(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2013-535859
(P2013-535859A)
(43)公表日　平成25年9月12日(2013.9.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675Z	5J104
G06F 21/33	(2013.01)	G06F	21/20	133	

審査請求 未請求　予備審査請求 未請求　（全 34 頁）

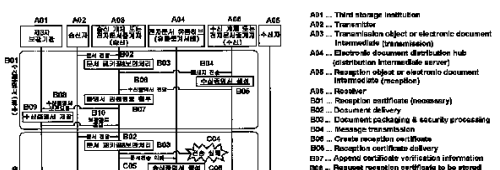
(21)出願番号	特願2013-518282 (P2013-518282)
(86)(22)出願日	平成23年7月8日 (2011.7.8)
(85)翻訳文提出日	平成25年1月7日 (2013.1.7)
(86)国際出願番号	PCT/KR2011/005039
(87)国際公開番号	WO2012/005555
(87)国際公開日	平成24年1月12日 (2012.1.12)
(31)優先権主張番号	10-2011-0067188
(32)優先日	平成23年7月7日 (2011.7.7)
(33)優先権主張国	韓国 (KR)
(31)優先権主張番号	10-2010-0131936
(32)優先日	平成22年12月21日 (2010.12.21)
(33)優先権主張国	韓国 (KR)
(31)優先権主張番号	10-2010-0131935
(32)優先日	平成22年12月21日 (2010.12.21)
(33)優先権主張国	韓国 (KR)

(71)出願人　313010987
ナショナル　アイティー　インダストリー　プロモーション　エージェンシー
ＮＡＴＩＯＮＡＬ　ＩＴ　ＩＮＤＵＳＴＲＹ　ＰＲＯＭＯＴＩＯＮ　ＡＧＥＮＣＹ
大韓民国、１３８－１６０、ソウル、ソンパ－グ、ガラク－ドン　７９－２
７９－２，　Ｇａｒａｋ－ｄｏｎｇ，　Ｓｏｎｇｐａ－ｇｕ　Ｓｅｏｕｌ　１３８－１６０　（ＫＲ）
(74)代理人　110001139
ＳＫ特許業務法人
(74)代理人　100130328
弁理士　奥野　彰彦

最終頁に続く

(54)【発明の名称】電子文書流通証明書の生成／発給方法、電子文書流通証明書の検証方法、および電子文書の流通システム

(57)【要約】
本発明は、公認電子アドレス基盤の電子文書の流通体系内で流通証明書を生成し流通、保管するにおいて透明で効率的な発給サービスを提供し、証明書の互換性の確保によって電子文書の流通信頼性を向上できる電子文書流通証明書の生成／発給方法、電子文書流通証明書の検証方法、および電子文書の流通システムに関する。このような本発明の好ましい実施形態による電子文書流通証明書の生成／発給方法は、送受信個体と流通ハブとを含む電子文書の流通体系において流通証明書を生成／発給する方法であって、送信個体は受信個体に送信者の電子文書を含む流通メッセージを転送するステップ；受信個体は流通メッセージを受信した後に必須情報を獲得して受信証明書を生成するステップ；受信個体は生成した受信証明書を送信個体に転送するステップ；送信個体は受信した受信証明書に対する検証を完了した後に受信証明書の電子署名認証書に対する検証情報を受信証明書に添付するステップ；および送信個体は受信証明書を第３者保管機関に転送して保管を依頼するステップ；を含む。



【特許請求の範囲】
【請求項１】
送受信個体と流通ハブとを含む電子文書の流通体系において流通証明書を生成／発給する方法であって、
（ａ）送信個体は受信個体に送信者の電子文書を含む流通メッセージを転送するステップ；
（ｂ）受信個体は流通メッセージを受信した後に必須情報を獲得して受信証明書を生成するステップ；
（ｃ）受信個体は生成した受信証明書を送信個体に転送するステップ；
（ｄ）送信個体は受信した受信証明書に対する検証を完了した後に受信証明書の電子署名認証書に対する検証情報を受信証明書に添付するステップ；および
（ｅ）送信個体は受信証明書を第３者保管機関に転送して保管を依頼するステップ；
を含む電子文書流通証明書の生成／発給方法。
【請求項２】
前記（ｂ）ステップにおいて、受信個体が受信証明書を生成する時に必要な必須情報は、電子文書情報、送信者、受信者、送信者の送信時刻、受信者の受信時刻を含むことを特徴とする、請求項１に記載の電子文書流通証明書の生成／発給方法。
【請求項３】
前記（ａ）ステップにおいて、送信個体が受信個体に流通メッセージの転送を試みたが、流通メッセージの転送を失敗した場合には、
（ａ１）送信個体は流通ハブの流通中継サーバに流通メッセージの転送を依頼するステップ；
（ａ２）流通中継サーバは依頼を受けた転送に対する送信証明書を生成するステップ；
（ａ３）流通中継サーバは送信証明書を送信個体に転送するステップ；
（ａ４）送信個体は受信した受信証明書に対する検証を完了した後に受信証明書の電子署名認証書に対する検証情報を受信証明書に添付するステップ；
（ａ５）送信個体は受信証明書を第３者保管機関に転送して保管を依頼するステップ；
（ａ６）流通中継サーバは流通メッセージを受信個体に伝達するステップ；
（ａ７）受信個体は電子文書の受信直後に受信証明書を生成するステップ；
（ａ８）受信個体は受信証明書を流通中継サーバに転送するステップ；
（ａ９）流通中継サーバは受信証明書を送信個体に伝達するステップ；および
（ａ１０）送信個体は前記（ｄ）ステップと（ｅ）ステップを順に行うステップ；
を含むことを特徴とする、請求項１に記載の電子文書流通証明書の生成／発給方法。
【請求項４】
前記（ａ２）ステップにおいて、流通中継サーバが送信証明書を生成する時に必要な必須情報は、電子文書情報、送信者、受信者、送信者の送信依頼時刻を含むことを特徴とする、請求項３に記載の電子文書流通証明書の生成／発給方法。
【請求項５】
前記（ｅ）ステップ後には、
（ｆ１）受信者は受信個体に流通メッセージの閲覧を要請して受けた流通メッセージを閲覧するステップ；
（ｆ２）受信個体は閲覧証明書を生成するステップ；
（ｆ３）受信閲覧証明書に対する検証を完了した後に閲覧証明書の電子署名認証書に対する検証情報を閲覧証明書に添付するステップ；および
（ｆ４）送信個体は閲覧証明書を第３字保管機関に転送して保管を依頼するステップ；
を含むことを特徴とする、請求項１に記載の電子文書流通証明書の生成／発給方法。
【請求項６】
前記（ａ１０）ステップ後には、
（ａ１１）受信者は受信個体に流通メッセージの閲覧を要請して受けた流通メッセージを閲覧するステップ；

（ａ１２）受信個体は閲覧証明書を生成するステップ；
（ａ１３）受信閲覧証明書に対する検証を完了した後に閲覧証明書の電子署名認証書に対する検証情報を閲覧証明書に添付するステップ；および
（ａ１４）送信個体は閲覧証明書を第３字保管機関に転送して保管を依頼するステップ；
を含むことを特徴とする、請求項３に記載の電子文書流通証明書の生成／発給方法。
【請求項７】
受信個体が閲覧証明書を生成する時に必要な必須情報は、電子文書情報、送信者、受信者、送信者の送信時刻、受信者の受信時刻、受信者の閲覧時刻を含むことを特徴とする、請求項５～６のいずれか１項に記載の電子文書流通証明書の生成／発給方法。
【請求項８】
送受信個体と流通ハブとを含む電子文書の流通体系内で生成／発給された流通証明書を検証する方法であって、
流通証明書のフォーマットが予め定められた構造および値の制約事項を守っているかを検証するステップ；
流通証明書に設定された流通メッセージの送信日時、受信日時、閲覧日時、流通証明書の発給日、証明書の検証時点、および証明書の効力満期日が順序をなしているかを検証するステップ；
流通証明書に添付された電子署名を検証するステップ；および
流通証明書に電子署名を行った認証書の有効性有無を検証し、流通証明書の発給者情報との同一性有無を検証するステップ；
を含むことを特徴とする電子文書流通証明書の検証方法。
【請求項９】
流通証明書に含まれた流通メッセージの情報と実際の流通メッセージを比較検証するステップがさらに遂行されることを特徴とする、請求項８に記載の電子文書流通証明書の検証方法。
【請求項１０】
前記比較検証をするステップは、
流通証明書に含まれた送信者の公認電子アドレスおよび受信者の公認電子アドレスは、実際の流通メッセージの送信者の公認電子アドレスおよび受信者の公認電子アドレスと一致するかを確認するステップ；および
流通証明書に含まれた流通ファイル個数は、実際の流通メッセージに添付された電子文書ファイルの個数と同一であるかを確認するステップ；
を含むことを特徴とする、請求項９に記載の電子文書流通証明書の検証方法。
【請求項１１】
前記比較検証をするステップは、
流通証明書が受信証明書または閲覧証明書である場合に、流通証明書に含まれた送信一時が"メッセージ転送"の流通メッセージ内のＳＯＡＰメッセージに含まれたＴｉｍｅＳｔａｍｐフィールドの値と一致するかを確認するステップ；および
流通証明書が送信証明書である場合に、流通証明書に含まれた送信一時は流通中継サーバが"メッセージ転送依頼"の流通メッセージを受信するのに合理的な時刻であるかを確認するステップ；
を含むことを特徴とする、請求項９に記載の電子文書流通証明書の検証方法。
【請求項１２】
前記比較検証をするステップは、
前記流通証明書が送信個体が受信個体に直接転送した"メッセージ転送"の流通メッセージに対する受信証明書または閲覧証明書である場合に、流通証明書の受信日時は受信個体の流通メッセージングサーバが"メッセージ転送"の流通メッセージを受信するのに合理的な時刻であるかを確認するステップ；および
前記流通証明書が送信個体が流通ハブの流通中継サーバに依頼した"メッセージ転送依

頼"の流通メッセージに対する受信証明書または閲覧証明書である場合に、流通証明書の受信日時は受信個体の流通メッセージングサーバが"メッセージ転送"の流通メッセージを受信するのに合理的な時刻であるかを確認するステップ；
を含むことを特徴とする、請求項９に記載の電子文書流通証明書の検証方法。
【請求項１３】
前記比較検証をするステップは、
前記流通証明書が閲覧証明書である場合に、流通証明書の閲覧日時は受信個体が受信者の"メッセージ詳細情報要請"に対して応答した流通連係メッセージ内のＳＯＡＰメッセージに含まれたＴｉｍｅＳｔａｍｐフィールド値と一致するかを確認するステップを含むことを特徴とする、請求項９に記載の電子文書流通証明書の検証方法。
【請求項１４】
前記比較検証をするステップは、
流通証明書に含まれた流通識別値は、流通証明書の発給対象の流通メッセージの固有識別値（Ｉｄｅｎｔｉｆｉｅｒ）と一致するかを確認するステップと；
流通証明書の流通文書情報内に含まれた個別ファイルのファイル識別値またはファイル名が実際の流通メッセージに添付された電子文書ファイルのＣｏｎｔｅｎｔ－ＩＤ値と全て一致するかを確認するステップ；および
流通証明書の流通文書情報内に含まれた個別ファイルが、ファイルハッシュ情報が実際の流通メッセージに添付された電子文書ファイルをハッシュした値と全て一致するかを確認するステップ；
を含むことを特徴とする、請求項９に記載の電子文書流通証明書の検証方法。
【請求項１５】
電子文書を流通するシステムであって、
電子アドレスを基盤にメッセージを送受信し、メッセージの送受信に対する流通証明書を発給および管理する流通メッセージングサーバを介して電子文書を流通する送受信個体；
前記送受信個体の電子アドレスを登録／管理し、前記送受信個体間の電子文書の流通経路を設定し、送受信個体間の電子文書の流通過程でエラーが発生した時にメッセージ転送を代行し、流通証明書を発給する流通ハブ；および
流通証明書の伝達を受けて保管し、信頼できる第３者保管機関；
を含み、
前記流通証明書は、受信個体のメッセージの受信事実に対する否認防止のための受信証明書と、送信個体の送信試みに対する証明のための送信証明書と、受信者の受信メッセージの閲覧事実に対する否認防止のための閲覧証明書とを含むことを特徴とする電子文書の流通システム。
【請求項１６】
前記流通証明書は、
流通証明書構造のバージョン、流通証明書の識別情報、流通証明書を発給する主体、流通証明書の発給日、流通証明書の効力満期日、流通証明書政策、流通証明書の要請のメッセージ情報、証明対象を含むことを特徴とする、請求項１５に記載の電子文書の流通システム。
【請求項１７】
前記証明対象は、
流通メッセージを送信した送信者の公認電子アドレス、流通メッセージを受信した受信者の公認電子アドレス、送信者が流通メッセージを送信した時刻、受信者が流通メッセージを受信した時刻、受信者が電子文書を受信した後に閲覧した時刻、流通メッセージに対する識別値、流通メッセージに添付された電子文書ファイルの個数、流通メッセージに添付された電子文書の各々に対する情報、流通メッセージに添付された個別電子文書ファイルのハッシュ値、流通メッセージに添付された個別電子文書ファイルの識別子、流通メッセージに添付された個別電子文書ファイルのファイル名を含むことを特徴とする、請求項

１６に記載の電子文書の流通システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、公認電子アドレス基盤の電子文書の流通体系内で流通証明書を生成し流通、保管するにおいて透明で効率的な発給サービスを提供し、証明書の互換性の確保によって電子文書の流通信頼性を向上できる電子文書流通証明書の生成／発給方法、電子文書流通証明書の検証方法、および電子文書の流通システムに関する。
【背景技術】
【０００２】
一般的に、電子文書の流通は、企業／機関が個別的な固有規約を基盤に特定産業群またはコミュニティ内でのみ限定的に行われてきた。
【０００３】
また、一般個人の間、個人と企業／機関の間には、信頼的な電子流通の概念がなく、Ｅメールを補助手段として活用するか、個人、個人事業者、小企業が大企業サイトに接続する方法を通じてのみオンライン疎通が可能な短所があった。
【０００４】
したがって、一定規模の流通システムを保有できる企業だけでなく、一般個人、個人事業者、小企業にとっても流通に対する信頼性が保証できる電子文書流通基盤のインフラ構築が期待されている。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
本発明は、前記のような従来の問題点を解決するためのものであり、本発明の目的は、公認電子アドレス基盤の電子文書の流通体系内で流通証明書を生成し流通、保管するにおいて透明で効率的な発給サービスを提供し、証明書の互換性の確保によって電子文書の流通信頼性を向上できる電子文書流通証明書の生成／発給方法を提供することにある。また、本発明の他の目的は、流通証明書の標準化した検証方法を定義して証明書の正しい活用に役に立つ流通証明書の検証方法を提供することにある。また、本発明の他の目的は、流通に対する信頼性が保証できる電子文書の流通システムを提供することにある。
【課題を解決するための手段】
【０００６】
前記のような目的を達成するための本発明の好ましい実施形態による電子文書流通証明書の生成／発給方法は、送受信個体と流通ハブとを含む電子文書の流通体系において流通証明書を生成／発給する方法であって、（ａ）送信個体は受信個体に送信者の電子文書を含む流通メッセージを転送するステップ；（ｂ）受信個体は流通メッセージを受信した後に必須情報を獲得して受信証明書を生成するステップ；（ｃ）受信個体は生成した受信証明書を送信個体に転送するステップ；（ｄ）送信個体は受信した受信証明書に対する検証を完了した後に受信証明書の電子署名認証書に対する検証情報を受信証明書に添付するステップ；および（ｅ）送信個体は受信証明書を第３者保管機関に転送して保管を依頼するステップ；を含む。
【０００７】
前記のような目的を達成するための本発明の好ましい実施形態による電子文書流通証明書の検証方法は、送受信個体と流通ハブとを含む電子文書の流通体系内で生成／発給された流通証明書を検証する方法であって、流通証明書のフォーマットが予め定められた構造および値の制約事項を守っているかを検証するステップ；流通証明書に設定された流通メッセージの送信日時、受信日時、閲覧日時、流通証明書の発給日、証明書の検証時点、および証明書の効力満期日が順序をなしているかを検証するステップ；流通証明書に添付された電子署名を検証するステップ；および流通証明書に電子署名を行った認証書の有効性有無を検証し、流通証明書の発給者情報との同一性有無を検証するステップ；を含む。

【０００８】
前記のような目的を達成するための本発明の好ましい実施形態による電子文書の流通方法は、電子文書を流通するシステムであって、電子アドレスを基盤にメッセージを送受信し、メッセージの送受信に対する流通証明書を発給および管理する流通メッセージングサーバを介して電子文書を流通する送受信個体；前記送受信個体の電子アドレスを登録／管理し、前記送受信個体間の電子文書の流通経路を設定し、送受信個体間の電子文書の流通過程でエラーが発生した時にメッセージの転送を代行し、流通証明書を発給する流通ハブ；および流通証明書の伝達を受けて保管し、信頼できる第３者保管機関；を含み、前記流通証明書は、受信個体のメッセージの受信事実に対する否認防止のための受信証明書と、送信個体の送信試みに対する証明のための送信証明書と、受信者の受信メッセージの閲覧事実に対する否認防止のための閲覧証明書とを含む。
【０００９】
前記のような本発明は、公認電子アドレス基盤の電子文書の流通体系内で流通証明書を生成し流通、保管するにおいて透明で効率的な発給サービスを提供できる効果がある。
また、前記のような本発明は、公認電子アドレス基盤の電子文書の流通体系内で証明書の互換性の確保によって電子文書の流通信頼性を向上できる効果がある。
【００１０】
なお、前記のような本発明は、流通証明書の標準化した検証方法を定義することにより、証明書の正しい活用に役に立つ流通証明書の検証方法を提供できる効果がある。
【図面の簡単な説明】
【００１１】
【図１】本発明による流通証明書の生成および発給について説明するための図面である。
【図２】本発明による流通証明書の生成および発給プロセスを示す図面である。
【発明を実施するための形態】
【００１２】
以下、添付した図面および表を参照し、本発明の好ましい実施形態による電子文書流通証明書の生成／発給方法、および電子文書流通証明書の検証方法、および電子文書の流通システムについて説明すれば、次の通りである。
【００１３】
本発明の好ましい実施形態による電子文書流通証明書の生成方法は、（ａ）送信個体は受信個体に送信者の電子文書を含む流通メッセージを転送するステップ；（ｂ）受信個体は流通メッセージを受信した後に必須情報を獲得して受信証明書を生成するステップ；（ｃ）受信個体は生成した受信証明書を送信個体に転送するステップ；（ｄ）送信個体は受信した受信証明書に対する検証を完了した後に受信証明書の電子署名認証書に対する検証情報を受信証明書に添付するステップ；および（ｅ）送信個体は受信証明書を第３者保管機関に転送して保管を依頼するステップ；を含む。
【００１４】
本発明の好ましい実施形態による電子文書流通証明書の証明方法は、流通証明書のフォーマットが予め定められた構造および値の制約事項を守っているかを検証するステップ；流通証明書に設定された流通メッセージの送信日時、受信日時、閲覧日時、流通証明書の発給日、証明書の検証時点、および証明書の効力満期日が順序をなしているかを検証するステップ；流通証明書に添付された電子署名を検証するステップ；および流通証明書に電子署名を行った認証書の有効性有無を検証し、流通証明書の発給者情報との同一性有無を検証するステップ；を含む。
【００１５】
本発明の好ましい実施形態による電子文書の流通システムは、電子アドレスを基盤にメッセージを送受信し、メッセージの送受信に対する流通証明書を発給および管理する流通メッセージングサーバを介して電子文書を流通する送受信個体；前記送受信個体の電子アドレスを登録／管理し、前記送受信個体間の電子文書の流通経路を設定し、送受信個体間の電子文書の流通過程でエラーが発生した時にメッセージの転送を代行し、流通証明書を

発給する流通ハブ；および流通証明書の伝達を受けて保管し、信頼できる第３者保管機関；を含み、前記流通証明書は、受信個体のメッセージの受信事実に対する否認防止のための受信証明書と、送信個体の送信試みに対する証明のための送信証明書と、受信者の受信メッセージの閲覧事実に対する否認防止のための閲覧証明書とを含む。

【００１６】

上述したような構成を有する本発明の好ましい実施形態による電子文書流通証明書の生成方法、電子文書流通証明書の検証方法、および電子文書の流通システムに対し、図１および図２を参照して詳細に説明すれば次の通りである。

［電子文書流通証明書の生成および発給モデル］

図１は本発明において流通証明書の生成および発給と関連した構成要素を示し、各構成要素について説明すれば、下記１）～２）の通りである。

【００１７】

１）送信個体（または送信電子文書の中継者、以下、送信個体、１０１）：基本的に送信者の電子文書を受信個体に転送したり、必要によっては、流通中継サーバに転送依頼を要請したりする。流通証明書と関連し、受信個体または流通中継サーバから受信した流通証明書を検証した後、検証情報を流通証明書に添付して第３者保管機関に保管する役割を遂行する。

【００１８】

２）受信個体（または受信電子文書の中継者、以下、受信個体、１０２）：基本的に送信個体または流通中継サーバから受信した電子文書を受信者に伝達する。流通証明書と関連し、送信個体または流通中継サーバから電子文書を受信した後、直ちに受信証明書を生成して送信個体または流通中継サーバに応答メッセージとして転送したり、受信者が電子文書を閲覧した後、直ちに閲覧証明書を生成して送信個体に転送したりする役割を遂行する。

【００１９】

３）電子文書流通ハブ（または流通中継サーバ、１０３）：基本的に送信個体から転送依頼を受けた電子文書を受信個体に伝達する。流通証明書と関連し、送信個体から電子文書の転送依頼を受けた後、直ちに送信証明書を生成して送信個体に転送したり、受信個体に電子文書を伝達した後、これに対する応答として受信した受信証明書を送信個体に伝達したりする役割を遂行する。

４）第３者保管機関（公認電子文書保管所；１０４）：信頼機関として流通証明書を安全に保管する役割を遂行する。

以下、本発明を説明するにおいて図１の図面符号は省略する。

［電子文書流通証明書の種類およびプロセス］

本発明による電子文書流通証明書および生成に必要な必須情報は下記表１の通りである。

【００２０】

【表１】

類型	目的	生成主体/時点	必須情報
受信 証明書	受信個体のメッセージの受信事実に対する否認防止	受信個体 /受信直後	文書情報、送信者、受信者、送信者の送信時刻、受信者の受信時刻
送信 証明書	送信個体の送信試みに対する証明	流通中継サーバ /送信依頼メッセージの受信直後	文書情報、送信者、受信者、送信者の送信依頼時刻
閲覧 証明書	受信者の受信メッセージの閲覧事実に対する否認防止	受信個体 /受信者の閲覧直後	文書情報、送信者、受信者、送信者の送信時刻、受信者の受信時刻、受信者の閲覧時刻

本発明による電子文書流通証明書の必須情報の獲得方法は下記表２の通りである。

【００２１】

【表２】

類型	必須情報	情報獲得方法
受信証明書	文書情報、送信者、受信者、送信者の送信時刻	送信個体が転送した流通連係メッセージ内の流通メッセージおよびＳＯＡＰメッセージの関連フィールド値を利用
	受信者の受信時刻	受信個体の流通メッセージングサーバの受信時刻を利用
送信証明書	文書情報、送信者、受信者	送信個体が転送した流通連係メッセージ内の流通メッセージの関連フィールド値を利用
	送信者の送信依頼時刻	流通中継サーバの受信時刻を利用
閲覧証明書	文書情報、送信者、受信者、送信者の送信時刻	送信個体が転送した流通連係メッセージ内の流通メッセージおよびＳＯＡＰメッセージの関連フィールド値を利用
	受信者の受信時刻	受信個体の流通メッセージングサーバの受信時刻を利用
	受信者の閲覧時刻	受信者の文書情報要請に対する受信個体の応答時刻を利用

※流通メッセージングサーバおよび流通中継サーバのシステム時刻は、周期的に外部公認された機関の時刻と同期化しなければならない。

本発明による電子文書流通証明書に関連した全体プロセスは図２の通りである。

【００２２】

受信証明書は送信個体から電子文書流通メッセージを受信した事実を証明するために生成する電子文書流通証明書であり、受信証明書と関連したプロセスは下記表３の通りである。

【００２３】

【表３】

番号	プロセス名
1	送信個体は受信個体に送信者の電子文書を含む流通メッセージを転送する。
2	受信個体は流通メッセージを受信した後、直ちに必須情報を獲得して受信証明書を生成する。
3	受信個体は生成した受信証明書を送信個体に転送する。
4	送信個体は受信証明書に対する検証を完了した後、受信証明書の電子署名認証書に対する検証情報を受信証明書に添付する。
5	送信個体は受信証明書を公認電子文書保管所に転送、保管する。

【００２４】

送信証明書は、送信個体が受信個体に流通メッセージの転送を試みたが、失敗して流通中継サーバに該当メッセージの転送を依頼する場合に、送信個体の送信依頼事実を証明するために流通中継サーバが生成して送信個体に転送する証明書であり、送信証明書と関連したプロセスは下記表４の通りである。

【００２５】

【表４】

番号	プロセス名
1	送信個体は受信個体に流通メッセージを転送する。
2	流通メッセージの転送が失敗した場合、送信個体は流通中継サーバに流通メッセージの転送を依頼する。
3	流通中継サーバは依頼を受けた転送に対する送信証明書を生成する。
4	流通中継サーバは送信証明書を送信個体に転送する。
5	送信個体は送信証明書に対する検証を完了した後、送信証明書の電子署名認証書に対する検証情報を送信証明書に添付する。
6	送信個体は送信証明書を公認電子文書保管所に保管する。
7	流通中継サーバは流通メッセージを受信個体に伝達する。
8	受信個体は電子文書を受信した直後に受信証明書を生成する。
9	受信個体は受信証明書を流通中継サーバに転送する。
10	流通中継サーバは受信証明書を送信個体に伝達する。
11	送信個体は受信証明書に対する検証を完了した後、受信証明書の電子署名認証書に対する検証情報を受信証明書に添付する。
12	送信個体は受信証明書を公認電子文書保管所に転送、保管する。

【００２６】

閲覧証明書は受信個体が送信個体から受信したメッセージを受信者が閲覧したことを証明するために受信個体が生成して送信個体に転送する証明書であり、閲覧証明書と関連したプロセスは下記表５の通りである。

【００２７】

【表５】

番号	プロセス名
1	受信者は受信個体に流通メッセージの閲覧を要請して応答として伝達を受けた流通メッセージを閲覧する。
2	受信個体は閲覧証明書を生成する。
3	受信個体は閲覧証明書に対する検証を完了した後、閲覧証明書の電子署名認証書に対する検証情報を閲覧証明書に添付する。
4	送信個体は閲覧証明書を公認電子文書保管所に転送、保管する。

［流通証明書の発給および検証と関連した基本的な前提条件および考慮事項］

流通証明書の発給および検証と関連し、基本的な前提条件および考慮しなければならな

い内容は次の１）～９）の通りである。
１）流通証明書は送受信個体の流通メッセージングサーバと流通中継サーバにおいて生成して検証する。
２）本発明において、流通証明書はＮＰＫＩ認証書を基盤にして電子署名して生成する。
【００２８】
３）流通メッセージを基準にこれに対応する流通証明書を生成する。１個の流通メッセージ内に２個以上の電子文書が含まれていても１個の流通証明書で対応しなければならない。
４）流通証明書は流通メッセージを識別できるＩＤと流通メッセージ内の電子文書を識別できる電子文書識別子または電子文書名を付与しなければならない。
５）流通証明書の一連番号は個別送受信個体が生成するので、唯一性の付与のために３２ｂｙｔｅの乱数を使う。
６）流通体系の特性上、流通証明書の更新および廃止は定義しない。
７）流通メッセージングサーバは、流通証明書内の時刻情報の信頼性の確保のために外部信頼機関の時刻情報と同期化を常に維持しなければならない。
８）流通証明書政策は、本技術規格で定義されたＯＩＤ（Ｏｂｊｅｃｔ　Ｉｄｅｎｔｉｆｉｅｒ；オブジェクト識別子）および名称だけを使う。
９）送信個体は、受信した流通証明書を検証した後、流通証明書の署名認証書に対する検証情報を流通証明書に添付する。
［電子文書流通証明書の構造］
【００２９】
電子文書流通証明書は送受信個体が生成し、送受信個体のＮＰＫＩ認証書を利用して電子署名する。電子文書流通証明書の基本構造は、ＣＭＳ標準のＳｉｇｎｅｄＤａｔａ構造を使って、公認電子文書保管所の証明書と同一のコンテンツ識別子を使用する。
電子文書流通証明書のｃｏｎｔｅｎｔＴｙｐｅは下記表６の通りである。
【００３０】

【表６】

```
id-kiec-arcCertReseponse OBJECT IDENTIFIER ::= { iso(1) member-body(2)
korea(410) kiec(200032) certificate(2) 2 }
ARCCertResponse ::= CHOICE {
arcCertInfo [0] EXPLICIT ARCCertInfo,
arcErrorNotice [1] EXPLICIT ARCErrorNotice }
```

電子文書流通証明書の基本フィールドは下記表７の通りである。
【００３１】

【表７】

```
ARCCertInfo ::= SEQUENCE {
version [0] EXPLICIT ARCVersion DEFAULT v1,
serialNumber SerialNumber,
issuer GeneralNames,
dateOfIssue GeneralizedTime,
dateOfExpire DateOfExpiration,
policy ARCCertificatePolicies,
requestInfo RequestInfo,
target TargetToCertify,
extionsions [1] EXPLICIT Extensions OPTIONAL }
```

上記のような流通証明書の基本フィールドについて詳細に説明すれば、次の１）～８）の通りである。

１）Ｖｅｒｓｉｏｎ、バージョン

電子文書流通証明書構造のバージョンを示す。

電子文書流通証明書のためにはｖ９に設定するべきであり、ｔａｒｇｅｔフィールドのｄｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓ方式を使う。

【００３２】

【表８】

```
ARCVersion ::= INTEGER {v1(1), v2(2), v9(9)}
```

２）ｓｅｒｉａｌＮｕｍｂｅｒ、一連番号

電子文書流通証明書の識別情報を示す。

【００３３】

電子文書流通証明書の一連番号は３２ｂｙｔｅの乱数を使い、唯一の陽の整数値として生成するようにする。電子文書流通証明書を処理するためには３２ｂｙｔｅの一連番号を処理できるべきである。

【００３４】

【表９】

```
SerialNumber ::= INTEGER
```

３）ｉｓｓｕｅｒ、証明書の発給者

電子文書流通証明書を発給する主体を示す。

【００３５】

本フィールドの値を生成する時には、必ずＧｅｎｅｒａｌＮａｍｅ構造体のｄｉｒｅｃｔｏｒｙＮａｍｅフィールドを使うようにし、受信個体または流通中継サーバが電子文書

流通証明書に電子署名を行った認証書のｓｕｂｊｅｃｔＤＮ値を抽出してそのまま設定する。

【００３６】

【表１０】

```
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
otherName                                       [0] OtherName,
rfc822Name                                      [1] IA5String,
dNSName                                         [2] IA5String,
x400Address                                     [3] ORAddress,
directoryName                                   [4] Name,
ediPartyName                                    [5] EDIPartyName,
uniformResourceIdentifier               [6] IA5String,
iPAddress                                           [7] OCTET STRING,
registeredID
[8] OBJECT IDENTIFIER }

Name ::= CHOICE {
RDNSequence }
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
type AttributeType,
value AttributeValue }

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

DirectoryString ::= CHOICE {
teletexString                     TeletexString (SIZE (1..MAX)),
printableString                PrintableString (SIZE (1..MAX)),
universalString                UniversalString (SIZE (1..MAX)),
utf8String                          UTF8String (SIZE (1..MAX)),
bmpString                         BMPString (SIZE (1..MAX)) }
```

４）ｄａｔａＯｆＩｓｓｕｅ、証明書の発給日

電子文書流通証明書を発給した時点を示す。

証明書の発給日はＧｅｎｅｒａｌｉｚｅｄＴｉｍｅ形式を使う。

５）ｄａｔａＯｆＥｘｐｉｒｅ、証明書の効力満期日

電子文書流通証明書の満了時点を示す。

【００３７】

電子文書流通証明書の効力満期日は証明書の発給日より未来であるべきであり、流通事実に対する証明を必要とする期間を考慮して十分に余裕をもって設定するようにする。

【００３８】

【表１１】

```
DateOfExpiration ::= GeneralizedTime
```

６）ｐｏｌｉｃｙ、証明書政策

電子文書流通証明書政策を示す。

【００３９】

本フィールドは、電子文書流通証明書の種類に応じた政策ＯＩＤと電子文書流通証明書の種類を表示するためのＱｕａｌｉｆｉｅｒ情報で構成される。Ｑｕａｌｉｆｉｅｒ情報としてｕｓｅｒＮｏｔｉｃｅのみを使っており、ｃＰＳｕｒｉは使わないことに注意する。電子文書流通証明書の種類はｕｓｅｒＮｏｔｉｃｅフィールド下位のｅｘｐｌｉｃｉｔＴｅｘｔフィールドを利用して表示するようにし、形式はＢＭＰＳｔｒｉｎｇを使わなければならない。

【００４０】

【表１２】

```
ARCCertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
policyIdentifier         CertPolicyId,
policyQualifiers         SEQUENCE SIZE (1..MAX) OF
PolicyQualifierInfo OPTIONAL }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
policyQualifierId           PolicyQualifierId,
qualifier                   ANY DEFINED BY policyQualifierId }

PolicyQualifierId ::= OBJECT IDENTIFIER ( id-qt-cps | id-qt-unotice )

Qualifier ::= CHOICE {
cPSuri              CPSuri,
userNotice          UserNotice }

UserNotice ::= SEQUENCE {
noticeRef          NoticeReference OPTIONAL,
explicitText        DisplayText OPTIONAL}

NoticeReference ::= SEQUENCE {
organization           DisplayText,
noticeNumbers           SEQUENCE OF INTEGER }

DisplayText ::= CHOICE {
ia5String             IA5String(SIZE (1..200)),
visibleString         VisibleString(SIZE (1..200)),
bmpString             BMPString(SIZE (1..200)),
utf8String           UTF8String(SIZE (1..200)) }
```

電子文書流通証明書内の政策ＯＩＤは証明書の種類に従うものであり、本発明で指定した値だけを使うべきである。

電子文書流通証明書の種類に応じたＯＩＤとＱｕａｌｉｆｉｅｒ情報は次の通りである。

【００４１】

【表１３】

証明書種類	政策 OID	Qualifier
送信証明書	1.2.410.200032.6.1	“送信証明書”
受信証明書	1.2.410.200032.6.2	“受信証明書”
閲覧証明書	1.2.410.200032.6.3	“閲覧証明書”

７）ｒｅｑｕｅｓｔＩｎｆｏ、証明書要請メッセージ情報
本フィールドはｎｕｌｌに設定する。
【００４２】

【表１４】

```
RequestInfo ::= CHOICE {
arcCertRequest              ARCCertRequest,
null                                    NULL }
```

８）ｔａｒｇｅｔ、証明対象
証明しようとする内容が含まれるフィールドである。
本フィールドは、必ず下位のｄｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓフィールドを使って流通メッセージに対する情報を設定するようにする。
【００４３】

【表１５】

```
TargetToCertify ::= CHOICE {
opRecord                        [0] EXPLICIT OperationRecord,
orgAndIssued                [1] EXPLICIT OriginalAndIssuedDocumentInfo,
dataHash                        [2] EXPLICIT HashedDataInfo
distributionInfos           [10] EXPLICIT DistributionInfos }

DistributionInfos ::= SEQUENCE OF DistributionInfo

DistributionInfo ::= SEQUENCE {
senderAdd                                   UTF8String,
receiverAdd                                 UTF8String,
dateOfSend                                   GeneralizedTime,
dateOfReceive                               [0] EXPLICIT GeneralizedTime
OPTIONAL,
dateOfReceiveConfirm          [1] EXPLICIT GeneralizedTime OPTIONAL,
distributionId                          UTF8String,
numberOfFiles                          INTEGER,
distributedFileInfos              DistributedFileInfos }
```

１）ｓｅｎｄｅｒＡｄｄ、送信者の公認電子アドレス
電子文書流通メッセージを送信した送信者の公認電子アドレスを示す。
２）ｒｅｃｅｉｖｅｒＡｄｄ、受信者の公認電子アドレス
電子文書流通メッセージを受信した受信者の公認電子アドレスを示す。
３）ｄａｔｅＯｆＳｅｎｄ、送信一時
送信者が流通メッセージを送信した時刻を示す。

【００４４】

受信証明書と閲覧証明書の送信一時は送信個体が流通メッセージを送信した時刻を意味し、"メッセージ転送"の流通連係メッセージ内のＳＯＡＰメッセージに含まれたＴｉｍｅＳｔａｍｐフィールドの値をＧｅｎｅｒａｌｉｚｅｄＴｉｍｅ形式で表示する。

【００４５】

送信証明書の送信一時は送信個体が流通中継サーバに流通メッセージを送信依頼した時刻を意味し、流通連係メッセージ内の時刻値を使う他の流通証明書とは異なり、流通中継サーバが"メッセージ転送依頼"の流通メッセージを受信した時刻を使うことに注意する。時刻フィールドと関連し、送信証明書には本フィールドだけが含まれ、受信日時フィールドおよび閲覧日時フィールドは生成しない。

４）ｄａｔｅＯｆＲｅｃｅｉｖｅ、受信日時
受信者が流通メッセージを受信した時刻を示す。

【００４６】

受信日時は受信証明書と閲覧証明書にのみ生成されるフィールドであり、受信個体の流通メッセージングサーバが"メッセージ転送"の流通メッセージを受信した時刻を設定するようにする。

受信日時は送信一時より以後であるべきであり、証明書を生成した時刻と同じであるか以前であるべきである。

５）ｄａｔｅＯｆＲｅｃｅｉｖｅＣｏｎｆｉｒｍ、閲覧日時

受信者が電子文書を受信した後に閲覧した時刻を示す。

【００４７】

閲覧日時は閲覧証明書にのみ生成されるフィールドであり、受信者の"メッセージ詳細情報要請"に対して受信個体の流通メッセージングサーバが応答した時刻を設定するようにする。この時刻は、受信個体が受信者に応答した流通連係メッセージ内のＳＯＡＰメッセージに含まれたＴｉｍｅＳｔａｍｐフィールドの値をＧｅｎｅｒａｌｉｚｅｄＴｉｍｅ形式で表示した値と同一であるべきである。

閲覧日時は証明書を生成した時刻と同じであるか以前であるべきであり、受信日時と同じであるか以後であるべきである。

６）ｄｉｓｔｒｉｂｕｔｉｏｎＩｄ、流通識別値

流通メッセージに対する識別値を示す。

電子文書流通証明書の発給対象の流通メッセージの固有識別値（Ｉｄｅｎｔｉｆｉｅｒ）をそのまま設定する。

７）ｎｕｍｂｅｒＯｆＦｉｌｅｓ、流通ファイル個数

流通メッセージに添付された電子文書ファイルの個数を示す。

実際の流通メッセージに添付された電子文書ファイルの個数を設定する。

８）ｄｉｅｔｒｉｂｕｔｅｄＦｉｌｅＩｎｆｏｓ、流通文書情報

【００４８】

流通メッセージは１つ以上の電子文書ファイルが添付されてもよく、個別ファイルに対する情報をＤｉｓｔｒｉｂｕｔｅｄＦｉｌｅ構造を使って設定するようにする。

【００４９】

【表１６】

```
DistributedFileInfos ::= SEQUENCE OF DistributedFile

DistributedFile ::= SEQUENCE {
fileHashedData                  HashedDataInfo,
fileId                                          [0] EXPLICIT UTF8String
OPTIONAL,
fileName                              [1] EXPLICIT UTF8String OPTIONAL }

HashedDataInfo ::= SEQUENCE {
hashAlg                                 HashAlgorithm,
hashedData                            BIT STRING }

HashAlgorithm ::= AlgorithmIdentifier
```

９）ｆｉｌｅＨａｓｈｅｄＤａｔａ、ファイルハッシュ情報

流通メッセージに添付された個別電子文書ファイルのハッシュ値を示す。

個別電子文書ファイルをｈａｓｈＡｌｇフィールドのハッシュアルゴリズムを使ってハッシュ値を生成した後にｈａｓｈｅｄＤａｔａフィールドに設定する。

１０）ｆｉｌｅｄ、ファイル識別値

流通メッセージに添付された個別電子文書ファイルの識別子を示す。

【００５０】

ファイル識別値は流通メッセージ内には存在せず、Ｍｕｌｔｉ　Ｐａｒｔメッセージで構成された全体流通連係メッセージにＭＩＭＥ形式で添付された個別電子文書ファイルのＣｏｎｔｅｎｔ－ＩＤ値をそのまま設定する。

本フィールドは選択的に使ってもよいが、ファイル名フィールドを使わない場合には必ず使うべきであり、ファイル識別値フィールドの使用を勧告する。

【００５１】

流通証明書の検証時、ファイル識別値フィールドとファイル名フィールドが両方とも存在すれば、ファイル識別値フィールドを優先的に使って証明対象の電子文書ファイルと比較検証をするようにする。

１１）ｆｉｌｅＮａｍｅ、ファイル名

流通メッセージに添付された個別電子文書ファイルのファイル名を示す。

【００５２】

前記のファイル識別値フィールドを生成しない場合にはファイル名フィールドが必ず生成されるべきであり、値としてはＭｕｌｔｉ　Ｐａｒｔメッセージで構成された全体流通連係メッセージにＭＩＭＥ形式で添付された個別電子文書ファイルのＣｏｎｔｅｎｔ－ＩＤ値をそのまま設定するようにする。仮にファイル識別値フィールドが生成されているのであれば、ファイル名フィールドは省略することができ、生成時には電子文書ファイルを補助的に識別できる値を設定するようにする。

電子文書流通証明書のプロファイルは下記表１７の通りである。

【００５３】

【表１７】

基本フィールド	内容	特異事項
version	バージョン	v9
serialNumber	一連番号	32byte の乱数
issuer	証明書発給者	署名認証書の subject DN
dateOfIssue	証明書の発給日	GeneralizedTime
dateOfExpire	証明書の効力満期日	GeneralizedTime
policy	証明書政策	OID ： 1.2.410.200032.6.1 （送信） ： 1.2.410.200032.6.2 （受信） ： 1.2.410.200032.6.3 （閲覧）
requestInfo	証明書要請メッセージ情報	null
target	証明対象	DistributionInfos 構造使用
senderAdd	送信者の公認電子アドレス	UTF8String
receiverAdd	受信者の公認電子アドレス	UTF8String
dateOfSend	送信日時	GeneralizedTime,必須
dateOfReceive	受信日時	GeneralizedTime,選択
dateOfReceiveConfirm	受信確認日時	GeneralizedTime,選択
distributionId	流通識別子	UTF8String
numberOfFiles	転送ファイル個数	
distributedFileInfos	転送ファイル情報	１つ以上の　DistributedFile
DistributedFile		
fileHashedData	ファイルハッシュ値	SHA256
fileId	ファイル ID	fileId と fileName ２つのフィールドのうちの１つは必須
fileName	ファイル名	

電子文書流通証明書のプロファイルと関連した考慮事項は次の１）～３）の通りである。

１）電子署名時の公開キー暗号アルゴリズムはＲＳＡを使い、ハッシュアルゴリズムはＳＨＡ２５６を使う。

２）ｓｉｇｎｅｄＤａｔａ内に電子署名認証書が必ず含まれなければならない。

３）ｓｉｇｎｅｒＩｎｆｏｓフィールドには１つのｓｉｇｎｅｒＩｎｆｏのみ含まれる。

［電子文書流通証明書の検証方法］

流通メッセージの送信個体は、電子文書流通証明書を受信した後、直ちに証明書に対する検証を遂行しなければならない。

【００５４】

流通証明書の検証過程は、大きく、証明書の有効性検証と証明書の内容検証に区分される。証明書の有効性検証は証明書としての効力を持つための条件の満足有無を確認する過程であり、証明書の内容検証は証明書を通じて証明しようとする流通メッセージとの対照を通じた事実確認の過程である。したがって、証明書の内容検証は、証明書に対する検証というよりは、流通事実に対する真偽有無を確認するために遂行すると見ることができる。

【００５５】

電子文書流通証明書の有効性検証は、１、証明書のフォーマット検証、２、証明書の時刻検証、３、証明書の電子署名の検証、４、署名認証書の検証の過程を通じて遂行され、証明書の内容検証は、５、流通メッセージの比較検証の過程を通じて遂行される。

１、証明書のフォーマット検証

【００５６】

証明書のフォーマット検証は、検証対象となる流通証明書のフォーマットが本規格で定義された構造および値の制約事項を守っているかを確認する過程であり、証明書のフォーマット検証時には、基本的に、下記１）～７）の事項を確認する。

１）流通証明書の全体構造がｓｉｇｎｅｄＤａｔａ形式を満足し、本規格で定義された下位フィールドの生成有無に対する規則を守っているのか？

２）バージョンがｖ９に設定されているのか？

３）一連番号は３２ｂｙｔｅの乱数を使って陽の整数値として生成されたのか？

４）証明書発給者はＧｅｎｅｒａｌＮａｍｅ構造体のｄｉｒｅｃｔｏｒｙＮａｍｅフィールドを使って設定されたのか？

５）証明書の発給日と証明書の効力満期日はＧｅｎｅｒａｌｉｚｅｄＴｉｍｅ形式を使って設定されたのか？

６）証明書政策は本規格で定義された下位フィールドの構造および値を使って生成されたのか？

【００５７】

７）証明対象フィールドはｄｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓフィールドを使って生成され、証明書政策で提示された証明書の種類に応じた下位フィールドの生成有無に対する規則を守っているのか？

２、証明書の時刻検証

【００５８】

証明書の時刻検証は検証基準となる時点に流通証明書に設定された各時刻フィールドの値が正常であるを確認する過程である。すなわち、本過程においては、流通証明書に設定された各時刻フィールドの値が検証基準時点と比較して下記表１８の規則を満足していることを確認するようにする。

【００５９】

【表１８】

送信日時＜受信日時≦閲覧日時≦証明書の発給日≦証明書の検証時点≦証明書の効力満期日

３、証明書の電子署名の検証

【００６０】

電子署名の検証は流通証明書が証明しようとする内容に対する無欠性の保障および否認防止のために流通証明書に添付された電子署名を検証する過程であり、一般的なＣＭＳの

ｓｉｇｎｅｄＤａｔａに対する電子署名の検証方法に従う。

４、署名認証書の検証

署名認証書の検証は、流通証明書に電子署名を行った認証書の有効性有無および流通証明書の発給者情報との同一性有無を検証する過程である。

【００６１】

電子署名認証書の有効性の検証は一般的に電子署名の検証過程の一部として含まれる手続きであり、認証書の有効期間の検証、廃止有無の検証、そして上位ＣＡ認証書との経路検証の過程などを通じて遂行される。このために公認認証体系の"公認認証書の経路検証の技術規格［ＫＣＡＣ．ＴＳ．ＣＥＲＴＶＡＬ］"を準用して検証するようにする。

【００６２】

電子署名認証書の有効性の検証に成功したのであれば、流通証明書の発給者情報との比較検証を遂行しなければならない。流通証明書の発給者情報は電子署名認証書のｓｕｂｊｅｃｔ　ＤＮ値をそのまま設定するようになっているので、２つの値を抽出して一致するか否かの比較検証を行う。

５、流通メッセージの比較検証

【００６３】

流通メッセージの比較検証の過程は、流通証明書の有効性有無を検証する過程ではなく、流通証明書に含まれた流通メッセージの情報と実際の流通メッセージとを比較検証することにより、流通事実に対する真偽有無を確認する過程である。

【００６４】

送信個体が流通メッセージを転送または転送依頼した後に流通証明書を受信するようになれば、本流通メッセージの比較検証を必ず遂行して、該当流通証明書が自身が送信した流通メッセージに対する情報を含んでいることを確認しなければならない。

流通メッセージの比較検証時に基本的に下記の事項を確認する。

－送信者の公認電子アドレスおよび受信者の公認電子アドレスが流通メッセージと一致するのか？

【００６５】

－受信証明書および閲覧証明書の送信一時の場合、"メッセージ転送"の流通連係メッセージ内のＳＯＡＰメッセージに含まれたＴｉｍｅＳｔａｍｐフィールドの値と一致するのか？

－送信証明書の送信一時の場合、流通中継サーバが"メッセージ転送依頼"の流通メッセージを受信するのに合理的な時刻であるのか？

【００６６】

－送信個体が受信個体に直接転送した"メッセージ転送"の流通メッセージに対する受信証明書と閲覧証明書の受信日時の場合、受信個体の流通メッセージングサーバが"メッセージ転送"の流通メッセージを受信するのに合理的な時刻であるのか？

【００６７】

－送信個体が流通中継サーバに依頼した"メッセージ転送依頼"の流通メッセージに対する受信証明書と閲覧証明書の受信日時の場合、受信個体の流通メッセージングサーバが"メッセージ転送"の流通メッセージを受信するのに合理的な時刻であるのか？（但し、流通中継サーバが受信個体に流通メッセージを伝達した時刻を送信個体が知ることができる場合に限る）

【００６８】

－閲覧証明書の閲覧日時の場合、受信個体が受信者の"メッセージ詳細情報要請"に対して応答した流通連係メッセージ内のＳＯＡＰメッセージに含まれたＴｉｍｅＳｔａｍｐフィールドの値と一致するのか？（但し、該当ＴｉｍｅＳｔａｍｐフィールドの値を送信個体が知ることができる場合に限る）

－流通識別値は、流通証明書の発給対象の流通メッセージの固有識別値（Ｉｄｅｎｔｉｆｉｅｒ）と一致するのか？

－流通ファイル個数は、実際の流通メッセージに添付された電子文書ファイルの個数と

同一であるのか？

【００６９】

－流通文書情報内に含まれた個別ファイルのファイル識別値またはファイル名が実際の流通メッセージに添付された電子文書ファイルのＣｏｎｔｅｎｔ－ＩＤ値と全て一致するのか？

【００７０】

－流通文書情報内に含まれた個別ファイルのファイルハッシュ情報が実際の流通メッセージに添付された電子文書ファイルをハッシュした値と全て一致するのか？

［電子署名の長期検証情報］

【００７１】

流通証明書の重要度を考慮し、発給された流通証明書に対する検証が完了すれば、公認電子文書保管所に登録して保管するようにしているが、これは、流通証明書の保管時点および無欠性に対する長期保障機能を提供するだけであって、電子署名認証書の有効期間が満了した後、流通証明書の発給時点の電子署名認証書に対する有効性まで長期的に保障することはできない。すなわち、電子署名認証書の有効期間が満了した後には流通証明書の有効性保障が不可となる。これを解決するために、流通証明書が発給された時点に該当電子署名認証書が有効であったことを確認できる検証情報を流通証明書と共に保管することにより、流通証明書に電子署名を行った認証書の有効期間が満了した後にも流通証明書に対する検証を可能にする。

１）電子署名認証書の検証情報の獲得

【００７２】

送信個体は、受信した流通証明書の有効性を検証する過程中、"５．２．４署名認証書の検証"過程を遂行するために、電子署名認証書の廃止有無および経路検証のためにＣＲＬとＡＲＬ、そして上位ＣＡ認証書とＲｏｏｔ　ＣＡ認証書を収集する。該当データを流通証明書と共に公認電子文書保管所に保管することにより、流通証明書の発給時点の電子署名認証書の有効性を保障し、その結果、流通証明書の有効性まで保障するようになる。

２）電子署名認証書の検証情報の格納

【００７３】

送信個体は電子署名認証書に対する検証に成功した後、検証に使われたＣＲＬとＡＲＬ、そして上位ＣＡ認証書とＲｏｏｔ　ＣＡ認証書を流通証明書のｓｉｇｎｅｄＤａｔａ構造内のｃｅｒｔｉｆｉｃａｔｅｓフィールドとｃｒｌｓフィールドに含ませる。各々の情報を含ませる順は関係なく、注意しなければならない点は単に該当フィールドに各々の情報を含ませる作業だけを遂行しなければならないということである。ｃｅｒｔｉｆｉｃａｔｅｓフィールドとｃｒｌｓフィールドはｓｉｇｎｅｄＤａｔａの電子署名の対象情報ではないため、該当作業を遂行した後にも流通証明書に対する検証は相変らず成功するようになる。

【００７４】

【表１９】

```
SignedData ::= SEQUENCE {
version                  CMSVersion,
digestAlgorithms          DigestAlgorithmIdentifiers,
encapContentInfo          EncapsulatedContentInfo,
certificates              [0] IMPLICIT CertificateSet OPTIONAL,
crls                      [1] IMPLICIT RevocationInfoChoices OPTIONAL,
signerInfosSignerInfos }
```

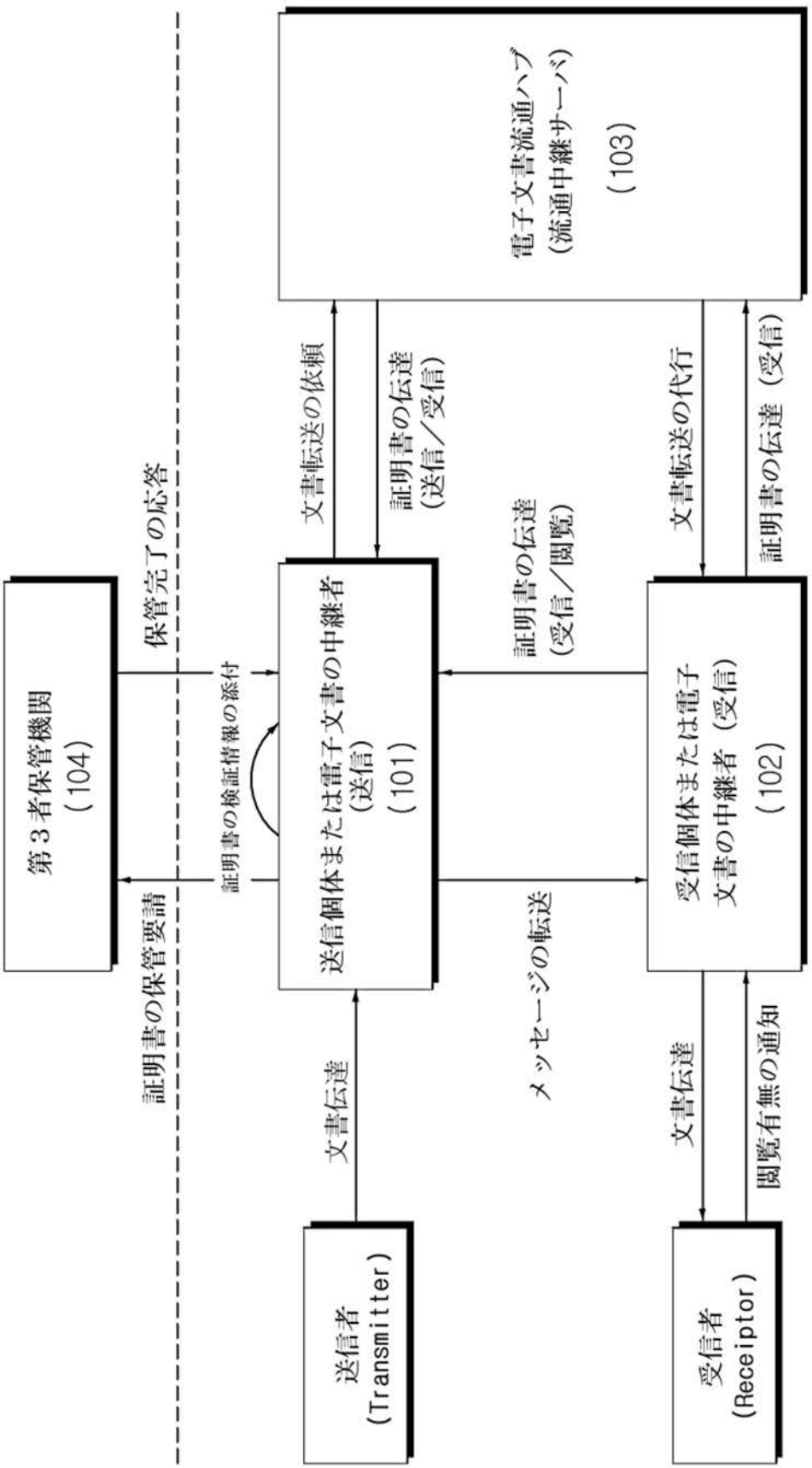
３）公認電子文書保管所の保管

【００７５】

送信個体は電子署名認証書の検証情報が含まれた流通証明書を公認電子文書保管所に保管するべきであり、これによって流通証明書に対する長期検証が可能となる。

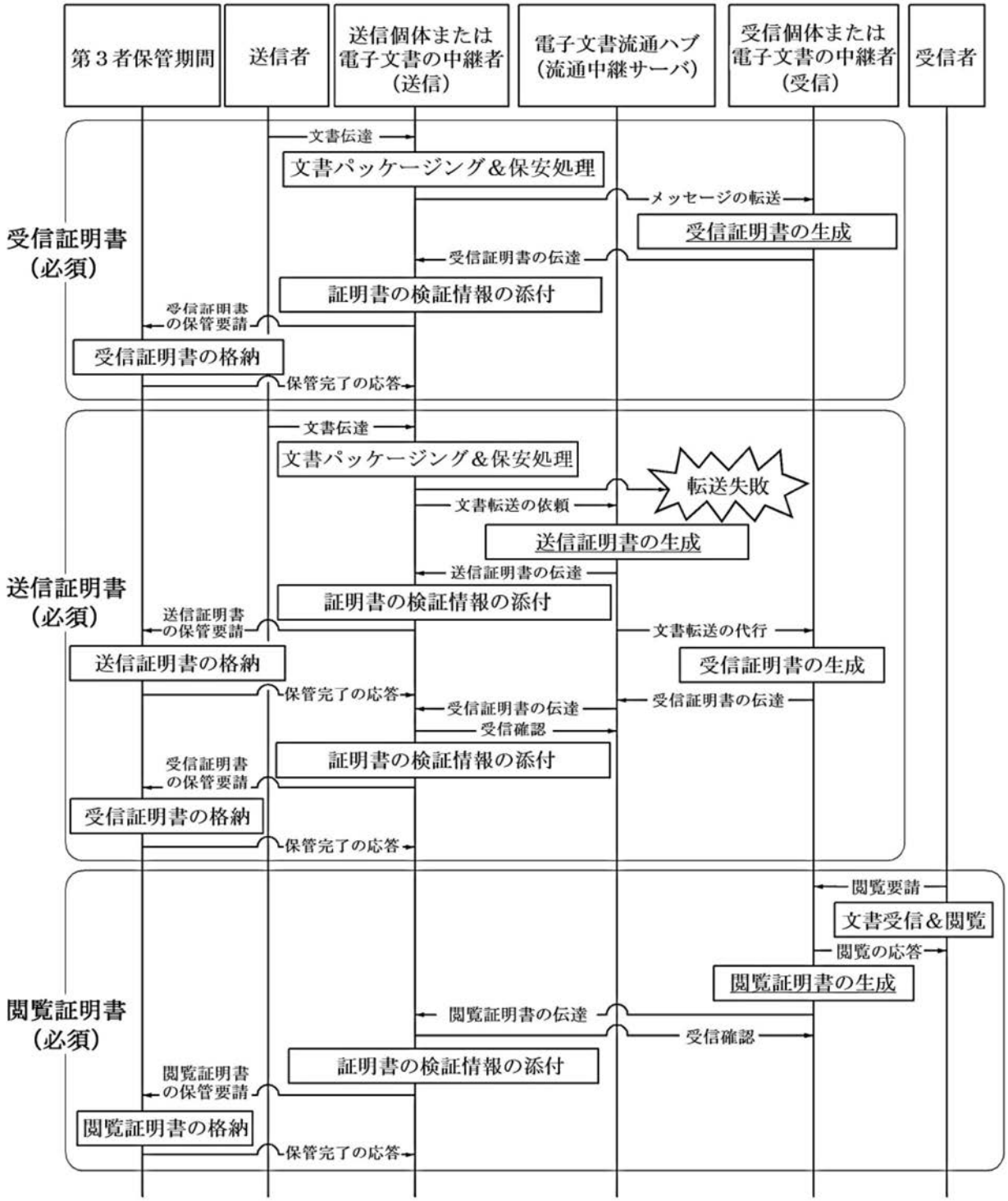
【図１】

【図１】


第３者保管機関
(104)
保管完了の応答
証明書の保管要請
証明書の検証情報の添付
送信個体または電子文書の中継者
(送信)
(101)
文書転送の依頼
証明書の伝達
(送信／受信)
電子文書流通ハブ
(流通中継サーバ)
(103)
証明書の伝達
(受信／閲覧)
文書転送の代行
証明書の伝達（受信）
受信個体または電子
文書の中継者（受信）
(102)
メッセージの転送
文書伝達
閲覧有無の通知
送信者
(Transmitter)
受信者
(Receiptor)

【図２】

【図２】


第３者保管期間
送信者
送信個体または
電子文書の中継者
（送信）
電子文書流通ハブ
（流通中継サーバ）
受信個体または
電子文書の中継者
（受信）
受信者
受信証明書
（必須）
文書伝達
文書パッケージング＆保安処理
メッセージの転送
受信証明書の生成
受信証明書の伝達
証明書の検証情報の添付
受信証明書
の保管要請
受信証明書の格納
保管完了の応答
送信証明書
（必須）
文書伝達
文書パッケージング＆保安処理
転送失敗
文書転送の依頼
送信証明書の生成
送信証明書の伝達
証明書の検証情報の添付
送信証明書
の保管要請
文書転送の代行
送信証明書の格納
受信証明書の生成
保管完了の応答
受信証明書の伝達
受信証明書の伝達
受信確認
証明書の検証情報の添付
受信証明書
の保管要請
受信証明書の格納
保管完了の応答
閲覧証明書
（必須）
閲覧要請
文書受信＆閲覧
閲覧の応答
閲覧証明書の生成
閲覧証明書の伝達
受信確認
証明書の検証情報の添付
閲覧証明書
の保管要請
閲覧証明書の格納
保管完了の応答

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2011/005039

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 50/00(2006.01)i, G06F 17/21(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q 50/00; G06F 15/16; G06F 15/00; G06Q 10/00; H04L 12/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: certificate, document distribution, verification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2009-0027554 A (KOREA INSTITUTE FOR ELECTRONIC COMMERCE) 17 March 2009 See abstract, figures 1-7, claims 1-19, paragraphs <120>, <231>-<254>.	1-7
Y	KR 10-2008-0014194 A (KOREA INSTITUTE FOR ELECTRONIC COMMERCE) 14 February 2008 See abstract, figures 1-8, claims 1-23.	1-7
A	KR 10-0653512 B1 (SAMSUNG S.D.S CO., LTD.) 05 December 2006 See abstract, figures 1-5, claims 1-12.	1-7
A	KR 10-2005-0078402 A (DREAM TO REALITY) 05 August 2005 See abstract, figures 1-6, claims 1-10.	1-7

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 APRIL 2012 (05.04.2012)	**09 APRIL 2012 (09.04.2012)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2011/005039

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The invention of group 1: claims 1 to 7 pertain to a method for generating and issuing a distribution certificate in an electronic document distribution system,

The invention of group 2: claims 8 to 14 pertain to a method for verifying a distribution certificate,

The invention of group 3: claims 15 to 17 pertain to an electronic document distribution system which distributes an electronic document using a distribution certificate, transmits a message when an error occurs in a distribution process, and includes a storage device storing a distribution certificate.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
claims 1 to 7

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2011/005039

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0027554 A	17.03.2009	NONE	
KR 10-2008-0014194 A	14.02.2008	CN 101326517 A	17.12.2008
		EP 1917604 A1	07.05.2008
		JP 2009-512001 A	19.03.2009
		US 2009-0307756 A1	10.12.2009
		WO 2008-018744 A1	14.02.2008
KR 10-0653512 B1	05.12.2006	NONE	
KR 10-2005-0078402 A	05.08.2005	NONE	

Form PCT/ISA/210 (patent family annex) (July 2009)

국제조사보고서

국제출원번호
PCT/KR2011/005039

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06Q 50/00(2006.01)i, G06F 17/21(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06Q 50/00; G06F 15/16; G06F 15/00; G06Q 10/00; H04L 12/22

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 증명서, 문서유통, 검증

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2009-0027554 A (한국전자거래진흥원) 2009.03.17 요약, 도면 1-7, 청구항 제1-19항, 단락 <120>. <231>-<254> 참조.	1-7
Y	KR 10-2008-0014194 A (한국전자거래진흥원) 2008.02.14 요약, 도면 1-8, 청구항 제1-23항 참조.	1-7
A	KR 10-0653512 B1 (삼성에스디에스 주식회사) 2006.12.05 요약, 도면 1-5, 청구항 제1-12항 참조.	1-7
A	KR 10-2005-0078402 A ((주)드림부리얼리티) 2005.08.05 요약, 도면 1-6, 청구항 제1-10항 참조.	1-7

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2012년 04월 05일 (05.04.2012)	**2012년 04월 09일 (09.04.2012)**

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
정부대전청사
팩스 번호 82-42-472-7140

심사관
최석규
전화번호 82-42-481-5778

서식 PCT/ISA/210 (두 번째 용지) (2009년 7월)

국제조사보고서

국제출원번호
PCT/KR2011/005039

제2기재란 일부 청구항을 조사할 수 없는 경우의 의견(첫 번째 용지의 2의 계속)

PCT 제17조(2)(a)의 규정에 따라 다음과 같은 이유로 일부 청구항에 대하여 본 국제조사보고서가 작성되지 아니하였습니다.

1. ☐ 청구항:
이 청구항은 본 기관이 조사할 필요가 없는 대상에 관련됩니다. 즉,

2. ☐ 청구항:
이 청구항은 유효한 국제조사를 수행할 수 없을 정도로 소정의 요건을 충족하지 아니하는 국제출원의 부분과 관련됩니다. 구체적으로는,

3. ☐ 청구항:
이 청구항은 종속청구항이나 PCT규칙 6.4(a)의 두 번째 및 세 번째 문장의 규정에 따라 작성되어 있지 않습니다.

제3기재란 발명의 단일성이 결여된 경우의 의견(첫 번째 용지의 3의 계속)

본 국제조사기관은 본 국제출원에 다음과 같이 다수의 발명이 있다고 봅니다.

제1군 발명: 청구항 1-7은 전자문서 유통 체계에서 유통증명서를 생성, 발급하는 방법에 관한 것이고,

제2군 발명: 청구항 8-14는 유통증명서를 검증하는 방법에 관한 것이고,

제3군 발명: 청구항 15-17은 유통증명서를 이용해 전자문서를 유통하고 유통과정에 오류 발생시 메시지 전송을 대행하며 유통증명서를 보관하는 보관기관을 포함하는 전자문서 유통 시스템에 관한 것입니다.

1. ☐ 출원인이 모든 추가수수료를 기간 내에 납부하였으므로, 본 국제조사보고서는 모든 조사 가능한 청구항을 대상으로 합니다.

2. ☐ 추가수수료 납부를 요구하지 않고도 모든 조사 가능한 청구항을 조사할 수 있었으므로, 본 기관은 추가수수료 납부를 요구하지 아니하였습니다.

3. ☐ 출원인이 추가수수료의 일부만을 기간 내에 납부하였으므로, 본 국제조사보고서는 수수료가 납부된 청구항만을 대상으로 합니다. 구체적인 청구항은 아래와 같습니다.

4. ☒ 출원인이 기간 내에 추가수수료를 납부하지 아니하였습니다. 따라서 본 국제조사보고서는 청구범위에 처음 기재된 발명에 한정되어 있으며, 해당 청구항은 아래와 같습니다.
청구항 제1항 내지 제7항

이의신청에 관한 기재

☐ 출원인의 이의신청 및 이의신청료 납부(해당하는 경우)와 함께 추가수수료가 납부되었습니다.

☐ 출원인의 이의신청과 함께 추가수수료가 납부되었으나 이의신청료가 보정요구서에 명시된 기간 내에 납부되지 아니하였습니다.

☐ 이의신청 없이 추가수수료가 납부되었습니다.

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2011/005039

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0027554 A	2009.03.17	없음	
KR 10-2008-0014194 A	2008.02.14	CN 101326517 A	2008.12.17
		EP 1917604 A1	2008.05.07
		JP 2009-512001 A	2009.03.19
		US 2009-0307756 A1	2009.12.10
		WO 2008-018744 A1	2008.02.14
KR 10-0653512 B1	2006.12.05	없음	
KR 10-2005-0078402 A	2005.08.05	없음	

서식 PCT/ISA/210 (대응특허 추가용지) (2009년 7월)

フロントページの続き

(31)優先権主張番号 10-2010-0065985
(32)優先日 平成22年7月8日(2010.7.8)
(33)優先権主張国 韓国(KR)

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100130672
弁理士 伊藤 寛之
(72)発明者 アン、デソブ
大韓民国、１３９－７７７、ソウル、ノウォン－グ、ハゲードン、サムイク ソンギョン アパート １－６０６
(72)発明者 イ、ズング
大韓民国、１３８－９３０、ソウル、ソンパーグ、ザムシル４－ドン、パクリオ アパート １１４－２３０３
(72)発明者 ゴン、ソンピル
大韓民国、４６３－７６４、ギョンギード、ソンナム－シ、ブンダン－グ、ソヒョン－ドン、ヒョザチョン ラッキ アパート ６２５－３０１
(72)発明者 イム、ヨンチョル
大韓民国、１５１－０５０、ソウル、グァンアク－グ、ボンチョン－２ドン、ドンアアパート １０７－８０８

Ｆターム(参考) 5J104 AA09 AA16 EA08 LA06 MA01 NA38 PA07