PC ネットワークの管理活用を考える会

クライアント管理勉強会
第3回

IT 資産管理と情報セキュリティの第一歩

柳原秀基
hide3@yanagihara.cc

本日のお題

- IT マネジメントのために最低でも実施すべきクライアントPC の管理法を解説します。
- フリーソフトウェアなどを活用しつつ、クライアントPC 管理と、セキュリティレベル向上はどこまで可能になるか、参加者の皆さんと議論したいと考えています。

対象者とゴール

- 対象
  - IT資産管理が必要だが，どこから始めれば良いか迷っている方。
  - 最初から大きな予算が掛けられないので，最低限のIT資産管理を検討している方。
- ゴール
  - 最低限必要なIT 資産管理レベルを理解する。
  - IT資産管理に活用できるオープンソース or フリーソフトウェア，無償ツールを理解する。

アジェンダ

- IT資産管理の復習
- どのような業務が発生するか
- オープンソース，フリーソフトウェア，無償ツールなどを使って，何が自動化でき，何ができないか。

クライアントPC 管理のあるべき姿

- 管理者は単なるPC の手配屋ではない
  - 社内 PC の現状とユーザの IT リテラシーを把握し,
  - 組織が IT に求める役割を理解した上で,
  - 限られたリソースを有効活用し,
  - IT ガバナンスの確立に寄与すること。
- IT ガバナンスとは
  - 「企業が競争優位性の構築を目的として IT 戦略の策定及び実行を**コントロール**し、**あるべき方向へと導く**組織能力 」
  - 「企業が、IT に関する企画・導入・運営および活用を行うにあたって、すべての活動、成果および関係者を**適正に統制し**、**目指すべき姿へと導く**ための**仕組みを組織に組み込む**こと、または、組み込まれた状態」

ITガバナンスの 6 分野

IT ガバナンスの 6 分野	9 項目の取り組み
1．基本戦略	1-1．IT 利用の基本方針策定
	1-2．全体組織化の取り組み
2．推進体制	2-1．組織体制の確立
	2-2．人材の確保・配置
3．予算・実施計画・評価	3-1．予算・実施計画の策定
	3-2．評価の実施
4．調達・開発・運用	4．調達・開発・運用の管理
5．情報セキュリティ	5．情報セキュリティの確保
6．標準化・知識共有・人材育成	6-1．標準化・知識共有
	6-2．人材の育成

ITライフサイクルマネジメント

◆機器入替計画策定、予算確保
◆PC利用基準作成、導入PC標準仕様メニュー化

◆データ消去
◆廃棄
◆返却

◆機器発注
◆経理処理

◆障害切り分け応
◆予備機準備、発送
◆機器修理

◆PC キッティング
◆配送・設置
◆データ入替
◆資産登録

◆資産管理
◆セキュリティ対応
◆ヘルプデスク
◆棚卸し
◆ソフトウェア管理

想定する状況

- クライアントに Windows PC が使われている。
- クライアント PC の機種も OS もばらばら。
- Active Directory が導入されていない。
- Windows Update がユーザに委ねられている。
- PC やネットワークを私的に使うことは禁止しているが，実際は使われているかもしれない。

想定する状況

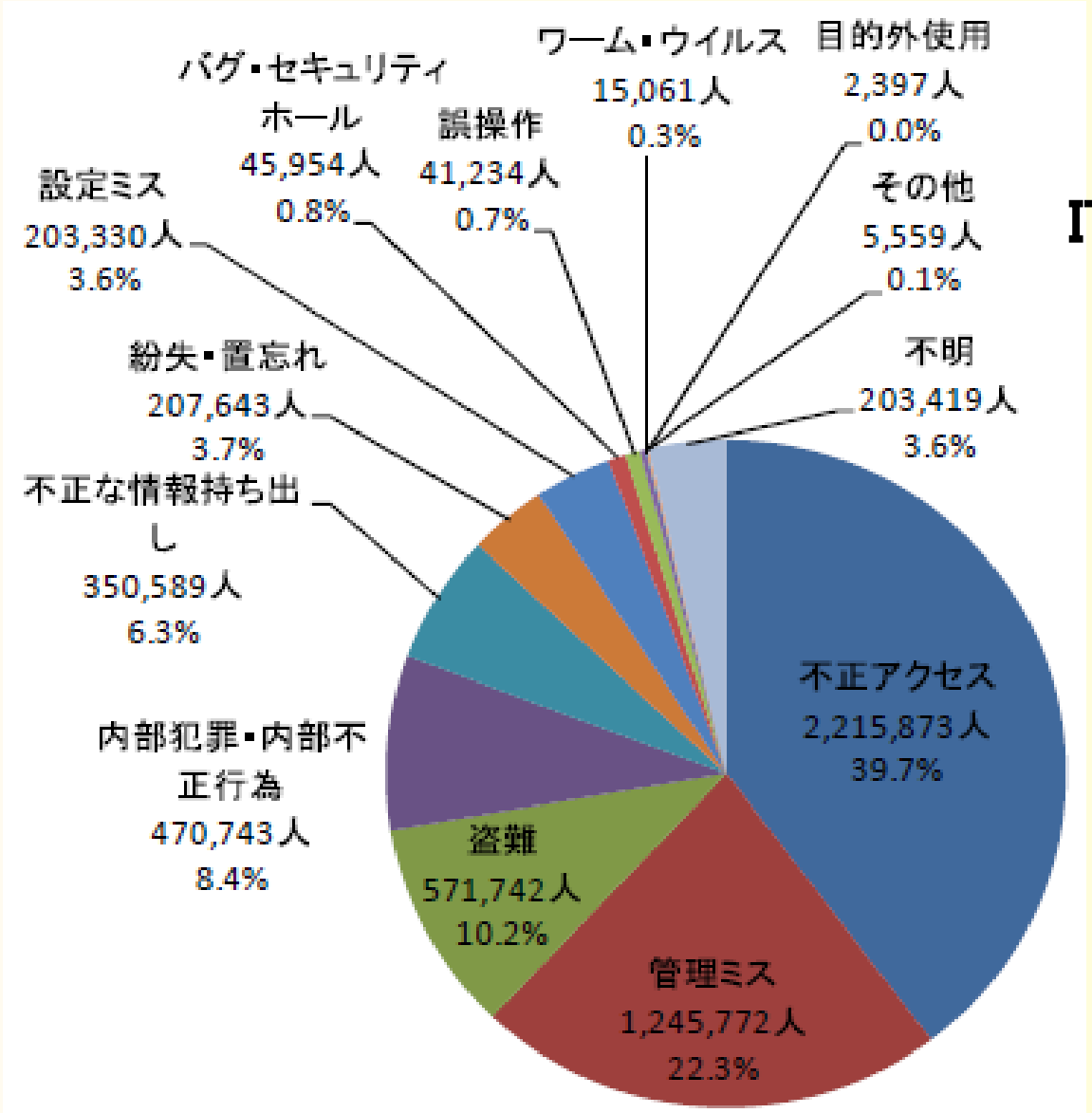
- クライアントに Windows PC が使われている。
- クライアント PC の機種も OS もばらばら。
- Active Directory が導入されていない。
- Windows Update がユーザに委ねられている。
- PC やネットワークを私的に使うことは禁止しているが，実際は使われているかもしれない。

問題点

- クライアントPCの現状が把握できない。
- ユーザが勝手にNASや私物PCをLANに接続する。
- Windows Updateによるホットフィックス適用状況が，リモートで分からない。
- ネットゲームで遊ぶユーザがいるようだが，いくら注意喚起しても止まらない。

- 要するに，ほぼ一般家庭の延長線。

個人情報漏えいの原因（人数比）



IT資産管理による対策項目

・管理ミス
・盗難
・内部犯行・内部不正
・不正な情報持ち出し
・紛失・置忘れ

JNSA「2010年 情報セキュリティインシデントに関する調査報告書」
http://www.jnsa.org/result/incident/2010.html

最低でも実施すべき
クライアントPC 管理

- IT 資産の「見える化」
  - PC のハード，ソフト・NAS・Printer の見える化
  - 台帳化と迅速な更新，人との紐付け。
- ホットフィックス適用の確認
  - リモートチェック
- 情報漏えい対策と私的利用の抑制
  - PC 操作ログの取得による，不自然な操作の抑止。
  - クライアントPC スクリーンショットの取得。
- リモート操作を可能に

フリーソフトでどこまで出来る？

- フリーソフトを駆使する
  - データベースは作らない。
  - 属人的なデータは，手入力する。
- bat ファイル，WSH スクリプトを駆使する。
  - データはテキストで入手。あとは Excel でごにょごにょ・・
- キーロガーとスクリーンショット取得で，ユーザの無茶を抑止。

IT 資産の「見える化」

- e-Inventory IT 資産管理
  - http://www.vector.co.jp/soft/dl/winnt/net/se468072.htm
  - クライアント PC 側にはエージェント不要。
  - 手作業で追加 IT 資産情報を入力できる。
  - NAS, Printer なども探索できる。
- 用途
  - とりあえず，PC の一覧データを入手し，CSV 化。
  - 定期的に実行しておくと，勝手に接続された PC や NAS を発見できる。
  - memo 欄を活用すれば，リースやレンタル管理も可能？

e-Inventory

		Status	Computer	IP	MAC	ComputerExp	Platform	PlatformVersion	Memo
1		on	AKIYAMA	192.168.1.1	00:00:00:00:00:00	Akiyama's PC	Windows	5.1	レンタル品
2		on	AKAGI	192.168.1.2	00:00:00:00:00:00		Windows	5.1	レンタル品
3		on	ABC-SV	192.168.1.3	00:00:00:00:00:00	ABCプロジェクトサーバ	Windows [MASTER]	5.2	資産 0010023
4		on	AKAGI-NOTE	192.168.1.5	00:00:00:00:00:00	Akagi's Note	Windows	5.1	レンタル品
5		on	APPMAIN	192.168.1.6	00:00:00:00:00:00		Windows	5.1	レンタル品
6		on	ASAKA	192.168.1.7	00:00:00:00:00:00	作業用	Windows	5.1	レンタル品
7		off	BACKUPSV	192.168.1.8	00:00:00:00:00:00	Backup:CentOS5.1	UNIX		資産 0010024
8		on	CHERRY	192.168.1.9	00:00:00:00:00:00	資料格納用	Windows	5.2	資産 0010025
9		off	GROGRO	192.168.1.10	00:00:00:00:00:00	ドキュメントサーバ	Windows	5.1	資産 0010025
10		on	COSMOS	192.168.1.11	00:00:00:00:00:00		Windows	6.0	レンタル品
11		on	XX-PC01	192.168.1.21	00:00:00:00:00:00	XXプロジェクト用端末XP	Windows	5.1	レンタル品
12		off	XX-PC02	192.168.1.22	00:00:00:00:00:00	XXプロジェクト用端末VISTA	Windows	6.0	レンタル品
13		on	OKI C830DN	192.168.1.30	00:00:00:00:00:00		Printer		XXリース(地下)
14		on	EPSON-S5000	192.168.1.31	00:00:00:00:00:00		Printer		XXリース(2F)
15		off	FUJI	192.168.1.32	00:00:00:00:00:00	Fuji's PC	Windows	5.1	レンタル品
16		on	GORI	192.168.1.33	00:00:00:00:00:00	Gori's PC	Windows	5.1	レンタル品

検出精度を期待するな

- PC 台帳一覧を作成する手助けに。
  - 検出→ csv ファイル→ Excel
- リース，レンタル，使用者などの情報は手入力。
- 定期的に実行しておくと，無断で設置された Printer や NAS などを検出できる（可能性有）。
-

オープンソースの
IT 資産台帳管理システム

- SARMS
  - http://www.sarms.jp/
- ISO/IEC 19770-1，JIS X 0164-1，SAMAC ソフトウェア資産管理基準及びソフトウェア資産管理評価規準に準拠したソフトウェア資産管理（SAM）を行うための、オープンソースの IT 資産台帳管理システム。
- インベントリツールではなく、組織における資産の状況を登録する台帳である。

Sysinternals の活用

IT 資産管理に活用するツール

- PsTools
  - すべてがコンソールユーティリティ。
    - バッチファイルからの実行が容易。
    - 実行結果は標準出力へ。
  - ローカルとリモートコンピュータを操作できる。
    - リモートコンピュータへクライアントソフトウェアのインストールは不要。
  - 実行時の資格情報を指定できる。
    - リモートコンピュータの管理者権限で実行可能。

注意点

- PsTools がマルウェアとして検出される可能性
  - PsExec が不正使用され，マルウェア本体に組み込まれた事がある。
- サポート対象
  - WindowsXP, Windows Vista, Windows 7(x86,x64)
  - Windows Server 2003, Windows Server 2008, Windows Server 2008R2(x86,x64,IA-64)
  - 64 ビット環境では WOW64 が必要

PsTools のユーティリティ

- PsExec
  - リモートでプロセスを実行。結果のリダイレクトが可能。
- PsFile
  - リモートコンピュータから開いているファイルを確認。
- PsInfo
  - ローカル・リモートコンピュータのシステム情報。
- PsList
  - プロセスの情報を表示。

PsTools のユーティリティ

- PsLoggedOn
  - ローカルログオン，リモート接続ログオンしているアカウントを表示。
- PsLogList
  - イベントログをダンプ。
- PsPassword
  - ローカル，リモートコンピュータのパスワード変更。
- PsShutdown
- PsSuspend

PsExec でできることの例

- 指定したリモートコンピュータ上，またはローカルコンピュータ上で，コマンドプロンプトでの操作が可能。
  - psexec \\ コンピュータ名 cmd.exe /accepteula
  - リモートコンピュータ上の GUI は返って来ない事に注意が必要。
- リモートコンピュータへバッチファイルを送り，実行させる。
- 複数コンピュータを一気にリモート操作可能。
  - psexec \\ server1,server2,sever3 ・・・・
  - コンピュータ名をテキストファイルから読み込み可能

ユーザアカウント制御（UAC）の問題

- Windows XP，Windows Server 2003 では，管理者アカウントで全て実行可能。
- Windows Vista 以降
  - UAC が導入されている。
  - 対話的にログオンする以外に，管理者としてネットワーク接続，ログオンする方法は無い。（ドメインアカウントは除く）
- よって，ドメインアカウントが使えない場合，LocalAccountTokenFilterPolicy を設定し，UAC リモートの制限を無効にする必要がある。（サポート技術情報 951016 ）
  http://support.microsoft.com/kb/951016/ja#fixit4me

インベントリ情報の収集

- ハードウェア
  - PsInfo からの情報を収集する。→ Excel へ
  - X64 ではメモリ容量の取得ができない。
- インストールされているソフトウェアの一覧
  - Psinfo –s
- CSV 形式での出力
  - Psinfo オプション –c

ホットフィックス適用の確認

- 基本
  - C:¥> wmic qfe > hotfix.txt
  - Systeminfo で得られるホットフィックス一覧は信用できない。
  - PsInfo によるホットフィックス一覧は不安定
  - 「プログラムの追加と削除」や「プログラムと機能」で提供される履歴情報は、「 Windows Update Agent (WUA)」の COM API を使用することで取得が可能。
  - つまり，WSH などでプログラムを作ればいい！

WSH によるホットフィックスの確認

```
"SearchUpdate.vbs
'
Set arg = WScript.Arguments
SearchString = arg(0)
Set objSession = CreateObject("Microsoft.Update.Session")
Set objSearcher = objSession.CreateUpdateSearcher
intCount = objSearcher.GetTotalHistoryCount
If intCount > 0 then
  Set colHistory = objSearcher.QueryHistory(0, intCount)
    WScript.Echo "Date Title"
    WScript.Echo "---- -----"
    For Each objHistory In colHistory
      if (objHistory.HResult = 0) AND (InStr(objHistory.Title,SearchString) > 0) then
        WScript.Echo Mid(objHistory.Date,1,19) & " " & objHistory.Title
      End If
    Next
End If
```

COMPUTER WORLD「システム管理 完全自動化プロジェクト」より，山市良氏によるスクリプト
http://www.computerworld.jp/

KB 番号「 KB2529073 」の更新プログラムを検索したい場合，次コマンドを実行する。
C:\>Cscript SearchUpdate.vbs "KB2529073"

情報漏えい対策と私的利用の抑制

- クライアントPCのスクリーンショットを保存する。
  - スクリーンショット監視ツール（NonShotScreen）
    http://homepage2.nifty.com/nonnon/
  - PCに詳しくない人でも判別可能であり，ユーザにも分かり易い→告知によって抑止効果は絶大。
  - リモートからスクリーンショットを確認できる。
- キーロガー
  - ControlCatcher
    http://www.vector.co.jp/soft/dl/winnt/util/se469439.html

限界

- 操作に詳しい担当者でしか管理できない。
  - 今回紹介したツールは，次の担当者はすぐに使いこなせないだろう。→ 引継ぎが困難。
- 単なるファイル配布などの操作は可能だが，アプリケーションの自動配布（自動インストール）は不可能。
- Windows のホットフィックス適用チェックは，人力に頼らざるを得ない。→ 台数が少なければ可能。

Q&A