マイナンバー業務プロセス・リスク分析シート

マイナンバー対応情報セキュリティ検討 WG
構築検討チーム

多くの企業はマイナンバーの漏洩をリスクと考え、対策を打つ必要があると感じています。しかし、「具体的に、業務上のどこにどのようなリスクがあるのか」というところまでは検討が出来ておらず、「どのような手を打てば良いのか？」というところで止まってしまっているのが実態です。

そこで、JNSA マイナンバー対応情報セキュリティ検討 WG では、企業のみなさまに活用していただけるよう「マイナンバー業務プロセス・リスク分析シート」を作成・公開しました。

◆「マイナンバー業務プロセス・リスク分析シート」の概要

○　マイナンバーの管理の為に利用するツールの視点から、マイナンバー取扱業務（収集・保管・利用・提供・廃棄）を特定の業務パターンに集約しました。各企業のマイナンバー取扱業務プロセスは、細かい点は差異はあれども、いずれかの業務パターンに分類できると考えます。

○　各業務パターンについて、どういった情報漏洩リスクや運用上の留意点があるのかを分析・整理し、想定される対応策を明確化致しました。

○　本成果物によって業務に潜むリスク・留意点が可視化され、自社にとって最適な業務プロセスの選択と構築、また、不足している対策の発見などの為、ご利用頂けると考えております。

マイナンバー業務プロセス・リスク分析シート」は、業務パターン別に「業務プロセスにおける懸念点」を整理し、各懸念点に対応する形で「対策例」を記載しています。
ぜひ組織内でのマイナンバー取扱プロセスの構築の為にご活用いただければ幸いです。また、既にプロセスを構築済の企業様におかれましては、当該プロセスにおけるリスク分析・レビューの為にご活用ください。

※なお、本成果物は、平成 26 年 12 月 11 日付「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）」に基づき作成しております。

以上

【マイナンバー 業務プロセス･リスク分析（収集プロセス）】

Version 1.0：2015/9/15

業務範囲	･事業者が、社員（及びその扶養家族）や個人支払先からマイナンバーを受領し、本人確認を通して、正しいマイナンバーを取得するまでのプロセス。 ･前提事項として、マイナンバーを提供する各個人が、自分のマイナンバーを正しく認識していること。

業務パターン			業務プロセス			業務プロセスにおける懸念点	対策例 ※【】内は該当する安全管理措置のカテゴリ
	パターン	概要	No.	主体	業務		
	【前提】	-	-	マイナンバー提供者	･マイナンバー提供者が、自らのマイナンバーを適切に保管する	①個人番号通知カードの紛失/誤って処分 ②住民票住所と実際の居住地が異なっており、個人番号通知カードを受領出来ていない ※例えば住民票の住所を移さないまま、特別養護老人ホームなどの施設に入居している高齢者など。また、そういった人が扶養家族である場合も考えられる。	①【人的】社員への教育（取扱担当者に限らず、社員･パート等、全体への教育） ※マイナンバー発行の基準日までに住民票を適切な住所に移動しておくこと。 ②会社での一括収集
A	電子ファイル	･電子ファイルにマイナンバーを記入し、受渡しを行う。 ※例えば、支社店等、遠隔地からマイナンバーを収集する場合など	1	マイナンバー管理者（本社）	･本社のマイナンバー管理者（人事部等）がマイナンバーの記入フォームを作成し、各部署の取り纏め担当者（組織長等）に配布		
			2	マイナンバー管理者（本社）	･マイナンバー（個人番号通知カード等）及び本人確認書類を持参し、各部署の取り纏め担当者に提示	①個人番号通知カード/個人番号カードの紛失 ②盗難等による不正取得 ③マイナンバー提供者による提示の拒否	①【人的】社員への教育（事務取扱担当者に限らず、社員･パート等、全体への教育） ②マイナンバー提供者が提示を拒否した場合は、書類提出先の機関の指示に従う。
			3	マイナンバー管理者（各部署）	･部署員の本人確認を行ったうえで、フォームに記入 ･本人確認の方法と本人確認した人、確認した日など、本人確認の履歴を残す	①本人確認の不実施 ②本人確認の間違い ③マイナンバー記入フォームの漏洩	①【組織】本人確認書類の取得･保管と実施状況の監査 ②【技術】記入フォームのアクセス制御 ③【技術】記入フォームのアクセスログ取得
			4	マイナンバー管理者（各部署）	･記入済フォームを本社のマイナンバー管理者にメール等で送付	①メールの誤送信 ※中継サーバーやアーカイブにメールのデータが残るなどのリスクも考えられるので、メールを利用の際には留意すること	①【技術】メールに添付した記入フォームの暗号化やアクセス制御
			5	マイナンバー管理者（本社）	･フォームの内容を確認（本人確認を含む）	①マイナンバー記入フォームの漏洩	①【技術】記入フォームの暗号化やアクセス制御 ②【技術】記入済フォームのファイルアクセスログ取得
B	対面で提示	･社員がマイナンバー管理者（人事部等）に直接マイナンバー･本人確認書類を提示	1	マイナンバー提供者	･マイナンバー（個人番号通知カード等）及び本人確認書類を持参し、マイナンバー管理者に提示	①個人番号通知カード/個人番号カードの紛失 ②盗難等による不正取得 ③マイナンバー提供者による提示の拒否	①【人的】社員への教育（事務取扱担当者に限らず、社員･パート等、全体への教育） ②マイナンバー提供者が提示を拒否した場合は、書類提出先の機関の指示に従う
			2	マイナンバー管理者	･提示された書類を以て、本人確認を実施 ･本人確認の方法と本人確認した人、確認した日など、本人確認の履歴を残す	①本人確認の不実施 ②本人確認の間違い	①【組織】本人確認書類の取得･保管（実施の記録）と実施状況の監査
C	収集･保管クラウドサービス	･収集･保管クラウドサービスを利用 社員等が、自らのマイナンバーと本人確認書類をクラウドサービスに登録する ※社員個々人がクラウドサービスを利用するためのIT環境が整っていることが条件	1	マイナンバー提供者	･マイナンバー（個人番号通知カード等）及び本人確認書類をデジタル化（スキャニング或いはスマホ等での写真撮影等）	①データ化したマイナンバーや本人確認書類の漏洩 ②提出者が、マイナンバー等をデジタル化する手段を持たない	①【人的】社員への教育（事務取扱担当者に限らず、社員･パート等、全体への教育） ②郵送等、他の手段の併用 ※誰からマイナンバーを収集するかによって手段が分かれ、管理が煩雑になる点には留意すること

業務パターン			業務プロセス			業務プロセスにおける懸念点	対策例 ※【】内は該当する安全管理措置のカテゴリ
パターン		概要	No.	主体	業務		
			2	マイナンバー提供者	・マイナンバー収集・保管クラウドサービスの画面に必要事項を入力、マイナンバー/本人確認書類のデジタルデータを添付して登録 ※提供者の扶養家族については、代表者が本人確認を行ったうえで、まとめてクラウドサービスに登録	①提出者のITリテラシーの低さ ②ログインID、パスワードの漏洩 ③情報入力のミス（特に扶養家族等）	①【人的】社員への教育（事務取扱担当者に限らず、社員・パート等、全体への教育） ②システムによる入力内容の正誤チェック
			3	マイナンバー管理者	・クラウドサービスに登録された情報を確認（本人確認を含む） ・不備があれば訂正依頼	①本人確認の不実施 ②本人確認の間違い ③ログインID、パスワードの漏洩 ④ダウンロードしたファイル（CSV等）の漏洩	①【組織】本人確認実施状況の監査 ②【技術】ダウンロードしたファイルの暗号化・アクセス制御
D	郵送・社内便	・社員がマイナンバー管理者（人事部等）に対し、郵送でマイナンバーと本人確認書類を送付	1	マイナンバー提供者	・人事部等の主管部所から、マイナンバー提供依頼・返信用封筒等を、マイナンバー提供者に配布		
			2	マイナンバー提供者	・マイナンバー、本人確認書類の写しを封入し、マイナンバー管理者宛に郵送	①マイナンバー、本人確認書類の写し取得時に原本を紛失 ②郵送経路での紛失	①【物理】追跡可能な移送手段の利用
			3	マイナンバー管理者	・郵送された書類を確認（本人確認を含む）	①受領したマイナンバー・本人確認書類を紛失・盗難	①【物理】マイナンバー・本人確認書類を施錠管理

【マイナンバー 業務プロセス･リスク分析（保管プロセス）】

Version 1.0：2015/9/15

業務範囲	･事業者が、社員（及びその扶養家族）や個人支払先からマイナンバーを受領し、正しいマイナンバーを保管する ･社員の退職などマイナンバーが不要になったら保管しているマイナンバーを削除する ･マイナンバーが付与されている法定調書の保管期限（５～７年など）が経過したら削除する

業務パターン			業務プロセス			想定されるリスク	リスクへの対策 ※安全管理措置にて具体的に検討する
パターン		概要	No.	主体	業務		
A	電子ファイル	･電子ファイルにて保管	1	マイナンバー管理者	･収集したマイナンバーを基に特定個人情報ファイルを作成	①関係者外が閲覧 ②オペレーションミスによる、破損、漏洩 ③不正な流用	①【技術】【組織】マイナンバー取扱担当者の限定、アクセス制御、定期的な点検･監査 ②【技術】データバックアップ、メール誤送信対策等 ③【技術】【人的】従業員教育、定期的な点検、監査
B	システム	･システム（パッケージソフト或いは自社開発）にて保管	1	マイナンバー管理者	【パッケージソフト】 ･既存の人事･給与システムにて管理	①パッケージソフトの機能拡張（マイナンバー対応）遅れ、機能不足 ②既存システム（帳票出力システムなど人給パッケージ以外）との連携における不具合 ③ マイナンバーを含むDB（特定個人情報ファイル）の安全管理措置の漏れ	①パッケージのマイナンバー制度対応の評価（安全管理措置*、帳票フォーマット等） *：アクセス制御、利用実績の記録等 ②パッケージベンダーより、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
			2	マイナンバー管理者	【自社開発】 ･既存の人事･給与システムにて管理	①既存システム（帳票出力システムなど人給パッケージ以外）との連携における不具合 ②要件定義の漏れ（マイナンバー制度の要件を充足しない、目的外利用に該当） ③マイナンバーを含むDB（特定個人情報ファイル）の安全管理措置の漏れ	①自社開発システムのマイナンバー制度対応の評価 （安全管理措置*、帳票フォーマット等） *：アクセス制御、利用実績の記録等
C	収集･保管クラウドサービス	･収集時に社員等が登録したデータを、そのまま保管	1	マイナンバー管理者	･収集プロセスで得たマイナンバーを収集･保管クラウドサービスで保存	①クラウド事業者からの漏洩	①委託先/再委託先の安全管理措置の運用状況を監査 ※収集･保管クラウドサービスは「委託」にあたると考えられる為
D	書面	･紙媒体の書面で保管	1	マイナンバー管理者	･収集プロセスで得たマイナンバーを台帳等にて保管	①盗難や紛失 ②記載ミス ③オペレーションミスによる毀損	①【物理】台帳等の施錠管理 ②【組織】【人的】管理者等によるダブルチェック ③【技術】【物理】入退室管理（指紋認証、静脈認証等）、キャビネットの使用履歴管理等

【マイナンバー 業務プロセス･リスク分析（利用プロセス）】

Version 1.0：2015/9/15

業務範囲	･事業者が、社員（及びその扶養家族）や個人支払先から提供されたマイナンバーを法定調書に付与する ･（将来）民間活用を通じて既存ビジネスの付加価値を高める ･（将来）民間活用を通じて新規ビジネスモデルを検討する

業務パターン			業務プロセス			想定されるリスク	リスクへの対策 ※安全管理措置にて具体的に検討する
パターン		概要	No.	主体	業務		
A	システム	･帳票作成システム等で書類作成･出力	1	マイナンバー管理者	･既存の法定調書作成システムにマイナンバー付番機能を実装	①保管システムとの連携 ②出力された法定調書の紛失（盗難、印刷の取り忘れ等）	①【技術】【組織】マイナンバーの閲覧･出力機能の権限制御、出力した帳票の施錠管理
B	手書き	･書類に手書きで記入	2	マイナンバー管理者	･既存の法定調書作成システム（帳票作成パッケージ、Excel等）で出力された調書に手書きする	①個人番号関係事務実施者以外の者がマイナンバーへのアクセスをする ②個人番号関係事務実施者による不正取得･持ち出し ③記入ミス	①【人的】管理者によるダブルチェック、定期的な点検 ②【組織】利用実績を記録
			3	マイナンバー管理者	･法定調書へのマイナンバー記載を本人に依頼 ※本人確認を行ったうえで実施すること	①記入済帳票からの漏洩 ②記入ミス	①【組織】郵送経路の追跡･本人限定受取り

【マイナンバー 業務プロセス･リスク分析（提供プロセス）】

Version 1.0：2015/9/15

業務範囲	･税、社会保障の申告を税務署、市区町村、社会保険事務所、ハローワークに行う ･税、社会保障に関する申告処理のために税理士、社労士に帳票･マイナンバーを提供する ･人事給与に関する業務を委託するためマイナンバーを委託先に提供する

業務パターン			業務プロセス			想定されるリスク	リスクへの対策 ※安全管理措置等
パターン		概要	No.	主体	業務		
A	ファイル	･全般	1	マイナンバー管理者	･税理士、社労士に対してメール等で帳票を送付	①宛先間違いによる誤送信 ②メールの盗聴による漏えい	①【物理】【技術】暗号化およびメール以外の手段によるパスワード通知 ②メール誤送信対策ソフトの活用
B	システム連携	社内人事給与システムと下記システムとの連携 ･e-Tax（国税電子申告･納税システム） ･eLTAX（地方税ポータルシステム）	1	マイナンバー管理者	･国税、地方税に関する電子申告	①個人番号関係事務実施者による不正持ち出し ②管理者以外がサイト（情報）にアクセスできる	①【人的】事務担当者の監督･教育（研修）（就業規則） ②【技術】ネットワークセグメントの分離、IP制限、アカウント管理
		社内人事給与システムと下記システムとの連携 ･e-Gov（電子政府の総合窓口）	2	マイナンバー管理者	･健康保険、厚生年金保険、雇用保険などの社会保障に関する届出	①個人番号関係事務実施者による不正持ち出し ②管理者以外がサイト（情報）にアクセスできる	①【人的】事務担当者の監督･教育（研修）（就業規則） ②【技術】ネットワークセグメントの分離、IP制限、アカウント管理
C	収集･保管クラウドサービス	･収集･保管クラウドサービスに登録されたマイナンバーを、業務委託先等が参照	1	マイナンバー管理者	【委託元が契約するクラウドサービスを利用】 ･収集、保管したマイナンバーを収集･保管クラウドサービスで保管し、当該データを委託先等が参照	①クラウド事業者からの漏えい ②フィッシングによる漏えい（収集･保管サービスの名を語って入力させる）	①【人的】委託先選定基準の設定、対策状況の確認、全社員、事務担当者の教育
			2	マイナンバー管理者	【委託先が契約するクラウドサービスを利用】 ･マイナンバーを使用する業務を委託先システムに登録 ※アウトソーシング業者が収集･保管サービスを提供している場合	①委託先からの漏えい ②外部からのハッキングによる漏えい	①【人的】委託先選定基準の設定、対策状況の確認 ②【技術】システムの脆弱性監査
C	郵送	社会保険事務所、税務署、ハローワーク、税理士、社労士等への書類送付	1	マイナンバー管理者	･税理士、社労士、マイナンバー提供者へ郵送で帳票送付	①郵送時の誤送付及び不達	①【物理】追跡可能なサービスを利用（簡易書留、開封検知付き/GPS付き郵送サービス等）
D	手渡し	マイナンバー記入済みの書類	1	マイナンバー管理者	･税理士、社労士、マイナンバー提供者への帳票提出	①盗難や紛失	①【物理】鞄や持ち出し用容器の施錠
		USBメモリ、CD-R等記憶媒体	2	マイナンバー管理者	･業務委託先、税理士等へ社員･扶養家族等のマイナンバーデータを提供	①盗難や紛失 ②個人番号関係事務実施者による不正持ち出し ③委託先での目的外利用	①【物理】鞄や持ち出し用容器の施錠 ②【人的】事務担当者の監督･教育（研修）（就業規則） ③【人的】委託先選定基準の設定、対策状況の確認（監査･監督） ④【物理】マイナンバーデータの暗号化

【マイナンバー 業務プロセス･リスク分析（廃棄プロセス）】

Version 1.0：2015/9/15

業務範囲	･保有しているマイナンバーを廃棄･削除する

業務パターン			業務プロセス			想定されるリスク	リスクへの対策 ※安全管理措置等
パターン		概要	No.	主体	業務		
	【前提】	-	1	-	･特定個人情報は、番号法で限定的に明記された事務を行う必要がある場合に限り保管し続けることが可能。 ･個人番号が記載された書類等のうち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は、その期間保管する。 ･個人番号部分を復元できない程度にマスキング又は削除した上で他の情報の保管を継続することは可能。 ※退職者等についても個人情報を利用する場合があるため（社会保障関連等）、マイナンバーの部分のみ削除できるような仕組みにしておくことが重要 ※特定個人情報の管理規程には、廃棄の仕方を規程に織り込んでおくこと 保存年限経過後に削除することが基本	-	-
A	電子ファイル	･マイナンバーを削除（マイナンバーの部分だけ削除） <削除が必要になるケース例> ･退職者 ･マイナンバーが変更になった際の旧番号 ･扶養から外れた家族 ･契約が終了した支払先（産業医等）	1	マイナンバー管理者	･該当マイナンバーデータを電子ファイルから削除	①誤削除 ②削除漏れ	①【組織】廃棄業務の管理体制構築（廃棄対象の把握、確認、承認）
B	システム	･マイナンバーを削除（マイナンバーの部分だけ削除） <削除が必要になるケース例> ･退職者 ･マイナンバーが変更になった際の旧番号 ･扶養から外れた家族 ･契約が終了した支払先（産業医等） ※以下同様	1	マイナンバー管理者	･該当マイナンバーデータをシステムから削除	①誤削除 ②削除漏れ ※パッケージソフトの場合、削除の方式を確認すること（無効フラグを立てるだけか、完全にデータを削除しているのか、等） ③バックアップデータの漏えい ※マイナンバーと個人情報が紐づいた状態になっていると特定個人情報とみなされる為、バックアップの取り方に注意（バックアップデータに残る可能性がある）	①【組織】廃棄業務の管理体制構築（廃棄対象の把握、確認、承認） ②パッケージソフトの削除の仕組みを確認
C	収集･保管クラウドサービス	･マイナンバーを削除	1	マイナンバー管理者	･該当マイナンバーデータをシステムから削除	①誤削除 ②削除漏れ ※クラウドサービスの利用時は、サービス業者の責任の範囲や国内法が適用されるか等を確認しておくこと。 3.クラウド事業者からのバックアップデータの漏えい	①【組織】廃棄業務の管理体制構築（廃棄対象の把握、確認、承認） ②クラウド事業者から削除したことの証明書を取得
D	紙	･法定保存年限を経過した書類を廃棄	1	マイナンバー管理者	･対象となる書類を廃棄 ※廃棄の記録は残しておくこと	①保存年限経過後の廃棄漏れ ②誤廃棄 ③廃棄書類の盗難、盗み見による漏えい ④廃棄委託業者による盗難、漏えい ⑤廃棄の記録漏れ	①【組織】廃棄業務の管理体制構築（廃棄対象の把握、確認、承認） ②【物理】書類の焼却、溶解等の復元不可能な廃棄方法を採用 ③【組織】委託先が確実に廃棄したことを証明書等で確認
		･マイナンバーを削除（マイナンバーの部分だけ削除）	2	マイナンバー管理者	･台帳等から当該番号を削除 ※廃棄の記録は残しておくこと	①誤削除 ②削除漏れ ③廃棄の記録漏れ	①【組織】廃棄業務の管理体制構築（廃棄対象の把握、確認、承認）