Close-Up

米国CBP「10+2ルール」(ISF)とフォワーダーの対応について

CBPへの対応―ISF・AMSの事前電子申告を支える第三者サービス

株式会社ブレインネッタ　代表取締役　野田 誠孫

はじめに

2009年1月26日、CBPによる暫定最終規則―ISF10+2の施行により米国の海上輸入貨物向けのテロ対策、つまり「貨物セキュリティの電子事前申告制度」は船社及びNVOCCを対象とするAMS（Automated Manifest System）から、輸入者及びその関係者を対象とするISF（Importer Security Filing）という次の段階に進んだ。ISF10+2の施行によりCBPはこれまでのAMS情報、即ち貨物輸送のデータ（物流）から貨物内容のデータ（商流）に対テロのセキュリティ対象を拡げることとなった。これによりCBPは輸出港での米国向け船舶への貨物の船積前にサプライチェーン上の関連情報を入手することでセキュリティ監視を一層強化したことを意味する。以下、新たな制度であるISFがどのように機能するのか、当事者である輸入者はこれにどう対応するかを説明する。また、そのために必要となる情報システムに求められる能力とは何であるのかを述べる。（脚注：この文中で使用する「フォワーダー」と「NVOCC」の定義[1]）

貨物セキュリティの基本―土台はAMS（物流）、これを強化するISF（商流）

CBPでは2003年1月に施行したAMSで貨物セキュリティ対策として最も有効な手段である“DO NOT LOAD”（DNL）の指示を船社（輸送事業者）に対して出すことができる。つまり、AMSで規定された輸送事業者に対して電子データで事前申告した内容に基づき必要に応じてCBPは輸出港にいる船舶に対し船積24時間前にDNL指示ができる。このCBPによるDNL指示は新たなISF制度でも同じ意味を持つ。即ち、CBPは「不審な貨物は船積しない、させない」をISFが原因の場合でも適用する。海上貨物によるテロと言う物理的危険を排除できるのは「貨物を持ち込まない」ことであり、米国はこれが最大の防御であるとしている。つまり、船舶に物理的に「積まない、積ませない」ことをどのように徹底できるかが米国のテロ対策の基本である。この場合、物流を管理するAMSこそが基本となり、今回の商流を対象とするISFがAMSをさらに強化し、商流に関わる情報提供を通じてCBPはサプライチェーン全体に監視の対象を拡大した。つまり、CBPはISFとAMSの連携を通じて「物流＋商流」を一体化して、より安全な貨物セキュリティ体制の構築を目指している。

ISF10+2ルール施行―暫定期間の対応と正式施行に向けた準備

2009年1月26日施行のISFは「暫定最終規則 Interim Final Rule」として6月1日までをパブリックコメント（注：対象を6項目[2]に限定）の受付期限としている。また、2010年1月26日までの猶予期間はDNLを含む罰則は原則適用しないとされ、実際の運用での問題点に配慮しながら柔軟な対応Flexible Enforcementを行う旨を明記している。今回のISF施行に先立ち、数多くの組織団体から様々な意見が表明された。このためCBPは強制的な施行を急がずに現実的な対応に時間を掛けていることが指摘できる。他方、柔軟な対応と言いながらも注意を要することもある。つまり、CBPの公式文書では猶予期間であっても輸入者には相応の努力（a good faith effort to comply with the rule）をすることが求められ、その間何もしなくて良い訳ではな

1 フォワーダー(Forwarder) ーここでは国際物流事業に従事する広義の意味で使用する。即ち、英文の定義としては次の通りである。A freight forwarder (often just forwarder) is a third party logistics provider. As a third party (or non asset based) provider a forwarder dispatches shipments via asset-based carriers and books or otherwise arranges space for those shipments. Carrier types include waterborne vessels, airplanes, trucks or railroads. (Wikipediaより)
NVOCCーNon Vessel Operating Common Carrier。利用運送事業者。自らは船舶を所有していないが、荷主に対しては運送業者として貨物を引き受け、実際には船会社を利用して海上輸送を行う者。この事業を行うには国土交通大臣への登録又は許可が必要となる。

2 パブリックコメント対象項目ーManufacturer (Supplier) name/address, Ship to Party, Country of Origin and Commodity HTSUS number, Container Stuffing Location and Consolidator (Stuffer) name/address

Close-Up

い。そして、CBPが必要と認める場合には執行（to take enforcement action）[3]もあり得るとしている。これらの点を考えると、当事者である米国の輸入者は準備を怠ることなく対応をする必要がある。同時に輸出側の日本でも米国の輸入者側の動きに足並みを揃えながら必要な協力や業務引き受けなどの対応が求められよう。

10+2の内容―ISF-10とISF-5で輸出国のフォワーダーの関与が不可欠

10+2とは―実は10+5+2

ISF規則は3つの要素、10-Regular、5-Transit、2-Carrierで構成される。基本となるのは「ISF-10 Regular（図-1）」であり、ここでは10項目に関する問題を中心に説明する。その前に「ISF-5 Transit」について簡単に述べる。Transitとは米国内で消費されず第三国を最終仕向地とする貨物が対象とされる。船舶が米国に一時寄港、或いは貨物が積み替えや陸上回送等で異なる第三国向け輸送媒体に渡される場合、輸送事業者（Carrier & NVOCC）に事前申告の義務を課している。当該5項目[4]はISFと言いながらも、その内容は輸送情報が基本となる。何れにしても、ISFデータとしてCBPで処理される。また、2-Carrierとは船社の船積計画書（Vessel Stow Plan）とコンテナ使用状況（Container Status Message）をCBPが求めるもので、ここでは言及しない。

DNLとの関連で必要な注意点

10-RegularではAMSとの連動を含めて、留意すべき問題を幾つか指摘できる。CBPではISF処理のためAMSとABIという電子申告システムを使用するが、テロ対策としての「貨物セキュリティ」の基本となる鍵はDNLを管理するAMSシステムである。CBPが管理する3つのシステム、AMS、ISFとABIの相互関係を図-2に示す。ここではISFデータとして事実上11番目の項目と言われる「B／L番号」でのISF-AMSの連動が最大のポイントである。CBPの貨物セキュリティの原則は「不審な貨物は船積しない、させない」ことであり、それを実現するのはAMSシステムである。従って、問題の原因が仮にISFにあるとしても、AMS、即ち「輸送」という物理的手段に対し強制力を持つDNL指示を出すことが貨物セキュリティの基本である。そのためにフォワーダー（NVOCC機能を含む）に必要なのは、何らかの形でAMSを「自分の管理下に置く」ことである。つまり、AMSを通じてDNLを含めISFで何が起きているか、その見える化が業務のポイントとなる。これこそが顧客サービスを基本とするISF対応の必須条件であると思われる。なお、船社によってはNVOCC事業者がAMSを紙媒体で委託した場合、ドキュメント（ハードコピー）に記載されたNVOCCのHouse B／L No.（ISFの照合に必須項目としてCBPが定義）を使用せずに船社での処理には自社Filing No.を使用することがあると言われる。仮に船社が業務上の都合から便宜的に自社Filing No.を使用した場合、CBPが規定したAMSとISFが連動しない可能性があり、ISFとの関連で注意が必要と思われる。何れにしても、物流と商流を結ぶのはCBP規則が明記するLowest House B／L No.であることを認識する必要がある。

電子申告制度への取り組み

今回のISFでは最終責任者は輸入者である。同時に多くの関係者が輸出側でも関与することになる。従って、フォワーダーは輸入者や輸入者と取引のある輸出者、製造者等から状況に応じて何らかの要請や相談等を受ける可能性がある。こうした輸出・輸入の両側で多くの関係者が携わる状況はフォワーダーやNVOCCに電子申告制度という新しい要素を持ち込む可能性がある。例えば、NVOCCはAMSの対応ではこれまで船社へのドキュメント（ハードコピー）による委託としてきたが、ISF施行を機会にこの手順を見直す等である。何故なら、以下に述べるようにISFがAMSと密接に関係するからである。欧米系大手フォワーダーではISF制度の導入を前向きに捉えて、これを顧客サービスでのビジネス機会と考えて積極的に活動しているとも言われる。

第三者サービス―ISFに必要な情報処理には有効な手段

電子申告を自ら行うことの意味

ここまではISFがもたらした現行制度への影響や必要な取り組みを述べたが、輸入者を含めて難しく見えるISFへの対応も工夫次第では容易になる。第三者サービス（CBP

3 CBP reserves the right to take enforcement action, including the use of the DNL option, in order to mitigate potential security and safety risks.

4 ISF-5　1. Booking Party Name/Address, 2. Ship to name/address, 3. Commodity HTS-6. 4. Foreign Port of Unlading, 5. Place of Delivery

Close-Up

の規定―Data Processing Service Provider）の有効活用である。図-3／-4を参照願いたい。この二つ図（第三者サービスが提供するポータル機能）の中にそうした対策の答があるように思う。つまり、フォワーダーとして貨物セキュリティ対策を世界的流れとして認識して、自らはその業務対応に電子化、情報システムを積極的に活用をする。即ち、CBPの新たな制度では紙媒体を認めないが、この機会に従来からの社内業務を見直して電子化の契機とする。また、これは同時にAMS24時間ルール施行が予定される中国やEUなどのへの準備になるかも知れない。

米国CBP―第三者サービスの有効性を認識

AMSではCBPは輸送事業者に船積24時間前の電子データ提出を求める。電子データによりCBPと直接EDI（電子データ交換[5]）を行うのは長い実績のある大手船社を除くと多くはない。第三者サービス（CBPの正式名SEA AMS DATA PROCESSING SERVICES）が電子データの入力業務『Messaging』を当事者（AMS―輸送事業者、ISF―輸入事業者）に替って行うことは既に一般的であり、他方CBP自体は安全対策や徴税等の本来的な処理業務『Processing』を基本にする。特にテロ対策では関係諸機関（CIA, DoD, FBI, FEMA,USCG etc.）との緊密な連携が不可欠でMessagingの周辺業務を外部サービスが代替することでCBPは『Processing』に集中できる。こうした制度は世界の他地域、例えば豪州（実施中）やEU（計画中）でも同じと思われる。CBPはISFでもこれまでのAMSやABIと基本的に同じこうした仕組みを認めている。

ISFの特徴を最新の情報システム、ポータル機能で克服

それではISFが第三者サービスとして輸入者（含む代理人）に対してどのような支援機能を提供するかを説明する。ISFはAMSと異なり、①当事者以外にも関係者が多数いること、②輸出国、輸入国の間での緊密な連携が地域的広がりの中で必要であること、③業務処理に関わる時間、リードタイム、がAMSに比べて長いこと、④電子データ以外の媒体は認めずISFの対応には情報システムが不可欠なこと、と言った課題が挙げられる。これら問題への対応には輸出事業に従事する企業でも大企業では対応は容易に可能と思われるが、中小企業では自ら時間や場所の異なる輸入者と連携、解決するには課題は多い。一方、第三者サービスを利用することでこれらを解決することができる。前提となるのは最新の情報技術、即ち、インターネット基盤の最大活用である。

第三者サービス―「PC+Web」でISFなどの貨物セキュリティ対応が容易

現在、ほとんどの企業では事業規模を問わずパソコンが一人一台の時代である。事務所で仕事をする誰もが「パソコン+インターネット」により世界、つまりCBPとも自分の机の上で結びついている。こうした業務環境は実は十年前はまったく想定できなかった。これが第三者サービス、特にSaaS[6]を有効活用できる基盤になる。この情報システムの基盤を使うことでISF対応は誰もが関わることができる。数多くの関係者、地域的拡がり、時間の違い等、ISFの業務対応には一見難しい要素があるが、これらにポータル機能（個々の逐次情報を全体として取り纏め、管理する機能）を活用することで克服できる。また、仮にCBPが規則変更等をした場合でもSaaSの場合は容易に対応することができる。こうして第三者サービスの活用により貨物セキュリティ問題への有効な対策とすることができる。

おわりに

今回の「10+2」の説明機会を通じて、フォワーダー

5 EDI Electronic Data Interchange（電子データ交換）の略で「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」

6 SaaS- Software as a Serviceの略。ソフトウェアの機能のうち、ユーザが必要とするものだけをサービスとして配布し利用できるようにしたソフトウェアの配布形態。サービス型ソフトウェアとも呼ばれる。ユーザは必要な機能のみを必要なときに利用でき、利用する機能に応じた料金を支払う。サーバ上で動作するソフトウェアの機能をネットワークを介してオンラインで利用する形態が多くなっている。

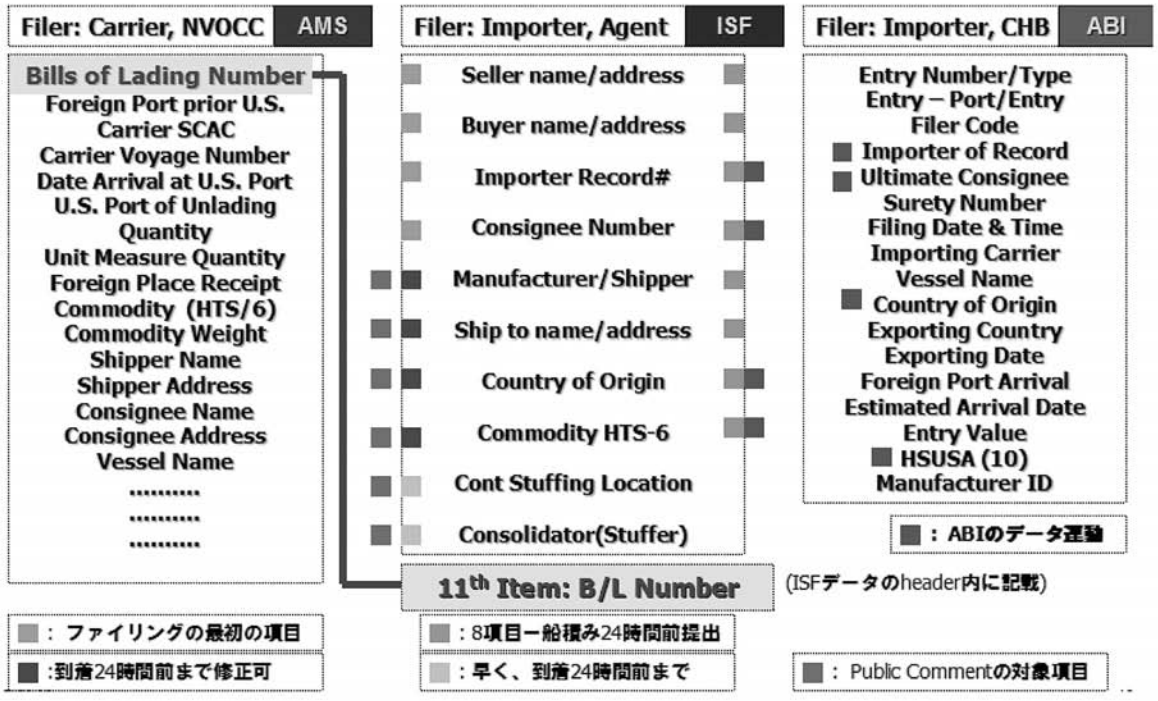
Close-Up

やNVOCC事業に従事するJIFFA会員の多くの方が米国が進める貨物セキュリティ対策に強い関心を持つことを改めて知ることとなった。ISF10＋2ではCBPの考えるテロ対策が物流から商流に範囲を拡げたこととなったが、これによりCBPは米国との貿易に携わる関係者の情報を巨大なデータベースを構築する過程にあるとも言われている。同時にAMSとISFの二つの制度は「車の両輪」として日常的な安全対策を行い、危険を持ち込む可能性のある海上貨物を徹底的に排除すると理解すべきかも知れない。何れにしても、海上貨物輸送のセキュリティ対策におけるキーワードは「輸出港、電子データ、船積24時間前、事前申告、通関手続」である。それを基本として制度的枠組みを構築することで米国はテロ対策の最大の防御壁となる有効な手段を持つのである。

（図-1）ISF-10 項目

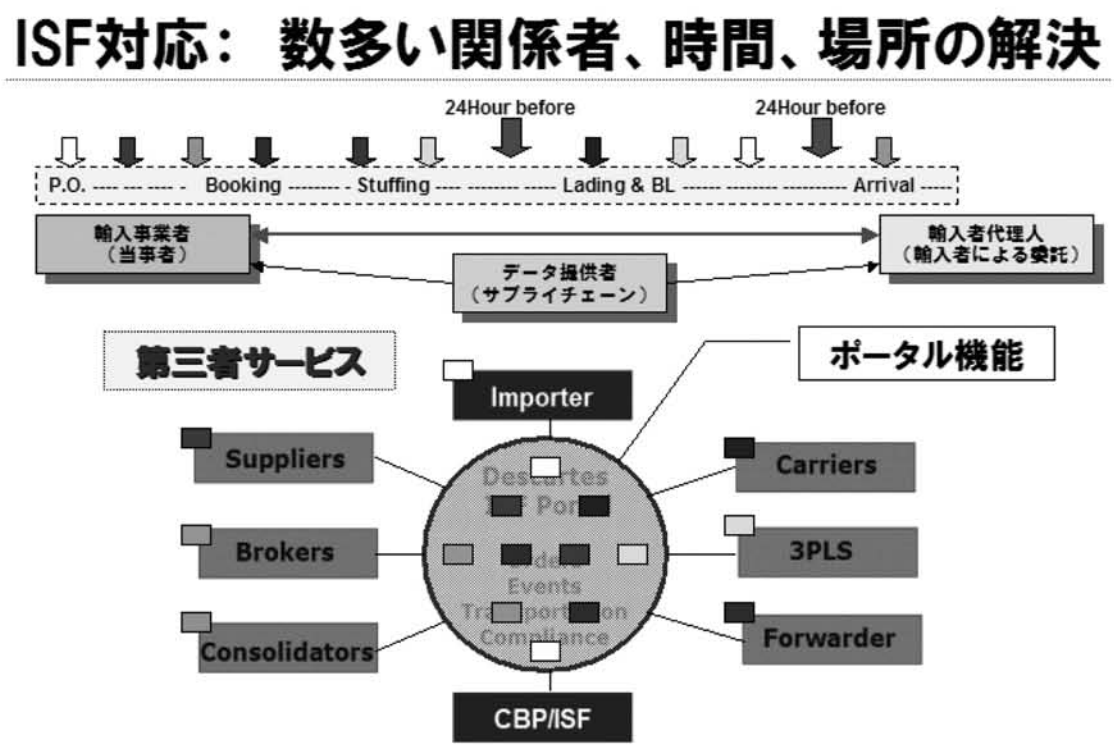
データ項目	主な内容	情報源
販売者の名前/住所 Seller Name/Address	当該商品を売却した、又は売却することを合意した者。売却が完了していない場合は所有者	輸入側
買主の名前/住所 Buyer Name/Address	当該商品を購入する、又は購入することを合意した者	輸入側
輸入業者登録番号 Importer of record number	当該事業者の関税の支払い及びすべての輸入手続に必要な納税者番号、雇用者番号、社会保障番号、又はCBP指定の番号	輸入側
荷受人番号 Consignee number	当該事業者の関税の支払い及びすべての輸入手続に必要な納税者番号、雇用者番号、社会保障番号、又はCBP指定の番号	輸入側
製造者/出荷者の名前/住所 Manufacturer name/address	当該貨物を製造、組立て、生産、或いは成育した最終的な当事者	輸出側
送り先の名前/住所 Ship To name/address	通関後の貨物リリースについて、当該商品の物理的な引渡しを受ける者	輸入側
原産国 Country of origin code	輸入関連法令及びその他規則に基づく製造者、生産又は成育をした国を明らかにするもの	輸入側
貨物の6桁の関税率表の番号 Commodity HTS number	6桁の番号が必要。但し、場合によっては8又は10桁での報告も可	輸入側
コンテナ詰めした場所 Container stuffing location	当該貨物が物理的に詰込まれた場所の名前と住所、又は混載貨物の場合は出荷準備が完了した場所の名前と住所	輸出側
コンテナ詰めした者の名前住所 Consolidator name/address	コンテナに貨物を詰込んだ者、又はその手配をした者。混載貨物の場合はその出荷手配をした者	輸出側

（図-2）CBP－３つのシステムの相互関係



Close-Up

（図-3）



（図-4）