

マイナンバー対応ソフトウェアの 対応範囲を“見える化”する 評価シート

1 はじめに

2013年5月、社会保障・税の共通番号（マイナンバー）法が参院本会議で可決、成立し、2016年1月から新制度開始となりました。

CSAJには社会保険関係の届出書や所得税関係書類作成に使用する給与計算ソフトウェアを開発する会員企業が多数加盟しており、事業者様のマイナンバー制度対応を支援するとともに、対応コストの低減に貢献すべき立場にあると認識しております。

昨年、特定個人情報保護委員会から「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」が公表されたことを受け、CSAJはマイナンバーWGを編成し、ガイドラインの素案の段階から中小事業者への緩和措置拡大を中心に改善要望をする活動をしてまいりました。

また、行政当局と社会保険システム業界との窓口として、社会、経済の情報化に即応しつつ、ユーザの利便性の向上を図るとともに、社会保険届出書等の規格化、電子申請等の促進に貢献することにより、社会保険行政のICT化に寄与し、もって適正な電子申請制度の確立に努めることを目的として、「社会保険システム連絡協議会」を設立しました。

以上を踏まえ、このたび、マイナンバー対応ソフトウェアの対応範囲を“見える化”する評価シートを用意させて頂きました。

ガイドラインが要求する事項の内、必須事項、努力義務、対応が望ましい事項、の違いが明確になり、事業者様の判断に資するものと期待しております。

CSAJには国際規格であるISO/IEC 25051：2014に準拠したソフトウェアの品質認証制度（PSQ認証制度）がありますが、マイナンバー対応ソフトウェアについても、PSQ認証を準用した認証制度をご利用頂けるように、この評価シートを設計しております。

2015年10月以降、通知カードが各個人に届き、事業者様もマイナンバー対応を開始することになりますが、この評価シートがそのお役にたてますことを期待しております。

政策委員会／マイナンバーWG 主査 水谷 学
(ピー・シー・エー株式会社 代表取締役社長 公認会計士)

マイナンバー制度は、いよいよ本年10月より通知が開始され、2016年1月から運用が開始されます。制度の認知が進むにつれて、給与計算ソフトやセキュリティソフトなど様々な分野でマイナンバー対応を謳うものが目に付くようになってきました。

ソフトウェア業界として、当然のことながら、マイナンバー制度で要求されている事項について対応することになりますが、ソフトウェアで対応できる部分は一部に過ぎません。例えば「マイナンバーの保管」、「データの暗号化」や「パスワード設定」といった技術的な措置はソフトウェアの得意分野であり、当然に対応されることになります。一方でマイナンバー制度では「個人番号漏えい防止のための組織体制の整備」、「安全管理に関する取扱規程等の策定」のように組織の制度設計部分についても要求されており、これらの事項に関しては事業者自らが行っていくことになります。

このようにソフトウェアを導入しただけでは必ずしもマイナンバー制度に対応したとは言えず、事業者が、ソフトウェアで対応している事項、そして自らが対応しなければならない事項について把握する必要があります。しかしながらマイナンバー制度で要求されている事項を正確に理解して、これら事項の洗い出しを行うには高い専門知識と多くの労力を要します。

こういった背景から、ソフトウェアを提供する側の責任として、単にソフトウェアを提供するだけに終わらず、事業者としての対応を整えるための情報提供も行うことが必要であると考え、CSAJ政策委員会/マイナンバーWGを組成し、ソフトウェアを利用して安心してマイナンバー制度への対応を進めていただくために「マイナンバー対応評価シート」を策定することといたしました。ソフトウェアベンダがこの評価シートを活用し、自社で提供しているソフトウェアを評価することで、事業者の皆さまの円滑なマイナンバー制度の運用設計のお役に立てることを切に願っております。

政策委員会/マイナンバーWG 副主査 岡本 浩一郎
(弥生株式会社 代表取締役社長)

2

評価シートの利用方法



作成主体

本報告書及び評価シートは、特定個人情報保護委員会が平成26年12月11日に公表しました「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」をもとに、CSAJ政策委員会／マイナンバーWGにて議論・検討を行い、作成したものです。



目的

- 本評価シートは、ソフトウェアベンダが事業者向けに自社ソフトウェアのマイナンバー対応範囲を説明する際に利用できるよう作成しました。「メーカー個別対応機能」の欄に、自社ソフトウェアで対応できる内容を記載し、ご活用ください。但し、金融機関、行政機関向けには対応していませんので、利用できません。
- 個人番号の取り扱いを中心に、取得、保管、利用、提供、廃棄及び安全管理措置（組織的、人的、物理的、技術的）という事業者が取り扱う流れに沿って、分かりやすくまとめています。
- なお、CSAJ では本評価シートを用いた機能実装の第三者認証も実施します。自社製品のマイナンバー対応をPRする際にぜひご利用ください。



対象

原則で求められている事業者を念頭に作成しています。中小規模事業者（事業者のうち従業員の数が100人以下の事業者）にもご活用いただけますが、中小規模事業者への対応方法は、特定個人情報の適正な取扱いに関するガイドライン（事業者編）に、特例的な対応方法が示されているものもありますので、そちらもご参考ください。



評価シートの利用にあたって

- 本評価シートの情報は、本評価シートに記載の作成日付時点の情報であり、ご参照いただく時点の情報とは異なる可能性がありますので、ご注意ください。
- 本報告書及び評価シートは、特定個人情報保護委員会の承認を受けたものではなく、CSAJ政策委員会／マイナンバーWGとして、内容の正確性及び完全性に関して保証及び責任を負うものではありませんので、ご注意ください。



用語説明

▶ ガイド

「特定個人情報の適正な取扱いに関するガイドライン（事業者編）（本文及び（別添）特定個人情報に関する安全管理措置）事業者編」のことであり、別添資料である安全管理措置も含む。

▶ 保護法

「個人情報の保護に関する法律」を指す。

▶ 業務ソフト

個人番号情報を保管、利用が可能なソフトウェアやサービス

▶ 支援ソフト

個人番号情報自体は取り扱わないが、マイナンバー事務作業を支援するソフトウェアやサービス



評価シート項目説明

▶ No.

管理用の番号

▶ 番号管理区分

ガイドラインに記載されている内容を元に、「取得」「保管」「利用」「提供」「開示・訂正・利用停止」「廃棄・削除」「安全管理措置」「安全管理措置（組織的）」「安全管理措置（人的）」「安全管理措置（物理的）」「安全管理措置（技術的）」、11項目の区分に分類。

▶ 参照先

ガイドラインや個人情報保護法の参照先を記載。

▶ 項目

ガイドラインや個人情報保護法に記載されている項目。

▶ 概要

ガイドラインや個人情報保護法に記載されている項目の内容。

▶ 必須

ガイドラインに記載されている「しなければならない」は「◎」、「望ましい」は「-」、保護法の「努めなければならない」は「○」で分類。

▶ 該当者

項目の対象となる該当者を「個人情報取扱事業者」「全事業者」の2種に区分。

▶ 事業者対応

各項目による事業者の対応方法を具体的に記載。

▶ 業務ソフト要否

「業務ソフト」において、基本的に対応機能を有している必要がある項目を「○」にて記載。

▶ 業務ソフト基本対応機能

「業務ソフト」で対応すべき必要最低限の機能を記載。

▶ メーカー個別対応機能

「業務ソフト」および「支援ソフト」が対応する個別機能の参考例を記載

3 評価シート

作成日:平成 年 月 日 会社名:		対象製品: 対象区分: <input type="checkbox"/> 業務ソフトウェア <input type="checkbox"/> 支援ソフトウェア 適用範囲: <input type="checkbox"/> 取得 <input type="checkbox"/> 保管 <input type="checkbox"/> 利用 <input type="checkbox"/> 提供 <input type="checkbox"/> 廃棄/削除 <input type="checkbox"/> 安全管理措置			製品特徴: 製品価格: 製品紹介URL:			ソフト対応		
No.	番号管理区分	参照先	項目	概要	必須	該当者	事業者対応	ソフト対応		
								業務ソフト要否	業務ソフト基本対応機能	メーカー個別対応機能
1	取得	保護法第15条	個人情報の利用目的の特定	個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的をできる限り特定しなければならない。	◎	個人情報取扱事業者	・個人情報取扱事業者にあたる事業者は、従業員等の個人情報の取得に当たり、取扱規程等に利用目的の範囲を記載すること。 (個人番号の取り扱いについてはNo.4を参照)	-	-	
2	取得	保護法第17条	個人情報の適正な取得	個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。	◎	個人情報取扱事業者	・個人情報取扱事業者にあたる事業者は、従業員等の個人情報の取得に当たり、不正取得・不正使用・不正開示を行わないよう、取扱規程等に記載すること。	-	-	
3	取得	保護法第18条	個人情報の利用目的の通知等	個人情報取扱事業者は、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、本人に通知し、又は公表しなければならない。	◎	個人情報取扱事業者	・個人情報取扱事業者にあたる事業者は、従業員等に利用目的を公表せず個人情報を取得した場合は、速やかに利用目的を、本人に通知、または公表すること。	-	-	
4	取得	ガイド第4-3-(1)	個人番号の提供の要求	個人番号関係事務実施者又は個人番号利用事務実施者は、個人番号関係事務又は個人番号利用事務を処理するために必要がある場合に限り、本人又は他の個人番号関係事務実施者若しくは個人番号利用事務実施者に対して個人番号の提供を求めることができる。	◎	全事業者	・事業者は、従業員等の個人番号の取得に当たり、利用目的、取扱事務等の範囲を明確にした上で、個人番号の提供を求める対象者等を取扱規程等に記載すること。	-	-	
5	取得(提供)	ガイド第4-3-(2)	個人番号の提供の求めの制限	何人も、番号法第19条各号のいずれかに該当し特定個人情報の提供を受けることができる場合を除き、他人の個人番号の提供を求めてはならない。 他人とは「自己と同一の世帯に属する者以外の者」であり、子、配偶者等の自己と同一の世帯に属する者に対しては、同法第19条各号のいずれかに該当しなくても、個人番号の提供を求めることができる。	◎	全事業者	・事業者は番号法で限定的に明記された場合に限り(「番号法第19条各号」、個人番号の提供を求めること。	-	-	
6	取得	ガイド第4-3-(3)A	収集・保管制限(収集制限)	何人も、番号法第19条各号のいずれかに該当する場合を除き、他人の個人番号を含む特定個人情報を収集又は保管してはならない。	◎	全事業者	・事業者が特定個人情報の収集又は保管をおこなえるのは番号法で限定的に明記された場合に限られる。(「番号法第19条各号」)	-	-	・従業員の雇用区分等に応じて、個人番号の収集・保管の可否を設定できる機能 ・従業員ごとの利用目的を記録できる機能(税、社会保障、あるいは財形手続き等の利用目的を記録できる)。
7	取得	ガイド第4-3-(4)	本人確認の措置	本人確認については、番号法、番号法施行令、番号法施行規則及び個人番号利用事務実施者が認める方法に従うこととなるため、適切に対応する必要がある。	◎	全事業者	・事業者は以下の方法を参考に本人確認を行うこと。 -本人から個人番号の提供を受ける場合 1)個人番号カードの確認 2)通知カード+本人の身元確認書類の確認 3)番号確認書類+本人の身元確認書類の確認 など -本人の代理人から個人番号の提供を受ける場合 1)代理兼確認書類+代理人の身元確認書類+本人の番号確認書類 など	-	-	・本人確認を行った結果情報を保持、閲覧できる機能。
8	保管	保護法第19条	正確性の確保	個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。	○	個人情報取扱事業者	・個人情報取扱事業者にあたる事業者は、情報提供者本人からの修正・変更依頼に対して迅速に対応を行うこと。 また、正しい個人データを収集するために情報の正確性を確認すること。	○	○	・個人番号を含む特定個人情報に変更・相違があった場合に修正入力出来る機能を有すること ・正確性を確保できる機能を有すること ・チェックデジット ・その他機能
9	保管	保護法第24条	保有個人データに関する事項の公表等	個人情報取扱事業者は、保有個人データに関し、本人の知り得る状態に置かなければならない。	◎	個人情報取扱事業者	・個人情報取扱事業者にあたる事業者は以下の事項を本人の知り得る状態(ウェブ画面への掲載、パンフレットの配布、本人の求めに応じて遅滞なく回答を行うこと等、本人が知ろうとすれば、知ることができる状態)とする。 ・個人情報取扱事業者の氏名または名称 ・利用目的 ・開示などの手続きの方法と、それに伴う手数料 ・本人から開示請求があった場合、遅延なく開示すること。 ・本人から訂正要求があった場合、誤りがあった場合には応じること。 ・本人から利用目的外の利用や同意のない第三者提供について利用停止を求められた場合、応じること。	-	-	
10	保管	ガイド第4-3-(3)B	収集・保管制限(保管制限と廃棄)	個人番号は、番号法で限定的に明記された事務を処理するために収集又は保管されるものであるから、それらの事務を行う必要がある場合に限り特定個人情報を保管し続けることができる。また、個人番号が記載された書類等については、所管法令によって一定期間保存が義務付けられているものがあるが、これらの書類等に記載された個人番号については、その期間保管することとなる。	◎	全事業者	・事業者は番号法で限定的に明記された場合(「番号法第19条各号」参考情報Sheet参照)を除き、特定個人情報を保管しないこと。	○	○	・個人番号を保管できる機能を有すること ・入力された個人番号情報を保存する機能。

評価シート ver.1 (平成 27 年 7 月 31 日作成)

No.	番号管理区分	参照先	項目	概要	必須	該当者	事業者対応	ソフト対応		
								業務ソフト 要否	業務ソフト基本対応機能	メーカー個別対応機能
11	利用	保護法 第16条	利用目的による制限 ※番号法による読替及び適用除外あり	個人情報取扱事業者は、あらかじめ本人の同意を得ないで、利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。	◎	個人情報取扱事業者	・個人情報取扱事業者にあたる事業者は、あらかじめ本人の同意を得て利用目的の達成に必要な範囲内で個人情報を取り扱うこと。	-	-	・個人番号関係事務に関係しない処理にて、番号の表示/印刷ができない機能
12	利用	保護法 第18条第3項	利用目的の通知等	個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。	◎	個人情報取扱事業者	・個人情報取扱事業者にあたる事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表すること。	-	-	・就業規則(利用目的一覧含む)の出力機能
13	利用	ガイド 第4-1-(1)	個人番号の利用制限	個人番号を利用できる事務については、番号法によって限定的に定められており、事業者が個人番号を利用するのは、主として、源泉徴収票及び社会保障の申請書類に従業員等の個人番号を記載して行政機関等及び健康保険組合等に提出する場合である。 また、例外的な利用について、番号法は個人情報保護法に比べ、より限定的に定めている。事業者の場合、利用目的を超えて個人番号を利用することができるのは、①激甚災害が発生したとき等に金融機関が金銭の支払をするために個人番号を利用する場合及び②人の生命、身体又は財産の保護のために個人番号を利用する必要がある場合である。	◎	全事業者	事業者が個人番号を利用できるのは次の範囲で行政機関等及び健康保険組合等に提出する場合である。 ①源泉徴収票等 ②社会保障の申請書類等 例外的な利用について、利用目的を超えて個人番号を利用することができるのは以下の場合である。 ①激甚災害が発生したとき等に金融機関が金銭の支払をするために個人番号を利用する場合 ②人の生命、身体又は財産の保護のために個人番号を利用する必要がある場合	-	-	・個人番号を利用できない事務処理の場合は、個人番号(入力欄など含む)が表示されない機能
14	利用	ガイド 第4-1-(2)	特定個人情報ファイルの作成の制限	個人番号関係事務又は個人番号利用事務を処理するために必要な範囲に限って、特定個人情報ファイルを作成することができる。 従業員等の源泉徴収票作成事務、健康保険・厚生年金保険被保険者資格取得届作成事務等に限って、特定個人情報ファイルを作成することができるものであり、これらの場合を除き特定個人情報ファイルを作成してはならない。	◎	全事業者	事業者が特定個人情報ファイルを作成することができるのは以下の場合のみである。 ①従業員等の源泉徴収票作成事務 ②健康保険・厚生年金保険被保険者資格取得届作成事務等	-	-	
15	提供	保護法 第23条	第三者提供の制限 ※番号法では適用除外	個人情報取扱事業者は、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。	◎	個人情報取扱事業者	・個人情報取扱事業者にあたる事業者は、あらかじめ本人の同意を得ないで、個人データを第三者に提供をしないこと。	-	-	
16	提供	ガイド 第4-3-(2)	特定個人情報の提供制限	何人も、番号法で限定的に明記された場合を除き、特定個人情報を「提供」してはならない。	◎	全事業者	何人も、番号法で限定的に明記された場合を除き、特定個人情報を「提供」してはならない。	-	-	・グループ会社管理機能において、個人番号以外のマスター移動が可能な転籍・出向処理機能
17	開示 訂正 利用停止	保護法 第25条～第30条	開示、訂正等、利用停止等 ※利用停止等(第27条)は、[No.18]を参照	開示・訂正等に関しては、個人情報保護法の25・26・28・29・30条の内容を確認すること 個人情報保護法: 第25条(開示) 第26条(訂正等) 第28条(理由の説明) 第29条(開示等の求めに応じる手続) 第30条(手数料)	◎	個人情報取扱事業者	個人情報取扱事業者は個人情報保護法の25・26・28・29・30条の内容を確認し、対応をおこなうこと。	-	-	
18	開示 訂正 利用停止	ガイド 第4-4	第三者提供の停止に関する取扱い	特定個人情報を提供することができるのは、番号法第19条各号に当てはまる場合に限定されている。したがって、特定個人情報が違法に第三者に提供されていることを知った本人から、その提供の停止が求められた場合であって、その求めに理由があることが判明したときには、第三者への提供を停止しなければならない。 特定個人情報を適正に取り扱っていれば、第三者への提供の停止を求められる事態は生じない。	◎	全事業者	事業者は特定個人情報が違法に第三者に提供されていることを知った本人から、その提供の停止が求められた場合であって、その求めに理由があることが判明したときには、第三者への提供を停止すること。	-	-	
19	廃棄・削除	ガイド 第4-3-(3)B	収集・保管制限(保管制限と廃棄)	事務を処理する必要がなくなった場合で、所管法令において定められている保存期間を経過した場合には、個人番号をできるだけ速やかに廃棄又は削除しなければならない。 詳細は「安全管理措置No.34」を参照。	◎	全事業者	事業者は「安全管理措置No.34」を参照し、対応を行うこと。	-	-	
20	安全管理措置	ガイド 第4-2-(1)	委託の取扱い	・委託先において、番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。 ・「委託を受けた者」は、委託者の許諾を得た場合に限り、再委託を行うことができる。	◎	全事業者	○委託 委託先に対して必要かつ適切な監督を行うため、以下の3点の対策を行うこと。 ・委託先の適切な選定をおこなうため、「委託先の選定チェックリスト」等を作成する。 ・委託先に安全管理措置を遵守させるための必要な「委託契約書」等を作成し、締結する。 ・委託先における特定個人情報の取扱状況の把握をするため、確認項目を選定し、明文化すること。なお、確認項目に関しては「委託先の設備、技術水準、従業員に対する監督・教育の状況、その他委託先の経営環境等」を検討する。 ○再委託 ・再委託先が発生することを想定し、委託契約書等に事前許諾の取決めを記載する。また、再委託先、再々委託先以降の委託先についても委託先と同等の情報提供を要求できることを記載すること	-	-	

No.	番号管理区分	参照先	項目	概要	必須	該当者	事業者対応	ソフト対応		
								業務ソフト要否	業務ソフト基本対応機能	メーカー個別対応機能
21	安全管理措置	ガイド第4-2-(2)	安全管理措置	個人番号及び特定個人情報(以下「特定個人情報等」という。)の漏えい、滅失又は毀損の防止等、特定個人情報等の管理のために、必要かつ適切な安全管理措置を講じなければならない。詳細は安全管理措置No.22-38を参照。	◎	全事業者	事業者は「安全管理措置No.22-38」を参照し、対応を行うこと。	-	-	
22	安全管理措置	ガイド別添2四	基本方針の策定	特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。	-	全事業者	特定個人情報等の適正な取扱いの確保について組織として取り組むための「特定個人情報基本方針」等を策定する。 記載する項目は手法の例示事項である次の4点等を検討する ・事業者の名称 ・関係法令・ガイドライン等の遵守 ・安全管理措置に関する事項 ・質問および苦情処理の窓口	-	-	
23	安全管理措置	ガイド別添2四	取扱規程等の策定	ガイド別添「1」安全管理措置の検討手順A～C)で明確化した事務において事務の流れを整理し、特定個人情報等の具体的な取扱いを定める取扱規程等を策定しなければならない。	◎	全事業者	「特定個人情報取扱規程」を策定するにあたり、①取得、②利用、③保存、④提供、⑤削除・廃棄の管理毎に次の3点を盛り込む ・個人番号を取り扱う事務の範囲の明確化 ・特定個人情報等の範囲の明確化 ・事務取扱担当者の明確化 また、組織的・人的・物理的・技術的安全管理措置についての対応も記載すること。	-	-	
24	安全管理措置(組織的)	ガイド別添2四a	組織体制の整備	安全管理措置を講ずるための組織体制を整備する。	◎	全事業者	安全管理措置を講ずるための組織体制を「特定個人情報取扱規程」等に記載する。記載する項目は手法の例示を参考に以下の点を記載する。 ・事務における責任者の設置及び責任の明確化 ・事務取扱担当者の明確化及びその役割の明確化 ・事務取扱担当者が取り扱う特定個人情報等の範囲の明確化 ・事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制 ・情報漏えい等事案の発生又は兆候を把握した場合の従業者から責任者等への報告連絡体制 ・特定個人情報を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化	-	-	
25	安全管理措置(組織的)	ガイド別添2四b	取扱規程等に基づく運用	取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する。	◎	全事業者	取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する。 記載する項目は手法の例示を参照すること。 ・特定個人情報ファイルの利用・出力状況の記録 ・書類・媒体等の持出しの記録 ・特定個人情報ファイルの削除・廃棄記録 ・削除・廃棄を委託した場合、これを証明する記録等 ・特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況(ログイン実績、アクセスログ等)の記録	○	・システムログ又は利用実績を記録する機能を有すること。 ・記載する項目は以下のいずれかもしくは複数の内容を含むこと。 ・特定個人情報ファイルの利用・出力状況の記録 ・特定個人情報ファイルの削除・廃棄記録 ・事務取扱担当者の情報システムの利用状況(ログイン実績、アクセスログ等)の記録 ・その他適切な内容	・システム操作ログ、個人番号操作ログを自動記録する機能
26	安全管理措置(組織的)	ガイド別添2四c	取扱状況を確認する手段の整備	特定個人情報ファイルの取扱状況を確認するための手段を整備する。 なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。	◎	全事業者	特定個人情報ファイルの取扱状況を確認するための手段を整備する。 取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録し、照会できるようにする。 記載する項目は手法の例示を参照すること。 ・特定個人情報ファイルの種類、名称 ・責任者、取扱部署 ・利用目的 ・削除・廃棄状況 ・アクセス権を有する者 なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。	○	・記録されたシステムログを開覧することができる機能を有すること	・記録されたシステムログの検索、削除、出力できる機能 ・特定個人情報ファイルへのアクセス可能なIDのリスト出力機能
27	安全管理措置(組織的)	ガイド別添2四d	情報漏えい等事案に対する体制の整備	情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する。 情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。	◎	全事業者	情報漏えい等の事案の発生時に、次のような対応を行うことを念頭に、体制を整備する。 ・事実関係の調査及び原因の究明 ・影響を受ける可能性のある本人への連絡 ・委員会及び主務大臣等への報告 ・再発防止策の検討及び決定 ・事実関係及び再発防止策等の公表	-	-	
28	安全管理措置(組織的)	ガイド別添2四e	取扱状況の把握及び安全管理措置の見直し	特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組む。	◎	全事業者	手法の例示を参考にし、次の2点の対応を検討する。 * 特定個人情報等の取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。 * 外部の主体による他の監査活動と合わせて、監査を実施することも考えられる。	-	-	・監査支援資料として、指定期間でのログ統計情報を出力する機能
29	安全管理措置(人的)	ガイド別添2四a	事務取扱担当者の監督	事業者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。	◎	全事業者	特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。	-	-	
30	安全管理措置(人的)	ガイド別添2四b	事務取扱担当者の教育	事業者は、事務取扱担当者に、特定個人情報等の適正な取扱いを周知徹底するとともに適切な教育を行う。	◎	全事業者	事務取扱担当者に、特定個人情報等の適正な取扱いを周知徹底するとともに適切な教育を行う。 * 従業者に定期的な研修等を行う * 秘密保持に関する事項を就業規則等に盛り込む	-	-	

No.	番号管理区分	参照先	項目	概要	必須	該当者	事業者対応	ソフト対応		
								業務ソフト要否	業務ソフト基本対応機能	メーカー個別対応機能
31	安全管理措置 (物理的)	ガイド別添[2]Eh	特定個人情報等を取り扱う区域の管理	特定個人情報等の情報漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域(以下「管理区域」という。)及び特定個人情報等を取り扱う事務を実施する区域(以下「取扱区域」という。)を明確にし、物理的な安全管理措置を講ずる。	◎	全事業者	特定個人情報ファイルを取り扱う管理区域及び特定個人情報等を取り扱う事務を実施する取扱区域を明確にする。 対応内容については手法の例示を参考にする。 * 管理区域への対策-入室管理及び管理区域へ持ち込む機器等の制限等。 * 入室管理方法-ICカード、ナンバーキー等による入室管理システムの設置等。 * 取扱区域への対策-壁又は間仕切り等の設置及び座席配置等。	-	-	・盗み見対策として、入力された番号をマスク表示する機能
32	安全管理措置 (物理的)	ガイド別添[2]Eh	機器及び電子媒体等の盗難等の防止	管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。	◎	全事業者	管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。 対応内容については手法の例示を参考にする。 * 特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット・書庫等に保管する。 * 特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定する。	-	-	
33	安全管理措置 (物理的)	ガイド別添[2]Eh	電子媒体等を持ち出す場合の漏えい等の防止	特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等、安全な方策を講ずる。 「持出し」とは、特定個人情報等を、管理区域又は取扱区域の外へ移動させることをいい、事業所内での移動等であっても、紛失・盗難等に留意する必要がある。	◎	全事業者	特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等、安全な方策を講ずる。 * 電子媒体の場合-持出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等。 * 書類の場合-封緘、目隠しシールの貼付を行うこと等。	-	-	・データの暗号化 ・パスワードによる保護 ・その他適切な保護
34	安全管理措置 (物理的)	ガイド別添[2]Eh	個人番号の削除、機器及び電子媒体等の廃棄	個人番号関係事務又は個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、個人番号をできるだけ速やかに復元できない手段で削除又は廃棄する。 →ガイドライン第4-3-(3)B「保管制限と廃棄」参照 個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。	◎	全事業者	個人番号関係事務又は個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、個人番号をできるだけ速やかに復元できない手段で削除又は廃棄する。 * 書類等を廃棄する場合、焼却又は溶解等の復元不可能な手段を採用。 * 機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用。 * 特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合、容易に復元できない手段を採用。 * 保存期間経過後における個人番号の削除を前提とした情報システムを構築する。 * 個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定める。 * OSのゴミ箱中に個人番号が残らないよう削除する。	○	○	・個人番号の削除について次の要件を満たしていること ・保存期間経過後の個人番号を復元できない手段で削除ができる機能を有すること ・個人番号を削除をした場合には削除した記録を保存できる機能を有すること
35	安全管理措置 (技術的)	ガイド別添[2]Eh	アクセス制御	情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。	◎	全事業者	適切なアクセス制御を行う方法としては、手法の例示にある3点をすべて考慮する。 ・個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定 ・特定個人情報ファイルを取り扱う情報システムを、アクセス制御により限定する。 ・ユーザーIDに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する	○	○	・特定個人情報ファイルを取り扱える(閲覧、登録、利用、削除)事務取扱担当者の登録機能を有すること ・アクセス権限のレベルを設定できる機能 ↳ 閲覧、登録、利用、削除 ↳ 業務の範囲(社保、年調など)
36	安全管理措置 (技術的)	ガイド別添[2]Eh	アクセス者の識別と認証	特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する。	◎	全事業者	特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する。具体的な方法としては手法の例示に記載のある次のいずれか、または組み合わせによる手法を選択する。 ユーザーID パスワード 磁気・ICカード その他適切な手法	○	○	・以下のいずれかまたは組み合わせの方法で事務取扱担当者を識別する機能を有すること ・ユーザーID ・パスワード ・磁気/ICカード ・生体認証 ・その他識別できる方法
37	安全管理措置 (技術的)	ガイド別添[2]Eh	外部からの不正アクセス等の防止	情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。	◎	全事業者	手法の例示にある①②を参考にし、情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入する。また、③④⑤を参考にし、適切な運用を実施する。 ①ファイアウォール等を設置し、不正アクセスを遮断する ②セキュリティ対策ソフトウェア等(ウイルス対策ソフトウェア等)を導入する ③入出力データにおける不正ソフトウェアの有無を確認する。 ④機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする ⑤ログ等の分析を定期的に行い、不正アクセス等を検知する	-	-	・入出力データにおける不正ソフトウェアの有無を確認できる機能 ・ソフトウェアを最新状態に保てる自動更新機能 ・不正アクセス等を検知するためのログ機能
38	安全管理措置 (技術的)	ガイド別添[2]Eh	情報漏えい等の防止	特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。	◎	全事業者	特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。 ①通信経路の暗号化等 ②データの暗号化又はパスワードによる保護等	○	○	・インターネットを通じた送受信データを暗号/保護する機能 ・エクスポートデータをパスワード/暗号化する機能

4

参考情報

- ▶ 特定個人情報の適正な取扱いに関するガイドライン(事業者編)
(本文及び(別添)特定個人情報に関する安全管理措置)
<http://www.ppc.go.jp/files/pdf/261211guideline2.pdf>
- ▶ 個人情報の保護に関する法律(個人情報保護法)
<http://law.e-gov.go.jp/htmldata/H15/H15HO057.html>
- ▶ 行政手続における特定の個人を識別するための番号の利用等に関する法律(番号法)
<http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/260717bangouhou.pdf>

5

WGメンバー一覧

主査	水谷 学	ピー・シー・エー株式会社 代表取締役社長
副主査	岡本 浩一郎	弥生株式会社 代表取締役社長
メンバー	日野 和麻呂	株式会社オービックビジネスコンサルタント 開発部 部長
	// 山崎 真一	株式会社オービックビジネスコンサルタント 開発部 次長
	// 岸川 剛	応研株式会社 取締役営業部長
	// 中島 隆	応研株式会社 開発部 給与プロジェクト
	// 保倉 豊	グローバルフレンドシップ株式会社 代表取締役社長
	// 大口 鉄雄	ソリマチ株式会社 農業情報事業部 農業情報開発部 課長
	// 大崎 孝志	ソリマチ株式会社 SMB事業部 SMB開発部 開発2課 課長
	// 外処 幸樹	東京システムハウス株式会社 システムソリューション部 部長
	// 田邨 公伸	ピー・シー・エー株式会社 戦略企画部 課長代理
	// 林 和彦	ピー・シー・エー株式会社 システム開発部 課長代理
	// 菊池 龍信	弥生株式会社 マーケティング本部マーケティング部 ビジネス戦略チーム・担当マネージャー
	// 北原 佳郎	ラクラス株式会社 代表取締役社長
	// 伊藤 秀也	株式会社ワークスアプリケーションズ HR Div ゼネラルマネージャー
	// 橋本 文雄	株式会社ワークスアプリケーションズ HR Div
事務局	戸島 拓生	一般社団法人コンピュータソフトウェア協会 業務課 係長

※敬称略、メンバー社名五十音順

※部署・役職は平成27年7月時点

**マイナンバー対応ソフトウェアの対応範囲
を“見える化”する評価シート**

2015年7月31日 第1版



Computer Software Association of Japan
一般社団法人コンピュータソフトウェア協会

政策委員会／マイナンバーWG

〒107-0052 東京都港区赤坂1-3-6
赤坂グレースビル4F

TEL : 03-3560-8440 FAX : 03-3560-8441
<http://www.csaj.jp/>