

オンラインストレージ業務に関する チェックシート兼報告書 ～手引き～

1. 報告書の入力にあたって

2. 入力要領

3. 確認事項

4. 用語の説明

当社委託業務の範囲内で顧客情報の取扱いを含む業務で外部事業者のサービスを利用する場合は、あらかじめ当社に報告する必要があります。

委託先において顧客情報の不適切な取扱いが行われないよう、委託先の選定や監督を行わなければなりません。



SOMPOひまわり生命

1. 報告書の入力にあたって

- 確認事項は全て、事業者について確認いただく事項です。
- 確認事項No.1～23が「○」となることで利用基準を満たします。
(★)の表記がある項目について確認時に「×」がある場合には、サービスを利用することが出来ません。
- クラウドサービスの利用に際しては、漏えいを防止するため、サービスの利用方法が大変重要であることから、以下の点にご留意ください。

- ① ID・PWの厳重管理
サービス利用のためのID・PWは、他人に知られることの無いよう厳重に管理する。
- ② IDの共有禁止
IDは1人につき1IDを利用することとし、複数人での共有は行わない。
- ③ PWの設定
誕生日等の推測されやすい数字や、ユーザーIDと同一のPWは避ける。
- ④ 顧客情報等の公開禁止
サービスによっては不特定多数のサービス利用者に対して掲載しているファイルを公開する機能があるが、このようなサービスでは顧客情報や機密性の高い情報を取扱わないこととする。
- ⑤ ファイルPWの設定
クラウドサービス上に顧客情報を含むファイルを保存する際は、ファイルPWを設定する。
- ⑥ 社外からのアクセス制限(推奨)
電子証明書やIPアドレス制御等により、代理店内で認めた端末以外からのアクセスを制御する。



SNSの利用は禁止です！

【 SNSの例 】LINE(個人用)、Facebook、Twitterなど。

SNSの利用に関しては、誤投稿・誤送信した場合に情報が拡散し非常に広範囲な漏えいに繋がること、また、サーバーの所在を含めセキュリティ対策の水準が不明な事も多く適切な管理が困難なことから、ひまわり生命では顧客情報を含む利用は禁止としています。

1

SOMPOひまわり生命保険株式会社 行		年	月	日
代理店名				
代表者・店主名				
<p>代理店業務で利用するオンラインストレージサービス(以下、クラウドサービス)について、下記の通り報告いたします。</p> <p>① クラウドサービスの利用にあたっては、会社の顧客情報取扱ルールを遵守するとともに、一切の責任を当番間で負担することと誓約いたします。</p> <p>また、代理店店長等の際に会社の請求があるときは、クラウドサービスの管理状況に係る記録等を提出いたします。</p>				
代理店コード	情報管理責任者	代理店確認記者	確認日	
			年	月
			日	

②

事業者名	契約時期		契約時期	
所在地	年	月	日	～ 年 月 日
連絡先	<input type="checkbox"/> 依頼の定めなし <input type="checkbox"/> または、自動更新 → <input type="text"/>			
利用するサービス名				

③

確認事項	No.	確認事項の具体的な内容	評価 ○ ×
有償サービスの利用	1	有償のクラウドサービスを利用する。(※) (有償は、利用することによって発生するサービスと見なす。例えば、登録保証期間の未料金が発生するサービスは有償には含まれません。)	
事業者の信頼性	2	クラウドサービスを提供する事業者は、ISMS認証や国際規格 ISO27001、クラウドサービス未対応 (ISO2013)、クラウドサービス (PaaS) 向け、個人情報保護法第 30 条第 2 項 (SaaS) 等を参照している、信頼できる事業者である。(※) (「取組の認証・規格など」(信頼性の根拠))	
	3	クラウドサービスの利用に際し、日本語による問合せ窓口がある。(※) (実際に問合せが可能である。)	
サポート・情報開示姿勢	4	システムトラブル等の障害発生時や外部・内部者の不正による情報漏えい事故の発生時、影響範囲などの事故情報の通知、再発防止などの協力が必要となることを確認できる。(※)	
	5	業務委託契約や利用規約に基づきサービス利用の通知は、双方の取り決めは日本語でなされている。(※)	
	6	業務委託契約書や利用規約などから、サービスレベルが適切に定められ、サービス内容に開示の内容と一致を確認できる。(※)	
サービスレベル	7	当該クラウドサービスが予定し停止する場合は事前通知期間は、定められている。(※)	
	8	当該クラウドサービスの保証レベル (SL) は定められており、業務上支障と見做される。(※) (※)保証レベルが「障害が少なく、障害発生しても迅速な対応と回復の保証がとれます」	

③

評価事項	取組事項	取組事項の具体的な内容	回答欄 ○ ×
セキュリティ対策	9	クラウドサービスにおけるセキュリティ対策が実施されていることがHP等で具体的に確認できる。	
	10	アカウントのログインをする際に、二段階認証の機能が提供されている。	
	11	操作ログの取得・保管機能がある。	
	12	データの保護に関するセキュリティ対策が実施されている。 データ保護に関するセキュリティ対策には以下の例があります。 ・保管データ、送信データの暗号化機能の提供。 ・データのバックアップ機能の提供。	
サービス終了時、利用終了時の条件	13	サービス終了時、利用終了時の連絡やデータが適切に管理されることを、業務委託契約書や利用約款などで確認し、内容に問題がないことを確認できる。(★)	
	14	クラウドサービス終了時に、データが必要なタイミングで取得できる。(★)	
	15	サービスの利用が終了時に、クラウドのシステム上に残るデータは確実に消去され、第三者による再利用や悪用が起らないよう対策されている。(★)	
	16	サービス終了は十分な期前期間をもって通知される。(★)	
リスクのリスク	17	日本企業もしくは、外国企業の日本法人がサービス提供者であり、紛争が生じた場合の準拠法は日本法である。(★)	
データの取扱い	18	データの管理責任は利用者側にあり、サービス事業者は利用者のデータに許可なくアクセスしないことと、業務委託契約書や利用約款などで定められている。(★)	
リスク管理・コンプライアンス	19	顧客情報を意図せずに他人に公開されてしまうような機能の利用(設定)はない、または当該機能を利用(設定)するが顧客情報は公開されずようなフォルダ等に搭載もしくは保存しない。(★)	
	20	クラウドサービス事業者は再委託をしていない。 〔再委託している場合〕 日本の法令に準拠した再委託先の管理・管理プロセスが定められており、内部監査、第三者監査で、そのプロセスの実効性が確認されている。(★)	
	21	事業者の所在地は国内である。 ※事業者が委託する委託先および最終の委託先まで含む、事業者の親会社等の支配先会社を含む。	
【海外データ移行】 委託データの海外移転の有無	22	データの保存先は国内である。	
	23	海外の事業者からデータにアクセスされることはない。 上記21～23のいずれかの項目に「×」がある場合は、海外移転審査の対象です。 【委託データの海外移転審査別記】が別途必要です。	

-2-

【3. 確認事項】

有償サービスの利用

No. 1

有償のクラウドサービスを利用する。(★)

(有償とは、利用することで料金が発生するサービスとします。例えば、容量拡張時のみ料金が発生するサービスは有償には含みません。)

○	<ul style="list-style-type: none">■ 有償のサービスを利用する。<ul style="list-style-type: none">・月額または年額等の利用料金が発生する。
×	<ul style="list-style-type: none">■ 有償のサービスを利用しない。■ 無料のサービスを利用する。<ul style="list-style-type: none">・サービスの利用に料金が発生しない。・ストレージ容量の拡張のみ料金が発生する。


事業者の信頼性

No. 2

クラウドサービスを提供する事業者は、ISMS認証や国際規格(ISO 27001)、クラウドサービスセキュリティ(ISO27017)、プライバシーマーク(Pマーク)、内部統制第三者評価(SOC2)等を取得している等、信頼できる事業者である。(★)

【確認のポイント】

事業者が認定等を取得しているかインターネット等で確認します。

○	<ul style="list-style-type: none">■ 認証や第三者評価等を取得している。
<div>○の場合</div> <div></div> <div>「取得済の認証名・規格名など信頼性の根拠」を入力してください。</div>	
×	<ul style="list-style-type: none">■ 取得していない。

【3. 確認事項】

サポート・情報開示姿勢

No. 3

クラウドサービスの利用に際し、日本語による問合せ窓口がある。

(★)

(実際に問合せが可能である。)

【確認のポイント】

海外の事業者が提供しているクラウドサービス等の場合、日本語によるヘルプデスクやサポートがあるかを確認します。

○

- 日本語による問合せ窓口がある。
- 日本語によるサポートを受けることができる。

×

- 日本語による問合せに対応していない。

サポート・情報開示姿勢

No. 4

システムトラブル等の障害発生時や外部・内部者の不正による情報漏えい事故の発覚時に、影響範囲などの事故情報の連絡、再発防止などへの協力が得られることを確認できる。(★)

【確認のポイント】

システムトラブルや漏えい事案等の不測の事態が発生した際に、復旧までの見込み時間や情報提供の方法等、事業者との連絡体制やサポート体制が整っていることを確認します。

○

- サポート体制が整っている。
- 事業者の協力が得られる。

×

- サポート体制が整っていない。
- 協力が得られない。

【3. 確認事項】

サポート・情報開示姿勢

No. 5

業務委託契約や利用約款に基づくサービス利用の場合は、双方の
取り決めは日本語でされている。(★)

○	<ul style="list-style-type: none">■ 取り決めは日本語でされている。・委託契約内容や利用約款を日本語で確認できる。
×	<ul style="list-style-type: none">■ 取り決めが他国語でされている。■ 取り決め内容が日本語で確認できない。

サービスレベル

No. 6

業務委託契約書や利用約款などから、サービスレベルが適切に定
められ、サービス内容に問題のないことを確認できる。(★)

【確認のポイント】

利用するサービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービスレ
ベルが示されているか確認します。

○	<ul style="list-style-type: none">■ サービス内容に問題はない。■ サービスレベルが定められている。
×	<ul style="list-style-type: none">■ サービス内容に問題がある。■ サービスレベルが定められていない。

【3. 確認事項】

サービスレベル

No. 7

当該クラウドサービスが予告して停止する場合の事前周知期間は、定められている。(★)

【確認のポイント】

クラウドサービスがメンテナンス等により停止する場合に、利用者に対して周知期間が十分であるか、事前に知る方法が示されている等、不都合が生じる恐れがないかを確認します。

○

- 事前周知期間が定められている。
- 事前周知期間が十分にある。

×

- 周知期間が定められていない。

サービスレベル

No. 8

当該クラウドサービスの保証稼働率(※)は定められており、業務上受入れ可能である。(★)

(※)保証稼働率が高ければ、障害が少ない、障害があっても復旧までの時間が短いといえます。

○

- 保証稼働率が定められている。
・業務上支障がない稼働率となっている。

×

- 保証稼働率が定められていない。
- 現在の稼働率では業務に不都合が生じる。

【3. 確認事項】

セキュリティ対策

No. 9

クラウドサービスにおけるセキュリティ対策が実施されていることがHP等で具体的に確認できる。

【確認のポイント】

ウィルス感染や不正アクセスへの対策、データセンターの防犯設備等のセキュリティ対策をHP等で確認します。



■ セキュリティ対策の実施を確認できる。

- ・事業者のHP等にセキュリティ対策について明記されている。
- ・クラウド事業者のセキュリティ報告書等で確認できる。



■ セキュリティ対策の実施が確認できない。

- ・事業者のHP等にセキュリティ対策について明記されていない。

セキュリティ対策

No. 10

アカウントのログインをする際に、二段階認証の機能が提供されている。

【確認のポイント】

クラウドサービスやサイトにログインをする際には二段階の認証を行うことになっているかを確認します。



■ 二段階認証の機能がある。



■ 二段階認証の機能がない。

【3. 確認事項】

セキュリティ対策

No. 11

操作ログの取得・保管機能がある。

【確認のポイント】

クラウドサービスにアクセスしたアカウント等の操作履歴を記録する機能があるか確認します。



■ ログ取得・保管機能がある。

・クラウドサービスへのアクセスや操作履歴を記録する機能がある。



■ ログ取得・保管機能がない。

・クラウドサービスへのアクセスや操作履歴を記録できない。

セキュリティ対策

No. 12

データの保護に関するセキュリティ対策が実施されている。

データ保護に関するセキュリティ対策には以下の例があります。

- ・保管データ、通信データの暗号化機能の提供。
- ・データのバックアップ機能の提供。

【確認のポイント】

クラウドに保管するデータの暗号化の自動実施や、事業者側での自動バックアップ等の対策が実施されているか確認します。



■ データ保護のセキュリティ対策が実施されている。

- ・データを暗号化する機能が備えられている。
- ・事業者による定期的なバックアップがされている。



■ データ保護のセキュリティ対策が実施されていない。

- ・事業者によるクラウドデータのバックアップがされていない。

【3. 確認事項】

サービス終了時、利用終了時の条件

No. 13

サービス終了時、利用終了時の連絡やデータが適切に管理されることを、業務委託契約書や利用約款などで確認し、内容に問題がないことを確認できる。(★)

【確認のポイント】

クラウドサービスの利用を終了する場合に、利用者に対する連絡やデータの取扱いについて契約書等に定められているか確認します。



- 内容に問題がないことを確認できる。
- 業務委託契約書や利用約款等に定められている。



- 内容に問題がある。
 - ・サービス終了時について保証されていない。
- 業務委託契約書や利用約款等に記載がない。

サービス終了時、利用終了時の条件

No. 14

クラウドサービス終了時に、データが必要なタイミングで取得できる。(★)

【確認のポイント】

クラウドサービスの利用を終了する場合に、クラウドに預けているデータを自社内のシステムに戻したり、他のサービス事業者に預けなおしたりする必要があるため、利用者が必要なタイミングでデータを確保することができるか確認します。



- 取得できる。
 - ・データを確保するための期間が設けられている。



- 取得できない。
 - ・データを確保するための期間が設けられていない。

【3. 確認事項】

サービス終了時、利用終了時の条件

No. 15

サービスの利用が終了時に、クラウドのシステム上に残るデータは確実に消去され、第三者による再利用や悪用が起こらないよう対策されている。(★)

【確認のポイント】

クラウドサービスの利用を終了する場合に、クラウド上の保管データが確実に消去され、復元されたり再利用されたり流出したりすることが起こらないことが保証されているか確認します。



■ データの消去等により対策されている。
・クラウドのシステム上に残るデータは確実に消去される。



■ 対策されていない。
・クラウドのシステム上に残るデータは消去されない。

サービス終了時、利用終了時の条件

No. 16

サービス終了は十分な猶予期間をもって通知される。(★)

【確認のポイント】

利用しているサービスが終了する際には、事前に通知されることになっているか確認します。



■ 十分な猶予期間をもって通知される。



■ 猶予期間が十分ではない。
■ 事前に通知されない。

【3. 確認事項】

法的リスク

No. 17

日本企業もしくは、外国企業の日本法人がサービス提供者であり、紛争が生じた場合の準拠法は日本法である。(★)

【確認のポイント】

海外の事業者が提供しているクラウドサービス等の場合、利用に際して紛争が生じた場合には日本法が適用されるか確認します。

○

■ 日本法である。

×

■ 日本法ではない。
・外国企業の母国法となっている。

データの取扱い

No. 18

データの管理責任は利用者側にあり、サービス事業者は利用者のデータに許可なくアクセスしないことを、業務委託契約書や利用約款などで定められている。(★)

○

■ 契約書や約款等で定められている。
・事業者は利用者のデータにアクセスしないことを定めている。

×

■ 契約書や約款等で定められていない。
・事業者が利用者のデータにアクセスすることが可能となっている。

【3. 確認事項】

リスク管理・コンプライアンス

No. 19

顧客情報が意図せずに他人に公開されてしまうような機能の利用(設定)はない、または当該機能を利用(設定)するが顧客情報は公開されてしまうようなフォルダ等に掲載もしくは保存しない。(★)

【確認のポイント】

Web公開機能等により、アカウントを所持しないユーザーにもファイル等を提供することができる機能がないか確認します。

○	<ul style="list-style-type: none">■ 公開機能の利用はない。■ 公開機能を利用するが顧客情報は保存しないよう定めている。
×	<ul style="list-style-type: none">■ 公開機能のあるフォルダに顧客情報を保存する。

リスク管理・コンプライアンス

No. 20

クラウドサービス事業者は再委託をしていない。

○	<ul style="list-style-type: none">■ 再委託をしていない。■ 再委託をしない規程となっている。
×	<ul style="list-style-type: none">■ 再委託をする。 ・事業者がさらに外部の会社へ業務委託をする。

×の場合



日本の法令に準拠した再委託先の審査・管理プロセスが定められており、内部監査、第三者監査で、そのプロセスの実効性が検証されている。(★)

○

×

【3. 確認事項】

委託データの海外移転の有無

No. 21

事業者の所在地は国内である。

※事業者が委託する委託先および最終の委託先まで含む。事業者の親会社等の支配会社を含む。

○	■ 委託先の事業者の所在地は国内である
×	■ 委託先の事業者の所在地は海外である

×の場合



委託データの海外移転審査別紙の提出が必要。
海外事業者名・外国名および委託先の海外事業者における安全管理措置を含む個人情報取扱事業者としての措置の実施状況を別途報告。

委託データの海外移転の有無

No. 22

データの保存先は国内である。

○	■ 国内で保存 ・国内でデータ保存、管理を行っている
×	■ 海外で保存 ・国外でデータ保存、管理を行っている

×の場合



委託データの海外移転審査別紙の提出が必要。
海外事業者名・外国名および委託先の海外事業者における安全管理措置を含む個人情報取扱事業者としての措置の実施状況を別途報告。

【3. 確認事項】

委託データの海外移転の有無

No. 23

海外の委託先からデータアクセスされることはない。

○	■ 国内で保存 ・国内でデータ保存、管理を行っている
×	■ 海外で保存 ・国外でデータ保存、管理を行っている

× の場合



委託データの海外移転審査別紙の提出が必要。
海外事業者名・外国名および委託先の海外事業者における安全管理措置を含む個人情報取扱事業者としての措置の実施状況を別途報告。

【3. 確認事項】

参考：委託データの海外移審査別紙

委託データの海外移審査別紙

①

SOMPOひまわり生命保険株式会社 行
 代理店名
 代表者・店主名

年 月 日

以下の確認事項についてご回答ください。

②

海外移審査用確認事項	回答欄
(1) 移転先の海外事業者名(再委託先等の場合を含む。)を記載してください。	
(2) 外国名(再委託先等の場合を含む。)を記載してください。	
(3) 委託先の海外事業者における安全管理措置を含む個人情報取扱事業者としての措置の実施状況 ① OECDプライバシーガイドライン(8原則)に対応する措置の実施状況(注1) 下記1)～8)全て対応できていますか？対応できていない項目がありますか？ 1) 収集制限の原則 2) データ内容の原則 3) 目的明確化の原則 4) 利用制限の原則 5) 安全保護の原則 6) 公開の原則 7) 個人参加の原則 8) 責任の原則 ② 基準適合体制整備事業者の要件をすべて充足していますか？(注2) ※個人情報保護委員会の法令・ガイドライン等 (https://www.ppc.go.jp/personalinfo/legal/)の「個人情報の保護に関する法律」についてのガイドライン(外国にある第三者への提供編)令和4年4月1日施行の「4. 個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制の基準」 ③ 安全管理措置対策 ※同法令・ガイドライン等の「個人情報の保護に関する法律」についてのガイドライン(通則編)令和4年4月1日施行の「8(別添)講ずべき安全管理措置の内容」	【該当する方に○を入力】 () 全て対応できている。 () 対応できていない項目がある。 【上記で対応できていない項目がある場合、以下に項目番号を記載】 【該当する方に○を入力】 () 全て対応できている。 () 対応できていない項目がある。 【上記で対応できていない項目がある場合、以下に項目を記載】
(4) (任意) 添付資料があれば資料名を記載ください。(委託契約書、プライバシーポリシー、点検・監査結果等)(注3)	

①	代理店情報を入力します。	■ 報告日、代理店名、代表者・店主名
②	海外移審査用確認事項を確認し、内容を入力します。	■ (1)～(3)を漏れなく回答します。 ※海外移審査用確認事項欄の注釈については次頁に説明あり

【3. 確認事項】

参考：委託データの海外移審査別紙

【OECDプライバシーガイドライン8原則と個人情報保護法の対応】

・以下のとおり、日本の個人情報保護法の各対応条項の内容を充足していれば、そのOECD原則に対応していることと考えることができます。

OECD 8 原則	個人情報保護法
①収集制限の原則	適正な取得(第17条) 取得に際しての利用目的の通知等(第18条)
②データ内容の原則	利用目的による制限(第16条) データ内容の正確性の確保(第19条)
③目的明確化の原則	利用目的の特定(第15条)
④利用制限の原則	利用目的による制限(第16条) 第三者提供の制限(第23条)
⑤安全保護の原則	安全管理措置(第20条) 従業員の監督(第21条) 委託先の監督(第22条)
⑥公開の原則	保有個人データに関する事項の公表等(第27条)
⑦個人参加の原則	開示(第28条)訂正等(第29条) 利用停止等(第30条) 理由の説明(第31条) 開示等の請求等に応じる手続き(第32条) 手数料(第33条)
⑧責任の原則	個人情報取扱事業者による苦情の処理(第35条)

※OECDのWebサイト

<https://www.oecd.org/digital/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm>

【3. 確認事項】

参考: 委託データの海外移審査別紙

基準適合体制整備事業者の要件

個人情報保護法第4章第1節(2022年4月1日以降においては第2節)の以下の規定の趣旨に沿った措置をすべて講じていることが要件となります。

第15条	利用目的の特定(2022年4月1日以降においては第17条。以下括弧記載について同様)
第16条	利用目的による制限(第18条) (不適正な利用の禁止 第19条)
第17条	適正な取得(第20条)
第18条	取得に際しての利用目的の通知等(第21条)
第19条	データ内容の正確性の確保等(第22条)
第20条	安全管理措置(第23条)
第21条	従業員の監督(第24条)
第22条	委託先の監督(第25条) (漏えい等の報告等 第26条)
第23条	第三者提供の制限(第27条)
第24条	外国にある第三者への提供の制限(第28条)
第27条	保有個人データに関する事項の公表等(第32条)
第28条	開示(第33条)
第29条	訂正等(第34条)
第30条	利用停止等(第35条)
第31条	理由の説明(第36条)
第32条	開示等の請求等に応じる手続(第37条)
第33条	手数料(第38条)
第35条	個人情報取扱事業者による苦情の処理(第40条)

【4. 用語の説明】

「委託」とは

- ・ 目的の達成に必要な範囲内において、代理店内で処理できない業務や委託したほうが効率や効果が期待できる業務を外部に任せる行為です。
本書内では「委託元＝代理店」「委託先＝外部企業」を意味します。

「顧客情報」とは

- ・ 顧客に関する情報であって、個人・法人を問わず、特定の顧客を識別できるものです。
※「顧客」には契約者・被保険者のみならず相続人や見込客も含まれます。

「準拠法」とは

- ・ 準拠法というのは、その契約書に関する争いや解釈について疑義が生じたような場合に、どの国の法律を適用するかという問題です。

「プライバシーマーク制度」とは

- ・ プライバシーマーク制度は、事業者が個人情報の取扱いを適切に行う体制等を整備していることを評価し、その証として“プライバシーマーク”の使用を認める制度です
【日本情報経済社会推進協会】https://privacymark.jp/certification_info/index.html

「ISMS制度(ISO27001)」とは

- ・ ISMS適合性評価制度は、国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者適合性評価制度です。
【情報マネジメントシステム認証センター】<https://isms.jp/index.html>

「クラウドサービスセキュリティ(ISO27017)」とは

- ・ ISO27017認証とは、クラウドサービスの提供や利用に対して適用されるクラウドセキュリティの第三者認証です。
※ISMS認証を補完する位置づけの規格であり、前提としてISMS認証の取得が必要です。

＜参考＞ 「ISMS・ISO」および「プライバシーマーク」の付与状況は下記のサイトで確認することができます。
【ISMS・ISO】情報マネジメントシステム認証センター
<https://isms.jp/index.html>
【プライバシーマーク】日本情報経済社会推進協会
https://privacymark.jp/certification_info/index.html

「二段階認証」とは

- ・ ID・パスワード入力の他に、アプリでのログイン可否の選択や、セキュリティコードの入力を追加することで、利用者以外が不正に情報にアクセスすることを防止する仕組みです。