(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6254414号
(P6254414)
(45)発行日　平成29年12月27日(2017.12.27)　(24)登録日　平成29年12月8日(2017.12.8)

(51)Int.Cl.　　F I
G06F 9/445 (2006.01)　　G06F 9/06 650C
G06F 11/00 (2006.01)　　G06F 9/06 630B
　　G06F 9/06 610L

請求項の数 16　(全 17 頁)

(21)出願番号　特願2013-211423(P2013-211423)
(22)出願日　平成25年10月8日(2013.10.8)
(65)公開番号　特開2014-96142(P2014-96142A)
(43)公開日　平成26年5月22日(2014.5.22)
審査請求日　平成28年9月13日(2016.9.13)
(31)優先権主張番号　特願2012-224574(P2012-224574)
(32)優先日　平成24年10月9日(2012.10.9)
(33)優先権主張国　日本国(JP)

(73)特許権者　000104652
キヤノン電子株式会社
埼玉県秩父市下影森１２４８番地
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理システムおよび情報処理方法

(57)【特許請求の範囲】
【請求項１】
プログラムの起動およびプログラムの生成または変更の検知、もしくは、プログラムの検索を行う検知手段と、
プログラムを識別する識別手段と、
実行が許可されたプログラムのリストであるホワイトリスト、および実行が禁止されたプログラムのリストであるブラックリストのうち一方のリストにプログラムを登録する登録手段とを有し、
前記識別手段は、前記検知手段によって起動が検知されたプログラムまたは前記検知手段の検索によって検出されたプログラムのプログラム情報に基づき、前記プログラムがプログラム情報に関する所定の基準を満たすか否かを判定し、
前記登録手段は、前記所定の基準を満たすと判定されたプログラムを前記一方のリストに登録し、
前記登録手段は、前記所定の基準を満たすと判定されたプログラムに昇格権限を付与するために、前記プログラムと前記昇格権限の対応を前記一方のリストに登録し、
前記検知手段によって前記昇格権限が付与されたプログラムによる子プログラムの生成または変更が検知された場合、前記登録手段は、前記子プログラムを前記一方のリストに登録することを特徴とする情報処理装置。
【請求項２】
前記識別手段は、前記検知または検出されたプログラムが前記ホワイトリストおよび前

記ブラックリストのうち他方のリストに登録されているか否かを判定し、
前記登録手段は、前記他方のリストに登録されていないと判定された前記検知または検出されたプログラムに前記昇格権限を付与する請求項１に記載された情報処理装置。
【請求項３】
前記登録手段は、前記検知手段によって前記昇格権限が付与されたプログラムによる次の世代のプログラムの生成または変更が検知されると、前記次の世代のプログラムを前記一方のリストに登録する処理を再帰的に繰り返すことを特徴とする請求項１に記載された情報処理装置。
【請求項４】
前記検知手段によって前記昇格権限が付与されたプログラムによる前記次の世代のプログラムの起動が検知された場合、前記登録手段は、前記次の世代のプログラムに前記昇格権限を付与することを特徴とする請求項３に記載された情報処理装置。
【請求項５】
前記検知手段によって前記昇格権限が付与された前記次の世代のプログラムによる他の次の世代のプログラムの起動が検知された場合、前記登録手段は、前記他の次の世代のプログラムに前記昇格権限を付与することを特徴とする請求項３に記載された情報処理装置。
【請求項６】
前記検知手段によって前記昇格権限を付与されたプログラムによるインストーラの起動が検知された場合、前記登録手段は、前記インストーラに前記昇格権限を付与することを特徴とする請求項１に記載された情報処理装置。
【請求項７】
前記登録手段は、予め記憶された生成プログラム群に属するプログラムから生成され、かつ、予め記憶された起動プログラム群に属するプログラムから起動されたプログラムに、前記昇格権限を付与することを特徴とする請求項１に記載された情報処理装置。
【請求項８】
前記識別手段は、前記検知手段によって前記昇格権限が付与されたプログラムによる次の世代のプログラムの生成または変更が検知されると、前記次の世代のプログラムのプログラム情報に基づき、前記次の世代のプログラムが前記他方のリストに登録されているか否かを判定し、
前記登録手段は、前記他方のリストに登録されていないと判定された次の世代のプログラムに前記昇格権限を付与することを特徴とする請求項２に記載された情報処理装置。
【請求項９】
前記登録手段は、前記他方のリストに登録されていると判定された次の世代のプログラムの登録を前記一方のリストから削除することを特徴とする請求項８に記載された情報処理装置。
【請求項１０】
前記検知手段によって前記昇格権限が付与されたプログラムによる次の世代のプログラムの起動が検知された場合、前記識別手段は、前記起動が検知されたプログラムのプログラム情報に基づき、前記プログラムが、前記他方のリストに登録されているか否かの判定、または、前記一方のリストに登録されているか否かの判定を行い、
前記登録手段は、前記他方のリストに登録されていないと判定されたプログラム、または、前記一方のリストに登録されていないと判定されたプログラムについて、前記一方のリストに登録するための処理を実行することを特徴とする請求項２、８、９の何れか一項に記載された情報処理装置。
【請求項１１】
さらに、前記一方のリストに基づいてプログラムの起動を許可または阻止する制御手段を有することを特徴とする請求項１から請求項１０の何れか一項に記載された情報処理装置。
【請求項１２】

前記プログラム情報にはディジタル署名が含まれることを特徴とする請求項１から請求項１１の何れか一項に記載された情報処理装置。
【請求項１３】
プログラムの起動およびプログラムの生成または変更の検知、もしくは、プログラムの検索を行う検知手段、プログラムを識別する識別手段、実行が許可されたプログラムのリストであるホワイトリスト、および実行が禁止されたプログラムのリストであるブラックリストのうち一方のリストにプログラムを登録する登録手段を有する情報処理装置の情報処理方法であって、
前記識別手段が、前記検知手段によって起動が検知されたプログラムまたは前記検知手段の検索によって検出されたプログラムのプログラム情報に基づき、前記プログラムがプログラム情報に関する所定の基準を満たすか否かを判定し、
前記登録手段が、前記所定の基準を満たすと判定されたプログラムを前記一方のリストに登録し、
前記登録手段は、前記所定の基準を満たすと判定されたプログラムに昇格権限を付与するために、前記プログラムと前記昇格権限の対応を前記一方のリストに登録し、
前記検知手段によって前記昇格権限が付与されたプログラムによる子プログラムの生成または変更が検知された場合、前記登録手段は、前記子プログラムを前記一方のリストに登録することを特徴とする情報処理方法。
【請求項１４】
請求項１から請求項１２の何れか一項に記載された情報処理装置と、
ネットワークを介して、前記情報処理装置に前記一方のリストのデータを送信するサーバ装置とを有することを特徴とする情報処理システム。
【請求項１５】
前記サーバ装置は、前記ネットワークを介して、前記情報処理装置から前記一方のリストに登録すべきプログラムに関する情報を受信することを特徴とする請求項１４に記載された情報処理システム。
【請求項１６】
コンピュータを請求項１から請求項１２の何れか一項に記載された情報処理装置の各手段として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、プログラムの起動可否を制御する情報処理に関する。
【背景技術】
【０００２】
近年、企業に対するサイバー攻撃の新しい形態として、企業内の特定の社員が使用または所有するコンピュータを標的にし、そのコンピュータにマルウェアを感染させ、企業内の情報を盗み出す、標的型攻撃という手法が増えている。
【０００３】
従来のアンチウィルスソフトなどは、ブラックリスト方式によるウィルス定義ファイルを用いる。しかし、コンピュータウィルスを含むマルウェアの種類は日に万単位で増加している。そのため、ウィルス定義ソフトの更新は、マルウェアの急増に追いつかない状況にあり、従来のアンチウィルスソフトによる標的型攻撃への対処は難しい状況にある。
【０００４】
一方、既知のプログラムの実行を許可し、それ以外のプログラムの実行を制限する、いわゆるホワイトリスト型の制御方式を用いる標的型攻撃への対処が存在する（例えば、特許文献1）。ホワイトリスト型の制御方式を用いるコンピュータのプログラムをアップデートする場合、当該アップデート用のアップデータをホワイトリストに登録すればよい。
【０００５】
しかし、アップデータは、通常、別の実行ファイルを複数生成することが多い。従って

、アップデータをホワイトリストに登録したとしても、アップデータが生成する実行ファイルはホワイトリストに登録されない。その結果、アップデータが生成した実行ファイルがコンピュータにインストールされてアップデートが完了したとしても、それら実行ファイルを起動することができず、アップデート後のプログラムが正常に動作しない場合がある。

【０００６】

従来、システム管理者などは、アップデータが生成する実行ファイルを抽出し、当該実行ファイルをホワイトリストに登録する作業を行っていた。この方法によれば、アップデータが信頼できるか否かの判断だけでなく、実行ファイルを抽出しホワイトリストを更新する負担が大きい作業が必要になる。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特開2009-259160号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

本発明は、リスト型の制御方式を用いる場合の、リストの更新にかかる作業を軽減することを目的とする。

【課題を解決するための手段】

【０００９】

本発明は、前記の目的を達成する一手段として、以下の構成を備える。

【００１０】

本発明にかかる情報処理装置は、プログラムの起動およびプログラムの生成または変更の検知、もしくは、プログラムの検索を行う検知手段と、プログラムを識別する識別手段と、実行が許可されたプログラムのリストであるホワイトリスト、および実行が禁止されたプログラムのリストであるブラックリストのうち一方のリストにプログラムを登録する登録手段とを有し、前記識別手段は、前記検知手段によって起動が検知されたプログラムまたは前記検知手段の検索によって検出されたプログラムのプログラム情報に基づき、前記プログラムがプログラム情報に関する所定の基準を満たすか否かを判定し、前記登録手段は、前記所定の基準を満たすと判定されたプログラムを前記一方のリストに登録し、前記登録手段は、前記所定の基準を満たすと判定されたプログラムに昇格権限を付与するために、前記プログラムと前記昇格権限の対応を前記一方のリストに登録し、前記検知手段によって前記昇格権限が付与されたプログラムによる子プログラムの生成または変更が検知された場合、前記登録手段は、前記子プログラムを前記一方のリストに登録することを特徴とする。

【発明の効果】

【００１１】

本発明によれば、リスト型の制御方式を用いる場合の、リストの更新にかかる作業を軽減することができる。

【図面の簡単な説明】

【００１２】

【図１】ホワイトリスト制御システムの構成例を示すブロック。

【図２】サーバが存在しないホワイトリスト制御システムの構成例を示すブロック図。

【図３】ホワイトリストの一例を示す図。

【図４】サーバに存在するホワイトリストマスタの一例を示す図。

【図５】ホワイトリスト制御処理の一例を説明するフローチャート。

【図６】インストーラが起動された場合のホワイトリスト制御処理の一例を説明するフローチャート。

【図７】プログラム起動をトリガとするホワイトリストの更新処理を説明するフローチャ

ート。
【図８】プログラム検索をトリガとするホワイトリストの更新処理を説明するフローチャート。
【発明を実施するための形態】
【００１３】
以下、本発明にかかる実施例の情報処理システムの情報処理を図面を参照して詳細に説明する。
【００１４】
［システムの構成］
図1のブロックによりホワイトリスト制御システムの構成例を示す。ホワイトリスト制御システムは、情報処理装置と、情報処理装置を管理するサーバ装置を含む。
【００１５】
図1において、クライアントコンピュータ（以下、クライアント）10は、ホワイトリスト制御システムにおける情報処理装置である。クライアント10は、例えば、企業、学校、行政機関または家庭などに設置されたパーソナルコンピュータ(PC)や、個人が使用または所有するタブレット端末やスマートフォンなどのコンピュータ機器である。
【００１６】
サーバコンピュータ（以下、サーバ）20は、ホワイトリスト制御システムにおける情報処理装置を管理するサーバ装置である。サーバ20は、複数のクライアント10からホワイトリスト120の情報を取得してデータベース化したり、定期的にクライアント10にホワイトリストデータを送信してホワイトリスト120の更新を行う。
【００１７】
ネットワーク300は、インターネットやイントラネットなどのコンピュータネットワークである。クライアント10は、ネットワーク300を介して、サーバ20や、図示しないウェブサーバやFTPサーバなどと接続する。
【００１８】
なお、簡潔化のため図1にはクライアント10とサーバ20を一台ずつ示すが、実際には、ホワイトリスト制御システムに複数のクライアントや複数のサーバが存在することができる。
【００１９】
●クライアント
クライアント10において、演算装置10Cはマイクロプロセッサ(CPU)である。演算装置10Cは、メモリ10EのROMに格納されたBIOSなどのブートプログラムに従い記憶装置10Bに格納されたオペレーティングシステム(OS)を起動し、さらにOSに従い各種の常駐プログラム（例えば制御プログラム113など）を起動する。その際、演算装置10Cは、メモリ10EのRAMをワークエリアとして使用する。また、OSは例えばWindows（登録商標）、Mac OS（登録商標）、Linux（登録商標）、iOS（商標）、Android（商標）などである。
【００２０】
記憶装置10Bは、ハードディスクドライブ(HDD)やソリッドステートドライブ(SSD)などであり、OSのほかにクライアント10上で稼働する各種のプログラム100やデータ101を格納する。詳細は後述するが、記憶装置10Bが格納する各種プログラム100には識別プログラム110、登録プログラム111、検知プログラム112、制御プログラム113、ファイル検索ツール114などが含まれる。
【００２１】
なお、プログラム100は、識別プログラム110など各種機能ごとのプログラムを複数備えてもよいし、各種機能を備えた一つのプログラムでもよい。また、詳細は後述するが、記憶装置10Bが格納する各種データ101にはホワイトリスト120、昇格基準ルール130、ブラックリスト140などが含まれる。
【００２２】
I/Oデバイス10Aは、ポインティングデバイス（マウスなど）やキーボードに接続するた

めの入出力インタフェース(I/F)、または、タッチパネルを組み込んだディスプレイなどである。なお、キーボードはソフトウェアキーボードでもよい。また、I/Oデバイス10Aは、入力された操作者の音声を音声認識機能によって認識し、認識した音声を演算装置10Cへ伝達する、マイク等を含む音声式入力部でもよい。また、I/Oデバイス10Aは、情報を表示するためのユーザインタフェース(UI)としても機能する。

【００２３】

ネットワークI/F 10Dは、ネットワーク300とのインタフェースであり、他のコンピュータと通信するための通信回路である。演算装置10Cは、ネットワークI/F 10Dを介して、例えばホワイトリスト120の一部データなどの情報をサーバ20から受信し、また、各種情報をサーバ20に送信する。

【００２４】

●サーバ

サーバ20において、演算装置20Cはマイクロプロセッサ(CPU)である。演算装置20Cは、メモリ20EのROMに格納されたBIOSなどのブートプログラムに従い記憶装置20Bに格納されたOSを起動する。さらに、演算装置20Cは、記憶装置20Bから管理コンソール210をメモリ20EのRAMにロードする。そして、複数のクライアント10から情報（例えば、ホワイトリスト120の情報など）を取得してデータベース化したり、逆に、クライアント10に対して情報を送信してホワイトリスト120の更新などを行う。

【００２５】

記憶装置20Bは、HDDやSSDなどであり、OSのほかにサーバ20上で稼働する管理コンソール210を含む各種のプログラム200やデータ201を格納する。詳細は後述するが、記憶装置10Bが格納する各種データ201にはホワイトリストマスタ220、昇格基準ルール230、ブラックリストマスタ240、ホワイトリスト候補250などが含まれる。

【００２６】

I/Oデバイス20Aは、ポインティングデバイス（マウスなど）、キーボード、モニタに接続するためのインタフェース(I/F)であり、モニタは情報を表示するためのUIとして機能する。ネットワークI/F 20Dは、ネットワーク300とのインタフェースであり、クライアント10など他のコンピュータと通信するための通信回路である。

【００２７】

演算装置20Cは、ネットワークI/F 20Dを介して、複数のクライアント10からホワイトリスト120やブラックリスト140に関する情報を受信し、受信した情報に基づき、ホワイトリストマスタ220やブラックリストマスタ250を管理する。

【００２８】

ホワイトリスト制御システムにおいて、サーバ20は必須の構成ではない。図2のブロック図によりサーバ20が存在しないホワイトリスト制御システムの構成例を示す。図2の構成においては、クライアント10とサーバ20の通信は不要になるため、ネットワーク300およびネットワークI/F 10Dもオプションである。

【００２９】

また、ホワイトリスト制御システムはシンクライアント（例えば、ターミナルサービスなど）を利用した構成としてもよい。シンクライアントは、クライアントがサーバにリモート接続し、サーバ上に生成された仮想デスクトップ環境を利用してサーバ上でアプリケーションプログラムを実行できるようにするシステムである。

【００３０】

［プログラムおよびデータ］

識別プログラム110は、演算装置10Cによって実行され、別途起動されるプログラムからファイル名（プログラム名）、ハッシュ値、バージョン情報、ファイルサイズ、ファイルパス、ディジタル署名などの情報（以下、プログラム情報）を取得する。そして、取得したプログラム情報に基づき当該プログラムを識別する識別機能を有する。また、識別プログラム110は、取得したプログラム情報と後述する昇格基準ルール130を照会して、当該プログラムが昇格基準を満たすか否かを判定する。

【００３１】
ホワイトリスト120は、実行してもよいプログラムに関する情報をリスト化したものである。ホワイトリスト120を構成する情報には、識別プログラム110によって取得されたプログラム情報が用いられる。
【００３２】
図3によりホワイトリスト120の一例を示す。ホワイトリスト120は、各プログラムについて、プログラム名、ハッシュ値、バージョン情報、ファイルサイズ、後述する昇格権限フラグの四種類の情報を保持する。なお、図3は一例であり、ホワイトリスト120として保持する情報の種類と数は図3に限定されるものではない。
【００３３】
ホワイトリストマスタ220は、複数のホワイトリスト120をリスト化したものである。図4によりサーバ20に存在するホワイトリストマスタ220の一例を示す。ホワイトリストマスタ220は、複数のクライアントのホワイトリスト120に関連する情報をクライアントの名称や符号に対応付けて保持する。図4の例では、クライアントPC003に対応するホワイトリスト003として、複数のプログラムのプロセス名、ハッシュ値、登録日時、最終起動日時が保持された例を示す。なお、図4は一例であり、ホワイトリストマスタ220として保持する情報の種類と数は図4に限定されるものではない。
【００３４】
検知プログラム112は、演算装置10Cによって実行され、プログラムの起動と、起動されたプログラムによる別のプログラムの生成を監視する監視機能と、それらを検知する検知機能を有する。
【００３５】
登録プログラム111は、演算装置10Cによって実行され、検知プログラム112に起動や生成が検知されたプログラムの、識別プログラム110が取得したプログラム情報に基づき、当該プログラムをホワイトリスト120に登録する登録機能を有する。
【００３６】
制御プログラム113は、演算装置10Cによって実行され、クライアント10上で起動されようとするプログラムの起動を許可または禁止（阻止）する起動可否の制御機能を有する。
【００３７】
昇格基準ルール130は、プログラムやファイルが、信頼できる発行者によって発行されたものか否かを判断するためのルールである。昇格基準ルール130は、プログラム情報を元に、管理者やユーザなどが定義したルールである。ルールには、例えば、プログラムやファイルに付加されたディジタル署名、ディジタル証明書が正当か否かの検証、ファイルの署名者名が予め記憶された名前か否かの判定、ファイル名が指定条件を満たすか否かの判定などがある。
【００３８】
また、昇格基準ルール130として適用するルールの種類や数は、前記の具体例に限定されるものではない。例えば「ディジタル署名やディジタル証明書が正当であり、かつ、ファイル名に"Setup"または"Update"という文字が含まれている」という複数の組み合わせのルールを適用することもできる。この場合「画像ビューワ(Viewer.exe)の脆弱性を突いてマルウェアを生成させるマルウェア」が動作したとき、画像ビューワのディジタル署名が正当でも、そのファイル名に前記の文字列が含まれない。その結果、画像ビューワの脆弱性を突く攻撃を防ぐ効果が得られる。
【００３９】
ブラックリスト140は、起動・実行が禁止されたプログラムをリスト化したものである。ブラックリスト140のデータ構造は、図3に示すホワイトリスト120と略同一である。また、ブラックリスト140は必須ではなく、クライアント10上に存在しなくてもよいし、ブラックリスト140を使用しない場合はサーバ20のブラックリストマスタ240も必須ではない。
【００４０】

［ホワイトリスト制御処理］
●処理の概要
検知プログラム112は、グローバルフック（APIフック、フィルタドライバ）などを用いて、クライアント10におけるプログラムの起動を検知し、プログラムの起動を検知すると識別プログラム110を呼び出す。識別プログラム110は、起動されるプログラムのプログラム情報を取得して、当該プログラムが昇格基準ルール130を満たすか否かを検証する。
【００４１】
検証の結果、当該プログラムが昇格基準ルール130を満たすと判断された場合、制御プログラム113は、当該プログラムの起動を許可し、登録プログラム111を呼び出す。登録プログラム111は、識別プログラム110から当該プログラムのプログラム情報を受け取り、当該プログラムをホワイトリスト120に登録する。
【００４２】
なお、起動されるプログラムが昇格基準ルール130を満たすとしても、当該プログラムがブラックリスト140に登録されている場合、制御プログラム113は登録プログラム111に当該プログラムの登録を実行させない。つまり、当該プログラムの起動・実行の禁止が維持される。
【００４３】
次に、登録プログラム111は、ホワイトリスト120に登録したプログラムに「昇格権限」を与える。昇格権限の有無は、例えば、ホワイトリスト120の昇格権限フラグに設定する。あるいは、ホワイトリスト120に対応するテーブルを記憶装置10Bに格納し、当該テーブルの各レコードに昇格権限の有無を登録してもよい。昇格権限は、以下のように定義される権限である。
【００４４】
昇格権限を有するプログラム（親プログラム）が何らかのプログラム（子プログラム）を生成した場合、子プログラムは無条件にホワイトリスト120に登録される。そして、親プログラムが子プログラムを起動した場合、子プログラムにも昇格権限が与えられる。この昇格権限に関する登録処理を、図1に示す構成が行う場合、以下のような処理になる。
【００４５】
検知プログラム112は、親プログラムの挙動をグローバルフックなどを用いて監視する。検知プログラム112は、親プログラムによる子プログラムの生成を検知すると、識別プログラム110に子プログラムのプログラム情報を取得させる。識別プログラム110は、取得したプログラム情報を登録プログラム111に渡す。登録プログラム111は、受け取ったプログラム情報に基づきホワイトリスト120に追加するレコードのデータを作成し、作成したデータをホワイトリスト120に追加する。
【００４６】
このとき、次の方式の採用も可能である。つまり、検知プログラム112は、子プログラムの生成を検知すると、生成されたファイルを解析し、生成されたファイルに関する情報をホワイトリストへ登録する必要の有無を判断する。そして、登録不要と判断した場合、識別プログラム110によるプログラム情報の取得を行わずに以降の処理を打ち切る。登録不要と判断される場合は、例えば、生成されたファイルのバイナリヘッダを解析し、その構成がPE (Portable Executable)形式ではなく、実行ファイルではないと判断することができる場合などである。
【００４７】
次に、検知プログラム112は、親プログラムによる子プログラムの起動を監視する。検知プログラム112は、親プログラムによる子プログラムの起動を検知すると、登録プログラム111を呼び出す。呼び出された登録プログラム111は、子プログラムの昇格権限フラグに「有」を設定する。また、制御プログラム113は、子プログラムの起動を許可する。
【００４８】
昇格権限を利用すれば、例えばソフトウェアのセキュリティパッチなど、子プログラムを生成する挙動を有するプログラムが生成したプログラムを自動的にホワイトリスト120

に追加することができる。言い換えれば、生成される子プログラムをホワイトリスト120に登録する、ホワイトリストの更新にかかる作業を軽減することができる。

【００４９】

なお、昇格権限に関する処理は、親プログラムから子プログラムを生成した場合に限らず、親プログラムに対する変更（例えば、リネーム）、または、子プログラムに対する変更の場合でも可能である。

【００５０】

また、昇格基準ルール130に「プログラムに正当なディジタル署名が付加されているかを判定する」を適用する。こうすれば、信頼できる発行元が発行したプログラムであり、マルウェアのような悪意のあるプログラムではないことを操作者の意識を介さずに判断可能である。なお、正当なディジタル署名が付加されているか否かは、例えばWindows（登録商標）アプリケーションプログラミングインタフェース(API)などを用いる方法などがある。

【００５１】

また、昇格基準ルール130を満たさないプログラムと判断された場合、制御プログラム113は一般的なホワイトリスト制御を行う。つまり、識別プログラム110は、当該プログラムが昇格基準ルール130を満たさないと判断すると、当該プログラムがホワイトリスト120に登録されているか否かを判定する。制御プログラム113は、当該プログラムがホワイトリスト120に登録されていると判定されると、昇格権限を有するか否か判定し、当該プログラムの起動を許可する。また、当該プログラムがホワイトリスト120に登録されていないと判定されると当該プログラムの起動をグローバルフックなどを用いて阻止する。

【００５２】

また、識別プログラム110により、起動されるプログラムがブラックリスト140に登録されているか否かを判定する。そして、ブラックリスト140に登録されている場合は当該プログラムの起動を阻止し、ブラックリスト140に登録されていない場合は当該プログラムの起動を許可する方式の採用も可能である。

【００５３】

なお、以下の説明において、プログラムなどがホワイトリスト120またはブラックリスト140に登録されている状態を「リストに存在する」、登録されていない状態を「リストに存在しない」と表現する場合がある。

【００５４】

●処理の詳細

図5のフローチャートによりホワイトリスト制御処理の一例を説明する。

【００５５】

検知プログラム112はプログラムの起動を監視し(S201)、プログラムの起動を検知すると処理をステップS202に進める。

【００５６】

プログラムの起動が検知されると、識別プログラム110は、当該プログラムのプログラム情報を取得し(S202)、当該プログラムがブラックリスト140に存在するか否か判定する(S203)。当該プログラムがブラックリスト140に存在すると判定された場合、制御プログラム113は、当該プログラムの起動を阻止し(S204)、処理をステップS201に戻す。

【００５７】

また、当該プログラムがブラックリスト140に存在しない場合、識別プログラム110は、当該プログラムが昇格基準ルール130を満たすか否かを判定する(S205)。当該プログラムが昇格基準ルール130を満たさない場合、識別プログラム110は、当該プログラムがホワイトリスト120に存在するか否かを判定する(S206)。

【００５８】

当該プログラムがホワイトリスト120に存在すると判定された場合、識別プログラム110は、当該プログラムが昇格権限を有するか否かを判定する(S206B)。昇格権限を有すると判定された場合、制御プログラム113は当該プログラムの起動を許可する(S210)。

【００５９】
昇格権限が無いと判定された場合、制御プログラム113は当該プログラムの起動を許可し(S207)、処理をステップS201に戻す。また、当該プログラムがホワイトリスト120に存在しないと判定された場合、制御プログラム113は当該プログラムの起動を阻止し(S204)、処理をステップS201に戻す。
【００６０】
一方、当該プログラムが昇格基準ルール130を満たすと判定された場合、制御プログラム113は、当該プログラムのプログラム情報を登録プログラム111に渡す。これにより、登録プログラム111は、当該プログラム（親プログラム）をホワイトリスト120に登録し(S208)、昇格権限フラグに「有」を設定する(S209)。続いて、制御プログラム113は、親プログラムの起動を許可する(S210)。
【００６１】
次に、検知プログラム112は、昇格権限が付与された親プログラムによる子プログラムの生成を監視する(S211)。検知プログラム112は、親プログラムが子プログラムを生成した場合は処理をステップS212に進め、親プログラムが子プログラムを生成しない場合は処理をステップS201に戻す。
【００６２】
なお、ステップS211において、検知プログラム112は、子プログラムの生成だけでなく、子プログラムもしくは親プログラムに対する変更（例えば、リネーム）を監視してもよい。親プログラムの変更が検知された場合、当該プログラム（親プログラム）に対して、子プログラムと同様の処理を行う。
【００６３】
子プログラムの生成が検知されると、識別プログラム110は、子プログラムのプログラム情報を取得し(S212)、取得したプログラム情報を登録プログラム111に渡す。これにより、登録プログラム111は、子プログラムをホワイトリスト120に登録する(S213)。
【００６４】
続いて、検知プログラム112は、昇格権限が付与された親プログラムが子プログラムを起動するか否かを監視する(S214)。検知プログラム112は、親プログラムが子プログラムを起動する場合は処理をステップS215に進め、親プログラムが子プログラムを起動しない場合は処理をステップS201に戻す。
【００６５】
親プログラムによる子プログラムの起動が検知されると、識別プログラム110は、子プログラムがブラックリスト140に存在するか否かを判定する(S215)。子プログラムがブラックリスト140に存在すると判定された場合、制御プログラム113は子プログラムの起動を阻止する(S216)。そして、登録プログラム111は、ホワイトリスト120から子プログラムの登録を削除し(S217)、処理をステップS201に戻す。
【００６６】
他方、子プログラムがブラックリスト140に存在しないと判定された場合、処理はステップS209に戻る。従って、子プログラムの昇格権限フラグに「有」が設定され(S209)、子プログラムの起動が許可され(S210)、昇格権限が付与された子プログラムによる孫プログラムの生成が監視される(S211)。そして、子プログラムが孫プログラムを生成すると、孫プログラムをホワイトリスト120に登録し、昇格権限が付与された子プログラムが孫プログラムを起動すると孫プログラムに昇格権限を与える処理（S209からS215）が再帰的に繰り返される。
【００６７】
なお、ブラックリスト140が存在しない場合、識別プログラム110は、ステップS215の判定をスルーパスする。その場合、親プログラムによって起動された子プログラムや子プログラムによって起動された孫プログラムの昇格権限フラグに「有」が設定され(S209)、子プログラムの起動が許可される(S210)。
【００６８】

なお、親プログラム/子孫プログラムをホワイトリスト120に登録する際に、当該プログラムがホワイトリスト120に登録されているか否かを判定し、未登録と判定した場合に当該プログラムをホワイトリスト120に登録してもよい。また、ホワイトリスト120に既登録の場合は登録を行わずに、次の処理に進む。ホワイトリスト120に登録されているか否かを判定することにより、プログラムの重複登録を防ぐことができる。

【００６９】

以下では、第一の世代の親プログラムが元になって生成される子プログラムや孫プログラムなど、第二の世代以降のプログラムを「子孫プログラム」と呼ぶことにする。

【００７０】

●インストーラへの対応

ステップS201において、検知プログラム112は、リストとの比較により、起動されるプログラムが記憶装置10Bに予め格納されているインストーラプログラム（例えばWindows（登録商標）におけるmsiexec.exe）か否かを判定する。そして、インストーラプログラム（以下、インストーラ）の起動と判定された場合、インストーラの動作が他のプログラムの動作と異なるため、ステップS202以降の処理を切り替える。

【００７１】

操作者がインストーラパッケージファイル（msiファイル、mspファイル、msuファイルなど）の実行を指示するとインストーラが起動され、インストーラは、インストーラパッケージファイル（以下、パッケージ）に格納されたファイルを展開する。従って、昇格基準ルール130に基づく判定は、インストーラではなく、パッケージに対して行う必要があり、図5に示す処理を直接適用することができない。

【００７２】

図6のフローチャートによりインストーラが起動された場合のホワイトリスト制御処理の一例を説明する。

【００７３】

識別プログラム110は、パッケージのファイル情報を取得し(S221)、パッケージがブラックリスト140に存在するか否かを判定する(S222)。当該パッケージがブラックリスト140に存在すると判定された場合、制御プログラム113は、インストーラの起動を阻止し(S223)、処理をステップS201に戻す。なお、ブラックリスト140が存在しない場合、識別プログラム110は、ステップS222の判定をスルーパスする。

【００７４】

また、当該パッケージがブラックリスト140に存在しない場合、識別プログラム110は、当該パッケージが昇格基準ルール130を満たすか否かを判定する(S224)。当該パッケージが昇格基準ルール130を満たさない場合、識別プログラム110は、当該パッケージがホワイトリスト120に存在するか否かを判定する(S225)。当該パッケージがホワイトリスト120に存在すると判定された場合、制御プログラム113は、インストーラの昇格権限フラグを「有」に設定し(S209)、インストーラの起動を許可する(S210)。また、当該パッケージがホワイトリスト120に存在しないと判定された場合はインストーラの起動を阻止し(S223)、処理をステップS201に戻す。

【００７５】

一方、当該パッケージが昇格基準ルール130を満たす場合の処理は図5に示すステップS209からS217と同様であり、インストーラの昇格権限フラグに「有」が設定され(S209)、インストーラの起動が許可される(S210)。そして、インストーラによってパッケージから取り出されたプログラムは、親プログラム（この場合はインストーラ）によって生成された子プログラムと同等に扱われる。つまり、パッケージから取り出されたプログラムは子孫プログラムとしてホワイトリスト120に登録され、子孫プログラムが次の世代のプログラムを起動すると、起動されるプログラムに昇格権限を与える処理（S209からS215）が再帰的に繰り返される。

【００７６】

なお、ステップS211において、親プログラムによる子プログラムの生成ではなく、当該

プログラム（親プログラム）によるインストーラパッケージが生成された場合は、そのパッケージファイルに対して、図6の処理を適用することも可能である。

【００７７】

［親プログラムが生成した子プログラム以外に昇格権限を継承/付与する場合］

昇格権限を持った親プログラムから生成された子プログラムが親プログラムによって起動された場合、昇格権限を継承するが、以下のような場合も昇格権限を継承または付与してもよい。

【００７８】

●パターン1

図5において、同一の親プログラムから複数の子孫プログラムが生成される場合を考える。このとき、子孫プログラムの中で親プログラムから昇格権限を継承したものがあり、昇格権限を継承した子孫プログラムが、他の子孫プログラムを起動した場合、昇格権限を継承してもよいものとする。

【００７９】

例えば、Windows（登録商標）のアップデート動作の中には上記のような動作がある。パターン1の手法を実施することで、Windows（登録商標）のアップデートをブロックすることなく行うことが可能になる。

【００８０】

パターン1を実施する場合、図5に示すステップS214において「親プログラム、または、同じ親プログラムから生成され、当該親プログラムから昇格権限を継承したプログラムによって、子孫プログラムが起動されるか？」という判定が行われる。

【００８１】

●パターン2

図6において、インストーラが他のプログラムから起動される場合を考える。このとき、昇格権限をもつプログラムがインストーラを起動した場合、インストーラが昇格権限を継承してもよいものとする。

【００８２】

市販のソフトウェアには、インストール時にインストーラを起動するものがある。パターン2の手法を実施することで、そのようなソフトウェアのインストールをブロックすることなく行うことが可能になる。

【００８３】

●パターン3

図5において、昇格権限をもつプログラムから生成された子プログラムを、昇格権限をもたないプログラムが起動する場合を考える。このとき「生成プログラム群」と「起動プログラム群」という二種類のプログラム群を予め定義する。そして、生成プログラム群に属すプログラムから生成され、かつ、起動プログラム群に属すプログラムから起動されたプログラムには昇格権限を付与する処理を行ってもよいものとする。

【００８４】

市販のソフトウェアには、インストール時に上記のような動作を行うものがある。パターン3の手法を実施することで、そのようなソフトウェアのインストールをブロックすることなく行うことが可能になる。

【００８５】

［ホワイトリストの作成］

ホワイトリスト制御システムの運用には、運用環境に適したホワイトリスト120を作成する必要がある。

【００８６】

●プログラム起動をトリガとする処理

図5、図6においては、プログラムやパッケージが昇格基準ルール130を満たさず、かつ、ホワイトリスト120に存在しない場合（S206やS225のNO）、制御プログラム113はプログラムの起動を阻止する（S204やS223）と説明した。しかし、そのようなプログラムやパッ

ケージ（以下、未登録プログラム）が検出された場合、ホワイトリスト120の更新を試みることが可能である。

【００８７】

図7のフローチャートによりプログラム起動をトリガとするホワイトリスト120の更新処理を説明する。

【００８８】

登録プログラム111は、未登録プログラムが検出されると(S301)、識別プログラム110から渡された未登録プログラムのプログラム情報（以下、未登録情報）をサーバ20に送信する(S302)。そして、処理をステップS301に戻す。

【００８９】

なお、未登録プログラムの検出直後に未登録情報を送信せずに、所定のサイクルで未登録情報をサーバ20に送信するようにしてもよい。例えば、登録プログラム111は、未登録情報を例えば記憶装置10Bやメモリ10Eの所定領域に一時保存する。そして、所定のサイクルで（例えば五分ごとや一時間ごとに）保存された未登録情報があるか否かを判定し、未登録情報が保存されている場合は当該情報をサーバ20に送信する。

【００９０】

サーバ20の管理コンソール210は、クライアント10から未登録情報を受信すると(S311)、受信した未登録情報に一致する情報がホワイトリスト候補250に存在するか否かを判定する(S312)。受信した未登録情報に一致する情報がホワイトリスト候補250に存在する場合は処理をステップS311に戻す。

【００９１】

一方、受信した未登録情報に一致する情報がホワイトリスト候補250に存在しない場合、管理コンソール210は、受信した未登録情報をホワイトリスト候補250へ追加する(S313)。そして、例えば電子メールやアラートウィンドウなどにより、ホワイトリスト候補250に追加した未登録情報をサーバ20の操作者に提示する(S314)。

【００９２】

操作者は、提示された情報を参照して、未登録プログラムをホワイトリストに登録するか否かを判断し、判断結果に応じた指示を管理コンソール210に入力する。管理コンソール210は、操作者の指示が当該プログラムの登録を示すか否かを判定する(S315)。操作者の指示が登録を示す場合は、当該プログラムをホワイトリストマスタ220に登録し(S316)、ホワイトリスト候補250の当該プログラムのレコードに「登録済」を記録する(S317)。また、操作者の指示が非登録を示す場合は、当該プログラムをホワイトリストマスタ220に登録せずに、ホワイトリスト候補250の当該プログラムのレコードに「非登録」を記録する(S318)。そして、処理をステップS311に戻す。

【００９３】

管理コンソール210は、定期的（例えば、一時間置きや一日置き）にホワイトリストマスタ220のデータをクライアント10へ送信する。これにより、クライアント10のホワイトリスト120が更新される。

【００９４】

●プログラム検索をトリガとする処理

上記では、プログラム起動をトリガとしてホワイトリスト候補250にプログラムを追加する処理を説明した。しかし、例えばOS標準のファイル検索ツールなどを用いてプログラムを検索し、検出したプログラムをホワイトリスト候補250の登録することもできる。このようにすれば、クライアント10の記憶装置10Bに格納されたすべてのプログラムをホワイトリスト候補250に追加することができる。

【００９５】

図8のフローチャートによりプログラム検索をトリガとするホワイトリストの更新処理を説明する。

【００９６】

クライアント10の操作者（またはサーバ20）の指示により、ファイル検索ツール114が

起動され、指示された検索条件に基づきファイル検索が実行される(S401)。ホワイトリスト候補250にプログラムを追加する場合、記憶装置10Bに格納されたすべてのプログラムが検索され、識別プログラム110は検索結果を受け取る(S402)。

【００９７】

検索結果を受け取った識別プログラム110は、検出されたプログラムのプログラム情報を取得する(S403)。そして、検出されたプログラムから、プログラムが昇格基準ルール130を満たさず、かつ、ホワイトリスト120に存在しない未登録プログラムを抽出する(S404)。登録プログラム111は、未登録プログラムが抽出されると(S405)、未登録プログラムのプログラム情報をサーバ20に送信する(S406)。

【００９８】

管理コンソール210の処理は、プログラム起動をトリガとする場合の処理（図7のS311からS318）と同様であり、詳細説明を省略する。

【００９９】

上記では、ホワイトリスト120に登録されていないプログラムをホワイトリスト120に登録する例を説明したが、ホワイトリスト120に登録されていないパッケージをホワイトリスト120に登録する場合も同様の処理になる。

【０１００】

また、図2に示すサーバ20が存在しない構成の場合、図7に示す管理コンソール210の処理（S311からS318）もクライアント10上で実行されることは言うまでもない。

【０１０１】

［変形例］

上記では、クライアント10の例としてPC、タブレット端末、スマートフォンを例に挙げた。しかし、ポインティングデバイスを持たない端末（例えばネットワークスキャナ）や、ディスプレイを持たない端末（例えば組込端末）などをクライアントとして、上記処理を適用することができる。

【０１０２】

このように、ホワイトリスト型の制御方式を用いる場合の、ホワイトリストの更新にかかる作業を軽減することができる。従って、システム管理者などの、実行ファイルを抽出しホワイトリストを更新する負担が軽減される。さらに、昇格規準ルール130を用いた判断により、アップデータが信頼できるか否かの判断作業も軽減される。

【０１０３】

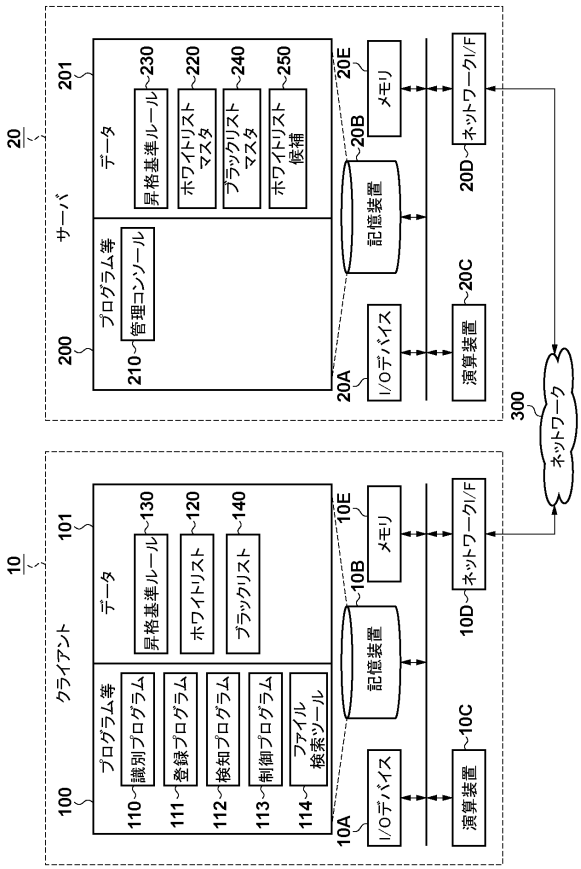
また、上記では、ホワイトリストを用いたホワイトリスト制御システムについて説明したが、ホワイトリストに限定されず、ブラックリストを用いたブラックリスト制御システムにも上記処理を適用することができる。

【０１０４】

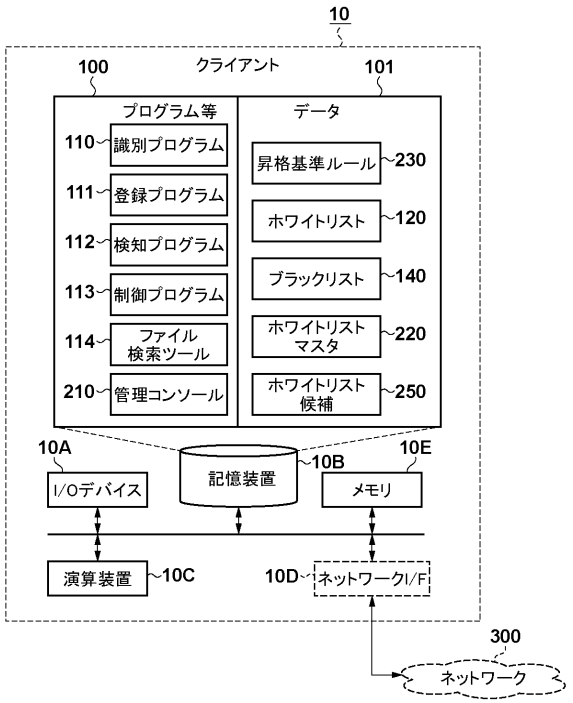
［その他の実施例］

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記録媒体を介してシステム或いは装置に供給し、そのシステムあるいは装置のコンピュータ（又はCPUやMPU等）がプログラムを読み出して実行する処理である。

【図１】



【図２】



【図３】

120

プログラム名	ハッシュ値	バージョン	ファイルサイズ	昇格権限
lexplore.exe	72AE6B5FDA794D2	1.0.0.1	56.3KB	無
svchost.exe	1A8C6D902A1200B	2.1	1.43MB	無
dwn.exe	A8C6D902A120089	10.7.1	321.8KB	有
xcel.exe	F41B4C736164DD0	4.0	214KB	無
inword.exe	5BC866A3F1C29B8	1.10.2	2.1MB	無
…	…	…	…	…

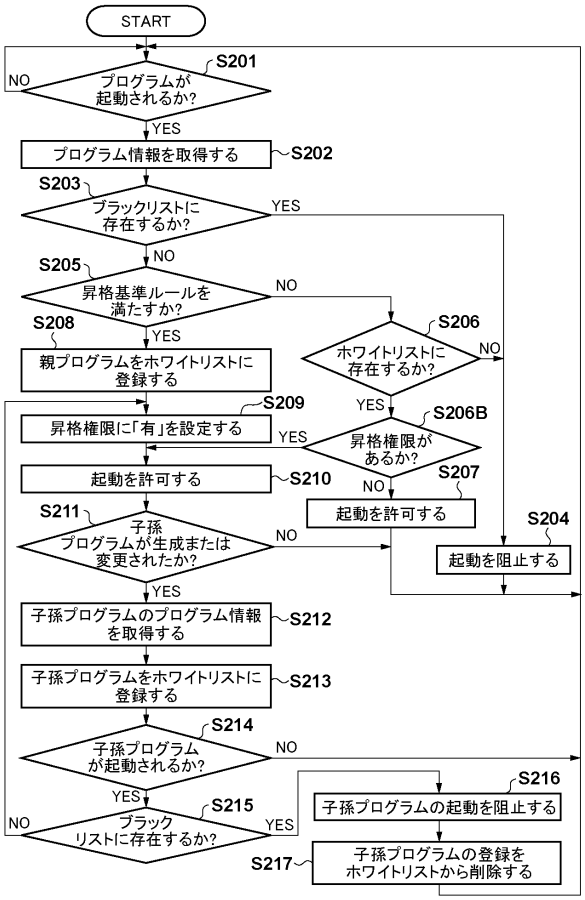
【図４】

プロセス名	ハッシュ値	登録日時	最終起動日時
lexplore.exe	72AE685FDA794D2	2012/3/4 10:00	2012/3/4 11:00
svchost.exe	1A8C6D902A1200B	2012/3/5 03:00	2012/3/5 10:00
dwn.exe	A8C6D902A120089	2012/3/13 10:00	2012/3/14 10:00
xcel.exe	F41B4C736164DD0	2012/3/21 11:00	2012/3/26 10:00
inword.exe	58C866A3F1C2988	2012/3/24 20:00	2012/4/1 10:00

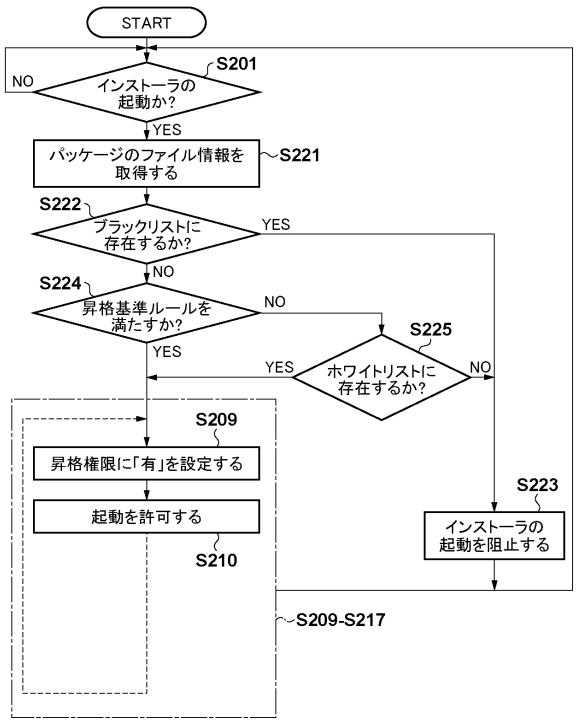
220

PC001	ホワイトリスト001
PC002	ホワイトリスト002
PC003	ホワイトリスト003
…	…

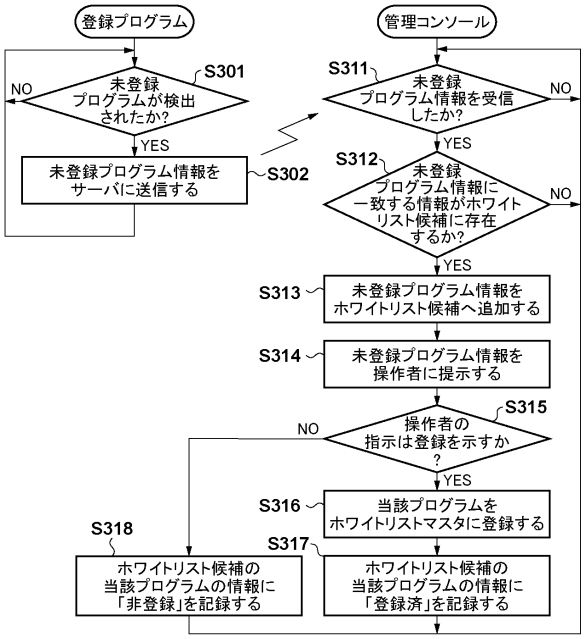
【図５】


START
S201
プログラムが起動されるか?
NO
YES
プログラム情報を取得する
S202
S203
ブラックリストに存在するか?
YES
NO
S205
昇格基準ルールを満たすか?
NO
YES
S208
親プログラムをホワイトリストに登録する
S206
ホワイトリストに存在するか?
NO
YES
S209
昇格権限に「有」を設定する
S206B
昇格権限があるか?
YES
起動を許可する
S210
NO
S207
起動を許可する
S211
子孫プログラムが生成または変更されたか?
NO
S204
起動を阻止する
YES
子孫プログラムのプログラム情報を取得する
S212
子孫プログラムをホワイトリストに登録する
S213
S214
子孫プログラムが起動されるか?
NO
YES
S216
子孫プログラムの起動を阻止する
S215
ブラックリストに存在するか?
NO
YES
S217
子孫プログラムの登録をホワイトリストから削除する

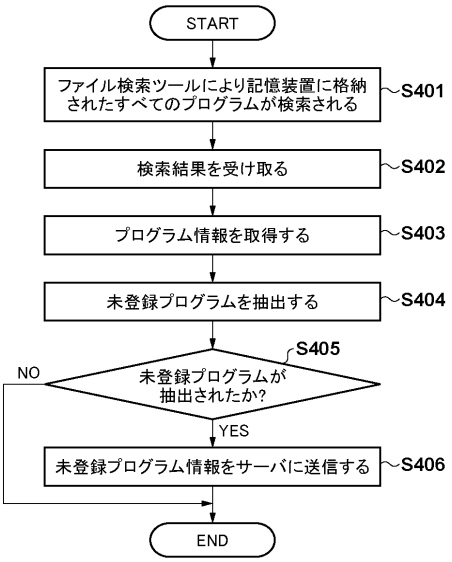
【図６】


START
S201
インストーラの起動か?
NO
YES
パッケージのファイル情報を取得する
S221
S222
ブラックリストに存在するか?
YES
NO
S224
昇格基準ルールを満たすか?
NO
YES
S225
ホワイトリストに存在するか?
YES
NO
S209
昇格権限に「有」を設定する
起動を許可する
S210
S223
インストーラの起動を阻止する
S209-S217

【図７】


登録プログラム
管理コンソール
S301
未登録プログラムが検出されたか?
NO
YES
未登録プログラム情報をサーバに送信する
S302
S311
未登録プログラム情報を受信したか?
NO
YES
S312
未登録プログラム情報に一致する情報がホワイトリスト候補に存在するか?
NO
YES
S313
未登録プログラム情報をホワイトリスト候補へ追加する
S314
未登録プログラム情報を操作者に提示する
S315
操作者の指示は登録を示すか?
NO
YES
S316
当該プログラムをホワイトリストマスタに登録する
S317
ホワイトリスト候補の当該プログラムの情報に「登録済」を記録する
S318
ホワイトリスト候補の当該プログラムの情報に「非登録」を記録する

【図８】


START
ファイル検索ツールにより記憶装置に格納されたすべてのプログラムが検索される
S401
検索結果を受け取る
S402
プログラム情報を取得する
S403
未登録プログラムを抽出する
S404
S405
未登録プログラムが抽出されたか?
NO
YES
未登録プログラム情報をサーバに送信する
S406
END

フロントページの続き

(72)発明者　高野　和希
埼玉県秩父市下影森１２４８番地　キヤノン電子株式会社内
(72)発明者　米川　智
埼玉県秩父市下影森１２４８番地　キヤノン電子株式会社内

審査官　大塚　俊範

(56)参考文献　特開２０１２－１８５７４５（ＪＰ，Ａ）
特開２０１０－２３８１６８（ＪＰ，Ａ）
国際公開第２０１２／０４６４０６（WO，Ａ１）
特開２００７－３１６７８０（ＪＰ，Ａ）
植松 建至，構造計算書不正検知システムの提案，情報処理学会論文誌　論文誌ジャーナル［ＣＤ－ＲＯＭ］，日本，社団法人情報処理学会，２００８年　９月１５日，第49巻，第9号，第3199-3208頁，ISSN:1882-7837

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　９／４４５
Ｇ０６Ｆ　１１／００