「サプライチェーン・セキュリティ規格の国際動向　ＩＳＯとＷＣＯ」セミナー

議題と講師紹介（司会は、日本機械輸出組合部会・貿易業務グループリーダー　橋本弘二）

第一議題は、「ISO/TC8 でのセキュリティ規格提案の経緯等について」。ＴＣというのは Technical Committee の略。ＩＳＯのセキュリティ規格が定められる基本的なプロセスについてご説明いただく。講師は、財団法人日本船舶技術研究協会基準・規格グループ（ＩＳＯ／ＴＣ８船舶及び海洋技術セクレタリー）の小郷一郎氏。

第二議題は、「ISO/ＰＡＳ２８０００シリーズとサプライチェーン・セキュリティマネジメントについて」。ＰＡＳというのは、Publicly Available Specification の略、日本語訳では公開仕様書となる。講師は、独立行政法人海上安全研究所運航・システム部門上席研究員の太田進氏。

第三議題は、「ISO/ＰＡＳ２８００１の概要」。講師は、東京海洋大学海洋工学流通情報工学教授の渡邉豊氏。

この３つの議題のあと、事務局から、ＷＣＯ（World Customs Organization、世界税関機構）の「民間協議グループ」会合についてご報告したい。現在、ＷＣＯでは、サプライチェーンセキュリティの国際的な標準ルールつくりのための検討を行っているが、その一環として、民間企業・団体を集め、ＷＣＯと民間との協議グループを設置した。そして、第１回会合を３月３０日から３１日に開催した。日本機械輸出組合ではその会合に参加し、私が出席したので、その模様をご報告する。

第Ｉ議題
「ISO/TC8 でのセキュリティ規格提案の経緯等について」
小郷　一郎氏　財団法人　日本船舶技術研究協会
基準・規格グループ（ＩＳＯ／ＴＣ８船舶及び海洋技術セクレタリー）
（資料Ｎｏ．０～２）

まず、私の職場、財団法人日本船舶技術研究協会について、ご紹介させていただきたい。財団法人日本船舶技術研究協会は、２００５年４月に旧来の３つの団体が合併して作られ、ＩＭＯ，ＩＳＯ等の国際基準策定に係る調査研究、船舶技術に関する研究開発を行う団体である。

ＩＭＯ（International Maritime Organization：国際海事機関）とは、国連の下部組織であり、各国政府の海事産業全体に関わる技術的事項に関連するルールづくりを主目的とする機関である。本会の仕事は、このＩＭＯに対する日本の対応の作成、これが一つ。また、船は総合産業といわれるようにＩＳＯ／ＩＥＣ等の多くのテクニカルコミッティに係っている。 この中で、ＩＳＯ／ＴＣ8（船舶及び海洋技術関係については、一番大きい組織)、ＴＣ１８８（スモールクラフト)，ＩＥＣ／ＴＣ１８（船用電気設備）等の日本の受

け皿として、日本船舶技術研究協会を通じて、関係テーマの調査研究、日本回答の作成、あるいは専門家の派遣といった仕事を行っている。このように、国際基準作成機関であるＩMO及びＩＳＯ等の両方を受け持っているのが、日本船舶技術研究協会である。

私の本日の目的は、あとに続く専門講師の方々のご講演の理解を深められるように、イントロとして、これまでのＴＣ８でのセキュリティの国際規格の経緯について、簡単に報告することである。今回のセミナーにご出席の方々は貿易実務のエクスパートの方ばかりと聞いておりますので、国際規格に関する知識は大体ご理解しておられるという前提で、講演テーマに関係の深い事柄を中心に、ＴＣ８でのセキュリティ関係国際規格の審議経過に焦点をあて、ご説明したい。

ご存知のとおり、国際規格というものの国際的な背景は、最近とみに、広がりを見せている。特に、船舶については、強制規則を作るＩMOと、任意規格をつくるＩＳＯ／ＩＥＣとが、密接に協力している現実があることを念頭においていただきたい。

ＩＳＯ／ＴＣ８（船舶及び海洋技術）の基本的な活動指針のひとつとして、ＩMOと海運造船業界との間をとりもつ’リンク機構’として機能するという戦略的な位置づけがなされている。任意規格であるＩＳＯ規格等は、ＩMOで策定する条約等の附属コードの脚注等に、引用されることが多くなってきている。 引用のされ方は、例えば、附属コードの脚注に、該当国際規格番号がそのまま引用されるという形である。このように、任意規格が強制規則をサポートする形で利用されはじめるようになった結果、強制規則と任意規格とが一体となって、安全、環境、保安対策等重要分野に貢献する形になりつつある。

今回、セキュリティ関係国際規格が審議されているＩＳＯ／ＩＥＣ等国際標準化機関の現在の参加国数は、ＩＳＯが１４６カ国、ＩＥＣがその半分以下の５２カ国である。参加資格のところにあるＰとＯは、のちほど詳しく説明するが、規格をつくる場での、Participation（参加）のＰ、Observer のＯの略である。

上記国際標準化機関と日本との関係については、日本は平成１７年度の実績で、ＩＳＯに１億４０００万円、ＩＥＣには８０００万円を拠出している。日本はお金をこれだけ出しているが、専門委員会の議長への就任とか幹事（セクレタリー）への就任といった人的な貢献の面では、ヨーロッパ、アメリカに対してかなり差をつけられているのが現状である。 それでも、ＩＳＯ会長職は現在、日本化学協会の田中正躬氏、ＩＥＣでは東芝技術顧問の高柳誠一氏が務めている。また、資料には書かれていないが、国連機関のＩＴＵ（International Telecommunication Union：国際電気通信連合）では日本人が事務総長である。このように、国際標準化機関の場で日本人が３機関ともトップとして活躍している状況にある。

制定規格数は、ＩＳＯは約１５０００規格、ＩＥＣは４４００規格。更に、船舶部門だ

けに限ると、ＩＳＯは約２１０規格、ＩＥＣは約９０規格程度である。
先程のＰメンバーとＯメンバーであるが、特にＰメンバーは、国際規格の審議ステップであるＮＷＩ（新規提案項目）－ＷＤ（作業原案）－ＣＤ〈委員会原案〉－ＤＩＳ（国際規格案）－ＦＤＩＳ（最終規格原案）の各ステップにおいて、Ｐメンバーの過半数以上の賛成とか３分の２以上の賛成という承認条件に基づいて国際規格発行に向けてステップアップしていくルールがＩＳＯ／ＩＥＣ専用業務指針で定められており、Ｐメンバーになることは各ステップにおいて投票権が発生することを意味するので、重要である。ＩＳＯでは、仮に政府からの圧力やどこかの国の強力な要請などが審議ステップであったとしても、最終的には投票で決めている。ＩＳＯが技術の民主主義でできているといわれる所以であり、ＩＭＯや各国政府の策定する強制規則類とはその策定手順が大きく違うのはこの辺にある。

上述のように国際規格は一度にできるわけではなく、段階１（ＮＷＩＰ）：新業務項目提案、段階２（ＷＤ）：専門家によるコンセンサスの形成、段階３（ＣＤ）：国代表団体からの意見の反映、段階４（ＤＩＳ）：国代表団体からの意見の取り上げ、最終原案（ＦＤＩＳ）の作成と段階を踏んで国際規格ができていく。以上が、ＩＳＯの概要である。

次に、本論に入り、ＩＳＯでセキュリティ関係国際規格が審議されてきたいきさつについてお話する。
米国では、２００１年９月にニューヨーク同時多発テロ事件があり、この事件を契機に、貨物輸送の安全性確保に関心が高まった。このテロ事件は、その後、ヨーロッパでも、例えば、ロンドンやマドリッドでの列車爆破事件等が起こり、最近では、アジアではジャカルタでもテロ事件が起きている。テロ対策については、総理大臣が出席しているＧ８でも国際問題の大きなテーマとして共同で対処していこうという合意が形成されている。
また、アメリカでは、事件後幾つかの省庁を統合して国土安全保障省という新たな省を設置して、ホームランドセキュリティという方針の下で、テロ対策に全力で対応している。

こういった背景をもとに２００１年同時多発テロ後、米国は同年開かれたＩＭＯ総会において、ＳＳＴ計画（Smart and Secure Trade Lanes）を提示した。ＳＳＴ計画とは、国防総省の肝入りでできた団体であるＳＣＳＴ(Strategic Council for Security Technology：米国保安技術戦略会議)が、今後技術的な側面からテロ対策を行うために、安全かつ迅速確実なトレードレーン（輸送路）を確保するためのプロジェクトを計画し、アメリカ政府と産業界の協力により主としてコンテナに係るサプライチェーンの保安の脆弱性を現状分析した上で評価、改善提案し、それを国際規格に反映していこうというものである。ＳＳＴ計画の中身は、貨物データの管理方法、識別方法、貨物の自動追跡、荷送り人の情報管理等を実際に船を動かして現状分析、評価・解析し、必要であれば国際規格として開発していこうというものである。ＩＭＯ総会ではこれが認められたというか、任意の動きではあ

るが、そういったことをやるということを承認した旨議事録に記載されている。

ＩＳＯでは、このＳＳＴ計画に基づいて、実船上での実証をとおしてその結果を国際規格に反映させるという動きが、フェーズの１、２、３という形で行われてきた。ＩＳＯにおいて、関係ＴＣであらゆるテロ対策に関係する国際規格の開発が進められるきっかけとなったと言える。

実証実験については、フェーズ１では、４つの大陸から６５を越す参加者、１２の港湾、３５のトレードレーン、１４の荷送り人で約１０００個のコンテナをサプライチェーンを通して監視するという実証実験を行った。フェーズ２は２００３年から行われ、２４時間の集荷情報の処理、使用技術の向上、検査システムの向上、電子シールの活用についてバリデーションが行われている。フェーズ３もすでに行われ始めていると思う。

残念ながら、こういった実証実験に関する詳細な情報はＩＳＯのメンバーにはクローズドにされており、ＴＣ８の幹事をやっている私にも良く分らない。ただ、海事産業界には参加を呼びかけ、そして、参加企業にはこの結果をオープンにしている。

次に、ＴＣ８で開発中の保安国際規格関係であるが、当初物流効率化を目的としてＸＭＬ言語で統一した貨物の情報データ管理を行う予定を立てていたが、テロ関係の情報の交換をスムーズに行いたいということで、急遽、海事複合輸送及び保安のためのデータ伝送という形に変えて２００２年に公開仕様書として制定した。これが、ＰＡＳ１６９１７で、最初のＰＡＳ（Publicly Available Specification：公開仕様書）となった。

次に、２００３年の6月、ＰＡＳ２０８５８（海事港湾保安評価と保安計画の作成）を制定した。このＰＡＳ２０８５８は、ＩＭＯのＳＯＬＡＳ条約（海上における人命の安全のための国際条約）の１１章の２に付属書として追加されたＩＳＰＳコード（The International Ship and Port Facility Security Code：船舶及び港湾施設保安のための国際コード）をサポートするもので、２００４年7月1日、ＩＳＰＳコードが発行されると同時に発行した。このようにＩＭＯのＳＯＬＡＳ条約と連携して、ＴＣ８でセキュリティの規格（公開仕様書）が作られている。

ここで、ＰＡＳについて、少し説明したい。ＰＡＳは、一般にＩＳＯ規格として発行する前、ワーキンググループでコンセンサスに到達した段階（委員会原案：ＣＤと同じ）で各国投票にかけたあと承認されれば、ＰＡＳ（公開仕様書）として発行するものであり、国際規格ではない。　ＰＡＳとして制定する目的は、未だ委員会での審議途中の規格案をクローズドである委員会メンバー以外の広い関係分野の方に一般公開し、見てもらって意見をもらう、あるいは、試用してみて問題がないかどうかを検証し、その後、ＩＳＯ規格のステップに戻して国際規格としてブラッシュアップしていこうとする考え方から生まれた。ＰＡＳ発行後３年以内には見直しを行い、更に３年継続するか、もう止めるか、あるいはＩＳＯにブラッシュアップするか、を決定することが義務付けられている。見直しをして更に３年継続するとしてもその間は６年なので、ＰＡＳは、長くて６年という短命な規

格ということになる。
　通常の手順では国際規格が出来上がるまでには３年以上かかるところを、社会的ニーズの強いもの、緊急性を要するものをこのような形で早い段階で公開することにより、関係者のニーズに即応することができることも特徴の一つといえる。

　２００４年１０月、ＩＳＯ／ＴＣ８の大連会議で、アメリカから、セキュリティ関係ＰＡＳ２８０００及び２８００１の新規提案が行われた。当初は、ＤＮＶ（Det Norske Veritas）という 船級協会が提案した案が基になっていたが、翌２００５年1月、ＴＣ８幹事から、ＩＳＯの書式に則り、新規標準化項目提案として投票に付され、その結果、両項目とも棄権が二つあったが、反対なしで承認された。この時、承認された項目が、ＰＡＳ／ＣＤ２８０００－サプライチェーンのためのセキュリティマネジメントシステムの仕様書及びＰＡＳ／ＣＤ２８００１－サプライチェーンのためのセキュリティの監督のための最適実施法の二つである。その後各WGで審議に付され、ＰＡＳ発行のための投票は、２８０００が同年（２００５年）の１１月、賛成１１、反対４という結果で承認され、１１月１５日に発行した。この規格は、後刻講師から内容説明があるが、セキュリティ管理をマネジメントの一環として実施するための規格である。
　マネジメント規格となると、そのためのガイドラインや監査するための規格も必要となる。２８００３と２８００４は２８０００の姉妹規格とされ、２８００３は認証及び監査機関の要件を規定し、２８００４は２８０００実施のためのガイドラインである。
　セキュリティ管理の最適実施法を規定している２８００１は、本年３月に最終的な審議を終了した。この６月に承認されると８月頃には発行になると予想されている。
　ＩMOとの関係では、こういった一連のＩＳＯ／ＴＣ８で開発したセキュリティ規格を５月開催のＩMO／ＭＳＣ（海上安全委員会）に提出し、説明する予定である。
　ＩＳＯの他の技術委員会（ＴＣ）の動向については、現在、セキュリティ関連としてテロ対策の一環として各分野で手分けして対応しているのが実情である。例えば、ＴＣ３４では食品関係のセキュリティチェーンの安全性確保を目的とした２２０００シリーズ（マネジメント規格）があるし、ＩＳＯとＩＥＣの合同委員会のなかのＪＴＣ１／ＳＣ２７では情報セキュリティ技術を審議しＩＳＯ２７００１として制定した。これ以外の委員会でも、乗組員の個別の識別方法、ＴＣ１０４では、コンテナの電子シールの開発などが審議中であり、当初道路交通を基本に行っていたＴＣ２０４では、現在では航空機とトラックのデータの互換性などを中心にした情報交換、メッセージフォアマットの統一等の検討が行われている。
　ＴＣ８で開発中の一連のセキュリティ関係国際規格は、日本船舶技術研究会のなかに、ＴＣ８セキュリティ分科委員会を設置して、関係業界からの参加者、専門家により対応している。 本分科会長には、日本貨物検数協会の佐藤守信氏を委員長とし、委員及び関係官庁も含め１５名ほどである。

以上　イントロとしての説明を終わらせていただく。ご清聴感謝いたします。

第 2 議題
「ISO/PAS28000 シリーズとサプライチェーン・セキュリティ・マネージメント」
太田　進氏　独立行政法人　海上技術安全研究所
　　運航・システム部門　上席研究員
（資料Ｎｏ．3～4）

今、小郷氏からフェアで偏見の無い素晴らしい説明があったが、私の方は一人の研究者として、自分の偏見も含めた判断で説明をさせていただきたいと思う。小郷氏とは若干説明内容が異なるかもしれないが、ご了承いただきたい。

スライドの写真は、リンバークというフランス籍のタンカーに爆弾を積んだボートが突入したときのものである。最近は、船舶の分野でもテロ対策は無視できない状況にある。本日の講演内容は小郷氏の講演と一部重複するが、まず背景から始まり、28000 シリーズの各規格の位置づけ、内容を説明した上で、最後に国際条項について一言述べたい。

まず、背景について。IMO では、1980 年代から海賊などの不法行為に対する総会決議といったものを作ってきた。お手許の資料にあるように、1988 年に出来たもので、いわゆる不法行為防止条約：SUA 条約と言っているものである。この条約は、ほとんど誰も批准せず、まったく使われていない条約の一つである。IMO では、このように昔から、不法行為に対して検討していたが、同時多発テロ以降、急遽アメリカが、「不法行為防止条約などという役にたたない条約では仕方がない、160 カ国が批准している SOLAS 条約（国際海上人命安全条約）でちゃんとやろうではないか」と主張したことによって、IMO はテロ事件から 1 年そこそこで条約を改正した。そして、先ほどの ISPS コードができたのである。

ISPS コードは、SOLAS 条約の手順にしたがい、2004 年 7 月 1 日に発行した。この ISPS コードで要求されているのは、まず保安責任者を決定し、次に保安の評価をすることである。保安評価については、ISPS コードでは、セキュリティアセスメントと言っているが、一般には、Vulnerability Assessment と言った方が馴染み深く、いわゆる、脆弱性評価である。この脆弱性評価をやった上でセキュリティプランを立てなさい、そして実施しなさい、更には、もう一度評価をやって、セキュリティプランをブラッシュアップしなさい、これが ISPS コードの基本である。一部には、シップセキュリティアラート（保安警報装置）等の装置に関する要件があるものの、基本はこのようになっている。

この ISPS コードは、SOLAS 条約という既存の枠組みを利用したがために、適用対象外がたくさんある。例えば、適用対象船舶は、国際航海に従事する総トン数 500 トン以上の貨物船、客船（トン数関係なし）で、内航船や漁船は適用対象外としている。また、ポートファシリティと言っているのは船舶とのインターフェイス部分だけであり内陸には一切

かからない、それも SOLAS 条約対象船が出入りする施設だけである。こうなると、適用対象外の船が沢山あり、その上、港湾施設も適用対象外があって、更には港では水際にしか規則が適用されない。それでは困るということで、ISO では、アメリカ主導で、20858（海事港湾施設の保安評価と保安計画の策定、講師訳）という ISO/PAS をつくった。この 20858 の目的は、アメリカに武器が入ってくるのを防止することにある。

ただ、このように港に関するセキュリティ要件を作ってみたもののこの 20858 はほとんど使われていない。ご承知の方は多いと思うが、実際に大量破壊兵器や兵器の密輸防止は、水際でいくらやっても駄目なのである。コンテナは 8 割くらいが内陸で詰められて港にやってくる。港湾地域でコンテナを詰めるというのは 2 割くらいしかない。このため、保安対策は物流全体で実施する必要がある。そこでアメリカは、水際だけではなくより広い適用範囲の規格が必要だ、更には運送事業者のみならず、メーカーも含めて物流に関与するすべての人に適用する規格を作らなければならない、と主張した。こうして、サプライチェーン・セキュリティ規格が提案された。

20858 をつくるときに、12 月、1 月、3 月と 3 回の会議を行った。この 3 回の会議であっという間に決まってしまった。通常、コミッティ・ドラフトをつくるまでには半年に 1 回の会議で 1 年半や 2 年かかるのに比べてこの動きは非常に早い。早いという点では、他のセキュリティ規格も同様で、28000 は 3 月の会議から始まって 11 月にはもう投票していた。このように、セキュリティ規格は動きが非常に早いというのが特徴である。逆に、このことが、みんながついていけない原因にもなっている。

TC8 第 8 技術委員会ではサプライチェーン・セキュリティ・マネジメントを担当している。TC8 で作った ISO/PAS28000 については、ISO のテクニカル・マネージメント・ボードの下に、セキュリティ・アドバイザリー・グループというのがあり、ここで今、ISO/PAS28000 がサプライチェーン以外のセキュリティ・マネジメントの規格になるかどうかと検討中である。まだ、答えが出ていないと理解している。

今、28000 シリーズと言えるものは、28000、28001、28003、28004 の 4 本である。28000 というのはすでに投票が終わって PAS になったもので、サプライチェーンのための保安管理システムの使用のための規格である。28001 は、あとで述べるが、マネジメントではなくより実務的なものである。28004 は 28000 を実施するためのガイドライン、28003 は、第三者機関による監査とか認証を行う場合の要件である。図解すると資料の 5 ページのようになる。28000 がトップに君臨する規格としてあり、その下に 20858 や ISO28001 の実務規格が入る。28000 をサポートするものとして 28004 が入る。ここまでが、各社、各事業所が使うための規格である。さらに、第三者認証機関のための規格である 28003 の上に、もうひとつ、ISO/IEC17011（認定機関が守るべき要求事項）という、この適合性の認証を行うための機関を認証する、アプリケーションボディと言っている規格がある。

28000 と 28004 は、もともと、28000 パート A、パート B にしようとしていたくらいで、

一体のものである。因みに、28004 を購入すると 28000 も入っているので両方買う必要はなく、28004 だけ買えば良い。

28000 は、環境用の 14001 をベースにしている。28000 は、考え方として、PDCA サイクルを要求しているが、このことは、9000 シリーズ、14000 シリーズと同様である。PDCA は、Plan, Do, Check, Action の略で、ポリシーにそって手順と目標を決め、手順を実施し、さらに実施状況をポリシー及び目標に沿って点検する。その上で必要な改善を行い、更に、ずっと改善し続けるというものである。

28000 の構成については、他の ISO 規格の構成と同様、1 番がスコープ、2 番が関係文書、3 番が定義となっている。4 番は内容であるが、その中では、評価とか保安計画の策定が詳細に論じられている。大事なことは、責任の明確化と責任者を決めることで、言っていることは、ISPS と同じである。能力、認識力訓練も明確に要求されている。データ管理というのは、コンフィデンシャル・インフォメーションの管理という意味である。

28004 に話を移す。28004 は、語数で約 16000 語。どの分野にどれだけの語数を費やしているかによってどこに重点が置かれているかを見てみると、4.3 評価と計画、4.4 導入と運用、4.5 確認と修正のところに記述の多くが費やされ、重点がこれらに置かれていることが分かる。これをまとめると、28004 で実行するよう言われていることは、ポリシーを決めて評価し（脆弱性評価）、計画を作って実施して、確認修正して、ずっと見直しをやって、改善しなさい、ということである。先の ISPS と比較してみても、装置の設置を除くとほぼ同様となる。実は 28001 もエッセンスを取り出して比較してみると同様となる。

セキュリティの専門家の方ならお分かりのように、対策について具体的に書くことは、セキュリティ上全くセンスの悪い話である。相手は意図的に攻めてくる犯罪者であり、このような者に対しては、セキュリティ対策それ自体が非常に重要な機密情報になる。我々はこれをセキュリティ・センシィティブインフォメーションと呼んでいる。セキュリティ・プランというものはめったに公開するものではなく、なかに何が書いてあるかは、厳重に管理されるべきものである。こうしたことから、規格の方も具体的に何をしろとはなかなか書けない、というのが実態である。

28001 は、インターナショナルを念頭に置いている。国際サプライチェーンの要素に適切な水準の保安の実施を可能とするもので、まずやるべきことは、この保安対策でカバーする範囲を明確にしよう、ということである。

メーカーの例で考えてみる。原材料の搬入に関し、原材料提供会社や運送会社でのセキュリティ対策は、自社のセキュリティに大きく関係してくる。次に、できた製品を出荷した場合、自社から安全に出荷しても、どこかにセキュリティ上の問題があって、その製品がお客様に届かないと意味がない。そうしたことから、自社のアップストリーム・ダウンストリームをちゃんと踏まえてサプライチェーン全体を眺めて保安をしなさい、と述べ、

これが 28001 の特徴である。保安評価を実施して、計画を作成して訓練をやれということがはっきり書かれており、これがイントロダクションになる。

内容に関しては、ビジネスパートナー(下請けと関係者)と保安対策上の関係者の範囲をまず決めましょう、そして、ビジネスパートナーの保安状況を確認しましょう、ということ。特徴的なのは同等性のみなし規定というものがあるということ。例えば、先の ISPS コードをやっていれば、この 28001 はやらなくても良い。保安プロセス（Supply Chain Security Process）とは何をやるかというと、このように計画をつくって実施チームを作って云々とだいたい同じようなことが出てくる。この中では、特に、5.7 の保安上の情報の保護が重要である。

この 28001 にはアネックスが 3 つある。アネックス A はサプライチェーン保安プロセスについて書かれ、保安の現状把握のためのチェックリストや脅威シナリオのリストが入っている。アネックス B は、保安リスク評価及び保安対策開発の方法論で、リスクマネジメントはできているという会社のためのものである。アネックス C は、助言及び審査の指針で、要は、監査を行うときとか、コンサルテーションを受けるときのアドバイスである。実は、この 28001 には、28003 と矛盾していることが書かれており、どうしたものかと悩みの種となっている。資料 13 ページは、サプライチェーン・セキュリティのフローチャートである。ここでは、継続的な改善を要求している点がポイントとなる。

余談になるが、セキュリティの訓練とは実際には何を訓練するのか。資料 14 ページの「参考：Security Awareness 」は、IMO のセキュリティオフィサーのトレーニングマニュアルに書いてあるものを私が一般化して抜粋したものである。要は怪しい人を見分ける訓練が一番重要なのである。ここでは、怪しい人を見分ける手法が書いてある。国連の IMO が作った資料なので、宗教や国籍といった問題を全部落としたものとなっている。

次に、28003 について。ISO の適合性評価委員会（committee of conformity Assessment ）では、現在、ISO/IEC 規格案である 17021 を作成中である。年内にできるかどうかというペースだそうである。28003 はこの 17021 をベースにサプライチェーン・セキュリティ・マネジメントに引きなおしたものである。内容的には、認証機関の原則というのがまず書かれ、そのなかでは、公平性/普遍性、力量/能力/適格性、責任/信頼性、公開/透明性、機密性/守秘性等について書かれている。これらの要素は、セキュリティの場合には非常に重要なものであるが、セキュリティ独特の表現に書き下ろすことはむずかしい。セキュリティ・マネジメントの認証機関の原則に関しては、情報の守秘性の確保の規定が一般規定のままでよいのかという疑問が出されている。もう一つ大事なのは、監査を行う人物がテロリストではないということをどうやって保証するのか、ということ。英語ではセキュリティ・クリアランスと言っているが（日本語では「人物証明」というのが一番しっくりくるようであるが)、そのセキュリティ・クリアランスは必要だという意見では一致しているものの、

実際に規定しようとすると、各国の法律もあって非常に難しい。このため、セキュリティ・クリアランスの要件は、今、28003 に入っていない。その代わりに、第三者認証機関の認可取消し、のようなものを入れたらどうかと、今、検討されている。

ところで、28000、28001 を採用するか否かと、第三者機関による監査や認証を受けるかどうかとは別の問題である。この第三者機関の認証を受けるか否かについては、二つの問題点がある。一つは、セキュリティにおける重要事項はアクセス・コントロールで、セキュリティプランはやたらな人に見せてはいけないものであるが、第三者認証を受ける際には、どうしても外部に情報を開示する必要がある、という点。28003（第三者認証機関の要件）には、現地に来て立ち入ってその場でセキュリティの状況を見なさいと書いてあり、ということは、第三者認証を受ける各社は保安対策を外部の人間を入れて見せなければならないということになる。

他一つは、第三者認証を受けることが、もっと言えば名刺に ISO28000 適合と書くことが実際の商売に結びつくかどうかという点。幾ら自分で 28000、28001 をやっていると言ったところで、それだけでは外部へのアピールにならない。また、一人よがりなだけで実はちゃんとできていないかもしれない。こういう問題があって、第三者認証を考えることになるが、本当に第三者認証を受けるべきかどうするかの判断は難しいところとなる。

最後に蛇足になるが、国際動向について一言。資料 15 ページの図に示したものは、セキュリティ問題に関係するアメリカの組織である。エネルギー省、国土安全保障省、運輸省、保険福祉省、食品医薬局、税関・国境保護局等々がある。 税関・国境保護局は、ご存知の 24 時間前申告ルール、C-TPAT，CSI 、Smart Container Initiative をやっている。メガポートというのは、Container Security Initiative の放射線物質バージョンで、放射線物質の探知を指導にくるというもの。Port Security Grants は港に補助金を出しましょう、というもの。バイオテロリズム法は食品の輸入に関係するものは完全登録制にしている法律。因みに、この法律に基づいてアメリカに登録した世界の機関のうちの半分は日本だそうである。以上が昨年 12 月時点のアメリカで行われている 8 つのイニシアティブある。WCO では、随分前から、税関の簡素化に関する改正京都条約というのができているが、これも非常に批准率が悪くてあまり実効があがっていない。この第 6 章にリスクコントロールという欄があり、税関で全部コンテナを開けて調べるのはやめましょう、と書いてある。余談であるが、第 5 章セキュリティとあるのは、税金をとりっぱぐれないという担保の意味のセキュリティであるので、テロ対策とは関係ない。こういうリスクコントロールで貨物の全数検査をやめようというベースがあって、Framework of Standards to Secure and Facilitate Global Trade 概念を出して、AEO いわゆる C-TPAT の国際世界バージョンをやろう、そして、危険性の低い荷主とか業者を調べて検査の手間を省きましょう、と WCO は考えているのである。

第三議題
「ISO/PAS28001 の概要」
渡邉　豊氏　東京海洋大学海洋工学部流通情報工学科教授
（資料Ｎｏ．５）

プログラムをちょっと訂正したい。

当初は、太田氏が２８０００を中心に、私が２８００１の方を中心に、ということであったが、参加者の関心に合わせて、ＩＳＯ規格を実際の社会の現場でどのように使っていくか、もしくは普及したらどのような問題が出てくるのか、というアプリケーションのほうを私が担当しようということになった。本日参加の皆さんにとって、一番の関心は、荷主の将来のためにと考えたときにこの規格がどうなっていくのか、というところではないか。この観点から、ＩＳＯになぜ矛先が向いたのか、をもう一度検証してみたい。

ＩＳＯ２８０００シリーズという場合、２０８５８、２８０００、２８００１の3つに絞ってお話したい。２８００３と２８００４は運用上の話だから、ここでは省く。

この3つについて、どうしたらどうなるか、について考えてみたい。例えば、９０００や１４０００の場合、社会に広まったあとは、それらを持っていれば、持っていない同業他社に対して何らかの差別化が出てきたり、国の入札のいわゆる足きりをクリアできたりするなど、1社でとることでメリットが出てくる。しかし、２８０００シリーズに関しては、そうは行かないだろう。では、各社が個別にとって意味がないとすればどうすれば良いか、２８０００シリーズを活かしていくとすると、どうしたら良いか。

国際サプライチェーンというのはいろんなところに盲点がある。その盲点は、セキュリティをしっかりやろうとすると、ますますクローズアップされてしまう。「安ければ何でも良いのではないか」、今まではそれでも良かったのだろう。しかし、セキュリティを無視できなくなると、安ければ何でも良い、という考えかただけは改めなければならない。

皆さんは物流の競争力を何と考えるか？　安ければ良い、便利ならば良い、安くて便利であればなお良い、皆さんは、そういう物流に興味を持つ。しかし、安かったり便利だったりする物流は、当然、皆さん以外のあまり良ろしからぬ人たちにとっても非常に魅力的なのである。安いからいろいろ仕込めるからである。港に誰もいなくなったらどうなるか。テロリスト、入場フリーパス！そうなると爆弾でも何でも仕掛けられるではないか。つまり、皆さんが安いからといって興味を持つものはそれ以上にテロリストたちは興味を持つと考えられるのである。

コンテナ 1 個の中身は１億、２億というのはザラ、場合によりもっと高い金額になる。そして、船には５０００個、６０００個、小さな船でも１０００個積む。これを、１億、２億、１０億で掛けたらどうなるか。莫大な損失額となる。安い物流というのはいざとな

ると入場フリーパスのテロリストによって爆弾が仕掛けられるというようなことも起こり得、時間トータルで考えた場合に本当に安かったのかどうか、ということになってしまう。

２００１年9月１１日が、Ｃ－ＴＰＡＴや、最終的にＩＳＯ２８０００シリーズが生まれてくるきっかけとなったのは確かである。しかし、実は9月１１日がすべてではない。それ以前にも、船がやられたとか、アタックされたなどのテロ事件があった。アフリカで、アメリカ大使館が完全に木っ端微塵とされたテロ事件が起きたのも２００１年9月１１日以前であったが、この事件は、特にサプライチェーンとか国際物流にかかわる話では注目すべきものである。このアメリカ大使館二つを爆発するのに使われた爆薬等は、海運を使われて堂々と港湾を経由してアフリカに持ちこまれたそうである。この事実はアフリカ当局では周知の事実であるし、米国当局も認めざるを得なかった。米国政府内では、いわゆるサプライチェーンと呼んで良いものかどうか分からないものの港湾や海運を使う国際物流が危ないぞ、いつかやられるというが意見があったそうである。しかし、この意見はマイナーなものとして無視され続けた。セプテンバーイレブンも、テロリストが３年間くらいアメリカ国内に潜んで準備したのであり、そういうことから考えると9月１１日がすべてのはじまりと考えるのは少し問題がある。

アメリカ政府は、セプテンバーイレブンが起きてしまったので、矢継ぎ早にいろんなことを行った。一言でいうと、コンプライアンスである。アメリカ政府は、いわゆる法律的な圧力によって、絶対従わなければならないという枠組みで、Ｃ－ＴＰＡＴ、ＣＳＩ、２４時間ルールを制定した。ＩＭＯのＩＳＰＳコードも同じころに制定されたが、これらは全部２００２年に出た。２００２年に徹底的にやって、ちょっとほっとしているときに、実際にはコンプライアンスではどうにもならないぞ、という事件が世界各地で起こってきた。

貨物の全数検査は、はじめから不可能である。４０フィートコンテナなら、最短１０分でスキャンできる、と検査機メーカーは言う。しかし、これは、何の問題もない場合のことである。中で何かおかしいものがあって、それが何だか確かめなければならないということになると、４０分、場合によっては１時間、余計な時間がかかってしまう。そして、メーカーは決してこのことを謳わない。ここに盲点がある。Ｘ線検査装置を設置すれば、おかしいな、というのがどんどん見える。検査に要する時間は技術的には１０分かも知れないが、人間の目や手でやる異常の有無の確認まで考えると、貨物の全数検査は無理である。アメリカの統計によると、実際の貨物の物流チェック率は１パーセント未満である。これを機械的に１００パーセントにもって行こうとすることが現実的かどうか、それが、だんだんアメリカ政府の上のほうにも分かってきた。

もう行政指導ではどうにもならない、Ｘ線で検査してもコーストガードに検査させても貨物の１パーセント前後しか検査できない、これでは、爆弾がどんどんアメリカに入って

きてしまうなどと危機感を抱いているうちに、ヨーローッパでも、マドリッドやロンドンでテロ事件がおきた。欧米は本当におしりに火がついてしまったという感じがする。このような背景と小郷氏の言うような背景とがあって、解決を求める矛先が全部ＩＳＯに向かってきたのではないか。こうして、２００４年からＩＳＯ／ＰＡＳが出てきたと考えられる。

第一議題の小郷氏は、ＩＳＯは民間ではあるがもはや民間ではない、と話された。ＩＳＯ規格を脚注であってもそのまま引用するようなアメリカやヨーローッパの法律が出てきたということは、重大な意味がある。ＩＳＯ規格が名目ボランタリーだけれども実質コンプライアンスになりかねない、という状況になってきたと言えるからである。この潮流に対して、日本は動きが早かった。産官学で対応して代表をＩＳＯ２８０００シリーズ策定委員会に送った。本日講師を務める我々３人も送っていただいた。

ＩＳＯ規格の取得について、皆さんは、アメリカとヨーロッパに先行されても致し方ない、と思われているかもしれない。しかし、この点、もし東南アジアに先行されたらどうなるか。今、ＩＳＯを一番沢山取得しているのは中国だそうである。太田氏と意見が異なるのは次の点であるが、規格が良いかどうかは別として、競争相手に規格取得を先行されると商売として負けではないだろうか。そういう観点から、情報の取得にしても、日本の業界の対応ははたしてこれで良いの？と言いたい。東南アジアで日本より情報が周知され２８０００シリーズをとる会社が増えたらどうするのか。とにかく民間企業の動きが非常に鈍く、これで良いのかと私は言いたいのである。

２８０００シリーズ、これをどうやって使うのか、また、どこに問題点があるのか。
大手の荷主の場合、トップマネジメントでセキュリティをやるということで２８０００が適していると思う。
不特定多数の無数の顧客のコンテナを扱う船会社や港湾ターミナルの場合は、貨物を受けるだけなので、２０８５８が適している。
マネジメントがなく、受けたものを処理するしかなく、現場がすべてである港湾と船舶のファシリティ（facility、施設)、中間介在するフォワーダーや代理店、トラッカー、中小の倉庫の場合は、２８００１向きかなと思う。
先程太田さんがいみじくも言っておられたように、一社でとっても仕方ないではないか、物流のアップストリーム、ダウンストリームで良からぬ会社と組んでしまったら、自分たちの努力（２８０００をとった）は、水泡に帰す。この辺が１４０００、９０００とは違うところである。単独では利が出ないのではないか。ただし、みんなで手をつないで、一つの線が、全部セキュリティパス（私はセキュリティ規格で繋がることをこう呼ぶ、和製英語かも知れないが）が繋がっていけば、アメリカからもヨーロッパからも評価されて良

い面もでてくる。

ＩＳＯシリーズが良い規格だということを前提として、セキュリティが完璧である、テロリスト防止対策としては一番良い状態のレベルというのは、輸出国側でも輸入国側でも、つまり、送り荷主、受け荷主の両方とも同時に２８０００を取得することである。２８０００の条項のなかには、下請けをつかう場合には、下請けの安全性は自分で調べなさいという条項がある。ということは、出す側も受ける側も自分で、自分が使っている物流の子会社に対しては、監査しなければならない。自分で監査できなければ当然２８０００はとれないので、２８０００をとったとなると、一応下々の会社までＯＫだということになる。残るは、水際だけ、港湾と港湾の間だけとなる。そこで、港湾には、２０８５８を取得してもらう。こうすれば、一応、いわゆる最高と言えるかどうか分からないにしても、理論上は、セキュリティレベルは一番高くなる。船会社に乗る段階ではコンテナが閉められ場合によってはスマートタグなどが付いてしまっているので、この段階では、別に船会社がとろうがとらまいが私の考えとしては一切セキュリティレベルには関係ない。要するに、船会社さんは体制に影響はない。

では、荷主の皆さんが２８０００はとりたくない、金もかかっていやだと言ったら、どうするか。荷主が２８０００をとらずして、セキュリティレベルを高めテロリストからの攻撃をかわし、アメリカ・ヨーロッパ・日本の行政から認めてもらえ将来さらによい商売をと思ったとき、この２８０００をどう活用するか。そういった場合は、以下のようにすれば良いと考えられる。荷主が使っている物流業者になるべく彼らの負担のならない形で２８００１を取得させ、そして、港湾ターミナルにも２０８５８、もしくはＩＳＰＳコードをとってもらうことである。こういう状態が輸出国側と輸入国側で成り立てば、これはかなり高いセキュリティレベルとなる。こうなれば、荷主は何もやらなくても良い。荷主の皆さんは、この状態にもって行く努力ができるだろうか。その努力の方が、荷主自身で２８０００をとるよりは、負担が少ないかも知れない。ただ、貿易というのは相手国がいるので、相手国側でも同様にしてもらう必要がある。

いろんな組み合わせを考えてみる。一つ一つの条件が満たされなくなってくると、セキュリティレベルは下がってくる。例えば、輸出国側で皆さんの下請けがなんとか２８００１をとってくれた、港もなんとか頑張ってくれた、ところが輸入国側がなにもやってくれなかったらとしたら、どうなるか。この時点でセキュリティレベルは中程度。これを改善するにはどうしたら良いか。こういう場合には、２０８５８か２８０００をとっている船会社と組む。そういう船会社に皆さんの貨物を流せば良い。この２５８５８、とくに２８０００だと、自分が使っている下請けに対しては、自分の会社の枠組みのなかでセキュリティをちゃんと監督管理しなさい、セキュリティレベルを高めなさいという内部監査の仕組みがあるので、それでなんとか相手側のいたらない部分をカバーできるかな、という気がしている。こうすれば、かなり高いセキュリティレベルになる。

輸入国側が規格をとったのに、日本の荷主が何もやらないケースを考えてみよう。トップの荷主が何もやらないので、下請けも何もやらない。なにもやらないというのは、セキュリティ関係の規格をとろうとしない、ということ。一方の相手国側は港のセキュリティが完備されている。こういう状態ではセキュリティレベルは高まらない。理由は簡単である。出るところでいろんなものを入れられて、港についてコンテナ船に乗せられる。コンテナの箱は閉まってしまうと、相手国で貨物の実物検査をやっても１パーセントではないか。実際に見つけられるのが１パーセントだとすると、残り９９パーセントはフリーパスになる。このような状態では、いくら輸入国側でＩＳＯのセキュリティ規格をみんな揃ってとったとしても、何の役にも立たない。

この段階で日本としてなんとかしようと思ったらどうするか。日本の荷主もとりたくない、下請けの人たちも言うことを聞かない、港も言うことを聞かないと言ったときには、船会社が頑張るしかない。船会社に認証をとってもらうしかない。船会社は、国内物流サイドとか国内物流ターミナルを自分たちの子会社として使っている。特に日系船会社の場合は、船会社が一番上に立っているピラミッド型。港湾ターミナル、ドレージ会社、つまり、コンテナ陸上輸送会社、系列、系列・・と続くピラミッド型。こういう状態のなかで、船会社が認証をとって自分の系列にいる荷主さんに繋がっているようなところのセキュリティを維持するしかない。

では、輸出国側も輸入国側も何もとらない、もうお手上げという状態で、なんとかギリギリ、セキュリティレベルを高めるには、どうすれば良いか。結局、この場合も船会社に頼るしかない。船会社には輸出国側も輸入国側も来るので、どちら側にも系列の子会社を持っている。だから、大きな船会社に２８０００をとってもらえば何とかなるかもしれない。でも、船会社は大変である。輸出国側でも、輸入国側でもセキュリティを確認し、たとえば中国の奥地の人までの教育もしなければならない。相当のお金と労力がいる話で、船会社は潰れてしまうかもしれない。荷主の皆さん、それでよろしいのか。船会社にすべてを任せるのは難しいと思う。

テロリストが皆さんのサプライチェーンに介在しないようにするためにはどうするか。９０００や１４０００のように点で見るやりかたは駄目で、あくまでもセキュリティパスというものを考えなければならない。しかし、セキュリティパスを完全に繋げるのは容易ではない。物流企業、港湾ターミナル、トラック業者等々、認証済みの会社もあれば未認証の会社もあり、そのなかで、認証済みの会社だけで繋いで行くというのは本当に難しい。そしてこの困難な状況が世界レベルで起こるわけである。

皆さんの貨物はダイレクトコールでアメリカに行っているか。安さを理由に中継港が使われることが多い。しかし、この中継港には、全世界津々浦々から貨物がやってくる。つまりセキュリティパスがある貨物もあればない貨物も全部この中継港で積み換えられるのである。皆さんは、日本の港までセキュリティパスを繋げばそれでＯＫだ、と思ってい

るかもしれない。でも、それは大間違いである。日本の海までセキュリティパスが繋がっても安い中継港を使った海運サービスを利用すると、セキュリティパスは、そこで途切れてしまう。極東の世界的な港のＩＳＰＳコード準拠は疑問である。その港で、私は、太田氏資料にある不審者発見マニュアルの三つか四つに当てはまるようなことを、つまり、ビデオを持ちながら、ノートをとりながら、金網からデジカメつっこんで写真を撮りながら、半日、歩きまわったことがある。いつか必ずおまわりさんがやってくる、と思いながら。しかし、誰もこない、横にＩＳＰＳコードＣＣＤカメラがあるにもかかわらず誰も来なかった。これでは、セキュリティは維持できない。日本では、港湾の職員が私と同じようなことをＩＳＰＳコードのことなど知らないでやったら、いきなりビデオに写って大騒ぎになって捕まってしまったと聞く。

話を戻すが、安い中継港を使っている限りは、結局は外国までセキュリティパスは繋がりにくい。中継港には、もう一つ、問題がある。メーカーの皆さんは、海外でフリートレードゾーンを使ってアッセンブリーを行っていないか。フリートレードゾーンというのは港湾ターミナルの外側にある。だからフリートレードゾーンという。税関の管理をはずれるから、フリーという。その港が、ＩＳＯ認証、ＩＳＰＳコード認証の港湾だったとしても、そして皆さんが使っている、サードパーティロジステクスがやはりＩＳＯ認証で連携したセキュリティパスを持ったリンクだったとしても、フリートレードゾーンのなかに部品を運んでそこでアッセンブリーをして半製品もしくは製品にして再出荷するとなると、セキュリティパスが途切れてしまう可能性がある。勿論、皆さんが再出荷するために使うサプライチェーンもＩＳＯ認証を受け連携したセキュリティパスが整ったものであれば、フリートレードゾーンでのアッセンブリーも大丈夫である。しかし、すべてのサードパーティロジステクスがＩＳＯ認証を受けしかもすべて連携してセキュリティパスまで成り立たせるなどは稀だと考えられるから、フリートレードゾーンのなかでアセンブリーをした結果、セキュリティパスが途切れる可能性が出てくるのである。このフリートレードゾーンの危険性については、私は２８００１の一番最初のマドリッド会議で指摘し、そのあとのパナマ会議でも指摘し、その後もずっと指摘し続けている。さすがにＷＣＯがその危険性に気が付き、どうやらＷＣＯで正式に問題点の一つとしてとりあげたと聞く。

時間となったので、これで纏めるが、セキュリティの意識の高まりのなかでは、やはり安ければ良い、日本にある港からフィーダを利用して出荷し、安い中継港を使って適当にというのは、考え直したほうが良い時期に来ている。ある代表的な自動車メーカーの例を挙げよう。そのメーカーは地元の港を使っている。高級車の部品をフィーダで物流やっていると聞いたことがない。みんな日本にある地元の港からダイレクトで送っている。日本の港の湾物流料金は世界で一番高い。それなのに、そのメーカーは地元の港を使い、今後は事実上自社専用のコンテナターミナルをつくって、自身で運営しようとするところまで

行っている。安ければ良いということであれば、こういうことはしない。セキュリティを考えた上のことだと思う。

中継港の多くにはフリートレードゾーンがある。中継港には輸出と輸入がないわけだから、儲けようとしたら中継、さらに儲けようとしたらフリートレードゾーンしかない。だから、中継港には１０中８、９大きなフリートレードゾーンがあり、物流ロジセンターがあって関税を軽減して外国企業をたくさん呼んでいる。そういうところに対してはそろそろ注意して行かなければならない。テロ事件がおこっても、その中継港の政府から保障が得られるとは考えにくい。多くのコンテナを巻き込んだ保障は皆さんが行うことになる。だから中継港は安いのである。

今少し、日本からのダイレクト、直行便を見直していただきたい。皆で使うと安くなる。日本人だけしか使わないということであるなら、日本人流のセキュリティも維持できることにもなる。そういうことを今一度考えていただきたい。

第４議題
「ＷＣＯ・民間との協議グループ第一回会合の概要」
事務局（部会・貿易業務グループ　グループリーダー　橋本　弘二）
（資料Ｎｏ．６）

ＷＣＯの民間との協議グループ会合が、３月下旬に開催された。その席では、このＩＳＯ２８０００絡みで２８００１のドラフトも提出されている。本協議グループ会合には私が出席したので、ごく簡単にご報告したい。

ＷＣＯ（世界税関機構）は、世界の税関当局が集まる国際的な枠組みである。本日もたびたび話が出てきたように、２００１年９月１１日の同時多発テロ事件を契機として、米国政府はサプライチェーンのセキュリティ対策に非常に力を入れてきており、米国内では、Ｃ－ＴＰＡＴ，２４時間ルール、ＣＳＩ、といったような一連のプログラムを実施している。そのＷＣＯでも、米国政府の強い働きかけもあって、サプライチェーンセキュリティの税関にかかわるルールの国際的な標準ルールをつくろうという趣旨で、検討を進めている。

ＷＣＯは、昨年６月下旬の総会で国際貿易の安全確保及び円滑化のための基準の枠組みを採択した。それ以降は、どのような具体的な実施ガイドラインを作っていくかに焦点が移ったが、この実施ガイドラインを作成するにあたって、ＷＣＯのなかでおそらく初めてと言われる民間企業に集まってもらっての検討会議をやり、そこから助言を得ようということになった。これが民間との協議グループＰＳＣＧ（Private Sector Consultative Group）と言われるものである。ここで注意したいのは、ＷＣＯで決められることはすべてノンバインディング(Non-Binding、非拘束)であり、ガイドラインになる、ということである。し

たがって、条約のように必ず各国強制的に同一の基準、同一の期日をもってこの内容を実施するというようなものではなく、非常に緩やかな結びつきであるというようにお考えいただきたい。いつから始めるか、取り決められたもののうち何を実施するか、どのように実施するか等も、それぞれ各国税関の裁量に委ねられる。

このＰＳＣＧが３月末に初めて集まり協議をもった。そして、４月の２５、２６日には上海で第二回会合を行うとしている。ＰＳＣＧは、ＷＣＯのハイレベルストラテジックグループ（ＨＬＳＧ）というところに、アドバイスを行うことになっているが、このアドバイスそのものもＷＣＯ当局がすべて取り入れなければならないものではなく、あくまでもアドバイスという性格のものである。極端な想定ケースとしては、ＷＣＯがこのＰＳＣＧからのアドバイスをすべて無視してしまうということも可能性としてはあり得る。

まず、２００５年６月末にＷＣＯ総会で採択された「国際貿易の安全確保および円滑化のための基準の枠組み」がどのようなものかということをごく簡単に説明したい。資料６の１ページにあるように、基準の枠組みは、４つのエレメント、２本のピラーから構成される。アメリカ政府からの強い働きかけをベースに始まったイニシアティブであるので、アメリカのセキュリティプログラムをベースとした内容になっている。

まず、４つのエレメントを見ていく。

① 「輸出入及び通過貨物に関する事前電子貨物情報要件を調和化させる。」これに対応するアメリカのプログラムは、２４時間前ルールである。

② 「安全確保に関する脅威に取組むために、整合的なリスク管理アプローチの利用にコミットする。」米国サイドでいえば、Automatic Targeting System である。リスクマネジメントの手法でハイリスク貨物を選別する、そういう手法を各国とも採用しましょう、ということを進めているということである。

③ ここでの、受入国というのは輸入国ということ。仕出国というのは輸出国ということ。すなわち、輸入国からリクエストがあって、輸出国の税関当局が、例えば、大型Ｘ線装置、放射線検知機のような非破壊探知機を使用してハイリスクコンテナ及び輸出貨物の輸出検査を行う。これはＣＳＩで行われているものに相当し、すなわち、輸出国で貨物のプレスクリーニングを行う、ということである。

④「最低限のサプライチェーン安全基準及びベストプラクティクスに適合する民間に対して税関が与えるベネフィットを明確にする。」これは、すなわち、Ｃ－ＴＰＡＴである。

この４つのエレメントに基づいてセキュリティ管理を実施際の実施の柱として、２本のピラーを挙げている。すなわち、①税関相互の協力と②税関と民間とのパートナーシップである。

因みに、この基準の枠組みの原文（英文）及び仮訳の和文は、財務省関税局のホームページにアクセスするとダウンロードできる。

昨年６月末の基準の枠組み採択後、この基準の枠組みを実施することを表明している国

の数は、当日のＷＣＯ事務局からの説明によれば、すでに 131 カ国になっている。
　ＰＳＣＧがどのような構成メンバーになっているかと言えば、物流あるいはサプライチェーンに関わるさまざまな要素あるいは世界各地の地域的に偏らないように配慮して３０の企業と業界団体を募集したということであった。資料の最後のページに参加企業・団体を列挙した。

　会議では、まず、ＷＣＯ事務局長が挨拶をし、ついで、出席者のなかから議長と副議長を選出した。議長にはルネ　スタイン女史（マイクロソフト）が、副議長にはイアン　インペイ氏（グローバル・エクスプレス・アソシエーション）が選出された。
　挨拶等の儀式が済んだ後、ＷＣＯ事務局の人たちは全員会議室から退出した。これは、あとは民間だけで自由に活発にご議論ください、という配慮であった。
　当初予定された議題は、①ＡＥＯの条件・要件とベネフィット、②ＡＥＯの確認と認定（Validation・Accreditation）、③相互認証（Mutual Recognition）、④ＩＳＯ２８００１、⑤キャパシティ・ビルディングであった。
　このうち、最も焦点をあてて議論したのが、①ＡＥＯの条件・要件とベネフィットについてであった。
　①のＡＥＯとは、Authorized Economic Operator の略で、米国のＣ－ＴＰＡＴに相当する。すなわち、社内の自主管理が優良な企業をＡＥＯとして認定し、認定された企業にはベネフィットを与えるという制度のＡＥＯになるための要件、それに対するベネフィットを議論した。
　②は、ＡＥＯに認定された企業はどのようにセキュリティ管理を行っているか、ちゃんと報告した通りに行っているのか、そういうことを立ち入って on sight　で検証する。ここでいう Validation は、実施調査と訳して良い。Accreditation という言葉の概念は、実施調査に入って、企業の管理内容を見ながら、その質的なレベルを見ること。Ｃ－ＴＰＡＴでは、アメリカの場合、ティア１から、ティア２、ティア３と段階分けをしており、ティア３が最もレベルの高いベネフィットが受けられる、すなわち、管理内容が一番質が高いという認定をしている。そういう認定に対応するものと考えていただきたい。
　③は、各国税関が認定したＡＥＯを相互認証しましょう、というもの。
　④については、資料としてＩＳＯ２８００１の英文原文が配布された。
　⑤は、途上国に対する支援について。

　私が、会議を通して最も強い印象を受けたのは、出席企業のすべてが相互認証の実現を強く望んでいる、ということであった。会議参加前は、アメリカがセキュリティ強化を主張するのに対して、その他の国がそれは厳しすぎると反対する、という色合いを予想していた。ところが、まったくそのような要素はなかった。まさに税関に対する注文、企業のオペレーションを効率化させるためにどのように税関当局に注文をつけていくか、という

トーンで一色であった。その中で、最もリクエストが強いものが相互認証であった。規制制度は各国ごとにあるし、手続きについても各国ごとに差異がある。こうしたものをできるだけ標準化し統一された一貫性のあるものとすることによって相互認証を実現させたい、ということである。この相互認証そのものについては十分な議論ができなかったが、相互認証に対する要求の強さということだけは極めて明確に印象付けられた。他一つの印象としては、ＡＥＯとなるための条件あるいは要件というものをセキュリティ管理に関わるものだけに限定すべきとする主張が非常に強かった、ということ。例えば、企業の財務健全性を要件としたいと述べられると、即、セキュリティに関係ないから外すべきであるといった反対があったり、できる限りセキュリティにフォーカスをあてたＡＥＯにしたいとする主張が多かった。

資料３ページの「・各国税関当局は、ＡＥＯに係わる統計データを公表すべき」も、各出席者に共通のリクエストであった。ＡＥＯの認定数、ＡＥＯに対してはどの程度検査を行っているか、検査率はどうなのか、そして、それらは一般企業に比較するとどうなのか、ということ。このような統計データを公表させるべきだ、というものである。企業がセキュリティ管理をやるには当然投資を行うことになるが、このような統計データを公表することによって、そのためのＲＯＩを計測するのに有用なデータが得られる、あるいは、国際的な運用に関するベンチマークを提供することによって、相互認証に道をひらく、あるいは、キャパシティ・ビルディングとして途上国を支援する場合の支援目標とすることができる。そういうことからくる要望である。米国は早くからＣ－ＴＰＡＴを行っているので、この種の統計データを公表している。例えば、Ｃ－ＴＰＡＴ参加企業はすでに１万社を超え、認定されている企業は５０００社を超え、立ち入り検査が入った企業数はすでに２０００社になろうとしている、Ｃ－ＴＰＡＴ認定企業に対する検査率は他の企業に比べて４分の１である、などである。このようなプログラムを実施しているのは、一部を除けば、今のところまだアメリカだけであるが、今後、ＥＵが実施する、あるいは日本が実施するといったようなことになると、各国間でこのような統計データの比較が行われるようになるだろう。

ＩＳＯ２８０００シリーズに関する議題については、ＩＳＯの中身そのものに踏み込んだ議論は行われなかった。ＩＳＯ２８００１の資料が配布されたが、その中身は例えばＣ－ＴＰＡＴの内容と非常に類似しており、きわめて業務直接的なサプライチェーンセキュリティの管理の内容が書かれている。これに対して、各国税関が国際ルールを決めずともＩＳＯ２８００１に準拠していきましょうと強く主張する一部の企業があり、この主張に対して、反対する企業もあった。認証方式については、ＩＳＯ９０００のような認証方式では、おそらく税関は受け入れないであろう、また、そもそも十分な認証能力をもった認証機関が存在するのか、という問題の提起。外部認証機関とする案では、中小企業にはコスト負担が重過ぎる、といったような反対論。また、自分（運送業界）の業界の中では国際標準ルールというものがあり優良な運送人を決めるスタンダードが決められており、Ｉ

ＳＯという国際標準をもってくれば国際標準が二重になってしまう、というような反対論。これら議論は当日結論が出るというものではなく、今後の会合でも一足飛びに結論が出るという雰囲気ではない。ただ概念的なところで言うと、国際標準に基づいて一貫性のある統一的な運用が国際的に行われて相互認証が図られることについての反対はないということである。

当組合からの提案は、主に以下を内容とするものである。すなわち、現在米国が行っている２４時間ルールでは船積み前申告となっているが、これはリードタイムが伸びる等々の負担を生じさせるので、このような弊害をなくすように、ＡＥＯについては船積み前ではなくて到着前の貨物情報の申告が認められるようにしてもらいたい、ということ。この提案に対しては、世界各国とも荷主の考えることは同じであるのか荷主団体からの支持を得たが、オーシャンキャリア、船舶の業界団体の方からは強い反対があった。今後物流におけるサプライチェーンセキュリティ、優良企業の認定とベネフィットということを考える場合には、オペレーションの問題からプライベートセクター間でベネフィットのコンフリクトが起こり得るということが分かった。ＡＥＯに対するベネフィットを検討する場合、このような可能性に対して十分配慮して検討すべだということを改めて次回会合の場で提案をしていきたい。

以上

資料目録

資料Ｎｏ．０：ＩＳＯ／ＴＣ８でのセキュリティ国際規格提案の経緯について
資料Ｎｏ．１：別紙　ＩＳＯ（国際標準化機構）／ＴＣ８（船舶及び海洋技術）の戦略的役目
資料Ｎｏ．２：ＩＳＯのプレスリリース
資料Ｎｏ．３：ＩＳＯ／ＰＡＳ２８０００と Supply Security Management 規格
資料Ｎｏ．４：ＩＳＯ／ＰＡＳ２８０００シリーズ（海事保安関係国際規格）の概要
資料ＮＯ．５：ＩＳＯ２８０００シリーズの普及の方向性について
資料Ｎｏ．６：ＷＣＯの「民間との協議グループ」第一回会合参加報告
参考資料：公開仕様書　ＩＳＯ／ＰＡＳ　２８００１　日本語訳（日本船舶技術研究協会提供）