システム監査学会　第30回研究大会

# 個人情報保護専門監査人部会 ＆マイナンバー特別研究プロジェクト 研究成果 中間 報告 「マイナンバーとシステム監査」

2016年6月3日

報告者　白川 里至 CISA

# 目次

# 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 | | ● | |

# 2. 活動状況

- 月に一回ペース　平日　18:30開始　1.5~2時間
- 第2回から合同開催

| 回数 | 開催日 | 場所 | 備考 |
|---|---|---|---|
| 第1回 | 8月3日(月) | 城西国際大学紀尾井町キャンパス1号棟 | |
| 第2回 | 9月7日(月) | 稲垣法律事務所 | |
| 第3回 | 11月16日(月) | 城西国際大学紀尾井町キャンパス1号棟 | |
| 第4回 | 12月18日(金) | 城西国際大学紀尾井町キャンパス1号棟 | |
| 第5回 | 1月28日(木) | 稲垣法律事務所 | |
| 第6回 | 3月1日(木) | 城西国際大学紀尾井町キャンパス1号棟 | |
| 第7回 | 3月29日(火) | 城西国際大学紀尾井町キャンパス1号棟 | |
| 第8回 | 4月22日(水) | 城西国際大学紀尾井町キャンパス1号棟 | |
| 第9回 | 5月11日(水) | 稲垣法律事務所 | |

# 3-1. 個人情報保護専門監査人部会の背景

個人情報保護に関し、主に次の二項目について法令、制度、開発状況等を検討・調査し、システム監査として行うべき情報について発信する。

→ マイナンバー（社会保障・税番号制度）研究・調査する。

・個人情報保護法改正/特定個人情報保護

・附番、情報連携、本人確認のプロセス

＝背景＝

- 改正した個人情報保護法では個人情報を含んだデータベースを不正に提供した場合に刑事罰を科す「データベース保護法案」を新設した。
- 蓄積された個人情報をビッグデータとして活用し、個人が特定できない形式で第三者へ提供できるようにした。
- 「個人情報データベース提供罪」は、ベネッセの情報漏えい事件を受けて新設した。課題として、匿名加工情報の規制対象範囲及び、第三者提供の記録義務がかかる範囲等がある。

マイナンバー制度/システムへシステム監査を適用することを検討する。

# 3-2. 研究プロジェクトの背景

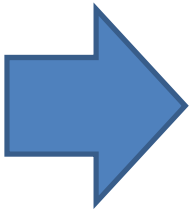
- 2013年からの2箇年「共通フレームをベースとしたシステム管理基準検討研究プロジェクト」にて
  ① 共通フレームを考慮したシステム管理基準改定案
  ② システム管理基準と共通フレームワーク2013対応表
  を作成した。
- 今期は「中小企業におけるマイナンバー対応」という具体的なシーンを想定し、導入時の留意点、管理項目（コントロール）に対応した監査対象ドキュメント、監査の観点などを検証した。

# 4-1.合同研究会の趣旨

- 2016年からのマイナンバーの利用開始にあたって、企業では業務の見直し、システムの改修、管理体制の見直し等を開始しているが、多くの中小企業ではまだ十分に対応していない。当面手作業で対応している企業でも、いずれシステムの改修をすることになる。
- 本合同研究会では、マイナンバー制度導入にあたって、システム管理基準を利用して、企画、開発、運用、保守の各工程でのなすべき作業を研究した。
- システム管理基準には、昨年度の「共通フレーム2013をベースとしたシステム管理基準検討」研究プロジェクトの成果物を採用する（システム管理基準改定案と呼ぶ）。
- 今年度は、マイナンバー制度の基礎的な理解、システム管理基準改定案の理解をした上で、企画、開発、運用、保守における考慮すべき項目を研究し、次年度は共通業務を中心に、考慮すべき項目を研究する。

# 4-2.合同研究会の目的

- 合同研究会の成果物は実際に役立つものにする
- 対象は中小企業向けとする。



「中小企業に向けたマイナンバー導入の
システム構築・運用時の留意点」という内容で、
以下の区分からのガイドラインとする。

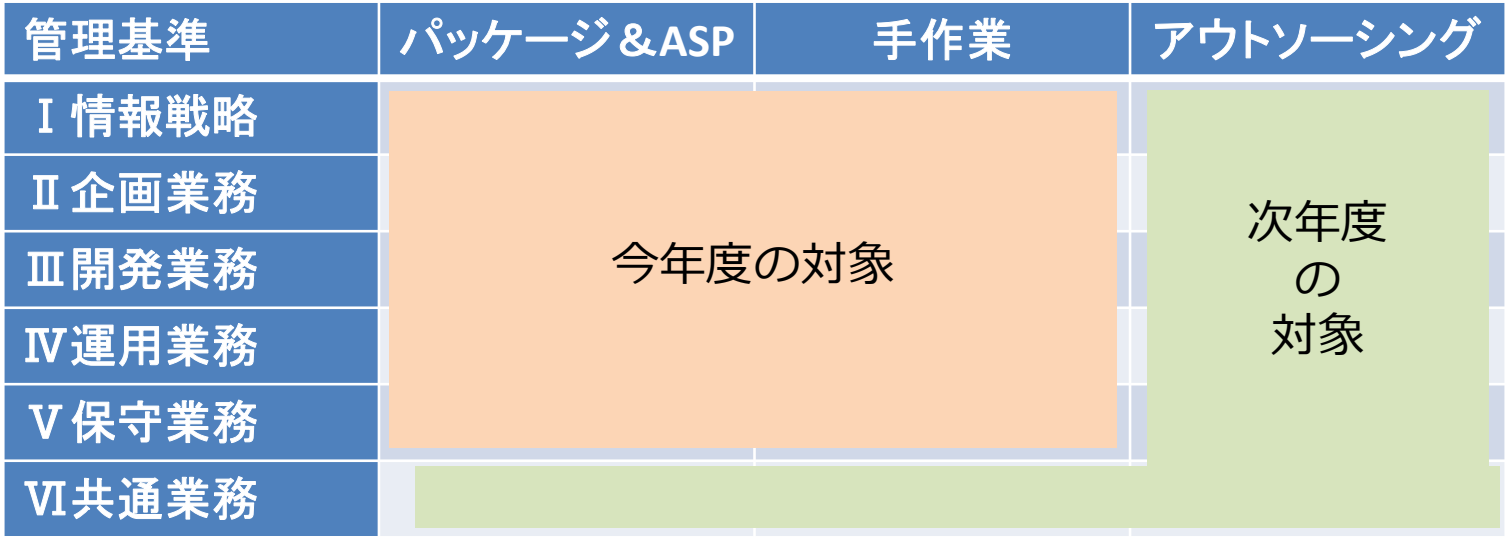
①パッケージ＆ＡＳＰ利用
②手作業
（③アウトソーシング）
㊟来年度の作業とする。

ガイドラインは、ホームページにて公開し利活用を促す。

# 5.合同研究会の検討範囲

　マイナンバー法への対応として、一般的な企業に選択され得る３方式について、共通フレームをベースにシステム監査視点から留意が必要な観点を洗い出した。

＝一般的に選択され得る２っの方式＝
1．パッケージソフトウェア＆ASPサービスの活用
2．手作業での対応
(３．マイナンバーに関わる業務自体をアウトソーシング
　　←　来年度作業 )



# 6.合同研究会の作業手順（1）

作業手順は以下の通り

①システム管理基準改定案に中小企業向けの区分をつける。

- パッケージ＆ASP利用
- 手作業
- （アウトソーシング　←　来年度作業）

② パケージ販売業者へのヒアリング

- 株式会社オービックビジネスコンサルティング様による資料説明、質疑応答

③ 区分ごとの管理基準（項目）、着眼点の追加

その際に、項目×着眼点の関係性を十分に吟味する。
例）着眼点が満足できなければ、項目も満足できない。

# 6.合同研究会の作業手順（2）

前項からの続き

④ システム管理基準改定案に監査の観点を追加。

・効率性、有効性、信頼性、遵守性、可用性、完全性、機密性

⑤ 区分ごとの項目が同様と判断できるものや区分以前のものと判断できるものは、区分単位に分けない。

# 7.合同研究会の作業結果

## パッケージソフトウェア＆ＡＳＰサービスの活用

## パッケージ販売業者へのヒアリング

日時：2015年11月16日 18:30開始／場所：城西国際大学@紀尾井町
対象：株式会社オービックビジネスコンサルティング 様

「マイナンバー収集・保管サービス」の仕組み

- スマホから撮影した個人番号通知カード等の確認書類をクラウドサービスに提出
- 奉行シリーズの給与システムとはインターネット経由にて連携
  印刷時のみマイナンバーを照会させる仕組み、給与システム側には残さない
- 奉行シリーズの保守料金で利用できる
  法改正対応の扱い

# 7.合同研究会の作業結果

## パッケージ販売業者へのヒアリング　前項からの続き

「マイナンバー収集・保管サービス」の導入サポート

- まず、お客様には外部講師によるマイナンバーのレクチャーを受けて頂き、基本的な知識が共有できたところで商品を案内。
- 導入支援キッド（ソフトウェアではなく、マニュアルや書類の様式集の冊子）も有償提供。

マイナンバーの保護対策

- 印刷するときだけインターネットで連携する方式。
  個人番号入力者のメニューを他の業務と分けている。
  一覧表示機能でも特定者分だけしか表示させない。
- 今回のマイナンバー要件にある期間経過後に削除を促す機能もあり
  バックアップの削除については、読み込まないと削除されない。

# 7.合同研究会の作業結果

## パッケージ＆ASPサービスの主な着眼点（サブコントロール）

企画業務／分析
- ・マイナンバー制度の要件、ガイドラインへの準拠性の確認
- ・関連する業務の洗い出し　／　実務担当者の選定、手順の確立
- ・リスクの洗い出し　／　定期的なチェック、評価

企画業務／調達
- ・パッケージ＆ASPへの適合性（件数、予算、納期、運用）
- ・サービスレベルの確認

データ管理／出力管理
- ・帳票/画面　印字/出力項目の確認
- ・操作、管理の取り扱い基準、担当者制限
- ・用途外利用の制限

データ管理／構成（ソフトウェア/ハードウェア/ネットワーク）管理
- ・単体構成
- ・連動構成（給与システム、支払いシステム）

保守・バックアップ
- ・障害・復旧　／　バージョンアップ

# 7.合同研究会の作業結果

## 手作業での対応

※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

## 主なサブコントロール

情報戦略／全体最適化

・手作業対応の周知徹底

情報戦略／コンプライアンス

・取扱部署と責任者の決定　／　規程の制定　／　遵守状況の監査

運用業務／入力管理

・取得ルールの制定と周知徹底　／　取得ルールでの業務遂行　／　保管と廃棄の記録

運用業務／データ管理

・運用ルールの制定と周知徹底　／　作業場所の限定　／　書類の複製禁止

・利用状況の記録と責任者による確認・評価

・運用ルールに基づく書類・電子媒体の持ち出し　／　保管と廃棄の記録

運用業務／出力管理

・利用ルールの制定と周知徹底　／　利用ルールに基づく業務遂行

・保管と廃棄の記録　／　利用状況の記録と責任者による確認・評価

共通業務／人的資源管理

・担当者と責任者の責務を周知徹底　／　責任者による教育・訓練

共通業務／委託・受託

・委託先水準の確認　／　委託契約への安全管理措置遵守規程の盛り込み

・再委託の条件　／　委託業務で提供したデータ・資料の回収・廃棄の確認

# 7.合同研究会の作業結果

## ガイドラインの表記

着眼点

監査の観点

| No | 管理基準（項目）　＋検討結果 | 着眼点 | | 監査の観点 | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | パッケージ&ASP利用 | 手作業 | 効率性 | 有効性 | 信頼性 | 遵守性 | 可用性 | 完全性 | 機密性 |
| 1 | **Ⅰ．情報戦略** | | | | | | | | | |
| 2 | **1．全体最適化** | | | | | | | | | |
| 3 | **1.1　全体最適化の方針･目標** | | | | | | | | | |
| 4 | （1）　ＩＴガバナンスの方針を明確にすること。 | | 「マイナンバーの管理･入力等を行うシステムの導入は行われず、マイナンバーの書類等への記載は、基本的に手書きで行い紙ベースで管理する」方針を周知徹底すること。 | ○ | ◎ | ○ | ○ | ○ | ○ | ○ |
| 5 | （2）情報化投資及び情報化構想の決定における原則を定めること。 | | | ○ | ○ | | ○ | | | |
| 6 | （3）情報システム全体の最適化目標を経営戦略に基づいて設定すること。 | | | ○ | ◎ | | | | | |
| 7 | （4）組織体全体の情報システムのあるべき姿を明確にすること。 | | | ○ | ○ | | | | | |
| 8 | （5）システム化によって生ずる組織及び業務の変更の方針を明確にすること。 | | | ○ | ○ | | ○ | | | |
| 9 | （6）情報セキュリティ基本方針を明確にすること。 | 共通(1)：個人番号を含む情報資産に係るリスクを幅広く検討すること。 | | △ | △ | ○ | △ | ◎ | ◎ | ◎ |
| 10 | **1.2　全体最適化計画の承認** | | | | | | | | | |
| 11 | （1）全体最適化計画の立案体制は、組織体の長の承認を得ること。 | | | | ○ | | | | | |
| 12 | （2）全体最適化計画は、組織体の長の承認を得ること。 | | | | ○ | | | | | |
| 13 | （3）全体最適化計画は、利害関係者の合意を得ること。 | | | | ○ | | | | | |
| 14 | **1.3　全体最適化計画の策定** | | | | | | | | | |
| 15 | （1）全体最適化計画は、方針及び目標に基づいていること。 | | | | ○ | | | | | |
| 16 | （2）全体最適化計画は、コンプライアンスを考慮すること。 | | | | ○ | | ○ | | | |
| 17 | （3）全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。 | | | | ○ | | | | | |
| 18 | （4）全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。 | | | ○ | ○ | | | | | |
| 19 | （5））全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること。 | 共通(1)：システム構築の方針として、パッケージ＆ASP利用、手作業、アウトソーシング等の方針を明文化すること。 | | | ○ | | ○ | | | |
| 20 | （6）全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。 | | | | ○ | | ○ | | | |
| 21 | （7）全体最適化計画は、外部資源の活用を考慮すること。 | | | △ | ○ | | | | | |

# 8.今後の課題（来年度の作業）

## (1)2015年度成果物のレビュー

✓ 2015年度成果物のレビュー（特に監査の観点など）。

## (2)ガイドラインの訴求

✓ 中小企業の経営軸に向けて、ガイドラインの使い方を提示。

## (3)区分としてアウトソーシングの追加

✓ パッケージ＆ASP利用、手作業にアウトソーシングを追加。

## (4)コンプライアンスの強化

✓ ルール、法令、契約、規制事項を特定すること。
✓ その内容を組織の状況に応じて具体的に定めること。
✓ その内容を組織の長、関係者に周知すること。
✓ マイナンバーの取扱いに際し、具体的なルールを遵守すること。
✓ 継続的にモニタリングすること。
✓ 継続的にコンプライアンスレベルを上げること。

## (5)検証

✓ ガイドライン適用結果の検証。

ガイドライン適用に、ご協力ください。

ご連絡、お待ちしております。

satoshishirakawa1964@icloud.com

ご清聴、ありがとうございました。