8－I002

ＥＣ法的問題調査研究報告書

―新しい企業間電子データ交換についての検討―

平成９年３月

財団法人　日本情報処理開発協会

産業情報化推進センター

KEIRIN
この資料は、競輪の補助金を受けて作成したものです。

はじめに

我が国の産業界における情報化は、企業内利用にとどまらず産業間を横断的に網羅した企業間ネットワークの利用へと急速に拡大・進展するのに伴い、業界、業際にまたがる企業間において、これまでの書類を中心とした取引形態からネットワークを利用したＥＤＩ（電子データ交換）への動きが活発化し、ＥＤＩは、企業系列を越え、業種を越え、そして国境を越えてグローバルに自由に展開されようとしている。最近ではオープンなコンピュータネットワークを用いた電子商取引（ＥＣ：Electronic Commerce）が注目されており、廉価な設備投資で利用出来ることから、対消費者だけでなく企業間での利用も検討され始めている。

ＥＤＩを円滑に推進するに当たっては、通信プロトコル、ビジネスプロトコル等の各種取り決めについての標準化やルール化が必要不可欠であるとともに、法的諸問題への対処を検討、整備する必要がある。

当センターでは、昭和63年度以来、法律の専門家および企業等の実務家による「電子取引調査研究委員会」を設けて、主に法的側面から電子取引の実態把握と問題の分析、対策等の検討を行ってきた。その検討結果は、主に受発注業務を対象として、ＥＤＩにおける取引契約を締結する場合に留意すべき基本的な事項や参考となる契約文例などを示し、紙ベースの取引とＥＤＩによる取引の相違点について検討し、平成７年度にその成果を「データ交換協定書（参考試案）」としてとりまとめた。

本年度は、今まで対象としてきた受払処理から物流、請求支払業務まで対象業務範囲を広げて法的問題の検討を行う一方、インターネット上でＥＤＩを行なう場合の法的課題およびオープン業務形態の１例としてＣＡＬＳにおける法的課題を検討し、「新しい企業間電子データ交換についての検討」としてとりまとめた。

この報告書が、わが国ＥＤＩの更なる発展に寄与すれば幸いである。

最後に、本調査研究の実施にあたってご協力を頂いた委員をはじめ、関係各位に対し、深く感謝の意を表する。

平成９年３月

財団法人　日本情報処理開発協会
産業情報化推進センター

平成８年度　ＥＣ法的問題調査研究委員会名簿

委員長	堀部政男	一橋大学　法学部	教　授
委　員	上濱隆一	（財）日本貿易関係手続簡易化協会	常務理事
〃	大野幸夫	新潟大学　法学部	教　授
〃	小野耕三	（財）流通システム開発センター	常務理事
〃	曽野和明	北海道大学　法学部	教　授
〃	種部信夫	日本電子機械工業会ＥＤＩセンター	事務局長
〃	永田眞三郎	関西大学　法学部	教　授
〃	中原志郎	日本電信電話（株）　法務考査部	法務部門長
〃	西田哲也	（財）金融情報システムセンター 調査企画部	部　長
〃	野村豊弘	学習院大学　法学部	教　授
〃	舟田正之	立教大学　法学部	教　授
〃	本田八郎	日本通運(株)情報システム部 物流システムグループ	担当部長
〃	松尾　明	中央監査法人　システム監査部	公認会計士
〃	松本恒雄	一橋大学　法学部	教　授
〃	室町正実	東京丸の内法律事務所	弁護士
〃	村上統英	住友化学工業（株）情報システム室	主席スタッフ

平成８年度　ＥＣ法的問題調査研究作業部会名簿

主　査	野村豊弘	学習院大学　法学部	教　授
委　員	大野幸夫	新潟大学　法学部	教　授
〃	小川憲久	紀尾井坂法律特許事務所	弁護士
〃	加藤貞晴	加藤法律特許事務所	弁護士
〃	筒井邦恵	（株）日本総合研究所　法務部	
〃	永田眞三郎	関西大学　法学部	教　授
〃	室町正実	東京丸の内法律事務所	弁護士

目　次

Ⅰ．本　　論

1．概　　説

1．概　　説

（執筆担当：野村豊弘）

1.1　EDI から EC （電子商取引）への進展

(1) EC／CALS の意義

EDI（Electronic Data Interchange ）ということばは、そのまま翻訳すれば、「電子的なデータ交換」である。すなわち、通信回線を通じてコンピュータ（端末）を利用してデータの交換を行うことをを意味するものである。しかし、このことばは必ずしも電子的データ交換を意味するものとしてのみ用いられてきたとはいえないように思われる。たとえば、財団法人日本情報開発処理協会・産業情報化推進センターが国内標準として定めている CII 標準では、「異なる企業間において商取引のためのデータを通信回線を解してコンピュータ（端末を含む）間で交換すること、その際当事者間で必要となる各種の取り決めが可能な限り広く合意された標準的な規約であること」とされている。このような EDI の定義に従って、本調査研究委員会の前身である電子取引調査研究委員会では、「企業間の電子取引システム」を意味するものとして EDI ということばを用いてきた(1)。このように、EDI ということばの中に取引概念を含めてきたのである。もっとも、ことばの本来的な意味である「電子的なデータ交換」の意味に EDI ということばを用いることもないわけではなかった。すなわち、電子取引調査研究委員会による平成 8 年度の報告書では、EDI を電子的データ交換の意味に用いている(2)。

そして、EDI ということばがようやく多くの人によって知られるようになったのであるが、ここ 2、3 年前から EC あるいは CALS ということばが用いられるようになってきた。EC というのは、《Electronic Commerce 》の略語であるが、電子商取引と訳されている。電子ネットワーク上の商取引を意味するものとして用いられている。また、CALS については、そのもととなることばがややはっきりしていない。本来、《Computer-aided Acquisition and Logistic Support 》の略語として用いられていたが、その後、CALS に《Continuous

Acquisition and Life-cycle Support》の語があてはめられるようになったということである。前者は、「コンピュータによる調達と戦略の支援」と訳され、後者は、「継続的な調達とライフサイクルの支援」と訳される。いずれにせよ、「企業の調達活動を支援する情報システム」を意味するものである(3)。

(2) EDI と EC／CALS の比較

EC および CALS については、それぞれ別稿において詳細に論じられるが、ここでは、EDI と EC／CALS への進展によって商取引に関する情報交換の状況がどのように変化するのかについて考察する。

従来、EDI においては、専用回線あるいは公衆回線を介して特定の当事者間において予め定められた基本契約およびデータ交換協定の内容に従ってデータ交換を行うことを想定していた。すなわち、特定の企業間における閉鎖された商取引システムである。これに対して、EC／CALS においては、オープン化された取引システムを想定している。ここで、オープン化というのは、かなり多義的に用いられている。まず第一に、取引当事者の範囲が拡大し、企業間取引から消費者取引へと変化した。すなわち、EDI では、企業対企業の取引を対象としていたのに、EC／CALS では、企業対企業の取引のみならず、企業対消費者の取引をもその対象とするに至ったのである。そして第二に、これに伴って、取引の相手方の範囲も、EDI では特定されていたのに、EC／CALS では不特定多数を対象とするものとなったのである。すなわち、事前に基本契約による合意のない当事者間において電子的なデータ交換が行われ、それによって個別的な取引契約が成立することが考えられている。第三に、取引の地域も拡大し、EDI では主として国内取引が考えられていたのに対して、EC／CALS では国境を越える国際取引をも含むものと考えられるようになった。第四に、EDI では取引に伴う決済方法について別に考えられていたが、EC／CALS では電子決済（EFT）を組み込んだ事務処理が考えられている。第五に、EDI では主として専用回線によるネットワークの構築によるものであったが、EC／CALS ではインターネットを積極的に利用することが考えられている。

このように、EC／CALS は、情報通信技術の発展を利用して、EDIによる取引をいろいろな意味において拡大するものであるといえよう。

1.2 EC／CALS への進展と法的な問題点

このような EC／CALS への進展がもたらす法的な問題点について概観する（それぞれの詳細については後に述べられる）。

(1) オープン化

まず、取引システムのオープン化がもたらす法的な問題点として、取引の当事者が限定されないために生ずる危険が存在する。すなわち、相手方の資力に対する不安が生ずる場合がある。従来の EDI では閉鎖された取引システムであるから未知の相手方と取引することは考えられないが、オープン化するとそのような場合が出てくる。とくに、取引当事者が必ずしも自己の同一性を明らかにすることなしに（匿名）取引することを可能にする場合にこのような問題が生じやすい。また、詐欺などの背信的な取引、反倫理的な取引などを生ずる可能性も否定できない。

(2) 情報基盤の脆弱性

次に、EC／CALS においては、基盤となるネットワークとしてインターネットが重要な役割を果たすものと考えられているが、情報基盤としての脆弱性に対する危惧が指摘されている。具体的には、通信されるデータを他人に知られることによるプライバシーの侵害、クレジットカードの番号を他人に知られる場合のような決済手段の盗用、知的財産権の侵害、システムの事故・障害などがあげられている。これらは従来からネットワークの安全性として論じられてきた問題点であって、とくに目新しいものではないが、広範な利用が想定されているインターネットの法的な性格（法的な責任主体としての資格を有するか）が不明確であるだけに、これらの問題は重要である。

1.3 報告書の構成

本報告書では、これまでの調査研究の経緯を踏まえ、一方で EDI からEC／CALS への進展に伴う法的な問題を考察し、他方で業際 EDI の法的問題を検討することとした。前者は、情報通信技術の進展に伴い、EDI からEC／CALS へと発

展していく現象に対して法的考察をしようとするものである。具体的には、電子商取引、インターネットを利用したEDI、CALSの三つのテーマを取り上げている。いずれもこれからどのように展開していくか必ずしも予測できないが、将来の進展を視野に入れながら、法的な問題点を検討するものである。これに対して、後者は、これまで検討してきたEDIの実務における応用について考察するものである。具体的には、物流EDIと決済EDIを取り上げている。いずれも、実際にある程度行われているものではあって、発展途上にあるとはいえ、EC／CALSとは多少異なった側面を有している。

(注) (1) 日本情報処理開発協会・産業情報化推進センター『電子取引契約条項作成のポイントーＥＤＩにおける法律問題の検討－』（平成５年３月）11頁。

(2) 日本情報処理開発協会・産業情報化推進センター『ＥＤＩ法律問題調査研究報告書－ＥＤＩに関する標準契約の検討－』（平成８年３月）
なお、EDIの定義については、野村豊弘「ＥＤＩによる取引の法的諸問題」ＮＢＬ５４９号１８頁以下参照。

(3) 石黒憲彦・奥田耕士『ＣＡＬＳ　米国情報ネットワークの脅威』９頁以下参照。　なお、最近では、CALSに、《Commerce at Light Speed》（光速の商取引）という表現をあてはめることもあるようである。

2．　EDIからEC／CALSへ

2　EDI から EC／CALS

2.1　電子商取引

（執筆担当：室町正実）

2.1.1　電子商取引の検討課題の変化

「電子商取引（Electronic Commerce）」という用語はここ数年間で一般的にも普及した。そして、電子商取引の普及のためには、インフラストラクチャーとしての法制度の検討が重要であることは、国際的に見てもほぼ定着し、わが国においても、このような検討は徐々にではあるが進行しつつある。

電子商取引に関する契約・法律上の問題は、継続的取引関係にある企業間おける受発注データ交換、いわば閉鎖的な環境下における諸問題の検討を経て、近時では認証や電子公証などいわゆるオープンな環境をも視野に入れた諸問題の検討が行われている。このような検討が電子商取引の健全な発展のために必要な検討であることは大方、共通の理解となっているといえる。海外の検討の状況を検討すると、この検討は、

(イ) 電子商取引、しかも、徐々にではあるが類型化しうる個別の電子商取引ごとの特性やこれに関連する法律問題をはっきりさせ、

(ロ) それに対して現行の法制度のうえでの支障（legal obstacles）があるかどうか、

(ハ) その電子商取引の安全性や信頼性を高めるためにはどのような新しい社会的基盤としての法制度の対応が必要か、

を検討することが重要であるという認識のもとに行われているように思われる。

本報告で後にふれるように（永田論文）、「電子商取引」の実用化は、急速に、かつ、予想することが困難な利用のされ方をもって進展しつつあり、特に、インターネットの爆発的な普及に伴い、「オープン」な「電子商取引」に関する問題の検討の必要性が強く指摘されている。しかしながら、上記の（イ）、（ロ）、（ハ）の検討を視野に入れれば、「オープン」や「電子商取引」をどのように把握するべき

かを検討することも必ずしも無用のこととはいえず、むしろ、どちらかといえば必ずしも共通の認識のない「オープン」な「電子商取引」についてある程度の整理を行うべき時期にあるようにも思える。そこで、本節においては、この報告に必要な範囲において、「オープン」な「電子商取引」の整理を行うこととする。

2.1.2 電子商取引の整理

(1) 電子商取引の範疇

電子商取引という用語は極めて多義的に使用される。企業間のネットワーク（電子通信手段）とコンピューターを利用した契約（注）の締結が含電子商取引の範疇に属することはほぼ疑いがないが、

＊消費者が関与する取引を含む用語なのか、

＊契約の締結、法律的用語に従えば、「契約の成立」に必要な意思表示以外の電子的情報の交換を含む用語であるのか、

＊電子的情報による金銭債務の弁済を含むのか（いわゆる「電子決済」である。なお、わが国においては、弁済は準法律行為である。しかし、いわゆる「電子マネー」による弁済は、採用される方式にもよろうが、必ずしも準法律行為にとどまらない場合もあろう。）、

＊例えば、デジタル・コンテンツの交付方法のみに通信手段が用いられたり、デジタル・コンテンツの制限解除のために用いる「鍵」の配送のみに電子的情報が用いられる場合を含むか、

などについては実は明確な共通の認識があるわけではない。

「電子商取引に関する法律的問題」を検討するといっても、それが契約の成立に関する問題なのか、弁済に関する問題なのかなどにより、法律的検討課題は大きく異なる。現実のネットワークにおいて、上述のごときさまざまな電子的情報の交換が取引のために行われている現状からすれば、当該の電子的情報交換のもつ目的・機能に応じた法律的検討を行うべき必要があろう。

(2) 電子商取引の範疇の再検討

こうした観点から、電子取引について、最も広い意味でその範囲を考えれば、「コンピュータと通信ネットワークを利用する取引」ということになろう。ただ、

このような意味で電子商取引の範囲を検討すると、鉄道会社、航空会社の窓口で行われている指定券の発券業務や銀行におけるATMやCDを利用した預金の払戻などもこの範疇に入ることになる。

しかしながら、これらの「取引」を現在議論されている「電子商取引」の範疇に含めることには、いささかの躊躇を覚える。なぜならば、指定券の発券業務については、いわゆるホームリザーベーションと異なり、購入者自らがコンピュータを操作することはなく、ATMやCDを利用した取引においては、預金者自らが端末を操作するものの、その端末自体や通信回線を自らが占有管理するわけではないし、データの伝送も、現実的には、提携銀行を含む銀行の内部間で行われており、ホームバンキングやファームバンキングとは異なるものと理解しうるからである。

こうした観点や現在ネットワークを経由して伝達されている取引のための電子的情報の実情を考慮すれば、現在議論されている「電子商取引」の範疇を広い意味において整理するとしても、とりあえず、電子的情報の作成者・発信者が、自ら占有管理するコンピュータ、端末等を利用して電子的情報を作成することを前提として、「取引当事者間または取引の潜在的当事者の間で、契約締結に必要な情報、契約成立に関する情報、契約の履行に必要な情報や履行状況に関する情報、契約の履行そのものまたは弁済・これに準ずる行為に関する情報の全部または一部が通信手段を用いた電子的情報の伝達によって行われる取引行為」という位置づけを与えることも一応は可能であろう。

(3) 具体的な事例と範疇

電子商取引にかかる位置づけを与えた場合には、例えば、（商）取引それ自体は紙ベースで行うが、その前提として必要な行政手続き上の申請行為を電子的情報の授受によって行う場合は、その電子的情報の授受が取引の当事者間や潜在的当事者間で行われないから、これを電子商取引と位置づけることにはならない（もっとも、かかる問題を含めて電子商取引の問題を考慮する必要性がないとはいえない）。また、クレジットカードのペーパーベースでの利用の場合に、CAT端末を利用したオーソライゼーションが行われて場合も、クレジットカード保有者と加盟店においては、電子的情報の交換は行われていないから、この間

の取引は電子商取引の範疇には属さないことになる。ただし、クレジットカード会社と加盟店の間の取引は電子商取引として位置づけられることになる。

以上に対して、決済のみがファームバンキング（EFT）によって行われる取引の場合には、これは電子商取引ということになし、さらに、例えばCALSにおける電子カタログの配布または公表は、取引の潜在的な当事者間における「契約締結に必要な情報」の伝達に該当するという意味で「電子商取引」の範疇に属するであろう。そして、オンラインによるデータベース情報の提供は、電子的情報の伝達によって契約の履行を行う場合、場合によってはデータベース利用契約を電子的情報の伝達・交換により成立させる契約締結という意味で「電子商取引」の範疇に属することになろうし、いわゆる政府調達も、当然のことながら電子商取引の範疇に入る場合があり得る。

(4) 機能・利用形態に対応した法律問題検討の必要性

電子商取引についてかかる位置づけを与えたことが可能であったとしても、その範疇は必ずしも確定することにはならないことには留意する必要があろう。

例えば、カード電話によるクレジットカード通話を考えると、端末に該当するカード電話は利用者が占有管理するものとはいえないが、そのシステム如何により、例えば暗証番号を入力して初めて通話が可能になるとすれば、プリペイドカードによる通話とは異なり、自らが取引に必要な情報を作成しているとも考えられ、電子商取引に準じた法律的検討を行う必要がある可能性があるからである。このように考えると、「電子商取引」について全般な位置づけ、定義を定めることやこれに共通する法律問題を検討するという作業は極めて困難な側面もある。

ただ、少なくとも、電子商取引について上記のごとき一応の位置づけを与えるとすれば、これに共通する問題として、情報のデジタル化に伴う諸問題、例えば、複製の容易性、改竄・変更のおそれなど想定することが可能であり、また電子的情報の匿名性や電子的情報の共有化に伴う諸問題をあげることは可能であろう。こうした問題についての法律的検討を行う必要は当然のことであるが、このような共通の問題を越えて、各行為ごとに特有な法律問題を検討する場合には、別個の検討が必要であり、一律の議論をすることは、むしろ危険であるとさえいえる。

インターネットなどの普及により、取引に関する情報の伝達が既に多様化して

いる現状にあっては、このような視点を持ちつつ、その電子的情報の伝達が取引の中でいかなる機能を果たすかを具体的に想定し、その機能や利用形態に即した法律問題を個々に検討する必要性があろう。

(注) EDIについては、産業情報化推進センターでは、通商産業省の「電子計算機相互運用環境整備委員会」（平成元年度）で定められた「異なる組織間で、取引のためのメッセージを、通信回線を介して標準的な規約（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」という定義を使っているが、世界的にみれば、UN/EDIFACTの定義、すなわち「情報を構造化するために合意された標準を用いてなされる、コンピューター間の情報の電子的移動をいう」との定義がほぼ定着しつつある。この定義によれば、電子的移動の対象となる情報は必ずしも取引情報には限らず、行政情報その他の情報も含まれることになるし、また、「合意された標準」は必ずしも多数の当事者間で合意されたいわゆる「業界標準」である必要はない。ただ、わが国においては、EDIは、特定事業者間で実施される受発注データ交換を中心とする商取引のためのデータ交換の趣旨で使用されることが多いため、本報告書においては、特に断らない限り、「EDI」という用語をこの趣旨で使用する。

2.1.3 「オープン化」の整理

法的観点のうえからは、「電子商取引」のオープン化については三つの側面からの検討が必要と思われる。すなわち（やや比喩的になり、かつ、このような表現が技術的に正しいかどうかは別として）、

(イ) 「通信経路のオープン化」、すなわち、インターネットに代表される通信経路が必ずしも特定されない形態による電子的情報の移動の側面、

(ロ) 「情報伝達当事者（最近では「情報移動」という表現がとられることがある）のオープン化」、すなわち、電子的情報が必ずしも特定されない作成者・送信者から伝達されるという側面、

(ハ) 「情報それ自体のオープン化」、すなわち、通信手段を経由して伝達される情報が、その名宛人だけでなく、第三者にも開示されることや、そもそもホームページに掲出された電子的情報のように、そもそも電子的情報の名宛人が

ない情報伝達により、情報それ自体が共通化するという側面、

についての検討である。

現在のわが国における「オープンEDI」や「オープンループの電子取引」の議論は、この三者の側面を兼ね備えたネットワークにおける取引情報の移動を想定した議論のように思える。

しかしながら、インターネットは、「非同期分散処理型のパケット交換システム」であり、特定の通信経路を用いて情報の移動が行われないという意味で「通信経路のオープン化」があるといえるが、このようにオープンな経路を使用した場合であってもパスワードなどによるアクセスコントロールを設定することにより、特定の当事者間でのみ商取引に関するデータの移動を行うことも可能である（ただ、インターネットはその特性上、共通鍵方式による暗号技術などを利用した何らかの情報秘匿措置をとらない限りその情報が第三者に漏洩する虞がある。したがって、「情報それ自体のオープン化・共通化」という側面、より端的に言えばリスクが存在するということになろう）。しかしながら、上記のようなアクセスコントロールを行う場合には、「情報伝達当事者のオープン化」すなわち、不特定の当事者間で商取引情報が移動するということは考えにくい。

また、いわゆる「オープンなサイバーマート」、例えば、インターネットのホームページ上でそのアクセス制限を行わずに商品情報を掲出し、これを利用して不特定の顧客（消費者）から商品の発注を受ける場合であっても、そのサイバーマートがクレジットカードによる決済を指定していれば、結果としては、そのサイバーマートに利用可能なクレジットカード保有者のみが利用しうるサイバーマートであるという見方もできないわけではない。しかも、この場合には、クレジットカード会社とクレジットカード保有者との間においては、クレジット利用契約が存在するし、クレジットカード会社とサイバーマートの営業主体（サイバーマートの運営主体・営業主体は一様ではない）との間には加盟店契約が存在し、場合によっては、抗弁権の接続の法理によりサイバーマートの営業主体と消費者の間の紛争が処理されることもあろう。こうした運営形態をとる「オープンなサイバーマート」のすべてを「情報それ自体の移動がオープン」すなわち「不特定の当事者間で情報が移動する」形態とすることには躊躇を覚える。

もっとも、「情報の移動それ自体がオープン」という形態も想定できないわけで

はなく、むしろこうした側面・特性を有する形態の取引情報の移動もありうると考えるべきではあろう。

たとえば、不動産に関して必要な情報をネットワークを通じて入手しうるようにし、その入札や入札保証金、支払・決済に関する情報もネットワークを通じて伝達・移動することができれば、いわば電子不動産競売システムを構築することも不可能ではない。このような具体的システムは、もちろん「情報の移動それ自体がオープン」、すなわち、不特定の者の間で情報の移動を行うことも可能となり、それに対応して、入札者の同一性確認を行うシステム（この「同一性確認」はメッセージに表示されたメッセージ作成者が当該のメッセージを作成したことを確認することをいう）や、メッセージの完全性を確認するシステム（この「完全性」は、メッセージについて変更が加えられていないことを確認することをいう）、場合によっては、メッセージの受領確認を行うシステムも必要となり、これに付随する電子的な資金移動システムをも必要とする。これらのシステムの多くは、暗号技術などの技術を利用することになろうが、これらのシステムを利用することにより、メッセージの作成者や受領者がどのような法律的地位に立つかを検討することは欠かせまい。

2.1.4　電子商取引に関する法律的検討の課題

本節においては、「電子商取引」と「オープン」について若干の考察を行ったが、急速に利用が普及し、かつその利用の形態が多様化している電子商取引の実情をみれば、その利用形態ごとに、個別の考察・検討を必要とする課題が増加しているように思える。その意味で、電子商取引の普及のためには、その背景となる共通の社会的基盤としての技術・法制度の検討を行うとともに、利用形態ごとの法律的課題の検討を具体的に行う必要があろう。

2.2　インターネットを利用した EDI

（執筆担当：小川憲久）

2.2.1　EDIのオープン化とインターネットの利用

(1)　クローズド EDI

EDI は、特定企業間のコンピュータ間において取引データの交換を実現するという形態の取引を当初の目的として始まった。そこでは、特定企業間の継続的取引を前提に、取引データの整合性を確保する手順を合意し，VAN、専用回線等のクローズドネットワークを介してコンピュータ間のデータ交換を実現している。したがって、EDI は特定企業間の取引基本契約及び電子データ交換（オンライン取引）に関する協定が前提とされているとともに、トラブルの対応等に関する EDI のシステム運用規約、メッセージ、データエレメント、シンタックス等の情報表現に関するビジネスプロトコル、情報伝達手順である通信プロトコルについての合意も必然となっている。つまり、この形態の EDI は特定企業間の特別な約束に従った取引データ交換が実現されているもので、そのデータ交換は両企業間において完結するという意味において概念的にクローズドであり、また、VAN や専用回線を利用するという伝達手段の面においてもクローズドである。

上記のようなクローズド EDI において、インターネットを利用することはいかなる意味を持つのであろうか。

まず検討すべきことは、伝達手段としてのインターネットの利用である。インターネットの普及が急速に拡大していることを考えた場合、設備投資、運用にかかる費用は逓減し、通信・伝達手段としての利用はきわめて容易かつ安価になりつつある。そこでは、VAN におけるメール・ボックスがインターネット・プロバイダのメール・ボックスで代替しうるかもしれないし、専用回線の代わりにインターネットに接続したホスト・コンピュータを用意することで足りるとも考えられる。そしてインターネットは単なる通信回線以上の意味はな

い。したがって、インターネットを伝達手段とする場合の問題点は、盗聴、成りすまし、改竄、否認という一般にインターネット上での通信セキュリティの問題とされること及びネットワーク管理者の不存在による責任所在の問題に一致し、通信の暗号化、認証、電子署名等の煩雑さを除けば、EDI データの送受信であることをもって特有の問題が生ずることはないと考えられる。

他方、特定企業間の基本契約を前提とした取引データ交換という概念的なクローズド面は、伝達手段にインターネットを利用することで影響を受けるとは考えにくい。伝達が安全に行なえるとの前提の元では、特定企業間での特別な約束に従った取引データの交換自体に変更すべき点はないからである。

ところで、クローズドな EDI は、特定企業間で、取引頻度も多く、取引金額も大きいという場合に多く想定される。そこでは通信のトランザクションも頻繁であり、取引データは加工されずに受信側コンピュータのデータとして取り込まれ、自動的な処理がなされることも予想される。かかる場合にインターネットを利用するために、通信セキュリティのための暗号化、復号化、電子署名の確認等の手続きは（仮に自動化プログラムによってなされ得るとしても）処理手順を複雑化させるのみで、果たして実用的であろうかとの疑問も起こりうるであろう。このような観点からは、既に実用に供されているクローズド EDI においてはインターネットの利用は不要なものであろうし、これから実用化予定の概念的にクローズド形態の EDI についてもインターネットの利用は設備投資にどれほどのものをかけるかという選択対象としての意味しかないと思われる。クローズド EDI においては、インターネットの利用は伝達手段の選択肢の一つとしては成立しうるとしても、大勢においてインターネットに依存する形態とはなり得ないものと考えることもできる。

(2) オープン EDI

オープン EDI とは、不特定企業間のオープン・ネットワークを利用した電子取引を指す。それは、例えば部品調達等において、オープン・ネットワーク上に調達部品の仕様、数量、設計図面等を掲示し、これに応募する企業が自社の概要、対応できる製品等を電子メールで応答し、募集側が再度質問等をネッ

トワーク経由でなすなどして相手を選別して契約に至るという形態を典型的なものとして想定している。ところが、そこでは必ずしも契約後（多くは契約締結それ自体も含めて）のEDIをオープン・ネットワークで行うことを予定しているとは限らない。むしろ、契約後のEDIはクローズドなネットワークを予定していることが多いとも思われる。それは、契約締結後に交わされる取引情報は、調達部品の詳細仕様を含めて営業秘密に属する事項も多く、前記の通り必ずしもオープン・ネットワークを利用することに特段の利点があるとはいえないことからくる。

つまり、ここで言われているオープンEDIとは、取引の誘引時点での当事者が不特定であって、取引誘引情報は全ての人に向けたものであること、ネットワークに掲示される取引情報は誰でもアクセス可能な汎用性のあるデータベースのコンテンツの意味があること、利用されるネットワークは可能な限りオープンなものであることを意味している。したがって、ここでのEDIとは、基本的概念がクローズドEDIとは異なるものであり、別の場面を想定しているものということになる。クローズドEDIは取引開始後の取引データの交換を対象としているのに対し、ここにいうオープンEDIは取引に至る前の段階の、契約法的に言えば、申し込みの誘引から契約締結までの段階をオープンなネットワークを利用して行なおうとする試みだからである。

オープンEDIが上記のような形態のものであるとした場合、そこでのインターネットの利用による問題は、契約締結に至るまでの交信過程において新たな法的問題が生ずるかとの問題に帰着する。契約締結後のデータ交換についてはクローズドEDIにおける回線としてのインターネットの利用と同じ問題だからである。

そこで、再度、上記典型例でのオープンEDIの取り組みをみてみると、先ず、部品調達企業がインターネット上のホームページに調達部品の仕様、数量、納期等の情報を掲載し、応募する企業に電子メールによる応募を求める。応募する企業は募集企業のホームページをみて、自社の概要、納品可能な部品製品、価格等を電子メールで募集企業に応募する。その際には応募企業の同一性を担保するために認証手続きが必要となり、応募内容に改変が行われないよう電子

署名を施した暗号化が必要となる。したがってその前提として一定の暗号方式の普及が必要となる。募集企業は応募された電子メールを復号化し、内容を検討して更に応募企業に暗号化した電子メールで質問を送付し、応募側はこれに回答するという過程を繰り返す。また、場合によっては（むしろ、殆どの場合に）応答の前に秘密保持契約を交わすこともあり得る。そして両者が合意に達した時点で取引契約を交わすことになる。これらの一連の過程における暗号、認証、電子署名等の問題は通信セキュリティの問題であり、契約に直接反映される法律問題ではない。これに対して秘密保持契約の締結、取引契約の締結は法律行為であり、仮にこれが全てネットワークを通じてなされた場合には、既に電子取引の問題として議論されている契約の成立時期の問題、契約締結権限、錯誤の問題が生じることになる。

なお、オープンEDIについての上記の手続きにおいては、当事者企業の信用の点については全く担保するものがないことに注意する必要がある。認証手続きは企業の信用に関しては全く関与するものではない。そこでネットワーク加入に資格制限を設ける、企業評価の第三者機関を作る等の環境整備がなされなくてはオープンEDIの実現は難しいのではないかとの意見もある（内田貴・電子商取引と法・NBL600・41頁）が、資格制限はオープンの中にクローズドな環境を作ろうとすることに他ならずここでいうオープンEDIの枠外の問題となるし、評価機関は実現し難いと思われる。したがって、現実には、EDI取引をなそうとする企業が現実に一度も対面交渉することなく契約し、取引を開始することはあり得ないことにならざるを得ない。上記の意味でのオープンEDIは単に取引の機会を作る以上の意味はないことに帰着する可能性がある。

2.2.2 インターネットによるEDI

(1) IETFによるインターネットEDIの要件文書

インターネット上のEDIを安全に行うことを目的として、インターネットの保守管理改善を目的とする非営利団体であるIETF (Internet Engeneering Task Force) がInternetT-Draftを発表している。これは、インターネット上での取引安全性確保のための技術方式の提案であり、基本はデータの公開鍵方式暗号化と電子署名付き受領確認、送信データの追跡機能、メール・ボックスへの配信

通知機能の標準化である。この提案は電子取引自体の法律問題については触れるところはないが、インターネットを経由してのEDI取引を安全に行うことを目的としており、そこには上記のクローズドEDI、オープンEDIという概念ではなく電子取引（EC）という広い視野でのEDIを念頭に置いていると思われる。

(2) 電子商取引に関するUNCITRALモデル法

国連の国際商取引法委員会は1996年に電子商取引に関するモデル法を採択し、電子商取引（Electronic Commerce :EC）についての制度的障害を除去しその法的枠組みについて国際的な協調を目指している。そこでは、EDIを「情報を構造化するために合意された標準を用いてなされる、コンピュータ間の情報の電子的移動」と定義し、このEDIを含む電子的、光学的及び類似の情報を「データメッセージ」として、データメッセージの交換による契約の成立、有効性等について法的制度の提案をなしている。すなわち、そこにはEDIはデータメッセージの一態様であり、ECの一部であるとの理解がある。

(3) まとめ

上記の通り、インターネットを利用したEDIは、既にインターネット上のECの特殊な領域となりつつある。EDIは企業間で標準化されたビジネス・プロトコルによって構造化された取引データの移動であるが、それは想定され、実現されてきた順序とは逆に、既に始まりつつあるインターネットを利用した消費者取引 －電子現金等による電子的な決済を含む、日常言語によるEC－の特化された領域を占めるものとみることもできる。前記の通り、EDIをクローズドなものからオープンなものへの発展とみる捉え方は、クローズドな環境を如何にしたらオープンなもので代替できるのかという思考であり、クローズドな基本視点に変更はない。EDIをECの一態様と見る視点は、完全にクローズドな環境下でのEDIとインターネット等の本質的にオープンで規制や秩序の採りにくい環境下でのEDIを別のものとして考えてみる必要性を示しているのではないかと思われる。

2.3　CALSの展開とその法的問題

（執筆担当：永田眞三郎）

2.3.1　CALS の基本的な考え方

(1)　EDI・EFT から EC へ

①　EDIとEC

通産省では、国際的に広く用いられるようになってきたエレクトロニック・コマース(Electronic Commerce)を、文字どおり「電子商取引」と訳し、「一部にせよ全体にせよ取引を電子的に行うことすべてを総称してこの言葉を用いる」としている。

「取引を電子的に行うこと」、このこと自体は、特定企業間の取引において、すでに10年以上も以前から行われ、広く進展してきている。これが、これまでEDI (Electronic Data Interchange：電子データ交換取引あるいは電子取引) とよばれてきたものである。財団法人金融情報システムセンターの1995年春の実態調査によると、回答企業（510社）のうち 33.9 %が、EDI、すなわち取引先とのコンピュータを利用したデータ交換を実施していると回答している。また、「１年以内に実施」ないし「実施を検討中」と回答した企業を入れると46.3%になり、そのうち大・中堅企業(380社) では、その割合は53.7%にのぼる、と報告されている。これは、商品の受発注取引や在庫・物流管理に関わるデータ交換についての数値であり、金融機関との決済に関するデータ交換は含まれていない（財団法人金融情報システムセンター (FISC) 編「EDI 研究会報告書－フイナンシャル EDI 実現にあたっての課題－」(1995 年10月) による。）。

②　EFT と EC

金融機関との取引、すなわち入金や預金の引出し、振込みや振替え等の銀行取引では、CD や ATM を介して「電子的に行うこと」は、すでに一般的になってきている。このデータ交換の流れは、国内でも国際的にも EFT (Electronic Funds Transfer: 電子資金移動) とよばれ、受発注取引の電子取引化である EDI

よりはるかに早くから、企業と金融機関との間だけでなく、消費者と金融機関との間においても普及してきた取引のツールである。

このような情況の中で、今日、「電子商取引」という言葉や、やや唐突に広がってきたのは、これまでのEDIやEFTを包括する形で、広く取引社会に、あるいは社会生活一般に電子的に情報交換を行うことが普及してきたことによる。

③ ECの特質

「取引を電子的に行うこと」は、前述のように、EFTやEDIという形態でかなり広い範囲ですでに実施されていたとすると、この「電子商取引」と呼ばれているものは、一体何なのか、そして、この数年に何が起こりつつあるのか、そしてそれがCALSへとどう繋がるのかを整理してみる必要がある。

たしかに「取引を電子的に行うこと」は、前述のとおり、すでにかなりの進展をみてきた。しかし、まず留意すべきことは、EDIもEFTも、これまでは、ほとんどが「特定の回線（多くは専用回線）」を用いたデータ交換であった。また、EFTは、ビジネスのうちの、もっぱら振込みと振替えという「決済のための資金移動」という事務処理を実施するものであった。一方、EDIは、少なくとも国内的には、ほとんどが「受発注取引（契約の締結）」という事務処理を実施するものであった。また、EFTについては銀行と消費者を含めた多数の顧客という関係にあり、当事者にやや拡がりがみられるが、EDIは、特定の企業者間の取引に限られ、継続的取引関係のある取引、すなわち顧客関係のある取引に用いられてきた。

このように、これまで展開されてきた「取引の電子化」は、総じていえばclosedな取引関係の当事者が、closedな通信メディアを用いて、ある限定された事務処理を対象にして実施されてきた、といえる。これに対して、今、「電子商取引」が注目され、新たな新時代のキーワードとしての位置を占めつつあるのは、総じていえば、いわばその「オープン性」という特質にあると思われる。

この電子商取引の「オープン性」は、1990年のインターネットの商用化が決定的な契機となったことは否定できない。電子商取引の特質は、そのインター

ネットの拡大を契機とし、それをも含めて、次の四つの状況に集約される。1)通信メディアないしツールの拡がり＝専用回線 (closed loop) 型からインターネット(open loop) 型へ、2)取引当事者ないし関係の拡がり＝特定企業 (顧客) 間取引から対不特定企業の取引さらには対消費者の取引へ、3)取引プロセスのうちの対象となるデータ処理の拡がりないし結合＝EFTからのEDIの取込み（いわゆるフイナンシャルEDI）あるいはEDI（受発注）とEFTあるいはEDIと電子マネーとの結合、4)取引地域の拡がり＝国内取引からcross borderの取引へ、以上の四つである。

(2) EDIとCALS

① CALSの誕生とその変遷

CALSは、まずアメリカ国防省が生み出した1) Computer-Aided Logistic Support（コンピュータによる兵站業務の支援)、その発展形態である2) Computer-aided Acquisition and Logistic Support（＝コンピュータによる調達と兵站業務の支援)に端を発する。そこから、民間事業への展開に向かって、CALSは、3) Continuous Acquisition and Life-cycle Support (継続的な調達とライフサイクルの支援＝生産・調達・運用支援統合情報システム) を意味するものと解されるようになった。光ファイバーによるディジタル通信網によるビジネス革命をイメージするものとして、CALSは、Commerce At Light Speed（光速の商取引）なのだともいわれている。

② ECの動向とCALSとの基本的な違い

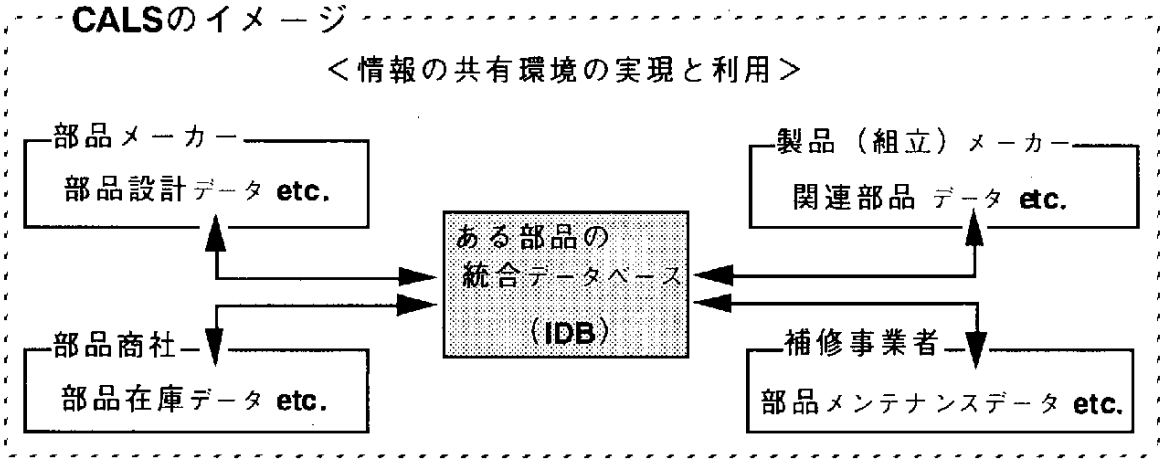
ECは、取引を電子的に行うことのすべてを総称して用いられるが、その方向は、もっぱらデータ交換の電子化に向けられている。すなわち、受発注という事務処理の電子化、決済という事務処理の電子化、また、それらの事務処理と事務処理の連携をめざすものである。そしてEDIやEFTからのECへのシフトは、個々の事務処理の効率性を追求した結果としての前記の「オープン性」への志向であり、その実現である。

これに対して、CALSのめざすところは、EDIやEFTによる技術革新を前提とはしているが、電子データ交換による個々の事務処理の効率性そのものを志

向するものではない。

現在CALSの実現を考える者の頭の中にあるイメージ、あるいは、そのいくつかのパイロットプランでは、その中心的志向は、EDI や EFT の事務処理の効率性の追求を越え、そこでは、情報の共有環境を実現し、その共同利用に図ることである。そこでは、一つの製品のライフサイクル（例えば、設計⇒製造⇒据付⇒試験⇒運用⇒調達⇒設計⇒・・・）に係る文字・図形・製品モデルを含む全ての情報の統合データベース（ IDB＝Integrated Data Base ）を構築し、その製品の情報の共有環境を実現する。その製品のライフサイクルに係るあらゆるビジネスが、EDI（電子データ交換）や IGES（CADデータ交換仕様）など共通のツールを通じてそのデータベースにアクセスし、情報の共同利用を図る。

それによって、製品のライフサイクル全体をみて、もっとも優れた製品をもっとも効率的かつ低コストで供給していこうとするものである。



このように、CALS の基本的コンセプトは、EDI や EFT のように、いわば直線的な契約プロセスの一部の事務処理を対象とするものでなく、いわば循環的な製品のライフサイクルのプロセスを基軸とする。したがって、契約のプロセスを時系列的に分断して、契約の成立 (受発注) の部分に関する伝統的な契約理論を、あるいは、契約義務の履行としての代金の支払い (決済) に関する部分の伝統的な弁済に関する法理論を、どのように変容させて新しい事態に対応させるか、という思考方法は、ここではうまく適合しない。

2.3.2 CALS の法的問題

(1) CALS 実現のための環境

① CALS 実現のための二つの視点

CALS は、情報の統合データベース（IDB）を構築し、その製品の情報の共有環境を実現し、それを用いて、製品のライフサイクルを整合的にコントロールしていくことを意味する。とすると、その実現を見通すためには、二つの視点からの検討が必要である。その第一は、そのような情報の共有環境を実際に実現することができるか、という技術上ないしシステム形成上の視点である。第二は、その共有環境を利用して、製品のライフサイクルを整合的にコントロールしていこうとする構想が実際にビジネスとして結実するか、という活用可能性の視点である。これらの二つの視点からの検討の結果、それがネガティヴなものであるとすると、CALS は、夢のコンセプトであり、情報産業の世界、あるいはマネジメントの世界の一つのブームにすぎないという結果になる。

② CALS 導入の障害

上記の二つの視点から、特殊日本的なものも含めて、CALS 導入については、いくつかの障害が指摘されている。まず、技術上ないしシステム形成上の視点からは、企業内でのデータ管理の一元化の問題、企業間でのデータの管理体系や構造定義の整理・再統合の問題、ネットワーク及びデータベースを中心とするインフラの整備の問題、ネットワークの安全性の問題、アプリケーションのインターフェイスの統一の問題等、克服されなければならない実に多くの問題が挙げられる。また、ビジネス上の視点からも、CALS は、情報の統合データベース（IDB）を構築し情報の共有環境を実現することになるが、多大な費用と厖大な時間を費やしてその環境整備に関わった者が、それに相応するビジネスにありつけるという保証があるわけではない、という点が最大の問題点が指摘される。国防省のようなビッグ・ユーザー主導で始まった CALS では捨象できたこの問題性が、民間主導では、最初のネックとなっている、といえよう。もっと卑近な障害要因として、系列の企業グループ間などでの固定的な偏った取引慣行の中にある日本の産業社会が、このような開かれた製品企画や調達のシステムに移行できるのかどうかということも挙げられよう。

③　CALS のための法的なルールづくりに必要性

CALS 導入には、上記のような障害ないしは障害のおそれが指摘され、その取り組みへの歩調が整っておらず、その速度もやや減速気味といわれている。しかしながら、CALS の基本的なコンセプトは、統合データベースのもとで、製品のライフサイクルすべての段階を整合的にコントロールしていくという、製品の質、コスト、その他の効率性からみて、ビジネス上もっとも合理的なものを志向しているとすれば、最終的に、CALS をうまく実現し活用できた産業社会が、他を凌駕して成功をおさめることになる。

そこで、CALS 実現のための障害となっているという点を分析・整理してより明解なものにし、その不透明な部分をできるかぎり少なくすることが、まず必要である。その一つとして、CALS という新しい企業システムに係る法的問題を整理し、その法的枠組みの方向性を提示することが有用である。

④　法的問題の二つの側面

ビジネスにかかるネットワークシステムを法的に整理する場合には、1) ビジネス関係の形成システムという側面、2) 情報利用ないし情報交換システムという側面、この二つの側面に分けて整理し、その上で両者が競合する部分について精査していくという手法が適切であろう。以下、その手法にしたがって、CALS に係る法的問題を整理するために必要ないくつかの事項を挙げる。

(2)　ビジネス関係形成システムとしての CALS の法的問題

①　CALS の当事者関係のイメージ

まず、CALS の当事者を 1) 「特定企業間ネットワーク」(closed) を基本型とするか、2) 「不特定企業間ネットワーク」(open) をも対象とする場合をモデル形態とするか、が前提問題となる。前者であれば、これまで EDI で形成されてきた法律構成が CALS のかなりの部分に適用できることになる。しかし、「開かれた調達」を CALS の基本要素とみるならば、後者の形態で展開していくことを前提とせざるをえない。その場合、情報の開示、契約の成立からその履行に至る法律問題のきめ細かな構成が必要となる。

② 製品の Life-cycle に対応したビジネスの態様と法律関係

製品の Life-cycle が、仮に 1) 開発段階、2) 原材料・部品調達段階、3) 製造・施工段階、4) 流通段階、5) 保守・管理段階に分かれるとすれば、それらの業態に応じて、例えば、それぞれ、設計請負、売買、工事請負、倉庫、運送、修補請負等の契約が存在し、その契約類型に応じた法的問題ピックアップするだけでよいのか否か、が問題となる。

③ CALS の参加事業者の法律関係 (取引関係)

上記の②に続いて、CALS の法律関係を 1) それぞれの段階で独立した個別の受発注関係があるとみるのか、2)全体として業務提携関係 (ないし組合) として法律構成することがより適切なのか、ということが問題となる。それに応じて、IDB（統合データベース）への情報提供・利用関係の法律構成にも違いが生ずることになる。

(3) データ交換・利用システムとしての CALS の法的問題

① CALS の通信ツールのイメージ

CALS の通信ツールを 1)「専用回線の利用」を基本型とするか、2)「インターネットの利用」をも対象とする場合をモデル形態とするか、が前提問題となる。前者であれば、情報の伝送に関しては、EDI や EFT で展開されてきた法的ルールが適用できる。後者であれば、現状では、コンピュータ・セキュリティやトランザクション・セキュリティの面で前者と大きな差異があることから、その点で新たなルール作りが必要となる。

② IDB（統合データベース）の実現と利用のための標準化の法律関係

IDB（統合データベース）を構築していくとなると、当然 EDI（電子データ交換）やIGES（CADデータ交換仕様）など共通のツールをもちいることになり、その標準化・企画化が前提となる。となると、CALS は、1) 標準化の主導主体と競争制限法上の問題、2) 標準化と知的財産権法上の問題が、克服さるべき障害となる。

③ 「仮想データベース」としての IDB の利用関係

EDI や EFT は、多くの場合、いわゆる VAN 事業者が提供するシステムを、取引当事者がユーザーとしてシステム利用契約に基づいて使用する関係にたつ。あるいは、取引当事者の一方がシステムを構築して提供したり、双方が構築したシステムを接合して、データ交換することもある。しかし、CALSの基礎となる IDB（統合データベース）は、各事業者に分属する部分データをシステム上統合されたものとして利用できる、いわば「仮想データベース」である。したがって、CALS のシステム運営主体と参加事業者との間のシステム利用の関係をいかにとらえるかが問題となる。少なくとも、EDI や EFT の場合のように「システム提供者とユーザー」というような関係としてはとらえられないことは確かである。

2.3.3 CALS の法的問題の検討

以上の整理は、CALS を係る法的問題について、検討すべき事項の項目をいくつか挙げたにとどまる。今後は、それぞれの事項のより具体的問題点、その法的解決の方向の提示が必要となる。今、CALS がビジネスの世界で現実にどう展開していくかは明確ではない。したがって、上記の事項を念頭において、その具体的な進展に応じて詳細を詰めていくことが適切であろう。

3．　業際EDI

3. 業際 EDI

3.1 物流 EDI の実際

（執筆担当：野村豊弘）

本委員会の作業部会では運送会社における電子データ交換システムの実態について実際に行われている事例を中心にヒアリングを行った。本報告書では、どのような電子データ交換システムが実施されているのかをまとめ、そこに含まれる問題点について考察することにする。

3.1.1 電子データ交換システムの実態

(1) データ交換の形態

物流に関して、運送会社と荷送人、荷受人、倉庫会社、他の運送会社などとの間で行われるデータの交換および運送会社内部で行われるデータ交換（たとえば、顧客情報センター、本社、各営業所間のデータ交換）は、必ずしもコンピュータシステムを利用した EDI のみによっているのでないことはいうまでもない。電話、ファックス等の手段も併用されている。

(2) 電子データ交換の具体的な事例

物流といっても、運送会社が関与する取引の形態あるいは物流の形態にはさまざまなものがあり、そのそれぞれについて個別的に電子データ交換を含めた物流システムが構築されている。したがって、一つの運送会社におけるシステム数はかなりの数になるようである。たとえば、ある運送会社の具体例をあげると、配送指図システム（本社が顧客から受信した配送指図情報および運賃データを各拠点に通知するもの）、出荷指図システム（本社が顧客から受信した出荷指図情報を他の運送会社および倉庫会社に送信し、運送会社から受信した配車情報を倉庫会社および顧客に送信するもの）、配送デポ管理システム（本社が顧客から受信した配送指図情報を各拠点に送信し、拠点から受信した入庫完

了情報を顧客に送信するもの）、配送在庫デポ照会システム（顧客が配送センターの在庫状況を各営業者から即時に把握できるもの）、運送状況情報サービスシステム（運送中の貨物の追跡情報を顧客に提供するもの）、POS レジ情報連携システム（コンビニエンスストアが客から受け付けた宅配便の処理に関するもの）などが実施されている。これらにおいては、商品の集配、在庫等に伴う電子データ交換が組み込まれている。また、商品の売主である荷送人に代わって売買代金を回収するサービスも提供されている。

(3) 電子データ交換システムの意義

ところで、物流においてこのような電子データ交換が行われているのは、企業の効率化を目的としている。たとえば、大手の運送業者において行われている貨物の追跡システムによれば、運送中の貨物がどこにあるのかをリアルタイムで知ることができ、荷送人はそのデータを有効に利用することができるのである。すなわち、このようなシステムを利用すれば、デパートの配送品について顧客からの問い合わせに即座に対応できるようになるのである。また、効率化のためにはデータ交換の標準化が重要な課題であるが、物流に関しては必ずしも標準化が進んでいるとはいえないようである。それには、さまざまな原因が考えられる。たとえば、運送業者には中小規模の業者が少なくないが、中小の運送業者にとってデータ交換を標準化することは大きな経済的負担になるということである。また、運送会社は製造業、倉庫業、流通業などさまざまな企業を相手として取引関係を結んでいるが、それぞれ独自に情報の電子化が進んでいて、それらをすべて取り込むような標準化が極めて困難である。

3.1.2 電子データ交換システムの法的問題点

(1) データ交換と商取引

物流の前提として、継続的な売買契約などの取引関係が当事者間に存在するのであるが、それらの取引と物流にかかわる電子データ交換との関係が必ずしも明瞭ではないように思われる。とくに電子データ交換システムに関する契約

書が存在しないことが少なくないようである。そのために、取引契約と電子データ交換システムとの間に十分な整合性がとられているのかがあまり明瞭でないように思われる。

新しいデータ交換システムによって物流が行われるのであるから、契約書を作成し、重要な事項については合意の内容を明確にし、将来の紛争を予防することが必要であろう。

(2) 守秘義務

電子データ交換が行われることによってそれに関与する事業者に関する重要な情報を運送会社が知ることになるが、それについての守秘義務が明確でない。それぞれのシステムによって、問題となるデータの内容は異なると思われるが、システムに関与する当事者間において、契約の履行によって得たデータについての守秘義務を明確にしておく必要があるであろう。

(3) 三者以上の当事者の法的な関係

荷送人からの依頼を受けて、荷送人（売主）に代わって荷受人（買主）から売買代金を回収することも行われているが、運送料を売買代金から差し引くことが行われている例もある。このようなシステムにおいて、当事者の債務不履行の場合に（とくに破産などの場合に）、当事者間の関係がどのようになるのか明確でない。やはり、契約によって当事者間の権利義務関係について明確な合意をしておく必要があるであろう。

3.2　金融 EDI の問題点

（執筆担当：大野幸夫）

3.2.1　はじめに

1）　金融 EDI は、最終的な決済機能を有する為、生産、物流、販売分野でのEDI 化が進展した結果として現在最も求められているネットワークシステムである。

金融EDIが重要なのは、社会的役割としてそれが不可欠であるというだけでなく受発注や請求書に関する事務の効率化にコマーシャルデータの一貫したデータ処理が多きな効用を発揮するからである。ペーパーレスで自動的に（人手を用いずに）正確なデータ授受を行える EDI の本来の機能は、売掛金、買掛金の消込みについて振込人の特定や請求書の照合作業等多くの人手と時間がかかっている事務部分の合理化を促すことは間違いない。

例えば日立製作所では月々約 1 万件近くの売掛金の照合件数を有し名寄せを行っても一度で売掛金明細と入金通知が合うのは全体の 4 割程度にすぎないという（日経産業新聞1996年12月24日）。

このため産業界からの要望に応えて現行の金融システムをベースとした「マッチングキー方式の金融 EDI」が実施される運びとなった。これは受注企業側が、発注企業側との資金決済時に、金融機関から送られてくる入金通知と発注企業側とで交換されるデータとの照合（マッチング）、特に「売掛金の消込み事務」を自動消し込みの実現を狙いとしている。また発注企業側にとっても、振込手数料の集約化によって、振込料金のコストを削減する効果が見込まれている。具体的方法は後述するが、全国銀行データ通信システム（以下では”全銀”と呼ぶ）の為替データに、企業コード＋識別コード20桁をマッチングキーとして付け加えて利用するものである。

2）　また貿易金融EDI面でも、貿易関係に必要な書類作成と照合とが手作業で行われており、日本の場合その非効率性は、様々な矛盾を生んでいる。海上運送業務（ex.コンテナ）は、輸出・輸入面で極めて重要だが、例えば阪神大震災後、神戸港の復旧にもその取扱量は激減したまま元に戻らない状態となっている。日本向けのコンテナが、高雄（台湾）や釜山（韓国）で小口に分けて日本に送られる

からなのである。これには２つ理由が考えられる。一つは、日本の港湾のコストの高さである。二は、船荷証券（B/L→Bill of Lading）等の貿易関連書類電子化の遅れである。例えば、最近の船はスピードが速く、日本国内で書面上の複雑なB/L処理をしている間に、船（荷物）が港に着いてしまい待たされる事態も生じる。そこで、コスト高の上にシステム化の遅れた日本の港湾が敬遠され、「中抜きする現象」が起きつつあるのである。

貿易取引の効率（就中、金融面）は、日本の国家基盤運営上の大問題であって、このまま足元のアジアでの中抜き状態が続けば、グローバルな貿易金融競争に勝てないのは明白である。生産拠点と市場を依存している他のアジア諸国より高い取引コストがかかるうえに、非効率的なシステムに依存していては世界市場でも競争力を失うからである。各省庁、業界や社内の縦割組織を乗越えて国家プロジェクトとして貿易金融EDIに着手する時期にきている。

3.2.2　マッチングキー方式の金融EDIについてのデータフロー（図-２参照）

①発注（買掛側）

発注（買主）企業は、受注（売主）企業に対し発注データを送付する。

②請求（売掛側）

受注企業は、発注企業に対し、確定した請求明細データ（納品情報）を送付する。

③マッチングキーの設定

受注企業は、確定した請求明細データに基づきマッチングキーを設定する。マッチングキーは、20桁以内で、使用できる文字は、数字、英大文字、カナ、「　」等になる。例えば、標準企業コード或は共通取引先コード（12桁）＋識別コード（８桁）という形で用いられる。

④振込依頼と支払い情報の送付

発注企業は、

(a) 取引銀行Ａに対し、受注企業あての振込依頼データにマッチングキーを付け加えてファームバンキング（FB）システム等によって送信すると共に、

(b) 受注企業に対し、同じマッチングキーを付した支払い明細データを送付する。

⑤銀行間の処理

(a) 取引銀行Ａは、受注企業の取引銀行Ｂに対し、マッチングキーを付した振込情報を送信する（為替通知）。

（b）取引銀行Ｂは、送信された振込情報に基づき受注企業の口座に資金を入金すると共に、受注企業に対し振込入金通知データにマッチングキーを付してFBシステム等により送信する。

⑥売掛金の消込み

受注企業は、取引銀行Ｂから送信されたマッチングキー〔⑤（b）〕と、発注企業から別途送付されたマッチングキー〔④（b）〕とを照合することにより、該当する売掛債権を特定し、売掛金の消込みを自動的に行う。

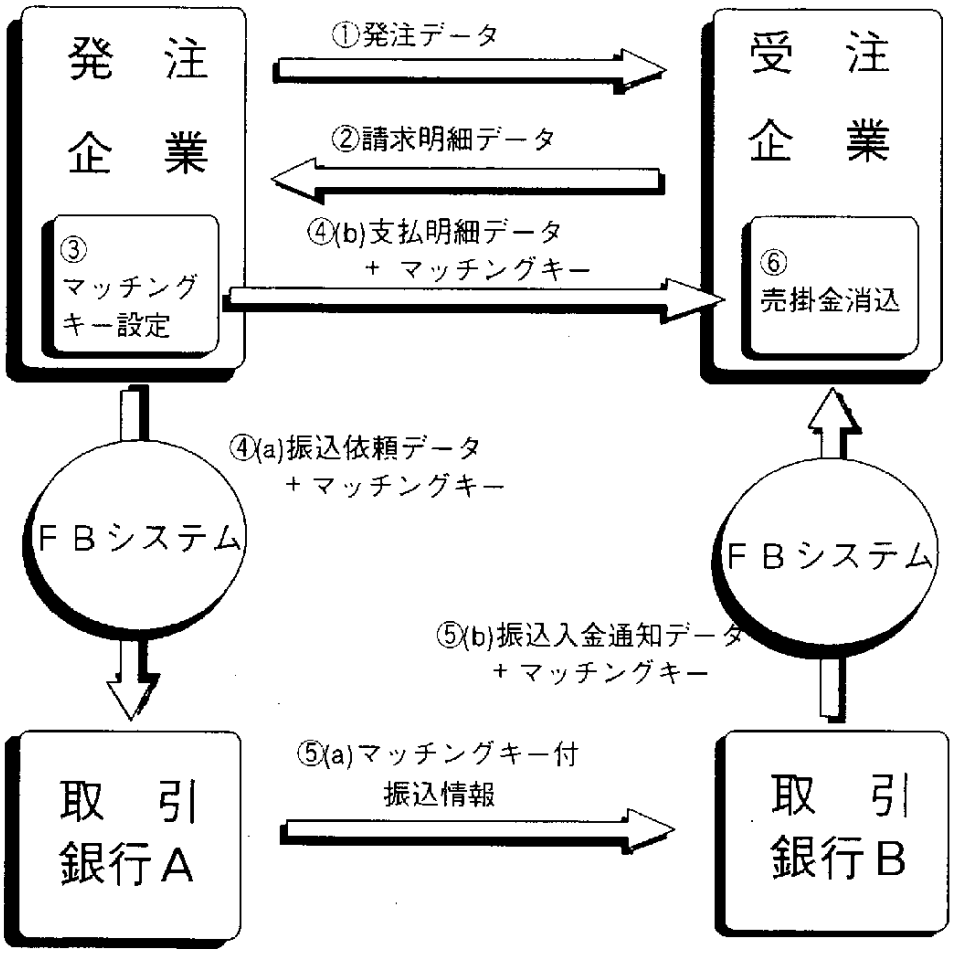


図 2 マッチングキー方式による金融ＥＤＩ

（出典：全国銀行協会　「マッチングキー方式」による金融ＥＤＩのご案内）

＊マッチングキーの送受信には、FBシステムの他、MTデータ伝送（大量データを一度に送れる）やFD授受による方法が可能。

3.2.3 課題と問題点

1）発注企業側の買掛情報（支払い計画）、受注企業の売掛情報（請求額）確定手法の標準化（情報交換ルールと入力データの書式統一）

買掛情報（支払い計画）と売掛情報（請求額）については常に相互の計算相違が生ずる。この原因としては次のような理由があげられている。

○経理上の締日の相違があり、支払い日が月末に団子状に固まる現象がおきる。

○差引計算のやり方の違い（バーター取引、物と物との相殺取引、運賃・振込手数料の扱い）がある。

○リベート、販促手数料の扱いの複雑性

業界ごとに上記に指摘した従来の商慣行を変えていく努力がないと買掛・売掛情報そのものの確定自体が難しい状況が続きマッチングキー方式が導入されても事務効率の向上は望めない。従って、複雑な商慣行の打破と業界の共通ルール策定という EDI には欠かせない事務手続標準化に向けた一層の努力が必要である。具体的には、業界毎ないし当事者間での契約、情報交換ルールと入力データの書式統一や事務取扱準則を早急に定めるのは勿論、アンマッチング（不突合）が生じた場合の対応についても明確な取り決めが必要とみられる。

2）ソフト変更・事務負担軽減のメリットが不均衡である

受注（売掛）企業側に恩恵が集中し、発注（買掛）企業側は FB ソフトやマッチングキー作成の負担などが一方的にかかってきてメリットがない。従って手数料を両者で分担する仕組や契約作りが課題となっている。また、金融機関内部のシステム変更（EDI 情報を為替通知にセットし、入金通知にマッチングキー・EDI 情報をセット）には、一行あたり数百万から一千万円かかるといわれる。銀行自体においても一律に導入する体制にはなっておらず大企業（EDI、ECに積極的）との取引の少ない地方銀行や信用金庫ではマッチングキーサービスのためのソフト変更を見送っている例も多い。次の段階では、多くの企業、金融機関がメリット・デメリットを勘案して参加できる多様なソフトメニューの提案が望まれる。

3.2.4 今後の展開について

1997年１月より大手電機会社11社が、マッチングキー方式の金融 EDI の実用実験を開始し、この結果によって参加企業は増える見とおしである。売掛金の消込業

務の自動化によって事務効率が高まれば、FB（フアームバンキング）も一層推進されると期待されている。

但し、既存の利用企業への影響を少なくする為、FB 先のみを対象とし全銀標準フーマット変更は最小限として新規作成は行わず、全銀システム（平成７年11月稼働）への影響も最小限に抑える等が、導入の前提方針とされた。その結果、セキュリティ上の問題もあって ANSWER、CMS との接続や各分野でのEDI推進体制（EDIFACT、CII）との協調には至らなかった。今後のグローバルな展開を考慮すれば、商流データ（受発注・納品・請求・支払い関連）や手形決済情報が入力できる汎用システムが必要不可欠である。

金融EDIが進捗すれば、金融機関が情報から疎外されるという懸念もみられるが、これは全く逆であって、商流データと金融データの融合が実現すれば、銀行等の新しい情報処理機能（信用照会・DBサービス）が可能となり企業、個人いずれもシステム化金融機関された金融機関を利用する頻度は増えるだろう。

3.2.5　貿易金融EDIの課題

1）貿易取引実務の効率化の必要性

日本の既存の商取引のなかで現在最も効率化の効果の大きいと見られるのが、貿易取引実務と金融機関での事務処理手続分野である。EDI の相手たる企業は外国にあり、商慣習や通信システムの利用レベルには格差があって決済方法も国内でのように協調する対応（例えば、マッチングキー方式の採用）は難しい。一方、金融機関での実務処理は、今だに人手に頼る書類上の作業が主体であり、前述した国際的な金融EDI推進の動きは、この分野の非効率性を打破すべく急速な展開を見せ始めている（後述のアジア各国の取り組み、EU の BOLERO 計画等）。わが国における貿易取引面での年間事務コストは、年間輸出入総額80兆円の約７％（５兆６千億円→国連の調査による）といわれ、そのうち30％がEDI化によって削減可能と試算されている（SWIFT による）。従って約１兆７千億円ものコストが、既に貿易金融 EDI システムを作り上げている周辺諸国より余分に付加されていることになる。一件の取引毎に他国より高い限界コストがかかる上に事務効率も低いとすれば、取引対象の財貨・サービス自体の価格競争力が失墜することは免れない。

2）貿易取引のプロセスの特徴

①契約書による責任範囲の明確化と多数当事者の存在

貿易取引は、商慣習が異なる相手方との商取引である為、当事者は契約書によって各自の責任を明確にして作業を進めるのが通例だが、当事者は多様である。商社、銀行、船会社（外航・内航）、保険、通関業者、運送業等多くの企業が関わるので１体１の取引に比べると情報伝送上の過誤が取引全体に影響を及ぼす範囲広く、収拾に時間がかかれば契約の不履行を招くことにもなる。EDIによる正確・迅速な事務処理が求められる分野なのである。

②書類による情報処理が原則

売り渡す商品について、売主側が事前に他国の買主側の信用調査を十分に行うことはできないから、買主側発行の信用状（L/C ; Letter of Credit）による決済が必要になる。このように現実の貿易取引実務においては、契約書、船積書類から有価証券である船荷証券、作業指示書の様なものまで様々な書類が交換される。取引の正確性を期するためには、個々の書類の役割を知り適切な処理が必要となる。このため各プロセスにおいて膨大なコピーやファクシミリによる記録保全が行われているといわれる。デジタルな標準フォーマットを自動処理することが法的に承認されればEDIが最も有効に機能することになる。

3）貿易取引の課題

EDI は、その本質においてN対Nの取り引きすなわち（オープン化対応）を目指しており、共通の標準フォーマットに構造化されたデータの交換を前提としている。ペーパーレスで自動的に、人手を要せず、正確なデータ授受が可能となって、ビジネスプロセスの簡素化と迅速性が実現できるのである。輸出入取り引きにおいても、EDI システムが〈迅速性と正確性〉〈自動化と個別対応〉〈小さなコストと大きな効果〉〈集中と分散〉等従来の発想では実現できなかった事務処理への要求を可能としてきた観点から、全体のビジネスプロセスを再構築する必要がある。貿易取引実務の状況は、書類作成と照合に多くの人手と時間がかけられているのが特徴であって、紙（ハードコピー）に依存する旧態依然たる様子がうかがわれ、これが取引のコストをあげ迅速な取引を阻んでおり、わが国貿易全体の競争力を下げる要因ともなっている。EDI の本来の機能最もいかせる分野なので以下の諸点から検討をしてみる。

① 貿易書類作成の非効率性

貿易関係書類の作成にあたっては、手作業が多く、EDIの利用による合理化のケースは少ない。たとえば貿易関係書類の代表であるB/Lをみると、コンテナ輸送の場合、海貨業者から船会社に送られるD/R（Dock Receit → コンテナヤードで発行）という書類に記載された情報を手作業で入力したデータを集めてB/Lが作成される。この部分を効率化するため、D/Rを伝達するPOLINETというネットワークシステムが構築されているが（後述）、D/Rのフォーマットが統一化されていない等の理由から、利用者は約二割にとどまり、残りは依然紙ベースで情報をやりとりされている。なお、入力データから紙で出力されるB/Lの最終的発行についても、シッピングマークなど電子化されていない情報が存在するため、更に手作業で追記がなされている。

こうした作業が貿易に関連する多くの種類について、取扱う企業ごとに重複して行われているのが当業界の特徴である。例えば貨物保険業務でみると、顧客による保険申込に必要な情報はインボイス、L/C、B/Lいずれも共通なものがほとんどで保険特有のものは少ない。それにもかかわらず取引企業毎に書類作成が行われるため、申込者は同じ情報を重複して記載し、保険会社も重複した入力作業を行うといった具合である。保険会社では、顧客のインボイスや通関用データを転用して、一部データ伝送による保険申込の合理化をはかっている例もあるが、大部分は手入力に依存しているのが現状である。

自動化による正確な入力が1回なされれば、後は重複記帳を避けられるのがEDIの大きな効用の1つであり、書類作成面の非効率性は、EDI化によって大きく改善されるとみられる。

② 貿易書類の授受（受け渡し）上での非効率性

作成された貿易書類の受け渡しにおいても非効率的側面が見受けられる。書類の配送（クーリエサービス）や配送方法、料金についても対応が煩雑であり、時間がかかる点も問題である。その結果前述したように、貨物船が到着しているにもかかわらず、配送（郵便やクーリエサービス）の遅れによって書類が未着となって貨物の受取が遅れる結果、銀行保証を差し入れるという追加的事務コストを負担するケースも出てくるのである。

合理化が求められている書類のチェック体制をみても、同一の情報を別個に手作業で入力するゆえに誤りが生ずるので、L/C条件と書類内容の一致や書類相互

間の整合性を人件費の高いベテランが担当せざるを得ないというパラドックス的現象が生じている。このようなチェックは、決済に関わる金融機関毎に重複して行われ、更に手作業で重複した作業を行う故に発生する書類不備のために、銀行からの与信が得られず、貨物の受取に障害が起きる例すら少なくない。

書類用の用語の不統一を克服し、標準フォーマットでEDI データを交換すれば、書類授受にまつわる問題は全て解決する。貿易取引に時間がかかり、外貨建て決済等の場合に、売主に為替変動リスクを負担させる結果を招くのは、国際的な信用力にも関わってくる問題である。貿易金融EDIの早急な取組が求められるのである。

③ 貿易規制・為替関係の事務軽減

銀行が顧客と輸送・輸入等の外国為替取引を行うにあたり、外為法は確認・主務大臣への報告義務を課してきた。この確認・報告義務は、顧客の提出する報告書や許可証を船積書類と個別取引毎に手作業で突き合わせる必要がありかなりの事務量であった。来年から外為法が改正され、この面の事務は軽減されるとみられるものの、各国政府の許認可事項がなくなることはないので、やはり文書で情報交換している部分をEDI 化すれば効用は大きい。EDI によるペーパーレス体制への移行を急ぐべきであろう。

4） 海外における貿易金融 EDI への取組み

事務処理コストの削減のためには、全ての取引をシームレスなネットワークで一貫して処理できる統合ネットワークシステムが必要となる。海外の取組事例の幾つかを示す。

① BOLERO (Bill of Lading for Europe) プロジェクト

EU が主となって電子式船荷証券の開発から各種船積書類を登録、保管、認証の実行を試行し成功した。海運、電子取引、銀行、通信各分野の26の多国籍企業が参加した。この試みの原案は、万国海法会（CMI）の「電子式船荷証券に関するCMI統一規則（→ 海商法法律家協会のリーガルルール）」によっており、システムの実現可能性が確認された。なお、全世界に向けての本稼働ではSWIFTが協力する予定となっている。

② アジア諸国における貿易金融EDI構築例

台湾では、航空貨物自動通関プロジェクトに始まる政府主導の「TRADE-VAN」というネットワークがあり、約4500のユーザが利用している。このネットワークは、貨物のコントロール・通関情報を扱うのみでなく、銀行間のネットワークとも接続されていて、商業データ・金融データの両方を取扱うことができるので関税の支払い等に使われている。更に取引の効率化をめざすため、EDIの世界標準であるEDIFACTに準拠したメインボイスメッセージを開発している。

香港では、「TRADELINK」と呼ぶ半官半民のネットワークが開発され、今年1月より商業サービスを開始した。当初は輸出許可の申請・発行手続と輸出入申告の受付を行っているが、今後はペーパーレス化を進め（紙ベース受付は廃止）、次には原産地証明の電子化を予定している。

この他韓国においては、1991年に貿易事業自動化促進法が制定され、「Trade EDI」プロジェクトが進行しており、マレーシアでも「SMK-Dagang NET」プロジェクトが実施され、シンガポールでは「Trade NET」への取組もなされている。

わが国からのアジアへの直接投資が拡大する中で、アジアはわが国の市場としても重要な役割を占めつつある（地域内貿易比率は51%（1994年））に達している。ビジネスセンターとしての日本の地位低下が目立つのも（物流面では例えばコンテナ扱い高は、香港やシンガポールの2割、金融面での地位低下もこのところ著しい）。結局は、情報システム化の遅れが大きいとみられる。これら諸国を見做っての統合的EDIへのプロジェクトを始動させないと日本はますます競争力をなくすだろう。

5）わが国における貿易金融EDIの取組み

日本の場合部分的に下記のようなネットワークが構築されているもののクロスオーバー的な連携がなく、統合的な処理がなされるレベルには程遠い状況である。

① NACCS（貨物通関情報処理システム）

輸出入貨物の通関手続きを迅速かつ的確に処理するため大蔵省関税局・税関と通関業界及び銀行業界との間で開発された共同システムである。航空貨物（Air-NACCS）は、1978年8月、海上貨物（Sea-NACCS）は、1991年10月に稼働を開始している。なお、1999年10月には、対象業務の拡大やEDIFACT対応を盛り込んだ新しいSea-NACCSの稼働が計画されている。

② POLINET等

海貨業者、船会社、検量機関及び検数機関の間で船積貨物情報を交換するためのネットワークである（180企業が参加）。又、海上貨物の運送に関する業務効率化のため、荷主と船会社間のネットワークであるS.C.NETや荷主と船貨業者間のS.F.NETも構築されている。

③ ファームバンキング

本来は、金融機関と企業のコンピュータ・端末とを結び、残高照会や資金移動等のサービスを提供するネットワークだが一部金融機関では、L/Cの発行依頼の受付や到達通知あるいは外国送金依頼の受付などのサービスを提供している。

6）金融EDIの法的課題

貿易金融EDIシステム実現のための契約法制に関する検討としては、貿易取引に使用される中心的な有価証券である船荷証券（B/L）が電子化された場合を想定して、「貨物取引の遂行に際し、「書類」ではなく、電子データを用いても問題は生じないか（有価証券性、物権的効力の問題）」、および「後日の訴訟に際し、「文書」から電子データへの変換手続・証拠性の問題、電子化を担保する諸制度やセキュリティ、秘密保全問題などいくつかの側面に分けて考察する必要がある。

なお、行政法分野について付言すると、平成10年度に予定されている外為法改正に際しては、輸出入報告の廃止等、報告義務者の負担軽減にも配慮した事後報告制度の整備が行われることとなっており、船荷証券、為替手形、輸出入報告等現在ペーパーベースで作成されている書類の電子化を展望し、簡易化および効率化を志向した内容となることが期待される。

(1) 法律上の問題点とその検討

貿易金EDI システム実現のための法律的側面について現状のインフラ整備状況を検討するにあたって、例として貿易取引に使用される中心的な有価証券である船荷証券（B/L）を電子化するという前提で、以下に、①船荷証券の有価証券性、②船荷証券の物権的効力、③書式の単純化と証拠性、④EDI 化推進のための制度、⑤セキュリティと秘密保持（ノウハウ）の点から考察を行ってみる。

① 船荷証券の有価証券性

(a) 日本では、有価証券とは「財産的価値を有する私法上の権利を表章する証券であって、権利の移転又は行使に証券の占有を必要とするもの」とされている（国際海上物品運送法10条、商584条）。米国においては、日本のような「有価証券」（Valuable Instruments）の概念そのものが存在しない。「流通証券」（Negotiable Instruments）や「商業証券（Commercial Paper）の用語が用いられており、日本のように権利の発生、移転、行使の全部又は一部に証券を必要とするという厳格な解釈はなされていない。現実の取引においても、Sea Waybill や Air Waybill（ワルソー条約11条）が船荷証券（B/L）に代替する場が増えてきている。但し、前者は証拠証券なので荷送人（運送人）の反証を許すものであり、荷受人（銀行）の地位が脅かされる可能性がある（CMI 統一規則「UP500」）。

(b) 電子化のための手法

○「株式の保管振替制度（株式等の保管及び振替に関する法律）」→証券不発行

○「プロ私募債CP」→ 記名債権された約束手形であり裏書は禁止される

等の制度を勘案すれば有価証券概念を電子式権利データにまで拡げるか否かの問題にすぎなくなる。機能的代替性が保全される制度的・技術的担保さえあればいいとみることができる。

※有価証券性がどうしてもネックになる場合： LC 決済、D/P、D/A決済では手形そのもののトランケーションシステムを当初から想定しておくことも可能であろう（イメージ、磁性文字認識）。EDI 化による省力化メリットを阻害しないためである。⇒ 現物を手形交換所に持出さないので、手形小切手法に特則を設ける必要があるかもしれない。

② 船荷証券（B/L・倉庫証券等）の物権的効力

(a) 貨物引換証の物権的効力

貨物引換証に関する商法575条によれば、証券の引渡しが運送品のうえに行使する権利の取得につき「運送品の引渡しと同一の効力」を有するとされており、これが船荷証券（B/L）の物権的効力と呼ばれる。「運送品の引渡しと同一の効力」とは、証券の引渡しが運送品の占有の移転と等しい効力をもつことと理解されている。学説では、B/L の引渡しがあれば、物権取得について直接占有と同一の効力があり（間接占有の擬制）、運送品が運送人の直接占有下

にある限り、民法一般の原則にかかわらずB/Lが運送品を代表する力をもつとする「相対説（代表説）」が多数説である。これに対しB/Lの物権的効力を否定し、証券本来の債権的効力と売買質入等に関する民法一般の原則から導かれる効果であって証券の債権的効力（運送品の引渡請求権）の反射的効果にしかすぎないという「否定説」も有効に主張されている。「否定説」はB/Lに物権的効力が認められるといっても、それは処分証券性（商573条）と受戻証券性（商584条）によって実質的に保証されているにすぎず、B/Lを所持していれば運送品の直接占有が原則として期待できるという。民法の意思主義の原則（民176条）からすれば、運送中の運送品の所有権の移転は、意思表示のみで行われ、対抗要件たる引渡（民178条）も証券の所持で保証されている以上強いて現実の引渡以前に証券の引渡によって運送品の引渡を擬制する（物権的効力を認める）必要はないというわけである。

質券についても、動産質の他に債権質も認められている以上（民362条）、B/Lにより貨物引渡請求権の質入がなされたと考えればよいし、善意取得についても同様に貨物引渡請求権の善意取得がまず生じ、その結果として運送品の入手が保証されるのだから、B/Lの善意取得を運送品自体の善意取得と構成する必要はないとみる。

この考え方に立脚すれば、電子的なペーパーレスのB/LがEDIシステム上で転々譲渡される場合、認証された請求者からの運送中の運送品に対する処分、指図、受戻し、引渡しなどの一連の権利変動プロセスが中央登録機関（CR）での登録ファイルの書き換えにより可能となる。

(b)　CNCITRAL電子商取引モデル法17条(3)

権利義務の移転に書面の交付または使用が義務づけられている場合には、「データメッセージの唯一性（uniqueness）を確保するための信頼できる手段が用いられていれば要件を満たすとしている。この手段とは、BOLEROの中央登録機関（central registry）のような組織を指すとみられる（内田貴　NBL No.603 P36）。

※米国は、16条、17条設定に際し、CMIやBOLEROではB/Lの法的側面を明確にする規定が必要と主張し、今後電子署名のルール（Rule of digital signature）及び電子商取引契約とその履行（Electronic commerce contract and performance

rules）を将来の課題とするよう提案した。これに仏、加が登録機関（Electronic registries）や第三者情報・サービス提供機関（The third-party information and service providers）も重要との提案があり、電子署名及び認証が作業テーマとして選ばれ、法的根拠、適応性、責任の配分が論じられることとなっている。

③　複雑な取引の整理と書式の単純化（証拠性）

(a)　保険分野ではO/P（包括予定保険契約）で事務合理化がはかられ、L/C書式の「UCP500」：運送書類では国際商工会議のURC（複合運送書類に関する統一規則）：電子式船荷証券については、CMIルールが採用され統一化が図られている。

(b)　実務においては、B/Lについては、非定型条件が多く、付帯情報量が多すぎる等の指摘もある。EDI化にあたっては、不要な事務を全部捨て書式を必要最低限度に絞ることがまず第一歩と見られる。

このためには、共用できる書式（Sea WaybillとAir Waybillの共通フォーマット化）の統一とか、人力によるデリバリー、ファックスによる送信等を全てシステム上で画面取引に置換えられないかの検討が必要。

(c)　まずどこまで現状業務の複雑さを解消できるかと考え、その後に輸入、輸出、保険、金融分野の特殊事情を付加していけばよい。（原産証明等EDI化しにくいものは手形同様できる限りイメージで送る工夫をする）

(d)　証拠能力、証拠価値、原本性

UNCITRALモデル法（６条、７条、８条）、ここではデータメッセージに含まれる情報が後で参照できるように、アクセス可能であれば紙の文書（証券・文書本体）の機能的等価物であるとみてよい。

○形式的証拠力（民訴325条　新法228条）→契約書をプリントアウト

○証拠調べ→書証か検証か（立法的解決が必要）

○原本性→原本概念はEDI化においては不要とみるべき（証拠方法としてのデータメッセージの信頼性の問題である。）

※「書式の斗い（battle of forms）」→国際取引では、当事者は、自己に有利な内容の契約を締結するため、自己の用意した契約形式をベースとして契約締結を図ろうとすることを指す。これがシステム化を伴うと事実上標準化していく（江頭憲治郎、「商取引法 第２版」（弘文堂）52～53頁参照）。

④　貿易面の金融EDIを担保する制度

(a)・電子的船荷証券に関するCMI規則（万国海法会　1990年）

・INCOTERMS（インコタームス）→（国際商業会議所　1990年）

・複合運送書類に関する規則→（国際商業会議所、国連貿易開発会議　1991年）

・信用状統一規則　（「UCP500」→海上船荷証券以外の運送書類につき規定　1993年）

・BOLEROプロジェクト実験（1996年）

・UNCITRAL電子商取引モデル法（1996年）

(b)　上記の例はいずれも、船荷証券からそれ以外の運送証券に電子化が進み、貿易取引全体のEDI化進展の事実を示している。今後の展開をみていく点では、BOLEROとUNCITRALモデル法が重要である。

(c)　複雑な貿易金融手続をEDI化するためには以下の要素が重要となる。

ⅰ．認証（authentication）

署名には「作成者と記載内容の結合」という認証行為が存在するが、これが電子式船荷証券でも保全されなければならない（裏書も同様）。

発信者及びシステムの身元を証明する手段→暗号化、デジタル署名

ⅱ．完全性保証（integrity）

メッセージデータ（証券内容）が、故意又は偶然に改変されるのを防止する手段が必要→メッセージ認証

ⅲ．否認防止（non repudeation rule）

メッセージデータが送信・受信されたことを証明し、送信・受信者が送・受信について否認することを防止する→暗号化、公証機関設置（CA）

※この目的でBORELOでは、中央登録機関（CR）やCA、レジストレーションオーソリティ（RA→荷主に秘密キーを渡す）などが設置されている。

⑤　セキュリティと秘密（ノウハウ）の保全

(a)　セキュリティには、ハード・ソフト・人的側面がある。金さえ掛ければいいわけではない。

i．システム構成

○クローズド型かオープン型か → いずれにせよシームレスにすべきである。

○利用する回線 → 回線交換方式、パケット交換方式、無線方式

ii．ソフト（OS 、アプリケーション、その他ツール等）

暗号ソフトも多種類存在する。将来展望が重要。SWIFT との接続を想定するなら各エリアの情報量はかなり入るような工夫が必要。

iii．責任分担（分界）の原則を明確にする

責任をもつ領域（エリア）と損失発生時の分担額を定める。

(b) 参加会社の営業情報やノウハウが保全される仕組を工夫する。

CMI 規則作成時には、金融機関が中央登録機関（CR）として想定されたため、物流情報が把握される懸念が生じ、当初頓挫したといわれる。従って、この役割は中立的な第三者機関（Trusted third Party）が担うのが望ましい。

i．電子船荷証券の集中管理センターの役割

○グローバルロジスティックスの実現 → コンテナなどパッケージは世界のどこでも確認できる。国内的には全銀データ通信、SWIFT、SHIPNET、NACCSとの接続が可能になれば効用は更に高まる。

○金融EDI 面 → 証券データの磁気ファイル化を進める際に、担保エリアを設け担保設定と解除を簡単にできるようにする。担保に関しては第三者への公示への配慮も重要である。又輸出商の債権を輸出地銀行が買い取るファクタリングの構成もしやすくなり、証券の集中管理機構設定も可能となる。

ii．第三者機関にはその信頼性を担保する制度が要求される。

情報の漏洩、ハッカーの侵入など備えるのみでなく、当該機関そのものの信頼性を保つシステムチェック制度（公的規則も含める）を考えるべきである。

（参考文献）

「業際 EDI の動向」産業と情報 第33号　産業情報化推進センター

八尾晃「国際取引と電子決済」　東京経済情報出版

Ⅱ. 参考資料

1　データ交換協定書（参考試案）英訳

昨年度検討し作成しました「データ交換協定書（参考試案）」の条文を室町委員により英訳してもらったものです。解説の部分につきましても、近々作業部会で英訳することを予定しております。

Data Interchange Agreement (Reference Model)

(Tentative translation)

This Agreement made and entered into by and between _____ ("Seller") and _____ ("Purchaser") establishes an agreement to facilitate an individual agreement based upon continuing commercial transaction ("Transaction) of the products prescribed in Schedule attached hereto by an electronic data interchange("EDI").

Article 1. Implementation of Data Interchange

The parties hereto agree that an individual agreement of the Transactions is completed by EDI.

Article 2 Operation Manual

1. A system required for EDI, a transmission protocol, a message configuration, type of data to be transmitted, system operation time, and/or other details shall be defined by the data interchange operation manual (the "Operation Manual") mutually agreed by the parties.
2. The parties hereto agree that the Operation Manual shall be an integral part of this Agreement and provide the same effects as this Agreement.
3. When the Operation Manual shall be modified or amended by reason of the alteration of the system or other reason, the parties hereto shall negotiate for agreement including but not limited to the matter which party should bear costs for this modification or amendment.

Article 3 Procedure for Security and Reliability

The parties hereto should carry out all or any of the procedures prescribed below for a secured data interchange and agree that the details of those procedures should be defined in the Operation Manual;

(1) Procedure for confirming the identity of an originator,

(2) Procedure for confirming the originator's authority to create data,

(3) Procedure for isolating data input errors,
(4) Procedure for confirming data integrity during data transmission,
(5) Other items agreed to by the parties hereto.

Article 4 Data Transfer.

Data shall be transferred into the designated mail box according to a method prescribed in the Operation Manual.

Article 5 Treatment of Non-readable Data.

1. If transferred data cannot be readable, the data addressee shall provide the originator with the fact by _____ immediately after the addressee has known it.
2. If the originator has been notified according to the above provision, it shall be considered as having withdrawn the data.

Article 6 Acknowledgment

1. Either party hereto may request the other party to provide the acknowledgment of transferred offering or acceptance data. This acknowledgment shall be provided by the method of _____ unless otherwise specified.
2. If above acknowledgment has been received, the transfer of the offering or acceptance data is deemed as having been completed and if such an acknowledgment has not been received such data is deemed as having been not completed.

Article 7 Finality of Data Contents

The parties hereto agree that, if data has been originated and transferred according to the procedure for security and reliability prescribed in each Paragraph in Article 3, each content of date transferred shall be finalized as the confirmed items.

Article 8 Establishment of Individual Agreement

An individual agreement of the Transactions shall be established when

acceptance data is received by the Purchaser. However if Seller requests Purchaser the acknowledgment prescribed in Article 6, an individual agreement shall be established upon the reception of such acknowledgment. Notwithstanding above when the Parties hereto agree any separate definitions the parties hereto shall follow such definition.

Article 9 Data Storage and Issue

1. Each party shall store and maintain data originating and receiving and deliver such data to the other party upon request of other party. However the cost of printing-out, duplication or other processing , if any, shall be born by the requesting party.
2. Details of storage and delivery shall be defined in the Operation Manual.

Article 10 Imposition of Costs

Costs for data interchanges defined in this Agreement shall be born by the parties hereto according to a separate agreement.

Article 11 System Operation

1. Each party shall provide, maintain and operate its own system necessary for smooth and reliable EDI.
2. Dispositions to be taken against system errors or system failure shall be defined in the Operation Manual.

Article 12 Relationships with Basic Agreement

If there is a discrepancy between the provisions in this Agreement and those of the Basic Agreement dated _____ by the parties hereto the provisions of this Agreement shall have the prevailing effect..

Article 13 Term

This Agreement shall be in full force in the period beginning on _____ and ending on _____ . Unless either party hereto provides the written notice of rejecting renewing or offering the modification of the contents of this Agreement to the other party not later than three (3) months before the

expiration hereof, this Agreement shall be effective for further _____ years under the same terms and conditions, and shall be updated thereafter on this temporal basis.

Binding signature

Date: _____

the Purchaser:	the Seller:
Name: _____	Name: _____
Address: _____	address: _____
Sign.: _____	Sign.: _____

2. ITEF Internet Draft

Internet 上でEDIを行うことについて、ITEFの中のWG（Electronic Data Interchange-Internet Integration (ediint))で検討を行っています。まだ検討途中ですが、参考にご紹介します。一応和訳していますが、不明の点は原文（http://www.ietf.org/html.charters/ediint-charter.html)を参照して下さい。

(ITEF（The Internet Engineering Task Force）：
Internet Society (ISOC) の中で、規格等を検討しているグループ

2.1 MIMEベースの安全なEDI (MIME-Based Secure EDI)

インターネット・ドラフト
draft-ictf-ediint-as1-01.txt
Nancy Turaj, Mitre Corp.
Rik Drummond, Drummond Group

Mats Jansson, LiNK
Chuck Shih, Actra

1996年11月19日

MIMEベースの安全なEDI

本覚書の状態

本文書は、インターネット・ドラフトのひとつである。インターネット・ドラフトとは、インターネット・エンジニアリング・タスクフォース（IETF）、同エリア、及び同作業グループの作業文書である。他のグループも、インターネット・ドラフトとして作業文書を配布可能である点に注意すること。

インターネット・ドラフトは、最高で6ヶ月間有効な草案文書であり、いつでも他の文書により更新、差し替え、あるいは廃棄される可能性がある。インターネット・ドラフトを参考資料として使用したり、「進行中の作業」として以外に引用することは不適切である。

インターネット・ドラフトの現状について知るために、ftp.is.co.za（アフリカ）、nic.nordu.net（ヨーロッパ）、munnari.oz.au（環太平洋）、ds.internic.net（米国東海岸）またはftp.isi.edu（米国西海岸）上のインターネット・ドラフツ・シャドウ・ディレクトリに含まれている「lid-abstracts.txt」リストをチェックしていただきたい。

要約

本文書は、MIME及びパブリック・キー暗号作成法を利用して、EDI文書を安全に交換する方法について記している。

フィードバックに関する指示：

本草案に関してフィードバックを希望する場合は、以下のガイドラインに従うこと。

- 主体（Subject）フィールドに「AS#1」と記入して、mjansson@agathon.com宛に、e-mailでフィードバックを送信する。
- 貴殿が言及している部分に関して具体的に示すこと。できれば修正が必要な箇所を引用して、その後に貴殿のコメントを書いてほしい。
- あるテキストを貴殿の提案するテキストと差し替えることを推奨される場合も、差し替えるべき部分を引用し、問題となる部分を明確にすること。
- 基本的な方法について質問する場合は、そのことを我々にわかるように示してもらいたい。我々はその問題をediintoリストに載せ、後から協議する。協議の内容をフォローするためには、ietf-ediint@imc.org.で申し込む必要がある。

目次

1．序文

執筆者一同は、貴重な、また非常に綿密なフィードバックを有するチームを提供していただいた、Carl Hage氏に対して心から感謝の意を表したい。Carl氏らの参加を得られなければ、当該技術のユーザにとって有益な方法でこれらの作業を終えることは困難なものとなった。

インターネットでのEDIに関する前の作業では、EDIデータ向けのMIME内容タイプを指定することに焦点を当てた（[2] RFC 1767）。本適用可能性説明書は、RFC 1767を発展させ、一連の包括的なデータの機密保護に関する特性、特にデータの機密、データの完全性／真正、起点の非拒否（non-repudiation）、受信確認の非拒否に関する使用を明記する。本草案は最新のRFC及びインターネット・ドラフトを承認しており、できる限り「再創作」しないように務める。

以下に記されているように（3.1.8）、「受信確認（receipts）」の領域を強化することにより、以下のRFC及び草案を利用し、また同草案に従って、EDIに基づく安全なインターネットMIMEが完成される。

－RFC 821 SMTP
－RFC 822 テキスト・メッセージ形式
－RFC 1521 MIME
－RFC 1767 EDI内容タイプ
－RFC 1847 MIMEに関する機密保護複数パート
－RFC 1892 複数パート／報告
－インターネット・ドラフト：　メッセージ処置通知（fajman）
－RFC 2015 MIME/PGP（elkins）
－インターネット・ドラフト：　S/MIME仕様（dusse）

ここでの我々の意図は、これらがどのように継ぎ合わされ、また本適用可能性説明書に従うためにユーザ・エージェントに求められることを明確かつ正確に定義することである。

2．概観

2.1　MIME EDIに関する機密保護ガイドラインの目的

これらの仕様の目的は、通常期待される機密保護特性の一部または全部を引き合いに出して、EDIユーザ・エージェント間の相互操作性を確保することである。本標準はまた、厳密なEDIの使用に限定されるのではなく、安全な方法で、インターネットを介してビジネスデータを交換する必要がある、いかなるエレクトロニック・コマース（電子商取引）にも適用される。

2.2　定義

2.2.1　用語

EDI	電子データ交換
EC	エレクトロニック・コマース（電子商取引）
受信確認	EDI/EC交換の受信確認を通知するために、受信側から送信側に送られる機能メッセージ
署名付き受信確認	上記と同じであるが、ディジタル署名が付いている
メッセージ処置通知（MDN）	受信確認または署名付き受信確認が、インターネット・メッセージング内で完了される方法
受信確認の非拒否（NRR）	NRRは、EDI/EC交換の起点である送信者が、受信者から返送さ

	れてくる署名付き受信確認を確認した際に発生する「法的事象」である。NRRは、機能メッセージまたはテクニカル・メッセージではない。
PGP/MIME	MIME機密保護複数パート[6]と融和された、プリティー・グッド・プライバシー（PGP）標準（Zimmerman）に基づく、ディジタル・エンベロープ式機密保護
S/MIME	暗号署名及びまたは符号化サービスをインターネットMIMEメッセージに付加するためのプロトコル

2.2.2　安全な伝送ループ

機能要件文書、[9]「相互操作可能なインターネットEDIに関する必要条件」（www.ietf.org.で参照可能）は、EDIの機密保護、及びEDIの機密保護の必要性及び使用に関わるユーザ／ビジネス関連処理に関する広範囲の情報を提供している。本文書においては、読者が要件文書に通じているものと想定している。

本文書は、インターネットのメッセージング移送を利用する、機密保護が適用されているEDI内容の交換に関する形式及びプロトコルに焦点を置いている。

EDIの「安全な伝送ループ」には、「署名付き受信確認」を要求して、署名付きかつ符号化されたEDI交換を他方の組織に送信する組織、さらに当該「署名付き受信確認」を送信側の組織に送り返す受信側の組織を伴う。言い換えれば、以下のことが行われる。

－EDI/ECデータを送信する組織が当該データを符号化し、PGP/MIMEまたはS/MIMEを利用して、ディジタル署名を提供する。さらに、同組織は「署名付き受信確認」を要求する。

－受信側の組織がメッセージを復号し、署名を確認し、結果的にデータの完全性と送信者の真正が証明される。

－受信側の組織は次に、前段階からのハッシュに関して、署名形式で「署名付き受信確認」を送信する。

上記は、実施されれば、全ての機密保護要件を満たすであろう機能性について記している。但し本仕様は、ユーザがEDIの取引相手とこれらの特性を展開させたいと希望する程度を決定できる完全な柔軟性を残している。

2.2.3　受信確認の定義

EDI/EC交換の受信確認を通知するための機能行動及びメッセージの両方に使用される用語は、「受信確認（receipt）」または「署名付き受信確認（signed receipt）」である。前者は、署名されていなかった交換に関して、受信確認が通知される場合に使用され、したがって署名なしの受信確認ということになる。後者は、署名されていた交換に関して、受信確認が通知される場合に使用され、したがって署名付きの受信確認になる。ここでの規則は次の通りである。受信確認が要求される場合、最初の交換が署名付きであった場合にのみ、受信確認にも署名がなされる。「受信確認」とともに頻繁に使用される用語が、「受信確認の非拒否（Non-repudiation of Receipt: NRR）」である。NRRは、交換の最初の送信者が、「署名付き受信確認」の送信者及び内容を確認した場合にのみ発生する法的事象に言及する。NRRは署名が無ければ不可能である点に注意すること。

2.3　想定

2.3.1　EDI処理想定

－符号化される対象はEDI交換である

本仕様は、典型的なEDI交換を、機密保護特性に従う最低レベルの対象であると想定している。ANSI X12では、これはセグメントのISAとIEAの中間の何か、及び両セグメントを含む何かを意味する。EDIFACTでは、これはセグメントのUNA/UNBとUNZの中間の何か、及び両セグメントを含む何かを意味する。言い換えれば、エンベロープ・セグメントを含むEDI交換は、安全な移送中は完全で、解読不能な状態のままである。

－EDIエンベロープ・ヘッダは符号化されている

上記内容と一致して、EDIエンベロープ・ヘッダは、MIMEパッケージ内では目に見えない。VAN-to-Internetルーチンを最適化するためには、将来、エンベロープ情報の一部を目に見えるように引き出す方法を定義する作業を行う必要が出てくるかもしれない。しかし本仕様は、それに関するいかなる詳細にも触れない。

－X12.58及びUN/EDIFACTの機密保護に関する考慮

最も一般的なEDI標準である、ANSI X12及びEDIFACTは、機密保護に関する内部規定を定義している。X12.58はANSI X12の機密保護メカニズムであり、AUTACKはEDIFACTの機密保護を規定している。本仕様は、これらの機密保護標準の使用または非使用を命ずるものではない。両標準はともに、重複するかもしれないが、本仕様と完全に両立する。

2.3.2　柔軟性想定

－符号化または非符号化データ

本仕様は、EDIデータが符号化により保護されていない、または保護されているかのいずれかの場合のEDIメッセージ交換を考慮に入れている。

－署名付きまたは署名なしデータ

本仕様は、最初のEDI伝送の際にディジタル署名がある、または同署名がない場合のEDIメッセージ交換を考慮に入れている。

－受信確認の使用または非使用（「署名付き受信確認」に関して要求される署名）

本仕様は、受信確認通知の要求がある、または同要求がない場合のEDIメッセージ伝送を考慮に入れている。しかし受信確認通知が要求される場合、署名は最初のEDI伝送と返送される受信確認の両方の一部として要求される。

フォーマッティングの選択

本仕様は、以下の通り、機密保護が適用されているEDIの内容をフォーマットする２つの方法の使用を定義している。

－PGP/MIME

－S/MIME

本仕様は、[4] MIME Security with Pretty Good Privacy (PGP)及び[8] S/MIME Specification from RSA Security, Inc.に表わされるように、PGP/MIMEに関するインターネット・ドラフトに記されるガイドラインに依存している。本仕様の準拠は、少なくとも、これらの方法のひとつがサポートされていることを命ずる。

－ハッシュ機能、メッセージ要覧の選択

署名が使用される際には、選択された方法（PGP/MIMEまたはS/MIME）によって別に明示される場合を除いて、MD5チェックサム・ハッシュ機能が推奨される。

要約すると、いかなる取引関係においても、以下の８つの順列が可能である。

（1）送信者が符号化されていないデータを送信し、受信確認を要求しない。
（2）送信者が符号化されていないデータを送信し、受信確認を要求する。受信者は受信確認を送り返す。
（3）送信者は符号化されたデータを送信し、受信確認を要求しない。
（4）送信者は符号化されたデータを送信し、受信確認を要求する。受信者は受信確認を送り返す。
（5）送信者は署名付きのデータを送信し、署名付きの受信確認を要求しない。
（6）送信者は署名付きのデータを送信し、署名付きの受信確認を要求する。受信者は署名付きの受信確認を送り返す。
（7）送信者は符号化された、署名付きのデータを送信し、署名付きの受信確認を要求しない。
（8）送信者は符号化された、署名付きのデータを送信し、署名付きの受信確認を要求する。受信者は署名付きの受信確認を送り返す。

注意：　ユーザはこれら８つの可能性のいずれをも選択できるが、上述の「安全な伝送ループ」に記述されている機密保護特性の一式全てを提供するのは、（8）の例のみである。
注意：　署名付きの受信確認を要求した場合は、署名付きの受信確認を入手しなければならない。署名のない受信確認を要求した場合は、署名のない受信確認を入手しなければならない。

3．EDI MIMEメッセージの構造

以下の項では、様々な機密保護特性を利用して、EDI MIMEメッセージの構造について記している。署名付きの受信確認が戻ってくると予想される場合は、最初のEDI伝送もまた署名付きでなければならなかったことに注意してほしい。

下に示される構造は、以下のRFC及びインターネット・ドラフトに概要が記載されている仕様の使用を紹介しており、また構造そのものについて説明する前に、各文書が寄稿する内容について簡単に概観している。

注意：　以下の例は、あくまでも例である。これらの例に従って、符号化してはならない。各ケースにおける正しい文法を明記しているRFCを参照するように。

3.1　参照されるRFC及びそれらの貢献

3.1.1　RFC 821 SMTP [7]

これは全てのMTAが厳守しなければならない核心的なメール転送標準である。

3.1.2　RFC 822 テキスト・メッセージ形式[3]

メッセージのヘッダ・フィールド、及びメッセージを構築する部分を定義する。

3.1.3　RFC 1521 MIME [1]

これは基本的なMIME標準で、本標準をはじめとして、全てのMIME関連のRFCがこれに基づいている。主要な貢献としては、符号化ガイドラインに加えて、使用される最小共通分母として７ビットのUS-ASCIIを構築する、「内容タイプ（content type)」及びサブタイプ「複数パート(multipart）」の定義が含まれる。

3.1.4　RFC 1847 MIME機密保護複数パート[6]

本文書は、複数パート／符号化及び複数パート／署名付きといった、MIMEに関する機密保護複

数パートを定義している。

3.1.5　RFC 1892 複数パート／報告[10]

本RFCは、複数パート／報告の内容タイプ、すなわち受信確認機能性に関してMDNドラフト（fajman）が依存しているものの使用を定義している。

3.1.6 RFC 1767 EDIの内容[2]

本RFCは、ANSI X12（アプリケーション／EDI-X12）、EDIFACT（アプリケーション／EDIFACT）、及び相互に定義されたEDI（アプリケーション／EDI-Consent）に関する内容タイプ「アプリケーション」の使用について定義している。

3.1.7　RFC 2015 PGP/MIME [4]

本RFCは、MIME PGPの内容を定義する「複数パート／符号化」、「複数パート／署名付き」、「アプリケーション／PGP符号化」、「アプリケーション／PGP署名」といった内容タイプの使用について定義している。

3.1.8　インターネット・ドラフト（fajman）：　メッセージ処置通知[5]

本インターネット・ドラフトは、メッセージ処置通知（MDN）が要求される方法、及びMDNの構造について定義している。

注意：　これは、我々が「現状のままで」採用することができなかった仕様にすぎない。「X-」で始まる拡張フィールド名は、標準フィールドとしては定義されないと考えられる。「X-」で始まらないMDNフィールド名は、Internet Assigned Numbers Authority（IANA）に登録する必要があり、またRFCの中に記述される必要がある。本文書に記述されるX-Received-MICフィールドは、IANAに登録されることになる。

3.1.9　インターネット・ドラフト（dusse)：　S/MIMEメッセージ仕様[8]

本仕様は、MIMEがPKCS7署名及びエンベロープ情報を載せる方法について定義している。

3.2　語彙

<recipient email>	受信側組織のEDI処理システムのemailアドレス
<sender email>	送信側組織のEDI処理システムのemailアドレス
<date>	伝送日
<EDI standard>	「EDI-FACT」、「EDI-X12」、または「EDI-consent」
<encoding>	「Quote-printable」または「Base64」
<EDI Object>	ANSI X12またはEDIFACTのEDI交換、あるいは相互に合意されているエレクトロニック・コマース・ファイル
<char set>	「us-ascii」または「iso-8859-1」（iso-8859-1が使用される場合は、ほとんどのケースで符号化は「Quoted printable」または「Base 64」が要求されることに注意。
<hash symbol>	「md5」または「sha1」
<pgp control information>	－受信者のパブリック・キーのキーID －セッション・キー（対称） －タイムスタンプ －送信者のパブリック・キーのキーID －メッセージ要覧の主要な２つのオクテット －メッセージ要覧 －ファイル名

－タイムスタンプ

<RKCS#7 control information - enveloped>

－contentType = EnvelopedData
－version = Version
－recipientInfos = RecipientInfos

－contentType = Data
－contentEncryptionAlgorithm =
－ContentEncryptionAlgorithmIdentifier

－encrytedContent =

<PKCS#7 control information - signed>

－ContentType = SignedData
－version = Version
－digestAlgorithms = DigestAlgorithmIdentifiers
－contentType = Data
－content =

<PKCS#7 signature information>

－signerInfos = SignerInfo

注意： 以下の例は、あくまでも例にすぎない。これらの例は、例証のみを目的として提示されている。実際の文法及びプロトコル定義に関しては、「７．参考資料」に記載されているRFCまたはドラフトを参照するように。

3.3 EDI MIMEメッセージの構造－符号化なし／署名なし

To:	<recipient email>
Subject:	
From:	<sender email>
Date:	<date>
Mime-Version:	1.0
Content-Type :	Application／<EDI standard>
Content-Transfer-Encoding:	<encoding>

<EDI object>

3.4 EDI MIMEメッセージの構造－S/MIME

3.4.1 S/MIMEの概観

S/MIME、すなわち安全な／多目的インターネット・メール拡張（Secure/Multipurpose Internet Mail Extensions）は、本物確認、メッセージの完全性、起点の非拒絶、機密保護の暗号法によるセキュリティ・サービスがインターネットMIMEメッセージに適用される際の、形式及び手順を定める。

S/MIMEは、draft-dusse-mime-msg-spec-00.txtドラフトで明記されており、S/MIME実行ガイドはRSA Data Securities, Inc.から入手可能である。

本適用可能性説明書は、インターネットでEDIを送信する際に、S/MIMEを利用する上で必要とさ

れる実行要求及び推奨事項を明記している。同実行要求及び推奨事項は、S/MIME EDI実行間の基本レベルの相互操作可能性を保証することを意図している。

注意： S/MIME実行ガイド第２版は、移出を目的とする利用に関しては限定プロファイルを、ドメスティックな利用に関しては非限定プロファイルを指定している。これらのプロファイルは、準拠したS/MIME実行がサポートしなければならない暗号アルゴリズム、及びキーの長さを指定している。インターネットEDIに関しては、これらのプロファイルを守ることが推奨されている。しかし、暗号アルゴリズム及びキーの長さは、取引パートナーシップにより定められる必要のあるパラメーターであり、S/MIME標準の指定内容とは変わる可能性がある。

内容タイプ（Content Types）：

SignedAndEnvelopedDataという内容タイプは、インターネットでEDIを送信する際には使用してはいけない。signedAndEnvelopedData内容の各署名者に関するissuerAndSerialNumberが明確に残されるという事実に関して、異論が出ている。同情報は、メッセージの署名者のアイデンティティーを引き出すために利用可能である。signedAndEnvelopedDataの利用はまた、初期に署名された内容に加わるが、それとは別個である情報に署名する能力を妨げる。S/MIMEの「本物確認された属性」の利用は、インターネットのEDIに関しては要求されない。普通は、EDI MIME内容に署名するだけで十分だからである。

S/MIME実行ガイド第２版は、入力、出力メッセージの両方に関して、エンベロープ入りメッセージ内での署名されたメッセージ形式のネスティングをサポートする従順なS/MIMEエージェントを要求する。このEDI AS#1仕様はまた、エンベロープ入りメッセージ内のネストされた署名メッセージのサポートを要求する。したがって、インターネットでEDIを送信する目的でS/MIMEを使用する際には、２段階のプロセスが実行される。最初に、ユーザ・エージェントがアプリケーション／X-pkcs7のmime署名メッセージを作成し、同メッセージをアプリケーション／x pkcs7-mimeエンベロープ・メッセージの作成に対するインプットとして利用する。

復号され、署名されたアプリケーション／x-pkcs 7-mimeタイプが含まれていることが判明している、入力エンベロープ入りメッセージの受取り手は、署名された内容を処理し、署名の状態と対応する「データ」内容をメッセージ処置通知処理に提示しなければならない－－メッセージ処置通知の要求がなされた場合。そうでない場合は、「データ」内容は一般のMIMEプロセッサにパスされる。

「データ」内容タイプは、signedData及びenvelopedData内容タイプ内の内容として、セキュリティ・サービスが適用されているMIMEメッセージ内容を示すために使用される。インターネット上のEDIを目的とする場合は、同「データ」内容タイプはRFC 1767指定のMIME EDI内容、あるいは複数パート内容の一部として、RFC 1767 MIME EDI内容を有するMIME複数パート内容を含む。

署名付きメッセージ・タイプ（Signed Message Type）：

S/MIME仕様は、signedData内容形式のサポートを要求し、複数パート／署名付き形式のサポートを推奨する。インターネット上のEDIにおける使用に関しては、メッセージの本物確認、完全性、及び起点の非拒絶が要求される場合は、signedData内容形式に関するサポートが要求される。複数パート／署名付き形式のサポートに関する大きな価値は、S/MIME可能でないエージェントが、署名されたボディの内容を処理できることである。

複数パート／署名付き形式は、署名されているメッセージを、その全てがS/MIME可能なエージェントを持っているかわからない一連の受取り手に送る場合に推奨される。インターネット上のEDI処理にS/MIMEを使用している取引相手は、S/MIME可能なエージェントを持っていることは確実なので、複数パート／署名付きはそのユーティリティの多くを失う。したがって、インターネットEDIで

の使用に関しては、複数パート／署名付き形式のサポートは任意選択となる。

3.4.2　例：　S/MIME－署名のみ

To:	<recipient email>
Subject:	
From:	<sender email>
Date:	<date>
Mime-Version:	1.0
Content-Type:	application／x-pkcs7 mime
Content-Transfer Encoding：	base64

<PKCS#7 control information - signed>

&MIME-Version:　1.0
&Content-Type:　Application／<EDI standard>
&Content-Transfer Encoding: <encoding>
&
&<EDI object>

<PKCS#7 signature information>

注意：
－「&」が先頭についている行は、署名（signature）が計算済みであることを示す。
－<PKCS#' control information - signed>は、以下の構成となっている（参照：PKCS#7: RSA LABS, INC.の符号メッセージ構文標準）。

ContentType = SignedData
version = Version
digestAlgorithms = DigestAlgorithmIdentifiers
contentType = Data
content =

注意：　ContentType及びContentを除いて、実際のオブジェクト識別子またはフィールド値は指定されていない。（これらのオブジェクト識別子に関しては、PKCS#7及びRSA Labs, INC.のS/MIME実行ガイド第２版を参照のこと。）

－<PKCS#7 signature information>は、以下の構成となっている。（参照：PKCS#7：RSA LABS, INC.の符号メッセージ構文標準）。

signerInfos = SignerInfo

注意：　signerInfoは、digerstAlgorithm、digestEmcryptionAlgorithm、及びencryptedDigestまたはdigital signatureを含む。signerInfos内で定義されるIssuerAndSerialNumberフィールドは、署名する取引相手のパブリック・キー証明を識別する。インターネットEDIは自己証明を認めるので、このフィールドはissuerの識別された名前に関して、送信側の取引相手の識別された名前を含むことができる。

3.4.3　例：　S/MIME －符号化のみ

To:	<recipient email>

Subject:
From: <sender email>
Date: <date>
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime
Content-Transfer-Encoding: base64

<PKCS#7 control information - enveloped>
&Mime-Version: 1.0
&Content Type: Application/<EDI standard>;
&Content-Transfer-Encoding: <encoding>
&
&<EDI object>

注意：
－「&」が先頭についているテキストは、実際には符号化されているが、わかりやすくするためにテキストとして表示されていることを示す。

－<PKCS#7 control information-enveloped>は、以下のように構成されている（PKCS#7:RSA Labs, Inc.の 符号メッセージ構文標準を参照のこと）。

contentType = EnvelopedData
version = Version
recipientInfos = RecipientInfos

contentType = Data
contentEncryptionAlgotirhm = ContentEncryptionAlgorithmIdentifier
encryptedContent =

注意： contentTypeを除いて、実際のオブジェクト識別子またはフィールド値は指定されていない。（これらオブジェクトに関しては、PKCS#9及びRSA Labs, INC.のS/MIME実行ガイド第２版を参照のこと。）

注意： recipientInfosは、受信者のパブリック・キーで符号化された対称の符号化キーを含む。recipientInfos内で定義されるissuerAndSerialNumberフィールドは、受信側取引相手のパブリック・キー証明を識別する。インターネットEDIは自己証明を認めるので、同フィールドはissureの識別された名前に関して、受信側取引相手の識別された名前を含むことができる。

注意： 一般には、１個のrecipientInfosが指定されるが、RFQsの場合は、n個のrecipientInfosが指定される。

3.4.4 例： S/MIME － 署名及び符号化

EDIインターネットに関して要求されるサポートは、まず第一に、アプリケーション／x-pkcs7-mime signedDataメッセージを作成することであり、次にアプリケーション／x-pkcs7-mime envelopedDataメッセージへのインプットとして、アプリケーション／x-pkcs7-mime signedDataメッセージを伴うアプリケーション／x-pkcs7-mime envelopedDataメッセージを作成することである。

To: <recipient email>
Subject:

From: <sender email>
Date: <date>
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime
Content-Transfer-Encoding: base64

<PKCS#7 control information - enveloped>
*Mime-Version: 1.0
*Content-type: application/x-pkcs7-mime

*<PKCS#7 control information - signed>

*&MIME Version: 1.0
*&Content-Type: Application/<EDI standard>
*&Content-Transfer-Encoding: <encoding>

&<EDI object>

*<PKCS#7 signature information>

注意：
－「&」が先頭についている行は、署名が計算済みであることを示す。
－「*」が先頭についているテキストは、実際には符号化されているが、わかりやすくするためにテキストとして表示されていることを示す。
－<PKCS#7 control information - enveloped>は以下のように構成されている（PKCS#7：RSA Labs, Inc.の符号メッセージ構文標準を参照のこと）。

contentType = EnvelopedData
version = Version
recipientInfos = RecipientInfos

contentType = Data
contentEncryptionAlgotithm = ContentEncriptionAlgorithmIdentifier
encryptedContent =

注意： contentTypeを除いて、実際のオブジェクト識別子またはフィールド値は指定されていない。（これらオブジェクトに関しては、PKCS#9及びRSA Labs, INC.のS/MIME実行ガイド第２版を参照のこと。）

注意： recipientInfosは、受信者のパブリック・キーで符号化された対称の符号化キーを含む。recipientInfos内で定義されるissuerAndSerialNumberフィールドは、受信側取引相手のパブリック・キー証明を識別する。インターネットEDIは自己証明を認めるので、同フィールドはissureの識別された名前に関して、受信側取引相手の識別された名前を含むことができる。

注意： 一般には、１個のrecipientInfosが指定されるが、RFQsの場合は、n個のrecipientInfosが指定される。

－<PKCS#7 signature information>は以下の用に構成される（参照：PKCS#7：RSA Labs, Inc.の符号メッ

セージ構文標準）。

signerInfos = SignerInfo

注意： signerInfoは、digerstAlgorithm、digestEmcryptionAlgorithm、及びencryptedDigestまたはdigital signatureを含む。signerInfos内で定義されるIssuerAndSerialNumberフィールドは、署名する取引相手のパブリック・キー証明を識別する。インターネットEDIは自己証明を認めるので、このフィールドはissuerの識別された名前に関して、送信側の取引相手の識別された名前を含むことができる。

3.5 EDI MIMEメッセージの構造－PGP/MIME

3.5.1 概観

PGPは、署名と符号化の２つの機能サービスを提供するが、現実にはそれらを効果的に実行するために以下の５つの機能を果たしている。

1）ディジタル署名（MD5、RSA）
2）圧縮（ZIP）
3）メッセージの符号化（IDEA）
4）ASCII Armor
5）メッセージの区分化

メッセージを送信するときには、これらのサービスがこの順序で実施される。

第５）項を例外として、これらのサービスはオプションであり、ユーザは署名、符号化、圧縮、ASCII armorを利用するかどうか選ぶことができるが、普通は第２）、４）項は常に利用され、第１）、３）項は以下の３通りの方法で利用される。

1）署名のみ。この場合、ASCII armorはメッセージを読みとれる状態に維持するために、署名ブロックにのみ適用することが可能である。
2）符号化のみ。
3）署名と符号化の両方。

インターネットEDIでの利用に関するPGP/MIMEとRFC 2015の適用可能性については、以下の通り規定されている。

－符号化と署名特性の両方が利用される場合、EDIデータは最初に署名され、次に例に示されるように、２段階のプロセスで符号化される。
－圧縮及びASCII Armorはオプションであり、ユーザにより構成可能である。
以下の例は、圧縮及びASCII armorなしの場合のPGP/MIMEの使用について記述している。当該サービスはPGPにより管理されており、本ドラフトに関してはオプションだからである。

3.5.2 例： PGP/MIME－署名のみ

To: <recipient email>
Subject:
From: <sender email>
Date: <date>
MIME-Version: 1.0
Content-Type: multipart/signed; boundary="separator";

micalg=pgp-<hash symbol> ; protocol="application/pgp-signature"

--separator

&Content-Type: Application/<EDI standard>

&Content-Transfer-Encoding: <encoding>

&

&<EDI object>

--separator

Content-Type: application/pgp-signature

-----BEGIN PGP MESSAGE-----

Version 2.6.2

fgfjhHjhJhgIjhgJGHGJHGJHJHJhghjhJHJuytIYTiutTYT34553//YRytdhfFFOcre/876

JHJHGIUIUgsdIUYgYTRdgggguytUTIUlbXssfdsfdREWrewREWREEWE88POF/DF

frtFFKFG+GFff=

=ndaj

-----END PGP MESSAGE-----

--separator--

注意：

－「&」が先頭についている行は、署名（signature）が計算済みのものである。

3.5.3 例： PGP/MIME－符号化のみ

To: <recipient email>

Subject:

From: <sender email>

Date: <date>

MIME-Version: 1.0

Content-Type: multipart/encrypted; boundary="separator";protocol="application/pgp-encrypted"

--separator

&Content-Type: application/pgp-encrypted

Version: 1

--separator

Content Type: application/octet-stream

-----BEGIN PGP MESSAGE-----

Version 2.6.2

&<pgp control information>

&Content-Type: Application/<EDI standard>;

&Content-Transfer-Encoding: <encoding>

&

&<EDI object>

-----END PGP MESSAGE

--separator

注意：

- 「&」が先頭についているテキストは、実際には符号化されているが、わかりやすくするためにテキストとして表示されていることを示す。
- 「pgp control information」は、以下の内容を含むが、詳細については、PGP仕様またはツールキットを参照するように。

  －受取り手のパブリック・キーのキーID
  －セッション・キー（対称）
  －タイムスタンプ
  －送り手のパブリック・キーのキーID
  －メッセージ要覧の主要な２つのオクテット
  －メッセージ要覧
  －ファイル名
  －タイムスタンプ

3.5.4 例： PGP/MIME 署名及び符号化

ここでの順序は、最初にEDIデータが複数パート／署名ボディとして署名され、次にデータと署名が符号化され、最終的な複数パート／符号化ボディを形成する。以下の要領で行われる。

To: <recipient email>
Subject:
From: <sender email>
Date: <date>
MIME-Version: 1.0
Content-Type: multipart/encrypted; boundary="separator";
protocol="application/pgp-encrypted"

--separator
Content-Type: application/pgp-encrypted

Version: 1

--separator
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version 2.6.2

* <pgp control information>
* Content-Type: multipart/signed; boundary="signed separator";
* micalg=pgp-<hash symbol>; protocol="application/pgp-signature"
*
* --signed separator
* &Content-Type: Application/<EDI standard>
* &Content Transfer Encoding: <encoding>

```
*     &
*     &<EDI object>
*
*  --signed separator
*   Content-Type: application/pgp-signature
*
*     -----BEGIN PGP MESSAGE-----
*     Version 2.6.2
*
*     fgfjhHjhJhgIjhgJGHGJHGJHJHJhghjhJHJuytIYTiutTYT34553//YRytd
*     /GIUIUgsIUYgYTRdgggguytUTIUlbXssfdsfdREWrewREWREEWE88POF/DF
*     frtFFKFG+GFff=
*     =ndaj
*     -----END PGP MESSAGE-----
*
*  --signed separator
   ----END PGP MESSAGE

--separator--
```

注意：

- 「&」が先頭についている行は、署名が計算済みのものである。
- 「*」が先頭についているテキストは、実際には符号化されているが、わかりやすくするためにテキストとして表示されていることを示す。
- 「pgp control information」は、以下の内容を含むが、詳細については、PGP仕様またはツールキットを参照するように。
  - 受取り手のパブリック・キーのキーID
  - セッション・キー（対称）
  - タイムスタンプ
  - 送り手のパブリック・キーのキーID
  - メッセージ要覧の主要な２つのオクテット
  - メッセージ要覧
  - ファイル名
  - タイムスタンプ
- RFC 2015は、上記内容を組み合わせたやり方で処理する別の方法を認めている。しかしEDIを目的とする場合は、MIME安全複数パート（MIME Security Multiparts）[4] RFC 1847に基づく上記方法を要求する。この方法は、署名と符号化を、最初にデータに署名し、次にそれを符号化するという２段階のプロセスで実行する。この方法はまた、PGPの推奨事項とも一致している。

4．受信確認

4.1 序文

受信確認の非拒否（non-repudiation of receipt: NRR）または署名付き受信確認を提供するために、受信側取引相手のUA（ユーザ・エージェント）が、draft-ietf-receipt-mdn-01で規定されるメッセージ処置通知（MDN）を実施することになっている。その後、メッセージ処置通知はディジタル方式で署名され、複数パート／署名付き内容の一部として、送信側取引相手に戻される。

EDIインターネットを実施するときに、署名付き受信確認に関して要求されるサポートは以下の通りである。

1）複数パート／報告を作成する：　report-type=disposition notification
2）メッセージ処置通知上のMICを計算する。
3）ディジタル方式でMICに署名する。
4）第１ボディ・パートとして、メッセージ処置通知を伴う複数パート／署名付き内容を作成し、第２ボディ・パートとして、署名済みMICがメッセージ処置通知上で計算される。
5）署名された受信確認を送信側取引相手に戻す。

MDNは、署名付き、または署名付きかつ符号化されたEDI交換を送信した送信側取引相手に、以下の内容を通知するために使用される。

1）受信側取引相手は、送信されたEDI交換の受取りを通知する。
2）受信側取引相手は、EDI交換の送信者が本物であることを確認した。
3）受信側取引相手は、受信したEDI交換が完全な状態であることを確認した。

EDI交換が、S/MIMEまたはPGP/MIMEのどちらの形式で送信されたかどうかにかかわらず、受信側取引相手のUAは、以下の基本的な処理を提供しなければならない。

1）送信されたEDI交換が符号化されている場合は、受信者のプライベート・キーを使って、符号化されている対称キー、及び初期設定ベクトル（該当する場合は）を復号する。
2）復号された対称符号キーを使用して、EDI交換を復号する。
3）受信側取引相手は、送信者のパブリック・キーを使用して、メッセージ内の署名が本物であることを確認する。同確認のアルゴリズムは以下のように機能する。
　a）署名に含まれるメッセージの完全性チェック（MICまたはメッセージ要覧）が、送信者のパブリック・キーを使用して復号される。
　b）受信したメッセージ内の署名付き内容（RFC1767に関しては、MIMEヘッダ、及び符号化されたEDIオブジェクト）上のMICが、送信側取引相手が使用したものと同じ片方向のハッシュ機能を使って計算される。
　c）署名から抽出されたMICが、送信側取引相手が使用したのと同じ片方向のハッシュ機能を利用して計算されたMICと比較される。
4）受信側取引相手は、MDNをフォーマットし、計算されたMICをMDN拡張フィールドにセットする。
5）受信側取引相手は、RFC 1847にしたがって、複数パート／署名付きMIMEメッセージを作成する。
6）MDNは複数パート／署名付きメッセージの最初の部分であり、MIMEヘッダを含めて、同MDNに関してディジタル署名がなされる。
7）複数パート／署名付きメッセージの２番目の部分は、ディジタル署名を含む。複数パート／署名付きで指定される「プロトコル」オプションは以下の通りである。

S/MIME：protocol ＝ 「application/pkcs-7-mime」
PGP/MIME：protocol＝「application/pgp signature」

EDI交換及びRFC 1767 MIME EDI内容ヘッダは、実際に複数パートのMIME内容タイプの一部となり得る。EDI交換が複数パートのMIME内容タイプの一部である場合、MICは、MIMEヘッダを含む、複数パートの内容全体にわたって計算される。次に、EDI交換を含む複数パートのMIME内容は、PKCS #7かPGP形式のいずれかでエンベロープに入れられる。MDNで返送された署名付きMICは、複数パートのMIME内容全体に関する署名付き受信確認となる。

署名付きMDNは、EDI交換の送信者が受け取った時点で、送信者により以下のように利用可能とな

る。

1）EDI交換が送信され、届けられ、受信側取引相手により承認されたという承認として。受信者は、署名付きMDNで送られたメッセージのオリジナルのメッセージidを戻すことにより、この作業を行う。
2）EDI交換の完全性が受信側取引相手により確認されたという承認として。受信者は、署名付きMDNのX-Received-MICフィールドで受信されたEDI交換（及び1767 MIMEヘッダ）の計算済みMICを戻すことにより、この作業を行う。
3）受信側取引相手が、EDI交換の送信者が本物であることを確認したという承認として。
4）MDNに関して計算された署名付きMICが、受信者のパブリック・キーを利用して、送信者が復号に成功した場合の、受信確認の非拒否として。

4.2　署名付き受信確認の要求

メッセージ処置通知（Message Disposition Notifications）は、draft-ietf-receipt-mdn-01.txtに従って要求される。受信側のユーザ・エージェントが、メッセージ処置通知を発行するよう要求するには、以下のヘッダを送信するメッセージの中に入れればよい。

mdn-request-header = "Disposition-notification-to" ":" address

アドレス・フィールドは、RFC 822 user@domain addressとして指定されており、またメッセージ処置通知の返送アドレスである。

実行者への注意：　本RFCは、EDI交換が取引相手により受信される場合はいつでも、署名付き受信確認の送信を妨げない。署名付き受信確認の送信は、構成可能なパラメーターで行うことができ、また署名付き受信確認は、オリジナル・メッセージが受信確認要求を含んでいない場合でも、戻すことができる。

4.3　メッセージ処置通知形式

メッセージ処置通知の形式は、draft-ietf-receipt-mdn-01.txtに指定されている通りである。インターネットを介するEDIの中で使用する場合には、以下の形式が使用される。

- content-type - per RFC1892 and the ietf-receipt-mdn specification
- reporting-ua-field - per ietf-receipt-mdn specification
- mdn-gateway-field - per ietf-receipt-mdn specification
- original-recipient-field - per ietf-receipt-mdn specification
- final-recipient-field - per ietf-receipt-mdn specification
- original-message-id-field - per ietf-receipt-mdn specification
- disposition-field - for EDI use:

    * autoprocessed（自動処理）－受信された内容が適切に処理されている場合
    * decryption_failed（復号の失敗）－受信者が内容を復号できなかった場合
    * authentication_failed（本物確認の失敗）－受信者が送信者が本物であるか確認できなかった場合
    * integrity_check_failed（完全性チェックの失敗）－受信者が内容の完全性を確認できなかった場合

- extension field （拡張フィールド）－RFC 1767の指定内容タイプ、及びRFC 1767の内容タイプを含む複数パートの指定内容タイプに関する署名付き受信確認をサポートするため

に、以下の拡張フィールドが付加される。拡張フィールドは、受信された内容が適切に処理された場合にのみ送られる。

- extension field = "X-" "Received-MIC" ":" MIC

MIC、すなわちメッセージ完全性チェックは、受信されたEDI交換及びRFC 1767 MIME内容タイプ情報、あるいはRFC 1767 MIME EDI内容情報を含む複数パートのMIME内容に適用された片方向のハッシュ機能の結果として定義される。MICはまた、MD5の片方向ハッシュ機能を利用する場合に、メッセージ要覧として言及される。

4.4 メッセージ処置通知処理

4.4.1 大型ファイル処理

SMTPを介して送信される大型のEDI交換は、複数のメッセージ転送エージェントにより、自動的に細分化される。メッセージのサブタイプである「パーシャル（partial）」は、RFC 1521で定義されており、大型オブジェクトがメールの別個の部分として届けられ、受信側のユーザ・エージェントにより自動的に再組立てされることを認めている。"partial"というメッセージの使用は、様々なメッセージ転送エージェントによる大型メッセージの細分化を緩和する助けとなるが、問題を完全に除去するわけではない。それでも、一個一個のパーシャル・メッセージが、再組立てされる際に、それぞれが同様にパーシャル・メッセージを含んでいることを証明することは可能であろう。これはインターネット標準によって認められており、細分化された断片を再組立てするのは、ユーザ・エージェントの責任である。

SMTPを介して送信されるEDI交換の大きさは、細分化が発生した場合に、"partial"というメッセージを使って、大型のEDI交換をいくつかのより小さな部分に分けて送信できるように、配列可能であることが望ましい。RFC 1521は、Content-Type: message/partialの使用を定義している。インターネットEDIにおいて使用する際のmessage/partialのサポートはオプションである。

受信側のUAは、メッセージ処置通知をメッセージの最初の送信者に送る前に、オリジナル・メッセージを再組立てすることが要求される。メッセージ処置通知は、送信されたメッセージ全体の処置を指定するために使用され、処理を行うUAは、メッセージ全体が受信されるまで、たとえ受け取ったメッセージが再組立てを要求していても、同通知を返送してはならない。

大半のEDI交換には反復データが存在するので、一般に、EDIの圧縮はうまくいく。message/partialを実行する代わりに、EDI交換の圧縮は、署名がEDI交換に対して実施された後、また符号化の前に行うことができる。署名が実施されない場合は、圧縮は符号化の前に行われる。圧縮は、インターネット上で大規模なEDI交換を送信する際に、Content-Type: message/partialを実行するための解決策のひとつである。

符号化の前に圧縮を実施すると、反復するストリングが削減されるので、符号化による機密保護が強化される。同順序は、PGPの順序にも一致する。

4.4.2 例

以下は、UAが署名されたMIME EDI内容タイプを処理した後に、返送してきた署名付き受信確認の一例である。

注意： この例は、例証のみを目的としているものであり、プロトコル使用の一部と考えられるものではない。上で、または他の参照されるRFCの中で指定されているプロトコル定義に矛盾する例があったとしたら、その例は間違っている。

To: <recipient email>
Subject:
From: <sender email>
Date: <date>
MIME-Version 1.0
Content-Type: multipart/signed; boundary="separator"
micalg=rsa-md5; protocol="application/x.pkcs7-mime"

- separator
&Content-Type: multipart/report; report type=disposition
& notification; boundary = "xxxxx"
&
&--xxxxx
& Edi Recipient<Edi_Recipient@edicorp.com>に送られたメッセ
& ージは、受け取られており、EDI交換は復号に成功し、その完全
& 性が証明された。さらに、メッセージの送信者であるEdi Send
& er <Edi_Sender@othercopr.com>は、メッセージの発信元として
& 本物であることが確認された。しかし、当該EDI交換が構文的に
& 正しかったとか、EDIアプリケーションによって受信されたとい
& う保証はない。
&
&--xxxxx
& Content-Type: message/diposition-notification
&
& Reporting-UA: good-edi-internet-ua.edicorp.com (ediua & 1.0)
& Original-Recipient: rfc822: Edi_Recipient@edicorp.com
& Final-Recipient: rfc822: Edi_Recipient@edicorp.com
& Original Message-ID: <17759920005.12345@edicorp.com>
& Disposition: autoprocessed
& X-Received-MIC: Q2h1Y2sgSW50XwsyaXRIQ
&
&--xxxxx
& Content-Type: message/rfc822
&
&--xxxxx--
--separator
Content-Type: application/x-pkcs7-mime

@ContentType = SignedData
@version = Version
@digestAlgorithms = DigestAlgorithmIdentifiers
@contentType = Data
@content =

fgfjhHjhJhgIjhgJGHGJHGJHJHJhghjhJHJuytIYTiutTYT34553//YRytdhFFQere
/876JHJHGIUIUgsdIUYgYTRdgggguytUTIUlbXssfdsfdREWrewREWREEWE88POF/DF
frtFFKFG+GFff=
=ndaj

@signerInfos = SignerInfo
--separator--

注意：
- 「&」が先頭についている行は、署名が計算済みのものである。
- 「@」が先頭についているテキストは、PKCS#7で定義されたフィールド及びタイプを示す（PKCS#7： RSA Labs, Inc.の符号メッセージ構文標準を参照のこと）。

RFC 1892の指定通り。オリジナル・メッセージの返送は必要ない。これはオプショナルなボディ部分である。受け取られたヘッダは、追跡の問題で利用できるように、第3のボディ・パートに置いておくことを推奨する。

5．パブリック・キー証明処理

5.1 ニアターム・アプローチ

短期的には、パブリック・キーの交換及び同キーの証明は、取引相手を確立するプロセスの一部として処理されなければならない。UA及びまたはEDIのアプリケーション・インターフェースは、EDI取引相手のIDと、RFD822のe-mailアドレスの間のマッピングに加えて、符号化または署名に関して使用されるパブリック・キーのデータベースを維持しなければならない。取引パートナーシップの確立と、安全なEDIメッセージング・システムの構成に関する手順は、取引相手、及びソフトウエア・パッケージの間で変わる可能性がある。

X.509証明を利用するシステムに関しては、合意された証明機関が利用されない場合は、取引相手自身が互いに証明しあうことが推奨される。取引相手がS/MIMEを使用している場合は、S/MIME実行ガイド第2版に明記される推奨事項を利用して、取引相手はパブリック・キー証明も交換することが特に推奨されている。証明の交換に関するメッセージ形式及びS/MIME準拠要求は、同書に指定されている。

本適用可能性説明書は、証明機関の使用は一切要求していない。

5.2 ロングターム・アプローチ

長期的には、追加のインターネットーEDI標準が開発され、取引相手、及び取引関係の属性の第三者による確認をはじめとする、取引パートナーシップの確立プロセスを簡素化することができるようになるだろう。

6．執筆者のアドレス

Mats Jansson
mjansson@agathon.com
LiNK
1026 Wilmington Way
Redwood City, CA 94062 USA

Chuck Shih
chucks@actracorp.com
Actra Corp.

610 East Caribbean Drive
Sunnyvale, CA 94089 USA

Nancy Turaj
nturaj@mitre.org
MITRE Corporation
Mailstop: W657
1820 Dolley Madison Blvd.
Mclean, VA 22102-3481 USA

Rik Drummond
drummond@onramp.com
The Drummond Group
5008 Bentwood Ct.
Ft. Worth, TX 76132 USA

7．参考資料

[1] N. Borenstein、N. Freed、「MIME（Multipurpose Internet Mail Extensions：多目的インターネット・メール拡張）第1部：インターネット・メッセージ・ボディの形式を指定及び記述するメカニズム」、RFC 1521、1993年9月23日

[2] D. Crocker、「EDIオブジェクトのMIME密閉（EDI Encapsulation of EDI Objects）」、RFC 1767、1995年3月2日

[3] D. Crocker、「ARPAインターネット・テキスト・メッセージの形式に関する標準（Standard for the Format of ARPA Internet Text Messages）、STD 11、RFC 822、1982年8月13日

[4] M. Elkins、「MIME Security With Pretty Good Privacy (PGP)」、RFC 2015、1996年9月

[5] R. Fajman、「メッセージ処置通知に関する拡張可能なメッセージ形式（An Extensible Message Format for Message Disposition Notifications）」、draft ietf-receipt-mdn-01.txt、1996年5月13日

[6] J. Galvin、S. Murphy、S. Crocker、N. Freed、「MIMEに関する安全複数パート：複数パート／署名付き及び複数パート／符号化（Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted）」、RFC 1847、1995年

[7] J. Postel、「単純メール転送プロトコル（Simple Mail Transfer Protocol）」、STD 10、RFC 821、1982年8月1日

[8] S. Dusse、「S/MIMEメッセージ仕様： MIMEに関するPKCSセキュリティ・サービス（S/MIME Message Specification: PKCS Security Services for MIME）」、インターネット・ドラフト：draft dusse-mime-msg-spec00.txt

[9] C. Shih、「相互操作可能なインターネットEDIに関する要件（Requirements for Inter-operable Internet EDI）」、1996年7月

[10] G. Vaudreuil、「メールシステム管理メッセージの報告に関する複数パート／報告内容タイプ（The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages）」、RFC 1892、1996年1月15日

2.2 相互利用可能なインターネットEDIの要件
(Requirements for Inter-operable Internet EDI)

EDIINT機能仕様

1996年11月

EDIINT作業部会
Internet-Draft
有効期限:1997年5月

Chuck Shin
Mats Jansson
Rik Dummond
Lincoln Yarbrough

相互利用可能なインターネットEDIの要件

本覚え書きの現状

本書はInternet-Draftです。Internet-Draftは、Internet Engineering Task Force（IETF）と、そのエリアおよび作業部会の調査書です。また、Internet-Draftとしての調査書には、その他のグループも貢献しています。Internet-Draftは、最長6ヶ月を有効期限とする草稿で、他の文書により随時更新、交換、または陳腐化されることがあります。Internet-Draftを参考文献として使用すること、あるいは「現在進行中の調査」として以外に引用することは不適当です。

Internet-Draftの現状を知るには、ftp.is.co.za（アフリカ）、nic.nordu.net（ヨーロッパ）、unnari.oz.au（太平洋沿岸）、ds.internic.net（米国東海岸）、またはftp.isi.edu（米国西海岸）で、Internet Drafts Shadow Directories に含まれる"lid-abstract.txt"リストを調べてください。

本仕様について質問、コメント、欠陥の報告、または曖昧な点などがありましたら、アドレス<ietf-ediint@imc.org>を使って、IETFのEDIINT作業部会のメーリング・リストまでお送りください。メーリング・リストへの加入申込は、<ietf-ediint-request@imc.org>宛にお送りください。

抄録

本書は、相互利用可能なEDIの要件について述べる機能仕様であり、インターネットのEDIコミュニティ、並びにセキュリティ関連問題について説明する詳細な背景資料を備えています。

ご意見をお寄せくださる方に

本ドラフトに関するご意見がありましたら、次の指示に従ってください。

- 件名の欄にEDIINT Requirementsと記入して、電子メールでchucks@actracorp.com宛に送信してください。
- できれば、説明または修正が必要な部分を引用して、本書のどのセクションについてのご意見なのかを明確にしてください。セクションを明記して、その後にコメントを続けてください。
- テキストの差し替えを提案される場合も、置き換えられるセクションを引用して、テキストはどう書かれるべきかを明確に説明してください。
- 基本的な前提条件に疑問がある場合は、何が問題なのかを明確にしてください。編集者は問題をEDIINTリストに載せ、討論のテーマとします。読者の方が討論内容を読むには、ietf-ediint@imc.orgで討論リストの購読契約をする必要があります。

目　次

1.0 序論

電子データ交換（EDI）は、購買または割賦要求の初期化など、高度に構造化された組織間交換を行うためのプロトコル・セットです。初期RFC1767は、EDI X12とUN/EDIFACTトランザクション・セットをMIMEエンベロープにパッケージするための方法を定義しています。ただし、EDIトランザクションをどのようにパッケージするかに加えて、その結論が出た後の複数ベンダーの相互利用可能なサービス要件を提案する必要があります。現在これらの要件は、EDIトランザクションの完全性、信頼性および様々な形態での受諾など、セキュリティの問題を中心に検討されています。

X.435 EDIメッセージに見られる様々な見出し項目分野（交換送信元、交換受信先、交換コントロール・リファレンス、通信契約ID、および構文の識別子など）を模擬的に実現する追加の要件も、ゲートウェイと付加価値網（VAN）による効果的な交換をサポートするために必要です。インターネットによるEDI間の相互利用可能性を保証するためには、これらの分野の標準が必要です。これらの追加特性については、すでに様々なテクノロジーが存在しており、第1の要件は、EDIコミュニティがインターネットを利用してEDIを送信する際に使用する、共通コンポーネントセットを検討し、選択することです。実際の活動としては、"Internet Requirements Document"および"Applicability Statement Document"を通してEDIに情報を提供することです。

この文献の現在の中心課題は、インターネットのメールまたはメッセージ送信システムである、SMTP（簡易メール転送プロトコル）を使って転送されるEDI MIMEの内容です。

従来のVAN接続は、遅くて、しかも高価でした。インターネットは従来の通信方法に比べ、より低価格で利用でき、より簡単にアクセスできます。EDIにインターネットを使用する上での主な問題点は、特に完全性、信頼性、デジタル・シグネチャ、および拒否不能の領域におけるベンダー製品間の相互利用可能性にあります。EDIINET作業部会の中心課題は、可能な場合は既存の標準を使用して、これらの各領域の解決策を勧告することです。

1.1 対象読者

本書の対象読者は、直接間接にEDI通信の意志決定に関わる個人、現在または将来EDI文献を取り扱う会社、ならびにEDI製品を開発し販売するベンダーです。また、EDIコミュニティに対しサービスやコンサルティングを行う個人も本書の対象読者に含まれます。

2.0 インターネット - 沿革概略

インターネットは、TCP/IPプロトコルセットを使って接続されたコンピュータ、ルータ、およびネットワークの世界規模の集積です。インターネットそれ自体はネットワークではありませんが、ネットワークの集合です。

インターネットは、分散化されるよう設計されており、その実行には単独の権限を必要としません。インターネット上のすべてのホストは相互に対等に通信でき、すべての通信プロトコルは「オープン」されています。すなわち、公開ドメインが標準であり、標準化プロセスは、標準の定義を支援するハードな作業に参加しようとする者にはすべてオープンされています。

インターネットが多種多様なマシン（たとえばトースタ）を収容可能であるのも、この標準の「公開性」の結果の1つといえます。このため、そのプロトコル--TCP/IPセット--は事実上、異種コンピュータ・ネットワーキングの標準となりました。あるレベルでは、インターネットは共通プロトコルによって接続され

たコンピュータの物理的集合ですが、別のレベルでは、EDIの実行に多大な利益をもたらす分散メディアとみなされます。たとえば、インターネットには数十万のグローバルホストが接続されており、数千万のユーザがいます。インターネットは、均一料金の、量と使用時間に無関係のデータ送信価格構造を持っています。インターネットは冗長度が高く、データを代替パスとともにルーティングすることができます。インターネットの分散構造は、新規ホストを比較的簡単に追加することができ、拡張が容易で、高帯域通信テクノロジーをサポートします。

2.1 インターネット - 神話と現実

インターネットは、1969年にARPANETと呼ばれる米国国防省のネットワークとして誕生しました。このネットワークは、ネットワークの一部が故障しても機能し続けることができるネットワークを構築する方法の調査のために構築されました。インターネットに関連するアーキテクチャとプロトコルを開発する際は、ネットワークの信頼性が基本設計点とされました。ネットワークの信頼性が本質的に低い（その一部はいつでも破壊される可能性がある）という前提から、耐久性と信頼性のある設計が出現しました。当初は、インターネットを構成していたのは、主として官庁や教育機関のネットワークでした。インターネットへのアクセスは、コンピュータサイエンス研究者や政府職員およびその契約者に限定されていました。

1986年に国立科学基金（NSF）は、当時希少資源と見なされていたものへアクセスを可能にするため、TCP/IPプロトコルを使って、5つのスーパーコンピュータセンタを1つにリンクしようという発議を行いました。このNSFNET発議の2つの重要な成果が、さらにパワフルなプロセッサと高速リンクを使ったインターネット基礎構造のアップグレードと、より大きなユーザコミュニティへのアクセスの拡張でした。1990年代はさらにインターネットの基礎構造のアップグレードと、従来の政府機関や大学研究コミュニティ以外の新顧客へアクセスの拡張が進みました。インターネットの商用性に対する関心は現在最も高まっており、最も急速に成長している領域です。

Performance Systems International（PSI）やUUNET（Alternetネットワーク）などの商用インターネット・プロバイダは、NSFNET発議の結果として登場した中間レベルのネットワークの集成によって生まれました。MCI、AT&T、Sprintなどの国内長距離キャリアもすべて商用ネットワーク・サービスを提供しています。これらの商用プロバイダは、インターネット・サービス・プロバイダまたは短縮してISPと呼ばれ、インターネット接続やその他の様々なインターネット・サービスを顧客に提供しています。実験的で、主に教育および研究活動に利用されるものというインターネットの認識のルーツは、インターネットの過去にあり、現在の状況を反映していません。ISPの成長にともなう、インターネットへの商用アクセスの発展は、インターネットのネットワーク構成を根本から変えつつあります。

インターネットの基礎となる設計およびアーキテクチャは、かってない規模への拡張によって、その耐久性が証明されました。インターネットは、次のような視野からも信頼できます。

1) インターネットの基礎となるTCP/IPプロトコルセットとアーキテクチャは、技術的に安定しており、成熟しています。
2) TCP/IPセットに基づく製品の導入も、同様に安定しており、成熟しています。
3) インターネット・ルーティングは動的なため、インターネットによって送信されるパケットは、その途中でネットワークの機能不全があっても宛先に到着します。
4) インターネットの商用ISPが管理する部分は、基本的に既存のEDI付加価値網（VANS）と同レベルのネットワーク信頼性、使用可能性、監視、処理能力、インプリメンテーション、およびサポートサービスをより低価格で、さらに広範な帯域で提供します。

インターネットは確かに信頼性があり、低価格で、アクセスが容易で、高帯域通信をサポートし、技術的にも成熟していますが、インターネットをEDIに使用することについては、いくつか懸念があることも事実です。これらの懸念は主としてセキュリティ、メッセージ追跡、監査証跡、および認証に関するものです。暗号化は、どんなタイプのネットワークを経由するかに無関係に必要です。その他の追跡などは、EDIがそれを必要とするために生ずる懸念であり、既存の付加価値網（VAN）によってサポートされます。

2.2 インターネットのルーティングとセキュリティの考慮事項

Tracerouteという共通ネットワーク追跡プログラムを使用して、パケットがソースホストからインターネット上の宛先ホストへ転送される経路を追跡することができます。インターネット上の経路の追跡は、おもしろい特性があります。予想どおりに、転送経路は各取引相手のISPにより管理されるネットワークを通って進みます。各経路は、各ネットワークを通る複数のノードで構成されています。経路は変わることもありますが、これは例外です。IPパケットは確実に、指定された時間内に渡されます。標準的な商用ISPが使用される場合、経路内のノードは政府にも教育期間にも管理されません。

インターネット・ネットワーク追跡を検討した結果、インターネットはパケットをソースから宛先へ届ける上で非常に効果的であるという結論に達しました。ただし、ソースと宛先間で、パケットは多数の中間ノードを経由してルーティングされます。マシンの1つでパケットを処理する者が、EDI交換を構成するパケットを再アセンブルすることができ、それによってパケットを読み取り、コピーし、変更または削除することができる場所が中間ノードです。電子メール転送（SMTP）を使ってEDI交換が行われる場合、メッセージが最終受信先に渡らないという事態が起こることがあるので、メッセージは中間ノードで保存しなければなりません。ここでもメッセージは、上述のセキュリティ上の脅威にさらされます。

セキュリィティの脅威の可能性は（特に良質のISPによって管理される中間ノードを経由する場合）非常に低く、実際にはほとんど有り得ません。しかしその可能性はあるので、特にパケットに高価値または機密に関わるEDI、すなわち電子商取引が含まれる場合には、懸念されます。

本書の中心課題はインターネットによるEDIであるので、本論ではインターネットが優先的に論じられます。ネットワーキングは、本質的にセキュリティの脅威に晒される傾向があります。情報は共用メディアに乗せられ、送り手の管理下にないノードを経てルーティングされます。それが悪意のハッカーによるものであれ、管理上のミスによるものであれ、ネットワークによって送信される情報が違法な手段によって読み取られ、コピーされ、変更され、あるいは削除される危険は、たとえEDI交換がEDI VANを通して行われても存在する可能性があります。

EDI VANの提供する「付加価値」サービスの中心的要素は、VANを経て送信されるEDI交換がいかなる危険にも晒されないという保証です。ただし、インターネットのような「オープンな」ネットワークによってEDI交換が転送される場合には、セキュリティの脅威に対して防衛の措置を講ずることができます。これらのセキュリティ対策は、インターネットでEDIを行う場合の基本要件です。

これらのセキュリティ対策については、本書のセクション3.0で個別に説明します。各措置に伴う問題についても解説し、推奨解決策を提案します。

2.3 EDI VAN通信とセキュリティ

このセクションでは、現在のVANセキュリティ・サービスを簡単に説明します。本書のセクション3.0で推奨するセキュリティ対策は、本質的には以下で説明するVANセキュリティ・サービスと同じです。

EDI取引相手に提供される最も一般的なEDI VAN通信サービスは、非同期メールボックッス・サービスです。取引相手は一般に、VANネットワーク・アクセスポイントにダイヤルインでアクセスし、次にファイル転送プロトコル（FTP）を使って、EDI交換をVANに送信します。VANは、EDI交換を受信側取引相手のVANメールボックスに送ります。その後、受信側取引相手がVANにダイヤルインして、EDI交換をVANメールボックスからダウンロードします。

多数の通信プロトコルのサポートと一般に低速の回線速度を除いて、EDI VANへの接続はインターネット・サービス・プロバイダへの接続と大差ありません。ただしEDI VANは、ISPよりも高品質のEDIサービスをEDI取引相手に提供します。これらのサービスの中で最も重要なことは、EDI VANが信任されサードパーティとして活動し、VAN経由で送信されるEDI交換がいかなる危険にも晒されないことを保証することです。

EDI VANは、EDI交換の完全性、認証、および付加価値網（VAN）によるEDI交換を追跡する多数の肯定応答（ACK）サービスを提供します。EDI交換の完全性サービスは、いったんVANに転送されたEDI交換は、いかなる変更もなく受信側取引相手にルーティングされることを取引相手に保証します。

取引相手の認証は、VANによって認証された後でなければ、取引相手はEDI交換を送受信できないことを保証します。VANは、取引相手に正しいユーザIDとパスワードでネットワークにログインさせて、取引相手を認証します。VANには、取引相手のアカウントを保守し、アカウントが有効であることを保証する管理責任があります。そのほかにVANは、取引相手がVANによるEDI交換の進行を追跡できる様々なレベルのサービスを提供します。取引相手は、メールボックス配信通知またはメールボックス・ピックアップ通知の申し込みをすることができます。メールボックス配信通知は、EDI交換が受信側取引相手に送信されると、VANにより送信側取引相手に送られます。メールボックス・ピックアップ通知は、EDI交換が受信側取引相手によってダウンロードされると、VANにより送信側取引相手に送られます。

追跡の問題については、セクション4.0で詳しく説明します。

3.0 機能要件

3.1 概論と定義

以降のセクションでは、機能要件と相互利用可能性要件について説明し、またインターネットを使ったEDIトランザクションの送受信の実際の考慮事項について述べます。読者は、EDI全般に精通していることが前提になっています。

3.2 標準暗号化アルゴリズムと世界規模の暗号化

3.2.1 概論と説明

暗号化の目的は、他では読み取り可能なテキストを読取りも理解も不能なものにすることです。テキストを理解不能にすることによって、誰かがEDI交換をその取引相手間の転送中に読み取ったり

コピーしたりすることを防止します。暗号化はEDI交換に機密性を与えます。多くの場合、見出し情報は暗号化されないので、トラフィックの分析は常に可能です。（トラフィック分析とは、有効な情報を見出し情報から引き出すための、見出し情報の分析のことです。）

暗号化は、アルゴリズムとキーの2つの構成要素を基礎にしています。アルゴリズムは、プレーンテキストまたはその他のわかりやすい情報を取り出して、それを理解不能な暗号テキストに変換する、数学的変換です。暗号テキストを元のテキストに戻す逆の数学的変換も行われ、これは暗号解読と呼ばれます。プレーンテキストを暗号化するには、暗号化アルゴリズムとともに入力する、キーを使用します。アルゴリズムは、多数の可能キーの中から1つを使用します。各アルゴリズムがサポートできるキーの数は、キーのビット数によって決まります。たとえば、キーの長さが40の場合、2のn乗となります。このnはキーのビット数で、結果は1,000,000,000,000のキー組み合わせが可能となり、それぞれ異なるキーがアルゴリズムに少しずつ異なる暗号出力を生成させます。

暗号化アルゴリズムは、そのセキュリティがそのキーの長さのみに依存している場合は、安全と見なされています。セキュリティは、アルゴリズムの秘密、暗号またはプレーンテキストのアクセス不能性、またはキーの長さ以外のその他の要素に依存することはできません。個々のアルゴリズムにこのようなセキュリティが適用されるなら、アルゴリズムへの最も効果的な、そして唯一の攻撃は、1つの正しいキーを見つけるためにすべてのキーの組み合わせを試みなければならない力ずくの攻撃です（対象型暗号化アルゴリズムについてはこのとおりですが、非対象型アルゴリズムの場合は多少事情が異なります。これについては後で詳しく説明します。）したがって、十分なキー長さnを指定することによって、安全性アルゴリズムに対する力ずくの攻撃を全く実行不能にすることができます。

3.2.2 対象型暗号化

2つの取引相手が同じキーを使ってEDI交換を暗号化または暗号解読しなければならない暗号化アルゴリズムは、対象型暗号化アルゴリズムと呼ばれます。言い換えると、EDI交換があるキーで暗号化された場合、別のキーでは暗号解読できないということです。大部分の対象型暗号化アルゴリズムに使用されるキーは、nビットの長さの、ランダムビット文字列にすぎません。これらのキーは、多くの場合、ソースコンピュータから派生するランダムデータから生成されます。

対象型暗号化を使用すれば、暗号化プロセスは簡易化され、各取引相手は秘密の暗号化アルゴリズムを取引相手とともに開発したり、交換したりする必要がありません（ちなみにこれはほとんど不可能なタスクです）。その代わりに、各取引相手は同じ暗号化アルゴリズムを使って、共用の秘密キーを使用すればいいのです。

ただし、対象型暗号化計画には、共用秘密キーについて両当事者が合意しなければならないという欠点があります。取引相手がn個の取引関係を持つばあい、各取引相手ごとに1つの、n個の秘密キーを保守しなければなりません。対称型暗号化計画には、発信元または宛先の真正（発信元と受信確認の拒否不能）を証明できないという問題もあります。両当事者が秘密暗号キーを共用するので、対象型キーによって暗号化されたEDI交換は、どちらの取引相手も送信することができました。非対称型暗号化アルゴリズムを使用する、公開キー暗号と呼ばれる暗号を使用することにより、発信元と受信確認の拒否不能の問題は解決できます。

3.2.3 非対象型暗号化 - 公開キー暗号化

公開キー暗号化は、キー対の概念を基礎にしています。対の各半分（1つのキー）が、対のもう半分（1つのキー）だけによって解読できる情報を暗号化できます。このキー対は、一方の取引相手だ

けに指定され、関連付けられています。キー対の一方（秘密キー）だけが指定された取引相手に知らされ、キー対の他方（公開キー）は広く公開されますが、やはり指定された取引相手に関連付けられています。

これらのキーの使用法は、機密性とデジタル・シグネチャの点で異なっています。機密性とシグネチャは、当事者のみのが識別できるキー対を持つ各事業体によって異なり、各当事者はキー対の中の1対を他のキー対から秘密にしておきます。

シグネチャは、次のような働きをします。取引相手Aは、その秘密キーを使ってメッセージの一部を暗号化し、それから暗号化されたメッセージを取引相手Bに送信します。Bは取引相手Aの公開キー（誰でも取得可能）を取得し、取引相手Aのメッセージの暗号化された部分の解読を試みます。メッセージが解読されると、取引相手Bは、それがAからのものであることを知ります。なぜなら、Aの公開キーのみがAの秘密キーによって暗号化されたメッセージを解読でき、Aだけが秘密キーを知っているからです。

機密性は、シグネチャとは異なる方法で非対象型キー対を適用します。取引相手Aが機密メッセージを取引相手Bに送信したい場合、Aはキー対を次のように適用します。取引相手Aは、取引相手Bの公開キーを検索し、それを使ってメッセージを暗号化します。取引相手Bがメッセージを受信すると、Bはメッセージをその秘密キーを使って解読します。Bの秘密キーのみが、Bの公開キーを使って暗号化された情報を解読することができます。言い換えると、Bの公開キーによって暗号化されたものは何でも、Bの秘密キーによってのみ解読できます。

公開キー暗号化アルゴリズムは、対象型キー暗号化アルゴリズムに比べ著しく処理速度が遅いので、一般に実際の大規模なEDI交換の暗号化には使用されません。たとえば、RSA Data Security社は、DES（対象型キーアルゴリズム）を使用するソフトウェア暗号化は、RSA（RSA Data Security社の公開キー暗号化アルゴリズム）を使用するソフトウェア暗号化の100倍も速いと見積もっています。DESを使用するハードウェア暗号化は、概してRSA非対象型暗号化アルゴリズムを使用するハードウェア暗号化の1,000～10,000倍も速いと見積もられています。大容量の暗号化に使用される代わりに、公開キー暗号化アルゴリズムは対象型暗号化キーの暗号化に使用されます。また、対象型暗号化キーを交換および管理する効果的な手段としても使用されます。

3.2.4　必要事項

インターネットによるEDI交換に機密性を与えるためには、標準暗号化アルゴリズムとキーの長さの指定が必要です。2つの取引相手間の相互利用可能性を実現するには、事前に、あるいは個々のトランザクション内で、暗号化アルゴリズムとキーの長さが合意されてなければなりません。

3.2.5　問題点

暗号化アルゴリズムを選択する際は、次の基準を考慮する必要があります。アルゴリズムはどの程度安全か、アルゴリズムはどのくらい速くインプリメントできるか、国内および国際用途へのアルゴリズムの使用可能性、アルゴリズムをインプリメントするためのAPIとツールキットの使用可能性、ならびに既存のインプリメンテーションにおけるアルゴリズムの使用頻度。

EDI交換価値ついては、交換価値に比べて力ずくの攻撃のための時間と労力が見合わないように、十分に長いキーを選択しなければなりません。3.2.6　勧告

DES:　最も普及している商用暗号化アルゴリズムはDESです。DESは、電子資金移行決済（EFT）に金融機関で広範に使用されています。DESは、米国政府暗号化標準でもあります。DESは公開ド

メインで使用されており、つまり国際コミュニティを含め、誰でもこのアルゴリズムをインプリメントできるということです。DESはデータの大量暗号化用に設計されており、そのように使用されています。DESは、米国政府によって輸出が禁止されています。

DESアルゴリズムは、1970年代半ばから暗号作成者によって解析され、安全であるとみなされています。言い換えると、DESのセキュリティはそのキーの長さに全面的に依存しています。DESは56ビットのキーを指定するので、2の56乗または10の16乗のキーが可能です。各キーごとに既知の暗号テキストの8バイトを対応する既知のプレーンテキストの8バイトに復号することを意味する力ずくの攻撃は、このアルゴリズムで最良の攻撃と言えます。

力ずくの攻撃を成功させるために必要な時間料と費用は、使用される処理能力と、攻撃者が元のEDI交換の暗号化に使用されたキーに近いキーを生成できる好運によって異なります。これまでに行われた試算によると、DESの力ずくの攻撃によってDESキーを見つけるには、100万ドルのハードウェアをベースにして3.6時間を要します。ところが、対応する100万ドルのソフトウェアをベースとするDESの力ずくの攻撃では、3年の月日を要します。プロセッサの価格対性能比が下がるにつれ、56ビットのキーでは、高価なEDI交換を保護するには不十分になってきます。この場合、より長いキーを持つアルゴリズムであるTriple-DES（以下で説明します）を使用することをお勧めします。

Triple-DESはDESの別型で、2つの独立した56ビットキーを使って、EDI交換を3回暗号化し、112ビットの有効なキー長さを与えます。これによって、Triple-DESの力ずくの攻撃は不可能となります。DESとTrippe-DESは、実際には3つの異なるモードでインプリメントできます。DESとTriple-DESは、暗号ブロック連鎖（CBC）モードで使用することをお勧めします。このモードでは、各暗号テキストブロックを相互に依存させることによって、暗号テキストの変更が検出可能になるので、保護が強化されます。

RC2とRC4: RC2とRC4は、RSA Data Security社が所有権を持つ対象型アルゴリズムです。RC2とRC4は、DESと異なり、可変長キーアルゴリズムです。異なるキー長さを指定することによって、RC2とRC4はセキュリティをより大きく、あるいはより小さく構成することができます。RC2とRC4はDESの代替手段で、特殊な輸出ステータスを持っており、それによってRC2とRC4の40ビット・バージョンと米国企業の外国子会社と海外事業所のための56ビット・バージョンは、米国政府からの輸出認可を促しました。RSAによれば、ソフトウェアにインプリメントする場合、RC2とRC4はDESよりも高速だそうです。Lotus Notes、Netscape Navigator、およびApple社のOpen Collaboration Environmetなどのいくつかの電子メール製品は、これらのアルゴリズムを使用しています。RC2とRC4を使用する場合は、128ビット以上の長さのキーを使用することをお勧めします。128ビット以上の長さのキーであれば、現在と予測できる将来の力ずくの攻撃を不可能にすることができます。

IDEA: International Data Encryption Algorithm（IDEA）は、1991年に公開されました。この対象型アルゴリズムは、64ビット・ブロックサイズと128ビット・キーサイズを使用する、反復ブロック暗号です。IDEAのキーの長さは、DESのキーの2倍以上であり、Triple-DESよりも長くなります。IDEAアルゴリズムは、米国内と海外で特許を得ています。CBCモードのIDEAアルゴリズムは、PGP（Pretty Good Privacy - 有名な電子メール・セキュリティ・プログラム）によって暗号に使用されています。PGPの個々のユーザは、IDEAアルゴリズムを使用するロイヤルティ無料のライセンスを持っています。

安全で、EDI交換に機密性を与えることのできる暗号化アルゴリズムは多数あります。あまり価値の高くない交換には、40ビットのRC2かまたは56ビットのDESで十分でしょう。もっと価値の高い交換には、Triple-DES、IDEA、あるいは長いキーのRC2またはRC4をご使用になることをお勧めし

ます。

現在DESは広く普及していますが、56ビットDESキーの限界がセキュリティにとって徐々に不十分になってきたため、Triple-DESの普及が企画されています。DESアルゴリズムは米国以外でもインプリメンテーションが可能であり、長年の調査によって、DESアルゴリズムは安全であることが明らかになっています。RC2とRC4は、暗号化のセキュリティ（キーの長さの指定）が構成可能であるため、とても便利です。RC2およびRC4アルゴリズムは所有権のある財産ですが、これらのアルゴリズムを組み込んだ製品は、キーの長さが40ビット以下のものに限って、米国外に輸出することができます。

IDEAは比較的新しいアルゴリズムであり、DESほどには調査されていません。IDEAは、構成可能ではありませんが、十分なキーの長さを持っています。IDEAは安全なアルゴリズムと言われており、PGPに登用されたことから、インターネット電子メールに最も広く使用されている暗号化アルゴリズムとなりました。

3.3 キーの管理 - 対象型キー

3.3.1 概論と説明

対象型暗号化の使用は、共用の秘密を基礎にしています。対象型暗号化アルゴリズムを使用する2つの取引相手は、次のことを実行できなければなりません。すなわち、ランダムな対象型キーを生成し、その使用に合意すること。その対象型キーを他方の取引相手と安全に交換すること。危険に晒された、あるいは変更が必要な対象型キーを無効にするプロセスをセットアップすること。各取引相手は、以上の条件をそのすべての取引相手について個別に満たしていなければなりません。対象型キーの管理と配布は、煩わしく、しかも安全性に問題のあるプロセスとなりがちです。

純粋な対象型キー管理計画にも、発信元の真正さを証明できないという問題があります。2人の取引相手が秘密暗号化キーを共用しているので、対称型キーによって暗号化されたEDI交換は、キーの知識を持つ2人の取引相手のいずれかによって送信されたことになります。

公開キー暗号化を使用することによって、対象型キーの管理は簡易化され、安全性も向上します。取引相手は、取引相手との関係の一部として、秘密の対象型キーについて合意する必要がなくなります。公開キー暗号化は、純粋な対称型キー管理計画に特有の発信元の真正の問題も解決します。

固有の対象暗号化キーを各EDI交換ごとに生成し、公開キー暗号化を使用することによって、取引相手は、取引相手との関係で秘密に共用対象型キーについて合意する必要がなくなります。対象型キーは、取引相手間のEDI交換のためのソフトウェアによってランダムに生成できます。各EDI交換ごとに固有の対象型キーが生成されるので、キーの保守は不要です。取引相手は、危険に晒された、あるいは期限切れとなったキーを無効にする必要もありません。各対象型キーは、1度だけ使用されます。

上記の方法を使用することによって、さらに別のセキュリティも実現されます。万が一対象型キーの1つが危険に晒されても、1つのEDIトランザクションが影響を受けるだけで、取引相手との関係ですべてのトランザクションが影響を受ける訳ではありません。公開キー暗号化は、対象型キーを取引相手間で安全に配布する手段も提供します。受信側の取引相手だけが秘密の非対象型キーを知っているので、受信側の公開非対象型キーを使って暗号化された対象型キーを解読できるのは受信側取引相手だけです。したがって、対象型キーを使ってEDI交換を解読できるのも受信側取引相手だけということになります。

取引相手ABCが取引相手XYZに送信するEDI交換に機密性を与えるため、次のようなステップが実行されます。

1) EDIトランスレータがEDI交換を出力します。
2) 指定された長さのランダム対象型キーが生成されます。
3) 選択された暗号化アルゴリズムを使ってランダムに生成された対象型キーを使って、EDI交換が暗号化されます。
4) 次に、XYZの、すなわち受信側取引相手の公開非対称型キーを使って、ランダム対称型キーが暗号化されます。
5) 暗号化された対称型キーと暗号化されたEDI交換がエンベロープされ、取引相手に送信されます。

受信側では、次のステップが実行されます。

1) 対象型キーが、XYZの秘密非対象型キーを使って暗号化されます。
2) 暗号化された対象型キーを使って、EDI交換が解読されます。
3) 解読されたEDI交換がEDIトランスレータにルーティングされます。

3.3.2 必要事項

EDI交換の暗号化に使用される対象暗号化キーを管理する方法。この方法は、対象暗号化キーの生成、保守、および配布を簡易化します。また、対象暗号化キーを取引相手間で配布するための安全なチャネルも提供します。

3.3.3 問題点

対象暗号化キーの管理を容易にする公開キー暗号化アルゴリズムを選択してください。対象暗号化キーは、各EDI交換ごとに即時に生成されます。

公開キー暗号化アルゴリズムを選択する際は、次の基準を考慮する必要があります。アルゴリズムはどの程度安全か、アルゴリズムはどのくらい速くインプリメントできるか、国内および国際用途へのアルゴリズムの使用可能性、アルゴリズムをインプリメントするためのAPIとツールキットの使用可能性、ならびに既存のインプリメンテーションにおけるアルゴリズムの使用頻度。

EDI交換価値ついては、交換価値に比べて力ずくの攻撃のための時間と労力が見合わないように、十分に長いキーを選択しなければなりません。

3.3.4 勧告

1) RSAは、キー管理におけるその使用が事実上の標準となっている、公開キー暗号化アルゴリズムです。インターネットによってEDIを行う場合は、対象暗号化キーの管理と配布に、RSAを使用することをお勧めします。RSA公開キーアルゴリズムには、米国以外でも自由に使用できるという利点もあります。
2) RSAの数学処理は複雑ですが、大きな素数を因数分解することの難しさが基礎になっています。公開キーは、2つの大きな素数を掛け合わせることによって生成され、公開キーからの秘密キーの導出には、大きな素数を因数分解しなければなりません。素数が非常に大きければ、このタスクは不可能となります。RSAのキーの長さは構成可能であり、少なくとも512ビット（154桁の長さ）、できれば1024ビット（あるいは308桁の長さ）以上にすることをお勧めします。

3.4 キーの管理 - 公開キーと秘密キー

3.4.1 概論と説明

対象暗号化キーの管理を容易にするために公開キー暗号化を利用する場合、ユーザには、秘密キーの保護の問題と、取引相手の識別名をその公開キーにバインドする問題の2つの問題が生じます。一般にユーザは、その秘密キーが何であるかを知らないものです。ソフトウェアがランダム秘密キーを生成し、暗号化して、ファイルまたはデータベースに保存します。ユーザが秘密キーにアクセスするには、キーを生成したソフトウェアにアクセスすることによって、間接的にアクセスします。ソフトウェアへのユーザ・アクセスは、一般にパスワード、パス・フレーズ、または特定のアクセス権のいずれかまたは全部によって管理されます。これらは社内セキュリティ方針であり、各社固有のものです。未許可のアクセスは、最悪の場合対応する公開キーの廃止という事態を引き起こすこともあるので、秘密キーへのアクセスの管理は非常に重要です。

3.4.2 公開キー

公開キーは、発信側取引相手が対称型キーを暗号化するために、また後で説明するように、受信側取引相手が発信元の真正を確認するために使用します。取引相手は、公開キー証明を使用して公開キーを交換します。

公開キー証明は、X.509標準に定義されており、事業体の識別名（X.500において誰かまたは何かを識別する正規の手段。この場合は取引相手）を公開キーにバインドするものです。公開キー証明には、証明の発行元のデジタル・シグネチャ、証明の発行元の識別名、発行元の固有のシリアル番号、証明の有効期限、ならびに発行元のデジタル・シグネチャを確認するための情報が記載されています。証明発行者は、認可当局（Certification Authorities）と呼ばれ、両取引相手により信任されています。証明とは、本質において、取引相手と公開キーのバインドをデジタルに認証したものです。

3.4.3 必要事項

信頼できるモデルの採用と、商用グレード/クラス3の証明書を発行する証明機関の利用。各取引相手は、他方の取引相手が信任する証明機関を選択しなければなりません。

証明機関と取引相手間および取引相手相互間における証明書および証明取消リストの申請、取消、および交換のための書式とプロトコル。

3.4.4 問題点

実際の商用アプリケーションで証明機関の利用が普及していないこと。並びに、X.509v3証明と、証明書および証明取消リストを申請、取消、および交換するための標準をさらにプロファイリングする必要性があること。

3.4.5 勧告

3.4.5.1 短期的アプローチ

EDI取引相手の間にはすでに信頼関係が存在しているので、証明機関の利用がさらに普及し、X.509v3証明にさらにプロファイリングが行われるまでは、証明機関を利用しないことに合意するのであれば、取引相手は相互に自己証明を行うことをお勧めします。

短期的には、公開キーの交換とこれらのキーの証明は、取引相手設定プロセスの一環として処理されなければなりません。UAおよび/またはEDIアプリケーション・インタフェースは、EDI取

引相手IDとRFC822電子メール・アドレス間のマッピングのほかに、暗号化と認証に使用される公開キーのデータベースを保守しなければなりません。取引相手の設定手順および安全なEDIメッセージ交換システムのコンフィギュレーションの手順は、取引相手とソフトウェア・パッケージによって異なることがあります。

それでもやはり、取引相手双方は、両者によって信任された証明機関からX.509 v3証明を取得することを是非お勧めします。証明取得プロセスは、証明機関によって異なります。取引相手同士は、証明をPCKS#7およびS/MIMEに指定される書式とプロトコルを使って交換することをお勧めします。

3.4.5.2 長期的アプローチ

長期的には、証明の取得、取消、交換、およびサードパーティの認証を含め、取引相手の設定プロセスを簡単にするために、追加のインターネットEDI標準を開発する必要があります。

PKCS#7およびPKCS#10、ならびにIETF-pkix（公開キーインフラストラクチャX.509作業部会）により開発中の標準をインターネットEDIの標準として評価し、採用する必要があります。

3.5 内容の完全性

3.5.1 概論と説明

暗号化は、EDI交換の機密性を保証します。内容の完全性は、受信側取引相手がEDI交換を発信側が送信した状態で受け取ることを保証します。内容の完全性は、取引相手間を移動中にEDI交換にいかなる変更も、すなわち追加、削除、あるいは変更が行われていないことを保証します。

内容の完全性は、送信側がEDI交換に完全性制御値を含めることによって達成されます。この値は、EDI交換を「特徴で識別」する適当な暗号化アルゴリズムを使って計算できます。これらの暗号化アルゴリズムは、一方向ハッシュ関数あるいはメッセージ完全性チェックと呼ばれます。暗号化と同様、一方向ハッシュ関数は、EDIの理解可能なプレーンテキストを理解不能にします。

ただし、暗号化アルゴリズムと異なり、一方向ハッシュ関数は解読することはできません。一方向ハッシュ関数は、確率が無限に小さいため、任意の長さのプレーンテキスト片が特定の値にハッシングされるよう、あるいは2つのプレーンテキスト片が同じ値にハッシングされるように構成されています。通常、一方向ハッシュ値は112～160のビット長です。ハッシュ値が長くなれば、それだけ安全性が増します。

一方向ハッシュ関数はキーを必要とせず、使用されるアルゴリズムは取引相手の間で合意されなければなりません。内容の完全性を保証するには、送信側取引相手は、EDI交換の一方向ハッシュ値を計算しなければなりません。この値は他に同じのものがない固有値で、EDI交換を「特徴で識別」します。送信側取引相手は、ハッシュ値をEDI交換とともに送信します。受信側取引相手は、同じ一方向ハッシュ関数を使って、受信したEDI交換のハッシュ値を計算します。受信したハッシュ値が計算されたハッシュ値と一致すれば、受信側取引相手は、EDI交換が変更を加えられていないと判断します。

3.5.2 必要事項

内容の完全性を保証するために必要なハッシュ値を計算するには、一方向ハッシュ・アルゴリズムを選択します。

3.5.3 問題点

一方向ハッシュ・アルゴリズムは安全であること、公に使用可能であること、ならびに128ビット以上のハッシュ値を生成するものでなければなりません。

3.5.4 勧告

SHA-1は安全ハッシュ・アルゴリズムであり、国家安全保障局（NSA）によって開発された一方向ハッシュ関数です。SHA-1は、このアルゴリズムへの暴力的攻撃を実行不能にする、160ビットのハッシュ値を生成します。MD5の弱点が発見されたため、ほとんどの電子メール・セキュリティ・プログラムとその他のセキュリティ仕様が、SHA-1を推奨しています。

MDS5は、公に使用可能な、メッセージ・ダイジェストと呼ばれる128ビットハッシュ値を生成する一方向ハッシュ関数です。現在MD5は、PEM、PGP、およびS/MINEなどの、ほとんどの電子メール・セキュリティ・プログラムに広範に利用されています。

すべての新規インプリメンテーションにSHA-1を使用することをお勧めしますが、多くのMD5インプリメンテーションが既に存在するので、MD5の着信を引き続き受信できるようにしておくことをお勧めします。

3.6 発信元の認証と受諾

3.6.1 概論と説明

暗号化は、機密性を保証します。一方向ハッシュ関数を適用することにより、内容の完全性が保養されます。発信元の認証と受諾によって、EDI交換の送信側の身元が保証されます。発信元の受諾は発信元を識別し、EDI交換が2点間で送信される場合、すなわち転送が関わらない場合には、認証と同じ働きをします。発信元の認証と受諾は、EDI交換が取引相手間で移動中に発生する可能性のある、いたずらによる攻撃を防止します。

発信元の認証も受諾も、デジタル・シグネチャを使って適用されます。デジタル・シグネチャは、公開キー暗号化のもう1つの応用であり、次の段落で詳細に説明します。

この時点までは、受信側取引相手の公開キーが対象型キーの暗号化に使用され、この対象型キーは受信側取引相手の秘密キーによってのみ解読されました。ところが、秘密キーと公開キーの役割を逆転して、秘密キーを使って暗号化して、公開キーを使って解読することができます。ここでもキーは相反関係にあるので、暗号化に秘密キーが使用される場合は、解読は秘密キーによってのみ行われます。

取引相手ABCのみがABC固有の秘密キーを知っているので、取引相手ABCだけがその秘密キーを使って暗号化を行えます。このため、秘密キーによる暗号化には、暗号化を行う個人または企業体を特定して識別する効果があります。実際には、これはデジタル・シグネチャを意味します。ABCの公開キーは、そのすべての取引相手に知られているので、ABCの秘密キーによって暗号化されたものは取引相手全員が解読できることになります。ABCの秘密キーを使って暗号化されたものをABCの公開キーを使って解読できるということは、ABCを暗号化を行った取引相手として認証する、つまりABCをデジタル・シグネチャの適用として識別する効果があります。

ABCの秘密キーを知っているのはABCだけなので、ABCは暗号化を行ったことを否認できません。発信元の拒否不能は、このように適用されます。

では、発信元の認証と受諾を保証するには、取引相手は秘密キーを使って何を署名し、何を暗号化すればいいのでしょうか? 公開キー暗号化アルゴリズムは、大容量データを暗号化するものではなく、それを行うと非常に時間がかかることを思い出してください。対象型キーは公開キーによって暗号化されます。これを秘密キーを使って暗号化することは、認可された受信者以外の者がEDI交換を解読できることになるので、お勧めできません。一方向ハッシュ値はかなり小さく、普通は112～160ビット長にすぎず、デジタルに署名されるものには、これを選択するのが自然です。メッセージ完全性の値に秘密キーによる署名がある場合、発信元の認証と受諾のみが保証されるのではなく、メッセージの完全性も保証されます。

3.6.2 必要事項

デジタル・シグネチャ・アルゴリズムの選択。

3.6.3 問題点

デジタル・シグネチャ・アルゴリズムを選択する際は、次の基準を考慮する必要があります。アルゴリズムはどの程度安全か、アルゴリズムはどのくらい速くインプリメントできるか、国内および国際用途へのアルゴリズムの使用可能性、アルゴリズムをインプリメントするためのAPIとツールキットの使用可能性、ならびに既存のインプリメンテーションにおけるアルゴリズムの使用頻度。

EDI交換価値ついては、交換価値に比べて力ずくの攻撃のための時間と労力が見合わないように、十分に長いキーを選択しなければなりません。

3.6.4 編集者の勧告

RSA公開キーアルゴリズムをキーの暗号化に使用するほかに、RSAをデジタル・シグネチャにも使用することをお勧めします。

暗号化アルゴリズムと異なり、強力な（キーの長さ40ビット以上の）デジタル・シグネチャ・アルゴリズムを米国外に自由に輸出できます。

3.7 署名入り受信確認または受信確認の受諾

3.7.1 概論と説明

署名入り受信確認（または受信確認の受諾）は、受信側取引相手が送信側取引相手に送る受信肯定応答です。署名入り受信確認は、EDIをインターネットによって実行する際の次のような問題の解決に使用されます。

1) 現在、RFC 1891～1894内では検討中ですが、インターネット標準にはメールボックス配信通知がありません。
2) VANメールボックス配信通知に相当する通知の提供。
3) VANメールボックス・ピックアップ通知に相当する通知の提供。
4) VANメールボックス認証に相当する認証の提供。
5) EDI交換が不当に削除されたり、トランスポートによって配信されない状況の検出。

署名入り受信確認の送信者による受信は、メールボックスが正しく配信されたことの暗黙的な肯定応答です。

署名入り受信確認の受信は、メールボックスから交換の検索が行われたことの明示的肯定応答でもあります（ピックアップ通知）。受信者に受信確認の署名をさせることによって、宛先受信者が

EDI交換をピックアップしたこと（メールボックス認証）と、宛先受信者がEDI交換の完全性と送信者の身分を確認したことが認証されます。元のメッセージIDと受信したメッセージの一方向ハッシュ値を署名入り受信確認で返すことによって、送信者は肯定応答されたEDI交換を実際に送信されたものと突き合わせることができます。

3.7.2 必要事項

署名入り受信確認の書式とプロトコルが、次の応答をできるように定義します。

1) 受信者へのEDI交換のメールボックス配信の暗黙的な肯定応答。
2) 受信者が送信者を認証し、送信されたEDI交換の完全性を確認したことの明示的肯定応答。
3) 署名入り受信確認が受信側取引相手によってデジタルに署名される場合、受信確認の拒否不能を保証する。
4) 追跡、ログ、および調整のために使用できるように、署名入り受信確認で情報を提供する。

再送信タイマと、破損された交換を検出するための再試行カウントの使用をお勧めしますが、構成可能でなければなりません。また、受信者は重複交換を受信するとき何を実行すべきか、送信者は重複受信肯定応答を受信するとき何を実行すべきかを指定しなければなりません。

3.7.3 勧告

署名入り受信確認の構文は、署名入り受信確認の用途の多くが他のMIMEエンキャプスレーティド・オブジェクトに広範に応用されるため、EDIの内容に固有のものではありません。IETF受信確認作業部会の成果を署名入り受信確認の導入のために採用することをお勧めします。受信確認作業部会は、IETE Word Wide Web（WWW）サイトから入手可能なInternet-Draft（draft-ietf-receipt-mdn-01）を公開しました。EDIINT作業部会は、追加の廃棄フィールド値と、EDI環境内でのMDN（メッセージ廃棄通知）の使用方法の仕様を指定するために、受信確認作業部会とともに作業を進めています。特に、EDI環境においては、メッセージ廃棄要求は黙って無視することはできません。また、受信確認の拒否不能が両取引相手によって合意される場合、受信側取引相手によって確認されるメッセージ完全性チェックは、MDNで発信側取引相手に返されなければなりません。

署名入り受信確認のタイムアウト値と再試行値は、構成可能でなければなりません。重複はUAによってチェックされ、放棄されます。

署名入り受信確認は、（マルチパート/署名入り仕様の）最初の部分がMDNで、MDNにはデジタル・シグネチャの署名がある、MIMEマルチパート/署名入り仕様を使ってインプリメントする必要があります。

3.8 EDIオブジェクトの限界とトランザクションの機密

3.8.1 概論と説明

この作業部会の提案する仕様は、部会またはドキュメントレベルではなく、EDI交換レベルで適用されます。セキュリティ・サービス、梱包、トランスポート、あるいは受諾サービスは、EDI交換に適用されることが想定されています。X12.58およびUN/EDIFACT 9735-5および9735-6の安全基準と異なり、セキュリティ・サービスは部会またはドキュメント・レベルでは適用できません。この仕様の目的は、これらのサービスをトランスレータから「通信」サブシステムに移すことです。「通信」サブシステムは、EDIデータ構造についてはほとんど何も知る必要はありません。

見出し（ISA/IEAまたはUNA/UNB/UNZ）のエンベロープを含めて、EDI交換全体も暗号化されま

す。EDI交換は、VANではなくインターネットによってルーティングされるので、送信者/受信者のIDはメールボックス・ルーティングには使用されず、EDIをインターネットで送信する際にEDIエンベロープを暗号化することができます。

3.8.2 ゲートウェイ機能

VAN、すなわち内部ゲートウェイがインターネットで受信したEDI交換をルーティングするには、EDIエンベロープ内の情報にアクセスできなければならないという状況があります。エンベロープ情報もその他の有効なゲートウェイ情報も、独立したMIME本体部分としてコピーされ、送信されなければなりません。新規のMIME内容は、このタイプの情報として定義されなければなりません。

3.9 暗号作成サービスを指定する構文とプロトコル

3.9.1 概論と説明

暗号作成サービスがEDI交換に適用されると、EDIメッセージの交換の際に暗号化情報を送信する方法について、書式とプロトコルを指定しなければなりません。暗号化アルゴリズム情報、一方向ハッシュ・アルゴリズム情報、対象型キー、初期設定ベクトル、一方向ハッシュ値、および公開キー証明はエンベロープして、EDI交換とともに送信する必要があります。

3.9.2 必要事項

暗号の適用されたEDI交換を指定する構文とプロトコルを指定する必要があります。適当な標準がいくつか既に存在しているので、新規に指定するよりも、これらの既存の標準を選択することをお勧めします。

3.9.3 問題点

構文は、様々なインターネット・トランスポートに使用できるように、トランスポートに無関係でなければなりません。標準構文は幅広いサポートを行い、またインプリメンテーションが可能でなければなりません。要するに、構文の性格は国際的でなければなりません。

3.9.4 勧告

IETF EDIINT作業部会は、暗号化の適用されたEDIを送信できる様々な方法を比較したマトリックスをまとめました。S/MIMEおよびPGP/MIME（elkinsドラフト付きのバージョン3.0）の使用は、いずれも実行可能な代替案です。マトリックスの比較によると、どちらにもそれぞれ長所と短所があります。

S/MIME仕様では、「署名入り」と「暗号化/署名入り」を識別できます。S/MIMEの暗号化/署名入りメッセージ内の署名者は識別可能です。署名入りで、暗号化された内容を持つS/MIMEの署名者は識別可能です。ただしこれは特定のEDIおよび電子取引状況では不可能です。S/MIMEは、デフォルトの暗号化アルゴリズムとして40ビットRC2と、キーの長さを指定します。アプリケーションの中には、このデフォルトのアルゴリズムもキーの長さも受容できないものがあります。ただしS/MIMEは、セクション3.3.2で推奨されているその他のセキュリティ・アルゴリズムとキー長さに適応可能です。

PGP/MIMEは、セキュリティ・アルゴリズムのプロファイルセットとユーザが構成可能なキーの長さをサポートします。PGP/MIMEには、上記のS/MIMEの説明で述べた署名者の問題はありません。ただし、PGP/MIMEの使用するセキュリティ・プロファイルは機密性、発信元の受諾、およびメッセージの完全性を保証する上で十分ですが、PGP/MIMEはアルゴリズムとキーの長さの選択にフレキシビリティがあまりありません。

4.0 追跡とエラー処理の基本

4.1 概論

付加価値網（VAN）には、EDI取引相手間の追跡機構が本質的に備わっていることを認識しておく必要があります。インターネットEDIでは、ISPがTCP/IPプロトコルと同様の一定レベルの転送追跡を行います。ただし、現在のTCP/IPプロトコル・セットまたはISP追跡は、EDI VANの提供するすべての追跡を完全にカバーしている訳ではありません。インターネットIDEをVAN EDIとして追跡できるようにするには、追加セキュリティ要件や署名入り受信確認のサポートに関連する新しい追跡情報をEDI UAに導入する必要があります。

会社間の通信のほかにも、「追跡」は取引関係内の他の多くの問題に関わります。たとえば、997関数肯定応答が使用される場合や、EDIFACT CONTRLメッセージ、および連続グループ・コントロール番号の共有トランスレータ追跡などです。これらはすべて、インターネットEDI追跡と見なさなければなりません。そのほかにも、S/MIMEにおける最近の開発は、一部の分析（正の肯定応答）を保証しています。これは、配信が失敗した場合だけでなく成功した場合にも、メール応答を参照させます。

以下に挙げるのは、取引相手間のEDI交換の送信および受信に必要な共通追跡情報のリストです。

1) 内部書式からEDI標準書式へ正しく変換された送信。
2) 正しくコード化され、署名され、暗号化されて送られた送信（VANによって正しく受信された送信に相当する）。
3) 受信者のメールボックスに正しく配信された送信（送信が受信者のVANメールボックスに転送されたというVAN肯定応答に相当するもの）。
4) 送信は受信者によって正しく取り出された（VANメールボックス取出肯定応答に相当する）。
5) 受信者によって正しく変換された送信（EDI交換は構文上正しいと判断された）。
6) 遅延または破損された送信の検出と復元。
7) 重複送信の検出と処理。

以降のセクションで、新しいインターネットEDI追跡情報を保守すべき構成要素について説明し、この新しい追跡情報をEDIアプリケーションが保存する追跡情報とどのように関連付けるかについて解説します。

4.2 内部書式から標準EDI書式へ正しく変換された転送

4.2.1 必要事項

EDI送信が正しく変換されて、アウトバウンド送信の準備が完了していることを送信者に保証できる機能が必要です。

4.2.2 勧告

これは、すべてのEDIトランスレータではないにせよ、大部分のEDIトランスレータにとっての標準機能です。これは、EDI UAの必須機能ではありません。

4.3 正しく暗号化され、署名され、送信された転送

4.3.1 必要事項

EDI送信が正しくコード化され、暗号化され、署名されて送信されたことを送信者が確認できる機

能が必要です。

4.3.2 勧告

インターネットEDIに必要なセキュリティ・サービスの成功または失敗の追跡は、EDI UAによって保守されなければなりません。

EDI UAは、その交換コントロール番号、また希望ならばユーザが定義する値によって送信を識別できなければなりません。

4.4 受信者のメールボックスに正しく配信された送信

4.4.1 必要事項

EDI送信が受信者のメールボックスに正しく配信されたことを送信者が確認できる機能が必要です。

4.4.2 勧告

このタイプの追跡情報は、UAによって保守され、送信者に配信通知として返されます。配信通知は、RFC1891-1894に指定されています。

4.5 正しく受信された送信

4.5.1 必要事項

送信が宛先の受信者によって正しく受信されたことを送信者が確認できる機能が必要です。

4.5.2 勧告

このタイプの追跡情報は、EDI UAによって保守され、送信者に署名入り受信確認として返されます。（署名入り受信確認については、セクション3.7.3を参照してください。）

注：X.12 997またはEDIFACT CONTRLメッセージも、受信した肯定応答の暗黙の転送に相当する情報を提供できます。ただし、以下の理由から、やはり署名入り受信確認の使用をお勧めします。

・読み取り可能997の受信による受信者の暗号化の暗黙の成功は、コントロールID（997）のみを証明するもので、実際のデータ（NRR）は証明されたことになりません。
・トランスレータは非常に多種多様で、CONTRLメッセージがEDIトランスレータによってサポートされていなかったり、まだ一般に普及していないこともあります。（訳者注：原文の"...or is it in widespread use yet"は、"...or isn't in widespread use yet"の間違いだと思います）

4.6 受信者によって正しく変換された送信

4.6.1 必要事項

受信者が送信を（EDIに置き換えて）「理解できる」ことを送信者が確認できる機能が必要です。

4.6.2 勧告

この情報は、オブジェクトの限界に関するわれわれの勧告に従い、EDI UAによって追跡する必要はありません。

機能肯定応答997とEDIFACT CONTRLがこの目的を果たします - この情報はEDIトランスレータによって追跡されます。

4.7 遅延または破損された転送の検出と復元

4.7.1 必要事項

送信者が、指定された、構成可能な時間内に正しく受信されたという肯定応答を受けていない送信を検出でき、それに応じてアクションを構成できる機能が必要です。

4.7.2 勧告

1) 次の2つのイベントのそれぞれにタイム・スタンプを使用。
   * 送信されたMIMEメッセージ
   * 受信された署名入り受信確認
2) タイム・トリガに失敗した送信を自動的に検出する機能。
3) 失敗に基づいて自動アクションを構成する機能。次のようなアクションが想定されます。
   * 再送信。再送信される場合、受信側UAは第2の送信を重複として検出し、それを放棄することができなければなりません。
   * 警告/報告
   * 無視/削除 - このオプションは、EDIトランスレータ・レベルでのみ997/CONTROLによる追跡を行おうとする場合に選択できます）。

4.8 重複転送の検出と処理

4.8.1 必要事項

EDI送信の受信者が、様々なタイプの重複送信を検出でき、検出された送信をしかるべき方法で処理できる機能が必要です。第一に、トランスレータが開始した重複送信は、いかなる方法でも停止できません - トランスレータの処理レベルはそのように想定すべきです。言い換えると、UAによるISAコントロール番号のチェックは不要ということです。第二に、送信の即時配信に再送信機能を使用することによって、UAは送信側UAにより生成された重複送信を識別でき、最初の送信が受信された後で、重複送信を放棄することができます。

4.8.2 勧告

トランスレータが開始した再送信を、ハッチなしで受信側トランスレータにパススルーできること。これは、ISAコントロール番号のようなEDI関連コントロール番号を、EDI UAによってチェックする必要がないことを意味します。

付録A - セキュリティ・プロトコルの比較

バージョン:3.0
日付:1996年7月18日

ソース:

EDIINT - インターネットによるEDI、インターネット・メール協会研究集会資料、Chuck Shih、Steve Dusse'、David Darnell、Kent Landfield、David Chia、Rik Drummond、Jeff Cook、Alan Cox、Raph Levien、Uess Housley、および他多数。

1) 米国外に輸出可能

PGP V3.0
* PGPはすでに米国外で使用されており、（単に長いキー長のアルゴリズムを輸入禁止する代わりに）長いキーを使用する暗号メッセージを禁止している国を除いて、PGPの長いキーのメッセージは読み取り可能です。これは、PGP ViaCryptドキュメンテーションに含まれています。
* 指定された暗号化アルゴリズムがIDEAの場合は、輸出不可。

S/MIME
* 暗号化にRC2またはRC4が使用される場合は、40ビットと56ビットの輸出制限があります。

MOSS
* フル・キー長については輸出不可。
* 使用されるデータ暗号化アルゴリズムによります。RFC1423はCBCモードのDESを指定しており、これは輸出できません。ただしMossは、様々な暗号化アルゴリズムを使用できます。

MSP
* 使用されるキー管理とデータ暗号化アルゴリズムによります。MSPは、様々な暗号化アルゴリズムを使用できます。

2) ユーザに見えない方法で容易に製品に統合ができる

PGP V3.0
* V3.0なら多分可能。それ以前のバージョンでは不可能。
* これについては、一般的な合意はないようです。

S/MIME
* 可能です。

MOSS
* 不明

MSP
* 可能です。 - 署名入り受信確認のサポートには、GUIエンハンスメントが必要です。

3) 国際的に同種バージョンと完全に互換可能

PGP V3.0
* PGPバージョン2.6は、それ以前のバージョンと互換可能です。バージョン3.0も多分可能と思われます。

S/MIME
* RSAは相互利用可能プログラムを適所に活用しています。
* 仕様へのインプリメントによって相互利用可能性が保証されます。

MOSS
* Mossは特定のセキュリティ・アルゴリズムを必要としません。Mossは、各メッセージにどのアルゴリズムが使用されているかを識別する手段を提供します。RFC 1423に、一連のアルゴリズムが定義されています。

MSP
* 同じ暗号化が使用される場合、仕様へのインプリメントによって相互利用可能性が保証されます。

4) 現在のインプリメンテーション状況

PGP V3.0
* バージョン3.0は完了（3Q96）
* バージョン2.6は使用可能

	*	Qualcomm
	*	Premail
	*	MichaelのPGPMIME
S/MIME	*	2社がインプリメント完了、他の数社が着手。現在12社が、Commercenetがスポンサーであるパイロット計画でインプリメント中。
	*	製品と開発ツールキット出荷中。
MOSS	*	TIS、InnosoftおよびSupplyTech
MSP	*	SPYRUS, Nortel, Xerox, LJL、BBN、およびJ.G.Van Dykeはすべてインプリメント完了。
	*	製品出荷中
	*	軍メッセージに使用中。

5) 機密性

-PGP V3.0	*	Yes
S/MIME	*	Yes
MOSS	*	Yes
MSP	*	Yes

6) シグネチャ

PGP V3.0	*	Yes
S/MIME	*	Yes
MOSS	*	Yes
MSP	*	Yes

7) 受信確認返送

PGP V3.0	*	No
S/MIME	*	No
MOSS	*	No
MSP	*	Yes - 配信証明付きの受諾をサポート。

8) 配信通知

PGP V3.0	*	MIME拡張RFC1891-94による
S/MIME	*	MIME拡張RFC1891-94による
MOSS	*	MIME拡張RFC1891-94による
MSP	*	MIME拡張RFC1891-94による

9) 認証

PGP V3.0	*	Yes
S/MIME	*	Yes
MOSS	*	Yes
MSP	*	Yes

10) マルチメディア

PGP V3.0	*	Yes
S/MIME	*	Yes
MOSS	*	Yes
MSP	*	Yes

11) 完全性

PGP V3.0 * Yes
S/MIME * Yes
MOSS * Yes
MSP * Yes

12) 信頼モデル（キーの管理と取消）

PGP V3.0 * PGP 3.0は公開キー証明の階層モデルを持っています。
* 現行バージョンではキー管理にRFAが使用されています。
* 特別なキー取消
S/MIME * RSAベースのX.509全バージョンの使用
* この製品には、程なくNTのEntrusが使用可能になります。
MOSS * RSAとDESに基づくキー管理。
MSP * X.509全バージョン

13) 証明（情報、書式、配布）

PGP V3.0 * Yes - 所有権のある"Key rings"を使用。V3が何を使用するかは不明。
S/MIME * Yes - X.509全バージョンを使用。
MOSS * Yes - オプションX.509を使用。
MSP * Yes - X.509を使用。

14) 基礎構造オーバヘッド

PGP V3.0 * Base64エンコーディング
S/MIME * ASN.1 - BERおよびDERエンコーディング
MOSS * Base64エンコーディング
MSP * Base64エンコーディングとANSI.1エンコーディング

15) エンベロープのタイプ

PGP V3.0 * MIME/ASCII
S/MIME * PKCS #7 ASN.1およびMIME
MOSS * MIME/ASCKK
MSP * MIME/ASN.1

16) エンベロープ/構造仕様（ASN1またはASCII）

PGP V3.0 * ASCII
S/MIME * ASN.1およびASCII
MOSS * ASCII
MSP * ASN.1

17) サポートされるアルゴリズム（リストすると:暗号化、キー管理、一方向ハッシュ、デジタル・シグネチャ、暗号化キー長さ）

PGP V3.0 * 3.0以前はRSAおよびIDEA
* V3.0にはDiffie HellmanおよびDSA
* CBCにはIDEA
* MD5およびRSA
* 一般用には128、商用には512、軍用には2048。
* 128ビットIDEAキー長さ

S/MIME
* RSA
* RC2、RC4およびRC5
* MD5およびRSA
* SHA-V
* 注:S/MIMEはMossと同様、書式であり、どのタイプのアルゴリズムも指定できます。RSAは当然独自のアルゴリズムを指定します。
* Triple-DES/RC5

MOSS
* CBCにはDES
* RSAまたはDES
* MD2/MD5およびRSA
* DES用の56ビット・キー長さ
* FORTEZZA
* 注:MossはS/MIMEと同様、様々な暗号化アルゴリズムを使用できます。上記の定義された一連のアルゴリズムは、RFC 1423にあります。

MSP
* アルゴリズム無関係。以下を使用するインプリメンテーションはあります。
* RSAおよびDES
* FOTEZZA（DSS SHA-1、KEA、Skipjack）

18) EDIFACT AUTACKコード・リストのある共通アルゴリズム

PGP V3.0
* RSA（Yes）
* IDEA（Yes）
* DSA（Yes）
* MD5（Yes）

S/MIME
* RSA（Yes）
* RC2およびRC4（Yes）
* DES（Yes）
* MD5（Yes）

MOSS
* RSA（Yes）
* DES（Yes）
* MD5（Yes）

MSP
* RSA（Yes）
* DES（Yes）
* MD5（Yes）
* DSS（Yes）
* SHA-1（Yes?）

19) MIMEマルチパート/署名入りデータの受信（読み取り不能シグネチャ）のための他との共存

PGP V3.0
* Yes - V3.0

S/MIME
* Yes - ただしユーザ選択可能

MOSS
* Yes

MSP
* MIMEエンキャプスレーションとともに使用されるならYes（<draft-housley-msp-mine-01.txt>を参照）。

20) RFC822/MIMEリーダによって読み取り可能な署名入りメッセージ本体

PGP V3.0
* V3.0ならYes

S/MIME
* マルチパート/署名入りのいずれかのオプションが使用されるならYes。

MOSS
* Yes

MSP * MIMEエンキャプスレーションとともに使用されるならYes

21) 署名入りドキュメントと独立したシグネチャ

PGP V3.0 * Yes
S/MIME * No
MOSS * Yes
MSP * Yes

22) 逆互換性

PGP V3.0 * PGPへ
S/MIME * PEMへ
MOSS * PEMへ
MSP * なし

23) 所有権のあるアルゴリズムを使用するか?

PGP V3.0 * バージョン3.0は、1997年に期限切れとなる特許権を持つDiffie-Hallmanを使用することになっています。バージョン3.0はDSA（NASで開発されたデジタル・シグネチャ・アルゴリズム）を使用する予定です。
S/MIME * Yes、ただし様々なオプションをサポートします。
MOSS * Yes、ただし様々なサポートをします。
MSP * 標準アルゴリズム（FIPSとX9）と所有権のあるアルゴリズムの両方を使用します。

24) EDIのための十分なセキュリティ

PGP V3.0 * Yes
S/MIME * Yes
MOSS * Yes
MSP * Yes

25) スケーラブルかどうか

PGP V3.0 * 経験不足のため評価できません。現在の信頼モデルは、十分にスケーラブルとは言えません。
S/MIME * 経験不足のため評価できません。
MOSS * 経験不足のため評価できません。
MSP * Yes

26) 強固なMIMEの統合

PGP V3.0 * V3.0ならYes
S/MIME * Yes - ただしPKCSテクノロジーとMIMEが混在しています。純粋インターネット派は、この混合は気に入らないようです。
MOSS * Yes
MSP * Yes（<draft-housley-msp-mime-01.txt>を参照）

27) 可変キーサイズがサポートされているか

PGP V3.0 * No
S/MIME * Yes - 40～128ビット。
* 対象型512～2048ビットRSA
MOSS * Yes

MSP
* Yes
* 対象型（DES = 56ビット、SKIPJACK = 80ビット）
* シグネチャ（DDS = 512..1024ビット、RSA = 512..2048ビット）
* キー管理（KEA = 1024ビット、RSA = 512..2048ビット）

28) X.509のみかまたは他の証明配信方法か

PGP V3.0
S/MINE * X.509の全バージョン
MOSS
MSP * X.509の全バージョン

29) 強力なAPIとツールキット

PGP V3.0 * V3.0はYes - 予測
S/MIME * Yes
MOSS * No
MSP * Yes - DISAはAPIをX/Openに提示。
* 2つ以上のツールキットを販売。

30) ツールキットはUNの通商停止を受けずにすべての国で入手可能

PGP V3.0 * 代替ソースから多分入手可能
S/MIME * 大部分の国で輸出バージョンが入手可能
MOSS * 大部分の国で輸出バージョンが入手可能（40ビットDESか?）
MSP * 大部分の国で輸出バージョンが入手可能。ツールキットは、フランスを含む多くの国へ輸出されています。
* 代替ソースも同様。

31) 将来のEDIの方向に合っているか

PGP V3.0 * 不明
S/MIM * 不明
MOSS * 不明
MSP * 不明

著者住所:
Chuck Shih
610 Caribbean Drive
Sunnyvale, CA. 94089
TEL:408-542-3282
FAX:408-542-3282
<drummond@onramp.net>

3．海外におけるＥＤＩ標準活動の一例

（NORSK EDIPRO INTERCHANGE AGREEMENT）

ノルウェーEDIPROで作成されたデータ交換協定書で、ECE/WP.4 GE.1，GE.2 第55会期(18-20 March 1997)に提案されたものです。海外のＥＤＩ標準活動の１つとしてご紹介します。

UNITED
NATIONS

E

Economic and Social
Council

Distr.
RESTRICTED

TRADE/WP.4/R.1282
3 February 1997

ENGLISH ONLY

ECONOMIC COMMISSION FOR EUROPE

COMMITTEE ON THE DEVELOPMENT OF TRADE

Working Party on Facilitation of International
Trade Procedures
(Item 11 of the provisional agenda of the
Meeting of Experts on Data Elements
and Automatic Data Interchange (GE.1),
Fifty-fifth session, 19-20 March 1997
and Item 8 of the provisional agenda of the
Meeting of Experts on Procedures and Documentation
(GE.2), fifty-fifth session, 18-19 March 1997)

NORSK EDIPRO INTERCHANGE AGREEMENT

* * *

Submitted by the Norwegian Delegation *

This document is a contribution from NORSK EDIPRO to the Legal Rapporteur team's work on interchange agreements and is for information and discussion.

* The present document is reproduced in the form in which it was received by the secretariat.

GE.97- 30169

Table of Contents

1. Introduction

Norsk EDIPRO has designed a model interchange agreement for parties exchanging EDI messages based on extensive preparations involving many participants. The present model agreement is updated as of August 1995, and is the second issued version of this agreement. The first version was released in March 1993 as version 2.0, and has subsequently been introduced among many EDI users in Norway. We have endeavoured to include the experiences from this process in the present agreement (version 3.0).

As part of the interchange agreement it is assumed that the parties design the necessary appendices, notably Appendix 1 - Use of Various Message Types, which regulates the relevant message(s) between the parties. In an EDIFACT context there are many different message types that may be applied.

In order to further help the parties Norsk EDIPRO has also developed a standard text for Appendix 1, which covers general terms for the many different EDI messages. This model text includes several blanks for users to fill in with more details for easy adaptation to individual contracts. By using this appendix as a basis together with the interchange agreement one has achieved a comprehensive agreement that is carefully prepared "from A to Z", thus creating a sense of security, as well as effectiveness and cost savings upon entering a new field. A brief guide for completing Appendix 1 on message types has also been developed by Norsk EDIPRO.

Norsk EDIPRO's model agreement for exchange of EDI messages in Norway has been evaluated closely in relation to the EU "European Model EDI Agreement" for exchange of EDI messages in Europe, adopted in 1994, and the corresponding UN 1995 draft agreement on international or global EDI interchange "UN/ECE Model Interchange Agreement for the International Commercial Use of Electronic Data Interchange".

The work on translation of this agreement has been performed by Ms Anki Thestrup in assistance with Mr.Knut Vala and Mr.Asbjørn Hovstø.

The existance of this agreement will be announced between the UN/ECE member countries..

In my opinion, Norsk EDIPRO's model interchange agreement with the attached standard text for Appendix 1 - Use of Various Message Types is a good starting point for achieving legal security in a relatively new field of agreements.

Amund Eriksen, L.L.B.

Head of Norsk EDIPRO's technical committee on legal, security and auditing matters

2. Norsk EDIPRO Interchange Agreement

Signing of the Interchange Agreement

Norsk EDIPRO
Interchange Agreement
Version 3.0
is concluded by and between the following parties:

_____
(hereinafter called Party A)(hereinafter called Party B)

_____
(identification no.)(identification no.)

(If desired, further identification of the parties can be made here, for instance by specifying the business register number)

Check the appendices which are part of the agreement Appendix no.	Name of Appendix	Part of the Agreement? Yes	No
1	**Use of Various Message Types** (List every single Appendix 1 that is specified between the parties. Point A in Appendix 1 is entered here):		
2	**GENERAL MODIFICATIONS OF THE STANDARD TEXT**		
3	**INFORMATION ABOUT THE PARTIES**		
4	**OPTIONS IN EDIFACT SYNTAX**		
5	**COMMUNICATION METHOD**		
6	**LIST OF MEMBERS** (only for Group agreement)		

The agreement is valid from: (date) _____
In the Norsk EDIPRO Interchange Agreement version 3.0 of August 1995 the entire standard text applies. Deviations are specified in appendices.

Binding signature

For Party A: For Party B:
Date:_____ Date:_____

Sign.:_____ Sign.:_____

The agreement has been signed in _____ copies, of which each party keeps _____copy(ies).

Written communications

To Party A: To Party B:
Name:_____ Name:_____

Address:_____ Address:_____

Postal code:_____ Postal code:_____

Standard text

Table of contents for standard text

1. Objective

The signatories aim to achieve an electronic interchange of documents that is rapid, effective and correct for both parties.
Furthermore, the purpose of this agreement is to provide legal security and legal obligations for both parties in the EDI cooperation.
The agreement does not regulate the commercial interests related to the exchange of EDI messages.

2. Structure and amendment rules

The Norsk EDIPRO Interchange Agreement consists of the standard text (this) and appendices. The interchange agreement and relevant appendices regulate the parties' liabilities, obligations and rights related to exchange of electronic data. The appendices used between the parties are specified above under *Signing of Interchange Agreement*:
The interchange agreement includes the following appendices:

3. Order of precedence

In case of disputes, the following order of precedence applies:

1. A general business agreement between the parties
2. Specification(s) of EDI message(s) referring to implementation guide (*cf. Appendix 1).*
3. Amendments and supplements (*cf. Appendix 2).*
4. *Norsk EDIPRO Interchange Agreement (this text).*

4. Services from a third party (e.g. computer network supplier)

The contracting party which employs a third party to transmit EDI messages is equally responsible for this party's actions, errors or omissions as for his own conduct. The third party in this context is considered to be acting on his behalf.
Each contracting party is committed to entering an agreement with his third party which as a minimum shall regulate responsibilities for:
- transmitting the content of an EDI message without alterations, in the correct format to the right receiver within the time limits that have been determined for each message type.
- maintaining professional secrecy about the information which this company and its staff may become familiar with while performing their services.
- safeguarding access to the computer network.

Moreover, the party which tells another party to use a given third party supplier shall be liable for all actions, errors or omissions from the third party supplier.

5. Operational equipment and modifications

Each party is responsible for acquiring, testing and maintaining the necessary equipment, programs and services for transmitting, receiving, translating, recording and storing EDI messages.
None of the parties shall carry out any modifications of their operational equipment or routines that affect the exchange of EDI messages between the parties, without these modifications having been agreed on between the parties.

6. Cost sharing

Under regular operations each party bears his own costs for the exchange of EDI messages, unless otherwise specifically agreed (*cf. Appendix 2).*
The parties are obliged to be capable of transmitting and receiving test data for interchange and trial purposes during introduction of EDI and during upgrading or modification of equipment by the other party. If this entails unreasonable costs/additional work for the other party, he can demand another distribution of costs than agreed on for normal operations.

7. Supervision of transmission

The EDI message must conform to the agreed message definition in terms of the EDIFACT syntax described in Appendix 4 and according to the implementation guide attached to *Appendix 1 Use of Various Message Types*. In addition, the data must be subjected to necessary control at the time of transmission, both of the commercial content and of the EDI message itself, to avoid repeated, incomplete or faulty transmissions.

8. Verification and acknowledgement of EDI messages

The receiver shall immediately check that the EDI message is from the right sender and that it conforms to the agreed EDIFACT syntax and to the implementation guide. The receiver shall as soon as possible inform the sender of errors, such as a faulty transmission, a double transmission of EDI messages, or errors or shortcomings in the received data.
Appendix 1 Use of Various Message Types regulates the use of verification and acknowledgement messages.
If a rejected or faulty EDI message is sent once more it must be clearly expressed that this is a corrected EDI message.

9. Processing time

Each party is obliged, manually and/or automatically, to process received EDI messages within one business day of the time of receipt, or within the time limits specified in *Appendix 1 Use of Various Message Types*. Other time limits can be agreed on for a particular transmission or specific period of time.

10. Security

The parties are committed to implementing and maintaining the agreed measures and procedures to secure protection of EDI messages from unauthorized persons and to ensure that messages are not altered, delayed, destroyed or lost. Security measures are listed in *Appendix 1 Use of Various Message Types*.

11. Protection of confidential information

The parties are obliged to protect EDI messages, that at least one party claims contains confidential information, from access by unauthorized personnel. Such information shall only be used for the purposes decided on by the parties, according to established business practice, or in accordance with the existing rules.

12. Conformity with applicable law

For exchange of EDI messages containing information in which applicable laws and regulations establish specific requirements, the received information must be dealt with in accordance with the relevant rules.

13. Requirements for interchange log and storage

Each party must keep a complete interchange log for storing EDI messages, specifying date, time, address of sender and receiver, and the version of the applied implementation guide. These data must be stored by the sender in the transmitted format, and by the receiver in the received format.
Adequate protective measures must be implemented to protect the stored data from being intentionally or unintentionally deleted or altered.
Unless Norwegian law stipulates specific requirements for storage time, it is up to the parties to decide how long the data shall be stored. The storage times for various message types may be established in *Appendix 1 Use of Various Message Types*. The interchange log must usually be preserved for a minimum of six months.
The parties must take precautions to ensure that the EDI messages are stored in such a way that they can later be printed out on paper.

14. Legal status

The parties accept that EDI messages which are prepared and transmitted in accordance with the interchange agreement shall have the same legal status for both parties as the equivalent paper document.

15. Force majeure

Should an exceptional situation arise that is beyond the control of the parties, making it impossible for one party to fulfil his obligations, and which is considered force majeure according to Norwegian law, then the other party must immediately be notified in writing. The obligations of the affected party will be suspended for the duration of the exceptional situation. The other party's obligations are suspended for the same period.
In a force majeure situation the other party can only cancel the agreement provided the affected party consents. If the situation lasts, or is expected to last longer than 30 calendar days, counting from the day it occurred, then the agreement can be cancelled unilaterally, after a notice of only 15 calendar days. Other duration periods can be agreed on between the parties and will be included in Appendix 2.
In a force majeure situation each party is obliged to inform the other party of all matters that may be considered important for the other party. Such information must be given as soon as possible.

16. Financial losses for which none of the parties is to blame

Each party must bear the financial loss for his part of the contract if the loss is the result of an accidental circumstance or mishap for which none of the parties can be blamed.

17. Breach of contract

If one party does not fulfil his obligations in accordance with the interchange agreement and appendices, and circumstances as described in 15 and 16 do not apply, this constitutes a breach or contract. A defective and/or delayed fulfilment of obligations may also constitute a breach of contract.
The parties have a mutual obligation to notify each other as soon as possible if situations arise that have resulted in, or will result in a defective or delayed fulfilment of obligations.
If one party wishes to charge the other party with breach of contract, he must do so in writing as soon as possible after having become aware of the situation.

18. Sanctions by breach of contract

The party which has been affected by the other's breach of contract can retain a proportionate share of his contribution according to the contract until the matter has been put right, or may demand a reduction in price or other compensation.
If one of the parties significantly fails to fulfil his obligations and has not taken the necessary remedial action within 14 days after having received written notice, the other party is entitled to cancel the agreement immediately.

19. Damages

Each party is entitled to claim damages against the other party for losses that could reasonably be expected to have been the result of the breach of contract, unless the other party can prove that he is not to blame.

Compensation is not granted for indirect losses (interruptions, expected profits, etc.) unless gross negligence or intent has been shown by the party himself of by someone for whom he is responsible.

20. Duration and terminability of agreement

Each party can terminate this agreement at 2 months' written notice. Termination of the agreement shall not affect the exchanges or related transactions that have taken place before the termination date. Article 11 of the agreement (protection of confidential information), article 12 (conformity with applicable law) and article 13 (requirements for interchange log and storage) shall continue to apply after termination of the agreement.

21. Conveyance

The parties are not entitled to transfer rights and obligations regulated by this agreement and appendices to a third party without the other party's written consent.

22. Disputes

Disputes concerning this agreement that are not resolved amicably shall be settled by a Norwegian court of law, unless the parties agree on arbitration pursuant to chapter 32 of the Norwegian Civil Dispute Law.
The arbitration tribunal is composed of three members. Each party selects an arbitrator, the two arbitrators then elect a third arbitrator as chairman of the tribunal.

23. Definitions

EDI:
Abbreviation for Electronic Data Interchange. EDI means electronic interchange of data in a standardized format (in the form of a message) between parties for subsequent computer processing.
EDI software:
By EDI software is meant the computer programs used to transfer and receive EDI messages. The main functions carried out by EDI software are the following:

1. An **operative and administrative module**, for updating purposes, status reports, etc.
2. Sending and receiving data to/from application (**interface**). The actual application(s) is/are not considered part of the EDI software.
3. Translation between internal message formats and agreed standard format (**EDI conversion**).
4. Operative and administrative functions for processing message definitions (**Mess.def.**), partner profiles (**Part prof.**), interchange log (**Int.log**) or error log (**Err. log**).
5. Sending and receiving EDI messages to/from computer network supplier or EDI partner (**Communication interface**).

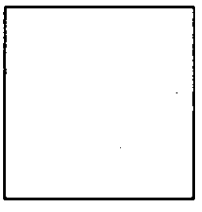


Figure 1: Illustration of a possible EDI solution

Interchange log:
Historical data journal preserving all EDI messages in the transmitted or received format, also including status information, e.g. *date and hour* of each transmission. The status information will usually be included as an integral part of the interchange log, or registered in a separate "status log". It is assumed that the interchange log is adequately protected to ensure that data are not deleted or altered.
EDI message:
A continuous set of data, structured according to the UN/EDIFACT rules.
UN/EDIFACT
The United Nations rules for electronic data interchange for administration, commerce and transport (United Nations Rules for Electronic Data Interchange for Administration, Commerce and Transport). The rules encompass a set of standards, catalogues and guidelines for exchange of structured data, especially related to trade of commodities and services between independent computer-based information systems. The rules are recommended within the framework of the UN, are approved and published by the UN/ECE as the UN catalogue for exchange of commercial data (UNTDID) and is maintained through fixed procedures.

UN/ECE
The UN economic commission for Europe (United Nations Economic Commission for Europe) is one of five regional commissions within the UN. The UN/ECE covers North America, Western Europe and Eastern Europe, with its head office in Geneva. The UN/ECE's working group no. 4 (UN/ECE/WO.4 - Working Party on Facilitation of International Trade Procedures) is also in charge of developing and maintaining UN/EDIFACT.

UNB segment:
A service segment which introduces and identifies an exchange in EDIFACT.

Interchange:
By interchange in this agreement is meant all data transmitted between the parties in the form of a structured set of messages and service segments, starting with an interchange head and ending with an interchange tail.

Interchange agreement:
By interchange agreement in the agreement is meant an agreement between parties, regulating on a general basis their rights and obligations in the use of EDI.

Group agreement:
In a group agreement the second party constitutes a group, identified for instance by the name of an organization. Upon signing the agreement, the individual members are connected to each other in such a way that each individual in interaction with other members accepts that the stipulations of this agreement and appendices are equally valid as if they had been approved bilaterally by the two parties.

Third party:
A third party acts as an intermediary for one or both parties and enables EDI transmission. The relationship is regulated in a communication agreement between each trading party and his third party (usually a computer network supplier).

Transmission service:
By transmission service is understood the sum of services and functions carried out by the communications service (functions offered by a given communications system) and the EDI software for handling and transmitting EDI messages. Manual routines, documentation and rules for the services/functions are also included.

Trusted Third Party (TTP):
A Trusted Third Party in this context is an important element in the electronic data interchange infrastructure, and is accessible to users requiring various types of security services to establish confidence in the EDI and business functions that shall be carried out.

Message manual:
The message manual describes aspects related to one or more message types, or the relationship between various message types. It is the result of message interpretations and the development of new message types. It describes the functions of the message types included in the manual, as well as implementation guides for each message type. Message manuals can be compiled by anybody requiring them, for instance the parties themselves, the user community, trade associations, or Norsk EDIPRO.

Implementation Guide:
This is a precise description of how to employ segments (a previously defined and identified sequence of functionally dependent data element values) and data elements (a data unit with a detailed specification of identification, description and value) in a particular message type. The Norwegian Guide to Using EDIFACT (part 5) provides a more detailed description of the EDIFACT structure. Implementation Guides can be formulated by anybody requiring them, for instance the parties themselves, the user community, trade associations, or Norsk EDIPRO.

Control message:
This is a message generated by the receiver's EDI software, and is sent to the sender to acknowledge receipt of the initial EDI message (the EDIFACT message CONTRL is one example of a control message).

Acknowledgement message:
This is a status message received by a third party with information about an EDI message which the sender has just sent (attempted to send) via this third party.

Business receipt:
By business receipt is meant an EDI message sent by one party to confirm handling of the business content of a received EDI message (e.g. order confirmation).

Message group:
By message group is understood one or more message of the same type, introduced by a message group head and concluded by a message group tail.
Requirements for written communication between the parties:
By written communication is understood a handwritten signature on a paper document or telefax. E-mail and other types of electronic transmission of messages may also be used.

Appendix 1 -
Use of Various Message Types

The following is to be regarded as Norsk EDIPRO's recommendation, specifying how similar message types are to be used between the parties in electronic transmission of documents (EDI) based on UN/EDIFACT. A guide to completing and using the appendix is provided in a separate chapter (chapter 4).

Table of contents for the appendix

1. Registration of Appendix 1

This appendix regulates the use of EDI messages for

A

and is entered into between

B

Party A
and

C

Party B

The appendix is based on the Interchange Agreement between the parties dated
D

The following sub-appendices make up an integrated section of this appendix:

E

Sub-appendix	Description	Part of the Agreement? Yes	No
1	Particular modifications, specifications and additions to aspects regulated in the Interchange Agreement (IA)		
2	Modifications, specifications and additions to Appendix 1		
3	Modifications, specifications and additions to the Implementation Guide		
4	Operating routines		

Reference is made to the provisions of the Interchange Agreement's article 2, in which the parties agree that Appendix 1 - Use of Various Message Types can be applied to new EDI messages on the basis on the Interchange Agreement and without having to modify the Agreement itself.

Binding signature:
F *Party A Party B*

Date *Signature* *Title*		

2. Identification of the parties

To identify the parties in transmitted exchanges and message groups, the identification number listed in Appendix 3 shall be used, unless otherwise stated in sub-appendix 1.

3. EDI messages and implementation guides

All EDI messages exchanged between the parties shall follow the message definition documented in the following Implementation Guides:

Message type	Reference to Implementation Guide

In transmissions between the parties EDI messages shall be identified in accordance with the Implementation Guides listed above. Modifications, specifications or additions to the listed Implementation Guides are described in sub-appendix 3.

Times and frequency of EDI message transmission
Transmission of EDI messages between the parties shall take place at the following times:

	Party A	*Party B*
Send to the transmission service (mailbox)		
Collect from the transmission service (mailbox)		

A transmission including all the necessary EDI messages is considered received at the moment that it is made accessible for the receiver at the latter's transmission service (mailbox).

Processing of received EDI messages
EDI messages that have been received must be processed by the receiver within

Message type	*Party A*	*Party B*

4. Acknowledgements and control messages

Use of control message
The service message CONTRL is used by the parties as follows:

	Party A	*Party B*
Acknowledge receipt of transmission		
Confirm that the EDI messages have correct syntax		

If an acknowledgement has not been requested (data element 0031 - acknowledgement request in the received UNB segment), the sender shall still be notified by CONTRL if there is an error in the transmission.

Received transmissions and messages shall be processed and reported by the receiver within:

Message type	*Party A*	*Party B*

If Acknowledgements are missing then the contact person listed in Appendix 3 of the Interchange Agreement must be contacted immediately.

CONTRL messages shall follow specifications given in the document *TRADE/WP.4/R.1010* with corrigendum, issued by UN/ECE.
A positive acknowledgement in the form of CONTRL means that no syntax errors are found in the particular section for which the message applies, that the receiver will assume responsibility for processing this part, and that it is the receiver's responsibility to notify the sender as soon as possible (by other means than CONTRL) if the data are not to be processed by the receiver after all.
A negative acknowledgement in the form of CONTRL means that an error has been detected, or that the receiver for other reasons rejects the section covered by the acknowledgement.

Use of business receipt
The business content of the received EDI messages shall be acknowledged as follows:

Received message type	*Business receipt to be returned? (yes/no)*	*Message type*

5. Use of EDIFACT syntax

EDIFACT syntax shall be used as described in *The Norwegian Guide to Using EDIFACT*, version 2.0, part 5 for all exchanges between the parties unless otherwise specifically agreed on between them.

6. Security

The following security mechanisms shall be used for EDI messages transmitted between the parties:

Message type	*Security mechanism used (yes/no)?*						
	Sequence number	Control count	Signed controlcount	Digital signature	Crypto-graphy	Use of TTP	Other
Algorithm for cryptography							
Algorithm for signature							

(TTP - Trusted Third Party)
Details concerning use of the various security procedures are listed in sub-appendix 2.

7. Storage of EDI messages

Exchanged EDI-messages are stored by both parties. The following minimum storage time is agreed on:

Message type	*Party A*	*Party B*

8. Operating routines and deviations

Operating routines regulating transmission and processing of EDI messages and procedures in the case of possible deviations are specified in sub-appendix 4.

9. Validity of the appendix

In the case of a termination of the Interchange Agreement there will be no reason to keep this appendix. A termination of the Agreement will thus automatically mean a termination of this appendix.

Each party can terminate this appendix at 2 - two - months notice without also terminating the Interchange Agreement.

If a termination occurs this appendix's requirements as to storage time (cf. article 7) will still be valid for both parties, until the agreed storage time for the last exchange has expired.

10. Modification of the appendix

Modifications of the appendix must be done in writing and require a binding signature from both parties. All specifications, modifications and additions shall be listed in Appendix 2.

11. Sub-appendix 1

Particular modifications, specifications and additions to aspects regulated in the Interchange Agreement that are unique for message types included in Appendix 1

For Party A For Party B:

Sign.: _____ Sign.: _____

Title: _____ Title: _____

12. Sub-appendix 2

Modifications, specifications and additions to Appendix 1

For Party A For Party B:

Sign.: _____ Sign.: _____

Title: _____ Title: _____

13. Sub-appendix 3 -

Modifications, specifications and additions to the Implementation Guides

For Party A For Party B:

Sign.: _____ Sign.: _____

Title: _____ Title: _____

14. Sub-appendix 4 -

Operating routines

For Party A For Party B:

Sign.: _____ Sign.: _____

Title: _____ Title: _____

Appendix 2
GENERAL MODIFICATIONS OF THE STANDARD TEXT

For Party A For Party B:

Sign.: _____ Sign.: _____

Title: _____ Title: _____

Note:
This appendix is updated as of_____ and valid from the same date. The appendix is a specification of deviations to the **Norsk EDIPRO Interchange Agreement** concluded by the parties on_____with entry into force on _____.

Appendix 3
INFORMATION ABOUT THE PARTIES

Contact persons by errors/problems (administrative)
For Party A: For Party B:

Name: _____ Name: _____

Tel: _____ Tel: _____

Contact persons by errors/problems (technical)
For Party A: For Party B:

Name: _____ Name: _____

Tel: _____ Tel: _____

Identification of the parties (sender/receiver) shall be done by means of an identifying element in the UNB segment. Use of the following table is recommended:

Syntax element	Data element	Agreed usage
Identifying element	UNB-0004/0010	
Party identification qualifier	UNB-0007	
Address for reply transmission	UNB-0008	
Address for forwarding	UNB-0014	
Receiver's reference/password	UNB-0022	
Receiver's reference/password qualifier	UNB-0025	
Communications address		

For Party A For Party B:
Sign.: _____ Sign.: _____

Title: _____ Title: _____

Note:
This appendix is updated as of, and valid from the _____. Information in this appendix can be altered without this affecting the validity of **Norsk EDIPRO Interchange Agreement** concluded by the parties.

Appendix 4
OPTIONS IN EDIFACT SYNTAX

The EDIFACT syntax includes several options that the parties (1) may choose to employ and (2) may implement in various ways. Use of the following table is recommended:

EDIFACT syntax shall be used as described in Norwegian Guide to Using EDIFACT, version 2.0 with the following specifications:

Use of UNA		
Use of functional message groups (UNG/UNE)		
Syntax element	Segment/data element	Agreed usage
Syntax level	UNB-0001	
Syntax version	UNB-0002	
Application reference	UNB-0026	
Processing priority	UNB-0029	
Acknowledgement request	UNB-0031	
Exchange identification	UNB-0032	
Test indicator	UNB-0035	
Exchange reference	UNB-0020	
Date (for preparation)	UNB-0017	
Time (for preparation)	UNB-0019	
Common reference	UNH-0068	
Transmission status	UNH-S010	

For Party AFor Party B:

Sign.: _____Sign.: _____

Title: _____Title: _____

Note:

This appendix is updated as of, and valid from the _____. Information in this appendix can be altered without this affecting the validity of **Norsk EDIPRO Interchange Agreement** concluded by the parties.

Appendix 5
COMMUNICATION METHODS

The following telecommunications protocols are used:

By Party A: By Party B:

_____:_____ _____:_____

_____:_____ _____:_____

The following third party suppliers/Computer network are used:

By Party A: By Party B:

_____:_____:_____

_____:_____:_____

For Party A For Party B:

Sign.: _____ Sign.: _____

Title:_____ Title:_____

Note:

This appendix is updated as of, and valid from the _____. Information in this appendix can be altered without this affecting the validity of **Norsk EDIPRO Interchange Agreement** concluded by the parties.

Appendix 6
LIST OF MEMBERS

No.:Name of company:ID no.Contact personTel:

Note:

This appendix is updated as of, and valid from the _____. Information in this appendix can be altered without this affecting the validity of **Norsk EDIPRO Interchange Agreement** concluded by the parties.

3. Guide to completing the Interchange Agreement

General Information about Norsk EDIPRO Interchange Agreement

Background

The Norsk EDIPRO Interchange Agreement has been developed in two stages:

1. Version 2.0 March 1993Includes the Interchange Agreement itself
2. Version 3.0 August 1995Includes a revision of the Interchange Agreement and preparation of Appendix 1 Use of Various Message Types (previously called the Document Agreement).

The development work has been led by Norsk EDIPRO, involving several users from both the public and private sector, together with lawyers with expertise in this area.

New elements in Interchange Agreement Version 3.0

Users who have utilized Interchange Agreement Version 2.0 will find some new elements in Version 3.0, although the structure of the agreement has not been changed. Input elements in Version 3.0 are the following:

1. Needs and requirements that have emerged during the preparatory work forAppendix1 Use of Various Message Types (previously called the Document Agreement).
2. Harmonization of the Interchange Agreement with the UN and EU International EDI agreements.

The main innovations in Norsk EDIPRO Interchange Agreement Version 3.0 are:

Appendices:Appendix 1 Use of Various Message Types.
Appendix 3 Information about the parties requires more thorough specification.
Appendix 4 Options in EDIFACT syntax.
Appendix 5 Communication method.

New articles in the agreement:
Art. 5 Operational equipment and modifications
Art. 10 Security
Art. 12 Conformity with applicable law

Modified articles in the agreement:
Art. 1 Objective
Art. 2 Structure and amendment rules
Art. 4 Contributions from third party
Art. 7 Control during transmission
Art. 8 Verification and acknowledgement of EDI-messages
Art. 11 Protection of confidential information
Art. 17 Breach of contract
Art. 20 Duration and terminability of contract
Art. 21 Conveyance
Art. 23 Definitions

Use of Norsk EDIPRO Interchange Agreement

The Norsk EDIPRO Interchange Agreement is a **model agreement** that can be used for one or more players exchanging EDI messages.

The Interchange agreement can be used for **all types of EDI messages**. Still, the Agreement is limited to exchange of EDI messages following UN/EDIFACT standards.

The Interchange Agreement is primarily for **use in domestic trade**. The agreement can also be used for exchange of EDI messages to other countries, but one should in such cases also consider using UN/EDIFACT Interchange Agreement and/or EU Model EDI agreements.

Structure of the Interchange Agreement
The Interchange Agreement has the following structure:

Main agreement:	Appendix:	Sub-appendix:
The Interchange Agreement (standard text)	Appendix to the Interchange Agreement	Appendix to Use of the Various Message Types
	1. Use of messages	1. Special modifications and additions to the Interchange Agreement 2. Modifications, specifications and additions to Appendix 1 3. Modifications, specifications and additions to Implementation Guide 4. Operating routines
	2. General modifications to the standard text. 3. Information about the parties 4. Options in EDIFACT syntax 5. Communication method 6. List of members	

Completion of the Norsk EDIPRO Interchange Agreement

The **Norsk EDIPRO Interchange Agreement** consists of a main agreement (standard text) and attached appendices:

1. The Interchange Agreement itself is the main contract between the EDI partners, in which the parties regulate general terms, i.e. that are not tied to a particular EDI message. This agreement is a standard text. If modifications or additions to this text are desired, it must be done in Appendix 2. Only one Interchange Agreement is concluded between the parties.

Preceding the Interchange Agreement there are 2 pages for signing of the agreement itself. The following items need to be filled in:

- Names of the parties and identification no.
- In the table *Check the appendices which are part of the agreement* check **Yes** or **No** for each appendix. If **Appendix 1 Use of Various Message Types** is part of the agreement, list the message types activated, i.e. art. A in Appendix 1. Up to 5 different Appendix 1's can be listed in the table.
- Finally write the date for the entry into force of the agreement and sign.

2. Completion of each Appendix

Appendix 1 Use of Various Message Types is formulated as a filling-in agreement, but is not an independent agreement between the parties. This means that filling in Appendix 1 Use of Various Message Types presupposes that the parties have already concluded an Interchange Agreement. Appendix 1 is used for reaching agreement on aspects that apply to one or more types of EDI messages. Note that one filling-in agreement may specify several EDI messages. Besides, the parties can list as many types of EDI messages as they want in Appendix 1. In specifying each Appendix 1 in the table *Check the appendices that are part of the agreement* you will maintain control of how many filling-in agreements (Appendix 1) that are used by the parties. There is also a guide to completing Appendix 1.

You should also note that Appendix 1 has 5 Sub-Appendices, only Appendix 1 has sub-appendices. They are helpful in further specifying use of the Message types.

Appendix 3 Information about the parties, 4 Options in EDIFACT syntax and **5 Communication method** are used to specify some values that are similar, i.e. independent of the EDI message type.

Appendix 6 List of members is used when a Group Agreement has been concluded.

Note that **all active appendices, apart from Appendix 6, must be signed**. One must also fill in the date for the entry into force.

Comments to the Norsk EDIPRO Interchange Agreement

Finally, we have included a questionnaire to be used for comments or suggested changes in the Interchange Agreement.

Completion of the Norsk EDIPRO Interchange Agreement

The **Norsk EDIPRO Interchange Agreement** consists of a main agreement (standard text) and attached appendices:

1. The Interchange Agreement itself is the main contract between the EDI partners, in which the parties regulate general terms, i.e. that are not tied to a particular EDI message. This agreement is a standard text. If modifications or additions to this text are desired, it must be done in Appendix 2. Only one Interchange Agreement is concluded between the parties.

Preceding the Interchange Agreement there are 2 pages for signing of the agreement itself. The following items need to be filled in:

- Names of the parties and identification no.
- In the table *Check the appendices which are part of the agreement* check **Yes** or **No** for each appendix. If **Appendix 1 Use of Various Message Types** is part of the agreement, list the message types activated, i.e. art. A in Appendix 1. Up to 5 different Appendix 1's can be listed in the table.
- Finally write the date for the entry into force of the agreement and sign.

2. Completion of each Appendix

Appendix 1 Use of Various Message Types is formulated as a filling-in agreement, but is not an independent agreement between the parties. This means that filling in Appendix 1 Use of Various Message Types presupposes that the parties have already concluded an Interchange Agreement. Appendix 1 is used for reaching agreement on aspects that apply to one or more types of EDI messages. Note that one filling-in agreement may specify several EDI messages. Besides, the parties can list as many types of EDI messages as they want in Appendix 1. In specifying each Appendix 1 in the table *Check the appendices that are part of the agreement* you will maintain control of how many filling-in agreements (Appendix 1) that are used by the parties. There is also a guide to completing Appendix 1.

You should also note that Appendix 1 has 5 Sub-Appendices, only Appendix 1 has sub-appendices. They are helpful in further specifying use of the Message types.

Appendix 3 Information about the parties, 4 Options in EDIFACT syntax and **5 Communication method** are used to specify some values that are similar, i.e. independent of the EDI message type.

Appendix 6 List of members is used when a Group Agreement has been concluded.

Note that **all active appendices, apart from Appendix 6, must be signed**. One must also fill in the date for the entry into force.

Comments to the Norsk EDIPRO Interchange Agreement

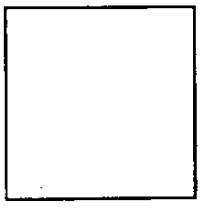
Finally, we have included a questionnaire to be used for comments or suggested changes in the Interchange Agreement.

4. Guide to completing Appendix 1 Use of Various Message Types

This chapter provides a guide to completing and using Appendix 1 - Use of Various Message Types.
The text itself is found in a separate chapter (chapter 2.3).

The connection between various documents and agreements in an EDI relationship

Norsk EDIPRO's Interchange Agreement with attached appendices makes up one element in a comprehensive structure of necessary agreements and specifications to regulate all technical and business-related aspects in the use of EDI. The figure below illustrates the elements involved and the connection between them.



1 Agreements

The following agreements are normally present to regulate the parties' rights and obligations in an EDI relationship:

Business agreement, regulating the business relationship between the parties. Typical factors of a business agreement are discounts, delivery and payment terms. Business agreements are not unique for an EDI-based relationship and often exist from before.

Interchange agreement, regulating the parties rights' and obligations in the use of EDI. The Interchange Agreement will usually be independent of the message type that is exchanged between the parties.

In addition to these agreements the parties will also enter into separate agreements with their service suppliers (e.g. communications contract with computer network supplier).

2 Specifications

The following documents will normally be used to specify the use of EDI messages:

Message manual, which describes and explains the use of various message types and the connection between certain message types. A message manual is the result of a message interpretation or the development of a new message type. A message manual describes how the messages function and provides an implementation guide for each message type.

The description of functions describes the area covered by the message manual (e.g. order processing, payments, etc.), giving a description of the aspects that apply generally to all message types or that concern the connection between certain message types.

The implementation guide is a precise description of how segments and data elements are used in the Various Message Types.

Principles for formulating Appendix 1-Use of Various Message Types

1 What is included in the appendix

The aspects normally covered by the Interchange Agreement's Appendix 1 are mainly technical and operational, related to the parties' EDI solutions. Typical elements covered include:

- what message types are exchanged and which Implementation Guide is applied
- use of the CONTRL message
- required processing time of the receiver
- when messages shall/can be sent
- etc.

The question of which aspects shall/should be agreed on is largely independent of what message types are exchanged between the parties. For example, it will always be relevant to agree on the processing time for all types of EDI messages. The exact values, on the other hand, will possibly vary, depending on the parties, message types and the parties' requirements to security, for instance. For example, it will be appropriate to establish various requirements for processing time, depending on the message type, since some EDI messages have shorter time limits than others.

Appendix 1 to Norsk EDIPRO's Interchange Agreement aims to cover as many factors as possible that apply for a large number of EDI messages. The appendix is prepared in such a way that the parties must fill in the relevant values that apply to their use of the messages. **It is assumed that all blanks in the agreement are filled in.**

2 Connection to a business agreement

The existence and extent of Business agreements within different trades vary greatly. In addition to the purely technical aspects it may thus be relevant to specify some factors on the business-related use and understanding of EDI messages. In this way the Interchange Agreement, and in particular Appendix 1, may contribute to a formalization of the business relationship between the parties. This is especially relevant in those cases where there is no business agreement. Such factors in the wholesale and retail trade may include:

- time limits for changing an EDI order
- which products/services can be ordered by means of EDI
- time limits for executing an order according to when the EDI order has been received

Such business aspects are not covered by the Norsk EDIPRO Interchange Agreement. If the parties wish to specify such aspects as part of the Interchange Agreement they must be listed in separate appendices.

3 The number of EDI messages included in Appendix 1

The parties often formulate a separate appendices for all message types that are exchanged, and they are often established bilaterally between the parties. This means that one appendix regulates one, and only one message type, e.g. an order between two parties. As the use of EDI becomes increasingly customary this will mean that the parties have to administrate a great deal of agreements with attached appendices. The following table illustrates this problem seen from one party's side:

The number of parties	The number of messages	The number of Interchange Agreements	The number of Appendix 1's
2	1	2	2
2	2	2	4
50	2	50	100
200	4	200	800

Ideally, it would therefore be desirable that the same contract document with appendices can be used for several messages between the parties. In this context one must also assess the need for a precise specification of operative and business-related aspects that are often typical of a message between two parties.

Appendix 1 to Norsk EDIPRO's Interchange Agreement is based on the assumption that the same document can regulate several message types. The appendix can also be used for one single EDI message.

In an operational perspective an EDI relationship will often encompass a couple of message types that are used to solve a given business function. Typically this would be a "request" and a "business receipt" to the former. Examples are:

Business function	*Message types*
Order processing	Order (ORDERS) and Order confirmation (ORDRSP)
Consignment note	Transport instruction (IFTMIN) and contract (IFTMCS)

4 Group agreement

The standard text of the Interchange Agreement and Appendix 1 are designed for two parties, it is possible, however, for several parties to adopt the same agreement through a so-called "Group agreement". In a Group agreement the second party is a group, identified by the name of an organization, for instance. Upon signing the agreement, the individual members are connected to each other in such a way that each individual in interaction with other members accepts that the provisions of this agreement and appendices are equally valid as if they had been approved bilaterally by the two parties.

5 Separate appendix for use of CONTRL?

In addition to a business acknowledgement of receiving an EDI message it may be relevant to use EDIFACT's standard control message - CONTRL to indicate that the message has reached the receiver and that it is correct according to the EDIFACT rules. **In Norsk EDIPRO's Interchange Agreement it is not required to formulate separate appendices for use of CONTRL.**

The items in Appendix 1

Several comments are given on how the various articles in Appendix 1 to Norsk EDIPRO's Interchange Agreement are supposed to be used.

1 Identification of Appendix 1

The front page of the Appendix is designed to identify the appendix and which parties have agreed to it.

A -...use of EDI messages for...

Here are listed the business documents or the business area covered by the appendix. Examples are:

- EDI messages for orders and order confirmations
- EDI messages for invoice (INVOIC) and remittance advice (REMADV)
- Transport instruction and contract

Example

...use of EDI messages for

A

Exchanging Order and Order Confirmation

B/C - The Parties

Here are listed the signatories (i.e. organizations) to the agreement.

If the Interchange Agreement is formulated as a "group agreement" the group shall be listed as party B, and reference should also be made to the appendix listing the members of the group.

It should be noted that since the appendix refers to an Interchange Agreement it will not be possible to establish Appendix 1 within a group and at the same time have bilateral Interchange Agreements. The reverse situation is possible, however.

Example:

B

EDI Company Ltd.
Party A
and

C

User group EDI (see Appendix 6)
Party B

D - Reference to IA

The relevant Interchange Agreement between the parties is identified here.

Example

The appendix is based on Interchange Agreement already concluded between the parties dated

D

1 January 1995

E - Attached sub-appendices

Appendix 1 to Norsk EDIPRO's Interchange Agreement is designed to cover the most usual aspects in an EDI relationship. Nevertheless, there may still be some parties and message types that have requirements which are not covered by the standard text. The standard text therefore identifies a set of sub-appendices where such aspects can be specified. In this blank one shall mark off the sub-appendices actually used. All sub-appendices shall be marked with a yes or no.

Example:

The following sub-appendix makes up an integrated part of the this document:

E

Sub-ppendix	Description	Part of the Agreement? Yes	No
1	Particular modifications, specifications and additions to aspects regulated in the Interchange Agreement		
2	Modifications, specifications and additions to Appendix 1		
3	Modifications, specifications and additions to the Implementation Guide		
4	Operating routines		

Reference is made to the provisions in article 2 of the Interchange Agreement in which the parties agree that Appendix 1 - Use of Various Message Types can be concluded for new types of EDI messages based on the Interchange Agreement without having to change the latter.

F - Signature

If the Interchange Agreement is part of a Group Agreement it shall be signed by a representative of the Group.

It should be noted that Norsk EDIPRO's Interchange Agreement is designed to be written out on paper and signed by the parties, but does not exclude the possibility of using EDI messages with their security procedures (digital signatures) for an electronic signing of the agreement.

Example:

Binding signature

F

	Party A	*Party B*
Date	**95.01.01**	**95.01.01**
Signature	**<sign>**	**<sign for the group>**
Title	**Man. Dir.**	**Head of Secretariat**

2 Identification of the parties

Norsk EDIPRO's Interchange Agreement requires that an identification number is given for the parties included in the agreement. This identification number must be regarded as the parties' EDI address for use in the UNB/UNG segments. Only one ID number can be given for each party. This will usually be sufficient for the majority of users. If it is necessary to list other or different ID numbers, this can be done in sub-appendix 1.

3 EDI messages and implementation guides

Here can be listed the Implementation Guides used for interpreting the EDI messages. If there are other rules for use of the messages (modifications, specifications or additions), these shall be listed in sub-appendix 3.

It should be noted that the appendix prescribes that "*In transmissions between the parties EDI messages shall be identified as listed in the above mentioned Implementation Guides.*" This refers to the values given in the UNH segment in the transmitted messages. One must therefore check that the Implementation Guide actually lists these values.

Example:

All EDI messages exchanged between the parties shall follow the message definition documented in the following Implementation Guides:

Message type	*Reference to Implementation Guide*
ORDERS	**NEP (Norsk EDIPRO) ORDERS, D.93A**
ORDRSP	**NEP (Norsk EDIPRO) ORDRSP, D.93A**

Times and frequency of EDI message transmissions

The precise point of time for transmitting messages can in some cases be crucial for the business relationship between the parties. Take for example the wholesale and retail trade, in which one often agrees that an order received by 9 am must be executed within the same day. Hence, it will often be necessary to agree when EDI messages are to be sent/collected from the transmission service. The business consequences shall be determined in a business agreement or in sub-appendix 2.

In an EDI relationship in which no direct communication has been established between the parties, i.e an intermediary network is used, each party will only control some parts of the total processing sequence:

- The sender processes the business document (e.g. the order) in his application
- The sender initiates a transmission to the network
- The network supplier processes the message and places it in the receiver's mailbox
- The receiver processes the business document (e.g. the order) in his application

Depending on how the processing has been organized by each party, the total processing sequence may be long or short. In order for the parties to be able to calculate the entire processing time, requirements for transmission (i.e. the exact hour that the sender transfers the messages from his EDI system) and collection (i.e. the exact hour that the receiver can pick up the messages from the transmission service) of exchanges to/from the network supplier (transmission service). This can be listed in various ways, for example:

- on a daily basis, i.e. daily sending/collecting without specifying the exact time
- every hour, i.e. the parties send/collect messages every hour
- at a given hour
- before a given hour
- etc.

It is worth noting that even though demands have been made on both parties, no demands are made on the processing time of the intermediary network. This must be covered by the parties' communication agreements with the network supplier.

Example:

Transmission of EDI messages between the parties shall occur at the following times:

	Party A	*Party B*
Sending to the transmission service (mailbox)	**No particular requirements**	**No particular requirements**
Collection from the transmission service (mailbox)	**Once an hour**	**Once an hour**

Processing of received EDI messages

In order to calculate the total processing time, demands must be made on the processing of the EDI messages at the receiving end, i.e. in the receiver's applications. Applications in this context are regarded as the parties' total EDI system, i.e. both the EDI functions and the administrative application (e.g. the order processing system). Such requirements can be indicated in several different ways, for example:

- on the same day, i.e. the message shall be processed the same day without specifying the exact time
- within an hour, i.e. the parties shall process messages within an hour after they have been placed in his mailbox
- as soon as possible
- within a business day
- etc.

It will often be natural to specify the processing time in relation to when the messages are actually received, for example:

- For messages received on normal workdays between 8 am and 2 pm: within two hours.
- For messages received at other times: by 10 am on the following workday.

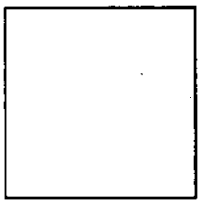
It is worth noting that Appendix 1 to Norsk EDIPRO's Interchange Agreement prescribes that "*An exchange with all its EDI messages is considered received at the moment that it is made available in the other party's transmission service (mailbox).*" This means that the receiver is responsible for collecting messages from the mailbox (transmission service) and to process them within the given time limits.

Example:
Received EDI messages shall by processed by the receiver within:

Message type	*Party A*	*Party B*
all message types	_ within two hours for messages received on regular workdays between 8am and 2pm _ by 10am the following workday for messages received at other hours	_ within two hours for messages received on regular workdays between 8am and 2pm _ by 10am the following workday for messages received at other hours

4 Acknowledgements and control messages

Use of the control message
The service message CONTRL can be used by the receiver of a transmission to send a receipt for, or rejection of, the entire exchange or parts of it. CONTRL is the only general mechanism in EDIFACT which can be used to produce receipts or report errors. CONTRL is primarily designed for reporting syntax errors, i.e. wrong use of ISO 9735 (the syntax rules). The CONTRL message, if used, will be generated by the receiver's EDI software.
In other words, CONTRL is used as a receipt between the parties' EDI software. It is also worth noting that in those cases in which one or both parties use a third party supplier for EDI conversion one risks that the CONTRL message does not return to the initial sender (cf. the figure below). In such cases the third party instead sends another agreed upon acknowledgement back to the party in question.



It is worth noting that Appendix 1 to Norsk EDIPRO's Interchange Agreement states that *"If no confirmation has been requested (data element 0031 - acknowledgement request in the* received UNB segment), the sender shall nevertheless be notified by a CONTRL message if errors have been found in the received interchange." In other words, it is assumed that the party's EDI systems are able to use CONTRL.
Moreover, the standard text prescribes that *"CONTRL messages* shall *follow the specification given in document TRADE/WP.4/R.1010 with corrections,* issued by

UN/ECE." This is the most complete and updated version of the CONTRL message. The document is available from Norsk EDIPRO.

The CONTRL message shall be used to:

1. acknowledge receipt of an exchange
2. acknowledge receipt of a message and if necessary report errors

In general we can distinguish between two kinds of acknowledgements:
A positive acknowledgement, i.e. confirming that everything is accepted and approved;
A negative acknowledgement, i.e. indicating that errors have been discovered or that the part which is to be acknowledged is rejected by the receiver.
The Norwegian Guide to Using EDIFACT recommends that positive acknowledgements are returned after most of the processing on the receiver side has been done. To acknowledge an order it would therefore be preferable to send an order confirmation, but if for instance there is a long processing time the parties can agree that a CONTRL message shall be returned immediately after receipt of the exchange.
In article 4, under Use of the Control Message, one can specify how CONTRL shall be used between the parties and also time limit requirements if necessary.
Alternative ways to describe the use of CONTRL:

1. To acknowledge receipt of an exchange
   _ yes, i.e. receipt of an exchange shall always be confirmed with CONTRL
   _ no, i.e. receipt of an exchange shall not be confirmed with CONTRL unless errors have been discovered
   _ only when this is requested in the UNB segment data element 0031 in the received exchange
2. To confirm correct messages
   _ yes, i.e. all messages shall be confirmed with CONTRL
   _ no, i.e. no messages shall be confirmed with CONTRL unless errors have been found in the message

For time-limit requirements in the use of CONTRL these can be listed in the same manner as in article 3, under Processing of Received Messages.
It must be emphasized that the time-limit requirements in article 4, under Use of the Control Message is included as part of the total time requirements given in article 3, under Processing of Received EDI Messages.
Example:
The service message CONTRL is used by the parties as follows:

	Party A	*Party B*
To acknowledge receipt of an exchange	**only when requested in the UNB segment data element 0031 in the received exchange**	**only when requested in the UNB segment data element 0031 in the received exchange**
Confirm that EDI messages have correct syntax	**no**	**no**

If acknowledgement is not requested (data element 0031 - request of acknowledgement in the received UNB segment), the sender shall still be notified by sending CONTRL if errors have been discovered in the received exchange.

Received exchanges and messages shall be processed and reported by the receiver within

Message type	*Party A*	*Party B*
All message types	**Within 1 hour**	**Within 1 hour**

Use of business receipts
By business receipt is meant an EDI message that it sent from one party to confirm the processing of the commercial contents in a received EDI message (e.g. order confirmation). Such business receipts are often necessary to ensure that the parties have an equal commercial understanding of the EDI message contents.

Example:

The commercial content of received EDI messages shall be acknowledged as follows:

Received message type	*Business receipt to be returned? (yes/no)*	*Message type*
ORDERS	**yes**	**ORDRSP**
ORDRSP	**no**	**not necessary**

The above shall then be understood as follows:
- a received ORDERS (order) shall always be confirmed by an ORDRSP (order confirmation)
- a received ORDRSP (order confirmation) shall not be confirmed

5 Use of EDIFACT syntax

Questions concerning use of the EDIFACT syntax shall be dealt with in the parties' EDI software.

Since the EDIFACT syntax contains several options, it is vital that the parties' EDI software is organized in such a way that the parties are actually capable of exchanging EDI messages. The specifications in *The Norwegian Guide to Using EDIFACT* are helpful in this respect. Exceptions are specified in sub-appendix 2.

6 Security

For some EDI messages it may be appropriate to specify particular security measures. The standard text of Appendix 1 identifies which security procedures that are used, while details concerning each procedure are given in sub-appendix 2.

In cases where the use of security procedures are subject to grading provisions one must ensure that sub-appendix 2 is stored and dealt with according to these provisions.

Example:
The following security procedures shall be used for EDI messages that are transmitted between the parties:

Message type	*Security mechanism used (yes/no)?*						
	Sequence number	Control count	Signed controlcount	Digital signature	Crypto-graphy	Use of TTP	Other
ORDERS	**yes**	**yes**	**no**	**no**	**no**	**no**	**no**
ORDRSP	**no**	**yes**	**no**	**no**	**no**	**no**	**no**
Algorithm for cryptography			**Not relevant**				
Algorithm for signature			**Not relevant**				

(TTP - Trusted Third Party)

Sub-appendix 2 may then have a text like the following:

The **sequence number** is generated as a sequential counter of all messages that are transmitted between the parties. The sequence number shall be stated as a unique message reference in the UNH segment, data element 0062.

The **control count** is calculated as a "nonsense sum" by adding up all the article numbers.

7 Storage

Norsk EDIPRO's Interchange Agreement states that messages normally shall be stored in 6 - six - months unless otherwise stipulated in Norwegian law or specifically agreed on in Appendix 1.

Example:
Exchanged EDI messages shall be stored by both parties. The following minimum storage time has been agreed on:

Message type	*Party A*	*Party B*
All message types	**According to Interchange Agreement**	**According to Interchange Agreement**

8 Operating routines and deviations

Operating routines that regulate transmissions and processing of EDI messages and procedures for deviations are assumed to be specified in sub-appendix 4.

9 The validity of the agreement

If the Interchange Agreement is terminated, there will be no reason for keeping Appendix 1. A termination of the Interchange Agreement will therefore automatically also mean a termination of all Appendix 1's based on the terminated IA.

In a termination of Appendix 1 the Agreement's requirements concerning storage of information (cf. article 7) will still be valid for both parties until the agreed storage time for the last exchange has expired.

10 Modification of the appendix

As mentioned earlier, the Norsk EDIPRO Interchange Agreement with appendices is supposed to be written out on paper and signed by the parties. Modifications of the appendix must also be done in writing and require a binding signature from both parties. All specifications, modifications and additions shall be listed in Appendix 2.

11 Sub-appendix 1 particular modifications, specifications and additions to aspects regulated in the Interchange Agreement that are unique for message types included in Appendix 1

This sub-appendix is included to specify possible deviations to the Interchange Agreement concluded between the parties, based on the use of certain message types. Examples of this kind of situation:

- separate addresses
- identification of party where this is done at department level for instance
- special circumstances concerning use of third party
- cost sharing
- exchange of test data
- the parties' obligations at the sending and receiving end, for instance control procedures before sending and verification upon receiving EDI messages.
- special requirements to log and storage that go beyond what has been decided in the Interchange Agreement
- special rules for economic losses, breach of contract and damages
- etc.

12 Sub-appendix 2 Modifications, specifications and additions to Appendix 1

The purpose of this annex is to specify deviations to the standard text in Appendix 1 which may include aspects based on the business relationship between the parties, or in those cases where the standard text does not cover all the elements that the parties wish to regulate. Examples of business aspects that need to be described are as follows:

- Consequences of discrepancy between data given in the message (e.g. the owner of the account stated in an NAD segment does not tally with the account number stated in an FII segment)
- specifications concerning the commercial understanding of data that are transmitted.
- specifications concerning the commercial consequences of the data that are transmitted (e.g. a sum that is made available in the receiver's account on the same day that it is drawn from the payer's account)
- use of the promise or contract principle when entering into the agreement
- etc.

Such aspects will be particularly relevant in those cases when the Interchange Agreement is formulated as a group agreement covering several message types.

13 Sub-appendix 3 - Modifications, specifications and additions to the Implementation Guides

This annex is included to specify anomalous use of an Implementation Guide, and will e.g. cover aspects based on the business relationship between the parties, for example:

- a specification of the segments, composite elements, data elements or codes that shall (shall not) be used between the parties
- details concerning how data elements are to be understood and interpreted
- specification of data field lengths
- requirements for what must be controlled by the receiver (e.g. control counts)
- use of control counts and consequences if there are anomalies
- etc.

14 Sub-appendix 4 - Operating routines

This annex is included to specify the operating routines that apply for transmission of messages between the parties, for example:

- survey of message flow which shows the parties or perhaps service suppliers and their technical infrastructure in the form of machines, software and net services. Critical points in the message flow should be described in particular detail.
- routines that are crucial to ensure that sending, receiving and processing of EDI messages function properly. This will not only include automatized routines, but also manual processing and control.
- etc.

In relation to the operating routines it is also necessary to specify what procedures shall be introduced if deviations to the described routines occur, i.e. in case one of the parties is not able to maintain normal operation. Examples of such procedures include:

- pre-defined routines for fault-finding in one's own systems and connections with a particular person in charge
- a description of the order in which the routines are to be performed
- specification of situations in which the service supplier shall be notified
- specification of situations which require that the other party is notified
- fault lists indicating who shall be contacted and which alternative routines shall be applied
- when are data to be retransmitted and how shall it be shown that this is a retransmission.
- etc.

It should here be noted that some operative messages such as orders often are critical in terms of time. For this type of message there will often be a need for clear guidelines to handle deviations, and these guidelines should be relatively simple to specify (e.g. by fax). For other message types, on the other hand, it may be more difficult to specify effective deviation routines. However, these messages are not so critical time-wise, e.g. invoice, and message transmission can often be postponed until normal operation has recommenced. It is therefore not so vital to specify deviation procedures for these messages.

平成9年3月発行
発行所　財団法人　日本情報処理開発協会
産業情報化推進センター

東京都港区芝公園3丁目5番8号
機械振興会館内
ＴＥＬ　(3432) 9386

印刷所　山　陽　株式会社
東京都千代田区神田神保町1-18
ＴＥＬ (3293) 5411