

マイナンバー情報セキュリティ対策 ポータルについて

マイナンバー対応情報セキュリティ検討WG

WGサブリーダー

松森 健一

(デジタルアーツ株式会社)

1. マイナンバーの動向
2. 本WGの目的と取り組み
3. 成果物の概要
 - マイナンバー対応のための公的情報
 - マイナンバー業務プロセス・分析シート
 - マイナンバーの安全間措置チェックシート

1. マイナンバーの動向

マイナンバー制度とは



2016年1月から、社会保障、税、災害対策における行政事務にマイナンバーが利用される制度

【番号法の改正】

- 平成27年9月3日成立
- 金融分野、医療分野等における利用範囲の拡充
 - 預貯金口座
 - 特定健康診査
 - 予防接種記録 等

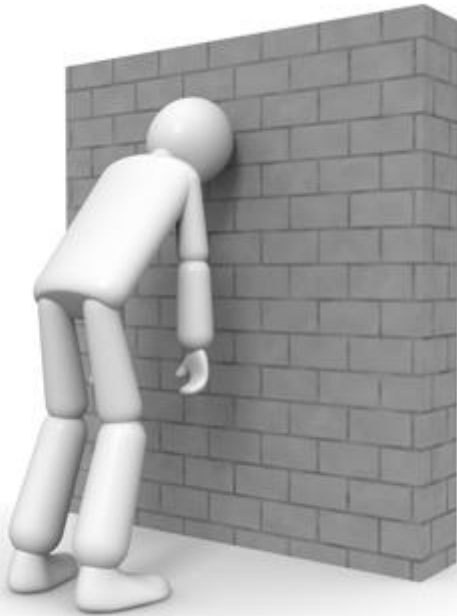
資料6



2. 本WGの目的と取り組み

マイナンバー制度に対して、企業がどのような準備を行えばよいのか、また現在行っている準備が適当なのか等、現場の拠り所となる成果物を目指し、検討・作成を行うこと。

マイナンバー対応の壁



①情報収集の壁

- 発信される情報ソースが複数
- 情報量が多量、集め切れない、読みきれない

②プロセス・体制構築の壁

- 業務がどう変わる？
- 社内の体制はどうすべき？

③安全管理措置の壁

- ガイドラインの安全管理措置、どこまでやればいいのか？

「壁」への対応を検討(サブWG) **JNSA**

①情報収集の壁

情報集約チーム

- ・リーダー: 根津 研介 (NTTデータ先端技術)
- ・サブ: 富田高樹 (みずほ情報総研)

②プロセス・体制構築の壁

構築検討チーム

- ・リーダー: 松森健一 (デジタルアーツ)
- ・サブ: 持田啓司 (大塚商会)

③安全管理措置の壁

情報セキュリティチーム

- ・リーダー: 工藤雄大 (大日本印刷)
- ・サブ: 古川勝也 (SecureWorks Japan)

主な活動

5月 発足検討会

6月 WG発足

7～9月 各WGにて検討・
成果物完成

10月 セミナー開催



監督省庁を招いてのセミナー



2015年10月5日 JNSA主催セミナー

「待ったなし！マイナンバーの取扱と安全管理～監督省庁の実務担当者に聞く～」



国税庁
厚労省
特定個人情報保護委員会

+

サブWGより成果物発表

満員御礼！
(180名)

3.成果物の概要

- マイナンバー対応のための公的情報
- マイナンバー業務プロセス・分析シート
- マイナンバーの安全間措置チェックシート

マイナンバー制度開始に伴う企業の対策を支援

- 「マイナンバー対応のための公的情報リンク集」
- 「マイナンバーの取得から廃棄までの業務プロセスのリスク分析シート」
- 「マイナンバーの安全管理措置チェックリスト」



特定非営利活動法人日本ネットワークセキュリティ協会

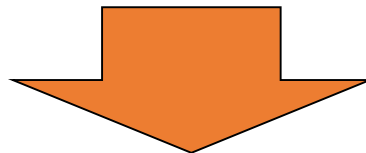
マイナンバー対応のための情報ポータル(企業向け)

<http://www.jnsa.org/mynumber/info.html>

情報集約チーム

「マイナンバー対応のための公的情報リンク集」

- マイナンバー対応情報が各担当官庁や個人情報保護委員会に分散している。
- 中央省庁、地方自治体、大中企業、小企業で見るところや観点が異なり、提供されているガイドラインにも違いがあり、情報錯綜のもと。
- 各官庁ごとに進捗状況に差がある。



**企業のマイナンバー担当が
一元的に情報収集できるポータルページを提供**

情報ポータル参照

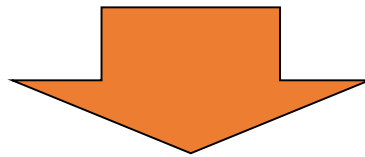
<http://www.jnsa.org/mynumber/info.html>

構築検討チーム

「マイナンバーの取得から廃棄までの
業務プロセスのリスク分析シート」

構築検討チームの目的

- 規模の大小を問わず、全ての企業がマイナンバーを取り扱うことになる。
- 情報漏洩及び個人情報の不正利用に関して、国民の懸念は強い。
- 本ワーキンググループ発足時点(2015年6月)では、民間企業のマイナンバー対策はほぼ進捗無し。



民間企業がマイナンバーを取り扱うにあたり、その**リスクを理解し、自社に適した対策を打つためのガイド**を提供する

業務のパターンごとに、想定されるリスク・懸念点を洗い出し、対応方法を検討

1. ファイル管理

- Excel等のデジタルファイルで管理

2. システム管理

- 人事給与パッケージ等のシステムを利用

3. クラウドサービス

- 業者が提供する「マイナンバー収集・保管クラウドサービス」を利用

4. 紙媒体での管理

- 紙媒体で管理

管理プロセス例（自社中心）



プロセス	例1	例2	例3	例4
取得	紙	・紙 ・表計算ソフト等に入力	・紙 ・専用フォーム 等	
保管	・紙をファイリング ・金庫等で保管する	・表計算ソフト等で管理する ・パスワードをかけて保管	自社のサーバで保管する(人事給与のPKGを使用)	クラウドサービスを活用する
利用	利用時に金庫から出して利用する	利用時にファイルを開いて利用する	利用時にアクセスして利用する	
提供	各種申告、届出等で提供する			
開示・訂正・利用停止	-			
廃棄	シュレッダーで廃棄する	ファイルを更新し、古いファイルは廃棄	管理サーバ上から削除する	

管理プロセス例（委託中心）

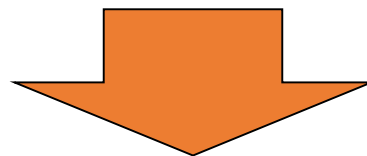


プロセス	例5	例6	例7
取得	紙や専用フォーム等で収集する	<u>収集代行サービスの利用</u>	<u>収集代行サービスの利用</u>
保管	<u>保管サービス等の活用</u>	<u>保管サービス等の活用</u>	<u>保管サービス等の活用</u>
利用	利用時にアクセスして利用する		<u>利用代行サービス等の利用</u>
提供	各種申告、届出等で提供する		
開示・訂正 ・利用停止	－		
廃棄	保管サービス等に含む（廃棄証明）		

3.クラウド サービス

<WGで上がった留意事項>

- クラウドサービスは業務委託に該当するのか？
- もしサービス業者から情報漏洩があった場合、誰が責任を取るのか？
- 適用されるのはどの法律？（特に海外のクラウドサービスの場合）
- マイナンバーの「廃棄」まで適切に処理してくれるのか？



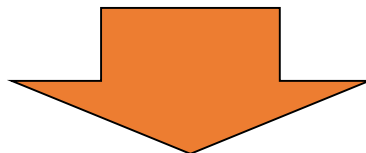
<ポイント>

サービス内容、責任範囲をしっかりと理解したうえで利用すること。
（規約の確認、万が一の場合の対応方法など）

業者に委託

<WGで上がった留意事項>

- 業者に委託するのは良いが、委託先の管理責任は自社にあることを認識すべき。
※社労士・税理士など、受託者側では危機感を持っているところも。
業者によって管理レベルはまちまち。
- 収集を自社で行う場合は、業者にマイナンバーを渡すまでのリスクを考える必要がある。



<ポイント>

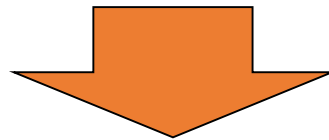
ガイドラインに基づき、業者の選定を行ったうえで、業者とのマイナンバー取扱いプロセスの構築を行うこと。

自社でマイナンバーを扱うプロセスにおいては、対策が必要。

情報セキュリティ検討チーム

「マイナンバーの安全管理措置チェックリスト

- 個人情報保護委員会は、番号法に基づき適正な取扱いに必要な措置を求めている。
- 対象は事業者の別を問わず、個人番号を取り扱う全ての者に適用される。
- 罰則、提供/収集等の制限が厳しく、どこまで対策を取ればいいのか分からない。



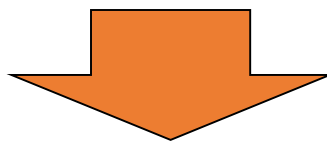
民間企業がマイナンバーを取り扱うにあたり、
「どこまでセキュリティ対策を取ればいいのか？」
に答えるべくチェックシートを提供する。

WGでの検討事項

- 主なソリューションと留意点

<WGで上がった留意事項>

- 会社規模により、措置策を変える必要があるか？
 - ⇒ 会社規模によりセキュリティを下げることはできない。
 - ⇒ 「最低限取るべき措置」と「オプションとして取るべき措置」に分けチェックリストを作成する。
- 措置策の記載だけでは、分かりにくくないか？
 - ⇒ コメントを付与し、理解できる様にサポート



<ポイント>

マイナンバーを扱う全ての事業者が理解し、セルフチェックによりどの措置が不足しているかを洗い出せるチェックシートとする。

チェックシート イメージ



組織的（43項目）/人的（7項目）/物理的（16項目）/技術的（24項目）毎に作成

マイナンバーの安全管理措置チェックシート Ver.1(2015/9/18)					
C 組織的安全管理措置 ※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）を参照ください。（ http://www.ppc.go.jp/files/pdf/261211guideline2.pdf ）					
P51 事業者は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。					
a 組織体制の整備					
P51 安全管理措置を講ずるための組織体制を整備する。					
最低限取るべき措置		コメント	プラスα (オプションとして取るべき措置)		コメント
1	【前提条件】事業者は、安全管理措置を講ずるための取扱規程等を作成する。	☐			☐
2	事務における責任者の配置および責任と権限を明確にする。	☐	②	個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（CPO））を配置する。	☐
3	監督責任者を配置する。	☐	③	特定個人情報管理者の任命および「特定個人情報の利用者の識別および認証」として「本人確認に関する情報」の管理者を任命する。	☐
4	特定個人情報を取扱う情報システム運用責任者の配置および担当者（システム管理者を含む）を限定する。	☐	④	特定個人情報の安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定める。	☐
5	事務取扱担当者の明確化およびその役割を明確にする。	☐	⑤	事務取扱担当者が複数いる場合、責任者と事務取扱担当者を区分する。	☐
6	個人番号関係事務担当者の明確化のために部所名（〇〇課、△△係）、事務名（××事務担当者）等を定める。	☐			☐
7	特定個人情報の取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の配置および作業担当者を限定する。	☐			☐
8	事務取扱担当者が取り扱う特定個人情報の範囲の明確にする。	☐			☐
9	個人番号関係事務の範囲を明確にする。	☐			☐
10	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を整備する。	☐			☐
11	特定個人情報の取扱いに関する規程等に違反している事実、又は兆候があることに気づいた場合、代表者等への報告連絡体制を整備する。	☐		おかしいなと感じたら直ぐ窓口（社内担当者や弁護士等専門家）へ連絡・相談することが重要。	☐
12	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を整備し、周知する。	☐			☐

最低限対応頂きたい項目

できればここまで考慮頂きたい項目

組織的安全管理措置

～a.組織体制の整備(抜粋)～

最低限取るべき措置		プラスα (オプションとして取るべき措置)	
3	事務における責任者の設置および 責任と権限を明確にする 。	③	個人情報保護管理者 (いわゆる、チーフ・プライバシー・オフィサー(CPO))を設置する。
4	監査責任者 を設置する。	④	特定個人情報管理者の任命 および「特定個人情報の利用者の識別および認証」として「 本人確認に関する情報 」の 管理者を任命 する。
5	特定個人情報を取扱う 情報システム運用責任者の設置 および 担当者 (システム管理者を含む)を 限定 する。	⑤	特定個人情報の安全管理に関する従業者の役割・責任を 職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書 等に具体的に定める。

人的安全管理措置 ～b.事務取扱担当者の教育(抜粋)～



最低限取るべき措置		プラスα (オプションとして取るべき措置)	
1	事務取扱担当者へ内部規程・手順書等の周知、教育・訓練を実施する。	①	関与する者の役割と責任を定めた内部規程等について周知徹底をする。
2	全従業員へマイナンバーを収集する範囲・利用目的等を周知し、2015年10月以降に通知カードが届いた後の対応(収集等の手順等)について教育をする。	②	事務取扱担当者以外のシステム(DB)管理者や関連従事者へも内部規程等の周知と教育・訓練を実施する。
3	新入社員・中途社員の入社時にマイナンバーを収集できる仕組み作り(運用手順書・マニュアル整備など)と入社時教育(安全管理に関する内容も含む)を行う。	③	教育・訓練を定期的に計画し、実施する。
4	全従業員へマイナンバーに限らず個人情報漏洩事件が起きた際の事業者への影響等を周知、教育する。	④	関与する者の教育実施記録、教育受講記録を取り、適切なフォローや見直しを実施する。(評価分析や力量管理など) マイナンバー法のみならず、個人情報保護法の内容についても周知、教育を行う。

技術的安全管理措置

～c.外部からの不正アクセス等の防止(抜粋)～



最低限取るべき措置		プラスα (オプションとして取るべき措置)	
2	利用している ソフトウェアを最新状態にする よう努める。	②	脆弱性情報を Push通知 で受け取れる仕組みを導入し、素早く脆弱性を認知、対応する(脆弱性情報提供サービスの利用)
3	セキュリティ対策製品を最新状態にする よう努める。	③	OS、利用機器、ソフトウェアの IT資産管理を自動化 するシステムを利用し、更新プログラムの確実な自動適用や許可しないソフトウェア・サービスの導入防止、運用ポリシーに沿わない端末のアクセスを許可しない等の措置を講じる。 自動更新が望ましいが、 難しい場合は運用フローを策定し、定期的な見直し を実施する
		④	システムに対し定期的な脆弱性診断を実施し、対策を講じることでセキュリティ侵害のリスクを軽減する。

物理的安全管理措置

～d.個人番号の削除、機器及び電子媒体等の廃棄～



最低限取るべき措置

①	書類、メディア等の廃棄は シュレッダー、焼却または溶解等の復元不可能な手段 を用いる。
②	廃棄管理記録簿による、 削除または廃棄の記録(委託の場合は証明書) 作成(取得)、保管をする。
③	電子データの廃棄時は、 復元不可能な専用の削除ソフトウェア 等を利用する。外部記憶装置自体の廃棄時は、装置そのものにデータの復元が不可能な物理的破壊を行う。
④	特定個人情報から一定の保存期間経過後に個人番号が削除される前提での情報処理システム、管理マニュアルを作成する。
⑤	個人番号が記載された書類が一定の保存期間経過後に廃棄される前提での保管手続きを作成する。

プラスα(オプションとして取るべき措置)

a)	シュレッダーはDIN規格レベル6以上など、 復元が極めて困難な製品 を使用する。
----	---

ご静聴ありがとうございました。