

クラウドサービス利用時の注意

- ✓ 昨今、クラウドサービスが不正アクセス被害を受け、クラウドサービス内のデータ等が暗号化されたり、漏えいのおそれが生じたりする事案が複数発生しています。
- ✓ クラウドサービス利用時の注意点を確認の上、適切な管理に努めていただくようお願いします。

1. クラウドサービスの不正アクセス被害によるリスク

近年、クラウドサービスにおける不正アクセス被害・情報漏えい事故が増加しており、個人情報保護委員会から注意喚起※が発信されました。クラウドサービス利用が広がる一方で、利用者としてのサービス選択の責任・規約の理解・契約後の委託先の監督の重要性が高まっています。

クラウドサービスが不正アクセスを受けた場合、大量の顧客情報漏えい・お客様の二次被害が発生する可能性があります。

また、クラウドサービスの利用中断や情報の滅失による代理店業務の停止、信頼低下による顧客離れ、損害賠償請求等、経済的損失のリスクも高く、お客様の大切な情報を取扱う事業者として、慎重なサービス選択・利用が求められています。

個人情報保護委員会 注意喚起の要点

サービスの機能やサポート体制のみならず、セキュリティ対策についても十分理解・確認の上サービスを選択すること

必要かつ適切な安全管理措置（個人データの取扱いに関する責任範囲を含む）の合意内容を、規約や契約等でできるだけ明確化すること

セキュリティ対策を含めた安全管理措置の状況について、定期的に報告を受ける等の方法により確認すること

※個人情報保護委員会「クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点に関する注意喚起について」
https://www.ppc.go.jp/news/careful_information/240325_alert_cloud_service_provider/



2. クラウドサービス利用時の注意点

利用にあたっては以下の点に注意し、顧客情報の漏えい防止に努めていただくようお願いします。

✓ クラウドサービス利用は、外部委託です！

クラウドサービス事業者が提示する「利用規約」への同意の契約形態であっても、外部委託となります。代理店内で委託先選定基準を定め、基準に従って委託先を選定しなければなりません。

✓ 事前に当社への報告が必要です！

当社が代理店様に取扱いを委託した顧客情報を、クラウドサービスで利用・保管等する場合、事前に当社への報告が必要です。



✓ 委託先に対する定期的な監督が必要です！

委託先（クラウドサービス事業者）において顧客情報の不適切な取扱いがされないよう、契約後においても、定期的にまたは随時に、委託先選定基準に定めた事項や安全管理措置の順守状況を確認する等で、委託先の監督が必要です（個人情報保護法第25条）。情報漏えいが発生した際、委託元の委託先に対する監督が不十分だった場合は、委託元として責任が問われる場合があります。

当社への報告方法やチェックシート等、詳細は『代理店顧客情報取扱マニュアル（CHAPTERIV 個人データの安全管理措置 ⑦委託先の監督）』を参照いただくようお願いします。 掲載場所：ひまわり掲示板>規程・マニュアル>代理店顧客情報取扱マニュアル



代理店のみなさまへのおねがい

万が一サイバー攻撃（おそれを含む）※を受けた場合、被害の拡大防止・お客様の情報を守るため、速やかに当社担当者へご連絡をお願いいたします！

※ランサムウェア等のウイルス感染、不正アクセスによる被害のほか、サポート詐欺、フィッシングサイトによるID・パスワード等の詐取被害等も含みます。サイバー攻撃による個人情報漏えい（おそれも含む）は、当局報告の対象になります。

eラーニングの動画もぜひ視聴ください！

