

〔研究論文〕

第4次産業革命における情報化実践と監査

Information Systems Practices and Audit for the Industry 4.0

成田 和弘
Kazuhiro Narita

概要

「第4次産業革命」がビジネス環境を劇的に変化させている。生産性が先進国中最低水準まで落ち込んでいる我が国にとって、これをリードし、勝ち残ることは喫緊の課題である。「第4次産業革命」では、自律的にかつ相互に連携した Cyber Physical Systems（以下「CPS」という）が、「人に代わって働く」。そして CPS による IT サービスは「商品」として顧客に提供される。組織は激しい環境変化の中で、「顧客満足」を創出する新たな IT サービスを「安心安全」とともに提供し、迅速かつ継続的に改善し、維持し続けなければならない。この課題解決のヒントは、「アジャイル開発」にある。難易度の高い開発手法であるが、リスクを最小にしながら、「迅速」、「高品質」で「柔軟性」のあるソフトウェア開発と「イノベーション」を可能にする。組織が国際競争力のある IT サービスを生み出すためには、この「イノベーション」と「安心と安全」、そして、その担い手である組織の信用が必要である。システム監査人は、「アジャイル開発」の精神と「安心と安全を作り込む技術」を十分理解し、「独立した専門家」としての評価を通じ、組織の信用の確立を効果的に支援することで、第4次産業革命における情報化実践に貢献することができる。

キーワード：第4次産業革命、Cyber Physical Systems、イノベーション、アジャイル開発、安心と安全、アシュアランスケース、ディペンダビリティ

1. はじめに

「第4次産業革命」における勝ち残りは、他に見えない少子高齢化社会を迎える我が国にとって喫緊の課題である。本稿では、「第4次産業革命」において必要となる情報システムの要件と我が国の課題、その担い手となる IT 人材の状況と組織の在り方を踏まえ、IT サービスの「イノベーション」と「安心と安全」の必要性およびその実践と、システム監査人が取り組むべき課題について考察する。

2. 第4次産業革命と日本の課題

(1) 第4次産業革命と Cyber Physical Systems

ドイツの「インダストリー 4.0」、米国の「先進

製造パートナーシップ」、中国の「中国製造 2025」等、「第4次産業革命」への取り組みを各国が競っており、我が国も「Society 5.0」を推進している。「インダストリー 4.0」では、自律的な情報交換により起動し、互いに独立して制御されるスマートマシン、ストレージシステム、および生産設備で構成された、Cyber Physical Systems（以下「CPS」という）により、製造、エンジニアリング、原材料、サプライチェーンおよびライフサイクル管理に関わる産業プロセスを根本から変えるとしている¹⁾。さらに、今日は生産技術そのものだけでなく、遺伝子配列解析、ナノテクノロジー、再生可能エネルギー、量子コンピュータ等、複数の分野で新しい技術的なブレークスルーが起こっており、これらのテクノロジーが融合し、

投稿受理日	2017年3月31日
再投稿受理日	2017年10月10日
再々投稿受理日	2017年12月27日
査読完了日	2018年1月10日

相互作用を起こし、変化はさらに加速している^[2]。CPSは「人に代わって機械が働く」ため、信頼性の高い品質による「安心と安全」が必要である。さらに「自動運転」や「スマートハウス」のように、ITサービス自体が顧客に提供される「商品」でもあるため、適時に市場に投入できる「迅速さ」と、加速する変化のなかで顧客満足を維持し続ける「柔軟性」も必要となる。

(2) 20年前より低い日本の生産性

図1で示す通り日本の一人当たりGDPは他国に比較し長期に停滞しており、先進国最低水準となった。各国の生産性が向上する中、日本だけが「低下」している。「立派なインターネット通信のインフラを作りながら、規制緩和の遅れが、産業構造自体への影響につながった」^[3]との指摘や、産業別のICT（Information and Communication Technology：情報通信技術）投資の経済成長への寄与度の分析に基づく、「非製造業を中心に、ICT投資をしないためにICT革命の果実が得られないという当然のことが起きた」^[4]との指摘がある。2008年のリーマンショック以降、世界の人々が互いに助け合い知恵を出し合う「共創」を重視する経済活動へと軸足が移りつつあるにもかかわらず、構造化主義の罠にはまったまま、論理分析過多、経営計画過多、コンプライアンス過多に陥ったままであることが、企業の経営力の喪失につながっているとの指摘^[5]は特に重要である。「共創（co-creation：共同による創造）」には他者に依存する不確実性があり、新しい技術の活用には「試行錯誤」も必要である。経営は必ずしも思惑どお

りに進むものではないことが前提であり、過度に詳細な報告や説明ばかりを求めるような「過剰管理」や当初計画に過度にこだわる「予定調和」に陥っているのは、「共創」や新しい技術の活用による成長は難しい。

(3) 日本のソフトウェア開発力と人材マーケット

日本ではIT企業以外の組織に所属しているIT技術者は28%しかいない。米国の65%、ドイツの61%等、他の先進諸国において半分以上のIT技術者がIT企業以外の組織に所属しているのに比べて特異な状況である。また、米国のプログラマの年収が他の職業の平均年収の174.6%に達するのに対し、日本のプログラマの年収は83.5%である^[6]。これは日本のソフトウェア開発の中心が請負契約による外部委託となっており、その下で多重下請けが行われてきたことが影響している。請負契約は固定価格契約のため委託側の予算管理は容易であるが、受託側は「要件の追加・変更」には対応しない方が得になり、プロジェクトの途中で発見された新しいニーズは、当初の約束に反するものとして嫌われ、「共創」となりにくい。さらに、多重下請けによる価格競争が「人月単価」の低下圧力となっている。優秀な人材を獲得し、国際競争に打ち勝つためには人材マーケットを整備し、グローバルに通用する水準の優秀な人材を新しいサービスを生み出すソフトウェア開発のために投入できるよう、改めなければならない。情報システムの開発力は「IT技術者の質」で決まる。米国では、雇用統計が整備されており、どのような種類のIT技術者が何人いて、どの程度報酬を

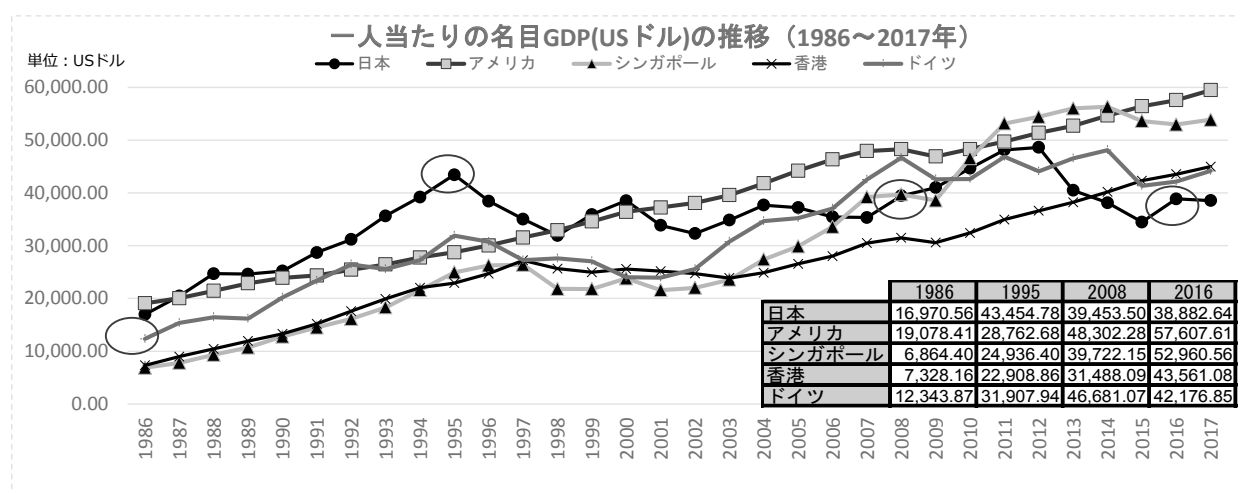


図1 一人当たり名目GDP推移

【出典】世界経済のネタ帳

http://ecodb.net/exec/trans_image.php?type=WEO&d=NGDPDPC&c1=US&c2=JP&c3=SG&c4=HK&c5=DE&s=1986&e=2017 (参照 2017/9/21)

得ているかがインターネットで開示されている^[7]が、日本の「雇用動向調査」には、性別と就業形態（一般労働者、パートタイム労働者）と雇用形態（雇用期間の定めのあるなし）の区分しかなく、自国のIT技術者の公式な統計はない。技術者が適正な報酬で処遇される人材マーケットを整備し、タイムアンドマテリアル契約（技術者の時間単価等を決め、実績により支払う契約）の採用等、組織とIT技術者および外部委託先との関係の見直しが必要である。

3. ソフトウェア開発の生産性向上とイノベーションのテクノロジー

（1）計画駆動ソフトウェア開発の問題

図2に示すとおり、ソフトウェア開発において「取得される要件の質」は、プロジェクトが進むにつれて高まり、特に実際のアウトプットを確認できる「テスト」によって大きく向上する。しかし、計画駆動開発では、開発メンバーのプロダクトに対する知識が不十分な初期の「分析」時に要件をたくさん集めて計画を策定し、以後はその初期の計画に合うように開発を進めるため、環境の変化による当初計画との不整合や収束しない要件変更悩まされる。特に新商品の開発には試行錯誤からのフィードバックが必要であり、ITサービス自体を「商品」として顧客に提供しようという組織には不向きといえる。この計画駆動開発が、日本のソフトウェア開発の96.8%を占めている^[8]。

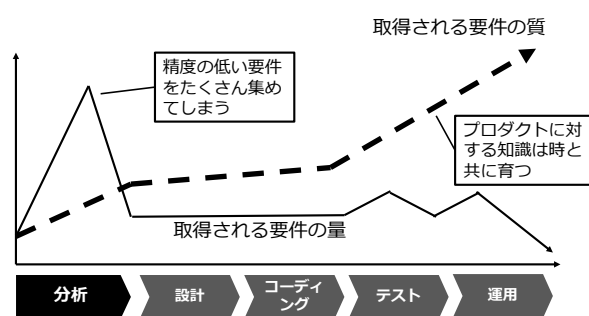


図2 要件の取得タイミングと質

【出典】Kenneth S. Rubin, エssenシャルスクラム (kindle 版), 翔泳社 2014, 位置 No.1718 図 3.7 より

（2）日本の製造業の優れた文化を受け継ぐアジャイル開発手法

アジャイル開発は、さまざまなフレームワークとメソッドをカバーする包括的な用語である。リーン開発、カンバン、XP、スクラム、スクラ

ムバン等の種々の手法があるが、これらの手法は「個人と対話」、「動くソフトウェア」、「顧客との協調」、「変化への対応」を重視する共通の理念を持つ^[9]。

日本ではあまり普及の進んでいないアジャイル開発手法であるが、グローバルでは急速に普及が進んでおり、図3に示す通り既に71%の組織が「ときどき」以上の頻度でアジャイル開発手法を使用している^[10]。

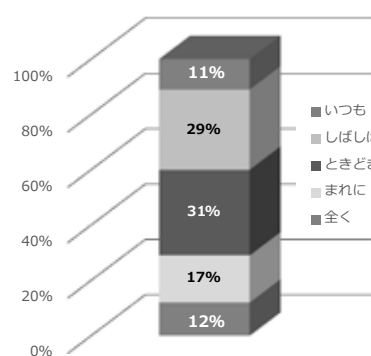


図3 アジャイル開発の動向

【出典】Project Management Institute, Success Rate Rise, 2017.

米国では80年代後半に、安くて高品質な日本車へ危機感を抱き、その技術を徹底的に研究してきた。アジャイル開発手法のベースとなっている「リーン開発」は「リーン生産方式」や「ジャストインタイム」といった「トヨタ生産方式」の技術をソフトウェア開発に応用したものである。①無駄をなくす、②品質を作りこむ、③知識を作り出す、④決定を遅らせる（ジャストインタイム）、⑤早く提供する、⑥人を尊重する、⑦全体を最適化する、の7つの原則^[11]に基づき、短納期かつ高品質な柔軟性のあるソフトウェア開発を可能としている。「無駄」は、「顧客に対する価値を付加しないもの、なくても何とかなるもの」と定義され、「未完成の作業」「余分なプロセス」「余分な機能」「タスクの切り替え」「待ち」「移動」「欠陥」「管理作業」の徹底的な削減を図り、短納期での開発を実現する。また、「イテレーション（固定した短い期間で動作する製品を作成、関係者との良好なコミュニケーションと良質なフィードバックの反映を繰り返す技法）」のほか「5S」「標準化」「ペアプログラミング（2人がペアで行うことで、プログラミングと同時並行でレビューを行う技法）」「ポカヨケのためのビルド、リリース、インストールの自動化」、「テスト駆動開発（仕様書からテストケースを作成するのではなく、仕様書と

しても十分なテストケースを準備する技法)」等の品質向上施策を駆使し、「品質」を徹底的に作りこむ。「柔軟性」は「決定を遅らせる」ことで実現する。これは自動車の金型製造において、厳密に仕様を決め厳格に変更管理をしたデトロイト方式では変更コストが大きかったのに対し、とりあえず作り始めるが、最終確定はなるべく後にして変更を取り込みながら作業する日本式のほうが低コストだったことを応用したものである。ソフトウェア開発においては、「モジュール化」「API化」「パラメタ化」「抽象化」「カスタムツールや重複の回避」「関心の分離」「バリエーションのカプセル化」「将来機能や余分な機能は作らない」ことを徹底してビジネスの変更に合わせ「決定を遅らせる」ことの影響を小さくする。

(3) スクラム開発とイノベーション

スクラム開発は、複雑で変化の激しい問題に対応し、価値の高いプロダクトを生産的かつ創造的に届けるための手法である^[12]。分野横断チームが協働し、フェーズをオーバーラップして進めるホンダとキャノンの新製品開発チームの手法をラグビーにたとえてスクラムと呼び^[13]、それをソフトウェア開発に応用したことに由来する^[14]。スクラム開発の工程を図4で示す。開発は固定の短期間で「インクリメント（動作する成果物）」を作成するスプリントを繰り返す。インクリメントから得られたフィードバックに対し、次のスプリントで「適応」しながら進められる。スプリントは、「プロダクトオーナー（開発するインクリメントの選定権を持つユーザ）」、「スクラムマスター（スクラムの運営管理者）」、「開発者」が同じ場所に集まって行われ、この三者が分析・設計・構築・結合・テストの一連の開発プロセスを一体となって実施する。

イノベーションとは「知識を新たに作り出すプロセスそのもの」であり、「形式知（客観的で言語化された理性的な知）と暗黙知（主観的で身体的な経験から得られる知）の相互変換 (SECI モデル)」「人と人が文脈を共有し、相互にありのままの他者をそのまま丸ごと受け容れ合う関係ができるところ（場）」「善い目的、直観能力で場を作り、組織すること（知創リーダーシップ）」「オープン・イノベーション（共創）」「スピードと持続性（実践力）」を必要とする^[15]。スクラム開発は、「経験的プロセス制御（経験主義）」を採用し、利用可能な成果物を「SECI モデル」に従って反復的かつ漸進的に作成する。そして、以下の通りイノベーションの手法があらかじめビルトインされている。

スクラムチームは、コマンド&コントロールの従来型の管理ではなく、人と人が文脈を共有し、実践する「場」として運営される。「スクラムマスター」が、メンバーが成果を上げるために支援や奉仕をする「サーバントリーダー」として「知創リーダーシップ」を担う。さらにビジネスサイドが開発チームの作業とプロダクトの価値の最大化に責任を持つ「プロダクトオーナー」として参加し、開発者とイノベーションを「共創」する。

スクラム開発チームは自己組織化され、自ら考え、自ら学び、自ら工夫して成果物を作成する。このため、スクラムの開発チームメンバーには、

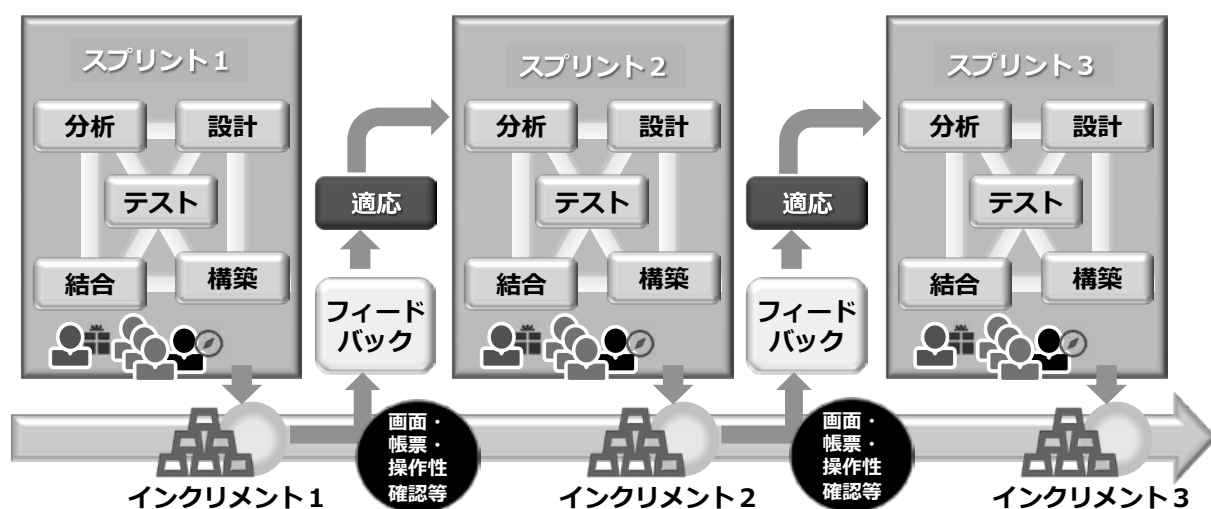


図4 スクラム開発の工程

【出典】Kenneth S. Rubin, エッセンシャルスクラム (kindle 版), 翔泳社 2014, 位置 No.1610 図 3.4 を参考に作成

1-4週間の限られたスプリント期間内に自ら答えを出す、高い「実践力」が必要とされる^[16]。スクラムによる開発は、動作する成果物に対するプロダクトオーナーとの合意を反復し、漸進的に進める。改良が必要なものは次のスプリントでレベルアップされるため、試行錯誤により得た知識を反映した開発が可能となるのである。なお、スクラムは3-9人の開発者を前提とした手法であるが、大規模開発向けに並行スプリントを行う、エンタープライズ・アジャイル手法もある。

現在実施されているアジャイル開発の76%をこのスクラム（スクラム58%、スクラム/XPハイブリッド10%、スクラムバン8%）が占めており^[17]、「トヨタ生産方式」と「SECIモデル」を応用したスクラム開発は、ソフトウェア開発手法のグローバルスタンダードとなっている。

4. 繋がるシステムとその安全と安心のテクノロジー

（1）ディペンダビリティとアシュアランスケース

システムが提供するサービスを利用者が安心して継続的に利用するために、システムが備えるべき能力を総合してディペンダビリティ（Dependability）といい、機器やシステムの安全性やディペンダビリティについて、論理的かつ事実に基づいたエビデンスで説明する枠組みをアシュアランスケース（Assurance Case）という。航空、鉄道、軍事、自動車、医療機器などクリティカルな領域ではこのアシュアランスケースの確立を求める規格やガイドラインの整備が進んでいる^[18]。

システムや機器の誤りや故障はゼロにならない。クリティカルなCPSでは、そのような場合でも人の命や環境に重大な影響を与えないようなセーフティ（Safety）が必要である。事故が潜在する具体的状況であるハザード（hazard）の特定と分析を行い、その低減策を作り込むのである。CPSでは、個々の機器やシステムの安全安心の設計・評価に加え、つながった場合でも安全安心を維持できる設計・評価を行い、システム全体の安全安心を高めること、さらに、その設計内容や条件を利用側に分かりやすく伝えることが必要である。ハザードの影響を分析・評価し、対策の優先順位を明確化するため、過酷度（被害の深刻さ）、発生頻度、回避可能性のマトリクスでリスク指標を決定する。リスクの高いハザードについては、厳格な品質管理策が要求されることになる。他のシステム等から期待した情報が得られなかった場

合の振る舞いのなかから、コンポーネント間でやり取りされる「コントロールアクション（コマンド）」毎にハザードを洗い出し、発生しうるアクシデントとアクシデントを防止するための安全制約を分析するSTAMP（System Theoretic Accident Model and Processes）/STPA（System Theoretic Process Analysis）という手法がある。アシュアランスケースは、このような対策状況を説明できるようにするため、要件と対応するシステム機能のテスト結果をエビデンスとして可視化し、システムの妥当性を客観的に論証できるようにする。具体的手法として、IPA/SECが策定し、OMGの国際標準規格として認定された「Dependability Assurance Framework for Safety-Sensitive Consumer Devices (DAF)」^[19]や「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」（DEOSプロジェクト）の成果で、The Open Groupの「Dependability through Assuredness (O-DA) Framework」として採用されたD-Case等があり、いずれも日本発の技術である。

（2）高まるサイバーリスクとセキュリティ対策

ウクライナ変電所への不正侵入による大規模停電等、重要インフラに対するサイバー攻撃が世界的に深刻になっている。2015年の日本年金機構等、情報の窃取も続いており、サイバー犯罪の検挙件数、相談件数も増加している^[20]。このサイバーリスクは発生確率が極めて高く、かつ大きな損害をもたらす厄介なリスクである。特に日本では、従業員による内部不正の可能性は低いという性善説前提のもと、システムによる不正監視よりも人手による管理に頼ってきた。年金機構では、ネットワークは内閣サイバーセキュリティセンターが監視し、不信な通信を検知し、マルウェアまで解析していたにもかかわらず、人手で管理していた重要なデータが窃取され、守り切れなかった。サイバー攻撃はシステムを使用して組織的かつ網羅的に脆弱性を攻撃し、内部に侵入する。年金機構事案は、これまでの「性善説」前提の人手による情報セキュリティが、サイバー攻撃に対して役に立たないことを示した。CPSも同じリスクにさらされている。

（3）NISTのサイバーセキュリティフレームワークとFedRAMP

攻撃者はセキュリティの弱い組織を踏み台にして攻撃を行うため、サイバーセキュリティは、社

会全体で対策する必要がある。米国ではNIST (National Institute of Standards and Technology：米国標準技術局) により業界ベストプラクティス等をもとにした「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」が策定されている。これにより中小企業であっても重要インフラのベストプラクティスを参考に、自らのセキュリティ対策を進めることができる。さらに、政府のクラウド調達のために設立された組織であるFedRAMP (The Federal Risk and Authorization Management Program：連邦リスクおよび許可検査プログラム) が、連邦政府組織間でセキュリティ評価を相互運用することによるコスト削減と業務効率化、リアルタイムでのセキュリティの可視化、一貫したマネジメント手法の適用、連邦政府とクラウド業者間の透明性の向上に取り組んでいる。各省庁は原則として他省庁と共用することを前提にシステムを構築することになっており、高いセキュリティが要求されるFedRAMPの認証を得たセキュアなサービスを、他省庁も使うことで全体のセキュリティ向上とコスト削減が両立できる。米国の調達基準のセキュリティベースライン (NIST SP800-53-r4)^[21]のレベルは高く、規定する管理項目は、ISMS (ISO/IEC27001・27002) の管理項目を網羅し、かつより具体的で、さらに多数の項目が上乘せされたものとなっている。FedRAMPはこれらのセキュリティを紙に書いたルールではなく、FedRAMPの認証を受けた「動くシステムそのもの」で共有する仕組みであるといえる。サイバー攻撃の攻撃者は、攻撃システムを使って網羅的に脆弱性を検索し、少しでも隙があれば侵入してくる。システムの調達においては、組織の規模に関わらず関係者全体で高いレベルの対策が必要になるので、ベースラインの高いセキュリティを共用することは合理的である。

(4) 社会の効率を高めるクラウドによるソフトウェア資産の共用

サプライチェーンを構成する中小企業が、個々に前述のような高いレベルのセキュリティ対策を行って、さらに個別に継続的にレベルアップを図っていくのは現実的でない。サプライチェーン全体をサイバーリスクから守るためには、米国のFedRAMPのように高いセキュリティを備えた「動くシステム」をクラウドで共用することで、全体として対策していくのが効果的であると考え

られる。文書管理やメールシステム、人事給与・会計システムや、インフラシステム等のような共通機能を個別に開発し、それぞれに独自のセキュリティ機能を開発するのではなく、高いセキュリティを備えた共通機能や基盤システムを提供する「中小企業クラウド」のようなもので安全を安く使えるようにし、個々の組織が、独自に提供するシステムのセキュリティ確保にだけ集中することができれば極めて効率的に新しいビジネスが進められるようになる。

クラウドのセキュリティと活用はここ数年で目覚ましく発展し、例えばAWS(Amazon Web Service：アマゾンウェブサービス) では、「NIST Compliance on AWS」という、米国調達基準のベースライン管理策を予め組み込んだ30分でインストール可能なテンプレートが用意され、AWSの利用者はだれでも使用できる^[22]。さらに、ハードウェア等の稼働環境を仮想化する「コンテナ」技術が注目を浴びている。これらはアプリケーションの可搬性を格段に向上させ、ソフトウェアの共用による大幅なコスト削減を可能にする。日本の企業の99.7%は中小企業である^[23]。新しいビジネスは必ずこれら中小企業のなかから起こる。中小企業が未来を切り開く新しいITサービスに取り組み易くすることが、日本が「第4次産業革命」に勝ち残るための、最も大きなポイントであると考えている。すでに多くのスタートアップがクラウドを利用している。クラウドサービスには、まだ未熟な点があり、データセンターのリスクや能力の開示や改善など、さらなるレベルアップが必要であるが、ソフトウェア資産を共用し、社会の効率を高める「第4次産業革命」ためのインフラとして必要不可欠のものになる。

5. つながるシステムを提供する組織の信頼

(1) 組織に透明性を提供するフレームワークと三線防御モデル

「内部統制の統合的フレームワーク」は、組織の経営上の意思決定及びガバナンスを支える内部統制システムの「透明性」のために2013年に改訂された。「ガバナンス監督に関する期待」「市場と業務の国際化」「ビジネスの変化と複雑性の増大」「法律、規則、規制および基準への要請とそれらの複雑性」「業務遂行能力および説明責任に対する期待」「進展するテクノロジーの利用とそれへの依存」「不正の防止と摘発に関する期待」

の7つの環境変化が反映された17の原則が示され、特に、「統制活動」に関する3つの原則では、より強力な統制手段である情報システムを活用した統制を適切に実施する必要性が明確にされた。また、三線防御の考え方が明示され、第一線の事業ユニットは、リスクを取ることも含め、個別のリスクをリアルタイムに管理する責任と説明義務を負い、第二線の間接管理部門は、リスク管理の戦略、方針、手続きにより全体のリスクを網羅的な管理を担うことでこれを支援し、監査は「リスクベースで独立した評価・保証を行う^[24]」ことでこれを説明可能にするとされ、内部統制における監査の役割も明確化された。三線防御は、二線と三線の適切な支援により現場を強くする、リスク管理の考え方である。実際のリスクが発現したときに第一線で守れなければ、二線、三線が発見しても当該リスクに対しては事後的な対応しか行えない。この枠組みに、前述のアシュアランスケースの考え方を取り入れ、リスクへの対応を「可視化し、客観的に論証できるように」一線から三線まで共有することで、透明性の高い「信用できる組織」が効率的に実現できるようになると考える。

この「内部統制の統合的フレームワーク」は組織のガバナンスのためのデファクトスタンダードである。「誠実性」「透明性」「説明責任」が組織に対する利害関係者の期待であり、7つの環境変化は我が国が「第4次産業革命」で勝ち残るために取り組まなければならない課題そのものである。最近の日本の企業の事例にみられるように、根拠の希薄な目標に固執し、その達成を迫る「過剰管理」と「予定調和」は不正の呼び水にもなりうる。隠し事の無い「透明な組織」の確立は、効率的な内部統制による「市場と業務の国際化」「ビジネスの変化と複雑性の増大」「法律、規則、規制および基準への要請とそれらの複雑性」への迅速な対応を可能にし、第4次産業に向けた「進展するテクノロジーの利用」を促進すると考えられる。

(2) ガバナンスとマネジメントの見える化

BSC (Balanced Scorecard: バランスド・スコアカード) は、「財務的視点」に、「顧客の視点」、「社内ビジネスプロセスの視点」、「イノベーションと学習の視点」を加えた、「業績評価システム」である。BSCは新しい戦略を効果的に導入することにも用い、①エグゼクティブのリーダーシップを通じて変革を促す。②戦略を現場の言葉に置き

換える。③組織の戦略へのアラインメント。④戦略を全社員の業績に関係させて動機づける。⑤戦略を継続的なプロセスにさせるべく管理する。の5つの原則が提唱されている。「品質」「タイミング」「納期」等の組織間での業績を測定するための「サプライヤー・スコアカード」や、サプライチェーン全体の「サプライチェーン・スコアカード」、特定の顧客との「顧客スコアカード」、業務提携における「アライアンス・スコアカード」を策定し、組織を越えて戦略を共有している事例もある^[25]。戦略マップはBSCの多数の複雑に連動する尺度を、企業やその従業員が理解できるよう「戦略目標がどのように統合し結びつくのかについての1枚に収めた概念図」である。この戦略マップは、アジャイル開発チームなど、既存の職務分掌になじまない組織内外の関係者と戦略・方針・目標と、顧客価値を獲得するシナリオおよびその役割分担を共有するために役立つ。投資家向けに公開して経営の透明性を高めた先進事例もあり、CPSに関連する組織同士が「サプライチェーン・スコアカード」を戦略マップで表現することで目標を効果的に共有し、さらにこれを公開して、サプライチェーン全体の「透明性」の説明に活用する等、組織が共創を重視した経済活動を行っていくための有力なツールであると考えられる。

6. これからの監査

(1) イノベーションとアジャイル開発の監査

「内部監査の使命」は、「リスクベースで、客観的なアシュアランス、アドバイス、見識を提供することにより、組織体の価値を高め、保全する」と定義されている^[26]。ガバナンスの目的は、企業戦略・方針と整合したIT戦略・方針の維持である。激しい環境変化の中で、「顧客満足」を創出し、迅速かつ継続的に改善していくためには、イノベーションやアジャイル開発を行うチームの、知的生産性を高め、イノベーションの機会を広げ、力付けなければならない。この目的の達成を阻害するものがリスクである。

アジャイルでの考え方では、チームはお互いを信頼し、尊敬する。ガバナンスも「指示」ではなく、「方向付け」の姿勢が重要である。イノベーションやアジャイル開発チームとはコマンド&コントロールではなく、イネーブル(enable)と動機付け(motivate)によるコミュニケーションをしなければならない。ガバナンス戦略やそのガイダンス

もチームと協調して作るべきものなのである^[27]。

監査は、自己完結性の高いイノベーションやアジャイル開発を行うチームの「透明性」に「説明性」を提供する。アジャイル開発においても、組織として透明性を説明可能にしておくことは重要であり、法規制対応の上で必要な場合も多い。第二線のリスク管理部署は、開発チームの効率を損なわないよう、メトリクスを可能な限り自動収集して第一線をモニタリングする。第三線の監査は、開発チームと合意している監査プロセスを使用し、計画的かつリスクベースで、一線のリスク対応の状況と二線によるそのモニタリングの状況を組織横断的に確認し、報告することで「透明性」に「説明性」を提供する。

アジャイル開発チームは、アジリティ（機敏性）とコントロールのバランスをとって運営されているので、その達成の観点からリスクを判断する必要がある。今までの監査の標準をそのまま適用はできない。開発チームの自律性を尊重しつつそのプロジェクトに必要な監査プロセスを適切に実施するため、監査人のアプローチをチームに伝達し、チームと調整してガバナンスと監査のための仕組みを合意することが重要である。さらにプロセスではなく「成果物」の品質に着目するため、監査人はアジャイル開発を正しく理解するだけでなく、アジャイル開発の監査を行うために必要な知識、技能、経験を有し、成果物そのものの品質を見極めるための技術を持っている必要がある。

（2）つながる技術の監査と保証

例えば「自動運転」等では、セーフティの観点で重要な機能の選定やハザードの洗い出しに、漏れや評価の誤りがないか、対応する安全機能または対策が整備され、テストされているかを確認する必要がある。セキュリティの観点でも保護すべき資産に対して脅威を特定し、対応する防御機能等の対策を含めてシステムを構築し、テストされているかを確認する必要がある。監査人はこれらの実施に必要なディペンダビリティやアシュアランスケースのような専門的な技術や、関連する基準や規制を理解すべきである。

セーフティとセキュリティのアセスメント（要件の洗い出し）は膨大な手間を要するが、その確認は避けて通ることはできない。これを効率的かつ確実に実現するためには、監査や第三者検証に耐えられるような標準化と自動化が必要と考えられる。第一線で管理状況が適切にシステムに記録

されていれば、第二線や第三線による確認が適切に行え、場合によってはAI技術を活用した、システムによる自動チェックが可能になる。さらに第三者評価や不測の事態に品質管理状況の証拠として疎明することも効率的に実施できる。監査のためだけに記録を取り繕う必要がなくなるため、第一線は業務を妨げられることなく、常に見られている前提で業務が行われることによる健全な相互牽制が期待できる。特にCPSではクラウド事業者等の他の組織の提供するシステムやソフトウェアへの依存は避けられない。このような場合には「アシュアランス業務やコンサルティング業務を提供する組織体内部および外部の者と、情報を共有し、活動について連携し、これらの者の仕事に依拠する」^[28] ことになるので、監査や第三者検証に耐えられるような標準化と自動化の実現は、これらの信頼関係を、生産性を落とすことなく確立し、維持することに寄与すると考えられる。

（3）システム監査人の専門性とその実施

多くの分野で新しい技術的なブレイクスルーが起こり、変化がさらに加速している今日、システム監査人には「組織体に影響を与える可能性のあるトレンドや新しい課題に注意を払っていること」がこれまで以上に要求される。誠実に「専門的能力と専門職としての正当な注意を実践」し、独立的に「組織体の戦略、目標、リスクと整合」して、効果的なコミュニケーションにより「見識に富み、率先的で、未来志向である」「リスクベースのアシュアランスを提供」し、組織体の改善を促進することが必要であり、このために十分な人材を確保し、監査組織の品質の継続的改善を実践する必要がある。

日本の生産性の低下は20年前から指摘され、多くの研究が行われ、打開を狙った政策も繰り返し実施されてきたにもかかわらず解決していない根の深い課題である。この解決のヒントとなるアジャイル開発は、決して簡易開発ではなく、科学的に洗練されたソフトウェア開発手法であり、しかもその原点は日本の製造業のノウハウにある。日本が官僚的な過剰管理と予定調和で忘れてしまった「互いの尊重に基づく文化を確立」し、組織の「透明性」を高めることが課題解決の鍵のように思われる。

組織の「透明性」は内部統制の目的そのものであり、監査のミッションでもある。システム監査

人は、新しいテクノロジーを正しく理解する「基本に立ち返った監査」により組織の価値を高める「説明性」を付加する必要がある、このことが、「第4次産業革命」を牽引する、「迅速」、「高品質」で「柔軟性」のある情報システムの実現に向けたシステム監査人の役割と考える。

7. 終わりに

第4次産業革命における情報化実践のためのヒントは日本の製造業のノウハウが詰まった「アジャイル開発」にある。「計画駆動開発」の対極にあり、難易度の高い開発手法であるが、リスクを最小にしながら、「迅速」、「高品質」で「柔軟性」のあるソフトウェア開発を可能にする「イノベーション」のプロセスでもある。さらに自律的に連携し合う情報システムに「安心と安全」を作り込む技術の国際標準にも日本は貢献している。我が国において遅れているのは、既に持っている「知的財産」の理解と活用なのではないだろうか。「日本のモノ作りの精神」を思い出し、論理分析過多、経営計画過多、コンプライアンス過多を脱し、「迅速」、「高品質」で「柔軟性」のあるソフトウェア開発に挑戦することが重要である。そして、作り上げたソフトウェアの信頼を担保するためには、組織の「透明性」を確保する内部統制が重要になる。システム監査人は、「アジャイル開発」の精神と「安心と安全を作り込む技術」を十分理解したうえで、「独立した専門家」としての評価を通じ、組織が「透明性」によって信頼を獲得することを効果的に支援することで、第4次産業革命における情報化実践に貢献することができる。

参考・引用文献

1. ドイツ連邦教育研究省。
Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. : ドイツ連邦教育研究省、2013. ページ : 9.
2. Klaus Schwab. 第四次産業革命 ダボス会議が予測する未来 (Kindle 版). : 日本経済新聞社、2016. ページ : 位置 No.176.
3. 藤原洋. 日本はなぜ負けるのか【新版】インターネットが創り出す 21 世紀の経済力学 (kindle 版). : インプレス R&D、2016. ページ : (Kindle の位置 No.280-331).
4. 深尾京司. 「失われた 20 年」と日本経済. : 日本経済新聞社、2012. ページ : 83-101.
5. 野中郁次郎・徳岡晃一郎. ビジネスモデル・イノベーション (Kindle 版). : 東洋経済新報社、2013. ページ : 18-19.
6. 独立行政法人 情報処理推進機構 IT 人材育成本部. IT 人材白書 2017. : 独立行政法人 情報処理推進機構、2017. ページ : 75 図表 2-2-3、ページ : 82.
7. 米国労働省労働統計局. Databases, Tables & Calculators by Subject. The Bureau of Labor Statistics of the U.S. Department of Labor. (オンライン) (引用日 : 2017 年 4 月 1 日.) <https://www.bls.gov/data/>.
8. 独立行政法人 情報処理推進機構技術本部 ソフトウェア高信頼化センター. ソフトウェア開発データ白書 2016-2017 年. : 独立行政法人 情報処理推進機構、2016. ページ : 51.
9. Kent Beck 他 17 名の著者たち. Manifesto for Agile Software Development. Agile Manifesto. (オンライン) 2001 年. (引用日 : 2017 年 9 月 18 日.) <http://agilemanifesto.org/iso/en/manifesto.html>.
10. Project Management Institute. Success Rate Rise. : Project Management Institute、2017. ページ : 4.
11. Mary Poppendieck & Tom Poppendieck. リーン開発の本質. : 日経 BP、2008.
12. Jeff Sutherland & Ken Schwaber. スクラムガイド (日本語版). : sucurumguide、2016. ページ : 3.
13. Hirotaka Takeuchi & Ikujiro Nonaka. The New New Product Development Game. : Harvard Business Review、1986.
14. 平鍋健児・野中郁次郎. アジャイル開発とスクラム 顧客・技術・経営をつなぐ協調的ソフトウェア開発マネジメント (Kindle 版). : 翔泳社、2016 (2013). ページ : 位置 No.2222-2260.
15. 野中郁次郎・西原文乃. イノベーションを起こす組織 (Kindle 版). : 日経 BP 社、2017. ページ : 位置 No.290.
16. Jeff Sutherland & Ken Schwaber. スクラムガイド (日本語版). : sucurumguide. ページ : 5-6.
17. VERSIONONE. 11th annual STATE OF AGILE REPORT. : VERSIONONE、2017.

ページ：10.

18. IPA. つながる世界のセーフティ&セキュリティ設計入門. : 独立行政法人 情報処理推進機構 (IPA)、2015. ページ：68-89.
19. OMG.Dependability Assurance Framework for Safety-Sensitive Consumer Devices (DAF)、version 1.0. (オンライン) 2016 年. (引用日：2017 年 4 月 1 日.) <http://www.omg.org/spec/DAF/1.0/PDF>.
20. 警察庁. 平成 28 年上半期におけるサイバー空間をめぐる脅威の情勢等について. (オンライン) 2016 年. (引用日：2017 年 4 月 1 日.) https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf.
21. National Institute of Standards and Technology. SP800-53 r4 Security and Privacy Controls for Federal Information Systems and Organizations. 2013.
22. Amazon Web Service. NIST Compliance on AWS. AWS. (オンライン) (引用日：2017 年 9 月 18 日.) <https://aws.amazon.com/jp/quickstart/architecture/accelerator-nist/>.
23. 中小企業庁調査室. 2017 年版中小企業白書概要. : 中小企業庁、2017. ページ：1.
24. COSO. Internal Control — Integrated Framework. : COSO、2013. ページ：183-192.
25. Robert Kaplan and David Norton. 戦略 マップ [復刻版] バランスト・スコアカードによる戦略策定・実行フレームワーク (Kindle 版). : 東洋経済新報社、2014. ページ：(Kindle の位置 No.1651-1652).
26. 内部監査人協会. 内部監査の使命. 日本内部監査人協会. (オンライン) 2015 年 7 月. (引用日：2017 年 09 月 18 日.) http://www.iiajapan.com/pdf/guide/IPPF_Mission_Japanese.pdf.
27. Mark Lines & Scott W. Ambler. ディシプリンド・アジャイル・デリバリー エンタープライズ・アジャイル実践ガイド (kindle 版). : 翔泳社、2013. ページ：位置 No.9409-9420.
28. 内部監査人協会. 内部監査の専門職的实施の国際基準. 日本内部監査協会. (オンライン) 2017 年 1 月. (引用日：2017 年 10 月 9 日.) 2050 — 連携と依拠. <https://global.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Japanese.pdf>.

org/translations/PublicDocuments/IPPF-Standards-2017-Japanese.pdf.

成田 和弘 システム監査技術者、CIA、CISA
(三菱 UFJ トラストシステム株式会社 品質管理部)