

SaaSを利用した セキュリティ維持管理のすすめ

クオリティ株式会社

クオリティのご紹介

▶クオリティ株式会社

従業員数： 74名（2008年4月末現在）
グループ計 約160名

東京本社： 東京都千代田区平河町1-4-5平和第一ビル

大阪支店： 大阪府大阪市中央区本町2-5-7 丸紅大阪本社ビル12F

名古屋支店： 名古屋市中区錦1-10-27 カネヨビル

▶グループ会社

[和歌山]

株式会社エスアールアイ(Shirahama Research Institute)
和歌山県西牟婁郡白浜町字東谷83番68

[米国]

QualitySoft Corporation, Seattle
13400 Northup Way NE, Suite 50 Bellevue, WA 98005 USA

[中国]

QualitySoft Corporation, Shanghai (闊利達軟件（上海）有限公司)
中国 上海市 北京東路689号東銀大廈21F

[韓国]

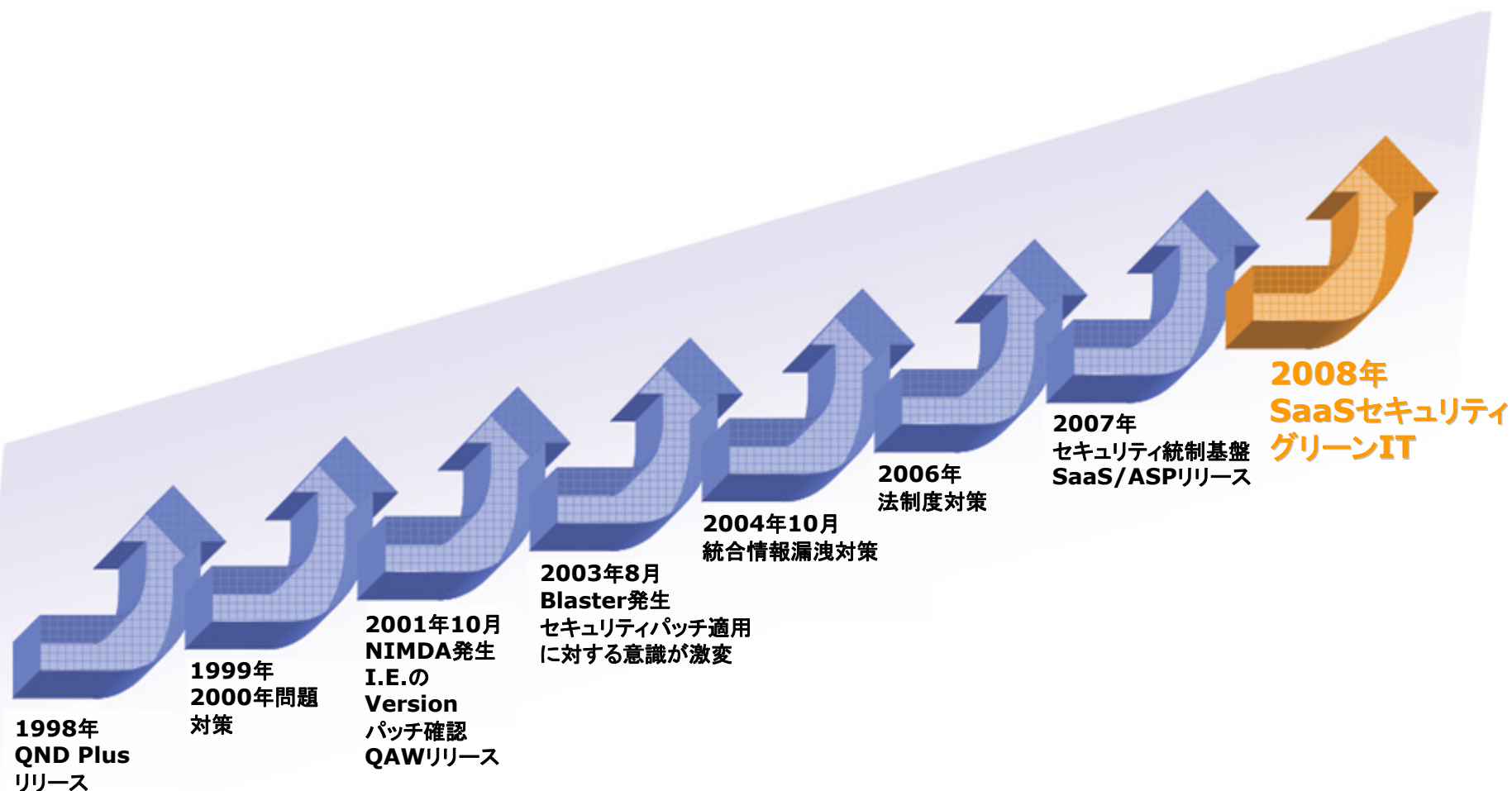
QualitySoft Corporation, Seoul
10F, HyoChangB/D, 181-3, Jamsil-Dong, Songpa-Gu, Seoul, Korea



本日のAgenda

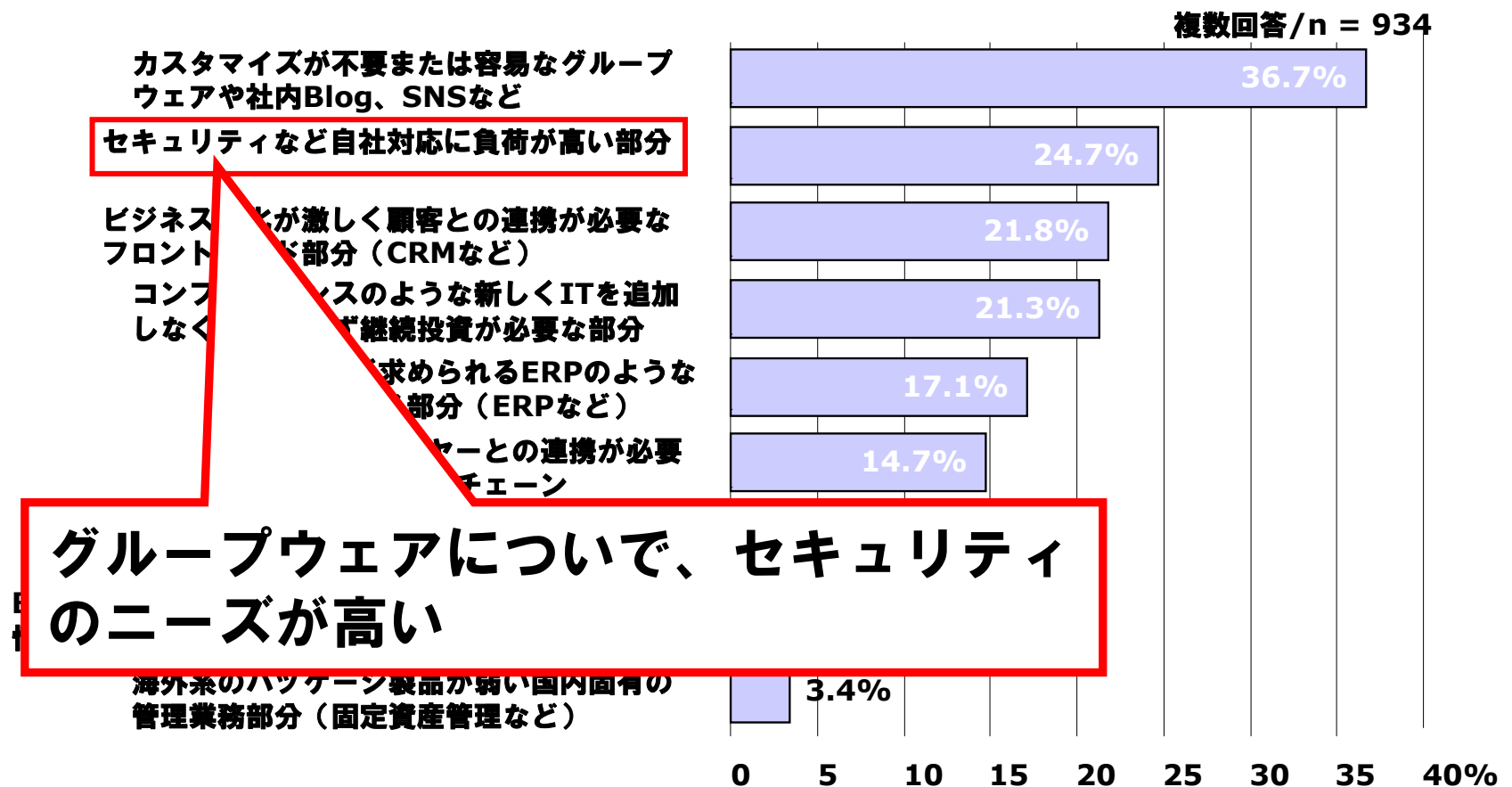
- クオリティの歩み
- ASP、SaaS型セキュリティ
- ISMとは？
- DKSとは？
- クオリティのSaaS戦略

クオリティの歩み



ASP/SaaSに関するアンケート

SaaS/ASPで利用したいサービス



Source: IDC Japan, 11/2007

クオリティのアプローチ

- 人件費の面で、自社に専任管理者を置くのは困難
- 変化し続けるITインフラを管理し続けるのは困難
- ただ、セキュリティ事故は起こしたくない
- ✓ セキュリティ対策は社外にアウトソース
- ✓ 必要な機能を選択

Security as a Service

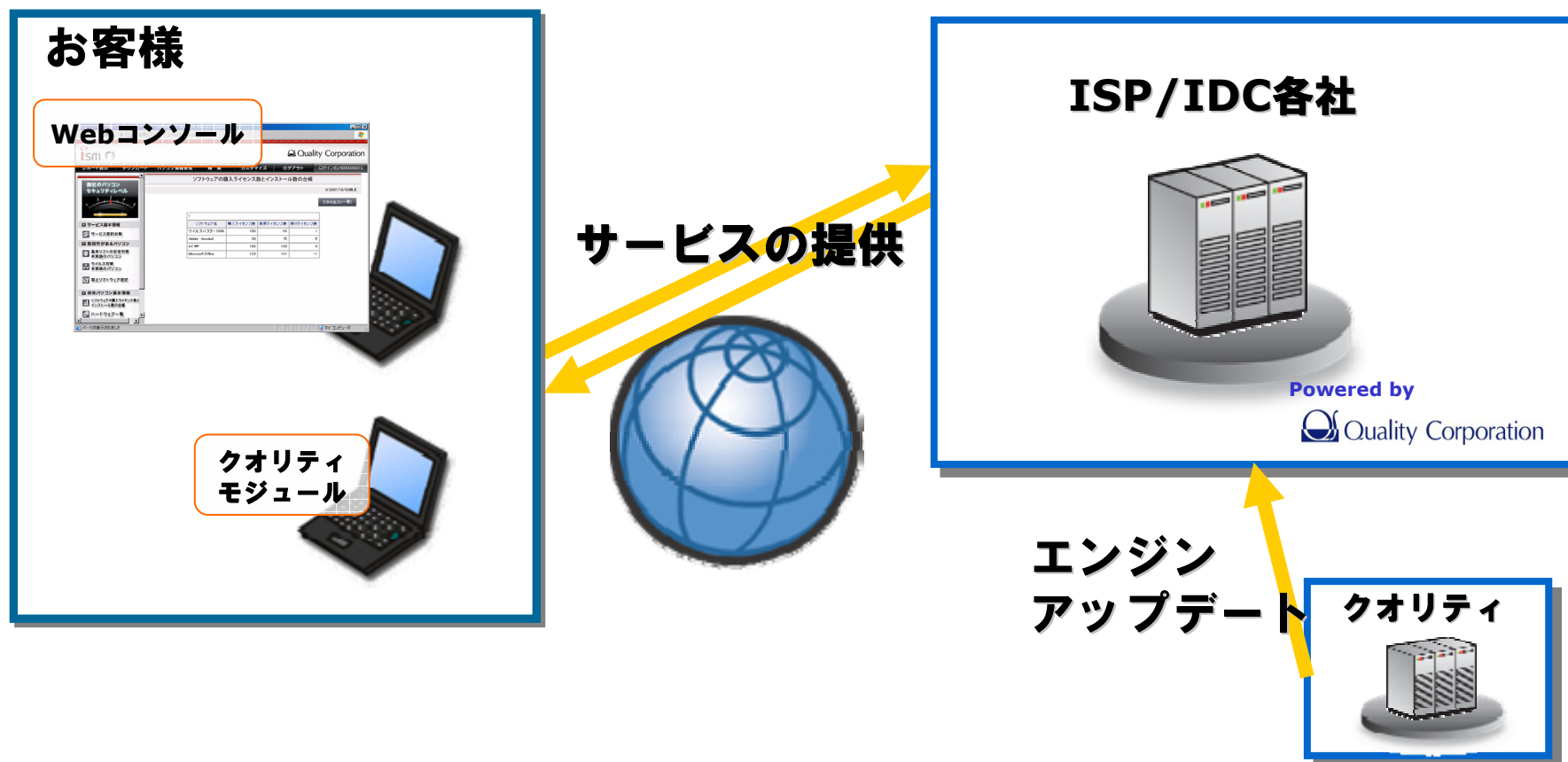
SaaSセキュリティのメリット

- **サーバレス、安全安心運用！**
- **専任の管理者不在でも利用可能！**
- **Webコンソールで状況の把握も簡単！**
- **面倒なライセンス管理も自動更新**



クオリティのサービスモデル

クオリティは、ASP・SaaS型サービスのエンジンをアップデートしていきます。
このエンジンを利用して、お客様にISP・IDC各社がサービスを提供します。



クオリティSaaSパートナー

➤ クオリティSaaSエンジンを利用したサービス、提供中

- ➡ (株)アイネット
Security and Asset Checkup ASP Service
- ➡ (株)大塚商会
たよれーるワンコインセキュリティ
- ➡ サイトロック(株)
siteROCK Client Care
- ➡ スターネット(株)
STAR-ISM
- ➡ ソフトバンクBB(株)
TEKI-PAKI資産管理 ISM Client Care
- ➡ (株)ネットワールド
ISM Client Care
- ➡ チロロプリント
DKS for SaaS(近日リリース予定)

クオリティのSaaSエンジン

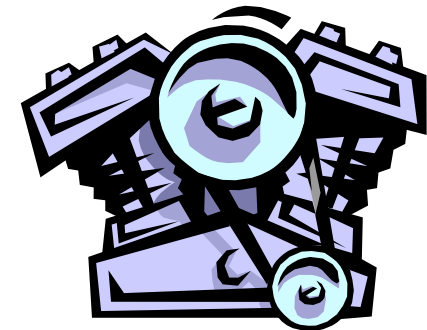
2つのSaaSエンジンを提供します

➤ **ISM(IT Security Manager)**

PCのセキュリティ維持管理

➤ **DKS for SaaS**

ドキュメントのアクセスコントロール



ISM基本サービスについて

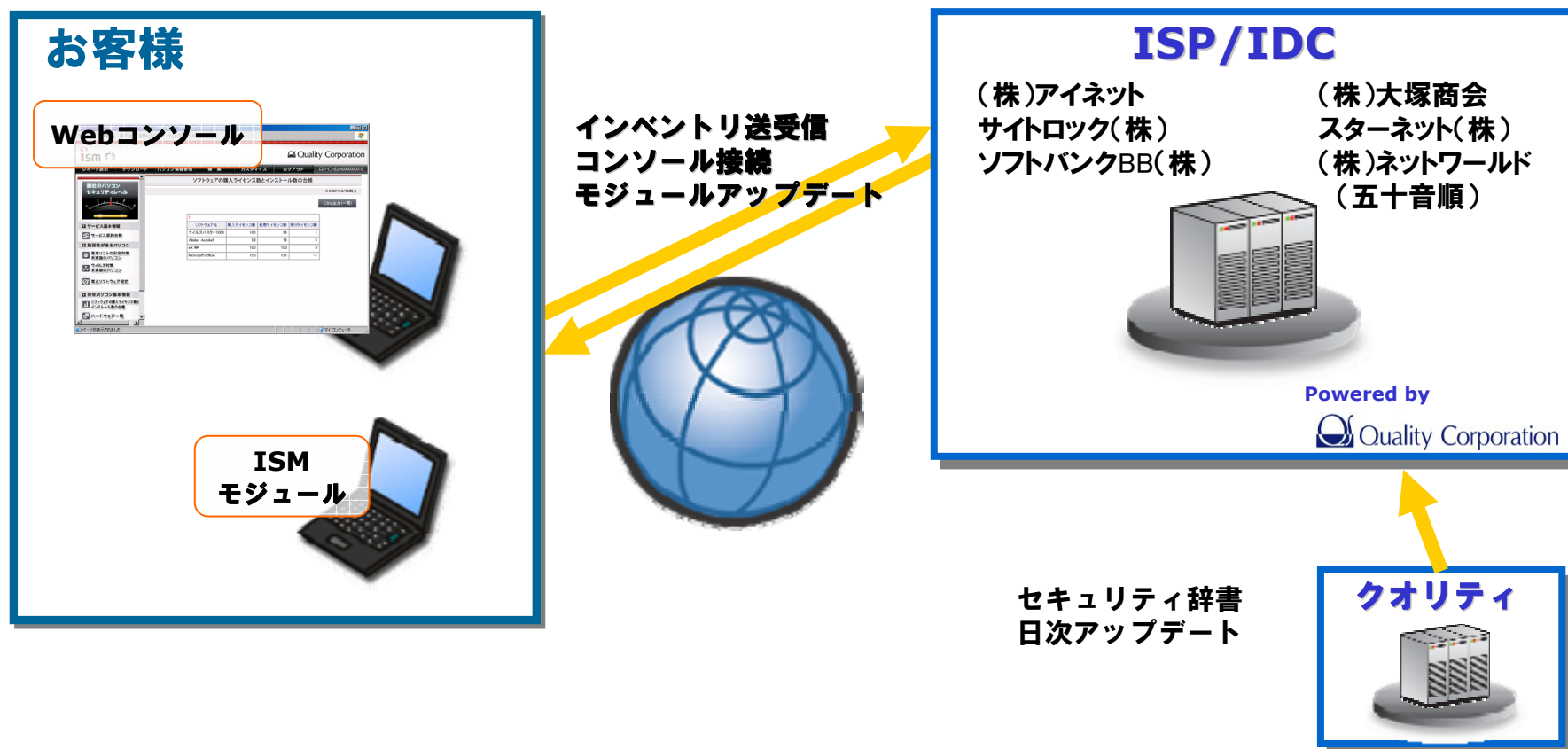
現在、5つのサービスをご提供しています。

- セキュリティレベル診断
- Windows Update更新支援
- 不正ソフトの検出&レポート
- ライセンス管理レポート
- HW/SWレポート



サービス提供モデル

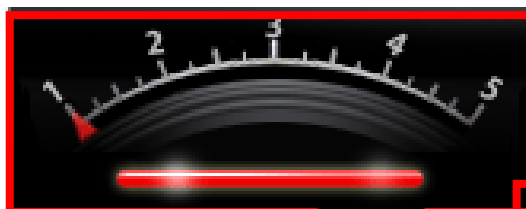
「クライアント/サーバ」+ Webコンソールで、よりリッチなセキュリティ対策をご提供します。



ISM管理コンソール

①まずは、全体のセキュリティレベルのチェックから！

ISMメニュー



- ☒ 脆弱性があるパソコン
- ☒ 基本ソフトの安全対策未実施のパソコン
- ☒ ウイルス対策未実施のパソコン
- ☒ 禁止ソフトウェアを保有しているパソコン

②セキュリティレベルが下がっていたら、問題を確認！

IT Security Manager (ISM) - Microsoft Internet Explorer

Quality Corporation

ログイン名: Eism0001

基本ソフトの安全対策未実施のパソコン

※ 2008/03/05時点

CSV出力(一覧) CSV出力(詳細)

No	ホスト名	ユーザ名	部署	OS	SP	Ver.	ブラウザ	Ver.
1	IBB168	岡部幸雄	SLT	Microsoft Windows 2000 Professional	4	5.0.2195	InternetExplorer6.0	6.0.2800.1106
2	IBB172	森 裕一	ISB	Microsoft Windows 2000 Professional	4	5.0.2195	InternetExplorer6.0	6.0.2800.1106
3	IBB175	松坂大輔	BRS	Microsoft Windows XP Professional	2	5.1.2600	InternetExplorer6.0	6.0.2800.1106
4	IBB185	打味一範	ISB	Microsoft Windows 2000 Professional	4	5.0.2195	InternetExplorer6.0	6.0.2800.1106
5	IBB206	岡新太郎	本社営業グループ	Microsoft Windows XP Professional	2	5.1.2600	InternetExplorer6.0	6.0.2800.1106
6	IBB209	大塚 祐輔	SLT	Microsoft Windows XP Professional	2	5.1.2600	InternetExplorer6.0	6.0.2800.1106
7	TOB064	木下 昂男	LAT	Microsoft Windows 2000 Professional	4	5.0.2195	InternetExplorer6.0	6.0.2800.1106

③脆弱性を特定！

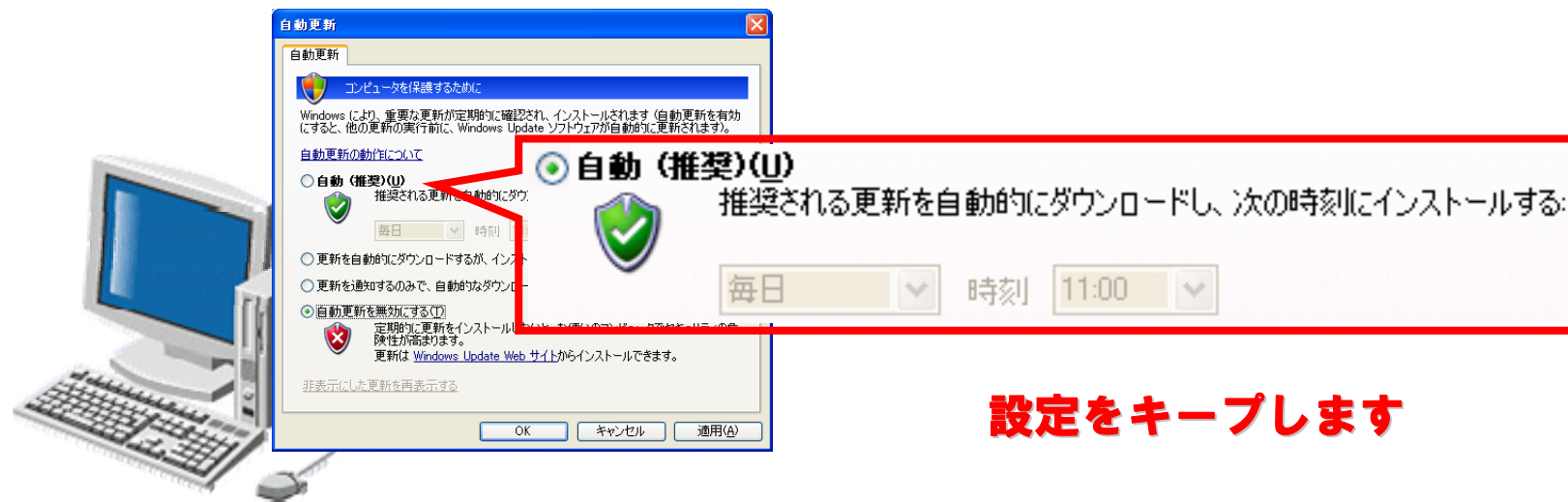
セキュリティ対策状況把握

- 収集したインベントリからセキュリティレベル診断
OS、ウイルスワクチン、不正ソフト、ISM運用状況から診断
- 「セキュリティ辞書」は、デイリー更新



セキュリティパッチ更新対策

- PCのWindows Updateの自動更新設定を変更
- 変更指示の確認をクライアントPCから定期的に実施
- セキュリティレベルの維持を実現

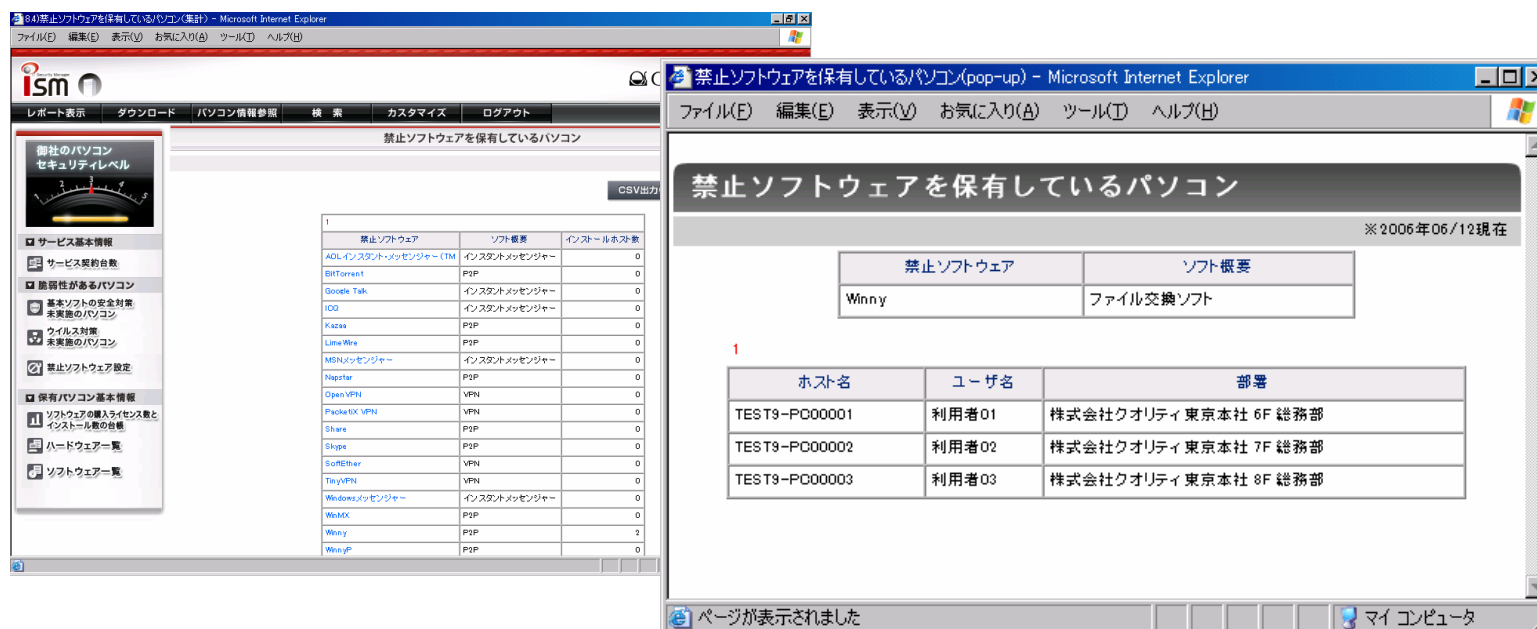


設定をキープします

不正ソフト検出 & レポート

WEBコンソール上で、クライアントPCにインストールされた不正ソフトをレポーティングします。

- WinnyやShare等のインストール状況が把握できます。
- 社員の自宅PCの状況も把握可能



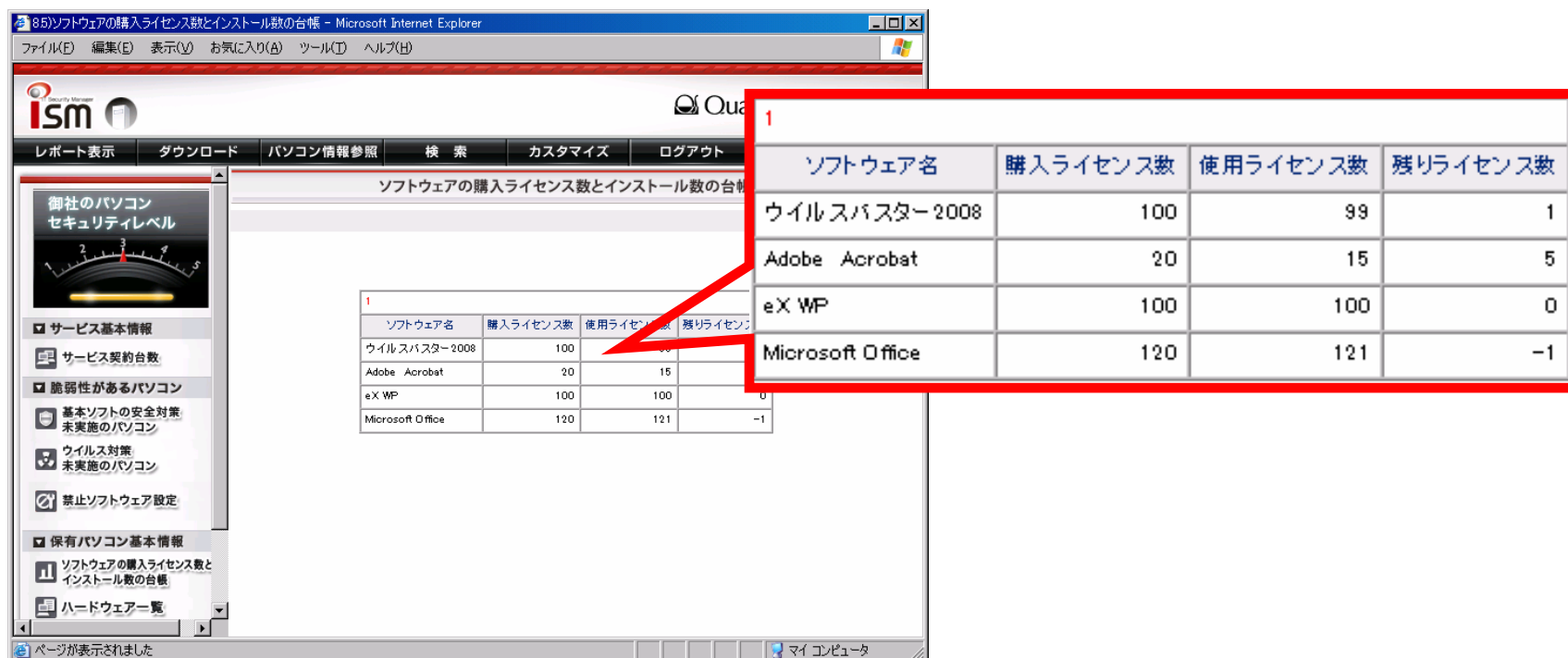
The screenshot displays the ISM Web Console interface. The main window shows a list of detected unauthorized software. A pop-up window titled '禁止ソフトウェアを保有しているパソコン' (PCs holding prohibited software) provides a detailed view of the detected software.

禁止ソフトウェア	ソフト概要	インストールホスト数
Winny	ファイル交換ソフト	0

ホスト名	ユーザ名	部署
TEST9-PC00001	利用者01	株式会社クオリティ 東京本社 6F 総務部
TEST9-PC00002	利用者02	株式会社クオリティ 東京本社 7F 総務部
TEST9-PC00003	利用者03	株式会社クオリティ 東京本社 8F 総務部

ライセンス管理レポート

- ライセンス利用状況のレポートニング
- インストール数と購入ライセンスを比較

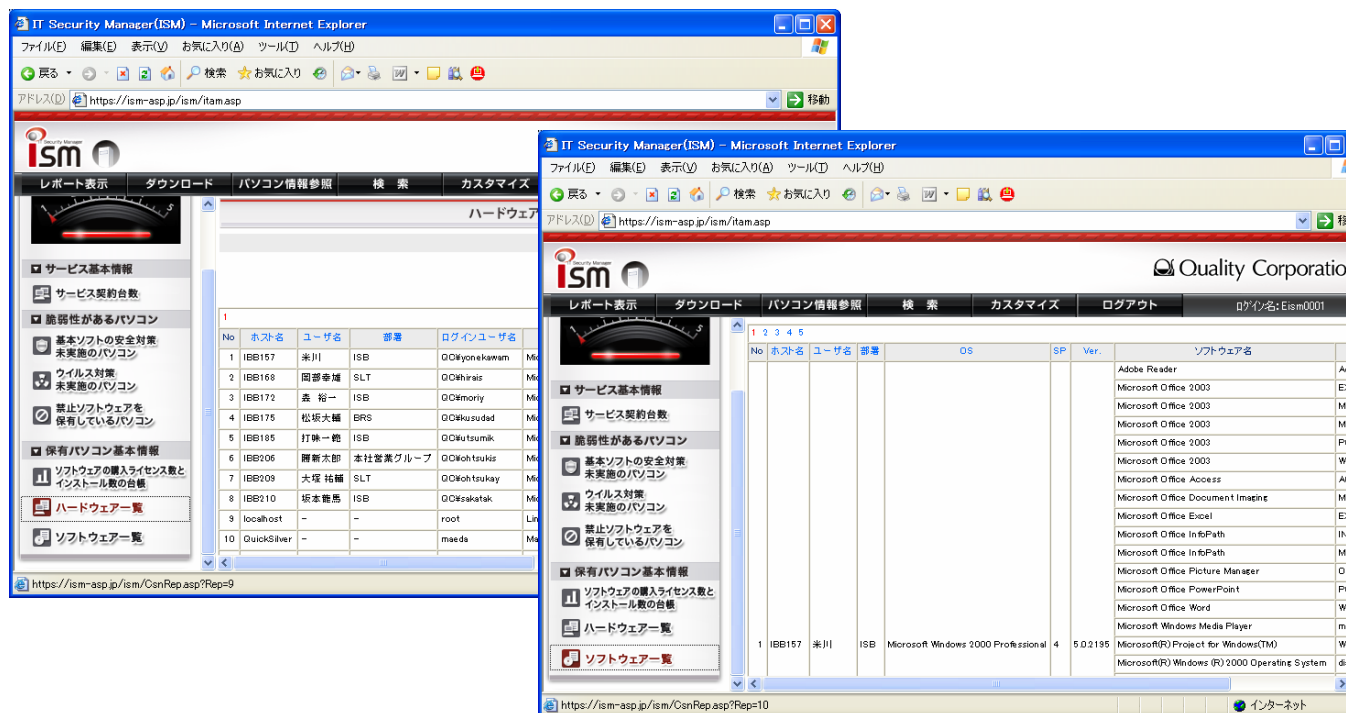


The screenshot shows the ISM (IT Security Manager) interface in a Microsoft Internet Explorer browser window. The main content area displays a table titled "ソフトウェアの購入ライセンス数とインストール数の台帳" (Software Purchase License and Installation Count Ledger). A red box highlights a portion of this table, and a red arrow points from the table to a larger, detailed view of the same data.

ソフトウェア名	購入ライセンス数	使用ライセンス数	残りライセンス数
ウイルスバスター2008	100	99	1
Adobe Acrobat	20	15	5
eX WP	100	100	0
Microsoft Office	120	121	-1

ハードウェア・ソフトウェアレポート

- 収集したインベントリ情報からレポート作成
WEBコンソールにより、7つのレポートをご提供
SSL通信でのセキュアな接続が可能

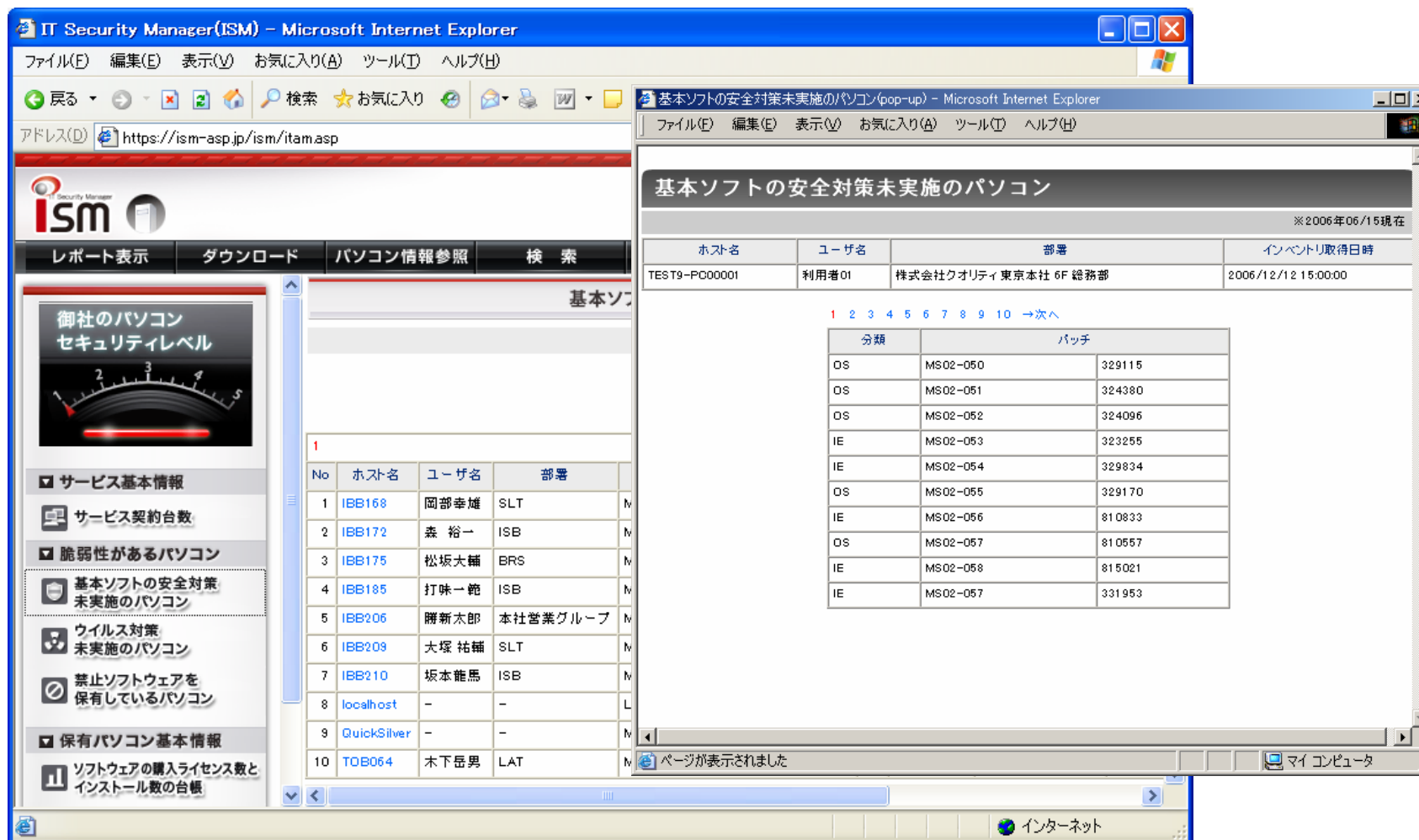


The screenshot displays the IT Security Manager (ISM) web console interface, which is accessible via a Microsoft Internet Explorer browser. The console is divided into several sections:

- Left Sidebar:** Contains navigation links for various reports, including 'サービス基本情報' (Service Basic Information), 'サービス契約台数' (Service Contract Count), '脆弱性があるパソコン' (Vulnerable PCs), '基本ソフトの安全対策' (Basic Software Security Measures), 'ウィルス対策' (Virus Protection), '禁止ソフトウェアを保有しているパソコン' (PCs with Prohibited Software), '保有パソコン基本情報' (Basic Information of Existing PCs), 'ソフトウェアの購入ライセンス数とインストール数の台数' (Number of Purchased Licenses and Installed Software), 'ハードウェア一覧' (Hardware List), and 'ソフトウェア一覧' (Software List).
- Main Content Area:** Displays two reports:
 - Hardware Report (ハードウェア):** A table listing 10 PCs with columns for No., Host Name, User Name, Department, and Login User Name. The data includes entries like IBB157, IBB158, IBB172, etc.
 - Software Report (ソフトウェア):** A table listing software installed on the PCs, with columns for No., Host Name, User Name, Department, OS, SP, Ver., and Software Name. The data includes entries like Adobe Reader, Microsoft Office 2003, Microsoft Office Access, etc.
- Top Navigation Bar:** Includes links for 'レポート表示' (Report Display), 'ダウンロード' (Download), 'パソコン情報参照' (PC Information Reference), '検索' (Search), 'カスタマイズ' (Customize), and 'ログアウト' (Logout).

基本ソフトの安全対策未実施のパソコンレポート

WindowsOSのセキュリティパッチの適応状況の確認を行います。



The screenshot shows the IT Security Manager (ISM) web interface in Microsoft Internet Explorer. The main window displays a report titled "基本ソフトの安全対策未実施のパソコン" (PCs with unimplemented security measures for basic software). The report includes a table with columns for Host Name, User Name, Department, and Inventory Acquisition Date. Below this, there is a detailed table of security patches for various operating systems and applications.

ホスト名	ユーザ名	部署	インベントリ取得日時
TEST9-PC00001	利用者01	株式会社クオリティ 東京本社 6F 総務部	2006/12/15 00:00

分類	パッチ	バージョン
OS	MS02-050	329115
OS	MS02-051	324380
OS	MS02-052	324096
IE	MS02-053	323255
IE	MS02-054	329834
OS	MS02-055	329170
IE	MS02-056	810833
OS	MS02-057	810557
IE	MS02-058	815021
IE	MS02-057	331953

ウイルス対策ソフト更新未実施のパソコンレポート

ウイルス対策ソフトのパターンファイルの状況やインストール状況を確認します。

対応製品:
TrendMicro社
Symantec社
MacAfee社

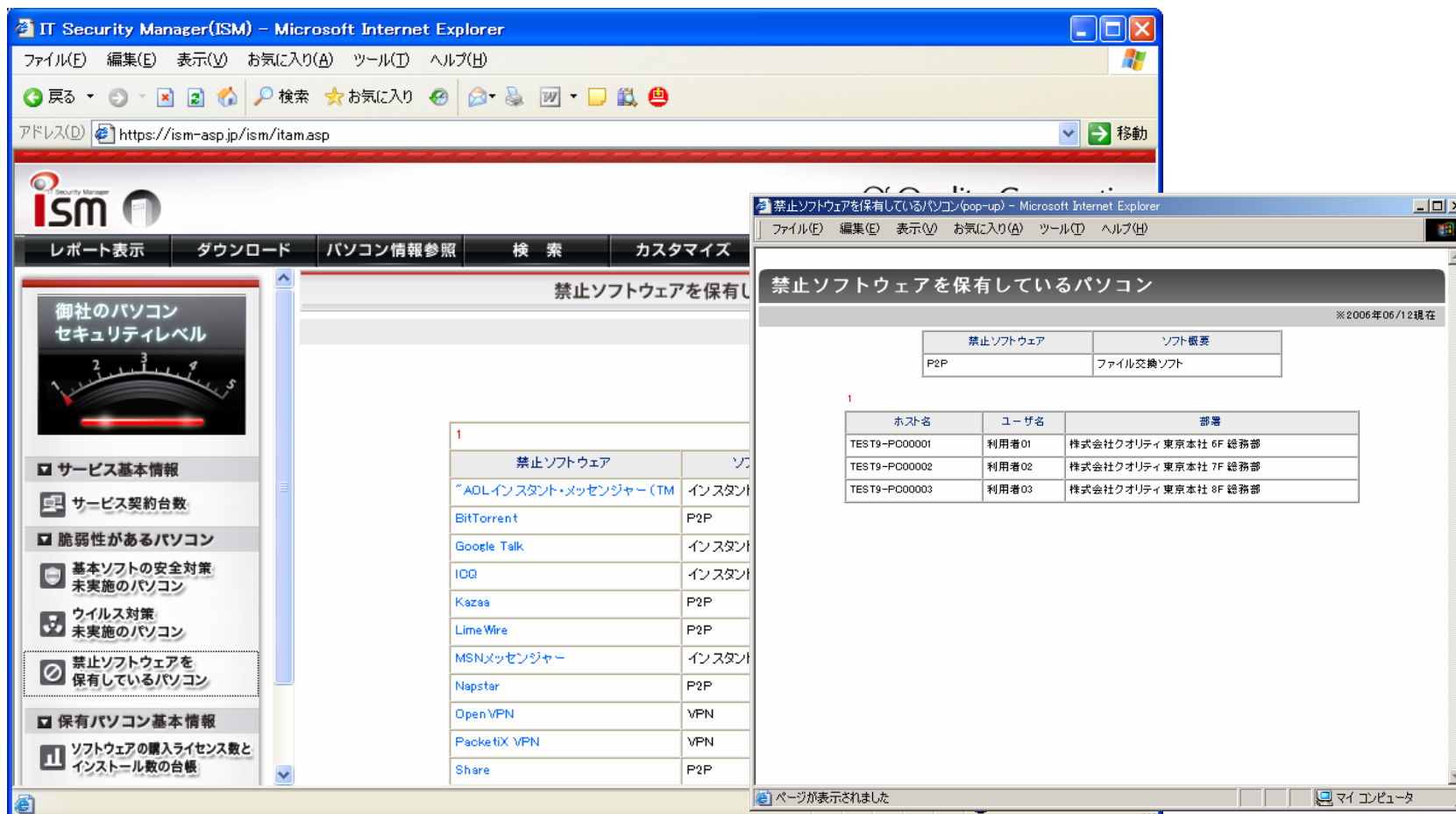


The screenshot shows the IT Security Manager (ISM) web interface in Microsoft Internet Explorer. The page title is "ウイルス対策未実施のパソコン" (PCs with no virus protection implemented). The report is dated 2008/02/21. A table lists the details of these PCs, including host names, user names, departments, and the status of virus protection software.

No	ホスト名	ユーザ名	部署	ウイルス対策ソフト	Ver.	エンジンVer.	パターンVer.	メール
1	IBB206	勝新太郎	本社営業グループ	VirusBuster Corporate Edition 7.3/NT	7.3.0.1034	8.550-1001	495300	-
2	IBB209	大塚 祐輔	SLT	VirusBuster Corporate Edition 7.3/NT	7.3.0.1034	8.550-1001	494500	-
3	IBB210	坂本龍馬	ISB	VirusBuster Corporate Edition 7.3/NT	7.3.0.1034	8.550-1001	510700	-
4	localhost	-	-	-	-	-	-	-
5	QuickSilver	-	-	-	-	-	-	-
6	TOB064	木下岳男	LAT	VirusBuster Corporate Edition 7.3/NT	7.3.0.1034	8.550-1001	511100	-

禁止ソフトウェアを保有しているパソコンレポート

社内ポリシーで認めていないソフトウェアの利用状況を確認します。



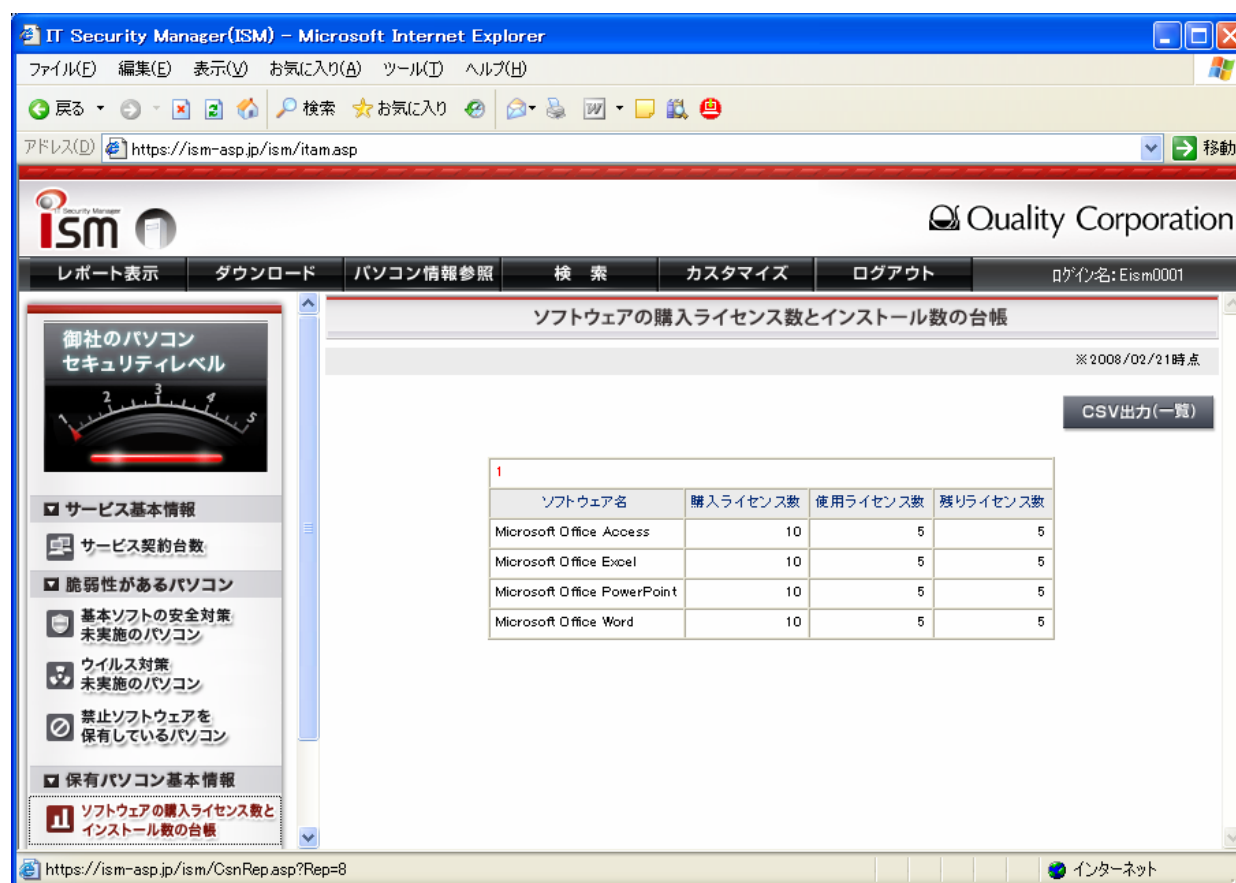
The screenshot displays the IT Security Manager (ISM) web interface in Microsoft Internet Explorer. The main window shows a report titled "禁止ソフトウェアを保有しているパソコン" (PCs holding prohibited software). The report includes a table with columns for Host Name, User Name, and Department, listing several test users and their associated departments.

ホスト名	ユーザ名	部署
TEST9-PC000001	利用者01	株式会社クオリティ 東京本社 6F 総務部
TEST9-PC000002	利用者02	株式会社クオリティ 東京本社 7F 総務部
TEST9-PC000003	利用者03	株式会社クオリティ 東京本社 8F 総務部

Below the main report, there is a detailed table of prohibited software installed on the PCs, including applications like AOL Instant Messenger, BitTorrent, Google Talk, and various P2P and VPN software.

ソフトウェアの購入ライセンス数とインストール数のレポート

ソフトウェアのライセンス数と実際にインストールされている数字をつき合わせて、ライセンス違反を確認します。

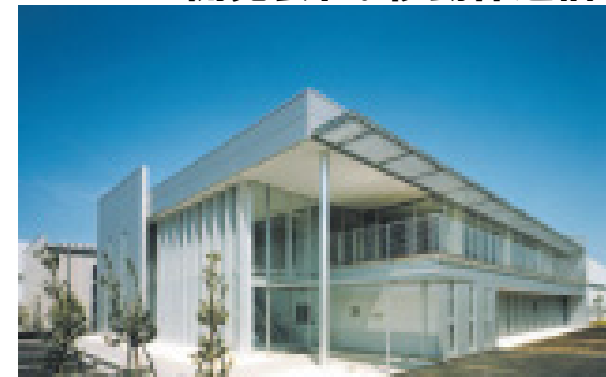


The screenshot shows the IT Security Manager (ISM) web interface in Microsoft Internet Explorer. The browser address bar shows the URL: <https://ism-asp.jp/ism/itam.asp>. The page title is "IT Security Manager(ISM) - Microsoft Internet Explorer". The interface includes a navigation menu with options like "レポート表示", "ダウンロード", "パソコン情報参照", "検索", "カスタマイズ", and "ログアウト". The main content area displays a report titled "ソフトウェアの購入ライセンス数とインストール数の台帳" (Software Purchase License and Installation Count Ledger) as of 2008/02/21. A table lists software names, purchase license counts, usage license counts, and remaining license counts.

ソフトウェア名	購入ライセンス数	使用ライセンス数	残りライセンス数
Microsoft Office Access	10	5	5
Microsoft Office Excel	10	5	5
Microsoft Office PowerPoint	10	5	5
Microsoft Office Word	10	5	5

ISM導入事例 (株)ステップ様

- 導入の背景
内部統制の関係上、取引先へのセキュリティチェックシート提出が義務化
- 導入の目的
セキュリティの向上と管理・運用工数の低減を実現
- メリット
ツール導入の障壁である、コスト面がクリアできた。
- シナジー
自社開発のツールとのマッシュアップで管理・運用工数も大幅に低減
- 今後
将来は海外拠点にも導入をしていきたい。
- (株)ステップ様コーポレートプロフィール
神奈川県横須賀市に本社を構える従業員数80名というソフトウェア開発会社。移動体通信関連ソフトウェア開発を主とし「基地局ソフトウェア開発」「携帯端末ソフトウェア」を2本柱に事業を展開。1986年の設立以来、技術力の高さを背景に、コンピュータネットワークや移動体通信の拡大という追い風にも乗り、順調に業務を拡大中。2004年には中国・南京に合併で開発拠点を開設し、広大な中国市場の展開も視野に入れた活動を行っている。



ISM導入事例 (株)アドバネクス様

- **導入の背景**
作業工数の増大が課題!手作業での管理は限界に
 - **導入の目的**
機器は設置せずに必要なサービスだけを利用したい
 - **導入効果**
潜在的なニーズ応え、システム管理者の精神的な負担も大幅に軽減できた
 - **今後**
内部統制の運用も視野にいれ盤石の体制を築く
-
- **(株)アドバネクス様コーポレートプロフィール**
は、1946年に設立して以来、精密ばね、精密組立部品、モーターなどの製造販売を主な事業としており、高度な技術・ノウハウを蓄積している企業としても知られている。従業員数は単体で470名弱、連結で3400名弱、資本金は34億5161万円という企業だ。柏崎工場や福島工場のほか、コンビニプラント、試作センターなど日本国内に拠点を設けているほか、多くのグループ企業も抱え、海外とのつながりも深い。
最近では、ファクスやプリンタといったOA機器向けや自動車関連部品、携帯電話向けのヒンジなどが順調に推移している。



DKS for SaaSについて

「ファイルは流出するもの」を前提とした対策！

➤ **ファイル単位にアクセス権を設定**

- ✓ 6つの権限設定が可能
(読み込み・印刷・コピー・注釈・取出し・添付)
- ✓ スクリーンショットも不可
- ✓ 公開期間の設定が可能
- ✓ ファイル配信後でもアクセス権の変更可

➤ **文書の閲覧ログを取得**

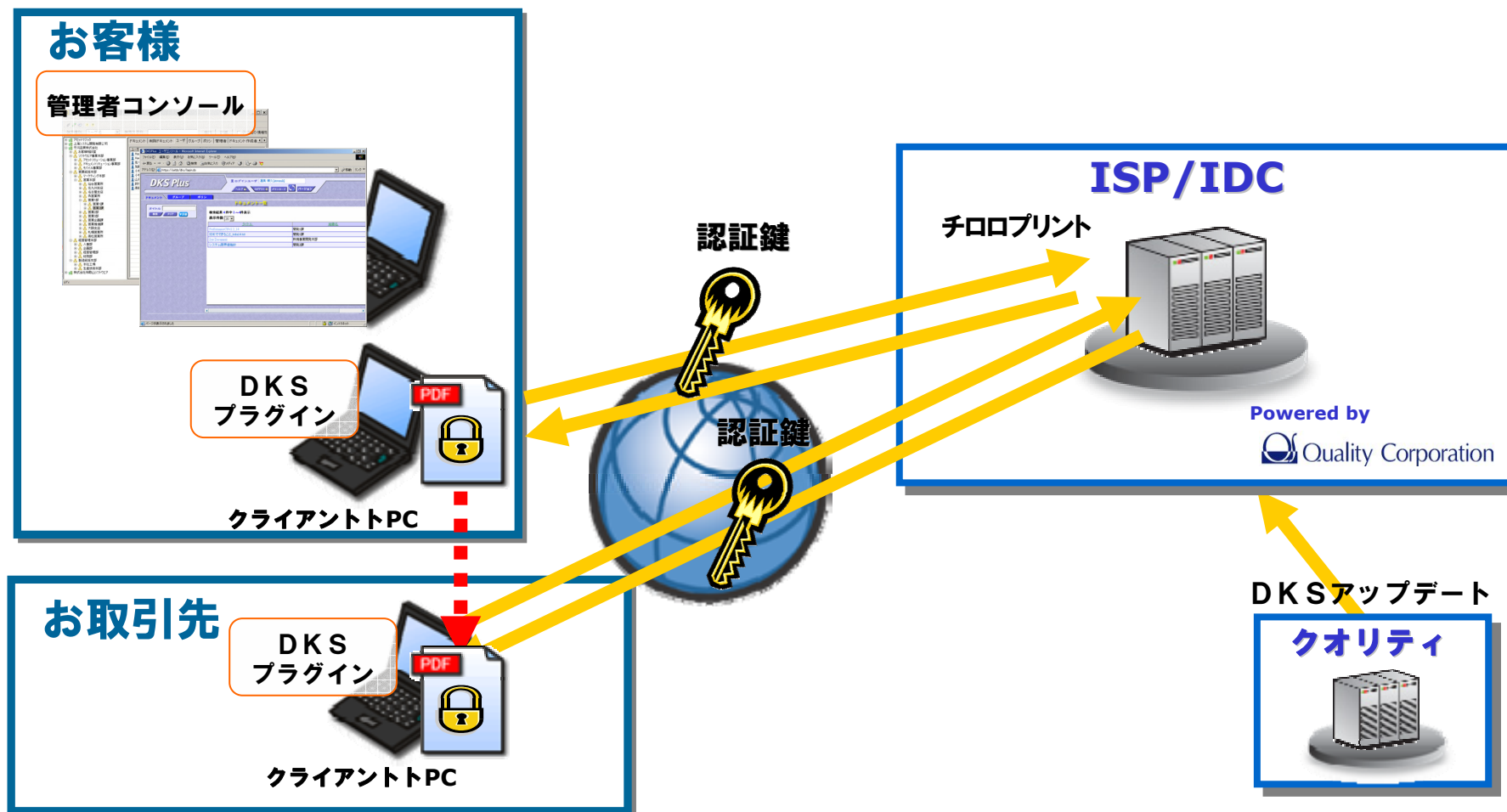
- ✓ 権限所有者の行動を把握

➤ **B to Bでの利用**

- ✓ 様々なビジネスシーンでセキュアな情報提供



DKS for SaaS サービス提供の仕組み



DKS for SaaS ユーザオペレーション

Acrobat Reader - [TCO.pdf]

ファイル(F) 編集(E) 文書(D) ツール DKS(K) 表示(V) ウィンドウ(W) ヘルプ(H)

81%

社外秘

IT資産管理・情報システムの価値を確認すること

各業務の売出しにより問題点の絞り込みから始める。

この診断に加えて、これまでに投資してきた資産とその維持費用・管理費の人体費・エンドユーザの教育費も計算する。これにより、その合計費用コストを分析してみよう。この総費用コストが、TCO(Total Cost of Ownership)です。相対的評価のもとにおいて、TCOのうち無駄と思われる部分を削減の対象と考え、目標を明確にし、対応していくことが重要です。

次に考えることは、ここで立てた目標を達成するためのツールの選定です。目的にあったツールの選定が、TCO削減の鍵になります。しかしツールを導入すれば、解決する訳ではありません。ツールを活用して業務の改善をするには、ツール以外にも、運用のルールなどユーザに明確に提示することが必要です。また、常に変化していく状況を管理することになるために、運用は、段階的プロセスでなければならぬです。

IT資産管理の段階的改善

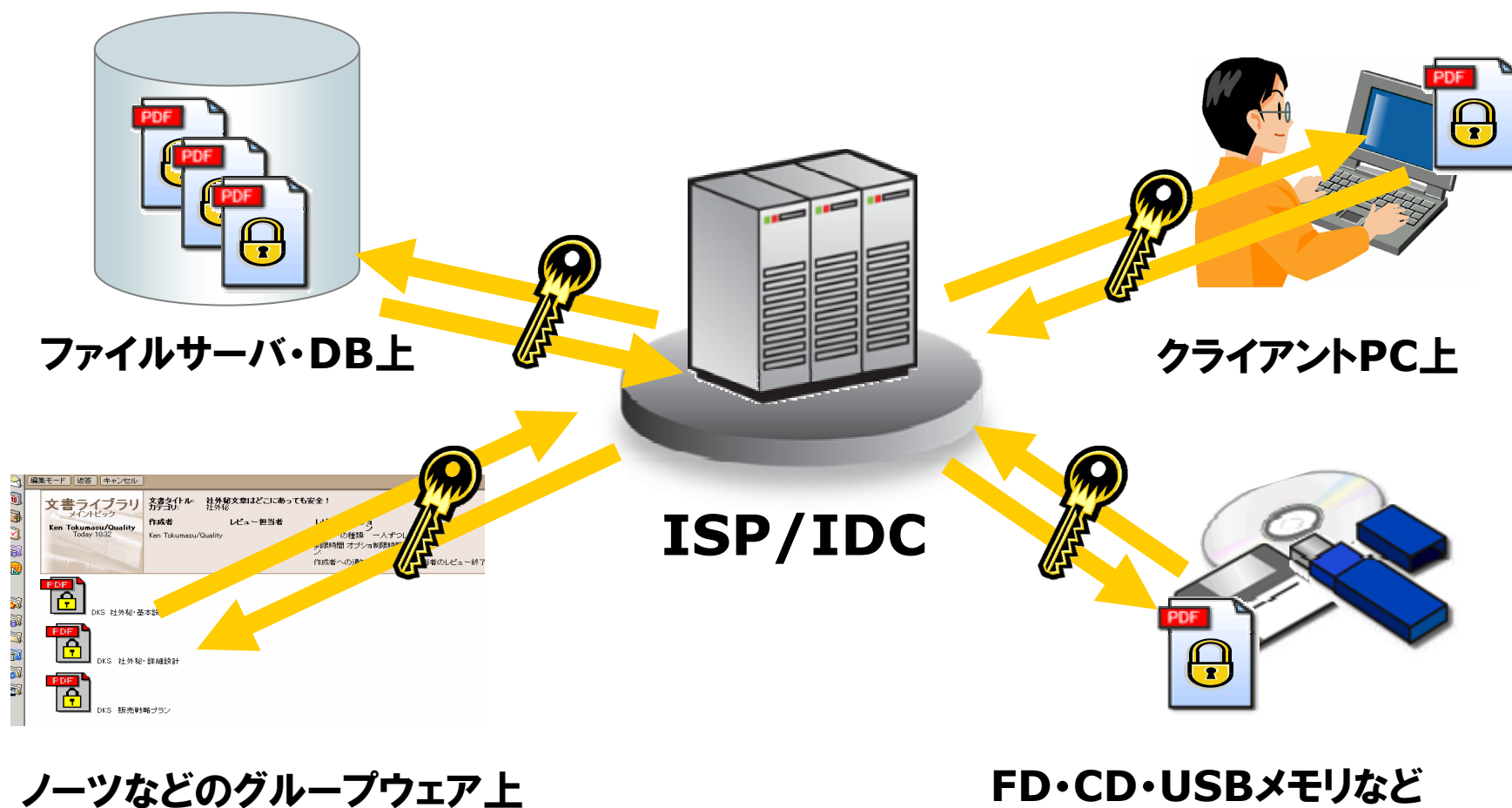
TCOの要素は主に、「資産」、「管理」、「エンドユーザオペレーション」、「テクニカルサポート」という四つの分野から構成されています。そして、そこから派生する「業務の要素」として「トラブルによる業務上の機会損失」も認識しておく必要があります。下記に示す表は、項目別の業務内容とそれに対する解決ツールの紹介です。この表に基づいて項目別に解決していきます。

- 資産
- テクニカルサポート
- 管理
- エンドユーザオペレーション

項目	内容	解決ツール
管理	インベントリ管理(ハード/ソフト) アドレス管理(IP/メール) ソフトウェア配布 ライセンス管理 管理台帳作成	資産情報の収集、管理 IPやメール等、変更ことの管理 新規、VerUp、や必要のない GetUp ライセンス管理、管理工数の削減 資産情報と発注の連携
資産	ハードウェア購入費用 ソフトウェア購入費用 ネットワーク費用	利用されているハードウェアの発見 管理コストでの購入、不要ソフト検出 利用権限管理
エンドユーザ オペレーション	データ管理・ファイルの連携 新業務な設定変更によるトラブル 標準的なソフトウェアインストール 独自知識によるトラブル診断 独自セキュリティポリシーの活用	ファイルの保存先指定 コントロールパネルの使用制限 利用プログラムの制御 統一連携の徹底 統一したセキュリティの提供
テクニカル サポート	クライアントへのリモートコントロール 所蔵されたファイルの転送 日常からのネットワーク監視	トラブルへの即時対応 遠隔地でもネットワーク経由で故障 エラーパケット監視で障害、早期発見
トラブルによる業務上の 機会損失	上記のトラブルによるシステム利用ができなかった時間帯の営業的機会損失	危険な操作の制限の設定 ネットワークの常時監視で問題点の早期発見とキャパシティ拡張

1/1 182 x 257.2 ミリ

DKSファイルのセキュリティは場所に依存しません



クオリティSaaSビジネスの方向性

発見 管理 & 監視

ITを利用した企業活動におけるセキュリティリスクの発見や監視ソリューションを提供させます。

報告 レポート & アラート

発見したリスクを、分かりやすく見易い形で提供します。インシデントの重要度によりアラートを上げる仕組みを提供します。

対策 自動修復

発生したインシデントに対し、なるべく管理者リソースが発生しない仕組みを提供します。

ASP・SaaS

導入が簡易なASP・SaaSモデルでのサービステリバリープラットフォームを提供します。

Coming Soon

ISM Main Engine

➤ ISM

セキュリティアラート機能
アプリケーション起動制御

ISM Extension Engine

➤ ISM GC (Green Computer)

クライアントPCの省電力設定の維持サービス

➤ ISM WP (Write Protector)

外部記憶媒体への書き出し制御

➤ ISM DW (Disk Watcher)

HDDの健康状態を監視サービス

➤ ISM TC (Trouble Care)

クライアントPCのトラブルを修復

➤ ISM International

海外対応版

※実際のリリースを確約するものではありません。

ISM GC

外出中に電源がついたままのPCを見かけます。セキュリティ上の問題もありますし、CO2削減という観点からも解決すべき問題点です。京都議定書では、1990年を基準として6パーセントの温室効果ガス削減が目標となっています。1990年当時のオフィスと比較して、PCの台数が急増した為に、それに比例して電力消費も急増しています。政府の調査結果からも分かるとおり「クライアントPCの電源管理」もオフィスの省エネ対策につながります。ISMの**グリーンPCソリューション**(Coming Soon)を利用すると、PCの電源設定をエコに保つことが可能です。

ソリューション適応前

PC台数	台当り電力消費量	トータル電力消費量
デスクトップPC: 600台	14KWh/1台月	8,400KWh
ノートPC: 400台	4KWh/1台月	1,600KWh
合計		10,000KWh

3,780kg-CO2

ソリューション適応後

PC台数	台当り電力消費量	トータル電力消費量
デスクトップPC: 600台	7KWh/1台月	4,200KWh
ノートPC: 400台	2KWh/1台月	800KWh
合計		5,000KWh

1,890kg-CO2

月間約1,890KgのCO2を削減
年間 CO2 約22.6t/電気代 約65万円を削減)

まとめ

- 人件費の面で、自社に専任管理者を置くのは困難
- 変化し続けるITインフラを管理し続けるのは困難
- ただ、セキュリティ事故は起こしたくない

- ✓ セキュリティ対策は**SaaS**で！
- ✓ 専門のベンダーへアウトソース

まずは1ヶ月間無料トライアルから！

http://www.quality.co.jp/products/ISM/ISM_trial_usr.html

