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

特許第4560051号
(P4560051)

(45)発行日　平成22年10月13日(2010.10.13)　(24)登録日　平成22年7月30日(2010.7.30)

(51)Int.Cl.　　F I
*G06Q 50/00 (2006.01)*　　G06F 17/60 142
*H04L 9/08 (2006.01)*　　H04L 9/00 601B
　　H04L 9/00 601E

請求項の数 40　(全 24 頁)

(21)出願番号　特願2006-537968 (P2006-537968)
(86)(22)出願日　平成16年7月30日 (2004.7.30)
(65)公表番号　特表2007-510219 (P2007-510219A)
(43)公表日　平成19年4月19日 (2007.4.19)
(86)国際出願番号　PCT/US2004/024640
(87)国際公開番号　WO2005/046100
(87)国際公開日　平成17年5月19日 (2005.5.19)
審査請求日　平成19年7月30日 (2007.7.30)
(31)優先権主張番号　10/697,916
(32)優先日　平成15年10月29日 (2003.10.29)
(33)優先権主張国　米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ジョン　ジェラルド　スピアー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】権利管理保護されたコンテンツのプレライセンス供与

(57)【特許請求の範囲】
【請求項１】
プリンシパルが保護されたメッセージコンテンツに対して実行することができる操作のタイプを制限する権利管理サーバと、メッセージコンテンツを受信し、該メッセージコンテンツをプリンシパル、または該プリンシパルのエージェントに提供するメッセージサーバとを含むメッセージングシステムにおいて、プリンシパルに、前記プリンシパルが前記権利管理サーバへのアクセスを有さない場合にメッセージコンテンツへのアクセスを許すために、権利管理の対象である該メッセージコンテンツのプレライセンス供与を行う方法であって、
権利管理サーバとは異なる前記メッセージサーバによって、送信コンピューティングシステムからメッセージの少なくとも一部分へのアクセスが権利管理サーバを介して制御されるという点で権利管理の対象であるメッセージを受信する動作と、前記メッセージサーバは前記メッセージが権利管理の対象であることを認識しており、
前記メッセージサーバによって、前記送信コンピューティングシステムから前記メッセージの少なくとも一部分が権利管理の対象であることを識別する権利表現を含んだ発行ライセンスを受信する動作と、前記権利表現は権利管理の対象である前記メッセージの少なくとも一部分についての一つ又は複数の意図された受領者を特定し及び前記一つ又は複数の意図された受領者の各々についての１つ又は複数の権利を特定し、そして前記権利表現は前記メッセージの共有、転送、印刷、及び再ライセンスの少なくとも１つについて１つ又は複数のプリンシパルの操作を制限し、前記発行ライセンスは前記権利管理サーバから

前記送信コンピューティングシステムによって前もって獲得されているものであり、
前記メッセージサーバが前記メッセージは権利管理の対象であることを認識した場合、前記メッセージサーバによって前記１つまたは複数のプリンシパルのために、前記１つまたは複数のプリンシパルに前記メッセージへのアクセスを許すための少なくとも１つの使用ライセンスを要求する動作であって、前記要求は、前記権利管理サーバに対して権利管理の対象である前記メッセージの少なくとも一部を識別する前記発行ライセンスを含む動作と、
前記権利管理サーバは、前記メッセージサーバにその後に権利管理サーバへアクセスすることなく権利管理の対象である前記メッセージの少なくとも一部をアクセスすることを１つ又は複数のプリンシパルに許可する少なくとも１つの使用ライセンスを発行し、
前記メッセージサーバによって前記１つまたは複数のプリンシパルのために、前記少なくとも１つの使用ライセンスを受信して、前記１つまたは複数のプリンシパルが、前記メッセージサーバから少なくとも１つの使用ライセンスを獲得して、前記権利管理サーバから前記少なくとも１つの使用ライセンスを要求する必要なしに、権利管理の対象である前記メッセージの少なくとも一部分にアクセスすることができるようにする動作と、
前記メッセージサーバによって、１つ又は複数の前記プリンシパルの少なくとも１つに前記少なくとも１つの使用ライセンスの１つ又は複数を提供する動作と、
前記プリンシパルによって、前記メッセージサーバから、前記プリンシパルが権利管理サーバにアクセスを有しない時に前記使用ライセンスに従いコンテンツにアクセスできるように前記使用ライセンス及び前記コンテンツを受信する動作と、
を含み、
前記少なくとも１つのプリンシパルは、プロセス、ユーザ、マシン、サーバ、またはクライアントであることを特徴とする方法。
【請求項２】
前記権利管理サーバを介して制限される前記メッセージの前記少なくとも一部分は、暗号化され、前記使用ライセンスは、暗号化されている前記メッセージの前記一部分を解読するのに使用されるコンテンツキーを含むことを特徴とする請求項１に記載の方法。
【請求項３】
暗号化されている前記メッセージの前記一部分は、保護された連絡先、保護されたドキュメント、保護された予定表のアイテム、または保護された会合要求の少なくとも１つであることを特徴とする請求項２に記載の方法。
【請求項４】
少なくとも１つの使用ライセンスを要求する前記動作は、前記権利管理サーバに認証を送信して、前記メッセージサーバが、前記１つまたは複数のプリンシパルに代行して前記少なくとも１つの使用ライセンスを獲得する権限を有することを確認する動作をさらに含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記メッセージサーバは、前記１つまたは複数のプリンシパルのために複数の使用ライセンスを要求して、前記１つまたは複数のプリンシパルが、複数のマシン上で前記メッセージにアクセスすることができるようにすることを特徴とする請求項１に記載の方法。
【請求項６】
前記少なくとも１つの使用ライセンスは、前記メッセージサーバによって前記メッセージとは別個に格納されることを特徴とする請求項１に記載の方法。
【請求項７】
前記発行ライセンスは、前記１つまたは複数のプリンシパルへの参照を含み、前記メッセージサーバが前記少なくとも１つの使用ライセンスを要求した場合、前記１つまたは複数のプリンシパルが前記メッセージへのアクセスを有することが意図されていることを前記権利管理サーバが検証することができるようにすることを特徴とする請求項１に記載の方法。
【請求項８】

前記発行ライセンスは、前記１つまたは複数のプリンシパルが前記メッセージの複製に対して実行することが許される操作のタイプを制限する少なくとも１つの権利表現をさらに含むことを特徴とする請求項７に記載の方法。

【請求項９】

前記権利表現は、読み取り専用の既定値であることを特徴とする請求項８に記載の方法。

【請求項１０】

前記発行ライセンス中の少なくとも１つの前記権利表現は、前記メッセージの印刷の前記１つまたは複数のプリンシパルの操作を制限するものであることを特徴とする請求項７に記載の方法。

【請求項１１】

前記権利表現は、前記少なくとも１つの権利表現が利用できる回数または期間の少なくとも１つを制限する有効期限の機能を含むことを特徴とする請求項１０に記載の方法。

【請求項１２】

前記発行ライセンスは、前記メッセージが変わっていないことを確認するのに使用されるハッシュ、および前記発行ライセンスが有効であることを確認するのに使用される前記権利管理サーバによる署名の１つまたは複数をさらに含むことを特徴とする請求項１に記載の方法。

【請求項１３】

前記発行ライセンスは、前記メッセージの宛先である複数のプリンシパルを参照し、前記メッセージサーバは、前記権利管理サーバにかかる負荷を分散させるために、前記複数のプリンシパルのために使用ライセンスをバッチ要求プロセスによって取得することを特徴とする請求項１に記載の方法。

【請求項１４】

プリンシパルが保護されたメッセージコンテンツに対して実行することができる操作のタイプを制限する権利管理サーバと、メッセージコンテンツを受信し、該メッセージコンテンツをプリンシパル、または該プリンシパルのエージェントに提供するメッセージサーバとを含むメッセージングシステムにおいて、プリンシパルに、前記プリンシパルが前記権利管理サーバへのアクセスを有さない場合にメッセージコンテンツへのアクセスを許すために、権利管理の対象である該メッセージコンテンツのプレライセンス供与を行う方法であって、

メッセージサーバによって送信コンピューティングシステムからメッセージ及び発行ライセンスを受信するステップと、前記メッセージは保護されたコンテンツを含み、

送信コンピューティングシステムから受信された前記メッセージが、前記メッセージの少なくとも一部分へのアクセスが権利管理サーバを介して制御されるという点で権利管理の対象である保護されたコンテンツを含むことを前記メッセージサーバによって判定するステップと、前記権利管理サーバは１つ又は複数のプリンシパルが権利管理の対象である前記メッセージの少なくとも一部にアクセスすることを許可する１つ又は複数のユーザ・ライセンスを発行し、

前記メッセージサーバにより送信コンピユーティングシステムから受信した前記メッセージが保護されたコンテンツを含むと判定される際、前記メッセージサーバによって少なくとも１つの使用ライセンスを権利管理サーバから要求するステップと、前記発行ライセンスは前記権利管理サーバから前記送信コンピューティングシステムによって前もって獲得されており、

前記権利管理サーバは前記メッセージサーバに、１つ又は複数のプリンシパルが権利管理サーバへその後のアクセスをすることなしに、権利管理の対象である前記メッセージの少なくとも一部へアクセスすることを許可する１つ又は複数の使用ライセンスを発行するステップと、

を含み、

前記権利管理サーバとは異なる前記メッセージサーバによって、前記権利管理サーバか

ら１つ又は複数のプリンシパルのために、前記少なくとも１つの使用ライセンスを獲得するステップと、前記使用ライセンスは前記プリンシパルが前記権利管理サーバにアクセスを有しない時に前記使用ライセンスに従って前記コンテンツにアクセスすることを与えるものであり、

前記少なくとも１つのプリンシパルは、プロセス、ユーザ、マシン、サーバ、またはクライアントである

ことを特徴とする方法。

【請求項１５】

前記権利管理サーバを介して制限される前記メッセージの前記少なくとも一部分は、暗号化され、前記使用ライセンスは、暗号化されている前記メッセージの前記一部分を解読するのに使用されるコンテンツキーを含むことを特徴とする請求項１４に記載の方法。

【請求項１６】

暗号化されている前記メッセージの前記一部分は、保護された連絡先、保護されたドキュメント、保護された予定表のアイテム、または保護された会合要求の少なくとも１つであることを特徴とする請求項１５に記載の方法。

【請求項１７】

前記少なくとも１つの使用ライセンスを獲得するためのステップは、前記メッセージサーバによって前記１つまたは複数のプリンシパルのために、前記少なくとも１つの使用ライセンスを要求する動作を含み、前記要求は、前記権利管理サーバに対して前記メッセージを明らかにするための前記受信された発行ライセンスを含み、前記要求は、前記メッセージサーバが、前記１つまたは複数のプリンシパルのために前記少なくとも１つの使用ライセンスを獲得する権限を有することを確認するための前記権利管理サーバに対する認証証明書を含むことを特徴とする請求項１４に記載の方法。

【請求項１８】

前記受信された発行ライセンスは、前記メッセージサーバが少なくとも１つの使用ライセンスを要求した時、前記権利管理サーバが前記１つまたは複数のプリンシパルを前記メッセージにアクセスする意図を有効化できるように前記１つ又は複数のプリンシパルへの参照を含むことを特徴とする請求項１７に記載の方法。

【請求項１９】

前記発行ライセンスは、前記メッセージの前記１つまたは複数のプリンシパルによって前記メッセージを転送することを制限する少なくとも１つの権利表現を含むことを特徴とする請求項１８に記載の方法。

【請求項２０】

前記発行ライセンス中の少なくとも１つの前記権利表現は、前記１つまたは複数のプリンシパルの再ライセンスの操作を制限することを含むことを特徴とする請求項１８に記載の方法。

【請求項２１】

前記権利表現は、前記少なくとも１つの権利表現が利用できる回数を制限する有効期限の機能を含むことを特徴とする請求項２０に記載の方法。

【請求項２２】

前記権利表現は、読み取り専用の既定値であることを特徴とする請求項１８に記載の方法。

【請求項２３】

前記メッセージサーバは前記１つ又は複数のプリンシパルのために複数の使用ライセンスをユーザ別に又はマシン別に発行されることを要求し、前記１つ又は複数のプリンシパルは複数のマシン上の前記メッセージをアクセスできるようにしたことを特徴とする請求項１４に記載の方法。

【請求項２４】

前記少なくとも１つの使用ライセンスは前記メッセージとは別にして前記メッセージサーバにより格納されることを特徴とする請求項１４に記載の方法。

【請求項２５】
前記受信された発行ライセンスは、前記メッセージが変わっていないことを確認するのに使用されるハッシュ、および前記発行ライセンスが有効であることを確認するのに使用される前記権利管理サーバによる署名の１つまたは複数をさらに含むことを特徴とする請求項１４に記載の方法。
【請求項２６】
前記受信された発行ライセンスは、前記メッセージの宛先である複数のプリンシパルを参照し、前記メッセージサーバは、前記権利管理サーバにかかる負荷を分散させるために、前記複数のプリンシパルのために使用ライセンスをバッチ要求プロセスによって取得することを特徴とする請求項１４に記載の方法。
【請求項２７】
プリンシパルが保護されたメッセージコンテンツに対して実行することができる操作のタイプを制限する権利管理サーバと、メッセージコンテンツを受信し、該メッセージコンテンツをプリンシパル、または該プリンシパルのエージェントに提供するメッセージサーバとを含むメッセージングシステムにおいて、プリンシパルに、前記プリンシパルが前記権利管理サーバへのアクセスを有さない場合にメッセージコンテンツへのアクセスを許すために、権利管理の対象である該メッセージコンテンツのプレライセンス供与を行う方法を実施するコンピュータ実行可能命令を含むコンピュータプログラムであって、前記方法は、
権利管理サーバとは異なる前記メッセージサーバによって、送信コンピューティングシステムからメッセージの少なくとも一部分へのアクセスが権利管理サーバを介して制御されるという点で権利管理の対象であるメッセージを受信する動作と、前記メッセージサーバは前記メッセージが権利管理の対象であることを認識しており、
前記メッセージサーバによって、前記送信コンピューティングシステムから前記メッセージの少なくとも一部分が権利管理の対象であることを識別する権利表現を含んだ発行ライセンスを受信する動作と、前記権利表現は権利管理の対象である前記メッセージの少なくとも一部分についての一つ又は複数の意図された受領者を特定し及び前記一つ又は複数の意図された受領者の各々についての１つ又は複数の権利を特定し、そして前記権利表現は前記メッセージの共有、転送、印刷、及び再ライセンスの少なくとも１つについて１つ又は複数のプリンシパルの操作を制限し、前記発行ライセンスは前記権利管理サーバから前記送信コンピューティングシステムによって前もって獲得されているものであり、
前記メッセージサーバが前記メッセージは権利管理の対象であることを認識した場合、前記メッセージサーバによって前記１つまたは複数のプリンシパルのために、前記１つまたは複数のプリンシパルに前記メッセージへのアクセスを許すための少なくとも１つの使用ライセンスを要求する動作であって、前記要求は、前記権利管理サーバに対して権利管理の対象である前記メッセージの少なくとも一部を識別する前記発行ライセンスを含む動作と、
前記権利管理サーバは、前記メッセージサーバにその後に権利管理サーバへアクセスすることなく権利管理の対象である前記メッセージの少なくとも一部をアクセスすることを１つ又は複数のプリンシパルに許可する少なくとも１つの使用ライセンスを発行し、
前記メッセージサーバによって前記１つまたは複数のプリンシパルのために、前記少なくとも１つの使用ライセンスを受信して、前記１つまたは複数のプリンシパルが、前記メッセージサーバから少なくとも１つの使用ライセンスを獲得して、前記権利管理サーバから前記少なくとも１つの使用ライセンスを要求する必要なしに、権利管理の対象である前記メッセージの少なくとも一部分にアクセスすることができるようにする動作と、
前記メッセージサーバによって、１つ又は複数の前記プリンシパルの少なくとも１つに前記少なくとも１つの使用ライセンスの１つ又は複数を提供する動作と、
前記プリンシパルによって、前記メッセージサーバから、前記プリンシパルが権利管理サーバにアクセスを有しない時に前記使用ライセンスに従いコンテンツにアクセスできるように前記使用ライセンス及び前記コンテンツを受信する動作と、

を含み、
前記少なくとも１つのプリンシパルは、プロセス、ユーザ、マシン、サーバ、またはクライアントである
ことを特徴とするコンピュータプログラム。
【請求項２８】
前記発行ライセンスは、前記１つまたは複数のプリンシパルへの参照を含み、前記メッセージサーバが前記少なくとも１つの使用ライセンスを要求した場合、前記１つまたは複数のプリンシパルが前記メッセージへのアクセスを有することが意図されていることを前記権利管理サーバが検証することができるようにすることを特徴とする請求項２７に記載のコンピュータプログラム。
【請求項２９】
前記発行ライセンスは、コピーと委託の少なくとも１つを制限する少なくとも１つの権利表現をさらに含むことを特徴とする請求項２８に記載のコンピュータプログラム。
【請求項３０】
前記発行ライセンスの中の前記少なくとも１つの権利表現は、保存中の前記１つまたは複数のプリンシパルの操作を、制限することを特徴とする請求項２８に記載のコンピュータプログラム。
【請求項３１】
前記権利表現は、前記少なくとも１つの権利表現が利用できる回数または期間の少なくとも１つを制限する有効期限の機能を含むことを特徴とする請求項３０に記載のコンピュータプログラム。
【請求項３２】
前記権利表現は、読み取り専用の既定値であることを特徴とする請求項２８に記載のコンピュータプログラム。
【請求項３３】
前記発行ライセンスは、前記メッセージの宛先である複数のプリンシパルを参照し、前記メッセージサーバは、前記権利管理サーバにかかる負荷を分散させるために、前記複数のプリンシパルのために使用ライセンスをバッチ要求プロセスによって取得することを特徴とする請求項２７に記載のコンピュータプログラム。
【請求項３４】
プリンシパルが保護されたメッセージコンテンツに対して実行することができる操作のタイプを制限する権利管理サーバと、メッセージコンテンツを受信し、該メッセージコンテンツをプリンシパル、または該プリンシパルのエージェントに提供するメッセージサーバとを含むメッセージングシステムにおいて、プリンシパルに、前記プリンシパルが前記権利管理サーバへのアクセスを有さない場合にメッセージコンテンツへのアクセスを許すために、権利管理の対象である該メッセージコンテンツのプレライセンス供与を行う方法を実施するコンピュータ実行可能命令を含むコンピュータプログラムであって、前記方法は、
メッセージサーバによって送信コンピューティングシステムからメッセージ及び発行ライセンスを受信するステップと、前記メッセージは保護されたコンテンツを含み、
送信コンピューティングシステムから受信された前記メッセージが、前記メッセージの少なくとも一部分へのアクセスが権利管理サーバを介して制御されるという点で権利管理の対象である保護されたコンテンツを含むことを前記メッセージサーバによって判定するステップと、前記権利管理サーバは１つ又は複数のプリンシパルが権利管理の対象である前記メッセージの少なくとも一部にアクセスすることを許可する１つ又は複数のユーザ・ライセンスを発行し、
前記メッセージサーバにより送信コンピューティングシステムから受信した前記メッセージが保護されたコンテンツを含むと判定される際、前記メッセージサーバによって少なくとも１つの使用ライセンスを権利管理サーバから要求するステップと、前記発行ライセンスは前記権利管理サーバから前記送信コンピューティングシステムによって前もって獲

得されており、
前記権利管理サーバは前記メッセージサーバに、１つ又は複数のプリンシパルが権利管理サーバへその後にアクセスをすることなしに、権利管理の対象である前記メッセージの少なくとも一部へアクセスすることを許可する１つ又は複数の使用ライセンスを発行するステップと、
前記権利管理サーバとは異なる前記メッセージサーバによって、前記権利管理サーバから１つ又は複数のプリンシパルのために、前記少なくとも１つの使用ライセンスを獲得するステップと、前記使用ライセンスは前記プリンシパルが前記権利管理サーバにアクセスを有しない時に前記使用ライセンスに従って前記コンテンツにアクセスすることを与えるものであり、
前記少なくとも１つのプリンシパルは、プロセス、ユーザ、マシン、サーバ、またはクライアントである
ことを特徴とするコンピュータプログラム。
【請求項３５】
前記権利管理サーバを介して制限される前記メッセージの前記少なくとも一部分は、暗号化され、前記使用ライセンスは、暗号化されている前記メッセージの前記一部分を解読するのに使用されるコンテンツキーを含み、暗号化されている前記メッセージの前記一部分は、保護された連絡先、保護されたドキュメント、保護された予定表のアイテム、または保護された会合要求の少なくとも１つであることを特徴とする請求項３４に記載のコンピュータプログラム。
【請求項３６】
前記少なくとも１つの使用ライセンスを獲得するためのステップは、前記メッセージサーバによって前記１つまたは複数のプリンシパルのために、前記少なくとも１つの使用ライセンスを要求する動作を含み、前記要求は、前記権利管理サーバに対して前記メッセージを明らかにするための前記受信された発行ライセンスを含み、前記要求は、前記メッセージサーバが、前記１つまたは複数のプリンシパルのために前記少なくとも１つの使用ライセンスを獲得する権限を有することを確認するための前記権利管理サーバに対する認証を含むことを特徴とする請求項３４に記載のコンピュータプログラム。
【請求項３７】
前記メッセージサーバは、前記１つまたは複数のプリンシパルのために複数の使用ライセンスをユーザ別に又はマシン別に発行されることを要求して、前記１つまたは複数のプリンシパルが、複数のマシン上で前記メッセージにアクセスすることができるようにすることを特徴とする請求項３４に記載のコンピュータプログラム。
【請求項３８】
前記少なくとも１つの使用ライセンスは、前記メッセージサーバによって前記メッセージとは別にして格納されることを特徴とする請求項３４に記載のコンピュータプログラム。
【請求項３９】
前記受信された発行ライセンスは、少なくとも１つの権利表現をさらに含み、前記権利表現は、前記少なくとも１つの権利表現が利用できる回数を制限する有効期限の機能を含むことを特徴とする請求項３４に記載のコンピュータプログラム。
【請求項４０】
前記受信された発行ライセンスは、前記メッセージの宛先である複数のプリンシパルを参照し、前記メッセージサーバは、前記権利管理サーバにかかる負荷を分散させるために、前記複数のプリンシパルのために使用ライセンスをバッチ要求プロセスによって取得することを特徴とする請求項３４に記載のコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、権利管理システムにおける保護されたコンテンツの配信に関する。

より詳細には、本発明は、プリンシパルが権利管理サーバへのアクセスを有さない場合に、プリンシパル（principal）にコンテンツへのアクセスを許すために、権利管理の対象であるコンテンツのプレライセンス供与を行うこと(prelicensing)を可能にする。

【背景技術】

【０００２】

権利管理サービス（ＲＭＳ）は、電子コンテンツの所有権／著作権を、そのコンテンツに関して許可された受信者がどのようなアクションを行うことができるかを制限することによって保護するソフトウェアを提供する。コンテンツという用語は、ピクチャ、ムービー、ビデオ、音楽、プログラム、マルチメディア、ゲーム、ドキュメントなどを含め、デジタル形式で格納された情報およびデータを指す。ＲＭＳの主要な機能のいくつかは、ライセンスを獲得している許可された中間ユーザまたはエンドユーザだけがコンテンツをロック解除することができるようにライセンス許可を管理すること、また、購入の条件、またはライセンスの条件、または別の形で作成者によって課せられた条件（例えば、許されるコピー回数、再生回数、ライセンスが有効であることが可能な時間間隔または期間、あるいはさらに配布すること、開くこと、またはアクセスすること、印刷することなどの、コンテンツに対して実行することができるアクション）に従ってコンテンツ使用を制限することである。ＲＭＳの別の機能は、コンテンツの無許可コピーの出所を明らかにして、違法コピーとさらに闘うことであることが可能である。

【０００３】

最初、権利管理の考えは、デジタルの雑誌、書籍、写真、教育資料、ビデオ、音楽などの、市販される資料のオンライン違法コピーから守るために使用された。しかし、権利管理の使用は、ビジネスネットワーク内の独自（ｐｒｏｐｒｉｅｔａｒｙ）情報および機密情報を保護するためにビジネス環境においてますます普及している。例えば、大企業のＣＥＯが、企業秘密を含む電子メールを配信することを所望することが可能である。しかし、その情報の機密性のため、ＣＥＯは、そのメッセージに対して受信者が行うことができるアクションを制限することを所望することが可能である。例えば、ＣＥＯは、上位レベルの経営陣が、機密情報を読み取ること、コピーすること、印刷すること、および保存することを許すが、読み取り専用アクセス、またはまったくアクセスがないことに他の従業員を制限することを所望する可能性がある。したがって、ＲＭＳの使用を介して、ＣＥＯは、誰が保護されたメッセージを見ることを許可されるか、そのメッセージに関してその人がどのようなアクションを行うことができるかを指定することができる。

【０００４】

以上は、ビジネスネットワーク環境においてコンテンツを管理することの重要さの多くの例の１つを示すに過ぎない。権利管理は、ビジネス環境において人気の高いツールになりつつあるが、現在、このシステムにはいくつかの欠点および欠陥が存在する。例えば、通常、保護されたコンテンツの受信者は、保護されたコンテンツを開き、使用するために、ＲＭＳサーバから使用ライセンスを獲得することを要求される。しかし、ユーザが、遠隔の場所にいる場合、またはそれ以外でＲＭＳサーバへのアクセスを有さない場合、ユーザは、ライセンスを獲得することができない可能性がある。そのような事例は、従業員が、保護された電子メールを自分のラップトップにダウンロードし、後に、ネットワークに接続されていないときに、例えば、移動しているときにそのアイテムを開く場合に生じる可能性がある。代替として、ＲＭＳサーバ内部の機微なキーをネットワーク外部の者から保護する企業ポリシーが、確立されていることも可能である。したがって、企業は、遠隔の場所にいる従業員にＲＭＳサーバへのアクセスを許さない可能性がある。このため、遠隔の場所に向かう前に保護されたコンテンツをあらかじめダウンロードした、または、それ以外で、例えば、メッセージサーバを介して保護されたコンテンツを受信する遠隔ユーザは、ＲＭＳサーバから許可を得ることができないために、そのコンテンツにアクセスすることができない可能性がある。

【０００５】

現行の権利管理サービスの別の欠点は、ＲＭＳサーバにかかる負荷を分散させることに

関するコントロールが限られていることである。したがって、ＲＭＳは、使用ライセンスを求める要求の過負荷のために障害を生じる可能性がある。例えば、大企業が、保護されたコンテンツを従業員の全員に送信し、従業員の全員が、ほぼ同時に使用ライセンスを獲得しようと試みた場合、ＲＭＳサーバが圧倒され（ｏｖｅｒｗｈｅｌｍｅｄ）、障害を生じる可能性がある。

【０００６】

したがって、ユーザがＲＭＳサーバへのアクセスを有さない場合に、ユーザに保護されたコンテンツへのアクセスを許すことを可能にするための方法、システム、およびコンピュータプログラム製品の必要性が存在する。さらに、ＲＭＳサーバにかかる負荷を絞り、ＲＭＳサーバが扱うことができるペースでバッチ要求をもたらすようにする必要性が存在する。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

従来のシステムには上述したような種々の問題があり、さらなる改善が望まれている。

【０００８】

本発明は、このような状況に鑑みてなされたもので、その目的とするところは、権利管理保護されたコンテンツのプレライセンス供与を可能にする方法を提供することにある。

【課題を解決するための手段】

【０００９】

本発明の典型的な諸実施形態によれば、現在の権利管理サービスシステムの以上に明らかにした欠点および欠陥が克服される。例えば、典型的な諸実施形態は、保護されたコンテンツに対してプリンシパルが実行することができる操作のタイプを制限する権利管理サーバ、およびメッセージを受信し、そのメッセージをプリンシパル、またはプリンシパルのエージェントに提供するメッセージサーバを有するメッセージングシステムを提供する。さらに、本発明は、プリンシパルが権利管理サーバへのアクセスを有さない場合に、プリンシパルにコンテンツへのアクセスを許すために、権利管理の対象であるコンテンツのプレライセンス供与を行うこと（ｐｒｅ－ｌｉｃｅｎｓｉｎｇ）を提供する。例えば、メッセージサーバが、メッセージの少なくとも一部分へのアクセスが、権利管理サーバを介して制限されているという点で、権利管理の対象であるメッセージを受信することが可能である。次に、メッセージサーバは、権利管理サーバに対してメッセージを明らかにするのに使用するための発行ライセンスを受信することができる。さらに、メッセージサーバは、プリンシパルに代行して、プリンシパルにメッセージへのアクセスを許すための１つまたは複数の使用ライセンスを要求することができる。要求は、メッセージを権利管理サーバに明らかにする発行ライセンスを含むことが可能である。

【００１０】

本発明の別の典型的な実施形態によれば、プリンシパルが権利管理サーバへのアクセスを有さない場合に、プリンシパルにコンテンツへのアクセスを許すために、権利管理の対象であるコンテンツのプレライセンス供与を行うメッセージングシステムが提供される。このシステムは、メッセージの少なくとも一部分へのアクセスが、権利管理サーバを介して制限されるという点で、受信されたメッセージが権利管理を受けると判定する。システムは、権利管理サーバにメッセージを明らかにするために、受信された発行ライセンスを使用する。メッセージサーバが、プリンシパルに権利管理サーバから使用ライセンスを要求させることなしに、プリンシパルにメッセージへのアクセスを許すため、プリンシパルに代行して使用ライセンスを獲得する。

【００１１】

本発明のさらなる特徴および利点は、以下の説明に記載し、一部は、その説明から明白となるか、あるいは、本発明の実施によって知ることができる。本発明の特徴および利点は、添付の特許請求の範囲において特に指摘する手段および組合せを使用して実現し、得ることができる。本発明の以上、およびその他の特徴は、以下の説明、および添付の特許

請求の範囲からより十分に明白となるか、あるいは、以下に記載する本発明の実施によって知ることができる。

【００１２】

本発明の前述した利点および特徴、ならびにその他の利点および特徴を得ることができる仕方を説明するため、以上に簡単に説明した本発明のより詳細な説明を、添付の図面に示す本発明の特定の諸実施形態を参照して行う。それらの図面は、本発明の典型的な諸実施形態を例示するに過ぎず、したがって、本発明の範囲を限定するものと考えられるべきでないものと理解して、本発明を、添付の図面の使用を介してさらに具体的に、さらに詳細に記述し、説明する。

【発明を実施するための最良の形態】

【００１３】

本発明は、権利管理保護されたコンテンツのプレライセンス供与のための方法、システム、およびコンピュータプログラム製品を範囲に含む。本発明の諸実施形態は、以下により詳細に説明する、様々なコンピュータハードウェアを含む専用または汎用のコンピュータを含むことが可能である。

【００１４】

典型的な諸実施形態は、プレライセンス供与プロセスを提供することにより、他の権利管理サービスシステムの欠陥を克服するための方法、システム、およびコンピュータプログラム製品を提供する。したがって、保護されたコンテンツ（例えば、電子メールの添付ファイル）を開くために使用ライセンスを獲得することを所望するプリンシパルは、権利管理サービス（ＲＭＳ）サーバにアクセスする必要なしに、そうすることができる。以下の実施例は、メッセージングシステム（すなわち、メッセージサーバを介して保護されたメッセージコンテンツを送信するプロセス）の文脈で説明するが、本発明は、共有フォルダ、インスタントメッセージングおよび／またはテキストメッセージングなどの、他の形態の保護されたコンテンツにも適用できる可能性がある。このため、プレライセンス供与プロセスのための本明細書で説明する実施例は、例示のために使用されるに過ぎず、本発明の範囲を限定することを意図するものではない。

【００１５】

権利管理サービスに参加するため、プリンシパルはまず、登録されなければならない。一般に、プリンシパルという用語は、言及する機能を実行することができるユーザ、プロセス、マシン、サーバ、クライアント、または他の任意のデバイスまたは事物を包含するように広く解釈されるものとする。ただし、特定のタイプのプリンシパルが所望される諸実施形態が存在する。例えば、図１Ａの登録プロセスに関して以下により詳細に説明するとおり、ロックボックスｄｌｌを受け取ることによって登録するのは、通常、マシンである。これに対して、図１Ｂに示す登録プロセスに関連して、ユーザまたはサーバは、通常、登録済みのマシン上で権利管理アカウント証明書（ＲＡＣ）を受け取ることにより登録する。したがって、本発明の典型的な諸実施形態を特定のタイプのプリンシパルの文脈で説明するが、それでも、プリンシパルという用語は、以上に説明した広い意味を保持しなければならない。

【００１６】

図１Ａは、登録１００プロセスにおける通常の第１のアクションの実施例を強調する。プリンシパル１２０（詳細には、クライアントまたはマシン）がまず、ロックボックスサーバ１１０から適切なソフトウェアを獲得しなければならない。したがって、プリンシパル１２０は、ロックボックス要求１０１をロックボックスサーバ１１０に送信し、そのマシンに固有のデータをロックボックスサーバ１１０に提供する。より詳細には、提供される情報は、マシンの物理的特性、例えば、プロセッサ速度、ＣＰＵシリアル番号、ネットワークアドレスなどであることが可能である。ロックボックスサーバ１００は、その固有データを使用してロックボックスｄｌｌ１１５を構築し、１０２においてプリンシパル１２０によって受信される。以下により詳細に説明するとおり、アクセスを制限してコンテンツを保護するのはロックボックスｄｌｌ１１５である。さらに、ロックボックスｄｌｌ

１１５は、マシンからの固有データを使用して構築されたため、マシン固有であり、その特定のマシン上でだけ機能するようになっている。ロックボックス１１５は、マシンが実行される際にマシンの特性について調べることができる。

【００１７】

今やプリンシパル１２０は、保護されたコンテンツにアクセスするソフトウェアを有するので、プリンシパル１２０（詳細には、ユーザまたはサーバ）は、プリンシパル１２０が利用することを所望する各権利管理サービス（ＲＭＳ）サーバに登録する。例えば、プリンシパル１２０が、特定のビジネスネットワークに関する権利管理サービスに参加することを所望する場合、プリンシパル１２０は、そのシステムに関するＲＭＳサーバに登録する。つまり、特定のＲＭＳから管理されるコンテンツにアクセスするのに、プリンシパルは、そのＲＭＳサーバに対して自らを明らかにする。本発明では、ＲＭＳサーバは、１つまたは複数のＲＭＳサーバを表わし、登録以外のいくつかの対話（例えば、以下に説明するとおり、発行ライセンスまたは使用ライセンスを獲得すること）も、利用可能なＲＭＳサーバ群のいずれかにアクセスすることが可能であることに留意されたい。

【００１８】

図１Ｂは、プリンシパル登録１００プロセスにおいてどのようにプリンシパル１２０、すなわち、ユーザまたはサーバが、ＲＭＳサーバ１２５に登録することができるかの実施例を示す。第１に、プリンシパル１２０は、ＲＭＳサーバ１２５に解読キーを要求する１０３。プリンシパルは、基本的プロトコル、ケルベロス（Ｋｅｒｂｅｒｏｓ）プロトコル、Ｘ５０９証明書プロトコル、Ｐａｓｓｐｏｒｔプロトコルなどの多くの慣用の認証プロトコルのいずれか１つ、ＲＭＳサーバに対して自らを明らかにすることができる。プリンシパル１２０は、通常、ＲＭＳサーバ１２５から、権利アカウント証明書（ＲＡＣ）を受け取り１０４、ＲＡＣは、プリンシパル１２０を権利管理サービスにおける信頼される参加者として後に明らかにするのに使用することができる。プリンシパル１２０は、ＲＭＳサーバ１２５から秘密キー１３０も受け取る。秘密キー１３０は、通常、トランスポート中にキー１３０を秘密に保つように要求１０３の中で提供されるキーを使用して暗号化される。以下に説明するとおり、秘密キー１３０は、ＲＭＳサーバ１２５によって、保護されたコンテンツを解読するのにプリンシパル１２０が使用するコンテンツキーを暗号化するのに使用される。したがって、プリンシパル１２０が、保護されたコンテンツを受信すると、ロックボックスｄｌｌ１１５は、コンテンツの真正性を確認し、コンテンツキーを取り出して解読し、プリンシパル１２０のためにコンテンツを開くことができる。

【００１９】

この時点で、プリンシパル１２０は、権利管理サービスに参加する準備ができる。保護されたコンテンツを送信することにより、または保護されたコンテンツを解読しようと試みることで権利管理に参加することを所望するいずれのプリンシパルも、通常、同様なユーザ登録１００ルーチンを経る。保護されたコンテンツを送信するプリンシパルは、登録してからでないとコンテンツを公開することができないが（以下により詳細に説明するとおり）、プリンシパルは、ＲＭＳシステムに登録されておらずに、保護されたコンテンツを受信することができることに留意されたい。それでも、保護されたコンテンツを受信した未登録のプリンシプルは、登録してからでないと、保護されたコンテンツを解読することができない。したがって、未登録のプリンシプルは、保護されたコンテンツにアクセスしようと試みると、登録するように誘導されることが可能である。

【００２０】

保護されたコンテンツのプレライセンス供与を行う典型的な諸実施形態を図３Ａ～３Ｄに関連して以下に説明する。これに対して、図２Ａ～Ｃは、保護されたコンテンツの送信側２１０およびプリンシパル２４０が、プリンシパルがＲＭＳサーバへのアクセスを有する場合に、どのように権利管理プロセスに参加することができるかの実施例を示す。第１に、図２Ａに示すとおり、送信側は、保護されたコンテンツ２２０とともにプリンシパル２４０に送信する発行ライセンス２０２を獲得しなければならない。したがって、送信側２１０は、コンテンツを暗号化し、ＲＭＳ２１５から発行ライセンスを求める要求２０１

を行う。この要求２０１は、権利表現、ＲＭＳサーバの公開キーに暗号化されたコンテンツキー、コンテンツのハッシュなどを含むことが可能である。権利表現は、通常、保護されたコンテンツが誰を宛先としているか、およびそのコンテンツの受信者が何を行うことができるかを指定する。コンテンツキー（図示せず）は、保護されたコンテンツを暗号化する／解読するのに使用されるように送信側２１０によって通常、作成される対称キーである。一実施形態は、ＲＭＳサーバ２１５が、コンテンツキーをデータベース（図示せず）の中に保存することができるようにし、そのキーをサーバ２１５は、後に、以下に説明する使用ライセンスプロセスにおいてプリンシパル２４０に送信する。（代替として、以下により詳細に説明するとおり、ＲＭＳサーバ２１５は、コンテンツキーの暗号化されたバージョンを発行ライセンス２０２の中に含めてもよい。）最後に、ハッシュを後に使用して、それぞれのロックボックスｄｌｌ２４５によって受け取られ、開かれた際に、コンテンツが変わらないことを確認することができる。

【００２１】

発行ライセンスを求める要求２０１を受信した後、次に、ＲＭＳサーバ２１５は、ＲＭＳサーバによって署名された、暗号化された情報であることが可能な発行ライセンス２０２を作成することができる。情報は、単に、権利表現、コンテンツキー、コンテンツキー識別子、および／またはコンテンツのハッシュの任意の組合せであることが可能である。したがって、ＲＭＳサーバ２１５は、発行ライセンス２０２、および使用ライセンス（以下に説明する）を求める要求２０３を後に受信すると、ＲＭＳサーバ２１５が、発行ライセンス２０２を作成したサーバであると保証されることが可能である。

【００２２】

前述したとおり、ＲＭＳサーバは、コンテンツキーを格納するか、またはコンテンツキーの暗号化されたバージョンを発行ライセンス２０２の中に含めることができる。ＲＭＳサーバは、コンテンツキーを格納する場合、以下に説明するとおり、使用ライセンスを発行する際、コンテンツキー識別子を使用して、ＲＭＳサーバのデータベースの中でコンテンツキーを探し出す。代替として、発行ライセンス２０２が、例えば、ＲＭＳサーバ２１５の公開キーに暗号化されたコンテンツキーを含む。ＲＭＳサーバは、以下に説明する諸実施形態に従って、後に、使用ライセンスを発行する際にコンテンツキーを解読することができる。いずれにしても、コンテンツキー識別子という用語が様々な実施形態において使用される場合、この用語は、コンテンツキーの識別子、コンテンツキーの暗号化されたバージョン、またはコンテンツキーを獲得するのに使用される他の任意の手段を含むように広く解釈されなければならない。

【００２３】

その後、送信側２１０が、発行ライセンス２０２を受け取り、次に、このライセンス２０２を送信側２１０は、保護されたコンテンツ２２０に付加してプリンシパル２４０に送信することができる。これは、通常、１回限りの操作であり、通常、送信者が保護されたコンテンツを送信しようと最初に試みる際に行われる。図２Ｂは、保護されたメッセージ２２０および発行ライセンス２０２が、どのように送信側２１０からプリンシパル２４０に送信されることが可能であるかの高レベルの概略を示す。送信側２１０は、単に、発行ライセンス２０２を保護されたメッセージ２２０に付加し、メッセージ２２０を送信側２１０のメッセージサーバ２２５に転送することができる。次に、送信側のメッセージサーバ２２５が、適切なプリンシパルのメッセージサーバ２３０を探し出し、保護されたメッセージ２２０および発行ライセンス２０２をそのプリンシパルのメッセージサーバ２３０に転送する。プリンシパル２４０が、プリンシパル２４０のメッセージサーバ２３０にログオンすると、プリンシパルのメッセージサーバ２３０が、保護されたメッセージ２２０および発行ライセンス２０２をプリンシパル２４０に送信する。

【００２４】

プリンシパル２４０は、そのメッセージを保護されたメッセージとして認識し、ＲＭＳサーバ２１５から使用ライセンス２０４を獲得しようと試みることができる。図２Ｃは、プリンシパル２４０がＲＭＳサーバ２１５へのアクセスを有する場合に、使用ライセンス

２０４を獲得するためにプリンシパル２４０が経ることが可能なプロセスを示す。第１に、プリンシパル２４０が、ＲＭＳ２１５から使用ライセンスを求める要求２０３を行うことができる。通常、使用ライセンスを求める要求は、発行ライセンス２０２およびプリンシパル２４０のＲＡＣを含み、このＲＡＣをＲＭＳ２１５は、プリンシパル２４０が許可されたユーザであることを確認するのに使用する。

【００２５】

ＲＭＳサーバ２１５は、発行ライセンス２０２の真正性、およびプリンシパル２４０のＩＤを確認すると、コンテンツキー２３５を含む使用ライセンス２０４をプリンシパル２４０に送信することができる。もちろん、前述したとおり、コンテンツキーは、ＲＭＳサーバ２１５のデータベースの中に格納されること、または暗号化された形態で発行ライセンスの中に含められることも可能である。使用ライセンス２０４の中で送信される場合、コンテンツキー２３５は、登録プロセスにおいてあらかじめ獲得され、ロックボックス２４５の中に格納されているプリンシパルの秘密キー（図示せず）に暗号化されなければならない。したがって、プリンシパル２４０は、暗号化されたコンテンツキー２３５を含む使用ライセンス２０４を受信すると、その使用ライセンス２０４をロックボックス２４５に提供することができる。例えば、解読されたコンテンツを使用することになるアプリケーション（図示せず）が、暗号化されたコンテンツ、および使用ライセンス２０４をロックボックス２４５に提供することができる。アプリケーションが解読されたコンテンツを扱うのに信頼が置けることを確実にするため、アプリケーションは、認定されなければならず、そのような認定を使用ライセンス２０４とともにロックボックスに提示しなければならない。次に、ロックボックス２４５は、登録プロセスにおいて作成された秘密キーを使用して、コンテンツキー２３５を解読し、その後、コンテンツキー２３５を使用して、保護されているコンテンツ２２０を解読することができる。次に、ロックボックス２４５が、適切なアプリケーションに、発行ライセンス２０２および／または使用ライセンス２０４の中で定義された制限とともに解読されたコンテンツを提供して、保護されたコンテンツに適切な制限を課すことができる。

【００２６】

しかし、プリンシパルがＲＭＳサーバへのアクセスを有さない場合、典型的な諸実施形態は、プレライセンス供与プロセスも提供する。以下の説明は、図３Ａ～Ｄとともに、プリンシパルが、ＲＭＳサーバへのアクセスを有することなしに、どのように保護されたコンテンツ、および使用ライセンスを受信することができるかを示す。

【００２７】

図３Ａを参照すると、図２Ａに関連して前述した公開プロセスと同様に、権利管理サービスに登録され、保護されたコンテンツを送信することを所望する送信側３１０が、ＲＭＳサーバ３１５から発行ライセンスを要求する３０１ことができる。前述したとおり、発行ライセンスを求める要求３０１は、権利表現、コンテンツキー、およびコンテンツのハッシュを含むことが可能である。権利表現は、誰が保護されたコンテンツを受信することを許可されているか、およびその人がそのようなコンテンツに対して何を行うことができるかを定義する。例えば、権利表現は、コンテンツの再ライセンス供与（ｒｅ－ｌｉｃｅｎｓｉｎｇ）を行う際、コンテンツを印刷する、コピーする、転送する、共有する、委託する、または保存する際、コンテンツに対するプリンシパルの操作上の権利を制限することができる。さらに、権利表現は、例えば、前述した権利が利用できる回数、または期間を制限する、有効期限の機能を含むことが可能である。

【００２８】

前述したとおり、発行ライセンスを求める要求３０１は、コンテンツキー３０５も含まなければならない。コンテンツキー３０５は、送信側３１０によって作成された対称キーであることが可能である。以下に説明するとおり、このコンテンツキー３０５は、プリンシパル３３５に保護されたコンテンツ３２０へのアクセスを許すのに使用される。

【００２９】

権利表現およびコンテンツキーに、加えて、発行ライセンスを求める要求３０１は、コ

ンテンツのハッシュも含むことが可能である。以下により詳細に説明するとおり、ハッシュは、ロックボックスｄｌｌ３４０によって、コンテンツが改ざんされていない、またはそれ以外で壊れていないことを確認するのに使用されることが可能である。

【００３０】

ＲＭＳサーバ３１５は、発行ライセンスを求める要求３０１を受信し、発行ライセンスを求める要求３０１の中で提供される情報の少なくとも一部分を取り込み、その一部分に署名して発行ライセンス３０２を作成することができる。前述したとおり、提供される情報は、発行ライセンス３０２をもたらすように署名され、暗号化される権利表現、コンテンツキー、および／またはコンテンツのハッシュの任意の組合せであることが可能である。前述したとおり、典型的な諸実施形態は、ＲＭＳサーバが、発行ライセンスを求める要求３０１を受信した後、コンテンツキーをデータベースの中に格納するか、またはコンテンツキーの暗号化されたバージョンを発行ライセンス３０２の中に含めることができるようにする。次に、発行ライセンス３０２が、送信側３１０に提供されることが可能であり、その時点で送信側３１０は、保護されたコンテンツ３２０および発行ライセンス３０２をプリンシパル３３５に提供することができる。

【００３１】

図３Ｂは、保護されたコンテンツ３２０および発行ライセンス３０２が、送信側３１０から送信側のメッセージサーバ３２５を介してプリンシパルのメッセージサーバ３３０に送信されるのを単に示す。典型的な諸実施形態によれば、プリンシパル３３５が、ＲＭＳサーバ３１５から直接に使用ライセンスを要求しなければならないのではなく、プリンシパルのメッセージサーバ３３０は、以下により詳細に説明するとおり、プリンシパル３３５に代行して使用ライセンス３０４を獲得することができる。

【００３２】

図３Ｃを参照すると、プリンシパルのメッセージサーバ３３０が、保護されたコンテンツ３２０を受信すると、使用ライセンス３０３を求める要求を行う。より詳細には、プリンシパルのメッセージサーバ３３０は、受信された、保護されたコンテンツ３２０が権利管理の対象となっていると認識する。したがって、プリンシパルのメッセージサーバ３３０は、使用ライセンス３０３を求める要求を行い、発行ライセンス３０２をＲＭＳサーバ３１５に送信する。

【００３３】

発行ライセンスに加え、ＲＭＳサーバは、前述したとおり、使用ライセンス３０４の要求側が信頼されるべきであると示すことができる権利アカウント証明書（ＲＡＣ）も要求することができる。通常の権利管理サービスは、使用ライセンスを求める要求３０３の中でプリンシパル３３５のＲＡＣが使用されることを要求するが、この追加のセキュリティ機構は、必要とされない可能性がある。詳細には、使用ライセンス内のコンテンツキーは、ＲＭＳ３１５によって、プリンシパルのロックボックス３４０の中に格納されたキーに暗号化されるので、使用ライセンス３０４を誤ったプリンシパルに送信することのリスクは、あったとしてもわずかである。つまり、特定のプリンシパルだけが、保護コンテンツを解読するためにコンテンツキーをロック解除する適切なキーを有する。したがって、別のプリンシパルが、プリンシパル３３５の秘密キーに暗号化されたコンテンツキー３０５を有する使用ライセンス３０４を受信した場合、そのプリンシパルは、コンテンツキー３０５を解読して、保護されたコンテンツ３２０にアクセスすることができない。

【００３４】

ＲＭＳサーバ３１５は、プリンシパル３３５のＲＡＣを要求しない可能性があるが、典型的な諸実施形態は、プリンシパルのメッセージサーバ３３０が、基本的なＷｉｎｄｏｗｓ（登録商標）ＮＴＬＭプロトコル、ケルベロスプロトコル、Ｘ５０９証明書プロトコル、Ｐａｓｓｐｏｒｔプロトコルなどの慣用のプロトコルのいずれかを使用して、自らをＲＭＳサーバに対して認証するように要求される可能性があるようにする。代替として、メッセージサーバ３３０は、サーバ３３０のＲＡＣを送信すること、および／またはＲＡＣに関連する秘密キーで要求（または要求の一部分）に署名することにより、カスタム証明

書認証プロセスを介して認証を行うこともできる。認証プロセスは、プリンシパルのメッセージサーバ３３０が、プリンシパル３３５に代行して使用ライセンス３０４を獲得することができる権限（ａｕｔｈｏｒｉｔｙ）であることを少なくとも確実にする。

【００３５】

ＲＭＳサーバ３１５は、発行ライセンス３０２を確認する（さらに、プリンシパルのメッセージサーバ３３０をプリンシパル３３５に代行して使用ライセンス３０４を受信する権限として認識する）と、使用ライセンス３０４をメッセージサーバ３３０に送信することができる。この使用ライセンス３０４は、コンテンツキー３０５を含み、コンテンツキー３０５は、前述したとおり、ＲＭＳ３１５のデータベースの中にあらかじめ格納されていたか、または暗号化され、ＲＭＳサーバに送信された発行ライセンス３０２の中に含められていた。前述したとおり、使用ライセンス３０４の中で提供される場合、コンテンツキー３０５は、ロックボックス３４０内に格納されたプリンシパル３３５の秘密キー（図示せず）に暗号化される。

【００３６】

次に、プリンシパルのメッセージサーバ３３０は、プリンシパル３３５が将来に取り出すために、使用ライセンス３０４を暗号化されたコンテンツキー３０５および保護されたメッセージ３２０とともに格納する。典型的な諸実施形態は、暗号化されたコンテンツキー３０５を含む使用ライセンス３０４が、保護されたメッセージ３２０とは別に格納されることが可能であるようにする。したがって、保護されたコンテンツが複数の受信者を有する場合、１つの保護されたメッセージ３２０だけが、格納のために必要とされて、貴重なメモリが節約される。

【００３７】

他の典型的な諸実施形態は、プリンシパルのメッセージサーバ３３０が、権利管理サーバ３１５にかかる負荷を絞る能力を提供する。詳細には、保護されたメッセージ３２０が複数のプリンシパルを宛先としている場合、プリンシパルのメッセージサーバ３３０は、使用ライセンス３０４を求める要求をＲＭＳサーバが対応することができるバッチで処理できることが可能である。メールは、わずかに遅延させられる可能性があるが、ＲＭＳサーバが圧倒され、クラッシュする、またはサーバが、要求で圧倒された、または過負荷になったためにプリンシパルへのライセンスを拒否することがない。

【００３８】

図３Ｄに示すとおり、プリンシパル３３５は、保護されたコンテンツ３２０、ならびに暗号化されたコンテンツキー３０５を有する使用ライセンス３０４を、ＲＭＳサーバ３１５に接触することなしに、プリンシパルメッセージサーバ３３０から獲得することができる。前の場合と同様に、その時点で、プリンシパルは、保護されたコンテンツキーを有する使用ライセンスをロックボックスｄｌｌ３４０に送ることができ、次に、ロックボックスｄｌｌ３４０が、コンテンツキー３０５を解読し、その後、コンテンツ３２０を解読することができる。コンテンツは、次に、権利表現に従って表示するため、または別の形で使用するために、適切なアプリケーションに送られることが可能である。

【００３９】

典型的な諸実施形態は、ロックボックス３４０が、受け取られたハッシュを実際のコンテンツに照らして調べて、コンテンツが変更されていない、またはそれ以外で壊れていないことを確認することもできるようにさらにする。コンテンツが損なわれている（ｃｏｍｐｒｏｍｉｓｅｄ）場合、そのコンテンツは、破棄されなければならない。

【００４０】

他の典型的な諸実施形態では、使用ライセンスは、ユーザ別に、またはマシン別に発行されることが可能である。ユーザ別に発行される場合、単一の使用ライセンスが、複数のマシン上に登録されたユーザによってコピーされ、使用されることになる。この実施形態では、図１Ａおよび図１Ｂに関連して前述した登録プロセス中、ユーザは、各マシンからＲＭＳサーバに登録しなければならない。コンテンツキーを暗号化する際、および解読する際に使用するために受け取られる解読キーは、各マシンに関して作成される各ロックボ

ックスｄｌｌに関して同一である。したがって、ユーザは、使用ライセンスを、ユーザが登録している任意のマシン上にコピーし、そのマシン上でロックボックスを使用して、保護されたコンテンツを見る、または別の形で使用することができる。

【００４１】

他の諸実施形態は、使用ライセンスが、マシン別に発行されることを可能にする。すなわち、使用ライセンスの中に含められるコンテンツキーを暗号化するのに使用される秘密キーが、マシン固有であり、したがって、ユーザがアクセスを有する各マシンは、独自の使用ライセンスを有さなければならない。この実施形態では、プリンシパルのメッセージサーバ３３０は、プリンシパル３３５が有する可能性がある複数のマシンに関して複数の使用ライセンス３０４を獲得するか、または別の形で受け取ることができる。例えば、プリンシパルのメッセージサーバ３３０は、プリンシパル３３５が複数のマシンを有することを認識して、プリンシパル３３５のマシンのそれぞれに関して複数の使用ライセンス３０４を獲得することができる。代替として、ＲＭＳサーバ３１５は、プリンシパル３３５が、独自の特定の使用ライセンス３０４を全部が必要とする複数のマシンを有することを認識して、プリンシパルのメッセージサーバ３３０にすべての適切な使用ライセンス３０４を提供することもできる。

【００４２】

本発明は、機能ステップおよび／または非機能的な動作を含む方法に関して説明することもできる。以下は、本発明を実施する際に実行されることが可能な動作およびステップの説明である。普通、機能ステップは、達せられる結果に関して本発明を説明するのに対して、非機能的な動作は、特定の結果を達するためのより具体的な動作を説明する。機能ステップおよび非機能的な動作を特定の順序で説明する、または請求する可能性があるが、本発明は、動作および／またはステップのいずれの特定の順序または組合せにも、必ずしも限定されない。

【００４３】

図４は、プリンシパルが権利管理サーバへのアクセスを有さない場合に、プリンシパルにコンテンツへのアクセスを許すために、権利管理の対象であるコンテンツのプレライセンス供与を行う際に使用される典型的なステップおよび動作を示す。メッセージが権利管理の対象であることを判定するためのステップ（４１０）が、メッセージサーバによって、メッセージへのアクセスが権利管理サーバを介して制限されるという点で権利管理の対象であるメッセージを受信する動作（４０５）を含むことが可能である。受信されたメッセージが権利管理の対象であると判定されるのに、メッセージの一部分だけが、権利管理サーバを介して制限される必要がある。権利管理の対象であるメッセージの部分は、暗号化されていることが可能であり、保護された連絡先、保護されたドキュメント、保護された予定表のアイテム、または保護された会合要求であることも可能である。

【００４４】

権利管理サーバに対してメッセージを明らかにするために受信された発行ライセンスを使用するためのステップ（４２０）が、メッセージサーバによって、発行ライセンスを受信する動作（４１５）を含むことが可能である。発行ライセンスは、いくつかのプリンシパルへの参照を含み、メッセージサーバが使用ライセンスを要求した場合、プリンシパルがメッセージへのアクセスを有することが意図されていることを権利管理サーバが検証できるようにすることが可能である。発行ライセンスは、プリンシパルがメッセージに対して実行されることが許される操作のタイプを制限する権利表現をさらに含むことが可能である。例えば、権利表現は、プリンシパルの操作を再ライセンス供与、印刷、コピー、転送、共有、委託、および保存に制限することが可能である。代替として、権利表現は、管理者が各企業に関して異なる形で構成することができる既定値、例えば、読み取り専用であることが可能である。権利表現は、権利表現が利用できる回数または期間を制限する、有効期限の機能をさらに含むことが可能である。さらに、発行ライセンスは、メッセージが変わっていないことを確認するのに使用されるハッシュ、および発行ライセンスが有効であることを確認するのに使用される権利管理サーバによる署名を含むことが可能である

。

【００４５】

使用ライセンスを獲得するためのステップ（４３０）は、メッセージサーバによってプリンシパルに代行して、使用ライセンスを要求する動作（４２５）、および使用ライセンスを受信する動作（４２７）を含むことが可能である。使用ライセンスを求める要求は、プリンシパルにメッセージへのアクセスを許すために行われ、権利管理サーバに対してメッセージを明らかにする発行ライセンスを含む。使用ライセンスは、プリンシパルが、権利管理サーバから使用ライセンスを要求する必要なしに、メッセージにアクセスすることができるように受信される。権利管理サーバを介して制限されるメッセージの部分は、暗号化されることが可能であり、使用ライセンスは、暗号化されているメッセージの部分を解読するのに使用することができるコンテンツキーを含むことが可能である。使用ライセンスを要求する動作（４２５）は、権利アカウント証明書を権利管理サーバに送信して、メッセージサーバがプリンシパルに代行して使用ライセンスを獲得する権限を有することを確認することをさらに含むことが可能である。さらに、メッセージサーバは、プリンシパルに代行して複数の使用ライセンスを要求して、プリンシパルが、複数のマシン上のメッセージにアクセスすることができるようにすることもできる。さらに、使用ライセンスは、メッセージとは別個にメッセージサーバ上に格納することもできる。

【００４６】

本発明の範囲内の諸実施形態は、コンピュータ実行可能命令またはデータ構造を担持するため、または格納しておくためのコンピュータ可読媒体も含む。そのようなコンピュータ可読媒体は、汎用または専用のコンピュータによってアクセスすることができる任意の利用可能な媒体であることが可能である。例として、限定としてではなく、そのようなコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭまたは他の光ディスクストレージ、磁気ディスクストレージまたは他の磁気記憶装置、あるいは、コンピュータ実行可能命令またはデータ構造の形態で所望のプログラムコード手段を担持する、または格納するのに使用することができ、汎用または専用のコンピュータがアクセスすることができる他の任意の媒体を含むことが可能である。ネットワークまたは別の通信接続（ハードワイヤド、無線、またはハードワイヤドまたは無線の組合せ）を介して情報がコンピュータに転送された、または提供された場合、コンピュータが、その接続をコンピュータ可読媒体として適切に見なす。このため、いずれのそのような接続も、コンピュータ可読媒体と適切に呼ばれる。以上の組合せも、コンピュータ可読媒体の範囲内に含められるべきである。コンピュータ実行可能命令は、例えば、汎用コンピュータ、専用コンピュータ、または専用処理装置が、ある機能またはグループの機能を実行するようにさせる命令およびデータを含む。

【００４７】

図５、および以下の説明は、本発明を実施することができる適切なコンピューティング環境の簡単な一般的説明を提供することを目的とする。必須ではないが、本発明を、ネットワーク環境におけるコンピュータ群によって実行される、プログラムモジュール群などの、コンピュータ実行可能命令の一般的な文脈で説明する。一般に、プログラムモジュール群には、特定のタスクを実行する、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などが含まれる。コンピュータ実行可能命令、関連するデータ構造、およびプログラムモジュールは、本明細書で開示する方法のステップを実行するためのプログラムコード手段の実施例を表す。そのような実行可能命令、または関連するデータ構造の特定のシーケンスは、そのようなステップにおいて示す諸機能を実施するための対応する動作の実施例を表す。

【００４８】

本発明は、パーソナルコンピュータ、ハンドヘルドデバイス、マルチプロセッサシステム、マイクロプロセッサベースの家庭用電化製品またはプログラマブル家庭用電化製品、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータなどを含め、多くのタイプのコンピュータシステム構成を有するネットワークコンピューティング環境におい

て実施できることが当業者には理解されよう。本発明は、通信ネットワークを介してリンクされた（ハードワイヤドリンクで、無線リンクで、またはハードワイヤドリンクまたは無線リンクの組合せで）ローカル処理装置群およびリモート処理装置群によってタスクが実行される分散コンピューティング環境において実施することもできる。分散コンピューティング環境では、プログラムモジュール群は、ローカルメモリ記憶装置とリモートメモリ記憶装置の両方の中に配置することができる。

【００４９】

図５を参照すると、本発明を実施するための典型的なシステムが、プロセッサ５２１、システムメモリ５２２、ならびにシステムメモリ５２２からプロセッサ５２１までを含む様々なシステムコンポーネントを結合するシステムバス５２３を含む、慣用のコンピュータ５２０の形態の汎用コンピューティングデバイスを含む。システムバス５２３は、様々なバスアーキテクチャのいずれかを使用するメモリバスまたはメモリコントローラ、周辺バス、およびローカルバスを含め、いくつかのタイプのバス構造のいずれであってもよい。システムメモリは、読み取り専用メモリ（ＲＯＭ）５２４およびランダムアクセスメモリ（ＲＡＭ）５２５を含む。始動中などに、コンピュータ５２０内部の要素間で情報を転送するのを助ける基本ルーチンを含む基本入出力システム（ＢＩＯＳ）５２６が、ＲＯＭ５２４の中に格納される。

【００５０】

コンピュータ５２０は、磁気ハードディスク５３９に対して読み取りおよび書き込みを行うための磁気ハードディスクドライブ５２７、リムーバブルな磁気ディスク５２９に対して読み取りまたは書き込みを行うための磁気ディスクドライブ５２８、およびＣＤ－ＲＯＭまたは他の光媒体などのリムーバブルな光ディスク５３１に対して読み取りまたは書き込みを行うための光ディスクドライブ５３０も含むことが可能である。光ディスクドライブ５３０は、光媒体レコーダの一実施例である。磁気ハードディスクドライブ５２７、磁気ディスクドライブ５２８、および光ディスクドライブ５３０は、それぞれ、ハードディスクドライブインタフェース５３２、磁気ディスクドライブインタフェース５３３、および光ドライブインタフェース５３４でシステムバス５２３に接続される。以上のドライブ群、および関連するコンピュータ可読媒体により、コンピュータ実行可能命令、データ構造、プログラムモジュール、およびその他のデータの不揮発性ストレージがコンピュータ５２０に提供される。本明細書で説明する典型的な環境は、磁気ハードディスク５３９、リムーバブルな磁気ディスク５２９、およびリムーバブルな光ディスク５３１を使用するが、磁気カセット、フラッシュメモリカード、デジタルバーサタイルディスク、ベルヌーイカートリッジ、ＲＡＭ、ＲＯＭなどを含め、データを格納するための他のタイプのコンピュータ可読媒体も使用することができる。

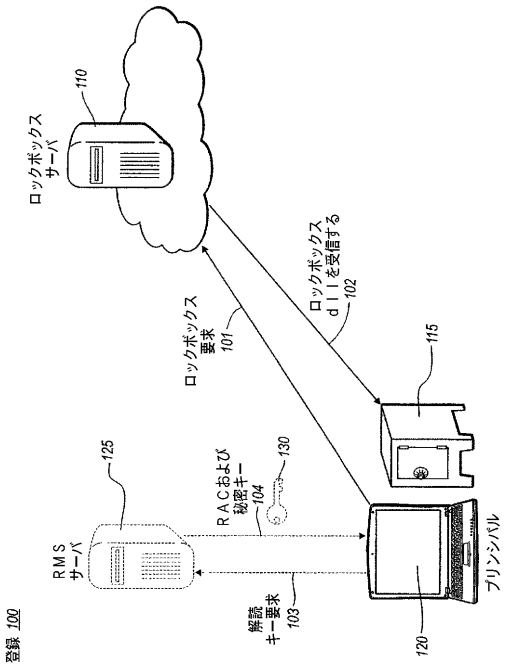
【００５１】

オペレーティングシステム５３５、１つまたは複数のアプリケーションプログラム５３６、その他のプログラムモジュール群５３７、およびプログラムデータ５３８を含め、１つまたは複数のプログラムモジュールを含むプログラムコード手段が、ハードディスク５３９、磁気ディスク５２９、光ディスク５３１、ＲＯＭ５２４、またはＲＡＭ５２５に格納されることが可能である。プリンシパルは、キーボード５４０、ポインティングデバイス５４２、あるいはマイク、ジョイスティック、ゲームパッド、サテライトディッシュ、スキャナなどの他の入力デバイス群（図示せず）を介して、コマンドおよび情報をコンピュータ５２０に入力することができる。以上、およびその他の入力デバイス群は、しばしば、システムバス５２３に結合されたシリアルポートインタフェース５４６を介してプロセッサ５２１に接続される。代替として、入力デバイス群は、パラレルポート、ゲームポート、またはユニバーサルシリアルバス（ＵＳＢ）などの他のインタフェース群で接続してもよい。モニタ５４７、または別のディスプレイデバイスも、ビデオアダプタ５４８などのインタフェースを介してシステムバス５２３に接続される。モニタに加えて、パーソナルコンピュータは、通常、スピーカやプリンタなどの他の周辺出力デバイス群（図示せず）も含む。

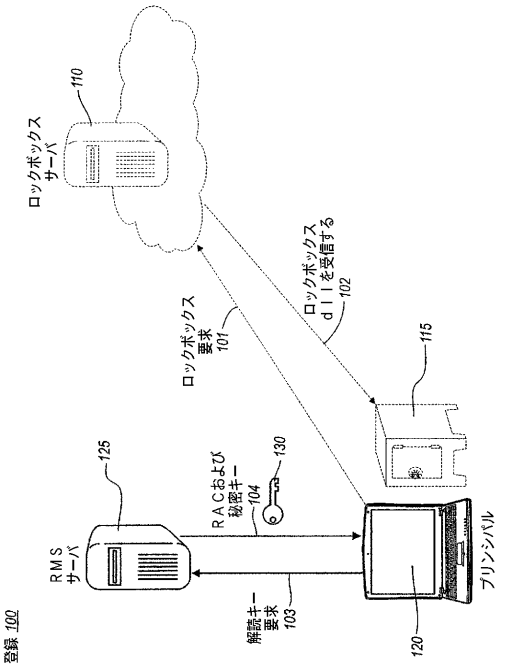
【００５２】
コンピュータ５２０は、リモートコンピュータ５４９ａおよび５４９ｂのような１つまたは複数のリモートコンピュータに対する論理接続を使用する、ネットワーク化された環境において動作することができる。リモートコンピュータ５４９ａおよび５４９ｂはそれぞれ、別のパーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイス、または他の一般的なネットワークノードであることが可能であり、通常、コンピュータ５２０に関連して前述した要素の多く、またはすべてを含むが、メモリ記憶装置５５０ａおよび５５０ｂ、ならびに関連するアプリケーションプログラム５３６ａおよび５３６ｂだけを図５に示している。図５に示した論理接続は、例として、限定としてではなく、図に提示するローカルエリアネットワーク（ＬＡＮ）５５１およびワイドエリアネットワーク（ＷＡＮ）５５２を含む。そのようなネットワーキング環境は、オフィス全体または企業全体のコンピュータ網、イントラネット、およびインターネットで一般的である。
【００５３】
したがって、本発明は、コンピュータ網を介して光媒体レコーダに接続されたコンピュータにおいて実施することができる。一部の新たなシステムでは、システムバス５２３は、カプセル化され、ＴＣＰ／ＩＰ網などの新たなトランスポートを介して送信される。例えば、ＩＳＣＳＩ（インターネットＳＣＳＩまたはインターネットスモールコンピュータシステムズインタフェース（Ｉｎｔｅｒｎｅｔ Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍｓ Ｉｎｔｅｒｆａｃｅ））が、ＩＰベースの記憶装置、ホスト、およびプリンシパルの間で接続を確立し、維持するためのＴＣＰ／ＩＰベースのプロトコルの１つの相当によく知られたインプリメンテーションである。
【００５４】
ＬＡＮネットワーキング環境で使用される場合、コンピュータ５２０は、ネットワークインタフェースまたはネットワークアダプタ５５３を介してローカルネットワーク５５１に接続される。ＷＡＮネットワーキング環境で使用される場合、コンピュータ５２０は、インターネットなどのワイドエリアネットワーク５５２を介して通信を確立するためのモデム５５４、無線リンク、または他の手段を含むことが可能である。内部にあることも、外部にあることも可能なモデム５５４は、シリアルポートインタフェース５４６を介してシステムバス５２３に接続される。ネットワーク化された環境では、コンピュータ５２０に関連して示したプログラムモジュール群、またはプログラムモジュール群の諸部分は、リモートメモリ記憶装置の中に格納されることが可能である。図示したネットワーク接続は、典型的であり、ワイドエリアネットワーク５５２を介して通信を確立する他の手段も使用できることが認められよう。
【００５５】
本発明は、本発明の趣旨または本質的な特徴を逸脱することなく、他の特定の諸形態で実施することもできる。説明した諸実施形態は、すべての点で、例示的であり、限定的ではないものと考えられたい。したがって、本発明の範囲は、以上の説明によってではなく、添付の特許請求の範囲によって示される。特許請求の範囲の均等の意味および範囲に含まれるすべての変更が、特許請求の範囲に包含されるものとする。
【図面の簡単な説明】
【００５６】
【図１Ａ】権利管理システムに参加するのに使用される要求側ソフトウェアおよび受信側ソフトウェアに関するユーザ登録プロセスの実施例を示す図である。
【図１Ｂ】権利管理サーバに登録するためのユーザ登録プロセスの実施例を示す図である。
【図２Ａ】保護されたコンテンツを送信するために、どのように送信側が権利管理サーバから発行ライセンスを獲得することができるかの実施例を示す図である。
【図２Ｂ】プリンシパルに保護されたコンテンツを送信するプロセスの実施例を示す図である。
【図２Ｃ】受信された、保護されたコンテンツを解読するために、権利管理サーバから使

用ライセンスを獲得するためのプロセスの実施例を示す図である。
【図３Ａ】プリンシパルが、権利管理サーバから発行ライセンスを要求し、受信することの実施例を示す図である。
【図３Ｂ】送信側が、保護されたコンテンツ、および発行ライセンスを送信側のメッセージサーバを介してプリンシパルのメッセージサーバに送信することの実施例を示す図である。
【図３Ｃ】例示的な諸実施形態による、メッセージングサーバが、プリンシパルに代行して使用ライセンスを要求し、獲得することを示す図である。
【図３Ｄ】典型的な諸実施形態による、プリンシパルが、保護されたコンテンツを使用ライセンスとともにメッセージサーバから受信することを示す図である。
【図４】典型的な諸実施形態による、権利管理の対象であるコンテンツのプレライセンス供与を行う典型的な動作およびステップを示す図である。
【図５】本発明に適切な動作環境を提供する典型的なシステムを示す図である。

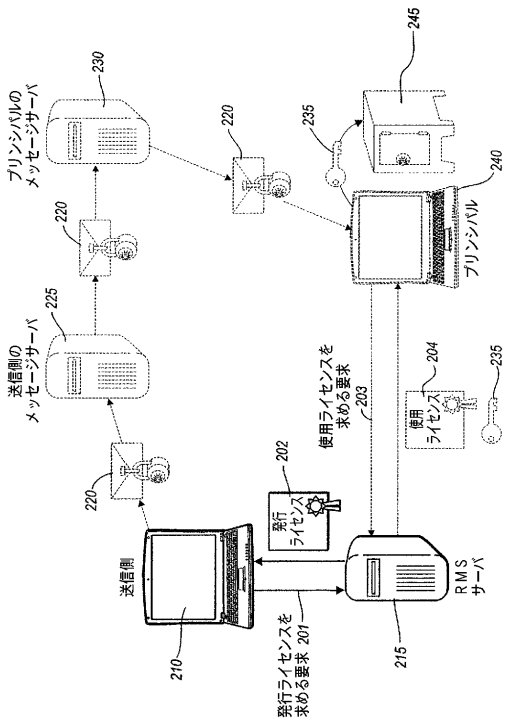
【図１Ａ】



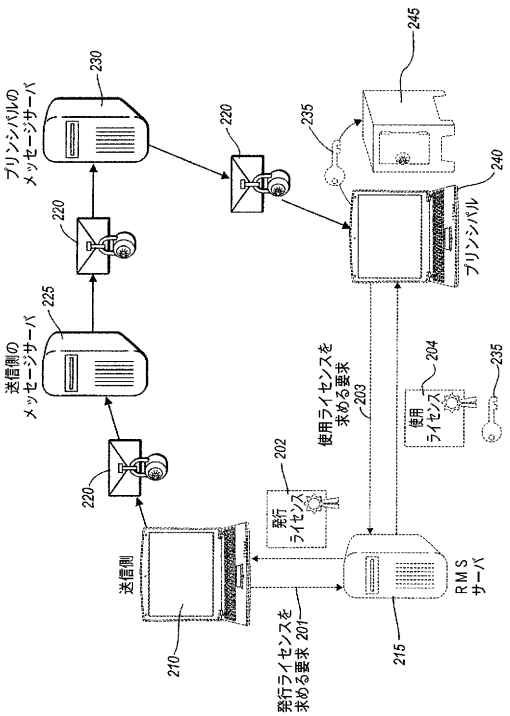

【図１Ｂ】



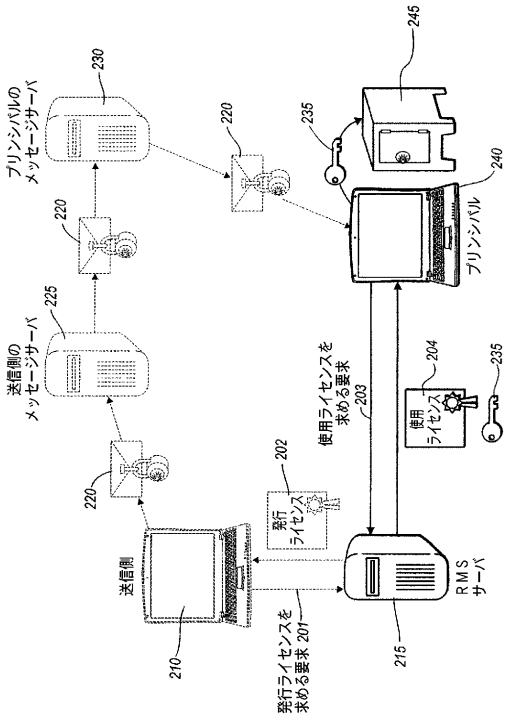
【図２Ａ】



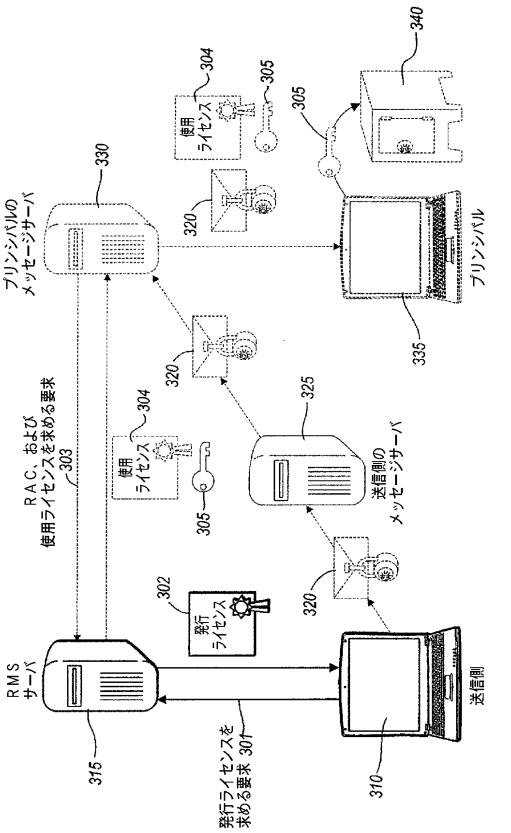

【図２Ｂ】



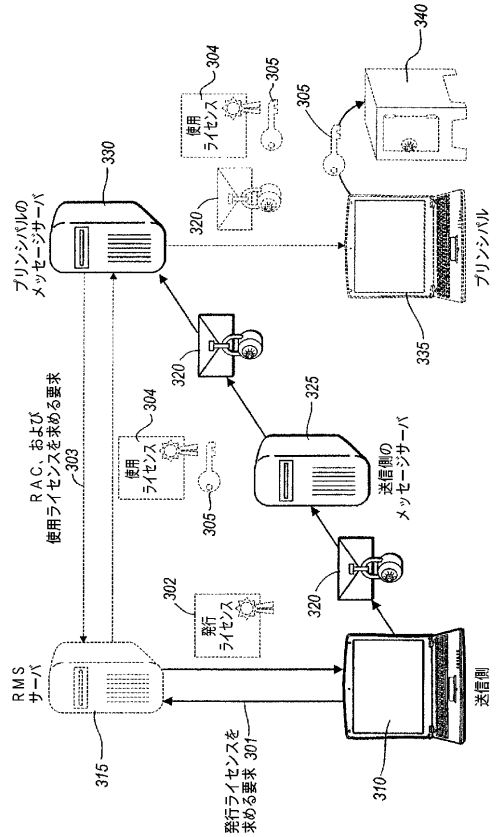

【図２Ｃ】



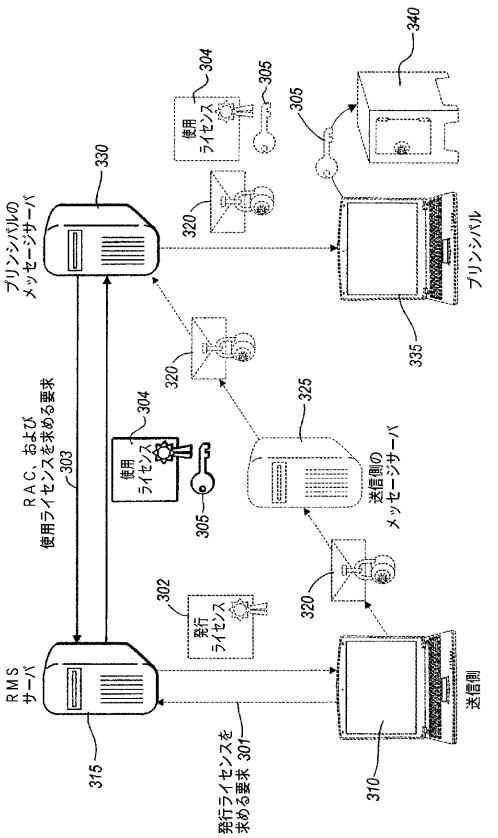

【図３Ａ】



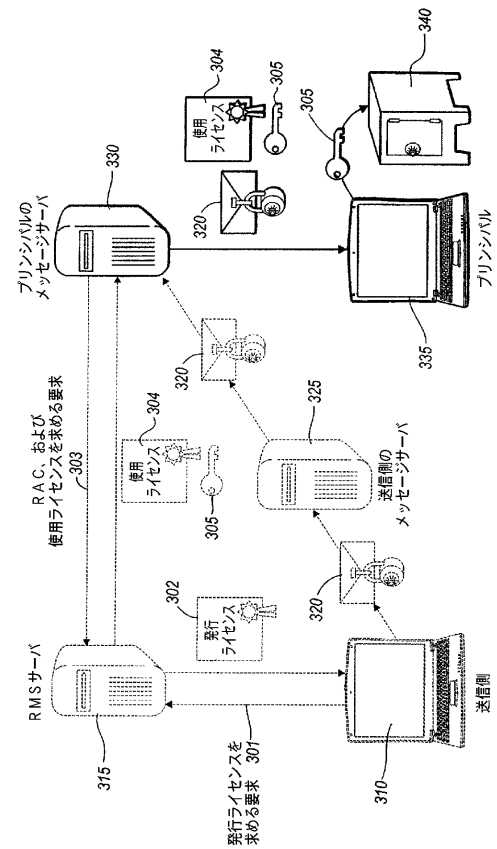
【図３Ｂ】



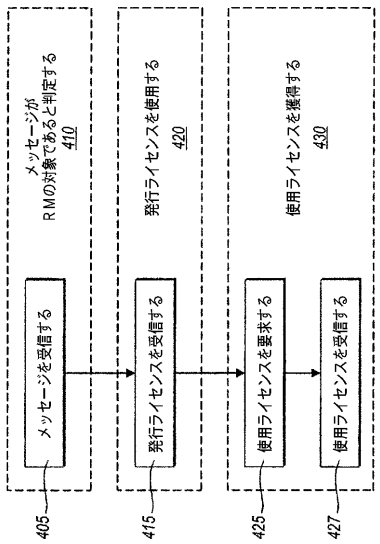

【図３Ｃ】



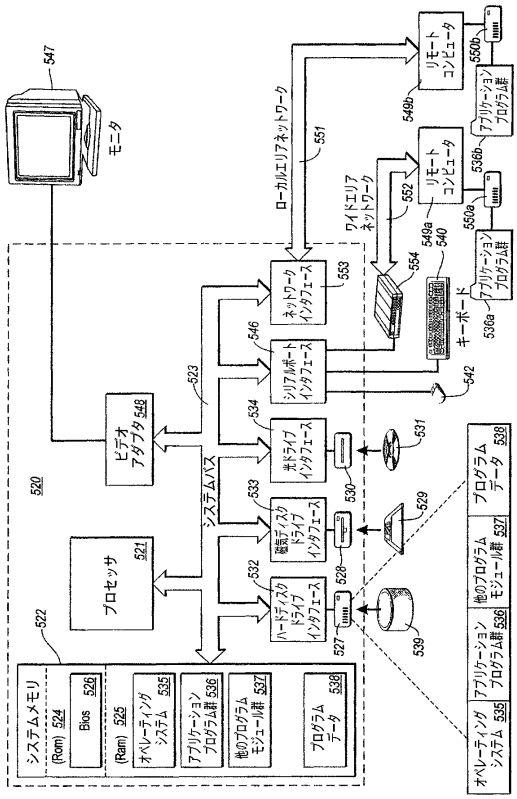

【図３Ｄ】




【図４】



【図５】


547
モニタ
ローカルエリアネットワーク
551
ワイドエリア
ネットワーク
552
リモート
コンピュータ
549b
550b
536b
アプリケーション
プログラム群
リモート
コンピュータ
549a
550a
536a
アプリケーション
プログラム群
キーボード
540
554
553
ネットワーク
インタフェース
546
シリアルポート
インタフェース
542
534
光ドライブ
インタフェース
531
530
533
磁気ディスク
ドライブ
インタフェース
529
528
532
ハードディスク
ドライブ
インタフェース
527
539
523
システムバス
520
ビデオ
アダプタ
548
プロセッサ
521
522
システムメモリ
(Rom) 524
Bios 526
(Ram) 525
オペレーティング
システム 535
アプリケーション
プログラム群 536
他のプログラム
モジュール群 537
プログラム
データ 538
プログラム
データ 538
他のプログラム
モジュール群 537
アプリケーション
プログラム群 536
オペレーティング
システム 535

フロントページの続き

(72)発明者 マルコム エイチ. デービス
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内
(72)発明者 ピーター ディー. ワックスマン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内
(72)発明者 マルコ エー. デメロ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内
(72)発明者 クリストファー エフ. グラハム
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内
(72)発明者 ジェーソン エム. カヒル
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内

審査官 田内 幸治

(56)参考文献 特開２００２－００９８１５（ＪＰ，Ａ）
特開平１１－３１３０５５（ＪＰ，Ａ）
特開２００１－３４５８３７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06Q 10/00-50/00
H04L 9/08