認定 NPO 法人
日本システム監査人協会報
2020 年 3 月号
No.228
No.228（2020 年 3 月号）<2 月 25 日発行>

2月1日～3月18日は

「サイバーセキュリティ月間」です。

サイバーセキュリティに関する普及啓発強化を推進しましょう！

✧#サイバーセキュリティは全員参加

画像提供：西場師守

巻頭言

『正解なき時代のアジャイル的経営』

会員番号:0555　松枝憲司（副会長　IT アセスメント研）

デジタル経済社会に突入している今、既存のビジネスモデルや市場、金融、税制までも根底から覆されそうとしており、ダイナミックに変化し続ける経営環境に従来のビジネスが立ち行かなくなってきた多くの事業者は、新たなビジネスモデルへの転換を余儀なくされている。しかしながら、このような複雑な環境下でかつ加速度的変化に対して、果たして自らの「正解」を見つけることができるのか。そもそも「正解」が存在しているのだろうか。企業の戦略を検討する場合、これまでは経営戦略に関する様々な理論やモデル、法則といったものを参考にしたものであった。それらに共通しているのは「論理的思考」をベースにしたものであり、問題への正解にたどり着くための方法論であった。しかし「正解」が存在しないもしくは「正解」が変化し続けているとすれば、論理的思考を試みただけでは進むべき道を見つけることはできない。

これに関連して 2018 年のシステム管理基準の改訂で「全体最適化」の考え方を止めたことが思い出される。従来のシステム管理基準では「Ⅰ.情報戦略 1.全体最適化計画の策定と承認」から始まっていた。言い換えると最初に全体最適化計画という「正解」を描いてから、それに向かって各情報化の計画に落とし込もうとするものであった。しかしこれも「全体最適解は存在しない」経営環境となったため取り下げられたと筆者は考えている。そして全体最適化に代わって採用されたのが、EDM モデルによる IT ガバナンスであった。IT ガバナンスは、経営陣が指示した方針に基づくマネジメント層の計画等を評価し、活動状況を常にモニタリングし、目標に達しなければ変更の方針を指示して随時計画を変更させていく。

不確実で複雑な環境下で何が正解かわからない時代には、いち早く新サービスを立ち上げてトライアンドエラーを繰り返してより良いものに変化していくことが正解に近づいていく有力な方策の一つである。そして早期にサービスを実現させる手段としてのアジャイル開発の採用は不可欠であり、それに同期して有効な IT ガバナンスを発揮するアジャイル的経営が目指すべき一つのモデルかもしれない。

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**
『正解なき時代のアジャイル的経営』

1．めだか **3**
【システム監査人のターニングポイント – サービスとコントロールを考える】

2．投稿 **4**
【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？（3)】
【書評　『ひとり情シス「セキュリティ寺」へ駆け込む！』】

3．本部報告 **9**
【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 3 章 個別検討事項】
【第 249 回月例研究会：講演録 クラウドサービスの安全性評価に関するガイドラインについて】

4．支部報告 **15**
【北海道支部　2020 年 1 月の月例研究会】

5．注目情報 **19**
【「情報セキュリティ 10 大脅威 2020」を決定　IPA】
【サイバーセキュリティ月間　NISC】

6．セミナー開催案内 **20**
【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 **22**
【２０２０年度春期 公認システム監査人及びシステム監査人補の募集】
【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 **26**

2020.02

めだか　【　システム監査人のターニングポイント –　サービスとコントロールを考える　】

経済発展に向けてイノベーションとともに情報サービスなどのサービス事業の展開が期待されている。サービス事業の基盤は、情報システムとデータであり、システム監査の対象でもある。サービス事業に関わる SOC（Service Organization Control）では、事業者は、アメリカ公認会計士協会（AICPA）とカナダ公認会計士協会（CICA）が制定した「トラストサービスの原則と基準（Trust Services Principles and Criteria）」に基づいて評価される。

SOC が会計士協会の制定した原則と基準に依拠するのは内部統制（internal control）という背景があり、内部統制はリーマン・ショックの再発防止のため財務報告の信頼性確保や不正取引を防止するプロセスの整備と運用を図るものである。内部統制は、事業者が、業務の有効性と効率性、財務報告の信頼性、事業活動に関わる法令等の遵守、資産の保全という 4 つの目的を達成していることの合理的な保証が得られるために、業務のプロセスが、統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング及び IT への対応という 6 つの基本的要素を組み込んで全ての従業者によって行われている必要がある。

SOC は、内部統制から導かれた、セキュリティ（security）、可用性（availability）、処理の整合性（processing integrity）、機密性（confidentiality）、プライバシー（privacy）の原則と基準である。

https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

クラウドサービスの情報セキュリティ規格は、「JIS Q 27017：2016 情報技術－セキュリティ技術－JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」である。序文に、“適切な情報セキュリティ管理策の選択及び提示されている実施の手引の適用は、リスクアセスメント及び法的、契約上、規制又はその他のクラウド分野固有の情報セキュリティ要求事項に依存する。”とあり、システム監査は、個々のクラウドサービスに適合した管理目的と管理策を選択して行うことになる。

1 月 21 日（火）開催の SAAJ 月例研究会は、「クラウドサービスに関する安全性評価制度について」をテーマに、総務省と経済産業省が 2020 年度中の制度立上げを目指し検討中の、府省庁から、独立行政法人、及び地方公共団体に適用されるクラウドサービスの安全性評価制度に関わる講演である。講演後の質疑応答を含め、白熱した研究会であり、また、SAAJ 公認システム監査人資格は同制度の監査人資格になるともいわれていた。

システム監査人は、情報システムとデータに関わるシステム監査を通じて、情報サービスなどのサービス事業の展開に寄与する監査人でありたい。（空心菜）

（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。）

<目次>

2020.02

【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？（3）

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

前々回より、「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 点の疑問であった。

・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？

前回も述べたように、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 月号)
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(⇒1 月号)
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

★今回は、④を取り上げることとします。

2.「平成」が「失われた 30 年」になった元凶④：「製造物責任法」(1994 年)の立法不備による、不備ソフトウェアの放置

まず、製造物責任法の条文を確認する。

（定義）
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。
２　この法律において「欠陥」とは、当該製造物の特性、その通常予見される使用形態、その製造業者等が当該製造物を引き渡した時期その他の当該製造物に係る事情を考慮して、**当該製造物が通常有すべき安全性**を欠いていることをいう。
３　略

（製造物責任）
第三条　製造業者等は、その製造、加工、輸入又は前条第三項第二号若しくは第三号の氏名等の表示をした製造物であって、**その引き渡したものの欠陥により他人の生命、身体又は財産を侵害したときは、これによって生じた損害を賠償する責めに任ずる**。ただし、その損害が当該製造物についてのみ生じたときは、この限りでない。

（免責事由）
第四条　前条の場合において、**製造業者等は、次の各号に掲げる事項を証明したときは、同条に規定する賠償の責めに任じない。**
一　当該製造物をその製造業者等が引き渡した時における科学又は技術に関する知見によっては、当該製造物にその欠陥があることを認識することができなかったこと。
二　当該製造物が他の製造物の部品又は原材料として使用された場合において、その欠陥が専ら当該他の製造物の製造業者が行った設計に関する指示に従ったことにより生じ、かつ、その欠陥が生じたことにつき過失がないこと。
伏期間が経過した後に症状が現れる損害については、その損害が生じた時から起算する。

（民法の適用）
第六条　製造物の欠陥による製造業者等の損害賠償の責任については、この法律の規定によるほか、民法（明治二十九年法律第八十九号）の規定による。

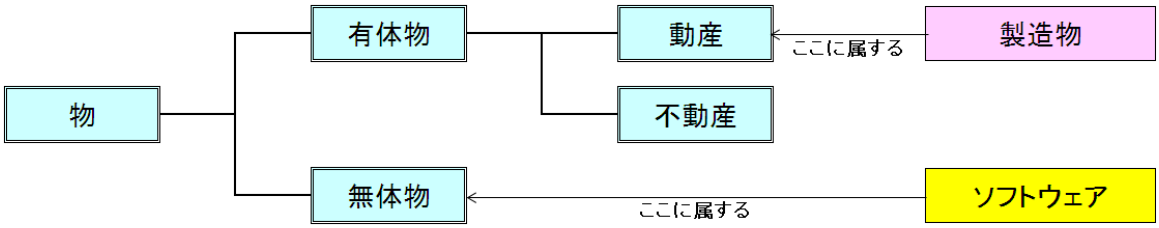
民法における損害賠償の根拠法は、債務不履行による損害賠償(415 条)と不法行為による損害賠償(709 条)である。これらと製造物責任法第 3 条による損害賠償について、近畿支部法制化研究会の神尾氏・中田氏・横山氏とともに纏めたものが、以下の表である。

損害賠償の根拠	根拠法	成立要件	時効(※1)		立証責任	ソフトウェアの不備の場合に、ユーザ側が損害賠償請求を行う場合のハードル
			主観的基準	客観的基準		
債務不履行	民法415条	債務者の帰責事由	5年	10年	原告(ユーザ)側	個別開発・個別仕様のソフトウェアの場合は、合意した設計書との差異について債務不履行を問えるが、パッケージ・ソフトの場合は難しい(※2)
不法行為	民法709条	故意又は過失	3年	20年	原告(ユーザ)側	「故意または過失」があったことの立証責任が原告(ユーザ)側にあるため、立証が困難
製造物責任法	製造物責任法第3条	債務者の帰責事由	3年	10年	被告(メーカー)側	ソフトウェアは適用対象外(下記参照)

※1. 2020年4月1日以降の新基準で記載。ただし、「生命・身体の侵害による損害賠償請求」については、債務不履行・不法行為ともに主観的基準は5年、客観的基準は20年である。
※2. 現在はパッケージ・ソフトが大半である。

原則として民事訴訟においては、原告側に立証責任がある。つまり、グレーであれば原告敗訴となる。この製造物責任法は、民法の特別法と位置付けられており、第 4 条において、立証責任が被告側に転換されている。例えば家電製品の欠陥により発火して家屋が全焼した場合、**当該製品が火災の原因ではなかったことを製造者側が証明**しなければならない（同様の規定は、自動車損害賠償保障法第 30 条などに見られる)。この点で、「製造物責任法」はユーザ側に有利な法律である。

しかしながら、ソフトウェアには適用されない。何故なら、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、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のである（会計上も「ソフトウェア」は無形固定資産である)。



このため、個別開発ではない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ような場合、メーカー側の責任を追及することが極めて困難となっている。これについては、法律が情報化社会の発展に追い付いていない例であり、何らかの法的な措置が必要であると思われる。

また、製造物責任法第 2 条第 2 項では、欠陥の定義として「当該製造物が通常有すべき安全性を欠いている」としている。つまり、「安全側故障」は適用対象外なのである。

3. システム監査人の”翻訳力”の重要性【システム監査専門家の出番】

システム開発の現場で、このような事例に遭遇したら、皆様ならどうされるだろうか？

【事例 A】「売上」の計上基準についてユーザ内の意見の統一が取れておらず、営業部が表計算ソフトで管理している売上高の数値の基準は「出荷時点」であり、経理部が管理している売上高の数値の基準は「検収時点」であったが、この調整が不備のままシステム開発が進行してしまった。

【事例 B】ユーザ側の幹部 X 氏は、①と②は理解していた。
①入出庫基準の『理論在庫数』(在庫帳)と『実在庫数』が異なる場合がある(棚卸差異)こと。
②入出庫基準の『理論在庫数』(在庫帳)と『売上仕入基準の理論在庫数（商品有高帳)』はタイムラグがあること。
⇒しかし、X は『実在庫数』と『売上仕入基準の理論在庫数』が同じにならねばならない、と思いこんでいて、両者の数値が一致しないのはバグであると強く主張した。

○事例 A：これはユーザの立場・職務経験による背景が大きく影響している。システム監査人としては、現場で「売上」という用語をどのような意味で用いているのか、しっかりと、ヒヤリングすることが必要である。一部の未熟な SE や PM は、このような場合、どちらか一方に統一しようとするが、それは多くの場合悲劇をもたらす。**このような微妙な差異を適切に"翻訳"できる能力こそが、AI 時代に負けないシステム監査人の素養として極めて重要**である。

この能力を養うには、「英語を科学する能力」を身につけることが最も有効であり、近道であると思われる。大学で英語とフランス語の比較、英語とドイツ語の比較を真剣に学んだ人は、この能力が高い傾向にあると思われる。これは、言語により、微妙な差異があることを日常的に経験できる為であろう。

★ベンダー側に「企業会計では、出荷時点で売上が原則である」と強弁する幹部クラスがいるケースも仄聞するが、これは論外。1 月号で取り上げた「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の当然の帰結である。なお、2021 年 4 月から強制適用となる企業会計基準第 29 号では、原則として「検収時点で売上」に統一されることに注意(⇒参考文献[2])。

○事例 B：論理学において「『P と Q は異なる』かつ『P と R は異なる』、故に、『Q=R』」となる筈が無い。そのような実現不可能な思いこみをユーザ側のキーマンが声高に主張した場合、これはシステム崩壊の危機である。このような概念の混乱が生じている場合、例えば、下記のような表が有効であろう。

各種の「在庫数」

※2021年4月から強制適用となる企業会計基準第29号では、制限される。

項番	在庫数の名称	理論値/実測値	定 義	仕入側			売上側			直送取引	
				入荷予定	入荷	仕入	出荷指示(引当)	出荷	売上	仕入	売上
1	有効在庫数	理論上の数値	引当可能数	増 ※1	増 ※1		減				
2	物流在庫数		入出庫基準の在庫数(入出庫表の在庫数) ※2		増			減			
	物流在庫数(保留品)										
3	経理在庫数		売上仕入基準の在庫数(商品有高帳の在庫数)			増			減	増	減
	経理在庫数(保留品)										
4	棚卸実在庫数	実測値	棚卸作業による実測数								
	棚卸実在庫数(保留品)										

※2021 年 4 月に強制適用される企業会計基準第 29 号により、直送取引の場合で「代理人」と認定される場合には「売上」と「仕入」の両建ては出来なくなるので、「増」「減」ともに無しである。

4. 補足 2：産業競争力の観点からの、「英語プラス 1」の語学力の必要性

前々回から指摘しているように、ドイツ語とフランス語の語学力は急務である。**2020 年 2 月 1 日欧州標準時午前 0 時**(日本時間同午前 8 時)を以って、**英国が EU(欧州連合)から離脱**した。2016 年 6 月 23 日の国民投票から 3 年半後のことであった。筆者は日本時間の 1 月 30 日未明、欧州議会の討論・投票の模様をリアルタイムで見ていた。表決の結果、621 対 49 の大差で、ブレグジット協定案は批准された。討論に際し、スコットランド選出の議員たちが涙を流し、表決後、議場ではスコットランドの非公式国歌ともされる名曲"Auld Lang Syne"(蛍の光)(英：Old Long Since,独：Alt Lang Seit)の大合唱となったのは感激的であった。ただ、この曲、もともとは「別れの曲」ではなく、「旧友との再会を懐かしむ曲」である。合唱したのが英国の離脱に反対する人々であったのはその為であろう。

しかし、日本では逆のニュアンスで伝えられていたように思われる。一種の「言葉の壁」と言えるであろう。また、我が国の評論家の意見を見聞する限り、「グローバリズムからの英国の独立」と捉える向きも多い。しかし、筆者は寧ろ逆であると考えている。実は、スコットランド・北アイルランドのみならず、英国の経済的弱者の多くが EU 残留を望んでいた。何故なら、RoHS 指令（Hg,Cd,Pb,Cr(Ⅵ)等の規制）を始めとする環境規制・食品安全・労働規制など、グローバリズムにとっては抑制要素となる規制は EU 法または EU 指令に根拠を有していたからである。これは英語一辺倒教育の弊害であろう。

※日本では殆ど知られていないが、実は、英国の貴族院にも政党がある。しかも、最大会派はなんと「労働党」である。何故なら、近年の上院改革により、約 800 人もいる貴族議員議員の内、英国国教会の聖職者を含む終身議員は 98 名であり、多くは Baron(男爵)や Sir だからである。

なお、一部で言われている「日本の参議院の権限が強すぎる」というのも誤りである。他の G7 諸国を見ると、米国もイタリアも上院・下院は対等である。ドイツの連邦参議院(Bundesrat)についても、州の利害に関する法律については「連邦議会(Bundestag)の 2/3 再可決による優越」は無いのである。

（実は、我が国の憲法第 59 条第 2 項の規定はドイツのワイマール憲法の規定と同じである。1934 年、ドイツは独裁政権の下、Reichsrat を廃止して一院制となったが、戦後の連邦参議院は権限を強化して復活した。G7 先進国で一院制は、この例のみである。）これも、英語一辺倒教育の弊害であろう。

英国の EU 離脱により、日本企業が英国を窓口として欧州市場にアクセスすることは従前より困難になると考えられる。2016 年 6 月 23 日の国民投票の時点では、1000 社余りの日本企業が欧州市場の統括子会社を英国においていたが、少なからぬ会社が、事業の縮小や工場の閉鎖、統括子会社の欧州大陸(パリ、フランクフルト、ベルリン等)への移動をせざるを得なくなった。EU 憲法によれば、加盟国は 1 個の言語のみを「公用語」として申請することができるが、英語を申請したのは英国のみである(アイルランドは「ゲール語」を申請)。従って、英語は暫定的に「作業言語」としては残るものの、EU の公用語でなくなる可能性はかなり高いようである。E U高官が 2017 年 6 月 28 日に**「公式の場では、フランス語とドイツ語の使用を増やす」**と明言するなど、EU 域内での英語の地位は急速に低下しつつある。

また、EU においては 2040 年以降、ガソリン車・ディーゼル社の販売が禁止されることが決まっていた。我が国の産業界の一部は、英国の EU 離脱により、英国市場での日本製のガソリン車・ディーゼル社の販売ができるものと受け止められていたが、2 月 4 日、英国のジョンソン首相は、突如、「同規制を英国では 5 年前倒しして 2035 年からとするとともに、**日本が優位性を持つハイブリッド・カーも禁止対象に含める**」と発表した(⇒参考文献(5))。また、昨年 12 月 18 日、フランスの自動車 PSA(Peugeot)と、イタリア系の FCA(Fiat-Chrysler Automobiles）の経営統合が発表された。（以前、旧米国 Gig 3 の Chrysler は、F1 で有名な Ferrari の傘下に入っている）。更に、2 月 11 日、英国の Johnson 首相は「英国と EU は FTA 無しも有り得る」と発言し、現地では大騒ぎになっている。このように我が国の自動車等の工業製品の欧州市場へのアクセスはハードルが高くなりつつある。特に、2020 年 1 月末時点でも、欧州における特許権・商標権等の審査においては、英語・フランス語・ドイツ語の三カ国語の書類の提出が義務づけられているが、今後の欧州における英語の地位の低下を考えると、欧州市場のアクセスのためには、**ドイツ語とフランス語が必要不可欠であることは明らか**であろう。早急に大学入試の外国語を 2 カ国語に増やすとともに、大学の卒業要件として外国語の 3 カ国語を義務化するへきである。（ドイツの高校(Gymnasium)では、3 カ国語の習得が必要であり、多くの場合、第 1 外国語：フランス語、第 2 外国語：英語、第 3 外国語：日本語/中国語/ラテン語）となっている。

※ラテン語は死語ではない。例えば EU の標語"In Varietate Concordia"(多様性の中の統合)はラテン語であり、EU 法に基づく法人組織「欧州会社」Societas Europaea もラテン語である(societas は女性名詞(第 3 変化)、europaea は europaeus(ギリシャ語 εὐρωπαῖος からの輸入語)の女性単数主格形)

我が国の工業製品の国際競争力を考えると、輸出先の国民に一定の購買力が必要である。一部のセレブ層がいることと、その国の国民全体に購買力があるかは別の問題である。従って、欧州市場へのアクセスの維持は、我が国の製造業にとっては死活問題である。このままでは、戦後、我が国の日本人は、欧米＝英米と考えてきたことのツケが来そうである。(⇒参考文献(2))

※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 の知恵に学べ　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、「在庫数・棚卸資産評価」再考(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）
(5)イギリス、2035 年からガソリン車とディーゼル車を販売禁止へ　5 年前倒し
https://www.newsweekjapan.jp/stories/world/2020/02/20355.php
(6)フィアットとプジョー、経営統合で正式合意
https://www.nikkei.com/article/DGXMZO53504050Y9A211C1MM8000/

<目次>

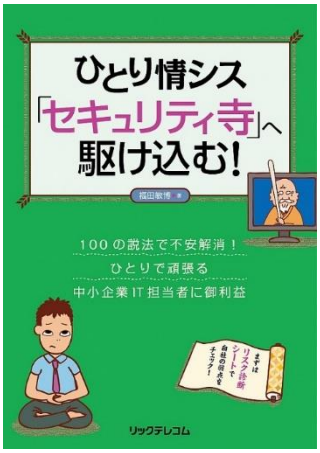
2020.2

投稿【　書評　『ひとり情シス「セキュリティ寺」へ駆け込む！』　】

会員番号　2574 竹原豊和

２月１日から３月 18 日までをサイバーセキュリティ月間として政府より発表されています。

昨今、企業活動及び個人の日常生活において、様々な種類のサイバーセキュリティ脅威があり、情報セキュリティやサイバーセキュリティへの対応は、今まで以上に重要視される時代になりました。また、システム監査という観点からも、情報セキュリティやサイバーセキュリティを踏まえたシステム監査への注目度が高まっており、今後はより一層、システム監査において情報セキュリティ及びサイバーセキュリティへの対応が求められるのでは、と考えます。



今回ご紹介する『ひとり情シス「セキュリティ寺」へ駆け込む！』は、日頃からセキュリティについて研究活動をされているＳＡＡＪ会員が執筆された書籍で、情報セキュリティ対策及びサイバーセキュリティ対策に有用な、様々な事故事例及びその対策方法を解説されており、単なる読み物という類のものではなく、現状の危険度チェックや実際の対策に向けた演習、具体的な対策例が掲載されており、とても読みごたえがある内容です。

情報セキュリティに関する解説に際しては、「富安野 仁里（ふあんの・ひとり）君」という、ひとり情シスを担当している主人公と、セキュリティ寺の「西場 師守（さいば・もろもり） 住職」の二人の会話形式で展開されており、この手の情報セキュリティ対策本の中ではとてもわかりやすい内容となっています。

今後、IT がより発展していくことは必然と考えられますが、本書を参考にすることで、日々の業務における情報セキュリティ対策及びサイバーセキュリティ対策のみならず、IT 時代の生活全般にもお役立ていただけるのではないかと思います。

書籍名：『ひとり情シス「セキュリティ寺」へ駆け込む！』

著者：福田 敏博（西場 師守）　発行：リックテレコム　A5 判（248 ページ）

<目次>

2020.02

【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３章 個別検討事項

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 日公表「個人情報保護法 いわゆる 3 年ごと見直し 制度改正大綱」について今回は第 3 章のポイントを見て行く。公表文書は分かりやすく記述されているので、全文は本文をご参照いただきたい。

→　https://www.ppc.go.jp/news/press/2019/20191213/

（記述について）□枠：2015 年改正法、個人情報保護委員会告示の条文

赤字：着目点、

青字：SAAJPMS 研究会のコメント

「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）

第 3 章 個別検討事項

第 1 節 個人データに関する個人の権利の在り方（抜粋）

5. 開示等の対象となる保有個人データの範囲の拡大

2015 年改正法　第 2 条（定義）7

この法律において**「保有個人データ」とは**、個人情報取扱事業者が、**開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止**を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間(*1：施行令第 5 条：6 月)以内に消去することとなるもの以外のものをいう。

（以下、「大綱」より抜粋）

○ （略）個人情報取扱事業者に請求に対応するコストを負担させることの不利益が、本人に開示等を請求する権利を認めることの利益を上回るとはいえないものと考えられる。（以下省略）

○ そこで、本人の開示等の請求対象となる保有個人データについて、保存期間により限定しないこととし、現在除外されている 6 か月以内に消去する短期保存データを保有個人データに含める。(*1)

6. オプトアウト規制の強化（抜粋）

(2)オプトアウトの対象となる個人データの限定（抜粋）

○ （略）、名簿の流通により本人の関与が困難となっている現状を踏まえ、オプトアウト届出事業者によって個人情報が不適切に取得されることがないよう、個人の権利利益を保護する観点から、オプトアウト規定に基づいて本人同意なく第三者提供できる個人データの範囲をより限定していくこととする。

※：2015 年改正法では要配慮個人情報だけが除外されている。(*2)

2015 年改正法　第 23 条（第三者提供の制限） (オプトアウト規制)

2　個人情報取扱事業者は、第三者に提供される個人データ（**要配慮個人情報を除く。**(*2)以下この項において同じ。）について、**本人の求めに応じて当該本人が識別される個人データの第三者への提供を**

停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人データの項目

三　第三者への提供の方法

四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

五　本人の求めを受け付ける方法

(3)届出対象事項の追加（抜粋）

○　（略）事業者の名称や住所といった基本的事項を届出事項として追加するとともに、変更があった場合の届出を求め、委員会がオプトアウト届出事業者の所在を把握できるようにする。

(4)第三者提供時の確認記録義務の開示義務化（抜粋）

○　（略）、第三者への提供時・第三者からの受領時の記録(*3)も、開示請求の対象とすることとする。

2015 年改正法　第 26 条（第三者提供を受ける際の確認等）（抜粋）

個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。（略）

一　当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者（略）の氏名

二　当該第三者による当該個人データの取得の経緯

2　(略)

3　個人情報取扱事業者は、第一項の規定による確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人データの**提供を受けた年月日、当該確認に係る事項その他の、個人情報保護委員会規則で定める事項に関する記録(*3)を作成しなければならない。**

4　個人情報取扱事業者は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間(*4)保存しなければならない。

＊4　法令に基づく場合等ただし書きにより、第三者提供を受けた場合：1 年を経過するまで
その他の方法により、第三者提供を受けた場合：3 年を経過するまで

第 2 節　事業者の守るべき責務の在り方（抜粋）

1 .漏えい等報告及び本人通知の義務化（抜粋）

○ 諸外国においては、多くの国で漏えい等報告が義務とされている。一方、 我が国では、制度上は努力義務である（以下省略）

○（略）　漏えい等報告(*5)について、法令上の義務として明記することとする。

＊5　個人情報保護委員会告示第 1 号における「漏えい等報告」が、明文化される可能性。

2017 年　個人情報保護委員会告示第 1 号
「個人データの漏えい等の事案が発生した場合等の対応について」

1.対象とする事案

本告示は、次の（1）から（3）までのいずれかに該当する事案（以下「漏えい等事案」と いう。）を対象とする。

（1）個人情報取扱事業者が保有する個人データ（特定個人情報に係るものを除く。）の漏えい、滅失又は毀損

（2）個人情報取扱事業者が保有する加工方法等情報（中略）の漏えい

（3）上記（1）又は（2）のおそれ

2.漏えい等事案が発覚した場合に講ずべき措置

個人情報取扱事業者は、漏えい等事案が発覚した場合は、次の（1）から（6）に掲げる事項について必要な措置を講ずることが望ましい。

（1）事業者内部における報告及び被害の拡大防止

責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。

（2）事実関係の調査及び原因の究明

漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。

（3）影響範囲の特定 上記(2)で把握した事実関係による影響の範囲を特定する。

（4）再発防止策の検討及び実施

上記（2）の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を速やかに講ずる。

（5）影響を受ける可能性のある本人への連絡等

漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係等について、速やかに本人へ連絡し、又は本人が容易に知り得る状態に置く。

（6）事実関係及び再発防止策等の公表

漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表する。

3.個人情報保護委員会等への報告 (*5)

個人情報取扱事業者は、漏えい等事案が発覚した場合は、その事実関係及び再発防止策等 について、個人情報保護委員会等に対し、次のとおり速やかに報告するよう努める。

（1）報告の方法

原則として、個人情報保護委員会に対して報告する。ただし、法第 47 条第 1 項に規定する認定個人情報保護団体の対象事業者である個人情報取扱事業者は、当該認定個人情報保護団体に報告する。

上記にかかわらず、法第 44 条第 1 項に基づき法第 40 条第 1 項に規定する個人情報保護委員会の権限（報告徴収及び立入検査）が事業所管大臣に委任されている分野における個人情報取扱事業者の報告先については、別途公表するところによる。

（2）報告を要しない場合

次の①又は②のいずれかに該当する場合は、報告を要しない

①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合

②FAX 若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合

2.　民間の自主的取組の推進（抜粋）

(1) 省略

(2) PIA (Privacy Impact Assessment、個人情報保護評価) の推奨

PIA については、自社の基準に基づいて自主的に実施する事業者が増加してきているとともに、民間において、国際規格(ISO/IEC 29134:2017)の JIS 化が進められている中、現時点において、評価の項目や手法等を規定して義務化することは、かえってこうした自主的な取組を阻害するおそれもあるため、このような民間の動向を踏まえつつ、民間の自主的な取組を促すことが望ましいと考えられる。

(3) 個人データの取扱いに関する責任者の推奨

責任者の設置について一部義務化することも考えられるが、個人情報の取扱いに関して横断的に対応するための部署の自主的な設置が一定程度進展していること等を考慮すると、その要件や業務等を規定して一律に義務付けることは、こうした自主的な取組を阻害するおそれがある。したがって、PIA と同様に、自主的な取組を促進することが望ましいと考えられる。

(4) 保有個人データに関する公表事項の充実

個人情報取扱事業者による保有個人データの本人に対する説明の充実を通じて、本人の適切な理解と関与を可能としつつ、個人情報取扱事業者の適正な取扱いを促す観点から、個人情報の取扱体制や講じている措置の内容、保有個人データの処理の方法等の本人に説明すべき事項を、法に基づく公表事項(政令事項)として追加(*6)することとする。

2015 年改正法　第 27 条（保有個人データに関する事項の公表等）（抜粋）

個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

一　当該個人情報取扱事業者の氏名又は名称

二　全ての保有個人データの利用目的(第 18 条第 4 項第 1 号から第 3 号までに該当する場合を除く。)

三　次項の規定による求め又は次条第 1 項、第 29 条第 1 項若しくは第 30 条第 1 項若しくは第三項の規定による請求に応じる手続（第 33 条第 2 項の規定により手数料の額を定めたときは、その手数料の額を含む。）

四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの (*6)

紙面の制限から、第 3 章は第 3 節までの注目情報を引用しました。

次回は、「大綱」第 3 章第 4 節　データ利活用に関する施策の在り方　について引用する予定です。

<目次>

2020.2

第 249 回月例研究会：講演録

テーマ：【クラウドサービスの安全性評価に関するガイドラインについて】

会員番号　0647　清水 惠子　（月例研究会）

【講師】経済産業省 商務情報政策局　情報経済課

課長補佐 関根悠介 氏

【日時・場所】2020 年 1 月 21 日（火）18：30 – 20:30、機械振興会館　地下 2 階ホール（神谷町）

【テーマ】テーマ ： 「クラウドサービスの安全性評価に関するガイドラインについて」

【要旨】

総務省・経済産業省において 2020 年度中の制度立上げを目指して現在検討されている標題制度に関する主旨、概要、今後の予定について解説する。

【講演録】

Ⅰ．経緯と主旨

クラウドサービスの安全性評価について、世界の潮流として２０２０年には３０兆円以上の市場規模になるとの予想があり、２０１８年には政府情報システムにおけるクラウドサービスに係る基本方針クラウド・バイ・デフォルト原則を受けて検討を開始することが閣議決定された。２０１９年度に IT 政策大綱、成長戦略において２０２０年のクラウドサービスの安全性評価制度利用開始が政府決定された。IT 政策大綱は「データ」は「２１世紀の石油」としてデータの安全・安心を確保し官民のデジタル化の推進しデータや AI を活用することを決定している。

官民のクラウド利用の現状の課題としてセキュリティ不安が最多であり、セキュリティに対する統一的な評価を実施することが有効であり、特にセキュリティを求められる政府の情報システムを念頭に置いた制度構築が急務とされた。現状で多くのセキュリティ基準等が存在するが、個々の対応は非能率であるため共通する統一的な基準を明確化し、実効性・効率性のある安全性評価制度を検討する。世界各国もクラウドファーストを掲げ、その直後に政府のクラウドサービスの政府調達評価制度を導入している。

Ⅱ．クラウドサービスの安全性評価に関する検討会とフレームワーク概要と基本的流れ

クラウドサービス安全性評価に関する検討会は、２０１８年８月２７日第１回から 2019 年 12 月まで９回開催され、2019 年７月に中間とりまとめ、2020 年１月にとりまとめが行われている。委員会の他に管理基準 WG 監査基準 WG が開催されている。

制度設計フレームワークの基本的視座は調達だけでなく、運用までみる、技術変化を見据える、運用における実効性を確保する、民間が評価結果を活用することも視野に入れるである。フレームワークの必要な要件は、評価の対象は CSP 単位でなくサービス単位とする、情報システムのクラス分けに応じたサービス選択が可能であること、既存の仕組みや認証制度の最大限活用できるようにすること、クラウドサービスの経済性・効率性を損なわないこと、クラウドサービス形態（IaaS,PaaS,SaaS）の差異を踏まえた制度にすること、クラウドサービスが複数の運用主体・要素で構成されることを考慮すること、過度に日本に特異な制度にならないことである。これらに加えて既に民間でセキュリティ監査の知見が集積し一定の評価水準を確保でき継続的な確認が可能であることから監査の仕組みを活用した枠組みとする。

評価制度は、基準の策定、調達前審査、調達、更新審査の基本的流れで調整中。CSP がサービス範囲を特定し、管理基準から管理策を選択し選択しない管理策は理由を明示し、選択した管理策について実際に実装・運用が行われていることを監査によって担保する。この制度により、調達省庁は、従来は個々で確認していたサービス範囲、セキュリティ対策、実装の妥当性についての情報を同一の登録結果から知り調達の判断材料とすることが可能となる。

Ⅲ．整備を進めている基準等と今後の予定

整備を進めている基準は管理基準、管理主体の選定基準、監査基準、標準監査手続である。この他に各種ガイドラインやフォーマットを作成中。2020 年度の立ち上げに向けて①評価対象は一定期間整備状況のみ②ガイドラインは基準レベルまでの規定とする。③管理基準は 3 つにレベル分けをして立ち上げ時はレベル 2 の一種類までとする。

管理基準はガバナンス基準、マネジメント基準、管理策基準からなり ISO27001,27017 をベースとして統一基準と SP800-53 から不足部分を補う。

監査主体登録基準は更新頻度 2 年、日本法人で情報セキュリティ基準適合サービスに登録されていること責任者は日本国籍を有し、定められた資格を有すること倫理審査機能があることなどが規定される。

監査基準は情報セキュリティ監査基準を軸として日本公認会計士協会の専門業務実務指針４４００（合意された手続）を特に参考し、JISQ17020 等も参考にする。監査のプロセスは適正表示、個別管理策の整備、個別管理策の運用の 3 つのフェーズに分かれる。CSP は自身のサービス内容に対応する管理策の言明書を作成し、監査主体は、サービス範囲に照らして適切な管理策が言明書に記載されているか確認する。既存監査制度等の証跡等の活用、リージョンとサンプリング、登録申請、発見事項と登録、他社サービスの活用等について記載例を示して説明がされた。２０１９年度内のパブリックコメント、2020 年度内での立ち上げ、実施を目指す。

【所感】

安全性評価制度のフレームワーク、管理基準、監査基準の策定状況について丁寧にご説明をいただいた。会場からは、監査人の独立性や監査基準に合意された手続が参考にされていることなどについて質問があった。今後のガイドラインの公表により、内容が明確になり安全性評価が実施されることが期待される。

以　上.

<目次>

2020.02

支部報告【　北海道支部　2020 年 1 月の月例研究会　】

会員番号　1448 宮崎雅年（北海道支部）

北海道支部では、以下のとおり 2020 年 1 月の月例研究会を開催しました。

・日時：2020 年 1 月 16 日（木）18:30～20:30　　参加者：3 名

・会場：札幌市男女共同参画センター OA 研修室（札幌市）

・演題：「2020 年オリンピック・パラリンピックのサイバーセキュリティ」

・講師：北海道支部長　宮崎雅年

＜講演概要＞

2020 年は、7 月 24 日から 8 月 9 日までの期間でオリンピック東京大会、8 月 25 日から 9 月 6 日までの期間でパラリンピック東京大会が開催されます。

過去に開催されたオリンピック・パラリンピックでは、情報システムおよび制御システムに対して各種サイバー攻撃を受けましたが、幸いにも大きな被害に至りませんでした。

今年開催される東京大会においても、情報システムおよび制御システムに対して各種サイバー攻撃を受けるとの前提で対策・準備が整えられています。

マラソンおよび競歩、サッカーの競技が開催されることになった札幌においても、各種サイバー攻撃に対して同様の対策・準備が求められます。

この対策・準備の中でシステム監査がどのように関わっているのか、公開情報に基づいて発表します。

なお、本発表の内容は講師の個人的意見であり、講師の所属する企業・団体の意見を代弁するものではありません。(セキュリティに関わる事項のため、講演内容に記載できない事項があることをご了承ください。)

＜講演内容＞

1. 大会運営業務とテクノロジー

オリンピック・パラリンピックの組織委員会が携わる大会運営業務は、モノと人の管理を行うイベントオペレーション、競技運営、放送・メディアオペレーションなどを行うスポーツオペレーション、会場整備・運営、選手村管理などを行うファシリティオペレーション、チケット販売管理、ライセンス商品販売などを行うビジネスオペレーションの 4 つに大きく分類されます。

イベントオペレーションでは、モノとして調達、物流、食料・飲料供給、清掃などを管理し、人として出入国管理、スタッフの輸送・移動、宿泊管理、VIP 警護、観客誘導、入場管理、サイネージなどを管理します。

スポーツオペレーションでは、競技運営、メディカルサービス、ドーピングコントロール、選手の輸送・移動、放送・メディアオペレーションなどを行います。

ファシリティオペレーションでは、会場整備、会場運営、選手村管理、電力供給、通信インフラ提供、会場フェンス設営などを行います。

ビジネスオペレーションでは、チケット販売管理、ライセンス商品販売管理、ビジネス開発、収支管理などを行います。

これらの大会運営業務を支えるシステムは、下記のようになります。

・イベントオペレーション

輸送管理システム、宿泊管理システム、受発注管理システムなど

セレモニー用システム、放送・プレス用機材など

・スポーツオペレーション

競技計測機器、審判判定ツール、競技ボランティア管理システム、会場の A&V 機器など

ドーピング検体管理システムなど

・ファシリティオペレーション

LAN、WAN、インターネット

電力供給、予備電源

ビル管理システム、CAD 図面管理

・ビジネスオペレーション

EC サイト、チケット販売管理システム、CRM など

偽サイト監視など

一方、これらのシステムを構築するテクノロジーの変遷は、下記のとおりです。

・1964 年　東京大会

大会運営の観点：オンラインシステムによる競技結果の集計・配信

大会観戦の観点：初の衛星放送による中継

・1988 年　ソウル大会

大会運営の観点：大会用統合情報システム

・2012 年　ロンドン大会

大会運営の観点：モバイルトラフィック対策およびサイバーセキュリティが課題として顕在化

大会観戦の観点：スマートフォン、SNS の普及（テレビ以外による観戦スタイルの普及）

・2016 年　リオデジャネイロ大会

大会運営の観点：クラウドベースの情報システムへ移行

大会観戦の観点：360 度カメラ映像の試験導入

会員向け映像アーカイブサービス開始（Olympic Channel）

・2018 年　ピョンチャン大会

大会運営の観点：完全クラウドベースの情報システムへ移行

大会観戦の観点：5G および VR 試験導入

・2020 年　東京大会

大会運営の観点：フルクラウドの情報システム

2. 過去のサイバー防衛

ロンドン、リオデジャネイロ、ピョンチャンの各大会では、組織委員会がサイバー攻撃を受けたことを公式に発表しました。サイバー攻撃は、政治的な意図を持ったもののほか、大会の開催そのものを妨害する明確な意図を持ったものがあったようです。

これは、プロテスト集団による政治的主張、アラブ・イスラム武装勢力によるテロ、分離独立勢力によるテロ、麻薬、マフィアなどによる犯罪、隣国との関係、海外への模造品流通（偽サイトなど）、インバウンドのハクティビスト（過激な自然保護団体など）など、現実での出来事がサイバー空間でも起こっていることを示しています。

過去の大会の具体的なサイバー攻撃の事例と対応は、下記のとおりです。最近になるほど、サイバー攻撃が高度化しているのが分かります。

・ロンドン大会（2012 年 7 月 27 日～8 月 10 日）
　大会公式サイトにサイバー攻撃（DDoS 攻撃）
　電力システムを狙った攻撃予告→技術者を要所ごとに配置するマニュアル操作に切替て対応
・リオデジャネイロ大会（2016 年 8 月 5 日～8 月 21 日）
　大会公式サイトにサイバー攻撃（DDoS 攻撃）
　組織委員会内では Bot 感染による情報（暗号化されたファイル）漏えい
　POS レジのマルウェア感染
　チケット販売の偽サイト
　大会関連のフィッシングサイト
　偽ホットスポット
・ピョンチャン冬季大会（2018 年 2 月 9 日～2 月 25 日）
　会場の無線 LAN（Wi-Fi）が使えなくなった
　チケットの印刷ができなくなった
　認証システムのサーバが攻撃を受けた
　サーバを 1 台復旧すると､ウィルスの変種が現れて別のサーバに感染していった(→拡散型のウィルス)
　認証システムを通じて ID とパスワードを入手し、乗っ取ったアカウントから認証システムを破壊し、その認証システムがウィルスを連鎖的に伝播していった（50 のサーバ、52 のサービスに影響）
　インターネットを遮断して対応し、競技開始 1 時間前に復旧（最終的に 40 種類のウィルスを発見）
　大会に関連する海外の IT サービス会社から侵入

過去の事例から、大会用のシステムやネットワークだけを守っても、大会運営を守ることにはならず、周辺に社会インフラを含めて、総合的に守る視点が必要であることが明らかです。

つまり、大会運営の視点から、大会システムへのハッキング、内部情報漏えいなど、組織委員会側で管理すべきリスク、パートナー・周辺環境の視点から、サプライチェーン・リスク、偽チケット販売サイト、重要インフラの障害など、パートナーや周辺環境に内在するリスク、社会全般の視点から、自然災害、会場外で発生するテロ・サイバーテロ、SNS 上での日本・東京に対する評価・評判など、間接的に大会に影響するリスクがあるということです。

3. 今回のサイバー防衛

今回は、内閣官房内閣サイバーセキュリティセンター（NISC）を中心に、JPCERT/CC、IPA などの公的機関、同じ業界の民間事業者同士でサイバーセキュリティに関する情報を共有する金融、Telecom、電力、Software などの ISAC 等でサイバー防衛の体制を構築しています。

また、リスクを洗い出して、分析し、必要な対策を実施して、監査・合同演習訓練を実施しています。

想定されるサイバーセキュリティのリクスは下記のしおりです。

○金銭目的のサイバー犯罪（国内だけでなく海外でも想定されます）

・偽チケット販売サイト

・フィッシング、偽サイト、偽アクセスポイントなどによる個人情報の搾取

・ランサムウェアによる脅迫

○ハクティビストの攻撃

・大会サイトへの攻撃（DoS 攻撃、改ざん）

・スポンサーや開催都市など関連サイトへの攻撃→周辺サイトがとばっちりを受けやすい

・競技対戦国の関連サイトへの攻撃→スポーツイベントにつきもの

○サイバーテロ（狙われるかどうかは、大会開催時の国内外の情勢にも依存）

・大会システムへの侵入によるシステム破壊、データ破壊

・大会システムの乗っ取り

・重要インフラへのサイバー攻撃

○サイバー戦争

・要人（海外要人も多数来訪）を狙ったサイバースパイ

4. リスクアセスメント

2018 年 4 月 4 日、サイバーセキュリティ戦略本部より「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第 1 版）」が発表され、2019 年 1 月、内閣官房内閣サイバーセキュリティセンターより「機能保証のためのリスクアセスメント・ガイドライン 3.0 版　～2020 年東京オリンピック・パラリンピック競技大会に向けて～」が発表されて、組織委員会以外の民間でもサイバー防衛の質の向上が求められました。

5. 電力業界の対応

電力業界では電力の安定供給に向けて、電力制御システム、情報システムおよびスマートメーターシステムのセキュリティ対策を行い、セキュリティ監査を実施するとともに、単独・合同の演習訓練を実施しています。

6. サイバーセキュリティ監査

「電力制御システムセキュリティガイドライン」、「スマートメーターシステムセキュリティガイドライン」に基づいてサイバーセキュリティ監査を実施しています。

<目次>

2020.02

【　注目情報（2020 年 1 月 ～ 2020 年 2 月）　】

■「情報セキュリティ10大脅威 2020」を決定　【IPA】2020/1/29

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、情報セキュリティにおける脅威のうち、2019 年に社会的影響が大きかったトピックなどを「10 大脅威選考会」の投票によりトップ 10 を選出し、「情報セキュリティ 10 大脅威 2020」として順位を決定し、公表しました。

https://www.ipa.go.jp/about/press/20200129.html

■2月1日～3月18日は「サイバーセキュリティ月間」です。普及啓発活動へご協力ください。【NISC】2020/2/3

不審なメールによる情報漏えい被害や個人情報の流出など、生活に影響を及ぼすサイバーセキュリティに関する問題が多数報じられています。

誰もが安心して IT の恩恵を享受するためには、国民一人ひとりがセキュリティについての関心を高め、これらの問題に対応していく必要があります。

このため、政府では、サイバーセキュリティに関する普及啓発強化のため、２月１日から３月１８日までを「サイバーセキュリティ月間」としています。

https://www.nisc.go.jp/security-site/month/index.html

<目次>

2020.02

【 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35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250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ろう。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	http://www.saaj.or.jp/kenkyu/kenkyu/250.html

■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>

2020.02

協会からのお知らせ　【２０２０年度春期 公認システム監査人及びシステム監査人補の募集】

２０２０年度春期 公認システム監査人及びシステム監査人補の募集の〔公告〕が協会のホームページに掲載されています。資格取得を企図されている各位はご参照願います。〔公告〕の概略は下記の通りですが、申請書等の資料のダウンロードなども、ホームページからお願い致します。

（https://www.saaj.or.jp/csa/csaboshu/csaboshu.html）

[補足]

システム監査技術者試験の合格者以外でも、従来から情報セキュリティその他の高度情報処理技術者試験合格者、中小企業診断士、公認会計士、技術士、ITC、CISA、ISMS／プライバシーマーク主任審査員などの各位も、「特別認定講習」を修了することでシステム監査人補の認定申請が出来ました。2017年からこれに加え、情報処理安全確保支援士、米国公認会計士、内部監査人、ＱＭＳ主任審査員、公認情報セキュリティ監査人が、「特別認定講習」を修了することでシステム監査人補の認定申請が出来るようになりました。また、申請前直近６年間のシステム監査実務経験（実務経験みなし期間）が２年以上あれば、公認システム監査人の認定申請が出来ます。(https://www.saaj.or.jp/csa/csaboshu/620301CSAASAbosyuyoko.pdf)

---------- 記 ----------

2020 年 2 月 1 日
認定特定非営利活動法人日本システム監査人協会
公認システム監査人認定委員会

2020 年度春期
公認システム監査人及びシステム監査人補の募集について

〔公告〕

認定特定非営利活動法人日本システム監査人協会（以下、協会という）は、公認システム監査人認定制度（2002 年 2 月 25 日制定）（以下、制度という）に基づき、「公認システム監査人(Certified Systems Auditor：CSA)」および「システム監査人補(Associate Systems Auditor：ASA)」を認定するため、2018 年度春期公認システム監査人およびシステム監査人補の募集を行います。募集の概要と申請書等の資料の入手方法は、以下のとおりです。

1．認定資格

公認システム監査人およびシステム監査人補とする。

2．申請条件

（1）　認定申請者は、経済産業省が実施するシステム監査技術者（旧情報処理システム監査技術者）試験に合格していること。（制度２（5）特別認定制度に基づく特別認定講習の修了により、上記試験の合格者と同様に取り扱う者を含む）

（2）　公認システム監査人の申請者は、申請前直近 6 年間のシステム監査実務経験（実務経験みなし期間）が 2 年以上あること。

3．認定申請

（1）　申請書類（記入方法は、募集要項参照）

公認システム監査人およびシステム監査人補の申請書類は、次表のとおりとする。

申請書類	公認システム監査人	システム監査人補	記事
⑴認定申請書	○	○	様式１
⑵監査実務経歴書	○	―	様式２
⑶小論文	○	―	様式３
⑷宣誓書	○	○	様式４
⑸資格証明（写）	○	○	
⑹申請手数料振込書（写）	○	○	
⑺面接試験	□	―	別途通知

（注１）　○印の資料一式を申請書類として提出する。
（注２）　□印については、面接試験を実施する。
備考：公認システム監査人とシステム監査人補を同時申請する場合は、公認システム監査人用の申請書類を提出する。

（2）　面接試験
申請書類審査後、認定委員会が別途指定・通知する日時場所において、面接試験を受ける。

4．募集期間
2020 年 2 月 1 日（土）～2020 年 3 月 31 日（火）（同日消印まで有効）

5．認定申請手数料（消費税 10%を含む）

申請手数料	協会会員	非会員
⑴ 公認システム監査人認定申請手数料 （注 1）システム監査人補と同時申請する場合も手数料は同じです。	22,000 円	33,000 円
⑵ システム監査人補が申請する場合の公認システム監査人認定申請手数料	11,000 円	16,500 円
⑶ システム監査人補認定申請手数料	11,000 円	16,500 円

6．資料の入手方法
（https://www.saaj.or.jp/csa/csaboshu/csaboshu.html）から
【個人情報の取り扱いについて】 ⇒「同意する」ボタンを押下
(1) 「公認システム監査人、システム監査人補 募集要項」
ダウンロード（PDF 形式）
(2) 申請書等様式一式
・認定申請書（様式１）：Word 形式
・監査実務経歴書（様式２）：Word 形式
・小論文（様式３）：Word 形式
・宣誓書（様式４）：Word 形式
(3) 公認システム監査人認定制度のダウンロード
・PDF 形式
(4)「公認システム監査人制度」創設のお知らせ（2002 年 7 月 1 日）のダウンロード
・PDF 形式
(5) 特別認定講習に関する情報
（・特別認定講習機関認定については HP の当該 URL から参照）

以上

<目次>

2020.02

【 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.saaj.or.jp/index.html
・会員規程　http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・会員情報の変更方法　http://www.saaj.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.saaj.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.saaj.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.saaj.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.saaj.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.saaj.or.jp/csa/index.html

会報

・過去の会報を公開　https://www.saaj.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.saaj.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>

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2020.2
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
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 7-8：第 35 回システム監査実務セミナー(日帰り 4 日間コース)前半 17：第 250 回月例研究会 21-22：第 34 回システム監査実務セミナー後半	
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）
7 月	6：支部助成金支給 9：理事会	中旬：秋期 CSA・ASA 募集案内	13：支部会計報告〆切
	前年度に実施した行事一覧		
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
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

<目次>

2020.02

【 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>

2020.02

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.saaj.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.saaj.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.saaj.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。

■□■ＳＡＡＪ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： saajeditor ☆ saaj.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>