【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成26年5月22日(2014.5.22)

【公表番号】特表2013-535858(P2013-535858A)
【公表日】平成25年9月12日(2013.9.12)
【年通号数】公開・登録公報2013-050
【出願番号】特願2013-518281(P2013-518281)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｑ　50/10　(2012.01)
Ｇ０６Ｆ　21/33　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０６Ｑ　50/10　１９０
Ｇ０６Ｆ　21/20　１３３

【手続補正書】
【提出日】平成26年4月4日(2014.4.4)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【発明の詳細な説明】
【発明の名称】電子文書流通システムおよび電子文書流通方法
【技術分野】
【０００１】
本発明は、企業／機関などと共に一般個人、小企業も信頼性が確保できる電子文書流通体系を構築することが可能な電子文書流通システムおよび電子文書流通方法に関する。
【背景技術】
【０００２】
一般的に、電子文書流通は、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にのみ限定的に行われてきた。
【０００３】
また、一般個人間、個人と企業／機関間には、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、一定規模の電子文書流通システムを保有できる企業／機関などと共に一般個人、小企業にも信頼性が確保できる電子文書流通システムおよび電子文書流通方法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有する本発明の好ましい実施形態による電子文書流通システムは、電子文書を流通するシステムにおいて、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と；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、前記送受信個体に電子文書の標準書式を提供し、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；を含む。
【０００７】
前記のような目的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システムは、送受信個体と流通ハブを含む電子文書流通システムで電子文書を流通する方法において、（ａ）送信個体は、受信個体のアドレス情報に対応する物理アドレス情報を流通ハブを介して獲得した後に、電子文書を添付したメッセージを前記物理アドレスに転送するステップと；（ｂ）メッセージを受信した受信個体は、受信メッセージおよび送信個体に対する適合性の検証結果に応じて受信証明書またはエラー証明書を発給して、送信個体に伝達するステップ；および（ｃ）受信個体にメッセージを転送したものの失敗した送信個体は、流通ハブにメッセージ転送の代行を依頼し、メッセージ転送の代行依頼を受けた流通ハブは、送信証明書を発給して送信個体に伝達し、受信個体にメッセージを転送した後に、前記（ｂ）ステップを遂行するステップ；を含む。
【０００８】
前記のような構成および方法を有する本発明は、企業／機関などと共に個人、小企業にも信頼性が確保できる電子文書流通体系を構築することが可能な効果がある。
【図面の簡単な説明】
【０００９】
【図１】本発明の好ましい実施形態による電子文書流通システムの構成例を示す図面である。
【図２】図１の流通メッセージングサーバについて説明するための図面である。
【図３】図１の流通クライアントについて説明するための図面である。
【図４】図１のアドレスディレクトリサーバについて説明するための図面である。
【図５】図１の電子文書の書式登録機について説明するための図面である。
【図６】図１の流通中継サーバについて説明するための図面である。
【図７】図１の外部連係ゲートウェイについて説明するための図面である。
【図８】図１の電子文書流通システム内で公認電子アドレスが有する効力範囲を説明するための図面である。
【図９】本発明の好ましい実施形態において、公認電子アドレスの申請／発給および運営体系を説明するための図面である。
【図１０】本発明の好ましい実施形態において、電子文書を流通する時のメッセージ保安について説明するための図面である。
【図１１】本発明の好ましい実施形態において、電子文書を流通する時のメッセージ保安について説明するための図面である。
【図１２】本発明の好ましい実施形態において、電子文書を流通する時のメッセージ保安について説明するための図面である。
【図１３】本発明の好ましい実施形態において、電子文書を流通する時のメッセージ保安について説明するための図面である。
【図１４】本発明の好ましい実施形態において、メッセージ送受信プロセスについて説明するための図面である。
【図１５】本発明の好ましい実施形態において、メッセージ送受信プロセスについて説明するための図面である。
【図１６】本発明の好ましい実施形態において、メッセージ送受信プロセスについて説明

するための図面である。
【図１７】本発明の好ましい実施形態において、メッセージ送受信プロセスについて説明するための図面である。
【図１８】本発明の好ましい実施形態において、物理アドレス獲得プロセスを説明するための図面である。
【図１９】本発明の好ましい実施形態において、流通中継支援プロセスを説明するための図面である。
【図２０】本発明の好ましい実施形態において、流通中継支援プロセスを説明するための図面である。
【図２１】本発明の好ましい実施形態において、流通中継支援プロセスを説明するための図面である。
【図２２】本発明の好ましい実施形態において、公認電子アドレス登録などの管理プロセスを説明するための図面である。
【図２３】本発明の好ましい実施形態において、公認電子アドレス登録などの管理プロセスを説明するための図面である。
【図２４】本発明の好ましい実施形態において、公認電子アドレス登録などの管理プロセスを説明するための図面である。
【図２５】本発明の好ましい実施形態において、電子文書の書式適用プロセスを説明するための図面である。
【図２６】本発明の好ましい実施形態において、電子文書の書式適用プロセスを説明するための図面である。
【図２７】本発明の好ましい実施形態において、スパムメッセージ処理プロセスを説明するための図面である。
【図２８】本発明の好ましい実施形態において、スパムメッセージ処理プロセスを説明するための図面である。
【図２９】本発明の好ましい実施形態において、スパムメッセージ処理プロセスを説明するための図面である。
【図３０】本発明の好ましい実施形態において、電子文書閲覧サービスの概念図を示す図面である。
【図３１】本発明の好ましい実施形態において、電子文書閲覧サービスの概念図を示す図面である。
【図３２】本発明の好ましい実施形態において、外部連係ゲートウェイサーバの概念図を示す図面である。
【図３３】本発明の好ましい実施形態において、外部システムと連係して電子文書が流通される手続きを説明するための図面である。
【図３４】本発明の好ましい実施形態において、スパムメッセージ処理プロセスを説明するための図面である。
【図３５】本発明の好ましい実施形態において、スパムメッセージ処理プロセスを説明するための図面である。
【図３６】本発明の好ましい実施形態において、スパムメッセージ処理プロセスを説明するための図面である。
【図３７】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図３８】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図３９】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図４０】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図４１】本発明の好ましい実施形態による流通メッセージングサーバシステムについて

説明するための図面である。
【図４２】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図４３】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図４４】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図４５】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図４６】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図４７】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図４８】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図４９】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図５０】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図５１】本発明の好ましい実施形態による流通メッセージングサーバシステムについて説明するための図面である。
【図５２】本発明の好ましい実施形態による電子文書流通システムおよび方法に適用される流通プロトコルについて説明するための図面である。
【図５３】本発明の好ましい実施形態による電子文書流通システムおよび方法に適用される流通プロトコルについて説明するための図面である。
【図５４】本発明の好ましい実施形態による電子文書流通システムおよび方法に適用される流通プロトコルについて説明するための図面である。
【図５５】本発明の好ましい実施形態による電子文書流通システムおよび方法に適用される流通プロトコルについて説明するための図面である。
【図５６】本発明の好ましい実施形態による電子文書流通システムおよび方法に適用される流通プロトコルについて説明するための図面である。
【図５７】本発明の好ましい実施形態による電子文書の書式登録機について説明するための図面である。
【図５８】本発明の好ましい実施形態による電子文書の書式登録機について説明するための図面である。
【図５９】本発明の好ましい実施形態による電子文書流通システムおよび方法に適用される電子文書パッケージングについて説明するための図面である。
【図６０】本発明の好ましい実施形態による流通クライアントアプリケーションについて説明するための図面である。
【図６１】本発明の好ましい実施形態による流通クライアントアプリケーションについて説明するための図面である。
【図６２】本発明の好ましい実施形態による流通クライアントアプリケーションについて説明するための図面である。
【図６３】本発明の好ましい実施形態による流通クライアントアプリケーションについて説明するための図面である。
【図６４】本発明の好ましい実施形態による流通クライアントアプリケーションについて説明するための図面である。
【図６５】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバシステムが認証を受けて公認電子アドレスとして登録を受けるための手続きを示す図面である。

【図６６】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントアプリケーションについて説明するための図面である。
【図６７】本発明の好ましい実施形態による電子文書流通システムにおいて、電子文書流通のために各構成要素間に互いに連係して動作するための通信プロトコルの構成を説明するための図面である。
【図６８】本発明の好ましい実施形態による電子文書流通システムにおいて、電子文書流通のために各構成要素間に互いに連係して動作するための通信プロトコルの構成を説明するための図面である。
【図６９】本発明の好ましい実施形態による電子文書流通システムにおいて、電子文書流通のために各構成要素間に互いに連係して動作するための通信プロトコルの構成を説明するための図面である。
【図７０】本発明の好ましい実施形態による電子文書流通システムにおいて、電子文書流通のために各構成要素間に互いに連係して動作するための通信プロトコルの構成を説明するための図面である。
【図７１】本発明の好ましい実施形態による電子文書流通システムにおいて、電子文書流通のために各構成要素間に互いに連係して動作するための通信プロトコルの構成を説明するための図面である。
【図７２】本発明の好ましい実施形態による電子文書流通システムにおいて、エラー処理方法を説明するための図面である。
【図７３】本発明の好ましい実施形態による電子文書流通システムにおいて、エラー処理方法を説明するための図面である。
【図７４】本発明の好ましい実施形態による電子文書流通システムにおいて、エラー処理方法を説明するための図面である。
【図７５】本発明の好ましい実施形態による電子文書流通システムにおいて、エラー処理方法を説明するための図面である。
【図７６】本発明の好ましい実施形態による電子文書流通システムにおいて、エラー処理方法を説明するための図面である。
【図７７】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースを説明するための図面である。
【図７８】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースを説明するための図面である。
【図７９】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースを説明するための図面である。
【図８０】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースを説明するための図面である。
【図８１】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースを説明するための図面である。
【図８２】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースを説明するための図面である。
【図８３】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースを説明するための図面である。
【図８４】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースを説明するため

の図面である。
【図８５】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図８６】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図８７】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図８８】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図８９】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９０】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９１】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９２】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９３】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９４】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９５】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９６】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９７】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９８】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図９９】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバ相互間の連係インターフェースを説明するための図面である。
【図１００】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１０１】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１０２】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１０３】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１０４】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１０５】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１０６】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クラ

イアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１０７】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１０８】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１０９】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１１０】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１１１】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１１２】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１１３】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１１４】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１１５】本発明の好ましい実施形態による電子文書流通システムにおいて、流通クライアントと流通メッセージングサーバ間の連係インターフェースを説明するための図面である。
【図１１６】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバと流通中継サーバ間の連係インターフェースを説明するための図面である。
【図１１７】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバと流通中継サーバ間の連係インターフェースを説明するための図面である。
【図１１８】本発明の好ましい実施形態による電子文書流通システムにおいて、流通メッセージングサーバと流通中継サーバ間の連係インターフェースを説明するための図面である。
【図１１９】（ａ）は表３７の郵便流通体系を示す図面であり、（ｂ）は表３７のｅ－メール流通体系を示す図面であり、（ｃ）は表３７の電子文書交換（ＥＤＩ）流通体系を示す図面であり、（ｄ）は表３７の業務関連システム流通体系を示す図面である。
【図１２０】（ａ）は表３８の自動処理方式を示す図面であり、（ｂ）は表３８の半自動処理方式を示す図面である。
【図１２１】（ａ）は表３９のウェブ方式を示す図面であり、（ｂ）は表３９のアプリケーション方式を示す図面である。
【発明を実施するための形態】
【００１０】
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システムおよび電子文書流通方法について説明すれば、次の通りである。
図１は本発明の好ましい実施形態による電子文書流通システムの構成例を示す。

【００１１】
図１を参照すれば、本発明の好ましい実施形態による電子文書流通システムは、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１０１と；前記送受信個体１０１の電子アドレスを登録／管理し、前記送受信個体１０１間の電子文書の流通経路を設定し、前記送受信個体１０１に電子文書の標準書式を提供し、送受信個体１０１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電子文書流通ハブ１０２；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（公電所（公認電子文書保管所）１０３）；を含んで構成される。
【００１２】
前記送受信個体１０１の流通メッセージングサーバは、送受信したメッセージはユーザ別に状態情報を含ませてメッセージ箱に保管し、メッセージ送受信履歴を編集および削除が不可能な媒体に所定期間保管し、メッセージ送受信に対する流通証明書を発給して前記第３者保管機関に保管を依頼し、前記電子文書流通ハブ１０２のアドレスディレクトリサーバとの連係を通じて前記送受信個体１０１に電子アドレスの登録および検索、修正、削除を含む機能を使えるようにし、所定期間以上保管されたメッセージを外部格納装置に移管して保管する。
【００１３】
前記電子アドレスは、前記送受信個体１０１が前記電子文書流通ハブ１０２のアドレスディレクトリサーバを介して発給を受けたユーザ識別記号と；前記送受信個体１０１が必要な場合に自体的に付与する固有な値であり、該当送受信個体１０１内において固有な値である追加識別記号；および前記ユーザ識別記号と追加識別記号との間に位置する区分記号；を含む。
【００１４】
前記電子文書流通ハブ１０２は、電子文書の書式登録機を備え、前記電子文書の書式登録機は、電子文書の標準書式の登録、削除、および情報修正を含む管理を遂行し、電子文書の標準書式を文脈（ｃｏｎｔｅｘｔ）に応じてさらに分類し、電子文書の標準書式が使用され得る文脈（ｃｏｎｔｅｘｔ）に対する登録、修正を含む管理を遂行する。
【００１５】
前記電子文書流通ハブ１０２は、送受信個体１０１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中継サーバを備え、前記流通中継サーバは、送受信個体１０１からメッセージ転送の依頼を受ければ、メッセージ転送を代行した後に、メッセージ転送を依頼した送受信個体１０１に送信証明書を発給し、依頼を受けたメッセージ転送を失敗した時には、メッセージ転送を依頼した送受信個体１０１にエラーメッセージを転送する。
【００１６】
前記電子文書流通ハブ１０２は、外部システムとの連係のための外部連係ゲートウェイサーバを備え、前記外部連係ゲートウェイサーバは、電子アドレスを基盤にメッセージを送受信する流通メッセージングサーバを備え、連係した外部システムと電子文書流通システム間の送受信電子アドレスの検証／変換機能と、連係した外部システムと電子文書流通システム間のメッセージの検証／変換機能、連係した外部システムと電子文書流通システム間の電子文書に適用された保安の検証／変換機能、連係した外部システムと電子文書流通システム間の電子文書の適合性を検証し相互間に変換する機能を提供する。
【００１７】
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システムおよびこれを利用した電子文書流通方法について図１～図１１８を参照して詳細に説明すれば、次の通りである。以下、本発明について詳細に説明する際に図１の図面符号は省略する。
【００１８】

［電子文書流通システムの構造］
電子文書流通の信頼性および安全性を保障するために、本発明による電子文書流通システムの流通体系が備えなければならない要件は次の１）～７）の通りである。
１）流通体系に参加する送受信個体および送受信者は事前に定義された方式で電子文書を送受信するべきであり、管理機関または電子文書中継者のサービスレベル協約（ＳＬＡ）に同意するべきである。
【００１９】
２）流通体系内に参加する送受信個体および公認送受信者は身元確認が可能であるべきであり、電子文書の流通行為はその事実に対する否認防止が可能であるべきである。
【００２０】
３）流通体系において送受信個体および公認送受信者を識別するための情報である公認電子アドレスは法人または個人単位で付与され、登録機関によって登録および管理されるべきである。
【００２１】
４）流通体系内での電子文書の流通時、流通証明書は必ず生成されるべきであり、流通行為に参加した送信個体および第３者保管機関に転送および保管されるべきである。
【００２２】
５）全ての電子文書の流通行為はＰ２Ｐ（Ｐｅｅｒ　ｔｏ　Ｐｅｅｒ）通信を基本とするが、様々な環境的な要因のために通信に失敗した場合、これを支援するための体系があるべきである。
６）流通体系内において当事者間の電子文書の交換だけでなく、電子文書閲覧サービスなどの様々な付加サービスも支援されるべきである。
７）流通体系以外の外部システムとの連係を支援するゲートウェイが提供されるべきである。
【００２３】
本発明による電子文書流通システムは公認電子アドレスを基盤にし、流通メッセージングサーバを所有している送受信個体間に電子文書をやり取りするＰ２Ｐ通信を基本とする。
【００２４】
このような本発明による電子文書流通システムの構造は図１の通りであり、システム内の構成要素に対する説明は下記表１および表２の通りであり、主要プロセスは下記表３の通りである。
【００２５】

【表１】

【表1】

番号	個体名	説明
1	送受信個体	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞなどの電子文書流通に必要なｼｽﾃﾑなどを備え、流通体系において事前に約束された方式で電子文書流通に参加する企業または機関。電子文書中継者を含む一般的な概念
2	電子文書中継者	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞなどの電子文書流通に必要なｼｽﾃﾑを備えていない送受信者に電子文書流通ｻｰﾋﾞｽを提供するために認証を受けた第3者機関
3	電子文書流通ﾊﾌﾞ	送受信個体間の電子文書流通を支援するｼｽﾃﾑを通称するものであり、ｱﾄﾞﾚｽ管理、経路設定、ｴﾗｰおよび保安の処理、外部との連係などの作業を遂行
4	送受信者	電子文書を流通する基本単位として実際の電子文書を送信受信する最終ﾕｰｻﾞ。公認送受信者を含む一般的な概念
5	公認送受信者	電子文書中継者に加入し、公認電子ｱﾄﾞﾚｽの発給を受けて電子文書流通ｻｰﾋﾞｽを利用する送受信者
6	第3者保管機関	知識経済部長官の指定を受け、他人のために電子文書を保管または証明したり、その他の電子文書と関連した業務を遂行したりする法人

【００２６】

【表２】

【表2】

番号	個体名	説明
1	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ	送受信者を代行し、事前に約束された方式で電子文書を流通するﾒｯｾｰｼﾞﾝｸﾞｼｽﾃﾑであり、送受信個体または電子文書中継者に設置されるｼｽﾃﾑ
2	流通ｸﾗｲｱﾝﾄ	送受信者が電子文書を流通するために使うｱﾌﾟﾘｹｰｼｮﾝを通称する言葉であり、ﾒｯｾｰｼﾞの編集と流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞを介してﾒｯｾｰｼﾞ送受信などの機能を提供するｱﾌﾟﾘｹｰｼｮﾝ(例:ｱｳﾄﾙｯｸ、ｳｪﾌﾞﾒｰﾙｸﾗｲｱﾝﾄなど)
3	ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞ	公認電子ｱﾄﾞﾚｽ基盤の電子文書流通体系に参加する送受信個体および送受信者の公認電子ｱﾄﾞﾚｽを登録、管理し、送受信のために必要なｱﾄﾞﾚｽ情報を提供するｼｽﾃﾑ
4	電子文書の書式登録機	注文書、送り状、税金計算書などの構造化できる電子文書の標準書式を送受信個体が公開的に利用できるように登録、管理、提供するｼｽﾃﾑ
5	流通中継ｻｰﾊﾞ	流通体系において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、送信個体の代わりにﾒｯｾｰｼﾞ転送を代行するｼｽﾃﾑ
6	外部連係ｹﾞｰﾄｳｪｲｻｰﾊﾞ	流通体系が外部ｼｽﾃﾑなどと連係するための信頼性のある通路役割をするｼｽﾃﾑ
7	NTP ｻｰﾊﾞ	Network Time Protocol ｻｰﾊﾞであり、流通体系内の時間を要請するｼｽﾃﾑに時間を送る役割をするｻｰﾊﾞ
8	登録代行ｼｽﾃﾑ	登録代行機関が公認電子ｱﾄﾞﾚｽの申請受付および登録などの業務を処理するためのｼｽﾃﾑ

【００２７】

【表３】

【表3】

番号	ﾌﾟﾛｾｽ名	説明
1	ﾒｯｾｰｼﾞ送受信	送受信個体間に(電子文書を含む)ﾒｯｾｰｼﾞをやりとりする行為であり、送受信個体内にある流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞを介してﾒｯｾｰｼﾞを送信および受信し、流通証跡情報を含んだ流通証明書をやり取りする行為
2	物理ｱﾄﾞﾚｽの獲得	電子文書を転送するに先立ち、受信者の公認電子ｱﾄﾞﾚｽに該当する物理ｱﾄﾞﾚｽを知るために電子文書流通ﾊﾌﾞ内にあるｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに問い合わせて物理ｱﾄﾞﾚｽを受信する行為
3	流通中継支援	ﾈｯﾄﾜｰｸおよび受信者ｼｽﾃﾑのｴﾗｰなどの様々なｴﾗｰのために送受信個体間の電子文書流通が円滑ではない時、流通中継ｻｰﾊﾞが電子文書の転送を代行するﾌﾟﾛｾｽ
4	流通証明書の保管など	送信個体が受信した流通証明書を事前に協約した第 3 者保管機関に保管する行為(必要によってはﾒｯｾｰｼﾞも保管)
5	公認電子ｱﾄﾞﾚｽ登録などの管理	送受信個体または公認送受信者の公認電子ｱﾄﾞﾚｽの登録、変更などをするためのﾌﾟﾛｾｽ
6	電子文書の書式適用	流通ｸﾗｲｱﾝﾄにおいて電子文書の書式登録機に登録されている電子文書を活用するﾌﾟﾛｾｽ
7	ｽﾊﾟﾑﾒｯｾｰｼﾞの処理	特定の送受信者がｽﾊﾟﾑ発送などの流通体系内で不適切な行為をした時、これを申告および処理するﾌﾟﾛｾｽ
8	ｴﾗｰ処理	流通体系内で電子文書流通などの様々な失敗事例が発生した時、これに対する原因分析およびこれに対して対応、補完する行為

【００２８】

［電子文書流通システムの構成要素］

１）流通メッセージングサーバ

流通メッセージングサーバは、送受信個体内にあるメッセージングシステムであって、電子文書流通の核心的な役割を担当する。流通メッセージングサーバは物理的に１つの電子アドレス（ＩＰ　Ａｄｄｒｅｓｓ）を有するが、下位のユーザのために複数のユーザアカウントを発給し管理できなければならない。各ユーザアカウントを管理するために、流通メッセージングサーバはユーザアカウント別にメッセージ箱を管理するべきであり、流通メッセージングサーバはユーザのアカウントとメッセージ箱を安全で信頼性のあるように管理する責任がある。

流通メッセージングサーバの機能概念図は図２の通りであり、機能に対する説明は下記表４の通りである。

【００２９】

【表４】

【表4】

番号	機能名	説明
1	ﾒｯｾｰｼﾞの送信、受信	-流通ﾌﾟﾛﾄｺﾙに応じてﾒｯｾｰｼﾞを送信し受信
2	ﾕｰｻﾞ別のﾒｯｾｰｼﾞ箱の管理	-送受信したﾒｯｾｰｼﾞはﾕｰｻﾞｱｶｳﾝﾄまたは内部区分子に応じてﾒｯｾｰｼﾞ箱に保管 -ﾒｯｾｰｼﾞ箱に保管された送信文書は次の 6 ｽﾃｯﾌﾟの状態情報を管理 1)送信中:文書転送後、受信者から何の応答も受けていない状態 2)送信完了:受信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞから ' 受信証明書 ' を受けた状態 3)送信委託:送信失敗した後、流通中継ｻｰﾊﾞに送信を委託した状態 4)送信失敗:受信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞの内部でｴﾗｰが発生して SOAP Fault ﾒｯｾｰｼﾞをﾘﾀｰﾝするか、送受信する過程でﾈｯﾄﾜｰｸｴﾗｰが発生した場合 5)閲覧失敗:受信者がﾒｯｾｰｼﾞを閲覧する過程でｴﾗｰが発生した場合 6)閲覧完了:受信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞから ' 閲覧証明書 ' を受けた状態 -ﾒｯｾｰｼﾞ箱に保管された受信文書は次の 4 ｽﾃｯﾌﾟの状態情報を管理 1)検証ｴﾗｰ:受信したﾒｯｾｰｼﾞに対する基本構造の検証でｴﾗｰが発生 2)受信確認前:当該文書の受信者が受信文書目録を読む前 3)受信確認:当該文書の受信者が受信文書目録を読む 4)閲覧確認:当該文書の受信者が受信文書に対する詳細内容を読む -受信者によって削除要請が届くと、該当受信文書を物理的に削除処理するべきである -ﾒｯｾｰｼﾞ箱において、送信ﾒｯｾｰｼﾞ、受信証明書、閲覧証明書などは互いに連関するように連関情報を有するべきである
3	送受信履歴の管理	-流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、送受信履歴を編集および削除が不可能な媒体に一定期間保管できるべきである -保管するべき送受信履歴情報 1)送信履歴:ﾒｯｾｰｼﾞ id、連関ﾒｯｾｰｼﾞ id、送信者、受信者、送信時間、送信文書に対するﾊｯｼｭ値 2)受信履歴:送信者、受信者(ﾕｰｻﾞｱｶｳﾝﾄを含む)、受信時間、受信文書に対するﾊｯｼｭ値

【表４の継続】

4	ﾒｯｾｰｼﾞ補完	-流通ﾌﾟﾛﾄｺﾙから提示するﾒｯｾｰｼﾞ保安機能(電子署名、署名検証、暗号/復号化など)を遂行するべきである
5	ﾒｯｾｰｼﾞﾊﾟｯｹｰｼﾞﾝｸﾞおよび検証処理	-送信する文書は、転送前に流通ﾌﾟﾛﾄｺﾙで定義されたﾒｯｾｰｼﾞ構造にﾊﾟｯｹｰｼﾞﾝｸﾞされるべきである -受信した文書は受信後に流通ﾌﾟﾛﾄｺﾙで定義されたﾒｯｾｰｼﾞ構造によって検証、ﾊﾟｰｼﾝｸﾞし、必要な情報を抽出するべきである
6	流通証明書の発給および管理	-流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、文書の送受信事実に対する内容を証明できるように流通証明書を発給し、これを管理するべきである -発給された流通証明書を受信した後に直ちに第３者保管機関に保管、依頼 -流通証明書の履歴情報:流通証明書id、発給時刻、連関ﾒｯｾｰｼﾞid、流通証明書の原本(選択的)、第３者保管機関に保管後に受信した第３者保管機関の登録証明書など -＇電子文書の流通証明書＇技術規格を参照
7	ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞ連係	-ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞが提供するｱﾄﾞﾚｽ情報の登録および検索ﾌﾟﾛｾｽに応じてｱﾄﾞﾚｽ情報を管理できるべきである -ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞが提供するｻｰﾋﾞｽを呼び出しできるｸﾗｲｱﾝﾄ機能があるべきである -ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞが提供するｱﾄﾞﾚｽ情報の登録、検索、修正、削除の機能を遠隔から呼び出しするｻｰﾋﾞｽｸﾗｲｱﾝﾄ機能が提供されるべきである
8	第３者保管機関連係	-流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、流通証明書の保管要請のために第３者保管機関の外部に設置されている流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに保管要請ﾒｯｾｰｼﾞを転送 -第３者保管機関の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、第３者保管機関に流通証明書の保管のための保管要請ｸﾗｲｱﾝﾄを呼び出す -第３者保管機関の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞが直接流通証明書を生成した場合には、生成時点で保管要請ｸﾗｲｱﾝﾄを呼び出す -保管要請ｸﾗｲｱﾝﾄは、第３者保管機関の連係ｲﾝﾀｰﾌｪｰｽ規格に応じて第３者保管機関に保管を要請する
9	内部ｼｽﾃﾑ連係ｲﾝﾀｰﾌｪｰｽ	-流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞが流通ｸﾗｲｱﾝﾄではなく企業の内部ｼｽﾃﾑである場合、企業の内部ｼｽﾃﾑと直接連係できる機能を提供するべきである
10	流通ｸﾗｲｱﾝﾄの管理	-流通ｸﾗｲｱﾝﾄと関連したﾕｰｻﾞｱｶｳﾝﾄの管理、ﾕｰｻﾞ認証、環境情報などを管理

【表４の継続】

11	付加機能の管理	-ﾒｯｾｰｼﾞ流通と関連した履歴および統計情報など -ｼｽﾃﾑ管理:ｼｽﾃﾑﾓﾆﾀﾘﾝｸﾞなど -環境情報管理:流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ全体に対する環境情報の管理とﾕｰｻﾞ別に環境設定機能などを提供するべきである -文書様式(Form)の管理
12	ﾒｯｾｰｼﾞの保存管理	-1 年以上保管されたﾒｯｾｰｼﾞを自動で保存するために外部格納装置に移管するｼｽﾃﾑ機能

【００３０】
上記表４に開示された機能の以外に、流通メッセージングサーバの信頼性を向上させるためには、サーバシステム管理において、次の１）～４）のような原則を遵守するべきである。
１）システム管理者は、個人のメッセージ箱を見たり任意に削除したりすることはできない。
２）サーバシステム管理と関連した履歴情報は任意に削除することができず、不変更媒体などに１０年以上保管するべきである。
３）システム管理者は、認証された流通メッセージングサーバ・ソルーションの基本機能などを任意に変更することができない。
４）システム管理と関連した業務指針を作成し、それに応じて管理がなされるべきである。
【００３１】
２）流通クライアント
流通クライアントは、流通体系内に参加する送受信者のために、メッセージの送信および受信、受信された電子文書の閲覧および管理などのＵＩ（Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）を提供するアプリケーションである。流通クライアントは、独自に文書を送受信することができず、必ず流通メッセージングサーバと連係しなければならない。
【００３２】
流通クライアントは、流通メッセージングサーバを介してメッセージ転送を要請するか、流通メッセージングサーバを介して受信されたメッセージを照会する。流通メッセージングサーバは、ユーザアカウント別にメッセージ箱を管理し、流通クライアントは、受信文書中のユーザアカウント情報の確認を通じて本人のアカウントに保管されているメッセージにのみアクセスが可能であるべきである。
流通クライアントは、送受信個体の要求に応じて、Ｃ／Ｓ形態のアプリケーションまたはウェブ形態の画面に実現することができる。
流通クライアントの機能概念図は図３の通りであり、機能に対する説明は下記表５の通りである。
【００３３】

【表５】

【表5】

番号	機能名	説明
1	ﾕｰｻﾞ認証	-流通ｸﾗｲｱﾝﾄは、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞからﾕｰｻﾞｱｶｳﾝﾄを確認した後、ﾛｸﾞｲﾝｾｯｼｮﾝ情報を受けるべきである -流通ｸﾗｲｱﾝﾄがﾕｰｻﾞ認証を受けるための方法としては、1)認証書を基盤にしたﾕｰｻﾞ認証、または 2)ID/PW を基盤にしたﾕｰｻﾞ認証などがある -ID/PW 基盤に運用する時、PW に対する保安政策を強制できるべきである。1 週単位の PW 変更、難しい文字/数字の組み合わせ、IPｱﾄﾞﾚｽの変更禁止など
2	ﾒｯｾｰｼﾞ生成	-流通ｸﾗｲｱﾝﾄは、新規ﾒｯｾｰｼﾞを作成できるﾕｰｻﾞｲﾝﾀｰﾌｪｰｽを提供するべきである -ﾒｯｾｰｼﾞを転送するために必要な基本情報中、環境情報によって既に設定された値ではない項目は入力できるように提供 -ﾒｯｾｰｼﾞ本文は必須項目ではなく、選択的に本文を追加、作成することができる
	ﾒｯｾｰｼﾞ目録の照会および詳細内容の閲覧	-流通ｸﾗｲｱﾝﾄは、ﾕｰｻﾞｱｶｳﾝﾄに該当する各ﾒｯｾｰｼﾞの目録を照会する機能を提供するべきである -添付文書を含んでﾒｯｾｰｼﾞの詳細情報を閲覧できる機能を提供するべきである
4	ﾒｯｾｰｼﾞﾌｫﾙﾀﾞの管理	-流通ｸﾗｲｱﾝﾄは、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞのﾒｯｾｰｼﾞ箱を基盤に送信と受信ﾒｯｾｰｼﾞを流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞが提供する状態情報に応じてﾕｰｻﾞに各ﾒｯｾｰｼﾞの状態を知らせるべきである -ｱｳﾄﾎﾞｯｸｽ、削除したﾒｯｾｰｼﾞ箱を提供したり、ﾕｰｻﾞが直接ﾒｯｾｰｼﾞﾌｫﾙﾀﾞを定義し管理できるようにする機能を提供したりすることは選択事項
5	基本情報および環境情報の管理	-流通ｸﾗｲｱﾝﾄは、ﾒｯｾｰｼﾞ送受信と関連し、必要な環境情報を管理する機能を提供するべきである -流通ｸﾗｲｱﾝﾄは、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞにおいて管理している環境情報と同期化されるべきである。さらに、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞの個別環境情報を設定し管理する機能を提供 -流通ｸﾗｲｱﾝﾄのｼｽﾃﾑ環境に対する付加情報の管理はｱﾌﾟﾘｹｰｼｮﾝの開発範囲に応じて定義して提供

【表５の継続】

6	文書作成	-登録されている電子文書の書式を取り込んで電子文書を作成する機能
7	ﾒｯｾｰｼﾞの送信要請&受信ﾒｯｾｰｼﾞ Get	-流通ｸﾗｲｱﾝﾄは、ﾕｰｻﾞｱｶｳﾝﾄ情報に基づいて流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞとの連係ｲﾝﾀｰﾌｪｰｽを介してﾒｯｾｰｼﾞの送信機能と受信ﾒｯｾｰｼﾞの持ち込み機能を遂行するべきである
8	ﾒｯｾｰｼﾞの保安処理	-電子署名または暗号化/復号化などのﾒｯｾｰｼﾞに対する保安処理ができるべきである
9	文書書式の登録および検索	-電子文書の書式登録機または外部に位置する電子文書の書式を流通ｸﾗｲｱﾝﾄに登録できる機能 -流通ｸﾗｲｱﾝﾄ内にある電子文書の書式を検索できる機能
10	住所録管理	-よく使用する公認電子ｱﾄﾞﾚｽなどを管理する機能 -受信したﾒｯｾｰｼﾞを通じて自動で公認電子ｱﾄﾞﾚｽを登録、管理する機能を選択的に実現
11	企業内ｼｽﾃﾑと連係	-ﾒｯｾｰｼﾞ内の電子文書を企業内のｸﾞﾙｰﾌﾟｳｪｱ、業務関連ｼｽﾃﾑに登録させるなどの連係機能
12	ﾒｯｾｰｼﾞの保存管理	-政策的に設定しておいた保管年限が過ぎたﾒｯｾｰｼﾞの保存のために、外部格納装置などに移管する機能 -この場合、ﾒｯｾｰｼﾞと関連した文脈を把握できるように流通証明書、ﾛｸﾞ情報などの関連情報まで包括的に保存処理されるべきである
13	ｽﾊﾟﾑ申告	-ｽﾊﾟﾑなどの不適切な目的で受信されたﾒｯｾｰｼﾞを申告する機能
14	文書閲覧の支援	-選択的機能であって、送信個体のｼｽﾃﾑまたは第３者保管機関に電子文書を保管し、これを閲覧できる権限だけを転送する機能 -受信者は閲覧権限を有し、電子文書をﾀﾞｳﾝﾛｰﾄﾞすることはできず、単に閲覧のみが可能

【００３４】

３）アドレスディレクトリサーバ

アドレスディレクトリサーバは、送・受信個体と公認送・受信者に対するアドレス情報を管理し、物理アドレスを提供するためのシステムである。

アドレスディレクトリサーバは、次の１）および２）のような基本機能を提供する。

１）受信個体の流通メッセージングサーバの物理アドレス（ＩＰアドレス）の管理および提供

２）公認電子アドレスの情報を登録、修正するなどの管理機能

【００３５】

さらに、アドレスディレクトリサーバは、ホワイトリスト情報を管理する機能を基本的に有し、ユーザからスパムメッセージに対する申告を受け付け、これを基準にブラックリ

スト情報を管理する。

【００３６】

アドレスディレクトリサーバは、ウェブポータル画面を介して公認電子アドレスと関連した情報を送受信個体または公認送受信者に提供し、連係インターフェースを介して流通メッセージングサーバおよび関連アプリケーションがアドレスディレクトリサーバから提供するサービスを利用することができる。

アドレスディレクトリサーバの機能概念図は図４の通りであり、機能に対する説明は下記表６の通りである。

【００３７】

【表６】

【表6】

番号	機能名	説明
1	公認電子ｱﾄﾞﾚｽの管理	-送受信個体および公認送受信者の公認電子ｱﾄﾞﾚｽの新規登録および変更などの管理 -公認電子ｱﾄﾞﾚｽを所有した送受信個体の情報および履歴情報の閲覧など
2	ｽﾊﾟﾑ申告の管理	-流通ｸﾗｲｱﾝﾄから受信したｽﾊﾟﾑなどに対する申告受付および結果通知の機能など
3	ﾎﾜｲﾄ/ﾌﾞﾗｯｸﾘｽﾄの管理	-公認電子ｱﾄﾞﾚｽ目録であるﾎﾜｲﾄﾘｽﾄの生成および管理/保管 -ﾎﾜｲﾄﾘｽﾄに対する検索要請の受付および処理機能 -ｽﾊﾟﾑなどの不適切な目的で使った公認電子ｱﾄﾞﾚｽに対するﾌﾞﾗｯｸﾘｽﾄの生成および修正などの管理 -ﾌﾞﾗｯｸﾘｽﾄに対する検索機能
4	ｱﾄﾞﾚｽ情報の検索および物理ｱﾄﾞﾚｽのやり取り	-流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞから要請を受けた公認電子ｱﾄﾞﾚｽの物理ｱﾄﾞﾚｽ要請の受付およびこれをﾘﾀｰﾝする機能 -これと関連した履歴情報の検索機能
5	ｳｪﾌﾞﾎﾟｰﾀﾙの管理	-ｱﾄﾞﾚｽ管理と関連したﾕｰｻﾞｲﾝﾀｰﾌｪｰｽの提供 -ｱﾄﾞﾚｽ管理と関連したｼｽﾃﾑ管理者ｲﾝﾀｰﾌｪｰｽの提供 -ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞのｼｽﾃﾑ環境情報の管理 -ｱﾄﾞﾚｽ関連の各種統計情報の管理

４）電子文書の書式登録機

【００３８】

電子文書の書式登録機は、送受信個体間に事前に約束された標準電子文書を利用して自動で処理するか、ｅ－Ｆｏｒｍ形態の電子文書などを活用できるように、電子文書流通ハブから提供するシステムである。

【００３９】

電子文書の書式登録機は、電子文書の書式を管理するサーバエンジンと流通クライアントがこれを検索およびダウンロードできるように機能を提供するインターフェースとウェ

ブポータルインターフェースなどを提供する。

電子文書の書式登録機の機能概念図は図５の通りであり、機能に対する説明は下記表７の通りである。

【００４０】

【表７】

【表 7】

番号	機能名	説明
1	電子文書の書式管理	-電子文書の書式の登録、削除、情報修正などの管理 -電子文書の登録/削除などと関連した内訳通知
2	電子文書の検索および受信管理	-電子文書の書式の検索機能を提供 -検索された電子文書の書式のﾀﾞｳﾝﾛｰﾄﾞなどの受信
3	電子文書の書式連係ｲﾝﾀｰﾌｪｰｽ	-流通ｸﾗｲｱﾝﾄと直接連係した状態で電子文書を検索、ﾀﾞｳﾝﾛｰﾄﾞする機能などを提供
4	文脈(ｺﾝﾃｷｽﾄ)管理	-該当電子文書の書式名が同一であるとしても国家や産業などの文脈(ｺﾝﾃｷｽﾄ)に応じて他の書式が使われ得るので、電子文書の書式を文脈に応じて追加分類 -国家、地域、産業、企業、ﾌﾟﾛｾｽなど、電子文書の書式が使われ得る文脈(ｺﾝﾃｷｽﾄ)に対する登録、修正などの管理
5	電子文書の書式審査&評価機能	-ﾕｰｻﾞが電子文書の書式を登録するために提出して待機 -評価者によって評価された後、正式登録されるか返還するﾌﾟﾛｾｽ ※電子文書の書式、提出方法などについては追加公知
6	ｳｪﾌﾞﾎﾟｰﾀﾙの管理	-電子文書の管理と関連したﾕｰｻﾞｲﾝﾀｰﾌｪｰｽの提供 -電子文書の管理と関連したｼｽﾃﾑ管理者ｲﾝﾀｰﾌｪｰｽの提供 -電子文書の書式登録機ｻｰﾊﾞのｼｽﾃﾑ環境情報の管理 -電子文書の書式登録機の各種統計情報の管理

【００４１】

５）流通中継サーバ

流通中継サーバは、電子文書流通ハブ内にあるシステムであり、流通体系において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、送信個体の代わりにメッセージ転送を代行するシステムである。

【００４２】

流通中継サーバは内部的に流通メッセージングサーバの機能を内蔵しているので、これによって基本的な電子文書の送受信サービスを提供するだけでなく、流通中継サーバのみが有する中継依頼の受付および最終失敗時のエラーメッセージの転送などのサービスを連係インターフェースを介して流通メッセージングサーバに提供する。

流通中継サーバの機能概念図は図６の通りであり、機能に対する説明は下記表８の通りである。

【００４３】

【表８】

【表8】

番号	機能名	説明
1	ﾒｯｾｰｼﾞ Routing 情報処理	送受信個体にある流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに対する経路の設定機能
2	転送ｴﾗｰ時の再処理作業	ﾒｯｾｰｼﾞを受信個体に転送する際にｴﾗｰが発生した時に再転送などの処理をする機能
3	送信証明書の発給	ﾒｯｾｰｼﾞ転送を依頼した送信個体に送信証明書を発給する機能
4	転送失敗時のｴﾗｰﾒｯｾｰｼﾞ転送	依頼を受けたﾒｯｾｰｼﾞ転送が失敗した時に送信個体にｴﾗｰﾒｯｾｰｼﾞを転送する機能
5	電子文書の中継依頼	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞと連係した状態でﾒｯｾｰｼﾞ中継の依頼を受ける機能
6	履歴/統計情報の管理	ﾒｯｾｰｼﾞ流通中継と関連した履歴や統計情報を保管および処理する機能
7	中継現況のﾓﾆﾀﾘﾝｸﾞ	送受信個体に対する流通中継現況の提供およびｼｽﾃﾑ管理者による中継現況のﾓﾆﾀﾘﾝｸﾞ機能

【００４４】

６）外部連係ゲートウェイサーバ

外部連係ゲートウェイサーバは、既存に運用されているか、流通体系内に含まれ難い外部システムと流通体系が連係するための信頼性のある通路役割をするシステムである。

【００４５】

公共部門の場合、行政情報共同利用センターまたは電子文書流通支援センターなどを通じて苦情や民生に係る書類などを電子的に流通しているが、このようなシステムと連係するためのチャネルとして外部連係ゲートウェイサーバを活用することができる。公共部門だけでなく、その他の外部システムとも連係するためのチャネル役割を遂行することができる。

外部連係ゲートウェイサーバの機能概念図は図７の通りであり、機能に対する説明は下記表９の通りである。

【００４６】

【表９】

【表9】

番号	機能名	説明
1	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞﾓｼﾞｭｰﾙ	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞにある機能中の一部使用
2	検証/変換ﾓｼﾞｭｰﾙ	連係する外部ｼｽﾃﾑ別に対応する、検証/変換するﾓｼﾞｭｰﾙ
3	電子ｱﾄﾞﾚｽの検証/変換	流通体系と外部連係ｼｽﾃﾑ間の送受信ｱﾄﾞﾚｽの検証および変換機能
4	ﾒｯｾｰｼﾞﾊﾟｯｹｰｼﾞの検証/変換	流通体系と外部連係ｼｽﾃﾑ間のﾒｯｾｰｼﾞﾊﾟｯｹｰｼﾞの検証および変換機能
5	電子文書保安の検証/変換	流通体系と外部連係ｼｽﾃﾑ間の電子文書に適用された保安の検証および変換機能
6	文書適合性の検証/変換	流通体系と外部連係ｼｽﾃﾑ間の電子文書の適合性を検証し、相互間に変換する機能
7	ｼｽﾃﾑ管理	外部連係ｹﾞｰﾄｳｪｲｻｰﾊﾞのｼｽﾃﾑ管理
8	統計情報の照会	外部連係ｹﾞｰﾄｳｪｲの利用と関連した統計情報の照会機能

【００４７】

７）公認電子アドレス

流通体系に参加する送受信個体と公認送受信者は固有の公認電子アドレスの発給を受けるべきである。

公認電子アドレスは、ｓｈａｒｐ［＃］、数字［０－９］、ハイフン［－］、ピリオド［。］の組み合わせで構成する。

公認電子アドレスの構成体系は下記表１０の通りである。

【００４８】

【表１０】

【表10】

区分	公認電子ｱﾄﾞﾚｽ		内容
	区分子	ﾕｰｻﾞ識別記号	
個人用途	#	000-0000-0000	数字およびﾊｲﾌﾝで構成された13桁の記号で組み合わせられた申請者の任意で付与した数字
その他の用途		000-00-00000	数字およびﾊｲﾌﾝで構成された12桁の記号で組み合わせられた事業者登録番号または固有登録番号

公認電子アドレスの構成体系と関連した原則は次の１）～３）の通りである。

【００４９】

１）"＃"の前部分はユーザの便宜のために、文字［Ａ－Ｚ］［ａ－ｚ］、ハングル［完

成されたハングル文字２，３５０字］、数字［０－９］、ハイフン［－］、ピリオド［。］の組み合わせで構成されたユーザ追加識別記号を選択的に使うことができる。この場合、ユーザ追加識別記号は、電子文書流通メッセージングサーバにおいて自体管理する。

２）公認電子アドレスのユーザ追加識別記号は、ハイフンまたはピリオドで始まったり終わったりしてはいけず、長さは３０バイト以下にする。

【００５０】

３）公認電子アドレスのユーザ追加識別記号としては、社会的慣習、美風良俗を害する文字および数字の組み合わせ、その他の管理機関長が定める制限記号は使えない。

【００５１】

公認電子アドレスと実の物理アドレス（流通メッセージングサーバの実の物理アドレス）であるＩＰ　Ａｄｄｒｅｓｓとは、連関関係に対してはアドレスディレクトリサーバを通してのみ管理される。公認電子アドレスと流通メッセージングサーバの実の物理アドレスは１：１またはＮ：１の関係を有し、これにより、１つの公認電子アドレスがいくつかの物理アドレスを有する場合は存在しない。

【００５２】

公認電子アドレスに対する情報（文書）の法的な受信責任は"＃"の後に存在する企業／機関／個人が持つべきであり、ユーザ追加識別記号による配付は企業／機関／個人が便宜のために区分したものであるため、送受信個体はユーザ追加識別記号による配布に対して自体的に責任を負わなければならない。この場合、送受信個体は、ユーザ追加識別記号に該当するユーザ認証に対する政策および管理要領を準備するべきであり、要領に応じて徹底的に管理するべきである。さらに、送受信個体は、流通体系に参加するに先立ち、管理機関とサービスレベル協約（ＳＬＡ）を締結し、内部区分子を含む公認電子アドレス内容を含ませて締結しなければならない。

流通体系内で公認電子アドレスが有する効力範囲は図８のように表現することができる。

【００５３】

ユーザ追加識別記号は、送受信個体内で固有な値でなければならない。ユーザ追加識別記号に対する付与方式は個別の送受信個体が責任を負うことを基本とし、ユーザ追加識別記号による電子文書の配付も送受信個体が責任を負うべきであり、問題発生時には送受信個体が解決しなければならない。このようなユーザ追加識別記号は流通体系の効力範囲には含まれないが、管理機関とのサービスレベル協約（ＳＬＡ）などによって規定を受けられる。

【００５４】

ユーザ追加識別記号は、企業の業務便宜のために電子文書を分配するための用途として使われ、アドレスディレクトリサーバに登録せずに企業内部の情報としてのみ使用する。

上述したような公認電子アドレスの他例として、次のような構造が可能である。

公認電子アドレス＝ＩＤ＋区分記号＋登録者

【００５５】

ここで、前記"ＩＤ"は英文（またはハングル、数字）、ハイフン［－］、およびピリオド［。］などが組み合わせられて構成され、前記"区分記号"は＃であり、前記"登録者"は英文（またはハングル、数字）とピリオド［。］が組み合わせられて構成される。

【００５６】

このような公認電子アドレスの一例として"ｓｗｃｏｎｖｅｒｇｅｎｃｅ＃ｍｋｅ．ｇｏ．ｋｒ"があり、このような例を構成するにおいて、"ｓｗｃｏｎｖｅｒｇｅｎｃｅ"は政府機関の部署名、"ｍｋｅ"は政府機関、"ｇｏ"は特性、"ｋｒ"は国家を示すようにした。

公認電子アドレスの申請／発給と運営体系は図９の通りであり、これと関連した構成要素に対する説明は下記表１１の通りである。

【００５７】

【表１１】

【表 11】

構成要素	役割
管理機関(公認電子ｱﾄﾞﾚｽの管理総括)	-管理機関は公認電子ｱﾄﾞﾚｽの最上位管理主体として、狭義の公認電子ｱﾄﾞﾚｽ情報を管理 -送受信個体および公認送受信者に対する固有の公認電子ｱﾄﾞﾚｽ ID の発給および変更管理
登録代行機関	-管理機関の委任を受けて公認電子ｱﾄﾞﾚｽの申請および審査をする機関
送受信個体	-狭義の公認電子ｱﾄﾞﾚｽ(登録ｱﾄﾞﾚｽ)の最も基本となる単位 -企業/機関の場合、1 つの公認電子ｱﾄﾞﾚｽの下位に複数ﾕｰｻﾞのためのﾕｰｻﾞｱｶｳﾝﾄまたはﾕｰｻﾞ追加識別記号を発給、管理、および唯一性の保障
(公認または内部)送受信者	-電子文書流通に参加する実ﾕｰｻﾞ -公認送受信者は、電子文書中継者を介して開設したﾕｰｻﾞｱｶｳﾝﾄを有した公認電子ｱﾄﾞﾚｽを有し、法的責任を持った送受信単位である -内部送受信者は、送受信に対する法的責任を持った送受信個体内においてﾕｰｻﾞ追加識別記号を通じて管理される送受信単位として、法的責任を負わず、電子ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに登録されない

【００５８】

８）電子文書情報パッケージ

電子文書情報パッケージは、メッセージ内部に含まれている電子文書に対するメタデータを明示することにより、グループウェアなどのような企業の内部システムで該当電子文書を自動で登録したり処理したりすることを支援するために必要である。

【００５９】

電子文書情報パッケージは、メッセージ流通における必須要素ではないため、業務上、必要なところだけに選択的に使われることができる。但し、使用時には次の１）２）および２）のような要件を遵守するべきである。

１）電子文書情報パッケージは、メッセージに含まれる電子文書とは別個のファイル形態で転送されるべきである。

２）電子文書情報パッケージは、ＸＭＬファイル形態で提供されるべきである。

電子文書情報パッケージのメタデータは下記表１２の通りである。

【００６０】

【表１２】

【表 12】

番号	ﾒﾀ情報	必須/選択	説明
1	電子文書名	必須	ﾒｯｾｰｼﾞ内に含まれている電子文書に対するﾌｧｲﾙ名
2	電子文書識別子	必須	電子文書を識別できる固有識別子
3	電子文書類型の区分	必須	該当電子文書が電子文書の書式登録機に登録されている電子文書であるのか、企業/機関内で使われる電子文書であるのか、自体的な電子文書であるのかを区分する識別子 0:電子文書の書式登録機にある電子文書 1:企業/機関内で共通に使われる電子文書 2:自体的に使われる電子文書
4	電子文書類型識別子	選択	電子文書の類型区分が 0 または 1 である場合に、類型を識別できる識別子
5	電子文書の署名値	選択	電子文書に対する電子署名値
6	その他情報	選択	電子文書と関連したその他情報

【００６１】

［メッセージ保安］

流通体系で最も重要な部分中の１つが転送メッセージに対する保安である。流通されるメッセージに対する保安としては、１）送受信事実に対する否認防止、２）転送メッセージに対する無欠性の保障、３）転送相手方に対する認証、および４）転送メッセージに対する機密性の保障が要求されるが、この中、１）、２）、３）は転送メッセージに対する転送者の電子署名で支援することができ、４）は転送メッセージに対する暗号化を通じて提供されるべきである。

【００６２】

流通体系の最も基本となる流通メッセージングサーバ間の電子文書流通において適用される保安は、図１０のようにメッセージの電子署名と暗号化を支援している。各区間には転送保安のためにネットワーク暗号化が適用されるべきである。

【００６３】

コンテンツに対する電子署名はアプリケーション別の固有領域であり、本発明を説明するにおいては言及しない。そして、本発明では、受信者の公開キーで暗号化をするのが基本であるが、受信者の認証書がない場合または受信者が内部送受信者である場合には、受信個体の暗号化だけを選択可能である。また、メッセージ転送過程において、メッセージに対する認証情報を含ませて流通メッセージングサーバに転送し、この時、認証情報は、流通メッセージングサーバがクライアントを認証するための用途として主に使われる。また、流通メッセージングサーバが流通クライアントを認証するために認証書基盤の電子署名の他に、ＩＤ／ＰＷ基盤、ＳＳＯ（Ｓｉｎｇｌｅ　Ｓｉｇｎ　Ｏｎ）によるトークン情報基盤などの様々な認証方式を採択することができる。

以下、電子署名方法について詳細に説明すれば、次の通りである。

【００６４】

流通メッセージングサーバは、他のシステム（他の流通メッセージングサーバ、アドレスディレクトリサーバ、流通中継サーバ）との連係時、必ず自身の公認認証書を基盤に電子署名がなされるべきである。流通体系内の構成要素間の連係のための全ての流通メッセージは基本的に電子署名がなされるべきであるが、流通クライアントと流通メッセージングサーバ間の電子署名は選択事項であり、認証書基盤のユーザ認証方式である場合にのみ電子署名を適用する。但し、この場合、流通メッセージングサーバは、流通クライアントとの流通メッセージに対するユーザ認証、無欠性、送受信事実の否認防止に対する全ての責任を負わなければならない。

以下、暗号化方案について詳細に説明すれば、次の通りである。

【００６５】

流通体系で添付される文書は、保安のために転送者が暗号化を選択した後、転送が可能である。この部分は文書に対する機密性のための部分であり、ネットワーク暗号化とは区別され、ネットワーク暗号化が適用された場合にも流通文書をさらに暗号化することができる。

【００６６】

暗号化する区間は、図１０のように、１）送信者の流通クライアントから受信者の流通メッセージングサーバ、または２）送信者の流通クライアントから受信者の流通クライアントまでとなる。受信者が公認送・受信者であり、公認認証書をアドレスディレクトリサーバに共に登録しておいた場合には、"２）送信者から受信者までの区間"において暗号化を遂行し、そうではない場合には、"１）送信者から受信個体までの区間"において暗号化が遂行される。

【００６７】

添付する文書を暗号化する時、送信者は、"１）送信者から受信個体までの区間"において暗号化が維持される場合には、送信者の流通メッセージングサーバ、受信者の流通メッセージングサーバ、受信者の流通クライアントなどの３ステップにおいて全て復号化が可能となるように暗号化をするべきである。"２）送信者から受信個体までの区間"において暗号化が維持されるべきである場合には、送信者は、送信者の流通メッセージングサーバと受信者の流通メッセージングサーバが復号化が可能となるように暗号化をするべきである。

【００６８】

送信個体と受信個体の流通メッセージングサーバは、添付された電子文書が暗号化された場合には、暗号化された状態で履歴管理のために保管し、送受信者が復号化された文書を基準に流通証明書を検証しようとする時に復号化をして検証できなければならない。このために流通メッセージングサーバは、廃棄された認証書の個人キーおよび個人キーへのアクセスのためのパスワードを続けて管理しなければならない。

以下、暗号化方案において、暗号化の概要を説明すれば、次の通りである。

【００６９】

流通体系で流通されるメッセージが送信者によって機密性を保障するべきであると判断された場合には、必ず次のような暗号化過程を遵守しなければならない。

【００７０】

暗号文は、国内外で各種標準として使われるＩＥＴＦ　ＲＦＣ３８５２　"ＣＭＳ（Ｃｒｙｐｔｏｇｒａｐｈｉｃ　Ｍｅｓｓａｇｅ　Ｓｙｎｔａｘ）"から提示するＣｏｎｔｅｎｔＩｎｆｏ構造体で表現されたＥｎｖｅｌｏｐｅｄ－Ｄａｔａ　Ｃｏｎｔｅｎｔ　Ｔｙｐｅを使う。

※ＲＦＣ３８５２　ＣＭＳ

【００７１】

１）ＩＥＴＦは、ＴＣＰ／ＩＰのようなインターネット運営プロトコルの標準を定義する主体である。ＩＥＴＦはＩＡＢ（Ｉｎｔｅｒｎｅｔ　Ａｒｃｈｉｔｅｃｔｕｒｅ　Ｂｏ

ａｒｄ、インターネットの技術的進化に対するＩｎｔｅｒｎｅｔ　Ｓｏｃｉｅｔｙの監督機構）の監督を受け、ＩＥＴＦ構成員はＩｎｔｅｒｎｅｔ　Ｓｏｃｉｅｔｙの個人または組織の構成員から選抜される。ＩＥＴＦにおいて製作された標準はＲＦＣの形態で表され、国内外の多くのＰＫＩ基盤のソリューション（各種の認証システム、タイムスタンプ、第３者保管機関の規格など）はこのようなＲＦＣ標準文書を基盤に作られる。

【００７２】

２）ＣＭＳ（Ｃｒｙｐｔｏｇｒａｐｈｉｃ　Ｍｅｓｓａｇｅ　Ｓｙｎｔａｘ）は最初にＲＳＡ社が作成した"ＰＫＣＳ＃７　ｖ１．５"を根幹に作られ、これをＩＥＴＦにおいて規格化したＲＦＣ標準で作成したものがＲＦＣ２６３０である。最初のＰＫＣＳ＃７にはｋｅｙ　ｔｒａｎｓｆｅｒ（暗号化に用いられた対称キーを、ＲＳＡを利用して相手方に伝達）方式だけがあったが、ＲＦＣ２６３０のＣＭＳにおいてはｋｅｙ　ａｇｒｅｅｍｅｎｔ（ＤＨアルゴリズムを利用してキーを伝達する方式）などが追加された。

【００７３】

３）その後、アルゴリズム部分を別途に分離および様々なキー管理技法を適用したＲＦＣ３３６９が２００２年度に制定されたが、ＲＦＣ３３６９の内容中の問題となる部分が多く報告されており、これを最終修正したバージョンが本発明に適用したＲＦＣ３８５２である。

【００７４】

追加適用標準として、暗号文の生成時、Ｃｏｎｔｅｎｔ　Ｅｎｃｒｙｐｔｉｏｎ（実際に転送される電子税金計算書パッケージ）において使われるアルゴリズムおよびアルゴリズムに該当するパラメータなどは、ＩＥＴＦ　ＲＦＣ３３７０　"Ｃｒｙｐｔｏｇｒａｐｈｉｃ　Ｍｅｓｓａｇｅ　Ｓｙｎｔａｘ（ＣＭＳ）　Ａｌｇｏｒｉｔｈｍ"およびＩＥＴＦ　ＲＦＣ４０１０　"Ｕｓｅ　ｏｆ　ｔｈｅ　ＳＥＥＤ　Ｅｎｃｒｙｐｔｉｏｎ　Ａｌｇｏｒｉｔｈｍ　ｉｎ　Ｃｒｙｐｔｏｇｒａｐｈｉｃ　Ｍｅｓｓａｇｅ　Ｓｙｎｔａｘ（ＣＭＳ）"に従う。

以下、暗号化方案において、暗号化対象データについて説明すれば、次の通りである。

【００７５】

図１１を参照すれば、伝達されるメッセージの暗号化対象は次の１）および２）の通りである。

１）メッセージの２番目のＭＩＭＥに入る流通情報

２）メッセージ本文の内容中、本文の実内容が入る＜Ｔｅｘｔ＞領域と添付文書

メッセージ本文にあるＴｅｘｔおよび添付文書は各々独立に暗号化され、該当位置に収録される。

１番目の暗号化対象は受信者に伝達しようとする本文内容であり、ＸＭＬ本文中の＜Ｔｅｘｔ＞項目内の値を対象とする。

【００７６】

次は、対象データの構成方法である。データはＡＳＮ．１　Ｂａｓｉｃ　Ｅｎｃｏｄｉｎｇ　Ｒｕｌｅｓ（ＢＥＲ）を従い、Ｄｉｓｔｉｎｇｕｉｓｈｅｄ　Ｅｎｃｏｄｉｎｇ　Ｒｕｌｅｓ（ＤＥＲ）を遵守するようにする。

【００７７】

【表１３】

【表 13】

MainText::= OCTET STRING

【００７８】

上記表１３のＭａｉｎＴｅｘｔはテキスト形態の本文内容である。

２番目以後の暗号化対象データは、３番目のＭＩＭＥから添付される添付文書であり、各添付文書の単位に独立に暗号化された後、該当ＭＩＭＥに入る。

【００７９】
次は、対象データの構成方法であり、データ構成は、１番目の暗号化方式と同様にＡＳＮ．１　Ｂａｓｉｃ　Ｅｎｃｏｄｉｎｇ　Ｒｕｌｅｓ（ＢＥＲ）を従い、Ｄｉｓｔｉｎｇｕｉｓｈｅｄ　Ｅｎｃｏｄｉｎｇ　Ｒｕｌｅｓ（ＤＥＲ）を遵守しなければならない。
【００８０】
【表１４】

【表 14】

AttachedDoc::= URL

【００８１】
上記表１４のＡｔｔａｃｈｅｄＤｏｃはｂｉｎａｒｙ形態の添付される文書である。
以下、暗号化方案において、暗号化処理手続きおよび構造を説明すれば、次の通りである。
下記表１５は、ＲＦＣ３８５２のＥｎｖｅｌｏｐｅｄＤａｔａの構成である。
【００８２】
【表１５】

【表 15】

EnvelopedData::= SEQUENCE {
version CMSversion,
originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
recipientInfos RecipientInfos,
encryptedContentInfo EncryptedContentInfo,
unprotectedAttrs [1] IMPLICIT UnprotectedAttributes OPTIONAL }

【００８３】
表１５において、ｖｅｒｓｉｏｎはＲＦＣ３８５２のｓｙｎｔａｘ　ｖｅｒｓｉｏｎ　ｎｕｍｂｅｒ構成に従う。
ｉｇｉｎａｔｏｒＩｎｆｏはｋｅｙ　ｍａｎａｇｅｍｅｎｔアルゴリズムを利用せず、ＣＲＬを転送する必要がないので使わない（ＲＦＣ３８５２に定義されている）。
【００８４】
現在利用できる暗号用認証書のアルゴリズムがＲＳＡであるため、ＲｅｃｉｐｉｅｎｔＩｎｆｏｓのＫｅｙＴｒａｎｓＲｅｃｉｐｉｅｎｔＩｎｆｏを通じて受信者が復号化できるキー（ｃｏｎｔｅｎｔ－ｅｎｃｒｙｐｔｉｏｎ　ｋｅｙ）を伝達する。
【００８５】
ｅｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔＩｎｆｏには、内部に定義されたＡｌｇｏｒｉｔｈｍ　Ｉｄｅｎｔｉｆｉｅｒのアルゴリズムを基盤に暗号化したＭａｉｎＴｅｘｔまたはＡｔｔａｃｈｅｄＤｏｃを入れる。
【００８６】
ｕｎｐｒｏｔｅｃｔｅｄＡｔｔｒｓは、このバージョンでは別途に利用しないため、送信者側においては管理の目的で値を入れることができるが、受信者側においてはこれを解いてみたり値を利用したりする必要はない。
次の１）および２）は、ＲＦＣ３８５２のＥｎｖｅｌｏｐｅｄＤａｔａの生成における主要部分に対する説明である。

１）ＥｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔＩｎｆｏの生成
【００８７】
【表１６】

【表 16】

```
EncryptedContentInfo::= SEQUENCE {
contentType ContentType,
contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier,
encryptedContent [0] IMPLICIT EncryptedContent OPTIONAL }
```

【００８８】
－ＣｏｎｔｅｎｔＴｙｐｅは、ｉｄ－ｄａｔａ（暗号化されたデータがどのような情報であるかを知らせる区分子－ＯＩＤ－情報である）を入れる。
－ｃｏｎｔｅｎｔＥｎｃｒｙｐｔｉｏｎＡｌｇｏｒｉｔｈｍは、実際の暗号化に使われた対称キーアルゴリズム情報を入れる。
【００８９】
－ｅｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔの入力は、上記で定義されたＴａｘＩｎｖｏｉｃｅＰａｃｋａｇｅのＤＥＲエンコードされた値をｃｏｎｔｅｎｔＥｎｃｒｙｐｔｉｏｎＡｌｇｏｒｉｔｈｍに定義されたアルゴリズム方式で暗号化したＯＣＴＥＴ　ＳＴＲＩＮＧ（Ｂｉｎａｒｙ値）である。
２）ＲｅｃｅｐｉｅｎｔＩｎｆｏの生成
【００９０】
【表１７】

【表 17】

```
RecipientInfos::= SET SIZE (1..MAX) OF RecipientInfo
RecipientInfo::= CHOICE {
ktri KeyTransRecipientInfo,
kari [1] KeyAgreeRecipientInfo,
kekri [2] KEKRecipientInfo,
pwri [3] PasswordRecipientInfo,
ori [4] OtherRecipientInfo }
```

【００９１】
－復号化をする対象が、送信個体、受信個体は必須であり、受信者は公認認証書がある場合にのみ可能であるため、実際ＲｅｃｉｐｉｅｎｔＩｎｆｏｓは下位にＲｅｃｉｐｉｅｎｔＩｎｆｏを最小２つから最大３つまで持つようになる。
【００９２】
－暗号用認証書がＲＳＡを利用するため、ｋｔｒｉ（相手方ＲＳＡ公開キーなどを利用してデータを暗号化した対称キーを送る方式）のみを利用して構成するようにする。
以下、暗号化方案において、メッセージに対するＯＩＤ定義を説明する。
メッセージ構成のためのＯｂｊｅｃｔ　Ｉｄｅｎｔｉｆｉｅｒは次の１）および２）の通りである。

【００９３】
１）ＥｎｖｅｌｏｐｅｄＤａｔａ　Ｔｙｐｅ：ＲＦＣ３８５２　ＣＭＳにおいて実際データを伝達するフォーマットはＣｏｎｔｅｎｔＩｎｆｏという構造体であり、内部にあるデータがどのようなデータであるかを確認できるようにＣｏｎｔｅｎｔＴｙｐｅに入れる情報である。
【００９４】
【表１８】

【表 18】

- id-envelopedData - OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 3 }

【００９５】
２）ＥｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔＩｎｆｏのＣｏｎｔｅｎｔＴｙｐｅ：暗号化されたデータを入れる構造体であるＥｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔＩｎｆｏ構造体において、内部にあるデータがどのようなデータであるかを確認できるようにＣｏｎｔｅｎｔＴｙｐｅに入れる情報である。
【００９６】
【表１９】

【表 19】

- id-data - OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 1 }

【００９７】
以下、暗号化方案において、暗号化アルゴリズムを説明する。
暗号化に使われるアルゴリズムは、大きく、２つに区分される。
１）対象データを直接暗号化するのに使う対称キーアルゴリズム
２）対称キーを受信者のみが復号化できるように伝達する公開キーアルゴリズム
【００９８】
公開キーアルゴリズムは、使われる認証書がＧＰＫＩまたはＮＰＫＩ体系の暗号用認証書であるため、ＲＳＡ基盤のアルゴリズムを利用するようになり、対称キーアルゴリズムに対しては、必ず、下に属した対称キー暗号アルゴリズムの３種類（ＳＥＥＤ、ＡＲＩＡ、３ＤＥＳ）のうちの１つを選択して使用するべきである。
【００９９】
送信者側は、対称キー暗号アルゴリズムの３種類のうちの１つだけを支援しても関係ないが、受信者側は、３種類のアルゴリズムに対して全て支援可能でなければならない。
【０１００】
１）非対称キーアルゴリズム（ＲＳＡ）：ランダムに生成され、データを暗号化した対称キー情報を相手方に安全に暗号化して伝達するのに使われ、例題は下記表２０の通りである。
【０１０１】

【表２０】

【表 20】

RSA Encryption - rsaEncryption - OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }

【０１０２】

２）対称キーアルゴリズム（ＳＥＥＤ、ＡＲＩＡ、３ＤＥＳ）：ランダムに生成され、実際の伝達データを暗号化するのに使われ、例題は下記表２１の通りである。

【０１０３】

【表２１】

【表21】

Triple-DES CBC
- des-ede3-cbc
- OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) rsadsi(113549) encryptionAlgorithm(3) 7 }
- Algorithm のﾊﾟﾗﾒｰﾀは必ず存在するべきであり、parameters は必ず CBCParameter を有するべきである。
または
SEED CBC
- id-seedCBC
- OBJECT IDENTIFIER::= { iso(1) member-body(2) korea(410) kisa(200004) algorithm(1) seedCBC(4)
- Algorithm のﾊﾟﾗﾒｰﾀは必ず存在するべきであり、parameters は必ず SeedCBCParameter を有するべきである。
または
ARIA CBC
- id-aria128-cbc OBJECT IDENTIFIER::=
{ iso(1) member-body(2) korea(410) gcma(100001) gpki-alg(1)
aria128-cbc(20) }
- id-aria192-cbc OBJECT IDENTIFIER::=
{ iso(1) member-body(2) korea(410) gcma(100001) gpki-alg(1)
aria192-cbc(21) }
- id-aria256-cbc OBJECT IDENTIFIER::=
{ iso(1) member-body(2) korea(410) gcma(100001) gpki-alg(1)
aria256-cbc(22) }
Algorithm のﾊﾟﾗﾒｰﾀは必ず存在するべきであり、parameters は必ず
ARIACBCParameter を有するべきである。
ARIACBCParameter::= ARIAIV -- Initialization Vector
ARIAIV::= OCTET STRING(SIZE(16))

【０１０４】

以下、暗号化方案において、暗号化用認証書の獲得と検証について説明する。

暗号文生成のためには、実際データを復号化しようとする受信者側の認証書を獲得してこそ可能である。認証書の獲得のために、送信者は、アドレスディレクトリサーバに連係して、受信者（または受信個体）に対する認証書を獲得しなければならない。この時、獲得した認証書が受信個体の認証書であるか、公認受信者の認証書であるかによって機密性が維持される区間が変わる。

【０１０５】

送信者は、転送メッセージに対して暗号化を選択した場合、獲得した受信者（または受信個体）の認証書に基づいて暗号化を遂行した後、受信者にメッセージを転送する。メッセージ転送過程でエラーが発生して、流通中継ハブにメッセージ転送を依頼する場合にも、暗号化された内容は変更せずにそのまま伝達する。

以下、暗号化方案において、ＥｎｖｅｌｏｐｅｄＤａｔａの構成について説明する。

図１２は実際に受信者に伝達される暗号化された本文を示し、実際値の連係関係についてより正確に把握できるはずである。

【０１０６】

－ＣｏｎｔｅｎｔＩｎｆｏ：ＲＦＣ３８５２に表現されたものであり、ＲＦＣ３８５２の構成データであるＳｉｇｎｅｄＤａｔａ、ＥｎｖｅｌｏｐｅｄＤａｔａ、ＥｎｃｒｙｐｔｅｄＤａｔａなどを入れる一種のコンテナーである。構造体のｃｏｎｔｅｎｔＴｙｐｅは、ｃｏｎｔｅｎｔがどのような情報であるかを示す。本指針では、ｉｄ－ｅｎｖｅｌｏｐｅｄＤａｔａという区分子（Ｏｂｊｅｃｔ　Ｉｄｅｎｔｉｆｉｅｒ）を入れるべきである。

－ＥｎｖｅｌｏｐｅｄＤａｔａ：暗号化情報を伝達するための構造体（前節の説明を参照）

【０１０７】

－ＥｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔＩｎｆｏ：暗号化された情報を保管する構造体である。構造体のｃｏｎｔｅｎｔＴｙｐｅは、ｅｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔがどのような情報であるかを示す。本指針では、ｉｄ－ｄａｔａという区分子（Ｏｂｊｅｃｔ　Ｉｄｅｎｔｉｆｉｅｒ）を入れるべきである。ｃｏｎｔｅｎｔＥｎｃｒｙｐｔｉｏｎＡｌｇｏｒｉｔｈｍは、ＳＥＥＤ、ＡＲＩＡ、３ＤＥＳ中の１つに対する区分子（ＯＩＤ）を入れるべきであり、ｅｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔにランダムに生成された秘密キーを利用して該当アルゴリズムで暗号化したデータをＯＣＴＥＴ　ＳＴＲＩＮＧ（バイナリデータ）に入れる。

【０１０８】

－ＲｅｃｉｐｉｅｎｔＩｎｆｏ：どのような方法を利用して受信者が復号化するかを選択する構造体である。本指針では、ＫｅｙＴｒａｎｓＲｅｃｉｐｉｅｎｔＩｎｆｏを利用しなければならない。

【０１０９】

－ＫｅｙＴｒａｎｓＲｅｃｉｐｉｅｎｔＩｎｆｏ：受信者が復号化できるように上記で述べたｅｎｃｒｙｐｔｅｄＣｏｎｔｅｎｔを暗号化したランダムな秘密キーを、受信者の公開キーを利用して暗号化して伝達するのに利用する構造体である。暗号化した秘密キーはｅｎｃｒｙｐｔｅｄＫｅｙに入れ、誰の公開キーを利用したかに対する情報であるＲｅｃｉｐｉｅｎｔＩｄｅｎｔｉｆｉｅｒおよび秘密キーを暗号化するのに利用したアルゴリズム情報であるＫｅｙＥｎｃｒｙｐｔｉｏｎＡｌｇｏｒｉｔｈｍＩｄｅｎｔｉｆｉｅｒなどを含む。

以下、復号化方案について説明する。

【０１１０】

暗号化された電子文書を受信した受信者は、図１２を通じて説明する手続きに応じて暗号化された本文と添付文書を復号化する。受信者は、暗号化された本文と添付文書を各々復号化することにより、平文形態の本文と添付文書を得ることができる。

【０１１１】

－１ステップ：暗号文からＥｎｖｅｌｏｐｅｄＤａｔａ構造を抽出し、これを読み込む

。

－２ステップ：ＥｎｖｅｌｏｐｅｄＤａｔａ構造体から復号用情報構造体（ＲｅｃｉｐｉｅｎｔＩｎｆｏ）を抽出した後、抽出した復号用情報構造体から暗号化された対称キー情報（ＫｅｙＴｒａｎｓＲｅｃｉｐｉｅｎｔＩｎｆｏ）を得る。

【０１１２】

－３ステップ：受信者は、暗号化された対称キー情報から抽出したｅｎｃｒｙｐｔｅｄＫｅｙを受信者の個人キー（認証書の公開キーとマッピングされる）を通じて復号化することにより、本文および添付文書を暗号化する時に使った対称キーを得る。

－４ステップ：１ステップで抽出したＥｎｖｅｌｏｐｅｄＤａｔａ構造体から本文または添付文書の暗号化された構造体を得る。

－５ステップ：３ステップを通じて獲得した対称キーを利用して４ステップで抽出した暗号化された本文または添付文書を復号化する。

－６ステップ：最終的に復号化された本文と添付文書を獲得する。

【０１１３】

［ネットワーク保安］

送信者と受信者間に流通されるメッセージの機密性のために電子文書流通の全区間（メッセージング送信者の流通クライアントと流通メッセージングサーバ間、送信者と受信者の流通メッセージングサーバ間、受信者の流通メッセージングサーバと流通クライアント間）において、ネットワーク保安のためにＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）を適用する。

【０１１４】

［メッセージ送受信プロセス］

流通体系内の関係者間、システム間には様々な業務プロセスが存在する。流通体系内で最も基本的なメッセージ送受信プロセスがあり、これを支援するための色々なプロセスが存在する。

【０１１５】

メッセージ送受信プロセスは、送信者と受信者間にメッセージを直接やり取りする形態で郵便やｅ－メールのように相手方に文書が交換されるプロセスである。

【０１１６】

送信者と受信者間にメッセージを送受信するために、１）受信者に対する物理アドレスおよび保安情報の獲得、２）メッセージ転送および転送確認、３）業務受信者の受信確認、４）流通証明書の発給および保管の４ステップのプロセスからなる。この時、流通証明書に対するプロセスは、証明を受けようとする内容に応じて詳細プロセスの流れが変われるが、これに対する基本的な流れを図１４で提示しており、詳細な説明は下記表２２の通りである。

【０１１７】

【表２２】

【表 22】

番号	ﾌﾟﾛｾｽ名	説明
1	受信者に対する物理ｱﾄﾞﾚｽおよび保安情報の獲得	◆送信個体は、相手方に対するｱﾄﾞﾚｽ情報に基づいて実際ﾒｯｾｰｼﾞが伝達されるべき物理ｱﾄﾞﾚｽ情報および保安情報(送信ﾒｯｾｰｼﾞに対する受信暗号を必要とする場合)をｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに要請することによってこれを獲得 ◆この過程で、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞは、要請した受信個体の公認電子ｱﾄﾞﾚｽがﾌﾞﾗｯｸﾘｽﾄにあるかまたはﾎﾜｲﾄﾘｽﾄにあるかを確認(ﾌﾞﾗｯｸﾘｽﾄにある場合、ﾒｯｾｰｼﾞ転送ｴﾗｰを送信個体に通知) ◆送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞがｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに受信者に対する物理ｱﾄﾞﾚｽおよび保安情報を要請した後、これを受信
2	ﾒｯｾｰｼﾞ送受信および転送の確認	◆送信個体は、ﾒｯｾｰｼﾞを技術規格に合わせてﾊﾟｯｹｰｼﾞﾝｸﾞした後、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞの公認認証書を基盤に電子署名を遂行 ◆流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、先に獲得した物理ｱﾄﾞﾚｽにﾊﾟｯｹｰｼﾞﾝｸﾞし、電子署名されたﾒｯｾｰｼﾞを転送する ◆ﾒｯｾｰｼﾞを受信した受信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、ﾒｯｾｰｼﾞの基本ﾊﾟｯｹｰｼﾞﾝｸﾞ構造、電子署名に対する有効性、送信者に対する適合性を検証した後、受信確認のための受信証明書またはｴﾗｰﾒｯｾｰｼﾞを生成する ◆受信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、生成した受信証明書を送信個体に転送する ◆送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、受信証明書を受信して、1)受信証明書の適合性を検証、2)検証された情報を受信証明書に添付、3)受信証明書を自体保管および第 3 者保管機関に保管要請 ◆転送と転送確認の過程は同期式ﾒｯｾｰｼﾞ処理でなされる
3	業務受信者の受信確認	◆送信者がﾒｯｾｰｼﾞ転送時点で受信個体の閲覧証明書を要請した場合、受信個体は、ﾒｯｾｰｼﾞ閲覧時点で送信個体に閲覧確認を証明できる閲覧証明書を生成し、これを転送 ◆受信個体が送信個体に閲覧証明書を転送すれば、これを受信した送信個体は、1)閲覧証明書の適合性を検証し、2)検証された情報を閲覧証明書に添付、3)閲覧証明書を自体保管および第 3 者保管機関に保管要請、4)受信個体に受信確認ﾒｯｾｰｼﾞを同期式で転送
4	流通証明書の発給および保管	◆各ｽﾃｯﾌﾟ別に流通に対する証明を受けようとする場合、送信個体は、各ｽﾃｯﾌﾟに応じて受信、閲覧、送信に対する証明書を受信個体または流通中継ｻｰﾊﾞから発給を受け、これを第 3 者保管機関に保管することにより、流通に対する法的証明の根拠を確保

【０１１８】

メッセージ送受信プロセスは、転送プロセスと受信プロセスに区分することができ、転送プロセスは、流通クライアントと流通メッセージングサーバ間の連係方式によって同期式転送と非同期式転送に細分化される。

以下、図１５および表２３を参照し、同期式メッセージ送受信プロセスについて説明すれば、次の通りである。

【０１１９】

同期式メッセージ送受信プロセスは、送信個体の流通クライアントが流通メッセージングサーバに転送を要請すれば、これを受信個体の流通メッセージングサーバにリアルタイムで転送し、これに対する応答を送信者の流通メッセージングサーバを介して同期式で返してもらうプロセスである。同期式プロセスは、転送に対する結果を即刻に流通クライアントが確認することができるので、業務プロセスに対する定義が単純になる。

このような同期式メッセージ送受信プロセスに対する詳細な説明は下記表２３の通りである。

【０１２０】

【表２３】

【表 23】

番号	ﾌﾟﾛｾｽ名	説明
1	受信者に対する物理ｱﾄﾞﾚｽおよび保安情報の獲得	◆上述したﾒｯｾｰｼﾞ送受信ﾌﾟﾛｾｽと同一であり、細部ﾌﾟﾛｾｽは、後述する物理ｱﾄﾞﾚｽ獲得ﾌﾟﾛｾｽを参照
2	ﾒｯｾｰｼﾞ転送および転送確認	◆送信個体の流通ｸﾗｲｱﾝﾄは、文書を作成して添付した後、転送対象および方式(暗号化有無、閲覧証明書の受信有無など)を設定して、送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに転送要請をし、これに対する応答を受けるために通信を切らないで待つ ◆送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、これを受けて、直ちに受信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに転送する ◆送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、受信個体から転送に対する応答ﾒｯｾｰｼﾞを受信する(これに対する手続きは、上述したﾒｯｾｰｼﾞ送受信ﾌﾟﾛｾｽのﾒｯｾｰｼﾞ転送および転送確認ﾌﾟﾛｾｽを参照) ◆送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、受信した応答ﾒｯｾｰｼﾞを流通ｸﾗｲｱﾝﾄと連結された通信区間を通じて同期式で返す
3	業務受信者の受信確認	◆上述したﾒｯｾｰｼﾞ送受信ﾌﾟﾛｾｽと同一
4	流通証明書の発給および保管	◆上述したﾒｯｾｰｼﾞ送受信ﾌﾟﾛｾｽと同一

【０１２１】

以下、図１６および表２４を参照し、非同期式メッセージ送受信プロセスについて説明

すれば、次の通りである。

【０１２２】

非同期式転送プロセスは、送信個体の流通クライアントが流通メッセージングサーバに転送を要請すれば、流通メッセージングサーバに転送要請に有効性有無だけを検証した後、要請に対する受信確認メッセージを流通クライアントに返す。これを受信個体の流通メッセージングサーバにリアルタイムで転送し、これに対する応答を送信個体の流通メッセージングサーバを介して同期式で返してもらうプロセスである。

【０１２３】

非同期式プロセスは、転送しようとするメッセージの容量が大きかったり、１つのメッセージに対して複数の受信者を指定したりする場合のように、メッセージ転送に対する時間が多くかかるためにクライアントが応答を待つことが困難な状況で使う。

このような同期式メッセージ送受信プロセスに対する詳細な説明は下記表２４の通りである。

【０１２４】

【表２４】

【表 24】

番号	ﾌﾟﾛｾｽ名	説明
1	受信者に対する物理ｱﾄﾞﾚｽおよび保安情報の獲得	◆上述したﾒｯｾｰｼﾞ送受信ﾌﾟﾛｾｽと同一であり、細部ﾌﾟﾛｾｽは、後述する物理ｱﾄﾞﾚｽ獲得ﾌﾟﾛｾｽを参照
2	ﾒｯｾｰｼﾞ転送の要請	◆送信個体の流通ｸﾗｲｱﾝﾄは、文書を作成して添付した後、転送対象および方式(暗号化有無、閲覧証明書の受信有無など)を設定して、送信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに転送要請をする ◆送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、これを受けて、転送要請に対する有効性を検証した後、転送要請に対する受信確認を同期式で流通ｸﾗｲｱﾝﾄに返し、通信を終了する
3	受信者にﾒｯｾｰｼﾞ転送	◆送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、流通ｸﾗｲｱﾝﾄから受けた転送要請ﾒｯｾｰｼﾞを探し、受信者に転送する ◆送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、受信者から同期式で転送に対する応答ﾒｯｾｰｼﾞ(受信証明書またはｴﾗｰﾒｯｾｰｼﾞ)を受けた後、これを最初に転送要請した流通ｸﾗｲｱﾝﾄの受信箱に入れておく
4	転送結果の受信	◆流通ｸﾗｲｱﾝﾄは、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに接続して、自身に受信されたﾒｯｾｰｼﾞを持ってくるために受信ﾒｯｾｰｼﾞ Get 要請をする ◆受信個体から転送された応答ﾒｯｾｰｼﾞがあれば、流通ｸﾗｲｱﾝﾄはこれを応答ﾒｯｾｰｼﾞとして受信する
5	業務受信者の受信確認	◆上述したﾒｯｾｰｼﾞ送受信ﾌﾟﾛｾｽと同一
6	流通証明書の発給および保管	◆上述したﾒｯｾｰｼﾞ送受信ﾌﾟﾛｾｽと同一

【０１２５】

以下、メッセージ受信プロセスについて詳細に説明すれば、次の通りである。

【０１２６】

文書受信者が流通クライアントを介してメッセージを受信するプロセスは図１７の通りであり、プロセスに対する説明は下記表２５の通りである。受信者の流通メッセージングサーバが送信者からメッセージを受信すれば、これに対する応答として受信証明書を転送し、最終受信者のメッセージ箱に文書を入れておく。

【０１２７】

流通クライアントは、随時に流通メッセージングサーバに受信されたメッセージに対する目録を要請し、新たに受信されたメッセージがあれば、受信メッセージ目録を応答メッ

セージとして受けるようになり、この中、詳細情報を要請するメッセージを通じて受信文書をＧｅｔする。

【０１２８】

【表２５】

【表 25】

番号	ﾌﾟﾛｾｽ名	説明
1	ﾒｯｾｰｼﾞ受信	◆受信個体はﾒｯｾｰｼﾞを受信すれば、受信したﾒｯｾｰｼﾞに対する受信応答ﾒｯｾｰｼﾞを送信個体に返し、受信ﾒｯｾｰｼﾞを該当ﾕｰｻﾞの私書箱に保管
2	受信ﾒｯｾｰｼﾞ目録 Get	◆受信個体の流通ｸﾗｲｱﾝﾄは、連係した流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞｼｽﾃﾑに認証を経た後、受信文書を要請 ◆受信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、受信文書を要請したﾕｰｻﾞの私書箱に保管された受信文書目録を同期式応答で流通ｸﾗｲｱﾝﾄに伝達
3	受信文書 Get	◆受信者が受信ﾒｯｾｰｼﾞの目録からﾒｯｾｰｼﾞに対する詳細情報を見ることを要請すれば、流通ｸﾗｲｱﾝﾄは、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞｼｽﾃﾑに該当ﾒｯｾｰｼﾞの添付文書を含む詳細情報の伝達を要請 ◆受信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、私書箱に保管された受信文書の詳細情報および添付文書の原本を流通ｸﾗｲｱﾝﾄに同期式応答で伝達
4	閲覧証明書の転送(選択的ﾌﾟﾛｾｽ)	◆最初送信者が受信担当者の閲覧確認を要請した場合、受信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞｼｽﾃﾑは、ﾕｰｻﾞが受信文書に対する詳細情報の要請をした時点で、該当ﾒｯｾｰｼﾞの送信者に閲覧証明書を含むﾒｯｾｰｼﾞを転送 ◆但し、添付文書に暗号化がなされた場合には、詳細情報を持っていった時点ではなく、ﾕｰｻﾞが添付文書を復号化した後に閲覧状態を流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに伝達した時点で、閲覧証明書を生成して、転送者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに伝達するべきである。この時、復号化過程でｴﾗｰが発生すれば、ｴﾗｰに対する状態情報を伝達し、受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、閲覧証明書の代わりに復号化ｴﾗｰﾒｯｾｰｼﾞを転送者に伝達する ◆受信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、送信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞから転送した閲覧証明書ﾒｯｾｰｼﾞ(またはｴﾗｰﾒｯｾｰｼﾞ)に対する受信応答ﾒｯｾｰｼﾞを受信

【０１２９】

［物理アドレス獲得プロセス］

流通体系に参加する送信個体は、相手方にメッセージを転送する前に、公認電子アドレス情報に基づいて物理的な実アドレス情報を必ず知るべきであり、付加的に添付する文書を暗号化するためには、アドレスディレクトリサーバにある受信者の公開キー情報を獲得し

なければならない。
公認電子アドレスの物理アドレスを獲得する手続きは必須ステップとして下記の１）～４）がある。
【０１３０】
１）送信個体は、受信個体のアドレス情報を基準に受信個体に対する物理アドレス情報および保安情報の獲得のためにアドレスディレクトリサーバに問い合わせる
２）アドレスディレクトリサーバは、送信個体の問い合わせを受信／検証した後、これを処理
３）送信個体は、受信した物理アドレスを基準に経路設定をして、受信個体にメッセージ転送
４）受信個体の流通メッセージングサーバは、これを受けて、ユーザアカウントまたは内部区分子に応じてメッセージを内部的に分配
また、流通体系において、公認電子アドレスの物理アドレスを獲得する方式は２つに区分することができ、下記の１）および２）の通りである。
【０１３１】
１）流通クライアントが受信者のアドレス情報を入力する時点でアドレスディレクトリサーバに検索要請をして、物理アドレスと受信者の公開キーを持ってくる方式：１）公認電子アドレスの有効性を事前にチェックするためのものである、２）流通クライアントと流通メッセージングサーバ（送信個体）間にメッセージ暗号化が必要な時
【０１３２】
２）流通クライアントが流通メッセージングサーバにメッセージ送信を要請した後、流通メッセージングサーバがアドレスディレクトリサーバから物理アドレスを持ってくる方式
公認電子アドレスの物理アドレスおよび保安情報の獲得プロセスは図１９の通りである。
【０１３３】
［流通中継支援プロセス］
流通体系は、送信個体と受信個体間の直接通信（Ｐ２Ｐ）を基本とする。しかし、付加的にネットワーク、受信個体の流通メッセージングサーバのエラーなどによってメッセージ流通に障害が発生した場合、ユーザの便宜および流通の円滑な支援のために流通を中継／代行する中継プロセスを提供する。
【０１３４】
送信個体がメッセージを受信個体に転送する過程でエラーが発生して転送が失敗する場合に、電子文書流通ハブ内の流通中継サーバは、送信個体を代行してメッセージを委託／転送することによって送信個体の転送事実を立証し、送信個体のシステム的な負担を減らす役割を遂行する。
図２３はこれに対する基本的な流れを提示し、図２４は流通中継サーバがメッセージを中継するプロセスを示している。
下記表２６は流通中継プロセスを段階的に説明している。
【０１３５】

【表２６】

【表 26】

番号	ﾌﾟﾛｾｽ名	説明
1	ﾒｯｾｰｼﾞ送信代行の要請	◆送信個体は、ﾒｯｾｰｼﾞﾊﾟｯｹｰｼﾞﾝｸﾞおよび保安処理後、受信個体にﾒｯｾｰｼﾞを転送 ◆転送過程でｴﾗｰが発生して転送が最終的に失敗した時、送信個体は、流通中継ｻｰﾊﾞにﾒｯｾｰｼﾞを代行して転送するように依頼 ◆転送依頼を受け付けした流通中継ｻｰﾊﾞは、送信個体に送信証明書を同期式で発給、転送
2	ﾒｯｾｰｼﾞの委託中継	◆流通中継ｻｰﾊﾞは、中継依頼を受けたﾒｯｾｰｼﾞを転送。転送失敗時には一定間隔で再試しをする(再試し回数および間隔は流通中継ｻｰﾊﾞの政策に応じて決定) ◆流通中継ｻｰﾊﾞが転送に最終的に失敗した場合、ﾒｯｾｰｼﾞ中継を依頼した送信個体に転送失敗ﾒｯｾｰｼﾞを伝達
3	受信および閲覧証明書の発給	◆受信個体がﾒｯｾｰｼﾞを正常に受信した後、受信証明書を流通中継ｻｰﾊﾞに転送 ◆受信者が電子文書を閲覧した後、受信個体は、閲覧証明書を流通中継ｻｰﾊﾞを経由せずに送信個体に直接転送

【０１３６】

［流通証明書などの保管プロセス］

流通体系内で行われる全ての流通行為と関連し、その結果として、流通証明書は必ず生成され、第３者保管機関に保管されなければならない。これは、流通証跡を含んだ流通証明書を法的に認められた第３者保管機関に保管することにより、流通事実に対する法的推定力が確保できるためである。

【０１３７】

流通証明書を保管するプロセスは、電子文書流通とは別個のプロセスであって、流通行為事実を証明するための支援プロセスである。そのために、全ての流通メッセージングサーバは、事前に流通証明書を受信、保管できる機能を備えた特定第３者保管機関に加入するべきである。

【０１３８】

さらには、送信個体が電子文書の内容証明を望む場合、流通証明書の以外にメッセージ全体を第３者保管機関に保管することもできる。

第３者保管機関が流通証明書を受信して保管するためには、次の１）および２）のような２つの付加的なシステムを具備しなければならない。

１）第３者保管機関事業者の流通メッセージングサーバ：流通体系内の流通メッセージングサーバと流通証明書を送受信するために必要なシステム

【０１３９】

２）第３者保管機関連係クライアントモジュール：第３者保管機関事業者の流通メッセ

ージングサーバを介して受信した流通証明書を第３者保管機関に保管するために第３者保管機関連係インターフェースと通信するためのモジュール

但し、第３者保管機関事業者が電子文書中継者を兼ねる場合には、流通メッセージングサーバは追加的に必要ではなくなる。

【０１４０】

図２８は送受信個体と第３者保管機関事業者間の流通証明書を保管するプロセスを示しており、流通証明書保管プロセスを段階的に説明すれば、下記表２７の通りである。

【０１４１】

【表２７】

【表 27】

番号	ﾌﾟﾛｾｽ名
1	送信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、受信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞから流通証明書を受信 ◆受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞから受信証明書を受けたり中継ﾊﾌﾞから送信証明書を受けたりする場合は、応答ﾒｯｾｰｼﾞとして流通証明書を受信 ◆受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞから閲覧証明書を受けたり中継ﾊﾌﾞを介して受信証明書を受けたりする場合は、要請ﾒｯｾｰｼﾞとして流通証明書を受信
2	-受信した流通証明書を検証して有効性が確認されれば、流通証明書と証明書の検証情報を事前に設定された第 3 者保管機関の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに転送 -流通証明書が有効でなければ、受信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに流通証明書の検証ｴﾗｰﾒｯｾｰｼﾞを通知して再転送を要請 ◆要請ﾒｯｾｰｼﾞとして流通証明書を受けた場合は、これに対する応答ﾒｯｾｰｼﾞとして検証ｴﾗｰﾒｯｾｰｼﾞを転送(同期式) ◆応答ﾒｯｾｰｼﾞとして流通証明書を受けた場合は、新しい要請ﾒｯｾｰｼﾞとして検証ｴﾗｰﾒｯｾｰｼﾞを転送(非同期式) ◆流通証明書の検証ｴﾗｰﾒｯｾｰｼﾞを受けた場合には、新しい要請ﾒｯｾｰｼﾞとして流通証明書を再転送するか、証明発給失敗ﾒｯｾｰｼﾞを転送(非同期式) ◆有効な流通証明書を受けなかった場合には、電子文書転送に失敗したものとみなして電子文書を再び転送するべきである
3	第 3 者保管機関の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、第 3 者保管機関の保管要請ﾒｯｾｰｼﾞを受信すれば、流通証明書および検証情報の保管のための保管要請 Client を呼び出す(第 3 者保管機関が電子文書中継者を兼ねている場合、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞが第 3 者保管機関の保管要請 Client を直接呼び出す(ﾛｰｶﾙ保管要請))
4	流通証明書の保管要請 Client は、第 3 者保管機関の連係ｲﾝﾀｰﾌｪｰｽ規格に応じて流通証明書と検証情報を第 3 者保管機関に保管要請

【０１４２】

［公認電子アドレス登録などの管理プロセス］
送受信個体が流通体系に参加するためには、公認電子アドレスを申請して登録を受けるべきであり、登録代行機関および管理機関は、公認電子アドレスと関連した情報の登録などを管理するべきである。公認電子アドレス情報の管理プロセスには、公認電子アドレスと関連した登録、変更、削除などに対する管理プロセスとブラックリスト／ホワイトリストの管理プロセスがある。
【０１４３】
管理機関は、公認電子アドレスの効率的な管理のために、公認電子アドレスの登録代行機関を設けて公認電子アドレスを管理する。
登録代行機関は、次の１）～４）のような業務を遂行する。
１）公認電子アドレス申請者の身元確認などの審査業務
２）公認電子アドレス登録者の登録情報の変更業務
３）公認電子アドレスの登録抹消などの業務支援
４）その他の公認電子アドレスの管理と関連した業務
管理機関は、登録代行機関として第３者保管機関および電子文書中継者のうちから要件を満足する者を選定することができる。
以下、公認電子アドレス登録プロセスについて説明すれば、次の通りである。
【０１４４】
流通体系に参加しようとする企業／機関／個人などは公認電子アドレスを申請するべきであり、登録代行機関は申請された情報を審査、処理して結果を通知するべきである。これと関連したプロセスは図２２の通りである。
以下、公認電子アドレス登録情報の変更プロセスについて説明すれば、次の通りである。
【０１４５】
既に登録された公認電子アドレスと関連した情報は色々な事情のために変更し得るが、但し、公認電子アドレスと所有者情報は同一性を維持しなければならないため、変更することはできない。
【０１４６】
公認電子アドレスと関連した情報変更に対する権限は、登録代行機関に委任して処理するようにする。但し、情報変更に対する履歴情報を管理機関と登録代行機関間のサービスレベル協約（ＳＬＡ）に応じて保管しなければならない。
【０１４７】
これと関連したプロセスは図２３の通りであり、図２３を参照すれば、公認電子アドレスの変更は本人だけが可能である。個人の場合、公認電子アドレス、登録番号、名前は変更不可であるため、公認電子アドレスを脱退し、新規で生成しなければならない。そして、企業の場合、公認電子アドレスは変更不可であり、登録番号（事業者登録番号）および商号名は、変更時、必ず該当情報に変更してもらった新規公認認証書と共に変更しなければならない。
【０１４８】
図２４は登録代行機関の変更プロセスを示し、このような図２４を参照すれば、登録代行機関を変更しようとする場合には、１）既存の登録代行機関から脱退、２）新規な登録代行機関を介した新規登録過程を経なければならない。この場合、アドレスディレクトリサーバに公認電子アドレスの一時留保を要請できなければならない。アドレスディレクトリサーバは、全ての公認電子アドレスの脱退時、公認電子アドレスの一時留保を選択できるようにすることにより、登録代行機関の変更時に一定期間公認電子アドレスを維持できるようにする。
以下、公認電子アドレスの更新および使用停止、削除のプロセスについて説明すれば、次の通りである。
【０１４９】
既に登録された公認電子アドレスは、設定した使用年限に合わせて更新しなければなら

ない。公認電子アドレスの登録後、サービス政策に基づいて設定しておいた使用年限が過ぎる前に所有者が更新するべきである。仮に所有者が更新しなければ、公認電子アドレスに対する所有権を失い、公認電子アドレスは自動抹消される。

さらには、公認電子アドレスの満了期間にならなくても申請者が使用停止や抹消を望む場合、これに対する機能を提供するべきである。

【０１５０】

［電子文書の書式適用プロセス］

このプロセスは、メッセージ流通以後のステップの活用度を高めるためのプロセスである。メッセージ内に含まれている電子文書を、企業の内部システムにおいて、自動または半自動化された方式で処理するためのものである。流通メッセージングサーバは、当事者間のメッセージ送受信機能を専担し、流通クライアントは、送受信するためのメッセージを送受信者が利用しやすいようにインターフェースを提供する。その後のステップは、メッセージ内にある電子文書を活用するステップである。電子文書の書式登録機や電子文書の書式は電子文書の活用段階をより効率的に運用するための方法などを提供する。

【０１５１】

流通体系に応じて流通される文書の様式には制限はない。イメージ、オフィス文書、動画などが可能であるが、ユーザの便宜性を高めるために、流通体系においては書式形態の文書作成機能を付加的に提示する。

【０１５２】

このような付加機能は電子文書交換（ＥＤＩ）機能を導入したものであり、送受信個体間に約束された電子文書フォーマットを基盤に文書データを送受信して、受信個体の内部システムにおいて受信した電子文書を自動で変換処理できるようにした。

電子文書の書式は次の１）および２）のような２つの方式で活用可能である。

１）電子文書流通ハブにある電子文書の書式登録機を活用する方式で電子税金計算書のように標準化された電子文書の書式を主に使用

２）送受信個体間に合意した電子文書の書式を共有して活用する方式で特定企業に特化した非標準化された電子文書の書式を主に使用

以下、電子文書の書式登録機の活用について詳細に説明すれば、次の通りである。

【０１５３】

企業、機関や個人ユーザは、電子文書の書式登録機に登録された電子文書の書式を検索した後、流通クライアントに登録して使える。電子文書の書式登録機を活用する方式は、次の１）および２）のような２つの方式がある。

１）流通クライアントから直接電子文書の書式登録機にある電子文書を検索して持ってくる方式

２）電子文書の書式登録機サイトから電子文書を検索してローカルＰＣにダウンロード後、流通クライアントに登録して使う方式

【０１５４】

電子文書の書式登録機は、標準化された電子文書の書式を登録／活用するため、管理機関が体系的に運営／管理しなければならず、次の１）～３）のような基準を有し得る。

１）ユーザは、電子文書の書式登録機サイトを通して申請しなければならない。申請はサイトから提供するフォーマットと手続きに従わなければならない。

２）登録／申請した電子文書は管理機関の審査を経て登録されるべきである。

３）各々の電子文書は体系的なコンテキスト（文脈）を基盤に分類されるべきである。

【０１５５】

【表２８】

【表 28】

区分	説明	備考
地域	該当電子文書が国際的に流通できるか、特定地域で流通できるか、特定国家にのみ流通できるかを区分	
構文	該当電子文書に適用された構文が EDIFACT 基盤であるか、XML 基盤であるか、ﾌﾟﾗｲﾍﾞｰﾄﾌｫｰﾏｯﾄであるかを区分	
産業	該当電子文書が特定産業にのみ適用される時に使用。例えば、購買注文書が貿易部門で使われるか、でなければ、製造または流通、物流部門で使われるかを区分	
製品	該当電子文書が特定会社製品のﾌｫｰﾏｯﾄを使う場合。PDF ﾌｫｰﾏｯﾄであるか、特定会社の e-Form ﾌｫｰﾏｯﾄであるかなどを区分	
企業	該当電子文書が特定企業にのみ使用できる場合に区分	
その他	上記区分の以外に他のｺﾝﾃｷｽﾄ(文脈)で区分できる場合	

【０１５６】
図２５は電子文書の書式登録機を活用するプロセスに対する基本的な流れを提示し、具体的には、図２５ａは電子文書の書式登録機と流通クライアントが直接連係する場合を示し、図２５ｂは電子文書の書式登録機サイトを利用する場合を示している。
下記表２９は、流通クライアントと直接連係して書式を活用するプロセスについて示す。
【０１５７】
【表２９】

【表 29】

番号	区分	説明
1	電子文書の書式検索	流通ｸﾗｲｱﾝﾄから直接電子文書の書式登録機にある電子文書の書式を検索
2	書式持ち込み	書式を探した場合、これを流通ｸﾗｲｱﾝﾄに持ってくる
3	書式登録	流通ｸﾗｲｱﾝﾄに持ってきた書式を流通ｸﾗｲｱﾝﾄに登録
4	電子文書書式の取り込み/作成	流通ｸﾗｲｱﾝﾄに登録されている電子文書の書式を取り込んで電子文書を作成し、これをﾒｯｾｰｼﾞに添付

【０１５８】
下記表３０は電子文書の書式登録機サイトを活用するプロセスについて示す。
【０１５９】

【表３０】

【表 30】

番号	区分	説明
1	電子文書の書式検索	電子文書の書式登録機ｻｲﾄに接続して、必要とする電子文書の書式を検索
2	書式をﾛｰｶﾙ PC に格納	検索された書式をﾀﾞｳﾝﾛｰﾄﾞしてﾛｰｶﾙ PC に格納
3	書式登録	ﾛｰｶﾙ PC に格納された書式を流通ｸﾗｲｱﾝﾄに登録
4	電子文書書式の取り込み/作成	流通ｸﾗｲｱﾝﾄに登録されている電子文書の書式を取り込んで電子文書を作成し、これをﾒｯｾｰｼﾞに添付

以下、合意した電子文書の書式活用について説明すれば、次の通りである。

【０１６０】

特定企業に限定された書式を、企業が運営するサイトなどにおいて書式を配布して、特定企業と関連した当事者と取り引きをするための目的で使うためのものである。

図２６は合意した電子文書の書式を利用する手続きを示しており、図２６と関連したプロセスに対する説明は下記表３１の通りである。

【０１６１】

【表３１】

【表 31】

番号	区分	説明
1	電子文書の書式配布	企業 A は、自身のｼｽﾃﾑで処理できる電子文書の書式を自身が運営するｳｪﾌﾞｻｲﾄにおいて配布し、取り引きする企業がこれを活用できるように支援
2	書式をﾛｰｶﾙ PC に格納	企業 B2 は、ｳｪﾌﾞｻｲﾄから書式をﾀﾞｳﾝﾛｰﾄﾞしてﾛｰｶﾙ PC に格納
3	書式登録	ﾛｰｶﾙ PC に格納された書式を企業 B の流通ｸﾗｲｱﾝﾄに登録
4	電子文書書式の取り込み/作成	流通ｸﾗｲｱﾝﾄに登録されている電子文書書式を取り込んで電子文書を作成し、これをﾒｯｾｰｼﾞに添付
5	ﾒｯｾｰｼﾞ転送	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞを介してﾒｯｾｰｼﾞを転送
6	添付された電子文書の自動/半自動処理	受信したﾒｯｾｰｼﾞに添付されている電子文書を、変換などの処理を通じて企業 A の内部ｼｽﾃﾑに自動または半自動で登録

【０１６２】

［スパムメッセージの処理プロセス］

流通体系において、送信者は認証された流通メッセージングサーバを介して転送をし、受信者もこれを通じて受信するので、スパムが発送された時、送信者に責任を問える基盤構造を有している。

【０１６３】

しかし、特定送信者が電子文書中継者にユーザアカウントを開設し、これを利用して商業的な目的のためのメッセージなどを転送する場合がある。現在の認証方式がシステムの技術的内容に対する認証だけを対象にしているため、スパムメッセージなどを初期に根本的に遮断することが容易ではない状況である。

【０１６４】

このようなスパムメッセージなどの流通を遮断するために、流通体系においては、認証目録管理基盤のホワイトリスト、スパムや悪意的な意図を有したブラックリストを管理できる体系を提供して、流通体系の安全性と信頼性を向上させるようにする。

【０１６５】

スパムメッセージ申告および送信相手方に対する確認のための機能は必須機能であり、全ての流通メッセージングサーバはこの機能を必ず構築しなければならない。

以下、スパムメッセージ申告方案について説明すれば、次の通りである。

スパムメッセージの申告手続きを段階的に説明すれば、下記表３２の通りである。

【０１６６】

【表３２】

【表 32】

番号	ﾌﾟﾛｾｽ名
1	受信者がﾒｯｾｰｼﾞを受信した時点でｽﾊﾟﾑﾒｯｾｰｼﾞと判断されれば、受信者は、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞを介してｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに該当ﾒｯｾｰｼﾞを受信ﾒｯｾｰｼﾞとして申告する
2	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞからｽﾊﾟﾑﾒｯｾｰｼﾞ申告を受け付けたｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞは、受付済みに対する確認ﾒｯｾｰｼﾞを返す
3	ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞを管理する主体である管理機関は、該当ﾒｯｾｰｼﾞを分析し、送信者に対する調査を通じて送信者の公認電子ｱﾄﾞﾚｽに対してﾌﾞﾗｯｸﾘｽﾄへの追加有無を審査し判断する
4	最終的にﾌﾞﾗｯｸﾘｽﾄ対象者に確定されれば、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞは、該当公認電子ｱﾄﾞﾚｽをﾌﾞﾗｯｸﾘｽﾄに追加した後、送信者にﾌﾞﾗｯｸﾘｽﾄ追加に対する内容を通知する
5	ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞは、ｽﾊﾟﾑﾒｯｾｰｼﾞ要請に対する処理結果をｽﾊﾟﾑ申告者(受信者)に伝達する

【０１６７】

受信者は、受信したメッセージがスパムメッセージと判断されれば、図２７のようなプロセスによってスパムメッセージをアドレスディレクトリサーバに申告する。

ホワイトリストとブラックリストの役割は次の通りである。

１）ホワイトリスト：送信流通メッセージングサーバが認証を受けて正式に登録されたメッセージングサーバに対する情報のみが記録される

２）ブラックリスト：転送者のアドレスがスパム発送者として登録された場合、ブラックリストに登録される

【０１６８】

※同一の流通メッセージングサーバを介してブラックリストに登録されるスパムアドレスが重複して発生する場合、管理機関は、流通メッセージングサーバに対する認証取り消しの有無を判断した後、認証を取り消し、ホワイトリストから削除することができる。

以下、スパムメッセージ受信時の処理方案について説明すれば、次の通りである。

【０１６９】
受信個体は、メッセージ受信時、送信相手方が信頼できるほどの正当なユーザであるか否かを確認するために、アドレスディレクトリサーバのホワイトリストとブラックリストを確認した後、受信拒否をするか否かを決定する。
【０１７０】
送信者に対する確認は、受信時点で１）リアルタイムで確認するか、受信者の流通メッセージングサーバシステムにＣａｃｈｅ形態で管理している目録を通じて確認する２）周期的な確認方法がある。
【０１７１】
１）リアルタイム確認プロセス：受信個体は、メッセージを受信する時点でアドレスディレクトリサーバに送信個体のアドレスがホワイトリスト、ブラックリストに登録されているか否かを判断した後、メッセージに対する受信拒否の可否を決定する。
【０１７２】
【表３３】

【表 33】

番号	ﾌﾟﾛｾｽ名
1	受信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、ﾒｯｾｰｼﾞを受信すれば、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに正当なﾕｰｻﾞであるか否かを確認するために、確認要請ﾒｯｾｰｼﾞを伝達
2	ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞは、要請を受けたﾕｰｻﾞのｱﾄﾞﾚｽ情報がﾎﾜｲﾄﾘｽﾄに含まれているか否かを確認
3	該当ｱﾄﾞﾚｽがﾎﾜｲﾄﾘｽﾄになければ、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞは、直ちに確認要請者に登録されていないﾕｰｻﾞであることを結果ﾒｯｾｰｼﾞとして返し、ﾎﾜｲﾄﾘｽﾄにあれば、再び該当ｱﾄﾞﾚｽがﾌﾞﾗｯｸﾘｽﾄに登録されたｱﾄﾞﾚｽであるか否かを確認
4	ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞは、確認要請者にﾌﾞﾗｯｸﾘｽﾄの登録有無に対する結果ﾒｯｾｰｼﾞをﾘﾀｰﾝ
5	受信者は、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞから送信者が正当なﾕｰｻﾞではないもの(ﾎﾜｲﾄﾘｽﾄになかったりﾌﾞﾗｯｸﾘｽﾄに登録されたりした場合)として結果ﾒｯｾｰｼﾞを受けた場合、受信ﾒｯｾｰｼﾞを自体的にｽﾊﾟﾑﾒｯｾｰｼﾞとして処理した後、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞから受けた処理結果ﾒｯｾｰｼﾞとｽﾊﾟﾑﾒｯｾｰｼﾞの受信履歴を記録して保管
6	ｽﾊﾟﾑﾒｯｾｰｼﾞに対する処理履歴は必ず 1 ヶ月以上保管することにより、該当送信者に対する受信拒否の正当性を確認

【０１７３】
図２８はスパムメッセージをリアルタイムで確認するプロセスを示す。
２）周期的な確認プロセス：受信者は、アドレスディレクトリサーバからホワイトリストとブラックリストを周期的にもらって自体管理し、これを基盤に送信者のアドレスがホワイトリスト、ブラックリストに登録されたか否かを判断した後、メッセージに対する受信拒否の可否を決定
【０１７４】

【表３４】

【表 34】

番号	ﾌﾟﾛｾｽ名
1	受信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、予めｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞから最新のﾎﾜｲﾄﾘｽﾄとﾌﾞﾗｯｸﾘｽﾄを要請した後に自体的に管理。この時、ﾘｽﾄの変動事項の発生時、自動通知の要請有無を共に伝達する(変動事項発生の自動通知を要請した場合にも、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに最新ﾘｽﾄを持ってくるための要請を周期的に行うことにより、ﾘｽﾄ情報が最大限１日以上の差が生じないようにする)
2	ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞは、ﾎﾜｲﾄﾘｽﾄおよびﾌﾞﾗｯｸﾘｽﾄに変動事項が発生すれば、変動通知の要請をしたﾕｰｻﾞに変動内訳を broadcasting する
3	ﾘｽﾄに対する変動事項を受けた流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、自体管理するﾘｽﾄの情報を修正することによって同期化させる
4	受信者は、ﾒｯｾｰｼﾞを受信すれば、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに正当なﾕｰｻﾞであるか否かを確認するために自体管理するﾘｽﾄを確認
5	受信者は、自体管理するﾘｽﾄ点検の結果、送信者が正当なﾕｰｻﾞではないもの(ﾎﾜｲﾄﾘｽﾄになかったりﾌﾞﾗｯｸﾘｽﾄに登録されたりした場合)と判断した場合、受信ﾒｯｾｰｼﾞを自体的にｽﾊﾟﾑﾒｯｾｰｼﾞとして処理した後、ｽﾊﾟﾑﾒｯｾｰｼﾞの受信履歴を記録し保管する
6	ｽﾊﾟﾑﾒｯｾｰｼﾞに対する処理履歴は必ず １ ヶ月以上保管することにより、該当送信者に対する受信拒否の正当性を確認できるようにする

【０１７５】
図２９は流通メッセージングサーバとアドレスディレクトリサーバ間のスパムメッセージ管理のために周期的に確認を行うプロセスを示す。
【０１７６】
［エラー処理プロセス］
流通体系において、エラー発生類型は下記の１）と２）を含む２つに区分される。
【０１７７】
１）同期式応答に対するエラー発生：同期式応答に対するエラーの場合は、要請メッセージに対する処理結果を受ける時まで要請者は待機している状態であるので、エラーを直ちに認知可能
【０１７８】
２）非同期式応答に対するエラー発生：要請者は、要請内容のみを伝達した後、それに対する処理結果をその後に受けるので、追加的なエラー処理が行われるべきである
以下、同期式エラー処理方案について説明すれば、次の通りである。
【０１７９】
同期式転送に対する全てのエラーは、転送者が直ちに確認可能であるので、再転送することを基本とする。再転送方式については流通体系に参加する企業や機関のシステム政策に応じて決定されるが、同一のメッセージ転送に対しては同一のＭｅｓｓａｇｅＩｄ値を設定して再度送ることを基本とする。
同期式エラー処理と関連した類型は次の１）～４）の通りである。
【０１８０】
１）要請メッセージの送信失敗：送信者がメッセージを転送する過程で転送エラーが発生して、受信者に要請メッセージが伝達できなかった場合であり、送信者は、転送試みに対するｔｉｍｅｏｕｔまたはネットワークエラーメッセージなどを通じて送信失敗を認知するようになる。

【０１８１】
２）応答メッセージの受信失敗：送信者がメッセージを正常に転送したが、受信者から応答メッセージを受ける過程でエラーが発生した場合である。"１）要請メッセージの送信失敗"と区分されないのでエラーに対して同一の方式で処理するが、受信者は要請メッセージを正常に受けたので処理方式が異なる。
【０１８２】
３）エラーメッセージの受信：送信者がメッセージを正常に転送したが、受信者がメッセージを処理する過程でエラーが発生した場合である。この場合、送信者の処理方式はエラーメッセージの類型に応じて異なる。
【０１８３】
４）３段階同期式エラー：流通クライアントが流通メッセージングサーバを介して他の流通メッセージングサーバ、アドレスディレクトリサーバ、流通中継ハブと連係する３個体間のメッセージ流通は、連係類型中、最終結果を即刻に確認するために同期式で連係する方案を支援する。この過程で流通メッセージングサーバと受信者間の連係ステップでエラーが発生すれば、流通メッセージングサーバは、即刻にエラーを発生させた後、これを流通メッセージングサーバに応答メッセージとして伝達するべきである。
以下、非同期式エラー処理方案について説明すれば、次の通りである。
【０１８４】
流通クライアントが流通メッセージングサーバを介して他の流通メッセージングサーバ、アドレスディレクトリサーバ、流通中継サーバと連係する３個体間のメッセージ流通は、流通クライアントが最終受信者の状況に独立に運営できるように非同期式方式の連係を支援したりもする。
【０１８５】
非同期式転送に対する最終エラーは同期式転送とは異なり、転送者が直ちに確認できないため、流通メッセージングサーバが最終的にエラーを確認した時点で流通クライアントのためのエラーメッセージを発生させ、これを流通クライアントが受信できるようにするべきである。
【０１８６】
［電子文書閲覧サービス］
電子文書閲覧サービスは、送信者と受信者間に電子文書を直接やり取りする交換の形態ではない、送信者のシステムまたは第３者保管機関に保管されている電子文書を閲覧できるように提供するサービスである。
【０１８７】
電子文書閲覧サービスは既存の流通体系をそのまま利用する。但し、送信者は、受信者に電子文書を含んだメッセージを転送するのではなく、送信者システムまたは第３者保管機関に保管されている電子文書を閲覧できる閲覧権限を含んだメッセージを転送することが特徴である。
【０１８８】
これと関連した手続きは次の通りである。
１）受信者の公開キー獲得
２）電子文書の保管
３）閲覧権限およびＤＲＭなどの保安が適用された証書生成
４）閲覧権限などの証書の転送および転送確認
５）受信者による電子文書の閲覧
６）流通（閲覧）証明書または閲覧証跡の発給および保管
電子文書閲覧サービスは、送信者が自体システムを利用する方法と第３者を利用する方法に区分することができる。
【０１８９】
図３０は送信者が自体システムを活用して電子文書閲覧サービスを利用する流れを提示しており、図３０で明示している手続きについて説明すれば、下記表３５の通りである。

【０１９０】
【表３５】

【表35】

番号	ﾌﾟﾛｾｽ名	説明
1	受信個体の認証書の公開ｷｰ獲得	電子文書の閲覧権限を生成する時に必要な受信個体の認証書の公開ｷｰをｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞから獲得
2	電子文書の保管および閲覧権限の生成	電子文書を送信個体の自体ｼｽﾃﾑに保管
3	閲覧権限およびDRMなどの保安適用した証書生成	保管された電子文書を閲覧できる権限およびDRMなどの保安を適用した閲覧権限証書を生成
4	閲覧権限の転送	閲覧権限を含む証明書を受信個体に転送
5	電子文書の閲覧	受信個体の受信者は閲覧権限を有し、送信個体の電子文書閲覧ｼｽﾃﾑに接続して電子文書を閲覧
6	流通(閲覧)証明書の保管	受信個体の受信者が電子文書を閲覧した場合、送信個体は流通(閲覧)証明書を生成し、これを第3者保管機関に保管

【０１９１】
上記のようなサービスを提供するために、送信者は、流通体系の以外に電子文書閲覧サービスを提供できるシステムを具備しなければならない。
【０１９２】
図３１は送信個体が第３者を活用して電子文書閲覧サービスを利用する流れを示しており、図３１で提示している手続きについて説明すれば、下記表３６の通りである。
【０１９３】

【表３６】

【表 36】

番号	ﾌﾟﾛｾｽ名	説明
1	受信個体の認証書の公開ｷｰ獲得	電子文書の閲覧権限を生成する時に必要な受信個体の認証書の公開ｷｰをｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞから獲得
2	電子文書の保管および閲覧ｻｰﾋﾞｽの依頼	送信個体は、電子文書を第3者保管機関に保管、依頼し、これに対する閲覧ｻｰﾋﾞｽを依頼(受信個体の公認電子ｱﾄﾞﾚｽ記載)
3	閲覧権限およびDRMなどの保安が適用された証書生成	第3者保管機関に保管依頼した電子文書を閲覧できる権限証書とDRMなどの保安が適用された証書を生成
4	閲覧権限証書の転送	第3者保管機関の閲覧権限を含む証書を受信個体に転送
5	電子文書の閲覧	受信個体の受信者は閲覧権限を有し、第3者保管機関に接続して電子文書を閲覧
6	流通(閲覧)証明書の保管	第3者保管機関受信個体の受信者が電子文書を閲覧した場合、流通(閲覧)証明書を生成し、これを保管
7	流通(閲覧)証明書の転送	さらに、第3者保管機関の閲覧ｻｰﾋﾞｽを依頼した送信個体に流通(閲覧)証明書を転送

【０１９４】

［企業内のシステムとの連係方法］

企業／機関は、内部的に様々な電子文書を生産し保管したり、外部の企業／機関などと様々な方式で電子文書をやりとりしたりする。

【０１９５】

郵便などのようなオフラインで交換したり、ｅ－メールや業務関連システムで交換したりする。これらの各々の流通体系は、企業／機関の内部と連係する時、下記表３７および図１１９のような方式で連係する。

【０１９６】

【表３７】

【表 37】

区分	説明
郵便流通体系	-取り引き当事者は公文書などの書類を郵便で発送 -企業/機関の担当者が公文書などの書類が入られた郵便を受信 -郵便をはがして公文書などの書類を受領、登録し、内部決済 -決済後、文書受信箱に書類形態で保管
	-(長所)1)以前から使われたので慣れた方式、2)IT ｼｽﾃﾑ費用などがかからない -(短所)1)流通に多くの時間がかかる、2)ｻｰﾋﾞｽ手数料および書類保管などに費用発生、3)検索などに多くの時間がかかる
e-ﾒｰﾙ流通体系	-取り引き当事者は公文書などの書類を e-ﾒｰﾙで発送 -企業/機関の担当者が e-ﾒｰﾙﾌﾟﾛｸﾞﾗﾑで公文書などの書類を含んだ e-ﾒｰﾙを受信 -(内部ｼｽﾃﾑと連動する場合)受信されたﾒｯｾｰｼﾞ内にある電子文書を内部ｼｽﾃﾑで半自動形態で登録、処理 -(内部ｼｽﾃﾑと連動しない場合)受信されたﾒｯｾｰｼﾞ内にある電子文書を担当者のﾛｰｶﾙ PC に格納。内部ｼｽﾃﾑに接続して格納された電子文書を登録、処理
	-(長所) 1)使いやすさ、 2)業務の補助手段として世界的に広く活用、 3)費用がほぼかからない -(短所) 1)担当者間に交換されるので担当者の追加的な業務処理が必要であり、担当者の誤りや変動などによって業務障害が発生し得る 2)e-ﾒｰﾙﾌﾟﾛﾄｺﾙの不安定性のために受信ｴﾗｰなどが発生した場合、法的な紛争が発生し得る 3)流通される電子文書を企業/機関が総括的に管理できず、担当者によって地域的に処理、管理される 4)業務の単純な補助手段として 1 回性の使用目的、保管/削除に対する概念が脆弱 5)個人による e-ﾒｰﾙ管理が普遍化し、企業 e-ﾒｰﾙに対する使用と管理原則および統制の不足 6)大概のﾜｰﾄﾞ文書などの非構造化された文書に対する流通で、自動化した処理が不可(半自動~手動処理)
電子文書交換(EDI)流通体系	-取り引き当事者は電子文書を EDI を通じて発送 -受信者は EDI ｱﾌﾟﾘｹｰｼｮﾝを通じて電子文書を受信 -受信された電子文書は自動変換、処理され、内部ｼｽﾃﾑに登録 -企業/機関の担当者は内部ｼｽﾃﾑに登録された電子文書を業務に応じて確認、処理
	-(長所) 1)人の干渉なしで電子文書を自動で変換、処理することによって業務効率性が高い、 2)正確な転送が可能であり、転送ｴﾗｰに対する紛争時に中継者の責任 -(短所) 1)初期投資費用が多くかかるか、ｱｳﾄｿｰｼﾝｸﾞする場合にはｻｰﾋﾞｽ手数料が発生、 2)事前に取り引き当事者と業務、文書などに対する合意が必要、 3)構造化された(標準化された)文書のみ流通可能。非構造化された文書流通は不可
業務関連ｼｽﾃﾑ流通体系	-取り引き当事者はｳｪﾌﾞﾌﾞﾗｳｻﾞを通じて受信者が運営するｳｪﾌﾞｻｲﾄにﾛｸﾞｲﾝなどのﾕｰｻﾞ認証を通じて接続 -ｳｪﾌﾞｻｲﾄから提供する手続きと方法の通りに文書作成およびﾌｧｲﾙ添付処理 -企業/機関の担当者は、業務関連ｼｽﾃﾑに接続して受信した電子文書を確認。業務関連ｼｽﾃﾑそのものが内部ｼｽﾃﾑであるので特別な処理はない
	-(長所) 1)受信者は自動で電子文書などを受信するので受信者の業務効率性が高い、 2)送信者は、追加的なﾌﾟﾛｸﾞﾗﾑ設置が不要および流通費用が発生しない -(短所) 1)受信者中心の流通体系であり、送信者はいちいち受信者が運営するｼｽﾃﾑに接続しなければならないので送信者の不便が加重、 2)電子文書が受信者ｼｽﾃﾑにのみ残るので今後の紛争発生時に送信者に不利

【０１９７】

公認電子アドレス基盤の電子文書流通体系は、次のような方式で企業／機関の内部と連係することができる。

以下、内部システムと連動する方式について説明すれば、次の通りである。

【０１９８】

内部システムと連動する方式は、主に企業や機関において流通メッセージングサーバを

設置する時に使用する形態で、流通クライアントを内部システムにシステム統合（ＳＩ）形態で開発する方式であり、詳細な説明および図は下記表３８および図１２０の通りである。

【０１９９】

【表３８】

【表 38】

区分	説明
自動処理方式	-企業の内部ｼｽﾃﾑにおいて利用するﾕｰｻﾞ認証体系の共有 -電子文書は標準電子文書の書式または合意した電子文書の書式を使用 -特定の公認電子ｱﾄﾞﾚｽに届いたﾒｯｾｰｼﾞの場合、自動処理できるように流通文書処理ｼｽﾃﾑが必要(ﾒｯｾｰｼﾞ内の電子文書のﾊﾟｰｼﾝｸﾞ、適合性の検証など) -公認電子ｱﾄﾞﾚｽに応じて該当の内部ｼｽﾃﾑに転送、登録
半自動処理方式	-企業の内部ｼｽﾃﾑにおいて利用するﾕｰｻﾞ認証体系の共有 -流通ｸﾗｲｱﾝﾄには電子契約ｼｽﾃﾑなどの内部ｼｽﾃﾑと連動体系が既に構築されていなければならない -企業/機関の担当者は流通ｸﾗｲｱﾝﾄ内容に応じて内部ｼｽﾃﾑに半自動形態で登録

【０２００】

以下、内部システムと連動しない方式について説明すれば、次の通りである。

【０２０１】

内部システムと連動しない方式は、主に電子文書中継者からユーザアカウントの発給を受けて利用する公認送受信者に好適な形態であり、電子文書中継者が提供するウェブ形態の流通クライアントを利用するか、電子文書中継者が配布する流通クライアントアプリケーションをローカルＰＣに設置して利用する方式であり、詳細な説明および図面は下記表３９および図１２１の通りである。

【０２０２】

【表３９】

【表 39】

区分	説明
ｳｪﾌﾞ方式	-電子文書中継者が運営するｳｪﾌﾞｻｲﾄに会員加入してﾕｰｻﾞｱｶｳﾝﾄを確保 -ｳｪﾌﾞｻｲﾄを基盤に流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに接続。受信したﾒｯｾｰｼﾞ内の電子文書をﾛｰｶﾙPCに格納 -企業内部ｼｽﾃﾑがある小企業の場合、ﾛｰｶﾙPCに格納されている電子文書を内部ｼｽﾃﾑに登録、保管
ｱﾌﾟﾘｹｰｼｮﾝ方式	-電子文書中継者は流通ｸﾗｲｱﾝﾄ設置ﾌｧｲﾙを配布 -送受信者は流通ｸﾗｲｱﾝﾄｱﾌﾟﾘｹｰｼｮﾝをﾛｰｶﾙPCに設置 -流通ｸﾗｲｱﾝﾄｱﾌﾟﾘｹｰｼｮﾝで流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに接続。受信したﾒｯｾｰｼﾞ内の電子文書をﾛｰｶﾙPCに格納 -企業内部ｼｽﾃﾑがある小企業の場合、ﾛｰｶﾙPCに格納された電子文書を内部ｼｽﾃﾑに登録、保管

※ｳｪﾌﾞ方式はｳｪﾌﾞ方式でﾕｰｻﾞが接続、処理する方式であり、個別ﾕｰｻﾞがﾛｰｶﾙPCにﾌﾟﾛｸﾞﾗﾑを設置する必要がない。

※ｱﾌﾟﾘｹｰｼｮﾝ方式は個別ﾕｰｻﾞが設置ﾌﾟﾛｸﾞﾗﾑをﾀﾞｳﾝﾛｰﾄﾞしてﾛｰｶﾙPCにﾌﾟﾛｸﾞﾗﾑを設置した後、流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに接続して使用。

【０２０３】

［外部システムとの連係方案］

流通体系は、自体システムとインターネットを基盤に流通ネットワークを有する。電子文書流通は流通体系内だけで行われるので制約がある。流通体系は、直接連結されていないシステムとの電子文書流通のために外部連係ゲートウェイサーバを設けている。

外部連係ゲートウェイサーバの基本概念図は図３２の通りである。

【０２０４】

外部連係ゲートウェイサーバは中間経由地の役割を遂行する。一方は流通体系のための流通メッセージングサーバなどを有しており、他方は外部システムとの連係のための各々のアダプターを有している。

【０２０５】

このように、外部システムと連係するためには、業務的な要素と技術的な要素を考慮しなければならない。

【０２０６】

業務的な要素は、連係と関連した業務手続き、方法などに対する当事者間の合意により、管理機関と外部連係システム管理機関は相互間にサービスレベル協約（ＳＬＡ）を結ばなければならない。

技術的な要素は、連係と関連して必要なユーザ認証、メッセージング、メッセージフォーマットなどと関連した技術要素をいう。

外部システムと連係をするための技術的な原則を整理すれば、次の１）～６）の通りである。

【０２０７】

１）（アドレス）送信者は、中間経由地アドレスと最終目的地アドレスを記載するべきである。

２）（ユーザ認証）送信者は、外部システムが送信者を認証できるようにユーザ情報を

提供するべきである。事前に外部システムに加入している場合、外部システムの認証識別子を使える。

３）（メッセージ分解＆組み立て）受信したメッセージを分解して外部システムに合せたメッセージに組み立てるべきである。

４）（メッセージ保安など）メッセージに適用された暗号化、ＤＲＭなどに対する保安などを検証／変換するべきである。

５）（メタデータ情報）メッセージ内に含まれてメッセージおよび電子文書の関連情報を検証／変換するべきである。

【０２０８】

６）（外部連係システムに対する識別）流通体系と連係する外部システムは追加や変更することができる。外部システムに対する情報はアドレスディレクトリサーバにおいて管理し、流通メッセージングサーバにおいては、必要な場合、アドレスディレクトリサーバに問い合わせして処理しなければならない。

外部システムと連係して電子文書が流通される手続きは図３３の通りである。

【０２０９】

上述したような本発明の好ましい実施形態による電子文書流通システムおよびこれを用いた電子文書流通方法において、電子文書流通が行われるためには、アドレスディレクトリサーバ、流通メッセージングサーバ、流通クライアント、流通中継サーバのような構成要素が必要であり、これらの構成要素は、電子文書流通の全体的な流れの中で互いに連係しなければならない。このように各構成要素間において互いに連係して動作するためには、連係のための通信プロトコル、メッセージ交換方式、連係メッセージ構造などが定義されなければならない。

【０２１０】

以下では、各構成要素間の連係のために先ず共通の基盤通信プロトコルおよびメッセージ交換方式を定義し、各連係類型別のメッセージ構造を標準で定義して提示し、これにより、本発明は、相異なる環境および開発方法によって構築された構成要素間の連係が円滑になって、相互運用を可能にすることができる。

【０２１１】

［連係のための基盤通信プロトコル］

公認電子アドレス基盤の電子文書の流通体系下で、各構成要素間の情報および電子文書を流通するために必要な電子文書流通連係インターフェースにおいて、流通連係メッセージは"ｅｂＸＭＬ　Ｍｅｓｓａｇｅ　Ｓｅｒｖｉｃｅｓ　ｖ２．０規格"（以下、ｅｂＭＳ）を基盤にし、これを階層的に拡張してより一般化された形態で定義される。ｅｂＸＭＬ基盤の構造は、ＳＯＡＰ、ＳＯＡＰ　ｗｉｔｈ　Ａｔｔａｃｈｍｅｎｔ、Ｓｅｃｕｒｉｔｙ、そしてＲｅｌｉａｂｉｌｉｔｙなど、独立的ではあるが、互いに密接な関係のある要素で構成されている。"連係のための基盤通信プロトコル"（以下、基盤通信プロトコル）は、このような基本要素を基盤に流通体系で必要な要素を定義し、これを有機的に再組み合わせした形態で構成される。

【０２１２】

基盤通信プロトコルは、転送しようとするメッセージを構成するパッケージング、メッセージ封筒の構成、メッセージ保安、そして最終的にメッセージを転送し受信するメッセージ送受信で構成される。

以下、基盤プロトコル構成において、メッセージパッケージングについて説明すれば、次の通りである。

【０２１３】

流通連係メッセージの全体メッセージ構造はｅｂＭＳ　ｖ２．０規格を準用する。本基盤通信プロトコルで定義するメッセージは２つの論理的なＭＩＭＥ　Ｐａｒｔを有する。

【０２１４】

１番目のＭＩＭＥ　Ｐａｒｔはヘッダコンテナーと呼ばれ、ＳＯＡＰメッセージを含んでおり、ＳＯＡＰメッセージは再びＨｅａｄｅｒとＢｏｄｙとから構成される。

２番目のＭＩＭＥ　Ｐａｒｔからはペイロードコンテナーと呼ばれ、アプリケーションレベルのメッセージおよび添付文書を含む。
【０２１５】
１番目のＭＩＭＥ　Ｐａｒｔに対する詳細説明は下記で述べる。この領域には、メッセージ流通のための共通情報（メッセージのルーティング関連情報、ＳＯＡＰメッセージ交換パターン、電子署名、エラー情報、および２番目に添付されるデータに対する位置情報など）が記述される。
【０２１６】
２番目のＭＩＭＥ　Ｐａｒｔは各連係インターフェース別の要請および応答メッセージを添付し、この連係インターフェースの類型に応じて、３番目以後のＭＩＭＥ　Ｐａｒｔの存在有無が決定される。流通体系を利用して電子文書や証明書を伝達する時、３番目のＭＩＭＥ　Ｐａｒｔに含まれる。
【０２１７】
流通連係メッセージの基本的な構造は図３４の通りであり、図３４において、１）"ＳＯＡＰ－ＥＮＶ：Ｈｅａｄｅｒ"は流通プロトコル規格に応じて構成され、ＭｅｓａｇｅＨｅａｄｅｒおよびＳｉｇｎａｔｕｒｅ情報で構成され、２）"ＳＯＡＰ－ＥＮＶ：ＢＯＤＹ"は流通プロトコル規格で定義されたＭａｉｎｆｅｓｔ要素情報およびユーザログイン情報が入り、３）"転送コンテナー＃１（ペイロードコンテナー＃１）"は要請メッセージおよび応答メッセージを含む部分であり、連係インターフェースの類型および要請、応答、エラーメッセージの有無に応じてビジネス文書の詳細内容が定義され、４）"転送コンテナー＃２（ペイロードコンテナー＃２）"は連係インターフェースの類型に応じて添付されるべき文書がペイロードコンテナー＃２から順次入る。
【０２１８】
このような流通連係メッセージは、Ｓｉｍｐｌｅ　Ｏｂｊｅｃｔ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ（ＳＯＡＰ）１．１、およびＳＯＡＰ　Ｍｅｓｓａｇｅｓ　ｗｉｔｈ　Ａｔｔａｃｈｍｅｎｔのような標準規格を遵守しなければならない。
【０２１９】
図３４において、流通連係メッセージの全てのＭＩＭＥ　Ｈｅａｄｅｒ要素は、ＳＯＡＰ　Ｍｅｓｓａｇｅｓ　ｗｉｔｈ　Ａｔｔａｃｈｍｅｎｔｓ規格を遵守しなければならない。さらに、メッセージ内のＣｏｎｔｅｎｔ－Ｔｙｐｅ　ＭＩＭＥ　Ｈｅａｄｅｒは、必ずＳＯＡＰメッセージ文書を含むＭＩＭＥ　Ｂｏｄｙ部分のＭＩＭＥメディア類型と同一のｔｙｐｅ属性を有するべきである。ＳＯＡＰ規格に応じたＳＯＡＰメッセージのＭＩＭＥ類型は、"ｔｅｘｔ／ｘｍｌ"値を有するべきであるとなっている。ルート部分は、［ＲＦＣ２０４５］に準ずる構造を有するＣｏｎｔｅｎｔ－ＩＤ　ＭＩＭＥ　Ｈｅａｄｅｒを含むことと、Ｍｕｌｔｉｐａｒｔ／Ｒｅｌａｔｅｄメディア類型に対する必須のパラメータに追加して、ｓｔａｒｔパラメータ（［ＲＦＣ２３８７］においては選択事項）が常に存在しなければならない。ｍｕｌｔｉｐａｒｔ／ｒｅｌａｔｅｄメッセージパッケージのＭＩＭＥ　Ｈｅａｄｅｒの例題は下記表４０の通りである。
【０２２０】

【表４０】

【表 40】

```
Content-Type:multipart/related;type=" text/xml " ;boundary=" boundaryValue " ;
start=messagepackage-123@example.com


--boundaryValue
Content-ID:<messagepackage-123@example.com>
```

【０２２１】

図３４において、１番目のＭＩＭＥ　Ｐａｒｔヘッダコンテナーは必ずＳＯＡＰメッセージを含むべきである。ヘッダコンテナーのＭＩＭＥ　Ｃｏｎｔｅｎｔ－Ｔｙｐｅ　ｈｅａｄｅｒは、ＳＯＡＰ規格に応じ、"ｔｅｘｔ／ｘｍｌ"値を有するべきである。Ｃｏｎｔｅｎｔ－Ｔｙｐｅヘッダは"ｃｈａｒｓｅｔ"属性を含むべきであり、例題は下記表４１の通りである。そして、ＭＩＭＥ　ｃｈａｒｓｅｔ属性は、ＳＯＡＰメッセージを生成するのに用いられる文字群を識別するために使われる。ＭＩＭＥ　ｃｈａｒｓｅｔ属性値とヘッダコンテナーに位置するＳＯＡＰメッセージのエンコード宣言部は必ず一致するべきであり、その値はＵＴＦ－８であるべきである。ヘッダコンテナーの例題は下記表４２の通りである。

【０２２２】

【表４１】

【表 41】

```
Content-Type:text/xml;charset=" UTF-8 "
```

【０２２３】

【表４２】

【表 42】

```
Ctent-ID:<messagepackage-123@example.com> ---| Header
Content-Type:text/xml;charset=" UTF-8 " .                                    |
                                                                             |
<SOAP:Envelope --|SOAP Message |
    xmlns:SOAP=" http://schemas.xmlsoap.org/soap/envelope/ " > | |
  <SOAP:Header> | |
    … | |
  </SOAP:Header> | |
  <SOAP:Body> | |
    … | |
  </SOAP:Body> | |
</SOAP:Envelope> --| |
                                                                             |
```

【０２２４】

図３４において、ペイロードコンテナーの個数は、連係インターフェース種類に応じて異なり得る。各ペイロードコンテナーは、ｅｂＭＳ規格に応じ、ＳＯＡＰ　Ｂｏｄｙ内のＭａｎｉｆｅｓｔ要素によって参照されるべきである。例題は下記表４３の通りである。

【０２２５】

【表４３】

【表 43】

```
Content-ID:<domainname.example.com> -------------| ebXML MIME |
Content-Type:application/xml -------------| |
                                                    | Payload
<Invoice> -------------| | Container
<Invoicedata> | Payload |
   … | |
</Invoicedata> | |
</Invoice> -------------| |
```

【０２２６】

図３４において、本発明で必須要素として指定したＭＩＭＥ　Ｈｅａｄｅｒの他、実現

便宜上、ＭＩＭＥ　Ｈｅａｄｅｒを追加することも可能である。この時、追加されるＭＩＭＥ　Ｈｅａｄｅｒは必ず［ＲＦＣ２０４５］に明示された項目でなければならない。しかし、追加的なＭＩＭＥ　Ｈｅａｄｅｒに対しては、これを追加しない側がこれを認知し解釈する必要はない。

以下、基盤プロトコル構成において、メッセージ封筒の構成について説明すれば、次の通りである。

【０２２７】

ＳＯＡＰ規格に準じて全ての拡張要素内容は、有効なネームスペースに限定されるべきである。本発明で定義された全てのｅｂＸＭＬ　ＳＯＡＰ拡張要素内容は、ｅｂＸＭＬ　ＳＯＡＰ　Ｅｎｖｅｌｏｐｅ拡張ネームスペースに限定されるべきである。ネームスペース宣言部は、ＳＯＡＰ　Ｅｎｖｅｌｏｐ、ＨｅａｄｅｒまたはＢｏｄｙ要素に含まれているか、各ＳＯＡＰ拡張要素に直接含まれていてもよい。

【０２２８】

ＳＯＡＰ　Ｅｎｖｅｌｏｐは、ＳＯＡＰメッセージのＲｏｏｔ項目でＳＯＡＰメッセージ内の各種Ｎａｍｅｓｐａｃｅを宣言する。宣言するべきＮａｍｅｓｐａｃｅは次の通りである。

【０２２９】

【表４４】

【表 44】

項目	Namespace URL
SOAP	http://schemas.xmlsoap.org/soap/envelope/
Digital Signature	http://www.w3.org/2000/09/xmldsig#
Xlink	http://www.w3.org/1999/xlink
Xsi	http://www.w3.org/2001/XMLSchema-instance

メッセージ封筒スキーマ構造は図３５の通りであり、メッセージ封筒の例題は下記表４５の通りである。

【０２３０】

【表４５】

【表 45】

```
<SOAP:Envelope xmlns:SOAP=" http://schemas.xmlsoap.org/soap/envelope/ "
  xmlns:xsi=" http://www.w3.org/2001/XMLSchema-instance "
  xsi:schemaLocation=" http://schemas.xmlsoap.org/soap/envelope/
  http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd " >
 <SOAP:Header
xmlns:eb=  "  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
 "


xsi:schemaLocation=    "    http://www.oasis-open.org/committees/ebxml-msg/schema/msg-
header-2_0.xsd
   http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd " >
   <eb:MessageHeader...>
      ...
   </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body
xmlns:eb=  "  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
 "


xsi:schemaLocation=                                                              "
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
   http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd " >
   <eb:Manifest eb:version=" 2.0 " >
      ...
   </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>
```

【０２３１】

ＳＯＡＰ　Ｈｅａｄｅｒ要素は、ＳＯＡＰ　Ｅｎｖｅｌｏｐ要素の１番目の子要素として次の１）～４）のような拡張要素を含む。

１）ＭｅｓｓａｇｅＨｅａｄｅｒ：メッセージのルーティング情報（Ｔｏ／Ｆｒｏｍ、

など）とメッセージに関する他の文脈情報を含む必須要素
２）ＳｙｎｃＲｅｐｌｙ：メッセージを送受信する方式が同期式であることを示す要素
３）Ｓｉｇｎａｔｕｒｅ：ＳＯＡＰメッセージおよび添付文書に対する電子署名値を示す要素
４）ＥｒｒｏｒＬｉｓｔ：メッセージ構文の検証、メッセージ電子署名の検証などのメッセージを処理する過程でエラーが発生して、エラーメッセージを返す時に該当エラー内訳を入れる要素
【０２３２】
ＳＯＡＰ Ｂｏｄｙ要素は、ＳＯＡＰ Ｅｎｖｅｌｏｐｅ要素の２番目の子要素としてＭａｎｉｆｅｓｔのような拡張要素を含む。Ｍａｎｉｆｅｓｔは、ペイロードコンテナーまたはウェブのように他の場所に位置したデータを示す要素である。
【０２３３】
Ｍａｎｉｆｅｓｔ要素は、ペイロードコンテナーを参照するために必ず存在しなければならない。Ｍａｎｉｆｅｓｔ要素は、１個以上のＲｅｆｅｒｅｎｃｅ要素で構成された複合要素である。各Ｒｅｆｅｒｅｎｃｅ要素は、ペイロードコンテナーに含まれたペイロード文書の一部として含まれるか、ＵＲＬにアクセス可能な遠距離のリソースであるメッセージに関連したデータを識別する。ＳＯＡＰ Ｂｏｄｙには、ペイロードデータをのせないように勧告している。Ｍａｎｉｆｅｓｔの目的は次の１）および２）の通りである。
【０２３４】
１）ｅｂＸＭＬメッセージと関連した特定のペイロードを容易で直接的にアクセスできるようにする
２）パーシング作業がなくてもアプリケーションがペイロードを処理できるか否かを判断できるようにする
Ｍａｎｉｆｅｓｔ要素は、次の１）～３）のような属性と要素とから構成されている。
１）１個のｉｄ属性
２）１個のｖｅｒｓｉｏｎ属性
３）１個以上のＲｅｆｅｒｅｎｃｅ要素
Ｒｅｆｅｒｅｎｃｅ要素は、次の１）～２）のような下位要素で構成された複合要素である。
１）０個以上のＳｃｈｅｍａ要素：親Ｒｅｆｅｒｅｎｃｅ要素から識別されたインスタンス文書を定義するスキーマに対する情報
２）０個以上のＤｅｓｃｒｉｐｔｉｏｎ要素：親参照要素によってＲｅｆｅｒｅｎｃｅされたペイロードオブジェクトに対する説明
【０２３５】
Ｒｅｆｅｒｅｎｃｅ要素は、それ自体が［ＸＬＩＮＫ］の単純リンクである。ＸＬＩＮＫは、現在Ｗ３Ｃの候補勧告案（ＣＲ）である。ここで、ＸＬＩＮＫが使われたことは、連関関係の説明を明確にするための用語として提供されていることを知らせる。ＸＬＩＮＫプロセッサまたはエンジンの使用が必須ではないが、実現要求事項によっては有用である。Ｒｅｆｅｒｅｎｃｅ要素は、上記で提供された要素の内容と共に次の１）～５）のような属性内容を含んでいる。
【０２３６】
１）ｉｄ：Ｒｅｆｅｒｅｎｃｅ要素に対するＸＭＬ ＩＤ
２）ｘｌｉｎｋ－ｔｙｐｅ：この属性はＸＬＩＮＫ単純リンクで要素を定義。これは、"ｓｉｍｐｌｅ"という固定された値を有する
【０２３７】
３）ｘｌｉｎｋ：ｈｒｅｆ：この必須属性は参照されたペイロードオブジェクトのＵＲＩ値。これは、［ＸＬＩＮＫ］明細の単純リンクに準ずるものであるべきである
【０２３８】
４）ｘｌｉｎｋ：ｒｏｌｅ：この属性は、ペイロードオブジェクトやその目的を説明するリソースを識別。存在するのであれば、［ＸＬＩＮＫ］明細に準ずる有効なＵＲＩ値を

有するべきである
【０２３９】
５）この他に他の有効ネームスペースの属性が存在することができる。受信ＭＳＨは、上記で定義されたものの以外に外部のネームスペース属性は無視することができる
【０２４０】
Ｓｃｈｅｍａ要素は、参照する項目がそれを記述するスキーマを有しているのであれば（例：ＸＭＬ　Ｓｃｈｅｍａ、ＤＴＤ、またはＤａｔａｂａｓｅ　Ｓｃｈｅｍａ）、そのＳｃｈｅｍａ要素は、Ｒｅｆｅｒｅｎｃｅ要素の子要素として存在しなければならない。これは、スキーマとバージョンを識別する方法として使われ、親Ｒｅｆｅｒｅｎｃｅ要素によって識別されるペイロードオブジェクトを定義する。Ｓｃｈｅｍａ要素は、次の１）および２）のような属性を有する。
１）ｌｏｃａｔｉｏｎ：スキーマの必須ＵＲＩ
２）ｖｅｒｓｉｏｎ：スキーマのバージョン識別子
【０２４１】
ｘｌｉｎｋ：ｈｒｅｆ属性がｃｏｎｔｅｎｔ　ｉｄ（ＵＲＩ　ｓｃｈｅｍｅ　"ｃｉｄ"）であるＵＲＩを含んでいれば、そのｃｏｎｔｅｎｔ－ｉｄを有するＭＩＭＥはメッセージのペイロードコンテナーに表現されるべきである。そうでなければ、ｅｒｒｏｒＣｏｄｅをＭｉｍｅＰｒｏｂｌｅｍに、ｓｅｖｅｒｉｔｙをＥｒｒｏｒにするエラーを発信当事者に伝達するべきである。ｘｍｌ：ｈｒｅｆ属性がｃｏｎｔｅｎｔ　ｉｄ（ＵＲＩ　ｓｃｈｅｍｅ　"ｃｉｄ"）であるＵＲＩを含んでいなければ、ＵＲＩは解釈されず、実現に応じて、エラーを伝達するべきか否かを決定しなければならない。エラーが伝達されるべきであると決定されれば、ｅｒｒｏｒＣｏｄｅをＭｉｍｅＰｒｏｂｌｅｍに、ｓｅｖｅｒｉｔｙをＥｒｒｏｒにするエラーを発信当事者に伝達するべきである。
下記表４６は典型的な１個のペイロードＭＩＭＥ　Ｂｏｄｙ部分を有するメッセージのＭａｉｎｆｅｓｔを示す。
【０２４２】
【表４６】

【表46】

```
<eb:Manifest eb:id=" Manifest "  eb:version=" 2.0 " >
<eb:Reference eb:id=" pay01 "  xlink:href=" cid:payload-1 "  xlink:role=" http://regrep.
org/gci/purchaseOrder " >
<eb:Schema eb:location=" http://regrep.org/gci/purchaseOrder/po.xsd "  eb:version
=" 2.0 " />
<eb:Description xml:lang=" en-US " >Purchase Order for 100,000 widgets</eb:
Description>
</eb:Reference>
</eb:Manifest>
```

【０２４３】
以下、基盤プロトコル構成において、メッセージの細部構成要素について説明すれば、次の通りである。
【０２４４】
ＭｅｓｓａｇｅＨｅａｄｅｒ要素は、全てのｅｂＸＭＬメッセージに表現されるべき必須要素であり、必ずＳＯＡＰ　Ｈｅａｄｅｒ要素の子要素として表現されるべきである。

ＭｅｓｓａｇｅＨｅａｄｅｒ要素は、次のような下位要素で構成された複合要素である。
ＭｅｓｓａｇｅＨｅａｄｅｒのＥｌｅｍｅｎｔ構造は下記表４７の通りである。
【０２４５】
【表４７】

【表47】

項目名	説明			反復回数	類型	長さ
From	■ﾒｯｾｰｼﾞ送信の送受信個体情報			1..1		
	PartyId	type	■'ecf_cd'に固定			
		■送信者を識別するｺｰﾄﾞ ■流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞの場合、認証番号 ■流通ｸﾗｲｱﾝﾄの場合、自体管理番号を設定 ■ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞ、流通中継ｻｰﾊﾞの場合、個体ｺｰﾄﾞ値を設定		1..1	S	13
	Role	■送信者の役割 ■'sender'に固定		1..1	S	最大256
To	■ﾒｯｾｰｼﾞ受信の送受信個体情報			1..1		
	PartyId	■type	■'ecf_cd'に固定	1..1	S	13
		■受信者を識別するｺｰﾄﾞ ■流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞの場合、認証番号 ■流通ｸﾗｲｱﾝﾄの場合、自体管理番号を設定 ■ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞ、流通中継ｻｰﾊﾞの場合、個体ｺｰﾄﾞ値を設定		1..1	S	13
	Role	■受信者の役割 ■'receiver'に固定		1..1	S	最大256
CPAId	■取り引き協業定義書ID ■連係ｲﾝﾀｰﾌｪｰｽ類型に応じてｺｰﾄﾞ値を設定			1..1	S	最大256
ConversationId	■送受信ﾄﾗﾝｻﾞｸｼｮﾝ区分子			1..1	S	最大256
Service	■取り引き協業定義書に定義された業務ｻｰﾋﾞｽ区分子			1..1	S	最大256
Action	■Service内の特定業務ﾌﾟﾛｾｽ区分子 ■Service内で唯一の値			1..1	S	最大256

【表 47 の継続】

MessageData	■ﾒｯｾｰｼﾞを識別するためのﾃﾞｰﾀ		1..1		
	MessageId	■1 つのﾒｯｾｰｼﾞが有する唯一の識別子	1..1	S	最大 256
	Timestamp	■ﾒｯｾｰｼﾞ生成時間 ■UTC 形式 ■ex>2008-07-31T06:29:39.724Z	1..1	S	24
	RefToMessageId	■応答ﾒｯｾｰｼﾞにのみ存在 ■要請ﾒｯｾｰｼﾞの MessageId	0..1	S	最大 256
Other	■ｲﾝﾀｰﾌｪｰｽ種類に応じた拡張要素 ■要素名は該当ｲﾝﾀｰﾌｪｰｽに応じて他の名称を持つ ■細部な詳細内容は該当連係ｲﾝﾀｰﾌｪｰｽ(5 章、6 章、7 章、8 章)を参照		0..1		

【０２４６】

ＭｅｓｓａｇｅＨｅａｄｅｒのスキーマ構造は図３６の通りであり、ＭｅｓｓａｇｅＨｅａｄｅｒ項目コード表は下記表４８の通りであり、業務別Ｓｅｒｖｉｃｅ／Ａｃｔｉｏｎ項目は下記表４９の通りである。

【０２４７】

【表４８】

【表 48】

識別ｺｰﾄﾞ項目	ｺｰﾄﾞ値	ｺｰﾄﾞ値定義
PartyId	ads	ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞ個体ｺｰﾄﾞ
	ech	流通中継ｻｰﾊﾞ個体ｺｰﾄﾞ
CPAId	urn:ads-and-ecm-cpa	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞとｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞ間の連係ｲﾝﾀｰﾌｪｰｽ使用時
	urn:ecm-and-ecm-cpa	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ相互間の連係ｲﾝﾀｰﾌｪｰｽ使用時
	urn:ecm-and-ecc-cpa	流通ｸﾗｲｱﾝﾄと流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ間の連係ｲﾝﾀｰﾌｪｰｽ使用時
	urn:ech-and-ecm-cpa	流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞと流通中継ｻｰﾊﾞ間の連係ｲﾝﾀｰﾌｪｰｽ使用時

【０２４８】

【表４９】

【表 49】

項目	Service	Action	定義
流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞとｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞ間の連係ｲﾝﾀｰﾌｪｰｽ使用時	urn:ads-service	request	要請
		response	応答
流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ相互間の連係ｲﾝﾀｰﾌｪｰｽ使用時	urn:ecm-service	request	要請
		response	応答
流通ｸﾗｲｱﾝﾄと流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ間の連係ｲﾝﾀｰﾌｪｰｽ使用時	urn:ecc-service	request	要請
		response	応答
流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞと流通中継ｻｰﾊﾞ間の連係ｲﾝﾀｰﾌｪｰｽ使用時	urn:ech-service	request	要請
		response	応答

【０２４９】
ＭｅｓｓａｇｅＨｅａｄｅｒの例示は下記表５０の通りである。
【０２５０】

【表５０】

【表 50】

```
<eb:MessageHeader SOAP:mustUnderstand=" 1 " eb:id=" MessageHeader " eb:version=
" 2.0 " >
 <eb:From>
  <eb:PartyId eb:type=" ecf_cd " >1234567</eb:PartyId>
  <eb:Role>sender</eb:Role>
 </eb:From>
 <eb:To>
  <eb:PartyId eb:type=" ecf_cd " >4567899</eb:PartyId>
  <eb:Role>receiver</eb:Role>
</eb:To>
 <eb:CPAId>urn:ecm-and-ecm-cpa</eb:CPAId>
<eb:ConversationId>urn:ecm-and-ecm-cpa:0210050643</eb:ConversationId>
 <eb:Service>urn:ecm-service</eb:Service>
 <eb:Action>request</eb:Action>
 <eb:MessageData>
<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-4049-9fdb-a6c0ed9af4
67</eb:MessageId>
  <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
 </eb:MessageData>
 <eb:DuplicateElimination></eb:DuplicateElimination>
</eb:MessageHeader>
```

【０２５１】
ＳｙｎｃＲｅｐｌｙが存在するのであれば、同期式送信であることを意味し、次の１）～４）の属性を有する。
１）ｉｄ属性
２）ｖｅｒｓｉｏｎ属性
３）ＳＯＡＰ　ａｃｔｏｒ属性（必ず"ｈｔｔｐ：／／ｓｃｈｅｍａｓ．ｘｍｌｓｏａｐ．ｏｒｇ／ｓｏａｐ／ａｃｔｏｒ／ｎｅｘｔ"値を有するべきである）
４）ＳＯＡＰ　ｍｕｓｔＵｎｄｅｒｓｔａｎｄ属性
ＳｙｎｃＲｅｐｌｙ要素の例題は下記表５１の通りである。
【０２５２】

【表５１】

【表 51】

```
<eb:SyncReply eb:id=" 3833kkj9 " eb:version=" 2.0 " SOAP:mustUnderstand=" 1 "
 SOAP:actor=" http://schemas.xmlsoap.org/soap/actor/next " />
```

【０２５３】

流通連係メッセージは、送受信過程で生じ得る様々な危険要素に対応するために必ず電子的に署名されなければならない。したがって、Ｓｉｇｎａｔｕｒｅ要素がＳＯＡＰ Ｈｅａｄｅｒの子要素として必ず存在するべきである。

【０２５４】

流通連係メッセージにおいて電子署名の対象となる部分は、ＳＯＡＰメッセージ全体とペイロードコンテナーに含まれたメッセージおよび添付文書である。各署名対象情報はＤｉｇｅｓｔされ、電子署名情報内に各々含まれる。

［ＸＭＬＤＳＩＧ］規格に応じて電子署名を遂行する過程は次の１）～４）の通りである。

【０２５５】

１）ＳＯＡＰ ＥｎｖｅｌｏｐｅにＳｉｇｎａｔｕｒｅＭｅｔｈｏｄ、ＣａｎｏｎｉｃａｌｉｚａｔｉｏｎＭｅｔｈｏｄ、Ｒｅｆｅｒｅｎｃｅ要素を有したＳｉｇｎｅｄＩｎｆｏ要素と、必須ペイロードオブジェクトを［ＸＭＬＤＳＩＧ］に規定された通りに生成

－ＳｉｇｎｅｄＩｎｆｏ下位の１番目のＲｅｆｅｒｅｎｃｅ項目は、ＳＯＡＰメッセージ全体を対象にするので、ＵＲＩ値に""を記述する。

【０２５６】

－２番目のＲｅｆｅｒｅｎｃｅ項目からは、ペイロードコンテナーの個数だけ反復て記述するようにし、この時、ＵＲＩ値は添付文書のＭＩＭＥ Ｈｅａｄｅｒに定義されたｃｏｎｔｅｎｔ ＩＤ値を記述する（Ｄｉｇｅｓｔ対象は、Ｍｉｍｅ Ｈｅａｄｅｒを除いたＣｏｎｔｅｎｔ部分である）。

【０２５７】

２）正規化した後、［ＸＭＬＤＳＩＧ］に指定された通り、ＳｉｇｎｅｄＩｎｆｏに指定されたアルゴリズムを基準にＳｉｇｎｅｄＩｎｆｏのＳｉｇｎａｔｕｒｅＶａｌｕｅを算出

３）［ＸＭＬＤＳＩＧ］に指定された通り、ＳｉｇｎｅｄＩｎｆｏ、ＫｅｙＩｎｆｏ、ＳｉｇｎａｔｕｒｅＶａｌｕｅ要素を含むＳｉｇｎａｔｕｒｅ要素を生成

４）ＳＯＡＰ ＨｅａｄｅｒのＳｉｇｎａｔｕｒｅ要素をＳＯＡＰ Ｈｅａｄｅｒ要素に含ませる

【０２５８】

電子署名時に使われるアルゴリズム情報は次の通りである。アルゴリズムは、Ｗ３Ｃ "ＸＭＬ－Ｓｉｇｎａｔｕｒｅ Ｓｙｎｔａｘ ａｎｄ Ｐｒｏｃｅｓｓｉｎｇ" （ＲＦＣ３２７５）のアルゴリズム部分（６．０ Ａｌｇｏｒｉｔｈｍｓ）に基本的に従う。また、国内固有のアルゴリズムを支援するために、ＴＴＡＳ．ＩＦ－ＲＦＣ３０７５ "拡張性生成言語の電子署名構文と処理（ＸＭＬ－Ｓｉｇｎａｔｕｒｅ Ｓｙｎｔａｘ ａｎｄ Ｐｒｏｃｅｓｓｉｎｇ）" （韓国情報通信技術協会、２００４年）で定義されたアルゴリズムを利用する。

【０２５９】

次は流通プロトコルにおいて利用するアルゴリズム目録である。メッセージ送受信時、電子署名の生成および検証過程における曖昧性を最小化するために、次の１）～ ５）目録以外のアルゴリズムはその使用を制限する。

１）電子署名Ｎａｍｅｓｐａｃｅ

【０２６０】

【表５２】

【表 52】

<...xmlns:ds=＂http://www.w3.org/2000/09/xmldsig#＂...>

【０２６１】
２）ハッシュ（Ｄｉｇｅｓｔ）
；データを縮約するのに使われるアルゴリズムは、公認認証体系の関連規定を遵守するようにする。
【０２６２】
【表５３】

【表 53】

<ds:DigestMethod Algorithm=＂http://www.w3.org/2000/09/xmldsig#sha1＂/> または <ds:DigestMethod Algorithm=＂http://www.w3.org/2001/04/xmlenc#sha256/>

【０２６３】
３）電子署名（Ｓｉｇｎａｔｕｒｅ）
；メッセージの電子署名時に使われるアルゴリズムは、公認認証体系の関連規定を遵守するようにする。
【０２６４】
【表５４】

【表 54】

<ds:SignatureMethod Algorithm=＂http://www.w3.org/2000/09/xmldsig#rsa-sha1＂/> または <ds:SignatureMethod Algorithm=＂ http://www.w3.org/2001/04/xmldsig-more#rsa-sha256＂/>

【０２６５】
４）正規化（Ｃａｎｏｎｉｃａｌｉｚａｔｉｏｎ）
；論理的に同一の文書に対して物理的に色々な表現が可能なＸＭＬの特性のため、同じ文書に対して電子署名値が異に出ることがある。このような現象を防止するために必ず正規化過程を経なければならない。正規化は、注釈のない正規ＸＭＬ（Ｃａｎｏｎｉｃａｌ ＸＭＬ、ｏｍｉｔｓ ｃｏｍｍｅｎｔｓ）を使うようにする。
【０２６６】

【表５５】

【表 55】

```
<ds:CanonicalizationMethod Algorithm= "
http://www.w3.org/TR/2001/REC-xml-c14n-20010315 " />
```

【０２６７】
５）変換（Ｔｒａｎｓｆｏｒｍ）
；全体ＸＭＬデータ中の実際の署名対象となるデータを加工し選択する過程を経るアルゴリズムとして様々な変換アルゴリズムが存在するが、その中の３つだけを利用するようにする。第１は電子署名が署名対象内に含まれる形式に従うのでＥｎｖｅｌｏｐｅｄ Ｓｉｇｎａｔｕｒｅ変換であり、第２は前記で説明した正規化（Ｃａｎｏｎｉｃａｌｉｚａｔｉｏｎ）、そして第３は署名対象情報を選択するＸＰａｔｈフィルタリング（ＸＰａｔｈ Ｆｉｌｔｅｒｉｎｇ）である。
【０２６８】
【表５６】

【表 56】

```
<Transform Algorithm= " http://www.w3.org/2000/09/xmldsig#enveloped-signature " />
および
<ds:Transform Algorithm= " http://www.w3.org/TR/2001/REC-xml-c14n-20010315 " />
および
<ds:Transform Algorithm= " http://www.w3.org/TR/1999/REC-xpath-19991116 " >
<ds:XPath>not(ancestor-or-self::node()[@SOAP:actor=&amp;quot;urn:oasis:names:tc:ebxml-msg:
actor:nextMSH&amp;quot;]
    | ancestor-or-self::node()[@SOAP:actor= &amp;quot;http://schemas.xmlsoap.org/soap/
actor/next&amp;quot;])
  </ds:XPath>
</ds:Transform>
```

【０２６９】
電子署名構文の構造は図３７の通りであり、電子署名されたメッセージの例題は下記表５７の通りである。
【０２７０】

【表５７】

【表 57】

```
<?xml version= " 1.0 "  encoding= " utf-8 " ?>
<SOAP:Envelope xmlns:xlink= " http://www.w3.org/1999/xlink "
xmlns:SOAP= " http://schemas.xmlsoap.org/soap/envelope/ "
xmlns:eb=                                                                    "
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd "
xmlns:xsi= " http://www.w3.org/2001/XMLSchema-instance "
xsi:schemaLocation= " http://schemas.xmlsoap.org/soap/envelope/
http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd " >
  <SOAP:Header>
   <eb:MessageHeader eb:id= " ... "  eb:version= " 2.0 "  SOAP:mustUnderstand= " 1 "
>
   ...
   </eb:MessageHeader>
   <Signature xmlns= " http://www.w3.org/2000/09/xmldsig# " >
    <SignedInfo>
     <CanonicalizationMethod
      Algorithm= " http://www.w3.org/TR/2001/REC-xml-c14n-20010315 " />
     <SignatureMethod Algorithm= " http://www.w3.org/2001/04/xmldsig-more#rsa
-sha256 " />
     <Reference URI= "  " >
      <Transforms>
       <Transform
      Algorithm= " http://www.w3.org/2000/09/xmldsig#enveloped-signature " />
     <Transform Algorithm= " http://www.w3.org/TR/1999/REC-xpath-19991116 " >
      <XPath> not(ancestor-or-self::node()[@SOAP:actor=
        &amp;quot;urn:oasis:names:tc:ebxml-msg:actor:nextMSH&amp;quot;]
        | ancestor-or-self::node()[@SOAP:actor=  " http://schemas.xmlsoap.org/
soap/actor
/next " ])
      </XPath>
     </Transform>
     <Transform  Algorithm= " http://www.w3.org/TR/2001/REC-xml-c14n-20010315 "
/>
     </Transforms>
     <DigestMethod Algorithm= " http://www.w3.org/2000/09/xmldsig#sha1 " />
     <DigestValue>...</DigestValue>
    </Reference>
    <Reference URI= " cid://blahblahblah/ " >
     <DigestMethod Algorithm= " http://www.w3.org/2000/09/xmldsig#sha1 " />
     <DigestValue>...</DigestValue>
    </Reference>
   </SignedInfo>
   <SignatureValue>...</SignatureValue>
   <KeyInfo>...</KeyInfo>
  </Signature>
 </SOAP:Header>
 <SOAP:Body>
  <eb:Manifest eb:id= " Mani01 "  eb:version= " 2.0 " >
   <eb:Reference xlink:href= " cid://blahblahblah/ "  xlink:role= " http://ebxml.org/gci
/invoice " >
    <eb:Schema eb:version= " 2.0 "
     eb:location= " http://ebxml.org/gci/busdocs/invoice.dtd " />   </eb:Reference>
  </eb:Manifest>
 </SOAP:Body>
</SOAP:Envelope>
```

【０２７１】

ＥｒｒｏｒＬｉｓｔ要素は、メッセージ構文の検証、メッセージ電子署名の検証などの通信プロトコル処理過程でエラーが発生する場合に、Ｈｅａｄｅｒ下位に生成して送信者に同期式で返すべきである。ＥｒｒｏｒＬｉｓｔ要素が生成される場合には、必ずＭｅｓｓａｇｅＨｅａｄｅｒ要素内にＲｅｆＴｏＭｅｓｓａｇｅＩｄが存在するべきであり、ＲｅｆＴｏＭｅｓｓａｇｅＩｄはエラーが発生したメッセージのＭｅｓｓａｇｅＩｄを指し示すべきである。

ＥｒｒｏｒＬｉｓｔ要素は次の１）～５）のような属性を有する。

【０２７２】

１）ｉｄ属性

２）ＳＯＡＰ　ｍｕｓｔＵｎｄｅｒｓｔａｎｄ属性

３）ｖｅｒｓｉｏｎ属性

４）ｈｉｇｈｅｓｔＳｅｖｅｒｉｔｙ属性

５）１個以上のＥｒｒｏｒ要素

報告されるエラーがなければ、ＥｒｒｏｒＬｉｓｔ要素は存在してはいけない。ＥｒｒｏｒＬｉｓｔの構造は図３８の通りである。

【０２７３】

ｈｉｇｈｅｓｔＳｅｖｅｒｉｔｙ属性は、全てのＥｒｒｏｒ要素の最も深刻な状態を示す。特に、あるＥｒｒｏｒ要素がｓｅｖｅｒｉｔｙをＥｒｒｏｒに設定していれば、ｈｉｇｈｅｓｔＳｅｖｅｒｉｔｙはＥｒｒｏｒに設定するべきであり、そうではない場合には、ｈｉｇｈｅｓｔＳｅｖｅｒｉｔｙをＷａｒｎｉｎｇに設定するべきである。

Ｅｒｒｏｒ要素は次の１）～６）のような属性を有する。

１）ｉｄ属性

；ｉｄ属性は文書内でＥｒｒｏｒＬｉｓｔ要素を唯一に識別する役割をする。

２）ｃｏｄｅＣｏｎｔｅｘｔ属性

【０２７４】

；ｃｏｄｅＣｏｎｔｅｘｔ属性はｅｒｒｏｒＣｏｄｅｓのネームスペースまたはスキーマを示す。これは必ずＵＲＩでなければならない。この属性の基本値はｕｒｎ：ｏａｓｉｓ：ｎａｍｅｓ：ｔｃ：ｅｂｘｍｌ－ｍｓｇ：ｓｅｒｖｉｃｅ：ｅｒｒｏｒｓである。この属性に基本値がなければ、その明細の実現はｅｒｒｏｒＣｏｄｅｓを使用するということを示す。

３）ｅｒｒｏｒＣｏｄｅ属性

；必須ｅｒｒｏｒＣｏｄｅ属性はエラーを持つメッセージのエラーが有した本質を指示する。

４）ｓｅｖｅｒｉｔｙ属性

【０２７５】

；必須属性であるｓｅｖｅｒｉｔｙ属性はエラーの深刻性を示す。有効な値はＷａｒｎｉｎｇおよびＥｒｒｏｒのようである。Ｗａｒｎｉｎｇは、エラーは存在するが、対話中の他のメッセージは正常に生成されることを示し、Ｅｒｒｏｒは、復旧不可能なエラーがメッセージに存在し、対話中にこれ以上他のメッセージは生成されないことを示す。

５）ｌｏｃａｔｉｏｎ属性

【０２７６】

；ｌｏｃａｔｉｏｎ属性はエラーが存在するメッセージ部分を示す。仮にエラーがｅｂＸＭＬ要素内に存在し、要素が"ｗｅｌｌ－ｆｏｒｍｅｄ"であれば、ｌｏｃａｔｉｏｎ属性の内容は［Ｘｐｏｉｎｔｅｒ］であるべきである。

６）Ｄｅｓｃｒｉｐｔｉｏｎ属性

【０２７７】

；Ｄｅｓｃｒｉｐｔｉｏｎ要素の内容は、ｘｍｌ：ｌａｎｇ属性において定義された言語でエラーの叙述的な説明を提供する。通常、これは、ＸＭＬパーサーやメッセージを検証するソフトウェアが生成したメッセージとなる。この意味は、この内容はＥｒｒｏｒ要素を生成したソフトウェアの販売者や開発者によって定義されるということを意味する。

ＥｒｒｏｒＬｉｓｔの例題は下記表５８の通りである。

【０２７８】

【表５８】

【表 58】

```
<eb:ErrorList eb:id=" 3490sdo " ,eb:highestSeverity=" error " eb:version=" 2.0 "
SOAP:mustUnderstand=" 1 " >
  <eb:Error eb:errorCode=" SecurityFailure " eb:severity=" Error " eb:location="
URI_of_ds
:Signature " >
    <eb:Description xml:lang=" en-US " >Validation of signature failed<eb:Description>
  </eb:Error>
  <eb:Error...>... </eb:Error>
</eb:ErrorList>
```

【０２７９】

流通プロトコルを基盤にメッセージを送受信する過程でエラーが発生すれば、エラーを認知した送受信個体は相手方にエラー内容を報告しなければならない。報告するべきエラーは、メッセージ構造エラー、メッセージングエラー、および保安エラーのようである。

【０２８０】

本発明で定義する流通プロトコルより下位レイヤーに属するＨＴＴＰおよびＳｏｃｋｅｔのようなデータ通信プロトコルと関連したエラーは、データ通信プロトコルにおいて支援する標準メカニズムによって発見し報告されるべきであり、本発明で定義するエラー報告メカニズムは使わない。

エラーコードはエラー対象および類型別に区分され、詳しい内容は下記表５９の通りである。

【０２８１】

【表５９】

【表 59】

ｴﾗｰｺｰﾄﾞ	内容	詳細説明
ValueNotRecognized	要素内容や属性値が認識されない。	たとえ文書が well formed で有効であるものの、要素/属性の値が認識できない値であり、よって、ebXML ﾒｯｾｰｼﾞ ｻｰﾋﾞｽによって使用できない値を含む。
NotSupported	要素や属性が支援されない。	たとえ文書が well formed で有効であり、要素や属性がこの明細の規則や制約に従っているものの、ﾒｯｾｰｼﾞを処理できる ebXML ﾒｯｾｰｼﾞ ｻｰﾋﾞｽによって支援されない。
Inconsistent	要素内容や属性値がまた他の要素や属性に不一致する。	たとえ文書が well formed で有効であり、この明細の規則と制約に従うものの、要素と属性の内容が他の要素やそれらの属性に一致しない。
OtherXml	要素内容や属性値中のまた他のｴﾗｰ	たとえ文書が well formed で有効であるものの、その要素内容や属性値がこの明細内の規則と制約に従わず、他のｴﾗｰｺｰﾄﾞに属しない。Error 要素の内容は問題の本質を示すのに使われるべきである。
Delivery Failure	ﾒｯｾｰｼﾞ転送の失敗	受信されたﾒｯｾｰｼﾞが大概にあるいは確実に次の目的地に送られなかった。仮に severity が Warning に設定されていれば、ﾒｯｾｰｼﾞが配達される可能性は小さい。
TimeToLive Expired	ﾒｯｾｰｼﾞが存在できる時間が超過する	ﾒｯｾｰｼﾞが受信されたものの、MessageHeader 要素の TimeToLive 要素が制約した時間を超過した時刻に受信された。
Security Failure	ﾒｯｾｰｼﾞの保安検査に失敗	ﾒｯｾｰｼﾞを送った当事者の署名検証または権限または実名検査に失敗した。
Unknown	分からないｴﾗｰ	どのようなｴﾗｰ種類にも属しないｴﾗｰが発生したことを意味する。Error 要素の内容が問題の本質を示すのに使われるべきである。

【０２８２】
以下、ＨＴＴＰバインディング方案において、ＨＴＴＰを通じたメッセージ転送方案について説明すれば、次の通りである。
ＨＴＴＰバインディングの例題は下記表６０の通りである。
【０２８３】

【表６０】

【表 60】

```
POST /servlet/ebXMLhandler HTTP/1.1
Host:www.example2.com
SOAPAction: " ebXML "
Content-type:multipart/related;boundary= " BoundarY " ;type= " text/xml " ;
start= " <ebxhmheader111@example.com> "

--BoundarY
Content-ID:<ebxhmheader111@example.com>
Content-Type:text/xml

<?xml version= " 1.0 "  encoding= " UTF-8 " ?>
<SOAP:Envelope xmlns:xlink= " http://www.w3.org/1999/xlink "
  xmlns:xsi= " http://www.w3.org/2001/XMLSchema-instance "
  xmlns:SOAP= " http://schemas.xmlsoap.org/soap/envelope/ "

xmlns:eb=                                                                    "
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd "
  xsi:schemaLocation= " http://schemas.xmlsoap.org/soap/envelope/
  http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd " >
 <SOAP:Header>
  <eb:MessageHeader SOAP:mustUnderstand= " 1 "  eb:version= " 2.0 " >
   <eb:From>
    <eb:PartyId eb:type= " ecf_cd " >123456789</eb:PartyId>
    <eb:Role>sender</eb:Role>
   </eb:From>
   <eb:To>
    <eb:PartyId eb:type= " ecf_cd " >912345678</eb:PartyId>
    <eb:Role>receiver</eb:Role>
   </eb:To>
   <eb:CPAId>urn:ecm-and-ecm-cpa</eb:CPAId>
   <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
   <eb:Service>>urn:ecm-service</eb:Service>
   <eb:Action>request</eb:Action>
   <eb:MessageData>
    <eb:MessageId>20001209-133003-28572@example.com</eb:MessageId>
    <eb:Timestamp>2001-02-15T11:12:12.724Z</eb:Timestamp>
   </eb:MessageData>
  </eb:MessageHeader>
 </SOAP:Header>
 <SOAP:Body>
  <eb:Manifest eb:version= " 2.0 " >
   <eb:Reference xlink:href= " cid:ebxmlpayload111@example.com "
     xlink:role= " XLinkRole "  xlink:type= " simple " >
    <eb:Description xml:lang= " en-US " >Purchase Order 1</eb:Description>
   </eb:Reference>
  </eb:Manifest>
 </SOAP:Body>
</SOAP:Envelope>

--BoundarY
Content-ID:<ebxmlpayload111@example.com>
Content-Type:text/xml

<?xml version= " 1.0 "  encoding= " UTF-8 " ?>
<purchase_order>
 <po_number>1</po_number>
 <part_number>123</part_number>
 <price currency= " USD " >500.00</price>
</purchase_order>

--BoundarY--
```

以下、ＨＴＴＰバインディング方案において、ＨＴＴＰ　Ｒｅｓｐｏｎｓｅコードにつ

いて説明すれば、次の通りである。

【０２８４】

本発明において、ＨＴＴＰレベルの応答コードを返すために、［ＲＦＣ２６１６］に定義されたＨＴＴＰ応答コードを利用しなければならない。主な応答コードは下記表６１の通りである。

【表６１】

【表 61】

状態ｺｰﾄﾞ	連関ﾒｯｾｰｼﾞ	意味
200	OK	要請が確実に処理される
400	Bad Request	要請に文法的に誤った部分がある
401	Unauthorized	ｸﾗｲｱﾝﾄが正しい許可を受けずに許可が必要なﾍﾟｰｼﾞにｱｸｾｽしようとする
404	Not Found	このｱﾄﾞﾚｽでは、いかなる内容も発見できない
500	Internal Server Error	ｻｰﾊﾞ内部のｴﾗｰによって要請を正常に処理できない
503	Service Unavailable	処理できる限界を超えて過度に要請が入ってきて、ｻｰﾊﾞが現在の該当要請を処理できない

【０２８５】

以下、ＨＴＴＰバインディング方案において、ＨＴＴＰ転送の保安方案について説明すれば、次の通りである。

【０２８６】

流通体系内の全ての流通メッセージングサーバと流通メッセージングサーバ間の転送や流通メッセージングサーバと流通クライアント間の転送は、ネットワーク転送保安のために、必ずＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ） Ｖ３．０を利用したＨＴＴＰ／Ｓ（Ｓｅｃｕｒｅ Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）を使って処理するべきである。

本発明による流通体系において、エラーの発生類型は、大きく、同期式応答に対するエラー発生の場合と非同期式応答に対するエラー発生の場合に区分される。

【０２８７】

同期式応答に対するエラーの場合は、要請メッセージに対する処理結果を受ける時まで、最初の要請者は待機している状態であるのでエラーを直ちに認知することができるが、非同期式応答に対するエラーは、要請者は要請内容だけを伝達した後、それに対する処理結果を後で受けるので、追加的なエラー処理が行われるべきである。

以下、エラー処理方案において、同期式エラー処理方案について説明すれば、次の通りである。

【０２８８】

流通メッセージングサーバと他の流通メッセージングサーバ、アドレスディレクトリサーバ、流通クライアント、流通中継サーバ間の２個体間の全てのメッセージ流通は同期式方式の流通である。この他にも、流通クライアントが流通メッセージングサーバを介して他の流通メッセージングサーバ、アドレスディレクトリサーバ、流通中継サーバと連係する３個体間のメッセージ流通は、連係類型に応じて同期式または非同期式方式で連係する。

【０２８９】

同期式転送に対する全てのエラーは転送者が直ちに確認可能であるので再転送することを基本とする。再転送方式に対しては、流通体系に参加する企業や機関のシステム政策に応じて決定されるが、同一のメッセージ転送に対しては同一のＭｅｓｓａｇｅＩｄ値を設

定して再び送ることを基本とする。
【０２９０】
同一のＭｅｓｓａｇｅＩｄ値でメッセージを送ることにより、メッセージ転送過程のエラーが転送時点のエラーではなく、受信者が受信成功後に同期式で応答メッセージを転送する過程でエラーが発生した場合に対しても、重複メッセージ受信を検知することによって同一の要請を重複して処理することを防止する。
【０２９１】
同期式エラーの送信者と受信者は、各々連係類型に応じ、流通メッセージングサーバ、アドレスディレクトリサーバ、流通クライアント、流通中継サーバであってもよい。
【０２９２】
１）要請メッセージの送信失敗：送信者がメッセージを転送する過程で転送エラーが発生して、受信者に要請メッセージが伝達できない場合であり、送信者は転送試みに対するｔｉｍｅｏｕｔまたはネットワークエラーメッセージなどを通じて送信失敗を認知するようになる。図４１は要請メッセージ送信失敗時のプロセスを示しており、処理手続きは下記の１）～３）の通りである。
１）メッセージ送信者が転送する過程で転送エラーが発生する場合であって、多くの場合がネットワークエラーによって発生する
２）送信者は、ＨＴＴＰエラーのようなエラーメッセージを受けると、同一のメッセージを再び再転送要請するべきである
３）送信者は受信者に受信確認メッセージを受けた場合にのみ転送成功として認識する
【０２９３】
２）応答メッセージの受信失敗：送信者がメッセージを正常に転送したが、受信者から応答メッセージを受ける過程でエラーが発生した場合である。送信者の立場では、"１）要請メッセージの送信失敗"と区分できないのでエラーに対して同一の方式で処理するが、受信者は要請メッセージを正常に受けたので処理方式が異なる。図４２は応答メッセージの受信失敗と関連したプロセスを示し、処理手続きは下記の１）～３）の通りである。
１）メッセージが受信者に正常に伝達されたが、送信者が受信者から受信確認メッセージを受けていない場合
２）この場合、送信者は送信失敗エラーとして認識し、受信者に同一のメッセージを同一のＭｅｓｓａｇｅＩｄで再転送するようになる
３）受信者は、受信した文書のＭｅｓｓａｇｅＩｄが以前の受信メッセージと同一である場合には、重複受信として受信確認メッセージを送った後に内部処理
【０２９４】
３）エラーメッセージ受信：送信者がメッセージを正常に転送したが、転送したメッセージを受信した受信者がメッセージを処理する過程でエラーが発生した場合である。この場合、送信者の処理方式はエラーメッセージの類型に応じて異なる。通信プロトコル上のエラー類型は、上述した"ＥｒｒｏｒＬｉｓｔ"項目を、各連係インターフェース別に要請メッセージに対する内部処理過程で発生したエラーに対しては、各連係インターフェースのメッセージ構造を参照する。図４１はエラーメッセージ受信と関連したプロセスについて示し、処理手続きは下記の１）～３）の通りである。
１）送信者が受信者に転送したメッセージが正確に伝達されたが、転送メッセージそのものに誤りがあって、エラーメッセージの応答を受けた場合
【０２９５】
２）この場合、送信者は、要請メッセージを再生成した後にメッセージを再転送することが一般的であるが、エラー類型に応じてメッセージ処理を異にすることができる
【０２９６】
３）送信者が要請メッセージを再転送する時、転送するメッセージのＭｅｓｓａｇｅＩｄは同一である必要はなく、業務状況に応じて異に処理することができる
【０２９７】

４）３段階同期式エラー：流通クライアントが流通メッセージングサーバを介して他の流通メッセージングサーバ、アドレスディレクトリサーバ、流通中継サーバと連係する３個体間のメッセージ流通は、連係類型中、最終的な結果を即刻に確認するために同期式で連係する方案を支援する。この過程中、流通メッセージングサーバと受信者間の連係ステップでエラーが発生すれば、流通メッセージングサーバは、即刻にエラーを発生させた後、これを流通メッセージングサーバに応答メッセージとして伝達しなければならない。図４２は３段階同期式エラーと関連したプロセスについて示し、処理手続きは下記の１）～３）の通りである。

【０２９８】

１）流通クライアントが流通メッセージングサーバと連係してメッセージ転送をするステップにおいては転送成功をしたが、流通メッセージングサーバの次の受信者（アドレスディレクトリサーバ、他の流通メッセージングサーバ、流通中継サーバなど）に転送する過程でエラーが発生する

２）この時のエラーは、流通メッセージングサーバと受信者間の同期式転送において発生する全てのエラーの場合を指し示す

【０２９９】

３）流通メッセージングサーバは、エラーを認知した時点で流通クライアントのためのエラーメッセージを発生させ、これを流通クライアントに応答メッセージとして伝達する

流通メッセージングサーバが生成するエラーメッセージは下記表６２のような構造で構成される。

【０３００】

【表６２】

【表 62】

項目名		説明	反復回数	類型	長さ
Content		■Root ｴﾘﾒﾝﾄ			
	DocType	■流通ﾒｯｾｰｼﾞの類型 -ｴﾗｰ:9	1..1	Integer	1
	Sender	■要請ﾒｯｾｰｼﾞの受信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
	Receiver	■要請ﾒｯｾｰｼﾞの送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
	RefIdentifier	■要請ﾒｯｾｰｼﾞの固有識別値	1..1	String	36
	Identifier	■UUID 形式で生成したｴﾗｰﾒｯｾｰｼﾞの固有識別値	1..1	String	36
	ErrorCode	■該当ｴﾗｰｺｰﾄﾞ	1..1	Integer	4

【０３０１】

以下、エラー処理方案において非同期式エラー処理方案について説明すれば、次の通りである。

【０３０２】

流通クライアントが流通メッセージングサーバを介して他の流通メッセージングサーバ、アドレスディレクトリサーバ、流通中継サーバと連件する３個体間のメッセージ流通は、連係類型中、流通クライアントユーザが最終受信者の状況に独立に運営できるように非同期式方式の連係を支援したりもする。

【０３０３】

非同期式転送に対する最終エラーは同期式転送とは異なり、転送者が直ちに確認することができないので、流通メッセージングサーバが最終的にエラーを確認した時点で流通クライアントのためのエラーメッセージを発生させ、これを流通クライアントが受信できるようにする。

図４３は非同期式エラー処理方案と関連したプロセスを示し、処理方案は下記の１）～４）の通りである。

【０３０４】

１）流通クライアントが流通メッセージングサーバと連係してメッセージ転送をするステップにおいては転送成功をしたが、流通メッセージングサーバの次の受信者（アドレスディレクトリサーバ、他の流通メッセージングサーバ、流通中継サーバなど）に転送する過程でエラーが発生する

２）この時のエラーは流通メッセージングサーバと受信者間の同期式転送において発生する全てのエラーの場合を指し示す

【０３０５】

３）流通メッセージングサーバは、再試し後、最終的にエラーを認知した時点で流通クライアントのためのエラーメッセージを発生させた後、流通クライアントの受信箱に伝達する

【０３０６】

４）流通クライアントが流通メッセージングサーバに受信メッセージを要請するステップにおいて、自身の受信箱に受信されたエラーメッセージを通じて以前の要請メッセージに対するエラーを認知する

流通メッセージングサーバが生成するエラーメッセージは下記表６３のような構造で構成される。

【０３０７】

【表６３】

【表 63】

項目名		説明	反復回数	類型	長さ
Content		■Root ｴﾘﾒﾝﾄ			
	DocType	■流通ﾒｯｾｰｼﾞの類型 -ｴﾗｰ:9	1..1	Integer	1
	Sender	■要請ﾒｯｾｰｼﾞの受信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
	Receiver	■要請ﾒｯｾｰｼﾞの送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
	RefIdentifier	■要請ﾒｯｾｰｼﾞの固有識別値	1..1	String	36
	Identifier	■UUID 形式で生成したｴﾗｰﾒｯｾｰｼﾞの固有識別値	1..1	String	36
	ErrorCode	■該当ｴﾗｰｺｰﾄﾞ	1..1	Integer	4

【０３０８】

［流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェース］

アドレスディレクトリサーバは、流通体系で最も基本となる公認電子アドレス情報を管理しているシステムであり、電子文書流通において必ず必要なシステムである。

【０３０９】

流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースは、大きく、２つに機能が区分される。第１は登録代行機関との公認電子アドレスの登録などの業務に関するインターフェースであり、第２は流通メッセージングサーバとの物理アドレスの問い合わせ／応答、スパム申告などの業務に関するインターフェースである。

【０３１０】

上記の登録代行機関との公認電子アドレスの登録などの業務に関するインターフェースは別に区分することができるが、登録代行機関を電子文書中継者または第３者保管機関事業者が行うため、流通メッセージングサーバ内にインターフェース機能を挿入した。

但し、送受信個体に設置される流通メッセージングサーバには、公認電子アドレスの登録などと関連した連係インターフェースは入らない。

流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェース機能は下記表６４の通りである。

【０３１１】

【表６４】

【表 64】

ｲﾝﾀｰﾌｪｰｽ区分		ｲﾝﾀｰﾌｪｰｽ説明	備考
ｱﾄﾞﾚｽ管理	公認電子ｱﾄﾞﾚｽの登録(公認送受信者のｱﾄﾞﾚｽを登録する場合)	□電子文書中継者を介して文書を送受信する公認送･受信者の公認電子ｱﾄﾞﾚｽ情報をｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに登録するためのｲﾝﾀｰﾌｪｰｽ □要請した公認電子ｱﾄﾞﾚｽがｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞにおいてunique ではない場合には登録に失敗する	要請者は電子文書中継者である
	公認電子ｱﾄﾞﾚｽ情報の変更	□公認電子ｱﾄﾞﾚｽに対する関連情報(ex:保安情報､ID に対して変更が発生した場合､ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに変更要請した後､その結果を受けるｲﾝﾀｰﾌｪｰｽ	
	公認電子ｱﾄﾞﾚｽの削除	□ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに登録された公認電子ｱﾄﾞﾚｽをこれ以上使わない場合､ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに削除要請をした後､その結果を受けるｲﾝﾀｰﾌｪｰｽ	
ｱﾄﾞﾚｽ検索	物理ｱﾄﾞﾚｽ情報の検索	□ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに公認電子ｱﾄﾞﾚｽ情報に該当するﾕｰｻﾞの保安情報(公認認証書)と物理ｱﾄﾞﾚｽ情報を検索要請した後､その結果を受けるｲﾝﾀｰﾌｪｰｽ	要請者は電子文書中継者と送受信個体である
ﾌﾞﾗｯｸﾘｽﾄの管理	ｽﾊﾟﾑﾒｯｾｰｼﾞ申告	□ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞにｽﾊﾟﾑﾒｯｾｰｼﾞを申告し､受付有無を結果として受けるｲﾝﾀｰﾌｪｰｽ □ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞは､ｽﾊﾟﾑ申告されたﾒｯｾｰｼﾞに対する最終処理結果(ｽﾊﾟﾑﾒｯｾｰｼﾞとして確定したか否か)を申告者およびｽﾊﾟﾑ発送者に " ﾒｯｾｰｼﾞ転送ｲﾝﾀｰﾌｪｰｽ " を使って通知する	
通知	ﾎﾜｲﾄﾘｽﾄ通知	□ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞから送受信個体にﾎﾜｲﾄﾘｽﾄを伝達するｲﾝﾀｰﾌｪｰｽ	
	ﾌﾞﾗｯｸﾘｽﾄ通知	□ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞから送受信個体にﾌﾞﾗｯｸﾘｽﾄを伝達するｲﾝﾀｰﾌｪｰｽ	

【０３１２】
このような流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェースの詳細内容について説明すれば、次の通りである。
【０３１３】
先ず、流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェースにおいて、共通事項について説明すれば、次の１）および２）の通りである。
１）要請メッセージのＭｅｓｓａｇｅＨｅａｄｅｒ拡張
【０３１４】
送信個体の流通メッセージングサーバがアドレスディレクトリサーバに送信する要請メッセージの１番目のＭＩＭＥ　ＰａｒｔのＳＯＡＰメッセージ内には送信個体の電子署名情報が含まれて伝達されるべきであり、アドレスディレクトリサーバがＳＯＡＰメッセージの電子署名に使われた認証書の所有者が該当送信個体と一致するかを検証（ＶＩＤ検証

）するのに必要な追加的な送信個体の情報（ＣｏｒｐＮｕｍ、ＲＶａｌｕｅ）も含まれて伝達されるべきである。

【０３１５】

追加的な送信個体の情報は、要請メッセージのＳＯＡＰメッセージ内のＭｅｓｓａｇｅＨｅａｄｅｒ要素の下位に拡張要素（ａｎｙ　＃＃ｏｔｈｅｒ位置）として位置するべきである。

拡張要素の構造は下記表６５の通りであり、拡張要素の例示は下記表６６の通りである。

【０３１６】

【表６５】

【表 65】

項目名		説明	反復回数	類型	長さ
Extension		■拡張要素ｴﾘﾒﾝﾄ	1..1		
	CorpNum	■中継者あるいは送受信個体の事業者登録番号	1..1	String	10
	RValue	■中継者あるいは送受信個体の公認認証書の個人ｷｰから抽出した RValue ■RValue を Base64 でｴﾝｺｰﾄﾞして入力する	1..1	String	28

【０３１７】

【表６６】

【表 66】

```
<eb:MessageHeader SOAP:mustUnderstand=" 1 " eb:id=" MessageHeader "
eb:version=" 2.0 " >
 <eb:From>
  <eb:PartyId eb:type=" ecf_cd " >123456789</eb:PartyId>
  <eb:Role>sender</eb:Role>
 </eb:From>
 <eb:To>
  <eb:PartyId eb:type=" ecf_cd " >ads</eb:PartyId>
  <eb:Role>receiver</eb:Role>
 </eb:To>
 <eb:CPAId>urn:ads-and-ecm-cpa</eb:CPAId>
 <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
 <eb:Service>>urn:ads-service</eb:Service>
 <eb:Action>request</eb:Action>
 <eb:MessageData>

<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-4049-9fdb-a6c0ed9
af46 7</eb:MessageId>
  <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
  </eb:MessageData>
  <eb:DuplicateElimination></eb:DuplicateElimination>
  <Extention>
   <CorpNum>2208203228</CorpNum>
   <RValue>asdfasdf</RValue>
  </Extention>
</eb:MessageHeader>
```

【０３１８】

２）全体メッセージ構造

流通メッセージングサーバとアドレスディレクトリサーバ間の連係インターフェースは、メッセージの１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージが位置し、２番目の

ＭＩＭＥ　Ｐａｒｔには該当要請および応答に対する流通メッセージが位置する。
流通メッセチンサーバとアドレスディレクトリサーバ間のＳＯＡＰ構造は図４４の通りである。
【０３１９】
以下、流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェースにおいて、公認電子アドレスの登録について説明すれば、次の通りである。
公認電子アドレスの登録処理と関連したメッセージ交換流れは図４５の通りである。
要請流通メッセージの構造は下記表６７の通りであり、メッセージの例題は下記表６８の通りである。
【０３２０】

【表６７】

【表 67】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	RegAddrReq		■公認送受信者の公認電子ｱﾄﾞﾚｽの登録要請ｴﾘﾒﾝﾄ			
		PeerCorpNum	■送受信個体の事業者登録番号	1..1	String	10
		PeerRegNum	■送受信個体の認証番号	0..1	String	10
		Name	■会員名	1..1	String	70
		Type	■会員類型 -個人:U -事業者:C	1..1	String	1
		IDN	■会員識別番号 -個人:住民登録番号 -事業者:事業者登録番号	1..1	String	最小 10 最大 13
		RAddress	■公認電子ｱﾄﾞﾚｽ	1..1	String	最小 1 最大 128
		Cert	■公認認証書	0..1	Base64	-
		Representative	■事業者の場合、代表者名	0..1	String	30
		Addr	■個人または事業者のｱﾄﾞﾚｽ	0..1	String	256
		Tel	■個人または事業者の電話番号(-なしに入力)	0..1	Integer	最小 9 最大 12
		Fax	■個人または事業者のﾌｧｯｸｽ番号	0..1	Integer	最小 9 最大 12
		Mobile	■個人または事業者の携帯電話番号(-なしに入力)	0..1	Integer	最小 10 最大 12
		EMail	■個人または事業者の e-ﾒｰﾙ	0..1	String	256
		RegDate	■公認電子ｱﾄﾞﾚｽの登録日	0..1	Long	-
		EndDate	■公認電子ｱﾄﾞﾚｽの満了日	0..1	Long	-
		ManagerName	■公認電子ｱﾄﾞﾚｽの責任者名	0..1	String	70
		ManagerAddr	■公認電子ｱﾄﾞﾚｽ責任者のｱﾄﾞﾚｽ	0..1	String	256
		ManagerEMail	■公認電子ｱﾄﾞﾚｽ責任者の e-ﾒｰﾙ	0..1	String	256
		ManagerTel	■公認電子ｱﾄﾞﾚｽ責任者の電話番号	0..1	Integer	最小 9 最大 12
		ManagerMobile	■公認電子ｱﾄﾞﾚｽ責任者の携帯電話番号	0..1	Integer	最小 10 最大 12

【０３２１】

【表６８】

【表 68】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
 <RegAddReq>
  <PeerCorpNum>1234567890</PeerCorpNum>
  <PeerRegNum>5555555555</PeerRegNum>
  <Name>洪吉童</Name>
  <Type>U</Type>
  <IDN>1111112222222</IDN>
  <RAddress>#000-0000-0000</RAddress>
  <Cert>MIDJAHjhh46dhkfjsjfsj...</Cert>
  <Addr>ｿｳﾙ市</Addr>
  <Tel>021113333</Tel>
  <Mobile>0101112222</Mobile>
 </RegAddReq>
</Request>
```

応答流通メッセージの構造は下記表６９の通りであり、メッセージの例題は下記表７０の通りである。

【０３２２】

【表６９】

【表 69】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	RegAddrRes		■登録代行機関(電子文書中継者)の会員登録応答ｴﾘﾒﾝﾄ			
		ResultCode	■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(処理結果が失敗(0)の場合にだけ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

【０３２３】

【表７０】

【表 70】

```
<Response xmlns= " http://www.nipa.kr/eDocument_Circulation " >
 <RegAddRes>
  <ResultCode>1</ResultCode>
 </RegAddRes>
</Response>
```

【０３２４】
以下、流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェースにおいて、公認電子アドレス情報の変更インターフェースについて説明すれば、次の通りである。
【０３２５】
公認電子アドレス情報の変更インターフェースは、電子文書中継者がアドレスディレクトリサーバに登録された公認送受信者の公認電子アドレス情報に対する変更を要請して応答を受けるインターフェースであり、変更しようとするユーザ情報および公認電子アドレス情報を要請メッセージに含ませて転送した後、アドレスディレクトリサーバの変更処理の結果を応答メッセージとして受信する。
公認電子アドレス情報の変更処理と関連したメッセージ交換流れは図４６の通りである。
要請流通メッセージの構造は下記表７１の通りであり、メッセージの例題は下記表７２の通りである。
【０３２６】

【表７１】

【表 71】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	ModAddrReq		■公認送受信者の公認電子ｱﾄﾞﾚｽの登録要請ｴﾘﾒﾝﾄ			
		PeerCorpNum	■送受信個体の事業者登録番号	1..1	String	10
		PeerRegNum	■送受信個体の認証番号	0..1	String	10
		Name	■会員名	0..1	String	70
		Type	■会員類型 -個人:U -事業者:C	0..1	String	1
		IDN	■会員識別番号 -個人:住民登録番号 -事業者:事業者登録番号	0..1	String	最小 10 最大 13
		RAddress	■公認電子ｱﾄﾞﾚｽ	1..1	String	最小 1 最大 128
		Cert	■公認認証書	0..1	Base64	-
		Representative	■事業者の場合、代表者名	0..1	String	30
		Addr	■個人または事業者のｱﾄﾞﾚｽ	0..1	String	256
		Tel	■個人または事業者の電話番号(-なしに入力)	0..1	Integer	最小 9 最大 12
		Fax	■個人または事業者のﾌｧｯｸｽ番号	0..1	Integer	最小 9 最大 12
		Mobile	■個人または事業者の携帯電話番号(-なしに入力)	0..1	Integer	最小 10 最大 12
		EMail	■個人または事業者の e-ﾒｰﾙ	0..1	String	256
		RegDate	■公認電子ｱﾄﾞﾚｽの登録日	0..1	Long	-
		EndDate	■公認電子ｱﾄﾞﾚｽの満了日	0..1	Long	-
		ManagerName	■公認電子ｱﾄﾞﾚｽの責任者名	0..1	String	70
		ManagerAddr	■公認電子ｱﾄﾞﾚｽ責任者のｱﾄﾞﾚｽ	0..1	String	256
		ManagerEMail	■公認電子ｱﾄﾞﾚｽ責任者の e-ﾒｰﾙ	0..1	String	256
		ManagerTel	■公認電子ｱﾄﾞﾚｽ責任者の電話番号	0..1	Integer	最小 9 最大 12
		ManagerMobile	■公認電子ｱﾄﾞﾚｽ責任者の携帯電話番号	0..1	Integer	最小 10 最大 12

【０３２７】

【表７２】

【表 72】

```
<Request xmlns=" http://www.nipa.kr/eDocument_Circulation " >
 <ModAddrReq>
  <PeerCorpNum>1234567890</PeerCorpNum>
  <PeerRegNum>5555555555</PeerRegNum>
  <Name>洪吉童</Name>
  <Type>U</Type>
  <IDN>1111112222222</IDN>
  <RAddress>#000-0000-0000</RAddress>
  <Cert>MIDJAHjhh46dhkfjsjfsj...</Cert>
  <Addr>ｿｳﾙ市</Addr>
  <Tel>021113333</Tel>
  <Mobile>0101112222</Mobile>
 </ModAddrReq>
</Request>
```

【０３２８】
応答流通メッセージの構造は下記表７３の通りであり、メッセージの例題は下記表７４の通りである。

【０３２９】

【表７３】

【表 73】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾚﾒﾝﾄ			
	ModAddrRes		■電子文書中継者の会員修正応答ｴﾚﾒﾝﾄ			
		ResultCode	■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(処理結果が失敗(0)の場合にだけ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

【０３３０】
表７３において、ＥｒｒｏｒＣｏｄｅは、ＲｅｓｕｌｔＣｏｄｅが失敗（０）として入力された場合、エラー原因に該当するエラーコードを入力する。

【０３３１】
【表７４】

【表 74】

```
<Response xmlns= " http://www.nipa.kr/eDocument_Circulation " >
 <ModAddrRes>
  <ResultCode>1</ResultCode>
 </ModAddrRes>
</Response>
```

【０３３２】
以下、流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェースにおいて、公認電子アドレスの削除インターフェースについて説明すれば、次の通りである。
【０３３３】
公認電子アドレスの削除インターフェースは、電子文書中継者がアドレスディレクトリサーバに登録された公認送受信者の公認電子アドレス情報の公認電子アドレス情報に対する削除を要請して応答を受けるインターフェースであり、削除しようとするユーザ情報および公認電子アドレス情報を要請メッセージに含ませて転送した後、アドレスディレクトリサーバの削除処理の結果を応答メッセージとして受信する。
公認電子アドレスの削除処理と関連したメッセージ交換流れは図４７の通りである。
要請流通メッセージの構造は下記表７５の通りであり、メッセージの例題は下記表７６の通りである。
【０３３４】
【表７５】

【表 75】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	DelAddrReq		■会員公認電子ｱﾄﾞﾚｽの削除要請ｴﾘﾒﾝﾄ			
		Name	■会員名	1..1	String	最大 70
		IDN	■会員識別番号 -個人:住民登録番号 -事業者:事業者登録番号	1..1	String	最小 10 最大 13
		RAddress	■公認電子ｱﾄﾞﾚｽ	1..1	String	最小 1 最大 128

【０３３５】

【表７６】

【表 76】

```
<Request xmlns=" http://www.nipa.kr/eDocument_Circulation " >
 <DelAddrReq>
  <Name>洪吉童</Name>
  <IDN>1111112222222</IDN>
  <RAddress>#000-0000-0000</RAddress>
 </DelAddrReq>
</Request>
```

【０３３６】

応答流通メッセージの構造は下記表７７の通りであり、メッセージの例題は下記表７８の通りである。

【０３３７】

【表７７】

【表 77】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	DelAddrRes		■電子文書中継者会員削除応答ｴﾘﾒﾝﾄ			
		ResultCode	■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
		RAddress	■公認電子ｱﾄﾞﾚｽ	0..∞	String	最小 1 最大 128
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(処理結果が失敗(0)の場合にだけ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

【０３３８】

表７７において、ＥｒｒｏｒＣｏｄｅは、ＲｅｓｕｌｔＣｏｄｅが失敗（０）として入力された場合、エラー原因に該当するエラーコードを入力。

【０３３９】

【表７８】

【表 78】

```
<Response xmlns= " http://www.nipa.kr/eDocument_Circulation " >
 <DelAddrRes>
  <ResultCode>1</ResultCode>
 </DelAddrRes>
</Response>
```

【０３４０】

以下、流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェースにおいて、物理アドレス情報の検索インターフェースについて説明すれば、次の通りである。

【０３４１】

物理アドレス情報の検索インターフェースは、電子文書中継者または送受信個体がアドレスディレクトリサーバに電子文書受信者の公認電子アドレスに該当する物理アドレス情報とメッセージ保安処理のための公認認証書情報を要請して応答を受けるインターフェースであり、電子文書受信者の公認電子アドレスおよび公認認証書の要請有無を要請メッセージに含ませて転送した後、アドレスディレクトリサーバから電子文書受信者の物理アドレス情報（ＩＰアドレスまたはＤｏｍａｉｎアドレス）および公認認証書情報を応答メッセージとして受信する。

物理アドレス情報の検索処理と関連したメッセージ交換流れは図４８の通りである。

要請流通メッセージの構造は下記表７９の通りであり、メッセージの例題は下記表８０の通りである。

【０３４２】

【表７９】

【表 79】

項目名	説明	反復回数	類型	長さ
Request	■要請 Root ｴﾘﾒﾝﾄ			
SchAddrReq	■公認電子ｱﾄﾞﾚｽの照会要請ｴﾘﾒﾝﾄ			
ReqInfo	■要請公認電子ｱﾄﾞﾚｽの情報ｴﾘﾒﾝﾄ	1..∞		
RAddress	■公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
IsCert	■公認認証書の要請有無 -要請:1 -要請しない:0	1..1	Integer	1

【０３４３】

【表８０】

【表 80】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
 <SchAddrReq>
  <ReqInfo>
   <RAddress>#000-0000-0000</RAddress>
   <IsCert>0</IsCert>
  </ReqInfo>
 </SchAddrReq>
</Request>
```

【０３４４】

応答流通メッセージの構造は下記表８１の通りであり、メッセージの例題は下記表８２の通りである。

【０３４５】

【表８１】

【表 81】

項目名	説明	反復回数	類型	長さ
Response	■応答 Root ｴﾘﾒﾝﾄ			
SchAddrRes	■公認電子ｱﾄﾞﾚｽの照会応答ｴﾘﾒﾝﾄ			
ResultCode	■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
ResultData	■結果目録	0..∞		
RAddress	■公認電子ｱﾄﾞﾚｽ	0..∞	String	最小 1 最大 128
IsExist	■ｱﾄﾞﾚｽ情報の存在有無(Attribute) -存在:1 -未存在:0	1..1	Integer	1
Endpoint	■公認電子ｱﾄﾞﾚｽの物理ｱﾄﾞﾚｽ	0..1	String	最大 256
PeerRegNum	■送受信個体の認証番号	0..1	String	10
Cert	■受信者の公開ｷｰ	0..1	Base64	-
PeerCert	■送受信個体の公開ｷｰ	0..1	Base64	-
ErrorCode	■ｴﾗｰｺｰﾄﾞ(処理結果が失敗(0)の場合にだけ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

【０３４６】

【表８２】

【表 82】

```
<Response xmlns=" http://www.nipa.kr/eDocument_Circulation " >
 <SchAddrRes>
  <ResultCode>1</ResultCode>
  <ResultData>
   <RAddress IsExist=" 1 ">#000-0000-0000</RAddress>
   <Endpoint>http://111.111.111.111:8080/imxs/msh</Endpoint>
   <Cert>MFJIFDjfksdfjsl...</Cert>
  </ResultData>
 </SchAddrRes>
</Response>
```

【０３４７】

以下、流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェースにおいて、スパムメッセージの申告受付インターフェースについて説明すれば、次の通りである。

【０３４８】

スパムメッセージの申告受付インターフェースは、電子文書中継者または送受信個体がアドレスディレクトリサーバにスパムメッセージを申告するインターフェースであり、スパム送信者の公認電子アドレスとスパムメッセージ情報を要請メッセージに含ませて転送した後、アドレスディレクトリサーバからスパム申告の受付有無を応答メッセージとして受信する。アドレスディレクトリサーバは、申告受付されたスパムメッセージに対するスパム有無の判断が完了すれば、流通メッセージングサーバ相互間の連係インターフェースの"メッセージ転送"インターフェースを使って処理結果を通知する。

【０３４９】

スパムメッセージの申告受付処理と関連したメッセージ交換流れは図４９の通りである。

要請流通メッセージの構造は下記表８３の通りであり、メッセージの例題は下記表８４の通りである。

【０３５０】

【表８３】

【表 83】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	ReportSpamReq		■ｽﾊﾟﾑ申告要請ｴﾘﾒﾝﾄ			
		ReportRAdderss	■申告者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		SpamRAdderss	■ｽﾊﾟﾑ送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		ContentsPid	■ｽﾊﾟﾑ送信者が送った Content ﾌｧｲﾙの参照 ID(ｽﾊﾟﾑ申告ﾒｯｾｰｼﾞの MIME Part cid)	1..1	String	最大 256
		AttacheFileInfo	■ｽﾊﾟﾑ送信者が送った添付文書情報	0..*		
		FilePid	■ｽﾊﾟﾑ送信者が送った添付文書の参照 ID(ｽﾊﾟﾑ申告ﾒｯｾｰｼﾞの MIME Part cid)	1..1	String	最大 256
		FileName	■ｽﾊﾟﾑ送信者が送った添付文書の参照名	1..1	String	最大 256
		SpamPeerCorpNum	■ｽﾊﾟﾑﾕｰｻﾞが利用する流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ運営者の事業者番号	1..1	String	最大 10

【０３５１】

【表８４】

【表 84】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
 <ReportSpamReq>
  <ReportRAddress>#000-0000-0000</ReportRAddress>
  <SpamRAddress>#000-0000-0000</SpamRAddress>
  <ContentsPid>cid-1</ContentsPid>
  <AttacheFileInfo>
   <FilePid>cid-2</FilePid>
   <FileName>License.txt</FileName>
  </AttacheFileInfo>
  <SpamPeerCorpNum>1234567890</SpamPeerCorpNum>
 </ReportSpamReq>
</Request>
```

【０３５２】

応答流通メッセージの構造は下記表８５の通りであり、メッセージの例題は下記表８６の

通りである。

【０３５３】

【表８５】

【表 85】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	ReportSpamRes		■ｽﾊﾟﾑ申告応答ｴﾘﾒﾝﾄ			
		ResultCode	■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
		RAddress	■ｽﾊﾟﾑ送信者の公認電子ｱﾄﾞﾚｽ	0..1	String	最小 1 最大 128
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(処理結果が失敗(0)の場合にだけ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

*表 85 において、ResultCode は、ｽﾊﾟﾑ申告ﾒｯｾｰｼﾞに対する単純な受付処理結果であることに注意。

【０３５４】

【表８６】

【表 86】

```
<Response xmlns=" http://www.nipa.kr/eDocument_Circulation " >
 <ReportSpamRes>
  <ResultCode>1</ResultCode>
  <RAddress>#ｽﾊﾟﾏｰ。個人</RAddress>
 </ReportSpamRes>
</Response>
```

【０３５５】

以下、流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェースにおいて、ホワイトリスト通知インターフェースについて説明すれば、次の通りである。

【０３５６】

ホワイトリスト通知インターフェースは、送受信個体にホワイトリスト（流通体系に参加する送受信個体および送受信者の公認電子アドレス目録）を通知するためのインターフェースである。

ホワイトリスト通知と関連したメッセージ交換流れは図５０の通りである。

要請流通メッセージの構造は下記表８７の通りであり、メッセージの例題は下記表８８の通りである。

【０３５７】

【表８７】

【表 87】

項目名				説明	反復回数	類型	長さ
Request				■要請 Root ｴﾘﾒﾝﾄ			
	BroadcastWlistReq			■ﾎﾜｲﾄﾘｽﾄの通知要請ｴﾘﾒﾝﾄ			
		PeerInfo		■送受信個体情報	1..∞		
			Name	■登録者の実名(個人:名前、機関:事業者名)	1..1	String	最大 128
			PeerCorpNum	■所属流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞの運営者の事業者番号	1..1	String	最大 128
			CorpType	■(一般企業:C、ASP 事業者:A)	1..1	String	最大 256
			RAddress	■公認電子ｱﾄﾞﾚｽ	1..∞	String	最小 1 最大 128
			Tel	■電話番号(' - ' なしに入力する)	0..1	Integer	最小 9 最大 12

【０３５８】

【表８８】

【表 88】

```
<Request xmlns=" http://www.nipa.kr/eDocument_Circulation " >
 <BoradcastWlistReq>
  <PeerInfo>
   <Name>洪吉童</Name>
   <PeerCorpNum>22432456</PeerCorpNum>
   <CorpType>C</CorpType>
    <RAddress>#000-0000-0000</RAddress>
  </PeerInfo>
 </BroadcastWlistReq>
</Request>
```

【０３５９】

応答流通メッセージの構造は下記表８９の通りであり、メッセージの例題は下記表９０の通りである。

【０３６０】

【表８９】

【表 89】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	BroadcastWlistRes		■ﾎﾜｲﾄﾘｽﾄ通知応答ｴﾘﾒﾝﾄ			
		ResultCode	■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(処理結果が失敗(0)の場合にだけ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

*表 89 において、ResultCode は、ｽﾊﾟﾑ申告ﾒｯｾｰｼﾞに対する単純な受付処理結果であることに注意。

【０３６１】

【表９０】

【表 90】

```
<Response xmlns= " http://www.nipa.kr/eDocument_Circulation " >
 <BroadcastWlistRes>
  <ResultCode>1</ResultCode>
 </BroadcastWlistRes>
</Response>
```

【０３６２】

以下、流通メッセージングサーバとアドレスディレクトリサーバ間のインターフェースにおいて、ブラックリスト通知インターフェースについて説明すれば、次の通りである。

【０３６３】

ブラックリスト通知インターフェースは、送受信個体にブラックリスト（受信拒否リスト）を通知するためのインターフェースである。通知されたブラックリストは、送受信個体によってブラックリストの管理に使われる。

ブラックリスト通知と関連したメッセージ交換流れは図８４の通りである。

要請流通メッセージの構造は下記表９１の通りであり、メッセージの例題は下記表９２の通りである。

【０３６４】

【表９１】

【表 91】

項目名	説明	反復回数	類型	長さ
Request	■要請 Root ｴﾘﾒﾝﾄ			
BroadcastBlistReq	■ﾌﾞﾗｯｸﾘｽﾄ通知要請ｴﾘﾒﾝﾄ			
UserInfo	■ﾌﾞﾗｯｸﾘｽﾄｴﾘﾒﾝﾄ	1..∞		
SpamPeerCorpNum	■ｽﾊﾟﾑを送信した流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞの運営者の事業者番号	1..1	String	最大 128
Name	■登録者の実名(個人:名前、機関:事業者名)	0..1	String	最大 128
RAddress	■公認電子ｱﾄﾞﾚｽ	1..∞	String	最小 1 最大 128
Tel	■電話番号(' - ' なしに入力する)	0..1	Integer	最小 9 最大 12

【０３６５】

【表９２】

【表 92】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
 <BoradcastBlistReq>
  <UserInfo>
   <SpamPeerCorpNum>32345633</SpamPeerCorpNum>
   <Name>朴ｲﾝｽ</Name>
   <RAddress>#000-0000-0000</RAddress>
  </UserInfo>
 </BroadcastBlistReq>
</Request>
```

【０３６６】

応答流通メッセージの構造は下記表９３の通りであり、メッセージの例題は下記表９４の通りである。

【０３６７】

【表９３】

【表 93】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	BroadcastBlistRes		■ｽﾊﾟﾑ申告応答ｴﾘﾒﾝﾄ			
		ResultCode	■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(処理結果が失敗(0)の場合にだけ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

【０３６８】

【表９４】

【表 94】

```
<Response xmlns= " http://www.nipa.kr/eDocument_Circulation " >
 <BroadcastBlistRes>
  <ResultCode>1</ResultCode>
 </BroadcastBlistRes>
</Response>
```

【０３６９】

［流通メッセージングサーバ相互間の連係インターフェース］

流通メッセージングサーバは、基本的に他の送受信個体または電子文書中継者が構築した流通メッセージングサーバとメッセージ送受信のために連係をしなければならない。

【０３７０】

このような基本機能の他に、流通証明書を第３者保管機関に保管するために第３者保管機関事業者の流通メッセージングサーバと他のメッセージングサーバ間には、流通証明書の伝達連係機能もさらに提供されるべきである。

【０３７１】

流通メッセージングサーバ相互間の連係インターフェースは、メッセージングサーバ相互間のメッセージおよび流通証明書を送受信するためのプロトコルとして、下記表９５のようなインターフェースに区分される。

【０３７２】

【表９５】

【表95】

ｲﾝﾀｰﾌｪｰｽ区分		ｲﾝﾀｰﾌｪｰｽ説明
流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ相互間の連係	ﾒｯｾｰｼﾞ転送	□送信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞが受信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞにﾒｯｾｰｼﾞを転送するためのｲﾝﾀｰﾌｪｰｽ □ﾒｯｾｰｼﾞ受信後、受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、受信証明書またはｴﾗｰﾒｯｾｰｼﾞを応答ﾒｯｾｰｼﾞとして送信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに返す
	流通証明書の伝達	□ﾒｯｾｰｼﾞ受信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞがﾒｯｾｰｼﾞ送信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに閲覧証明書を転送するためのｲﾝﾀｰﾌｪｰｽ □ﾒｯｾｰｼﾞ受信者がﾒｯｾｰｼﾞを閲覧した時、ﾒｯｾｰｼﾞ受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、閲覧証明書をﾒｯｾｰｼﾞ送信ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに送信するべきである □流通証明書を受信した流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、受信確認ACKまたはｴﾗｰﾒｯｾｰｼﾞを応答ﾒｯｾｰｼﾞとして返す
	流通証明書の保管要請	□一般流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞが第3者保管機関事業者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに流通証明書を保管要請するｲﾝﾀｰﾌｪｰｽ □第 3 者保管機関事業者が構築した流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、一般流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞから流通証明書の伝達を受けて、第 3 者保管機関に保管するｻｰﾋﾞｽを必ず構築するべきである □第3者保管機関事業者ではない一般企業/機関/個人の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞにおいては、このｻｰﾋﾞｽは構築対象ではない
	第3者保管機関の保管結果伝達	□第3者保管機関事業者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞが流通証明書/流通文書を保管した後、保管結果(最初登録証明書)を保管要請流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに伝達するｲﾝﾀｰﾌｪｰｽ

【０３７３】

このような流通メッセージングサーバ相互間のインターフェースの詳細内容について説明すれば、次の通りである。

先ず、流通メッセージングサーバ相互間のインターフェースにおいて、共通事項について説明すれば、次の１）の通りである。

１）要請および応答メッセージのＭｅｓｓａｇｅＨｅａｄｅｒ拡張

【０３７４】

流通メッセージングサーバ相互間の連係インターフェースメッセージの１番目のＭＩＭ

Ｅ　Ｐａｒｔであるｓｏａｐメッセージ内には送信者の電子署名情報が含まれて伝達されるべきであり、受信者がｓｏａｐメッセージの電子署名に使われた認証書の所有者が該当送信者と一致するかを検証（ＶＩＤ検証）するのに必要な追加の送信者の情報（ＣｏｒｐＮｕｍ、ＲＶａｌｕｅ）も含まれて伝達されるべきである。

【０３７５】

追加の送信者の情報は、要請および応答メッセージのｓｏａｐメッセージ内のＭｅｓｓａｇｅＨｅａｄｅｒ要素の下位に拡張要素（ａｎｙ　＃＃ｏｔｈｅｒ位置）として位置するべきである。

拡張要素の構造は下記表９６の通りであり、スキーマ構造は下記表９７の通りである。

【０３７６】

【表９６】

【表 96】

項目名		説明	反復回数	類型	長さ
Extension		■拡張要素ｴﾘﾒﾝﾄ	1..1		
	CorpNum	■送信者の事業者登録番号	1..1	String	10
	RValue	■送信者の公認認証書の個人ｷｰから抽出した RValue ■RValue を Base64 でｴﾝｺｰﾄﾞして入力するべきである	1..1	String	28

【０３７７】

【表９７】

【表 97】

```
<eb:MessageHeader SOAP:mustUnderstand=" 1 " eb:id=" MessageHeader "
eb:version=" 2.0 " >
  <eb:From>
    <eb:PartyId eb:type=" ecf_cd " >123456789</eb:PartyId>
    <eb:Role>sender</eb:Role>
  </eb:From>
  <eb:To>
    <eb:PartyId eb:type=" ecf_cd " >567890123</eb:PartyId>
    <eb:Role>receiver</eb:Role>
   </eb:To>
   <eb:CPAId>urn:ecm-and-ecm-cpa</eb:CPAId>
   <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
   <eb:Service>>urn:ecm-service</eb:Service>
   <eb:Action>request</eb:Action>
  <eb:MessageData>

<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-4049-9fdb-a6c0ed9af
46
7</eb:MessageId>
   <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
  </eb:MessageData>
  <eb:DuplicateElimination></eb:DuplicateElimination>
  <Extention>
   <CorpNum>2208203228</CorpNum>
  <RValue>asdfasdf</RValue>
 </Extention>
</eb:MessageHeader>
```

【０３７８】

以下、流通メッセージングサーバ相互間のインターフェースにおいて、メッセージ転送

インターフェースについて説明すれば、次の通りである。
メッセージ転送インターフェースは、流通メッセージングサーバが他の流通メシジングサーバにメッセージを転送する時に使われる。
メッセージ転送において、メッセージ交換流れは図８５の通りである。
【０３７９】
メッセージ交換時の要請フォーマットは図８６の通りであり、図８６のような全体メッセージ構造において、１番目のＭＩＭＥ　ＰａｒｔにはＳＯＡＰメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージ、そしてユーザが添付した文書がある場合には３番目のＭＩＭＥ　Ｐａｒｔから位置する。
要請流通メッセージの構造は下記表９８の通りであり、実際の例示は次の通りである。
【０３８０】
【表９８】

【表 98】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	SendMsgReq		■ﾒｯｾｰｼﾞ転送要請ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -文書:0	1..1	Integer	1
		Title	■ﾒｯｾｰｼﾞの題名	1..1	String	最大 256
		Text	■ﾒｯｾｰｼﾞ本文 -送信者によって受信者の認証書で暗号化できる	0..1	String	-
		Sender	■送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		Receiver	■受信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		ReqConfirm	■閲覧証明書の要請 -未要請:0 -要請:1	1..1	Integer	1
		IsEncrypted	■ﾒｯｾｰｼﾞの暗号化有無 -平文:0 -暗号化文:1	1..1	Integer	1
		Identifier	■本要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36

*表 98 において、文書の伝達目的で本文が必要ない場合には Text の省略が可能

【０３８１】

【表９９】

【表 99】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
    <SendMsgReq>
        <DocType>0</DocType>
        <Title>発送文書</Title>
        <Text>発送文書本文</Text>
        <Sender>#000-0000-0000</Sender>
        <Receiver>#000-0000-0000</Receiver>
        <ReqConfirm>1</ReqConfirm>
        <IsEncrypted>0</IsEncrypted>
        <Identifier>b366ff65-16c8-4d9d-a0ba-d76a2cc95ad2</Identifier>
    </SendMsgReq>
</Request>
```

【０３８２】

メッセージ交換時の応答フォーマットは図８７の通りであり、図８７のような全体メッセージ構造において、１番目のＭＩＭＥ　Ｐａｒｔ にはＳＯＡＰメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには応答流通メッセージ、そして３番目のＭＩＭＥ　Ｐａｒｔには受信証明書が位置する。仮に要請メッセージに対する処理過程でエラーが発生したとすれば、３番目のＭＩＭＥ　Ｐａｒｔは生成しない。

応答流通メッセージの構造は下記表１００の通りであり、実際の例示は下記表１０１の通りである。

【０３８３】

【表１００】

【表 100】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	SendMsgRes		■ﾒｯｾｰｼﾞ転送応答ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -受信証明書:1 -ｴﾗｰ:9	1..1	Integer	1
		RefIdentifier	■本応答流通ﾒｯｾｰｼﾞに対応する要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(流通ﾒｯｾｰｼﾞの類型がｴﾗｰ(9)の場合にだけ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

*表 100 において、DocType がｴﾗｰ(9)の場合は、受信証明書が位置する MIME PArt3 を生成しない。

【０３８４】

【表１０１】

【表 101】

```
<Response xmlns= " http://www.nipa.kr/eDocument_Circulation " >
  <SendMsgRes>
    <DocType>1</DocType>
    <RefIdentifier>b366ff65-16c8-4d9d-a0ba-d76a2cc95ad2</Identifier>
  </SendMsgRes>
</Response>
```

【０３８５】

以下、流通メッセージングサーバ相互間のインターフェースにおいて、流通証明書の伝達インターフェースについて説明すれば、次の通りである。

【０３８６】

流通証明書の伝達インターフェースは、流通メッセージングサーバが他の流通メッセージングサーバに閲覧証明書を転送する時に使われる。また、流通中継サーバが電子文書転送の依頼を受けて受信流通メッセージングサーバに送信した後、応答メッセージとして受信した受信証明書を転送依頼流通メッセージングサーバに転送する時にも使われる。

流通証明書伝達処理と関連したメッセージ交換流れは図８８の通りである。

【０３８７】

流通証明書の伝達要請のフォーマットは図８９の通りであり、図８９のような全体メッセージ構造において、１番目のＭＩＭＥ　ＰａｒｔにはＳＯＡＰメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージ、そして３番目のＭＩＭＥ　Ｐａｒｔには流通証明書が位置する。

要請流通メッセージの構造は下記表１０２の通りであり、実際の例示は下記表１０３の通りである。

【０３８８】
【表１０２】

【表 102】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	SendCertReq		■流通証明書の伝達要請ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -受信証明書:1 -送信証明書:2 -閲覧証明書:3	1..1	Integer	1
		Sender	■証明書の送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		Receiver	■受信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		Identifier	■本要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36
		TargetIdentifier	■証明書発給の対象となるﾒｯｾｰｼﾞ転送要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36

【０３８９】
【表１０３】

【表 103】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
  <SendCertReq>
    <DocType>1</DocType>
    <Sender>#000-0000-0000</Sender>
    <Receiver>#000-0000-0000</Receiver>
    <Identifier>5347146a-3528-4469-8ef7-9c346ab36d54</Identifier>
    <TargetIdentifier>b366ff65-16c8-4d9d-a0ba-d76a2cc95ad2</TargetIdentifier>
  </SendCertReq>
</Request>
```

【０３９０】
流通証明書の伝達応答のフォーマットは図９０、図９１（図９０は成功の場合、図９１はエラーの場合）の通りであり、図９０、図９１のような全体メッセージ構造において、要請メッセージに対する処理が成功である場合、１番目のＭＩＭＥ　Ｐａｒｔに受信確認Ａ

ｃｋｎｏｗｌｅｄｇｅｍｅｎｔ　ＳＯＡＰメッセージだけが位置し、エラーの場合は、１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔにはエラー応答流通メッセージが位置する。

応答流通メッセージの構造は下記表１０４の通りであり、表１０４は処理結果がエラーの場合にだけ該当される。

【０３９１】

【表１０４】

【表 104】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	SendCertRes		■流通証明書の伝達応答ｴﾘﾒﾝﾄ			
		DocType	■転送ﾒｯｾｰｼﾞの類型 -ｴﾗｰ:9	1..1	Integer	1
		RefIdentifier	■本応答流通ﾒｯｾｰｼﾞに対応する要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36
		ErrorCode	■ｴﾗｰｺｰﾄﾞ	1..1	String	256

【０３９２】

以下、流通メッセージングサーバ相互間のインターフェースにおいて、流通証明書の保管要請インターフェースについて説明すれば、次の通りである。

【０３９３】

流通証明書の保管要請インターフェースは、送受信個体の流通メッセージングサーバが流通証明書を第３者保管機関に保管するために、第３者保管機関事業者の流通メッセージングサーバに流通証明書に対する保管要請をする時に使われる。本インターフェース上の応答メッセージには受信確認情報だけが含まれ、流通証明書を第３者保管機関に保管した結果として発給を受けた最初登録証明書は、後述する"第３者保管機関の保管結果の伝達インターフェース"を使って保管要請流通メッセージングサーバに伝達する。

流通証明書の保管要請処理と関連したメッセージ交換流れは図９２の通りである。

【０３９４】

流通証明書の保管要請のフォーマットは図９３の通りであり、図９３のような全体メッセージ構造において、１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージ、そして３番目のＭＩＭＥ　Ｐａｒｔには流通証明書が位置する。

要請流通メッセージの構造は下記表１０５の通りであり、実際の例示は下記表１０６の通りである。

【０３９５】

【表１０５】

【表 105】

項目名	説明	反復回数	類型	長さ
Request	■要請 Root ｴﾘﾒﾝﾄ			
RegCertReq	■流通証明書の保管要請ｴﾘﾒﾝﾄ			
DocType	■流通ﾒｯｾｰｼﾞの類型 -受信証明書:1 -送信証明書:2 -閲覧証明書:3	1..1	Integer	1
Sender	■送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
Receiver	■受信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
Identifier	■本要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36

【０３９６】

【表１０６】

【表106】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
  <RegCertReq>
    <DocType>1</DocType>
    <Sender>#000-0000-0000</Sender>
    <Receiver>#000-0000-0000</Receiver>
    <Identifier>5347146a-3528-4469-8ef7-9c346ab36d54</Identifier>
  </RegCertReq>
</Request>
```

【０３９７】

流通証明書の保管応答のフォーマットは、図９４，図９５（図９４は成功の場合、図９５はエラーの場合）の通りであり、図９４，図９５のような同じ全体メッセージ構造において、要請メッセージに対する処理が成功の場合、１番目のＭＩＭＥ　Ｐａｒｔに受信確認Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ　ＳＯＡＰメッセージだけが位置し、エラーの場合は、１番目のＭＩＭＥ　ＰａｒｔにはＳＯＡＰメッセージ、２番目のＭＩＭＥ　Ｐａｒｔにはエラー応答流通メッセージが位置する。

応答流通メッセージの構造は下記表１０７の通りであり、表１０７は処理結果がエラーの場合だけに該当される。

【０３９８】

【表１０７】

【表 107】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	RegCertRes		■流通証明書の保管応答ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -ｴﾗｰ:9	1..1	Integer	1
		RefIdentifier	■本応答流通ﾒｯｾｰｼﾞに対応する要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36
		ErrorCode	■ｴﾗｰｺｰﾄﾞ	1..1	String	256

【０３９９】

以下、流通メッセージングサーバ相互間のインターフェースにおいて、第３者保管機関の保管結果の伝達インターフェースについて説明すれば、次の通りである。

【０４００】

第３者保管機関の保管結果の伝達インターフェースは、第３者保管機関事業者の流通メッセージングサーバが第３者保管機関に流通証明書を保管した後、該当結果として受信した最初登録証明書を、流通証明書の保管を要請した流通メッセージングサーバに送信する時に使われる。

第３者保管機関の保管結果の伝達処理と関連したメッセージ交換流れは図６１の通りである。

【０４０１】

第３者保管機関の保管結果伝達のフォーマットは図６２の通りであり、図６２のような全体メッセージ構造において、１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージ、そして３番目のＭＩＭＥ　Ｐａｒｔには最初登録証明書が位置する。仮に流通証明書を第３者保管機関に保管する過程でエラーが発生したとすれば、３番目のＭＩＭＥ　Ｐａｒｔは生成しない。

要請流通メッセージの構造は下記表１０８の通りであり、実際の例示は下記表１０９の通りである。

【０４０２】

【表１０８】

【表 108】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	RegResultReq		■第 3 者保管機関の保管結果の伝達処理要請ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -最初登録証明書:4 -ｴﾗｰ:9	1..1	Integer	1
		Sender	■送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		Receiver	■受信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		Identifier	■本要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	0..1	String	最大 128
		TargetIdentifier	■本要請流通ﾒｯｾｰｼﾞの対象となる流通証明書の保管要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	最大 128
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(流通ﾒｯｾｰｼﾞの類型がｴﾗｰ(9)の場合にだけ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	最大 256

*表 108 において、DocType がｴﾗｰ(9)の場合は、最初登録証明書が位置する MIME Part3 を生成しない

【０４０３】

【表１０９】

【表 109】

```
-- 成功
<Requuest xmlns= " http://www.nipa.kr/eDocument_Circulation " >
   <ReqResultReq>
      <DocType>4</DocType>
      <Sender>#000-0000-0000</Sender>
      <Receiver>#000-0000-0000</Receiver>
      <Identifier>dd27e2e2-4731-4da1-8043-a250dcc8690c</Identifier>
      <TargetIdentifier>5347146a-3528-4469-8ef7-9c346ab36d54</RefIdentifier>
   </regResultReq>
</Request>

-- エラー

<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
   <RegResultReq>
      <DocType>9</DocType>
      <Sender>#000-0000-0000</Sender>
      <Receiver>#000-0000-0000</Receiver>
      <TargetIdentifier>5347146a-3528-4469-8ef7-9c346ab36d54</RefIdentifier>
      <ErrorCode>ERR-01-0001</ErrorCode>
   </RegResultReq>
</Request>
```

【０４０４】

第３者保管機関の保管結果応答のフォーマットは図９８、図９９（図９８は成功の場合、図９９はエラーの場合）の通りであり、図９８、図９９のような全体メッセージ構造において、要請メッセージに対する処理が成功である場合は、１番目のＭＩＭＥ　Ｐａｒｔに受信確認Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ　ＳＯＡＰメッセージだけが位置し、エラーの場合は、１番目のＭＩＭＥ　ＰａｒｔにはＳＯＡＰメッセージ、２番目のＭＩＭＥ　Ｐａｒｔにはエラー応答流通メッセージが位置する。

応答流通メッセージの構造は下記表１１０の通りであり、表１１０は処理結果がエラーの場合だけに該当される。

【０４０５】

【表１１０】

【表 110】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	RegResultRes		■第 3 者保管機関の保管結果の伝達処理結果ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -ｴﾗｰ:9	1..1	Integer	1
		RefIdentifier	■本応答流通ﾒｯｾｰｼﾞに対応する要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36
		ErrorCode	■ｴﾗｰｺｰﾄﾞ	1..1	String	256

【０４０６】

［流通クライアントと流通メッセージングサーバ間の連係インターフェース］

流通メッセージングサーバは、実際に電子文書流通を要請するユーザ（内部送受信者または公認送受信者）のためのシステム（流通クライアント）と連係して、ユーザに文書送受信の基本機能を提供しなければならない。

【０４０７】

流通クライアントと流通メッセージングサーバ間の連係インターフェースは、流通クライアントが電子文書を送信し受信するために、一次的に流通メッセージングサーバと通信するためのプロトコルとして、下記表１１１のようなインターフェースに区分される。

【０４０８】

【表１１１】

【表 111】

ｲﾝﾀｰﾌｪｰｽ区分		ｲﾝﾀｰﾌｪｰｽ説明
流通ｸﾗｲｱﾝﾄと流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ間の連係ｲﾝﾀｰﾌｪｰｽ	ﾒｯｾｰｼﾞ転送の要請	□流通ｸﾗｲｱﾝﾄが流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞにﾒｯｾｰｼﾞ転送を要請するためのｲﾝﾀｰﾌｪｰｽ
	ﾒｯｾｰｼﾞ目録の要請	□流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに受信された受信ﾒｯｾｰｼﾞの目録を要請するためのｲﾝﾀｰﾌｪｰｽ □流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、流通ｸﾗｲｱﾝﾄﾕｰｻﾞを認証した後、該当ﾕｰｻﾞに受信されたﾒｯｾｰｼﾞ目録を伝達する
	ﾒｯｾｰｼﾞ詳細情報の要請	□流通ｸﾗｲｱﾝﾄが流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞにﾕｰｻﾞに受信された特定ﾒｯｾｰｼﾞの全体情報を要請するためのｲﾝﾀｰﾌｪｰｽ □流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、流通ｸﾗｲｱﾝﾄﾕｰｻﾞを認証した後、該当ﾕｰｻﾞが要請したﾒｯｾｰｼﾞの全体情報を伝達する
	ｽﾊﾟﾑﾒｯｾｰｼﾞ申告	□流通ｸﾗｲｱﾝﾄがｽﾊﾟﾑﾒｯｾｰｼﾞを申告するためのｲﾝﾀｰﾌｪｰｽ □流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、流通ｸﾗｲｱﾝﾄﾕｰｻﾞを認証した後、該当ﾕｰｻﾞが申告した内容をｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに伝達する
	物理ｱﾄﾞﾚｽ情報の検索	□流通ｸﾗｲｱﾝﾄが物理ｱﾄﾞﾚｽ情報を検索するためのｲﾝﾀｰﾌｪｰｽ □流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞは、流通ｸﾗｲｱﾝﾄﾕｰｻﾞを認証した後、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに検索要請後、結果を伝達する

【０４０９】

流通クライアントと流通メッセージングサーバ間の連係インターフェースの詳細内容を説明すれば、次の通りである。

先ず、流通クライアントと流通メッセージングサーバ間の連係インターフェースの共通事項について説明すれば、次の１）の通りである。

１）要請メッセージのＭｅｓｓａｇｅＨｅａｄｅｒ拡張

【０４１０】

流通クライアントが流通メッセージングサーバに送信する要請メッセージの１番目のＭＩＭＥ　Ｐａｒｔであるｓｏａｐメッセージ内にはユーザの電子署名情報が含まれて伝達されるべきであり、流通メッセージングサーバがｓｏａｐメッセージの電子署名に使われた認証書の所有者が該当ユーザと一致するかを検証（ＶＩＤ検証）するのに必要な追加のユーザの情報（ＩＤＮ、ＲＶａｌｕｅ）も含まれて伝達されるべきである。

【０４１１】

該当情報は、要請メッセージのｓｏａｐメッセージ内のＭｅｓｓａｇｅＨｅａｄｅｒ要素の下位に拡張要素（ａｎｙ　＃＃ｏｔｈｅｒ位置）として位置するべきである。

また、同一認証書を使う複数の内部ユーザに対する個別の認証情報が追加されてもよい。

拡張要素の構造は下記表１１２の通りであり、拡張要素の例示は下記表１１３の通りで

ある。

【０４１２】

【表１１２】

【表 112】

項目名		説明	反復回数	類型	長さ
UserInfo		■拡張要素ｴﾘﾒﾝﾄ	1..1		
	IDN	■ﾕｰｻﾞ識別番号 -個人:住民登録番号 -事業者:事業者登録番号	1..1	String	10
	RValue	■ﾕｰｻﾞの公認認証書の個人ｷｰから抽出したRValue ■RValue を Base64 でｴﾝｺｰﾄﾞして入力する	1..1	String	28
	Id	■流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに登録されたﾕｰｻﾞ ID	0..1	String	最大 20
	Password	■流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに登録されたﾕｰｻﾞﾊﾟｽﾜｰﾄﾞ	0..1	String	8
	AuthType	■複数の内部ﾕｰｻﾞの認証方式 ■ID、ﾊﾟｽﾜｰﾄﾞ方式は基本的に 0 に設定 ■ID、ﾊﾟｽﾜｰﾄﾞ方式以外の方式でﾕｰｻﾞを認証しようとする場合、AuthType 値および下の拡張要素を自体的に定義して使用	1..1	Integer	1
	Any Extension	■ID、ﾊﾟｽﾜｰﾄﾞ方式以外の方式でﾕｰｻﾞを認証しようとする場合、新しい要素を自体的に定義して使用 ■ex>Token、Certificate	0..1	Any	-

【０４１３】

【表１１３】

【表 113】

```
<eb:MessageHeader SOAP:mustUnderstand=" 1 " eb:id=" MessageHeader "
eb:version=" 2.0 " >
 <eb:From>
  <eb:PartyId eb:type=" urn:oasis:names:tc:ebxml-cppa:partyid-type:duns " >openAPI
_Sender</eb:PartyId>
  <eb:Role>http://www.rosettanet.org/processes/3A4.xml#Buyer</eb:Role>
 </eb:From>
 <eb:To>
 <eb:PartyId eb:type=" urn:oasis:names:tc:ebxml-cppa:partyid-type:duns " >openAPI_
Receiver</eb:PartyId>
  <eb:Role>http://www.rosettanet.org/processes/3A4.xml#seller</eb:Role>
 </eb:To>
 <eb:CPAId>uri:openapi-and-openapi-cpa_mxs</eb:CPAId>

<eb:ConversationId>uri:openapi-and-openapi-cpa_mxs:0210050643</eb:ConversationId
>
 <eb:Service>bpid:icann:rosettanet.org:3A4$2.0</eb:Service>
 <eb:Action>RequestRelaySend</eb:Action>
 <eb:MessageData>

<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-4049-9fdb-a6c0ed9
af
467</eb:MessageId>
  <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
 </eb:MessageData>
 <eb:DuplicateElimination></eb:DuplicateElimination>
 <UserInfo>
  <IDN>2208203228</CorpNum>
  <RValue>asdfasdf</RValue>
  <Id>tester1</Id>
  <Password>test</Password>
  <AuthType>0</AuthType>
 </UserInfo>
</eb:MessageHeader>
```

【０４１４】

以下、流通クライアントと流通メッセージングサーバ間の連係インターフェースにおい

て、メッセージ転送要請インターフェースについて説明すれば、次の通りである。

【０４１５】

メッセージ転送要請インターフェースは、流通クライアントが流通メッセージングサーバを介してメッセージを転送するために流通メッセージングサーバにメッセージを転送する時に使われる。

流通クライアントのメッセージ転送処理の流れは図１００の通りである。

【０４１６】

流通クライアントのメッセージ転送要請のフォーマットは図１０１の通りであり、図１０１のような全体メッセージ構造において、１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージが位置する。そして、ユーザが添付した文書がある場合、３番目のＭＩＭＥ　Ｐａｒｔから位置する。

要請流通メッセージの構造は下記表１１４の通りであり、実際の例示は下記表１１５の通りである。

【０４１７】

【表１１４】

【表 114】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	SendMsgReq		■ﾒｯｾｰｼﾞ転送要請ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -文書:0	1..1	Integer	1
		Title	■ﾒｯｾｰｼﾞの題名	1..1	String	最大 256
		Text	■ﾒｯｾｰｼﾞ本文 -送信者によって､受信者の認証書で暗号化できる	0..1	String	-
		Sender	■送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		Receiver	■受信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		ReqConfirm	■閲覧証明書の要請 -未要請:0 -要請:1	1..1	Integer	1
		IsEncrypted	■ﾒｯｾｰｼﾞの暗号化有無 -平文:0 -暗号化文:1	1..1	Integer	1
		Identifier	■本要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36

*表 114 において､文書の伝達目的で本文が必要ない場合､Text は省略可能である。

【０４１８】
【表１１５】

【表 115】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
    <SendMsgReq>
        <DocType>0</DocType>
        <Title>発送文書</Title>
        <Text>発送文書本文</Text>
        <Sender>#000-0000-0000</Sender>
        <Receiver>#000-0000-0000</Receiver>
        <ReqConfirm>1</ReqConfirm>          <IsEncrypted>1</IsEncrypted>
        <Identifier>b366ff65-16c8-4d9d-a0ba-d76a2cc95ad2</Identifier>
     </SendMsgReq>
</Request>
```

【０４１９】
流通クライアントのメッセージ転送応答のフォーマットは図１０２、図１０３（図１０２は成功の場合、図１０３はエラーの場合）の通りであり、図１０２、図１０３のような全体メッセージ構造において、要請メッセージに対する処理が成功の場合は、１番目のＭＩＭＥ　Ｐａｒｔに受信確認Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ　ＳＯＡＰメッセージだけが位置し、エラーの場合は、１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔにはエラー応答流通メッセージが位置する。
応答流通メッセージの構造は表１１６の通りであり、表１１６は処理結果がエラーの場合にだけ該当される。
【表１１６】

【表 116】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	SendMsgRes		■ﾒｯｾｰｼﾞ転送応答ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -ｴﾗｰ:9	1..1	Integer	1
		RefIdentifier	■本応答流通ﾒｯｾｰｼﾞに対応する要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36
		ErrorCode	■ｴﾗｰｺｰﾄﾞ	1..1	String	256

【０４２０】
以下、流通クライアントと流通メッセージングサーバ間の連係インターフェースにおい

て、メッセージ目録要請インターフェースについて説明すれば、次の通りである。
メッセージ目録要請インターフェースは、流通クライアントが流通メッセージングサーバに受信されたメッセージ目録を要請する時に使われる。
流通クライアントのメッセージ目録処理の流れは図１０４の通りである。
【０４２１】
流通クライアントのメッセージ目録要請のフォーマットは図１０５の通りであり、図１０５のような全体メッセージ構造において１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージが位置する。
要請流通メッセージの構造は下記表１１７の通りであり、実際の例示は下記表１１８の通りである。
【０４２２】
【表１１７】

【表 117】

項目名			説明	反復 回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	MsgListReq		■ﾒｯｾｰｼﾞ 目録要請ｴﾘﾒﾝﾄ			
		Requester	■要請者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		MsgSize	■流通ﾒｯｾｰｼﾞ 目録の個数	1..1	Integer	最大 100

【０４２３】
【表１１８】

【表 118】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
  <MsgListReq>
    <Requester>#000-0000-0000</Requester>
    <MsgSize>100</MsgSize>
  </MsgListReq>
</Request>
```

【０４２４】
流通クライアントのメッセージ目録応答のフォーマットは表６７の通りであり、表６７のような全体メッセージ構造において、１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには応答流通メッセージ（流通メッセージングサーバに受信された流通メッセージ目録）が位置する。
応答流通メッセージの構造は下記表１１９の通りであり、実際の例示は下記表１２０の通りである。
【０４２５】

【表１１９】

【表 119】

項目名				説明	反復回数	類型	長さ
Response				■応答 Root ｴﾘﾒﾝﾄ			
	MsgListRes			■ﾒｯｾｰｼﾞ目録応答ｴﾘﾒﾝﾄ			
		ResultCode		■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
		ErrorCode		■ｴﾗｰｺｰﾄﾞ(ResultCode が失敗(0)の場合にのみ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	Integer	1
		List		■受信流通ﾒｯｾｰｼﾞﾘｽﾄ	0..∞		
			DocType	■流通ﾒｯｾｰｼﾞの類型 -文書:0 -受信証明書:1 -発信証明書:2 -閲覧証明書:3 -保管証明書:4 -ｴﾗｰ:9	1..1	Integer	最大 100
			Title	■ﾒｯｾｰｼﾞの題名	0..1	String	最大 256
			Sender	■送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
			Identifier	■流通ﾒｯｾｰｼﾞの固有識別値(UUID)	0..1	String	36
			TargetIdentifier	■流通ﾒｯｾｰｼﾞの類型が流通証明書である場合、証明書の発給対象となる流通ﾒｯｾｰｼﾞの固有識別値(UUID)	0..1	String	36
			IsExistPayloads	■添付ﾌｧｲﾙの存在有無 -ない:0 -ある:1	1..1	Integer	1
			IsEncrypted	■ﾒｯｾｰｼﾞの暗号化有無 -平文:0 -暗号化文:1	1..1	Integer	1
			SendDate	■文書送信時間	0..1	Long	-
			ReceiveDate	■文書受信時間	0..1	Long	-

【０４２６】

【表１２０】

【表 120】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
  <MsgListRes>
    <ResultCode>1</ResultCode>
    <List>
      <DocType>0</DocType>
      <Title>文書の題名</Title>
      <Sender>#000-0000-0000</Sender>
      <Identifier>e82fae92-981e-4d36-80b8-ec16cb6b7993</Identifier>
      <IsExistPayloads>0</IsExistPayloads>
      <IsEncrypted>0</IsEncrypted>
      <SendDate>1286263498929</SendDate>
      <ReceiveDate>1286273498929</ReceiveDate>
    </List>
    <List>
      <DocType>9</DocType>
      <Sender>#000-0000-0000</Sender>
      <RefIdentifier>e82fae92-981e-4d36-80b8-ec16cb6b7993</RefIdentifier>
      <IsExistPayloads>0</IsExistPayloads>
      <IsEncrypted>0</IsEncrypted>
    </List>
  </MsgListRes>
</Response>
```

【０４２７】
以下、流通クライアントと流通メッセージングサーバ間の連係インターフェースにおいて、メッセージ詳細情報の要請インターフェースについて説明すれば、次の通りである。
【０４２８】
メッセージ詳細情報の要請インターフェースは、流通クライアントが流通メッセージングサーバに受信された特定メッセージと添付文書を要請する時に使われる。
流通クライアントの詳細情報の要請処理流れは図１０７の通りである。
【０４２９】
流通クライアントのメッセージ詳細情報要請のフォーマットは図１０８の通りであり、図１０８のような全体メッセージ構造において、１番目のＭＩＭＥ　ＰａｒｔにはＳＯＡ

Ｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージ本文が位置する。
　要請流通メッセージの構造は下記表１２１の通りであり、実際の例示は下記表１２２の通りである。
【０４３０】
【表１２１】

【表 121】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	MsgDetailReq		■ﾒｯｾｰｼﾞ詳細情報要請ｴﾘﾒﾝﾄ			
		Requester	■要請者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		RefIdentifier	■要請対象流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36

【０４３１】
【表１２２】

【表 122】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
   <MsgDetailReq>
      <Requester>#000-0000-0000</Requester>
      <RefIdentifier>5f6d8126-a691-452b-b17a-e3a8b8ce3ac5</RefIdentifier>
   </MsgDetailReq>
</Request>
```

【０４３２】
流通クライアントのメッセージ詳細情報応答のフォーマットは図１０９の通りであり、図１０９のような全体メッセージ構造において、１番目のＭＩＭＥ　ＰａｒｔにはＳＯＡＰメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには応答流通メッセージ（流通メッセージの詳細情報）、そして添付文書がある場合、３番目のＭＩＭＥ　Ｐａｒｔから順に位置する。
　応答流通メッセージの構造は下記表１２３の通りであり、実際の例示は下記表１２４の通りである。
【０４３３】

【表１２３】

【表 123】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	MsgDetailRes		■ﾒｯｾｰｼﾞ詳細情報応答ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -文書:0 -受信、発送、閲覧証明書:1、2、3 -保管証明書:4 -ｴﾗｰ:9	1..1	Integer	最大 100
		Title	■ﾒｯｾｰｼﾞの題名	0..1	String	最大 256
		Text	■ﾒｯｾｰｼﾞ本文	0..1	String	-
		Sender	■発送者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		Receiver	■受信者の公認電子ｱﾄﾞﾚｽ	0..1	String	最大 128
		ReqConfirm	■閲覧証明書の要請 -未要請:0 -要請:1	0..1	Integer	1
		IsEncrypted	■ﾒｯｾｰｼﾞの暗号化有無 -平文:0 -暗号化文:1	1..1	Integer	1
		Identifier	■流通ﾒｯｾｰｼﾞの固有識別値(UUID)	0..1	String	36
		TargetIdentifier	■流通ﾒｯｾｰｼﾞの類型が流通証明書である場合、証明書の発給対象となる流通ﾒｯｾｰｼﾞの固有識別値(UUID)	0..1	String	36
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(流通ﾒｯｾｰｼﾞの類型がｴﾗｰ(9)の場合にのみ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	Integer	1

【０４３４】

【表１２４】

【表 124】

```
<Response xmlns=" http://www.nipa.kr/eDocument_Circulation " >
  <MsgDetailRes>
    <DocType>0</DocType>
    <Title>文書の題名</Title>      <Text>文書本文</Text>
    <Sender>#000-0000-0000</Sender>
    <Receiver>#000-0000-0000</Receiver>
    <ReqConfirm>1</ReqConfirm>
    <IsEncrypted>0</IsEncrypted>
    <Identifier>e82fae92-981e-4d36-80b8-ec16cb6b7993</Identifier>
  </MsgDetailRes>
</Content>
```

【０４３５】

以下、流通クライアントと流通メッセージングサーバ間の連係インターフェースにおいて、スパムメッセージ申告インターフェースについて説明すれば、次の通りである。

【０４３６】

スパムメッセージ申告インターフェースは、流通クライアントが流通メッセージングサーバにスパムメッセージを申告する時に使われる。流通メッセージングサーバは、アドレスディレクトリサーバにスパムメッセージを申告後、結果を流通クライアントに伝達する。

流通クライアントのスパムメッセージ申告処理の流れは図１１０の通りである。

【０４３７】

流通クライアントのスパムメッセージ申告のフォーマットは図１１１の通りであり、図１１１のような全体メッセージ構造において１番目のＭＩＭＥ　ＰａｒｔにはＳＯＡＰメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージが位置する。

要請流通メッセージの構造は下記表１２５の通りであり、メッセージの例題は下記表１２６の通りである。

【０４３８】

【表１２５】

【表 125】

項目名	説明	反復回数	類型	長さ
Request	■要請 Root ｴﾘﾒﾝﾄ			
ReportSpamReq	■ｽﾊﾟﾑ申告要請ｴﾘﾒﾝﾄ			
ReportRAdderss	■申告者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
SpamRAdderss	■ｽﾊﾟﾑ送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
ContentsPid	■ｽﾊﾟﾑ送信者が送った Content ﾌｧｲﾙの参照 ID(ｽﾊﾟﾑ申告ﾒｯｾｰｼﾞの MIME Part cid)	1..1	String	最大 256
AttacheFileInfo	■ｽﾊﾟﾑ送信者が送った添付文書情報			
FilePid	■ｽﾊﾟﾑ送信者が送った添付文書の参照 ID(ｽﾊﾟﾑ申告ﾒｯｾｰｼﾞの MIME Part cid)	1..1	String	最大 256

【０４３９】
【表１２６】

【表 126】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
  <ReportSpamReq>
    <ReportRAddress>#000-0000-0000</ReportRAddress>
    <SpamRAddress>#000-0000-0000</SpamRAddress>
    <ContentsPid>cid-1</ContentsPid>
    <AttacheFileInfo>
      <FilePid>cid-2</FilePid>
      <FileName>License.txt</FileName>
    </AttacheFileInfo>
    <SpamPeerCorpNum>1234567890</SpamPeerCorpNum>
  </ReportSpamReq>
</Request>
```

【０４４０】
流通クライアントのスパムメッセージ応答のフォーマットは図１１２の通りであり、図１１２のような全体メッセージ構造において、１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには応答流通メッセージ（流通メッセージングサーバに受信された流通メッセージ目録）が位置する。
応答流通メッセージの構造は下記表１２７の通りであり、メッセージの例題は下記表１

２８の通りである。

【０４４１】

【表１２７】

【表 127】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾚﾒﾝﾄ			
	ReportSpamRes		■ｽﾊﾟﾑ申告応答ｴﾚﾒﾝﾄ	1..1		
		ResultCode	■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
		RAddress	■ｽﾊﾟﾑ送信者の公認電子ｱﾄﾞﾚｽ	0..1	String	最小 1 最大 128
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(処理結果が失敗(0)の場合にのみ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

*表 127 において、ResultCode は、ｽﾊﾟﾑ申告ﾒｯｾｰｼﾞに対する単純な受付処理結果であることに注意。

【０４４２】

【表１２８】

【表 128】

```
<Response xmlns= " http://www.nipa.kr/eDocument_Circulation " >
  <ReportSpamRes>
    <ResultCode>1</ResultCode>
    <RAddress>#000-0000-0000</RAddress>
  </ReportSpamRes>
</Response>
```

【０４４３】

以下、流通クライアントと流通メッセージングサーバ間の連係インターフェースにおいて、物理アドレス検索インターフェースについて説明すれば、次の通りである。

【０４４４】

物理アドレス検索インターフェースは、流通クライアントが流通メッセージングサーバに物理アドレス検索を要請する時に使う。流通メッセージングサーバは、アドレスディレクトリサーバに物理アドレスを検索後、結果を伝達する。

物理アドレス検索処理と関連し、メッセージ交換の流れは図１１３の通りである。

【０４４５】

物理アドレス検索要請メッセージのフォーマットは図１１４の通りであり、図１１４のような全体メッセージ構造において、１番目のＭＩＭＥ　ＰａｒｔにはＳＯＡＰメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージが位置する。

要請流通メッセージの構造は下記表１２９の通りであり、メッセージの例題は下記表１３０の通りである。

【０４４６】

【表１２９】

【表 129】

項目名	説明	反復回数	類型	長さ
Request	■要請 Root ｴﾘﾒﾝﾄ			
SchAddrReq	■会員公認電子ｱﾄﾞﾚｽ照会要請ｴﾘﾒﾝﾄ			
ReqInfo	■要請公認電子ｱﾄﾞﾚｽ情報ｴﾘﾒﾝﾄ	1..∞		
RAddress	■公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
IsCert	■公認認証書の要請有無 -要請:1 -要請しない:0	1..1	Integer	1

【０４４７】

【表１３０】

【表 130】

```
<Request xmlns=" http://www.nipa.kr/eDocument_Circulation " >
  <SchAddrReq>
    <ReqInfo>
      <RAddress>#000-0000-0000</RAddress>
      <IsCert>0</IsCert>
    </ReqInfo>
  </SchAddrReq>
</Request>
```

【０４４８】

物理アドレスの検索応答メッセージのフォーマットは図１１５の通りであり、図１１５のような全体メッセージ構造において、１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには応答流通メッセージ（流通メッセージングサーバに受信された流通メッセージ目録）が位置する。

応答流通メッセージの構造は下記表１３１の通りであり、実際の例示は下記表１３２の通りである。

【０４４９】

【表１３１】

【表 131】

項目名	説明	反復回数	類型	長さ
Response	■応答 Root ｴﾘﾒﾝﾄ			
SchAddrRes	■公認電子ｱﾄﾞﾚｽ照会応答ｴﾘﾒﾝﾄ			
ResultCode	■処理結果 -成功:1 -失敗:0	1..1	Boolean	-
ResultData	■結果目録	0..∞		
RAddress	■公認電子ｱﾄﾞﾚｽ	1..1	String	最小 1 最大 128
IsExist	■ｱﾄﾞﾚｽ情報の存在有無(Attribute) -存在:1 -未存在:0	1..1	Integer	1
Endpoint	■公認電子ｱﾄﾞﾚｽの物理ｱﾄﾞﾚｽ	0..1	String	最大 256
PeerRegNum	■送受信個体の認証番号	0..1	String	10
Cert	■受信者の公認認証書	0..1	Base64	-
PeerCert	■送受信個体の公開ｷｰ	0..1	Base64	-
ErrorCode	■ｴﾗｰｺｰﾄﾞ(処理結果が失敗(0)の場合にのみ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

*複数の RAddress 中の一部または全体ｱﾄﾞﾚｽに対して検索は正常に遂行されたが、ｱﾄﾞﾚｽ不在のｴﾗｰが発生する場合、他のｲﾝﾀｰﾌｪｰｽとは異なり、ResultCode を成功(1)として入力することに注意。

*RAddress は ResultCode の成功(1)/失敗(0)の有無に関係なく記述するようにし、属性情報である IsExist に各 RAddress に対する存在有無を入力

*Endpoint と Cert は IsExist の値が存在(1)の場合に入力

*要請ﾒｯｾｰｼﾞのｴﾗｰで RAddress をﾊﾟｰｼﾝｸﾞできない場合、RAddress は省略可能である(Endpoint および Cert も結果的に省略される)

*ErrorCode は、ResultCode が失敗(0)として入力された場合、すなわちｱﾄﾞﾚｽ不在のｴﾗｰを除いた他のｴﾗｰが発生した場合、ｴﾗｰ原因に該当するｴﾗｰｺｰﾄﾞを入力

【０４５０】

【表１３２】

【表 132】

```
<Response xmlns=" http://www.nipa.kr/eDocument_Circulation " >
  <SchAddrRes>
    <ResultCode>1</ResultCode>
    <ResultData>
      <RAddress IsExist=" 1 ">#000-0000-0000</RAddress>
      <Endpoint>http://111.111.111.111:8080/imxs/msh</Endpoint>
      <Cert>MFJIFDjfksdfjsl...</Cert>
    </ResultData>
  </SchAddrRes>
</Response>
```

【０４５１】

［流通メッセージングサーバと流通中継サーバ間の連係インターフェース］

流通中継サーバは、電子文書流通体系で流通メッセージングサーバ間に直接電子文書を転送する過程でエラーが発生して転送が失敗した場合、送信流通メッセージングサーバを代行して電子文書転送を遂行するシステムである。

【０４５２】

流通中継サーバは情報通信産業振興院が管理しており、全ての流通メッセージングサーバは流通中継サーバと連係してＰ２Ｐ流通過程でのエラー時の支援を受けることができる。

【０４５３】

流通メッセージングサーバと流通中継サーバ間の連係インターフェースは、流通メッセージングサーバが流通中継サーバに電子文書転送を依頼するためのプロトコルとして、下記表１３３のようなインターフェースに区分される。

【０４５４】

【表１３３】

【表 133】

ｲﾝﾀｰﾌｪｰｽ区分		ｲﾝﾀｰﾌｪｰｽ説明
転送代行	ﾒｯｾｰｼﾞ転送の依頼	□送信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞがﾒｯｾｰｼﾞの転送過程で受信者のｼｽﾃﾑおよびﾈｯﾄﾜｰｸ環境などによってｴﾗｰが発生した場合、流通中継ｻｰﾊﾞに転送ﾒｯｾｰｼﾞを代行して転送するように要請するｲﾝﾀｰﾌｪｰｽ □流通中継ｻｰﾊﾞは、応答ﾒｯｾｰｼﾞとして送信者の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞが送信を試みたことを証明する送信証明書を返す

先ず、流通メッセージングサーバと流通中継サーバ間の連係インターフェースの共通事項について説明すれば、次の１）の通りである。

１）要請メッセージのＭｅｓｓａｇｅＨｅａｄｅｒ拡張

流通メッセージングサーバと流通中継サーバ間の連係インターフェースメッセージの１番目のＭＩＭＥ　ＰａｒｔであるＳＯＡＰメッセージ内には流通メッセージングサーバの電子署名情報が含まれて伝達されるべきであり、流通中継サーバがＳＯＡＰメッセージの電子署名に使われた認証書の所有者が該当流通メッセージングサーバと一致するかを検証（ＶＩＤ検証）するのに必要な追加の流通メッセージングサーバの情報（ＣｏｒｐＮｕｍ、ＲＶａｌｕｅ）も含まれて伝達されるべきである。

【０４５５】

追加の流通メッセージングサーバの情報は、ＳＯＡＰメッセージ内のＭｅｓｓａｇｅＨｅａｄｅｒ要素の下位に拡張要素（ａｎｙ　＃＃ｏｔｈｅｒ位置）として位置するべきである。

【０４５６】

拡張要素の構造は下記表１３４の通りであり、拡張要素の例示は下記表１３５の通りである。

【０４５７】

【表１３４】

【表 134】

項目名		説明	反復回数	類型	長さ
Extension		■拡張要素ｴﾘﾒﾝﾄ	1..1		
	CorpNum	■送信者の事業者登録番号	1..1	String	10
	RValue	■送信者の公認認証書の個人ｷｰから抽出した RValue ■RValue を Base64 でｴﾝｺｰﾄﾞして入力する	1..1	String	28

【０４５８】

【表１３５】

【表 135】

```
<eb:MessageHeader SOAP:mustUnderstand= " 1 " eb:id= " MessageHeader "
eb:version= " 2.0 " >
  <eb:From>
    <eb:PartyId eb:type= " ecf_cd " >123456789</eb:PartyId>
    <eb:Role>sender</eb:Role>
  </eb:From>
  <eb:To>
    <eb:PartyId eb:type= " ecf_cd " >ech</eb:PartyId>
    <eb:Role>receiver</eb:Role>
  </eb:To>
  <eb:CPAId>urn:ech-and-ecm-cpa</eb:CPAId>
  <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
  <eb:Service>>urn:ech-service</eb:Service>
   <eb:Action>request</eb:Action>
 <eb:MessageData>



<eb:MessageId>20110210-170644Z-00057@127.0.0.18d1f96bf-9cd6-4049-9fdb-a6c0ed9
af46
 7</eb:MessageId>
    <eb:Timestamp>2011-02-10T08:06:44.810Z</eb:Timestamp>
  </eb:MessageData>
  <eb:DuplicateElimination></eb:DuplicateElimination>
  <Extention>
    <CorpNum>2208203228</CorpNum>
    <RValue>asdfasdf</RValue>
  </Extention>
 </eb:MessageHeader>
```

【０４５９】

以下、流通メッセージングサーバと流通中継サーバ間の連係インターフェースのメッセージ転送依頼インターフェースについて説明すれば、次の通りである。

【０４６０】

メッセージ転送依頼インターフェースは、流通メッセージングサーバが他の流通メッセージングサーバにメッセージを転送する過程で他の流通メッセージングサーバ側の受信エラーが発生した場合、流通中継サーバにメッセージ転送を依頼し、送信証明書の発給を受ける時に使われる。流通中継サーバは、流通メッセージングサーバのメッセージ転送依頼に対する受付結果だけを直ちにリターンし、受信流通メッセージングサーバにメッセージを転送した後、受信した受信証明書は、上述した"流通証明書伝達インターフェース"を使って転送依頼流通メッセージングサーバに転送する。

【０４６１】

メッセージ中継処理の流れは図１１６の通りである。

【０４６２】

メッセージ中継要請メッセージのフォーマットは図１１７の通りであり、図１１７のような全体メッセージ構造において、１番目のＭＩＭＥ　Ｐａｒｔにはｓｏａｐメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには要請流通メッセージが位置する。そして、ユーザが添付した文書がある場合、３番目のＭＩＭＥ　Ｐａｒｔから位置する。

【０４６３】

要請流通メッセージの構造は下記表１３６の通りであり、実際の例示は下記表１３７の通りである。

【０４６４】

【表１３６】

【表 136】

項目名			説明	反復回数	類型	長さ
Request			■要請 Root ｴﾘﾒﾝﾄ			
	SendMsgReq		■ﾒｯｾｰｼﾞ転送依頼ｴﾘﾒﾝﾄ			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -文書:0	1..1	Integer	1
		Title	■ﾒｯｾｰｼﾞの題名	1..1	String	最大 256
		Text	■ﾒｯｾｰｼﾞ本文 -送信者によって受信者の認証書で暗号化できる	0..1	String	-
		Sender	■送信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		Receiver	■受信者の公認電子ｱﾄﾞﾚｽ	1..1	String	最大 128
		ReqConfirm	■閲覧証明書の要請 -未要請:0 -要請:1	1..1	Integer	1
		IsEncrypted	■ﾒｯｾｰｼﾞの暗号化有無 -平文:0 -暗号化文:1	1..1	Integer	1
		Identifier	■本要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36

*表 136 において、文書の伝達目的で本文が必要ない場合、Text は省略可能である。

【０４６５】

【表１３７】

【表 137】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
    <SendMsgReq>
        <DocType>0</DocType>
        <Title>発送文書</Title>
        <Text>発送文書本文</Text>
        <Sender>#000-0000-0000</Sender>
        <Receiver>#000-0000-0000</Receiver>
        <ReqConfirm>1</ReqConfirm>
        <IsEncrypted>0</IsEncrypted>
        <Identifier>b366ff65-16c8-4d9d-a0ba-d76a2cc95ad2</Identifier>
    </SendMsgReq>
</Request>
```

【０４６６】

メッセージ中継応答メッセージのフォーマットは図１１８の通りであり、図１１８のような全体メッセージ構造において、１番目のＭＩＭＥ　ＰａｒｔにはＳＯＡＰメッセージ、２番目のＭＩＭＥ　Ｐａｒｔには応答流通メッセージ、そして３番目のＭＩＭＥ　Ｐａｒｔには受信証明書が位置する。仮に要請メッセージに対する処理過程でエラーが発生したとすれば、３番目のＭＩＭＥ　Ｐａｒｔは生成しない。

【０４６７】

応答流通メッセージの構造は下記表１３８の通りであり、実際の例示は下記表１３９の通りである。

【０４６８】

【表１３８】

【表 138】

項目名			説明	反復回数	類型	長さ
Response			■応答 Root ｴﾘﾒﾝﾄ			
	SendMsgRes		■ﾒｯｾｰｼﾞ転送依頼応答			
		DocType	■流通ﾒｯｾｰｼﾞの類型 -送信証明書:2 -ｴﾗｰ:9	1..1	Integer	1
		RefIdentifier	■本応答流通ﾒｯｾｰｼﾞに対応する要請流通ﾒｯｾｰｼﾞの固有識別値(UUID)	1..1	String	36
		ErrorCode	■ｴﾗｰｺｰﾄﾞ(流通ﾒｯｾｰｼﾞの類型がｴﾗｰ(9)の場合にのみ該当ｴﾗｰｺｰﾄﾞを入力)	0..1	String	256

*表 138 において、DocType がｴﾗｰ(9)の場合は、送信証明書が位置する MIME Part3 を生成しない。

【０４６９】
【表１３９】

【表 139】

```
<Request xmlns= " http://www.nipa.kr/eDocument_Circulation " >
    <SendMsgRes>
        <DocType>2</DocType>
        <RefIdentifier>b366ff65-16c8-4d9d-a0ba-d76a2cc95ad2</Identifier>
    </SendMsgRes>
 </Request>
```

【０４７０】
以下、上述したような本発明の好ましい実施形態による電子文書流通システムおよびこれを用いた電子文書流通方法の他の実施形態について詳細に説明すれば、次の通りである。

【０４７１】
［電子文書流通システムの構造および電子文書流通プロセス］
電子文書の流通は、信頼流通のための規格を遵守する企業／機関が直接に互いに電子文書をやりとりするＰ２Ｐ通信を基本とする。このようなＰ２Ｐ通信を遂行するための本発明による電子文書流通システムの基本要素は、アドレス情報を管理しているアドレスディレクトリサーバと各送受信個体間の流通ができるように支援する標準規格基盤の流通メッセージングサーバシステムである。このようなアドレスディレクトリサーバと流通メッセージングサーバシステムさえあれば、企業や機関が電子文書を流通できる基本構造は備えた状態であり、これに送受信者間の文書流通を証明するために流通証明書を発給すると同時に、これを第３者保管機関（公電所；公認電子文書保管所）に保管することにより、流通に対する法的根拠を確保することができる。

【０４７２】

本発明による電子文書流通システムは、前記基本要素の他にも、一般ユーザ（企業／機関、個人）が容易に電子文書を流通できるようにするためには、文書送受信機能に対するユーザインターフェースを提供する流通クライアントアプリケーション（ＡＰＰ）、文書作成の便宜性を向上させるために標準文書様式を提供する電子文書の書式登録機、行政機関と電子文書を中継するための公共部門連係ゲートウェイなどが追加構成要素として備えられる。

【０４７３】

前記のような電子文書流通システムにおいて発生する基本的なプロセスは下記の表１４０の通りである。

【０４７４】

【表１４０】

【表 140】

区分	ﾌﾟﾛｾｽ	備考
ｱﾄﾞﾚｽ情報の登録および管理	ｱﾄﾞﾚｽ情報の登録	基本ﾌﾟﾛｾｽ
	ｱﾄﾞﾚｽ情報の変更	基本ﾌﾟﾛｾｽ
	ｱﾄﾞﾚｽ情報の検索	基本ﾌﾟﾛｾｽ
送受信個体間のP2P 文書流通	実ﾕｰｻﾞと送受信個体の流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾋﾞｽｼｽﾃﾑ間の電子文書送受信の要請	基本ﾌﾟﾛｾｽ
	流通証明書の発給および公認電子文書保管所に保管を要請	基本ﾌﾟﾛｾｽ
	流通ｸﾗｲｱﾝﾄ APP と電子文書の書式登録機間の電子文書 Form 検索およびﾀﾞｳﾝﾛｰﾄﾞ	選択的ﾌﾟﾛｾｽ
	送/受信文書に対して公認電子文書保管所に保管を要請	選択的ﾌﾟﾛｾｽ
公共/行政部門と企業/個人ﾕｰｻﾞ間の電子文書流通	公共連係ｹﾞｰﾄｳｪｲを経由した文書流通	公共/行政機関において流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞ規格に応じて流通ｼｽﾃﾑを構築することが難しい場合､公共連係ｹﾞｰﾄｳｪｲを経由して文書を流通する

【０４７５】

［電子文書流通システムの各構成要素］

電子文書流通システムを構成する要素をより体系的に説明すれば、次の通りである。電子文書流通が行われるためには先ず流通の主体となる"１）送受信個体"が存在するべきであり、各送受信個体は文書を流通するために流通メッセージングサーバ規格を遵守する"２）流通メッセージングサーバシステム"を保有するべきである。また、電子文書流通の基本構成要素として、各送受信個体およびユーザの公認電子アドレスを登録、管理する"３）アドレスディレクトリサーバ"が存在するべきである。

【０４７６】

このような基本構成要素に基づいてユーザに流通便宜性を提供するために"４）流通クライアントＡＰＰ"が提供されるべきであり、行政／公共機関の連係を支援する"５）公共部門連係ゲートウェイ"と文書の書式を管理する"６）電子文書の書式登録機"が付加的に

提供されるべきである。
前記のような各構成要素に対して順に詳細に説明すれば、次の通りである。
【０４７７】
１）送受信個体
電子文書流通の基盤インフラ構成要素中、流通の基準となる単位が送受信個体であるが、送受信個体は流通に参加する役割に応じて送信者（Ｓｅｎｄｅｒ）または受信者（Ｒｅｃｅｉｖｅｒ）を共に遂行するようになり、この個体は流通メッセージングサーバシステムを介して流通プロトコル規格に応じて文書（情報）を流通する。
【０４７８】
流通に参加する全ての送受信個体は、流通メッセージング規格に応じて文書を送受信できる流通メッセージングサーバシステムを構築した後、流通メッセージングサーバシステムの物理アドレス情報をアドレスディレクトリサーバに登録することにより、電子文書流通に参加できる基盤を作ることになる。この時、各送受信個体は、下位に１つ以上の公認電子アドレスを有する実の流通ユーザを有するようになる。
【０４７９】
電子文書流通において、送受信個体として認められる個体は、メッセージングサーバ規格を遵守したシステムを構築した後、情報通信産業振興院によって標準適合性と相互運用性の認証を受けた個体に限定され、流通を証明するためには、１）認証を受けた送受信個体を介して電子文書が流通された後、２）標準規格に合わせて流通証明書を発給して第３者保管機関に保管するべきである。
【０４８０】
この時、送受信個体は、電子文書に対する法的所有者および責任者として直接電子文書転送の責任を負う個体と、流通される電子文書の実所有者であり、責任者であるユーザのために電子文書を代行する個体に区分される。電子文書の所有者が直接電子文書を転送する送受信個体である場合には、流通メッセージングサーバシステムの標準適合性と相互運用性の認証を受け、流通証明書を安全に第３者保管機関に保管することだけでも送受信個体に参加することができる。
【０４８１】
しかし、電子文書所有者（ユーザ）を代行して３者転送の責任を負わなければならない送受信個体である場合には、送受信個体が安全で信頼性のある方法で転送メッセージを管理し、ユーザ情報を管理し認証するかに対する部分まで立証しなければならない。３者流通の安全性および信頼性を保障するために、一時的にこのような３者流通が可能な送受信個体としては第３者保管機関事業者のみに限定する。
２）流通メッセージングサーバシステム
【０４８２】
流通メッセージングサーバシステムは、流通メッセージングサーバ規格に基づいて電子文書（情報）を流通するために、メッセージの送受信機能とアドレスディレクトリサーバと連係して受信者に対するアドレス情報および保安関連情報を検索する機能を必ず構築するべきである。流通メッセージングサーバシステムは、物理的に１つの電子アドレス（ＩＰ　Ａｄｄｒｅｓｓ）を有するが、下位のユーザのために複数のユーザアカウントを発給し管理することができ、ユーザアカウントは各々１つの公認電子アドレスを有するようになる。
【０４８３】
流通メッセージングサーバシステムは、各ユーザアカウントを管理するためにユーザアカウント別に電子文書の私書箱を管理するべきであり、流通メッセージングサーバシステムは、このユーザアカウントを代表して安全で信頼性のある電子文書流通の責任を持つようになる。
【０４８４】
このような流通メッセージングサーバシステムが電子文書流通内に送受信個体として参加するためには、本発明による要件に好適に実現されているのか、他のソリューションと

の相互運用に問題がないのかの認証を受ける過程を経なければならない。

【０４８５】

流通メッセージングサーバシステムに対する標準適合性および相互運用性を認証する認証システムは、認証された送受信個体を管理するべきであり、アドレスディレクトリサーバが公認電子アドレスを登録する過程で認証通過有無の確認を要請すれば、その結果を返すべきである。

【０４８６】

流通メッセージングサーバシステムが認証を受けて公認電子アドレスとして登録をするためには、図６５および下記のような手続きに従わなければならない。

先ず、送受信個体になろうとする企業／機関または個人ユーザは、本技術規格に合わせて流通メッセージングサーバシステムを構築する。

【０４８７】

次に、認証テストベッドが提供する自動化された検証ツールを通じて構築された流通メッセージングサーバシステムの標準適合性および相互運用性を検証する。

次に、自体検証を全て完了した送受信個体は、認証テストベッドに認証試験を要請する。

【０４８８】

次に、認証テストベッドのテスト手続きに応じてシステムに対する認証を終えた後、結果が"通過"となれば、送受信個体は、公認電子アドレス登録のための次の手続きを準備する。

【０４８９】

次に、認証テストベッドは、認証審査を通過した送受信個体に対する情報をアドレスディレクトリサーバに伝達し、アドレスディレクトリサーバは、この情報をアドレス登録の条件として活用する。

【０４９０】

次に、送受信個体は、認証通過した流通メッセージングサーバシステムを登録するために、アドレスディレクトリサーバに固有のＩＤ発給を申請する。

【０４９１】

次に、流通メッセージングサーバシステムがアドレスディレクトリサーバに登録が完了すれば、流通メッセージングサーバシステムは、電子文書流通に参加できるようになる。

【０４９２】

次に、流通メッセージングサーバシステムの認証が完了すれば、ユーザアカウントを開設し、代表公認電子アドレスである場合に、ユーザアカウントは公認電子アドレスに登録要請をする。

３）アドレスディレクトリサーバ

信頼できる電子文書流通に参加するために、全てのユーザは固有の電子アドレスの発給を受けるべきである。

【０４９３】

４）流通クライアントＡＰＰ

流通クライアントＡＰＰは、文書流通に参加するユーザたちのために、文書送信および受信、受信文書の閲覧および管理などのＵＩを提供するアプリケーションを指し示す。流通クライアントＡＰＰは、独自に文書を送受信することはできず、必ず流通メッセージングサーバシステムと連係しなければならない。

【０４９４】

流通クライアントＡＰＰにおいて作成されたり添付されたりした文書は、流通メッセージングサーバシステムに伝達されて転送を要請するようになり、流通メッセージングサーバシステムを介して受信された文書を照会するようになる。流通メッセージングサーバシステムがユーザアカウントを通じて送受信の私書箱を管理する場合であれば、流通クライアントＡＰＰは、受信文書中のユーザアカウント情報の確認を通じて該当文書にのみアクセスが可能である。

流通クライアントＡＰＰは、ユーザの要求によってＣ／Ｓ形態のアプリケーションに実現することもでき、ウェブ形態の画面に実現することもできる。

【０４９５】

５）公共部門連係ゲートウェイ

電子文書流通を収容し難い行政および公共機関の場合、公共部門連係ゲートウェイを介して行政、公共機関と電子文書の流通体系下の民間企業、機関、個人間の文書を中継する役割を遂行する。

【０４９６】

６）電子文書の書式登録機

電子文書の書式登録機は、流通メッセージングサーバシステムを利用して電子文書を転送しようとするユーザがＯｆｆｉｃｅツールを利用して直接転送文書を作成することもできるが、ユーザがより容易に電子文書を生成できるように支援するために、標準文書様式を登録し管理しつつ、流通クライアントＡＰＰのようなユーザ用アプリケーションが利用できるように文書様式の登録および管理、文書様式の検索、閲覧、およびダウンロード、文書様式の削除などの管理を支援するシステムである。

【０４９７】

電子文書の書式登録機は、文書標準様式を管理するサーバエンジンとクライアントアプリケーション（ＡＰＰ）がこれを検索し、ダウンロードした後に内部プログラムにプラグイン（Ｐｌｕｇ－Ｉｎ）して使えるようにする標準インターフェースを提供する。

【０４９８】

［電子文書流通方法］

電子文書流通において電子文書を流通するための全体プロセスは、"１）流通前の事前準備ステップ"、"２）電子文書の流通ステップ"、"３）流通のための証明ステップ"の３ステップに大きく区分して見ることができる。以下では、前記３ステップに対する詳細な説明と共に、"文書送受信方案"と"流通証明方案"と"スパムメッセージ処理方案"について詳細に説明する。

【０４９９】

１）流通前の事前準備ステップ

－電子文書の書式登録機の管理者は、電子文書の書式登録機を利用して、使用する標準文書の書式を登録する。

－送受信参加者は、自体的に信頼流通のための流通メッセージングサーバシステムを構築するか、既に構築された流通メッセージングサーバシステムにユーザアカウントを開設して使用するかを決定する。自体的に信頼流通のための流通メッセージングサーバシステムを構築する場合には、電子文書の送受信のための流通メッセージングサーバシステムを構築した後、認証機関を介して流通メッセージングサーバシステムの標準適合性、相互運用性に対する認証テストを遂行した後、アドレスディレクトリサーバに接続した後、認証された流通メッセージングサーバシステムのための送受信個体ＩＤを申請し発給を受けた後、内部の実ユーザのために自体的に内部区分子を登録して管理し、標準文書の書式基盤の文書作成機能を利用するために一般ユーザのためのクライアントアプリケーションに標準文書の書式作成機能をプラグイン（Ｐｌｕｇ－Ｉｎ）する（選択的事項）。これに対し、３者流通が可能な流通メッセージングサーバシステムを保有した送受信個体を利用する場合には、流通メッセージングサーバシステムを介して企業／機関／個人のためのユーザアカウント開設を要請した後、ユーザアカウントに対する公認電子アドレス情報をアドレスディレクトリサーバに登録した後、標準文書の書式基盤の文書作成機能を利用するために一般ユーザのためのクライアントアプリケーションに標準文書様式の作成機能をプラグイン（Ｐｌｕｇ－Ｉｎ）する（選択的事項）。

【０５００】

２）電子文書の流通ステップ

○文書送信者

－文書送信者は、流通する文書を選択するか、文書作成機を通じて転送する文書を作成

する。
－文書受信相手方のアドレス情報および伝達文書、文書暗号化の有無および電子署名の有無を選択する（暗号化および電子署名は、転送メッセージではない、添付する伝達文書を対象にし、この手続きは選択的事項である）。
【０５０１】
－流通クライアントＡＰＰは、アドレスディレクトリサーバに連係して受信相手方の公認電子アドレスを基盤に物理アドレス情報および暗号化のための公開キー情報を獲得する（選択的事項であり、流通クライアントＡＰＰが物理アドレスを獲得しない場合、流通メッセージングサーバがこの作業を遂行する）。
【０５０２】
－流通クライアントＡＰＰは、流通メッセージングサーバに受信者のアドレス情報を基盤に転送要請をする（物理アドレス情報または公認電子アドレスの両方とも可能）。
○送信者の流通メッセージングサーバ
【０５０３】
－流通クライアントＡＰＰから要請した転送要請メッセージが受信者に対する物理アドレス情報ではない場合、流通メッセージングサーバは、公認電子アドレスを基盤に受信者の送受信個体に対する物理アドレス情報をアドレスディレクトリサーバに問い合わせる。
－電子文書を流通プロトコル規格で定義されたメッセージ構造体にパッケージングする。
－送信者の流通メッセージングサーバの公認認証書を基盤にメッセージに電子署名をする。
－受信者の物理アドレス情報にメッセージを転送する。
○受信者の流通メッセージングサーバ
－メッセージ受信後、受信メッセージ検証し、メッセージから文書を抽出する。
－同期式応答で受信証明書を含むメッセージを送信者に転送する。
【０５０４】
３）流通のための証明ステップ
－受信者は、文書受信事実の確認のために文書受信時点で"受信証明書"を生成した後に送信者に伝達するべきであり、これを受信した文書送信者は、"受信証明書"を第３者保管機関に保管する。
【０５０５】
－送信者が要求する場合、受信者は、受信文書を実文書担当者（ユーザ）に伝達した後、担当者が受信文書を確認した時点で"閲覧証明書"を生成して送信者に伝達し、"閲覧証明書"を受信した文書送信者は"閲覧証明書"を第３者保管機関に保管する（閲覧証明書の発給は送信者の要請がある場合にのみ適用される）。
【０５０６】
－送信者が受信者に文書伝達を試みたものの、失敗した場合には、送信試みに対して証明するために客観的３者である電子文書流通ハブに文書転送を依頼し、転送依頼を受けた電子文書流通ハブは、転送依頼を受けたことを立証するために"送信証明書"を発給して送信依頼者に伝達し、これを受信した送信依頼者は、"送信証明書"を第３者保管機関に保管する。
【０５０７】
○文書送受信方案
流通メッセージングサーバシステムを介して送信者と受信者は文書を電子的に流通する。流通メッセージングサーバシステムは流通プロトコルに応じて電子文書を送受信し、信頼メッセージ流通のために全てのメッセージは転送と受信確認（または受信証明書）メッセージの組み合わせからなり、受信者に対する物理アドレス情報はアドレスディレクトリサーバを介して獲得するようになる。
【０５０８】
○流通証明方案

"流通証明"とは電子文書流通と関連した送信、受信、閲覧に対して該当事実を信頼性のある方法で証明することをいい、この時、電子文書流通と関連した行為に対して発給する証明書を通称して"流通証明書"という。

【０５０９】

流通メッセージングサーバシステムは、送信、受信に対する行為立証のために送信および受信時点で流通証明書を発給し、発給した流通証明書を公認電子文書第３者保管機関に保管することにより、流通行為に対する証明資料として活用できるようにする。

【０５１０】

流通メッセージングサーバシステムは、電子文書の送信、受信、閲覧に対する事実を証明し、各事実に対する流通証明書を生成し、流通証明書は、流通証明書の識別情報、流通証明書の生成時刻および満了時刻、流通証明書政策および流通証明対象を含む。

【０５１１】

電子文書送信に対する流通証明書は、電子文書流通ハブが生成し、流通証明対象に発信者の識別情報、受信者の識別情報、流通識別情報、文書識別情報、電子文書の送信依頼時刻を含む。

【０５１２】

電子文書受信に対する流通証明書は、電子文書を受信した受信者が生成し、流通証明対象に発信者の識別情報、受信者の識別情報、流通識別情報、文書識別情報、電子文書の送信時刻、電子文書の受信時刻を含む。

【０５１３】

電子文書閲覧に対する流通証明書は、電子文書を受信確認したユーザが生成し、流通証明対象に発信者の識別情報、受信者の識別情報、流通識別情報、文書識別情報、電子文書の送信時刻、電子文書の受信時刻、電子文書の受信確認時刻を含むべきである。

【０５１４】

このように生成された流通証明書はＮＰＫＩまたはＧＰＫＩ認証書で電子署名されるべきであり、生成された流通証明書は電子文書送信者に伝達されるべきであり、全ての流通証明書は第３者保管機関に保管されることが好ましい。

【０５１５】

○スパムメッセージの処理方案

電子文書流通は、基本的に送信者が認証された流通メッセージングサーバシステムを介して転送をし、受信者もこれを基本に受信するため、スパムを発送した時に転送者に責任を問える基盤構造を有する。しかし、スパム発送者が流通メッセージングサーバシステムにユーザアカウントを開設し、これを利用して転送する場合があり得る。また、現在の認証方式がシステムの技術的内容に対する認証のみを対象にしており、スパム発送者が流通メッセージングサーバシステムを構築し、これを技術的に認証した後にスパム発送手段として使用した時には、初期に根本的に遮断するのが容易ではない状況である。

【０５１６】

したがって、このような問題点を解決するために、本発明による標準文書流通のインフラにおいては、認証目録管理基盤のホワイトリスト、ユーザの申告方式によるスパム対象目録管理基盤のブラックリストの体系を提供し、このような体系によって受信者が受信拒否できるプロセスを適用してスパムメッセージを防止できるようにする。

【０５１７】

スパムメッセージの申告および送信相手方に対する確認のための機能は必須機能であり、全ての流通メッセージングサーバはこの機能を必ず構築しなければならない。

【０５１８】

受信者は、受信したメッセージがスパムメッセージであると判断されれば、図２７に示すようなプロセスによってスパムメッセージを電子文書流通ハブのアドレスディレクトリサーバに申告し、これと関連した処理手続きは次の通りである。

【０５１９】

先ず、受信者がメッセージを受信した時点でスパムメッセージであると判断すれば、受

信者は、流通メッセージングサーバシステムを介してアドレスディレクトリサーバに該当メッセージを受信メッセージとして申告する。

【０５２０】

次に、流通メッセージングサーバシステムからスパムメッセージの申告を受け付けしたアドレスディレクトリサーバは、受付済みの確認メッセージを返す。

【０５２１】

次に、アドレスディレクトリサーバを管理する主体である情報通信産業振興院は、該当メッセージを分析し、送信者に対する調査を通じ、送信者の公認電子アドレスに対してブラックリストに追加するか否かを審査し判断する。

【０５２２】

次に、最終的にブラックリスト対象者に確定されれば、アドレスディレクトリサーバは、該当公認電子アドレスをブラックリストに追加した後、送信者にブラックリスト追加に対する内容を通知する。

次に、アドレスディレクトリサーバは、スパムメッセージ要請に対する処理結果をスパム申告者（受信者）に伝達する。

【０５２３】

前記のような処理手続きにおいて、ホワイトリストは、送信流通メッセージングサーバシステムが認証を受けて正式に登録されたメッセージングサーバシステムに対する情報のみが記録され、ブラックリストは、転送者のアドレスがスパム発送者として登録された場合に登録され、同一の流通メッセージングサーバシステムを介してブラックリストに登録されるスパムアドレスが重複発生する場合には、電子文書流通ハブにおいて該当流通メッセージングサーバシステムに対する認証取り消し有無を判断した後、認証を取り消し、ホワイトリストから削除することができる。

【０５２４】

受信者は、メッセージ受信時、送信相手方が信頼できるほどの正当なユーザであるかを確認するためにアドレスディレクトリサーバのホワイトリストとブラックリストを確認した後、受信拒否をするか否かを決定する。送信者に対する確認は、受信時点でリアルタイムで確認をするか、受信者の流通メッセージングサーバシステムにＣａｃｈｅ形態で管理している目録を通じて確認する周期的な確認方法がある。

【０５２５】

リアルタイムで送信者に対する確認を遂行するプロセスは、図２８に示すように、受信者がメッセージを受信する時点でアドレスディレクトリサーバに送信者のアドレスがホワイトリスト、ブラックリストに登録されたか否かを判断した後にメッセージに対する受信拒否の可否を決定し、このようにリアルタイムで送信者に対する確認を遂行するプロセスの詳細な処理手続きは次の通りである。

【０５２６】

先ず、受信者の流通メッセージングサーバシステムは、メッセージを受信すれば、アドレスディレクトリサーバに正当なユーザであるかを確認するために確認要請メッセージを伝達する。

次に、アドレスディレクトリサーバは、要請を受けたユーザのアドレス情報がホワイトリストに含まれているか否かを確認する。

【０５２７】

次に、該当アドレスがホワイトリストになければ、アドレスディレクトリサーバは、直ちに確認要請者に登録されていないユーザであることを結果メッセージとして返し、ホワイトリストにあれば、再び該当アドレスがブラックリストに登録されたアドレスであるか否かを確認する。

次に、アドレスディレクトリサーバは、確認要請者にブラックリストへの登録有無に対する結果メッセージを返す。

【０５２８】

次に、受信者は、アドレスディレクトリサーバから送信者が正当なユーザではないとい

う（ホワイトリストにないか、ブラックリストに登録された場合）結果メッセージを受けた場合には、受信メッセージを自体的にスパムメッセージとして処理した後、アドレスディレクトリサーバから受けた処理結果メッセージとスパムメッセージの受信履歴を記録し保管する。

次に、スパムメッセージに対する処理履歴は必ず１ヶ月以上保管することにより、該当送信者に対する受信拒否の正当性を確認できるようにする。

【０５２９】

そして、周期的に送信者に対する確認を遂行するプロセスは、図２９に示すように、受信者は事前にアドレスディレクトリサーバからホワイトリストとブラックリストをもらって自体的に管理し、これを基盤に送信者のアドレスがホワイトリスト、ブラックリストに登録されたか否かを判断した後にメッセージに対する受信拒否の可否を決定し、このように周期的に送信者に対する確認を遂行するプロセスの詳細な処理手続きは次の通りである。

【０５３０】

先ず、受信者の流通メッセージングサーバシステムは、予めアドレスディレクトリサーバから最新のホワイトリストとブラックリストを要請した後に自体的に管理する。この時、リストの変動事項の発生時、自動通知の要請有無を共に伝達する。このような変動事項発生の自動通知を要請した場合にも、アドレスディレクトリサーバに最新リストを持ってくるための要請を周期的に行うことにより、リスト情報が最大限１日以上の差が生じないようにする。

【０５３１】

次に、アドレスディレクトリサーバは、ホワイトリストおよびブラックリストに変動事項が発生すれば、変動通知の要請をしたユーザに変動内訳をブロードキャスティング（ｂｒｏａｄｃａｓｔｉｎｇ）する。

次に、リストに対する変動事項を受けたユーザ流通メッセージングサーバシステムは、自体管理するリスト情報を修正することによって同期化させる。

【０５３２】

次に、受信者は、メッセージを受信すれば、アドレスディレクトリサーバに正当なユーザであるか否かを確認するために、自体管理するリストを確認する。

【０５３３】

次に、受信者は、自体管理するリストをチェックした結果、送信者が正当なユーザではないと（ホワイトリストにないか、ブラックリストに登録された場合）判断した場合には、受信メッセージを自体的にスパムメッセージとして処理した後、スパムメッセージの受信履歴を記録し保管する。

次に、スパムメッセージに対する処理履歴は必ず１ヶ月以上保管することにより、該当送信者に対する受信拒否の正当性を確認できるようにする。

【０５３４】

［流通メッセージングサーバシステム］

以下では、上述したような本発明の好ましい実施形態による電子文書流通システムの流通メッセージングサーバシステムと関連して詳細に説明する。

【０５３５】

流通メッセージングサーバシステムは、大きく、メッセージ送信、メッセージ受信、受信メッセージに対する私書箱管理、メッセージ保安（ユーザ認証、文書の暗号／復号化など）、送受信履歴の管理、アドレスディレクトリサーバ連係、メッセージ検証、内部システム連係インターフェース、流通証明書の発給および管理、第３者保管機関連係などで構成される。

【０５３６】

図３７は流通メッセージングサーバシステムの構造を示し、このような図３７を参照し、流通メッセージングサーバシステムの構成要素の各々（１）～９））について詳細に説明すれば、次の通りである。

【０５３７】
１）メッセージ送受信
－流通プロトコルに応じてメッセージを送信し受信する。
２）ユーザ別のアカウント（私書箱）管理
－送受信したメッセージをユーザアカウントまたは内部区分子に応じてアカウント別の私書箱に保管する。
【０５３８】
－私書箱に保管した送信文書に対し、"送信中"、"送信完了"、"送信失敗"、"担当者の受信完了"を含む４ステップの状態情報を管理する。この時、"送信中"の状態は文書転送後に受信者から何の応答を受けていない状態であり、"送信完了"の状態は受信者の流通メッセージングサーバシステムから"受信証明書"を受けた状態であり、"送信失敗"の状態は受信流通メッセージングサーバシステム内部においてエラーが発生してＳＯＡＰ　Ｆａｕｌｔメッセージをリターンするか、送受信過程でネットワークエラーが発生した場合であり、"担当者の受信完了"の状態は送信流通メッセージングサーバシステムが受信者から担当者の文書を確認したことを証明する"閲覧証明書"を受けた場合である。
【０５３９】
－ユーザアカウント別の私書箱に保管された受信文書に対し、"検証エラー"、"受信確認前"、"受信確認"、"閲覧確認"を含む４ステップの状態情報を管理する。この時、"検証エラー"の状態は受信したメッセージに対する基本構造の検証においてエラーが発生した状態であり、"受信確認前"の状態は受信文書担当者が私書箱の受信文書目録を読む前であり、"受信確認"の状態は受信文書担当者が私書箱の受信文書目録を読んだ状態であり、"閲覧確認"の状態は受信文書担当者が受信文書に対する詳細内容を閲覧した状態であって、この時点で受信者の流通メッセージングサーバシステムは"閲覧証明書"を発給した後に送信者に伝達する。
－受信ユーザによって削除要請が届くと、該当受信文書を物理的に削除処理する。
－私書箱において、送信文書、送信に対する受信確認メッセージ、受信担当者の受信確認メッセージは互いに連関されるように連関情報を有する。
【０５４０】
３）アドレスディレクトリサーバ連係
－アドレスディレクトリサーバが提供するアドレス情報の登録および検索プロセスに応じてアドレス情報を管理する。
【０５４１】
－アドレスディレクトリサーバが提供するサービスを呼び出しできるクライアント機能を含む。すなわち、アドレスディレクトリサーバが提供するアドレス情報の登録、検索、修正、削除機能を遠隔から呼び出すサービスクライアント機能を提供する。
【０５４２】
４）メッセージ保安（ユーザ認証、文書の暗号／復号化など）
－流通プロトコルにおいて提示するメッセージ保安機能（メッセージの電子署名、署名検証）を基本的に遂行する。
５）送受信履歴の管理
－流通メッセージングサーバシステムは、送受信履歴に対して最小１年以上は必ず保管／管理する。
－保管する送受信履歴に対する情報は送信履歴と受信履歴であり、送信履歴はメッセージｉｄ、連関メッセージｉｄ、送信者（ユーザアカウント含む）、受信者、送信時間、送信文書に対するハッシュ値を含み、受信履歴は送信者、受信者（ユーザアカウント含む）、受信時間、受信文書に対するハッシュ値を含む。
【０５４３】
６）流通証明書の発給および管理
－流通メッセージングサーバシステムは、文書の送受信事実に対する内容を証明できるように流通証明書を発給し管理する。

－発給された流通証明書は、伝達を受けた後、直ちに第３者保管機関に保管依頼することによってその信頼性が保証される。
－発給された後に第３者保管機関に保管された流通証明書の履歴を管理し、流通証明書の発給履歴は、流通証明書ｉｄ、流通証明書の発給時刻、連関メッセージｉｄ、流通証明書原本（選択的）、第３者保管機関の保管後に受信した保管－ｋｅｙ情報を含む。
【０５４４】
７）メッセージのパッケージ処理（Ｐａｃｋａｇｉｎｇ、Ｐａｒｓｉｎｇ、Ｅｘｔｒａｃｔｉｎｇ）
－送信文書を転送前に流通プロトコルで定義されたメッセージ構造にパッケージング（Ｐａｃｋａｇｉｎｇ）する。
【０５４５】
－受信した文書を流通プロトコルで定義されたメッセージ構造によってパーシング（Ｐａｒｓｉｎｇ、構文解釈）し、必要な情報を抽出（Ｅｘｔｒａｃｔｉｎｇ）する。
【０５４６】
８）流通証明書の保管要請
－一般送受信個体が流通証明書を保管要請するためには、第３者保管機関の流通メッセージングサーバシステムに第３者保管機関への保管要請メッセージを転送する（遠隔保管要請）。
【０５４７】
－第３者保管機関の流通メッセージングサーバシステムは、公認電子文書保管所の保管要請メッセージを受信すれば、第３者保管機関に流通証明書保管のための保管要請Ｃｌｉｅｎｔを呼び出す。
【０５４８】
－第３者保管機関の流通メッセージングサーバシステムが直接流通証明書を生成した場合には、生成時点で第３者保管機関への保管要請Ｃｌｉｅｎｔを直接呼び出す（ローカル保管要請）。
－流通証明書の保管要請のためのＣｌｉｅｎｔは、第３者保管機関の送受信連係インターフェース規格に応じて第３者保管機関に保管を要請する。
【０５４９】
９）付加サービス
－流通クライアントＡＰＰ管理の配布、バージョン管理などを遂行する。
－メッセージ流通管理（履歴、統計情報など）を遂行する。
－システム管理（システムモニタリング、環境情報など）を遂行する。
－文書様式（Ｆｏｒｍ）の管理を遂行する。
【０５５０】
前記のような１）～９）の構成要素を有する本発明による流通メッセージングサーバシステムを図３８のように第３者保管機関に適用した場合には、流通証明書を保管する時に流通証明書の保管要請モジュールは、第３者保管機関連係インターフェースの規格に応じて開発された連係インターフェースクライアントを呼び出して保管要請をする。
【０５５１】
前記のような１）～９）の構成要素を有する本発明による流通メッセージングサーバシステムを図３９のように一般送受信個体（一般事業者）に適用した場合には、流通証明書を保管する時に第３者保管機関事業者の流通メッセージングサーバシステムに流通証明書の保管を要請するメッセージを転送し、処理結果を受ける方式で処理する。
【０５５２】
前記のような１）～９）の構成要素を有する本発明による流通メッセージングサーバシステムを利用して送信者と受信者間に直接メッセージを流通するプロセスは、"１）受信者に対する物理アドレスおよび保安情報の獲得"、"２）メッセージ転送および転送確認"、"３）業務受信者の受信確認"、"４）流通証明書の発給および保管"を含む４ステップからなり、このような４ステップと関連し、図４０を参照して詳細に説明すれば、次の通り

である。
【０５５３】
１）受信者に対する物理アドレスおよび保安情報の獲得
－送信者のシステムは、相手方に対するアドレス情報に基づいて実際メッセージが伝達されるべき物理アドレス情報および保安情報（送信メッセージに対する受信暗号を必要とする場合）をアドレスディレクトリサーバに要請することによってこれを獲得する。
【０５５４】
－受信者に対する物理アドレスおよび保安情報は、流通クライアントＡＰＰがアドレスディレクトリサーバに要請した後に、受信者の物理アドレス情報を流通メッセージングサーバに伝達するようにする。
【０５５５】
－ユーザに対するｉｄ（例：住民登録番号、事業者登録番号など）だけで受信者に対するアドレス情報を獲得することもできるが、この場合には、受信者が送信者にｉｄ基盤のアドレス情報検索を許容した場合にのみ可能である。
＊送信者が受信者の物理アドレス情報および保安情報を既に知っている場合には、この手続きは省略可能である。
【０５５６】
２）メッセージ転送および転送確認
－送信者は、メッセージを流通プロトコル規格に合わせてパッケージングした後、流通メッセージングサーバシステムの公認認証書を基盤に電子署名を遂行する。
－流通メッセージングサーバシステムは、先に獲得した物理アドレスにパッケージングし電子署名されたメッセージを転送する。
【０５５７】
－メッセージを受信した受信流通メッセージングサーバシステムは、メッセージの基本パッケージング構造、電子署名に対する有効性、送信者に対する適合性（検証に対する詳細内容は"２．４．６メッセージ検証"部分を参照）を検証した後、受信確認のための受信証明書またはエラーメッセージを生成する。
－受信流通メッセージングサーバシステムは、生成した応答メッセージを送信者に転送する。
－転送と転送確認の過程は同期式メッセージ処理でなされる。
【０５５８】
３）業務受信者の受信確認
－送信者がメッセージ転送時点で業務受信者の担当者の閲覧確認メッセージを要請した場合には、受信者は、メッセージに対する業務的な受信確認時点で送信者に必ず担当者の閲覧確認を証明できる閲覧証明書を生成し、これを転送しなければならない。
【０５５９】
－受信者がメッセージ送信者に担当者の閲覧確認のための閲覧証明書メッセージを送れば、元のメッセージ送信者にこれに対する受信確認メッセージを同期式で送る。
【０５６０】
４）流通証明書の発給および保管
－各ステップ別に流通に対する証明を受けようとする場合、送信者は各ステップに応じて受信、閲覧、送信に対する証明書を発給し、これを第３者保管機関に保管することによって流通に対する法的証明の根拠を確保する。
【０５６１】
本発明による流通メッセージングサーバシステムを利用して送信者と受信者間に直接メッセージを流通するプロセスは、前記のような"１）受信者に対する物理アドレスおよび保安情報の獲得"、"２）メッセージ転送および転送確認"、"３）業務受信者の受信確認"、"４）流通証明書の発給および保管"の他に"５）エラー処理"も遂行するが、図４１～図４３を参照し、エラー処理機能と関連して詳細に説明すれば、次の通りである。
【０５６２】

５）エラー処理機能
流通メッセージングサーバシステムの全てのメッセージ送受信プロセスは同期式処理を基本とする。したがって、転送に対する全てのエラーは転送者が確認可能であるので再転送することを基本とし、同一のメッセージ転送は同一のＭｅｓｓａｇｅＩｄ値を設定して再び送ることにより、受信者が受信成功後に受信確認メッセージの転送過程でのエラーに対しても重複メッセージ受信を検知できるようにする。
【０５６３】
流通メッセージングサーバシステムは、要請メッセージの送信に失敗した場合に、図４１のような処理フローチャートに従う。すなわち、メッセージ送信者が転送する過程でネットワークエラーなどによって転送エラーが発生した場合に、送信者は、ＨＴＴＰエラーのようなエラーメッセージを受けると、同一のメッセージを再び再転送するように要請し、送信者は、受信者に受信確認メッセージを受けた場合にのみ転送成功として認識する。
【０５６４】
流通メッセージングサーバシステムは、応答メッセージの受信に失敗した場合に、図４２のような処理フローチャートに従う。すなわち、メッセージが受信者に正常に伝達されたものの、送信者が受信者から受信確認メッセージを受けていない場合に、送信者は、送信失敗エラーとして認識し、受信者に同一のメッセージを同一のＭｅｓｓａｇｅＩｄに再転送するようになり、受信者は、受信した文書のＭｅｓｓａｇｅＩｄが以前の受信メッセージと同一である場合には、重複受信として受信確認メッセージを送った後に内部処理をする。
【０５６５】
流通メッセージングサーバシステムは、エラーメッセージの受信に失敗した場合に、図４３のような処理フローチャートに従う。すなわち、送信者が受信者に転送したメッセージが正確に伝達されたものの、転送メッセージそのものに誤りがあってエラーメッセージの応答を受けた場合に、送信者はエラー類型に応じてメッセージ処理を異にし、再要請時に転送するメッセージのＭｅｓｓａｇｅＩｄは同一である必要はなく、業務状況に応じて異に処理することができる。
【０５６６】
上述したような本発明による流通メッセージングサーバシステムにおいて必須に要求される機能である、"１）メッセージ送受信"、"２）受信メッセージ私書箱の管理"、"３）メッセージ保安"、"４）送受信履歴の管理"、"５）アドレスディレクトリサーバ連係"、"６）メッセージ検証"、"７）内部システム連係インターフェース"、"８）流通証明書の発給および管理"機能について詳細に説明すれば、次の通りである。
【０５６７】
１）メッセージ送受信
流通メッセージングサーバシステムがメッセージを送受信する基本プロセスは、上述した本発明による［電子文書流通方法］の"文書送受信方案"を従う。メッセージ送受信のための基本となるメッセージ交換類型はメッセージ流通プロトコルの同期式応答を基本とし、送信メッセージと受信確認メッセージ、送信メッセージと受信エラーメッセージ、送信メッセージとビジネス的な応答メッセージ（受信確認メッセージの意味を含む）の構成からなってもよい。
【０５６８】
メッセージ送受信の類型としては、送信と受信確認応答メッセージの組み合わせと、送信とビジニーズ応答メッセージの組み合わせを含む２つの類型がある。
【０５６９】
メッセージ送受信の類型が送信と受信確認応答メッセージの組み合わせである場合の処理流れは図４４の通りであり、送信メッセージと受信確認（または受信エラー）メッセージはＳＯＡＰ（Ｓｉｍｐｌｅ Ｏｂｊｅｃｔ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ） Ｒｅｑｕｅｓｔ－Ｒｅｓｐｏｎｓｅの組み合わせからなり、送信メッセージとそれに対する応答メッセージは送信メッセージのＭｅｓｓａｇｅＩｄを応答メッセージのＲｅｆＴｏＭｅ

ｓｓａｇｅＩｄに入れて送ることによって連関関係を持つようにするが、これと関連した詳細な説明は後述する［流通プロトコル］を参照する。

【０５７０】

メッセージ送受信の類型が送信とビジネス応答メッセージの組み合わせである場合の処理流れは図４５の通りであり、送信メッセージと受信確認（または受信エラー）メッセージを含む応答メッセージはＳＯＡＰ　Ｒｅｑｕｅｓｔ－Ｒｅｓｐｏｎｓｅの組み合わせからなり、受信者がメッセージを受信した後、内部システムにリアルタイムで連係してビジネス処理した応答文書を生成した後、応答文書と受信確認ＡＣＫメッセージを共に応答メッセージにのせて送信者に伝達し、送信メッセージとそれに対する応答メッセージは送信メッセージのＭｅｓｓａｇｅＩｄを応答メッセージのＲｅｆＴｏＭｅｓｓａｇｅＩｄに入れて送ることによって連関関係を持つようにするが、これと関連した詳細な説明は後述する［流通プロトコル］を参照する。

【０５７１】

送受信されるメッセージの構造は図４６に示すようにＭｕｌｔｉＰａｒｔ－ＭＩＭＥ構造を有し、１番目のＭＩＭＥ部分にはＳＯＡＰメッセージが、２番目のＭＩＭＥからは転送しようとする文書が入る。

【０５７２】

１番目のＭＩＭＥにはＳＯＡＰヘッダとＳＯＡＰ　Ｂｏｄｙとから構成されたＳＯＡＰ　Ｅｎｖｅｌｏｐｅが入り、ＳＯＡＰヘッダはメッセージ送受信のためのメッセージヘッダ情報、電子署名、受信確認メッセージ、同期式の転送表示、エラーメッセージなどが入る。そして、２番目のＭＩＭＥにはメッセージ受信者に伝達する文書（情報）が入り、担当者の受信確認メッセージを伝達する場合にこの位置に入る。そして、３番目のＭＩＭＥは、メッセージ受信者に伝達する文書（情報）が２つ以上である場合、３番目のＭＩＭＥから順次入る。

【０５７３】

２）受信メッセージ私書箱の管理

流通メッセージングサーバシステムは、メッセージを受信すれば、受信メッセージをアカウント別に私書箱に格納する。受信メッセージ私書箱は１つ以上のユーザアカウント別に区分されてメッセージを格納管理し、ユーザの要請（新しい受信メッセージの存在有無、受信メッセージの閲覧、受信メッセージのダウンロード、受信メッセージの削除など）に応じて必要な処理後、結果を返すインターフェースを必ず標準化された方式で提供しなければならない。

【０５７４】

流通メッセージングサーバシステムが管理するユーザアカウントが電子文書流通に含まれる公認電子アドレスとして資格を持つためには、流通メッセージングサーバシステムは、信頼ユーザアカウントを持つための認証要件（今後、別途の評価指針によって要件を定義することであり、現時点では第３者保管機関のみがこの認証要件を充足したものとして認める）を通過しなければならない。

【０５７５】

したがって、個人または企業（機関）が電子文書流通において公認電子アドレスを獲得するための方案としては次のような２つの方案がある。第１方案は、自体的に流通メッセージングサーバシステムを構築し、認証を受けた後に獲得した送受信個体ＩＤをアドレスディレクトリサーバに登録することであり、第２方案は、認証を受けた流通メッセージングサーバシステム中、信頼ユーザアカウントを有する要件を追加的に充足した送受信個体に私書箱を開設して、ユーザＩＤの発給を受けた後、これをアドレスディレクトリサーバに登録することである。

【０５７６】

３）メッセージ保安

転送メッセージに対する保安は、無欠性保障のための電子署名と機密性保障のための暗号／復号化に分けられる。流通メッセージングサーバシステムを介して転送されるメッセー

ジはＳＯＡＰメッセージと添付文書に分けられる。この時、添付文書は流通クライアントＡＰＰにおいて既に暗号化されている状態であり、ＳＯＡＰ　Ｅｎｖｅｌｏｐｅには単にメッセージ送受信のためのヘッダ情報だけが含まれるので、流通メッセージングサーバシステムにおいては、追加的な暗号化過程を経ず、メッセージの送受信過程で偽変造防止のための電子署名過程は遂行する。電子署名方式および細部手続きは後述する［流通プロトコル］を参照する。

【０５７７】

４）送受信履歴の管理

流通メッセージングサーバシステムは、今後、送受信に関連した紛争が発生したり問題が提起されたりする時、これを確認するために送受信に対する履歴情報を管理しなければならない。履歴情報は、送受信行為に対する情報だけでなく、実際に送受信した文書に対する情報も管理するべきであるが、実文書を第３者保管機関に保管した場合には、文書の原本ではない第３者保管機関から受けた登録証明書のみを保管することも可能である。

【０５７８】

５）アドレスディレクトリサーバ連係

流通メッセージングサーバシステムは、アドレスディレクトリサーバが提供するサービス連係インターフェースを使って、アドレスディレクトリサーバと連係をする。アドレスディレクトリサーバは、２種類のアドレス検索サービスとアドレス登録サービス、アドレス変更サービスを提供するが、流通メッセージングサーバシステムは、アドレス検索サービス中、"公認電子アドレスに対する物理アドレス検索"サービスの連係機能は必須に提供する。

【０５７９】

検索サービスの他にアドレス登録およびアドレス変更サービスは、流通メッセージングサーバシステムが下位に登録／管理するユーザアカウントを企業や個人の公認電子アドレスとして使用できるか否かに応じて使用可否が決定される。流通メッセージングサーバシステムが登録／管理するユーザアカウントが公認電子アドレスとして登録可能となるように認証を受けた場合には、公認電子アドレスに対する登録および変更サービスを代行しなければならないので、アドレスディレクトリサーバの該当サービスを連係する。

【０５８０】

６）メッセージ検証

－流通メッセージングサーバシステムがメッセージを送受信する時、受信者は、メッセージの受信時点でメッセージの有効性に対する検証を遂行し、図４７に示すプロセスのように、受信者は、メッセージの有効性検証をした後、検証に通過した場合にのみメッセージの受信確認メッセージを送信者に伝達し、そうではない場合には、受信メッセージに対するエラーメッセージを転送する。

【０５８１】

－検証対象：受信メッセージのスキーマ検証（受信メッセージが流通プロトコルに応じて正確にパッケージングされたかを検証）、メッセージの無欠性検証（受信したメッセージの電子署名値を検証することによって、メッセージの偽変造が発生せずに無欠であるかを検証）、メッセージ送信者の検証（メッセージに電子署名をした送信者がメッセージに表記された送信者と一致するかを認証するために電子署名に使われた認証書とメッセージの送信者が同一であるかを検証）

【０５８２】

７）内部システム連係インターフェース

流通メッセージングサーバシステムは、内部システムが流通メッセージングサーバシステムを介して文書を転送し受信できるように送受信のための標準化されたインターフェースを提供するべきである。このインターフェースに対する詳細な内容は後述する［流通クライアントＡＰＰ］を参照する。

【０５８３】

８）流通証明書の発給および管理

流通証明書の基本要件は、１）流通証明書は発信および受信流通メッセージングサーバシステムが生成するということと、２）流通証明書はＧＰＫＩおよびＮＰＫＩ認証書を基盤に電子署名して生成されるということと、３）流通証明書は電子文書の流通行為を基準に生成（この時、１回の電子文書の流通時に１つ以上の電子文書が伝達される場合、１つの流通証明書を生成し、１つの電子文書流通のためには必ず該当流通を識別できるＩＤが付与され、これを基準にした流通で流通証明書を生成する）されるということである。

【０５８４】

流通証明書の発給時点で考慮しなければならない内容は、１）流通証明書の一連番号は個別の送受信個体が生成するので、唯一性の付与のために、既存の証明書の規格とは異なって２０ｂｙｔｅ乱数を使用するということと、２）流通証明の更新および廃止は定義しないということと、３）流通証明書を生成する流通メッセージングサーバシステムおよび流通クライアントＡＰＰのシステム時刻は常に現在時刻を維持しなければならないということと、４）流通証明書政策は技術規格で定義されたＯＩＤおよび名称だけを使用するということである。

【０５８５】

流通証明書の発給プロセスは図４８に示す通りであり、流通証明書の類型および生成に必要な必須情報は下記表１４１の通りであり、流通証明書の必須情報の獲得方法は下記表１４２の通りである。

【０５８６】

【表１４１】

【表 141】

類型	生成主体/時点	目的	必須情報
受信 証明書	受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞｼｽﾃﾑ/受信直後	受信者のﾒｯｾｰｼﾞの受信事実に対する否認防止	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
閲覧 証明書	受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞｼｽﾃﾑ/担当者の閲覧直後	受信者の受信ﾒｯｾｰｼﾞの閲覧事実に対する否認防止	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
送信 証明書	電子文書流通ﾊﾌﾞ/送信依頼ﾒｯｾｰｼﾞの受信直後	送信者の送信試みに対する証明	文書情報、送信者、受信者、送信者の送信依頼時刻

【０５８７】

【表１４２】

【表 142】

類型	必須情報	生成方法
受信証明書	文書情報、送信者、受信者、送信者の送信時刻	送信者が転送した流通ﾒｯｾｰｼﾞ内のﾌｨｰﾙﾄﾞ値を利用
	受信者の受信時刻	受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞｼｽﾃﾑの時刻を利用
閲覧証明書	文書情報、送信者、受信者、送信者の送信時刻	送信者が転送した流通ﾒｯｾｰｼﾞ内のﾌｨｰﾙﾄﾞ値を利用
	受信者の受信時刻、受信者の閲覧時刻	受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞｼｽﾃﾑの時刻を利用
送信証明書	文書情報、送信者、受信者	送信者が転送した流通ﾒｯｾｰｼﾞ内のﾌｨｰﾙﾄﾞ値を利用
	送信者の送信依頼時刻	電子文書流通ﾊﾌﾞｼｽﾃﾑの時刻を利用

【０５８８】

流通証明書は送受信個体が生成し、送受信個体のＮＰＫＩおよびＧＰＫＩ認証書を利用して電子署名し、流通証明書の基本構造はＣＭＳ標準のＳｉｇｎｅｄＤａｔａ構造を使用し、証明書と同一のコンテンツ識別子を使用する。

流通証明書のｃｏｎｔｅｎｔＴｙｐｅは次の通りである。

【０５８９】

```
ｉｄ－ｋｉｅｃ－ａｒｃＣｅｒｔＲｅｓｅｐｏｎｓｅ ＯＢＪＥＣＴ ＩＤＥＮＴＩＦＩＥＲ ：：＝ ｛ ｉｓｏ（１） ｍｅｍｂｅｒ－ｂｏｄｙ（２） ｋｏｒｅａ（４１０） ｋｉｅｃ（２００３２） ｃｅｒｔｉｆｉｃａｔｅ（２） ２ ｝
    ＡＲＣＣｅｒｔＲｅｓｐｏｎｓｅ ：：＝ ＣＨＯＩＣＥ ｛
    ａｒｃＣｅｒｔＩｎｆｏ                [０] ＥＸＰＬＩＣＩＴ ＡＲＣＣｅｒｔＩｎｆｏ，
    ａｒｃＥｒｒｏｒＮｏｔｉｃｅ          [１] ＥＸＰＬＩＣＩＴ ＡＲＣＥｒｒｏｒＮｏｔｉｃｅ ｝
```

流通証明書の基本フィールドは次の通りである。

```
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
　　｝
前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、次の通りである。
１）ｖｅｒｓｉｏｎ、バージョン
－流通証明書構造のバージョンを示す。流通証明書のためにはｖ２に設定するべきであり、ｔａｒｇｅｔフィールドにｄａｔａＨａｓｈを使う。
ＡＲＣＶｅｒｓｉｏｎ　：：＝　ＩＮＴＥＧＥＲ　｛ｖ１（１），　ｖ２（２）｝
２）Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ、一連番号
【０５９０】
－流通証明書の識別情報を示す。流通証明書は、電子文書を受信した送受信個体が生成するので、一連番号方式の識別番号は意味がない。また、送受信個体の流通クライアントが再設置されるなどの場合には、一連番号の維持が不可能である。
したがって、流通証明書の識別情報は２０ｂｙｔｅ乱数を使う。流通証明書を処理するためには２０ｂｙｔｅ乱数を処理できなければならない。
ＳｅｒｉａｌＮｕｍｂｅｒ　：：＝　ＩＮＴＥＧＥＲ
３）ｉｓｓｕｅｒ、証明書の発給者
【０５９１】
－流通証明書を発給する発給者の認証書識別値を入れる。本フィールドの値は流通証明書を電子署名した署名者の認証書内のＳｕｂｊｅｃｔＮａｍｅフィールドと同一の値を有しなければならない。
４）ｄａｔｅＯｆＩｓｓｕｅ、証明書の発給日
－発給者が流通証明書を発給した時点を示す。
５）ｄａｔｅＯｆＥｘｐｉｒｅ、証明書の効力満期日
－流通証明書の満了時点を示す。
６）ｐｏｌｉｃｙ、証明書政策
－流通証明書政策を示す。全ての流通証明書内の政策ＯＩＤは証明書の種類に応じて異なり、技術規格において格納した値のみを使用するべきである。
－流通証明書は証明書の種類に応じて一括的に１つのＯＩＤを有する。
【０５９２】
－Ｑｕａｌｉｆｉｅｒ値としてはＵｓｅｒＮｏｔｉｃｅ＞ＥｘｐｌｉｃｉｔＴｅｘｔ＞ＤｉｓｐｌｙＴｅｘｔにＵＴＦ８Ｓｔｒｉｎｇ形式で表され、指定された文章を使う。
－流通証明書の類型に応じて下記表１４３のような政策情報を使用するべきである。
【０５９３】
【表１４３】

【表 143】

証明書の種類	政策 OID	Qualifier
発信証明書	1.2.410.200032.2.?.1	発信証明書
受信証明書	1.2.410.200032.2.?.2	受信証明書
受信確認証明書	1.2.410.200032.2.?.3	受信確認証明書

【０５９４】
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。
ＲｅｑｕｅｓｔＩｎｆｏ：：＝　ＣＨＯＩＣＥ　｛
ａｒｃＣｅｒｔＲｅｑｕｅｓｔ　ＡＲＣＣｅｒｔＲｅｑｕｅｓｔ、
ｎｕｌｌ　ＮＵＬＬ　｝

８）ｔａｒｇｅｔ、証明対象
【０５９５】
－流通された全体電子文書のハッシュ値を指定する。本フィールドは必ずｄｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓ方式を使用するべきである。ｏｐＲｅｃｏｒｄおよびｏｒｇＡｎｄＩｓｓｕｅｄ、ｄａｔａＨａｓｈフィールドに対する構造は、第３者保管機関の'証明書フォーマットおよび運用手続き技術規格'を参照する。
－流通される電子文書に対する情報はＤｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓフィールドに含まれる。

```
ＴａｒｇｅｔＴｏＣｅｒｔｉｆｙ　：：＝　ＣＨＯＩＣＥ　｛
　　ｏｐＲｅｃｏｒｄ　　［０］　ＥＸＰＬＩＣＩＴ
ＯｐｅｒａｔｉｏｎＲｅｃｏｒｄ，
　　ｏｒｇＡｎｄＩｓｓｕｅｄ　　［１］　ＥＸＰＬＩＣＩＴ
ＯｒｉｇｉｎａｌＡｎｄＩｓｓｕｅｄＤｏｃｕｍｅｎｔＩｎｆｏ，
　　ｄａｔａＨａｓｈ　　［２］　ＥＸＰＬＩＣＩＴ
ＨａｓｈｅｄＤａｔａＩｎｆｏ
　　ｄｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓ　　［１０］　ＥＸＰＬＩＣＩＴ
　ＤｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓ｝
　　ＤｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓ　：：＝　ＳＥＱＵＥＮＣＥ　ＯＦ　Ｄｉ
ｓｔｒｉｂｕｔｉｏｎＩｎｆｏ
　　ＤｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏ　：：＝　ＳＥＱＵＥＮＣＥ　｛
　　ｓｅｎｄｅｒＡｄｄ　　ＧｅｎｅｒａｌＮａｍｅｓ，
　　ｒｅｃｅｉｖｅｒＡｄｄ　　ＧｅｎｅｒａｌＮａｍｅｓ，
　　ｄａｔｅＯｆＳｅｎｄ　　ＧｅｎｅｒａｌｉｚｅｄＴｉ
ｍｅ，
　　ｄａｔｅＯｆＲｅｃｅｉｖｅ　　［０］　ＥＸＰＬＩＣＩＴ
ＧｅｎｅｒａｌｉｚｅｄＴｉｍｅ　ＯＰＴＩＯＮＡＬ，
　　ｄａｔｅＯｆＲｅｃｅｉｖｅＣｏｎｆｉｒｍ　　［１］　ＥＸＰＬＩＣＩＴ
ＧｅｎｅｒａｌｉｚｅｄＴｉｍｅ　ＯＰＴＩＯＮＡＬ，
　　ｄｉｓｔｒｉｂｕｔｉｏｎＩｄ　　ＩＮＴＥＧＥＲ，
　　ｎｕｍｂｅｒＯｆＦｉｌｅｓ　　ＩＮＴＥＧＥＲ，
　　ｄｉｓｔｒｉｂｕｔｅｄＦｉｌｅＩｎｆｏｓ　　ＤｉｓｔｒｉｂｕｔｅｄＦｉ
ｌｅＩｎｆｏｓ｝
```

１）－１）ｓｅｎｄｅｒＡｄｄ、公認電子アドレス
－送信者の公認電子アドレスを示す。
１）－２）ｒｅｃｅｉｖｅｒＡｄｄ、受信者の公認電子アドレス
－受信者の公認電子アドレスを示す。
１）－３）ｄａｔｅＯｆＳｅｎｄ、送信日時
－送信者が電子文書を発送した時点を示す。
－送信証明書の場合、送信者が電子文書流通ハブに送信依頼した時刻を指定する。
－送信証明書は本フィールドのみを含むべきであり、ｄａｔｅＯｆＲｅｃｅｉｖｅおよびｄａｔｅＯｆＲｅｃｅｉｖｅＣｏｎｆｉｒｍは含んではいけない。
１）－４）ｄａｔｅＯｆＲｅｃｅｉｖｅ、受信日時
【０５９６】
－受信者が電子文書を受信した時点を示す。該当時点は証明書を生成した時点より同じであるか以前であるべきである。受信証明書および閲覧証明書は必ず本フィールドを含むべきである。送信証明書は本フィールドを含んではいけない。
１）－５）ｄａｔｅＯｆＲｅｃｅｉｖｅＣｏｎｆｉｒｍ、閲覧日時
【０５９７】
－受信者が電子文書を受信して確認した時点を示す。該当時点は受信日時より同じであるか以後であるべきであり、証明書を生成した時点より同じであるか以前であるべきであ

る。閲覧証明書は必ず本フィールドを含むべきである。送信証明書および受信証明書は必ず本フィールドを含んではいけない。

１）－６）ｄｉｓｔｒｉｂｕｔｉｏｎＩｄ、流通識別値

【０５９８】

－電子文書の流通件に対する識別値を示す。本フィールドの生成のために２０ｂｙｔｅ乱数を生成して使う。本フィールド値は、電子文書流通に対して流通メッセージに付与される識別値を意味する。

１）－７）ｎｕｍｂｅｒＯｆＦｉｌｅｓ、流通ファイル個数

－流通時に１つ以上の電子文書が伝達されてもよく、本フィールドは１回の流通で伝達されるファイルの個数を示す。

１）－８）ｄｉｓｔｒｉｂｕｔｅｄＦｉｌｅＩｎｆｏｓ、流通文書情報

－流通時に１つ以上の電子文書が伝達されてもよく、本フィールドには伝達される全ての文書に対する情報が含まれるべきである。

ＤｉｓｔｒｉｂｕｔｅｄＦｉｌｅＩｎｆｏｓ：：＝ ＳＥＱＵＥＮＣＥ ＯＦ ＤｉｓｔｒｉｂｕｔｅｄＦｉｌｅ

ＤｉｓｔｒｉｂｕｔｅｄＦｉｌｅ：：＝ ＳＥＱＵＥＮＣＥ ｛

ｆｉｌｅＨａｓｈｅｄＤａｔａ ＨａｓｈｅｄＤａｔａＩｎｆｏ、

ｆｉｌｅＩｄ ［０］ ＵＴＦ８Ｓｔｒｉｎｇ ＯＰＴＩＯＮＡＬ、

ｆｉｌｅＮａｍｅ ［１］ ＵＴＦ８Ｓｔｒｉｎｇ ＯＰＴＩＯＮＡＬ

｝

１）－８）－１）ｆｉｌｅＨａｓｈｅｄＤａｔａ、ファイルハッシュ情報

－本フィールドは流通して伝達された電子文書に対するハッシュ値を示す。

１）－８）－２）ｆｉｌｅＩｄ、ファイル識別値

【０５９９】

－流通される電子文書に識別値を付与した場合に該当文書に対する識別値を指定する。ファイル識別値は送信者が生成し、電子文書を受信者に伝達する時に共に伝達されるべきである。受信者は、伝達を受けたファイル識別値を利用して本フィールドに適用するべきである。

－送信者は、本フィールドの生成のためにｕｕｉｄ方式で生成するべきである。

【０６００】

－本フィールドは選択的に使われてもよいが、ｆｉｌｅＮａｍｅフィールドを使用しない場合には必ず使われるべきであり、ｆｉｅｌｄフィールドの使用を勧告する。

１）－８）－３）ｆｉｌｅＮａｍｅ、ファイル名

【０６０１】

－流通される電子文書に対するファイル名を示す。ファイル名は送信者が指定し、電子文書を受信者に伝達する時に共に伝達されるべきである。受信者は、伝達を受けたファイル識別値を利用して本フィールドに適用するべきである。

－本フィールドは選択的に使われてもよいが、ｆｉｌｅＩＤフィールドを使用しない場合には必ず使われるべきである。

上述したような流通証明書の時刻情報関連の整合性基準は下記表１４４の通りである。

【０６０２】

【表１４４】

【表 144】

番号	ﾌｨｰﾙﾄﾞ	内容
1	dateOfSend	送信日時/送信依頼日時
2	dateOfReceive	受信日時
3	dateOfReceiveConfirm	閲覧日時
4	dateOfIssue	証明書発給日
5	dateOfExpire	証明書効力満期日

【０６０３】
時刻情報の順序は発送日時＜受信日時≦閲覧日時≦証明書の発給日＜証明書の効力満期日であり、流通証明書の検証時に時刻情報が前記順序に沿っているか否かを確認しなければならない。
流通証明書の検証は、証明書構造の検証、証明書の電子署名の検証、証明書の主要フィールドの確認、証明書の時刻情報の整合性の検証を含む。
証明書構造の検証は、証明書がＡＳＮ．１で定義されたものと同一であるかを検証する過程である。
証明書の電子署名の検証は、流通証明書に適用された電子署名を検証する過程である。
【０６０４】
証明書の主要フィールドの確認は、ｖｅｒｓｉｏｎフィールド値がｖ２であるかを確認するバージョンフィールドの確認、ｔａｒｇｅｔフィールドがｈａｓｈＤａｔａであるかを確認するｔａｒｇｅｔフィールドの確認、電子署名に使われた認証書のＤＮと証明書の基本フィールドのＤＮが同一であるかを検証する発給者情報の検証、ｒｅｑｕｅｓｔＩｎｆｏフィールドがＮｕｌｌであるかを確認するｒｅｑｕｅｓｔＩｎｆｏフィールドの確認、ｄｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓ拡張フィールドが存在するかを確認し、ｃｒｉｔｉｃａｌがＴＲＵＥであるかを確認する拡張フィールドの確認、ｎｕｍｂｅｒＯｆＦｉｌｅｓフィールドの値とｄｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓ拡張フィールド内のＤｉｓｔｒｉｂｕｔｅｄＦｉｌｅの個数が同一であるかを確認するファイル個数の確認、ｔａｒｇｅｔフィールドのハッシュ値とｄｉｓｔｒｉｂｕｔｉｏｎＩｎｆｏｓ拡張フィールドのハッシュ値が同一であるかを確認するｔａｒｇｅｔフィールドハッシュ値の確認、流通証明書の時刻情報の整合性の検証基準に応じて検証する時刻情報の整合性の検証を含む。
証明書の時刻情報の整合性の検証は、流通証明書の時刻情報の整合性の検証基準に応じて検証する。
【０６０５】
一方、流通証明は、電子文書の流通過程で発生した発信、受信、受信確認に対する事実に対して信頼性のある方式で証明する行為をいう。流通証明は別途の応用プログラムで遂行し、流通証明書ビューアーおよび流通証明ＡＰＩにおいては遂行しない。流通証明は、流通証明書の検証に追加的に遂行しようとする場合に、次の内容を遂行する。
－流通証明書の検証：流通証明書の検証を遂行する。
－流通証明書政策の確認：発信、受信、受信確認に対する流通証明書政策ＯＩＤおよびＱｕａｌｉｆｉｅｒ値を確認する。
－送信者のアドレス確認：電子文書を発送した送受信個体のアドレスが正確であるかを確認する。
－受信者のアドレス確認：電子文書を受信した送受信個体のアドレスが正確であるかを確認する。

－発送日時の確認：送信者が電子文書を発送した時刻が正確であるかを確認する。
－受信日時の確認：受信者が電子文書を受信した時刻が正確であるかを確認する。
－受信確認日時の確認：受信者が電子文書を受信確認した時刻が正確であるかを確認する。

【０６０６】
－流通ＩＤの確認：流通個別件に付与された流通ＩＤが正確であるかを確認する。送信者および受信者が流通ＩＤを別途に保管して管理する場合、これを比較して管理することができる。

【０６０７】
－流通ファイルの識別子またはファイル名の確認：流通されるファイルのＩＤまたはファイル名が正確であるかを確認する。送信者および受信者がファイルＩＤおよびファイル名を別途に保管して管理する場合、これを比較して管理することができる。

【０６０８】
－流通ファイルのハッシュ値の確認：流通対象となるファイルの各々のハッシュ値と拡張フィールドのＤｉｓｔｒｉｂｕｔｅｄＦｉｌｅフィールドの値が同一であるかを確認する。この時に使うハッシュアルゴリズムは流通証明書内に指定されたもので遂行して比較する。

【０６０９】
一方、流通証明書プロファイルは下記表１４５の通りであり、考慮する事項は、電子署名はＲＳＡ２０４８ｂｉｔおよびＳＨＡ２５６アルゴリズムを適用するということと、ｓｉｇｎｅｄＤａｔａ構造において認証書は必ず含まれるべきであるということと、ｓｉｇｎｅｒＩｎｆｏｓフィールドには１つのｓｉｇｎｅｒＩｎｆｏだけが含まれるということである。

【０６１０】

【表１４５】

【表 145】

基本ﾌｨｰﾙﾄﾞ	内容	特異事項
version	ﾊﾞｰｼﾞｮﾝ	V3
serialNumber	一連番号	20byte 乱数
dateOfIssue	発給日時	GeneralizedTime
dateOfExire	証明書の効力満期日時	GeneralizedTime
policy	証明書政策	OID:1.2.410.200032.2.?.?
requestInfo	証明書の要請ﾒｯｾｰｼﾞ情報	null
target	証明対象	distributionInfos 構造使用
senderAdd	送信者の公認電子ｱﾄﾞﾚｽ	
receiverAdd	受信者の公認電子ｱﾄﾞﾚｽ	
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	20byte 乱数乱数
numaberOfFiles	転送ﾌｧｲﾙ個数	
distributedFileInfos	転送ﾌｧｲﾙ情報	1 つ以上の distributedFile
distributedFile		
fileHachedData	ﾌｧｲﾙﾊｯｼｭ値	SHA256
FileId	ﾌｧｲﾙ ID	fileid と filename の 2 つのﾌｨｰﾙﾄﾞのうちの 1 つは必須
Filename	ﾌｧｲﾙ名	

【０６１１】

上述したような流通証明書を第３者保管機関と連係する方案は、流通証明書を発給すると同時に第３者保管機関に格納（保管）依頼することにより、発給された流通証明書の信頼性が保証されるものである。

【０６１２】

第３者保管機関事業者の流通メッセージングサーバシステムの場合の流通証明書の保管プロセスは図４９の通りであり、流通メッセージングサーバシステムにおいて発給した流通証明書を直接第３者保管機関連係モジュールを介して第３者保管機関内部に保管要請をし、第３者保管機関連係モジュールは流通証明書の保管要請モジュールと第３者保管機関連係インターフェースクライアントモジュールとから構成され、既存の第３者保管機関連係インターフェース規格に応じて第３者保管機関に保管される。

【０６１３】

一般送受信個体の流通メッセージングサーバシステムの場合の流通証明書の保管プロセスは図５０の通りであり、発給された流通証明書の保管のために第３者保管機関事業者に

要請をするために第３者保管機関事業者の流通メッセージングサーバシステムに要請メッセージを伝達し、外部から流通証明書の保管要請を受けた第３者保管機関事業者の流通メッセージングサーバシステムは第３者保管機関連係モジュールを介して第３者保管機関の内部に保管要請をし、第３者保管機関連係モジュールは既存の第３者保管機関連係インターフェース規格に応じて第３者保管機関に保管要請をする。

送受信個体が流通証明書を第３者保管機関に保管する詳細処理は図５１に示すような手続きからなり、詳細な説明は次の通りである。

【０６１４】

○流通証明書登録者

－第３者保管機関に流通証明書を保管する時に、第３者保管機関事業者と送受信個体間の契約によって保管代行者を指定することができ、第３者保管機関事業者は保管代行者が登録者となって保管代行者の公認認証書を基盤に流通証明書を保管するようになる。

○第３者保管機関への保管要請プロセスの類型

【０６１５】

－第３者保管機関事業者は同期式または非同期式処理のうちの１つ以上を提供するべきであり、流通メッセージングサーバは連係しようとする第３者保管機関事業者が提供する方式に応じて連係する。

【０６１６】

－Ｃａｓｅ１：同期式処理プロセス（送信者が流通証明書の保管要請時、第３者保管機関に登録が完了した後に登録証明書が発給される全てのプロセスが同期式で行われることにより、送信者の流通メッセージングサーバは同期式応答メッセージで登録証明書の伝達を受ける。要請に対する応答メッセージが最終的な第３者保管機関の登録結果であるため、保管要請に対するエラー発生時の再処理は送信者の流通メッセージングサーバが遂行するべきである）

【０６１７】

－Ｃａｓｅ２：非同期式処理プロセス（送信者が第３者保管機関の流通メッセージングサーバに流通証明書の保管要請をすれば、第３者保管機関の流通メッセージングサーバが先に要請メッセージの有効性を検証した後、保管要請を受け付ける。第３者保管機関事業者は、保管要請メッセージに応じて、第３者保管機関に登録し発給を受けた登録証明書を最初保管要請者である送信者の流通メッセージングサーバに伝達するべきである。受け付けた保管要請に対して第３者保管機関に登録することは第３者保管機関事業者の責任であるため、保管エラー発生時の再処理も第３者保管機関事業者が遂行するべきである）

【０６１８】

［流通プロトコル］

以下では、上述したような本発明の好ましい実施形態による電子文書流通システムおよび方法に適用される流通プロトコルについて詳細に説明する。

本発明の好ましい実施形態による電子文書流通システムおよび方法に適用される流通プロトコルを説明するにおいて、"１）メッセージパッケージング"、"２）メッセージ封筒構成"、"３）ＨＴＴＰバインディング"について順に説明する。

【０６１９】

１）メッセージパッケージング

流通プロトコルのメッセージ構造はｅｂＭＳ　Ｖ２．０規格を準用し、２つの論理的なＭＩＭＥパートを持つ。

【０６２０】

１番目のＭＩＭＥパートは、ＳＯＡＰメッセージを含み、ヘッダコンテナーと呼ばれ、ＳＯＡＰメッセージは、ＨｅａｄｅｒとＢｏｄｙとから構成され、２番目のＭＩＭＥパートは、０個以上の追加のＭＩＭＥパートであって、ペイロードコンテナーと呼ばれるが、アプリケーションレベルの添付文書を含む。

【０６２１】

このような流通メッセージの基本的な構造は図５２の通りであり、Ｓｉｍｐｌｅ　Ｏｂ

ｊｅｃｔ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ（ＳＯＡＰ）１．１および、ＳＯＡＰ Ｍｅｓｓａｇｅｓ ｗｉｔｈ Ａｔｔａｃｈｍｅｎｔのような標準規格を遵守する。

【０６２２】

流通メッセージパッケージの全てのＭＩＭＥ Ｈｅａｄｅｒ要素は、ＳＯＡＰ Ｍｅｓｓａｇｅｓ ｗｉｔｈ Ａｔｔａｃｈｍｅｎｔｓ規格を遵守する。さらに、メッセージパッケージ内のＣｏｎｔｅｎｔ－Ｔｙｐｅ ＭＩＭＥ Ｈｅａｄｅｒは、必ずＳＯＡＰメッセージ文書を含むＭＩＭＥ Ｂｏｄｙ部分のＭＩＭＥメディア類型と同一のｔｙｐｅ属性を有する。ＳＯＡＰ規格によれば、ＳＯＡＰメッセージのＭＩＭＥメディア類型は"ｔｅｘｔ／ｘｍｌ"値を有するべきであるとなっている。

【０６２３】

ルート部分は、［ＲＦＣ２０４５］に準ずる構造を有するＣｏｎｔｅｎｔ－ＩＤ ＭＩＭＥヘッダを含み、Ｍｕｌｔｉｐａｒｔ／Ｒｅｌａｔｅｄメディア類型に対する必須のパラメータに追加して、ｓｔａｒｔパラメータ（［ＲＦＣ２３８７］においては選択事項）が常に存在するべきである。ｍｕｌｔｉｐａｒｔ／ｒｅｌａｔｅｄメッセージパッケージのＭＩＭＥヘッダの例題は次の表１４６の通りである。

【０６２４】

【表１４６】

【表 146】

```
Content-Type: multipart/related; type="text/xml"; boundary="boundaryValue";
start=messagepackage-123@example.com

--boundaryValue
Content-ID: <messagepackage-123@example.com>
```

【０６２５】

以下では、本発明による流通メッセージについて説明するにおいて、メッセージパッケージのルートＢｏｄｙ部分をＨｅａｄｅｒ（ヘッダ）コンテナーと定義する。Ｈｅａｄｅｒコンテナーは、ＭＩＭＥ Ｂｏｄｙ部分として、ＳＯＡＰ Ｍｅｓｓａｇｅｓ ｗｉｔｈ Ａｔｔａｃｈｍｅｎｔ明細で定義したように１つのＳＯＡＰメッセージを含む。

【０６２６】

ヘッダコンテナーのＭＩＭＥ Ｃｏｎｔｅｎｔ－Ｔｙｐｅ ｈｅａｄｅｒは、ＳＯＡＰ規格に応じ、"ｔｅｘｔ／ｘｍｌ"値を有するべきである。Ｃｏｎｔｅｎｔ－Ｔｙｐｅヘッダは"ｃｈａｒｓｅｔ"属性を含んでもよく、例題は次の表１４７の通りである。

【０６２７】

【表１４７】

【表 147】

```
Content-Type: text/xml; charset="UTF-8"
```

【０６２８】

ＭＩＭＥ ｃｈａｒｓｅｔ属性は、ＳＯＡＰメッセージを生成するのに用いられる文字群を識別するために使われる。この属性の意味論は、［ＸＭＬＭｅｄｉａ］に明示されたｔｅｘｔ／ｘｍｌの"ｃｈａｒｓｅｔ ｐａｒａｍｅｔｅｒ／ｅｎｃｏｄｉｎｇ ｃｏｎ

ｓｉｄｅｒａｔｉｏｎ"に説明されている。有効な値の目録はｈｔｔｐ：／／ｗｗｗ．ｉａｎａ．ｏｒｇ／から探すことができる。

【０６２９】

仮に２つが全て含まれていれば、ＭＩＭＥ　ｃｈａｒｓｅｔ属性はＳＯＡＰメッセージのエンコード宣言部と同一であるべきである。仮に提供されているとすれば、ＭＩＭＥ　ｃｈａｒｓｅｔ属性は、ＳＯＡＰメッセージを生成する時にエンコードと相反する値を含んでいてはいけない。

【０６３０】

この文書をエンコードする時は、最大限の互換性のために、必ず［ＵＴＦ－８］を使用するべきである。ｔｅｘｔ／ｘｍｌ［ＸＭＬＭｅｄｉａ］から導き出したメディア類型のために定義された処理規則のためにこのＭＩＭＥ属性は基本値を有しない。

ヘッダコンテナーの例題は下記表１４８の通りである。

【０６３１】

【表１４８】

【表 148】

```
Content-ID: <messagepackage-123@example.com>                    ---| Header
Content-Type: text/xml; charset="UTF-8"                            |
                                                                   |
<SOAP:Envelope                                          --|SOAP Message |
   xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"> |       |
  <SOAP:Header>                                            |       |
   ...                                                     |       |
  </SOAP:Header>                                           |       |
  <SOAP:Body>                                              |       |
   ...                                                     |       |
  </SOAP:Body>                                             |       |
</SOAP:Envelope>                                        --|       |
                                                                   |
--boundaryValue                                                 ---|
```

【０６３２】

ＳＯＡＰ　Ｍｅｓｓａｇｅｓ　ｗｉｔｈ　Ａｔｔａｃｈｍｅｎｔｓ規格に応じて、メッセージパッケージ内には０個以上のペイロードコンテナーが含まれてもよい。仮にメッセージパッケージがアプリケーションペイロードを含んでいるのであれば、これは、必ずペイロードコンテナーに含まれるべきである。

【０６３３】

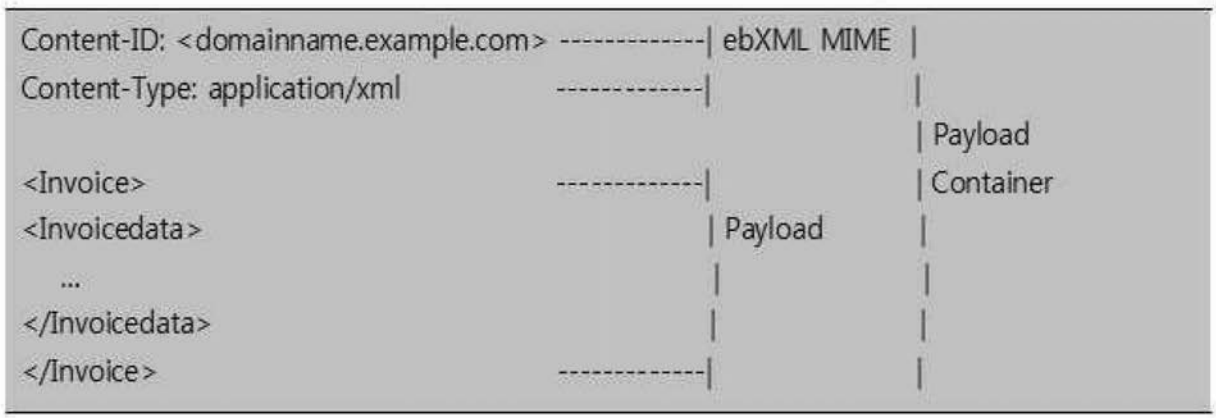
仮に、メッセージパッケージがアプリケーションペイロードを含んでいないのであれば、ペイロードコンテナーを表示してはいけない。各ペイロードコンテナーの内容物は、ＳＯＡＰ　Ｂｏｄｙ内のｅｂＸＭＬメッセージのＭａｎｉｆｅｓｔ要素によって識別されなければならない。

【０６３４】

ｅｂＸＭＬメッセージサービスの明細は、アプリケーションペイロードの構造と内容物に対し、いかなる規定もいかなる方法の制約も定めていない。ペイロードは、ｓｉｍｐｌｅ－ｐｌａｉｎ－ｔｅｘｔオブジェクトまたは複雑に重なった色々な部分のオブジェクトもなり得る。ペイロードオブジェクトの構造と構成に対する明細は、ｅｂＸＭＬメッセージサービスを使用する業務プロセスや情報交換をどのように定義するかによって変わり得

る。ペイロードコンテナーの例題は次の表１４９の通りである。
【０６３５】
【表１４９】

【表 149】



【０６３６】
本発明による流通メッセージの全てのＭＩＭＥ部分は、［ＲＦＣ２０４５］規格に準ずる追加のＭＩＭＥヘッダを含むことができる。実現時には、この発明で定義されていないＭＩＭＥヘッダを無視することもでき、識別できないＭＩＭＥヘッダらは必ず無視するべきである。例えば、実現時にｃｏｎｔｅｎｔ－ｌｅｎｇｔｈをメッセージに含むことができるが、ｃｏｎｔｅｎｔ－ｌｅｎｇｔｈが表れているメッセージの受給者はこれを無視することもできる。
【０６３７】
２）メッセージ封筒構成
ＳＯＡＰ規格に準じて全ての拡張要素内容は有効なネームスペースに限定されるべきである。本発明で定義された全てのｅｂＸＭＬ　ＳＯＡＰ拡張要素内容は、ｅｂＸＭＬ　ＳＯＡＰ　Ｅｎｖｅｌｏｐｅ拡張ネームスペースに限定されるべきである。ネームスペース宣言部は、ＳＯＡＰ　Ｅｎｖｅｌｏｐｅ、ＨｅａｄｅｒまたはＢｏｄｙ要素に含まれているか、各ＳＯＡＰ拡張要素に直接含まれてもよい。
【０６３８】
ＳＯＡＰ　Ｅｎｖｅｌｏｐｅは、ＳＯＡＰメッセージのＲｏｏｔ項目としてＳＯＡＰメッセージ内の各種Ｎａｍｅｓｐａｃｅを宣言する。宣言するべきＮａｍｅｓｐａｃｅは次の表１５０の通りである。
【０６３９】
【表１５０】

【表 150】

項目	Namespace URL
SOAP	http://schemas.xmlsoap.org/soap/envelope
Digital Signature	http://www.w3.org/2000/09/xmldsig#
xlink	http:// www.w3.org/1999/xlink
xsi	http:// www.w3.org/2001/XMLSchema-instance

メッセージ封筒のスキーマ構造は図１０２の通りであり、メッセージ封筒の例題は下記表１５１の通りである。

【０６４０】
【表１５１】

【表 151】

```
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
  http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
 <SOAP:Header
  xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
  xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
  <eb:MessageHeader ...>
    ...
  </eb:MessageHeader>
 </SOAP:Header>
 <SOAP:Body
  xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
  xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
  http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
  <eb:Manifest eb:version="2.0">
    ...
  </eb:Manifest>
 </SOAP:Body>
</SOAP:Envelope>
```

【０６４１】
ＳＯＡＰ　Ｅｎｖｅｌｏｐｅ要素の子要素であるＳＯＡＰ　Ｈｅａｄｅｒ要素とＳＯＡＰ　Ｂｏｄｙ要素について順に詳細に説明すれば、次の通りである。
【０６４２】
ＳＯＡＰ　Ｈｅａｄｅｒ要素はＳＯＡＰ　Ｅｎｖｅｌｏｐｅ要素の１番目の子要素であり、ＭｅｓｓａｇｅＨｅａｄｅｒ、ＳｙｎｃＲｅｐｌｙ、Ｓｉｇｎａｔｕｒｅ、ＥｒｒｏｒＬｉｓｔのような拡張要素を含む。
【０６４３】
ＭｅｓｓａｇｅＨｅａｄｅｒはメッセージのルーティング情報（Ｔｏ／Ｆｒｏｍ、など）とメッセージに関する他の文脈情報を含む必須要素であり、ＳｙｎｃＲｅｐｌｙは次のＳＯＡＰノードに行く必須転送状態を示す要素であり、Ｓｉｇｎａｔｕｒｅはメッセージと関連したデータを署名する［ＸＭＬＤＳＩＧ］に準ずる電子署名を表示する要素であり、ＥｒｒｏｒＬｉｓｔは以前のメッセージを対象に報告されたエラー目録を入れた要素であり、以前のメッセージに対するエラーを報告する時にのみ使用されるが、このようなＭｅｓｓａｇｅＨｅａｄｅｒの要素の各々について詳細に説明すれば、次の通りである。
【０６４４】
ＭｅｓｓａｇｅＨｅａｄｅｒ要素は、全てのｅｂＸＭＬメッセージに表現されるべき必須要素として、必ずＳＯＡＰ　Ｈｅａｄｅｒ要素の子要素として表現されるべきである。

ＭｅｓｓａｇｅＨｅａｄｅｒ要素は次のような下位要素で構成された複合要素であり、ＭｅｓｓａｇｅＨｅａｄｅｒのｅｌｅｍｅｎｔ構造は下記表１５２の通りであり、ＭｅｓｓａｇｅＨｅａｄｅｒのスキーマ構造は図５４の通りである。

【０６４５】

【表１５２】

【表 152】

項目名	説明		反復回数	類型	長さ
From	ﾒｯｾｰｼﾞ送信の送受信個体情報		1..1		
	PartyId	■送信者を識別するｺｰﾄﾞ	1..1	S	13
	Role	■送信者役割	1..1	S	最大 256
To	■ﾒｯｾｰｼﾞ受信の送受信個体情報		1..1		
	Partyid	■受信者を識別するｺｰﾄﾞ	1..1	S	13
	Role	■受信者役割	1..1	S	最大 256
CPAID	■取引協業定義書 ID		1..1	S	最大 256
ConversationId	■送受信ﾄﾗﾝｻﾞｸｼｮﾝ区分子		1..1	S	最大 256
Service	■CPA に定義されたﾒｯｾｰｼﾞｻｰﾋﾞｽ		1..1	S	最大 256
Action	■ｻｰﾋﾞｽ内の特定業務ﾌﾟﾛｾｽ区分子 ■ｻｰﾋﾞｽ内の唯一の値		1..1	S	最大 256
Message Data	■ﾒｯｾｰｼﾞを識別するためのﾃﾞｰﾀ		1..1		
	MessageId	■1 つのﾒｯｾｰｼﾞが有する識別子	1..1	S	最大 256
	Timestamp	■ﾒｯｾｰｼﾞの生成時間 ■UTC 形式 ■ex>2008-07-31T06:29:39.724Z	1..1	S	24
	RefToMessage Id	■応答ﾒｯｾｰｼﾞにのみ存在 ■要請ﾒｯｾｰｼﾞの MessageId	0..1	S	最大 256

【０６４６】

ＳｙｎｃＲｅｐｌｙ要素は同期式送信を意味するものであって、ｉｄ属性、ｖｅｒｓｉｏｎ属性、ＳＯＡＰ　ａｃｔｏｒ属性（必ず"ｈｔｔｐ：／／ｓｃｈｅｍａｓ．ｘｍｌｓｏａｐ．ｏｒｇ／ｓｏａｐ／ａｃｔｏｒ／ｎｅｘｔ"値を有するべきである）、ＳＯＡＰ　ｍｕｓｔＵｎｄｅｒｓｔａｎｄ属性値を有し、ＳｙｎｃＲｅｐｌｙ要素の例題は次の表１５３の通りである。

【０６４７】

【表１５３】

【表 153】

```
<eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
 SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
```

【０６４８】
Ｓｉｇｎａｔｕｒｅ要素はＳＯＡＰ　Ｈｅａｄｅｒの子要素として必ず存在するべきであるが、これは、流通メッセージは上記で言及した危険要素に対応するために必ず電子的に署名されるべきであるためである。
［ＸＭＬＤＳＩＧ］規格に応じて電子署名を遂行する過程は次の通りである。
【０６４９】
先ず、ＳＯＡＰ　ＥｎｖｅｌｏｐｅにＳｉｇｎａｔｕｒｅＭｅｔｈｏｄ、ＣａｎｏｎｉｃａｌｉｚａｔｉｏｎＭｅｔｈｏｄ、Ｒｅｆｅｒｅｎｃｅ要素を有したＳｉｇｎｅｄＩｎｆｏ要素と必須ペイロードオブジェクトを［ＸＭＬＤＳＩＧ］に規定された通りに生成する。
【０６５０】
次に、正規化した後、［ＸＭＬＤＳＩＧ］に指定された通り、ＳｉｇｎｅｄＩｎｆｏに指定されたアルゴリズムを基準にＳｉｇｎｅｄＩｎｆｏのＳｉｇｎａｔｕｒｅＶａｌｕｅを算出する。
【０６５１】
次に、［ＸＭＬＤＳＩＧ］に指定された通り、ＳｉｇｎｅｄＩｎｆｏ、ＫｅｙＩｎｆｏ（勧告事項）、ＳｉｇｎａｔｕｒｅＶａｌｕｅ要素を含むＳｉｇｎａｔｕｒｅ要素を生成する。
次に、ＳＯＡＰ　ＨｅａｄｅｒのＳｉｇｎａｔｕｒｅ要素をＳＯＡＰ　Ｈｅａｄｅｒ要素に含ませる。
【０６５２】
上述したような電子署名時に使われるアルゴリズム情報は次の通りである。アルゴリズムは、Ｗ３Ｃ "ＸＭＬ－Ｓｉｇｎａｔｕｒｅ　Ｓｙｎｔａｘ　ａｎｄ　Ｐｒｏｃｅｓｓｉｎｇ"（ＲＦＣ３２７５）のアルゴリズム部分（６．０　Ａｌｇｏｒｉｔｈｍｓ）を基本的に従う。また、国内固有のアルゴリズムを支援するために、ＴＴＡＳ．ＩＦ－ＲＦＣ３０７５　"拡張性生成言語の電子署名構文と処理（ＸＭＬ－Ｓｉｇｎａｔｕｒｅ　Ｓｙｎｔａｘ　ａｎｄ　Ｐｒｏｃｅｓｓｉｎｇ）"（韓国情報通信技術協会、２００４年）で定義されたアルゴリズムを利用する。
【０６５３】
本発明による流通プロトコルにおいて利用するアルゴリズム目録は、電子署名ＮａｍｅＳｐａｃｅ、ハッシュ（Ｄｉｇｅｓｔ）、電子署名（Ｓｉｇｎａｔｕｒｅ）、正規化（Ｃａｎｏｎｉｃａｌｉｚａｔｉｏｎ）、変換（Ｔｒａｎｓｆｏｒｍ）を含む。メッセージ送受信時の電子署名の生成および検証過程における曖昧性を最小化するために、次の目録以外のアルゴリズムは使用しないことが好ましい。
電子署名のＮａｍｅｓｐａｃｅの例題は次の表１５４の通りである。
【０６５４】

【表１５４】

【表 154】

```
<... xmlns:ds="http://www.w3.org/2000/09/xmldsig#" ... >
```

【０６５５】
データを縮約するのに利用するアルゴリズムとしてＳＨＡ１とＳＨＡ２５６を利用することができ、例題は次の表１５５の通りである。但し、ＨＡ１は'公認認証書の暗号体系の高度化'が完全に適用される時点である２０１２年からはその使用が制限される。
【０６５６】
【表１５５】

【表 155】

```
<ds:SignatureMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#rsa-sha1”/>
or
<ds:SignatureMethod
Algorithm=”http://www.w3.org/2001/04/xmldsig-more#rsa-sha256”/>
```

【０６５７】
メッセージ電子署名時に使われるアルゴリズムはＲＳＡｗｉｔｈＳＨＡ１、ＲＳＡｗｉｔｈＳＨＡ２５６であり、例題は次の表１５６の通りである。但し、ＲＳＡｗｉｔｈＳＨＡ１を利用する場合は、'公認認証書の暗号体系の高度化'が完全に適用される時点である２０１２年からはその使用が制限される。
【０６５８】
【表１５６】

【表 156】

```
<ds:SignatureMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#rsa-sha1”/>
or
<ds:SignatureMethod
Algorithm=”http://www.w3.org/2001/04/xmldsig-more#rsa-sha256”/>
```

【０６５９】
論理的に同一な文書に対して物理的に色々な表現が可能なＸＭＬの特性のため、同じ文書に対して電子署名値が異に出ることがあるので、このような現象を防止するために必ず正規化（Ｃａｎｏｎｉｃａｌｉｚａｔｉｏｎ）過程を経るべきであり、例題は次の表１５７の通りである。正規化は、注釈のない正規ＸＭＬ（Ｃａｎｏｎｉｃａｌ　ＸＭＬ、ｏｍｉｔｓ　ｃｏｍｍｅｎｔｓ）を使う。
【０６６０】

【表１５７】

【表 157】

```
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

【０６６１】
全体ＸＭＬデータ中の実際の署名対象となるデータを加工し選択する過程を経るアルゴリズムとして様々な変換アルゴリズムが存在するが、その中の３つだけを利用するようにする。第１は電子署名が署名対象内に含まれる形式に従うのでＥｎｖｅｌｏｐｅｄ　Ｓｉｇｎａｔｕｒｅ変換であり、第２は前記で説明した正規化（Ｃａｎｏｎｉｃａｌｉｚａｔｉｏｎ）、そして第３は署名対象情報を選択するＸＰａｔｈフィルタリング（ＸＰａｔｈ　Ｆｉｌｔｅｒｉｎｇ）であり、例題は次の表１５８の通りである。
【０６６２】
【表１５８】

【表 158】

```
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
and
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
and
<ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
<ds:XPath>not(ancestor-or-self::node()[@SOAP:actor=&amp;quot;urn:oasis:names:tc:ebxml-msg:actor:next
MSH&amp;quot;]
        | ancestor-or-self::node()[@SOAP:actor= &amp;quot;http://schemas.xmlsoap.org/soap/
actor/next&amp;quot;])
    </ds:XPath>
</ds:Transform>
```

【０６６３】
電子署名構文の構造は図５５の通りであり、上述した方式の通りに電子署名が遂行されたメッセージの例題は次の表１５９の通りである。
【０６６４】

【表１５９】

【表 159】

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
 <SOAP:Header>
  <eb:MessageHeader eb:id="..." eb:version="2.0" SOAP:mustUnderstand="1">
  ...
  </eb:MessageHeader>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
   <SignedInfo>
    <CanonicalizationMethod
     Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <Reference URI="">
      <Transforms>
       <Transform
       Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
       <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
        <XPath> not(ancestor-or-self::node()[@SOAP:actor=
         &amp;quot;urn:oasis:names:tc:ebxml-msg:actor:nextMSH&amp;quot;]
         | ancestor-or-self::node()[@SOAP:actor=
         &amp;quot;http://schemas.xmlsoap.org/soap/actor/next&amp;quot;])
        </XPath>
       </Transform>
       <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
       </Transforms>
       <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
       <DigestValue>...</DigestValue>
    </Reference>
    <Reference URI="cid://blahblahblah/">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>...</DigestValue>
      <Transforms>
       <Transform
       Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
       <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
        <XPath> not(ancestor-or-self::node()[@SOAP:actor=
         &amp;quot;urn:oasis:names:tc:ebxml-msg:actor:nextMSH&amp;quot;]
         | ancestor-or-self::node()[@SOAP:actor=
         &amp;quot;http://schemas.xmlsoap.org/soap/actor/next&amp;quot;])
        </XPath>
       </Transform>
       <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
       </Transforms>
       <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
       <DigestValue>...</DigestValue>
    </Reference>
    <Reference URI="cid://blahblahblah/">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>...</DigestValue>
```

【０６６５】

Ｅｒｒｏｒｌｉｓｔ要素は、メッセージを受信して処理過程を遂行する時、エラーが発生する場合にのみＨｅａｄｅｒの下位に位置する。ＥｒｒｏｒＬｉｓｔ要素が生成される場合には、必ずＭｅｓｓａｇｅＨｅａｄｅｒ要素内にＲｅｆＴｏＭｅｓｓａｇｅＩｄが存在するべきであり、ＲｅｆＴｏＭｅｓｓａｇｅＩｄは、エラーが発生したメッセージのＭｅｓｓａｇｅＩｄを指し示さなければならない。ＥｒｒｏｒＬｉｓｔ要素はｉｄ属性、ＯＡＰ　ｍｕｓｔＵｎｄｅｒｓｔａｎｄ属性、ｖｅｒｓｉｏｎ属性、ｈｉｇｈｅｓｔＳｅｖｅｒｉｔｙ属性、１つ以上のＥｒｒｏｒ要素のような属性を有し、ＥｒｒｏｒＬｉｓｔの構造は図５６の通りである。この時、報告されるエラーがなければ、ＥｒｒｏｒＬｉｓｔ要素は存在してはいけない。

【０６６６】

ｈｉｇｈｅｓｔＳｅｖｅｒｉｔｙ属性は、全てのＥｒｒｏｒ要素の最も深刻な状態を表示する。特に、あるＥｒｒｏｒ要素がｓｅｖｅｒｉｔｙをＥｒｒｏｒに設定していれば、ｈｉｇｈｅｓｔＳｅｖｅｒｉｔｙはＥｒｒｏｒに設定するべきであり、そうではない場合には、ｈｉｇｈｅｓｔＳｅｖｅｒｉｔｙをＷａｒｎｉｎｇに設定するべきである。

【０６６７】

Ｅｒｒｏｒ要素は、ｉｄ属性、ｃｏｄｅＣｏｎｔｅｘｔ属性、ｅｒｒｏｒＣｏｄｅ属性、ｓｅｖｅｒｉｔｙ属性、ｌｏｃａｔｉｏｎ属性、Ｄｅｓｃｒｉｐｔｉｏｎ属性を有する。

ｉｄ属性は、文書内において、ＥｒｒｏｒＬｉｓｔ要素を唯一に識別する役割をする。

【０６６８】

ｃｏｄｅＣｏｎｔｅｘｔ属性は、ｅｒｒｏｒＣｏｄｅｓのネームスペースまたはスキーマを示す。これは、必ずＵＲＩでなければならない。この属性の基本値は、ｕｒｎ：ｏａｓｉｓ：ｎａｍｅｓ：ｔｃ：ｅｂｘｍｌ－ｍｓｇ：ｓｅｒｖｉｃｅ：ｅｒｒｏｒｓである。この属性に基本値がなければ、その明細の実現はｅｒｒｏｒＣｏｄｅｓを使うということを示す。

【０６６９】

必須属性であるｅｒｒｏｒＣｏｄｅ属性は、エラーを持つメッセージのエラーが有した本質を指示する。ｅｒｒｏｒＣｏｄｅの有効な値とコードの意味は下記で説明する。

【０６７０】

必須属性であるｓｅｖｅｒｉｔｙ属性はエラーの深刻性を示す値であって、有効な値はＷａｒｎｉｎｇ、Ｅｒｒｏｒがあるが、Ｗａｒｎｉｎｇは、エラーが存在するが、対話中の他のメッセージは正常に生成されることを示し、Ｅｒｒｏｒは、復旧不可能なエラーがメッセージに存在し、対話中にこれ以上他のメッセージは生成されないことを示す。

【０６７１】

ｌｏｃａｔｉｏｎ属性は、エラーが存在するメッセージ部分を指し示す。仮にエラーがｅｂＸＭＬ要素内に存在し、要素が"ｗｅｌｌ－ｆｏｒｍｅｄ"であれば、ｌｏｃａｔｉｏｎ属性の内容は［Ｘｐｏｉｎｔｅｒ］でなければならない。

【０６７２】

Ｄｅｓｃｒｉｐｔｉｏｎ属性の内容は、ｘｍｌ：ｌａｎｇ属性において定義された言語でエラーの叙述的な説明を提供する。通常、これは、ＸＭＬパーサーやメッセージを検証するソフトウェアが生成したメッセージとなる。この意味は、この内容はＥｒｒｏｒ要素を生成したソフトウェアの販売者や開発者によって定義されるということを意味する。

ＥｒｒｏｒＬｉｓｔの例題は次の表１６０の通りである。

【０６７３】

【表１６０】

【表 160】

```
<eb:ErrorList eb:id="3490sdo", eb:highestSeverity="error" eb:version="2.0"
SOAP:mustUnderstand="1">
 <eb:Error eb:errorCode="SecurityFailure" eb:severity="Error"eb:location="URI_of_ds:Signature">
   <eb:Description xml:lang="en-US">Validation of signature failed<eb:Description>
  </eb:Error>
  <eb:Error ...> ... </eb:Error>
</eb:ErrorList>
```

【０６７４】

流通プロトコルを基盤にメッセージを送受信する過程でエラーが発生すれば、エラーを認知した送受信個体は相手方にエラー内容を報告するべきであり、報告するべきエラーはメッセージ構造エラー、信頼メッセージングエラー、保安エラーを含む。

【０６７５】

本発明で定義する流通プロトコルより下位レイヤーに属するＨＴＴＰおよびＳｏｃｋｅｔのようなデータ通信プロトコルと関連したエラーは、データ通信プロトコルにおいて支援する標準メカニズムによって発見し報告されるべきであり、本発明で定義するエラー報告メカニズムは使わない。

エラーコードはエラー対象および類型別に区分され、詳しい内容は次の表１６１の通りである。

【０６７６】

【表１６１】

【表 161】

ｴﾗｰｺｰﾄﾞ	内容	詳細説明
ValueNot Recognized	要素内容や属性値が認識されない。	たとえ文書が wellformed で有効であるものの、要素/属性の値が認識できない値であり、そのために ebXML ﾒｯｾｰｼﾞｻｰﾋﾞｽによって使用できない値を含む。
Not Supported	要素や属性が支援されない。	たとえ文書が wellformed で有効であり、要素や属性がこの明細の規則や制約に従うものの、ﾒｯｾｰｼﾞを処理できる ebxml ﾒｯｾｰｼﾞｻｰﾋﾞｽによって支援されない。
Inconsistent	要素内容や属性値がまた他の要素や属性に不一致する。	たとえ文書 wellformed で有効であり、この明細の規則と制約に従うものの、要素と属性の内容が他の要素や属性に一致しない。
OthrXml	要素内容や属性値の中のまた他のｴﾗｰ	たとえ文書が wellformed で有効であるものの、その要素内容や属性値がこの明細内の規則や制約に従わず、他のｴﾗｰｺｰﾄﾞに属しない。ｴﾗｰ要素の内容は問題の本質を示すのに使われるべきである。
Delivery Failule	ﾒｯｾｰｼﾞ転送の失敗	受信されたﾒｯｾｰｼﾞが大概にもしくは確実に次の目的地に送られれていない。仮に Severity が Warning に設定されていれば、ﾒｯｾｰｼﾞが配達される可能性は小さい。
TimeToLive Expired	ﾒｯｾｰｼﾞが存在できる時間が超過する。	ﾒｯｾｰｼﾞが受信されたものの、MessageHeader 要素の TimeToLive 要素が制約した時間を超過した時刻に受信された。
Security Failure	ﾒｯｾｰｼﾞの保安検査に失敗	ﾒｯｾｰｼﾞを送った当事者の署名の検証または権限または実名の検査に失敗した。
Unknown	分からないｴﾗｰ	いかなるｴﾗｰの種類にも属しないｴﾗｰが発生したことを意味する。ｴﾗｰ要素の内容が問題の本質を示すのに使われるべきである。

【０６７７】

一方、ＳＯＡＰ　Ｂｏｄｙ要素はＳＯＡＰ　Ｅｎｖｅｌｏｐｅ要素の２番目の子要素であり、Ｍａｎｉｆｅｓｔのような拡張要素を含み、Ｍａｎｉｆｅｓｔはペイロードコンテナーまたはウェブのように他の場所に位置したデータを示す要素である。

【０６７８】

Ｍａｎｉｆｅｓｔ要素は、１個以上のＲｅｆｅｒｅｎｃｅ要素で構成された複合要素である。各Ｒｅｆｅｒｅｎｃｅ要素は、ペイロードコンテナーに含まれたペイロード文書の一部として含まれるか、ＵＲＬにアクセス可能な遠距離のリソースであるメッセージに関連したデータを識別する。ＳＯＡＰ　Ｂｏｄｙにはペイロードデータをのせないことが好ましく、Ｍａｎｉｆｅｓｔの目的は、ＸＭＬメッセージと関連した特定のペイロードを容易に直接にアクセスできるようにすることと、パーシング作業がなくてもアプリケーションがペイロードを処理できるか否かを判断できるようにすることである。

Ｍａｎｉｆｅｓｔ要素は、次のような１個のｉｄ属性、１個のｖｅｒｓｉｏｎ属性および１個以上のＲｅｆｅｒｅｎｃｅ要素で構成されている。

【０６７９】

Ｒｅｆｅｒｅｎｃｅ要素は、０個以上のＳｃｈｅｍａ要素および０個以上のＤｅｓｃｒｉｐｔｉｏｎ要素を含む下位要素で構成された複合要素である。この時、０個以上のＳｃｈｅｍａ要素は親Ｒｅｆｅｒｅｎｃｅ要素から識別されたインスタンス文書を定義するスキーマに対する情報であり、０個以上のＤｅｓｃｒｉｐｔｉｏｎ要素：親参照要素によってＲｅｆｅｒｅｎｃｅされたペイロードオブジェクトに対する説明である。

【０６８０】

Ｒｅｆｅｒｅｎｃｅ要素は、それ自体が［ＸＬＩＮＫ］の単純リンクである。ＸＬＩＮＫプロセッサまたはエンジンの使用が必須ではないが、実現要求事項によっては有用である。Ｒｅｆｅｒｅｎｃｅ要素は、上記で提供された要素の内容と共に、ｉｄ、ｘｌｉｎｋ－ｔｙｐｅ、ｘｌｉｎｋ：ｈｒｅｆ、ｘｌｉｎｋ：ｒｏｌｅのような属性内容を含んでおり、この他に他の有効ネームスペースである属性が存在することができ、受信ＭＳＨは上記で定義したものの以外に外部のネームスペース属性は無視することができる。この時、ｉｄはＲｅｆｅｒｅｎｃｅ要素に対するＸＭＬ　ＩＤであり、ｘｌｉｎｋ－ｔｙｐｅはＸＬＩＮＫ単純リンクで要素を定義し、"ｓｉｍｐｌｅ"という固定された値を有し、ｘｌｉｎｋ：ｈｒｅｆは参照されたペイロードオブジェクトのＵＲＩ値であり、［ＸＬＩＮＫ］明細の単純リンクに準ずるものであるべきである。そして、ｘｌｉｎｋ：ｒｏｌｅはペイロードオブジェクトやその目的を説明するリソースを識別するものであって、存在するのであれば、［ＸＬＩＮＫ］明細に準ずる有効なＵＲＩ値を有しなければならない。

【０６８１】

Ｓｃｈｅｍａ要素は、参照する項目がそれを記述するスキーマを持っているのであれば（例：ＸＭＬ　Ｓｃｈｅｍａ、ＤＴＤ、またはＤａｔａｂａｓｅ　Ｓｃｈｅｍａ）、そのＳｃｈｅｍａ要素はＲｅｆｅｒｅｎｃｅ要素の子要素として存在しなければならない。これは、スキーマとバージョンを識別する方法として使われ、親Ｒｅｆｅｒｅｎｃｅ要素によって識別されるペイロードオブジェクトを定義する。Ｓｃｈｅｍａ要素は、ｌｏｃａｔｉｏｎおよびｖｅｒｓｉｏｎのような属性を有する。この時、ｌｏｃａｔｉｏｎはスキーマの必須ＵＲＩであり、ｖｅｒｓｉｏｎはスキーマのバージョン識別子である。

【０６８２】

ｘｌｉｎｋ：ｈｒｅｆ属性がｃｏｎｔｅｎｔ　ｉｄ（ＵＲＩ　ｓｃｈｅｍｅ　"ｃｉｄ"）であるＵＲＩを含んでいれば、そのｃｏｎｔｅｎｔ－ｉｄを有するＭＩＭＥはメッセージのペイロードコンテナーに表現されているか、そうでなければ、ｅｒｒｏｒＣｏｄｅをＭｉｍｅＰｒｏｂｌｅｍに、ｓｅｖｅｒｉｔｙをＥｒｒｏｒにするエラーを発信当事者に伝達するべきである。ｘｍｌ：ｈｒｅｆ属性がｃｏｎｔｅｎｔ　ｉｄ（ＵＲＩ　ｓｃｈｅｍｅ　"ｃｉｄ"）であるＵＲＩを含んでいなければ、ＵＲＩは解釈されず、実現に応じてエラーを伝達するべきか否かを決定しなければならない。エラーが伝達されるべきであると決定されれば、ｅｒｒｏｒＣｏｄｅをＭｉｍｅＰｒｏｂｌｅｍに、ｓｅｖｅｒｉｔｙをＥｒｒｏｒにするエラーを発信当事者に伝達するべきである。

下記の表１６２は典型的な１個のペイロードＭＩＭＥ　Ｂｏｄｙ部分を有するメッセージのＭａｎｉｆｅｓｔを示す。

【０６８３】

【表１６２】

【表 162】

```
<eb:Manifest eb:id="Manifest" eb:version="2.0">
  <eb:Reference eb:id="pay01" xlink:href="cid:payload-1" xlink:role="http://regrep.org/gci/purchaseOrder">
    <eb:Schema eb:location="http://regrep.org/gci/purchaseOrder/po.xsd" eb:version="2.0"/>
    <eb:Description xml:lang="en-US">Purchase Order for 100,000 widgets</eb:Description>
  </eb:Reference>
</eb:Manifest>
```

【０６８４】

３）ＨＴＴＰバインディング

ＨＴＴＰを通してメッセージを転送する方案において、ＨＴＴＰバインディング例題は次の表１６３の通りである。

【０６８５】

【表１６３】

【表 163】

```
POST /servlet/ebXMLhandler HTTP/1.1
Host: www.example2.com
SOAPAction: "ebXML"
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
    xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
    http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
    http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
    http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId>urn:duns:123456789</eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId>urn:duns:912345678</eb:PartyId>
      </eb:To>
      <eb:CPAId>20001209-133003-28572</eb:CPAId>
      <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
      <eb:Service>urn:services:SupplierOrderProcessing</eb:Service>
      <eb:Action>NewOrder</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20001209-133003-28572@example.com</eb:MessageId>
        <eb:Timestamp>2001-02-15T11:12:12</eb:Timestamp>
      </eb:MessageData>
    </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body>
    <eb:Manifest eb:version="2.0">
      <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
          xlink:role="XLinkRole" xlink:type="simple">
        <eb:Description xml:lang="en-US">Purchase Order 1</eb:Description>
      </eb:Reference>
    </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>

--BoundarY
Content-ID: <ebxmlpayload111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<purchase_order>
  <po_number>1</po_number>
  <part_number>123</part_number>
  <price currency="USD">500.00</price>
</purchase_order>

--BoundarY--
```

【０６８６】

本発明による流通プロトコルにおいて、ＨＴＴＰレベルの応答コードを返すために、［ＲＦＣ２６１６］で定義されたＨＴＴＰ応答コードを利用するべきであり、主要応答コードは次の表１６４の通りである。

【０６８７】

【表１６４】

【表 164】

状態ｺｰﾄﾞ	連関ﾒｯｾｰｼﾞ	意味
200	OK	要請が成功的に処理される
400	Bad Request	要請に文法的に誤った部分がある
401	Unauthorized	ｸﾗｲｱﾝﾄが正しい許可を受けずに許可が必要なﾍﾟｰｼﾞにｱｸｾｽしようとする
404	Not Found	このｱﾄﾞﾚｽでは、いかなる内容も発見できない
500	Internal Server Error	ｻｰﾊﾞ内部のｴﾗｰによって要請を正常に処理できない
503	Service Unavailable	処理できる限界を超えて過度に要請が入ってきて、ｻｰﾊﾞが現在の該当要請を処理できない

【０６８８】

［電子文書の書式登録機］

以下では、上述したような本発明の好ましい実施形態による電子文書流通システムの電子文書の書式登録機と関連して詳細に説明する。

電子文書の書式登録機は、電子文書流通において、送受信個体が文書を流通するために必要な書式を生成、登録、管理できるシステムである。

電子文書の書式登録機は、書式生成機、書式登録機、書式管理機、および標準連係モジュールで構成される。

【０６８９】

書式生成機はＰＤＦ変換モジュールとＰＤＦ　Ｆｏｒｍ　Ｄｅｓｉｇｎｅｒとからなり、ＰＤＦ変換モジュールは一般書式をＰＤＦに変換する機能（例：標準ＰＤＦ－Ａで生成）を提供し、ＰＤＦ　Ｆｏｒｍ　Ｄｅｓｉｇｎｅｒは入力可能なＦｏｒｍ　ＰＤＦを生成できる機能を提供し、２次元バーコードおよびコピー防止マークなどの文書保安機能を提供する。

書式登録機は、ユーザが書式（例：ハングル、ＭＳ－Ｗｏｒｄなどの一般書式）を登録できる機能を提供する。

【０６９０】

書式管理機は、書式管理者が書式を登録、管理できる機能を提供し、カテゴリー別の登録、バージョン別の履歴管理機能を提供し、書式別の閲覧期間、閲覧回数、印刷回数の制御などの設定機能を提供する。

【０６９１】

標準連係モジュールは、流通クライアントアプリケーションと連係できる機能を提供し、書式リスト、検索機能を提供し、ファイルダウンロード機能を提供する。

本発明による電子文書の書式登録機の書式登録プロセスは図５７の通りである。

標準電子文書はＦｏｒｍ　ｄｅｓｉｇｎｅｒを利用してＦｏｒｍＰＤＦで生成し、必須要件は下記表１６５の通りである。

【０６９２】

【表１６５】

【表 165】

区分	説明
ﾃﾞｰﾀ入力ﾌｨｰﾙﾄﾞ	内容入力のためのﾃﾞｰﾀ入力ﾌｨｰﾙﾄﾞ
2 次元ﾊﾞｰｺｰﾄﾞ	印刷された文書の原本証明のために原本文書および原本文書の電子署名ﾃﾞｰﾀが挿入される
ｺﾋﾟｰ防止ﾏｰｸ	印刷された文書のｺﾋﾟｰを防止するための機能であり、亡失消去ﾊﾟﾀｰﾝを利用してｺﾋﾟｰ時に原本表示が消える形態である
案内文句	文書の有効期間および検証方法などの内容を収録

【０６９３】
標準電子文書の構造は文書下段に５ｃｍ程度の空間確保が必要であり、バーコード大きさはデータ量に応じて可変的であり、コピー防止マーク大きさは３＞１．３にし、位置は書式模様に応じて適切な位置に配置される。
【０６９４】
標準連係モジュール（標準インターフェース）は、流通クライアントアプリケーションからユーザが書式を検索しダウンロードして書式を生成できるようにし、Ｗｅｂ　ＵＩ（Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）に提供して流通クライアントアプリケーションに含まれるようにし、カテゴリー別の検索、書式目録、ファイルダウンロードなどの機能を提供する。
【０６９５】
［電子文書パッケージング］
以下では、上述したような本発明の好ましい実施形態による電子文書流通システムおよび方法に適用される電子文書パッケージングと関連して詳細に説明する。
電子文書パッケージングは、電子文書流通において、送受信個体が文書を流通するために必要なメッセージングシステムの規格である。
【０６９６】
電子文書パッケージングは標準電子文書、添付文書で構成され、標準電子文書に対するメタデータで構成されている。標準電子文書はＰＤＦ－Ａを基盤に生成され、メタデータは文書保安機能などの情報で構成されている。添付文書は、ＰＤＦに変換せずに原本そのままパッケージングする。
標準電子文書は、ユーザの公認認証書で電子署名し、パッケージング後、電子文書パッケージを電子署名してパッケージに含ませる。
【０６９７】
図５９は電子文書パッケージの構造を示しており、このような図５９を参照すれば、本発明による電子文書のパッケージ構造はパッケージヘッダ、メタデータ、標準電子文書、添付文書、電子署名データを含み、各々の細部的な構成要素は下記表２７～表３１の通りである。
【０６９８】
パッケージヘッダはパッケージ全体の構造情報を含み、メタデータは標準電子文書の文書保安機能情報を含み、文書の閲覧回数、印刷回数、２次元バーコード情報などの情報を含み、標準電子文書は標準ＰＤＦ－Ａ形式で構成され、ＰＤＦファイル内のイメージ領域に２Ｄバーコードデータを含み、標準ＰＤＦ　Ｓｉｇｎｅｄ　Ｄａｔａ領域に電子署名データを含み、添付文書は標準電子文書ではない非定型文書であるため、文書保安機能の適

用対象から除外し、個別的な電子署名は除外し、電子署名データはパッケージングされたデータをユーザの公認認証書を使って電子署名してパッケージングに含ませる。

【０６９９】

【表１６６】

【表 166】

番号	構成要素	備考
1	全体ﾌｧｲﾙ大きさ	
2	ﾒﾀﾃﾞｰﾀ大きさ	
3	標準電子文書大きさ	
4	添付ﾌｧｲﾙ個数	
5	添付ﾌｧｲﾙ大きさ	

【０７００】

【表１６７】

【表 167】

番号	構成要素	備考
1	閲覧回数	
2	印刷回数	
3	格納機能	
4	ﾃｷｽﾄ抽出機能	
5	臨時保存/取り込み機能	
6	文書形態	
7	2D ﾊﾞｰｺｰﾄﾞ大きさ(横)	

【０７０１】

【表１６８】

【表 168】

番号	構成要素	備考
1	PDF ﾌｧｲﾙ	

【０７０２】

【表１６９】

【表 169】

番号	構成要素	備考
1	添付ﾌｧｲﾙ	

【０７０３】
【表１７０】

【表 170】

番号	構成要素	備考
1	電子署名ﾃﾞｰﾀ	

【０７０４】
電子文書パッケージングを検証する方案としては１）電子文書パッケージングの電子署名の検証方案、２）標準電子文書の検証方案、３）印刷された電子文書の検証方案があり、各方案について説明すれば、次の通りである。
【０７０５】
１）電子文書パッケージングの電子署名の検証方案
－クライアントＡｐｐは、電子署名パッケージングを処理する時に電子署名を検証し、検証を成功した場合にのみ標準電子文書を電子文書ビューアーに伝達する。
－また、手動の電子署名の検証機能を支援して、紛争発生時に電子署名の検証ができるようにする。
２）標準電子文書の検証方案
－電子文書ビューアーは、標準電子文書を閲覧する時に電子署名の検証を遂行し、成功した場合にのみ電子文書ビューアーにおいてファイルを閲覧できるようにする。
３）印刷された電子文書の検証方案
－別途に提供される検証プログラムとフラットベッドスキャナを利用して、２次元バーコード内の電子署名データの検証、および原本の文書内容と印刷された文書内容とを肉眼で比較する。
一方、コピー防止マークは、電子文書を最終に受けるユーザのプリンタパターンに応じて生成しなければならないので、パッケージングには含まれない。
【０７０６】
［流通クライアントアプリケーション］
以下では、上述したような本発明の好ましい実施形態による電子文書流通システムの流通クライアントアプリケーションと関連して詳細に説明する。
【０７０７】
企業または個人が公認電子アドレスに基づいて文書（情報）を送受信するためには、これを支援するためのユーザインターフェース（Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ、以下、ＵＩという）を提供するアプリケーションが必要である。流通メッセージングサーバシステムがメッセージをやりとりするためのメッセージングエンジンとしてｅ－メールと比較した時にメールサーバのような役割をするのであれば、流通クライアントアプリケーション（以下、ＡＰＰという）は、ユーザがｅ－メールサーバと連係してｅ－メールをやりとりするために提供されるメールクライアントのようなユーザ用アプリケーションの役割をする。
【０７０８】

図６０は流通クライアントＡＰＰの構造図を示し、このような図６０を参照すれば、流通クライアントＡＰＰは、流通メッセージングサーバシステムを利用して文書を交換しようとする一般ユーザのためのＵＩ環境のアプリケーションとして、基本的に"１）ユーザ認証"、"２）メッセージ作成"、"３）メッセージ目録の照会および詳細内容の閲覧機能"、"４）流通メッセージングサーバシステム連係"で構成される。クライアントＡＰＰは、このような基本機能の他に追加的にメッセージ送受信およびアプリケーション管理のための"５）基本情報と環境情報の管理"、"６）メッセージフォルダの管理"、"７）文書書式の管理"、"８）文書作成機"などの機能を提供することができるが、これは、アプリケーション開発者によって選択的に提供される機能である。

【０７０９】

１）ユーザ認証

－流通クライアントＡＰＰが流通メッセージングサーバシステムと連係する前に、流通メッセージングサーバシステムは、ユーザアカウントを確認した後にログインセッション情報を受けるべきである。

【０７１０】

－流通クライアントＡＰＰがユーザ認証を受けるための方法としては、認証書（公認または私設の全てを許容）を基盤にしたユーザ認証、またはＩＤ／ＰＷを基盤にしたユーザ認証などがある。

【０７１１】

２）メッセージ作成機能

－流通クライアントＡＰＰは新規メッセージを作成できるユーザインターフェースを提供するべきであり、作成された文書を流通メッセージングサーバシステムと連係して受信相手方に伝達するべきである。

【０７１２】

－メッセージ作成機能は、メッセージを転送するために流通メッセージングサーバシステムの転送インターフェースを呼び出す時、必要な基本情報のうち、環境情報によって既に設定された値ではない項目は入力できるように提供しなければならない。

【０７１３】

３）メッセージ目録の照会および詳細内容の閲覧機能

－流通メッセージングサーバシステムは、メッセージを送信メッセージ、受信メッセージに区分して管理をする。流通クライアントＡＰＰは、ログインされたユーザアカウントを基盤に流通メッセージングサーバシステムと連係して、ユーザアカウントに該当する各メッセージの目録を照会する機能と、メッセージの詳細内容を見ようとする時、添付文書を含んでメッセージの詳細情報を全て閲覧できる機能を必ず提供しなければならない。

【０７１４】

４）流通メッセージングサーバシステム連係

－流通クライアントＡＰＰの最も重要な機能は、流通メッセージングサーバシステムと連係してメッセージを送受信する機能である。流通クライアントＡＰＰは、流通メッセージングサーバシステムが提供するメッセージ送信機能と受信メッセージ読みインターフェースを介してログインしたアカウントを基盤にメッセージを転送し受信する。

【０７１５】

５）基本情報と環境情報の管理

－クライアントＡＰＰは、メッセージの転送時に基本的に必要な環境情報を管理する機能を提供しなければならない。流通クライアントＡＰＰは独立に存在するアプリケーションではないため、必ず流通メッセージングサーバシステムとの連係を通じて流通基盤のインフラに参加可能である。したがって、基本的に流通メッセージングサーバシステムとの連係のために必要な流通メッセージングサーバシステム連係情報（流通メッセージングサーバシステムのアドレス情報）を基本的に設定し管理しなければならない。

【０７１６】

－その他に文書の書式登録機との連係のための登録機サーバ情報の管理や、流通クライ

アントＡＰＰのシステム環境に対する付加情報の管理は、アプリケーションの開発範囲に応じて定義して提供すれば良い。

【０７１７】

６）メッセージフォルダの管理

－流通メッセージングサーバシステムが管理するメッセージは、送信、受信メッセージを基本に分類して管理し、送受信メッセージは、各々の処理状態に応じて状態情報を管理する。各メッセージの状態情報として、送信メッセージは送信前、送信完了、送信失敗、担当者の受信完了の状態を、受信メッセージは検証エラー、受信確認前、受信確認、閲覧確認の状態を管理し、流通クライアントＡＰＰは流通メッセージングサーバシステムが提供する基本状態情報に基づいてメッセージフォルダを管理してユーザに提供する。

【０７１８】

－流通クライアントＡＰＰは、送受信フォルダを基準に送信と受信メッセージを区分して、流通メッセージングサーバシステムが提供する状態情報に応じ、ユーザに各メッセージの状態を知らせることを基本として提供しなければならない。しかし、その他にアウトボックス、ゴミ箱のような削除したメッセージ箱を提供したり、ユーザが直接フォルダを定義し管理できるようにする機能を提供したりすることは、アプリケーション開発者の選択事項であるので、本発明の説明では省略する。

【０７１９】

７）文書書式の管理機能

－流通メッセージングサーバシステムは、転送するメッセージに添付される文書の様式を制限しないため、送受信対象の文書としては、一般のテキストファイルから、オフィスファイル、ＸＭＬ文書、マルチメディアファイルなど、いかなる種類のファイルも全て可能である。しかし、ユーザが流通クライアントＡＰＰを業務に活用するように便宜を提供するために、基本的な文書に対しては書式基盤に文書作成を支援する機能を付加的に提供することが可能である。流通クライアントＡＰＰは、文書書式登録機から提供する文書書式を登録機の標準インターフェースを介して検索してダウンロードした後、ダウンロードした文書書式を基盤に文書を作成し、これをメッセージに添付して送る機能を提供することができる。

【０７２０】

－流通クライアントＡＰＰは、電子文書流通ハブにおいて提供する文書書式登録機と連係し、該当文書書式登録機と連係して文書書式を管理することもでき、独自に文書書式の管理体系を構築し、この体系と連係して文書書式を管理する方法がある。電子文書流通ハブにおいて提供する文書書式登録機と連係して書式を検索しダウンロードする方法に対する詳細な内容は、上述した［電子文書の書式登録機］に対する説明を参照する。

【０７２１】

８）文書作成機

－文書作成機は、文書書式の管理機能を通じて流通クライアントＡＰＰがダウンロードした書式を基盤にユーザが文書を作成できるように支援する作成機である。文書作成機は、電子文書流通ハブが提供する文書書式登録機を利用する場合には、上述した［電子文書の書式登録機］に対する説明を参照して設計すれば良く、自体的に文書書式の管理体系を構築した場合には、該当書式管理体系に応じて文書作成機を設計すれば良い。

【０７２２】

前記のような流通クライアントＡＰＰの最も基本となるプロセスとしては"１）文書転送プロセス"、"２）文書受信プロセス"があり、付加的なプロセスとしては"３）電子文書の書式ダウンロードプロセス"がある。文書転送および文書受信のために、流通クライアントＡＰはサーバとなる流通メッセージングサーバシステムと連係し、標準文書様式の登録のためには、電子文書の書式登録機サーバと連係する。

【０７２３】

１）文書転送プロセス

流通クライアントＡＰＰが連係した流通メッセージングサーバシステムを介して他の"送

受信個体"に電子文書を転送するステップは図６１の通りであり、処理手続きは下記の通りである。

【０７２４】

先ず、流通クライアントＡＰＰを介して受信者に転送するメッセージを生成する。この時、メッセージは、既に送信者が作成した文書を添付するか、流通クライアントＡＰＰが提供する文書作成機を通じて作成した文書を添付して、受信者を指定した後にメッセージを生成する。

【０７２５】

次に、受信者のアドレス情報を入力した後、流通メッセージングサーバシステムの転送インターフェースを呼び出すことによってメッセージ転送を要請する。

【０７２６】

次に、転送者の流通メッセージングサーバシステムは、転送プロセスに応じて受信者にメッセージを転送した後、受信者から受信に対する応答メッセージ（受信証明書または受信エラー）を受信する。

【０７２７】

次に、転送者の流通メッセージングサーバシステムは、受信に対する応答メッセージを受信した後、流通クライアントＡＰＰに転送に対する応答として伝達する。

ここで、第１～第４ステップは必須手続きであり、第２～第４ステップは必ず同期式で行われなければならない。

【０７２８】

次に、転送者の流通メッセージングサーバシステムが受信者から受信担当者の閲覧を確認する閲覧証明書を含むメッセージを受ければ、転送流通メッセージングサーバシステムは、受信に対する応答メッセージを返し、受信メッセージを該当ユーザの私書箱に保管する。

次に、最初転送者の流通クライアントＡＰＰは、連係した流通メッセージングサーバシステムに受信文書を要請する。

【０７２９】

次に、転送者の流通メッセージングサーバシステムは、私書箱に保管された受信文書目録を、受信文書を要請したユーザの流通クライアントＡＰＰに伝達する。

【０７３０】

ここで、第５～第７ステップは選択的な事項であり、最初メッセージの転送時に受信担当者の閲覧確認を要請した場合にだけ発生する選択的な手続きである。

【０７３１】

２）文書受信プロセス

流通クライアントＡＰＰが他の"送受信個体"から電子文書を受信するプロセスは図６２の通りであり、処理手続きは次の通りである。

【０７３２】

先ず、受信者の流通メッセージングサーバシステムは、メッセージを受信すれば、受信したメッセージに対する受信応答メッセージを受信者に返し、受信メッセージを該当ユーザの私書箱に保管する。

【０７３３】

次に、受信者の流通クライアントＡＰＰは、連係した流通メッセージングサーバシステムにログインした後、受信文書を要請する。

次に、受信者の流通メッセージングサーバシステムは、受信文書を要請したユーザの私書箱に保管された受信文書目録を伝達する。

ここで、第２～第３ステップは同期式である。

【０７３４】

次に、受信者が受信メッセージの目録において、メッセージに対する詳細情報を見ることを要請すれば、流通クライアントＡＰＰは、流通メッセージングサーバシステムに該当メッセージの添付文書を含む詳細情報を伝達する。

【０７３５】
次に、最初転送者が受信担当者の閲覧確認を要請した場合、受信者の流通メッセージングサーバシステムは、ユーザが受信文書に対する詳細情報要請をした時点で、該当メッセージの送信者に閲覧証明書を含むメッセージを転送する。
【０７３６】
次に、受信者の流通メッセージングサーバシステムは、第５ステップで転送された担当者の閲覧確認メッセージ（閲覧証明書）に対する受信応答メッセージを受信する。
【０７３７】
３）電子文書書式のダウンロードプロセス
流通クライアントＡＰＰが電子文書の書式をダウンロードするプロセスは図６３の通りであり、処理手続きは次の通りである。
【０７３８】
先ず、流通クライアントＡＰＰは、電子文書の書式登録機サーバに直接連係して、文書書式に対する検索を要請する。この時、電子文書の書式登録機サーバが提供する標準連係インターフェースを基盤に連係する。
次に、電子文書の書式登録機サーバは、検索された文書書式に対する情報を結果として返す。
この時、第１～第２ステップは同期式である。
【０７３９】
次に、流通クライアントＡＰＰは、検索された書式目録をユーザに見せることにより、ユーザが書式を選択できるようにする。
次に、流通クライアントＡＰＰは、電子文書の書式登録機サーバに選択された電子文書の書式に対するダウンロードを要請する。
次に、電子文書の書式登録機サーバは、要請を受けた書式を流通クライアントＡＰＰに返す。
次に、流通クライアントＡＰＰは、ダウンロードした電子文書の書式を登録して、文書作成機で使えるようにＰｌｕｇ－Ｉｎする。
【０７４０】
前記のような流通クライアントＡＰＰのために流通メッセージングサーバシステムが提供するインターフェースの類型としては、ユーザ認証（ログイン）、ログアウト、メッセージ転送の要請、受信メッセージＧｅｔ、メッセージ詳細情報の要請、メッセージ削除がある。
流通クライアントＡＰＰと流通メッセージングサーバシステムの連係方案（１）～５））について説明すれば、次の通りである。
【０７４１】
１）流通メッセージングサーバシステムの連係プロトコル
流通メッセージングサーバシステムが流通クライアントＡＰＰのために提供する連係インターフェースは、流通メッセージングサーバシステムの送受信プロトコルと同一のプロトコルを基盤にする。但し、流通メッセージングサーバシステム間に送受信する場合とは異なり、流通クライアントＡＰＰと流通メッセージングサーバシステムは図６４のようにワンウェイ（Ｏｎｅ－Ｗａｙ）同期式通信だけを提供し、両者の間ではメッセージに対する電子署名認証またはユーザ認証の方式を使う。
【０７４２】
転送メッセージは流通メッセージングサーバシステムのメッセージ構造をそのまま活用するが、ユーザ情報および要請と応答メッセージは図６６のような構造で構成され、詳細な説明は次の通りである。
【０７４３】
－ＳＯＡＰ　Ｈｅａｄｅｒ：流通クライアントＡＰＰおよび流通メッセージングサーバシステムが業務類型に応じて送信者または受信者となって、上述した［流通プロトコル］に応じて構成され、ｍｅｓｓａｇｅＨｅａｄｅｒおよびＳｉｇｎａｔｕｒｅ情報で構成さ

れる。
－ＳＯＡＰ　Ｂｏｄｙ：上述した［流通プロトコル］で定義されたＭａｎｉｆｅｓｔ要素情報およびユーザログイン情報が入る。
【０７４４】
－転送文書コンテナー＃１：メッセージ転送の要請、受信メッセージＧｅｔ、メッセージ詳細情報の受信の場合、本文の文書（Ｃｏｎｔｅｎｔｓ）が入る。
－転送文書コンテナー＃２：メッセージ転送の要請、メッセージ詳細情報の受信の場合、添付文書が＃２から順次入る。
【０７４５】
ＳＯＡＰ　Ｈｅａｄｅｒの構造は下記表１７１の通りであり、ＭｅｓｓａｇｅＨｅａｄｅｒの構造は下記表１７２の通りであり、ＳＯＡＰ　Ｂｏｄｙの構造は下記表１７３の通りであり、本文メッセージの構造は下記表１７４の通りである。
【０７４６】
【表１７１】

【表 171】

項目名	説明	反復回数	類型	長さ
MessageHeader	■ MessageHeader	1..1		
SyncReply	■ 同期式送信を意味 ■ " 流通ﾌﾟﾛﾄｺﾙ規格 " を参照	1..1		
Signature	■ 電子署名要素 ■ " 流通ﾌﾟﾛﾄｺﾙ規格 " を参照	1..1		

【０７４７】

【表１７２】

【表 172】

項目名	説明		反復回数	類型	長さ
From	ﾒｯｾｰｼﾞ送信者情報		1..1		
	PartyId	固定値:”Clientapp”	1..1	S	9
	Role	●送信者役割 ●使用時の固定値:”Sender”	1..1	S	6
To	ﾒｯｾｰｼﾞ受信者情報		1..1		
	PartyId	固定値:”openapi”	1..1	S	7
	Role	●送信者役割 ●使用時の固定値:”Receiver”	1..1	S	8
CPAID	●取引協業定義書 ID ●Clientapp-openapi 値を必ず使用		1..1	S	17
Conversation Id	●送受信ﾄﾗﾝｻﾞｸｼｮﾝ区分子 ●英文を用いて長さ 256 以下に任意の値を設定 ●ex>2e2cbl-4603-4909-9bef-ee435bc56cb3		1..1	S	最大 256
Service	●CPA 定義されたﾒｯｾｰｼﾞｻｰﾋﾞｽ ●urn:ebxml:nipa:ClientToOa 値を必ず使用		1..1	S	25
Action	●Service ｻｰﾋﾞｽ内の特定業務ﾌﾟﾛｾｽ区分子 -文書送信要請の場合:RequestSend -文書送信要請に対する応答の場合:RespondSend -文書受信要請の場合:RequestReceive -文書受信要請に対する応答の場合:RespondReceive -文書詳細情報の受信要請の場合:RequestDeailInfio -文書詳細情報の受信要請に対する応答の場合: RespondInfio -文書削除要請の場合:RequestDelete -文書削除要請に対する応答の場合:RespondDelete		1..1	S	11
Message Data	●ﾒｯｾｰｼﾞを識別するためのﾃﾞｰﾀ		1..1		
	MessageId	●1 つのﾒｯｾｰｼﾞが有する唯一の識別子 ●英文を用いて長さ 256 以下に任意の値を設定 ●ex>42e2c2bl-46O3-4919-9bef-ee435bc56cb3	1..1	S	256
	Time Stamp	●ﾒｯｾｰｼﾞの生成時間 ●UTC 形式 ●ex>2008-07-31T06:29:39.724Z	1..1	S	24
	ReTo MessageId	●応答ﾒｯｾｰｼﾞにのみ存在 ●要請ﾒｯｾｰｼﾞの MessageId	1..1	S	最大 256

【０７４８】

【表１７３】

【表 173】

項目名	説明		反復回数	類型	長さ
Manifest	•ﾍﾟｲﾛｰﾄﾞ情報 •添付文書がある場合にのみ存在(ﾒｯｾｰｼﾞ転送の要請、受信ﾒｯｾｰｼﾞ Get、ﾒｯｾｰｼﾞ詳細情報の受信)		0..1		
	Reference	•Manifest がある場合には必ず存在 •ﾍﾟｲﾛｰﾄﾞ数だけ繰り返す •“流通ﾌﾟﾛﾄｺﾙ規格を参照”	0..∞		
UserInfo	•ﾕｰｻﾞ情報 •ﾒｯｾｰｼﾞの転送要請、受信ﾒｯｾｰｼﾞ Get、ﾒｯｾｰｼﾞ詳細情報の受信の場合にのみ存在		0..1		
	Id	•ﾕｰｻﾞ情報がある場合には必ず存在 •流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞに登録されたﾕｰｻﾞ ID	0..1	S	20
	Password	•ﾕｰｻﾞ情報がある場合には必ず存在 •ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞにﾕｰｻﾞ登録時に設定したﾊﾟｽﾜｰﾄﾞ情報 •流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞの公認認証書で暗号化した後に設定	0..1	S	15

【０７４９】

【表１７４】

【表 174】

項目名		説明	反復回数	類型	長さ
Content		■文書詳細情報 ■文書 Get の場合に文書目録個数だけ存在	1.∞	S	200
	Title	■文書の題名 ■文書送信要請、文書 Get 応答、文書詳細情報の応答にのみ存在	0..1	S	200
	Text	■ﾕｰｻﾞｺﾒﾝﾄ ■文書送信要請、文書 Get 応答、文書詳細情報の応答にのみ存在	0..1	S	5000
	Sender	■送信者信頼ｱﾄﾞﾚｽ ■文書送信要請、文書 Get 応答、文書詳細情報の応答にのみ存在	0..1	S	256
	Receiver	■受信者信頼ｱﾄﾞﾚｽ ■文書送信要請、文書 Get 応答、文書詳細情報の応答にのみ存在	0..1	S	256
	GetMessage Id	■詳細情報要請 MessgeId ■詳細情報要請の場合にのみ存在	0..1	S	256
	Delete MessageId	■削除要請 MessgeId ■削除要請の場合にのみ存在	0..1	S	256

【０７５０】

２）メッセージ転送の要請

【０７５１】

メッセージの転送時に流通クライアントＡＰＰが流通メッセージングサーバシステムに伝達しなければならない基本情報は次の通りである。転送完了した後に私書箱に保管された送信文書は下記表１７５のように４ステップの状態情報を有する。

【０７５２】

【表１７５】

【表 175】

状態	説明
送信中	•文書転送後に受信者から何の応答も受けていない状態
送信完了	•受信者から受信確認のための応答ﾒｯｾｰｼﾞ(受信証明書)を受けた状態
送信失敗	•受信流通ﾒｯｾｰｼﾞﾝｸﾞｻｰﾊﾞｼｽﾃﾑの内部でｴﾗｰが発生して SOAP Fault ﾒｯｾｰｼﾞをﾘﾀｰﾝするか、送受信過程でﾈｯﾄﾜｰｸｴﾗｰが発生した場合
受付完了	•受信ﾕｰｻﾞが受信文書に対する詳細内容(添付ﾌｧｲﾙを含む)を閲覧したか否か

【０７５３】
要請メッセージの例題は下記表１７６の通りである。
【０７５４】

【表１７６】

【表 176】

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RequestSend</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
        <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
      </eb:MessageData>
    </eb:MessageHeader>
    <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
      SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
    <Signature ...> ... </Signature>
  </SOAP:Header>
  <SOAP:Body>
    <eb:Manifest eb:version="2.0">
      <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
        xlinkrole="XLinkRole" xlink:type="simple">
      </eb:Reference>
      <eb:Reference xlink:href="cid:ebxmlpayload222@example.com"
        xlinkrole="XLinkRole" xlink:type="simple">
      </eb:Reference>
    </eb:Manifest>
    <UserInfo>
          <Id>gazuo</Id>
          <password>FJDHS6IDFJFMCD</passwd>
    </UserInfo>
  </SOAP:Body>
</SOAP:Envelope>
```

【表 176 の継続】

```
--BoundarY
Content-ID:ebxmlpayload111@example.com
Content-Type:text/xml
<Contents>
  <Content>
   <Title>ﾃｽﾄ</Title>
   <Title>ﾃｽﾄﾒｯｾｰｼﾞ です。</Title>
   <Sender>gazuo#ceda001</Sender>
   <Receiver>jnlee#ceda002</Receiver>
 </Content>
</Contents>

--BoundarY
Content-ID:ebxmlpayload222@example.com
Content-Type:application/octet-stream

実際の添付文書

--BoundarY--
```

【０７５５】
応答メッセージの例題は下記表１７７の通りである。
【０７５６】

【表１７７】

【表 177】

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RespondSend</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20100209-133004-38572@example.com</eb:MessageId>
        <eb:Timestamp>2010-02-09T13:31:03</eb:Timestamp>
      </eb:MessageData>
      <eb:RefToMessageId>20100209-133003-28572@example.com</eb:RefToMessageId>
    </eb:MessageHeader>
    <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
      SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
    <Signature ...> ... </Signature>
  </SOAP:Header>
  <SOAP:Body/>
</SOAP:Envelope>

--BoundarY--
```

【０７５７】

３）受信メッセージＧｅｔ

流通クライアントＡＰＰが流通メッセージングサーバシステムと連係して、ログインしたユーザアカウントに受信メッセージを読んでくる行為と、流通メッセージングサーバシステムにおいてメッセージを削除する行為とは分離している。メッセージ受信の各プロセスに応じ、次のような２ステップの状態情報を管理しなければならない。

－受信ユーザが私書箱の受信文書目録を閲覧したか否か

－受信ユーザが受信文書に対する詳細内容を閲覧したか否か

要請メッセージの例題は下記表１７８の通りである。

【０７５８】

【表１７８】

【表 178】

```
    <eb:To>
      <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
        openapi
      </eb:PartyId>
    </eb:To>
    <eb:CPAId>clientapp-openapi</eb:CPAId>
    <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
    <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
    <eb:Action>RequestReceive</eb:Action>
    <eb:MessageData>
      <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
      <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
    </eb:MessageData>
  </eb:MessageHeader>
  <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
    SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
  <Signature ...> ... </Signature>
 </SOAP:Header>
 <SOAP:Body>
  <UserInfo>
      <Id>gazuo</Id>
      <password>FJDHS6IDFJFMCD</passwd>
  </UserInfo>
 </SOAP:Body>
</SOAP:Envelope>

--BoundarY--
```

```
    <eb:To>
      <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
        openapi
      </eb:PartyId>
    </eb:To>
    <eb:CPAId>clientapp-openapi</eb:CPAId>
    <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
    <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
    <eb:Action>RequestReceive</eb:Action>
    <eb:MessageData>
      <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
      <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
    </eb:MessageData>
  </eb:MessageHeader>
  <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
    SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
  <Signature ...> ... </Signature>
 </SOAP:Header>
 <SOAP:Body>
  <UserInfo>
      <Id>gazuo</Id>
      <password>FJDHS6IDFJFMCD</passwd>
  </UserInfo>
 </SOAP:Body>
</SOAP:Envelope>

--BoundarY--
```

【０７５９】

応答メッセージの例題は下記表１７９の通りである。
【０７６０】

【表１７９】

【表 179】

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml
```

```
--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
 <SOAP:Header>
  <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
   <eb:From>
    <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
     openapi
    </eb:PartyId>
   </eb:From>
   <eb:To>
    <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
     clientapp
    </eb:PartyId>
   </eb:To>
   <eb:CPAId>clientapp-openapi</eb:CPAId>
   <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
   <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
   <eb:Action>RespondReceive</eb:Action>
   <eb:MessageData>
    <eb:MessageId>20100209-133004-38572@example.com</eb:MessageId>
    <eb:Timestamp>2010-02-09T13:31:03</eb:Timestamp>
   </eb:MessageData>
   <eb:RefToMessageId>20100209-133003-28572@example.com</eb:RefToMessageId>
  </eb:MessageHeader>
  <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
   SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
  <Signature ...> ... </Signature>
 </SOAP:Header>
 <SOAP:Body>
  <eb:Manifest eb:version="2.0">
   <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
    xlinkrole="XLinkRole" xlink:type="simple">
   </eb:Reference>
```

【表 179 の継続】

```
  </SOA:Body>
</SOAP:Envelope>
-BoundarY
Content-ID:ebxmlpayload111@example.com
Content-Type:text/xml
<Contents>
  <Content>
   <Title>ﾃｽﾄ</Title>
   <Title>ﾃｽﾄﾒｯｾｰｼﾞです。</Title>
   <Sender>gazuo#ceda001</Sender>
   <Receiver>jnlee#ceda002</Receiver>
 </Content>
</Content>
  <Title>ﾃｽﾄ 2</Title>
  <Title>ﾃｽﾄﾒｯｾｰｼﾞです。</Title>
  <Sender>gazuo#ceda001</Sender>
  <Receiver>jnlee#ceda002</Receiver>
 </Content>
</Contents>

--BoundarY--
```

【０７６１】

４）メッセージ詳細情報の要請

受信した文書目録を基盤にユーザが詳細内容を閲覧しようとする場合に、流通クライアントＡＰＰは流通メッセージングサーバシステムのメッセージ詳細情報を要請する。詳細情報の要請を受けた流通メッセージングサーバシステムは、メッセージの詳細属性情報と該当メッセージの添付文書など、全てのメッセージ内容を流通クライアントＡＰＰに応答メッセージとして伝達する。

要請メッセージの例題は下記表１８０の通りである。

【０７６２】

【表１８０】

【表 180】

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RequestDetailInfo</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
        <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
      </eb:MessageData>
    </eb:MessageHeader>
    <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
      SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
    <Signature ...> ... </Signature>
  </SOAP:Header>
  <SOAP:Body>
    <UserInfo>
          <Id>gazuo</Id>
          <Password>FJDHS6IDFJFMCD</Passwd>
          <GetMessageId>20100209-133003-28572@example.com</GetMessageId>
    </UserInfo>
  </SOAP:Body>
</SOAP:Envelope>

--BoundarY--
```

【０７６３】

応答メッセージの例題は下記表１８１の通りである。
【０７６４】

【表１８１】

【表 181】

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RespondDetailInfo</eb:Action>
```

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RespondDetailInfo</eb:Action>
```

【表 181 の継続】

```
   <eb:MessageData>
    <eb:MessageId>20100209-133004-38572@example.com</eb:MessageId>
    <eb:Timestamp>2010-02-09T13:31:03<eb:Timestamp>
   <eb:MessageData>
   <eb:Ref ToMessageId>20100209-28572@example.com</eb: RefToMessageId>
  <eb:MassageHeader>
  <eb:SyncReplyeb:id="3833kkj9"eb:version="20"SOAP:must Understand="1"
    SOAP:actor=http://schemas.xmlsoap.org/soap/actor/next"/>
  <Signature...>...</Signature>
</SOAP:Header>
<SOAP: Body>
   <eb:Manifest eb:version="20">
   <eb:Reference xlink:href=cid:ebxmlpayload111@example.com"
     Xlink:role="XlinkRole"xlink:type="simple">
    <eb:Reference>
   </eb:Manifest>
  </SOAP:Body>
</SOAP:envelope>

--BoundarY
Content-ID:ebxmlpayload111@example.com
Content-Type:test/xml

<Contents>
 <Content>
  <Title>ﾃｽﾄ</Title>
  <Text>ﾃｽﾄﾒｯｾｰｼﾞです。</Text>
  <Sender>gazuo#ceda001</Sender>
  <Receiver>jnlee#ceda002</Receiver
 </Content>
</Contents>
<Contents>
 <Content>ﾃｽﾄ Title>
 <Text>ﾃｽﾄﾒｯｾｰｼﾞです。</Text>
 <Sender>gazuo#ceda001</Sender>
  <Receiver>jnlee#ceda002</Receiver
 </Content>
</Contents>

--BoundarY
Content-ID:ebxmlpayload222@example.com
Content-Type:application/octet-stream

実際の添付文書

--BoundarY--
```

【０７６５】

５）メッセージ削除

流通クライアントＡＰＰは、ユーザが削除要請をする場合に、流通メッセージングサーバシステムに該当文書に対する削除要請を伝達し、その結果をユーザに知らせなければならない。ユーザの削除時、ゴミ箱概念の臨時削除機能の付与有無は、実際サーバ上での行為ではなく流通クライアントＡＰＰの付加機能であるので、流通クライアントＡＰＰの開発者が提供有無を決定することができるが、最終的に流通メッセージングサーバシステムに削除要請をする機能は必ず提供されるべきである。

要請メッセージの例題は下記表１８２の通りである。

【０７６６】

【表１８２】

【表 182】

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RequestDelete</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20100209-133003-28572@example.com</eb:MessageId>
        <eb:Timestamp>2010-02-09T13:30:03</eb:Timestamp>
      </eb:MessageData>
    </eb:MessageHeader>
    <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
      SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
    <Signature ...> ... </Signature>
  </SOAP:Header>
  <SOAP:Body>
    <UserInfo>
        <Id>gazuo</Id>
        <Password>FJDHS6IDFJFMCD</Passwd>
        <DeleteMessageId>20100209-133003-28572@example.com</DeleteMessageId>
    </UserInfo>
  </SOAP:Body>
</SOAP:Envelope>

--BoundarY--
```

【０７６７】

応答メッセージの例題は下記表１８３の通りである。
【０７６８】

【表１８３】

【表 183】

```
Content-type: multipart/related; boundary="BoundarY"; type="text/xml";
start="<ebxhmheader111@example.com>"

--BoundarY
Content-ID: <ebxhmheader111@example.com>
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope ...>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          openapi
        </eb:PartyId>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns">
          clientapp
        </eb:PartyId>
      </eb:To>
      <eb:CPAId>clientapp-openapi</eb:CPAId>
      <eb:ConversationId>42e2c2b1-4603-4919-9bef-ee435bc56cb3</eb:ConversationId>
      <eb:Service>urn:ebxml:nipa:ClientToOa</eb:Service>
      <eb:Action>RespondDelete</eb:Action>
      <eb:MessageData>
        <eb:MessageId>20100209-133004-38572@example.com</eb:MessageId>
        <eb:Timestamp>2010-02-09T13:31:03</eb:Timestamp>
      </eb:MessageData>
      <eb:RefToMessageId>20100209-133003-28572@example.com</eb:RefToMessageId>
    </eb:MessageHeader>
    <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"
      SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
    <Signature ...> ... </Signature>
  </SOAP:Header>
  <SOAP:Body/>
</SOAP:Envelope>

--BoundarY--
```

【０７６９】

［記録媒体］
一方、上述した本発明による電子文書流通方法はコンピュータにて実行できるプログラムで作成可能であり、コンピュータで読み取りできる記録媒体を利用してプログラムを動作させる汎用ディジタルコンピューターにて実現することができる。コンピュータで読み取りできる記録媒体は、マグネチック格納媒体（例：ＲＯＭ、フロッピー(登録商標)ディスク、ハードディスク、磁気テープなど）、光学的読み取り媒体（例：ＣＤ－ＲＯＭ、ＤＶＤ、光データ格納装置など）および搬送波（例えば、インターネットを介した転送）のような格納媒体を含む。
【０７７０】
以下、上述したような本発明において、アドレスディレクトリサーバと関連し、また他の実施形態について説明すれば、次の通りである。
【０７７１】
［アドレスディレクトリサーバ］
信頼できる電子文書流通に参加するために全てのユーザは固有の電子アドレスの発給を受けるべきである。
電子アドレスは次のような構造で表現される。
電子アドレス：内部区分子＋区分記号＋固有登録アドレス
このような電子アドレスの一例として"ｇｄｈｏｎｇ＃ｎｉｐａ．ｋｒ"がある。
【０７７２】
前記電子アドレスの内部区分子は、固有登録アドレスの所有者が内部的な処理の便宜のために選択的に追加する情報であり、必要によっては省略可能である。
【０７７３】
前記電子アドレスの区分記号は、固有登録アドレスの前に位置するか、内部区分子と固有登録アドレスとの間に存在する記号であり、一例として"＃"が可能であり、必要によっては他の記号が使える。
【０７７４】
前記電子アドレスの固有登録アドレスは、企業／機関／個人が発給要請した固有のＩＤ値であり、区分記号の後に存在する固有登録アドレス単位が送受信に対する法的な責任単位となる。このような固有登録アドレスは、送受信個体が流通メッセージングサーバを自体的に構築した後に発給を受けるか、または送受信個体が電子文書の３者流通代行機関を介して発給を受けた固有登録アドレスであって、電子アドレスの必須構成要素である。
【０７７５】
前記送受信個体は自身が保有した流通メッセージングサーバシステムに対する実際物理アドレス（ＩＰ　Ａｄｄｒｅｓｓ）を有するが、このような物理アドレスと前記電子アドレスは連関関係がなく、物理アドレスと電子アドレスは１：Ｎの関係を持つ。１つの電子アドレスがいくつかの物理アドレスを有する場合は存在しない。
【０７７６】
電子アドレスに対する情報（電子文書）の法的な受信責任は、区分記号の後に存在する企業／機関／個人が持つべきであり、内部区分子による配付は、企業／機関／個人が便宜のために区分したものであるので、自体的に責任を負わなければならない。
電子文書流通システム内で電子アドレスが有する意味は、図３に示した電子文書流通システム参加者の関係図のように表現することができる。
このように内部区分子と固有登録アドレスを有する電子アドレスに対してさらに整理すれば、次の通りである。
１）内部区分子
－内部区分子は、アドレスディレクトリサーバとは関係なく、各送受信個体が自体的に発給し管理する。
－内部区分子は、送受信個体内においては固有な値であるべきであり、省略可能な情報である。
【０７７７】

－内部区分子に対する付与方式は各企業／機関／個人が責任を持つことを基本とし、内部区分子による電子文書の配付も電子文書流通基盤のインフラ体系下で公式的な意味は持たない。

【０７７８】

－固有登録アドレスが受信に対する責任を負える政府／公共／法人／機関／団体／個人が３者流通可能な送受信個体にアカウントを開設し、公式的にアドレスディレクトリサーバに登録して使う個体であれば、内部区分子は企業の業務便宜のために電子文書を分配するための用途として使われ、アドレスディレクトリサーバに登録せず、企業内部の情報としてのみ使う。

【０７７９】

２）固有登録アドレス

－電子文書流通システムに参加して電子文書を流通しようとする政府／公共／法人／機関／団体／個人は、流通メッセージングサーバシステムを自体的に構築した後に送受信個体として固有登録アドレスの発給を受けるか、３者流通（流通代行）機関を介して固有登録アドレスの発給を受けなければならない。

【０７８０】

－固有登録アドレスは、発給時点でアドレスディレクトリサーバに固有登録アドレスの唯一性（ｕｎｉｑｕｅｎｅｓｓ）を確認することにより、重複して発給されないように管理される。

－政府／法人／機関／団体／個人の固有登録アドレスの構成方式は、公認電子アドレス管理総括の政策によって決定される。

【０７８１】

上述したような電子アドレスは基本的に２－ｌｅｖｅｌによって管理される。公認電子アドレスの最上段にはアドレスディレクトリサーバを管理する公認電子アドレス管理総括（例：情報通信産業振興院）があり、公認電子アドレス管理総括は、下位送受信個体に対する固有登録アドレスを発給し、これを管理する。公認電子アドレス管理総括の下位送受信個体中の３者流通（流通代行）が可能な送受信個体は、３次流通を望むユーザに対する登録アドレスを開設した後、これに対するアドレス情報をアドレスディレクトリサーバに登録する。この時、ユーザ固有登録アドレス値の唯一性（ｕｎｉｑｕｅｎｅｓｓ）を保障するために、必ずアドレスディレクトリサーバに重複有無を確認するべきである。

【０７８２】

電子アドレス中、公式的なユーザではなく、内部で業務便宜のために発給して使う内部区分子は、アドレスディレクトリサーバとは関係なく、各送受信個体が自体的に発給し管理する。

電子アドレスを発給する体系は図４の通りであり、図４に示す各構成要素の役割は下記表１８４の通りである。

【０７８３】

【表１８４】

【表 184】

構成要素	役割
情報通信産業振興院 (公認電子ｱﾄﾞﾚｽの 管理総括)	- 情報通信産業振興院は公認電子ｱﾄﾞﾚｽの最上位管理主体であって、全ての公認電子ｱﾄﾞﾚｽ情報を管理する - 送受信個体に対する固有 ID を発給する - ﾕｰｻﾞｱｶｳﾝﾄに対する公認電子ｱﾄﾞﾚｽの登録要請時、新規登録であるか、既存のｱﾄﾞﾚｽ変更であるかを知らせる - ﾕｰｻﾞｱｶｳﾝﾄの新規登録時、ｱｶｳﾝﾄ ID が固有であるか否かを知らせる - ﾕｰｻﾞの物理ｱﾄﾞﾚｽ情報の検索要請に対する結果値を伝達
送受信個体	- 物理公認電子ｱﾄﾞﾚｽの最も基本となる単位である - 1 つの公認電子ｱﾄﾞﾚｽの下位に複数ﾕｰｻﾞのためのﾕｰｻﾞｱｶｳﾝﾄまたは内部区分子情報を発給、管理し、1 つの公認電子ｱﾄﾞﾚｽ内においてはﾕｰｻﾞｱｶｳﾝﾄまたは内部区分子の唯一性を保障
ﾕｰｻﾞ (個人、企業、機関 など) ｱｶｳﾝﾄまたは 内部区分子の ための ID	- 電子文書流通に参加する実ﾕｰｻﾞであって、同一の送受信個体において Id の発給を受けた場合、物理公認電子ｱﾄﾞﾚｽは同一であるが、信頼流通の実質的な基盤となる単位である - ﾕｰｻﾞｱｶｳﾝﾄは 3 者流通が可能な送受信個体を通じて開設した電子ｱﾄﾞﾚｽとして法的責任を有した送受信単位であり、必ず電子ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに登録するべきである - 内部区分子は送受信に対する法的責任を有した送受信個体が内部管理の便宜のために管理する情報として、法的責任は内部区分子上位の送受信個体が持ち、電子ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞに登録されない

【０７８４】
電子アドレスを発給するプロセスは図５の通りであり、ユーザ（企業）が直接アドレスディレクトリサーバが提供する画面に接続してアドレスを登録したり修正したりする方法と、公認電子アドレスを代行発給する流通メッセージングサーバシステム（システムが提供するウェブサイト）を介して発給を受ける方法がある。
【０７８５】
流通に参加するユーザは、相手方にメッセージを転送する前に電子アドレス情報に基づいて物理的な実アドレス情報を必ず知るべきであり、付加的に添付する文書を暗号化するためには受信者の公開キー情報も獲得しなければならない。
【０７８６】
電子文書流通プロセスにおいて、電子アドレスの物理アドレスを獲得する手続きは必須

ステップであって、送信者は、受信者のアドレス情報を基準に受信相手方に対する物理アドレス情報および保安情報の獲得のためにアドレスディレクトリサーバに問い合わせる。この物理アドレスを基準に送信者が受信者に転送文書を伝達すれば、受信者の流通メッセージングサーバシステムは、これを受け、受信者のアドレス情報を基盤にユーザアカウントまたは内部区分子に応じて受信文書を内部的に分配する。

【０７８７】

電子アドレスの物理アドレスおよび保安情報の獲得プロセスは図６の通りである。電子文書流通において、公認電子アドレスを基盤に受信者に文書を転送するためには、１）流通クライアントＡＰＰが受信相手方のアドレス情報を入力する時点で、アドレスディレクトリサーバに連係して必要情報を獲得した後、検索された実の物理アドレス情報に基づいて流通メッセージングサーバに転送要請をする方法と、２）流通クライアントＡＰＰが受信者に対する公認電子アドレスを基盤に流通メッセージングサーバに転送要請をし、流通メッセージングサーバが転送前にアドレスディレクトリサーバに物理アドレスおよび保安情報を獲得した後、受信者に文書を転送する方法がある。このような２つの方法に対する手続きは図７に示す通りである。

【０７８８】

アドレスディレクトリサーバは、流通メッセージングサーバシステムがアドレス情報を検索したり、アドレス発給を代行したりできるように遠隔サービスを提供する。アドレスディレクトリサーバが提供するサービスはアドレス検索サービス、アドレス登録サービス、アドレス変更サービスがあり、流通プロトコル規格を基盤に次のようなサービスインターフェースを提供する。

【０７８９】

アドレス検索サービスは、アドレスディレクトリサーバが公認電子アドレスに該当する物理アドレス情報（例：ＩＰアドレス、Ｄｏｍａｉｎアドレス）と公開キー情報を検索要請者に返すサービスであって、一般的に送信者が文書を転送する前に受信者の実際アドレス情報と暗号化のための保安情報を獲得するために使う。この時、要請メッセージと応答メッセージの役割は下記表１８５の通りである。

【０７９０】

【表１８５】

【表 185】

構成要素	役割
要請ﾒｯｾｰｼﾞ	受信者が個人であるか企業/機関であるか、受信者の固有 ID(住民登録番号、事業者登録番号、外国人登録番号など)、公開ｷｰ要請有無
応答ﾒｯｾｰｼﾞ	受信者固有 ID、受信者ｱﾄﾞﾚｽ、公開ｷｰ(要請有無に応じて選択的)

【０７９１】

アドレス登録サービスは、アドレスディレクトリサーバが提供するＵＩを通じてだけでなく、遠隔からもユーザの公認電子アドレスを登録できるように提供するサービスであって、ユーザ情報および公認電子アドレス情報を要請メッセージとして受けてアドレスディレクトリサーバが登録処理した後、これに対する結果を応答メッセージとして受信する。アドレス登録サービスに対する要請メッセージは必ず要請者に対する電子署名情報が含まれて伝達されるべきであり、アドレスディレクトリサーバは、要請メッセージに含まれたユーザ情報と電子署名に使われた認証書情報が同一であるかを検証しなければならない。この時、要請メッセージと応答メッセージの役割は下記表１８６の通りである。

【０７９２】

【表１８６】

【表 186】

構成要素	役割
要請ﾒｯｾｰｼﾞ	ﾕｰｻﾞ固有 ID、ﾕｰｻﾞ付加情報の構造体(ﾕｰｻﾞ名、連絡先情報など)、ﾕｰｻﾞが個人であるか企業/機関であるか、ﾕｰｻﾞのｱﾄﾞﾚｽ情報、公開ｷｰ情報(選択的)、ｱﾄﾞﾚｽ情報の公開範囲を定義した構造体
応答ﾒｯｾｰｼﾞ	ﾕｰｻﾞ固有 ID、登録結果値(成功、失敗-要請情報ｴﾗｰ、失敗-既登録、失敗-認証された送受信個体ではない、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞｴﾗｰなど)

【０７９３】
アドレス変更サービスは、登録されたユーザに対するアドレス情報を遠隔から直接ユーザが変更できるようにする機能を提供する遠隔サービスで、変更するべき情報を含んでアドレスディレクトリサーバに変更要請メッセージを転送し、これに対する結果を応答メッセージとして受信する。アドレス変更サービスに対する要請メッセージは必ず要請者に対する電子署名情報が含まれて伝達されるべきであり、アドレスディレクトリサーバは、要請メッセージに含まれたユーザ情報と電子署名に使われた認証書情報が同一であるかを検証しなければならない。この時、要請メッセージと応答メッセージの役割は下記表１８７の通りである。
【０７９４】
【表１８７】

【表 187】

構成要素	役割
要請ﾒｯｾｰｼﾞ	ﾕｰｻﾞ固有 ID、ﾕｰｻﾞ付加情報の構造体(ﾕｰｻﾞ名、連絡先情報など)中の変更された情報のみ、ﾕｰｻﾞが個人であるか企業/機関であるか、ﾕｰｻﾞのｱﾄﾞﾚｽ情報、公開ｷｰ情報(選択的)、ｱﾄﾞﾚｽ情報の公開範囲を定義した構造体
応答ﾒｯｾｰｼﾞ	ﾕｰｻﾞ固有 ID、情報変更の結果値(成功、失敗-要請情報ｴﾗｰ、失敗-登録されていないﾕｰｻﾞ、失敗-変更権限がない、ｱﾄﾞﾚｽﾃﾞｨﾚｸﾄﾘｻｰﾊﾞｴﾗｰなど)

【手続補正２】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
電子文書を流通するシステムにおいて、
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と；
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、前記送受信個体に電子文書の標準書式を提供し、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；
を含むことを特徴とする電子文書流通システム。
【請求項２】
前記送受信個体の流通メッセージングサーバは、送受信したメッセージは、ユーザ別に状態情報を含んでメッセージ箱に保管し、メッセージ送受信履歴を編集および削除が不可能な媒体に所定期間保管し、メッセージ送受信に対する流通証明書を発給して前記第３者保管機関に保管を依頼し、前記流通ハブのアドレスディレクトリサーバとの連係を通じて前記送受信個体に電子アドレスの登録および検索、修正、削除を含む機能を使えるようにし、
所定期間以上保管されたメッセージを外部格納装置に移管して保管することを特徴とする、請求項１に記載の電子文書流通システム。
【請求項３】
前記電子アドレスは、
前記送受信個体が前記流通ハブのアドレスディレクトリサーバを介して発給を受けたユーザ識別記号と；前記送受信個体が必要な場合に自体的に付与する固有な値であり、該当送受信個体内で固有な値である追加識別記号；および前記ユーザ識別記号と追加識別記号との間に位置する区分記号；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システム。
【請求項４】
電子文書流通に対する主体は、固有登録アドレスの発給を受けたユーザであることを特徴とする、請求項３に記載の電子文書流通システム。
【請求項５】
前記区分記号は'＃'であることを特徴とする、請求項３に記載の電子文書流通システム。
【請求項６】
前記流通ハブは電子文書の書式登録機を備え、前記電子文書の書式登録機は、電子文書の標準書式の登録、削除、および情報修正を含む管理を遂行し、電子文書の標準書式を文脈（ｃｏｎｔｅｘｔ）に応じてさらに分類し、電子文書の標準書式が使用され得る文脈（ｃｏｎｔｅｘｔ）に対する登録、修正を含む管理を遂行することを特徴とする、請求項１に記載の電子文書流通システム。
【請求項７】
前記電子文書の書式登録機は、文書様式を管理するサーバエンジン；および送受信個体を使用するユーザが文書様式を検索しダウンロードして使用できるようにする標準インターフェース；を含み、前記送受信個体は、送受信個体を使用するユーザが流通メッセージングサーバを介してメッセージを送受信できるようにするユーザインターフェースである流通クライアントアプリケーションをさらに備え、前記流通クライアントアプリケーションを使用するユーザは、前記電子文書の書式登録機の標準インターフェースを介して文書書式を検索しダウンロードした後に、該当文書書式を利用して電子文書を生成することを特徴とする、請求項６に記載の電子文書流通システム。
【請求項８】
前記流通ハブは、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中継サーバを備え、前記流通中継サーバは、送受信個体からメッセージ転送の依頼を受ければ、メッセージ転送を代行した後に、メッセージ転送を依頼した送受信個体に送信証明書を発給し、依頼を受けたメッセージ転送を失敗した時には、メッセージ転送を依頼した送受信個体にエラーメッセージを転送することを特徴とする、請求項１に記載の電子文書流通システム。
【請求項９】

前記流通ハブは、外部システムとの連係のための外部連係ゲートウェイサーバを備え、前記外部連係ゲートウェイサーバは、電子アドレスを基盤にメッセージを送受信する流通メッセージングサーバを備え、連係した外部システムと電子文書流通システム間の送受信電子アドレスの検証／変換機能と、連係した外部システムと電子文書流通システム間のメッセージの検証／変換機能、連係した外部システムと電子文書流通システム間の電子文書に適用された保安の検証／変換機能、連係した外部システムと電子文書流通システム間の電子文書の適合性を検証し相互間に変換する機能を提供することを特徴とする、請求項１に記載の電子文書流通システム。

【請求項１０】

電子アドレス登録代行機関がアドレスディレクトリサーバに電子アドレスを登録要請して応答を受けるのに用いられる第１インターフェースと；電子アドレス登録代行機関がアドレスディレクトリサーバに登録された電子アドレス情報に対する変更を要請して応答を受けるのに用いられる第２インターフェース；および電子アドレス登録代行機関がアドレスディレクトリサーバに登録された電子アドレス情報の削除を要請して応答を受ける第３インターフェース；が備えられ、前記電子アドレス登録代行機関は、第１インターフェースを介して電子アドレスの申請者情報および電子アドレス情報を要請メッセージに含ませて転送した後に、アドレスディレクトリサーバの登録処理結果を応答メッセージとして受信し、前記電子アドレス登録代行機関は、第２インターフェースを介して変更しようとするユーザ情報および電子アドレス情報を要請メッセージに含ませて転送した後に、アドレスディレクトリサーバの変更処理結果を応答メッセージとして受信し、前記電子アドレス登録代行機関は、第３インターフェースを介して削除しようとするユーザ情報および電子アドレス情報を要請メッセージに含ませて転送した後に、アドレスディレクトリサーバの削除処理結果を応答メッセージとして受信することを特徴とする、請求項１に記載の電子文書流通システム。

【請求項１１】

前記電子アドレス登録代行機関または送受信個体がアドレスディレクトリサーバに電子文書受信者の電子アドレスに該当する物理アドレス情報とメッセージ保安処理のための公認認証書情報を要請して応答を受けるのに用いられる第４インターフェースが備えられ、電子アドレス登録代行機関または送受信個体の流通メッセージングサーバは、電子文書受信者の電子アドレスおよび公認認証書の要請有無を要請メッセージに含ませて転送した後に、アドレスディレクトリサーバから電子文書受信者の物理アドレス情報および公認認証書情報を応答メッセージとして受信することを特徴とする、請求項１０に記載の電子文書流通システム。

【請求項１２】

送受信個体の流通メッセージングサーバまたは電子アドレス登録代行機関の流通メッセージングサーバは、メッセージ転送、流通証明書の伝達、流通証明書の保管要請、および第３者保管機関の保管結果伝達に用いる第５インターフェースを備えることを特徴とする、請求項１に記載の電子文書流通システム。

【請求項１３】

送受信個体内のユーザは、ユーザインターフェースである流通クライアントアプリケーションを備え、送受信個体の流通メッセージングサーバは、電子文書流通を要請するユーザのための流通クライアントアプリケーションと連係して、ユーザに文書送受信機能を提供する第６インターフェースを備え、前記第６インターフェースは、メッセージ転送の要請、メッセージ目録の要請、メッセージ詳細情報の要請、スパムメッセージ申告、および物理アドレス情報の検索機能を流通クライアントユーザに提供することを特徴とする、請求項１に記載の電子文書流通システム。

【請求項１４】

送受信個体と流通ハブを含む電子文書流通システムで電子文書を流通する方法において、

（ａ）送信個体は、受信個体のアドレス情報に対応する物理アドレス情報を流通ハブを介

して獲得した後に、電子文書を添付したメッセージを前記物理アドレスに転送するステップと；
（ｂ）メッセージを受信した受信個体は、受信メッセージおよび送信個体に対する適合性の検証結果に応じて受信証明書またはエラー証明書を発給して送信個体に伝達するステップ；および
（ｃ）受信個体にメッセージを転送したものの失敗した送信個体は、流通ハブにメッセージ転送の代行を依頼し、メッセージ転送の代行依頼を受けた流通ハブは、送信証明書を発給して送信個体に伝達し、受信個体にメッセージを転送した後に前記（ｂ）ステップを遂行するステップ；
を含む電子文書流通方法。
【請求項１５】
前記（ａ）ステップは、
（ａ１）送信個体は、受信個体の電子アドレス情報を基準に受信個体に対する物理アドレス情報および保安情報を流通ハブのアドレスディレクトリサーバに問い合わせるステップと；
（ａ２）前記アドレスディレクトリサーバは、送信個体の問い合わせを受信して検証した後に、電子アドレスがホワイトリストにある場合、電子アドレスに対応する物理アドレス情報を送信個体に提供するステップ；および
（ａ３）前記送信個体は、電子文書を添付したメッセージを前記アドレスディレクトリサーバから提供された物理アドレス情報を基準に経路設定をして受信個体に転送するステップ；
を含むことを特徴とする、請求項１４に記載の電子文書流通方法。
【請求項１６】
前記（ｂ）ステップ後に、受信証明書を受信した送信個体は、受信証明書の適合性を検証し、検証した情報を受信証明書に添付した後、受信証明書を自体保管すると同時に、第３者保管機関に保管依頼することを特徴とする、請求項１４に記載の電子文書流通方法。
【請求項１７】
前記（ｃ）ステップは、
（ｃ１）受信個体にメッセージを転送したものの失敗した送信個体は、流通ハブにメッセージ転送の代行を依頼するステップと；
（ｃ２）流通ハブはメッセージ転送を始めるが、転送失敗時には、所定の時間間隔で再試し、メッセージ転送に最終的に失敗した場合には、送信個体に転送失敗メッセージを伝達するステップと；
（ｃ３）メッセージを正常に受信した受信個体は、受信証明書を発給して流通ハブに転送するステップ；および
（ｃ４）電子文書の受信者が電子文書を閲覧した場合、受信個体は、閲覧証明書を発給して、流通ハブを経ることなく送信個体に直接転送するステップ；
を含むことを特徴とする、請求項１４に記載の電子文書流通方法。
【請求項１８】
送信者または受信者の役割をする送受信個体と電子文書流通ハブを含む電子文書流通システムで電子文書を流通する方法において、
（ａ）送信者は、受信者の電子アドレス情報を獲得するステップと；
（ｂ）送信者は、送信する文書を予め定められたメッセージ構造体にパッケージングしたメッセージを生成した後に受信者の電子アドレスに転送するステップと；
（ｃ）前記（ｂ）ステップで転送失敗した場合に、送信者は、電子文書流通ハブにメッセージ転送を依頼し、メッセージ転送の依頼を受けた電子文書流通ハブは、送信証明書を発給して送信者に伝達した後にメッセージ転送を代行するステップと；
（ｄ）受信者は、送信者または電子文書流通ハブから受信したメッセージを検証し、検証が通過すれば、受信したメッセージから文書を抽出し、受信証明書を発給して送信者に伝達するステップと；

（ｅ）送信者は、伝達を受けた受信証明書を信頼できる第３者保管機関を活用して保管するステップ；および
（ｆ）受信者は、抽出した文書を文書担当者に伝達するステップ；
を含む電子文書流通方法。
【請求項１９】
前記（ａ）ステップ前には、
（ｇ）送信者および受信者は、文書流通のための流通メッセージングサーバを構築するか、３者流通が可能な流通メッセージングサーバを保有した送受信個体を利用するかについて決定するステップと；
（ｈ）前記（ｇ）ステップで文書流通のための流通メッセージングサーバを構築すると決めた場合には、送信者および受信者は、文書流通のための流通メッセージングサーバを構築した後に、認証機関を介して流通メッセージングサーバの認証テストを遂行し、電子文書流通ハブのアドレスディレクトリサーバに接続した後、送受信個体としての電子アドレスの発給を受けた後に、内部の実ユーザのために自体的に内部区分子を登録し管理するステップと；
（ｉ）前記（ｇ）ステップで３者流通が可能な流通メッセージングサーバを保有した送受信個体を利用すると決めた場合には、送信者および受信者は、３者流通が可能な流通メッセージングサーバを介して電子アドレスの開設を要請した後に、電子アドレス情報を電子文書流通ハブのアドレスディレクトリサーバに登録するステップ；および
（ｊ）前記（ｈ）ステップまたは（ｉ）ステップ後に、前記送信者は、電子文書流通ハブの電子文書の書式登録機から文書書式を検索しダウンロードして登録するステップ；
を含み、
前記（ｂ）ステップ前には、送信する文書を選択するか、または前記（ｊ）ステップで登録した文書書式を利用して送信する文書を作成する（ｋ）ステップがさらに遂行されることを特徴とする、請求項１８に記載の電子文書流通方法。
【請求項２０】
コンピュータで読み取り可能な記録媒体において、請求項１４～１９のいずれか１項による方法を実現するプログラムが格納される記録媒体。
【請求項２１】
電子文書を流通するシステムにおいて、
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と；
電子文書の流通のための公認電子アドレスを登録し、登録されているアドレスシステムを通じて流通メッセージングサーバと他の流通メッセージングサーバの間の電子文書を流通し、流通メッセージングサーバと他の流通メッセージングサーバの間の送受信部に対し信頼性を提供するために送受信部の暗号化が実行され、流通メッセージングサーバから他の流通メッセージングサーバにメッセージを送受信しない場合に流通メッセージングサーバにメッセージを伝送し、メッセージを送受信を検証する流通証明書を発給又は管理する流通ハブ；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；
を含むことを特徴とする電子文書流通システム。
【請求項２２】
送受信個体は、受信した証明書の書式又は内容を認証し、認証された流通証明書を信頼できる第３者保管機関へ伝送することを特徴とする、請求項２１に記載の電子文書流通システム。