STEP **01** 

エモテットの感染が発覚した場合、感染が疑われる 端末をネットワークから、また、感染が疑われる端末 が繋がっているネットワークを外部のインターネット から遮断しましょう。

発覚した時期が感染から間もない場合には、他の端 末に感染を広げてしまうリスクを下げることができる ため、確実に実施しましょう。



step 02 タスクマネージャーを起動し、詳細タブから実行 結果に表示されている「プロセス ID」を選択し、 タスクの終了を選択します。

ブロセス バフォーマンス アブリの履歴	<b>メタート</b> アツブ	ユーザー 詳細	サービス			
名前	PID	状態	CPU	メモリ (アクテ	UAC の仮想化	,
• ррисаловителенновиска	5340	実行中	00	4,216 K	無効	
C OUTODIOS CAR	6472	実行中	00	12,436 K	不許可	
FIET have seen the second	6184	実行中	00	3,208 K	無効	
@certreq.exe	8468	実行中	00	3,548 K	有効	
a much come	1696	実行中	00	504 K	無効	
Compatibilitation exe	960	実行中	00	80 K	不許可	
Conhosticke	9952	実行中	00	88 K	不許可	
conhost.exe	2892	実行中	00	6,936 K	無効	
Sand sectors et	1680	実行中	00	248 K	不許可	
Contraction Contraction	432	実行中	00	484 K	个計可	
The state of the state	520	実行中	00	680 K	不許可	
2 d Imenseve	5556	実行中	00	5,364 K	無効	
dihostext	7960	実行中	00	132 K	無効	
dumpcaplexe	9996	実行中	00	476 K	不許可	
S box in concernant	324	実行中	00	43,244 K	無効	
and the second s	5876	実行中	01	36,876 K	無効	

(♀ ダスク マネージャー

STEP 03 実行結果に表示されている「イメージパス」のう ちフォルダ部をエクスプローラーで開き、表示され ている exe を削除します。

L   ピ L =  certreq ファイル ホーム 共有	表示		-	
← → • ↑ 🖡 « Aj	ppData > Local > certreq	v O		2
- 01-0 TONT	名前	更新日時	種類	サイズ
■ デスクトップ ×	certreq.exe	2020/02/07 18:21	アプリケーション	429 KB
Aata				
🧯 log				
∎ log				
■ log ● PC ● ネットワーク				



再度 EmoCheck を実行し、Emotet を検知しない ことを確認ください。 C:¥Users¥k⊥n∙ ¥Downloads>emocheck x64 v002.exe

04. C



Emotet detection tool by JPCERT/CC. /ersion : 0.0.2 Nelease Date : 2020/02/10 ML : https://github.com/JPCERTCC/EmoCheck

motetは検知されませんでした。 以下のファイルに結果を出力しました。 **メ۷TT \_i= →、I**\_20200210110612\_emocheck.txt ツールのご利用ありがとうございました。 続行するには何かキーを押してください . . . C: Wusers Ni . r i NOownloads>

STEP 05

感染した端末が利用していたメールアカウントな どのパスワード変更。

横断的侵害で組織内に感染を広げる能力を持って いるため、添付ファイルを開いた端末だけでなく、 他の端末も併せて調査を実施する。

