

Message Control and Choreography (MCC) Profile-Applicability Statement 2 (AS2)

確定 V 11.00.00

| 仕様書情報 | |
|-----------|---------------------------------------|
| 名前 | MCC – プロファイル AS2 MCC – Profile-AS2 |
| 公開日 | 2011年4月13日 |
| Version情報 | V11.00.00 |

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。
又、翻訳文への疑問点、訂正箇所等お気づきの場合には、RNJ事務局まで、Mailにてご連絡頂ければ幸いです。
翻訳品質向上に向け、ご協力をお願い致します。

目次

| | | |
|----------|--|-----------|
| 1 | ドキュメント管理 (Document Management) | 3 |
| 1.1 | 免責事項 (Legal Disclaimer)..... | 3 |
| 1.3 | 商標 (Trademarks)..... | 3 |
| 1.4 | 謝辞 (Acknowledgments)..... | 3 |
| 1.5 | 関連ドキュメント (Related Documents)..... | 4 |
| 1.6 | ドキュメントのバージョン履歴 (Document Version History) | 4 |
| 1.7 | 文書の目的 (Document Purpose) | 4 |
| 2 | 一方向ビジネス文書用 PIP 定義と要件 (Single Business Document PIP Definition and Requirements) | 5 |
| 2.1 | 一方向ビジネス文書テンプレート (Single business document Template) | 7 |
| 2.1.1 | 関係者 (Parties involved) | 7 |
| 2.1.2 | ビジネス文書 (Business Document) | 8 |
| 2.1.3 | ビジネス状態に関する合意の特徴 (Business State Alignment features) | 9 |
| 2.2 | PIP 実行結果 (PIP execution outcome) | 12 |
| 2.3 | QoS (サービス品質) の特徴 (Quality of Service Features) | 12 |
| 3 | PIP パラメータ化と実行管理 (PIP Parameterization and Execution Control) | 16 |
| 3.1 | PIP プロパティ・パラメータ (PIP Property Parameters) | 17 |
| 3.2 | PIP 実行形式と関連パラメータ (PIP execution modes and related parameters)..... | 19 |
| 3.3 | PIP インスタンス相関関係及び識別 (PIP Instance Correlation and Identification) | 19 |
| 3.3.1 | PIP の識別 (PIP Identification)..... | 19 |
| 3.3.2 | メッセージの相関関係 (Message Correlation) | 20 |
| 4 | PIP 明確化の事例 (Use Cases of PIP definition) | 21 |
| 4.1 | 事例 1 全て包括 (Use Case 1 – Full features)..... | 21 |
| 4.2 | 事例 2 ビジネス文書のみ (Use Case 2 – Business Document Only) | 22 |

1 ドキュメント管理 (Document Management)

1.1 免責事項 (Legal Disclaimer)

RosettaNet™ 及びそのメンバー、職員、管理者、従業員、代理店は、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。

1.2 著作権 (Copyright)

©2011 RosettaNet. All rights reserved. 本書の一部あるいは全部について、この著作権告示を含むことなく、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、あるいは転送を行うことを禁じる。いかなる派生物にも著作権告示を特記しなければならない。本出版物の一般への再配布または販売、あるいは派生作業を行う前には、出版元からの文書による許諾が必要である。

1.3 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。

1.4 謝辞 (Acknowledgments)

本書は、RosettaNet (<http://www.rosettanet.org/>) により準備されたものであり、マイルストーンプログラムにおいて集められたRosettaNet メソッドロジへの適合要件に基づくものである。この PIP の設計及び開発に携わった法人は次の通りである。

| | |
|---------------------------------|--------------------|
| Axway | Cisco |
| DHL | IBM |
| KJC Solutions | Oracle |
| OASIS | Software AG |
| Tibco | University Bamberg |
| Vienna University of Technology | |

1.5 関連ドキュメント (Related Documents)

- MCC Single Business Document PIP Template V11.00.00

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

| バージョン | 日付 | 解説 |
|-------------------|------------|-------|
| リリース版 R 11.00.00A | 2010年8月16日 | リリース版 |
| 確定版 V 11.00.00 | 2011年4月13日 | 確定版 |

1.7 文書の目的 (Document Purpose)

文書の目的は、一般の読者(非技術者)に、構造、オブジェクト間の関係、オブジェクトの内容、要素の定義等を説明することである。

2 一方向ビジネス文書用PIP定義と要件 (Single Business Document PIP Definition and Requirements)

The “Single Business Document Template” section defines a model for single business document PIPs that is aligned with ebBP Single business document Business Transactions. It is abstract in two different ways:

“一方向ビジネス文書PIP用テンプレート“Single Business Document Template”の章は、ebMS ビジネス文書‘Business Transactions（商取引）’と連携し、一方向ビジネス文書用PIPのためのモデルを定義する。これは、2つの異なる方法において抽象的である。

1. The realization of a PIP definition component may vary with the communication technology selected for implementing the PIP.

PIP の明確化は、PIP の実装に対して選定される通信技術によって、異なる可能性がある。

2. The realization of a PIP definition may vary depending on the execution context assumed.

PIP の明確化は、想定される実行コンテキストによって、異なる可能性がある。

Also, the template for Single Business Document PIP definition is general in the sense that the definition of a concrete PIP will select from the model components offered. Section “Execution Parameters and Configuration” therefore describes rules for defining a customized, or “concrete” PIP.

又、一方向ビジネス文書PIP明確化用のテンプレートは、実際のPIPが提供されたモデル部分から選択するという意味で一般的である。従って、“Execution Parameters and Configuration(パラメータ実行と構成)”の章は、カスタマイズされた、又は、“実際の”PIPを明確化するルールを記載する。

To summarize, there are four levels at which PIP material is defined:
要約すると、PIP構成要素を明確化する4つのレベルがある：

- (1) PIP template: This level defines the general structure – or model - of a PIP and the features that may be used in a particular PIP definition. This is the object of this document.

PIPテンプレート: このレベルは、PIPの一般構成 -又はモデル- 及び特定のPIPの明確化で使用されるであろう機能を定義する。これがこの文書の目的である。

- (2) PIP definition: This level defines particular PIPs usable for business exchanges. These will usually contain parameters that are left for users to define, e.g. via an agreement between members of a supply chain. A PIP definition is prescriptive and states the conditions for a PIP instance to be considered conforming to a PIP definition.

PIPの明確化: このレベルはビジネス情報交換で使用可能な特定のPIPを明確化する。これらは、通常、ユーザーが決めて良い - 例えば、サプライチェーンのメンバー間の合意を介して - パラメータを含む。PIPの明確化は規範的であり、PIPの明確化に従うPIPインスタンスを記載する。

- (3) Customized PIP: (or concrete PIP): At this level, all elements of a PIP are fully defined, and all parameters (such as QoS, timing) are given a specific value or specific range that is agreed between partners. The execution of such PIPs is determined in terms of QoS, alignment features and execution mode. The factors that condition a successful or a failed outcome are fully determined and known from partners.

カスタマイズされた PIP: (又は実際の PIP): このレベルでは、PIP の全ての要素が完全に明確になり、全てのパラメータ (QoS、タイミング等)はパートナー間で合意される特定の値、又は特定の範囲値として与えられる。当該 PIP の実行は、QoS、合意に関する機能及び実行モードの観点から決定される。成功、又は失敗の結果を条件付ける要因は、全てパートナー間で決定されて知らされる。

- (4) PIP instance: This is an image of a particular execution of a PIP, i.e. a particular sequence of concrete messages where all components and PIP properties are given a value – e.g. a fully defined business document between two identified partners, a particular timing between these messages, etc.

PIPインスタンス: これは、PIPの特別な実行のイメージ、即ち、全てのコンポーネント及びPIP属性が値を与えられる具体的なメッセージの特定のシーケンスである。例えば、2つの特定されたパートナー間の完全に定義されたビジネス文書、これらのメッセージ間の特定のタイミングなどである。

2.1 一方向ビジネス文書テンプレート (Single business document Template)

2.1.1 関係者 (Parties involved)

In RosettaNet there is the concept of “Party and “Role”
RosettaNetにおいては、“関係者”と“役割”について、概念がある。

- The PIP requester party (or Requester), sending the Single Business Document message
PIPで要求する人々 (又は、要求者) は、一方向ビジネス文書メッセージを送る。
- The PIP responder party (or Responder), receiving the Single Business Document message
PIPで返信する人々 (又は、返信者) は、一方向ビジネス文書メッセージを受け取る。

Properties that are associated with each party are:

各パーティに連携する属性:

- Requester role for the PIP (specific to a PIP definition).
PIPに対する要求者の役割 (PIPの明確化に特定)
- Responder role for the PIP (specific to a PIP definition).
PIPに対する返信者の役割 (PIPの明確化に特定)

The “Party ID” associated with each role (varies across instances of the same PIP definition)

各役割に関連した”パーティ ID”(同じPIPでも、インスタンスはパーティIDが追加されるので異なる)

- The PIP Business Document contains two structures “fromRole” and “toRole“, that contain the following definitions:
PIPビジネス文書は、2つの構造“fromRole”と“toRole”構造を含んでおり、以下の定義がされる。
 - Party: <GlobalBusinessIdentifier> 123456789
 </GlobalBusinessIdentifier>
 - Role: <GlobalPartnerRoleClassificationCode>Buyer
 </GlobalPartnerRoleClassificationCode>
- The RosettaNet Implementation Framework (RNIF) contains:
 - Service and Delivery Header contains:
 <GlobalBusinessIdentifier> 123456789
 </GlobalBusinessIdentifier>
 - Service Header contains:
 <GlobalPartnerRoleClassificationCode>Buyer
 </GlobalPartnerRoleClassificationCode>

The "Party / Role" would not be used for the AS2 exchange. AS2 is defined to be independent of any business intelligence. Concepts such as business roles are not supported. The sender and intended receiver of a document exchanged using AS2 are identified by AS2-specific HTTP headers, which are prepended to the data being exchanged. The header "AS2-From" is used to identify the sender of a message and the header "AS2-To" is used to identify the intended recipient of a message.

"Party / Role"は、AS2の交換用には使用されない。AS2は、いかなるビジネス・インテリジェンスとも無関係であるように定義される。ビジネス上の役割のような概念はサポートしない。AS2を使用して交換される文書の送信者と所定の受信者はAS2-指定のHTTPヘッダーによって識別され、交換されるデータの先頭に付加される。ヘッダー"AS2-From"は、メッセージの送信者を特定するために使用され、ヘッダー"AS2-To"は、メッセージの受信者を識別するために使用される。

Reference:

- RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1"
- RFC4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)

2.1.2 ビジネス文書 (Business Document)

The Business Document Represents the actual business content of the PIP as defined in RosettaNet business document definitions, as well as additional collateral, like drawings.

ビジネス文書は、図面の様な追加の関連資料だけでなく、RosettaNetビジネス文書定義で定義されるPIPの実際の業務内容を説明する。

In AS2 business data may be XML, Electronic Data Interchange (EDI) in either the American National Standards Committee (ANSI) X12 format or in the UN Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT) format, or in other structured data formats.

AS2 では、業務データは American National Standards Committee (ANSI) X12 フォーマット、あるいは UN Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT)フォーマットのいずれか、又は他の構造化されたデータフォーマットの XML、Electronic Data Interchange (EDI) であろう。

The business document is encapsulated in a MIME message and can be signed, encrypted and/or compressed.

ビジネス文書は、MIME メッセージに封入され、署名、暗号化および/または圧縮をすることができる。

Reference:

- RFC4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)
- RFC1767 - MIME Encapsulation of EDI Objects
- RFC3023 - XML Media Types
- RFC5322 - Internet Message Format
- RFC1847 - Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
- RFC3850 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling
- RFC3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification

- RFC3852 - Cryptographic Message Syntax (CMS)
- RFC3274 - Compressed Data Content Type for Cryptographic Message Syntax (CMS)

2.1.3 ビジネス状態に関する合意の特徴 (Business State Alignment features)

The objective of these alignment features is to provide to each business party participating to a PIP, a common understanding about the status of the action message in terms of its reception, validity and processing prospects. Two features stand out:

ビジネス状態に関する合意の目的は、PIPを使うビジネスの各当事者に、アクション・メッセージの状態、即ち、受領、有効性、及び処理の状況に関して共通理解を提供することである。以下の2つの卓越した機能がある：

- (1)Delivery Alignment: Gives the Requester party an assurance that the Responder e.g. has received the action message. Acknowledgement of Receipt), or on the contrary that it has not been received (eg. Notification of Reception Failure). Semantic variants of this reception can be: (a) simple acknowledgement of reception by the messaging layer, (b) confirmation that the message has been delivered to the application layer

(1) **配信に関する合意**:アクション・メッセージが応答側によって受信されたことの確認(例:受領確認)、又は反対に受信されていないことの確認(例:受領不能通知)を要求者側に伝える。この受領の意味は同じで確認内容の異なるものは次の通りである: (a)メッセージ層による受領の簡単な確認、(b)メッセージがアプリケーション層に届けられたという確認。

- *NOTE: Some QoS capability such as reliable messaging may support this alignment feature. However proper relay to the business layer is required for this feature to be fulfilled.*
- 注記:信頼できるメッセージングのような QoS は、この配信に関する合意機能に対応できる。しかし、この機能を実現するには、ビジネス層への適切な中継が必要である。

In AS2 the sender of a message can optionally request that the receiver of the message return a Message Disposition Notification (MDN). The MDN only indicates that either the message was received and successfully unpackaged (e.g. decrypted and signature verified) or it will relay information about the errors that occurred while the message was being unpackaged.

AS2 では、メッセージの受信者が開封確認通知(Message Disposition Notification-MDN)を返送することを、メッセージの送信者は任意で要求できる。MDN はメッセージが受信されて首尾よく開封された(例えば、暗号が解除され、署名が認証された)、又はメッセージを開封中に発生したエラー情報を伝えるだけである。

For our purposes, the sender of an AS2 message should always request a signed MDN to be returned. When the signed MDN is received and processed, the sender of the message will know whether the intended recipient received the message and whether the message was successfully retrieved from its MIME packaging.

私達の用途では、AS2 メッセージの送信者は常に署名された MDN が返送されるように要求するべきである。メッセージの送信者には、署名された MDN が受信されて処理されると、所定の受信者がメールを受信したかどうか、およびメッセージがうまく MIME 梱包から復元されたかがわかる。

- (2) Validity Alignment : Gives the Requester an assurance that the action message has been statically validated by the Responder's integration system (Acknowledgement of Validity) or on the contrary that it failed to validate (Notification of Validation Failure).
- (2) 有効性に関する合意:アクション・メッセージが応答側の統合システムによって、静的に検証されたという確認(有効性の確認)、又は反対に検証できなかったこと(検証不能通知)を要求者側に伝える。

Different types of validation may be performed before aligning states about validity (e.g. before sending a ValidityAcknowledgement message, or by sending a validation failure notice). "Within an EDI trading relationship, if a signed receipt is expected and is not returned, then the validity of the transaction is up to the trading partners to resolve." "In general, if a signed receipt is required in the trading relationship and is not received, the transaction will likely not be considered valid"

有効性について合意する前に(例えば、有効性確認メッセージ(ValidityAcknowledgement)を送信する前、又は検証不能通知を送信するなど)、様々な種類の検証が実行される可能性がある。このテンプレートは、次の検証手順、又はレベルを定義する。“EDI 取引関係内で、署名受領が求められて、返事がない場合は、取引の有効性の解決は取引相手次第である”。“一般的に、取引関係で署名受領が必要であるのに受信されない場合、取引はおそらく有効とは見なされない”。

AS2 does not validate the payload. This functionality may be provided by the gateway software but is not part of the specification. This template defines the following validation steps or levels:

AS2 は、ペイロードを検証しない。この機能はゲートウェイ・ソフトウェアによって提供される可能性があるが、本仕様の一部ではない。このテンプレートは、次の検証の手順、又はレベルを規定する:

- Syntax validation: Check whether the business document is a well-formed document.
シンタクス(構文)検証: 即ち、ビジネス文書が正しいフォームの文書であることを確認する。
- Type validation: Check whether the business document is valid according to a schema definition file.
タイプ検証: 即ち、ビジネス文書がスキーマ定義のファイルに従った正しい文書であることを確認する。

- Business Rules validation: Check whether the business document is in line with a set of business rules that can be automatically checked without touching business applications.
ビジネス・ルール検証: 即ち、ビジネス文書がビジネス・アプリケーションと絡まずに、自動的にビジネス・ルール式に合致するかどうかを確認する。
- Sequence validation: Check whether this kind of business document is expected at the current state of the super-ordinate collaboration (applies only to execution context).
シーケンス検証: 即ち、この種類のビジネス文書が、上位コラボレーションの状況において要求されるかどうかを確認する(実行コンテキストにのみ適応)。

Additional steps 追加のステップ:

This functionality is NOT part of the AS2 specification.

この機能は、AS2 の仕様ではない。

- Business entity dereferencing: Check whether the business entities defined in the business document can be resolved within the business application.
企業逆参照: 即ち、ビジネス文書に記載の企業をビジネス・アプリケーション内で決定できるかどうかをチェックする。
- Document completeness check: Check whether the business document is complete from a business perspective. This may concern completeness of line items as defined in a business document of a prior PIP or as required by a business application.
書類完全性検査: 即ち、ビジネス文書がビジネスの視点から完全であるかどうかをチェックする。前の PIP ビジネス文書に記載される、あるいはビジネス・アプリケーションが必要とする行項目が全て記載されているかに関わるであろう。
- Business application check: The responder party must make sure that any validation checks have been applied to the action message that are necessary for ensuring processability of the business message.
ビジネス・アプリケーション検査: 即ち、応答側は、ビジネス・メッセージが処理できることを保証するために必要な、何らかの検証チェックがアクション・メッセージに適用されたことを確認しなければならない。
- Delegation to business application: The business document has successfully been imported by the business application.
ビジネス・アプリケーションへの委任: 即ち、ビジネス文書がビジネス・アプリケーションによって成功裡に取り入れられた。

Reference:

- RFC4130 – MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)

- RFC4130 – MIME-Based Secure Peer-to-Peer Business Data Interchange Using

2.2 PIP実行結果 (PIP execution outcome)

The state alignment features above will be used by the MCC messaging technology profiles to compute one of the following result values of a PIP execution (aligned with ebBP).

PIP実行の以下の結果の値の1つを計算するために、上記の状態に関する合意機能がMCC通信技術プロファイルによって使用されるでしょう (ebBPと協調して)。

The AS2 MDNs response status is at the Messaging Service level

- Successful processing status indication
- Unsuccessful processed content
- Unsuccessful non-content processing
- Processing warnings

- Protocol-outcome **プロトコル結果**

- SUCCESS means: The PIP execution can be considered as fully conforming to the PIP definition or to the concrete PIP: alignment requirements, QoS requirements and other execution mode requirements have been satisfied.
成功とは: PIP 実行において、PIP の明確化、又は最終の PIP に完全に適合すると見なすことができる: 合意要件、QoS 要件及びその他実行モード要件を満たしている。
- FAILURE means: The PIP execution has been deficient in some way and violated some requirements in the PIP definition or the concrete PIP: alignment requirements, QoS requirements and other execution mode requirements, have not been observed.
- **失敗とは:** PIP 実行において何らかの点で不十分であり、PIP の明確化あるいは最終の PIP の一部要件に違反している: 合意要件、QoS 要件及びその他実行モード要件が順守されなかった。

2.3 QoS (サービス品質) の特徴 (Quality of Service Features)

(1) 安全に関する選択肢 (Security options)

The data is packaged using standard MIME structures. Using Cryptographic Message Syntax with S/MIME security body parts obtains authentication and data confidentiality. Authenticated acknowledgements make use of multipart/signed Message Disposition Notification (MDN) responses to the original HTTP message.

データは標準的な MIME の構造を使用して梱包される。S/SMIME セキュリティ本体部を備える暗号メッセージ構文を使用することで、認証及びデータの機密性が得られる。認証確認は、元の HTTP メッセージへの返答のマルチパート/署名済み開封確認通知 (MDN) を利用する。

- Authentication **認証**

Authentication is accomplished digitally signing the message and/or receipt. At the transport level by HTTP Secure Socket Layer (SSL)

認証は、その通知および/または受領に HTTP Secure Socket Layer (SSL)による転送レベルでデジタル署名をして成し遂げられる。

1. Digitally sign the message

- SMIME 3.0 with MD5 - RSA
- SMIME 3.0 with SHA1 - RSA

Note:

- SHA1 supported by all AS2 Certified Products.
- No guarantee of vendor support for MD5.

2. HTTP Secure Socket Layer (SSL)

- Confidentiality **機密性**

Confidentiality is accomplished by encrypting the business document.

機密性は、ビジネス文書を暗号化することによって 成し遂げられる。

- Encryption:
 - o SMIME 3.0 with DES
 - o SMIME 3.0 with 3DES
 - o SMIME 3.0 with RC2 - 40
 - o SMIME 3.0 with RC2 - 64
 - o SMIME 3.0 with RC2 - 128

Note: 注

3DES supported by all AS2 Certified products. No guarantee of vendor support for encryption algorithms such as DES, RC2 variants and AES variants.

トリプル DES は、全ての AS2 認定製品によってサポートされる。DES、RC2 変種及び AES 変種のような暗号化アルゴリズムに対するベンダサポートの保証はない。

- Integrity **完全性**

The message sender creates a message digest using a hash algorithm, also referred to as the message integrity check (MIC). The sender then computes a digital signature over the MIC. When the recipient receives the message, the recipient verifies the digital signature and MIC.

メッセージの送信者は、ハッシュ・アルゴリズムを使用するメッセージ・ダイジェストを作成し、それがまたメッセージの完全性確認(MIC)と見なされる。送信者は、次に MIC 上でデジタル署名を演算する。受信者は、メッセージを受信すると、デジタル署名及び MIC を検証する。

- Digital Signature
 - o SMIME 3.0 with MD5 - RSA
 - o SMIME 3.0 with SHA1 - RSA

- Non Repudiation of Origin /Non Repudiation Of Receipt
否認防止/受領の否認防止

The receipt contains data identifying the original message for which it is a receipt, including the message-ID and a cryptographic hash (MIC). The original sender must retain suitable records providing evidence concerning the message content, its message-ID, and its hash value. The original sender verifies that the retained hash value is the same as the digest of the original message, as reported in the signed receipt.

受領書には、メッセージ-ID 及び完全性確認(MIC)など受領を示す元のメッセージの識別データが入っている。送信者は、メッセージ内容、メッセージ ID 及びハッシュ値に関する証拠を提供する適切な記録を保存しておかなければならない。保有されるハッシュ値は、署名受領で報告された元のメッセージのダイジェストと同じであることを、送信者は確認する。

- Authentication is accomplished digitally signing the message and/or receipt
メッセージおよび/または受領書にデジタル署名をして、認証は成し遂げられる。
 - Digital Signature
 - o SMIME 3.0 with MD5 – RSA
 - o SMIME 3.0 with SHA1 – RSA

- Authorization **認可**

Authorization is accomplished by the trading partner agreement.
認証は、取引当事者間協定書によって成し遂げられる。

(2) Reliable Messaging: **高信頼性メッセージング:**

- Guaranteed delivery (At-least-Once delivery)
保証された配信 (最低でも一度の保証された配信)

Guaranteed delivery is accomplished by using the Message Disposition Notification (MDN). This is an optional specification for AS2 and may not implement by all AS2 vendors. However, most AS2 vendors provide for some level of reliable messaging.

保証された配信は、Message Disposition Notification (MDN)を使用して、成し遂げられる。これは、AS2 に関して任意指定であり、全ての AS2 ベンダーが実装しているわけではない。しかし、ほとんどの AS2 ベンダーは、相当なレベルの信頼性あるメッセージングを提供している。

- Duplicate elimination (At-Most-Once delivery)
重複排除 (最大で一度の重複なしの配信)

In the AS2 standard, detection of duplicates by Message-Id or by business transaction identifiers is recommended.

AS2 標準では、メッセージ ID、又はビジネス取引識別子による重複の検出が推奨される。

(3) Timing Constraints **時間的制約:**

- Time to acknowledge validity (or invalidity):
有効(あるいは無効)な受領通知までの時間 :

This QoS setting is part of the trading partner agreement.

この QoS 設定は、取引当事者間協定書の一部である。

- Time to Perform:
実行までの時間

This QoS setting is part of the trading partner agreement.

この QoS 設定は、取引当事者間協定書の一部である。

Reference: Operational Reliability for EDIINT AS2

参照: EDIINT AS2 用の動作信頼性

3 PIPパラメータ化と実行管理 (PIP Parameterization and Execution Control)

1. PIP property parameters: these are parameters that control the use of features defined above as PIP properties: level of state alignment and various QoS features.

PIP属性パラメータ: これらは、PIP属性として上記に定義された機能の使用を制御するパラメータである:状態に関する合意レベル及び様々なQoS機能。

2. PIP execution parameters: these are parameters that control the actual execution of the PIP.

PIP実行パラメータ: これらは、実際のPIP実行を制御するパラメータである。

3.1 PIP プロパティ・パラメータ (PIP Property Parameters)

The following parameters are configurable on a PIP definition and a PIP implementation instance basis:

以下のパラメータは、PIP明確化及びPIP実装インスタンスのベースで構成可能である。

| Specification item | Configurable | Implication | Explanation |
|-----------------------------|--------------|--|--|
| Send Request Document | NO | | A request document must be sent いつも要求書を送付しなければならない。 |
| Overall Time To Perform | YES | In Trading Partner Agreement | <ul style="list-style-type: none"> AS2 exchanges a single document with a receipt (MDN). This setting equals Time To Acknowledge AS2 は単一の文書と受領書(MDN)を交換する。この設定は、確認までの時間と等しい。 The “Operational Reliability for EDIINT AS2” specifications are more about “fire and forget” and how long before you ultimately give up on sending the message. 「EDIINT AS2 用の動作信頼性」の仕様は、「撃ちっ放し能力」であり、最終的にメッセージ送信をあきらめるまでの時間について記述する。 The MDN timeout is part of AS2 MDNタイムアウトはAS2の重要な部分である。 |
| Receipt-Acknowledgement | YES | Message Disposition Notification (MDN) | Sync / Async / None |
| Non Repudiation | YES | Digitally signing the Payload | Refer to: RFC4130 |
| Non Repudiation of Receipt | YES | Digitally signing the MDN | Refer to: RFC4130 |
| Time To Acknowledge Receipt | YES | In Trading Partner Agreement | The MDN timeout is part of AS2 MDNのタイムアウトは、AS2の重要な部分である。 |
| Reliability | Yes | In Trading Partner Agreement | <ul style="list-style-type: none"> Retry sending unsuccessful POSTs. 失敗したPOSTの送信をやり直す。 Resend messages when MDNs not received. MDNを受信できなかった場合、メッセージを再送する。 Refer to: Operational Reliability for EDIINT AS2. EDIINTAS2のための動作信頼性を参照。 |

| | | | |
|-----------------------------|-----|---|--|
| | | | <ul style="list-style-type: none"> • Retry when message not successfully POSTed. メッセージが上手くPOSTされなかった場合、再送する。 |
| Confidentiality | YES | HTTPs and/or Encryption | <ul style="list-style-type: none"> • HTTPs is an encrypted channel. HTTPsは、暗号化チャンネルである。 • AS2 messages can also be encrypted before they are sent. AS2メッセージは、送信する前にも暗号化できる。 |
| Integrity | YES | Message Integrity Check (MIC) calculation of signed messages 署名メッセージのメッセージ完全性チェックの演算 | Calculating the MIC of the message received and verifying that MIC with the MIC extracted from the signature applied to the message will ensure that the message has not been tampered with. 受信メッセージのMICを演算し、メッセージに適用された署名から抽出されたMICで当該MICを検証することによって、メッセージが改ざんされていないことを保証する。 |
| Authentication | YES | Digital Signatures | The receiver of a message can authenticate the sender of a message if digital signatures are used. デジタル署名が使用される場合、メッセージの受信者は、メールの送信者を認証できる。 |
| Authorization | YES | In Trading Partner Agreement | Valid relationship exist between the agreement in sender / recipient 送信者/受信者の同意の間には、有効な関係が存在する。 |
| Intelligible Check Required | YES | In Trading Partner Agreement | Validation of message not in AS2 Specification AS2仕様ではないメッセージの検証。 |
| RetryCount | YES | In Trading Partner Agreement | Refers to HTTP Error Recovery HTTPエラー修復処理を参照。 |

Examples for defining PIPs will be given in the use cases section.

PIPの明確化についての例は、4 PIP 明確化の事例の章で説明される。

3.2 PIP実行形式と関連パラメータ (PIP execution modes and related parameters)

AS2 exchanges a single document with a receipt Acknowledgement, the Message Disposition Notification (MDN). These modes are related to it.

AS2 は単一の文書と受領確認 (Message Disposition Notification (MDN)) を交換する。これらの形態は、以下に関連する。

- Synchronous execution: **同期実行:**
Synchronous Receipt - A receipt returned to the sender during the same HTTP session as the sender's original message.
同期受信 受領書は、送信者の当初のメッセージと同じ HTTP セッションの中で、送信者に返される。
- Asynchronous execution with callback: **コールバック付きの非同期実行:**
Asynchronous Receipt - A receipt returned to the sender on a different communication session than the sender's original message session.
非同期受信 受領書は、送信者の当初のメッセージと違う通信セッションで、送信者に返される。
- Asynchronous execution with pulling: **プル付き非同期実行:** Asynchronous Receipt - A receipt returned to the sender on a different communication session than the sender's original message session.
非同期受信 受領書は、送信者の当初のメッセージと違う通信セッションで、送信者に返される。

3.3 PIPインスタンス相関関係及び識別 (PIP Instance Correlation and Identification)

3.3.1 PIPの識別 (PIP Identification)

Generation of Globally Unique Ids (GUIDs) for PIP instances

PIPインスタンスに対するグローバルに一意的識別子(GUID)の生成:

PIP instance ids are to be generated by the PIP requester by appending an id that is unique within their systems to their globally unique partner id, preferably a GLN or a DUNS number. This is locate in the PIP Business Document, the Service Header and Delivery Header

PIPインスタンスIDは、グローバルに一意的パートナーIDに対して自らのシステム内で一意のID -GLN 又はDUNS番号が好ましい- を付加することにより、PIP要求者が生成することになっている。これは、PIP ビジネス文書のサービスヘッダーとデリバリーヘッダーに配置されている。

The AS2 Header contains a unique messaging id "Message-ID"

AS2ヘッダーは、一意なメッセージID "Message-ID"を持っている。

Note: A 'n' Action PIP will require PIP instance ID

注: 'n' アクションPIPは、PIPインスタンスIDを要求する。

Inclusion of PIP instance GUIDs within RosettaNet message definitions RosettaNetメッセージで定義するPIPインスタンスGUIDの内包

The inclusion of PIP instance GUIDs is not addressed at this point in time. MCC Phase 2 will address this topic and provide a detailed specification for this topic.

現在時点で、PIPインスタンスGUIDの内包については言及しない。MCCフェーズ 2では、このテーマについて詳細な仕様を提供するでしょう。

3.3.2 メッセージの相関関係 (Message Correlation)

Message correlation denotes the act of associating messages with process instances, which may be implemented at the messaging level or at the PIP process level.

メッセージの相関については、メッセージング・レベルあるいはPIPプロセス・レベルで実装されるであろうプロセス例にメッセージを関連付ける動作をいう。

- MDNs are automatically correlated per the specification.
MDNsは、仕様毎に自動的に相関付ける。

- Business document correlation (n-Action PIPs) and is in the payload

```
Requestor <thisDocumentIdentifier>  
           <ProprietaryDocumentIdentifier>2222</ProprietaryDocumentIdentifier>  
           </thisDocumentIdentifier>  
Responder <requestingDocumentIdentifier>  
           <ProprietaryDocumentIdentifier>2222</ProprietaryDocumentIdentifier>  
           </requestingDocumentIdentifier>
```

4 PIP明確化の事例 (Use Cases of PIP definition)

This section gives some sample configurations of PIPs according to the configurability matrix above. The MCC messaging technology profiles are expected to describe the implementation of these use cases.

この章では、前述の構成可能マトリックスによるいくつかのPIPの構成サンプルを示す。MCC通信技術のプロファイルは、これらの事例を説明することが期待される。

4.1 事例 1 全て包括 (Use Case 1 – Full features)

```
<DataExchange
  name="bt-PIP3A20"
  nameID="bt-PIP3A20"
  isGuaranteedDeliveryRequired="true">
  <RequestingRole name="Purchase Order Confirmation Sender" nameID="bt-PIP3A20-role-
sender"/>
  <RespondingRole name="Purchase Order Confirmation Receiver" nameID="bt-PIP3A20-role-
receiver"/>
  <RequestingBusinessActivity
    name="Send Purchase Order Confirmation"
    nameID="bt-PIP3A20-ba-req"
    isIntelligibleCheckRequired="true"
    isNonRepudiationRequired="true"
    isNonRepudiationReceiptRequired="true"
    retryCount="3"
    timeToAcknowledgeReceipt="PT3M"
  >
  <DocumentEnvelope
    name="doc-PIP3A20-PurchaseOrderConfirmation"
    businessDocumentRef="doc-PIP3A20-PurchaseOrderConfirmation"
    nameID="doc-PIP3A20-PurchaseOrderConfirmation-de"
    isAuthenticated="transient"
    isConfidential="transient"
    isTamperDetectable="transient"
  />
  <ReceiptAcknowledgement
    name="ra"
    nameID="bt-PIP3A20-ack-ra"
    signalDefinitionRef="ra2"/>
  <ReceiptAcknowledgementException
    name="rae"
    nameID="bt-PIP3A20-ack-rae"
    signalDefinitionRef="rae2"/>
  </RequestingBusinessActivity>
  <RespondingBusinessActivity name="xsd-pacifier" nameID="bt-PIP3A20-ba-resp"/>
</DataExchange>
```

4.2 事例 2 ビジネス文書のみ (Use Case 2 – Business Document Only)

```
<DataExchange
  name="bt-PIP3A20"
  nameID="bt-PIP3A20"
  isGuaranteedDeliveryRequired="true">
  <RequestingRole name="Purchase Order Confirmation Sender" nameID="bt-PIP3A20-
role-sender"/>
  <RespondingRole name="Purchase Order Confirmation Receiver" nameID="bt-PIP3A20-
role-receiver"/>
  <!-- No TTAR, nor isIntelligibleCheckRequired -->
  <RequestingBusinessActivity
    name="Send Purchase Order Confirmation"
    nameID="bt-PIP3A20-ba-req"
    isNonRepudiationRequired="true"
    isNonRepudiationReceiptRequired="true"
    retryCount="1"
  >
  <DocumentEnvelope
    name="doc-PIP3A20-PurchaseOrderConfirmation"
    businessDocumentRef="doc-PIP3A20-PurchaseOrderConfirmation"
    nameID="doc-PIP3A20-PurchaseOrderConfirmation-de"
    isAuthenticated="transient"
    isConfidential="transient"
    isTamperDetectable="transient"
  />
  <!-- No ReceiptAcknowledgement/Exception definitions here -->
</RequestingBusinessActivity>
<RespondingBusinessActivity name="xsd-pacifier" nameID="bt-PIP3A20-ba-resp"/>
</DataExchange>
```

The following specifications' requirements are incorporated into the Profile by reference, except where superseded by the Profile: (<http://ietfreport.isoc.org/>)

プロファイル(<http://ietfreport.isoc.org/>)によって取り代わられる場合を除き、以下の仕様要件は、参照先としてこのプロファイルに取り込まれる:

- RFC1767 - MIME Encapsulation of EDI Objects
- RFC1847 - Security Multiparts for MIME: Multipart/Signed & Multipart / Encrypted
- RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1
- RFC2634 - Enhanced Security Services for S/MIME
- RFC3023 - XML Media Types
- RFC3274 - Compressed Data Content Type for Cryptographic Message Syntax (CMS)
- RFC3798 - Message Disposition Notification
- RFC3850 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling
- RFC3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification
- RFC3852 - Cryptographic Message Syntax (CMS)
- RFC4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)
- RFC5322 - Internet Message Format
- RFC5323 - Web Distributed Authoring and Versioning (WebDAV) SEARCH
- Operational Reliability for EDIINT AS2: draft-duker-as2-reliability-06
- MIME-based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)