

マイナポータル自己情報取得API 利用条件確認書

組織名称	
Webサービス名	
作成年月日	
本件連絡先	
所属名	
担当者名	
電話番号	
e-mailアドレス	

【作成要領】

- APIを利用するサービスごとに作成して下さい。（一のWebサービス提供者が複数のWebサービスにおいて自己情報取得APIを利用する場合には、当該複数のWebサービスごとに本利用条件確認書を作成して下さい。）
- 事前申込み時点においては、項番1.1のみ確認しチェックして下さい。利用申請時点において、全ての項番について確認しチェックして下さい。

1 確認項目

項番	項目	チェック欄
1.1	組織役員等の要件（利用規約 3 条 2 項 1 号）	
1.2	自己情報の取扱い（利用規約 3 条 2 項 2 号）	
1.3	情報セキュリティ対策の実施（利用規約 3 条 2 項 3 号）	

【記載要領】

- 「1.3 情報セキュリティ対策の実施」については、「2 1.3 情報セキュリティ対策の実施 附表」における全ての項目について確認しチェックしたことを確認して、チェックを行ってください。
- 行政機関等（行政手続等における情報通信の技術の利用に関する法律第二条第二号に規定する行政機関等をいう。以下同じ。）においては、1.2 及び1.3について、確認・チェックして下さい。

2 1.3 情報セキュリティ対策の実施 附表

項番	項目	チェック欄
1.3.1	個別的対策の実施（インターフェイス仕様書に定める対策の実施）	
1.3.2	一般的対策の実施（以下全ての対策（4.1～4.5）の実施）	
4.1	情報セキュリティに対する組織的な取り組み状況	
4.1.1	情報セキュリティに関する経営者の意図が従業員に明確に示されていますか？	
4.1.2	情報セキュリティ対策に関わる責任者と担当者が明示されていますか？	
4.1.3	管理すべき重要な情報資産を区分していますか？	
4.1.4	重要な情報については、入手、作成、利用、保管、交換、提供、消去、破棄における取り扱い手順を定めていますか？	
4.1.5	外部の組織と情報をやり取りする際に、情報の取り扱いに関する注意事項について合意を取っていますか？	
4.1.6	従業者（派遣を含む）に対してセキュリティに関して就業上何をしなければいけないかを明確にしていますか？	
4.1.7	情報セキュリティに関するルールの周知と、情報セキュリティに関わる知識習得の機会を与えていますか？	

項番	項目	チェック欄
4.2	物理的セキュリティ	/
4.2.1	重要な情報を保管したり、扱ったりする場所の入退管理と施錠管理を行っていますか？	
4.2.2	重要なコンピュータや配線は地震などの自然災害や、ケーブルの引っ掛けなどの人的災害に配慮し適切に配置・設置していますか？	
4.2.3	重要な書類、モバイルPC、記憶媒体などについて、整理整頓を行うと共に、盗難防止対策や確実な廃棄を行っていますか？	
4.3	情報システム及び通信ネットワークの運用管理状況	/
4.3.1	情報システムの運用に関して運用ルールを策定していますか？	
4.3.2	ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行っていますか？	
4.3.3	導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行っていますか？	
4.3.4	通信ネットワークを流れる重要なデータに対して、暗号化などの保護策を実施していますか？	
4.3.5	モバイルPC やUSB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施していますか？	

項番	項目	チェック欄
4.4	情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況	/
4.4.1	情報（データ）や情報システムへのアクセスを制限するために、利用者ID の管理（パスワードの管理など）を行っていますか？	
4.4.2	重要な情報に対するアクセス権限の設定を行っていますか？	
4.4.3	インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISP サービス等）を行っていますか？	
4.4.4	無線LAN のセキュリティ対策（WPA2 の導入等）を行っていますか？	
4.4.5	ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行っていますか？	
4.5	情報セキュリティ上の事故対応状況	/
4.5.1	情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握していますか？	
4.5.2	情報セキュリティに関連する事件や事故等（ウイルス感染、情報漏えい等）の緊急時に、何をすべきかを把握していますか？	

【記載要領】

- 「1.3.1 個別的対策の実施」については、インターフェイス仕様書に定める対策を実施したことを確認し、チェックして下さい。
- 「1.3.2 一般的対策の実施」については、4.1~4.5の全ての対策を実施したことを確認しチェックしたことを確認して、チェックを行ってください。
- 4.1~4.5の対策については、「中小企業における組織的な情報セキュリティ対策ガイドライン」の「4 共通して実施すべき対策」を参照し、確認・チェックして下さい。
(URL:https://www.ipa.go.jp/security/manager/known/sme-guide/sme-security_guidline.html)
- 行政機関等においては、1.3.1のみについて、確認・チェックして下さい。