Computer Security Symposium 2019
21 - 24 October 2019

トラストの言語化を試みる
～トラストとセキュリティ技術の関係～

木村 泰司[1]　島岡 政基[2]　菅野 哲[3]　佐古 和恵[4]

概要：情報セキュリティに深く関連する言葉として「トラスト」がしばしば使われる．しかし，この言葉は多義的であり，使われ方によって解釈が異なるため，一見，つじつまがあっているようでいて，実際には話が合っていない事がある．トラストとセキュリティ技術の関係はどう位置付けられるのか．セキュリティ技術を使っているシステムやサービスにおけるトラストとは何なのか．本稿では，これらについて我々が考える定義やモデルを整理して示し，考察する．

キーワード：トラスト, PKI, 認証, セキュリティ

Defining Trust
- relationships with security -

Taiji Kimura[1]　Masaki SHIMAOKA[2]　Satoru Kanno[3]　Kazue Sako[4]

Abstract: "Trust" is often used as a word deeply related to information security. However, this word is ambiguous, and its interpretation differs depending on how it is used. How is the relationship between trust and security technology positioned? What is trust in systems and services that use security technology? In this paper, we organize and present the definitions and models we consider.

Keywords: Trust, PKI, Certification, Security

1. はじめに

「トラスト」という言葉は，様々な立場で，その都合に合わせて使われる．IT システムを提供する立場では顧客に対して「自分たちのシステムは信用に足るから使ってください.」という説得のために使われる．これまでに使われてきた「安心・安全」や「セキュリティ」より，新しい時代の言葉であるかのような表現として位置付けられている．これにより，前の時代には「セキュリティ技術」があっても「安心・安全」じゃなかったシステムには「トラスト」がなかった，あるいは，「安心・安全」をうたうシステムに足りなかったのは「トラスト」だった，という錯覚を起こすような言葉になっている．しかし「トラスト」が表すコンテキストを明確にしてみると，時代や錯覚といったみなし方による思考停止を招かずに，具体的に議論を積み上げることが可能であると考える．

IT システムやサービスを利用する利用者目線で「トラスト」を考える観点と，IT システムやサービスを提供する技術者目線からの観点の２つが考えられる．

1 一般社団法人日本ネットワークインフォメーションセンター
Japan Network Information Center
2 セコム株式会社 IS 研究所
Intelligent Systems Laboratory, SECOM CO., LTD.
3 株式会社レピダム
Lepidum Corporation
4 NEC セキュリティ研究所
NEC Security Research Labs

システムの利用者目線では，「利用者」が「IT システムが安全であること」を「他の人も問題なく使えている状況で，安全でなければ運営者の評判が落ちるだろうから」信頼し，その「IT システム」を利用するのかもしれない．一方で，利用者は「信頼しないとサービスが使えない」から「IT サービス」を利用するかもしれない．この場合は，はたからみると，サービスを信頼しているように見えるだろう．

システムを提供する技術者目線では，技術者が自分の手の及ばないところを「トラスト」せざるを得ない場面が多い．あるいは，すべてのセキュリティ技術で凝り固めてしまうと，コストが高い開発になってしまう場合もある．RSA 暗号を使う場面を例にとると，「素因数分解が難しいこと」からはじまり，「正しくソフトウェア実装されていること」や「ハードウェアにウイルスが潜入していないこと」や「秘密鍵が漏えいするような運営がされないこと」などの様々な点を踏まえて，利用者に IT システムを提供している．

本稿は，これらの「トラスト」という概念の使われ方を踏まえて，言語化するための第一歩を試行するものである．まず 2 章でトラストとセキュリティ技術との関係を述べ，次に 3 章でトラストの関係性を整理するためのモデルを示す．4 章では一例として Web PKI を挙げて考察する．5 章で議論をまとめる．

2. トラストとセキュリティ技術の関係

ここで，ユーザ（利用者）はその情報（IT)システムあるいは運用されたものに対して，それが「トラスト」できるなら，サービスを利用するというシンプルなモデルで議論を始めたい. また, サービスを構成する情報システムには，それが安全に運用されるためにセキュリティ技術が活用されているものとする．そのサービスを利用したり提供するかどうかの判断や，判断のための観測を行う者をここではトラストの「主体」と呼び，その対象を「対象系」と呼ぶ．

主体（ユーザ）が，対象系のサービスに対する期待の持ち方を示したのが図 1 である．右上の主体（ユーザ）はセキュリティ技術を含む対象系を「トラスト」している．対象系は実際には要素技術で満たされてはおらず，その空いた部分のことが開発者・提供者目線では「トラスト」と呼ばれることがあった．しかし，この図ではユーザである主体のトラストとは表面(サーフェイス)に対して行われるものであることを示している．対象系におけるリスクや，次に述べるセキュリティ技術によって守られる範囲は，主体には必ずしも適切に認知されているとは限らない．

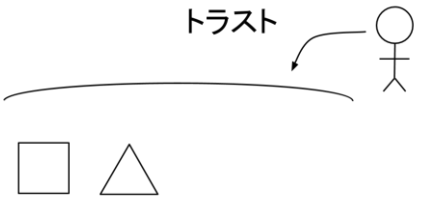

図 1　トラストのサーフェイス

この表面を下支えする情報システムの中身に対して，対象系の提供者は, セキュリティ技術を用いて対策を講じて，対策が取られていない範囲を少なくしていく．対象系の提供者もまたトラストの主体であり，要素技術を構成する技術に対する表面に接している(図 2 参照).

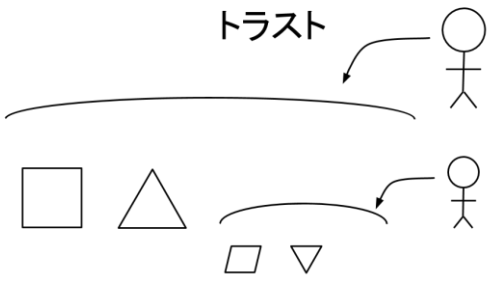

図 2　トラストの重層

いずれの層においても，セキュリティ技術で担保できる安全性の範囲が狭い場合，担保されていない脅威に対しては，自分の提供する対象系を利用する主体に対して「Trust Me」という具合に，トラストに頼らざるを得ない．

3. トラストの形態

次に主体と対象系の関係性について述べる．一つ目のモデルは，主体と対象系が一対一の，図 3 に示す最も単純なモデルである．これを「ベーシックモデル」と呼ぶ．

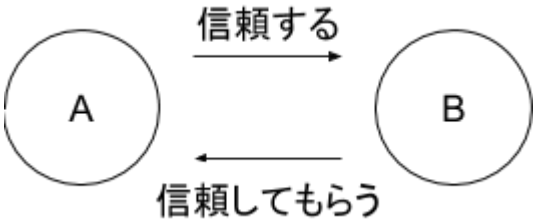

図 3　ベーシックモデル

この関係性において, まず A が何をもって B をトラストするのかという観点がある．この基本的なトラストの関係性は，主体である A が対象 B の備える能力や公正さ・誠実さをどのように認知しているかによって規定されることが知られている[1].

二つ目のモデルは，あるセキュリティ技術やその運用を内包するものを対象とする、図 4 に示すモデルである．ここでは「内包モデル」と呼ぶ．

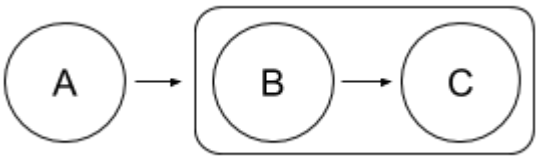

図 4　内包モデル

BはCを信頼し, 図4の丸四角で囲まれた部分に対して，A は期待した動作をするのかどうかといった判断を行う．内包モデルでは C の B に対する確からしさが, A の丸四角に対する信頼に影響する．A は丸四角の中を関知しなくてよい．C は更に別の技術や運用を内包することがある．

三つ目のモデルは，対象を介して信頼が推移する、図 5 に示すモデルである．これを「推移モデル」と呼ぶ．

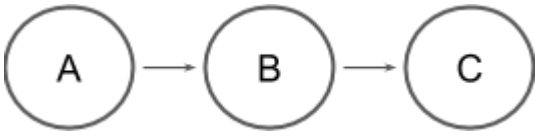

図 5　推移モデル

A が B を信頼するとき, B が信頼する C を A にとっても信頼し得る. B が C を信頼していることを前提に A が C を信頼する関係を，信頼の推移と呼ぶ．B と C の信頼関係が失

われた場合は，A と C の信頼関係もまた失われる．Pretty Good Privacy (PGP) などいわゆる Web of trust [2] は典型的な推移モデルとして知られている．

4. ケーススタディとしての Web PKI

サービス・システムのトラストを考えるにあたり，ここでは Web PKI における認証局システムを事例として扱うことにする．同システムは主に Web サーバに対して一定の身元確認を行った上で証明書を発行するシステムであり，Web サイトの利用者にとっては，当該証明書を発行された Web サーバであれば一定の信頼性aがあるとみなすことができる．即ち，Web サイトの利用者は当該認証局システムを信頼することで様々な Web サイトに対する信頼を容易に判断できることになる．この，Web PKI における認証局システムに対する信頼は，セキュリティ技術以外の要素も含めて重層的かつ明示的に構成されており，セキュリティ技術とトラストの関係性を考察する上でわかりやすい．

4.1 Web PKI の推移性

Web PKI における認証局システムは，一般的に図 6 に示すような階層構造を持ち，最上位の認証局はルート認証局と呼ばれる．実線は証明書発行(とそれに伴う間接的な信頼関係)を，破線は直接的な信頼関係を示す．Web ブラウザや OS 等の各ベンダは，所定の要件を満たすいくつかのルート認証局(の証明書)を各製品に予め格納しており，Web ブラウザや OS の利用者はこれらの下位認証局が発行するサーバ証明書を信頼することが容易に可能となる．

図 6　認証局の階層構造

ここで，利用者が信頼する対象として Web サイトと認証局の 2 種類が登場している．前述の通り利用者は認証局が身元確認した Web サイトだから信頼しているのであり，これは 3 節の内包モデルである．

4.2 ルート認証局(トラストアンカ)の重層性

一方で，ルート認証局に対する信頼は図 7 に示すように重層的である．ルート認証局が Web ブラウザや OS に予め格納されるためには，下位認証局も含め各認証局が認証局管理基準として知られる CA/Browser Forum の規定するいわゆる Baseline Requirements(以下 BR) [3] に準拠bする必要がある．

認証局管理基準では，技術，プロトコル，身元確認，ライフサイクル管理，監査について要件を規定しており，各認証局はこれを満たしていることを宣言するために，BR に準拠する形で証明書ポリシ(Certificate Policy)および認証局運用規程(Certification Practice Statements)(以下 CP/CPS)を規定・公開する必要がある．また，BR では定期的な外部監査を要件しているため，CP/CPS に準拠した運用管理が行われていることを外部監査人によって定期的に確認される．

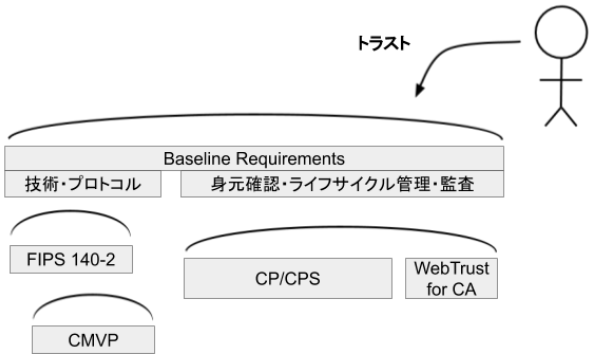

図 7　Web PKI のトラストの重層性c

主要な技術・プロトコルについては，例えば FIPS140-2 や Cryptographic Module Validation Program (CMVP)などの認定基準や，標準規格(RFC 5280, SP800-63 など)がそれぞれ定められている．現状では対象となる実装の多くは(不備がない限り)設計通りに動作するものであるため，認定取得や規格準拠などによって客観的な充足性を示しやすい．

一方で，身元確認やライフサイクル管理などは運用主体である組織や人の意思が介在するため，設計通りの振舞いが行われるとは限らない．このため CP/CPS に対する継続的な遵守を確認する必要がある．Web PKI では CP/CPS を遵守する形で継続的に運用管理が行われていることを担保するために，前述の定期的な外部監査を要件としている．

4.3 曖昧性を最小化した Web PKI

図 7 に示したように，利用者がルート認証局を信頼できるのは BR に準拠しているからであり，準拠性も技術やプロトコルはそれぞれに認定基準があり，重層的な関係にある．また，身元確認，ライフサイクル管理，監査については CP/CPS で運用方針が明文化され，当該規定への準拠性を定期的な外部監査によって担保する，という形でひも解くことができる．こうした関係性は，BR や CP/CPS などで明文化されていることによって客観的な評価が可能であり，曖昧な要素を最小化している．

Web PKI の大きな貢献のひとつは，技術やプロトコルといった客観性の高い要素だけでなく，身元確認，ライフサイクル管理，監査といった，従来は明文化されることの少なかった運用管理の要素についても CP/CPS で明文化する

a 例えばドメインの所有権を持っていることを保証する Domain Validation(DV)や，それに加えて法人格を有していることを保証する Extended Validation(EV)などがある．

b 正確には，BR は最低要件であり，これに加えて Web ブラウザや OS の各ベンダがそれぞれに課す大同小異の追加要件を満たす必要がある．

c 簡略化のため一部割愛

ことを求め，また明文化された CP/CPS への準拠性を外部監査によって担保することにより，一定の客観性を与えたことにある．不特定多数の利用者に高い信頼性を訴求するには，このように信頼にできるだけ透明性や客観性を与える枠組みを整備することが必要であろう．

5. おわりに

本稿では多義的に使われている現状の認識を踏まえ，モデルを紹介した．またそれらのモデルを踏まえて Web PKI の事例を通じて紹介した．「トラスト」が表す内容を，コンテキストを明確にして詳細に見てみると，具体的に議論を積み上げることが可能であるはずである．「誰」が「何がどうであること・何がどうでないこと」を「どういう前提」で「信頼」することを議論しているのか，そして「信頼」しているから，どういう「行動」をするのか，とブレークダウンしてみることをおすすめしたい．もしかしたら「信頼」はその「行動」をするために，自分自身を納得させるための理由なのかもしれない．あるいは，「信頼」が本当はなくても，はたからみて「信頼がある」ような行動をしているようにみえるのかもしれない．

言葉を都合よく使うのではなく，意味に対する期待のレベルを合わせていくことで，思考停止せずに，現実を良くしていけるような議論ができるように願いたい．

参考文献

[1] 中谷内一也．リスクの社会心理学―人間の理解と信頼の構築に向けて. 306p.. 有斐閣. 2012.

[2] Abdul-Rahman, Alfarez. “The pgp trust model. ” EDI-Forum: the Journal of Electronic Commerce. Vol. 10. No. 3. 1997.

[3] ---, “Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, v. 1.6.5,” CA/ Browser Forum, 16 Apr. 2019; https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.5.pdf.