Rev.20180605\_B0.2

**簡易証拠保全手順書**

**Windows編（β版）**

2018年6月5日

セクタンラボ

1. 本書の概要

本書は、マルウェア感染の疑いがあるWindowsパソコン（以下、調査対象PC）にログインし、フォレンジック調査に必要となる証拠（以下、エビデンス）を保全するための簡易証拠保全手順を記載します。

1. 前提条件と事前準備
   1. 前提条件
      1. 調査対象PCに管理者権限（Administrator権限）でログオンできること。
      2. 調査対象PCに調査用USBストレージを接続することができ、かつ書き込み可能な状態で認識できること。
      3. 調査対象PCで、調査用USBストレージに格納した証拠保全用プログラムを起動できること。
   2. 事前準備
      1. 調査対象PCの台数と同じ数の調査用USBストレージを用意し、個体を識別できるよう、ラベルを貼り付けするなどします。
      2. 調査対象PCごとに、1個の調査用USBストレージを割り当てます。  
         （例：調査用USBストレージNo.01は、調査対象PC-A専用とする。）
      3. 調査用USBストレージに、調査用プログラムを格納します。
2. 証拠保全手順

以下の手順を実行で証拠保全を実施します。また、各手順を開始した時刻を都度記録します。

* 1. 調査対象PCに、管理者権限でログインします。なお、すでに管理者権限でログインしている状態となっていた場合は、本手順は省略します。
  2. 調査対象PCに、調査用USBストレージを接続します。
  3. エクスプローラーで調査用USBストレージを開き、調査用スクリプトを実行します。
     1. Windows XPの場合

「ir-winxp.vbs」をダブルクリックして実行する。

* + 1. Windows Vista以降の場合

「ir-win7.vbs」をダブルクリックして実行する。

* 1. 「エビデンス取得処理を開始してよろしいですか？」というメッセージが表示されたら  
     「はい」をクリックします。
  2. 証拠保全スクリプトにより、USBストレージの「Evidence」フォルダに必要なエビデンスが収集されます。
  3. 全ての処理が終了すると「処理が終了しました」というメッセージが表示されます。
  4. 「Evidence」フォルダの内容を確認し、別表１のエビデンスが正常に収集できていることを確認し、USBストレージを取り外します。

1. 注意事項
   1. 本手順により、調査用USBストレージにマルウェアが混入している可能性があります。  
      作業後の調査用USBストレージは、他のパソコン等には絶対に接続しないでください。

以上

［別表１］　保全すべきエビデンス

Windows7環境

|  |  |  |
| --- | --- | --- |
| フォルダ名 | 内容 | 確認方法 |
| ルートフォルダ | ライブレスポンスデータ ほか | 次のファイルが格納されていることを確認する。   * ir-ListAutoruns.log * ir-ListDlls.log * ir-ListHandles.log * ir-ListTCPVcon.csv * ir-live.log * log.txt * setupapi.dev.log |
| EventLog | イベントログファイル | 拡張子がEvtxのファイルが複数格納されていることを確認する。 |
| NTFS | ファイルシステム関連 ファイル | 次のファイルが格納されていることを確認する。   * $MFT * $UsnJrnl\_$J.bin |
| Prefetch | Prefetchファイル | 拡張子pfのファイルが複数格納されていることを確認する。 |
| Registry | レジストリファイル | 次のファイルが格納されていることを確認する。   * SAM * security * software * system |
| UserProfiles | ユーザープロファイル | ログオンしたユーザー名のフォルダ、および「All Users」など、複数のフォルダが格納されていることを確認する。 |

Windows XP環境

|  |  |  |
| --- | --- | --- |
| フォルダ名 | 内容 | 確認方法 |
| ルートフォルダ | ライブレスポンスデータ ほか | 次のファイルが格納されていることを確認する。   * ir-ListAutoruns.log * ir-ListDlls.log * ir-ListHandles.log * ir-ListTCPVcon.csv * ir-live.log * log.txt * setupapi.log |
| config | イベントログファイル、 レジストリファイルほか | 拡張子がEvtのファイルなど、複数のファイルが格納されていることを確認する。 |
| NTFS | ファイルシステム関連 ファイル | 次のファイルが格納されていることを確認する。   * $MFT |
| Prefetch | Prefetchファイル | 拡張子pfのファイルが複数格納されていることを確認する。 |
| UserProfiles | ユーザープロファイル | ログオンしたユーザー名のフォルダ、および「All Users」など、複数のフォルダが格納されていることを確認する。 |