【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成17年8月4日(2005.8.4)

【公開番号】特開2002-319935(P2002-319935A)
【公開日】平成14年10月31日(2002.10.31)
【出願番号】特願2002-8824(P2002-8824)
【国際特許分類第７版】
　Ｈ０４Ｌ　 9/32
　Ｇ０６Ｆ　15/00
　Ｈ０４Ｌ　 9/10
【ＦＩ】
　Ｈ０４Ｌ　 9/00　　６７５Ｚ
　Ｇ０６Ｆ　15/00　　３３０Ａ
　Ｈ０４Ｌ　 9/00　　６２１Ａ

【手続補正書】
【提出日】平成17年1月12日(2005.1.12)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項２６
【補正方法】変更
【補正の内容】
【請求項２６】
　デジタル署名されたデータを受信して処理するデータ処理装置であって、
　ネットワークで接続されたサーバから、デジタル署名されたデータを受信する受信手段と、
　前記受信手段で受信されたデータについて、当該データの署名者にとって署名可能なデータの種別を記載した署名者証明書を取得する署名者証明書取得手段と、
　前記受信手段で受信されたデータについて、当該データの種別が前記署名者証明書取得手段で取得された署名者証明書に記載されているときに、当該データに対する署名を有効であると判断する署名検証手段とを備えた、データ処理装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】請求項３２
【補正方法】変更
【補正の内容】
【請求項３２】
　デジタル署名されたデータを受信して処理するデータ処理方法であって、
　ネットワークで接続されたサーバから、デジタル署名されたデータを受信する受信ステップと、
　前記受信ステップで受信されたデータについて、当該データの署名者にとって署名可能なデータの種別を記載した署名者証明書を取得する署名者証明書取得ステップと、
　前記受信ステップで受信されたデータについて、当該データの種別が前記署名者証明書取得ステップで取得された署名者証明書に記載されているときに、当該データに対する署名を有効であると判断する署名検証ステップとを備えた、データ処理方法。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００４０
【補正方法】変更

【補正の内容】
【００４０】
第２６の発明は、デジタル署名されたデータを受信して処理するデータ処理装置であって、
ネットワークで接続されたサーバから、デジタル署名されたデータを受信する受信手段と、
受信手段で受信されたデータについて、そのデータの署名者にとって署名可能なデータの種別を記載した署名者証明書を取得する署名者証明書取得手段と、
受信手段で受信されたデータについて、そのデータの種別が署名者証明書取得手段で取得された署名者証明書に記載されているときに、そのデータに対する署名を有効であると判断する署名検証手段とを備える。
このような第２６の発明によれば、任意の種別のデータについて同じアルゴリズムを用いて、受信したデータに対して署名者が署名権限を有するか否かを判定できる。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００４６
【補正方法】変更
【補正の内容】
【００４６】
第３２の発明は、デジタル署名されたデータを受信して処理するデータ処理方法であって、
ネットワークで接続されたサーバから、デジタル署名されたデータを受信する受信ステップと、
受信ステップで受信されたデータについて、そのデータの署名者にとって署名可能なデータの種別を記載した署名者証明書を取得する署名者証明書取得ステップと、
受信ステップで受信されたデータについて、そのデータの種別が署名者証明書取得ステップで取得された署名者証明書に記載されているときに、そのデータに対する署名を有効であると判断する署名検証ステップとを備える。
このような第３２の発明によれば、任意の種別のデータについて同じアルゴリズムを用いて、受信したデータに対して署名者が署名権限を有するか否かを判定できる。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００７４
【補正方法】変更
【補正の内容】
【００７４】
取得した端末用データが端末用データ妥当性判定処理で妥当であると判定された場合には（ステップＳ１５３のＹＥＳ）、端末内データ格納処理（ステップＳ１５４）が実行される。この処理では、動作制御部１０７が、取得した端末用データを端末内データ格納部１０８に書き込む。その後、動作制御部１０７は、ステップＳ１５１へ進み、次の端末用データを処理する。取得した指示データに含まれるすべてのＵＲＬについてステップＳ１５１からＳ１５４の処理を終えた場合には（ステップＳ１５１のＮＯ）、動作制御部１０７は、動作制御処理を完了する。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００８６
【補正方法】変更
【補正の内容】
【００８６】
なお、第１および第２の実施形態では、動作制御部１０７、１２７は、ＣＰＵ３１がＲ

ＡＭ３２またはＲＯＭ３３に格納されたプログラムを実行することによって構成されることとした。特に、動作制御部１０７、１２７は、ＣＰＵ３１がＪＡＶＡ（Ｒ）の仮想マシンとして、ＲＡＭ３２に格納されたＪＡＶＡ（Ｒ）アプレットを実行することによって構成されることとしてもよい。この場合、ＪＡＶＡ（Ｒ）アプレットは、利用者からの指示に応じて、通信ネットワーク１０を介して動的にデータ処理装置１００、１２０にダウンロードされることとしてもよい。また、データ処理装置１００、１２０は、指示データ１１１に基づき取得した端末用データ１１２（または、指示データ１３１から取得した端末用データ１３２）を、端末内データ格納部１０８に格納することとしたが、周辺機器やＩｒＤＡ（Ｉｎｆｒａｒｅｄ　Ｄａｔａ　Ａｓｓｏｃｉａｔｉｏｎ）通信インターフェイス部などのデータ出力部に直接出力することとしてもよい。

【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００９９
【補正方法】変更
【補正の内容】
【００９９】

一方、非保護データ領域２４２に相当するｕｎｐｒｏｔｅｃｔｅｄタグ２６２には、改竄されてもよい一時的な情報が配置される。図１９に示すスケジュール更新用データでは、セッションＩＤおよび更新日時情報が、改竄されてもよいデータとして扱われる。このため、ｕｎｐｒｏｔｅｃｔｅｄタグ２６２には、セッションＩＤを含んだｓｅｓｓｉｏｎＩＤタグ２７４、および、更新日時情報を含んだｍｏｄｉｆｉｅｄタグ２７５が配置されている。なお、ｃｏｍｍａｎｄタグ２７６は、データが改竄された結果、ｕｎｐｒｏｔｅｃｔｅｄタグ２６２に配置されているものとする。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】０１０３
【補正方法】変更
【補正の内容】
【０１０３】

非保護データ検証部２０３は、アプリケーション部２０４に対して、ｐｒｏｔｅｃｔｅｄタグ２６１に含まれるデータと、ｕｎｐｒｏｔｅｃｔｅｄタグ２６２に含まれるデータとを出力する（ステップＳ２０９）。ｐｒｏｔｅｃｔｅｄタグ２６１に含まれるデータについては、改竄されていないことが保証されている。また、ｕｎｐｒｏｔｅｃｔｅｄタグ２６２に含まれるデータのうち、データの種別がｕｎｐｒｏｔｅｃｔｅｄＴａｇタグ２６５に記載されていないデータは、非保護データ検証部２０３の作用により除去されている。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】０１１８
【補正方法】変更
【補正の内容】
【０１１８】

また、第４の実施形態では、入力部２２１には非保護対象リスト２４５に含まれるデータ（またはタグ）の種別が入力されることとしたが、入力部２２１から入力される情報は、保護データ領域および非保護データ領域にどのデータ（またはタグ）を配置するかを識別できる情報であれば足りる。したがって、入力部２２１には、保護データ領域に含まれるデータ（またはタグ）の種別が入力されることとしてもよい。また、非保護対象リスト生成部２２２は、非保護対象リスト２４５に含まれるデータ（またはタグ）の種別を記憶する記憶部を有しており、入力部２２１には前回の設定に対する変更部分のみが入力されることとしてもよい。