(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第5435392号
(P5435392)
(45)発行日　平成26年3月5日(2014.3.5)　(24)登録日　平成25年12月20日(2013.12.20)

(51)Int.Cl.　　F I
G06F 21/62 (2013.01)　　GO6F 21/24 １６３Ａ
G06F 21/52 (2013.01)　　GO6F 21/00 １５２

請求項の数 1　(全 6 頁)

(21)出願番号　特願2012-236036 (P2012-236036)
(22)出願日　平成24年10月9日 (2012.10.9)
審査請求日　平成24年11月6日 (2012.11.6)

(73)特許権者　512276692
朝田　昌男
神奈川県相模原市中央区相模原２－１２－１２　クリオ相模原２番館１０３号
(72)発明者　朝田　昌男
神奈川県相模原市中央区相模原２－１２－１２　クリオ相模原２番館１０３号

審査官　石田　信行

最終頁に続く

(54)【発明の名称】ＯＳに免疫機能を持たせる方法

(57)【特許請求の範囲】
【請求項１】
プロセス情報に
・資源へのアクセス権
・入力元
を有し、入力元の異物レベルを認識する為の異物レベル管理情報と、プロセスの資源へのアクセス権を決める為の資源アクセス情報より構成されるＯＳに免疫機能（システムの資源へのアクセスを制限する機能）を持たせる方法である。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＯＳに免疫機能を持たせる方法に関するものである。
【背景技術】
【０００２】
従来、プロセスは、異物のプロセスと通常のプロセスの区別なく生成されている。また、コマンドにおいても、異物のコマンドと通常のコマンドの区別なく実行されている。
【先行技術文献】
【特許文献】
【０００３】

【特許文献１】なし
【０００４】
ＯＳ及びサービスプログラムにおいて、異物の処理と通常の処理の区別がないなら、免疫機能を持たせる事は、不可能である。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
本発明は、ＯＳに免疫機能（プロセスの異物情報に応じてシステム資源のアクセスを制限する機能）を持たせる事により、異物の処理（ウイルス、ハッキング等）からシステムを守るためになされたものである。
【課題を解決するための手段】
【０００６】
ＯＳのカーネルは、異物レベルの情報を認識するために、データの入力元に異物レベルを設定した異物レベル管理情報を有する。
異物レベルが低いほど重要な資源である。
【０００７】
プロセスはプロセス情報に、異物情報として
・資源アクセス権
・異物レベル
の情報を有する。
資源アクセス権は、異物レベルが割り当てられた資源へのアクセス権である。
プロセス情報の異物レベルはプロセス生成時に使用した入力元、または、入力データの入力元の異物レベルである。
【０００８】
ＯＳのカーネルは、プロセス生成時のプロセスに、資源アクセス権を割り当てるための資源アクセス情報を有する。
資源アクセス情報は、対象（プログラム等）と対象に割り当てる資源アクセス権より構成される情報である。
【０００９】
プロセス情報の異物レベルは、低レベルから高レベルに遷移するが、反対に高レベルから低レベルに遷移しない。
【００１０】
ＯＳのカーネルは、プロセスの異物情報によってシステム資源（記憶媒体等）へのアクセスを制限する機能（免疫機能）を有する。
【発明の効果】
【００１１】
異物レベル０のプロセスが、外部インターネットからのコマンド要求を受け取ると、異物レベル２のプロセスに遷移するため、低い異物レベル（異物レベル０、異物レベル１）の資源へのアクセスが制限され、機密情報が漏れるのを防ぐことが出来る。また、異物レベル０のプロセスが特殊回線（異物レベル０のデバイス）からのコマンド要求に対しては、異物レベルが遷移しないのでアクセスが制限される事は無い。
ＵＳＢ等の異物レベル２に存在するプログラムの実行は、異物レベル２のプログラムと認識され、異物レベル２の資源にアクセスが制限されるので悪意のプログラムであってもシステムが壊される事を防げる。
【図面の簡単な説明】
【００１２】
【図１】本発明の実施の形態に係るＯＳに免疫機能を持たせる方法の関連図。
【発明を実施するための形態】
【００１３】
本発明は、入力元データの異物レベルを認識する為の異物レベル管理情報と、プロセス

の資源アクセス権を決める為の資源アクセス情報、及び、異物情報を有するプロセスより構成され、プロセスの異物情報よって免疫機能（システム資源へのアクセスを制限する機能）を実現する方法である。

【００１４】

異物レベル管理情報を具体例を用いて表現すると、

・異物レベル管理情報

（入力元）	（異物レベル）
キーボード	異物レベル０
専用回線	異物レベル０
社内イントラネットＬＡＮカード	異物レベル１
外部インターネットＬＡＮカード	異物レベル２
Ｃ：ドライブ	異物レベル０
Ｄ：ドライブ	異物レベル１
Ｄ：／ｔｅｍｐ／	異物レベル９
上記以外	異物レベル２

【００１５】

資源アクセス情報を具体例を用いて表現すると、

・資源アクセス情報

（対象）	（資源アクセス権）
プログラムＡ	０３０
プログラムＢ	１１１
異物レベル９のプロセス	０１１
上記以外	０３３

資源アクセス権の構成

▲１▼▲２▼▲３▼

▲１▼：異物レベルがプロセスの異物レベルよりも低い資源へのアクセス権

▲２▼：異物レベルがプロセスの異物レベルと同じ資源へのアクセス権

▲３▼：異物レベルがプロセスの異物レベルよりも高い資源へのアクセス権

資源アクセス権の構成その２

▲４▼▲５▼▲６▼

▲４▼：異物レベル０の資源へのアクセス権

▲５▼：異物レベル１の資源へのアクセス権

▲６▼：異物レベル２の資源へのアクセス権

資源アクセス権の数字の内容

０：アクセス拒否

１：読み込み許可

２：書き込み許可

３：読み書き許可

資源アクセス権の意味

０３０：異物レベルが同レベルの資源のみアクセス許可

１１１：全資源への読み込み許可

０３３：異物レベルが同レベルと高レベルの資源のみアクセス許可

【実施例】

【００１６】

以下、本発明の実施の形態について図１を用いて説明する。

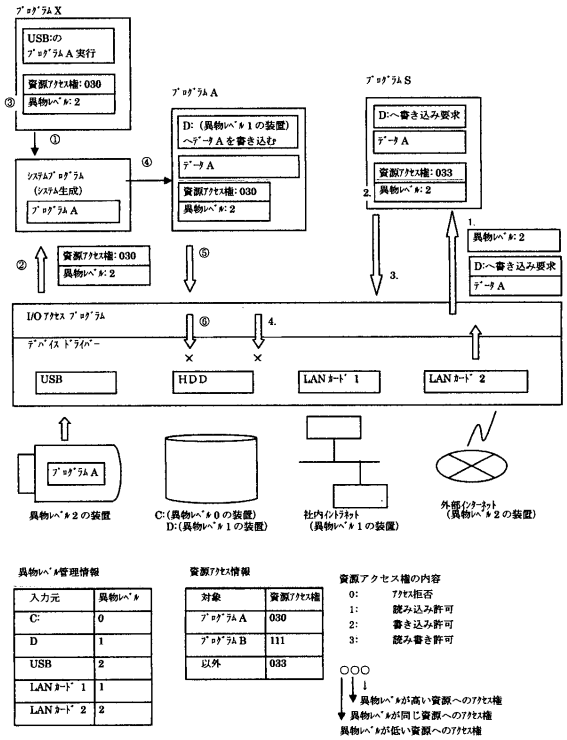
ＵＳＢカードに存在するプログラムＡを実行する場合を図１を用いて説明する。

▲１▼　プログラムＸは、ＵＳＢカードに存在するプログラムＡのプロセス生成をシステムプログラムに依頼する。

▲２▼　システムプログラムは、Ｉ／Ｏアクセスプログラムにデバイス（異物レベル２）からプログラムＡの読み込みを依頼する。

▲３▼　Ｉ／Ｏアクセスプログラムは、資源アクセス情報よりプログラムＸの異物レベルを２に設定する。
▲４▼　システムプログラムは、新しいプロセスを生成し、生成したプロセスの異物レベルに２、資源アクセス権に０３０（異物レベルが同レベルの資源のみアクセス許可）を設定する。
▲５▼　プログラムＡが、Ｉ／Ｏアクセスプログラムに、Ｄ：ドライブ（異物レベル１の資源）へデータＡの書き込み要求をする。
▲６▼　Ｉ／Ｏアクセスプログラムは、プログラムＡの異物レベルと資源アクセス権から、Ｄ：ドライブへデータＡの書き込み要求を拒否する。
　次に、サービスプログラムが外部インターネットからコマンドを受けた場合を図１を用いて説明する。
　１．プログラムＳはＩ／Ｏアクセスプログラムからデータを読み込む。
　２．Ｉ／Ｏアクセスプログラムは、データの入力元（ＬＡＮカード２）の異物レベル２をプログラムＳの異物レベルに設定する。
　３．プログラムＳはＩ／ＯアクセスプログラムにＤ：ドライブへデータＡの書き込みを要求する。
　４．Ｉ／Ｏアクセスプログラムは、プログラムＳの資源アクセス権と異物レベルより、Ｄ：ドライブへの書き込みを拒否する。
【産業上の利用可能性】
【００１７】
　ＯＳ自身に免疫機能を持つので、比較的容易に情報の流失や改ざんを防ぐことが出来る。
【符号の説明】
【００１８】
　０３０　　異物レベルが同レベルの資源のみ読み書き許可
　１１１　　全資源への読み込み許可
　０３３　　異物レベルが同レベルと高レベルの資源のみ読み書き許可
【要約】
【課題】・プログラムを実行する場合、異物の処理と通常の処理の区別なく実行されている。また、コマンド要求においても、異物のコマンド要求と通常のコマンド要求の区別なく実行されている。このため悪意のプログラムやコマンド要求からシステムの資源を守ることは困難である。
【解決手段】上記の目的を達成するために、本発明では、以下のような手段を講じる。
プロセス情報に
　・資源へのアクセス権
　・入力元
を持たせ、どの入力元からプロセスを生成したか、またどの入力元からのコマンド要求かを識別することで、異物の処理と通常の処理を区別する。異物の処理からシステムの資源へのアクセスを制限することで、システムを守る。
【選択図】図１

【図１】



異物ﾚﾍﾞﾙ管理情報

入力元	異物ﾚﾍﾞﾙ
C:	0
D	1
USB	2
LANｶｰﾄﾞ 1	1
LANｶｰﾄﾞ 2	2

資源ｱｸｾｽ情報

対象	資源ｱｸｾｽ権
ﾌﾟﾛｸﾞﾗﾑA	030
ﾌﾟﾛｸﾞﾗﾑB	111
以外	033

資源アクセス権の内容

0: ｱｸｾｽ拒否
1: 読み込み許可
2: 書き込み許可
3: 読み書き許可

○○○
↓
異物ﾚﾍﾞﾙが高い資源へのｱｸｾｽ権
異物ﾚﾍﾞﾙが同じ資源へのｱｸｾｽ権
異物ﾚﾍﾞﾙが低い資源へのｱｸｾｽ権

フロントページの続き

(56)参考文献 特開２００２－１３３３８８（ＪＰ，Ａ）
特開２００４－７０６７４（ＪＰ，Ａ）
特開２０１０－１２３１１５（ＪＰ，Ａ）
特開２０１３－５４１０８７（ＪＰ，Ａ）
国際公開第２００９／０９６５６１（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　２１／５２