第三者証明書
マイナンバー制度における安全管理措置

№２０１５－ＩＳＲ－７０３
平成２７年１０月１５日
株式会社アイ・エス・レーティング

株式会社アイ・エス・レーティングは、三谷産業株式会社のマイナンバークラウドソリューション（マイナンバー専用クラウドサービス）における安全管理措置に関する調査を実施しました。

本書において、以下に掲載した事案が事実であることを第三者として証明します。

１．調査概要

企業・団体名	三谷産業株式会社
調査スコープ	三谷マイナンバークラウドソリューション
調査対象	マイナンバー専用クラウドサービス
調査事項	マイナンバー専用クラウドサービス提供における安全管理措置状況（※１）
リファレンス	「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）」 特定個人情報保護委員会（平成２６年１２月１１日）
調査日	２０１５年９月２０日～２０１５年１０月１４日
本書交付日	２０１５年１０月１５日
利用期限	本書交付日から１年（※２）
証明 ID コード	10000230115M1501

※１　調査の方法は、責任者等へのヒアリング、規程および台帳類の閲覧、関連設備の視察を用いております。

※２　当証明書は、調査実施日における事象について事実であることを証明するものであり、継続的に当該事象が必ず存在することを保証するものではありません。また、調査対象の仕様変更や社会環境の変化に応じ、緊急時には随時、また平常時には年一回の再調査による点検を推奨しています。

●お問い合わせ先　株式会社アイ・エス・レーティング　〒103-0023 東京都中央区日本橋本町 1-10-2 第 20 ビル　8 階
TEL：03-3273-8830　http://www.israting.com

第三者証明書
マイナンバー制度における安全管理措置

２．確認結果

（１）経営管理

①三谷産業グループとしての統制に加えてクラウドサービスを提供しているアウトソーシング事業のためのＩＳＭＳ推進組織である情報セキュリティフォーラムが機能しており、管理組織体制、情報セキュリティ規程類の整備、情報資産の識別、リスクアセスメント、人的セキュリティ、委託先（子会社）管理、インシデント対応・危機管理、コンプライアンス等、非常に高いレベルで統制が進められている。また、データセンターを運営する現場部門では、お客様からの預かり資産を確実に守るため、物理的アクセス管理やITシステムの運用管理等が着実に実施されている。

②リスクへの対応、事業継続計画（ＢＣＰ）の取り組みとして、リスクマネジメント委員会が設置され、リスクマネジメントに係る計画等の重要事項の承認及びマネジメントレビューが実施されている。

③当該サービスを提供しているデータセンターの建物・設備は、「総務省：公共ＩＴにおけるアウトソーシングに関するガイドライン」「ＩＤＣイニシアティブ：ＩＤＣ活用ガイドライン（高品位規格）」の指針に準拠したデータセンター専用の建物・設備である。また、「日本データセンター協会：データセンターファシリティスタンダードVersion2.1」の評価項目について、第三者による客観的な評価を実施している。

（２）マイナンバー専用クラウドサービスの特徴

①　マイナンバーで求められる安全管理措置に対する万全なセキュリティを実装している。

・お客様毎にプライベートＩａａＳ環境を提供している。
・ファイアウォールによるアクセス制御、攻撃検知を標準提供している。
・クライアントをシンクライアント化することで、標的型攻撃等によるクライアント端末へのウィルス感染による情報漏えいリスクを回避している。
・お客様管理者の負荷軽減実現の為、ファイアウォールの運用管理（ポリシー管理、ログ管理）、マイナンバー保管サーバ／クライアント端末へのセキュリティパッチ適用、標的型攻撃検知時の初期対応等のセキュリティ運用サービス（オプションサービス）を提供している。

②　情報セキュリティ格付けＡＡＡｉｓのデータセンターにて安心安全なサービスを提供している。

・お客様に運用者の顔が見えるクラウドサービスを提供することで、クラウド利用の不安を払拭している。
・データセンターとして、国内トップクラスのセキュリティ対策を実施している。
・免震構造、電力２系統受電、自家発電燃料の７２時間備蓄及び自社調達で、災害発生時も万全な対応が可能である。

●お問い合わせ先　株式会社アイ・エス・レーティング　〒103-0023 東京都中央区日本橋本町 1-10-2 第 20 ビル　8 階
TEL：03-3273-8830　http://www.israting.com

第三者証明書
マイナンバー制度における安全管理措置

（３）マイナンバー専用クラウドサービス提供における安全管理措置状況

特定個人情報保護委員会は、番号法第３７条に基づき、国民生活にとっての個人番号その他の特定個人情報の有用性に配慮しつつ、その適正な取扱いを確保する措置を講じることを任務としている。その特定個人情報保護委員会のガイドライン「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）は、番号法第４条及び第３７条に基づき、事業者が特定個人情報の適正な取扱いを確保するための具体的な指針を定めたものである。三谷産業株式会社のマイナンバー専用クラウドサービスは、そのガイドラインに示されている安全管理措置を講じている。ガイドラインに示されているすべての項目について状況を確認した。

・お客様による安全管理措置

No.	項目	状況
1	**基本方針の策定**	「基本方針」、「取扱規程」等の策定は、お客様作業になります。 ・規程に基づく、組織体制の整備や運用 ・取扱状況の確認や漏えい時の体制整備 ・事務取扱担当者の監督・教育
2	**取扱規程等の策定**	
3	**組織的安全管理措置**	
4	**人的安全管理措置**	

・マイナンバー専用クラウドサービスで対応している安全管理措置

No.	項目	内容	詳細	状況
5	**物理的安全管理措置**	特定個人情報を取り扱う区域の管理	入退室管理及び管理区域への持ち込む機器等の制限	・クラウド基盤は、不正侵入防止対策を実施している自社のデータセンターに設置している。さらに、データセンターでは、金属探知機により持ち込み機器のチェックを実施している。なお、データセンターでは、携帯電話、スマホ、カメラ等所持品の持ち込みを原則禁止している。
			入退室管理方法としては、ＩＣカード、ナンバーキー等による入退室管理システムの設置	・クラウド基盤は、ＩＣカード、パスワード、指紋認証の３要素認証による入退室管理を実施している自社のデータセンターに設置している。
			壁又は間仕切り等の設置及び座席配置の工夫	・クラウド基盤は、自社のデータセンターサーバルームに設置している。サーバルームは共連れ防止のサークルゲートにより仕切られている。

●お問い合わせ先 **株式会社アイ・エス・レーティング**
〒103-0023 東京都中央区日本橋本町 1-10-2 第 20 ビル 8 階
TEL：03-3273-8830 http://www.israting.com

	物理的安全管理措置	機器及び電子媒体等の盗難等の防止	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	・クラウド基盤は、自社のデータセンターサーバルームに設置し施錠されたラックに格納している。ラックの鍵についても、鍵管理システムにより厳重に管理されている。
			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こと	・クラウド基盤は、自社のデータセンターサーバルームに設置しており、持出しが不可能。
		電子媒体等を持ち出す場合の漏えい等の防止	電子媒体を持ち出す場合は、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（但し行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う）	・クラウド基盤では、電子機器媒体の持出しを禁止している。 ・データの暗号化、パスワードによる保護についてはお客様作業です。 ・お客様サイトのクライアントは、クラウド基盤上の仮想クライアントの操作のみ行う運用とすることで、データは保存されない。
			書類等を持ち出す場合は、封緘、目隠しシールの貼付を行う	・お客様作業です。
		個人番号の削除、機器及び電子媒体等の廃棄	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する	・お客様作業です。
			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する	・クラウド基盤の機器を廃棄する場合は、復元不可能な状態で廃棄している。

●お問い合わせ先 **株式会社アイ・エス・レーティング**　〒103-0023 東京都中央区日本橋本町 1-10-2 第 20 ビル　8 階
TEL：03-3273-8830　http://www.israting.com

	物理的安全管理措置	個人番号の削除、機器及び電子媒体等の廃棄	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する	・お客様作業です。
			特定個人情報を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提にした情報システムを構築する	・お客様作業です。
			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きを定める	・お客様作業です。
6	**技術的安全管理措置**	アクセス制御	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する	・クラウド基盤上の特定個人情報保管サーバシステム（※）へアクセス出来るクライアントは、同基盤上の仮想クライアントのみとなっている。このクライアントにリモート接続するお客様サイトのお客様準備クライアントも、ファイアウォールにより限定している。 ・ユーザＩＤ制御は、お客様ご準備の特定個人情報保管サーバシステム（※）にて対応する作業です。
			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	
		アクセス者の識別と認証	事務取扱担当者の識別方法としては、ユーザーID、パスワード、磁気・IC カード等が考えられる	

●お問い合わせ先 **株式会社アイ・エス・レーティング** 〒103-0023 東京都中央区日本橋本町 1-10-2 第 20 ビル 8 階
TEL：03-3273-8830 http://www.israting.com

第三者証明書
マイナンバー制度における安全管理措置

	技術的安全管理措置	外部からの不正アクセス等の防止	情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する	・ファイアウォールにより外部及び内部ネットワーク経由の不正アクセスを遮断している。なお、ファイアウォールは攻撃検知遮断機能を有している。
			情報システム及び機器に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	・クラウド基盤上の特定個人情報保管サーバ・仮想クライアントのウィルス対策はお客様作業です。 ・お客様サイトのリモート操作クライアントを、シンクライアントにてご利用頂く事で標的型攻撃やマルウェアによる情報漏えい防止対策をより強化することが可能です。
			導入したセキュリティ対策ソフトウェア等により、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	
			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にする	・お客様作業です。但し、セキュリティ運用サービスオプションにより、ＯＳセキュリティパッチ適用、ファイアウォール運用管理（監査等へのログ提示）、攻撃検知時の物理ＬＡＮ切断を提供している。
			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	
		情報漏えい等の防止	通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる	・ＶＰＮ等によるプライベートネットワーク構築はお客様作業です。
			情報システム内に保存されている特定個人情報等の情報漏えい等の防止策としては、データの暗号化又はパスワードによる保護等が考えられる	・データの暗号化やパスワード保護はお客様ご準備の特定個人情報保管サーバシステム（※）にて対応する作業です。

（※）特定個人情報を取り扱うお客様にて整備頂く業務システム（例えば、人事給与システムなど）

●お問い合わせ先 **株式会社アイ・エス・レーティング**
〒103-0023 東京都中央区日本橋本町 1-10-2 第 20 ビル 8 階
TEL：03-3273-8830 http://www.israting.com

第三者証明書
マイナンバー制度における安全管理措置

３．アピールポイント

三谷産業株式会社アウトソーシングデータセンターは、「総務省：公共ＩＴにおけるアウトソーシングに関するガイドライン」、「ＩＤＣイニシアティブ：ＩＤＣ活用ガイドライン（高品位規格）」の指針に準拠したデータセンター専用の建物・設備である。また、セキュリティ対策は、第三者による客観的な評価である情報セキュリティ格付けとして、中堅ＩＤＣ(Internet Data Center)ながら最高位（ＡＡＡis）を取得・維持している。強固なセキュリティレベルと合わせて、ファシリティについても優れた対策を講じている。さらに、ＩＴサービス継続対策についても、対策を講じている。徹底した安全管理措置による「情報漏えいリスクの低減」が図られる。また、クラウドサービスの活用により「短期導入」と「初期費用低減」が図られる。

ポイント	内容
【マイナンバーで求められる安全管理措置に対する万全なセキュリティ】	・お客様毎に専用の物理サーバを利用した仮想基盤環境を提供。 ・特定個人情報保管サーバ、クライアントを仮想基盤環境に構築しファイアウォールにてネットワークアクセスを制限します。**お客様サイトにご準備頂くリモート接続用クライアントをシンクライアント化することで、標的型攻撃等による端末へのウィルス感染による情報漏えいリスクを回避出来ます。** **・ファイアウォールの運用管理（ポリシー管理、ログ管理）、マイナンバー保管サーバ／クライアントのセキュリティパッチ適用、攻撃検知時の初期対応などのセキュリティ運用サービス（オプションサービス）により管理者の負荷軽減が図られます。**
【徹底した安全管理措置による「情報漏えいリスクの低減」】	・極めて高いセキュリティで保護されたクラウド環境でマイナンバー業務を行うことができるので、情報漏えいリスクの大幅な低減が図れます。 ・セキュリティ運用サービス（有償オプション）により、システム要員の工数削減とセキュリティ対策抜け漏れ防止が図れます。
【情報セキュリティ評価・認証】	**・ＩＳＭＳ（ISO27001）認証に加え、第三者の客観的な評価として情報セキュリティ格付け最高位ＡＡＡis（トリプルＡ）を取得・維持。**
【セキュリティ格付けＡＡＡｉｓのデータセンターによる安心安全なサービス提供】	・お客様に運用者の顔が見えるクラウドサービスを提供することで、クラウド利用の不安を払拭。 ・データセンターとして、国内トップクラスのセキュリティ対策を実施。 ・免震構造、電力２系統受電、自家発電燃料の７２時間備蓄及び自社調達で、災害時にも万全な対応。

●お問い合わせ先 **株式会社アイ・エス・レーティング**　〒103-0023 東京都中央区日本橋本町 1-10-2 第 20 ビル　8 階
TEL：03-3273-8830　http://www.israting.com

第三者証明書
マイナンバー制度における安全管理措置

【クラウド化による「短期間導入」と「初期費用低減」】	・マイナンバー取り扱いに関する安全管理措置ガイドラインに対し、ワンストップで対応するクラウドサービスであるため、以下の導入効果があります。 □短期間での運用開始 －サーバ設置型に比べ短期間での構築／運用が可能 －極めてセキュアなデータセンターとシンクライアント化により、ガイドラインで要求されている取扱い区域や盗難防止対策の構築が不要なため、即運用可能 □初期費用／一時費用の低減 －セキュアなサーバ／ネットワーク構築が不要であるため、初期費用が低減 －取り扱い区域や盗難防止対策やクライアント情報漏えい対策システムコストの低減
【ＩＴサービス継続対策評価】	・「経済産業省：ＩＴサービス継続ガイドライン改訂版」をリファレンスとし、第三者による客観的な評価を実施。
【ファシリティに関する評価】	・「日本データセンター協会：データセンターファシリティスタンダード Version2.1」をリファレンスとし、第三者による客観的な評価を実施。
【安心安全なクラウドサービス】 （高い情報セキュリティを確保したクラウドサービスを提供しています）	・クラウドサービス利用者の情報資産は、利用者ごとに仮想資源を割り当て明確に区分して管理している。このため、マルチテナント型のクラウドサービスでは得られない高い情報セキュリティを確保している。日本国内の自社資源でのみクラウドサービスを提供しており、他組織である供給者のサービスを利用したクラウドサービスは提供していない。このため、他国の資源、サービスの利用や他組織である供給者のサービスの利用に起因するリスクがなく高い情報セキュリティを確保している。 ・「総務省：クラウドサービス提供における情報セキュリティ対策ガイドライン」をリファレンスとし、第三者による客観的な評価を実施。

以上

●お問い合わせ先 株式会社アイ・エス・レーティング
〒103-0023 東京都中央区日本橋本町 1-10-2 第 20 ビル 8 階
TEL：03-3273-8830 http://www.israting.com