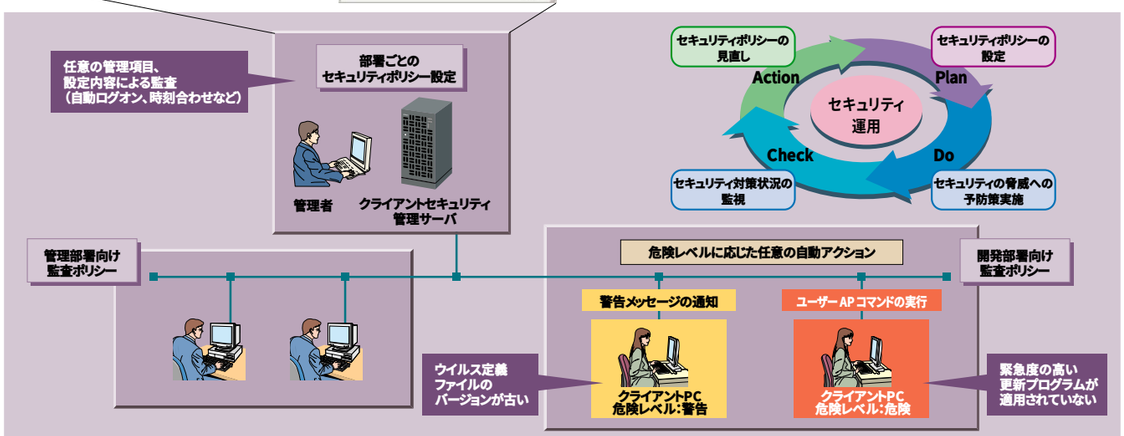
危険レベルの判定によりセキュリティ対策が必要なクライアントPCを検知した場合、危険レベルに応じたアクションを自動的に実行できます。例えば、クライアントPCに対して警告メッセージを通知したり、[不正PC接続監視・強制排除]製品、またはIEEE802.1x認証スイッチとの連携によってネットワークへの接続を拒否できます。

●セキュリティレベルの評価（Check & Action）

全体や部署ごとの現状を点数で評価できます。また、任意の期間について評価の推移をグラフで表示できるので、部署間の比較やセキュリティレベルの動向を把握できます。これにより管理者は、セキュリティ対策上の問題点が一時的な原因によるものか、長期的な原因によるものかを把握しやすくなるため、いっそう効果的な対策を講じることができます。

●セキュリティポリシーの自動更新（Plan-2巡目以降）

ウイルス対策製品については、エンジンバージョン、ウイルス定義バージョンを更新すると、セキュリティポリシーが自動更新されます。同様に、新しいWindows®パッチがリリースされた場合も、セキュリティポリシーは自動更新されます。



不正接続PCを自動的に排除する　不正PC接続監視・強制排除

「JP1/NETM/Network Monitor」

不正に接続されたクライアントPCを業務ネットワークから自動排除する仕組みを、
既存ネットワーク環境で実現できます。また、排除後に脆弱なPCを治療する検疫システムも構築できます。

不正なPCの社内ネットワーク接続を拒否し、企業リスクを最小限に抑えたい。

●不正接続クライアントPCを自動排除

システムに接続されたPCのIPアドレスやMACアドレスを収集し、接続を許可すべきPCのリストを作成します。このリストと自動照合することで、正規の利用者に影響を与えずに、不正接続したクライアントPCだけをピンポイントでネットワークから排除できます。なお、[統合資産管理:JP1/NETM/Asset Information Manager]が持つ情報を利用して、接続を許可すべきPCのリストを作成することもできます。また、[クライアントセキュリティ管理：JP1/NETM/Client Security Control]との連携により、その時のクライアントPCの状態に応じて接続可否を制御することもできます。

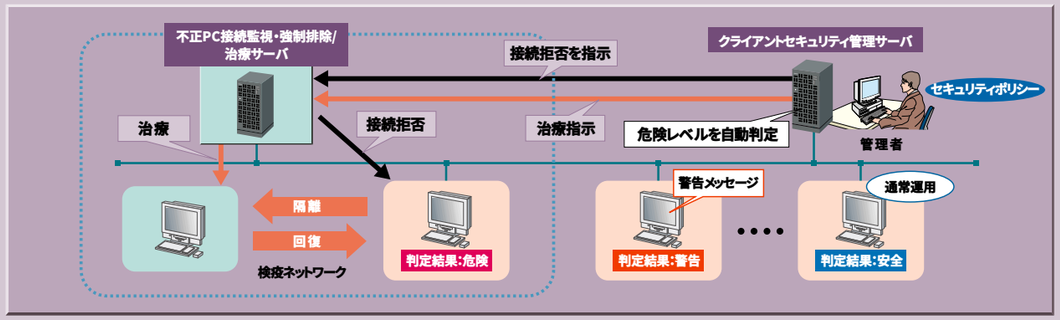
●新たなクライアントソフトウェアは不要

クライアントPCに新たなソフトウェアは不要なので、導入・維持が容易です。また、監視対象PCのOSや業務処理との相性を心配する必要もありません。

●既存ネットワークで運用可能

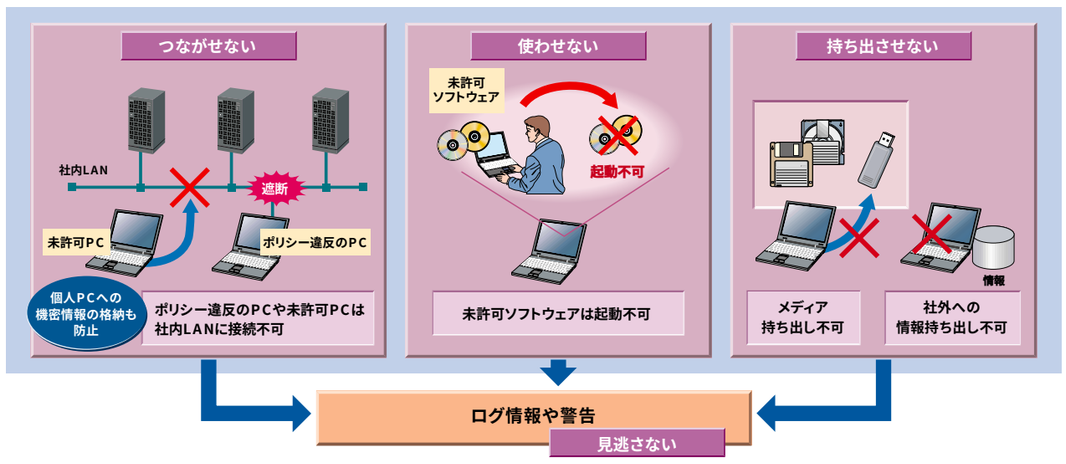
アドレス環境（固定IP、DHCP）や有線（ハブ、スイッチ）、無線を問わず導入できます。また、VLANに対応した環境での集中監視も可能。機器に依存しないため、既存システムをそのまま利用できます。

【検疫システムの実現】「クライアントセキュリティ管理」製品と「不正PC接続監視・強制排除」製品とを連携させることで、特別な機器がなくても脆弱なクライアントPCの隔離から治療までを実現する、検疫システムを構築できます。



4つの視点で実現するクライアント統制

近年、情報漏えい事件が多発し、さまざまな問題点が指摘されています。
重要データの社外への持ち出し、個人PCの業務利用、さらにウイルス感染など、それぞれのリスクに適切に対処することが不可欠です。JP1では「つながせない」「使わせない」「持ち出させない」「見逃さない」という4つの視点からクライアント全般を統制し、企業の健全性・信頼性の維持を支援します。



システム監査に不可欠な変更管理やライセンス管理を実現する

統合資産管理

「JP1/NETM/Asset Information Manager」

JP1が管理するIT資産情報を集約。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、さまざまな視点からのIT資産管理を実現します。

IT資産を一元管理し、内部統制へ向けた万全の体制を備えたい。

●「資産管理システム」によるIT資産の統合的な管理

［ソフトウェア配布・資産管理:JP1/NETM/DM］が、ハードウェアの使用状況やインストールされているソフトウェアの種類といったクライアント管理に必要なインベントリ情報を取得。さらに［ネットワーク・ノード・マネージャ:JP1/Cm2/Network Node Manager］が取得したネットワークに関する情報、そのほかの資産管理ツールが取得した保守やリース契約に関する情報などを相互に関連付けながら、資産管理データベース（構成管理DB）として統合的に管理できます。

●メンテナンスを省力化しつつ、一元管理が可能

インベントリ情報は定期的に収集してデータベースに反映するので、常に実態と合った情報で管理可能。また、異動やレイアウト変更の際には、機器の管理情報である「部署」、「設置場所」、「機器状態」などを一括して変更できます。

●IT資産の検索と集計、レポート化を支援

機器やライセンス、契約情報や問題点などの台帳から、目的に応じて必要な情報を取り出して、活用できます。例えば、「登録日の古い機器」や「一定レベル以下の性能の機器」、「棚卸が終わっていない機器」など、さまざまな目的に合わせて機器をリストアップ。また、検索結果は部署や設置場所ごとに集計したり、グラフ化が可能。各種報告書へも利用できます。

●柔軟な運用にも対応するインタフェース

資産管理情報はWebブラウザで参照できます。利用者の役割や権限に応じて参照範囲を限定したり、業務をしやすい画面に表示内容をカスタマイズするなど、柔軟な運用に対応できます。

内部統制の強化に役立つ、各種情報の管理機能

・ソフトウェア適用管理
機器に、ウイルス対策製品やパッチなどがインストールされているかどうかを調査。これらがインストールされていない機器に対しては、［ソフトウェア配布・資産管理:JP1/NETM/DM］と連携し、パッケージング済みのソフトウェアやパッチを配布可能です。

・契約管理
契約日、契約期間、契約会社などの契約情報を登録管理します。契約情報とその契約の対象となる機器やソフトウェアを関連付けて管理。また、契約書のデータを添付して登録しておくこともできます。

・変更管理
機器の現時点の状況だけではなく、これまでの変更の履歴も管理できます。変更時期と変更内容はもちろん、CPU/メモリー/ディスク容量/システム装置/ソフトウェアなど、変更対象ごとに検索が可能。「特定のソフトウェアをインストールしたことのある機器」を調べたりできます。

＜その他、管理できる主な情報＞
資産情報、ハードウェア資産情報、ネットワーク情報、IPアドレス管理情報、ライセンス情報、ソフトウェア稼働情報、移管履歴、保守履歴、ユーザー管理情報、部署情報、設置場所情報　など

一元管理した情報を活用し、迅速かつ確実な対応を実現したい。

●進ちょく把握と正当性の証明が容易な「案件の 見える化 」

「機器導入依頼」、「機器発注依頼」など、機器やソフトウェアの導入・変更手続きや承認の流れをフローにして「見える化」。指定された処理期限を超過した案件が「赤色」表示で強調されます。また、送信した案件がいつ処理されたか、どこの管理ノードまで処理が終わっているかなどを確認できます。手続きで使用した情報はサーバに登録されるので、より確実に申請・承認でき、正式な処理ルートで承認された内容であるという証明にも役立ちます。

●問題点管理

IT資産管理システムで発生している問題点とその対処状況を管理します。類似した障害の対策情報を参考にすることで、発生した障害に迅速に対応できるため、システムの安定運用を維持できます。

●「不正PCの接続拒否」にも管理台帳を活用

[JP1/NETM/Asset Information Manager]の管理台帳に登録されている機器情報（IPアドレス、MACアドレス）は、[不正PC接続監視・強制排除機能：JP1/NETM/Network Monitor]でも利用できます。これにより、管理台帳に登録されていない機器のネットワーク接続を、[JP1/NETM/Network Monitor]の機能で拒否できます。

案件一覧画面

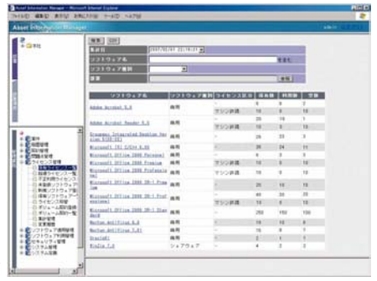
案件進ちょく確認画面

ライセンス管理により、コンプライアンスの徹底と資産の有効利用を図りたい。

●ソフトウェアの不正使用を防止し、コンプライアンスを維持

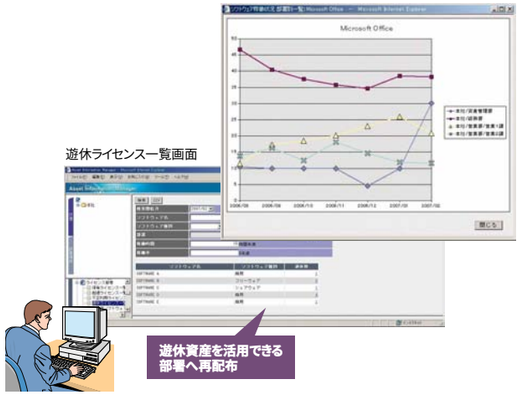
●ライセンス管理
ソフトウェアのライセンス保有数、利用数および空き数を集計して、利用状況を調査します。各部署の保有数、割り当て数、利用数、空き数、および下位の部署も含めた累計を表示。ボリュームライセンスの契約情報を登録すれば、ポイント制のライセンス管理も実施できます。また、組織改変などに伴なう、移管（ライセンスの管理部署を変更）にも対応。ライセンス数の推移はグラフでも表示できます。

●不許可ソフトウェアの監視
許可されていないソフトウェアが、インストールされていないかを調査し、該当するソフトウェアをインストールしている機器の一覧を表示できます。使用者への通知も可能です。


保有ライセンス一覧画面

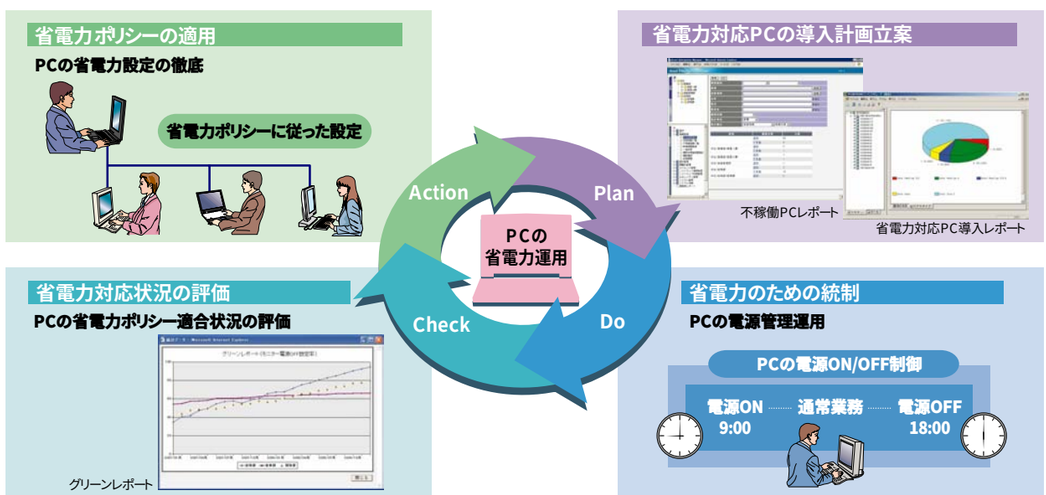
●遊休資産を探し出し、有効利用を促進
ソフトウェアの稼働状況を調査し、稼働時間を月ごとや部署ごとに集計できます。また、ユーザーが使用したプログラムや、操作したウィンドウのタイトルの履歴も取得。これにより、あまり使用されていないソフトウェアを探し出せます。さらに、ソフトウェアの稼働状況から、利用されていない機器も抽出。遊休資産を探し出すことで、活用できる部署への再配布など、より効果的なIT投資計画の策定が可能となります。

稼働状況確認画面



グリーンITのPDCAサイクル　～JP1の資産・配布管理製品の活用例～

グリーンITとは「環境負荷の少ないITインフラを導入すること」、また「ITの活用によって、企業活動の環境負荷を減らすこと」の2点を示すキーワードです。ITを導入したり活用したりする際には「グリーンIT」を意識することが社会的に求められつつあります。JP1の資産・配布管理製品は、グリーンITへの対応を支える機能も充実しています。これらを活用することで、例えば、PCの省電力運用をPDCAサイクルにより継続的に改善できます



業務システムの運用実績についての監査を支援する

監査証跡管理

「JP1/NETM/Audit」

内部統制が機能していることを証明するために、必要とされる監査証跡（証跡記録）を収集・管理し、
長期間にわたる保管を実現します。

業務プロセスの証跡記録を管理することで、監査に備えたい。

●証跡記録の収集

業務手順やシステムの変更履歴、ユーザー情報の登録・削除履歴など、業務システムにかかわる監査で必要となる証跡記録を自動収集できます。証跡記録は、監査証跡管理サーバから製品名を指定すれば、自動的に収集対象に設定可能。証跡記録では、「いつ」「誰が」「どのような権限で」「どこから」「何をした」といった内容が確認できます。

●バックアップ/保管履歴の管理

長期保管が必要となる監査証跡のバックアップ効率を上げるため、収集された証跡記録は一定期間ごとに分割してバックアップできます。その際は、「いつからいつまでの証跡記録」を「どんなファイル名で保管したか」の情報やアクセス履歴も管理できます。また、証跡記録を削除したり、閲覧サーバに取り込んだりする際にはユーザー認証を行います。さらに、閲覧サーバに取り込む際は記録の改ざんを自動検知できます。これらの機能により、証跡記録の正当性を一層強固に保てます。

監査証跡管理

●証跡記録の提示を強力に支援

監査時に求められる観点で証跡記録を検索・集計し、必要な記録を効率良く抽出できます。代表的な検索・集計条件はテンプレートとして提供しています。テンプレートはそのまま利用するほかに、カスタマイズも可能です。検索・集計条件は保存できるので、次回の評価・監査時にも利用できます。また、検索・集計結果はCSV形式、PDF形式*のデータとして、集計結果はグラフ化して出力することもできます。

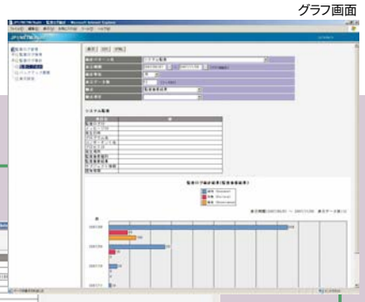
＊［帳票システム構築支援 EUR］との連携が必要です。

＜提供する検索・集計テンプレート＞
アカウント監査（ユーザー監査）
・ユーザー作成監査：指定期間に作成されたユーザーを一覧形式で抽出
・ユーザー削除監査：指定期間に削除されたユーザーを一覧形式で抽出
・パスワード監査：指定した期間内にパスワードが変更されていることを抽出
ログ監査（変更アクティビティ監査）
・ポリシー監査：指定した期間に変更されたポリシーを一覧を抽出　など

●内部統制の有効性評価や監査時に利用

過去の証跡記録を参照することで、あらかじめ規定されているルールどおりに業務が行われているかどうかを検証できます。自動出力される証跡データは、人手を介する記録より信憑性が高いことから、少ないテスト、サンプル抽出で評価・監査できるため、評価・監査時の負担も大幅に軽減できます。

グラフ画面



運用例

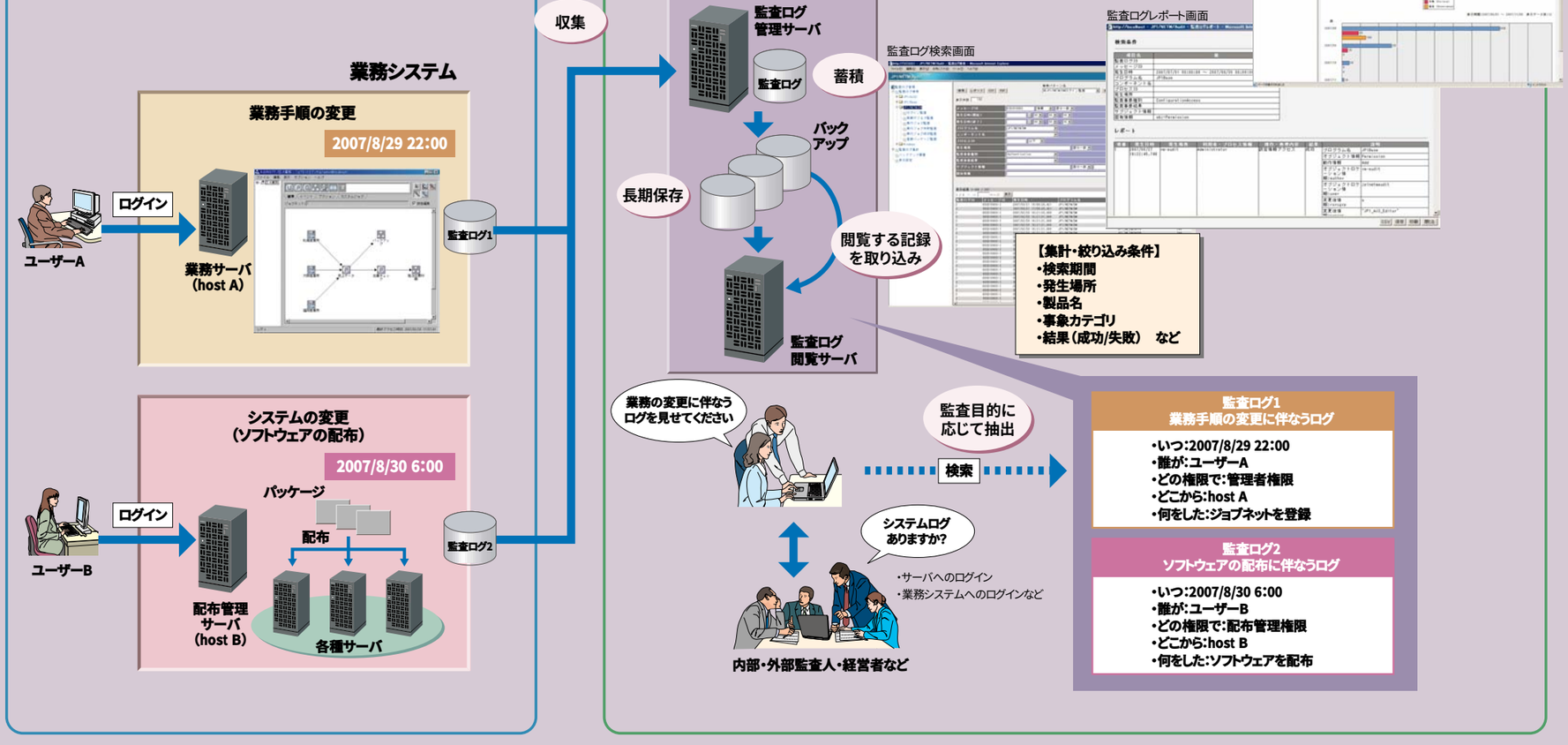
日々の業務の運用や変更に伴うログ（証跡記録）を一元管理します。証跡記録を検証することで、内部統制を強化できるとともに、監査にかかる工数も削減できます。

この運用例で使用する主なＪＰ１製品

監査証跡管理（資産・配布管理）
業務システムに関連する操作履歴やシステム変更履歴、OS（Windows®、UNIX、Linux）へのログイン/ログアウト履歴などの証跡記録を自動収集し、証跡記録の長期保管とバックアップ運用を実現します。発生期間などに基づいて、証跡記録を容易に参照できます。

ソフトウェア配布・資産管理（資産・配布管理）
内部統制を行うには、IT資産の現状はどうなっているのか、必要なパッチがあたっているのかといった状況把握が必要です。本製品では、これらのインベントリの情報収集・管理を実現します。また、許可していないソフトウェアの起動抑止および、クライアントPCの利用状況や不正操作などの把握が可能。監視の事実を告知したり、禁止操作について利用者に警告したりすることで、不正な操作や行動を抑止できます。

ジョブスケジューラ（ジョブ管理）
業務の中には、毎日の売り上げデータの集計や日報の作成、月末ごとの締め処理、受注伝票の発行など、定型的・定期的な業務が数多くあります。本製品は、このような定型的・定期的な業務を自動化します。日々実行される業務を自動化することで、コストの削減と正確な業務実行を実現できます。また、自動化により、人手による改ざんやミスの入るリスクを軽減します。



設備資産やネットワーク構成をビジュアルに管理する

設備資産管理

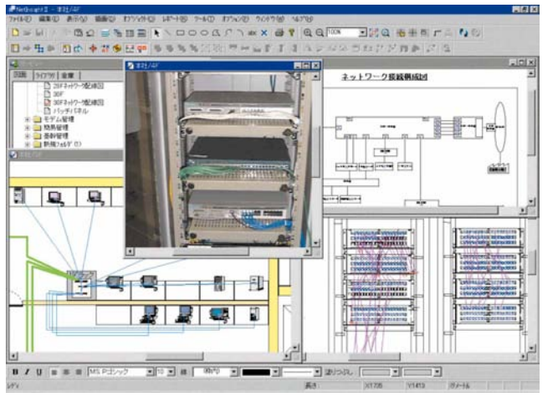
「JP1/NetInsight Ⅱ」

複雑化するネットワーク環境、変化するLAN設備資産をフロアレイアウト図やネットワーク構成図で
視覚的に管理できます。資産台帳にあるマシン情報の参照や機器の設置場所を画面上に表示できます。

ネットワーク設備の資産情報を容易に管理したい。

●資産情報をフロアレイアウト図でリアルに一元管理

サーバやハブ、ケーブルなどの設備資産情報をフロアレイアウト図とリンクしたデータベースで管理します。フロアレイアウト図上の機器をマウスでクリックするだけで必要な情報を参照できます。しかも、ツリー構造で表示するので、目的の情報をすばやく検索できます。



ネットワーク構成図/機器配置図画面

●写真や表などの関連情報の呼び出し

Microsoft® WordやMicrosoft® Excelなどで作成されたデータや、管理に必要となる写真などをフロアレイアウト図から呼び出せます。

●図情報のインポート

CADやMicrosoft® Visioで作成したフロアレイアウト図はそのままインポートできます。これまで管理のために作成していたフロアレイアウト図をそのまま使用できるため、新たに作成する必要がなく、すぐに管理を始められます。

●先行統合配線管理のサポート

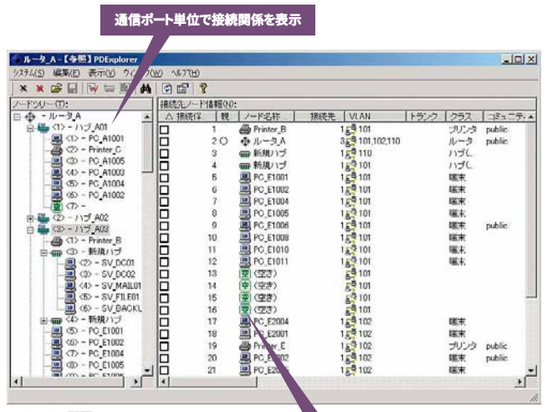
複雑化するパッチパネルや情報コンセントの配線を管理する際は、接続関係を専用ダイアログに表示できるため、容易にメンテナンスできます。また、情報コンセントとパッチパネルまでの接続経路の表示や、パッチパネルの接続一覧の自動生成なども可能です。

●Webブラウザからの資産情報参照・更新オプション

フロアレイアウト図・ラック収容図などの図面や、ネットワーク機器のプロパティ情報や接続情報をWebブラウザで参照および更新できるため、場所を選ばない管理が可能になります。

●ポート単位の接続構成も自動収集

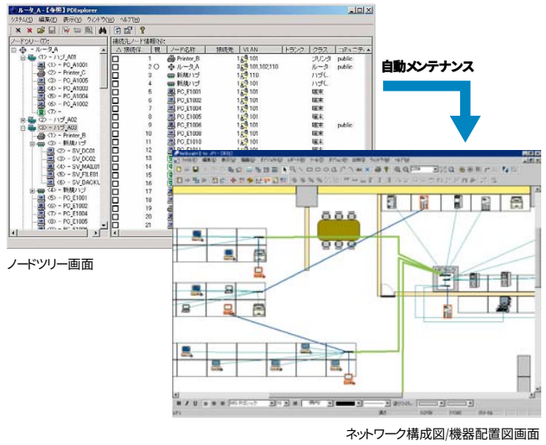
SNMPのMIB情報を収集し、通信ポート単位の接続構成を自動作成。ルータやスイッチングハブ、インテリジェントハブなどの接続関係（ポートの使用状況）を表示するため、ひと目で空きポートを把握できます。また、ネットワーク設備資産を管理するためのフロアレイアウト図の作成が容易。推論機能により、ノンインテリジェントハブの存在も予測できます。



ノードツリー画面

●メンテナンスフリーのフロアレイアウト図

定期的な監視により、ネットワーク接続の変化、機器の追加・削除などを発見し、画面を自動的に更新します。面倒だったフロアレイアウト図のメンテナンスの手間を大幅に軽減できます。



ノードツリー画面

ネットワーク構成図/機器配置図画面

情報漏えいからクライアントＰＣを強固に守る

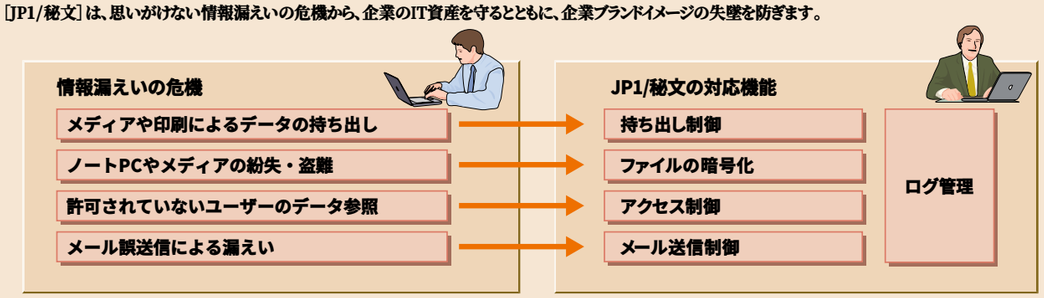
情報漏えい防止

「JP1/秘文」

メディアや印刷による機密情報の不正な持ち出しを防止します。
さらに、これらのログを管理することで高いセキュリティレベルを維持。
万一情報が漏えいした場合にも、ファイルの暗号化により第三者による閲覧を防止できます。

■多彩な情報漏えい防止機能

［JP1/秘文］は、思いがけない情報漏えいの危機から、企業のIT資産を守るとともに、企業ブランドイメージの失墜を防ぎます。



クライアントＰＣやサーバ内の機密情報の持ち出しを防ぎたい。

●メディアや印刷物の持ち出し制御

リムーバブルメディア（FD、MO、USBメモリーなど）や、共有ファイルなどネットワークドライブへのデータの無断コピーを禁止。プリンタへの無断印刷も禁止できます。これにより、メディア・印刷物の持ち出しによる情報漏えいを防げます。また、印刷を許可した場合には、印刷物に透かし文字を強制的に挿入することもでき、機密情報の取り扱いモラルの向上を期待できます。

●より安全なデータ持ち出し

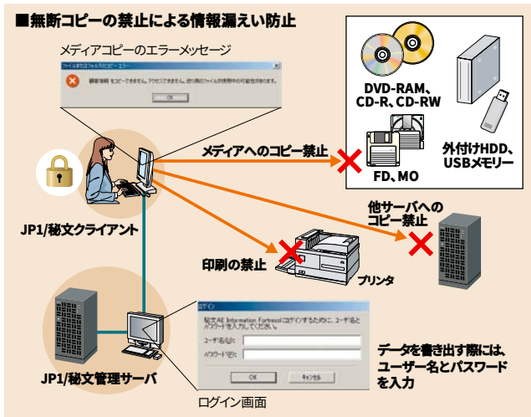
USBメモリーに、Microsoft® Office文書*などをより安全に持ち出すためのポリシーを設定できます。ポリシー設定済みのUSBメモリーに格納した文書は暗号化され、外出先のPCや別メディアにはコピーできません。USBメモリー上では編集/保存が可能です。さらに、持ち出し操作や文書に対する操作ログが残るため、持ち帰ったログは［JP1/秘文AEログサーバ］で管理できます。業務上、どうしても持ち出さなくてはならない文書は、このUSBメモリーに格納することで、流出を防止しつつ、より安全に使用できます。

*Microsoft® Office（Word、Excel、Powerpoint）で作成した文書に対応します。

＜編集時に抑制できる操作＞

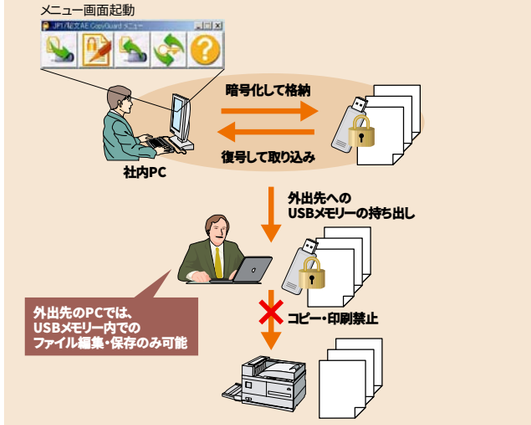
- 印刷
- 文書内の情報の他ウィンドウへのドラッグ&ドロップ
- ［PrintScreen］キーによるハードコピーの採取
- ショートカットキーによる操作
- 特定アプリケーションの起動

■無断コピーの禁止による情報漏えい防止



ログイン画面

■USBメモリーを使ったより安全なデータ持ち出し



機密情報を第三者に閲覧されることなく、安全にやりとりしたい。

●クライアントPCのファイル暗号化

PC上のデータをドライブ単位で暗号化して、PCの盗難、置き忘れなどによる情報漏えいを防止します。ユーザーはファイルの暗号化や復号を意識する必要はありません。また、PC所有者以外がデータを参照できないように、以下のような認証機能を用意しています。

- ID/パスワード(Windows®ログオン画面と[JP1/秘文]独自認証画面のどちらかを選択可能)
- ID/パスワード+iKey*
- ID/パスワード+拡張認証(ID/パスワードに加え、[JP1/秘文]独自のパスワード認証を追加可能)

*iKey:PCのUSBポートに鍵のように差し込んで利用する認証用USB機器

●自己復号型の暗号ファイル

組織外へデータを提供したり、メールにファイルを添付したりする際には、パスワードを入力するだけで復号できる自己復号型機密ファイルを利用できます。

●持ち出しメディアの暗号化

[JP1/秘文]でフォーマットしたリムーバブルメディアにデータを格納することで、メディア内のデータが暗号化され、メディアの置き忘れや紛失に起因する情報漏えいを防止できます。[JP1/秘文]をインストールしたPCだけが参照・更新できるので、組織内のデータのやりとりに便利です。

許可されていないユーザーによるファイル参照を防ぎたい。

●共有ファイルへのアクセス制御

ファイルサーバ上の共有ファイルを暗号化し、フォルダ単位でユーザーの所属や役職に応じたアクセス権を設定できます。フォルダ内のデータは、たとえシステム管理者であっても、アクセス権がなければ自由にアクセスできません。参照だけが許可されたユーザーは、保存や印刷も禁止されます。アクセス権をきめ細かく設定した厳重なセキュリティで、不正アクセスから共有データを守ります。

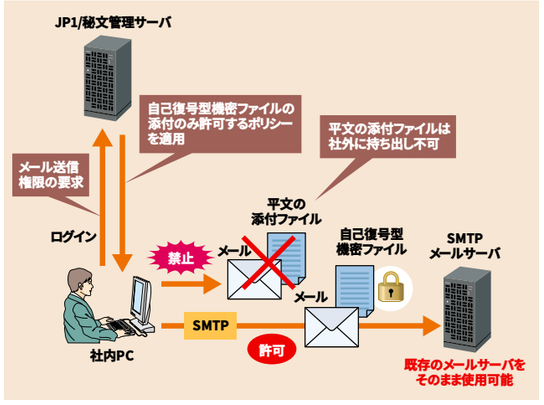
<アクセス権の設定例>

管理者(自部署):共有ファイルの参照および更新を許可。
管理者(他部署):共有ファイルの参照およびクライアントPCへの保存を許可。
一般ユーザー:共有ファイルの参照を許可。参照以外の操作(クライアントPCへの保存、印刷、PrintScreen、コピー、編集、メール添付 など)を禁止。

メール誤送信による情報漏えいを防ぎたい。

●メール送信制御(クライアント単位)

持ち出し制御の1つとして、クライアントのメール送信制御を行えます。ユーザーやグループ単位でポリシーを設定でき、柔軟なメール送信制御(SMTPを使用したメールに対応)が可能です。



<ポリシー設定例>

- 添付ファイル付きメールの送信許可
- 添付ファイル付きメールの送信禁止
- 自己復号型機密ファイル付きメールの送信のみ許可

●メール送信制御(ドメイン単位)

●グループウェア環境のメール制御

ドメイン単位でポリシーを設定し、添付ファイルのあるメール送信を制御可能。グループウェア環境でもメール(非SMTP)による情報の持ち出しを防止できます。また、送信メールのログを取得し、ポリシー違反時には送信者や管理者にメール通知できます。

●添付ファイルの自動暗号化

全あて先に共通のポリシーを設定し、ユーザーが意識することなく、添付ファイルをサーバ上で自動的に自己復号型機密ファイルに変換できます。また、必要に応じてあて先ドメインごとに個別ポリシーを設定することもできます。

各種操作ログを管理し、不正なユーザー操作を抑止したい。

●ログ管理(アクセスやイベントログの一元管理)

「いつ」「誰が」「どんな」ファイルを持ち出したのか、アクセスしたのかといったログがサーバに自動送信され、セキュリティ管理者が一括管理できます。メディアにコピーして持ち出した場合、ファイルそのもののコピーをサーバ上に残すこともできます。また、ログファイルは暗号化して保存されるので、セキュリティ管理者だけが専用ツールで復号して参照・解析可能。ログ画面では項目ごとに表示/非表示を選択でき、検索機能も充実しています。

●ログ管理([JP1/秘文]ログの一元管理)

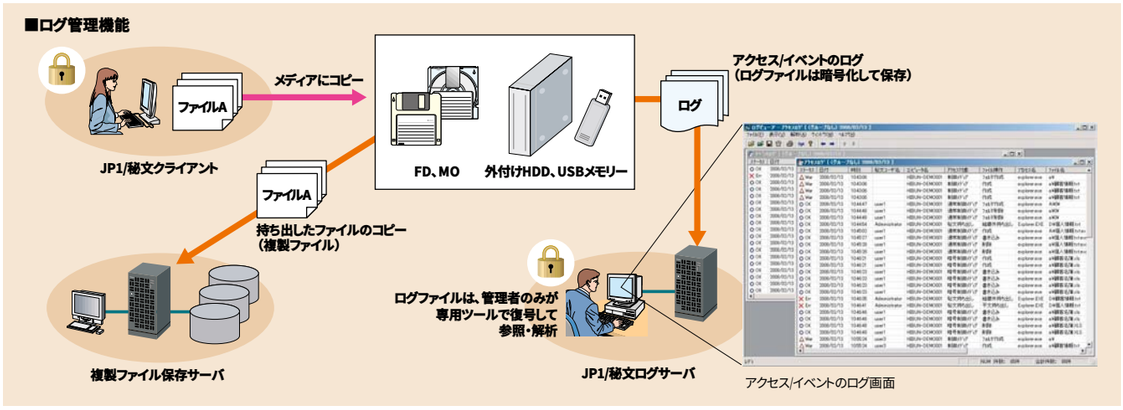
各拠点に分散する[JP1/秘文]ログを一元管理できます。

●[JP1/秘文]ログの解析・CSV出力

事前に設定した定義ファイルに基づいて[JP1/秘文]ログを自動解析し、CSV形式へ出力。ログ解析からレポート作成まで、面倒な作業を簡略化できます。

●Web上での[JP1/秘文]ログの解析・管理

離れた拠点からでもWebブラウザ上で[JP1/秘文]ログを管理できます。さらに、充実した検索機能を活用することで、不審なユーザーを抽出できるため、早期の対応が可能です。



情報漏えい防止製品の導入や運用を効率化したい。*

●インストール可能な環境をチェック

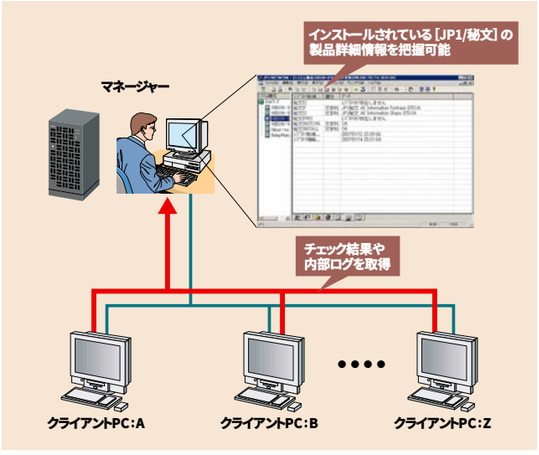
空きディスク容量の十分/不十分など、[JP1/秘文]をインストールするために必要な条件を満たしているかどうかをチェックできます。インストール条件を満たしている場合、[JP1/秘文]をリモートでインストールすることができます。これにより、初期導入時やバージョンアップ時の作業負担を軽減できます。

●内部ログの収集

[JP1/秘文]の内部ログをリモートで取得できます。[JP1/秘文]に関する調査時のユーザー作業負担を軽減できます。

●[JP1/秘文]の製品詳細情報の取得

[JP1/秘文]製品のうち、どの製品がインストールされているか把握できます。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。これにより、必要な[JP1/秘文]製品が的確にインストールされているかどうかを把握できます。



*ソフトウェア配布・資産管理[JP1/NETM/DM]が提供する機能です。