

導入事例

Active Directory 及び ファイルサーバ監査ソフトウェア導入

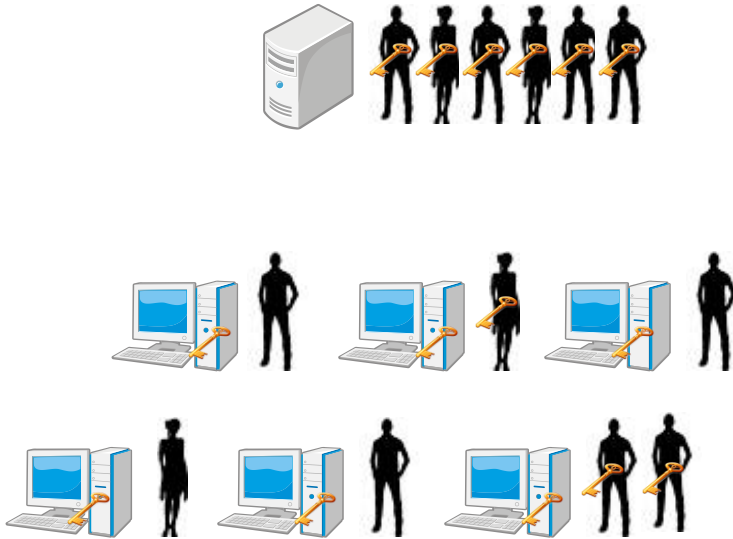
株式会社 セカンドオフィス

兵庫県神戸市中央区江戸町101 三共生興スカイビル
TEL 078(326)8818 FAX 078(326)8814

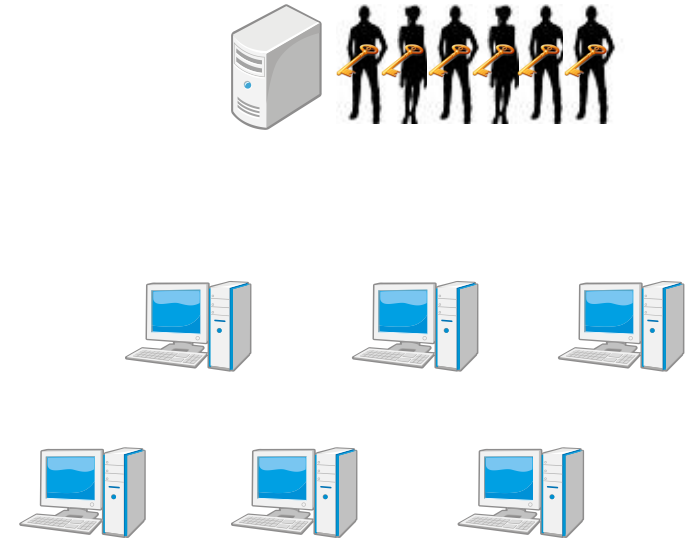
| | |
|---------|---|
| 件名 | Active Directory 及び ファイルサーバ監査ソフトウェア導入 |
| 業種 | 福祉サービス |
| 規模 | 50台 |
| 導入された製品 | Microsoft® Windows Server 2008 MOTEX LAN Scope CAT6 + Server CAT |
| 概要 | <p>お客様では多数のご利用者様やそのご家族の個人情報などを多く扱うため、それらのデータを漏えいから守ることは必須の課題でした。</p> <p>そのためActive DirectoryによるクライアントPCの管理、またサーバ上のファイルアクセス履歴を記録しそれに素早くアクセスできる環境を整備いたしました。</p> |
| | |

クライアントPC, ユーザ管理の向上

Active Directory導入前



Active Directory導入後



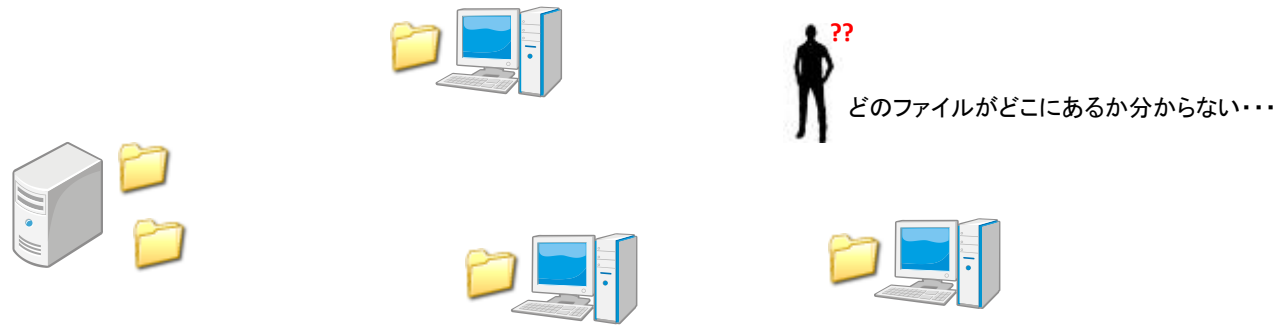
導入以前は、コンピュータに使用するログイン名、パスワードを個別に管理していました。また「使う人」と「使うPC」が決まっておらずそのために各クライアントPCとサーバの両方での管理が困難なために「パソコンで共通のログイン名を使う」「どのPCが、誰がどんなログイン名で利用しているか分からない」状態に陥っていました。

「必要な情報のみを必要な人間がアクセスできる」環境を作るためにはログイン名とパスワードの管理は必須です。

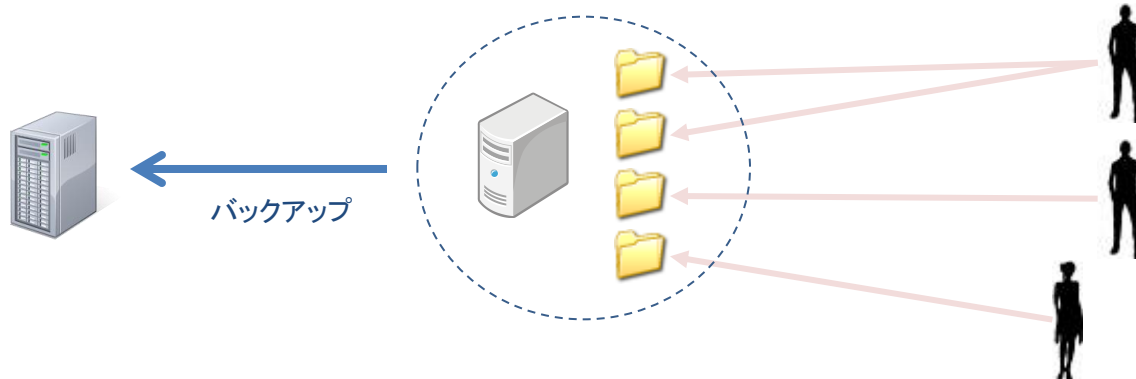
そのため、Active Directoryによって「誰がどのPCを使う」ときであっても「その人に与えられたログイン名しか使えない」環境を構築しました。またそのログイン名はサーバでの単一ポイントですべてを管理できます。

情報資産管理の向上

導入前



導入後



ログイン名の管理などを行うことで「仕事に使うファイルは全てサーバに置く」ルールを徹底できます。以前は全ての情報管理は各個人の裁量に委ねられていました。そのため、「バックアップは取れているのか」「担当が退職して欲しいファイルがどこにあるのかわからない」「勝手に持ち出していないか」などの問題が常に付きまとっていました。

サーバでファイルのルール付けされた管理をすることで、これらの問題をクリアします。

ファイルの操作ログの管理

The screenshot shows the LanScope Cat6 console interface. A table titled 'サーバファイル操作一覧 - FILESERVER01' displays file operation logs. Red callout boxes with arrows point to specific columns in the table, each with a question in Japanese:

- どのサーバに (Which server)
- どのユーザーが (Which user)
- どのIPアドレスで (Which IP address)
- どのPCから (Which PC)
- いつ (When)
- どのファイルに (Which file)
- どんなアクセスをしたのか (What access was performed)

| プライマリユーザ名 | クライアントユーザ名 | IPアドレス | ホスト名 | イベント時刻 | 状態 | ファイルパス | 操作 | アラーム種別 |
|----------------|------------|-----------------|---------|----------|----|------------------------------------|-------|--------|
| - | uchida | 192.168.102.208 | PC-0026 | 08:30:44 | 成功 | - | - | - |
| FILESERVER01\$ | uchida | 192.168.102.208 | PC-0026 | 08:40:44 | 成功 | F:\Shared Data\社外秘 | 読出 | 時間外 |
| FILESERVER01\$ | uchida | 192.168.102.208 | PC-0026 | 08:41:30 | 失敗 | F:\Shared Data\社外秘\顧客名簿\顧客リスト.xls | 読出 | 失敗 |
| - | uchida | - | - | 08:45:57 | 成功 | - | - | 切断 |
| FILESERVER01\$ | murai | 192.168.103.14 | PC-022 | 08:49:11 | 成功 | D:\共有\【社外秘】営業部\実績フォルダ\地区別売上げ実績.xls | 読出 | - |
| - | sudou | 192.168.102.209 | PC-0029 | 08:50:01 | 成功 | - | - | 接続 |
| FILESERVER01\$ | sudou | 192.168.102.209 | PC-0029 | 08:53:41 | 成功 | D:\共有\【社外秘】営業部\営業資料\最新営業資料.ppt | 読出 | - |
| FILESERVER01\$ | sudou | 192.168.102.209 | PC-0029 | 08:55:11 | 成功 | D:\共有\【社外秘】営業部\営業資料\最新営業資料.ppt | 読出 | - |
| FILESERVER01\$ | sudou | 192.168.102.209 | PC-0029 | 08:55:11 | 成功 | D:\共有\【社外秘】営業部\営業資料\最新営業資料.ppt | 読出/書込 | - |

Windows Serverの標準機能でもファイルへのアクセス履歴は取得・閲覧ができます。しかし、それらの操作は極めて難解かつ困難で、実質多くのユーザにとっては不可能なものです。

そのため専用のソフトウェアとして「MOTEX LAN Scope Cat」を導入しました。これにより「どのサーバの」「どのファイルに」「どのPCから」「誰が」「いつ」「何をしたか」を素早く確認することができ、万が一の漏えい時にも原因の特定を速やかに行うことができます。