明　細　書

発明の名称 ： 不正アプリケーション検知システム及び、方法

技術分野

[0001] 本発明は、端末装置にインストールしたアプリケーションの不正動作性を検知するシステム及び方法に関し、不正検知サーバ装置と組み合わせた検知技術に係る。

背景技術

[0002] 近年、スマートフォンに代表される携帯型端末装置の高性能化が進み、パソコンと同様に様々なアプリケーションがインストールされるようになっている。一方で、携帯型端末装置で動作するアプリケーションが不正な動作を行うコンピュータウイルスや、マルウェアの存在が問題となっており、不正動作を行うアプリケーションの検知が重要な課題である。

[0003] パソコン等で動作するコンピュータウイルスの検知ソフトウェアにおいては、ウイルス検出ソフトをコンピュータ上で動作させて、不正なアプリケーションがインストールされていないか、不審な挙動が認められないかを検出する方法が一般的である。

しかし、携帯型の端末装置では、ハードウェア資源に限りがあるため、パソコン等とは異なる手法が提案されてきた。

[0004] 例えば、特許文献１には、ダウンロード前にユーザ携帯電話からコンテンツサーバに接続し、コンテンツサーバからウイルスチェックサーバにコンテンツを送ってウイルスチェックを行う技術が開示されている。

[0005] 特許文献２には、監視装置によりネットワークに接続された端末装置のソフトウェアの状態を監視するシステムが開示されている。本システムの監視装置は、脆弱性の原因となるファイルやマルウェア感染時に生成されるファイルの特徴情報などを含んで定義されたソフトウェアの特徴情報を格納する第1DBを有し、また、端末装置は自ら有するファイルの特徴情報を逐次取得して保持する第2DBを有する。監視装置は、ネットワークを介して検証要求と共

に、上記第 1DBに格納された特徴情報を端末装置へ送信する。端末装置では、第2DBを検索して上記特徴情報に関連するファイルの有無を検証し、検証結果を監視装置へ送信する。監視装置では受信した検証結果に基づいて、端末装置の脆弱性又はマルウェア感染状況を判断し、アクセス制御を実施し、被害の拡大を防止する。

[0006] 特許文献３の技術は、メールサーバからクライアント端末に送信されたメールと同一のメールを保存するメール保存部を設けて、ウイルス定義ファイルが最新化された後に、メール保存部に保存されているメールに潜んでいるウイルスを検知する技術を開示している。

[0007] 特許文献４には、一度ウイルスチェックを実施したファイルに対して、その時に使用したウイルスチェック手段およびウイルス定義ファイルの情報を添付し、次回のウイルスチェック時に同じウイルスチェック手段およびウイルス定義ファイルを使用しているか否か判断して、ウイルスチェックの実行が必要か否かを決定する技術が開示されている。

先行技術文献

特許文献

[0008] 特許文献1：特開２００２－１９７００６号公報

特許文献2：特開２００６－４０１９６号公報

特許文献3：特開２００７－０１８１８２号公報

特許文献4：特開２００７－２００１０２号公報

発明の概要

発明が解決しようとする課題

[0009] 上記特許文献１に記載の技術では、ダウンロード時にウイルスチェックサーバでウイルスチェックを行うため、ダウンロードまでに時間がかかる問題と、チェック時に発見されないウイルスから携帯電話を保護することができない問題がある。

[0010] 特許文献２に記載の技術では、監視装置から強力に端末装置を監視出来る

反面、監視装置から送った特徴情報に一致するかどうかを端末装置側で検索する構成のため、極めて多数のアプリケーションが流通する現在の状況では、すべての特徴情報を端末装置に送ることは現実的でない。

[0011] 特許文献３の技術は、常に最新のウイルス定義ファイルでウイルスチェックを行うことができる点で優れているが、大容量のメールや、アプリケーションをすべて保存しておくことは大容量の記憶領域を必要とし、効率的な方法とは言えない。

[0012] 特許文献４の技術は、非力なコンピュータ上で高速にウイルスチェックを行える点で優位性を有するが、不特定のユーザが使用する端末装置を対象にするための技術や、端末装置上から削除した後にも、アプリケーションの不正動作性を検知するための技術を提供していない。

[0013] 本発明は上記従来技術の有する問題点に鑑み、端末装置上でのアプリケーションの不正動作性を低負荷で検知すると共に、検知精度を高める技術を提供することを目的とする。特に、端末装置上で削除されたアプリケーションについても検知することのできる技術を提供する。

課題を解決するための手段

[0014] 本発明は上記課題を解決するため、本発明は、ユーザが適宜アプリケーションをインストール可能な端末装置と、端末装置にインストールされたアプリケーションの不正動作性を検知する不正検知サーバ装置とから構成される不正アプリケーション検知システムを提供する。

端末装置には、アプリケーションのインストール状態が変化したことを検出するインストール状態検出処理部と、インストール状態が変化した時に、インストールされたアプリケーション情報を、不正検知サーバ装置に通知するインストール通知処理部と、当該アプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を計算する特徴値計算処理部と、アプリケーション情報とその特徴値を、不正検知サーバ装置に通知する特徴値送信処理部と、不正検知サーバ装置から少なくとも当該アプリケーションの不正動作性が検知された場合に不正検知

情報を受信する不正検知情報受信処理部と、不正検知情報の受信時に、端末装置上で所定の対応処理を行う不正時対応処理部とを備える。

[0015] 一方、不正検知サーバ装置には、端末装置のインストール通知処理部からインストールされたアプリケーション情報を受信するインストール通知受信処理部と、端末装置の特徴値送信処理部から特徴値を受信する特徴値受信処理部と、登録したアプリケーションの不正動作性を装置内で検出、又は外部から取得して検知する不正検知処理部と、特徴値と不正動作性の情報とを関連付けてアプリケーションデータベースに登録する不正検知結果記録処理部と、少なくとも当該アプリケーションの不正動作性が検知された場合に不正検知情報を端末装置に送信する不正検知情報送信処理部とを備える。

[0016] 上記の不正検知サーバ装置において、通知されたアプリケーション情報についてアプリケーションデータベースに登録済みか否かを検索するアプリケーション情報検索処理部と、端末装置に向けて、登録済みか否かの検索結果を通知する登録状態通知処理部とを備え、端末装置の特徴値送信処理部が、不正検知サーバ装置において当該アプリケーション情報が登録済みか否かに応じ、アプリケーション情報とその特徴値を、不正検知サーバ装置に通知する構成でもよい。

[0017] 上記の不正検知サーバ装置において、不正検知結果記録部が、端末装置からのインストール通知を契機として、端末装置毎にアプリケーションのインストール状態を上記のアプリケーションデータベースに記録し、不正検知処理部において当該アプリケーションの不正動作性が検知されたときに、すでに端末装置上から当該アプリケーションが削除された後であっても、不正検知情報送信処理部が不正検知情報を送信する構成でもよい。

[0018] 上記のアプリケーションデータベースが、端末毎のインストール状態を記録した端末毎アプリデータベースと、上記の特徴値と上記の不正動作性の情報とを関連づけて記録した不正動作性データベースとに分割して構成してもよい。

[0019] 上記の不正検知サーバ装置に、入力された任意のアプリケーションファイ

ル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を計算する特徴値計算処理部を備えると共に、不正検知処理部において当該アプリケーションの不正動作性を検知し、不正検知結果記録部が、特徴値と不正動作性の情報とを関連付けてアプリケーションデータベースに登録することもできる。

[0020] 本発明は、上記不正アプリケーション検知システムで用いられる端末装置のみで提供することもできる。また、不正検知サーバ装置のみで提供することもできる。

[0021] また、本発明は、ユーザが適宜アプリケーションをインストール可能な端末装置と、端末装置にインストールされたアプリケーションの不正動作性を検知する不正検知サーバ装置とを用いて端末装置にインストールされた不正アプリケーションを検知する方法を提供することもできる。本方法は次のステップからなる。

・端末装置におけるアプリケーションのインストール状態が変化したことを検出するインストール状態検出ステップ

・インストール状態が変化した時に、インストールされたアプリケーション情報を、不正検知サーバ装置に通知するインストール通知ステップ

・アプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を不正検知サーバ装置に通知する特徴値送信ステップ

・特徴値と、当該アプリケーションの不正動作性とを関連付けてアプリケーションデータベースに登録する不正検知結果記録ステップ

・少なくとも当該アプリケーションの不正動作性が検知された場合に不正検知情報を端末装置に送信する不正検知情報送信ステップ

・不正検知情報の受信時に、端末装置上で所定の対応処理を行う不正時対応処理ステップ

を有することを特徴とする。

[0022] 前記インストール通知ステップに続いて、

・不正検知サーバ装置において、端末装置から通知されたアプリケーション情報についてアプリケーションデータベースに登録済みか否かを検索するアプリケーション情報検索ステップ

・端末装置に向けて、登録済みか否かの検索結果を通知する登録状態通知ステップ

をさらに有し、特徴値送信ステップでは登録されていなかったアプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を該不正検知サーバ装置に通知するようにしてもよい。

[0023] 上記の不正検知サーバ装置において、端末装置からのインストール通知を契機として、端末装置毎にアプリケーションのインストール状態を上記のアプリケーションデータベースに記録し、当該アプリケーションの不正動作性が検知されたときに、すでに端末装置上から当該アプリケーションが削除された後であっても、端末装置に不正検知情報を送信する構成でもよい。

[0024] 上記の不正検知サーバ装置において、入力された任意のアプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を計算すると共に、当該アプリケーションの不正動作性を検知し、特徴値と不正動作性の情報とを関連付けてアプリケーションデータベースに登録する構成でもよい。

発明の効果

[0025] 本発明は以上の構成をとることによって次のような効果を奏する。

すなわち、端末装置ではアプリケーションのインストール状態が変化した時だけ、特徴値の計算などの簡易な処理を行えば足りるので、端末装置における負荷を最小限にすることができる。特に、端末装置において重要な省電力化にも寄与する。

アプリケーションの不正動作性の検知は不正検知サーバ装置で集中的に行うので、常に最新のシグネチャファイルを用いることができるほか、処理能力の高いサーバ装置で不正検知を行うことで、検知精度の向上、高速な検知

を実現できる。

[0026] 端末装置におけるアプリケーションのインストール状態を不正検知サーバ装置に記録しておくことで、最新のシグネチャファイルでそのアプリケーションの不正動作性が確認された時には、仮にアプリケーションが削除された後であっても端末装置に通知し、必要な対策を行うことができる。

図面の簡単な説明

[0027] [図1]本発明における不正アプリケーション検知システムの全体図である。

[図2]本発明の不正アプリケーション検知方法のフローチャートである。

[図3]アプリケーションが未登録の場合のシーケンス図である。

[図4]アプリケーションが登録済みの場合のシーケンス図である。

[図5]アプリケーションを端末側で削除した時のシーケンス図である。

[図6]検知結果が更新された時にシーケンス図である。

発明を実施するための形態

[0028] 以下、本発明の実施形態を図面を用いて説明する。本発明は以下の実施例に限定されず請求項記載の範囲で適宜実施することができる。

図１は、本発明における不正アプリケーション検知システムの全体図である。本システムは、ユーザが適宜アプリケーションをインストール可能な端末装置（以下、端末と呼ぶ）（１）と、各端末装置にインストールされたアプリケーションの不正動作性を検知する不正検知サーバ装置（以下、サーバと呼ぶ）（２）から構成される。

端末（１）とサーバ（２）はインターネットやＬＡＮ、携帯電話網などのネットワーク（３）で接続される。

[0029] 端末（１）は公知のスマートフォン、携帯電話、タブレットＰＣなど携帯型端末装置を主に想定しているが、パソコン等でもよい。これらの機器には周知のようにネットワークとの接続手段、ＣＰＵ、メモリ、液晶画面などの表示手段、キーボード・タッチパネルなどの入力手段などが備えられている。

またサーバ（２）も、一般的なパソコン、サーバ機器によって構成するの

が簡便であり、これらも同様にＣＰＵ、メモリ、ハードディスク等の外部記憶手段、表示手段、入力手段が備えられている。

[0030] 端末（１）ではＣＰＵとメモリの協働により、次の処理手段が設けられる。

まず、インストール状態検出部（１０）は、端末（１）上でアプリケーションのインストール状態が変化したことを検出し、インストール通知部（１１）は、インストール状態が変化した時に、ネットワーク（３）を通じてインストールされたアプリケーション情報を、サーバ（２）側に通知する。

[0031] 特徴値計算処理部（１２）では、インストールされたアプリケーションファイル、又はそのアプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を計算する。本実施例では特徴値としてハッシュ値などを用いることができる。

計算された特徴値は、特徴値送信部（１３）からネットワーク（３）を通じてサーバ（２）側に通知する。

[0032] さらに、サーバ（２）でアプリケーションの不正動作性が検知された場合に不正検知情報を受信する不正検知情報受信部（１４）と、その不正検知情報の受信時に、端末装置上で所定の対応処理を行う不正時対応部（１５）と備えている。

[0033] 一方、サーバ（２）にはＣＰＵとメモリの協働により、次の処理手段が設けられる。

すなわち、インストール通知受信部（２０）では、端末のインストール通知部（１１）からインストールされたアプリケーション情報を受信する。アプリケーション情報検索部（２１）は、通知された該アプリケーション情報についてアプリケーションデータベースに登録済みか否かを検索する。登録状態通知部（２２）から端末（１）に向けて、登録済みか否かの検索結果を通知する。

[0034] 特徴値受信部（２３）は、端末（１）の特徴値送信部（１３）から特徴値を受信する。さらに、登録したアプリケーションの不正動作性を装置内で検

出、又は外部から取得して検知する不正検知部（２４）と、特徴値と不正動作性の情報とを関連付けてアプリケーションデータベース（２８）に登録する不正検知結果記録部（２５）と、不正検知情報を端末（１）に送信する不正検知情報送信部（２６）と備える。

さらに、別実施例としてサーバ（２）に特徴値計算部（２７）を備えてもよい。

[0035] 図２は本発明の不正アプリケーション検知方法のフローチャートである。このフローチャートを用いて本発明の具体的な実施例を説明する。

不正アプリケーションの検知は、まず端末（１）側でアプリケーションのインストール状態を検出したことを契機に動作が開始する。（インストール状態検出ステップ：Ｓ１）

[0036] インストール状態とは、アプリケーションのインストール、削除、バージョンの更新、試用版から正規版への変更など、端末におけるアプリケーションの様々な状態を指す。インストール状態検出部（１０）の処理は、常時バックグラウンドで動作させてもよいが、処理負荷を軽減するために、インストール状態の変更時に発生するイベントを契機としてインストール状態を検出することが望ましい。

[0037] アプリケーションがインストールされた場合など、インストール状態が検出されると、インストール通知部（１１）からインストール通知受信部（２０）に対してインストール通知（Ｓ２）が行われる。

[0038] 本発明は、サーバ（２）側でアプリケーション情報が登録されているか否かに関わらず特徴値を送信してもよいが、端末装置における処理、通信量の軽減を図るために、サーバ（２）におけるアプリケーション情報の登録状態を事前に検索することが好ましい。

そのため、サーバ（２）上では、アプリケーション情報検索部（２１）が、通知されたアプリケーションに係る情報が登録済みか否か、アプリケーションデータベース（２８）を検索する。（アプリケーション情報検索ステップ：Ｓ３）

そして、登録状態通知部（２２）から、端末（１）に向けて登録状態を通知（Ｓ４）する。端末（１）側では、登録状態に応じて処理が異なる。

[0039] すなわち、サーバ（２）上で登録されているか（Ｓ５）に応じて、登録されていないアプリケーションに関しては、予め特徴値計算部（１２）で計算した特徴値をサーバに送信（Ｓ６）し、登録済みのアプリケーションに関しては送信しない。

このように未登録の特徴値があったときだけ特徴値送信部（１３）から特徴値受信部（２３）に特徴値を送信することにより、処理の高速化、通信量の軽減に寄与する。

[0040] 特徴値が送られたアプリケーションについてはアプリケーション情報と共に、アプリケーションデータベース（２８）に記録される。

このとき、不正検知部（２４）によって不正動作性に関する情報が得られた場合には、不正検知結果記録部（２５）が特徴値と共にアプリケーションデータベース（２８）に記録する。（不正検知結果記録ステップ：Ｓ８）

[0041] ここで不正検知部（２４）は公知のウイルス、マルウェア等の検出方法を任意に利用することができ、不正検知方法に関する説明は省略する。不正検知部（２４）自体がアプリケーションの不正動作性を検知してもよいし、別に設けられた不正なアプリケーションの情報データベースから情報を取得する構成でもよい。

不正検知部（２４）による検知は、一定の周期で行ってもよいし、新しいアプリケーションが登録される毎に行ってもよく、そのたびに最新のシグネチャファイルに更新する。

[0042] 上記不正動作性に関する情報は、不正動作性が認められた場合に限らず、不正が認められない情報を含んでもよい。また、十分に確認できない場合に、不完全情報として記録してもよい。

さらに、不正検知部（２４）による検知がすぐに行われない場合には、特徴値を受信した直後はとりあえず不正動作性未検知として登録し、後に検知が行われた時にアプリケーションデータベース（２８）を更新する構成でも

よい。

[0043] 不正検知結果に基づき、不正検知情報送信部（２６）は不正検知情報受信部（１４）に向けて当該アプリケーションに不正動作性が認められるかどうかを送信する。不正動作性が認められた場合のみ送信してもよいし、不正動作性の有無を送信してもよい。（不正検知情報送信ステップ：Ｓ９）

[0044] 不正検知情報受信部（１４）がアプリケーションの不正動作性を受信した場合、不正時対応部（１５）が不正時対応処理（Ｓ１０）を行う。

不正時対応処理としては、ユーザに当該アプリケーションの削除を促す画面表示や、自動的な削除処理などが挙げられる。

また、不正動作性が認められなかった場合にも、アプリケーションが安全である旨の表示を行うなどの対応処理を行っても良い。

[0045] 本発明の構成は以上の通りであるが、さらに詳細な処理方法をシーケンス図を用いて説明する。本実施例では端末装置としてAndroid（登録商標）を使用したスマートフォン等の端末を用い、アプリケーションのパッケージ構造も同OSに従った例として説明する。

図３はサーバ（２）においてアプリケーションが未登録の場合のシーケンス図である。

[0046] ユーザ（３０）がアプリをインストール（Ｓ３０）すると、端末（１）はapk（Androidアプリケーションパッケージ）の情報がアプリケーションデータベース（２８）に存在するかを問い合わせる。アプリケーションが未登録の場合、Noを返す。これは本発明のインストール通知ステップ（Ｓ２）から登録状態通知ステップ（Ｓ４）に該当する。

[0047] apk情報が登録されていないので、特徴値送信部（１３）は、apk情報をサーバ（２）に送信する。ここでapk情報としては、apkに含まれるファイルのハッシュ値、例えばハッシュ関数としてSHA1を用いたハッシュ値を用いることができる。その他、ファイル名や、バージョンなどを含めることもできる。

ハッシュ関数を用いた特徴値の計算方法は公知であり、特徴値計算部（１

２）により送信前のいずれかのタイミングで適宜行われる。

[0048] 本実施例では、apk情報のアップロード（Ｓ３１）と共に、apkに含まれる部品要素（dnaと表記）に関する特徴値を送信（Ｓ３２）する。dnaはapk内に複数含まれているため、検査対象とするdnaの数だけ送信は繰り返される。dnaに係る特徴値としては、dnaの名前(name)、種類(dna_type)、ハッシュ値(filehash)、ハッシュの種類(hash_type)を送信する。

検査対象としては、不正動作性に影響の強いdnaを予め定義しておき、必要最小限なdnaだけを検査することが端末装置の負荷の軽減の観点から好ましい。

本処理は、本発明の特徴値送信ステップ（Ｓ６）及び不正検知結果記録ステップ（ｓ７）に該当する。

[0049] 次に、端末インストール情報の追加（Ｓ３３）処理を行う。すなわち、端末の識別番号（device id）とapkのハッシュ値をアプリケーションデータベース（２８）に登録する。本処理はこの時点で行っても良いし、上記インストール通知ステップ（Ｓ２）と同時に行ってもよい。

[0050] 本発明ではアプリケーションデータベース（２８）に端末毎のアプリケーションのインストール状態を格納することを１つの特徴としている。これにより、サーバ（２）側で各端末（１）のアプリケーションのインストール履歴を管理し、後から不正動作性が確認された場合に、その履歴に従って、端末に必要な情報提供を行うことができる。この点については後述する。

[0051] また、本実施例ではアプリケーションデータベースを１つのデータベースとして説明しているが、端末毎のインストール状態を記録した端末毎アプリデータベースと、特徴値と不正動作性の情報とを関連づけて記録した不正動作性データベースとを分割して構成してもよい。

この場合、不正動作性データベースの管理主体をセキュリティ専門会社に委ね、端末毎アプリデータベースのみを会社や学校等の組織で管理することもできる。

[0052] 最後に、本実施例では端末（１）側からapkが不正か否かを照会（Ｓ３４）

し、それに対して不正検知情報送信部（２６）が回答（Ｓ３５）する。これは不正検知情報送信ステップ（Ｓ９）に該当する。

不正アプリの場合は、警告表示を行い、アンインストールを促す画面をユーザ（３０）に対して表示する処理を行う。これは不正時対応処理（Ｓ１０）に該当する。

[0053] 次に、図４はアプリケーションが登録済みの場合のシーケンス図である。

図３の場合と同様に、apk情報がサーバ上に存在するかを照会した時、アプリケーションデータベース（２８）にapk情報が記録されている場合はYesを返す。上記のように、apk情報が登録されている場合には、dnaに係る情報が紐付いて登録されているため、この一覧を要求（Ｓ４０）する。

[0054] 登録状態通知部（２２）からは、アプリケーションデータベース（２８）に記録されたdnaの特徴値の一覧を返す（Ｓ４１）。上記で格納した特徴値のうち、例えばfilehash、hash_type、dna_typeを提供する。

[0055] このうち、登録されていない特徴値があった場合、特徴値送信部（１３）から不足分のdnaに係る特徴値を送信（Ｓ４２）し、サーバ（２）ではアプリケーションデータベース（２８）に記録する。

以後の処理は図３と同様であるので説明は省略する。

[0056] 図５は、アプリケーションを端末側で削除した時のシーケンス図である。ユーザがアプリをアンインストール（Ｓ５０）したとき、インストール状態検出部（１０）がこれを検出し、インストール通知部（１１）からインストール情報の更新処理（Ｓ５１）を行う。インストール情報としては、端末の識別番号（device id)、アプリのハッシュ値(hash)に加えて、アンインストールされた旨の情報(uninstall)が含まれる。

サーバ（２）ではアプリケーションデータベース（２８）が更新される。

[0057] このように本発明では端末上でアプリケーションが削除された後でも、過去にインストールされ、その後アンインストールされた旨の情報がサーバ（２）に記録されている。不正な動作を行うアプリケーションは、削除された場合であってもＯＳや他のアプリケーションの改ざんによって不正な動作を

続けることが多いため、削除されたアプリケーションの情報であっても重要である。

このインストール履歴を利用する例として、図６には、検知結果が更新された時にシーケンス図を示す。

[0058] まず本システムの管理者（６０）が、最新のシグネチャによって不正動作性が確認された新しい不正アプリをアプリケーションデータベース（２８）に登録（Ｓ６０）する。あるいは、本発明の不正検知ステップ（Ｓ７）において、アプリケーションの不正動作性が検知され、アプリケーションデータベース（２８）に登録した場合でもよい。

この時、不正検知情報送信部（２６）は、アプリケーションデータベースの上記インストール履歴に照会し、インストールされた記録がある端末（１）に対して、不正検知情報を送信する。端末（１）では上記と同様に不正時対応部（１５）によって処理される。

[0059] 不正検知情報送信部（２６）は、現在のインストール状態によって通知する不正検知情報を変化させてもよい。例えば、アンインストール後にも不正動作性を示すアプリケーションの場合には、不正検知情報を送信する一方で、アンインストールすると問題がないアプリケーションの場合には不正検知情報を送信しないこともできる。

[0060] また、各端末のアプリケーションをすべて記録しているので、アプリケーションの組み合わせによって不正検知情報を変化させてもよい。例えば、アプリＡとアプリＢがインストールされている場合のみ不正動作性を示す場合には、両アプリがインストールされた端末（１）のみに不正検知情報を送信する構成でもよい。

[0061] 図示したシーケンス図の処理は以上に説明した通りである。最後に、各処理ステップにおける実施例の詳細をいくつか挙げる。

まず、特徴値送信ステップ（Ｓ６）において、最初にサーバ（２）にアプリケーション情報を登録する場合には、特徴値だけでなくアプリケーション自体をサーバ（２）にアップロードすることもできる。サーバ（２）はこの

アップロードされたアプリケーションを対象に不正検知処理（Ｓ７）を行うことができる。

端末（１）からアプリケーション自体を送信せず、その入手先のＵＲＬ等をサーバ（２）に通知し、サーバ（２）が該ＵＲＬからダウンロードして取得する構成でもよい。

[0062] 図３においてapkが不正か否かを問い合わせる処理（Ｓ３４）は、図中の契機の他、端末（１）の起動時や、アプリケーションのアンインストール時、スマートフォン・携帯電話端末において通信圏外から通信圏内に入った時、などの所定の契機で繰り返し行うことも検知の精度向上の点で好適である。

[0063] 本発明に係る特徴値は上記のハッシュ値に限定されない。

まずハッシュ関数としては上記SHA1に限らず、ハッシュの種類はSHA1, SHA256, MD5など任意の関数を用いることができる。本システム用に定義したハッシュ関数でもよいし、ハッシュをとる対象に応じて種類を変化させてもよい。

[0064] ハッシュ値を計算する対象としては、アプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルである。

好適な例としては、androidのapkパッケージに含まれるdexファイル（プログラムコード）、manifest（アプリ構成のXMLファイルで、パッケージ名などが含まれる）、CERT（署名ファイル）、elf（Linux(登録商標）の実行コード）が挙げられる。

apkに別のapkが内包されている場合には、内包されているapkのハッシュ値を用いても良い。

[0065] 上記でファイルそのもののハッシュ値に限らず、ファイルに含まれる一部分のハッシュ値を計算してもよい。すなわち、上記dexファイル内の各クラスコードのハッシュ値を用いても良い。この場合、dexファイルから１つのハッシュ値をとるのではなく、dexファイルに含まれる各クラスコードについてそれぞれ別のハッシュ値を計算することになる。

[0066] 特徴値にはハッシュ値に限らず、アプリケーションファイルやそのパッケ

ージを構成する要素ファイルに基づくメタデータや、文字列を用いても良い。

例えば、dexファイル内のクラス名一覧を特徴値とし、その部分一致をとる構成でもよい。

[0067] 上記実施例では端末（１）側にのみ特徴値計算部（１２）を設けているが、本発明ではサーバ（２）にも特徴値計算部（２７）を備えることができる。例えば、サーバ（２）において端末（１）でのインストールの有無に関わらずアプリケーションの不正動作性を検知してデータベースに記録しておく場合には、アプリケーションのダウンロード、特徴値の計算、不正検知を単独で行い、アプリケーションデータベース（２８）に蓄積する。

符号の説明

[0068] １　端末装置

１０　インストール状態検出部

１１　インストール通知部

１２　特徴値計算部

１３　特徴値送信部

１４　不正検知情報受信部

１５　不正時対応部

２　不正検知サーバ

２０　インストール通知受信部

２１　アプリケーション情報検索部

２２　登録状態通知部

２３　特徴値受信部

２４　不正検知部

２５　不正検知結果記録部

２６　不正検知情報送信部

２７　特徴値計算部

２８　アプリケーションデータベース

３　ネットワーク

請求の範囲

［請求項1］ ユーザが適宜アプリケーションをインストール可能な端末装置と、該端末装置にインストールされたアプリケーションの不正動作性を検知する不正検知サーバ装置とから構成される不正アプリケーション検知システムであって、

該端末装置には、

アプリケーションのインストール状態が変化したことを検出するインストール状態検出処理部と、

インストール状態が変化した時に、該インストールされたアプリケーション情報を、該不正検知サーバ装置に通知するインストール通知処理部と、

当該アプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を計算する特徴値計算処理部と、

該アプリケーション情報とその特徴値を、該不正検知サーバ装置に通知する特徴値送信処理部と、

該不正検知サーバ装置から少なくとも当該アプリケーションの不正動作性が検知された場合に不正検知情報を受信する不正検知情報受信処理部と、

該不正検知情報の受信時に、該端末装置上で所定の対応処理を行う不正時対応処理部と

を備えると共に、

該不正検知サーバ装置には、

端末装置の該インストール通知処理部からインストールされたアプリケーション情報を受信するインストール通知受信処理部と、

端末装置の該特徴値送信処理部から該特徴値を受信する特徴値受信処理部と、

登録したアプリケーションの不正動作性を装置内で検出、又は外部

から取得して検知する不正検知処理部と、

該特徴値と該不正動作性の情報とを関連付けてアプリケーションデータベースに登録する不正検知結果記録処理部と、

少なくとも当該アプリケーションの不正動作性が検知された場合に不正検知情報を該端末装置に送信する不正検知情報送信処理部と

を備えた

ことを特徴とする不正アプリケーション検知システム。

[請求項2] 前記不正検知サーバ装置に、

通知された該アプリケーション情報についてアプリケーションデータベースに登録済みか否かを検索するアプリケーション情報検索処理部と、

該端末装置に向けて、登録済みか否かの該検索結果を通知する登録状態通知処理部と

を備え、

前記端末装置の特徴値送信処理部が、

該不正検知サーバ装置において当該アプリケーション情報が登録済みか否かに応じ、該アプリケーション情報とその特徴値を、該不正検知サーバ装置に通知する

請求項１に記載の不正アプリケーション検知システム。

[請求項3] 前記不正検知サーバ装置において、

前記不正検知結果記録部が、前記端末装置からのインストール通知を契機として、端末装置毎にアプリケーションのインストール状態を前記アプリケーションデータベースに記録し、

前記不正検知処理部において当該アプリケーションの不正動作性が検知されたときに、

すでに端末装置上から当該アプリケーションが削除された後であっても、前記不正検知情報送信処理部が不正検知情報を送信する

請求項１又は２に記載の不正アプリケーション検知システム。

［請求項4］ 前記アプリケーションデータベースが、

端末毎のインストール状態を記録した端末毎アプリデータベースと、

前記特徴値と前記不正動作性の情報とを関連づけて記録した不正動作性データベースと

に分割して構成される

請求項１ないし３のいずれかに記載の不正アプリケーション検知システム。

［請求項5］ 前記不正検知サーバ装置に、

入力された任意のアプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を計算する特徴値計算処理部を備えると共に、

前記不正検知処理部において当該アプリケーションの不正動作性を検知し、

前記不正検知結果記録部が、該特徴値と該不正動作性の情報とを関連付けてアプリケーションデータベースに登録する

請求項１ないし４のいずれかに記載の不正アプリケーション検知システム。

［請求項6］ ユーザが適宜アプリケーションをインストール可能な端末装置と、該端末装置にインストールされたアプリケーションの不正動作性を検知する不正検知サーバ装置とから構成される不正アプリケーション検知システムで用いられる端末装置であって、

アプリケーションのインストール状態が変化したことを検出するインストール状態検出処理部と、

インストール状態が変化した時に、該インストールされたアプリケーション情報を、該不正検知サーバ装置に通知するインストール通知処理部と、

当該アプリケーションファイル、又は当該アプリケーションのパッ

ケージを構成する要素ファイルに基づく所定の特徴値を計算する特徴値計算処理部と、

該アプリケーション情報とその特徴値を、該不正検知サーバ装置に通知する特徴値送信処理部と、

該不正検知サーバ装置から少なくとも当該アプリケーションの不正動作性が検知された場合に不正検知情報を受信する不正検知情報受信処理部と、

該不正検知情報の受信時に、該端末装置上で所定の対応処理を行う不正時対応処理部と

を備えたことを特徴とする端末装置。

[請求項7] ユーザが適宜アプリケーションをインストール可能な端末装置と、該端末装置にインストールされたアプリケーションの不正動作性を検知する不正検知サーバ装置とから構成される不正アプリケーション検知システムで用いられる不正検知サーバ装置であって、

該端末装置のインストール通知処理部からインストールされたアプリケーション情報を受信するインストール通知受信処理部と、

端末装置の該特徴値送信処理部から該特徴値を受信する特徴値受信処理部と、

登録したアプリケーションの不正動作性を装置内で検出、又は外部から取得して検知する不正検知処理部と、

該特徴値と該不正動作性の情報とを関連付けてアプリケーションデータベースに登録する不正検知結果記録処理部と、

少なくとも当該アプリケーションの不正動作性が検知された場合に不正検知情報を該端末装置に送信する不正検知情報送信処理部と

を備えたことを特徴とする不正検知サーバ装置。

[請求項8] ユーザが適宜アプリケーションをインストール可能な端末装置と、該端末装置にインストールされたアプリケーションの不正動作性を検知する不正検知サーバ装置とを用いて端末装置にインストールされた

不正アプリケーションを検知する方法であって、

端末装置におけるアプリケーションのインストール状態が変化したことを検出するインストール状態検出ステップ、

インストール状態が変化した時に、該インストールされたアプリケーション情報を、該不正検知サーバ装置に通知するインストール通知ステップ、

アプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を該不正検知サーバ装置に通知する特徴値送信ステップ、

該特徴値と、当該アプリケーションの不正動作性とを関連付けてアプリケーションデータベースに登録する不正検知結果記録ステップ、

少なくとも当該アプリケーションの不正動作性が検知された場合に不正検知情報を該端末装置に送信する不正検知情報送信ステップ、

該不正検知情報の受信時に、該端末装置上で所定の対応処理を行う不正時対応処理ステップ、

を有する

ことを特徴とする不正アプリケーション検知方法。

[請求項9] 前記インストール通知ステップに続いて、

不正検知サーバ装置において、前記端末装置から通知されたアプリケーション情報についてアプリケーションデータベースに登録済みか否かを検索するアプリケーション情報検索ステップ、

該端末装置に向けて、登録済みか否かの該検索結果を通知する登録状態通知ステップ、

をさらに有し、

前記特徴値送信ステップでは登録されていなかったアプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を該不正検知サーバ装置に通知するようにした

請求項８に記載の不正アプリケーション検知方法。

[請求項10] 前記不正検知サーバ装置において、前記端末装置からのインストール通知を契機として、端末装置毎にアプリケーションのインストール状態を前記アプリケーションデータベースに記録し、

当該アプリケーションの不正動作性が検知されたときに、すでに端末装置上から当該アプリケーションが削除された後であっても、該端末装置に不正検知情報を送信する

請求項８又は９に記載の不正アプリケーション検知方法。

[請求項11] 前記不正検知サーバ装置において、入力された任意のアプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を計算すると共に、当該アプリケーションの不正動作性を検知し、該特徴値と該不正動作性の情報とを関連付けてアプリケーションデータベースに登録する

請求項８ないし１０のいずれかに記載の不正アプリケーション検知方法。