隔離保存フォルダからアイテムを復元する

この記事では、隔離保存フォルダからアイテムを復元する方法について説明します。

■Client Security/PSB wks/PSB Computer Protection/その他の Windows 製品
1.タスクトレイの f-secure アイコンをクリックし、コントロール画面を表示
2.「設定」ボタンをクリックし、設定画面を表示
3.「ウイルスとスパイウェアスキャン」をクリック
4.「リアルタイムスキャンを有効にする」のチェックを解除
5.「隔離保存フォルダを開く」をクリック
6.隔離処理されているファイルの一覧が表示されます。
7.復元するファイルを選択し「復元」ボタンをクリックします。
8.選択されたファイルが「パス名」記載の位置に復元されます
9.「閉じる」→「OK」でアクションセンタを閉じます
10.パス名の場所に移動し、復元されたファイルを暗号化 ZIP 圧縮します。(パスワード:infected)
11.【重要】手順 4 で解除したチェックを再度チェックしてリアルタイムスキャンを有効化して下さい
12.検体窓口まで検体ファイルを送付してください。

【手順】
■ServerSecurity の場合
1.WEB コンソールから、コントロール画面を表示
2.「リアルタイムスキャン」をクリックし、設定画面移動
3.「リアルタイムスキャン」のスイッチをクリックしオフに設定
4.「保存して適用」をクリック
5.「ファイルの隔離保存データベース」ボタンをクリックし、設定画面を表示
6.「隔離保存コンテンツ」欄で、復元するファイルのチェックボックスをチェック
7.「復元」ボタンをクリック
8.選択されたファイルが「パス名」記載の位置に復元されます
9.パス名の場所に移動し、復元されたファイルを暗号化 ZIP 圧縮します。(パスワード:infected)
10.【重要】手順 3 で解除したスイッチを再度オンにしてリアルタイムスキャンを有効化して下さい
11.検体窓口まで検体ファイルを送付してください。

隔離保存フォルダの復元ツールについて

隔離保存フォルダの復元ツール (**unquar.exe**) は、誤って隔離保存されたファイルを復元するために使用されます。また、アンインストール ツールで製品が削除された後に隔離保存されたフォルダを完全に削除するためにも使用できます。
Unquar.exe は https://download.f-secure.com/support/tools/unquar/unquar.exe からダウンロードできます。

1. **unquar.exe** を `c:\temp\` などの一時フォルダにコピーします。
2. コマンド プロンプトを開きます。
    a. **Windows XP** の場合、 **スタート** メニューから [**ファイル名を指定して実行**] を選択し、[**名前**] フィールドに `cmd` を入力して [**OK**] をクリックします。
    b. **Windows Vista/7** の場合、 **スタート** メニューで `cmd` を入力して [**OK**] をクリックします。
3. コマンド プロンプトで一時フォルダに移動します。たとえば、 `c:\temp\` に移動する場合、 `cd c:\temp\` を入力して **Enter** を押します。
4. 隔離保存したアイテムを表示するには
   a) 検出名: `unquar.exe -m recovery -i Trojan:W32/F-Secure_testfile.A`
   指定した種類のマルウェアを表示します (この例では Trojan:W32/F-Secure_testfile.A)
   b) 隔離保存した日付: `unquar.exe -m recovery -d 2011.04.15-2011.04.16`
   指定した日付/期間に隔離保存したマルウェアを表示します (この例では 2011/4/15～2011/4/16)。日付の形式は YYYY.MM.DD-YYYY.MM.DD で指定されます。
5. アイテムを復元するには

   参考: 隔離保存されたファイルの中にはマルウェアが含まれているものもありますので、復元するファイルが正しく選択されていることを確認してください。ファイルの安全性に確信がない場合、エフセキュアのサポートにご連絡ください。

   a) 検出名: `unquar.exe -m recovery -i Trojan:W32/F-Secure_testfile.A --doit`
   指定した種類のマルウェアを隔離保存フォルダから解除します (この例では Trojan:W32/F-Secure_testfile.A)。
   b) 隔離保存した日付: `unquar.exe -m recovery -d 2011.04.15-2011.04.16 --doit`
   指定した日付/期間に隔離保存したマルウェアを表示します (この例では 2011/4/15～2011/4/16)。日付の形式は YYYY.MM.DD-YYYY.MM.DD で指定されます。
6. 対象のファイルが元の場所に移動され、関連するレジストリの設定も復元されます。
   参考: スクリプトの使い方がよくわからない場合、エフセキュアのサポートにご連絡ください。

削除モード

ツールを使用して隔離保存フォルダそのものを削除することもできます。隔離保存フォルダは厳密な ACL によって保護されているため、通常は削除することができません。.ツールによって、ACL が無効になり、対象のコンテンツが再帰的に削除されます。

隔離保存フォルダを削除するには

1. **unquar.exe** を `c:\temp\` などの一時フォルダにコピーします。
2. コマンド プロンプトを開きます。
    a. **Windows XP** の場合、 **スタート** メニューから [**ファイル名を指定して実行**] を選択し、[**名前**] フィールドに `cmd` を入力して [**OK**] をクリックします。
    b. **Windows Vista/7** の場合、 **スタート** メニューで `cmd` を入力して [**OK**] をクリックします。
3. コマンド プロンプトで一時フォルダに移動します。たとえば、 `c:\temp\` に移動する場合、 `cd c:\temp\` を入力して **Enter** を押します。
4. `unquar.exe -del` を実行します

詳細

unquar.exe をコマンド プロンプトでパラメータなしで実行すると、ツールのパラメータに関するヘルプが表示されます。