認定 NPO 法人
日本システム監査人協会報
2019 年 3 月号
No 216
No.216（2019 年 3 月号）<2 月 25 日発行>

◎今月号の注目情報

「セキュリティ 10 大脅威 2019」（ＩＰＡ）

◎第 18 期通常総会の開催速報

（次号会報で総会特集を予定）

巻頭言

システム監査のターニングポイント ― 新時代のシステム監査

会員番号：1342　安部晃生（副会長）

会報では、毎年、テーマを設定し、皆様からのご意見・ご提案を募集しています。

今年度の年間テーマは、「システム監査のターニングポイント」です。

振り返ってみますと、通商産業省（現経済産業省）によるシステム監査制度創設が 1985 年（昭和 60 年）、当協会の発足が 1987 年（昭和 62 年）ですので、システム監査が歩みだしたのは昭和の終わりでした。その意味で、システム監査は平成の時代とともに歩んできたものといってもよいでしょう。

システム監査制度創設の当時は、銀行の第 3 次オンライン時代で、大型コンピュータ全盛の時代でした。その後、この 30 年余りの間には、パソコン、クライアントサーバー、インターネット、モバイル、クラウドなど、コンピュータ技術も大きく進展しました。また、制度等の面でも、2000 年問題、個人情報保護法対応、Ｊ－ＳＯＸなど、新たな課題が次々に発生しました。システム監査はそれらの時代環境に対応し、監査の高度化が図られてきました、

しかし、最近のシステム監査をめぐる動き ― ＡＩ、自動運転、ＩｏＴ、ビッグデータ、ブロックチェーン等の IT 技術の進展や、グローバル化の流れなど ― を見ていると、これまでのシステム監査では対応が難しい状況が生まれてきているように思えてなりません。

今年 4 月で平成の時代も終わり、5 月からは新元号の時代が始まります。この時代の変わり目は、システム監査の変わり目でもあるような気がしています。

そうした状況を踏まえて、会報の年間テーマを「システム監査のターニングポイント」としました。

これからのシステム監査はいかにあるべきか、皆様のご意見をお聞かせ願いたく、会報へのご投稿をお待ちしています。

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>

2019.2

めだか　【　システム監査人のターニングポイント　】

システム監査人は、基準と手続きを明らかにし、システム監査の目的やテーマを明確にして監査を計画、実施、報告する責務がある。システム監査基準とシステム管理基準の 2018 年 4 月 20 日改訂版の公表は、あらためて基準と手続きを明らかにしたが、これは、システム監査人のターニングポイントである。システム監査の目的やテーマの選択は、対象となる情報システムが経営課題などの解決に合っているかという視点が重要である。

情報システムで取り扱うデータは、ID（Identifier）によって識別され、その情報システムの中でユニークである必要がある。個人は、姓名によって識別され、同姓同名の場合など、誕生日そのほかの情報で確認するが本人ではない可能性を否定できないためマイナンバーで確かめることになる。

マイナンバーとは、日本に住民票を有するすべての人（外国人も含まれる。）が持つ 12 桁の番号で、原則として生涯同じ番号を使う。マイナンバーが漏えいして不正に用いられるおそれがあると認められる場合を除いて、自由に変更することはできない番号である。マイナンバーは、社会保障、税、災害対策の 3 分野で、複数の機関に存在する個人の情報が同一人の情報であることを確認するために活用される。マイナンバーを導入することで、個人の特定を確実かつ迅速に行うことが可能になり、これにより、行政の効率化、国民の利便性の向上、さらに公平・公正な社会を実現するという課題の解決に資するものである。

ID といえば、マイナンバーをはじめ、バーコード、QR コード、IC タグ（RFID）、電子カード・電子定期券、指紋認証、静脈認証、顔認識、話者認識・音声認識と、利用場面が多岐にわたる。D 社が開発した QR コードは、近年、スマートフォンで URL を読み取ることに使われているが、もともとは T 社の自動車生産管理において部品などに ID をつけるのが当初の目的であったという優れた ID である。昨今、ID は、ビッグデータの利活用や、なりすましなどの個人情報の問題に大きくかかわるようになってきている。

個人情報保護法シンポジウムが、2019 年 1 月 25 日、「暮らしの中の個人情報のこれからを考える」をテーマに開催された。シンポジウムは、「個人情報保護委員会の活動から見える最新動向」の講演や、「個人情報の保護・利活用の今後について」のパネルディスカッションで構成され、はじめに、2019 年 1 月 23 日付け「日 EU 間の相互の円滑な個人データの移転 ～ボーダレスな越境移転が実現～ 」について報告があり、新しい時代の幕開けを感じさせた。また、全国の小学生から募集した個人情報の大切さに係る標語の発表があり、「大切な 僕の分身 個人情報」や、「悔やんでも アップしてからじゃ もうおそい」などの作品が紹介され、若い世代が考えた標語に感心した。（空心菜）

参考：「ID の秘密」佐藤一郎著、国立情報学研究所監修 丸善ライブラリー

（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>

2019.2

投稿　【　金融機関におけるこれからの内部監査（システム監査のターニングポイント）　】

会員番号　1342 安部晃生　（副会長）

金融機関において監査を行う際の重要な拠り所としていた金融庁「金融検査マニュアル」が、今年 4 月以降、廃止される予定とされている。

「金融検査マニュアル」は、もともとは金融庁の検査官が金融機関の検査を行う際に用いるマニュアルであったが、金融庁検査に用いられるだけでなく、各金融機関が態勢整備を行う際の基準としても用いられてきた。しかし、ここにきて、金融庁は、「金融検査マニュアル」による画一的な検査を改め、今後は、金融機関それぞれの経営課題に応じた自主的な改善を促すという方針で、金融機関に対する指導にあたっていくようだ。

この「金融検査マニュアル」廃止は、金融機関の内部監査のあり方・監査方法を大きく変える「ターニングポイント」になるように思われる。

では、金融機関の内部監査は、どのように変わっていくのであろうか。ここで、考えてみたい。

１．金融庁が求める“金融機関におけるこれからの内部監査”

金融機関における内部監査はどのように変わっていくべきだと、金融庁は考えているのだろうか。

昨年 9 月に、金融庁から公表された「変革期における金融サービスに向上に向けて～金融行政のこれまでの実践と今後の方針（平成 30 事務年度）～について」（以下、「金融庁方針」）から、金融庁の考えを見てみよう。

（1）「ガバナンス」の重要性と「内部監査の高度化」の必要性

金融庁では、従前より「実効性のある内部監査態勢を整備することが、経営相談・経営指導等をはじめとした金融円滑化、適切な法令等遵守、顧客保護等及びリスク管理に必要不可欠である」（「金融検査マニュアル」）として、金融機関における「内部監査の重要性」について強調してきた。

今回の金融庁方針では、デジタライゼーションの加速等により、金融を巡る環境が大きく変化している変革期において、内部監査は、今以上に「高度化」していく必要があるとされている。

具体的には、金融庁方針において、「内部監査の高度化」の必要性について、以下のように述べてられている。

> 金融機関が持続可能なビジネスモデルを構築することにより、業務の適切性や財務の健全性を確保し、金融システムの安定に寄与していくためには、ガバナンスが有効に機能していることが重要である。
>
> そのためには、内部監査部門が、リスクベースかつフォワードルッキングな観点から、組織活動の有効性等についての客観的・独立的な保証、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いう内部監査の使命を適切に果たすことが必要であり、・・・(略)・・・内部監査を高度化していくことが求められている。

（2）「内部監査の高度化」に向けて

では、「内部監査の高度化」のためには、内部監査は、具体的にどう変わっていけばよいのであろうか。
金融庁方針では、「内部監査の高度化」の具体策として、次のような「転換」が必要だとしている。

① 事後チェック型監査からフォワードルッキング型監査への転換

- 損失やリスクが顕在化した後に行う事後チェック型の監査から、損失やリスクが顕在化する前の段階での未然予防に重点をおいたフォワードルッキングな監査への転換（過去から未来へ）

② 準拠性監査から経営監査への転換

- 金融機関の内部規程やリスク・リミット等の遵守状況を検証する準拠性の監査から、内部統制の有効性の評価や実質的に良質な金融サービスが提供されているかといった点に重点を置いた監査、経営環境の変化や収益・リスク・自己資本のバランスに着目した監査等、経営に資する監査への転換（形式から実質へ）

③ 部分監査から全体監査への転換

- 問題発生部署における表層的な課題を指摘する監査から、ビジネスモデルやガバナンス等、金融機関が有する問題の根本原因分析を充実させた監査への転換（部分から全体へ）

もちろん、金融庁方針は、これまで行われてきた「事後チェック型監査」「準拠性監査」「部分監査」が必要ないと言っているわけではない。だが、これからは、経営目線に立った「フォワードルッキング型監査」「経営監査」「全体監査」がより重要であり、そうした監査を目指して対応していく必要があるということである。

2．これからの監査人に求められること

このように経営目線に立った「フォワードルッキング型監査」「経営監査」「全体監査」が求められる時代になると、内部監査・システム監査を担う我々監査人には、何が求められることになるのであろうか。

まず求められるのは、監査人の「見識」であろう。
「事後チェック型監査」「準拠性監査」「部分監査」であれば、誰が監査しても監査結果に大差はないと考えられる。問題があるかどうかは明確で、異論を挟む余地があまりないからだ。しかし、経営目線での監査となると、問題点としてどう考えるかは、監査人によって違いがでてくるのではないかと思われる。その意味で、監査人の「見識」が今まで以上に問われる時代になってくるように思える。

もう一点あげるとすると、監査人の「コミュニケーション能力（説明力）」であろう。
経営目線で考えると、問題かどうかについて、被監査部門と認識が異なるケースも多くなると思われる。その場合に、被監査部門にどう納得させるかは、監査人の腕の見せ所とも言える。

これからの監査においては、監査人は、「見識」と「コミュニケーション能力（説明力）」とを磨いていく必要がありそうだ。

以上

<目次>

2019.2

投稿　【　越境移転個人情報の取扱いとシステム監査人の対応　】

会員番号　557 仲厚吉　（個人情報保護監査研究会）

昨今、電子商取引の活性化のため国境を越境して移転する個人情報についてその取扱いが課題になっています。越境移転個人情報の取扱いのレポートを行い、また、システム監査人の対応について報告します。

越境移転個人情報の取扱いについて（レポート）

１．国境を越えた個人情報の移転の附帯決議

衆議院内閣委員会における附帯決議（平成 27 年 5 月 20 日）

“国境を越えた個人情報の移転は、合理的で安全なサービスの提供を可能にし、社会に裨益するものであることを踏まえ、海外における個人情報の保護を図りつつ、国境を越えた個人情報の移転を不当に阻害しないよう必要な措置を講ずること。”

参議院内閣委員会における附帯決議（平成 27 年 8 月 27 日）

“国境を越えた個人情報の移転は、合理的で安全なサービスの提供を可能にし、社会に役立つものであることを踏まえ、海外における個人情報の保護を図りつつ、個人情報の移転を不当に阻害しないよう必要な措置を講ずること。”

２．個人情報保護法第 24 条（外国にある第三者への提供の制限）

個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下同じ。）（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきとされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会で定める基準に適合する体制を整備している者を除く。以下この条において同じ。）に個人データを提供する場合には、前条第 1 項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は適用しない。

３．法令等の定めに基づく外国にある第三者

外国にある第三者には、提供元の組織と法人格が別の関連会社又は子会社も含まれる。一方で、日本の法人格を有する当該組織の外国支店などは第三者には当たらない。提供元の組織と法人格が別の関連会社又は子会社であっても、法第 24 条の外国にある第三者から除かれる者として、“当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として規則で定める基準に適合する体制を整備している場合”に当たる者がある。

４．規則で定める基準（規則第 11 条）

第 1 号

個人情報取扱事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、法第 4 章第 1 節（個人情報取扱事業者の義務（第 15 条-第 35 条））の規定の趣旨に沿った措置の実施が確保されていること。

第 2 号

個人データの提供を受けるものが、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること。

５．適切かつ合理的な方法（規則第 11 条第 1 号）

事例１）外国にある事業者に個人データの取扱いを委託する場合

・提供元及び提供先間の契約、確認書、覚書等

※GDPR/SCC(standard contractual clauses)に相当

事例２）同一の企業グループ内で個人データを移転する場合

・提供元及び提供先に共通して適用される内規、

プライバシーポリシー等

※GDPR/BCR(binding corporate rules)に相当

6．適切かつ合理的な方法（規則第 11 条第 2 号）

個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること（規則第 11 条第 2 号）は、提供先の外国にある第三者が、APEC/CBPR システムの認証を取得していることが該当する。

7．APEC/CBPR 認証システム

個人情報保護委員会は、APEC 内における電子商取引の活性化のための環境整備を目的とし、個人情報の保護等の議論を行う貿易・投資委員会電子商取引運営グループの会議等に出席している。APEC/CBPR 認証システムは、事業者の APEC プライバシーフレームワークへの適合性を国際的に認証する制度である。APEC の参加国・地域が本制度への参加を希望し、参加を認められた国がアカウンタビリティ・エージェント（AA）を登録する。この AA が事業者について、その申請に基づき APEC プライバシーフレームワークへの適合性を認証する。日本では AA に JIPDEC が登録されている。事業者は、CBPR 認証基準 2016/06/01（JIPDEC）、及び APEC/CBPR ホームページの AA のページに公表されている基準（英文）に基づいて認証審査を受ける。

8．CBPR 認証基準 2016/06/01（JIPDEC）

１．通知の原則：APEC 通知原則に照らし、

・取得される個人情報、移転先、及び利用目的に関する貴社のポリシーを本人に必ず理解してもらっていること。

・必要最低限の取得になっていることを条件として、本人の個人情報が取得されるタイミング、移転先、及び利用目的を本人に必ず通知していること。

（事前質問書 Q1-Q4）

２．取得の制限の原則：APEC 取得原則に照らし、個人情報の取得がその取得のために表明した目的に確実に限定されていること。

（事前質問書 Q5-Q7）

３．個人情報の利用：APEC 利用原則に照らし、個人情報の利用が取得目的及びこれに適合又は関連するその他の目的を達成することに限定されていること。

（事前質問書 Q8-Q13）

４．選択：選択手順に関する規定の条件に照らし、個人情報の取得、利用及び開示に関して本人が必ず選択できるようになっていること。

（事前質問書 Q14-Q20）

５．個人情報の完全性：記録について正確性及び完全性を維持させ、並びに最新な状態に維持していること。

（事前質問書 Q21-Q25）

※個人情報の完全性の原則の質問項目の事例

質問２３（転送後の修正の連絡）

不正確、不完全、または古くなった情報が利用目的に影響すると思われ、当該情報の転送後に修正がなされた場合、その修正について、当該個人情報の転送先である処理業者等に連絡をしていますか？

質問２４（開示後の修正の連絡）

不正確、不完全、または古くなった情報が利用目的に影響すると思われ、 情報の開示後に修正が行われた場合、その修正について個人情報の転送先であるその他の第三者に伝えていますか？

質問２５（委託先からの連絡）

不正確、不完全、または古くなった情報に気づいた場合は連絡をするよう、委託先や共同利用を行う事業者に求めていますか？

６．セキュリティ対策：個人がその個人情報を組織に預けるときに、個人情報の紛失、不正なアクセス、不正な破壊・利用・変更若しくは開示、又はその他の不正使用を防ぐために、その個人情報が合理的なセキュリティ対策によって確実に保護されていること。

（事前質問書 Q26-Q35）

７．アクセス及び訂正の原則：本人がその個人情報にアクセスして、訂正することができることを保証していること。

（事前質問書 Q36-Q38）

８．責任の原則：APEC 原則の実施方法を遵守することについて確実に責任を果たしているか、また、移転後にこの原則に従って個人情報を確実に保護するための合理的な措置を用意していること。

（事前質問書 Q39-Q50）

9．APEC/CBPR ホームページの AA のページに公表されている基準（英文）

1.1 General requirements

The applicant business entity shall establish, implement, maintain, and improve its personal information protection management system.

・・・

本基準は、プライバシーマーク認証基準に相当する個人情報保護マネジメントシステムを要求している。ただし、審査対象は、越境移転個人情報のみである。

10. GDPR

１．一般データ保護規則（General Dada Protection Regulation：GDPR）が、2018 年 5 月 25 日に適用された。GDPR は、欧州経済領域（European Economic Area: EEA、EU 加盟国 28 カ国とアイスランド、リヒテンシュタイン及びノルウェー）の域内で個人データの取扱いと移転を行う個人情報取扱事業者が適用を受ける規則である。この規則は、個人情報保護委員会ホームページの GDPR のページに移ると、仮日本語訳付きで掲載されている。また、EC's Infographics（中小企業向けの簡単にまとめられた GDPR 説明）や、GDPR によるデータ保護改革案についての質疑応答概略（欧州委員会）が、日本語仮訳付 PDF で掲載されている。
https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/
EEA 域内の個人情報を取り扱う事業者は、GDPR に対応する必要がある。また、日本と EU 間で、2019 年 1 月 23 日、相互の円滑な個人データ移転を図る枠組み構築に係る最終合意がなされた。EEA 域内から日本への個人データの移転は、十分性認定に基づく移転（GDPR 第 45 条）として適法になる。ただし、電子商取引などで EEA 域内の個人情報を取り扱う場合や､日本以外への移転やその他の規則は GDPR に対応が必要である。
個人情報保護委員会は、個人情報の保護に関する法律に係る EU 域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルールを、2018 年 8 月 24 日に公表している。
https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf
GDPR 条文は、
第 1 章に一般規則、第 2 章に基本原則を規定している。
※個人情報の本人は、GDPR では、データ主体という。
第 3 章（第 12 条～第 23 条）でデータ主体の権利について規定している。
※個人情報取扱事業者は、GDPR では、立場に応じて管理者（Controller）又は処理者（Processor）という。
第 4 章（第 24 条～第 43 条）で、管理者（Controller）と処理者（Processor）の義務を規定している。GDPR 第 40 条の行動規範（Code of conduct）の考え方が内部規程を策定する場合の参考になる。

システム監査人の対応

「SAAJ システム監査人倫理規定」第 4 条（監査基準・手続き）は、"システム監査人は、システム監査の基準、手続きを明らかにし、それに基づきシステム監査を行わなければならない。"と、規定しています。基準、手続きが文書化され、受査側に明らかにされている必要があり、認証審査に先立つ監査では、審査基準を監査基準に使います。個人情報を取り扱う情報システムを監査する場合、システム監査人は、システム監査基準・システム管理基準をベースに管理策を策定し、監査します。SAAJ 監修「個人情報保護マネジメントシステム実施ハンドブック第 2 版」に管理策や詳細管理策の例を挙げていますので監査する際の参考にしていただきたいと思います。

<目次>

2019.2

第 239 回月例研究会：講演録【 今、振り返る安対基準第９版 】

会員番号　0647　清水惠子　（月例研究会）

【講師】公益財団法人 金融情報システムセンター 監査安全部

主任研究員 坂上昇 氏　　研究員 宮島吉昭 氏

【日時・場所】2019 年 1 月 22 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】「今、振り返る安対基準第９版」

【要旨】

金融機関等コンピュータシステムの安全対策基準・解説書（第 9 版）が発刊されて 1 年弱の期間が経過し、実際に当該安全対策基準・解説書を利用した監査を経験したシステム監査人も出てきている中、改めて第 9 版発刊の意図や狙いを解説頂き、その内容を振り返ることで、実務経験も踏まえた理解を深める。

【講演録】

Ⅰ．安全対策基準とは

安全対策基準は、金融情報システム（金融機関等のコンピュータシステム。金融機関等が業法等に基づきサービスを提供するために利用するシステム）が対象であり、安全対策の考え方と障害等を未然に予防するための対策等を示した業界の標準ガイドラインである。FISC 会員企業や有識者から構成される安全対策専門委員会と検討部会が、継続的に検討･審議し維持改訂を行っている。1985 年 12 月に初版が発刊。1984 年に業界団体として FISC が設立され、自主的なガイドラインとして作成された。環境の変化に合わせて改訂を重ねていること、第 9 版にいたるまでの過程、各版の改訂の内容をご説明いただいた。

Ⅱ．外部委託及び FinTech に関する 有識者検討会

第 9 版の改訂は、有識者検討会での提言を基に改訂が行われている。「外部委託に関する有識者検討会」からは、IT ガバナンスの発揮とリスクベースアプローチ・外部委託（再委託を含む）におけるリスク管理策・共同センター固有の問題に対するリスク管理策・IT 人材の確保・育成に関する検討の必要性が提言され、「FinTech に関する有識者検討会」からは、FinTech に関する安全対策の在り方・重要な情報システムにクラウドサービスを利用する際のリスク管理策の検討の必要性が提言された。

Ⅲ．安全対策基準（第９版） の概要

第９版では、経営戦略策、事業戦略とＩＴ戦略を一体として経営層がＩＴガバナンス体制を整備し、安全対策目標を定めることの必要性が示されている。第 8 版までのレガシー前提のリスクゼロ目標の安全対策ではなく、金融情報システムをリスクベースアプローチにより重点を置く「特定システム」とそれ以外の「通常システム」に分類し、残存リスクについてはコンティンジェンシープランを立て対策することになる。

第８版の構成の「運用基準」、「技術基準」は、第９版では「統制基準」、「実務基準」、「監査基準」に再編されており、基準もリスク特性に応じて安全対策の目標を定めるにあたり不確実性を低減するため、最低限の「基

礎基準」とリスク特性により追加付加する「付加基準」に分類されている。また、外部委託管理に関する基準は、クラウドサービス利用時に関する基準と重複している個所があったため、内容を整理した上で統合・整理がされている。概要の説明をいただき、更に具体的な安全対策基準の使い方について事例により詳細な解説をいただいた。

Ⅳ．今後の取組みについて

FISC では、リスクベースアプローチ導入に伴う安全対策の考え方など会員向けに普及推進を行っている。今後も金融機関等の規模、業態等ごとにリスクベースアプローチの対応事例等、有益な情報の還元がされる。現在は検討部会にて「継続検討課題（設備、暗号技術等）」及び「パスワードの取扱いに関する課題」等をテーマとして第９版の改訂が検討されており、今後会員の意見募集を経て第９版改訂版が発刊される予定（平成 31 年３月末目途）である。

【所感】

安全対策基準第９版が外部環境の変化に対応してＩＴガバナンス体制、リスクベースアプローチと大きく舵をきり、更に、継続して現状の課題を解決に向けて改訂を検討されていることを丁寧にご説明いただき、この第９版が活用されることにより、金融システムの安全性が高まることが期待され、第９版が理解され普及することが望まれると感じた。

以　上.

<目次>

2019.2

支部報告　【　北海道支部　2019 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 2019 年 1 月の月例研究会を開催しました。

・日時：2019 年 1 月 18 日（金）18:30～20:30　　参加者：2 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：「2019 年に来る脅威と機会」

・講師：北海道支部長　宮崎雅年

＜講演概要＞

2019 年は、Java SE 8 の商用向け更新版の無償サポート終了、改元、消費税率引き上げのほか、働き方改革関連法施行、個人情報保護法・マイナンバー法改正、サイバーセキュリティ基本法改正といった IT 業界にとって脅威ともいうべきイベントが目白押しです。

これを機会と捉えてシステム監査の普及につなげられないか考えます。

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。

＜講演内容＞

0. はじめに

総務省の通信利用動向調査によれば、企業におけるインターネット利用率は 2015 年に 100%となり、個人にインターネット利用率は 2017 年に 80.9%となっており、インターネット利用が日本全体に普及していることが分かります。

また、主な情報通信機器の普及状況は、携帯電話およびスマートフォン、タブレット端末が増か傾向にある一方、固定電話および FAX、パソコンが低下傾向にあり、2017 年に固定電話(70.6%)は携帯電話(94.8%)およびスマートフォン(75.1%)の普及率を下回り、FAX(35.3%)はタブレット端末(36.4%)の普及率を下回りました。

さらに、2017 年の個人におけるインターネット利用の機能・サービスは、「電子メールの受発信」(80.2%)、「天気予報の利用」(65.8%)、「地図・交通情報の提供サービス」(63.4%)、「ニュースサイトの利用」(57.6%)、「無料通話アプリやボイスチャットの利用」(55.4%)、「ソーシャルメディアの利用」(54.7%)、「動画投稿・共有サービスの利用」(53.1%)、「商品・サービスの購入・取引」(49.1%)ですが、5 年前の 2012 年では、「電子メールの受発信」(63.2%)、「ホームページ(Web)・ブログの閲覧」(62.6%)、「商品・サービスの購入・取引」(56.9%)であったことから、大きく変化していることが分かります。

1. Java SE 8 無償サポート終了

Java SE は Java のアプリケーション開発に必須のツールで、Java SE 8 の商用向け更新版の無償サポート

が 2019 年 1 月に終了しました。(個人ユーザは 2020 年 12 月末まで無償サポートが継続します。)有償のサポート契約を結んでいないと、新たな脆弱性が発見されても、更新プログラムが提供されなくなり、脆弱性を悪用した攻撃による被害を受ける可能性が高くなります。

つまり、2019 年 2 月以降も Java SE 8 を商用で安全に利用するためには、有償のサポート契約を結ばなくてはならなくなります。

Java は、1990 年代前半に Sun Microsystems 社で設計・開発されたプログラミング言語で、オブジェクト指向プログラミングをサポートしています。

また、ソースコードは中間言語にコンパイルされ、仮想マシン上で動作することから、プラットフォームに依存しないアプリケーションソフトウェアを開発することが可能で、しかも無償でした。

ほぼすべてのパソコン、携帯電話、スマートフォン、タブレット端末にブラウザがインストールされている環境が普及している状況と、Java はブラウザと親和性が高いことから、インターネットの普及とともに Java が広く普及していきました。

さらに、J2EE(Java 2 Platform, Enterprise Edition)による各種情報サービスのリリースおよび情報システムの開発において、UML(Unified Modeling Language)で設計し、ジェネレータで Java のソースコードを生成して EJB(Enterprise Java Beans)を得るということが広がりました。

ちなみに、2019 年 2 月において無償サポートされている Java SE のバージョンは、7(2019 年 7 月まで)、8(個人のみ)、12(2019 年 9 月まで)で、有償サポートされている 11(2023 年 9 月まで)となっていることから、永く Java SE を利用するためには、有償のサポート契約は避けられない状況にあります。

2010 年 1 月に Oracle 社が Sun Microsystems 社を吸収合併したときから Java 有償化の予感がありましたが、ついにその時が来たという印象です。

Java SE 8 無償サポート終了への対応として、Java を使用しているシステムの有無を確認し、「有償のサポート契約を締結して Java を使い続ける」、「一時的にでも有償のサポート契約を締結して Java を使い続け、Java 以外への移行準備が整ったら脱 Java」、「無償サポート期間内で脱 Java」の選択が迫られます。

移行先として、例えば「.net Framework」、「Python」、「C#」、「C/C++」などが挙げられます。

脱 Java の具体例として、日本建設情報総合センター(JACIC)では、日本オラクルと特別契約を締結し、「電子入札コアシステム」向けに 30 万ライセンスを上限に 2 年間延長利用することとし、2019 年 1 月以降に専用ダウンロード・システムで無償提供を行う一方、2 年間で「脱 Java」システムを開発する計画です。

また、総務省　電子政府の総合窓口(e-Gov)では、現行システムを開発した F 社が新たに「.net Framework」を利用するクライアント・アプリケーションを提供するため、2020 年秋を目途にシステムの全面刷新を予定しています。

さらに、日本情報処理推進機構(IPA)では、「My JVN バージョンチェッカ」を 2019 年 1 月 16 日で JRE 版のツールの公開を終了し、2019 年 1 月 17 日以降は「.net Framework」版のツールに一本化しました。

2. 改元

前回の「昭和」から「平成」への改元は、30 年前の 1989 年 1 月 8 日で崩御に伴うものでした。

「平成」は、1989 年 1 月 7 日に当時の内閣官房長官であった小渕恵三 氏が公表しました。

今回、新元号は 2019 年 4 月 1 日に公表され、「改元の日」は 2019 年 5 月 1 日であることが決まっていま

す。(元号法に「元号は、皇位の継承があった場合に限り改める」と定められていますが、今回は 2019 年 4 月 1 日に公布する「改元政令」で定めます。)

改元に向けた現状把握として、和暦で処理しているシステムおよび和暦を使用しているデータを洗い出し、どの和暦を使用しているか確認します。

ここで、「どの和暦」という意味ですが、前回の改元の際に「昭和」継続利用することとし、変換テーブル等で表示・印字だけを「平成」にしたシステムが存在することがあるからです。

ちなみに、「昭和」だと今年 2019 年は「昭和 94 年」なので、「昭和 100 年」以降の年の取り扱いで桁が不足する恐れがあります。

また、和暦を使用していなければ問題ないかというと、内外の他システムとのデータ連携があることから、こちらも確認も必要です。

改元対応の要件定義は、下記のようなります。

・2019 年 5 月 1 日(「改元の日」)以降、新元号または新元号の略称アルファベットを使用

・1998 年 1 月 8 日以降で 2019 年 4 月 30 日(改元の前日)までは、「平成」または「H」を使用

・新元号は、2019 年 4 月 1 日に公表

・「改元の日」は、2019 年 5 月 1 日(元号法に定める「皇位の継承があった」と見なされる新天皇の即位は 2019 年 5 月 1 日の日中なので、2019 年 5 月 1 日午前 0 時は新元号の 5 月 1 日ではなく、平成 31 年 5 月 1 日と見なすことができるので、2019 年 5 月 2 日が「改元の日」という解釈が成り立つため、改元に関する新たな政令が必要であった。)

現時点で改修できることは、和暦を使い続けるならば

・新元号が公表されるまで、「仮の新元号」を使用して改修

・2019 年 4 月 30 日 23 時 59 分 59 秒までは「平成」を適用

・2019 年 5 月 1 日 0 時 00 分 00 秒以降は新元号を適用

ですし、許容されるならば和暦の使用をやめて

・データの日付を西暦に変換し、データの日付を西暦で処理するように改修

です。

また、新元号公表前の仮のテストとして、和暦を使い続けるならば

・新元号が公表されるまで、「仮の新元号」を使用してテスト

・「改元の日」が正しく反映されるかテスト

しますし、和暦の使用をやめるのならば

・データの日付を西暦に統一できており、西暦で正しく処理できるかテスト

します。

そして、新元号が公表されたら、和暦を使い続けるならば

・プログラムに記述した「仮の新元号」を「公表された新元号」に置換

・「公表された新改元」が正しく入力・表示でき、正しく処理できるかテスト

します。和暦の使用をやめるのならば特に影響はありません。

改修後のシステムへの移行は、4 月 27 日から 5 月 6 日までの 10 連休(特に、前半の 4 月 27 日から 4 月

30 日)に行われることが予想されます。

和暦を使い続けるならば

・改修後のプログラムをリリース

・新元号を含めたデータに変換して登録

しますし、和暦の使用をやめるのならば

・改修後のプログラムをリリース

・西暦のデータに変換して登録

します。

内外の他システムとのデータ連携では、相手のある問題ですので双方の合意が必要になります。

まずは、現在の仕様を確認し、改元対応の仕様をどのようにするのか決定します。そして、テストをどのように実施するのか、本番切り替えをいつ実施するのか、本番切り替え後に問題が生じた場合、どこを窓口として、どのように対応するのか合意します。

改元以外の問題があります。

10 連休明けの 5 月 7 日には、休日明けのバッチ処理で 10 日間分のデータを一斉に処理(しかも改元が絡む)しなくてはなりません。これまでの経験は、年末年始の 8 連休が最長(改元は無関係)でしたが、休日明けのバッチ処理に、過去の経験の 25%増しのデータ量を処理することが求められます。具体的には、金融機関の口座振替等が挙げられます。

また、平日と土曜日、日曜日、祝日、休日で異なる処理をしているシステムの対応があります。

2019 年には、現在の天皇誕生日(12 月 23 日)が平日に、新天皇即位の日(5 月 1 日)が祝日に、祝日の間の平日(4 月 30 日、5 月 2 日)が国民の休日に、それぞれ変わります。

2020 年には、新天皇誕生日(2 月 23 日)が祝日に、新天皇即位の日(5 月 1 日)が平日に、それぞれ変わります。

3. 消費税率引き上げ

前回の「5%」から「8%」への消費税率引き上げは、5 年前の 2014 年 4 月 1 日に実施されました。

今回は、「8%」から「10%」への消費税率引き上げと同時に軽減税率が導入されますが、本当に 2019 年 10 月 1 日に実施されるのか未確定であることが問題です。

消費税率引き上げの要件定義は、下記のようなります。

・2019 年 10 月 1 日？以降、軽減税率が適用されない物・サービスの消費税率は 10%

・2019 年 10 月 1 日？以降、軽減税率が適用される物・サービスの消費税率は 8%

要件定義にあたっての問題点は、下記のとおりです。

・本当に 2019 年 10 月 1 日に消費税率引き上げを実施するのか

・軽減税率が適用される物・サービスは、何が該当するのか

・軽減税率への対応として、テイクアウトと店内で飲食する物・サービスの場合、同一の物・サービスなので、外食(消費税率 10%)でも食料品(消費税率 8%)でもテイクアウトの容器代として 2%を徴収することで、支払総額を同額とすることも考えられています。

ここで、軽減税率の場合は消費税率が同じ 8%であっても、会計処理上の区分が異なるという隠れた問題点

があります。

・広義の「消費税」=国税の「消費税」+「地方消費税」

・現在の割合　8%=6.3%+1.7%(国税の「消費税」の 17/63)

・引き上げ後の割合　10.0%=7.8%+2.2%(国税の「消費税」の 22/78)

・軽減税率の場合の割合　8.0%=6.24%+1.76%(国税の「消費税」の 22/78)

消費税率引き上げ以外の問題点として、期間限定で実施されるポイント還元があります。

4. システム監査の立場から

いずれの対応であっても、早期の対応方針の決定および対応策の着手をしなくてはなりません。

そして、正しく間違いのない要件定義を行い、漏れのないテストの実施および確実な結果の確認、適切な時期で改修プログラム等の本番環境へリリースすることが求められます。

Java SE 8 無償サポート終了ならば、早期の対応方針決定および対応策の着手が必要です。

果たして Java を利用したシステムは、事業に必要なシステムなのか、事業に不必要なシステムならば廃止することも対応策です。事業に必要なシステムならば、有償でも Java を継続利用するのか、有償になる前に別の環境に移行するのか、一時的にでも有償で Java を継続利用し、移行準備が整ってから別の環境に移行するのか、とうことです。

改元ならば、今回は事前に時期が分かっているので、内外の他システムとのデータ連携を忘れずに、早期の対応方針の決定および対応策の着手、正しく間違いのない要件定義の実施、漏れのないテストの実施および確実な結果の確認、適切な時期で改修プログラム等を本番環境へリリースすることが必要です。

消費税引き上げならば、何が軽減税率の対象となり、どのようなポイント還元となるのか、早期の対応方針の決定および対応策の着手、正しく間違いのない要件定義の実施、漏れのないテストの実施および確実な結果の確認、適切な時期で改修プログラム等を本番環境へリリースすることが必要です。

＜講演後の討議＞

参加者の中に前回の改元に際してシステム改修等の対応をされた方がおり、30 年前という今ほど広く一般に IT が普及していない時期であっても、対応を要するシステムが多岐にわたっていたこと、「平成」の発表の翌日に改元があり、システム上は「昭和」と「平成」の並行期間があったことなど、当時の経験をお聞きすることができました。

また、今回は改元の時期があらかじめ決められており、計画的に対応を進めることが可能であるのは良いが、広く一般に IT が普及しているので、対応に間違いがあった場合の影響は計り知れないということなどの意見が出されました。

Java SE 8 無償サポート終了については、簡単な Java の歴史と位置付けを振り返ることができて良かったという感想も聞かれました。

その他、参加者の経験を踏まえた多数の意見・質問があり、貴重な時間を共有することができましたが、非常に良い内容だったのに参加者が少なかったので、時期を改めて北海道 IT コーディネータ協議会等との合同研究会で発表の機会があればとの提案がありました。

<目次>

2019.2

支部報告　【　近畿支部　第１７６回定例研究会 兼 ＩＳＡＣＡ大阪支部１２月度特別講演会　】

会員番号　1324　椋野誠司（近畿支部）

１．テーマ　**「ガバナンスを考える**
－企業社会でのガバンスと多様な健全化対策の位置付け－」

２．講師　**大阪成蹊大学名誉教授　大阪経済法科大学客員教授**
大阪市立大学大学院都市経営研究科非常勤講師
松田　貴典　様

３．開催日時　**2018 年 12 月 15 日（土）　15:00~17:00**

４．開催場所　**大阪大学中之島センター　３階　講義室 301**

５．講演概要　企業や団体、大学等が、不祥事をおこすと「ガバナンス」の問題だと一言で済まされる。 不祥事は、多様なステークホルダーに損害を及ぼし積上げてきた「コーポレート・レピュテーション（企業名声）」を失い、 企業価値を一気に消失することになる。そこで、企業等は、コーポレートガバンスの強化や内部統制の構築、ＣＳＲやコンプライサンス意識の改革などを実行してきた。また、ガバナンスの考え方のもとで、コーポレートガバナンスやＩＴガバナンス・情報セキュリティガバナンス、 内部統制、ＣＳＲ，コンプライアンス等が、どのように定義され、どのように関連し位置付けられているのか、調査・分析し考察する。

第１章　ガバナンスとは何か

（ガバナンスのもとでのコーポレートガバナンスと CSR とサステナビリティとの関係）

（１）ガバナンスについて

①ガバナンスの進化

ガバナンスとは、「統治」「管理」「支配」と訳され、組織や社会に関与するメンバーが主体的に関与する意思決定・合意形成の仕組みである。

近年、ビジネス社会では多様な不祥事が発生しており、そのたびに、統治や管理機能が改革され、ガバナンスの概念が少しずつ、変化と進化している。。

②コーポレートガバナンスの定義

企業統治と訳されるが、一律の定義はない。企業の不正行為の防止と競争力の向上が目的とされる。

③JPX（東京証券取引所）のコーポレートガバナンスコード

企業統治の指針：上場企業が守るべき行動規範。2015 年 6 月に施行。2018 年 6 月に改正。

2017 年 7 月には、上場企業の 89%までが適用している。

（２）ガバナンスの上位概念として密接に関連する CSR とサステナビリティ

①CSR とその位置付け

企業が永続的に存在していくために、経済的活動のみならず、社会的貢献、地球環境問題への取り組み、法令の順守や企業倫理を遵守するなど社会的責任を果たすことである。企業は大規模になるほど、株主の私的所有物から社会の所有物としての社会的存在という性格を強める。

②戦略的 CSR と基盤的 CSR、攻めの CSR と守りの CSR

SCSK や、ダイハツ工業の例がある。

③サステナビリティとその位置付け

持続可能性、または持続することができる、という意味である。サステナビリティへの対象は広く社会と地球環境全般をさす。経営戦略や商品の提供などにおいてサステナビリティを確保することは、CSR の観点からも最重視されている。

④サステナビリティと ESG

ESG とは、環境(E)、社会(S)、ガバナンス(G)の頭文字である。

企業の長期的成長のために ESG の３つの観点が必要だという考え方が世界的に広まっている。

ESG 投資や SDG s （持続可能な開発目標）など注目されている。

（３）【事例から学ぶ】主要な企業のガバナンス　コーポレートガバナンス等の位置づけ

日本を代表する主要な企業の経営方針や戦略等により、ガバナンスの考え方や位置付けの違いがあり、その企業のホームページから調査分析した。ガバナンスの多様な考え方や位置づけが見られ、その進化を見ることができる。

①事例１：大手自動車メーカー　トヨタ自動車

持続的成長と長期安定的な企業価値の向上を経営の重要課題

ステークホルダーとの良好な関係、顧客満足が得られる商品の提供を続けることが重要

「ＣＳＲ・環境・社会貢献」を最上位の概念として、そのなかにガバナンスを位置付け、さらになかに「コーポレートガバナンス」「リスクマネジメント」「コンプライアンス」を位置付けている。

サステナビリティの考えの中に、ESG である環境(E)、社会(S)、ガバナンス(G)を位置付けている

②事例２．大手コンピュータベンダー　富士通

「企業理念（FUJITSU　Way)」のもとに、「コーポレートガバナンス」を位置付けている。

目先の利益を追いかけるのではなく、顧客本位、社員が誇りをもち、社会に貢献するような経営

「社会・環境分野の取り組み」を最上位概念とし、マネジメント体制の中で、「コーポレートガバナンス」「リスクマネジメント」「コンプライアンス」「情報セキュリティ」を位置付けている。

③事例３．大手空調機器メーカー　ダイキン

「ダイキンについて」の中で「コーポレートガバナンス」「ＣＳＲ・環境」を位置付けて、さらに「コーポレートガバナンスの基本的な考え方」の中に、基盤的 CSR とコーポレートガバナンスを位置付けている。

コーポレートガバナンスの中に、「コーポレートガバナンス」「コンプライアンス」「リスクマネジメント」「情報セキュリティ」「知的財産権の尊重」「自由な競争と公正な取引」を位置付けており、情報セキュリティ、知的財産権の尊重、自由な競争と公正な取引の位置付けは、ダイキンの特徴である。

基盤的 CSR：意思決定と実行のスピードアップ、透明性・健全性の絶えざる高度化

④事例４．大手通信会社　NTTdocomo

経営方針を最上位にして「経営方針」「経営戦略」「コーポレートガバンス」を位置付けて、その中に、「コーポレートガバナンス体制」「情報管理」「内部統制」を位置付けている。

情報管理には、「個人情報の保護」「組織的・人的・物理的・技術的セキュリティ」が位置付けられていることは、情報セキュリティを重んじる通信会社ならの特徴と言える。

⑤事例５．大手金融機関　みずほファイナンシャルグループ

「みずほファイナンシャルグループにおける企業統治システムに関する考え方」の中に、「ＣＳＲ」と「経営体制」を最上位に置き、ＣＳＲの中で「コーポレートガバナンス」「コンプライアンス」「リスク管理」「事業継続管理」を制定している。

経営体制の中で「コーポレートガバナンス」「リスクガバナンス」「ＩＴ戦略」などが位置付けられており、ＩＴ戦略のなかで「ＩＴガバナンス」「ＩＴサイバーセキュリティ」「ＩＴ次期システム」等が位置付けられている。「ＩＴガバナンス」の明確の記述は、金融機関ならでの特徴と言える。

企業統治システムとして「1)監督と経営の分離、2)迅速かつ機動的な意思決定、3)意思決定プロセスの透明性・公正性と経営に対する監督の実効性、4) 1)~3)を実現する」を制度化

（４）【事例からの考察】企業のガバナンスの多様な考え方

事例から言えることは、企業の経営方針や経営戦略等により、ガバナンスの多様な考え方や位置づけをしている。しかし、共通的にいえることは以下である。

①持続的な成長、社会の発展に貢献、企業価値の向上の実現を目指して取り組む

②CSR やサステナビリティを掲げて、永続的に生き、持続的に発展するために企業と社会がともに成長し、社会貢献、地球環境問題に取り組み、法令遵守することや企業倫理を遵守するなど社会的責任を果たすこと。

③ガバナンス項目：コーポレートガバナンス、コンプライアンス、リスク管理、内部統制、IT 戦略、情報管理（個人情報・知的財産保護、情報セキュリティ等）等がある。

④IT ガバナンスや情報セキュリティガバナンスは表題としては掲げられず、それぞれの表題の内容のなかで記載されている。例えば、ＩＴ戦略の中で、ＩＴガバナンスを記述している。

⑤ビジネス社会では、ガバナンスを「統治」と訳し、コーポレートガバナンス、リスクマネジメント、コンプライアンスの他、業種によっては情報セキュリティ、知的財産権の尊重等の統治機能を位置付けている。

第２章　コーポレートガバナンスと情報システムのガバナンス
（IT ガバナンスと情報セキュリティガバナンス）

（１）情報システムのガバナンス

①経済産業省が定義する情報システムのガバナンス

コーポレートガバナンスの一環としての「IT ガバナンス」と「情報セキュリティガバナンス」がある。

情報システムのガバナンスの確立は企業全体の経営課題であり、経営者の仕事、経営者がなさなければならない。経営者の責任である。

②コーポレートガバナンスと IT ガバナンス、情報セキュリティガバナンスとの関係

IT ガバナンスと情報セキュリティガバナンスは一方が他方を包含する関係ではなく、一部を重複し、明確に異なる関係になる。

（2）IT ガバナンス

①IT ガバナンスのあり方と国際標準

IT ガバナンスは 2008 年 6 月に国際標準 ISO/IEC38500:JISQ38500 として規格化された。

②諸団体の IT ガバナンスの定義

・1999 年　通商産業省と日本情報処理開発協会:「企業が競争優位性構築を目的に、IT 戦略の策定・　実行をコントロールし、あるべき方向へ導く組織能力」

・日本監査役協会：IT ガバナンス委員会　「主に IT 化により新たに生じるリスクの極小化と的確な投資判断に基ずく経営効果の最大化」

・ISACA：IT Governance Institute「IT ガバナンスは取締役会および経営陣の責任である。それは企業ガバナンスの不可欠な部分で、リーダーシップおよび組織的な構造、および組織の IT がその組織の戦略および目的を保持し拡張することを保証するプロセスから成る。」

③IT ガバナンスでの経営者の役割

ISO/IEC38500:JISQ38500 が示す経営陣の 3 つの役割　EDM モデル

1)評価（Evaluate)、2)指示・方向付け（Direct)、3)モニタリング（Monitor）

④IT ガバナンスの国際標準での 6 原則

1)責任、2 戦略、3)取得、4)パフォーマンス、5)適合、6)人間行動

（3）情報セキュリティガバナンス（経済産業省が進める情報セキュリティガバナンス）

①情報セキュリティガバナンス導入の重要性

リスク管理の一環としての「情報セキュリティ対策」が重要

②情報セキュリティガバナンスの仕組み

EDM＋R モデル　EDM の結果を利害関係者に報告（Report）する。

③情報セキュリティガバナンスと IT ガバナンスのフレームワーク

情報セキュリティガバナンスと IT ガバナンスの位置付けは異なるが、実務上は多くの職員が両方の業務を携わることから、フレームワークは整合性がとれていることが望ましい。

【参考文献】経済産業省「情報セキュリティガバナンス導入ガイダンス」

（4）事例研究　IT ガバナンス及び情報セキュリティガバナンスの確立を実行する企業

①みずほ FG

経営体制のＩＴ戦略の中で、「システム構造改革推進の他ＩＴガバナンスの強化」を実践

②NTT グループ

情報セキュリティマネジメント体制を構築し、情報セキュリティがナンスを確立している。

IT ガバナンスの中に監査部をおき、各事業本部の職場業務やプロジェクトのマネジメントを監査

③キヤノン

CSR 委員会による情報セキュリティガバナンスの強化。経営層による情報セキュリティガバナンスを確

立し、情報セキュリティマネジメントの EDM モデルを実践している。

情報セキュリティガバナンスは外部からの「監督」が実施され、情報セキュリティマネジメントは「内部監査」が実施される。

（５）情報システムのガバナンスの監督とシステム監査との関係

情報システムのガバナンスである IT ガバナンスと情報セキュリティガバナンスの自律的な監視機能は、経営陣の活動の監督（Oversee）とステークホルダーによる評価である。また、監督は問題点を指摘し改善を求めることになり、監査役監査が行われる。

現場部門が実施するマネジメントシステム（IT マネジメント、情報セキュリティシステム）を対象にシステム監査が実施されるが、情報システムのガバナンスと密接に連携しており、監査役監査にシステム監査人が支援する体制で実施されることが現実的である。このことから、システム監査はＩＴガバナンスの実現に貢献することになる。

なお、FISC（金融情報システムセンター）の細溝清史理事長によれば、現在の「金融機関等のシステム監査指針」を、2019 年 3 月を目標に「金融機関等のシステム監査基準」として改訂し、「ＩＴガバナンス・ＩＴマネジメント・ＩＴコントロール」のシステム監査を実施を制度化するとしている。金融機関でのＩＴガバナンス他を対象としたシステム監査は、先進的なことと言える。

（６）コーポレートガバナンスの要となる内部統制　基本要素の COSO フレームワーク

①内部統制

コーポレートガバナンスの要は「内部統制」である。日本では「会社法」によって内部統制を整備・運用することが明確にされ、大会社に義務付けられている。

上場企業には「金融商品取引法」において、「内部統制報告書」を経営者が作成し、公認会計士が監査し、公表が義務化されている。

②金融商品取引法と会社法の求める内部統制

対象となる企業、目的、基準指針、評価、監査、罰則等に違いがある。

③内部統制のフレームワーク

COSO フレームワーク

日本では、「IT への対応」が追加され、4 つの目的と 6 つの基本的要素から構成された。

④BCM・BCP と ERM をどう位置付けるか

内部統制に関連して BCM・BCP と ERM があり、会社法上のリスク管理体制の一環でもある。

（７）ガバナンスはどのように位置づけられるか（ガバナンスモデルを事例から考察）

共通していえることは、企業経営体制で、「ガバナンス」「CSR」「サステナビリティ」が位置付けられ、その中に、「コーポレートガバナンス」「リスクマネジメント」「コンプライアンス」が位置付けられている。企業の考え方や業種によって、「情報資産管理」「情報セキュリティ」等も位置付けられている。

第３章　不祥事は何故続くのか（ガバナンス強化は不祥事を抑えられるのか）

（１）近年の企業不祥事、不祥事とその発覚

不祥事が発覚し公に認知されるに至る原因

①内部告発、②容疑者として検挙、③自ら不正行為を暴露、④外部関係者による通知

（2）不祥事とコーポレート・レピュテ―ション

不祥事を起こす企業は社会から糾弾を受ける時代

不祥事がもたらすコーポレートレピュテ―ションへの影響

「社会の変化」を正しく認識できず、「社会の認識とのギャップ」が発生する。

（3）企業不祥事の分類

縦軸：組織的⇔個人的

横軸：恣的／犯罪的⇔偶発的／事故的

（4）何故、不祥事がおこるのか

企業の組織、マネジメント能力や技術力の不足、環境や風土の違いなどにより異なる。

不祥事発生後の対応や原因の追究が再発防止策の重要課題

（5）ガバナンスの強化が不祥事の防止・減少になるのか

常に限界に突き当たることになる。

業務、組織、情報技術等の変化と進展に、「人間力とガバナンス力」の強化への投資と技術力を充足させていくことが求められる。

追加情報

ガバナンス問題を研究しているときに、日産の不祥事に対するガバナンス不全の記事がでた。

「日産　遅れた統治改革」（2019 年 12 月 11 日付け読売新聞を引用）

「NISSAN のガバナンスに関する方針・考え方について」において、NISSAN 自ら宣言していたにもかかわらず、ゴーン元会長の問題が発覚している。記事で、何故、ガバナンス不全が起こるのかを指摘している。以下、そのポイントである。

・昇進・昇格　全てゴーン容疑者の専権事項である。「ゴーンに逆らえば将来はない」

・取締役の審議は形骸化

・ガバナンスコードでは独立した社外取締役を 2 人以上とされていたが、実際には 1 人だけ

・ゴーン容疑者による会社の私物化

・グローバル企業として、統治体制の整備が遅れている等

6．所感

講師は、長年企業でのシステム監査経験等が豊富であり、ガバナンスに精通した教授として複数の大学で教鞭をとり活躍している。その知識、経験を踏まえて、様々な観点からガバナンスを捉え、事例も交えて具体的に解説していただき、非常に参考になった。

以上

<目次>

2019.2

注目情報（2019.1～2019.2）

■「情報セキュリティ 10 大脅威　2019」を公表（ＩＰＡ）

独立行政法人情報処理推進機構（ＩＰＡ）は、情報セキュリティにおける脅威のうち、2018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2019」として順位を決定し、1月30日に公表した。

新たな脅威として、「メールやSNSを使った脅迫・詐欺の手口による金銭要求」(個人4位)と「サプライチェーンの弱点を利用した攻撃の高まり」（組織4位）がランクインした。

URL：https://www.ipa.go.jp/security/vuln/10threats2019.html

＊情報セキュリティ10大脅威　2019

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1 位（注）	クレジットカード情報の不正利用	1 位	標的型攻撃による被害	1 位
1 位	フィッシングによる個人情報等の詐取	2 位	ビジネスメール詐欺による被害	3 位
4 位	不正アプリによるスマートフォン利用者の被害	3 位	ランサムウェアによる被害	2 位
NEW	メールや SNS を使った脅迫・詐欺の手口による金銭要求	4 位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
3 位	ネット上の誹謗・中傷・デマ	5 位	内部不正による情報漏えい	8 位
10 位	偽警告によるインターネット詐欺	6 位	サービス妨害攻撃によるサービスの停止	9 位
1 位	インターネットバンキングの不正利用	7 位	インターネットサービスからの個人情報の窃取	6 位
5 位	インターネットサービスへの不正ログイン	8 位	IoT 機器の脆弱性の顕在化	7 位
2 位	ランサムウェアによる被害	9 位	脆弱性対策情報の公開に伴う悪用増加	4 位
9 位	IoT 機器の不適切な管理	10 位	不注意による情報漏えい	12 位

（注）　クレジットカード被害の増加とフィッシング手口の多様化に鑑み、2018 年個人 1 位の「インターネットバンキングやクレジットカード情報等の不正利用」を本年から、①インターネットバンキングの不正利用、②クレジットカード情報の不正利用、③仮想通貨交換所を狙った攻撃、④仮想通貨採掘に加担させる手口、⑤フィッシングによる個人情報等の詐取、に分割。

<目次>

2019.2

【 協会主催イベント・セミナーのご案内 】

■SAAJ 月例研究会（東京）		
第240回	日時	2019 年 3 月 12 日(火)18:30～20:30
	場所	港区芝公園　3-5-8　機械振興会館 地下 2 階ホール http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm
	テーマ	次世代の会計業務と会計監査
	講師	株式会社 JBA ホールディングス　代表取締役／グループ CEO 脇　一郎　氏
	講演骨子	「会計業務と会計監査」と言えば、AI や RPA により「将来なくなる仕事」とされた業務だが、近年まさにアナリティクス技術や監査業界を中心とした（会計監査用）確認状デジタル化など、革新的な取り組みを進めている。当講義では、日本公認会計士協会 IT 委員会が研究報告として 2018 年 10 月 25 日に公開した「次世代の監査への展望と課題（公開草案）」などを参考に、将来の会計業務と会計監査を考察する。
	参加費	SAAJ 会員 1,000 円　非会員 3,000 円
	お申込み	https://www.saaj.or.jp/kenkyu/kenkyu/240.html

■SAAJ 近畿支部定例研究会（大阪）		
第178回	日時	2019 年 3 月 15 日(金)18:30～20:30
	場所	大阪市北区中之島　4-3-53　大阪大学中之島センター　2 階　講義室 201 http://www.onc.osaka-u.ac.jp/others/map/index.php
	テーマ	働き方改革におけるシステム監査の有用性
	講師	株式会社ディレクタイズ　エグゼクティブコンサルタント 米国公認会計士　社会保険労務士　システム監査技術者 島﨑　智久　氏
	講演骨子	2019 年４月から働き方改革関連法が本格的に施行され、多様な働き方の選択、長時間労働の是正、公正な待遇確保などが求められるようになります。その一方、企業においては、少子高齢化社会の潮流の中で、生産性向上が喫緊の課題として挙げられ、様々なツール（AI,RPA,テレワークなど）の導入が活発になってきています。 間もなく新元号になり、大きく時代が変わろうとしています。 そこで、今回は、働き方改革としてテレワークなどの多様な労働環境が選択される中で、情報シスム活用におけるシステム監査の有用性について述べたいと思います。
	参加費	SAAJ 会員 1,000 円　ISACA 大阪支部会員 1,000 円　非会員 3,000 円
	お申込み	https://www.saaj.or.jp/shibu/kinki/kenkyukai/kenkyukai178.html

<目次>

2019.2

協会からのお知らせ　【 第 18 期通常総会　開催速報 】

会員番号 2581 斉藤茂雄（事務局長）

■第 18 期通常総会開催

日本システム監査人協会第 18 期通常総会を 2 月 22 日､下記のとおり開催致しました。総会審議事項については、各審議事項について、異議なく可決しました。特別講演も多数の参加者が熱心に聴講致しました。その後、会場を倶楽部に移し、懇親会を和やかに実施致しました。

総会詳報、特別講演講演録、議事報告等は次号の会報に掲載致します。

1．日時：2019 年 2 月 22 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

3．第 18 期通常総会 議事　　13 時 30 分～15 時

13:30 開会

(1) 2018 年度 事業報告の件

(2) 2019 年度 事業計画の件

(3) 2019 年度 予算の件

14:30 閉 会

（休 憩）

4．特別講演　　15 時 30 分～17 時

15:30 開演

演題：「日本内部監査協会青木賞受賞 ー IT 会計帳簿論

～IT 会計帳簿が変える経営と監査の未来～」

講師：千葉商科大学大学院 会計ファイナンス研究科 教授 中村 元彦 氏

(日本公認会計士協会常務理事 公認会計士・税理士・IT コーディネータ)

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>

2019.2

協会からのお知らせ　【２０１９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】

２０１９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/guide.pdf）**

---------- 記 ----------

2019 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

2019 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
(1)認定申請書	○	○	様式１
(2)監査実務経歴書	○	―	様式２
(3)小論文	○	―	様式３
(4)宣誓書	○	○	様式４
(5)資格証明（写）	○	○	
(6)申請手数料振込書（写）	○	○	
(7)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

2019 年 2 月 1 日（金）～2019 年 3 月 31 日（日）（同日消印まで有効）

5．認定申請手数料（消費税 8%を含む）

申請手数料	協会会員	非会員
(1) 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。	21,000 円	31,500 円
(2) 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	10,500 円	15,750 円
(3) システム監査人補認定申請手数料	10,500 円	15,750 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参照）

以上

<目次>

2019.2

【 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			2019.2
	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	7：理事会：通常総会議案承認 28：2019 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	22：第 18 期通常総会
3月	8：年会費未納者宛督促メール発信 14：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 2-3　：第 33 回システム監査実務セミナー (日帰り 4 日間コース)前半 16-17：第 33 回システム監査実務セミナー (日帰り 4 日間コース)後半 12：第 240 回月例研究会	15：近畿支部第 178 回定例研究会
4月	11：理事会	初旬：春期 CSA・ASA 書類審査 中旬：春期 ASA 認定証発行 25：第 241 回月例研究会	21：春期情報技術者試験
5月	9：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 13：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 7/14） 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	5：支部助成金支給 11：理事会	中旬：秋期 CSA・ASA 募集案内	14：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） 25：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30 30、31:第 32 回システム監査実務セミナー (日帰り 4 日間コース)前半	
9月	13：理事会	～　秋期 CSA・ASA 募集中　～9/30 迄 7：第 235 回月例研究会 13,14:　第 32 回システム監査実務セミナー (日帰り 4 日間コース)後半	
10月	11：理事会	22：第 236 回月例研究会 27：会員向け活動説明会	21：秋期情報処理技術者試験
11月	8：理事会 8：予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/7〆切） 16：2019 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	10,17,24：秋期 CSA 面接 21：第 237 回月例研究会 下旬：CSA・ASA　更新手続案内 〔申請期間　1/1～1/31〕 30：　CSA 面接結果通知	17:「2018 年度西日本支部合同研究会　in Fukui」
12月	1：　2018 年度年会費請求書発送 1：　個人番号関係事務教育 13：理事会：2019 年度予算案 会費未納者除名承認 第 18 期総会審議事項確認 14：総会資料提出依頼（1/7〆切） 14：総会開催予告掲示 19：2018 年度経費提出期限	5：第 238 回月例研究会 13,14：第 33 回システム監査実践セミナー(日帰り 2 日間コース) 15：　CSA/ASA 更新手続案内メール 〔申請期間 1/1～1/31〕 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 10：理事会：総会資料原案審議 26：2018 年度会計監査 30：総会申込受付開始（資料公表） 31：償却資産税・消費税申告	1-31：CSA・ASA 更新申請受付 18：　春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕 22：第 239 回月例研究会	7：支部会計報告期限

<目次>

2019.2

【 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

2019 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。

分類は次の通りです。

投稿要項が変更になっておりますので、下記をご確認の上、投稿をお願いします。

□■ 会報投稿要項

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）	会報掲載「論文」募集要項（2018. 1.11 改訂） 6000 字以上。17,000 字程度。図表を含める。 システム監査の啓発、普及、理論深化、情報提供、実践、手法開発等に役立つ論文であること。 既発表論文は除く。

■投稿について

・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

・投稿された記事については「会報編集委員会」から表現の訂正や削除を求めることがあります。又は、採用しないことがあります。

・編集担当の判断で、字体やレイアウトなどの変更をさせて戴くことがあります。

お問い合わせ先：　saajeditor@saaj.jp

<目次>

2019.2

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 6 F

■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

■□■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）

<目次>