# CSA と ISO の世界に挑戦！

**日本システム監査人協会　理事**
**IT アセスメント研究会　　主査　松尾正行**

## 1．はじめに

60歳定年という会社人生から見ると、私がシステム監査人の世界に入ったのは会社卒業後ということになる。

本稿では現役時代の経験を IT ガバナンスの視点で振り返るとともに、ISO での活動を紹介して CSA や CSA を目指す方々のお役に立てればと考え筆をとる次第である。

私は大手海運会社（以下当社）に入社し、20 歳代からコンピュータ部門（当時は事務管理室）勤務となり、IBM S/360 をはじめメインフレームのプログラマーがキャリアのスタートであった。その後、システム設計やシステム企画部門を経験して、国際オンラインシステムの開発・運営に携わり、IT 部門の責任者に至った。会社生活で半分の期間は海外とのシステム開発や運用に関わり、うち 11 年間は米国に駐在してインド、香港などの拠点と協業する形でシステム開発と運用の責任者を勤めた。本社からの出向者数名をのぞき、300 名近い技術者はすべて外国人で出身国籍は 30 か国を超えていた。

IT 部門がコストセンターとみなされる傾向は当社でも同様だが、国際オンラインシステムはコンテナ輸送業務の中核であり、ユーザは世界中におり、費用も巨額に上るため、ビジネス部門や経営の要求は極めて厳しいものであった。社内でも突出して IT ニーズが高く、本社用とは別の IT 部門を組織していた。経営のリーダシップによる組織の大改革と IT ガバナンスの改革も経験した。

61 歳で米国勤務から帰国し（2006 年）、いよいよ引退と考えていたのだが、内部監査部門（現経営監査部）からオファーを受けた。2008 年度から始まる内部統制制度（J-SOX）の IT 関連の整備を頼みたいとの要請であった。結局その後 13 年間にわたって J-SOX とシステム監査を担当することとなった。

## 2．現役時代の業務（背景）

### 2.1　海運はネットワークビジネス

国際海上輸送は古くは外国航路（略して外航）と言われ、横浜や神戸の港からロサンゼルスやサザンプトンといった外国の港へ貨物を運ぶビジネスである。世界中のあらゆる国・港に代理店を置き、貨物の集荷営業、積み込みと引き渡し、運賃の回収、費用の支払いから船の入出港手続きに至る現場業務を行っていた。世界中に張った営業ネットワーク資産があってのビジネスである。

コンテナの海上輸送は 1956 年米国の国内輸送から始まり、私の米国勤務の最終年となった 2006 年は海上コンテナ輸送開始の 50 周年といわれる。米国から帰任する際に友人が餞別にくれた書籍（＊1）に輸送モードの変革過程が詳しく書かれており、単なる輸送技術の変革ではなく、既存の輸送インフラ（道路、鉄道、船舶）、商慣習と権益、法制などを巻き込んだ輸送ビジネスの革命だと述べられている。

＊1　The Box That Changed The World,　Containerization and Intermodal Institute

### 2.2　ビジネス変革の波

#### 2.2.1　輸送方式の変化（モーダルシフト）

米国におけるモーダルシフトが 10 年以上遅れて日本やアジア諸国に押し寄せてきた。日本のコンテナ専用船が太平洋航路に初就航したのは 1968 年であった。

長年「港から港まで」という海上部分のみの輸送ビジネスが、コンテナ輸送では「Door to Door」というコンセプトでビジネスの範囲が広がり、かつ輸送の手段もコンテナを単位として陸上輸送までカバーし、いわゆる複合一貫輸送（マルチモーダル）に拡大した。船は輸送の一セグメントに過ぎなくなり、膨大な情報を扱うため IT の支援がないとビジネスが成り立たない劇的な変化が発生した。

#### 2.2.2　組織の変化（代理店網から現法化へ）

ビジネスの変革は組織の変化も求める。伝統的な代理店ネットワークでコンテナ輸送ビジネスを行うことは不可能となり、当社も各国、地域に現地法人を設立して自営形態へと変わらざるを得なくなった。

業務体制も代理店任せから、自前の体制へと変化を余儀なくされた。業務プロセスの標準化と IT の支援が不可欠になったことは言うまでもない。しかし、100 か国を超える国、地域の業務プロセスを一気に標準化することはそれまでの海運業界では至難の業だし、要員も十分ではなかった。

#### 2.2.3　IT ニーズの顕在化

前述のとおり現場の業務はすべて代理店依存というのが伝統的なビジネス形態である。本社の社員は現場の業務については詳しくはない。現場では本社の意向がどうであれ、現場の都合を優先することになる。典型的な部分最適の構造であった。

コンテナ輸送ビジネスでは、旧来の代理店依存の仕組みから脱却し、全体最適かつグローバルな自前の仕組みが必要とされた。特に IT を活用したビジネスプロセスの標準化、最適化、スピード化の重要性が認識された所以でもあり、経営レベルでの IT ガバナンスの重要性が顕在化したといえる。IT を業務プロセス革新のツールとして位置付けることも認識された。

## 3．IT 化競争と IT リテラシー（米国での IT 利用）

### 3.1　IT 化の歩み

コンテナ輸送は北米航路を皮切りに、豪州航路、欧州航路・・・と順を追って拡大していった。IT 化といってもいきなりオンラインシステムができるわけではなく、まずは必要な情報のデータ化と輸出側と輸入側でのデータ交換システムの構築や双方でのシステム化が必要になった。

大まかに変遷を記すと次のようになる。

| | |
|---|---|
| 1968 年～ | 輸出側、輸入側のドキュメンテーション業務の機械化（分散型システムの導入） |
| | 日本国内オンラインシステムの導入 |
| 1973 年～ | GE 社のタイムシェアリングシステムを使った電子データ交換網（EDI）の稼働 |
| 1980 年頃 | 第一次北米オンラインシステムの稼働（東京のメインフレームと米国の分散機） |

### 3.2　北米システムの開発と失敗

第一次北米システムは大掛かりなプロジェクトで開発されたが、米国、カナダ、メキシコの現場の不満は解消せず、評価は芳しくなかった。当時の日本人のシステム感とは大きく異なり、北米のシステム依存度が数段高かったためである。

抜本的な解決策として、本社のシステム部門に全面的に頼るのではなく、北米にシステム専門会社を設立してシステムの開発運用も自主的に行うことを決定した。

1988 年頃、米国（ニュージャージ州）にシステム専門の現地法人が設立され、システム開発が始まったが、ビジネス用には普及していなかった UNIX 系のサーバー、ワークステーションで GUI を使ったシステム開発を提案してきた米国の業者に発注してしまった（Windows 95 発売の 8 年前のこと）。

私は自己都合で米国赴任できず直接かかわってはいないが、プロジェクトの進捗に不安を持った事業部門から、プロジェクトの具体的進捗、技術などに関する診断を頼まれ、1990 年に約半年間ニューヨーク事務所に常駐した。いわゆるプロジェクト監査で、米国とオランダの開発拠点を調査して、報告書を本社に提出した。

報告書は、プロジェクト管理、外注管理、技術の適合性などに各種の問題を抱えているという内容で、関係者を驚かせた。その正しさは稼働初日にシステムを停止せざるを得なくなったことが証明している。2 年の時間と百億円を超える予算の浪費であった。(*2)

＊2　「私の履歴書　生田正治」　日本経済新聞　2011 年 1 月

### 3.3　米国赴任で再挑戦

本社は現地法人の改組、システム開発体制の刷新、技術の見直しなどの方針を決め、プロジェクトの責任者に私が指名され、副社長として 1991 年 8 月赴任した。組織、要員、技術、業務プロセスなどすべてを短期間でやり直すことが至上命題であった。数か月後、プロジェクト計画と予算書を携えて、私は本社の予算委員会で承認を求めたのだが、経営層、他部門から猛烈な批判に晒されたことは生涯忘れられないだろう。

それでも何とか 2 年で新システムの基本部分を稼働させ、その後も順調に機能拡張を続けることができた。施策の内容を書く余裕はないが、次のようなポイントであった。

1，組織の改組とプロジェクト体制の明確化

2，現地採用の技術者、ビジネスプロセスの専門家などの入れ替え

3，業務部門のビジネス要件整理体制の再編成

4，開発手順の明確化とプロトタイピング体制の設定

5，サーバー、OS、ミドルウェア、データベース管理システムの選定のやり直し

実態はこのような整然としたものではなかった。現地要員の採用だけでも 100 名近い面接を行った。メーカ各社の提案審査にも苦労したし、圧力も受けた。最も大変だったのはユーザ対応であった。米国でもユーザが主体でシステム部門は下請け的な発想があり、米人の上層部までそのような考えだったのでその対応にも神経を使わざるを得なかった。本社の立場から現法へと立場が変わるとかくも大変かと身に染みた次第である。

新システムの稼働によりようやく希望通りの機能を手にしたユーザ部門の不満は激減し、批判一本やりであった本社側に北米システムの認識変化が出てきたのは収穫であった。

### 3.4　アジアへの展開

1997 年春に帰国して情報システム室の専任部長となったが、アジア地域本社(香港)から、北米システムをアジア（日本を含む 15 か国）向けに展開したいという提案が出てきた。開発部隊を香港とインドに置いてプロジェクト化したいという。アジア地域を統一システムでカバーするという構想は大きな効果が期待できること、北米システムのノウハウ活用と米人技術者にも挑戦の機会ができること等、メリットも大きいので本社は推進を決め、私は本社側で支援することとなった。2000 年にはアジア全域をカバーすることができた。

当時、欧州地区では別のシステムを利用していたが、アジアと北米が同じシステムを使うことで、コンテナ輸送の大動脈をカバーでき、本社には安心感が漂ったと思う。しかし、この考えは甘かった。

## 4．　世界統一システムへ

### 4.1　トップの交代とガバナンスの違い

1999 年 6 月、当時世界最強のコンテナ船会社であった米国の A 社の会長であった GH 氏が当社の副社長に迎えられ、コンテナ輸送部門のトップになった。(*2)　まもなく私は彼に当社の IT 状況を詳しく聞かれた。本社の経営者で IT に関心を寄せた数少ない人物である。

GH 氏は当社の組織とシステムが航路・地域・国ごとのサイロ状態であることに驚き、これでは競争力の維持は難しいと直感したようである。北米、アジア、欧州それぞれでシステムは円滑に動いていたので、経営陣は、なぜシステムを統一しないのかという GH 氏の指摘を受けて驚いたと思う。このころ海外の競合大手は盛んに自社の IT のすばらしさを喧伝していたし、E-コマースのスタートアップが続々とこの分野へ進出してきた時期でもあった。

＊2　「私の履歴書　生田正治」　日本経済新聞　2011 年 1 月

### 4.2　組織の大改革と再渡米

2000 年 3 月、私は役職定年で退職となったが、コンテナ事業部門がシステム担当専任部長のポストを用意して迎えてくれた。

GH 氏を中心に、コンテナ輸送ビジネスの大改革が始まった。

組織面では仮想の社内分社「仮想コンテナ会社」を実施し、GH 氏がリーダシップをとって本社、各地域のトップに経営、投資、業務戦略を説き、それを支える IT 機能では、各地に分散しているシステムを統一して、単一のシステムで世界をカバーすることを決めた。明確なガバナンス目標である。

私は IT 責任者としてエグゼクティブ会議のメンバーとなった。ガバナンスやリーダシップの最前線に出たわけである。2001 年 8 月、GH 氏により私は古巣の米国現法社長に任命され再渡米した。今度の役割は、地域システムからの脱却と世界統一システムの整備であり、組織的には米国、香港、インドおよび欧州（オランダ）の IT 現法の社長兼務であった。要するに世界中のビジネスプロセスを標準化しそのツールとしての IT ネットワークを整備せよということであった。

GH 氏はただ指示を出すだけではなく、各地の人事管理や問題対応でも親身に支えていただいた。毎年の予算説明でも開発計画や懸案事項などを詳しく聞き、問題解決のポイントも十分掌握して各部門へ指示を出してくれた。日本の会社ではあるが、彼のガバナンス行動は目的指向かつフラットで階層や障壁を感じさせず、スピ

ード感があった。

世界統一システムプロジェクトはIT技術者たちを大いに鼓舞し、開発は順調に進み2004年にはほぼ世界中を単一のビジネスプロセスと標準システムでカバーする体制が整った。私は南米、アフリカを含め各国を回って現地トップの支援を求めた。東京本社で開かれるエグゼクティブ会議の折には、必ず香港とインドの開発拠点にも出向き多くの技術者と話し合う機会を設けた。内部ステークホルダーエンゲージメントの一環といえる。

**【コラム】**

2001年の渡米直後、9月11日8:45世界貿易センター（WTC）の同時多発テロ事件が起こった。私はちょうど通勤中で高速道路を南下しており WTC は視野から離れていた。事務所について社員が騒いでいて初めてテロに気づいた。当時息子が日本から夏休み休暇に来ており外出する直前であった。急いで電話して外出はやめさせたのだが、自宅からは現場の黒煙が見えているとのことであった。社員の家族で一人犠牲者がでたのだが、高速道路をはじめ主要道路はほぼ閉鎖され、米人スタッフが懸命に社員の帰宅、帰宅困難者の宿泊など手配してくれた。自分は大きく迂回ルートを使って検問渋滞の中、帰宅できたのは夜中であった。実は当社の事務所はWTC1にあり慣れ親しんでいたのだが 1990 年に対岸のニュージャージ州側に移転しており 1993 年の地下爆破事件からも免れた。在米中に2回のWTCテロがあったことになる。

9/11・米国赤十字社への寄付贈呈式

### 4.3 ガバナンスの成果

世界統一システムの完成は、輸送の可視化、業務の効率化は言うまでもなく、組織にも大きな変化をもたらした。成果の一例として、各国で行っていた船積み書類の作成業務がインドと中国のドキュメンテーションセンターで集中処理可能となり、24時間体制で世界中をカバーできるようになった。今では多くのバックオフィス業務を受託するまで発展して実質社内の BPO センターとなっている。実はこの構想は1995年米国A社のコロラド州デンバーおよびフィリピン（マニラ）のドキュメンテーションセンターを見学させてもらって以来のアイデアであった。A社は統一のITネットワークを活用して世界中のドキュメンテーション業務を、遠く離れたコロラド州とマニラで処理していたのである。2017年、私はシステム監査でムンバイを訪れたことがあった。その機会に同地のドキュメンテーションセンターを訪れたが、500人を超える社員が北米、欧州、アジアなど各地の時間帯に合わせて整然と業務をこなし、休憩時間には若者が交流する姿は感慨深いものであった。

ドキュメンテーションセンターの開設準備（2005年ムンバイ）

長々と書いたが、IT は組織において多層のステークホルダー（経営陣、管理者、技術者、ユーザ、サプライヤーなど）の期待と尽力によって成り立っている。コンテナ輸送ビジネスにおける DX ともいうべき組織や IT の進化は持続しており、後年 IT ガバナンスに関わって、体系的な理論を学び、過去の経験を当てはめてみると驚くほど合致していることがわかった。

## 5．システム監査の世界へ

### 5.1　内部監査部門

61 歳で米国勤務から帰国した（2006 年 9 月）。 帰国の挨拶に行くと、担当専務が、「大変ご苦労様でした。これからもできるだけ長く会社にいて後進達を指導してください」と変なことをいう。

システムアドバイザという名目で一年ほどリハビリしていた 2007 年夏、内部監査室（現経営監査部）からオファーを受けた。専務の意図は、内部監査室のポストを用意してあるということであった。その後 13 年間にわたってシステム監査制度の導入と運用を担当することとなった。まずはシステム監査の知識が必要と考え、ISACA で CISA 資格を取得した（2008 年）。

本社のシステム部門は常々管理系システムの開発や運用に追われている。一方で、多くのグループ会社は IT 化のニーズは増えるものの本社の支援が受けられず不満を持っている。内部統制や内部監査を担当してグループが抱える IT リスクが良く分かった。内部監査部門はグループ全体を客観的に俯瞰できる立場であり、IT の問題にも切り込めるのではないかと考えた。そのためにはシステム監査の理論や実践を学ぶ必要があり、CSA 資格の認定に挑戦した（2010 年）。

本社および国内、海外の多数の関係会社はそれぞれ個別に IT を導入しており、安定運用やセキュリティ状況を把握し改善することは本社 CIO の責任であることが認識され、J-SOX に加えてシステム監査制度を導入する提案が承認された。（2009 年）

システム監査制度の導入にあたり、システム監査規程、システム監査手順、全般統制を基にしたチェックシート(COBIT ベース)、サイバーセキュリティ/標的型攻撃対策のチェックシート(経済産業省、NIST ベース)、船上サイバーセキュリティガイドライン（BIMCO 他）なども整備し、監査体制、監査内容の標準化を図った。

2018 年 3 月で退職するまでに本社 IT 部門を含め年間 3～4 社のシステム監査を実施した。日本、英国、香港、シンガポール、タイ、インド、フィリピンと範囲が広がり、様々な業種で構成するグループの IT 事情に関する視認性が大きく向上し、システム監査制度は定着した。グループの情報セキュリティ向上にも寄与したと考えている。さらに初めてグループの IT 資産、要員、費用やセキュリティ対策などの全貌が把握できた。CIO や経営陣の視点に立てば大きな収穫であったと思う。課題はこれだけの制度の運用を継承できる人材がどこまで続くかということである。

退職後も、会社の要請でグループの会社でコンサルタントを続けている。いずれも大手企業だがプロジェクト管理や品質評価の人材は手薄である。

### 5.2　システム監査基準研究会（現 IT アセスメント研究会）と ISO プロジェクト

2010 年、日本システム監査人協会へ入会し、鈴木会長（当時）にシステム監査基準研究会への参加を勧められるままに、同研究会(松枝主査)の門をたたいた。社内のシステム監査制度や内部統制制度の整備で監査・管

理基準やCOBITは利用していたし、現場でのシステム開発、運用にも詳しいのだが、システム監査の専門家の視点や実践事例を学びたい期待は前述の通りである。

監査基準研究会では、当初ISOプロジェクトの話はなかったが、2012年10月、ISOの国内小委員会メンバーであった力副会長の代理でダブリンでのSC7（当時：SC40の前身）中間会議に出てはどうかという話が持ち上がった。ISOの会議には自国の標準機関（National Board：NB）での「Expert」登録者が参加でき、私はもちろん資格はないが、力副会長の代理で参加せよという。別の懸念は勤務先が会社業務以外での出張を認めるかという点であった。幸い会社の人事部は特別休暇でどうかと助け船を出して承認してくれた。当協会の予算支援を受け、私は年二回の会議にほぼ継続して参加することとなった。正式に「Expert」になったのは2017年に情報セキュリティ大学院大学の客員研究員として、日本規格協会の「エキスパート」となってからである。

### 5.3　ISO SC40の活動

ITガバナンス標準は豪州規格AS8015:2005を基にISO/IEC 38500:2008（2015年に改定）を中心とした標準シリーズで構成されるが、その開発や改定はISO/IEC　JTC1 SC40（ITサービスマネジメントとITガバナンス）で行われる。SC40はJTC 1/WG 8, SC 7/WG 25, SC7/WG 27を母体として2013年JTC 1総会（第一合同技術委員会）で設立された。その目的は「IT ガバナンス及び IT サービスマネジメントに関する標準, ツール, 枠組み, ベストプラクティス及び関連する文書の作成を行うこと. そのIT活動領域には, 監査, デジタルフォレンジック, ガバナンス, リスクマネジメント, アウトソーシング, サービス運用及びサービス維持が含まれる」となっている。

現在はWG1（ITガバナンス）,WG2（ITサービスマネジメント、同インフラストラクチャー(旧WG4)）,WG3（ITを使ったBPO）という3つの作業グループで構成されている。

会議の構成は議長（Chair）と事務局(Manager)が総括して、作業グループ(WG's)にはそれぞれコンビナー・招集者（Convener）が任命されている。現在、議長はMs.ジャン ベッグ（豪）、事務局はMs.スバ アナンス（豪）、コンビナーはMr.レイ ウオルシー（WG1、アイルランド、2022年1月から）、Dr.スーザン D. バンホーブ（WG2、米）、榎本氏-日本IBM（WG3）である。

リスボン会議の開会式(2018年)

標準規格の開発は各WG内のプロジェクトで行われるが、それぞれのリーダーとして編集長（Editor）が当たり、各国のExpertが参加する。WG1が扱うISO/IEC 38503の開発の場合、Editorは日本の原田教授、Co-Editorに南アフリカ、インド、ポルトガル、スペインの代表が当たり、他はエキスパートとなる。私はEditorの要請によりすべての編集会議に参加した。

WG1 が扱う IT ガバナンス標準は多数あるので ISO/IEC38500 シリーズとして下図（点線内）を参照いただきたい。

WG2 は ISO/IEC 20000 - Service management 、WG3 は ISO/IEC 30105 IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes などを扱っている。

テーマによっては SC40 のみでは扱えない案件があり、他の委員会と共同で開発にあたる。

SC27:　IT セキュリティ技術

SC42:　人工知能（AI）

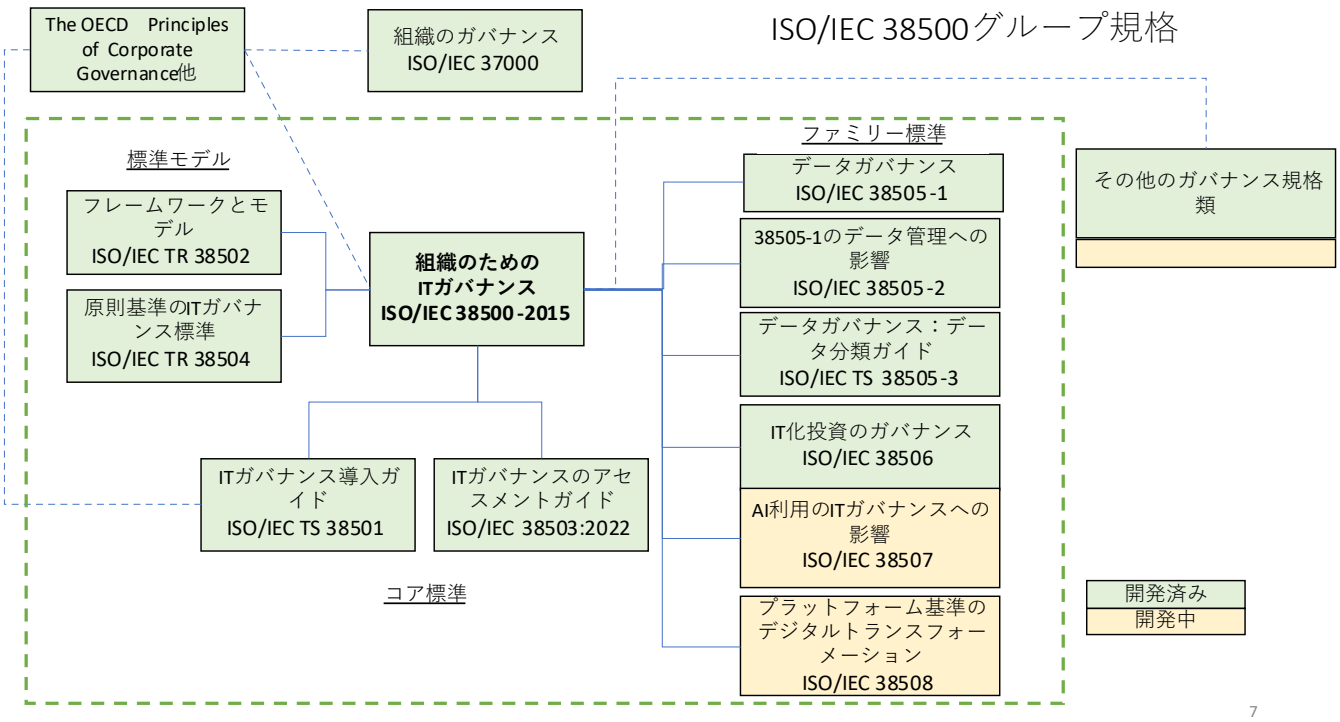
TC307:　ブロックチェーンと分散台帳技術

TC309:　組織のガバナンス

などで、SC40 はこれらの委員会とは相互に連絡役(Liaison)を任命して情報交換をしている。

日本の窓口（National Body : NB）としては SC40 委員会があり、WG1 レベルでは SC40 WG1 小委員会がある。国際標準の投票には NB が当たるため、その審議やコメントの作成は小委員会、委員会で行われる。

SC40 が扱う ISO 標準の概観は下図の通りである。（緑破線内）




TR: Technical Report(標準報告書)

TS: Technical Specification（標準仕様書）

## 5.4　ISO/IEC 38503 の開発

### 5.4.1　沿革

「IT ガバナンスのアセスメント」標準（ISO/IEC 38503）は日本が提案した標準であるが、長期にわたる開発期間を要し、3 度目の挑戦でようやく発行できた。

主な沿革は次の通りである。

2011 年頃　ISO/IEC TR 30120　“IT Audit – Guideline for Governance of IT”

(中略)

2014　　ISO/IEC PDTR 38503 “IT Governance – Assessment of Governance of IT”

2017/10　SAAJ より SC40WG1 国内委員会に参加

2017/5　岡山会議

2017/11　レドモンド会議（米国ワシントン州；新規プロジェクト方針の決定）

2018/6　リスボン会議で NWIP 承認（3 度目）

2018/11　シドニー会議

2019/6　パリ会議

2019/10　ソウル会議（以後、新型コロナのため、オンライン会議に変更）

2021/12　FDIS（Final Draft IS）承認

2022/1　ISO/IEC38503:2022　発行

当初の日本提案には「システム監査」というタイトルがついており、日本のシステム監査基準、システム管理基準を母体とした「IT ガバナンスの監査」提案となっている。諸外国の専門家からは IT ガバナンスを監査するというコンセプトの違和感、プロセスアセスメントには ISO/IEC 33000 シリーズがすでにあること、そもそも経営陣を監査する内部組織などあり得ない（韓国）など反対論が根強く、2017 年までに 2 回ほどプロジェクトは期限切れとなった。

「システム監査」を「IT アセスメント」に変更したのは 2014 年だが、文書案にはガバナンスとマネジメントが混在しているなどの理由で大幅な見直しを要請され、「IT ガバナンスのアセスメント」に収斂した。

2018 年 6 月、リスボン会議でようやく 3 度目のプロジェクトが承認された。同時に WG1 のコンビナー選挙が行われ、韓国の Dr.キムが選出された。この時点から韓国の反対論はなくなった。

### 5.4.2　編集メンバーと編集手順

別の項でも触れたが、38503 の開発に中心的に関わったメンバーは次の通りであった。

日本：　原田要之助 (情報セキュリティ大学院大学客員教授, JISC ,Editor),　松尾 正行(JISC)

南アフリカ：　Mr.マックス ブレチャー（Co-Editor, SABS)

スペイン：　Dr. カルロス フイス (バレアリス諸島大学教授)

ポルトガル：　Mr.ホセ A. コスタ(Co-Editor, リスボン大学)

インド：　Mr.サンジブ アガルワラ (Co-Editor, BIS)

メンバーは文書の各章、付属表を分担して執筆し、全員でレビュー、修正する作業であった。私は　“7 章 アセスメント活動”と“付属表; アセスメント フレームワーク”を担当した。実は付属表が最も分量が多く、当初日本が提案した部分が中心となっていた。とはいえ。文書は全員参加で完成したものであった。

編集会議は英語ネイティブのマックス(南アフリカ)が進行役を勤めることが多く、会議の効率化に貢献大であった。彼は ISO/IEC TS38501 開発のキーマンでコンサル会社の創業者、セミナーでの講演も多い。2012 年のダブリン会議以来の“盟友”でもある。 ホセは WG1 のセクレタリーも務め、ブラジルをはじめ出張が多く

エネルギッシュで日本大好き人間、カルロスは自分の勤める大学の IT ガバナンス実践の事例論文を提供してくれたので邦訳して IT アセスメント研で共有した。サンジブは博士論文挑戦中のコンサルタントで、分析力、聡明さにはいつも感心させられる。

他にも節目で助言をしてくれた方々がいる。ISO に限らず ISACA や他団体でも著名な人々である。

オーストラリア： Mr.マックス シャナハン、Mr.ジェフ クラーク (SA)

デンマーク： Ms.カレン L. ロウリツセン（SC40 Secretary）

カナダ： Mr.ジョン ソープ、Mr.ジョン ウォン (SCC)

韓国： Dr.グエン-ミン キム (梨花女子大学校教授, WG1 Convener): 2021 年 12 月まで。

ISO/IEC 38503 の開発（2018 年以降）にあたって、賛否投票とともに各国から出されたコメント総数は 563 件に上り、Editor を中心として編集会議で個別に審査して採否をきめ、CRM（コメント処理会議：各国代表参加）で討議・決定する。担当者は採択されたコメントを反映して文書を改訂して次のステップに進み投票にかける。編集会議では最初の WD 文書の作成から始まり、各段階でコメントを反映した文書を作成するため膨大な作業と会議をこなす必要があった。このような手順の繰り返しにより当初 3 年間の予定は一年延びて 4 年間のプロジェクトとなり、サンジブの集計によると編集会議は 111 回に及んだ。会議は主としてオンラインで開催した。時差があるため、深夜、早朝の会議も避けられなかった。年２回ほどあったオンサイト会議は重要な進展の機会であったが、コロナ禍ですべてオンライン会議を余儀なくされたのが残念であった。

| ステップ | コメント数 | 時期 | 文書のレベル |
|---|---|---|---|
| WD： | 220 | 2018/7 | エキスパートレベルの作業文書（Working Draft） |
| CD： | 152 | 2019/5 | 委員会レベルの公式文書（Committee Draft） |
| CD2： | 123 | 2020/5 | 同上（第二版） |
| DIS： | 65 | 2021/5 | 国際標準のドラフト（Draft International Standard） |
| FDIS： | 3 | 2021/12 | 国際標準の最終ドラフト（Final DIS） |
| IS： | - | 2022/1 | 国際標準完成版発行（International Standard） |

WD、CD は SC40 事務局が管理するが、DIS 以降の文書・コメントは ISO 中央事務局（Central Secretary：スイス）の管理となり、中央事務局がコメントを出す場合もある。コメントには 3 種類ある。

GE　一般：　文書全般の内容や構成

ED　編集：　文法、用語など

TE　技術：　モデル、フレームワーク、記述等技術的コメント

GE と TE は標準規格の本質に関わることが多く、編集会議、各国 NB を交えた CRM などで議論が集中するので、編集チームにはそれをまとめる見識と準備作業が必要である。

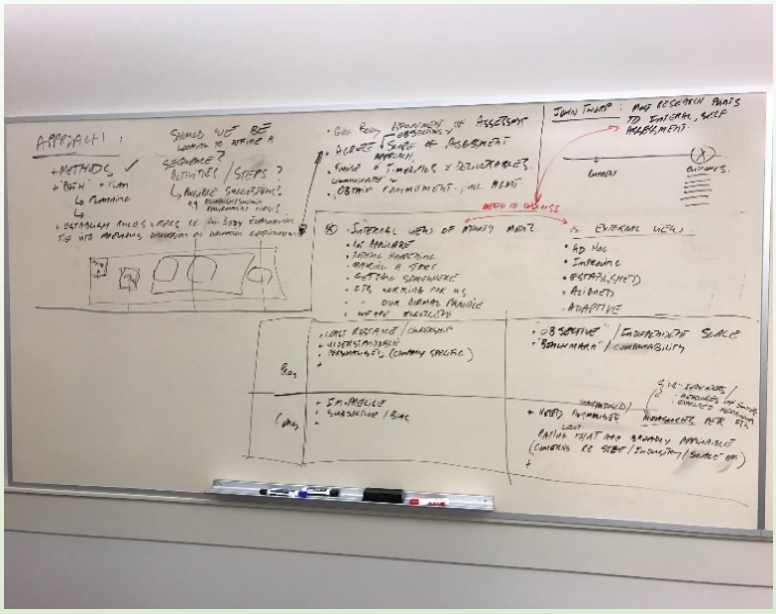
ISO の活動、委員会の設置、文書の構成、用語の使用法、図式の構成など多岐にわたる方針を定めた標準ルールとなる専門業務用指針（Directives）が準備されている。すべての標準文書が整然と作成されるためのルールで、意見が分かれた場合などに参照する機会が少なからずあった。

SAAJ が 2020 年 6 月発行した「情報システム監査実践マニュアル(第 3 版)」第 3 部 “IT ガバナンスにおけるアセスメントのポイント”に IT ガバナンス制度の導入サイクル、アセスメントの手法、具体的なフレームワーク（別表）などを詳しく記載している。ISO/IEC 38503:2022 は 2022 年 1 月に正式発行されたので、そちらと合わせて利用いただきい。また、38503 の JIS 化計画も進められている。

【コラム】

写真はマイクロソフト本社(レドモンド)で WD を議論したときのものである。会議室の壁全体が白板に囲まれており、ホワイトボードに向かって議論をまとめていくことは、いずこも同じである

一週間の会期中、ソーシャルアクティビティと称して一度は合同の夕食会、飲み会がある。岡山会議では岡山市による神楽のパフォーマンス付きの夕食会、レドモンドでは MS キャンパスのキャンティーンでの飲み会、リスボンは老舗ホテル最上階から旧市街とテージョ河畔を見ながらの夕食会、シドニーでは SA 主催のカクテルパーティやロック歴史地区での飲み会、パリでは AFNOR 招待で「ワイン博物館」の地下レストランでの夕食会、ソウルでは JS ホテルでの夕食会など多彩である。多くは自己負担だが、皆で無礼講の話ができる貴重な機会であり、出張中の僅かな楽しみでもある。



### 5.5 IT ガバナンスをめぐる新しい取り組み

ISO/IEC 38500:2015 シリーズの在り方を検討するため、SC40 はアドホック会議を編成し一年かけて現状分析、今後の方向性の調査検討を行い、報告書を提出した。2020 年 5 月に出された最終報告によると ISO にはガバナンスを扱う委員会が 10，ガバナンスをテーマにするプロジェクトが 15 あることが判明した。これらは相互に整合がとられているものと、いないものが混在している。

38500 改定プロジェクトは 2020 年に SC40 内に編成され、3 年かけて新標準 ISO/IEC 38500:202x を発行すべく活動している。日本も SC40WG1 小委員会を中心として参加しており、私も継続して会議に参加している。

#### 5.5.1 プロジェクトの方針

SC 40/WG 1 が活動の中心(The centre of excellence)となり、IT、データ、デジタル能力の責任ある戦略的利用のためのガバナンスの決定的な知識源となる。

1. インプット
   - 「デジタルトランスフォーメーションと新しいデジタルリアリティに関するJTC 1/SC 40 WG 1 AHGの報告書」改善の機会
   - JETI（JTC 1 Emerging Technology and Innovation advisory group）の2019年報告書で概説された技術から表面化する可能性のあるガバナンスの意味合い
   - 他の新興技術諮問グループ及びリエゾンからの報告書
   - ガバナンスの側面を扱うISO/TC 309などの他のISO技術委員会
2. プロジェクト日程（現状）
   - 2020年11月：第1回WG会合：以後一年間毎月一回(2時間程度)のZoom会議
   - 2021年3月：最初のWD発行
   - 2022年2月：CD投票で可決
   - 2023年3月：DIS提出発行　予定

2022年3月現在では、CD投票で提起された379件のコメント・意見に対する各国の見解を整理中で、CRMを通じて、CD文書の改訂が行われる見込みである。

### 5.5.2 改定のポイント

SC40/WG1は前項のインプットに掲げた報告書および各国エキスパートの意見を集約して、改定の方向性を取りまとめた。主なポイントは次の通りである。

1. デジタル革命
   - サプライチェーンとのシームレスな統合や顧客との関わり。クラウドなどIT サービスベースの仕組みの変化。
   - 顧客とテクノロジーを通じた円滑なインターフェース、エコシステム。
2. データ
   - データはすべてのレベルで意思決定のために組織内で使用される。
   - 組織が収集、生成、取得したデータは、その製品やサービスだけでなく、サプライヤー、顧客、規制当局など、組織の外でも利用される。
3. 新常態
   - ビッグデータ・アナリティクス、ブロックチェーン、人工知能などの新しいテクノロジー
   - テクノロジーのビジネスへの応用が常態化する
4. 新しいガバナンスモデル
   - 単一組織のガバナンス　->ネットワークガバナンスモデル、意思決定自動化のガバナンス
   - プライバシー、セキュリティ、データと技術の責任ある使用に関する説明責任
5. 組織の変革
   - ガバナンス、リーダシップ、マネジメントのための役割、システム、プロセスの見直し
   - ステークホルダーの期待の変化とエコシステム
   - ISO-37000（組織のガバナンス）との整合

6. 原則（プリンシプル）セットの見直し

・ デジタル革命、データガバナンスを包含し、組織のガバナンスとの調和した原則セット

### 5.5.3 他の標準への影響

「ISO/IEC 38500 グループ規格」図に示した通り、38500 ファミリーには多くの標準が関連している。38500 の改定はそれらにも影響する。標準モデル（TR38502、TR38504）、コア標準（TS38501、38503）は直接影響を受けることとなり、38500:202x 発行後に順次改定する見込みである。その他ファミリー標準（38505、38506、38507、38508）は比較的新しいものであるが、影響の度合いによっては改定が必要となる。

## 6. おわりに

大変冗長な話にお付き合いいただきありがとうございました。海運会社のシステム開発の現場から CSA や ISO の世界に入った私の経験や取り組みを紹介しましたが、業種の違いはあれ類似の経験をしてきた方は多いと思う。システム監査の方向性も、従来型のシステム監査から IT ガバナンスの世界へと広がり、さらにその実践へと向かっている。ISO など世界のエキスパートと交流の機会もぐっと近づいてきた。本稿が少しでも CSA や CSA を目指す方々の参考になれば幸甚だし、IT アセスメント研究会の活動に参加いただき共同研究ができれば更なる喜びである。

完