



認定 NPO 法人

日本システム監査人協会報

2020 年 2 月号

No 227

No.227 (2020 年 2 月号) <1 月 25 日発行>

第19期通常総会のご案内

！ 2 月 21 日（金） 13:30 開始 ！
2 月初より参加申込みを受付けます。

予告： https://www.saa.or.jp/soukai/tsujou_19_soukai.html



巻頭言

『2020東京オリンピック、パラリンピック』の成功を願って！！

会員番号：0281 力利則（副会長 月例研担当）

令和2年になりました。今年もいろいろと話題はあると思いますが、やはりオリンピックの年ですね。私は小学生の時に東京オリンピックがあって、内容はほとんど覚えていませんが、東京オリンピックを体験したというのは良い思い出になっているように感じます。オリンピックに向けてシステム監査人ができることがないかな！？と思っていたのですが、すでに時遅しで受付けて頂けませんでした。会員の皆様の中で何らかの形でオリンピックに関わっている方も多くいらっしゃると思いますが、スポーツの祭典としてITを生かした中継やリアルタイム&3次元放送、顔認証などいろいろと進められていると思います。一方、セキュリティの面で世界中から攻撃される危険性もあります。それをいかに守るか！これは情報戦だけでなく、IoT機器への攻撃も考えると、守備範囲も情報だけでなく、IoT機器を含め社会全体に及ぶと思います。

現在の東京オリンピックのサイトをみると、プライバシーポリシー(<https://tokyo2020.org/jp/privacy-policy/>) 個人情報取扱規程(<https://tokyo2020.org/jp/organising-committee/regulation/data/personal-information.pdf>) コンプライアンス規程(<https://tokyo2020.org/jp/organising-committee/regulation/data/compliance.pdf>) 等は公表されていますが、情報セキュリティに関するポリシーや規程類は公開されていません。しかしチーフ・セキュリティ・オフィサー(CSO)がしっかり任命されていてそのバックには体制とポリシー・規程と訓練、非常事態対応等がしっかりと準備されていると思います。日本国民の一人として東京オリンピックが無事に開催され世界から盛大な拍手が送られるような大会になって欲しいと思っています。

SAAJ会員の皆様で東京オリンピック・パラリンピックに関わっている方は、ぜひ頑張って活動してください。期待しています。そして今からでもSAAJがお手伝いできることがあれば何なりとお声掛けをして頂ければと思います。年初の巻頭言として、日本全体に関わる東京オリンピック・パラリンピックについて書いてみました。皆様、良い年をお過ごしください！！

以上

各行から Ctrl キー+クリックで
該当記事にジャンプできます。

<目次>

○ 巻頭言	1
『2020東京オリンピック、パラリンピック』の成功を願って！！	
1. めだか	3
【システム監査人のターニングポイント – イノベーションを考える】	
2. 投稿	4
【エッセイ 曽根崎心中】	
【コラム AI 時代に負けないために、システム監査人はどうあるべきか？ (2)】	
3. 本部報告	9
【第 248 回月例研究会：講演録 企業不正に関わる心理学的考察】	
【法人部会：法人会員紹介】NPO 法人 東京 IT コーディネータ	
【個人情報保護法 いわゆる 3 年ごと見直し制度改正大綱】第 1 章総論、第 2 章検討の経緯	
4. 支部報告	16
【北信越支部 2019 年度 石川県例会報告】	
【近畿支部 システム監査 基本学習セミナー】	
5. 注目情報	23
「2020 年 4 月に施行される改正民法に対応した「情報システムモデル取引契約書」を公開 【IPA】	
6. セミナー開催案内	24
【協会主催イベント・セミナーのご案内】	
7. 協会からのお知らせ	26
（予告）【第 19 期通常総会の開催】	
【新たに会員になられた方へ】	
【協会行事一覧】	
8. 会報編集部からのお知らせ	29

めだか 【 システム監査人のターニングポイント – イノベーションを考える 】

SAAJ システム監査人倫理規定は、第 2 条（使命）で、「システム監査人は、情報システムの信頼性・安全性・効率性・有効性を高めるため、その専門的知識と経験に基づき誠実に業務を行い、情報化社会の健全な発展に寄与することを使命とする。」としている。情報システムは情報化社会の基盤であり、イノベーションは情報システムを進化させる。innovation の定義は次の通り。



1. 革新、刷新、イノベーション ◆日本では「技術革新」の意味で用いられることがある。

・ Technological innovation has drastically changed our way of life. : 技術革新は私たちの生活を劇的に変えてきた。

2. 新機軸、新しい考え [工夫]

(出典 <https://eow.alc.co.jp/search?q=innovation>)

経済学者シュンペーターは、「経済発展の理論」の中で、“経済発展は、人口増加や気候変動などの外的な要因よりも、イノベーションのような内的な要因が主要な役割を果たす。”と論じている。人口増加や気候変動などへの対応は、グローバルな重要課題である。また、経済発展や生活レベルの向上には、イノベーションが求められ、2008 年に人口減少に転じた日本は、イノベーションを必要とする国である。

日本人がイノベーションに資する事例は、リチウムイオン電池、青色発光ダイオードなどの発明が挙げられる。また、生体高分子の同定および構造解析のための手法の開発は、アルツハイマー病などの治療に資することが期待されている。昨今、異分野が協力し合う、オープンイノベーションが話題である。情報システムに係るイノベーションは、アジャイル開発、AI、Block Chain、DFFT、DevOps、DX が挙げられ、量子コンピュータが最適化問題を劇的に解く機械として登場している。また、クラウド技術の進歩によりクラウドコンピューティングが普及しクラウドセキュリティが課題である。2018 年改正のシステム監査基準/システム管理基準は、管理目的と管理策に IT ガバナンスとアジャイル開発が追加された。

“シュンペーターは、イノベーションの担い手にとっては、金銭的なリターンもさることながら、何よりも未来に向けた自らのビジョンの実現こそが本質的だと言った。”と参考資料にある。SAAJ は、システム監査の活性化や IT ガバナンスのアセスメントに向けて、「システム監査を核にした“IT アセスメント”の普及を図り、SAAJ の活動を“IT アセスメント”の実践に焦点を当てて取り組む。この取り組みによって、システム監査人のビジネス機会の拡大を図り、SAAJ の知名度向上、会員の増強に繋げる。」と論じている。

システム監査人は、情報システムに係るイノベーションを担う一員であると自覚したい。(空心菜)

参考資料 : 「人口と日本経済 長寿、イノベーション、経済成長」吉川洋 著 中公新書 2388

(このコラム文書は、投稿者の個人的な意見表明であり、SAAJ の見解ではありません。)

2020.01

【エッセイ】 曽根崎心中

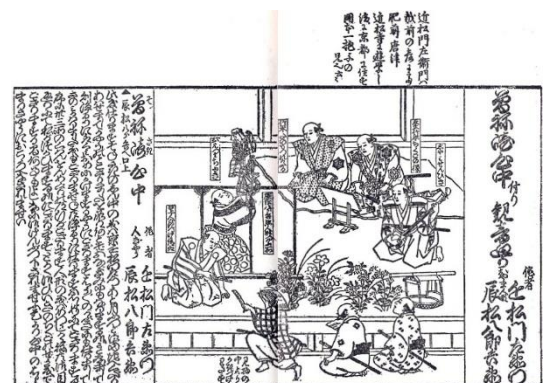
会員番号 0707 神尾博

近松門左衛門作の「曽根崎心中」は、元禄時代に上方で一世を風靡した、人形浄瑠璃の代表的な演目である。舞台は露天神社（大阪市北区）。若い女性には遊女の名を冠する「お初天神」の方が、通りが良いかも知れない。遊女のお初と相思相愛である徳兵衛が、奉公先の主人との確執からの金銭をめぐる騒動に巻き込まれ、追い詰められて情死するというストーリーは、諸氏もご存じの通りである。彼女や彼にとって、二人がセットでないとこの世に存在する意味がないと思い詰めての行動だっただろう。

ITの世界で一揃えでないと意味をなさないといえ、電子割符（でんしわっぷ）が想起される。暗号技術を用いデータを複数に分割し、それらがすべて揃わないと復元出来ないというものだ。3つの割符をそれぞれサーバ、PC、ユーザに持たせることで、PCの盗難対策にも使えるそうだ。2019年12月に大騒動となったHDD転売事件においても、有効な情報漏洩防止策のひとつになっただろう。

そういえば、仮面ライダー（1971～1973）に敵対した、悪の秘密結社であるショッカーが送り出した怪人は、敗北とともにベルトに仕組まれた装置で爆死させられていた。任務遂行の失敗への制裁という意味もあるが、機密保持のため兵器本体とセットでの破壊を図ったと、捉えることも出来るだろう。現実世界では、強奪や破棄された米軍戦闘機からの機密データ盗難を受けて、2014年にはDARPAがIBMへ「自爆するチップ」の開発を依頼したというニュースも報道されている。

民生に目を移すと、廃棄するPCもさることながら、盗難や紛失したスマホ内のデータ秘匿の問題がある。米国では2014年からカリフォルニア州やミネソタ州等で、相次いでスマホへのキルスイッチ搭載を義務付けする法案が成立している。お馴染みのリモートロックやリモートワイプ機能のことだ。



さて、近松の曽根崎心中をモチーフにした後世の作品には、実は相対死は偽装であり二人は生き延びていたという結末のものもあり、それはそれで興味を覚える。しかしながら、元々PCやサーバ等にあった、本来なら抹消されるべきデータが残存し流通しているとなると、憤慨以外の何物でもない。PCなら外部へ出す前にHDDを物理的に破壊、サーバなら電源から切り離された時点でデータを無効化するHDDの採用等、損害の規模に応じた予算確保といったアセスメントが不可欠だろう。

（このエッセイは、記事提供者の個人的な意見表明であり、SAAJの公式見解ではありません。画像はWikiにより著作権保護期間満了後のものを引用しています。）

<目次>

【コラム】AI 時代に負けないために、システム監査人はどうあるべきか？（2）

会員番号 1644 田淵隆明（近畿支部 システム監査法制化推進プロジェクト）

1. はじめに

前回より、「AI 時代に負けないために、システム監査人はどうあるべきか」の連載を始めました。その契機となったのは、下記の 3 点の疑問である。

- ・何故、平成の時代に、日本人がここまで劣化してしまったのか？
- ・何故、このようなデタラメがまかり通る時代になってしまったのか？
- ・何故、他の G7 先進国と異なり、日本だけが回復出来ないのか？

前回は述べたように、それには次の 8 個の原因・元凶があると筆者は考えている。

★平成が「暗黒の時代」となった「8 個の元凶」★

- ①「新自由主義」的政策による、中間層の破壊と階級の固定化。
- ②「ゆとり教育」による、学力低下・学級崩壊、及び、モラルの低下
- ③「SI 認定・登録」の廃止(2003 年、2010 年)による、IT 業界の劣化及び IT 有資格者の地位の低下
- ④「製造物責任法」の立法不備による、不備ソフトウェアの放置
- ⑤「研究開発費の一律費用処理」による、頭脳軽視と近視眼的経営
- ⑥ ⑤と合わせ技での「金融検査マニュアル」による開発力低下
- ⑦誤った時価会計の導入による混乱、及び、会計基準の不備
- ⑧数学を知らない経済学者・アナリストの闊歩

★この連載では、令和新時代を迎えて、我々システム監査人が、「失われた 30 年」とも揶揄される、我が国の閉塞状況を打破する上で、いかに重要な任務を担っているのか、どのような能力が期待されているのかについて掘り下げて行きたい。ただし、関連性の関係で、上記の 8 項目の掘り下げについては、順不同となることを御容赦頂きたい。今回は①をメインに、そして、予告編として④を取り上げる。

2. 「平成」が「失われた 30 年」になった元凶①：「新自由主義」的政策による、中間層の破壊と階級の固定化。

バブルが崩壊し、我々日本人は、自信を失い、迷走した。そして、解決策を求めて無限の迷路をさまよった挙句、行き着いた策は「破壊的治療」とも言うべき新自由主義的政策であった。当時、彼らは、「既得権打破」を標榜するだけではなく、「累進課税をやめて税をフラット化したほうが、人々の労働意欲を掻き立て、努力した者が報われる社会になり社会は豊かになる」と称して累進課税に反対し、給付型奨学金に反対するなど、社会のセーフティー・ネットの縮小も標榜していた。結局、非正規雇用が増大し、格差が拡大し、「絶対に這いあがれない社会」が出現した。人々の労働意欲が掻き立てられるどころか、絶望と失望が社会に蔓延し、雇用の不安定化による購買力の低下は慢性的な不況を深刻化させた。やはり、この政策については、明らかに失敗であったように思われる。隣国と異なり、**我が国は内需主導型の国であり、現在でもなお GDP の 88%は内需により支えられている。つまり、「我が国の労働者は、同時に、優良な購買力をもった消費者でもあった」**のである。

結局、暗黒の平成の「失われた 30 年間」は、改革に熱狂し、改革に暴走し、改革に翻弄され、改革で自滅し、改革に疲れた 30 年であったと思われる。

何故、そんなことになったのか？それは、「既得権打破」のスローガンばかりが先行し、国民の多くが、「改革の中身と影響」も、「出口戦略」も、「セーフティネット」も考えず、「規制緩和」のスローガンに陶醉し、思考停止に陥り、ひたすら、官僚叩きを始めとする「既存のシステムの破壊」にばかり熱狂したためであると思われる。また、「自己責任」というフレーズに象徴されるように、「情報弱者」や「生活弱者」の権利よりも、「効率」が優先され、あたかも「騙されるほうが悪い」という風潮が蔓延してしまった。我が国伝統の「勤勉さ」・「誠実さ」は軽視されるようになってしまった。

★「情報弱者」や「生活弱者」が守られ、「正義がまかり通る」ためには、一定の適正な規制は必要であることを、我々日本人の多くは、「失われた 30 年」という高い代償を払って、ようやく認識したようである。この状況を深刻化させた大きな原因として、バブル崩壊による閉塞感があったのは当然であるが、同時に、「第一次ゆとり教育」が深く影を落としていたことについては、別の機会に触れることとしたい。

★**最近の動向**：昨年 11 月 23 日の西日本合同研究会でも詳述したように、2013 年以降については、次のように、全般的に改善傾向が見られる。このまま景気が緩やかに回復し、社会の傷が治癒することを願ってやまない。

- ・公立高校の無償化、及び、幼保無償化
- ・給付型奨学金の拡充、及び、リボルビング型返済の奨学金の拡充
- ・正社員化の推進
- ・消費税の軽減税率導入
- ・食品ロス防止法
- ・ホワイト・カラー・エグゼンプションの縮小
- ・我が国にとって極めて深刻な、TPP による制度変更の排除の成功
- ・ひとり親世帯の保護拡充

3. 「AI」によって、取って代わられる可能性のある専門職とは？

AI とは「人工知能」(英：artificial intelligence, 独：künstliche Intelligenz, 仏：intelligence artificielle) のことである。2015 年に英国の有名大学が「あと 10 年で無くなる職業」のランキングを発表し、各方面は騒然となった。現に、米国では、例えば薬剤師などでも、典型的な症例については処方箋の作成を AI で代替することが急速に広がっており、人間の出番は「AI よりレベルの高い専門的知識」を有するケース、または、「AI に使われるケース」のどちらかに二極化しつつあるようである。

このことは、排他的独占業務である、弁護士や税理士などの「士業」についても発生しており、我が国でも各「士業」は戦々恐々としている状況にある。

★下記をご覧ください。これは昨年の西日本合同研究会でも御紹介した資料である。

AI 時代と「士業」の関係

★8 士業：戸籍・住所等について、「職務上請求書」による請求権が認められているもの

士業名	監督官庁	登録者	登録法人	クライアントの業界・依頼内容による業務の差異
弁護士	(日弁連による自治)	35,031 人	557 法人	大
司法書士	法務省	22,632 人 認定：17,002 人	700 法人	小 (大半が商業登記・不動産登記)
土地家屋調査士	法務省	16,471 人	360 法人	小
行政書士	総務省	46,957 人 特定：3,912 人	554 法人	大
海事代理士	国土交通省	338 人 (任意加入)		中 (海事に関する行政書士・社労士)
税理士	国税庁 (財務省の外局)	78,570 人	4,104 法人	小～中
弁理士	特許庁 (経産省の外局)	13,505 人	257 法人	大
社会保険労務士	厚生労働省	24,015 人	1,725 法人	小～中

AI との競合では、次のような土業が危ないと言われている。

- ・ 定型的業務が多い
- ・ 官公庁のサイトで、専門的知識がなくても、本人申請を容易に行うことができる。
- ・ 一定の金銭の納付が必要な場合において、その計算式が複雑ではないもの

このことは、我々システム監査人にも当てはまると思われる。我々、システム監査人としても、「自衛」しなければならない時が迫っている。

4. 「AI」の弱点の1つ---多義語の解析力

下記の表は、漢文と日本語、現代中国語、英語、ドイツ語、フランス語の比較である。

項番	漢文	意味★	日本語	現代中国語	英語	ドイツ語	フランス語
1	為	①★	ために(利害)	为	for	für	pour
		②	なる	变成	become	werden	se faire(再帰形) devenir
		③	たり(断定)	是	be	sein	être
		④	受動(為～所)	(別の構文)			
		⑤	なす/つくる(作る)	做/造など	make	machen	faire
		⑥	なす(する)	做	do	tun	faire
		⑦	行為	行为	act/action	Tat	acte/action
		⑧	作為	作为	artificiality	Künstlichkeit	nature artificielle
		⑨	作業/仕事	工作	work	Arbeit	travail
		⑩	おさむ(統治する)	统治	govern	regieren	gouverner
		⑪	变成作用(Aを以ってB(名詞)となす)	成为A的B(名詞)	make A B	machen A zu B	faire/render A B
		⑫	变成作用(Aを以ってC(形容詞)となす)	C(形容詞) 做 A	make A C	machen A C	faire/render A C
2	見	①★	見る	看/见	see watch look at	sehen beobachten anschauen	voir regarder
		②★	まみゆ(会う)	见	meet	treffen	recontrer
		③	現れる	出现	appear	erscheinen	paraître
		④	受動(見～於)	被	be + 過去分詞	過去分詞+werden 過去分詞+sein	être+ 過去分詞
3	与(與)	①	与える	給	give	geben	donner
		②★	と/及び	和/(与)	and	und	et
		③★	～に/～とともに/ ～向かって	与	to ~ with ~ against ~	zu ~ mit ~ gegen~/wider~	à ~ avec ~ contre ~
		④	ともに	一起	together	zusammen	ensemble
		⑤	くみず(組む/ グルになる)	和～結成一伙	conspire with ~ pair with ~	sich mit~ verschwören mit~ paaren	conspirer avec ~ assortir avec ~
		⑥	あずかる(関与/参与)	正干預	participate in ~	an ~ teilnehmen	participer à ~
		⑦	あずかる(関わりがある)	有关系	have a relation for~ be connected with~	eine Verbindung für ~ haben mit~Verbindung gebracht werden	avoir une relation pour~ être associé à ~
		⑧	疑問(「欺」の代用) 反語(「欺」の代用)	吗	?	?	?
		⑨	ために(為)	为	for	für	pour
		⑩	もって(以)	以	by with	durch mit	par avec
		⑪	比較(同一)	和～一样	as	wie	que
		⑫	比較(不同一)	和～不一样	than	als	que

これは、日本の高校生を悩ませる漢文の多義語の例である。実は現代中国語では、1951 年から大規模な言語改革が行われ、上記のように多義語の意味が大幅に制限されたり、「何」「之」「於」「所」のように、事実上廃止された多義語文字もある。

※近年、フランスは、大幅な言語改革を行っているようである。特に①倒置が殆ど消滅していること、②非人称代名詞 *on* と中性代名詞 *ça* の用法が大幅に増加している。その結果、NHK のフランス語講座も 2018 年から採用する文法が大幅に変更されている。Brexit により、ドイツ語とフランス語の重要度は大幅に上昇するため、システム監査人諸氏には両言語の習得を強くお勧めしたい。

実は、この多義語は「AI」の苦手分野である。このことは AI に対抗する上での 1 つのヒントとなると思われる。同様に、英語の *that, as, of* や、フランス語の *que, de, en, faire* など極めて多義的であるため、AI の苦手分野である。

5. (次回予告)「平成」が「失われた 30 年」になった元凶④：「製造物責任法」の立法不備による、不備ソフトウェアの放置

まず、製造物責任法第 2 条を確認する。

第二条 この法律において「製造物」とは、製造又は加工された**動産**をいう。

我が国の民法では、「物」は「有体物」と「無体物」に分かれ、「有体物」は「動産」と「不動産」に分かれる。ソフトウェアは「無体物」であるため、製造物責任法は適用されない。製造物責任法の第 4 条では欠陥による被害が発生した場合の民事訴訟における「立証責任」が、被告(メーカー)側に転換されている。そのため、ユーザとしては利用しやすい法律ではあるが、ソフトウェアには適用されないため、ソフトウェアの欠陥(設計誤り・法令対応不備)により、脱税や会計報告の開示に誤りが発生した場合、メーカー側の責任を追及することが極めて困難である。

今回は、民事訴訟法の要である「立証責任」を軸に、この問題を掘り下げることにする。

6. 補足

2019 年 12 月 29 日、まるでスパイ映画かと思いがうようなニュースが全世界を駆け廻った。一昨年 11 月に金融商品取引法違反の容疑で、神奈川県に本社を置く、某自動車会社の元会長が逮捕されたが、保釈中に荷物に隠れて関西空港の出国審査をすり抜け、海外に逃亡するという事件が発生した。その結果、ICPO(国際刑事警察機構=インターポール)の手配を受けることとなった。日本を代表する企業のトップが ICPO の手配を受けるという、前代未聞の事態が発生したことは、極めて遺憾である。

今回のことを受けて、法務省では「保釈基準の見直し」が行われるとともに、急遽、保釈に関する刑法の規定の改正のため、法制審議会を開催し、今国会で改正が行われる見込みである。また、今回の逃走では(運営が民間委託されていた)関西国際空港のプライベート・ジェット専用ゲートの脆弱性が問題となったことが明らかとなっているが、(係員の動きを含めた)システムの外部監査を行っていれば、逃走を防止できた可能性が高い。

今後、公共機関の民間委託のあり方の再検討も不可避と思われるが、特に公共性が高いインフラに関する、外部システム監査の必要性もクローズ・アップされることとなった。**【システム監査の専門家の出番】**

また、今回の事案を会計基準の観点から見れば、いわゆる「連結外し」が悪用された形と言われているが、**「連結外し」を容認している連結財務諸表第 5 条、第 10 条、第 13 条の改正は急務**であると考えられる。

※以上述べたことは筆者の私見であり、いかなる団体をも代表するものではありません。また、法令の適用・会計基準の適用等については、必ず、御自身でご担当の会計士その他の専門家の方々への御確認・照会をお願いします。

<参考文献>

- (1)日本システム監査人協会 2019 年西日本合同研究会講演資料
- (2)「軽減税率」田淵隆明が語る、IFRS&連結会計〔Ⅰ〕〔Ⅱ〕: "In Varietate Concordia", EU の知恵に学ぶ IFRS では何故そう考えるのか? (MyISBN - デザインエッグ社)
- (3)「軽減税率」田淵隆明が語る、「国際取引における連結上の照合・相殺消去」再考: ~洋上在庫をどう把握するか?~ ~コンテナ船の Incoterms に注意~ (MyISBN - デザインエッグ社)
- (4)ジョセフ・スティグリッツ「これから始まる「新しい世界経済」の教科書」(徳間書店)

<目次>

2020.01

第 248 回月例研究会：講演録**テーマ：【企業不正に関わる心理学的考察】**

会員番号 2574 竹原豊和 (月例研究会)

【講師】 帝京大学経済学部経営学科 教授**博士（経営学） 公認不正検査士 公認内部監査人 伍井和夫 氏****【日時・場所】 2019 年 12 月 13 日（金） 18：30 - 20:30、機械振興会館 地下 2 階ホール（神谷町）****【テーマ】 「企業不正に関わる心理学的考察」****【要旨】****(1)経営者不正に関わる心理学的考察****(2)技術者・有資格労働者の倫理的ジレンマ****(3)従業員による内部告発の心理学的考察****【講演録】****1. 経営者不正に関わる心理学的考察**

1 章においては「倫理学のフレームワーク」「ステークホルダーと経営倫理」「コーポレート・ガバナンス」「バスケットボールにおける【ファウル・ゲーム】に関わる議論」という 4 つの観点から経営者不正に関わる心理学的考察をご講演いただいた。

産業革命以前においては、神学者・宗教関係者といった教会に属する人物はラテン語が読めるために医者や法律家の役割を担っており、倫理観を持った対応が可能となっていたが、産業革命以降においてはそれらが教会から離れていき、それに伴い倫理学が必要となっていた。ジレンマがあるからこそ倫理が必要であり、様々な「道徳的なジレンマと解決の型」が存在している。

コーポレート・ガバナンスにおいては「企業と利害関係者との関係」という意味と「経営者や、その経営を監視・監督する仕組み」という 2 つの意味がある。但し、前者においては「企業は誰のために経営されるべきか」という問題があり、後者においては「経営者や、その経営に対する監視・監督は誰の観点からなされるべきか」という問題がある。そのため、前提条件にて内部統制、内部監査がどうすべきなのか、を考える必要がある。

ファウルにより相手チームのフリースローの失敗にて自チームのリバウンドによる攻撃権を得ることが可能となり、逆転勝利が可能となるファウル・ゲームという戦術がプロのチームのみならず、中学生のチームでも行うことがあり、勝利至上主義と健全スポーツとの間にジレンマが発生している。その意味では、勝利至上主義のプロ・スポーツにはスポーツ倫理等は存在せず、今後も醸成されることはない。

2. 技術者・有資格労働者の倫理的ジレンマ

スペースシャトル・チャレンジャー事故の教訓をもとに、技術的観点からのジレンマ（人道的観点からのジレンマ）と経営的観点からのジレンマとの線引き問題をご講演いただいた。

線引き問題として、ある倫理的規則に照らしてみても、そのつど現実的な行為が許されるかどうかの問題にな

ることがある。「使用不可領域（あきらかに問題が発生する領域）」「受容可能範囲」「使用可能範囲（合格範囲）」の3つの範囲に対して、どこで線引きを行うのかというのはジレンマである。線引き問題は、ある倫理的規則の妥当性を前提とした上で、それを具体的に行為に適用する際に規則の定める基準や概念をどのように理解し判断するかという場面で生じる。そのうえで、内部監査人もジレンマが発生することがある。

3. 従業員による内部告発の心理学的考察

内部告発は、不正への対策としては有効なツールである旨と、内部告発が発生した際のプロセス及び内部告発をどのように活用していくかについてご講演いただいた。

内部告発を行うことで不正への対応が行える半面、内部告発を行った本人は報復行為にて解雇されたり訴えられたりすることとなる。ここにジレンマが存在する。この問題については、公益通報者保護法にて以前より改善されているものの、報復行為そのものは依然として存在している。

日本の内部告発は「真面目」「正義感」という動機から行われるが、欧米の内部告発は「自分の利益」という動機から行われており、日本と欧米において違いがある。

21世紀に発覚した企業不祥事の多くは内部告発にて明らかになった。この内部告発を内部通報として社内に取り込むという議論がある。但し、その前提条件として経営者による「是正の約束」というのは信頼関係においても大きなポイントとなる。近年、若い世代の所属意識は会社ではなく SNS の仲間になりつつある。こういった所属意識によって内部通報が今後機能していく可能性がある。

内部通報がしっかりと機能しているかは監査の対象である。但し、監査人が当事者になってしまうと、監査等他のことに対して手が回らなくなるため、監査人としては内部通報のサポート対応が適切となる。

【所感】

なぜ、不正が発生するのか、そしてその根底にあるジレンマや倫理観、不正への対応策について学ばせていただいた。特に、ファイル・ゲームのような不正を「必要悪」という捉え方をせざるを得ない勝利至上主義というジレンマは、利益至上主義である経営とのジレンマと大変似ている節があり、このような一見必要悪と思われる点についてしっかりと発見し、是正する必要があることをシステム監査人として切に感じた。

以 上.

<目次>

法人部会【法人会員紹介】NPO 法人 東京 IT コーディネータ

会員番号 6068 矢野一男（法人部会）

法人部会にはさまざまな企業があり、各会員企業がシステム監査を通じて交流することで、情報収集や人脈などさまざまなことを自社の役に立てています。今回は 2019 年 4 月に設立満 15 年を迎えた「特定非営利活動法人 東京 IT コーディネータ」を紹介します。

NPO 法人 東京 IT コーディネータ**<沿革>**

当 NPO 法人は、2001 年に発足した経済産業省の推進資格である IT コーディネータの有志が、IT コーディネータの本来の役割を企業経営の場で果たすための活動組織として、2004 年 4 月 27 日に設立しました。

現在は、複数の資格と多分野の経験を持つコンサルタント 10 数名が参加しており、中堅・中小企業の IT 経営分野や情報セキュリティ分野の支援を中心に、コンサルティング業務及び研修業務に携わっております。

<事業内容>

当 NPO 法人は、ベンチャー精神とボランティア精神を両立させながら、中堅・中小企業の経営基盤の強化を、中立的な立場から支援することを目的に活動しております。

IT の利活用や情報化に関する「コンサルティング」や「啓発・相談活動」、そして「研修」を通して、以下の分野を支援しております。

- 経営改革・改善のための IT 戦略を中心とした IT 経営導入の支援
- IT 経営の有効性向上のための システム監査・情報セキュリティ監査業務
- 企業のマネジメントシステム高度化のための リスク管理システムの構築と評価
- 情報セキュリティに係わるマネジメントシステム診断および脆弱性診断
- ケース研修による ITC 等の育成
- 中小企業海外展開のためのハンズオン支援

なお当社のサービスの具体的な内容は以下の URL をご参照下さい。

<https://npo-tokyoitc.jp/>

関係機関への登録

- NPO 法人 IT コーディネータ協会：ITC 届出組織（ビジネス志向）
- 経済産業省：「システム監査企業台帳」に登録
- NPO 法人日本セキュリティ監査協会：「情報セキュリティサービス台帳/情報セキュリティ監査サービス 019-0010-10」及び、情報処理推進機構(IPA)：「情報セキュリティサービス基準適合サービスリスト/情報セキュリティ監査サービス」に登録

<システム監査について>

最近のシステム監査関連の動向として、“IT ガバナンス”と“サイバーセキュリティ”が有ります。

IT コーディネータはその使命として企業の IT 経営、即ち戦略に基づいた IT の利活用による経営の変革及び持続的な成長を支援することを担っていますので、従来より経営ガバナンスの一環として“IT ガバナンス”についてもテーマにしてきております。

当 NPO 法人では設立当初よりシステム監査を手がけてきておりますが、特に情報セキュリティ分野に注力し ISMS や P マークの認証取得、内部統制システムの構築・評価を支援してきています。昨今はサイバーセキュリティの脅威が急速に増大してきており、中堅・中小企業でもその安全対策が急務になっています。当 NPO 法人には専門性の高いスキルを有する IT コーディネータも参加しており、直接“情報セキュリティ脆弱性診断”や“ペネトレーションテスト”等を行い、情報セキュリティ監査を総合的に実施出来る態勢を整えております。

当 NPO 法人では、これらの実施に際してはリスクアプローチによるマネジメントシステムの構築を奨めております。

<まとめ>

当 NPO 法人では多くの会員が日本システム監査人協会(SAAJ) の公認システム監査人の資格を取得し、監査品質の向上に努めております。又、SAAJ の法人会員にも登録し法人部会に参加することにより、法人会員同士がお互いの強みを活かしたコラボレーションによる業務の実績も出てきています。

今後とも、より多くの業種・業態の中堅・中小企業の方々との出会い、そしてご支援できることを期待しておりますので、宜しくお願い致します。

<目次>

2020.01

【 個人情報保護法 いわゆる 3 年ごと見直し制度改正大綱 】 第 1 章総論、第 2 章検討の経緯

会員番号 1760 斎藤由紀子 （個人情報保護監査研究会）

2019 年 12 月 13 日、「個人情報保護法 いわゆる 3 年ごと見直し 制度改正大綱」が公表された。大綱へのパブリックコメントは 2020 年 1 月 14 日に締切られ、2020 年の通常国会（1 月 20 日召集）に個人情報保護法の改正法案が提出される予定である。 <https://www.ppc.go.jp/news/press/2019/20191213/>

【個人情報保護法 いわゆる 3 年ごと見直し制度改正大綱】 目次

第 1 章 総論	3
第 2 章 検討の経緯	5
第 3 章 個別検討事項	7
第 1 節 個人データに関する個人の権利の在り方	7
1. 基本的考え方	7
2. 個人情報保護法相談ダイヤルの充実	7
3. 利用停止、消去、第三者提供の停止の請求に係る要件の緩和	8
4. 開示請求の充実	9
5. 開示等の対象となる保有個人データの範囲の拡大	10
6. オプトアウト規制の強化	11
第 2 節 事業者の守るべき責務の在り方	14
1. 漏えい等報告及び本人通知の義務化	14
2. 適正な利用義務の明確化	16
第 3 節 事業者における自主的な取組を促す仕組みの在り方	17
1. 認定個人情報保護団体制度	17
2. 民間の自主的取組の推進	19
第 4 節 データ利活用に関する施策の在り方	21
1. 匿名加工情報制度	21
2. 「仮名化情報(仮称)」の創設	21
3. 公益目的による個人情報の取扱いに係る例外規定の運用の明確化	22
4. 端末識別子等の取扱い	23
5. 個人情報の保護と有用性に配慮した利活用相談の充実	25
6. データ利活用に関する国際的な取組の必要性	26
第 5 節 ペナルティの在り方	27
第 6 節 法の域外適用の在り方及び国際的制度調和への取組と越境移転の在り方	28
1. 基本的考え方	28
2. 域外適用の範囲の拡大	28
3. 外国にある第三者への個人データの提供制限の強化	29
第 7 節 官民を通じた個人情報の取扱い	32
1. 基本的考え方	32
2. 行政機関、独立行政法人等に係る法制と民間部門に係る法制との一元化	32
3. 地方公共団体の個人情報保護制度	32
第 8 節 継続的な検討課題	34
・ (課徴金制度)	34

ページの見やすさと全体的把握の観点から、「個人情報保護法 いわゆる 3 年ごと見直し 制度改正大綱」(以下、「大綱」と呼ぶ)の目次を先に掲げたが、罰則を伴う法律ということで、例えば、第 8 節(継続的な検討課題・課徴金制度)からは、GDPR の制裁金 250 億円(英国 British Airways 社)、62 億円(google)と同様な制度となるのかどうか、少なくとも現行の罰則だけでは不十分と考えられている。また、第 4 節 2「仮名化情報(仮称)」の創設では、データ利活用と言いながら、安全対策の強化を求められるのかどうかなど、詳細は明確になっていない。これまで何もして来なかった事業者にとっては、何とも恐ろしい改正に見えるのかもしれない。

「大綱」は、概要と方向性が示されているだけで、条文にまで落とし込まれていないため、今後提出される法案を待ちたいが、今回は、第 1 章 総論に述べられている 5 項目から、法改正のポイントを確認する。また、個人情報保護委員会の見直し作業は、2015(平成 27)年改正法附則第 12 条に基づき実施された。この「大綱」では、個人情報保護法を制定し、運用し、点検し、見直すという、PDCA を確実に実施していることを報告しており、国民にもよく理解できる内容となっている。

「個人情報保護法 いわゆる 3 年ごと見直し 制度改正大綱」

第 1 章 総論(抜粋)

- 第一に、情報を提供する個人の、自らの情報の取扱いに対する関心や、関与への期待が高まっており、**個人情報保護法第 1 条**の目的に掲げている「個人の権利利益を保護」するために必要十分な措置を整備することに配慮しながら制度を見直す必要がある。
- 第二に、2015(平成 27)年改正法で特に重視された保護と利用のバランスをとることの必要性は、引き続き重要であり、個人情報や個人に関連する情報を巡る技術革新の成果が、経済成長等と個人の権利利益の保護との両面で行き渡るような制度を目指すことが重要である。

2015(平成 27)年改正法 第 1 条(目的)

この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、**個人情報の適正かつ効果的な活用**が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の**個人情報の有用性**に配慮しつつ、**個人の権利利益を保護することを目的とする。**

- 第三に、デジタル化された個人情報を用いる多様な利活用が、グローバルに展開されており、国際的な制度調和や連携に配慮しながら制度を見直す必要がある。
- 第四に、海外事業者によるサービスの利用や、国境を越えて個人情報を扱うビジネスの増大により、個人が直面するリスクも変化しており、これに対応する必要がある。
- 第五に、AI・ビッグデータ時代を迎え、個人情報の活用が一層多岐にわたる中、本人があらかじめ自身の個人情報の取扱いを網羅的に把握することが困難になりつつある。このような環境の下で、事業者が個人情報を取り扱う際に、本人の権利利益との関係で説明責任を果たしつつ、本人の予測可能な範囲内で適正な利用がなされるよう、環境を整備していくことが重要である。

第 2 章 検討の経緯（抜粋）

- 2015(平成 27)年改正法**附則第 12 条第 3 項**において、政府は、同法の施行後 3 年ごとに、個人情報の保護に関する国際的動向、情報通信技術の進展、それに伴う個人情報を活用した新たな産業の創出及び発展の状況等を勘案し、2015(平成 27)年改正法による改正後の個人情報保護法(以下「改正個人情報保護法」という。)の施行の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとされている。

2015(平成 27)年改正法 附則 第 12 条 (検討)

1. 2. (略)
3. 政府は、前項に定める事項のほか、この法律の施行後 3 年ごとに、個人情報の保護に関する国際的動向、情報通信技術の進展、それに伴う個人情報を活用した新たな産業の創出及び発展の状況等を勘案し、新個人情報保護法の施行の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとする。

- また、**同条(附則第 12 条)第 3 項**において、政府は、改正個人情報保護法の施行後 3 年を目途として、個人情報の保護に関する基本方針の策定及び推進その他の委員会の所掌事務について、これを実効的に行うために必要な人的体制の整備、財源の確保その他の措置の状況を勘案し、その改善について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとされている。
- さらに、**同条(附則第 12 条)第 6 項**においては、政府は、改正個人情報保護法の施行の状況、第 1 項(附則第 12 条第 1 項)の措置の実施の状況その他の状況を踏まえ、改正個人情報保護法第 2 条第 1 項に規定する個人情報及び行政機関等保有個人情報の保護に関する規定を集約し、一体的に規定することを含め、個人情報の保護に関する法制の在り方について検討するものとされている。

2015(平成 27)年改正法 附則 第 12 条 (検討)

6. 政府は、新個人情報保護法の施行の状況、第一項の措置の実施の状況その他の状況を踏まえ、新個人情報保護法第 2 条第 1 項に規定する個人情報及び行政機関等保有個人情報の保護に関する規定を集約し、一体的に規定することを含め、個人情報の保護に関する法制の在り方について検討するものとする。

- 委員会は、2015(平成 27)年改正法**附則第 12 条**の規定を踏まえ、いわゆる 3 年ごと見直しについて具体的に検討を進めてきた。第 83 回個人情報保護委員会(2018(平成 30)年 12 月 17 日)において、「個人情報保護委員会の第一期を終えるにあたって」を公表し、当時の委員長の下で運営されてきた第一期目の終了に際し、これまで 5 年間の経緯を踏まえ、次期委員会への申し送りとして、現下の状況を基に主な論点を取りまとめた。また、これを踏まえ、第 86 回個人情報保護委員会 2019(平成 31)年 1 月 28 日)において、「いわゆる 3 年ごと見直しに係る検討の着眼点」を公表した。

次回は、「大綱」第 3 章 個別検討事項 の内容について、紙面が許す範囲で、現行法や GDPR などを引用していく予定である。国会会期が 150 日であることを考慮すると 5 回を超えないシリーズとしたい。

<目次>

2020.01

支部報告【 北信越支部 2019 年度 石川県例会報告 】

会員番号 1281 宮本茂明（北信越支部）

以下のとおり 2019 年度 北信越支部・石川県例会を開催しました。

- ・日時：2019 年 12 月 7 日（土） 13:00～17:00 参加者：13 名
- ・会場：IT ビジネスプラザ武蔵 4F 情報化研修室（金沢市）
- ・議題：1.SAAJ 中部支部・北信越支部・JISTA 中部合同研究会 参加報告/2020 年度企画
テーマ：「強固な品質体制を構築するプロセスイノベーション人材の育成」
- 2.西日本支部合同研究会 in Osaka 参加報告 「スマート社会とシステム監査」
（北信越支部報告）「AI システムをどう監査するのか？」 栃川昌文 氏
- 3. 2020 年度計画意見交換
- 4.研究報告：「CIS Controls の概要」 宮本茂明

◇ 研究報告 1**「AI システムをどう監査するのか？」**

報告者（会員番号 1354 栃川昌文）

AI が様々な分野に利用されるようになってきました。一方、AI が間違った判断をした事例なども報告されています。そんな折、日本経済新聞に「採点される人生」というテーマで連載記事が載っていました。この記事を読んだとき、AI システムのリスクを認識し適切に対応することが必要だと感じました。

そこで、AI システムを監査するためにはどのようなことに留意しなければならないのか、ということ調べてみました。AI に関して深い知識があるわけでもないのですが、自分なりにこういう点に気を付けなければならないのではということが整理できたので、それを支部の例会で発表させていただきました。発表内容は、以下の通りです。

①データが重要な経営資源に（データ資本主義）

デジタルトランスフォーメーション（DX）という言葉が、あちこちで聞くようになりました。『IT の力で人・モノ・コトをつなげ、新しい価値を生み出し、人々の生活やビジネスをより良く変化させる』ことで、人類史に残る革命とも言われています。革命後の社会は「デジタル社会」であり、政府は「Society5.0」と定義しています。

20 世紀は工業社会であり、大量生産・大量消費を前提に匿名大衆を取引の対象とした企業活動によって経済が成長し、石油資源が不可欠でした。一方、21 世紀はデジタル社会であり、個人情報収集してパーソナライズされたサービスを提供するような顧客を取引の対象とした企業活動によって経済が成長しており、データが不可欠になっています。

こうした社会を「データ資本主義」と言い、ヒト、モノ、カネに並び、データが企業の資本になる時代がやってきています。

②情報（データ）管理が重要に

デジタル社会においては大量のデータが蓄積されることとなりますが、一方で情報が漏洩したり、不適切に利用されることで、個人のプライバシーが侵害されるなどのリスクが内在しています。

そこで、EU では GDPR によって規制を強化したり、GAFA に代表される巨大プラットフォームを規制するような動きがあります。また、個人情報個人が管理する「データポータビリティ」の考えも生まれており、情報銀行構想が試験的に始まっています。

③AI 時代におけるリスク

このようにデジタル社会が進展する中で、重要なキーテクノロジーの一つに「AI（人工知能）」があります。第3次ブームと言われている AI ですが、ディープラーニングに代表される機械学習の進展によって、AI が社会に深く浸透しています。一方、『Google Photos が黒人をゴリラと誤認』『マイクロソフトの AI がヘイト発言を「学習」して停止』など、AI に関するトラブルも発生しています。

分類や回帰といった高度な統計的処理によって判断をするのが AI の本質ですので、AI が出した答えは確率的にこのくらい正しいというものですので、誤認識も発生します。また、データを使って機械学習を行うことで AI が作られて成長するわけですが、学習の過程で、汚れたデータや偏りのあるデータが使われると、AI が出した答えの信ぴょう性は低くなります。

従来のプログラムは、決定論として演繹法的に作成されたものであり、答えが間違っているのはプログラムに瑕疵があるということになります。一方、AI は、確率論として帰納法的に作成されたものであり、答えが間違っているのは、学習が足りなかったり、適切なデータが使われていなかったりということになります。AI の多くが「統計的機械学習」といわれる手法を使っているため、精度として「100%」の保証が永久にできないというリスクが存在しています。

④AI システムをどう監査するのか？

システム監査の目的は、情報システムにまつわるリスクに適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすことです。

AI が企業活動に利用されるようになると、システム監査人は上記したような AI 特有のリスクを理解した上で、AI を「点検・評価・検証」しなければなりません。PoC（実証実験）を通じて AI の導入を決める手順が一般的になっていますが、こうした過程で監査に必要な記録を残せるのか？ 精度は企業リスクを想定した KPI をもとに算出する必要がありますが、経営者を巻き込んで検討が行われているのか？

AI の判断について企業に説明責任が求められるようになっていきます。一般的に保管・記録しておくべき情報は、モデルの再現が可能な情報です。そのためには、以下のような記録が残されている必要があります。

- ・学習データ関連（学習データ、データ定義）
- ・学習方法関連（アルゴリズム、パラメーター）
- ・精度確認結果（精度確認に使用したデータ、精度指標値）

こうした記録をもとに、AI システムを監査することになると考えられます。

⑤人間中心の AI 社会原則（内閣府）

内閣府の「統合イノベーション戦略推進会議」が、2019 年 3 月 29 日に『人間中心の AI 社会原則』を発表しました。その中では、以下の 3 つの価値を理念として尊重し、その実現を追求する社会を構築していくべきと書かれています。

- ・人間の尊厳が尊重される社会（Dignity）
- ・多様な背景を持つ人々が多様な幸せを追求できる社会（Diversity & Inclusion）
- ・持続性ある社会（Sustainability）

そして、以下のように人間が中心となって AI 社会を作らなければならないと提言しています。

AI を用いて複雑な処理を機械にある程度任せられることが可能になっても、「何のために AI を用いるのか」という目的設定は人間が行う必要がある。

AI は、社会を良くするために使うことも可能であれば、望ましくない目的達成のために使われたり、無自覚に不適切に使われたりすることもありうる。

そのため、我々は、「何のために AI を用いるのか」に答えられるような「人」、「社会システム」、「産業構造」、「イノベーションシステム」、「ガバナンス」の在り方について、技術の進展との相互作用に留意しながら考える必要がある。

原則の中にある「公平性、説明責任及び透明性の原則」には、以下のように書かれています。

AI の利用によって、人々が、その人の持つ背景によって不当な差別を受けたり、人間の尊厳に照らして不当な扱いを受けたりすることがないように、公平性及び透明性のある意思決定とその結果に対する説明責任（アカウンタビリティ）が適切に確保されると共に、技術に対する信頼性（Trust）が担保される必要がある。

このような国の動向も踏まえながら、AI 時代のシステム監査のあり方を今後も考えていく必要があると思います。

（資料作成にあたり参考にしたサイトおよび書籍）

Work × IT 働くを IT で心地よく <https://workit.vaio.com/i-digital-transformation/>

情報コンプライアンス研究室 https://www.infocomp-labo.jp/articles/about_gafa_regulations_in_japan/

WIRED <https://wired.jp/2018/01/18/gorillas-and-google-photos/>

WIRED <https://wired.jp/2016/03/25/tay-tweet-microsoft/>

日経 xTECH 「AI システムの作り方」

<https://tech.nikkeibp.co.jp/atcl/nxt/mag/sys/18/091800037/010800004>

人間中心の AI 社会原則 <https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/aigensoku.pdf>

「AI をビジネスに実装する方法」（著者：岡田陽介、出版：日本実業出版社）

◇ 研究報告 2

「CIS Controls の概要」

報告者 (会員番号 1281 宮本茂明)

経済産業省の「サイバー・フィジカル・セキュリティ対策フレームワーク」から"CIS CSC : Critical Security Controls V6"として参照されている CIS Controls の概要について報告する。

CIS Controls は、米国の非営利団体 The Center for Internet Security(CIS)より発行されている情報セキュリティ対策と管理策の優先付けされたガイドラインである。最新版は、V7.1 (2019 年 4 月) がリリースされている。

[<https://learn.cisecurity.org/control-download>]

現在、多種多様な情報セキュリティの標準、フレームワーク、ガイドライン等があり、セキュリティ対策のための選択肢が混沌(Fog of More)とした状況にある。CIS Controls は、様々なセキュリティ対策におけるこれらの「膨大な選択肢による混沌」を解決することを目的としている。

実施すべきセキュリティ対策を以下の 20 領域に分類し、現在発生しているサイバー攻撃と今後近いうちに発生が予測されるサイバー攻撃への具体的な管理策を、それぞれの領域ごとに示している。既知の攻撃を阻止できる効果が明らかになっている管理策が組み込まれている。

1	ハードウェア資産のインベントリとコントロール	11	ファイアウォール、ルータ、スイッチなどのネットワーク機器のセキュアな設定
2	ソフトウェア資産のインベントリとコントロール	12	境界防御
3	継続的な脆弱性管理	13	データ保護
4	管理権限のコントロールされた使用	14	Need-to-Know に基づいたアクセスコントロール
5	モバイルデバイス、ラップトップ、ワークステーションおよびサーバに関するハードウェアおよびソフトウェアのセキュアな設定	15	無線アクセスコントロール
6	監査ログの保守、監視および分析	16	アカウントの監視およびコントロール
7	電子メールと Web ブラウザの保護	17	セキュリティ意識向上トレーニングプログラムを実施する
8	マルウェア対策	18	アプリケーションソフトウェアセキュリティ
9	ネットワークポート、プロトコル、およびサービスの制限およびコントロール	19	インシデントレスポンスと管理
10	データ復旧能力	20	ペネトレーションテストおよびレッドチームの訓練

CIS Controls の各管理策の実装について、グループ分け (IG1 : 従業員 10 人程の小規模企業、IG2 : 中小企業、IG3 : 大企業) されており、企業規模に合わせて実装すべきベースラインが示されている。

企業規模に応じて、管理策として具体的に実施すべき事項が示されているので、各企業が情報セキュリティ対策を策定するにあたって、実装の優先度をつけたロードマップを考える上で有効なガイドラインとなっていると考える。

以上
<目次>

支部報告【 近畿支部 システム監査 基本学習セミナー 】

会員番号 2700 石嶋藤代（近畿支部）

1. テーマ 「システム監査の基本、および、監査プロセスの概要について」
2. 講師 【講義の部】 三橋潤 氏（近畿支部）
【演習の部】 浦上豊蔵 氏（近畿支部）
3. 開催日時 2019 年 11 月 30 日（土） 13:00～17:00
4. 開催場所 大阪市立大学 梅田サテライト 文化交流センター 大セミナー室
5. 講座概要

「システム監査」に興味を持っていただくことを目的として、「システム監査の基本」について二部構成のセミナーを開催した。

【講義の部】 システム監査の手順と技法概説

【演習の部】 情報処理技術者試験（過去問題）を題材としたシステム監査の演習

本セミナーでは、システム監査の理論だけでなく、講師の実務ノウハウをからめた「システム監査の基本」について解説した。

【講義の部】 システム監査の手順と技法概説**（１）システム監査とは**

「監査」および「システム監査」とは何か。システム管理基準・システム監査基準はどのように構成されているのか。「システム監査」と「情報セキュリティ監査」の対象範囲は重複する部分があるものの、システム監査の方が広く、情報システムそのものだけでなく、情報システムに係る業務すべてを対象としている。

**（２）システム監査実施手順について**

システム監査は、①監査計画→②予備調査→③本調査→④評価・結論→⑤監査報告の順で実施し、各工程ごとに残すべきアウトプットが存在する。

- ① 監査計画においては、まず監査依頼者（内部監査担当など）にヒアリングした内容を基に、トップヒアリングシート・現状調査票・自己評価票を作成する。その後、トップインタビューを実施してインタビュー結果を記載し、監査テーマ設定後、監査個別計画書を作成する。
- ② 予備調査では、被監査部門からのインタビュー、アンケートやマニュアル類等の情報収集により監査対象の業務概要を把握し、「監査手続」を監査チェックリストに記載する。
- ③ 本調査では、「監査手続」に従って、監査対象のコントロールを検証し、客観的な監査証拠に基づいて

問題点を抽出し、問題が HW、SW、要員、手続等のどこに起因するのかを明確にする。本調査における確認結果は「監査調書」として監査チェックリストに追記する。

- ④ 評価・結論では、予備調査・本調査で収集した監査証拠を整理分析し、監査対象のコントロール状況を評価する。監査結果の評価において、単に、できている／できていない、といった評価ではなく、監査項目に対して評価基準や重みづけを設定しておき、監査結果を定量化して示すことが有効である。評価結果として、問題点・指摘事項評価点等を記録する。

- ⑤ 監査報告では、監査報告書を作成する。監査報告書作成においては、まず監査証拠に基づいた評価・結論の結果を、監査人の意見、発見した問題点と改善策を中心に、システム監査報告書原案を作成する。

作成した原案に基づいて、関係部署に事実誤認の有無や改善勧告レベル等について意見交換を行い、それらを踏まえてシステム監査報告書を完成させる。

システム管理基準等を Excel 化して、予備調査や本調査の調査内容を記入できる様式の監査チェックリストを作成しておくとなつた有効なツールとなる。このツールを活用すれば、予備調査の結果から本調査へ進む管理項目が簡単にわかるなど、監査作業を効率できる以外に、分析や成熟度評価にも利用可能となつたといったメリットがある。

（３）システム監査の手法・技法

監査技法には多くの技法があるが、主に活用する技法としては、チェックリスト法、ドキュメントレビュー法、突合・照合法、現地調査法、インタビュー法などがある。

（４）効果のあるシステム監査

企業経営に役立つシステム監査において重要となるポイントおよびシステム監査とコンサルティングの違いとは何か、について説明があり、講義の部は締めくくられた。

【演習の部】情報処理技術者試験（過去問題）を題材としたシステム監査の演習

（１）午前Ⅱ 選択式問題を例に演習と解説

システム監査手順、監査証拠、改善勧告、ITAC と ITGC、試査・サンプリングに関する過去問題を受講者に出題。実際の試験における制限時間（１問あたり 90 秒）を体感できるように、時間計測し、時間内で問題を解く形式で実施した。問題の解説だけでなく、講師から内部統制に係わるシステム管理基準（追補版）および運用評価のサンプリングについて、補足資料による解説が行われた。



（２）午後Ⅰ 記述式問題を例に演習と解説

直近４年の出題テーマについての説明後、そのうちの１問、「基幹システムのオープン化の監査」に関する問題を受講者に出題。まず、講師から「問題文の読み方」についての説明があり、各自で問題の読込を行った。その後、グループに分かれ、問題を解く過程の理解を深められるように、討議を行い、グループごとに解答をまとめ、提出していただいた。

最後に講師から、グループごとの答案の紹介および解答の解説が行われた。

6. 所感

筆者は日常業務ではシステム開発に携わっており、システム監査の実務経験は無い。本セミナーにスタッフとして参画することでシステム監査の実務をイメージでき、違った観点からシステム開発業務を考察できるようになり、今後の業務に役立つ良い経験となった。また、本セミナーは情報処理技術者試験の対策を目的とした受講者が多く、「午後Ⅰの問題を使った疑似体験を行う演習は有効であると感じた」といった感想等があり等好評であった。受講者にとっても有意義なセミナーになったと感じている。

以上

<目次>



【 注目情報（2019 年 12 月 ～ 2020 年 1 月） 】**■「2020年4月に施行される改正民法に対応した「情報システムモデル取引契約書」を公開
【IPA】 2019/12/24**

システム開発などの契約に関する債権法を見直した改正民法が 2020 年 4 月に施行されることを受け、IPA は、経済産業省が 2007 年に公開した「情報システム・モデル取引・契約書」のうち民法改正に直接関係する論点を見直した「情報システム・モデル取引・契約書」＜民法改正を踏まえた、第一版の見直し整理反映版＞を公開しました。

例えば、民法改正で、請負契約における瑕疵担保責任が契約不適合責任へ再構成され、責任の存続期間が最長 10 年間に延長されました。改正前の瑕疵担保責任の存続期間は目的物の引渡時／仕事の終了時から 1 年でしたが、改正後の契約不適合責任では契約不適合を知った時から 1 年以内に通知をすればよいことになり、注文者が契約不適合を「知る」までの間は、消滅時効一般の規定に基づき、10 年間権利の行使ができることとなりました。＜見直し整理反映版＞では、期間制限は検収完了時という客観的な起算点は維持しつつ、IT ベンダーの落ち度に起因する場合等を適用除外にするといった点が追加されています。

尚、IPA では、DX 時代に求められるアジャイル開発への対応や、セキュリティ対策関連など、民法改正に直接かわらない点を含めた改訂版を 2020 年中に公開する予定です。

URL : <https://www.ipa.go.jp/ikc/reports/20191224.html>

<目次>

2020.01

【 協会主催イベント・セミナーのご案内 】

■ SAAJ システム監査実務セミナー（東京：日帰り 4 日間コース）

第 3 5 回	日時	2020 年 3 月 7 日(土)～ 8 日(日) 2020 年 3 月 21 日(土)～22 日(日) 土曜は 9:30～18:30、日曜は 9:30～17:00
	場所	市ヶ谷健保会館 〒162-0064 東京都新宿区市谷仲之町 4-39
	概要	金融系データセンタにおけるシステム運用に関する監査
	参加費	132,000 円（日本システム監査人協会会員） 154,000 円（一般） （費用には、教材費・消費税が含まれます。）
	副教材	情報システム監査実践マニュアル(第 2 版) 森北出版社
	定員	定員 20 名（最小催行人員 6 名） 応募締切日：2 月 10 日（月）
	お申込み	https://www.saaj.or.jp/kenkyu/jitsumuseminar/jitsumuseminar35.html

■ SAAJ 月例研究会（東京）

第 2 5 0 回	日時	2020 年 3 月 17 日(火) 18:30～20:30
	場所	機械振興会館 地下 2 階ホール
	テーマ	コーポレートガバナンスコード時代の IT ガバナンス ～ガバナンス機関から内部監査部門への期待～
	講師	一般社団法人 実践コーポレートガバナンス研究会 理事 大谷 剛 氏
	講演骨子	2018 年に一回目の改訂を受けたコーポレートガバナンス コードに対して、所謂「フルコンプライ」を表明する会社は決して珍しくなくなった。 上場各社にとって、同コードへの外形的準拠はもはや所与の条件である。一方同コード の本質は取締役会の在り方を、マネジメント型からモニタリング型への移行を促進する 点にあり。この本質を如何に捉えて実現していくか、そのプロセスをステークホル ダーに対して透明性をもって説明していくことが、次の段階として各社に求められるタ スクとなる。このプロセスを確行するため、取締役会が取り組むべき今日的課題を俯瞰 し、IT ガバナンスに関する論点を整理する。さらに内部監査部門を課題解決ための重 要なプロフェッショナル・パートナーとして再定義し、双方の新たな関係性について考 察する。
	参加費	SAAJ 会員 1,000 円 非会員 3,000 円
	お申込み	後日協会ホームページに掲載します。

■ SAAJ 月例研究会（東京）

第 251 回	日時	2020 年 4 月 10 日(金) 18:30~20:30
	場所	機械振興会館 地下 2 階ホール
	テーマ	マネロン・テロ資金供与対策と IT システムの活用
	講師	弁護士 鈴木 正人氏 ニューヨーク州弁護士登録。金融庁・証券取引等監視委員会にて執務経験あり。主な業務は金融・証券規制の助言、マネロン・テロ資金供与対策、反社対応、ガバナンス・コンプライアンス態勢構築支援、IT・パーソナルデータ規制対応、M&A、訴訟紛争対応その他一般企業法務。
	講演骨子	近時、金融機関を中心とした企業につきマネロン・テロ資金供与対策を講じることの重要性が高まってきている。同対策においては IT システムの活用が重要となる。本研究会では、マネロン・テロ資金供与対策の背景・必要性やリスクベース・アプローチの重要性、個別対策の概要を説明した上で IT システムの活用の重要性について検討する。
	参加費	SAAJ 会員 1,000 円 非会員 3,000 円
	お申込み	後日協会ホームページに掲載します。

<目次>



2020.01

協会からのお知らせ（予告）【第19期通常総会の開催】

会員番号 2581 斉藤茂雄（事務局長）

日本システム監査人協会（SAAJ）会員各位**■第19期通常総会のご案内**

日本システム監査人協会の第19期通常総会を、下記の通り開催致します。

万障お繰り合わせの上ご出席をお願い申し上げます。

総会、懇親会の参加申込は 2020 年 2 月初より、協会ホームページにて受け付けます。

https://www.saa-j.or.jp/soukai/tsujou_19_soukai.html

1. 日時：2020 年 2 月 21 日（金） 13 時 30 分～（受付開始：13：00）

2. 場所：東京都港区芝公園 3 丁目 5 番 8 号 機械振興会館 地下 3 階 研修 1 室

アクセス：<http://www.jspmi.or.jp/kaigishitsu/access.html>

3. 第19期通常総会 議事（予定） 13 時 30 分～15 時

13:30 開会

(1) 2019 年度 事業報告の件

(2) 2020 年度 事業計画の件

(3) 2020 年度 予算の件

(4) 理事選任の件

(5) その他

15:00 閉会

（休憩）

4. 特別講演 15 時 30 分～17 時

15:30 開演

演題：日本企業の IT ガバナンスの将来

講師：日本 IT ガバナンス協会 理事長 松原榮一 氏

※ CPE：5H で申請できます

17:00 閉演

5. 懇親会 17 時 30 分～19 時

17:30 開場（機械振興会館 5 階 倶楽部 1）

19:00 閉場

以上
<目次>

【 新たに会員になられた方々へ 】



新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。
協会の活用方法や各種活動に参加される方法などの一端をご案内します。

**ご確認
ください**

- ・ ホームページでは協会活動全般をご案内 <http://www.saa-j.or.jp/index.html>
- ・ 会員規程 http://www.saa-j.or.jp/gaiyo/kaiin_kitei.pdf
- ・ 会員情報の変更方法 <http://www.saa-j.or.jp/members/henkou.html>

特典

- ・ セミナーやイベント等の会員割引や優遇 <http://www.saa-j.or.jp/nyukai/index.html>
公認システム監査人制度における、会員割引制度など。

**ぜひ
ご参加を**

- ・ 各支部・各部会・各研究会等の活動。 <http://www.saa-j.or.jp/shibu/index.html>
皆様の積極的なご参加をお待ちしております。門戸は広く、見学も大歓迎です。

**ご意見
募集中**

- ・ 皆様からのご意見などの投稿を募集。
ペンネームによる「めだか」や実名投稿には多くの方から投稿いただいております。
この会報の「会報編集部からのお知らせ」をご覧ください。

出版物

- ・ 「発注者のプロジェクトマネジメントと監査」「情報システム監査実践マニュアル」「6か月で構築する個人情報保護マネジメントシステム」などの協会出版物が会員割引価格で購入できます。
<http://www.saa-j.or.jp/shuppan/index.html>

セミナー

- ・ 月例研究会など、セミナー等のお知らせ <http://www.saa-j.or.jp/kenkyu/index.html>
月例研究会は毎月100名以上参加の活況です。過去履歴もご覧になれます。

**CSA
・
ASA**

- ・ 公認システム監査人へのSTEP-UPを支援します。
「公認システム監査人」と「システム監査人補」で構成されています。
監査実務の習得支援や継続教育メニューも豊富です。
CSAサイトで詳細確認ができます。 <http://www.saa-j.or.jp/csa/index.html>

会報

- ・ 過去の会報を公開 <https://www.saa-j.jp/03Kaiho/0305kaihoIndex.html>
会報に対するご意見は、下記のお問合せページをご利用ください。

**お問
い合
わせ**

- ・ お問い合わせページをご利用ください。 <http://www.saa-j.or.jp/toiawase/index.html>
各サイトに連絡先がある場合はそちらでも問い合わせができます。

<目次>

【 S A A J 協会行事一覧 】 赤字：前回から変更された予定			2020.01
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
1 月	7：総会資料提出期限 16:00 7：役員改選公示（1/21 立候補締切） 9：理事会：総会資料原案審議 21：17:00 役員立候補締切 31：償却資産税・消費税申告	1-31：CSA・ASA 更新申請受付 21：春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕 21：第 249 回月例研究会	8：支部会計報告期限
2 月	1：2019 年度会計監査 1：総会申込受付開始（資料公表） 6：理事会：通常総会議案承認 29：2020 年度年会費納入期限	2/1-3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	21：第 19 期通常総会
3 月	6：年会費未納者宛督促メール発信 12：理事会 27：法務局：資産登記、理事変更登記 活動報告書提出 東京都：NPO 事業報告書提出	1-31：春期 CSA・ASA 書類審査 17：第 250 回月例研究会	
4 月	9：理事会	初旬：春期 CSA・ASA 書類審査 10：第 251 回月例研究会 中旬：春期 ASA 認定証発行	19：春期情報技術者試験
5 月	14：理事会	中旬・下旬土曜：春期 CSA 面接	
6 月	1：年会費未納者宛督促メール発信 11：理事会 20：年会費未納者督促状発送 21～：会費督促電話作業（役員） 28：支部会計報告依頼（〆切 7/13） 30：助成金配賦額決定（支部別会員数）	中旬：春期 CSA 面接結果通知 下旬：春期 CSA 認定証発送	認定 NPO 法人東京都認定日 （2015/6/3）
前年度に実施した行事一覧			
7 月	5：支部助成金支給 11：理事会	18～19：第 34 回システム監査実践セミナー （日帰り 2 日間コース） 22：月例研究会 中旬：秋期 CSA・ASA 募集案内	14：支部会計報告〆切 20：PMS ハンドブック V2 出版
8 月	（理事会休会） 24：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	
9 月	12：理事会	5-6：第 34 回システム監査実務セミナー（日 帰り 4 日間コース）前半 11：第 245 回月例研究会 19-20：第 34 回システム監査実務セミナー 後半 ～ 秋期 CSA・ASA 募集中 ～9/30 迄	
10 月	10：理事会	8：第 246 回月例研究会	19：秋期情報処理技術者試験 26：活動説明会
11 月	14：理事会 14：予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/8〆切） 15：2020 年度年会費請求書発送準備 26：会費未納者除名予告通知発送 30：本部・支部予算提出期限	8：第 247 回月例研究会 中旬：秋期 CSA 面接 下旬：CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 下旬：CSA 面接結果通知	23：「2019 年度西日本支部合同研 究会 in OSAKA」 30：近畿支部主催 システム監査 基本学習セミナー
12 月	1：2019 年度年会費請求書発送 1：個人番号関係事務教育 12：理事会：2020 年度予算案 会費未納者除名承認 第 19 期総会審議事項確認 13：総会資料提出依頼（1/7〆切） 13：総会開催予告掲示（役員改選あり） 20：2019 年度経費提出期限	13：第 248 回月例研究会 16：CSA/ASA 更新手続案内メール 〔申請期間 1/1～1/31〕 19-20：第 35 回システム監査実践セミナー 26：秋期 CSA 認定証発送	12：協会創立記念日

<目次>

【 会報編集部からのお知らせ 】

1. 会報テーマについて
2. 会報バックナンバーについて
3. 会員の皆様からの投稿を募集しております

□ ■ 1. 会報テーマについて

2020 年の会報年間テーマは

「システム監査人のターニングポイント」です。

システム監査の過去、未来においてターニングポイントとなった①外部環境の変化、②技術的な変化、③今後予想されることを焦点に議論し、お互いの知見や意見を交換することを目的として設定しました。

参考までに例示を紹介させていただきます。

- ①の例示：マイナンバー制度
- ②の例示：クラウドコンピューティング、ブロックチェーン
- ③の例示：AI、自動運転、IoT、ビッグデータ等に関する技術的な進展と法制度

あくまでも例示ですのでこれらにとらわれる必要はありません。

会報テーマ以外の皆様任意のテーマもちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

□ ■ 2. 会報のバックナンバーについて

協会設立からの会報第1号からのバックナンバーをダウンロードできます。

<https://www.saaj.jp/03Kaiho/0305kaihoIndex.html>

□ ■ 3. 会員の皆様からの投稿を募集しております。

募集記事は次の通りです。

□ ■ 募集記事		
1.	めだか	匿名（ペンネーム）による投稿 原則 1 ページ ※Word の投稿用フォーム（毎月メール配信）を利用してください。
2.	記名投稿	原則 4 ページ以内 ※Word の投稿用フォーム（毎月メール配信）を利用してください。
3.	会報掲載論文 (投稿は会員限定)	現在「論文」の募集は行っておりません。

■ 投稿について 「会報投稿要項」

- ・ 投稿締切：15 日（発行日：25 日）
- ・ 投稿用フォーマット ※毎月メール配信を利用してください。
- ・ 投稿先： saajeditor@saaj.jp 宛メール添付ファイル
- ・ 投稿メールには、以下を記載してください。
 - ✓ 会員番号
 - ✓ 氏名
 - ✓ メールアドレス
 - ✓ 連絡が取れる電話番号
- ・ めだか、記名投稿には、会員のほか、非会員 CSA/ASA、および SAAJ 関連団体の会員の方も投稿できます。
 - ✓ 会員以外の方は、会員番号に代えて、CSA/ASA 番号、もしくは団体名を表記ください。

■ 注意事項

- ・ 原稿の主題は、[定款](#)に記載された協会活動の目的に沿った内容にして下さい。
- ・ 特定非営利活動促進法第 2 条第 2 項の規定に反する内容（宗教の教義を広める、政治上の主義を推進・支持、又は反対する、公職にある者又は政党を推薦・支持、又は反対するなど）は、ご遠慮下さい。
- ・ 原稿の掲載、不掲載については会報部会が総合的に判断します。
- ・ なお会報部会より、表現の訂正を求め、見直しを依頼することがあります。また内容の趣旨を変えずに、字体やレイアウトなどの変更をさせていただくことがあります。

お問い合わせ先： saajeditor@saaj.jp

<目次>

会員限定記事

【本部・理事会議事録】（会員サイトから閲覧ください。会員パスワードが必要です）

https://www.saa-j.or.jp/members_site/KaiinStart

ログイン ID（8 桁）は、年会費請求書に記載しています。

=====

■発行：認定 NPO 法人 日本システム監査人協会 会報編集部

〒103-0025 東京都中央区日本橋茅場町 2 - 8 - 8 共同ビル 6F

■ご質問は、下記のお問い合わせフォームよりお願いします。

【お問い合わせ】 <http://www.saa-j.or.jp/toiawase/>

■会報は、会員宛の連絡事項を記載し登録メールアドレス宛に配信します。登録メールアドレス等を変更された場合は、会員サイトより訂正してください。

https://www.saa-j.or.jp/members_site/KaiinStart

掲載記事の転載は自由ですが、内容は改変せず、出典を明記していただくようお願いします。

■□■ S A A J 会報担当

編集委員：桜井由美子、安部晃生、越野雅晴、竹原豊和、豊田諭、福田敏博、柳田正、山口達也

編集支援：会長、各副会長、各支部長

投稿用アドレス：saa-jeditor ☆ saa-j.jp（☆は投稿時には@に変換してください）

Copyright(C)1997-2020、認定 NPO 法人 日本システム監査人協会

<目次>