4F-01

IT サービスにおける信頼概念

神橋　基博†
情報セキュリティ大学院大学　客員研究員†

1. はじめに

デジタルトランスフォーメーション(DX)によって変革を遂げた社会である Society 5.0 では、様々な IT サービスが相互運用されることから、セキュリティを確保するために、情報・技術に加えて IT サービスを提供・利用する組織のつながりにおける信頼の確保が求められる。[1]
一方、このような信頼の確保はセキュリティリスクに限定されるものではない。例えば、開発プロジェクトの遅延、サービスレベルの低下といった IT ガバナンス・IT マネジメントに起因するリスクは他の組織のサービスの品質や安定性にも影響を及ぼすこととなる。しかしながら、セキュリティマネジメントについては ISMS 等の認証制度が整備されているものの、IT サービスを提供する組織の IT ガバナンス・IT マネジメントに対する信頼を確保するための制度や具体的な指針は存在しない。
本稿では IT サービスを提供する組織に対する信頼概念を主観確率に基づくものとして位置づけ、ベイズ定理を適用することで、組織間の信頼形成をモデル化することを提言する。

2. 信頼に関する 2 つの概念

IT サービスへの信頼には2つの概念が存在する。信頼性(Reliability)は JIS において、「アイテムが，与えられた条件の下で，与えられた期間，故障せずに，要求どおりに遂行できる能力」と定義されている。[2]
トラストワージネス(Trustworthiness)は、近年提唱されるようになった概念であり、「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」とされている。[3]
この 2 つの概念を比較すると、信頼性は技術によって実現される IT サービスの能力に関する概念である一方、トラストワージネスは IT サービスを提供する組織の能力に関する概念であることが判る。この違いは、信頼性については故障率や稼働率、MTTR(Mean Time Between Failure)といった客観的な指標によって測定可能であるのに対し、トラストワージネスについて同様の指標を定義できないという点にも表れる。
確率論、統計学においては、この違いを客観確率および主観確率として区別する。客観確率とは生起する度数が先験的に分かっている場合の確率、および統計的な観察を続けた結果として得られる相対度数を意味するのに対し、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を意味する。
主観確率は、理論や実験によって求めることができないために、ベイズ定理[a]を用いた推定が行われる。したがって、トラストワージネスに基づく信頼はベイズ定理に基づいて推定する必要がある。
組織への信頼についてベイズ定理を用いた推定を試みた先行研究として、山形他(1996)では、原子力発電所に対する信頼をベイズ定理に基づいて推定することを試みた。[4]
次節では先行研究を参考に IT サービスを提供する組織への信頼を推定することを試みる。

3. 金融 API における信頼

家計簿ソフト等を提供する FinTech 企業は、2017 年の銀行法改正により、FinTech 企業は電子決済等代行業者（電代業者）としての登録が求められるとともに、金融機関には電代業者に対して、より安全な接続方式であるオープン API を提供する努力義務が課された。

Concept of Trust on IT service
† Motohiro Kambashi, Institute of Information Security

[a] ベイズ定理とは、発生した事象に関する事前の知識に基づいて、その事象の発生確率を求めるものである。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 Ci、発生した事象を Ek とすると、事象 Ek が発生した際の原因が Ci である確率 P(Ci|Ek)は以下の式で求められる。

$$P(Ci|Ek) = \frac{P(Ci)P(Ek|Ci)}{\sum_i P(Ci)P(Ek|Ci)}$$

金融 API において、金融機関は自らのインターネットバンキングサービスに、電代業者が接続することから、電代業者におけるシステム障害およびサービスレベルの低下は自社の顧客に影響を及ぼすこととなる一方、金融機関は電代業者の IT ガバナンスが十分であるかを直接的に知ることができない。
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より、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、接続開始時点において、電代業者における IT ガバナンスが十分である確率を 50%と考えていると仮定する。

表 1 電代業者の運用状況に関する確率

	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%

金融機関は 1 年が経過する毎にベイズ定理を用いて、IT ガバナンスに対する推定を更新すると、接続開始以降、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は図 1 となる。

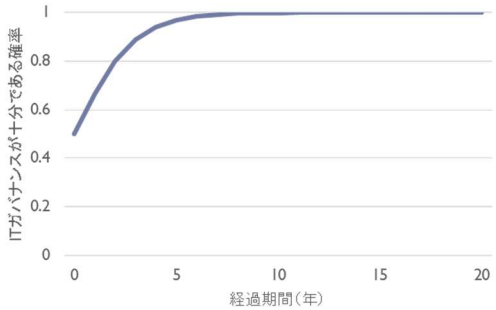

図 1 インシデントが発生しなかった場合における
電代業者の IT ガバナンスが十分である確率

この、金融機関からみた電代業者の IT ガバナンスが十分である主観確率に対する更新を繰りかえす過程を山形他(1996)では、信頼形成過程と名づけており、この確率が IT サービスを提供する組織に対するトラストワージネスの指標となると考えられる。
一方、インシデントが発生すると電代業者の IT ガバナンスが十分である確率は低下する。図 2 および図 3 に示す通り、IT ガバナンスが十分である確率が高い程、インシデントが発生した時の低下幅は小さくなり、インシデント発生前の水準まで確率が回復に要する期間が短縮する。

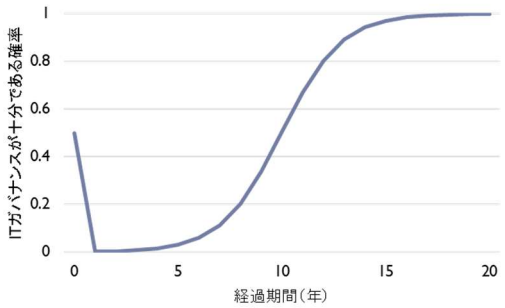

図 2 1 年以内にインシデントが発生した場合

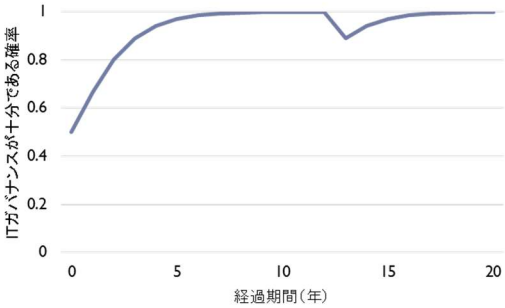

図 3 12 年後にインシデントが発生した場合

4. まとめ

本稿では IT サービスを提供する組織への信頼を主観的確率に基づくものと捉え、ベイズ定理を用いることでモデルの推定を試みた。
今回用いたモデルはインシデント発生のみを考慮した非常に単純なものであるが、ベイズ定理による推定は様々な分野で活用されている。
他分野の知見を活用し、今後は、IT サービスの信頼の向上に向けた施策に対する有効性評価に取り組んでいきたい。

〈参考文献〉

[1]経済産業省(2019), サイバー・フィジカル・セキュリティ対策フレームワーク Society5.0 における新たなサプライチェーン（バリュークリエイションプロセス）の信頼性の確保に向けて, https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf
[2]JIS X 8115:2019
[3]IPA, IoT 製品・サービスにセーフティ・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～, https://www.ipa.go.jp/ikc/info/20210621.htm
[4]山形浩史, 神田啓治, (1996), 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), 683-688.