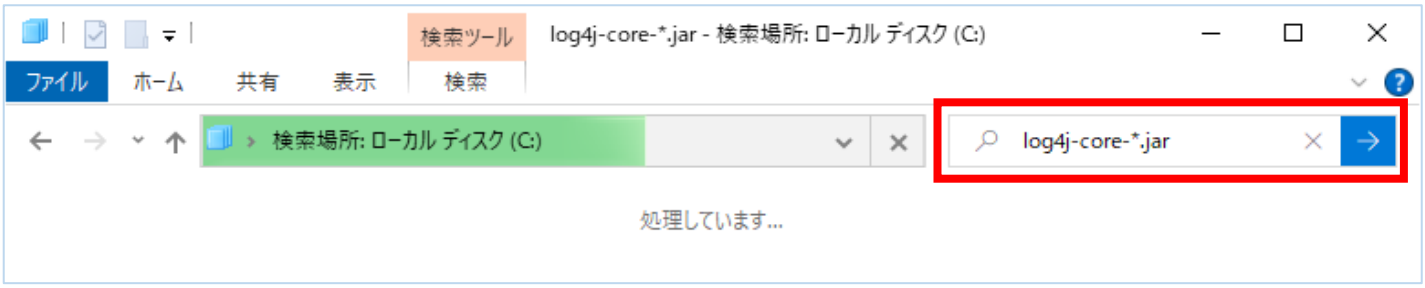
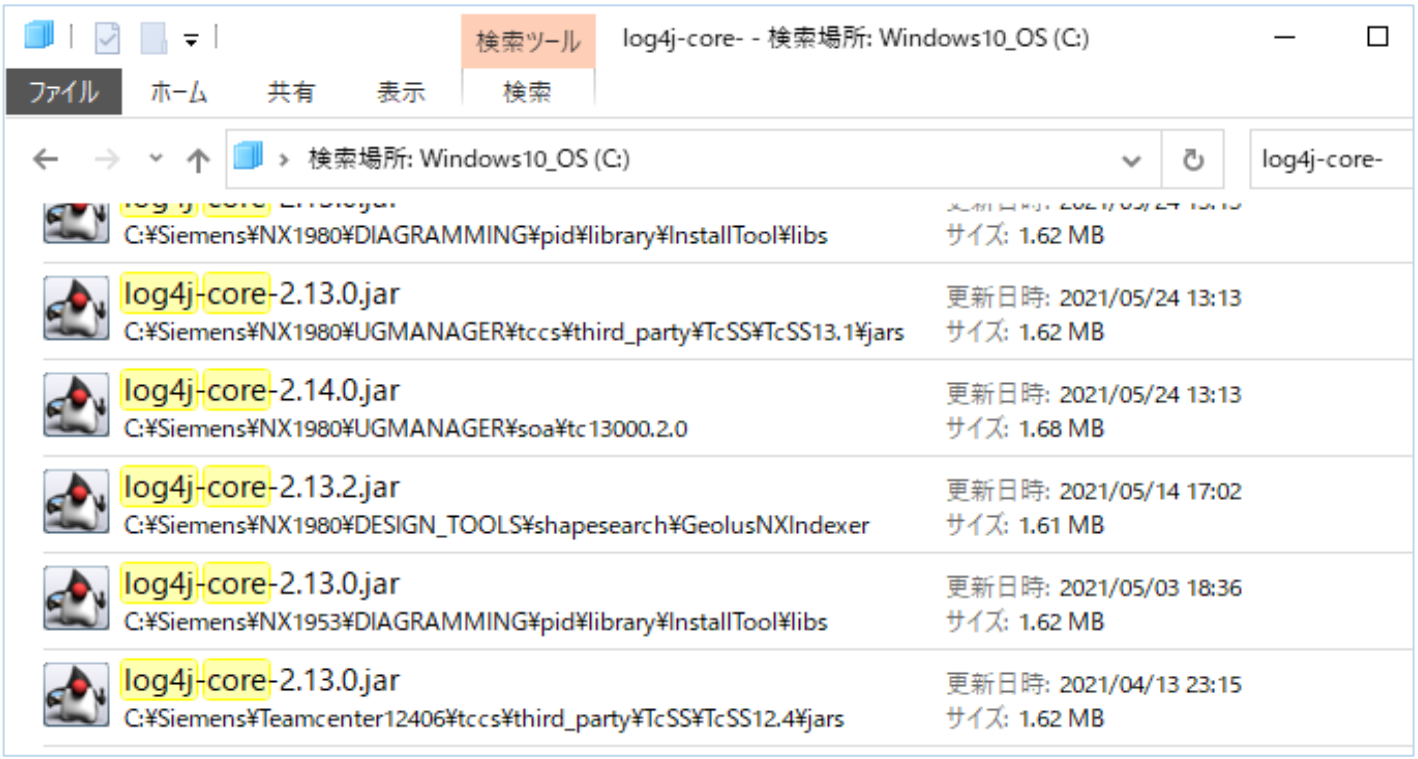
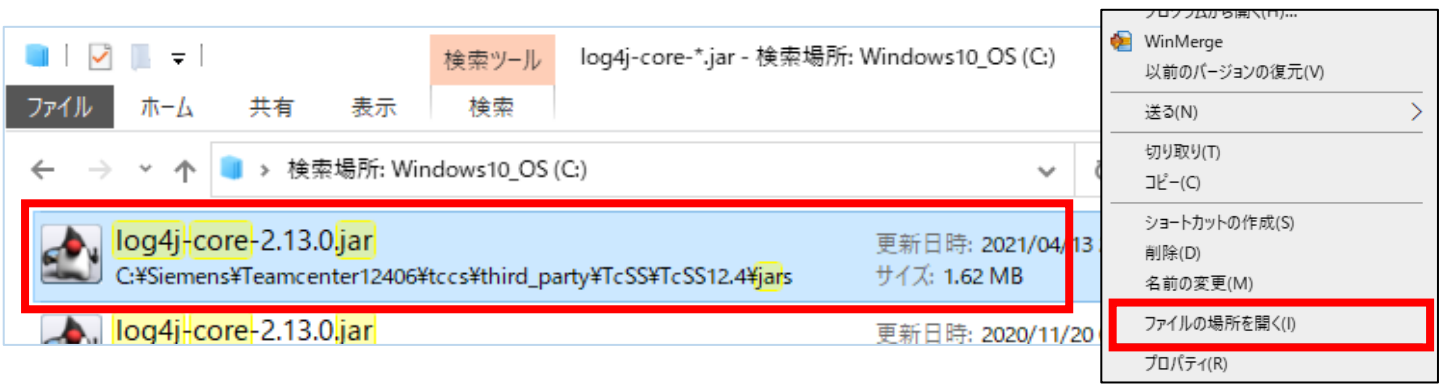
①. シーメンス製品のインストールフォルダのあるドライブ内で『log4j-core-*.jar』ファイルの検索をエクスプローラを使用して行います。



②. エクスプローラ上に表示される『log4j-core-<Version>.jar』ファイルで<Version>部が【2.16.0】未満のファイル全てに対して以降の回避策を実行します。（下図の場合、全てが対象となります）
※『log4j-core-<Version>.jar』の配置場所はご使用環境による為、本手順書の表示とは異なります。
※ 対象のファイルが検索（表示）されない場合は、これで終了です。（③以降の手順は不要です）



③. 以降、1つのファイルを例に手順を進めます。
対象の『log4j-core-<Version>.jar』ファイルを選択し、右クリックで[ファイルの場所を開く]を選択します。

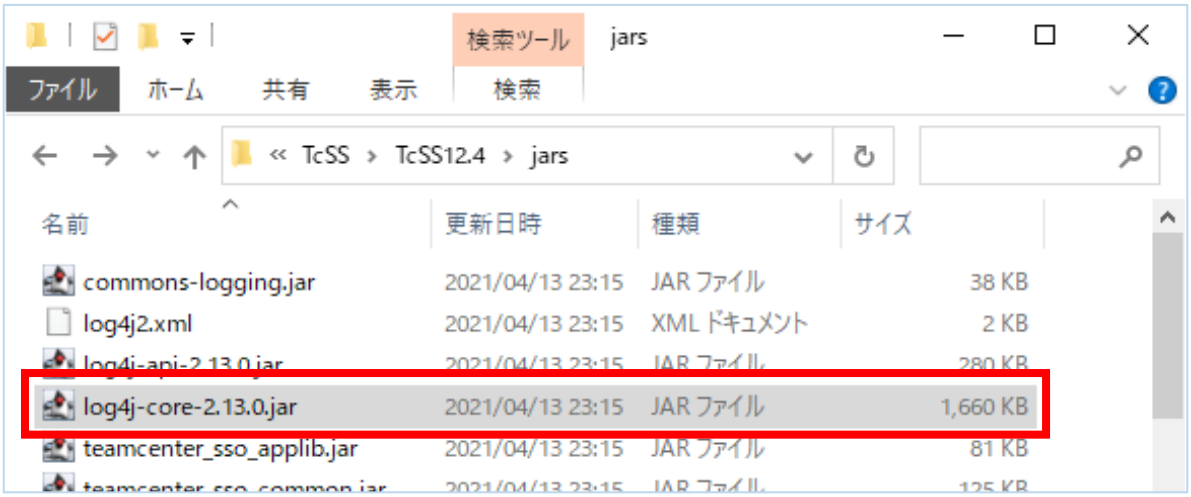


④. 対象の『log4j-core-<Version>.jar』ファイルの配置場所に移ります。

※念の為、対象となる『log4j-core-<Version>.jar』ファイルのバックアップをお取りください。

※バックアップは、拡張子を変更してお取りください。（例：***.jar_backup等）

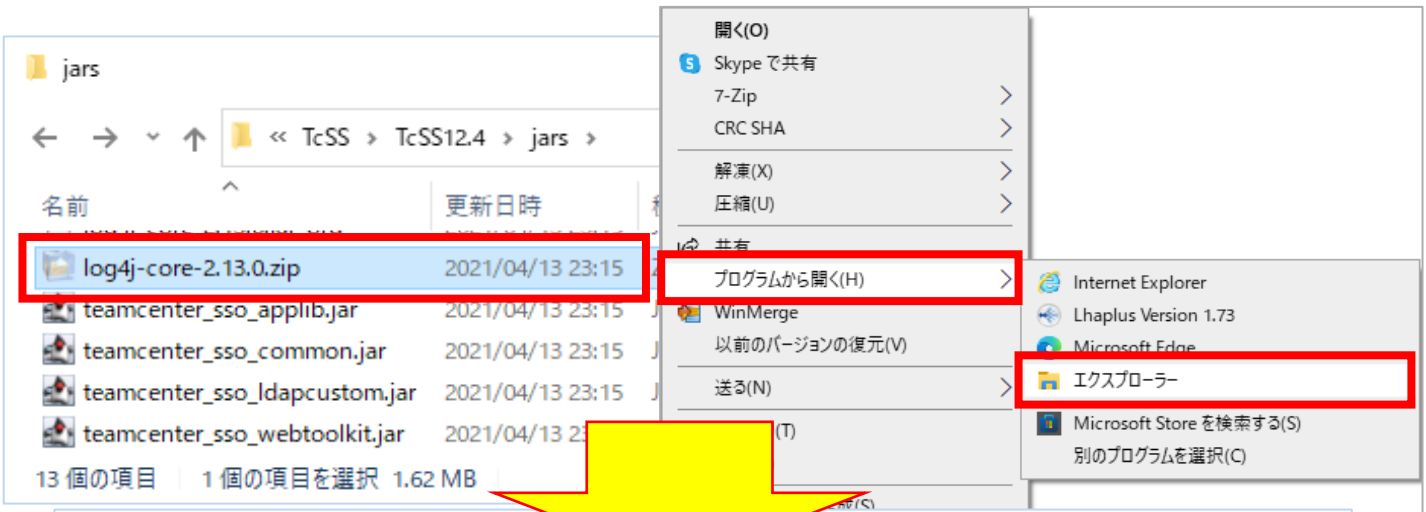
また、対象の『log4j-core-<Version>.jar』ファイルが「読取り専用」かどうかを確認し、「読取り専用」の場合は、「読取り専用」を解除します。

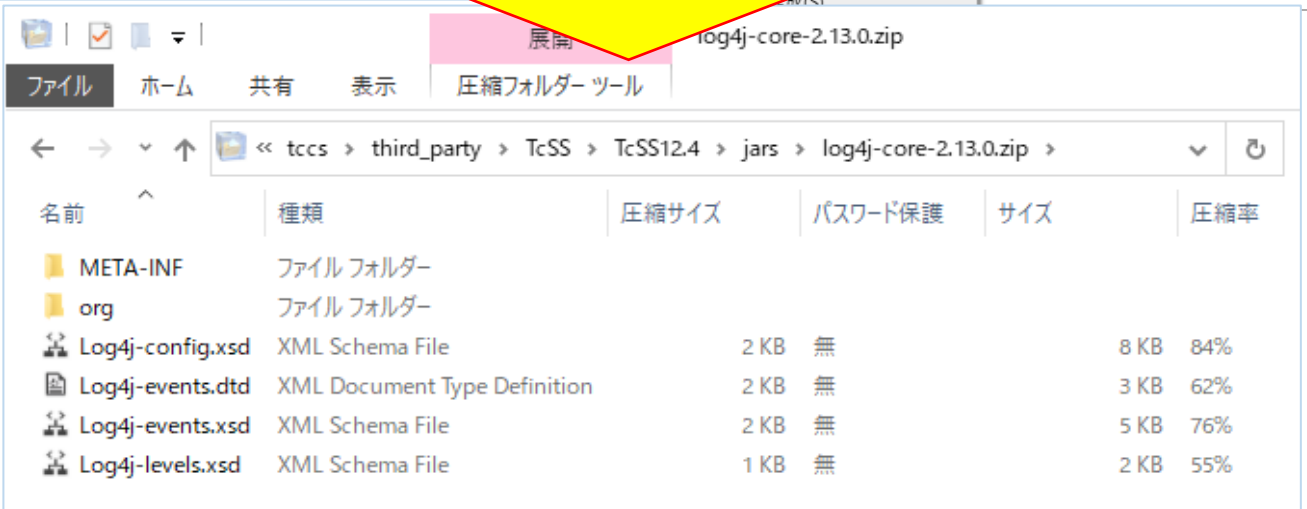


⑤. 対象の『log4j-core-<Version>.jar』ファイルの拡張子【.jar】を【.zip】に変更します。

変更後『log4j-core-<Version>.zip』ファイルを選択し、右クリックで、[プログラムから開く]-[エクスプローラ]を選択します。

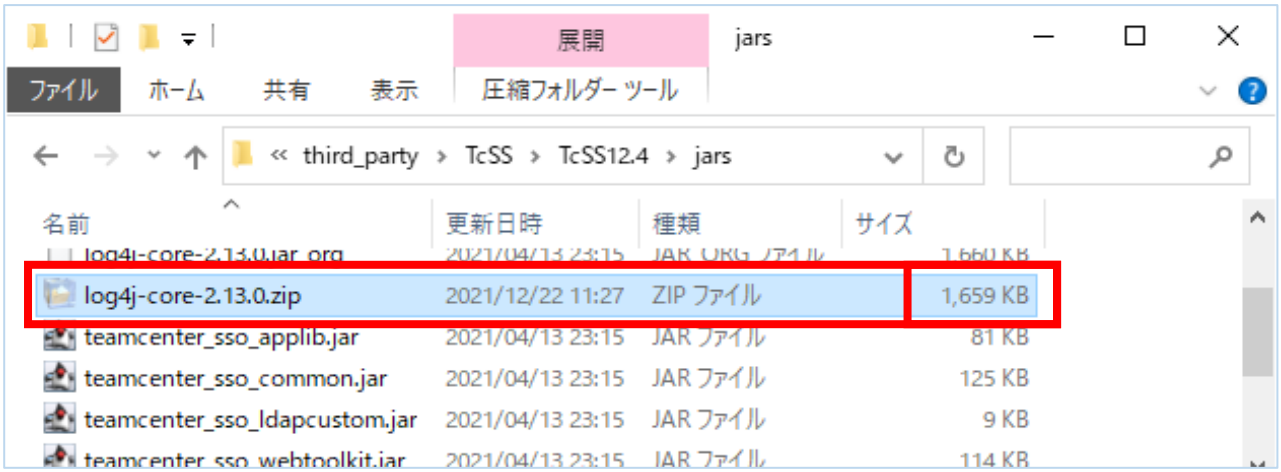
『log4j-core-<Version>.zip』ファイルの展開表示となります。





⑥. 前項から[org] - [apache] - [logging] - [log4j] - [core] - [lookup]フォルダまで展開します。
今回の脆弱性の問題は、[JndiLookup.class]ファイルが狙われることによって起こるので、
[JndiLookup.class]ファイルを【削除】します。

⑦. ⑤項の『log4j-core-<Version>.zip』ファイルの配置フォルダに戻ります。
⑥項でファイルを削除しているので、ファイルサイズが減少しています。



⑧. 『log4j-core-<Version>.zip』ファイルの拡張子【.zip】を【.jar】に変更します。
④項で「読取り専用」だった場合は、「読取り専用」に戻します。

本回避策の手順は終了です。
※④項のバックアップファイル（例：***.jar_backup等）は、不要な場合は適宜削除します。