【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成27年4月23日(2015.4.23)

【公表番号】特表2014-518582(P2014-518582A)
【公表日】平成26年7月31日(2014.7.31)
【年通号数】公開・登録公報2014-041
【出願番号】特願2014-508278(P2014-508278)
【国際特許分類】
Ｇ０６Ｆ　9/44　(2006.01)
Ｇ０６Ｆ　9/50　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　9/06　６２０Ａ
Ｇ０６Ｆ　9/06　６４０Ｈ

【誤訳訂正書】
【提出日】平成27年2月27日(2015.2.27)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
対象プロセスにＤＬＬインジェクションを行うためのインジェクションプログラム及びオペレーティングシステムを実行するプロセッサと、
前記オペレーティングシステム、前記インジェクションプログラム及び前記対象プロセスが保存されるメモリと、を備え、
前記インジェクションプログラムは、
ランチャープロセスを実行して実行プロセス経路及び実行プロセスパラメータを入力して前記ランチャープロセスの子プロセスとして前記対象プロセスを生成し、前記対象プロセスをサスペンドモードに設定するプロセス生成モジュールと、
前記対象プロセスのプロセスハンドルを用いて前記対象プロセスが積載されたメモリ領域を割り当てられ、前記対象プロセスにインジェクションしようとするＤＬＬファイルを実行するコードを挿入するコード挿入モジュールと、
前記対象プロセスのサスペンドモードを解除して前記対象プロセスを行わせる復元モジュールと、を備えることを特徴とするコンピュータ装置。
【請求項２】
前記インジェクションプログラムは、
前記オペレーティングシステムでシステム権限で動作するプロセスのプロセスＩＤを使って前記対象プロセスをシステム権限で行わせる権限変更モジュールをさらに備えることを特徴とする請求項１に記載のコンピュータ装置。
【請求項３】
前記権限変更モジュールは、前記オペレーティングシステムでシステム権限で動作するプロセスのプロセスＩＤを使って得られたプロセスハンドルによってトークンを開き、前記トークンをコピーし、
前記プロセス生成モジュールは、前記コピーされたトークンを使って前記対象プロセスを生成することを特徴とする請求項２に記載のコンピュータ装置。
【請求項４】
前記プロセス生成モジュールは、前記オペレーティングシステムでシステム権限で動作

するプロセスのプロセスＩＤを使って前記ランチャープロセスをシステム権限で行わせることを特徴とする請求項１に記載のコンピュータ装置。
【請求項５】
（ａ）オペレーティングシステムから、ユーザが実行を命令したプログラムに対応する対象プロセスの生成如何を通知される段階と、
（ｂ）ランチャープロセスを実行して実行プロセス経路及び実行プロセスパラメータを入力して前記ランチャープロセスの子プロセスとして前記対象プロセスを生成し、前記対象プロセスをサスペンドモードに設定する段階と、
（ｃ）前記対象プロセスのプロセスハンドルを用いて前記対象プロセスの積載されたメモリ領域を割り当てられ、前記対象プロセスにインジェクションしようとするＤＬＬファイルを実行するコードを挿入する段階と、
（ｄ）前記対象プロセスのサスペンドモードを解除して前記対象プロセスを行わせる段階と、を含むことを特徴とするＤＬＬインジェクション方法。
【請求項６】
前記（ａ）段階及び前記（ｂ）段階の間に、
（ｅ）前記オペレーティングシステムでシステム権限で動作するプロセスのプロセスＩＤを使って前記対象プロセスをシステム権限で行わせる段階をさらに含むことを特徴とする請求項５に記載のＤＬＬインジェクション方法。
【請求項７】
請求項５または６に記載のＤＬＬインジェクション方法をコンピュータで行わせるためのプログラムを記録したコンピュータで読み取り可能な記録媒体。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】０００７
【訂正方法】変更
【訂正の内容】
【０００７】
前記技術的課題を解決すための本発明によるＤＬＬインジェクション機能を持つコンピュータ装置は、対象プロセスにＤＬＬインジェクションを行うためのインジェクションプログラム及びオペレーティングシステムを実行するプロセッサと、前記オペレーティングシステム、前記インジェクションプログラム及び前記対象プロセスが保存されるメモリと、を備え、前記インジェクションプログラムは、ランチャープロセスを実行して実行プロセス経路及び実行プロセスパラメータを入力して前記ランチャープロセスの子プロセスとして前記対象プロセスを生成し、前記対象プロセスをサスペンドモードに設定するプロセス生成モジュールと、前記対象プロセスのプロセスハンドルを用いて前記対象プロセスが積載されたメモリ領域を割り当てられ、前記対象プロセスにインジェクションしようとするＤＬＬファイルを実行するコードを挿入するコード挿入モジュールと、前記対象プロセスのサスペンドモードを解除して前記対象プロセスを行わせる復元モジュールと、を備える。
【誤訳訂正３】
【訂正対象書類名】明細書
【訂正対象項目名】０００８
【訂正方法】変更
【訂正の内容】
【０００８】
前記技術的課題を解決すための、本発明によるＤＬＬインジェクション方法は、（ａ）オペレーティングシステムから、ユーザが実行を命令したプログラムに対応する対象プロセスの生成如何を通知される段階と、（ｂ）ランチャープロセスを実行して実行プロセス経路及び実行プロセスパラメータを入力して前記ランチャープロセスの子プロセスとして前記対象プロセスを生成し、前記対象プロセスをサスペンドモードに設定する段階と、（

ｃ）前記対象プロセスのプロセスハンドルを用いて前記対象プロセスの積載されたメモリ領域を割り当てられ、前記対象プロセスにインジェクションしようとするＤＬＬファイルを実行するコードを挿入する段階と、（ｄ）前記対象プロセスのサスペンドモードを解除して前記対象プロセスを行わせる段階と、を含む。
【誤訳訂正４】
【訂正対象書類名】明細書
【訂正対象項目名】０００９
【訂正方法】変更
【訂正の内容】
【０００９】
本発明によるＤＬＬインジェクション機能を持つコンピュータ装置及びＤＬＬインジェクション方法によれば、サスペンドモードで生成された対象プロセスのメモリ領域にＤＬＬ実行コードを挿入することで、他のＤＬＬインジェクション技法と衝突せずに安定してＤＬＬインジェクションを行える。また対象プロセスをシステム権限で行うことで、ＤＬＬインジェクションを行う他のプロセスが対象プロセスに対して行われることを防止する。

【誤訳訂正５】
【訂正対象書類名】明細書
【訂正対象項目名】００１４
【訂正方法】変更
【訂正の内容】
【００１４】
図１に示したように、プロセッサ１１０はオペレーティングシステム１１２を実行し、オペレーティングシステム１１２は、メモリ１２０に保存される。またプロセッサ１１０は、メモリ１２０に保存されているプログラムアプリケーション１２２からコンピュータプログラム指示事項を検索して実行し、インジェクションプログラム１１４を実行する。この時、インジェクションプログラム１１４はドライバ形態に具現され、レジストリ設定によりオペレーティングシステム１１２の起動時に適切な時点に自動で実行され、共通プログラムアプリケーションの一要素として具現されることもある。
【誤訳訂正６】
【訂正対象書類名】明細書
【訂正対象項目名】００２０
【訂正方法】変更
【訂正の内容】
【００２０】
プロセス生成モジュール１１４－１は、ランチャープロセスを行ってランチャープロセスの子プロセスとして対象プロセスを生成し、生成した対象プロセスをサスペンドモードに設定する。これは、対象プロセスが実行のためにメモリに積載された状態で、プロセス実行の完了前にインジェクションコードを挿入するためである。また対象プロセスは、ランチャープロセスの子プロセスとして生成されるので、プロセス生成モジュール１１４－１は、‘実行プロセス経路’及び‘実行プロセスパラメータ’を入力して子プロセスを生成する。
【誤訳訂正７】
【訂正対象書類名】明細書
【訂正対象項目名】００２１
【訂正方法】変更
【訂正の内容】
【００２１】
このように本発明で提案するインジェクションプログラム１１４が、サスペンドモード

として実行が中止された対象プロセスのメモリ領域にインジェクションコードを挿入した後、サスペンドモードを解除して対象プロセスを行わせれば、ＤＬＬインジェクションの時点が調節できてＤＬＬインジェクションの失敗を防止する。
【誤訳訂正８】
【訂正対象書類名】明細書
【訂正対象項目名】００２９
【訂正方法】変更
【訂正の内容】
【００２９】
以上で説明した過程によって、ＤＬＬインジェクションのためのＬｏａｄ　ＤＬＬＣｏｄｅの挿入過程が完了する。最後にコード挿入モジュール１１４－２は、エントリーポイントへの接近権限を元の状態で復旧させる（Ｓ２９０）。このように対象プロセスのメモリ領域にＬｏａｄ　ＤＬＬ　Ｃｏｄｅが挿入された後、復元モジュール１１４－３は、対象プロセスのサスペンドモードを解除し、対象プロセスを正常に行わせる。この時、コード挿入モジュール１１４－２によって対象プロセスのメモリ領域に挿入されたＬｏａｄ　ＤＬＬ　Ｃｏｄｅによってインジェクションされたｄｌｌが対象プロセスと共に行われる。
【誤訳訂正９】
【訂正対象書類名】明細書
【訂正対象項目名】００３０
【訂正方法】変更
【訂正の内容】
【００３０】
一方、インジェクションプログラム１１４が対象プロセスをサスペンドモードで実行してＤＬＬインジェクションを行うのは、他のＤＬＬインジェクション技法との衝突を防止して安定的にＤＬＬインジェクションを行わせるためである。このためには、前述したようにＤＬＬインジェクションの時点を異ならせるだけではなく、対象プロセスを他のＤＬＬインジェクション技法から防御する必要がある。
【誤訳訂正１０】
【訂正対象書類名】明細書
【訂正対象項目名】００３３
【訂正方法】変更
【訂正の内容】
【００３３】
図５は、権限変更モジュール１１４－４によって対象プログラムをシステム権限で行わせる過程を示すフローチャートである。図５を参照すれば、権限変更モジュール１１４－４は、先ず、すべてのウィンドウズ（登録商標）オペレーティングシステムで常にシステム権限で動作しているプロセス、例えば、‘ｗｉｎｌｏｇｏｎ．ｅｘｅ’のプロセスＩＤを得る（Ｓ４１０）。プロセスＩＤを得る方式としては、マイクロソフト社でプロセス情報を得られるように提供するＴｏｏｌ　Ｈｅｌｐライブラリのスナップショット方式を使う。

【誤訳訂正１１】
【訂正対象書類名】明細書
【訂正対象項目名】００３４
【訂正方法】変更
【訂正の内容】
【００３４】
次いで、権限変更モジュール１１４－４は、得たプロセスＩＤを使って‘ｗｉｎｌｏｇｏｎ．ｅｘｅ’のプロセスハンドルを開き（Ｓ４２０）、これを使って‘ｗｉｎｌｏｇｏ

ｎ．ｅｘｅ’のトークンを開く（Ｓ４３０）。一つのトークンには、ログオンセッションについての保安情報が含まれており、ユーザがオペレーティングシステムにログオンする時に作られた一つのトークンをコピーし、ユーザーが行うすべてのプロセスが行われる。

【誤訳訂正１２】
【訂正対象書類名】明細書
【訂正対象項目名】００３５
【訂正方法】変更
【訂正の内容】
【００３５】
ウィンドウズオペレーティングシステムでは、それぞれのユーザを独立して管理するためにセッションで権限を管理するが、基本的に一つのユーザがログオンすれば、一つのセッションを割り当てられて、割り当てられたセッション内で作業を行う。ログオンしたユーザに割り当てられるセッションと類似した方式で、最上位権限であるシステムについてもセッションが割り当てられ、オペレーティングシステム内部の重要な作業が処理される。

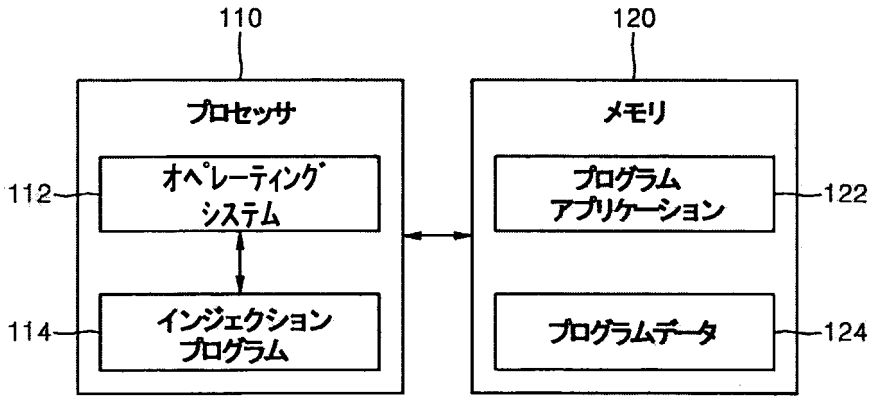
【誤訳訂正１３】
【訂正対象書類名】明細書
【訂正対象項目名】００３８
【訂正方法】変更
【訂正の内容】
【００３８】
最後に、権限変更モジュール１１４－４は、プロセス生成モジュール１１４－１がコピーされたトークンを使って対象プロセスを生成させる（Ｓ４７０）。この時、プロセス経路及びプロセスパラメータを指定することで、所望のプロセスを生成する。また本発明で対象プロセスが、本発明によるＤＬＬインジェクション装置の子プロセスとして生成されるという点は、前述した通りである。一方、プロセス生成モジュール１１４－１は、オペレーティングシステムでシステム権限で動作するプロセスのプロセスＩＤを使って、対象プロセスではないランチャープロセスをシステム権限で行え、それによって生成される子プロセスである対象プロセスもシステム権限で行われる。

【誤訳訂正１４】
【訂正対象書類名】明細書
【訂正対象項目名】００４１
【訂正方法】変更
【訂正の内容】
【００４１】
図６は、本発明によるＤＬＬインジェクション方法についての望ましい実施形態の実行過程を示すフローチャートである。図６を参照すれば、オペレーティングシステム１１２からユーザが実行を命令したプログラムに対応する対象プロセスの生成如何が通知されれば（Ｓ５１０）、インジェクションプログラム１１４のプロセス生成モジュール１１４－１は、ランチャープロセスを行ってランチャープロセスの子プロセスとして対象プロセスを生成し、生成された対象プロセスをサスペンドモードに設定する（Ｓ５２０）。この時、前述したように、権限変更モジュール１１４－４がシステム権限で行われる‘ｗｉｎｌｏｇｏｎ．ｅｘｅ’のトークンをコピーし、対象プロセスをシステム権限で生成させる。

【誤訳訂正１５】
【訂正対象書類名】明細書
【訂正対象項目名】００４３
【訂正方法】変更
【訂正の内容】
【００４３】
コード挿入モジュール１１４－２によって対象プロセスのメモリ領域にＤＬＬファイル

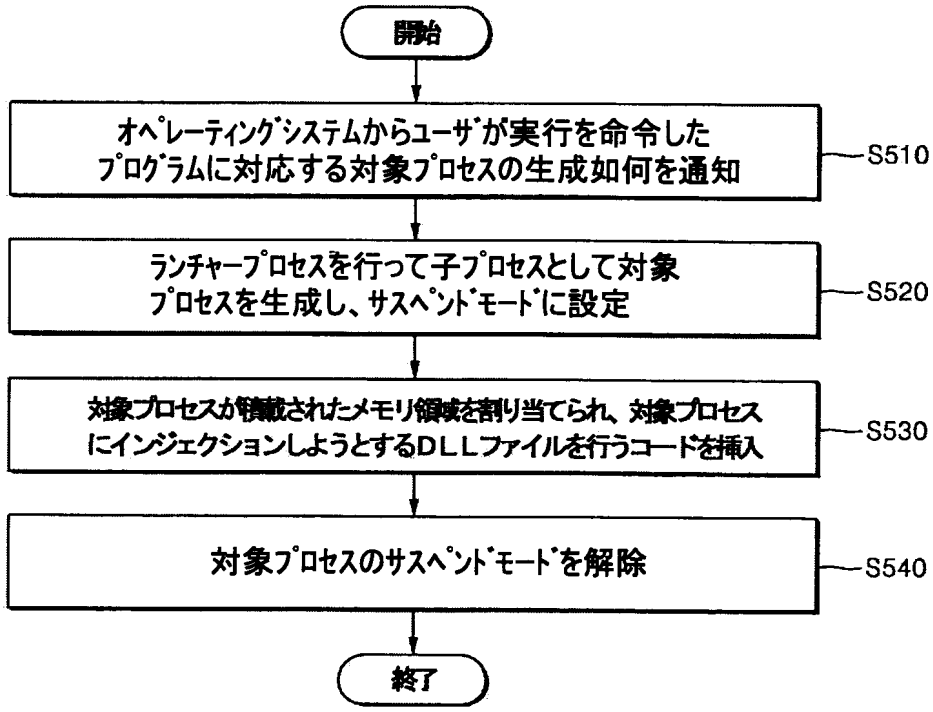
を行うためのＬｏａｄ　ＤＬＬ　Ｃｏｄｅが挿入されれば、復元モジュール１１４－３は、対象プロセスのサスペンドモードを解除して対象プロセスを行わせる（Ｓ５４０）。

【誤訳訂正１６】
【訂正対象書類名】図面
【訂正対象項目名】図１
【訂正方法】変更
【訂正の内容】
【図１】



【誤訳訂正１７】
【訂正対象書類名】図面
【訂正対象項目名】図６
【訂正方法】変更
【訂正の内容】

【図６】


開始
オペレーティングシステムからユーザが実行を命令した
プログラムに対応する対象プロセスの生成如何を通知
S510
ランチャープロセスを行って子プロセスとして対象
プロセスを生成し、サスペンドモードに設定
S520
対象プロセスが領域されたメモリ領域を割り当てられ、対象プロセス
にインジェクションしようとするDLLファイルを行うコードを挿入
S530
対象プロセスのサスペンドモードを解除
S540
終了