システム監査学会　設立30周年記念研究大会

マイナンバー特別研究プロジェクト
＆　個人情報保護専門監査人部会
研究成果 報告
マイナンバーとシステム監査について
ー 事例・ヒアリング結果と課題 ー

My number systems and Systems audits
- Case studies, interview Results and Problems -

2017年6月2日

報告者　白川 里至
Satoshi Shirakawa CISA

1

目次

1. 活動メンバ
2. 活動状況
3. 事例１：地方自治体
4. 事例２：総合サービス企業
5. 事例３：パッケージサービス提供者
6. 管理基準への反映

2

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

1. 活動メンバ

個人情報保護専門監査人部会メンバ
研究プロジェクトメンバ　12名

氏名	所属		個人	研P
朝倉　俊道	エムビーケーメタルソリューション株式会社			●
足立　憲昭	イオンエンターテイメント株式会社			●
稲垣　隆一	稲垣隆一法律事務所	主査	●	
大島　誠	第一屋製パン株式会社			●
木村　裕一	一般財団法人日本情報経済社会推進協会		●	
黒澤　兵夫	TAKE国際技術士研究所	副主査	●	●
久山　真宏	東京電機大学		●	●
最首　克也	株式会社最首克也事務所			●
白川　里至	KDDI株式会社			●
高野　美久	NECソリューションイノベータ株式会社			●
本田　実	城西国際大学	主査		●
桃澤　正和	富士通株式会社		●	

3

2. 活動状況

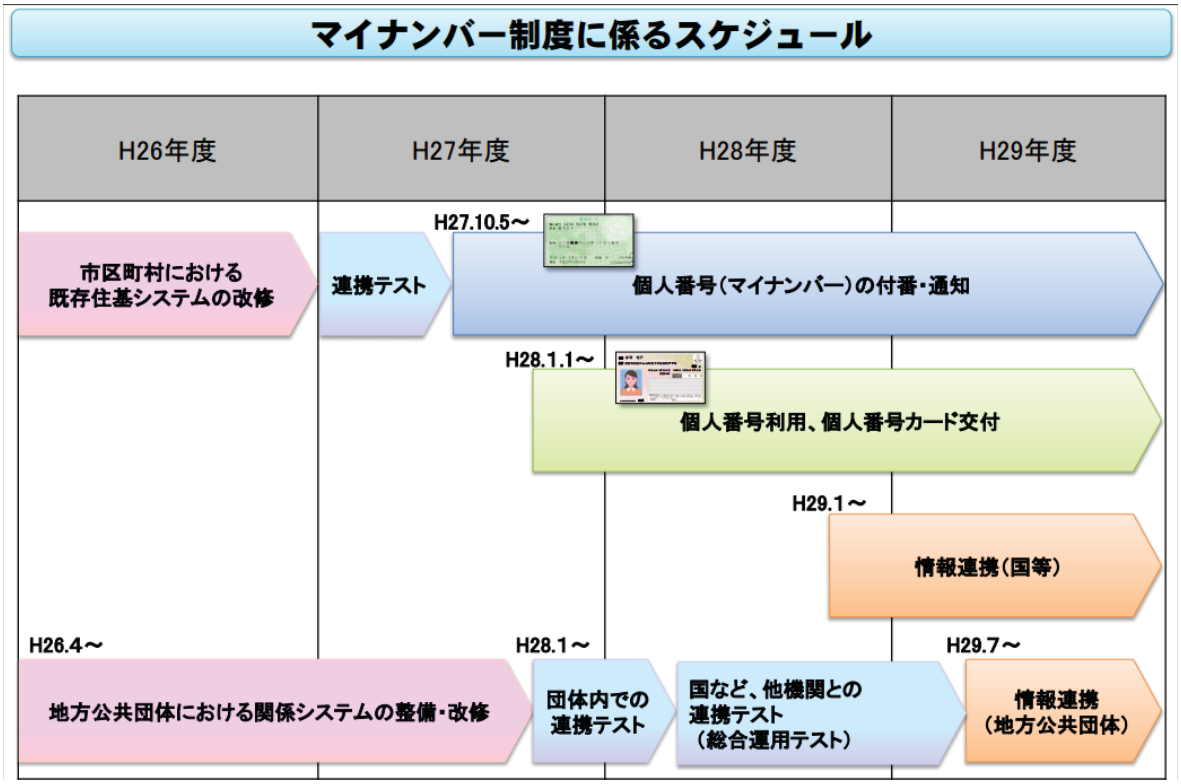
- 月に一回ペース　平日　18:30開始　約2時間

回数	開催日	場所	内容
第1回	8月２５日	稲垣法律事務所	今年度の方針
第2回	9月２７日	稲垣法律事務所	ヒアリング・スケジュール
第3回	10月２７日	稲垣法律事務所	サービス業ヒアリング
第4回	11月２４日	稲垣法律事務所	PKGヒアリング
第5回	12月２２日	稲垣法律事務所	課題検討
第6回	1月１７日	稲垣法律事務所	Ｆ自治体ヒアリング
第7回	2月２２日	稲垣法律事務所	研究発表大会について
第８回	4月７日	稲垣法律事務所	まとめ

4

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

マイナンバー制度に係るスケジュール



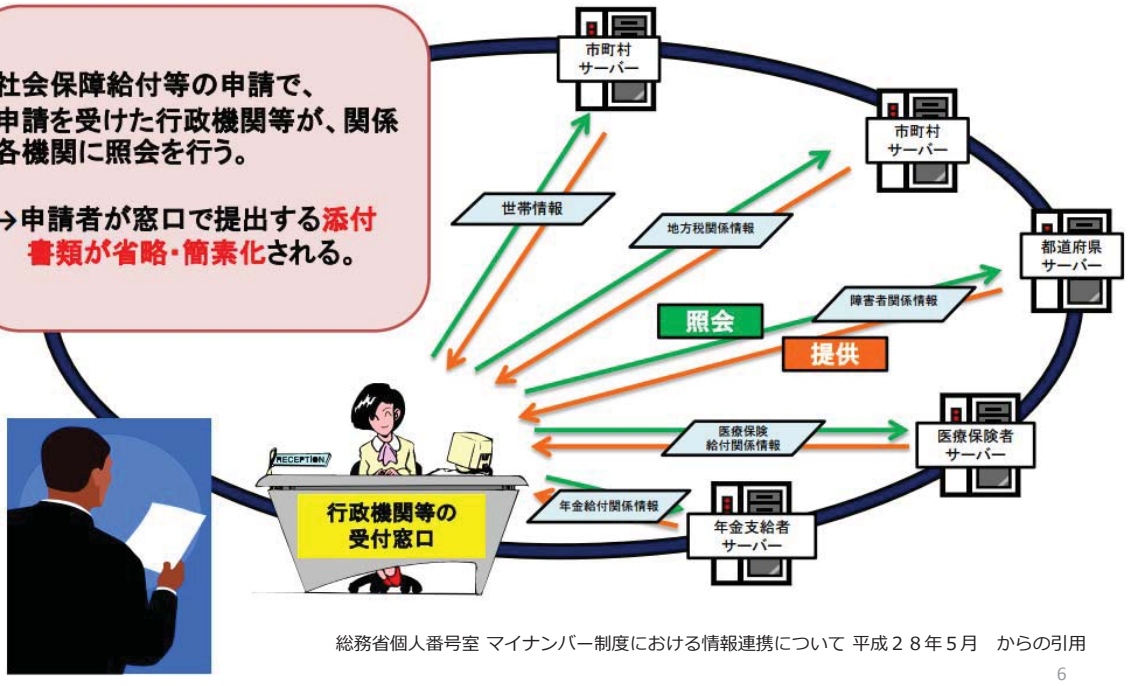
総務省個人番号室 マイナンバー制度における情報連携について 平成２８年５月　からの引用

5

情報連携により国民の負担軽減が実現します。

社会保障給付等の申請で、
申請を受けた行政機関等が、関係
各機関に照会を行う。

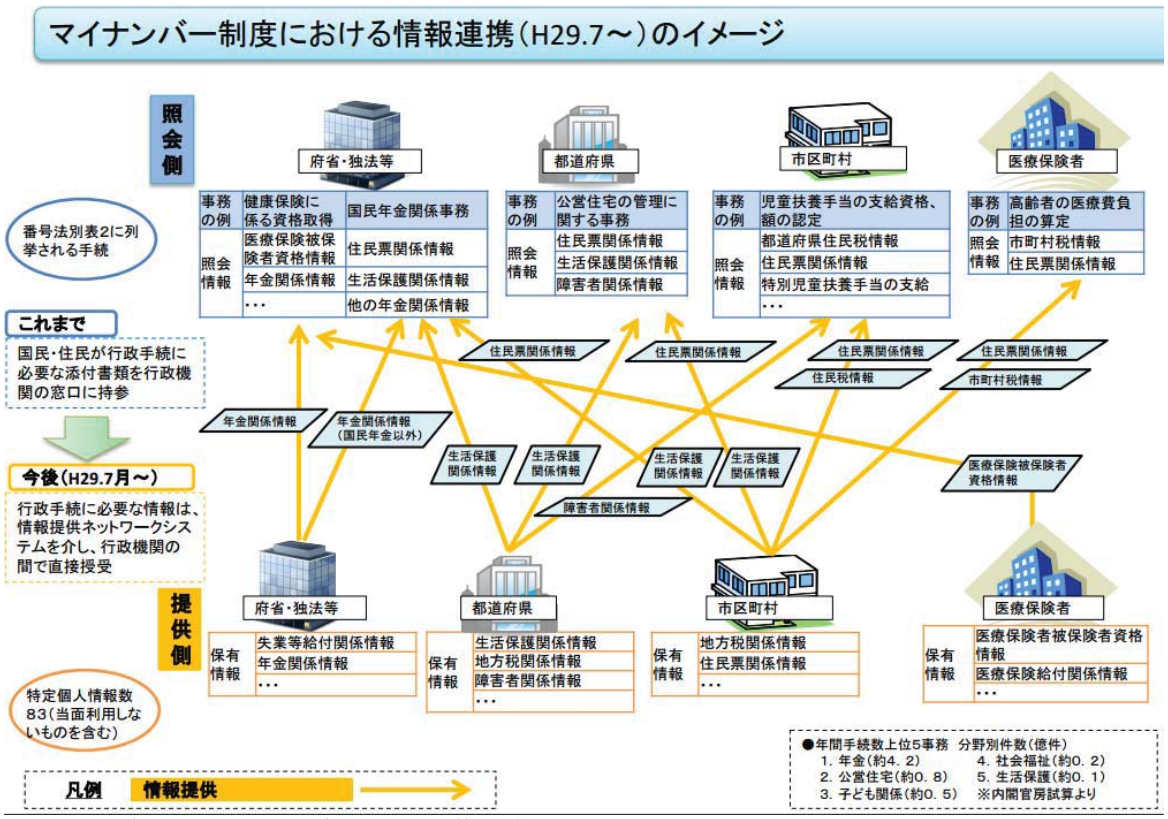
→申請者が窓口で提出する**添付書類が省略・簡素化**される。



総務省個人番号室 マイナンバー制度における情報連携について 平成２８年５月　からの引用

6

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.



総務省個人番号室 マイナンバー制度における情報連携について 平成２８年５月　からの引用

7

地方自治体（F）

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

地方自治体・マイナンバー制度の展開と課題

1．マイナンバー制度の動向
・他機関への情報提供ネットワーク（情報連携）総合運用テスト
2．安全管理措置
・マイナンバーシステム監査
・マイナンバー研修
・情報セキュリティ対策
**　インターネットの分離とメール、ファイルの扱い（ログ管理）**
3．マイナンバー制度利活用の検討
・マイナンバーカード
**　マイキープラットフォーム（図書館貸出証、スポーツ施設券等）**
・マイナポータル
**　子育てワンストップサービス**

9

地方自治体におけるシステム監査の取組

1．システム調査（S57内部）
⇒　システム監査（H17外部のシステム監査人）
2．マイナンバーシステム監査

・マイナンバーを含む個人情報の保護で、自治体に実施を義務付け
　：**PIA**（Privacy Impact Assessment）
・PIA実施ガイドライン（内閣官房）
　：マイナンバー関係事務と予測されるリスクの評価、システムや業務、教育におけるプライバシー保護施策、国民への公表、運用の評価と改善などに取り組む

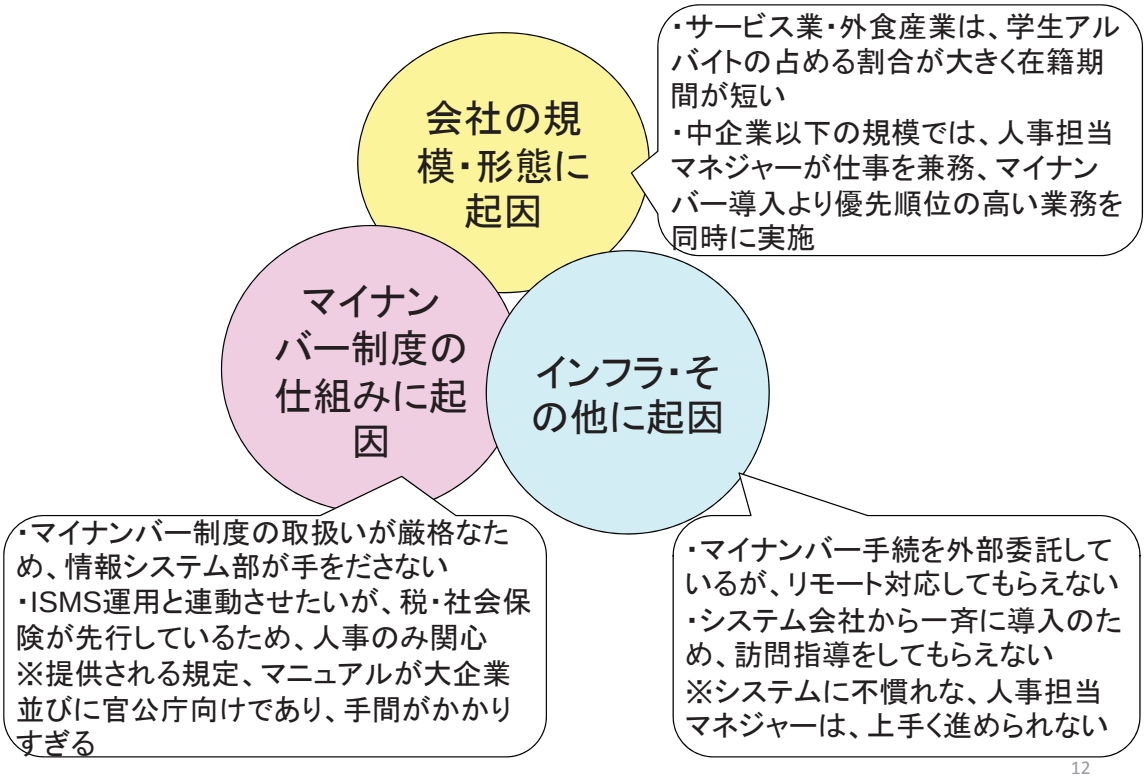
3．情報セキュリティ
・**機密性**（情報漏洩、個人情報保護）
・**完全性**（正しい情報の担保）
・**可用性**（行政事務へ利活用）

10

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

総合サービス企業

マイナンバー運用についての問題・課題



12

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

マイナンバー制度の課題を整理すると

内部要因

共通課題①

・人事部門の出来事となり、会社全体のタスクになっていない。（個人に負担）
・アルバイトの構成比が高い、サービス、外食では、入替りが激しく、保存手続が難しい

外部要因

共通課題②

・単純に外部委託できない、受託先が責任回避のため、訪問指導との深入りを避けている
・政府の啓蒙活動もトーンダウンして、自治体の窓口任せになっている

動機づけ

共通課題③

・税・社会保険の徴収漏れが前面に出て、民間企業には“コスト増”だけでメリットがない
・お役所仕事で、手続きに長い時間を要するため、“公的サービス”としてのレベルが低い

13

マイナンバー制度を振り返ってみると

プロジェクト体制がうまくいかず、“人事部門の仕事”と認識された。現場から本社までの流れで実施できなかった。

サービス業・外食産業等のアルバイトが多く在籍し、入替りの激しい業態では、“退職日より7年間保存”は膨大な量となり保管料も大きくなる

マイナンバー特別研究プロジェクト話合い

今後、医療分野、金融分野は進んでくるが、他の民間事業者がどのようにするかの検討が開始された。“マイナンバーが、本人認証に代わってくる”ことが切り替えの動機になるか？

14

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

パッケージサービス提供者

マイナンバーサービス提供者からの視点

日時：2016年11月24日 19:00開始／場所：稲垣隆一法律事務所
協力：株式会社オービックビジネスコンサルティング　日野様 堀江様

昨年度は、サービスの仕組みと展望、構築時の苦労談を伺った。
需要期のピークを乗り越えた現在、顧客の反応、ガイドラインの評価、
更に今後の展望についてお話を伺った。

株式会社オービックビジネスコンサルティング社 マイナンバーサービス紹介ホームページからの引用

16

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

OBCマイナンバーサービス（クラウド型）利用実績

10,000社	⇒	14,000社	6百万件
2015年11月時点		2016年11月現在	収容マイナンバー数

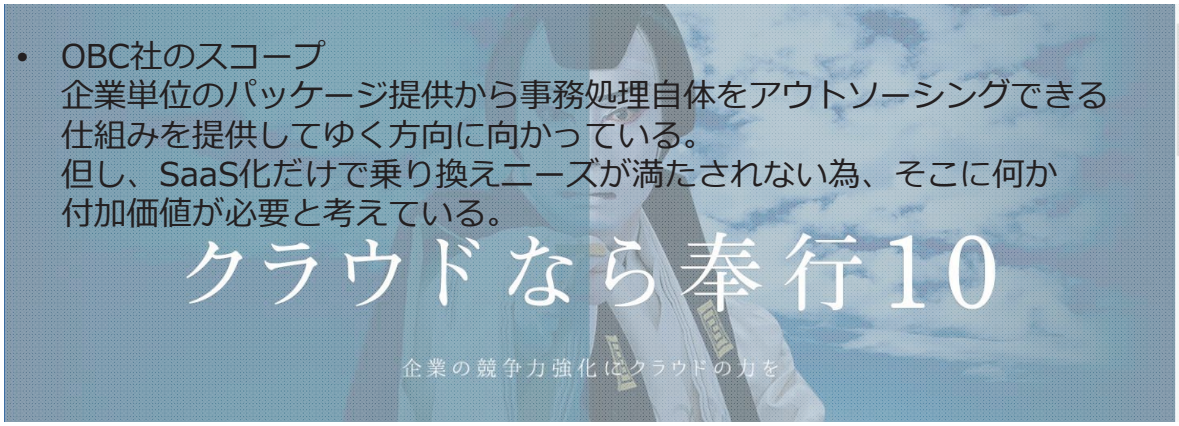
顧客の反応
- クラウド利用は、消極的　・・・　８：２　（手対応：クラウド）
- 大手企業は、オンプレミス型への対応を要望

ガイドラインについて
- 政府主導の制度検討は大手SI企業メンバで構成されるケースが多いことから、中小企業規模の視点が欠けているように感じられる。結果、社会性の低いシステム要件が形成されてしまっている。
- 細かな対応方法をタイムリーに把握しておくために、CSAJ協会のメンバ内でQAの共有を図っていた。

システム監査に係る点では
- クラウドの運用管理（IT全般統制）に係る質問対応が挙げられる。
- 内容の粒度や様式の異なる質問票に個別に対応する負荷が高い一方で、SOCレポートの様な第三者認証を得る為には多くのコストがかかることから、標準的な質問回答集を作成して提供する対応を取った。

17

今後の展望
- マイナンバーについて
  2次利用が始まらなければ、充分な導入効果が得られない制度と理解。
  現行でのマイナンバー利用範囲においてはシステムへの対応ニーズは収束しているが、2次利用（民間解放）が始まると新たなマイナンバー確認・記録事務処理に係るシステム対応ニーズが見込まれる。



- OBC社のスコープ
  企業単位のパッケージ提供から事務処理自体をアウトソーシングできる仕組みを提供してゆく方向に向かっている。
  但し、SaaS化だけで乗り換えニーズが満たされない為、そこに何か付加価値が必要と考えている。

株式会社オービックビジネスコンサルティング社 ホームページからの引用

18

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

管理基準への反映

No	管理基準	アウト	パッケージ&ASP利用	手作業 （作業の自由度が高いので、作業手順の標準化・マニュアル化と作業手順の順守・管理台帳への記録が不可欠）	クラウドコンピューティング
		着眼点			
78	**2. 分析**				
79	(1)開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認すること。				
80	(2)ユーザニーズの調査は、対象、範囲及び方法を明確にすること。 ((4)要求定義の実施計画に、問題解決プロセス、リスク分析など必要な作業を組み込むこと。)		※マイナンバー対応のケースでは・・・ ・マイナンバー制度の要件を明確にしておくこと。		
81	(3)実務に精通しているユーザ、開発、運用及び保守担当者が参画して現状分析を行うこと。		・マイナンバーの取り扱いに関わる担当者（ユーザ及び保守担当者）を洗い出すこと。		
82	(4)ユーザニーズは文書化し、ユーザ部門が確認すること。		・マイナンバー対応要件を文章化すること、該当する担当者が確認すること。		
83	(5)情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。		・パッケージの導入及びASP利用に伴って発生する可能性のあるリスク分析を実施すること。		
84	(6)情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。 ((5)要求定義には、要求の追跡可能性を維持すること。)		・パッケージの導入及びASP利用によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。		
85	(7)情報システムの導入効果の定量的及び定性的評価を行うこと。	(1)マイナンバー制度にきちんと対応できているかチェックする方法を検討しておくこと。			
86	(8)パッケージ・ソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。		・調達予定のパッケージ及びASPサービスの適合性を確認すること。		
87	(9)ソフトウェアサービスの使用にあたってはユーザニーズとの適合性を検討すること。				
88	**3. 調達**				
89	(1)調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。		・パッケージ及びASPサービスを動かすソフト・環境は、導入計画及びユーザニーズに基づき作成し、ユーザ、運用及び保守の責任者が承認すること。		
90	(2)ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。		・ソフトウェア、ハードウェア及びネットワークは、パッケージ及びASPサービスを動かすソフト・環境を基に選択すること。		
91	(3)開発を遂行するために必要な要員、予算、設備、期間等を確保すること。				
92	(4)要員に必要なスキルを明確にすること。		・パッケージの導入及びASP利用、運用に必要なスキル（インストール、操作等）を明確にすること。		
93	(5)ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って実施すること。		・サービス利用環境、契約条件（途中解約、価格改定、権利・ライセンス、損害賠償の範囲）、サービスレベル（稼働率、パフォーマンス）が社内のルールに適合すること。		

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

No	管理基準	アウトソーシング	パッケージ&ASP利用	手作業 (作業の自由度が高いので、作業手順の標準化・マニュアル化と作業手順の順守・管理台帳への記録が不可欠)	クラウドコンピューティング
		着眼点			
172	(13)情報システムのユーザに対する支援体制を確立すること。	・ヘルプデスクのオペレータを指導・サポートする者に専門知識のある人材を配置する等			
173	(14)情報セキュリティに関する教育及び訓練をユーザに対して実施すること。				
174	(15)情報システムの稼動に関するモニタリング体制を確立すること。				
175	(16)情報システムの稼動実績を把握し、性能管理及び資源の有効利用を図ること。 ((7)サービス提供者は、サービスの予算業務及び会計業務の文書化された手順に従って管理すること。)				
176	**3. 入力管理**				
177	(1)入力管理ルールを定め、遵守すること。			・特定個人情報の取得ルールを『特定個人情報取扱規程』に定め、周知徹底すること。	
178	(2)データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。			・事務取扱担当者が特定個人情報を取扱う業務に従事する際は、『特定個人情報取扱規程』その他関連ルールに従って業務を行うこと。	
179	(3)入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。			・事務取扱担当者が特定個人情報を取扱う業務に従事する際は、『特定個人情報取扱規程』その他関連ルールに従って業務を行うこと。	
180	(4)データの入力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。			・書類を送付する際は、追跡可能なサービス(簡易書留、開封検知付き/GPS付き郵送サービス等)を利用すること。	
181	(5)入力データの保管及び廃棄は、入力管理ルールに基づいて行うこと。			・事務取扱担当者は、個人番号を取扱う事務の範囲に該当する書類は最新の状態で、保存期間を経過するまで保管すること。 事務取扱担当者は、個人番号を取扱う事務の必要がなくなった場合で保存期間を経過した場合、該当する書類を速やかに廃棄又は削除し、「個人番号管理台帳」に記録すること。	
182	**4. データ管理**				
183	(1)データ管理ルールを定め、遵守すること。			・特定個人情報の利用制限、保管制限、提供制限、訂正、廃棄・削除のルールを『特定個人情報取扱規程』に定め、周知徹底すること。	
184	(2)データへのアクセスコントロール及びモニタリングは、有効に機能すること。			特定個人情報を取り扱う区域を、事務取扱担当者以外の往来が少ない場所や覗き見される可能性が低い場所へ配置すること。	

No	管理基準	アウトソーシング	パッケージ&ASP利用	手作業 (作業の自由度が高いので、作業手順の標準化・マニュアル化と作業手順の順守・管理台帳への記録が不可欠)	クラウドコンピューティング
		着眼点			
309	**5. 委託・受託**				
310	**5.1 計画**				
311	(1)委託または受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。				
312	(2)委託または受託の目的、対象範囲、予算、体制等を明確にすること。				
313	(3)委託または受託は、具体的な効果、問題点等を評価して決定すること。				
314	**5.2 委託先選定**				
315	(1)委託先の選定基準を明確にすること。			・事務取扱責任者及び事務取扱担当者は、①～⑦について委託元の定める水準を満たしているか、あらかじめ確認すること。 ①規定、②体制、③人的安全管理措置、④従業者の役割・責任の明確化、⑤組織的安全管理措置の周知・教育、⑥技術的安全管理措置の確認、⑦利用者の認証・許可・監査及び監査証跡の記録	
316	(2)委託候補先に必要な要求仕様を提示すること。		・マイナンバーを含む委託であることを要求仕様に記述すること。		
317	(3)委託候補先が提示した提案書の比較検討を行うこと。				
318	**5.3 契約**				
319	(1)契約は、委託契約ルールまたは受託契約ルールに基づいて締結すること。 ((4)契約書の内容を関係者に周知徹底すること。)		・システム設定時などの対応は契約書に明確に定義すること。 ・委託・受託契約のルールにマイナンバーの取り扱いに必要な要件を規定すること。	・委託契約には、安全管理措置を遵守させるために必要な以下①～⑧の規定等を盛り込むこと。 ①秘密保持義務、②事業所内からの特定個人情報の持出し禁止、③特定個人情報の目的外利用の禁止、④再委託における条件、⑤漏えい事案等が発生した場合の委託先の責任、⑥委託契約終了後の特定個人情報の返却又は廃棄、⑦従業者に対する監督・教育、⑧契約内容の遵守状況について報告を求める規定	・クラウド事業者とのSLAが適切であること。
	(1)'マイナンバー制度に準拠していることの保証を書面で取得すること。				
320	(2)コンプライアンスに関する条項を明確にすること。				
321	(3)再委託の可否について明確にすること。			・委託元の許諾が得られた場合に限り、再委託可能とし、再委託契約に委託先契約と同等の規定を盛り込むこと。	

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.

ご清聴、ありがとうございました。

23

©2017JSSAシステム監査学会-「マイナンバー特別研究プロジェクト＆個人情報保護専門監査人部会」 All right reserved.