IT統合管理ソフトウェア

Protect Anyware 2.0

～ご紹介資料～

2015/7

JBアドバンスト・テクノロジー株式会社
セールス・マーケティング

情報漏洩に関する事件

クライアントソフトの脆弱性を突いた攻撃

クライアントソフトの脆弱性（ Adobe Reader、Adobe Flash Player、JRE等）
を攻撃されウイルスに感染、システム内の情報が窃取された。

標的型諜報攻撃の脅威

取引先をかたって企業の関係者にウイルス付きのメールを送り付け、
メールに記載されたウェブサイトにアクセスすることでウイルスに感染した。

内部犯行

内部の人間による故意の情報漏洩や不正操作による被害があった。

セキュリティ事故は他人事ではない！

Protect Anyware 2.0 とは・・・

IT資産管理、ログ管理などのIT統合管理ツール

- ✓ 様々な情報を自動取得、効率よくIT資産を管理
- ✓ USBメモリによる情報漏洩対策を強化
- ✓ クライアント端末の操作ログを取得
- ✓ 個人情報をファイルの中まで検索
- ✓ 管理されていないコンピューターを検知・遮断

３つのコンセプト

かんたん

導入、設定、運用、必要なことはかんたんに

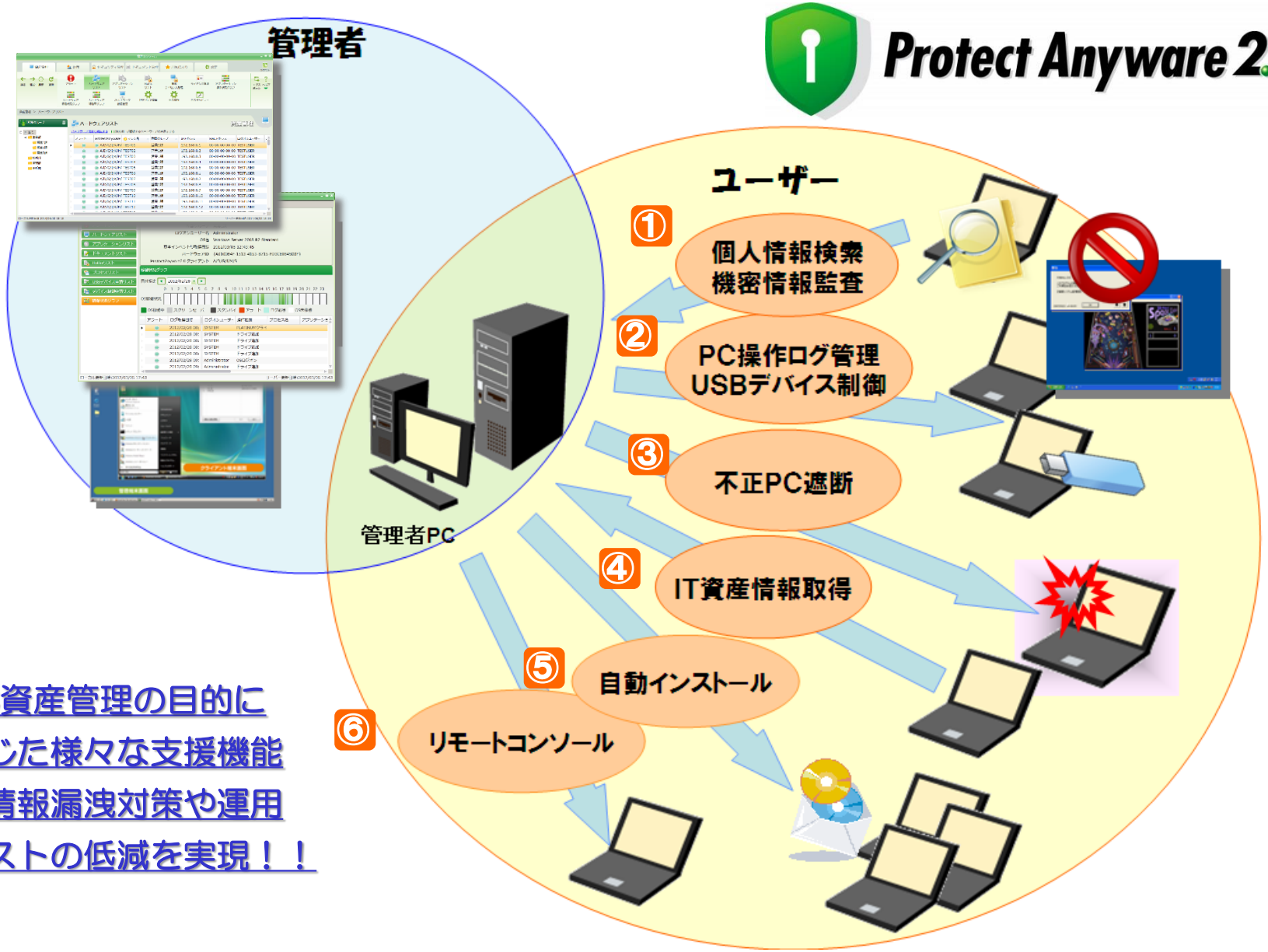
使いやすい

使いやすさにおけるさまざまな工夫で管理者にやさしい製品

オールインワン

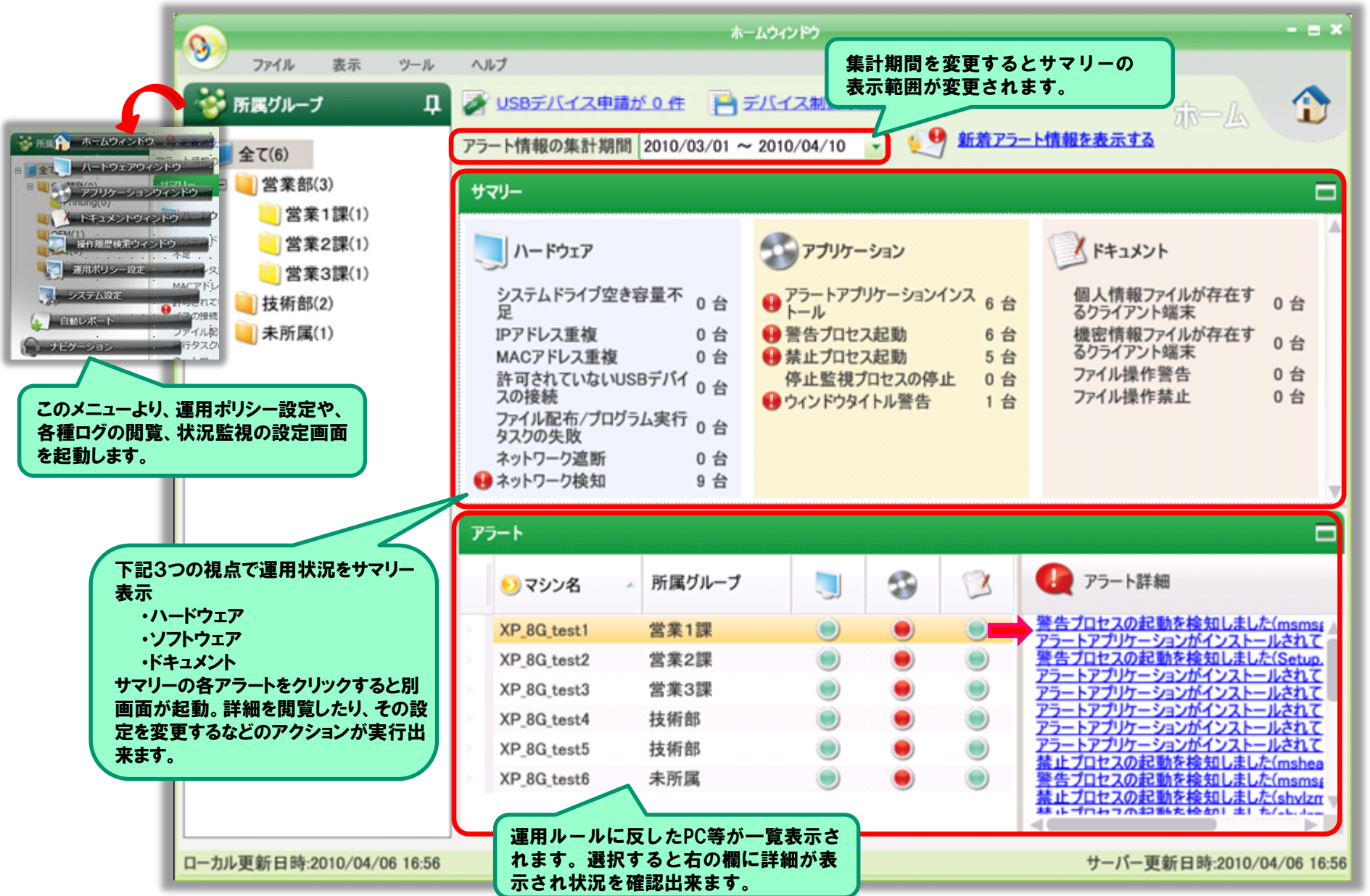
様々な機能がオールインワンの高いコストパフォーマンス

情報資産を「まもる」トータルＰＣ管理をかんたん実現！



PC資産管理の目的に
応じた様々な支援機能
で情報漏洩対策や運用
コストの低減を実現！！

全ての情報資産はホーム（管理画面）から集中管理



このメニューより、運用ポリシー設定や、各種ログの閲覧、状況監視の設定画面を起動します。

下記3つの視点で運用状況をサマリー表示
- ・ハードウェア
- ・ソフトウェア
- ・ドキュメント

サマリーの各アラートをクリックすると別画面が起動。詳細を閲覧したり、その設定を変更するなどのアクションが実行出来ます。

運用ルールに反したPC等が一覧表示されます。選択すると右の欄に詳細が表示され状況を確認出来ます。

NEW!

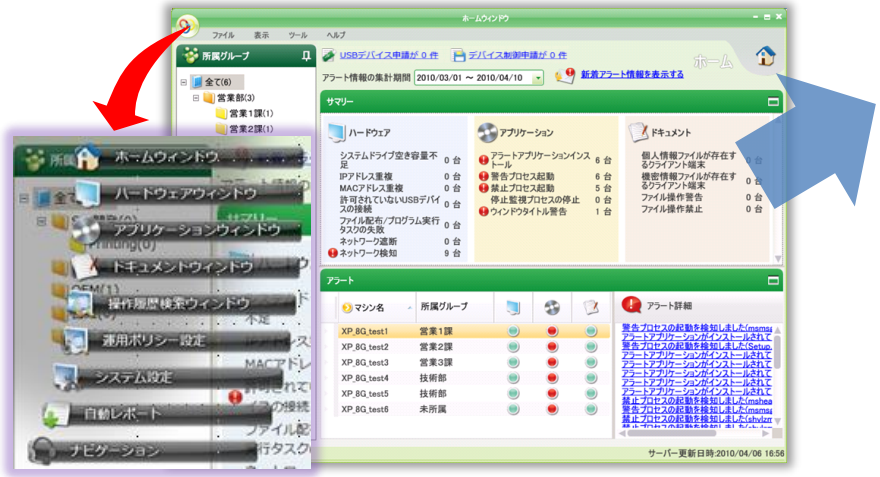
新バージョンVer.7では管理者にとって、さらに使いやすいインターフェイスに生まれ変わりました！

つかいやすさの向上

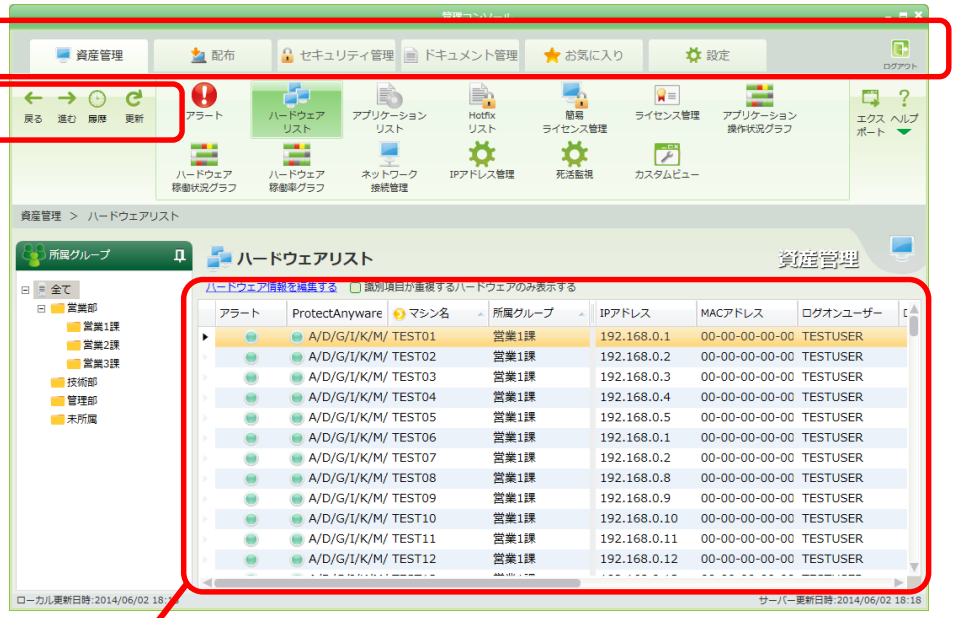
タブの導入により、ひとつのウインドウのまま目的の管理画面を表示できます。

操作に迷うことはありません。

Ver.5



Ver.7



画面上の情報を直接編集できます。
フィルターですばやく必要な情報を抽出。

Webブラウザのような操作性でワンクリックで一つ前の画面に戻れます。

NEW!

新バージョンVer.7では、
オプション機能としてファイル暗号化機能が追加されました！

ファイルが外部に流出しても
『**追跡**』して『**削除**』できる。

まったく新しい仕組みの暗号化です。

ファイルを守る。

ファイルを
暗号化して制御

制御内容
- 閲覧回数 / 閲覧の期限
- 保存禁止
- 印刷禁止
- 文字列や画像のコピー
- プリントスクリーン禁止

追跡する。

どこで、
開いても追跡

アクセスログの確認
- いつ？
- どのファイルに？
- 誰が？
- 何をした？

削除する。

渡したファイルを、
あとから削除

リモート制御
- ファイルの消去
- 制御内容の変更
- アクセス権限の変更

IT資産管理機能

Protect Anyware 2.0

ソフトウェア資産管理（SAM）実現に向けた現状把握や情報の突合作業を効率化

<こんな課題を解決します>

- 手作業での資産管理の手間がかかっている
- ソフトウェア資産管理（SAM）を実現するための作業を効率化したい
- 情報資産を有効活用できず、コスト削減がなかなかできない

様々な情報を自動取得、効率よくIT資産を管理

社内で稼働するハードウェア、アプリケーションの情報を収集し、管理します。

多彩なライセンス/管理形態に対応したソフトウェア管理でコンプライアンス実現

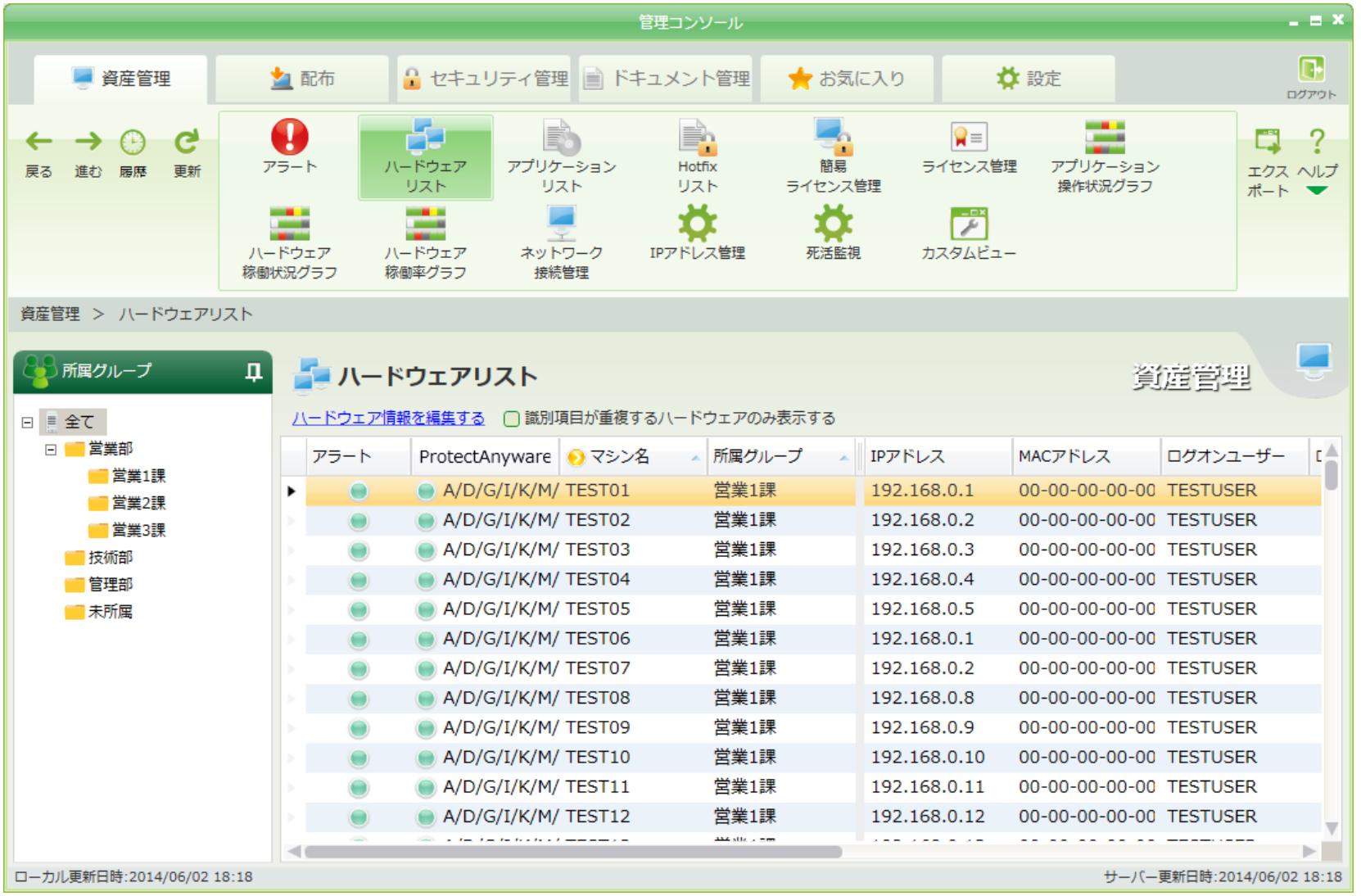
アップグレードやダウングレード等にも対応、煩雑な管理を一元化できます。

アラートをチェックし問題をすぐに解決

管理コンソールと、自動アラート通知メール機能で問題を迅速に把握できます。

ハードウェアリスト画面

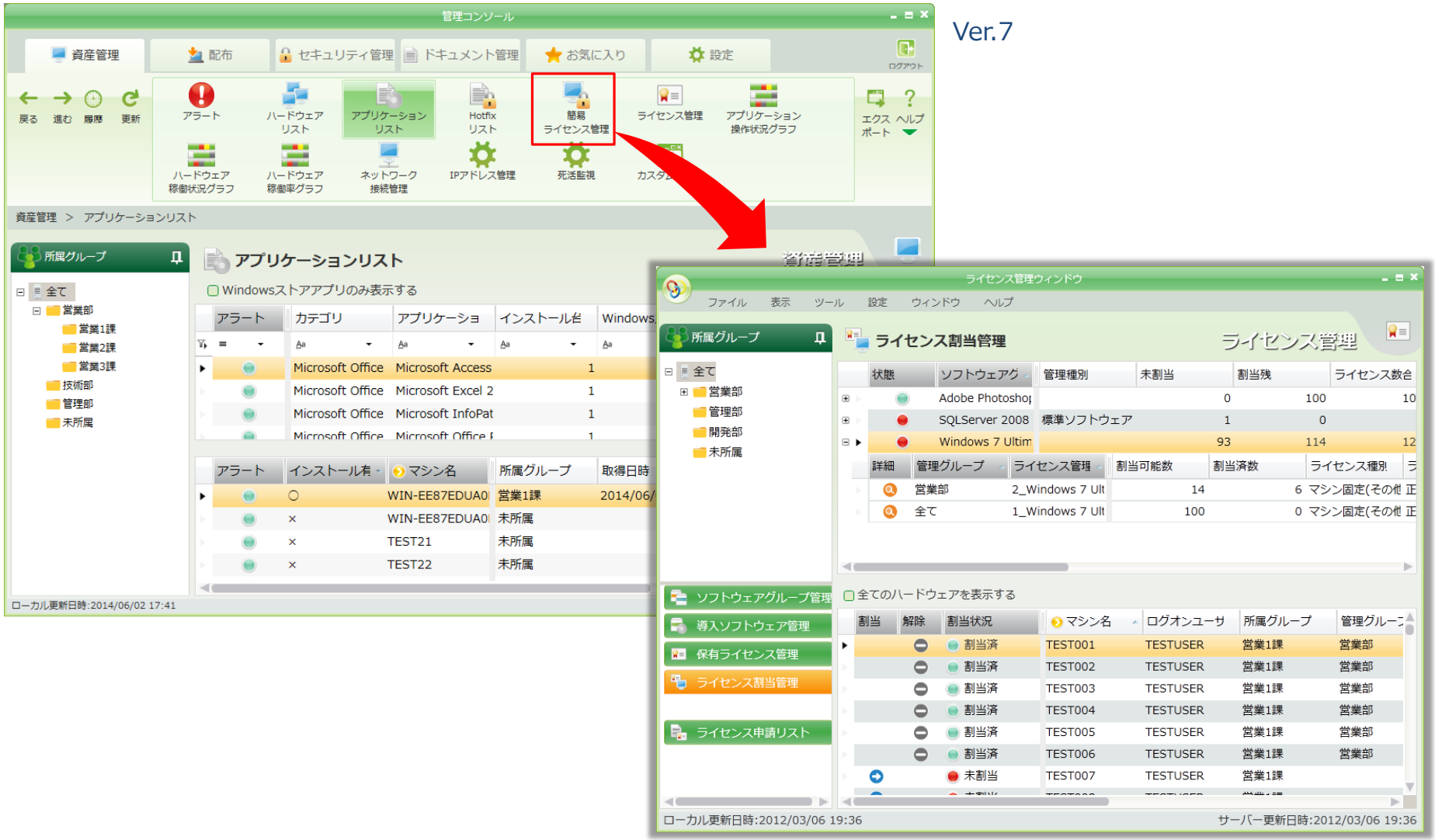
収集情報：マシン名、ログオンユーザー名、IPアドレス、MACアドレス、CPU容量、メモリ容量、ハードウェアドライブの空き容量・総容量、OS名、OSサービスパック、ベンダー名、モデル名 等



Ver.7

ソフトウェア管理画面

端末にインストールされているソフトウエアは自動収集されますので、購入しているライセンス数を入力頂ければ、簡単にライセンスの過不足を把握頂けます。

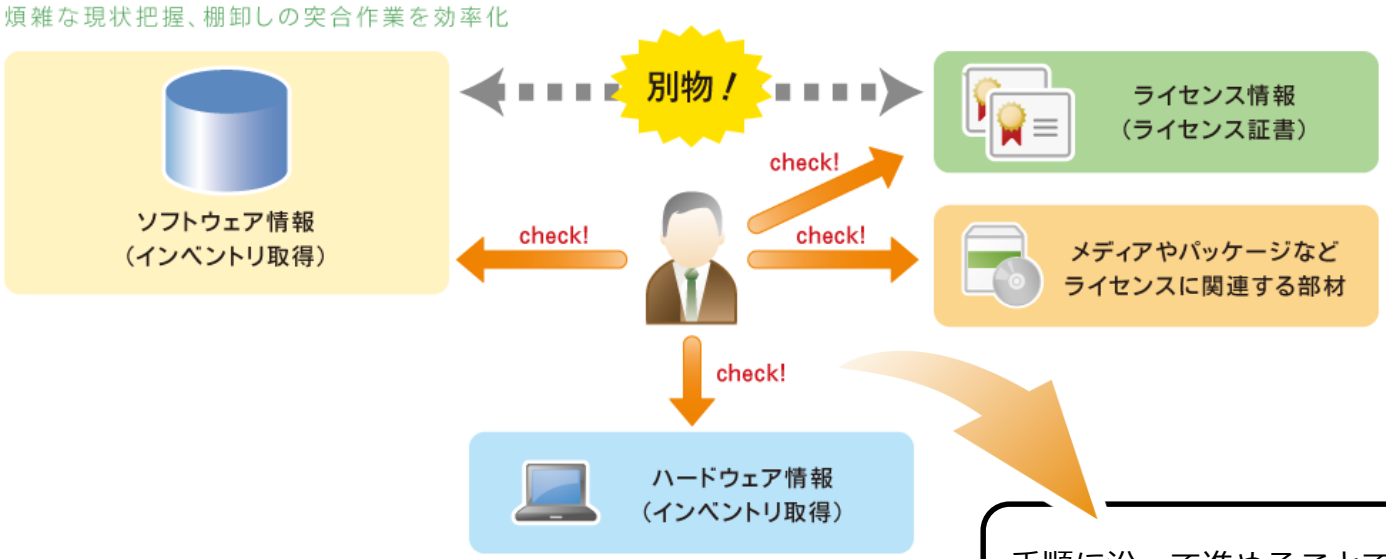


Ver.7

ソフトウェア資産管理（SAM）支援

ソフトウェア資産管理（SAM）実現に向けた現状把握や煩雑な情報の突合作業を効率化します。

組織で利用しているソフトウェアの情報収集、および保有するライセンス情報や部材などの
管理、突合作業を効率化し、SAMに必要とされる4つの台帳作成を支援します。



ポイント

自動収集したインベントリ情報と、お客様が実際に保有しているライセンスの情報は
必ずしも一致しているとは言えません。
SAM実現においては、よく現状把握を行った上で、ハードウェアを含めた情報の突合作
業が必要になります。Protect Anyware2.0ではその煩雑な作業の効率化を支援いたしま
す。

手順に沿って進めることで、以下4つの台帳を効率良く作成できます！

- ハードウェア台帳
- 利用ソフトウェア台帳
- ライセンス台帳
- ライセンス関連部材台帳

自動インストール機能

Protect Anyware 2.0

様々なアプリケーションの
インストールや環境設定を自動化して効率アップ

<こんな課題を解決します>

- ファイル配布やアプリケーションのインストールに多くの時間を費やしている
- インストール時に出てくるウィザード操作が自動化できず困っている
- セキュリティを高めるため、セキュリティパッチを強制適用したいがなかなかできない

さまざまなインストール・環境設定を実現

ウィザード形式で、自動実行タスクを登録しておけば自動的に実行されます。

マクロメーション機能でさらに便利に

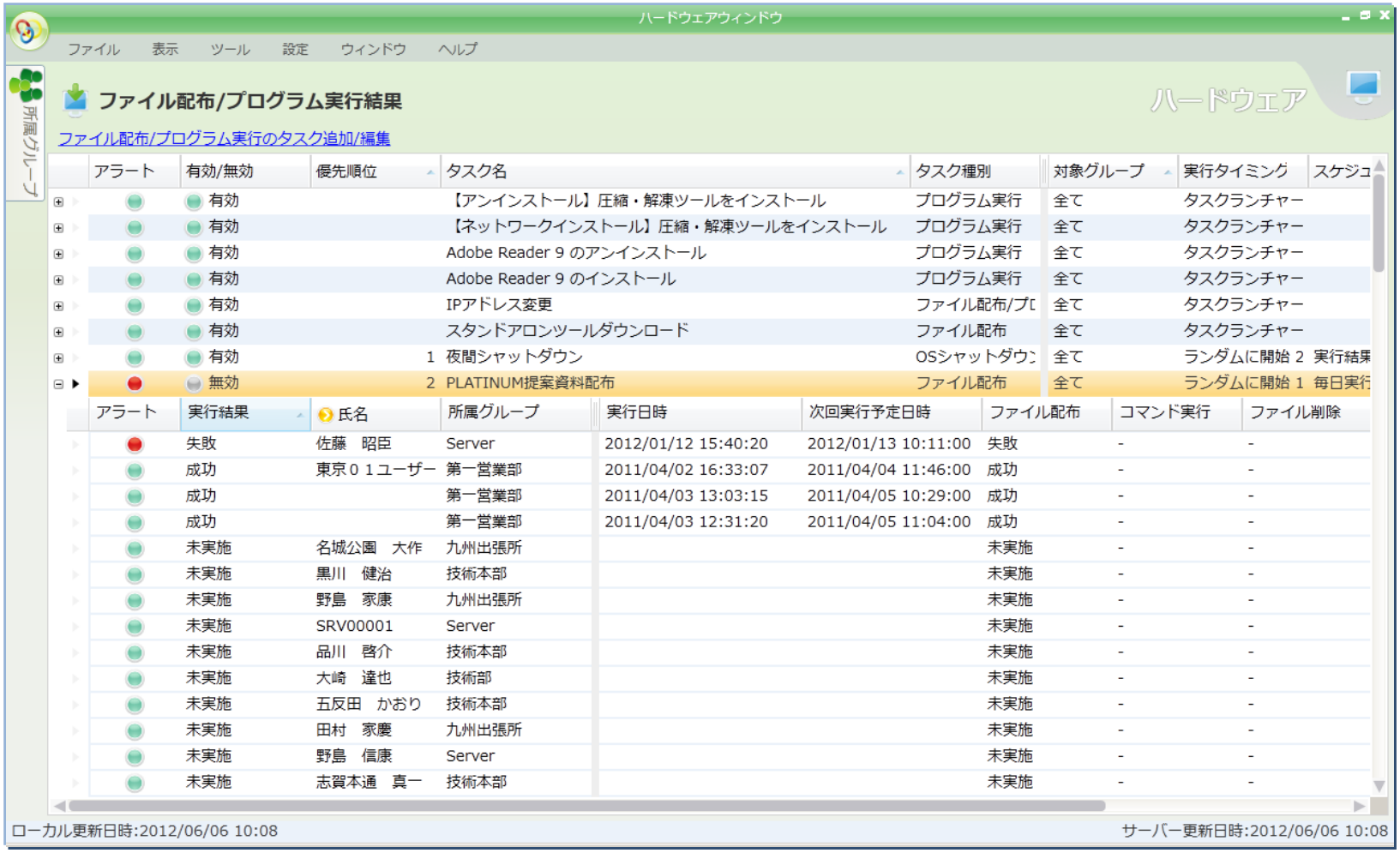
サイレントインストール未対応のソフトのインストールにも対応します。

運用や環境に合わせて細やかな設定が可能

さまざまな項目をタスクの実行条件として設定することができます。

ファイル配布/自動インストール画面

管理者が設定したファイルの配布/インストールプランの一覧から、各端末の実行状況が一目でわかります。もちろん、配布/インストールプラン作成も簡単です。



パッチ適用、ソフトウェアインストール、プリンタードライバインストール、環境設定の変更が可能

マクロメーション機能（端末画面自動操作機能）

管理者端末で操作した内容（インストール手順）を記録し、クライアン側で再現する機能です。
ウィザード形式のインストールなどをクライアント側が操作することなく実行することが可能です。

※再生中はマウス / キーボード操作を受け付けないといった制御も可能！

◆自動インストール
- OSやOfficeのセキュリティパッチ
- 一太郎のパッチ
- 独自アプリケーション
- Adobe Reader
- Java
- 各種ドライバ　など

◆環境設定変更
- IPアドレス変更
- InternetExploreトップページ変更
- プリンタドライバの設定変更　など

作業自動化による効率化＝コスト削減

デバイス制御

Protect Anyware 2.0

デバイスの使用を制御し、情報漏えい対策
申請機能でフレキシブルな運用を支援

<こんな課題を解決します>

- 社内に存在するUSBデバイスを把握できていない
- デバイス使用ルールが守られているか分からない、ルールを徹底できない
- 禁止デバイスの使用を一時的に認める仕組みがないため、業務に支障が出てしまう

USBデバイスの情報を自動収集して管理

収集した情報をもとに、インポート／エクスポートで一括設定で導入時の作業も軽減。

情報漏えい経路となりうるデバイスを制御

CD/DVD、FD、共有フォルダ―もグループごとに制御できます。

申請機能で業務を妨げないフレキシブルな運用を支援

通常ポリシーの他、ユーザー申請／所属管理者承認による一時ポリシーの適用が可能。

USBメモリによるPC使用制限

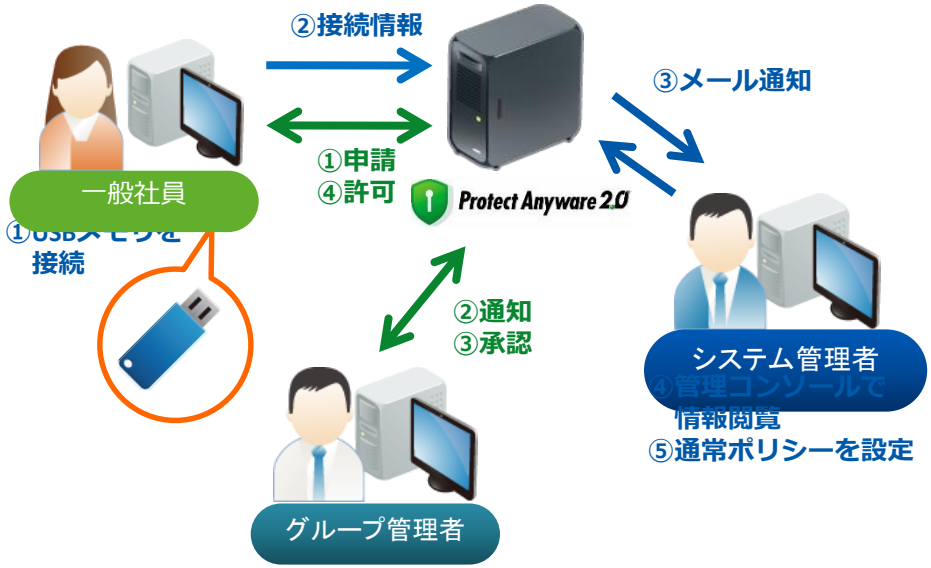
デバイス制御機能

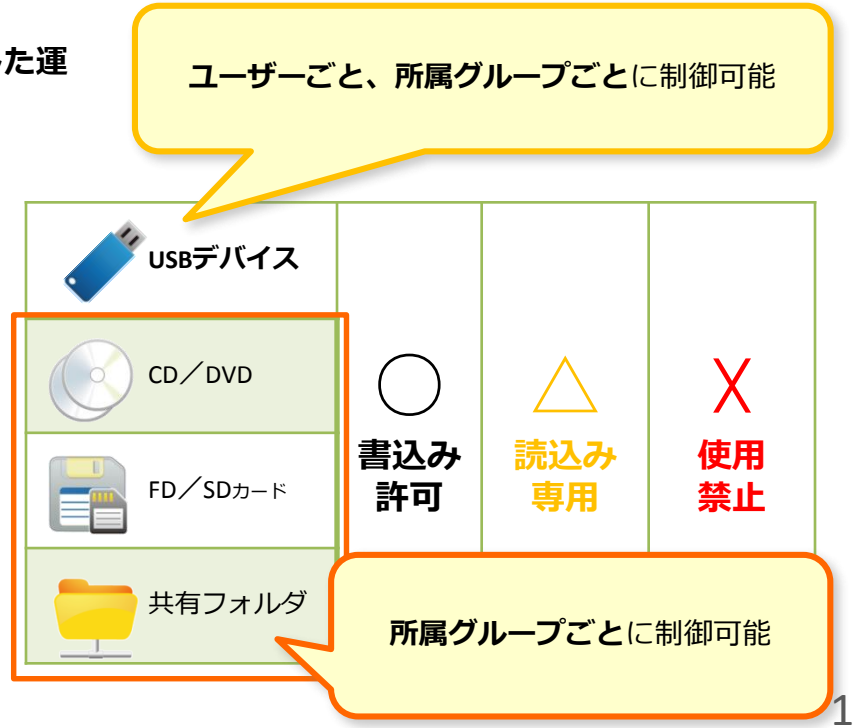
こんなことで お困りの方に

- ✓ 社内で使われているUSBメモリを管理したい
- ✓ 外部デバイスの利用ポリシーが守られているか心配
- ✓ USBメモリは業務に必要な場合だけ使わせたい

USBメモリによる情報漏洩対策を強化

例 **通常の運用ポリシーとは異なる「一時ポリシー」を適用した運用**





iPhone/iPad ポータブルデバイス個体識別制御

- **iPhone/iPad 等のポータブルデバイスを識別し、PCへの接続制御ができます。**
- **例えば、社内所有のポータブルデバイスのPCへの接続のみを許可し、個人所有の接続は禁止する運用ができます。**
- **個体ごとに識別制御ができますので、お客様のポリシーにあわせた運用を実現！**

NEW

<ポータブルデバイスの情報を自動収集>

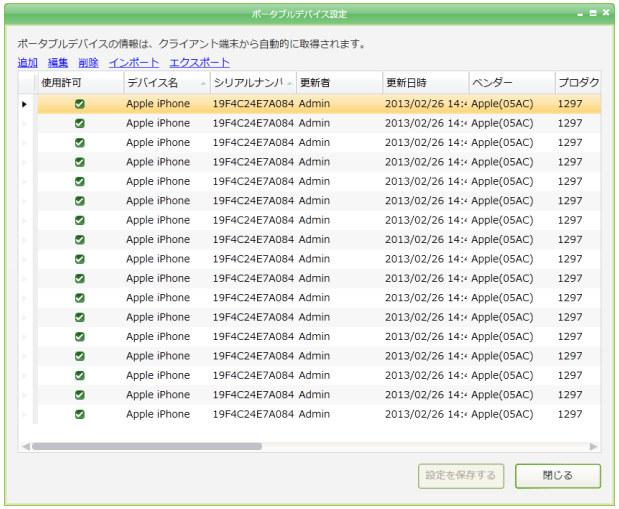
USBデバイスと同様に、以下の値を取得して個体識別します。

- ベンダー
- プロダクトID
- シリアルナンバー（※UDID）

※iPhone/iPadの場合のみ

<管理コンソールから使用許可設定>

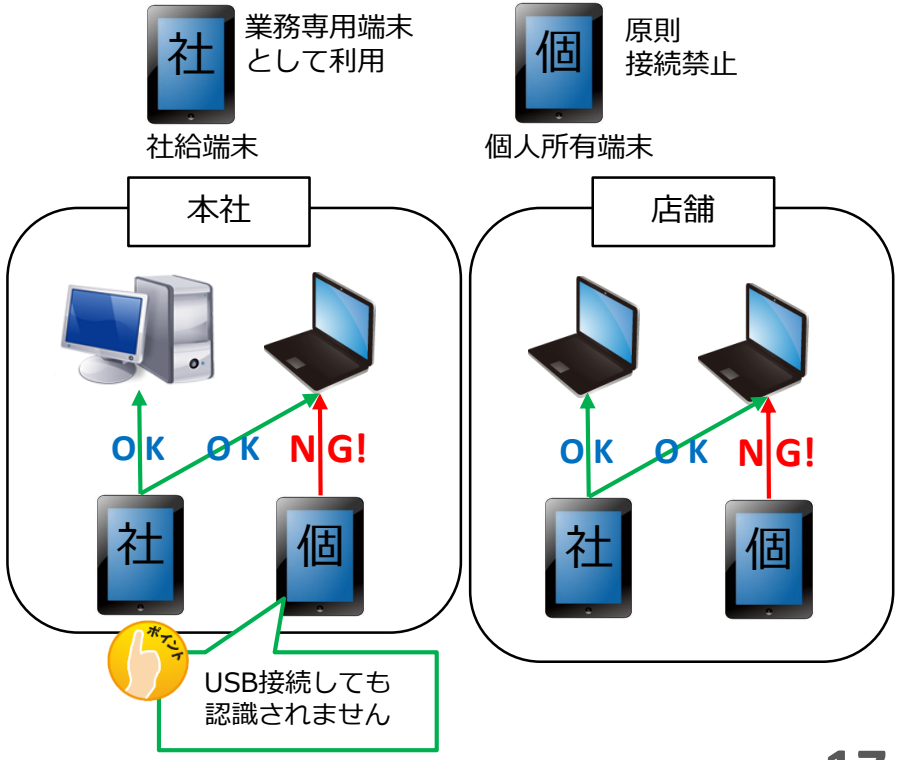
使用許可するポータブルデバイスはチェックを入れる操作のみ。



※新規に導入されるポータブルデバイスは『未定義』の設定が反映されます。

例

業種：スーパー業界　A社
要件：社給 iPadの接続は許可し、
それ以外のiPad（個人所有端末）は認識させない



PC操作ログ管理

Protect Anyware 2.0

クライアント端末の操作ログを取得し、
アラートで効率的に把握、詳細情報を追跡します。

<こんな課題を解決します>

- 業務外の利用や、内部不正に繋がる操作を禁止したい
- ファイル操作やアプリケーションの利用状況を把握できていない
- 社内のPC利用モラルやセキュリティリテラシーを高める必要がある

操作ログの検索・追跡も可能

詳細な条件設定から素早く特定ファイルを検索し、その遷移を確認できます。

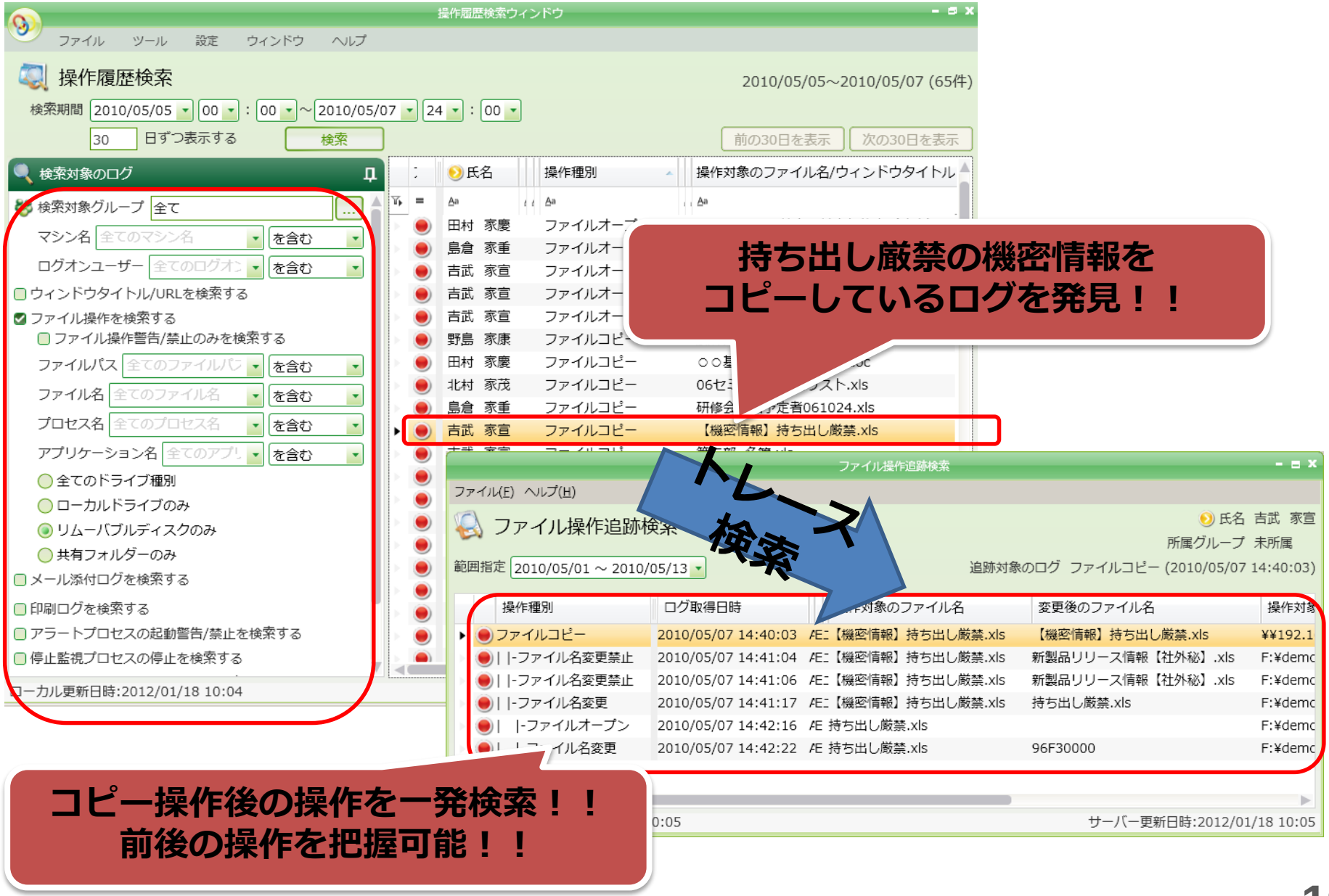
不正操作を警告・禁止でセキュリティ強化

あらかじめ設定した不正操作を禁止し、警告メッセージを表示することができます。

クライアント端末の稼働状況を視覚的に把握

時間帯ごとのクライアント端末の稼働状況を色分けしたグラフで表示することができます。

ログ管理：収集したログのトレース機能



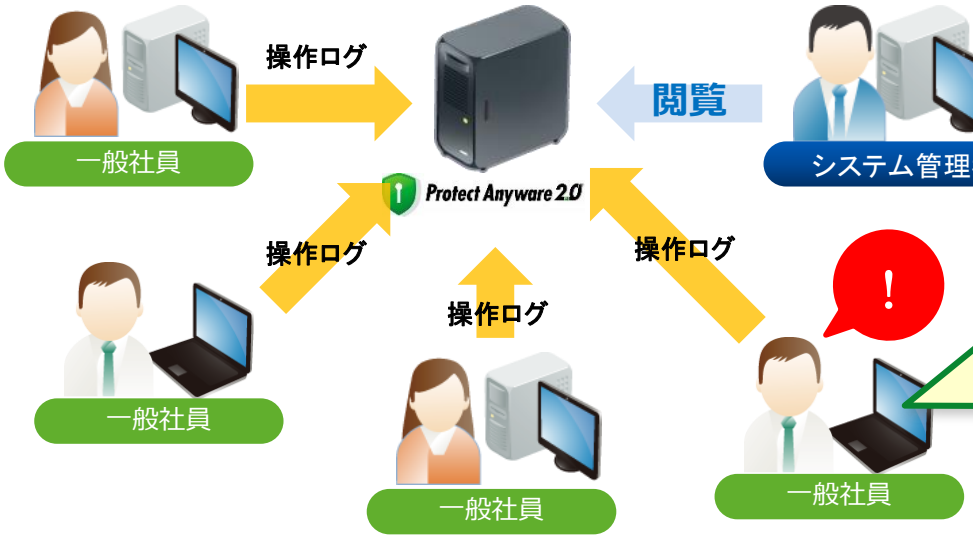
機能対応表への対応

PC操作ログ管理

こんなことで お困りの方に

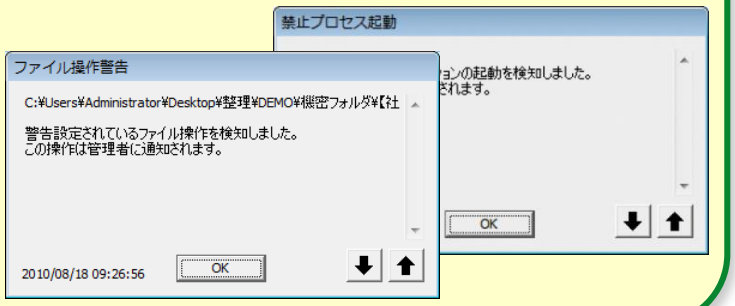
- ✓ セキュリティインシデント時に必要なログを取得したい
- ✓ セキュリティリスクのある操作をさせたくない
- ✓ 社内のモラルやセキュリティリテラシーを高めたい

IT統制に必要な操作ログを取得、制御により不正操作を防止



操作ログを 効率的に把握、 検索、追跡が可能

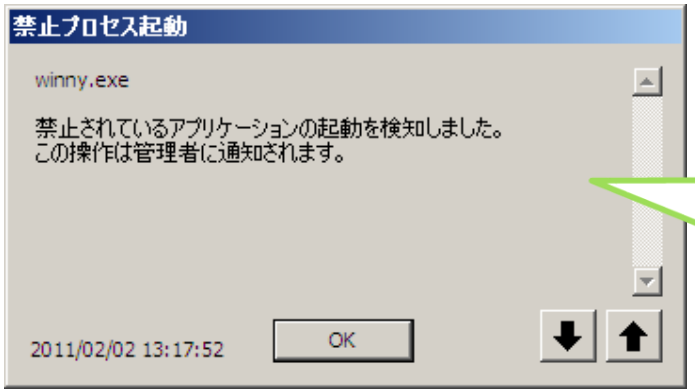
不正操作禁止・警告で問題を未然に解決



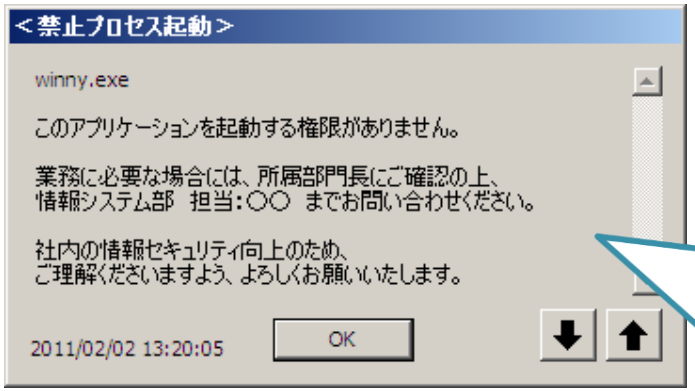
ログ管理：アラート機能

PC操作ログ機能の活用 実際の操作に基づいた警告が有効

実際に行われようとしたポリシー違反の操作を禁止して
セキュリティを強化するだけでなく、
警告メッセージを表示させることで、社員教育にも活用できます。



初期設定の
メッセージ



社内ルールを周知する
内容を含めた
**オリジナル
メッセージ**

操作ログ取得は
こんな効果も！

- **不正操作の抑制**
- **業務効率化**

個人情報検索

Protect Anyware 2.0

個人情報をファイルの中まで検索、棚卸しして
情報漏洩のリスク管理を実現

＜こんな課題を解決します＞

●情報漏洩したら困る重要ファイルを棚卸し、情報資産のリスク管理を始める必要がある

●社内のセキュリティポリシー、ルールが守られているか確認、徹底できない

個人情報を含むファイルを検出

設定した定義をもとに、ファイル内部までチェックして検出します。

キーワードで機密情報ファイルを定義

「社外秘」「機密ファイル」など重要キーワードで定義づけして検索することも可能です。

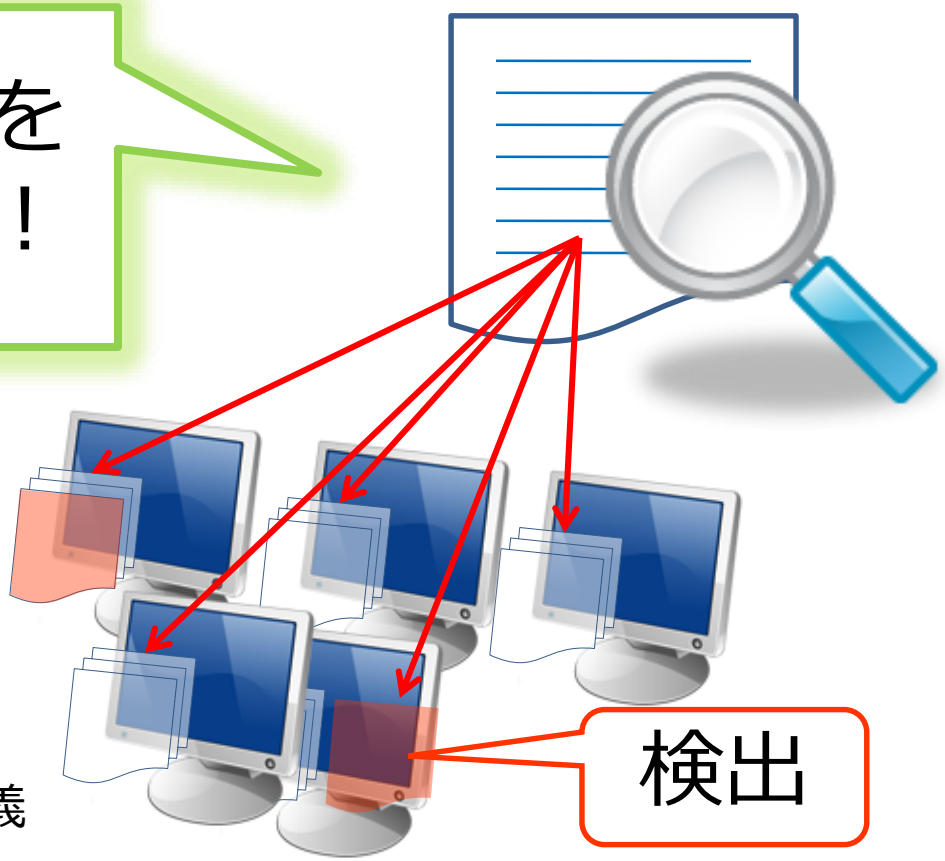
個人情報の監査で法令順守

社内ルールが守られているかの確認や、社員のセキュリティ意識向上にも活用できます。

個人情報検索

個人情報をファイルの中まで検索、棚卸しして
情報漏洩のリスク管理を実現

ファイルの中身を
チェックします！

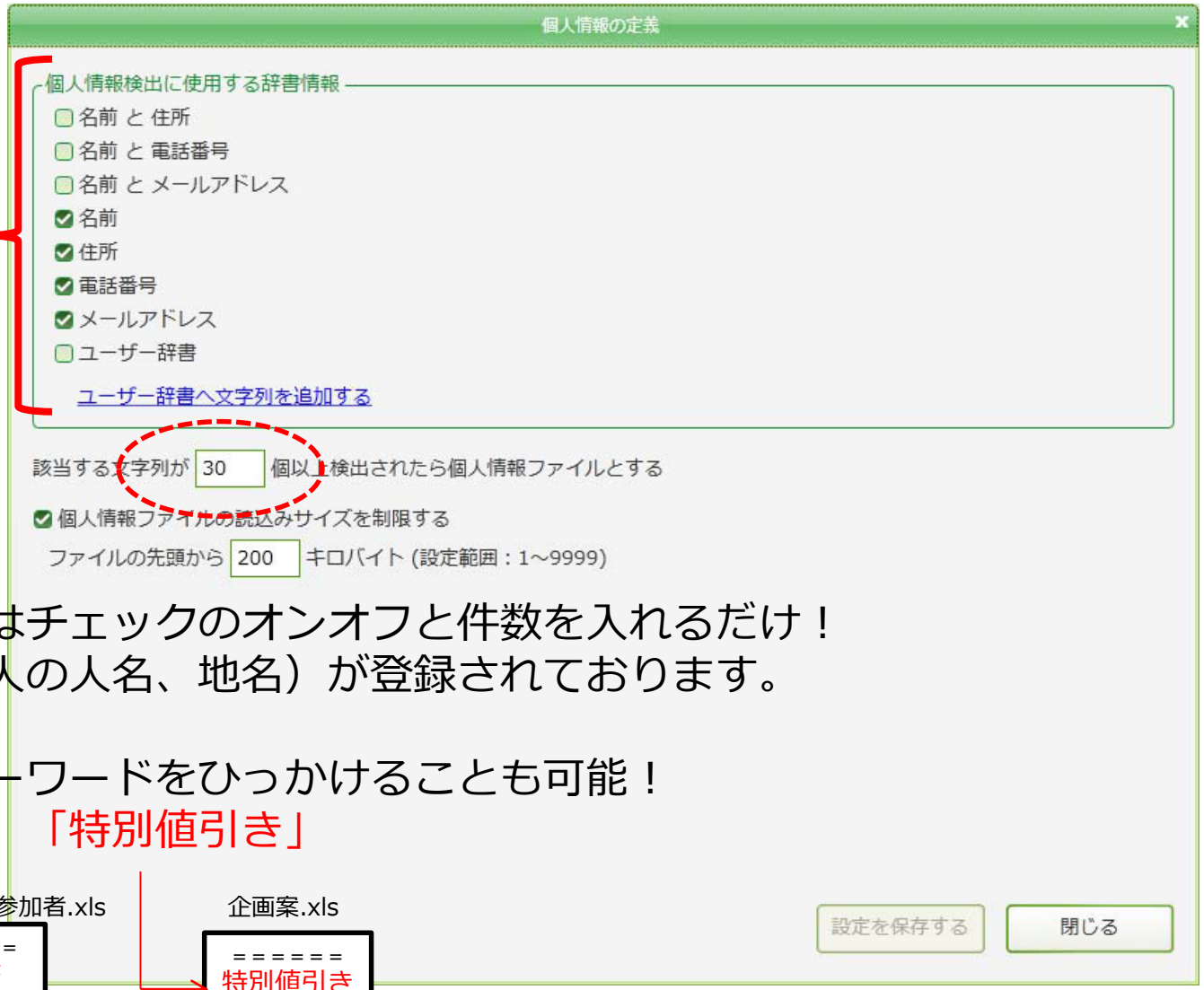


- 名前+電話番号
- 名前+住所
- 名前+メールアドレス

などで個人情報を定義

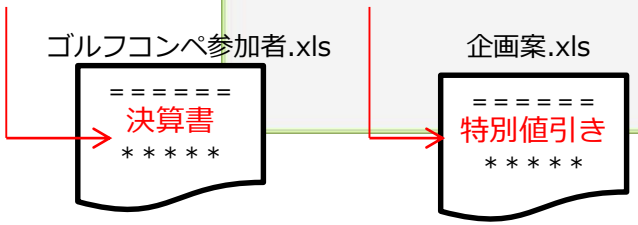
個人情報の設定方法

チェックのオンオフ



個人情報の定義はチェックのオンオフと件数を入れるだけ！
辞書機能（日本人の人名、地名）が登録されております。

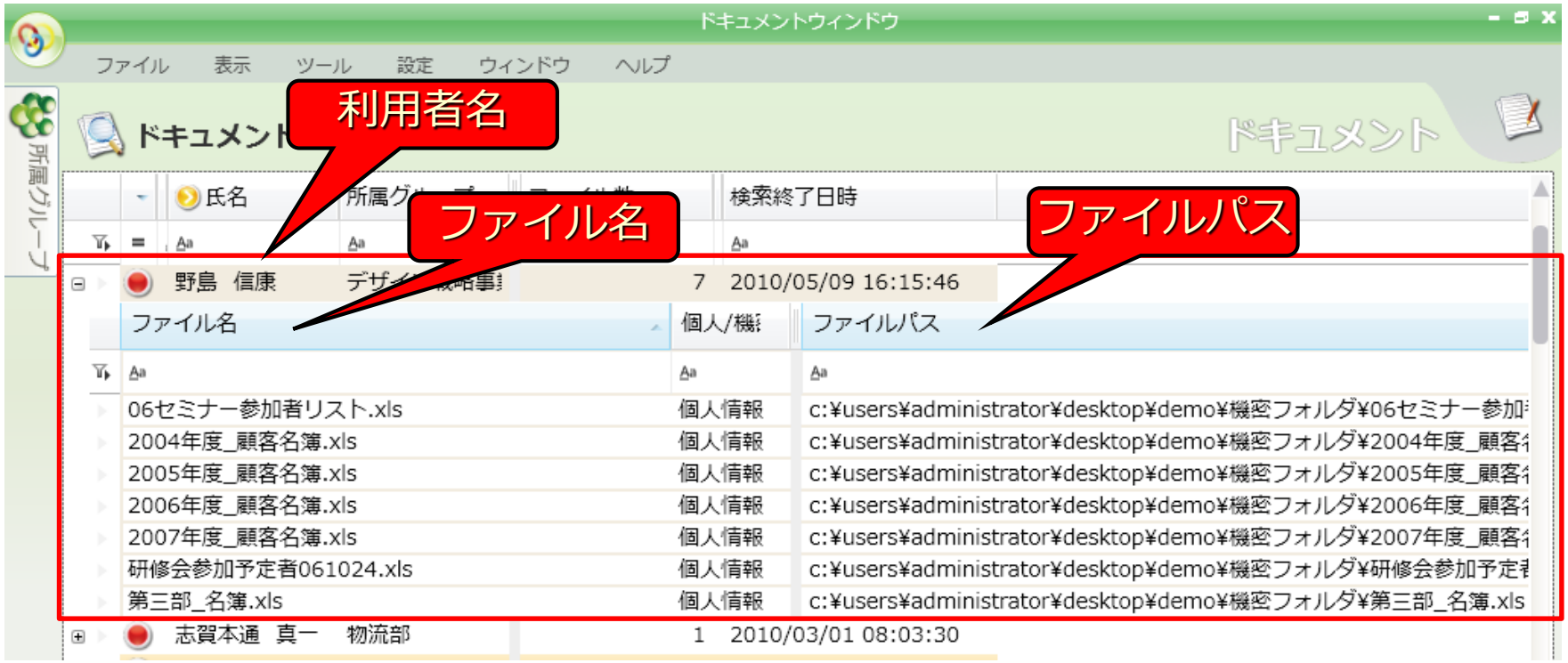
任意のフリーキーワードをひっかけることも可能！
例：「決算書」　「特別値引き」



個人情報／機密情報ファイルの棚卸し

検索結果画面

●**クライアントPC内に存在する個人情報/機密情報ファイルを見つけ出します。**
取得ログ：ファイル名、ファイルパス、ファイルサイズ、ファイル作成日時、ファイル更新日時



誰が、どこに、個人情報を持っているか一目瞭然！！

不正PC遮断

Protect Anyware 2.0

管理されていないコンピューターを検知・遮断し、
社内のネットワークを安全に保ちます。

<こんな課題を解決します>

- 管理されていないコンピューターからの情報漏洩、ウイルス感染を防ぐ必要がある
- 管理対象外になっている社内のコンピューターがわからない
- ネットワーク機器もクライアント端末と一緒に管理できなくて困っている

ソフトウェアによる遮断を実現

専用の機器をなしで、不許可コンピュータの接続を排除できます。

IT統合管理の徹底に活用

管理対象外コンピューターの発見により管理を徹底し、社内セキュリティを高めます。

ネットワーク機器の自動登録が可能

MACアドレス認証により、接続されたネットワーク機器を検知して自動的に登録できます。

不正PC遮断・検知

●管理対象外のコンピューターによる情報漏洩を防ぎ、ウイルス感染から社内ネットワークを守ります。
●「これから管理するべきコンピューター」を発見し、管理を徹底できます。

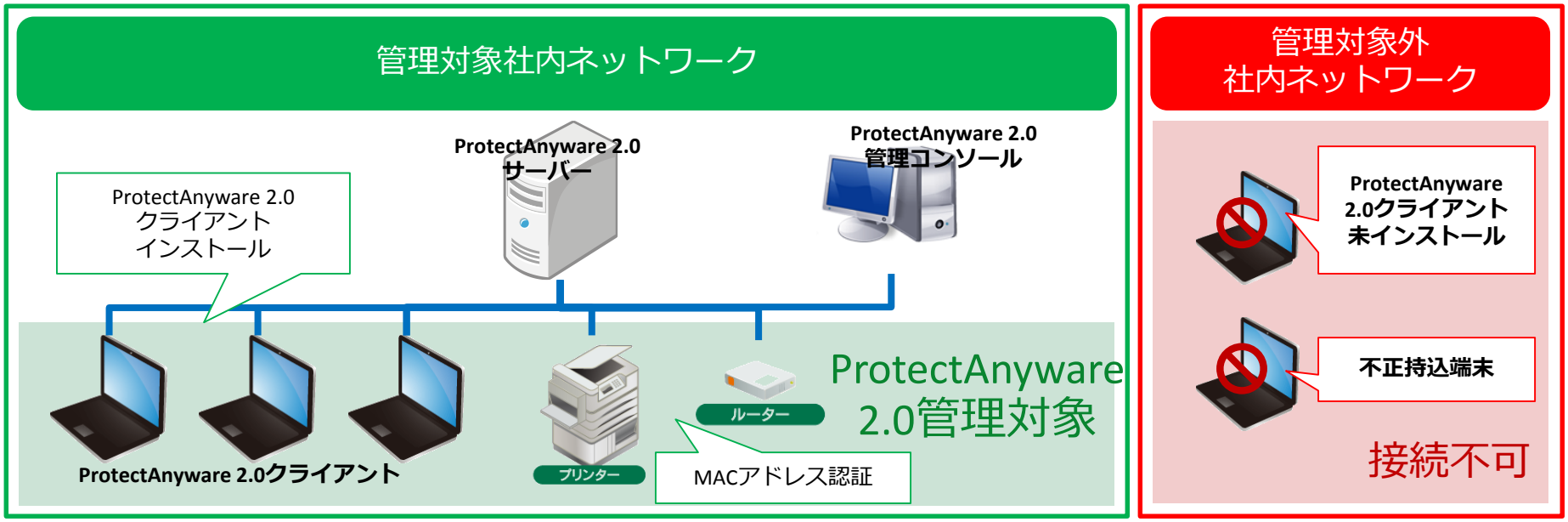
<ソフトウェアによる遮断を実現>

クライアントのインストール認証、MACアドレス認証により、社内ネットワークへの接続を検知し、許可していないコンピューターの接続を遮断します。

※Protect Anyware2.0の機能が有効になっているクライアント端末が同一セグメント内を監視し、検知・遮断する役割を担います。

<ネットワーク機器の自動追加が可能>

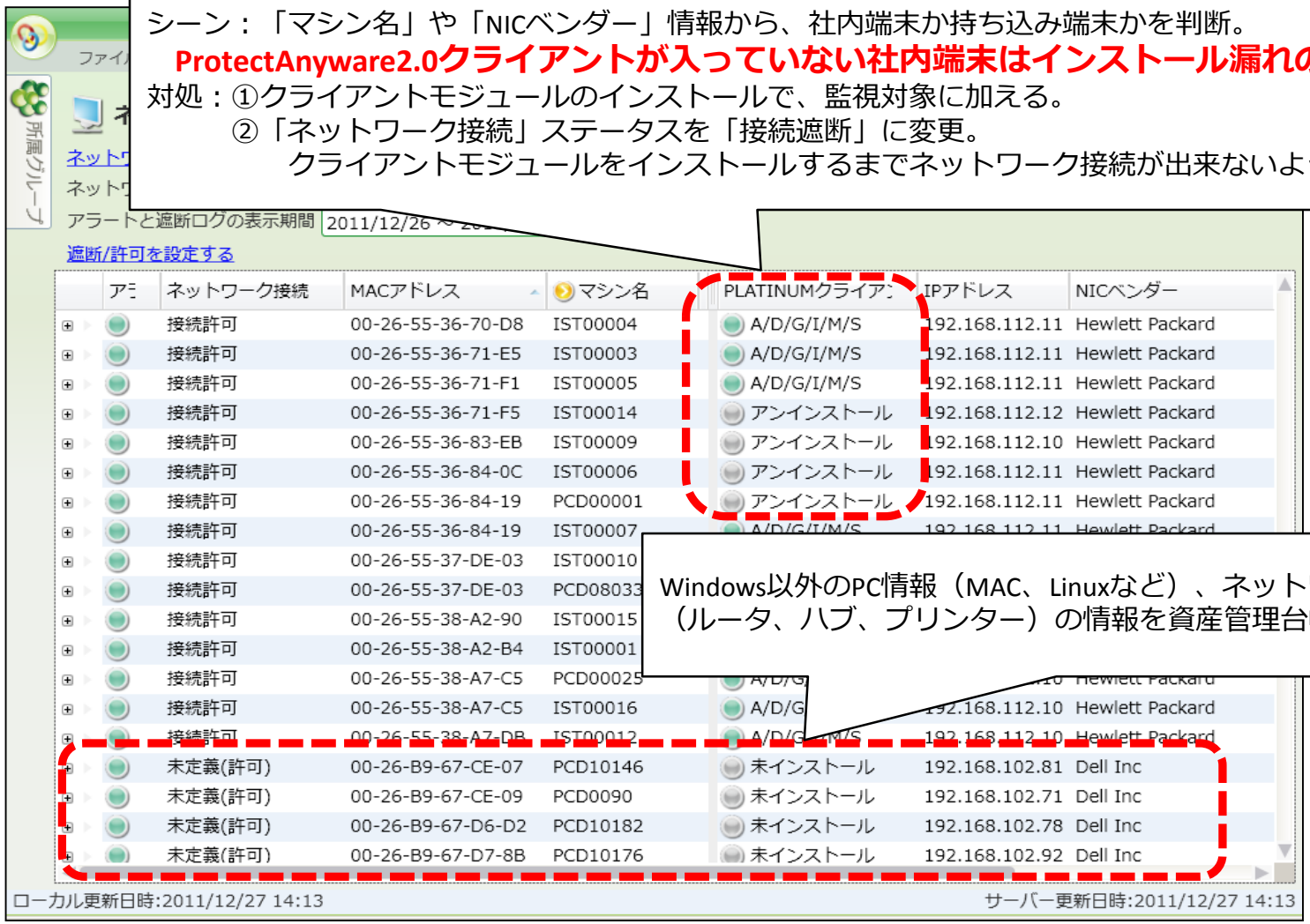
クライアントがインストールできないコンピューター（対象外OSなど）やMACアドレスを持つネットワークプリンターなどのネットワーク機器を検知し、自動的に追加します。これらの機器はProtectAnyware 2.0クライアントと同様に管理コンソール上で管理できます。



不正端末の洗い出し

資産管理情報とネットワーク接続端末情報を突き合わせ出来るため、
不正端末の洗い出しが簡単。

シーン：「マシン名」や「NICベンダー」情報から、社内端末か持ち込み端末かを判断。
ProtectAnyware2.0クライアントが入っていない社内端末はインストール漏れの可能性大！！
対処：①クライアントモジュールのインストールで、監視対象に加える。
②「ネットワーク接続」ステータスを「接続遮断」に変更。
クライアントモジュールをインストールするまでネットワーク接続が出来ないように設定。



ネットワーク接続	MACアドレス	マシン名	PLATINUMクライアン	IPアドレス	NICベンダー
接続許可	00-26-55-36-70-D8	IST00004	A/D/G/I/M/S	192.168.112.11	Hewlett Packard
接続許可	00-26-55-36-71-E5	IST00003	A/D/G/I/M/S	192.168.112.11	Hewlett Packard
接続許可	00-26-55-36-71-F1	IST00005	A/D/G/I/M/S	192.168.112.11	Hewlett Packard
接続許可	00-26-55-36-71-F5	IST00014	アンインストール	192.168.112.12	Hewlett Packard
接続許可	00-26-55-36-83-EB	IST00009	アンインストール	192.168.112.10	Hewlett Packard
接続許可	00-26-55-36-84-0C	IST00006	アンインストール	192.168.112.11	Hewlett Packard
接続許可	00-26-55-36-84-19	PCD00001	アンインストール	192.168.112.11	Hewlett Packard
接続許可	00-26-55-36-84-19	IST00007			
接続許可	00-26-55-37-DE-03	IST00010			
接続許可	00-26-55-37-DE-03	PCD08033			
接続許可	00-26-55-38-A2-90	IST00015			
接続許可	00-26-55-38-A2-B4	IST00001			
接続許可	00-26-55-38-A7-C5	PCD00025			
接続許可	00-26-55-38-A7-C5	IST00016	A/D/G	192.168.112.10	Hewlett Packard
接続許可	00-26-55-38-A7-DB	IST00012			
未定義(許可)	00-26-B9-67-CE-07	PCD10146	未インストール	192.168.102.81	Dell Inc
未定義(許可)	00-26-B9-67-CE-09	PCD0090	未インストール	192.168.102.71	Dell Inc
未定義(許可)	00-26-B9-67-D6-D2	PCD10182	未インストール	192.168.102.78	Dell Inc
未定義(許可)	00-26-B9-67-D7-8B	PCD10176	未インストール	192.168.102.92	Dell Inc

Windows以外のPC情報（MAC、Linuxなど）、ネットワーク機器
（ルータ、ハブ、プリンター）の情報を資産管理台帳に取り込み可能。

リモートコンソール

Protect Anyware 2.0

遠隔地のクライアント端末をリモート操作。
メンテナンス・ヘルプデスク業務をサポートします。

<こんな課題を解決します>

●ヘルプデスク業務の効率化を図りたい

●遠隔地へのサポートに出向く時間・コストを削減しなくてはならない

コンソール画面からPush型アクションを実行

かんたん操作でコマンド実行、メッセージ送信、インストールなども可能です。

複数台同時接続・監視

管理端末から複数台のクライアント端末への同時接続・監視を実現しました。

ファイル認証でセキュリティを確保

暗号化された証明書ファイルでの認証を行うので安心して接続できます。

リモートコンソール

●管理端末から、遠隔地のクライアント端末にリモート接続し、直接操作が可能です。
●リモートKVM機能との併用で、メンテナンス・ヘルプデスク業務をより効率的に行えます。

<クライアント端末一覧からかんたんに接続>

※RemoteConsole専用画面からアクションを実行できます。

- 開始／接続停止
- プログラム実行
- シャットダウン
- メッセージ送信
- 動作確認

複数台同時接続もできます。

<インテル®vPro™との連携でさらに便利に！>

リモートKVM機能に対応しており、クライアント端末の電源が入っていなかったり、OSが起動できずブルースクリーンや、BIOS設定画面であっても、リモート接続が可能です。これまでオンサイトやセンドバックでしか対応できなかったトラブルにも対応可能になります。

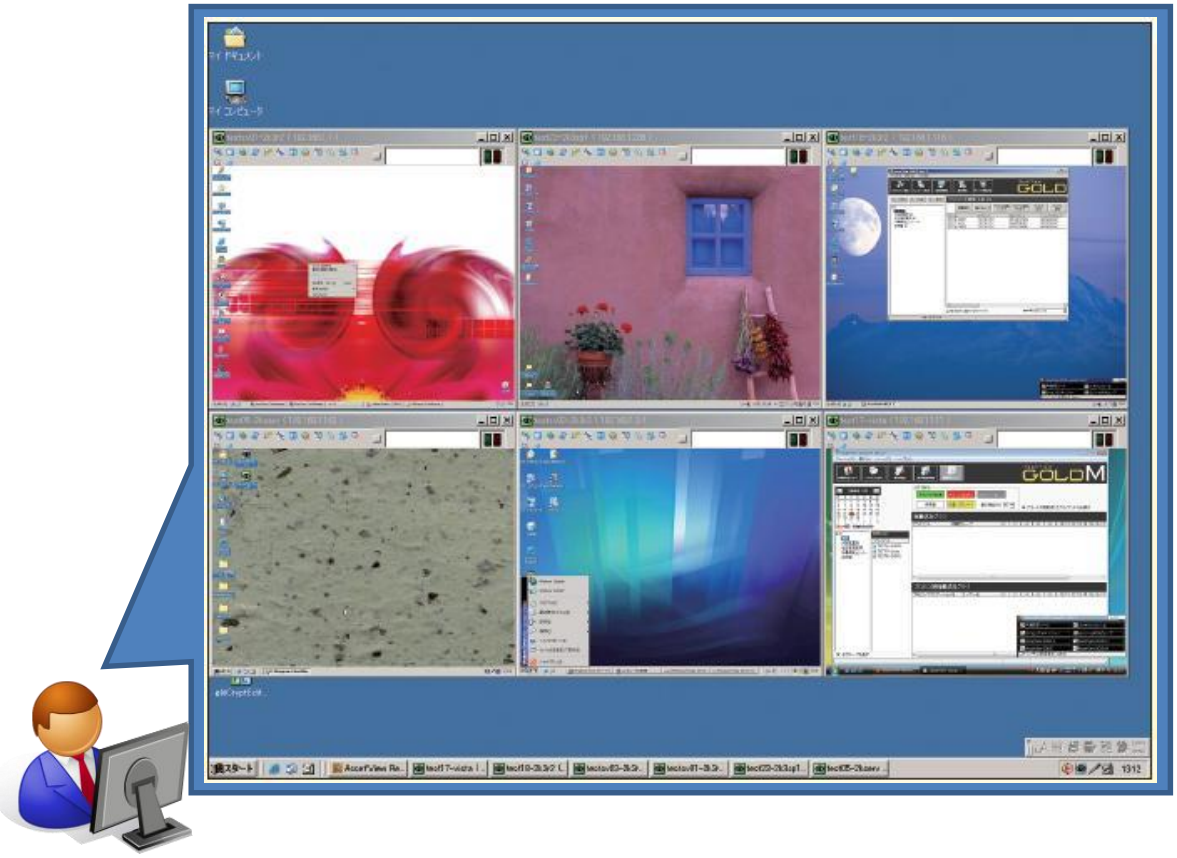
出張コスト削減！トラブル解決までの時間短縮！

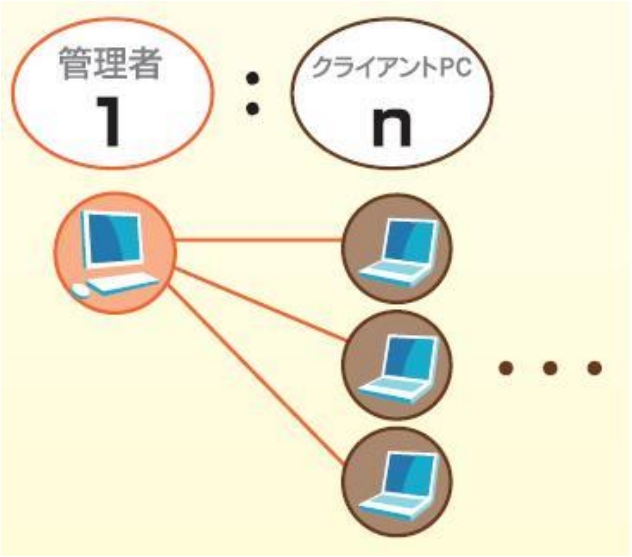
<暗号化させた証明書ファイル認証>

RemoteConsoleは、専用の暗号化された証明書ファイルが管理端末とクライアント端末間で一致した場合のみ、Push型アクションができるようになります。

リモコン機能

管理機から複数台のクライアントPCへ同時接続・監視を実現！





複数同時接続・操作が可能のため
インストール進捗状況など、
リアルタイムで把握、
作業の効率化を図る事が可能です。

遠隔操作業務の効率化を実現！

サーバースペック

■サーバースペック(データベースサーバー、アプリケーションサーバー共通事項)

OS	Microsoft Windows Server 2003 SP2
	Microsoft Windows Server 2003 R2 SP2
	Microsoft Windows Server 2008 SP1/SP2
	Microsoft Windows Server 2008 R2 SPなし/SP1
	Microsoft Windows Server 2012
	※ .NET Framework 3.5 SP1以降がインストールされている必要があります。
	※ 以下のOSは64Bit版では動作保証していません。 Microsoft Windows Server 2003 Microsoft Windows Server 2003 R2 Microsoft Windows Server 2008
	※ 対象OSは日本語版Windowsのみです。
	※ アップグレードしたOSでは動作保証しておりません。
CPU	OS推奨値以上
	推奨：クアッドコア Intel Xeon 2.33GHz同等以上
メモリ	OS推奨値以上
	推奨： 4GB以上

サーバースペック

■データベースサーバー注意事項

OS	※ Microsoft Excel 2003以降がインストールされている必要があります。
HDD容量	データベースサーバーのインストールには、システムドライブに30MB以上の空き容量が必要です。
	データベースファイルの配置先となるドライブと、バックアップデータの配置先となるドライブは、十分な空き容量のあるシステムドライブ以外のローカルドライブを指定されることを推奨します。
データベース	Microsoft SQL Server 2005 SP3/SP4 Standard Edition
	Microsoft SQL Server 2005 SP3/SP4 Enterprise Edition
	Microsoft SQL Server 2008 SP1/SP2 Standard
	Microsoft SQL Server 2008 SP1/SP2 Enterprise
	Microsoft SQL Server 2008 R2 SP1/SP2 Express
	Microsoft SQL Server 2008 R2 SP1/SP2 Standard
	Microsoft SQL Server 2008 R2 SP1/SP2 Enterprise
	Microsoft SQL Server 2012 SPなし/SP1 Express
	Microsoft SQL Server 2012 SPなし/SP1 Standard
	Microsoft SQL Server 2012 SPなし/SP1 Enterprise
	※Microsoft SQL Server 2005、Microsoft SQL Server 2008は64Bit版には非対応です。

■アプリケーションサーバー注意事項

HDD容量	アプリケーションサーバーのインストールには、システムドライブに150MB以上の空き容量が必要です。
	ProtectAnyware 2.0フォルダの配置先となるドライブは、システムドライブ以外の十分な空き容量のあるローカルドライブを指定されることを推奨します。

■管理コンソール

管理コンソールPCスペック

OS	Microsoft Windows Server 2003 SP2
	Microsoft Windows Server 2003 R2 SP2
	Microsoft Windows Vista Business SP1/SP2
	Microsoft Windows Vista Ultimate SP1/SP2
	Microsoft Windows Vista Enterprise SP1/SP2
	Microsoft Windows Server 2008 SP1/SP2
	Microsoft Windows Server 2008 R2 SPなし/SP1
	Microsoft Windows 7 Professional SPなし/SP1
	Microsoft Windows 7 Ultimate SPなし/SP1
	Microsoft Windows 7 Enterprise SPなし/SP1
	Microsoft Windows 8 Pro
	Microsoft Windows 8 Enterprise
	Microsoft Windows Server 2012
	※ .NET Framework 4がインストールされている必要があります。 .NET Framework 4の更新プログラム KB2468871v2を適用してください。
	※ Microsoft Excel 2003以降がインストールされている必要があります。
	※ 以下のOSは64Bit版では動作保証していません。 Microsoft Windows Vista / Server 2003 / Server 2003 R2 / Server 2008
	※ 対象OSは日本語版Windowsのみです。
	※ アップグレードしたOSでは動作保証しておりません。
CPU	OS推奨値以上
	推奨： 2GHz 以上
メモリ	OS推奨値以上
	推奨：4GB以上
HDD容量	管理コンソールのインストールには、システムドライブに650MB以上の空き容量が必要です。
ディスプレイ	1024×768以上の画面解像度で運用してください。

クライアントPCスペック

■ProtectAnyware 2.0クライアント

OS	Microsoft Windows 2000 Server SP4
	Microsoft Windows 2000 Professional SP4
	Microsoft Windows Server 2003 SP1/SP2
	Microsoft Windows Server 2003 R2 SP1/SP2
	Microsoft Windows Vista Business SP1/SP2
	Microsoft Windows Vista Ultimate SP1/SP2
	Microsoft Windows Vista Enterprise SP1/SP2
	Microsoft Windows Server 2008 SP1/SP2
	Microsoft Windows 7 Professional SPなし/SP1
	Microsoft Windows 7 Ultimate SPなし/SP1
	Microsoft Windows 7 Enterprise SPなし/SP1
	Microsoft Windows 8 Pro
	Microsoft Windows 8 Enterprise
	Microsoft Windows Server 2012
	※ 以下のOSは64Bit版では動作保証していません。 Microsoft Windows Vista / Server 2008
	※ 対象OSは日本語版Windowsのみです。
	※ アップグレードしたOSでは動作保証しておりません。
	※ Windows 2000 Professional/Serverでは、『Windows2000 SP4対応の更新プログラム ロールアップ1』が適用されている必要があります。
CPU	OS推奨値以上
メモリ	OS推奨値以上
	※ ProtectAnyware 2.0クライアントが動作するに十分なメモリ容量が必要です。
	※他のアプリケーションが動作している環境などで、メモリの空き容量が極端に少ない場合は、OSの動作が極端に遅くなる可能性があります。
HDD容量	ProtectAnyware 2.0クライアントのインストールには、システムドライブに120MB以上の空き容量が必要です。
	※導入製品や運用方法によって異なります。

商品ライセンス体系

■ProtectAnyware2.0

商品コード	商品名	定価価格	備考
CV787001	ProtectAnyware 2.0 ver7 10User JSWSP 1年付	OPEN価格	
CV787005	ProtectAnyware 2.0 ver7 50User JSWSP 1年付	OPEN価格	
CV787010	ProtectAnyware 2.0 ver7 100User JSWSP 1年付	OPEN価格	
CV787020	ProtectAnyware 2.0 ver7 200User JSWSP 1年付	OPEN価格	
CV787030	ProtectAnyware 2.0 ver7 300User JSWSP 1年付	OPEN価格	
CV787040	ProtectAnyware 2.0 ver7 400User JSWSP 1年付	OPEN価格	
CV787050	ProtectAnyware 2.0 ver7 500User JSWSP 1年付	OPEN価格	
CV787100	ProtectAnyware 2.0 ver7 1,000User JSWSP 1年付	OPEN価格	
CV787200	ProtectAnyware 2.0 ver7 2,000User JSWSP 1年付	OPEN価格	
CV787300	ProtectAnyware 2.0 ver7 3,000User JSWSP 1年付	OPEN価格	

■ファイル制御・暗号化(K)オプション機能

商品コード	商品名	定価価格	備考
CV78K001	ProtectAnyware 2.0 Kオプション 10User JSWSP 1年付	OPEN価格	
CV78K005	ProtectAnyware 2.0 Kオプション 50User JSWSP 1年付	OPEN価格	
CV78K010	ProtectAnyware 2.0 Kオプション 100User JSWSP 1年付	OPEN価格	
CV78K020	ProtectAnyware 2.0 Kオプション 200User JSWSP 1年付	OPEN価格	
CV78K030	ProtectAnyware 2.0 Kオプション 300User JSWSP 1年付	OPEN価格	
CV78K040	ProtectAnyware 2.0 Kオプション 400User JSWSP 1年付	OPEN価格	
CV78K050	ProtectAnyware 2.0 Kオプション 500User JSWSP 1年付	OPEN価格	
CV78K100	ProtectAnyware 2.0 Kオプション 1,000User JSWSP 1年付	OPEN価格	
CV78K200	ProtectAnyware 2.0 Kオプション 2,000User JSWSP 1年付	OPEN価格	
CV78K300	ProtectAnyware 2.0 Kオプション 3,000User JSWSP 1年付	OPEN価格	

*1年間の「JBソフトウェアサポートパック（JSWSP）」が付いています。
*ライセンスはクライアント課金となり、サーバーライセンスはフリーです。
*別途Microsoft SQL Serverプロセッサライセンス、Microsoft Excelライセンスが必要です。

ＪＢソフトウェア サポートサービス(JSWSP)

JBソフトウェア サポートサービス

1. バージョンアップ　サービス

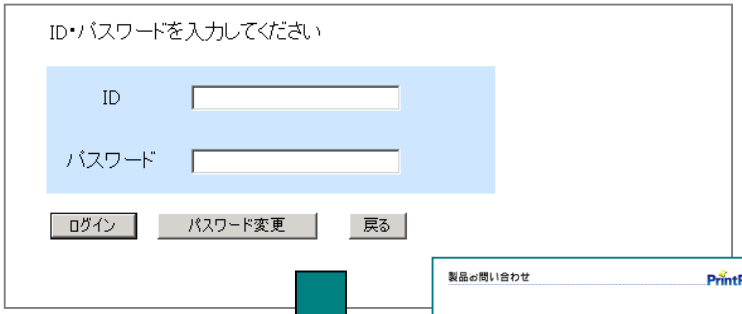
・最新のプログラムをご提供します。

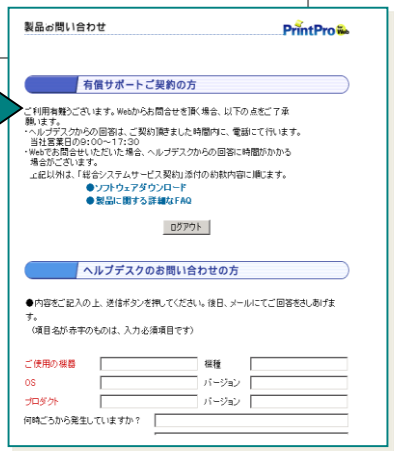
製品コンセプト変更、アーキテクチャー変更などによる次期製品へのアップグレードは除きます。

2. ヘルプデスク　サービス

・操作に関する質問、技術的な質問、問題切り分けに関する質問に対するメールでの回答

お客様専用IDにてWebサイトからログインすることで、ご利用可能です。





・Webでの受付時間
　365日24時間
※回答などの対応時間は、
　月－金 9:00～17:00となります。

補　足

ProtectAnywa2.0　Ver.7について

Ver.7での新機能

分類	追加機能	概　　要
IT資産管理　A	死活監視機能	ネットワーク機器の死活監視
	ライセンス管理機能の強化	
	アプリケーション情報取得範囲の拡張	Windowsストアアプリの情報取得
アプリケーション配布 D	自動インストール/アンインストールスクリプトの提供	作業を自動化するスクリプトの作成
PC操作ログ管理 M	スマートフォン経由でのファイル流出対策の強化	
	簡易Webフィルタリング	
	Windowsストアアプリログの取得	
	Google Apps操作ログの取得	
デバイス制御 G	デバイス制御の強化	Bluetooth接続の制御
	Active Directory連携のデバイス制御	ユーザー単位でのデバイス制御
	特権ユーザー機能	デバイス制御の影響を受けないユーザー定義
	メディア個体識別でのデバイス制御	USBデバイス、SDカード、MOを個別制御

なぜ、ファイルが流出した後に消せるのか？

Protect Anyware 2.0

① **暗号化時に制御情報を保管**
いつでも設定変更が可能。

④ **復号化時に認証状況を確認**
操作ログを保存。

ファイル暗号化
クラウドサーバー
制御情報/アカウント/アクセスログ

ファイル制御情報をクラウドで管理。
だから、
「あとから削除、あとから追跡」できる。

暗号化ファイル
配布元

暗号化ファイル
配布先

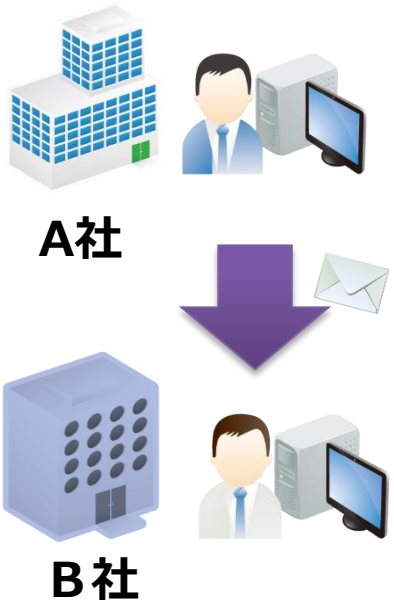
② 暗号化ファイル
受け渡し。

③ 専用アプリで、
暗号を復号化。

JBAT

Protect Anyware 2.0

渡した『ファイルを守る。』



**重要ファイルは、
不正に使われないようファイル制御！**

**データの中身は、
コピーできない！**

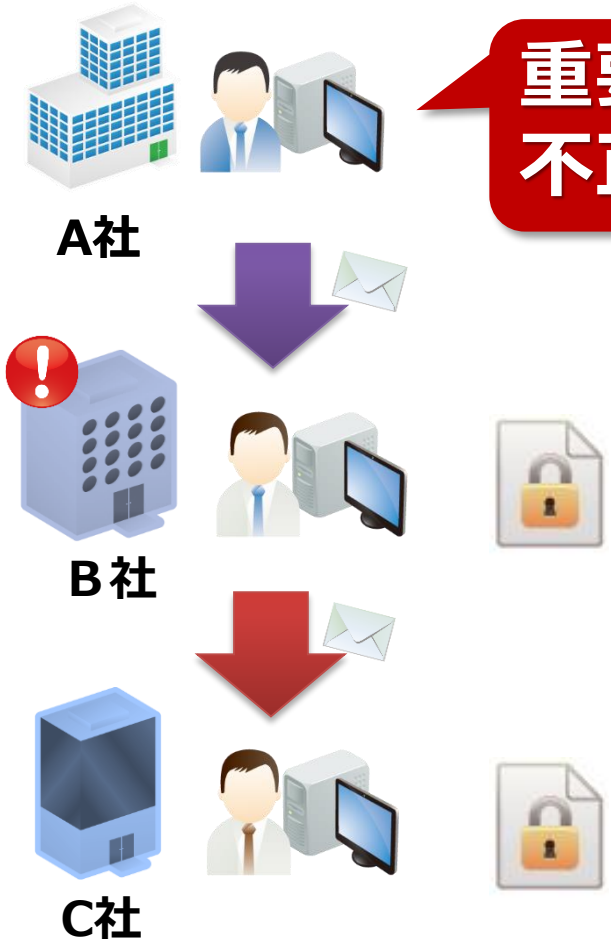
ファイルへの制御

- アカウント指定での
  アクセス制御
- 閲覧回数 / 閲覧の期限

- 保存禁止
- 印刷禁止
- 文字列や画像のコピー
- プリントスクリーン禁止

JBAT

渡したファイルを後から『追跡』



重要ファイルの証跡を管理。
不正なアクセスを把握できます。

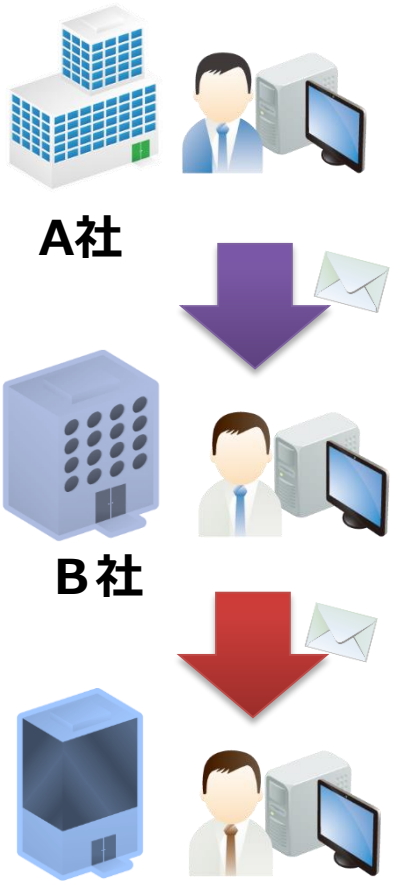
情報漏えい事故の発生！
C社に重要ファイルが流出・・

証跡管理
- いつ、誰が、どのファイルを操作したか。
- 権限のないアカウントでのアクセス
- パスワード入力ミス等のログインの失敗
- 閲覧可能な残り回数
- 閲覧回数を超えたことでのファイルの自動削除

ファイルへのアクセスは証跡が残る。

ファイルアクセス時のユーザーアカウント、接続元IPアドレスが判明

渡したファイルを後から『削除』



情報漏えい事故を起こした『B社』に
渡したファイルは削除！

削除

削除

拡散したファイルまで
削除できる。

かんたんな暗号化設定ツール（利用者）

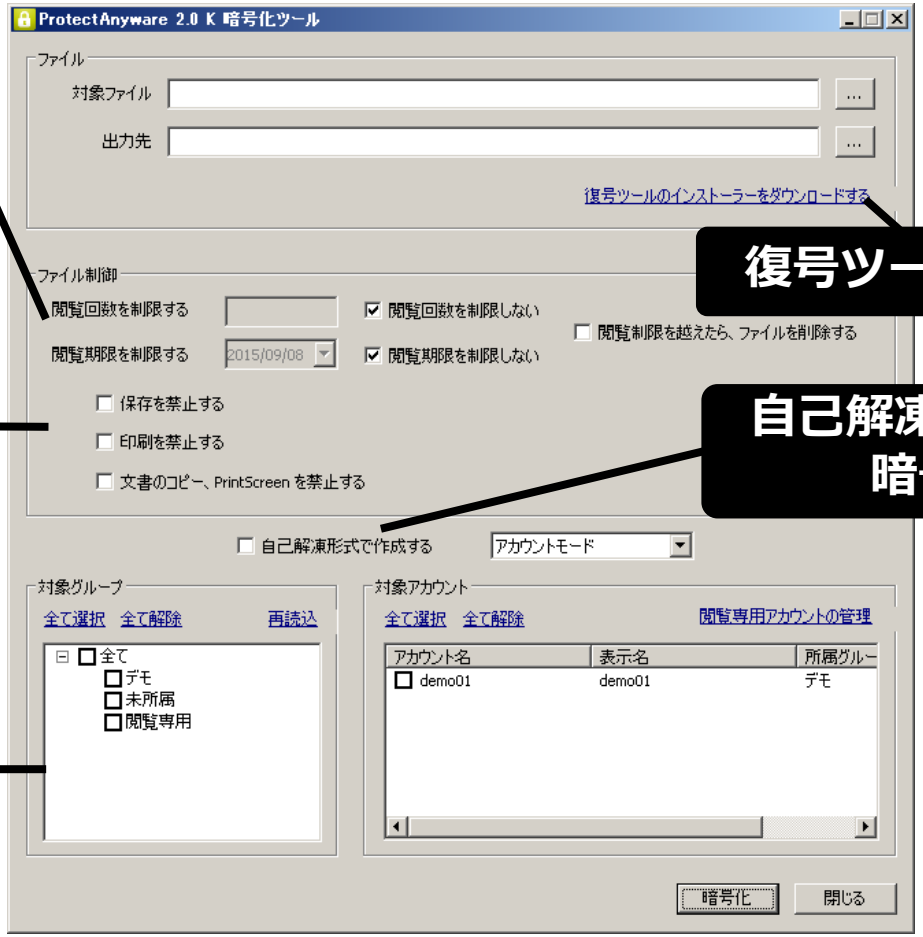
何回閲覧させるか？

・重要ファイルの閲覧は必要最小限の回数に抑えることができます。
・指定した閲覧回数を超過した場合は、ファイル自体を**自動削除**し重要ファイルの消し忘れを防止します。

どんな操作を禁止するか？

誰に操作をさせるか？

・パスワード認証だけでなく、ユーザーアカウント部門グループ単位にてファイル操作権限を付与できます。



復号ツールの入手

自己解凍形式での暗号化

暗号化ファイル作成者の設定画面

情報漏洩対策の強化

Protect Anyware 2.0

利用者が意識しなくても自動的に暗号化

利用者のセキュリティ意識の向上と、うっかりミス、誤操作などを、自動暗号化することで情報流出を防止します。

USBデバイスへのファイル書出し時に自動暗号化

個人情報や機密情報ファイルの操作を検出した際に自動暗号化

個人情報や機密情報を含むファイルの検出時に自動暗号化

JBAT

クライアントPCへのデスクトップメッセージ

グループ毎に表示期限を決めて設定！
上部が個別インベントリ情報、下部が任意メッセージ表示

【ユーザー画面】

マシン名 ： demo
OS名 ： Microsoft Windows Server 2003 Standard Edition
メモリ容量(MB) ： 1,023.45MB

【情報システム部よりお知らせ】

来週末31日(土)にシステムメンテナンス
作業を実施します。

前日30日(金)の退社時は、パソコンの電源を
落とさずに、そのままご帰宅ください。
ご協力お願いいたします。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
情報システム部： 内線：XXX 4月20日
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

管理機から送信した
メッセージを表示可能！

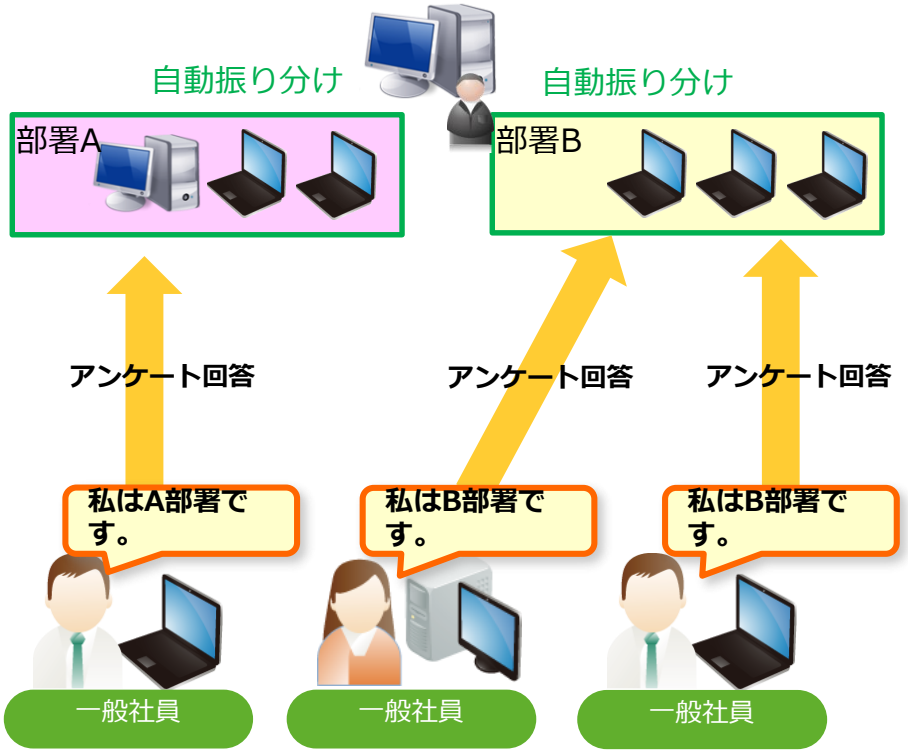
ユーザー画面に任意メッセージ、個別インベントリ情報を表示可能！

その他、資産管理を助ける便利な補助機能

<自動グループ振り分け機能>

自動的にクライアント端末の所属グループを振り分けることができます。

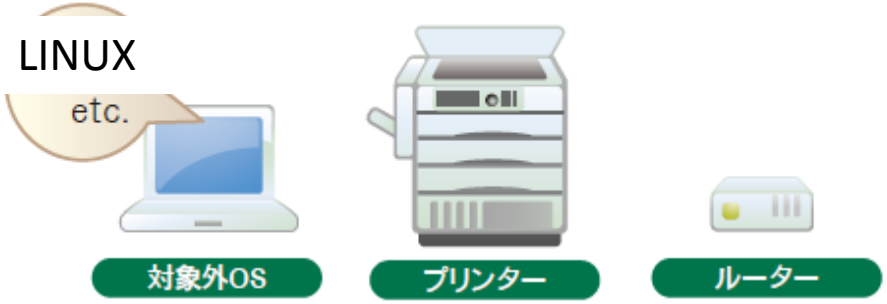
1.管理者が所属グループを作成
2.クライアント端末のユーザーがアンケートでグループ選択
3.アンケート結果に基づき自動で所属グループを振り分け



◆人事異動時のグループ変更も楽々対応
職員様がアンケートに答えるだけで
自動的に所属グループに振り分けられます。

<クライアント端末以外も登録が可能>

対象外OS（LINUXなど）のコンピューターやネットワークプリンターなどを手動で追加し、管理者コンソール上で管理することもできます。※手動追加した機器の情報は自動収集できません。



◆PC以外の機器も同じ台帳で管理したい。
PC端末の台帳とそれ以外の機器の台帳が分かれることなく、１つの台帳で機器管理を実現できます。

<サーバー、クライアントが仮想環境に対応>

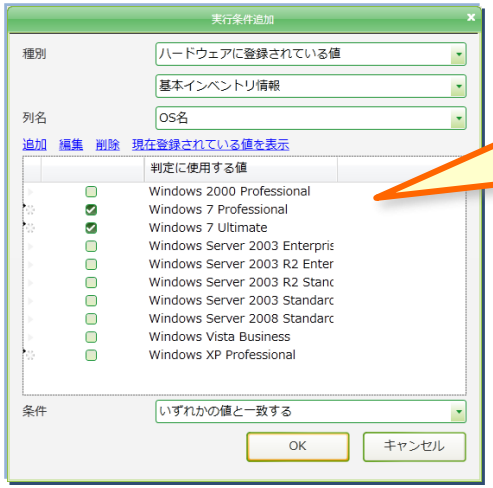
ProtectAnyware2.0サーバーを仮想化すれば、サーバーのシステムクラッシュなどの際に、高速に過去のサーバー環境への復元ができます。（HYPER –V、Virtual PC、VM wareに対応）

<Windows XP Modeはライセンスフリー>

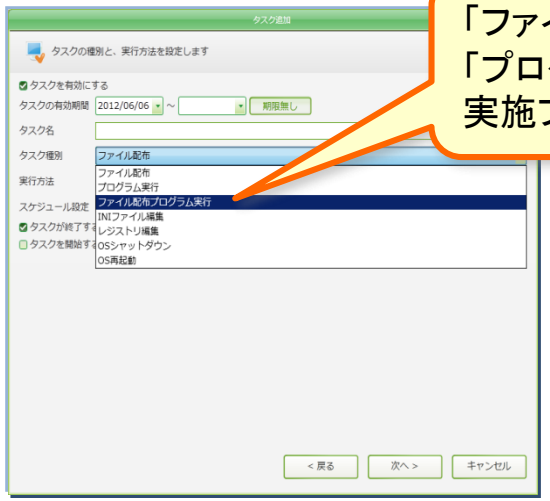
Windows7の「Windows XP Mode」にクライアントを入れて頂いてもライセンスは不要です。
必要以上にライセンス費用を購入頂く必要が御座いません。

配布/インストールプラン作成手順

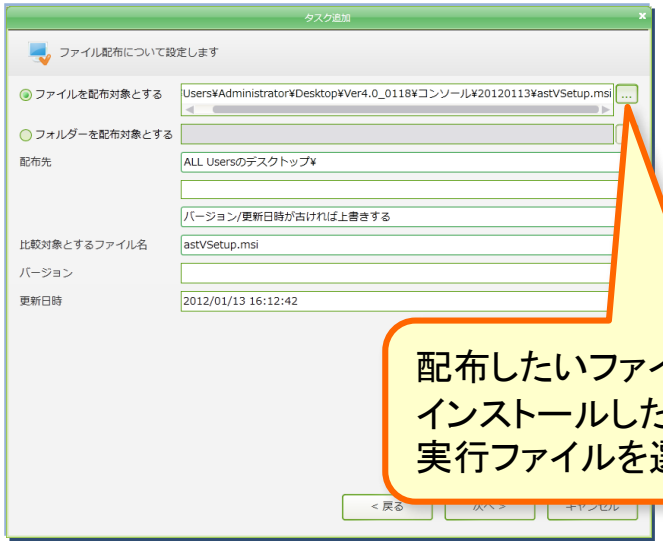
プラン作成はソフトウェアが必要な設定をウィザード形式で順番に確認していきますので、
設定漏れがなく誰でも簡単に思い通りのプランを作成頂けます。



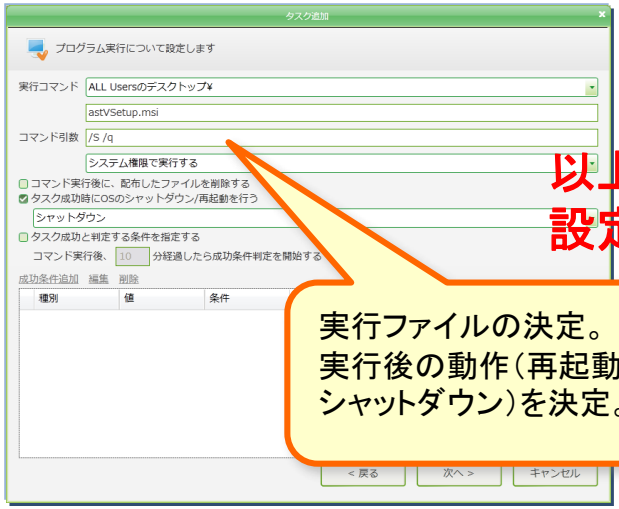
配布対象を選択。
左記の情報から選択可能。



「ファイル配布」、
「プログラム実行」等、
実施プランを決定。



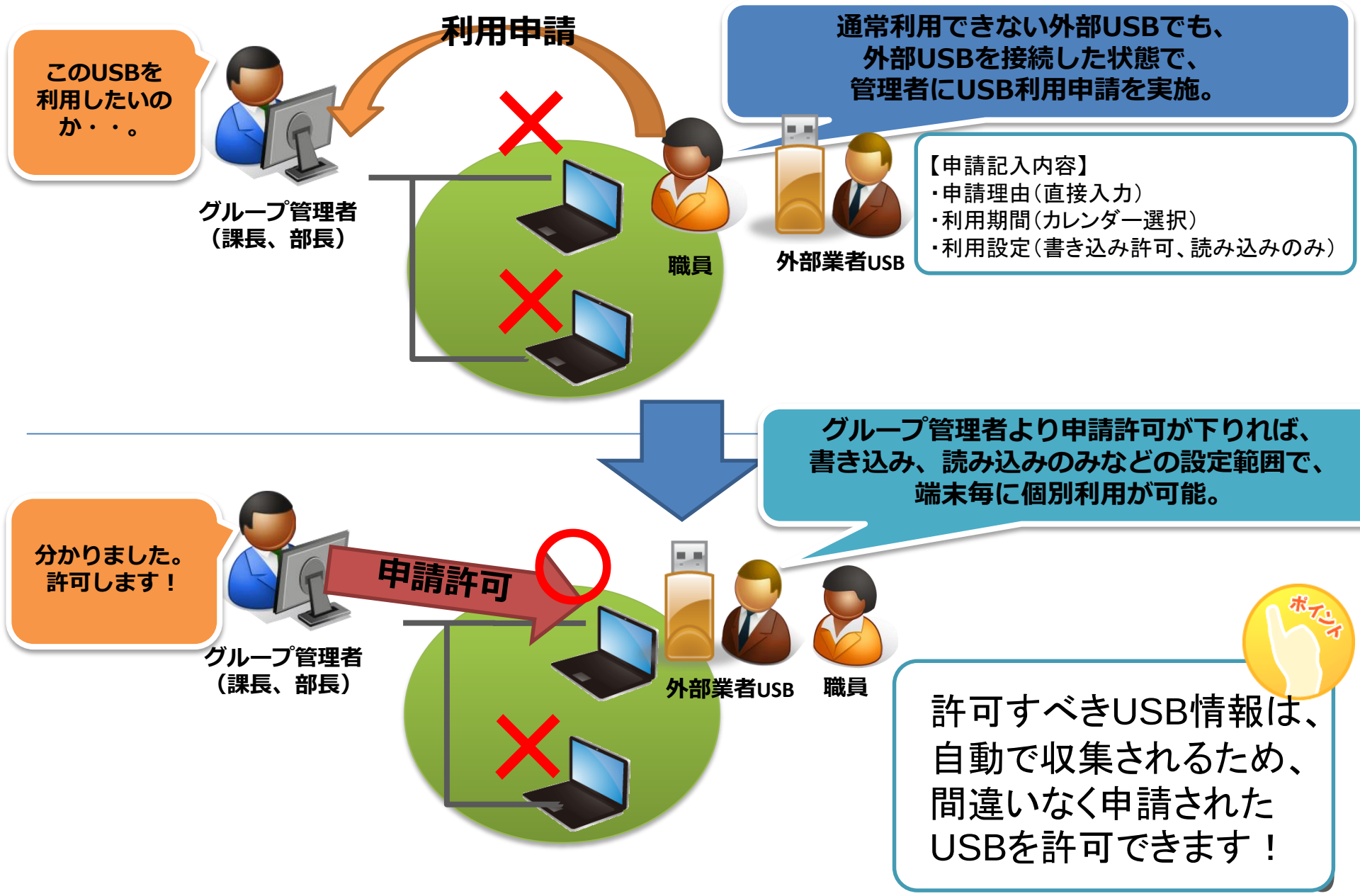
配布したいファイル、
インストールしたい
実行ファイルを選択。



実行ファイルの決定。
実行後の動作（再起動、
シャットダウン）を決定。

以上で、
設定完了！！

運用例① 外部のUSB端末を利用する場合



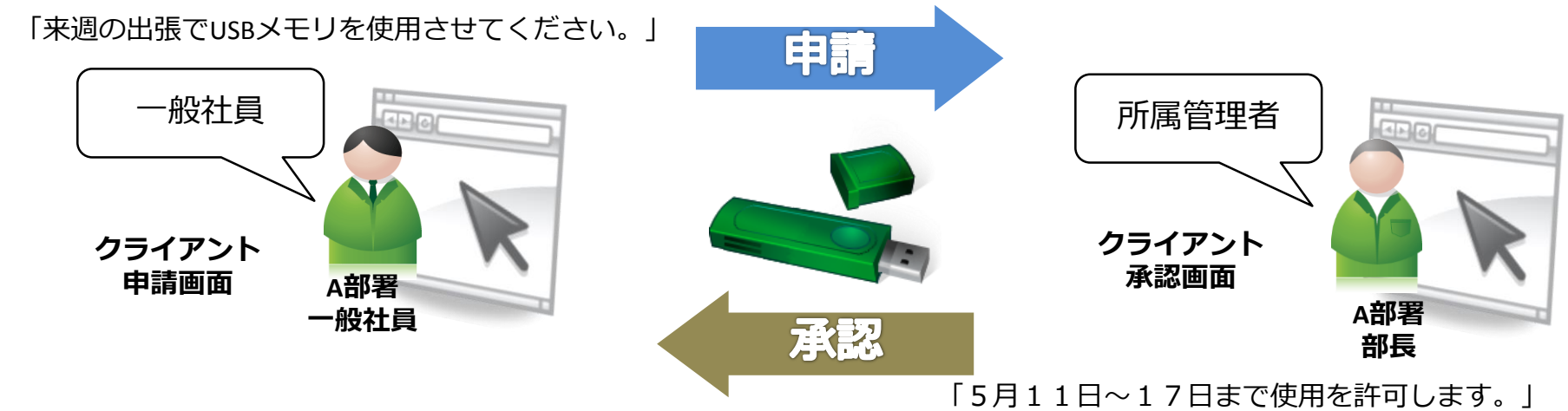
お客様のニーズからデバイス利用申請/承認機能を実装致しました。

ニーズ　従業員の外部デバイスの使用には申請制を採用したい

ニーズ　外部デバイスの管理責任はグループ単位で持たせたい

ProtectAnyware2.0には申請／承認機能があります。
USBメモリ等のデバイスを使用したい場合には、
どのデバイスを、どの期間、どのような理由で利用するのかの申請を行う事ができ、
所属（グループ）管理者はその申請に対する承認を行う事が可能です。
システム管理者はすべての申請／承認履歴を確認する事ができます。

例　USBデバイスの制御機能を有効。
会社指定のUSBデバイス（登録されていないUSBデバイス）は認識されない環境です。



ポイント　バックアップ機能

■ 2種類のデータベース構造で、過去に取得したログの再取込閲覧も実現！

↓　例えばこんなケースで効果を発揮　↓

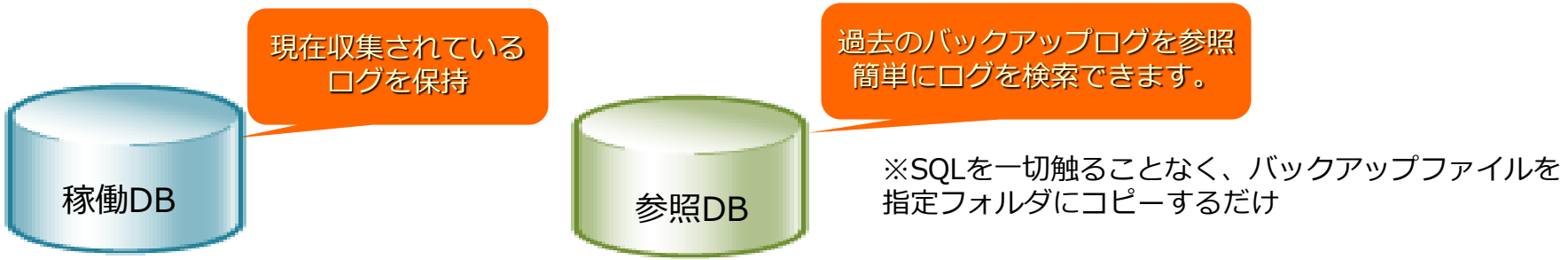
・ログを長期保管しておきたい
　→ 再利用し難いCSV出力の必要はありません！

・2年前のログより、ファイル操作履歴をトレースしたい
　→ バックアップファイルの再取込で簡単に実現します！

【Point!】
①ログの保存期間の設定は、任意設定（最大999日）

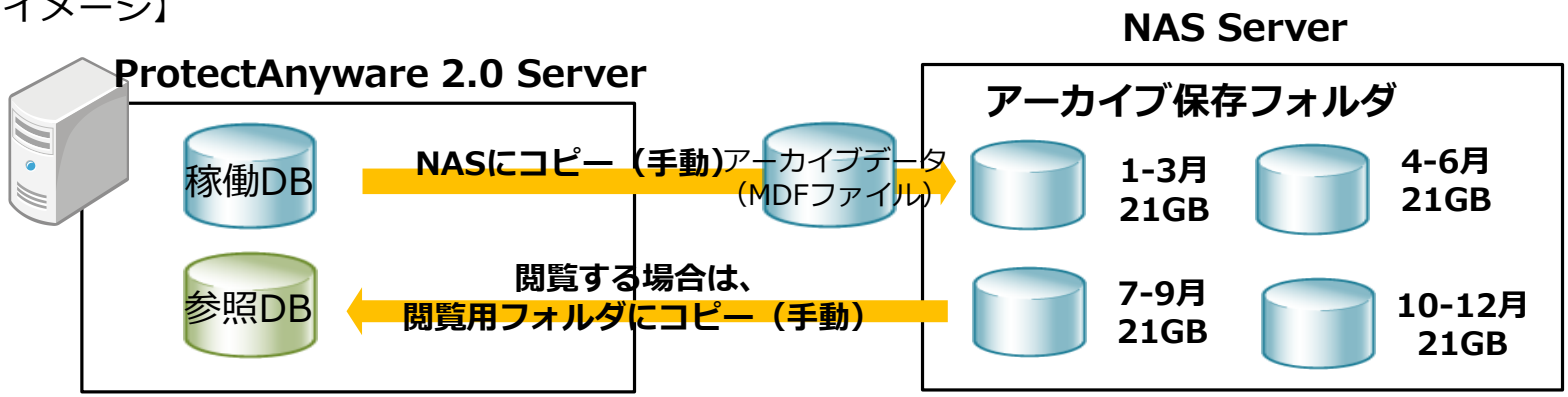
②バックアップスケジュールにより、設定内容や取得データの状態をSQL Serverより自動的にバックアップ

③稼動用と参照用の2種類データベースを装備しており、現在稼動しているデータベースを止めることなく、過去にバックアップしたデータを再取込し、情報の閲覧・トレースを実現する画期的な仕組みを搭載！



※SQLを一切触ることなく、バックアップファイルを指定フォルダにコピーするだけ

【運用イメージ】

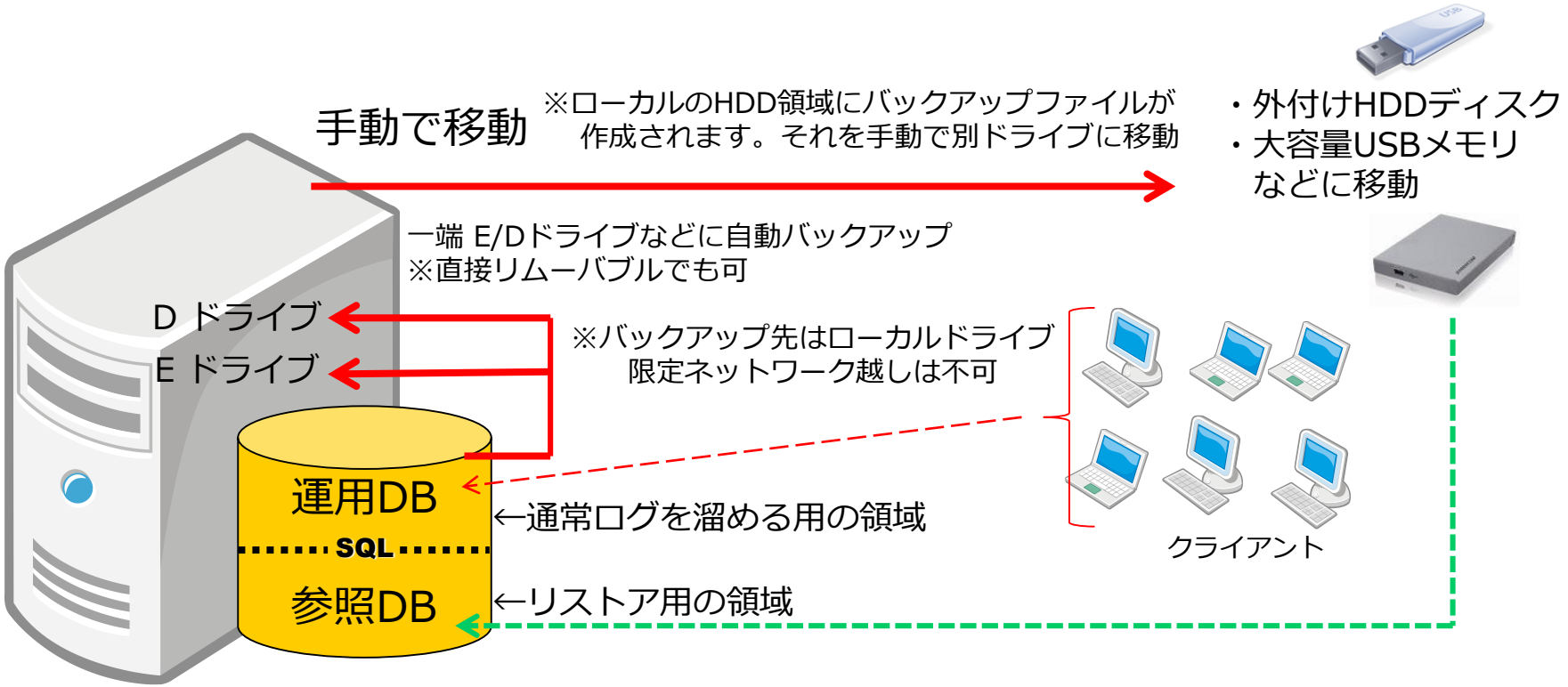


ログの試算について　例：５００台

ログ試算

■1.5MB（１日にクライアントが発するログ容量　最大の目安値　）×20日間（1ヶ月稼動日数/土日を除く）＝30MB
３０MB×５００台＝15GB

１ヶ月にサーバーに溜める容量　⇒　約 15GB　　ログの保存期間は任意設定が可能　最高9,999日まで上限有り



ポイント　管理者権限設定機能

●複数の管理者で運用を適切に分散できる「管理者権限設定機能」を搭載致します。

＜管理者権限設定機能＞

管理者ごとに運用管理を行う機能の有効／無効を設定することができます。

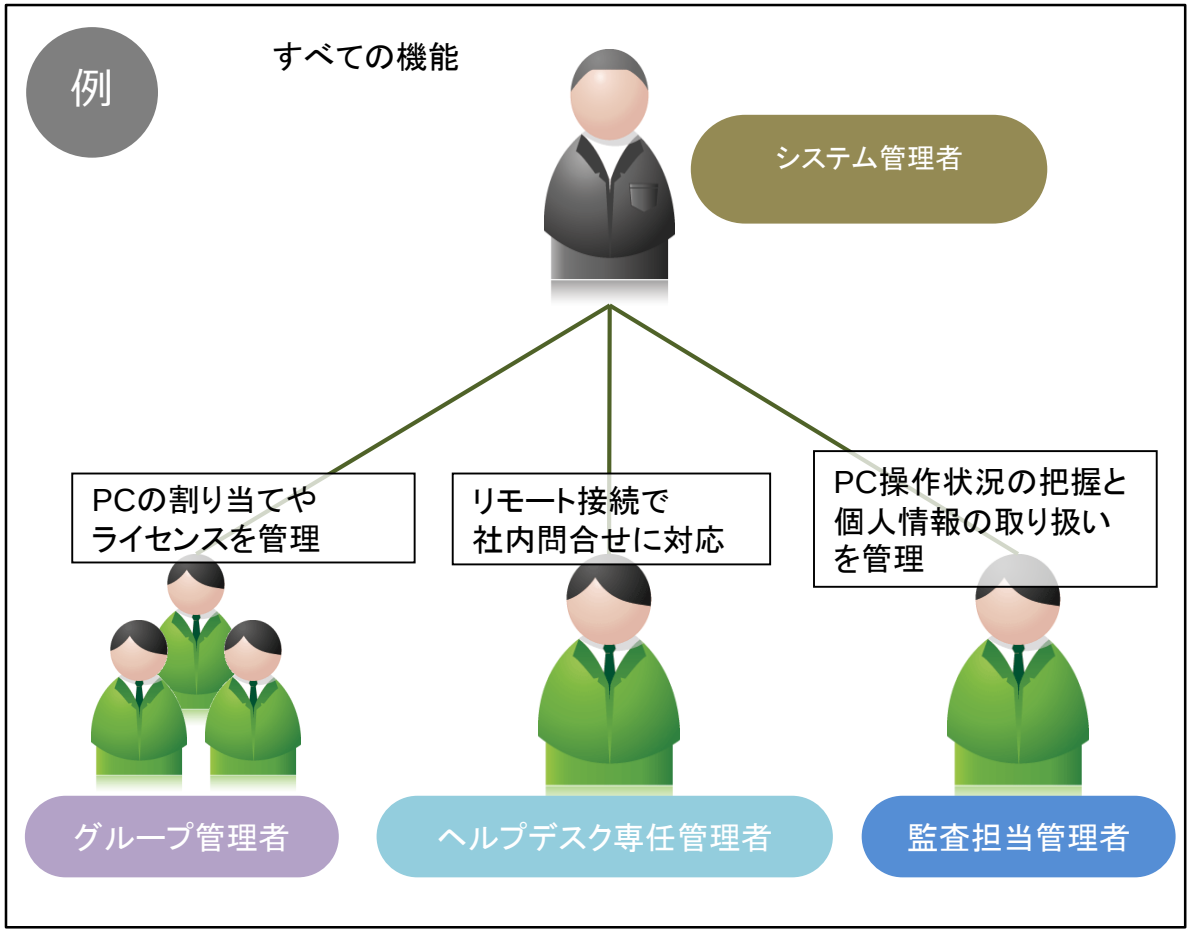
社内全体の管理を行うシステム管理者の他に、拠点や部署、グループごとに管理者を設置して運用負荷を適切に分散できます。

※システム管理者はすべての機能が有効になります。

【システム管理者】
管理コンソールの全ての操作を
行うことが出来る。
管理対象グループは、
『全て』以外選択出来ない。

【グループ管理者】
管理対象グループ配下に所属する
クライアント端末のログデータ閲覧と、
運用ポリシーの設定を行うことが出来る。
システム設定や、ネットワークの制御などの
システム全体に関わる運用ポリシーの
設定を行う事は出来ない。

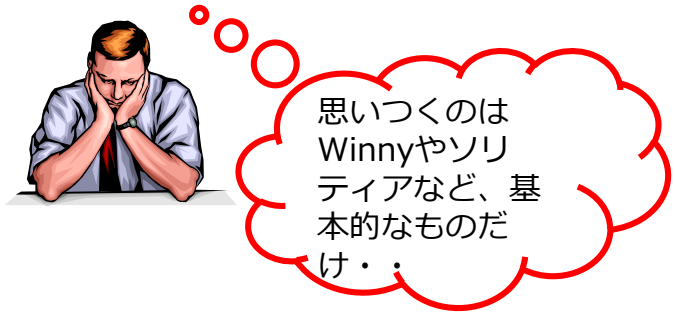
【グループ閲覧者】
管理グループ配下に所属する
クライアント端末のログデータ閲覧のみを
行うことが出来る。



アラート登録について

運用者様がぶつかる壁

アラート対象とするプロセス名をどのように登録すれば良いか？



ポリシー登録する内容、数によってセキュリティーレベルは変わって来ます。
ここの登録内容が欠けていると、ただログを取るだけの運用になりかねません。

ナビゲーション機能をONにすることによってアラートプロセスが100種類以上、自動で設定されます。

カテゴリ種別	プロセス名	アプリケーション名	セキュリティレベル1		セキュリティレベル2	
			アラートレベル	警告メッセージ	アラートレベル	警告メッセージ
ファイル共有	winny.exe	Winny	警告	表示	禁止	表示
	winny2.exe	Winny2				
	WINMX.exe	WinMX				
	Kazaa.exe	Kazaa				
	KazaaLite.exe	Kazaa Lite				
	limewire.exe	LimeWire				
	Shareza.exe	Shareza				
	Grokster.exe	Grokster				
	Cabos.exe	Cabos				
	Bittorrent.exe	Bittorrent				
	emule.exe	eMule				
	bitcomet.exe	Bitcomet				
	hamachi.exe	Hamachi				
	amembo.exe	amembo				
	uTorrent.exe	uTorrent				
	NapsterClient.exe	NapsterClient				
	ApexDC.exe	ApexDC				
	imeem-jp.exe	imeem-jp				
	Ares.exe	Ares				
	Azureus.exe	Azureus				
	BearShare.exe	BearShare				
	winnyp.exe	winnyp				
	BitComent Turbo.exe	BitComent Turbo				
	beaeshare.exe	beaeshare				
	Morpheus.exe	Morpheus				
	MagicMirror.exe	MagicMirror				
	Share.exe	Share				
	perfect dark.exe	Perfect Dark				
	Groove.exe	Groove			警告	
2チャンネルビューアー	gikoNavi.exe	ギコナビ	警告	表示	禁止	表示
	katjusha.exe	かちゅ～しゃ				
	hzb20.exe	ホットソヌ2				
	Jane2ch.exe	JaneStyle				
	tora3aux.exe	禁断の壺				
ファイル転送	FFFTP.exe	FFFTP	警告	非表示	警告	非表示
	RootFTP.exe	RootFTP				
	TidyFtp.exe	TidyFtp				
	msmsgs.exe	Microsoftメッセンジャー				

アラート登録について

設定例

カテゴリ種別	プロセス名	アプリケーション名
ファイル共有	winny.exe	Winny
	winny2.exe	Winny2
	WINMX.exe	WinMX
	Kazaa.exe	Kazaa
	KazaaLite.exe	Kazaa Lite
	limewire.exe	LimeWire
	Shareza.exe	Shareza
	Grokster.exe	Grokster
	Cabos.exe	Cabos
	Bittorrent.exe	Bittorrent
	emule.exe	eMule
	bitcomet.exe	Bitcomet
	hamachi.exe	Hamachi
	amembo.exe	amembo
	uTorrent.exe	uTorrent
	NapsterClient.exe	NapsterClient
	ApexDC.exe	ApexDC
	imeem-jp.exe	imeem-jp
	Ares.exe	Ares
	Azureus.exe	Azureus
	BearShare.exe	BearShare
	winnyp.exe	winnyp
	BitComent Turbo.exe	BitComent Turbo
	beaeshare.exe	beaeshare
	Morpheus.exe	Morpheus
	MagicMirror.exe	MagicMirror
	Share.exe	Share
	perfect dark.exe	Perfect Dark
	Groove.exe	Groove
2チャンネルビューアー	gikoNavi.exe	ギコナビ
	katjusha.exe	かちゅ～しゃ
	hzb20.exe	ホットゾヌ2
	Jane2ch.exe	JaneStyle
	tora3aux.exe	禁断の壺
ファイル転送	FFFTP.exe	FFFTP
	RootFTP.exe	RootFTP
	TidyFtp.exe	TidyFtp

カテゴリ種別	プロセス名	アプリケーション名
メッセンジャー	msmsgs.exe	Microsoftメッセンジャー
	icq.exe	ICQ
	icqlite.exe	ICQLite
	ipmsg.exe	IPメッセンジャー
	ymsgriej.exe	Yahoo! メッセンジャー
	YPagerj.exe	Yahoo! メッセンジャー
	conf.exe	NetMeeting
skype	skype.exe	Skype
	skypePM.exe	Skype
音楽/映像	wmplayer.exe	Windowsメディアプレーヤー
	mplayer2.exe	Windowsメディアプレーヤー
	realplayer.exe	リアルプレイヤー
	realone.exe	リアルワンプレイヤー
	itunes.exe	iTunes
	ituneshelper.exe	iTunes
	ipodservice.exe	iPod
	divx.exe	Divx
	DivX Player.exe	Divx
	Quicktime.exe	QuickTime
	qttask.exe	QuickTime
	Gom.exe	GOM PLAYER
	Omgjbox.exe	SonicStage
	winamp.exe	Winamp
GAME（Windows標準）	sol.exe	ソリティア
	Solitaire.exe	ソリティア
	freecell.exe	フリーセル
	winmine.exe	マインスイーパ
	Minesweeper.exe	マインスイーパ
	PINBALL.EXE	ピンボール
	shvlzm.exe	インターネットスペード
	chkrzm.exe	インターネットチェッカー
	hrtzzm.exe	インターネットハーツ
	bckgzm.exe	インターネットバックギャモン
	Rvsezm.exe	インターネットリバーシ
	mshearts.exe	ハーツ
	Hearts.exe	ハーツ
	spider.exe	スパイダ ソリティア
	SpiderSolitaire.exe	スパイダ ソリティア
	chess.exe	Chess Titans
	Mahjong.exe	Mahjong Titans
	PurblePlace.exe	Purble Place
	InkBall.exe	インクボール

カテゴリ種別	プロセス名	アプリケーション名
GAME（オンラインゲーム）	hgstarterjp.exe	インストーラー
	Pachinko.exe	パチンコ
	PachinkoDX.exe	パチンコDX
	Pachislot.exe	パチスロ
	PslotDX.exe	パチスロDX
	Majak2.exe	麻雀
	Samma.exe	3人麻雀
	MSDuelgo.exe	花札
	Shougi2.exe	将棋
	Othello.exe	オセロ
	Bingo.exe	ビンゴ
ブラウザー	netscape.exe	Netscape
	Sleipnir.exe	Sleipnir
	Lunascape.exe	Lunascape
	Opera.exe	Opera
	mozilla.exe	Mozilla
	Firefox.exe	Firefox.exe
	Chrome.exe	Google Chrome
	Craving Explorer.exe	Craving Explorer
	kiki.exe	KIKI
	TextBrowser.exe	TextBrowser
	Donut.exe	Donut RAPT
	sxf_browser.exe	SXF ブラウザ
インストーラー	Setup.exe	インストーラー
	Install.exe	インストーラー
	Setup.msi	インストーラー
	Install.msi	インストーラー

重要ファイル監査

重要ファイル監査機能（個人情報／機密情報監査機能）

こんな課題・目的を持つお客様へは効果絶大です！

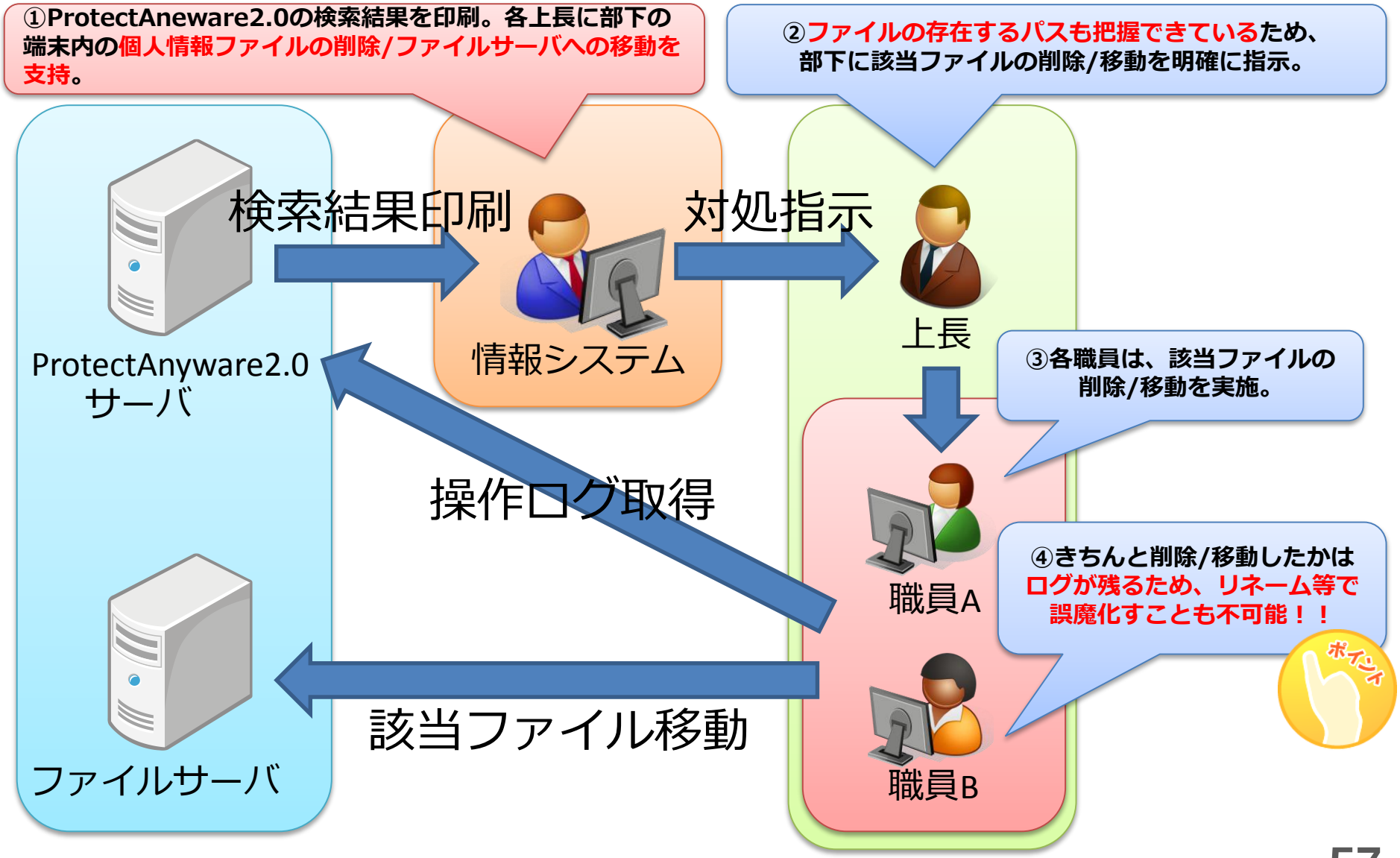
- ●組織にとって重要な情報資産がどこにあるのか棚卸しを実施したい・・・
- ●個人情報を含むファイルを利用する機会が多く、その取扱いにリスクを感じている・・・
- ●職員様がデスクトップやマイドキュメントにファイルを放置する傾向があり不安だ・・・
- ●PCへの対策は講じてきているが、そもそも重要情報がどこにあるかは分からない・・・
- ●重要ファイルは共有サーバに集約する決まりだが、本当に守られているのか・・・

人手では管理しきれない『情報資産の棚卸し』を実現！

（PC内の個人情報／機密情報ファイル監査機能）

個人情報／機密情報がみつかったら・・・

運用例①



個人情報の棚卸のメリット

個人情報ファイルの所在がわかるため、

情報漏えいの根本である原因の徹底管理が可能。

ログ取得だけでは簡単に把握できない、

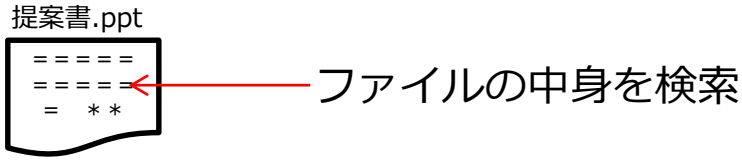
個人情報ファイルの操作に注力したログ監視が可能。

操作ログのみでの情報対策の限界

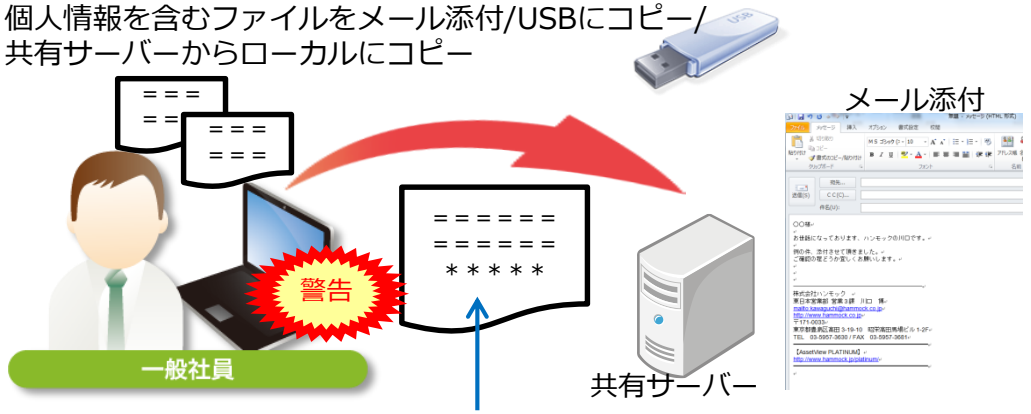
操作ログはあくまで操作をした（事故が起こる）後に取れる情報です。

「事故を未然に防ぐ」という視点では**限界**があります。

根本となる原因（情報の在りか）をきちんと把握できます。
根本となる情報が何処にあるかを把握して、対策を行っていくことが
情報漏洩を防ぐ意味では有効な対策であると考えます。



個人/機密情報が含まれたファイルコピー、移動 等の操作を行った際、
ファイル内をチェック（ファイル名ではありません）して警告メッセージを
クライアントPC上に表示。利用者の操作を操作履歴として記録しつつ注意を促します。



個人情報を含むファイル
（ファイル名を見て判断している分けではありません）

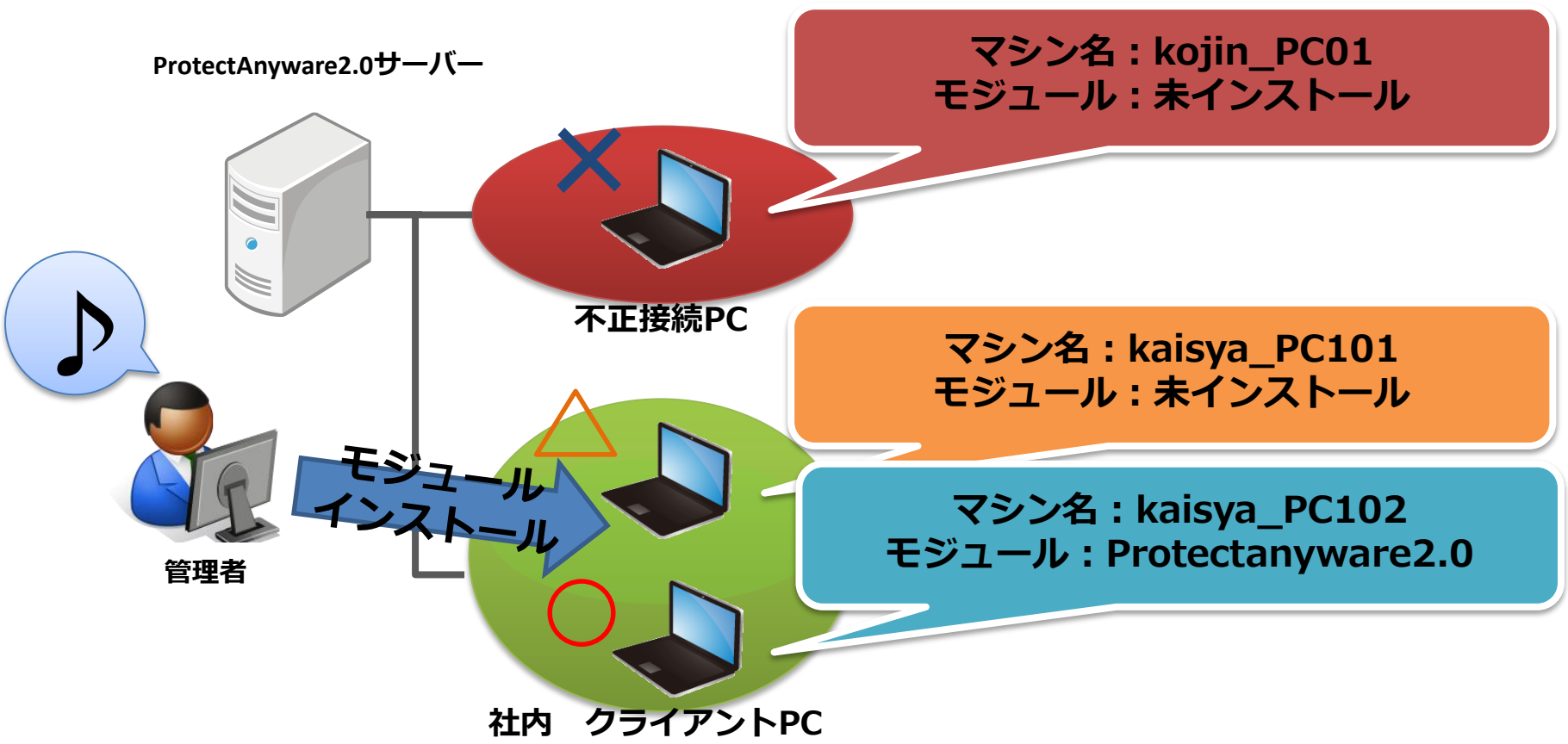
【警告メッセージ表示の条件】※勿論、操作ファイル操作ログも取れています。

- リムーバブルディスクに関連するファイル操作をした場合
- ネットワーク上の共有フォルダーに関連するファイル操作をした場合
- ファイルのメール添付をした場合
  ※Outlook、Outlook Express、Windowsメール利用時
- Microsoft Officeファイルのオープン/上書き保存をした場合

不正PC遮断

ポイント

マシン名、以外にProtectAnyware2.0モジュールの有無が分かるため、**不正接続端末か、社内端末（未許可）端末かの判断が容易。**



他システムの場合、社内端末台帳とぶつけ合わせが必要になるため管理が面倒

取得ログ一覧

●クライアントPCに関するさまざまな操作ログを取得、監視します。
●取得の可否も細やかに設定でき、ポリシーや運用環境に合わせた監視体制を構築することができます。

取得情報	内容
ファイル操作	クライアントPCで行われた、ファイル操作の情報を取得します。 ・操作対象のファイル名 ・操作対象のファイルパス ・操作元のドライブ種別 ・変更後のファイル名 ・プロセス名 ・コピー/移動先のファイルパス ・コピー/移動先のドライブ種別
インターネットへのファイルアップロード	クライアントPCから、Webサイトにアップロードされたファイルの情報を取得します。 ・操作対象のファイル名 ・アップロード先のURL
メール添付 ※Outlook、Outlook Express、Windowsメール対象	メール作成時に指定した添付ファイルの情報を取得します。 ・操作対象のファイル名 ・操作対象のファイルパス ・プロセス名 ・操作元のドライブ種別
NEW メール送信 ※SMTP/ESMTPログ取得	メール送信ログを取得します。 ・件名 ・送信日時 ・送信元メールアドレス ・送信先メールアドレス ・添付ファイル名
印刷	クライアントPCで印刷された、ドキュメントの情報を取得します。 ・ドキュメント名 ・ファイル名 ・プリンター名 ・印刷枚数 ・印刷データタイプ

取得情報	内容
NEW ドライブの追加と削除	ドライブの追加と削除を検知して、以下の情報を取得します。 ・ドライブ種別 (ローカルディスク、リムーバブルディスク、ネットワークドライブ、FD、CD/DVD、ポータブルデバイス) ・ドライブ名 ・UNCパス (ネットワークドライブの場合) ・デバイス名 (USBデバイス/ポータブルデバイスの場合) ・ベンダー (USBデバイス/ポータブルデバイスの場合) ・プロダクトID (USBデバイス/ポータブルデバイスの場合) ・シリアルナンバー (USBデバイス/ポータブルデバイスの場合)
クリップボード操作	クライアントPCで行われた、以下のクリップボード操作を取得します。 ・文字列のコピー ・ファイルのコピー ・画像のコピー/プリントスクリーン
チャットメッセージ	テンセントQQ（インスタントメッセンジャー）でチャットした際に送受信された文字列を取得します。
ウィンドウタイトル	クライアントPCでアクティブになっているウィンドウの情報を取得します。 ・プロセス名 ・ウィンドウタイトル ・URL （Internet Explorerの場合）
プロセス	クライアントPCで起動している、プロセスの情報を取得します。 ・プロセス名 ・アカウント名 ・バージョン ・起動日時 ・起動していた時間

メール送信ログ取得

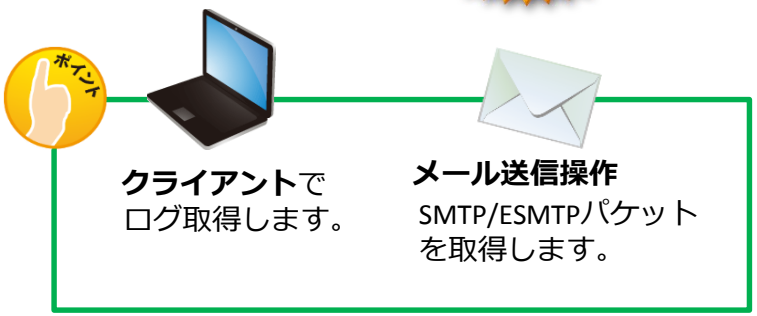
●クライアント端末からのメール送信ログを取得できるので、
持ち出しPCのメール送信ログも取得できます。
●SMTP/ESMTPパケットを取得する仕組みなので、メールソフトに依存しません。

NEW

<メール送信ログ>

以下のメール送信情報を取得します。

・件名　　・送信日時
・送信元メールアドレス　　・送信先メールアドレス
・添付ファイル名



<操作履歴検索ウィンドウで表示>

メール送信情報は操作履歴検索ウィンドウで表示できるので、メール送信前後のファイル操作やウィンドウタイトルの遷移を確認できます。

管理コンソール画面イメージ

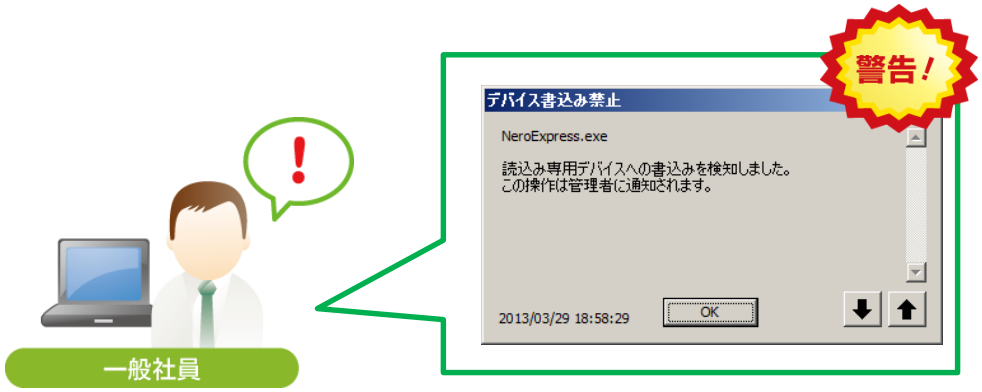
ログ取得日時	ログオンユーザー	操作種別	操作対象のファイル名/ウィンド
2013/03/28 20:41:47	HAMMOCK	個人情報ファイルメール添付	2007年度_顧客名簿.xls
2013/03/28 20:41:47	HAMMOCK	個人情報ファイルメール添付	2007年度_顧客名簿.xls
2013/03/28 20:41:47	HAMMOCK	個人情報ファイル削除	2007年度_顧客名簿.xls
2013/03/28 20:42:02	HAMMOCK	ファイルオープン	2006年度_顧客名簿.xls
2013/03/28 20:42:11	HAMMOCK	個人情報ファイルコピー	2006年度_顧客名簿.xls
2013/03/28 20:42:18	HAMMOCK	個人情報ファイルメール添付	2006年度_顧客名簿.xls
2013/03/28 20:50:33	HAMMOCK	メール送信	個人情報

ポイント
・ProtectAnyware2.0を導入すれば、個人情報ファイルのメール添付の判別も可 能です。
・ファイル操作追跡検索はメール添付イベントから操作します。

ライティングソフト制御/書込み検知ログ

- CD/DVDを読込み専用または使用禁止に設定している場合、以下のライティングソフトの起動禁止ができます。
- ライティングソフトでのCD/DVDへファイルの書込みを検知し、ログ取得します。

NEW



※制御設定した場合には書込み検知はされません。

ポイント

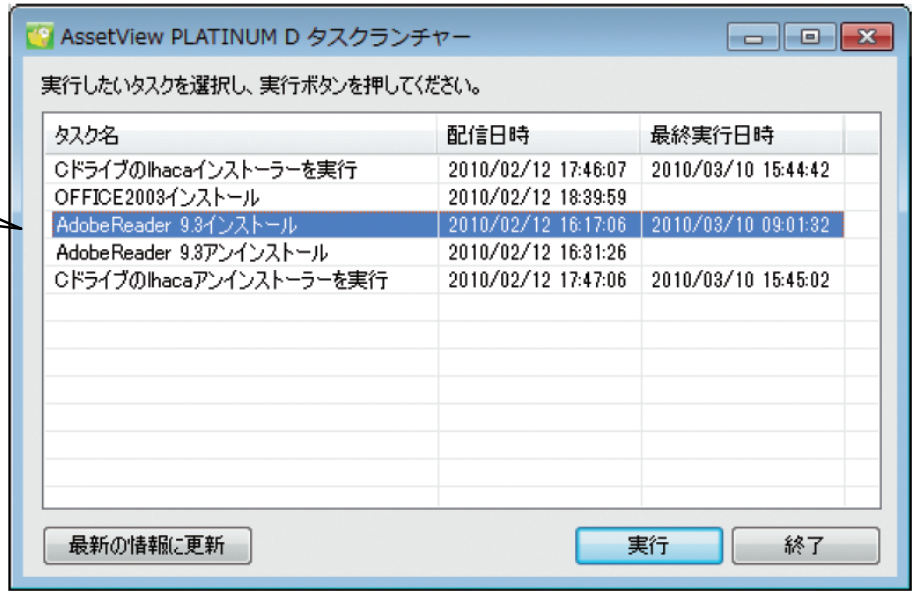
対象製品
- B's Recorder GOLD 11
- Nero 9 StartSmart Essentials
- Roxio Easy Media Creator 10

※今後のバージョンアップで順次対応製品／バージョンを拡張します。

プリンタドライバインストール・設定変更

●クライアントの任意のタイミングで配布実行プランを実行出来る。
「タスクランチャー」を搭載。

管理者から強制的に実行するのではなく、
クライアント端末を使うユーザーの
任意のタイミングでインストール実行可能。



配布条件を作る際に実行アカウントを指定
できるため、配布を実行したいクライアント端末の
ログオンユーザーに管理者権限がなくても
アプリケーションのインストールや
セキュリティーパッチの適用が出来ます。

ニーズ

遠方や数多くの拠点を持っている製造業様、自治体様にて
人事異動などの際に、異動先のプリンタードライバーや環境設定がされておらず、
すぐにプリンターの利用などが出来ないという相談を良く頂きます。

ご提案

「タスクランチャー」を活用頂きますと、ユーザー自身が必要なタイミングで
事前に用意されたインストールプランを実施する事が出来るため、
情報システムの対応を待たずにセットアップを実施し利用する事が可能となります。