【詳細手順】

以下に、手順とファイル名情報の詳細を説明します。

１．不審なファイルの存在有無の確認(注1)

利用者の端末（パソコン）にウイルス感染の可能性がないか、不審ファイル（ウイルス、ツール、表示用ダミー(デコイ)ファイル（ウイルス感染時に画面に表示される囮の文書ファイル)）の名称と、不審なファイルが存在する可能性のある箇所を検査します。ファイルの存在確認と、自動起動の 2 つの観点で検査します。

① ファイルの存在確認(注2)

「１－１：ファイル名(ウイルス)」「１－２：ファイル名(ツール)」「１－３：表示用ダミー(デコイ)ファイル名」に示すファイルが、下記の「検索場所」に存在していないか確認してください。

【１－１：ファイル名（ウイルス)】の一覧

leanp.exe	nvsvcv.exe	vmatam.exe	vmwere.exe
leassap.exe	nvvscv.exe	vmatap.exe	windump.exe
leassaq.exe	slwga.exe	vmater.exe	
leassnp.exe	upsl.dll	vmmat.exe	
mdm.exe	vmat.exe	vmnatam.exe	

【１－２：ファイル名（ツール)】の一覧

ct.exe	msver.exe
yrar.exe	ss.exe
csvde.exe	mailfinal.exe
GetPassword.exe	mail_noArgv_final.exe
mimikatz.exe	result.log
mimikatzx64.exe	14068.rar
mimikatz1.exe	ms14-068.exe
gp.exe	
Gp64.exe	
ps.txt	

【１－３：表示用ダミー（デコイ）ファイル名】の一覧

kptl.doc	kenpo.doc

【検索場所】

- スタートアップフォルダ　（※1）
- %TEMP%　（※2）

(注1) ウイルス感染発覚後にセキュリティベンダ等の専門機関へフォレンジック依頼をすることを想定し、本作業の操作ログと攻撃の痕跡が混在してしまわないよう、作業記録をつけることなどをお勧めします。

(注2) 不審ファイルの確認先としては、本文書にある通りですので、今後の恒常的な対策実施にもご活用ください。

（※1）
スタートアップフォルダは、Windows Vista、Windows 7、Windows 8/8.1、Windows Server 2008 (R2)、Windows Server 2012 (R2)の場合は、以下のパスとなります。

C:¥Users¥[ユーザー名]¥AppData¥Roaming¥Microsoft¥Windows¥Start Menu¥Programs¥Startup

C:¥Users¥All Users¥Microsoft¥Windows¥Start Menu¥Programs¥Startup

（※2）
%TEMP%は、利用者の環境変数の設定により異なります。
Windows Vista、Windows 7、Windows 8/8.1、Windows Server 2008(R2)、Windows Server 2012 (R2)の初期設定は以下のパスとなります。

C:¥Users¥[ユーザー名]¥AppData¥Local¥Temp

なお、これらの情報は IPA にて得た知見と、下記セキュリティベンダの情報を参考にしています。

株式会社カスペルスキー：BLUE TERMITE（ブルーターマイト）～日本を標的にする APT 攻撃～
http://media.kaspersky.com/jp/Kaspersky_BlueTermite-PR-1013.pdf
マクニカネットワークス株式会社：Emdivi を使う攻撃者の素性
http://blog.macnica.net/blog/2015/06/emdivi-201405-eea5.html
マクニカネットワークス株式会社：医療費通知に偽装した攻撃（Backdoor.Emdivi） その後
http://blog.macnica.net/blog/2015/01/post-39d4.html

【確認方法（例）】 一般利用者向け

ご自身のパソコンを確認する際の手順例を示します。

1. デスクトップ上で「**スタートボタン**」（またはキーボードの Windows ロゴキー）を押します。
2. 図１で示す通り、「**プログラムとファイルの検索**」欄に、【検索場所】に記載したパスを入力します。

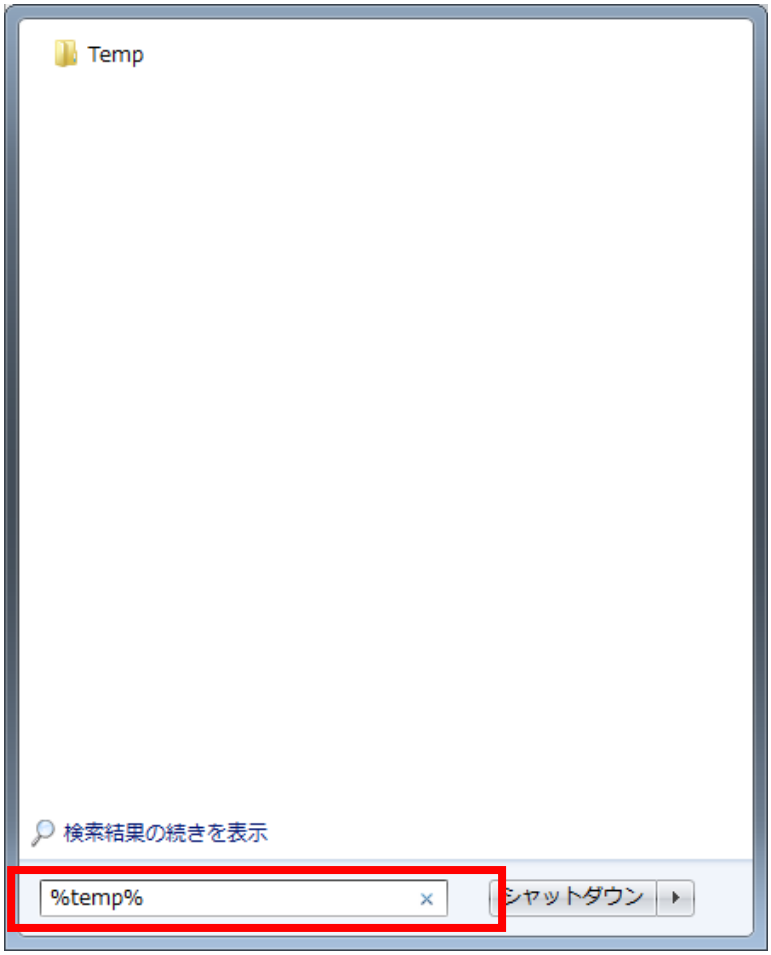

図１ 「プログラムとファイルの検索」で「Temp」フォルダを検索

３．Enter キーを押下すると当該フォルダが表示されます。

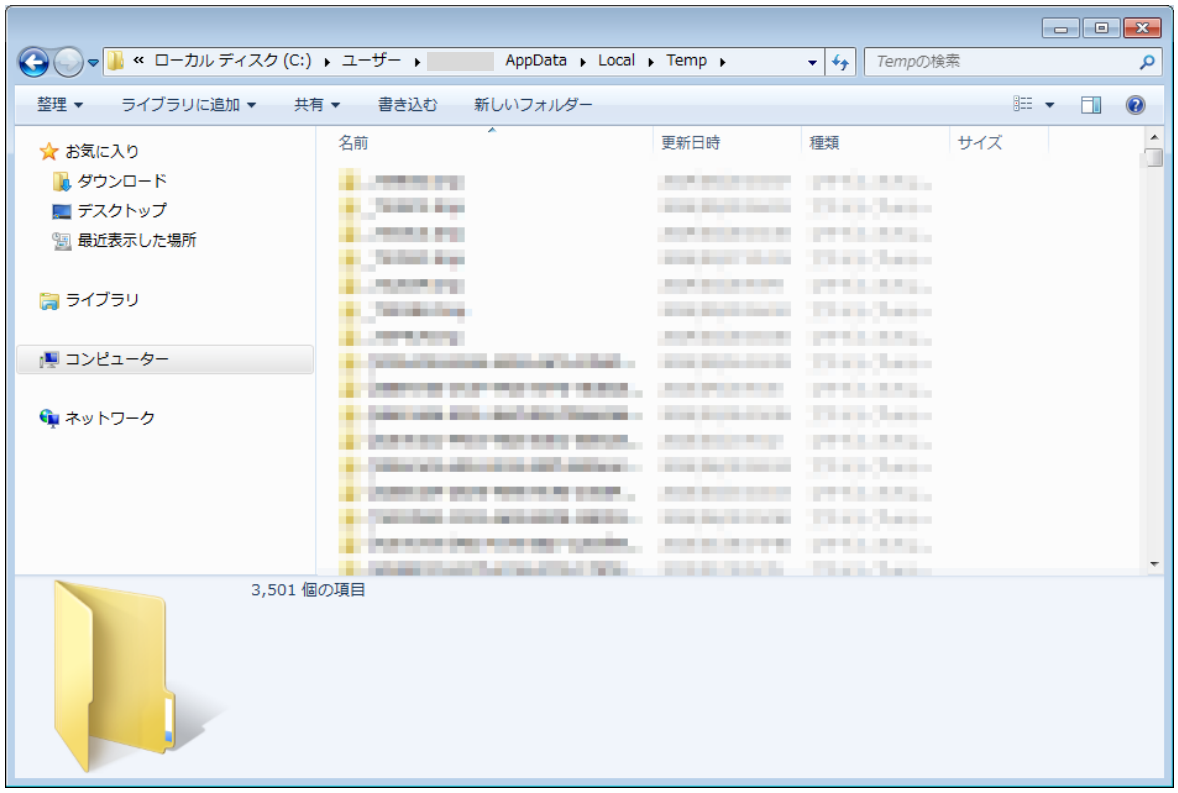

図２　【検索場所】である Temp フォルダが表示された場合の例

４．開いているウィンドウの検索ボックスに、「１－１：ファイル名（ウイルス）」や「１－２：ファイル名（ツール）」、「１－３：表示用ダミー（デコイ）ファイル名」を都度入力して検索を実施します。

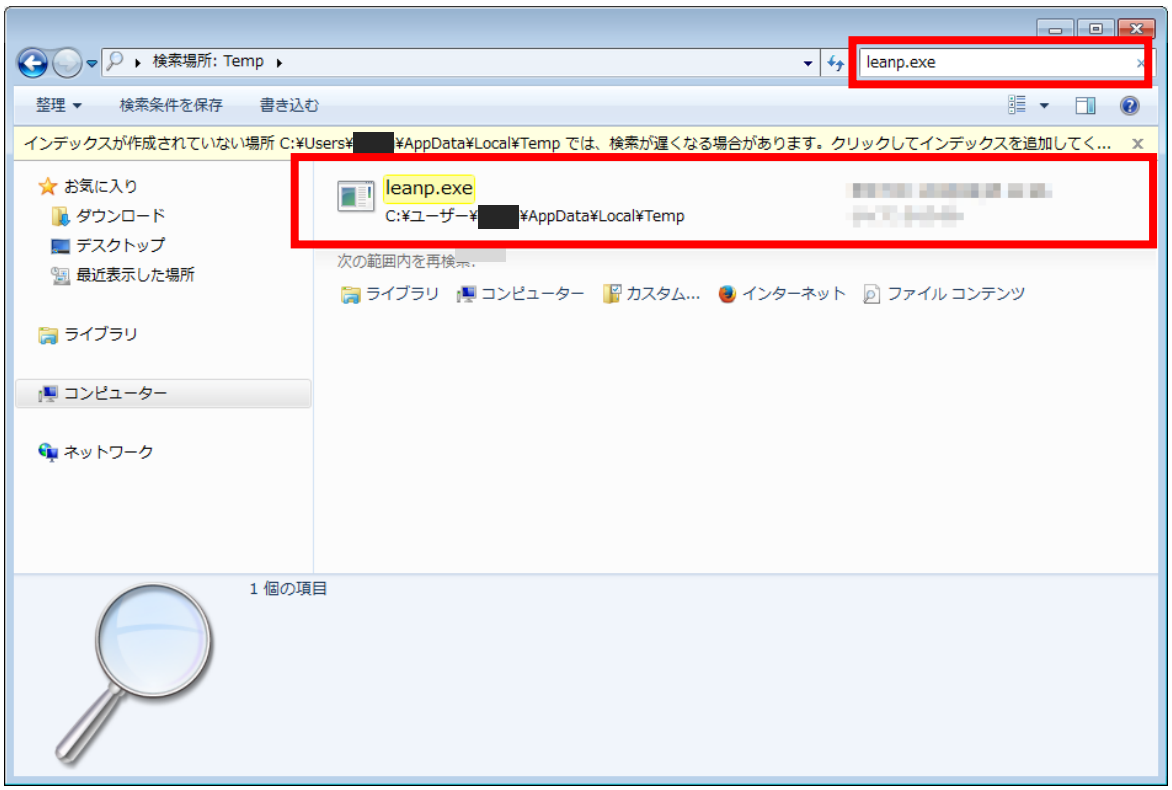

図３　Temp フォルダで不審なファイルを検索し、同一ファイルが見つかった場合の例

【確認方法（例）】 システム管理者向け

システム管理者が利用者の各端末を確認する際の例を示します。

利用者端末のコマンドプロンプト上にて、下記のコマンドを実行してください。（バッチの配布でも可能です）

＜コマンド例＞

```
dir /a /r /s /b [検索フォルダ 1] [検索フォルダ 2]… |findstr /I /R ¥¥[ファイル名]¥[拡張子] …
```

＜実行結果イメージ＞

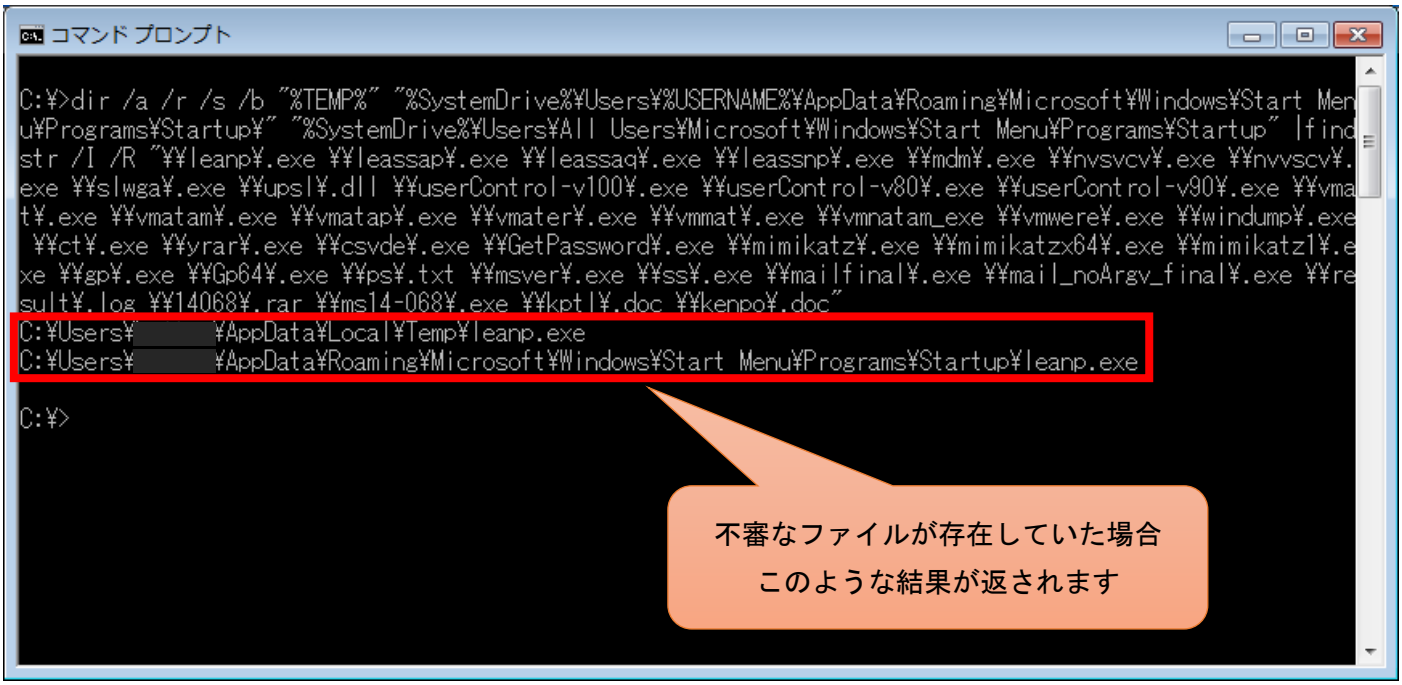

図 4　コマンドプロンプトによるファイル検索の実行結果の例

「①ファイルの存在確認」は以上となります。

② 自動起動設定に不審なファイルが登録されていないかの確認方法

利用者の端末（パソコン）起動時に、自動的に実行されるプログラムの中に、「１－１ファイル名(ウイルス)」が登録されていないか確認します。下記の「検索場所」に登録されていないか確認してください。

【検索場所】

- スタートアップフォルダ（※）
- タスクスケジューラ
- レジストリ

（拡張子が .exe ではなく .lnk（ショートカットファイル） となっている場合もあります。）

（※）

スタートアップフォルダは、Windows Vista、Windows 7、Windows 8/8.1、Windows Server 2008 (R2)、Windows Server 2012 (R2)の場合は、以下のパスとなります。

C:¥Users¥[ユーザー名]¥AppData¥Roaming¥Microsoft¥Windows¥Start Menu¥Programs¥Startup

C:¥Users¥All Users¥Microsoft¥Windows¥Start Menu¥Programs¥Startup

【スタートアップフォルダの確認方法（例)】　一般利用者向け

１.「マイコンピュータ」などエクスプローラーを開いた状態で、フォルダパスに【検索場所】に記載したパスを入力します。

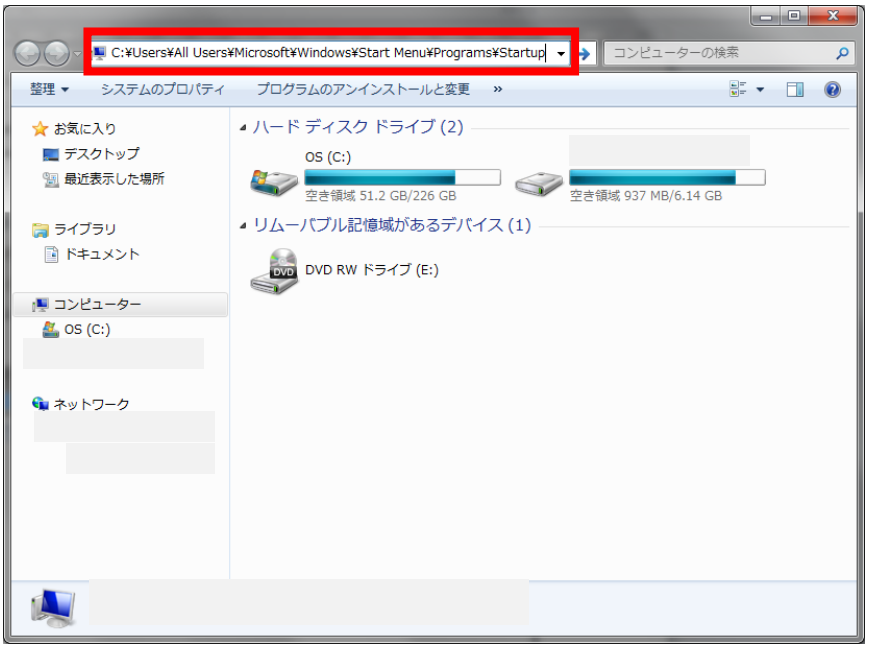

図５　エクスプローラー上で、スタートアップフォルダのパスを入力

２. Enter キーを押下すると、図６で示す通り、スタートアップフォルダが表示されますので、不審なファイルが登録されていないか確認してください。

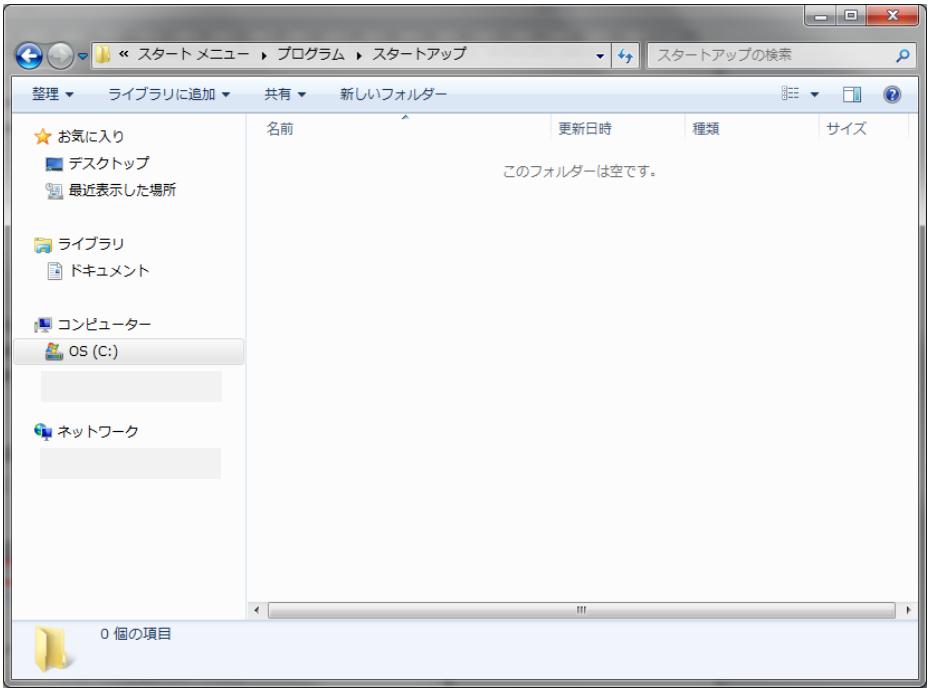

図 6　スタートアップフォルダを表示した場合の例

【タスクスケジューラの確認方法（例）】システム管理者向け

コマンドプロンプトからコマンドを実行することでタスクスケジューラに登録されたタスク一覧が確認できます。
タスク一覧から不審なファイル（ウイルス）が登録されていないかを確認します。

1．デスクトップ上で「**スタートボタン**」（またはキーボードの Windows ロゴキー）を押します。
2．「プログラムとファイルの検索」欄に『**cmd**』と入力し、Enter キーを押下します。

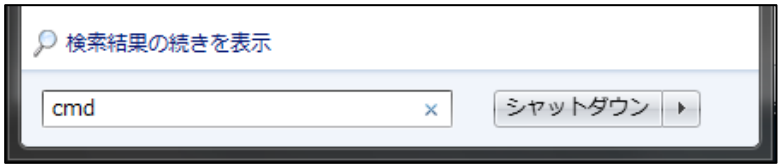

図 7　「プログラムとファイルの検索」に『cmd』を入力

3．起動したコマンドプロンプト上で、以下のコマンドを実行し、図 8 で示す実行結果を確認してください。

＜コマンド例＞

```
schtasks /query /v |findstr /I /R ¥¥[ファイル名]¥[拡張子] …
```

＜実行結果イメージ＞

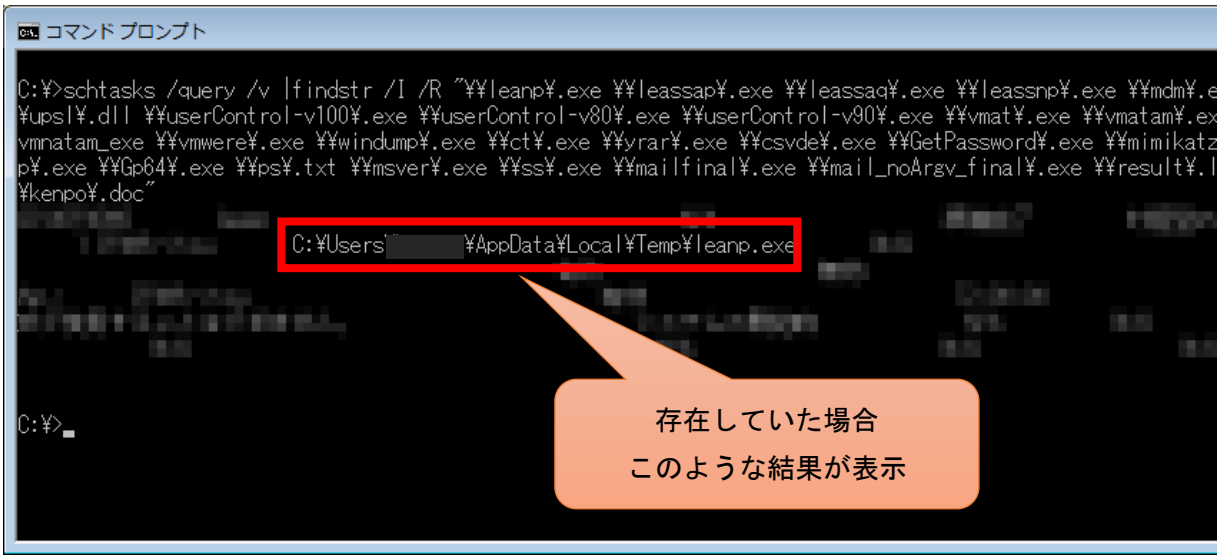

図 8　コマンドプロンプトの実行結果の例（タスクスケジューラ）

【レジストリーの確認方法（例）】システム管理者向け

コマンドプロンプトからコマンドを実行することで、登録されたレジストリーキーが確認できます。

1．コマンドプロンプトから以下のコマンドを実行してください。

＜コマンド例＞

```
reg query "HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥Run" /s
```

＜実行結果イメージ＞

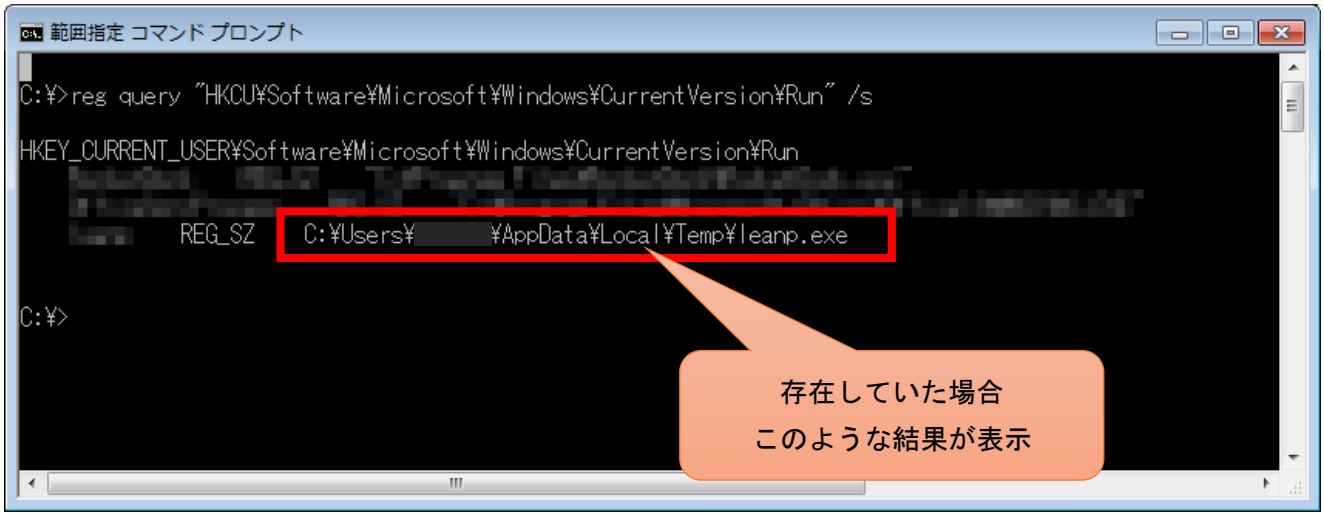

図 9　コマンドプロンプトの実行結果の例（レジストリー）

「②自動起動設定に不審なファイルが登録されていないかの確認方法」は以上となります。

■不審なファイルを発見した場合の対応

不審なファイルを発見した場合、ウイルス感染あるいはウイルスが侵入を試みた可能性が高くなります。可能であれば、次ページ以降の「不審な通信の確認」も行い、ウイルスの活動が行われていないか確認することをお勧めします。感染が疑われた場合の対応を以下に示します。

該当端末をネットワークから切り離す

被害を最小限に抑えるためには、まず感染が疑わしい該当端末をネットワークから切り離すことが重要です。その上で該当端末や通信ログなどの詳細な調査を行ってください。

セキュリティベンダなど専門家への相談

該当端末が踏み台とされ、他の端末へ感染が広がっている可能性も考えられます。セキュリティベンダなどの専門家に相談するなど、正確な被害範囲や感染原因を把握した上で対応を進めることが重要です。

２．不審な通信の確認

① 通信状況の取得

調査結果に含まれるノイズを減らすため、一度、利用者端末（パソコン）を再起動した状態で確認を実施します。再起動後、利用者が端末を操作する前にコマンドプロンプトから以下のコマンドを実行することで、そのパソコンの通信の接続情報一覧を確認することができます。

接続情報一覧を確認し、外部と通信を行っている接続の「外部アドレス」と「PID」を記録します。

② 通信先の確認

「外部アドレス」として記録した IP アドレスの Whois 検索やインターネット検索を行い、組織や端末利用者が意図している通信であるかを確認してください。IP アドレスの管理組織が意図していない組織の場合(端末で利用しているソフトウェアのメーカー等でない場合)次項の「プロセス確認」を行ってください。

③ 接続を行っているプロセスの確認

コマンドを実行し、接続を行っているプロセス名を確認します。

表示されたプロセスとプロセスが行う通信が、組織や端末利用者の意図するものであるかを確認してください。

インストールしていない、または起動したはずのないプロセスが外部へ通信を行っている場合は詳細な調査を行ってください。

【利用者端末における通信の確認方法（例)】システム管理者向け

利用者の端末（パソコン）を確認する際の手順例を示します。

１．デスクトップ上で「**スタートボタン**」（またはキーボードの Windows ロゴキー）を押します。

２．「プログラムとファイルの検索」欄に『**cmd**』と入力し、Enter キーを押下します。

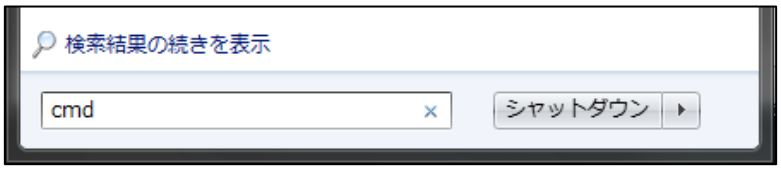

図 10　「プログラムとファイルの検索」に cmd を入力

３．コマンドプロンプト上で、**netstat** コマンドを実行します。

＜コマンド例＞

```
netstat -nao
```

※コマンドオプションはパソコンの環境に合わせて使い分けてください。

netstat /nao

netstat /naob

netstat /fao

netstat /faob

４．図 11 で示す通り、その端末の通信の接続情報一覧が表示されますので、外部と通信を行っている接続の「**外部アドレス**」と「**PID**」を確認し、記録します。

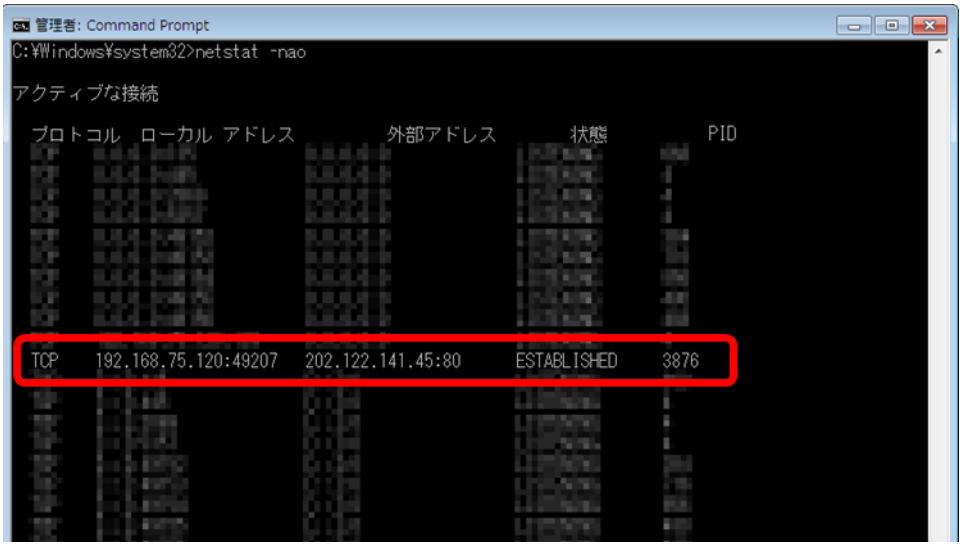

図 11　コマンドプロンプト上で通信の接続情報一覧を表示した場合の例
（外部アドレスはダミー）

５．コマンドプロンプト上で **tasklist** コマンドを実行します。コマンドには先ほど記録した PID を入力します。

＜コマンド例＞

```
tasklist /FI "PID eq 【記録した PID】"
```

６．表示されたプロセスとプロセスが行う通信が、組織や端末利用者の意図するものであるかを確認してください。

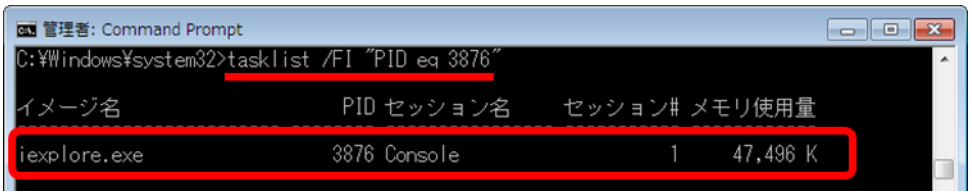

図 12　PID のプロセスを表示した場合の例

■不審な通信を発見した際の対応

万が一、不審と思われる通信などを行っている端末を発見した際の対応を以下に示します。

該当端末をネットワークから切り離す

被害を最小限に抑えるためには、まず該当端末をネットワークから切り離すことが重要です。その上で該当の端末や通信ログなどの詳細な調査を行ってください。

ファイアウォールやプロキシサーバーで通信をブロックする

不審な通信先を発見した場合、さらなる通信をさせないために、ファイアウォールやプロキシサーバー、導入済みの場合はウェブフィルタリングシステムで、不審な通信先との通信をブロックしてください。また、その不審な通信先との通信を試みる別の端末が存在しないかをチェックし、同様の端末があった場合は、こちらについても詳細な調査をしてください。

セキュリティベンダなどの専門家への相談

該当端末が踏み台とされ、他の端末へ感染が広がっている可能性も考えられます。セキュリティベンダなどの専門家に相談するなどして、正確な被害範囲や感染原因を把握した上で対応を進めることが重要です。

本件に関するお問い合わせ先
IPA　技術本部　セキュリティセンター
E-mail：tokusou@ipa.go.jp