

Society 5.0 における信頼

神橋基博¹

概要 : Society 5.0 において, IT サービスは複数の組織のつながりにより提供されることから, ある組織における IT ガバナンスに対する信頼の欠如は他の組織の IT サービスの品質や安定性に影響を及ぼすこととなる. 信頼に関する用語としては Reliability と Trustworthiness があるが, 本稿において, 確率論の観点から Society 5.0 における信頼は Trustworthiness であることを示し, IT サービスに関する信頼の推定方法について提案する.

キーワード : Society 5.0, 信頼, 信頼性, Reliability, Trustworthiness, ベイズ定理

Trust in Society 5.0

MOTOHIRO KAMBASHI^{†1}

Abstract: As IT services are provided by multiple organization connections in Society 5.0, the lack of trust in IT governance of one organization will affect quality and stability of IT services in other organization. Reliability and Trustworthiness are terms related to Trust. In this paper, it is showed that Trust in Society 5.0 is Trustworthiness from the viewpoint of probability theory, and proposed a method for estimating Trust of IT services.

Keywords: Society 5.0, Trust, Reliability, Trustworthiness, Bayes' theorem

1. はじめに

デジタル技術によって変革を遂げた社会である Society 5.0 において, IT サービスは複数の組織に跨る IT システムが連携することによって提供される. そのため, ある組織が提供する IT サービスで障害が発生すると, その IT サービスを利用する他の IT サービスにも障害の影響が波及する恐れがある. また, ある IT サービスにおける脆弱性は, その IT サービスを利用する他の IT サービスのセキュリティを低下させる恐れがある.

例えば, 2020 年 9 月に発覚したドコモ口座事件においては, 「ドコモ口座」という IT サービスを入口とし, 複数の組織に跨る以下の”弱い”ポイントが結び付けられたために, 銀行口座から不正に預金引き出されてしまったことが指摘されている. [1]

- ・ NTT ドコモは回線契約があることを前提で作られていたサービスを, 誰でも作れるキャリアフリーアカウントにまで開放した.
- ・ 資金移動業者が残高をチャージする際に, 銀行が提供する「Web 口座振替」での認証作業をもって本人確認完了とみなしていた.
- ・ 銀行によって「Web 口座振替」のセキュリティに差があり, 本人確認項目の弱い銀行が狙われた.

この事例が示すように, 自社の IT サービスにおけるセキュリティや安全性等を確保するためには, 自らの IT ガバナンスおよび IT マネジメントを発揮するだけでなく, IT サービス

の接続する先の組織において, セキュリティや安全性等を確保するだけの IT ガバナンスおよび IT マネジメントが発揮されていることも必要となる. しかしながら, 一般的に他組織の IT ガバナンスおよび IT マネジメントを直接確認することには限界があり, 相手の組織への信頼に頼らざるを得ない面がある. また, 情報セキュリティに対する信頼を支えるものとして, ISMS 等の認証制度が存在するものの, Society 5.0 における組織の IT ガバナンスや IT マネジメントを保証する制度は存在しない.

このような状況を改善するため, 本稿では IT サービスを提供する組織への信頼形成過程を対象とし, ベイズ定理[a]を用いて信頼形成過程を数理的に表現するモデルを用いて, 組織間における信頼を考察する.

2. 信頼概念の整理

2.1 信頼と信頼性

信頼は人間が円滑な関係を結ぶ上で重要な役割を果たしているものの, 信頼は研究者によって異なる多義的な概念で

a) ベイズ定理とは, 確率論における定理であり, 英国の Thomas Bayes(1710-1761)の名にちなんでいる. ベイズ定理を意思決定に役立てることを「ベイズ的意思決定」と呼び, 経済学, 工学, 医学等の広い分野で応用されている. ベイズ定理においては, $P(A|B)$ を事象 B が真であるときに事象 A が発生する確率, $P(A)$ および $P(B)$ を前提条件無しで事象 A および事象 B が発生する確率とする時に, 原因と推測される事象を C_i , 発生した事象を E_k とすると, 事象 E_k が発生した原因が C_i である確率 $P(C_i|E_k)$ は以下の式で表される.

$$P(C_i|E_k) = \frac{P(C_i)P(E_k|C_i)}{\sum_j P(C_j)P(E_k|C_j)}$$

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

あることが指摘されている。[2][3][4]

山岸は、信頼(trustfulness)と信頼性(trustworthiness)を区別し、「信頼」は信頼する側すなわち信頼者(truster)の属性であり、「信頼性」は信頼される側すなわち被信頼者(trustee)の属性としている。[5]

また、山岸によると、そもそも他者に対する信頼が必要となるのは、相互作用を行う相手に裏切る要因があり、相手の意図についての情報が必要とされながらそれを十分に得ることができない状況、すなわち社会的不確実性の高い状況である。この社会的不確実性に対する効果的な対処法として、特定の相手とコミットメント関係の形成がある。特定の相手との間にコミットメント関係、すなわち長期的な関係を築けば、互いに相手を裏切ることによって短期的な利益を追求する誘因が客観的に低くなり、相手の有効的な行動を期待することができるようになる。この場合の相手の有効な行動に対する期待は、裏切らない方がその相手にとって得になるだろうという、相手の自己利益の客観的な評価に根差したものであり、山岸はこれを「安心」と定義し、「信頼」とは異なるものとし、「安心」のように相手が自分に友好的に振る舞ってくれるだろうという考える客観的な根拠がないにも関わらず、相手の意図についての肯定的な信念のゆえに抱く期待を「信頼」と定義した。[6]

その上で、他者に対する「信頼性」について、「信頼」が必要となる社会的な不確実性において、特定の他者が相互作用の相手に多大な損害を与えるような自己利益追求行動を行うかどうかを正確に予測すること[7]と定義した。また、特定の相手に対する「信頼性」とは別に、相手についての情報がない場合の相手の信頼性に対する"デフォルト推定値"を「一般的信頼」(general trust)と定義した。[8]

清成・山岸らは、日米における心理学的な実験結果の比較研究より、「信頼」と「信頼性」に一貫した関係が存在しないことを示した。[9]

2.2 Reliability と Trustworthiness

山岸らの研究では、「信頼性」の訳語として Trustworthiness を用いているが、一般的に信頼性と訳される語として Reliability がある。

Reliability も Trustworthiness も研究者によって異なる概念として議論されている。

Moralres らによるインターネット上のコミュニティを対象とした研究では、Reliability をコミュニティにて発言を行う利用者の属性として、Trustworthy を利用者の発言に対する形容詞として用いている。[10]

Golafshani による社会調査手法に関する検討においては、研究対象に対して、時間経過に対して一貫した結果を得られ、かつ同じ手法で繰り返し同じ結果が得られることを Reliability であると定義する一方、Trustworthiness を研究それ自体の属性として用いている。[11]

IT サービスに関連する信頼性として、JIS Z 8115:2019 ではサービス信頼性(Service reliability)を「利用者に対し提供されるサービスが、与えられた条件の範囲で、与えられた期間、支障なく遂行できる能力」として定義し、サービス信頼性の尺度として、信頼度、故障率、故障強度、平均寿命、MTTF、MTBF、アベイラビリティなどが挙げられている。それぞれの尺度は確率、期待値、期待値の極限值等として定義している。このことから、JIS Z 8115:2019 における信頼性は確率に基づく計量的な概念として認識されていることが判る。

Trustworthiness を JIS では定義していないものの、日本から ISO に提案した IoT に関する国際規格「ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes」には含まれており、IPA は「トラストワージネス」を、「セキュリティ、プライバシー、セーフティ、リライアビリティ、レジリエンスなどによって、システムがその関係者の期待に応える能力」と説明している。[12]

一方、セキュリティマネジメントシステムに関する JIS 規格である JIS Q 27001:2014 は、組織の情報セキュリティマネジメントシステムに対して「リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を維持し、かつ、リスクを適切に管理しているという信頼を利害関係者に与える。」と述べており、信頼とは組織のマネジメントシステムによって与えられるものとしている。この定義において、前節における山岸による「信頼」の定義における個人の「意図」に該当するのが、組織におけるマネジメントシステムとなる。したがって、組織のガバナンスあるいはマネジメントシステムに対する肯定的な信念のゆえに抱く期待が、組織に対する「信頼」であり、組織に対する「信頼性」を社会的な不確実性において、組織が相手に対して自己利益追求行動を行うかどうかに関する予測(期待)となる。このような組織の「信頼」および「信頼性」に対する定義より、「トラストワージネス」の定義における「システム」とは、ハードウェア・ソフトウェア・ネットワーク等によって構成される狭義の IT システムではなく、組織のガバナンスあるいはマネジメントシステムを指していることが判る。

以上より、IT サービスにおける Reliability は狭義の IT システムを対象とした信頼性であり、Trustworthiness は IT サービスを提供する組織のガバナンスあるいはマネジメントシステムを対象とした信頼性として対応づけられる。

2.3 信頼と確率

前節において、IT サービスにおける Reliability とは狭義の IT システムを対象とした信頼性であり、確率に基づく計量的な概念として認識されていることを示した。それでは Trustworthiness は、同様に確率として取り扱うことは可能

だろうか。

確率論において、確率には客観確率と主観確率が存在する。客観確率とは、私たちが一般的に確率として認識する概念であり、ある事象が生起する度数が先験的に分かっている、あるいは統計的な観察を続けた結果として得られる相対度数である。一方、主観確率とは、ある事柄の生起に対する個人の確信の度合である。例えば「このプロジェクトは99%失敗する」という文章において、発言者はプロジェクトが失敗する確率を理論的・統計的に99%と見積もっているのではなく、プロジェクトの失敗に対する確信を99%として表明している。このような確信の強さを表す概念が主観確率である。

前節において「トラストワージネス」における信頼を組織のガバナンスあるいはマネジメントシステムに対する肯定的な信念のゆえに抱く期待として定義した。主観確率における確信とは、信念と同義であり、Trustworthiness は主観確率に属する概念である。

以上より、本稿において、Reliability は狭義の IT システムの信頼性であり、客観的確率を用いて表現される概念であるのに対して、Trustworthiness は IT サービスを提供する組織のガバナンスあるいはマネジメントシステムの信頼性であり、主観的確率を用いて表現される概念として対比することが可能となる。また、本稿が対象とする Society 5.0 における組織間のつながりにおける信頼および信頼性は Trustworthiness すなわち主観確率によって表現されることとなる。

2.4 ベイズ定理による推定

前節の通り、組織間のつながりにおける信頼を主観確率として捉える場合、その確率分布を得ることは不可能である。このような確率を推定するための手法の一つがベイズ推定であり、注 a) の通り、ベイズ定理を用いて発生した事象からその原因を推定する。例えば、IT サービスの利用者が、IT ガバナンスが十分な組織では障害の発生確率が低く、不十分な組織では障害の発生確率が高いという信念を有している場合、一定期間に発生した障害の有無を用いて、組織の IT ガバナンスが十分であったかどうかを推定する。

この時、IT ガバナンスが十分であった確率とは、利用者の信念の度合いを示す主観確率であり、IT サービスを提供する組織に対して利用者から見た Trustworthiness となる。

このようなベイズ推定を繰り返すことで、組織に対する信頼を更新する過程を山形らは信頼形成過程[13]とし、原子力発電所に対する信頼をモデル化したものの、なぜ、ベイズ推定を行うのか理論的な説明は行っていない。

次章では、金融機関におけるオープン API による電子決済等代行業者（電代業者）との接続を事例とし、金融機関の電代業者に対する信頼形成過程の推定を試みる。

3. 金融機関におけるオープン API の分析

3.1 分析の対象

家計簿ソフト等を提供する FinTech 企業は、顧客の口座残高等を取り込むため、スクレイピングと呼ばれる技術を用いて、顧客に成り代わって金融機関にアクセスするサービス（アグリゲーション）を提供していた。

アグリゲーションによって、金融機関の IT サービスにアクセスするための ID/パスワードを第三者に預けることになることから、金融庁は 2017 年に銀行法を改正し、FinTech 企業に電代業者としての登録を求めるとともに、銀行に対して、図 1 のような、より安全な接続方式であるオープン API を電代業者に提供する努力義務を課した。

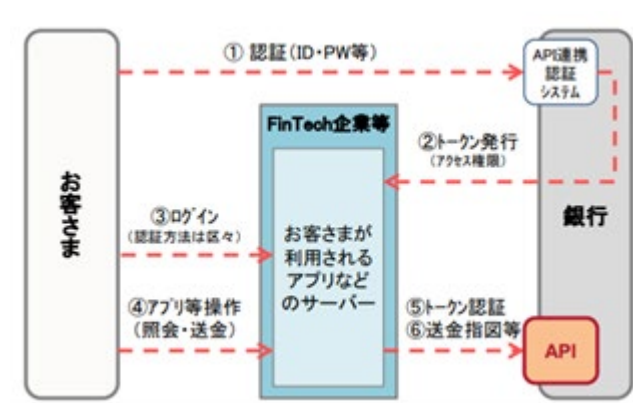


図 1 金融機関によるオープン API [14]

3.2 信頼形成過程

金融機関にとって、電代業者の利用者は自社の顧客であり、オープン API を提供する電代業者は、自らの提供する IT サービスに適切な投資を行い、安定稼働に向けた適切な管理を行っている等、十分な IT ガバナンスを発揮している先を選択することが望ましい。金融情報システムセンター (FISC) は、オープン API を提供する金融機関および利用する FinTech 企業の双方が安全対策に関するコミュニケーションを図るためのツールとして「API 接続チェックリスト」および「金融機関と API 接続先のための API 接続チェックリスト解説書」を公開している。しかしながら、電代業者が利用者に利便性を提供するためには多数の金融機関と接続する必要があり、各金融機関が自らチェックリストを用いて電代業者の安全対策を直接点検することは困難である。また、電代業者が実施した点検結果を金融機関が受領したとしても、結果の適切性を保証する仕組みが存在しない。そのため、各金融機関は電代業者の IT サービスで発生した障害等のインシデントという観測された事象を用いて、電代業者における IT ガバナンスが十分かどうかを推定する。金融機関は IT ガバナンスが十分な電代業者と不十分な電代業者について表 1 のように考えており、接続開始時点に

において、電代業者における IT ガバナンスが十分である確率 p_0 を 50%と考えていると仮定する。

	1年間インシデント が発生せず(E_1)	1年間にインシデ ントが発生(E_2)
ITガバナンスが十分な 電代業者(C_1)	99.9%	0.1%
ITガバナンスが不十分 な電代業者(C_2)	50%	50%

表 1 電代業者の IT ガバナンスに関する信念

金融機関は 1 年毎にベイズ定理を用いて、電代業者の IT ガバナンスに対する推定を更新するものとする。この時、図 2 の通り、インシデントが発生しないケースにおいては、電代業者の IT ガバナンスが十分である確率は時間経過とともに上昇する。この時、金融機関から見た電代業者の IT ガバナンスが十分である確率が、電代業者に対する信頼であり、障害が発生しない限り、電代業者への信頼は時間とともに向上する。これがオープン API における信頼形成過程である。

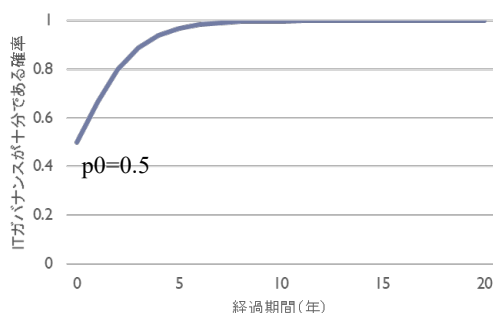


図 2 インシデントが発生しなかった場合における電代業者の IT ガバナンスが十分である確率

3.3 インシデントの発生による信頼形成過程への影響

一方、インシデントが発生すると金融機関から見た電代業者の IT ガバナンスが十分である確率は低下する。低下幅は、図 3 および図 4 に示す通り、事前確率が高い程、低下幅は小さくなり、回復に要する期間は短縮される。

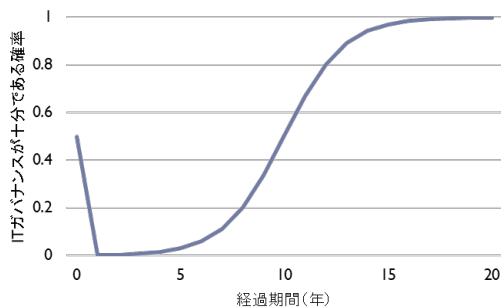


図 3 1 年以内にインシデントが発生した場合

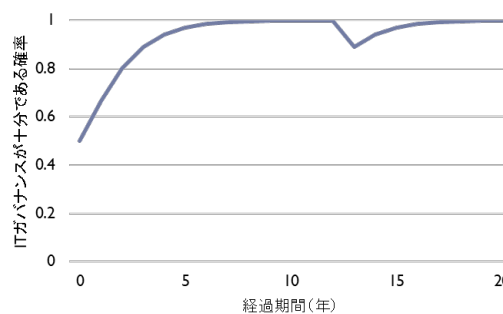


図 4 12 年後にインシデントが発生した場合

3.4 過度な期待による信頼形成過程への影響

図 2 から図 4 において 1 年間インシデントが発生しない確率 $P(E_1|C_1)$ は、金融機関から見た電代業者の能力への期待であり、前章で検討した Trustworthiness である。反面、図 5 に示す通り、電代業者への期待が高いほど、インシデントが発生した時の低下幅は大きくなり、信頼形成に要する期間も長くなる。

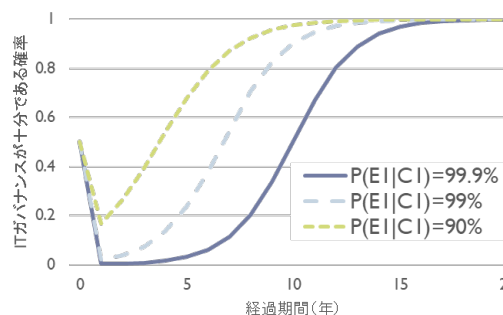


図 5 電代業者への期待による信頼形成過程の差異

4. まとめ

4.1 本稿の意義

本稿では、信頼および信頼性に関する概念を整理し、IT サービスに対する Reliability は、狭義の IT システムに対する信頼性、Trustworthiness は、IT サービスを提供する組織の IT ガバナンスあるいは IT マネジメントプロセスに対する信頼性として対応づけた。また、Reliability は客観確率に属する概念であり、Trustworthiness は主観確率に属する概念であることを示した。主観確率とは個人の信念の度合いであり、確率分布を得ることができず、ベイズ理論を用いた推定が必要となる。以上の概念整理により、組織に対する信頼の推移について、ベイズ推定を用いる信頼形成過程という山形等のアイデアに理論的な裏付けを与えることが可能となった。

金融機関におけるオープン API 事例に対する分析から、信頼の形成には時間を要し、初期のインシデント発生は、信頼の大幅な低下に繋がる。そのため、電代業者は接続開始後しばらくの期間、未然防止に注力することが望ましいこ

とが示された。

一方、金融機関が電代業者の IT ガバナンスに対して過剰に高い期待を持つことは、インシデントが発生した際の信頼低下が大きくなり、電代業者との関係が不安定になる恐れがある。そのため、セキュリティだけでなく IT サービスについても「ゼロトラスト」[15]のように、敢えて「信頼できないもの」として検証するアプローチが有効となる。

4.2 今後の展望

本稿から得られる知見はシステム管理の現場における経験則としては珍しいものではないが、理論的な説明を試みた点に新規性がある。

また、本稿で用いた信頼形成過程のモデルは信頼する側と信頼される側が 1 対 1 とするシンプルなモデルであった。今後、1 対多、多対多とモデルを拡張するとともに、信頼される側からのシグナリングといった働きかけをモデルに組み込むことで、より現実に近いモデル化が可能となることが期待される。本稿で得られた知見をベースとし、更なる拡張に取り組みたい。

参考文献

- [1] 鈴木淳也,「ドコモ口座」事件の教訓はこれからのキャッシュレス業界をどう変えるか, ITmedia, 2021 年 2 月 9 日
<https://www.itmedia.co.jp/news/articles/2102/09/news048.html>
- [2] 山岸俊男,信頼の構造 こころと社会の進化ゲーム, 東京大学出版会, 1998 年, p.31
- [3] 清成透子, 山岸俊男, 分配委任ゲームを用いた信頼と信頼性の比較研究, 社会心理学研究, 1999 年, 第 15 巻第 2 号, pp.100
- [4] 石川博康,「信頼」に関する学際的研究の一動向, COE ソフトロー・ディスカッション・ペーパー・シリーズ, 2004 年, p.2
- [5] [2], p.48
- [6] [2], p.47-48
- [7] 菊地雅子, 渡邊席子, 山岸俊男, 他社の信頼性判断の正確さと一般的信頼—実験研究, The Japanese Journal of Experimental Social Psychology, 1997 年, Vol. 37, No. 1, pp.24
- [8] [2], p.42
- [9] [3], pp.106-107
- [10] MORALES, Alex, et al. CrowdQM: Learning aspect-level user reliability and comment trustworthiness in discussion forums. Advances in Knowledge Discovery and Data Mining, 2020, 12084: 592.
- [11] GOLAFSHANI, Nahid. Understanding reliability and validity in qualitative research. The qualitative report, 2003, 8.4: 597-607.
- [12] IPA, IoT 製品・サービスにセキュリティ・セキュリティ等を実装するプロセスが国際標準として出版 ～日本提案の規格が国際標準化団体 ISO/IEC にて出版～, 2021 年 6 月 21 日
<https://www.ipa.go.jp/ikc/info/20210621.html>
- [13] 山形浩史, 神田啓治, 原子力開発における信頼形成過程に関するベイズ的考察, 日本原子力学会誌, 38(8), 1996 年, pp.683-688.
- [14] 全国銀行協会, オープン API のあり方に関する検討会報告書—オープン・イノベーションの活性化に向けて—, 2017 年, p.6, 図表 1
- [15] PwC あらた有限責任監査法人, ゼロトラストの現状調査と事例分析に関する調査報告書, 2021 年 3 月 31 日
<https://www.fsa.go.jp/common/about/research/20210630/zerotrust.pdf>