インターネットＥＤＩの手引き

平成１９年２月

社団法人　日本鉄鋼連盟

鉄鋼ＥＤＩセンター

目次

はじめに １

１．インターネットＥＤＩを使うメリット ２

２．インターネットＥＤＩの定義 ４

３．インターネットＥＤＩにおけるセキュリティ対策 ６

３－１．ネットワーク上のセキュリティ対策技術 ６

３－２．情報システム機器のセキュリティ ８

４．インターネットＥＤＩの種類 ９

５．実際の利用形態 11

　５－１．インターネットEDIの利用形態

５－１－１．ファイル転送型・メール型ＥＤＩの特徴 12

５－１－２．Ｗｅｂ型ＥＤＩの特徴 13

５－２．ファイル転送型ＥＤＩ 15

５－３．メール型ＥＤＩ 16

５－４．Ｗｅｂ型ＥＤＩ 18

６．業務内容に応じた使い分け 20

６－１．方式による使い分け 20

６－２．導入拠点による使い分け 21

７．鉄鋼版インターネットＥＤＩの推奨化 23

７－１．インターネットＥＤＩの推奨化項目 24

７－２．インターネットＥＤＩの運用ルールについて 26

７－２－１．標準企業コードの適用 26

７－２－２．読み出し不能データ 26

７－２－３．データ授受確認の取り決め 26

７－２－４．データ未達時の扱い 26

７－２－５．到達順序の逆転や二重送付 27

７－２－６．ゼロ件データの扱い 27

７－２－７．個別契約の成立（受発注業務が対象） 27

　　　７－２－８．責任範囲・責任分界点 28

　　　７－２－９．運用スケジュール 30

　　　７－２－１０．メッセージの保存 30

　　　７－２－１１．ファイル名 30

　　　７－２－１２．メールのアドレス、容量、サブジェクト名、データの分割・圧縮等 30

　　　７－２－１３．その他の付帯業務機能 30

　　７－３．インターネットＥＤＩ契約書例 32

　　　７－３－１．Ｅメール型 32

　　　７－３－２．Ｗｅｂ型 37

　　７－４．運用マニュアルの内容 42

【付録】

　インターネットＥＤＩパッケージ製品に関するベンダーへのアンケート調査結果

はじめに

１９９４年に制定された鉄鋼ＥＤＩ標準では、通信回線は主としてＶＡＮが想定され、通信プロトコルとして全銀手順を使用することが定められている。このいわゆるトラディショナルなＥＤＩは大手企業を中心に鉄鋼業界の情報化に一定の成果をあげてきた。コンピュータ設備、ＶＡＮ加入等の初期投資やランニングコストの負担が大であり、これがボトルネックとなり中小規模企業へのＥＤＩ導入が進展しない要因になっているとの指摘もあり、インターネット環境をベースにして情報システム基盤の発展に併せ、通信プロトコル・技術をＴＣＰ／ＩＰ、ＦＴＰ、ＳＭＴＰ、ＨＴＴＰ、ＷＷＷサーバ／ブラウザを前提に鉄鋼ＥＤＩ標準／インターネットＥＤＩの手引きとして、２００１年に見直しを行った。

その結果、需要家から鉄鋼ＥＤＩ標準の枠内に収まらない方式でのＥＤＩ連結要請に対して鉄鋼ＥＤＩセンターとして、新方式のＥＤＩを整理し、どの範囲までを標準化し、あるいは推奨利用方法を取り決めていくべきか取り決め、成果を上げてきた。

インターネットＥＤＩの手引き作成して5年が経過し、情報システムの進歩、情報セキュリティリスク対応などの要求をうけ、鉄鋼業界に属する企業がインターネットＥＤＩを進める際の指針となることを念頭に、ここで利用するメリット、インターネットＥＤＩの種類について整理し、次の鉄鋼業界におけるインターネットＥＤＩの運用標準として見直しを行った。

１．インターネットＥＤＩを使うメリット

コスト

インターネットＥＤＩはVAN等の専用線をベースとしたＥＤＩに比べて導入・運用・保守にかかるコストが小さく、通信速度も速い。

また、通信コストは通信相手との距離に関わらず一定であり、従来型の回線に比べて海外ユーザとの取引など通信相手との距離が遠くなるほどコストパフォーマンスが高くなる特徴がある。

使用する機器の面からみると、パフォーマンス的には市販のＰＣレベルの能力で十分であり、ソフトウェアも市販のものが使用できるため、ハードと基本・応用ソフトにかかるコストが小さい。

しかしながら、インターネットは公衆網と位置付けられ、様々な利用者が存在する網となっている。よって、専用線環境と比較してセキュリティは低下する。そのため、情報漏洩リスク（暗号化、誤送信等）、社外からの脅威（ウィルス、不正アクセス）について、施策を検討する必要性があり、別途、対策への負担が発生する。

グローバルネットワーク（接続容易性）

インターネットの特長として世界中の拠点とシームレスに接続できるため、少ない取引量の取引先との小規模なＥＤＩや特定多数との情報交換が簡単に実現できる。

また、インターネットＥＤＩ用のパッケージソフトを導入することによって、取引量・情報種に応じてデータ交換方式が簡便に選択できる。

ローカル環境設定スキル

市販のＰＣを使用し、ブラウザとインターネット接続の設定だけでデータ交換が可能になるなど、ハード、ソフトとも技術面で高度なスキルが必要とされず、特に一部のファイル転送型・メール型ＥＤＩやＷｅｂ－ＥＤＩにおいてはＥＤＩ標準の理解が必須ではなく、ＣＩＩ等の特別なﾄﾗﾝｽﾚｰﾀも基本的に不要なことなどから、導入における技術的な障壁が低い。

しかしながら、個別ローカルのPCが前提となることにより、個々のシステム環境の運用管理レベルに負う範囲が広がっている、特にセキュリティに関しては別途検討する必要がある。

セキュリティ

インターネットの特性上、取引するメッセージの秘匿性保証、データ改竄、受発信者のなりすまし等の脅威に対するセキュリティ対策を講じることが必須となる。

ローカルＰＣについても基本的ソフトウェアの導入については容易ではあるが､ﾍﾞﾝﾀﾞｰｻﾎﾟｰﾄがあるソフトウェアを利用し的確なﾊﾟｯﾁﾏﾈｼﾞﾒﾝﾄを実施する、ウィルス対策ソフトを導入し適宜パターンファイルを更新することなどローカルPCにおける運用管理が重要となる。

【第１表】インターネットＥＤＩと従来型ＥＤＩの対比

|  |  |  |
| --- | --- | --- |
|  | インターネットＥＤＩ | 従来型ＥＤＩ |
| 利用する通信サービスとそのコスト | * ＩＳＰ※によるインターネット接続サー（回線は専用線、ｱﾅﾛｸﾞ、ISDN、xDSL、ｹｰﾌﾞﾙ、無線など）   ・通信速度(128Kbps～100Mbps)  ・低料金 | ・ＶＡＮサービス  ・回線速度（14.4K～33.6Kbps）  ・高額な利用料金 |
| 接続拠点 | インターネットに接続されている拠点全て | ＶＡＮ加入が必要 |
| 利用するハードウェア | 標準的レベルのPC | ホスト、ワークステーションなど |
| 利用するソフトウェア | 比較的低価格の市販品の利用が可能 | 専用ソフトウェア |
| セキュリティ | 特別な対策を施すことが必要。  細やかなセキュリティ計画と施策が必須となる。 | 専用ＶＡＮのためセキュリティは高い |

　　　　　　※ＩＳＰ　インターネット接続業者

２．インターネットＥＤＩの定義

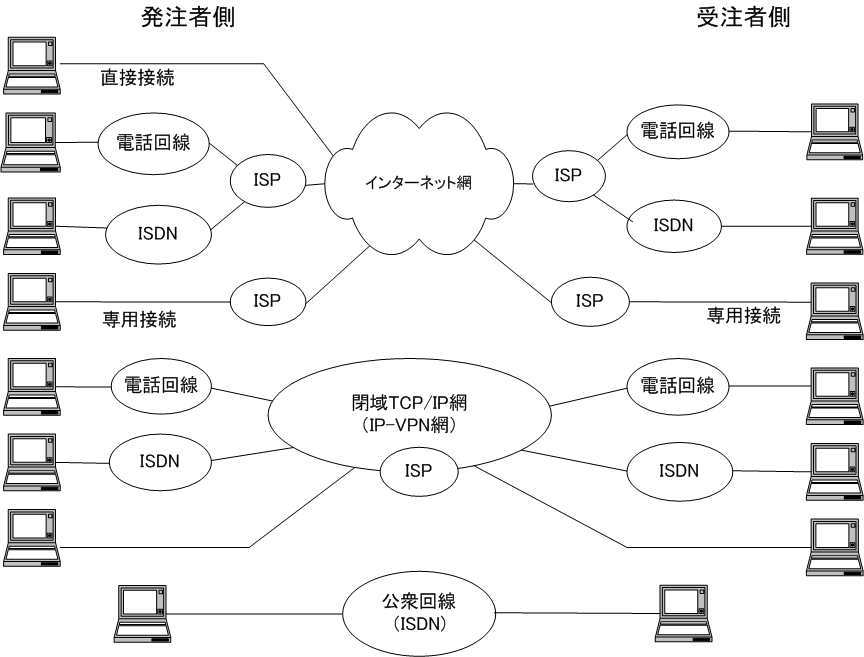
本手引きでは、インターネットＥＤＩを次のように定義する。

異なる組織間で、取引のためのメッセージを、インターネット関連技術と標準的な規約（可能な限り広く合意された各種規約）を用いて、コンピュータ（端末を含む）間で交換すること。

通信プロトコルにはＴＣＰ／ＩＰを使用し、通信回線は**インターネット**に限らない。

交換するデータは業界標準、国際標準に準拠したメッセージもしくは項目を使用する。

【第１図】インターネットＥＤＩ通信基盤



【第２表】インターネットＥＤＩ通信分類

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 分類 | 通信回線 | 通信方式 | 通信プロトコル | |
| ﾄﾗﾝｽﾎﾟｰﾄ・NW層 | AP層 |
| インターネット | インターネット網 | E-mail | TCP/IP | SMTP/MIME |
| Weｂ型 | TCP/IP | HTTP |
| IP-VPN網 | ファイル転送 | TCP/IP | FTP |
| E-mail | TCP/IP | SMTP/MIME |
| Weｂ型 | TCP/IP | HTTP |
| 公衆網（ISDN） | Web型 | TCP/IP | HTTP |

【第３表】通信回線の違いによる機能について

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | IP-VPN網 | インターネットVPN | インターネット網 | 公衆回線(ISDN) |
| 使用するネットワーク | ISPが提供するﾊﾞｯｸﾎﾞｰﾝﾈｯﾄﾜｰｸ | インターネット網 | インターネット網 | 電話網 |
| ネットワークへの接続 | ﾙｰﾀ経由IP-VPNに接続  (相互接続には費用発生) | VPN機器経由インターネット網に接続 | ファイアウォール経由インターネット網に接続 | ﾙｰﾀ経由電話網に接続 |
| VPN管理 | IP-VPNプロバイダが実施 | ユーザで実施  （VPNネットワーク情報、NAT管理、FW） | 対象なし。 | 対象なし。 |
| パフォーマンス | 遅延・ｽﾙｰﾌﾟｯﾄの保証あり。 | 遅延、ｽﾙｰﾌﾟｯﾄの保証無し。 | 遅延、ｽﾙｰﾌﾟｯﾄの保証無し。 | 遅延、ｽﾙｰﾌﾟｯﾄの保証無し。 |
| セキュリティ | 安全 | 比較的安全 | なし | 比較的安全 |
| 信頼性 | 稼働率指標（MTBF等あり） | 明確な信頼性保証なし。 | 明確な信頼性保証なし。 | 明確な信頼性保証なし。 |
| 問題発生時に切り分け容易 | 問題発生時に切り分け比較的困難 | 問題発生時に切り分け困難 | 問題発生時に切り分け困難 |
| 初期費用 | 高い | 比較的安い | 安い | 安い |
| ランニング費用  （送受信データ量/円） | 高い | IP-VPN網よりは安い  (接続拠点数に比例して運用コストが増) | 安い | 高い |

MTBF: Mean Time Between Failure　ある機器やシステムが故障するまでの時間の平均値。使用を開始して、あるいは故障から回復してから、次に故障するまでの平均時間。

NAT：Network Address Translation　組織内でのみ通用するIPアドレス（ローカルアドレス）と、インターネット上のアドレス（グローバルアドレス）を透過的に相互変換すること。

３．インターネットＥＤＩにおけるセキュリティ対策

インターネットを利用したＥＤＩでは、メッセージの秘匿性保証、データ改竄・変質、受発信者のなりすまし等のセキュリティ問題への対応策を講じる必要がある。一般的には、インターネットを利用したメッセージ送受でのセキュリティ課題に対しては、以下のような対策が考えられ、以下のＯＳＩ参照モデルより、セキュリティリスクをどの階層で意識するか、情報秘匿性をどのレベルで意識するのかを判断し、適用する技術を決めることがポイントとなる。

３－１．ネットワーク上（情報経路の安全性）のセキュリティ対策技術

【第２図】ＯＳＩ参照モデルとセキュリティ技術適用範囲

　　　　　　注：SETおよびTLSについては対象外とする。

　　　　　　SET（Secure Electronic Transactions）：ｲﾝﾀｰﾈｯﾄを通じて安全なｸﾚｼﾞｯﾄｶｰﾄﾞ決済を行なうための技術仕様。

　　 　　　　　TLS(Transport Layer Security)：ｲﾝﾀｰﾈｯﾄ上で情報を暗号化して送受信するﾌﾟﾛﾄｺﾙの一つ。

【第４表】セキュリティの課題と対策

|  |  |
| --- | --- |
| メッセージ送受でのセキュリティ課題 | セキュリティ対策 |
| ①盗聴、改竄防止…機密性、情報の完全性  第三者により盗聴された場合にその機密性を最大限に確保するためにデータを暗号化し、また、やりとりされるデータが改竄されていないかを判定する必要がある | ・暗号化による情報の秘匿  ・メッセージ･ﾀﾞｲｼﾞｪｽﾄの照合 |
| ②なりすましへの対応策…認証  メッセージの送信者、受信者が正しい通信相手かどうか、システムへのアクセス者が利用資格のある相手かどうかを確認する必要がある。 | ・ＩＤ，パスワードチェック  ・暗号技術による相互認証 |
| ③否認への対応策…否認防止  メッセージの送信元が誰であるかを確かにし、送信者が送信後にメッセージ送付の事実を否認できないようにする。 | ・デジタル署名 |

（１）盗聴、改竄に対する対策

　盗聴、改竄防止の暗号化手法としては、伝送路そのものを暗号化するＩＰｓｅｃや、伝送されるデータ部分を暗号化するＳＳＬ、Ｓ／ＭＩＭＥなどが使用される。

（２）なりすましに対する対策

　インターネットのような第三者が送受信者になりすましてデータ授受を行う可能性のある伝送路を使用する場合は、サービスの利用資格を確認するＩＤ、パスワードや認証局（ＣＡ）の発行する証明書を用いて、相手認証を行う。前記ＳＳＬには、ＣＡの発行する証明書を用いて、サーバ認証およびクライアント認証の、双方向の認証機能がある。

（３）否認に対する対策

　否認を防止するため、送信者の電子署名（デジタル署名）を受信者側で検証する手法が使用される。

（４）ＰＫＩ技術

　前記（１）～（３）のセキュリティ対策に使用される暗号化の技術は、公開鍵インフラストラクチャ（ＰＫＩ；Public Key Infrastructure）と呼ばれる技術で実現できる。この技術は認証機関（ＣＡ；Certification Authority）の発行する電子証明書（デジタル証明書あるいはデジタルＩＤとも呼ぶ）を、実物の書簡などを通信する場合の身分証明書、印章、署名として使用するものである。

3-2．情報システム機器のセキュリティ

　インターネットを利用したＥＤＩでは、メッセージの秘匿性保証、データ改竄・変質、受発信者のなりすまし等のセキュリティ問題としての対応策を記述したが、加えて、EDIサービスを運用、維持する上での機器のセキュリティ管理も重要なポイントとなる。インターネットを利用したメッセージ送受でのセキュリティリスク（脅威）に対しては、防御策となり、以下の項目について検討することが望ましい。

【第5表】IPレベル、通信方式レベル

|  |  |
| --- | --- |
| ファイアウォール | 社外、社内との接続点における、特定アドレス、サービス（HTTP、FTP等）について中継の許可、不許可の管理を行う。  不要なサービス（Port）は、空けないことがポイント。  サービスサーバはファイアウォールの内側に設置。 |
| 利用者認証  （IDとパスワード） | あらかじめ登録して秘密の文字列、数字列で相手の本人認証を行う。  不正アクセス予防の観点より、定期的なPW更新を義務付けることが望ましい。 |

【第6表】情報機器のセキュリティ

|  |  |
| --- | --- |
| ウィルスチェック・駆除 | サーバおよびクライアントにウィルス検知ソフトウェアを導入。  運用として適宜、ウィルス検知のパターンファイルを更新することを心掛けることが重要。   1. 悪意をもった第三者によるデータの破壊を防止。 2. ウィルス感染により、設置機器自身が感染源にならないための予防。 |
| IDとパスワード | あらかじめ登録して秘密の文字列、数字列で相手の本人認証を行う方式（クライアント認証）（なりすまし防止）。  運用として、ユーザ管理とログ管理が重要となる。 |
| 導入ソフトウェアのセキュリティパッチ適用 | 情報システム機器の基本OSに加えて、パッケージソフトウェアには脆弱性が存在し、その脆弱性の修正のためのパッチと呼ばれるプログラムが提供される。悪意の持った第三者は、この脆弱性を狙って、攻撃を行う事が殆どである。適宜、セキュリティパッチを適用することが重要となる。 |

４．インターネットＥＤＩの種類

インターネットＥＤＩは通信手順の違いによって、以下の３つに大別できる。

①ファイル転送型ＥＤＩ

ＥＤＩメッセージをファイル形式で送受信するもの。通信プロトコルとしては、FTP、全銀TCP/IPなどがある。

②メール型ＥＤＩ

ＥＤＩメッセージをメールの添付ファイル形式で送受信するもの。

SMTPでは、文字列しか送受信できないが、MIME方式によりバイナリデータを含むファイルを送受信する。

③Ｗｅｂ－ＥＤＩ

ＥＤＩメッセージをＨＴＭＬ形式に変換し、ＷＷＷサーバに登録することにより、ＷＷＷブラウザからＥＤＩメッセージの閲覧および簡易入力、ファイルのダウンロード等を可能とするもの。

　　　受信者側は基本的には人間が介在し、ファイル情報はダウンロードとアップロードも可能である。

【第4図】通信手順の違いによる分類

インターネットＥＤＩ

ファイル転送型ＥＤＩ

（全銀ＴＣＰ／ＩＰ、拡張Ｚ手順、ＦＴＰ等）

メール型ＥＤＩ

（ＳＭＴＰ／ＭＩＭＥ等）

Ｗｅｂ－ＥＤＩ

（ＨＴＴＰ等）

また、ファイル転送型ＥＤＩとメール型ＥＤＩは、通信手順のみにインターネット関連通信プロトコルを使用する。通信フォーマットは、従来型ＥＤＩの延長型と送受信するデータに固定長フォーマットを使用したものとに分け検討する。

この２つの方式の違いは、ﾄﾗﾝｽﾚｰﾀを使用するか否かによって明確に区分される。

【第5図】データフォーマットの違いによる分類

インターネットＥＤＩ

（ファイル転送型とメール型）

可変長フォーマットによる従来型ＥＤＩタイプ

（トランスレータを使用）

固定長フォーマットを使用したタイプ

（トランスレータは不使用）

５．実際の利用形態

ファイル転送型、メール型、Ｗｅｂ型、それぞれインターネットＥＤＩの利用形態はセキュリティ方式、利用するネットワークの種類等によって多種多様なバリエーションが考えられる。

なお、インターネットＥＤＩパッケージソフトの利用も、送達確認など必要なサービスがパッケージで手に入ることや、情報種・相手先に応じてメール型、Ｗｅｂ－ＥＤＩの併用も可能になるなど、効果的な場合がある。パッケージソフトの詳細については巻末の付録を参照のこと。

【第6図】インターネットＥＤＩの利用形態

**送信者**

基幹業務システム

メール

サーバ

WEB

サーバ

FTP

サーバ

**SMTP**

**HTTP**

**FTP**

ISP

メールボックス

**SMTP**

# Internet

**POP3**

**受信者**

メール

サーバ

メール

ソフト

**IMAP**

**/POP3**

WEB

ブラウザ

FTP

クライ

アント

ソフト

業務アプリケーション

MS-Excelなど

メール

ソフト

5－1．インターネットＥＤＩのタイプ毎の特徴

5－1－1．ファイル転送型・メール型ＥＤＩの特徴

　（１）ﾄﾗﾝｽﾚｰﾀを使用した方式

【第7図】ファイル転送型・メール型ＥＤＩ（ﾄﾗﾝｽﾚｰﾀ使用）



インターネット



CIIﾄﾗﾝｽﾚｰﾀ

CIIﾄﾗﾝｽﾚｰﾀ

・ﾄﾗﾝｽﾚｰﾀを利用して、ユーザ個別フォーマットと標準フォーマットの形式変換を行い、標準メッセージを生成する。従来型ＥＤＩとの違いは通信プロトコルにインターネット関連技術を用いた点のみで、基本的には従来型ＥＤＩの延長上にあると言える。

・基本的にデータ転送はﾊﾞｯﾁ型。ファイル転送型、メール型ともに効率的な運用のためには自動的送受信の仕組みや、自社システムとのデータ連携の仕組みについてのシステム構築が必要となる。

・授受するデータは、一般には受発注データ、販売情報データ、物流データなどといったﾊﾞｯﾁ型に向いたもの。鉄鋼業界においては既存の鉄鋼ＥＤＩ標準メッセージとなる。

　（２）ﾄﾗﾝｽﾚｰﾀを使用しない方式

【第8図】ファイル転送型・メール型ＥＤＩ（ﾄﾗﾝｽﾚｰﾀ不使用）



インターネット

CSV形式ﾌｧｲﾙの受け渡し可能



・送受信するデータのフォーマットは相互の取り決めによる。

・データ転送は自動化が理想的だが、少量、非定期的データ交換の場合は、人手を介するケースが多くなると考えられる。

・システム構築に際してＥＤＩ諸規約の理解や社内の基幹システムとの連携は必ずしも必要とはならない。

5－1－2．Ｗｅｂ型ＥＤＩの特徴

【第9図】Ｗｅｂ－ＥＤＩ



インターネット

Ａ社

Ｂ社

Webサーバー

Webﾌﾞﾗｳｻﾞ



Webﾌﾞﾗｳｻﾞ

クライアント



・当事者のどちらか一方がＷｅｂサーバを構えることが前提。ＩＳＰ等のＷｅｂサーバをレンタルし共同運用する形態もある。

・クライアントは、Ｗｅｂブラウザのみを使用して所定のＷｅｂサーバにログインして情報の検索、表示、印刷、入力、ダウンロード、アップロードを行う。また、拡張性を高めるためにはクライアント側に集計、印刷など独自アプリケーションの導入も行うことが有効である。

・人手を仲介した、会話形式によるデータ処理

・ＥＤＩ諸規約の理解が不要

・サーバ側は、社内基幹システムとＷｅｂサーバの間でデータの自動変換処理が必要。

・クライアントが必要に応じてダウンロード・アップロードするデータ形式は相互取り決めで柔軟に対応可能。

・非定期的に情報が発生し、その情報が随時変更される可能性がある情報に有効。従って業界内で共有する新商品情報データベース、今後の製品製造計画や長期的な発注予定情報をデータベース化して取引企業との間で共有する資材受発注システムなどに向いている。

【第7表】インターネットＥＤＩの種類による機能比較

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 比較項目 | | ファイル転送型 | メール型 | Ｗｅｂ型 |
| セキュリティ | 電子署名 | △ | ◎ | △ |
| 暗号強度（情報） | △  IP-SEC活用 | ◎  S/MIME活用 | △  SSL活用 |
| 構築の容易性 | 出側 | ○ | ○ | △  基本的にＡＰ開発が必要 |
| 受側 | ○ | ◎ | ◎  ＰＣブラウザのみ |
| 運用の容易性 | 送達確認 | ○  ログを残すことができる。 | △  一部ﾒｰﾗでは送達確認可能。  ＡＰ改造もしくは人手の運用で対応 | ○  ログを残すことができる。 |
| ファイルの再受信 | ×  ＡＰで対応可能 | × | △  人間介在が基本  APで対応可能。 |
| サイクル管理 | ×  ＡＰで対応可能 | ×  ＡＰで対応可能 | ×  人間介在が基本 |
| 二重交換防止 | ×  ＡＰで対応可能 | ×  ＡＰで対応可能 | △  人間介在が基本 |
| １回の転送データ量 | ◎  特に制限なし | △  ローカル環境に依存。  １ＭＢ～10ＭＢ以下が目安、大量データはＡＰによる分割・結合で対応可能 | ○  ダウンロード、アップロード方式。  ローカル環境に依存。 |

（注）◎：特に優れている、○：問題なく対応できる、

　　　　　　　 △：機能的に不足している、×：機能的に対応できない

5－2．ファイル転送型ＥＤＩ

ファイル転送型のＥＤＩでは、エンド・エンド間の伝送路を、 ＩＰＳｅｃ（IP Security Protocol）に代表されるＶＰＮ(仮想プライベート網)技術を利用して暗号化する場合は、専用線と同じ手法でデータ交換が可能である。すなわち、利用者はあたかも社内ＬＡＮを利用しているように、ファイル転送を行うことができる。

　一方、メール型やＷｅｂ型と同様にエンド・エンド間でのデータ暗号化を行う手法としては、ＳＳＬがあるが、標準ツールとして提供されているわけではないので、利用者側でのソフト導入、利用上の工夫が必要である。

　以下では、ＩＰＳｅｃを適用した場合の処理手順、注意点等について述べる。

【第9図】IP-secによる暗号化通信

カプセル化されたﾊﾟｹｯﾄﾃﾞｰﾀ

受信者

送信者

IPSec装置

IPSec装置

インターネット／イントラネット

復号化ﾃﾞｰﾀ

暗号化ﾃﾞｰﾀ

送受ヘッダ

暗号化ﾃﾞｰﾀ

仮想的な社内ネットワーク

社内ネットワーク

社内ネットワーク

（１）ＩＰＳｅｃの動作概要

　ＩＰＳｅｃは、暗号化および復号化の処理と、ユーザ認証の処理機能を備えている。ただし、認証および暗号化のアルゴリズムは仕様に含まれておらず、認証方式や暗号化方式を通知し合うための枠組みのみ提供している。このため実際の使用では、ＩＰＳｅｃ製品同士での相互運用性確認が必要である。

　・送信側ではデータを暗号化し、電子署名を付与し、暗号データをカプセル化して送信する

　・受信側はカプセルから取り出し暗号文を復号化し、電子署名により相手認証を行う

（２）ＩＰＳｅｃのデータ構成

　ＩＰＳｅｃの規定は、認証ヘッダ、パケット暗号化、鍵配送の三つから構成されている。

　・認証ヘッダ ：ＩＰデータそのものを認証するために、ＩＰヘッダに付加するシーケンス番号、ハッシュ関数によるダイジェストデータなど

　・パケット暗号化：IPパケット全体の暗号化(トンネルモード)またはＩＰパケットのデータ部分のみの暗号化(トランスポートモード)の２種類のモードを選択できる．ネットワーク構成により、利用できるモードに差が生じるが、ファイアウォールでＩＰＳｅｃ処理を行う場合は、トンネルモードしか採用できない

　・鍵配送　　 ：鍵の管理、交換の規定．ユーザが手作業で鍵を一致させる方法とＩＳＡＫＭＰ(Internet Security Association and Key Management Protocol)プロトコルを利用して動的に交換する方法がある．データ交換拠点数が多くなるとＩＳＡＫＭＰによる鍵交換が望ましいが、製品によってはこの機能を実装していないこともある

5－3．メール型ＥＤＩ

　電子メールでファイルを送受信する場合に選択できる手法には、Ｓ／ＭＩＭＥ（Secure Multipurpose Internet Mail Extensions）とＰＧＰ(Pretty Good Privacy)がある。

　両者とも、電子メールの暗号化／復号化、電子署名の作成、添付、確認という機能を備えているが、公開鍵の保証方法が異なる。Ｓ／ＭＩＭＥではＣＡの証明書が公開鍵の正当性を保証するが、ＰＧＰではＣＡを利用せず、知り合い同士で公開鍵の信頼性を保証する手法を用いる。

　以下では、Ｓ／ＭＩＭＥの使用指針について述べる。

（１）Ｓ／ＭＩＭＥによるデータ交換方式の概要

【第7図】Ｓ／ＭＩＭＥによるデータ交換方式

（２）データ処理手順

　暗号化メールを送受する場合は、送受信双方の電子証明書の取得が必要である。電子証明書の取得は、商用のＣＡを利用が望ましいが、データ交換者相互間の合意に基づく方法で行うことも可能である。

電子証明書の取得から、データ送受信の手順概要は以下の通りとなる。

・電子証明書を取得（秘密鍵と公開鍵を生成することと等しい）

秘密鍵は自分の手元に保管し、公開鍵を郵送、Web等の手段で通信相手に通知

・送信側の処理

①電子署名の作成

送信する電子メールを元にメッセージ･ﾀﾞｲｼﾞｪｽﾄと呼ばれるデータを作成し、これを送信側の秘密鍵で暗号化する。電子署名は、改竄の有無などを受信側で確認するために使用する。

②メール全体の暗号化

送信する電子メールと電子署名および証明書を一つのファイルにして、メール本文にファイルとして添付して共通鍵で暗号化する。

③共通鍵の暗号化…共通鍵を受信相手の公開鍵で暗号化する

④電子メールの送信…暗号文と暗号化された共通鍵を電子メールに記載して送信する。

・受信側の処理

⑤共通鍵の復号

受信された電子メールを元に戻すには、暗号化に使用された共通鍵の暗号を解く必要がある。ここでは受信者の公開鍵で暗号化されているので、受信者の秘密鍵のみで復号化できる。

⑥暗号文の復号…前記の復号された共通鍵を使用して、受信したメールと電子署名を復号する。

⑦電子署名のチェック

電子署名および証明書を用いて、受信された電子メールが途中で改ざんされていないことを確認する。

（３）Ｓ／ＭＩＭＥにおいて選択する暗号化方式

Ｓ／ＭＩＭＥを採用する場合のアルゴリズム例として以下のものがある

・メッセージ･ﾀﾞｲｼﾞｪｽﾄのアルゴリズム…**ＳＨＡ１（20ﾊﾞｲﾄ）**，ＭＤ５（16バイト）

・公開鍵暗号化方式…**ＲＳＡ**、DSA、ECDSA

・秘密鍵暗号化方式…**ＤＥＳ,３DES**,IDEA、RC2

5－4．Ｗｅｂ型ＥＤＩ

WWWサーバとWWWブラウザ間でＥＤＩを実現する場合は、ほとんどのＷｅｂツールに標準装備されているＳＳＬを使用する。ＳＳＬも、前記Ｓ／ＭＩＭＥと類似のクライアント／サーバの認証、データの暗号化／復号化の機能を持っており、インターネット上の通信を安全に行うための標準的な仕組みとして広く使われている。

（１）ＳＳＬの動作概要

【第8図】ＳＳＬによる通信方式

サーバ側

クライアント側

SSLリクエスト

WWWサーバの証明書送出

ｸﾗｲｱﾝﾄ証明書のﾘｸｴｽﾄ

クライアント証明書送出

データ暗号化用の共通鍵送信

データを暗号化して送受信

暗号化仕様の交換

サーバの認証

サーバ公開鍵の取得

クライアントの認証

クライアント公開鍵の取得

共通鍵の生成

サーバデータ暗号化

クライアントデータ暗号化

サーバデータ復号化

ｸﾗｲｱﾝﾄﾃﾞｰﾀ暗号化

（２）処理手順

・クライアントがＳＳＬリクエストを送ると、サーバはブラウザに証明書(サーバの公開鍵を含む)を送付する。ブラウザは、ＣＡの公開鍵で電子署名を復号化してメッセージ･ﾀﾞｲｼﾞｪｽﾄを取り出し、同時に受け取った証明書からメッセージ･ﾀﾞｲｼﾞｪｽﾄを作成し、その一致を確認する。両者が一致すれば証明書が確かなものであり、サーバの認証が完了する。

注)ＣＡの電子署名の復号化に必要なＣＡ公開鍵は、Internet Explorerのような主要なブラウザ製品に組み込まれている。したがって、Verisignのような著名な商用ＣＡを使用する場合は、ＣＡ公開鍵の入手は不要である。

・サーバ側がクライアントを認証する場合は、クライアントに対して証明書送付をリクエストし、クライアント側からサーバに証明書(クライアントの公開鍵を含む)が送付される（オプション）

・相互認証、証明書からの公開鍵取り出しの後、この公開鍵を利用してデータ送受のための共通鍵(秘密鍵)が生成され、その秘密鍵で暗号化されたデータが送受信される。

（３）ＳＳＬにおいて選択する暗号化方式

　ＳＳＬでは、複数の暗号化方式が使用できるようになっており、通信の最初にブラウザとサーバ間で、相互に使用可能な暗号化方式を自動的に折衝する。したがって、あらかじめ標準的な暗号化方式を定める必要はない。なお、ＳＳＬでは秘密鍵暗号化方式として、**ＤＥＳ、トリプルＤＥＳ**、ＩＤＥＡ、ＲＣ２などが、公開鍵暗号化方式として**ＲＳＡ**、DSA、ECDSAなどが使用できる。

＜脚注＞

PKI:公開鍵暗号を用いた技術・製品全般を指す言葉。RSAや楕円曲線暗号などの公開鍵暗号技術、SSLを組みこんだWebサーバ/ブラウザ、S/MIME・PGPなどを使った暗号化電子メール、デジタル証明書を発行する認証局(CA)構築サーバなどが含まれる。

公開鍵暗号:対になる2つの鍵を使ってデータの暗号化・復号化を行う暗号方式。非対称暗号とも呼ばれる。片方は他人に広く公開するため公開鍵と呼ばれ、もう片方は本人だけがわかるように厳重に管理されるため秘密鍵と呼ばれる。秘密鍵で暗号化されたデータは対応する公開鍵でしか復号できず、公開鍵で暗号化されたデータは対応する秘密鍵でしか復号できない。暗号化と復号化を同じ鍵で行う秘密鍵暗号方式に比べ、鍵を安全な経路で輸送する必要がないため、鍵の管理が楽で安全性が高い。現在では公開鍵暗号の標準としてRSA暗号が広く普及している。

秘密鍵暗号：暗号化と復号化に同じ鍵を用いる暗号方式。暗号文の送信者と受信者で同じ鍵を共有する必要があるため、「共有鍵暗号」「共通鍵暗号」とも呼ばれる。暗号文を送受信する前に、あらかじめ安全な経路を使って秘密の鍵を共有する必要がある。代表的な秘密鍵暗号としては、アメリカ政府標準になっているDESや、FEAL、MISTY、IDEAなどがある

S/MIME:電子メールの暗号化方式の標準。RSA 公開鍵暗号方式を用いてメッセージを暗号化して送受信する。

SSL：Netscape Communications社が開発した、インターネット上で情報を暗号化して送受信するプロトコル。現在インターネットで広く使われているWWWやFTPなどのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信することができる。SSLは公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改竄、なりすましを防ぐことができる。HTTPやFTPなどの上位のプロトコルを利用するアプリケーションソフトからは、特に意識することなく透過的に利用することができる。

ハッシュ関数：与えられた原文から固定長の疑似乱数を生成する演算手法。通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないか調べることができる。不可逆な一方向関数を含むため、ハッシュ値から原文を再現することはできず、また同じハッシュ値を持つ、異なるデータを作成することは極めて困難である。

IP-sec：「Security Architecture for Internet Protocol」の略。IPsecは、暗号技術を使ってIPパケットの完全性や機密性を実現する仕組み。IPパケットの保護によって、HTTPやFTPといったアプリケーションプロトコルを使って転送されるデータが保護される。また既存のアプリケーションプログラムを変更しなくても、その通信でIPsecを利用することが可能。IPsecを使うホストは、相手のホストと事前にIPsecで使う暗号の種類や暗号鍵を取り決めます。この取り決めはSA（Security Association）と呼ばれます。SAの交換と、交換する相手ホストの認証にIKE（Internet Key Exchange）が使われます。

6．業務内容に応じた使い分け

6－1．方式による使い分け

ファイル転送型は情報量や種類についても従来型ＥＤＩに準じた利用が想定される。一方メール型およびＷｅｂ型は一般に情報量や件数が少ないものへの対応に優れており、その活用のために、より簡易な形での情報交換スタイルを指向し、新たなビジネスモデルを策定するケースも考えられる。

【第8表】情報件数による使い分け

|  |  |
| --- | --- |
|  | ファイル転送型(100件/日)　⇒メール型(100→10件/日)　⇒Ｗｅｂ型（数件/日） |
| 情報件数 | 多い　　　　　　　　　　　　　　　　　　　　　　　　　　少ない |

【第9表】情報伝達信頼性による使い分け（伝達　Ｐｕｔ式⇒Ｇｅｔ式の違い）

|  |  |
| --- | --- |
|  | ファイル転送型　　　　　⇒　　　　　　メール型　　　　　⇒　Ｗｅｂ型（数件/日） |
| 信頼性 | 高い　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　低い  　　　　　　　　　　　　　　　　　　　　　　　　　　　　　（ﾌｧｲﾙ転送型の補完的利用等） |

【第10表】情報の種類による使い分け

|  |  |
| --- | --- |
|  | ファイル転送型　　　　　　メール型　　　　　　　　　Ｗｅｂ型 |
| 情報の種類 | 商品情報、発注予定など新規のビジネスモデル  従来型ビジネスモデル |

6－2．導入拠点による使い分け

鉄鋼業界でインターネットＥＤＩを導入・利用する際に、従来型ＥＤＩの基盤の有無や商流上の位置付けによって、導入されるインターネットＥＤＩのタイプを想定した。特に従来型ＥＤＩの基盤のない企業は当初、コストや運用面で導入が比較的容易なメール型やＷｅｂ型クライアントとしての利用が想定される。

○従来型ＥＤＩの基盤がある鉄鋼ﾒｰｶ、総合商社、サービスセンター、コイルセンターなど

・従来型ＥＤＩの継続利用が主となる。

・必要に応じて従来型ＥＤＩの延長としてファイル転送型を補完的に利用する（通信コストの引き下げ、ＶＡＮ未加入業者とのＥＤＩ）。

・下流商流を対象としたメール型ＥＤＩやＷｅｂ－ＥＤＩのサーバ運用（ＥＤＩ利用の裾野の拡大）。

・ケースによってはＷｅｂクライアントとしての利用。

○従来型ＥＤＩ未導入のサービスセンター、ｺｲﾙｾﾝﾀｰ、特約店など

・当初はメール型ＥＤＩもしくはＷｅｂ－ＥＤＩクライアントとしてＥＤＩを導入する（最小の投資で最大の効果を期待）。

・取引量が増加し、人手がかかるようになったら、送受信の自動化を図るか、段階的にファイル転送型もしくは従来型ＥＤＩの活用を考慮する。

【第8図】今後のＥＤＩの活用方向



【第11表】インターネットＥＤＩの種類のまとめ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | ファイル転送型  （ﾄﾗﾝｽﾚｰﾀ使用） | | メール型  （ﾄﾗﾝｽﾚｰﾀ不使用） | | Ｗｅｂ型 | |
| サーバ | クライアント |
| 投資額 | 大(通信基盤以外の部分では従来型EDI導入と同様のシステム構築が必要) | | 小(基本的にPCとメール環境のみ) | | 大(サーバ機器､DBの準備､システム運用) | 小(基本的にPCとWWWへの接続のみ) |
| 技術的困難度 | EDI標準の理解､CIIﾄﾗﾝｽﾚｰﾀの導入､保守などﾊｰﾄﾞﾙが高い | | 容易(インターネットへの接続程度のスキルでよい) | | Webサーバの構築､比較的高い | 容易(インターネットへの接続程度のスキルでよい) |
| 使用回線 | 公衆網、VAN､VPN､インターネット(専用線､ﾀﾞｲﾔﾙｱｯﾌﾟ) | | | | | |
| 使用する通信プロトコル | 拡張Z手順  全銀TCP/IP  FTP等 | | SMTP/MIME等 | | HTTP等  (ファイルのアップロード、ダウンロードに必要に応じてFTP等も併用) | |
| 処理の型 | 人手を介さないﾊﾞｯﾁ処理 | | 人手を介した処理  (APでの作りこみ可能) | | 自動処理 | 人手を介した処理 |
| 社内情報システムとの連携 | 必要 | 必須ではない | | | 必要 | 必須ではない |
| 情報種類 | 基本的に大量･定期的な情報  受発注データ､販売情報データ､物流データなどといったﾊﾞｯﾁ型に向いたもの | | | 基本的に小規模･不定期な情報で、商品情報DB､資材受発注システムなど随時変更､入力される情報 | | |
| 業務内容 | 社内情報システムと一貫連携した業務 | | | 検索､表示､印刷､入力｡社内システムとは独立可 | 社内情報システムとの連携 | 検索､表示､印刷､入力｡社内システムとは独立可 |
| 対象拠点 | 鉄鋼ﾒｰｶ､大手商社､一部ｺｲﾙｾﾝﾀｰ等の従来型EDIを導入している企業 | | | 中小規模の従来型EDI未導入のｺｲﾙｾﾝﾀｰ､特約店等 | 鉄鋼ﾒｰｶ･大手商社等 | 中小規模の従来型EDI未導入のｺｲﾙｾﾝﾀｰ､特約店等 |

7．鉄鋼版インターネットＥＤＩの推奨化項目

　鉄鋼インターネットＥＤＩも業界標準としてあくまでも鉄鋼ＥＤＩ標準の延長上に位置付けられるものである。一方で、インターネットＥＤＩの特性を考える場合、メッセージの表現形式や運用ルール等にこれまでの枠組みでは対応しきれない部分も出てくる。

　鉄鋼版インターネットＥＤＩの推奨化項目の範囲とその内容を定めるにあたっては、基本的部分では鉄鋼ＥＤＩ標準に準拠しつつ、必要に応じて特有の規定を設けた。また、実際の運用にあたって考慮すべき箇所は当事者間の協議に委ねることにした部分も少なくない。これらは、各企業がインターネット導入にあたって必要となる検討項目を洗い出す際の参考としていただきたい。

【第9図】インターネットＥＤＩの推奨化項目の範囲

インターネット、ＶＰＮ、ＶＡＮなど

手動／自動化ツール等

プライベートメッセージ

ネットワーク契約など　　　　　　　　 　　　　（覚書、取り決め書の事例を掲載）

運用マニュアル　　　　　　　　　　　　　　　　（遵守項目と参考項目を制定）

取引基本契約

業務運用規約

情報表現規約

情報伝達規約

通 信 回 線

全銀協手順

（送受の運用手順を含む）

ＳＮＡ，

独自プロトコル

標準メッセージ

HTTP

FTP

SMTP

ＴＣＰ／ＩＰ

ＶＡＮ

標準データ項目、標準コード

今回の検討の対象

7－1．インターネットＥＤＩの推奨化項目

【第１２表】　インターネットＥＤＩの推奨化項目

|  |  |  |  |
| --- | --- | --- | --- |
|  | ファイル転送型・メール型ＥＤＩ | | Ｗｅｂ－ＥＤＩ |
| ＣＩＩﾄﾗﾝｽﾚｰﾀを使用するタイプ | ＣＩＩﾄﾗﾝｽﾚｰﾀを使用しないタイプ |
| データ項目・データコード | 鉄鋼ＥＤＩ標準に準拠する | 鉄鋼ＥＤＩ標準に準拠する | 鉄鋼ＥＤＩ標準に準拠する  （ダウンロード・アップロード用のデータも同様） |
| メッセージ | 鉄鋼ＥＤＩ標準準拠 | 基本的には鉄鋼ＥＤＩ標準に準拠するものとする＊。 | 基本的には鉄鋼ＥＤＩ標準に準拠するものとする＊。 |
| メッセージのデータ表現形式 | 鉄鋼ＥＤＩ標準準拠 | 当事者間の取り決めによる | 当事者間の取り決めによる  （ダウンロード・アップロード用のデータフォーマットも同様） |
| 画面表示および項目の表示レイアウト |  |  | 規定しない |
| 通信プロトコル | インターネット上の標準プロトコルを使用するものとする | | |
| 通信方式 |  | データの送受信頻度、取引の厳正度より、要求に応じた通信方式を採用するものとする。 | |
| 暗号化方式 |  | 送受信するデータの秘匿性より暗号化方式を双方の合意の下、決定することとする。 | |
| 標準機能 | 鉄鋼ＥＤＩ標準準拠 | 備えるのが望ましい・必須である機能 | 備えるのが望ましい・必須である機能 |

＊標準ＭＳＧの範囲内で予め運用する項目を当事者間で取り決めることも可

○データ項目・データコード

　使用するデータ項目・データコードは、Ｗｅｂ－ＥＤＩでダウンロード・アップロードに使用されるデータも含め、鉄鋼ＥＤＩ標準データ項目・標準コードに準拠するものとする。

○メッセージ

　鉄鋼インターネットＥＤＩで使用するメッセージの種類と名称は、原則として鉄鋼ＥＤＩ標準に定義されている標準メッセージに準拠するものとする。

　使用されない項目については、当事者間で運用項目を標準メッセージの範囲内で取り決めて、その取り決めた項目のみの運用もできる。

○メッセージのデータ表現形式

　ＣＩＩﾄﾗﾝｽﾚｰﾀを使用するファイル転送型・メール型ＥＤＩで使用するメッセージのデータ表現形式は鉄鋼ＥＤＩ標準に準拠するものとする。

　その他の型で使用するメッセージのデータ表現形式は、汎用的なCSV形式や固定長形式などを使用することを認め、具体的には当事者間で協議の上決定するものとする。Ｗｅｂ－ＥＤＩでダウンロード・アップデートに使用するデータの表現形式も同様である。

　なお、CSV形式については、以下の点について当事者で十分検討の上、フォーマットを取り決めることが望ましい。

CSV形式等を使用した場合のメッセージフォーマットについて当事者間で検討すべき事項の例

・ＢＰＩＤや情報区分コード等の表現方法。

・データ項目とデータの運用

　従来型のＥＤＩではデータが可変長であり、データタグとデータがセットで運用されるが、CSV形式を含めた固定長の場合はデータの並び順がデータの意味を表すことになる。このため、当事者間で予めデータの並び順などを合意しておく必要がある。

　また、Excel表をそのままCSV形式に変換して授受する場合などはデータ項目とデータをセットで運用するケースもあるものと想定される。

・文字コード、外字の取扱い

　必要に応じて使用する文字コードを決めること。外字は使用しないことが望ましいが、使用する場合は当事者間で協議すること。

・その他必要事項。

○画面表示および項目の表示レイアウト（Ｗｅｂ－ＥＤＩを対象）

　画面表示等については標準化の対象とはしない。

○通信プロトコル

　インターネット上の標準プロトコルを使用するものとする。

○標準機能

　標準機能として、０件データ、受信確認機能等が必要である。その実装については運用ルールを参照の上、当事者間で十分に協議して取り決めるものとする。

7－2．インターネットＥＤＩの運用ルールについて

インターネットＥＤＩの運用ルールについても基本的に鉄鋼ＥＤＩ標準に準拠すべきものであるが、従来型ＥＤＩとインターネットＥＤＩの利用環境の違いに応じて、特に以下の項目については、特別な運用ルールを設けることが望ましい。

7－2－1．標準企業コードの適用

　【Ｅメール型、Ｗｅｂ型、ＦＴＰ型】

　鉄鋼ＥＤＩ標準同様、その企業自身を示す企業コードとして、電子商取引推進センターが発番・管理する「標準企業コード」を用いるものとする。

7－2－2．読み出し不能データ

　【Ｅメール型、Ｗｅｂ型、ＦＴＰ型】

　伝送されたデータの読み出しができない場合、受信者はその事情を知った後直ちにその旨を相手方に通知するものとする。（その場合、発信者は当該のデータを撤回したものとみなす）

7－2－3．データ授受確認の取り決め

　【Ｅメール型、ＦＴＰ型】

　受信確認メッセージは原則としてこれを伝送するものとし、その方法の詳細については当事者間で協議の上、運用マニュアルに定めるものとする。

　【Ｗｅｂ型】

　情報提供サービス業務等の場合、Ｗｅｂ型の場合ログにより相手側のアクセス記録が残ることや参照の有無自体が問題とならないケースもあるため、特に取り決めの必要はないが、受発注業務等に使用する場合で厳密な受信確認が必要なケースでは、Ｗｅｂ上で未確認データと確認済データを明確に区分し、利用者が何らかのアクションをすることで（受信確認ボタンを押す、ファイルをダウンロードするなど）未確認から確認済に移行されるようなシステムを運用するなど、特別な運用ルールを当事者間で定めることができる。

7－2－4．データ未達時の扱い

　【Ｅメール型】

　データを送信した側は相応の時間内に受信確認メッセージがこない場合、あるいは受信確認メッセージにエラーがある場合はその旨相手方に通知する。

　データを受信する側は、データが到達しない場合、その事実を知った後直ちにその旨を相手方に通知する。発信者はこの通知を受け取った場合当該情報を再送もしくはファクシミリなどにより伝送する。

7－2－5．到達順序の逆転や二重送付

　【Ｅメール型、Ｗｅｂ型、ＦＴＰ型】

　運用マニュアルで、注文番号その他により重複チェック等を義務づけることが望ましい。

7－2－6．ゼロ件データの扱い

　【Ｅメール型、Ｗｅｂ型、ＦＴＰ型】

　稼働日にデータが発生しない場合の運用方法についてゼロ件データを送付するか否か、Ｗｅｂ型の場合はＷｅｂ上でゼロ件データをどのように表示するか否かを当事者間で事前に運用マニュアルで取り決める。

7－2－7．個別契約の成立（受発注業務が対象）

　受発注業務をインターネットＥＤＩで行う場合、どの時点で個別契約が成立するかを定めておく必要がある。本手引きでは産業情報化推進センターが発行している「ＥＣ法的問題調査研究報告書」を参考に、以下のケースを挙げたが、実運用にあたっては当事者同士で検討の上、覚書等で定めておく必要がある。

　【Ｅメール型】

　１．発注データに対する受信確認から一定時間の経過

　２．受注データ伝達時（＝承諾）（受注データに対する受信確認不要の場合）

　３．受注データに対する受信確認時

　４．履行時

　【Ｗｅｂ型】

　１．発注者によるＷｅｂ上への発注データ書き込みから一定時間の経過。（受注者の現実の閲覧を要しないが、受注者が読み出す義務を課することによって、発注データ書き込みからさほど時間が経過しないうちに、読み出されるという期待があることを前提とする）

　２．受注者によるＷｅｂ閲覧時

　３．受注者によるＷｅｂ閲覧から一定時間の経過

　４．受注者によるＷｅｂ上への受注データ書き込み

　５．履行時

　ＦＴＰ型も上記に準ずる。

7－2－8．責任範囲・責任分界点

　【Ｅメール型】

　当事者の責任範囲は、自身の使用するプロバイダのアクセスポイント（ﾒｰﾙﾎﾞｯｸｽを含む）までとする。

　・自社でメールサーバーを構える場合はプロバイダのアクセスポイントまで

　・プロバイダのメールサーバーを利用する場合はプロバイダのﾒｰﾙﾎﾞｯｸｽまで

　・プロバイダから先のいずれの管理内にも属さない領域についての責任はいずれも負わない。

【第10図】Ｅメール型の責任範囲



　【Ｗｅｂ型】

　当事者の責任範囲は、自身の使用するプロバイダのアクセスポイント（Ｗｅｂサーバを含む）までとする。

　・自社でＷｅｂサーバを構える場合はプロバイダのアクセスポイントまで

　・プロバイダのＷｅｂサーバを利用する場合はプロバイダのＷｅｂサーバまで

　・プロバイダから先のいずれの管理内にも属さない領域についての責任はいずれも負わない。

【第11図】Ｗｅｂ型の責任範囲（自前でＷｅｂサーバを構える場合）



【第12図】Ｗｅｂ型の責任範囲（プロバイダのＷｅｂサーバを利用する場合）



　【ＦＴＰ型】

　当事者の責任範囲は、自身の使用するプロバイダのアクセスポイント（ＦＴＰサーバを含む）までとする。

　・自社でＦＴＰサーバを構える場合はプロバイダのアクセスポイントまで

　・プロバイダのＦＴＰサーバを利用する場合はプロバイダのＦＴＰサーバまで

　・プロバイダから先のいずれの管理内にも属さない領域についての責任はいずれも負わない。

【第13図】ＦＴＰ型の責任範囲（自社でFTPサーバを構える場合）



0

【第14図】ＦＴＰ型の責任範囲（プロバイダのFTPサーバを使用する場合）



7－2－9．運用スケジュール

　【Ｗｅｂ型】

　３６５日２４時間稼働の機能を実現できることが望ましい。都合上やむを得ず稼働を停止する場合は、事前にスケジュール連絡を行うものとする。その他の詳細は運用マニュアルにおいて取り決める。

7－2－10．メッセージの保存

　【Ｅメール型】

　当事者はデータを保存するものとし、相手方の請求がある場合は、これを相手方に交付しなければならない（費用は請求者負担）。

　データ保存期間等の細目は当事者間で協議の上、運用マニュアルで定める。

　【Ｗｅｂ型・ＦＴＰ型】

　ホームページの設定者もしくはＦＴＰサーバの設定者はホームページサーバ、ＦＴＰサーバの改訂歴、全てのアクセス記録にかかるデータを保存するものとし、相手方の請求がある場合は、これを相手方に交付しなければならない（費用は請求者負担）。

　データ保存期間等の細目は当事者が協議し決めることとし、運用マニュアルに定める。

7－2－11．ファイル名

　【Ｅメール型、Ｗｅｂ型、ＦＴＰ型】

　ファイル名は運用するシステムの必要に応じて、当事者同士で協議の上、運用マニュアルにおいて定めるものとする。

7－2－12．メールのアドレス、容量、サブジェクト名、データの分割・圧縮等

　【Ｅメール型】

　メールアドレスは送受信側ともＥＤＩ取引専用のアドレスを取得し運用することが望ましい。

　伝送する最大データ容量は当事者のシステム環境に依存するため、協議の上、運用マニュアルにおいて定めるものとする。

　サブジェクト名、データの分割・圧縮等についても当事者同士で協議の上、運用マニュアルにおいて定めるものとする。

7－2－13．その他の付帯業務機能

　【Ｗｅｂ型】

　法制上において書面または電子データの交付・保存が義務づけられている場合は、対象データについてCSV形式などによるデータダウンロード機能、帳簿帳票出力機能、伝票発行機能等を設けておくことが望ましい。

|  |  |  |  |
| --- | --- | --- | --- |
|  | Ｅメール型 | Ｗｅｂ型 | ＦＴＰ型 |
| 標準企業コードの  適用 | 鉄鋼ＥＤＩ標準に準拠し、「標準企業コード」を用いるものとする。 | | |
| 読み出し不能データ | 伝送されたデータの読み出しができない場合、受信者はその事情を知った後直ちにその旨を相手方に通知する。（その場合、発信者は当該のデータを撤回したものとみなす） | | |
| データ授受確認の  取り決め | 受信確認メッセージはこれを伝送する。 | ログに残るアクセス記録　or  使用者による明確なアクションを必要とする。 | 受信確認メッセージはこれを伝送する。 |
| データ未達時の扱い | 送信側は一定時間の内に受信確認メッセージがこない場合はその旨通知する。  受信側はデータが到達しない事実を知った後、直ちに通知し、発信者は再送する。 |  |  |
| 到達順序の逆転や二重送付 | 運用マニュアルで、注文番号その他により重複チェック等を義務づける。 | | |
| ゼロ件データの扱い | 稼働日にデータが発生しない場合の運用方法についてゼロ件データを送付するか否か、Ｗｅｂ型の場合はＷｅｂ上でどのように表示するか否かを当事者間で運用マニュアルに取り決める。 | | |
| 個別契約の成立  （受発注業務を対象） | 発注データに対する受信確認から一定時間の経過 | 発注データの書き込みから一定時間の経過後  一定期間毎に受注者が読み出す義務を課す | |
| 責任範囲・責任分界点 | 自身の使用するプロバイダのアクセスポイント（ﾒｰﾙﾎﾞｯｸｽ、Ｗｅｂサーバ、ＦＴＰサーバを含む）まで | | |
| 運用スケジュール | 鉄鋼ＥＤＩ標準に準拠し、詳細は運用マニュアルで定める。 | ３６５日２４時間が望ましい。詳細は運用マニュアルで定める。 | 鉄鋼ＥＤＩ標準に準拠し、詳細は運用マニュアルで定める。 |
| メッセージの保存 | 当事者はデータを保存するものとし、請求がある場合はこれを交付する。（費用は請求者負担）。 | ホームページの設定者は改訂履歴、全てのアクセス記録を保存し、請求がある場合はこれを交付する。（費用は請求者負担） | ＦＴＰサーバの設定者は全ての履歴、アクセス記録を保存し、請求がある場合はこれを交付する。（費用は請求者負担） |
| ファイル名 | 詳細は運用マニュアルで定める。 | | |
| メールのアドレス、  容量、サブジェクト名、データの分割・圧縮 | アドレスは専用のものを用意することが望ましい。  サブジェクト名は情報区分コードとする。  伝送する最大データ容量、データの分割・圧縮等については運用マニュアルで定める。 |  |  |
| セキュリティ | クライアントPCにはウィルスチェックツールを導入。  ユーザ管理（承認されたユーザの登録）と、認証管理（ID,PW）を必要に応じて実施すること。 | | |
| その他の付帯業務 |  | 法制上において書面または電子データの交付・保存が義務づけられている場合は、対象データについてCSV形式などによるデータダウンロード機能、帳簿帳票出力機能等を設けておくことが望ましい。 |  |

【第13表】インターネットＥＤＩ運用ルールのまとめ

7－3．インターネットＥＤＩ契約書例

7－3－1．Ｅメール型

　Ｅメール型インターネットＥＤＩを用いてデータ交換を行う場合に取り交わす覚書の内容事例を以下に示す。

**企業間データ交換に関する覚書**

平成　　年　　月　　日

Ａ　　株式会社

Ｂ　　株式会社

　Ａ株式会社（以下「甲」という）とＢ株式会社（以下「乙」という）とは、甲乙間のデータ交換に関し、次の通り覚書を締結する。

**第１条 目的**

本覚書は、甲乙間の鋼材取引業務を円滑かつ合理的に運営する為に締結するものとし、両者は誠意をもってこれを履行する。

**第２条 適用範囲**

本覚書は、甲乙間の鋼材取引に関連して、甲乙間で行われる鋼材取引情報のコンピュータおよびそれに接続されたネットワークを利用した電子データ交換に適用する。

**第３条 用語の定義**

本覚書において用いられる以下の語は、文脈上、別段の断りがない場合には、それぞれ次の意味で用いられるものとする。

１．ﾒｰﾙﾎﾞｯｸｽ

データの発信者が、相手方に取引関係情報を提供するため、当該取引関係情報を記憶させて､当該相手方に受信可能ならしめる、当該相手方が指定したインターネット上のＥメールアドレスによって表示されるメールサーバー上の電子ファイルをいう。

２．受信確認

甲の発注データが乙のﾒｰﾙﾎﾞｯｸｽに書き込まれた旨のみを内容とする通知をいう。ただし、受信確認なしに乙の受諾の通知がなされた場合には、その受諾をもって受信確認と見なす。

その他、必要に応じて、伝送、伝達、受信、発信、電子署名、認証、暗号等の用語について適宜、定義する。

**第４条 運用マニュアル**

1. データ交換の実施に必要なシステム、送信手順、メッセージ構成、伝達するデータの種類、システムの稼働時間その他の細目は、甲乙間で別に定めるデータ交換運用マニュアル（以下「運用マニュアル」という）で定める｡
2. 甲および乙は、運用マニュアルがこの覚書と一体をなし、この覚書と同一の効力を有することを相互に確認する｡
3. システムの変更その他の事由により運用マニュアルを変更する必要が生じた場合には、必要に応じ、甲乙間で協議を行い変更する｡

**第５条 費用負担**

本覚書に定めるデータ交換の運用に伴う費用の負担は別に定めるとおりとする。

**第６条 データ交換の安全および信頼確保のための手順**

甲および乙は、データ交換の安全確保のため下記各号の全部またはいずれかの手順を実施するものとし、その実施の手順の内容は運用マニュアルに定めることに合意する｡

（１） 発信者の同一性の確認手順

（２） 発信者の作成権限の確認手順

（３） データ入力誤りの確認手順

（４） 伝送途上におけるデータ変質の確認手順

（５） その他甲および乙が合意する事項

**第７条 データの伝達**

データの伝達は、運用マニュアルに定める方法により、相手方のﾒｰﾙﾎﾞｯｸｽに書き込むことにより行う。

**第８条 読み出し不能データの取扱い**

伝達されたデータの読み出しができない場合の受信者は、これらの事情を知った後、直ちに、相手方に対してその旨を＿＿＿＿＿＿により通知する。

**第９条 受信確認**

* + - 1. 乙は、甲の伝達にかかる発注データの受信確認をなすものとする。この受信確認の方法は、特段の指定のない限り＿＿＿＿＿＿の方法によるものとする。
      2. 前項の受信確認を受領した場合、当該発注データの伝達は完了したものとみなし、その受領がない場合には伝達がなかったものとみなす。

**第10条 データの確定**

甲および乙は、伝達されたデータが第４条各号に定める安全確保のための手順にしたがって作成・伝達された場合には、それぞれ確認された事項につき受信データの内容が確定することに合意する｡

以下の２条文は基本的な取引契約書が別にある場合に適用する

**第11条 個別契約の成立**

「６－２－７．個別契約の成立」を参照の上、当事者間で協議・決定した内容を記述する。

**第12条 個別契約の変更**

個別契約の内容を変更する必要が生じた場合は、乙は甲に書面又はそれに変わるものをもって変更を依頼する。変更の結果は本システムを通じ甲から乙に報告を行う。

**第13条 システムの管理**

甲および乙は、データ交換が円滑かつ安全に実施されるようそれぞれのシステムを管理するものとする。

**第14条 本システム障害時の措置**

1. コンピュータのハード・ソフト、通信回線の故障又はその他の理由により、本システムに障害が発生した場合の対応については、運用マニュアルに定めるところによる。
2. 障害等に基づく損害については、甲乙のうち、当該障害の発生について責任の有する側が負担し、その負担金額および負担方法は両者協議の上、決定する。

**第15条 データの保存および交付**

* 1. 甲および乙は、それぞれの発信にかかるデータおよび受信にかかるデータを保存するものとし、相手方の請求がある場合には、これを相手方に交付しなければならない。ただし、プリントアウト・複製その他によりこの交付に費用が発生する場合には、その費用は請求者の負担とする｡
  2. 保存および交付の細目に関しては運用マニュアルに定める｡

**第16条 記憶内容の改竄禁止**

１． 甲および乙は、本システムにおいて、ﾒｰﾙﾎﾞｯｸｽに記録された取引関係情報の内容を改ざんしてはならない。

２． 前項の規定は、ﾒｰﾙﾎﾞｯｸｽに記録された取引関係情報を受信した後も同様とする。

**第17条 秘密保持**

甲および乙は、本覚書に基づくデータ交換の実施により知りえた相手方の情報を、その有効期間中はもとより完了後といえども秘密に保持するものとし、本来の目的以外に使用してはならない。

**第18条 協議事項**

本覚書および個別契約に定めのない事項については、原契約による。又いずれの契約にも定めがない事項について疑義が生じた場合は、その都度甲乙協議の上解決するものとする。

**第19条 覚書内容の変更**

当覚書内容に変更が生じた場合、甲乙にて協議を行い、両者合意の基に変更するものとする。

**第20条 紛争処理**

甲および乙は、本覚書に関連して訴訟の要が生じた場合には、＿＿＿＿＿＿裁判所を第一審の専属合意管轄裁判所とする。ただし管轄裁判所を定めないときは、民事訴訟法の定めによる。

**第21条 有効期間**

本覚書の有効期間は、取り決めの日より＿＿年間とする。但し、期間満了の＿＿カ月前までに甲乙いずれか一方から相手方に対し書面による解除の申し入れがないときは、同一条件をもって更に＿＿年間延長されるものとし、以後も同様とする。

本覚書の成立を証するため、本書２通を作成し、甲乙記名捺印の上、甲乙各１通を保有する。

平成　　年　　月　　日

甲 Ａ株式会社 印

乙 Ｂ株式会社 印

7－3－2．Ｗｅｂ型

　Ｗｅｂ型インターネットＥＤＩを用いてデータ交換を行う場合に取り交わす覚書の内容事例を以下に示す。

**企業間データ交換に関する覚書**

平成　　年　　月　　日

Ａ　　株式会社

Ｂ　　株式会社

　Ａ株式会社（以下「甲」という）とＢ株式会社（以下「乙」という）とは、甲乙間のデータ交換に関し、次の通り覚書を締結した。

**第１条 目的**

本覚書は、甲乙間の鋼材取引業務を円滑かつ合理的に運営する為に締結するものとし、両者は誠意をもってこれを履行する。

**第２条 適用範囲**

本覚書は、甲乙間の鋼材取引に関連して、甲乙間で行われる鋼材取引情報のコンピュータおよびそれに接続されたネットワークを利用した電子データ交換に適用する。

**第３条 用語の定義**

本覚書において用いられる以下の語は、文脈上、別段の断りがない場合には、それぞれ次の意味で用いられるものとする。

必要に応じて、伝送、伝達、受信、発信、受信確認、電子署名、認証、暗号等の用語について適宜、定義する。

**第４条 運用マニュアル**

1. データ交換の実施に必要なシステム、送信手順、メッセージ構成、伝達するデータの種類、システムの稼働時間その他の細目は、甲乙間で別に定めるデータ交換運用マニュアル（以下「運用マニュアル」という）で定める｡
2. 甲および乙は、運用マニュアルがこの覚書と一体をなし、この覚書と同一の効力を有することを相互に確認する｡
3. システムの変更その他の事由により運用マニュアルを変更する必要が生じた場合には、必要に応じ、甲乙間で協議を行い変更する｡

**第５条 費用負担**

この協定に定めるデータ交換の運用に伴う費用の負担は別に定めるとおりとする。

**第６条 データ交換の安全および信頼確保のための手順**

甲および乙は、データ交換の安全確保のため下記各号の全部またはいずれかの手順を実施するものとし、その実施の手順の内容は運用マニュアルに定めることに合意する｡

（１） 発信者の同一性の確認手順

（２） 発信者の作成権限の確認点順

（３） データ入力誤りの確認手順

（４） 伝送途上におけるデータ変質の確認手順

（５） その他甲および乙が合意する事項

**第７条 データの伝達**

データの伝達は、運用マニュアルに定める方法により、甲乙の合意したシステム上に書き込むことにより完了したものとみなす。

**第８条 読み出し不能データの取扱い**

伝達されたデータの読み出しができない場合データの受信者は、これらの事情を知った後、直ちに、相手方に対してその旨を＿＿＿＿＿により通知する｡

**第９条 データの確定**

甲および乙は、伝達されたデータが第４条各号に定める安全確保のための手順にしたがって作成・伝達された場合には、それぞれ確認された事項につき受信データの内容が確定することに合意する｡

以下の２条文は基本的な取引契約書が別にある場合に適用する

**第10条 個別契約の成立**

「６－２－７．個別契約の成立」を参照の上、当事者間で協議・決定した内容を記述する。

**第11条 個別契約の変更**

個別契約の内容を変更する必要が生じた場合は、乙は甲に書面又はそれに変わるものをもって変更を依頼する。変更の結果は本システムを通じ甲から乙に報告を行う。

**第12条 システムの管理**

甲および乙は、データ交換が円滑かつ安全に実施されるようそれぞれのシステムを管理するものとする。

**第13条 本システム障害時の措置**

1. コンピュータのハード・ソフト、通信回線の故障又はその他の理由により、本システムに障害が発生した場合の対応については、運用マニュアルに定めるところによる。
2. 障害等に基づく損害については、甲乙のうち、当該障害の発生について責任の有する側が負担し、その負担金額および負担方法は両者協議の上、決定する。

**第14条 データの保存および交付**

* + - 1. ホームページの設定者は、ホームページの改訂履歴、および全てのアクセス記録にかかるデータを保存するものとし、相手方の請求がある場合には、これを相手方に交付しなければならない。但し、プリントアウト、複製その他によりこの交付に費用が発生する場合には、その費用は請求者の負担とする。
      2. 保存および交付の細目に関しては運用マニュアルに定める｡

**第15条 記憶内容の改竄禁止**

１． 甲および乙は、本システムにおいて、ホームページに記録された取引関係情報の内容を改ざんしてはならない。

２． 前項の規定は、ホームページに記録された取引関係情報を受信した後も同様とする。

**第16条 秘密保持**

甲および乙は、本覚書に基づくデータ交換の実施により知りえた相手方の情報を、その有効期間中はもとより完了後といえども秘密に保持するものとし、本来の目的以外に使用してはならない。

**第17条 協議事項**

本覚書および個別契約に定めのない事項については、原契約による。又いずれの契約にも定めがない事項について疑義が生じた場合は、その都度甲乙協議の上解決するものとする。

**第18条 覚書内容の変更**

当覚書内容に変更が生じた場合、甲乙にて協議を行い、両者合意の基に変更するものとする。

**第19条 紛争処理**

甲および乙は、本覚書に関連して訴訟の要が生じた場合には、＿＿＿＿＿＿裁判所を第一審の専属合意管轄裁判所とする。ただし管轄裁判所を定めないときは、民事訴訟法の定めによる。

**第20条 有効期間**

本覚書の有効期間は、取り決めの日より＿＿年間とする。但し、期間満了の＿＿カ月前までに甲乙いずれか一方から相手方に対し書面による解除の申し入れがないときは、同一条件をもって更に＿＿年間延長されるものとし、以後も同様とする。

本覚書の成立を証するため、本書２通を作成し、甲乙記名捺印の上、甲乙各１通を保有する。

平成　　年　　月　　日

甲 Ａ株式会社 印

乙 Ｂ株式会社 印

7－4．運用マニュアルの内容

運用マニュアルで取り決めるべき内容について一例を挙げる。

（産業情報化推進センター発行「ＥＣ法的問題調査研究報告書」より一部を修正のうえ引用）

１．（協定書および）運用マニュアル上使用する用語の定義

２．システムの内容

２－１．システムの適用範囲

２－２．システム概念図およびシステム構成

３．運用手順

３－１．伝送するデータの種類

３－２．伝達するデータの内容

３－３．伝達方法

通信プロトコル、接続形態、通信回線種別、通信手順等

３－４．運用日時

運用日、時間

時間外に受領したデータの取扱い

受注データ伝達までの期間、返送がなかった場合の効果

データの重複チェック

ゼロ件データ

３－５．読み出し不能データの取扱い

通知方法、通知がなかった場合の当該データの効力）

３－６．受信確認

受信確認が必要な場合の方法、受信確認受信までの期間

３－７．データの保存

保存する主体、データの範囲、期間、態様

４．安全対策

４－１．システムの管理

システム管理および保守の方法、責任範囲、相手方への連絡方法、

管理責任者、管理責任者変更の連絡方法

４－２．安全確保のための手順

①発信者の同一性の確認手順

認証（ID、パスワード）、電子署名、暗号化等

②発信者の作成権限の確認手順

電子署名等

③データ入力誤りの確認手段

④伝送途上におけるデータ変質の確認手段

パリティチェック、暗号化等

⑤その他の手段

４－３．異常発生時の措置

異常発見時の報告義務・報告体制

主任担当者の氏名、連絡先および連絡方法

休業時の連絡方法（通常時の運用、管理等の担当者と同じとは限らない）

予想される障害と対処方法

責任分担

代替的な情報伝達方法（電話、ＦＡＸ、郵便、手渡し等）

緊急用設備の設置方法、さらには応急措置

原因究明および回復のための見通し、措置、報告

（コモンキャリア、ハードメーカー等第三者との連絡、協調の体制）

既処理データの点検

損害の拡大を防ぐための一般的な協力義務および拡大損害についての賠償責任の定め

５．費用負担

５－１．原則

５－２．イニシアルコスト、ランニングコスト、その他

６．運用マニュアル変更の方法

（変更履歴の記録）