ネットワーク通信中のプロセスを取得する

仕事で要り様になったので。

.NET Framework のクラスだけだと その通信を行っているプロセスを特定できないので Windowsの iphlpapi.dll にあるエントリを呼び出す必要があります。

ここの部分は C# で iphlpapi.dll のGetExtendedTcpTable を使うためのラッパーを利用しました。

ダウンロード

tcplistenerlist.zip TcpListenerList.exe 実行にはwrapGetExtendedTable.dllと.NET Framework4.0が必要です。

サンプル

```
C:\Work>TcpListenerList.exe > list.txt
C:\Work>
```

C:\Work\list.txtはこんな感じに netstat -nb コマンド的な出力になります。
STATEがMIB_TCP_STATE_LISTENのものがリスナーです。

```
STATE                  LocalAddress          RemoteAddress            PID
Command & CommandLine
MIB_TCP_STATE_LISTEN             0.0.0.0:  135         0.0.0.0:    0    860
svchost.exe C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe
-k RPCSS
MIB_TCP_STATE_LISTEN             0.0.0.0:  445         0.0.0.0:    0      4
System
MIB_TCP_STATE_LISTEN             0.0.0.0:  523         0.0.0.0:    0   1924
db2dasrrm.exe F:\Program Files\IBM\SQLLIB\bin\db2dasrrm.exe "F:\Program
Files\IBM\SQLLIB\bin\db2dasrrm.exe"
MIB_TCP_STATE_LISTEN             0.0.0.0:  554         0.0.0.0:    0    360
wmpnetwk.exe C:\Program Files\Windows Media Player\wmpnetwk.exe "C:\Program
Files\Windows Media Player\wmpnetwk.exe"
MIB_TCP_STATE_LISTEN             0.0.0.0: 1110         0.0.0.0:    0   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_LISTEN             0.0.0.0: 1111         0.0.0.0:    0   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_LISTEN             0.0.0.0: 2869         0.0.0.0:    0      4
```

```
System
MIB_TCP_STATE_LISTEN            0.0.0.0: 3389         0.0.0.0:    0   1284
svchost.exe C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe
-k NetworkService
MIB_TCP_STATE_LISTEN            0.0.0.0: 5357         0.0.0.0:    0      4
System
MIB_TCP_STATE_LISTEN            0.0.0.0:10243         0.0.0.0:    0      4
System
MIB_TCP_STATE_LISTEN            0.0.0.0:49152         0.0.0.0:    0    556
wininit.exe C:\Windows\system32\wininit.exe wininit.exe
MIB_TCP_STATE_LISTEN            0.0.0.0:49153         0.0.0.0:    0    996
svchost.exe C:\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe
-k LocalServiceNetworkRestricted
MIB_TCP_STATE_LISTEN            0.0.0.0:49154         0.0.0.0:    0    636
lsass.exe C:\Windows\system32\lsass.exe C:\Windows\system32\lsass.exe
MIB_TCP_STATE_LISTEN            0.0.0.0:49155         0.0.0.0:    0    408
svchost.exe C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe
-k netsvcs
MIB_TCP_STATE_LISTEN            0.0.0.0:49159         0.0.0.0:    0    620
services.exe C:\Windows\system32\services.exe
C:\Windows\system32\services.exe
MIB_TCP_STATE_LISTEN            0.0.0.0:50000         0.0.0.0:    0   2560
db2syscs.exe F:\PROGRA~1\IBM\SQLLIB\bin\db2syscs.exe
F:\PROGRA~1\IBM\SQLLIB\bin\db2syscs.exe
MIB_TCP_STATE_ESTAB           127.0.0.1: 1110       127.0.0.1:52926   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB           127.0.0.1: 1110       127.0.0.1:52982   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB           127.0.0.1: 1110       127.0.0.1:53087   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB           127.0.0.1: 1110       127.0.0.1:53157   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB           127.0.0.1: 1110       127.0.0.1:55858   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB           127.0.0.1: 1110       127.0.0.1:61717   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_TIME_WAIT       127.0.0.1: 1110       127.0.0.1:62010      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT       127.0.0.1: 1110       127.0.0.1:62021      0
```

```
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1: 1110       127.0.0.1:62023      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1: 1110       127.0.0.1:62038      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1: 1110       127.0.0.1:62040      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1: 1110       127.0.0.1:62042      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1: 1110       127.0.0.1:62048      0
System Idle Process
MIB_TCP_STATE_ESTAB            127.0.0.1: 1110       127.0.0.1:62050   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_TIME_WAIT        127.0.0.1: 1110       127.0.0.1:62066      0
System Idle Process
MIB_TCP_STATE_FIN_WAIT2        127.0.0.1: 1110       127.0.0.1:62078   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB            127.0.0.1: 1110       127.0.0.1:62090   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB            127.0.0.1: 1110       127.0.0.1:64570   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB            127.0.0.1: 1110       127.0.0.1:64572   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB            127.0.0.1: 2869       127.0.0.1:62056      4
System
MIB_TCP_STATE_LISTEN           127.0.0.1: 5354         0.0.0.0:    0   1832
mDNSResponder.exe C:\Program Files (x86)\Bonjour\mDNSResponder.exe
"C:\Program Files (x86)\Bonjour\mDNSResponder.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1: 5354       127.0.0.1:49156   1832
mDNSResponder.exe C:\Program Files (x86)\Bonjour\mDNSResponder.exe
"C:\Program Files (x86)\Bonjour\mDNSResponder.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1: 5354       127.0.0.1:49157   1832
mDNSResponder.exe C:\Program Files (x86)\Bonjour\mDNSResponder.exe
"C:\Program Files (x86)\Bonjour\mDNSResponder.exe"
MIB_TCP_STATE_TIME_WAIT        127.0.0.1: 5357       127.0.0.1:62064      0
System Idle Process
MIB_TCP_STATE_LISTEN           127.0.0.1:27015         0.0.0.0:    0   1772
AppleMobileDeviceService.exe C:\Program Files (x86)\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe "C:\Program
Files (x86)\Common Files\Apple\Mobile Device
Support\AppleMobileDeviceService.exe"
```

```
MIB_TCP_STATE_ESTAB            127.0.0.1:27015       127.0.0.1:49391   1772
AppleMobileDeviceService.exe C:\Program Files (x86)\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe "C:\Program
Files (x86)\Common Files\Apple\Mobile Device
Support\AppleMobileDeviceService.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:49156       127.0.0.1: 5354   1772
AppleMobileDeviceService.exe C:\Program Files (x86)\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe "C:\Program
Files (x86)\Common Files\Apple\Mobile Device
Support\AppleMobileDeviceService.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:49157       127.0.0.1: 5354   1772
AppleMobileDeviceService.exe C:\Program Files (x86)\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe "C:\Program
Files (x86)\Common Files\Apple\Mobile Device
Support\AppleMobileDeviceService.exe"
MIB_TCP_STATE_LISTEN           127.0.0.1:49158         0.0.0.0:    0   2000
dirmngr.exe C:\Program Files (x86)\GNU\GnuPG\dirmngr.exe "C:\Program Files
(x86)\GNU\GnuPG\dirmngr.exe" --service
MIB_TCP_STATE_ESTAB            127.0.0.1:49391       127.0.0.1:27015   1440
iTunesHelper.exe D:\Program Files (x86)\iTunes\iTunesHelper.exe "D:\Program
Files (x86)\iTunes\iTunesHelper.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:49411       127.0.0.1:49412   1728
SugarSyncManager.exe C:\Program Files (x86)\SugarSync\SugarSyncManager.exe
"C:\Program Files (x86)\SugarSync\SugarSyncManager.exe" -startInTray -
usedelay=true
MIB_TCP_STATE_ESTAB            127.0.0.1:49412       127.0.0.1:49411   1728
SugarSyncManager.exe C:\Program Files (x86)\SugarSync\SugarSyncManager.exe
"C:\Program Files (x86)\SugarSync\SugarSyncManager.exe" -startInTray -
usedelay=true
MIB_TCP_STATE_ESTAB            127.0.0.1:49425       127.0.0.1:49426   1728
SugarSyncManager.exe C:\Program Files (x86)\SugarSync\SugarSyncManager.exe
"C:\Program Files (x86)\SugarSync\SugarSyncManager.exe" -startInTray -
usedelay=true
MIB_TCP_STATE_ESTAB            127.0.0.1:49426       127.0.0.1:49425   1728
SugarSyncManager.exe C:\Program Files (x86)\SugarSync\SugarSyncManager.exe
"C:\Program Files (x86)\SugarSync\SugarSyncManager.exe" -startInTray -
usedelay=true
MIB_TCP_STATE_ESTAB            127.0.0.1:49459       127.0.0.1:49460   5244
firefox.exe C:\Program Files (x86)\Mozilla Firefox\firefox.exe "C:\Program
Files (x86)\Mozilla Firefox\firefox.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:49460       127.0.0.1:49459   5244
firefox.exe C:\Program Files (x86)\Mozilla Firefox\firefox.exe "C:\Program
Files (x86)\Mozilla Firefox\firefox.exe"
MIB_TCP_STATE_LISTEN           127.0.0.1:52807         0.0.0.0:    0   7888
gpg-agent.exe C:\Program Files (x86)\GNU\GnuPG\gpg-agent.exe "C:\Program
Files (x86)\GNU\GnuPG\gpg-agent.exe" --daemon --use-standard-socket
MIB_TCP_STATE_ESTAB            127.0.0.1:52926       127.0.0.1: 1110   1728
SugarSyncManager.exe C:\Program Files (x86)\SugarSync\SugarSyncManager.exe
"C:\Program Files (x86)\SugarSync\SugarSyncManager.exe" -startInTray -
usedelay=true
MIB_TCP_STATE_ESTAB            127.0.0.1:52982       127.0.0.1: 1110   3304
```

```
SkyDrive.exe
C:\Users\tomason510\AppData\Local\Microsoft\SkyDrive\SkyDrive.exe
"C:\Users\tomason510\AppData\Local\Microsoft\SkyDrive\SkyDrive.exe"
/background
MIB_TCP_STATE_ESTAB            127.0.0.1:53087       127.0.0.1: 1110  10428
thunderbird.exe C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
"C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:53157       127.0.0.1: 1110   5244
firefox.exe C:\Program Files (x86)\Mozilla Firefox\firefox.exe "C:\Program
Files (x86)\Mozilla Firefox\firefox.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:53620       127.0.0.1:53621  16192
Yoono Desktop.exe C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe
"C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:53621       127.0.0.1:53620  16192
Yoono Desktop.exe C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe
"C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:53622       127.0.0.1:53623  16192
Yoono Desktop.exe C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe
"C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:53623       127.0.0.1:53622  16192
Yoono Desktop.exe C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe
"C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:55858       127.0.0.1: 1110  10428
thunderbird.exe C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
"C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:61717       127.0.0.1: 1110  10428
thunderbird.exe C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
"C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe"
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62025       127.0.0.1: 1110      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62027       127.0.0.1: 1110      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62029       127.0.0.1: 1110      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62031       127.0.0.1: 1110      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62033       127.0.0.1: 1110      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62047       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_ESTAB            127.0.0.1:62050       127.0.0.1: 1110   5244
firefox.exe C:\Program Files (x86)\Mozilla Firefox\firefox.exe "C:\Program
Files (x86)\Mozilla Firefox\firefox.exe"
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62052       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62054       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62055       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_ESTAB            127.0.0.1:62056       127.0.0.1: 2869   1108
svchost.exe C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe
```

```
-k LocalService
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62068       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62072       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62074       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62077       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_CLOSE_WAIT       127.0.0.1:62078       127.0.0.1: 1110  16192
Yoono Desktop.exe C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe
"C:\Program Files (x86)\Yoono Desktop\Yoono Desktop.exe"
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62083       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62085       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62089       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_ESTAB            127.0.0.1:62090       127.0.0.1: 1110 321168
MpCmdRun.exe c:\program files\windows defender\MpCmdRun.exe "c:\program
files\windows defender\MpCmdRun.exe" SpyNetService -RestrictPrivileges -
AccessKey xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx -Reinvoke
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62092       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT        127.0.0.1:62093       127.0.0.1: 1111      0
System Idle Process
MIB_TCP_STATE_ESTAB            127.0.0.1:64561       127.0.0.1:64562  10428
thunderbird.exe C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
"C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:64562       127.0.0.1:64561  10428
thunderbird.exe C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
"C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:64570       127.0.0.1: 1110  10428
thunderbird.exe C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
"C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe"
MIB_TCP_STATE_ESTAB            127.0.0.1:64572       127.0.0.1: 1110  10428
thunderbird.exe C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
"C:\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe"
MIB_TCP_STATE_LISTEN       192.168.1.200:  139         0.0.0.0:    0      4
System
MIB_TCP_STATE_TIME_WAIT    192.168.1.200: 2869     192.168.1.1:52483      0
System Idle Process
MIB_TCP_STATE_SYN_RCVD     192.168.1.200: 2869   192.168.1.254: 1535      4
System
MIB_TCP_STATE_ESTAB        192.168.1.200:52672    192.168.1.20:   22  15448
putty.exe C:\Program Files (x86)\PuTTY\putty.exe "C:\Program Files
(x86)\PuTTY\putty.exe"
MIB_TCP_STATE_ESTAB        192.168.1.200:52929    74.201.86.29:  443   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
```

```
MIB_TCP_STATE_ESTAB        192.168.1.200:52983  157.56.100.143:  443   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB        192.168.1.200:53088   74.125.196.16:  993   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB        192.168.1.200:53158  199.59.149.201:  443   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB        192.168.1.200:53791  119.110.92.177: 1935   9580
FlashPlayerPlugin_12_0_0_77.exe
C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerPlugin_12_0_0_77.exe
"C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerPlugin_12_0_0_77.exe" --
channel=xxxxx.xxxxxxxx.xxxxxxxxxx --proxy-stub-
channel=Flash11984.56977F48.30734 --plugin-
path="C:\Windows\SysWOW64\Macromed\Flash\NPSWF32_12_0_0_77.dll" --host-
npapi-version=27 --type=renderer
MIB_TCP_STATE_ESTAB        192.168.1.200:55859   74.125.196.16:  993   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_CLOSE_WAIT   192.168.1.200:56687   192.168.1.100:  445      4
System
MIB_TCP_STATE_ESTAB        192.168.1.200:61718    192.168.1.20:  143   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62009  184.87.194.208:   80      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62026  202.221.143.14:   80      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62028  202.221.143.14:   80      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62030  202.221.143.14:   80      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62032  202.221.143.14:   80      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62034  202.221.143.14:   80      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62035    81.19.104.99:  443      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62044   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62045   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62046   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_ESTAB        192.168.1.200:62051  93.184.216.146:  443   1800
```

```
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62058   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62061     192.168.1.1:54383      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62062     192.168.1.1:54383      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62063     192.168.1.1:54383      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62065    192.168.1.20:  139      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62069   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62070   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62071   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62073   62.128.100.41:  443      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62075   62.128.100.39:  443      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62076   62.128.100.39:  443      0
System Idle Process
MIB_TCP_STATE_CLOSE_WAIT   192.168.1.200:62079   199.59.148.20:  443   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62080   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62081   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_TIME_WAIT    192.168.1.200:62082   192.168.1.254: 1900      0
System Idle Process
MIB_TCP_STATE_ESTAB        192.168.1.200:62086   62.128.100.41:  443   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB        192.168.1.200:62087   62.128.100.39:  443   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB        192.168.1.200:62088   62.128.100.39:  443   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB        192.168.1.200:62091    157.56.30.46:  443   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
```

```
MIB_TCP_STATE_ESTAB        192.168.1.200:64571    192.168.1.20:  143   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
MIB_TCP_STATE_ESTAB        192.168.1.200:64574   74.125.196.16:  993   1800
avp.exe C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet Security
14.0.0\avp.exe "C:\Program Files (x86)\Kaspersky Lab\Kaspersky Internet
Security 14.0.0\avp.exe" -r
```

やってること

やってることは

1. wrapGetExtendedTable.dll のxGetExtendedTCPTableOwnerPid(TCP_TABLE_CLASS.TCP_TABLE_OWNER_PID_ALL)を呼び出して通信状況を得る。
2. WMIを使い通信を行っているプロセスIDのプロセス名、実行イメージのパス、引数情報を得る。
3. フォーマットして標準出力へ出力。

wrapGetExtendedTable.dllの中でiphlpapi.dllを呼び出ししています。これが使えない環境では動作しません。

本当にリスナーだけ一覧に出したいなら xGetExtendedTcpTableOwnerPid() の引数を TCP_TABLE_CLASS.TCP_TABLE_OWNER_PID_LISTENER に書き直せばよろしいかと。

あと、管理者権限のあるアカウントで実行しないとプロセスイメージの情報が取れないものがあります。たぶんWMIの仕様かなーと思うんですが。
avp.exe のプロセスがその例で、一般ユーザでの実行ではインストール先までの情報が取れないのですが、管理者で実行すると上記例のようにインストール場所まで取得できるようになります。

ソース

コピペで使うための雛形的なもの。コメント等はほぼ無い。

コンパイルのコマンドライン

Visual Studioの出力をそのままコピーした Program.cs と wrapGetExtendedTable.dll を同じフォルダにおいてコンパイルし、TcpListenerList.exeを出力します。 自分の環境に合わせて修正してください。

実行の際にも TcpListenerList.exe と wrapGetExtendedTable.dll は同じフォルダに配置しておく必要があります。

make.bat

```
SET CSPATH="C:\Windows\Microsoft.NET\Framework\v4.0.30319"
SET DLLPATH="C:\Program Files (x86)\Reference
Assemblies\Microsoft\Framework\.NETFramework\v4.0"
```

```
%CSPATH%\Csc.exe /noconfig /nowarn:1701,1702 /nostdlib+ /platform:x86
/errorreport:prompt /warn:4 /errorendlocation /preferreduilang:ja-JP
/highentropyva- /reference:%DLLPATH%\Microsoft.CSharp.dll
/reference:%DLLPATH%\mscorlib.dll /reference:%DLLPATH%\System.Core.dll
/reference:%DLLPATH%\System.dll
/reference:%DLLPATH%\System.Management.dll
/reference:wrapGetExtendedTable.dll /filealign:512 /optimize+
/out:TcpListenerList.exe /target:exe /utf8output Program.cs
```

TcpListenerList.exe本体

WMIでプロセスの情報を取得しています。Handleプロパティはプロセスidのことです。

Program.cs

```
using System;
using System.Collections.Generic;
using System.Net;
using wrapGetExtendedTable;
using System.Management;

namespace TcpListenerList
{

    class Program
    {
        static String getProcessImage(long pid)
        {
            String q = String.Format("Win32_Process.Handle={0}",pid);
            String ans = "";

            try
            {
                ManagementObject mo = new ManagementObject(q);
                ans = mo.Properties["Caption"].Value.ToString() + " ";
                ans += mo.Properties["ExecutablePath"].Value.ToString()
+ " ";
                ans += mo.Properties["CommandLine"].Value.ToString();
            }
            catch (Exception)
            {
            }

            return ans;
        }
        static void Main(string[] args)
        {
```

```
            iphlpapi aa = new iphlpapi();
            MIB_TCPTABLE_OWNER_PID z =
aa.xGetExtendedTcpTableOwnerPid(TCP_TABLE_CLASS.TCP_TABLE_OWNER_PID_ALL
);

            Console.WriteLine("{0,-24} {1,-21} {2,-21} {3,6} {4}",
"STATE", "LocalAddress", "RemoteAddress", "PID", "Command &
CommandLine");
            for (int i = 0; i < z.table.Length; i++)
            {
                IPAddress a = new IPAddress(z.table[i].dwLocalAddr);
                IPAddress b = new IPAddress(z.table[i].dwRemoteAddr);

                Console.WriteLine("{0,-24} {1,15}:{2,5} {3,15}:{4,5}
{5,6:#####0} {6}"
                                  ,
Enum.GetName(typeof(MIB_TCP_STATE),  z.table[i].dwState)
                                  , a.ToString()
                                  , z.table[i].dwLocalPort
                                  , b.ToString()
                                  , z.table[i].dwRemotePort
                                  , z.table[i].dwOwningPid
                                  ,
getProcessImage((long)z.table[i].dwOwningPid));
            }
        }
    }
}
```

リスナーのみ□UDP入り TcpListenerList.exe本体

TcpListenerList.exeにリスナーのみの出力□UDPの出力も付け加えたもの。先のmake.batでコンパイルできます。

Program.cs

```
using System;
using System.Collections.Generic;
using System.Net;
using wrapGetExtendedTable;
using System.Management;

namespace TcpListenerList
{

    class Program
    {
        static String getProcessImage(long pid)
```

```
        {
            String q = String.Format("Win32_Process.Handle={0}",pid);
            String ans = "";

            try
            {
                ManagementObject mo = new ManagementObject(q);
                ans = mo.Properties["Caption"].Value.ToString() + " ";
                ans += mo.Properties["ExecutablePath"].Value.ToString()
+ " ";
                ans += mo.Properties["CommandLine"].Value.ToString();
            }
            catch (Exception)
            {
            }

            return ans;
        }
        static void Main(string[] args)
        {

            iphlpapi aa = new iphlpapi();
            MIB_TCPTABLE_OWNER_PID z1 =
aa.xGetExtendedTcpTableOwnerPid(TCP_TABLE_CLASS.TCP_TABLE_OWNER_PID_LIS
TENER);
            MIB_UDPTABLE_OWNER_PID z2 =
aa.xGetExtendedUdpTableOwnerPid(UDP_TABLE_CLASS.UDP_TABLE_OWNER_PID);

            Console.WriteLine("{0,-4} {1,21} {2,6} {3}", "TYPE",
"LocalAddress", "PID", "Command & CommandLine");
            for (int i = 0; i < z1.table.Length; i++)
            {
                IPAddress a = new IPAddress(z1.table[i].dwLocalAddr);
                IPAddress b = new IPAddress(z1.table[i].dwRemoteAddr);

                Console.WriteLine("{0,-4} {1,15}:{2,5} {3,6:#####0}
{4}"
                                  , "TCP"
                                  , a.ToString()
                                  , z1.table[i].dwLocalPort
                                  , z1.table[i].dwOwningPid
                                  ,
getProcessImage((long)z1.table[i].dwOwningPid));
            }
            for (int i = 0; i < z2.table.Length; i++)
            {
                IPAddress a = new IPAddress(z2.table[i].dwLocalAddr);

                Console.WriteLine("{0,-4} {1,15}:{2,5} {3,6:#####0}
{4}"
                                  , "UDP"
```

```
                                        , a.ToString()
                                        , z2.table[i].dwLocalPort
                                        , z2.table[i].dwOwningPid
                                        ,
getProcessImage((long)z2.table[i].dwOwningPid));
                }
            }
        }
}
```

結果はこんな感じ。UDPのポート3702はプロセスのエントリが2回出ちゃう理由がわかんない。なんだろね。

```
TYPE          LocalAddress    PID Command & CommandLine
TCP          0.0.0.0:  135    860 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k RPCSS
TCP          0.0.0.0:  445      4 System
TCP          0.0.0.0:  523   1924 db2dasrrm.exe F:\Program
Files\IBM\SQLLIB\bin\db2dasrrm.exe "F:\Program
Files\IBM\SQLLIB\bin\db2dasrrm.exe"
TCP          0.0.0.0:  554    360 wmpnetwk.exe C:\Program Files\Windows
Media Player\wmpnetwk.exe "C:\Program Files\Windows Media
Player\wmpnetwk.exe"
TCP          0.0.0.0: 1110   1800 avp.exe C:\Program Files (x86)\Kaspersky
Lab\Kaspersky Internet Security 14.0.0\avp.exe "C:\Program Files
(x86)\Kaspersky Lab\Kaspersky Internet Security 14.0.0\avp.exe" -r
TCP          0.0.0.0: 1111   1800 avp.exe C:\Program Files (x86)\Kaspersky
Lab\Kaspersky Internet Security 14.0.0\avp.exe "C:\Program Files
(x86)\Kaspersky Lab\Kaspersky Internet Security 14.0.0\avp.exe" -r
TCP          0.0.0.0: 2869      4 System
TCP          0.0.0.0: 3389   1284 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
NetworkService
TCP          0.0.0.0: 5357      4 System
TCP          0.0.0.0:10243      4 System
TCP          0.0.0.0:49152    556 wininit.exe
C:\Windows\system32\wininit.exe wininit.exe
TCP          0.0.0.0:49153    996 svchost.exe
C:\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe -k
LocalServiceNetworkRestricted
TCP          0.0.0.0:49154    636 lsass.exe C:\Windows\system32\lsass.exe
C:\Windows\system32\lsass.exe
TCP          0.0.0.0:49155    408 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k netsvcs
TCP          0.0.0.0:49159    620 services.exe
C:\Windows\system32\services.exe C:\Windows\system32\services.exe
TCP          0.0.0.0:50000   2560 db2syscs.exe
F:\PROGRA~1\IBM\SQLLIB\bin\db2syscs.exe
F:\PROGRA~1\IBM\SQLLIB\bin\db2syscs.exe
TCP        127.0.0.1: 5354   1832 mDNSResponder.exe C:\Program Files
```

```
(x86)\Bonjour\mDNSResponder.exe "C:\Program Files
(x86)\Bonjour\mDNSResponder.exe"
TCP        127.0.0.1:27015   1772 AppleMobileDeviceService.exe C:\Program
Files (x86)\Common Files\Apple\Mobile Device
Support\AppleMobileDeviceService.exe "C:\Program Files (x86)\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe"
TCP        127.0.0.1:49158   2000 dirmngr.exe C:\Program Files
(x86)\GNU\GnuPG\dirmngr.exe "C:\Program Files (x86)\GNU\GnuPG\dirmngr.exe" -
-service
TCP        127.0.0.1:52807   7888 gpg-agent.exe C:\Program Files
(x86)\GNU\GnuPG\gpg-agent.exe "C:\Program Files (x86)\GNU\GnuPG\gpg-
agent.exe" --daemon --use-standard-socket
TCP    192.168.1.200:  139      4 System
UDP          0.0.0.0:  500    408 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k netsvcs
UDP          0.0.0.0:  523   1924 db2dasrrm.exe F:\Program
Files\IBM\SQLLIB\bin\db2dasrrm.exe "F:\Program
Files\IBM\SQLLIB\bin\db2dasrrm.exe"
UDP          0.0.0.0: 3544    408 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k netsvcs
UDP          0.0.0.0: 3702   1108 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalService
UDP          0.0.0.0: 3702   2036 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalServiceAndNoImpersonation
UDP          0.0.0.0: 3702   1108 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalService
UDP          0.0.0.0: 3702   2036 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalServiceAndNoImpersonation
UDP          0.0.0.0: 4500    408 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k netsvcs
UDP          0.0.0.0: 5004    360 wmpnetwk.exe C:\Program Files\Windows
Media Player\wmpnetwk.exe "C:\Program Files\Windows Media
Player\wmpnetwk.exe"
UDP          0.0.0.0: 5005    360 wmpnetwk.exe C:\Program Files\Windows
Media Player\wmpnetwk.exe "C:\Program Files\Windows Media
Player\wmpnetwk.exe"
UDP          0.0.0.0:49489   1108 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalService
UDP          0.0.0.0:53605   1832 mDNSResponder.exe C:\Program Files
(x86)\Bonjour\mDNSResponder.exe "C:\Program Files
(x86)\Bonjour\mDNSResponder.exe"
UDP          0.0.0.0:53607   2036 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalServiceAndNoImpersonation
UDP          0.0.0.0:61566   1108 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
```

```
LocalService
UDP        127.0.0.1: 1900   2036 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalServiceAndNoImpersonation
UDP        127.0.0.1:53603   1772 AppleMobileDeviceService.exe C:\Program
Files (x86)\Common Files\Apple\Mobile Device
Support\AppleMobileDeviceService.exe "C:\Program Files (x86)\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe"
UDP        127.0.0.1:53604   1772 AppleMobileDeviceService.exe C:\Program
Files (x86)\Common Files\Apple\Mobile Device
Support\AppleMobileDeviceService.exe "C:\Program Files (x86)\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe"
UDP        127.0.0.1:53679 449904 iexplore.exe C:\Program Files
(x86)\Internet Explorer\iexplore.exe "C:\Program Files (x86)\Internet
Explorer\iexplore.exe"
UDP        127.0.0.1:56398  12164 iexplore.exe C:\Program Files
(x86)\Internet Explorer\iexplore.exe "C:\Program Files (x86)\Internet
Explorer\iexplore.exe" SCODEF:449904 CREDAT:203009
UDP        127.0.0.1:59806   3880 sidebar.exe C:\Program Files\Windows
Sidebar\sidebar.exe "C:\Program Files\Windows Sidebar\sidebar.exe" /autoRun
UDP        127.0.0.1:59807   1440 iTunesHelper.exe D:\Program Files
(x86)\iTunes\iTunesHelper.exe "D:\Program Files
(x86)\iTunes\iTunesHelper.exe"
UDP        127.0.0.1:59808   1440 iTunesHelper.exe D:\Program Files
(x86)\iTunes\iTunesHelper.exe "D:\Program Files
(x86)\iTunes\iTunesHelper.exe"
UDP        127.0.0.1:65180   2036 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalServiceAndNoImpersonation
UDP    192.168.1.200:  137      4 System
UDP    192.168.1.200:  138      4 System
UDP    192.168.1.200: 1900   2036 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalServiceAndNoImpersonation
UDP    192.168.1.200: 5353   1832 mDNSResponder.exe C:\Program Files
(x86)\Bonjour\mDNSResponder.exe "C:\Program Files
(x86)\Bonjour\mDNSResponder.exe"
UDP    192.168.1.200:49378    408 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k netsvcs
UDP    192.168.1.200:65179   2036 svchost.exe
C:\Windows\system32\svchost.exe C:\Windows\system32\svchost.exe -k
LocalServiceAndNoImpersonation
```

技術資料, Windows, tcp/ip, tool