2012 年度～2013 年度
メッセージング基盤タスクフォース
／
2014 年度　国際連携タスクフォース
グローバルネットワーク相互運用検討サブタスク

活動報告書

SIPS

一般社団法人サプライチェーン情報基盤研究会

はじめに

本書は、SIPS 設立の 2012 年から 2014 年度までの活動記録である。

ただし、2012 年～2013 年は「メッセージング基盤 TF（タスクフォース)」、2014 年は「国際連携 TF 相互運用性検討サブタスク」の活動となっている。

組織としては、2012 年 SIPS 設立の折、「国境を越えて電子文書を交換するための相互互換性がある信頼性メッセージング基盤構築のためのガイドラインを策定し、国内外に向けた合意形成を行う」ことを目指していた。ただ 2014 年、前年までの実稼働メンバー全員が異動等により参加できなくなったため、独立 TF として継続できなくなり、国際連携 TF の中のサブタスクとして組織を再編成することとなった。

ガイドライン策定にかかわる作業については、いったん情報収取段階で終息、本報告書に作業実績を記録として残している。

よって、本書は「メッセージング基盤構築ガイドライン」の完成版ではなく、あくまでガイドライン策定にかかわる調査・研究の活動報告である。

コンテンツとしては情報収集段階のものも含まれており、目次と本文タイトルが不一致のところもある。

なお、2014 年度より新規に調査を始めた「パブリッククラウド相互運用性調査」については、2015 年度以降継続した活動を進めている。

背景

本ガイドラインは次のような背景のもとに調査研究がはじめられた。

現在、日本では海外企業と直接繋ぐようなグローバル EDI は、限られた業界の一部の企業以外ではほとんど実施されていない、もしくは必要とされていない。その理由は、海外とは社内ネットワークで接続しそこから現地の企業と取引を行う、もしくは商社経由で取引をするなどのパターンが多いからと考えられる。

また、実際に EDI をしたいと思っても、各国ごとのビジネスボリュームが小さく EDI 化のコストを吸収できない、国情や慣習の違いがあり EDI 化できないなどの問題も大きな壁として立ちふさがっている。

あわせて海外と EDI をするとしても、どのようにしてよいかわからないというのも現実。自社での接続が難しい場合、ESP 経由が有効となるが、海外と接続可能な ESP も数は限られている。現時点で海外接続の必要性が少なくとも、今後取引量が増え必要となる情報が

多様になった場合、コンピュータとコンピュータを直接接続する必要性が高まることは間違いない。その時に備えて、まず ESP がその役割を担う準備が必要。

本書では、各企業が直接海外と接続するのではなく、ESP が海外と繋ぐため、もしくは海外と繋ぐことができる ESP と接続するための仕様をまとめる。

> グローバル EDI とは、日本国内の企業が、インターネットを介して海外の企業とコンピュータ同士を接続し、可能な限り標準に準拠した仕様によりデータ交換を行うこと。
>
> ESP（EDI Services Provider）とは、EDI とそれにかかわるサービスを提供する。通信プロトコル変換、データのフォーマット変換、データの管理・蓄積など従来の VAN サービスにあわせ、インターネットにかかわるセキュリティ対策や業界特有の業務代行、接続先のサポートなど、EDI にかかわるさまざまなサービスを提供する事業者。
>
> グローバル ESP とは、海外との接続・連携をサポートする ESP。

ガイドラインの目的

日本の企業にとって海外、特にアジア各国と情報連携を行うための基盤を作ることが必要となっている。各企業が独自に海外企業と情報連携を図るのは、現時点で非常にハードルが高い。それを可能にするには ESP の利用が有効。

ここでは、各企業が直接海外と接続するのではなく、身近な ESP 経由で海外に出ることができる環境作りを目指す。

また、すでに利用している ESP が海外接続できなくとも、その ESP がグローバル ESP と接続することができるようになれば、企業としては問題なく ESP 経由で海外に出ることができる。

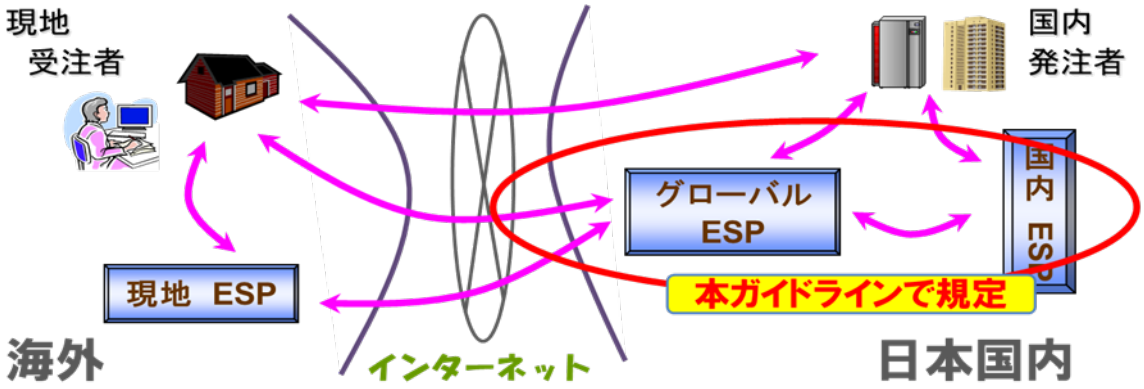
しかし、海外に接続可能なグローバル ESP が個々に独自の仕様を取りまとめてしまうと、そこに繋ぐための企業もしくは ESP は、異なる接続仕様を持たなくてはならないことになり、非常に効率が悪くなる。

本書は、国内の企業が海外と接続するため利用する ESP が準備しなければならない機能、また国内 ESP が海外に接続可能なグローバル ESP と接続するための ESP 間接続のための仕様をまとめたものである。

グローバル EDI の位置づけ

国内企業が海外と接続するには多くの接続パターンが想定できる。本書では、以下のパターンを前提とし、その接続において必要とされる仕様の範囲を定める。

海外との接続パターン



本ガイドラインの範囲

［注記：本ガイドラインでは未完の部分あり　2016.03］

本ガイドラインでは、国内 ESP とグローバル ESP 間での接続について仕様を定める。仕様には、グローバル ESP が海外と接続するときに考慮すべき点や運用上の注意点も含む。また国内企業が、実際の導入・保守にかかわる考慮点についても、ESP 側の準備事項として記載する。

活動の流れ

2012 年度

□「メッセージング基盤 TF」立ち上げ

□「メッセージング基盤構築ガイドライン」の大枠を定め、調査を開始

2013 年度

□「メッセージング基盤 TF」として活動

□ガイドラインの構成に基づき、情報を収集・分類・整理

2014 年度

□メッセージング基盤 TF を解散し、国際連携 TF のもとに「パブリッククラウド相互運用性調査」サブタスクとして編入。

□ガイドラインにかかわる情報収集・分析・整理を継続

□新たに「パブリッククラウドの相互運用性調査」を検討のテーマに追加

□本テーマは、2015 年度以降も継続

以上

2016 年 3 月

国連 CEFACT 日本委員会

サプライチェーン情報基盤研究会

国際連携タスクフォース

委員

2012 年度～2013 年度　メッセージング基盤タスクフォース委員

リーダー	藤野　裕司	株式会社データ・アプリケーション
会員	兼子　邦彦	小島プレス工業株式会社
会員	菅野　修一	小島プレス工業株式会社
会員	柴田　鎮雅	日本情報通信株式会社
会員	高橋　朗	株式会社データ・アプリケーション
会員	菊間　裕二	日本アイ・ビー・エム株式会社
会員	種　明日香	日本アイ・ビー・エム株式会社
会員	遠城　秀和	株式会社 NTT データ
会員	阪口　信吾	NEC システムテクノロジー株式会社
会員	仲矢　靖之	ＴＩＳ株式会社
会員	須田　尚克	ＴＩＳ株式会社
会員	竹内　正人	株式会社インテック
業界委員	川内　晟宏	IT コーディネータ協会
業界委員	内田　宏樹	石油化学工業協会　CEDI 小委員会
業界委員	武山　一史	一般社団法人日本物流団体連合会
業界委員	藤岡　慎弥	NPO 法人観光情報流通機構
業界委員	坂本　真人	一般財団法人流通システム開発センター
業界委員	栗田　和則	一般財団法人流通システム開発センター
オブザーバー	久田　洋平	日本銀行金融研究所
オブザーバー	河野　祐一	住友化学株式会社
オブザーバー	江頭　顕	SCSK 株式会社
オブザーバー	木戸　啓介	GMO グローバルサイン株式会社
オブザーバー	大江　賢治	サトーホールディングス株式会社
オブザーバー	谷川　伸司	キャノンソフト情報システム株式会社
オブザーバー	津田　智	キャノンソフト情報システム株式会社

委員

2014 年度　国際連携タスクフォース
グローバルネットワーク相互運用検討サブタスク 委員

リーダー	藤野　裕司	株式会社データ・アプリケーション
会員	黒渕　達也	株式会社データ・アプリケーション
会員	谷川　伸司	キャノンソフトウェア株式会社
会員	琴賀岡　忠宏	キャノンソフトウェア株式会社
会員	安部　和人	株式会社ＪＳＯＬ
会員	小川　楽	株式会社ＪＳＯＬ
会員	須田　尚克	ＴＩＳ株式会社
会員	竹内　正人	株式会社インテック
会員	吉田　敦	株式会社インテック

目次

第一編.　　通信プロトコル

1.　目的

本編は、国内 ESP およびグローバル ESP 同士が連携する折に必要とされる通信プロトコルの仕様を定めている。これにより、国内企業は自社保有の通信プロトコルで国内 ESP もしくはグローバル ESP に接続すると、その ESP 経由で海外の企業や海外の ESP とグローバル EDI を行うことが可能となる。

2.　通信方式と推奨通信プロトコル

2.1.　通信方式

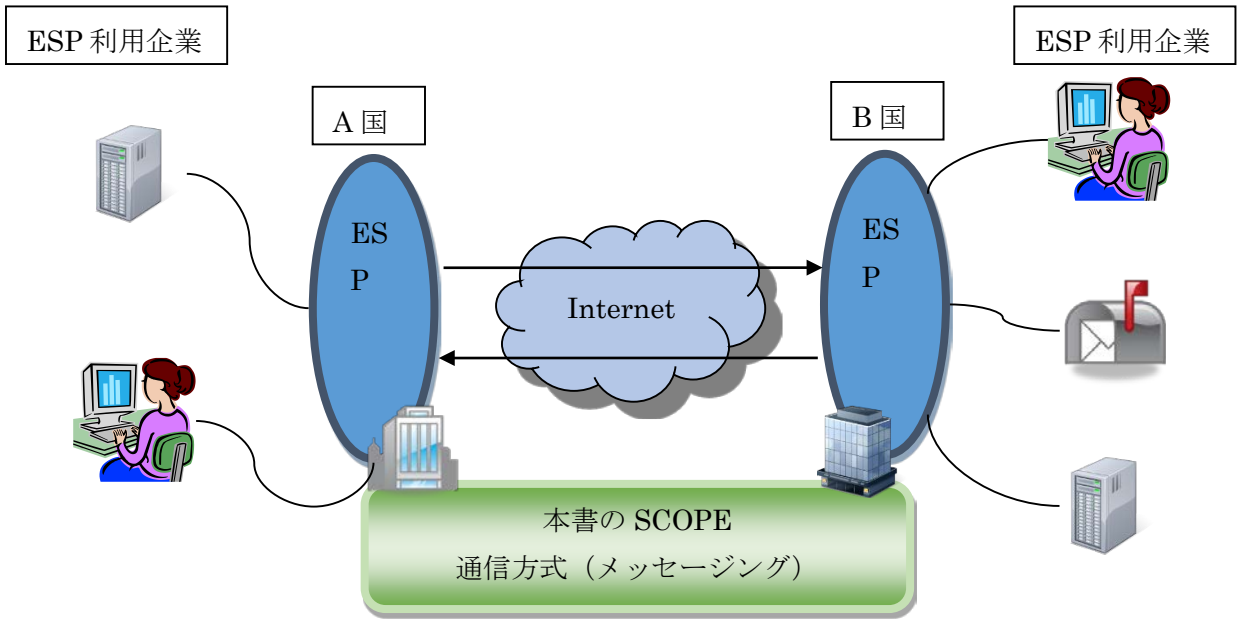
本章においては、下図のような ESP 間国際接続を想定して通信方式を検討した。A 国の ESP を使う A 社と、B 国の ESP を使う B 社の 2 社間の EDI を実現する際に必要となるサービス機能(プロトコル)について記述する。

ESP の利用を必要としない企業（大企業を想定）が新興国等、IT 基盤が未成熟な地域と EDI を行う場合など、相手国 ESP との接続が必要となるケースが想定される。その場合においては、該当企業は自社の立場を ESP と読み替えることで本書を利用することが可能となる。

ネットワーク環境

本書では、ESP 間国際接続が目的であり、各国に海外との I/F が必須となるため、既に各国に経路のある Internet 環境を想定している。

次章から Internet 環境上で稼働し、EDI メッセージの授受が可能なプロトコルについて説明する。尚、本書は ESP 間の接続について定めるものであり、各国 ESP と利用企業との I/F については言及しない。



通信プロトコル

アジア地域での国際間取引を主な目的として税関手続き業務で実績のある ebXML Messaging Service Specification. Version 2.0（ebMS2）の採用に加えて、将来的な北米方面への展開も見据え AS2（Applicability Statement 2）も併せて採用し、各国 ESP 間での推奨パラメータセットを定めることで調整余地を少なくし、早期のサービスインを実現するものである。

対象のプロトコルはサーバーto サーバーモデルであることは共通だが、機能に若干の違いがあり、特に一回の伝送で複数ドキュメントの搬送の可否に大きな違いがある。

ESP 利用企業は業務用件により、どちらのプロトコルを利用すべきかの判断をして契約する。各国 ESP は本書で定める 2 プロトコルのどちらか一方ではなく、両プロトコルの実装を強く推奨する。

2.2.　推奨通信プロトコル

AS2

プロトコル概要

AS2（Applicability Statement 2）は HTTP を利用することでインターネットを通じて ビジネスドキュメントをセキュアに送受信するための国際標準プロトコルであり、リアルタイムにデータを交換できることが特徴である。

プロトコルのセキュリティとして、電子署名と暗号化を使用することで、データの改ざん防止、機密性を実現する。また受信確認通知である MDN（Message Disposition Notification）を送信者側に返信することで、送信否認・受信否認防止を実現する。

> 補足：AS2 は HTTP を利用したプロトコルである。このほかに、SMTP を利用した AS1、FTP を利用した AS3、更に ebXML Message Service Version 3.0 を基礎とした AS4 が存在する。

上記プロトコルはセキュアで信頼性のあるビジネスプロトコルとして、AS1, AS2, AS3 が IETF（Internet Engineering Task Force）の EDIINT ワークグループにより定められ、AS4 は OASIS の ebXML Messaging Service **Technical Committees により定められている。**

AS2 の構成要素

ドキュメントダイジェスト（Document Digist）

授受するビジネスドキュメントのダイジェスト値。**送信者がドキュメントのダイジェスト値を予め計算、保存する。署名付き MDN で通知される受信者が計算したダイジェスト値と照合する。**

□署名（Signing）

送信者の秘密鍵込み公開鍵証明書を用いて、通信メッセージの署名を行う。

□暗号（Encryption）

受信者の公開鍵証明書を用いて、通信メッセージの暗号化を行う。

□・データ送信（Sending）

□複合（Decryption）

受信者の秘密鍵込み公開鍵証明書を用いて、通信メッセージの複号化を行う。

□署名検証（Signature Verification）

送信者の公開鍵証明書を用いて、通信メッセージの署名検証を行う。

□受信確認通知（MDN:Message Disposition Notification）

ビジネスドキュメントの受信、処理結果通知。

□署名付き MDN（Signed MDN）

ビジネスドキュメント受信者の電子署名が施された受信確認通知（MDN）。**プロトコル仕様で MIC（ドキュメントダイジェスト）通知が必須。送受信者双方で計算した MIC 値が合うことを確認する。受信者の秘密鍵込み公開鍵証明書を用いて、MDN の署名を行う。**

□MDN 署名検証（Verification of MDN Signature）

受信者の公開鍵証明書を用いて、MDN の署名検証を行う。

□MDN 処理（MDN Processing）

MDN 内にあるデータ送信の実行結果情報を判別し、それぞれに対応する処理を行う。

セキュリティ要件と AS2 構成要素の対応

EDI メッセージ授受におけるセキュリティ要件と AS2 で実現可能なセキュリティ実施パターンを以下に説明する。なお、AS2 プロトコルで実現可能なセキュリティの範囲は ESP 間接続に限定されたものであることに留意されたい。

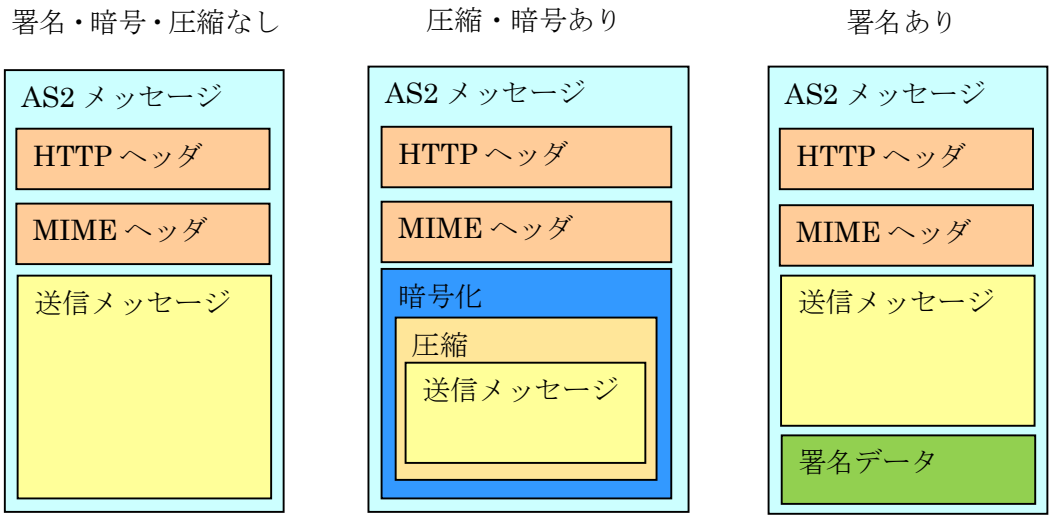
□メッセージの信頼性

AS2 の構成要素とメッセージの信頼性の対応を下表に示す。

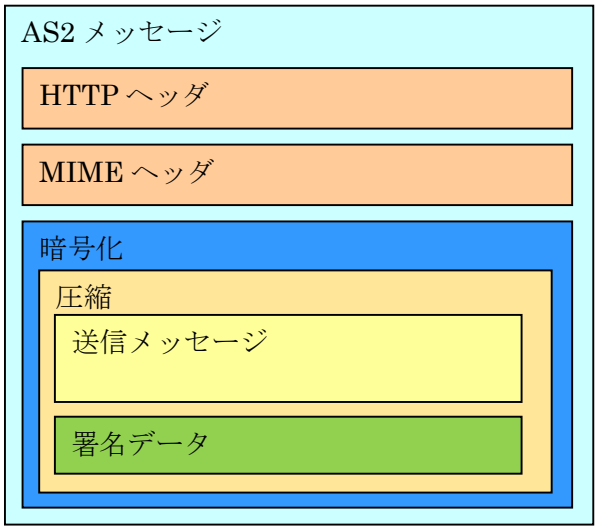
セキュリティ要件	AS2構成要素		
	署名	暗号	署名付きMDN
改ざん防止	○	－	－
発信者認証	○	－	－
送信否認防止	○	－	－
受信否認防止	－	－	○
機密保持	－	○	－

AS2 メッセージの構造

AS2 プロトコルで利用有無を選択できる機能と取りうるメッセージフォーマットの対応の一例を下図に示す。



さらに、SIPS 推奨パターンを以下に示す。



推奨パラメータセット（**SIPS** プロファイル）

		AS2
SSL/TLS		○(TLS1.0以上)
受信否認		○
メッセージ	署名	○
	暗号	○
	圧縮	プロトコル標準機能推奨
Ack/MDN	同期・非同期	非同期
	署名	○
圧縮範囲(本文のみ/署名含)		署名まで含む
署名部への証明書添付		運用毎に決定
Miultpart　Message		×
重複破棄		×
暗号アルゴリズム		選択可 (3DES、AES他)
ダイジェストアルゴリズム		選択可 (SHA-1,SHA-256)
再送	回数	運用毎に決定
	間隔	運用毎に決定
HTTP認証	Basic認証	×
	SSLクライアント認証	×
証明書	鍵長	2048
	バージョン	V3
	自己署名	×
Listenポート番号		運用毎に決定
授受可能データサイズ(推奨値)		500MB以下

参考資料

“MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)”, RFC 4130

http://www.ietf.org/rfc/rfc4130.txt

ebXML Messaging Service Specification. Version2.0 (ebMS2.0)

プロトコル概要

ebMS2.0 仕様は、インターネットを通じて ビジネスドキュメントをセキュアに送受信するための国際標準プロトコルであり、リアルタイムにデータを交換できることが特徴である。

プロトコルのセキュリティとして、電子署名と暗号化(SSL/TLS)を使用することで、データの改ざん防止、機密性を実現する。また受信確認通知である Acknowledgement を送信者側に返信することで、送信否認・受信否認防止を実現する。

ebMS2.0 は、OASIS（Organization for the Advancement of Structured Information Standards）により仕様策定され、ISO/TS 15000-2 として承認されている。

ebMS2.0 の主な機能

□Error Handling
受信したメッセージにエラーがある場合、送信元に原因等の情報通知(ErrorList)を行う。

□Security
盗聴防止、改ざん防止、否認防止などの機能を、電子署名と暗号化(SSL/TLS)により実現する。

□SyncReply
受信確認通知(Acknowledgement)や受信メッセージエラー通知(ErrorList)を、送信時と同じコネクションを用いて返信することを可能とする。

□Reliable Messaging
受信確認メッセージによる送達確認や二重受信の検出(重複破棄)、再送処理などを可能とする。

□Message Order
送信メッセージの順序保証を行う。

□MSH Ping Service
あるメッセージングサービスから通信相手先のメッセージングサービスが動作しているかの確認を行う。

□Multi-Hop
１つ以上の中間ノードがメッセージの最終的な送受信ノードの間に存在するメッセージ配送プロセス。

セキュリティ要件と ebMS2.0 構成要素の対応

EDI メッセージ授受におけるセキュリティ要件と ebMS2.0 で実現可能なセキュリティ実施パターンを以下に説明する。

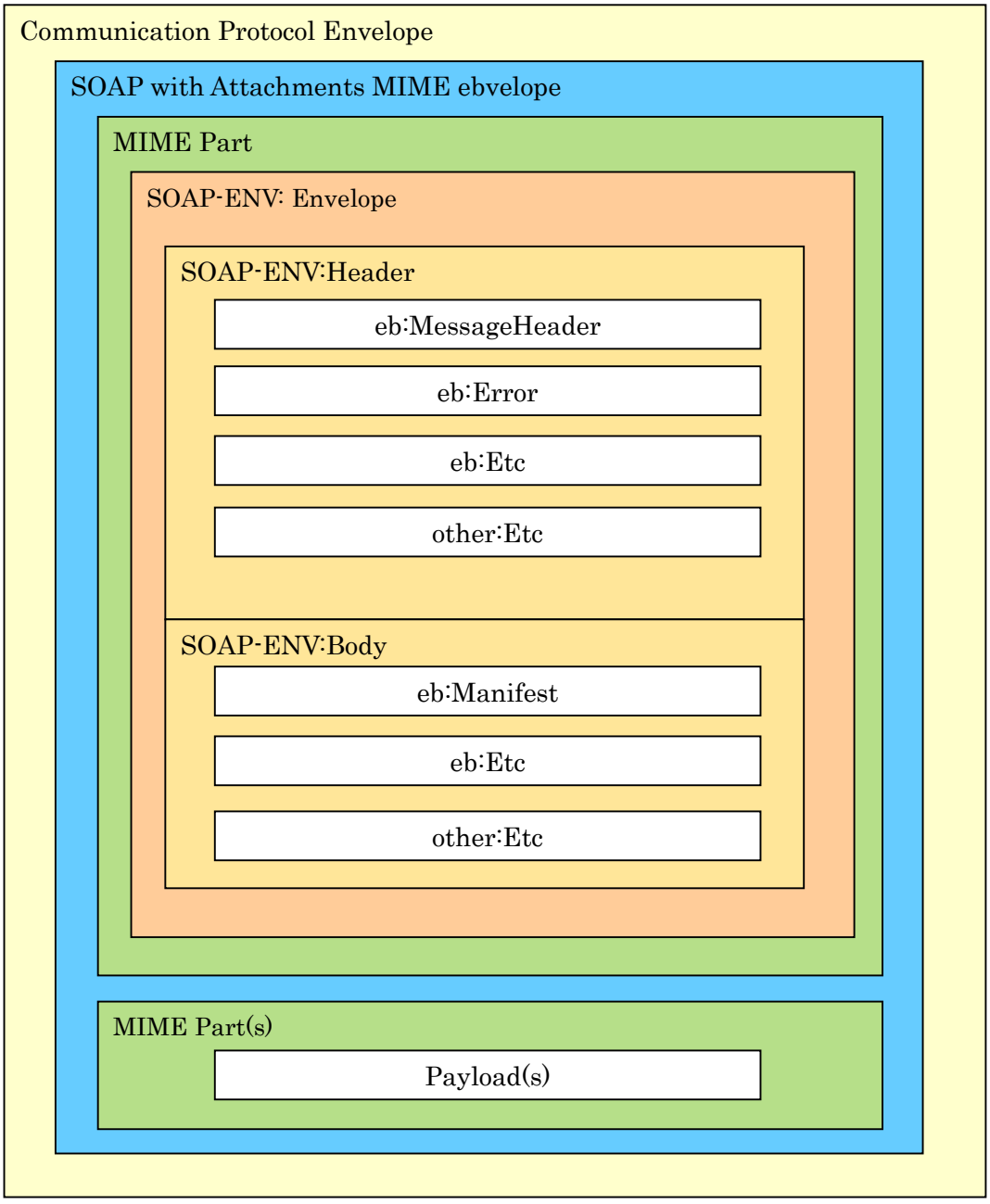
なお、ebMS2.0 プロトコルで実現可能なセキュリティの範囲は ESP 間接続に限定されたものであることに留意されたい。

□メッセージの信頼性

ebMS2.0 の構成要素とメッセージの信頼性の対応を下表に示す。

セキュリティ要件	ebMS2.0構成要素		
	署名	暗号(SSL/TLS)	署名付きAck
改ざん防止	○	－	－
発信者認証	○	－	－
送信否認防止	○	－	－
受信否認防止	－	－	○
機密保持	－	○	－

ebMS メッセージの構造



推奨パラメータセット（**SIPS** プロファイル）

		ebMS2
SSL/TLS		○(TLS1.0以上)
受信否認		○
メッセージ	署名	○
	暗号	×
	圧縮	×（プロトコル仕様で不可）
Ack/MDN	同期・非同期	非同期
	署名	○
署名部への証明書添付		運用毎に決定
Miultpart　Message		○
重複破棄		○
暗号アルゴリズム		×
ダイジェストアルゴリズム		SHA-2
再送	回数	運用毎に決定
	間隔	運用毎に決定
HTTP認証	Basic認証	×
	SSLクライアント認証	運用毎に決定
証明書	鍵長	2048
	バージョン	V3
	自己署名	×
Listenポート番号		運用毎に決定
授受可能データサイズ（要件）		500MB
CPAの利用		○

参考資料

“Message Service Specification Version 2.0”

http://www.ebxml.org/specs/ebMS2.pdf

＜＜AS2 用通信機能確認項目）＞＞

本シートは、AS2 における接続に必要な機能をまとめたものです。ESP 間の相互接続を確認するためにご利用ください。なお、接続性を保証するものではございませんので、必ず接続確認を行ってください。

		AS2	必須：○ オプション：△
準拠仕様		バージョン　AS2 1.1	○
利用可能な認証方式		SSL サーバ認証	○
		SSL クライアント認証	○
		HTTP ベーシック認証	△
		AS2 メッセージの署名と検定	○
信頼性通信		MDN 要求：あり	○
		MDN 要求：同期モード	○
		重複メッセージの検出	○
		MDN を一定時間内に受信できない場合の再送	○
通信機能	送信機能	本書で推奨されたプロトコルの推奨パラメータでメッセージを送信することができる	○
		MIME の添付ファイル名欄を使ったメッセージ種の送信機能	○
		AS2 として XML メッセージの送信時に圧縮し、送信する機能	○
	受信機能	本書で推奨されたプロトコルの推奨パラメータでメッセージを受信することができる	○
		MIME の添付ファイル名欄を使ったメッセージ種の送信機能	○
		AS2 として XML メッセージの送信時に圧縮し、送信する機能	○

＜＜ebXML MS 用通信機能確認シート）＞＞

本シートは、ebXML MS における接続に必要な機能をまとめたものです。ESP 間の相互接続を確認するためにご利用ください。なお、接続性を保証するものではございませんので、必ず接続確認を行ってください。

		ebXML MS	必須：○ オプション：△
準拠仕様		バージョン AS2 1.1	○
利用可能な認証方式		SSL サーバ認証	○
		SSL クライアント認証	○
		HTTP ベーシック認証	△
信頼性通信		ACK（MSH Acknowledgement）要求：あり	○
		ACK 要求：同期モード	○
		重複メッセージの検出	○
		ACK を一定時間内に受信できない場合の再送	○
通信機能	送信機能	本書で推奨されたプロトコルの推奨パラメータでメッセージを送信することができる	○
	受信機能	本書で推奨されたプロトコルの推奨パラメータでメッセージを受信することができる	○

第二編.　　トランスレーション機能

3.　目的

本編は、国内の ESP が海外の企業や ESP と接続するときに必要となるトランスレーション機能について記述している。

トランスレーションを実施するうえで必要となるサービスとそれを実現する機能をまとめている。サービスとはトランスレーションを行ううえで具体的にやりたいこと、機能とは具体的に実現する方法を示している。一般に、その折使われるトランスレータは、さまざまなパッケージベンダーから提供されている。ここでは、そのトランスレータを利用するときの操作イメージを利用方法としてまとめた。

最後に、各社トランスレータ機能一覧を掲載している。これは製品優劣を示すのではなく、ユーザが必要とする機能を選択するときの指標となるべき項目一覧である。自社が必要とする機能のみを追うことにより、最適な機能構成のトランスレータを選ぶことができる。

4.　サービス機能（トランスレーション）

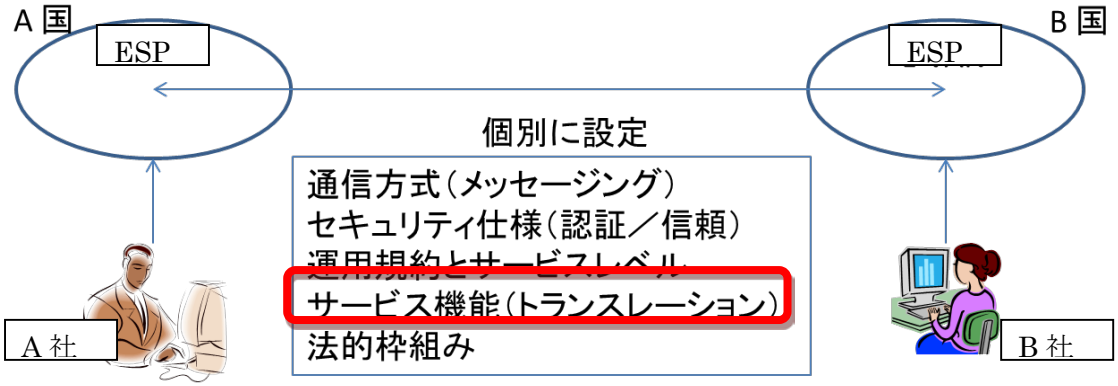
4. 1.　必要とされる機能の位置づけ

当資料での想定範囲

当資料作成においては、下図のような ESP 間国際接続(※１)を想定してサービス機能を検討している。A 国の ESP を使う A 社と、B 国の ESP を使う B 社の 2 社間の EDI を実現する際に必要となるサービス機能(トランスレーション)について記述する。

基本的に A 国 ESP と B 国 ESP 間は国際標準に準拠したメッセージ形式で交換されると想定するが、このメッセージ形式と A 社の採用する形式あるいは B 社の採用する形式へのトランスレーションが必要となる。

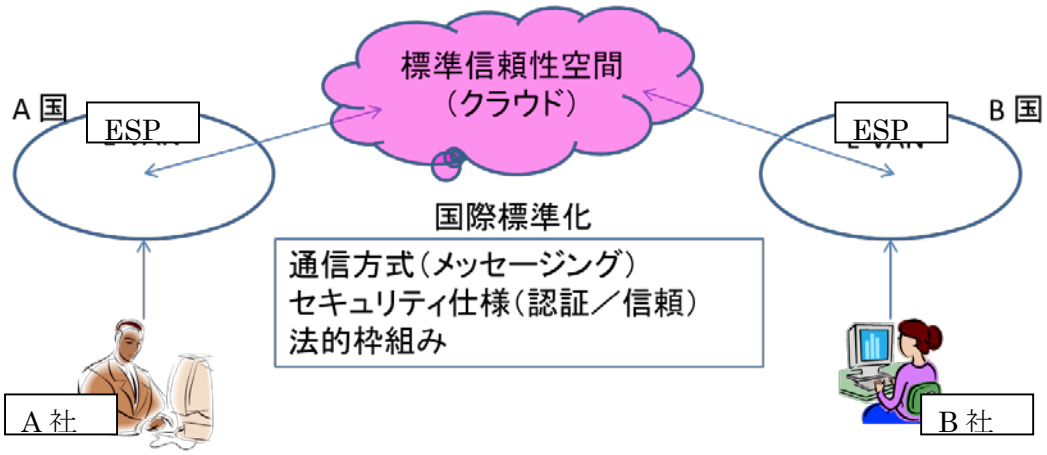
この際、各メッセージ形式で定義されるコードリストや値の取り方に互換性が無い場合には変換が困難となることも想定されるため、注意が必要である。このような非互換は法制度や慣習の違いに起因することが多い。（例：アレルゲンの分類など）



ESP 間の事前の合意により、メッセージのトランスレーションを必要としない（=メッセージを無加工で扱う）場合には、メッセージ形式・データ表現形式、メッセージで利用する文字エンコーディングなどを特に規定しない。双方で解釈できればよいものとする。

将来の検討可能性について

ESP 間国際接続にあたり、別途定義された標準信頼性空間を全ての ESP が利用することで個別の仕様調整を必要とせず接続性の確保ができることが望ましい。現段階では実現できていないが多くの ESP の賛同によりこのような形となることが理想的である。



1） 想定されるメッセージ形式・データ表現形式

取り扱うメッセージ形式は、これから挙げるようなものが想定される。

(ア) メッセージ標準

① ASC X12 系

1. ASC X12
2. HL-7
3. HIPAA

② EDIFACT 系

1. EDIFACT

   ※NACCS にも触れる
2. EANCOM
3. ODETTE
4. Tradacoms
5. VDA

③ XML 系

1. RosettaNet PIP
2. SWIFT MX

   (ア) ISO7775

   (イ) ISO20022 XML

   (ウ) ISO15022

3. ACORD
4. CIDX
5. NACHA
6. PAA
7. GS1 XML(BMS)

概要：

GS1 XML は EANCOM と並ぶ GS1 の EDI 標準である。BMS(Business Message Standards)と呼ばれることもある。UN/CEFACT Modelling Methodology に準じて開発が行われている。初期バージョンは 2002 年に発表され 2014 年 1 月現在の最新バージョンは 3.1 で、多くのビジネスプロセスを対象とした約 100 種類のメッセージが公開されている。

日本国内で小売業を中心とした流通業界で策定され現在普及が進みつつある『流通 BMS』は別のものである。

対象範囲：

小売業界を中心に導入されているが、外食産業や建設業界で導入が進んでいる国もある。ドイツ連邦銀行が商業銀行との間の現金輸送の情報交換に利用している。スペイン、オーストリアなどの欧州大陸の中央銀行にも広がる可能性がある。

対応方法・情報入手先：

GS1 のグローバルサイトから情報を入手可能である。

http:www.gs1.org/ecom/xml

④　CII 標準(EIAJ)

⑤　その他の日本国内の業界標準

※各標準は列記しない前提で、固定長の業界標準への対応指針を書く。

参考：全銀、J 手順、PLANET(固定長)、日食協、E-VAN などを想定して記述

(イ) アプリケーションベンダー独自表現形式

①　IDOC
②　Oracle
③　Microsoft(Excel)
④　People Soft
⑤　QAD

(ウ) その他の一般的なデータ表現形式

標準仕様が無い場合によく使われている形式について説明する。

① CSV　RFC4180
② 固定長
バイト列であり、レイアウトの確認が必要、等の説明。
バイト数(文字数)

4.2.　想定される文字コードと取扱い

ESP 間でメッセージのトランスレーションが必要となる場合、双方で共通した文字コードの理解が必要となる。

普段利用している言語が異なるもの同士が対話をする以上、文字集合としては国際的な共通言語である英語を利用するものと考える。

□英アルファベット
□数字
□記号
ただし、各言語で存在する固有の文字（例えば、漢字）を利用したいケースも想定される。この場合は、世界中すべての文字を共通の文字集合として利用できる Unicode（ISO/IEC 10646）を利用するのが自然と考える。

その観点で、各 ESP がサービスするトランスレーション機能としては、最低限、以下の文字エンコーディングをサポートする必要がある。

□ISO/IEC 646
□EBCDIC
□UTF-8
□UTF-16
ただし、上記に挙げた文字エンコーディング以外であっても、ESP 間双方が互いに理解できるトランスレーション機能を持っている場合においては、この範囲に限定しない。

以下、サポートする文字エンコーディングの概要を説明する。

ISO/IEC 646

□ISO/IEC 646 は、7 ビットの文字コードを規定する ISO（国際標準化機構）標準。

□ISO/IEC 646 IRV（International Reference Version：国際基準版)が、ASCII と同じ図形文字集合を用いている。

□ISO/IEC646 は、ASCII の図形文字集合を各国で使用できるようにしたもの。国際基準版をベースにして、各国の都合に応じて文字を変更してもよい符号位置を定めている。

□日本版の ISO/IEC646 は、JIS X 0201 として標準化されている。

文字表

	0	1	2	3	4	5	6	7
0	NUL	DLE	SP	0	@	P	`	P
1	SOH	DC1	!	1	A	Q	a	Q
2	STX	DC2	“	2	B	R	b	R
3	ETX	DC3	#	3	C	S	c	S
4	EOT	DC4	$	4	D	T	d	T
5	ENQ	NAC	%	5	E	U	e	u
6	ACK	SYN	&	6	F	V	f	v
7	BEL	ETB	‘	7	G	W	g	w
8	BS	CAN	(	8	H	X	h	x
9	HT	EM	)	9	I	Y	i	y
A	LF	SUB	*	:	J	Z	j	z
B	VT	ESC	+	;	K	[	k	{
C	FF	FS	,	<	L	＼	l	|
D	CR	GS	-	=	M	]	m	}
E	SO	RS	.	>	N	^	n	―
F	SI	US	/	?	O	_	o	DEL

国際基準版を基準とし、以下の 12 文字の割り当てを変更したものが各国版となる。

コード	国際基準版	各国版	JIS X 0201 ラテン文字集合
0x23	#	いずれかを選択 #（番号記号） £（ポンド）	#
0x24	$	いずれかを選択 $（ドル記号） ¤（不特定通貨記号）	$

コード	国際基準版	各国版	JIS X 0201 ラテン文字集合
0x40	@	任意の文字	
0x5B	[		
0x5C	＼		¥ (円記号)
0x5D	]		
0x5E	^		
0x60	`		
0x7B	{		
0x7C	|		
0x7D	}		
0x7E	~		￣ (オーバーライン)

EBCDIC

□IBM 社によって開発された、主に IBM 系のメインフレームで採用される 8 ビットの文字コード。

□256 個の文字、数字と記号の表示が可能であり、58 文字が規定されている。

□各ベンダーにより独自に拡張されているため、多数のコードが存在する。

□日本語用 EBCDIC としては、一般的に EBCDIK と呼ばれる、空き領域にカタカナを追加したものが存在する。

文字表

以下の 58 文字が規定されている。

	4	5	6	7	8	9	A	B	C	D	E	F
0	SP	&	-									0
1			/						A	J		1
2									B	K	S	2
3									C	L	T	3
4									D	M	U	4
5									E	N	V	5
6									F	O	W	6
7									G	P	X	7
8									H	Q	Y	8
9									I	R	Z	9
A				:								
B	.		,	#								
C	<	*	%	@								
D	(	)	_	'								
E	+	;	>	=								
F			?	"								

UTF-8

□Unicode（ISO/IEC 10646）の文字集合を表現するための文字エンコーディング方式のひとつ。

□1 文字を、8 ビットの可変長マルチバイト（1～4 バイト）で表現する。

□ISO/IEC 646 IRV（= ASCII）と互換性がある。

UTF-16

□Unicode（ISO/IEC 10646）の文字集合を表現するための文字エンコーディング方式のひとつ。

□1 文字を、16 ビットを単位とした可変長マルチバイト（2 または 4 バイト）で表現する。

□ISO/IEC 646 IRV（= ASCII）と互換性がない。

メッセージ標準における文字エンコーディング

前述したメッセージ標準とそのメッセージで利用する文字エンコーディングの関係について、以下に整理する。

X12 メッセージで利用可能な文字エンコーディング

X12 では、以下の文字集合が利用可能と規定されている。文字エンコーディング方式としては、「ISO/IEC 646 IRV（= ASCII）」と「UTF-8」が推奨されている。

基本文字集合									
A...Z	0...9	!	“	&	‘	(	)	*	+
,	-	.	/	:	;	?	=	SP	
拡張文字集合									
a...z	%	~	@	[	]	_	{	}	¥
|	<	>	#	$					

EDIFACT メッセージで利用可能な文字エンコーディング

EDIFACT では、メッセージヘッダーにあたる UNB セグメントに、メッセージで利用する文字エンコーディングをキーワード指定する。

Ex.
UNB+**UNOA**:3+5012345678901:14+4598765432198:14+000316:1402+INV73529++INVOIC'

キーワード	エンコーディング
UNOA	ISO 646（a...z の英子文字を除く） . , – ( ) / = (space)
UNOB	ISO 646　All of UNOA ' + : ? ! " % & * ; < >
UNOC	ISO 8859-1 (Part 1: Latin alphabet No. 1)
UNOD	ISO 8859-2 (Part 2: Latin alphabet No. 2)
UNOE	ISO 8859-5 (Part 5: Latin/Cyrillic alphabet)
UNOF	ISO 8859-7 (Part 7: Latin/Greek alphabet)
UNOG	ISO 8859-3 (Part 3: Latin alphabet)
UNOH	ISO 8859-4 (Part 4: Latin alphabet)
UNOI	ISO 8859-6 (Part 6: Latin/Arabic alphabet)
UNOJ	ISO 8859-8 (Part 8: Latin/Hebrew alphabet)
UNOK	ISO 8859-9 (Part 9: Latin alphabet)
UNOX	ISO 2022-JP（JIS コード）
UNOY	ISO 10646 (Unicode)

XML メッセージで利用可能な文字エンコーディング

XML では、メッセージの先頭に記述する XML 宣言中で、利用する文字エンコーディングを明示する。

Ex. <?xml version="1.0" **encoding="UTF-8"** standalone="yes"?>

Encoding 属性に記述できる値（名称）は、IANA（Internet Assigned Numbers Authority）に登録されたキャラクタセット名を使用する。IANA は、インターネットにおいて名前や番号の登録を必要とする情報に関して登録業務を行う組織

□キャラクタセット一覧：

http://www.iana.org/assignments/character-sets/character-sets.xhtml

5.　トランスレータの利用方法

多くのトランスレータは、「①変換定義体の作成」、「②データの変換」の 2 つの機能から構成されている。よって、トランスレータの利用方法は、「開発端末で変換定義体を作成」、変換定義体を「変換環境に反映」という流れになる。

変換定義体の作成は GUI 形式のマッピングツールが準備されており、開発担当者はこのマッピングツールを使用して行う。

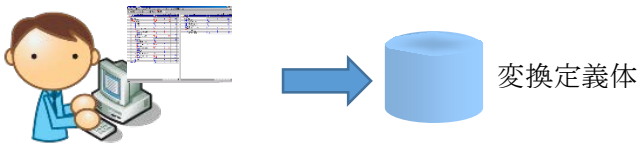
データの変換処理は、変換定義体、入力ファイル、出力ファイルなどを指定したパラメーターを元に変換を行う。

5.1.　変換定義の作成

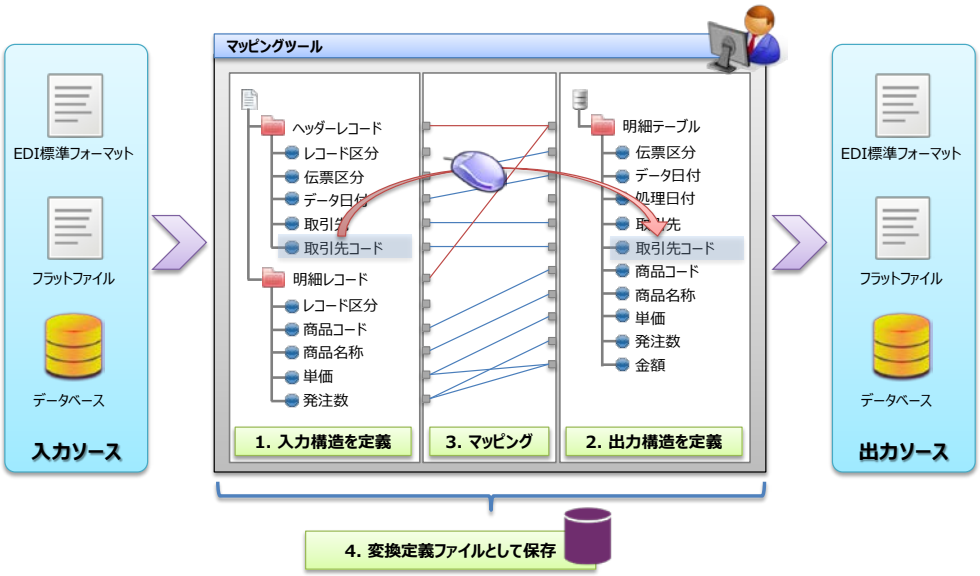
変換定義の作成は以下のようになる。

①入力ファイルおよび出力ファイルのレイアウト情報の作成
②出力ファイル作成に必要な変換処理（入力ファイルと出力ファイルの紐付け）を定義
　（文字コードの変換、レイアウトの変更など）
③変換定義体ツールの中で単体テストを実施
　　③　換定義体ファイルを作成

【変換定義の作成イメージ図】



【マッピングツールのイメージ図】

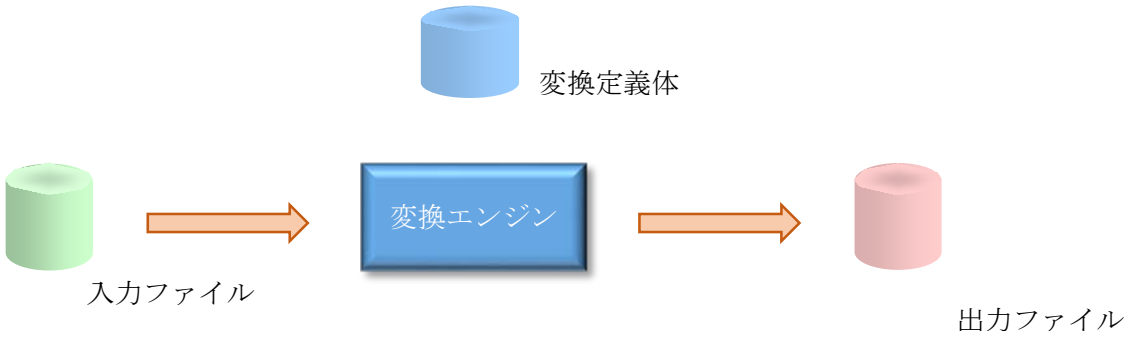


5. 2.　データの変換

データの変換処理を行う変換モジュールは、変換定義体、入力ファイル、出力ファイルなどを指定したパラメータを元に変換を行う

【コマンドイメージ】

変換モジュール.exe　　変換定義体　　入力ファイル　　出力ファイル　etc



6.　トランスレータ比較

比較項目＼企業名		A社	B社	C社	D社
基本情報	最新バージョン	Ver5.16.0	Ver4.0	Ver7.0	Ver 5.2.5
	構成の考え方	変換のマップを作成するマッパー 変換を行う変換エンジン	各種変換フォーマット用途に特化したパッケージソフトウェア （CII、EDIFACT、汎用、XMLで製品を	汎用機／オフコン／UNIXなどのホストのファイル転送データと、パソコンの標準であるWindowsファイルとのデータ交換をする汎用性の高いファイル変換ユーティリティ。 Windowsファイル間のデータ変換もできる。 Server系OSで動作するServer版とDesktop系OSで動作するDesktop版の2種類がある。	・シングルサーバ構成 ・分散構成(クラスタリング構成) ・別途、DBMSが必要 - MS-SQL Server 2008 R2 SP1/2012 SP1 - Oracle 11g R1/R2 - DB2 9.7/10.1/10.5 - MySQL Enterprise Edition 5.1.45 以上
	サポートOS	●マップ： Windows7,8、Windows Server 2003,2008,2012 ●変換エンジン：JDK 5,6,7,8 ●検索用DB： SQLServer2005,2008,2012,2014 Oracle:10,11,12C、 DB2:8，9、 MySQL：5 Symfoware：10,12	Windows Server 2003～2012、Windows 7,8等のMS系OS	Windows Server 2003, 2008, 2012 Windows XP, Vista, 7, 8, 8.1	・Windows Server 2008 R2(64bit) ・IBM AIX 5.3/6.1/7.1 ・Oracle Solaris 9/10/11 ・HP-UX 11.23/11.31 for IA64(Itanium) ・Red Hat Enterprise Linux Release 5.5/6.1 ・SuSE Linux Enterprise Server 10/11
変換定義ツール	GUIマッパー	○	○	○	○
	GUI連携フロー設計	×	×	×	○
	（書式・スキーマのインポート機能）				
	iDoc	○	×	×	○
	COBOL	○	×	×	○
	XML（ＤＴＤ，スキーマ）	○	○	×	○
	DB	○	○	×	○
	（書式・スキーマのエクスポート機能）				
	XML（スキーマ）	○	×	×	○
	その他	○	○	×	○
	ドラッグ＆ドロップでの対	○	×	×	○
	文字コード編集機能	○	○	○	×
	外字登録機能	○	○	○	×
	データベース接続機能	○	○	×	○

フォーマット変換	（ファイルフォーマット）				
	【ASC X12】				
	ASC X12	○	×	×	○
	HL-7	×	×	×	○
	HIPAA	×	×	×	○
	【EDIFACT】				
	EDIFACT（ODETTE）	×	○	×	○
	Tradacoms	×	×	×	○
	VDA	×	×	×	○
	【XML】				
	RosettaNet　PIP	○	○	×	○
	SWIFT MX	×	×	×	○
	ACORD	×	×	×	×
	CIDX	×	×	×	○
	NACHA	×	×	×	○
	PAA	×	×	×	×
	【CII】				
	テキストベース	○	○	×	○
	XMLベース	×	×	×	○
	【ベンダー独自】				
	IDoc	○	×	×	○
	【その他】				
	CSV、TSV	○	○	○	○
	固定文字形式（UTF-8）	○	○	×	○
	（DBフォーマット）				
	Oracle	○	○	×	○
	SQL Server	○	○	×	○
	DB2	○	○	×	○
	DB2 for iSeries	○	×	×	○
	MySQL	○	○	×	○
	PostgresSQL	○	○	×	×
	Symfoware	○	×	×	×
	その他DBフォーマット		MDB		

	ASCII	○	○	○	○
	EBCDIC	○	○	○	○
	SJIS漢字	○	○	○	○
	JIS漢字	○	○	○	○
	EUC漢字	○	○	○	×
	IBM漢字	○	○	○	×
	JEF漢字	○	○	○	×
	KEIS漢字	○	○	○	×
	NEC漢字	○	○	○	×
	UNISYS漢字	○	○	○	×
	UTF-8	○	○	○	○
	UTF-16	○	○	○	○
コード変換	Shift_JIS-2004	○	○	×	SJIS (Shift-JIS, Japanese)
	ISO-2022-JP-2004	○	○	×	ISO2022JP (JIS X 0201, 0208 in ISO 2022 form, Japanese)
	EUC-JIS-2004	○	○	×	EUC_JP (JIS X 0201, 0208, 0212, EUC encoding, Japanese)
	ISO/IEC 8859-1	×	○	×	ISO8859_1 (ISO 8859-1, Latin
	メーカー固有拡張漢字（要	○（要外字登録）	○	○	×
	その他文字コード			三菱MELCOM漢字、東芝標準漢字、カシオ標準漢	×

属性変換	（外部形式）				
	基本文字列	○	○	○	○
	漢字IN文字列	○	○	○	×
	10進数形式	○	○	○	○
	ゾーン10進数形式	○	○	○	×
	パック10進数形式	○	○	○	○
	DateTime形式	○	○	○	○
	指数形式	×	×	×	○
	バイナリ2進数	×	○	○	○
	RawBiary形式	×	×	○	○
	Base64Binary形式	×	×	×	×
	HexBinary形式	×	○	×	×
	Boolean形式	×	○	×	×
	（内部形式）				
	文字列型	○	○	○	○
	整数型	○	○	○	○
	実数型	○	×	○	○
	バイナリ列型	○	○	○	○
	日付時刻型	○	○	○	○
	論理型	○	×	×	×
	（書式）				
	日付（西暦・和暦）、時刻	○	○	○	○
	数字	○	○	○	○
	符号	○	○	○	○
	通貨	×	○	○	×
	桁区切り	○	○	○	×
	小数点	○	○	○	○
	パディング機能	○	○	○	○
	デフォルト値の設定	○	○	×	○
	マスク機能	○	○	○	×
	右詰・左詰・両詰機能	○（両詰だけ未対応）	○	×	○
	（数値の丸め処理）				
	切り上げ	○	○	×	
	切り捨て	○	○	○	
	四捨五入	○	○	×	○
	五社六入	○	×	×	
	丸め処理の必須／省略	○	○	×	

属性変換（続き）	項目の入れ替え	○	○	○	○
	レコード関連項目編集	○	○	×	○
	項目属性の変換	○	○	×	○
	項目統合	○	○	×	○
	大文字⇔小文字変換	○（関数を提供）	○	×	○
	半角⇔全角変換	〔半角カナ->全角変換はあ	○	○	×
	項目演算（数値、日付）	○	○	×	○
	空値判定	○	○	×	○
	出力条件	○	○	×	○
	レコード識別	○	○	×	○
	ループ構造処理	○	○	×	○
	環境変数・内部変数・定数	○	○	×	○
	妥当性検証	入力ファイルは構造チェックが可能。出力側では式を使って値の検証は可	○	×	○
	フィルター機能	出力先のデータ分岐条件で対応	○	×	×
	処理単位（読込単位（入力データを一定の単位で分割）・コミット単位）	○	○	×	○

エラー制御	継続	○	○	×	○
	スキップ	○	×	×	○
	エラー停止	○	○	○	○
	例外処理・代替処理	×	×	×	○
プロファイリング	プロファイリング機能	×	×	×	×
クレンジング	クレンジング機能	×	○	×	×
レポート	変換結果レポート	○	○	○	○
関数	四則関数	○	○	○	○
	日付関数	○	○	×	○
	文字列関数	○	○	×	○
収集集計機能	テーブル／レコード／DB核	○	○	×	○
	統計カウンタ（入力/出力のレコード件数や特定項目列の合計値/平均値/最大値/最小値な	○	○	×	○
多言語対応	日本語	○	○	○	○
	英語	○	×	×	○
	その他言語	×	×	×	German,Spanish,French,Italian,Korean,Dutch,他
サポート			○	「年間サポート・サービス」を標準提供（要ユーザ登録） ・ 電話による質問への対応 ・ Mailによる質問への回答 ・ バグ修正版の無償提供	平日9:00-17:30

第三編.　　セキュリティ

7.　通信路のセキュリティ

通信プロトコルで実現される内容のため、ここでは検討しない。

8.　認証と信頼性

8.1.　メッセージの信頼性

C.1 Security threats

The storage and transfer of EDIFACT messages/packages via electronic media and means expose them to a number of threats, notably:

* the unauthorized disclosure of message/package content
* the intentional insertion of non-bonafide messages/packages
* the duplication, loss or replay of messages/packages
* the modification of message/package content
* the deletion of messages/packages
* the repudiation of message/package responsibility by its sender or its receiver

These threats may be intentionally perpetrated, as with the unauthorized manipulation of message/package content, or unintentionally perpetrated, as with a communication error resulting in the modification of message/package content.

C.2 Security solutions - basic services and principles of usage

To counter the aforementioned threats a number of security mechanisms have been identified which utilize one or more methodologies to meet their objectives.

It is important to be able to identify unambiguously the parties involved when messages/packages are secured - the security originator, henceforth called the sender for simplicity, who secures the message/package prior to transmission, and the security recipient, henceforth called the receiver, who performs checks on the received message/package. These parties may be identified in the security segments. This identification may be performed by means of so-called certificates, (in fact, either the certificate itself or a certificate reference), explained below, if asymmetric algorithms are used.

Typically, the use of a certification authority (CA) is required in an open system. This is a third party which is trusted by the involved parties to a limited degree, namely to identify and register all users with their public key.

This information is conveyed to other users by means of a certificate, which is a digital signature issued by the CA on a message which consists of user identification information and the user's public key. In this situation, the trust is purely functional and does not involve secret or private keys.

Alternatively, if symmetric techniques are used the identity of the parties involved would be indicated in the security sender/recipient name fields.

A message/package may be secured by several parties (for example a essage/package may have multiple digital signatures) and so the security related information may be repeated to allow the identification of several signing or authenticating parties and correspondingly to include several digital signatures or control values.

C.2.1 Sequence integrity

Sequence integrity protects against the duplication, addition, deletion, loss or replay of a EDIFACT structure (message/package, group or interchange).

To detect lost messages/packages, groups or interchanges

- ☐the sender may include and the receiver check a sequence number (related to the message/package flow between the two parties concerned);
- ☐the sender may request and check an acknowledgement.

To detect added or duplicated messages/packages, groups or interchanges

- ☐the sender may include and the receiver check a sequence number.
- ☐the sender may include and the receiver check a time stamp.

When sequence numbers are used it shall be agreed between the parties how these are to be managed.

The timestamp will normally be produced by the sender‘s system. This implies, as in the paper world, that the initial accuracy of the value of the timestamp is solely under the control of the sender.

In order to give full protection, the integrity of timestamp or sequence number shall be guaranteed by one of the other functions mentioned below.

C.2.2 Content integrity

Content integrity protects against the modification of data.

Protection may be achieved by the sender including an integrity control value. This value may be computed by using an appropriate cryptographic algorithm, such as an MDC

(Modification Detection Code). As this control value in itself is unprotected, additional measures, such as forwarding the control value by a separate channel or calculating a digital signature, to actually provide non-repudiation of origin, on the control value are necessary.

Alternatively, origin authentication, which is obtained using a message authentication code, will imply content integrity. The receiver computes the integrity control value of the data actually received using the corresponding algorithms and parameters and compares the result with the value received.

In conclusion, content integrity in EDI is typically obtained as a sub-product of origin authentication or non-repudiation of origin.

C.2.3 Origin authentication

Origin authentication protects the receiver against the actual sender of a message/package, group or interchange claiming to be another (authorized) party.

Protection may be achieved by including an authentication value (for example, MAC: message authentication code). The value depends both on the data content and on a secret key in the possession of the sender.

This service may include content integrity and may be obtained as a sub-product of non-repudiation of origin.

In most cases, it would be desirable to have at least origin authentication.

C.2.4 Non-repudiation of origin

Non-repudiation of origin protects the receiver of a message/package, group or interchange from the sender's denial of having sent it.

Protection may be achieved by including a digital signature (or by using an appropriate implementation of the function described under "origin authentication" based on tamper resistant hardware or trusted third parties). A digital signature is obtained by encrypting, with an asymmetric algorithm and a private key, the object or a control value derived from the data (by using a hash function, for example).

The digital signature may be verified by using the public key which corresponds to the private key used to create it. This public key may be included with the interchange agreement signed by the parties or be included in a certificate digitally signed by a certification authority. The certificate may be sent as part of the EDIFACT structure.

The digital signature provides not only non-repudiation of origin but also content integrity and origin authentication.

C.2.5 Non-repudiation of receipt

Non-repudiation of receipt protects the sender of a message/package, group or interchange from the receiver's denial of having received it.

Protection may be achieved by the receiver sending an acknowledgement which includes a digital signature based on the data in the original EDIFACT structure. The acknowledgement takes the form of a service message from the receiver to the sender.

C.2.6 Confidentiality of content

Confidentiality of content protects against the unauthorized reading, copying or disclosure of the content of a message/package, group or interchange.

Protection may be assured by encrypting the data. Encryption may be performed by using a symmetric algorithm with a secret key shared by the sender and the receiver.

However the secret key may be transmitted securely by encrypting it under the receiver's public key using an asymmetric algorithm.

C.2.7 Interrelation among security services

As noted already, some services by nature encompass other services, and it is thus not necessary to additionally include the services which are achieved implicitly. For example, the use of the mechanism to provide non-repudiation of origin implies content integrity.

The following table summarizes these interrelations:

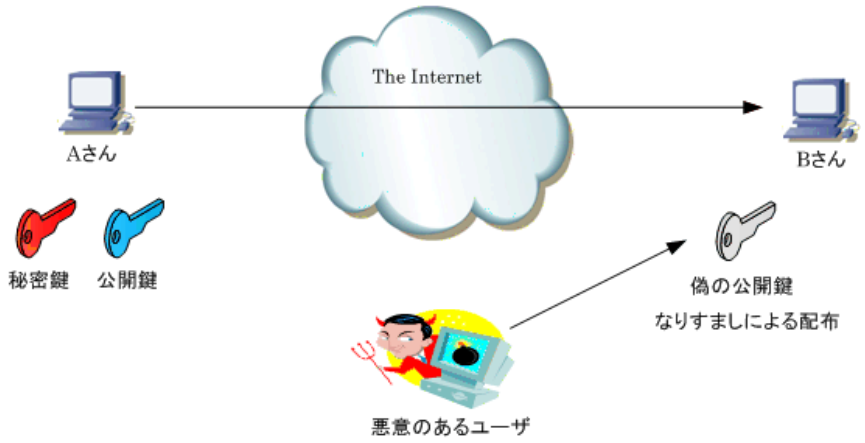
	Content Integrity	Origin Authentication	Non-repudiation of origin
Content Integrity	yes		
Origin Authentication	yes	yes	
Non-repudiation of origin	yes	yes	yes

8. 2.　デジタル署名の仕組み

デジタル証明書とは

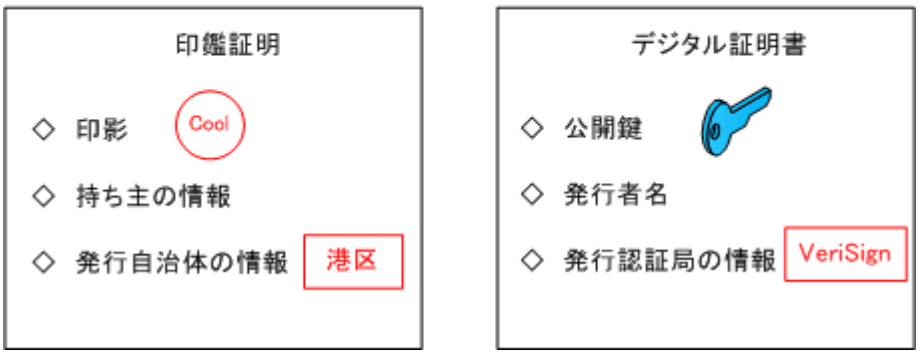
デジタル署名により、データの改ざんは検知することが分かりました。しかしながら、デジタル署名だけではそもそも配布されている公開鍵が本当に正しい公開鍵（下図では A さんの公開鍵）なのかを確認することができません。デジタル署名の解析用の公開鍵が正しいことを証明するためには**デジタル証明書**を使用する。

【 不正な公開鍵の配布 】



デジタル証明書をデジタル署名に付属させることで、データの改ざんを検知できるだけでなく、公開鍵が正しいものであると確認できて、さらには認証局(CA)を通してデータの作成者を証明することができます。
デジタル証明書のフォーマットは ITU-T X.509 で規定されています。印鑑証明書と比較して見てみましょう。

【 リアルの印鑑証明書 & バーチャルの電子証明書 】

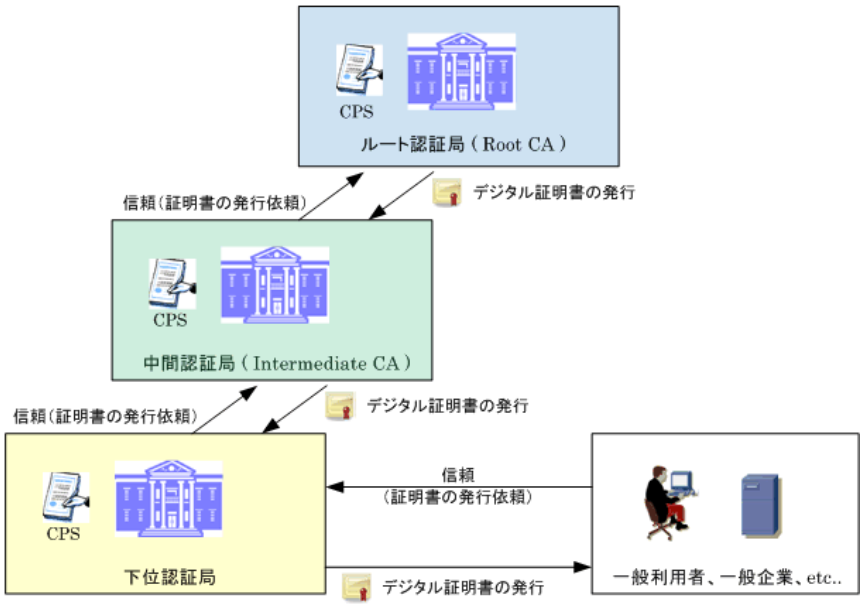


認証局（CA）と

デジタル証明書を発行する機関のことを認証局(CA)と言います。商用の有名な認証局にはベリサインがある。
商用の認証局からデジタル証明書の交付を受けるためには時間と費用がかかるため、組織内でローカルに認証局を構築して証明書を発行することもできます。しかしそのようなWeb サイトに一般ユーザがアクセスしてデジタル証明書を受け取ったとしても、Web ブラウザ上で警告メッセージが表示されることになります。一方でベリサインなどのデジタル証明書は、すでに Web ブラウザにインストールされているため警告表示は出ません。

最上位の位置づけの認証局は**ルート認証局**という。ルート認証局は最上位のため、上位の認証局による承認を受けることなく正当性を証明しています。ルート認証局以外の認証局は**中間認証局**と呼ばれている。中間認証局は、ルート認証局などの上位の局からデジタル証明書を発行してもらうことで正当性を証明します。ルート認証局自身は正当性を証明するために、厳しい監査を受けていることや、**CPS**(認証業務運用規程) を公開することにしています。また、今までの認証局の運用実績等の社会的な根拠に基づいて信頼されている。

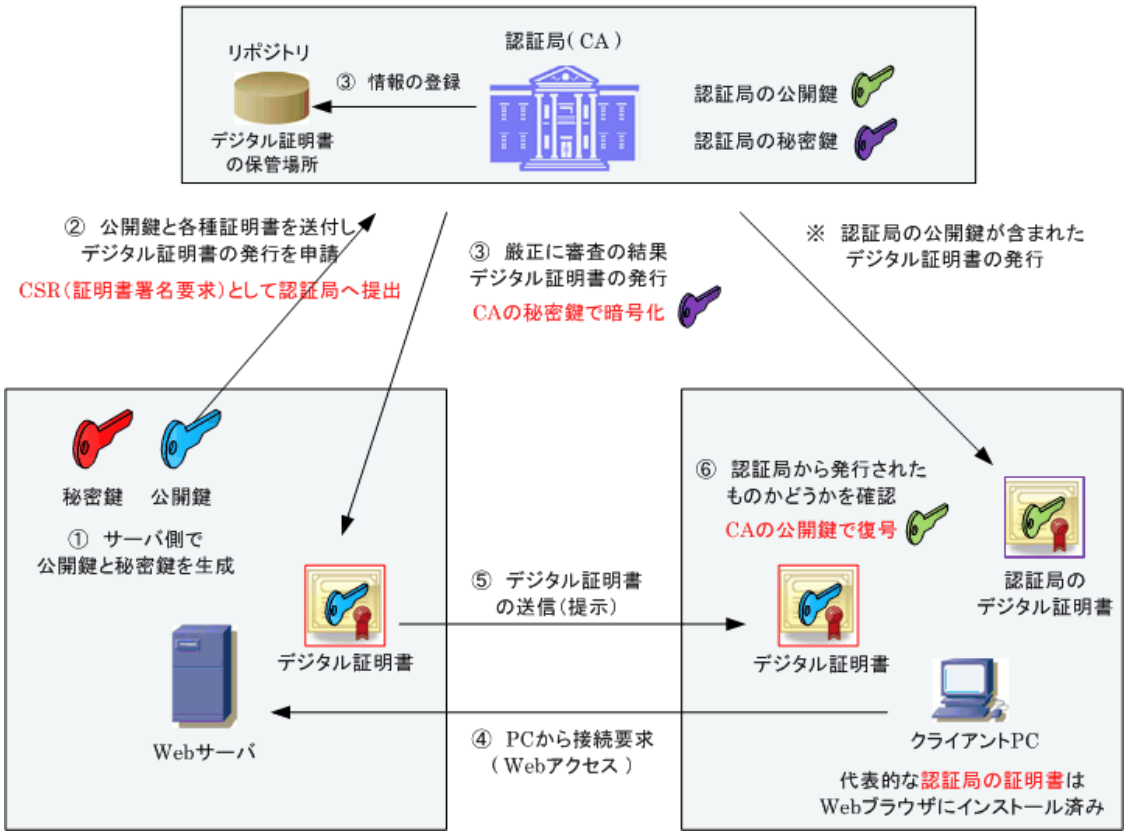
【 認証局（CA）の階層構造 】



デジタル証明書の仕組み

認証局（CA)から発行されたデジタル証明書を利用したデジタル署名により、データの改ざんを検知することができるだけでなく、公開鍵が正しいものであると確認できて、さらにはデータの作成者を証明することができます。

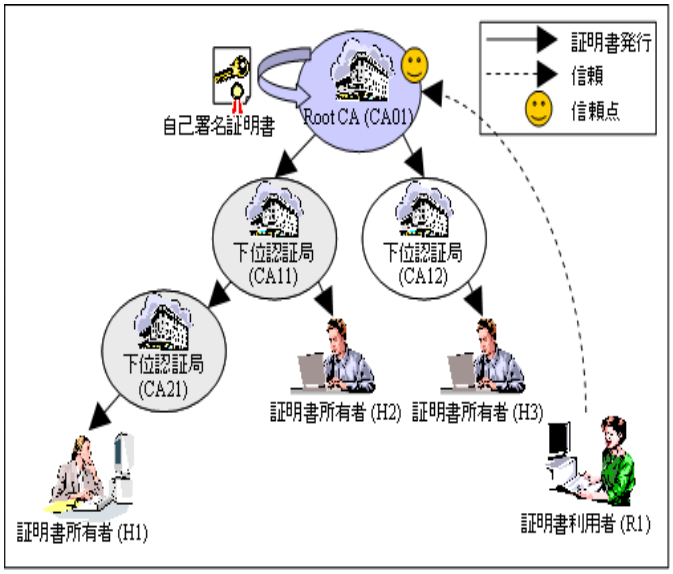
【 デジタル証明書を使用したデジタル署名の仕組み 】



8.3.　認証局の認証

階層型モデル

複数の CA を階層型（ツリー構造）に構成する方式



Pros:

□認証パスが簡単で、設定は容易
□信用点一個しかないので、検証の設定は簡単

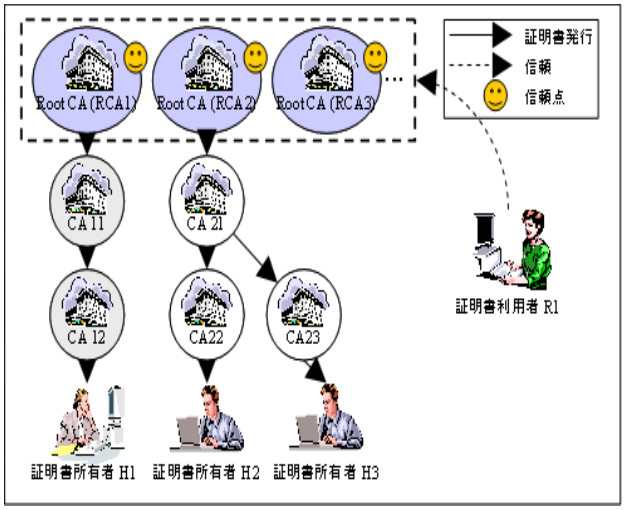
Cons:

□異なる CP の場合、対応は難しい
□万一 、ルート CA の信用が失われると、配下の全ての下位 CA の信用も失われてしまう

SIPS の場合、現実ではない

Web モデル

あらかじめクライアントのアプリケーションにルート CA の一覧を埋め込む方式（Web ブラウザで用いられている）



Pros:

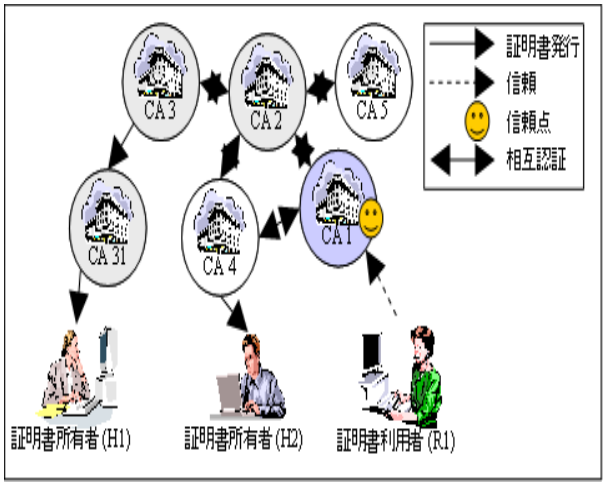
- 利用者側の設定なし
- ブラウザに事前登録されたルートを信用する
- Root は WebTrust または ETSI の定期監査を受けることで、信頼性がある
- 更に、CABForum の基本要件を満たすことで、一層信頼性が高まる

Cons:

- 第三者（ブラウザ、監査機構など）に依存
- 利用者はルートの信頼性は確認できない

３．メッシュ・モデル

複数の CA を相互認証により接続する方式



上図において、CA1 を信頼する R1 が、H1 の証明書を検証する場合、構築される認証パスは、「CA1→CA2→CA3→CA31→H1」および「CA1→CA4→CA2→CA3→CA31→H1」となる

Pros:

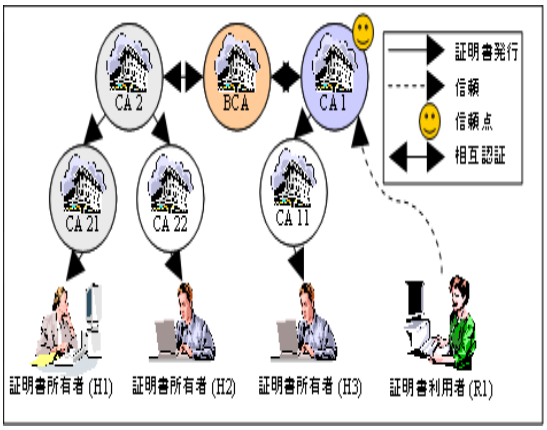
- 異なる CA ドメインを柔軟に接続することができる

Cons:

- 認証構造が複雑になるため、認証パスの構築にコストがかかる

4. ブリッジ CA モデル

複数の CA がブリッジ CA を介して接続する方式



上図において、CA1 を信頼する R1 が H1 の証明書を検証する場合、構築される認証パスは「CA1→BCA→CA2→CA21→H1」となる

Pros:

- 相互認証の数を抑えながら、柔軟な構成をとることができる

Cons:

- ポリシーのマッピングは煩雑
- 証明書のステータス確認は難しい

日本の GPKI には BCA があったが、現在は廃止されている,米国の FBCA は運営中

8. 4.　信頼性の実装

1.　ebXML CPP/CPA 解説

(1) CPPA の目的

ebXML のメッセージングの仕様(Message Service)は HTTP のような特定の転送プロトコルとは独立に設計されています。セキュリティ機構や信頼性通信のように、オプションで使用できる仕組みも用意されています。また、用いるメッセージの種類や交換順序の定義(ビジネスプロセス定義)は一つに決まっているわけではなく、BPSS (Business Process Specification Schema)によって様々に定義されます。

このため、取引を企業間で正しく実行するには、通信に用いる規約やパラメタ、ビジネスプロセス定義等を、取引の当事者双方で予め合意しておかなければなりません。例えば、自社の通信ソフトウェアが受領通知(acknowledgment)を必要としているのに、取引相手が受領通知を送らない設定でソフトウェアを動かしていたら、取引は全く進みません。

そこで、このような取り決めを厳密に合意し、ソフトウェアを正しく設定するための仕組みが ebXML の標準として用意されています。それが CPP (Collaboration Protocol Profile)、CPA (Collaboration Protocol Agreement)です。この二つをあわせて CPPA と呼ぶこともあります。

CPP は、取引を行う企業のメッセージ交換の能力を記述します。例えば、転送プロトコルに何を使うか、暗号化や署名はどのような方式で行うか、また、どのビジネスプロセス定義のどの役割を実行できるかといったことを表します。

CPA は、取引を行う企業双方で合意したメッセージ交換の合意内容を記述します。CPA は双方の CPP を元にして作成します。取引を実行する際は、CPA で合意した方式に則ってメッセージ交換を進めることになります。

CPP/CPA は XML 文書として記述します。人間が目で読むだけでなく、ソフトウェアが読み込んで自動的に設定できるよう設計されています。

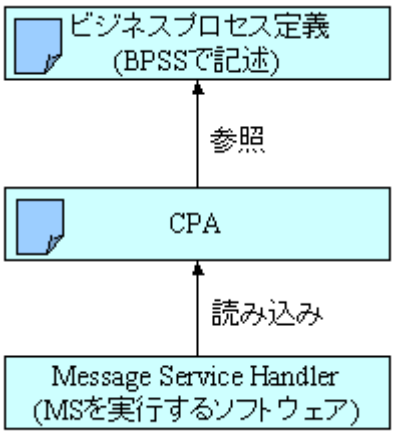
(2) ebXML の他の仕様との関係

CPA には通信に使うプロトコルやパラメタが書かれています。このため、ebXML Message Service (MS)を実装するメッセージサービスハンドラ(MSH)は、CPA から情報を得て設定を行います。また、MS のメッセージヘッダに設定する Service や Action といった要素の内容も CPA で決めます。

CPA は、各企業がビジネスプロセスのどの役割を実行するかを示します。このため、CPA には BPSS で記述したビジネスプロセス定義への参照を含みます。各企業は、参照先のビジネスプロセス定義に従って取引を進めなくてはなりません。

つまり、MS を使うための詳細を指定するために CPPA を利用し、CPPA は BPSS を参照するという形で、これらの仕様は関係しあっています。この様子を下図に示します。

なお、メッセージサービスやビジネスプロセス定義には、必ずしも ebXML の MS や BPSS を使う必要はなく、同等の機能を実現する仕様であれば CPPA とともに使用できることになっています。



(3) CPPA の使用の流れ

企業間で取引を開始するために CPPA がどう使われるか、一般的なストーリーを描いてみましょう。

ebXML で取引を行う企業は、自社の CPP を作成します。つまり、自社が実行できるビジネスプロセス定義(例えば電子部品の受発注業務)を参照し、そのプロセスのどの役割を実行できるか(発注者か受注者か)を示します。また、転送プロトコルとして HTTPS を使い、メッセージの再送は 3 回までといったことや、メッセージの受信に使う URL なども指定します。

次に、取引相手との間で互いの CPP を照らし合わせて、CPA を作成します。もし複数の企業との間で似たような CPA を作るなら、CPA のテンプレートを作成しておく方法もあります。取引相手の CPP との間で通信方式などに食い違っている点があれば、交渉してすりあわせます。CPP/CPA は XML 文書なのでテキストエディタや XML エディタでも編集できますが、CPA 専用のツールを使えばより効率的に作業できます。

取引相手との間で食い違いが解消されたら、合意に達した CPA として完成させます。完成した CPA は、取引当事者双方が同じコピーを保存します。

CPA が完成したら、ebXML の取引を実行するソフトウェアに CPA を入力として与え、合意内容に即して設定します。これで、取引を実行する準備が整いました。

(4) CPP の構成

それでは CPP の具体的な構成を見ていきましょう。CPP には多くの要素・属性がありますが、ここでは細部は省略して、重要な点を中心に説明します。

CPP の最上位要素は CollaborationProtocolProfile 要素です。以下の内容を持ちます。

(4-1) 企業の情報—PartyInfo 要素

PartyInfo 要素は CPP の中心的な役割を果たす要素です。子要素として以下を含みます。

・企業の識別子と参照情報—PartyId、PartyRef 要素

PartyId 要素は、企業コードなどの識別情報を表します。例えば DUNS 番号などが相当します。

PartyRef 要素は企業の情報が得られる Web サイトへのリンクを表します。

. 企業の役割—CollaborationRole 要素

CollaborationRole 要素は、その企業が実行できるビジネスプロセス上の役割を示します。役割とは例えば発注者・受注者などです。外部のビジネスプロセス定義文書と、その中で定義される役割の種類とを参照することで指定します。また、メッセージ交換の際にどのチャネルを使うかということも併せて指定します。この要素は以下の子要素をもちます。

＊ビジネスプロセス定義と役割の指定—ProcessSpecification、Role 要素

ProcessSpecification 要素でビジネスプロセス定義を指定します。URI によるリンクと、ビジネスプロセス定義内で指定されている名前、バージョン、uuid (URI 形式)を用いて指定します。ビジネスプロセス定義の中で自社が実行する役割を、Role 要素で指定します。以下に例を示します。

```
<tp:ProcessSpecification tp:version="2.0" tp:name="PurchaseOrder"
  xlink:type="simple"
  xlink:href="http://some-standard.org/order.xml"
  tp:uuid="urn:somestandard:bpid:order$2.0"/>
```

```
<tp:Role tp:name="Buyer"
xlink:type="simple"
xlink:href="http://some-standard.org/order.xml#Buyer"/>
```

＊送受信に使うチャネルの指定―ServiceBinding 要素

自社の担当する役割が決まると、送受信できるメッセージの種類も定まります。そこで、実行可能なメッセージ交換のそれぞれについて、どの配送チャネルを使うかを ServiceBinding 要素で指定します。配送チャネルについては 4.1.3 節を参照してください。

配送チャネルの指定に関して、Service と Action という二つの概念が使われます。これらは MS のメッセージヘッダに現れる同名の要素に対応するものです。Action は、メッセージ一つの送信または受信の種類ごとに名前を付けたものです。例えば、「見積り依頼の送信」というのが一つの Action になります。一方、Service はビジネスプロセス定義の中で実行可能な Action を束ねたものです。BPSS を使用する場合は ProcessSpecification 要素の uuid 属性の値を用いることが規定されています。Action は Service の中で一意であるように命名されます。Service と Action の組み合わせによって、あるメッセージ交換が何をするものなのかを特定できます。

ServiceBinding 要素では、まず Service 要素で Service を指定し、次に CanSend 要素と CanReceive 要素とによって、送信可能および受信可能な Action のそれぞれを列挙し、各 Action に対応する配送チャネルを指定します。

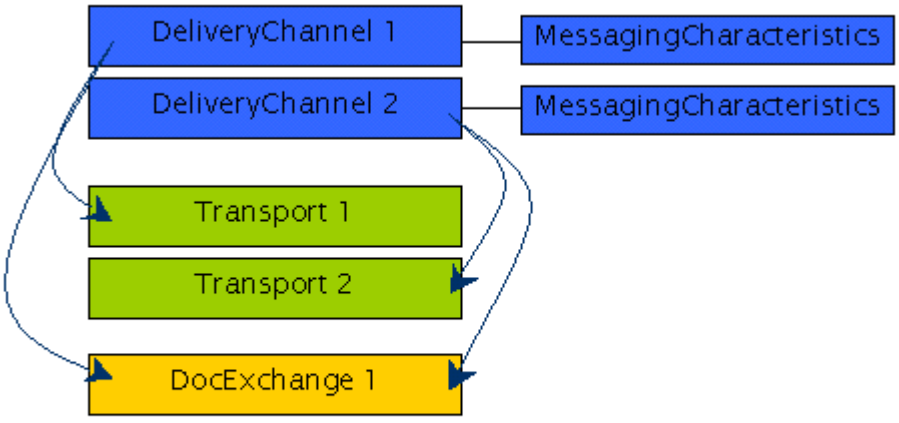
次の例では、「Purchase Order Request Action」という Action に対して「ChannelA1」という ID の配送チャネルを割り当てています。メッセージのパッケージング(4.4 節参照)として ID「Package_A」で示す定義を用いることも同時に指定しています。この Action がビジネスプロセス定義の中のどこにあたるものなのかは、ActionContext 要素で指定しています。また、BusinessTransactionCharacteristics 要素によって、ビジネスプロセス定義で指定された timeToPerform 属性を上書きしています。

```
<tp:ServiceBinding>
    <tp:Service>bpid:somestandard:order$2.0</tp:Service>
    <tp:CanSend>
      <tp:ThisPartyActionBinding
        tp:id="companyA_ABID1"
        tp:action="Purchase Order Request Action"
        tp:packageId="Package_A">
        <tp:BusinessTransactionCharacteristics tp:timeToPerform="P1D"/>
        <tp:ActionContext
```

```
            tp:binaryCollaboration="Request Purchase Order"
            tp:businessTransactionActivity="Request Purchase Order"
            tp:requestOrResponseAction="Purchase Order Request Action"/>
          <tp:ChannelId>ChannelA1</tp:ChannelId>
        </tp:ThisPartyActionBinding>
      </tp:CanSend>
      <!-- 以下同様に、送信可能な Action を CanSend で、受信可能な Action を CanReceive
で一つずつ指定。--> </tp:ServiceBinding>
```

＊配送チャネルの指定―DeliveryChannel 要素

配送チャネルとは、メッセージ交換に用いるプロトコルや URI、パラメタなどを集めて名前を付けたものです。Transport 要素と DocExchange 要素の組み合わせによって定義します。前者は転送プロトコル(HTTP 等)に関する特性、後者はより上位のメッセージサービスで指定する内容を記述します。用いる Transport、DocExchange は ID で指定します。この様子を下図に示します。また、子要素の MessagingCharacteristics 要素によって、同期応答の使用などの指定ができます。配送チャネルは複数定義でき、上述の ServiceBinding 要素の中で Action の種類に応じて使い分けることができます。



TransportとDocExchangeの組み合わせで
DeliveryChannelを定義する

下の例では、ID「transportA2」で示される Transport 要素と、ID「docExchangeA1」の DocExchange 要素とを組み合わせて、「ChannelA1」という ID の配送チャネルを定義しています。また、MessagingCharacteristics 要素によって、このチャネルでは非同期な通信を用いることと、毎回必ず受領通知を用いることを示しています。

```
<tp:DeliveryChannel
  tp:channelId="ChannelA1"
  tp:transportId="transportA2"
  tp:docExchangeId="docExchangeA1">
  <tp:MessagingCharacteristics
    tp:syncReplyMode="none"
    tp:ackRequested="always"/>
</tp:DeliveryChannel>
```

＊データ転送についての指定―Transport 要素

Transport 要素はデータ転送に用いるプロトコル(HTTP 等)や、通信層のセキュリティ機構(SSL 等)を指定します。子要素の TransportSender と TransportReceiver とで、それぞれ送信側と受信側の設定を記述します。送信側も受信側も設定できる内容はほぼ同じです。

TransportSender は以下の内容を持ちます。

□転送プロトコル(HTTP 等)
□認証方式(HTTP の Basic 認証等)
□セキュリティ機構(SSL 等)

TransportReceiver は上に加えて、データ受信のための URI を指定する Endpoint 要素を持ちます。TransportReceiver 要素の例を以下に示します。

```
<tp:TransportReceiver>
  <tp:TransportProtocol tp:version="1.1">HTTP</tp:TransportProtocol>
  <tp:AccessAuthentication>basic</tp:AccessAuthentication>
  <tp:AccessAuthentication>digest</tp:AccessAuthentication>
  <tp:Endpoint
    tp:uri="https://www.CompanyA.com/ebxmlhandler"
    tp:type="allPurpose"/>
  <tp:TransportServerSecurity>
    <tp:TransportSecurityProtocol
tp:version="3.0">SSL</tp:TransportSecurityProtocol>
    <tp:ServerCertificateRef tp:certId="CompanyA_ServerCert"/>
    <tp:ClientSecurityDetailsRef
tp:securityId="CompanyA_TransportSecurity"/>
  </tp:TransportServerSecurity>
</tp:TransportReceiver>
```

＊伝票交換の特性の指定―DocExchange 要素

DocExchange 要素はメッセージサービスに応じた特性の指定を行います。今のところ、ebXML の MS に対応した ebXMLSenderBinding ならびに ebXMLReceiverBinding 要素が子要素として用意されています。将来的には異なるメッセージサービスのための指定方法が用意される可能性があります。

ebXML{Sender|Receiver}Binding 要素では、以下の内容が指定できます。

□信頼性通信（Reliable Messaging)―再送回数、再送間隔、順序保証の有無
□メッセージ保存期間
□否認拒否―XML Signature の使用、用いるハッシュ関数等
□デジタルエンベロープ―S/MIME 等
□使用する XML 名前空間

＊OverrideMshActionBinding 要素

MSH レベルの Action (受領通知、エラー通知等)に使うチャネルは PartyInfo 要素の属性で設定しますが、このデフォルト値を OverrideMshActionBinding 要素によって上書きすることができます。action 属性で Action の種類を指定し、channelId 属性でその Action に用いるチャネルを ID 参照します。なお、MSH の Action の値は MS の仕様で定められています。

□証明書―Certificate 要素
CPP で用いる証明書の情報を Certificate 要素で表します。この要素の内容は XML Signature の ds:KeyInfo 要素です。Certificate 要素は必要な数だけ記述できます。各々に ID 型の certId 属性を設定し、他の要素から参照します。

□セキュリティ詳細―SecurityDetails 要素
SecurityDetails 要素には TrustAnchors 要素と SecurityPolicy 要素が入ります。

TrustAnchors には、その企業が信頼する証明書(Certificate 要素)への参照が複数入ります。これは証明書の連鎖を検証する際に用い、証明書が TrustAnchors のいずれかへ至らなければ検証が失敗したことになります。

SecurityPolicy はセキュリティポリシーを指定するための要素ですが、将来のための予約として用意されているもので、まだ使い方は決まっていません。

(4-2) パッケージングの情報―SimplePart、Packaging 要素

メッセージを送る際は通常、ebXML メッセージヘッダと本文(伝票)、もし必要なら添付ファイルが付くという構成になります。このような、メッセージのパッケージングを定義するのが SimplePart と Packaging 要素です。SimplePart 要素は MIME における個々のパートに相当し、各パートをどのように組み合わせるかを Packaging 要素で指定します。

定義した Packaging 要素は ID で他の要素から参照します。具体的には、ThisPartyActionBinding 要素で各 Action ごとに対応するパッケージを指定します。

(4-3) CPP の署名―Signature 要素

この CPP のデジタル署名です。Signature 要素の中に、XML Signature の ds:Signature 要素が入ります。

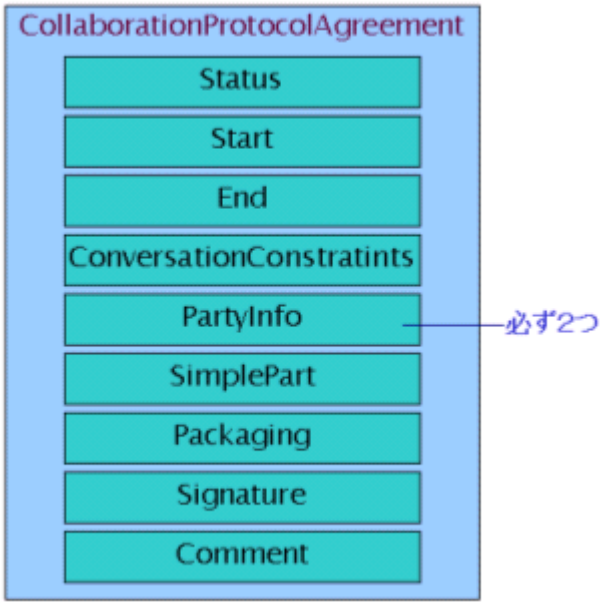
(4-4) コメント―Comment 要素

この CPP についてのコメントを、人間が読むテキストとして入れることができます。xml:lang 属性で言語の指定(日本語、英語など)ができます。

(5) CPA の構成

CPA は CPP を元に作成するので、構成要素は CPP とほぼ同じです。ただし、2 社分の PartyInfo が入ることと、CPA 特有の情報がいくつか入る点が異なります。

CPA の最上位要素は CollaborationProtocolAgreement 要素です。その中に以下の要素が入ります。



(5-1) 合意の状況―Status 要素

この CPA の現在の合意の状況を示します。“proposed”(交渉中)、“agreed”(合意に達した)、“signed”(署名済み)のいずれかの値をとります。

(5-2) 有効期間―Start、End 要素

CPA が効力をもつ期間を、Start 要素と End 要素のそれぞれに開始・終了の日時を設定することで表します。日時は XML スキーマの dateTime 型で表します。

(5-3) 会話の実行の制約―ConversationConstraints 要素

この CPA のもとで行う会話の最大数や、並行して行える会話の最大数を制限することができます。

(5-4) 2 社それぞれの企業情報―PartyInfo 要素

CPP に出てきた PartyInfo 要素を、取引を行う企業それぞれについて記述します。

CPA の場合、相手側 PartyInfo の中を指す ID 参照もあります。したがって、相手の定義内容から対応する ID 値を取得してきて自社の PartyInfo に入れる必要があります。このような要素としては、例えば CanSend 要素の中の OtherPartyActionBinding があります。

CPA においては、自社の送信と相手の受信、自社の受信と相手の送信の設定について、整合性がとれていなければなりません。

(5-5) パッケージングの情報―SimplePart、Packaging 要素

SimplePart 要素と Packaging 要素でメッセージのパッケージングを定義します。これは CPP と同様です。

(5-6) CPA の署名―Signature 要素

この CPA のデジタル署名を付けることができます。

(5-7) コメント―Comment 要素

CPP と同様、CPA のコメントを記述することができます。

2. 長期署名について

甲および乙は、電子署名が施された取引関係情報を長期保存する場合、その取引関係情報に付いている電子署名が正しいものかを検証する時刻について、「時刻」そのものの誤差を生じたり、甲乙互いのシステムの時刻の誤差が、業務的に双方に支障を来たさないよう、定期的に確認するなどの運用管理を行う。

【留意点】
なおここで使用している言葉について以下で説明する。

（a）電子署名とは、公開鍵暗号方式を利用することで、文書の作成者を証明し、かつその文書が改竄されていないことを保証する署名方式を指し、これにより作成された文書を電子署名文書という。

（b）電子署名文書の長期保存の対象期間について、商取引に関連する法規（民法、商法、法人税法等）では各書類、文書に対し、5～10 年程度の保存が義務付けられており、CI-NET においても電子署名文書をこれらの期間保存することを想定する。

（c）ここで触れている「時刻」とは、取引関係情報の作成時だけでなく電子署名文書を保存する際の署名検証時刻としても利用するため、より正確な時刻の運用が求められる。

「時刻」を確認するための時刻源としては、情報通信研究機構（JJY・NICT）の標準電波、日本電信電話（NTT）の 117 時報サービスあるいは日本放送協会（NHK）の時報等を利用する方法が考えられる。

取引関係情報の保存に際し、時刻に関わる処理についてより精度の高い厳密な運用を可能とするため、以下のような規定をデータ交換協定書に盛り込むことも可能である。

－CI-NET において送受信する情報には、契約時に相互に受け渡し保管される注文情報及び注文請情報といった取引業務の情報（メッセージ）以外に、システム運用上の「受信確認情報」がある。また契約前の見積情報や契約後の出来高・請求情報等や取引情報の送受信時の処理（通信、暗号化・復号、署名検証等）、電磁的記録等の保存の処理等に関する一部あるいは全てのログを保存し、内容や時刻を検証できる管理を行うこととする。

またこれらの情報の取得や保存については、これらの処理が容易にできるようシステム的に対応を組み込んでおくとともに、ユーザは必要なときにそれらを参照できるようにしておくこととする。

第四編.　　法的枠組

9.　国内関連法規

9.1.　電子帳簿保存法

「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律」

(電子取引の取引情報に係る電磁的記録の保存)

第十条所得税(源泉徴収に係る所得税を除く。)及び法人税に係る保存義務者は、電子取引を行った場合には、財務省令で定めるところにより、当該電子取引の取引情報に係る電磁的記録 を保存しなければならない。ただし、財務省令で定めるところにより、当該電磁的記録を出力することにより作成した書面文は電子計算機出力マイクロフィルムを保存する場合は、この限りでない。

＊電子取引取引情報(取引に関して受領し、又は交付する注文書、契約書、送り状、領収書、見積書その他これらに準ずる書類に通常記載される事項をいう。以下同じ。)の授受を電磁的方式により行う取引をいう。

9.2.　下請取引ガイドライン

「下請取引における電磁的記録の提供に関する留意事項」

例えば，親事業者が下請事業者に一方的に電子受発注を押し付けたり，親事業者から下請事業者に不当な費用負担を押し付けられるのではないかとの懸念がある。このため，電子受発注に伴って，下請事業者の利益を害するような行為その他下請法の趣旨に反する行為が行われることのないよう，下請法及び独占禁止法上の留意事項を取りまとめた。

(1) 書面の交付に代えて電子メールにより電磁的記録の提供を行う場合は，下請事業者の使用に係るメールボックスに送信しただけでは提供したとはいえず，下請事業者がメールを自己の使用に係る電子計算機に記録しなければ提供したことにはならない。例えば，通常の電子メールであれば，少なくとも，下請事業者が当該メールを受信していることが必要となる。また，携帯電話に電子メールを送信する方法は，電磁的記録が下請事業者のファイルに記録されないので，下請法で認められる電磁的記録の提供に該当しない。

(2) 書面の交付に代えてウェッブのホームページを閲覧させる場合は，下請事業者がブラウザ等で閲覧しただけでは，下請事業者のファイルに記録したことにはならず，下請事業者が閲覧した事項について，別途，電子メールで送信するか，ホームページにダウンロード機能を持たせるなどして下請事業者のファイルに記録できるような方策等の対応が必要となる。

9. 3.　e 文書法

「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（e 文書法）

第三条　民間事業者等は、保存のうち当該保存に関する他の法令の規定により書面により行わなければならないとされているもの（主務省令で定めるものに限る。）については、当該法令の規定にかかわらず、主務省令で定めるところにより、書面の保存に代えて当該書面に係る電磁的記録の保存を行うことができる。

２　前項の規定により行われた保存については、当該保存を書面により行わなければならないとした保存に関する法令の規定に規定する書面により行われたものとみなして、当該保存に関する法令の規定を適用する。

「書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律案（仮称）骨子（案）」（電子書面一括法）

(1) 総点検に対する各省庁からの回答を踏まえ、書面の交付あるいは書面による手続を義務付けている法律を改正。
(2) 法律改正のポイント
書面の交付あるいは書面による手続を義務付けている法律について、送付される側の承諾等を条件に、情報通信の技術を利用する方法による送付も認められるようにする。

9. 4.　電子署名法

1. 電磁的記録の真正な成立の推定

「本人による一定の条件を満たす電子署名」がなされた文書は、本人の手書署名・押印がある文書と同様、真正に成立したものと推定されることが定められています。

2. 特定認証業務に関する認定の制度

特定認証業務の認定を受けるためには、どのような技術・設備水準が必要なのかを示しています。具体的には、電子署名の方式や業務の用に供する設備、利用者の真偽確認の方法等が定められており、こうした認定を受けた認証局が発行する電子証明書は、一定レベルの信頼性を保ったものだと判断されます。

第 2 条　この法律において「電子署名」とは、電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

１. 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

２．当該情報について改変がいないかどうかを確認することができるものであること。

この法律において「認証業務」とは、自らが行う電子署名についてその業務を利用する者その他の者の求めに応じ、該当利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。

10.　国際関連ガイド

10.1.　国連国際商取引法委員会

UNCITRAL Model Law on Electronic Signatures (2002)

UN Convention on the Use of Electronic Communications in International Contract (2007)

10.2.　国連 CEFACT の活動

Recommendation N°. 14 - Authentication of Trade Documents by Means Other than Signature

Recommendation N°. 26 - The Commercial Use of Interchange Agreements for Electronic Data Interchange

Recommendation N°. 31 - Electronic Commerce Agreement

10.3.　国連 ESCAP の取組み

電子化された貿易のための地域協定

2012 年 6 月の国連 ESCAP コミッション会議にて採択された決議 68/3（アジア太平洋域内の持続可能な貿易手続簡易化のための、電子取引と国境を越えた電子データ／電子文書の認証の実現）に関わる地域協定（Regional Arrangement）の準備が進んでいる。

Draft Text of Arrangement/Agreement　On Facilitation of Cross-border Paperless Trade for the Asia – Pacific Region

一般原則

技術中立性、電子化による（紙との）機能同等、電子化による（紙との）差別排除、相互運用性を原則とする。

地域協定ドラフト骨子

協定調印国はシングルウィンドウ・システムを導入すべきである。
協定調印国は電子取引推進委員会を設置する。
協定調印国は電子取引の国家政策フレームワークを確立する。
協定調印国は電子取引のための有効な法規制を整備する。
国際電子貿易文書を法的に承認する。
貿易データ／文書交換における国際電子取引標準の採用。
国際的に識別可能な貨物識別子のための標準を採用。
国際標準の開発と導入。
国際契約における電子通信の使用についての国連協定に調印する。
国際間にわたるプライバシー、データ保護、知的所有権の地域および国際規約への調印を進める。

法的義務のフレームワーク整備。

ADR（Alternative Dispute Resolution）制度の整備。

11.　国別の考慮点

11.1.　中国で暗号利用は要申請！！

中国では、商用暗号管理条例によって、暗号システムの開発から製造、販売、使用、廃棄に至るまで、細かに規定され制限されています。中国以外の資本の入った法人または中国国籍を持っていない外国人が利用する場合には、暗号管理局に利用する製品と利用場所などを申請し、許可を得る必要があります。無許可で利用した場合には、機器没収などの罰則規定が、盛り込まれており企業活動においては無視できない法律です。

<該当する項目が、一つでもあれば申請対象です >

□社内スタッフの中国出張が多く、出張中にも社内機密情報を安全に扱いたい。

□日本国内で導入済みの暗号化製品を中国拠点にも導入し、同等のセキュリティ環境を構築したい。

□行政警告、改善命令を受けた場合は、不正記録に残され、今後、新しい法律及び条令が実施される都度、真っ先に監査の対象となるのを防ぎたい。

□政情が不安定なタイミングで、社員がうっかり暗号化製品を中国に持込み、中国で長期身柄拘束されるような事態を避けたい。

□日本国内のシステムを利用するために VPN 通信機能をノート PC または iPad などタブレットに導入し、中国出張者または、現地スタッフが、利用している。（すでに、要申請状態です。）

□現在、会社では、中国出張時の PC 携帯禁止措置を実施している。その為、スタッフの現地での通信手段が限られ、仕事の効率がかなり低下しているので、一刻も早く現状を改善したい。

第五編.　　アジアのプロバイダ

12.　東アジア各国の PAA プロバイダ

12.1.　東アジア各国の PAA プロバイダ

CIECC（中国）

Dagang Net（マレーシア）

Trade-Van（台湾）

CrimsonLogic（シンガポール）

TradeLink（香港）

CAT Telecom（タイ）

輸出入・港湾関連情報処理センター株式会社（日本）

Tradegate（ オーストラリア）

KTNET（韓国）

12.2.　ASW 参加プロバイダ

シンガポール ”Trade Net”（CrimsonLogic）

Malaysia “MyTRADeLINK”（Dagang Net）

タイ “Thai NSW”（タイ税関）

インドネシア “INSW”（EDI Indonesia）

フィリピン “PNSW”（フィリピン税関）

ベトナム “VNACCS”（ベトナム税関）

ラオス（構築中...）

カンボジア（構築中...）

NSW は一カ国に一つしか登録できない。インドネシアは AS2 を持っていると明記。

第六編.　　理想とするメッセージング基盤

13.　理想とするメッセージング基盤とは

１つの ESP に接続すると、ESP 間は相互接続され、海外と接続可能な ESP 経由で世界中の取引先との EDI が実現可能となる。

13.1.　現状

問題点

□Internet や電話は ISP や電話会社に依存せずどこへでも接続できるが、ESP は伝達可能な相手が限定される。

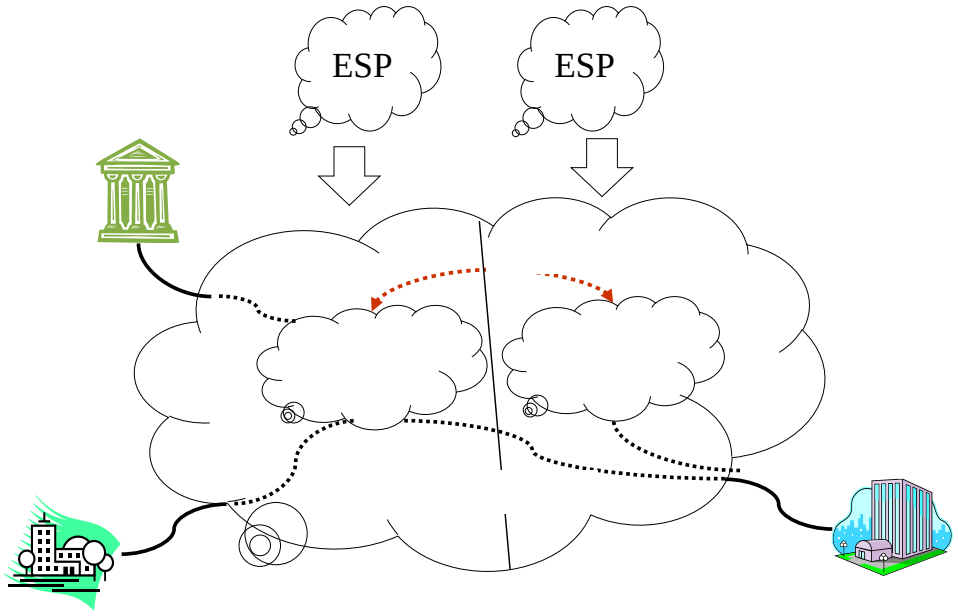
□ESP は伝達可能な企業が限定されるため、複数の ESP と繋がないといけない。

□ESP 毎にサービスレベルに違いがあると ESP 間接続が出来ない。

対策

□InterESP サービス

複数の ESP を相互接続し、あたかも一つの ESP のように見えるサービス



13.2.　実現のための課題

ネットワークサービスのサービスレベルが異なると相互接続できない。

ネットワークサービスを IP ベースにし、IP ネットワーク統合可能とする。

付加サービスのサービスレベルが異なるとサービスが統合できない。

付加サービスのサービスレベルを標準化し、標準的な付加サービスは容易に統合可能とする。

コスト負担が公正でなければならない。

コスト負担方針を明確にし、利用料体系可能とする。

＝　従量負担か定額負担か

＝　何が共通コストか個別コストか

第七編.　　パブリッククラウドの相互運用調査

14.　目的

本編は、企業が各々異なる ESP やクラウドと契約しているとき、企業と企業が EDI を行うには複数の ESP やクラウドを経由することとなる。その折、企業間ではその送達確認ができない。

ここでは、ESP やクラウド間でどのような準備をすれば、企業がエンド to エンドで最終的な必要情報を共有できるかを調査検討する。

本年度は、まず現在提供されているサービスについて調査をしてみた。

15.　成果

15.1.　調査の目的

メッセージング基盤実現要件の観点から、パブリッククラウドの相互運用性調査を行う。

□調査対象は、国内で利用可能なクラウド
□プライベート空間での利用を前提とした利用可否の調査
□オープンなクラウドでの n 対 n 接続での利用可否の調査

15.2.　調査について

調査内容：

パブリッククラウド基盤サービスについて、プライベート／オープンな接続方式に対する接続基盤有無を調査。

□プライベートな接続＝閉域網による接続＝LAN、専用線、IP-VPN 接続
□オープンな接続＝公開網による接続＝インターネット接続

調査対象・方法：

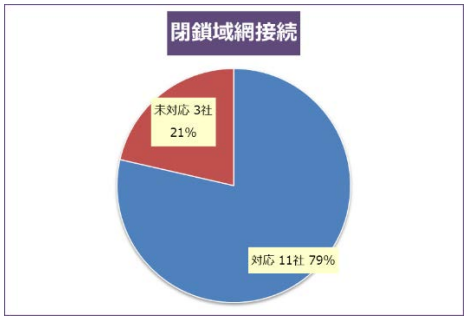
国内大手ベンダー提供サービスを中心に、14 社のサービスについて事業者に対するアンケートの形で調査実施。

調査期間：

2013/3～5

15. 3.　調査結果（プライベート空間利用の可否）

各クラウド基盤での LAN 接続、専用線、IP-VPN、いずれかの接続可能の比率を下図に示す。

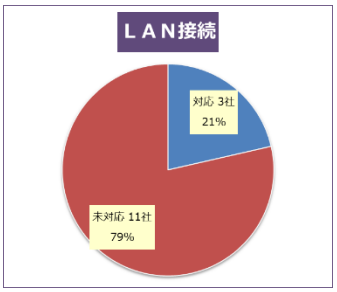


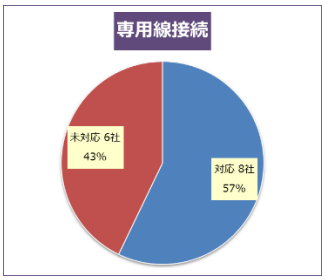
８割程度のクラウド基盤で、接続可能。

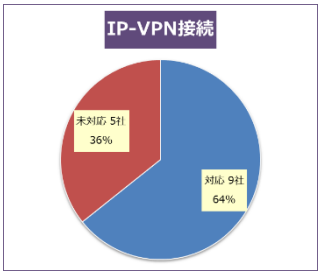
現状でプライベート空間利用を前提としたクラウドサービスを構築することは可能と思われる。

＊接続方式ごとの利用可否（閉域網接続）

LAN 接続、専用線、IP-VPN、それぞれの接続可否比率は下記の通り。



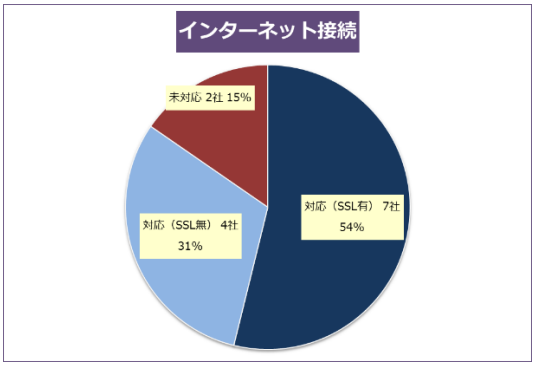




	ＬＡＮ接続	専用線等	IP-VPN 接続
対応	3 社 21 %	8 社 57 %	9 社 64 %
未対応	11 社 79 %	6 社 43 %	5 社 36 %

15.4.　調査結果（オープン空間利用の可否）

各クラウド基盤でのインターネット接続の可否と、SSL 対応可否の比率を下図に示す。

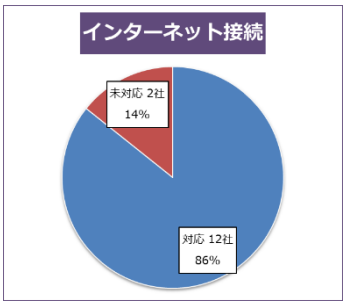


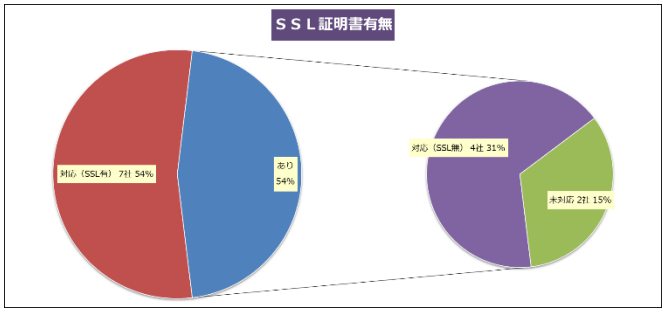
８割以上のクラウド基盤で、インターネット接続可能。

オープン利用を前提としたクラウドサービス構築は可能と思われる。ただし、ＳＳＬによるセキュアな通信可能な基盤は約 5 割程度。

＊インターネット接続可否詳細

インターネット接続可否、SSL 証明書接続可否それぞれの割合は下記の通り。





	インターネット接続
対応	12 社 86 %
未対応	2 社 14 %

	証明書対応状況
証明書なし	6 社 46 %
証明書あり （単体証明書）	7 社 54 %

15.5.　今後の検討課題

具体的な通信パラメーター、設定については、パラメータ検討チームでの検討結果を受けて検討が必要。

平成 28 年 3 月　発行

発行元　一般社団法人サプライチェーン情報基盤研究会