システム保守・運用業務に対する マイナンバー安全対策チェックリスト

2015 年 7 月 6 日

関連資料のご案内

本資料と合わせてご覧いただきたい関連資料は以下の通りです。

ホワイトペーパー
「人事・経理責任者が知っておくべきマイナンバー安全対策の盲点」

ホワイトペーパー
「システム管理者・外部委託先による情報漏えいを防ぐには」

マイナンバーの安全な管理と利用を実現するために

2016 年 1 月より施行されるマインバー制度。この制度によって付与される個人番号は、国民一人ひとりを識別する固有の番号であることから、その不正利用によって個人のプライバシー侵害につながらないよう、すべての事業者・公共団体に対し、適切な取扱いが求められます。このドキュメントは、マイナンバーを扱う IT システムに対する保守・運用業務に対して、現状の対策状況を確認し、必要に応じて追加の対策を検討いただくためのチェックリストです。

システム保守・運用業務に対する安全対策の必要性

システムの保守・運用担当者は業務上、サーバーやデータベースに管理者権限（特権 ID）を使用して直接アクセスすることがあります。したがって、その権限を悪用すれば、格納された個人番号の閲覧や変更、削除が可能です。 実際に過去に発生した情報漏えい事件の多くは、システムの保守・運用を担当する社員や委託先の技術者によって引き起こされています。従業員の特定個人情報に対する不適切なアクセスが発生しないよう安全対策を講じる必要があります。（詳細は左記関連資料をご参照ください）

対応方針別のチェックリストの利用方法

どのような形でマイナンバー制度に対応するのかは、企業ごとに様々です。中には自社でシステムを一切保有せず、すべての関連事務をアウトソーシングするケースもあるでしょう。
本チェックリストは、そのようなケースも含め、マイナンバー対応方針における様々なケースでご利用いただくことが可能です。ここでは、大きく 3 つの対応方針別に利用方法をご紹介します。

自社でマイナンバーシステムを保有する場合

自社でシステムを保有し、従業員の個人番号をシステム内に保有する場合、その保守・運用業務は、自社のシステム部門が担う形になります。この場合、本チェックリストは、自社におけるシステム保守・運用業務を対象に、その安全対策の実施状況を確認する目的で利用いただけます。

また、個人番号の取扱いを含む業務を外部に委託する場合は、番号法上の外部委託にあたるため、委託先の選定や安全管理措置の実施状況を監督する際のチェック項目としても利用できます。

クラウドサービスなど外部サービスを利用する場合

個人番号を保管するクラウドサービスなど、外部のサービスを利用する場合、システムの保守・運用はサービス提供を行う事業者が実施することになります。その場合、サービスを選定する際にチェックすべき項目として利用いただけます。

尚、IaaS サービスのように、利用するサービスの保守・運用業務の範囲で個人番号の取扱いが発生しない場合には、講じるべき安全対策は、サービスを利用する企業になるため、利用するサービス上で、必要な安全対策が実施可能かどうかという点でチェックリストを利用できます。

マイナンバー関連事務自体を外部に委託している場合

3 つ目のケースは、マイナンバー関連事務自体を外部のサービス会社にアウトソーシングする場合です。この場合、関連事務全体を外部委託するため、安全管理措置の実施は、サービス会社が講じることになり、企業はその実施状況を監督することになります。

サービス会社が、委託を受けたマイナンバー関連事務を遂行するにあたって IT システムを利用する場合、当該システムの保守・運用業務において、適切な安全対策が講じられている必要があります。つまり、本チェックリストは、外部委託先を選定する際のチェックリストとして、活用いただくことができます。

参考資料

本チェックリストの策定にあたり、以下の資料を参照しております。

- 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）
  平成 26 年 12 月 11 日　特定個人情報保護委員会
- 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
  平成 26 年 12 月 経済産業省
- 金融機関等コンピュータシステムの安全対策基準・解説書（第 8 版追補改訂）
  平成 27 年 6 月　金融情報システムセンター
- 情報セキュリティ管理基準（平成２０年改正版）　経済産業省

お問い合わせ

エンカレッジ・テクノロジ株式会社
東京都中央区日本橋浜町 3-3-2
トルナーレ日本橋浜町 7F
TEL 03-5623-2622
www.et-x.jp

システム保守・運用業務に対するマイナンバー安全対策チェックリスト(1/2)

最初のチェック項目は、システム保守・運用業務において、個人番号を取り扱う業務と担当者の明確化です。多様なシステム保守・運用業務において、個人番号の取り扱いが発生する業務を特定することは、適切な安全対策を講じる上で非常に重要です。対象業務を網羅的に特定できていないと、対策の網羅性が欠落し、思わぬリスクを抱えることになります。例えば、アプリケーションが出力するトランザクションログの中に個人番号が含まれてることが把握できておらず、安全対策を講じる範囲から外れていた、といったケースが想定されます。

チェック項目	チェックすべきポイント
個人番号取扱い業務と担当者/保護すべき情報の明確化	
保護すべき個人番号、特定個人情報の所在、保管場所（バックアップやログファイルに含まれる情報を含む）は網羅的に掌握されているか？	個人番号が保管されている場所を明確にしなければ、保護対象を特定できません。バックアップファイルや個人番号が情報に含まれるログファイルなどが盲点になりやすい情報ですので、網羅的に確認し、把握しておく必要があります。
「個人番号の取扱い」が発生する保守・運用業務は明確になっているか？	様々な保守・運用業務の中で、個人番号の取扱いが発生する業務を明確にし、対象業務における適切な取扱いと、対象業務における適切なアクセス制御を働かせる必要があります。一般的には個人番号データベースの管理作業、データベースのバックアップなどの業務が該当します。 留意すべき点は、個人番号を含むログファイルが生成される仕組みが存在する場合、このログファイルを扱う業務についても、適切な管理が必要ということです。
「個人番号の取扱い」に相当しない業務に対するアクセス制御の仕組みは存在するか？	対象とならない業務では、個人番号にアクセスできないよう適切に制御されている必要があります。例えば対象外の業務であっても、あらゆる権限を有する特権 ID を使用している場合には、適切なアクセス制御が施されているとは言えません。適切に権限を制御できない場合には、対象外の業務であっても、アクセス内容を記録し、不正な個人番号の取扱いがなかったかを確認する必要があります。
対象外の業務において、個人番号に不正にアクセスされていないこと確認・客観的に証明する手段・方法を装備しているか？	前項にある通り、対象外の業務において個人番号への不正なアクセスができないよう制御する仕組みの構築が困難な場合は、作業内容を監視・記録し、不正なアクセスがなかったことを確認する仕組みが必要になります。
「個人番号の取扱い」が発生する保守・運用業務を行う担当者・責任者は明確になっているか？	システム保守・運用業務を複数の担当者で実施している場合、対象業務の担当者と責任者を明確にし、必要な教育、監視を施す必要があります。
担当者が個人番号の取扱いが伴う保守・運用業務を行う際は事前に承認を受けるなどのプロセスが確立されているか？	システム保守・運用業務担当者が個人番号へアクセスする必要が生じた際は、どのようなプロセスで実施するか、承認ルール等を策定しておくことで、不正なアクセスの防止につながります。

システム保守・運用業務に対するマイナンバー安全対策チェックリスト(2/2)

2 つ目のチェック項目は、個人番号を取り扱う保守・運用業務に対する具体的な安全対策です。保守・運用業務の性質上、管理者権限を使用することが避けられないことから、権限を制御することで不適切な番号の取扱いを防止できる効果は、限定的となります。アクセス制御による予防的対策が大きな効果を発揮できない代わりに、相互牽制や監視・記録と点検といった発見的な対応を併用する必要があります。

チェック項目	チェックすべきポイント
個人番号取扱い業務と担当者に対する具体的な対策の確認	
担当者であっても、常には個人番号にアクセスできないように制御され、アクセスが必要な場合に限り、事前に申請・承認を経てアクセスできるように管理されているか ？	業務上、個人番号を取り扱う担当者であっても、常に個人番号にアクセスできる権限を与えておくことは、不適切なアクセスを許してしまう要因になります。必要な場合に限り、事前に日時、目的などを明確にし、適切な承認プロセスを経て初めてアクセスできるようなプロセスを構築しておくことが必要です。
個人番号へのアクセス権限は、第三者に使用されないよう十分保護されているか ？	個人番号へのアクセスが許可されているアカウントについては、不正に使用されないよう、十分な保護措置を講じておく必要があります。例えば、推測しづらいパスワードの設定、定期的なパスワードの変更。ワンタイムパスワードの使用、多要素認証の採用などの方法があります。
個人番号へアクセスした担当者を特定できるようアクセス者が識別できる仕組みを有しているか ？	複数の担当者が個人番号を取り扱う場合、誰がアクセスしたのかが明確にできるようアクセス者を識別できることが必要です。識別が困難ですと、有事の際のアクセス者の特定や原因究明が困難になります。 識別する方法は、アカウントを共有せず、担当者ごとに固有のアカウントを使用させることが推奨されますが、同一のアカウントを共有することがやむを得ない場合でも、貸出履歴を記録しておくことで、識別が可能になります。
不審な個人番号へのアクセスやアクセス試行が行われていないか、確認できる仕組みや体制を整えているか ？	個人番号へのアクセス権限を有するアカウントのログイン履歴（成功・失敗）を確認し、管理者が把握していないログイン記録や不審なアクセス試行（ログイン拒否）が記録されていないかを定期的など、確認プロセスを確立していることが必要です。
個人番号が保管されているシステムから個人データを持ち出す場合には、承認制や相互牽制等の仕組みにより無断で持ち出しできないような仕組みを有しているか ？	個人番号データベースからファイルを持ち出す場合には、管理者の承認を受けるなど単独で行えないようにする仕組みが必要です。例えば、可搬媒体を使う場合には、可搬媒体を管理する別の担当者から媒体の貸与を受けるなどの仕組みが有効です。しかし可搬媒体による情報持ち出しは、私物の媒体に対する持ち込み防止対策が不可欠です。代替策としては、ファイル持ち出し用の専用ファイルサーバー等を介して行うことで、可搬媒体の煩雑な管理を不要にするができます。
個人番号を取り扱う業務を実施する際は、複数人で実施するなど相互牽制の仕組みを取り入れているか ？	担当者が権限を濫用し、不適切なアクセスを行うことを防止する手段として、複数名による作業を徹底する方法があります。
個人番号へのアクセス内容は、すべて保管し必要に応じて内容をチェックしているか ？	システム保守・運用業務において適切に個人番号の取扱いを行っていることを確認するためには、アクセスログの記録と保管、定期的なチェックは欠かせない対策の一つです。
個人番号に対するアクセスログは、管理者権限であっても改ざん、削除されないよう、保護される仕組みが存在するか ？	アクセスログに対する権限は、個人番号取扱い担当者とは分離し、意図的なログの改ざんや削除が行われないようにすることが重要です。個人番号システム内にログを保管してしまうと、管理者権限の権限調整が難しいため、ログを保管するサーバーを分離して、異なるアカウントに対してのみ許可したり、暗号鍵など別の仕組みで保護する手段を用いたりする工夫が必要です。