「スマホde本人確認」セキュリティチェックシート

本セキュリティチェックシート(以下、「本シート」)は、GMOグローバルサイン株式会社（以下、「当社」）の提供する「スマホde本人確認」サービスのセキュリティに関する情報を、総務省の公表する「クラウドサービスの安全・信頼性に係る情報開示指針（第２版）」に則り開示するものです。
本シートは、当該サービスの利用者、またはその利用を検討中のお客様に開示をすることが目的であり、その他の用途には利用できないものとします。
本シートの内容については、当社の判断により変更できるものとし、変更のあった場合には速やかに改定されたものを開示するものとします。
当社の事業者情報・財務情報等の最新情報については、当社ホームページをご参照ください。
（https://www.globalsign.co.jp/）

【情報開示項目】			【内容】	必須／選択 （注）
1	開示情報の時点	開示情報の日付	開示情報の年月日（西暦）	2024/5/13
コンプライアンス				
2		情報セキュリティに関する組織体制 の状況	情報セキュリティに関する責任者の有無と、「有り」の場合は責任者名・役職	有り CISO: Arvid Vermote
			情報セキュリティに関する組織体制の有無	有り
3	個人情報	個人情報の取扱い	個人情報の取扱いに関する規程等の有無と、「有り」の場合は記載箇所	有り https://www.globalsign.co.jp/policy/privacy.html
4	守秘義務	守秘義務契約	守秘義務に係る契約又は条項の有無	基本的な守秘義務条項についてはサービス約款内第14条（秘密保持）に記載。 詳細については、必要に応じて個別に守秘義務契約を追加で 締結する。
			守秘義務違反があった場合のペナルティ条項の有無	
5	従業員教育等	従業員に対するセキュリティ教育の実施状況	従業員に対するセキュリティ教育実施に関する取組状況	年一度以上の内部監査及び教育活動
6		従業員に対する守秘義務等の状況	従業員に対する守秘義務対応の取組状況	年一度以上の内部監査及び教育活動
7	委託	委託情報に関する開示	サービス提供に係る委託先（再委託先）の情報開示の可否と、可能な場合の条件等	不可
8		委託先に対する管理状況	自社の個人情報保護指針に対する遵守規定の有無	委託先との基本契約に準ずる 原則として再委託禁止、または当社同様の義務・責任を負う 守秘義務契約については必須
			委託先（再委託先）の個人情報保護等の状況に関する情報提供の可否と、可能な場合の条件等	
			委託先（再委託先）との守秘義務対応状況	
9	文書類	情報セキュリティに関する規程等の整備	情報セキュリティに関する基本方針・規程・マニュアル等の状況と文書名	ISO27001基本規則、付随規則に準ずる
10		事業継続に関する規程の整備	事業継続に関する基本方針・規程・マニュアル等の有無と、「有り」の場合は文書名	
			BCP対応計画及び運用手順等の開示の可否と、可能な場合の条件等	
11		リスク管理に関する規程等の整備	リスク管理に関する基本方針・規程・マニュアル等の有無と、「有り」の場合は文書名	
サービス基本特性				
12	サービス内容	サービス名称	本ASP・SaaSのサービス名称	オンライン本人確認サービス スマホde本人確認
13		サービス開始時期	本ASP・SaaSのサービス開始年月日（西暦）	2024年3月1日 大規模な改変履歴はありません
			サービス開始から申請時までの間の大規模な改変等の有無と、「有り」の場合は改変年月日（西暦）	
14		サービスの内容・範囲	本ASP・SaaSのサービスの内容・特徴	本サービスは、銀行口座の開設、不動産の契約、古物商での取引などにおいて必要となる本人確認をオンラインで行う仕組みです。スマートフォンなどのカメラで本人確認書類と自分の顔を同時に撮影して送信するだけで、法律に則った本人確認が可能となります。 AmazonWebService、グループ内企業との機能面での連携 があります（詳細は機密事項）
			他の事業者との間で行っているサービス連携の有無と、「有り」の場合はその内容	

15		サービス提供時間	サービスの提供時間帯	24時間365日
16		サービスのカスタマイズ範囲	アプリケーションのカスタマイズの範囲（契約内容に依存する場合はその旨記述）	カスタマイズは個別相談
17		移行支援	本サービスを利用する際における既存システムからの移行支援の有無（契約内容に依存する場合はその旨記述）	各種支援は個別相談
18	サービスの変更・終了	サービス（事業）変更・終了時等の事前告知	利用者への告知時期（事前の告知時期を1ヶ月前、3ヶ月前、6ヶ月前、12ヶ月前等の単位で記述）	３ヶ月前告知
			告知方法	Web及びメールにて告知
19		サービス（事業）変更・終了後の対応・代替措置	対応・代替措置の基本方針の有無と、「有り」の場合はその概要	不要 当社内に保存を目的とする情報は蓄積しない
20	契約の終了等	情報の返却・削除・廃棄	契約終了時等の情報資産（利用者データ等）の返却責任の有無と、受託情報の返還方法・ファイル形式・費用等	システムの仕様として、一定期間経過後に完全削除されます。
			情報の削除又は廃棄方法の開示の可否と、可能な場合の条件等	
			削除又は廃棄したことの証明書等の提供	
21	サービス料金	料金体系	初期費用額	初期費用額および月額利用額は別途定めるサービス提供価格表に、最低利用契約期間については約款第19条(解約)に記載。
			月額利用額	
			最低利用契約期間	
22		解約時違約金支払いの有無	解約時違約金（利用者側）の有無と、「有り」の場合はその額	なし
23		利用者からの解約事前受付期限	利用者からのサービス解約の受付期限の有無と、「有り」の場合はその期限（何日・何ヶ月前かを記述）	約款第19条(解約)に記載。
24		サービス稼働設定値	サービス稼働率の目標値	サービス稼働目標:99.0% サービス稼働実績: サービス停止事故歴:停止を伴う事故歴なし
			サービス稼働率の実績値	
			サービス停止の事故歴	
25		サービスパフォーマンスの管理	システムリソース不足等による応答速度の低下の検知の有無と、「有り」の場合は、検知の場所、検知のインターバル、画面の表示チェック等の検知方法	サービスの死活監視、およびシステムリソースを1分間隔で監視。 問題が生じた場合、オペレーションチームよりサービス状態確認ののち、担当者へ通知しております。
			ネットワーク・機器等の増強判断基準又は計画の有無、「有り」の場合は増強の技術的措置（負荷分散対策、ネットワークルーティング、圧縮等）の概要	システムリソースの冗長構成や、CDN(コンテンツ・デリバリー・ネットワーク)による一部コンテンツをキャッシュを実施しています。
26	サービス品質	認証取得・監査実施	プライバシーマーク（JIS Q 15001）等、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1 等）の取得、監査基準委員会報告書第18号（米国監査基準SSAE16、国際監査基準 ISAE3402）の作成の有無と、「有り」の場合は認証名又は監査の名称	ISO/IEC27001: 2013 JIS Q 27001:2014 認証証明番号:01734-2006-AIS-KOB-ISMS-AC 01733-2006-AIS-KOB-UKAS https://www.gmogshd.com/isms/ *2024年3月1日に、GMOグローバルサインHD株式会社からGMOグローバルサイン株式会社に事業移管を行ったため、次回更新監査の際には上記ISMSのスコープには含まれませんが、運用方法に変更はございません。
27		脆弱性診断	脆弱性診断の有無と、「有り」の場合は、診断の対象（アプリケーション、OS、ハードウェア等）と、対策の概要	アプリケーション・OS・ハードウェアレベルでの定期的及び改修時のツールを利用した診断を実施
28		バックアップ対策	利用者データのバックアップ実施インターバル	AWS基本機能にて、プログラム部、マスターデータのバックアップ お客様データ部はAWS S3の冗長化利用
			世代バックアップ（何世代前までかを記述）	
29		サービス継続	サービスが停止しない仕組み（冗長化、負荷分散等）	AWS基本機能
			DR（ディザスターリカバリー）対策の有無と、「有り」の場合はその概要	
30		SLA（サービスレベル・アグリーメント）	本サービスに係るSLAがサービス利用約款に添付されるか否か	なし（別途「オンライン本人確認サービス スマホde本人確認の品質保証」にて規定）
31	連携	他のASP・SaaSとの連携状況に関する情報提供	他のASP・SaaSとの連携の有無と、「有り」の場合は情報提供の条件等	有り（一部は一般開示） 別途追加の機密保持契約を締結した場合、かつ先方からの開示許可があるものに関して提供可能。
32		死活監視	死活監視の有無と、「有り」の場合は死活監視の対象	有り 外部からのサービス死活監視、内部での各リソースへの死活監視
33		時刻同期	時刻同期への対応の有無と、「有り」の場合は時刻同期方法	有り、NTPでの自動同期
34		ウイルス対策	ウイルス対策の有無	有り
35		管理者権限の運用管理	システム運用部門の管理者権限の登録・登録削除の手順の有無	有り（ISMS内部規定）
36		ID・パスワードの運用管理	事業者側にて、利用者のID・PWを付与する場合におけるIDやパスワードの運用管理方法の規程の状況	有り（サービス運用マニュアル）

37	セキュリティ	記録（ログ等）	利用者の利用状況の記録（ログ等）取得の状況と、その保存期間及び利用者への提供可否	利用ログ記録:有り 保存期間:年間 利用者への提供:ログ解読情報のみ システムログ:有り 保存期間:年間 改ざん防止:別システムにバックアップ有り
			システム運用に関するログの取得の有無と、「有り」の場合は保存期間	
			ログの改ざん防止措置の有無	
38		セキュリティパッチ管理	パッチ管理の状況とパッチ更新間隔等、パッチ適用方針	インフラ系セキュリティ管理ツールにて診断 サービス運用上問題がない場合に随時適用
39		暗号化対策	暗号化措置（データベース）への対応の有無と、「有り」の場合はその概要	データベースの一部をプログラムにて暗号化
ネットワーク				
40	回線	推奨回線	専用線（VPNを含む）、インターネット等の回線の種類	特になし
			ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲	
41		推奨帯域	推奨帯域の有無と、「有り」の場合はそのデータ通信速度の範囲	特になし
42		推奨端末	パソコン、携帯電話等の端末の種類、OS等	各デバイス、OSにて最新の状態のブラウザ Chrome、Edge、Firefox、Safari等
			利用するブラウザの種類	
43	セキュリティ	ファイアウォール	ファイアウォール設置等の不正アクセスを防止する措置の有無	
44		不正侵入検知	不正パケット、非権限者による不正なサーバ侵入に対する検知等の有無と、「有り」の場合は対応方法	有り、WAF利用
45		ユーザ認証	ユーザ（利用者）のアクセスを管理するための認証方法、特定の場所及び装置からの接続を認証する方法	ID/PWにて認証
46		なりすまし対策（事業者サイド）	第三者によるなりすましサイトに関する対策の実施の有無と、「有り」の場合は認証の方法	httpsによるSSL証明書での証明
47		暗号化対策	暗号化措置（ネットワーク）への対応の有無と、「有り」の場合はその概要	httpsによる暗号化 TLS 1.2、ECDHE_RSA とP-256、AES_128_GCM
ハウジング（サーバ設置場所）				
48	施設建築物	建物形態	データセンター専用建物か否か	AWS EAST JAPANリージョン https://d1.awsstatic.com/whitepapers/compliance/JP_Whitepapers/AWS_Risk_and_Compliance_Whitepaper_JP.pdf
49		所在地	国名、日本の場合は地域ブロック名（例:関東、東北）	
			特筆すべき立地上の優位性があれば記述（例:標高、地盤等）	
50		耐震・免震構造	耐震数値	
			免震構造や制震構造の有無	
51	非常用電源設備	無停電電源	無停電電源装置（UPS）の有無と、「有り」の場合は電力供給時間	
52		給電ルート	異なる変電所を経由した給電ルート（系統）で２ルート以上が確保されているか否か （自家発電機、UPSを除く）	
53		非常用電源	非常用電源（自家発電機）の有無と、「有り」の場合は連続稼働時間の数値	
54	消火設備	サーバルーム内消火設備	自動消火設備の有無と、「有り」の場合はガス系消火設備か否か	
55		火災感知・報知システム	火災検知システムの有無	
56	避雷対策設備	直撃雷対策	直撃雷対策の有無	
57		誘導雷対策	誘導雷対策の有無	
58		空調設備	空調設備（床吹き上げ空調、コンピュータ専用個別空調等）の内容	
59	セキュリティ	入退室管理等	入退室記録の有無と、「有り」の場合はその保存期間	
			監視カメラの有無	
			個人認証システムの有無	
サービスサポート				
60	サービス窓口 （苦情受付・問合せ）	連絡先	電話／FAX、Web、電子メール等の連絡先	契約時に契約経路、条件などによりお知らせします
			代理店連絡先の有無と、「有り」の場合は代理店名称、代理店の本店の所在地と連絡先	
61		営業日・時間	営業曜日、営業時間（受付時間）	平日（月～金、休祭日を除く）10:00～18:00
62		サポート範囲・手段	サポート範囲	サービス状況問い合わせ、障害問い合わせ、導入のための相談、一部技術サポート サポート手段は電子メールとします
			サポート手段（電話、電子メールの返信等）	
63	サービス通知・報告	メンテナンス等の一時的サービス停止時の事前告知	利用者への告知時期（1ヵ月前、3ヵ月前、6ヵ月前、12ヵ月前等の単位で記述）	1ヶ月前告知
			告知方法	Webまたはメール
64		障害・災害発生時の通知	障害発生時通知の有無と、「有り」の場合は通知方法及び利用者への通知時間	Webサイトにて告知
65		定期報告	利用者への定期報告の有無（アプリケーション、サーバ、プラットフォーム、その他機器の監視結果、サービス稼働率、SLAの実施結果等）	特になし