(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5740646号
(P5740646)
(45)発行日　平成27年6月24日(2015.6.24)　(24)登録日　平成27年5月15日(2015.5.15)

(51)Int.Cl.　F I
G06F 21/57 (2013.01)　G06F 21/57 320
G06F 21/64 (2013.01)　G06F 21/64
G06F 13/00 (2006.01)　G06F 13/00 530A

請求項の数 4　(全 20 頁)

(21)出願番号　特願2011-946(P2011-946)
(22)出願日　平成23年1月6日(2011.1.6)
(65)公開番号　特開2011-165175(P2011-165175A)
(43)公開日　平成23年8月25日(2011.8.25)
審査請求日　平成25年12月4日(2013.12.4)
(31)優先権主張番号　特願2010-4414(P2010-4414)
(32)優先日　平成22年1月12日(2010.1.12)
(33)優先権主張国　日本国(JP)

(73)特許権者　000002233
日本電産サンキョー株式会社
長野県諏訪郡下諏訪町５３２９番地
(74)代理人　110000327
特許業務法人　クラスター
(72)発明者　馬場　勉
長野県諏訪郡下諏訪町５３２９番地　日本電産サンキョー株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】ソフトウェアのダウンロード方法

(57)【特許請求の範囲】
【請求項１】
上位装置から通信回線を介してソフトウェアを電子機器装置にダウンロードする方法において、
前記上位装置から取得済の更新前ソフトウェアの正真性を証明する更新前正真性証明用情報を前記電子機器装置の第１情報格納領域に格納する第１情報格納手段と、前記上位装置から取得して更新される更新ソフトウェアの正真性を証明する正真性証明用情報を前記電子機器装置の第２情報格納領域に格納する第２情報格納手段と、を備え、
前記更新ソフトウェアのダウンロード開始前に、前記電子機器装置が前記上位装置から前記正真性証明用情報を取得し、取得した前記正真性証明用情報を前記第２情報格納領域に格納する第２情報格納工程と、
前記上位装置から前記電子機器装置に前記更新ソフトウェアのダウンロードを実行するダウンロード工程と、
前記更新ソフトウェアのダウンロード完了後に、ダウンロードされた前記更新ソフトウェアに対して計算で求めた正真性確認用情報と、前記第２情報格納工程で取得した前記正真性証明用情報とを比較する情報比較工程と、
前記情報比較工程において、前記正真性証明用情報と前記正真性確認用情報が一致している場合に、前記正真性証明用情報を前記更新前正真性証明用情報として前記第１情報格納領域に格納する第１情報格納工程と、
前記情報比較工程において、前記正真性証明用情報と前記正真性確認用情報が一致して

いる場合に、前記電子機器装置がダウンロードされた前記更新ソフトウェアを起動する起動工程と、を有することを特徴とするソフトウェアのダウンロード方法。
【請求項２】
前記ダウンロード工程において、前記更新ソフトウェアのダウンロードが中断した場合に、前記第２情報格納工程を省略して、前記ダウンロード工程から再実行することを特徴とする請求項１記載のソフトウェアのダウンロード方法。
【請求項３】
前記第１情報格納工程を実行した後に、前記第２情報格納領域に格納された前記正真性証明用情報を無効状態にする工程を備えたことを特徴とする請求項１又は２記載のソフトウェアのダウンロード方法。
【請求項４】
前記情報比較工程において、前記正真性証明用情報と前記正真性確認用情報が一致していない場合に、ダウンロードされた前記更新ソフトウェアを無効状態にする工程を備えたことを特徴とする請求項１から３のいずれか記載のソフトウェアのダウンロード方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、上位装置から通信回線を介してソフトウェアを電子機器装置にダウンロードするソフトウェアのダウンロード方法に関する。
【背景技術】
【０００２】
上位装置と電子機器装置とが通信回線で接続されたシステムにおいて、高いセキュリティ性が要求されるシステムの場合、上位装置が電子機器装置に格納されているソフトウェアをアップデートする際に、電子機器装置はダウンロードされるソフトウェアの正真性を確認する必要がある。
【０００３】
電子機器装置は、ダウンロードされるソフトウェアの正真性を証明するための正真性証明用情報（例えばハッシュ関数で計算されたハッシュ値）を上位装置から取得し、一方で、実際に上位装置からダウンロードされたソフトウェアに対して正真性を確認するための正真性確認用情報を同じ計算で求め、双方の正真性証明用情報と正真性確認用情報を比較することで、ダウンロードされたソフトウェアが正当であることを確認し、正当であると判断したときのみ、ダウンロードされたソフトウェアの起動を許可するようにしている。
【０００４】
更に、より高いセキュリティ性が求められるシステムにおいては、セキュリティに関する規格が定められており、ダウンロードのような不正行為の危険にさらされるサービスを実施する際には、必ず上位装置と電子機器装置の間で相互認証処理を実施して、双方が信頼できる装置であることが証明できてからダウンロードを開始することが必要とされている。
【０００５】
また、特許文献１には、下位デバイス（電子機器装置）に設けられたプログラム実行装置が、上位装置からダウンロードされたソフトウェアのうち、安全性検証手段によって安全（正真性）が確認されたソフトウェアのみを安全な記憶装置に記憶し、この安全な記憶装置からソフトウェアを読み出して実行することが開示されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００１－１９５２４７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】

しかしながら、ソフトウェアのダウンロードの途中で、通信回線のトラブルによる通信破綻や、停電等の原因によりダウンロードが中断された場合には、下位デバイス（電子機器装置）が上位装置から取得した正真性証明用情報が消失する恐れがあった。このため、従来は、下位デバイスがダウンロードを再開するには、改めて正真性証明用情報を上位装置から取得する段階に立ち戻るのが一般的であった。さらに、セキュリティに関する規格が定められ、より高いセキュリティ性が求められるシステムにおいては、上位装置と下位デバイス（電子機器装置）の間で相互認証処理の再実行も必要となっていた。

【０００８】

従来のシステムでは、仮に、ダウンロードを再開するに当たって相互認証を省略すると、該当システムにおける機密情報を盗み出そうとする者が、相互認証の手続方法を知らなくても、正常なダウンロードを意図的に中断させて、次回ダウンロードを再開する時に悪意をもって改ざんされたソフトウェアにすりかえてダウンロードを行うことができるという恐れがあった。

【０００９】

従って、従来のシステムでは、ダウンロードを再開するに当たって、上位装置に対して相互認証および正真性証明用情報の取得という、処理手順が必須になるので、システムの通常運用を再開するまでに時間がかかってしまうという問題があった。

【００１０】

また、特許文献１に示す従来のシステムでは、安全性検証手段により安全性を検証するためにソフトウェアを一時的に格納するメモリが別途設けられている。ソフトウェアは一旦この一時的に格納するメモリに格納され、そこで安全性が検証されて安全と判断されたら、安全な記憶装置に記憶されることになる。このように、一時的な格納用メモリを別途設けなければならず、メモリ容量増加によるコスト増が問題となる。

【００１１】

本発明は、このような点に鑑みてなされたものであり、その目的は、上位装置から通信回線を介してソフトウェアを電子機器装置にダウンロードする方法において、ダウンロードが中断された場合でも、セキュリティ性を保ちつつ、ダウンロードを再開するまでの手順を簡略化することのできるソフトウェアのダウンロード方法を提供することにある。

【課題を解決するための手段】

【００１２】

以上のような課題を解決するために、本発明は、以下のものを提供する。

【００１３】

上位装置から通信回線を介してソフトウェアを電子機器装置にダウンロードする方法において、前記ソフトウェアのダウンロードを開始する前に、前記電子機器装置が前記上位装置から前記ソフトウェアの正真性を証明する正真性証明用情報を取得し、取得した前記正真性証明用情報を前記電子機器装置の不揮発性メモリに格納する第１工程と、前記上位装置から前記電子機器装置に前記ソフトウェアのダウンロードを実行する第２工程と、前記ソフトウェアのダウンロードを完了した後に、ダウンロードされた前記ソフトウェアに対して計算で求めた正真性確認用情報と、前記第１工程で取得した正真性証明用情報とを比較する第３工程と、前記第３工程において、前記正真性証明用情報と前記正真性確認用情報が一致している場合に、前記電子機器装置がダウンロードされた前記ソフトウェアを起動する第４工程と、を有することを特徴とするソフトウェアのダウンロード方法。

【００１４】

本発明によれば、第１工程で電子機器装置が上位装置から取得した正真性証明用情報を不揮発性メモリに格納し、第２工程で上位装置から電子機器装置にソフトウェアのダウンロードを実行し、第３工程でダウンロードされたソフトウェアに対して正真性確認用情報を計算して求め、この正真性確認用情報と第１工程で取得した正真性証明用情報とを比較し、第４工程で正真性証明用情報と正真性確認用情報が一致している場合にダウンロードされたソフトウェアを起動することから、ソフトウェアのダウンロードの途中で、通信回線のトラブルによる通信破綻や、停電等の原因によりダウンロードが中断された場合でも

、電子機器装置が上位装置から取得した正真性証明用情報は不揮発性メモリにおいて確実に保持することができ、ダウンロードを再開するに当たって、上位装置に対する正真性証明情報の取得処理を省略することができる。

【００１５】

また、中断後、ダウンロードを再開する時に、改ざんされたソフトウェアにすりかえてダウンロードされたとしても、ダウンロードされたソフトウェアに対して計算で求めた正真性確認用情報は、上位装置から取得し不揮発性メモリに格納された正真性証明用情報と一致しないから、誤って不正なソフトウェアが起動されることもなく、セキュリティ性を維持することができる。

【００１６】

すなわち、ダウンロードが中断され、再度ダウンロードを行う場合でも、ダウンロードされたソフトウェアに対して計算で求めた正真性確認用情報と、既に不揮発性メモリに格納されている正真性証明用情報とを比較して、双方の正真性情報が一致している場合にのみダウンロードされたソフトウェアを起動することができるから、セキュリティ性を保ちつつ、上位装置に対する正真性証明情報の取得処理を省略して、ダウンロードを再開するまでの手順を簡略化することができる。

【００１７】

前記第２工程において、前記ソフトウェアのダウンロードが中断した場合に、前記第１工程を省略して、前記第２工程から再実行することを特徴とするソフトウェアのダウンロード方法。

【００１８】

本発明によれば、ダウンロードが中断された際に、ダウンロードを再開するに当たって、正真性証明用情報を上位装置から再取得する処理を省略し、改ざんされた不正なソフトウェアにすりかえられてダウンロードされることがないので、上位装置と電子機器装置で構成されるシステムにおいてセキュリティ性を維持することができる。

【００１９】

従って、ダウンロードを中断した後に、セキュリティ性を損なうことなく、ダウンロードを再開するまでの手順を簡略化することができる。これにより、当該システムの通常運用を再開するまでの待ち時間を短縮することができ、システムの運用効率を向上させることができる。

【００２０】

前記第３工程を実行した後に、前記不揮発性メモリに格納された前記正真性証明用情報を無効状態にする工程を備えたことを特徴とするソフトウェアのダウンロード方法。

【００２１】

本発明によれば、第３工程を実行した後に、不揮発性メモリに格納された正真性証明用情報を無効状態（消去を含む）にすることから、二重にソフトウェアをダウンロードされたり、誤って古い（更新前）ソフトウェアをダウンロードしたりすることを阻止できる。

【００２２】

前記第３工程において、前記正真性証明用情報と前記正真性確認用情報が一致していない場合に、ダウンロードされた前記ソフトウェアを無効状態にする工程を備えたことを特徴とするソフトウェアのダウンロード方法。

【００２３】

本発明によれば、ダウンロードされたソフトウェアが、改ざんされた不正なソフトウェアである場合には、正真性証明用情報と正真性確認用情報が一致しないので、その場合にダウンロードされたソフトウェアを無効状態（消去を含む）にすることにより、誤って不正なソフトウェアを起動することを阻止できる。

【００２４】

上位装置から通信回線を介してソフトウェアを電子機器装置にダウンロードする方法において、前記上位装置から取得済の更新前ソフトウェアの正真性を証明する更新前正真性証明用情報を前記電子機器装置の第１情報格納領域に格納する第１情報格納手段と、前記

上位装置から取得して更新される更新ソフトウェアの正真性を証明する正真性証明用情報を前記電子機器装置の第２情報格納領域に格納する第２情報格納手段と、を備え、前記更新ソフトウェアのダウンロード開始前に、前記電子機器装置が前記上位装置から前記正真性証明用情報を取得し、取得した前記正真性証明用情報を前記第２情報格納領域に格納する第２情報格納工程と、前記上位装置から前記電子機器装置に前記更新ソフトウェアのダウンロードを実行するダウンロード工程と、前記更新ソフトウェアのダウンロード完了後に、ダウンロードされた前記更新ソフトウェアに対して計算で求めた正真性確認用情報と、前記第２情報格納工程で取得した前記正真性証明用情報とを比較する情報比較工程と、前記情報比較工程において、前記正真性証明用情報と前記正真性確認用情報が一致している場合に、前記正真性証明用情報を前記更新前正真性証明用情報として前記第１情報格納領域に格納する第１情報格納工程と、前記情報比較工程において、前記正真性証明用情報と前記正真性確認用情報が一致している場合に、前記電子機器装置がダウンロードされた前記更新ソフトウェアを起動する起動工程と、を有することを特徴とするソフトウェアのダウンロード方法。

【００２５】

本発明によれば、第２情報格納工程で電子機器装置が上位装置から取得した正真性証明用情報を不揮発性メモリの第２情報格納領域に格納し、ダウンロード工程で上位装置から電子機器装置に更新ソフトウェアのダウンロードを実行し、情報比較工程でダウンロードした更新ソフトウェアに対して正真性確認用情報を計算して求め、この正真性確認用情報と第２情報格納工程で取得した正真性証明用情報とを比較し、正真性証明用情報と正真性確認用情報が一致している場合に、起動工程でダウンロードした更新ソフトウェアを起動することから、更新ソフトウェアのダウンロードの途中で、通信回線のトラブルによる通信破綻や、停電等の原因によりダウンロードが中断された場合でも、電子機器装置が上位装置から取得した正真性証明用情報は不揮発性メモリの第２情報格納領域において確実に保持することができ、ダウンロードを再開するに当たって、上位装置に対する正真性証明情報の取得処理を省略することができる。

【００２６】

また、中断後、ダウンロードを再開する時に、改ざんされたソフトウェアにすりかえてダウンロードされたとしても、ダウンロードされた更新ソフトウェアに対して計算で求めた更新後正真性確認用情報は、上位装置から取得し第２情報格納領域に格納された正真性証明用情報と一致しないから、誤って不正なソフトウェアが起動されることもなく、セキュリティ性を維持することができる。

【００２７】

すなわち、ダウンロードが中断され、再度ダウンロードを行う場合でも、ダウンロードした更新ソフトウェアに対して計算で求めた正真性確認用情報と、既に第２情報格納領域に格納されている正真性証明用情報とを比較して、双方の正真性情報が一致している場合にのみダウンロードされた更新ソフトウェアを起動することができるから、セキュリティ性を保ちつつ、上位装置に対する正真性証明情報の取得処理を省略して、ダウンロードを再開するまでの手順を簡略化することができる。

【００２８】

さらに、本発明に係るソフトウェアのダウンロード方法は、電子機器装置の不揮発性メモリに第１情報格納領域と第２情報格納領域を備え、情報比較工程において、正真性証明用情報と正真性確認用情報が一致している場合に、第１情報格納工程で正真性証明用情報を更新前正真性証明用情報として第１情報格納領域に格納することにより、更新ソフトウェアのダウンロード処理が完了するまでは第１情報格納領域に更新前ソフトウェアの正真性を証明する更新前正真性証明用情報を格納することができる。このため、更新ソフトウェアをダウンロードする過程で停電等の原因によって処理が中断された場合でも、第１情報格納領域には更新前ソフトウェアに対応する更新前正真性証明用情報が格納されているから、次回電源立ち上げ時に照合不一致にはならず、不正ダウンロードであると誤認されるのを防止することができる。

【００２９】
例えば、第２情報格納工程で、ダウンロード対象となる更新ソフトウェアの正真性を証明する正真性証明用情報を上位装置から受信し、その情報を電子機器装置の不揮発性メモリの第２情報格納領域に格納している途中で、停電など何らかの原因で処理が中断されて、正真性証明用情報が完全に書き込まれなかった場合でも、次回電源立ち上げ時には、第１情報格納領域に格納されている更新前正真性証明用情報と、更新前ソフトウェアの正真性確認用情報の計算結果との照合が行われることになるから、照合不一致により不正ダウンロードであると誤認されることがなく、不正使用防止のための緊急停止モードに誤って遷移するのを防止することができる。
【００３０】
前記ダウンロード工程において、前記更新ソフトウェアのダウンロードが中断した場合に、前記第２情報格納工程を省略して、前記ダウンロード工程から再実行することを特徴とするソフトウェアのダウンロード方法。
【００３１】
本発明によれば、ダウンロードが中断された際に、ダウンロードを再開するに当たって、正真性証明用情報を上位装置から再取得する処理を省略し、改ざんされた不正なソフトウェアにすりかえられてダウンロードされることがないので、上位装置と電子機器装置で構成されるシステムにおいてセキュリティ性を維持することができる。
【００３２】
従って、ダウンロードを中断した後に、セキュリティ性を損なうことなく、ダウンロードを再開するまでの手順を簡略化することができる。これにより、当該システムの通常運用を再開するまでの待ち時間を短縮することができ、システムの運用効率を向上させることができる。
【００３３】
前記第１情報格納工程を実行した後に、前記第２情報格納領域に格納された前記正真性証明用情報を無効状態にする工程を備えたことを特徴とするソフトウェアのダウンロード方法。
【００３４】
本発明によれば、第１情報格納工程を実行した後に、第２情報格納領域に格納された正真性証明用情報を無効状態（消去を含む）にすることから、二重にソフトウェアをダウンロードしたり、誤って古い（更新前）ソフトウェアをダウンロードしたりすることを阻止できる。
【００３５】
前記情報比較工程において、前記正真性証明用情報と前記正真性確認用情報が一致していない場合に、ダウンロードされた前記更新ソフトウェアを無効状態にする工程を備えたことを特徴とするソフトウェアのダウンロード方法。
【００３６】
本発明によれば、ダウンロードされた更新ソフトウェアが、改ざんされた不正なソフトウェアである場合には、正真性証明用情報と正真性確認用情報が一致しないので、その場合にダウンロードされた更新ソフトウェアを無効状態（消去を含む）にすることにより、誤って不正なソフトウェアを起動することを阻止できる。
【発明の効果】
【００３７】
本発明に係るソフトウェアのダウンロード方法は、ダウンロードが中断された際に、ダウンロードを再開するに当たって、正真性証明用情報を上位装置から再取得する処理を省略することができ、さらに、改ざんされた不正なソフトウェアにすりかえられてダウンロードされることがないので、セキュリティ性を維持することができる。
【００３８】
従って、ダウンロードを中断した後に、セキュリティ性を損なうことなく、ダウンロードを再開するまでの手順を簡略化することができる。これにより、当該システムの通常運

用を再開するまでの待ち時間を短縮することができ、システムの運用効率を向上させることができる。

【００３９】

また、ダウンロードを中断した場合でも、次回電源立ち上げ時に照合不一致によって不正ダウンロードであると誤認されることがなく、不正使用防止のための緊急停止モードに誤って遷移するのを防止することができる。

【図面の簡単な説明】

【００４０】

【図１】本発明の実施の形態に係るソフトウェアのダウンロード方法にて使用するシステムの構成を示すブロック図である。

【図２】本発明の実施の形態に係るソフトウェアのダウンロード方法の処理の一例を示す構成図である。

【図３】図２の構成において通常実行されるソフトウェアのダウンロード方法の処理の一例を示すフローチャートである。

【図４】図２の構成において中断した場合に実行されるソフトウェアのダウンロード方法の処理の一例を示すフローチャートである。

【図５】本発明の実施の形態に係るソフトウェアのダウンロード方法の処理の他の一例を示す構成図である。

【図６】図５の構成において通常実行されるソフトウェアのダウンロード方法の処理の一例を示すフローチャートである。

【図７】図５の構成において中断した場合に実行されるソフトウェアのダウンロード方法の処理の一例を示すフローチャートである。

【図８】図５の構成において電源立ち上げ時に実行されるソフトウェアの正真性確認方法の処理の一例を示すフローチャートである。

【発明を実施するための形態】

【００４１】

以下、本発明を実施するための最良の形態について、図面を参照しながら説明する。

【００４２】

［第1実施形態のシステムの構成］

図１は、本発明の実施の形態に係るソフトウェアのダウンロード方法にて使用するシステムの構成を示すブロック図である。図２は、本発明の実施の形態に係るソフトウェアのダウンロード方法において、ダウンロードの状況の一例を示す構成図である。なお、図２においてかっこ付きアルファベットで示す符号は、処理の順番を示す。

【００４３】

本システムは、通信回線３を介して接続された上位装置１と電子機器装置２とから構成され、上位装置１から通信回線３を介して更新ソフトウェア１４を電子機器装置２にダウンロードすることができるようになっている。本実施の形態では、例えば、上位装置１はＨＯＳＴコンピュータ（以下、「ＨＯＳＴコンピュータ１」という）であり、電子機器装置２は、カードに記録された情報の読み出し、或いは同カードへの新たな情報の記録等を行なうカードリーダ（以下、「カードリーダ２」という）である。

【００４４】

ＨＯＳＴコンピュータ１は、ＨＯＳＴコンピュータ１全体の動作を制御する動作回路１１を備えている。この動作回路１１にはＣＰＵ１２が搭載されており、ＣＰＵ１２内にインストールされたソフトウェアがＨＯＳＴコンピュータ１全体の制御を司っている。またＨＯＳＴコンピュータ１はデータ記憶装置（例えばハードディスク）１３を備えている。本実施の形態では、データ記憶装置１３には、カードリーダ２に格納されているソフトウェアをアップデートするための更新ソフトウェア１４と、更新ソフトウェア１４の正真性証明用情報（例えばハッシュ値）１５を格納している。なお、一般的には、正真性証明用情報１５は、更新ソフトウェア１４の正真性を証明するための情報であるので、両者は同一の管理者から提供されるようになっており、例えば、更新ソフトウェア１４と、更新ソ

フトウェア１４の正真性証明用情報１５は、カードリーダ２を動作させるためのソフトウェアを提供するベンダからセットで配付されるものである。

【００４５】

カードリーダ２は、カードリーダ２全体の動作を制御する動作回路２１を備えている。この動作回路２１には、ＣＰＵ２２が搭載されており、ＣＰＵ２２内にインストールされたソフトウェアがカードリーダ２全体の制御を司っている。

【００４６】

ＣＰＵ２２には、Ｆ－ＲＯＭ（Ｆｌａｓｈ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）などの不揮発性メモリ２３と、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）２４とが内蔵されている。

【００４７】

不揮発性メモリ２３は、カードリーダ２を制御する制御プログラムや初期値などの情報を格納している。より具体的には、図２に示すように、スーパーバイザープログラム領域２３１、データ保存領域２３２、ユーザープログラム領域２３３を有している。スーパーバイザープログラム領域２３１は、ダウンロードを実行するためのソフウェアが格納されている。さらに、本実施の形態では、正真性証明用情報１５と正真性確認用情報とを比較することも行っている。データ保存領域２３２は、カードリーダを動作させる際に必要なデータ等を保存しており、本実施の形態ではＨＯＳＴコンピュータ１から送付された正真性証明用情報１５が格納される。ユーザープログラム領域２３３は、通常、カードリーダ２を運用するためのソフトウェアが格納されており、ダウンロードにより更新ソフトウェア１４が格納されるようになっている。

【００４８】

ＲＡＭ２４は、各種の作業用データが格納されており、ワーキングエリアとして機能している。なお、不揮発性メモリ２３及びＲＡＭ２４は、ＣＰＵ２２に内蔵されたものに限られず、外部接続された外部Ｆ－ＲＯＭや、外部ＲＡＭであってもよい。また、不揮発性メモリ２３には、Ｆ－ＲＯＭに限らず、各種ＲＯＭなど電源を供給しなくても記憶を保持可能なメモリや、バッテリバックアップを具備して電源がＯＦＦの状態でもデータを保持することができるＲＡＭ等を使用することができる。

【００４９】

通信回線３は、有線あるいは無線のネットワークを含むものであり、有線としてはＲＳ２３２Ｃや、ＵＳＢなどを用いることができる。本実施例では、カードリーダ２は、通信回線３を通じてＨＯＳＴコンピュータ１からのコマンドを受信し、該コマンドにより要求された処理を実行し、処理結果をＨＯＳＴコンピュータ１に返信するようにしている。

【００５０】

つぎに、更新ソフトウェアをダウンロードする手順を、図２を用いて説明する。図２において、カードリーダ２は、更新ソフトウェア１４のダウンロードを開始する前に、ダウンロードされる更新ソフトウェア１４の正真性を証明するための情報として正真性証明用情報１５をＨＯＳＴコンピュータ１からコマンドとともに受信し、ユーザープログラム領域２３３内に格納されているプログラムを用いてデータ処理を行い、カードリーダ２内で処理するための形態に変換する（符号（ａ））。取得した正真性証明用情報１５を、ＲＡＭ２４に保持する（符号（ｂ））。カードリーダ２は、ＲＡＭ２４に保持した正真性証明用情報１５を、カードリーダ２内の不揮発性メモリ２３のデータ保存領域２３２に格納する（符号（ｃ））。この不揮発性メモリ２３に格納された正真性証明用情報１５は、カードリーダ２の電源がＯＦＦになっても失われることはない。

【００５１】

次に、カードリーダ２は、ＨＯＳＴコンピュータ１からコマンドを受信して、ダウンロード実行モードに遷移する。すなわち、不揮発性メモリ２３内に格納されているスーパーバイザープログラムを起動させる（符号（ｄ））。スーパーバイザープログラムは、ＨＯＳＴコンピュータ１からダウンロード用のコマンドを受信する（符号（ｅ））。更新ソフトウェア１４のダウンロードを実行し、更新ソフトウェア１４を不揮発性メモリ２３のユ

ーザープログラム領域２３３に格納する（符号（ｆ））。
【００５２】
カードリーダ２のスーパーバイザープログラムは、更新ソフトウェア１４のダウンロードを完了した後に、ユーザープログラム領域２３３にダウンロードされた更新ソフトウェア１４に対して正真性確認用情報を所定の計算により求める（符号（ｇ））。さらに、スーパーバイザープログラムを用いて、カードリーダ２は、計算で求めた正真性確認用情報と、予め不揮発性メモリ２３に格納されている正真性証明用情報１５とを比較して、双方の正真性証明用情報１５と正真性確認用情報が一致している場合に、ダウンロードされた更新ソフトウェア１４を起動する（符号（ｈ））。
【００５３】
上述したように、本システムは、カードリーダ２が予めＨＯＳＴコンピュータ１から取得した正真性証明用情報１５を不揮発性メモリ２３のデータ保存領域２３２に保持する。従って、ダウンロードが停電によって中断された場合や、ダウンロードが中断した後にその状態のまま電源をＯＦＦした場合でも、正真性証明用情報１５の格納先が不揮発性メモリ２３なので、正真性証明用情報１５はカードリーダ２に保持されている。
【００５４】
従って、中断した後、ダウンロードを再開させる場合には、カードリーダ２は、改めてＨＯＳＴコンピュータ１から正真性証明用情報１５を取得せず、（ダウンロードされる）更新ソフトウェア１４のダウンロードを初めからやり直すことになる。
【００５５】
ダウンロードを完了した後に、カードリーダ２は、スーパーバイザープログラムにおいて、ダウンロードされた更新ソフトウェア１４に対して正真性確認用情報を計算により求め、予め不揮発性メモリ２３に格納されている正真性証明用情報１５と比較する。つまり、このときカードリーダ２が更新することができるソフトウェアは、ダウンロードが中断された更新ソフトウェア１４のみである。
【００５６】
カードリーダ２が、それ以外のソフトウェアに更新しようとした場合、ダウンロードを完了した後に行う正真性証明用情報１５と正真性確認用情報を比較する段階で不一致となり、カードリーダ２は、無効なソフトウェアの正真性確認用情報の計算結果と、予め格納されている正真性証明用情報１５とを比較しているとみなして起動しない。
【００５７】
カードリーダ２は、正真性証明用情報１５を不揮発性メモリ２３に保持することで、正真性証明用情報１５を改めてＨＯＳＴコンピュータ１から取得する処理を省略することができ、更に相互認証処理を改めて実行しなくても、不正に改ざんされたソフトウェアに更新されることを阻止することができる。
【００５８】
つぎに、カードリーダ２が、ＨＯＳＴコンピュータ１から更新ソフトウェア１４をコマンドにより受信してダウンロードするときの手順（上述した符号（ａ）～（ｈ）を含む）を以下に示す。
【００５９】
［通常実行されるダウンロードの処理］
図３は、本発明の実施の形態に係るソフトウェアのダウンロード方法において、通常実行されるダウンロードの一例を示すフローチャートである。
【００６０】
処理（１）カードリーダ２は、ＨＯＳＴコンピュータ１から更新ソフトウェア１４に関する正真性証明用情報１５をコマンドとともに受け取る（Ｓ１０１）。
【００６１】
処理（２）Ｓ１０１のコマンドに対して相互認証処理が正常に終了しているかチェックする（Ｓ１０２）。相互認証処理が正常に終了している状態ならばＳ１０１のコマンドを受け付け、次のＳ１０４に進む。一方、正常に終了していない状態ならば実行不可応答を

ＨＯＳＴコンピュータ１に返す（Ｓ１０３）。なお、相互認証とは、ＨＯＳＴコンピュータ１側からみて、通信相手となるカードリーダ２が正当であるか、またカードリーダ２側からみて、通信相手であるＨＯＳＴコンピュータ１が正当であるかを、相互に認証することである。

【００６２】

処理（３）ＨＯＳＴコンピュータ１はカードリーダ２に、ダウンロード実行モードに遷移するように促すコマンドを送信する（Ｓ１０４）。

【００６３】

処理（４）カードリーダ２はそのコマンドを受けて、（１）の処理で取得した正真性証明用情報１５を不揮発性メモリ２３のデータ保存領域２３２に書き込んだ後（Ｓ１０５）、ダウンロード実行モードに遷移する（Ｓ１０６）。

【００６４】

処理（５）ＨＯＳＴコンピュータ１はカードリーダ２に、更新ソフトウェア１４のダウンロードを実行するコマンドを送信する（Ｓ１０７）。すなわち、コマンドにより要求された処理が実行され、具体的には、更新ソフトウェア１４をダウンロードし、カードリーダ２のＦ－ＲＯＭ２２に格納する。

【００６５】

処理（６）カードリーダ２は更新ソフトウェア１４の全データのダウンロードが完了した時点で、スーパーバイザープログラムにおいて、ダウンロードされた更新ソフトウェア１４に対して正真性確認用情報を計算により求める（Ｓ１０８）。

【００６６】

処理（７）カードリーダ２は、スーパーバイザープログラムにおいて、不揮発性メモリ２３に格納した正真性証明用情報１５と、計算により求めた正真性確認用情報を比較する（Ｓ１０９）。

【００６７】

処理（７－１）カードリーダ２は、正真性証明用情報１５と正真性確認用情報が一致する場合には、ダウンロードされた更新ソフトウェア１４が正当であると判断し、ＨＯＳＴコンピュータ１にダウンロードが正常に終了した、すなわち、更新できたことを通知する（Ｓ１１０、Ｓ１１３）。

【００６８】

処理（８－１）ダウンロードが正常に終了したとの通知を受けたＨＯＳＴコンピュータ１は、カードリーダ２に、ダウンロード実行モードからの離脱命令コマンドを送信する（Ｓ１１４）。カードリーダ２は、離脱命令コマンドを受けて、不揮発性メモリ２３に格納されている正真性証明用情報１５を無効状態として、ダウンロードされた更新ソフトウェア１４を起動し、処理を終了する（Ｓ１１５）。

【００６９】

処理（７－２）一方、上記処理（７）で比較した結果、カードリーダ２が、正真性証明用情報１５と正真性確認用情報が不一致の場合には、ダウンロードされたソフトウェアは無効なソフトウェアとみなして、不揮発性メモリ２３に格納されている正真性証明用情報１５と、ダウンロードされたソフトウェアとを無効状態として、ダウンロードが異常終了であった、すなわち、更新できなかったことをＨＯＳＴコンピュータ１に通知する（Ｓ１１１、Ｓ１１２）。

【００７０】

処理（８－２）ダウンロードが異常終了した（Ｓ１１２）場合には、カードリーダ２は、その後にダウンロード実行モードからの離脱命令コマンドを受けても、ダウンロードされたソフトウェアを起動しない。また、カードリーダ２は、全てのコマンドに対して、セキュリティエラーを通知し、処理を終了する。

【００７１】

なお、ダウンロードされた更新ソフトウェア１４と正真性証明用情報１５は、一つにまとめてダウンロードファイルとしてパックすることも可能である。

【００７２】
［ダウンロードを中断した後の処理］
図４は、本発明の実施の形態に係るソフトウェアのダウンロード方法において、ダウンロードを中断した後の処理の一例を示すフローチャートである。
【００７３】
上記処理（５）に示すＳ１０７～（８－１）に示すＳ１１５を実施中に、通信破綻などによりダウンロードが中断された場合には、（５）の処理を初めからやり直す。
【００７４】
カードリーダ２は、電源立ち上げ時に、起動すべきソフトウェアが一連のダウンロードの途中で中断された状態であると判断された場合には、ダウンロード実行モードに入り、ダウンロードを開始することを待つ。すなわち、上記（１）～（４）の処理を省略して、（５）の処理の直前に戻る。
【００７５】
具体的には、カードリーダ２は、ダウンロードを中断した後に電源が再投入されると（Ｓ２０１）、スーパーバイザープログラムを起動し（Ｓ２０２）、ユーザープログラム領域２３３に格納されているプログラムのＣＲＣチェックを実行する（Ｓ２０３）。
【００７６】
カードリーダ２は、ＣＲＣチェックにより更新ソフトウェア１４のダウンロードが正常に終了していると判断した場合には、通常運用モードに遷移する（Ｓ２０４、Ｓ２０５）。
【００７７】
一方、カードリーダ２は、ＣＲＣチェックにより更新ソフトウェア１４のダウンロードが途中で中断された状態であると判断された場合には、ダウンロード実行モードに入り、ダウロードを開始することを待つ（Ｓ２０６）。その後、カードリーダ２は、Ｓ２０７以降のダウンロードを順に再実行する。なお、図４に示すＳ２０７からＳ２１２までの各処理は、図３に示すＳ１０７からＳ１１２までの各処理と同じであるので、ここでの説明は省略する。
【００７８】
［本実施の形態の主な効果］
仮に、上記のようなダウンロードを再実行する段階で、カードリーダ２が、前回とは異なるソフトウェアをダウンロードすると、上記（５）及び（６）の処理を実行した後、上記（７－２）及び（８－２）の処理に入ることになる。従って、カードリーダ２は、上記（１）～（４）の処理を省略しても、不正なソフトウェアを起動することはなく、セキュリティ性を維持することができる。
更に、本実施の形態では、ＨＯＳＴコンピュータ１とカードリーダ２との間で正当性を確認する相互認証処理の再実施を省略しているが、不正なソフトウェアを起動することはなく、セキュリティ性を維持することができる。
【００７９】
また、カードリーダ２は、従来技術にシステムに示すように、ソフトウェアを一時的に格納するためのメモリを別途設けることなく、既存の手段で処理することができるので、従来技術に示すシステムと同レベルのセキュリティ性を維持しながらも、メモリ容量増加によるコスト増を防ぐことができる。
【００８０】
（他の実施の形態）
カードリーダ２は、不正なソフトウェアがダウンロードされたと判断された場合に、ソフトウェアを無効（ソフトウェア消去を含む）にし、即再起不能状態にしてもよい。この場合でも、再びダウンロード可能な状態に遷移したとしても、その後に何回ダウンロードを実施しても中断したソフトウェア以外は、更新に失敗するので、セキュリティ性を維持することができる。
【００８１】

カードリーダ２は、不正なソフトウェアがダウンロードされたと判断された場合に、セキュリティエラー状態として、全てのコマンドに対してセキュリティエラーを通知することにしたが、エラーレスポンスを返さず、無応答の再起不能状態にしてもよい。

【００８２】

本システムの構成としては、ダウンロードにて直接Ｆ－ＲＯＭに書き込むような構成にしているが、従来技術のように、更新ソフトウェア１４を一旦ＲＡＭに保持して、正真性チェックをして、正当なソフトウェアと判断できたら、Ｆ－ＲＯＭに書き込むようにしてもよい。

【００８３】

［第２実施形態のシステムの構成］

図５は、本発明の実施の形態に係るソフトウェアのダウンロード方法において、ダウンロードの状況の他の一例を示す構成図である。なお、図５において丸付き数字で示す符号は、処理の順番を示す。また、図２に示す構成と同じものには同じ符号を付記している。

【００８４】

第２実施形態のシステムを構成するブロック図は、上述した第１実施形態で使用したブロック図（図１）と同じであるので、ここでの説明は省略する。

【００８５】

第２実施形態では、図５に示すように、不揮発性メモリ２３は、カードリーダ２を制御する制御プログラムや初期値などの情報を格納している。より具体的には、スーパーバイザープログラム領域２３１、データ保存領域としての第１情報格納領域２３２ａ及び第２情報格納領域２３２ｂ、ユーザープログラム領域２３３を有している。

スーパーバイザープログラム領域２３１は、ダウンロードを実行するためのソフウェアが格納されている。データ保存領域は、カードリーダを動作させる際に必要なデータ等を保存しており、第１情報格納領域２３２ａ、第２情報格納領域２３２ｂと分割されている。第１情報格納領域２３２ａは、ＨＯＳＴコンピュータ１から取得済の更新前ソフトウェアの正真性を証明する更新前正真性証明用情報を格納し、第２情報格納領域２３２ｂは、ＨＯＳＴコンピュータ１から取得して更新される更新ソフトウェアの正真性を証明する正真性証明用情報１５を格納する。ユーザープログラム領域２３３は、通常、カードリーダ２を運用するためのソフトウェアが格納されており、ダウンロードにより更新ソフトウェア１４が格納されるようになっている。

【００８６】

なお、データ保存領域２３１は第１情報格納領域２３２ａ及び第２情報格納領域２３２ｂの２分割された領域に限定されるものではない。

【００８７】

カードリーダ２は、ＨＯＳＴコンピュータ１から取得済の更新前ソフトウェアの正真性を証明する更新前正真性証明用情報を第１情報格納領域２３２ａに格納する第１情報格納手段と、ＨＯＳＴコンピュータ１から取得して更新される更新ソフトウェアの正真性を証明する正真性証明用情報１５を第２情報格納領域２３２ｂに格納する第２情報格納手段と、を備えている。なお、正真性証明情報１５及び更新前正真性証明情報を書き込む不揮発性メモリは、Ｆ－ＲＯＭでもよいが、バッテリ等でバックアップされたＲＡＭでもよい。なお、第１情報格納領域２３２ａ及び第２情報格納領域２３２ｂをＦ－ＲＯＭに設ける場合、双方の領域を異なる消去単位のブロックに配置する。

【００８８】

つぎに、ＨＯＳＴコンピュータ１から取得して更新される更新ソフトウェア１４をダウンロードする手順を、図５を用いて説明する。図５において、カードリーダ２は、更新ソフトウェア１４のダウンロードを開始する前に、ダウンロードされる更新ソフトウェア１４の正真性を証明するための情報として正真性証明用情報１５をＨＯＳＴコンピュータ１からコマンドとともに受信し、ユーザープログラム領域２３３内に格納されているプログラムを用いてデータ処理を行い、カードリーダ２内で処理するための形態に変換する（丸付符号１）。取得した正真性証明用情報１５を、ＲＡＭ２４に保持する（丸付符号２）。

カードリーダ２は、ＲＡＭ２４に保持した正真性証明用情報１５を、カードリーダ２内の不揮発性メモリ２３の第２の情報格納領域２３２ｂに格納する（丸付符号３）。この不揮発性メモリ２３に格納された正真性証明用情報１５は、カードリーダ２の電源がＯＦＦになっても失われることはない。

【００８９】

次に、カードリーダ２は、ＨＯＳＴコンピュータ１からコマンドを受信して、ダウンロード実行モードに遷移する。すなわち、不揮発性メモリ２３内に格納されているスーパーバイザープログラムを起動させる（丸付符号４）。スーパーバイザープログラムは、ＨＯＳＴコンピュータ１からダウンロード用のコマンドを受信する（丸付符号５）。更新ソフトウェア１４のダウンロードを実行し、更新ソフトウェア１４を不揮発性メモリ２３のユーザープログラム領域２３３に格納する（丸付符号６）。

【００９０】

カードリーダ２のスーパーバイザープログラムは、更新ソフトウェア１４のダウンロードを完了した後に、ユーザープログラム領域２３３にダウンロードされた更新ソフトウェア１４に対して正真性確認用情報を所定の計算により求める（丸付符号７）。さらに、スーパーバイザープログラムを用いて、カードリーダ２は、計算で求めた正真性確認用情報と、予め不揮発性メモリ２３の第２の情報格納領域２３２ｂに格納されている正真性証明用情報１５とを比較して、双方の正真性証明用情報１５と正真性確認用情報が一致している場合に、ダウンロードされた更新ソフトウェア１４を起動する（丸付符号８）。

【００９１】

また、カードリーダ２のスーパーバイザープログラムは、正真性証明用情報１５と計算により求めた正真性確認用情報が一致している場合に、第２情報格納領域２３２ｂに格納されている正真性証明用情報１５を更新前正真性証明用情報として第１情報格納領域２３２ａに格納する（丸付符号９）。

【００９２】

上述したように、第２実施形態における本システムは、カードリーダ２が不揮発性メモリ２３に第１情報格納領域２３２ａと第２情報格納領域２３２ｂを備え、丸付符号９の情報比較工程において、正真性証明用情報１５と計算により求めた正真性確認用情報が一致している場合に、第２情報格納領域２３２ｂに格納された正真性証明用情報１５を更新前正真性証明用情報として第１情報格納領域２３２ａに格納する。従って、本システムは、丸付符号３の第２情報格納工程で、ダウンロード対象となる更新ソフトウェア１４の正真性を証明する正真性証明用情報１５をＨＯＳＴコンピュータ１から受信し、その情報をカードリーダ２の不揮発性メモリ２３の第２情報格納領域２３２ｂに格納している途中で、停電などにより処理が中断されて、正真性証明用情報１５が完全に書き込まれなかった場合でも、次回電源立ち上げ時には、第１情報格納領域２３２ａに格納されている更新前正真性証明用情報と、更新前（未だ更新されていない）ソフトウェアの正真性確認情報の計算結果との照合が行われ、照合結果は一致する。すなわち、本システムが、照合不一致により不正ダウンロードであると誤認され、不正使用防止のための緊急停止モードに誤って遷移することがない。

【００９３】

また、本システムが、丸付符号６の更新ソフトウェア１４のダウンロード実行前に、停電等の原因によって処理が中断された場合でも、第１情報格納領域２３２ａには、更新前（未だ更新されていない）ソフトウェアに対応する更新前正真性証明用情報が格納されている。従って、本システムは、次回電源立ち上げ時に、第１情報格納領域２３２ａに格納されている更新前正真性証明用情報と、未だ更新されていないソフトウェアの正真性確認情報の計算結果との照合が行われ、照合結果は一致するから、緊急停止モードに誤って遷移することがない。

【００９４】

また、本システムは、丸付符号９の第１情報格納工程の途中で、停電等の原因によって処理が中断された場合には、第１情報格納領域２３２ａに格納された情報は破損している

が、第２情報格納領域２３２ｂには更新ソフトウェア１４に対応する正真性証明用情報１５が格納されている。従って、本システムは、次回電源立ち上げ時に、第２情報格納領域２３２ｂに格納されている正真性証明用情報１５と、更新ソフトウェア１４に対して計算により求めた正真性確認情報の計算結果との照合が行われ、照合結果は一致するから、緊急停止モードに誤って遷移することがない。

【００９５】

第２実施形態の本システムは、第１実施形態のシステムと同様に、ダウンロード処理が中断された場合でも、セキュリティ性を保ちつつ、ダウンロード処理再開までの手順を簡略化することができる。

【００９６】

つぎに、カードリーダ２が、ＨＯＳＴコンピュータ１から更新ソフトウェア１４をコマンドにより受信してダウンロードするときの手順（上述した丸付符号１～９を含む）を以下に示す。

【００９７】

［通常実行されるダウンロードの処理］

図６は、第２実施形態のソフトウェアのダウンロード方法において、通常実行されるダウンロードの一例を示すフローチャートである。

【００９８】

処理（一）カードリーダ２は、ＨＯＳＴコンピュータ１から更新ソフトウェア１４に関する正真性証明用情報１５をコマンドとともに受け取る（Ｓ３０１）。

【００９９】

処理（二）Ｓ３０１のコマンドに対して相互認証処理が正常に終了しているかチェックする（Ｓ３０２）。相互認証処理が正常に終了している状態ならばＳ３０１のコマンドを受け付け、次のＳ３０４に進む。一方、正常に終了していない状態ならば実行不可応答をＨＯＳＴコンピュータ１に返す（Ｓ３０３）。なお、相互認証とは、ＨＯＳＴコンピュータ１側からみて、通信相手となるカードリーダ２が正当であるか、またカードリーダ２側からみて、通信相手であるＨＯＳＴコンピュータ１が正当であるかを、相互に認証することである。

【０１００】

処理（三）ＨＯＳＴコンピュータ１はカードリーダ２に、ダウンロード実行モードに遷移するように促すコマンドを送信する（Ｓ３０４）。

【０１０１】

処理（四）カードリーダ２はそのコマンドを受けて、（一）の処理で取得した正真性証明用情報１５を不揮発性メモリ２３の第２情報格納領域２３２ｂに書き込んだ後（Ｓ３０５）、ダウンロード実行モードに遷移する（Ｓ３０６）。

【０１０２】

処理（五）ＨＯＳＴコンピュータ１からカードリーダ２に、更新ソフトウェア１４のダウンロードを実行するコマンドを送信する（Ｓ３０７）。

【０１０３】

処理（六）すなわち、コマンドにより要求された処理が実行され、具体的には、カードリーダ２は、更新ソフトウェア１４をダウンロードし、カードリーダ２のＦ－ＲＯＭ２２に格納する。

【０１０４】

処理（七）カードリーダ２は、更新ソフトウェア１４の全データのダウンロードが完了した時点で、スーパーバイザープログラムにおいて、ダウンロードされた更新ソフトウェア１４に対して正真性確認用情報を計算により求める（Ｓ３０８）。

【０１０５】

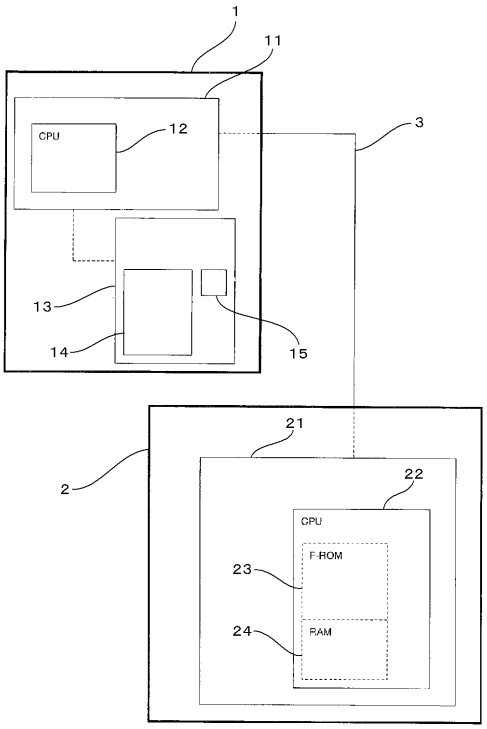
処理（八）カードリーダ２は、スーパーバイザープログラムにおいて、不揮発性メモリ２３の第２情報格納領域２３２ｂに格納した正真性証明用情報１５と、計算により求めた正真性確認用情報を比較する（Ｓ３０９）。

【０１０６】
処理（九）カードリーダ２は、正真性証明用情報１５と計算により求めた正真性確認用情報が一致する場合には、ダウンロードされた更新ソフトウェア１４が正当であると判断し（Ｓ３１０）、第２情報格納領域２３２ｂに格納した正真性証明用情報１５を第１情報格納領域２３２ａに複写し（Ｓ３１３）、ＨＯＳＴコンピュータ１にダウンロードが正常に終了したこと、すなわち、更新できたことを通知する（Ｓ３１４）。なお、カードリーダ２は、複写後に、第２情報格納領域２３２ｂに格納されている正真性証明用情報１５を削除してもよい。
【０１０７】
ダウンロードが正常に終了したとの通知を受けたＨＯＳＴコンピュータ１は、カードリーダ２に、ダウンロード実行モードからの離脱命令コマンドを送信する（Ｓ３１５）。カードリーダ２は、離脱命令コマンドを受けて、ダウンロードされた更新ソフトウェア１４を起動し、処理を終了する（Ｓ３１６）。なお、Ｓ３１５において、離脱命令コマンドでない場合には、引き続きスーパーバイザープログラムは各コマンドの処理を実施する。
【０１０８】
一方、カードリーダ２は、正真性証明用情報１５と計算により求めた正真性確認用情報が不一致の場合には、ダウンロードされたソフトウェアは無効なソフトウェアとみなして（Ｓ３１０）、不揮発性メモリ２３の第２情報格納領域２３２ｂに格納されている正真性証明用情報１５と、ダウンロードされたソフトウェアとを無効状態として、ダウンロードが異常終了であったこと、すなわち、更新できなかったことをＨＯＳＴコンピュータ１に通知する（Ｓ３１１、Ｓ３１２）。
【０１０９】
ダウンロードが異常終了した（Ｓ３１２）場合には、カードリーダ２は、その後にダウンロード実行モードからの離脱命令コマンドを受けても、ダウンロードされたソフトウェアを起動しない。また、カードリーダ２は、全てのコマンドに対して、セキュリティエラーを通知し、処理を終了する。
【０１１０】
［ダウンロードを中断した後の処理］
図７は、第２実施形態のソフトウェアのダウンロード方法において、ダウンロードを中断した場合に実行されるソフトウェアのダウンロード方法の処理の一例を示すフローチャートである。
【０１１１】
カードリーダ２は、更新ソフトウェア１４のダウンロード処理を中断した後に電源が再投入されると（Ｓ４０１）、スーパーバイザープログラムを起動し、ユーザープログラム領域２３３に格納されているプログラムのＣＲＣチェックを実行する（Ｓ４０２）。
【０１１２】
カードリーダ２は、ＣＲＣチェックにより更新ソフトウェア１４のダウンロードが正常に終了していると判断した場合には、通常運用モードに遷移する（Ｓ４０３、Ｓ４０４）。
【０１１３】
一方、カードリーダ２は、ＣＲＣチェックにより更新ソフトウェア１４のダウンロードが途中で中断された状態であると判断された場合には、ダウンロード実行モードに入り、更新ソフトウェア１４のダウロードを実施する（Ｓ４０５、Ｓ４０６）。
【０１１４】
カードリーダ２は、更新ソフトウェア１４の全データのダウンロードが完了した時点で、スーパーバイザープログラムにおいて、ダウンロードされた更新ソフトウェア１４に対して正真性確認用情報を計算により求める（Ｓ４０７）。
【０１１５】
カードリーダ２は、スーパーバイザープログラムを実行し、不揮発性メモリ２３の第２情報格納領域２３２ｂに格納した正真性証明用情報１５と、計算により求めた正真性確認

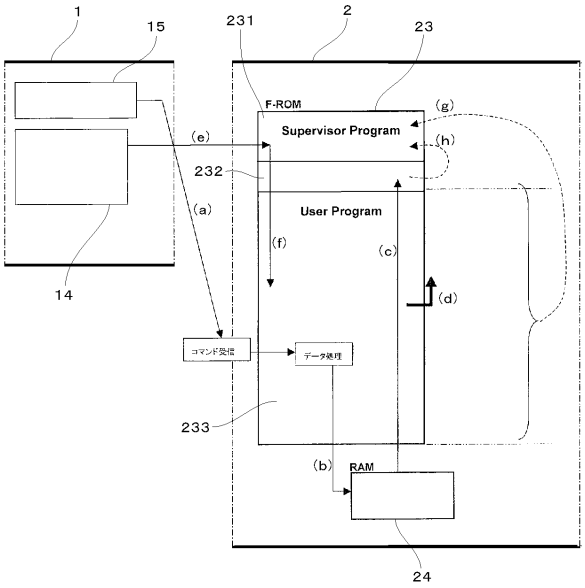
用情報を比較する（Ｓ４０８）。
【０１１６】
カードリーダ２は、正真性証明用情報１５と計算により求めた正真性確認用情報が一致する場合には、ダウンロードされた更新ソフトウェア１４が正当であると判断し（Ｓ４０９）、第２情報格納領域２３２ｂに格納した正真性証明用情報１５を第１情報格納領域２３２ａに複写し（Ｓ４１２）、ＨＯＳＴコンピュータ１にダウンロードが正常に終了したこと、すなわち、更新できたことを通知する。
【０１１７】
ダウンロードが正常に終了したとの通知を受けたＨＯＳＴコンピュータ１は、カードリーダ２に、ダウンロード実行モードからの離脱命令コマンドを送信する（Ｓ４１３）。カードリーダ２は、離脱命令コマンドを受けて、ダウンロードされた更新ソフトウェア１４を起動し、処理を終了する（Ｓ４１４）。なお、Ｓ４１３において、離脱命令コマンドでない場合には、引き続きスーパーバイザープログラムは各コマンドの処理を実施する。
【０１１８】
一方、カードリーダ２は、正真性証明用情報１５と計算により求めた正真性確認用情報が不一致の場合には、ダウンロードしたソフトウェアは無効なソフトウェアとみなして（Ｓ４０９）、不揮発性メモリ２３の第２情報格納領域２３２ｂに格納されている正真性証明用情報１５と、ダウンロードされたソフトウェアとを無効状態として、ダウンロードが異常終了であったこと、すなわち、更新できなかったことをＨＯＳＴコンピュータ１に通知する（Ｓ４１０、Ｓ４１１）。
【０１１９】
ダウンロードが異常終了した（Ｓ４１１）場合には、カードリーダ２は、その後にダウンロード実行モードからの離脱命令コマンドを受けても、ダウンロードされたソフトウェアを起動しない。また、カードリーダ２は、全てのコマンドに対して、セキュリティエラーを通知し、処理を終了する。
【０１２０】
［電源立ち上げ時の正真性確認処理］
図８は、第２実施形態のソフトウェアのダウンロード方法において、電源立ち上げ時に実行されるソフトウェアの正真性確認方法の処理の一例を示すフローチャートである。
【０１２１】
カードリーダ２は、電源が再投入されると（Ｓ５０１）、スーパーバイザープログラムを起動し、ユーザープログラム領域２３３に格納されているプログラムのＣＲＣチェックを実行する（Ｓ５０２）。
【０１２２】
カードリーダ２は、ＣＲＣチェックにより更新ソフトウェア１４のダウンロードが正常に終了していないと判断した場合には、ダウンロード実行モードに遷移する（Ｓ５０３、Ｓ５０４）。
【０１２３】
一方、カードリーダ２は、ＣＲＣチェックにより更新ソフトウェア１４のダウンロードが正常に完了していると判断した場合には、スーパーバイザープログラムにおいて、ダウンロードされた更新ソフトウェアに対して正真性確認用情報を計算により求める（Ｓ５０３、Ｓ５０５）。
【０１２４】
カードリーダ２は、スーパーバイザープログラムにおいて、不揮発性メモリ２３の第１情報格納領域２３２ａに格納された更新前の正真性証明用情報と、計算により求められた正真性確認用情報を比較する（Ｓ５０６）。
【０１２５】
カードリーダ２は、更新前の正真性証明用情報と計算により求められた正真性確認用情報が一致する場合には、ダウンロードされたソフトウェアが正当であると判断し（Ｓ５０７）、通常運用モードに遷移する（Ｓ５０８）。

【０１２６】
一方、カードリーダ２は、更新前の正真性証明用情報と計算により求められた正真性確認用情報が一致しない場合には、第２情報格納領域２３２ｂに格納されている正真性証明用情報１５と計算により求められた正真性確認用情報を比較する（Ｓ５０９）。
【０１２７】
カードリーダ２は、第２情報格納領域２３２ｂに格納した正真性証明用情報と計算により求めた正真性確認用情報が一致する場合には、更新ソフトウェア１４のダウンロード終了後に、第２情報格納領域２３２ｂに格納された正真性証明用情報を第１情報格納領域２３２ａに複写する途中で中断されたと判断し（Ｓ５１０）、第２情報格納領域２３２ｂに格納された正真性証明用情報１５を、更新前の正真性証明用情報として第１情報格納領域２３２ａに複写し（Ｓ５１３）、通常運用モードに遷移する（Ｓ５１４）。
【０１２８】
一方、カードリーダ２は、正真性証明用情報１５と計算により求めた正真性確認用情報が一致しない場合には、ダウンロードされているソフトウェアは無効なソフトウェアとみなして（Ｓ５１０）、不揮発性メモリ２３の第２情報格納領域２３２ｂに格納されている正真性証明用情報１５と、ダウンロードされたソフトウェアとを無効状態として、ダウンロードが異常終了であったこと、すなわち、更新できなかったことをＨＯＳＴコンピュータ１に通知する（Ｓ５１１、Ｓ５１２）。
【０１２９】
ダウンロードされたソフトウェアが異常と判断された（Ｓ５１２）場合には、カードリーダ２は、その後にダウンロード実行モードからの離脱命令コマンドを受けても、ダウンロードされたソフトウェアを起動しない。また、カードリーダ２は、全てのコマンドに対して、セキュリティエラーを通知し、処理を終了する。
【０１３０】
［本実施の形態の主な効果］
第２実施形態に示す本システムは、このような構成にすることで、一連のダウンロード処理が中断されても確実に復旧させることができるため、システムの信頼性を向上させることができる。
【０１３１】
また、本システムは、ソフトウェアをダウンロードする過程で停電等の原因によって処理が中断された場合でも、第１情報格納領域及び第２情報格納領域にそれぞれのソフトウェアに対応した正真性証明用情報が格納されているから、次回電源立ち上げ時に照合不一致になって、不正ダウンロードであると誤認されるのを防止することができる。
【符号の説明】
【０１３２】
１　上位装置
２　電子機器装置
３　通信回線
１２　ＣＰＵ
１３　データ記憶装置
１４　ソフトウェア（更新ソフトウェア）
１５　正真性証明用情報
２１　動作回路
２２　ＣＰＵ
２３　不揮発性メモリ
２４　ＲＡＭ

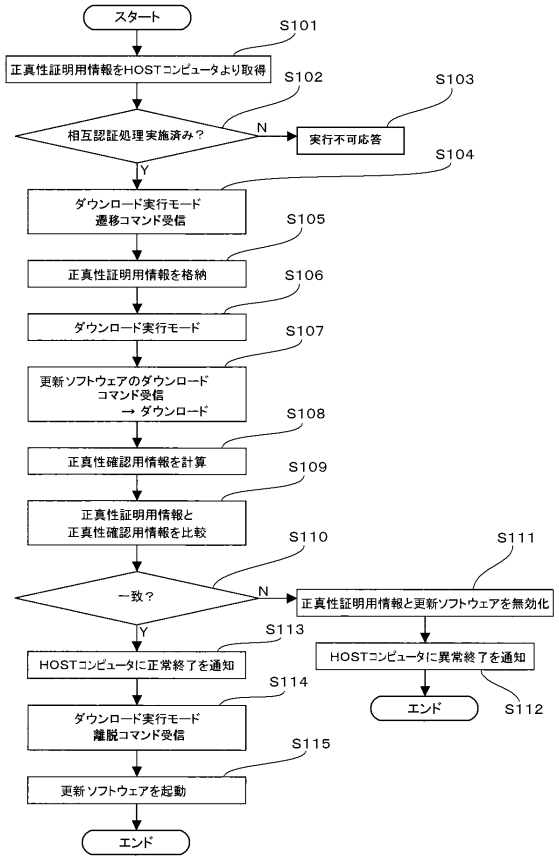
【図１】


1
11
CPU
12
3
13
14
15
2
21
22
CPU
F-ROM
23
24
RAM

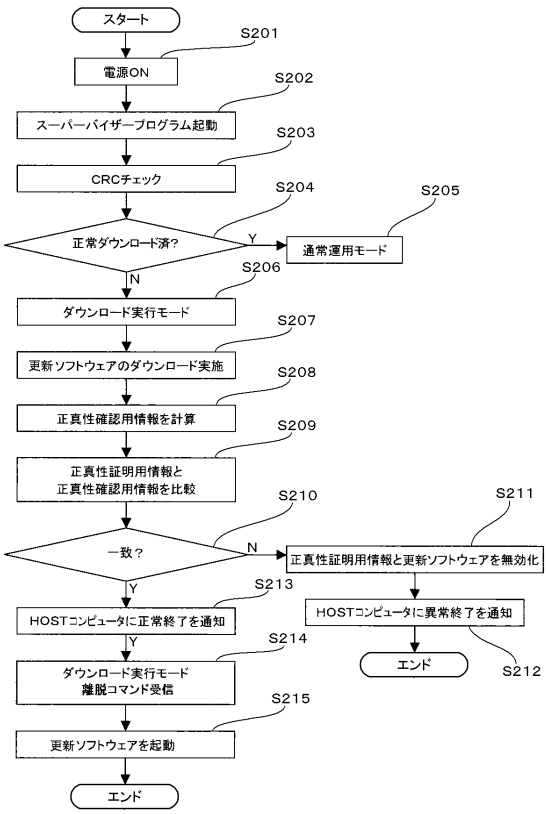
【図２】


1
15
231
2
23
F-ROM
(g)
Supervisor Program
(h)
(e)
232
(a)
User Program
(f)
(c)
(d)
14
コマンド受信
データ処理
233
(b)
RAM
24

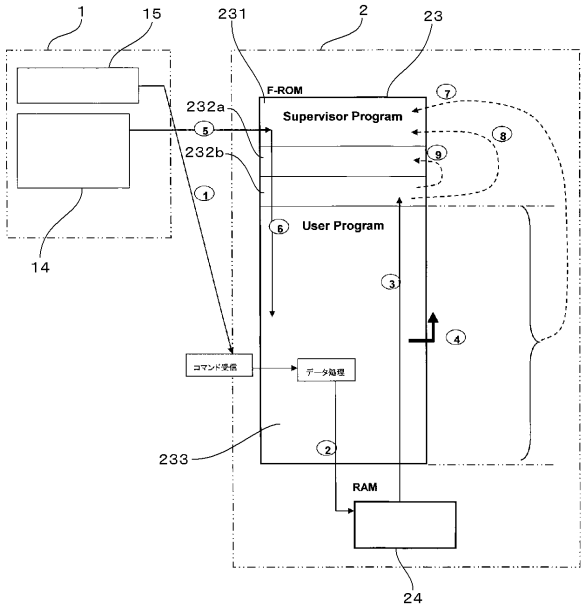
【図３】


スタート
S101
正真性証明用情報をHOSTコンピュータより取得
S102
S103
相互認証処理実施済み？
N
実行不可応答
Y
S104
ダウンロード実行モード
遷移コマンド受信
S105
正真性証明用情報を格納
S106
ダウンロード実行モード
S107
更新ソフトウェアのダウンロード
コマンド受信
→ ダウンロード
S108
正真性確認用情報を計算
S109
正真性証明用情報と
正真性確認用情報を比較
S110
S111
一致？
N
正真性証明用情報と更新ソフトウェアを無効化
Y
S113
HOSTコンピュータに正常終了を通知
HOSTコンピュータに異常終了を通知
S114
エンド
S112
ダウンロード実行モード
離脱コマンド受信
S115
更新ソフトウェアを起動
エンド

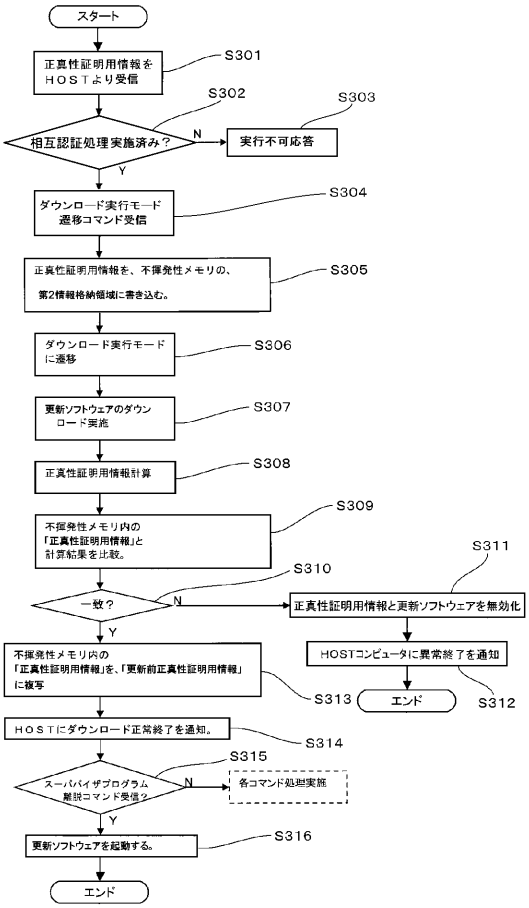
【図４】


スタート
S201
電源ON
S202
スーパーバイザープログラム起動
S203
CRCチェック
S204
S205
正常ダウンロード済?
Y
通常運用モード
N
S206
ダウンロード実行モード
S207
更新ソフトウェアのダウンロード実施
S208
正真性確認用情報を計算
S209
正真性証明用情報と
正真性確認用情報を比較
S210
S211
一致？
N
正真性証明用情報と更新ソフトウェアを無効化
Y
S213
HOSTコンピュータに正常終了を通知
HOSTコンピュータに異常終了を通知
Y
S214
エンド
S212
ダウンロード実行モード
離脱コマンド受信
S215
更新ソフトウェアを起動
エンド

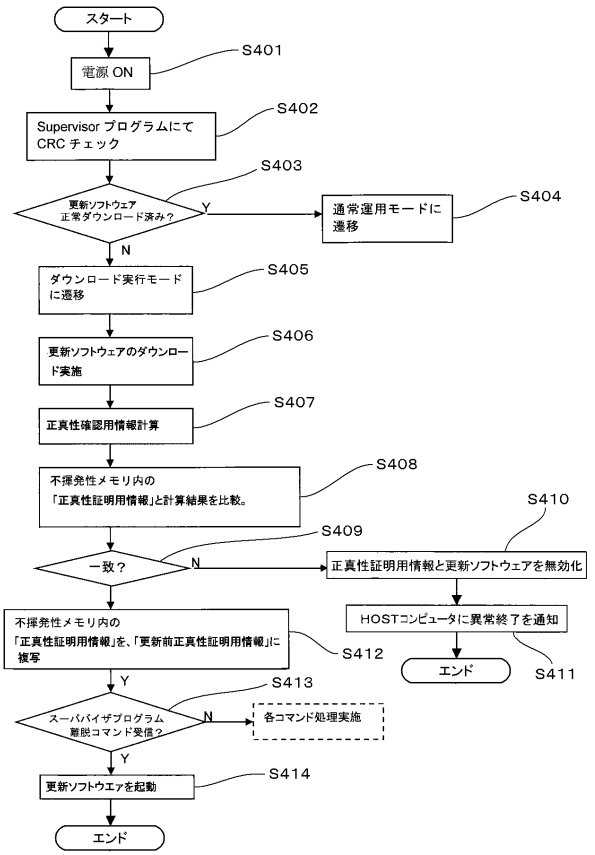
【図５】


1
15
231
2
23
F-ROM
Supervisor Program
232a
232b
User Program
14
コマンド受信
データ処理
233
RAM
24

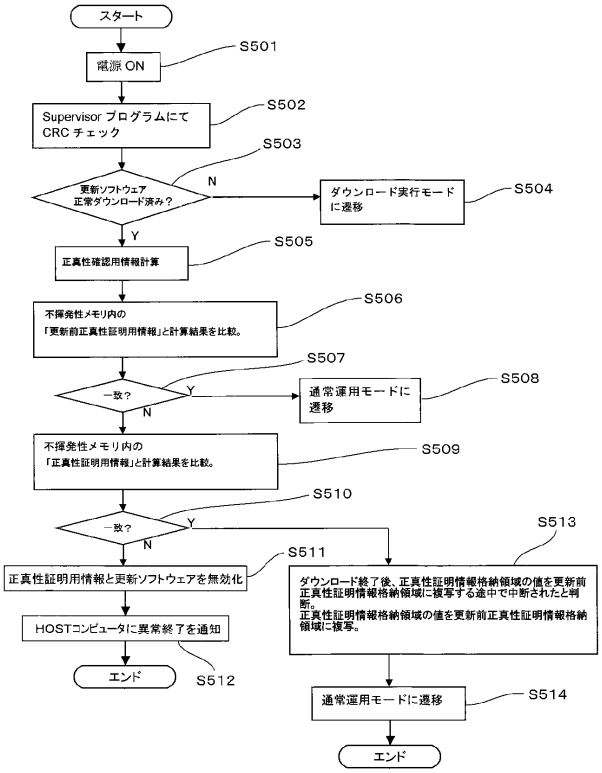
【図６】


スタート
正真性証明用情報をHOSTより受信
S301
相互認証処理実施済み？
S302
N
実行不可応答
S303
Y
ダウンロード実行モード遷移コマンド受信
S304
正真性証明用情報を、不揮発性メモリの、第2情報格納領域に書き込む。
S305
ダウンロード実行モードに遷移
S306
更新ソフトウェアのダウンロード実施
S307
正真性証明用情報計算
S308
不揮発性メモリ内の「正真性証明用情報」と計算結果を比較。
S309
一致？
S310
N
正真性証明用情報と更新ソフトウェアを無効化
S311
HOSTコンピュータに異常終了を通知
S312
エンド
Y
不揮発性メモリ内の「正真性証明用情報」を、「更新前正真性証明用情報」に複写
S313
HOSTにダウンロード正常終了を通知。
S314
スーパバイザプログラム離脱コマンド受信？
S315
N
各コマンド処理実施
Y
更新ソフトウェアを起動する。
S316
エンド

【図７】


スタート
電源 ON
S401
Supervisor プログラムにて CRC チェック
S402
更新ソフトウェア正常ダウンロード済み？
S403
Y
通常運用モードに遷移
S404
N
ダウンロード実行モードに遷移
S405
更新ソフトウェアのダウンロード実施
S406
正真性確認用情報計算
S407
不揮発性メモリ内の「正真性証明用情報」と計算結果を比較。
S408
一致？
S409
N
正真性証明用情報と更新ソフトウェアを無効化
S410
HOSTコンピュータに異常終了を通知
S411
エンド
不揮発性メモリ内の「正真性証明用情報」を、「更新前正真性証明用情報」に複写
S412
Y
スーパバイザプログラム離脱コマンド受信？
S413
N
各コマンド処理実施
Y
更新ソフトウエアを起動
S414
エンド

【図８】


スタート
電源 ON
S501
Supervisor プログラムにて CRC チェック
S502
更新ソフトウェア正常ダウンロード済み？
S503
N
ダウンロード実行モードに遷移
S504
Y
正真性確認用情報計算
S505
不揮発性メモリ内の「更新前正真性証明用情報」と計算結果を比較。
S506
一致？
S507
Y
通常運用モードに遷移
S508
N
不揮発性メモリ内の「正真性証明用情報」と計算結果を比較。
S509
一致？
S510
Y
N
正真性証明用情報と更新ソフトウェアを無効化
S511
HOSTコンピュータに異常終了を通知
エンド
S512
ダウンロード終了後、正真性証明情報格納領域の値を更新前正真性証明情報格納領域に複写する途中で中断されたと判断。
正真性証明情報格納領域の値を更新前正真性証明情報格納領域に複写。
S513
通常運用モードに遷移
S514
エンド

フロントページの続き

(56)参考文献 特開２００９－１０４６１８（ＪＰ，Ａ）
国際公開第０３／０６５２２５（WO，Ａ１）
特表２００５－５３２６１２（ＪＰ，Ａ）
特開２００３－１０８３８４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／