平成１８年（行ケ）第１０４２４号　審決取消請求事件

平成１９年１０月３０日判決言渡，平成１９年１０月４日口頭弁論終結

判　　決

原　告　インターシア　ソフトウエア　エルエルシー

訴訟代理人弁理士　石川泰男，今井孝弘，奥和幸，伊藤嘉昭

被　告　特許庁長官　肥塚雅博

指定代理人　佐藤敬介，田口英雄，小池正彦，森山啓

主　　文

原告の請求を棄却する。

訴訟費用は，原告の負担とする。

この判決に対する上告及び上告受理の申立てのための付加期間を３０日と定める。

事実及び理由

第１　原告の求めた裁判

「特許庁が不服２００３－２３９２９号事件について平成１８年５月９日にした審決を取り消す。」との判決

第２　事案の概要

本件は，三菱商事株式会社（以下「三菱商事」という。）がした後記特許出願（以下「本願」という。）に対し拒絶査定がされたため，同社が，これを不服として審判請求をした後，出願人を原告とする出願人名義変更届が提出されたところ，同請求は成り立たないとの審決がされたため，原告が，その取消しを求める事案である。

１　特許庁における手続の経緯

(1)　本願（甲２）

出願人：三菱商事

発明の名称：「データ著作権管理システム及びデータ著作権管理装置」

出願番号：平成７年特許願第２２８３６６号

出願日：平成７年９月５日（先の出願に基づく優先権主張：平成６年９月３０日）

手続補正日：平成１５年９月１２日（以下「本件補正」という。）

拒絶査定日：平成１５年１０月２２日

(2)　審判請求手続等

審判請求日：平成１５年１２月１１日（不服２００３－２３９２９号）

原告を出願人とする出願人名義変更届の提出：平成１７年８月２日付け

審決日：平成１８年５月９日

審決の結論：「本件審判の請求は，成り立たない。」

審決謄本送達日：平成１８年５月２３日

２　発明の要旨

審決が対象とした本件補正後の請求項１の記載は，次のとおりである（以下，この請求項に係る発明を「本願発明」という。）。

【請求項１】

「データベースからユーザに暗号化データとして供給されるデータの著作権を管理する，そのような著作権管理システムと通信する端末装置であって，

前記著作権管理システムから第１秘密鍵及び第２秘密鍵の交付を受ける手段と，

前記ネットワーク，人工衛星，または記憶媒体を経由して暗号化データの供給を受ける手段と，

前記暗号化データが表示される場合に，前記第１秘密鍵を用いて暗号化データを復号データに復号する手段と，

前記第２秘密鍵を用いてその表示されたデータを再暗号化データへ暗号化する再暗号化手段と

から構成されることを特徴とする端末装置。」

３　審決の要点

審決は，本願発明は，後記引用発明及び周知技術に基づいて，当業者が容易に発

明をすることができたものであるから，特許法２９条２項の規定により特許を受けることができないとした。

(1)　関一則外３名による「暗号を利用した新しいソフトウエア流通形態の提案」（情報処理学会研究報告９３巻６４号（９３－ＩＳ－４５－3）１９～２８頁，１９９３年7月２０日）と題する論文（以下「引用例」という。甲１３）に記載された発明（以下「引用発明」という。）

「データベースからユーザに暗号化された画像データとして供給される画像データの著作権を管理する，画像データ・サーバと通信するコンピュータであって，

画像データ・サーバから秘密鍵の交付を受ける手段と，

ネットワークを経由して暗号化された画像データの供給を受ける手段と，

前記暗号化された画像データが表示される場合に，前記秘密鍵を用いて暗号化された画像データを復号する手段と，

から構成されることを特徴とするコンピュータ。」

(2)　本願発明と引用発明との対比

ア　一致点

「データベースからユーザに暗号化データとして供給されるデータの著作権を管理する，そのような著作権管理システムと通信する端末装置であって，

前記著作権管理システムから秘密鍵の交付を受ける手段と，

前記ネットワークを経由して暗号化データの供給を受ける手段と，

前記暗号化データが表示される場合に，前記秘密鍵を用いて暗号化データを復号データに復号する手段と，

から構成されることを特徴とする端末装置。」

イ　相違点

「【相違点１】　本願発明は，「第２秘密鍵を用いてその表示されたデータを再暗号化データへ暗号化する再暗号化手段」を有しているのに対して，引用発明は，再暗号化手段を備えていない点。

【相違点２】　本願発明は，「第１秘密鍵及び第２秘密鍵」の交付を受けているのに対して，引用発明は，「秘密鍵」の交付を受けている点。

【相違点３】　本願発明は，「ネットワーク，人工衛星，または記憶媒体」を経由して暗号化データの供給を受けるのに対して，引用発明は，「ネットワーク」を経由して暗号化データの供給を受けている点。」

(3)　相違点についての判断

「【相違点１】について

一般に，画像データに変更を加えること，及び，変更を加えた画像データを記録することは，普通に行われている慣用手段であるから，引用発明においても，このような手段をコンピュータに設けることは，単に慣用手段の附加であり，慣用手段を附加する際に，復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うことは，特開平４－１８１２８２号公報（以下「周知例１」という。甲１４）の１頁右下欄１０行目から２頁左上欄７行目に「〔従来の技術〕従来の暗号方式については暗号（コンピュータ・データ保護の新展開）第２７６ページから第３０６ページにおいて論じられている。これによれば，回線暗号は通信する電子計算機同士が共通の暗号鍵を有し，この暗号鍵に従って回線に送出するデータを暗号化し，受信側は該暗号鍵により同様に復号化することになっている。ファイル暗号はファイル対応にファイル鍵を生成し，この鍵に従ってファイル内データを暗号／復号化することになっている。ある電子計算機上のデータを他の電子計算機のファイルに安全に格納するためには次の処理が必要である。まず，回線暗号手順を用いて作成元電子計算機と格納先電子計算機間で暗号通信を行い，データを安全に転送する。次に，ファイル暗号手順を用いて，データを暗号化してファイルに格納することとなる。」，及び，特公昭６２－４２３０４号公報（以下「周知例２」という。甲１５）の４頁７欄３５行目から８欄４行目に「要求されるファイル＃ＸはキーコードＫ０を使用して，従来の方法で脱暗号化され，明確な文章にて，呼出しデータ２９を提供することができる。次いで，データは販売，預金，引出し等のようなデータ使用による処理を反映する新しいデータ変更を伴って，もしくは伴わずに，記憶手段に戻され，新しいキーコードＫ１を使用して，暗号化形態にて再記憶される。これは，キーコード発生装置２３を設定器３８により

再設定し，暗号化モジュール２１にキーコードＫ１を供給し，変更された或いはされないデータ３３をモジュール２１内でキーコードＫ１と共に暗号化を行なうことにより行われ得る。」と記載されているように周知であるから，引用発明に上記慣用手段を附加する際に上記周知技術を用いて，「第２秘密鍵を用いてその表示されたデータを再暗号化データへ暗号化する再暗号化手段」を附加するようにすることは，当業者が容易に想到し得ることである。

【相違点２】について

上記【相違点１】についてに記載したように，復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うことは周知であるし，秘密鍵の生成を著作権を管理するサーバ側で行うことは，著作権を管理する上では，そのように成されることが普通であるから，引用発明において，秘密鍵と秘密鍵とは異なる別の秘密鍵を端末装置で用いる際に，著作権を管理する側である画像データ・サーバで，秘密鍵と共に，秘密鍵とは異なる別の秘密鍵を生成し，端末装置に提供するようにし，それにより，秘密鍵と共に，秘密鍵とは異なる別の秘密鍵を受ける手段を端末装置に設けることは，当業者が容易に想到し得ることである。

【相違点３】について

デジタル情報の流通形態として，ネットワーク，人工衛星，または記憶媒体を用いることは，周知であるから，引用発明において，ネットワークの他に，人工衛星，または記憶媒体を用いることは，当業者が容易に想到し得ることである。」

(4)　むすび

「以上のとおり，本願発明は，引用発明及び周知技術に基づいて，当業者が容易に発明をすることができたものであるから，特許法２９条２項の規定により特許を受けることができない。」

第３　審決取消事由の要点

審決は，以下のとおり，周知例２を審決において初めて引用するという手続違背を犯した上，相違点１及び２についての各判断を誤った結果，本願発明が特許法２９条２項の規定により特許を受けることができないと判断したものであるから，取り消されるべきである。

１　取消事由１（手続違背）

周知例２（復号されたデータに対し暗号通信に用いた鍵とは異なる鍵によって再暗号化を行いデータ保管する管理技術が周知技術であることを示すもの）は，審査手続又は審判請求手続の段階で示されていたものではなく，審決において初めて引用されたものであるところ，かかる取扱いは，特許庁の審査基準に反するばかりか，三菱商事及び原告は，これらの手続段階において，周知例２に対する意見開陳の機会を与えられていないから，審決には，特許法１５９条２項において準用する同法５０条の規定に違反する手続違背がある。

２　取消事由２（相違点１についての判断の誤り）

審決は，復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うことは周知技術であり，当該周知技術に基づいて相違点１に係る本願発明の構成を採用することは当業者が容易に想到し得ることである旨判断したが，以下のとおり，この判断は誤りである。

(1)　本願発明の再暗号化手段において，表示されたデータを再暗号化データに暗号化するために使用される第２秘密鍵は，著作権管理システムから第１秘密鍵とともに交付を受けるものであるところ，審決は，復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うことは周知であると説示するのみであり，秘密鍵及びこれとは異なる別の秘密鍵の供給元については，何ら言及していない。

(2)　また，周知例１の記載をみても，同周知例には，２つの電子計算機間でデータを転送する際に使用する回線暗号鍵及びデータをファイルに格納する際に使用するファイル暗号鍵の２つの暗号鍵を使用することが開示されているが，これら２つの暗号鍵の供給元については，何ら開示も示唆もなく，同周知例によっても，これら２つの暗号鍵の供給元は不明であるというほかない。

他方，周知例２の記載をみると，同周知例には，データの脱暗号化に使用されるキー発生装置からのキーコードＫ０及びデータの暗号化に使用されるキー発生装置からのキーコードＫ１の２つのキーコードを使用することが開示されているが，こ

れら２つのキーコードは，コンピュータ内のキー発生装置自体から発生するものであり，これとは別個の管理サーバ側から供給されるものではない。したがって，引用発明に周知例２を組み合わせると，暗号化された画像データを復号するための秘密鍵（供給元・画像データ・サーバ）と復号化された画像データを再暗号化するためのキーコード（再暗号鍵。供給元・コンピュータ内のキー発生装置）とは，異なる供給元から交付されるという構成になってしまう。

(3)　これに対し，相違点１に係る本願発明の構成においては，第１秘密鍵と第２秘密鍵が同一の供給元（著作権管理システム）から交付されることにより，第１秘密鍵についての暗号化データ及び第２秘密鍵についての再暗号化データを著作権管理システムで一元的に管理することができるという，引用例に記載された事項から当業者が普通に予測することができない格別顕著な作用効果を奏するものである。

(4)　なお，被告は，審決が，第１秘密鍵と第２秘密鍵の供給元について，相違点２についての判断において説示している旨主張するが，「データを再暗号化する再暗号化手段」と，「第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵を用いること」という本願発明の特徴事項は，一体的なものであり，これを２つに分けて判断すべきではないから，相違点１における判断に当たっては，単に再暗号化手段を引用発明に付加することが容易であるか否かを判断するのではなく，第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵を用いてデータを再暗号化する再暗号化手段を引用発明に付加することが容易であるか否かについて判断すべきである。

(5)　以上のとおり，引用発明に周知例１及び２を適用しても，相違点１に係る本願発明の構成（「著作権管理システムから第１秘密鍵とともに交付を受けた第２秘密鍵を用いて，その表示されたデータを再暗号化データへ暗号化する再暗号化手段」）を採用することが，当業者が容易に想到し得るものということはできない。

３　取消事由３（相違点２についての判断の誤り）

審決は，秘密鍵の生成を著作権管理サーバ側で行うことが普通であると認定した

上で，著作権管理サーバ側で秘密鍵とともに当該秘密鍵とは異なる別の秘密鍵を生成して端末装置に提供するようにすることは当業者が容易に想到し得ることである旨判断したが，以下のとおり，この判断は誤りである。

(1)　端末装置で使用される別の秘密鍵（著作権管理サーバ側で生成する秘密鍵とは異なる別の秘密鍵）をどのように生成するかは，従来技術では解決されなかった問題であるから，秘密鍵の生成を著作権管理サーバ側で行うことが普通であるとしても，このことをもって直ちに，著作権管理サーバ側で秘密鍵とともに当該秘密鍵とは異なる別の秘密鍵を生成して端末装置に提供することが，当業者が容易に想到し得るものであるとはいえない（例えば，「ネットワーク利用秘密及び署名通信方法」と称する発明に関する甲１７（特開平５－６８０３４号公報）や，「共有鍵生成方式」と称する発明に関する甲１８（特開昭６３－２５０２３６号公報）には，鍵の生成を端末装置側で行うことが開示されている。）。

(2)　上記２(2)において主張したところによると，周知例１及び２を検討しても，著作権管理サーバ側で秘密鍵とともに当該秘密鍵とは異なる別の秘密鍵を生成して，端末装置に提供するようにすることが，当業者が容易に想到し得るものであるとはいえない。

また，周知例１には，２つの暗号鍵により暗号手順を行うのは効率が悪く，さらに，鍵管理を簡素化する必要があるため，回線暗号とファイル暗号を１つの暗号鍵により１回の暗号処理で行う旨の記載があるのであるから，周知例１に接した当業者にとって，引用発明の暗号手順に，効率が悪いとされる２つの暗号鍵による暗号手段をあえて組み合わせようとする動機付けは存在しないばかりか，逆に，これを引用発明の暗号手順に組み合わせようとしないのが当然であるといえるから，周知例１には，相違点２に係る本願発明の構成を採用することについての阻害要因が存在するといえる。

(3)　これに対し，相違点２に係る本願発明の構成においては，第１秘密鍵と第２秘密鍵が同一の供給元（著作権管理システム）から交付されることにより，第１

秘密鍵についての暗号化データ及び第２秘密鍵についての再暗号化データを著作権管理システムで一元的に管理することができるという，引用例に記載された事項から当業者が普通に予測することができない格別顕著な作用効果を奏するものである。

(4)　以上のとおり，引用発明に周知例１及び２を適用しても，相違点２に係る本願発明の構成を採用することが，当業者が容易に想到し得るものということはできない。

第４　被告の反論の骨子

以下のとおり，審決に手続違背はないし，相違点１及び２についての審決の判断にも誤りはない。

１　取消事由１（手続違背）に対して

審決によれば，周知例１及び２は，「復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うこと」が周知技術であることを示すために引用されたものであるところ，周知技術とは，文献等を例示するまでもなく，「当業者ならば当然知っているはずの事項」であって，審査手続又は審判請求手続において周知技術を用いる際，そのことについて意見書の提出や補正の機会を与えなくても，当業者である出願人又は審判請求人に対して不意打ちとなることはないから，上記周知技術に係る周知例２を審決で初めて引用したとしても，特許法１５９条２項において準用する同法５０条の規定に違反することはないと解するのが相当である。

２　取消事由２（相違点１についての判断の誤り）に対して

(1)ア　原告は，審決が，秘密鍵及びこれとは異なる別の秘密鍵の供給元について何ら言及していない旨主張するが，審決は，相違点２について，「引用発明において，秘密鍵と秘密鍵とは異なる別の秘密鍵を端末装置で用いる際に，著作権を管理する側である画像データ・サーバで，秘密鍵と共に，秘密鍵とは異なる別の秘密鍵を生成し，端末装置に提供するようにし，それにより，秘密鍵と共に，秘密鍵とは異なる別の秘密鍵を受ける手段を端末装置に設けることは，当業者が容易に想到し得ることである。」と判断しており，後記のとおり，相違点２についての審決の

判断に誤りはないから，原告の上記主張は失当である。

イ　原告は，本願発明の特徴事項である「データを再暗号化する再暗号化手段」と，「第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵を用いること」とは一体的なものであるから，相違点１の判断に当たっては，第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵を用いてデータを再暗号化する再暗号化手段を引用発明に付加することが容易であるか否かについて判断すべきである旨主張する。

しかしながら，原告が主張する上記本願発明の特徴事項は，相違点１及び２を併せたものであるところ，これを分説し，「第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵」及び「第２秘密鍵を用いてデータを再暗号化する再暗号化手段」として検討することは，相違点の認定判断を行う手法として，通常のものである。そして，審決が相違点１及び２についての各判断において説示したところを併せると，原告が主張する「第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵を用いてデータを再暗号化する再暗号化手段を引用発明に付加する」ことは，当業者が容易に想到し得ることであるといえる。

ウ　なお，原告が主張する本願発明の上記特徴事項について補足すると，データを再暗号化することは，単に一度復号化したものを再度暗号化する程度の技術であって慣用手段であり，その際に，復号に用いる秘密鍵と再暗号化に用いる秘密鍵を異なるものとするか，あるいは，秘密鍵を自装置で作成するか外部から入手するかはいずれも設計事項であり，また，１次ユーザが２次ユーザにデータを供給する際，２次ユーザに供給されたデータが，原データに１次ユーザが手を加えたものである場合には，原データの著作権と１次ユーザの２次的著作権が含まれるところ，このようにして生じた２次的著作権を原データの著作権と同じ場所で管理しようとすることは，普通に想到し得ることであるから，再暗号化データへ暗号化する際に，第２秘密鍵を用い，これを著作権管理システムから交付を受けるようにすることは，引用発明に，上記周知技術，慣用手段及び普通に想到される事項を組み合わせるこ

とにより，当業者が容易に想到し得るものであるといえる。

(2)　引用発明と周知例１又は２との各組合せに係る原告の主張及び本願発明の作用効果に係る原告の主張に対する被告の反論は，取消事由３に対する後記反論において主張するとおりである。

(3)　以上のとおりであるから，相違点１についての審決の判断に誤りはない。

３　取消事由３（相違点２についての判断の誤り）に対して

(1)　原告は，秘密鍵の生成を著作権管理サーバ側で行うことが普通であるとしても，このことをもって直ちに，著作権管理サーバ側で秘密鍵とともに当該秘密鍵とは異なる別の秘密鍵を生成して端末装置に提供することが，当業者が容易に想到し得るものであるとはいえない旨主張する。

しかしながら，秘密鍵の生成を著作権管理サーバ側で行うことが普通であることからすると，例えば，秘密鍵とは異なる別の秘密鍵を生成する必要がある場合，別の秘密鍵も秘密鍵であることに変わりはなく，また，上記２(1)ウにおいて主張したとおり，秘密鍵を自装置で作成するか外部から入手するかは設計事項であるし，１次ユーザが２次ユーザにデータを供給する場合に生じる２次利用による著作権の保護も当然求められるところ，秘密鍵とこれと異なる別の秘密鍵を同じ場所で管理しようとすることは普通のことであるから，当該別の秘密鍵の生成を著作権管理サーバ側で行うようにすることは，自然なことである。

そうすると，引用発明において，秘密鍵とともに当該秘密鍵とは異なる別の秘密鍵を用いる場合に，２つの秘密鍵の生成を著作権管理サーバ側で行うようにすること，すなわち，著作権管理サーバ側を２つの秘密鍵の供給元とすることは，当業者が容易に想到し得ることである。

(2)　原告は，相違点２に係る本願発明の構成においては，第１秘密鍵と第２秘密鍵が同一の供給元（著作権管理システム）から交付されることにより，第１秘密鍵についての暗号化データ及び第２秘密鍵についての再暗号化データを著作権管理システムで一元的に管理することができるという格別顕著な作用効果を奏するもの

である旨主張する。

しかしながら，まず，本願発明は，「端末装置」であり，本願発明の要旨には，「再暗号化手段からの出力」や「第１秘密鍵と第２秘密鍵とが同一のものであるか否か」について何ら特定する規定がないのであるから，端末装置である本願発明は，原告が主張するような上記作用効果を奏するものではない。

また，引用例には，引用発明が，ソフトウェア復号鍵の通信状況により著作権保護を可能にし，流通するデータの著作権を管理することができるものであることが記載されており，これは，本願発明の上記作用効果と同様のものであるといえる。

そうすると，引用発明において，秘密鍵とともにこれとは異なる別の秘密鍵を用いる場合に，両者の生成を著作権管理サーバ側で行うことにより，著作権管理システムで暗号化データ及び再暗号化データの両者を一元的に管理することができることは，引用例に記載された事項から普通に予測し得る作用効果であるといえる。

(3)ア　引用発明と周知例１又は２との各組合せに係る原告の主張は，審決に記載されたものではなく，原告独自の解釈を前提としているものであるから，誤りである。

イ　原告は，周知例１の記載によれば，これに接した当業者にとって，引用発明の暗号手順に，効率が悪いとされる２つの暗号鍵による暗号手段をあえて組み合わせようとする動機付けが存在しない旨主張するが，一般に，引用発明と周知例に記載された発明とを組み合わせる際，周知例に記載された発明の構成に１つの問題点があったとしても，他の有利な作用効果がある場合には，当該有利な作用効果に基づき，その組合せを採用することは常套手段である。そして，周知例１に，２つの暗号鍵による暗号手順は効率が悪いとする問題点が記載されているとしても，回線の暗号化，ファイルの再暗号化については，ともに暗号化されているという有利な作用効果があるものと認められるから，暗号化をするという点においては，引用発明に，周知例１に記載された周知技術を組み合わせる動機付けが存在するといえる。

また，原告は，周知例１には，２つの暗号鍵の供給元についての開示も示唆もな

い旨主張するが，秘密鍵の生成を著作権管理サーバ側で行うことは，普通のことであるから，周知例１に原告が主張するような開示又は示唆がないとしても，２つの暗号鍵の供給元を著作権管理サーバ側とすることは，当業者が容易に想到し得るものである。

ウ　原告は，周知例２の記載によれば，引用発明に周知例２を組み合わせると，暗号化された画像データを復号するための秘密鍵と，復号化された画像データを再暗号化するためのキーコードとが，異なる供給元から交付されるという構成になる旨主張するが，暗号鍵を著作権管理サーバから供給することと，これを端末装置内部で作成することとは，ともに周知技術であり，前者の構成を採用することは，当業者による通常の創作能力の発揮にすぎないから，引用発明に周知例２を組み合わせる際に，上記周知技術を採用し，コンピュータ内のキー発生装置に替えて，画像データ・サーバからキーコードを供給するようにすることは，当業者が容易に想到し得るものである。

(4)　以上のとおりであるから，相違点２についての審決の判断に誤りはない。

第５　当裁判所の判断

１　取消事由１（手続違背）について

(1)　掲記の証拠及び弁論の全趣旨によれば，以下の事実経過が認められる。

ア　三菱商事は，特許庁に対し，平成１４年１２月１６日，手続補正書（甲６）を提出し，これにより，本願に係る特許請求の範囲の請求項１は，本願発明に係る請求項１に変更された。

イ　特許庁審査官は，三菱商事に対し，平成１５年７月７日（起案日），拒絶理由を通知したが（甲７），うち，本願発明に係る拒絶の理由は，以下のとおりである。

「【C】この出願の下記の請求項に係る発明は，・・・特許法２９条２項の規定により特許を受けることができない。

記（・・・）

・請求項：１，６

・引用文献等：引用例，特開平５－２７６４７６号公報（以下「引用文献２」という。）

・備考

引用例には，ソフトウェア・サーバからソフトウェア復号鍵の交付を受ける手段と，ネットワークを介して暗号化されたソフトウェアの供給を受ける手段と，前記暗号化されたソフトウェアの実行に際して，前記ソフトウェア復号鍵を用いて前記暗号化されたソフトウェアを復号する手段とから構成された端末装置が記載されている。

引用文献２には，ビデオテープを介して供給されたスクランブル処理された映像信号をデスクランブラ装置でデスクランブル処理して通常の映像信号に戻して再生し，再生された映像信号にコピー禁止信号を付加する端末装置が記載されている。

そして，引用例，引用文献２が共に著作権を有する情報の無制限な流通を防止する技術について記載したものである点を勘案すれば，引用例に記載されている端末装置において，引用文献２に記載されているものを採用し，ソフトウェア使用後に著作権保護処理を新たに施すように構成することは，当業者が容易になし得たことであるし，著作権保護処理として暗号化処理が慣用されている点を考慮して，前記著作権保護処理を新たな鍵での暗号化処理とすることは，当業者が容易に想到しうることである。」

ウ　これに対し，三菱商事は，平成１５年９月１２日，意見書（甲８）とともに，本件補正に係る手続補正書（甲９）を特許庁に提出した。

エ　特許庁審査官は，平成１５年１０月２２日（起案日），本願について拒絶査定（甲１０）をしたが，その内容は，以下のとおりである。

「この出願については，平成１５年７月７日付け拒絶理由通知書に記載した理由【C】によって，拒絶をすべきものである。

・・・

備考

一　平成１５年９月１２日付けで提出された意見書・・・において出願人は，上記拒絶理由通知書で示した引用例及び引用文献２，特開平５－３３４３２４号公報（以下，「引用文献３」

という）について，

(1)引用例，引用文献２のいずれにおいても，本願請求項１の構成要素１「前記第２秘密鍵を用いてその表示されたデータを再暗号化データへ暗号化する再暗号化手段」に対する課題の認識，構成を示唆する記載は全くなく，これらの引用文献からいわゆる当業者が本願に容易に想到し得たものではなく，・・・である点，

(2)・・・，

(3)・・・，

をそれぞれ理由として，本願請求項１－３２に係る発明が特許性を有する旨を主張している。

そこで，前記理由(1)－(3)並びに前記主張について，以下で検討する。

二　まず，前記理由(1)－(3)が前記主張に対する正当な理由であるかを考える。

１　最初に前記理由(1)について検討する。

本願請求項１の構成要素１「前記第２秘密鍵を用いてその表示されたデータを再暗号化データへ暗号化する再暗号化手段」は，著作権を有する情報の無制限な流通を防止し著作権を保護する目的で構成されたものであり，その意味において引用例，引用文献２に記載されているものと課題を同じくすることは，上記拒絶理由通知書で述べるとおりである。

その著作権保護の技術として，引用文献２に記載されているものではデスクランブル処理により再生された映像信号に対しコピー禁止信号を付加する技術を採用しているが，著作権保護処理技術として暗号処理を使用し暗号化されたソフトウェアの自由な複製を認める技術思想は引用例に記載されているし，例えば，周知例１の〔従来の技術〕に記載されているように復号されたデータに対し暗号通信に用いたものとは異なる鍵によって再暗号化を行いデータ保管する管理技術は本出願前において常套手段であることを勘案すれば，引用例，引用文献２に記載されているものを組み合わせるに際し，著作権保護技術として暗号処理を採用する構成として前記構成要素１を想到することは，本出願前において周知慣用されている技術を鑑みれば，当業者が容易になし得る範疇を凌駕するものではない。

よって，前記理由(1)は本出願前の周知慣用技術を考慮して引用例，引用文献２に記載されているものを組み合わせることにより，当業者が容易になし得る構成であるから，前記主張を

根拠付ける正当な理由ではない。

２　次に前記理由(2)について検討するに，・・・。

・・・

３　最後に前記理由(3)について検討するに，・・・。

・・・

三　前記理由(1)－(3)が前記主張を根拠付ける正当な理由でないとしても，本願特許請求の範囲自体に前記主張を根拠付ける機能構成が開示されているのではないか問題となるも，上記拒絶理由通知書で示すように本願請求項１－３２に係る発明は，本出願前における周知慣用技術を考慮して引用例，引用文献２，３に記載されたものを組み合わせることで当業者が容易になし得るものであるから，前記主張を根拠付ける正当な理由とはならない。

四　・・・。」

オ　これに対し，三菱商事は，平成１５年１２月１１日，拒絶査定不服審判の請求（甲１１）をするとともに，平成１６年1月１３日付けの手続補正書（甲１２）において，引用例並びに引用文献２及び３に，上記拒絶査定で新たに引用された周知例１をも併せ，これらに係る詳細な反論を行った。

カ　特許庁審判合議体は，審決において初めて周知例２を引用し，前記のとおり，相違点１について，画像データに変更を加えること及び変更を加えた画像データを記録することのような慣用手段をコンピュータに付加する際に，「復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うこと」が，周知例１及び２に記載されているように周知である旨の認定をした上，引用発明に上記慣用手段を付加する際に上記周知技術を用いて，相違点１に係る本願発明の構成を付加するようにすることは，当業者が容易に想到し得ることである旨の判断をした。

(2)　特許庁審査官は，上記認定のとおり，三菱商事に対してした拒絶査定において初めて，周知例１を引用し，これを，「復号されたデータに対し暗号通信に用いたものとは異なる鍵によって再暗号化を行いデータ保管する管理技術」が常套手段であることの例示とし（なお，三菱商事又は原告に，周知例１に係る意見を述べ

る機会が実質的に与えられたことについては，原告も，これを争うものではない。），特許庁審判合議体は，審決において初めて，周知例２を引用し，周知例１及び２を，「復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うこと」が周知技術であることの例示としたものである。

以上の事実経過によれば，確かに，周知例２については，審査手続及び審判請求手続を通じ，三菱商事又は原告に，これに係る意見を述べる機会が与えられなかったものであるが，特許庁審判合議体は，拒絶査定の段階で既に三菱商事に対して示されていた周知例１によって認定した技術事項とおおむね同旨の技術事項を更に裏付ける証拠として，新たに周知例２を引用したにすぎないといえる。

そして，拒絶査定不服審判の請求がされる前の段階から，証拠を例示して周知技術（常套手段）とされてきた技術事項につき，これを更に裏付ける証拠を審決において新たに引用したとしても，それにより，従前から周知技術として示されていた技術事項とは別の技術事項を新たに周知技術として付加したり，従前から周知技術として示されていた技術事項を実質的に変更したりするものではないから，当該新たな証拠につき，出願人又は審判請求人に対して重ねて意見を述べる機会が与えられなかったとしても，特段の不意打ちとなるおそれはない。したがって，本件における上記事実経過によれば，特許庁審判合議体が，周知例２を審決において初めて引用したことをもって，特許法１５９条２項において準用する同法５０条の規定に違反する手続違背があったとはいえない。

(3)　以上のとおりであるから，審決に手続違背があるとする取消事由１は，理由がない。

２　取消事由３（相違点２についての判断の誤り）について

理解の便の観点から，取消事由２に先立ち，同３について判断する。

(1)　各刊行物に記載された技術事項

ア　引用例には，以下の各記載が存在する。

「現在あるいは今後においてデジタル情報としてその価値が非常に注目されているものの一

つにソフトウェアがあげられる。ソフトウェアは，・・・その価値が非常に高まっている一方，ユーザ間での複製が大きな問題となっている。・・・この際，ソフトウェアは単にネットワークを通して販売されるだけではなく，利用に対する課金，すなわちレンタル的概念が実現されることが，よりユーザ及び提供者のニーズに合った流通形態であると考えられる。（。（判決注，原文の誤記である。））

そこで著者は，本論文において暗号技術をソフトウェアに適用し，これらをレンタル的概念の基にネットワークを通じて流通され，ユーザ間での複製による流通経路をも大きな流通能力を持つ一つの正規の流通経路（に）できる新しいソフトウェア流通形態（及）を提案するとともに，その支援システムの構築について述べる。」（２０頁左欄２２行～右欄１行）

「ソフトウェアも・・・利用に対する課金が利用者・提供者双方から要求される商品であると考えられるが，現在の段階では所有に対する課金しか行なわれていない。なぜなら，ソフトウェアのレンタルはソフトウェアの流通を妨げている最も大きな要因である複製につながるからである。・・・今後は，複製を認めた上でこの複製による利用を効果的に管理することが必要になる・・・。

本システムでは，このようなコンセプトを実現するために，ソフトウェアは暗号化されて流通されるためにそのままの形では利用できないこととし，実行に際しては，その都度これを復号化することにより行う。ここで，復号に必要となる鍵をネットワークを介して提供者から得ることにより，ソフトウェアを利用する権利を与えられる。したがって，ユーザはネットワークを通して容易にソフトウェアを入手でき，復号鍵をレンタルすることにより利用に対する課金が実現される。暗号化されたソフトウェアに対しては，自由な複製を認め，複製による価値の混乱を防ぐ。」（２０頁右欄１８行～２１頁左欄２行）

「2.2.2　暗号アーキテクチャ

暗号アーキテクチャでは，ＤＥＳ(Data Encryption Standard)，ＲＳＡ暗号をサポートする・・・。

ソフトウェアの実行制御，すなわちソフトウェアの暗号化に用いられる暗号においては，・・・処理速度の高速性が要求される。したがって，高速な秘密鍵暗号法が適している。ＤＥＳ

は，秘密鍵暗号法の中で現在安全性や処理速度などを総合的に判断した上でもっとも実用的な暗号アルゴリズムで，各方面で実用化の方向にある。」（２１頁左欄１４～２３行）

「ユーザの認証やソフトウェアの復号鍵通信時の暗号化は，非常に多くのユーザに対して管理されなければならない。したがって，処理速度が低速でも鍵管理が容易な公開鍵暗号法が適している。公開鍵暗号法は，暗号化と複合化の鍵が異なるという性質をもつもので，一般的には暗号鍵を公開鍵，復号鍵を秘密鍵と呼ぶ。公開鍵は公開されるが，公開鍵から秘密鍵を導くことは不可能とされている。ＲＳＡ暗号は，・・・によって提案された画期的（的）な公開鍵暗号法で，公開鍵から秘密鍵を導かれることへの安全性は，素因数分解の困難性に基づいている。」（２１頁左欄３１行～右欄下から２９行）

「2.2.4　鍵管理アーキテクチャ

鍵管理アーキテクチャでは，秘密鍵暗号法であるＤＥＳと公開鍵暗号法であるＲＳＡ暗号の双方に対してデザインされる・・・。

ユーザが初回の利用時にソフトウェアの復号鍵を記録して入手してしまうと，次回からはこの鍵を使用することによって鍵の通信を省略し不正に利用することが出来る。したがって，そのソフトウェアの暗号・復号に使用される鍵をユーザに通信する場合には，ユーザに記憶されないようなメモリ上に記憶させて暗号・復号の処理を行わなければならないし，ソフトウェア提供者はこの鍵を自分以外には分からないように管理しなければならない。この概念は，現在考案されている全ての鍵管理アーキテクチャに共通の概念であり，鍵管理アーキテクチャから暗号アーキテクチャへの鍵の受渡しに関わる全てのプロトコルがブラック・ボックス化されていることが必要である。」（２１頁右欄下から３行～２２頁左欄１４行）

「2.2.7　ソフトウェア管理アーキテクチャ

ソフトウェア管理アーキテクチャは，多くのソフトウェア著作権者から提供されたソフトウェアを管理するために必要となる。ソフトウェア管理アーキテクチャによって管理される情報は，暗号化された流通状態のソフトウェア，ソフトウェア暗号鍵，ソフトウェア識別番号，ソフトウェア著作権者の個人情報である。・・・これらのソフトウェア暗号鍵，ソフトウェア識別番号，ソフトウェア著作権者の個人情報は，まとめてソフトウェア管理ファイルに保存され

る。」（２２頁右欄１～１４行）

「2.3.1　ソフトウェア登録プロセス

ソフトウェア登録プロセスでは，ソフトウェア提供者によるソフトウェアの登録を受け付けている。ここでの機能は，流通されるソフトウェアの暗号化とそれに伴うソフトウェア暗号鍵の生成，ソフトウェアに付加される認証子の生成，通信に際してソフトウェア暗号鍵の暗号化である。

ソフトウェアの暗号化　ソフトウェア著作権者によって流通されるソフトウェアが指定されると，鍵管理アーキテクチャによってこのソフトウェアの暗号に用いられるソフトウェア暗号鍵が生成される。次に，ソフトウェアとソフトウェア暗号鍵は暗号アーキテクチャに渡されてＤＥＳによって暗号化される。

認証子の生成　・・・。

鍵の暗号化　ソフトウェアの暗号化に用いられたソフトウェア暗号鍵は，提供者とソフトウェア・サーバ以外には秘密にしておかなければならないので，ソフトウェア・サーバの公開鍵で暗号化される。

これらの情報が通信アーキテクチャに渡され，ソフトウェアサーバに送られる。」（２２頁右欄３６行～２３頁右欄２０行）

「2.3.2　ソフトウェア・サーバ

ソフトウェア・サーバは，ソフトウェア提供者とユーザの間でソフトウェアの流通・鍵の管理と送信・各ユーザの利用状況の管理などの仲介を行う。これを設置することによって様々な著作権者やユーザに対してそれぞれ個別にアクセスするのではなく，このサーバにアクセスすることによってローカルなエリアでのシステムの稼働をよりスムースなものにしている。

ソフトウェア・サーバにはソフトウェア著作（権）者側にあるソフトウェア登録プロセスとの通信に関する動作と，ユーザ側で立ち上がるユーザ管理プロセスとの通信に関する動作の２種類の動作がある。

まず，ソフトウェア登録プロセスとの通信に関する動作を述べる・・・。

認証　・・・。

ソフトウェアの登録　認証が成功すると，ソフトウェア暗号鍵，ソフトウェア著作権者の個人情報をソフトウェア管理プロセスに渡す。

次に，ユーザ管理プロセスとの通信に関する動作について述べる・・・。

ソフトウェアの送信　ユーザ側にソフトウェアが存在せず，そのソフトウェアの送信要求を受け取ると，該当するソフトウェアを選びだし，ユーザにこのソフトウェアを送信する。ここで，送信されるソフトウェアは流通状態のソフトウェアである。

ソフトウェア暗号鍵の送信　ユーザからのソフトウェア実行の要求，すなわちソフトウェア復号鍵（暗号鍵と同じもの）の送信要求をソフトウェア・サーバが受け取ると，そのユーザの認証情報を認証アーキテクチャに渡す。認証アーキテクチャでユーザのエンティティ認証が成功すると，ソフトウェア管理ファイルに保存されているソフトウェア復号鍵を，実行要求を送信したユーザの公開鍵で暗号してからユーザ管理プロセスに送信する。」（２３頁右欄２１行～２４頁左欄１６行）

「2.4　ユーザ管理プロセス

ユーザ管理プロセスでは，ユーザーの認証とソフトウェアの実行，実行状況の制御・管理，これらに伴うソフトウェア・サーバとの通信を（を）行う。

ソフトウェアの実行　ソフトウェアが存在しなければソフトウェア・サーバに対してこのソフトウェアの送信要求を出し，ソフトウェアを受けとる。この際，ソフトウェア認証が行われる。ソフトウェアが存在すれば，ソフトウェア・サーバからソフトウェア復号鍵を受け取り，実行に移行する。」（２４頁左欄２２～３１行）

「3.3　応用例

本システムで流通される商品はソフトウェアに限らず基本的にはあらゆるデジタル情報を扱うことができる。そこで，我々は試作システムにおいてプログラムとしてのソフトウェア以外に一般で扱われているソフトと呼ばれるデジタル情報として，音声データ（例ＣＤソフト）と画像データ（例ビデオソフト，ＬＤソフト）の流通をサポートすることを試みた。」（２４頁右欄３６行～２５頁左欄４行）

「4.1　本システムのもたらす効果

・・・。

ソフトウェア著作権の保護　本システムではユーザ間でのコピーによって流通したソフトウェアが利用されても，ソフトウェアの復号鍵の通信状況によってユーザに課金することで，著作権の保護を可能にする。」（２５頁左欄３６行～右欄４行）

イ　「ファイルの暗号方式」と称する発明に関する周知例１には，以下の各記載が存在する。

「〔産業上の利用分野〕

本発明は電子計算機のファイルの保管方法に関し，特に，通信回線で接続された別の電子計算機にデータを暗号化して保管する方法に関する。」（１頁右欄６～９行）

「〔従来の技術〕

従来の暗号方式については暗号（コンピュータ・データ保護の新展開）・・・において論じられている。

これによれば，回線暗号は通信する電子計算機同士が共通の暗号鍵を有し，この暗号鍵に従って回線に送出するデータを暗号化し，受信側は該暗号鍵により同様に復号化することになっている。

ファイル暗号はファイル対応にファイル鍵を生成し，この鍵に従ってファイル内データを暗号／復号化することになっている。

ある電子計算機上のデータを他の電子計算機のファイルに安全に格納するためには次の処理が必要である。まず，回線暗号手順を用いて作成元電子計算機と格納先電子計算機間で暗号通信を行い，データを安全に転送する。次に，ファイル暗号手段を用いて，データを暗号化してファイルに格納することとなる。」（１頁右欄１０行～２頁左上欄７行）

「〔発明が解決しようとする課題〕

上記従来技術は，ファイルサーバ方式などのような通信回線を介してファイルをアクセスするファイル制御の暗号方式について配慮されておらず，次のような問題点があった。

(1)回線上のデータ保護のために，ワークステーションからファイルサーバあるいはファイルサーバからワークステーションへのデータ送信の度に回線暗号を行い，また，ファイル保護の

ために，ファイルサーバにおいてファイルのデータの格納あるいはデータの読みだしの度にファイル暗号を行う必要がある。このように，回線暗号とファイル暗号を重複して行う必要があり，処理効率が悪い。

(2)暗号鍵管理は機密上，システム管理者がファイルサーバ上で厳格に行う必要がある。しかし，ファイルサーバの利用の利用形態からみて鍵をユーザが厳格に行うことは期待できない。故に，鍵管理者を簡素化する必要がある。」（２頁左上欄８行～右上欄６行）

「〔課題を解決するための手段〕

・・・各ワークステーションのみがファイルデータを暗号／復号化し，ファイルサーバは暗号化されたデータを直接ファイルに書き込み，あるいは，読みだしするようにしたものである。

また，暗号鍵管理も各ワークステーションで行い，管理を局所化したものである。」（２頁右上欄１２～１９行）

ウ　「フアイル呼出し機密の保護方法および装置」と称する発明に関する周知例２には，以下の各記載が存在する。

「この形式の体系は特に銀行業，預金出納の操作について有用である。」（３頁５欄４０～４１行）

「作動方法について説明すると，特定フアイルを呼出そうとする個人や機関Ｒはキーボード１３を介して，個人識別番号（PIN），特定フアイルに関する情報等を入力する。・・・メモリ１７内のフアイルは全て最初にキーコード発生装置２３からのキーコードＫ０と共に，暗号化モジユール２１内にフアイルデータを暗号化することにより，従来の方法・・・で暗号化される。

定められた権限２５によつて，特定のフアイル＃Ｘを呼出すことができるが，該フアイル＃Ｘを脱暗号化するには正確なキーコードを必要とする。・・・要求されたフアイル＃ＸはキーコードＫ０を使用して，従来の方法で脱暗号化され，明確な文章にて，呼出しデータ２９を提供することができる。次いで，データは販売，預金，引出し等のようなデータ使用による処理を反映する新しいデータ変更３１を伴つて，もしくは伴わずに，記憶手段に戻され，新しいキーコードＫ１を使用して，暗号化形態にて再記憶される。これは，キーコード発生装置２３を

設定器３８により再設定し，暗号化モジユール２１にキーコードＫ１を供給し，変更された或いはされないデータ３３をモジユール２１内でキーコードＫ１と共に暗号化を行なうことにより行われ得る。」（４頁７欄１行～８欄４行）

(2)ア　原告は，端末装置で使用される別の秘密鍵（著作権管理サーバ側で生成する秘密鍵とは異なる別の秘密鍵）をどのように生成するかは，従来技術では解決されなかった問題であるから，秘密鍵の生成を著作権管理サーバ側で行うことが普通であるとしても，このことをもって直ちに，著作権管理サーバ側で秘密鍵とともに当該秘密鍵とは異なる別の秘密鍵を生成して端末装置に提供することが，当業者が容易に想到し得るものであるとはいえない旨主張する。

イ　そこで検討するに，上記(1)イのとおり，周知例１には，暗号方式に係る従来の技術として，複数の電子計算機が回線暗号のための共通の暗号鍵を有し，うち，データの作成元の電子計算機がデータを回線に送出する際には，この暗号鍵を用いてデータを暗号化し（回線暗号），受信側であるデータの格納先の電子計算機は，同じ暗号鍵を用いてこれを復号化した上，データを安全に格納するため，ファイル対応に生成された別の暗号鍵を用いてデータを暗号化する（ファイル暗号）との技術が開示されており，また，周知例２には，上記(1)ウのとおり，特定のファイルを呼び出そうとする個人等が当該ファイルに関する情報等を入力すると，キーコード発生装置が生成したキーコードＫ０により暗号化された特定のファイル＃Ｘを呼び出すことができ，当該ファイル＃Ｘは，キーコードＫ０を使用して脱暗号化され，呼出しデータが得られるが，当該呼出しデータは，データ使用による処理を反映する新しいデータ変更を伴って，又はこれを伴わずに，記憶手段に戻され，キーコード発生装置が生成した新しいキーコードＫ１を用いて暗号化され，再記憶されるとの技術が開示されている。

そうすると，審決が認定したとおり，復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うことは，本願前から周知の技術であったものと認めるのが相当である。

ウ　そして，引用発明においては，上記(1)アのとおり，秘密鍵（ソフトウェア暗号鍵）は，ソフトウェア登録プロセス（ソフトウェア提供者によるソフトウェアの登録を受け付けるプロセスであって，著作権を管理するシステムの側に属するものであることは明らかである。）において生成された後，ソフトウェア・サーバに送られ，ソフトウェア・サーバにおいて管理及びユーザへの交付が行われ（この点に関しては，審決も，引用発明の「ソフトウェア・サーバ」が本願発明の「著作権管理システム」に相当するとした上，「前記著作権管理システムから秘密鍵の交付を受ける手段と，・・・から構成されることを特徴とする端末装置。」を本願発明と引用発明の一致点として認定したところであり，原告も，この認定を争っていない。），これにより，ソフトウェア著作権の保護が可能になるとされているのであるから，秘密鍵を著作権管理システム側において生成し，管理し，及びユーザへ交付することは，著作権保護の観点からは，極めて当然のことといえる。

エ　そうすると，引用発明に上記周知技術を適用するに際し，著作権保護（特に，ユーザの２次著作権の保護）の観点から，復号に用いる秘密鍵（本願発明の「第１秘密鍵」）と異なる別の秘密鍵（本願発明の「第２秘密鍵」）についても，これを著作権管理システム側において生成し，管理し，及びユーザへ交付することは，当業者であれば，格別の困難なく行い得たものといえる。

オ　したがって，原告の上記主張を採用することはできない。

(3)ア　原告は，周知例１及び２にそれぞれ記載された２つの暗号鍵の供給元が著作権管理サーバでないことを理由に，引用発明に周知例１及び２を適用しても，著作権管理サーバ側で秘密鍵とともに当該秘密鍵とは異なる別の秘密鍵を生成して端末装置に提供するようにすることは，当業者が容易に想到し得るものではない旨主張する。

しかしながら，上記(2)イにおいて説示したとおり，周知例１及び２は，「復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うこと」が，本願前から周知の技術であったものと認定する証拠として援用されたものであり，当該２つの秘

密鍵の供給元に関する何らかの技術事項を認定する証拠として援用されたものではないから，原告の上記主張は，審決が周知例１及び２によって認定した事実の内容を正解しないものとして，失当であるといわざるを得ない。

イ　また，原告は，周知例１には，２つの暗号鍵により暗号手順を行うのは効率が悪く，さらに，鍵管理（者）を簡素化する必要があるため，回線暗号とファイル暗号を１つの暗号鍵により１回の暗号処理で行う旨の記載があるのであるから，周知例１に接した当業者にとって，引用発明の暗号手順に，効率が悪いとされる２つの暗号鍵による暗号手段をあえて組み合わせようとする動機付けは存在しないばかりか，逆に，これを引用発明の暗号手順に組み合わせようとしないのが当然であるといえるから，周知例１には，相違点２に係る本願発明の構成を採用することについての阻害要因が存在する旨主張する。

しかしながら，上記アにおいて説示したとおり，周知例１は，「復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うこと」が，本願前から周知の技術であったものと認定する証拠として援用されたものであり，しかも，上記(1)イのとおり，この認定は，原告が上記主張において援用する周知例１に記載された発明（周知例１に記載された特許請求の範囲の請求項１ないし３によって規定される発明）が採用する技術に基づいてされたものではなく，周知例１に記載された従来技術に基づいてされたものであるから，原告の上記主張は，上記アと同様，審決が周知例１によって認定した技術事項を正解しないものとして，失当である。

ウ　さらに，原告は，相違点２に係る本願発明の構成においては，第１秘密鍵と第２秘密鍵が同一の供給元（著作権管理システム）から交付されることにより，第１秘密鍵についての暗号化データ及び第２秘密鍵についての再暗号化データを著作権管理システムで一元的に管理することができるという，引用例に記載された事項から当業者が普通に予測することができない格別顕著な作用効果を奏するものである旨主張する。

しかしながら，上記(2)において説示したとおり，引用発明に上記周知技術を適

用するに際し，復号に用いる秘密鍵（本願発明の「第１秘密鍵」）と異なる別の秘密鍵（本願発明の「第２秘密鍵」）についても，これを著作権管理システム側において生成し，管理し，及びユーザへ交付することは，当業者であれば，格別の困難なく行い得たものといえるところ，このような構成を採用することにより，第１秘密鍵についての暗号化データ及び第２秘密鍵についての再暗号化データを著作権管理システムで一元的に管理することができるとの作用効果を奏することは，当該構成の内容に照らし，当然かつ自明のことといえ，当業者が予測することのできる範囲を超えるものでないことは明らかであるから，かかる作用効果を格別顕著なものと評価することはできない。

したがって，原告の上記主張も，これを採用することができない。

(4)　以上のとおりであるから，相違点２についての判断の誤りをいう取消事由３は，理由がない。

３　取消事由２（相違点１についての判断の誤り）について

(1)　原告は，審決が秘密鍵及びこれと異なる別の秘密鍵の供給元について言及していないこと並びに周知例１及び２にそれぞれ記載された２つの暗号鍵の供給元が著作権管理サーバでないことを理由に，引用発明に周知例１及び２を適用しても，当業者が，相違点１に係る本願発明の構成に容易に想到し得るものではない旨主張する。

しかしながら，審決が認定したとおり，復号に用いる秘密鍵と異なる別の秘密鍵を用いて暗号化を行うことが，本願前から周知の技術であったことは，上記２(2)イにおいて説示したとおりであるところ，上記２(3)アにおいて説示したとおり，周知例１及び２は，上記技術が本願前から周知の技術であったものと認定する証拠として援用されたものであり，２つの秘密鍵の供給元に関する何らかの技術事項を認定する証拠として援用されたものではないから，原告の上記主張は，審決が周知例１及び２によって認定した事実の内容を正解しないものとして，失当である。

(2)　また，原告は，相違点１に係る本願発明の構成においては，第１秘密鍵と

第２秘密鍵が同一の供給元（著作権管理システム）から交付されることにより，第１秘密鍵についての暗号化データ及び第２秘密鍵についての再暗号化データを著作権管理システムで一元的に管理することができるという，引用例に記載された事項から当業者が普通に予測することができない格別顕著な作用効果を奏するものである旨主張する。

しかしながら，かかる作用効果について，当業者が予測することのできる範囲を超える格別顕著なものと評価することができないことは，上記２(3)ウにおいて説示したとおりであるから，原告の上記主張を採用することはできない。

(3)　さらに，原告は，「データを再暗号化する再暗号化手段」と，「第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵を用いること」という本願発明の特徴事項は，一体的なものであり，これを２つに分けて判断すべきではないから，相違点１における判断に当たっては，単に再暗号化手段を引用発明に付加することが容易であるか否かを判断するのではなく，第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵を用いてデータを再暗号化する再暗号化手段を引用発明に付加することが容易であるか否かについて判断すべきである旨主張する。

そこで検討するに，原告の主張の全趣旨に照らせば，原告の上記主張にいう「第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵」は，「『第１秘密鍵と同様に著作権管理システムから交付を受けた』第２秘密鍵」との趣旨であると解されるところ，上記２(2)において説示したとおり，第１秘密鍵のみならず，第２秘密鍵についても，これを著作権管理システム側において生成し，管理し，及びユーザへ交付することは，当業者であれば，格別の困難なく行い得たものである。そして，審決は，相違点２についての判断において，これと同趣旨の判断をしているところ，仮に，原告が主張するように，「第２秘密鍵が『第１秘密鍵と同様に著作権管理システムから交付を受けた』ものであること」を相違点１についての判断として判断するとしても，これが，当業者であれば格別の困難なく行い得たもので

あることは，前記のとおりであるし，また，原告は，取消事由２として，第２秘密鍵の供給元に係る主張をするにとどまり，「第２秘密鍵を用いてその表示されたデータを再暗号化データへ暗号化する再暗号化手段を付加すること」自体については，これが容易に想到し得るものではないとの具体的な主張をしないのであるから，結局，原告が主張するような「一体的な判断」をするとしても，相違点１に係る本願発明の構成を採用することは当業者が容易に想到し得るものであるとした審決の結論を左右するものではない。

なお，原告の上記主張にいう「第１秘密鍵とともに著作権管理システムから交付を受けた第２秘密鍵」が，「『第１秘密鍵と同時に』著作権管理システムから交付を受けた第２秘密鍵」との趣旨であるとすれば，本願発明の要旨は，第１秘密鍵及び第２秘密鍵が同時に交付されるか否かについて何ら規定するものではないから，相違点１の判断に当たり，「『第１秘密鍵と同時に』著作権管理システムから交付を受けた第２秘密鍵を用いること」についても判断すべきであるとの主張は，本願発明の要旨に基づかないものとして，失当であるというべきである。

したがって，原告の上記主張は，いずれにせよ，これを採用することができない。

(4)　以上のとおりであるから，相違点１についての判断の誤りをいう取消事由２は，理由がない。

４　結論

以上によれば，審決取消事由はいずれも理由がないから，原告の請求を棄却することとし，主文のとおり判決する。

知的財産高等裁判所第４部

裁判長裁判官　　田　　中　　信　　義

裁判官　　古　閑　裕　二

裁判官　　浅　井　憲