クラウドサービス利用時のカスタマ認証取得の重要性

～経営戦略及び経営資源としての意義
法的訴訟リスクの低減や事故発生時の対応における認証の重要性～

稲垣隆一法律事務所

弁護士 稲　垣　　隆　一

概念の整理　経営とリスクと責任

- 経営とリスク
  - 経営　リスクの処理
  - 経営は法的リスク（訴訟・事故対応リスク）の可視化を求める
  - 法的リスクの実体は責任発生原因事実に関するリスクと残存リスク

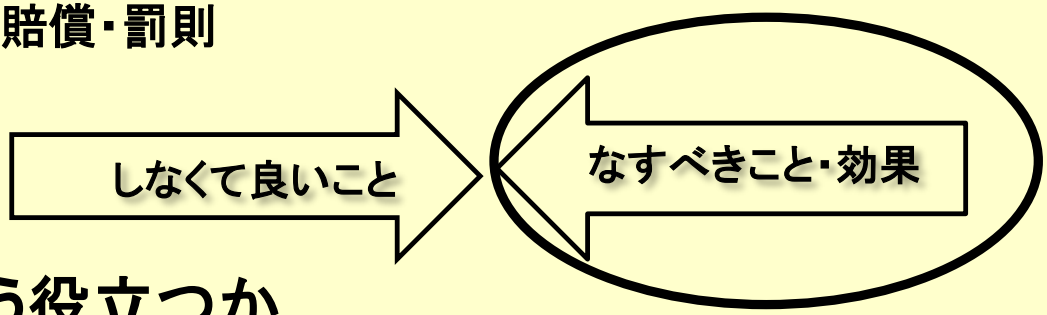
- 経営と責任
  - 責任はリスクの現実化による負担　責任はリスクそのもの

- ISMSの構築維持と認証はリスクと責任の可視化に資する
  - ISMSは情報資産を対象とするセキュリティリスクマネジメント
  - ISMSの構築はリスクと責任を可視化し、維持は精度を高める
  - ISMSの認証は受審企業の意思と能力を第三者に伝える

ISMSは法的リスクをどう可視化するか？

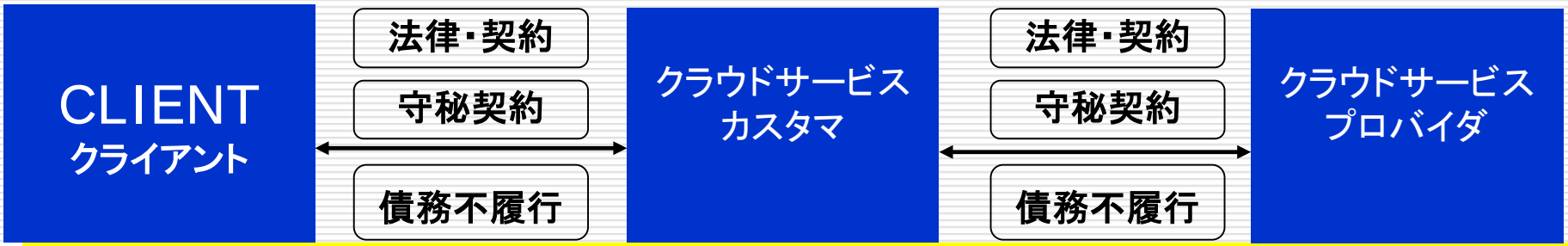
- 法的リスク＝責任発生原因事実の存在と残存に関するリスク
  - 責任発生原因事実
    - 法的責任　法（正義・衡平），法律，契約等が規定する責任の要件たる事実
    - 経営責任　倫理，ミッション，環境，経営資源等が求める責任の要件

- 法的責任の可視化には発生原因事実の存在内容を可視化する
  - 要件：何をすべきか・何をしなくて良いのか
  - 効果：賠償・罰則



- ISMSはどう役立つか
- リスクアセスメントを通じた責任発生原因事実の特定・明確化
- リスクマネジメントによる法的リスクの経営に対する意義の把握

ISMSクラウドセキュリティ認証をどう使う？　契約に入れる



法律（例：GDPR・個人情報保護法）上の義務を特定できればそのリスクを極小化できる→ガイドライン

契約にもとづく義務・義務がないことを特定できれば，そのリスクを極小化できる

- カスタマのクライアントに対する義務・プロバイダのカスタマに対する義務の特定
  - 上流・保守・運用契約等　準委任契約なら「履行すべき事務」「履行」を特定する
  - 開発契約等請負契約なら「仕事」と「完成」を特定する
  - 守秘契約なら，「守秘対策」と「行う」「実施する」を特定する

保守・運用委託契約の文例

第〇条　乙は，第〇条の目的（例えば稼働率）を達成する方法として，JISQ27017に準拠したセキュリティマネジメントを履行すべき事務と定める。

守秘契約の文例

【例1】第〇条　第〇条の守秘対策は，乙が，クラウドサービスカスタマとしてISMSクラウドセキュリティ認証（ISMSクラウドカスタマ認証）を受けたセキュリティ対策を行うことをもって足る。

【例2】第〇条　乙がISMSクラウドカスタマ認証を受けたときは，その認証の有効期間中，第〇条の安全対策を実施したものと看做す。

ISMSクラウドセキュリティ認証をどう使う？　実施する

契約でなすべきことを特定できないときにも，解釈の資料として役立つ

なすべきことを特定できていないのに，情報漏洩，システム障害でユーザや第三者を加害したら

- 債務不履行　新民法415条

  債務者がその債務の本旨に従った履行をしないとき又は債務の履行が不能であるときは、債権者は、これによって生じた損害の賠償を請求することができる。ただし、その債務の不履行が契約その他の債務の発生原因及び取引上の社会通念に照らして債務者の責めに帰することができない事由によるものであるときは、この限りでない。
- 請負人の担保責任（契約不適合責任）　本質は債務不履行責任であることが確認された

- 不法行為

  故意又は過失により（損害・損害発生原因の予見可能性＋結果回避可能性）他人の権利又は法律上保護される利益を侵害した者は，これによって生じた損害を賠償する責任を負う。

ISMSは，「その債務の不履行が契約その他の債務の発生原因及び取引上の社会通念に照らして債務者の責めに帰することができない事由による」か「予見可能か」，「結果回避可能か」の判断の資料となる

認証等が法的判断に用いられた例

債務不履行責任の判断にあたり各種ガイドラインが考慮された例として以下がある。

- 大阪地裁平成18年5月19日判決　（YahooJapan 個人情報漏洩事件）
- 東京地裁　平成31年4月25日判決（ベネッセ事件）
- 東京高裁　令和元年6月27日判決（ベネッセ事件高裁判決）
- 東京地裁　令和元年9月6日判決（ベネッセ事件）

ご清聴ありがとうございました

弁護士稲垣隆一　経歴

- 早稲田大学法学部卒業
  東京地検検事等を経て第二東京弁護士会弁護士登録
- 内閣官房
  - NISC重要インフラ専門調査会委員
- 経済産業省
  - 情報システムの信頼性向上のための取引慣行・契約に関する研究会TF委員
  - 経済産業省　電力取引監視等委員会委員（委員長代理）
- 技術研究組合制御システムセキュリティセンター（CSSC）監事
- 地方公共団体情報システム機構（JLIS）監事
- システム監査学会理事
- 日本セキュリティ監査協会顧問
- 一般財団法人日本情報経済社会推進協会(JIPDEC)BCMS,ISMS,ITSMS,CMMS運営委員
- 一般財団法人日本規格協会　ISOリスクマネジメントWG委員
- 平成20年度情報化月間平成20年度情報化促進貢献　個人表彰
  総務大臣表彰「情報セキュリティ部門」受賞
- 平成22年ISCスクエア　Information Security Leadership Achievments　受賞