第　Ⅴ　編

実　装　編

※ 前バージョンに対して追加・変更された箇所を下線で示しています。

Ⅴ 実 装 編

１．実装編の読み方

１．１ 「物流ＸＭＬ／ＥＤＩ標準」の導入方法

物流XML／ＥＤＩシステムの基本構成を図表５－１に示します。

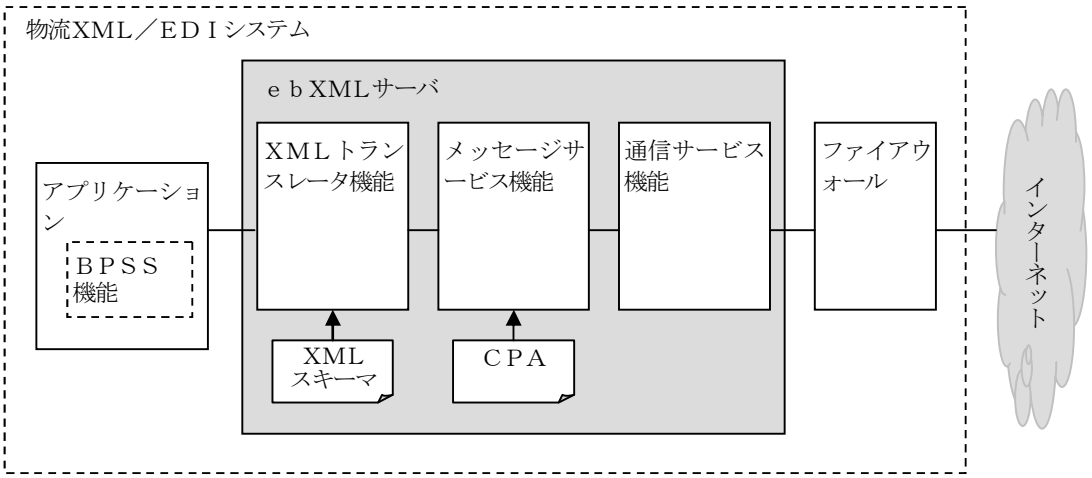
①ビジネスプロセス定義書に基づく企業間ビジネスプロセスの手順などは、アプリケーションで実現します。企業間ビジネスプロセス手順のコントロールをＢＰＳＳ[1]機能に委ねることもできます。

②ビジネスドキュメント定義書に基づいて作成されたXMLスキーマをXMLトランスレータ機能に入力し、事前にアプリケーションのデータと対応付け（マッピング作業）をしておきます。

③メッセージサービス機能は、通信サービス機能を通じて取引相手と安全確実にビジネスドキュメントを送受する機能です。ＣＰＡテンプレートを基にして作成したXML形式のＣＰＡ情報をｅｂXMLメッセージサービス（ｅｂMS）機能に入力し、ビジネスドキュメントを送受信するために必要な通信条件などを設定します。ここにはセキュリティ条件の設定なども含まれます。

④セキュリティ対策のために、暗号化キーの生成、デジタル証明書の取得と設定、ファイアウォールの設定などを行います。

図表５－１　物流ＸＭＬ／ＥＤＩシステムの基本構成



１．２ 実装編の記載内容

物流XML／ＥＤＩシステムの基本構成は図表５－１に示すとおりですが、実際の導入に当たっては、様々なバリエーションがあります。

この実装編では、物流XML／ＥＤＩシステム構成のバリエーションと導入に必要な技術、実装方法などを示します。

実装編の主な記載内容は、以下のとおりです。

①ネットワークの構成

・XML／ＥＤＩシステムの導入形態、XML／ＥＤＩシステムのネットワーク構成

②データ交換の方法

・通信プロトコル、シンタックスルール、受信確認の方法、ＣＰＡテンプレート

③ビジネスドキュメントの作成

・ビジネスドキュメントの構造、文字コード、XMLスキーマの作成方法

④セキュリティ対策

・セキュリティ対策の種類、セキュリティ対策の内容

[1] BPSS: Business Process Specification Schema

２　ネットワークの構成

２．１　ＸＭＬ／ＥＤＩシステムの導入形態

ＸＭＬ／ＥＤＩシステムを導入する形態として、図表５－２に示す４つの方式が考えられます。

図表５－２　ＸＭＬ／ＥＤＩシステムの導入形態

	サーバ方式	ｅＨｕｂ経由方式	クライアント方式	ＡＳＰ利用方式
特徴	①自社内にｅｂＸＭＬサーバ[2]を導入する方式。 ②自社の業務プロセスに合った柔軟なシステムが構築できます。 ③導入するための時間とコストがかかります。 ④サーバの運用体制の確立が必要です。	①取引先が従来型ＥＤＩ手順である場合に採用する方式で、ｅＨｕｂサーバ[3]でプロトコル変換を行います。 ②その他はサーバ方式に同じです。	①自社内にｅｂＸＭＬクライアント[4]を導入する方式。 ②比較的低コストで導入できます。 ③クライアントの運用に手間がかかりません。	①ＡＳＰサービスを利用して簡易な手順で接続する方式。 ②ブラウザ程度のソフトで利用できます。 ③業務システムとの連携が取りにくい。 ④利用者・ＡＳＰ間は独自手順です。[5]
留意点	①セキュリティを考慮したｅｂＸＭＬサーバの設置方法 ②ｅｂＸＭＬサーバと業務システムとの連携方法		①ｅｂＸＭＬクライアントの自社内ＬＡＮへの接続方法	①ＡＳＰクライアントの自社内ＬＡＮへの接続方法
設備	・インターネット接続[6] ・サーバのセキュリティ環境構築[7] ・ｅｂＸＭＬサーバ		・インターネット接続 ・ｅｂＸＭＬクライアント	・インターネット接続 ・ＡＳＰクライアント
要点	①取引量が比較的多い場合 ②リアルタイム応答処理が必要な場合		①取引量が比較的少ない場合 ②低コストで導入したい場合	

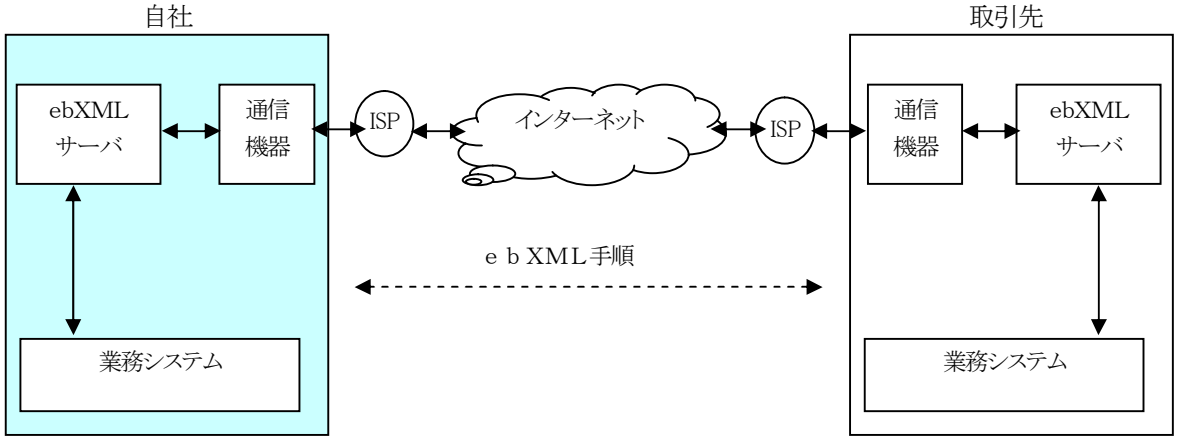
２．２　ＸＭＬ／ＥＤＩシステムのネットワークの構成

ＸＭＬ／ＥＤＩシステムの導入形態ごとの代表的なネットワーク構成を以下に示します。

（1）サーバ方式

最も基本的な方式です。

図表５－３　サーバ方式の代表的ネットワーク構成



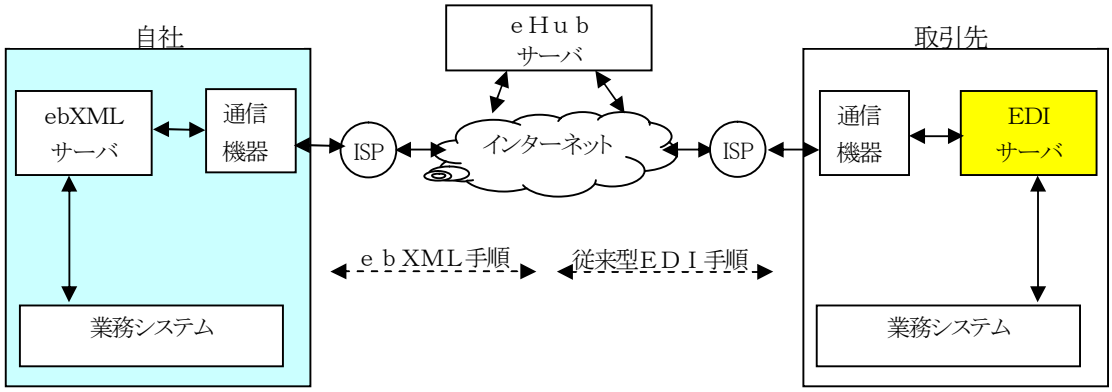
（注１）通信機器；ファイアウォール、ルータ等のこと。
（注２）ISP･･･Internet Service Provider（インターネットへの接続代行業者）

[2] ｅｂＸＭＬ通信機能を持っているサーバ
[3] インターネット上でプロトコル変換機能を有するサーバ
[4] ｅｂＸＭＬ通信機能を持っているクライアント
[5] ｅｂＭＳクライアント方式の標準仕様を採用することにより標準的な手順にできます。
[6] ファイアウォール、ルータ、インターネット接続プロバイダ契約など
[7] DMZ (DeMilitarized Zone, 非武装地帯)の構築など

（2） ｅＨｕｂ経由方式

取引相手が従来型ＥＤＩ手順などの場合にｅＨｕｂでプロトコル変換を行います。

図表５－４　ｅＨｕｂ方式の代表的ネットワーク構成

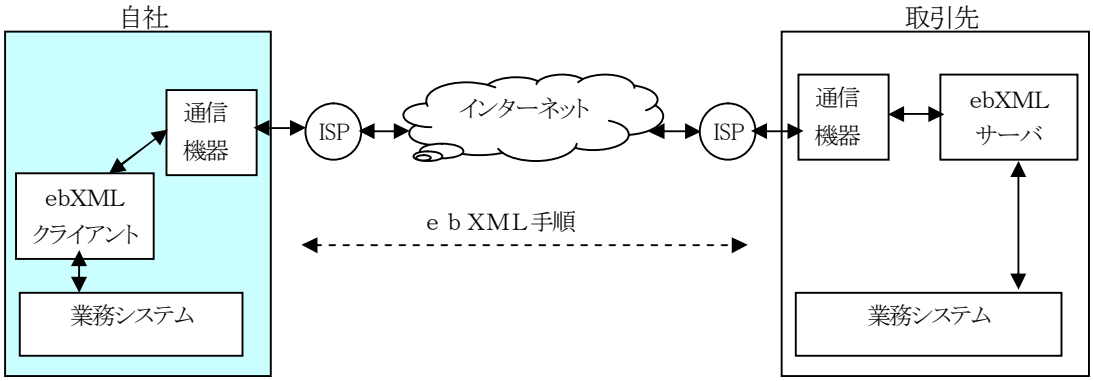


※ｅＨｕｂサーバは、プロトコル変換機能を持ちます。

（3）クライアント方式

サーバより簡易なｅｂXMLクライアントを導入する方式です。

図表５－５　クライアント方式の代表的ネットワーク構成

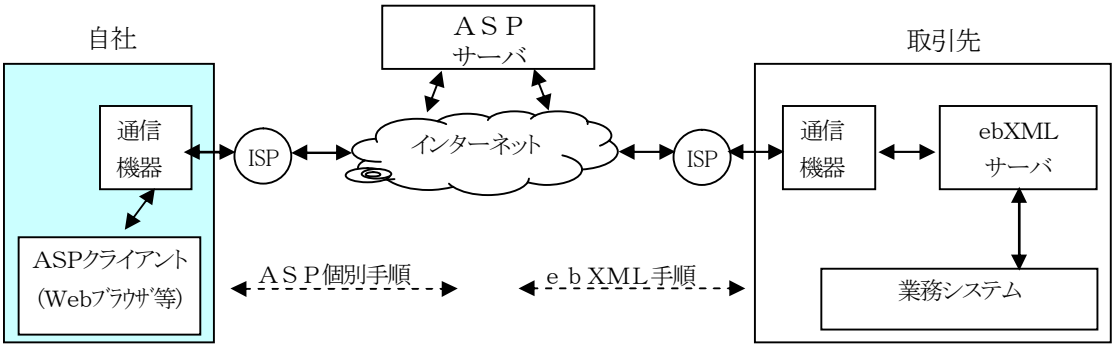


（4）ＡＳＰ方式

ＡＳＰサービスを利用して簡易な手順で接続する方式です。ＡＳＰクライアント相互間の通信も可能です。

ＯＡＳＩＳで検討されているｅｂMSクライアント方式の標準仕様を採用することにより、ＡＳＰ個別手順を標準手順にできます。

図表５－６　ＡＳＰ方式の代表的ネットワーク構成



※ＡＳＰサーバは、ｅｂXML通信機能および業務システム機能を持ちます。

３　データ交換の方法

３．１　通信プロトコル

ＥＤＩの通信制御方式は、下記の通信プロトコルを推奨します。

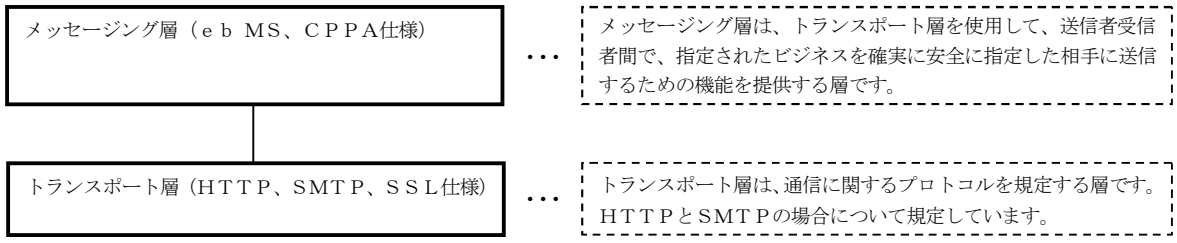
図表５－７　推奨する通信プロトコル

ベーシックＥＤＩ	コラボレイティブＥＤＩ
・ｅｂＭＳ手順 ・拡張Ｚ手順 ・その他のＴＣＰ／ＩＰ手順	・ｅｂＭＳ手順

（１）ｅｂＭＳ手順

ｅｂＭＳ（ｅｂＸＭＬメッセージサービス）手順とは、ｅｂＸＭＬメッセージサービス仕様に準拠した通信手順のことをいいます。

図表５－８　ｅｂＭＳ手順の構造



ｅｂＭＳ手順は、Ｗｅｂサービスの国際規格であるＳＯＡＰ規格をベースに、通信プロトコル、セキュリティ機能（認証、否認防止、暗号化）、および信頼性通信仕様などの機能を強化した規格です。

ｅｂＭＳ手順は多くの機能を有しており、取引当事者間でこれら機能を取捨選択したうえで使用する必要があります。取引当事者間でｅｂＭＳ手順の機能を選択し技術的な合意をとるための規格として、ｅｂＸＭＬ ＣＰＰ／ＣＰＡ仕様があります。

（２）拡張Ｚ手順

拡張Ｚ手順とは、（財）日本情報処理開発協会 産業情報化推進センター（JIPDEC/CII）[8]が、全銀協標準通信プロトコルＴＣＰ／ＩＰ手順（全銀ＴＣＰ／ＩＰ手順）をベースに制定した実装標準です。

拡張Ｚ手順による通信制御電文、ファイル制御電文、データ電文の運用ルールについて、取引当事者間で合意のうえで実装することとします。

（３）その他のＴＣＰ／ＩＰ手順

その他のＴＣＰ／ＩＰ手順とは、取引当事者間で合意した上記以外のＴＣＰ／ＩＰベースの通信プロトコルのことをいいます。

具体的な通信手順、運用ルールなどについて、取引当事者間で明確にしたうえで実装することとします。

３．２　シンタックスルール

（１）ビジネスドキュメントのシンタックスルール

ＸＭＬスキーマで指定するＸＭＬ形式のドキュメントとします。

ビジネスドキュメントのシンタックスルールは、以下のものに従います。

「ＸＭＬ １．０」（Ｗ３Ｃ勧告）

http://www.w3.org/TR/REC-xml/

ＸＭＬスキーマは、以下のＷ３Ｃ勧告に従う。

「ＸＭＬスキーマ パート０ 入門」(http://www.w3.org/TR/xmlschema-0/)

「ＸＭＬスキーマ パート１ 構造」(http://www.w3.org/TR/xmlschema-1/)

「ＸＭＬスキーマ パート２ データ型」(http://www.w3.org/TR/xmlschema-2/)

（２）ｅｂＸＭＬメッセージのシンタックスルール

ｅｂＸＭＬメッセージのシンタックスルール（構文規則）は、ｅｂＸＭＬメッセージサービスに基づくエンベロープに従います。

[8] 現在は、(一財)日本情報経済社会推進協会 電子利活用推進部(JIPDEC/DUPC)

３．３　受信確認の方法

（1）ｅｂＭＳ手順の場合

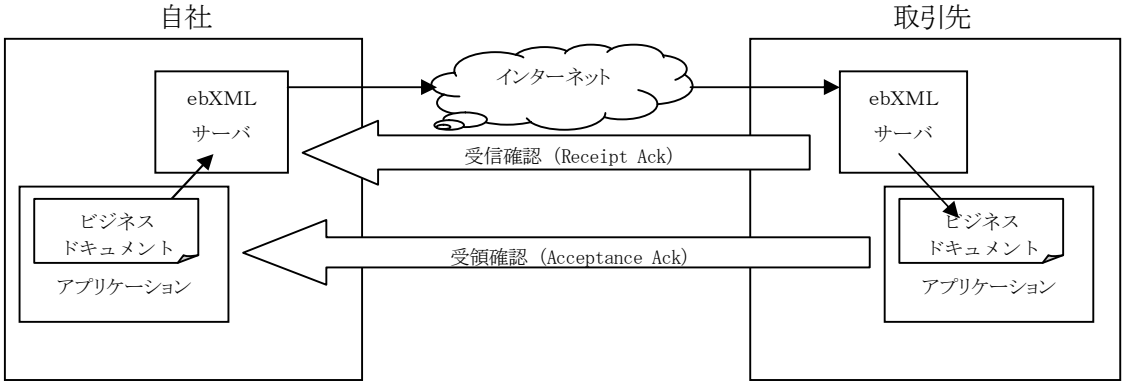
以下のビジネスシグナルの返送により、受信の確認を行います。

①取引相手のｅｂＸＭＬサーバがビジネスドキュメントを正常に受信したときに、ビジネスシグナル「受信確認（Receipt Acknowledgement)」を返送します。

②アプリケーションがビジネスドキュメントを正常に受取ったときに、ビジネスシグナル「受領確認（Acceptance Acknowledgement)」を返送します。

原則としてビジネスシグナル「受信確認」と「受領確認」の両方の返送を行うものとします。

図表５－９　受信確認の方法



（2）拡張Ｚ手順の場合

アプリケーションがビジネスドキュメントを正常に受取ったときに、受信確認ドキュメントを返送することで、受信の確認を行います。

受信確認ドキュメントの内容は取引当事者間で取り決めることとします。

３．４　ＣＰＡテンプレート

（1）コラボレーション・プロトコル合意書（ＣＰＡ）

取引当事者間で合意したデータ交換のルールをコラボレーション・プロトコル合意書（ＣＰＡ）といいます。

ＣＰＡ情報は、ｅｂＸＭＬメッセージサービス機能の初期設定情報として使用されます。ＣＰＡ情報はXMLで記述されるため、そのままコンピュータで処理することができます。

ＣＰＡの主な記述内容を、図５－10 に示します。取引相手ごとに、送受信メッセージの種類、通信プロトコルの種類、再送回数などを記述します。

図表５－10　ＣＰＡの主な記述内容

1）ＣＰＡ定義
- ・ＣＰＡ－ＩＤ、ＣＰＡバージョン
- ・ＣＰＡ有効開始日時、ＣＰＡ有効期限日時

2）取引当事者定義（当事者ごとに設定）
- ・取引当事者名、取引当事者ＩＤ（企業コード）
- ・ビジネスプロセス定義文書へのリンク
- ・ビジネスプロセス定義上の役割
- ・送受信メッセージのＩＤ、名称
- ・デジタル署名の有無、証明書情報、ＣＡ局、セキュリティポリシー
- ・受信確認メッセージの要否、重複メッセージ除去の要否
- ・使用する通信プロトコル
- ・相手サーバのＵＲＬ
- ・再送回数、再送間隔、
- ・メッセージの順序保証の要否

3）ＭＩＭＥパート定義

4）パッケージング定義

（2）ＣＰＡテンプレート

ＣＰＡ情報を入力することにより、ｅｂＭＳ機能の初期設定作業を簡易化することができます。

しかしながら、利用者がＣＰＡ情報を一から作成するのは大変であるため、利用環境ごとに予め決めておける機能については、ＣＰＡテンプレートとしてＣＰＡの雛型を提供することができます。

利用環境に合ったＣＰＡテンプレートを使用することにより、利用者ごとに定義しなければならない情報のみの設定で済み、ｅｂＭＳ機能の初期設定作業が簡単にできるようになります。

４．ビジネスドキュメントの作成

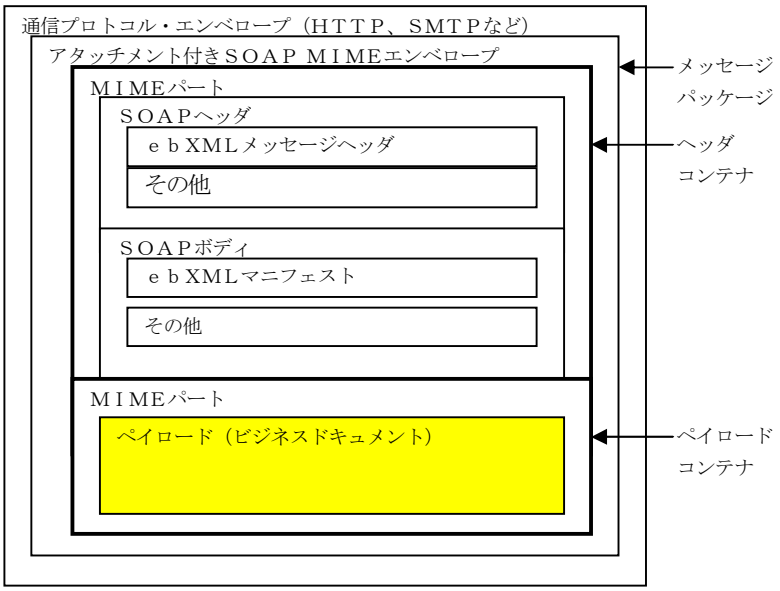
４．１　ビジネスドキュメントの構造

（1）ｅｂXMLメッセージの構造

インターネット上を流れるｅｂXMLメッセージの構造を図表５－11 に示します。

ｅｂXMLメッセージサービスでは、トランスポートプロトコルとしてＳＯＡＰを採用しており、それをｅｂXML用にＳＯＡＰエンベロープを拡張して使用しています。送受信データが格納されるペイロードコンテナは、複数個が存在できます。本標準に基づいて作成されるビジネスドキュメントは、ペイロードコンテナに格納されます。

図表５－11　ｅｂXMLメッセージの構造



（2）ビジネスドキュメントの構造

ｅｂXMLメッセージのペイロードコンテナに格納されるビジネスドキュメントの構造を図表５－12 に示します。

ビジネスドキュメントは、１つのビジネスドキュメント・ヘッダと１つ以上のビジネスドキュメント本体で構成されます。

なお、取引当事者間の合意により、ビジネスドキュメント・ヘッダを省略することができます。

ビジネスドキュメントの形式には、以下に示す一般型とバッチ型の２種類があります。

①一般型

通常の取引に使用する形式です。

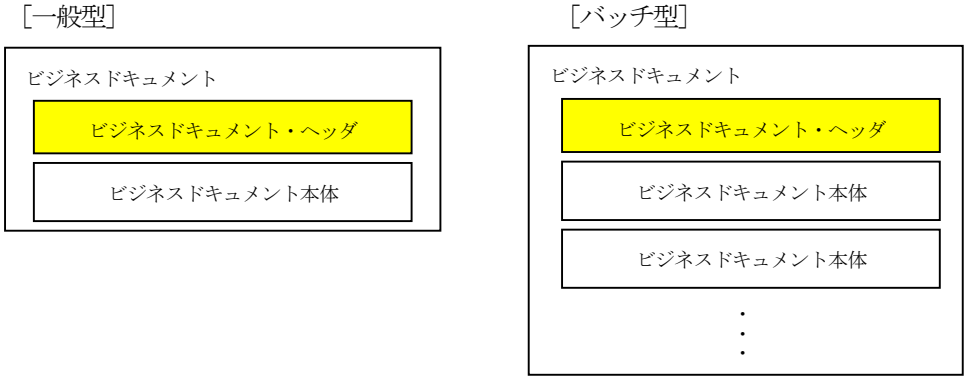
ビジネスドキュメントは、１つのビジネスドキュメント・ヘッダと１つのビジネスドキュメント本体から構成されます。

②バッチ型

複数のビジネスドキュメントをまとめて送る場合に使用する形式です。

ビジネスドキュメントは、１つのビジネスドキュメント・ヘッダと２つ以上のビジネスドキュメント本体から構成されます。ただし、２つ以上のビジネスドキュメント本体は、同一種類のビジネスドキュメントに限ります。

図表５－12　ビジネスドキュメントの構造



（注）取引当事者間の合意により、ビジネスドキュメント・ヘッダを省略することができます。

４．２　文字コード

（１）使用可能文字範囲

使用可能な文字範囲は、以下に示すＪＩＳ規格の規定範囲内とします。

①JIS X 0221-1 の範囲とし、かつ下記の規格が規定する文字集合とします。

ただし、Unicode でマッピングできない文字は使用禁止とします。

・JIS X 0201（英数字、半角カナ文字）
・JIS X 0208（第一・第二水準漢字）
・JIS X 0212（補助漢字）
・JIS X 0213（第三・第四水準漢字）

②ベーシック型ビジネスドキュメントについては、JIS X 0221-1 の範囲とし、かつ下記規格が規定する文字集合とします。

・JIS X 0201（英数字、半角カナ文字）
・JIS X 0208（第一・第二水準漢字）

（２）文字コードに関する補足事項

①符号化形式

ＵＴＦ－８とします。

②実装水準

実装水準：１（結合文字は使用しません）

③バージョン

使用するコンピュータに実装している Unicode のバージョンによって、上記の使用可能文字範囲に制約があることから、取引企業間で使用する文字についてあらかじめ取り決めておくものとします。

④使用するコンピュータのＯＳ

使用するＯＳにより、作成されるデータの文字コードが変わるため注意が必要です。

４．３　ＸＭＬスキーマの作成方法

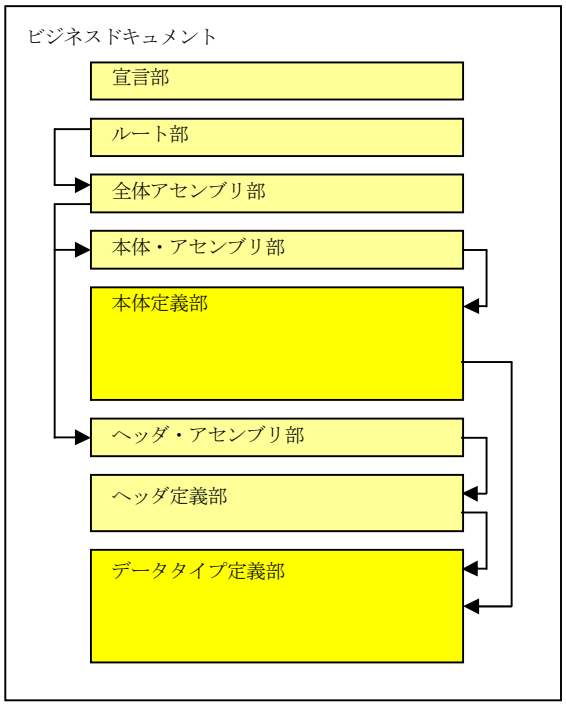
ＸＭＬスキーマは、ビジネスドキュメントの定義をＸＭＬで記述し、システムが処理できるようにしたものです。ＸＭＬスキーマは、トランスレータおよびマッピングツールに入力されて活用されます。

（１）ＸＭＬスキーマの構成

ＸＭＬスキーマの構成を図表５－13 に、各構成部の説明を図表５－14 に示します。

ビジネスドキュメントの構成要素を記述します。

図表５－13　ＸＭＬスキーマの構成



図表５－14　ＸＭＬスキーマの各構成部の説明

項番	構成部名	説明
1	宣言部	ＸＭＬスキーマの宣言を記述
2	ルート部	ビジネスドキュメントのルートを記述
3	全体アセンブリ部	ビジネスドキュメントの構成要素を記述
4	本体・アセンブリ部	本体の構成要素を記述
5	本体定義部	本体を構成するクラス、データ項目を記述
6	ヘッダ・アセンブリ部	ヘッダの構成要素を記述
7	ヘッダ定義部	ヘッダを構成するクラス、データ項目を記述
8	データタイプ定義部	データ項目のデータタイプを記述

（2）XMLスキーマの記述方法

（a）XMLタグの命名規則

①クラス、データ項目のXMLタグの場合

クラス　　：“JP”＋[クラスＩD]

データ項目　：“JP”＋[項目ＩD]

関係クラス　：“JP”＋[クラスＩDの“C”を“A”に置き換えたＩD]

②ルート部、全体アセンブリ部の場合

ビジネスドキュメント　　：クラス“JPCBD”、関係クラス“JPABD”

ビジネスドキュメント・ヘッダ：クラス“JPCBDH”、関係クラス“JPABDH”

ビジネスドキュメント本体　：クラス“JPCBDD”、関係クラス“JPABDD”

③データタイプ部の場合

整数　　：“Decimal”+[最大バイト数]

小数点付数値　：“Decimal”+[整数部最大バイト数]+“F”+[小数部バイト数]

英数字　　：“String”+[最小バイト数]+“to”+[最大バイト数]

漢字　　：“Kstring”+[最小バイト数の 1/2]+“to”+[最大バイト数の 1/2]

コード　　：“Cd”+[項目ID]

（b）クラス、データ項目の出現回数

・クラス、データ項目の出現回数を図表５－15 のように記述します。

図表５－15　クラス、データ項目の出現回数の記述

項番	ビジネスドキュメント定義書での出現回数表記	XMLスキーマでの出現回数記述
1	1	minOccurs=1, maxOccurs=1
2	0/1	minOccurs=0, maxOccurs=1
3	0-N	minOccurs=0, maxOccurs=N
4	1-N	minOccurs=1, maxOccurs=N

(注)"N"は、最大出現回数を表します。

（c）名前空間

・「物流XML／ＥＤＩ標準」の名前空間を宣言部で指定します。

・以下の名前空間とします。

http://www.butsuryu.or.jp/edi/schemas/"[ビジネスドキュメント ID]-[バージョン]-[リビジョン]"

(例)http://www.butsuryu.or.jp/edi/schemas/BDS3001-Ver01-01

（d）XMLスキーマのファイル名

・XMLスキーマのファイル名は以下のとおりとします。

[ビジネスドキュメント ID]-[バージョン]-[リビジョン]+“.xsd”

(例)BDS3001-Ver01-01.xsd

（e）任意項目の取扱い

・任意項目については、ビジネスドキュメント送信時にデータ値が無いときにはXMLタグは生成されません。

（f）クラスを構成するデータ項目

・クラスを構成するフルセットのデータ項目は、データ項目定義書で定義します。

・ビジネスドキュメントでは、クラスを構成するデータ項目の中から、必要なデータ項目のみ選択してXMLスキーマを定義します。従って、ビジネスドキュメントでは、出現回数が“0”のデータ項目は存在しません。

（3）XMLスキーマの記述例

```
<?xml version="1.0" encoding="UTF-8"?>                                                    宣言部
<xsd:schema
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.butsuryu.or.jp/edi/schemas/BDS3001-Ver01-01"
  xmlns="http://www.butsuryu.or.jp/edi/schemas/BDS3001-Ver01-01"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

  <xsd:element name="JPABD" type="TypeJPCBD"/>                                            ルート部

  <xsd:complexType name="TypeJPCBD">                                                      全体アセンブリ部
    <xsd:sequence>
      <xsd:element name="JPABDH" type="TypeJPCBDH"/>
      <xsd:element name="JPABDD" type="TypeJPCBDD" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="TypeJPCBDD">                                                     本体・アセンブリ部
    <xsd:sequence>
      <xsd:element name="JPA11701" type="TypeJPC11701" minOccurs="1" maxOccurs="1" />
      <xsd:element name="JPA11705" type="TypeJPC11705" minOccurs="1" maxOccurs="1" />
      <xsd:element name="JPA14201" type="TypeJPC14201" minOccurs="0" maxOccurs="1" />
        ・・・
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="TypeJPC11701">                                                   本体定義部
    <xsd:sequence>
      <xsd:element name="JP00001" type="String0to5" minOccurs="1" maxOccurs="1" />
      <xsd:element name="JP00002" type="Cd00002" minOccurs="1" maxOccurs="1" />
      <xsd:element name="JP00003" type="String0to8" minOccurs="0" maxOccurs="1" />
        ・・・
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="TypeJPCBDH">                                                     ヘッダ・アセンブリ部
    <xsd:sequence>
      <xsd:element name="JPA11706" type="TypeJPC11706" minOccurs="1" maxOccurs="1" />
      <xsd:element name="JPA12711" type="TypeJPC12711" minOccurs="1" maxOccurs="1" />
      <xsd:element name="JPA12712" type="TypeJPC12712" minOccurs="1" maxOccurs="1" />
      <xsd:element name="JPA11707" type="TypeJPC11707" minOccurs="1" maxOccurs="1" />
      <xsd:element name="JPA10901" type="TypeJPC10901" minOccurs="1" maxOccurs="1" />
      <xsd:element name="JPA14401" type="TypeJPC14401" minOccurs="1" maxOccurs="1" />
    </xsd:sequence>
  </xsd:complexType>

  (省略)                                                                                  ヘッダ定義部

  <xsd:simpleType name="String0to5">                                                      データタイプ定義部
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="5" />
    </xsd:restriction>
  </xsd:simpleType>
  ・・・
  ・・・
</xsd:schema>
```

５．セキュリティ対策

セキュリティ対策には、ＩＴを活用した技術面での対策と企業組織および人的資源を活用した運用面での対策があります。本編ではＩＴを活用した技術面のセキュリティ対策について記載します。

５．１　セキュリティ対策の種類

オープンなインターネットを通じて企業間で情報交換を行うためには、以下のセキュリティ対策が必要となります。

（1）盗聴に対する対策

第三者によるメッセージの盗聴を防止する対策です。

送信するメッセージを暗号化することにより、通信途中の盗聴を防止できます。暗号化する方法としては、個々のメッセージを暗号化する方法と通信路で一括して暗号化する方法があります。

（2）なりすまし、改ざんに対する対策

第三者による取引相手のなりすまし、第三者によるメッセージの改ざんを防止する対策です。

信頼のできる第三者の認証機関が発行したデジタル証明書を相手に送付することにより、なりすましを防止できます。

また、メッセージに添付したデジタル署名にデータのハッシュ値を含めることにより改ざんを検出できます。

（3）否認に対する対策

取引相手が事後にメッセージの送受信を否認することを防止する対策です。

メッセージに送信者のデジタル署名を添付して送信することにより、送信した事実を否認することを防止できます。また、受信確認データに受信者のデジタル署名を添付して送信することにより受信の事実を否認することも防止できます。

（4）不正アクセスに対する対策

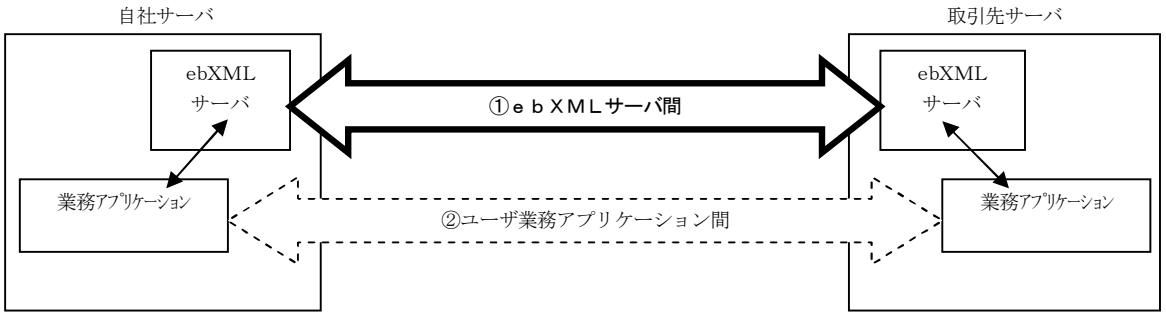
第三者からの不正なアクセスを防止する対策です。

ファイアウォールの設置により第三者からの不正なアクセスを排除することができます。

５．２　セキュリティ対策の内容

セキュリティ対策をとる範囲は、①ｅｂＸＭＬサーバ間、②ユーザ業務アプリケーション間、に大別されます。本編では、ｅｂＸＭＬサーバ間の通信経路上のセキュリティについてのみ記載します。アプリケーション間のセキュリティ対策については、取引当事者間でその必要性も含めて別途取り決めを行うものとします。

図表５－16　セキュリティ対策の範囲



（1）ＳＳＬ／ＴＬＳによるセキュリティ対策

前項の「（1）盗聴」、「（2）なりすまし、改ざん」に対する対策のため、サーバ間の通信路上では、ＳＳＬ／ＴＬＳ[9]を採用することを推奨します。

【ＳＳＬ／ＴＬＳ通信の準備】

サーバで鍵ペア（秘密鍵と公開鍵）とデジタル証明書要求ファイル（公開鍵を含む）を作成し、デジタル証明書要求ファイルを認証機関に送信してサーバ証明書の発行を受け、このサーバ証明書をサーバへインストールします。

【ＳＳＬ／ＴＬＳ通信の手順】

①自社サーバは、取引先サーバへの接続要求時に暗号化仕様の合意を取り、取引先サーバからサーバ証明書および公開鍵を受信します。

②自社サーバは、取得したサーバ証明書を参照し、証明書が信用する認証機関が発行したものか、有効期限が過ぎていないか等の確認を行います。

---

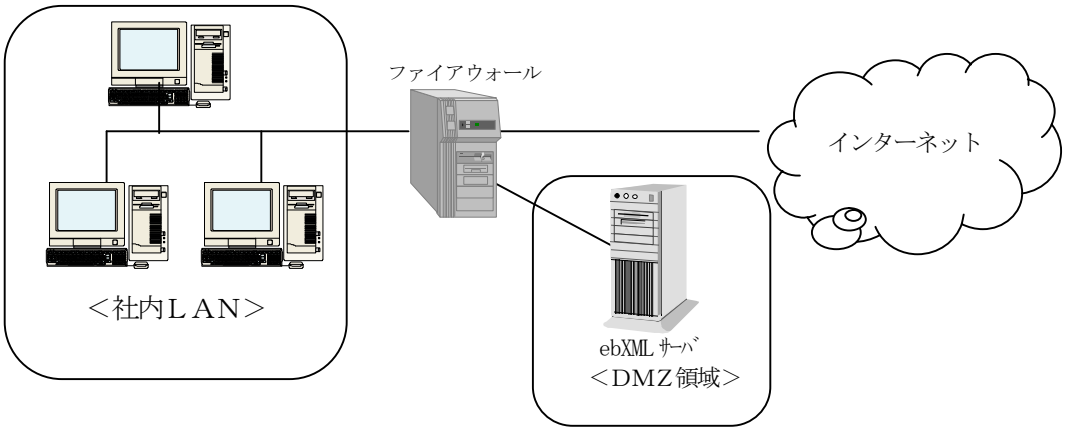
9 SSL/TLS: Secure Socket Layer/ Transport Layer Security, インターネット上でデータを暗号化して送受信するプロトコル。Netscape Communications 社が開発した SSL をＩＥＴＦが引継ぎ、若干の改良を加えて TLS として公開しました。

③自社サーバは共通鍵元データを生成し、それを取引先の公開鍵で暗号化して送信します。取引先サーバでは受信した共通鍵元データを自分の秘密鍵で復号化します。双方で共通鍵元データから共通鍵を生成します。
④自社サーバは送信データをこの共通鍵で暗号化して送信し、取引先サーバは受信データをこの共通鍵で復号化します。

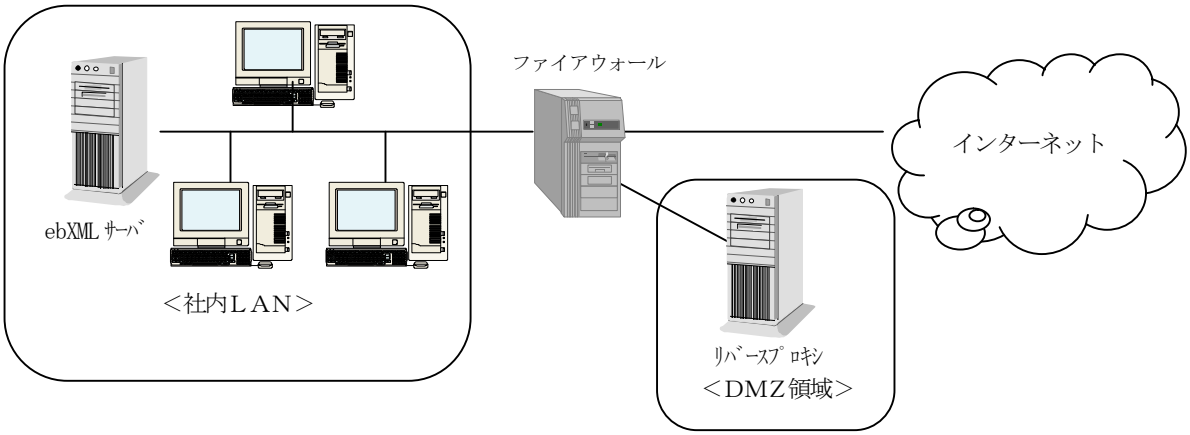
（2）ファイアウォールによる対策

前項の「（3）不正アクセス」に対する対策のため、ファイアウォールによるDMZ[10]領域を構築することを推奨します。
外部との通信はDMZ領域経由で行い、DMZ領域と社内ＬＡＮとの間の通信をファイアウォールで厳しく制限します。
ｅｂXMLサーバの設置には、①DMZ上に設置する方法と、②社内ＬＡＮ上に設置する方法があります。
ｅｂXMLサーバを社内ＬＡＮに設置する方法では、外部からのアクセスはリバースプロキシを経由するようにしておくことで、ｅｂXMLサーバが直接外部からアクセスを受けるリスクが低減できます。

図表５－17　ｅｂMSサーバをDMZ上に設置する方法



図表５－18　ｅｂMSサーバを社内ＬＡＮ上に設置する方法



10 DMZ: DeMilitarized Zone, 非武装地帯。ファイアウォールによって外部ネットワーク(インターネット)からも内部ネットワーク(組織内のネットワーク)からも隔離された区域のこと。