Vol.2020-DPS-182 No.37
Vol.2020-CSEC-88 No.37
2020/3/13

サブスクリプション型 IT サービス提供における セキュリティリスクコミュニケーション

藤井みゆき [1]　稲葉 緑 [1]

概要：サービス提供者と利用者間において、特にそのサービスが IT サービスのように機能が複雑であったり専門性が高い性質を持つ場合、そのセキュリティに関する情報は、利用者側に十分伝わらない可能性がある。この両者の 「情報の非対称性」の結果、利用者が不適切にサービスを利用することにより、セキュリティ被害をもたらす恐れがある。

セキュリティに関する利用上の注意についての情報は、旧来より提供者より利用者に対しマニュアルや利用規約等を通じてプッシュ型で提供されてきたが、残念ながら利用者が進んでこれらの情報を取得し、セキュリティ対策を行っているとは言い難い。

IT サービスが売り切り型からクラウドサービスのようなサブスクリプション型にシフトし、利用者の継続的な利用を目論んだサービス提供が必要となる中で、これまでユーザ側で自主的に実施することが当然と思われてきたセキュリティ対策も、専門的な IT サービス機能として利用者に提案する可能性が考えられる。またそのためには、必要な機能の一つであると利用者自身に認識させるための「啓発」が必要である。

本稿では、サブスクリプション型 IT サービスにおいて必要な、サービス提供者と利用者の間のリスクコミュニケーションの在り方について考察を行う。

キーワード：リスクコミュニケーション、サブスクリプション、情報の非対称性

Security risk communication in subscription-type IT service provision

MIYUKI FUJII [†1]　MIDORI INABA [†1]

Abstract: Frequently, a service specification cannot be understood by the service's users, especially when its function is highly complicated or specialized. There exists "information asymmetry," and as a result of this asymmetry users may inadvertently use the service and cause security damage. Information on security precautions has been provided by providers from the past as push-type information to users through manuals or terms of use. But unfortunately, it is hard to say that users are willing to acquire this information and take proper security measures. In recent years, as IT services have shifted their form of payment from sold out type to subscription type such as a cloud service, it has become necessary to provide services that aim for continuous use. Under such circumstances, there is a possibility that security measures that have been considered to be voluntarily implemented by the user can be proposed by providers as specialized IT service functions. In addition, in order for users to accept the proposal, "enlightenment" is needed to make the users themselves aware that security is one of the necessary service functions. In this paper, I consider how risk communication between service providers and users is required for subscription-type IT services.

Keywords: Risk Communication, Subscription, Information Asymmetry

1. はじめに

1.1 サービス提供者と利用者間における「情報の非対称性」

消費者が財およびサービスを購入する際には、対象の仕様や機能を吟味し、自らが求めている便益に合致するものかどうかを見極めた上で購入することが通常である。見極めに際しては、財やサービスをまずその外見や説明仕様、機能から確認する。例えば、衣服を購入する場合などは、店舗においてデザインや材質を確認し、試着することによりサイズを確認し、その品質や特性をある程度理解したうえで購入することができる。これは衣服の機能や品質が比較的単純であり、手に取ることによりその仕様の把握が容易であることによる。

しかし一方、保険商品はどうだろうか。営業員から説明を受けてもなかなか理解できず、小さい字でびっしりと書かれた約款を十分読まないまま契約してしまうこともままある。保険商品は理解するためには一定の知識を必要とし、また補償対象や制約に関する説明が複雑であることにより、仕様や品質を完全に理解することが通常困難である。このように、仕様や機能が複雑で容易に把握することが難しい

1 情報セキュリティ大学院大学
Institute of Information Security

Vol.2020-DPS-182 No.37
Vol.2020-CSEC-88 No.37
2020/3/13

財やサービスの仕様や質を「隠れた品質」と定義したい。このような財やサービスの「隠れた品質」については、サービス利用者と提供者の間に存在する「情報の非対称性」の問題として従来より議論されてきた。薮下(2002)は、情報の非対称性は、「経済発展により各人が”分業”により専門分野に特化してきたために、結果として情報を持つ分野と持たない分野が分化してきたことに起因する」と説明している。専門分化により多種多様のサービスが生まれ、利用側の選択肢が広がることは経済合理性に適うが、有利な選択を実現するための「隠れた品質」問題の解消は「情報劣位者」である利用者側の課題である。

先出の薮下(2002)においてはまた、情報の非対称性解消の方法として、提供者から個別に入手する情報ではなく、第三者が客観的な視点で収集した情報や公開情報を活用することが提案されていた。例えば、企業組織における株主と経営者間において、とかく株主利益を無視しかねない経営者側のモラルハザードを抑制するため、株主自身が経営者を監視（情報を入手）し、その活動の適切性を見極める必要がある。ここで、株主が直接監視することに加え、関係するステークホルダー、例えばメインバンクが持つ資金・決済・コンサルティングに関する情報、あるいは企業内部で働く労働者の持つ情報などを多面的に収集することも有効ではないかとしている。情報は、信頼のおける他者から入手し、複数の組織や人間の監視を経ることにより、より客観的なものとなり得る可能性がある。

さて一方、提供者側には、対価を得ながらもそれに相当する価値（財やサービス）を十分に提供しないという問題が存在する。旧来から、モラルハザードにより「情報を隠す」行動の解消が課題とされてきたが、果たして常に提供者はそのような「良くない」行動を取りがちなのだろうか。逆に、特に財やサービスの品質向上に対してモラルハザードが無い、いや、むしろモラルが高い提供者は、品質の高い財やサービスを準備し、利用者に対しその品質を理解してもらい、選択してもらいたいと考えるであろう。ここに、提供者側にも情報の非対称性を解消するための動機付けが存在することが考えられる。この場合の提供者はむしろ、サービスの品質向上のために費やした、見えない部分にかけるコストの価値を利用者に理解してもらい、その価値に見合う代金を支払ってもらうことを求めるであろう。ここでこの「隠れた品質」に対応する見えない部分にかけるコストを「隠れたコスト」と定義したい。

モラルの高い提供者はさらに、財やサービス利用のリスク（機能的な制限や限界など）を知った上で、利用上の注意や遵守事項を理解してもらうための情報提供に動くこともある。これは、利用者が財やサービスの便益を適切に享受し、それによる不利益を被ることのないこと（同時に利用者がその不利益による訴訟を起こすことのないこと）を狙っていると考えられる。

このようにサービスの提供者と利用者間における情報の非対称性は、「隠れた品質」および「隠れたコスト」の問題として、双方に解消を求めるための動機が存在する。この双方の動機づけがお互いのメリットになることが最も望ましいことであるが、解消に向けては双方に情報を収集する・提供するためのコストが発生すると考えられる。このコストを費やしてまで非対称性の解消に向かう動機付けが存在するかどうかは、提供者と利用者、それぞれの立場により差異があると考えられる。

本論ではこれより、提供者と利用者の間の情報の非対称性解消における課題を具体的に議論するために、特に解消が難しいと思われる財やサービスの条件を絞って考えていきたい。先の薮下(2002)のように「その条件を提供されるサービスが多面的、かつ多次元に亘り質に相違がある場合」が非対称性の原因となることから、「財やサービスの品質の複雑性」と「財やサービス提供者の不均一性」が非対称性においてまずは解消が課題となると考えられる。

まずは「財やサービスの品質の複雑性」についてである。これは冒頭に述べたような、衣服と保険商品の差であり、その品質が一見して判断できないような複雑なものであれば理解が難しい。表１に、扇風機の製造委託(OEM)とWebサイト(IT)の構築運営委託の事例を比較してみた。扇風機は外観が単純であり、機能的にも比較的単機能であるため、検品や検査が可能である。万一検品や検査をくぐり

表 1　製造委託と IT 委託の事例比較

	扇風機の製造委託	Webサイト構築委託
納品物の仕様決定	設計図やサンプル品で事前に確認	ホームページ自体はレイアウトで確認、アプリケーション、サーバインフラ、セキュリティの仕様はユーザに関連する部分を抽出し文書で説明。
検品	外観上の問題の有無の確認、動作上の問題の有無の確認（数が多い場合は抜き取り）	ホームページ自体の外観と基本動作上の問題の有無の確認（アプリケーション、サーバインフラ、セキュリティは一般的には確認できない）
問題発生時の対応	・事故品があれば、修理・交換対応 ・事故品による二次的損害（利用者が怪我など）があれば、製造物責任の範囲で補償対応	・事故があれば、契約内容に応じて改修や復旧対応 ・事故による二次的損害（情報漏洩/事業停止/マルウエアによる第三者被害など）があれば契約内容に応じて補償対応
継続対応	不良・市場不良の統計や問合せ対応を定期的に総括し、改善を議論	・運営作業を継続実施（要望に応じた更新や定期メンテナンス） ・運用実態を定期的に総括し改善を議論

Vol.2020-DPS-182 No.37
Vol.2020-CSEC-88 No.37
2020/3/13

抜けた残存した品質問題があっても、補償や品質不良の対応として市場における前例や制度も整っている。対して IT の委託においては、仕様が外観や機能に顕著に現れるものだけではないため、説明が難しく、外観の確認だけでは検品が難しい。また問題発生時は社会的にも判断や対応が分かれる現状にある。

２つめに「財やサービス提供者の不均一性」に関しては、提供者の質が多種多様であり、利用者がその質を判別することに非常に難があるケースである。中古車市場で言われる「レモン市場」は、その質の説明を担当する中古車ディーラーの信頼性の問題で、新車であればメーカー責任であるが、中古車に関しては、種々雑多な中古車ディーラーごとにその説明品質に差が出、品質の差異について知識を持たない利用者は適切な選択を誤ることが考えられる。

これら 2 つの要因から、今回は品質の複雑性が高く、さらに、提供者の質が多種多様であるサービスとして、インターネット上の IT サービスを挙げる。利用者には企業ユーザ、および一般消費者が想定されるが、今回は一般消費者の利用場面を特に想定し、非対称性の解消について論じていきたい。情報取得や監視にコストを費やすことが比較的可能と思われる企業ユーザに対して、一般消費者は特に非対称性の度合いが高く、非対称性においてより弱者ではないかと思われるからである。

1.2 インターネット IT サービス利用における「情報の非対称性」課題

クラウドサービスに代表される、インターネット上の IT サービスは近年、リソースの少ない中小企業でも小さい投資でスピーディに導入が可能である IT サービスとして需要が高まっている。一般消費者にとっても、簡易に電子メール、ファイル共有、情報検索などの機能を利用できる身近な IT サービスであり、サービス提供者は広告収入や消費者の個人データ入手を見返りとしてサービスを無償とするものも多い。このようなサービスはインターネット上に非常に多く存在し、その機能を利用するにおいては、十分にそのサービスの品質を検証することなく利用する一般消費者も多い。

サービスの仕様を確認せずにクラウドサービスを利用し情報セキュリティ事故を発生させた事例として、2015 年 2 月に報道された情報漏洩案件を取り上げたい。日本経済新聞および HUFFPOST の 2015 年 2 月 20 日付記事によると、インターネット上の無料翻訳サービス「I Love Translation」サイトに入力したとみられるメールの内容が、ネット上で誰でも見られる状態になっていた。メールの内容から、中央省庁や銀行、メーカーなどのやりとりが含まれており、個人情報も含まれていた。当該翻訳サービスの設定（翻訳のため入力した情報をそのまま公開する：事故当時）を理解しないまま安易に情報を入力した結果の事故である。

このような事故を受け、IPA セキュリティセンターが 2016 年に発行した「情報セキュリティ 10 大脅威 2016」には、15 位に「インターネットサービス利用に伴う意図しない情報漏えい」として注意喚起され、機能や危険性を理解せずにサービス利用することを利用者に対し注意喚起するとともに、サービス提供元に対しても、サービスのわかりやすい説明と、情報の取り扱い方針等について示すことを求めている。

1.3 サービス提供者と利用者間におけるリスクコミュニケーションの必要性

しかしながら、特に科学技術などの専門性の高い分野のリスク情報を利害関係者に正しく伝えることは簡単ではない。これについては旧来より「リスクコミュニケーション」という概念について、様々な努力がなされてきている。米国研究審議会（National Research Council）の定義（1989）によると、リスクコミュニケーションとは、「個人とグループそして組織の間で情報や意見を交換する相互作用的過程である。」とし、リスクの特質についての多種多様のメッセージと、それに関連する反応やリスク管理のための法的、制度的対処への反応についての他のメッセージを含むとしている。リスクコミュニケーションにおいては、リスク情報を発信する「送り手」はリスクの性格や危険性、リスクの意味、それに基づくリスク管理方法を適切に伝え、対する情報の「受け手」側では、自らのリスクの認知や許容水準について送り手側に伝達することが望ましい。

これらのコミュニケーションの多くは、旧来より多くのリスクを伴う環境やサービスの提供の場面で課題として取り上げられてきた。近本（2008）は、化学工業会、原子力業界、医療放射線分野、電磁界分野における現場のリスクコミュニケーションに関する課題を整理し、多くは受け手の関心や知識の低さゆえ、送り手が努力してもその発信内容が適切に受けられていない点を課題として提示している。これらを解決するために送り手側での工夫ポイントとして、受け手の状況により、与えるべき情報の内容やレベルを判断し情報を伝えることと、リスクゼロはありえないことを理解してもらい、双方向の議論により許容できるリスクを共に考えていく、「信頼関係の構築」が重要であることを示している。

IT サービスにおいても、提供者から利用者への同様のリスクコミュニケーションは必要と考えられ、さらに利用者自身の行為によりリスクが発生する可能性もあることから、より厳密な説明がなされるべきと考える。

2. IT サービス提供におけるリスク説明の現状

1 章で述べてきた課題提起を踏まえて、現状、インターネット IT サービスを提供する場合において、提供者からのリスク説明やリスク低減のための活動がどのように行われているのかを調査した。

2.1 認証および保証による信頼性の確保

1.1 において、第三者の客観的な視点で収集した情報を活用する利点については既に述べた。財やサービスの信頼性

を証明・確認でき、双方にとってメリットになる仕組みとして、ISO に代表される公的認証がある。これは、認証基準（規格）に従い、利害関係のない第三者機関が審査のうえ、認証を受けるものであり、提供者が自組織の活動、財やサービスの質に対し社会的な信頼を得、利用者はそれにより安全性を確認し安心して財やサービスを利用することが可能である。ただし、認証の取得や認証の維持には相当の費用がかかるため、提供者は費用（認証維持コスト）対効果(利用者への品質アピール)のバランスを考えながら、認証取得・維持の施策を推進することとなる。財やサービスを大量に多数の利用者に提供し相応の利益を得ることができなければ、認証取得のハードルは高い。

また、利用者をリスクから保護するという観点において、IT サービス利用における消費者保護について考えてみよう。「製造物責任」（PL 法）は、製造物の欠陥により利用者が損害を被った場合に、製造業者に無過失責任を負わせるという消費者保護の観点からの法律である。しかしその「製造物」の範囲は、消費者庁（2018）によると「製造または加工された動産」としており、無体物であるソフトウエアについては、製造物に組み込まれている場合を除き、これを含まないと定義されている。従って、クラウドサービスのようなサイバー空間において IT 機能を提供するサービスは、そのソフトウエアの瑕疵により少なくとも製造物責任を負わない。

これに対し、製造物責任の対象をソフトウエア にも広げるべきという意見がある。Leverett, Clayton, Anderson（2017）は、EU の PL Directive はサービスやシステムも対象にするべきだと主張している。組み込みのソフトウエアが製造物責任の対象であることから、サービス提供者はソフトウエアの瑕疵による責任を避けるため、しばしばソフトウエア を製品に組み込まず、クラウド上に設置している。彼らはこのような状況は望ましくないとしている。また、谷口（2005）は、ソフトウエアの脆弱性の問題を重視し、脆弱性低減インセンティヴの強化手段の一つとして、ソフトウェアを製造物責任法の対象に含め、但し、ソースコードを公開した場合はこれを免責することを提案している。ソースコードを公開することが利用者に対する情報提供であり、利用者自身が解読できなくとも、公開により多数の人々の確認を得、バグを減らすことが可能になるという考え方である。

ソフトウェアの製造物責任については、谷口も触れているように、例外なく製造物責任を問われるようになると、濫訴を恐れ、ソフトウェアの提供が中止されたり、新規開発が停滞することも考えられ、情報化促進にブレーキを掛ける可能性があり、現在の法律で定義されている通りに、責任範囲を有体物としての製造物に組み込まれたソフトウェアの欠陥に限定し、フィジカルの世界での損害を追及するに留めることは賢明な判断であると考える。しかし、ソースコードの公開は、免責の条件にはできるかもしれないが、ソフトウェア自体が著作物であり商品であることを考えると、開発戦略上、現実的に公開が進むことは考えにくい。また、一般消費者自身が内容やその結果として利用上のリスクが何であるかを判断するのが難しい。

以上のように、認証や保証の観点での様々な努力やアイデアは存在するが、いずれもその有効性は限定された範囲に留まる。認証制度は財やサービス、またそれを提供する組織の信頼性を高めるが、仕様を説明しているものではないため、サービス自体の利用者の理解を進め、誤用を避ける手段にはなり得ない。また、製造物責任は、製造物の瑕疵が原因で発生する損害を保証するが、誤用による損害は必ずしも保証されず、また利用者の利用目的の達成を保証するものではない。それゆえ、提供者による仕様やリスクの説明はやはり必要であると考える。

2.2 利用規約等による文書説明

では提供者が利用者に対する直接の説明はどのように行われているのだろうか。提供者によるリスク説明の内容を具体的なケースをもとに検証を行なった。取り上げたのは翻訳サービスである。翻訳サービスは無料サービスが多く、簡易に利用することができる一方、重要な情報を入力する機会が発生しやすく、かつ、その情報を蓄積するだけではなく、機械翻訳エンジンの精度向上のため、提供者が入力された情報を二次利用することが想定されるため、情報管理上のリスクが高まる可能性が高いからである。

表 2　調査対象の翻訳サービスと文書

調査対象	提供者	調査対象文書	発行／改版日
Google 翻訳	Google LLC *GAFAの1つ	Google 利用規約	Oct. 25, 2017年10月25日
		Google プライバシーポリシー	2019年1月22日
Microsoft Translator	Microsoft Corporation *米国のソフトウエア会社。時価総額1兆ドル（2019年4月現在）	Microsoft サービス規約	2018年3月1日
		Microsoft のプライバシーに関する声明	2019年4月
Weblio 辞書	Weblio株式会社 *日本のインターネットサービス会社。従業員100名の非上場企業（2019年2月現在）	利用規約	不明（「2006年1月26日に本条項の一部を改訂」の記載あり）
		プライバシーポリシー	2019年5月29日
I Love Translation	不明	(文書見当たらず)	–

Vol.2020-DPS-182 No.37
Vol.2020-CSEC-88 No.37
2020/3/13

一般消費者が翻訳サービスを利用するうえでの仕様説明や、注意事項を含む品質情報の提供は、ほぼインターネット上のドキュメントのみでなされる。人的コミュニケーションの可能性として問い合わせ窓口が設定されている場合があるが、ユーザ数の多いサービスや、あるいは無料のサービスについては、問い合わせに人的コストをかけることはあまり現実的ではないと思われる。現状ではサービスの仕様や品質定義は利用規約等を中心とした文書が中心的な役割を果たしており、利用者はこの文書を自発的に読み内容を理解する必要がある。この利用規約が現状、一般消費者に対してどの程度の品質説明を行なっているかを調査した。

検討の観点は以下３点とした。

① 利用規約等の品質説明の文書が存在しているか
② 品質説明の文書は、必要な品質説明（利用上のリスク、入力データを含む利用者情報の扱いの説明）を行なっているか
③ 当該文書は利用者にとって読みやすく、理解しやすいか

調査した４つのサービスとその対象文書について表２に記載した。

提供者が明確となっている３つのサービスについては、規約等の顧客に対する説明文書を持つ一方、提供者が不明である I Love Translation は何らの説明文書を持たない。インターネット情報サービスは何人でも提供でき、提供者はそれに対する説明責任を持つものではないからである。この手のサービスを私たちは排除することはできないため、選択しない、あるいはリスクを考慮して利用するというフィルタリングを行う必要がある。

品質説明の内容については、グローバルにサービスを提供する 2 社と、日本ローカルサービスである Weblio については顕著な差異が存在した。Weblio は個人情報取り扱いについては説明責任を果たしており法律上問題になるものではないが、翻訳入力文書に絞って検討するに、その説明については不十分であった。

Google および Microsoft の翻訳サービスについては、入力情報の取り扱いについての情報は文書によりある程度明らかになった。入力した情報はサービスの改善のために「安全に」再利用される可能性が高いが、情報の削除機能について明記はされておらず、また ID などの個人を特定する情報と紐づいていない限り、削除は現実的には困難であると思われる。公開を前提としていない機能であるため、他者に提供されることはないと推測されるが、取り扱い関係者による万一の不正利用による補償は基本的に期待できないことがわかった。ただし、規約等の文書説明は熟読に時間がかかり、また読まなくともサービスを利用できるため、利用者が内容を読まずに利用している可能性も否定できない。

まとめると、現状の翻訳サービスについての品質説明姿勢は、提供者・利用者ともに現状ではそれほど高くない状況であるといえる。

提供者の立場を考えると、翻訳サービス自体は無料サービスであり説明を義務づけられているわけではないため、Google、Microsoft が文書で適切に説明を行なっていることは、グローバルにサービスを提供している優良企業としての「社会責任」を果たしている観点から評価できる。利用者が多いサービスであるゆえ、一部の利用者より過去に「質問」や「説明要請」が寄せられた可能性が考えられる。

2.3 利用者が説明を受け入れる姿勢

これまで提供者側の説明の状況や情報提供の姿勢について議論してきたが、逆に、利用者が説明を受け入れる姿勢はどうだろうか。I Love Translation の情報漏えいが日本において大きく報じられたが、提供者側の提供姿勢を批判するのではなく、前掲の日経新聞ほかの記事のように、利用者側の自衛を求める論調が高まったことが特徴的であり、Facebook の個人情報の不正利用事案のように、サービスの提供者が強く批判される状況とは対象的である。これは前者の案件が、提供主体が不明である無料サービスであり、批判の対象が明確でなく責任の追及が困難であることに起因していることが推察される。ただ、報道や有識者の動きとは別に、一般消費者の意識レベルが総じて高まっているかどうかの検証は難しい。いかに提供者の説明が丁寧であっても、利用者側がその説明を受け理解しようとする意思がなければ、理解が進まない。

島他（2011）は、利用者がセキュリティ対策の行動を起こすためには、利用者に対するメッセージング手法に工夫を行うことが効果的であるという検証を行ない、検証の結果、利用者が個人として直面する脅威についての説明よりも、一個人での対応では十分ではないという集団での行動の必要性を訴える手法の方が、より対策行動につながるという結果が得られたという。効果的に伝達するため、メッセージングに工夫をする効果については理解できるが、利用者がセキュリティの必要性を理解し、さらに説明された対策を講じるための行動を起こすまでに、いくつかのハードルがあることではないかと思われる。すなわち、利用者が行動を起こすためには、情報提供者の ①説明を読み、②内容を理解し、③行動を起こすべきか判断し、④実際に行動を起こす、というプロセスを踏むことが考えられ、①でまず説明を読むに至らない、②で内容を理解するに至らない、③で判断を誤る、④で行動を起こすに至らない、というそれぞれの段階を突破した上で初めて行動に至る。島他の研究においては、実験アンケートに答えることに同意した段階で少なくとも①は予めクリアしてしまっており、被験者 2,254 人のうち、内容を理解できなかった 153 人を除き 2,101 人が一部なりとも理解をしているが、そのうち実際に行動すると回答したのは 541 名であり、歩留まりは良いとは言えない。また、ほとんどの利用者は、①の段階で説明文を自発的に読んでその内容を理解することに消極的である。Commerce Times (2001)によると、“Consumers want to feel safe, but they aren’t willing to do the

Vol.2020-DPS-182 No.37
Vol.2020-CSEC-88 No.37
2020/3/13

work.“（消費者は安全を望んでいますが、仕事をする気はありません。）とされており、まず説明を読むというところに辿り着く困難を考えると、いかに説明の内容を工夫したとしてもその効果は限定的であると考えざるを得ないであろう。

3. 提供者と利用者の関係性の変化

これまで、サービスの提供者と利用者の間の情報の非対称性の問題や情報提供・リスク説明についていくつか現状についての説明を実施してきた。しかし現状では、必ずしも両者の間のコミュニケーションが良好で、結果的に利用者が必要なリスク把握をしているという状況ではない。だが近年の IT 化の進展やサービス提供スタイルの変革により、この両者間のコミュニケーションを発展できる可能性がないのかを探っていきたい。

3.1 サブスクリプション化の進展

近年、「モノ消費からコト消費」へと、財やサービスの機能的な価値を単体で消費することではなく、一連の体験として消費することに消費者の価値観がシフトしている。経済産業庁(2016)の調査によると、消費者性向は、今後の生活における力点は物の豊かさよりは心の豊かさへ、物を所有することより得られる体験にお金をかけたいという、安くて経済的なものを求めることから付加価値志向へと変わってきていることを示している。

所有を目的としなくなった消費者に対し、利用を主眼においたビジネスモデルがマーケティングにおいて検討されるようになった。

川上(2019)は、継続的な収益の獲得を実現する収益化モデルを「リカーリングモデル」と呼び、「サブスクリプション」をリカーリングモデルの代表格として定義している。「消費者と事業者が一定期間において契約関係にあり、その間に利用に対する料金の支払いがある状態」を指す。同じリカーリングモデルである「リース」よりも契約の継続拘束力が弱いため利用者にとって有利である、としている。

また川上は、サブスクリプションの特性として「つながりの強さ」を挙げており、一般につながりの強い企業と弱い企業には表 3 に示す差があるとしており、利用者が片付けるべき用事を解決する、そのために積極的に利用者に働きかけ続け、ユーザへの価値提案を続けていくことが重要だとしている。

大きな違いは利用者の活動チェーンにおける提供者の関わりの強さと時期であるとしている。これまでの売り切りモデルは、販売し利益をえることが重要な活動であったため、購入以前の利用者とのタッチポイントが重要であったものを、購入以降に利用者～提供者のコミュニケーションを深め、継続的にサービスの魅力を伝えることが重要であるとしている。この継続的な関係性の構築が、提供者と利用者の間の情報の非対称性の問題を緩和し、リスクコミュニケーションも進化する可能性が考えられる。

もう一つの可能性は、IT 化、デジタル化の進展である。サービス提供や利用者とのコミュニケーションのために利用する手段として、Web システムや SNS などを利用するケースや、IoT による利用ログの常時収集など、利用状況の監視や、サービスに対する利用者からのフィードバックも格段に容易に行えるようになり、双方向でのリスクコミュニケーションが期待される。

表 3 つながりの強弱

	つながりが弱い企業	つながりが強い企業
①消費トレンド	所有時代に対応	利用時代に対応
②ユーザへの価値提案	プロダクト	アップデート
③ユーザへの分析視点	顕在的ニーズ	ジョブ（片づけるべき用事）
④ユーザへの対応	事後的	積極的
⑤事業設計の基準	事業活動（バリューチェーン）	ユーザ活動

3.2 マーケティングにおけるコミュニケーション構造の変化

一方で、ディジタル化の進展は、提供者と利用者間のコミュニケーションにとどまらず、利用者同士の情報交換の実態を生み出し、その構造を踏まえたマーケティングの可能性を示唆する。コトラー （2017）はマーケティング 4.0 において、ディジタルの時代における利用者同士のつながりが情報交換や相互推奨、また楽しみの共有となり、結果として顧客エンゲージメントが高まることを提唱している。また、新津（2017）によると、企業と消費者の間のコミュニケーションは、家族や友人、ディジタルの世界を通じてのインフルエンサーを介して行われる形式へと変化してきている（図 1）。

3.3 新しいリスクコミュニケーションの在り方

また一方で、リスクコミュニケーションの構造も時代とともに変化を遂げてきた。浦野(2001)は、旧来はマスコミ等を媒介として行政・企業・市民団体および地域住民等の三者が情報交換する形式を取っていたものを、意見交換の「場」を中心とした参加型のリスクコミュニケーションがこれからの形であるとしている。図 2 に示す。

基本的な変化点は、一方的な説明ではなく、双方向での意見交換をより重視したものだといえる。特に専門的・技術的でなじみにくい内容を身近に感じてもらうためのサイ

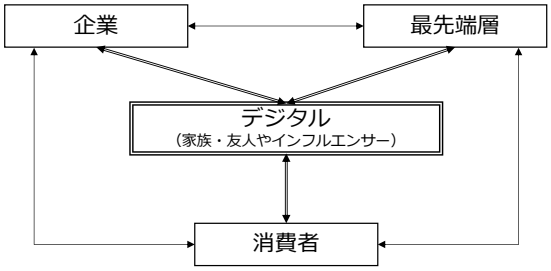

図 1 新しいコミュニケーションパターン

Vol.2020-DPS-182 No.37
Vol.2020-CSEC-88 No.37
2020/3/13

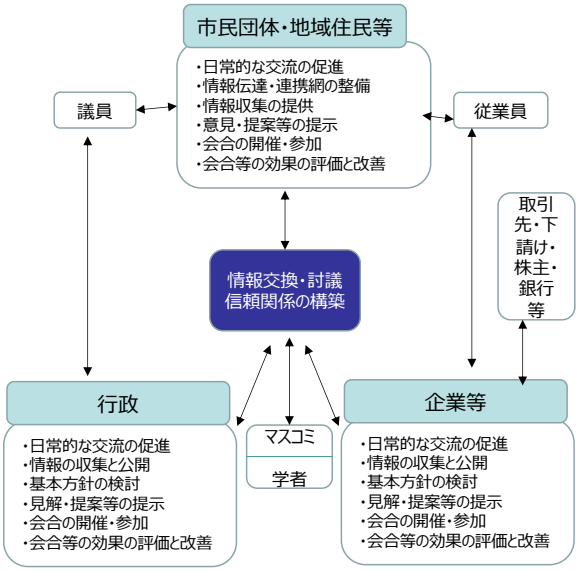

図 2 これからのリスクコミュニケーション

エンスカフェやワークショップなど、啓発の場や、行政が市民に対して意見収集を行うコンセンサス会議などのコミュニケーションの場づくりも進んできている。

このような双方向コミュニケーションの場において、どのような情報伝達が必要かについて、木下・吉川（1990）による、「リスクコミュニケーションのパラダイム」に加筆したものが図 3 である。

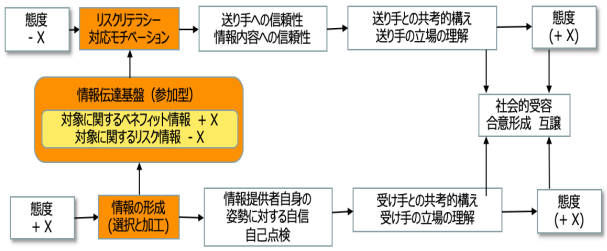

図 3 情報伝達とコミュニケーション基盤に着目したリスクコミュニケーションのパラダイム

木下・吉川のパラダイムは、送り手・受け手の態度、お互いの立場の理解、両者の信頼性の度合いなどに、伝達する情報のベネフィットとリスクの度合いを考慮したものとなっていた。このパラダイムは主に、両者の「人間関係」や「感情」に焦点を当てたものと理解できる。しかし、利害関係者が多数になり、IT の進展の中で直接の接触が難しいことも予想される昨今、人間関係だけでコミュニケーションの要素を語り尽くすことは難しい。そこで本論においては情報伝達の基盤や、伝える情報そのもの、受け手のスタンスに注目し、「送り側の情報の形成」「参加型の情報伝達基盤」「受け手側のリスクリテラシーと対応モチベーション」を追加したい。以降、これらに注目した、サブスクリプション型サービスにおけるセキュリティリスクコミュニケーションについて議論を進めていく。

4. サブスクリプション型 IT サービスにおけるセキュリティリスクコミュニケーション

4.1 セキュリティ機能の提案とコミュニケーション基盤構築

先に述べたように、コト消費の進展により、一般の利用者はモノ自体への興味を失い、自らの「ジョブ」を解決するためのサービス利用のみに興味を抱く。つまり、利用者は翻訳結果を得たいから翻訳サービスを使うのであって、翻訳サービスの内容やセキュリティの仕様を勉強したいわけでは無い。だから、懇切丁寧に記載された利用規約を読むことは、利用者の目的ではないのである。つまり、この研究の前段で述べてきた、利用者にサービス利用上のリスクを正しく理解してもらうために、サービス提供者が必要なリスク情報を「伝える」ということには限界がある。情報弱者である一般消費者が、サイバーの世界における新たなリスクを踏まえつつ仕様や品質を継続的に理解し、種々雑多な IT サービスを選定し続けるのはかなりの負担になることが考えられる。これらが一般消費者の努力のみに任せられている状態は放置されるべきではない。

むしろ、提供者はこのような利用者に寄り添い、契約を継続してもらうための工夫が必要である。利用者が本来求めている機能ではないセキュリティ機能に注意してもらうためには、理解してもらうのではなく、利用に支障がでないセキュリティ仕様を能動的に「提案」していくしかないと考える。サービスを利用する上での安全性は、基本的なものは提供者が責任をもって提供すべきであり、安全性のレベルが選択できるものについては、どのような選択をすべきかを提供者がリコメンドしていく必要がある。加えて、内容によりコストをかけて対策すべきものは、オプションとして有料で提供することも視野にいれていく必要がある。

水越他(2018)は、家電 IoT 機器の大量性と管理者不在による「Cyber Debris 化」の危険性への対応のため、情報セキュリティ向上ビジネスモデルに関する提案を行なっている。すなわち、家電 IoT 機器についてレンタル形態でサービスを提供し、提供者が実質的管理者として、脆弱性パッチの適用を含めたアップデートを行うということである。このモデルはインターネット全体での安全性の向上に非常に有益であり、セキュリティ対策意識が高い利用者に受け入れやすいモデルと考えられる。このようなモデルが一般的になり、ソフトウエア 管理対策のみならず、情報管理他のリスク対策も含めて利用者に訴えることができないだろうか。

4.2 今後の展開について

今後の研究においては、さらに進展していくと考えられ

るサブスクリプション型の IT サービスにおいて、提供者と利用者間の情報の非対称性を解決するために、リスクコミュニケーションをいかに進めるべきかについて、先に挙げた「送り側の情報の形成」「参加型の情報伝達基盤」「受け手側のリスクリテラシーと対応モチベーション」に着目し、提案型のセキュリティと、コミュニティ基盤の形を論証し、提案していきたい。全体イメージを図 4 に示す。

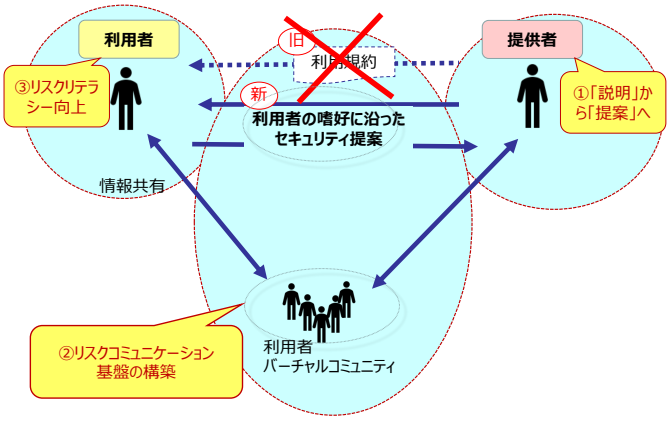

図 4　IT サービス提供者と利用者のリスクコミュニケーション基盤

先出の水越他の研究においては、レンタルでの IoT 機器提供の主目的は提供者による漏れない脆弱性パッチ適用であった。しかし本研究の目的は、2.1 において既に述べたように誤用を避け利用者の目的を達成することであり、製造物責任による提供物の瑕疵担保のみに留まらない。従い、提供者が利用者の行為をカバーするのみには留まらないことに注意が必要であり、それゆえ双方向のリスクコミュニケーションを確保すべきと考える。

リスク説明は単なる「利用規約」ドキュメントで一方的に伝えるものではなく、専門家が責任をもって提供する実効性のある対策でなければならない。提供者・利用者が双方歩み寄り、双方が理解し合えるコミュニケーションの在り方について今後探究していきたい。

参考文献

[1] 藪下史郎、「非対象情報の経済学」、[キンドル版]、検索元 amazon.com（藪下史郎（2002 年）第 3 章、1 項、4 段落、第 5 章、1 項、9 段落）
[2]日本経済新聞、「翻訳サイト入力の情報、閲覧状態に中央省庁や大手メーカー」（2015/2/20 付）、<https://www.nikkei.com/article/DGXLASDG20H2X_Q5A220C1CC0000/>、2019 年 6 月 1 日アクセス
[3]HUFFPOST、「翻訳サイトに入力した内容、丸見えだった不倫の示談や給与情報も」（2015/2/20 付）、<https://www.huffingtonpost.jp/2015/02/20/translation-online-service_n_6718922.html>、2019 年 6 月 8 日アクセス
[4] 独立行政法人情報処理推進機構(IPA)セキュリティセンター、「情報セキュリティ 10 大脅威 2016」、2016 年 3 月、p. 47
[5] National Research Council, Improving risk communication. Washington, DC: National Academy Press, 1989(林裕造・ 関沢純監訳 「リスクコミュニケーション- 前進への提言- 」、化学工業日報社、1997、p25
[6]近本一彦、「リスクコミュニケーションの現場における苦悩」日本リスク研究学会誌 18（2）：2008 年、pp. 23－31
[7]消費者庁、「製造物責任（PL）法の逐条解説」、2018 年 9 月、第 2 条（定義）
[8]Leverett, Clayton, Anderson(2017), Standardisation and Certification of the ‘Internet of Things’, Proceedings of WEIS 2017 (2017).
[9]谷口展郎、「ソフトウェアの製造物責任とオープンソースソフトウェアに関する一考察」、社団法人情報処理学会研究報告、2015-EIP-28(4)、2005 年、pp. 17-24
[10]島成佳、小松文子、高木大資、北村浩、「防護動機理論を援用したボット対策促進メッセージによる受信ユーザの態度変容要因の抽出と知識による影響の分析と検証」、情報処理学会論文誌 vol.53 No.2, 2011 年、pp.485-493
[11]Commerce Times as of Jun 15, 2001. Does Anyone Read Online Privacy Policy? https://www.ecommercetimes.com/story/11303.html
[12]経済産業庁、「消費者理解に基づく消費経済市場の活性化」研究会報告書、2016 年、pp. 6-11
[13]川上昌直、「『つながり』の創りかた」、東洋経済新報社、2019 年
[14]コトラー、「コトラー のマーケティング 4.0」、朝日出版、2017 年
[15]新津重幸、「日本型マーケティングの進化と未来：ビジネスパラダイムの変革とマーケティングの戦略的変革」、白桃書房、2017年
[16]浦野統平、「化学物質に関するリスクコミュニケーションの変遷」、2001 年
[17]木下冨雄・吉川肇子、「リスクコミュニケーションによる認知行動の変化(3)」、 日本社会心理学会第 31 回大会発表論文集、1990 年、PP. 162-163
[18]水越一郎・クロサカタツヤ、「家電 IoT のセキュリティ向上ビジネスモデル～レンタル形態による家電 IoT 提供がもたらす管理品質の改善」、2018 年春季全国研究発表大会、2018 年、pp150-153