



## JIPDECセミナー

# 「個人情報のクラウド保管 実務における対応ポイント」講演資料

### 講演資料02

## 「クラウドサービスと個人情報保護の実務」

本資料は、2023年9月5日（火）開催、JIPDECセミナーで配布した資料です。セミナーお申込み者様限定での配布となりますので、WEB、SNS等への掲載、転載はご遠慮ください。

また、本セミナー（資料）は、プライバシーマークの構築運用指針を解説するものではありません。

# クラウドサービスと個人情報保護の実務

アマゾン ウェブサービス ジャパン合同会社

公共部 法務統括 笹沼 穰 / 公共政策部 矢野 敏樹

# 自己紹介

- 笹沼穰

- 第一東京弁護士会所属の外国法事務弁護士。ニューヨーク州、ニュージャージー州弁護士登録。ニュージャージー州裁判所、ニューヨーク法律事務所勤務を経て16年にAWSに入社。19年より現職。

- 矢野敏樹

- 1997年弁護士登録。法律事務所、米ニューヨーク大学ロースクール留学（著作権情報センターCRIC在外研究員）、外務省（知的財産室）及びグーグルアジア太平洋地域公共政策部カウンセルなどを経て、19年より現職。

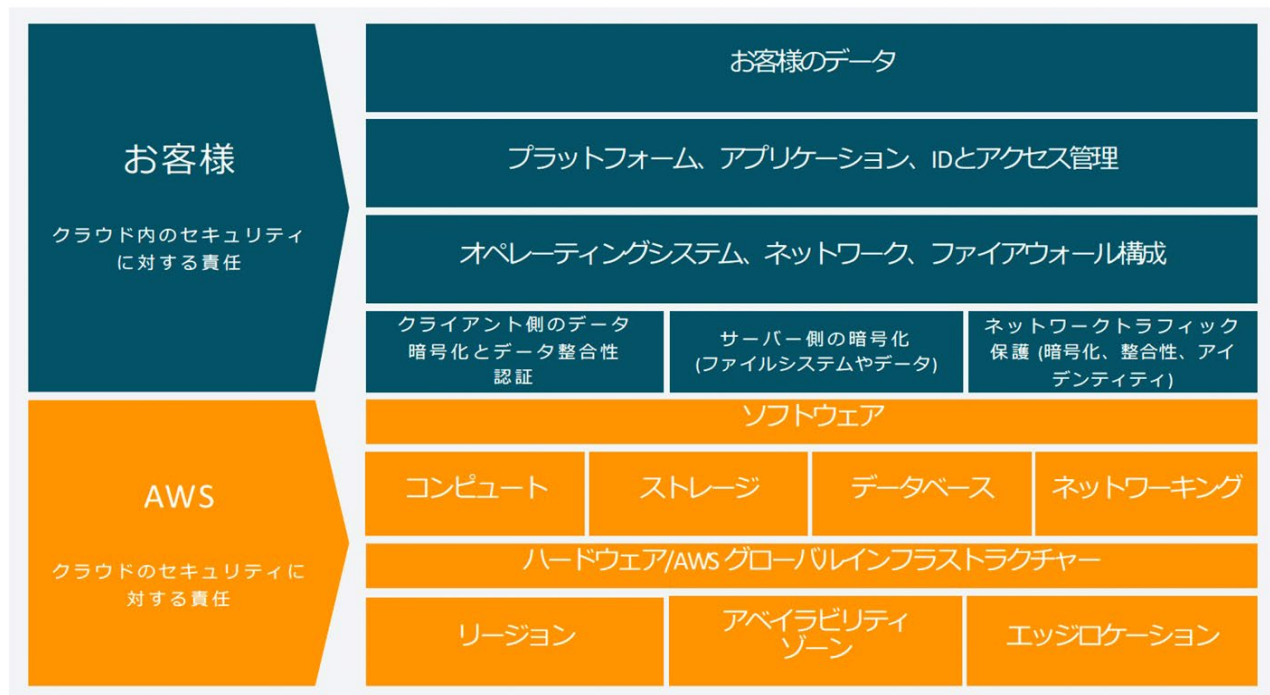
# クラウドサービス導入にあたる個人情報保護関連の論点

- クラウドサービスの利用は個人情報の第三者提供および越境移転にあたるか
- 米国CLOUD法によるデータアクセスのリスク
- 今後のクラウド普及に向けた課題

# クラウドサービスとは

- セルフサービスが重要な概念
  - インターネット経由で（いつでもどこからでも）
  - 従量課金で提供される（利用した分だけ払う）
  - オンデマンドの（電気スイッチみたいなもの）
  - ストレージ、暗号化等のITリソース（全ての利用者に同一のサービス）
- メリットは、デジタル・トランスフォーメーション（DX）の加速
  - コスト最適化
  - 最新の技術
  - 本来業務への集中
  - セキュリティへの投資 など

# 責任共有モデル



- いわゆるハイパースケールのクラウドを利用する場合の考え方として一般的になっている
- クラウド事業者側は、Security of the cloudであるインフラ部分の責任を負う
- クラウドサービスを利用する側が、クラウド内のデータやアクセス権限、アプリケーション開発などにSecurity in the cloudについて担当する








# 責任範囲は異なり得るが、考え方の基本は「責任共有モデル」

アプリケーション作成	アプリケーション作成	アプリケーション作成	アプリケーション作成
スケールアウト設計	スケールアウト設計	スケールアウト設計	スケールアウト設計
定形運用設計	定形運用設計	定形運用設計	定形運用設計
ミドルウェアパッチ	ミドルウェアパッチ	ミドルウェアパッチ	ミドルウェアパッチ
ミドルウェア導入	ミドルウェア導入	ミドルウェア導入	ミドルウェア導入
OSパッチ	OSパッチ	OSパッチ	OSパッチ
OS導入	OS導入	OS導入	OS導入
HWメンテナンス	HWメンテナンス	HWメンテナンス	HWメンテナンス
ラッキング	ラッキング	ラッキング	ラッキング
電源・ネットワーク	電源・ネットワーク	電源・ネットワーク	電源・ネットワーク
オンプレミス	独自構築 on EC2	マネージドサービス	サーバーレス アーキテクチャ
開発者が担当	AWSが担当		

- クラウド事業者側が「責任」外について何もしないと断言しているのではない
- トレーニングやベストプラクティスの提供、政府や団体との協働によるガイドブック作成支援等、多様な活動を提供

ID管理、データ保護、複数データセンターによる高可用性確保の要請や稼働状況のダッシュボード表示なども責任共有モデルから考えると、「どうしてそうなるのか」分かりやすい

# クラウドのセキュリティに対する責任：認証レポート

No.	認証ロゴ	レポート名	概要
1		AWS System & Organization Control (SOC)	AWS System & Organization Control (SOC) レポートは、独立したサードパーティーによるコンプライアンスの審査報告書です。このレポートは、セキュリティ統制（セキュリティ、可用性、機密性、プライバシー）の外部監査報告や実証結果を含んでいます。
2		ISO27001	ISO/IEC 27001は、情報セキュリティマネジメントシステム（ISMS）に関する国際規格です。情報の機密性・完全性・可用性の3つをバランスよくマネジメントし、情報を有効活用するための組織の枠組みを示します。
3		ISO27017	ISO/IEC 27017は、クラウドサービスに関する情報セキュリティ管理策のガイドライン規格です。情報セキュリティ全般に関するマネジメントシステム規格であるISO/IEC 27001の取り組みをISO/IEC 27017で強化することで、クラウドサービスにも対応した情報セキュリティ管理体制を構築することができます。
4		ISO27018	ISO27018認証とは、クラウドサービス事業者がパブリッククラウド上で管理する個人情報の保護に焦点を当てた国際規格です。仮想空間で実施する個人情報保護の実践規範として位置づけられる本規格に基づく認証を取得することで、各事業者は、個人情報の取り扱い方法における正確性やシステムの堅牢性、運用における透明性などにおいて、世界標準に準拠しているということを宣言できることとなります。
5		ISMAP	政府情報システムのためのセキュリティ評価制度 (ISMAP) は、パブリッククラウドサービスのセキュリティを評価するための日本政府のプログラムです。ISMAP の目的は、クラウドサービスプロバイダー (CSP) にとって共通の一連のセキュリティ標準が、政府調達のためのベースラインとなる要件を満たせることにあります。ISMAP は、クラウドサービスプロバイダーが実装する必要があるクラウドドメイン、運用、および手順のセキュリティ要件を規定します。
6		FedRAMP	FedRAMP (Federal Risk and Authorization Management Program) は、セキュリティ基準の中で最も高度なものの1つです。FedRAMPは、クラウドソフトウェアプロバイダーの評価、認可、監視を行う米国政府の取り組みとして運営されており、クラウドコンピューティング調達の際には、政府機関の機密データを高度な基準で保護されるように設計されています。
7		NIST 800-53 (NIST CSF)	NIST SP 800-53 (連邦政府情報システム、および連邦組織のためのセキュリティ管理策とプライバシー管理策) は、米国連邦政府の内部セキュリティ基準を示すガイドラインで、日本国内の各組織も無視できないガイドラインです。



# クラウドサービスの利用

- クラウド事業者はすべての利用者に同一の多種多様なサービスを提供



- 利用者は同じサービスをそれぞれの目的で利用

- ・ ホームページの構築
- ・ 個人情報の保存



- 利用者が自己のニーズに合った構築をする

- ・ 公開する写真は暗号化しない
- ・ 機密性の高い情報は暗号化



## 頻出論点：クラウドを使うことが個人情報上の第三者提供等に当たるか？

- クラウド事業者が個人データを「取り扱わない」こととなっている場合には「提供」にも「委託」にも該当しない（[個人情報保護委員会Q&A 7-53](#)）
  - ①契約条項によってクラウド事業者がサーバに保存された個人データを取り扱わない旨定められており、②適切にアクセス制御を行っている場合等
  - 参考：「取り扱わない」とは、①個人データへのアクセスを契約条項で禁止、②当該データ内容を適正に暗号化するなどして判読不能にすることが考えられる（岡村久道「個人情報保護法（第4版）」（2022年商事法務）313頁、下線は講演者が付記）
- 個人データの越境移転規制についても同様の考え方（[同Q&A 12-3](#)）
- 参考：「一般的には、利用するクラウドサービスが、IaaS（Infrastructure as a Service）の場合には通常委託又は第三者提供に該当しないが、SaaS（Software as a Service）の場合には、クラウドサービス提供事業者が個人データを取り扱うことが前提とされており、特別な事情がない限り委託又は第三者提供に該当すると考えられる。」との見解あり（渡邊涼介「データ利活用とプライバシー・個人情報保護（第2版）」（2023年）109頁など）。

# クラウドにおける個人情報チェックポイント

- Q&A 7-53のいわゆるクラウド例外に該当するか
  - 契約条項にクラウド事業者が個人データを取り扱わない旨が定められているか
    - 例：AWSカスタマーアグリーメント1.4条:「アマゾン...利用者コンテンツにアクセス...しない」
  - 適切にアクセス制御が行われているか
    - 責任共有モデルに基づいて、利用者側でデータの暗号化やアクセス制御を実現
    - クラウド事業者から暗号化ツール（例：AWS KMS）やアクセス管理ツール（例：AWS IAM)が提供されていることが多いので、利用を検討
- クラウド例外に該当すると、自社で管理しているのと同じこととなる（＝自ら適切な安全管理措置を講じる必要）

## 頻出論点 2 : 米国CLOUD法について

- 2018年に施行されたClarifying Lawful Overseas Use of Data法の略称
- 誤解：「米国籍のクラウド事業者が提供するクラウドサービスを利用してデータを保存すると、米CLOUD法によってデータが米国政府に筒抜けになる」
  - 米CLOUD法は**犯罪の証拠**であるデータへの**裁判所令状に基づく**アクセスを規定
  - 令状の発行には具体性が求められ、「探し出し」は認められない
  - 米国と接点がある**日本のクラウド事業者も対象となり得る** (米国司法省の見解)
- 米クラウド法にクラウド事業者がどう対応するのかを確認することが重要
  - 米政府の要請に対し法的異議申立てをするか
  - クラウド事業者は利用者に対して当局からの要求があったことを通知するか
  - 開示要請対応方針について白書等で情報公開しているか
- 日本政府の見解も参考
  - 2022年3月及び同年11月の衆院での国会答弁

## クラウド普及に向けた更なる課題（詳しくは座談会パートで）

- クラウドに応じた個人情報保護法の解釈について
- 新しいトピック（例えば生成AIサービスやPrivacy Enhancing Technologies, PETs）と個人情報保護法の関係について

The logo for JIPDEC features the word "JIPDEC" in a bold, black, sans-serif font. A solid red circle is positioned above the letter "I", serving as a distinctive dot or accent. The letters are closely spaced and centered horizontally on the page.

**JIPDEC**