

# Multiple Messaging Services (MMS) Profile for ebMS 2.0

ドキュメント情報	
名前	Multiple Messaging Services (MMS) Profile for ebMS 2.0 ebMS 2.0に関するMultiple Messaging Services (MMS)のプロファイル
バージョン	Release 11.00.00A
更新日付	2006年7月25日

リリース版 R11.00.00A

注) この翻訳資料は、英文資料を正式原文とし、あくまで皆様の参考資料として提供するものです。  
解釈、表現等で疑問点があれば、必ず原文にてご確認ください。また、翻訳文への疑問点、訂正箇所等お気づきの場合には、RNJ 事務局まで、Mail にてご連絡頂ければ幸いです。  
翻訳品質向上に向け、ご協力をお願い致します。

## 目次

<b>1</b>	<b>はじめに (Introduction)</b> .....	<b>5</b>
1.1	文書の約束事 (Document Conventions).....	5
1.2	一般的な目的と範囲 (General Intent and Scope) .....	5
1.3	一般的な方法論 (General Methodology).....	7
<b>2</b>	<b>ebXML メッセージング概論 (ebXML Messaging overview)</b> .....	<b>9</b>
2.1	ebXML フレームワーク (The ebXML Framework).....	9
2.2	ebMS メッセージング (ebXML Messaging).....	11
<b>3</b>	<b>商取引契約 (Trading Partner Agreement)</b> .....	<b>13</b>
3.1	TPAと基盤展開パラメータ (TPA and Infrastructure Deployment Parameters) .....	13
3.2	CPPとCPA プロファイリング (CPP and CPA Profiling).....	18
<b>4</b>	<b>メッセージの解説 (Message Description)</b> .....	<b>20</b>
4.1	ebMS2.0のプロファイリングに関する一般的な手引 (General approach for ebMS 2.0 profiling).....	20
4.2	ebMSヘッダープロファイリング (ebMS Header Profiling ).....	22
<b>5</b>	<b>メッセージ処理 (Message Processing)</b> .....	<b>31</b>
5.1	パッケージング (Packaging) .....	31
5.2	アンパッケージング (Un-packaging).....	31
<b>6</b>	<b>メッセージ交換パターンと再表現 (Message Exchange Patterns and Representation)</b> .....	<b>32</b>
6.1	ebMS 2.0におけるMEP (MEPs in ebMS 2.0).....	32
6.2	受信の操作 (Handling of Receipts).....	34
<b>7</b>	<b>QoSに関するTPA機能と展開構成 (TPA Features Specific to QoS and Deployment Configurations)</b> .....	<b>36</b>
7.1	セキュリティ (Security).....	36
7.2	信頼性 (Reliability).....	36
7.3	時折接続パートナー (Occasionally Connected Partners).....	37
7.4	ルーティングとマルチホップ (Routing and Multi-Hop).....	37

---

<b>8 その他 (Miscellaneous)</b> .....	<b>39</b>
<b>9 付録A:CPAプロファイリングと例題 (Appendix A: CPA Profiling and Sample)</b> .....	<b>39</b>
9.1 CPAプロファイリング形式 (CPA Profiling Forms).....	39
9.2 CPAアーティファクト名と参照のプロファイリング (Profiling the CPA Artifact Names and References).....	40
9.3 パーティ情報のプロファイリング (Profiling the Party Info).....	41
9.4 コラボレーション役割のプロファイリング (Profiling the Collaboration Roles).....	43
9.5 配信チャネルのプロファイリング (Profiling the Delivery Channels).....	45
9.6 文書交換のためのプロファイリング (Profiling the Document Exchanges).....	46
9.7 トランスポート層のプロファイリング (Profiling the Transport Protocol).....	48
9.8 PIP定義における表の実例 (Examples of Tables Used in PIP Definitions) .....	48
9.9 CPA 文書の例 (Sample CPA Material).....	49
<b>10 付録B: 用語集 (Appendix B: Glossary)</b> .....	<b>52</b>
<b>11 参照 (References)</b> .....	<b>53</b>

## 免責事項 (Legal Disclaimer)

RosettaNet™ 及びそのメンバー、職員、管理者、従業員、又は代理人は、本書や本書で提示する仕様及び関連するガイドラインやスキーマの使用によって発生した、あるいはそれらに関連した金銭的またはその他の損害、損失、障害に対して一切の責任を負うものではない。前述の仕様の使用をもって、本弁明への承諾の表明とみなされる。

## 著作権 (Copyright)

©2006 RosettaNet. All Rights Reserved. 本書の一部あるいは全部について、出版元からの文書による許諾を得ずに、電子的、機械的、写真複写、録音、あるいはその他いかなる形式または方法においても、再版、検索システムへの保存、あるいは移送を行うことを禁ずる。

## 商標 (Trademarks)

RosettaNet、Partner Interface Process、PIP及びRosettaNetロゴは、非営利組織「RosettaNet」の商標または登録商標である。その他の製品名及び企業のロゴは、それらの所有者の商標である。本書では、商標または登録商標として認知された表記について言及する場合、その表記が最初に登場した箇所のできる限り適切な確認を行うようにした。

## ドキュメントのバージョン履歴 (Document Version History)

バージョン	日付	コメント
リリース版 R11.00.00A	2006年7月24日	会員全体に仕様書をリリースすることが了承された

## MMS ebMS チーム

<u>Members</u>	<u>Company</u>
Jacques Durand	Fujitsu
Dale Moberg	Cyclone Commerce
Peter Hawtrey	ePSA / Tag Tools
Nikola Stojanovic	RosettaNet / GS1US
Wan Norhazlina	RosettaNet (on loan from Importek)
SooChin Yeoh	RosettaNet
Annabelle Kongkeo Marlow	RosettaNet
Ken Siu	Centre for E-Commerce Infrastructure Development (CECID) University of Hong Kong
Deepak Bhargava	Cisco Systems

Elham Ghassemzadeh	Cisco Systems
Jim Kao	Cisco Systems
John Voss	Cisco Systems
Mir Baqar	Cisco Systems
Gary Binder	DHL
Martin Evans	Formfill
Stewart Witchalls	Formfill
Kenji Nagahashi	Fujitsu
John Cartwright	Intel
Frederic Herzer	Motorola
Maggie Caligiuri	Motorola
Jeff Hutchins	Oracle
Wellwin Kwok	Centre for E-Commerce Infrastructure Development (CECID) University of Hong Kong
Mark Schenecker	SAP
Li Xueheng	Sterling Commerce
Ron Boutell	Sterling Commerce
Suresh Damodaran	Sterling Commerce
Terence Thambi Rajah	Sterling Commerce
Bill Wray	Tyco Electronics
Gary Sheetz	Tyco Electronics
Bala Yamandra	webMethods
David Smiley	webMethods

## 1 始めに (Introduction)

### 1.1 文書の約束事 (Document Conventions)

このドキュメントの中で、大文字で表示される "MUST", "REQUIRED", "SHALL", "SHOULD", "RECOMMENDED", "MAY", "OPTIONAL", "MUST NOT", "NOT REQUIRED", "SHALL NOT" and "SHOULD NOT" が本書類に現われる場合、[RFC2119]で記述される様に、解釈される。

### 1.2 一般的な目的と範囲 (General Intent and Scope)

#### 1.2.1 目的 (Intent)

RosettaNet implementations currently require users to buy a messaging system capable of running the RosettaNet Implementation Framework (RNIF). Although such systems are robust and widely adopted for XML payloads in the high-tech industry, such RNIF messaging systems are not commonly used by other vertical markets. As a result, companies who support both the high tech industry and other verticals are forced to support more than one messaging standard for e-business transactions. To alleviate the problem, RosettaNet created a Multiple Messaging (MMS) initiative that included three additional messaging systems, ebMS, AS2 and WS-I.

現在、RosettaNetの実装には、RosettaNet実装フレームワーク (RNIF)を実装できるシステムを購入する必要がある。こうしたシステムは安定しており、ハイテク業界においてXML本文の交換に広く採用されているが、しかしながら、このようなRNIFメッセージングシステムは、他の垂直市場では一般に使われていない。その結果、ハイテク産業と他の垂直市場の両方をサポートする企業は、eビジネス取引のために複数のメッセージング標準をサポートすることを強いられている。この問題に対処するためにRosettaNetは、ebMS、AS2、WS-Iという3つのさらなるメッセージングシステムを含んだマルチメッセージングサービス (MMS-Multiple Messaging Service) 構想を立ち上げた。

The purpose of this document is to recommend to users and developers how best to use an ebMS message handling system to transport RosettaNet PIP business messages between trading partners. Including ebMS in this way will add another messaging option for trading partners transporting RosettaNet business payloads and may lower the infrastructure investments required to exchange RosettaNet payloads across trading networks that employ ebMS. It is hoped that adding ebMS may also broaden the reach of RosettaNet by encouraging PIP implementations across ebMS based vertical industry and government boundaries.

本文書の目的は、取引企業でRosettaNetビジネスメッセージを送るために、ebMSメッセージ処理システムを最も有効に使う方法をユーザーや開発者に推奨することである。ebMSをこのように組み入れると、RosettaNetビジネス情報を送る取引相手にとってメッセージングのオプションが増え、ebMSを採用した取引ネットワークに亘ってRosettaNet PIPを交換するのに必要なインフラ投資を削減することが出来るかもしれない。又、ebMSを付け加えることは、ebMSベースの垂直産業や政府の境界を越えてPIPの実装を促進することにより、RosettaNetの適用範囲を広げることになるであろう。

#### 1.2.2 このドキュメントの範囲 (Scope of This Document)

This document is concerned with the profiling and the configuration of an ebXML framework, for carrying RosettaNet PIPs according to the requirements identified in the MMS - Abstract Message Definition (AMD) document.

本文書は、MMS で指定されている要求事項(即ちメッセージ定義の要約書(AMD-Abstract Message Definition))に従った RosettaNet PIP を実装するための ebXML フレームワークのプロファイリング及構成について述べている。

The approach we have taken is to focus on ebMS 2.0, include part of the CPA and limit Choreography to the lowest level covering one action PIPs.

我々の取ったアプローチは、ebMS 2.0に焦点を当てたもので、メッセージ交換プロトコル合意(CPA-Collaboration Protocol Agreement)の一部及び1アクションPIPのみに対応する制限付のコレオグラフィが含まれる。

- ebXML version: To focus on ebMS 2.0, although ebMS 3.0 will be a profiling target in a next release. It is expected that the profiling done for ebMS 2.0 can be largely leveraged by ebMS 3.0 profiling. Some desirable features that are likely to be natively supported by ebMS 3 (message pulling, bundling of payloads...) could be emulated to some extent in ebMS 2. However the approach has been to not do this. The ebXML context for this profiling document includes BPSS 1.x ((in RN PIPs: BPSS 1.01, though a customized version – validate against 1.01 at least. Some references will be made to ebBP 2.0 when appropriate), CPPA 2.0 / CPPA 2.1.

**ebXML バージョン (ebXML version) :** 次のリリースでは ebMS 3.0 がプロファイリングの対象となるが、今回は、ebMS 2.0 に焦点を当てる。ebMS 2.0 に対するプロファイリングは、ebMS 3.0 プロファイリングに大きく活用できると期待される。ebMS 3により本来サポートされる一部の魅力的な機能(メッセージの取り出しや、ペイロードを束ねる等)は、ebMS 2でもある程度対応することができるだろう。しかし、今回のアプローチではこれをしなかった。このプロファイル文書用の ebXML コンテキストは、BPSS 1.x (RN PIPs に対しては、BPSS 1.01 はカスタマイズされたバージョンであっても最低限 1.01 に対してバリデーションされる。リファレンスのいくつかは、適切であれば ebBP 2.0) 及び CPPA 2.0 / CPPA 2.1 に含まれるであろう。(CPPA- Collaboration Protocol Profile and Agreements : コラボレーション・プロトコル・プロファイル及び合意)

- Agreements: although ebMS is the target, the intent of this profiling goes beyond just wire interoperability and addresses some agreement aspects (CPA). Defining CPA templates or guidelines is the best way to represent the out-of-band agreement required for a practical deployment of PIPs. Only the part of the CPA that relates to messaging and maps to PIP definition data, will be profiled.

**合意 (Agreements) :** ebMS がターゲットではあるが、このプロファイリングの意図は、単なるワイヤ相互運用性の範囲を超え、いくつかの合意問題 (CPA: メッセージ交換プロトコル合意) を取り扱うことである。CPA テンプレート又はガイドラインを定義することは、PIP の実際の展開に必要な私的な合意 (out-of-band agreement) を示すもっともよい方法である。メッセージング及び PIP 定義データへのマップに関連した CPA の部分についてのみプロファイルする。

- Choreography: The approach is here to only cover the lowest level of choreography, involving signals possibly associated with only one action message. Any choreography that involves more than one action message (e.g. as in two-action PIPs) is out of scope of this profile specification.

**コレオグラフィ (Choreography) :** ここでのアプローチは、1アクション・メッセージのみに対応し、シグナルが関与する最も低いレベルのコレオグラフィのみをカバーする。複数のアクション・メッセージが関与するコレオグラフィ(2アクション PIP など)はこのプロファイル仕様の範囲外である。

### 1.3 一般的な方法論 (General Methodology)

- The Trading Partner Profiles (TPP) and resulting Abstract Trading Partner Agreement (ATPA) is a good starting point for users. Although the core of the ebXML profiling described here is defined solely based on mapping RNIF features into ebXML features (via the MMS-AMD [AMD] requirements), the ATPA represents parameters that need to be defined in order to complete a user-specific profiling of ebXML for a PIP deployment.

取引先プロフィール (TPP-Trading Partner Profiles) 及びその結果の取引先との取引契約要約 (ATPA-Abstract Trading Partner Agreement) はユーザーにとっていい出発点である。ここで示す ebXML プロファイリングの中核部分は、(MMS-AMD [AMD] 要件によって) RNIF 機能を ebXML 機能にマッピングすることによって単独で定義されるが、取引先との運用規約要約 (ATPA) は、PIP の展開のための ebXML のユーザー固有プロファイリングを完成させるために定義する必要があるパラメータを示す。

- From the TPP info, a CPP (Collaboration Protocol Profile) template can be filled for each partner, and a resulting agreement (TPA) can be mapped to a subset of the CPA. However, the suggested approach is for a business entity to directly define a partially-filled CPA with its capabilities and communication requirements (a “CPA profile”), then share this CPA profile with its business partner(s) who will complete it. The resulting document is a CPA instance.

TPP 情報から、取引先プロフィール (CPP- Collaboration Protocol Profile) テンプレートに各取引先について記入され、その結果得られる取引先との運用規約 (TPA) を CPA のサブセットにマップすることができる。しかし、提案されている方法は、企業体が能力および通信要件が部分的に記入された CPA (“CPA プロファイル”) を直接定義し、この CPA プロファイルを完成させる取引相手と共有するためのものである。結果として出てくる文書は、CPA インスタンスである。

- This CPA instance will be somehow orthogonal to PIPs: the deployment of several PIPs may share the same CPA instance. Conversely, several instances of the same PIP may use different CPAs, based on requirements that are specific to the nature of the document contents and other business considerations.

この CPA インスタンスは、どういうわけか PIP とは異なる。複数の PIP を展開することは、同じ CPA インスタンスを共有することになるかもしれない。逆に、同じ PIP の複数のインスタンスは、ドキュメント内容やその他のビジネス上の留意事項の性質に固有の要件に基づいた異なる CPA を使っているかもしれない。

- This document describes profiling rules for CPA and ebMS. These rules, when applied to data that is specific to business partners (TPA) and specific to targeted PIPs, will define specific messaging profiles.

この文書は、CPA 及び ebMS の **プロファイリング・ルール** を説明する。これらのルールは、取引先 (TP) 及び目的の PIP に特有のデータに適用される場合、特定の **メッセージ・プロファイル** を定義する。

- ebMS can be used with either BPSS or CPPA, and so both BPSS and CPPA can also be used when ebMS is used for RosettaNet. No attempt will be made to produce a complete profile for CPPA or BPSS for RosettaNet in this document. However, it will occasionally be explained what CPPA or BPSS features would need to be in a CPPA or BPSS that governed ebMS messaging when used for RosettaNet. These features can be understood as configuration input for the ebXML MSH mode of operation, as they may affect the MSH behavior without necessarily affecting the message header.

ebMS はBPSS とCPPAのいずれかが使用できるので、RosettaNetにebMS が使われている場合、BPSSとCPPA の両方を使用することもできる。本文書ではRosettaNet のためのCPPA またはBPSS の完全なプロファイルを提示することは試みていない。しかしながらRosettaNetに使用される場合、ebMS メッセージングにより支配されるCPPA またはBPSSの中に、どの CPPA またはBPSS 機能が必要であるか説明される場合もある。これらの機能は、メッセージヘッダーに影響するとは限らないもののMSH (Message Service Handler) の行動に影響するかもしれないので、ebXML MSH オペレーションモードのための設定入力として理解される。

Some general rules of ebMS profiling: ebMSプロファイリングのいくつかの一般的なルール:

- The proposed profiling in this document does not make use of extensibility points in the ebMS header, because it is unlikely that current MSH implementations can process these, even if they tolerate them.

本文書で提案されているプロファイリングは、ebMSヘッダーの拡張性ポイントを利用しない。というのは、現在のMSH実装は、こうしたポイントを許容するとしても、これらを処理できるとは考えられないからである。

- The ebMS header will fulfill the functions of the RNIF Delivery header, although it does not contain all the information present in the Delivery header. Some elements of the ebMS header will also map to elements from the Service header.

ebMSヘッダーには、デリバリー・ヘッダーにある全ての情報が含まれているわけではないが、RNIF デリバリー・ヘッダーの機能を果たす。ebMSヘッダーのいくつかの要素は、サービス・ヘッダーからの要素にもマップする。

- Clearly there is more data in Standard Business Document Header (SBDH) and/or RNIF Service Header than can be represented in ebMS headers (without using extensions). In case this data needs be preserved, then related XML parts need to be added in the payload, transparently to ebMS processing.

標準ビジネス文書ヘッダー (SBDH) および/またはRNIF サービス・ヘッダーの方が、(拡張なしの)ebMSヘッダーよりも明らかにデータが多い。このデータを保存する必要がある場合、関連するXML部品をebMS処理に透明な形でペイロードに追加する必要がある。

## 2 ebXML メッセージ概要 (ebXML Messaging Overview)

### 2.1 ebXML フレームワーク (The ebXML Framework)

The ebXML specifications support the exchange of business messages required to conduct electronic trading relationships between business partners. These capabilities logically separate but allow coordinated use of five key technologies important for eBusiness:

ebXML仕様は、ビジネスパートナー間で電子商取引を行う場合に要求されるビジネスメッセージの交換を支援する。これらの機能は理論的には別々であるが、eBusinessにとって重要な5つの主要な技術の相互活用を可能にする。

- Communicating data in common terms using a defined methodology (Core Components)

規定された手段(コアコンポーネント)を使った一般的な用語でのデータのやりとり。

- Defining business processes and assembling business transactions (ebXML Business Process Specification Schema, ebBP)

ビジネスプロセスを定義し、商取引(ebXML ビジネスプロセス仕様スキーマ, ebBP)を纏める。

- Providing secure and reliable transport (ebXML Messaging Service [ebMS]) . Registering and making available key eBusiness artifacts and services (ebXML Registry Services [ebRS] and Registry Information Model [ebRIM])

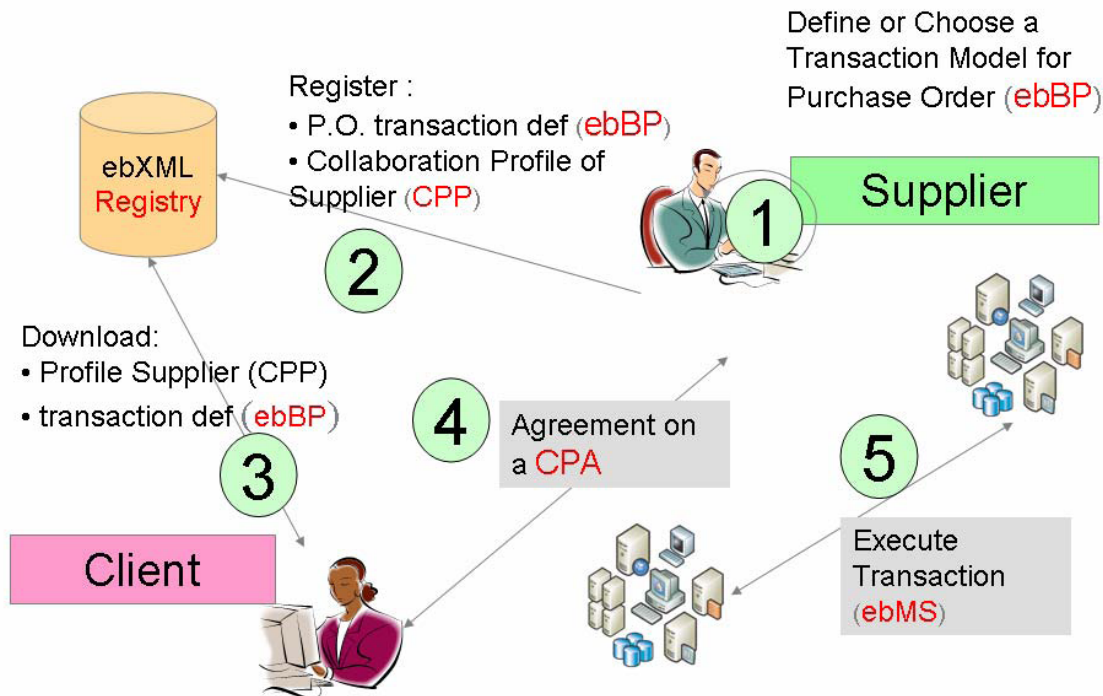
安心かつ信頼できるトランスポート層の提供。(ebXML メッセージングサービス[ebMS])。

重要なeBusinessの作成物やサービス(ebXML 登録サービス [ebRS] (ebXML Registry Services))及び登録情報モデル(登録情報モデル [ebRIM] (Registry Information Model))を登録し、利用可能にする。

- Providing a technical configuration contract between business partners (Collaboration Protocol Profile and Agreements [CPP/CPA])

ビジネスパートナー間の技術的設定契約を提供する。(取引先 プロファイル及びメッセージ交換プロトコル合意 [CPP/CPA])

## An ebXML Scenario



The business case and requirements that prompted the development of the set of ebXML specifications were to:

一連のebXML仕様の開発を促したビジネス事例及び要求事項は次のようなものであった。

- Provide a migration path for and leveraging of EDI-compatible technologies.  
EDI互換性技術の移行方法及び活用を提供すること。
- Develop openly accessible technologies for Small-Medium Enterprises whether in a managed or non-managed environment.

管理、無管理環境に関係なくオープンにアクセスできるSMEのためのテクノロジーを開発すること。

- Enable all supply-chain partners using XML technologies.

XML技術を用いて、全てのサプライチェーンパートナーとの連結を可能にすること。

- Provide an integrated eBusiness approach focused on interoperability needs, while maintaining loosed-coupling to backend systems.

バックエンド・システムとの疎結合を維持しながら、相互運用性ニーズを重視した統合的 eBusinessアプローチを提供すること。

The heterogeneous nature of eBusiness transactions require a flexible infrastructure and architectural framework that can support service calls (catalog status requests) and more complex document exchange (offers and acceptance).

eBusinessのやりとりが色々な種類のものである性質上、サービスコール(カタログ状況要求)や、より複雑なドキュメントの交換(オファー及び受諾)をサポートできる柔軟なインフラやアーキテクチャの枠組みが必要である。

The business document processing was decoupled from the messaging layer. The consumer of these documents may be a service, a business process instance, or middleware or business application interested in the business document contents.

ビジネス文書処理は、メッセージレイヤから分離させた。これらの文書の使われる先は、サービス、ビジネスプロセスインスタンス、またはビジネス文書の内容に関心があるミドルウェアまたはビジネスアプリケーションなどが考えられる。

Such documents cannot be directly associated with an application service in a predefined way. The coupling between the messaging system and the consumers of these messages must be supported in an adaptable way.

そのような文書は、所定の方法でアプリケーションサービスに直接的に関連している可能性はない。メッセージングシステムとこれらのメッセージの消費者の間の結合は、柔軟な方法でサポートしなければならない。

## 2.2 ebXML メッセージング (ebXML Messaging)

The ebXML Messaging Service technical specification defines a communications protocol neutral method for exchanging electronic business messages. It defines specific enveloping constructs that support reliable, secure delivery of business information and permits messages to contain payloads of any format type. This versatility ensures legacy electronic business systems employing traditional syntaxes (i.e. UN/EDIFACT, ASC X12, or HL7) can leverage the advantages of the ebXML infrastructure along with users of emerging technologies. For example, the ebMS may be used with the Collaboration Protocol Profile and Agreements (CPPA) and Business Process Specification Schema (ebBP).

ebXMLメッセージサービス技術的仕様は、電子ビジネスメッセージの交換のための中立的な方法の通信プロトコルを定義する。信頼でき、安全なビジネス情報の配信をサポートする特有の構造の封筒を定義し、いかなるタイプのフォーマットの本文も持つことができるようにする。この多様性は従来の構文を使っているレガシー電子ビジネスシステム(例: UN/EDIFACT, ASC X12, or HL7)が、新しいテクノロジーのユーザーと同様に、ebXMLインフラの利点を必ず活用できるようにする。例えば、ebMSは取引先・プロフィール及びメッセージ交換プロトコル合意(CPPA-Collaboration Protocol Profile and Agreements)やビジネスプロセス仕様スキーマ(ebBP-Business Process Specification Schema)と一緒に使うことができる。

### メッセージング概観 (Messaging Overview)

ebMS was developed to provide the secure and reliable transport of electronic messages, while enabling the transition from legacy to new and emerging technologies. The ebMS protocol supports any communication protocol, and provides bindings for HTTP and SMTP. Multiple message exchange patterns including push and pull that map to different types of business transactions.

ebMSは、レガシーから新技術や新興技術への移行を可能にしながら、安全で信頼できる電子メッセージのやりとりを提供するために開発された。 ebMSプロトコルはいかなる通信プロトコルもサポートし、HTTPとSMTPとの結合を提供する。異なるタイプの商取引交換をマップするプッシュ/プルなどを含む複数のメッセージ交換パターンをサポートする。

### ebXML メッセージ標準の状況 ( Status of ebXML Messaging Standards )

The ebMS v2.0 OASIS Standard was approved in August 2002, and, in May 2004, submitted and accepted an ISO standard, ISO/TS 15000-2. The v3.0 working draft is under development.

ebMS v2.0 OASIS標準は、2002年の8月に承認され、又、2004年5月にISO/TS 15000-2に提案、承諾された。v3.0のワーキングドラフトは、現在作成中である。

In v2.0, the current feature set for ebMS includes:

#### V2.0におけるebMSの現在の機能セットは次の物を含む:

- Packaging : パッケージング
- SOAP envelope extensions : SOAP封筒の拡張
- Error handling : エラー処理
- Security : セキュリティ
- Synchronous responses : 同期した応答
- Reliable messaging : 信頼のあるメッセージ(到達保証、重複防止、順序保証)  
(at-least-once, at-most-once, ordering)
- Message status service : メッセージの状況サービス
- Multi-hop : マルチホップ

The ebXML Messaging Service v3.0 working draft is seeking to express compatibility to or use with emerging web services standards or specifications. Seeking to leverage the ebXML capabilities and those of emerging standards and specifications, the ebMS will define how technologies such as WS-Reliability and WS-Security, for example, may be used and the role of WS-I Basic Profile conformance. Compensability with WS-Addressing is also under consideration.

ebXMLメッセージサービスv3.0のワーキングドラフトは、新しく出現したウェブサービス規格または仕様との互換性を示すことまたは使うことを目指している。ebXML 機能及び新しく出現した規格や仕様を活用することを目指し、ebMSは、例えばWS-信頼性 やWS-セキュリティー等の技術がどのように使えるか、そしてWS-I 基本プロファイルに対する適合性の役割を定義する。WS-アドレッシングとの補償可能性についても検討されている。

The ebMS technical specification v3.0 will support:

ebMS 技術仕様書 v3.0 は、以下をサポートする:

- Web services protocols for security, reliability and addressing.  
保障、信頼性、アドレッシングに関するWebサービスプロトコル
- Low-level payload processing (payload services)  
低レベルのペイロード処理(ペイロードサービス)
- Message exchange patterns that map to business transactions.  
メッセージ交換パターンをビジネス取引に対応させる。
- Connectivity constraints (occasional connectivity, firewall restrictions, ebMSlite clients, etc.)  
接続性の制限 (時折接続される、ファイヤーウォールの制限、ebMSlite端末、等)

### 3 取引先との運用規約 TPA (Trading Partner Agreement)

#### 3.1 TPA と 基盤展開パラメータ (TPA and Infrastructure Deployment Parameters)

This table shows the relationships between TPA and ebXML components. It shows how elements of a TPA relate to the ebXML components. A dependency in the table indicates that some features of the ebXML component are concerned by the TPA item, or even further, that the feature must comply with the profiling described in this document.

この表は、TPA と ebXML 構成要素の関係を表したものである。如何に TPA の各要素が ebXML の構成要素と関係しているかが良くわかる。ebXML コンポーネントの一部の機能が TPA 項目と関係がある、あるいは、更にその機能は本文書に記載のプロファイリングに適合しなければならないことを、表における従属関係は示している。

The elements of a TPA that do not directly affect the standardized features of an ebXML component may still concern this component, but its impact will be at implementation, administration or deployment level, i.e. will affect the operational aspect, which is outside the scope of this profiling guideline.

直接的に ebXML コンポーネントの標準化された機能に影響していない TPA の要素が、それでもこのコンポーネントと関係する可能性はあるが、その影響は、実装、管理、又は展開レベル等の運用面に見られ、このプロファイル基準の対象外である。

- An “F” means that the answer to the question will affect features that are specified in the related standard (ebMS, CPPA or BPSS). In other words, a compliant implementation to these standards explicitly supports answers to this question.

“F”は、質問に対する回答が関連規格(ebMS、CPPA または BPSS)で規定される機能に影響することを意味する。言い換えると、これらの基準に適合した実装は、この質問への回答を明白に支持する。

- An “X” means that depending on the user answer to the question, the usage of this ebXML component will be affected in a way that must comply with the profiling defined in this document. In other words, you need to be aware of this profiling in order to implement the answer in a compliant way.

“X”は、質問に対するユーザーの回答によっては、この ebXML コンポーネントの使用法は、本文書に記載のプロファイリングに適合しなければならないという形で影響を受けることを意味する。言い換えると、適合する方法で回答を実施するためには、このプロファイリングを知る必要がある。

- No mark means no direct effect or dependency on features that are specified in the related standard. The answer to the question becomes more a product implementation or deployment issue (how well this is handled depends more on additional product features than on conformance to the standard.)

マークがないのは、関連規格で規定される機能への直接的な作用または従属が一切ないことを意味する。質問に対する回答は、むしろ製品実装または展開上の問題となる(いかにうまくこれに対処するかは、基準への適合性よりも製品のその他の機能に依存する)。

TPA Item	ebMS	CPPA	BPSS (no profiling defined here)
General Operation Parameters 一般的な運用に関するパラメーター			
Specify the standard you will use to identify trading partners. (DUNS, GLN, other authority name) あなたが取引相手特定のために使う標準を指定してください。 (DUNS、GLN、他の標準機関名)	FX	FX	
What is the maximum volume of messages you expect to exchange with any specific trading partner? What is the average? 貴社が特定の取引相手と交換しようとしているメッセージの最大量は、どの位ですか？又、平均は、どの位と想定していますか？			
What is your peak time interval? 貴社のピーク時間帯は、どの位ですか？			
What is the average size of the message during the peak time interval? ピーク時間帯におけるメッセージの平均サイズは、どの位ですか？			
How many messages do you receive and send during the peak time interval? ピーク時間帯にどの位のメッセージを送受信しますか？			
Will you use peer-to-peer routing or will you be using a messaging service (MS) (temporary message store)? 1対1ルーティングを利用されますか？又は、メッセージングサービス (MS: 一時的メッセージ保管) を利用されますか？			
Will you operate via a message Hub, or directly point-to-point? メッセージハブを通して通信されますか？それとも直接1対1で、通信されますか？	FX	F	
If using a Hub, which message data will be used for doing routing? ハブを使うならば、どのメッセージデータを、ルーティングとして使用しますか？	FX		
Which of these Message Exchange Patterns will you be using? One-Way, Request-Response, Notification, Solicit-Response メッセージ交換方式としてどのような方式が使われますか？ 一方通行、要求-応答、通知、請求-応答	FX	FX	F
Will you need to correlate messages from a single PIP instance, or will you need to correlate messages from several PIP instances, as belonging to a same long-lasting conversation (e.g. for monitoring purpose) 同じ継続する会話として、一つのPIPインスタンスからのメッセージを関連づけますか？又はいくつかのPIPインスタンスからのメッセージを関	FX	FX	F

連づけますか?(例:モニターする目的のために)			
Will you be using a specific registry? If Yes, please specify 特定のレジストリーを使われますか? Yesならば、明示して下さい			
Will you be defining specific roles for each party of each business process? 各ビジネスプロセスで、各々の関係者の明確な役割を定められていますか?	FX	FX	F
Indicate the level of Management Services you will require for your messaging system メッセージシステムのために必要とするマネージメントサービスのレベルを示して下さい	F		
Do you need to track messages based on their participation in complex business processes? 複雑なビジネスプロセスにおいて、彼らの参加に関するメッセージの追跡が必要ですか?	FX (maybe)		
Do you need status services? 状況サービスは必要ですか?	F (maybe)		
Do you need remote management? 遠隔管理は必要ですか?			
Do you need monitoring? 監視機能は必要ですか?	FX (maybe)		
Do you need BI support? BIサポート機能は必要ですか?			
Do you require disaster recovery? 災害復旧機能は必要ですか?			
Do you require Debugging capabilities? デバッグ機能は必要ですか?			
Indicate the level of Connectivity you will have with the Internet インターネットで必要な接続性のレベルを示して下さい			
Are you occasionally connected (dialup with modem?) 時折接続ですか(モデムによるダイヤルアップ)?	F	F	
Are you permanently connected with a permanent IP address (T1, DSL)? 静的IPアドレスを使用して、常時接続を行いますか(T1, DSL)?	F	F	
Are you permanently connected without a permanent IP address (Cable)? 静的IPアドレスを使用しないで、常時接続を行いますか(ケーブル)?	F	F	
Indicate the Security Services you will require for your messaging system メッセージシステムにおけるセキュリティサービスの要望について			

Do you need the headers to be encrypted? ヘッダーの暗号化は必要ですか？	FX	FX	
Do you need the payload to be encrypted? Using which method? (S/MIME, XML Encryption) ペイロードの暗号化は、必要ですか？ どの方法を用いて？(S/MIME、XML暗号化)	FX	FX	
Do you need non-repudiation of origin? 発信元の否認防止を必要としますか？	F	F	
Do you need non-repudiation of receipt? 受領の否認防止を必要としますか？	FX	FX	
If need non-repudiation of receipt, is it required to have a digest of the acknowledged message in the acknowledgement, or is a simple reference to Message ID sufficient? 受領の否認防止が必要な場合、応答メッセージの中に応答確認の要約を必要としますか？又は、メッセージ IDへの単純な参照で充分ですか？	FX		
Do you need to digitally sign your messages (i.e.:X.509)? 電子署名(例:X.509) が必要ですか？	FX	FX	
Do you want to transport level encryption? (i.e.: TLS/SSL)? トランスポート層での暗号化が必要ですか？(例:TLS/SSL)	F	F	
Do you require timestamp of your messages? メッセージに対するタイムスタンプは必要ですか？	F		
Do you subscribe to authority domains? (i.e.: DUNS/GLN/EANUCC/ DUNS+ 4/Vertical) 標準機関と契約されていますか？ (例:DUNS/GLN/EANUCC/ DUNS+4/Vertical)	FX	F	
Indicate the Reliability you will require for your messaging system メッセージシステムにおける信頼性の要望について			
Do you need guaranteed message delivery? (include ACK signals) 保障されたメッセージの到達が必要ですか？(受信確認信号を含めて)	FX	FX	
Do you need de-duping? 重複削除が必要ですか？	FX	FX	
Do you require Ordered Delivery? 順序だてた配信が必要ですか？	FX	FX	
Do you require a Manifest? 目録が必要ですか？	F		
Do you require expiration control? 期限管理が必要ですか？	F		

Indicate what you will need to compress in your messages メッセージにおける圧縮の必要性について			
Do you need to compress headers? ヘッダーの圧縮は必要ですか？	F		
Do you need to compress payload? 本文の圧縮は必要ですか？			
Do you need to compress attachments? 添付の圧縮は必要ですか？			
Indicate the Error Handling you will require for your messaging system メッセージシステムにおけるエラー処理の要望について			
Do you need Message Service error handling (too many retries, etc.)? メッセージサービスにおけるエラー処理は必要ですか(再送制限等)	F	F	
Do you need Message Content error handling (invalid message, etc.)? メッセージ内容のエラー処理は必要ですか(無効メッセージ等)			
Do you need out of band error notification? 規定外データ(OOB) エラー処理は必要ですか？			
Indicate the Payload Capabilities you will require for your messaging system メッセージシステムにおける本文(Payload)能力に対する要望について			
Do you need Globalization/I18? グローバリゼーション/I18が必要ですか？	F		
Do you need attachments? 添付は必要ですか？	F		
Do you need payload validation? 本文(Payload)の検証は必要ですか？			
What type of payload will you be exchanging, ASCII, Binary or both? どの様な本文の交換を考えていますか？アスキーASCII, バイナリー又は両方どの様なPayloadの交換を考えていますか？ASCII, Binary 又は両方？			
Will you need to support different versions of PIPs? 異なったバージョンのPIPのサポートが必要ですか？			
Indicate the requirements imposed by integration with existing software 既存ソフトウェアとの統合に関する必要条件について			
Do you need to preserve (some) previous message header structures (not native to ebMS) as is, so that you	FX		

can reuse back-end binding technology? バックエンドの関連付け技術を再利用するために、前のメッセージヘッダー内容を (ebMS固有でない) そのまま保存する必要がありますか？			
Do you need to move message header data into your back-end? バックエンドシステムに、メッセージヘッダーのデータを移動させる必要はありますか？	FX		

### 3.2 CPP と CPA プロファイリング (CPP and CPA Profiling)

Part of the TPA options of the previous section will map to the CPA, or to the Collaboration Protocol Profiles (CPP).

前節のTPAオプションの部分は、メッセージ交換 プロトコル合意 (CPA-Collaboration Protocol Agreement)、又は取引先 プロファイル (CPP-Collaboration Protocol Profiles) に対応する。

Business partners may define CPP that represent their capabilities and roles they can assume. Another approach is for a business party to directly start by defining a CPA template that this party will pre-fill with its own data, and that it will communicate to its partners for them to complete. The partially created CPA (or CPA template) will narrow the options that a CPP would offer, down to a very specific way under which this party wishes to interoperate. This is the approach suggested here.

取引相手は、彼等が担うことのできる機能及び役割を表すCPPを定義するでしょう。別のアプローチは、取引当事者が自らのデータをCPAテンプレートに事前に記入することから始め、そして相手方に送って完成させることである。部分的に作成されたCPA(あるいは、CPAテンプレート)は、CPPにある選択肢を本当事者が希望する相互運用のための極めて限定された方法にまで範囲を狭めることになる。次は、ここで提案されるアプローチである。

A party may define a few of such CPA templates that express different modes of connectivity, different roles and collaborations and different QoS attributes. The reason for doing so is that its business partners may have different profiles. For example, three Trading Partner profiles have been identified in [AMD]. A CPA template may be intended for each one of these partner profiles.

当事者は異なる接続モード、異なる役割及びコラボレーション、また異なるQoS属性を表すいくつかのCPAテンプレートを定義することができる。なぜなら、各々のビジネスパートナーは、異なるプロファイルを持っているからである。例えば、3つの取引先データが[AMD]において識別されているとして、CPAテンプレートは、これらの取引先プロファイルのそれぞれに対して1つずつ作られる可能性がある。

There is no 1-to-1 correspondence between CPAs and PIP definitions.

CPAとPIP定義の間に1対1の対応はない。

- Instances of the same PIP may need to be executed using different CPA templates (or different CPA instances from the same template) depending on which types of partners are involved, and which QoS or execution context is required.

同じPIPのインスタンスであっても、関与する相手方のタイプがどれか、及び必要とされるのはどのQoSか？  
又は、実行に必要な情報であるかによって異なるCPAテンプレート(又は、同一テンプレートの異なるCPAインスタンス)を使用して、実行する必要があるだろう。

- Instances of different PIPs or TPIR-PIPs may use CPAs that derive from the same CPA template, yet these CPA instances will not be shared across different PIP definitions, since the PIP (or TPIR-PIP) identity appears as attribute of the CPA instance.

異なるPIPまたはTPIR-PIPのインスタンスは、同一CPAテンプレートからできたCPAを使用する可能性があるが、PIP識別子はCPAインスタンスの属性として現れるので、これらのCPAインスタンスは、異なるPIPにわたって共有されることはない。

The profiling and definition of CPA data (both instance and template) can be facilitated using a set of forms that we define in Appendix A.

CPAデータ(インスタンスとテンプレートの両方)のプロファイリング及び定義は、私たちが付録Aに記載するフォーム一式を使用して進めることができる。

## 4 メッセージの解説 (Message Description)

### 4.1 ebMS 2.0 プロファイリングに関する一般的な手引き (General approach for ebMS 2.0 profiling)

#### 4.1.1 ebMS メッセージヘッダーと RosettaNet メッセージヘッダー (ebMS message headers and RosettaNet message headers)

##### RNIFのヘッダー: RNIF Headers:

The existing RNIF headers are dealt with in the following way:  
既存のRNIFヘッダーは、以下の方法で対応する:

- The RNIF Preamble header is not supposed to appear anymore in the ebMS message.

RNIF前文ヘッダーは、もはやebMSメッセージに表示されない。

- It is replaced by the ebMS header. Although not all the information encoded in the Delivery header will be translated into the ebMS header, this header is not relevant anymore in the ebXML context.

それはebMSヘッダーに置き換わる。デリバリーヘッダーに符号化される全ての情報がebMSヘッダーに翻訳されるわけではないけれども、このヘッダーはもはやebXMLコンテキストに適しない。

- The RNIF Service header may still be present in the ebMS message, in case it is needed for binding a message to existing PIP software that needs to be reused with ebXML. Some but not all of its elements map to the ebMS header. The Service header may be preserved as a separate attachment in the ebMS payload. However, in case of conflict between data in Service header and analogous data in ebMS header, the ebMS header will prevail as long as the messaging transfer is still in progress (this includes routing in multi-hop environments).

RNIFサービスヘッダーは、ebXMLで再利用する必要がある既存のPIPソフトウェアにメッセージを結合するために必要とされる場合、依然としてebMSメッセージに記載されるであろう。その要素の全てではないが、一部はebMSヘッダーに組み込まれる。サービスヘッダーは、ebMSペイロードに別の添付ファイルとして保存される可能性がある。しかし、サービスヘッダーのデータとebMSヘッダーの類似データの間に矛盾が発生する場合は、メッセージの転送が進行中である限り(これはマルチホップ環境でのルーティングを含む)、ebMSヘッダーが優先する。

##### 標準[ビジネス]文書ヘッダー (SBDH): Standard [Business] Document Headers (SBDH):

Not all information in the SBDH will map to ebMS headers. In case where an SBDH structure is present and used in the binding of the message with backend processes, it is recommended to keep the SBDH in the payload. However, in case of conflict between data in SBDH and analogous data in ebMS header, the ebMS header will prevail as long as the messaging transfer is still in progress (this includes routing in multi-hop environments).

SBDH (Standard Business Document Headers)の全ての情報がebMSヘッダーに対応するわけではない。SBDH構造が存在し、情報のバックエンドプロセスとの結合に使用される場合、SBDHをペイロードに保つことが推奨される。しかし、サービスヘッダーのデータとebMSヘッダーの類似データの間に矛盾が発生する場合は、メッセージの転送が進行中である限り(これはマルチホップ環境でのルーティングを含む)、ebMSヘッダーが優先する。

There are two options to consider: 二つのオプションについて考える。

1. The PIP document is defined using XML schema. In this case the SBDH is bound to the PIP document, and both represent a single MIME part (SOAP attachment). The ebMS2 message has then two MIME parts: (a) the SOAP envelope (ebMS2 header), (b) the payload (SBDH + PIP).

PIP文書は、XMLスキーマを使用し定義される。この場合、SBDHはPIP文書に結合され、両方とも単一のMIMEパート(SOAP添付)となる。そこで、ebMS2メッセージは2つのMIMEパートを持つ：

(a) SOAPエンベロープ(ebMS2ヘッダー)、(b) ペイロード(SBDH + PIP)

2. The PIP document is defined using DTD. In this case, no SBDH instance is required (additional meta-data that may be needed and that is not in ebMS headers, is supposed to be found in Service header – which can be preserved as a separate MIME part in the ebMS payload if needed -, and FromRole + ToRole elements of PIPs.)

PIP文書は、DTDを使用し定義される。この場合は、SBDHインスタンスは一切必要とされない。(必要とされる可能性があるが、ebMSヘッダーにない追加のメタデータは、サービスヘッダーにあると思われ、必要な場合にはebMS本体の個別のMIMEパート、及びPIPのFromRole+ToRole要素として保管される)。

### ebMSヘッダーの拡張 (ebMS header extensions)

Although the ebMS header is extensible, extension elements should not be used to store data from previous headers (Delivery, Service) that could not be mapped. The reason for this is that MSH implementations are not required to process these extensions. Instead, in case the non-mapped information of legacy headers must be preserved in the message, these headers should be included as is in the payload (e.g. as attachments). A deployment that conforms to this messaging profile MUST NOT use such extensions.

ebMSヘッダーは拡張性があるが、マップできなかった元のヘッダー(デリバリー、サービス)のデータを保存するために、拡張エレメントは使用するべきでない。その理由は、MSH実装ではこれらの拡張を処理する必要がないからである。むしろ、古いヘッダーのマップされない情報をメッセージに保存しなければならない場合、これらのヘッダーは、今迄通り本体(例えば、添付ファイルとして)に包含されるべきである。このメッセージ・プロファイルに適合させる場合には、そのような拡張を使用してはならない。

### 既存のインフラストラクチャーとの統合 (Integrating with existing infrastructures:)

In order to preserve the ability to reconstruct the former RNIF structure (minus preamble and delivery headers), in case some users consider this a good integration approach with existing systems, the Service header MAY be included as a separate MIME part in the ebMS2 message, i.e. as an additional SOAP attachment element of the ebMS payload.

旧来のRNIF構造(前文ヘッダー及びデリバリー・ヘッダーを差し引いたもの)を再構築する能力を維持するために、一部のユーザーがこれを既存のシステムとの優れた統合方法と考える場合、サービス・ヘッダーはebMS2メッセージのMIME個別パートとして、即ち、ebMSペイロードのSOAP添付要素として、含まれる可能性がある。

#### 4.1.2 ペイロードバンドル及びメッセージバッチング(Payload bundling and message batching)

- **Bundling of payloads** is the grouping of several payloads within the same message, along with the ability to process each payload differently, as if they were carried in different messages. The message header is not repeated: it is common to all the payloads in the bundle. In case the payloads are not intended to share the same header elements (e.g. not intended to the same party, or same business process) then they cannot be bundled in ebMS 2.0. Although it is possible to group several payloads in the same message as attachments, an ebMS 2.0 MSH would not be able to process these differently as the same set of header elements would apply to all of them.

ペイロードのバンドリングとは、それぞれに違う処理をする能力を持ちながら、同一メッセージ内に複数のペイロードをグループ化することであり、それはあたかも各ペイロードが異なるメッセージで運ばれるようである。メッセージ・ヘッダーは、繰り返さない:バンドル内における全てのペイロードに共通しているため。ペイロードが同じヘッダー要素を共有することを意図しない(たとえば、同じ当事者または同じ取引プロセス用ではない)場合は、ebMS 2.0 でバンドルされない。同じメッセージに添付ファイルとして複数のペイロードをグループ化することは可能であるけれども、ebMS 2.0 MSHは、全てに適用されるであろう同じヘッダー要素の一式としてこれらを異なって処理することはできないだろう。

- **Message batching** is the ability to nest several ebMS messages (including their individual headers) within the same ebMS message, and on the receiver side to process them individually as if they had been received separately. The difference with payload bundling is that a set of well-formed ebMS messages would be bundled, not just their payloads. On receiver side, after unpackaging, each one of these messages is processed individually as if it had been received separately. This can be done by compressing each individual ebMS message as a MIME part. Although this can be implemented by using compressed attachments, ebMS 2.0 does not support batching of messages as a specified MSH function.

メッセージ・バッチングは、同一のebMSメッセージ内に複数のebMSデータ(個別ヘッダを含めて)をまとめ、受信者側でそれらを別々に受け取ったかのように、個別処理を行う能力である。ペイロード・バンドルとの差は、単にペイロードだけでなく、XMLに要求される文法に従ったebMSメッセージ1式がバンドルされるということである。受信側では、解梱後、あたかも別々に受け取ったように、それらは個別に処理される。個々のebMSメッセージをそれぞれMIMEの一つのパートとして圧縮することによって、これを行うことができる。圧縮された添付ファイルを使用することによって、これは実施できるけれども、ebMS 2.0 は規定のMSH機能としてメッセージのバッチングをサポートしていない。

For these reasons, neither message batching nor payload bundling is recommended when profiling of ebMS 2.0.

このような理由で、ebMS 2.0 のプロファイリングを行う時は、メッセージのバッチングも、またペイロード・バンドルも推奨されない。

## 4.2 ebMS ヘッダープロファイリング (ebMS Header Profiling)

The tables below are borrowed from the Deployment Profile Template 1.1 for ebMS 2.0, [DPT-ebMS2] a document guide for deploying ebMS that has been developed by the ebXML

Implementation, Interoperability and Conformance OASIS TC. It is recommended that business partners make use of the full document to define their own deployment profile. Only the subset of this document that is affected by the MMS profiling is used here.

以下の表は、ebXML実装、相互運用性及び適合性OASIS TCによって開発されたebMS展開用の文書ガイドである ebMS 2.0 のための展開用プロファイル・テンプレートからの引用である。取引先は、独自の展開用プロファイルを定義するために、必要事項が全て記載されている文書を使用することが推奨される。ここでは、MMSプロファイルに該当したこのドキュメントの一部を利用される。

#### 4.2.1 プロファイル要求事項 eb:PartyId (Profile Requirement Item eb:PartyId)

Specification Feature	Header elements: eb:MessageHeader/eb:From/eb:PartyId eb:MessageHeader/eb:From/eb:PartyId/@type eb:MessageHeader/eb:To/eb:PartyId eb:MessageHeader/eb:To/eb:PartyId/@type
Specification Reference	ebMS 2, section 3.1.1.1 "PartyId Element"
Profiling	<p>One instance of PartyId (in case several exist) must have as value either a DUNS (or DUNS+4) or Global Location Number (GLN). Both should not be found at the same time under the same From or To element.</p> <p>PartyId の 1 つのインスタンス(複数存在する場合)の値は、DUNS(又は DUNS+4)、又は GLN (Global Location Number)のどちらかでなくてはならない。どちらも、同一の From 要素、又は To 要素下で同時に見つからないものとする。</p> <p>When several PartyId are present, the one above should be the first PartyId element. It is allowed to have additional PartyId elements in eb:From or in eb:To (they just need to have different @type values)</p> <p>複数の PartyId が存在する場合、上記のものが最初の PartyId 要素となる。          eb:From 又は eb:To に追加の PartyId 要素があることは、許される。(但し、異なった@type 値を持つ必要がある)</p> <ul style="list-style-type: none"> <li>PartyID values MUST comply with ISO 6523 values, when applicable. That includes DUNS and GLN identifiers.              適用できる場合、PartyIDの値はISO 6523の値に準拠しなくてはならない。DUNS 及びGLNを含む。</li> <li>PartyID type attribute MUST be used to represent the Domain name and ICD (International Code Designator) according to section 24 "PartyID" of the CPPA V2.1 specification, found in: <a href="http://www.oasis-open.org/committees/ebxmlcppa/documents/ebCPP-2_1.pdf">http://www.oasis-open.org/committees/ebxmlcppa/documents/ebCPP-2_1.pdf</a> (April 2005)              PartyIDのタイプ属性は、CPPA V2.1仕様の24項"PartyID"に準拠し、ドメイン名およびICD: International Code Designator (国際コード指定子)を表すために使用されなければならない。 <a href="http://www.oasis-open.org/committees/ebxmlcppa/documents/ebCPP-2_1.pdf">http://www.oasis-open.org/committees/ebxmlcppa/documents/ebCPP-2_1.pdf</a> (April 2005)を参照。</li> </ul>

	<p>More generally:もっと一般的に:</p> <ul style="list-style-type: none"> <li>the type value of the type attribute MUST be a URN. If the type attribute is present, then it provides a scope or namespace for the content of the PartyId element. タイプ属性のタイプ値は URN でなければならない。タイプ属性が存在する場合、それは PartyId 要素の中味の範囲、又は名前空間を提供する。</li> <li>if the type attribute is not present, the content of the PartyId element MUST be a URI that conforms to [RFC2396]. タイプ属性が存在しない場合、PartyId 要素は[RFC2396]に準拠する URI でなければならない。</li> </ul> <p>If an abbreviated name is described in the item titled “Name of Coding System” within the ICD list, it should be used, followed by the ICD value. ICD リスト内の“コーディングシステム名”というタイトルのアイテムに略称が記述されている場合は、それを使用し、続いて ICD 値を使用するのがよい。</p> <p>Example: &lt;tp:PartyId tp:type=" urn:oasis:names:tc:ebxml-cppa:partyid-type:D-U-N-SNumber:0060"&gt;123456789&lt;/tp:PartyId&gt; Where “0060” is the ICD value of D-U-N-S Number.</p>
Alignment	<ul style="list-style-type: none"> <li>MUST map to (RNIF, Delivery Header) element: PartnerIdentification / GlobalBusinessIdentifier.</li> <li>MUST map to (Standard Bus. Doc Header - SBDH) element: PartnerIdentification (choice of Duns / Duns+4), when applicable.</li> <li>MUST map to ebXML CPPA 2.0 or 2.1 element: PartyInfo/PartyId, when used.</li> </ul> <p>Value and type MUST conform to ISO 6523 when applicable, and the type attribute to section 24 “PartyID” of the ebXML CPPA V2.1 specification.</p> <p>適用する場合、値ならびにタイプはISO 6523、タイプ属性はebXML CPPA V2.1仕様の24項“PartyID”に準拠しなければならない。</p>
Test References	

#### 4.2.2 プロファイル要求事項 eb:Role (Profile Requirement Item eb:Role)

Specification Feature	Header elements: eb:MessageHeader/eb:From/eb:Role eb:MessageHeader/eb:To/eb:Role
Specification Reference	ebMS 2, section 3.1.1.2 “Role Element”
Profiling	Role Name of the partner in this business transaction (in Partner Role Description of the PIP) Example: <eb:To>

	<pre>&lt;eb:PartyId eb:type=" urn:oasis:names:tc:ebxml-cppa:partyidtype: D-U-N- SNumber:0060"&gt;myDUNS&lt;/PartyId&gt; &lt;eb:Role&gt;Seller&lt;/eb:Role&gt; &lt;/eb:To&gt;</pre>
Alignment	<ul style="list-style-type: none"> <li>• MUST map to (RNIF, Service Header) element: from{ to} Role/GlobalPartnerRoleClassificationCode</li> <li>• MUST map to ebXML BPSS: the role value maps to the corresponding BinaryCollaboration/Role/@name in BPSS 1.* or ebBP 2.0 definition, when used.</li> <li>• MUST map to ebXML CPPA 2.0 or 2.1 element: CollaborationRole/ Role/@name, when used.</li> </ul>
Test References	

#### 4.2.3 プロファイル要求事項 eb:Service (Profile Requirement Item eb:Service)

Specification Feature	Header element Header element: eb:MessageHeader/eb:Service
Specification Reference	ebMS 2, section 3.1.4 "Service Element"
Profiling	<p>This value MUST be the same as the one used in the BPSS instance for the PIP. Its format must be:</p> <p>この値はPIPのBPSSインスタンスで使用される値と同一でなければならない。そのフォーマットは以下の通りでなければならない。</p> <p>"urn:rosettanet:specification:interchange:PIP" + &lt;alphanumeric name of PIP&gt; + ":xml:bpss:" + &lt;PIPVersionIdentifier&gt; .</p> <p>The Service element MUST have same value for all messages involved in a single PIP or TPIR-PIP (whether it is an Action, Confirmation or Signal message).</p> <p>サービス要素は、単一PIP 又はTPIR-PIPに含まれる全てのメッセージと同じ値を持たなければならない。(アクション、確認、又はシグナルメッセージのいずれであっても)</p> <p><u>Example:</u> If in BPSS: <b>nameID</b>="urn:rosettanet:specification:interchange:PIP7C7:xml :bpss:v11_00" <b>version</b>="V11.00"</p> <p>In ebMS header: &lt;eb:Service&gt; urn:rosettanet:specification:interchange:PIP7C7:xml:bpss:v11_00&lt;/ eb:Service&gt;</p>
Alignment	<ul style="list-style-type: none"> <li>• MUST map to ebXML BPSS 1.* or ebBP 2.0 element when used: ProcessSpecification/@uuid or if not present, ProcessSpecification/@NameId</li> </ul>

	<ul style="list-style-type: none"> <li>• MUST map to ebXML CPPA 2.0 or 2.1 element, when used: Service/@name</li> </ul>
Test References	

#### 4.2.4 プロファイル要求事項 eb:Action (Profile Requirement Item eb:Action)

Specification Feature	Header element: eb:MessageHeader/eb:Action
Specification Reference	ebMS 2, section 3.1.5 “Action Element”
Profiling	<p>In case of an Action message, the value MUST be consistent with Global Business Action Code (camel case version of this value).</p> <p>アクション・メッセージの場合には、値はグローバルビジネス・アクション・コード(この値のキャメルケースバージョン:単語の先頭が大文字)と一致しなければならない。</p> <p>In particular, it MUST map to (RNIF): &lt;Business Document Name&gt; + “Action”, or in case of 1-way PIP and a responding activity, specify Activity Name: &lt;Responding Business Activity&gt;.</p> <p>特に値が(RNIF)にマッピングしなければならない。  <b>&lt;Business Document Name&gt; + “Action”</b>、あるいは 1 Way PIP および応答アクティビティの場合  は、アクティビティ名:<b>&lt;Responding Business Activity&gt;</b>を指定する。</p> <p>In case of a RosettaNet signal, the value MUST be consistent with the following:  RosettaNetシグナルの場合は、値は以下と一致していなければならない</p> <p>If Signal is positive (ReceiptAcknowledgment):  :信号がポジティブ(ReceiptAcknowledgment)である場合:  Value= “ReceiptAcknowledgment”</p> <p>If Signal is negative (Exception):  信号がネガティブである場合:  Value= “Exception”  Map to ebXML BPSS 2.0 element when used:</p> <p>Examples: &lt; eb: Action&gt;PurchaseOrderRequestAction&lt;/eb: Action&gt;  &lt; eb: Action&gt;PurchaseOrderConfirmationAction&lt;/eb: Action&gt;  &lt; eb: Action&gt;SemiconductorTestDataNotification&lt;/eb: Action&gt;</p>
Alignment	<ul style="list-style-type: none"> <li>• MUST map to ebXML BPSS 1.* element when used: RequestingBusinessActivity/@nameId, RespondingBusinessActivity/@nameId</li> <li>• Map to ebXML BPSS 2.0 element when used: BinaryCollaboration//@name or BusinessCollaboration/@name, Or, more precisely, the no-space version of these values.</li> </ul>

Test References	
-----------------	--

#### 4.2.5 プロファイル要求事項 eb:Conversation Id (Profile Requirement Item eb:ConversationId)

Specification Feature	Header element: eb:MessageHeader/eb:ConversationId
Specification Reference	ebMS 2, section 3.1.3 "ConversationId Element"
Profiling	<p>It is RECOMMENDED that ConversationId represents the PIP instance ID value, i.e. has same value for all messages related to the same PIP instance.</p> <p>ConversationId が PIP インスタンス ID 値を表す (つまり、同一の PIP インスタンスに関連する全てのメッセージに対し同一の値を有する) ことが推奨される。</p> <p>In other words, messages from the same PIP instance MUST have same ConversationID, and it is recommended that this ConversationID be unique to this PIP instance (not shared with other PIP instances).</p> <p>つまり、同一PIPからのメッセージのConversationIDは同じでなければならないということであり、ConversationIDはこのPIPインスタンスに対して一意(他のPIPインスタンスと共有しない)であることが推奨される。</p>
Alignment	<ul style="list-style-type: none"> <li>MUST map to Standard Business Doc Header (SBDH) element when Applicable: RequestingDocumentInformation / BusinessProcessInstanceIdentifier</li> <li>MUST map to (in RNIF Service header) element: ServiceHeader/ProcessControl/pipInstanceId/InstanceIdentifier</li> </ul>
Test References	

#### 4.2.6 プロファイル要求事項 eb:RefToMessageId (Profile Requirement Item eb:RefToMessageId)

Specification Feature	Header element: eb:MessageHeader/eb:MessageData/eb:RefToMessageId
Specification Reference	ebMS 2, section 3.1.6.3 "RefToMessageId Element"
Profiling	<p>As a reminder, it MUST be used only for:</p> <ol style="list-style-type: none"> <li>(1) relating business signals messages to action messages, by referencing the ebMS ID.</li> <li>(2) Relating a business response to a business request.</li> </ol> <p>確認として、ConversationID は以下の目的のみに使用されなければならない。</p> <ol style="list-style-type: none"> <li>(1) ebMS ID を参照して、ビジネス信号メッセージをアクション・メッセージに関連づける。</li> <li>(2) ビジネス応答をビジネス要求に関連づける。</li> </ol> <p>Every message involved in a PIP instance MUST refer to another previous</p>

	<p>message of this instance (except for the initial message of the instance, which MUST NOT have a RefToMessageId element.)</p> <p>PIPインスタンスに含まれる全てのメッセージ(RefToMessageId要素を有してはならないインスタンスの最初のメッセージを除く)は、このインスタンスの前のメッセージを参照しなければならない。</p> <p>If several PIP instances must be correlated, this MUST NOT be achieved by this value (the first message of a PIP instance MUST NOT refer to another PIP).</p> <p>複数のPIPインスタンスを関連づけなければならない場合は、この値でそれを達成してはならない(PIPインスタンスの最初のメッセージは別のPIPを参照してはならない)。</p>
Alignment	<p>MUST map to RNIF Service header element, in the sense it plays a similar role: 同様の役割を担うという意味で、RNIFサービス・ヘッダー要素にマッピングしなければならない: ServiceHeader/ProcessControl/ActivityControl/MessageControl/inReplyTo/messageTrackingID</p>
Test References	

#### 4.2.7 プロファイル要求事項 eb:MessageId (Profile Requirement Item eb:MessageId)

Specification Feature	Header element: eb:MessageHeader/eb:MessageData/eb:MessageId
Specification Reference	ebMS 2, section 3.1.6.1 "MessageId Element"
Profiling	<p>Used for uniquely (globally) identifying a message (either signal or action). Normally, this identifier is automatically generated by an MSH, and out of control from applications. (However, an MSH provides visibility to applications on this value, so that an application can use it for referencing (see eb:RefToMessageId).</p> <p>メッセージ(信号またはアクション)を一意(グローバルで)に識別するために使用する。通常、この識別子は自動的にMSHによって生成され、アプリケーションからは制御できない。(しかし、MSHはアプリケーションに対しこの値を見えるようにするので、アプリケーションが参照に使用できるようになる(eb:RefToMessageIdを参照)。</p>
Alignment	MUST map to RNIF Delivery header, in the sense it plays a similar role: DeliveryHeader/messageTrackingID.InstanceIdentifier.
Test References	

#### 4.2.8 プロファイル要求事項 eb:CPAId (Profile Requirement Item eb:CPAId)

Specification Feature	Header element: eb:MessageHeader/eb:CPAId
-----------------------	--

Specification Reference	ebMS 2, section 3.1.2 “CPAId Element”
Profiling	See Section “CPA Profiling” in Appendix A, for recommended profiling.
Alignment	
Test References	

#### 4.2.9 プロファイル要求事項 eb:Manifest (Profile Requirement Item eb:Manifest)

Specification Feature	Header element: SOAP:Body/eb:Manifest/eb:Reference SOAP:Body/eb:Manifest/eb:Reference/eb:Schema
Specification Reference	ebMS 2, section 3.2 “Manifest Element”
Profiling	<p>The eb:Reference child element MUST comply with the following (i.e. the following attributes and child elements MUST be used):</p> <p>eb:Reference 子要素は、以下に準拠しなくてはならない(つまり、以下の属性ならびに子要素が使用されなければならない):</p> <p>Attribute xlink:type=“simple”.</p> <p>Attribute xlink:href: MUST contain a content id (URI scheme: “cid”) and not a URI that cannot be resolved locally. Example: xlink:href=cid:payload-1</p> <p>Element eb:Schema: This element SHOULD be present when the eb:Reference element is referring to the service content part (main XML document) of a PIP payload, or is referring to an XML RosettaNet signal.</p> <p>eb:Schema: この要素は、eb:Reference 要素が、PIP 本文のサービスコンテンツ部分(メインのXML 文書)、又は XML RosettaNet 信号を参照する際に存在すべきである。</p> <p>When present it MUST use an URN identifying the schema or DTD that applies to the part. The schema URN identifier MUST comply with <b>[RNNameSpaces]</b>.</p> <p>存在する場合、その部分に適用されるスキーマまたは DTD を識別する URN を使用しなければならない。スキーマ URN 識別子は[RNNameSpace]に準拠しなければならない。</p> <p>Example for a PIP service content with XML schema: urn:rosettanet:specification:interchange:PIP3A4PurchaseOrderRequest:xsdschema:1.0</p> <p>When a legacy RNIF header (such as Service header) is included in the message, it must be added as a single attachment. The eb:Reference element SHOULD contain an eb:Schema element to identify it, which conforms to <b>[RN-NameSpaces]</b>.</p> <p>レガシーなRNIFヘッダ(サービス・ヘッダなど)がメッセージに含まれている場合、単独の添付として追加しなければならない。eb:Reference要素にはそれを識別するeb:Schema 要素を持つべ</p>

	<p>きであり、それは[RN-NameSpaces]に準拠する。</p> <p>Example for a Service header: urn:rosettanet:specification:system:ServiceHeader:dtd:schema:2.0 NOTE: The use of an XLINK processor should not be required.</p>
Alignment	
Test References	

## 5 メッセージ処理 (Message Processing)

### 5.1 パッケージング (Packaging)

The packaging of the message headers and payloads, including security headers, follows the ebMS 2.0 specification. It is automatically implemented by conforming ebMS MSH implementations.

セキュリティ・ヘッダを含むメッセージ・ヘッダー及びペイロードのパッケージングは、ebMS 2.0 仕様に準拠する。それは、ebMS MSH 実装に準拠して、自動的に実行される。

### 5.2 アンパッケージング (Un-packaging)

The un-packaging of the message headers and payloads, including security headers, follows the ebMS 2.0 specification. It is automatically implemented by conforming ebMS MSH implementations.

セキュリティ・ヘッダを含むメッセージ・ヘッダー及びペイロードのアンパッケージングは、ebMS 2.0 仕様に準拠する。それは、ebMS MSH 実装に準拠して、自動的に実行される。

## 6 メッセージ交換パターン(MEP)と表示(Message Exchange Patterns and Representation)

This section only describes the lowest level of MEPs involving only one action message, and some RosettaNet signal message(s). Higher level choreographies, such as those involving more than one action message (including two-action PIPs), are out of scope of this message profiling.

この章では、1 アクション・メッセージのみを含む最下層の MEP、及び一部の RosettaNet 信号メッセージについてのみ記述する。複数のアクション・メッセージ(2 アクション PIP を含む)を含む MEP といったより上位層のコレオグラフィはこのメッセージ・プロファイリングの範囲外である。

In the following, a clear distinction must be made between ebMS signal messages and RosettaNet signal messages.

下記では、ebMS 信号メッセージと RosettaNet 信号メッセージとの明確な区別を行わなければならない。

- An ebMS signal message has no significance or visibility to the user layer: it is an error message or a reliability acknowledgement that is for the exclusive usage of the ebMS protocol. It would not be visible in any message choreography that RosettaNet defines. ebMS信号メッセージは、ユーザー層に対し意味や可視性を持たない:それはebMSプロトコル専用のエラーメッセージまたは信頼性確認である。それはRosettaNetが定義するメッセージ・コレオグラフィでは一切可視できない。
- A RosettaNet signal message (receipt, exception) is, from an ebMS perspective, like any other application level message. ebMS does not handle these any differently from action messages. The signal content is considered as any other application payload. RosettaNet 信号メッセージ(受信、エラー)は、ebMS の視点からは、その他のアプリケーション・レベルのメッセージのようである。EbMS ではこれらをアクション・メッセージと区別して扱わない。信号コンテンツはその他のアプリケーション・ペイロードと見なされる。

Note: It is however possible to piggyback ebMS acknowledgements or errors on application messages, merging into one message what could have been considered as two separate messages (an ebMS signal and an application message.)

注:しかし、ebMS 受信確認またはエラーをアプリケーションに便乗させ、2 つの別々のメッセージ(ebMS 信号とアプリケーション・メッセージ)と見なされるであろう1つのメッセージにまとめることが可能である。

### 6.1 ebMS2.0 におけるメッセージ交換パターン(MEP) (MEPs in ebMS 2.0)

Two basic MEPs are supported in ebMS 2.0.: 基本的な2つのMEPがebMS 2.0 でサポートされる。:

- **One-way Push MEP:** Supports the sending of one message (PIP signal or action) as ebMS message, initiated by the sender. A single ebMS message is exchanged in this MEP. In case a request-response protocol such as HTTP is used, no application-significant ebMS message is returned over the response leg of the MEP. In this mode of messaging, every message of a PIP instance would be sent over a separate instance of the One-way Push MEP. This is the default mode of operating in ebMS 2.0. **syncReplyMode** in the CPA must be either absent, or set to *mshSignalsOnly*. In the latter case, only ebMS signals can be sent back as response

(not RosettaNet signals.) In the context of this profiling specification, this MEP can be used for sending:

**1 方向プッシュ型 MEP:**送信者が開始した 1 つのメッセージ(PIP 信号またはアクション)の送信を ebMS メッセージとしてサポートする。この MEP では単体の ebMS メッセージが交換される。HTTP のような要求-応答プロトコルが使用される場合は、MEP の応答肢によってアプリケーション的に意味のある ebMS メッセージは返されない。このメッセージ・モードでは、PIP インスタンスの全てのメッセージが 1 方向プッシュ MEP の独立なインスタンスを介して送信される。これは ebMS 2.0 で作動する初期設定モードである。CPA の同期返答モード(SyncReplyMode)は使わない、あるいは msh 信号のみ(mshSignalsOnly)に設定されていなければならない。後者の場合では、ebMS 信号のみが応答として送り返される(RosettaNet 信号ではない)。このプロファイリング仕様の文脈では、この MEP を使用して以下のものを送信できる。

- o A RosettaNet Action message (with possibly an ebMS signal on the response leg)  
RosettaNetアクション・メッセージ(場合によると、応答肢のebMS信号と共に)
- o A RosettaNet Signal message (with possibly an ebMS signal on the response leg)  
RosettaNetシグナル・メッセージ(場合によると、応答肢のebMS信号と共に)
- Request-response MEP: Supports the sending of one message (PIP signal or action) as ebMS message, initiated by the sender, and the sending of an application-level response message as an ebMS message. Two ebMS messages are exchanged in this MEP, over the same request-response of the underlying protocol. This requires a request-response underlying protocol.  
**要求-応答 MEP:**送信者が開始した 1 つのメッセージ(PIP シグナルまたはアクション)を ebMS メッセージとして送信すること、ならびにアプリケーション・レベルの応答メッセージを ebMS メッセージとして送信することをサポートをする。2 つの ebMS メッセージが、下層プロトコルの同一の要求-応答を介して交換される。これには要求-応答下層プロトコルが求められる。
- *syncReplyMode* in the CPA must set to *signalsAndResponse* or *responseOnly*. This requires the first ebMS message to use syncReply mode. In the context of this profiling specification, this MEP can be used for sending:  
CPA の同期返答モード(syncReplyMode)は、信号と応答(signalsAndResponse)または返答のみ(responseOnly)に設定しなければならない。これには、同期返答(syncReply)モードを使用するために、最初の ebMS メッセージが求められる。このプロファイリング仕様の文脈では、この MEP を使用して以下のものを送信できる。
- o A RosettaNet Action message (request) followed by a RosettaNet Signal message (response).  
RosettaNetアクション・メッセージ(要求)、続いてRosettaNet信号メッセージ(応答)。

Pulling of messages is not supported in ebMS 2.0 but will be in ebMS 3.0. Although this feature could be emulated on top of ebMS 2.0, the recommendation is here to not use it with ebMS 2.0.

メッセージの引き取り(プル)は、ebMS 2.0 ではサポートされていないが、ebMS 3.0 ではサポートされる。この機能は ebMS 2.0 上で実行できるであろうが、ここでは ebMS 2.0 と共に使用しないことを推奨する。

An ebMS MSH does not require more configuration information other than what is the type of MEP a message being sent is participating in. This is concretized by the SyncReplyMode value, defined in the CPA associated with that PIP, for a particular trading partner. Any choreography at a level higher than those described above, is out of scope of ebMS messaging and will need to be controlled by a layer above messaging. However, in any case, some message correlation is

apparent in the ebMS message header: ConversationID and RefToMessageId must follow the profiling recommendations in Section 4.2.

ebMS MSH は、送信中のメッセージの MEP タイプは何であるかという以外の構成情報は要求しない。これは、特定の取引先のために、その PIP に関連する CPA において定義された同期返答モード (SyncReplyMode) 値によって具体化される。上記のものよりも高いレベルのコレオグラフィは ebMS メッセージの範囲外であり、メッセージ層よりも上位の層で制御する必要がある。しかし、どんな場合でも、ebMS メッセージ・ヘッダに幾つかのメッセージ相関が表れる場合がある：ConversationID と RefToMessageId は、4.2 項のプロファイリング推奨に準拠しなくてはならない。

## 6.2 受信処理 (Handling of Receipts)

We consider here the basic message sequence of sending an Action message, and getting back a Receipt Acknowledgement or an Exception. As ebMS 2 provides a reliable messaging feature, it appears that there is significant overlap of purpose with the Receipt Acknowledgement signal in RN:

我々はここで、アクション・メッセージの送信ならびに受信確認またはエラーの返信の基本的なメッセージ順序について考える。ebMS 2 は高信頼な送受信機能を提供するため、RN の受信確認信号と目的が同じ部分が多いように思われる。

- A retry mechanism is specified in RN, triggered by not receiving a Receipt Acknowledgement in time. It is controlled with a RetryCount parameter, and Time to Acknowledge.  
再試行メカニズムはRNにおいて指定され、時間内に受信確認を受け取らないことにより起動する。それは再試行回数ならびに受信確認までの時間で制御される。
- ebMS 2.0 has a similar mechanism of retries, until an acknowledgement is received. A maximum number of retries, as well as, a retry interval, are specified.  
確認が受信されるまで、ebMS 2.0 は同様の再試行メカニズムを有する。再試行の最大回数ならびに再試行の間隔は指定される。

The RN Retry mechanism can be largely supported by ebMS 2.0 reliability, except for two aspects: RN再試行メカニズムは下記の2つの側面を除き、大方はebMS 2.0信頼性によってサポートすることができる。

- the meaning of a Receipt Acknowledgement usually goes beyond message reception, to include document validation (grammar level). The ebMS acknowledgement does not have this semantics.  
受信確認とは通常、メッセージの受信を超え、ドキュメントバリデーション(文法レベル)を含む。ebMS の受信確認にはこの意味はない。
- Receipt Acknowledgements are meaningful for non-repudiation of receipt. The signed-ack in ebMS is not a substitute. It does not include a digest of the original message.  
受信確認は受信拒否防止にとって重要である。ebMS の署名された ack は代替にならない。それは、原文のダイジェストを含んでいない。

The recommended profiling is as follows: 推奨プロファイリングは以下の通りである。

When nonrepudiation Of receipt is not required	Do NOT use the Receipt Acknowledgement (positive) signals. Instead, use the reliable messaging feature. The mapping of the respective parameters of these features has been described in Appendix A 受信確認(ポジティブ)信号は使用しない。代わりに、高信頼性メッセージング機能を使用する。これらの機能の各パラメータのマッピングを付録 A に記述。
--	--

<p>受信拒否防止が要求されない場合</p>	<p><b>In case of invalid payload:</b> only then would an exception message (type: Receipt Acknowledgement Exception) be sent back, as the result of a validation check occurring at higher level than the messaging layer. The absence of such a signal tells the sender that the payload was valid. Note: a 0A1 PIP could be used too.</p> <p><b>無効なペイロードの場合:</b>その時のみ、メッセージ層よりも高レベルで生じるバリデーションチェックの結果として、エラーメッセージ (type: Receipt Acknowledgement Exception) が送り返される。</p> <p>そのような信号が無い場合には、送信者にペイロードが有効であったことを伝えている。 注: PIP0A1も使えるであろう。</p>
<p>When nonrepudiation of receipt is required</p> <p>受信拒否防止が要求された場合</p>	<p>Often there are several steps in a non-repudiation mechanism (or layers). Validation of the payload may not belong to the initial step. Also, it appears that different users give different meaning to non-repudiation, e.g. regarding the degree of payload validation. For these reasons, two options are available to users, depending on the precise semantics of non-repudiation that is required.</p> <p>拒否防止メカニズム(または層)には、複数のステップがあることが多い。ペイロードのバリデーションは最初のステップに属さない可能性がある。又、ユーザーが異なると拒否防止の意味も異なるように思われる(例:ペイロードバリデーションの深さ)。これらの理由により、要求される拒否防止の明確な意味によって、ユーザーは2つのオプションが利用可能である。</p> <p><b>Option 1:</b> No hash (digest) is required in the receipt, and no payload validation is required. This is just a certification that the ebMS message has been well received. In such case, the ebMS2.0 signed acknowledgement feature should be used. Only a reference to the MessageId of the acknowledged message is included in the Acknowledgement message. The <i>ackSignatureRequested</i> element of the CPA must be set.</p> <p><b>Option 1:</b> ハッシュ(ダイジェスト)は受信において必要ではない。又、ペイロードバリデーションも必要でない。これは単にebMSメッセージが問題なく受信されたという証明である。そのような場合、ebMS 2.0署名済み確認機能を使用すべきである。確認済みメッセージのMessageIdへの参照のみが確認メッセージに含まれる。CPAのack SignatureRequested要素が設定されなければならない。</p> <p><b>Option 2:</b> A hash (digest) is required in the receipt. This option may also assume payload validation. In that case, an RN Receipt Acknowledgement with digest will be sent back. From an ebMS messaging viewpoint, this is a business message to be handled in the same way as any other action message.</p> <p><b>Option 2:</b> ハッシュ(ダイジェスト)は受信で必要である。このオプションは本文のバリデーションが必要でしょう。その場合、ダイジェストを持ったRN受信確認が送り返される。ebMSメッセージの観点から言えば、これは他のアクション・メッセージと同じ方法で処理されるビジネス・メッセージである。</p>

## 7 QoS に関する TPA 機能と展開構成 (TPA Features Specific to QoS and Deployment Configurations)

### 7.1 セキュリティ (Security)

Security will follow the ebMS 2.0 specification requirements.

セキュリティは ebMS 2.0 仕様要件に準拠する。

- Signature of the ebMS header as well as ebXML payload(s) is supported by XMLDSIG. ebMS ヘッダならびに ebXML ペイロードの署名は XMLDSIG によってサポートされる。
- Confidentiality of the ebXML Headers is supported by S/MIME (XML Encryption was not finalized at the time ebMS2 has been released). ebXML ヘッダーの機密性は S/MIME によってサポートされる。(XML 暗号化は ebMS2 が公開された時には未だ完成していなかった。)
- Confidentiality of the ebXML payloads (SOAP attachments) can be supported by S/MIME, or another method (XML Encryption may be used). This has to be specified in the TPA (and CPA)  
ebXML ペイロード(SOAP 添付)の機密性は、S/MIME あるいは別の方法(XML 暗号化を使用してもよい)によってサポートすることができる。これは TPA(および CPA)で指定されなければならない。

### 7.2 信頼性 (Reliability)

Using the Reliable messaging feature (Guaranteed Delivery and Duplicate Elimination) is recommended. In particular, Guaranteed Delivery will provide the following features:

信頼性メッセージング機能(配信の保証及び重複の除去)の使用が推奨される。特に、配信の保証は以下の機能を提供する。:

- A notice of failure to the sender in case of non-delivery.  
配信できなかった場合の送信者への失敗の通知。
- A first level of Acknowledgement (not visible outside the MSH, used to control a message resending mechanism).  
確認の一次レベル(メッセージ再送信メカニズムの制御に使用されるMSHの外部では可視不可能)
- A message resending mechanism, controlled by parameters specified in the CPA (some of them mapping to PIP definition parameters)  
CPA において指定されるパラメータ(それらのうちのいくつかは PIP 定義パラメータにマッピングする)によって制御されるメッセージ再送信メカニズム)
- Optionally, a signed acknowledgement that can be used as a first step in non-repudiation. However, this acknowledgement does not contain a digest of the original message.  
任意として、拒否防止の最初のステップとして使用できる署名済み確認。しかし、この確認には元のメッセージのダイジェストは含まれていない。

### 7.3 時折接続パートナー (Occasionally Connected Partners)

In ebMS 2.0, a party has no other way to figure that a partner's MSH is down other than by getting repeated delivery failure notices, when trying to send messages to this partner. Dealing with occasionally connected partners may be done in two ways, that both involve a particular behavior from the layer above messaging:

ebMS 2.0 では、パートナーへのメッセージの送信を試みる際に、配信失敗通知を繰り返し取得する以外に、このパートナーの MSH がダウンしていることを推測する方法はない。時折接続しているパートナーとのやり取りは 2 つの方法でおこなうことができる。双方にはメッセージ層よりも上位の層からの特定の動作が含まれる。:

(a) In case the periods of non-connectivity are known, both partners should share such information using a TPA structure above. A sender would then avoid sending messages to the non-connected party while it is down.

非接続の期間が分かっている場合、両方のパートナーが上記のTPA構造を使用して、そうした情報を共有すべきである。その後、ダウン中は送信者から接続していないパーティーへのメッセージの送信を避ける。

(b) In case messages are still sent to a non-connected partner, the reliable messaging feature may trigger useless message resending, but in all cases will notify of delivery failures on sender side. A series of failure delivery notices should be interpreted by the application layer as a sign that efforts to send messages to this party should stop, until the connectivity can be verified in other ways.

接続していないパートナーへのメッセージの送信がまだおこなわれている場合は、信頼性メッセージング機能が、無駄なメッセージの再送信を誘因する可能性があるが、全ての場合において、送信者側に配信の失敗を通知する。一連の配信失敗通知は、アプリケーション層によって、他の方法で接続性が検証されるまで、このパーティーへのメッセージの送信の試みを停止するというサインと解釈されるべきである。

### 7.4 ルーティングとマルチホップ (Routing and Multi-Hop)

We consider here a two-hop scenario, via a Hub connection. The basic invariant of multi-hop, is that the ebMS message is not altered along the routing path. This is different from a routing mode where the Hub is treated as a final destination, and forwards the message payload based within a new ebMS envelope, e.g. with a new eb:To/PartyId, possibly with different QoS requirements. This mode is certainly possible but out of scope for this profiling specification.

ここでは、ハブ接続を介した2ホップシナリオと考える。マルチホップの基本的な不変条件は、ebMSメッセージがルーティング経路によって変わらないということである。これは、ハブが最終宛先として処理され、新しいebMS封筒(例えば新規eb:To/PartyId)に場合によっては異なるQoS要件を付けてメッセージ本文が転送されるというルーティングモードとは異なる。このモードは確かに可能であるが、このプロファイリング仕様の範囲外である。

We assume here that the final destination is already mentioned in the original message (eb:To / PartyID). We can roughly classify the different ways to achieve multi-hop routing as follows:

ここでは、最終宛先は既に元のメッセージ(eb:To / PartyID)で言及していると見なす。以下の様にマルチホップ・ルーティングを達成する異なる方法を大きく分類できる。:

1. Transport-level routing: The Hub is not acting as an ebXML MSH, and not even as a SOAP intermediary. It uses a routing mechanism that is independent from the ebMS header content. In that case the routing is transparent to the ebXML function. Such mechanism could be based on URL attributes.

1. トランスポートレベル・ルーティング: ハブはebXML MSHとしても、またSOAP仲介者としても機能しない。それは、ebMSヘッダコンテンツから独立したルーティング・メカニズムを使用する。その場合、ルーティングはebXML機能と同じと見ることができる。そのようなメカニズムはURL属性に基づいている可能性がある。

2. The Hub is acting as a SOAP intermediary. In that case also the routing is transparent to the ebXML function. Such mechanism could be based on some extra SOAP Header block (other than ebMS blocks), such as WS-Addressing header *wsa:To*. In such a case, SOAP faults may be generated.

2. ハブはSOAP仲介者として機能している。その場合も、ルーティングをebXML機能と同じと見ることができる。そのようなメカニズムは、WS-Addressingヘッダ (*wsa:To*) などのいくつかの追加のSOAPヘッダブロック (ebMSブロック以外) に基づく可能性がある。そのような場合、SOAP障害が生成されるであろう。

3. The Hub is acting as an ebXML MSH – i.e. it has a routing mechanism that is dependent on the ebMS header content. Typically, the *To/PartyId* header element would be used to determine the routing. The Hub will act in the “NextMSH” role, while the final MSH destination will act in both the “ToPartyMSH” and “NextMSH” roles. The Hub may then consume the *MessageHeader/To* header element (that must not be set to *ToPartyMSH* actor, in that case). In case the routing function requires other data, it MAY use data in the message body provided that this data does not conflict with ebMS header data.

3. ハブはebXML MSHとして機能している。つまり、ebMSヘッダコンテンツに依存するルーティング・メカニズムを有しているということである。一般的に、*To/PartyId*ヘッダ要素を使用して、ルーティングを決定する。ハブは“NextMSH”役割で機能し、一方、MSH最終宛先は“ToPartyMSH”と“NextMSH”役割の両方で機能する。その後、ハブは*MessageHeader/To* header要素 (その場合、*ToPartyMSH*アクターに設定してはいけない) を使うであろう。ルーティング機能が他のデータを要求する場合、データがebMSヘッダ・データと矛盾しなければ、メッセージ本文中のデータを使用してもよい。

- a. Regarding the reliability feature: no acknowledgement from the Hub (no intermediary Acks) should be expected. This profile requires that the actor attribute of the *AckRequested* element be set to *ToPartyMSH*.

信頼性機能に関して: ハブ(中間Ackはない)からの確認は予期されない。このプロファイルは、*AckRequested*要素のアクター属性が*ToPartyMSH*に設定されることを必要とする。

- b. Regarding Security: header elements used for routing must not be encrypted. The Hub is not supposed to have security capabilities.

セキュリティに関して: ルーティングに使用したヘッダ要素を、暗号化してはいけない。ハブは、セキュリティ能力を有するものではない。

## 8 その他 (MISCELLANEOUS)

なし

## 9 付録 A:CPA プロファイリングと例題 (Appendix A: CPA Profiling and Sample)

### 9.1 CPA プロファイリング形式 (CPA Profiling Forms)

The profiling and definition of CPA data (both instance and profile template) can be facilitated using a set of forms, such as those provided by the ebXML Implementation, Interoperability and Conformance (IIC) OASIS Committee. It is strongly recommended for business partners to use the "Deployment Profile Template for CPPA V2.0" published by the OASIS IIC, in order to finalize their collaboration agreements. A subset of these forms is presented here.

CPAデータ(インスタンスとプロファイル・テンプレートの両方)のプロファイリング及び定義は、ebXML実装、相互運用性、および準拠性(IIC)OASIS技術委員会によって提供されるフォームなどの一組のフォームにより促進することができる。ビジネスパートナーが、提携契約を結ぶために、OASIS IICによって発行された「CPPA V2.0のデプロイメント・プロファイル・テンプレート」を使用することを強く推奨する。これらのフォームのサブセットをここで提示する。

Each element (or entry) in each one of these forms maps to a CPA element. Either the name of the entry is explicit enough to refer to the corresponding CPA element, or the name of the corresponding CPA element is mentioned in clear, usually prefixed with the qualifier "tp:" (e.g. tp:channelID).

これらのそれぞれのフォームにおける各要素(又は、エントリー)がCPA要素にマッピングする。エントリー名が対応するCPA要素を参照するのに十分明示的であっても、または対応するCPA要素名が明確に言及されていても、通常は修飾子「tp:」(例えばtp:channelID)が接頭辞として付けられる。

- When entries in these forms must map to some PIP definition elements, it is indicated in the form entry.  
これらのフォームにおけるエントリーが一部のPIP定義要素にマッピングしなければならない場合、フォームエントリーで示される。
- When entries in these forms are left to the user to instantiate as s/he wants to, the entry value is left empty (or just referring to the actual name of the CPA element, e.g. tp:TransportID)  
これらのフォームにおけるエントリーがユーザーに任せられ、ユーザーが望むように例示する場合は、エントリー値は空のまま(またはCPA要素の実際の名前、例えばtp:TransportIDを参照するのみ)となる。

A sample CPA document is listed in the next sub-section.  
サンプルCPA文書は次の補助項にリストされている。

NOTE: These forms and their content are based on CPPA V2.1, which is very close to V2.0 (includes an errata from V2.0 and has additional extensibility points – some element names may be different. Please refer to the Errata for V2.0.)

注記:これらのフォームとそのコンテンツは、V2.0に非常に類似しているCPPA V2.1(V2.0からのバグを含み、追加拡張ポイントを有する。要素名の中には異なるものもある。V2.0の正誤表を参照されたい。)に基づいている。

## 9.2 CPA 関連書類名と参照のプロファイリング (Profiling the CPA Artifact Names and References)

This form is used to identify the CPA profile, and also any CPA instance that is derived from a profile. It recommends some naming conventions for the CPA artifacts.

このフォームは、CPAプロファイルならびにプロファイルに由来する全てのCPAインスタンスを識別するために使用される。それは、CPA関連書類アーティファクトのいくつかの命名規則を推奨する。

CPA Profile Info		
CPA Profile Info	Name	<p>[Provide a name for the Collaboration Protocol Agreement profile. The name should identify when applicable: (a) the version of CPA, (b) the community sharing this profile (here, RN), (c) type of artifact (here a profile), (d) name of profile, (e) party ID if this profile is attached to a party.]</p> <p>[コラボレーション・プロトコル合意書(CPA)プロファイルの名前付けをおこなう。適用する場合、この名前により以下を識別するものとする。:(a)CPAのバージョン、(b)このプロファイルを共有するコミュニティ(ここではRN)、(c)書類のタイプ(ここではプロファイル)、(d)プロファイル名、(e)もしこのプロファイルが当事者に添付される場合には、パーティーID。]</p> <p>Recommended:            "CPA2.0-RN-Profile-"&lt;profileID&gt;"- "&lt;partner1&gt;"</p> <p>Examples:            CPA2.0-RN-Profile-PIP3A4-222222            CPA2.0-RN-Profile-TP31-222222</p>
	File name	<p>[Provide a file name for the Collaboration Protocol Agreement profile file.]</p> <p>[コラボレーション・プロトコル合意書プロファイル書類に書類名を付ける。]</p> <p>"CPA2.0-RN-Profile-"&lt;profileID&gt;"- "&lt;partner1&gt;"-file"            (followed by appropriate suffix – e.g. .xml for the XML definition.)</p> <p>Examples:            CPA2.0-RN-Profile-PIP3A4-222222-file.pdf            CPA2.0-RN-Profile-TP31-222222-file.xml</p>
CPA Instance Info	Name	<p>[Define the name format for the CPA instances resulting from using this profile. The name should identify when applicable: (a) the version of CPA, (b) the community sharing this profile, (c) name of profile, (d) ID of instance, (e) party IDs.]</p> <p>[このプロファイルの使用に起因するCPAインスタンスの名前フォーマットを定義する。適用する場合、この名前により以下を識別するものとする。(a)CPAのバージョン (b)このプロファイルを共有するコミュニティ (c)プロファイル名 (d)インスタンスのID (e) パーティーID。]</p>

	<p>Recommended:  “CPA2.0-RN-“&lt;profileID&gt;”-“&lt;instID&gt;”-“&lt;partner1-partner2&gt;  Example:  CPA2.0-RN -P15-001-222222-333333  CPA2.0-RN -TP2-004-222222-333333</p>
<b>File name</b>	<p>[Define the file name format for a Collaboration Protocol Agreement instance.]  [コラボレーション・プロトコル合意書インスタンスの書類名フォーマットを定義する。]</p> <p>Recommended:  “CPA2.0-RN-“&lt; profileID &gt;”-“&lt;instID&gt;”-“&lt;partner1-partner2&gt;”- file”  (followed by appropriate suffix – e.g. .xml for the XML definition.)  Example:  CPA2.0-RN-P15-001-222222-333333-file.pdf  CPA2.0-RN-TP2-004-222222-333333-file.xml</p>
<b>CPA Id</b>	<p>[Define the format of the CPA Id. Must align with CPAId in message header.]  [CPA Idのフォーマットを定義する。メッセージ・ヘッダのCPAIdと連携すること]</p> <p>Recommended: same as CPA name, i.e.:  “CPA2.0-RN-“&lt; profileID &gt;”-“&lt;instID&gt;”-“&lt;partner1-partner2&gt;</p>
<b>Lifetime of CPA</b>	<b>Start:</b> [The starting date and time of the agreement.]
	<b>End:</b> [The end date and time of the agreement. The start and end date/times define the duration that the agreement is in effect.]
<b>Context of application</b>	<p><b>ConversationLimit:</b> [NONE or numeric value. The agreement is terminated (no longer valid) when the conversation limit is reached.]  <b>会話限界:</b> [NONEまたは数値。会話限界に到達すると、この合意は終了する(有効ではなくなる)。]</p>
	<p><b>Concurrent Conversation Limit:</b> [NONE or numeric value. The maximum number of conversations that can be in process at the same time. Provide this value when there are constraints that limit the number of business transactions that one or more of the parties can process simultaneously.]  <b>同時会話限界:</b> [NONEまたは数値。同時に処理できる会話の最大数。1名または複数名のパーティーが同時に処理できるビジネス取引数を制限する制約がある場合は、この値を提供する。]</p>

### 9.3 当事者情報のプロファイリング (Profiling the Party Info)

This form is used to identify the parties involve. A CPA profile will typically contain one of these fully instantiated. At least another one of these will need to be filled by another business partner in order to produce a complete CPA instance.

このフォームは、関連当事者の識別に使用される。CPAプロフィールは通常、十分に例示された当事者情報の1つを持つ。完全なCPAインスタンスを生成するために、少なくとも当事者情報のもう1つが相手方ビジネスパートナーによって作成される必要がある。

Profiling (alignment with data or QoS in Rosettanet PIPs, or with ebMS header data that is itself profiled) is required for some entries of this table The rest of this table is provided as a support for users.

プロファイリング (Rosettanet PIPにおけるデータまたはQoSとの合わせ、あるいはそれ自体がプロファイルされた ebMSヘッダ・データとの合わせ) はこのテーブルの一部のエントリーに要求される。このテーブルの残りはユーザーのサポートとして提供される。

Party Info	
<b>CPA Reference</b>	[CPA Profile name]
	[CPA Instance name, if used for instantiating a particular CPA] [もし特定のCPAを例示するために使用されるならば、CPAインスタンス名。]
<b>Party element</b>	<b>PartyId</b> [The formal unique identifier for the organization. Must align with eb:PartyId in message header (section 4).All Party ID elements present in CPA must appear in the message header. [組織のための正式な一意の識別子。メッセージ・ヘッダのeb:PartyIdと合わせなければならない。(4項)]CPAに存在する全ての当事者ID要素はメッセージ・ヘッダに表示されなければならない。
	<b>Type</b> [Must align with eb:PartyId/@type in message header (section 4)] [メッセージ・ヘッダのeb:PartyId/@typeと合わせなければならない(4項)。]
	<b>Reference</b> [A URL or URI that points to a location (e.g. web page or directory) where more information can be found on the party.] [当事者のより多くの情報が見つかる場所(ウェブ・ページまたはディレクトリなど)を指すURLあるいはURI。]
<b>Collaboration Roles elements</b>	[List the collaboration role names that this party is expected to fulfill. The role names need to be unique within this list. Each role will be detailed in a CollaborationRole form.] [この当事者が実行することが求められるコラボレーション役割名をリストする。役割名はこのリスト内で一意である必要がある。各役割はCollaborationRoleフォームで詳述される。]
	<b>CollaborationRole 1</b> Process Name [maps to eb:Service I header]      Role Name [maps to eb:Role in header]
	<b>CollaborationRole 2</b> Process Name [maps to eb:Service I header]      Role Name [maps to eb:Role in header]
	<b>(others?)</b>

<b>Certificates elements</b>	[List the certificates info and ID.]	
	<b>Certificate 1</b>	
	<b>Certificate 2</b>	
	<b>(others?)</b>	
DeliveryChannels elements	[describes a <i>Party's Message</i> -receiving and <i>Message</i> -sending characteristics. It consists of one document-exchange definition and one transport definition. The details of each DeliveryChannel element will be specified in a different form.] [当事者のメッセージ(受信ならびにメッセージ送信特性)を記述する。それは、1つの文書交換定義ならびに1つのトランスポート定義から成る。各DeliveryChannel要素の詳細は、別のフォームで指定する。]	
	<b>DeliveryChannel 1</b>	[give only the tp:channelId]
	<b>DeliveryChannel 2</b>	[give only the tp:channelId]
	<b>(others?)</b>	
Transports elements		
	Transport ID	[tp:TransportId]
Documents Exchanges		
	Exchange ID	[tp:docExchangeId]

#### 9.4 コラボレーションの際の役割のプロファイリング (Profiling the Collaboration Roles)

This form is used to identify the roles in which a party may be acting under this CPA or CPA profile. One form will be filled for each role.

このフォームは、当事者がこのCPAまたはCPAプロファイル下で作用する可能性がある役割を識別するために使用される。各役割につき1枚のフォームに記入する。

Profiling (alignment with data or QoS in Rosettanet PIPs) is required for some entries of this table. The rest of this table is provided as a support for users.

プロファイリング(Rosettanet PIPのデータまたはQoSとの合わせ)はこの表の一部の記載に要求される。この表の残りはユーザーのサポートとして提供される。

<b>CollaborationRole Info</b>	
<b>CPA Reference</b>	[CPA Profile name]
	[CPA Instance name, if used for instantiating a particular CPA ]

Role Identification	Name	[maps to eb:Role]	
	Type	[xlink:type], e.g. "simple"	
	href	[xlink:href] Example: xlink:href="http://www.rosettanet.org/processes/3A4.xml#Buyer">	
Application Certificate	ID:		
	Comments:		
Process Specification	name	[The name of the business process specification that this role applies to.] maps to ProcessSpecification nameID attribute in BPSS guideline (e.g. <b>urn:rosettanet:specification:interchange:PIP3A4:xml:bpss:d11_00</b> ), i.e. to eb:Service (see Section 4 Message Description) xlink:href : contains a reference to the BPSS definition (e.g. = <a href="http://www.rosettanet.org/processes/3A4.xml">http://www.rosettanet.org/processes/3A4.xml</a> )	
	version	[Version of the business process specification]	
	type		
	Uuid /nameid	tradingpartner uuid attribute uuid of BPSS definition when present (attr in process specification top element) (Example= "urn:icann:rosettanet.org:bpid:3A4\$2.0")	
Service Binding item (One for every Action or Signal message)	Associated Service name	[tp:ServiceBinding/tp:Service value] Maps to eb:Service (see Section 4 Message Description) Example: <tp:Service>urn:rosettanet:specification:interchange:PIP3A4:xml:bpss:d11_00</tp:Service>	
	Action direction	[send / receive ]	
	Action Binding	[tp:id] example: companyA_ABID1 (to be used for further references.Unique)	
		[tp:action] example: "Purchase Order Request Action" maps to eb:Action (see Section 4, Message Description)(e.g. ="PurchaseOrderRequestAction")	
		[tp:packageId] Example: tp:packageId="CompanyA_RequestPackage". Refers to MIME structure of payload.	
Business Transaction Characteristics	tp:isNonRepudiation Required	maps to "Non-Repudiation of Origin and Content", column 8 in PIP definition tables below. (= "true" in below example)	
	tp:isNonRepudiation ReceiptRequired	maps to "Non-Repudiation Required" column 3 in PIP tables below. (= "true" in below example)	

	tp:isConfidential	(using SSL or digital envelope)
	tp:isAuthenticated	NOTE: should map to DTD related docs
	tp:isTamperProof	(NOTE: authenticated gives integrity)
	tp:isAuthorization Required	maps to "Is Authorization Required" column 7 in PIP tables below. (= "true" in below example)
	tp:timeToAcknowledgeReceipt	maps to "Time to Acknowledge" column 4 in PIP tables below. (= "PT2H" in below example) NOTE: it should be equivalent to (retryInterval * Retries) in ebMS.
	tp:timeToPerform	maps to "Time to Perform" column 5 in PIP tables below (not really captured in CPA, about same as time to Ack)
	Tp:isIntelligibleCheck Required	
	Tp:timeToAcknowledgeReceipt	
	Tp:timeToAcknowledgeAcceptance	
	Tp: <b>retryCount</b>	Must NOT be used. Instead, the Retries element of the ReliableMessaging CPA element will map to "Retry Count" column 6 in PIP tables below.

### 9.5 配信チャネルのプロファイリング (Profiling the Delivery Channels)

**Delivery Channels** - A delivery channel describes a *Party's Message*-receiving and *Message*-sending characteristics. It consists of one document-exchange definition and one transport definition.

**配信チャネル** - 配信チャネルは、メッセージ受信ならびにメッセージ送信特性を記述する。それは、1つの文書交換定義ならびに1つのトランスポート定義から成る。

No profiling is required for this data. This table is provided as a support for users.  
このデータに関するプロファイリングは必要としない。この表は、ユーザーをサポートするためのものである。

Delivery Channel Info	
<b>CPA Reference</b>	[CPA Profile name]
<b>Identity and Components</b>	[CPA Instance name, if used for instantiating a particular CPA]
	<b>ChannelId</b>
	<b>transportId</b>

	<b>docExchangeld</b>	
<b>Messaging Characteristics</b>	<b>syncReplyMode</b>	
	<b>ackRequested</b>	Reliable Messaging parameter for Guaranteed Delivery (At Least Once)
	<b>ackSignatureRequested</b>	NOTE: this is a way to support a form of non-repudiation of Receipt, that is generally not sufficient for RosettaNet.
	<b>duplicateElimination</b>	Reliable Messaging parameter for No Duplicate Delivery (At Most Once)
	<b>actor</b>	

## 9.6 文書交換のためのプロファイリング (Profiling the Document Exchanges)

**Document Exchange** - The Document-exchange layer specifies processing of the business documents by the Message-exchange function. Properties specified include encryption, digital signature, and reliable-messaging characteristics. The options selected for the Document-exchange layer are complementary to those selected for the transport layer. For example, if Message security is desired and the selected transport protocol does not provide *Message* encryption, then *Message* encryption must be specified in the Document-exchange layer.

**文書交換**- 文書交換層は、メッセージ交換機能によってビジネス文書の処理を指定する。指定された特性には、暗号化、デジタル署名、及び信頼性メッセージング特性が含まれる。文書交換層に選ばれたオプションは、トランスポート層に選ばれたものと補完的である。例えば、メッセージセキュリティが望まれ、選択されたトランスポート・プロトコルがメッセージ暗号化を提供しない場合、メッセージの暗号化は文書交換層で指定されなければならない。

Profiling (alignment with data or QoS in Rosettanet PIPs) is required for some entries of this table. The rest of this table is provided as a support for users.

プロファイリング(Rosettanet PIPのデータまたはQoSとの合わせ)はこの表の一部の記載に要求される。この表の残りはユーザーのサポートとして提供される。

<b>Document Exchange Info</b>		
<b>CPA Reference</b>		[CPA Template name]
		[CPA Instance name, if used for instantiating a particular CPA]
<b>Doc Exchange ID</b>		[tp:docExchangeld]
<b>Sender Binding</b>	<b>Reliable</b>	[tp:ReliableMessaging]
	<b>Messaging</b>	- tp:Retries: [maps to "Retry Count" column 6 in above tables.] - tp:RetryInterval: [Example:

		<p>&lt;tp:RetryInterval&gt;PT2H&lt;/tp:RetryInterval&gt;]</p> <ul style="list-style-type: none"> <li>- tp:MessageOrderSemantics: [Example: "Guaranteed"]</li> </ul>
	<b>Persist Duration</b>	[tp:PersistDuration]
	<b>Non Repudiation of Origin</b>	<p>[tp:SenderNonRepudiation]</p> <ul style="list-style-type: none"> <li>- tp:NonRepudiationProtocol</li> <li>- tp:HashFunction</li> <li>- tp:SignatureAlgorithm</li> <li>- tp:SigningCertificateRef</li> </ul>
	<b>Digital Envelope</b>	<p>[tp:SenderDigitalEnvelope]</p> <ul style="list-style-type: none"> <li>- tp:DigitalEnvelopeProtocol</li> <li>- tp:EncryptionAlgorithm</li> <li>- tp:EncryptionSecurityDetailsRef</li> </ul>
	<b>Nemespaces</b>	[tp:NamespaceSupported]
<b>Receiver Binding</b>	<b>Reliable Messaging</b>	<p>[tp:ReliableMessaging]</p> <ul style="list-style-type: none"> <li>- tp:Retries</li> <li>- tp:RetryInterval</li> <li>- tp:MessageOrderSemantics</li> </ul>
	<b>Persist Duration</b>	[tp:PersistDuration]
	<b>Non Repudiation of Receipt</b>	<p>[tp:ReceiverNonRepudiation]</p> <ul style="list-style-type: none"> <li>- tp:NonRepudiationProtocol</li> <li>- tp:HashFunction</li> <li>- tp:SignatureAlgorithm</li> <li>- tp:SigningSecurityDetailsRef</li> </ul>
	<b>Digital Envelope</b>	<p>[tp:ReceiverDigitalEnvelope]</p> <ul style="list-style-type: none"> <li>- tp:DigitalEnvelopeProtocol</li> <li>- tp:EncryptionAlgorithm</li> <li>- tp:EncryptionCertificateRef</li> </ul>
	<b>Namespaces</b>	[tp:NamespaceSupported]

## 9.7 トランスポート層のプロファイリング (Profiling the Transport Protocol)

The transport layer identifies the transport protocol to be used in sending messages through the network and defines the endpoint addresses, along with various other properties of the transport protocol. Choices of properties in the transport layer are complementary to those in the document-exchange layer (see "Document-Exchange Layer" directly above.)

トランスポート層は、ネットワークを介したメッセージの送信で使用されるトランスポート・プロトコルを識別し、他の様々なトランスポート・プロトコルの特性と共に、終端アドレスを定義する。トランスポート層における特性の選択は文書交換層における特性の選択と補完的である(すぐ上の「文書交換層」を参照)。

No profiling is required for this data. This table is provided as a support for users. プロファイリングはこのデータには要求されない。この表はユーザーのサポートとして提供される。

Transport Info		
<b>CPA Reference</b>	[CPA Template name]	
	[CPA Instance name, if used for instantiating a particular CPA]	
<b>Transport Sender</b>	<b>protocol</b>	[tp: TransportProtocol]
	<b>Client security</b>	[tp:TransportSecurityProtocol]
		[tp:ClientCertificateRef]
<b>Transport Receiver</b>	<b>protocol</b>	[tp: TransportProtocol]
	<b>End Point</b>	[tp:Endpoint/@uri, tp:Endpoint/@type]
	<b>Server security</b>	[tp:TransportSecurityProtocol]
		[tp:ServerCertificateRef]
		[tp:ClientSecurityDetailsRef]

## 9.8 PIP 定義における表の利用実例 (Examples of Tables Used in PIP Definitions)

These tables are extracted from the PIP7C7 definition. Their purpose here is to illustrate the terms and properties that map to the concepts in above CPA forms. The last row in these tables has been added to identify columns that are referred to in the above CPA forms.

これらのテーブルはPIP7C7定義から抜粋したものである。ここでのそれらの目的は、上記のCPAフォームのコンセプトにマッピングする用語および特性を例証することである。これらの表の最後列は、上記のCPAフォームで言及しているカラムを識別するために追加された。

Table 7: Business Activity Performance Controls

役割名	アクティビティ名	受信の確認			再試行回数	許可が必要か	発信元および内容の否認防止
		否認防止が必要か	確認までの時間	実行までの時間			
ファウンダリーテストサービス	半導体テストデータの通知	Y	2時間	N/A	3	Y	Y

Table 10: Message Exchange Controls

番号	名前	確認までの時間	アクションに答えるまでの時間	実行時間を含む	許可が必要か?	否認防止が必要か?	安全な転送が必要か?
1.	半導体テストデータ通知の実行	2時間	N/A	N/A	Y	Y	Y
1.1.	受信確認	N/A	N/A	N/A	N	N	Y

## 9.9 CPA 文書の例 (Sample CPA Material)

This is extracted from a sample CPA V2.0 document. Note: this is not a complete CPA document. これはサンプルCPA V2.0文書から抜粋されたものである。注記:これは完全なCPA文書ではない。

References the detailed information describing the way the data is assembled before entering the network.

ネットワークに接続する前に、データが組み立てられる方法を記述した詳細情報を参照する。

```
<... tp:partyName="CompanyA">
<tp:PartyId>
  tp:type="urn:oasis:names:tc:ebxml-cppa:partyid-type:duns"
  123456789
</tp:PartyId>
```

```
<tp:PartyRef xlink:href="http://CompanyA.com/about.html" />
<tp:ProcessSpecification>
  tp:version="2.0"
  tp:name="PIP3A4RequestPurchaseOrder"
  xlink:href="http://www.rosettanet.org/processes/3A4.xml"
  tp:uuid="urn:icann:rosettanet.org:bpid:3A4$2.0" />
</tp:ProcessSpecification>
<tp:Role>
  tp:name="Buyer"
  xlink:type="simple"
  xlink:href="http://www.rosettanet.org/processes/3A4.xml#Buyer">
</tp:Role>
<tp:Service>bpid:icann:rosettanet.org:3A4$2.0</tp:Service>
Security Certificate References and Certificates
tp:action="Purchase Order Request Action"
tp:packageId="CompanyA_RequestPackage"
References the detailed information describing the way the data is assembled before entering the network.
<tp:BusinessTransactionCharacteristics
  tp:isNonRepudiationRequired="true"
  tp:isNonRepudiationReceiptRequired="true"
  tp:isConfidential="transient"
  tp:isAuthenticated="persistent"
  tp:isTamperProof="persistent"
  tp:isAuthorizationRequired="true"
  tp:timeToAcknowledgeReceipt="PT2H"
  tp:timeToPerform="P1D" />
<tp>ActionContext
  tp:binaryCollaboration="Request Purchase Order"
  tp:businessTransactionActivity="Request Purchase Order"
  tp:requestOrResponseAction="Purchase Order Request Action" />
```

From the BPSS instance

```
<tp:TransportProtocol tp:version="1.1">HTTP</tp:TransportProtocol>
  <tp:AccessAuthentication>basic</tp:AccessAuthentication>
  <tp:AccessAuthentication>digest</tp:AccessAuthentication>
  <tp:Endpoint
    tp:uri="https://www.CompanyA.com/servlets/ebxmlhandler/sync"
    tp:type="allPurpose" />
  <tp:TransportServerSecurity>
    <tp:TransportSecurityProtocol tp:version="3.0">SSL</tp:TransportSecurityProtocol>
    <tp:ServerCertificateRef tp:certId="CompanyA_ServerCert" />
    <tp:ClientSecurityDetailsRef tp:securityId="CompanyA_TransportSecurity" />
  <tp:ReliableMessaging>
    <tp:Retries>3</tp:Retries>
    <tp:RetryInterval>PT2H</tp:RetryInterval>
    <tp:MessageOrderSemantics>Guaranteed</tp:MessageOrderSemantics>
  </tp:ReliableMessaging>
  <tp:SenderNonRepudiation>
    <tp:NonRepudiationProtocol>http://www.w3.org/2000/09/xmldsig#</tp:NonRepudiationProtocol>
    <tp:HashFunction>http://www.w3.org/2000/09/xmldsig#sha1</tp:HashFunction>
    <tp:SignatureAlgorithm>http://www.w3.org/2000/09/xmldsig#dsasha1</tp:SignatureAlgorithm>
    <tp:SigningCertificateRef tp:certId="CompanyA_SigningCert" />
  </tp:SenderNonRepudiation>
  <tp:SenderDigitalEnvelope>
    <tp:DigitalEnvelopeProtocol tp:version="2.0">S/MIME</tp:DigitalEnvelopeProtocol>
    <tp:EncryptionAlgorithm>DES-CBC</tp:EncryptionAlgorithm>
    <tp:EncryptionSecurityDetailsRef tp:securityId="CompanyA_MessageSecurity" />
  </tp:SenderDigitalEnvelope>
  <tp:PersistDuration>P1D</tp:PersistDuration>
```

## 10 付録 (Appendix) B: 用語集 (Glossary)

AMD	Abstract Message Service
ATPA	Abstract Trading Partner Agreement
MEP	Message Exchange Profiles
RNIF	RosettaNet™ Implementation Framework
PIP	(RosettaNet terminology): Partner Interface Process
TP	Trading Profile
ebMS	ebXML Messaging Services specification (an ebXML standard)
BPSS	ebXML Business Process Specification Schema (an ebXML standard)
ebBP	ebXML Business Process specification (applies to new version of BPSS, renamed)
CPP	ebXML Collaboration Protocole Profile (described in CPPA specification, an ebXML standard)
CPA	ebXML Collaboration Protocole Agreement (described in CPPA specification, an ebXML standard)
SBDH	Standard Business Document Header (also known as “Generic Header”)

## 11 参照 (References)

- [AMD] *MMS Abstract Message Definition*, Draft 00.07.00, 7 January 2005
- [ebMS] OASIS, *ebXML Message Service Specification Version 2.0*,  
[http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS\\_v2\\_0.pdf](http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf), April 1, 2002.
- [DPT-ebMS2] *Deployment Profile Template 1.1 for ebMS 2.0*, OASIS IIC committee draft, July 2005.  
[http://www.oasis-open.org/committees/documents.php?wg\\_abbrev=ebxml-iic](http://www.oasis-open.org/committees/documents.php?wg_abbrev=ebxml-iic)
- [DPT-CPPA2] *Deployment Profile Template 0.2 for CPPA 2.0*, OASIS IIC working draft, August 2005.  
[http://www.oasis-open.org/committees/documents.php?wg\\_abbrev=ebxml-iic](http://www.oasis-open.org/committees/documents.php?wg_abbrev=ebxml-iic)
- [BPSS-PIP] *RosettaNet ebXML BPSS Guideline*, v1.11, August 2004.
- [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,  
<http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- [RN-NameSpaces] *RosettaNet Namespace Specification and Management*, v1.0, December 2003.

