認定 NPO 法人
日本システム監査人協会報
2018 年 7 月号
No 208
No.208（2018 年 7 月号）<6 月 25 日発行>

今月号の注目記事

- 『めだか【システム監査基準・管理基準改訂とこれからのシステム監査人】』
- 『システム監査基準・管理基準の改訂作業について（3）』

写真提供：0557　仲厚吉

巻頭言

経緯、背景を知る

会員番号：1342　安部晃生（副会長）

今年３月、総務省「国民のための情報セキュリティサイト」で、従来推奨してきたパスワードの定期的変更について、「定期的な変更は不要」との方針転換がなされました。これを、マスコミで「実は危ないパスワードの定期変更」などと報道したこともあって、「パスワード変更はしないほうがよい」といった誤解を招いている面があるようです。

総務省がこうした方針転換をしたのは、米国国立標準技術研究所（NIST）が昨年発表したガイドラインに準じたものです。そこで求められているのは、あくまで「強固なパスワード設定」です。パスワードの定期的変更を義務付けると、パターン化した脆弱なパスワードになりやすく、それよりは、定期的に変更をしなくてよいから強固なパスワードの設定をしなさいというものです。

総務省が「定期的な変更は不要」としたのには、こうした経緯や背景があることを知れば、「パスワード変更はしないほうがよい」といった誤解も生じません。その意味で、方針転換の趣旨を正しく理解するためには、その「経緯」や「背景」を知ることがとりわけ重要といえます。

皆様もご承知のとおり、４月には経済産業省「システム監査基準」「システム監査基準」が改訂されました。当協会では、これらの基準の改訂内容について皆様にご理解いただくために、説明会開催や会報での解説記事などで、できる限り改訂の「経緯」や「背景」についても、ご紹介するよう努めていきたいと考えています。基準の改訂内容だけでなく、改訂の「経緯」や「背景」にも注目してみましょう。

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>

2018.6

めだか　【　システム監査基準・管理基準改訂とこれからのシステム監査人　】

第 232 回特別月例研究会が、「システム監査基準／管理基準の改訂について」をテーマとして、5 月 19 日（土）午後、機械振興会館ホールで開催された。SAAJ をはじめ、経済産業省、システム監査学会、ISACA 東京支部、IT ガバナンス協会より改訂を担当された方々が発表し、質疑応答は中身の濃いものであった。「改訂のポイント」は、次の 3 点である。

■従来のシステム管理基準においても、「IT ガバナンス」の概念や業務継続計画について定めていましたが、その公開後、「IT ガバナンス」についての JISQ38500 や業務継続についての JISQ22301 等の国際規格が成立したため、これらの国際規格との整合性をとるとともに、米国における IT ガバナンスの規格であり、国際的に影響力を有する COBIT 等の内容を踏まえた見直しを行いました。

■従来のシステム管理基準では、企画、開発、運用及び保守という概念を前提としたウォーターフォール型のシステム開発を前提としていましたが、短期間での反復した開発を行うアジャイル型のシステム開発における取扱いについても管理策として含め、また、クラウドの利用等を念頭に置いた、整理等の見直しを行いました。

■従来のシステム監査基準及びシステム管理基準は、項目の詳細についての説明がなく、運用において、各項目の内容を解説した資料を参照することが必要となっていたため、今回の見直しにより、システム監査基準には「主旨」及び「解釈指針」を、システム管理基準には「主旨」及び「着眼点」を併せて記載することにより、基準の記載内容に基づく運用が行いやすくなるよう見直しを行いました。また、システム監査基準において、実務への適用を踏まえて監査実施の流れに沿った構成の見直しを行いました。

システム監査人は、これから、監査目的や監査対象範囲で「システム監査基準／システム管理基準」を読み解いて使い方を考える必要がある。時にはシステム監査人が集まって議論する場を持ちたいと思う。

読解力について、「AI vs. 教科書が読めない子どもたち 新井紀子著 東洋経済新報社」を紹介したい。著者は、国立情報学研究所教授であり、東ロボ君の挑戦などの AI 研究と並行して基礎的読解力を調査するため大規模な「リーディング スキル テスト（RST）」を実施、日本の中高生の多くは、教科書の文章を正確に理解できないと報告している。多くの仕事が AI に代替される将来、読解力のない人間は失業するしかないという最悪のシナリオに警鐘を鳴らしつつ、人間は、「いくつになっても、読解力は養える」という仮説を提示している。システム監査人は、読解力を養うこと、誰もが理解できる文章を書くこと、誤解がないように確認しあうことが求められる。（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>

2018.6

【農政の変容と農業構造の現状、農政改革への提言（「いま蘇る柳田国男の農政改革」を読んで）】

会員番号　1428 中田和男

■はじめに

私は、兼業農家の一員として、農政の推移と、農業の行方に関心を抱いており、戦後の農地改革に始まる、新たな農政が目指した我が国農業改革の変容と挫折の履歴を見るに連れ、なぜ、改革が挫折したか、改革の方向性は如何に改められるべきかを考究してきたが、今回は、戦前から戦中を経て、戦後の農地改革に結実した農政官僚の改革の動きを振り返り、戦前の地主・小作制を打破し、小作人の解放を果たした農地改革が、その後、如何に変容して現状に至ったか、農業構造改革は如何にして挫折したか、これに対する農政の責任は如何といったところに焦点を当ててみたいと考える。

ここで、この考察に大きく関連するであろう良書が最近上梓されたので、これを参照しながら検討を進める。

１．柳田国男の農政改革提言

この書籍とは、「いま蘇る柳田国男の農政改革」　山下一仁　（新潮選書　２０１８・０１）　である。
本書は、省創設以来、農学校出身者主体の農商務省に、初の法学士として入省した柳田国男が、1900 年から1910 年までの略１０年間に活発に発言した農政に対する提言を、戦後農政官僚出身の山下一仁氏が改めて掘り起こし、現在に続く農政の変遷に投影したもので、山下氏によれば、柳田農政改革は、農地改革に至る、農政官僚の意識に多大な影響を与え、その後も、農業構造改革に対する示唆に富んだ提言となっているとされる。

柳田の提言は、当時の農業界の基本的構造である地主・小作制を批判し、悲惨な状況に置かれている小作農の救済と農業構造の改革を唱えたもので、具体的には、地主・小作制による農業構造支配の元凶ともされる、（５割にも及ぶ）高率の小作料と、その小作料の現物米納制を、小作料の低減化を図るとともに金納制に改めようとするもので、当時の農業界主流である地主・政界関係者には到底受け入れがたいものであった。（柳田国男　農政学　1902）

一方、柳田の構造改革への提言は、農地規模を拡大して、２～３ｈａのいわゆる中農を育成することにより、自立営農を実現しようというもので、地主制の下での規模平準策に留まり、当時の状況では、実現性に乏しく、農業界にさほどのインパクトを与えなかった。（柳田国男　中農育成策　1904）

柳田の提言は、農政を支配する地主・政界・農商務省上層部から完全に無視され、やがて、葬りさられてしまったが、その精神は、柳田の衣鉢を継ぐ、石黒忠篤、東畑精一、小倉武一等、改革派の農政官僚に受け継がれ、敗戦を経て、戦後の農地改革（農地解放）に結実した訳である。

尚、農地改革の発端は、時の幣原内閣の農林大臣、松村謙三氏の就任時の提言（自作農の創出）で、GHQ の民主化方針とも合致し、強力に推進された。実務の責任者は、農政局長で、やはり、改革派の和田博雄であった。和田博雄は、続く、吉田内閣では、農相に就任し、２次に亘る農地改革を強力に推進した。

農林省出身者である山下氏の農政への主張は、先述の著書に記す如く、これら改革派の系譜を受け継ぐものといえ、従って本書は、農林省改革派の主張をなすものとして参照すべきものと考えたものである。
また、本書最終章において、山下氏の農政への提言が展開されている。

そこで、私は、山下氏の主張との対比を行いながら、私の提言を整理したいと考えた。
かいつまんで言うと、山下氏の提言は、主業農家に絞った助成農政ということになり、私の主張の兼業農家へ

の助成拡充政策とは対極に位置するものといえる。

２．農地解放に始まる戦後農政の推移と変容、農業界の変貌

ここで、改めて、敗戦直後に実現した農地解放に遡り、改革の成功から、以降の農政の変容、農業構造改革の挫折の履歴、現在に至る農業界の状況を振り返り、今後に対する提言を試みたい。

農地改革は、柳田の提言の如く、農地構造を支配した地主・小作制を打破し、小作人を解放して自作農とすることに成功したが、その方策は、地主の貸付け農地を、極めて低い価格で、政府が強制的に買収し、小作人に譲渡するというもので、敗戦直後のハイパーインフレもあり、只同然の地価で農地を分け与える結果となり、云わば、従来の地主に代わり、小作人を土地所有者にすげ替えるものとなった。

このことは、以後永く、土地を取り上げられた地主層の不満を招いたものともいえる。

一方、この農地改革の徹底（第２次農地改革）は、ただでさえ零細な戦前以来の農地所有体制を、更に多数の農地所有者に分割することになり、零細農地構造が永く継続する結果となった。

このように、戦後農地改革は、小作人解放という良い結果と零細農地構造の継続という悪い結果を併有するものとなった。

農地改革当初、この耕作者農地所有制は、農家の生産意欲を高め、食料不足の解消に大きく寄与し、1960 年頃までに米不足の解消を果たすこととなった。

同時に、日本経済は、高度成長期に入り、産業用地の需要も増して、只同然で手に入れた農地を産業用地に転用し、大きな利益を得る例も出るに至った。但し、この動向は、産業界の要請に応えるものといえ、必ずしも農家側に責任があるとは言えない。

また、工業化に伴う人手不足は、農家においても、農外収入の機会を得ることになり、さらに、その収入が農業収入を凌駕するという、いわゆる兼業化の動きを加速することになった。

このため、農家は、農外収入が農業収入を上回る第２種兼業農家が一般的になり、敢えて農業収入を増大する必要性は乏しくなり、農業の省力化（農業従事時間の短縮）がより重要となっていく。

このような省力化に寄与する農機が、田植え機とコンバイン収穫機であった。

兼業体制による零細農地構造の温存状態への対策として、農政は、規模拡大策を唱えたが、規模拡大のための農地供給者として、兼業層を期待したところ、兼業層は、省力化により、片手間で出来るようになった農業から退出する動機に乏しく、農政の期待は、空振りに終わった。その後も、農政は一貫して規模拡大策を唱えているが一向に実績が上がらず、云わば、破綻した農政と言わざるを得ない。

一方、食料不足解消後の米生産構造は、供出制度に伴う、高生産者米価の後遺症とも言える高米価構造のもと、一転して、供給過剰となり、高米価と相俟って、需要は一貫して減少、需給ギャップは拡大の一途をたどることとなった。この対策として取り入れられたのが、需給調整（減反）政策で、本来、市場の推移に任すべき米価を、高値に維持して農業収入を補填し、代わって、減反により需給ギャップを解消するという、逆立ちしたような政策が永く続けられた。

この結果は、減反率が３９％にも達するという維持不可能の状況に立ち至り、現在に至っている。

この間、このような体制の恩恵を受けたのは、農政の主張とは逆に、主業農家であったといえる。

即ち、主業農家に取って、米価の動向は、死活的要素であるが、兼業層に取っては、農業収入にあまり依存しないことから、米価は、さほど関心を持たれていない。

ここにきて、ようやく減反廃止、市場価格重視等の動きも出ているが、いささか遅きに失した感もあり、この間における農政は、必ずしも適切であったとは言えない。即ち、農政の重点は、高米価維持による主食米の

需要減少に対応する供給制限に終始し、それが、減反、転作、あるいは他用途米奨励等の政策に現れている。

典型的なのは、減反廃止による主食用米過剰への懸念から採り入れられた飼料用米補助で、主食用米の生産を抑え、米を飼料用に転用することにより、畜産飼料を米により賄うというもので、このための方策として、本来の飼料である麦・とうもろこしの価格に米の価格をさや寄せするため、高率の差額補填を行うもので、結果、補助率８０%にも達する飼料用米の奨励という馬鹿げた結果を招いている。

３．今後の農政への提言

ここで、今後の農政について検討を加えると、基本的に、米価は市場の推移に委ねるべきであり、その結果、農業が立ちいかないとすれば、生産原価と市場価格の差額を所得補償すべきということになり、これは、米国、EU はじめ、世界の趨勢にも合致するものである。

ここで、山下氏は、補助の対象を主業農家に絞るべきで、農家の多数を占める兼業農家は、退場を促すべきとの提言をされている。山下氏の提言は、主業農家育成、兼業農家退場こそが、農政の基本である経営規模の拡大にも寄与する、自立農家育成策であるとされるが、これは、柳田以来の中農育成の伝統を継ぐものともいえ、柳田同様、理想的農政の挫折の道をたどるものとも言える。

私は、経営規模拡大策は、すでに破綻しており、更に、このような政策は、農地改革による自作農創設の意義を失わしめるものと考える。そこで、私は、逆に、農家の太宗を占める、兼業農家の育成こそが、農業、農村、農地の維持につながると考え、以前にも、兼業農家育成策を提言したところである。

：会報投稿 2017.02［米補助金見直し報道に接して］

尚、その際、専業（主業）と兼業の生産原価の比較から、農政の主張する兼業の高コスト性が、必ずしも妥当と言えないことも説明したところであり、参照頂ければと思う。　：同投稿　2017.02

又、所得補償についても、兼業農家に於いては、所得の赤字を補填して、農業継続の意欲を高める程度に留める事ができ、主業農家に対する補償程の高率を要しないと考える。要は、少数の主業農家を保護するよりは、農家の太宗を占める兼業農家の生産意欲を高める事が、正当と考える。何故なら、兼業農家の衰退は、農村集落の崩壊に繋がると考えるからである。

以上、私は、農業、農村、農地の維持のためには、兼業農家の再育成こそが必須であり、仮にも、兼業農家の退出により、主業農家を保護することがあってはならないと考える。

その上で、兼業農家を中心とする、農村集落の再建策については、更に、提言を続けたいと考えている。最近、IOT,AI の取り入れ等、産業の第四次革命がとなえられているが、農業においても同様の方向性が考えられ、農業の高度化による農村の再建が必要となり、我々、システム監査人としても、このような動向にも着目すべきと考えている。

この場合、粗放的な主業農家の農業よりは、兼業農家の小規模農業こそが、高度農業技術の導入に適しており、兼業農家により有利な情勢と考えられる。従って、このような気運を捕え、第四次産業革命を兼業農家主体の農村・農業改革に結びつける視点も必要と考える。

（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>

2018.6

本部報告

第２２８回月例研究会　【事業者が考えるデータ利用及び今後の展望や課題】

会員番号　2574　竹原 豊和　（月例研究会）

【講師】　日本情報経済社会推進協会　常務理事　電子情報利活用研究部担当（部長兼務）
認定個人情報保護団体事務局担当
坂下　哲也　氏

【日時・場所】2017 年 12 月 15 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】　「事業者が考えるデータ利用及び今後の展望や課題」

【要旨】

官民データ活用推進基本法も成立し、データを利用したサービス検討が活発になっている。本講義では、最近のデータ利用を取り巻く産業界等の状況を俯瞰し、今後の展望や解決すべき課題について解説する。

【講演録】

1．準天頂衛星 4 号の打ち上げ成功から考えられること

準天頂衛星 4 号打ち上げ成功した事例から、今後どのような変化と利便性が国民生活にもたらされるか、ということを考えた場合、GPS の発展が非常に大きいと考える。今までの GPS においては精度の問題で、高さ情報を取得することは得意では無かったが、準天頂衛星 4 号の打ち上げ成功により、高さデータにおいても取得することが可能となる。

位置情報の活用として、広告マーケット効果が予測される。今後、位置情報による広告市場は 2020 年に約 65 億ドル（約 7450 億円）、2021 年は約 72 億ドル（8260 億円）と予測されている。但し、精度があがるということはセキュリティに関しても考慮することがあるということも同時に意味する。

2．データを利用したサービスの事例

製造業・建築業におけるデータを利用したサービスの事例として、最初に考えるべきことは、製造事業者が抱えている課題である。作業員は減少しており、故障発生時のタイムラグの圧縮も必要となる。実際に、現状においても「熟練作業者の勘」に頼って業務が行われていることが散見される。そんな状況の中、新しい試みとして、メーターや流量計をカメラで撮影し、画像解析によりデータを読み取る、という手法が開発されている。この撮影にて読み取った値をサーバに送信し、予防保守を行うことが可能となる。

さらに、走っている車でデータ収集も可能となる。車にセンサーを実装し、走りながら地図データを取得することや細かい道路の起伏においてのデータを取得することも可能となる。

様々な企業事例が既にある中で、「マイナンバーカード」に対する資格情報の格納を JIPDEC では提案していきたいと考える。マイナンバーカードの IC チップに資格・学歴の情報を格納することで、履歴書への記載や取引先において必要な資格（危険物取扱者など）を確認することができる。これらについて、マイナンバーカードが普及しているドイツでは、既に実用化されている状況となっている。

次に、農業におけるデータを利用したサービスの事例を考える前に、農業においても「熟練作業者の勘」についても課題となっている。川崎のルートレック・ネットワークスという企業において、M2M とクラウド技術

による全天候栽培アルゴリズムが開発されており、解決への糸口となる。

その他の業種の事例として、甲州呉服店のように着ていない着物を借りられるような仕組みや幼稚園児・保育園の園内見守りサービスのようなことが可能となる。そして、この試みにより、保育士さんの稼働は 4 割ほど減っている。

IoT に関するセキュリティとして、ガイドラインの ver1.0 を 2016 年 7 月に公開しているが、こちらについては「原則的なもの」しかない状況となっている。EU においては ENISA が Cybersecurity certification framework を提案しているが、ENISA が EU における認証機関になることを提案している状況であり、具体的なセキュリティの概要については標準規格を採用する旨が記載されているのみとなっている。これに対し、ドイツは ENISA に反対しており、米国と組む状況となっている。最終的には、各国に独自の認証機関が置かれる可能性が考えられる。

3. 官民データ活用推進基本法以後の動き

官民データ活用推進基本法という法律があり、この中の 12 条にある「個人の関与の仕組みの構築等」を見ればわかるようにデータの公開計画は動いている状況となっている。

様々な事業者において、行政が保有するデータについて個人を特定するために利用したい、というニーズや、営業等の目的で、事業者を特定するためにデータを利用したい、というニーズもある。例えば、障害者の方は普通のアパートが借りられずに困っている状況であるが、デイケアを利用することで解決が可能となる。しかし、障害者の方が利用できないと考えられており、そういった意味で情報をオープンにすることで利用が増えると考えられる。

また、非識別加工に関する相談の例として、小学校から得た情報を活用し、「朝ごはんを食べると数学の点数が高い」など学習能力を上げることも可能となる。

情報を預託する仕組みとして「データ流通推進協議会」が新たに設立されており、データをどのように流通させるかも含めて協議が行われている。経済産業省の仕組みとしては、データ共有事業者が、あくまでも公共性が高いことを条件として、事業計画書を提出することで認定が下りるということを検討している。

4. パーソナルデータに関する動き

EU では、データ移転を踏まえた一般データ保護規則として、GDPR を採択しており、こちらは 2018 年 5 月に完全施行となる。この中で重要なことは、忘れられる権利として、ネット上の個人データやリンクを本人からの削除要求に応じて削除を通知する義務があることが挙げられる。但し、日本で GDPR と同様の制度が施行されるのはまだ先と考える。

日本と EU にてデータ移転の交渉が進められており、この中で 2018 年の早い段階でデータの交換を実現する旨が大筋で合意がされている。

匿名加工情報に関する相談や問い合わせは、JIPDEC に多数ある状況となっており、こちらについては JIPDEC の認定団体に入っていない所からも多い。但し、相談は受け付けている。　この中で「カメラ画像の利用分類」については多数の相談があるため、総務省や経済産業省での協議が必要となっている。

なぜ、データを活用するのか、ということを考えた場合、「ディダクション」「アブダクション」「デザイン・アブダクション」「インダクション」というポートフォリオで考えることができる。ビッグデータの場合、Volume、Variety、Velocity が重要となり、ディープデータの場合、Operational、Historical、Relational が重要となる。また、知財を保護する仕組みも必要と考える。

ブロックチェーンの標準化において、ISO/TC307、ISO/PC308、ISO/TC309 という 3 つの技術委員会の設置が採択されており、日本においては JIPDEC が担当している。現状でもブロックチェーンはビットコイン以外で活用されており、私的契約をブロックチェーン上に記述するスマートコントラクトなどが開発されている。

5. まとめ（今後に向けて）

データにはオープンとクローズの 2 通りがある。例えば、ダヴィンチの場合、活動は王侯貴族のパトロンによる支援であったためクローズであり、死後にその存在が明らかになっている。また、デューラーの場合はオープンであり、公開にて新しい知の可能性が開かれている。学術研究に関しても 16 世紀以降は「新」が付く出版物が多く、これらはビッグデータ解析と同様にオープンデータから考証する学問となっている。

今後、日本においての人口構成の変化も注目すべきところであり、生産労働力が減ると考えられる。その際に、警察官や消防署員、自衛隊員も減っていき、超高齢化社会になっていくと考えられ、そちらについても対応が必要となる。例えばインドにおいても高齢化の波は押し寄せており、インターネットを老人に活用してもらうために、古い iPhone を使用して老人の IT 教育を実施している。

また、資源も枯渇していく方向となっており、資源価格も上昇すると考えられるが、一方で世界人口は 4 倍になるとも考えられる。企業においても再生をキーワードに様々な活動が行われており、H&M のように古着を持ち込むと割引券を配布する試みもある。

モノの見方は様々であり、鳥の目、虫の目、魚の目という具合に様々な視点から今後の将来や、生活におけるデータ活用を考える必要がある。イノベーションを興すためには、「様々なモノ、コトを機械処理要素に変える」「エネルギーの変化」「どこでもうながる、モノがつながる」「ロボット、自律、3D プリンタなどの労働合理化」という 4 つの要素が必要であり、業界を横断して対応していくことが今後は重要となっていく。

【所感】

データは使い方によっては、国民生活の経済的発展へと活かせれば、極端に言えば犯罪にも利用される可能性があり、非常に取扱が重要であることをあらためて認識した。その上で、先生がおっしゃっていたとおり、様々な視点から考えていく必要があり、また、データやセキュリティについて、適切な仕組みが構築されているかについて監査するのが我々の役割であるということも再認識した。

特に、今後は AI やビッグデータ、そして IoT が身近になる中で、それらに紐づくデータをどのように取り扱うか、どのようにデータ移転を行うか、またデータにおけるセキュリティ対策をどのように行うか、ということは、多くの国、企業、団体において課題であると考える。

これら課題に対して、今後はシステム監査人である我々がしっかりとシステム監査を行い、これら様々なデータを活用したイノベーションへの発展に寄与することが求められると感じた。最後に、マイナンバーカードは今後是非活用すべきであると、私自身強く感じたことも記載させていただく。

以　上

<目次>

2018.6

第３２回ＣＳＡフォーラム開催報告
【 解説！「発注者のプロジェクトマネジメントと監査」 】

会員番号 2581 斉藤 茂雄（CSA 利用推進 G）

協会では2018年2月に「発注者のプロジェクトマネジメントと監査」（同文館出版）を出版致しました。本書には、「システム開発トラブル未然防止の神髄に迫る」という副題で、プロジェクトを失敗させないための「肝」が述べられています。今回の第32回ＣＳＡフォーラムでは、プロジェクトマネジメントのシステム監査研究会を立ち上げ、3年数カ月の間本書の出版の企画から構成・執筆に心血を注いだ、協会理事の原田憲幸氏に、本書のポイントを解説いただきました。

原田氏は1973年に電電公社に入社、その後ＮＴＴコムウェアなどでシステムの構築やコンサルに豊富な経験をお持ちです。そのような経緯で、原田氏には2014年6月のＣＳＡフォーラムで『トラブルを未然防止するプロジェクトマネジメント』というお話頂きました。それが今回の出版にも繋がりました。

「プロジェクトを失敗させない」ということに皆さん非常に関心が高く、今回は30名の参加者がありました。大変熱心に聴講いただき、質疑もかなり実践に踏み込んだ内容になり、有意義なCSAフォーラムが開催できたと思います。また、終了後講師を囲んで短時間ですが懇親会を実施致しました。

【書籍ご案内】 https://www.saaj.jp/04Kaiin/KokaiYoshiki/130801PRJMChirashi.pdf

タイトル：解説！「発注者のプロジェクトマネジメントと監査」

概要：（以下の書籍の目次に従って解説いただきました）

導入 １章 トラブル事例と教訓
２章 トラブル未然防止の基本
３章 受/発注それぞれの役割

発注者のプロジェクトマネジメント
４章 企画/要件定義/調達…開発の成/否は企画で決まる
５章 プロジェクト計画
６章 外部設計………………仕様凍結が鍵
７章 実装設計………………高品質設計
８章 プログラミング、単体テスト、結合テスト…高品質と検証
９章 総合テスト、受入試験・検収、業務運用試験、移行、サービス開始判定、システムの効果検証
10 章 実践的品質管理
11 章 ＜発注者視点＞のプロジェクトマネジメントの基本

成功に導く「プロジェクト監査」
12 章 トラブルを未然防止する………なぜプロジェクト監査が必要か？
13 章 プロジェクト監査（企画フェーズ）
14 章 プロジェクト監査（設計開発フェーズ）
15 章 プロジェクト監査（サービス開始、効果検証フェーズ）

開催日時： 2018 年 5 月 28 日（月） 18 時 30 分～20 時 30 分
開催場所： 中央区日本橋兜町 12-7 兜町第 3 ビル NATULUCK 茅場町新館 2 階大会議室

ＣＳＡフォーラムはＣＳＡ・ＡＳＡの皆様が、「システム監査に関する実務や事例研究、理論研究等」を通して、システム監査業務に役に立つ研究を行う場です。ＣＳＡ・ＡＳＡ同士のフェイスｔｏフェイスの交流を図ることで、相互啓発や情報交換を行い、ＣＳＡ・ＡＳＡのスキルを高め、よってＣＳＡ・ＡＳＡのステータス向上を図ります。

ＣＳＡ利用推進Ｇのキャッチフレーズ
＊＊ＣＳＡ・ＡＳＡを取得してさらに良かったと思ってもらえる資格にしましょう！！

＜目次＞

2018.6

システム監査基準・管理基準の改訂作業について（3）

会員番号　0555 松枝憲司（IT アセスメント研究会）

1．システム監査基準・管理基準の公開

システム監査基準及び管理基準が 2018 年 4 月 20 日に公開されました。

http://www.meti.go.jp/policy/netsecurity/sys-kansa/h30kaitei.html

○改訂のポイント（経済産業省の HP から）

「 •従来のシステム管理基準においても、「IT ガバナンス」の概念や業務継続計画について定めていましたが、その公開後、「IT ガバナンス」についての JISQ38500 や業務継続についての JISQ22301 等の国際規格が成立したため、これらの国際規格との整合性をとるとともに、米国における IT ガバナンスの規格であり、国際的に影響力を有する COBIT 等の内容を踏まえた見直しを行いました。

•従来のシステム管理基準では、企画、開発、運用及び保守という概念を前提としたウォーターフォール型のシステム開発を前提としていましたが、短期間での反復した開発を行うアジャイル型のシステム開発における取扱いについても管理策として含め、また、クラウドの利用等を念頭に置いた、整理等の見直しを行いました。

•従来のシステム監査基準及びシステム管理基準は、項目の詳細についての説明がなく、運用において、各項目の内容を解説した資料を参照することが必要となっていたため、今回の見直しにより、システム監査基準には「主旨」及び「解釈指針」を、システム管理基準には「主旨」及び「着眼点」を併せて記載することにより、基準の記載内容に基づく運用が行いやすくなるよう見直しを行いました。」

具体的には、行為規範・基準として徹底させるために、

「誰が、なにを、どのように」に留意するのかを明確にするため、各項目上で「主語」を明示し、「すべきこと」と「することが望ましいこと」を区別しました。

【管理基準】各項目（誰が、なにを、どのように、すべきこと）、

主旨　（各項目の目的を記述）

留意点（誰が、なにを、どのように、すべきこと／することが望ましいこと）を記述した。

2．システム管理基準の概要

[1] 前文(システム管理基準の活用にあたって)

本基準は、どのような組織体においても情報システムの管理において共通して留意すべき基本的事項を体系化･一般化したものである。したがって、本基準の適用においては、基準に則って網羅的に項目を適用するような利用法は有効ではない。事業目的、事業分野における特性、組織体の業種・業態特性、情報システム特性などに照らして、適切な項目の取捨選択や各項目における対応内容の修正、情報システムの管理に関連する他の基準やガイドから必要な項目を補完するなど、監査及び管理の主旨が実現できるように独自の管理基準を策定して適用することが望ましい、としている。

[2] システム管理基準の枠組み

1. IT ガバナンスの定義

IT ガバナンスとは経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動

であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力である。

今日では、クラウドサービスやアウトソーシング等、外部の資源を組み合わせる手法が一般化していることから、本基準では情報システムをハードウェア、ソフトウェア、ネットワークに加えて、外部のサービスや業務プロセスを含む概念として用いている。そのため、本基準における IT ガバナンスとは情報システムのガバナンスであり、IT マネジメントとは情報システムのマネジメントである。

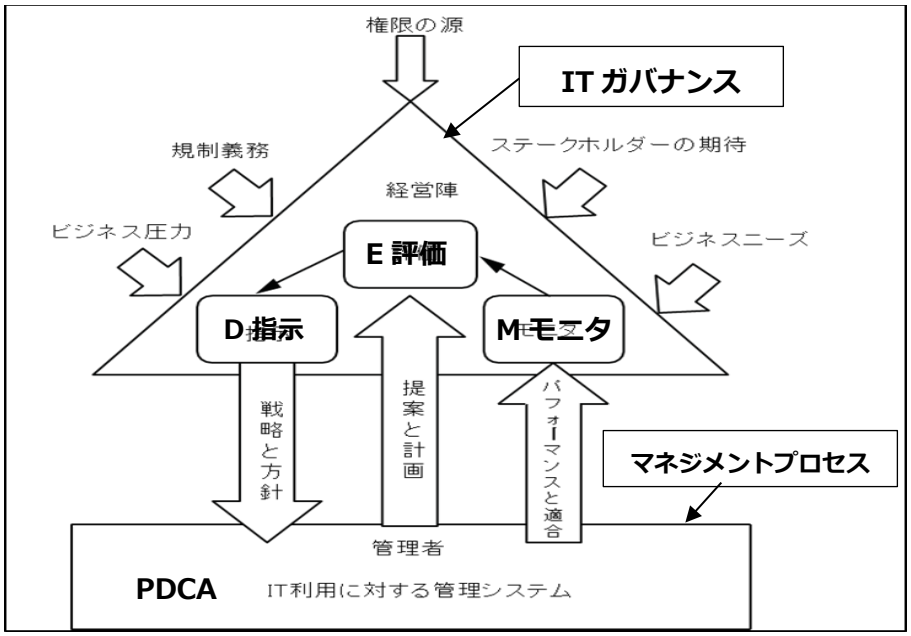
2. IT ガバナンスにおける EDM モデル

IT ガバナンスの定義における経営陣の行動を、情報システムの企画、開発、保守、運用に関わる IT マネジメントとそのプロセスに対して、経営陣が評価し、指示し、モニタすることとする。また、IT ガバナンスにおける国際標準である ISO/IEC 38500 シリーズ及び日本での規格である JIS Q 38500 より、評価（Evaluate）、指示（Direct）、モニタ（Monitor）の頭文字をとって EDM モデルと呼ぶ。

・評価とは、現在の情報システムと将来のあるべき姿を比較分析し、IT マネジメントに期待する効果と必要な資源、想定されるリスクを見積もることである。

・指示とは、情報システム戦略を実現するために必要な責任と資源を組織へ割り当て、期待する効果の実現と想定されるリスクに対処するよう、IT マネジメントを導くことである。

・モニタとは、現在の情報システムについて、情報システム戦略で見積もった効果をどの程度満たしているか、割り当てた資源をどの程度使用しているか、及び、想定したリスクの発現状況についての情報を得られるよう、IT マネジメントを整備すると共に、IT マネジメントの評価と指示のために必要な情報を収集することである。



出典 ISO/IEC38500:2015 の翻訳と加筆

3. IT ガバナンスにおける 6 つの原則

IT ガバナンスを成功に導くため、経営陣は、次の 6 つの原則を採用することが望ましい。

① 責任：役割に責任を負う人は、その役割を遂行する権限を持つ。

② 戦略：情報システム戦略は、情報システムの現在及び将来の能力を考慮して策定し、現在及び将来のニーズを満たす必要がある。

③ 取得：情報システムの導入は、短期・長期の両面で効果、リスク、資源のバランスが取れた意思決定に基づく必要がある。

④ パフォーマンス：情報システムは、現在及び将来のニーズを満たすサービスを提供する必要がある。

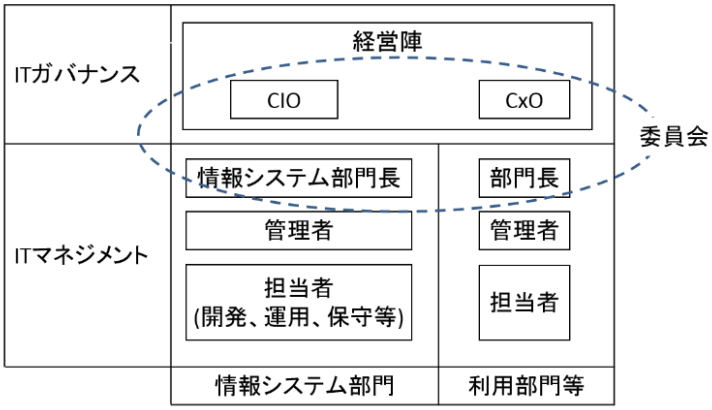
⑤ 適合：情報システムは、関連する全ての法律及び規制に適合する必要がある。

⑥ 人間行動:情報システムのパフォーマンスの維持に関わる人間の行動を尊重する必要がある。

4．システム管理基準の前提となる組織体制

本基準は判りやすく具体化したものとするために、モデル化した組織体制を前提とした記述となっている。そのため、本基準を利用する際に、自らの組織に適合するように読み替える必要がある。

本基準が想定する組織体制を示す。



①経営陣

経営陣は IT ガバナンスの担い手であり、業務執行に責任を有する。実際の組織では、取締役（会）、経営者、理事(会)等のことを指し、一人とは限らないため、経営陣という表現を用いている。

②CIO

CIO は経営陣に含まれる。小規模な組織等で CIO を任命しない組織では CIO に関する新基準の記載内容は「経営陣」として読み替える必要がある。

③委員会（情報システム戦略委員会，プロジェクト運営委員会等）

組織全体にまたがる利害関係者の調整が必要となる意思決定に際して、経営陣は複数の部門長を含む委員会を設置する場合があり、経営陣の権限を委譲されていることから、新基準では経営陣の一部と見做す。小規模な組織で調整が容易な場合等は委員会に関する記述は経営陣として読み替える。

④情報システム部門

組織内における IT マネジメントの担い手を新基準では「情報システム部門」と呼ぶ。情報システムに関する各種業務の「担当者」、担当者を管理する「管理者」、情報システム部門の長である「情報システム部門長」で構成され、組織によっては、経営陣・CIO が情報システム部門長を兼任しているケース、管理者が情報システム部門長の職務を兼ねるケースがありうる。

⑤利用部門等

「情報システム部門」以外の組織体制を「利用部門等」その長を「部門長」と呼ぶ。

情報システム部門と同様に、部門長を設置しない組織では、新基準の該当箇所を経営陣あるいは管理者として読み替える必要がある。

[3]システム管理基準のポイント

Ⅰ．IT ガバナンスに関する管理基準の構成

1.情報システム戦略の方針及び目標設定

2.情報システム戦略遂行のための組織体制

3.情報システム部門の役割と体制

4.情報システム戦略の策定の評価・指示・モニタ（EDM）

5.情報システム投資の評価・指示・モニタ（EDM）

6.情報システムの資源管理の評価・指示・モニタ（EDM）

7.コンプライアンスの評価・指示・モニタ（EDM）

8.情報セキュリティの評価・指示・モニタ（EDM）

9.リスクマネジメントの評価・指示・モニタ（EDM）

10.事業継続管理の評価・指示・モニタ（EDM）　となっている。

本フェーズにおける旧基準との最も大きな相違点は、「全体最適化」から「IT ガバナンス」へのコンセプトの変更である。旧基準では「全体最適化」という用語が、「全体最適化の方針」、および「全体最適化計画」という表現で多数出現していたが、「全体最適化」については、以下の点から見直しを行った。まず「全体最適化」の「全体」の対象が不明確であること、またある時点における「最適化」を検討したとしても、変化をし続ける環境の下では、常にその見直しが必要となり、この概念を中核に置くことは現実的ではないこと等である。

このような環境下において経営陣が備えるべきものとして、IT ガバナンスを採り上げた。

前述のシステム管理基準の枠組みにあるように、経営者の職務(Task)として、評価(Evaluate)、指示(Direct)、モニタ(Monitor)の 3 つを定義して「EDM モデル」と呼び、旧基準の「Ⅰ．全体最適化」の内容を「評価」「指示」「モニタ」の観点で整理した。

例えば、新基準「Ⅰ．IT ガバナンス　4．情報システム戦略の策定の評価・指示・モニタ」では、評価に関して「経営陣は、経営計画で示した事業の方針及び目標に基づいて、情報システム戦略を評価していること。」、指示について「経営陣は、情報システム戦略の策定を情報システム戦略委員会等に、指示していること。」、モニタについて「経営陣は、情報システム戦略を関係者への周知徹底を指示することと、その結果をモニタすること。」というように、それぞれの職務を示す動詞を用いて明確化した。

このフェーズにおけるポイントは、「経営者は、正解を見いだせにくい最適化問題を解くのではなく、環境の変化に適応すべく EDM を回していくことに注力すべきである。」としている点にあります。

<目次>

2018.6

本部報告　PMS 要求事項【JIS Q 15001:2017】と「個人情報取扱規程」の事例　　管理策 4

会員番号　1760 斎藤由紀子　（個人情報保護監査研究会）

新個人情報保護法において、「要配慮個人情報」が規定されました。法律が JIS に追いついてきたともいえます。要配慮個人情報を取得する場合は、”書面による”本人の同意が必要です。
また、2006 年版 JIS において、3.4.2.4 は「本人から直接書面によって取得」でしたが、「個人情報を取得した場合の措置」が、3.4.2.4 となりました。つまり、個人情報の取得における原則論が、3.4.2.4 に記述されることとなったものです。
今回も、附属書 A（規定）および附属書 B（参考）の要求事項を確認しつつ、できるかぎりシンプルな規程として「3300 個人情報取扱規程」のサンプルをご紹介したいと思います。

※ この連載を基にした HTML 版を公開しています。
規格本文＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/000JISQ15001_2017.html
管理策 1＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/001JISQ15001_2017.html
管理策 2＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/002JISQ15001_2017.html
管理策 3＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/003JISQ15001_2017.html
管理策 4＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/004JISQ15001_2017.html

引用：日本規格協会「日本工業規格 JIS Q 15001:2017 個人情報保護マネジメントシステム要求事項」

赤字：【2006 年版 JIS】から追加、変更となった規格

青字：PMS 監査研究会のコメント

A.3.4　実施及び運用　（2006：3.4） 目的　運用段階において個人情報の取扱いを行うため。		
A.3.4.1	運用手順 2006：3.4.1	組織は、個人情報保護マネジメントシステムを確実に実施するために、運用の手順を明確にしなければならない。
	附属書 B	なし
	【P マーク審査のポイント】 ・「運用の手順」には、手順書レベルの規定も含まれる。 ・手順書、様式等を規定した場合は上位規程に規定し、「PMS 文書体系」に含めること。	

【3300 個人情報取扱規程】サンプル

3.4　実施及び運用

3.4.1　運用手順

当社は PMS を確実に実施するために、運用の手順を明確にする。

■

A.3.4.2　取得・利用及び提供に関する原則　（2006：3.4.2）		
A.3.4.2.1	利用目的の特定 2006：3.4.2.1 法第 15 条	組織は、個人情報を取得するに当たっては、その利用目的をできる限り特定し、その目的の達成に必要な限度において行わなければならない。 組織は、利用目的の特定に当たっては、取得した情報の利用及び提供によって本人の受ける影響を予測できるように、利用及び提供の範囲を可能な限り具体的に明らかにするよう配慮しなければならない。
	附属書 B 3.4.2.1	“利用目的をできる限り特定し”とは、利用目的を単に抽象的、一般的に特定するのではなく、組織が最終的にどのような目的で個人情報を利用するのかを可能な限り具体的に特定することをいう。個人情報の利用目的は、個人情報の項目ごとにその利用目的が異なる場合、項目ごとに区別して特定することが望ましい。単に“事業活動に用いるため”、“提供するサービスの向上のため”、又は“マーケティング活動に用いるため”と表現することは、A.3.4.2.1 に適合しない。 また、消費者など、本人の権利利益の観点からは、事業活動の特性、規模及び実態に応じ、事業内容を勘案して顧客の種類ごとに利用目的を特定して示したり、本人の選択に

		よって利用目的の特定ができるようにしたりするなど、本人にとって利用目的がより明確になるような取組みが望ましい。 なお、特定した利用目的は、A.3.4.2.4 及び A.3.4.2.5 に基づき通知若しくは公表する、又は明示することが定められている。
	【P マーク審査のポイント】 ・利用目的は、本人から見て分かりやすい状態で明らかにされている必要がある。 ・取得する個人情報の項目（氏名、年齢、住所など）ごとに利用目的を特定することを必須とするものではない。 ・新規にプライバシーマークを取得する際は、利用目的の特定に関する記録（A.3.5.3 e)、個人情報の特定に関する記録（A.3.5.3 a)）として、「個人情報管理台帳」を用いて承認を得ても差し支えない。 ・PMS の運用開始以後にあらたに発生する個人情報の利用目的の特定に関する承認の記録は、「個人情報管理台帳」ではなく「個人情報取得・変更申請書」を用いる。 ・本人に対する通知又は公表の記録（A.3.4.2.4)は、公表文書「個人情報の取扱いについて」を定める。 ・本人に明示した書面（A.3.4.2.5)とは、通知文書「個人情報の取り扱いについて（従業者用）」などをいう。 ・通知・公表・明示された利用目的は「個人情報管理台帳」に特定された利用目的の範囲内であること。 ※明示とは文書で示すこと。明示する場合の同意は「文書」で取得することが望ましい。	

【3300 個人情報取扱規程】サンプル

3.4.2　取得、利用及び提供に関する原則

3.4.2.1　利用目的の特定

個人情報を取得するに当たっては、その利用目的をできる限り特定し、その目的の達成に必要な限度において行わなければならない。

a) 個人情報を取得する業務の部門長は、あらかじめ「3421 個人情報取得・変更申請書」に必要事項を記載し、必要文書を添付して、個人情報保護管理者へ提出する。
b) 個人情報保護管理者は「3421 個人情報取得・変更申請書」および添付書類の内容が妥当であるかを確認して承認する。
c) 部門長は、承認された「3421 個人情報取得・変更申請書」に基づき、個人情報を取得することができる。

■

A.3.4.2.2	適正な取得 2006：3.4.2.2 法第 17 条	組織は、適法、かつ、公正な手段によって個人情報を取得しなければならない。
	附属書 B 3.4.2.2	“適法、かつ、公正な手段によって個人情報を取得し” に反する例として、少なくとも次の事項がある。 a)利用目的を偽るなど不公正な手段によって個人情報を取得すること b)優越的な地位を利用して個人情報を取得すること 不正の利益を得る目的で、又はその保有者に損害を加える目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、不正に取得したり、不正に使用・開示した場合には、不正競争防止法（平成 5 年法律第 47 号）第 21 条、第 22 条によって刑事罰（行為者に対する 10 年以下の懲役もしくは 2,000 万円以下の罰金、又はその併科。 法人に対する 5 億円以下の罰金）が科され得る。 また、第三者からの提供（法第 23 条第 1 項各号に掲げる場合並びに個人情報の取扱いの委託、事業の承継及び共同利用に伴い、個人情報を提供する場合を除く。）によって、個人情報（政令第 2 条第 2 号に規定するものから取得した個人情報を除く。）を取得する場合には、提供元の方の遵守状況（例えば、オプトアウト、利用目的、開示手続き、問い合わせ・苦情の受付窓口を公表していることなど）を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、例えば、取得の経緯を示す契約書などの書面を点検するなどによって、当該個人情報の取得方法などを確認した上で、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段によって取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。 【不正の手段によって、個人情報を取得している事例】 事例 1)親の同意がなく、十分な判断能力を有していない子どもから、取得状況から考えて関係のない親の収入事情などの家族の個人情報を取得する場合。

		事例 2)法第 23 条に規定する第三者提供制限違反をするよう強要して個人情報を取得した場合。 事例 3)他の事業者に指示して上記事例 1）、事例 2)などの不正の手段で個人情報を取得させ、その事業者から個人情報を取得する場合。 事例 4)法第 23 条に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにも関わらず、個人情報を取得する場合。 事例 5)上記事例 1)、上記事例 2)などの不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにも関わらず、当該個人情報を取得する場合。
	【P マーク審査のポイント】 ・適正に取得されているかどうかについての審査では、「個人情報管理台帳」、公表文書「個人情報の取り扱いについて」、通知文書「個人情報の取り扱いについて（従業者用）」などにより確認する。 ・委託元、提供元が適正な取得をしていることを確認していることを、確認する。	

【3300 個人情報取扱規程】サンプル

3.4.2.2　適正な取得

a) 個人情報保護管理者は、個人情報が適法、かつ公正な手段で取得されることを確認しなければならない。

b) 受託する場合、および第三者から提供を受ける場合は、3.4.2.8.3（第三者提供を受ける際の確認など）の手順に従わなければならない。

■

A.3.4.2.3	要配慮個人情報 2006：3.4.2.3 2006：3.4.2.6 法第 2 条 第 3 項 法第 23 条 第 5 項 法 76 条 政令 2 条、7 条 規則第 5 条	組織は、新たに要配慮個人情報を取得する場合、あらかじめ書面による本人の同意を得ないで、要配慮個人情報を取得してはならない。ただし次に掲げるいずれかに該当する場合は、書面による本人の同意を得ることを要しない。 a)法令に基づく場合。 b)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。 c)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。 d)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。 e)その他、個人情報取扱事業者の義務などの適用除外とされている者及び個人情報保護委員会規則で定めた者によって公開された要配慮個人情報、又は政令で定められた要配慮個人情報であるとき 組織は、要配慮個人情報の利用又は提供についても、前項と同様に実施しなければならない。さらに、要配慮個人情報のデータの提供についても、同様に実施しなければならない。
	附属書 B	要配慮個人情報を取得する場合には、書面による本人の同意を得ることが、A.3.4.2.3 で求められており、それ以外の方法での同意の取得は、A.3.4.2.3 に適合しない。 書面による本人の同意取得は、新たに要配慮個人情報を取得する場合に限らず、要配慮個人情報の取得のつど行うことが望ましい。また、要配慮個人情報を直接書面によって取得する場合は、A.3.4.2.5 で求める本人への明示、および本人の同意取得とあわせて、A.3.4.2.3 の同意取得を行うことが望ましい。 A.3.4.2.3a)の“法令に基づく場合”には、組織が労働安全衛生法に基づき健康診断を実施し、これによって従業者の身体状況、病状、治療などの情報を健康診断実施機関から取得する場合が該当する。 A.3.4.2.3e)は、要配慮個人情報を取得する際に、あらかじめ書面による本人の同意を得ることを要しない要件を法令等で限定的に定めている。
	【P マーク審査のポイント】 ・要配慮個人情報を取得、利用又は提供する場合、あらかじめ書面による本人の同意を得ていること。 ・本人の同意を得ずに取得した要配慮個人情報は、A.3.4.2.3 のただし書きに該当すること。 ・ただし書きに該当することを、承認した文書の有無を確認する。 ・法第 2 条第 3 項　に規定する「要配慮個人情報」とは、施行令 2 条において、次に掲げる事項のいずれかを内容とする記述等とされている。（以下に記述は無いが、本人の病歴又は犯罪の経歴も「要配慮個人情報」である。） 一身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること。	

二本人に対して医師その他医療に関連する職務に従事する者（「医師等」）により行われた疾病の予防及び早期発見のための健康診断その他の検査（「健康診断等」）の結果
三健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと。
四本人を被疑者又は被告人として、逮捕、捜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと。
五本人を少年法（昭和二十三年法律第百六十八号）第三条第一項に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと。

・上記 e)個人情報取扱事業者の義務などの適用除外とされている者とは、法 76 条　に掲げる、報道機関、著述業、学術研究機関、宗教団体、政治団体等の機関やそれらに属する者等を指す。ただし、適用除外とされている者は、個人データ等の安全管理のために必要かつ適切な措置、個人情報等の取扱いに関する苦情の処理その他の個人情報等の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。とされている。
・上記 e)の後段の、"政令で定められた要配慮個人情報"とは、本人の同意なく取得することができる場合として、施行令 7 条に次に掲げる場合とされている。
一 本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得する場合
二 法第 23 条第 5 項各号に掲げる場合（1 委託、 2 合併等、 3 共同利用、）において、個人データである要配慮個人情報の提供を受けるとき。
上記一の場合とは、個人の外形上明らかな障害の事実が映像等に写り込んだ場合の取得について、事業者の負担を勘案するもので、本人も公に認識されることは想定していると考えられる状況を指す。ただし、取得した映像等を第三者提供する場合については、本人の同意を要する。

2006 年版 JIS との関係を以下に示す（※法律が、JIS に追い付いてきたともいえる。）

	2006：3.4.2.3　→	法第 2 条第 3 項
a)	思想、信条、及び宗教に関する事項	信条
b)	人種 民族、門地、本籍地（所在都道府県に関する情報を除く。） 身体・精神障害 犯罪歴 その他社会的差別の原因となる事項	人種 社会的身分 犯罪の経歴 犯罪により害を被った事実 身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害
c)	勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項	信条
d)	集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項	信条
e）	保健医療及び性生活	病歴 健康診断等 健康診断等の結果に基づく、医師等による指導・診療・調剤

※「人種」には、国籍や「外国人」という表現、肌の色は含まれない。
※「社会的身分」には、職業的地位や学歴は含まれない。

【3300 個人情報取扱規程】サンプル

3.4.2.3　要配慮個人情報の取得、利用及び提供の制限

当社は原則として、要配慮個人情報の取得、利用又は提供を行わない。

ただし、要配慮個人情報の取得、利用又は提供について、明示的な本人の同意がある場合および、4.例外的な処理手順 3.4.2.3 のただし書きのいずれかに該当する場合はこの限りでない。

a) 明示的な本人の同意を得て要配慮個人情報を取得、利用、提供する場合は、利用目的の範囲を最小限とし、「3421 個人情報取得・変更申請書」によって取扱者の限定、常時施錠など保管方法などを明記して、個人情報保護管理者の承認を得た後に、3.4.2.5 の a)～h)の事項を明記した「明示して同意を得るための書面」によって、本人の同意を得なければならない。
b) その他、4.例外的な処理手順 3.4.2.3 のただし書きのいずれかに該当する場合は、本人の同意を省略することができる。その場合は　4.例外的な処理手順に従わなければならない。

■

A.3.4.2.4	個人情報を取得した場合の措置 2006：3.4.2.5 法第 18 条	組織は、個人情報を取得した場合は、あらかじめ、その利用目的を公表している場合を除き速やかに、その利用目的を、本人に通知するか、又は公表しなければならない。ただし、次に掲げるいずれかに該当する場合は、本人への利用目的の通知又は公表は要しない。 a)利用目的を本人に通知するか、又は公表することによって本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合 b)利用目的を本人に通知するか、又は公表することによって当該組織の権利又は正当な利益を害するおそれがある場合 c)国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知するか、又は公表することによって当該事務の遂行に支障を及ぼすおそれがあるとき d)取得の状況からみて利用目的が明らかであると認められる場合
	附属書 B	個人情報の取得には、本人から直接書面により取得する場合、書面によらずに取得する場合（例えばカメラによって取得した場合、口頭によって取得した場合など）、本人以外の者から取得する場合（個人情報取扱業務の委託を受ける場合、第三者から個人情報の提供を受ける場合、公開情報から取得する場合など）が該当する。このうち、本人から直接書面により取得する場合の措置については、A.3.4.2.5 に規定されている。 A.3.4.2.4 の“利用目的”とは、A.3.4.2.1 に基づき、組織が特定した利用目的をいう。 本人から書面によらずに取得する場合、利用目的は、本人との契約類似の信頼関係の中で黙示的に了解されることが望ましい。 本人以外の者から取得する場合、組織は、委託元又は提供元との契約などにおいて、利用目的を、あらかじめ明示することが望ましい。 公開情報から取得する場合、組織は、A.3.4.2.1 に基づき、公開された目的の範囲内で利用目的を特定の上で、特定した利用目的について A.3.4.2.4 に基づく措置を講じる。 公表された範囲を超えて利用しようとする場合、組織は、A.3.4.2.5 ではなく、A.3.4.2.7 に基づく措置を講じることが求められる。 A.3.4.2.4 の“本人に通知”とは、本人に直接知らせることをいう。組織は、本人に通知するに当たり、事業の性質及び個人情報の取扱状況に応じ、本人が内容を理解できる合理的かつ適切な方法によることをいう。例えば、対面又は電話のように口頭によって個人情報を取得する場合などは、通知も書面によらずに口答で行ってもよい。 A.3.4.2.4 の“公表”とは、広く一般に自己の意思を知らせること（国民一般その他不特定多数の人々が知ることができるように発表すること）をいう。 A.3.4.2.4a)の場合とは、いわゆる総会屋などによる不当要求などの被害を防止するため、当該総会屋の個人に関する情報を取得し、企業相互に情報交換を行っている場合で、利用目的を通知又は公表することによって、当該総会屋等の逆恨みによって、第三者たる情報提供者が被害を被るおそれがある場合などをいう。 A.3.4.2.4b)の場合とは、例えば、通知又は公表される利用目的の内容によって、当該組織が行う新商品などの開発内容、営業ノウハウなどの企業秘密にかかわるようなものが明らかになる場合などをいう。 A.3.4.2.4c)の場合とは、 例えば、公開手配を行わないで、被疑者に関する個人情報を、警察から被疑者の立ち回りが予想される組織に限って提供された場合、警察から受け取った当該組織が、利用目的を本人に通知するか、又は公表することによって、捜査活動に重大な支障を及ぼすおそれがある場合などをいう。 A.3.4.2.4d)の場合であるかどうかは、条理又は社会通念による客観的判断によって、極力限定的に解釈することが望ましい。商品やサービスの販売・提供において住所・電話番号などの個人情報を取得する場合があるが、その利用目的が当該商品、サービスなどの販売・提供だけを確実に行うためという利用目的であるような場合（クリーニング店、デリバリーサービスなどで受取人を特定するために個人情報を取得するなど）、一般の慣行としての名刺交換（ただし、ダイレクトメールなどの目的に名刺の個人情報を用いることは、自明の利用目的に該当しない場合がある）の場合などはこれに該当する。また、請求書、見積書などの伝票に記載された担当者名、なつ（捺）印などもこれに該当する。ただし、A.3.4.2.4d)によって取得した個人情報であっても、その取扱いの委託を受けた場合は、A.3.4.2.4d)に該当しない。
	【P マーク審査のポイント】 ・「個人情報管理台帳」に特定した個人情報の利用目的について、公表文書「個人情報の取扱いについて」に利用目的が公表されていること。 ・受託によって取得した個人情報についても、その利用目的が公表されていること。 ・電話で取得する場合、本人が参照する電話番号が記載されている文書に利用目的が通知されているか、もしくは利用目的を口頭で行っていること。	

	・監視カメラについては「監視カメラ設置中」の掲示をすること。 ・上記“d) 取得の状況からみて利用目的が明らかであると認められる場合”について、拡大解釈していないこと。

【3300 個人情報取扱規程】サンプル

3.4.2.4　個人情報を取得した場合の措置

個人情報を取得した場合、「3210 個人情報の取扱いについて」にその利用目的が公表されていない場合は、速やかにその利用目的を本人に通知するか、又は公表しなければならない。

2　新規の種類の個人情報を取得する場合は、あらかじめ「3421 個人情報取得・変更申請書」に、「3210 個人情報の取扱いについて（訂正案）」を添付して、個人情報保護管理者の承認を得たのちに、本人に通知もしくは公表しなければならない。
3　本人に通知、又は公表する手段としては、当社ホームページに公表する。
4　電話によりはじめて個人情報を取得する場合は、「3425-22 電話メモ（通知事項）」に従い、口頭で利用目的を通知して同意を得る。
5　その他、4.例外的な処理手順　3.4.2.4 項のただし書きのいずれかに該当する場合は、通知もしくは公表を省略することができる。その場合は　4.例外的な処理手順に従わなければならない。

■

次回は、A.3.4.2.5　A.3.4.2.4 のうち本人から直接書面により取得する場合の措置　から考察します。

以上　■■

<目次>

2018.6

支部報告【北信越支部 2018 年度 福井県例会・研究報告】

会員番号　1281 宮本　茂明（北信越支部）

以下のとおり2018年度 北信越支部福井県例会を開催しました.

・日時：2018年6月2日（土） 13:00-17:00　　参加者：7名

・会場：福井市総合ボランティアセンター 研修室B

・議題：１．研究報告

「RPA(Robotics Process Automation)導入にあたっての考慮点」

長谷部　久夫　氏

「米国政府調達におけるセキュリティ・ベースラインとアセスメント」

宮本　茂明　氏

２．西日本支部合同研究会 北信越支部報告検討

「キャッシュレス社会におけるデータ利活用とシステム監査」

◇研究報告　1

「RPA(Robotics Process Automation)導入にあたっての考慮点」

報告者 (会員番号　1766 長谷部　久夫)

１．報告概要

本報告は，報告者が関与した金融機関における Robotic Process Automation（以下「RPA」という）の実証実験や先行事例の分析結果を踏まえて整理した，RPA 導入における考慮点を紹介するものである.

金融機関は，低金利政策により収益環境が厳しくなる中，融資業務の本部集中等，業務効率化をねらいとする施策を進めている．しかしながら，本部集中部署の大量業務は人手による作業に依存しており，効率化の余地は多分に残されている状況である．このため，現場からはデジタル技術活用による業務効率化の要請が高まり，昨今注目を集めている RPA による業務効率化を待望する声があがっていた．これに応えて，実証実験で RPA の有用性を検証するとともに，本格導入に向けた準備を進めている.

RPA 導入においては適用する業務プロセスの設定や，利用目的に適合する RPA 製品の選定に加え，稼働後のロボット展開を見据えた適正な運用管理，及びリスク管理態勢を構築することが重要と考えた．これらの要件を漏れなく充足するためには，想定される課題への対策を周到に準備してプロジェクトを進める必要があることを認識し，以下の３つの目指すべき方向性を設定した.

（１）RPA 初期導入における周到な準備

投資効果が高く適用が容易な業務選定，実証実験による自社に適したアーキテクチャ決定，内製化を実現する開発標準，及びプロセスの確立を初期導入段階にて準備する.

（２）効率的なシステム運用管理，保守を実現する体制構築

ロボットのプロフィール，仕様書と運用基盤の整備により，効率的なシステム運用管理，保守を実現する社内体制を構築する.

（3）適正なリスク管理態勢整備とガバナンス強化

RPA コントロールサーバーの構築と，既存の統合基盤システムを有効活用することで，適正なリスク管理態勢の整備とガバナンスの強化を図る.

2．具体的な考慮点

上記1．の3つの方向性を実現することにより，ガイドラインや標準等が確立していない RPA において，既存の情報システムと同様の標準化が整備され，拡張性を確保して，円滑な全社展開が可能になると考える．具体的な考慮点については，目指すべき方向性の3つのポイントに分けて，以下のとおり報告した.

（1）RPA 初期導入における周到な準備

ア．初期導入においては，早期に効果を出すためにも適用業務の選定が非常に重要．主な判断基準としてルール化が可能，発生頻度や業務ボリュームが多い，デジタルデータを扱う業務等があげられる.

イ．実証実験では自動化対象業務が多いと予想される部署が利用する業務システムや，社内 OA 環境での技術検証を併せて実施し，選定対象の RPA 製品の性質を押さえておくことが重要.

ウ．業務フローの変更に機動的に対応し，より高い ROI を達成するためには，早期に内製化可能な体制（開発・運用の標準化ガイドの策定や，ロボットの部品化）を構築すべきである.

（2）効率的なシステム運用管理，保守を実現する体制構築

ア．業務部門，及びシステム部門の担当者の異動等に伴う業務・ロボットの「ブラックボックス化」を防止するため，ロボットのプロフィールと仕様書を整備する.

イ．業務部門，システム部門のいずれか一方にロボット管理を任せるのではなく，ロボットの一元管理を推進する CoE（Center of Excellence）組織を設置することが有効．ロボットの障害や，利用部門による変更要求については，CoE 組織で一元的に管理し，適切な運用・管理を実現する.

（3）適正なリスク管理態勢整備とガバナンス強化

ア．RPA コントロールサーバーの構築によるロボットの稼働状況の監視と，障害発生時の管理担当者宛てに自動的に通知する仕組み，例えば既存の統合監視基盤との連携等を検討する.

イ．安全対策の網羅性確保のため，FISC「金融機関等コンピュータシステムの安全対策基準」をベースに情報セキュリティ対策の全体像を導出した「セキュリティ対策マップ」を RPA にも適用する.

上記の考慮点を整理すると，初期導入の準備，及び運用管理・保守に関しては，RPA 特有の考慮点がある．一方，リスク管理態勢は，既存の情報システムと同様の対策を考えるべきであり，統合基盤システムやセキュリティ対策マップを活用することにより，有効且つ適切なセキュリティ対策を実現できると考えている.

3．今後の展望

企業の成長を目指し，「労働生産性（付加価値額／労働力）」を高めるには，労働力の縮小にとどまらず，付加価値額を拡大することが必要である．RPA 活用で削減した人員を重点分野に再配置して，「稼ぐ力」をいかに高めるかが課題といえる．また，RPA には OCR との接続により取扱うデジタルデータを拡張し対象業務を拡大すること，更には AI と組み合わせてビッグデータを利活用する等により，付加価値額の拡大に貢献することが期待される．今後も技術動向を注視して，支部会員間で情報交換していきたい.

研究報告　2

「米国政府調達におけるセキュリティ・ベースラインとアセスメント」

報告者 (会員番号　1281 宮本　茂明)

米国政府は，2017 年に防衛関連調達でこれまで機密指定していなかった管理対象非機密情報情報（CUI：Controlled Unclassified Information）に対してもセキュリティ・ベースラインの遵守とサイバーインシデント発生時の報告を義務付ける規則を発効しました．契約条件として，末端の再委託先まで，同じセキュリティ・ベースラインの遵守が求められています．また，防衛関連以外のすべての米国政府調達に対象を広げる準備が進んでいます．

米国国防総省調達規則補遺 DFARS.252.204-7012「保護対象防衛情報（CDI）の保護とサイバーインシデント報告」で求められている要件の概要を以下に示します．

1．セキュリティ・ベースライン

（1）自社システム利用時のセキュリティ・ベースライン：NIST SP 800-171

自社システムを利用する場合，NIST SP 800-171 「非連邦政府情報組織および情報システムおける管理対象非機密情報（CUI）の保護」のセキュリティ・ベースラインを満たす必要があります．

NIST SP 800-171 は，110 項目のセキュリティ・ベースライン管理策が示されており，14 種類（1 アクセス制御，2 意識向上と訓練，3 監査と説明責任，4 構成管理，5 識別と認証，6 インシデント対応，7 メンテナンス，8 記憶媒体の保護，9 要員のセキュリティ，10 物理的保護，11 リスク・アセスメント，12 セキュリティ・アセスメント，13 システムと通信の保護，14 システムと情報の完全性）に分類されています．

NIST SP 800-171 は，ISMS のようにマネジメントシステムを求めているのではなく，最低限の守るべき管理策のベースラインを示しています．米国政府関係組織に対して出されている NIST SP 800-53「連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策」に比べて管理策要件の数も少なく、簡略化し，セキュリティ要件における機密性にフォーカスしたものになっています．

NIST SP 800-171 のセキュリティ管理策の中で，実装にあたって少しハードルが高いと思われる点として，情報システム利用時の多要素認証と，暗号に米国 FIPS 認定暗号モジュール使用が必須となっている点があります．

セキュリティ・ベースライン対応を次のステップで進めます．

①CUI 情報，保護対象契約事業者情報システムを特定

②セキュリティ管理策を実装

・NIST SP 800-171 のセキュリティ管理策を満たすよう実装し，対応状況を「システムセキュリティ計画（SSP: System Security Plan)」に記述します．

③セキュリティ管理策をセルフ・アセスメント

・アセスメント用のガイドライン NIST SP 800-171A，中小企業向けセルフ・アセスメント用のハンドブック NIST Handbook 162 等を参考に，アセスメントを行います．

④セキュリティ管理策未対応事項への対応

・アセスメント結果に基づき，セキュリティ管理策未対応事項への「対応実施計画（POAM: Plan of

Action and Milestone)」を作成します.「対応実施計画」に従って対応を進めます.

（2）外部クラウド利用時のセキュリティ・ベースライン：FedRAMP 中位ベースライン（同等）

クラウド・サービスを利用する場合, クラウド・サービスが FedRAMP（Federal Risk and Authorization Management Program）中位ベースラインと同等の要件を満たすことを，クラウド・サービス・プロバイダに要請し，保証する必要があります.

FedRAMP は，クラウド・サービスのセキュリティ・アセスメント，認可，継続的なモニタリングに関する標準化されたアプローチを提供する米国政府全体のプログラムです．第三者機関による脆弱性スキャンやペネトレーションテストを含むアセスメントが要求されています．FedRAMP 中位ベースラインには，325 項目のセキュリティ・ベースライン管理策が示されています.

2．その他の主な要件

（1）下請け契約事業者への DFARS 252.204-7012 要件をフローダウン

契約事業者は，CUI を取扱う業務を下請け契約事業者に再委託する場合、DFARS252.204-7012 の条項を、下請け契約の契約条件に含める必要があります.

（2）サイバーインシデント報告義務

サイバーインシデントの発見から 72 時間以内に、契約事業者/下請け契約事業者は,米国国防総省の DIB（Defense Industrial Base 防衛産業基盤）の Web サイトに直接報告する必要があります．DIB サイトへのアクセスには、米国国防総省承認のある中位レベルの PKI 証明書を取得しておく必要があります．末端の再委託先も，72 時間以内に直接報告しなければならない点は，ハードルが高いと思われます.

米国政府調達の事例から，サプライチェーン全体で同一の最低限守るべきセキュリティ・ベースラインを定め, アセスメント情報と指摘に対する対応実施計画をサプライチェーンの中で共有, 管理していくフレームワークを導入することで，サプライチェーン全体としてのセキュリティ信頼度向上につながると考えます.

<参考文献>

・DFARS 252.204-7012「Safeguarding Covered Defense Information and Cyber Incident Reporting」
https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
・NIST SP 800-171 Rev.1 「Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations」 https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
・NIST SP 800-171A (DRAFT) 「Assessing Security Requirements for Controlled Unclassified Information (Final Draft)」 https://csrc.nist.gov/publications/detail/sp/800-171a/draft
・NIST Handbook 162「NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements」
https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
・FedRAMP https://www.fedramp.gov/

以上

<目次>

2018.6

注目情報（2018.5～2018.6）

■情報処理安全確保支援士公開システムの開始について【IPA】

2018 年 7 月 2 日(月)に、「情報処理安全確保支援士公開システム」(以下、公開システム)のサービスが開始されます。本サービスにより、これまで PDF 形式で IPA のホームページに掲載されていた情報処理安全確保支援士の方のプロフィール（登録者公開情報）を専用のウェブサイト上で検索、閲覧することが可能となります。

また、情報処理安全確保支援士の方は、公開システムにログインし、ご自身の公開情報を編集することも可能になります。

【重要なお知らせ】

本サービスの開始にあわせて、2018 年 7 月 2 日(月)を目途に公開システムへのログイン情報(ログイン ID 等)通知書を情報処理安全確保支援士の方には簡易書留で郵送される予定です。

※簡易書留は、受取人不在等により 7 日間が経過すると、発送元に戻ってきます。

再送費用は IPA では負担されませんので、ご注意ください。

【注意事項】

当サービスの開始に伴い「登録事項等公開届出書」のフォーマットが変更されます。

2018 年 6 月 25 日(月)以降､旧フォーマットでの届出を受け付けることができませんので､ご注意ください。

URL：https://www.ipa.go.jp/siensi/formlist.htm

<目次>

2018.6

【 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234回	日時：2018年7月26日（水）　18時30分～20時30分 場所：機械振興会館　地下2階ホール	
	テーマ	企業IT動向調査2018
	講師	宮下 清 氏 一般社団法人　日本情報システム・ユーザー協会(JUAS) 常務理事
	講演骨子	「企業IT 動向調査」の調査テーマは、企業におけるIT 投資やIT 戦略動向等の現状と経年変化を明らかにするとともに、年度ごとに重点テーマを設定している。今回の調査では「ビジネスのデジタル化に向けて動き出したIT 部門の実像」を取り挙げる。 企業のIT予算は、現在も高い水準にあるが、ここにきてIT投資も一巡したためか、IT予算の増加基調にも頭打ちの傾向も見られるようになってきた。IT投資の目的を見ても、バックエンドでのプロセス効率化からフロントエンドでの価値創造へのシフトはいよいよ鮮明になってきており、新しいITを活用してこれまでにない価値を創出するビジネスのデジタル化は、いよいよ具体的な取り組みの段階に差し掛かってきた。 こうしたことから、デジタル化・グローバル化といったＩＴ戦略遂行のプラットホームとしてクラウドを活用するなど、これまでとは違った取り組みが求められるようになってきている。 今年度は、こうした大きな潮目の変化を現実のものとして受止め、企業IT部門における対応の方向を見極め、人材・資金・技術など必要な資源をいかに確保していくか、IT部門の組織変革や社内外の新たなネットワークの構築など、具体的な処方箋を探っていくことが大きな課題となる。
	お申込み	協会のＨＰからお申し込みください。（準備中）

■近畿支部 30 周年記念シンポジウム

近畿支部 30 周年記念シンポジウム	日時：2018年 6月30日（土）大会　13:00～17:00　/　情報交換会　17:30～19:30 場所：エル・おおさか(大阪府立労働センター)　6階 大会議室	
	テーマ	システム監査@ニューフロンティア
	プログラム	1 来賓挨拶（経済産業省 近畿経済産業局 地域経済部 次世代産業・情報政策課 様） 2 新システム監査基準／管理基準のポイント 3 地方自治体のICT監査に求められる役割と課題について 4 ブロックチェーン技術とシステム監査 5 次代を担うシステム監査のあり方について ---------- 6 情報交換会 ※都合により、講演内容・講師・時間等を変更する場合がありますのでご了承下さい。
	お申込み	https://www.saaj.or.jp/anniv_30th/anniv_kinki_30th_symposium.html

■事例に学ぶ課題解決セミナー（東京）

第21回	日時：2018年7月28日（土）　13:30～17:30 場所：TKPスター貸会議室お茶の水駅前	
	教材	教材は当日配布致します。
	講師	事例研究会メンバー
	セミナー概要	情報システムの事故・障害で、企業や顧客が損失を被る事例が後を絶ちません。システム監査の専門家が事故・障害の原因を解き明かし、システム監査の観点から見た有効な解決策を示します。事故・障害の原因は報道だけでは分かりません。事故・障害事例をリスクとコントロールの視点で分析して、皆様の課題解決に役立つ説明をします。情報システムの利用者から運営者、経営者から担当者まで多様な階層・職種の方のキャリアアップに、当セミナーをご活用下さい。事故・障害を未然に防ぐシステム監査の役割とその有効性の理解向上にも役立ちます。
	募集人員	定員24名（最小催行人員10名）
	応募締切日	2018年7月13日（金）
	お申込み	下記URLよりお申込みください。 https://www.saaj.or.jp/kenkyu/kadaiseminar/kadaiseminar_21.html

<目次>

2018.6

【 外部主催イベント・セミナーのご案内 】

■2018 年度 第 1 回 JASA 定例研究会

第1回	日時：2018年7月6日（金）　18:30～20:00（開場 18：20～） 場所：フォーラムミカサ エコ　7F ホール	
	テーマ	【講演1】クラウドシフト：CASB活用に見る日本と海外のギャップとこれから 【講演2】クレジットカード情報保護基準PCI DSS に対する事業体の準拠性評価について
	講師	【講演1】 高岡　隆佳　氏 株式会社シマンテック　エバンジェリスト 【講演2】 羽生　千亜紀　氏 NTTデータ先端技術株式会社 セキュリティ事業部　セキュリティコンサルティング担当 担当課長　シニアコンサルタント
	講演概要	【講演1】 日本企業におけるクラウドシフトに関連する記事はよく目にする一方、その実はどうでしょうか。欧米では平均10～20種類のクラウドアプリケーションが活用され、業務の中心がスマートフォンなどに移行し、クラウド上でのデータやユーザの保護にCASBが活用されていますが、日本での導入は未だ限定的です。本講演ではそのギャップとこれからの動きについて解説いたします。 【講演2】 PCI DSSは、6月1日に施行された改正割賦販売法の実務指針「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」で取り上げられているクレジットカード情報保護のためのセキュリティ基準です。本公演では、PCI DSS の概要、対象範囲、QSA(認定セキュリティ評価機関）によるオンサイトレビューとその報告書・証明書、管理団体である PCI SSC の役割などについて、QSAの立場でご紹介します。
	お申込み	下記URLよりお申込みください。 http://www.jasa.jp/seminar/monthly_seminar.html?year=2018&seminar_id=39

<目次>

2018.6

【 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

・「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。

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2018.6
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
6 月	1：年会費未納者宛督促メール発信 14：理事会 19：年会費未納者督促状発送 21～：会費督促電話作業（役員） 29：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）	13：第 233 回月例研究会 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） 30：近畿支部 30 周年記念 シンポジウム
7 月	5：支部助成金支給 12：理事会	12：第 32 回システム監査実践セミナー (日帰り 2 日間コース) 26：第 234 回月例研究会 28：第 21 回事例に学ぶ課題解決セミナー 下旬：秋期 CSA・ASA 募集案内	13：支部会計報告〆切
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	
9 月	13：理事会	～秋期 CSA・ASA 募集中　～9/30 迄	
10 月	11：理事会	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 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	
	前年度に実施した行事一覧		
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 14：理事会：2018 年度予算案 会費未納者除名承認 第 17 期総会審議事項確認 15：総会資料提出依頼（1/9〆切） 15：総会開催予告掲示 19：2017 年度経費提出期限	15：第 228 回月例研究会 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	9： 総会資料提出期限 16:00 10：役員改選公示（1/25 立候補締切） 11：理事会：総会資料原案審議 27：2017 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 19： 春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕 29：第 229 回月例研究会	6：支部会計報告期限
2 月	1：理事会：通常総会議案承認 28：2018 年度年会費納入期限	1-3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	23：第 17 期通常総会 役員改選
3 月	8：年会費未納者宛督促メール発信 8：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 3-4 &17-18:「第 31 回システム監査実務 セミナー(日帰り 4 日間コース)」 会場：関東 IT ソフトウェア健保会館 14：第 230 回月例研究会 31：第 20 回「事例に学ぶ課題解決セミナー」 会場：市ヶ谷健保会館	
4 月	12：理事会	初旬：春期 CSA・ASA 書類審査 中旬：春期 ASA 認定証発行 17：第 231 回月例研究会	15：春期情報技術者試験
5 月	10：理事会	13,26：春期 CSA 面接 19：システム監査制度カンファレンス 「新システム監査／管理基準」 （第 232 回特別開催月例研究会） 28：CSA フォーラム（茅場町 NATULUCK）	

<目次>

2018.6

【 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

2018 年度の年間テーマは、「システム監査人の新たな活躍」とし、さらに四半期ごとに具体的なテーマを設定して、皆様からのご意見ご提案を募集いたします。

4 月号から 6 月号までの四半期テーマは、「システム監査基準・管理基準改訂とこれからのシステム監査人」でした。システム監査人の皆様にとって、関心の高い重要なテーマであろうと思いますので、今月号から 9 月号までの四半期テーマも、引き続き「システム監査基準・管理基準改訂とこれからのシステム監査人」とします。システム監査基準・管理基準の改訂に対して、システム監査人としてどう対応していくのか、皆様のご意見をお待ちしています。

システム監査人にとって、報告や発表の機会は多く、より多くの機会を通じて表現力を磨くことは大切なスキルアップのひとつです。良識ある意見をより自由に投稿できるペンネームの「めだか」として始めたコラムも、投稿者が限定されているようです。また記名投稿のなかには、個人としての投稿と専門部会の報告と区別のつきにくい投稿もあります。会員相互のコミュニケーション手段として始まった会報誌は、情報発信メディアとしても成長しています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。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。

＊2018 年度会報テーマ

	四半期テーマ	年間テーマ
1 月号～3 月号	システム監査人に求められる能力	システム監査人の新たな活躍
4 月号～6 月号	システム監査基準・管理基準改訂と これからのシステム監査人	
7 月号～9 月号	システム監査基準・管理基準改訂と これからのシステム監査人	
10 月号～12 月号	（決まり次第ご連絡します）	

□■ 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

2018.6

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

■□■ＳＡＡＪ会報担当

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

編集支援：　小野修一（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>