スクリプトのお題

第一問

現在実行中のプロセスのうち、メモリ（ワーキングセット / WorkingSet）を100MB以上使用しているものを抽出し、その一覧をCSVファイルとして保存してください。

ヒント：プロセス取得、フィルタ、CSV出力の3コマンドレットをパイプラインで組み合わせる。「以上」は「-ge」。「100MB」は「100MB」と書くだけで良い。

第二問

イベントログのアプリケーションログのうち、24時間以内に発生したエラー(Error)と警告(Warning)をそれぞれ合計し、その数を「24時間以内にアプリケーションログでエラー：○件、警告○件が記録されています」のように表示してください。

ヒント：イベントログは変数に格納し、foreachでループする。24時間前は(get-date).AddDays(-1)で取得。if(エラーなら){エラー数インクリメント}elseif(警告なら){警告数インクリメント}。"文字列" + $count + ...のように文字列は連結できる。

第三問

某ブログのRSS2.0を読み込み、記事タイトルをリストにしてください。

アドレスはこちら⇒http://winscript.jp/powershell/rss2/

ヒント：$client = New-Object System.Net.WebClientでオブジェクトを作成。$client.Encoding = [System.Text.Encoding]::UTF8でエンコーディング指定。DownloadStringメソッドでダウンロード。結果を$xml=[xml]$stringのようにXML型にキャスト。$xml.rss.channel.itemのようにXMLノードを辿り、itemノードの配列を取得できる。あとはforeachでループを回してtitleを取得する。

★PSリモートを無効にするコマンド（管理者権限で実行）

Disable-PSRemoting # PSリモートを無効にする

Stop-Service winrm # WinRMサービスを停止

Set-Service winrm -StartupType Manual # WinRMサービスのスタートアップを手動に

winrm delete winrm/config/Listener?Address=\*+Transport=HTTP # リスナ削除（これだけコマンド必須）

winrm enumerate winrm/config/listener # 正常にリスナが削除されているか確認

netsh advfirewall firewall set rule name="Windows リモート管理 (HTTP 受信)" new enable=no # ファイアウォールの例外を無効に

Set-ItemProperty –path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System –name LocalAccountTokenFilterPolicy –propertyType DWord –value 0 # レジストリのリモートアクセスポリシー

Set-Item WSMan:\localhost\Client\TrustedHosts -value "" # 信頼済みホストの削除