(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4295684号
(P4295684)

(45)発行日　平成21年7月15日(2009.7.15)　(24)登録日　平成21年4月17日(2009.4.17)

(51)Int.Cl.		F I		
G06F 21/22	(2006.01)	G06F	9/06	660G
G06F 21/24	(2006.01)	G06F	12/14	530B
G09C 1/00	(2006.01)	G06F	12/14	560B
		G06F	12/14	560C
		G09C	1/00	660D

請求項の数 16　(全 36 頁)

(21)出願番号　特願2004-199677(P2004-199677)
(22)出願日　平成16年7月6日(2004.7.6)
(65)公開番号　特開2005-100347(P2005-100347A)
(43)公開日　平成17年4月14日(2005.4.14)
審査請求日　平成19年4月20日(2007.4.20)
(31)優先権主張番号　特願2003-305397(P2003-305397)
(32)優先日　平成15年8月28日(2003.8.28)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100105050
弁理士　鷲田　公一
(72)発明者　里　雄二
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　伊藤　智祥
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　山口　孝雄
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】プログラム製作装置

(57)【特許請求の範囲】
【請求項１】
販売者を特定する販売者用透かしを挿入したプログラムを配信するプログラム製作装置と、配信された前記プログラムに利用者を特定する利用者用透かしを挿入して配信するプログラム配信装置とを含むプログラム配信システムに使用されるプログラム製作装置であって、
前記販売者が前記利用者を特定する利用者用透かしを挿入可能なダミーモジュールを、前記プログラムの本体モジュールに追加するダミーモジュール追加手段と、
前記販売者を特定する販売者用透かしを、前記本体モジュールに挿入する透かし挿入手段と、
電子署名を、前記本体モジュールに付与する署名手段と、
前記ダミーモジュールと、前記販売者用透かしが挿入され前記電子署名が付与された前記本体モジュールとを含む前記プログラムを、前記プログラム配信装置に配信する送信手段と、
を具備することを特徴とするプログラム製作装置。
【請求項２】
前記プログラムの本体モジュールを複数のモジュールに分割するプログラム分割手段を具備したことを特徴とする請求項１記載のプログラム製作装置。
【請求項３】
前記送信手段は、前記販売者が前記ダミーモジュールに付与する電子署名用の秘密鍵を

、前記プログラム配信装置に送信することを特徴とする請求項１または請求項２記載のプログラム製作装置。
【請求項４】
前記送信手段は、前記販売者が挿入する前記利用者用透かしを検査するための検査プログラムを、前記プログラムに付加して送信することを特徴とする請求項１から請求項３のいずれかに記載のプログラム製作装置。
【請求項５】
前記プログラムを複数に分割し、複数の前記プログラム配信装置を介して前記利用者に配布することを特徴とする請求項１から請求項４のいずれかに記載のプログラム製作装置。
【請求項６】
プログラムの本体モジュールに、利用者を特定する利用者用透かしを挿入可能なダミーモジュールを追加し、かつ、販売者を特定する販売者用透かしを挿入し、かつ、製作者の電子署名を付与してなる販売者用プログラムを取得する取得手段と、
前記販売者用プログラムの前記ダミーモジュールに、利用者を特定する利用者用透かしを挿入する透かし挿入手段と、
前記利用者用透かしが挿入された前記ダミーモジュールに、電子署名を付与する署名手段と、
前記販売者用プログラムの前記ダミーモジュールに、前記利用者透かしを挿入し、かつ、前記販売者の電子署名を付与してなる利用者用プログラムを、前記プログラム利用装置に送信する送信手段と、
を具備したことを特徴とするプログラム配信装置。
【請求項７】
前記署名手段は、前記製作者から送信された電子署名用の秘密鍵を用いて前記ダミーモジュールに電子署名を付与することを特徴とする請求項６記載のプログラム配信装置。
【請求項８】
プログラムの本体モジュールに、利用者を特定する利用者用透かしを挿入可能なダミーモジュールを追加し、かつ、販売者を特定する販売者用透かしを挿入し、かつ、製作者の電子署名を付与してなる販売者用プログラムの前記ダミーモジュールに、前記利用者用透かしを挿入し、かつ、前記販売者の電子署名を付与してなる利用者用プログラムを受信する受信手段と、
前記利用者用プログラムから前記利用者用透かしを検査する透かし検査手段と、
を具備したことを特徴とするプログラム利用装置。
【請求項９】
前記プログラムが複数のモジュールに分割されている場合、前記複数のモジュールを結合して元の前記プログラムを生成する結合手段と、
生成された前記プログラム本体を実行する実行手段と、
を具備したことを特徴とする請求項８記載のプログラム利用装置。
【請求項１０】
前記透かし検査手段は、前記利用者用透かしを検査する検査プログラムを伝送路上の端末から取得することを特徴とする請求項８または請求項９記載のプログラム利用装置。
【請求項１１】
前記検査プログラムは、前記利用者用プログラムに実装されていることを特徴とする請求項８または請求項９記載のプログラム利用装置。
【請求項１２】
請求項１記載のプログラム製作装置と、請求項６記載のプログラム配信装置と、請求項８記載のプログラム利用装置と、を具備したことを特徴とするプログラム流通システム。
【請求項１３】
販売者を特定する販売者用透かしを挿入したプログラムを配信するプログラム製作装置と、配信された前記プログラムに利用者を特定する利用者用透かしを挿入して配信するプ

ログラム配信装置とを含むプログラム配信システムに使用されるプログラム製作装置におけるプログラム配信方法であって、
前記販売者が前記利用者を特定する利用者用透かしを挿入可能なダミーモジュールを、前記プログラムの本体モジュールに追加するダミーモジュール追加ステップと、
前記販売者を特定する販売者用透かしを、前記本体モジュールに挿入する透かし挿入ステップと、
電子署名を、前記本体モジュールに付与する署名付与ステップと、
前記ダミーモジュールと、前記販売者用透かしが挿入され前記電子署名が付与された前記本体モジュールとを含む前記プログラムを、前記プログラム配信装置に配信する送信ステップと、
を有することを特徴とするプログラム配信方法。
【請求項１４】
請求項１３記載のプログラム配信方法により配信された前記販売者用プログラムをプログラム利用装置に配信するプログラム配信装置におけるプログラム配信方法であって、
前記販売者用プログラムを取得するステップと、
前記販売者用プログラムの前記ダミーモジュールに、前記利用者を特定する利用者用透かしを挿入するステップと、
前記利用者用透かしが挿入された前記ダミーモジュールに、電子署名を付与するステップと、
前記販売者用プログラムの前記ダミーモジュールに、前記利用者透かしを挿入し、かつ、前記販売者の電子署名を付与してなる利用者用プログラムを、前記プログラム利用装置に送信するステップと、
を具備したことを特徴とするプログラム配信方法。
【請求項１５】
請求項１４記載のプログラム配信方法により送られてきた前記利用者プログラムを利用するプログラム利用装置におけるプログラム利用方法であって、
受信手段が、前記利用者プログラムを受信するステップと、
透かし検査手段が、前記利用者用プログラムから前記利用者用透かしを検査するステップと、
を具備したことを特徴とするプログラム利用方法。
【請求項１６】
プログラム製作者側の装置において、販売者を特定する販売者用透かしを挿入して配信用プログラムをプログラム配信者側の装置に配信し、
前記プログラム配信者側の装置において、利用者を特定する利用者用透かしを挿入して配信された前記配信用プログラムを配信するプログラム配信システム、において配信される配信用プログラムであって、
本体モジュールと、前記本体モジュールに付加されたダミーモジュールとを含んで構成され、
前記本体モジュールは、コンピュータから入力される、電子署名と販売者を特定する販売者用透かしとを、記録可能に構成され、
前記ダミーモジュールは、電子署名と販売者を特定する販売者用透かしが前記本体モジュールに記録された後にコンピュータから入力される、利用者を特定する利用者用透かしを、記録可能に構成された、
ことを特徴とする配信用プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、プログラム電子透かしを応用した安全なプログラム流通システムに関するも

のである。
【背景技術】
【０００２】
コンピュータ技術の進展に伴い、ネットワークを介したプログラムコード（以下プログラム）の流通が一般的になっている。それに伴い、ダウンロードしたプログラムが解析されプログラム内で使用されている方式やアイデアが漏洩する、プログラム自体が改竄されそのプログラムを利用して不正行為が行われる、といったことが問題となっている。
【０００３】
また、他人の開発したプログラムの全体もしくは一部を無断で使用する、プログラムの開発者に許可なく再配布する、などのプログラムの盗用も大きな問題となってきている。
【０００４】
今後、ネットワークを介したプログラムの流通が拡大していくことを考えると、これらの不正利用からプログラムを保護する仕組みが必要である。
【０００５】
例えば、利用者が端末を操作して、販売者からプログラムをダウンロードする場合を考える。この場合、まず、製作者がプログラムを作成する。次に、販売者の端末がこのプログラムを登録する。そして、利用者の端末が、販売者の端末にプログラム配信の要求をすると、販売者の端末が利用者の端末に対しプログラムを送信し、利用者の端末が配信されてきたプログラムをダウンロードし、格納する。
【０００６】
このような状況では、次のような脅威が想定される。
１．利用者がプログラムの流出や改竄を行う。
２．販売者がプログラムの流出や改竄を行う。
３．他製作者がプログラムの盗用を行う。
【０００７】
これらの脅威に対抗する流通システムとしては、暗号化やハードウェア耐タンパ、電子透かしを用いたシステムがある。
【０００８】
ここで、ハードウェア耐タンパとは、不正な内部解析を防止する機構を備えたハードウェアのことで、ＬＳＩ内部のプログラムを解析しようとするとＬＳＩがこれを自動検知しプログラムを消去する、といったものを指す。
【０００９】
また、暗号化を用いたシステムでは、例えば特許文献１に開示されたものがある。
【００１０】
この方法では、まず利用者の端末で、端末に固有のＩＤ（端末ＩＤ）を用いて公開鍵暗号方式の秘密鍵を生成する。次に、利用者の端末は、コンテンツをダウンロードする際に、端末ＩＤを販売者に送信し、販売者がこのＩＤを用いて公開鍵を作成し、コンテンツを暗号化する。そして、販売者が暗号化したコンテンツを利用者に送信し、利用者側で予め作成しておいた秘密鍵により復号化してコンテンツを利用する。
【００１１】
また、暗号化したコンテンツの復号化やコンテンツの利用は利用者の端末内のハードウェア耐タンパ領域で行われる。
【００１２】
このようにすることで、ダウンロードしたコンテンツの不正流出や改竄を防止している。
【００１３】
また、上述した脅威に対抗する別のシステムとして、特許文献２に開示されたものがある。
【００１４】
この方法では、製作者が、作成したコンテンツに、コンテンツの利用者を特定するユニ

ークなＩＤを電子透かしとして挿入する。さらに、製作者は、コンテンツを利用者に配布する際に、暗号化を行う。

【００１５】

そして、コンテンツが不正に利用された場合には、コンテンツの利用を監視する不正利用監視センタが、ネットワークを探索し、不正に利用されたコンテンツから抽出したＩＤとセンタで保存している利用条件（ＩＤ）を照合することにより、コンテンツを不正利用した利用者を特定する。

【００１６】

このように、コンテンツの不正流出と改竄を防止している。

【特許文献１】特開２０００－３２４０９６号公報

【特許文献２】特開２０００－３３０８７３号公報

【発明の開示】

【発明が解決しようとする課題】

【００１７】

しかし、従来のコンテンツ流通システムでプログラムを流通させた場合、販売者によるプログラムの不正流出や改竄を防止できないという問題がある。

【００１８】

製作者が作成したプログラムを販売者の端末に登録し、利用者が端末を操作して販売者の端末に登録されたプログラムをダウンロードする場合、利用者での不正流出を防ぐために、利用者を特定するためのユニークなＩＤを電子透かしとしてプログラムに挿入することは非常に有用である。また、利用者での改竄を防止するためにハードウェア耐タンパを用いることも有用である。

【００１９】

しかしながら、従来の方法では、プログラムには販売者を特定する情報が含まれていない。このため、仮に販売者での不正流出が行われた場合に、流出元となった販売者を特定することができない。よって、販売者に対して不正流出を抑止する効果がない。

【００２０】

さらに、利用者を特定するためのＩＤをプログラムに挿入する際には、販売者がプログラムに利用者のＩＤを挿入することになる。この場合、販売者はプログラムを平文として扱いう必要がある。

【００２１】

このため、販売者は、利用者のＩＤを挿入する操作だけでなく、異なる動作をするようにプログラムを改竄することができる。つまり、販売者においてプログラムを改竄されてしまうという危険性がある。

【００２２】

そこで、販売者を利用することなく、製作者でプログラムに利用者のＩＤを挿入することも考えられるが、製作者が販売者を兼ねることができないケースも多い。

【００２３】

本発明は、かかる点に鑑みてなされたものであり、販売者が利用者を特定する情報をプログラムに挿入できるようにすると共に、販売者によるプログラムの不正流出や、改竄を防止する仕組みを提供することを目的とする。

【課題を解決するための手段】

【００２４】

本発明は、プログラム本体に、プログラム本体の動作に影響を与えず透かしを挿入できるダミーモジュールと、電子署名と、を付与するようにしたものである。

【発明の効果】

【００２５】

これにより、販売者がダミーモジュールに利用者を特定する透かしを挿入することができる。また、プログラム本体に電子署名を付与することにより、販売者がプログラムの不正流出をしたり、改竄したりすることを防止できる。

【発明を実施するための最良の形態】
【００２６】
本発明の第１の態様にかかるプログラム製作装置は、販売者を介して利用者に製作したプログラムを配信するプログラム製作装置であって、前記プログラムの動作に影響を与えず前記販売者が前記利用者を特定する利用者用透かしを挿入できるダミーモジュールを前記プログラムに追加するダミーモジュール追加手段と、前記プログラムに電子署名を付与する署名手段と、前記ダミーモジュールを追加し前記電子署名を追加した販売者用プログラムを前記販売者に配布する送信手段と、を具備した構成を採る。
【００２７】
この構成により、プログラムとは別にダミーモジュールを追加することにより、販売者がダミーモジュールに利用者ＩＤを挿入することができる。また、プログラムに署名を付与することで、販売者にプログラムを操作させることを防止できる。これにより、販売者によるプログラムの改竄を防止することができる。
【００２８】
本発明の第２の態様は、第１の態様にかかるプログラム製作装置において、前記プログラムに前記販売者を特定できる販売者用透かしを挿入する透かし挿入手段を具備した構成を採る。
【００２９】
これにより、仮にプログラムの不正流出があった場合でも、プログラムに販売者を特定する販売者用透かしが挿入されているため、流出元となった販売者を特定することができる。これにより、販売者によるプログラムの改竄を防止できる。
【００３０】
本発明の第３の態様は、第１の態様または第２の態様にかかるプログラム製作装置において、前記プログラムを複数のモジュールに分割するプログラム分割手段を具備した構成を採る。
【００３１】
これにより、ダミーモジュールを含めた全モジュール数が増加することになり、利用者は自身のＩＤの挿入されているダミーモジュールを多数のモジュールから特定することになるため非常に困難となる。また、モジュールとダミーモジュールとのサイズの差が小さくなり、利用者はモジュールのサイズに基づいて自身のＩＤの挿入されているダミーモジュールを特定できなくなる。したがって、利用者によるプログラムの改竄を防止することができる。
【００３２】
本発明の第４の態様は、第１の態様から第３の態様のいずれかにかかるプログラム製作装置において、前記販売者が前記ダミーモジュールに付与する電子署名用の秘密鍵を、前記販売者に送信する。
【００３３】
これにより、販売者がダミーモジュールに、プログラム製作装置の秘密鍵を使用して電子署名を付与することが可能となる。販売者が自分自身の秘密鍵でダミーモジュールに電子署名を付与した場合には、本体モジュール用の秘密鍵の証明書とダミーモジュール用の秘密鍵の証明書との発行先が異なる。このために、利用者にダミーモジュールの部分を容易に特定され、透かし挿入箇所を容易に特定されてしまう。しかし、実施の形態１では、利用者が署名の検査に使う証明書は、すべて製作者に対して発行されたものとなるため、証明書の発行先による透かし挿入箇所の特定が不可能となり、利用者による透かしの削除を防止することができる。
【００３４】
本発明の第５の態様は、第１の態様から第４の態様のいずれかにかかるプログラム製作装置において、前記販売者が挿入した前記利用者用透かしを検査するための検査プログラムを、前記プログラムに付加して送信する。
【００３５】

これにより、プログラム製作装置が付与した透かしを他の端末において検査できる。

【００３６】

本発明の第６の態様は、第１の態様から第５の態様のいずれかにかかるプログラム製作装置において、前記販売者用プログラムを複数に分割し、前記販売者を介して前記利用者に配布する。

【００３７】

これにより、販売者が完全なプログラムを持つことができなくなり、販売者が利用者を偽ったプログラムの不正流出を防止することができる。

【００３８】

本発明の第７の態様にかかるプログラム配信装置は、プログラム本体に、プログラム本体の動作に影響を与えず透かしを挿入できるダミーモジュールと、電子署名と、を付与した販売者用プログラムの前記ダミーモジュールに前記利用者を特定する利用者用透かしを挿入する透かし挿入手段と、前記ダミーモジュールに前記利用者透かしを挿入した利用者用プログラムを前記利用者に送信する送信手段と、を具備した構成を採る。

【００３９】

これにより、ダミーモジュールに利用者を特定するＩＤを挿入することが可能となり、利用者によるプログラムの不正利用を防止できる。

【００４０】

本発明の第８の態様は、第７の態様にかかるプログラム配信装置において、前記ダミーモジュールに電子署名を付与する署名手段を具備した構成を採る。

【００４１】

このように、ダミーモジュールに、電子署名が付与されているので、ダミーモジュールを改竄することができない。

【００４２】

本発明の第９の態様は、第８の態様にかかるプログラム配信装置において、前記ダミーモジュールの電子署名の付与には前記プログラム製作装置から送信された前記電子署名用の秘密鍵を用いる。

【００４３】

このように、ダミーモジュールに付与された電子署名は、プログラム製作装置の秘密鍵を用いて暗号化されているので、利用者は復号化に使用される公開鍵の違いに基づいて自身のＩＤの挿入されているダミーモジュールを特定できなくなる。この結果、利用者が、ダミーモジュールを改竄することを確実に防止できる。

【００４４】

本発明の第１０の態様にかかるプログラム利用装置は、プログラム本体に、プログラム本体の動作に影響を与えず透かしを挿入できるダミーモジュールと、電子署名と、を付与した販売者用プログラムの前記ダミーモジュールに利用者を特定する利用者用透かしを挿入した利用者用プログラムを受信する受信手段と、前記利用者用プログラムから前記利用者用透かしを検査する透かし検査手段と、を具備した構成を採る。

【００４５】

これにより、ダミーモジュールに付与された利用者用透かしと、自身のＩＤ情報を比較することにより、受信したプログラムの正当性を判断できる。

【００４６】

本発明の第１１の態様は、第１０の態様にかかるプログラム利用装置において、複数に分割された前記利用者用プログラムを結合する結合手段と、結合した前記利用者用プログラムを実行する実行手段と、を具備した構成を採る。

【００４７】

これにより、複数に分割されているプログラムを実行できる。

【００４８】

本発明の第１２の態様は、第１０の態様または第１１の態様にかかるプログラム利用装置において、前記透かし検査手段は、前記利用者用透かしを検査する検査プログラムを伝

送路上の端末より取得する。

【００４９】

このようにして、伝送路上の端末から検査プログラムを取得することで、プログラム利用装置で、製作者端末で挿入された透かしを抽出して、プログラムを実行することが可能となる。

【００５０】

本発明の第１３の態様は、第１２の態様にかかるプログラム利用装置において、前記検査プログラムは、前記利用者用プログラムに実装されている。

【００５１】

これにより、製作者端末で挿入された透かしを抽出して、プログラムを実行することが可能となる。また、これによりプログラムとそれに対応する検査プログラムとの管理が容易となる。

【００５２】

本発明の第１４の態様は、第１の態様にかかるプログラム製作装置と、第７の態様にかかるプログラム配信装置と、第１０の態様にかかるプログラム利用装置と、を具備したことを特徴とするプログラム流通システムである。

【００５３】

本発明の第１５の態様は、販売者を介して利用者に製作したプログラムを配信するプログラム配信方法であって、前記プログラムの動作に影響を与えず前記販売者が前記利用者を特定する利用者用透かしを挿入できるダミーモジュールを前記プログラムに追加するステップと、前記プログラムに電子署名を付与するステップと、前記ダミーモジュールを追加し前記電子署名を追加した販売者用プログラムを前記販売者に配布するステップと、を具備したことを特徴とするプログラム配信方法である。

【００５４】

本発明の第１６の態様は、第１５の態様にかかるプログラム配信方法により送られてきた前記販売者用プログラムを利用者に配信するプログラム配信方法であって、前記販売者用プログラムの前記ダミーモジュールに前記利用者を特定する利用者用透かしを挿入するステップと、前記ダミーモジュールに前記利用者透かしを挿入した利用者用プログラムを前記利用者に送信するステップと、を具備したことを特徴とするプログラム配信方法である。

【００５５】

本発明の第１７の態様は、第１６の態様にかかるプログラム配信方法により送られてきた利用者プログラムを受信するステップと、前記利用者用プログラムから前記販売者用透かしを検査するステップと、を具備したことを特徴とするプログラム利用方法である。

【００５６】

本発明の第１８の態様は、プログラムの動作に影響を与えず透かしを挿入できるダミーモジュールを前記プログラムに追加するステップと、前記プログラムに電子署名を付与するステップと、を具備したことを特徴とするプログラム製作方法である。

【００５７】

（実施の形態１）

本発明の実施の形態１にかかるプログラム流通システムについて添付図面を用いて説明する。図１は、実施の形態１にかかるプログラム流通システムの構成図である。

【００５８】

実施の形態１にかかるプログラム流通システムには、プログラム製作装置１０が設けられている。

【００５９】

プログラム製作装置１０は、プログラムを製作するメーカや個人等の製作者の端末を表す。

【００６０】

プログラム製作装置１０には、蓄積部２０が設けられている。蓄積部２０は、製作者が

製作したプログラムを保存するための手段で、ＦＤやＨＤ、内部メモリなどの物理デバイスを示している。

【００６１】

また、プログラム製作装置１０には、プログラム構造変換部３０が設けられている。プログラム構造変換部３０は、蓄積部２０に蓄積されているプログラムを複数のモジュール（本体モジュール）に分割する。また、プログラム構造変換部３０は、分割したプログラムにプログラムの動作に影響を与えないダミーモジュールを追加する。そして、プログラム構造変換部３０は、上述したように変換したプログラムを透かし挿入部４０に出力する。なお、プログラム構造変換部３０の詳細は後で詳述する。

【００６２】

透かし挿入部４０は、プログラム構造変換部３０が変換したプログラムの本体モジュールに電子透かしを挿入する。具体的には、透かし挿入部４０は、販売者を特定するＩＤ情報から生成される電子透かしをプログラムに挿入する。そして、透かし挿入部４０は、電子透かしを挿入したプログラムを署名部５０に出力する。なお、透かし挿入部４０については、後で詳述する。

【００６３】

署名部５０は、透かし挿入部４０が出力したプログラムの透かしが挿入されたモジュールに電子署名を付与する。署名部５０が付与する電子署名は、本体モジュールのハッシュ値を用いる。そして、署名部５０は、電子署名を付与したプログラムを送信部６０に出力する。なお、署名部５０については、後で詳述する。

【００６４】

送信部６０は、署名部５０から送られてきたプログラムのモジュールのパッケージ化とパッケージの送信、およびプログラムの利用者の端末であるプログラム利用装置１５０ａ、１５０ｂが透かし挿入部４０の挿入した電子透かしを検査する際に使用する検査プログラムをプログラムの販売者の端末であるプログラム配信装置７０に送信する。なお、送信部６０については、後で詳述する。

【００６５】

なお、実施の形態１では、検査プログラムをプログラムの販売者の端末であるプログラム配信装置７０に送信しているが、必ずしもプログラム配信装置７０に送信する必要はなく、独立した検査プログラム配布者に送信してもよい。

【００６６】

プログラム配信装置７０は、通信キャリアやプログラム配信のポータルサイトなどであるプログラムの販売者の端末を表す。プログラム配信装置７０は、受信したプログラムにプログラムの利用者ＩＤを挿入し、利用者にプログラムを配布する役割を持っている。

【００６７】

プログラム配信装置７０には、受信部９０が設けられている。受信部９０は、プログラム製作装置１０の送信部６０から送られてきたパッケージを復号しプログラムにする。また、受信部９０は、送信部６０から送られてきた検査プログラムを受信する。

【００６８】

また、プログラム配信装置７０には、要求受信部１００が設けられている。要求受信部１００は、利用者からのダウンロードの要求メッセージを受けるための手段である。

【００６９】

また、プログラム配信装置７０には、蓄積部１１０が設けられている。蓄積部１１０は、受信部９０から送られてきたプログラムと検査プログラム、および要求受信部１１０から送られてきた要求メッセージを蓄積する。

【００７０】

また、プログラム配信装置７０には、透かし挿入部１２０が設けられている。透かし挿入部１２０は、蓄積部１１０に蓄積されたプログラムから本体モジュールとダミーモジュールを抽出し、抽出したダミーモジュールに電子透かしを挿入する。また、透かし挿入部１２０は、挿入する電子透かしを、利用者を特定するＩＤから生成する。そして、透かし

挿入部１２０は、利用者を特定する電子透かしを挿入したプログラムを署名部１３０に送る。

【００７１】

署名部１３０は、透かし挿入部１２０から送られてきたプログラムのダミーモジュールのハッシュ値を計算し、計算したハッシュ値等からなる電子署名を送られてきたプログラムに付与する。そして、署名部１３０は、電子署名を付与したプログラムを送信部１４０に送る。

【００７２】

送信部１４０は、署名部１３０から送られてきたプログラムのモジュールのパッケージ化とこのパッケージの送信、および検査プログラムをプログラムの利用者の端末であるプログラム利用装置１５０ａ、１５０ｂに送信する。

【００７３】

プログラム利用装置１５０ａ、１５０ｂは、プログラムを利用する側のユーザの端末を表す。以下では、プログラム利用装置１５０ａを用いて説明を行い、プログラム利用装置１５０ａ、１５０ｂを単にプログラム利用装置１５０と表記する。

【００７４】

プログラム利用装置１５０には、要求送信部１６０が設けられている。要求送信部１６０は、販売者の端末であるプログラム配信装置７０にプログラムの配信を要求するメッセージを送信するための手段を表す。

【００７５】

また、プログラム利用装置１５０には、受信部１７０が設けられている。受信部１７０は、プログラム配信装置７０の送信部１４０から送られてきたパッケージを受信し、復号してプログラムにする手段である。また、受信部１７０は、送信部１４０から送られてきた検査プログラムも受信する。そして、受信部１７０は、復号化したプログラムおよび検査プログラムを蓄積部１８０に送る。

【００７６】

蓄積部１８０は、受信部１７０から送られてきたプログラムを蓄積する。

【００７７】

また、プログラム利用装置１５０には、受信モジュール検査部１９０が設けられている。受信モジュール検査部１９０は、受信部１７０がダウンロード（受信した）したプログラムの電子透かしや電子署名を検査するための手段を表す。そして、受信モジュール検査部１９０は、検査したプログラムを蓄積部２００に送る。なお、受信モジュール検査部１９０については、後で詳述する。

【００７８】

蓄積部２００は、受信モジュール検査部１９０から送られてきた検査後のプログラムを蓄積する。

【００７９】

また、プログラム利用装置１５０には、実行部２１０が設けられている。実行部２１０は、ダウンロードしたプログラムを実行するための手段を表す。

【００８０】

以上のように、プログラム流通システムは構成されている。

【００８１】

次に、実施の形態１におけるプログラム構造変換部３０について、図２を用いて説明する。図２は、実施の形態１にかかるプログラム構造変換部３０の構成図である。

【００８２】

プログラム構造変換部３０には、プログラム入力部３０１が設けられている。プログラム入力部３０１は、ダミーモジュールを追加し複数のモジュールに分割するプログラムを入力する手段である。プログラム入力部３０１は、プログラムをダミーモジュール追加部３０５に出力する。

【００８３】

ダミーモジュール追加部３０５は、ダミーモジュール入力部３０３より入力されたダミーモジュールをプログラム入力部３０１が入力したプログラムに追加し、プログラム分割部３０２に出力する手段である。また、ダミーモジュール追加部３０５は、ダミーモジュールを追加する際に、ａｓｓｅｒｔ法などを用いて、少なくとも一度は本体モジュールでダミーモジュールが呼び出されるようにしておくことが望ましい。

【００８４】

ここでａｓｓｅｒｔ法とは、プログラム中のａｓｓｅｒｔ文を、必ず偽になるｉｆ文に置き換えて、そのｉｆ文の中身にダミーモジュールの呼び出し文を追加する方法である。詳細は、一杉裕志「ソフトウェア電子透かしの挿入法、攻撃法、評価法、実装法」、情報処理学会、夏のプログラミングシンポジウム報告集に記されている。

【００８５】

また、ダミーモジュール追加部３０５は、追加されたダミーモジュール名をダミー情報記憶部３０４に渡す。

【００８６】

プログラム分割部３０２は、ダミーモジュール追加部３０５において、ダミーモジュールの追加されたプログラムを複数のモジュールに分割する手段である。例えば、プログラム分割部３０２は、プログラムがＪａｖａ（登録商標）言語で書かれていた場合には、コンパイルしたあとのｃｌａｓｓファイルをモジュールとし、またプログラムがＣ言語の場合には、コンパイル後のオブジェクトファイルをモジュールとすることが考えられる。また、プログラム分割部３０２は、モジュールの分割数を分割情報記憶部３０６に出力する。

【００８７】

プログラム出力部３０７は、ダミーモジュール追加部３０５によりダミーモジュールが追加され、プログラム分割部３０２により複数のモジュールに分割されたプログラムを出力する手段である。

【００８８】

この構成により、プログラム構造変換部３０は、プログラムにダミーモジュールを追加し、ダミーモジュールを追加したプログラムを複数のモジュールに分割する。

【００８９】

次に、実施の形態１における透かし挿入部４０について図３を用いて説明する。図３は、実施の形態１の透かし挿入部４０の構成図である。

【００９０】

透かし挿入部４０には、プログラム入力部４０１が設けられている。プログラム入力部４０１は、透かしを入力するプログラム、つまりプログラム構造変換部３０において変換されたプログラムを入力する手段である。プログラム入力部４０１は、入力したプログラムを挿入部４０２に出力する。

【００９１】

透かし用データ入力部４０３は、透かしとして挿入するデータ（透かし用データ）を入力する手段である。入力する透かし用データは、プログラム配信装置７０、つまり販売者を特定するための情報であり、販売者の住所、電話番号、会社名、氏名、電子メールアドレスなどである。また、透かし用データにプログラムの製作者（プログラム製作装置１０）の情報を入力してもよい。

【００９２】

ＩＤ情報生成部４０４は、透かし用データ入力部４０３により入力された透かし用データから販売者（プログラム配信装置７０）を一意に特定できるＩＤ情報を生成する手段である。ＩＤ情報は、入力したデータそのものであってもよいし、それを暗号化したデータであってもよい。また、ＩＤ情報は、透かし用データを保存するデータベースにおいて透かし用データを一意に特定するためのＩＤであってもよい。

【００９３】

なお、実施の形態１においては、ＩＤ情報に基づいて透かし情報を生成する形態となっ

ているが、必ずしもＩＤ情報に基づいて透かし情報を生成する必要はなく、透かし情報から一意に配布先を特定可能となっていれば良い。例えば、送信するモジュールに１～Ｎシーケンス番号を透かし情報として挿入し、販売者（プログラム配信装置７０）にシーケンス番号ｉのモジュールを配布といったように透かし情報と配布先を一意に特定可能としてもよい。

【００９４】

モジュール情報記憶部４０８は、プログラム構造変換部３０において、追加されたダミーモジュール名を記憶しておく手段である。モジュール情報記憶部４０８は、予めプログラム構造変換部３０のダミー情報記憶部３０４からダミーモジュール名を取得し、記憶しておく。

【００９５】

挿入部４０２は、ＩＤ情報生成部４０４により生成されるＩＤ情報からプログラムに実際に挿入する透かしを生成し、モジュール情報記憶部４０８より得られるダミーモジュール名を用いてダミーモジュールと本体モジュールを区別し、本体モジュールに透かしを挿入する手段である。また、挿入部４０２は、透かしを挿入した本体モジュール名を透かし情報記憶部４０５に出力する。

【００９６】

なお、挿入部４０２が挿入する透かし情報は、販売者ＩＤだけでなく、プログラムの権利情報や利用者端末のアクセスコントロール情報、セキュリティポリシーなどを挿入してもよい。

【００９７】

例えば、プログラムの権利情報は、プログラムの実行期限や実行回数、プログラムの他の端末への転送の可否などの情報であり、アクセスコントロール情報やセキュリティポリシー情報は、メモリやＨＤを読み書き可能、ソケットを利用可能、など端末リソースへのアクセス権に関する情報である。

【００９８】

透かし情報記憶部４０５は、透かしを挿入したモジュール名を記憶しておく手段である。

【００９９】

プログラム出力部４０６は、挿入部４０２が透かしを挿入したプログラムを出力する手段である。

【０１００】

この構成により、透かし挿入部４０は、本体モジュールに販売者を特定する透かしを挿入する。

【０１０１】

次に、実施の形態１にかかる署名部５０について図４を用いて説明する。図４は、実施の形態１における署名部５０の構成図である。

【０１０２】

署名部５０には、プログラム入力部５０１が設けられている。プログラム入力部５０１は、署名を付与するプログラム、つまり透かし挿入部４０から送られてきたプログラムを入力する手段である。プログラム入力部５０１は、入力したプログラムを署名付与部５０２に出力する。

【０１０３】

モジュール情報記憶部５０８は、プログラム構造変換部３０において、追加されたダミーモジュール名を記憶しておく手段である。モジュール情報記憶部５０８は、予めプログラム構造変換部３０のダミー情報記憶部３０４からダミーモジュール名を取得し、記憶しておく。

【０１０４】

署名用鍵入力部５０３は、署名を暗号化するための秘密鍵を入力する手段である。

【０１０５】

署名付与部５０２は、モジュール情報記憶部５０８より得られたダミーモジュール名を用いて本体モジュールとダミーモジュールを判断し、本体モジュールのハッシュ値を計算する。次に、署名付与部５０２は、署名用鍵入力部５０３より入力される秘密鍵（製作者秘密鍵）を用いて、計算したハッシュ値を暗号化する。

【０１０６】

また、署名付与部５０２は、署名フォーマットを用いて、モジュールと署名であるハッシュ値、署名検証用の公開鍵（製作者公開鍵）を含む証明書を一つのファイルにまとめる。さらに、署名付与部５０２は、モジュール名とハッシュ値を対応付けて署名データ記憶部５０５に出力する。

【０１０７】

署名データ記憶部５０５は、署名付与部５０２が出力したモジュール名とハッシュ値を対応付けて記憶する。

【０１０８】

プログラム出力部５０６は、署名付与部５０２により署名等がつけられたプログラムを出力する手段である。

【０１０９】

この構成により、署名部５０は本体モジュールに署名を付与し、さらに署名を秘密鍵で暗号化する。

【０１１０】

次に、実施の形態１にかかる送信部６０について図５を用いて説明する。図５は、実施の形態１における送信部６０の構成図である。

【０１１１】

送信部６０には、署名部５０から出力されたプログラムを入力するプログラム入力部６０１が設けられている。プログラム入力部６０１は、販売者つまりプログラム配信装置７０に送信するプログラムを入力する手段である。プログラム入力部６０１は、入力したプログラムを送信データパッケージ化部６０２に出力する。

【０１１２】

送信データパッケージ化部６０２は、プログラムを含む種々のデータをまとめて、販売者、つまりプログラム配信装置７０に送信する販売者向けパッケージを作成する手段である。また、送信データパッケージ化部６０２は、販売者向けパッケージ化されたプログラムのデータサイズもしくはＣＲＣサイズをパッケージ情報記憶部６１０に渡す。なお、販売者向けパッケージについては、後で詳述する。

【０１１３】

パッケージデータ入力部６０８は、ダミーモジュール名の記述されたファイルを入力する。

【０１１４】

暗号鍵生成部６０５は、通信用の暗号鍵を生成する手段である。暗号鍵生成部６０５は、製作者と販売者で、つまりプログラム製作装置１０とプログラム配信装置７０との間でパッケージをやりとりするために使用される暗号鍵を生成する。

【０１１５】

検査プログラム入力部６０９は、透かし挿入部４０で挿入された透かしを検査するための検査プログラムを入力する手段である。

【０１１６】

インストールプログラム入力部６１１は、利用者、つまりプログラム利用装置１５０が、販売者、つまりプログラム配信装置７０から送られてきたプログラムをインストールするためのソフトを入力する手段である。

【０１１７】

暗号化部６０７は、暗号鍵生成部６０５により生成された通信用の暗号鍵を用いて、パッケージ化されたプログラムおよび、検査プログラム入力部６０８により入力された透かしの検査プログラムを暗号化し、プログラム送信部６０６に出力する手段である。

【０１１８】
プログラム送信部６０６は、送信データパッケージ化部６０２によりパッケージ化され、暗号化部６０７により暗号化されたプログラムをプログラム配信装置７０に対して送信する手段である。
【０１１９】
次に、送信データパッケージ化部６０２が作成する販売者向けパッケージについて図６を用いて説明する。図６は、実施の形態１にかかる販売者向けパッケージの構成図である。
【０１２０】
販売者向けパッケージ７００は、本体モジュール７０１と、ダミーモジュール７０２と、署名部５０の署名付与部５０２が計算した本体モジュールの署名値７０３と、秘密鍵で暗号化された署名値７０３を復号化するための公開鍵（製作者公開鍵）７０４と、ダミーモジュール名の記述されたファイル６０５と、ダミーモジュールに署名するための秘密鍵（製作者秘密鍵）７０６とダミーモジュールの署名を復号するための公開鍵（製作者公開鍵）７０７と、インストールプログラム７０９と、から構成されている。
ここで、公開鍵７０４及び７０６は、証明書発行機関により証明書が発行されているものとし、以下では公開鍵を含んだ証明書を、公開鍵と記述する。
【０１２１】
また、パッケージ化の例としては、ｊａｒファイルやｔａｒファイルなどが考えられ、パッケージ化したファイルは圧縮してもよい。
【０１２２】
また、プログラム送信部６０６は、販売者向けパッケージ７００と共に検査プログラム７０８をプログラム配信装置７０に送信する。これにより、プログラム製作装置１０が付与した透かしを他の端末において検査できる。
【０１２３】
なお、ここでは、ダミーモジュールに署名するための秘密鍵（製作者秘密鍵）７０６を配布しているが、かならずしも配布する必要はない。また、このとき、インストールプログラム７０９及び透かしの検査プログラム７０８は、難読化などのソフトウェア耐タンパ手法により保護されていることが望ましい。これにより、インストールプログラム７０９と検査プログラム７０８の動作が不正に解析されることによる透かしの削除や改変を防止できる。
【０１２４】
次に、実施の形態１における透かし挿入部１２０について図７を用いて説明する。図７は、実施の形態１の透かし挿入部１２０の構成図である。
【０１２５】
プログラム入力部１２０１は、蓄積部１１０から抽出した透かしを入力するプログラムを入力する手段である。プログラム入力部１２０１は、入力したプログラムを挿入部１２０２に出力する。
【０１２６】
透かし用データ入力部１２０３は、透かしとして挿入するデータ（透かし用データ）を入力する手段である。入力する透かし用データは、プログラム利用装置１５０、つまり利用者を特定するための情報であり、利用者の住所、電話番号、会社名、氏名、電子メールアドレスなどである。また、透かし用データにプログラムの販売者（プログラム配信装置７０）の情報を入力してもよい。
【０１２７】
ＩＤ情報生成部１２０４は、透かし用データ入力部１２０３により入力された透かし用データから利用者を一意に特定できるＩＤ情報を生成する手段である。ＩＤ情報は、入力したデータそのものであってもよいし、それを暗号化したデータであってもよい。また、ＩＤ情報は、透かし用データを保存するデータベースにおいて透かし用データを一意に特定するためのＩＤであってもよい。

【０１２８】
挿入部１２０２は、ＩＤ情報生成部１２０４により生成されるＩＤ情報からプログラムに実際に挿入する透かしを生成し、モジュール情報記憶部１２０８より得られるダミーモジュール名を用いてダミーモジュールと本体モジュールを区別し、ダミーモジュールに透かしである利用者ＩＤを挿入する手段である。そして、挿入部１２０２は、透かしを挿入したモジュール名を透かし情報記憶部１２０５に出力する。
【０１２９】
透かし情報記憶部１２０５は、透かしを挿入したモジュール名を記憶しておく手段である。
【０１３０】
プログラム出力部１２０６は、挿入部１２０２が透かしを挿入したプログラムを出力する手段である。
【０１３１】
この構成により、透かし挿入部１２０はダミーモジュールに利用者を特定する透かしを挿入する。
【０１３２】
なお、実施の形態１においては、ＩＤ情報に基づいて透かし情報を生成する形態となっているが、必ずしもＩＤ情報に基づいて透かし情報を生成する必要はなく、透かし情報から一意に利用者を特定可能となっていれば良い。例えば、送信するモジュールに１～Ｎシーケンス番号を透かし情報として挿入し、利用者（プログラム利用装置１５０）にシーケンス番号ｉのモジュールを配布といったように透かし情報と利用者を一意に特定可能としてもよい。
【０１３３】
また、透かし情報は利用者ＩＤだけでなく、プログラムの権利情報や利用者端末のアクセスコントロール情報、セキュリティポリシーなどを挿入してもよい。
【０１３４】
例えば、プログラムの権利情報は、プログラムの実行期限や実行回数、プログラムの他の端末への転送の可否などの情報であり、アクセスコントロール情報やセキュリティポリシー情報は、メモリやＨＤを読み書き可能、ソケットを利用可能、など端末リソースへのアクセス権に関する情報である。
【０１３５】
次に、実施の形態１にかかる署名部１３０について図８を用いて説明する。図８は、実施の形態１における署名部１３０の構成図である。
【０１３６】
署名部１３０には、プログラム入力部１３０１が設けられている。プログラム入力部１３０１は、署名を付与するプログラム、つまり透かし挿入部１２０から送られてきたプログラムを入力する手段である。プログラム入力部１３０１は、入力したプログラムを署名付与部１３０２に出力する。
【０１３７】
モジュール情報記憶部１３０８は、プログラム製作装置１０から送られてきた販売者向けパッケージ７００のダミーモジュール名７０５を記憶しておく。
【０１３８】
署名用鍵入力部１３０３は、プログラム製作装置１０から送られてきた販売者向けパッケージ７００のダミーモジュールに署名するための秘密鍵７０６とダミーモジュールの署名値を復号化するための公開鍵７０７を記憶しておく。
【０１３９】
署名付与部１３０２は、モジュール情報記憶部１３０８より得られたダミーモジュール名を用いて本体モジュールとダミーモジュールを判断し、ダミーモジュールのハッシュ値を計算する。次に、署名付与部１３０２は、署名用鍵入力部１３０３より入力される秘密鍵（製作者秘密鍵）７０６を用いてダミーモジュールのハッシュ値を暗号化する。

【０１４０】
また、署名付与部１３０２は、署名フォーマットを用いて、モジュールとハッシュ値、署名検証用の公開鍵書を一つのファイルにまとめる。さらに、署名付与部１３０２は、モジュール名とハッシュ値を対応付けて署名データ記憶部１３０５に出力し、ダミーモジュール用の秘密鍵７０６とダミーモジュール用の公開鍵７０７を合わせて出力する。
【０１４１】
プログラム出力部１３０６は、署名付与部１３０２により署名がつけられたプログラムを出力する手段である。
【０１４２】
この構成により、署名部１３０は、ダミーモジュールに署名をし、さらに署名を製作者の秘密鍵で暗号化する。
【０１４３】
次に、実施の形態１にかかる送信部１４０について図９を用いて説明する。図９は、実施の形態１における送信部１４０の構成図である。
【０１４４】
送信部１４０には、プログラム入力部１４０１が設けられている。プログラム入力部１４０１は、署名部１３０から送られてきたプログラムを入力する手段である。プログラム入力部１４０１は、入力したプログラムを送信データパッケージ化部１４０２に出力する。
【０１４５】
送信データパッケージ化部１４０２は、プログラムを含む種々のデータをまとめて、利用者（プログラム利用装置１５０）に送信する利用者向けパッケージを作成する手段である。また、送信データパッケージ化部１４０２は、利用者向けパッケージ化されたプログラムのデータサイズもしくはＣＲＣサイズをパッケージ情報記憶部１４１０に渡す。
【０１４６】
なお、利用者向けパッケージについては、後で詳述する。
【０１４７】
パッケージデータ入力部１４０８は、製作者、つまりプログラム製作装置１０から送られてきた販売者向けパッケージ７００を入力する。
【０１４８】
暗号鍵生成部１４０５は、通信用の暗号鍵を生成する手段である。暗号鍵生成部１４０５は、販売者と利用者で、つまりプログラム配信装置７０とプログラム利用装置１５０の間でパッケージをやりとりするために使用される暗号鍵を生成する。
【０１４９】
検査プログラム入力部１４１２は、透かし挿入部４０で挿入された透かしを検査するための検査プログラムを入力する手段である。
【０１５０】
暗号化部１４０７は、暗号鍵生成部１４０５により生成された通信用の暗号鍵を用いて、パッケージ化されたプログラムと、検査プログラム入力部１４１２により入力された透かしの検査プログラムを暗号化する手段である。
【０１５１】
プログラム送信部１４０６は、送信データパッケージ化部１４０２によりパッケージ化され、暗号化部１４０７により暗号化されたプログラムを、プログラム利用装置１５０に送信する手段である。
【０１５２】
次に、送信データパッケージ化部１４０２が作成する利用者向けパッケージについて図１０を用いて説明する。図１０は、実施の形態１にかかる利用者向けパッケージの構成図である。
【０１５３】
利用者向けパッケージ１０００には、本体モジュール７０１と、ダミーモジュール７０

２と、販売者向けパッケージ７００に含まれる本体モジュールの署名値７０３と、署名部１３０の署名付与部１３０２が計算したダミーモジュールの署名値１００４、販売者向けパッケージ７００に含まれる本体モジュールの署名値７０３の公開鍵（製作者公開鍵）７０４と、ダミーモジュールの署名値１００４の公開鍵（製作者公開鍵）７０７と、インストールプログラム７０９と、から構成されている。

【０１５４】

また、パッケージ化の例としては、ｊａｒファイルやｔａｒファイルなどが考えられ、パッケージ化したファイルは圧縮してもよい。

【０１５５】

また、プログラム送信部１４０６は、利用者向けパッケージ１０００と共に検査プログラム７０８をプログラム利用装置１５０に送信する。

【０１５６】

次に、実施の形態１にかかる受信モジュール検査部１９０について図１１を用いて説明する。図１１は、実施の形態１における受信モジュール検査部１９０の構成図である。

【０１５７】

受信モジュール検査部１９０には、プログラム入力部１９０１が設けられている。プログラム入力部１９０１は、受信部１７０から送られてきた、各モジュールの検査と結合を行うプログラムを入力する手段である。プログラム入力部１９０１は、プログラムを受信パッケージ検査部１９０２に出力する。

【０１５８】

パッケージ情報記憶部１９０３は、販売者（プログラム配信装置７０）より受信したパッケージのサイズもしくはＣＲＣサイズを記憶する手段である。パッケージ情報記憶部１９０３は、パッケージのサイズを予めプログラム配信装置７０から取得しておく。

【０１５９】

受信パッケージ検査部１９０２は、販売者（プログラム配信装置７０）より受信したパッケージが完全なものか判断する手段である。具体的には、受信パッケージ検査部１９０２は、パッケージ情報記憶部１９０３より得られたパッケージのサイズもしくはＣＲＣサイズと、受信したパッケージのサイズが一致しているか検査する。そして、受信パッケージ検査部１９０２は、パッケージ情報記憶部１９０３より得られたパッケージのサイズもしくはＣＲＣサイズと、受信したパッケージのサイズが一致する場合には、プログラムを署名検査部１９０４に出力し、一致しなかった場合には、受信したパッケージを破棄する。

【０１６０】

署名検査部１９０４は、受信したすべてのモジュールの署名が正しいか検査するための手段で、受信したモジュール毎のハッシュ値を計算する。次に、署名検査部１９０４は、利用者向けパッケージ１０００に記述された対応するモジュールの署名値（ハッシュ値）７０３、１００４を、利用者向けパッケージ１０００に付与された本体モジュールの公開鍵７０４とダミーモジュールの署名値１００４を復号化するための公開鍵７０７を用いて復号化する。そして、署名検査部１９０４は、計算した署名値と、モジュールに付与された署名値と比較し、一致する場合にはプログラムをモジュール結合部１９０５に出力し、一致しない場合には販売者から受信したモジュールをすべて破棄する。

【０１６１】

モジュール結合部１９０５は、販売者より受信したすべてのモジュールを一つに結合し、元のプログラムを生成する手段である。

【０１６２】

検査プログラム入力部１９０６は、販売者、つまりプログラム配信装置７０より獲得した透かしの検査プログラムを入力する手段である。

【０１６３】

端末情報入力部１９０８は、プログラム利用装置１５０の端末ＩＤ（利用者ＩＤ）を入力する手段である。

【０１６４】
透かし検査部１９０７は、結合されたプログラムの透かしを抽出し、端末ＩＤと一致しているかを判定するための手段である。
【０１６５】
具体的には、透かし検査部１９０７は、検査プログラム入力部１９０６により入力された検査プログラムを用いて、モジュール結合部１９０５で生成されたプログラムの透かしを抽出し、端末情報入力部１９０８により入力された端末ＩＤと比較する。そして、透かし検査部１９０７は、モジュール結合部１９０５で生成されたプログラムの透かしと端末情報入力部１９０８により入力された端末ＩＤとが一致する場合には、プログラムをプログラム出力部１９０９に出力し、一致しない場合には生成したプログラムを破棄する。
【０１６６】
プログラム出力部１９０９は、すべての検査を通過したプログラムを出力する手段である。
【０１６７】
この構成により、受信モジュール検査部１９０は、本体モジュールの署名値とダミーモジュールの署名値を用いてプログラムが正式か否かを判断する。また、受信モジュール検査部１９０は、透かしを用いてもプログラムが正式か否かを判断する。
【０１６８】
なお、プログラム配信装置７０からプログラム利用装置１５０に、検査プログラムがプログラムに一体となって付加された状態で送れてくる形態であっても良い。
【０１６９】
図１２に透かしの検査プログラムが一体となって付加されたプログラム例２００１を示す。
【０１７０】
この場合の受信モジュール検査部を図１３に示す。この場合の受信モジュール検査部２３０には、検査プログラム入力部１９０６と端末情報入力部１９０８が無い構成になっている。
【０１７１】
実行部２１０でプログラムが実行されると、検査プログラム２００２が最初に実行され、本体プログラム２００３に挿入された透かしの抽出と端末ＩＤとの比較が行われ、透かしと端末ＩＤが一致した場合に、本体プログラム２００３の実行が開始される。
【０１７２】
このようにして、透かしの検査プログラムが付加されているプログラムを動作させることができる。
【０１７３】
次に、製作者のプログラム製作装置１０で作成されたプログラムが販売者のプログラム配信装置７０に送信されて、さらに利用者のプログラム利用装置１５０にダウンロードされるときの動作を図１４～図１６を用いて説明する。
【０１７４】
図１４は、実施の形態１におけるプログラム製作装置１０の動作を示すフローチャートである。
【０１７５】
まず、プログラム製作装置１０は、作成してあったＮ－１個のモジュールからなるプログラムを入力し、蓄積部２０に保存する（ステップ１４０１）。
【０１７６】
次に、プログラム製作装置１０は、プログラム構造変換部３０のプログラム入力部３０１が、蓄積部２０に保存しておいたプログラムを入力する。次に、プログラム構造変換部３０のダミーモジュール追加部３０５が、ダミーモジュール入力部３０３から販売者が利用者ＩＤを挿入するためのダミーモジュールを入力する。そして、ダミーモジュール追加部３０５が、入力したダミーモジュールを１個、ステップ１４０１において保存してお

たプログラムに追加する（ステップ１４０２）。また、ダミーモジュール追加部３０５は、追加したダミーモジュール名をダミー情報記憶部３０４に渡す。

【０１７７】

その後、プログラム構造変換部３０は、プログラム分割部３０２において、ステップ１４０２においてダミーモジュールを追加したプログラムを、ダミーモジュールを含むＮ個のモジュールに分割する（ステップ１４０３）。また、プログラム分割部３０２は、モジュールの分割数を分割情報記憶部３０６に出力する。

【０１７８】

そして、プログラム出力部３０７が、ステップ１４０３において、分割したモジュールを透かし挿入部４０に出力する。

【０１７９】

次に、透かし挿入部４０は、プログラム入力部４０１において、プログラム構造変換部３０から出力されたモジュールを入力する。

【０１８０】

次に、透かし挿入部４０は、挿入部４０２において、モジュール情報記憶部４０８を参照し、ダミーモジュールに関する情報を取得する。次に、挿入部４０２は、取得したダミーモジュールに関する情報を用いて、モジュールの番号ｉが１のモジュールから（ステップ１４０４）、Ｎのモジュールまで（ステップ１４０５）、つまりすべてのモジュールに対して、モジュールがダミーモジュールであるか判定を行う（ステップ１４０６）。

【０１８１】

そして、ステップ１４０６においてモジュールがダミーモジュールでないと判断すると、挿入部４０２は、ＩＤ情報生成部４０４が生成した販売者ＩＤから透かしを生成し、モジュールに挿入する（ステップ１４０７）。また、挿入部４０２は、透かしを挿入したモジュール名を透かし情報記憶部４０５に出力する。

【０１８２】

そして、プログラム製作装置１０は、ｉをインクリメントして（ステップ１４０８）、ステップ１４０５に戻る。

【０１８３】

また、ステップ１４０６においてモジュールがダミーモジュールであると判断した場合は、モジュールに対して透かし挿入部４０による透かし挿入は行わずに、プログラム出力部４０６を介して、署名部５０に送る。そして、プログラム製作装置１０は、ｉをインクリメントして（ステップ１４０８）、ステップ１４０５に戻る。

【０１８４】

そして、すべてのモジュールに上記の処理を行ったら（ステップ１４０５）、挿入部４０２は、透かしを挿入したモジュール（本体モジュール）をプログラム出力部４０６に出力し、プログラム出力部４０６が署名部５０に送る。

【０１８５】

そして、署名部５０は、プログラム入力部５０１より透かしを挿入したモジュールを入力し、署名付与部５０２に送る。

【０１８６】

署名付与部５０２は、透かしを挿入したモジュール（本体モジュール）のハッシュ値を計算し、これを電子署名として付与する（ステップ１４０９）。

【０１８７】

次に、署名付与部５０２は、署名用鍵入力部５０３より秘密鍵を入力し、付与したハッシュ値を暗号化する。

【０１８８】

次に、署名付与部５０２は、署名および透かしが付与されたモジュール（本体モジュール）を、プログラム出力部５０６を介して、送信部６０に送る。

【０１８９】

最後に送信部６０がプログラム入力部６０１からモジュールを入力し、送信データパッ

ケージ化部６０２が、販売者向けパッケージの作成を行い、暗号化部６０７に送る。

【０１９０】

次に、暗号化部６０７が、プログラム製作装置１０とプログラム配信装置７０との間でパッケージをやりとりするために使用される暗号鍵を用いてパッケージの暗号化と（ステップ１４１０）、検査プログラム入力部６０８から入力された検査プログラムの暗号化を行う（ステップ１４１１）。そして、プログラム送信部６０６は、販売者に販売者向けパッケージ７００および検査プログラム７０８を送信する（ステップ１４１２）。

【０１９１】

また、販売者向けパッケージ７００には、Ｎ－１個の本体モジュール７０１と、１個のダミーモジュール７０２、Ｎ－１個の本体モジュール７０１に対応する署名値７０３、暗号化した署名値を復号化するための公開鍵７０４、ダミーモジュール名７０５、販売者がダミーモジュールに署名するための秘密鍵７０６と対応する公開鍵７０７、インストールプログラム７０９を入れる。

【０１９２】

なお、公開鍵を伝送路から別途入手できる場合には、証明書は必ずしも送らなくてもよい。

【０１９３】

また、署名と各モジュールは、ＸＭＬ署名などのフォーマット（署名フォーマット）などを用いて対応付けを行う。ＸＭＬ署名とは、署名対象、署名アルゴリズムや署名値および証明書などをＸＭＬの文法で統一して表現できるものである。

【０１９４】

このように、プログラム製作装置１０は、販売者が自由に使えるダミーモジュールと、透かしおよび電子署名を挿入した本体モジュールと、をパッケージ化した販売者向けパッケージを販売者に送信する。

【０１９５】

これにより、販売者は、ダミーモジュールに利用者を特定するＩＤなどを挿入することができる。

【０１９６】

また、本体モジュールには、電子署名が付与されているので、販売者は本体モジュールを改竄することができない。

【０１９７】

また、販売者向けパッケージ７００を、プログラム製作装置１０とプログラム配布装置７０との間で決めた暗号鍵により暗号化するので、正規の販売者以外が販売者パッケージ７００を改竄することも防げる。

【０１９８】

次に、販売者側のプログラム配信装置７０で行われる動作について図１５を用いて説明する。図１５は、販売者側のプログラム配信装置７０の動作に関するフローチャートである。

【０１９９】

プログラム配信装置７０は、受信部９０において、製作者のプログラム製作装置１０から送られた販売者向けパッケージを受けとり、復号化して蓄積部１１０に保存する（ステップ１５０１）。

【０２００】

次に、プログラム配信装置７０は、要求受信部１００により、利用者からダウンロードの要求を受け付け、受け付けた要求がパッケージに対するダウンロード要求かを判断する（ステップ１５０２）。

【０２０１】

要求がパッケージに対するダウンロード要求でなければ、検査プログラムに対する要求であるので、送信部１４０は、暗号化部１４０７において、暗号鍵生成部１４０５で生成された、プログラム配信装置７０とプログラム利用装置１５０の間でパッケージをやりと

りするために使用される暗号鍵を用いて、検査プログラムを暗号化して、プログラム送信部１４０６から利用者のプログラム利用装置１５０に送信する（ステップ１５１２）。

【０２０２】

一方、ステップ１５０２において、要求がパッケージに対する要求であれば、まず、透かし挿入部１２０のプログラム入力部１２０１が蓄積部１１０から販売者パッケージを入力する。次に、透かし挿入部１２０の挿入部１２０２が入力した、販売者パッケージのパッケージ化を解きＮ個のモジュールを取り出す（ステップ１５０３）。

【０２０３】

次に、挿入部１２０２は、モジュール情報記憶部１２０８を参照し、ダミーモジュールに関する情報を取り出す。そして、挿入部１２０２は、取り出したダミーモジュールに関する情報を用いて、取り出したＮ個のモジュールについて、モジュール番号ｉが１から（ステップ１５０４）、Ｎまで変化させ（ステップ１５０５）、各モジュールがダミーモジュールであるか検査を行う（ステップ１５０６）。

【０２０４】

そして、モジュールがダミーモジュールである場合には、挿入部１２０２は、ＩＤ情報生成部１２０４から利用者ＩＤを取り出し、ダミーモジュールに利用者ＩＤを用いた透かしを挿入する（ステップ１５０７）。そして、挿入部１２０２は、透かしを挿入したモジュールをプログラム出力部１２０６に送り、プログラム出力部１２０６が署名部１３０に送る。

【０２０５】

また、挿入部１２０２は、透かしを挿入したモジュール名を透かし情報記憶部１２０５に出力する。

【０２０６】

次に、署名部１３０は、送られてきたモジュールをプログラム入力部１３０１において入力する。次に、署名部１３０は、署名付与部１３０２において、ダミーモジュールのハッシュ値を計算する。次に、署名付与部１３０２は、計算したハッシュ値を、署名用鍵入力部１３０３から入力した、プログラム製作装置１０から送られてきた販売者向けパッケージ７００のダミーモジュールに署名するための秘密鍵（製作者秘密鍵）７０６を用いて暗号化する。次に、署名付与部１３０２は、暗号化した電子署名をダミーモジュールにつけ、プログラム出力部１３０６に送る（ステップ１５０８）。そして、プログラム出力部１３０６は、電子署名をつけたダミーモジュールを送信部１４０に送る。

【０２０７】

最後に、プログラム配信装置７０は、ｉをインクリメントして（ステップ１５０９）、ステップ１５０５に戻る。

【０２０８】

また、ステップ１５０６において、モジュールがダミーモジュールでない場合には、プログラム配信装置７０は、利用者ＩＤの挿入と署名は行わず、送信部１４０に送り、ｉをインクリメントしてステップ１５０５に戻る。

【０２０９】

そして、プログラム配信装置７０は、すべてのモジュールについて上記の処理を行う。

【０２１０】

次に、送信部１４０は、プログラム入力部１４０１において、プログラム出力部１３０６より送られたモジュールを入力し、送信データパッケージ化部１４０２に送る。

【０２１１】

送信データパッケージ化部１４０２は、利用者向けパッケージを作成し、暗号化部１４０７に送る。

【０２１２】

暗号化部１４０７は、暗号鍵生成部１４０５により生成された通信用の暗号鍵を用いて、パッケージ化された利用者向けパッケージ１０００を暗号化して（ステップ１５１０）、プログラム送信部１４０６に送る。そして、プログラム送信部１４０６は、暗号化した

パッケージをプログラム利用装置１５０に送信する（ステップ１５１１）。
【０２１３】
また、暗号化部１４０７は、利用者向けパッケージ１０００に、Ｎ－１個の本体モジュール７０１と、１個のダミーモジュール７０２と、Ｎ－１個の本体モジュールの署名値（ハッシュ値）７０３と、ダミーモジュールの署名値１００４、本体モジュールの署名値７０３の公開鍵７０４と、ダミーモジュールの署名値１００４に使用する公開鍵７０７と、インストールプログラム７０９を入れる。
【０２１４】
なお、公開鍵が伝送路から別途入手できる場合には、鍵の証明書は必ずしも送らなくてもよい。
【０２１５】
また、ダミーモジュールと署名の対応付けは、販売者向けパッケージと同じように、署名フォーマットを利用して行う。
【０２１６】
このように、プログラム配布装置７０は、ダミーモジュールに利用者を特定するＩＤなどを挿入することができる。これにより、利用者が、プログラムの不正利用を防止できる。
【０２１７】
また、ダミーモジュールには、電子署名が付与されているので、ダミーモジュールを改竄することができない。さらに、ダミーモジュールに付与された電子署名は、製作者の秘密鍵を用いて暗号化されているので、利用者は復号化に使用される公開鍵の違いに基づいて自身のＩＤの挿入されているダミーモジュールを特定できなくなる。この結果、利用者が、ダミーモジュールを改竄することを確実に防止できる。
【０２１８】
また、利用者向けパッケージ１０００を、プログラム配布装置７０とプログラム利用装置１５０との間で決めた暗号鍵により暗号化するので、正規の利用者以外が利用者パッケージ１０００を改竄することも防げる。
【０２１９】
次に、利用者１１０で行われる動作について、図１６を用いて説明する。図１６は、プログラム利用装置１５０の動作に関するフローチャートである。
【０２２０】
まず、プログラム利用装置１５０は、要求送信部１６０により、プログラムの送信要求と自分の端末ＩＤを販売者に送信する（ステップ１６０１）。
【０２２１】
そして、プログラム利用装置１５０は、受信部１７０により、プログラム配信装置７０から送られた利用者向けパッケージを受信し、復号化して蓄積部１８０に保存する（ステップ１６０２）。
【０２２２】
次に、受信モジュール検査部１９０が、プログラム入力部１９０１において、蓄積部１８０に蓄積されたパッケージを入力する。
【０２２３】
次に、受信モジュール検査部１９０は、受信パッケージ検査部１９０２において、パッケージ情報記憶部１９０３よりパッケージのサイズもしくはＣＲＣサイズを取得する。そして、受信パッケージ検査部１９０２は、パッケージ情報記憶部１９０３から取得したパッケージのサイズもしくはＣＲＣサイズと、受信したパッケージのサイズが一致しているか検査することにより、入力したパッケージがパケットロスなどにより不完全なデータとなっていないかを検査する（ステップ１６０３）。
【０２２４】
そして、ステップ１６０３において受信したパッケージが不完全なデータであった場合には、受信パッケージ検査部１９０２は、利用者に対してエラー表示を行い（ステップ１

６１５）、受信したパッケージを破棄する（ステップ１６１６）。
【０２２５】
一方、そして、ステップ１６０３において完全なデータが受信されていれば、受信パッケージ検査部１９０２は、受信したパッケージのパッケージ化を解きＮ個のモジュールを取り出す（ステップ１６０４）。そして、受信パッケージ検査部１９０２は、Ｎ個のモジュールを署名検査部１９０４に送る。
【０２２６】
次に、署名検査部１９０４は、Ｎ個のモジュールを取り出し、各モジュールについて番号ｉが１から（ステップ１６０５）、Ｎまで（ステップ１６０６）、モジュールの電子署名を計算する（ステップ１６０７）。次に、署名検査部１９０４は、各モジュールに付与されている電子署名を、利用者パッケージ１０００に付与されている公開鍵７０４、７０７を用いて復号化する。そして、署名検査部１９０４は、各モジュールに付与されている電子署名と計算した電子署名を比較することで、各モジュールが正規のものか検査する（ステップ１６０８）。
【０２２７】
署名が正しい場合には、署名検査部１９０４は、モジュールをモジュール結合部１９０５に送る。そして、検査部１９０４は、ｉをインクリメントして（ステップ１６０９）、ステップ１６０６に戻る。
【０２２８】
また、署名が正しくなかった場合には、署名検査部１９０４は、エラーの表示を行い（ステップ１６１５）、受信したパッケージを破棄する（ステップ１６１６）。
【０２２９】
次に、モジュール結合部１９０５は、署名の検査をすべてのモジュールが通過したら、モジュールを結合してプログラムを生成する（ステップ１６１０）。モジュール結合部１９０５は、プログラムを生成したら、プログラムを透かし検査部１９０７に送る。
【０２３０】
透かし検査部１９０７は、透かしの検査プログラムをプログラム配信装置７０に要求し、検査プログラム入力部１９０６において受信する（ステップ１６１１）。
【０２３１】
透かし検査部１９０７は、受信した検査プログラムを用いて生成したプログラムの透かしを抽出し（ステップ１６１２）、端末情報入力部１９０８から入力した端末ＩＤと一致するかを検査する（ステップ１６１３）。
【０２３２】
そして、透かしと端末ＩＤが一致したら、透かし検査部１９０７は、プログラムを、プログラム出力部１９０９を介して、一度蓄積部２００に保存する。
【０２３３】
そして、実行部２１０は、蓄積部２００に蓄積したプログラムに対して、インストールプログラム１００２を用いることで、プログラムをインストールし、実行する（ステップ１６１４）。
【０２３４】
一方、ＩＤが一致しなかった場合には、プログラムを保存せずに、エラー表示を行い（ステップ１６１５）、受信したパッケージを破棄する（ステップ１６１６）。
【０２３５】
このように、プログラム利用装置１５０は、モジュールに付与された電子署名と計算した電子署名とを比較することにより、受信したプログラムの正当性を判断できる。
【０２３６】
また、プログラム利用装置１５０は、ダミーモジュールに挿入された透かしと、自身のＩＤ情報を比較することにより、受信したプログラムの正当性を判断できる。
【０２３７】
また、プログラム利用装置１５０は、利用者向けパッケージ１０００から本体モジュー

ルの署名値の公開鍵７０４と、ダミーモジュールの署名値の公開鍵７０７を取得し、これらを用いて署名値を復号できる。また、正規の製作者の秘密鍵を用いず暗号化された署名値は復号化できないので、これにより、違法なプログラムを認識することもできる。

【０２３８】

次に、プログラムが不正流出した場合に、流出先を特定する構造について、図１７を用いて説明する。

【０２３９】

図１７に示すように、プログラムが不正流出した際には、製作者は透かし取り出し装置２２０を用いて、流出先端末１７０１に流出したプログラムから透かしを抽出し、流出元の販売者のプログラム配信装置７０を特定することが可能となる。

【０２４０】

次に、実施の形態１にかかる透かし取り出し装置２２０について図１８を用いて説明する。図１８は、実施の形態１における透かし取り出し装置２２０の構成図である。

【０２４１】

プログラム入力部２２０１は、透かしが挿入されたプログラムを入力する手段である。プログラム入力部２２０１は、プログラムを透かし検出部２２０２に出力する。

【０２４２】

ＩＤ情報記憶部２２０４は、透かし検出部２２０２より得られるＩＤ情報から、配布先の情報を生成する手段である。

【０２４３】

ＩＤ情報記憶部２２０４は、ＩＤ情報がデータベースのデータのＩＤである場合には、ＩＤからデータを取り出すことで、配布先の情報を取得する。また、ＩＤ情報記憶部２２０４は、ＩＤ情報が配布先の情報の暗号化データである場合には、復号して配布先の情報を取得する。

【０２４４】

透かし情報記憶部２２０５は、透かしが挿入されているモジュール名を記憶している手段である。これらの情報は、透かし挿入部４０の透かし情報記憶部４０５より得る。

【０２４５】

透かし検出部２２０２は、透かし情報記憶部２２０５より得られるモジュール名からそのモジュールに挿入された透かしを抽出する。そして、透かし検出部２２０２は、取り出した透かしからＩＤ情報を生成し、出力部２２０３に渡す。

【０２４６】

出力部２２０３は、ＩＤ情報記憶部２２０４を参照し、透かし検出部２２０２が生成した、ＩＤ情報から配布先の情報を抽出し、出力する手段である。

【０２４７】

このようにして、透かし取り出し装置２２０は、不正にプログラムを配布した配布元の情報を出力する。

【０２４８】

なお、本発明は、プログラム利用装置１５０が受信するプログラムに透かしの検査プログラムが付加されている場合も動作可能である。

【０２４９】

その場合、異なるのは送信部６０および受信モジュール検査部１９０の動作である。

【０２５０】

送信部６０では、検査プログラム入力部６０９による透かしの検査プログラムの入力は行われない。また、受信モジュール検査部１９０では、検査プログラム入力部１９０１、端末情報入力部１９０８および透かし検査部１９０７の動作は行われない。

【０２５１】

次に、実施の形態１により生成されるプログラムについて図２１を用いて説明する。

【０２５２】

図２１において、プログラム２９００ａは、蓄積部２０に保存されている基本プログラ

ムである。また、プログラム２９００ｂは、基本プログラム２９００ａに販売者の透かし情報及びダミーメソッドを追加したプログラムである。プログラム２９００ｃは、基本プログラム２９００ａをコンパイルしたプログラムで、２９００ｄは、２９００ｃに利用者の透かし情報を挿入したプログラムを示している。

【０２５３】

まず、プログラム製作装置１０において、プログラム構造変換部３０のダミーモジュール追加部３０５が、ステップ１４０２でダミーメソッドをプログラム２９００ａに追加する（図中２９０１に示す部分）。また、このとき、ａｓｓｅｒｔ法などを用いてダミーメソッドの呼び出し文をプログラム２９００ａに追加する（図中２９０２に示す部分）。

【０２５４】

次に、透かし挿入部４０の挿入部４０２が、ステップ１４０６において、それぞれのメソッドがダミーメソッドであるかを判断し、ダミーメソッドでない場合には、販売者のＩＤ情報（１１２２）より生成された透かし情報Ｓ１（１１）及びＳ２（２２）を挿入する（図中２９０３に示す部分）。そして、販売者の透かし情報を挿入した後で、ステップ１４０９において、プログラムをコンパイルし、ダミーメソッド以外の部分を用いて電子署名を付与する。なお、ここでは簡単のために、コンパイルしたあとのプログラムを逆アセンブルしたものを用いて説明する。

【０２５５】

次に、プログラム配信装置７０において、透かし挿入部１２０の挿入部１２０２が、ステップ１５０６で、それぞれのメソッドがダミーメソッドであるかを判断し、ダミーメソッドの場合には、利用者のＩＤ情報（（Ｃ）１１）より生成した透かし情報Ｕ１（１００１１１　００１１０１　１０１０００　００１０１１）を挿入し（図中２９０４に示す部分）、ステップ１５０８において、ダミーメソッドに対して電子署名を付与する。

【０２５６】

次に、プログラム利用装置１５０において、受信モジュール検査部１９０の署名検査部１９０４が、ステップ１６０７で、プログラム製作装置１０より配布されたインストールプログラムを用いて、プログラム２９００ｄに付与された電子署名を検証する。また、受信モジュール検査部１９０の透かし検査部１９０７が、ステップ１６１２で、プログラム製作装置１０より配布された検査プログラムを用いてダミーメソッドＭ２より透かしを抽出し、ステップ１６１３で端末ＩＤと比較する。ステップ１６０７とステップ１６１３の検証に通過した場合に、プログラム利用装置７０は、プログラム２９００ｄをインストールして実行する。

【０２５７】

なお、この例ではダミーモジュールとしてメソッドを追加した場合について説明したが、クラスを追加した場合にも適用可能である。

【０２５８】

以上説明したように、実施の形態１によれば、本体モジュールとは別にダミーモジュールを追加することにより、販売者がダミーモジュールに利用者ＩＤを挿入することができる。また、本体モジュールに署名を付与することで、販売者にプログラムの根幹にかかわる重要な部分である本体モジュールを操作させることを防止できる。これにより、販売者によるプログラムの改竄を防止することができる。

【０２５９】

さらに、実施の形態１によれば、本体モジュールに付与された電子署名は、製作者の本体モジュール用の秘密鍵を用いて暗号化されていて、かつ販売者は本体モジュール用の製作者の秘密鍵持っていない。これにより、仮に販売者が電子署名を公開鍵７０４で復号し改竄したとしても、製作者の秘密鍵で再度暗号化できない。よって、利用者が、本体モジュールの復号化をできない。この結果、販売者が、本体モジュールを改竄することを確実に防止できる。

【０２６０】

また、実施の形態１によれば、仮にプログラムの不正流出があった場合でも、本体モジ

ュールに販売者ＩＤが挿入されているため、流出元となった販売者を特定することができる。これにより、販売者によるプログラムの改竄を防止できる。

【０２６１】

また、実施の形態１によれば、プログラム部分を複数の本体モジュールに分割するので、ダミーモジュールを含めた全モジュール数が増加することになり、利用者は自身のＩＤの挿入されているダミーモジュールを多数のモジュールから特定することになるため非常に困難となる。また、モジュールとダミーモジュールとのサイズの差が小さくなり、利用者はモジュールのサイズに基づいて自身のＩＤの挿入されているダミーモジュールを特定できなくなる。したがって、利用者によるプログラムの改竄を防止することができる。

【０２６２】

また、実施の形態１によれば、販売者向けパッケージ７００にダミーモジュールの署名用の秘密鍵を送ることにより、販売者がダミーモジュールに、製作者の秘密鍵を使用して電子署名を付与することが可能となる。販売者が自分自身の秘密鍵でダミーモジュールに電子署名を付与した場合には、本体モジュール用の秘密鍵とダミーモジュール用に用いる秘密鍵の証明書の発行先が異なる。このために、利用者にダミーモジュールの部分を容易に特定され、透かし挿入箇所を容易に特定されてしまう。しかし、実施の形態１では、利用者が署名の検査に使う証明書は、すべて製作者に対して発行されたものとなるため、証明書の発行先による透かし挿入箇所の特定が不可能となり、利用者による透かしの削除を防止することができる。

【０２６３】

なお、プログラム製作装置１０、プログラム配信装置７０、およびプログラム利用装置１５０の動作をプログラムにし、記憶媒体に格納し、汎用のコンピュータが記憶媒体からプログラムをダウンロードして実行させる形態であっても良い。

【０２６４】

（実施の形態２）

本発明の実施の形態２にかかるプログラム流通システムについて添付図面を用いて説明する。本発明の実施の形態２は、利用者が複数の販売者よりプログラムの別々のモジュールをダウンロードする場合に対応するものである。図１９は、実施の形態２にかかるプログラム流通システムの構成図である。

【０２６５】

実施の形態２におけるプログラム流通システムと実施の形態１の違いは、製作者が複数の販売者にプログラムを分割して送り、複数の販売者を経由してきた分割されたプログラムを利用者が受信する点である。

【０２６６】

具体的には、製作者側のプログラム製作装置１８０１は、実施の形態１のプログラム製作装置１０と、プログラム構造変換部１８０２と透かし挿入部１８０２の動作が違う。また、利用者側のプログラム利用装置１８０５は、実施の形態１のプログラム利用装置１５０と、受信モジュール検査部１８０４の動作が違う。

【０２６７】

次に、実施の形態２におけるプログラム構造変換部１８０２について説明する。実施の形態２におけるプログラム構造変換部１８０２と、実施の形態１におけるプログラム構造変換部３０との違いは、ダミーモジュール追加部３０５の動作である。

【０２６８】

実施の形態２におけるダミーモジュール追加部３０５は、ダミーモジュール入力部３０３より入力された２個のダミーモジュールをプログラムに追加する手段である。ダミーモジュール追加部３０５は、それぞれ異なる本体モジュールに呼び出されるようにａｓｓｅｒｔ法を用いてダミーモジュールを追加する。

【０２６９】

なお、プログラム構造変換部１８０２のダミーモジュール追加部３０５以外の動作は、実施の形態１におけるプログラム構造変換部３０と同じであるので、説明は省略する。

【０２７０】
次に、実施の形態２にかかる透かし挿入部１８０３について説明する。実施の形態２における透かし挿入部１８０３と、実施の形態１における透かし挿入部４０との違いは、挿入部４０２の動作である。
【０２７１】
実施の形態２における挿入部４０２は、ＩＤ情報生成部４０４により生成されるＩＤ情報からプログラムに実際に挿入する透かしを生成し、モジュール情報記憶部４０８より入力されるダミーモジュール名以外のモジュール（本体モジュール）の、一部に販売者Ａを特定するための販売者ＩＤを挿入し、別の一部には販売者Ｂを特定するための販売者ＩＤを挿入する手段である。
【０２７２】
なお、実施の形態２における透かし挿入部１８０３のその他の部分は、実施の形態１における透かし挿入部４０と同じであるので説明は省略する。
【０２７３】
次に、受信モジュール検査部１８０４について、説明する。
【０２７４】
受信モジュール検査部１８０４は、販売者Ａおよび販売者Ｂから受信したパッケージを検査し、販売者Ａおよび販売者Ｂのパッケージをそれぞれ解き、合計Ｎ個のプログラムを取り出す。
【０２７５】
次に、製作者のプログラム製作装置１８０１で作成されたプログラムが販売者Ａのプログラム配信装置７０ａおよび販売者Ｂのプログラム配信装置７０ｂに送信されて、さらに利用者のプログラム利用装置１５０にダウンロードされるときの動作について説明する。
【０２７６】
まず、プログラム製作装置１８０１の処理について図２０を用いて説明する。図２０は、実施の形態２におけるプログラム製作装置１８０１で行われる動作を示すフローチャートである。
【０２７７】
まず、プログラム製作装置１８０１は、Ｎ－２個のモジュールからなるプログラムを作成し蓄積部２０に保存する（ステップ２００１）。次に、プログラム構造変換部１８０２が、利用者ＩＤを挿入するためのダミーモジュールを２個プログラムに追加し（ステップ２００２）、その後、プログラムを、ダミーモジュールを含むＮ個のモジュールに分割する（ステップ２００３）。
【０２７８】
なお、図１９では、販売者が２つの場合を示しているが、３つ以上でもよく、その場合にはその販売者数に対応する数のダミーモジュールを追加する。
【０２７９】
次に、透かし挿入部１８０３が、モジュール番号ｉを１から（ステップ２００４）、ｊまで変化させ（ステップ２００５）、それぞれの番号のモジュールがダミーモジュールかどうか判断する（ステップ２００６）。
【０２８０】
ダミーモジュールでない場合には、透かし挿入部１８０３は、販売者Ａを特定する販売者ＩＤを挿入する（ステップ２００７）。次に、署名部５０が、販売者ＩＤを挿入したダミーモジュールに電子署名をつける（ステップ２００８）。そして、プログラム製作装置１８０１は、ｉをインクリメントして（ステップ２００９）、ステップ２００５に戻る。
【０２８１】
また、ステップ２００６で、ダミーモジュールであると判断したときは、プログラム製作装置１８０１は、透かし挿入と電子署名を行わず、ｉをインクリメントしてステップ２００５に戻る。
【０２８２】

次に、透かし挿入部１８０３が、ｉをｊ＋１からＮまで変化させ（ステップ２０１０）、それぞれがダミーモジュールかどうかの判断をする（ステップ２０１１）。

【０２８３】

そして、ダミーモジュールでない場合には、透かし挿入部１８０３が、販売者Ｂを特定するＩＤを挿入し（ステップ２０１２）、署名部５０により電子署名をつける（ステップ２０１３）。そして、プログラム製作装置１８０１は、ｉをインクリメントして（ステップ２０１４）、ステップ２０１０に戻る。

【０２８４】

また、ステップ２０１１でダミーモジュールであると判断した場合は、プログラム製作装置１８０１は、透かし挿入と電子署名は行わず、ｉをインクリメントしてステップ２０１０に戻る。

【０２８５】

最後に、送信部６０により、販売者Ａと販売者Ｂに送るモジュールをそれぞれパッケージ化し暗号化して（ステップ２０１５）、販売者Ａのプログラム配信装置７０ａおよび販売者Ｂのプログラム配信装置７０ｂに送信する（ステップ２０１６）。

【０２８６】

次に、実施の形態２におけるプログラム配信装置７０ａおよびプログラム配信装置７０ｂの動作について説明する。実施の形態２におけるプログラム配信装置７０ａおよびプログラム配信装置７０ｂの動作と、実施の形態１におけるプログラム配信装置７０の動作との違いは、ステップ１５０３とステップ１５０５の動作である。

【０２８７】

実施の形態１におけるステップ１５０３は、実施の形態２では、取り出すモジュール数が販売者Ａのプログラム配信装置７０ａではｊ個で、販売者Ｂのプログラム配信装置７０ｂではＮ－ｊ個となる。

【０２８８】

また、実施の形態１におけるステップ１５０５は、実施の形態２では、販売者Ａのプログラム配信装置７０ａがｉを１からｊまで変化させ、販売者Ｂのプログラム配信装置７０ｂはｉをｊ＋１からＮまで変化させる。

【０２８９】

なお、実施の形態１におけるステップ１５０３およびステップ１５０５以外の各ステップは、実施の形態２において同様の動作をするので、説明を省略する。

【０２９０】

次に、実施の形態２における利用者のプログラム利用装置１８０５の動作について説明する。実施の形態２におけるプログラム利用装置１８０５の動作と、実施の形態１におけるプログラム利用装置１５０の動作との違いは、実施の形態１におけるステップ１６０１からステップ１６０４までの動作である。

【０２９１】

実施の形態１におけるステップ１６０１は、実施の形態２においては、販売者Ａのプログラム配信装置７０ａおよび販売者Ｂのプログラム配信装置７０ｂに対して端末ＩＤを送信する。

【０２９２】

次に、実施の形態１におけるステップ１６０２は、実施の形態２では、販売者Ａのプログラム配信装置７０ａおよび販売者Ｂのプログラム配信装置７０ｂからパッケージを受信し、それぞれを復号化して保存する動作となる。

【０２９３】

次に、ステップ１６０３は、実施の形態２では、販売者Ａのプログラム配信装置７０ａおよび販売者Ｂのプログラム配信装置７０ｂから受信したパッケージを検査する動作となる。

【０２９４】

そして、ステップ１６０４は、販売者Ａのプログラム配信装置７０ａおよび販売者Ｂの

プログラム配信装置７０ｂのパッケージをそれぞれ解き、合計Ｎ個のプログラムを取り出す動作となる。

【０２９５】

実施の形態１におけるステップ１６０４以降の各ステップは、実施の形態２で同じ動作をするので説明を省略する。

【０２９６】

以上説明したように、実施の形態２によれば、販売者Ａおよび販売者Ｂにはプログラムの一部を送信することになり、販売者Ａおよび販売者Ｂが完全なプログラムを持つことができなくなる。これにより、販売者Ａおよび販売者Ｂが利用者を偽った不正流出を防止することができる。

【産業上の利用可能性】

【０２９７】

以上説明したように、本発明によれば、販売者にプログラムの本体モジュールを操作させることなく、利用者ＩＤを挿入することができ、販売者によるプログラムの改竄を防止することができる。また、透かし情報として販売者のＩＤを挿入することで、不正流用を抑止することが可能となる。本発明は、プログラムだけでなく動画や音声などのコンテンツの流通にも適用でき、その利用範囲は広い。

【図面の簡単な説明】

【０２９８】

【図１】本発明の実施の形態１にかかるプログラム流通システムの構成図

【図２】実施の形態１にかかるプログラム構造変換部の構成図

【図３】実施の形態１の透かし挿入部の構成図

【図４】実施の形態１における署名部の構成図

【図５】実施の形態１における送信部の構成図

【図６】実施の形態１にかかる販売者向けパッケージの構成図

【図７】実施の形態１の透かし挿入部の構成図

【図８】実施の形態１における署名部の構成図

【図９】実施の形態１における送信部の構成図

【図１０】実施の形態１にかかる利用者向けパッケージの構成図

【図１１】実施の形態１における受信モジュール検査部の構成図

【図１２】実施の形態１における透かしの検査プログラムが一体となって付加されたプログラム例を示す図

【図１３】実施の形態１における透かしの検査プログラムが一体となって付加されているときの受信モジュール検査部の構成図

【図１４】実施の形態１におけるプログラム製作装置の動作を示すフローチャート

【図１５】実施の形態１におけるプログラム配信装置の動作に関するフローチャート

【図１６】実施の形態１におけるプログラム利用装置の動作に関するフローチャート

【図１７】実施の形態１におけるプログラムが不正流出した場合に、流出先を特定する構造を説明するための図

【図１８】実施の形態１における透かし取り出し装置の構成図

【図１９】本発明の実施の形態２にかかるプログラム流通システムの構成図

【図２０】実施の形態２におけるプログラム製作装置で行われる動作を示すフローチャート

【図２１】実施の形態１により生成されるプログラムを説明するための図

【符号の説明】

【０２９９】

１０、１８０１　プログラム製作装置

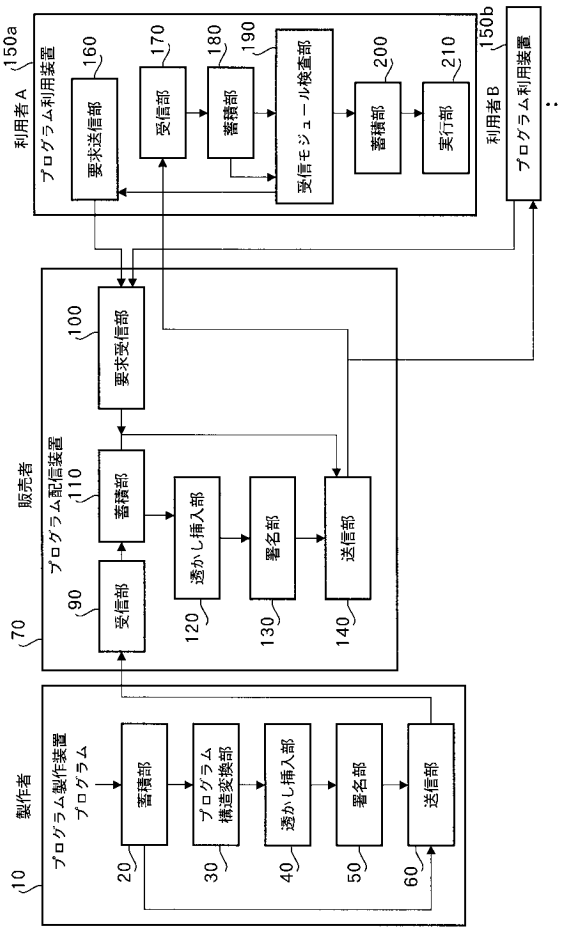
２０、１１０、１１０ａ、１１０ｂ、１８０、２００　蓄積部

３０、１８０２　プログラム構造変換部

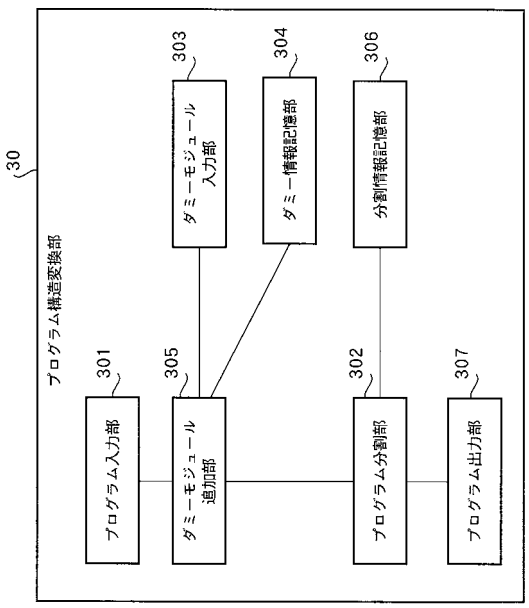
４０、１２０、１２０ａ、１２０ｂ、１８０３　透かし挿入部

５０、１３０、１３０ａ、１３０ｂ　署名部
６０、１４０、１４０ａ、１４０ｂ　送信部
７０、７０ａ、７０ｂ　プログラム配信装置
９０、９０ａ、９０ｂ、１７０　受信部
１００、１００ａ、１００ｂ　要求受信部
１５０ａ、１５０ｂ、１８０５　プログラム利用装置
１６０　要求送信部
１９０、１８０４　受信モジュール検査部
２１０　実行部

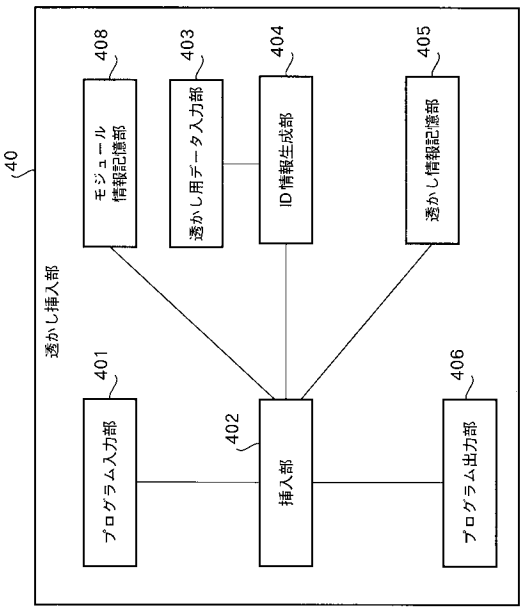
【図１】



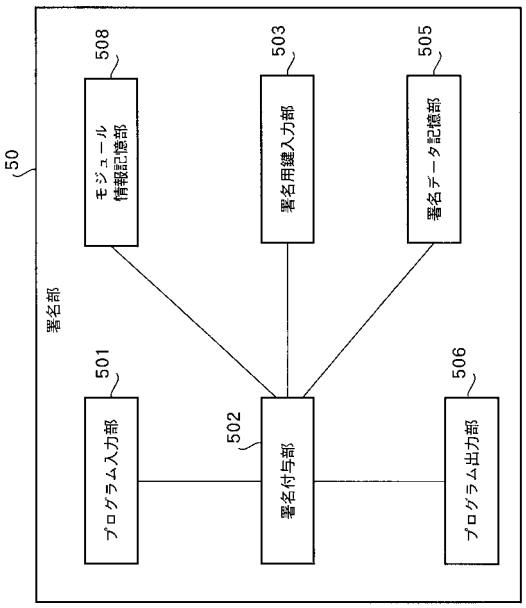
【図２】



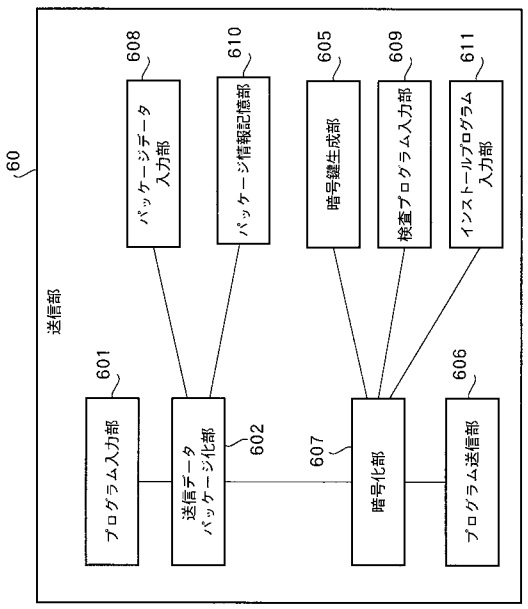
【図３】


40
透かし挿入部
408
モジュール情報記憶部
403
透かし用データ入力部
404
ID情報生成部
405
透かし情報記憶部
401
プログラム入力部
402
挿入部
406
プログラム出力部

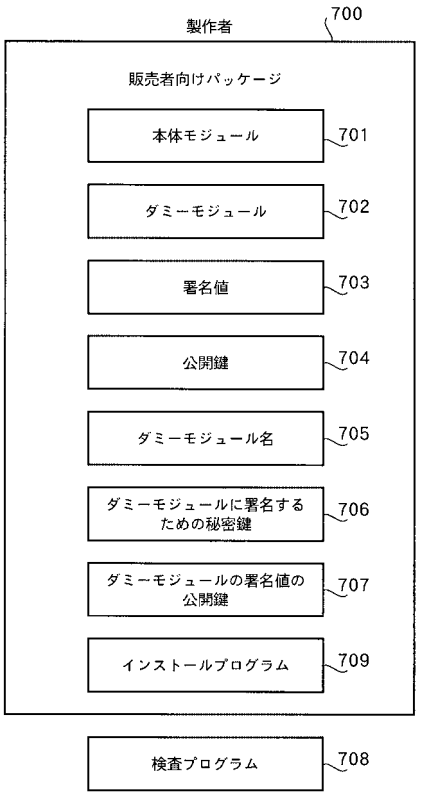
【図４】


50
署名部
508
モジュール情報記憶部
503
署名用鍵入力部
505
署名データ記憶部
501
プログラム入力部
502
署名付与部
506
プログラム出力部

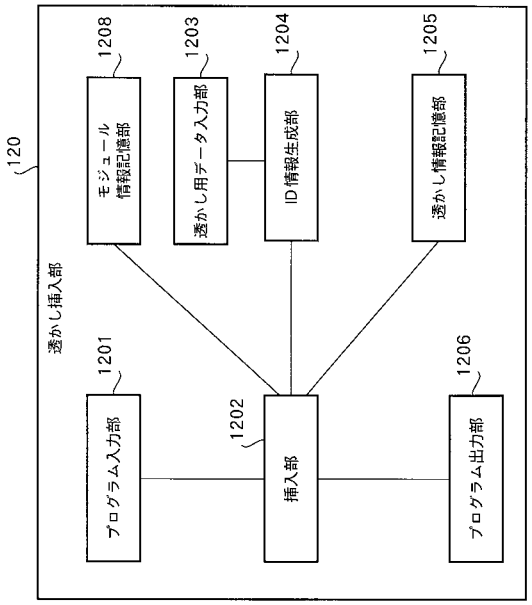
【図５】


60
送信部
608
パッケージデータ入力部
610
パッケージ情報記憶部
605
暗号鍵生成部
609
検査プログラム入力部
611
インストールプログラム入力部
601
プログラム入力部
602
送信データパッケージ化部
607
暗号化部
606
プログラム送信部

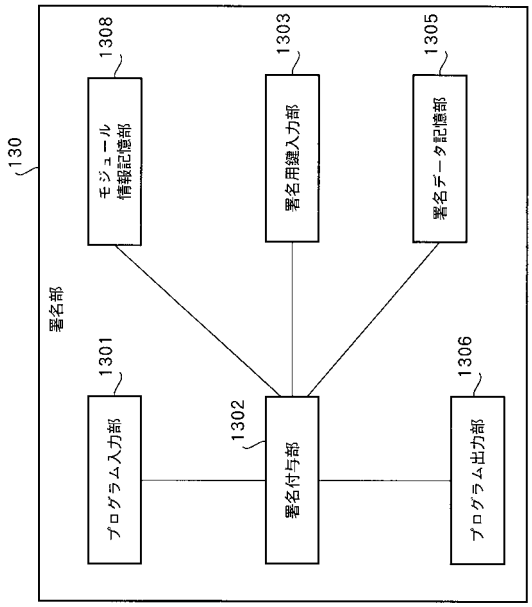
【図６】


製作者
700
販売者向けパッケージ
本体モジュール
701
ダミーモジュール
702
署名値
703
公開鍵
704
ダミーモジュール名
705
ダミーモジュールに署名するための秘密鍵
706
ダミーモジュールの署名値の公開鍵
707
インストールプログラム
709
検査プログラム
708

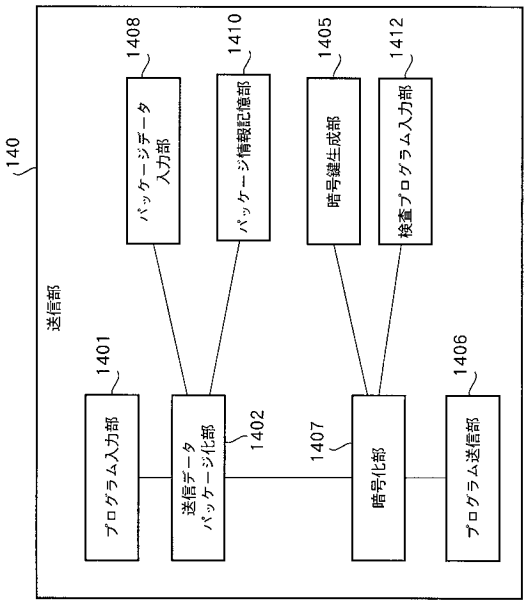
【図７】


120
透かし挿入部
1208
モジュール情報記憶部
1203
透かし用データ入力部
1204
ID情報生成部
1205
透かし情報記憶部
1201
プログラム入力部
1202
挿入部
1206
プログラム出力部

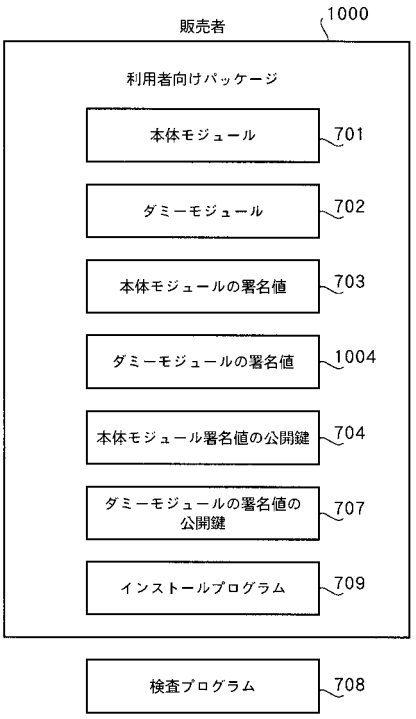
【図８】


130
署名部
1308
モジュール情報記憶部
1303
署名用鍵入力部
1305
署名データ記憶部
1301
プログラム入力部
1302
署名付与部
1306
プログラム出力部

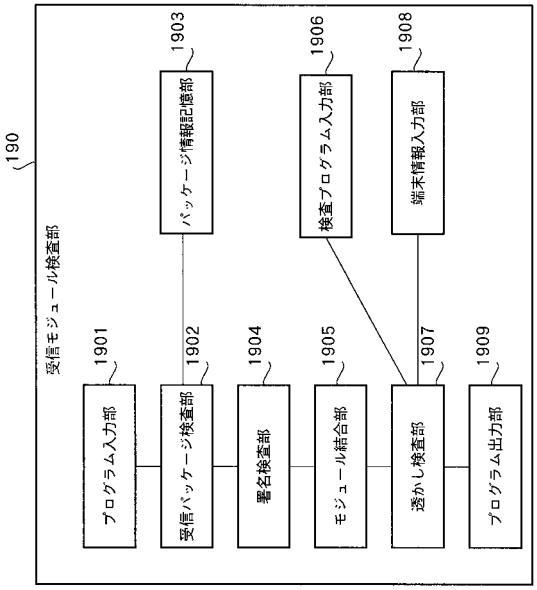
【図９】


140
送信部
1408
パッケージデータ入力部
1410
パッケージ情報記憶部
1405
暗号鍵生成部
1412
検査プログラム入力部
1401
プログラム入力部
送信データパッケージ化部
1402
1407
暗号化部
1406
プログラム送信部

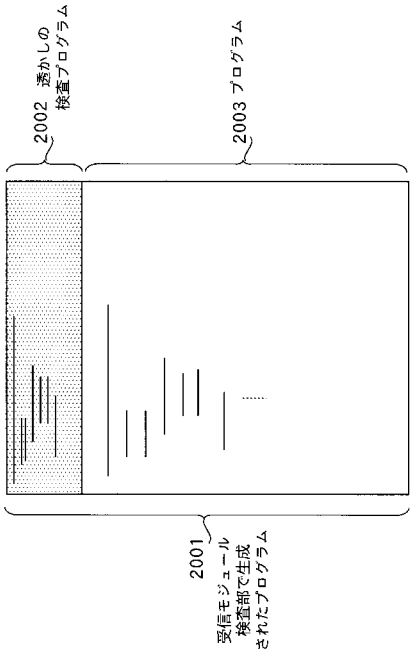
【図１０】


販売者
1000
利用者向けパッケージ
本体モジュール
701
ダミーモジュール
702
本体モジュールの署名値
703
ダミーモジュールの署名値
1004
本体モジュール署名値の公開鍵
704
ダミーモジュールの署名値の公開鍵
707
インストールプログラム
709
検査プログラム
708

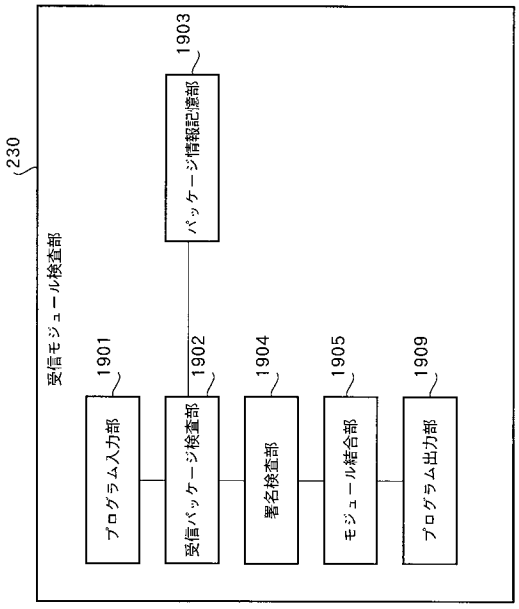
【図１１】



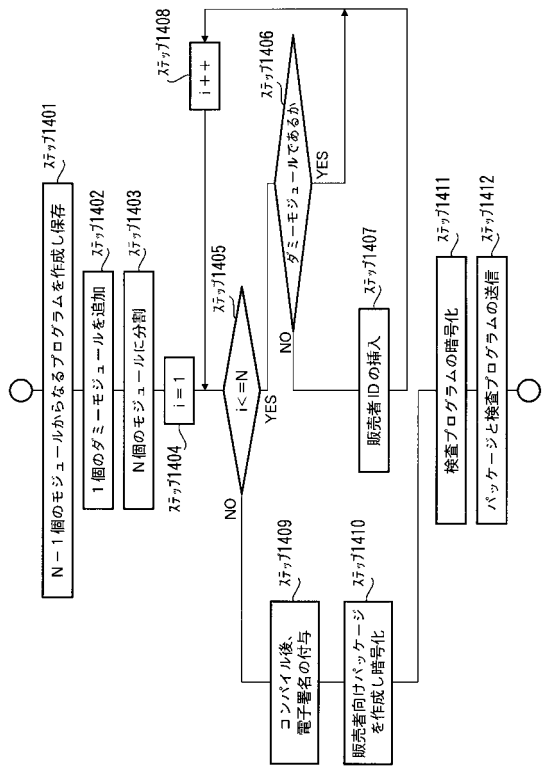
【図１２】



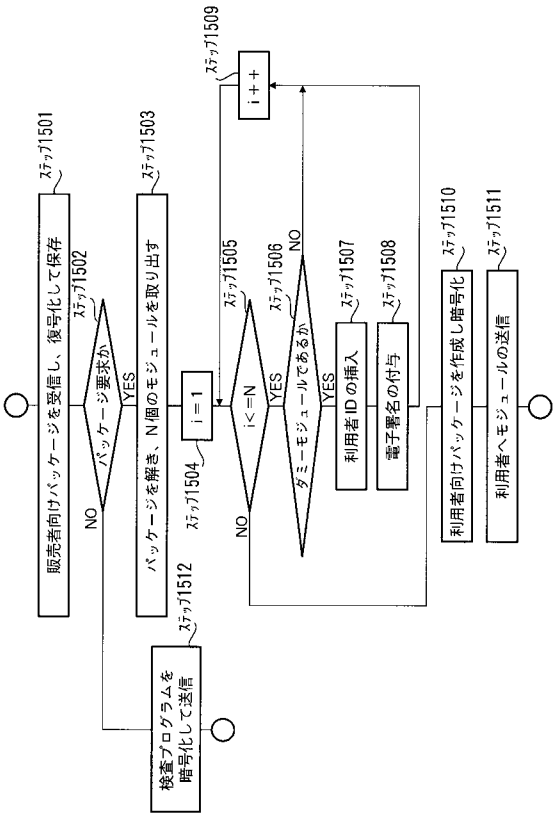
【図１３】



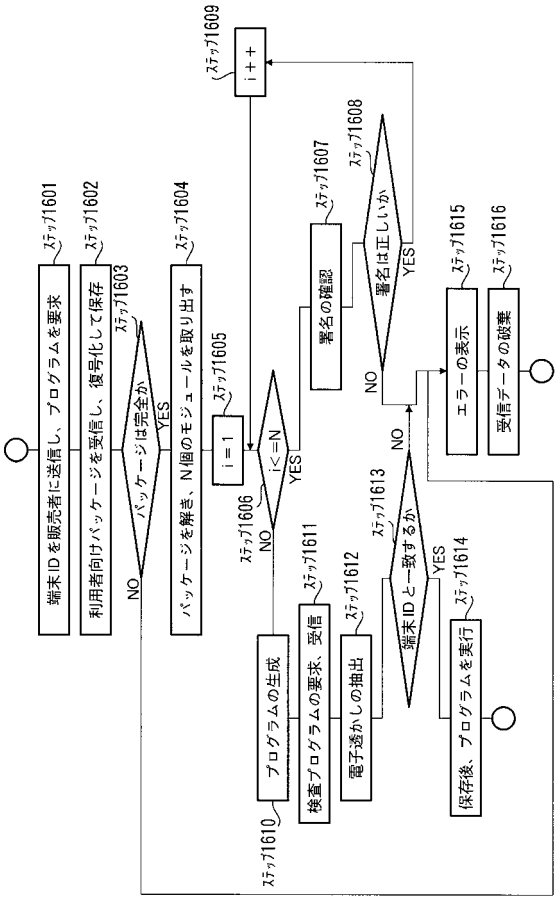
【図１４】



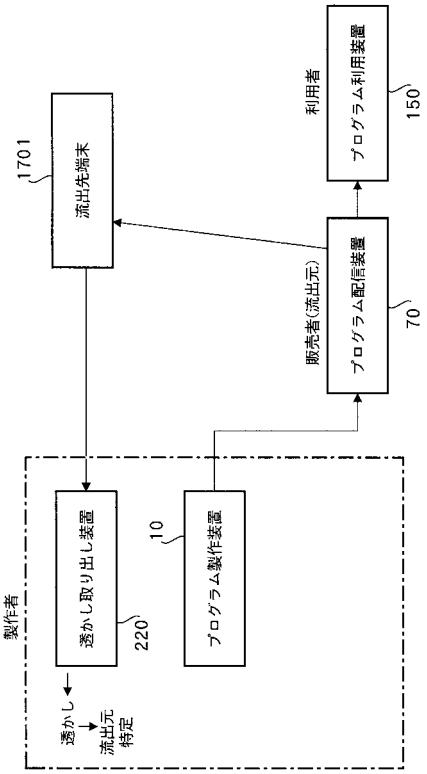
【図１５】



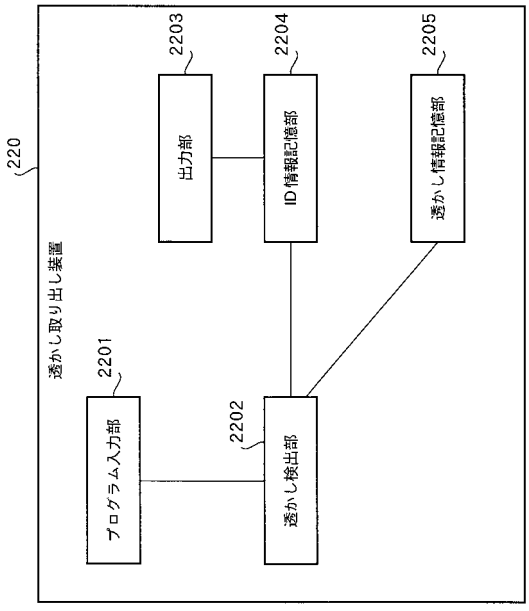
【図１６】



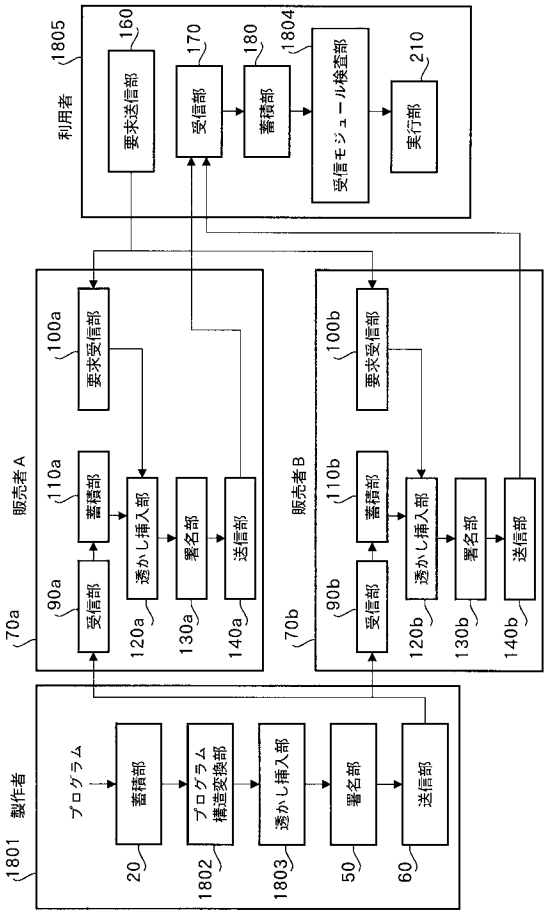
【図１７】



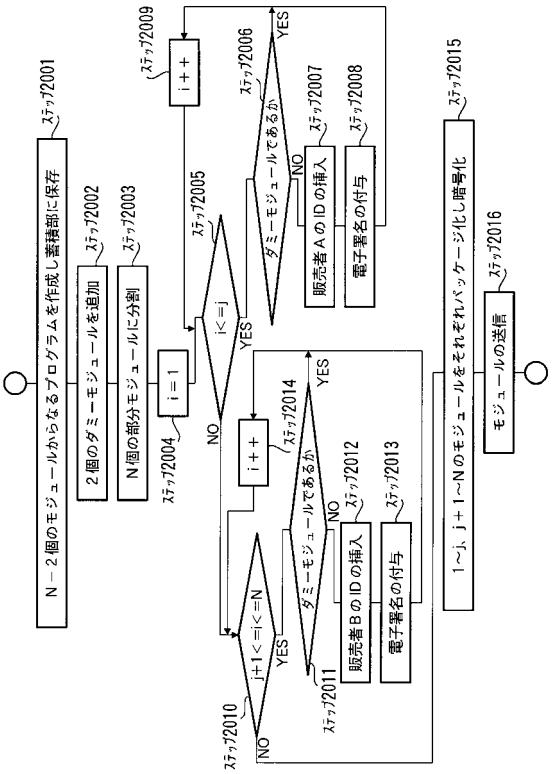
【図１８】



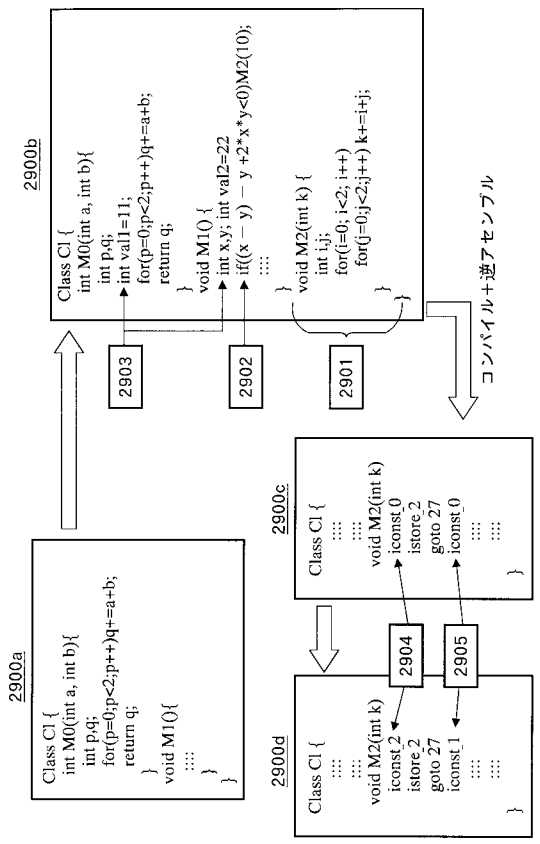
【図１９】


1801
製作者
プログラム
蓄積部
20
プログラム構造変換部
1802
透かし挿入部
1803
署名部
50
送信部
60
70a
販売者A
90a
受信部
110a
蓄積部
100a
要求受信部
120a
透かし挿入部
130a
署名部
140a
送信部
70b
販売者B
90b
受信部
110b
蓄積部
100b
要求受信部
120b
透かし挿入部
130b
署名部
140b
送信部
1805
利用者
160
要求送信部
170
受信部
180
蓄積部
1804
受信モジュール検査部
210
実行部

【図２０】


ステップ2001
N－2個のモジュールからなるプログラムを作成し蓄積部に保存
ステップ2002
2個のダミーモジュールを追加
ステップ2003
N個の部分モジュールに分割
ステップ2004
i＝1
ステップ2005
i<=j
YES
NO
ステップ2006
ダミーモジュールであるか
YES
NO
ステップ2007
販売者AのIDの挿入
ステップ2008
電子署名の付与
ステップ2009
i＋＋
ステップ2010
j+1<=i<=N
YES
NO
ステップ2011
ダミーモジュールであるか
YES
NO
ステップ2012
販売者BのIDの挿入
ステップ2013
電子署名の付与
ステップ2014
i＋＋
ステップ2015
1~j, j+1~Nのモジュールをそれぞれパッケージ化し暗号化
ステップ2016
モジュールの送信

【図２１】


2900a
Class Cl {
int M0(int a, int b){
int p,q;
for(p=0;p<2;p++)q+=a+b;
return q;
}
void M1(){
::::
}
}
2900b
Class Cl {
int M0(int a, int b){
int p,q;
int val1=11;
for(p=0;p<2;p++)q+=a+b;
return q;
}
void M1() {
int x,y; int val2=22
if((x － y) － y +2*x*y<0)M2(10);
::::
} void M2(int k) {
int i,j;
for(i=0; i<2; i++)
for(j=0;j<2;j++) k+=i+j;
}
}
2903
2902
2901
コンパイル＋逆アセンブル
2900c
Class Cl {
::::
::::
void M2(int k)
iconst_0
istore_2
goto 27
iconst_0
::::
::::
}
2904
2905
2900d
Class Cl {
::::
::::
void M2(int k)
iconst_2
istore_2
goto 27
iconst_1
::::
::::
}

フロントページの続き

審査官　高橋　克

(56)参考文献　特開平１１－１３６６１８（ＪＰ，Ａ）
特開平１０－２５４９０９（ＪＰ，Ａ）
特開２００４－１５７７０３（ＪＰ，Ａ）
特開２０００－０７６０６４（ＪＰ，Ａ）
門田 暁人，松本 健一，飯田 元，井上 克郎，鳥居 宏次，Ｊａｖａクラスファイルに対する電子透かし法，情報処理学会論文誌，日本，社団法人情報処理学会，２０００年１１月１６日，第41巻，第11号，pp.3001-3009

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２２
Ｇ０６Ｆ　２１／２４
Ｇ０９Ｃ　１／００