【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６部門第３区分
【発行日】平成17年11月10日(2005.11.10)

【公表番号】特表2001-517342(P2001-517342A)
【公表日】平成13年10月2日(2001.10.2)
【出願番号】特願平10-541278
【国際特許分類第７版】
　Ｇ０６Ｆ　12/14
　Ｇ０６Ｆ　 9/06
　Ｇ０６Ｆ　12/00
　Ｇ０６Ｆ　13/00
　Ｇ０９Ｃ　 5/00
　Ｈ０４Ｌ　12/22
　Ｈ０４Ｌ　12/54
　Ｈ０４Ｌ　12/58
【ＦＩ】
　Ｇ０６Ｆ　12/14　　３２０Ｅ
　Ｇ０６Ｆ　 9/06　　５５０Ｚ
　Ｇ０６Ｆ　12/00　　５４６Ｋ
　Ｇ０６Ｆ　13/00　　３５４Ｚ
　Ｇ０９Ｃ　 5/00
　Ｈ０４Ｌ　11/20　　１０１Ｂ
　Ｈ０４Ｌ　11/26

【手続補正書】
【提出日】平成17年3月2日(2005.3.2)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】補正の内容のとおり
【補正方法】変更
【補正の内容】

手　続　補　正　書

平成１７年３月２日

特許庁長官　殿

１　事件の表示　　平成１０年　特許願　第５４１２７８号

２　補正をする者

名称　ブリティッシュ・テレコミュニケーションズ・パブリック・リミテッド・カンパニー

３　代理人

東京都千代田区霞が関３丁目７番２号

鈴榮特許綜合事務所内

〒１００－００１３

電話０３（３５０２）３１８１（大代表）

（５８４７）弁理士　鈴　江　武　彦

４　自発補正

５　補正により減少する請求項の数　１２

６　補正の対象

請求の範囲

７　補正の内容

請求の範囲を別紙の通り訂正する。

特許庁 17.3.2 出願支援課 窓口

請　求　の　範　囲

１．　サーバコンピュータ（１）からクライアントコンピュータ（３）へダウンロードされたデータを保護する方法であって、該方法は、

要求されたデータの保護されたコピーをサーバ（１）からクライアント（３）へダウンロードすることと、

クライアント（３）でプログラムを実行して、（ａ）該ダウンロードされたデータを非保護にしてそれによって該要求されたデータの非保護のコピーへのアクセスを提供し、かつ（ｂ）該要求されたデータの非保護コピーに関してクライアントコンピュータのコピー機能を抑制すること、とを含む。

２．　該要求されたデータの保護されたコピーは暗号により保護されている請求項１に記載の方法。

３．　該要求されたデータの保護されたコピーの完全性がハッシングにより達成される請求項２に記載の方法。

４．　クライアント（３）が該ダウンロードされたデータの受信を許されることを認証することを含む請求項１ないし請求項３のいずれか１項に記載の方法。

５．　該データが該クライアント（３）にダウンロードされる前に該サーバ（１）に対して該クライアント（３）を識別することを含む請求項１ないし請求項４のいずれか１項に記載の方法。

６．　該クライアント（３）へプログラムをダウンロードすることと、該クライアント（３）上の該ダウンロードされたプログラムを実行して、要求されたデータの保護されたコピーを含んでいるファイルをダウンロードする要求をサーバ（１）へアップロードするようにすることを含む請求項１ないし請求項５に記載の方法。

７．該ダウンロードされたプログラムは暗号キーに関するデータを含み、また前記方法は該暗号キーを用いて該ダウンロードされた暗号で保護されたデータを非保護の形態にすることを含む、請求項２に従属するときに、請求項６に記載の方法。

８．該ダウンロードされたプログラムが、該要求されたデータへのアクセスに対するより早く受信された要求に応じて、かつ該受信された要求に関してダウンロ

ードされる請求項６または請求項７に記載の方法。

９．　前記サーバ（１）とクライアント（３）とはそれぞれが暗号キーとそのクライアント（３）を独特に識別するための機械識別子とに対応するデータを保持していて、該方法は、

クライアント（３）へチャレンジを送って、そこに保持されているキーと機械識別子の暗号の関数としてサインを付した応答を生成するようにすることと、

該サーバ（１）と関係して保持されている暗号キーと機械識別子から該キーと該機械識別子の暗号の関数として対応するサインを付した応答を生成し、

該クライアント（３）と該サーバ（１）とからの該サインを付した応答を比較して、もし両者が対応していれば該キーでデータの暗号保護を実行することと、

該暗号で保護されたデータをクライアント（３）で該キーを用いて非保護の形態に変換することとを含む請求項１ないし請求項８のいずれか１項に記載の方法。

１０．　該データがステガノグラフィカルにマークを付したものである請求項１ないし９のいずれか１項に記載の方法。

１１．　該クライアント（３）を該サーバ（１）に登録することを含む請求項１ないし請求項１０のいずれか１項に記載の方法。

１２．　クライアント（３）の機械識別子をそのハードウエア又はそのソフトウエア構成の少なくとも一つを解析することにより判断することと、

該機械識別子を該サーバ（１）に送信することと、

該送信された機械識別子を暗号キーと組合わせてクライアント（３）についての独特な決定子を形成することと、

該独特な決定子をクライアント（３）に送信して、そこに記憶するようにし、後にサーバ（１）に対してクライアント（３）を識別するのに使用するようにして、サーバ（１）からそこへ暗号化されたデータをダウンロードできるようにすることと、を含む請求項１ないし請求項１１のいずれか１項に記載の方法。

１３．　保護された形態でのデータの組へのアクセスを提供するサーバ（１）であって、該サーバ（１）は、

データの組へのアクセス要求を受領する入力と、

該要求されたデータの組を保護する保護手段（１３、１４）と、

該アクセス要求をソースへ送信するためのプログラム部分を生成する生成手段（１５）とを含み、

前記プログラム部分は、使用時に、

該保護されたデータの組へのアクセス要求を生成し、

該保護されたデータの組の受領時に、該データの組を非保護の形態へ変換し、

前記非保護の形態のときに該データの組に関してコピー機能へのアクセスを選択的に制御するように動作する。

１４．サーバにインストールされて実行されたときに、請求項（１３）に記載のサーバ（１）の機能を実現するコンピュータプログラムを含むコンピュータプログラムキャリア媒体。

１５．サーバコンピュータ（１）からダウンロードされた要求されたデータの保護されたコピーに関してコンピュータプログラムを実行するクライアントコンピュータ（３）であって、該コンピュータプログラムは該クライアントコンピュータ（３）を制御して、（ａ）該ダウンロードされたデータを非保護にしてそれによって該要求されたデータの非保護のコピーへのアクセスを提供し、かつ（ｂ）該要求されたデータの非保護のコピーに関してクライアント（３）でのコピー機能を抑制する、ように構成されている。