認定 NPO 法人
日本システム監査人協会報
2018 年 3 月号
No 204
No.204（2018 年 3 月号）<2 月 25 日発行>

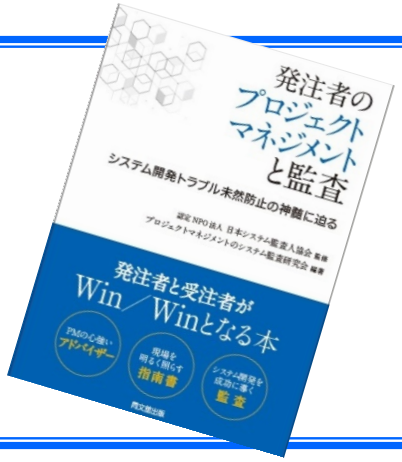
SAAJ 設立３０周年記念出版

システム開発トラブル未然防止の神髄に迫る

【発注者のプロジェクトマネジメントと監査】

２月２３日ＳＡＡＪ総会で記念発売！

ＰＪＭのシステム監査研究会（主査：原田）



巻頭言

「IT アセスメント研究会の活動報告」

会員番号：0555　松枝憲司（副会長・IT アセスメント研究会主査）

SAAJ の新たなビジョンに対する具体的な活動の一環として、2016 年 11 月に IT アセメント研究会を立ち上げ、この 1 年余り（2016/11-2017/12）で 23 回の研究会を開催しました。その活動成果を報告させていただきます。

1. テーマ「IT ガバナンスの基準作り」

（1）ISO38500 関連基準の日本語化

JISQ38500 の理解と活用を図るために、その関連基準である ISO/IEC_TS_38501:2015（Implementation guide 導入ガイド）、ISO/IEC_TR_38502（Framework and model　フレームワークとモデル）、ISO/IEC_TR_38504（Guidance for principles-based standards in the governance of information technology 原則基盤の標準ガイダンス）の日本語化を行い研究会メンバで情報共有を図りました。また概要については、月例会等で紹介しました。

（2）ISO38503（Assessment of the governance of IT）の ISO 化の支援

IT ガバナンスのアセスメント基準であり、過去数年に渡って支援してきた作業ですが、昨年の岡山のＩＳＯ会議後にＩＳＯ側の体制を一新してリスタートしました。当研究会メンバも加わって、２週間に１回のペースでＷｅｂ-ＥＸによる国際検討会を開催して議論を進めてきました。今年 6 月にリスボンで開催される次回のＩＳＯ会議に向けてのＷＤ（ワーキングドラフト）を提出予定です。

2. テーマ「システム監査基準／管理基準の改訂の検討」

昨年経済産業省の委員会が編成され、両基準の改定作業が開始されました。SAAJ 担当分の改訂原案作成作業は、当研究会のメンバ 8 名で担当しました。原案作成を分担している他団体や大学の先生も参加する全体の検討会等、委員会全体で 10 回以上の打合せを積み重ねてきました。この会報が出る頃には、パブリックコメントの案内を出せているものと思っています。また本改訂作業については、来年度以降も関連団体が共同で継続してことを計画しています。

上記 2 つのテーマについては、システム監査人の活躍の範囲を拡大させる可能性を持っており、引き続き取り組んでまいります。皆様の積極的なご参加をお待ちしています。

以上

各行から Ctrl キー+クリックで
該当記事にジャンプできます。

<目次>

○ **巻頭言** **1**
「IT アセスメント研究会の活動報告」

1. めだか **3**
【システム監査人に求められる能力】

2. 投稿 **4**
【システム監査人の新たな活躍】

3. 本部報告 **5**
【個人情報保護マネジメントシステム－要求事項【JIS Q 15001:2017】について　その１】

4. 支部報告 **10**
【北海道支部　2018 年 1 月の月例研究会】

5. 注目情報 **14**
【情報セキュリティ 10 大脅威　2018（IPA）】

6. 協会からのお知らせ **15**
【２０１８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】
【協会行事一覧】
【新たに会員になられた方へ】

7. 会報編集部からのお知らせ **19**
【会報編集部からのお知らせ】
【会員限定記事】

2018.2

めだか　【　システム監査人に求められる能力　】

システム監査人に求められる能力は、情報システムの知見、監査技法の修得、そしてコミュニケーションの能力である。情報システムの知見は、システム監査対象の業務アプリケーションについて、利用目的をよく理解し、信頼性、安全性、効率性及び有効性を調べる知見である。監査技法の修得は、監査基準、監査テーマを明確にし、予備調査、本調査、結果確認、監査報告と助言プロセスを行う技法の修得である。

会報２月号で、情報システムの知見に関して仮想通貨とブロックチェーンに言及したが、すぐその後、1 月 26 日、仮想通貨取引所「コインチェック」（東京都渋谷区）から約 26 万人の仮想通貨 NEM 約 580 億円分が不正流出したという事件が発生した。新聞によると金融庁は、1 月 29 日に業務改善命令を出し、2 月 2 日に改正資金決済法のもとづく強制力がある立入検査が行われ 10 人の検査官が同社に常駐して資料提出や幹部の説明を受けるとのことである。不正流出は、犯人にコインチェック社の安全対策上の不備を狙われたが、ブロックチェーンの機能によってネットコミュニティの監視が犯人に対して行われており、犯人は仮想通貨 NEM を窃取したものの仮想通貨取引所でドルや円と換金ができていない。

ブロックチェーンは、インターネット上でデータを改ざんできない情報記録として、さまざまな応用形態がある。IoT は、Internet of Things の略で、モノ（Things）をインターネットにつなげることであり、モノとモノの間のデータ交換ともいえる。インターネット上のデータ交換でデータの改ざんができないことは、データを改ざんして利益を得ようと意図する犯罪者に対抗するサイバーセキュリティ上の安全要件である。例えば、重要インフラのメンテナンスにおいて、遠隔監視センサーでデータ収集を安全に行い、壊れる前に部品交換をおこなうなどの予防保全を安全に行うことができるようになる。また、鍵の情報をインターネット上で安全に受け渡すスマートロックも応用事例である。

システム監査人は、監査テーマに関して被監査部門の人たちとコミュニケーションをとって監査を行っていくが、コミュニケーションにおいてお互いに相手の言葉を 100%理解できているかというと、それは実に難しい。しかし、監査テーマを限って行えば、相互理解はその範囲で大きく乖離しないものである。ただし、範囲を限定しすぎると全体的な問題が見えなくなる。監査テーマの範囲を決める匙加減の能力が求められる。

（空芯菜）

参考：「入門 ビットコインとブロックチェーン」野口悠紀雄著 PHP ビジネス新書 388

（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>

2018.2

投稿 【 システム監査人の新たな活躍 】

会員番号 0557 仲厚吉（会長）

2018 年度は、協会創立 30 周年を経てこれまでの 30 年間の実績を踏まえた新たな飛躍への端緒の年になります。これから 30 年後は、人の知能と人工知能がふつうにインタラクティブな会話をおこなう知能的にシンギュラリティな時代に入っているといわれますが、2018 年は、システム監査人の新たな活躍に、システム監査基準とシステム管理基準の大幅な改訂版が経済産業省より発行されるという画期的なトピックスの年になります。これらの基準は、当協会（IT アセスメント研究会（松枝憲司主査））、システム監査学会、ISACA 東京支部､IT ガバナンス協会の４団体のほか多くのシステム監査関係者が協力してできあがった成果であり、カンファレンスが、2018 年 5 月 19 日（土）に、経済産業省の隣にあるイイノホールで開催される予定です。カンファレンスへの会員の皆様のご参加をお願い申し上げます。

創立 30 周年記念行事として、2018 年度通常総会（2 月 23 日（金）午後）の特別講演に、人工知能学会会長国立情報学研究所山田誠二教授をお招きし､「人工知能研究の最新情報 - インタラクティブな人工知能を目指して - 」をご講演いただきます。会員の皆様には、通常総会に引き続き受講をお願い致します。また、総会では、創立 30 周年記念出版として、プロジェクトマネジメントのシステム監査研究会（原田憲幸主査）による「発注者のプロジェクトマネジメントと監査」（同文舘出版）がお披露目されます。ぜひ、手に取ってご覧のうえ購入いただき情報システム構築及びシステム監査にご活用をお願いしたいと思います。情報システムの構築を成功に導くために発注者や発注サイドが受注者とともに知っておくべきプロジェクトマネジメントの秘訣とシステム監査人の役割がわかりやすく解説されています。

2018 年は、1 年を通して創立 30 周年行事を行っていきます。「JIS Q 38500:2015 情報技術 - IT ガバナンス)」のシリーズとして「IT ガバナンスのアセスメント」を ISO/IEC38503 として規格化する活動に取り組むとともに次の記念行事などを予定しています。ほかの行事を含め詳しくは順次お知らせしてまいります。

日程	場所	行事
2 月 23 日	機械振興会館	通常総会特別講演「人工知能研究の最新情報 - インタラクティブな人工知能を目指して - 」人工知能学会会長国立情報学研究所山田誠二教授
		記念出版「発注者のプロジェクトマネジメントと監査」（同文舘出版）
5 月 19 日	イイノホール	4 団体共同カンファレンス 「システム監査基準、システム管理基準の改訂のポイント」など
6 月 30 日	エル大阪	近畿支部 30 周年記念シンポジウム 「システム監査のニューフロンティア」

<目次>

2018.2

本部報告　個人情報保護マネジメントシステム－要求事項【JIS Q 15001:2017】について　その１

会員番号　1760　斎藤由紀子　（個人情報保護監査研究会）

2017 年 12 月 20 日、日本規格協会から、個人情報保護マネジメントシステム－要求事項【JIS Q 15001:2017】が発表されました。2017 年版の規格本文は、事業者が個人情報保護マネジメントシステム（以下 PMS と呼ぶ）と、PMS 以外の他のマネジメントシステム規格を併用するため、「マネジメントシステム」の概念を統一し、本来 PMS には無かった概念（測定など）が追加され、用語の変更（パフォーマンス評価など）も示されています。また旧版（2006 年版）の本文に存在していた、「～すること」等の管理策は、附属書 A（規定）に示されることとなりました。

赤字：注目点

JIS Q 15001:2017 項目		頁	旧版（2006年版）項目	
0	序文	1		ー
0.1	概要	1		ー
0.2	**他のマネジメントシステム規格との近接性**	1		ー
1	適用範囲	2	1	適用範囲
2	**引用規格**	2		ー
3	用語及び定義　（**3.1 組織～3.47 リスク所有者**）	2	2	用語及び定義（2.1個人情報～2.8不適合）
4	組織の状況	9		ー
4.1	組織及びその状況の理解	9	3.3.2	法令、国が定める指針その他の規範
4.2	利害関係者のニーズ及び期待の理解	9		ー
4.3	個人情報保護マネジメントシステムの適用範囲の決定	9	3.3.1	個人情報の特定
4.4	個人情報保護マネジメントシステム	10	3	要求事項、3.3.1個人情報の特定
5	リーダーシップ	10		ー
5.1	リーダーシップ及びコミットメント	10	3.3.4	資源、役割、責任及び権限
5.2	方針	10	3.2	個人情報保護方針
5.3	組織の役割、役割、責任及び権限	11	3.3	資源、役割、責任及び権限
6	計画	11	3.3	計画
6.1	リスク及び機会に対処する活動	11	3.3.3	リスクなどの認識、分析及び対策
6.2	個人情報保護目的及びそれを達成するための計画策定	12	3.3.6	計画書
7	支援	13	3.3.4	資源、役割、責任及び権限
7.1	資源	13		
7.2	力量	13		
7.3	認識	13	3.4.5	教育
7.4	コミュニケーション	13	3.3.7	緊急事態への準備
7.5	文書化した情報	13	3.5	個人情報保護マネジメントシステム文書
8	運用	14	3.4	実施及び運用
8.1	運用の計画及び管理	14	3.4.1	運用手順
8.2	個人情報保護**リスクアセスメント**	14	3.4	実施及び運用
8.3	個人情報保護リスク対応	14		
9	**パフォーマンス評価**	15	3.7	点検
9.1	監視、測定、分析及び評価	15	3.7.1	運用の確認
9.2	内部監査	15	3.7.2	監査
9.3	**マネジメントレビュー**	15	3.9	事業者の代表者による見直し
10	**改善**	16	3.8	是正処置及び予防処置
10.1	**不適合及び是正処置**	16		
10.2	**継続的改善**	16	3.1	一般要求事項

付属書A（規定）管理目的及び管理策	17
付属書B（参考）管理策に関する補足	29
付属書C（参考）安全管理措置に関する管理目的及び管理策	48
付属書D（参考）新旧対応表	60
参考文献	63
解説	64

今回の会報から、【JIS Q 15001:2017】について、個人情報保護監査研究会としてできる限り客観的に、かつ独自の考察を加えて、「具体的に何を理解すればよいのか」を研究して参ります。様々なご意見があることを承知の上で、今後、建設的な論議ができればと考えています。

0. 序文

この規格は、“対応国際規格は現時点で制定されていない。”と書かれており、国際規格を多少なりとも視野に入れているようです。また、他のマネジメントシステムとこの規格との対応として、以下の表が、参考文献（附属書 D 末尾）に示されています。

	参考文献（附属書 D 末尾）	
①	JIS Q 0073:2010	リスクマネジメント−用語
②	JIS Q 10002:2015	品質マネジメント－顧客満足－組織における苦情対応のための指針
③	JIS Q 19011:2012	マネジメントシステム監査のための指針
④	JIS Q 27000 : 2014	情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語
⑤	JIS Q 27001 : 2014	情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項
⑥	JIS Q 27002 : 2014	情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範
⑦	JIS Q 31000 : 2010	リスクマネジメント－原則及び指針
⑧	ISO/IEC27005 : 2011	Information technology−Security techniques −Information security risk management　情報技術－セキュリティ技術－情報セキュリティリスクマネジメント
⑨	ISO/IEC 専門業務用指針（AnnexSL）	第一部 統合版 ISO 補足指針の附属書 SL に規定する上位構造（HLS）

0. 1 概要

PMS は、“リスクマネジメントプロセスを適用することによって個人情報の保護を維持し”と示されました。旧版 2006 年版規格においても、「個人情報の特定とリスク分析」をベースにしていましたので、この新規格でそれが明言されました。

0. 2 他のマネジメントシステム規格との近接性

2017 年規格は、ISO/IEC 専門業務用指針　第 1 部　統合版 ISO 補足指針の附属書 SL（マネジメントシステム規格の提案＝上記表の⑨、以下 AnnexSL と呼ぶ）を参考にしていると記されています。興味のある方は、これらの参考文献を紐解いていただくと、大いに参考となることでしょう。

また、新規格の 5.リーダーシップ　では、“組織のプロセスへの PMS 要求事項の統合を確実にする。”とし、6.計画＞6.1.1 一般　では、“組織”は、“その活動の PMS プロセスへの統合及び実施” を計画するよう求めています。

ご参考までに、「AnnexSL」と、各マネジメントシステムとの項目番号で比較してみました。

vocabulary	用語	**PMS**	AnnexSL	ISMS	QMS
organization	組織	**3.1**	3.1	2.57	3.2.1
interested party	利害関係者	**3.2**	3.2	2.41	3.2.3
requirement	要求事項	**3.3**	3.3	2.63	3.6.4
management system	マネジメントシステム	**3.4**	3.4	2.46	3.5.3
top management	トップマネジメント	**3.5**	3.5	2.84	3.1.1
effectiveness	有効性	**3.6**	3.6	2.24	3.7.11
policy	方針	**3.7**	3.7	2.6	3.5.8
objective	目的	**3.8**	3.8	2.56	3.7.1
risk	リスク	**3.9**	3.9	2.68	3.7.9
competence	力量	**3.10**	3.10	2.11	3.10.4
documented information	文書化した情報	**3.11**	3.11	2.23	3.8.6
process	プロセス	**3.12**	3.12	2.61	3.4.1
performance	パフォーマンス	**3.13**	3.13	2.59	3.7.8
monitoring	監視	**3.14**	3.15	2.52	3.11.3
measurement	測定	**3.15**	3.16	2.48	3.11.4
audit	監査	**3.16**	3.17	2.5	3.13.1
conformity	適合	**3.17**	3.18	2.13	3.6.11
nonconformity	不適合	**3.18**	3.19	–	3.6.9
corrective action	是正処置	**3.19**	3.20	2.19	3.12.2
continual improvement	継続的改善	**3.20**	3.21	2.15	3.3.2

Monitoring(監視)から、「PMS」と「AnnexSL」とは 0.01 ずつずれています。ISMS も QMS も独自の発展をしているので、気にするまでのことはないようです。

（なお、項目番号は文字列です。小数点ではないので注意が必要です。）

上記のように、PMS、ISMS、QMS で項目番号が異なるので、統一した規程番号とすることには無理があります。しかし、統合マネジメントシステムとして、せめて用語の統一を図ることは二つ以上のマネジメントシステム規格を運用する組織にとって有用な取り組みとなることでしょう。

以下、規格の見出しとトピックスのみを羅列します。

1．　適用範囲

・・・この組織は、個人情報の保護に関する法律（平成 15 年法律第 57 号）（以下、個人情報保護法という。）に定める個人情報取扱事業者を意味する。

※ 事業者→組織、と用語が変わり、個人情報保護法との関係が示されました。

2．　引用規格

この規格が引用する規格はない。

※ ただし、解説（P65）には、“個人情報保護と情報セキュリティとは安全管理措置の点で共通する事項が多いことから、**AnnexSL** に整合したマネジメントシステム規格として，先行して制定されている JIS Q 27001:2014（情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項）を参考とした。” と記載されています。

3．　用語及び定義

この規格で用いる主な用語及び定義は、個人情報保護法による。その他の主な用語及び定義は、次による。

※ 重要なのは、用語は個人情報保護法による。とされたことです。
“次による”と定義された用語で、重要な用語は、前ページに列挙しましたので、参考にしてください。

4．　組織の状況

※組織の目的、組織の能力、外部及び内部の課題、利害関係者のニーズを理解し、PMS の適用範囲を決定しなければならないことが明言されました。

5．リーダーシップ

5.2.1 内部向け個人情報保護方針、5.2.2 外部向け個人情報保護方針

※ 2018 年 2 月 1 日現在、正式な見解は出ていませんが、必ずしも内部向け、外部向けと、二つの個人情報保護方針を作成しなければならないということではないようです。
また、5.1 b) に、トップマネジメントは“組織のプロセスへの PMS 要求事項の統合を確実にする。”とあり、PMS に関するリーダーシップ及びコミットメントを実証しなければならないとされました。

6．計画

※ 計画には、PMS の活動をどのようにマネジメントシステムのプロセスに統合し、組織内に展開するかの決定を含んでいることが示されています。また、2006 年版にあった、特定、法令等の規範、緊急事態への準備などの具体的な取り組みは、「附属書 A（規定）」に記述されることになりました。

7．支援

組織は、PMS の確立、実施、維持及び継続的改善に必要な資源を決定し、提供しなければならない。

※ 資源、力量（意図した結果を達成するために，知識及び技能を適用する能力。）、認識、コミュニケーション、文書化した情報など、組織が、何が必要なのかを決定し確実に提供すべきとしています。

8．運用

必要なプロセスを計画し、実施し、かつ、管理しなければならない。
※さらに、個人情報保護リスクアセスメントを実施しなければならない。と原則的に明言されています。

9．パフォーマンス評価

※ パフォーマンスとは、“測定可能な結果” のこと。内部監査とマネジメントレビュー（2006 年版では“事業者の代表者による見直し”）について書かれています。2006 年版では、是正処置及び予防処置が含まれていましたが、他のマネジメントシステムの近接性に配慮し、別項目とされました。

10．改善

※ 不適合が発生した場合には、不適合をレビューし、また取った是正処置の有効性をレビューし、必要な場合に、PMS の変更を行うとしています。また PMS の適切性、妥当性及び有効性を継続的に改善しなければならない。としています。

次回から、実質的な新 JIS とも言える「附属書 A（規定）管理目的及び管理策」について連載していきます。

目次　＝https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/000JISQ15001_2017.html

ご参考：JIS 改正にともなう、プライバシーマーク申請時の注意

2018 年 1 月 12 日、JIPDEC プライバシーマーク推進センターより、新審査基準の「プライバシーマーク付与適格性審査基準」が公表されました。要旨は、PMS の対応において、

1．改正個人情報保護法への対応
2．個人情報の管理台帳に追記する事項（保管期限）
3．従業者の教育に盛り込む必要がある事項（個人情報保護方針）
4．運用の確認（日常点検や、それに伴う是正、代表者への報告など）

が必要になること、また、業務の必要に応じて、

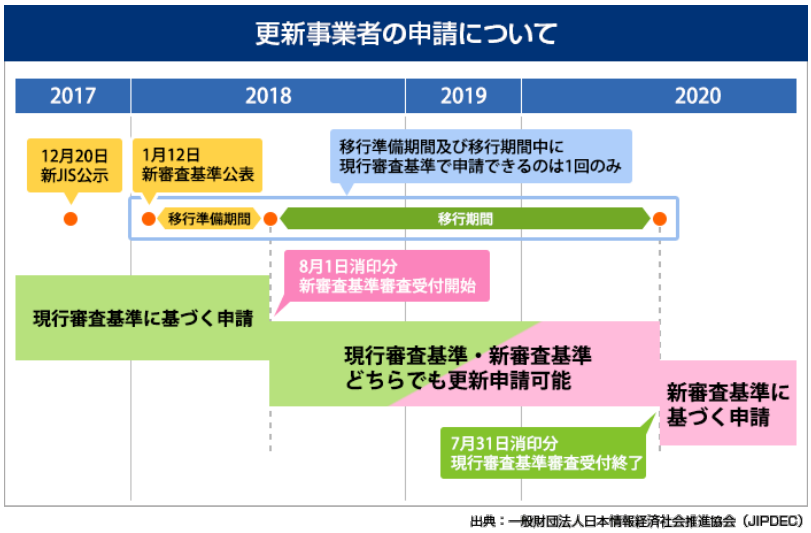
5．共同利用について、共同利用者間における契約で定める事項、
6．委託契約に盛り込むべき事項（委託契約終了時の措置）

が追加になります。

2018 年 8 月 1 日より、新審査基準によるプライバシーマーク審査の適用が開始されますが、更新事業者の申請については、移行期間が 2 年間設けられています。

ただし現行（2006 年版）審査基準による更新申請の場合、新審査基準未対応の運用状況は、継続的改善事項に準ずる指摘となり、次回（2 年後）の更新審査までに対応することになります。

新審査基準による更新申請の場合は、新審査基準への対応が完了していなかった場合、指摘事項もしくは、継続的改善事項に準ずる指摘となります。



JIPDEC ホームページより引用　**https://www.workstrust.com/info/p_newjisq.html**

！注意！：新規申請事業者は、2018 年 8 月 1 日より、「新審査基準に基づく申請」のみ受け付けられます。

以上　■

<目次>

2018.2

支部報告 【 北海道支部 2018 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 2018 年 1 月の月例研究会を開催しました。

・日時：2018 年 1 月 12 日（金）18:30～20:30　　参加者：5 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：「AI スピーカーとシステム監査」

・講師：北海道支部長 宮崎雅年

＜講演概要＞

物のインターネットとして IoT が話題になっていすます。

一般家庭における IoT の具体的な例として AI スピーカーが登場し、日本の家庭の中にも IoT が導入される流れとなってきました。

AI スピーカーとは、Google 社が 2017 年秋に「Google Home」を日本で発売し、Amazon.com 社も 2017 年末に「Amazon Echo」を日本で発売したものです。

その可能性については今後の推移を静観しようと思いますが、普及に向けた技術的な課題のほか、何がどこまでできるのか、「スピーカー」とはいうものの「マイクロフォン」に近い実態に期待と警戒が混在します。

そこで、システム監査の観点から AI スピーカーに斬り込んでみたいと思います。

なお、今回の発表は講師の個人的意見であり、講師の所属する会社の意見を代弁するものではありません。

＜講演内容＞

1. AI スピーカーが見据える世界

AI スピーカーの市場に参入しているメーカーは、Google、Amazaon.com のほか、ソニー、パナソニック、東芝映像ソリューション、NTT ドコモ、ソフトバンクなどがあります。また、富士通が開発中、LINE が限定発売となっています。

これらのメーカーが見据えているのは、家中の家電製品などが人と会話し、人の意思をくみ取って自動的に動く家である「ホームコネクテッド」といわれています。

2. AI スピーカーとは何か

機能としての AI スピーカーは、高音質・広帯域のオーディオ・スピーカーではなく、一般的なスピーカーとマイクロフォンをコンピューターで制御するといったイメージに近いものです。

では、コンピューターは何をやっているのでしょうか。

コンピューターは、音声認識技術と対話技術を組み合わせた「音声 AI」という人工知能を利用した人と機器とのインターフェースの役割を担っています。

3. AI スピーカーをめぐる戦い

AI スピーカーをとりまくシステムの全体構成は、音声 AI、API（Application Programming Interface）、プラットフォームですが、提供するサービスの主戦場は、IoT 機器間とのインターフェースとしての API から、IoT が稼働するプラットフォームへと移り変わりつつあります。

音声 AI の要素技術は、音声認識技術、音声対話技術、音声合成技術ですが、Apple 社の Siri や初音ミクなど、個々の要素技術は既に開発済みの技術といえるでしょう。

そのような場合、個々の要素技術を統合してサービスとして提供する構想・企画が肝要かと思います。自社開発にこだわっていては、実際のサービス提供までに長い期間が必要であることから、一刻も早くサービスとして提供を開始することが生き残るために求められますが、セキュリティ事故を含めた致命的な障害が発生しないことも必要です。

そのためには、下表に示すように自社内で不足している要素技術を先行他社から調達することもあり得るでしょう。

表．AI スピーカー等と採用している音声 AI

メーカー	AI スピーカー等の機器名	採用している音声 AI
Amazon.com	Amazon Echo	Amazon Alexa
LG Electronics	冷蔵庫	
TOSHIBA	TH-GW10（英語版）	
ONKYO	VC-FLX1、Elite	
HARMAN	Harman Kardon Allure	Google Assistant
Google	Google Home	
SONY	LF-GA10	
Panasonic	SC-GA10	
HARMAN	JBL LINK	
ONKYO	G3	
GE	調理器具	
NVIDIA	SHIELD TV	
HARMAN	Harman Kardon Invoke	Microsoft Cortana
Apple	Home Pod、Apple TV	Apple Siri
ONKYO	RAYZ	
ユカイ工業	こだま	A/UN（TOSHIBA）
NTT ドコモ	petoco	vGate ASR（フォートレック）
LINE	「WAVE」、「CHAMP」シリーズ	Clova を開発
SHARP	ホームアシスタント	COCORO+
TOSHIBA	TH-GW10（日本語対応）	リカレントを改善中
LG Electronics	白物家電群	Deep ThinQ を開発中

自社開発にこだわらない戦略をとっているメーカーは、「Time to Market」を重視し、できるだけ早く製品化することを優先したといえるでしょう。

例えば、AI スピーカーの「スピーカー」機能の高音質・広帯域という性能を高めることで差異化を図ったオーディオ機器メーカー（ONKYO、Panasonic、HARMAN、SONY）がある一方、人と機器との間のインターフェースである AI スピーカーよりも、むしろそれと連携して動作する多種多様なホーム IoT 機器の販売や、ホーム IoT 機器を用いたコネクテッドホームに関する事業から得られる様々なデータ活用に狙いが移ったメーカー（東芝映像ソリューション）があります。

実際、欧米では 2012 年ごろからホーム IoT が巨大市場に急成長しつつあり、2021 年には米国の 55%の世帯、欧州の 36%の世帯に普及するとの予測もあります。

さらに、ホーム・エネルギー・マネジメント・システム（HEMS）をはじめとする消費者向けサービスが拡大しています。

2018 年 1 月に米国ラスベガスで開催された CES 2018 では、コネクテッドホーム以外にもコネクテッドカーが大盛況であったと報じられました。（CES 2018 では、「AI スピーカー」という名称ではなく「スマートスピーカー」という名称が採用されていました。）

翻って日本国内では、ネットワーク家電自体に日本のメーカーも取り組んでいるものの、その仕様がメーカーごとに異なり、相互接続がほとんどできないことから、これから市場が立ち上がるか、という状況です。

4. IoT をとりまくセキュリティ事故

IoT 機器のセキュリティ事故等の事例では、Web カメラ等の IoT 機器への不正侵入・乗っ取り、意図しない遠隔操作・踏み台にした DDoS 攻撃が発生しています。

これらは、Mirai などの IoT 機器を狙ったマルウェアの拡散がある一方、パスワードを設定していないか初期パワードから変更としないなどのように利用者に問題があるほか、IoT 機器のファームウェアのバグによりパスワードが容易に漏えいしてしまうなど IoT 機器の設計に問題がある場合もあります。

5. IoT のシステム監査

IoT 機器の脅威として、不正侵入・乗っ取り・意図しない遠隔操作により、個人の日常の情報が筒抜けになるということが挙げられます。

つまり、プライバシー保護の必要性からセキュリティ対策が求められます。

IoT 機器のリスクとして、インターネットを介してすべてが繋がっているという状態が挙げられます、

そのため、セキュリティを意識した IoT 機器の企画・設計が求められることから、安全性、信頼性、効率性を確保するためのシステム監査というより、もっと監査目的を絞り込んだセキュリティ監査がより適しているのではないでかと思います。

また、監査する上での注意事項として、セキュリティ監査のためならば、短い時間でもサービスの停止が許容されるということがあります。サービスの利用者によって異なるでしょうが、一瞬たりとも停止することが許容されないインフラに近いサービスがあるのではないでしょうか。さらに、ペネトレーションテストなどのように、実際のシステムに侵入してテストを実施するには大変にリスクが高いでしょう。

パスワードを設定していない、初期パスワードから変更していないのは論外として、あるべきセキュリティ

対策は、不正侵入・乗っ取りされても何もできない、意図しない遠隔操作ができないというのが重要ではないでしょうか。

また、サービスの提供開始後ではなく、提供開始前にペネトレーションテスト等の侵入テストを実施してセキュリティ上の弱点を洗い出し、対策を講じてからサービスの提供を開始するのが好ましいと思います。

しかし、実際の IoT 機器は、一般の消費者が利用者なので、一般の消費者が設置している IoT 機器まで含めて侵入テストを実施することは非現実的であり、サービス提供の開始前では非常に困難でしょう。

次善の策として、市販の IoT 機器がある程度のセキュリティを確保できていることを認証する制度も必要でしょう。

6. IoT セキュリティガイドライン

認証の基準として参考になりそうなものとして、総務省ならびに経済産業省で開催した「IoT 推進コンソーシアム」が平成 28 年 7 月 5 日に公表した「IoT セキュリティガイドライン ver.1.0」（以下、「ガイドライン」と省略します。）が挙げられます。

ガイドラインの目的は、関係者が取り組むべき IoT のセキュリティ対策の認識を促すとともに、その認識のもと、関係者間の相互の情報共有を促すための材料を提供することとしており、サイバー攻撃などの被害発生時における関係者間の法的責任の所在を一律に明らかにすることには触れておりません。

また、守るべきものやリスクの大きさ等を踏まえ、役割・立場に応じて適切なセキュリティ対策の検討が行われることを期待するとしており、対象者に対して一律にセキュリティ対策の実施を求めてはいません。

ガイドラインには、以下のことが記載されています。

・方針：IoT の性質を考慮した基本方針を定める。
・分析：IoT のリスクを認識する。
・設計：守るべきものを守る設計を考える。
・構築・接続：ネットワーク上での対策を考える。
・運用・保守：安全安心な状態を維持し、情報発信・共有する。
・一般利用者のためのルール

さらに今後の検討事項として、以下のことが記載されています。

・リスク分析に基づく分野別の対策について
・法的責任関係について
・IoT 時代のデータ管理の在り方について
・IoT に対する総合的なセキュリティ対策について
・本ガイドラインの見直しについて

＜講演後の討議＞

すべてのものが繋がる IoT において、プライバシー保護のためのセキュリティ対策は、医療・介護の分野で先行している事例もありますが、これからのことであり、致命的なセキュリティ事故が発生しないことを願うばかりとの意見がありました。

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。

<目次>

2018.2

注目情報（2018.1～2018.2）

■「情報セキュリティ10大脅威　2018」の順位を発表（IPA)】

「情報セキュリティ 10 大脅威 2018」は、2017 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者などからなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。2018 年も昨年同様に「個人」と「組織」という異なる視点で 10 大脅威を選出しています。

なお、3 月下旬に「情報セキュリティ 10 大脅威 2018」の詳しい解説をウェブサイトで公開される予定です。

https://www.ipa.go.jp/security/vuln/10threats2018.html

■「情報セキュリティ 10 大脅威 2018」　　NEW：初めてランクインした脅威

昨年順位	「個人」の 10 大脅威	順位	「組織」の 10 大脅威	昨年順位
1 位	インターネットバンキングや クレジットカード情報の不正利用	1 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	2 位
7 位	ネット上の誹謗・中傷	3 位	ビジネスメール詐欺 NEW	ランク外
3 位	スマートフォンやスマートフォン アプリを狙った攻撃の可能性	4 位	脆弱性対策情報の公開に伴い 公知となる脆弱性の悪用増加	ランク外
4 位	ウェブサービスへの不正ログイン	5 位	セキュリティ人材の不足 NEW	ランク外
6 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサービスからの個人情報の窃取	3 位
8 位	情報モラル欠如に伴う犯罪の低年齢化	7 位	IoT 機器の脆弱性の顕在化	8 位
5 位	ワンクリック請求等の不当請求	8 位	内部不正による情報漏えい	5 位
10 位	IoT 機器の不適切な管理	9 位	サービス妨害攻撃による サービスの停止	4 位
ランク外	偽警告 NEW	10 位	犯罪のビジネス化 （アンダーグラウンドサービス）	9 位

<目次>

2018.2

協会からのお知らせ　【２０１８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】

２０１８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。昨年からこれに加え、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 ----------

2018 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

2018 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

2018 年 2 月 1 日（木）～2018 年 3 月 31 日（土）（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>

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2018.2
2018	**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：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	5：年会費未納者宛督促メール発信 8：理事会 9：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 30：法人住民税減免申請	初旬：春期 CSA・ASA 書類審査 中旬：春期 ASA 認定証発行	15：春期情報技術者試験
5 月	10：理事会	中旬：春期 CSA 面接	
6 月	1：年会費未納者宛督促メール発信 14：理事会 15：会費未納者督促状発送 16～：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）	 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 12：理事会	 下旬：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） 26：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	
9 月	14：理事会	～　秋期 CSA・ASA 募集中　～9/30 迄 2：第 19 回「事例に学ぶ課題解決セミナー」 5：第 225 回月例研究会「IoT 時代のセキュリ ティを実現する 3 視点とシフトレフト」 14-15 & 28-29：第 30 回システム監査実務セ ミナー(日帰り 4 日間コース)	 30：西日本支部合同研究会 in Fukuoka(福岡)
10 月	12：理事会	21:SAAJ 活動説明会（東京茅場町） 30：第 226 回月例研究会	15：秋期情報処理技術者試験
11 月	9：理事会 9：予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/9〆切） 18：2018 年度年会費請求書発送準備 25：会費未納者除名予告通知発送 30：本部・支部予算提出期限	11,18,25：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	
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

<目次>

2018.2

【 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

・「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>

2018.2

【 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

2018 年度の年間テーマは、「システム監査人の新たな活躍」です。
皆様のご投稿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。

□■ 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　（2018. 1.11 改訂）

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 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>

2018.2

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（市場通り）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：　藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、高橋典子
編集支援：　仲厚吉（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)1997-2018、認定 NPO 法人 日本システム監査人協会

<目次>