



Multiple Messaging Services (MMS) Profile for Web Services (WS)

ドキュメント情報

名前	Multiple Messaging Services (MMS) profile for Web Services WebサービスのためのMultiple Messaging Services (MMS)の プロファイル
バージョン	V11.00.01
更新日付	2009年8月05日

確定版 V11.00.01

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。

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)

©2009 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。

その他の確認事項 (Additional Disclaimers)

本仕様書の『文書型定義(DTD)』及び『要素記述』は、説明のためのものである。本仕様書の記載が個別に発表された『DTD』ファイル (*.dtd)、及び本仕様書と関連する『メッセージガイドライン仕様書』に一致するようあらゆる努力を払ったが、不一致がある場合は、『DTD』ファイルまたは『メッセージガイドライン仕様書』を優先して使用されたく。

本仕様書に記載された例は、対象の概念または規則を説明するためのものです。仕様ではありません。

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
V11.00.00	2008年7月29日	確定仕様として公開
V11.00.01	2009年8月05日	確定仕様として公開

謝辞 (Acknowledgments)

本書は、RosettaNet (<http://www.rosettanet.org/>) により準備されたものであり、ファウンデーション・プログラムにおいて集められた RosettaNet メソドロジへの適合要件に基づくものである。この設計及び開発に携わった会員・法人は次の通りである。

MMS WS Team

Member	Company	Member	Company
Mir Baqar	Cisco Systems	John Cartwright	Intel
Deepak Bhargava	Cisco Systems	Eric Hamer	Intel
Elham Ghassemzadeh	Cisco Systems	Jeremy Morrissey	Intel
Jim Kao	Cisco Systems	Frederic Herzer	Motorola
Abhijeet Ranadive	Cisco Systems	Thaddeus Marcelli	Motorola
Pranav Shahi	Cisco Systems	Mitri Abou-Rizk	Nokia
Gerald Silverman	Cisco Systems	Jeffrey Hutchins	Oracle
Sundar Subramanian	Cisco Systems	Annabelle Marlow	RosettaNet
John Voss	Cisco Systems	Nikola Stojanovic	RosettaNet
Dale Moberg	Cyclone Commerce	Kevin Liu	SAP
Garry Binder	DHL	Mark Schenecker	SAP
Peter Hawtrey	ePSA	Ron Boutell	Sterling Commerce
Martin Evans	Formfill	Suresh Damodaran	Sterling Commerce
Stewart Witchalls	Formfill	Tom Gindrup	TAG Business Tools
Jacques Durand	Fujitsu	Gary Sheetz	Tyco Electronics
Scott Hinkelman	IBM	Bill Wray	Tyco Electronics
Rania Khalaf	IBM	David Smiley	webMethods
Keeranoor Kumar	IBM	Bala Yanamandra	webMethods

Abstract

This document defines the RosettaNet Multiple Messaging Services profile for Web services. The Profile provides requirements, guidance and best practices about how to use a Web services message handling system to transport RosettaNet Business Messages between business partners.

要約

このドキュメントは、Webサービスに関するRosettaNet Multiple Messaging Servicesプロファイルを定める。このプロファイルは、ビジネス・パートナーの間でRosettaNet ビジネス・メッセージを転送するためにWebサービス・メッセージ処理システムを使う方法について、必要条件、ガイダンスと最も良い実行方法を提供する。

目次

1 目的の概要 (Overview of Intent)	7
1.1 マルチメッセージ通信サービスへの動機づけ (Motivation for Multiple Messaging Services)	7
1.2 MMS と MCC の関係 (The MMS relationship to MCC)	8
1.3 このプロファイルの目標及び範囲 (Goals and Scope of this Profile)	8
1.4 必要条件 (Prerequisites)	9
1.5 表記規約 (Notational Conventions)	10
2 アーキテクチャ概要 (Architecture Overview)	12
2.1 PIP を Web サービスにマッピングするアーキテクチャ(Architecture for Mapping a PIP to Web services)	12
2.1.1 異なる能力を持ったパートナーの調整 (Accommodating Partners of Different Capabilities)	12
2.1.2 メッセージ及びメッセージ交換パターン (Messages and Message Exchange Patterns)	12
2.1.3 サービスの説明 (Services Descriptions)	13
2.1.4 サービスの品質 (Quality of Service)	14
2.1.5 ビジネスプロセス (Business Process)	14
2.2 Web サービスを利用した RosettaNet ビジネス・メッセージ交換 (Using Web services to exchange RosettaNet Business Messages)	14
2.2.1 RosettaNet ビジネス・メッセージ交換 (Exchanging RosettaNet Business Messages)	14
2.2.2 PIP の実行 (Running a PIP)	15
3 サポートされた IT シナリオ及びメッセージ交換パターン (Supported IT Scenarios and Message Exchange Patterns)	17
3.1 能力の異なるパートナー (取引先) に適合させる (Accommodating Partners of Different Capabilities) ..	17
3.2 IT シナリオ: サービス・ツー・サービス (IT Scenario: Service to Service)	17
3.2.1 サービス・ツー・サービスの一方のコールバックへ (Service to Service One Way Callback)	18
3.3 IT シナリオ: ピア・クライアント・ツー・サービスへ (IT Scenario: Pure Client to Service)	18
3.3.1 ピア・クライアント・ツー・サービスへの要求応答 (Pure Client to Service Request Response)	18
3.3.2 ピア・クライアント・ツー・サービスへの要求応答プッシュ (Pure Client to Service Request Response Push)	19
3.3.3 ピア・クライアント・ツー・サービスへの要求応答プル (Pure Client to Service Request Response Pull) ..	19
3.4 例外処理の取り扱い (Exception Handling)	21
3.4.1 サービス・ツー・サービスの一方のコールバック (Service to Service One Way Callback)	21
3.4.2 ピア・クライアント・ツー・サービス へのメッセージ交換パターン (Pure Client to Service MEPs)	21
3.5 メッセージの相関について (Message Correlation)	22
3.5.1 受信確認 (Receipt Acknowledgements)	22
3.5.2 例外処理メッセージ / 例外処理操作 (Exception messages / ExceptionOp Operation)	23
3.6 IT シナリオのまとめ/ビジネス要件/パターン/WSDL (Summary IT Scenario / Business Requirements / Pattern / WSDL)	23
4 WSDL マッピング規則 (WSDL Mapping Rules)	24
4.1 メッセージ (Messages)	25
4.1.1 インポート・メッセージ・タイプ (Importing Message Types)	25
4.1.2 WSDL メッセージの定義 (Defining WSDL Messages)	26

4.2 操作 (Operations)	28
4.2.1 操作名取り決め (Operation Naming Convention)	28
4.2.2 信号操作の特徴 (Signature of Signal Operations)	29
4.2.3 メッセージ交換パターンのマッピングに必要な操作 (Operations Required for Mapping Message Exchange Patterns).....	29
4.3 結合 (バインディング) (Binding)	34
4.3.1 デフォルト結合 (Default binding)	35
4.3.2 MIME 結合&添付のサポート (MIME binding & Attachments support).....	35
4.3.3 圧縮のサポート (Compression support)	35
4.4 グルーピング操作に関するガイドライン (Guidelines for grouping operations).....	36
4.4.1 ガイドライン (Guidelines)	36
5 サービスの品質 (Quality of Services).....	42
5.1 QoS の設計視点 (QoS Design Points)	41
5.2 共通 QoS (Common QoS)	42
5.2.1 共通セキュリティ・ポリシーの使用方法 (Common Security Policy Usage)	42
5.3 QoS 及びピュア・クライアント・ツー・サービスへのパターン(QoS and Pure Client to Service Patterns)	51
5.3.1 ピュア・クライアントからのサービスに関する共通 QoS (Pure Client to Service Common QoS)	51
5.3.2 ピュア・クライアントからのサービス要求応答パターン (Pure Client to Service Request Response Pattern)	53
5.3.3 ピュア・クライアント・ツー・サービス要求応答プッシュ パターン (Pure Client to Service Request Response Push Pattern).....	54
5.3.4 ピュア・クライアント・ツー・サービスへの要求応答プル・パターン (Pure Client to Service Request Response Pull Pattern)	56
5.4 QoS とサービス・ツー・サービスのパターン (QoS and Service to Service Pattern)	58
5.4.1 サービス・ツー・サービスの一方向コールバック・パターン (Service To Service One Way Callback Pattern).....	58
6 用語集 (Glossary)	61
7 付録 A: 参照 (Appendix A: References)	63
8 付録 B: 使用事例 (Appendix B: Example Use Cases)	65
8.1 サービス・ツー・サービス (Service to Service)	65
8.1.1 サービス・ツー・サービスの一方向コールバック使用事例 (Service to Service One Way Callback Use Cases)	65
8.2 ピュア・クライアント・ツー・サービス (Pure Client to Service)	65
8.2.1 ピュア・クライアント・ツー・サービス要求応答での使用事例 (Pure Client to Service Request Response Use Cases)	65
8.2.2 プッシュ型ピュア・クライアント・ツー・サービスの使用事例 (Pure Client to Service Request Response Push Use Cases)	66
8.2.3 プッシュ型ピュア・クライアント・ツー・サービス要求 / 応答での使用事例 (Pure Client to Service Request Response Push Use Cases)	68
9 付録 C: 本プロファイルに特有のスキーマ (Appendix C: Schemas Specific To This Profile)	70
9.1 ReceiptAcknowledgment_00_01.xsd	70
9.2 WS_Exception_00_01.xsd.....	70
9.2.1 GEE (General Error).....	70
9.2.2 RAE (受信確認エラー) (Receipt Acknowledgement Error).....	71
9.3 WS_MessageError_00_01.xsd	71
9.4 WS_GetMessage_00_01.xsd.....	71

1 目的の概要 (Overview of Intent)

1.1 マルチメッセージ通信サービスへの動機づけ (Motivation for Multiple Messaging Services)

RosettaNet implementations today require each business partner to support an implementation of the RosettaNet Implementation Framework (RNIF). RNIF is a B2B message handling system intended for all XML message payloads defined within the RosettaNet standards. Although RNIF is fairly robust and is quite widely adopted within the high-tech industry, RosettaNet is looking for alternatives. The first reason is that RosettaNet sees its own future as a standards body supporting the upper layers relating to business messages and processes, rather than the lower layers concerned with messaging and other infrastructure. Therefore, as a home-grown standard, RNIF is likely to turn into a maintenance burden for RosettaNet in the long run. Secondly, there is great value in adopting message handling systems that serve multiple vertical markets. The presences of standards like RNIF that cater to specific verticals tend to add interoperability complexity and cost to organizations. Lastly, and perhaps most importantly, there is long-term payoff in making use of horizontal message handling systems that stand on their own right simply due to the fact that these standards will take care of their own evolution as times and technologies change. This is also the way to ensure that any evolution of the horizontal standard will result in the least impact to a vertical industry mission. For example, as pervasive devices become more prevalent, the horizontal standards will evolve to extend the reach to these devices thereby largely eliminating the need for the upper layers to worry about it. Consequently, many RosettaNet business partners view transition from RNIF into other horizontal message handling systems as a strategic business requirement.

今日、RosettaNetの導入には、各取引先がRosettaNet Implementation Framework(RNIF)の導入を支援することが必要である。RNIFは、RosettaNet標準で定義する全てのXMLメッセージのペイロードを対象としているB2Bメッセージ処理システムである。RNIFは非常にしっかりしていてハイテク産業界においてかなり広範囲に採用されているが、RosettaNetは代わりとなるものを求めている。第1の理由は、RosettaNetが自らの将来をメッセージング・インフラ、及び他のインフラを扱う下層よりむしろビジネス・メッセージ及びプロセスに関わる上層をサポートする標準化団体として見ていることである。それ故に、自分達で作った標準として、RNIFは長期的にはRosettaNetにとって保守の負担になる可能性が高い。第2に、複数の垂直市場に役立つメッセージ処理システムを採用することには大きな価値がある。特定の垂直市場に対応するRNIFのような規格の存在は、組織に対し互換に関する複雑性やコストを増大させる傾向がある。最後に恐らく最も重要なことにはこれらの規格が、時代や技術の変化に自ら進化するという事実から、彼等自身に権利があると認められる独立した横断的なメッセージ処理システムを利用するということが、長期的な利益があるのである。又、一切の横断的標準の発展が垂直業界へ最小限の影響しか与えないことを保証する。例えば、普及している機器が更に広く行き渡ると、横断的標準は発展してこれらの機器にまで対象範囲を広げ、その結果上層(ビジネスプロセスなど)がそれについて心配する必要性は無くなる。結果的に、RosettaNetの取引先の多くは、RNIFから他の横断的なメッセージ通信システムへの移行を戦略的ビジネス要件と考えるのである。

Multiple Messaging Services (MMS) is a RosettaNet Foundational Program chartered to address the support of RosettaNet XML business messages and business to business (B2B) collaboration over horizontal message handling systems. In its investigation, RosettaNet concluded that Web services, AS2 and ebMS were the three pre-dominant messaging systems for which specifications need to be derived for using them as a RosettaNet Business Message transport.

Multiple Messaging Services (MMS)は、横断的なメッセージ処理システム上でのロゼッタネットXML ビジネス・メッセージ及び企業間(B2B)共同作業のサポートに取り組むために特化されたロゼッタネットのファウンデーション・プログラムである。ロゼッタネットは調査の結果、Web サービス、AS2 及び ebMS が、RosettaNet ビジネス・メッセージ・トランスポート層として使用するために、適した仕様を生成する必要のある3つの優れたメッセージング・システムであると結論を下した。

1.2 MMS と MCC の関係 (The MMS relationship to MCC)

MMS also lays the foundation for the separation of the layers of implementation that is missing in the RNIF specification. Specifically, MMS separates what is now commonly understood to be choreography from message exchange. The subject of the MMS specification is message exchange. Message Exchange Patterns (MEPs) are the atomic units to be considered for how messaging will be implemented and may include information flow between two business partners in one or both directions.

MMS は更に、RNIF 規格に欠けている実装層の分離のための基盤となる。具体的には MMS はメッセージ交換から現在一般にコレオグラフィーと理解されているものを分離する。MMS 規格のテーマはメッセージ交換である。メッセージ交換パターン(MEPs)は、どのようにメッセージングが実装されるかを考える最小構成要素であり、一方向、又は、双方向で 2 社のビジネス・パートナー間での情報フローを含むであろう。

Choreography is the process that ties together the multiple MEPs to implement the full semantics of B2B transactions complete with handling of time constraints and exceptions. MMS specification will be complemented with an accompanying specification, Message Control and Choreography (MCC) whose scope will be addressing the choreography related gaps that emerge when the scope of MMS is set against that of RNIF. コレオグラフィーとは、時間制約及び例外処理の完備したB2B取引を最大限に実行するための多数の MEP (メッセージ交換パターン) を結ぶプロセスである。MMS規格は付随する規格、メッセージ管理とコレオグラフィー (MCC) によって補足され、それらのスコープはRNIFのスコープに対抗してMMSのスコープが決められる時出現するコレオグラフィー関連の差異に取り組むだろう。

1.3 このプロファイルの目標及び範囲 (Goals and Scope of this Profile)

The focus of this Profile is the specification of how RosettaNet XML business messages, in the context of RosettaNet business processes, will be transported with certain Quality of Service (QoS) guarantees, using Web services as the messaging infrastructure.

本プロファイルの焦点は、RosettaNet XMLビジネス・メッセージが、RosettaNetビジネス・プロセスと関連して、メッセージ伝達インフラとしてWebサービスを使用し、一定のサービス品質(QoS)保証の元で転送される方法の規格である。

While RNIF will serve as a very useful frame of reference for many issues relating to transportation, QoS and exception handling, the goal will not be to mimic or simulate RNIF. Accordingly, although RNIF has specifications as to how to package business messages, how to provide security and ensure message integrity, how to combine multiple messages and so on, these have been used as guidance to look for ways Web services can achieve the same objectives. There is maximum payoff from the use of a horizontal standard like Web services when and only when we use its features the way they were intended. Web services is an atypical messaging paradigm and has its special ways of handling the many transportation and quality issues, especially relating to addressing, security, reliable message delivery, and so on. Web service does not support all the features that RNIF does, but does provide other features RNIF does not.

RNIF はメッセージ伝送、QoS 及び例外処理に関連している多くの課題について大変役に立つフレームとして機能するが、MMS の目標は RNIF を模倣やシミュレーションすることではない。従って、RNIF にはビジネス・メッセージをパッケージする方法や安全性を提供し、メッセージの完全性を確保する方法、複数のメッセージを組み合わせた方法等についての規格があるが、これらは Web サービスが同じ目的を達成できる方法を探すための手引きとして使用されてきた。Web サービスのような横断的標準の使用には、その機能を意図されたように使用する場合に限り最大のメリットがある。Web サービスは非定型メッセージ伝達基準であり、多くのメッセージ伝送及び品質における課題、特にアドレス指定、安全性、信頼できるメッセージ配信等を処理する特別な方法を有する。Web サービスは、RNIF が行う全ての機能をサポートするとは限らないが、RNIF には持っていない他の機能を提供する。

In this Profile, the scope is to address a single RosettaNet Business Message exchange. A single message exchange may have the following variations:

このプロファイルでは、その対象範囲は1方向のRosettaNetビジネス・メッセージ交換に取り組むことである。1方向のメッセージ交換には下記の種類があるであろう：

- The sending of a RosettaNet Partner Interface Process (PIP) business document and the corresponding receipt of either a fault or a business acknowledgement.
RosettaNet Partner Interface Process (PIP) ビジネス文書の送付と、それに対する受領としての失敗又は業務確認メッセージ。
- The RosettaNet Business Message schema could be a Community PIP schema or TPIR-PIP schema.
RosettaNetビジネス・メッセージ・スキーマは、コミュニティ PIPスキーマ(標準PIP)、又は、TPIR-PIP(取引先が業務要件に合うように標準PIPをカスタマイズしたPIP)スキーマである可能性がある。
- Only schema PIPs are allowed. Community PIP schema must exist before the RosettaNet PIP can be used in MMS Web Services.
スキーマPIPしか許可されない。MMS Webサービスにおいて、ロゼッタネットPIPを使用するためには、コミュニティPIPスキーマが存在しなければならない。
- The sending of a RosettaNet Business Message and the corresponding receipt of a resulting RosettaNet Business Message.
RosettaNetビジネス・メッセージの送付と、それに対するRosettaNetビジネス・メッセージの受信。
- The sending of a request for a RosettaNet Business Message and the corresponding receipt of the requested RosettaNet Business Message
RosettaNetビジネス・メッセージの引き取り要求とそれに対する受領の送信。
- The specification is intended to be used for RosettaNet Community or TPIR PIP schemas, and may not support business document schemas or architecture of other standards.
この仕様書は、RosettaNet標準のPIPスキーマ、又はTPIR PIPスキーマの伝送手順として使用することを意図している。他の標準のビジネス文書スキーマやアーキテクチャはサポートされない。

Combining several RosettaNet Business Message exchanges to form a business transaction is out of scope for this Profile, and is in the space of choreography which will be handled by the MCC Foundational Program.

商取引を形成するために複数のRosettaNetビジネス・メッセージを組み合わせることは、本プロファイルの範囲外であり、MCC ファウンデーション・プログラムによって扱われるコレオグラフィー内にある。

1.4 必要条件 (Prerequisites)

This Profile assumes a good understanding of the basic concepts of Web services and the underlying standard specifications.

本プロファイルは、Webサービスの基本概念及び基本標準仕様の十分な理解を前提とする。

To get started, Appendix A provides non-normative information that is helpful for understanding the context of this Profile. It introduces the basic concepts of Web services and relates the concepts to the architectural approach of this Profile for mapping a RosettaNet PIP to Web services.

最初に、付録Aは、RosettaNetの標準ではないがこのプロファイルのコンセプトを理解するのに有用な情報を提供する。それはWebサービスの基本コンセプトを説明し、そのコンセプトをRosettaNet PIPをWebサービスにマップするための本プロファイルの構築方法に関連付ける。

1.5 表記規約 (Notational Conventions)

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119]:

キーワードMUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY 及びOPTIONALは、本書類に現われる場合、以下の[RFC2119]に記述される様に、解釈されることとなる:

MUST ねばなら ない	This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification. この単語、あるいは用語“REQUIRED(求められる)”ないし“SHALL(とする)”は、その定義が仕様の絶対的な要求であることを意味する。
MUST NOT してはなら ない	This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification. この句、あるいは“SHALL NOT(しないとする)”は、その定義が仕様の絶対的な禁止であることを意味する。
SHOULD すべきで ある	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. この言葉、あるいは形容詞“RECOMMENDED(勧められる)”は、特別な状況では特定の事項を無視すべき正当な理由が存在する可能性があるが、異なる過程を選択する前に、完全な影響を理解し慎重に検討しなければならないことを意味する。
SHOULD NOT すべきで ない	This phrase, or the phrase "NOT RECOMMENDED", means that there may exist valid reasons in particular circumstances when the particular behavior acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label. この句、あるいは“NOT RECOMMENDED(勧められない)”は、特定の行動が許容されるあるいは有用である特別な状況では正当な理由が存在する可能性があるが、完全な影響を理解し、この標示で記述されるどんな行動も実行する前にその事例を慎重に検討しなければならないことを意味する。
MAY してもよい	This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation, which does not include a particular option, MUST be prepared to interoperate with another implementation, which does include the option, though perhaps with reduced functionality. In the same vein an implementation, which does include a particular option, MUST be prepared to interoperate with another implementation, which does not include the option (except, of course, for the feature the option provides). この単語、あるいは形容詞“OPTIONAL(任意)”は、項目がまったく任意であることを意味する。あるベンダーはその専門市場がそれを必要とするか、又は別のベンダーは同じ項目を省略するかもしれない一方で、その製品を改善すると思うため、その項目を含むよう選択してよい。特定のオプションを含まない実装は、おそらく機能は減少してもそのオプションを含む、別の実装と相互運用するよう準備されなければならない。同様に、特定のオプションを含む実装は、(例題、当然、そのオプションが提供する機能)オプションを含まない別の実装と相互運用するよう準備されなければならない。

Normative statements of requirements in this Profile are presented in the following manner:

本プロファイルの要件の規範的な声明は、以下の方法で提示される：

Rnnnn Formal requirement text here.

Rnnnn 正式な要求された本文をここに記載。

The number "nnnn" above is replaced by a unique number in the Profile. To avoid conflicts with requirements defined in other profiles, the qualification MMS-WS should be used together with the Rnnnn number to form a unique requirement identifier, for example MMS-WS R0001.

上記の番号nnnnはこのプロファイルでは一意な番号が付与される。他のプロファイルで定義される要求事項とのバッティングを防ぐため、MMS-WSは一意の要求事項識別のためRnnnn番号とともに使われねばならない。例えばMMS-WS R0001である。

2 アーキテクチャ概要 (Architecture Overview)

2.1 PIP を Web サービスにマッピングするアーキテクチャ (Architecture for Mapping a PIP to Web services)

The approach presented in this Profile will take a PIP definition and illustrate how the corresponding XML files can be created to encode the PIP's requirements in Web services, as far as message exchanges are concerned. This section provides an outline of this mapping. It also explains how this Profile is organized to provide detail specification of the related mapping rules.

本プロファイルで提示されているアプローチは、PIP定義を例に挙げメッセージ交換に関してWebサービス内でPIPの要件をエンコードするために、対応するXMLファイルどのようにを作成するか説明している。このセクションでは、このマッピングの概要を提供する。又、関連するマッピングルールの詳細な仕様を提供するため、本プロファイルがどのように編成されているかについても説明する。

2.1.1 異なる能力を持ったパートナーの調整 (Accommodating Partners of Different Capabilities)

Partners participating in a RosettaNet PIP may not always have advanced infrastructure or constant Internet connection. This profile supports business partners with and without service-hosting capability.

RosettaNet PIPに参加しているパートナーが、必ずしも高度なインフラを持っていたり、インターネットに常時接続しているとは限らない。本プロファイルは、サービス・ホスティング機能の有無に関係なく、ビジネス・パートナーをサポートする。

Section 3 describes the different IT scenarios supported by this Profile.
セクション3は、このプロファイルによってサポートされる異なったITシナリオを記述する。

2.1.2 メッセージ及びメッセージ交換パターン (Messages and Message Exchange Patterns)

As explained in section 1.3, this profile only address a single RosettaNet Business Message exchange which consists of four patterns.

セクション1.3で説明したように、本プロファイルは、4つのパターンで構成される1方向のRosettaNetビジネス・メッセージの交換にのみ対応する。

Section 3 of this profile addresses these message exchange patterns in the context of different IT scenarios and business partner capabilities.

本プロファイルのセクション3は、異なるITシナリオ及びビジネス・パートナー能力を背景としたメッセージ交換に対応する。

Note that for PIP 0A1, the notification of failure (NOF) is assumed to go through another channel – as the specification says that the participant may no longer be there or running by then. NOF is its own PIP, and is mapped in the same manner as any other. No special provisions are made for it.

PIP 0A1については、失敗 (NOF) の通知が別のチャンネルを介すると想定されていることに注意されたい。 - 仕様書にも示されるように、実装している人は、もはやいないか又は実装しても使っていないだろう。NOFはそれ自体がPIPであり、他のものと同様の方法でマッピングされる。特殊条件はそのためにつ作られない。

This profile includes patterns involving 'pure clients', where this type of node is non-invokable, and can only have limited Web services capability. Within these patterns, specific fields within Web services specification structures may be specified for usage differently than for a 'classic', invokable Web services node. See the section on MEPs and message correlation for details on this topic.

本プロファイルは、このタイプのノードは呼び出し不可能で限られらWebサービス機能しか持たないピユ

アークライアント(純粋なクライアント)を含むパターンを持つ。これらのパターンの範囲内で、Webサービス仕様構造の範囲内の特定のフィールドが、「標準的な(classic)」呼び出し可能なWebサービスノードの場合とは異なる使い方として特定されるだろう。このトピックについての詳細については、MEP(メッセージ交換パターン)及びメッセージ相関性についてのセクションを参照されたい。

2.1.3 サービスの説明 (Services Descriptions)

Each participant in a PIP, with service hosting capabilities, must be described by a WSDL definition that defines its capabilities. Each of these WSDL definitions must contain one or more portTypes describing the services that the business partner offers for a particular PIP.

サービス・ホスティングの能力を持つ各PIP参加者は、能力を特定するWSDL定義により記述されていなければならない。それぞれのWSDL定義は、ビジネス・パートナーが特定のPIPに対して提供するサービスを説明した1つ以上のportTypeを持っていなければならない。

Section 4 of this Profile specifies rules for the creation of the corresponding WSDL operation definitions based on the XML Schema of the RosettaNet Business Messages that the operation will exchange and the interaction pattern being used. 本プロファイルのセクション4は、運用で交換するRosettaNet ビジネス・メッセージのXMLスキーマ、及び使用されている対話パターンに基づいた対応するWSDL オペレーション定義の作成のためのルールを示す。

2.1.3.1 TPIR-PIPs: PIP の特定化 (TPIR-PIPs: Specializing a PIP)

RosettaNet Automated Enablement [RAE] Trading Partner Implementation Requirements - Partner Interface Process [TPIR-PIP] Requirement documents are specializations of the community RosettaNet PIPs, usually through restrictions to the message definitions or possibly the QoS constraints. In this approach, we provide the steps required in order to define the proper Web services definitions at the WSDL level needed to enable TPIR-PIPs. This is done step-wise from the published specification files for that particular PIP and consists of minor changes to the target namespace of the WSDL definition and the schema data type of the messages carrying the TPIR-PIP RosettaNet Business Message. RAE (RosettaNet Automated Enablement) TPIR-PIP (Trading Partner Implementation Requirements - Partner Interface Process: 商取引パートナー実装要件PIP) 要件ドキュメントは、通常、標準の RosettaNet PIP から、メッセージ定義の制限や、場合によってはQoS制約を介して特定化したものである。このアプローチでは、WSDLレベルで TPIR-PIPの利用を可能にするのに必要な適切なWebサービスの定義を特定するために必要なステップを提供する。これは、その特定のPIP のために公開されている仕様ファイルから段階的に行われ、WSDL定義の対象ネームスペース及びTPIR-PIP RosettaNet ビジネス・メッセージを運ぶメッセージのXML Schemaのデータ型の小規模な変更からなる。

2.1.3.2 「サポートする連携方法」 (Supported Bindings)

SOAP over HTTP binding is considered as the default binding that each RosettaNet Web service must support.

「SOAP/HTTPは、各RosettaNet Webサービスがデフォルトでサポートしなければならない連携方法とみなされている。

Supporting attachments is a vital requirement in B2B business messaging. Today, Web services users use Message Transmission Optimization Mechanism (MTOM) or WS-I AP1.0 as two options to support attachments. However, a clear industry choice has not emerged and this specification would therefore allow the choice of either of them as per a Trading Partner Agreement (TPA) between the two business partners.

添付をサポートすることは、B2Bビジネス・メッセージングにおいて極めて重要な要件である。現在、Webサービスのユーザーは、添付をサポートする2つの選択肢として、Message Transmission Optimization Mechanism (最適化送信機能: MTOM) 又は、WS-I AP1.0 を使用している。しかしながら、産業界にお

る選択が未だ明らかになっていないので、本仕様書は、2社のビジネス・パートナーの間での Trading Partner Agreement (取引パートナー契約: TPA) に従っていずれかを選べるようになっている。

Since Web service does not provide a standard way for message compression, this specification does not endorse any particular compression technology. Business partners may choose to use specialized extensions that support compression. Compression is outside the scope of this specification.

Webサービスは標準的なメッセージ圧縮方法を提供しないので、本仕様書は特定の圧縮技術を支持することはしない。ビジネス・パートナーは、圧縮をサポートする専門の拡張子を選ぶことができる。圧縮は本仕様書の対象外である。

2.1.4 サービスの品質 (Quality of Service)

Given the different IT scenarios and different business partner capabilities as described in section 3, the QoS requirements are also different.

セクション3で述べたように、IT シナリオ及びビジネス・パートナー機能は異なることから、QoS要件も異なってくる。

Section 5 provides a detail specification of how QoS requirements of a PIP should be addressed using Web services.

セクション5は、Web サービスを利用する上で、PIPにおけるQoS要求の詳細仕様を記述している。

2.1.5 ビジネス・プロセス(Business Process)

Business processes describe the use of several messages as they relate to each other in order to fulfill a defined business goal.

メッセージは特定されたビジネス目標を達成するために相互に関連し合うため、ビジネス・プロセスはいくつかのメッセージの使い方について記述する。

The work in this Profile is targeted towards enabling the definition of business logic around a set of Web services interactions that handle RosettaNet Business Messages. At this point, we are concerned with being able to reliably and securely exchange these messages as Web services. We do not address business processes, but lay the foundation for its enablement. The space of business logic is expected to be addressed by a separate working group in the MCC Foundational Program.

本プロファイルの中の作業は、RosettaNet ビジネス・メッセージを扱う一連のWebサービスの相互のやり取りの周辺のビジネス・ロジック定義を有効にすることを目標にしている。我々は目下の所、Webサービスが確実にそして安全にこれらのメッセージの交換をできるよう取り組んでいる。我々は、ビジネス・プロセスは取り組まないが、それが実施できるように基礎を築く。ビジネス・ロジックの分野については、MCC Foundational Programの別の作業グループが取り組むことになっている。

2.2 Web サービスを利用した RosettaNet ビジネス・メッセージ交換 (Using Web services to exchange RosettaNet Business Messages)

2.2.1 RosettaNet ビジネス・メッセージ交換 (Exchanging RosettaNet Business Messages)

In order to implement a PIP, a user must download the relevant Community WSDL from RosettaNet, depending on the MEP. If RosettaNet has not yet provided Community WSDLs for a particular PIP, then two business partners can create them from the rules provided in this Profile.

PIPを実装するには、ユーザーはRosettaNetから、メッセージ交換パターン(MEP)に応じて、適切な RosettaNet標準のWSDL をダウンロードする必要がある。もしRosettaNet が特定のPIPのための標準

WSDLをまだ提供していない場合、2社のビジネス・パートナーは本プロファイルに記載されているルールにより作成することができる。

The hosting enabled business partner(s) must create an implementation from the given Community WSDL containing the messages that the business partner wishes to receive. The application logic is developed independently from the QoS requirements as these will be taken care of by the required middleware. Each hosting-enabled business partner then publishes the Web service at a URL of its choosing.

ホスティング可能なビジネス・パートナーは、与えられた標準 WSDL から、ビジネス・パートナーが受信したいメッセージを含んだ実行プログラムを作成しなければならない。アプリケーション・ロジックは、必要なミドルウェアにより処理されるため、QoS 要件から独立して開発される。そして、ホスティング可能な各ビジネス・パートナーは、好きな URL で Web サービスを公開する。

In this Profile, we provide the groundwork for exchanging RosettaNet documents over Web services. In practice, one would combine several related RosettaNet Business Message exchanges that are offered by a single (hosting-enabled) business partner and relating to the same business goal into a single WSDL portType that the business partner offers. The set of those operations and their ordering depends on the business logic surrounding them.

本プロファイルにおいて、我々はWebサービス上でのRosettaNetドキュメントの交換のための土台を提供する。実際には、単一の(ホスティング可能な)ビジネス・パートナーにより提供され、同じ事業目標に関連した複数の関連するRosettaNet ビジネス・メッセージの交換が、そのビジネス・パートナーが提供する単一のWSDL portTypeに統合されるであろう。これらの運用やその指示のセットはそれらを取り囲むビジネス・ロジックによる。

2.2.2 PIP の実行 (Running a PIP)

In order to execute a PIP-based exchange, the business partners must exchange the endpoint(s) of hosted services. This will be done by exchanging a WSDL that contains the WSDL <service> element that contains the URL inside its <port> element.

PIPに基づいた交換を実行するには、ビジネス・パートナーはホストされるサービスのエンドポイントを交換しなければならない。これは、<port> 要素の中にURLを持つWSDL <service> 要素を交換することによって行われる。

Each side must also be configured to handle the QoS requirements expressed in the WSDLs. If the middleware does not support WS-Policy, the user can manually configure the system to comply with the policy attachments; however, support for the underlying QoS mechanisms, such as WS-Security, is required in order to enact these policies.

又、両者共、WSDLで表されるQoS要件に対応するように設定されていなければならない。もしミドルウェアがWS-Policyをサポートしない場合、ユーザーは、WSポリシー・アタッチメントに従うようにシステムを手動で設定することができる；しかしながら、これらのポリシーを実行するためには、WS-Securityの様な基本的なQoS機構のためのサポートが必要である。

Once all is in place, the parties can start exchanging RosettaNet Business Messages using Web services.

全てがそろった場合、両者は、Webサービスを利用して、RosettaNetビジネス・メッセージを交換し始めることができる。

3 サポートされた IT シナリオ及びメッセージ交換パターン (Supported IT Scenarios and Message Exchange Patterns)

3.1 能力の異なるパートナー(取引先)に適合させる (Accommodating Partners of Different Capabilities)

Partners implementing a RosettaNet PIP may not always have advanced infrastructure or persistent Internet connection. In this Profile, we support two kinds of business partners: RosettaNet PIPを実装しているパートナーが、いつでも高度なインフラやインターネットの常時接続を備えているとは限らない。このプロファイルでは、私たちは2種類のビジネス・パートナーをサポートする:

- A pure-client business partner does not host services and cannot be invoked as a service. It can have varying Web service capabilities supporting at least the minimal set of specifications and standards listed earlier in the background section. **ピュア・クライアント**である(サーバー機能を持たない) **ビジネス・パートナー**は、ホストサービスを持たないし、サービスの起動もされない。彼等は、前の背景のセクションに記載した仕様及び標準の少なくとも最小セットをサポートしている種々のWebサービス能力は備えている。
- A hosting-enabled business partner has comprehensive Web service capabilities, supporting the full set of the specifications and standards listed earlier in the background section. It can host a Web service, and provide reliable, secure interactions using the relevant Web services specifications. A hosting-enabled business partner cannot invoke a pure-client. **ホスティング可能なビジネス・パートナー**は、包括的なWebサービス機能を有し、前の背景のセクションに記載した仕様及び標準の全セットをサポートしている。このパートナーはWebサービスをホストすることができ、該当するWebサービス仕様を使った信頼できる安全なやりとりを提供できる。ホスティング可能なビジネス・パートナーは、ピュア・クライアントを起動することができない。

Accordingly, we support PIP interactions in two basic IT scenarios:
従って、2つの基本的なITシナリオにおけるPIPのやり取りをサポートする。

- Service to service: Interactions between two hosting-enabled business partners. **サービス・ツー・サービス**: 2つのホスティング可能なビジネス・パートナー間のやり取り。
- Pure client to service: Interactions between a pure-client business partner and a hosting-enabled business partner. **ピュア・クライアント・ツー・サービス**: ピュア・クライアントであるビジネス・パートナーとホスティング可能なパートナー間のやり取り。

In the following section, the message exchange patterns associated with each of these IT scenarios is described.

次項で、それぞれのこれらのITシナリオに対応するメッセージ交換のパターンについて記述する。

3.2 IT シナリオ: サービス・ツー・サービス (IT Scenario: Service to Service)

In the service to service IT scenario, two hosting-enabled business partners interact with each other. The business requirement is for one business partner to send another a RosettaNet Business Message, and in return it receives a Receipt Acknowledgement or Exception for it.

サービス・ツー・サービスのITシナリオでは、2社のホスティング可能なビジネス・パートナーが相互通信を行う。ビジネス要件としては一社のビジネス・パートナーが他のパートナーにRosettaNetビジネス・メッセージを送り、返信として受信確認または「例外処理(Exception)」を受け取ることである。

3.2.1 サービス・ツー・サービス・一方向コールバック (Service to Service One Way Callback)

The Service to Service One Way Callback pattern requires all communication to be WSDL abstract layer one way and responses to be sent in separate connections. This pattern is mapped to a WSDL using two one way services with the first accepting a RosettaNet Business Message and the second accepting a Receipt Acknowledgement.

サービス・ツー・サービスの一方向のコールバック・パターンは、全ての通信が一方向でWSDLの抽象化層でなければならず、そして返答は別の接続で送信されなければならない。このパターンは、2つの一方向サービス(一つはRosettaNetビジネスメッセージの受信用、もうひとつは受信確認メッセージ(Ack)の受信用)のWSDLにマッピングされる。

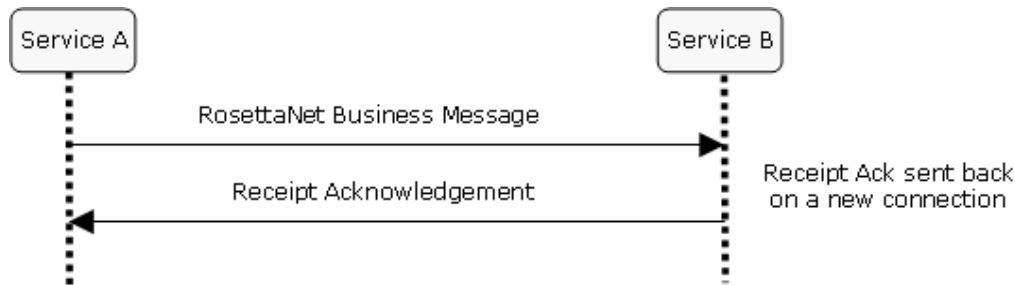


図 1: サービス・ツー・サービスの一方向のコールバック・パターン
(Service to Service One Way Callback Pattern)

3.3 IT シナリオ: ピュア・クライアント・ツー・サービス (IT Scenario: Pure Client to Service)

Not all businesses will have the luxury of being able to host a service listener. The barrier may be due to being occasionally connected or that hosting services requires more investment of time and resources and can be a burden to small to medium sized companies. It may also reduce their flexibility. These types of businesses use a pure client to initiate all connections interacting with services to push and pull RosettaNet Business Messages.

全ての事業者がサービス・リスナーに対して、賢沢なサービスを提供できるわけではない。時折接続するにすぎないことや、ホスティングサービスにより多くの時間と資源の投資が必要であることが障壁となっているのかもしれない。それは中小規模の会社にとっては負担となり得る。それはまた、柔軟性を欠くことにもなりかねない。これらのタイプの事業者は、RosettaNetビジネス・メッセージを送信したり受信したりするために、ピュア・クライアントを用いて、サービスと相互通信する全ての接続を開始する。

As does the service to service patterns, the pure client will still be expected to send and receive single RosettaNet Business Message, but the synchronous nature of the pure client to service interaction can also be used to meet the business need for real-time two action PIPs, such as a Price Check or Purchase Order Request.

サービス・ツー・サービスのパターンと同様、ピュア・クライアントは依然として単一のRosettaNet ビジネス・メッセージを送受信することが予想されるが、ピュア・クライアント・ツー・サービスへの交信の同期情報を使用して、「価格確認」(Price Check)または「発注依頼」(Purchase Order Request)のようなリアルタイムな2アクションPIPのためのビジネス・ニーズを満たすこともできる。

<u>ビジネス要求事項</u> <u>Business Requirement</u>	<u>ピュア・クライアント・ツー・サービスの</u> <u>パターン</u> <u>Pure Client To Service Pattern</u>
Pure Client needs to send a service a RosettaNet Business Message, and then receive a RosettaNet Response Business Message or Exception in return. ピュア・クライアントはサービスにRosettaNet ビジネス・メッセージを送信する必要があり、次に返信としてRosettaNet ビジネス・メッセージ返答又は「例外処理」を受け取る	Pure Client to Service Request Response ピュア・クライアント・ツー・サービス要求 / 応答
Pure Client needs to send a service a RosettaNet Business Message, and then receive a Receipt Acknowledgement or Exception in return. ピュア・クライアントはサービスにRosettaNet ビジネス・メッセージを送信する必要があり、次に返信として「受信確認」又は「例外処理」を受け取る。	Pure Client to Service Request Response Push プッシュ型ピュア・クライアント・ツー・サービス要求 / 応答
Pure Client needs to receive a RosettaNet Business Message from a service. ピュア・クライアントは、サービスからRosettaNetビジネス・メッセージを受信する必要がある。	Pure Client to Service Request Response Pull プル型ピュア・クライアント・ツー・サービス要求 / 応答

3.3.1 ピュア・クライアント・ツー・サービス要求 / 応答 (Pure Client to Service Request Response)

The Pure Client to Service Request Response pattern enables a pure client to send a RosettaNet Business Message and receive a RosettaNet Business Message on the same connection. This pattern is mapped to WSDL using one request response service. The pure client will send a RosettaNet Business Message to the service and the service will respond on the same connection with the resulting RosettaNet Response Business Message.

ピュア・クライアント・ツー・サービス要求 / 応答パターンは、ピュア・クライアントがRosettaNet ビジネス・メッセージを送り、同一セッションでRosettaNet ビジネス・メッセージを受信することが可能となる。このパターンは、1つの要求応答サービスを使用してWSDLにマッピングされる。ピュア・クライアントはサービスに向けて、RosettaNet ビジネス・メッセージを送り、サービスは同一セッションで、結果として得られたRosettaNet ビジネス・メッセージ応答によって応答する。

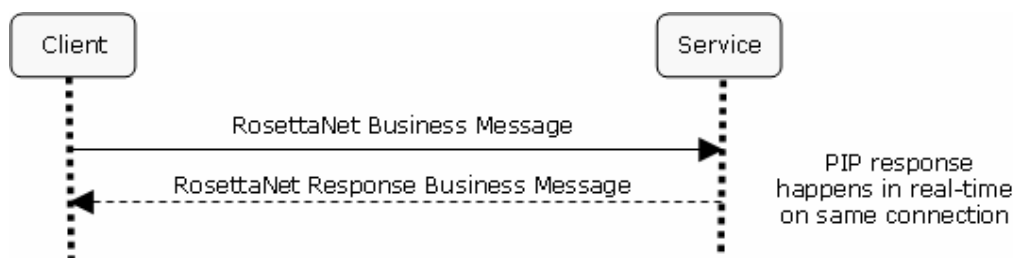


図4: ピュア・クライアント・ツー・サービス要求 / 応答
(Pure Client to Service Request Response)

3.3.2 プッシュ型ピュア・クライアント・ツー・サービス要求 / 応答 (Pure Client to Service Request Response Push)

The Pure Client to Service Request Response Push pattern enables a pure client to send RosettaNet Business Messages to other businesses. This pattern is mapped to a WSDL using one request response service. The pure client will send a RosettaNet Business Message to the service and the service will respond on the same connection with a Receipt Acknowledgement indicating that it received the document.

プッシュ型ピュア・クライアント・ツー・サービス要求 / 応答パターンは、ピュア・クライアントが他の事業者に向けて RosettaNet ビジネス・メッセージを送信することを可能にする。このパターンは、1つの要求応答サービスを使用して WSDL にマッピングされる。ピュア・クライアントはサービスに向けて、RosettaNet ビジネス・メッセージを送信し、サービスは同一セッションで、文書を受け取ったことを示す「受信確認」を返す。

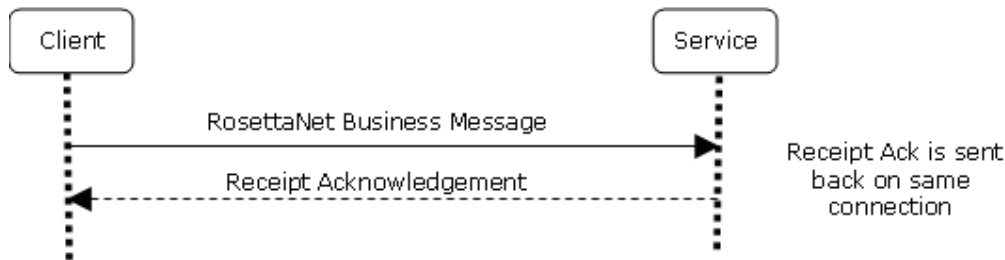


図 5: プッシュ型ピュア・クライアント・ツー・サービス要求 / 応答 (Pure Client to Service Request Response Push)

3.3.3 プル型ピュア・クライアント・ツー・サービス要求 / 応答 (Pure Client to Service Request Response Pull)

The Pure Client to Service Request Response Pull pattern enables businesses to send a RosettaNet Business Message to pure clients without requiring the pure clients to host web service listener. This pattern is mapped to a WSDL using one request response service. The pure client will send a soap message request to the service and the service will respond on the same connection with the RosettaNet Business Message requested.

プル型ピュア・クライアント・ツー・サービス要求 / 応答パターンは、ピュア・クライアントにWebサービス・リスナーをホストすることを要求することなく、事業者はピュア・クライアントにRosettaNet ビジネス・メッセージを送信することができる。このパターンは、1つの要求応答サービスを使用してWSDLにマッピングされる。ピュア・クライアントはSOAPメッセージ要求をサービスに送信し、サービスは同一セッションで、要求されたRosettaNet ビジネス・メッセージと共に応答する。

To indicate successful receipt of the RosettaNet Business Message, the pure client may initiate a new connection with the service and send a receipt acknowledgment. The client must then look for the HTTPS response code indicating a successful receipt of the Receipt Acknowledgement.

RosettaNet ビジネス・メッセージを正しく受信したことを表示させるために、ピュア・クライアントはサービスとの新しいセッションを開始し、受信確認を送信することができる。クライアントは次に、サービスが受信確認(Ack)を正常に受信したことを示すHTTPSの受信確認(レスポンス・コード)を待たなければならない。

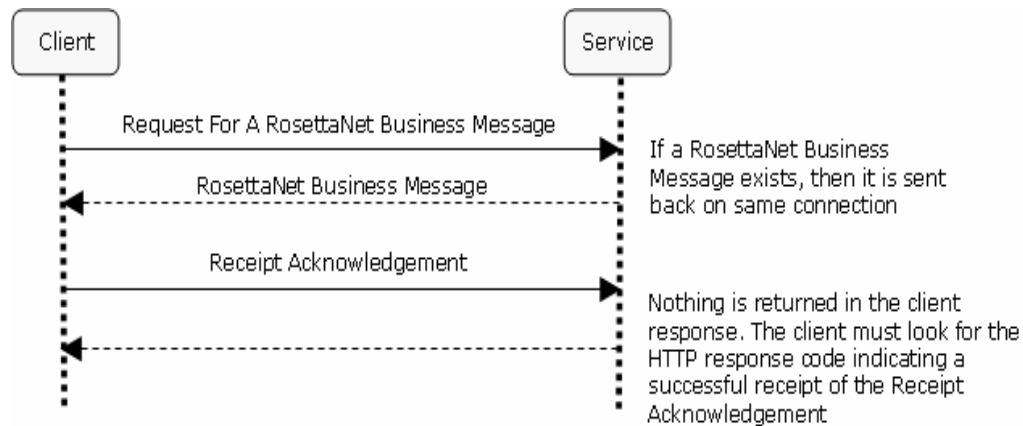


図 6: プル型ピュアクライアント・ツー・サービス要求 / 応答
(Pure Client to Service Request Response Pull)

3.4 例外処理の取り扱い (Exception Handling)

3.4.1 サービス・ツー・サービスの一方方向のコールバック (Service to Service One Way Callback)

Errors other than SOAP faults relating to the WS-* specifications MUST result in exceptions sent by in separate connection.

SOAP不具合以外のWS-*仕様に関連したエラーは、必ず別の接続で送信される「例外処理」に帰着すること。

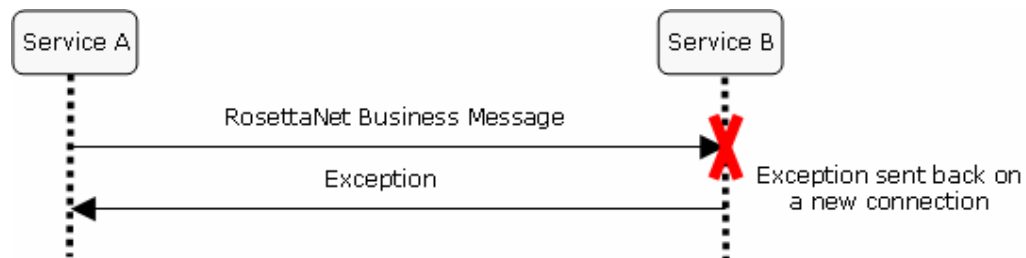


図 7: サービス・ツー・サービスの一方方向のコールバック の例外処理
(Exception handling in the Service to Service One Way Callback Pattern)

3.4.2 ピュア・クライアント・ツー・サービス へのメッセージ交換パターン (Pure Client to Service MEPs)

Errors encountered by the service receiving the initiating SOAP request message from the pure client MUST result in exceptions sent back in the same connection.

サービスがピュア・クライアントからSOAP開始要求メッセージを受け取る際に遭遇したエラーは必ず、同じ接続内で「例外処理」として送り返されなければならない。

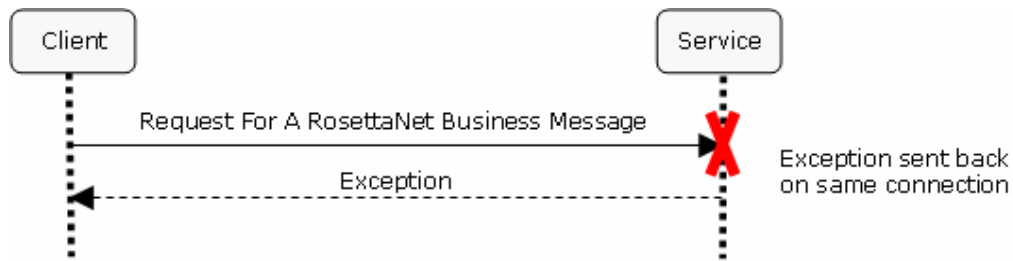


図 10: サービスがSOAP要求メッセージを受け取る際にエラーに遭遇した時、
 ピュア・クライアント・ツー・サービス へのメッセージ交換パターンにおける例外処理
 (Exception handling in the Pure Client to Service MEPs when the service fails to receive the SOAP request message)

3.5 メッセージの相関について (Message Correlation)

This section of the Profile incorporates the following specifications by reference to support message correlation:

プロファイルのこのセクションでは、サポートメッセージ相関を参照することにより、以下の仕様が組み込まれる。

- [Web Services Addressing 1.0 – Core](http://www.w3.org/TR/ws-addr-core/) W3C Recommendation 9 May 2006
- [Web Services Addressing 1.0 – SOAP Binding](http://www.w3.org/TR/ws-addr-soap/) W3C Recommendation 9 May 2006

Message correlation is the concept of relating one message to another. This is accomplished by identifying each message and using that unique identifier as a correlation token where needed.

メッセージの相関は、1つのメッセージを別のメッセージに関連付ける概念である。それは、各メッセージを識別し、その一意の識別子を必要とされる場所で相関トークンとして使用することによって成し遂げられる。

3.5.1 受信確認 (Receipt Acknowledgements)

R0001 Receipt Acknowledgement (RA SOAP) SOAP messages MUST be correlated to the SOAP message containing the related RosettaNet Business Message (PIP SOAP) by setting WS-Addressing RelatesTo in the (RA SOAP) to the WS-Addressing MessageID of the (PIP SOAP)

R0001 受信確認(RA SOAP)SOAPメッセージは、(PIP SOAP)のWS-Addressing MessageID を、(RA SOAP)のWS-Addressing RelatesToに設定することにより、関連するRosettaNet ビジネスメッセージ(PIP SOAP)を持っているSOAPメッセージに相関しなくてはならない。(MUST)

理論的根拠 Rationale

Receipt Acknowledgements are used by the service to track whether the RosettaNet Business Message was successfully received by the recipient and may carry non-repudiation of receipt information. Doing this is not possible without message correlation. 受信確認はRosettaNetビジネス・メッセージが受信者にうまく受信されたかどうかを追跡するためにサービスによって用いられ、受領情報の否認防止を実施するであろう。これはメッセージの相関なしでは不可能である。

3.5.2 例外処理メッセージ / 例外処理操作 (Exception messages / ExceptionOp Operation)

R0002 Exception (EM SOAP) SOAP messages sent back to the sender in a separate connection using the ExceptionOp operation MUST be correlated to the SOAP message (SR SOAP) that encountered an error on receipt by setting WS-Addressing RelatesTo in the (EM SOAP) to the WS-Addressing MessageID of the (SR SOAP)

R0002 ExceptionOpオペレーションを用いて別の接続で送信側に送り返される「例外処理」(EM SOAP) SOAPメッセージは、(SR SOAP)のWS-Addressing MessageIDを、(EM SOAP)のWS-Addressing RelatesToに設定することによって受信時にエラーが発生したSOAPメッセージ(SR SOAP)と関連しなくてはならない。(MUST)

理論的根拠 Rationale

Exception messages are used by the service to determine the Soap message that it is related to. Doing this is not possible without message correlation.
例外処理メッセージは、関連する SOAP メッセージを決定するために、サービスによって使用される。これはメッセージ相関なしでは不可能である。

3.6 IT シナリオのまとめ/ビジネス要件/パターン/WSDL (Summary IT Scenario / Business Requirements / Pattern / WSDL)

IT Scenario	Message Exchange Pattern	Business Requirement Met	WSDL
Service To Service	One Way Callback	Service needs to send another service a RosettaNet Business Message, and then receive a Receipt Acknowledgement or Exception in return. サービスは別のサービスに、RosettaNet ビジネス・メッセージを送信する必要があり、次に返信として「受信確認」、又は「例外処理」を受ける。	<u>WSDL Operations</u>
Pure Client To Service	Request Response	Pure Client needs to send a service a RosettaNet Business Message, and then receive a RosettaNet Response Business Message or Exception in return. ピュア・クライアントは、サービスに、RosettaNet ビジネス・メッセージを送信する必要があり、次に返信として「RosettaNet ビジネス・メッセージ応答」、又は「例外処理」を受ける。	<u>WSDL Operations</u>
Pure Client To Service	Request Response Push	Pure Client needs to send a service a RosettaNet Business Message, and then receive a Receipt Acknowledgement or Exception in return. ピュア・クライアントは、サービスに、RosettaNet ビジネス・メッセージを送信する必要があり、次に返信として「受信確認」、又は「例外処理」を受ける。	<u>WSDL Operations</u>
Pure Client To Service	Request Response Pull	Pure Client needs to receive a RosettaNet Business Message from a service. ピュア・クライアントは、サービスからRosettaNet ビジネス・メッセージを受信する必要がある。	<u>WSDL Operations</u>

更なる異なったユースケースパターンは、Appendix B を参照してください。
See Appendix B for more example use cases of the different patterns.

4 WSDL マッピング規則 (WSDL Mapping Rules)

This section of the Profile incorporates the following specifications by reference:
プロファイルのこのセクションは、参照として以下の仕様を組み込む:

- Web Service Description Language (WSDL) 1.1 W3C Note 15 March 2001
<http://www.w3.org/TR/wSDL>

Further, increased interoperability, the following profiles are incorporated by reference:
さらに、相互運用性の向上のため、参照として以下のプロファイルを組み込んだ:

- WS-I Basic Profile 1.1 WS-I Final Material 10 April 2005
<http://www.ws-i.org/Profiles/BasicProfile-1.1.html>

The use of WSDL 1.1 must follow the WS-I guidance as specified in its related profiles.
WSDL 1.1の使用の場合は、対応プロファイルで指定するように、WS-I ガイダンスに従うこと。

From a logical perspective, this profile views WSDL as 3 sections – “What”, “How” and “Where”. This profile is focused primarily on what layer, less focused on the How layer, and does not address the Where layer. The location of services, defined by the Where layer is to be defined by RosettaNet business partners deploying services on to a Web services infrastructure.

論理の視点から、本プロファイルは、WSDLを3つのセクションとして - 「What」、「How」及び「Where」を表示する。本プロファイルでは、主にWhat層にフォーカスし、How層にはあまりフォーカスせず、Where層は注視しない。Where層により定義されるサービスの位置は、Webサービス・インフラにサービスを展開しているRosettaNetビジネス・パートナーにより定義される。

In a service to service IT scenario for a single action PIP, where both endpoints are able to receive invocations, two services must be created, one by each business partner. First service provides an endpoint to receive the business document. Second service enables the receiving business partner to either acknowledge the receipt of the business document or indicate that an exception was encountered. Therefore, for a single action PIP, at minimum three WSDL operations must be created. Similarly, a dual action PIP requires six WSDL operations at minimum.

1 アクションPIPのサービス・ツー・サービスのITシナリオで、両方のエンドポイントが呼び出しを受け取ることができる場合、2つのサービス(各ビジネス・パートナーに1つ)が作成されなければならない。第1のサービスは、ビジネス文書を受信するためにエンドポイントを提供する。第2のサービスによって、受信ビジネス・パートナーは、ビジネス文書を受信を確認するか、例外処理が発生したことを認識することができる。従って、1アクションPIPで、最低3回のWSDLオペレーションが作成されなければならない。同様に、2アクションPIPは最低でも6回のWSDLオペレーションを要求する。

In a pure client to service IT scenario for a single action PIP, one service must be created by the hosting enabled business partner. The hosting enabled partner's service enables the pure client to either push or pull a RosettaNet Business Message. The service also enables the pure client to acknowledge the receipt of a pulled RosettaNet Business Message. Therefore, for a single action PIP, one WSDL operation must be created for the pure client push. Two WSDL operations must be created for the pure client pull.

1 アクションPIP用のピュア・クライアント・ツー・サービスへのITシナリオでは、ホスティング対応ビジネス・パートナーにより、1つのサービスが起きなければならない。ホスティング対応パートナーのサービスにより、ピュア・クライアントは、プッシュ又はプルでRosettaNet ビジネス・メッセージが使える。又サービスにより、ピュア・クライアントは、取り出したRosettaNet ビジネス・メッセージの受信を確認することが可能になる。従って、1 アクションPIPでは、ピュア・クライアントのプッシュ用に1回のWSDLオペレーションが作成されなければならない。2 回のWSDLオペレーションは、ピュア・クライアントのプル用に作成されなければならない。

4.1 メッセージ (Messages)

4.1.1 インポート・メッセージ・タイプ (Importing Message Types)

R1001 Types defined in the RosettaNet schemas MUST be imported into the WSDL Type section.

R1001 RosettaNetスキーマで定義されるデータ型Typeは、WSDLのTypeセクションにインポートすること。(MUST)

理論的根拠 Rationale

The RosettaNet schema defines several complex types, including the type that is used to define the WSDL message, and is provided by RosettaNet workgroups focused on the business content. In order to separate concerns and be consistent in RosettaNet MMS, this profile prohibits authoring of the business content schema directly inside the WSDL Type section.

RosettaNetスキーマは、数種のComplex Typeを定義している。それはWSDLメッセージを定義するために使用されるデータ型を含んでおり、業務内容に焦点を置いたRosettaNetワーク・グループによって提供される。懸念を切り離すため及びRosettaNet MMSで一貫するため、本プロファイルは、業務内容スキーマをWSDLのTypeセクション内に直接記述することを禁止する。

例 Example

In case of the purchase order request, the purchase order RosettaNet schema must be imported. It contains the XML Schema types required to exchange message containing the purchase order request.

購買発注依頼の場合は、購買発注RosettaNetスキーマがインポートされなければならない。それは購買発注依頼を含むメッセージを交換するのに必要なXMLスキーマデータ型を持つ。

```
<wsdl:types>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">

<xsd:import namespace="..."
schemaLocation="./Interchange/PurchaseOrderRequest.xsd" />

</xsd:schema>

...

</wsdl:types>
```

4.1.2 WSDL メッセージの定義 (Defining WSDL Messages)

RosettaNet has defined schema for business messages as well as signal messages. Business message schemas are located in the Interchange folder. Signal schemas are located in the System directory. Following rules apply to all WSDL messages that refer to RosettaNet defined business schemas as well as signal schemas.

RosettaNetは、シグナル・メッセージと同様にビジネス・メッセージ用にスキーマを定義した。ビジネス・メッセージ・スキーマは、Interchangeフォルダに保存されている。シグナル・スキーマは、Systemディレクトリに保存されている。以下のルールは、シグナル・スキーマと同様にRosettaNet定義のビジネス・スキーマを参照する全てのWSDLメッセージに適用する。

R1002 All WSDL messages that refer to RosettaNet business schemas or signal schemas MUST contain a single part.

R1002 RosettaNetビジネス・スキーマ、又はシグナル・スキーマを参照する全てのWSDLメッセージは、単一のパートを含むこと。(MUST)

R1003 If business partners have created TPIR-PIP schema, schemaLocation that refer to corresponding RosettaNet Business Message, MUST refer to TPIR-PIP schema location instead.

R1003 ビジネス・パートナーがTPIR-PIPスキーマを作成した場合、対応するRosettaNetビジネス・メッセージを参照するスキーマのロケーションは、TPIR-PIPスキーマのロケーションを代わりに参照すること。(MUST)

例 Example

```
<xsd:import namespace="..." schemaLocation="TPIRSchema.xsd"/>
```

R1004 The single part MUST refer to the root element within the RosettaNet schema.

R1004 単一のパートは、RosettaNetスキーマ中のルートエレメントを参照すること。(MUST)

R1005 The name of the WSDL message MUST be created by adding 'Msg' to the local name of the element.

R1005 WSDLメッセージ名は、エレメントのローカル名に「Msg」を追加することによって作成すること。(MUST)

R1006 The part name MUST be created by adding 'Part' to the name of the element.

R1006 パート名は、エレメント名に「Part」を追加することによって作成すること。(MUST)

例 - RosettaNetビジネス・メッセージ (Example - RosettaNet Business Message)

- 'PurchaseOrderRequestMsg' message contains a single part i.e. PurchaseOrderRequestPart.
- 'PurchaseOrderRequestMsg'メッセージは、シングルpartを含む。即ち、PurchaseOrderRequestPart.
- 'PurchaseOrderRequestPart' refers to the root element within the RosettaNet schema i.e. poreq:purchaseOrderRequest.
- 'PurchaseOrderRequestPart' は、RosettaNetスキーマ中のルートエレメントを参照する。即ち、poreq:purchaseOrderRequest.
- 'PurchaseOrderRequestMsg' is created by adding 'Msg' to the root element within the RosettaNet schema.
- 'PurchaseOrderRequestMsg' は、RosettaNetスキーマのルートエレメントに'Msg'を追加することによって作成される。
- PurchaseOrderRequestPart is created by adding 'Part' to the root element within the RosettaNet schema.
- 'PurchaseOrderRequestPart'は、RosettaNetスキーマのルートエレメントに'Part'を追加することによって作成される。

```
xmlns:poreq="urn:rosettanet:specification:interchange:PurchaseOrderRequest:xsd:
schema:1.0"
```

```
<wsdl:message name="PurchaseOrderRequestMsg">
```

```
<wsdl:part name="PurchaseOrderRequestPart"
element="poreq:PurchaseOrderRequest"/>
```

```
</wsdl:message>
```

例 受信確認メッセージ (Example - Receipt Acknowledgement Message)

In case of receipt acknowledgment message, the message and part definitions are based on the element 'receiptack: ReceiptAcknowledgment'.

受信確認メッセージの場合、メッセージ及びpartの定義は、エレメント' receiptack: ReceiptAcknowledgment 'に基づく。

```
<wsdl:message name="ReceiptAcknowledgmentMsg">
  <wsdl:part name="ReceiptAcknowledgmentPart"
    element="receiptack:ReceiptAcknowledgment"/>
</wsdl:message>
```

例 例外処理メッセージ Example - Exception Message

In case of Exception message, the message and part definitions are based on the element 'exception:Exception'.

例外処理メッセージの場合、メッセージ及びpartの定義はエレメント' exception:Exception 'に基づく。

```
<wsdl:message name="ExceptionMsg">
  <wsdl:part name="ExceptionPart" element="exception:Exception"/>
</wsdl:message>
```

R1007 An Exception message MUST be used in detail part of SOAP faults for all MEP except Service to Service One Way Callback.

R1007 例外処理メッセージは、サービス・ツー・サービスの一方向コールバックを除き、全てのメッセージ交換パターン(MEP)に対しSOAPエラーの詳細パートで使用すること。(MUST)

理論的根拠 Rationale

In case of all MEPs except Service to Service One Way Callback, exceptions are communicated as SOAP fault detail. In case of Service to Service One Way Callback, ExceptionMsg is used as input to an exception operation (ExceptionOp). Use of ExceptionMsg is SOAP fault, as well as input to ExceptionOp, provides a common exception schema for both the cases.

サービス・ツー・サービスの一方向コールバックを除く全てのメッセージ交換パターン(MEP)において、例外処理はSOAPエラーの詳細として通信される。サービス・ツー・サービスの一方向コールバックの場合、ExceptionMsgは例外処理のオペレーション(ExceptionOp)への入力として使用される。ExceptionMsgの使用はSOAPエラーであり、ExceptionOpへの入力と同様に、両方のケース用に一般的な例外処理スキーマを提供する。

例 Example

```
<wsdl:operation name="ProductInformationQueryAndSalesCatalogOp">
  ...
  <wsdl:fault message="tns:ExceptionMsg" />
</wsdl:operation>
```

4.2 操作 (Operations)

4.2.1 操作名取り決め (Operation Naming Convention)

The operation names are based on the operation parameters. In general RosettaNet PIP Activity gets mapped to operation name, and Action gets mapped to parameters. 操作名は動作パラメータに基づく。一般に、RosettaNet PIPアクティビティは操作名にマッピングされ、アクションはパラメータにマッピングされる。

R1009 For operations with a single input RosettaNet Business Message (no output), the operation name MUST be constructed by adding 'Op' to the root element of the input RosettaNet schema. Following is the convention used:

R1009 単一の入力RosettaNetビジネスメッセージ(出力がない)による操作において、操作名は、入力RosettaNetスキーマのルートエレメントに「Op」を追加することによって作成すること。(MUST)
以下は使用される取り決めである：

InputRootElementNameOp

例 Example

```
<wsdl:operation name=" PurchaseOrderStatusNotificationOp">
<wsdl:input message="tns:PurchaseOrderStatusNotificationMsg" />
</wsdl:operation>
```

R1010 For operations with an input and output RosettaNet Business Message the operation name MUST be constructed by appending root element of the output RosettaNet schema to root element of the input RosettaNet schema, and then appending 'Op' to this name.

R1010 入出力 RosettaNet ビジネス・メッセージの操作で、操作名は、入力 RosettaNet スキーマのルートエレメントに出力 RosettaNet スキーマのルートエレメントを追加することによりその名前に「Op」を追加すること。(MUST)

Following is the convention used:
以下は使用される取り決めである：

RequestRootElementNameAndResponseRootElementNameOp

例1 Example 1

```
<wsdl:operation name="ProductInformationQueryAndSalesCatalogOp">
<wsdl:input message="tns: ProductInformationQueryMsg" />
<wsdl:output message="tns: SalesCatalogMsg" />
</wsdl:operation>
```

例2 Example 2

In case of *pure client to service request response pull*, the input message is 'QueryCriterionMsg'. The 'QueryCriterionMsg' may refer to a RosettaNet Business Message specific Query Criterion XSD created based on the template schema (WS_GetMessage_00_01.xsd) defined by RosettaNet, or schema specific to the business partners.

プル型ビュー・クライアント・ツー・サービス要求 / 応答の場合、入力メッセージは 'QueryCriterionMsg' (問い合わせ標準メッセージ) である。'QueryCriterionMsg' は、RosettaNet によって定義されるテンプレート・スキーマ (WS_GetMessage_00_01.xsd) に基づいて作成される RosettaNet ビジネス・メッセージに

特有の Query Criterion XSD(問い合わせ標準 XSD)、又はビジネス・パートナーに特有のスキーマを参照するでしょう。

```
< wsdl:operation name="QueryCriterionAndPurchaseOrderRequestOp">
< wsdl:input message="tns:QueryCriterionMsg"/>
< wsdl:output message="tns:PurchaseOrderRequestMsg" />
</wsdl:operation>
```

R1011 Fault operation MUST be named 'ExceptionOp'

R1011 エラー操作では、'ExceptionOp(例外処理操作)'という名前を付けること。(MUST)

理論的根拠 Rationale

Input of fault operation is the Exception schema defined by RosettaNet. The operation name is constructed by appending 'Op' to root element of the Exception RosettaNet schema.

エラー操作の入力は、RosettaNetによって定義される例外処理スキーマである。操作名は、例外処理 RosettaNetスキーマのルートエレメントに「Op」を追加することによって作成される。

例 Example

```
< wsdl:operation name=" ExceptionOp">
< wsdl:input message="tns: ExceptionMsg" />
</wsdl:operation>
```

R1012 Receipt Acknowledgement operation MUST be named 'ReceiptAcknowledgmentOp'.

R0012 受信確認の操作では、「Receipt AcknowledgmentOp(受信確認操作)」という名前を付けること。(MUST)

理論的根拠 Rationale

Input of receipt operation is the ReceiptAcknowledgment schema defined by RosettaNet. The operation name is constructed by appending 'Op' to root element of the ReceiptAcknowledgment RosettaNet schema.

受領操作の入力は、RosettaNetで定義したReceiptAcknowledgmentスキーマである。操作名は、ReceiptAcknowledgment(受信確認)にRosettaNetスキーマのルートエレメントに「Op」を追加することによって作成される。

例 Example

```
< wsdl:operation name="ReceiptAcknowledgmentOp">
< wsdl:input message="tns: ReceiptAcknowledgmentMsg" />
</wsdl:operation>
```

4.2.2 信号操作の特徴 (Signature of Signal Operations)

Signal Operations is used to refer to following two operations: ReceiptAcknowledgmentOp, and ExceptionOp.

信号操作は、次の2つの操作を参照するのに使用される。ReceiptAcknowledgmentOp(受信確認操作)と ExceptionOp(例外処理操作)である。

R1013 'ReceiptAcknowledgmentOp' MUST have ONLY 'ReceiptAcknowledgmentMsg' as the input.

R1013 'ReceiptAcknowledgmentOp' (受信確認操作)は、入力として'ReceiptAcknowledgmentMsg' (受信確認メッセージ)のみを有すること。(MUST)

例 Example

```
<wsdl:operation name="ReceiptAcknowledgmentOp">
<wsdl:input message="tns:ReceiptAcknowledgmentMsg" />
</wsdl:operation>
```

R1014 ExceptionOp MUST have only 'ExceptionMsg' as the input.

R1014 ExceptionOp(例外処理操作)は、入力として'ExceptionMsg' (例外処理メッセージ)のみを有すること。(MUST)

例 Example

```
<wsdl:operation name="ExceptionOp">
<wsdl:input message="tns:ExceptionMsg" />
</wsdl:operation>
```

理論的根拠 Rationale

In Service to Service One Way Callback MEP errors must be communicated asynchronously using the Exception schema. Therefore, an operation (ExceptionOp) is defined to receive the exceptionMsg.

サービス・ツー・サービスの一方向コールバック・メッセージ交換パターンでは、エラーは例外処理スキーマを使用して、非同期的に通信されなければならない。従って、ExceptionOp(例外処理操作)操作は、exceptionMsg(例外処理メッセージ)を受領するように定義される。

4.2.3 メッセージ交換パターンのマッピングに必要な操作 (Operations Required for Mapping Message Exchange Patterns)

The WSDL operations and parameters vary with each MEP. In general, each PIP Activity maps to an operation and each PIP Action maps to a WSDL message.

WSDL操作及びパラメータは、それぞれのメッセージ交換パターン(MEP)ごとに異なる。一般的に、各PIPアクティビティが操作に対して、各PIPアクションがWSDLメッセージに対してマッピングされる。

Following table summarizes operations required for each MEP. Rules for this mapping are also detailed below.

次表に、それぞれのメッセージ交換パターン(MEP)のために必要な操作を要約する。このマッピングについてのルールも以下に詳説する。

As an example, first row of the table should be read as follows. Service to Service One Way Callback MEP involves two services - invoked service (e.g. Buyer service) and initiating service (e.g. Seller service). Invoked service provides a single operation "RequestRootElementNameOp" (e.g. PurchaseOrderStatusNotificationOp) with a single input "PurchaseOrderStatusNotificationMsg". Initiating service provides two operations: ReceiptAcknowledgmentOp, and ExceptionOp. ReceiptAcknowledgmentOp has a single input "ReceiptAcknowledgmentMsg". ExceptionOp operation has a single input "ExceptionMsg".

例として、表の第1行は以下の様に読むべきである。サービス・ツー・サービスの一方向コールバック・メッセージ交換パターン(MEP)には、2つのサービスが含まれる。呼び出されるサービス(例:バイヤー・サービス)及び起動されるサービス(例:セラー・サービス)である。呼び出されるサービスは、単一入力の "PurchaseOrderStatusNotificationMsg(発注状況通知メッセージ)"を持つ単一操作の "RequestRootElementNameOp(要求ルート要素名操作)"(例:PurchaseOrderStatusNotificationOp(発注状況通知操作))を提供する。起動サービスは2つの操作を提供する。ReceiptAcknowledgmentOp(受信確認操作)とExceptionOp(例外処理操作)である。ReceiptAcknowledgmentOp(受信確認操作)には単一入力の "ReceiptAcknowledgmentMsg(受信確認メッセージ)"が、ExceptionOp(例外処理操作)には単一入力の "ExceptionMsg(例外処理メッセージ)"がある。

Message Exchange Pattern	PIPNumber Role	Operation Convention	Example	Message [RootElementNameMsg]
Service to Service One Way Callback	PIP3A7 Buyer [Invoked Service] PIP3A7 Seller [Initiating Service]	RequestRootElementNameOp ReceiptAcknowledgmentOp ExceptionOp	PIP3A7 Buyer PurchaseOrderStatusNotificationOp PIP3A7 Seller ReceiptAcknowledgmentOp ExceptionOp	PurchaseOrderStatusNotificationOp input:PurchaseOrderStatusNotificationMsg ReceiptAcknowledgmentOp input:ReceiptAcknowledgmentMsg ExceptionOp input:ExceptionMsg
Pure client to service request response	PIP2A2 Seller [Invoked Service]	RequestRootElementNameAndResponseRootElementNameOp	PIP2A2 Seller ProductInformationQueryAndSalesCatalogOp	ProductInformationQueryAndSalesCatalogOp input:ProductInformationQuerymsg output:SalesCatalogMsg fault:ExceptionMsg
Pure client to service request response pull	PIP3A4 Buyer [Invoked Service]	QueryCriterionAndRootElementNameOp	PIP3A4 Buyer QueryCriterionAndPurchaseOrderRequestOp ReceiptAcknowledgmentOp (Optional)	QueryCriterionAndPurchaseOrderRequestOp input:QueryCriterionMsg (Schema based) output:PurchaseOrderRequestMsg fault:ExceptionMsg ReceiptAcknowledgmentOp (Optional) input: ReceiptAcknowledgmentMsg
pure client to service request response push	PIP3A4 Seller [Invoked Service] PIP3A4 Buyer [Initiating Service]	RequestRootElementNameAndReceiptAcknowledgmentOp	PIP3A4Seller PurchaseOrderRequestAndReceiptAcknowledgmentOp PIP3A4Buyer PurchaseOrderConfirmationAndReceiptAcknowledgmentOp	PurchaseOrderRequestAndReceiptAcknowledgmentOp input:PurchaseOrderRequestMsg output:ReceiptAcknowledgmentMsg fault:ExceptionMsg PurchaseOrderConfirmationAndReceiptAcknowledgmentOp input: PurchaseOrderConfirmationMsg output: ReceiptAcknowledgmentMsg fault:ExceptionMsg

4.2.3.1 サービス・ツー・サービスの一方向コールバック (Service to Service One Way Callback)

4.2.3.1.1 呼び出されるサービス (Invoked Service)

R1015 For Service to Service One Way Callback scenario, invoked service MUST define at least one business operation.

R1015 サービス・ツー・サービスの一方向コールバック・シナリオでは、呼び出されるサービスは少なくとも、1つのビジネス操作を定義しなければならない。(MUST)

例 Example

In following example 'PurchaseOrderStatusNotificationOp' operation is defined.

次の例では、'PurchaseOrderStatusNotificationOp'(発注状況通知操作)操作が定義される。

<wsdl:operation name="PurchaseOrderStatusNotificationOp">

R1016 The operation MUST have exactly one input.

R1016 操作には確実に1つの入力がないといけない。(MUST)

例 Example

<wsdl:input message="tns:PurchaseOrderStatusNotificationMsg" />

R1017 The input MUST be a WSDL message that refers to RosettaNet business message.

R1017 入力は、RosettaNetビジネス・メッセージを参照するWSDLメッセージでなければならない。(MUST)

例 Example

The input refers to RosettaNet 'PurchaseOrderStatusNotification' business message.

入力は、RosettaNetビジネス・メッセージの'PurchaseOrderStatusNotification' (発注状況通知)を参照する。

<wsdl:input message="tns:PurchaseOrderStatusNotificationMsg" />

4.2.3.1.2 起動するサービス (Initiating Service)

R1018 For Service to Service One Way Callback scenario, initiating service MUST define a 'ReceiptAcknowledgmentOp' operation.

R1018 サービス・ツー・サービスの一方向のコールバック・シナリオには、起動するサービスは'ReceiptAcknowledgmentOp' (受信確認操作)操作を定義しなければならない。(MUST)

例 Example

<wsdl:operation name="ReceiptAcknowledgmentOp">

R1019 For Service to Service One Way Callback scenario, initiating service MUST define an 'ExceptionOp' operation.

R1019 サービス・ツー・サービスの一方向のコールバックのシナリオでは、起動するサービスは'ExceptionOp' (例外処理操作)操作を定義しなければならない。(MUST)

例 Example

<wsdl:operation name="ExceptionOp">

4.2.3.2 ピュア・クライアント・ツー・サービスへの要求応答 (Pure client to service request response)

4.2.3.2.1 呼び出されるサービス (Invoked Service)

R1020 For Pure client to service request response MEP, invoked service MUST define at least one business operation.

R1020 ピュア・クライアント・ツー・サービス要求応答メッセージ交換パターン(MEP)では、呼び出されるサービスは少なくとも1つのビジネス操作を定義しなければならない。(MUST)

R1021 The operation MUST have a RosettaNet Business Message as the input, a

RosettaNet Business Message as the output, and an ExceptionMsg as the fault.

R1021 操作には、入力としてのRosettaNetビジネス・メッセージ、出力としてのRosettaNetビジネス・メッセージ及びエラー用としての'ExceptionMsg' (例外処理メッセージ)が必要である。(MUST)

例 Example

```
<wsdl:operation name="ProductInformationQueryAndSalesCatalogOp">
<wsdl:input message="tns:ProductInformationQuerymsg" />
<wsdl:output message="tns:SalesCatalogMsg" />
<wsdl:fault message="tns:ExceptionMsg" />
</wsdl:operation>
```

4.2.3.3 プル型ピュア・クライアント・ツー・サービス要求 / 応答 (Pure client to service request response pull)

4.2.3.3.1 呼び出されるサービス (Invoked Service)

R1022 For Pure client to service request response pull MEP, invoked service MUST define at least one business operation.

R1022 プル型ピュア・クライアント・ツー・サービス要求 / 応答メッセージ交換パターン(MEP)では、呼び出されるサービスは少なくとも1つのビジネス操作を定義しなければならない。(MUST)

R1023 First operation MUST have a QueryCriterionMsg as the input, RosettaNet Business Message as the output, and an ExceptionMsg as the fault.

R1023 最初の操作は、入力としての'Query CriterionMsg' (問い合わせ標準メッセージ)を、出力としてのRosettaNetビジネス・メッセージ、及びエラー用として'ExceptionMsg' (例外処理メッセージ)を持たなくてはならない。(MUST)

例 Example

```
<wsdl:operation name="QueryCriterionAndPurchaseOrderRequestOp">
<wsdl:input = "QueryCriterionMsg"/>
<wsdl:output = "PurchaseOrderRequestMsg"/>
<wsdl:fault = "ExceptionMsg"/>
</wsdl:operation>
```

R1024 The single part of the QueryCriterionMsg MAY refer to the RosettaNet Business Message specific Query Criterion XSD.

R1024 QueryCriterionMsg (問い合わせ標準メッセージ)の単一部分には、RosettaNetビジネス・メッセージ固有のQuery Criterion XSD(問い合わせ標準XSD)を参照することが許されるだろう。(MAY)

The RosettaNet Business Message specific Query Criterion XSD is created by changing the template schema 'WS_GetMessage' XML Schema Namespace to the response PIP schema namespace and prefix the PIP root element name found in the namespace with "WS_Get".

問合せ用のRosettaNetビジネス・メッセージの標準XMLスキーマは、テンプレート・スキーマである'WS_GetMessage'のXMLスキーマのネームスペースを応答PIPスキーマのネームスペースに変更し、ネームスペース中のPIPルート要素名の先頭に"WS_Get"をつけて作成される。

理論的根拠 Rationale

The template schema 'WS_GetMessage' has a single element and provides a standard way to request a message from the invoked service without any search criterion. This template schema has to be modified to be based on the RosettaNet Business Message queried. For example, a Pure Client to Service Request Response Pull WSDL appears as the following for a Community PIP 3A4 Purchase Order Request.

テンプレート・スキーマ「WS_GetMessage」は単一の要素を持ち、呼び出されるサービスから検索ルールなしでメッセージを要求する標準的な方法を提供する。このテンプレート・スキーマは、照会された RosettaNet ビジネス・メッセージに基づくように修正しなければならない。例えば、プル型ピュア・クライアント・ツー・サービス要求 / 応答の WSDL は、標準 PIP 3A4 の発注依頼の場合下記のようになる。

```
<wsdl:message name="QueryCriterionMsg">
  <wsdl:part name="QueryCriterionPart" element="c:GetMessage"/>
</wsdl:message>

<wsdl:types>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">

<xsd:import
  namespace="urn:rosettanet:specification:interchange:WS_GetPurchaseOrderRequest:
  xsd:schema:01.00" schemaLocation="..." />

</xsd:schema>

</wsdl:types>
```

R1025 The single part of the QueryCriterionMsg MAY refer to a schema agreed upon within the TPA.

R1025 QueryCriterionMsg(問い合わせ標準メッセージ)の単一部分は、TPA(取引者間契約)で合意済みのスキーマを参照することが許される**だろう**。(MAY)

理論的根拠 Rationale

This provides the business partners the ability to request a message from the invoked service based on a search criterion.

これは、検索ルールに基づいて呼び出されるサービスからメッセージを要求する能力を、取引先に提供する。

R1026 If business partner specific criterion is used, RosettaNet Business Message specific Query Criterion XSD using the template RosettaNet WS_GetMessage schema MUST be replaced with business partner schema.

R1026 取引先固有の基準が使用される場合、RosettaNet WS_GetMessageスキーマ テンプレートを使用した問合せ用のRosettaNetビジネス・メッセージの標準XMLスキーマは、取引先スキーマに置き換えなければならない。(MUST)

R1027 For Pure client to service request response pull MEP, invoked service MAY define a ReceiptAcknowledgmentOp operation.

R1027 プル型ピュア・クライアント・ツー・サービス要求 / 応答メッセージ交換パターン(MEP)では、呼び出されるサービスは 'ReceiptAcknowledgmentOp' (受信確認操作)操作を定義する**であろう**。(MAY)

理論的根拠 Rationale

For Pure client to service request response pull MEP, ReceiptAcknowledgment operation is optional since all business interactions may not require non- repudiation of receipt.

プル型ピュア・クライアント・ツー・サービス要求 / 応答メッセージ交換パターン (MEP) では、全ての業務やり取りが受信の否認防止を必要とするわけではないので、'ReceiptAcknowledgment' (受信確認操作) 操作はオプションである。

例 Example

```
<wsdl:operation name="ReceiptAcknowledgmentOp">
```

4.2.3.4 プッシュ型ピュア・クライアント・ツー・サービス要求応答 (Pure client to service request response push)

4.2.3.4.1 呼び出されるサービス (Invoked Service)

R1028 For Pure client to service request response push MEP, invoked service MUST define at least one business operation.

R1028 プッシュ型ピュア・クライアント・ツー・サービス要求応答メッセージ交換パターン (MEP) では、呼び出されるサービスは少なくとも1つのビジネス操作を定義しなければならない。(MUST)

R1029 The operation MUST have a RosettaNet Business Message as the input, ReceiptAcknowledgmentMsg as the output, and an ExceptionMsg as the fault.

R1029 操作は、入力としてRosettaNetビジネス・メッセージ、出力としてReceiptAcknowledgmentMsg (受信確認メッセージ)、及びエラー用としての'ExceptionMsg' (例外処理メッセージ) を持たなければならない。(MUST)

例 Example

```
<wsdl:operation name="PurchaseOrderRequestAndReceiptAcknowledgmentOp">
```

```
<wsdl:input message="tns:PurchaseOrderRequestMsg" />
```

```
<wsdl:output message="tns:ReceiptAcknowledgmentMsg" />
```

```
<wsdl:fault message="tns:ExceptionMsg" />
```

```
</wsdl:operation>
```

4.3 連携方法 (Binding)

Expect that both SOAP 1.1 and SOAP 1.2 will co-exist for the near future. This Profile supports either SOAP 1.1 or SOAP 1.2. It is up to the business partner's agreement on which version should be used.

しばらくの間は、SOAP 1.1とSOAP 1.2の両方が共存するだろう。本プロファイルは、SOAP 1.1かSOAP 1.2のどちらでもサポートする。どちらのバージョンを使用するかについては、取引先の合意次第である。

When SOAP 1.1 is in use, this section of the Profile incorporates the following specifications by reference:

SOAP 1.1が使用される場合、本プロファイルのこのセクションは、参照により以下の仕様を組み込む：

- [Simple Object Access Protocol \(SOAP\) 1.1 W3C Note 08 May 2000](http://www.w3.org/TR/2000/NOTE-SOAP-20000508/)

As constrained by the following WS-I profiles:

以下のWS-Iプロファイルによって制約される:

- WS-I Simple SOAP Binding Profile 1.0 WS-I Final Material 24 August 2004
<http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html>
- WS-I Attachment Profile 1.1 WS-I Final Material 10 April 2005
<http://www.ws-i.org/Profiles/BasicProfile-1.1.html>

When SOAP 1.2 is used, this section of the Profile incorporates the following specifications by reference:

SOAP 1.2が使用される場合、本プロファイルプロファイルのこのセクションは、参照により以下の仕様を組み込む:

- SOAP Version 1.2 Part1: Messaging Framework W3C Recommendation 24 June 2003
<http://www.w3.org/TR/2003/REC-soap12-part1-20030624/>
- SOAP Version 1.2 Part2: Adjuncts
W3C Recommendation 24 June 2003
<http://www.w3.org/TR/2003/REC-soap12-part2-20030624/>
- SOAP Message Transmission Optimization Mechanism W3C Recommendation 25 January 2005 <http://www.w3.org/TR/soap12-mtom/>

4.3.1 デフォルト連携 (Default binding)

R1030 A RosettaNet Web service MUST support at least SOAP over HTTP binding.
R1030 RosettaNet Webサービスは、少なくともSOAP/HTTPをサポートしなければならない。(MUST)

When no binding is provided for a portType, SOAP over HTTP is the default binding.
portTypeについて何の連携も提供されない場合、SOAP/HTTPがデフォルトの連携方法である。

4.3.2 MIMEパッケージングと添付のサポート (MIME binding & Attachments support)

Supporting attachments is a vital requirement in B2B business messaging. Today, Web services users use MTOM or WS-I AP1.0 as two options to support attachments. However a clear industry choice has not emerged and this specification would therefore allow the choice of either of them as per a Trading Partner Agreement (TPA) between the two business partners.

添付のサポートは、B2Bビジネス・メッセージにおける重要な要件である。今日では、Webサービス・ユーザは添付をサポートする2つのオプションとして、MTOM、又はWS-I AP1.0を使用している。しかしながら、業界での選択は未だ明確ではないため、本仕様では取引先二者間のTPA(取引者間契約)に従って、どちらの選択も許可するものである。

R1031 The attachments mechanism SHOULD be agreed upon in the TPA, it can be either MTOM or WS-I AP1.0.

R1031 添付(attachments)メカニズムはTPA(取引者間契約)にて合意すべきであり、MTOMあるいはWS-I AP1.0のいずれかである。(SHOULD)

4.3.3 圧縮のサポート (Compression support)

Since Web services does not provide a standard way for message compression, this specification does not endorse any particular compression technology. Business partners may choose to use specialized extensions that support compression. Compression is outside the scope of this specification.

Webサービスは、メッセージの圧縮に関する標準的方法を提供しないので、本仕様では特定の圧縮技術を推奨しない。取引先は、圧縮をサポートする専用の拡張機能を使用することを選択してよい。圧縮に関しては、本仕様の対象外である。

4.4 グルーピング操作に関するガイドライン (Guidelines for grouping operations)

This section provides guidelines on how to group operations into different interfaces. These guidelines are considered optional by this Profile. 本セクションは様々なインターフェースに操作をグルーピングする方法に関するガイドラインを提供する。これらの指針は、当プロファイルのオプションであるとする。

Even though a consistent operation grouping mechanism followed by all implementers would be ideal, we recognize that each implementer may have different architectural constraints for interface definitions, and the impact of operation grouping on wire-level interoperability is not as significant as message definitions. Implementers have the freedom to choose their preferred approach for operation grouping and interface definitions as long as they follow WSDL 1.1 specification and WS-I interoperability requirements.

全ての実装者が従う一貫性のあるグルーピング操作の仕組みが理想的ではあるけれど、それぞれの実装者がインターフェース定義について様々なアーキテクチャ上の制約を有するかもしれないし、通信レベルの相互運用性に関するグルーピング操作の影響は、メッセージ定義ほどは重要でないと私達は認識している。実装者は、グルーピング操作、及びインターフェース定義について、それがWSDL 1.1仕様及びWS-I 相互運用性要件に従っている限りは、自分達が好ましいと思う方法を選ぶ自由がある。

The keyword “MUST” used in this section is only applicable to RosettaNet community WSDLs. Of course, for those companies that choose to follow these guidelines, they may further restrict the profile by making the guidelines mandatory. 当セクションで用いているキーワード“MUST”は、RosettaNet標準WSDLに対してのみ適用される。勿論、これらのガイドラインに従うことを選択した会社では、ガイドラインを強制にすることにより、さらにプロファイルを制限してもかまわない。

The following guidelines apply to all MEPs for a “Single Action Business Interaction” and the “pure client to service request response” MEP for a “Dual Action Business Interaction”. Grouping of operations for “Multiple Action Business Interactions” is not addressed, except the Dual Action scenario noted above.

次のガイドラインは、‘1アクションの業務やり取り’のための全てのメッセージ交換パターン(MEP)及び‘2アクションの業務やり取り’のためのピュア・クライアント・ツー・サービス要求応答メッセージ交換パターン(MEP)に当てはまる。‘複数アクションの業務やり取り’のためのグルーピング操作は、上記の2アクション・シナリオ以外は取り組まない。

portType name Mapping is out of scope. Implementer should choose appropriate portType name (e.g. use Role Type as portType name). portType名のマッピングに関しては、本仕様の対象外である。実装者は適切なportType名(例: portType名として、Role Typeを使用)を選ぶべきである。

4.4.1 ガイドライン (Guidelines)

G0001 A portType MUST NOT mix operations from different Role Types.
G0001 portTypeは、異なるRole Typeからの操作を混在させてはならない。(MUST NOT)

理論的根拠 Rationale

Business functions in a Single Action Business Interaction are performed by two business partners with two different Role Types (e.g. Sold to, and Sold by). In Web services, the Business Interaction is typically represented as operations of two types - business

operations and signal operations. portType is used to group the operations.

1アクションの業務やり取りにおける業務機能は、2つの異なるRole Types(例えば、販売する人と購買する人)を持った2つの取引先によって行なわれる。Webサービスでは、業務のやり取りは典型的には2つのタイプの操作として表わされる - ビジネス操作と信号操作。portTypeは操作をグループ化するために使用される。

Each participant that supports service hosting should provide a portType that groups the operations performed by the participant. This ensures that each participant has a clear understanding about what operations it must provide based on its own role type. Even for a business partner that may support multiple roles with different business partners, it is considered a best practice to provide a separate portType for each role.

サービス・ホスティングをサポートする各当事者は、当事者が実行する操作をグループ化するportTypeを提供すべきである。これは各当事者が各自役割タイプに基づいて、どんな操作を提供しなければならないかについての明確な理解を得ることを保証する。異なる取引先と多面にわたる役割をサポートする可能性がある取引先にとっても、各役割に対して別々のportTypeを提供することが最善と考えられる。

例 Example

Business Interaction: Distribute Order Status

MEP: Service to Service One Way Callback

“Sold to” Role Type Operation: *PurchaseOrderStatusNotificationOp*

“Sold by” Role Type Operations: *ReceiptAcknowledgmentOp*, and *ExceptionOp*

ReceiptAcknowledgmentOp, and *ExceptionOp* operations should not be in same port as *PurchaseOrderStatusNotificationOp* because they are associated to different Role Types.

受信確認操作 (*ReceiptAcknowledgmentOp*) 及び例外処理操作 (*ExceptionOp* operations) は、発注状況通知操作 (*PurchaseOrderStatusNotificationOp*) とは異なるRole Typeに関連付けられるものなので、同じポートであるべきでない。

portType A provided by “Sold to” Role Type:

“Sold to” Role Typeにより提供されたportType A:

```
<wsdl:portType name="A">
```

```
<wsdl:operation name=" PurchaseOrderStatusNotificationOp ">
```

.....

```
</wsdl:portType>
```

portType B provided by “Sold by” Role Type:

“Sold by” Role Typeにより提供されたportType B:

```
<wsdl:portType name="B">
```

```
<wsdl:operation name="ReceiptAcknowledgmentOp">
```

.....

```
<wsdl:operation name="ExceptionOp ">
```

.....

</wsdl:portType>

G0002 A portType SHOULD contain ALL and ONLY operations of a single MEP, for a Role Type.

G0002 portTypeは、ひとつのRole Typeについて単一のMEP(メッセージ交換パターン)の「全て」かつ「唯一」の操作を含むべきである。(SHOULD)

理論的根拠 Rationale

It is important that each participant has a clear understanding about what operations it must provide based on the MEP. If operations of a MEP are not grouped in the same portType, it will not be clear to a participant which operations should be implemented to support a MEP. If operations of different MEPs are mixed in the same portType, it will not be clear to a participant which subset of the operations should be implemented to support a MEP.

各当事者は、メッセージ交換パターン(MEP)に基づいて、どんな操作を提供しなければならないかについての明確な理解を得ることが重要である。メッセージ交換パターンの操作が同一portType内でグループ化されない場合、当事者にとってメッセージ交換パターンをサポートするために、どの操作を行うべきかは明らかではないだろう。異なるメッセージ交換パターンの操作が同一portType内で混在する場合、当事者にとってメッセージ交換パターンをサポートするために、どの操作サブセットが実施されるべきであるかは明らかではないだろう。

Example for a portType to contain ALL operations of a single MEP, for a Role Type

ひとつの役割タイプに対して、単一メッセージ交換パターン(MEP)の操作「すべて」を持つportTypeの例

Business Interaction: Distribute Order Status

MEP: Service to Service One Way Callback

“Sold to” Role Type Operation: *PurchaseOrderStatusNotificationOp*

“Sold by” Role Type Operations: *ReceiptAcknowledgmentOp*, and *ExceptionOp*

PurchaseOrderStatusNotificationOp must be in a single portType provided by the “Sold to” party.

発注状況通知操作 (*PurchaseOrderStatusNotificationOp*) は“Sold to”グループにより提供される単一portType内になければならない。

ReceiptAcknowledgmentOp, and *ExceptionOp* must be in a single portType provided by the “Sold by” party.

受信確認操作 (*ReceiptAcknowledgmentOp*) 及び例外処理操作 (*ExceptionOp*) は“Sold by”グループにより提供される単一のportType内になければならない。

portType A provided by “Sold to” party:

“Sold to”グループにより提供されたportType A:

```
<wsdl:portType name="A">
```

```
<wsdl:operation name="PurchaseOrderStatusNotificationOp">
```

```
.....
```

```
</wsdl:portType>
```

portType B provided by “Sold by” party:

“Sold by”グループにより提供されたportType B:

```
< wsdl:portType name= "B">  
< wsdl:operation name= "ReceiptAcknowledgmentOp">  
.....  
< wsdl:operation name= "ExceptionOp ">  
.....  
</wsdl:portType>
```

Example for a portType to ONLY contain operations of a single MEP, for a Role Type.
ひとつの役割タイプに対して、単一メッセージ交換パターン (MEP) 操作のみを持つportTypeの例

Business Interaction: Distribute Order Status

MEP1: Service to Service One Way Callback MEP

"Sold to" Role Type Operation: PurchaseOrderStatusNotificationOp

"Sold by" Role Type Operations: ReceiptAcknowledgmentOp, and ExceptionOp

MEP2: Pure client to service request response pull

"Sold to" Role Type Operation: None

"Sold by" Role Type Operations: PullPurchaseOrderStatusOp

If the Seller (Sold by) groups *ReceiptAcknowledgmentOp*, *ExceptionOp* from *MEP1*, and *PullPurchaseOrderStatusOp* from *MEP2* in a single portType, then a "Sold to" participant is interested in only *MEP1* (e.g. Service to Service One Way Callback MEP) will not know which subset of the operations (from the combined portType) should be implemented. もし、販売者(Sold by)がメッセージ交換パターン1 (MEP1)からの受信確認操作(AcknowledgmentOp)、例外処理操作(ExceptionOp)、そしてメッセージ交換パターン2 (MEP2)からの発注状況操作プル (PullPurchaseOrderStatusOp)を単一portType内でグルーピングすれば、そこでメッセージ交換パターン1 (例えば、サービス・ツー・サービスの1方向のコールバック・メッセージ交換パターン)のみに興味がある購入者(Sold to)は、どの部分操作(結合されたportTypeの内)が実装されるべきであるかを分らないだろう。

Following is NOT correct since operations from Service to Service One Way Callback MEP, and Pure client to service request response pull are contained in same portType. サービス・ツー・サービスの1方向のコールバックメッセージ交換パターン(MEP)と、プル型ピュア・クライアント・ツー・サービス要求 / 応答は、同一portTypeに含まれるので、以下は正しくない。

portType provided by "Sold by" party:

"Sold by"グループから提供されたportType:

```
< wsdl:portType name= "B">  
< wsdl:operation name= "ReceiptAcknowledgmentOp">  
.....  
< wsdl:operation name= "ExceptionOp ">
```

.....

```
<wsdl:operation name=" PurchaseOrderStatusNotificationOp ">
```

.....

```
</wsdl:portType>
```

G0003 Following URN Scheme SHOULD be used for the target namespace (of the community WSDL). Alphanumeric text MAY BE indicative of the business interaction(s).

G0003 標準WSDLのターゲット・ネームスペースに対し、以下のURNスキームを使用すべきである。
(SHOULD) 英数字テキストは業務上のやり取りを表わせるであろう。(MAY)

Structure:urn:rosettanet:specification:interchange:Alphanumeric Text:xml:wsdl:1.0

理論的根拠 Rationale

“Alphanumeric text” ensures that the WSDL is not restricted to a single action, and provides flexibility to the group operations related to “*Multiple Action Business Interactions*” in a single WSDL. Note, the above guidelines are intended to be used for community WSDLs created by RosettaNet.

“英数字テキスト”は、WSDLが単一アクションに制限されず、単一WSDL中の“多重アクション業務やり取り”と関係するグループ操作に自由度を与えることを保証する。

注)上記のガイドラインは、ロゼッタネットによって作成される標準WSDLのために使用されることを意図したものであることに注意してください。

例 Example

targetNamespace=urn:rosettanet:specification:interchange:3A:xml:wsdl:1.0

targetNamespace=urn:rosettanet:specification:interchange:3A4:xml:wsdl:1.0

targetNamespace=urn:rosettanet:specification:interchange:PurchaseOrderRequest:xml:wsdl:1.0

targetNamespace=urn:rosettanet:specification:interchange:Procurement:xml:wsdl:1.0

5 サービスの品質 (Quality of Services)

This section of the profile incorporates the following specifications by reference:
プロファイルの本セクションは、参照により以下の仕様を組み込む:

- Web Services Reliable Messaging Protocol Submission version to OASIS WS-RX TC, February 2005 <http://specs.xmlsoap.org/ws/2005/02/rm/ws-reliablemessaging.pdf>
- Web Services Reliable Messaging Policy Assertion Submission version to OASIS WS-RX TC, February 2005
<ftp://www6.software.ibm.com/software/developer/library/ws-rmpolicy200502.pdf>
- Web Services Security: SOAP Message Security 1.1 OASIS Standard Specification, 1 February 2006 <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>
- Web Services Security Username Token Profile 1.1 OASIS Standard Specification, 1 February 2006 <http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf>
- Web Services Security X.509 Token Profile 1.1 OASIS Standard Specification, 1 February 2006 <http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf>
- Web Services Security SOAP with Attachment (SwA) Profile 1.1 OASIS Standard Specification, 1 February 2006 <http://www.oasis-open.org/committees/download.php/16672/wss-v1.1-spec-os-SwAProfile.pdf>
- Web Services Addressing 1.0 – Core W3C Recommendation 9 May 2006
<http://www.w3.org/TR/ws-addr-core/>
- Web Services Addressing 1.0 – SOAP Binding W3C Recommendation 9 May 2006
<http://www.w3.org/TR/ws-addr-soap/>
- Web Services Security Policy Language Submission Version to OASIS WS-SX TC, version 1.1 July 2005
<http://specs.xmlsoap.org/ws/2005/07/securitypolicy/ws-securitypolicy.pdf>

Further, increased interoperability, the following profiles are incorporated by reference:
さらに、相互運用性を増すために、次のプロファイルが参照によって組み込まれる:

- WS-I Basic Profile 1.1 WS-I Final Material 10 April 2005
<http://www.ws-i.org/Profiles/BasicProfile-1.1.html>
- WS-I Basic Security Profile 1.0 WS-I Working Group Draft 29 March 2006
<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>

5.1 QoS の設計ポイント (QoS Design Points)

The Web services infrastructure is payload-agnostic. However, any given set of (business) content, in this case RosettaNet PIPs, may present difficulties/mismatches when considering the content design with any given infrastructure design, such as the web services infrastructure. The design of the content may contain features which may be leveraged when using a given infrastructure.
Webサービス・インフラは、ペイロード(データ本体)にとらわれない。しかしながら、Webサービス・インフラの様な与えられたインフラ設計を使ってコンテンツ設計を考える場合、いかなる1組の(ビジネス)コンテ

ソツ集合(この場合RosettaNet PIP)にも、困難、又は不適合が生じる可能性がある。コンテンツ設計には、与えられたインフラを使用する場合に活用できる機能を含んでいるかもしれない。

This section is organized consistently with the message exchange patterns defined within this profile. The primary intention of this section focuses upon the service quality considerations primarily with wire formats and configurations identifying what Web services QoS aspects are relevant and applicable in context to the defined patterns. 本セクションは当プロファイル内で定義されたメッセージ交換パターンと矛盾なく構成される。本セクションの第一の意図は、通信フォーマット及び機器構成を考慮したサービス品質に注目することであり、定義されたパターンを考慮して、WebサービスのどのQoS(サービス品質)側面が該当し、そして適用可能であるかを特定する。

This profile's scope is constrained to primarily focus on the foundational information message exchanges of RosettaNet Business Messages over Web services, with the intention to be built upon or extended into the space of orchestration of services and formal process flow. The QoS section refrains from specifying aspects outside the scope of this profile. However, in order to provide an increased precision in detail concerning the QoS aspects, this section expresses examples and diagrams needed to establish a comprehensive technical understanding of the abilities and ramifications of the intended information mappings while leveraging the relevant QoS aspects in context of the sometimes substantially varying patterns identified.

当プロファイルの範囲は、主としてWebサービス上のRosettaNetビジネス・メッセージの基本情報メッセージ交換に焦点を当てることを強要される。それと共に、サービスのオーケストレーション領域及び正式なプロセス・フロー上に構築される、あるいはそこへ拡張されることを意図する。QoSセクションでは、当プロファイルの範囲外の側面を定めることは控える。しかし、QoS側面に関する詳細をより正確にするために、本セクションは目的の情報マッピングの能力及び効果の総合的な技術的理解を得るために必要な例と図を示す。一方、時には定義されたパターンが大幅に変わることを考慮した適切なQoS側面を利用する。

5.2 共通QoS (Common QoS)

This section addresses Web services QoS aspects which are common across all patterns. 本セクションは全てのパターンに共通するWebサービスのサービス品質(QoS)の面について取り上げる。

5.2.1 共通セキュリティ・ポリシーの使用法 (Common Security Policy Usage)

WS-SecurityPolicy specification defines a set of assertions relevant to security features in SOAP Message Security, WS-Trust, and WS-SecureConversation. WS-SecurityPolicy is, by definition, a "building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of security models".

WS-SecurityPolicy仕様では、SOAPメッセージ・セキュリティ、WS-Trust、WS-SecureConversationにおけるセキュリティ機能に関する一連の主張を定めている。WS-SecurityPolicyは、定義によれば、「多種多様なセキュリティモデルに対応するために、他のWebサービス及びアプリケーション特有のプロトコルと共に用いられる構成要素」です。

In practice, this means the possible combinations of the features of the security policy language is significant. This profile, while recognizing the emerging state of the WS-SecurityPolicy specification, provides recommendations, considerations, and constraints in specific areas concerning WS-SecurityPolicy.

實際上、これはセキュリティ・ポリシー言語の機能の可能な組み合わせが重要であることを意味する。当プロファイルは、WS-SecurityPolicy仕様の新しい状況を認識しつつ、WS-セキュリティ・ポリシーに関する特定の領域における推奨事項、考慮事項及び制約を提示する。

This profile requires the existence of a WS-SecurityPolicy assertion to specify security requirements for RosettaNet services and the expected wire-level representation at runtime.

当プロファイルは、RosettaNet サービス及び予期されるプログラム実行時の通信上の表現に関するセキュリティ要件を特定するために、WS-SecurityPolicy のアサーションを必要とする。

R2001 WS-SecurityPolicy document MUST be supported in alignment with the restrictions defined in this profile for defining security QoS for RosettaNet services.

R2001 WS-セキュリティ・ポリシー文書は、本プロファイルで RosettaNet サービス用のセキュリティ QoS を定義するために定義された制約事項に沿って、サポートされなければならない。(MUST)

R2002 Attachment of WS-SecurityPolicy assertions to WSDL MAY be supported.

R2002 WSDL 向け WS-セキュリティ・ポリシー・アサーションの付属文書がサポートされるであろう。(MAY)

R2003 Attachment of WS-SecurityPolicy assertions to WSDL MUST utilize WS-PolicyAttachment.

R2003 WSDL 向け WS-セキュリティ・ポリシー・アサーションの付属文書は、WS-PolicyAttachment を利用しなければならない。(MUST)

R2004 The expected wire representation of the WS-SecurityPolicy assertions MUST be supported.

R2004 WS-セキュリティ・ポリシー・アサーションの予期される通信上の表現が、サポートされなければならない。(MUST)

5.2.1.1 セキュアな連携方法の利用 (Use of Bindings)

WS-SecurityPolicy section 3 defines 3 "bindings" which represent patterns based on the individual security assertions, as a first order of reduction in assertion combinations. For simplicity in context of the defined use cases, this profile prohibits the use of the sp:SymmetricBinding.

WS-セキュリティ・ポリシーセクション3は、アサーションの組み合わせを減らすことを優先し、個々のセキュリティ・アサーションに基づくパターンを表す3つの「セキュアな連携方法を定義している。定義されるユースケースを考慮して単純化するため、本プロファイルはsp:SymmetricBinding (対称型アルゴリズムを用いた暗号化によるセキュアな連携)の使用を禁止する。

R2005 – Bindings within security policies MUST be either sp:TransportBinding or sp:AsymmetricBinding.

R2005 - セキュリティ・ポリシーのうち使用できるセキュアな連携方法は、sp:TransportBinding(通信におけるセキュアな連携方法)、又は、sp:AsymmetricBinding (非対称型アルゴリズムを用いた暗号化によるセキュアな連携非対称な性結合)のいずれかでなければならない。(MUST)

For simplicity and consistency, this profile requires the use of the widely implemented RSA-1_5 encryption algorithm for use in transport bindings. In WS-SecurityPolicy, this algorithm is included in the sp:TripleDesRsa15 suite property.

単純化及び一貫性のために本プロファイルは、通信におけるセキュアな連携方法で使用するために広範囲に実装されているRSA-1.5 暗号化アルゴリズムの使用が求められる。WS-セキュリティ・ポリシーでは、このアルゴリズムの一連のプロパティはsp:TripleDesRsa15にセットされる。

R2006 - All security policies specifying an algorithm suite assertion MUST contain the sp:AlgorithmSuite/wsp:Policy/sp:TripleDesRsa15 element.

R2006 - 暗号化操作を行うアルゴリズムに関する一連のプロパティについてのアサーションを規定する全てのセキュリティ・ポリシーは、sp:AlgorithmSuite/wsp:Policy/sp:TripleDesRsa15要素を含まなければならない。(MUST)

The sp:TransportBinding assertion is used to indicate that the message is protected using the means provided by the transport, such as HTTPS. This profile mandates the use of HTTPS as transport security, which is optional in WS-SecurityPolicy.

sp:TransportBinding (通信におけるセキュアな連携方法)アサーションは、HTTPSの様なトランスポートによって提供される手段を使用して、メッセージが保護されることを示すために使用される。本プロファイルは、トランスポート・セキュリティーとしてHTTPSの使用を義務付けるが、これはWS-セキュリティー・ポリシーにおいてはオプションである。

R2007 - Security policies containing an sp:TransportBinding element MUST contain one sp:HttpsToken element.

R2007 - sp:TransportBinding (通信におけるセキュアな連携方法)要素を含むセキュリティー・ポリシー は、sp:HttpsToken (HTTPS トークン)要素を 1 つ含まなければならない。 (MUST)

5.2.1.2 トークンの利用方法 (Use of Tokens)

WS-SecurityPolicy defines 10 types of tokens for protecting or associating tokens with the message (sp:UserName, sp:IssuedToken, sp:KerberosToken, sp:SpnegoContextToken, sp:SecurityContextToken, sp:SecureConversationToken, sp:SamlToken, sp:RelToken, sp:X509Token, sp:HttpsToken). For simplicity, and elimination of dependencies on WS-SecureConversation and WS-Trust for this version of this profile, this profile restricts the usage of security tokens to types X509 and HTTPS. WS-SecurityPolicy は、メッセージの保護や関連付けを行うためのセキュリティー情報を記述するために、10 種類のトークン(sp:UserName, sp:IssuedToken, sp:KerberosToken, sp:SpnegoContextToken, sp:SecurityContextToken, sp:SecureConversationToken, sp:SamlToken, sp:RelToken, sp:X509Token, sp:HttpsToken)を定義している。単純にするために、そして当プロファイルの本バージョンに関して WS-SecureConversation 及び WS-Trust に対する従属関係を排除するために、当プロファイルは、セキュリティー・トークンの使用を X509 と HTTPS の 2 種類に限定する。

X509 certificates leverage public key encryption where the sender generates ciphertext via the public key in the message recipient's X.509 certificate, and the recipient generates plaintext via its corresponding private key. The message sender has assurance that only the recipient will be able to read the message.

X509 証明書は、送信者がメッセージ受信者の X.509 証明書の公開鍵を介して暗号文を生成し、受信者がそれに対応する秘密鍵で平文を生成するという、公開鍵暗号化を活用している。メッセージ送信者は、受信者しかメールを読み出すことができないという保証を手にする。

R2008 - Security policies which contain security tokens, the tokens MUST be either an sp:X509Token element (Version 3 token as specified in WSS: X509 Certificate Token Profile 1.0) or an sp:HttpsToken element.

R2008 - セキュリティー・トークンを含むセキュリティー・ポリシーでは、トークンは、sp:X509Token 要素(WSS: X509 証明書トークン・プロファイル 1.0 で規定されるような X509V3 トークン型 "Version 3 token" あるいは sp:HttpsToken 要素のいずれかでなければならない。 (MUST)

Depending on the security token type, tokens have the ability to indicate message inclusion or its use in security processing. This indicator is optional in WS-SecurityPolicy. For simplicity and consistency, usage of message-level security within this profile requires tokens to be included within the messages.

WS-SecurityPolicy ではオプション扱いとなっているが、セキュリティー・トークンの種類によっては、トークンはセキュリティー処理においてメッセージの含有、又はその利用方法を示すことが出来る。単純化及び一貫性のために、当プロファイル中のメッセージ・レベル・セキュリティーの使用には、トークンがメッセージ内に含まれることが要求される。

R2009 – sp:X509token elements within security policies MUST include the sp:IncludeToken attribute with a value of “http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Always”.

R2009 – セキュリティ・ポリシー中のsp:X509token 要素は、“http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Always”の値を持ったsp:IncludeToken属性を含まなければならない。(MUST)

R2010 – sp:Httpstoken elements within security policies MUST include the sp:HttpsToken/@RequireClientCertificate attribute with a value of “true”.

R2010 – セキュリティ・ポリシー中のsp:Httpstoken要素は、“true”の値を持ったRequireClientCertificate属性を含まなければならない。(MUST)

5.2.1.3 完全性保護の利用方法 (Use of Integrity Protection)

WS-SecurityPolicy section 5.1 specifies QNames or XPath can be used to specify integrity assertions. In order to reduce complexity, this profile restricts the use of integrity protection assertions to being expressed only as QNames. Individual targeted parts of structures for integrity support are not permitted.

WS-セキュリティ・ポリシーセクション5.1は、完全性アサーションを指定するのにQNames又はXPathが使用できることを規定している。複雑さを軽減するために、当プロファイルは、完全性保護アサーションの使用をQNamesとしてしか表現できないように制限する。完全性サポートのための構造の個々のターゲット部分は許されない。

R2011 – Integrity assertions MUST be expressed using QNames.

R2011 – 完全性アサーションはQNamesを使用して表現されなければならない。(MUST)

The sp:SignedParts has ability to require all, or specific headers needing integrity protection, and if the SOAP body requires protection. In order to reduce complexity, this profile requires that all headers targeted for the SOAP ultimate receiver and the SOAP body of the message is to be integrity protected.

sp:SignedPartsは、もしSOAP本体が保護を必要とするならば、完全性保護を必要としている全ての、又は特定のヘッダーを要求することができる。複雑さを軽減するために、当プロファイルは、SOAP最終受信者向けの全てのヘッダー及びメッセージのSOAP本体が完全性を保護されることを要求する。

Further, WS-SecurityPolicy permits more than one sp:SignedParts elements. A cardinality of 1 element is sufficient to enforce this profile's integrity simplification restriction, and avoids any confusion if more than one is present.

更に、WS-セキュリティ・ポリシーは、1つ以上のsp:SignParts要素を許可する。一つの要素のカーディナリティは、当プロファイルの完全性を単純化するための制限としては1で十分であり、同一要素が2回以上出現した場合のどんな混乱をも回避します。

R2012 - All asymmetric security policies MUST have exactly one sp:SignedParts element with zero child elements.

R2012 - 全ての非対称なセキュリティ・ポリシーは、子要素を持たない、1つだけのsp:SignedParts要素を持たなければならない。(MUST)

The sp:SignedElements provides the ability to specify specific elements requiring integrity protection. In order to reduce complexity, this profile disallows this capability.

sp:SignedElementsは、完全性保護を必要としている特別な要素を特定することができる。複雑さを軽減するために、当プロファイルはこれを許可しない。

R2013 – All security policies MUST have zero sp:SignedElements elements.

R2013 – セキュリティ・トークンについて記述するpolicy要素において、sp:SignedElements要素は使用し

てはならない。(MUST)

5.2.1.4 機密保護の利用方法 (Use of Confidentiality Protection)

WS-SecurityPolicy 5.2 specifies QNames or XPath can be used to specify confidentiality assertions. In order to reduce complexity, this profile restricts the use of confidentiality protection assertions to being expressed only as QNames. Individual targeted parts of structures for confidentiality support are not permitted.

WS-セキュリティ・ポリシーのセクション 5.2は、秘密性アサーションを指定するために、QNames又はXPathが使用できることを規定する。複雑さを軽減するために、当プロファイルは、機密保護アサーションの使用をQNamesとしてしか表現できないよう制限する。機密性サポートのための構造の個々のターゲット部分は許可されない。

R2014 – Confidentiality assertions MUST be expressed using QNames.

R2014 – 機密保護アサーションは、QNamesを使用して表現されなければならない。(MUST)

The sp:EncryptedParts has ability to require specific headers which need confidentiality protection, and if the SOAP body requires protection. For simplicity and consistency, this profile views all RosettaNet Business Messages as confidential and requires confidentiality support during exchange. Other supporting information, such as Receipt

Acknowledgements are not necessarily required to have such protection.

sp:EncryptedParts (暗号化部分)は、もしSOAP本体が保護を必要とするならば、機密保護を必要とする特別なヘッダーを要求することができる。単純化及び一貫性のために、当プロファイルはRosettaNetビジネス・メッセージを全て機密と見なし、情報交換中の機密保護サポートを必要とする。受信確認の様な他のサポート情報は、必ずしもそのような保護を講じる必要はない。

R2015 - All asymmetric security policies MUST have exactly one sp:EncryptedParts element with zero child elements when the policy is associated with the exchange of a RosettaNet Business Message.

R2015 -非対称型アルゴリズムによる暗号化でのセキュリティを行う際に、セキュリティ・トークンについて記述するpolicy要素は、そのpolicy要素がRosettaNetビジネス・メッセージの交換と関連付けられる場合、子要素の無い1個だけのsp:EncryptedParts要素を持たなければならない。(MUST)

The sp:EncryptedElements provides the ability to specify specific elements requiring confidentiality protection. In order to reduce complexity, this profile disallows this capability.

sp:EncryptedElements (暗号化された要素)は、機密保護を必要とする特別な要素を特定することができる。複雑さを軽減するために、本プロファイルはこれを許可しない。

R2016 – All security policies MUST have zero sp:EncryptedElements elements.

R2016 – セキュリティ・トークンについて記述するpolicy要素において、sp:EncryptedElements要素は使用してはならない。(MUST)

The sp:EncryptedParts/sp:Header provides the ability to indicate that a specific header needs confidentiality protection. In order to provide a high level of protection against a cryptographic attack on a message signature, this profile requires that signatures be encrypted. However, this profile specifies the use of sp:EncryptSignature assertion to support this requirement.

sp:EncryptedParts/sp:Header は、特定ヘッダーが機密保護を必要とすることを示す能力を提供する。メッセージ署名に対する暗号攻撃からのハイレベルな保護を提供するために、当プロファイルは、署名が暗号化されることを要求する。しかしながら、本プロファイルはこの要件をサポートするために、sp:EncryptSignature (暗号署名) アサーションの使用を規定する。

This assertion facilitates confidentiality requirements specifically, and exclusively, targeted toward headers containing signatures. See the section on Signature Protection.

このアサーションは、署名付きヘッダーを特別に、限って目標にした機密保護要件を促進する。署名保護のセクションを参照のこと。

5.2.1.5 認証 (Authentication)

5.2.1.5.1 トランスポート層の基本認証 (Transport-level Basic Authentication)

It is important to note that concerning security, this profile is written under the assumption of using WS-SecurityPolicy assertions. At the time of writing, WS-SecurityPolicy does not provide assertions for HTTP basic authentication.

セキュリティに関して、本プロファイルがWS-セキュリティ・ポリシーに記述されているアサーションを使用する前提の下で書かれていることに留意することは重要である。本プロファイル作成時点では、WS-セキュリティ・ポリシーはHTTP基本認証に対するアサーションを提供していない。

This profile makes no additional assumptions about the semantics of the combination of security assertions of WS-SecurityPolicy – meaning this profile does not define semantics for the absence of any assertions, etc, concerning usage of HTTP basic authentication.

Therefore, the use of HTTP authentication is viewed as mutually exclusive to the use of security assertions and the specification of such must be done in a TPA.

本プロファイルは、WS-セキュリティ・ポリシーのセキュリティ・アサーション連携の意味について、追加の仮定を作らない。これは、当プロファイルがいかなるアサーションの欠如、例えば、HTTP基本認証の利用に関するものに対して、中身を定義しないことを意味している。それゆえ、HTTP認証の使用は、セキュリティ・アサーションの2社間に限定された使用と見なされ、その詳細はTPA (取引者間契約)の中に記載されなければならない。

R2017 – HTTP basic authentication MAY be used for authentication and SHOULD be specified as such within a TPA.

R2017 – HTTP基本認証は、認証に使用することが可能であり (MAY)、TPA (取引者間契約)の中で規定されるべきである。(SHOULD)

R2018 – If HTTP basic authentication is used for authentication, HTTPS MUST be used for confidentiality support and SHOULD be specified in a TPA.

R2018 – もしHTTP基本認証が認証に使用されるならば、HTTPSが機密性サポートに使用されなければならない (MUST)、TPA (取引者間契約)の中で規定されるべきである。(SHOULD)

5.2.1.5.2 ポリシーに基づいた認証 (Policy-based authentication)

R2019 – X.509 certificates MUST be used for authentication within asymmetric bindings.

R2019 – X.509証明書は、非対称型アルゴリズムの暗号化による連携における認証に使用されなければならない。(MUST)

R2020 – X.509 certificates MUST be used for authentication within transport bindings.

R2020 – X.509証明書は、通信においてセキュアな連携を行う場合の認証に使用されなければならない。(MUST)

5.2.1.6 発信元と受信の否認防止 (Non-Repudiation of Origin & Receipt)

While a digital signature generated by a sender provides the ability of verifying the integrity of the message to detect tampering and to provide sender identity, the use of digital signatures can provide evidence of some action on the associated data facilitating non-repudiation of the action. This is sometimes referred to as proof of possession.

送信者によって生成されるデジタル署名が、改ざんを検出するためのメッセージの完全性検証を可能にし、送信者の身元を提供する一方で、デジタル署名の利用はやりとりの否認防止を容易にして、関連データ上の何らかの行動に関する証拠を提供することができる。これは‘所有の証明’と呼ばれることが

ある。

Since this profile mandates the use of X.509 certificates to be indicated within all security policies, the certificate can be used to provide possession of the data through the action of signing by the sender, facilitating non-repudiation of origin. This is the mandated form of non-repudiation of origin used by this profile.

本プロファイルがX.509証明書の使用を全てのセキュリティ・ポリシー内で明示するよう義務付けるので、証明書は、送信者が署名し発信元の否認防止を促進する行動を通じて、データの所有に使用することができる。これは、本プロファイルによって使用される、発信元の否認防止に義務付けられた書式である。

R2021 – Signing using X.509 certificates MUST be used for non-repudiation purposes

R2021 – X.509証明書を使用する署名は、否認防止の目的のために使用されなければならない。
(MUST)

R2022 - For non repudiation of origin the entire SOAP message MUST be signed.

R2022 - 発信元の否認防止については、SOAPメッセージ全体が署名されなければならない。(MUST)

R2023 - For non repudiation of receipt, while the entire SOAP message will be signed, the contained receipt ack business document will hold the hash of the correlated RosettaNet Business document (SOAP body) that was received.

R2023 - 受信の否認防止のために、SOAPメッセージ全体が署名される一方、記載された受信確認ビジネス文書は、受け取られた関連RosettaNetビジネス文書(SOAP本体)のハッシュを保持するであろう。

5.2.1.7 保護順序の使用法と署名保護 (Use of Protection Order, and Signature Protection)

Protection Order refers to the sequence used for applying security enforcement. The highest level of protection is generally thought to come from signing the body, encrypting it, and then encrypting any signatures.

保護順序は、セキュリティを実施するために使用される順序である。保護の最も高いレベルは、本体に署名し、それを暗号化し、次にいくつかの署名を暗号化することで得られる。

R2024 – Security policies containing an asymmetric binding MUST contain zero

sp:EncryptBeforeSigning elements.

R2024 – セキュリティ・トークンについて記述するpolicy要素が非対称アルゴリズムの暗号化による連携に関する要素(sp:AsymmetricBinding)を含んでいる場合、policy要素にはsp:EncryptBeforeSigning要素を含んではならない。(MUST)

R2025 – Security policies containing an asymmetric binding MUST contain one

sp:EncryptSignature element.

R2025 – セキュリティ・トークンについて記述するpolicy要素が非対称アルゴリズムの暗号化による連携に関する要素(sp:AsymmetricBinding)を含んでいる場合、policy要素には1個のsp:EncryptSignature要素を含まなければならない。(MUST)

WS-SecurityPolicy 7.6 provides an assertion to specify signatures over the SOAP body and SOAP headers must always cover the entire body and entire header elements. It is thought that setting the value of this property to 'true' may help mitigate against some possible re-writing attacks, and to reduce complexity this profile requires the use of this assertion. The default value for this property is 'false'.

WS-セキュリティ・ポリシーのセクション 7.6 は、SOAP本体上の署名を指定するアサーションを提供し、SOAPヘッダーは常に本体全体及びヘッダー要素全体をカバーしなければならない。このプロパティの値として"true"をセットすることは、可能性のある書換え攻撃を軽減するのに役立つと考えられ、複雑さを減少させるために、本プロファイルはこのアサーションの使用を要求する。このプロパティのデフォルト値は"false"である。

R2026 – Security policies containing an asymmetric binding MUST contain exactly one sp:OnlySignEntireHeadersAndBody element.

R2026 – セキュリティトークンについて記述するpolicy要素が非対称アルゴリズムの暗号化による連携に関する要素(sp:AsymmetricBinding)を含んでいる場合、policy要素には、必ず1個のsp:OnlySignEntireHeadersAndBody 要素を含まなければならない。(MUST)

5.2.1.8 レイアウトの使用法 (Use of Layout)

WS-SecurityPolicy 7.7 provides an assertion concerning layout rules for security headers. This profile does not mandate the use of, or constrain this feature.

WS-SecurityPolicyのセクション 7.7 は、セキュリティヘッダーのためのレイアウト規則に関するアサーションを提供する。当プロファイルは、この機能の使用を義務付けても抑制してもいい。

5.2.1.9 例 (Examples)

An Asymmetric Binding Policy with an X509 token as the initiator token and requirement to always include it in messages, an X509 token as the recipient token and requirement to always include it in messages, the use of the TripleDesRSA15 algorithm suite, a requirement to encrypt signatures (<sp:encryptSignature/>), a requirement to sign the message parts before encrypting (expressed as the <sp:EncryptBeforeSigning/> element not present), and a requirement to only sign entire headers:

開始者トークンとしてのX.509トークンとそれを常にメッセージに含めるという要件、受取者トークンとしてのX.509トークンとそれを常にメッセージに含めるという要件、TripleDesRSA15アルゴリズム スウィートの使用、署名を暗号化するという要件(<sp:encryptSignature/>)、暗号化する前にメッセージ部分に署名するという要件<sp:EncryptBeforeSigning/>要素として表現される)、及びヘッダー全体にのみ署名するという要件を備えた非対称な結合ポリシー。

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<wsp:Policy xmlns:sp="http://schemas.xmlsoap.org/ws/2005/02/securitypolicy"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/ws/2005/02/securitypolicy:\Proj\Web
Services\docs\securitypolicyJuly2005.xsd">
```

```
<sp:AsymmetricBinding>
```

```
<wsp:Policy>
```

```
<sp:RecipientToken>
```

```
<wsp:Policy>
```

```
<sp:X509V3Token sp:IncludeToken=".../IncludeToken/Always"/>
```

```
</wsp:Policy>
```

```
</sp:RecipientToken>
```

```
<sp:InitiatorToken>
```

```
<wsp:Policy>
```

```
<sp:X509V3Token sp:IncludeToken=".../IncludeToken/Always"/>
```

```
</wsp:Policy>
</sp:InitiatorToken>
<sp:AlgorithmSuite>
<wsp:Policy>
<sp:TripleDesRsa15/>
</wsp:Policy>
</sp:AlgorithmSuite>
<sp:EncryptSignature/>
<sp:OnlySignEntireHeadersAndBody/>
<sp:SignedParts/>
</wsp:Policy>
</sp:AsymmetricBinding>
</wsp:Policy>
```

A Transport Binding policy indicating the use of HTTPs and a requirement for the client certificate to be included in the message.

通信におけるセキュアな連携方法としてHTTPsが使用され、クライアント証明書がメッセージに含まれることが要求される場合の例。

```
<?xml version="1.0" encoding="UTF-8"?>
<wsp:Policy xmlns:sp="http://schemas.xmlsoap.org/ws/2005/02/securitypolicy"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/ws/2005/02/securitypolicy:\Proj\
WebServices\docs\securitypolicyJuly2005.xsd">
<sp:TransportBinding>
<wsp:Policy>
<sp:TransportToken>
<wsp:Policy>
<sp:HttpsToken RequireClientCertificate="true"/>
</wsp:Policy>
</sp:TransportToken>
</wsp:Policy>
</sp:TransportBinding>
```

</wsp:Policy>

5.3 QoS及びピュア・クライアント・ツー・サービスへのパターン (QoS and Pure Client to Service Patterns)

This section addresses Web services QoS aspects which are specifically relevant to each pattern involving a Pure Client invoking a Service.

本セクションは、特にピュア・クライアント・ツー・サービスを呼び出すことを含む、各パターンに関するウェブサービスQoSの側面を取り上げる。

5.3.1 ピュア・クライアント・ツー・サービスに関する共通QoS (Pure Client to Service Common QoS)

This section addresses QoS aspects common to patterns with pure clients to services.

本セクションは、ピュア・クライアント・ツー・サービスに関する共通パターンのQoS側面を取り上げる。

5.3.1.1 安全 (Security)

The appropriate security approach for patterns involving a pure client vary on several factors which largely depend on the pure client endpoint capabilities. Since the capabilities of pure client endpoints can not be assumed, consistent security quality aspects can not be specified consistently in pure client patterns.

ピュア・クライアントを含んだパターンに対する適切な安全への取り組みは、主としてピュア・クライアントのエンドポイント能力に依存する複数の要因により変動する。ピュア・クライアント・エンドポイントの機能が想定できないので、安定的なセキュリティ品質側面をピュア・クライアントのパターンで一貫して指定することはできない。

R2030 – A security policy containing an sp:AsymmetricBinding SHOULD be utilized in patterns involving a pure client.

R2030 – sp:AsymmetricBindingを持つセキュリティ・ポリシーは、ピュア・クライアントを含んだパターンで利用されるべきである。(SHOULD)

R2031 – A security policy containing an sp:TransportBinding MAY be utilized in patterns involving a pure client.

R2031 – sp:TransportBinding を持ったセキュリティ・ポリシーは、ピュア・クライアントを含んだパターンで利用されるかもしれない。(MAY)

R2032 – Patterns involving a pure client MAY utilize HTTP basic authentication.

R2032 – ピュア・クライアントを含んだパターンは、HTTP基本認証を使用するであろう。(MAY)

R2033 – Patterns involving a pure client which utilize HTTP basic authentication MUST utilize HTTPS to provide confidentiality protection.

R2033 – HTTP基本認証を使用するピュア・クライアントを含んだパターンは、機密保護を提供するためにHTTPSsを利用しなければならない。(MUST)

5.3.1.2 信頼性 (Reliability)

Due to pure clients being noninvokable, the WS-ReliableMessaging Protocol can not be utilized between a pure client and an invokable service. Exchanges involving noninvokable endpoints in some cases allows WS-Addressing to be utilized outside the expected use between invokable services.

ピュア・クライアントは呼出すことが出来ないので、WS-ReliableMessaging Protocol (高信頼メッセージングプロトコル)を、ピュア・クライアント・ツー・サービスで利用することはできない。呼出すことが出来ないエンド

ポイントを含む情報交換は、WS-アドレッシングがサービス・ツー・サービスでの想定使用法以外で利用されることを許可することもある。

Pure clients may or may not support aspects of reliable messaging. Handling failures in a standard way enhances reliability in the pure client to service patterns.

ピュア・クライアントは、高信頼メッセージングの側面をサポートするかもしれないし、サポートしないかもしれない。標準的な方法でエラーを処理することは、ピュア・クライアント・ツー・サービスのパターンにおける信頼性を高める。

5.3.1.3 リトライ (Retries)

Note: This discussion about retries applies to all SOAP messages sent by the pure client to the service

注記: リトライに関するこの議論は、ピュア・クライアント・ツー・サービスに送られた全てのSOAPメッセージに適用される。

R2034 – When encountering connection failures or other transport related errors, the pure client MAY retry sending the Soap request message that previously resulted in an error.

R2034 – 接続エラーまたは他のトランスポート関連エラーを検出した場合、ピュア・クライアントは、直前にエラーになったSOAP要求メッセージの送信をやり直すでしょう。(MAY)

理論的根拠 Rationale

Retries are common practice for fault tolerance for connection failures or other transport related errors.

リトライは、接続エラーあるいはその他のトランスポート関連エラーに関する障害対応のための一般的な方法である。

R2035 – The SOAP request message that is retried MUST have a WS-Addressing:MessageID equal to the previous SOAP request message that resulted in an error.

R2035 – リトライされたSOAP要求メッセージは、直前にエラーになったSOAP要求メッセージと等しいWS-Addressingで定義されたwsa:MessageID要素を持たなければならない。(MUST)

理論的根拠 Rationale

The service in these pure client patterns can detect duplicate SOAP request messages by comparing WS-Addressing:MessageID values and in certain scenarios greatly improve aspects of reliability, such as eliminating message loss and duplicate messages. Although this rule enables such reliability aspects, this profile considers them as implementation details out of scope of this Profile.

これらのピュア・クライアント・パターンにおけるサービスは、WS-Addressingで定義されたwsa:MessageID要素の値を比較することにより、SOAP要求メッセージの重複を検出でき、特定のシナリオでは信頼性面で大いに改善する、それはメッセージ紛失及び重複メッセージを除去するなどである。このルールはそのような信頼性改善を可能にするけれども、本プロファイルでは、それを本プロファイルの範囲外の実装詳細と考える。

Implementation consideration for services capable of detecting duplicate messages: Services capable of detecting duplicate messages by comparing the WS-Addressing:MessageID to previously received messages can respond back to the pure client using original SOAP response sent back from the original client request. This implies that the service will need to store these original responses or have a way to

reproduce them when a duplicate is detected. In order to avoid requiring the service to store the original response for an indefinite amount of time, a retention timeframe should be set by the service. When a duplicate message is detected by the service and the original response cannot be found or recreated due to the retention timeframe being exceeded, then the service can respond back with a SOAP fault indicating that a “duplicate WS-Addressing message has been received”.

重複メッセージを検知可能なサービスに関する実装上の考慮点:先に受け取ったメッセージとWS-アドレスシング:MessageIDを比較することにより、重複メッセージを検知することができるサービスは、元のクライアント要求から送られたSOAP応答を使用して、ピュア・クライアントに応答を返すことができる。サービスがこれらオリジナルの応答を保管する、又は重複が検出された場合にそれを再生する方法を持つ必要があるだろうことを暗示する。サービスが無期限にオリジナルの応答を記憶する必要性を避けるために、サービスによって保持時間枠を設定するべきである。重複メッセージがサービスによって検知され、保持時間枠を超過しているためにオリジナルの応答が見つからない、又は再生できない場合、その後サービスは、“重複WSアドレスシング・メッセージを受け取った”ことを示すSOAPエラーと一緒に応答を返すことができる。

This profile provides specifications on what it passed on the wire when a retry is performed. This profile considers retry thresholds and policies, such as the use of an indicator for maximum number of retries and interval between retries, as implementation detail that would be agreed upon in the TPA if retries are to be used.

本プロファイルは、リトライが行われる時には、自分が通信に渡したものに関する仕様を提供する。本プロファイルは、もしリトライが使用されるならば、TPAの中で同意した実装詳細として、リトライ最大数及びリトライ間隔のインジケータの使用などのリトライしきい値及びポリシーを考慮する。

5.3.2 ピュア・クライアント・ツー・サービス要求応答パターン (Pure Client to Service Request Response Pattern)

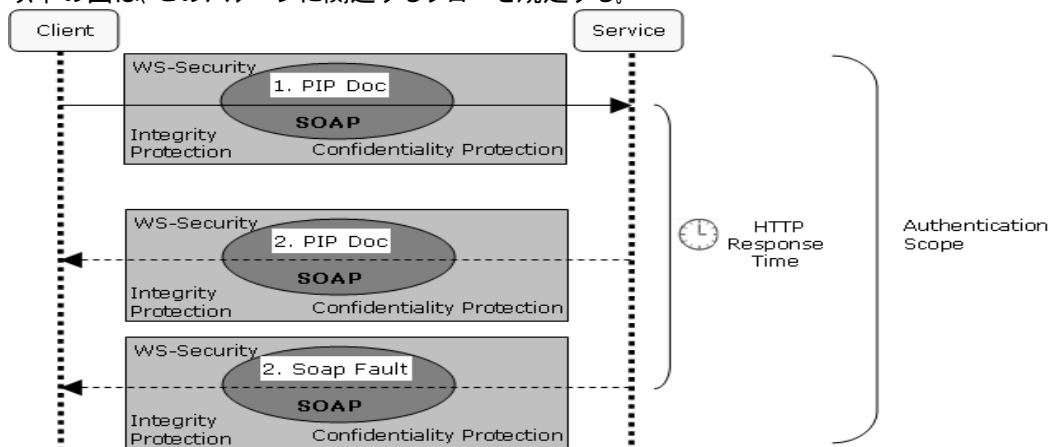
This environment contains pure client to service interaction. The request contains a RosettaNet Business Message and the response contains a resulting RosettaNet Business Message. The communication is synchronous in the sense that the request is sent and the response is received using the same transport connection.

この環境はピュア・クライアント・ツー・サービスへのやりとりを含む。その要求はRosettaNetビジネス・メッセージを含んでおり、応答はそのRosettaNetビジネス・メッセージの結果を含んでいる。通信は同一のトランスポート接続を使用して、要求が送られ応答が受信されるという意味で、同期をとって行われる。

5.3.2.1 QoS付きの全体フロー (Overall Flow with QoS)

The following diagram defines the flow associated with this pattern.

以下の図は、このパターンに関連するフローを規定する。



1) Confidentiality protection is required in this exchange. Client invokes Service's operation accepting a RosettaNet Business Message. At completion of sending the RosettaNet Business Message by the client, client starts its HTTP response time clock. The HTTP response time is what is considered a reasonable/acceptable time to leave an HTTP connection open which can vary depending on network latency and message size. At acceptance of the RosettaNet Business Message, Service starts its HTTP response time clock.

1) この交換では、機密保護が要求される。クライアントは、RosettaNetビジネス・メッセージを受信するサービス操作を呼び出す。クライアントによるRosettaNetビジネス・メッセージ送信が完了すると、クライアントはそのHTTP応答時間クロックをスタートさせる。HTTP応答時間は、HTTP接続を開いておくための合理的/受容可能な時間と考えられるものであり、ネットワーク待ち時間及びメッセージ・サイズによって変わりうる。RosettaNetビジネス・メッセージを受信すると、サービスはHTTP応答時間クロックをスタートさせる。

2) Within its HTTP response time limit, Service responds using the same connection with either a resulting RosettaNet Business Message or a SOAP fault indicating PIP failure.

2) そのHTTP応答時間制限内に、サービスは同一の接続を使用してRosettaNetビジネス・メッセージの結果、又はPIPエラーを示すSOAPエラーのどちらかを応答する。

5.3.2.2 タイマー (Timers)

Timers are useful in measuring time and triggering actions when a specific period of time has elapsed. In this pattern, the request and response is on the same connection and the HTTP response time should be no longer than what is a reasonable/acceptable time to leave an HTTP connection open. The duration of the HTTP response time would be agreed upon in the TPA. After such time has elapsed, the client MUST close the connection and treat it as a transport related error.

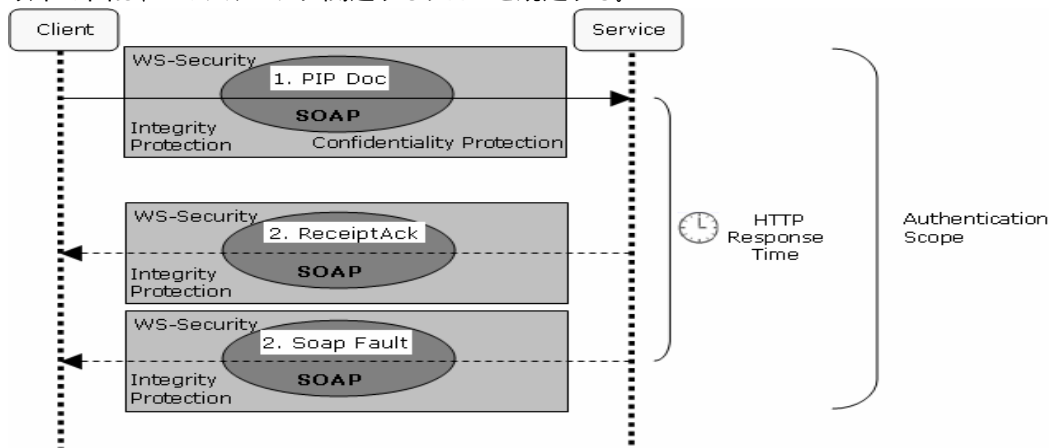
タイマーは時間を測定し、一定の時間が経過した時にアクションを起動する上で有用である。このパターンでは、要求及び応答が同一セッションで行われ、HTTP応答時間はHTTP接続を開いておくための合理的/受容可能な時間を超えるものであるべきでない。HTTP応答時間の長さは、TPA(取引者間契約)にて合意されるであろう。当該時間が経過すると、クライアントは接続を閉じ、トランスポート関連エラーとして取り扱わなければならない。MUST)

5.3.3 プッシュ型ピュア・クライアント・ツー・サービス要求 / 応答パターン (Pure Client to Service Request Response Push Pattern)

5.3.3.1 QoS 付きの全体フロー (Overall Flow with QoS)

The following diagram defines the flow associated with this pattern.

以下の図は、このパターンに関連するフローを規定する。



1) Confidentiality protection is required in this exchange. Client invokes Service's operation accepting a RosettaNet Business Message. At completion of sending the RosettaNet Business Message by the client, client starts its HTTP response time clock. The HTTP response time is what is considered a reasonable/acceptable time to leave an HTTP connection open which can vary depending on network latency and message size at acceptance of the RosettaNet Business Message, Service starts its HTTP response time clock.

1) この交換では、機密保護が要求される。クライアントは、RosettaNetビジネス・メッセージを受信するサービス操作を呼び出す。クライアントによるRosettaNetビジネス・メッセージ送信が完了すると、クライアントはそのHTTP応答時間クロックをスタートさせる。HTTP応答時間は、HTTP接続を開いておくための合理的/受容可能な時間と考えられるものであり、ネットワーク待ち時間及びメッセージ・サイズによって変わりうる。RosettaNetビジネス・メッセージを受信すると、サービスはHTTP応答時間クロックをスタートさせる。

2) Within its HTTP response time limit, Service responds using the same connection with either a Receipt Acknowledgement indicating that the RosettaNet Business Message has been received or a SOAP fault indicating PIP failure.

2) そのHTTP応答時間制限内に、サービスは同一の接続を使用してRosettaNetビジネス・メッセージの結果、又はPIPエラーを示すSOAPエラーのどちらかを応答する。

5.3.3.2 タイマー (Timers)

Timers are useful in measuring time and triggering actions when a specific period of time has elapsed. In this pattern, the request and response is on the same connection and the HTTP response time should be no longer than what is a reasonable/acceptable time to leave an HTTP connection open. The duration of the HTTP response time would be agreed upon in the TPA. After such time has elapsed, the client MUST close the connection and treat it as a transport related error.

タイマーは時間を測定し、一定の時間が経過した時にアクションを起動する上で有用である。このパターンでは、要求及び応答が同じ接続で行われ、HTTP応答時間はHTTP接続を開いておくための合理的/受容可能な時間を超えるものであるべきでない。HTTP応答時間の長さは、TPA(取引者間契約)にて合意されるだろう。当該時間が経過すると、クライアントは接続を閉じ、トランスポート関連エラーとして取り扱わなければならない。(MUST)

5.3.3.3 受信確認 (Receipt Acknowledgements)

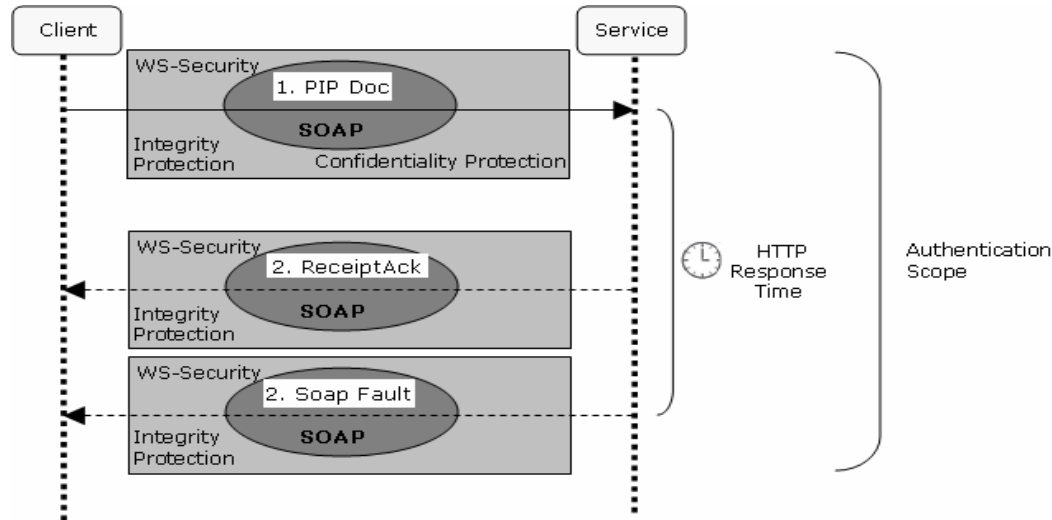
Receipt Acknowledgements exchanged indicate that a RosettaNet Business Message was received and it validated against its schema. The Receipt Acknowledgement can provide non-repudiation of receipt when it is digitally signed. They are returned from the recipient to the sender of the message exchange and are used to complete business transactions and support non-repudiation of receipt. The Receipt Acknowledgement in the pure client to service request response push MEP is returned by the recipient (Service) to the sender (Pure Client) on the same connection that the RosettaNet Business Message was sent on.

交換された受信確認は、RosettaNetビジネス・メッセージが受信され、そのスキーマに対して検証したことを示す。受信確認はそれがデジタル署名される場合、受信の否認防止を提供することができる。それはメッセージ交換の受信者から送信者に返され、ビジネス・トランザクション処理を終了させ、かつ受信の否認防止をサポートするために使用される。プッシュ型ピュア・クライアント・ツー・サービス要求/応答MEP(メッセージ交換パターン)における受信確認は、RosettaNetビジネス・メッセージが送られたのと同じ接続上で、受信者(サービス)から送信者(ピュア・クライアント)に返される。

5.3.4 プル型ピュア・クライアント・ツー・サービス要求 / 応答パターン (Pure Client to Service Request Response Pull Pattern)

5.3.4.1 QoS 付きの全体フロー (Overall Flow with QoS)

The following diagram defines the flow associated with this pattern.
以下の図は、このパターンに関連するフローを規定する。



1) Confidentiality protection is required in this exchange. Client invokes Service's operation to send a request for a RosettaNet Business Message. At completion of sending the request message by the client, client starts its HTTP response time clock. The HTTP response time is what is considered a reasonable/acceptable time to leave an HTTP connection open which can vary depending on network latency and message size. At acceptance of the request message, Service starts its HTTP response time clock.

1) この交換では、機密保護が要求される。クライアントは、RosettaNetビジネス・メッセージを受信するサービス操作を呼び出す。クライアントによるRosettaNetビジネス・メッセージ送信が完了すると、クライアントはそのHTTP応答時間クロックをスタートさせる。HTTP応答時間は、HTTP接続を開いておくための合理的/受容可能な時間と考えられるものであり、ネットワーク待ち時間及びメッセージ・サイズによって変わりうる。RosettaNetビジネス・メッセージを受信すると、サービスはHTTP応答時間クロックをスタートさせる。

2) Within its HTTP response time limit, Service responds using the same connection with either a resulting RosettaNet Business Message, an empty/null message indicating no RosettaNet Business Messages to receive, or a SOAP fault indicating a failure processing the request. If the Service responds back with a RosettaNet Business Message, then the Service will start its PIP Time To Acknowledge clock at completion of sending the RosettaNet Business Message by the service. At acceptance of the RosettaNet Business Message, client starts its PIP Time To Acknowledge clock.

2) そのHTTP応答時間制限内に、サービスは要求されたRosettaNetビジネスメッセージ、受け取るべきRosettaNetメッセージがないことを示す空 / nulメッセージまたは要求処理エラーを示すSOAPエラーのいずれかを同一の接続を使用して応答する。もしサービスがRosettaNetビジネス・メッセージに回答を返す場合、サービスは、サービスがRosettaNetビジネス・メッセージを送り終えた時点でそのPIPの「確認のための時間」クロックをスタートさせる。RosettaNetビジネス・メッセージの受信時点で、クライアントはそのPIPの「確認のための時間」クロックをスタートさせる。

3) Within its PIP Time To Acknowledge clock, Client initiates a new connection to the Service and sends a Receipt Acknowledgement indicating successful receipt of the RosettaNet Business Message. The service acknowledges the Receipt Acknowledgement with an HTTP response code indicating successful receipt.

3) そのPIPの「確認のための時間」内に、クライアントはサービスへの新しい接続を開始し、RosettaNetビジネス・メッセージの受信成功を示す受信確認を送る。サービスは、受信成功を示すHTTPレスポンス・コードによって受信確認を認める。

5.3.4.2 タイマー (Timers)

Timers are useful in measuring time and triggering actions when a specific period of time has elapsed. In this pattern, two measures of time are useful: HTTP response time and PIP Time To Acknowledge.

タイマーは時間を測定し、一定の時間が経過した時にアクションを起動する上で有用である。このパターンでは、2つの時間指標が有用である: HTTP応答時間とそのPIPの「確認のための時間」。

For each interaction with the service (RosettaNet Business Message pull and Receipt Acknowledgement send), the request and response is on the same connection and the HTTP response time should be no longer than what is a reasonable/acceptable time to leave an HTTP connection open. The duration of the HTTP response time would be agreed upon in the TPA. After such time has elapsed, the client MUST close the connection and treat it as a transport related error.

サービスとのそれぞれのやりとり(RosettaNetビジネス・メッセージ・プル及び受信確認送信)については、要求及び応答が同じ接続で行われ、HTTP応答時間は、HTTP接続を開いておくための合理的/受容可能な時間を超えるものであるべきでない。HTTP応答時間の長さは、TPA(取引者間契約)にて合意されるだろう。当該時間が経過すると、クライアントは接続を閉じ、トランスポート関連エラーとして取り扱わなければならない。(MUST)

The PIP Time To Acknowledge maps to the RosettaNet PIP Time To Acknowledgement for the particular RosettaNet Business Message being exchanged. This profile considers the behavior by either the pure client or service when the PIP Time To Acknowledge is exceeded as implementation detail out of scope of this profile.

タイマーで設定するPIPの「確認のための時間」は、交換される特定のRosettaNetビジネス・メッセージに対するRosettaNet PIPの「確認のための時間」にマッピングされる。実装詳細は、当プロファイルの対象外ではあるが、当プロファイルは、PIPの「確認のための時間」を超過する時のピュア・クライアントかサービスのどちらかの振る舞いを考慮する。

5.3.4.3 受信確認 (Receipt Acknowledgements)

Receipt Acknowledgements exchanged indicate that a RosettaNet Business Message was receiving and it was validated against its schema. They are sent from the recipient to the sender of the message exchange and are used to complete business transactions and support non-repudiation of receipt. The Receipt Acknowledgement in the pure client to service request response pull pattern is sent by the recipient (Pure Client) to the sender (Service) using a subsequent message sent by the Pure Client after successfully receiving a RosettaNet Business Message. This profile considers the behavior of the service after its PIP Time To Acknowledge clock has elapsed as implementation detail and is out of scope of this profile.

交換された受信確認は、RosettaNetビジネス・メッセージが受信され、そのスキーマに対して検証したことを示す。それはメッセージ交換の受信者から送信者に返され、ビジネス・トランザクション処理を終了させ、かつ受信の否認防止をサポートするために使用される。プル型ピュア・クライアント・ツー・サービス要求/応答パターンにおける受信確認は、RosettaNetビジネス・メッセージが首尾よく受け取られた後にピュア・クライアントによって送信される後続のメッセージを使用して、受信者(ピュア・クライアント)から送信者(サービス)に送信される。実装詳細については、当プロファイルの対象外ではあるが、当プロファイルは、そのPIPの「確認のための時間」を超過した後のサービスの振る舞いを考慮する。

5.4 QoS とサービス・ツー・サービスのパターン (QoS and Service to Service Pattern)

This section addresses Web services QoS aspects which are specifically relevant to the pattern involving a Service invoking a Service.

本セクションは、サービスがサービスを呼び出すことを含むパターンに、特に関係するWebサービスQoSの側面を取り上げる:

In order to provide comprehensive examples for QoS aspects of the pattern in this section, we define two Services, A and B. ServiceA acts as the initially invoking service, while ServiceB is the initially invoked service. It outlines the QoS aspects of using an RM sequence and which security protection mechanisms are required within the information exchange.

本セクション中のパターンのQoS側面に関する総合的な例を提供するために、2つのサービス、A及びBを定義する。ServiceAは、最初に呼び出すサービスとして行動し、一方ServiceBは、最初に呼び出されたサービスである。RM(WS-RM:高信頼性メッセージング)手順を使用するQoS側面と、情報交換内でのセキュリティ保護メカニズムが必要になるかを説明している。

5.4.1 サービス・ツー・サービスの一方向コールバック・パターン (Service To Service One Way Callback Pattern)

This section addresses QoS aspects common to patterns with Service To Services. It outlines the QoS aspects of using an RM sequence and which security protection mechanisms are required within the information exchange.

本セクションは、サービス・ツー・サービスのパターンに共通のQoS側面を取り上げる。RM(WS-RM:高信頼性メッセージング)手順を使用するQoS側面と、情報交換内でのセキュリティ保護機構が必要になるかを説明する。

5.4.1.1 安全 (Security)

Both the invoking and invoked services in this pattern are assumed to be deployed into an enterprise-level environment with robust IT functionality and involved entities where a brokered authentication model can be leveraged, avoiding the limitations of transport-level authentication mechanisms and the credential management tasks of a direct authentication model.

このパターンの呼び出し側と呼び出される側両方のサービスは、しっかりしたIT機能を備えた企業レベルの環境に配備されると想定される。そしてトランスポートレベル認証メカニズム及びダイレクト認証モデルの信用証明業務の限界を回避した、仲介された認証モデルを活用できる法人が含まれる。

R2036 – Services of these patterns must utilize a security policy containing a sp:AsymmetricBinding element.

R2036 – これらのパターンのサービスは、非対称アルゴリズムの暗号化による連携に関する要素 (sp:AsymmetricBinding) を含むセキュリティ・ポリシーを使用しなければならない。(MUST)

5.4.1.2 信頼性 (Reliability)

R2037 – WS-ReliableMessaging must be used by services in these patterns. All steps within this pattern must use ExactlyOnce and InOrder delivery assurances within the RM sequence.

R2037 – これらのパターンでは、サービスによってWS-ReliableMessaging(WS-高信頼性メッセージング)が使用されなければならない。このパターン内の全てのステップは、RM手順にある配信保証について記述する要素において、「ExactlyOnce(メッセージ配信は1回限り)」と「InOrder(メッセージは送信元と同一順序でメッセージシーケンス番号に従い配信)」を使用しなければならない。

5.4.1.3 タイマー (Timers)

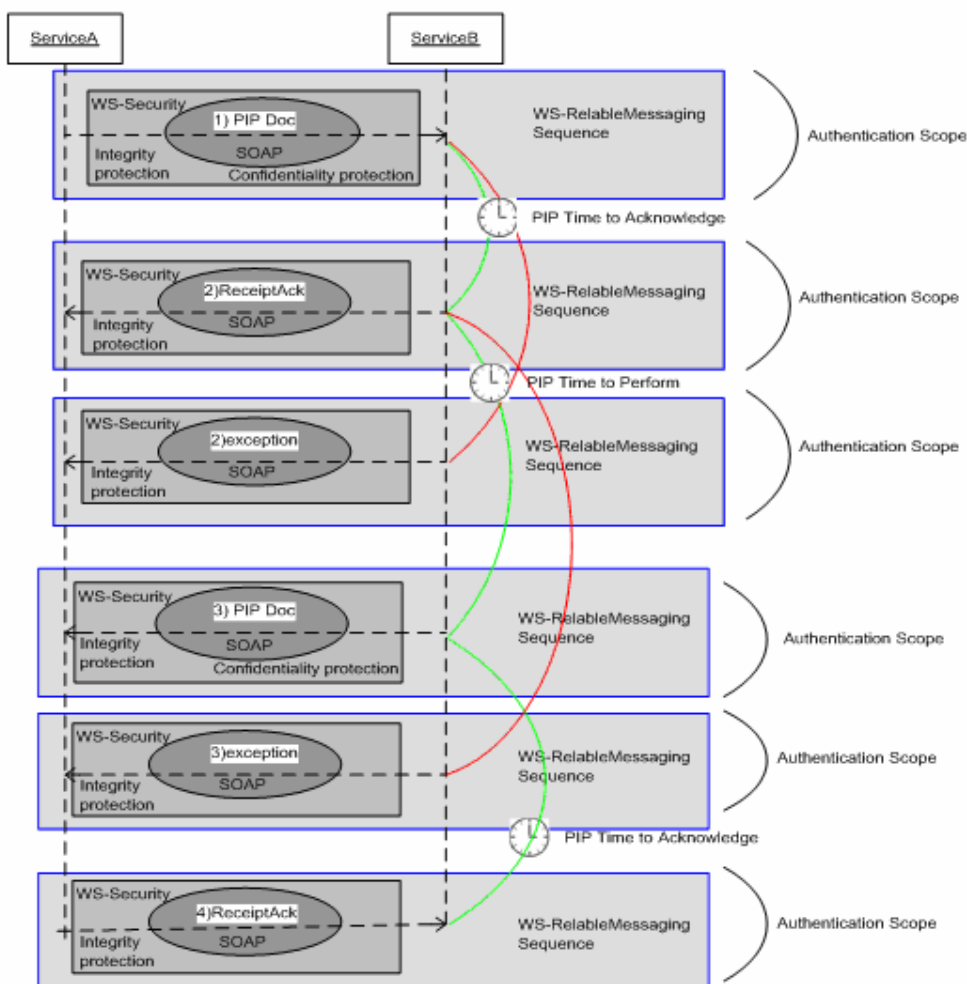
Timers are useful in measuring time and triggering actions when a specific period of time has elapsed. In these patterns, the duration of the PIP timers and the resulting actions if timer limits are reached would be agreed upon in the TPA.

タイマーは時間を測定し、一定の時間が経過した時にアクションを起動する上で有用である。これらのパターンでは、PIPタイマーの長さ及びタイマー制限に到達した場合に起こすアクションにつき、TPA(取引者間契約)の中で合意されるだろう:

5.4.1.4 QoS付の全体フロー (Overall Flow with QoS)

The following diagram defines the flow associated with this pattern.

以下の図は、このパターンに関連するフローを規定する。



In the following sequence a WS-ReliableMessaging Sequence is utilized during each exchange and integrity protection is always required.

以下の手順では、個々の交換の間でWS-高信頼メッセージング手順が利用され、つねに完全性保護が要求される:

1) Confidentiality protection is required in this exchange. ServiceA invokes ServiceB's operation accepting a RosettaNet Business Message. At completion of sending the RosettaNet Business Message by ServiceA, ServiceA starts its Time to Acknowledge clock. At acceptance of the RosettaNet Business Message, ServiceB starts its Time to Acknowledge clock.

1) この交換では機密保護が必要とされる。ServiceAは、RosettaNetビジネス・メッセージを受信するServiceBの操作を呼び出す。ServiceAがRosettaNetビジネス・メッセージの送信を完了した時点で、ServiceAはその「確認のための時間」クロックをスタートさせる。RosettaNetビジネス・メッセージを受信した時点で、ServiceBはその「確認のための時間」クロックをスタートさせる。

2) In the case of no errors, within its Time to Acknowledge clock limit, ServiceB invokes ServiceA's operation accepting the RosettaNet Receipt Acknowledgement document. At completion of sending the Receipt Acknowledgement document, ServiceB starts its Time to Perform clock. At acceptance of the Receipt Acknowledgement document, ServiceA starts its Time to Perform clock.

2) エラーがない場合、その「確認のための時間」クロック内で、ServiceBはロゼッタネット受信確認を受信するServiceAの操作を呼び出す。ServiceBは、受信確認送信を完了した時点で、その「実行のための時間」クロックをスタートさせる。ServiceAは、受信確認を受信した時点で、その「実行のための時間」クロックをスタートさせる。

In the case of errors, within its Time to Acknowledge clock limit, ServiceB invokes ServiceA's exceptionOp operation and the sequence is ended.

エラーの場合、その「確認のための時間」クロック制限内で、ServiceBはServiceAの例外処理操作(exceptionOp)を呼び出し、手順は終了する。

3) (*this text is non-normative*) At the completion of sending the ReceiptAcknowledgement, ServiceB starts its Time to Acknowledge clock. At acceptance of the ReceiptAcknowledgement, ServiceA starts its Time to Acknowledge clock.

(本ステップはRosettaNet標準ではない) 受信確認の送信を完了した時点で、ServiceBはその「確認のための時間」クロックをスタートさせる。受信確認を受信した時点で、ServiceAはその「確認のための時間」クロックをスタートさせる。

In the case of no errors, confidentiality protection is required. Within its Time to Perform clock limit, ServiceB invokes ServiceA's operation which accepts the resulting RosettaNet Business Message.

エラーがない場合には、機密保護が要求される。「実行のための時間」クロック制限内に、ServiceBはRosettaNetビジネス・メッセージの結果を受信するServiceAの操作を呼び出す。

In the case of errors, within its Time to Acknowledge clock limit, ServiceB invokes ServiceA's exceptionOp operation and the sequence is ended.

エラーの場合、その「確認のための時間」クロック制限内で、ServiceBはServiceAの例外処理操作を呼び出し、手順は終了する。

4) (*this text is non-normative*) Within its Time to Acknowledge clock limit, ServiceA invokes ServiceB's operation accepting the RosettaNet Business Acknowledgement document.

(本ステップはRosettaNet標準ではない) その「確認のための時間」クロック制限内で、ServiceAはRosettaNetビジネス確認ドキュメントを受信するServiceBの操作を呼び出す。

6 用語集 (Glossary)

Term	定義 Definition
Business Operation ビジネス・オペレーション	<p>A <i>Business Operation</i> is a web service operation that has RosettaNet defined business documents as input or output parameters.</p> <p>ビジネス・オペレーションとは、ロゼッタネット上で定義されたビジネス文書を入出力パラメータとして行うWebサービス・オペレーションである。</p>
Community WSDL コミュニティ WSDL	<p><i>Community WSDL</i> refers to an existing and approved RosettaNet WSDL document that follows the prescribed WSDL mapping rules. It serves as a template WSDL document that trading partners may use in constructing their own RosettaNet-compliant WSDL documents.</p> <p>コミュニティWSDLとは、規定されたWSDLマッピングルールに従う既存で、承認済のRosettaNet WSDL文書を指す。それは、取引先がロゼッタネットに準拠した自らのWSDLドキュメントを構築する際に使用することができるテンプレートWSDL文書として機能する。</p>
Dual Action Business Interaction 2アクションの業務やり取り	<p><i>Dual Action Business Interaction</i> is a special case of Multiple Action Business Interaction. It is an Interaction between business partners that involves exchange of two RosettaNet business document. For example, Request Purchase Order interaction involves exchange of two RosettaNet business documents i.e. Purchase Order Request from buyer to seller, and PurchaseOrderConfirmation from seller to buyer.</p> <p>2アクションの業務やり取りとは、複数アクションの業務やり取りの特別な例である。それは、2つのRosettaNetビジネス文書の交換を含む取引先間のやりとりである。例えば、発注要求のやりとりには、2つのRosettaNetビジネス文書、即ちバイヤーからセラーへの「注文依頼」、及びセラーからバイヤーへの「注文確認」の交換が伴う。</p>
Hosting-Enabled Partner ホスティング対応パートナー	<p>A <i>hosting-enabled partner</i> is a business partner that has full Web service capabilities, supporting the full set of the specifications and standards listed earlier in the background section. It can host a Web service, and provide reliable, secure interactions using the relevant Web services specifications. A hosting-enabled business partner cannot invoke a pure-client.</p> <p>ホスティング対応パートナーとは、包括的なWebサービス機能を有し、前記の背景のセクションに記載した仕様及び標準の全セットをサポートしている。このパートナーはWebサービスをホストすることができ、該当するWebサービス仕様を使った信頼できる安全なやりとりを提供できる。ホスティング対応ビジネス・パートナーは、ピュア・クライアントを呼び出すことができない。</p>
Multiple Action Business Interaction 複数アクションの業務やり取り	<p><i>Multiple Action Business Interaction</i> is an Interaction between business partners that involves exchange of more than one RosettaNet business document. For example, procurement process could involves exchange of several RosettaNet business documents e.g. Purchase Order Request from buyer to seller, PurchaseOrderConfirmation from seller to buyer, PurchaseOrderStatusNotification from seller to buyer etc.</p> <p>複数アクションの業務やり取りとは、複数のRosettaNetビジネス文書の交換が伴うビジネスパートナー間のやりとりである。例えば、調達プロセスにはいくつかのRosettaNetビジネス文書(バイヤーからセラーへの「発注依頼」、セラーからバイヤーへの「発注確認」、セラーからバイヤーへの「発注状況通知」など)の交換を伴う可能性がある。</p>

<p>Pure Client</p> <p>ピュア・クライアント</p>	<p>A <i>pure client</i> does not host services and cannot be invoked itself as a service. It can have varying Web service capabilities supporting at least the minimal set of specifications and standards listed earlier in the background section.</p> <p>ピュア・クライアントとは、ホストサービスを提供せず、それ自体サービスとして呼び出されることはない。前記の背景のセクションに記載された規格・基準の少なくとも最小セットをサポートしている多様なWebサービス機能を有する可能性がある。</p>
<p>Role Type</p> <p>役割タイプ</p>	<p><i>Role Type</i> is the type of role that performs activities in an e-Business process e.g. Sold to, Sold by, Distributed by etc. Valid PIP Roles are specified in the PIP description provided by RosettaNet (e.g. DescriptionOfPartnerInterfaceProcessFor3A4.doc)</p> <p>役割タイプとは、例えば「販売先」、「販売者」、「配給業者」等、e-ビジネス・プロセスにおける業務を遂行する役割のタイプである。「Valid PIP Roles」は、RosettaNetによって提供されるPIPの記述において指定される。(例、DescriptionOfPartnerInterfaceProcessFor3A4.doc)</p>
<p>Single Action Business Interaction</p> <p>1アクションの業務やり取り</p>	<p><i>Single Action Business Interaction</i> is an Interaction between business partners that involves exchange of a single RosettaNet business document. For example, to Distribute Order Status, seller sends a single RosettaNet business document (i.e. <i>PurchaseOrderStatusNotification</i>) to buyer.</p> <p>1アクションの業務やり取りとは、1つのRosettaNetビジネス文書の交換が伴うビジネス・パートナー間のやりとりである。例えばセラーは、「注文状況の通知」を送付のために、バイヤーに単一のRosettaNetビジネス文書を送信する。(例 PurchaseOrderStatusNotification)</p>
<p>Signal Operation</p> <p>シグナル・オペレーション</p>	<p>A <i>Signal Operation</i> is used to refer to following two operations: ReceiptAcknowledgmentOp, and ExceptionOp</p> <p>シグナル・オペレーションは、次の2つの操作を指示するのに使用される。ReceiptAcknowledgmentOp (受信確認操作)とExceptionOp (例外処理操作)である。</p>
<p>Signal Schema</p> <p>シグナル・スキーマ</p>	<p>A <i>Signal Schema</i> is used to refer to following three schemas: ReceiptAcknowledgment_00_01.xsd, WS_Exception_00_01.xsd, and WS_GetMessage_00_01.xsd. These schemas are located in ./system/sub directory.</p> <p>シグナル・スキーマとは、次の3つのスキーマを指すのに使用される。</p> <p>受信確認スキーマ ReceiptAcknowledgment_00_01.xsd WS 例外処理スキーマ WS_Exception_00_01.xsd WS メッセージ取得スキーマ WS_GetMessage_00_01.xsd. これ等は、./system/sub directory に保存されている。</p>
<p>Trading Partner Agreement (TPA)</p> <p>取引者間契約 (TPA)</p>	<p><i>Trading Partner Agreement (TPA)</i> is an agreement by two or more business partners. When this Profile does not specify something or only provides guidance, the TPA should be used to capture the integration requirements.</p> <p>取引者間契約 (TPA) は、2社又はそれ以上の取引先による契約である。本プロファイルが特別に何かを規定せず、ただガイダンスのみを行う場合、TPAが統合要件を取り込むために使用されるべきである。</p>

7 付録 A: 参照 (Appendix A: References)

Source	Description
[MCC]	Title: Message Choreography and Control RosettaNet Retrieved July 29, 2008 from: http://members.rosettanet.org/Standards/RosettaNetPrograms/FoundationalPrograms/FormingFoundationalPrograms/MessageControlChoreography/tabid/3096/Default.aspx
[MTOM]	Title: SOAP Message Transmission Optimization Mechanism W3C Recommendation 25 January 2005 Retrieved June 20, 2008 from: http://www.w3.org/TR/soap12-mtom/
[RAE]	Title: RosettaNet Automated Enablement RosettaNet Retrieved June 20, 2008 from: http://www.rosettanet.org/cms/sites/RosettaNet/Standards/Programs/milestone/completed/rae/index.html
[RFC2119]	Title : Key words for use in RFCs to Indicate Requirement Levels The Internet Engineering Task Force Retrieved June 20, 2008 from: http://www.ietf.org/rfc/rfc2119.txt
[SOAP11]	Title: Simple Object Access Protocol (SOAP) 1.1 World Wide Web Consortium (W3C) Retrieved June 20, 2008 from: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
[SOAP12]	Title: SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) World Wide Web Consortium (W3C) Retrieved June 20, 2008 from: http://www.w3.org/TR/soap12/
[SSL]	Title: The SSL Protocol Version 3.0 Netscape Communications Retrieved June 20, 2008 from: http://wp.netscape.com/eng/ssl3/draft302.txt
[TLS]	Title: The TLS Protocol Version 1.0 The Internet Society and The Internet Engineering Task Force Retrieved June 20, 2008 from: http://www.ietf.org/rfc/rfc2246
[TPIR-PIP]	Title: TPIR-PIP® Core Specification RosettaNet Retrieved June 20, 2008 from: http://www.rosettanet.org/cms/sites/RosettaNet/Standards/RStandards/tpir/index.html
[WSAddressing]	Title: Web Services Addressing 1.0 - Core World Wide Web Consortium (W3C) Retrieved June 20, 2008 from: http://www.w3.org/TR/ws-addr-core/
[WSDL]	Title: Web Services Description Language (WSDL) 1.1 World Wide Web Consortium (W3C) Retrieved June 20, 2008 from: http://www.w3.org/TR/wsdl
[WSI]	Web Services Interoperability Organization Retrieved June 20, 2008 from: http://www.ws-i.org/
[WSIBP]	Title: Basic Profile Version 1.1 Web Services Interoperability Organization Retrieved June 20, 2008 from: http://www.ws-i.org/Profiles/BasicProfile-1.1.html
[WSIBSP]	Title: Basic Security Profile Version 1.0 Web Services Interoperability Organization Retrieved June 20, 2008 from: http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html
[WSRM]	Title: Web Services Reliable Messaging (WS-ReliableMessaging) OASIS Retrieved July 02, 2008 from: http://docs.oasis-open.org/ws-rx/wsrn/200702
[WSSSOAP]	Title: Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) OASIS Retrieved June 20, 2008 from: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

[WSSUP]	Title: Web Services Security: UsernameToken Profile 1.0 OASIS Retrieved June 20, 2008 from: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf
[WSSX509P]	Title: Web Services Security: X.509 Certificate Token Profile 1.0 OASIS Retrieved June 20, 2008 from: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf
[WSPolicy]	Title: WS-Security Policy 1.2 OASIS Retrieved July 02, 2008 from: http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702
[WSSecurityPolicy]	Title: Web Services Policy 1.5 - Framework W3C Retrieved July 02, 2008 from: http://www.w3.org/TR/2007/REC-ws-policy-20070904/
[WSPolicyAttachment]	Title: Web Services Policy 1.5 - Attachment W3C Retrieved July 02, 2008 from: http://www.w3.org/TR/2007/REC-ws-policy-attach-20070904/
[WSRMPolicy]	Title: Web Services Reliable Messaging Policy Assertion (WS-RM Policy) OASIS Retrieved July 02, 2008 from: http://docs.oasis-open.org/ws-rx/wsrmp/200702
[XML]	Title: W3C Extensible Markup Language 1.0 (Third Edition) World Wide Web Consortium (W3C) Retrieved June 20, 2008 from: http://www.w3.org/TR/REC-xml/
[XMLSchemaLanguage]	Editors : Henry S. Thompson, David Beech, Murray Maloney, Noah Mendelsohn Title : "XML Schema Part 1: Structures" World Wide Web Consortium Retrieved October 20, 2003 from: http://www.w3.org/TR/xmlschema-1/ Editors : Paul V. Biron, Ashok Malhotra Title : "XML Schema Part 2: Datatypes" World Wide Web Consortium Retrieved October 20, 2003 from: http://www.w3.org/TR/xmlschema-2/

8 付録 B: 使用事例 (Appendix B: Example Use Cases)

8.1 サービス・ツー・サービス (Service to Service)

8.1.1 サービス・ツー・サービス一方向コールバック使用事例 (Service to Service One Way Callback Use Cases)

8.1.1.1 PIP 3A4: 発注の要求 (Request Purchase Order)

1. Within the Buyer's private process, Buyer enters rest of purchase order information (shipping, PO # etc.) in Buyer application.
1. バイヤーのプライベート・プロセスにおいて、バイヤーは自社システムに残りの発注情報 (出荷、PO # 等)を入力する。
2. Buyer presses send purchase order button.
2. バイヤーは、発注情報送信ボタンを押す。
3. Buyer application triggers the sending of a one way soap message containing purchase order request XML to the Seller Web service.
3. バイヤー側のシステムは、セラー側の Web サービスへ発注の XML (PIP 3A4 Request) を含む一方向 SOAP メッセージ送信処理を起動する。
4. Initiating connection closes without response.
4. 起動したセッションは、応答無しで終了する。
5. Seller Web service performs schema validation.
5. セラー側の Web サービスは、スキーマ・バリデーションを実行する。
6. If schema validation succeeds: Seller Web service stores purchase order. It then sends a one way soap message containing purchase order confirmation XML, with pending status, to the Buyer Service. Buyer service sends it to the Buyer's private process where it processes the purchase order confirmation, and updates purchase order status to pending.
6. スキーマ・バリデーションでエラーがなかった場合: セラー側の Web サービスは注文を保存する。次に、バイヤー側の Web サービスへステータスが保留状態の発注確認の XML (PIP 3A4 Confirmation) の一方向 SOAP メッセージを送信する。バイヤー側の Web サービスは発注確認の処理を行うプライベート・プロセスに PIP3A4 Confirmation の情報を送り、ステータスを保留状態に更新する。

8.2 ピュア・クライアント・ツー・サービス (Pure Client to Service)

8.2.1 ピュア・クライアント・ツー・サービス要求応答での使用事例 (Pure Client to Service Request Response Use Cases)

8.2.1.1 PIP 3A5: 注文状態の照会 (Query Order Status)

1. Buyer enters purchase order sales order # in Buyer application.
1. バイヤーは、自社システムに、購買注文# を入力する。
2. Buyer application queries Seller Web services for order status of the given sales order.
2. バイヤー側のシステムは、指定されたセールスオーダーの注文状況をセラー側の Web サービスに問い合わせる。
3. Seller Web service performs schema validation, looks up order status, and returns order status XML response synchronously as part of HTTP response.

3. セラー側の Web サービスは、スキーマ・バリデーションを実行し、注文状況を検索し、そして HTTP レスポンスの一部として、同期させて注文状況 XML 応答を返す。

4. Buyer application displays order status.

4. バイヤー側のシステムは、注文状況を表示する。

8.2.1.2 PIP 3A2: 価格と入手可能性の要求 (Request Price and Availability)

1. Buyer enters product names in Buyer application (e.g. custom or packaged application).

1. バイヤーは、自社システム(例: 独自構築のシステム又はパッケージ・アプリケーション)に製品名を入力する。

2. Buyer application queries Seller Web services for prices and availability.

2. バイヤーのシステムは、価格及び入手可能性について、セラーWeb サービスに問い合わせる。

3. Seller Web service performs schema validation, looks up pricing and availability, and returns pricing and availability XML response synchronously as part of HTTP response.

3. セラーWeb サービスは、スキーマ・バリデーションを実行し、価格及び入手可能性を検索し、そして HTTP レスポンスの一部として、同期させて料金及び入手可能性 XML 応答を返す。

4. Buyer application displays pricing and availability information.

4. バイヤーのシステムは、価格及び入手可能性情報を表示する。

8.2.1.3 PIP 3A1: 見積りの要求 (Request Quote)

1. Buyer enters rest of information to request quote (billing, and contract information etc.) in Buyer application.

1. バイヤーは、自社システムに見積価格を要求するために残りの情報(請求書及び契約情報等)を入力する。

2. Buyer application requests quote from Seller Web services.

2. バイヤーのシステムは、セラーWeb サービスに見積の要求をする。

3. Seller Web service performs schema validation, creates quote, and returns quote XML response synchronously as part of HTTP response.

3. セラーWeb サービスは、スキーマ・バリデーションを行い、見積書を作成し、HTTP レスポンスの一部として同期させて、見積り書の XML 応答を返す。

4. Buyer application converts the quote to a purchase order.

4. バイヤーのシステムは、見積り書を注文書に変換する。

8.2.2 プッシュ型ピュア・クライアント・ツー・サービス要求/応答の使用事例 (Pure Client to Service Request Response Push Use Cases)

8.2.2.1 PIP 3A7: 発注更新の通知 (Notify Of Purchase Order Update)

After reviewing the buyer's PO (3A4R) or PO change (3A8R), the seller responds to the buyer with the Notify of PO update (3A7).

バイヤーの発注要求 (PIP 3A4 Request)、又は発注変更の要求 (PIP 3A8 Request) を検討した後に、セラーは、発注更新の通知(3A7) をバイヤーに返信する。

1. Seller pushes Notify of Purchase Order Update (3A7) message to the Buyer service.

1. セラーは、発注更新の通知 (3A7) メッセージをバイヤー側の Web サービスに配信する。

2. Buyer performs schema validation and can optionally perform additional validations of the message as needed.

2. バイヤーは、スキーマバリデーションを行い、オプションとして必要に応じて、メッセージの追加バリデーションを実行することが出来る。

3. If (schema) validation succeeds: Buyer stores PO Update and then Buyer returns an acknowledgement in the HTTP response to the seller confirming the receipt/acceptance of the message.

3. (スキーマ)バリデーションでエラーがなかった場合: バイヤーは発注更新を格納し、次にバイヤーはセラーに、HTTP レスポンスでメッセージの受領/承諾を確認する確認メッセージを返信する。

8.2.2.2 PIP 3C3: 請求書の通知 (Notify of Invoice e)

After seller satisfies all or part of the PO

セラーは、発注の全部、又は一部を充足させた後、

1. Seller pushes Notify of Invoice message to the Buyer service.

1. セラーは、請求書の通知情報をバイヤーのWebサービスに配信する。

2. Buyer performs schema validation and can optionally perform additional validations of the message as needed.

2. バイヤーは、スキーマバリデーションを行い、任意で必要に応じてメッセージの追加バリデーションを実施することが出来る。

3. If (schema) validation succeeds: Buyer stores Invoice and then Buyer returns an acknowledgement in HTTP response to the seller confirming the receipt/acceptance of the message.

3. スキーマバリデーションでエラーがなかった場合: バイヤーは請求書を保管し、次にセラーに、HTTPレスポンスでメッセージの受領/承諾の確認をする確認メッセージを返信する。

8.2.2.3 PIP 3A4: 発注の要求 (Request Purchase Order)

1. Buyer enters rest of purchase order information (shipping, PO # etc.) in Buyer application.

1. バイヤーは、自社システムに残りの発注情報(出荷、PO # 等)を入力する。

2. Buyer presses send purchase order button.

2. バイヤーは、発注情報送信ボタンを押す。

3. Buyer application sends purchase order request XML to Seller Web service.

3. バイヤーのシステムは、セラーWebサービスに発注要求XMLを送信する。

4. Seller Web service performs schema validation.

4. セラーWebサービスは、スキーマバリデーションを実行する。

5. If schema validation succeeds: Seller Web service stores purchase order. It returns purchase order confirmation XML, with pending status, in HTTP response and then Buyer application processes the purchase order confirmation, and updates purchase order status to pending.

5. スキーマバリデーションでエラーがなかった場合: セラーWebサービスは注文を保存する。HTTP応答でステータスが保留状態の注文確認用XMLメッセージを返信する。次に、バイヤーのシステムは注文確認メッセージを処理し、注文データのステータスを保留状態に更新する。

8.2.3 プル型ピュア・クライアント・ツー・サービス要求 / 応答の使用事例 (Pure Client to Service Request Response Pull Use Cases)

8.2.3.1 PIP 3C4: 請求書拒否の通知 (Notify of Invoice Reject)

1. Out of band, the Buyer rejects the invoice received through their ERP system and generates a RosettaNet compliant XML Notify of Invoice Reject message.

1. バイヤーは、自社ERPシステムを経由して受信した請求書を拒否し、RosettaNet対応の「請求書拒否の通知」用XMLメッセージ(PIP 3C4)を生成する。

2. Seller application pulls Buyer Web service for the Notify Of Invoice Reject message.

2. セラー・アプリケーションは、請求書拒否の通知メッセージのため、バイヤーWebサービスから情報を取得する。

3. Seller performs schema validation on returned invoice reject message.

3. セラーは、返信された請求書拒否の通知メッセージについてスキーマ・バリデーションを行なう。

4. If schema validation succeeds: Seller stores Notify Of Invoice Reject message and then Seller pushes an acknowledgement message to the Buyer service confirming the receipt of the Notify of Invoice Reject message. The Buyer will update their systems with the notation that the Notify of Invoice Reject was acknowledged by the Seller. The pushed acknowledgement message from the seller is not "acked" and nothing is returned in the transport response.

4. スキーマ・バリデーションでエラーがなかった場合: セラーは、請求書拒否の通知メッセージを保存し、次に、請求書拒否の通知メッセージの受領を確認する確認メッセージをバイヤー・サービスへ配信する。バイヤーは、セラーによって請求書拒否の通知メッセージが確認された旨を記録するためシステムを更新する。セラーからの配信された確認メッセージは、“承認を意味した”ものではなく、又、輸送層応答での返信は一切ない。

8.2.3.2 PIP 3B2: 事前の出荷通知 (Advanced Ship Notification)

When the seller is ready to ship one or more line items from a PO or updated PO, they notify buyer with an Advanced Ship Notification (3B2).

セラーは、1つまたは複数行のPO、又は、更新されたPOの出荷の用意ができた場合、バイヤーに対し、事前の出荷通知(3B2)を、通知する。

1. Seller pushes Advanced Ship Notification message to the Buyer service.

1. セラーは、事前の出荷通知をバイヤー・サービスへ配信する。

2. Buyer performs schema validation and can optionally perform additional validations of the message as needed.

2. バイヤーは、スキーマ・バリデーションを行い、任意で必要に応じて、メッセージの追加バリデーションを実施することが出来る。

3. If (schema) validation succeeds: Buyer stores ASN and then Buyer returns an acknowledgement in HTTP response to the seller confirming the receipt/acceptance of the message.

スキーマ・バリデーションでエラーがなかった場合: バイヤーは事前の出荷通知を保管し、次にセラーに、HTTPレスポンスでメッセージの受領/承諾の確認をする確認メッセージを返信する。

8.2.3.3 PIP 3A4: 発注の要求 (Request Purchase Order)

1. Out of band, the Buyer initiates a purchase order through their ERP system and generates a RosettaNet compliant XML PO Request.

1. バイヤーは、自社のERPシステムを使用して発注を開始し、RosettaNet対応の「発注依頼」用XMLメッセージを生成する。

2. Seller application pulls Buyer Web service for purchase order request.

2. セラーのシステムは、発注依頼に対してバイヤーWebサービスから情報を取得する。

3. Seller performs schema validation on returned purchase order request.

3. セラーは、返信された発注依頼に対して、スキーマバリデーションを実行する。

4. If schema validation succeeds: Seller stores purchase order and then Seller pushes an acknowledgement message to the Buyer service confirming the receipt of the PO. The Buyer will update their systems with a pending PO status. The pushed acknowledgement message from the seller is not "acked" and nothing is returned in the transport response. スキーマバリデーションでエラーがなかった場合: セラーは発注書を保管し、次に、バイヤーのWebサービスにPOの受領を確認する確認メッセージを返信する。バイヤーは、PO保留状態でシステムを更新する。セラーの呼び出し確認メッセージは、「承認された」ものではなく、トランスポート層応答での返信は一切ない。

8.2.3.4 PIP 3A8: 発注変更の要求 (Request Purchase Order Change)

1. Out of band, the Buyer initiates a purchase order update through their ERP system and generates a RosettaNet compliant XML PO Change Request.

1. バイヤーは、自社のERPシステムを通じて発注の更新を開始し、RosettaNet対応の発注変更要求のXMLメッセージを生成する。

2. Seller application pulls Buyer Web service for purchase order change request.

2. セラーのシステムは、バイヤーのWebサービスから「発注変更の要求」を引き取る。

3. Seller performs schema validation.

3. セラーは、スキーマバリデーションを実行する。

4. If schema validation succeeds: Seller stores purchase order change request and then Seller pushes an acknowledgement message to the Buyer service confirming the receipt of the PO change. The Buyer will update their systems with a pending status for the PO change request. The pushed acknowledgement message from the seller is not "acked" and nothing is returned in the transport response.

4. スキーマバリデーションでエラーがなかった場合: セラーは発注変更を保管し、次に、バイヤーのWebサービスに発注変更の受領を確認する確認メッセージを返信する。バイヤーは、発注変更の要求を保留状態に更新する。セラーからの確認配信メッセージは、「承認された」ものではなく、トランスポート層応答での返信は一切ない。

9 付録C: 本プロファイルに特有のスキーマ (Appendix C: Schemas Specific To This Profile)

The following schemas can be found inside the profile package. Receipt Acknowledgment and Exception schema are required since MMS Web Services only uses schema (and not DTDs)

以下のスキーマは、プロファイルのファイル内に存在する。MMS Web サービスはスキーマ(DTDsではない)だけを使用するので、受信確認及び例外処理のスキーマが必要である。

- XML\System\ReceiptAcknowledgment_00_01.xsd
- XML\System\WS_Exception_00_01.xsd
- XML\System\CodeList\WS_MessageError_00_01.xsd
- XML\System\WS_GetMessage_00_01.xsd

9.1 受信確認スキーマ (ReceiptAcknowledgment_00_01.xsd)

The schema is created by converting RNIF Receipt Acknowledgment DTD to XML Schema. RNIFにおけるDTD版のReceipt Acknowledgement をXML Schema に変換することによって、スキーマは作成される。

9.2 WS例外処理スキーマ (WS_Exception_00_01.xsd)

The schema is created by converting RNIF Exception DTD to XML Schema. Note the following information which cannot be enforced within the schema. RNIFにおけるDTD版のException をXML Schemaに変換することによって、スキーマは作成される。当該スキーマ内で実行できない以下の情報に注意すること。

There are five Error Codes which are further classified as one of the two Exception Types - GEE (General Error), or RAE (Receipt Acknowledgement Error). 2つの例外タイプ、GEE(一般エラー)、又はRAE(受信確認エラー)の1つに、さらに分類される5つのエラーコードがある。

The Exception\Type element of the WS_Exception_00_01.xsd is used to specify the Exception type. Exception\Description\Error element is used to specify the Error code. 例外タイプを指定するために、WS_Exception_00_01.xsdのException\Type 要素が使用される。エラーコードを指定するために、Exception\Description\Error要素が使用される。

9.2.1 GEE (一般エラー) (General Error)

General.Error: This is catch all. If no other errors are appropriate to the implement, this error can be raised. This is similar to RosettaNet defined error: PRF.ACTN.GENERR: Error during action performance.

General.Error: (一般エラー): これは汎用である。他のエラーの全てが当該実装に適合しない場合、このエラーが発生した可能性がある。これは、RosettaNetで定義される'PRF.ACTION.GENERR'(アクション実行中のエラー)と同様のものである。

Business.Rule.Error: This should be used for any error encountered while validating against any custom business rule. This is not for schema validation errors.

Business.Rule.Error: (ビジネス規則のエラー): これは、一切のカスタム・ビジネス・ルールに対する

バリデーション中に検出された全てのエラーに使用されるべきである。これは、スキーマ・バリデーション時のエラーではない。

Content.Not.Available: It is generated for Pure Client Request Response Pull MEP when the service does not find response content.

Content.Not.Available: (コンテンツが利用できない): これは、サービスが応答コンテンツを見つけられない時、プル型ピュア・クライアント要求 / 応答ピュア・クライアントメッセージ交換パターン用に生成される。

Duplicate.MessageID: When WS-Addressing:MessageID is used in retries in the pure client scenarios duplicate messages can be detected. If duplicate message is detected by the service, then it uses this error code.

Duplicate.MessageID: (重複メッセージID): WS-AddressingのMessageID がピュア・クライアントのシナリオのリトライで使用される時、重複メッセージが検出される場合がある。重複メッセージがサービスによって検出される場合、このエラーコードを使用する。

9.2.2 RAE (受信確認エラー) (Receipt Acknowledgement Error)

Schema.Validation.Error: This is used when the schema validation failed. This is similar to RosettaNet defined error: UNP.SCON.VALERR: Error during unpackaging – Validating the Service Content.

Schema.Validation.Error: (スキーマ・バリデーション・エラー): スキーマ・バリデーションで失敗した時に使用される。これは、RosettaNetで定義される 'UNP.SCON.VALERR' (アンパッキング中のエラー - サービスコンテンツの検証)と同様のものである。

9.3 WSメッセージエラースキーマ (WS_MessageError_00_01.xsd)

This defines the error codes for the exception schema.
これは、例外処理スキーマ用のエラーコードを定義する。

9.4 WSメッセージ取得スキーマ (WS_GetMessage_00_01.xsd)

This schema is used in pure client to service request response pull. It is the template input schema for the MEP.

このスキーマは、プル型ピュア・クライアント・ツー・サービス要求 / 応答で使用される。メッセージ交換パターン用のテンプレート入力スキーマである。