

## 【個別テーマ】②

### 「クラウドサービスの法的責任と契約上の留意点」

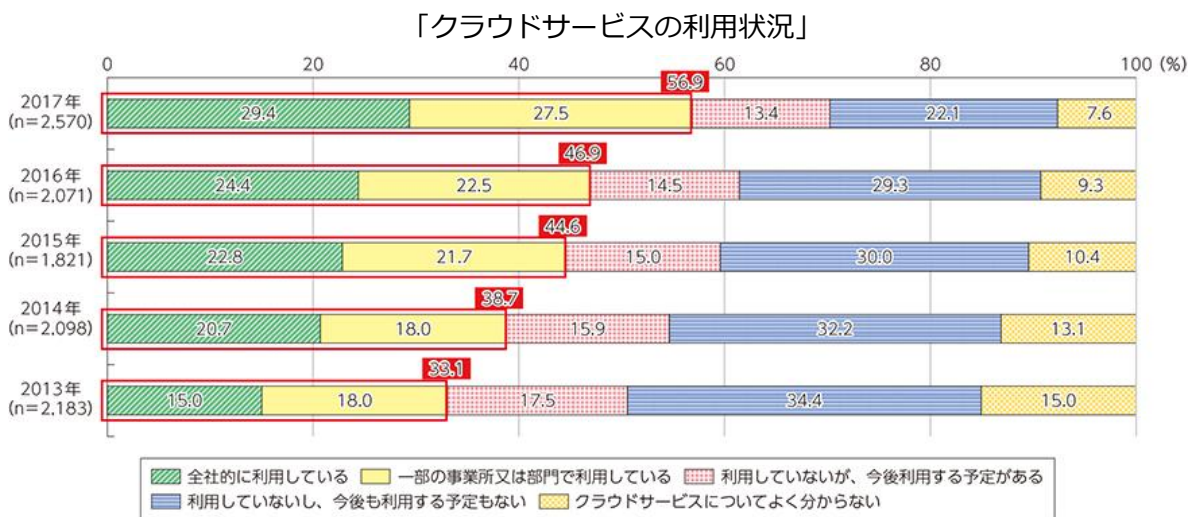
#### 1.はじめに

改正民法の考察でも概観した通り、現行民法制定時にはウェブサービスは影も形も無かったが、今では各種クラウドサービスの利用が急速に増加してきている。低コストで導入可能なクラウドサービスは、特に経営資源が限られた中小企業にとってメリットが大きいと考えられるが、一方で、クラウドサービスを利用することによる新たなリスクも発生している。本稿では、情報セキュリティの観点等から、クラウドサービスのリスクを整理したうえで、過去の事例や民法改正も踏まえて、クラウドサービスの利用における法律上の論点を整理するとともに、契約上の留意点を検討した。

#### 2.クラウドサービスの利用状況

##### (1) クラウドサービスの普及状況

クラウドサービスを一部でも利用している企業の割合は一貫して増加傾向にあり、2017年には半数以上に増加している。



出展：総務省「平成 30 年版 情報通信白書」

## (2) クラウドサービス利用増加の背景

クラウドサービスを利用している理由としては、「資産、保守体制を社内に持つ必要がないから」がトップであり、初期導入コストの安さや運用・保守体制が不要などの点が利用増加の背景と考えられる。経営資源が限られている中小企業にとっては、クラウドサービスを利用するメリットが特に大きいと考えられる。

### 「クラウドサービスを利用している理由」

	(%)
	2017年(n=1,561)
資産、保守体制を社内に持つ必要がないから	45.2
どこでもサービスを利用できるから	34.8
安定運用、可用性が高くなるから(アベイラビリティ)	32.6
災害時のバックアップとして利用できるから	32.4
サービスの信頼性が高いから	29.4
システムの容量の変更などが迅速に対応できるから	27.4
システムの拡張性が高いから(スケーラビリティ)	23.4
既存システムよりもコストが安いから	21.2
システムベンダーに提案されたから	14.8
その他	8.4

出展：総務省「平成 30 年版 情報通信白書」

## (3) クラウドサービスの問題点

クラウドサービスの利用が増加する一方で、下表に示すような情報漏えい、サービス停止などの事件・事故等が過去から継続的に発生している。今後、さらにクラウドサービスの種類や事業者数が増加していくことが想定される中、クラウドサービスを利用するにあたっては、考慮すべきリスクが存在すると考えられる。

### 「クラウドサービスにおける事件・事故の例」

事件・事故	内 容
AWS障害	2019年8月23日、Amazon AWS 東京リージョンの単一AZで、一部EC2サーバの停止が発生、多くの企業のサービスが影響を受けた。 冷却システムの故障に因るサーバのオーバーヒートが原因。
Jip-Base障害	2019年12月4日、自治体専用IaaSサービス「Jip-Base」で障害。多くの自治体でシステム利用不可、データ消失が発生。ファームウェアの不具合に因るストレージコントローラーの障害が原因。

個人情報漏えい (ソニー)	2010年4月、PlayStation Networkのサーバに対する不正アクセスで、約7700万人の個人情報が流出。
サービス終了	2008年10月末、プロの写真家が使用する写真アーカイブおよびコマースサイトであるDigital Railroadが、警告なしにサービスを終了。ユーザはサイトに保存された画像を回復するのに48時間しかなかった。

#### (4) クラウドサービスの特徴とメリット、リスク

クラウドサービスを利用することで、迅速にサービスを導入できたり、初期導入コストを削減できたりする等、IT利活用にかかる時間・コストの削減が可能となる。

その反面、クラウドサービスのブラックボックス化が進むとクラウドベンダ依存となり、提供されるクラウドサービスの内容や利用規約等についての理解が不十分な場合には、情報セキュリティなどのリスクが高まる可能性がある。

特徴	メリット	リスク
<ul style="list-style-type: none"> <li>サーバやソフトウェア等は所有せず利用</li> <li>インターネットを通じてどこからでも利用可能</li> <li>リソースを他社と共有することで効率化</li> </ul>	<ul style="list-style-type: none"> <li>迅速なサービスの開始</li> <li>初期導入コストの削減</li> <li>ITコストの変動費化（必要に応じて柔軟に変更可能）</li> <li>保守・運用の体制・コストの削減（OSのパッチ、ウィルス対応など）</li> <li>システムの拡張性（スケーラビリティ）の高さ</li> </ul>	<ul style="list-style-type: none"> <li>情報セキュリティのリスク <ul style="list-style-type: none"> <li>➢ 障害等によるサービス停止（可用性）</li> <li>➢ 顧客情報・営業秘密等の情報漏えい（機密性）</li> <li>➢ 受注・販売・財務会計等のデータ消失（完全性）</li> </ul> </li> <li>ガバナンス・コンプライアンスのリスク（個人情報保護法等の法令違反など）</li> <li>サービス継続のリスク（サービス事業者の廃業など）</li> </ul>

### 3.クラウドサービスに関連する過去の事件及び判例

クラウドサービスの法的論点を整理する前に、過去に発生した事件及び判例を取り上げ、そこからクラウドサービス契約の法的性質や法的意義について整理していくことにする。

#### (1) レンタルサーバデータ消滅事件（東京地裁 平成13年9月28日）

本事案は、クラウドサービスに該当するものではないが、先例として象徴的な事案であり、現在のクラウドサービスに関する法律専門書等でも取り上げられること多い事案である。

##### 《事件の概要》

- ・ インターネットプロバイダを営む事業者が、セキュリティ強化の作業中、ユーザ企業のホームページのコンテンツデータを作業ミスにより消滅させた。
- ・ ユーザ企業がコンテンツデータのバックアップを保管しておらず、ホームページの再構築に時間と費用を要したため、ユーザ企業が事業者に対して、ホームページの再構築に要した費用及びその間の営業上の逸失利益を損害賠償請求した。

##### 《ユーザ企業及び事業者の主張》

ユーザ企業と事業者の主張を主な争点毎に整理すると下表のとおりである。

争点	ユーザ企業の主張	事業者の主張
注意義務	事業者には、ユーザ企業のデータを適切に保管する <b>注意義務</b> がある。	事業者のサーバはユーザ企業が発信した情報の通過点に過ぎず、ユーザ企業が作成したファイルそれ自体の保存についてはユーザ企業が <b>自己の責任</b> で行うべき。
逸失利益	ホームページによる営業が出来なかった期間の <b>逸失利益についても賠償責任がある</b> 。	営業上の遺失利益は、データ消滅と <b>相当因果関係のある損害には含まれない</b> 。
過失相殺	データ消滅には何ら関与しておらず、 <b>過失相殺は考えられない</b> 。	ユーザ企業にはデータのバックアップを取っていなかったという <b>重大な過失</b> がある。
免責条項	<b>通信障害による債務不履行を想定したものであり、本件消滅事故には適用されない</b> 。	免責条項は、 <b>本件消滅事故による損害にも適用</b> される。

《裁判所の判断》

争点	結論	理由
注意義務	事業者に注意義務あり	電子情報であっても、保管対象物に関する注意義務として、それを損壊又は消滅させないように注意すべき義務がある。
逸失利益	消滅事故と因果関係のある損害と認められる	ユーザ企業が本件ホームページをその営業に利用していたことは疑いがなく、本件ホームページが原告の営業上の利益の発生に一定程度貢献していたことは否定し難い。本件消滅事故と本件逸失利益との相当因果関係を否定することはできない。
過失相殺	過失相殺の規定を適用する	ユーザ企業は、容易にバックアップをとることができ、損害の発生を防止し、又は損害の発生を極めて軽微なものにとどめることができたのに、本件ファイルのデータを何ら残していなかった。被告の損害賠償責任の負担額を決するに当たり、この点を斟酌して過失相殺の規定を適用することが、損害賠償法上の衡平の理念に適うというべき。
免責条項	本件には適用されない	事業者の積極的な行為によりユーザ企業が作成し開設したホームページを永久に失い損害が発生したような場合についてまで広く免責を認めることは、損害賠償法を支配する被害者救済や衡平の理念に著しく反する結果を招来しかねず、約款解釈としての妥当性を欠くことは明らか。

本事例では、ホームページの再構築費用に加えて逸失利益の賠償が認められているが、ユーザ企業がデータバックアップを取得していなかったことで過失相殺を認めており、最終的な事業者の賠償額は、裁判所が認定した損害額（1473万円）の1/2（736万5000円）に減額されている。

## (2) T B C顧客情報流出事件（東京地裁 平成19年2月8日）

本事案は、個人情報保護法施行前の事案であるが、大量の個人情報漏えいした事件としては慰謝料金額が比較的高い事案である。

### 《事件の概要》

- 平成14年頃、エステティックサロンを経営する事業者のウェブサイトでアンケート等により収集・保管していた個人情報がインターネット上において第三者が閲覧できる状態となってしまう、流出した。
- サーバを管理していた委託先の会社がサーバ移設時に設定ミスをしたことが原因。
- 情報漏えいに対し、被害者側はプライバシーを侵害されたとし、不法行為に基づき原告1人あたり慰謝料100万円および弁護士費用等の支払いを求めた。

### 《主な争点及び裁判所の判断》

本事案の主な争点における裁判所の判断は下表のとおりである。

争点	裁判所の判断
プライバシー侵害の程度	エステティック固有の事情に関する情報は、全体として顧客が個人ごとに有する人格的な法的利益に密接なプライバシーに係るものといえ、何人に対しても秘匿すべき必要が高く、また、顧客の合理的な期待としても強い法的保護に値するものというべきである。
委託先の監督責任	本件ウェブサイトのコンテンツの具体的な内容を自ら決定し、コンテンツ内容の更新や修正について、自ら確認していたものであり、また、委託先会社から随時運用に関する報告を受ける等、実質的に指揮・監督関係が認められる。よって事業者使用者責任（民法715条）がある。

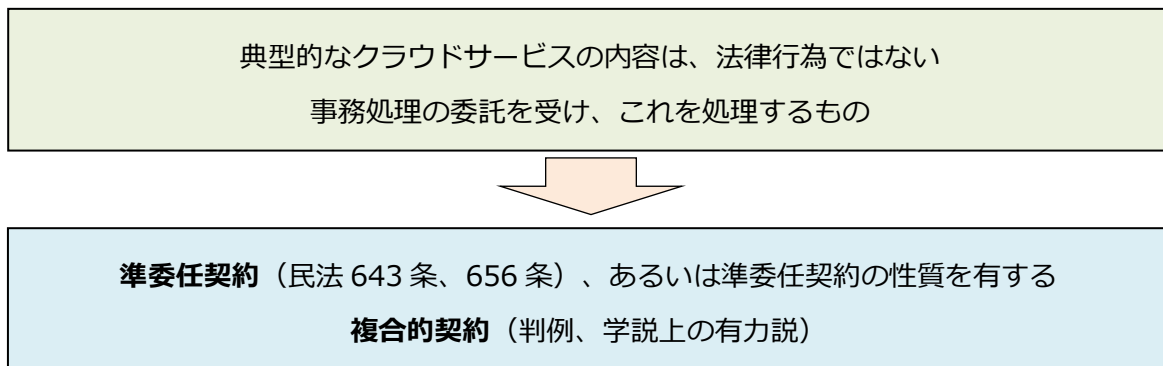
委託先の監督責任について、TBC側は専門的技術的な知識がなく、サーバ内部の仕様の検証等を任せていたので実質的に指揮命令監督する地位にはなかったと主張したが、裁判所に退けられている。なお、本事案発生時点では、個人情報保護法施行前であったが、現在は個人情報保護法によって、委託先の監督責任が明示的に定められている。

#### 4.クラウドサービスにおける法的論点

以下、クラウドサービスにおける法的論点について、クラウドサービス契約の法的性質から順を追って検討していく。

##### (1)クラウドサービス契約の法的性質

これまでの判例や学説上では、クラウドサービス契約の法的性質については、以下のように考えられている。



その結果として、クラウドサービス契約には、以下の法的効果が発生する。

- クラウドベンダは原則として「**善管注意義務**」を負う（民法 644 条）
- 契約に反した場合は**債務不履行**に基づく損害賠償責任が生じる（同 415 条）
- 対顧客上は、ユーザ企業の責任が問われることがある（クラウドベンダは**履行補助者**）
- 不法行為についてユーザ企業に**使用者責任**が問われることがある（同 715 条）
- 公序良俗（同 90 条）等に反しない限り、**免責条項は有効（契約自由の原則）**

上記法的性質における「複合的契約」とは、ソフトウェアライセンス等、準委任契約以外の性質を含む場合が該当する。なお、プライベートクラウドなどで、一定のサーバ等を使用する場合には、賃貸借契約（民法601条）の側面を持つこともある。



## (2)SLAの法的意義

### 《SLA の定義》

経済産業省「SaaS向けSLAガイドライン」によれば、SLA（Service Level Agreement）の定義は以下のとおりである。

提供されるサービスの範囲・内容・前提事項を踏まえた上で「サービス品質に対する利用者側の要求水準と提供者側の運営ルールについて明文化したもの」

（内容）・前提条件 ・委託範囲 ・役割と責任 ・サービスレベル項目 ・結果対応 ・運営ルール

SLAは通常、サービス利用契約書の付属資料であり、サービス契約の一部を構成するものである。また、事実上クラウドベンダのひな形（均一的で定型的なサービス）を多数の利用者が受け入れるものであることから、約款としての性質を有する。

従来の民法では、約款について明文規定が存在しなかったが、改正民法においては、以下のとおり明文規定化が行われている。

### 「定型約款」 ⇒ 改正民法（548条の2）において明文規定化

- 定型取引に合意したものは、次の場合、定型約款の個別の条項についても合意したものとみなす。

①定型約款を契約の内容とする旨の合意をしたとき、または、

②定型約款を準備した者があらかじめその定型約款を契約の内容とする旨を相手方に表示していたとき

- 但し、相手方の権利を制限し、又は相手方の義務を加重する条項であって、その定型取引の態様及びその実情並びに取引上の社会通念に照らして・・・相手方の利益を一方的に害すると認められるものについては合意をしなかったものとみなされる。（不当条項規制）



### (3)個人情報保護法との関係

#### 《国内のクラウドサービスを利用する場合》

ユーザ企業から個人情報の取り扱いをクラウドベンダへ「委託」する形になる。

個人情報取扱事業者が、利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合には、本人の同意は不要である。（個人情報保護法23条5項1号）

ユーザ企業には委託先の監督義務があり、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない（同22条）。また、適切な委託先の選定基準を整備する必要があり、第三者認証の利用も検討すべきである。（「ISO/IEC 27017：クラウドサービスセキュリティ」）

#### 《海外のクラウドサービスを利用する場合（サーバが海外にある場合も含む）》

外国にある第三者への提供については、以下の場合を除き、「委託」であっても本人の同意が必要となり、制限される（同24条）。

- ・ 個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国（十分性認定された国：EU）
- ・ 個人データの取扱いについて個人情報取扱事業者が講ずべきこととされている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を整備している者

### (4)知的財産権との関係

#### 《営業秘密》

一般的に営業秘密（ノウハウ、顧客リスト等）は不正競争防止法で保護される。保護要件は、①有用性、②非公知性、③秘密管理性の3つであるが、サーバの公開設定やセキュリティ管理状況によっては、非公知性や秘密管理性が問題になる。

cf. 「不正競争行為差止等請求事件」（東京地方裁判所 平成17年6月27日）

営業秘密を保管したコンピュータがインターネットに接続されていないことが秘密管理性を認める根拠の一つに挙げられている。

サーバが海外にある場合、現地の法令により開示義務が課される可能性があり、カントリリスクについて考慮する必要がある。cf. 米国 クラウド法、中国 国家情報法など

## 《著作権》

カラオケスナック店の著作権（演奏権）侵害が問われた「クラブキャッツアイ事件」（最高裁判所 昭和63年3月15日）で示された、いわゆる「カラオケ法理の問題」がある。

その後、「ファイルログ事件」（東京高裁 平成17年3月31日）では、直接的な著作権の侵害者（ファイルを不正コピーした者）だけでなく、ツールを提供した者についても著作権侵害を認め、損害賠償の支払いやサービスの停止を命じた。

## 5.クラウドサービス契約における留意点

### (1)リスク管理

クラウドサービスを利用するにあたっては、最初に、クラウドサービスを利用する業務及び情報が会社にとってどのような価値を有するのかをベースにリスクを評価し、回避、軽減、移転、保有のいずれにするかを検討することが重要である。

リスク影響度は次の式で計算する。

$$\text{リスクの影響度} = \text{資産価値} \times (\text{脅威} \times \text{脆弱性})$$

ユーザ企業の情報資産毎にリスク評価を行った場合のリスク影響度と対応策の例を下表に示す。

なお、リスクの影響度は、技術動向、法制度、事業環境等の変化に応じて変わってくるため、定期的にリスク評価を行い、見直すことが重要である。（P D C Aの実施）

「情報資産毎のリスク評価結果と対応策の例」

資産	脅威	影響度	対応策
個人情報 (要配慮個人情報)、 営業機密	情報漏洩	大	(回避) ・ 原則クラウドサービスを利用しない。  (軽減) ・ 業務上必要な場合は、クラウドベンダの信用情報、管

			<p>理体制（組織的、人的、物理的、技術的）等を厳格に評価し、利用サービスを選定。</p> <p>(移転)</p> <ul style="list-style-type: none"> <li>個人情報取扱事業者保険等への加入（補完的）</li> </ul>
取引情報、 生産情報、 財務・会計 情報	データ消失 サービス 停止	中	<p>(軽減)</p> <ul style="list-style-type: none"> <li>クラウドベンダを事前に定めた基準に基づき選定。</li> <li>クラウドサービス契約のSLA（稼働率、障害時対応等）を十分に検討。費用対効果のバランスも重視</li> <li>責任共有モデルに基づき、自社での対応策を検討（データバックアップ、ID管理等）</li> </ul> <p>(移転)</p> <ul style="list-style-type: none"> <li>サイバー保険等への加入</li> </ul>
公開情報 (HP等)	データ改竄	小	<p>(軽減)</p> <ul style="list-style-type: none"> <li>費用対効果を重視したSLAの設定</li> </ul> <p>(受容)</p> <ul style="list-style-type: none"> <li>現状で問題ないと判断した場合は、追加の対策は実施しない。ただし、適切な経営判断を行うために、十分な判断材料を収集することが重要</li> </ul>

## (2)契約内容の留意点

実務上は、リスク評価の結果、適切なリスク軽減策を行ったうえで、クラウドサービスを利用するというケースが多いと考えられるため、クラウドサービス契約を締結するにあたり、留意すべき点について、以下検討する。

### ① サービスレベルの内容と結果対応

クラウドサービス契約の一環として定義されたSLAの位置づけや内容を十分に理解したうえで、費用対効果も踏まえて契約内容を決定する。サービスレベルに関する検討項目及び検討内容を下表に示す。

「サービスレベルに関する検討項目及び検討内容」

検討項目	検討内容
サービスレベルの位置づけ	基準が確実に達成されるのかどうか、サービスレベルの位置づけを確認することが重要。 ＜法的義務の場合＞ SLAの基準はサービス契約内容の一部であり、基準未達時は補償対象 ＜努力義務の場合＞ SLAの基準達成に努力すれば、クラウドベンダの義務は果たされる
サービスレベル定義の理解	業務への影響を見極めるため、算定根拠を正確に理解する必要がある。 例) 稼働率99.9% ⇒ 月間であれば停止時間は最大約45分/月 年間であれば最大約9時間連続で停止することもあり得る。
サービスレベル未達時の補償	費用対効果も踏まえ、以下のような補償対象・内容を十分検討し、足りない部分は自社で補う等の検討を行う必要がある。 ✓ 将来のサービス無料使用チケットによる補償のパターンがあり、必ずしも利用料金が返却されるとは限らない。 ✓ 免責条項により、逸失利益までは補償されないケースが多い。 ✓ 保証対象外となる例外事由が設定されていることが多い。(クラウドベンダの責任に因らないもの) 例) ネットワーク障害、自然災害

## ② サービスの停止・廃止時の対応

クラウドサービスがベンダの都合等により停止・廃止された場合、自社の業務が停止し、再開までに長時間を要することで、再構築費用、機会損失が発生するリスクに備えることが重要である。検討項目及び検討内容を下表に示す。

「サービス停止・廃止時の対応に関する検討項目及び検討内容」

検討項目	検討内容
クラウドベンダの選定方法	クラウドベンダの信用情報、財務状況、営業実績、利用企業等の情報により、クラウドサービスが安定的に提供されるかを判断する。
サービス停止・廃止の事前通知	クラウドベンダの都合によりサービス停止する場合に、一定期間前に事前通知することが利用規約に含まれているかを確認する。（⇒代替サービスの選定、契約、導入期間を考慮）
データ移行の担保	クラウド上にある自社データの返還請求が可能となっているかを確認する。 他のサービスで利用可能なデータ形式での提供が可能かを確認する。
契約終了後の処理	契約終了後のデータ削除についての規定（ユーザ都合の契約解約時も含む）を確認する。
費用負担・賠償	クラウドベンダ都合によるサービス停止・廃止時の費用負担、損害賠償についての規定を確認する。

## (4)責任分担と免責条項

クラウドベンダとユーザ企業の責任範囲が曖昧な状態となっている場合、システム障害やセキュリティ事故が発生した際に、迅速な原因究明や対応が出来なかったり、費用負担や賠償責任を巡って紛争となったりする可能性がある。そのため、予めクラウドベンダとユーザ企業との責任範囲を明確化しておくことが重要である。

### ✓ 責任共有モデル

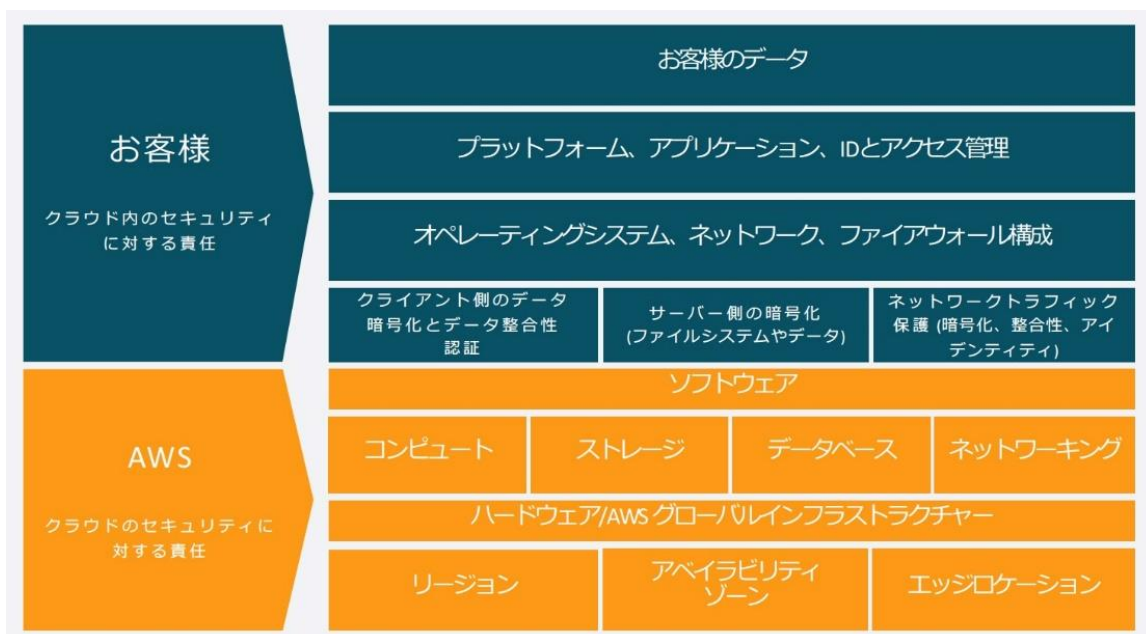
AWSを始め、最近の大手クラウドベンダがユーザ企業との責任範囲を明確にする際の考え方として一般的なものである。責任範囲を明確化することで、効率的・効果的にセ

セキュリティを確保することを目的としている。AWSの例を以下に示す。

#### - AWSの責任共有モデルの例（AWSのホームページより）

**AWS の“クラウドのセキュリティ”責任** – AWS は、AWS クラウドで提供されるすべてのサービスを実行するインフラストラクチャの保護について責任を負います。このインフラストラクチャはハードウェア、ソフトウェア、ネットワーキング、AWS クラウドのサービスを実行する施設で構成されます。

**お客様の“クラウドにおけるセキュリティ”責任** – お客様の責任は、選択した AWS クラウドのサービスに応じて異なります。選択によって、セキュリティに関する責任の一環としてお客様が実行する構成作業の量が決定されます。



#### ✓ 免責条項

クラウドベンダに故意・重過失がある場合や、一方的にユーザ企業に不利な免責条項は、無効となる可能性があるが、一般論としては、免責条項は有効と解されている。

したがって、免責条項の内容については、以下の点に注意が必要である。

- 損害賠償の上限額はクラウドベンダによって異なるため、比較検討しておく
- クラウドベンダが責任を負う範囲に注意する。（間接損害、逸失利益などは賠償しないことを規定している場合が多い。）

#### 参考文献

- 総務省「平成30年版 情報通信白書」
- 松尾剛行「クラウド情報管理の法律実務」（弘文堂）
- IPA セキュリティセンター「中小企業のための クラウドサービス 安全利用の手引き」
- JISA「ASPサービスモデル利用規約と利用申込書」（平成17年3月）
- 経済産業省「SaaS 向け SLA ガイドライン」（平成20年1月21日）
- 岡村久道「Cloud Computingと法令・契約」
- 東京地方裁判所「平成12年(ワ)第18468号損害賠償請求事件」
- 日経XTECH 「TBC情報漏えい事件高裁判決(1)～(3)」
- AWS「責任共有モデル」（<https://aws.amazon.com/jp/compliance/shared-responsibility-model/>）